CEL 51, DCCN, Monsoon 2020 Name : Prashansa Nalawade
Lab 2: Basic Network Utilities UID : 2019230067

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

```
C:\Users\Admin>ping -n 10 -l 64 google.com>Query.docs

C:\Users\Admin>
C:\Users\Admin>
C:\Users\Admin>
C:\Users\Admin>ping -n 10 -l 64 google.com

Pinging google.com [216.58.203.142] with 64 bytes of data:
Reply from 216.58.203.142: bytes=64 time=74ms TTL=118
Reply from 216.58.203.142: bytes=64 time=12ms TTL=118
Reply from 216.58.203.142: bytes=64 time=5ms TTL=118
Reply from 216.58.203.142: bytes=64 time=8ms TTL=118
Reply from 216.58.203.142: bytes=64 time=14ms TTL=118
Reply from 216.58.203.142: bytes=64 time=4ms TTL=118
Reply from 216.58.203.142: bytes=64 time=48ms TTL=118
Reply from 216.58.203.142: bytes=64 time=14ms TTL=118
Reply from 216.58.203.142: bytes=64 time=5ms TTL=118
Reply from 216.58.203.142: bytes=64 time=5ms TTL=118

Ping statistics for 216.58.203.142:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 74ms, Average = 18ms
```

```
C:\Users\Admin>ping -n 10 -l 100 google.com

Pinging google.com [216.58.203.142] with 100 bytes of data:
Reply from 216.58.203.142: bytes=68 (sent 100) time=121ms TTL=118
Reply from 216.58.203.142: bytes=68 (sent 100) time=210ms TTL=118
Reply from 216.58.203.142: bytes=68 (sent 100) time=14ms TTL=118
Reply from 216.58.203.142: bytes=68 (sent 100) time=13ms TTL=118
Reply from 216.58.203.142: bytes=68 (sent 100) time=28ms TTL=118
Reply from 216.58.203.142: bytes=68 (sent 100) time=4ms TTL=118
Reply from 216.58.203.142: bytes=68 (sent 100) time=31ms TTL=118
Reply from 216.58.203.142: bytes=68 (sent 100) time=31ms TTL=118
Reply from 216.58.203.142: bytes=68 (sent 100) time=17ms TTL=118
Reply from 216.58.203.142: bytes=68 (sent 100) time=15ms TTL=118

Ping statistics for 216.58.203.142:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 210ms, Average = 48ms
```

```
C:\Users\Admin>ping -n 10 -l 500 google.com

Pinging google.com [216.58.203.46] with 500 bytes of data:
Reply from 216.58.203.46: bytes=68 (sent 500) time=78ms TTL=118
Reply from 216.58.203.46: bytes=68 (sent 500) time=5ms TTL=118
Reply from 216.58.203.46: bytes=68 (sent 500) time=12ms TTL=118
Reply from 216.58.203.46: bytes=68 (sent 500) time=6ms TTL=118
Reply from 216.58.203.46: bytes=68 (sent 500) time=5ms TTL=118
Reply from 216.58.203.46: bytes=68 (sent 500) time=14ms TTL=118
Reply from 216.58.203.46: bytes=68 (sent 500) time=5ms TTL=118
Reply from 216.58.203.46: bytes=68 (sent 500) time=9ms TTL=118
Reply from 216.58.203.46: bytes=68 (sent 500) time=5ms TTL=118
Reply from 216.58.203.46: bytes=68 (sent 500) time=13ms TTL=118

Ping statistics for 216.58.203.46:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 78ms, Average = 15ms
```

```
C:\Users\Admin>ping -n 10 -l 1000 google.com

Pinging google.com [216.58.203.46] with 1000 bytes of data:
Reply from 216.58.203.46: bytes=68 (sent 1000) time=21ms TTL=118
Reply from 216.58.203.46: bytes=68 (sent 1000) time=7ms TTL=118
Reply from 216.58.203.46: bytes=68 (sent 1000) time=9ms TTL=118
Reply from 216.58.203.46: bytes=68 (sent 1000) time=5ms TTL=118
Reply from 216.58.203.46: bytes=68 (sent 1000) time=9ms TTL=118
Reply from 216.58.203.46: bytes=68 (sent 1000) time=6ms TTL=118
Reply from 216.58.203.46: bytes=68 (sent 1000) time=22ms TTL=118
Reply from 216.58.203.46: bytes=68 (sent 1000) time=6ms TTL=118
Reply from 216.58.203.46: bytes=68 (sent 1000) time=7ms TTL=118
Reply from 216.58.203.46: bytes=68 (sent 1000) time=6ms TTL=118

Ping statistics for 216.58.203.46:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 22ms, Average = 9ms
```

```
C:\Users\Admin>ping -n 10 -l 1400 google.com

Pinging google.com [216.58.203.142] with 1400 bytes of data:
Reply from 216.58.203.142: bytes=68 (sent 1400) time=68ms TTL=118
Reply from 216.58.203.142: bytes=68 (sent 1400) time=9ms TTL=118
Reply from 216.58.203.142: bytes=68 (sent 1400) time=18ms TTL=118
Reply from 216.58.203.142: bytes=68 (sent 1400) time=6ms TTL=118
Reply from 216.58.203.142: bytes=68 (sent 1400) time=9ms TTL=118
Reply from 216.58.203.142: bytes=68 (sent 1400) time=6ms TTL=118
Reply from 216.58.203.142: bytes=68 (sent 1400) time=13ms TTL=118
Reply from 216.58.203.142: bytes=68 (sent 1400) time=10ms TTL=118
Reply from 216.58.203.142: bytes=68 (sent 1400) time=6ms TTL=118
Reply from 216.58.203.142: bytes=68 (sent 1400) time=101ms TTL=118

Ping statistics for 216.58.203.142:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 101ms, Average = 24ms
```

