Name: Karan Shah
Class: TE Comps
UID: 2018130048
Roll no: 54
Batch: D

CEL 51, DCCN, Monsoon 2020
Lab 2: Basic Network Utilities

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

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

Some Basic command line Networking utilities

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

ping — The command ping <host> sends a series of packets and expects to receieve a response to each packet. When a return packet is received, ping reports the round trip time (the time between sending the packet and receiving the response). Some routers and firewalls block ping requests, so you might get no reponse at all. Ping can be used to check whether a computer is up and running, to measure network delay time, and to check for dropped packets indicating network congestion. Note that <host> can be either a domain name or an IP address. By default, ping will send a packet every second indefinitely; stop it with Control-C

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

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

The syntax in Windows is:

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

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

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

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

EXPERIMENTS WITH PING

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

QUESTIONS ABOUT LATENCY

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

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

Answers:

1. Average RTT can vary between different hosts due to Processing delay, queuing delay, Transmission delay , and Propagation delay.

• Processing delay – time it takes a router to process the packet header, depends on the processing speed of the switch.

• Queuing delay – time the packet spends in routing queues depends on the number of packets, size of the packet and bandwidth.

• Transmission delay – time it takes to push the packet's bits onto the link depends on size of the packet and the bandwidth of the network.

• Propagation delay – time for a signal to reach its destination depends on distance and propagation speed.

2. Yes, the average RTT increases with packet size as Queuing delay and Transmission delay increases as they both rely on size of packets eventually increasing the average RTT.

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).

Hostname: google.com
Count: 10

Packet size - 32 bytes

File Edit Format View Help

```
C:\Users\Karan>ping -n 10 google.com

Pinging google.com [172.217.160.206] with 32 bytes of data:
Reply from 172.217.160.206: bytes=32 time=2ms TTL=120
Reply from 172.217.160.206: bytes=32 time=3ms TTL=120
Reply from 172.217.160.206: bytes=32 time=2ms TTL=120
Reply from 172.217.160.206: bytes=32 time=13ms TTL=120
Reply from 172.217.160.206: bytes=32 time=2ms TTL=120
Reply from 172.217.160.206: bytes=32 time=1ms TTL=120
Reply from 172.217.160.206: bytes=32 time=42ms TTL=120
Reply from 172.217.160.206: bytes=32 time=33ms TTL=120
Reply from 172.217.160.206: bytes=32 time=48ms TTL=120
Reply from 172.217.160.206: bytes=32 time=101ms TTL=120

Ping statistics for 172.217.160.206:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 101ms, Average = 24ms
```

Packet size - 64 bytes

File Edit Format View Help

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

Pinging google.com [172.217.160.206] with 64 bytes of data:
Reply from 172.217.160.206: bytes=64 time=8ms TTL=120
Reply from 172.217.160.206: bytes=64 time=79ms TTL=120
Reply from 172.217.160.206: bytes=64 time=142ms TTL=120
Reply from 172.217.160.206: bytes=64 time=31ms TTL=120
Reply from 172.217.160.206: bytes=64 time=63ms TTL=120
Reply from 172.217.160.206: bytes=64 time=29ms TTL=120
Reply from 172.217.160.206: bytes=64 time=698ms TTL=120
Reply from 172.217.160.206: bytes=64 time=1244ms TTL=120
Reply from 172.217.160.206: bytes=64 time=998ms TTL=120
Reply from 172.217.160.206: bytes=64 time=2000ms TTL=120

Ping statistics for 172.217.160.206:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 2000ms, Average = 529ms
```

Packet size - 100 bytes

```
File  Edit  Format  View  Help
C:\Users\Karan>ping -n 10 -l 100 google.com

Pinging google.com [172.217.160.206] with 100 bytes of data:
Reply from 172.217.160.206: bytes=68 (sent 100) time=1888ms TTL=120
Reply from 172.217.160.206: bytes=68 (sent 100) time=1072ms TTL=120
Reply from 172.217.160.206: bytes=68 (sent 100) time=636ms TTL=120
Reply from 172.217.160.206: bytes=68 (sent 100) time=368ms TTL=120
Request timed out.
Reply from 172.217.160.206: bytes=68 (sent 100) time=843ms TTL=120
Reply from 172.217.160.206: bytes=68 (sent 100) time=646ms TTL=120
Reply from 172.217.160.206: bytes=68 (sent 100) time=6ms TTL=120
Reply from 172.217.160.206: bytes=68 (sent 100) time=5ms TTL=120
Reply from 172.217.160.206: bytes=68 (sent 100) time=118ms TTL=120

