Name: Gaurav Patil
Batch: C
UID: 2018130038

Experiment-2

Aim: To study the 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

```
C:\Users\Gaurav\Desktop
λ ping -n 10 -l 100 www.amazon.com

Pinging d3ag4hukkh62yn.cloudfront.net [13.227.226.21] with 100 bytes of data:
Reply from 13.227.226.21: bytes=100 time=3ms TTL=243
Reply from 13.227.226.21: bytes=100 time=2ms TTL=243
Reply from 13.227.226.21: bytes=100 time=2ms TTL=243
Reply from 13.227.226.21: bytes=100 time=3ms TTL=243
Reply from 13.227.226.21: bytes=100 time=2ms TTL=243
Reply from 13.227.226.21: bytes=100 time=3ms TTL=243
Reply from 13.227.226.21: bytes=100 time=2ms TTL=243
Reply from 13.227.226.21: bytes=100 time=2ms TTL=243
Reply from 13.227.226.21: bytes=100 time=2ms TTL=243
Reply from 13.227.226.21: bytes=100 time=2ms TTL=243

Ping statistics for 13.227.226.21:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms

C:\Users\Gaurav\Desktop
λ ping -n 10 -l 64 www.amazon.com

Pinging d3ag4hukkh62yn.cloudfront.net [13.227.226.21] with 64 bytes of data:
Reply from 13.227.226.21: bytes=64 time=4ms TTL=243
Reply from 13.227.226.21: bytes=64 time=2ms TTL=243
Reply from 13.227.226.21: bytes=64 time=2ms TTL=243
Reply from 13.227.226.21: bytes=64 time=2ms TTL=243
Reply from 13.227.226.21: bytes=64 time=2ms TTL=243
Reply from 13.227.226.21: bytes=64 time=3ms TTL=243
Reply from 13.227.226.21: bytes=64 time=2ms TTL=243
Reply from 13.227.226.21: bytes=64 time=3ms TTL=243
Reply from 13.227.226.21: bytes=64 time=2ms TTL=243
Reply from 13.227.226.21: bytes=64 time=2ms TTL=243

Ping statistics for 13.227.226.21:
```

```
λ ping -n 10 -l 500 www.amazon.com

Pinging e15316.e22.akamaiedge.net [104.90.201.153] with 500 bytes of data:
Reply from 104.90.201.153: bytes=500 time=6ms TTL=59
Reply from 104.90.201.153: bytes=500 time=3ms TTL=59
Reply from 104.90.201.153: bytes=500 time=2ms TTL=59
Reply from 104.90.201.153: bytes=500 time=3ms TTL=59
Reply from 104.90.201.153: bytes=500 time=3ms TTL=59
Reply from 104.90.201.153: bytes=500 time=15ms TTL=59
Reply from 104.90.201.153: bytes=500 time=6ms TTL=59
Reply from 104.90.201.153: bytes=500 time=2ms TTL=59
Reply from 104.90.201.153: bytes=500 time=2ms TTL=59
Reply from 104.90.201.153: bytes=500 time=3ms TTL=59

Ping statistics for 104.90.201.153:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 15ms, Average = 4ms

C:\Users\Gaurav\Desktop
λ ping -n 10 -l 1000 www.google.com

Pinging www.google.com [216.58.203.132] with 1000 bytes of data:
Reply from 216.58.203.132: bytes=68 (sent 1000) time=2ms TTL=118
Reply from 216.58.203.132: bytes=68 (sent 1000) time=3ms TTL=118
Reply from 216.58.203.132: bytes=68 (sent 1000) time=2ms TTL=118
Reply from 216.58.203.132: bytes=68 (sent 1000) time=3ms TTL=118
Reply from 216.58.203.132: bytes=68 (sent 1000) time=2ms TTL=118
Reply from 216.58.203.132: bytes=68 (sent 1000) time=2ms TTL=118
Reply from 216.58.203.132: bytes=68 (sent 1000) time=2ms TTL=118
Reply from 216.58.203.132: bytes=68 (sent 1000) time=3ms TTL=118
Reply from 216.58.203.132: bytes=68 (sent 1000) time=2ms TTL=118
Reply from 216.58.203.132: bytes=68 (sent 1000) time=3ms TTL=118

Ping statistics for 216.58.203.132:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms

C:\Users\Gaurav\Desktop
λ ping -n 10 -l 1400 www.google.com

Pinging www.google.com [216.58.203.132] with 1400 bytes of data:
Reply from 216.58.203.132: bytes=68 (sent 1400) time=3ms TTL=118
Reply from 216.58.203.132: bytes=68 (sent 1400) time=3ms TTL=118
Reply from 216.58.203.132: bytes=68 (sent 1400) time=2ms TTL=118
Reply from 216.58.203.132: bytes=68 (sent 1400) time=3ms TTL=118
Reply from 216.58.203.132: bytes=68 (sent 1400) time=2ms TTL=118
Reply from 216.58.203.132: bytes=68 (sent 1400) time=3ms TTL=118
Reply from 216.58.203.132: bytes=68 (sent 1400) time=2ms TTL=118
Reply from 216.58.203.132: bytes=68 (sent 1400) time=3ms TTL=118
Reply from 216.58.203.132: bytes=68 (sent 1400) time=3ms TTL=118
Reply from 216.58.203.132: bytes=68 (sent 1400) time=2ms TTL=118

Ping statistics for 216.58.203.132:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms
```

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?**

   Answer:
   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.
   Thus the different average RTT values of amazon.com and google.com can be because of the above mentioned factors.