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?

we can conclude that RTT is dependent on the host on which the 'ping' command is used. Transmission delay is the time taken to put a packet onto a link or simply, the time required to put data bits on the wire/communication medium. It depends on the size of the packet and the bandwidth of the network. Since the hosts are the only parameters changed, there is no transmission delay in the two cases. Propagation delay is the time taken by the first bit to travel from sender to receiver end of the link or simply the time required for bits to reach the destination from the start point. Factors on which propagation delay depends are distance and propagation speed(difference of distance from India between the 2 is around 5000km). So, there exists a propagation delay in the two cases. Queueing delay is the time difference between when the packet arrived at its destination and when the packet data was processed or executed. It depends on the number of packets, size of the packet and bandwidth of the network. Since all the parameters are non-varying in both cases, there is hardly any queueing delay

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

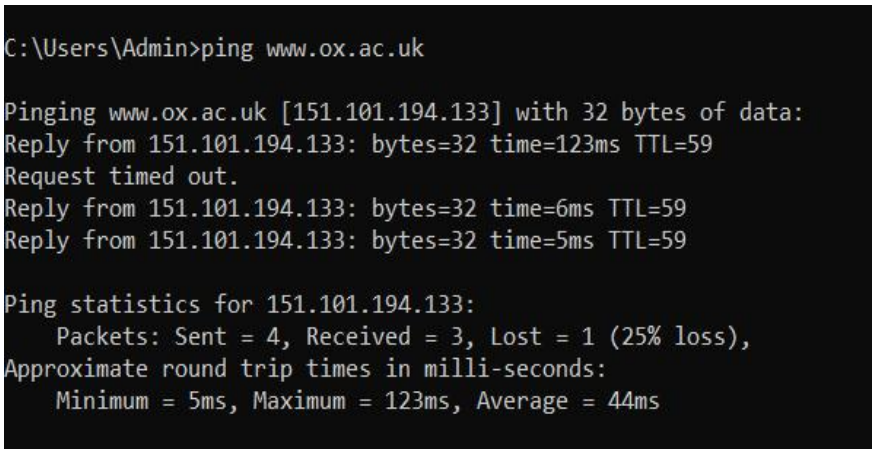
we can say that the Round Trip Time is impacted due to the difference in the size of the packets. This is because of the Transmission delay and the Queueing delay which depend on the size of the packets.RTT increases with increase in packet size. There would be increased latency for increased packet size due to transmission delay and propagation delay.

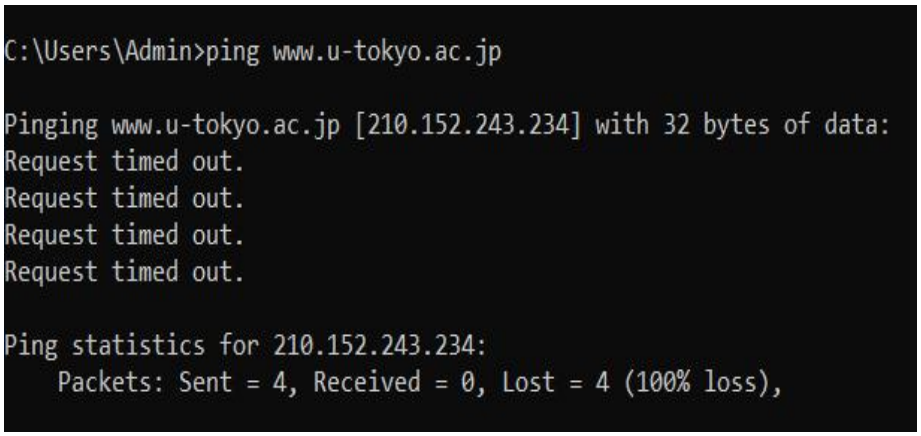
Exercise 1: Experiment with ping to find the round trip times to a variety of destinations. Write up any interesting observations, including in particular how the round trip time compares to the physical distance. Here are few places from who to get replies: www.uw.edu, www.cornell.edu, berkeley.edu,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

```
C:\Users\Admin>ping uw.edu

Pinging uw.edu [128.95.155.197] with 32 bytes of data:
Request timed out.
Request timed out.
Reply from 128.95.155.197: bytes=32 time=245ms TTL=45
Reply from 128.95.155.197: bytes=32 time=243ms TTL=45

Ping statistics for 128.95.155.197:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
    Minimum = 243ms, Maximum = 245ms, Average = 244ms
```

```
C:\Users\Admin>ping www.cornell.edu

Pinging ucomm-gw1.cornell.media3.us [20.42.25.107] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 20.42.25.107:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
C:\Users\Admin>ping www.berkeley.edu

Pinging www-production-1113102805.us-west-2.elb.amazonaws.com [52.88.59.144] with 32 bytes of data:
Request timed out.
Reply from 52.88.59.144: bytes=32 time=243ms TTL=224
Request timed out.
Reply from 52.88.59.144: bytes=32 time=331ms TTL=224

Ping statistics for 52.88.59.144:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
    Minimum = 243ms, Maximum = 331ms, Average = 287ms
```