Ping statistics for 172.217.160.206:
    Packets: Sent = 10, Received = 9, Lost = 1 (10% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 1888ms, Average = 620ms
```

Packet size - 500 bytes

```
File  Edit  Format  View  Help
C:\Users\Karan>ping -n 10 -l 500 google.com

Pinging google.com [172.217.160.206] with 500 bytes of data:
Reply from 172.217.160.206: bytes=68 (sent 500) time=91ms TTL=120
Reply from 172.217.160.206: bytes=68 (sent 500) time=381ms TTL=120
Reply from 172.217.160.206: bytes=68 (sent 500) time=42ms TTL=120
Reply from 172.217.160.206: bytes=68 (sent 500) time=291ms TTL=120
Reply from 172.217.160.206: bytes=68 (sent 500) time=121ms TTL=120
Reply from 172.217.160.206: bytes=68 (sent 500) time=63ms TTL=120
Reply from 172.217.160.206: bytes=68 (sent 500) time=399ms TTL=120
Reply from 172.217.160.206: bytes=68 (sent 500) time=655ms TTL=120
Reply from 172.217.160.206: bytes=68 (sent 500) time=449ms TTL=120
Reply from 172.217.160.206: bytes=68 (sent 500) time=157ms TTL=120

Ping statistics for 172.217.160.206:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 42ms, Maximum = 655ms, Average = 264ms
```

Packet size - 1000 bytes

File Edit Format View Help

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

Pinging google.com [172.217.160.206] with 1000 bytes of data:
Reply from 172.217.160.206: bytes=68 (sent 1000) time=1526ms TTL=120
Reply from 172.217.160.206: bytes=68 (sent 1000) time=1046ms TTL=120
Request timed out.
Reply from 172.217.160.206: bytes=68 (sent 1000) time=1133ms TTL=120
Request timed out.
Reply from 172.217.160.206: bytes=68 (sent 1000) time=1057ms TTL=120
Reply from 172.217.160.206: bytes=68 (sent 1000) time=1492ms TTL=120
Request timed out.
Reply from 172.217.160.206: bytes=68 (sent 1000) time=1131ms TTL=120
Reply from 172.217.160.206: bytes=68 (sent 1000) time=976ms TTL=120

Ping statistics for 172.217.160.206:
    Packets: Sent = 10, Received = 7, Lost = 3 (30% loss),
Approximate round trip times in milli-seconds:
    Minimum = 976ms, Maximum = 1526ms, Average = 1194ms
```

Packet size - 1400 bytes

File Edit Format View Help

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

Pinging google.com [172.217.160.206] with 1400 bytes of data:
Reply from 172.217.160.206: bytes=68 (sent 1400) time=860ms TTL=120
Reply from 172.217.160.206: bytes=68 (sent 1400) time=606ms TTL=120
Request timed out.
Reply from 172.217.160.206: bytes=68 (sent 1400) time=399ms TTL=120
Reply from 172.217.160.206: bytes=68 (sent 1400) time=737ms TTL=120
Reply from 172.217.160.206: bytes=68 (sent 1400) time=290ms TTL=120
Request timed out.
Reply from 172.217.160.206: bytes=68 (sent 1400) time=34ms TTL=120
Reply from 172.217.160.206: bytes=68 (sent 1400) time=187ms TTL=120
Reply from 172.217.160.206: bytes=68 (sent 1400) time=6ms TTL=120

Ping statistics for 172.217.160.206:
    Packets: Sent = 10, Received = 8, Lost = 2 (20% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 860ms, Average = 389ms
```

Observations:

When google.com is pinged with 10 packets of various sizes, IP address 172.217.160.206 is pinged in all cases. The average RTT varies for each size packets pinged and is not directly proportional with the size of the packets sent.

Pinging other hosts:

a) spit.ac.in

File Edit Format View Help