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

   Answer:

   Yes, the average RTT increases with packet size as queuing, transmission delay increases as they 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).

```
C:\Users\Gaurav\Desktop
λ ping www.uw.edu

Pinging www.washington.edu [128.95.155.135] with 32 bytes of data:
Reply from 128.95.155.135: bytes=32 time=260ms TTL=47
Reply from 128.95.155.135: bytes=32 time=260ms TTL=47
Reply from 128.95.155.135: bytes=32 time=260ms TTL=47
Reply from 128.95.155.135: bytes=32 time=260ms TTL=47

Ping statistics for 128.95.155.135:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 260ms, Maximum = 260ms, Average = 260ms

C:\Users\Gaurav\Desktop
λ ping www.cornell.edu

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

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

C:\Users\Gaurav\Desktop
λ ping berkeley.edu

Pinging berkeley.edu [35.163.72.93] with 32 bytes of data:
Reply from 35.163.72.93: bytes=32 time=252ms TTL=33
Reply from 35.163.72.93: bytes=32 time=252ms TTL=33
Reply from 35.163.72.93: bytes=32 time=252ms TTL=33
Reply from 35.163.72.93: bytes=32 time=252ms TTL=33

Ping statistics for 35.163.72.93:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 252ms, Maximum = 252ms, Average = 252ms

C:\Users\Gaurav\Desktop
λ ping www.uchicago.edu

Pinging wsee2.elb.uchicago.edu [3.224.151.213] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 3.224.151.213:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
C:\Users\Gaurav\Desktop
λ ping www.u-tokyo.ac.jp

Pinging www.u-tokyo.ac.jp [210.152.243.234] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 210.152.243.234:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

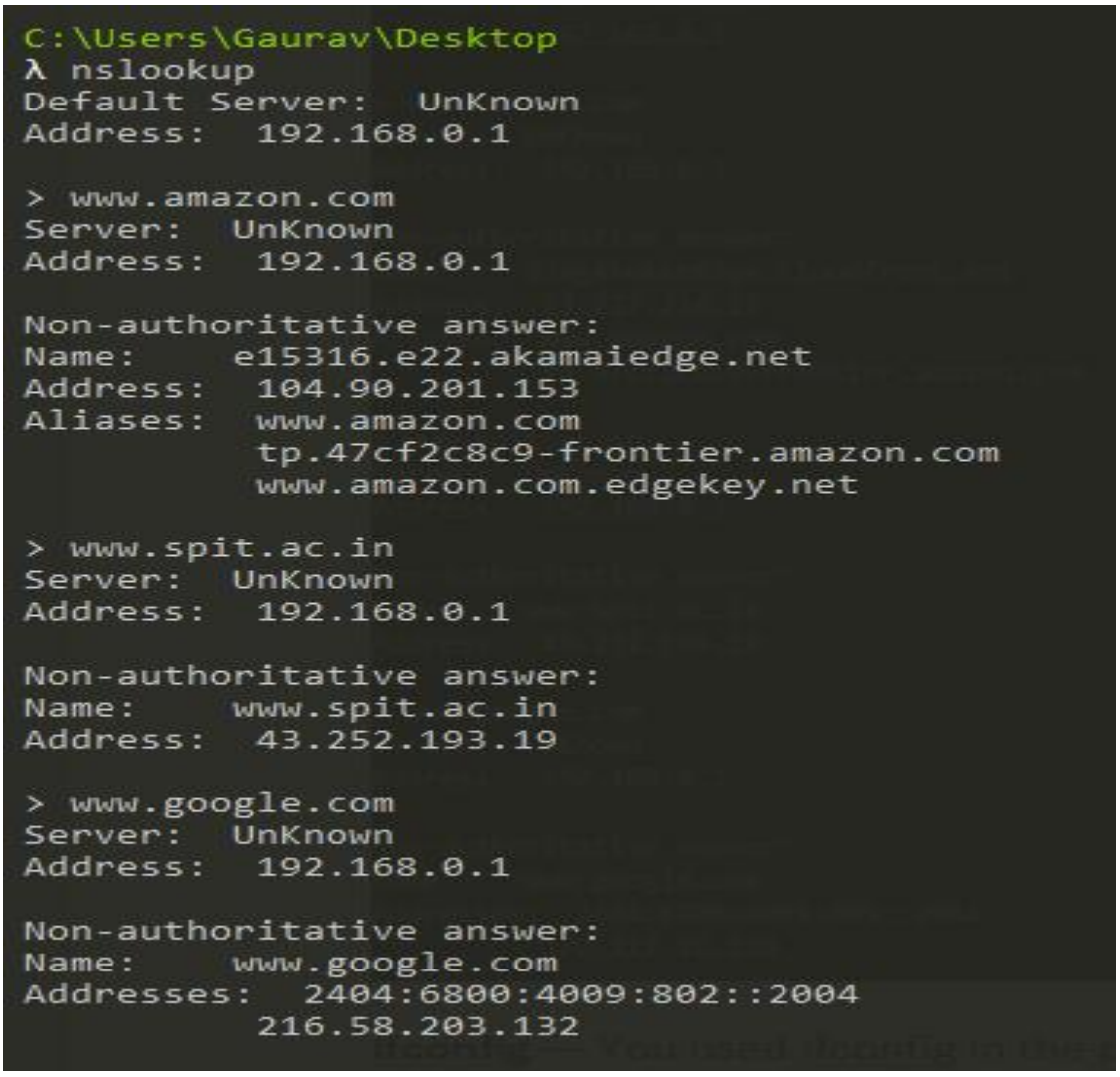
Factors that influences RTT: **Ref - [1]**

There are certain factors that can bring huge changes in the value of RTT. These are enlisted below:

- The nature of the transmission medium - the way in which connections are made affects how fast the connection moves; connections made over optical fiber will behave differently than connections made over copper. Likewise, a connection made over a wireless frequency will behave differently than that of a satellite communication.
