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 receive 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 response 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 (Internet Control Message Protocol) 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

Results –

Pinging www.google.com 10 times with a packet size of 64 bytes

```
C:\Users\Rohit Pai>ping -n 10 -l 64 www.google.com

Pinging www.google.com [142.250.67.164] with 64 bytes of data:
Reply from 142.250.67.164: bytes=64 time=1373ms TTL=120
Reply from 142.250.67.164: bytes=64 time=3ms TTL=120
Reply from 142.250.67.164: bytes=64 time=4ms TTL=120
Reply from 142.250.67.164: bytes=64 time=2ms TTL=120
Reply from 142.250.67.164: bytes=64 time=4ms TTL=120
Reply from 142.250.67.164: bytes=64 time=11ms TTL=120
Reply from 142.250.67.164: bytes=64 time=2ms TTL=120
Reply from 142.250.67.164: bytes=64 time=4ms TTL=120
Reply from 142.250.67.164: bytes=64 time=4ms TTL=120
Reply from 142.250.67.164: bytes=64 time=7ms TTL=120

Ping statistics for 142.250.67.164:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 1373ms, Average = 141ms
```

Pinging www.google.com 10 times with a packet size of 100 bytes

```
C:\Users\Rohit Pai>ping -n 10 -l 100 www.google.com

Pinging www.google.com [172.217.160.164] with 100 bytes of data:
Reply from 172.217.160.164: bytes=68 (sent 100) time=1405ms TTL=119
Reply from 172.217.160.164: bytes=68 (sent 100) time=6ms TTL=119
Reply from 172.217.160.164: bytes=68 (sent 100) time=4ms TTL=119
Reply from 172.217.160.164: bytes=68 (sent 100) time=4ms TTL=119
Reply from 172.217.160.164: bytes=68 (sent 100) time=3ms TTL=119
Reply from 172.217.160.164: bytes=68 (sent 100) time=3ms TTL=119
Reply from 172.217.160.164: bytes=68 (sent 100) time=3ms TTL=119
Reply from 172.217.160.164: bytes=68 (sent 100) time=3ms TTL=119
Reply from 172.217.160.164: bytes=68 (sent 100) time=6ms TTL=119
Reply from 172.217.160.164: bytes=68 (sent 100) time=2ms TTL=119

Ping statistics for 172.217.160.164:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 1405ms, Average = 143ms
```

Ping www.google.com 10 times with a packet size of 500 bytes

```
C:\Users\Rohit Pai>ping -n 10 -l 500 www.google.com

Pinging www.google.com [142.250.67.164] with 500 bytes of data:
Reply from 142.250.67.164: bytes=68 (sent 500) time=3ms TTL=120
Reply from 142.250.67.164: bytes=68 (sent 500) time=4ms TTL=120
Reply from 142.250.67.164: bytes=68 (sent 500) time=3ms TTL=120
Reply from 142.250.67.164: bytes=68 (sent 500) time=3ms TTL=120
Reply from 142.250.67.164: bytes=68 (sent 500) time=5ms TTL=120
Reply from 142.250.67.164: bytes=68 (sent 500) time=6ms TTL=120
Reply from 142.250.67.164: bytes=68 (sent 500) time=6ms TTL=120
Reply from 142.250.67.164: bytes=68 (sent 500) time=6ms TTL=120
Reply from 142.250.67.164: bytes=68 (sent 500) time=3ms TTL=120
Reply from 142.250.67.164: bytes=68 (sent 500) time=4ms TTL=120

Ping statistics for 142.250.67.164:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 6ms, Average = 4ms
```

Pinging www,google.com 10 times with a packet size of 1000 bytes

```
C:\Users\Rohit Pai>ping -n 10 -l 1000 www.google.com

Pinging www.google.com [142.250.67.164] with 1000 bytes of data:
Reply from 142.250.67.164: bytes=68 (sent 1000) time=6ms TTL=120
Reply from 142.250.67.164: bytes=68 (sent 1000) time=6ms TTL=120
Reply from 142.250.67.164: bytes=68 (sent 1000) time=5ms TTL=120
Reply from 142.250.67.164: bytes=68 (sent 1000) time=3ms TTL=120
Reply from 142.250.67.164: bytes=68 (sent 1000) time=6ms TTL=120
Reply from 142.250.67.164: bytes=68 (sent 1000) time=5ms TTL=120
Reply from 142.250.67.164: bytes=68 (sent 1000) time=3ms TTL=120
Reply from 142.250.67.164: bytes=68 (sent 1000) time=5ms TTL=120
Reply from 142.250.67.164: bytes=68 (sent 1000) time=4ms TTL=120
Reply from 142.250.67.164: bytes=68 (sent 1000) time=5ms TTL=120

Ping statistics for 142.250.67.164:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 6ms, Average = 4ms
```