```
C:\Users\Karan>ping -n 10 -l 100 spit.ac.in

Pinging spit.ac.in [43.252.193.19] with 100 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 43.252.193.19:
    Packets: Sent = 10, Received = 0, Lost = 10 (100% loss),
```

Observations:

When host spit.ac.in was pinged with 10 packets of size 100 bytes, there was 100% packet loss. This could be because some routers and firewalls block ping requests so no response is received on pinging.

b) berkeley.edu

```
File  Edit  Format  View  Help
C:\Users\Karan>ping -n 10 -l 100 berkeley.edu

Pinging berkeley.edu [35.163.72.93] with 100 bytes of data:
Reply from 35.163.72.93: bytes=100 time=350ms TTL=37
Reply from 35.163.72.93: bytes=100 time=327ms TTL=37
Reply from 35.163.72.93: bytes=100 time=331ms TTL=37
Reply from 35.163.72.93: bytes=100 time=344ms TTL=37
Reply from 35.163.72.93: bytes=100 time=358ms TTL=37
Reply from 35.163.72.93: bytes=100 time=375ms TTL=37
Reply from 35.163.72.93: bytes=100 time=699ms TTL=37
Reply from 35.163.72.93: bytes=100 time=312ms TTL=37
Reply from 35.163.72.93: bytes=100 time=318ms TTL=37
Reply from 35.163.72.93: bytes=100 time=338ms TTL=37

Ping statistics for 35.163.72.93:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 312ms, Maximum = 699ms, Average = 375ms
```

Observations:

When host berkeley.edu is pinged with 100 bytes packets, response is received from an IP address 35.163.72.93. The average RTT is almost 0.4 seconds.

Factors Influencing RTT

Actual round trip time can be influenced by:

- Distance – 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.
- Transmission medium – 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.
- Number of network hops – 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.
- Traffic levels – RTT typically increases when a network is congested with high levels of traffic. Conversely, low traffic times can result in decreased RTT.
- Server response time – 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>

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!!!.)

ipconfig:

File Edit Format View Help

```
C:\Users\Karan>ipconfig -all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-HODVLTA
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe FE Family Controller
   Physical Address. . . . . . . . . : 54-BF-64-16-C4-90
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Physical Address. . . . . . . . . : 94-B8-6D-23-AC-B3
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 11:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   Physical Address. . . . . . . . . : 96-B8-6D-23-AC-B2
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
```

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 3165
   Physical Address. . . . . . . . . : 94-B8-6D-23-AC-B2
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::a51a:60d5:6d87:f4b3%9(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.104(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 13 August 2020 09:03:24
   Lease Expires . . . . . . . . . . : 13 August 2020 18:23:44
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 110409837
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-22-9F-0B-B8-54-BF-64-16-C4-90
   DNS Servers . . . . . . . . . . . : 192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

netstat — The netstat command gives information about network connections. I often use netstat -t -n which lists currently open TCP connections (that's the "-t" option) by IP address rather than domain name (that's the "-n" option). Add the option "-l" (lower case ell) to list listening sockets, that is sockets that have been opened by server programs to wait for connection requests from clients: netstat -t -n -l.(On Mac, use netstat -p tcp to list tcp connections, and add "-a" to include listening sockets in the list.)

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

traceroute — Traceroute is discussed in man utility. The command traceroute <host> will show routers encountered by packets on their way from your computer to a specified <host>. For each n = 1, 2, 3,..., traceroute sends a packet with "time-to-live" (ttl) equal to n. Every time a router forwards a packet, it decreases the ttl of the packet by one. If the ttl drops to zero, the router discards the packet and sends an error message back to the sender of the packet. (Again, as with ping, the packets might be blocked or might not even be sent, so that the error messages will never be received.) The sender gets the identity of the router from the source of the error message. Traceroute will send packets until n reaches some set upper bound or until a packet actually gets through to the destination. It actually does this three times for each n. In this way, it identifies routers that are one step, two steps, three steps, ...

away from the source computer. A packet for which no response is received is indicated in the output as a *.

Traceroute is installed on the computers. If was not installed in your virtual server last week, but you can install it with the command sudo apt-get install traceroute

The path taken through a network, can be measured using traceroute. The syntax for the command in Linux is:

```
traceroute <hostname>
```

The syntax in Windows is:

```
tracert <hostname>
```

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

1.2.1 EXPERIMENTS WITH TRACEROUTE

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

1. ee.iitb.ac.in
2. mscs.mu.edu
3. www.cs.grinnell.edu
4. csail.mit.edu
5. cs.stanford.edu
6. cs.manchester.ac.uk

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

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.

Traceroute:

A) iitb.ac.in

File Edit Format View Help

```
C:\Users\Karan>tracert iitb.ac.in

Tracing route to iitb.ac.in [103.21.127.114]
over a maximum of 30 hops:

  1     1 ms    <1 ms     3 ms  192.168.1.1
  2     3 ms    15 ms     1 ms  172.20.0.1
  3     *        *        *     Request timed out.
  4     3 ms    10 ms     4 ms  14.143.59.13.static-mumbai.vsnl.net.in [14.143.59.13]
  5     4 ms     4 ms     3 ms  115.110.234.170.static.Mumbai.vsnl.net.in [115.110.234.170]
  6     *        *        *     Request timed out.
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  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.
```

B) berkeley.edu

File Edit Format View Help

```
C:\Users\Karan>tracert berkeley.edu

Tracing route to berkeley.edu [35.163.72.93]
over a maximum of 30 hops:

  1     7 ms     1 ms     1 ms  192.168.1.1
  2    62 ms     2 ms     4 ms  172.20.0.1
  3     *        *        *     Request timed out.
  4     2 ms     2 ms     2 ms  14.143.59.13.static-mumbai.vsnl.net.in [14.143.59.13]
  5     5 ms     3 ms     2 ms  172.23.78.233
  6    24 ms    24 ms    24 ms  172.31.244.45
  7    75 ms    30 ms    25 ms  ix-ae-4-2.tcore2.cxr-chennai.as6453.net [180.87.37.1]
  8   254 ms   286 ms   307 ms  if-ae-10-4.tcore2.svw-singapore.as6453.net [180.87.67.16]
  9   238 ms   248 ms   231 ms  if-ae-7-2.tcore2.lvw-losangeles.as6453.net [180.87.15.26]
 10   357 ms   341 ms   366 ms  if-ae-2-2.tcore1.lvw-losangeles.as6453.net [66.110.59.1]
 11   324 ms   280 ms   696 ms  64.86.197.113
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14   333 ms   311 ms   385 ms  54.239.44.20
 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.
```

C) math.hws.edu

```
File  Edit  Format  View  Help
C:\Users\Karan>tracert math.hws.edu

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

  1     1 ms     1 ms     1 ms  192.168.1.1
  2    47 ms    34 ms     2 ms  172.20.0.1
  3     *        *       92 ms  dhcp-192-196-29.in2cable.com [203.192.196.29]
  4     3 ms     6 ms     6 ms  115.113.165.121.static-mumbai.vsnl.net.in [115.113.165.121]
  5     5 ms   116 ms     4 ms  172.23.78.237
  6    14 ms     3 ms     4 ms  ix-ae-0-100.tcore1.mlv-mumbai.as6453.net [180.87.38.5]
  7   176 ms     *      239 ms  if-ae-5-2.tcore1.wyn-marseille.as6453.net [80.231.217.29]
  8   110 ms   115 ms   121 ms  if-ae-21-2.tcore1.pye-paris.as6453.net [80.231.154.208]
  9   177 ms   193 ms   230 ms  if-ae-11-2.tcore1.pvu-paris.as6453.net [80.231.153.49]
 10   115 ms   118 ms   114 ms  80.231.153.66
 11   376 ms   285 ms   133 ms  ae-2-3204.edge3.Paris1.Level3.net [4.69.161.114]
 12   121 ms   110 ms   136 ms  global-crossing-xe-level3.paris1.level3.net [4.68.63.230]
 13   217 ms   210 ms   209 ms  roc1-ar5-xe-11-0-0-0.us.twtelecom.net [35.248.1.162]
 14   210 ms   235 ms   258 ms  66-195-65-170.static.ctl.one [66.195.65.170]
 15   224 ms   206 ms   206 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.
```

D) www.hws.edu

