Experiment 2

Harsh Sandesara
Batch C, 49
UID: 2018130045

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

```
harshsandesara@DESKTOP-QMGI8AK:/mnt/c/Harsh$ ping -c 10 -s 64 google.com
PING google.com (142.250.67.142) 64(92) bytes of data.
72 bytes from bom12s06-in-f14.1e100.net (142.250.67.142): icmp_seq=1 ttl=119 time=8.47 ms
72 bytes from bom12s06-in-f14.1e100.net (142.250.67.142): icmp_seq=2 ttl=119 time=4.94 ms
72 bytes from bom12s06-in-f14.1e100.net (142.250.67.142): icmp_seq=3 ttl=119 time=5.51 ms
72 bytes from bom12s06-in-f14.1e100.net (142.250.67.142): icmp_seq=4 ttl=119 time=4.89 ms
72 bytes from bom12s06-in-f14.1e100.net (142.250.67.142): icmp_seq=5 ttl=119 time=4.72 ms
72 bytes from bom12s06-in-f14.1e100.net (142.250.67.142): icmp_seq=6 ttl=119 time=5.29 ms
72 bytes from bom12s06-in-f14.1e100.net (142.250.67.142): icmp_seq=7 ttl=119 time=8.45 ms
72 bytes from bom12s06-in-f14.1e100.net (142.250.67.142): icmp_seq=8 ttl=119 time=5.38 ms
72 bytes from bom12s06-in-f14.1e100.net (142.250.67.142): icmp_seq=9 ttl=119 time=6.35 ms
72 bytes from bom12s06-in-f14.1e100.net (142.250.67.142): icmp_seq=10 ttl=119 time=4.83 ms

--- google.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9009ms
rtt min/avg/max/mdev = 4.723/5.884/8.473/1.362 ms
```

Pinging different hosts:

google.com

```
PING google.com (142.250.67.142) 64(92) bytes of data.
72 bytes from bom12s06-in-f14.1e100.net (142.250.67.142): icmp_seq=1 ttl=118 time=23.6
72 bytes from bom12s06-in-f14.1e100.net (142.250.67.142): icmp_seq=2 ttl=118 time=28.1
72 bytes from bom12s06-in-f14.1e100.net (142.250.67.142): icmp_seq=3 ttl=118 time=891 m
72 bytes from bom12s06-in-f14.1e100.net (142.250.67.142): icmp_seq=4 ttl=118 time=75.2
72 bytes from bom12s06-in-f14.1e100.net (142.250.67.142): icmp_seq=6 ttl=118 time=309 m
72 bytes from bom12s06-in-f14.1e100.net (142.250.67.142): icmp_seq=7 ttl=118 time=40.7
72 bytes from bom12s06-in-f14.1e100.net (142.250.67.142): icmp_seq=8 ttl=118 time=20.8
72 bytes from bom12s06-in-f14.1e100.net (142.250.67.142): icmp_seq=9 ttl=118 time=24.1

--- google.com ping statistics ---
10 packets transmitted, 8 received, 20% packet loss, time 9010ms
rtt min/avg/max/mdev = 20.794/176.532/890.640/284.858 ms
PING google.com (142.250.67.142) 100(128) bytes of data.
```

bing.com

```
PING bing.com (13.107.21.200) 100(128) bytes of data.
108 bytes from 13.107.21.200 (13.107.21.200): icmp_seq=1 ttl=121 time=89.4 ms
108 bytes from 13.107.21.200 (13.107.21.200): icmp_seq=3 ttl=121 time=1017 ms
108 bytes from 13.107.21.200 (13.107.21.200): icmp_seq=4 ttl=121 time=47.4 ms
108 bytes from 13.107.21.200 (13.107.21.200): icmp_seq=5 ttl=121 time=1088 ms
108 bytes from 13.107.21.200 (13.107.21.200): icmp_seq=6 ttl=121 time=88.3 ms
108 bytes from 13.107.21.200 (13.107.21.200): icmp_seq=7 ttl=121 time=1014 ms
108 bytes from 13.107.21.200 (13.107.21.200): icmp_seq=8 ttl=121 time=8.82 ms
108 bytes from 13.107.21.200 (13.107.21.200): icmp_seq=9 ttl=121 time=327 ms
108 bytes from 13.107.21.200 (13.107.21.200): icmp_seq=10 ttl=121 time=83.2 ms

--- bing.com ping statistics ---
10 packets transmitted, 9 received, 10% packet loss, time 9017ms
rtt min/avg/max/mdev = 8.820/418.058/1087.545/447.678 ms, pipe 2
```