Observation :

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

1. The length a signal has to travel correlates with the time taken for a request to reach a server and a response to reach a browser.
2. The medium used to route a signal (e.g., copper wire, fiber optic cables) can impact how quickly a request is received by a server and routed back to a user.

3. Intermediate routers or servers take time to process a signal, increasing RTT. The more hops a signal has to travel through, the higher the RTT.
4. RTT typically increases when a network is congested with high levels of traffic. Conversely, low traffic times can result in decreased RTT.
5. The time taken for a target server to respond to a request depends on its processing capacity, the number of requests being handled and the nature of the request (i.e., how much server-side work is required). A longer server response time increases RTT.

nslookup — The command nslookup <host> will do a DNS query to find and report the IP address (or addresses) for a domain name or the domain name corresponding to an IP address. To do this, it contacts a "DNS server." Default DNS servers are part of a computer's network configuration. (For a static IP address in Linux, they are configured in the file /etc/network/interfaces that you encountered in the last lab.) You can specify a different DNS server to be used by nslokup by adding the server name or IP address to the command: nslookup <host> <server>

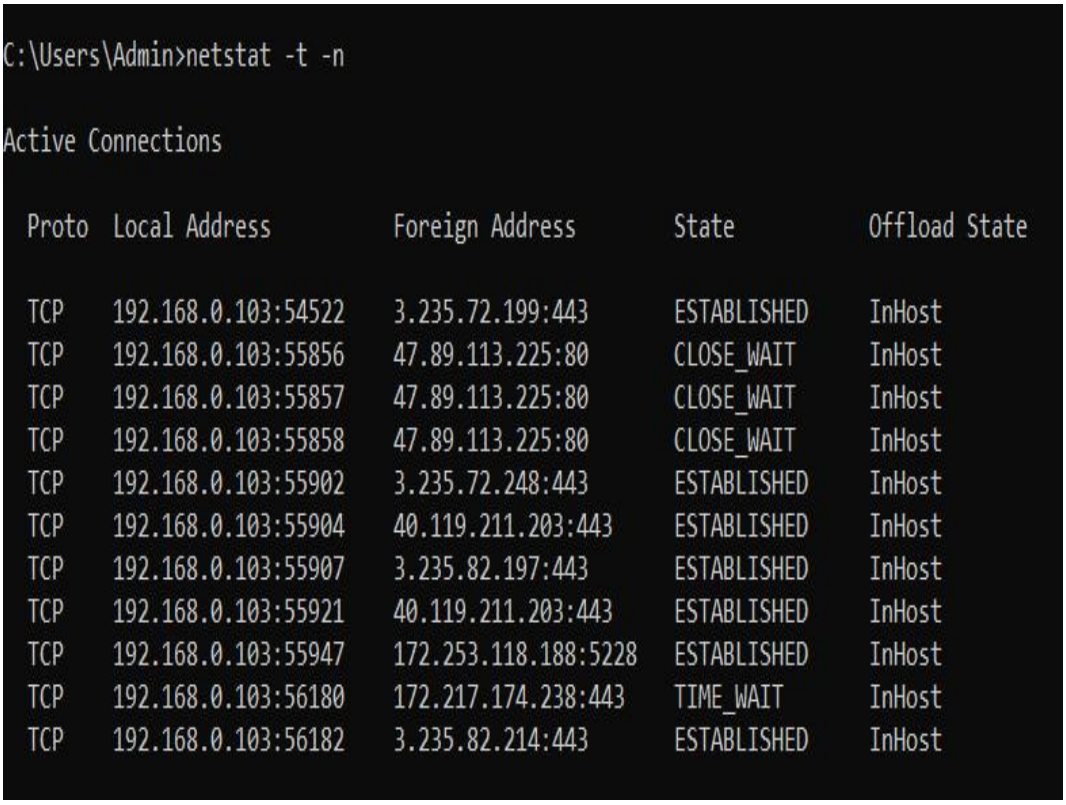
```
C:\Users\Admin>nslookup www.google.com
Server:  UnKnown
Address:  192.168.0.1

Non-authoritative answer:
Name:    www.google.com
Addresses:  2404:6800:4009:80e::2004
          216.58.199.164
```

```
C:\Users\Admin>nslookup www.wikipedia.com
Server:  UnKnown
Address:  192.168.0.1

Non-authoritative answer:
Name:    ncredir-lb.wikimedia.org
Addresses:  2001:df2:e500:ed1a::3
          103.102.166.226
Aliases:  www.wikipedia.com
```