- Local area network (LAN) traffic - the amount of traffic on the local area network can bottleneck a connection before it ever reaches the larger Internet. For example, if many users are using streaming video service simultaneously, round-trip time may be inhibited
  even though the external network has excess capacity and is functioning normally.
- Server response time – the amount of time it takes a server to process and respond to a request is a potential bottleneck in network latency. When a server is overwhelmed with
  requests, such as during a DDoS attack, its ability to respond efficiently can be inhibited, resulting in increased RTT.
- Node count and congestion – depending on the path that a connection takes across the Internet, it may be routed or “hop” through a different number of intermediate nodes. Generally speaking, the greater the number of nodes a connection touches the slower it will be. A node may also experience network congestion from other network traffic, which will slow down the connection and increase RTT.
- Physical distance – although a connection optimized by a CDN can often reduce the number of hops required to reach a destination, there is no way of getting around the limitation imposed by the speed of light; the distance between a start and end point is a limiting factor in network connectivity that can only be reduced by moving content closer to the requesting users. To overcome this obstacle, a CDN will cache content closer to the requesting users, thereby reducing RTT.

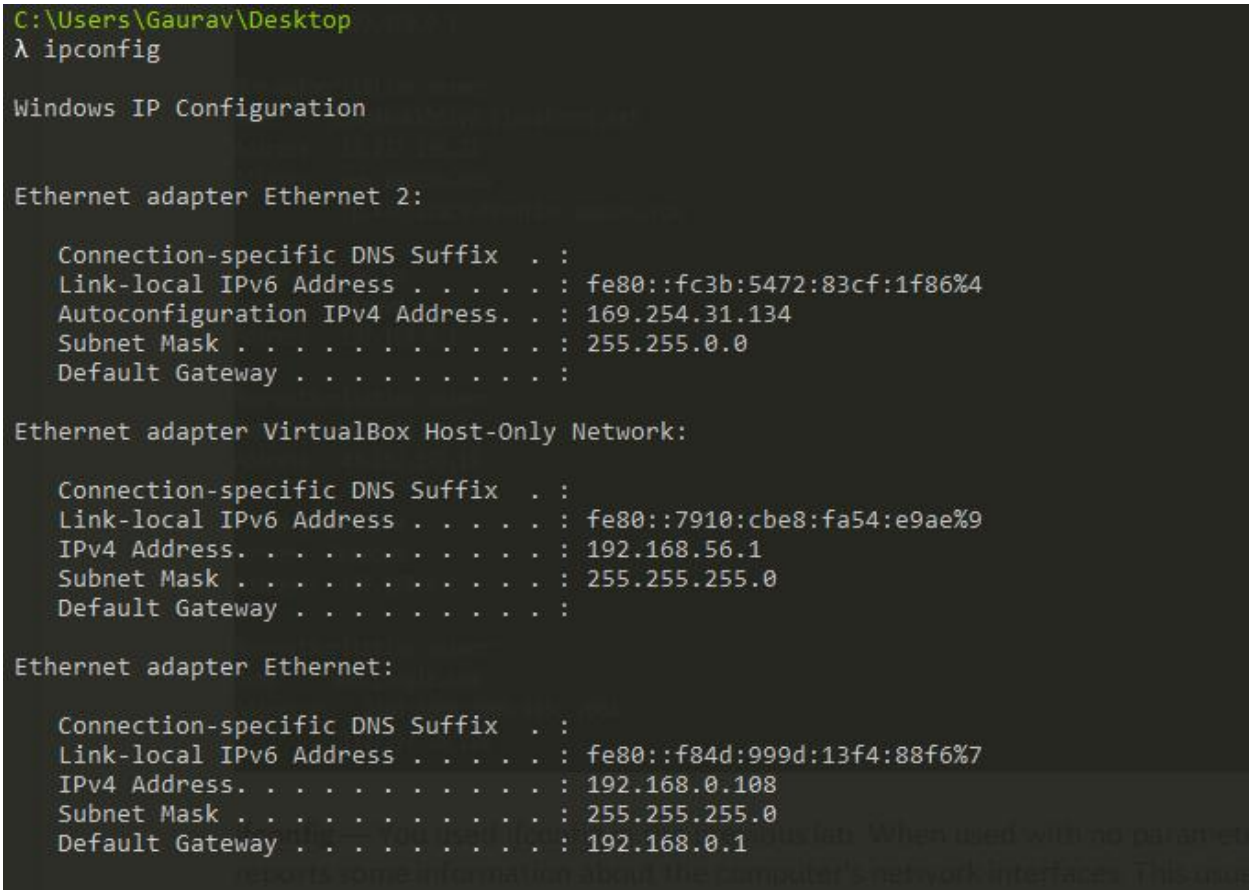
Thus the round trip times varies due to these factors.

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>



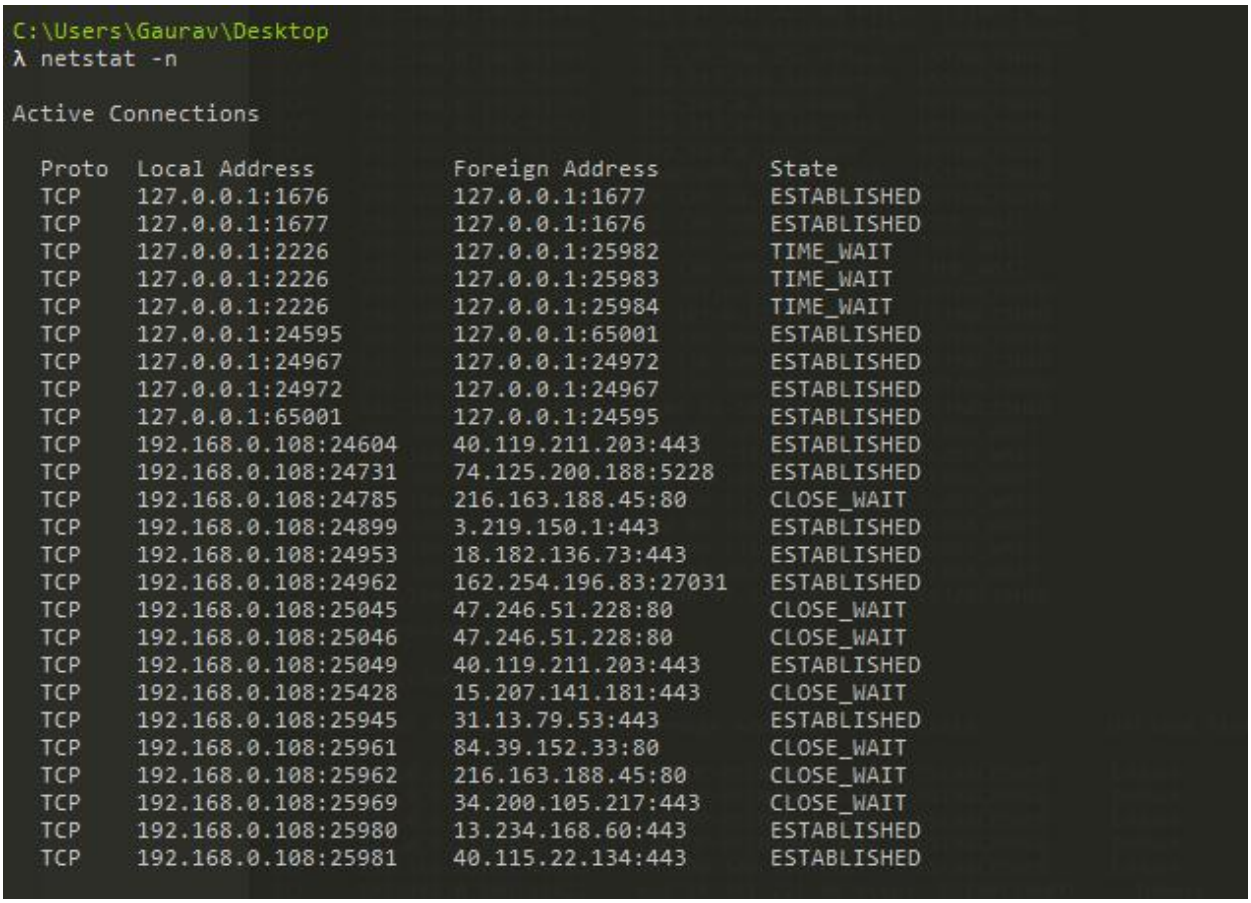
ifconfig — You used ifconfig in the previous lab. When used with no parameters, ifconfig reports some information about the computer's network interfaces. This usually includes lo which stands for localhost; it can be used for communication between programs running on the same computer. Linux often has 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!!!.)



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.). **Ref - [2]**