coursera.org

```
PING coursera.org (13.227.165.82) 500(528) bytes of data.
508 bytes from server-13-227-165-82.bom51.r.cloudfront.net (13.227.165.82): icmp_seq=1
508 bytes from server-13-227-165-82.bom51.r.cloudfront.net (13.227.165.82): icmp_seq=2
508 bytes from server-13-227-165-82.bom51.r.cloudfront.net (13.227.165.82): icmp_seq=3
508 bytes from server-13-227-165-82.bom51.r.cloudfront.net (13.227.165.82): icmp_seq=4
508 bytes from server-13-227-165-82.bom51.r.cloudfront.net (13.227.165.82): icmp_seq=5
508 bytes from server-13-227-165-82.bom51.r.cloudfront.net (13.227.165.82): icmp_seq=6
508 bytes from server-13-227-165-82.bom51.r.cloudfront.net (13.227.165.82): icmp_seq=7
508 bytes from server-13-227-165-82.bom51.r.cloudfront.net (13.227.165.82): icmp_seq=8
508 bytes from server-13-227-165-82.bom51.r.cloudfront.net (13.227.165.82): icmp_seq=9
508 bytes from server-13-227-165-82.bom51.r.cloudfront.net (13.227.165.82): icmp_seq=10

--- coursera.org ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9011ms
rtt min/avg/max/mdev = 4.815/98.629/336.085/122.489 ms
```

udemy.com

```
PING udemy.com (104.16.92.52) 1000(1028) bytes of data.
1008 bytes from 104.16.92.52 (104.16.92.52): icmp_seq=1 ttl=60 time=21.7 ms
1008 bytes from 104.16.92.52 (104.16.92.52): icmp_seq=2 ttl=60 time=616 ms
1008 bytes from 104.16.92.52 (104.16.92.52): icmp_seq=3 ttl=60 time=56.4 ms
1008 bytes from 104.16.92.52 (104.16.92.52): icmp_seq=4 ttl=60 time=69.8 ms
1008 bytes from 104.16.92.52 (104.16.92.52): icmp_seq=5 ttl=60 time=11.6 ms
1008 bytes from 104.16.92.52 (104.16.92.52): icmp_seq=6 ttl=60 time=371 ms
1008 bytes from 104.16.92.52 (104.16.92.52): icmp_seq=7 ttl=60 time=74.8 ms
1008 bytes from 104.16.92.52 (104.16.92.52): icmp_seq=8 ttl=60 time=960 ms
1008 bytes from 104.16.92.52 (104.16.92.52): icmp_seq=9 ttl=60 time=86.8 ms
1008 bytes from 104.16.92.52 (104.16.92.52): icmp_seq=10 ttl=60 time=9.24 ms

--- udemy.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9009ms
rtt min/avg/max/mdev = 9.240/227.692/959.570/306.766 ms
```

Pinging with different packet sizes:

Host: google.com

64 bytes:

```
PING google.com (142.250.67.142) 64(92) bytes of data.
72 bytes from bom12s06-in-f14.1e100.net (142.250.67.142): icmp_seq=1 ttl=118 time=23.6 ms
72 bytes from bom12s06-in-f14.1e100.net (142.250.67.142): icmp_seq=2 ttl=118 time=28.1 ms
72 bytes from bom12s06-in-f14.1e100.net (142.250.67.142): icmp_seq=3 ttl=118 time=891 ms
72 bytes from bom12s06-in-f14.1e100.net (142.250.67.142): icmp_seq=4 ttl=118 time=75.2 ms
72 bytes from bom12s06-in-f14.1e100.net (142.250.67.142): icmp_seq=6 ttl=118 time=309 ms
72 bytes from bom12s06-in-f14.1e100.net (142.250.67.142): icmp_seq=7 ttl=118 time=40.7 ms
72 bytes from bom12s06-in-f14.1e100.net (142.250.67.142): icmp_seq=8 ttl=118 time=20.8 ms
72 bytes from bom12s06-in-f14.1e100.net (142.250.67.142): icmp_seq=9 ttl=118 time=24.1 ms

--- google.com ping statistics ---
10 packets transmitted, 8 received, 20% packet loss, time 9010ms
rtt min/avg/max/mdev = 20.794/176.532/890.640/284.858 ms
PING google.com (142.250.67.142) 100(128) bytes of data.
```

100 bytes:

```
Pinging google.com [142.250.67.142] with 100 bytes of data:
Reply from 142.250.67.142: bytes=68 (sent 100) time=5ms TTL=119
Reply from 142.250.67.142: bytes=68 (sent 100) time=5ms TTL=119
Reply from 142.250.67.142: bytes=68 (sent 100) time=7ms TTL=119
Reply from 142.250.67.142: bytes=68 (sent 100) time=6ms TTL=119
Reply from 142.250.67.142: bytes=68 (sent 100) time=5ms TTL=119
Reply from 142.250.67.142: bytes=68 (sent 100) time=5ms TTL=119
Reply from 142.250.67.142: bytes=68 (sent 100) time=5ms TTL=119
Reply from 142.250.67.142: bytes=68 (sent 100) time=8ms TTL=119
Reply from 142.250.67.142: bytes=68 (sent 100) time=5ms TTL=119
Reply from 142.250.67.142: bytes=68 (sent 100) time=7ms TTL=119

Ping statistics for 142.250.67.142:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 8ms, Average = 5ms
```

500 bytes:

```
Pinging google.com [142.250.67.142] with 500 bytes of data:
Reply from 142.250.67.142: bytes=68 (sent 500) time=5ms TTL=119
Reply from 142.250.67.142: bytes=68 (sent 500) time=5ms TTL=119
Reply from 142.250.67.142: bytes=68 (sent 500) time=4ms TTL=119
Reply from 142.250.67.142: bytes=68 (sent 500) time=5ms TTL=119
Reply from 142.250.67.142: bytes=68 (sent 500) time=5ms TTL=119
Reply from 142.250.67.142: bytes=68 (sent 500) time=5ms TTL=119
Reply from 142.250.67.142: bytes=68 (sent 500) time=4ms TTL=119
Reply from 142.250.67.142: bytes=68 (sent 500) time=5ms TTL=119
Reply from 142.250.67.142: bytes=68 (sent 500) time=9ms TTL=119
Reply from 142.250.67.142: bytes=68 (sent 500) time=15ms TTL=119

Ping statistics for 142.250.67.142:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 15ms, Average = 6ms
```

1000 bytes:

```
Pinging google.com [142.250.67.142] with 1000 bytes of data:
Reply from 142.250.67.142: bytes=68 (sent 1000) time=8ms TTL=119
Reply from 142.250.67.142: bytes=68 (sent 1000) time=6ms TTL=119
Reply from 142.250.67.142: bytes=68 (sent 1000) time=5ms TTL=119
Reply from 142.250.67.142: bytes=68 (sent 1000) time=8ms TTL=119
Reply from 142.250.67.142: bytes=68 (sent 1000) time=6ms TTL=119
Reply from 142.250.67.142: bytes=68 (sent 1000) time=4ms TTL=119
Reply from 142.250.67.142: bytes=68 (sent 1000) time=6ms TTL=119
Reply from 142.250.67.142: bytes=68 (sent 1000) time=6ms TTL=119
Reply from 142.250.67.142: bytes=68 (sent 1000) time=5ms TTL=119
Reply from 142.250.67.142: bytes=68 (sent 1000) time=6ms TTL=119

Ping statistics for 142.250.67.142:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 8ms, Average = 6ms
```

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?