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.)



```
C:\Users\Admin>netstat -t -n

Active Connections

  Proto  Local Address          Foreign Address        State           Offload State

  TCP    192.168.0.103:54522    3.235.72.199:443       ESTABLISHED     InHost
  TCP    192.168.0.103:55856    47.89.113.225:80       CLOSE_WAIT      InHost
  TCP    192.168.0.103:55857    47.89.113.225:80       CLOSE_WAIT      InHost
  TCP    192.168.0.103:55858    47.89.113.225:80       CLOSE_WAIT      InHost
  TCP    192.168.0.103:55902    3.235.72.248:443       ESTABLISHED     InHost
  TCP    192.168.0.103:55904    40.119.211.203:443     ESTABLISHED     InHost
  TCP    192.168.0.103:55907    3.235.82.197:443       ESTABLISHED     InHost
  TCP    192.168.0.103:55921    40.119.211.203:443     ESTABLISHED     InHost
  TCP    192.168.0.103:55947    172.253.118.188:5228   ESTABLISHED     InHost
  TCP    192.168.0.103:56180    172.217.174.238:443    TIME_WAIT       InHost
  TCP    192.168.0.103:56182    3.235.82.214:443       ESTABLISHED     InHost
```

```
C:\Users\Admin>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            DESKTOP-ES77G88:0      LISTENING
  TCP    0.0.0.0:445            DESKTOP-ES77G88:0      LISTENING
  TCP    0.0.0.0:5040           DESKTOP-ES77G88:0      LISTENING
  TCP    0.0.0.0:49664          DESKTOP-ES77G88:0      LISTENING
  TCP    0.0.0.0:49665          DESKTOP-ES77G88:0      LISTENING
  TCP    0.0.0.0:49666          DESKTOP-ES77G88:0      LISTENING
  TCP    0.0.0.0:49667          DESKTOP-ES77G88:0      LISTENING
  TCP    0.0.0.0:49668          DESKTOP-ES77G88:0      LISTENING
  TCP    0.0.0.0:49670          DESKTOP-ES77G88:0      LISTENING
  TCP    127.0.0.1:5939         DESKTOP-ES77G88:0      LISTENING
  TCP    192.168.0.103:139      DESKTOP-ES77G88:0      LISTENING
  TCP    192.168.0.103:54522    ec2-3-235-72-199:https  ESTABLISHED
  TCP    192.168.0.103:55856    47.89.113.225:http     CLOSE_WAIT
  TCP    192.168.0.103:55857    47.89.113.225:http     CLOSE_WAIT
  TCP    192.168.0.103:55858    47.89.113.225:http     CLOSE_WAIT
  TCP    192.168.0.103:55902    ec2-3-235-72-248:https  ESTABLISHED
  TCP    192.168.0.103:55904    40.119.211.203:https   ESTABLISHED
  TCP    192.168.0.103:55907    ec2-3-235-82-197:https  ESTABLISHED
  TCP    192.168.0.103:55921    40.119.211.203:https   ESTABLISHED
  TCP    192.168.0.103:55947    172.253.118.188:5228   ESTABLISHED
  TCP    192.168.0.103:56182    ec2-3-235-82-214:https  CLOSE_WAIT
  TCP    192.168.0.103:56183    104.18.17.106:https    TIME_WAIT
  TCP    [::]:135               DESKTOP-ES77G88:0      LISTENING
  TCP    [::]:445               DESKTOP-ES77G88:0      LISTENING
  TCP    [::]:49664             DESKTOP-ES77G88:0      LISTENING
  TCP    [::]:49665             DESKTOP-ES77G88:0      LISTENING
  TCP    [::]:49666             DESKTOP-ES77G88:0      LISTENING
  TCP    [::]:49667             DESKTOP-ES77G88:0      LISTENING
  TCP    [::]:49668             DESKTOP-ES77G88:0      LISTENING
  TCP    [::]:49670             DESKTOP-ES77G88:0      LISTENING
  UDP    0.0.0.0:5050           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5355           *:*
  UDP    0.0.0.0:55672          *:*
  UDP    0.0.0.0:56757          *:*
  UDP    0.0.0.0:59820          *:*
  UDP    127.0.0.1:1900         *:*
  UDP    127.0.0.1:49666        *:*
  UDP    127.0.0.1:60926        *:*
  UDP    192.168.0.103:137      *:*
  UDP    192.168.0.103:138      *:*
  UDP    192.168.0.103:1900     *:*
  UDP    192.168.0.103:2177     *:*
```