Pinging www.google.com 10 times with a packet size of 1400 bytes

```
C:\Users\Rohit Pai>ping -n 10 -l 1400 www.google.com

Pinging www.google.com [142.250.67.164] with 1400 bytes of data:
Reply from 142.250.67.164: bytes=68 (sent 1400) time=5ms TTL=120
Reply from 142.250.67.164: bytes=68 (sent 1400) time=5ms TTL=120
Reply from 142.250.67.164: bytes=68 (sent 1400) time=6ms TTL=120
Reply from 142.250.67.164: bytes=68 (sent 1400) time=3ms TTL=120
Reply from 142.250.67.164: bytes=68 (sent 1400) time=3ms TTL=120
Reply from 142.250.67.164: bytes=68 (sent 1400) time=4ms TTL=120
Reply from 142.250.67.164: bytes=68 (sent 1400) time=7ms TTL=120
Reply from 142.250.67.164: bytes=68 (sent 1400) time=7ms TTL=120
Reply from 142.250.67.164: bytes=68 (sent 1400) time=5ms TTL=120
Reply from 142.250.67.164: bytes=68 (sent 1400) time=5ms TTL=120

Ping statistics for 142.250.67.164:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 7ms, Average = 5ms
```

Pinging pravda.ru 10 times with a packet size of 64 bytes

```
C:\Users\Rohit Pai>ping -n 10 -l 64 pravda.ru

Pinging pravda.ru [185.201.54.50] with 64 bytes of data:
Reply from 185.201.54.50: bytes=64 time=282ms TTL=51
Reply from 185.201.54.50: bytes=64 time=181ms TTL=51
Reply from 185.201.54.50: bytes=64 time=191ms TTL=51
Reply from 185.201.54.50: bytes=64 time=185ms TTL=51
Reply from 185.201.54.50: bytes=64 time=190ms TTL=51
Reply from 185.201.54.50: bytes=64 time=180ms TTL=51
Reply from 185.201.54.50: bytes=64 time=194ms TTL=51
Reply from 185.201.54.50: bytes=64 time=199ms TTL=51
Reply from 185.201.54.50: bytes=64 time=206ms TTL=51
Reply from 185.201.54.50: bytes=64 time=210ms TTL=51

Ping statistics for 185.201.54.50:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 180ms, Maximum = 282ms, Average = 201ms
```

Pinging pravda.ru 10 times with a packet size of 100 bytes

```
C:\Users\Rohit Pai>ping -n 10 -l 100 pravda.ru

Pinging pravda.ru [185.201.54.50] with 100 bytes of data:
Reply from 185.201.54.50: bytes=100 time=174ms TTL=51
Reply from 185.201.54.50: bytes=100 time=279ms TTL=51
Reply from 185.201.54.50: bytes=100 time=269ms TTL=51
Reply from 185.201.54.50: bytes=100 time=278ms TTL=51
Reply from 185.201.54.50: bytes=100 time=189ms TTL=51
Reply from 185.201.54.50: bytes=100 time=181ms TTL=51
Reply from 185.201.54.50: bytes=100 time=163ms TTL=51
Reply from 185.201.54.50: bytes=100 time=206ms TTL=51
Reply from 185.201.54.50: bytes=100 time=205ms TTL=51
Reply from 185.201.54.50: bytes=100 time=214ms TTL=51

Ping statistics for 185.201.54.50:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 163ms, Maximum = 279ms, Average = 215ms
```

Pinging pravda.ru 10 times with a packet size of 500 bytes

```
C:\Users\Rohit Pai>ping -n 10 -l 500 pravda.ru

Pinging pravda.ru [185.201.54.50] with 500 bytes of data:
Reply from 185.201.54.50: bytes=500 time=204ms TTL=51
Reply from 185.201.54.50: bytes=500 time=200ms TTL=51
Reply from 185.201.54.50: bytes=500 time=166ms TTL=51
Reply from 185.201.54.50: bytes=500 time=197ms TTL=51
Reply from 185.201.54.50: bytes=500 time=203ms TTL=51
Reply from 185.201.54.50: bytes=500 time=196ms TTL=51
Reply from 185.201.54.50: bytes=500 time=194ms TTL=51
Reply from 185.201.54.50: bytes=500 time=208ms TTL=51
Reply from 185.201.54.50: bytes=500 time=202ms TTL=51
Reply from 185.201.54.50: bytes=500 time=164ms TTL=51

Ping statistics for 185.201.54.50:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 164ms, Maximum = 208ms, Average = 193ms
```

Pinging pravda.ru 10 times with a packet size of 1000 bytes

```
C:\Users\Rohit Pai>ping -n 10 -l 1000 pravda.ru

Pinging pravda.ru [185.201.54.50] with 1000 bytes of data:
Reply from 185.201.54.50: bytes=1000 time=173ms TTL=51
Reply from 185.201.54.50: bytes=1000 time=164ms TTL=51
Reply from 185.201.54.50: bytes=1000 time=164ms TTL=51
Reply from 185.201.54.50: bytes=1000 time=165ms TTL=51
Reply from 185.201.54.50: bytes=1000 time=163ms TTL=51
Reply from 185.201.54.50: bytes=1000 time=163ms TTL=51
Reply from 185.201.54.50: bytes=1000 time=163ms TTL=51
Reply from 185.201.54.50: bytes=1000 time=164ms TTL=51
Reply from 185.201.54.50: bytes=1000 time=163ms TTL=51
Reply from 185.201.54.50: bytes=1000 time=167ms TTL=51

Ping statistics for 185.201.54.50:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 163ms, Maximum = 173ms, Average = 164ms
```