Yes, the RTT varies between different hosts. This is because the round-trip time is influenced by many factors like distance, transmission medium, number of network hops, traffic levels, and server response time.

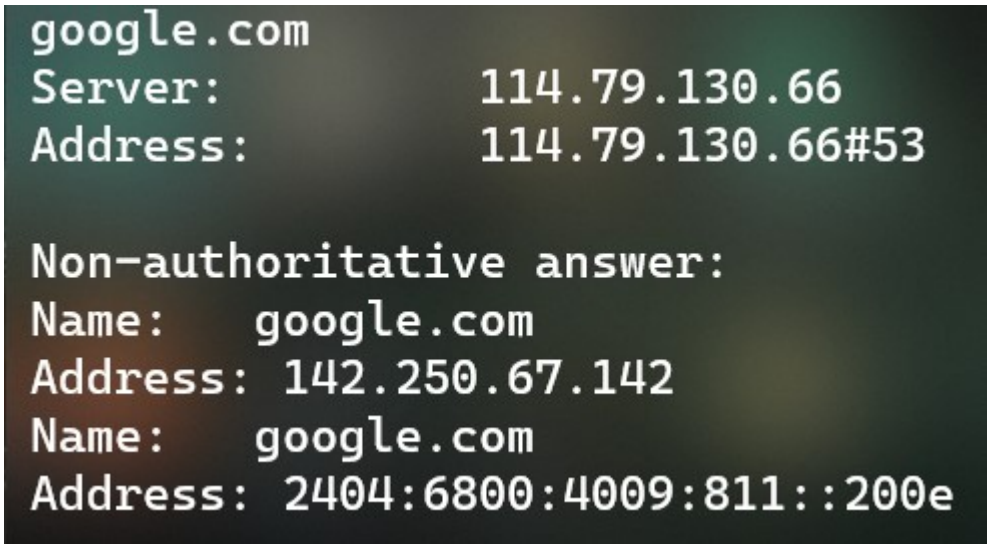
2. Does the average RTT vary with different packet sizes? What aspects of latency (transmit, propagation, and queueing delay) might impact this and why?

   Yes, the RTT varies with different packet sizes. The latency increases when we increase packet size. This is because every router and switch along the path must receive the entire packet before it can forward it. Hence, latency is introduced at every step and accumulates to cause delay.

   Observation:
   The average RTT varies between different hosts for the same packet size as it is influenced by distance, server response time, etc. which depend on the hosts, while it varies with packet size because the router must receive the entire packet before forwarding it.

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).

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!!!.)

```
Windows IP Configuration


Unknown adapter NordLynx:

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

Ethernet adapter Ethernet 2:

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

Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Local Area Connection* 2:

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

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : domain.name
   Link-local IPv6 Address . . . . . : fe80::d915:e93a:ad09:9e34%4
   IPv4 Address. . . . . . . . . . . : 192.168.2.6
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::217:7cff:fe70:4036%4
                                       192.168.2.1
```

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.)