```
C:\Users\Gaurav\Desktop
λ netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:1676         DESKTOP-UIV0JV3:1677   ESTABLISHED
  TCP    127.0.0.1:1677         DESKTOP-UIV0JV3:1676   ESTABLISHED
  TCP    127.0.0.1:24595        DESKTOP-UIV0JV3:65001  ESTABLISHED
  TCP    127.0.0.1:24967        DESKTOP-UIV0JV3:24972  ESTABLISHED
  TCP    127.0.0.1:24972        DESKTOP-UIV0JV3:24967  ESTABLISHED
  TCP    127.0.0.1:65001        DESKTOP-UIV0JV3:24595  ESTABLISHED
  TCP    192.168.0.108:24604    40.119.211.203:https   ESTABLISHED
  TCP    192.168.0.108:24731    sa-in-f188:5228        ESTABLISHED
  TCP    192.168.0.108:24785    c9resolver:http        CLOSE_WAIT
  TCP    192.168.0.108:24899    ec2-3-219-150-1:https  ESTABLISHED
  TCP    192.168.0.108:24953    ec2-18-182-136-73:https  ESTABLISHED
  TCP    192.168.0.108:24962    162.254.196.83:27031   ESTABLISHED
  TCP    192.168.0.108:25045    47.246.51.228:http     CLOSE_WAIT
  TCP    192.168.0.108:25046    47.246.51.228:http     CLOSE_WAIT
  TCP    192.168.0.108:25049    40.119.211.203:https   ESTABLISHED
  TCP    192.168.0.108:25428    ec2-15-207-141-181:https  CLOSE_WAIT
  TCP    192.168.0.108:25945    whatsapp-cdn-shv-02-bom1:https  ESTABLISHED
  TCP    192.168.0.108:25961    84.39.152.33:http      CLOSE_WAIT
  TCP    192.168.0.108:25962    c9resolver:http        CLOSE_WAIT
  TCP    192.168.0.108:25968    bom07s25-in-f14:https  TIME_WAIT
  TCP    192.168.0.108:25969    ec2-34-200-105-217:https  CLOSE_WAIT
  TCP    192.168.0.108:25980    ec2-13-234-168-60:https  ESTABLISHED
  TCP    192.168.0.108:25981    40.115.22.134:https    ESTABLISHED