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

```
C:\Users\Admin>tracert www.cc.iitb.ac.in

Tracing route to www.cc.iitb.ac.in [103.21.124.6]
over a maximum of 30 hops:

  1    26 ms     2 ms     2 ms  192.168.0.1
  2     4 ms     4 ms     4 ms  43.231.238.52
  3     *      109 ms     *     43.231.238.49
  4     6 ms     4 ms     5 ms  172.16.2.101
  5    38 ms    98 ms   100 ms  121.241.42.57.static-mumbai.vsnl.net.in [121.241.43.57]
  6    33 ms     6 ms     7 ms  115.113.165.62.static-mumbai.vsnl.net.in [115.113.165.62]
  7    14 ms    13 ms    14 ms  10.152.7.37
  8   868 ms    30 ms     7 ms  10.119.249.49
  9     7 ms     7 ms     7 ms  115.110.234.170.static.Mumbai.vsnl.net.in [115.110.234.170]
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.
```

2. mscs.mu.edu

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

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

  1     4 ms     2 ms     3 ms  192.168.0.1
  2    36 ms   101 ms    97 ms  43.231.238.52
  3     5 ms     *        7 ms  43.231.238.49
  4     5 ms     4 ms     4 ms  172.16.2.101
  5     6 ms     5 ms    34 ms  121.241.42.57.static-mumbai.vsnl.net.in [121.241.43.57]
  6     *        7 ms     5 ms  172.23.78.237
  7   111 ms   113 ms   103 ms  ix-ae-0-100.tcore1.mlv-mumbai.as6453.net [180.87.38.5]
  8   115 ms     *        *     if-ae-5-2.tcore1.wyn-marseille.as6453.net [80.231.217.29]
  9   119 ms   115 ms     *     if-ae-8-1600.tcore1.pye-paris.as6453.net [80.231.217.6]
 10   196 ms   201 ms   120 ms  if-ae-11-2.tcore1.pvu-paris.as6453.net [80.231.153.49]
 11     *        *        *     Request timed out.
 12   247 ms   248 ms   249 ms  ae-2-3603.ear3.Chicago2.Level3.net [4.69.159.186]
 13   263 ms   264 ms   263 ms  MARQUETTE-U.ear3.Chicago2.Level3.net [4.16.38.70]
 14   249 ms   248 ms   248 ms  134.48.10.27
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.
```

3. www.cs.grinnell.edu

```
C:\Users\Admin>tracert  www.cs.grinnell.edu

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

  1     5 ms     2 ms     6 ms  192.168.0.1
  2    97 ms    93 ms   100 ms  43.231.238.52
  3     *        *        *     Request timed out.
  4   115 ms    99 ms    97 ms  172.16.2.101
  5    67 ms    98 ms     8 ms  121.241.42.57.static-mumbai.vsnl.net.in [121.241.43.57]
  6     5 ms     5 ms     5 ms  172.23.78.237
  7    56 ms    96 ms    98 ms  172.31.244.45
  8   171 ms   203 ms   200 ms  ix-ae-4-2.tcore2.cxr-chennai.as6453.net [180.87.37.1]
  9   290 ms   296 ms   310 ms  if-ae-9-2.tcore2.mlv-mumbai.as6453.net [180.87.37.10]
 10     *        *        *     Request timed out.
 11   433 ms   368 ms   304 ms  if-ae-66-9.tcore2.nto-newyork.as6453.net [80.231.130.20]
 12   307 ms   293 ms   294 ms  if-ae-26-2.tcore1.ct8-chicago.as6453.net [216.6.81.29]
 13     *      386 ms     *     63.243.129.121
 14     *      295 ms     *     gi0-0-0-3.agr02.mtld01-fl.us.windstream.net [169.130.82.82]
 15   291 ms   305 ms   258 ms  et3-1-0-0.agr03.desm01-ia.us.windstream.net [40.128.250.43]
 16   296 ms   296 ms   296 ms  ae4-0.pe04.grnl01-ia.us.windstream.net [40.128.248.35]
 17   265 ms   265 ms   264 ms  h29.127.138.40.static.ip.windstream.net [40.138.127.29]
 18   300 ms   312 ms   304 ms  grnl-static-grinnellcollege0-0001.flex.iowatelecom.net [69.66.111.181]
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.
```

4. csail.mit.edu

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

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

  1   121 ms    33 ms     2 ms  192.168.0.1
  2    28 ms    98 ms    94 ms  43.231.238.52
  3     *       79 ms   102 ms  43.231.238.49
  4    93 ms    98 ms   303 ms  172.16.2.101
  5    67 ms    96 ms     5 ms  182.73.109.41
  6   274 ms   301 ms   304 ms  182.79.243.31
  7   271 ms   301 ms   224 ms  xe-5-1-0.edge1.LosAngeles6.Level3.net [4.26.0.89]
  8     *        *        *     Request timed out.
  9   347 ms   404 ms   310 ms  MASSACHUSET.bear1.Boston1.Level3.net [4.53.48.98]
 10   306 ms   310 ms   305 ms  dmz-rtr-1-external-rtr-1.mit.edu [18.0.161.17]
 11   301 ms   305 ms   301 ms  dmz-rtr-2-dmz-rtr-1-1.mit.edu [18.0.161.6]
 12   303 ms   302 ms   303 ms  mitnet.core-1-ext.csail.mit.edu [18.4.7.65]
 13     *        *        *     Request timed out.
 14   413 ms   404 ms   406 ms  bdr.core-1.csail.mit.edu [128.30.0.246]
 15   302 ms   305 ms   302 ms  inquir-3ld.csail.mit.edu [128.30.2.109]

Trace complete.
```