Active Connections

Proto	Local Address	Foreign Address	State	Offload State
TCP	127.0.0.1:49670	127.0.0.1:49671	ESTABLISHED	InHost
TCP	127.0.0.1:49671	127.0.0.1:49670	ESTABLISHED	InHost
TCP	127.0.0.1:49679	127.0.0.1:49852	ESTABLISHED	InHost
TCP	127.0.0.1:49679	127.0.0.1:49895	ESTABLISHED	InHost
TCP	127.0.0.1:49680	127.0.0.1:49681	ESTABLISHED	InHost
TCP	127.0.0.1:49681	127.0.0.1:49680	ESTABLISHED	InHost
TCP	127.0.0.1:49693	127.0.0.1:49957	ESTABLISHED	InHost
TCP	127.0.0.1:49699	127.0.0.1:49720	ESTABLISHED	InHost
TCP	127.0.0.1:49699	127.0.0.1:49729	ESTABLISHED	InHost
TCP	127.0.0.1:49699	127.0.0.1:49731	ESTABLISHED	InHost
TCP	127.0.0.1:49699	127.0.0.1:49732	ESTABLISHED	InHost
TCP	127.0.0.1:49699	127.0.0.1:49733	ESTABLISHED	InHost
TCP	127.0.0.1:49699	127.0.0.1:49738	ESTABLISHED	InHost
TCP	127.0.0.1:49699	127.0.0.1:49747	ESTABLISHED	InHost
TCP	127.0.0.1:49699	127.0.0.1:49809	ESTABLISHED	InHost
TCP	127.0.0.1:49706	127.0.0.1:49707	ESTABLISHED	InHost
TCP	127.0.0.1:49707	127.0.0.1:49706	ESTABLISHED	InHost
TCP	127.0.0.1:49708	127.0.0.1:61900	ESTABLISHED	InHost
TCP	127.0.0.1:49709	127.0.0.1:49710	ESTABLISHED	InHost
TCP	127.0.0.1:49710	127.0.0.1:49709	ESTABLISHED	InHost
TCP	127.0.0.1:49711	127.0.0.1:49712	ESTABLISHED	InHost
TCP	127.0.0.1:49712	127.0.0.1:49711	ESTABLISHED	InHost
TCP	127.0.0.1:49713	127.0.0.1:61900	ESTABLISHED	InHost
TCP	127.0.0.1:49714	127.0.0.1:49715	ESTABLISHED	InHost
TCP	127.0.0.1:49715	127.0.0.1:49714	ESTABLISHED	InHost
TCP	127.0.0.1:49720	127.0.0.1:49699	ESTABLISHED	InHost
TCP	127.0.0.1:49721	127.0.0.1:49722	ESTABLISHED	InHost
TCP	127.0.0.1:49722	127.0.0.1:49721	ESTABLISHED	InHost
TCP	127.0.0.1:49723	127.0.0.1:61900	ESTABLISHED	InHost
TCP	127.0.0.1:49724	127.0.0.1:49725	ESTABLISHED	InHost
TCP	127.0.0.1:49725	127.0.0.1:49724	ESTABLISHED	InHost
TCP	127.0.0.1:49729	127.0.0.1:49699	ESTABLISHED	InHost

(This is just a preview. Actual log longer than shown in picture and can be found on the drive link attached at the end of the document)

telnet — Telnet is an old program for remote login. It's not used so much for that anymore, 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 is 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

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

  1     1 ms     1 ms     1 ms  192.168.2.1
  2    38 ms     5 ms     5 ms  1.186.179.1.dvois.com [1.186.179.1]
  3     5 ms     3 ms     3 ms  114.79.129.97.dvois.com [114.79.129.97]
  4     *        *        *     Request timed out.
  5     *        *        *     Request timed out.
  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.

Trace complete.
```

2. mscs.mu.edu

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

  1     2 ms     2 ms     2 ms  192.168.2.1
  2     6 ms     3 ms     3 ms  1.186.179.1.dvois.com [1.186.179.1]
  3     8 ms     3 ms     3 ms  114.79.129.97.dvois.com [114.79.129.97]
  4     *        *        *     Request timed out.
  5     *        *        *     Request timed out.
  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     *        *
```

```
Tracing route to mscs.mu.edu [134.48.4.5]
over a maximum of 10 hops:

  1     1 ms     1 ms     1 ms  192.168.2.1
  2     4 ms     3 ms     4 ms  1.186.179.1.dvois.com [1.186.179.1]
  3     3 ms     4 ms    20 ms  114.79.129.97.dvois.com [114.79.129.97]
  4     *        *        *     Request timed out.
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.

Trace complete.
```