Pinging pravda.ru 10 times with a packet size of 1400 bytes

```
C:\Users\Rohit Pai>ping -n 10 -l 1400 pravda.ru

Pinging pravda.ru [185.201.54.50] with 1400 bytes of data:
Reply from 185.201.54.50: bytes=1400 time=163ms TTL=51
Reply from 185.201.54.50: bytes=1400 time=164ms TTL=51
Reply from 185.201.54.50: bytes=1400 time=161ms TTL=51
Reply from 185.201.54.50: bytes=1400 time=167ms TTL=51
Reply from 185.201.54.50: bytes=1400 time=163ms TTL=51
Reply from 185.201.54.50: bytes=1400 time=164ms TTL=51
Reply from 185.201.54.50: bytes=1400 time=164ms TTL=51
Reply from 185.201.54.50: bytes=1400 time=162ms TTL=51
Reply from 185.201.54.50: bytes=1400 time=172ms TTL=51
Reply from 185.201.54.50: bytes=1400 time=162ms TTL=51

Ping statistics for 185.201.54.50:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 161ms, Maximum = 172ms, Average = 164ms
```

QUESTIONS ABOUT LATENCY

Now look at the results you gathered and answer the following questions about latency. Store your answers in a file named `ping.txt`.

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

Ans. Yes, the average RTT varies between different hosts as there are many factors such as physical distance between the nodes, various delays such as processing delay, queuing delay that affect the transmission time. If the physical distance is more, the packet will have to go through more nodes and the time taken (RTT) will increase accordingly. Queuing delay occurs when a gateway receives multiple packets from different sources heading towards the same destination. Since typically only one packet can be transmitted at a time, some of the packets must queue for transmission, incurring additional delay. A processing delay is incurred while a gateway determines what to do with a newly received packet.

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

Ans. Yes, the average RTT usually varies with different packet sizes. If a packet size is bigger, it would hog the bandwidth of the channel during transmission and there are chances that some nodes may drop this packet. If the packet size is less, this problem would not occur during the ping command. But in my case, I assume that the bandwidth of my network is sufficient, hence the average RTT remains similar for all packet sizes.

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).

Pinging www.uw.edu (Washington, USA)

```
C:\Users\Rohit Pai>ping www.uw.edu

Pinging www.washington.edu [128.95.155.134] with 32 bytes of data:
Reply from 128.95.155.134: bytes=32 time=741ms TTL=49
Reply from 128.95.155.134: bytes=32 time=241ms TTL=49
Reply from 128.95.155.134: bytes=32 time=242ms TTL=49
Reply from 128.95.155.134: bytes=32 time=241ms TTL=49

Ping statistics for 128.95.155.134:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 241ms, Maximum = 741ms, Average = 366ms
```

Pinging www.cornell.edu (New York, USA)

```
C:\Users\Rohit Pai>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),
```

Pinging www.berkeley.edu (California, USA)

```
C:\Users\Rohit Pai>ping www.berkeley.edu

Pinging www-production-1113102805.us-west-2.elb.amazonaws.com [52.88.59.144]
 with 32 bytes of data:
Reply from 52.88.59.144: bytes=32 time=392ms TTL=228
Reply from 52.88.59.144: bytes=32 time=266ms TTL=228
Reply from 52.88.59.144: bytes=32 time=266ms TTL=228
Reply from 52.88.59.144: bytes=32 time=264ms TTL=228

Ping statistics for 52.88.59.144:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 264ms, Maximum = 392ms, Average = 297ms
```

Pinging www.uchicago.edu (Illinois, USA)

```
C:\Users\Rohit Pai>ping www.uchicago.edu

Pinging wsee2.elb.uchicago.edu [34.225.113.202] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 34.225.113.202:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Pinging www.ox.ac.uk (Oxford, England)

```
C:\Users\Rohit Pai>ping www.ox.ac.uk

Pinging www.ox.ac.uk [151.101.130.133] with 32 bytes of data:
Reply from 151.101.130.133: bytes=32 time=590ms TTL=61
Reply from 151.101.130.133: bytes=32 time=2ms TTL=61
Reply from 151.101.130.133: bytes=32 time=2ms TTL=61
Reply from 151.101.130.133: bytes=32 time=2ms TTL=61

Ping statistics for 151.101.130.133:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 590ms, Average = 149ms
```

Pinging www.nintendo.co.jp (Japan)