C:\Users\Gaurav\Desktop
λ netstat -t

Active Connections

  Proto  Local Address          Foreign Address        State           Offload State

  TCP    127.0.0.1:1676         DESKTOP-UIV0JV3:1677   ESTABLISHED     InHost
  TCP    127.0.0.1:1677         DESKTOP-UIV0JV3:1676   ESTABLISHED     InHost
  TCP    127.0.0.1:2226         DESKTOP-UIV0JV3:25982  TIME_WAIT       InHost
  TCP    127.0.0.1:2226         DESKTOP-UIV0JV3:25983  TIME_WAIT       InHost
  TCP    127.0.0.1:24595        DESKTOP-UIV0JV3:65001  ESTABLISHED     InHost
  TCP    127.0.0.1:24967        DESKTOP-UIV0JV3:24972  ESTABLISHED     InHost
  TCP    127.0.0.1:24972        DESKTOP-UIV0JV3:24967  ESTABLISHED     InHost
  TCP    127.0.0.1:65001        DESKTOP-UIV0JV3:24595  ESTABLISHED     InHost
  TCP    192.168.0.108:24604    40.119.211.203:https   ESTABLISHED     InHost
  TCP    192.168.0.108:24731    sa-in-f188:5228        ESTABLISHED     InHost
  TCP    192.168.0.108:24785    c9resolver:http        CLOSE_WAIT      InHost
  TCP    192.168.0.108:24899    ec2-3-219-150-1:https  ESTABLISHED     InHost
  TCP    192.168.0.108:24953    ec2-18-182-136-73:https  ESTABLISHED     InHost
  TCP    192.168.0.108:24962    162.254.196.83:27031   ESTABLISHED     InHost
  TCP    192.168.0.108:25045    47.246.51.228:http     CLOSE_WAIT      InHost
  TCP    192.168.0.108:25046    47.246.51.228:http     CLOSE_WAIT      InHost
  TCP    192.168.0.108:25049    40.119.211.203:https   ESTABLISHED     InHost
  TCP    192.168.0.108:25428    ec2-15-207-141-181:https  CLOSE_WAIT      InHost
  TCP    192.168.0.108:25945    whatsapp-cdn-shv-02-bom1:https  ESTABLISHED     InHost
  TCP    192.168.0.108:25961    84.39.152.33:http      CLOSE_WAIT      InHost
  TCP    192.168.0.108:25962    c9resolver:http        CLOSE_WAIT      InHost
  TCP    192.168.0.108:25969    ec2-34-200-105-217:https  CLOSE_WAIT      InHost
  TCP    192.168.0.108:25980    ec2-13-234-168-60:https  ESTABLISHED     InHost
  TCP    192.168.0.108:25981    40.115.22.134:https    ESTABLISHED     InHost
```



```
C:\Users\Gaurav\Desktop
λ netstat -n

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:1676         127.0.0.1:1677         ESTABLISHED
  TCP    127.0.0.1:1677         127.0.0.1:1676         ESTABLISHED
  TCP    127.0.0.1:2226         127.0.0.1:25982        TIME_WAIT
  TCP    127.0.0.1:2226         127.0.0.1:25983        TIME_WAIT
  TCP    127.0.0.1:2226         127.0.0.1:25984        TIME_WAIT
  TCP    127.0.0.1:24595        127.0.0.1:65001        ESTABLISHED
  TCP    127.0.0.1:24967        127.0.0.1:24972        ESTABLISHED
  TCP    127.0.0.1:24972        127.0.0.1:24967        ESTABLISHED
  TCP    127.0.0.1:65001        127.0.0.1:24595        ESTABLISHED
  TCP    192.168.0.108:24604    40.119.211.203:443     ESTABLISHED
  TCP    192.168.0.108:24731    74.125.200.188:5228    ESTABLISHED
  TCP    192.168.0.108:24785    216.163.188.45:80      CLOSE_WAIT
  TCP    192.168.0.108:24899    3.219.150.1:443        ESTABLISHED
  TCP    192.168.0.108:24953    18.182.136.73:443      ESTABLISHED
  TCP    192.168.0.108:24962    162.254.196.83:27031   ESTABLISHED
  TCP    192.168.0.108:25045    47.246.51.228:80       CLOSE_WAIT
  TCP    192.168.0.108:25046    47.246.51.228:80       CLOSE_WAIT
  TCP    192.168.0.108:25049    40.119.211.203:443     ESTABLISHED
  TCP    192.168.0.108:25428    15.207.141.181:443     CLOSE_WAIT
  TCP    192.168.0.108:25945    31.13.79.53:443        ESTABLISHED
  TCP    192.168.0.108:25961    84.39.152.33:80        CLOSE_WAIT
  TCP    192.168.0.108:25962    216.163.188.45:80      CLOSE_WAIT
  TCP    192.168.0.108:25969    34.200.105.217:443     CLOSE_WAIT
  TCP    192.168.0.108:25980    13.234.168.60:443      ESTABLISHED
  TCP    192.168.0.108:25981    40.115.22.134:443      ESTABLISHED
```

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).

Ref - [3]

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).