3. www.cs.grinnell.edu

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

  1     1 ms     1 ms     1 ms  192.168.2.1
  2     *        7 ms     *     1.186.179.1.dvois.com [1.186.179.1]
  3     4 ms     3 ms     3 ms  114.79.129.97.dvois.com [114.79.129.97]
  4     *        *        *     Request timed out.
  5     *        *        *     Request timed out.
  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.

Trace complete.
```

4. csail.mit.edu

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

  1     1 ms     1 ms     1 ms  192.168.2.1
  2     3 ms     3 ms     3 ms  1.186.179.1.dvois.com [1.186.179.1]
  3     4 ms     3 ms     3 ms  114.79.129.97.dvois.com [114.79.129.97]
  4     *        *        *     Request timed out.
  5     *        *        *     Request timed out.
  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.

Trace complete.
```

5. cs.stanford.edu

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

  1     1 ms     1 ms     2 ms  192.168.2.1
  2    21 ms     7 ms    13 ms  1.186.179.1.dvois.com [1.186.179.1]
  3     4 ms     3 ms     3 ms  114.79.129.97.dvois.com [114.79.129.97]
  4     5 ms     6 ms     5 ms  1.7.160.224
  5     *        *        *     Request timed out.
  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.

Trace complete.
```

6. cs.manchester.ac.uk

```
Tracing route to cs.manchester.ac.uk [130.88.101.49]
over a maximum of 10 hops:

  1     1 ms     1 ms     1 ms  192.168.2.1
  2     3 ms     *        7 ms  1.186.179.1.dvois.com [1.186.179.1]
  3     3 ms     3 ms     4 ms  114.79.129.97.dvois.com [114.79.129.97]
  4     5 ms     5 ms     5 ms  1.7.160.224
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.

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:\Harsh\Sem 5\DCCN>tracert -h 10 math.hws.edu

Tracing route to math.hws.edu [64.89.144.237]
over a maximum of 10 hops:

  1     2 ms     1 ms     1 ms  192.168.2.1
  2     3 ms     3 ms     4 ms  1.186.179.1.dvois.com [1.186.179.1
]
  3     3 ms     3 ms     3 ms  114.79.129.97.dvois.com [114.79.12
9.97]
  4     *        *        *     Request timed out.
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.

Trace complete.
```

```
C:\Harsh\Sem 5\DCCN>tracert -h 10 www.hws.edu

Tracing route to www.hws.edu [64.89.145.159]
over a maximum of 10 hops:

  1     1 ms     1 ms     1 ms  192.168.2.1
  2     4 ms     7 ms     *     1.186.179.1.dvois.com [1.186.179.
1]
  3     4 ms     3 ms     4 ms  114.79.129.97.dvois.com [114.79.1
29.97]
  4     *        *        *     Request timed out.
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.

Trace complete.
```

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 mit.edu 1 week apart:

Week 1:

```
Tracing route to mit.edu [104.120.75.121]
over a maximum of 30 hops:

  1     3 ms     2 ms     3 ms  192.168.2.1
  2     6 ms     7 ms     9 ms  1.186.179.1.dvois.com [1.186.179.1]
  3     6 ms     4 ms     4 ms  114.79.129.97.dvois.com [114.79.129.97]
  4     9 ms     7 ms     6 ms  1.7.160.224
  5     8 ms     6 ms     6 ms  100.66.8.21
  6     8 ms     6 ms     5 ms  100.66.8.21
  7   178 ms     7 ms     6 ms  as20940.bom.extreme-ix.net [103.77.108.134]
  8     9 ms     5 ms     6 ms  a104-120-75-121.deploy.static.akamaitechnologies.com [104.120.75.121]