```
C:\Users\Rohit Pai>ping www.nintendo.co.jp

Pinging e5192.b.akamaiedge.net [104.120.57.225] with 32 bytes of data:
Reply from 104.120.57.225: bytes=32 time=5ms TTL=61
Reply from 104.120.57.225: bytes=32 time=5ms TTL=61
Reply from 104.120.57.225: bytes=32 time=2ms TTL=61
Reply from 104.120.57.225: bytes=32 time=2ms TTL=61

Ping statistics for 104.120.57.225:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 5ms, Average = 3ms
```

Observations

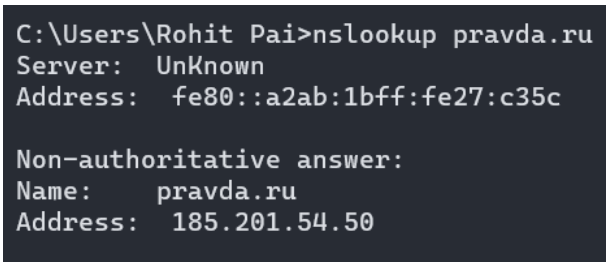
I observed that some of the sites that were mentioned in the exercise did not have their server open to ICMP requests and was the reason for Request Timed Out.

I also observed that RTT indeed depends on the physical distance between my device and the server. Pinging www.nintendo.co.jp in Japan (Average = 3 ms) took the least time as it is closest to Mumbai as compared to cities in USA (Average of 2 sites = 331.5 ms) and England (Average = 149 ms).

I also observed that the first packet that sent in while pinging a site for the first time has a very large RTT compared to the others.

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>

Using nslookup to find IP Address of pravda.ru



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!!!.)

Output (This is the output for ipconfig. The output for ipconfig /all is stored in a log file) –

```
Windows IP Configuration


Wireless LAN adapter Local Area Connection* 4:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::ed99:7b8e:2679:699e%11
   IPv4 Address. . . . . . . . . . . : 192.168.132.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::f518:f08d:c63b:66b5%17
   IPv4 Address. . . . . . . . . . . : 192.168.61.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : Dlink
   IPv6 Address. . . . . . . . . . . : fd01::b9ca:4100:1343:45a1
   Temporary IPv6 Address. . . . . . : fd01::791c:d72f:fd39:be51
   Link-local IPv6 Address . . . . . : fe80::b9ca:4100:1343:45a1%8
   IPv4 Address. . . . . . . . . . . : 192.168.0.26
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::a2ab:1bff:fe27:c35c%8
                                       192.168.0.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

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.)

Output (This is a sample of the output, the entire output is store in a log file) -

```
C:\Users\Rohit Pai\Desktop\DCCN>netstat -t -n

Active Connections

  Proto  Local Address          Foreign Address        State           Offload State
  TCP    127.0.0.1:5354         127.0.0.1:49671        ESTABLISHED     InHost
  TCP    127.0.0.1:5354         127.0.0.1:49672        ESTABLISHED     InHost
  TCP    127.0.0.1:27015        127.0.0.1:49737        ESTABLISHED     InHost
  TCP    127.0.0.1:49666        127.0.0.1:56851        ESTABLISHED     InHost
  TCP    127.0.0.1:49671        127.0.0.1:5354         ESTABLISHED     InHost
  TCP    127.0.0.1:49672        127.0.0.1:5354         ESTABLISHED     InHost
  TCP    127.0.0.1:49674        127.0.0.1:49675        ESTABLISHED     InHost
  TCP    127.0.0.1:49675        127.0.0.1:49674        ESTABLISHED     InHost
  TCP    127.0.0.1:49681        127.0.0.1:49690        ESTABLISHED     InHost
  TCP    127.0.0.1:49681        127.0.0.1:49701        ESTABLISHED     InHost
  TCP    127.0.0.1:49681        127.0.0.1:49703        ESTABLISHED     InHost
  TCP    127.0.0.1:49681        127.0.0.1:49705        ESTABLISHED     InHost
  TCP    127.0.0.1:49681        127.0.0.1:49706        ESTABLISHED     InHost
  TCP    127.0.0.1:49681        127.0.0.1:49711        ESTABLISHED     InHost
  TCP    127.0.0.1:49681        127.0.0.1:49718        ESTABLISHED     InHost
  TCP    127.0.0.1:49690        127.0.0.1:49681        ESTABLISHED     InHost
  TCP    127.0.0.1:49691        127.0.0.1:49692        ESTABLISHED     InHost
  TCP    127.0.0.1:49692        127.0.0.1:49691        ESTABLISHED     InHost
  TCP    127.0.0.1:49693        127.0.0.1:61900        ESTABLISHED     InHost
  TCP    127.0.0.1:49694        127.0.0.1:49695        ESTABLISHED     InHost
  TCP    127.0.0.1:49695        127.0.0.1:49694        ESTABLISHED     InHost
  TCP    127.0.0.1:49701        127.0.0.1:49681        ESTABLISHED     InHost
  TCP    127.0.0.1:49703        127.0.0.1:49681        ESTABLISHED     InHost
  TCP    127.0.0.1:49705        127.0.0.1:49681        ESTABLISHED     InHost
  TCP    127.0.0.1:49706        127.0.0.1:49681        ESTABLISHED     InHost
  TCP    127.0.0.1:49711        127.0.0.1:49681        ESTABLISHED     InHost
  TCP    127.0.0.1:49713        127.0.0.1:49714        ESTABLISHED     InHost
  TCP    127.0.0.1:49714        127.0.0.1:49713        ESTABLISHED     InHost
  TCP    127.0.0.1:49718        127.0.0.1:49681        ESTABLISHED     InHost
  TCP    127.0.0.1:49723        127.0.0.1:49724        ESTABLISHED     InHost
  TCP    127.0.0.1:49724        127.0.0.1:49723        ESTABLISHED     InHost
  TCP    127.0.0.1:49737        127.0.0.1:27015        ESTABLISHED     InHost
  TCP    127.0.0.1:56851        127.0.0.1:49666        ESTABLISHED     InHost
  TCP    127.0.0.1:61900        127.0.0.1:49693        ESTABLISHED     InHost
```