```
File  Edit  Format  View  Help
C:\Users\Karan>tracert www.hws.edu

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

  1    <1 ms     1 ms     1 ms  192.168.1.1
  2     1 ms     1 ms     3 ms  172.20.0.1
  3     4 ms     *        *     dhcp-192-196-29.in2cable.com [203.192.196.29]
  4     4 ms     3 ms     4 ms  115.113.165.121.static-mumbai.vsnl.net.in [115.113.165.121]
  5    43 ms     3 ms     5 ms  172.23.78.237
  6    30 ms     3 ms    24 ms  ix-ae-0-100.tcore1.mlv-mumbai.as6453.net [180.87.38.5]
  7   173 ms   113 ms   117 ms  if-ae-5-2.tcore1.wyn-marseille.as6453.net [80.231.217.29]
  8   112 ms   124 ms   114 ms  if-ae-21-2.tcore1.pye-paris.as6453.net [80.231.154.208]
  9   126 ms   159 ms   112 ms  if-ae-11-2.tcore1.pvu-paris.as6453.net [80.231.153.49]
 10     *        *        *     Request timed out.
 11   131 ms   135 ms   112 ms  ae-2-3204.edge3.Paris1.Level3.net [4.69.161.114]
 12   119 ms   116 ms   125 ms  global-crossing-xe-level3.paris1.level3.net [4.68.63.230]
 13   283 ms   298 ms   245 ms  roc1-ar5-xe-11-0-0-0.us.twtelecom.net [35.248.1.162]
 14   216 ms   215 ms   225 ms  66-195-65-170.static.ctl.one [66.195.65.170]
 15   216 ms   207 ms   207 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.
```

There are request timed out messages which mean that routers didn't respond to the packets.Tracing route happens for a maximum of 30 hops.
The time taken to reach an international router is large compared to reaching a router within the country.
So, we can conclude that distance plays a role in the time taken to transfer packets.

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.

Host: google.com

1 week earlier:

```
File  Edit  Format  View  Help
C:\Users\Karan>tracert google.com

Tracing route to google.com [172.217.160.206]
over a maximum of 30 hops:

  1   225 ms   340 ms     *     192.168.1.1
  2    64 ms    71 ms     6 ms  172.20.0.1
  3     *        3 ms     3 ms  dhcp-192-196-1.in2cable.com [203.192.196.1]
  4   112 ms     3 ms     *     209.85.241.175
  5    33 ms     6 ms     8 ms  216.239.47.149
  6   275 ms     *       67 ms  bom07s16-in-f14.1e100.net [172.217.160.206]

Trace complete.
```

Today:

```
File  Edit  Format  View  Help
C:\Users\Karan>tracert google.com

Tracing route to google.com [216.58.203.206]
over a maximum of 30 hops:

  1     1 ms    <1 ms    <1 ms  192.168.1.1
  2     2 ms     2 ms     2 ms  172.20.0.1
  3     3 ms     1 ms     1 ms  74.125.118.28
  4     4 ms     2 ms     2 ms  108.170.248.209
  5     3 ms     3 ms     3 ms  209.85.246.5
  6     3 ms     2 ms     3 ms  bom07s12-in-f14.1e100.net [216.58.203.206]

Trace complete.
```

Observations:

When the same host is pinged on two different days, the IP address pinged does not necessarily remain the same. The trace route also varies establishing the fact that for the same source and destination, routes taken need not be same.

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 one which is the source's IP address.

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?

   Geographic distance has no correlation with hop count.

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 and the latency of the host.

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.

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

File Edit Format View Help

```
C:\Users\Karan>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.

Conclusion:

I learnt about various network commands such as ping, tracert and ipconfig. I learnt that the main difference between ping and traceroute is that ping is a quick and easy utility to tell if the specified server is reachable and how long will it take to send and receive data from the server whereas traceroute finds the exact route taken to reach the server (upto 30 hops) and time taken by each step.

References:

1) https://mediatemple.net/community/products/dv/204643870/using-thetraceroute-command
2) https://docs.microsoft.com/en-us/windows-server/administration/windowscommands/netstat
3) https://www.geeksforgeeks.org/difference-between-ping-and-traceroute/
4) https://www.inmotionhosting.com/support/website/ssh/read-traceroute/
5)https://people.bath.ac.uk/masrjb/AOCN/exercises6.html#:~:text=Often%20traceroute%20is%20set%20to,weak%20correlation%20with%20hop%20count.&text=It%20can%20decrease%20hop%20count,in%20a%20single%20IP%20hop.