Trace complete.
```

Week 2:

```
Tracing route to mit.edu [104.120.75.121]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  192.168.2.1
  2    37 ms     4 ms     *     1.186.179.1.dvois.com [1.186.179.1]
  3     3 ms     4 ms     3 ms  114.79.129.97.dvois.com [114.79.129.97]
  4     *        *        *     Request timed out.
  5     5 ms     6 ms     6 ms  a104-120-75-121.deploy.static.akamaitechnologies.com [104.120.75.121]

Trace complete.
```

Observation:
Tracing routes from the same source to the same destination may follow different paths. As we can see, the first time, the route was traced across 8 nodes to reach the destinatipn, while the second time, it tok only 5 nodes to trace the routes. This shows that the routes don't always follow the same path when transferring packets from the same source to the same destination.

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?

   No, all have different paths. However, the first hop (home address) and the last hop (server address) remain the same.

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, there is a direct relation between the number of nodes that show up in the traceroute and the location of the host. This is because the farther the host is geographically, the more are the hops required to reach the host. This results in a longer trace route.

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?

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*).

```
Domain Name: spit.ac.in
Registry Domain ID: D2241401-IN
Registrar WHOIS Server:
Registrar URL: http://www.ernet.in
Updated Date: 2020-05-18T09:51:15Z
Creation Date: 2006-05-22T04:58:23Z
Registry Expiry Date: 2025-05-22T04:58:23Z
Registrar: ERNET India
Registrar IANA ID: 800068
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: ok http://www.icann.org/epp#OK
Registry Registrant ID:
Registrant Name:
Registrant Organization: Bharatiya Vidya Bhavans Sardar Patel Institute of Technology Mumbai
Registrant Street:
Registrant Street:
Registrant Street:
Registrant City:
Registrant State/Province:
Registrant Postal Code:
Registrant Country: IN
Registrant Phone:
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: Please contact the Registrar listed above
Registry Admin ID:
Admin Name:
Admin Organization:
Admin Street:
Admin Street:
Admin Street:
Admin City:
Admin State/Province:
Admin Postal Code:
Admin Country:
```

(This is just a preview. Actual log longer than shown in picture and can be found on the drive link attached at the end of the document)

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.

```
   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: 2020-08-21T10:26:53Z <<<

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

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

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
```

(This is just a preview. Actual log longer than shown in picture and can be found on the drive link attached at the end of the document)

Observation:
I tried the whois command with two hosts: spit.ac.in and google.com. The whois command shows the details of the particular host, like domain ID, registrar URL, Creation and Expiry dates, etc.

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

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

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

curl ipinfo.io/129.64.99.200

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

```
harshsandesara@DESKTOP-QMGI8AK:/mnt/c/Harsh/Sem 5/DCCN$ curl ipin
fo.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"
```

```
}harshsandesara@DESKTOP-QMGI8AK:/mnt/c/Harsh/Sem 5/DCCN$ curl ipi
nfo.io/1.1.1.1
{
  "ip": "1.1.1.1",
  "hostname": "one.one.one.one",
  "city": "New York City",
  "region": "New York",
  "country": "US",
  "loc": "40.7143,-74.0060",
  "org": "AS13335 Cloudflare, Inc.",
  "postal": "10004",
  "timezone": "America/New_York",
  "readme": "https://ipinfo.io/missingauth"
}harshsandesara@DESKTOP-QMGI8AK:/mnt/c/Harsh/Sem 5/DCCN$
```

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 have learned about the various commands in Linux and Windows like ping, traceroute, ipconfig, etc. and implemented these Networking Utilities on the terminal.
- Transferring packets is affected by a lot of factors like distance, server response time, number of hops (nodes), etc.
- The user address is the same every time.

Link to all log files:
https://drive.google.com/drive/folders/1KNyZGaXWsy2n8pAHtzDh9vL4MT0QTJ7e?usp=sharing