telnet — Telnet is an old program for remote login. It's not used so much for that any more, since it has no security features. But basically, all it does is open a connection to a server and allow server and client to send lines of plain text to each other. It can be used to check that it's possible to connect to a server and, if the server communicates in plain text, even to interact with the server by hand. Since the Web uses a plain text protocol, you can use telnet to connect to a web client and play the part of the web browser. I will suggest that you to do this with your own web server when you write it, but you might want to try it now. When you use telnet in this way, you need to specify both the host and the port number to which you want to connect: telnet <host> <port>. For example, to connect to the web server on www.spit.ac.in: telnet spit.ac.in 80

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`).

Tracing route to ee.iitb.ac.in

```
C:\Users\Rohit Pai>tracert www.ee.iitb.ac.in

Tracing route to www.ee.iitb.ac.in [103.21.125.132]
over a maximum of 30 hops:

  1    78 ms     *        6 ms  Dlink-Router.Dlink [192.168.0.1]
  2    14 ms    16 ms     5 ms  10.153.128.1
  3     9 ms     6 ms    11 ms  14.143.59.189.static-mumbai.vsnl.net.in [14.143.59.189]
  4     7 ms     6 ms    15 ms  172.23.78.230
  5    10 ms    10 ms     9 ms  115.113.165.62.static-mumbai.vsnl.net.in [115.113.165.62]
  6     *        *        *     Request timed out.
  7     *        *        *     Request timed out.
  8     9 ms     8 ms     5 ms  115.110.234.170.static.Mumbai.vsnl.net.in [115.110.234.170]
  9     *        *        *     Request timed out.
 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.
```

Tracing route to mscs.mu.edu

```
C:\Users\Rohit Pai\Desktop\DCCN\Lab\Experiment 2>tracert mscs.mu.edu

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

  1   324 ms     6 ms     4 ms  Dlink-Router.Dlink [192.168.0.1]
  2     5 ms     9 ms    10 ms  10.153.128.1
  3    24 ms     6 ms     4 ms  14.143.59.189.static-mumbai.vsnl.net.in [14.143.59.189]
  4    12 ms    10 ms     4 ms  172.28.132.241
  5    42 ms    11 ms     8 ms  ix-ae-0-100.tcore2.mlv-mumbai.as6453.net [180.87.39.25]
  6   114 ms   114 ms   116 ms  if-ae-2-2.tcore1.mlv-mumbai.as6453.net [180.87.38.1]
  7   117 ms   111 ms   112 ms  if-ae-5-6.tcore1.wyn-marseille.as6453.net [180.87.38.126]
  8   175 ms   115 ms   113 ms  if-ae-21-2.tcore1.pye-paris.as6453.net [80.231.154.208]
  9   115 ms   117 ms   110 ms  if-ae-11-2.tcore1.pvu-paris.as6453.net [80.231.153.49]
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12   306 ms   285 ms   254 ms  MARQUETTE-U.ear3.Chicago2.Level3.net [4.16.38.70]
 13   224 ms   231 ms   227 ms  134.48.10.27
 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.
```