5. cs.stanford.edu

```
C:\Users\Admin>tracert  cs.stanford.edu

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

  1    2 ms    2 ms    2 ms  192.168.0.1
  2   53 ms    3 ms    3 ms  43.231.238.52
  3    *      47 ms   99 ms  43.231.238.49
  4   97 ms   97 ms   77 ms  172.16.2.101
  5   47 ms   98 ms   62 ms  182.73.109.41
  6  330 ms  302 ms  229 ms  182.79.222.237
  7  226 ms  246 ms  222 ms  core1.nyc4.he.net [198.32.118.57]
  8  282 ms  277 ms  279 ms  100ge8-1.core1.sjc2.he.net [184.105.81.218]
  9  276 ms  275 ms  278 ms  100ge1-1.core1.pao1.he.net [72.52.92.158]
 10  276 ms  295 ms  274 ms  stanford-university.100gigabitethernet5-1.core1.pao1.he.net [184.105.177.238]
 11  358 ms  280 ms  301 ms  csee-west-rtr-vl3.SUNet [171.66.255.140]
 12  330 ms  279 ms  308 ms  CS.stanford.edu [171.64.64.64]

Trace complete.
```

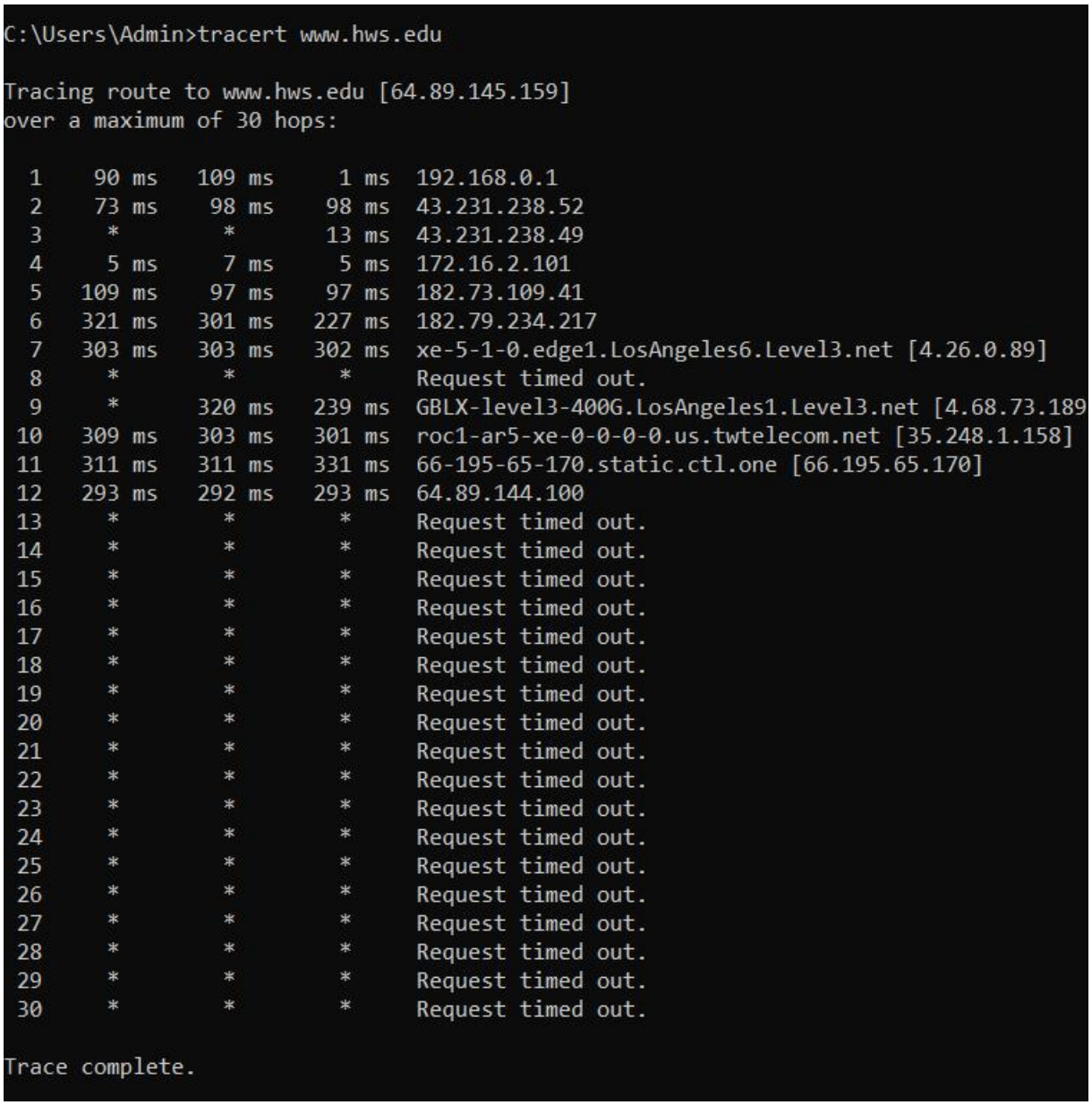
6. cs.manchester.ac.uk

```
C:\Users\Admin>tracert  cs.manchester.ac.uk

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

  1    81 ms     2 ms     2 ms  192.168.0.1
  2    29 ms   100 ms   303 ms  43.231.238.52
  3     *       31 ms     *     43.231.238.49
  4     5 ms     5 ms     4 ms  172.16.2.101
  5    57 ms    97 ms    99 ms  182.73.109.41
  6   246 ms   137 ms   137 ms  182.79.134.223
  7   152 ms     *      164 ms  ldn-b4-link.telia.net [62.115.162.232]
  8   137 ms   144 ms   137 ms  jisc-ic-345131-ldn-b4.c.telia.net [62.115.175.131]
  9   140 ms   140 ms   141 ms  ae24.londhx-sbr1.ja.net [146.97.35.197]
 10   137 ms   138 ms   137 ms  ae29.londpg-sbr2.ja.net [146.97.33.2]
 11   145 ms   141 ms   151 ms  ae31.erdiss-sbr2.ja.net [146.97.33.22]
 12   159 ms   144 ms   145 ms  ae29.manckh-sbr2.ja.net [146.97.33.42]
 13   143 ms   143 ms   143 ms  ae23.mancrh-rbr1.ja.net [146.97.38.42]
 14   172 ms     *        *     universityofmanchester.ja.net [146.97.169.2]
 15   190 ms   200 ms   143 ms  130.88.249.194
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18   207 ms   200 ms   200 ms  eps.its.man.ac.uk [130.88.101.49]

Trace complete.
```

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.