```
C:\Users\Gaurav\Desktop
λ tracert mscs.mu.edu

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

  1    <1 ms    <1 ms    <1 ms  192.168.0.1
  2    <1 ms    <1 ms     1 ms  103.76.56.132
  3     1 ms     1 ms     1 ms  103.76.56.129
  4     *        *        *     Request timed out.
  5     4 ms     4 ms     4 ms  nsg-static-173.107.75.182-airtel.com [182.75.107.173]
  6   198 ms   197 ms   199 ms  182.79.222.233
  7   187 ms   187 ms   187 ms  core1.nyc4.he.net [198.32.118.57]
  8   211 ms   212 ms   212 ms  100ge9-1.core2.chi1.he.net [184.105.223.161]
  9     *        *        *     Request timed out.
 10   245 ms   245 ms   245 ms  r-222wwash-isp-ae6-3926.wiscnet.net [140.189.8.126]
 11   247 ms   247 ms   247 ms  r-milwaukeeci-809-isp-ae3-0.wiscnet.net [140.189.8.230]
 12   246 ms   245 ms   246 ms  MarquetteUniv.site.wiscnet.net [216.56.1.202]
 13   252 ms   251 ms   251 ms  134.48.10.26
 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.
```

```
C:\Users\Gaurav\Desktop
λ tracert www.iitb.ac.in

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

  1    <1 ms    <1 ms    <1 ms  192.168.0.1
  2    <1 ms    <1 ms     1 ms  103.76.56.132
  3     2 ms     1 ms     1 ms  103.76.56.129
  4     1 ms     1 ms     2 ms  103.249.251.213
  5     4 ms     3 ms     3 ms  nsg-static-173.107.75.182-airtel.com [182.75.107.173]
  6     5 ms     4 ms     5 ms  182.79.146.180
  7     6 ms     4 ms     5 ms  115.110.234.141.static.Mumbai.vsnl.net.in [115.110.234.141]
  8     5 ms     5 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.
```

```
C:\Users\Gaurav\Desktop
λ tracert 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  192.168.0.1
  2     1 ms    <1 ms     1 ms  103.76.56.132
  3     1 ms     2 ms     1 ms  103.76.56.129
  4     *       12 ms     2 ms  103.249.251.213
  5     4 ms     4 ms     3 ms  nsg-static-173.107.75.182-airtel.com [182.75.107.173]
  6   190 ms   189 ms   189 ms  182.79.222.237
  7   190 ms   235 ms   191 ms  core1.nyc4.he.net [198.32.118.57]
  8   232 ms   232 ms   233 ms  100ge2-1.core2.chi1.he.net [184.104.193.173]
  9   213 ms   213 ms   214 ms  100ge14-2.core1.msp1.he.net [184.105.223.178]
 10   230 ms   229 ms   230 ms  216.66.77.218
 11   248 ms   248 ms   249 ms  peer-as5056.br02.msp1.tfbnw.net [157.240.76.37]
 12   259 ms   260 ms   259 ms  167.142.58.40
 13   258 ms   259 ms   259 ms  67.224.64.62
 14   262 ms   261 ms   261 ms  grinnellcollege1.desm.netins.net [167.142.65.43]
 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:\Users\Gaurav\Desktop
λ tracert 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  192.168.0.1
  2     1 ms     1 ms    <1 ms  103.76.56.132
  3     2 ms     1 ms     1 ms  103.76.56.129
  4     1 ms     1 ms     1 ms  103.249.251.213
  5     4 ms     4 ms     4 ms  nsg-static-173.107.75.182-airtel.com [182.75.107.173]
  6   235 ms   232 ms   232 ms  182.79.243.31
  7   243 ms   247 ms   243 ms  xe-9-1-0.edge1.LosAngeles6.Level3.net [4.26.0.61]
  8     *        *        *     Request timed out.
  9   299 ms   300 ms   300 ms  MASSACHUSET.bear1.Boston1.Level3.net [4.53.48.98]
 10   292 ms   292 ms   292 ms  dmz-rtr-1-external-rtr-1.mit.edu [18.0.161.17]
 11   301 ms   299 ms   299 ms  dmz-rtr-2-dmz-rtr-1-2.mit.edu [18.0.162.6]
 12   311 ms   305 ms   307 ms  mitnet.core-1-ext.csail.mit.edu [18.4.7.65]
 13     *        *        *     Request timed out.
 14   306 ms   306 ms   305 ms  bdr.core-1.csail.mit.edu [128.30.0.246]
 15   299 ms   299 ms   300 ms  inquir-3ld.csail.mit.edu [128.30.2.109]