Tracing route to www.cs.grinnell.edu

```
C:\Users\Rohit Pai\Desktop\DCCN\Lab\Experiment 2>tracert www.cs.grinnell.edu

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

  1    73 ms     9 ms     1 ms  Dlink-Router.Dlink [192.168.0.1]
  2     4 ms    12 ms     4 ms  10.153.128.1
  3     4 ms     6 ms     9 ms  14.143.59.193.static-mumbai.vsnl.net.in [14.143.59.193]
  4    31 ms    26 ms    42 ms  172.31.244.45
  5    27 ms    45 ms    26 ms  ix-ae-4-2.tcore2.cxr-chennai.as6453.net [180.87.37.1]
  6   241 ms   237 ms   239 ms  if-ae-9-2.tcore2.mlv-mumbai.as6453.net [180.87.37.10]
  7   241 ms   239 ms   241 ms  if-ae-2-2.tcore1.mlv-mumbai.as6453.net [180.87.38.1]
  8   248 ms     *      251 ms  if-ae-5-6.tcore1.wyn-marseille.as6453.net [180.87.38.126]
  9   239 ms   237 ms   238 ms  if-ae-2-2.tcore2.wyn-marseille.as6453.net [80.231.217.2]
 10   269 ms     *      255 ms  if-ae-9-2.tcore2.l78-london.as6453.net [80.231.200.14]
 11   478 ms   239 ms   258 ms  if-ae-15-2.tcore2.ldn-london.as6453.net [80.231.131.118]
 12   264 ms   275 ms   238 ms  if-ae-32-2.tcore2.nto-newyork.as6453.net [63.243.216.22]
 13   253 ms   252 ms   264 ms  if-ae-26-2.tcore1.ct8-chicago.as6453.net [216.6.81.29]
 14     *      238 ms     *     63.243.129.121
 15   240 ms   257 ms   246 ms  ae18.cr02.chcg23-il.us.windstream.net [169.130.82.11]
 16     *        *        *     Request timed out.
 17   246 ms   247 ms   251 ms  et3-1-0-0.agr03.desm01-ia.us.windstream.net [40.128.250.43]
 18   264 ms   250 ms   250 ms  et4-1-0-0.agr04.desm01-ia.us.windstream.net [40.136.117.253]
 19   248 ms   250 ms   248 ms  ae4-0.pe05.grnl01-ia.us.windstream.net [40.128.251.179]
 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.
```

Tracing route to csail.mit.edu

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

  1    73 ms     *        6 ms  Dlink-Router.Dlink [192.168.0.1]
  2     3 ms     4 ms     8 ms  10.153.128.1
  3     9 ms     5 ms     3 ms  14.143.59.189.static-mumbai.vsnl.net.in [14.143.59.189]
  4    12 ms     8 ms    11 ms  172.28.132.241
  5     7 ms     4 ms     8 ms  ix-ae-0-100.tcore2.mlv-mumbai.as6453.net [180.87.39.25]
  6   228 ms   207 ms   221 ms  if-ae-2-2.tcore1.mlv-mumbai.as6453.net [180.87.38.1]
  7     *      202 ms     *     if-ae-29-8.tcore1.wyn-marseille.as6453.net [80.231.217.110]
  8   203 ms   206 ms   229 ms  if-ae-2-2.tcore2.wyn-marseille.as6453.net [80.231.217.2]
  9   206 ms   224 ms   204 ms  if-ae-9-2.tcore2.l78-london.as6453.net [80.231.200.14]
 10   204 ms   212 ms   205 ms  if-ae-15-2.tcore2.ldn-london.as6453.net [80.231.131.118]
 11   201 ms   204 ms   205 ms  if-ae-32-3.tcore2.nto-newyork.as6453.net [80.231.20.107]
 12   204 ms   201 ms   204 ms  if-ae-12-2.tcore1.n75-newyork.as6453.net [66.110.96.5]
 13   202 ms   217 ms   202 ms  66.110.96.150
 14   203 ms   201 ms   201 ms  be-10390-cr02.newyork.ny.ibone.comcast.net [68.86.83.89]
 15   201 ms   266 ms   226 ms  be-1202-cs02.newyork.ny.ibone.comcast.net [96.110.38.37]
 16   214 ms   213 ms   208 ms  96.110.42.6
 17   237 ms   211 ms   212 ms  ae0-0-eg-bstpmall74w.boston.ma.boston.comcast.net [68.86.238.34]
 18   208 ms   205 ms   207 ms  50-201-57-174-static.hfc.comcastbusiness.net [50.201.57.174]
 19   208 ms   208 ms   210 ms  dmz-rtr-1-external-rtr-3.mit.edu [18.0.161.13]
 20   226 ms   206 ms   207 ms  dmz-rtr-2-dmz-rtr-1-1.mit.edu [18.0.161.6]
 21   209 ms   209 ms   205 ms  mitnet.core-1-ext.csail.mit.edu [18.4.7.65]
 22     *        *      219 ms  core-1-ext.bdr.csail.mit.edu [128.30.13.26]
 23   210 ms   210 ms   209 ms  bdr.core-1.csail.mit.edu [128.30.0.246]
 24   208 ms   209 ms   208 ms  inquir-3ld.csail.mit.edu [128.30.2.109]