```
C:\Users\Admin>tracert www.math.hws.edu

Tracing route to www.math.hws.edu [218.93.250.18]
over a maximum of 30 hops:

  1    37 ms     1 ms     2 ms  192.168.0.1
  2     8 ms     3 ms     3 ms  43.231.238.52
  3   113 ms     *        *     43.231.238.49
  4    91 ms    99 ms    98 ms  172.16.2.101
  5    62 ms    97 ms     4 ms  182.73.109.41
  6   134 ms    98 ms    97 ms  116.119.42.21
  7   173 ms   100 ms    97 ms  unknown.telstraglobal.net [202.127.73.101]
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11   258 ms   306 ms   304 ms  snj-edge-06.inet.qwest.net [65.123.13.173]
 12   231 ms   263 ms   233 ms  los-priv-20.inet.qwest.net [67.14.22.206]
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15   273 ms   303 ms   305 ms  CHINA-TELEC.ear1.LosAngeles1.Level3.net [4.35.157.166]
 16   260 ms   257 ms   260 ms  202.97.92.46
 17   452 ms   406 ms   365 ms  202.97.89.141
 18   481 ms   507 ms   376 ms  202.97.90.54
 19   486 ms   374 ms   371 ms  202.97.62.101
 20   391 ms   391 ms   398 ms  202.97.92.22
 21   393 ms   427 ms   389 ms  222.187.241.170
 22   437 ms  1039 ms     *     222.187.235.201
 23   388 ms   381 ms   380 ms  61.147.244.126
 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\Admin>tracert www.hws.edu

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

  1    90 ms   109 ms     1 ms  192.168.0.1
  2    73 ms    98 ms    98 ms  43.231.238.52
  3     *        *       13 ms  43.231.238.49
  4     5 ms     7 ms     5 ms  172.16.2.101
  5   109 ms    97 ms    97 ms  182.73.109.41
  6   321 ms   301 ms   227 ms  182.79.234.217
  7   303 ms   303 ms   302 ms  xe-5-1-0.edge1.LosAngeles6.Level3.net [4.26.0.89]
  8     *        *        *     Request timed out.
  9     *      320 ms   239 ms  GBLX-level3-400G.LosAngeles1.Level3.net [4.68.73.189
 10   309 ms   303 ms   301 ms  roc1-ar5-xe-0-0-0-0.us.twtelecom.net [35.248.1.158]
 11   311 ms   311 ms   331 ms  66-195-65-170.static.ctl.one [66.195.65.170]
 12   293 ms   292 ms   293 ms  64.89.144.100
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.
```