Trace complete.
```

```
C:\Users\Gaurav\Desktop
λ tracert cs.stanford.edu

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

  1    <1 ms    <1 ms    <1 ms  192.168.0.1
  2    <1 ms    <1 ms    <1 ms  103.76.56.132
  3     1 ms     1 ms     2 ms  103.76.56.129
  4     2 ms     1 ms     *     103.249.251.213
  5     5 ms     4 ms     4 ms  nsg-static-173.107.75.182-airtel.com [182.75.107.173]
  6   195 ms   195 ms   195 ms  182.79.222.233
  7   185 ms   186 ms   186 ms  core1.nyc4.he.net [198.32.118.57]
  8   247 ms   246 ms   247 ms  100ge8-1.core1.sjc2.he.net [184.105.81.218]
  9   248 ms   248 ms   247 ms  100ge1-1.core1.pao1.he.net [72.52.92.158]
 10   248 ms   255 ms   247 ms  stanford-university.100gigabitethernet5-1.core1.pao1.he.net [184.105.177.238]
 11   245 ms   245 ms   244 ms  csee-west-rtr-vl3.SUNet [171.66.255.140]
 12   244 ms   243 ms   243 ms  CS.stanford.edu [171.64.64.64]

Trace complete.
```

```
C:\Users\Gaurav\Desktop
λ tracert cs.manchester.ac.uk

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

  1    <1 ms    <1 ms    <1 ms  192.168.0.1
  2     1 ms    <1 ms     1 ms  103.76.56.132
  3     2 ms     2 ms     1 ms  103.76.56.129
  4     1 ms     1 ms     1 ms  103.249.251.213
  5     4 ms     4 ms     3 ms  nsg-static-173.107.75.182-airtel.com [182.75.107.173]
  6   136 ms   136 ms   137 ms  182.79.146.216
  7   134 ms     *      134 ms  ldn-b4-link.telia.net [62.115.162.232]
  8   138 ms   137 ms   137 ms  jisc-ic-345131-ldn-b4.c.telia.net [62.115.175.131]
  9   134 ms   133 ms   135 ms  ae24.londhx-sbr1.ja.net [146.97.35.197]
 10   134 ms   134 ms   133 ms  ae29.londpg-sbr2.ja.net [146.97.33.2]
 11   137 ms   156 ms   137 ms  ae31.erdiss-sbr2.ja.net [146.97.33.22]
 12   139 ms   139 ms   140 ms  ae29.manckh-sbr2.ja.net [146.97.33.42]
 13   147 ms   139 ms   139 ms  ae23.mancrh-rbr1.ja.net [146.97.38.42]
 14   140 ms     *        *     universityofmanchester.ja.net [146.97.169.2]
 15   139 ms   140 ms   139 ms  130.88.249.194
 16     *        *        *     Request timed out.
 17   141 ms   141 ms   141 ms  gw-jh.its.manchester.ac.uk [130.88.250.32]
 18   145 ms   143 ms   144 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.

```
C:\Users\Gaurav\Desktop
λ 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  192.168.0.1
  2    <1 ms    <1 ms     1 ms  103.76.56.132
  3     2 ms     1 ms     1 ms  103.76.56.129
  4     1 ms     1 ms     1 ms  103.249.251.213
  5     8 ms    14 ms     5 ms  nsg-static-173.107.75.182-airtel.com [182.75.107.173]
  6   232 ms   229 ms   230 ms  182.79.217.217
  7   241 ms   242 ms   241 ms  xe-9-1-0.edge1.LosAngeles6.Level3.net [4.26.0.61]
  8     *      224 ms   224 ms  ae-2-52.ear3.LosAngeles1.Level3.net [4.69.207.49]
  9     *        *        *     Request timed out.
 10   294 ms   294 ms   293 ms  roc1-ar5-xe-0-0-0-0.us.twtelecom.net [35.248.1.158]
 11   299 ms   299 ms   298 ms  66-195-65-170.static.ctl.one [66.195.65.170]
 12   291 ms   291 ms   292 ms  nat.hws.edu [64.89.144.100]
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.
```

```
C:\Users\Gaurav\Desktop
λ 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  192.168.0.1
  2     1 ms    <1 ms     1 ms  103.76.56.132
  3     1 ms     1 ms     1 ms  103.76.56.129
  4     1 ms     1 ms     1 ms  103.249.251.213
  5     3 ms     4 ms     4 ms  nsg-static-173.107.75.182-airtel.com [182.75.107.173]
  6   228 ms   230 ms   241 ms  182.79.245.81
  7   242 ms   242 ms   241 ms  ae58.edge1.LosAngeles6.Level3.net [4.26.0.17]
  8     *        *      221 ms  ae-2-52.ear3.LosAngeles1.Level3.net [4.69.207.49]
  9     *        *        *     Request timed out.
 10   290 ms   290 ms   290 ms  roc1-ar5-xe-0-0-0-0.us.twtelecom.net [35.248.1.158]
 11   295 ms   295 ms   296 ms  66-195-65-170.static.ctl.one [66.195.65.170]
 12   288 ms   288 ms   288 ms  nat.hws.edu [64.89.144.100]
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.
```