Trace complete.
```

Tracing route to cs.stanford.edu

```
C:\Users\Rohit Pai\Desktop\DCCN\Lab\Experiment 2>tracert cs.stanford.edu

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

  1   107 ms     5 ms     2 ms  Dlink-Router.Dlink [192.168.0.1]
  2    12 ms     5 ms    11 ms  10.153.128.1
  3    23 ms    22 ms     6 ms  14.143.59.193.static-mumbai.vsnl.net.in [14.143.59.193]
  4    32 ms    36 ms    29 ms  172.31.244.45
  5    35 ms    70 ms    67 ms  ix-ae-4-2.tcore2.cxr-chennai.as6453.net [180.87.37.1]
  6   240 ms   240 ms   239 ms  if-ae-10-4.tcore2.svw-singapore.as6453.net [180.87.67.16]
  7   252 ms   239 ms   240 ms  if-ae-7-2.tcore2.lvw-losangeles.as6453.net [180.87.15.26]
  8   316 ms   326 ms   237 ms  if-ae-2-2.tcore1.lvw-losangeles.as6453.net [66.110.59.1]
  9   239 ms   237 ms   263 ms  las-b24-link.telia.net [80.239.128.214]
 10   246 ms     *      246 ms  palo-b24-link.telia.net [62.115.119.90]
 11   252 ms   256 ms   252 ms  palo-b1-link.telia.net [62.115.122.169]
 12   246 ms   244 ms   246 ms  hurricane-ic-308019-palo-b1.c.telia.net [80.239.167.174]
 13   250 ms   251 ms   248 ms  stanford-university.100gigabitethernet5-1.core1.pao1.he.net [184.105.177.238]
 14   251 ms   249 ms   258 ms  csee-west-rtr-vl3.SUNet [171.66.255.140]
 15   251 ms   244 ms   254 ms  CS.stanford.edu [171.64.64.64]

Trace complete.
```

Tracing route to cs.manchester.ac.uk

```
C:\Users\Rohit Pai\Desktop\DCCN\Lab\Experiment 2>tracert cs.manchester.ac.uk

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

  1    71 ms     1 ms     1 ms  Dlink-Router.Dlink [192.168.0.1]
  2     8 ms     4 ms     2 ms  10.153.128.1
  3     7 ms     6 ms     3 ms  14.143.59.193.static-mumbai.vsnl.net.in [14.143.59.193]
  4     5 ms     6 ms     9 ms  172.28.132.238
  5     6 ms    14 ms    14 ms  ix-ae-0-100.tcore1.mlv-mumbai.as6453.net [180.87.38.5]
  6   117 ms   135 ms   123 ms  if-ae-29-8.tcore1.wyn-marseille.as6453.net [80.231.217.110]
  7   137 ms   118 ms   131 ms  if-ae-21-2.tcore1.pye-paris.as6453.net [80.231.154.208]
  8   119 ms   148 ms   111 ms  if-ae-11-2.tcore1.pvu-paris.as6453.net [80.231.153.49]
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11   130 ms   126 ms   129 ms  JANET.bear1.Manchester1.Level3.net [212.187.174.238]
 12   129 ms   134 ms   128 ms  ae22.manckh-sbr2.ja.net [146.97.35.189]
 13   147 ms   130 ms   177 ms  ae23.mancrh-rbr1.ja.net [146.97.38.42]
 14     *        *      153 ms  universityofmanchester.ja.net [146.97.169.2]
 15   139 ms   133 ms   130 ms  130.88.249.194
 16     *        *        *     Request timed out.
 17   140 ms   135 ms   135 ms  gw-jh.its.manchester.ac.uk [130.88.250.32]
 18   136 ms   130 ms   135 ms  eps.its.man.ac.uk [130.88.101.49]

Trace complete.
```

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

Tracing route to www.hws.edu

```
C:\Users\Rohit Pai\Desktop\DCCN\Lab\Experiment 2>tracert www.hws.edu

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

  1    71 ms     1 ms     1 ms  Dlink-Router.Dlink [192.168.0.1]
  2     4 ms     2 ms     4 ms  10.153.128.1
  3     9 ms     2 ms     3 ms  14.143.59.193.static-mumbai.vsnl.net.in [14.143.59.193]
  4     4 ms     4 ms     3 ms  172.28.132.238
  5     5 ms     3 ms     3 ms  ix-ae-0-100.tcore1.mlv-mumbai.as6453.net [180.87.38.5]
  6   121 ms   119 ms   111 ms  if-ae-29-8.tcore1.wyn-marseille.as6453.net [80.231.217.110]
  7   115 ms   120 ms   113 ms  if-ae-21-2.tcore1.pye-paris.as6453.net [80.231.154.208]
  8   111 ms   114 ms   111 ms  if-ae-11-2.tcore1.pvu-paris.as6453.net [80.231.153.49]
  9     *        *        *     Request timed out.
 10   111 ms   114 ms   114 ms  ae-1-3104.edge3.Paris1.Level3.net [4.69.161.110]
 11   111 ms   114 ms   112 ms  global-crossing-xe-level3.paris1.level3.net [4.68.63.230]
 12   205 ms   207 ms   208 ms  roc1-ar5-xe-11-0-0-0.us.twtelecom.net [35.248.1.162]
 13   214 ms   209 ms   221 ms  66-195-65-170.static.ctl.one [66.195.65.170]
 14   219 ms   210 ms   215 ms  nat.hws.edu [64.89.144.100]
 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.
```

Tracing route to math.hws.edu