Observation :

From the above images, 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.

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 www prefix is technically a subdomain, so it's possible that traces to example.com and www.example.com follow two very different paths.

Many domains use separate hosting for email. If you try to trace the domain, you'll get data for the website server, not the email server. This concept is popularly known as Caveats [1].

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\Admin>tracert www.google.com

Tracing route to www.google.com [172.217.166.164]
over a maximum of 30 hops:

  1    34 ms    97 ms     2 ms  192.168.0.1
  2    13 ms    12 ms    11 ms  43.231.238.52
  3     *        *        *     Request timed out.
  4    82 ms     *      194 ms  172.16.2.202
  5    86 ms    99 ms    98 ms  175.100.188.26
  6    99 ms    85 ms    99 ms  108.170.248.209
  7     *       97 ms   100 ms  216.239.57.189
  8   118 ms    96 ms    98 ms  bom07s20-in-f4.1e100.net [172.217.166.164]

Trace complete.
```

```
C:\Users\Admin>tracert www.mit.edu.in

Tracing route to mit.edu.in [198.71.205.226]
over a maximum of 30 hops:

  1    60 ms   100 ms     2 ms  192.168.0.1
  2    10 ms     8 ms     7 ms  43.231.238.52
  3   100 ms     *        *     43.231.238.49
  4    95 ms    97 ms     5 ms  172.16.2.101
  5   122 ms    96 ms    99 ms  182.73.109.41
  6   258 ms   199 ms   202 ms  182.79.134.223
  7     *      255 ms     *     ldn-b4-link.telia.net [62.115.162.232]
  8     *      252 ms   251 ms  ldn-bb4-link.telia.net [62.115.120.238]
  9   249 ms   253 ms     *     nyk-bb3-link.telia.net [62.115.112.244]
 10   242 ms   254 ms   253 ms  rest-bb1-link.telia.net [62.115.141.244]
 11   286 ms   262 ms   251 ms  las-b24-link.telia.net [62.115.114.86]
 12   242 ms   244 ms   242 ms  ae9.ibrsa0107-01.lax1.bb.godaddy.com [62.115.171.243]
 13   305 ms   293 ms   366 ms  148.72.34.34
 14   274 ms   298 ms   269 ms  be39.trmc0215-01.ars.mgmt.phx3.gdg [184.168.0.73]
 15   274 ms   337 ms   271 ms  ip-97-74-255-129.ip.secureserver.net [97.74.255.129]
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.
```

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 depends on which access point is ready to respond and which access point

or routers have firewalls configured for blocking the requests and accordingly, the destination can be reached through different paths at different times.

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, the number of nodes(number of hops subtract 1) is directly proportional to the distance between the source and 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?

   There is a direct relationship between the number of nodes (number of hops minus 1)and the latency of the host. It also depends on the packet size. The amount of latency is largely dependent on how far the visitor is from the server location and how many nodes the signal has to travel through.

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.

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.

```
C:\Users\Admin>nslookup spit.ac.in
Server:  UnKnown
Address:  192.168.0.1

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

nslookup command is a program for querying Internet domain name servers (DNS). nslookup has two modes, which are interactive and interactive.
Interactive mode allows the user to query name servers for information about various hosts and domains or to print a list of hosts in a domain.
Non-interactive mode is used to print just the name and requested information for a host or domain.
It is a network administration tool that helps diagnose and resolve DNS related issues. Hence,with the help of it the outside IP address for spit.ac.in was found out.[2] Alternatively, ping, fping and so on can be used to find out the IP address.

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

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

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

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.

```
C:\Users\Admin>ping www.spit.ac.in

Pinging www.spit.ac.in [43.252.193.19] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 43.252.193.19:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Reference:

1. https://network-tools.com/trace/
2. https://www.2daygeek.com/linux-command-find-check-domain-ip-address/
3. https://www.cloudflare.com/learning/cdn/glossary/round-trip-time-rtt/

Conclusion:

1. I learned about some basic command line network utilities.
2. Also came to know about Network Latency, RTT and the factors impacting RTT.