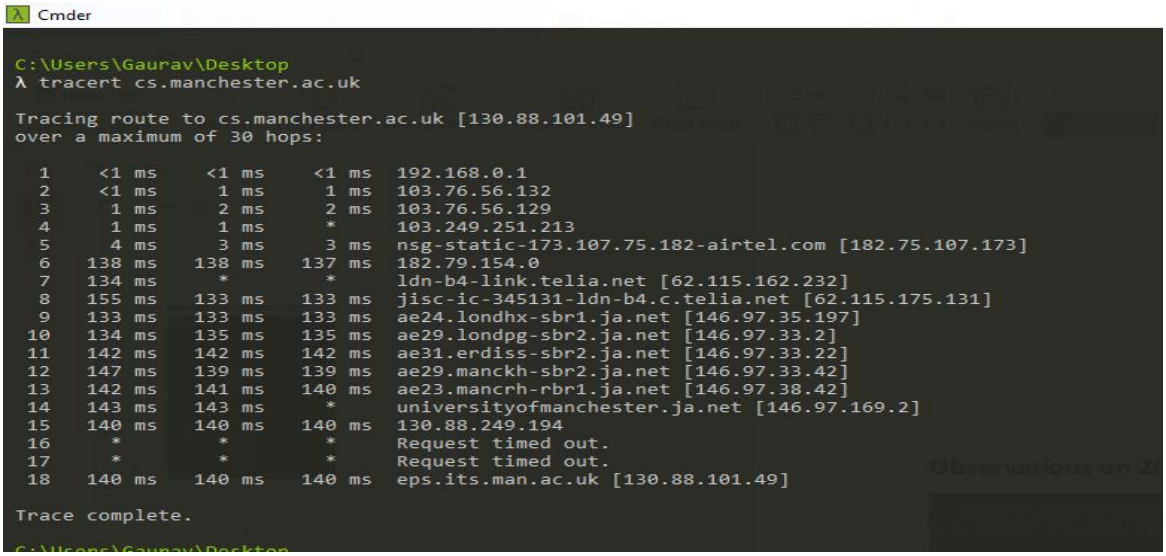
Results:
When we connect to another computer, traffic does not go directly to the machine we are attempting to connect to. Instead it goes through multiple machines on the Internet known as routers. These machines serve the sole purpose of controlling how your traffic gets to your destination. If any one connection fails, we will not be able to connect to the intended destination. Hence it is used for diagnostics. Each hop displays the time taken for each hop during its route to the destination. If a hop comes back with request timed out it denotes network congestion.
From the above results, we can see that the source i.e. the first 6 hops are the same and some variations in the round trip time can be observed.

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.

Observations on 27/08/2020

```
C:\Users\Gaurav\Desktop
λ tracert cs.manchester.ac.uk

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

  1    <1 ms    <1 ms    <1 ms  192.168.0.1
  2     1 ms    <1 ms     1 ms  103.76.56.132
  3     2 ms     2 ms     1 ms  103.76.56.129
  4     1 ms     1 ms     1 ms  103.249.251.213
  5     4 ms     4 ms     3 ms  nsg-static-173.107.75.182-airtel.com [182.75.107.173]
  6   136 ms   136 ms   137 ms  182.79.146.216
  7   134 ms     *      134 ms  ldn-b4-link.telia.net [62.115.162.232]
  8   138 ms   137 ms   137 ms  jisc-ic-345131-ldn-b4.c.telia.net [62.115.175.131]
  9   134 ms   133 ms   135 ms  ae24.londhx-sbr1.ja.net [146.97.35.197]
 10   134 ms   134 ms   133 ms  ae29.londpg-sbr2.ja.net [146.97.33.2]
 11   137 ms   156 ms   137 ms  ae31.erdiss-sbr2.ja.net [146.97.33.22]
 12   139 ms   139 ms   140 ms  ae29.manckh-sbr2.ja.net [146.97.33.42]
 13   147 ms   139 ms   139 ms  ae23.mancrh-rbr1.ja.net [146.97.38.42]
 14   140 ms     *        *     universityofmanchester.ja.net [146.97.169.2]
 15   139 ms   140 ms   139 ms  130.88.249.194
 16     *        *        *     Request timed out.
 17   141 ms   141 ms   141 ms  gw-jh.its.manchester.ac.uk [130.88.250.32]
 18   145 ms   143 ms   144 ms  eps.its.man.ac.uk [130.88.101.49]

Trace complete.
```

Observations on 28/08/2020



Through this we get to know that in spite of the source and destination being the same it is not necessary that the path of the route or the intermediate nodes and their respective RTTs will also be the 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?**

   Answer: 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?**

   Answer: No, the number of nodes and the location of the host are not related to each other. It even depends on the physical interface that is being used.

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?**

Answer - There is a direct relationship between the number of nodes and the latency of the host. The amount of latency is largely dependent on how far the visitor is from the server location and how many nodes the signal has to travel through.

Whois — The *whois* command can give detailed information about domain names and IP addresses. If it is not installed on the computers then install it with command sudo apt-get install whois in. *Whois* can tell you what organization owns or is responsible for the name or address and where to contact them. It often includes a list of domain name servers for the organization.

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

Exercise 4: (Short.) Use *whois* to investigate a well-known web site such as google.com or amazon.com, and write a couple of sentences about what you find out.

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

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

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

curl ipinfo.io/129.64.99.200

```
C:\Users\Gaurav\Desktop
λ 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 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 and time taken by each step (hop).

References:

- https://www.cloudflare.com/learning/cdn/glossary/round-trip-time-rtt/
- https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/netstat
- https://www.inmotionhosting.com/support/website/ssh/read-traceroute/