```
C:\Users\Rohit Pai\Desktop\DCCN\Lab\Experiment 2>tracert math.hws.edu

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

  1    76 ms     5 ms     1 ms  Dlink-Router.Dlink [192.168.0.1]
  2     2 ms     2 ms     4 ms  10.153.128.1
  3     6 ms     6 ms     7 ms  14.143.59.189.static-mumbai.vsnl.net.in [14.143.59.189]
  4     4 ms     5 ms     3 ms  172.28.132.241
  5     4 ms     8 ms     3 ms  ix-ae-0-100.tcore2.mlv-mumbai.as6453.net [180.87.39.25]
  6   133 ms   110 ms   110 ms  if-ae-2-2.tcore1.mlv-mumbai.as6453.net [180.87.38.1]
  7   118 ms   113 ms   112 ms  if-ae-5-2.tcore1.wyn-marseille.as6453.net [80.231.217.29]
  8   121 ms   115 ms   113 ms  if-ae-8-1600.tcore1.pye-paris.as6453.net [80.231.217.6]
  9   115 ms   114 ms   112 ms  if-ae-11-2.tcore1.pvu-paris.as6453.net [80.231.153.49]
 10     *        *        *     Request timed out.
 11   111 ms   116 ms   112 ms  ae-1-3104.edge3.Paris1.Level3.net [4.69.161.110]
 12   121 ms   135 ms   133 ms  global-crossing-xe-level3.paris1.level3.net [4.68.63.230]
 13   205 ms   205 ms   206 ms  roc1-ar5-xe-11-0-0-0.us.twtelecom.net [35.248.1.162]
 14   209 ms   209 ms   212 ms  66-195-65-170.static.ctl.one [66.195.65.170]
 15   210 ms   213 ms   210 ms  nat.hws.edu [64.89.144.100]
 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.
```

Observations

The difference is the two results is that the IP Address of the 2 destinations is slightly different. www.hws.edu translates to 64.89.145.159 while math.hws.edu translates to 64.89.144.237.

I can also see that the request gets timed out after the node nat.hws.edu on both the sites meaning that the node after that has blocked ICMP requests.

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.

Tracing route to www.google.com at 13:57 on 28th August, 2020

```
C:\Users\Rohit Pai\Desktop\DCCN\Lab\Experiment 2>tracert www.google.com

Tracing route to www.google.com [216.58.199.132]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  Dlink-Router.Dlink [192.168.0.1]
  2     3 ms     5 ms     2 ms  10.153.128.1
  3    44 ms     2 ms     5 ms  45.127.44.242
  4     4 ms     5 ms     3 ms  108.170.248.193
  5     4 ms     4 ms     4 ms  72.14.236.75
  6     4 ms     4 ms     3 ms  bom07s01-in-f132.1e100.net [216.58.199.132]

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 first two nodes are always common to all the routes I have traced.

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 the number of nodes and the location of the nodes. We might assume that the number of nodes increase with the physical distance but it is not guaranteed.

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?

   No, there isn't any defined relationship between number of nodes and latency.

I can see that the latency increases with an increase in the number of nodes but we cannot guarantee that x nodes would give y latency.

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*).
Note: Whois is not an inbuilt command in Windows. I installed the Sysinternals package by Mark Russinovich which has Whois implemented for windows.

Whois on windows (stored in a file called whois_spit.ac.in.log)

Whois on Ubuntu (stored in a file called whois_ubuntu_spit.ac.in.log)

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.

Redacted output (Full output in whois_ubuntu_google.com.log)

```
rohit@LAPTOP-VI0PE9HU:/mnt/c/Users/Rohit Pai$ 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: 2020-08-28T08:40:55Z <<<
```

Running the whois command on google.com gives us information on the registry domain id of Google and the name servers of google.com. We also get details on the registrant organization, admin organization and tech organization for the domain. This includes the name, state and country of each organization.

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.

I used nslookup to find out the external IP address of spit.ac.in

```
rohit@LAPTOP-VI0PE9HU:/mnt/c/Users/Rohit Pai/Desktop/DCCN/Lab/Experiment 2$ nslookup spit.ac.in
Server:         172.30.224.1
Address:        172.30.224.1#53

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

The IP Address of spit.ac.in is 43.252.193.19

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.)

Using geolocation program to find the location of spit.ac.in's server

```
C:\Users\Rohit Pai>curl ipinfo.io/43.252.193.19
{
  "ip": "43.252.193.19",
  "city": "Mumbai",
  "region": "Maharashtra",
  "country": "IN",
  "loc": "19.0728,72.8826",
  "org": "AS17625 BlazeNet's Network",
  "postal": "400070",
  "timezone": "Asia/Kolkata",
  "readme": "https://ipinfo.io/missingauth"
}
```

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.