Name : Priyav Mehta
UID : 2018130026
Batch : B

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

```
C:\Users\priyavmehta>ping -n 10 -l 64 cs.stanford.edu

Pinging cs.stanford.edu [171.64.64.64] with 64 bytes of data:
Reply from 171.64.64.64: bytes=64 time=281ms TTL=46
Reply from 171.64.64.64: bytes=64 time=285ms TTL=46
Reply from 171.64.64.64: bytes=64 time=280ms TTL=46
Reply from 171.64.64.64: bytes=64 time=281ms TTL=46
Reply from 171.64.64.64: bytes=64 time=284ms TTL=46
Reply from 171.64.64.64: bytes=64 time=268ms TTL=46
Reply from 171.64.64.64: bytes=64 time=283ms TTL=46
Reply from 171.64.64.64: bytes=64 time=283ms TTL=46
Reply from 171.64.64.64: bytes=64 time=276ms TTL=46
Reply from 171.64.64.64: bytes=64 time=300ms TTL=46

Ping statistics for 171.64.64.64:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 268ms, Maximum = 300ms, Average = 282ms
```

```
C:\Users\priyavmehta>ping -n 10 -l 100 cs.stanford.edu

Pinging cs.stanford.edu [171.64.64.64] with 100 bytes of data:
Reply from 171.64.64.64: bytes=100 time=279ms TTL=46
Reply from 171.64.64.64: bytes=100 time=271ms TTL=46
Reply from 171.64.64.64: bytes=100 time=275ms TTL=46
Reply from 171.64.64.64: bytes=100 time=278ms TTL=46
Reply from 171.64.64.64: bytes=100 time=292ms TTL=46
Reply from 171.64.64.64: bytes=100 time=291ms TTL=46
Reply from 171.64.64.64: bytes=100 time=284ms TTL=46
Reply from 171.64.64.64: bytes=100 time=277ms TTL=46
Reply from 171.64.64.64: bytes=100 time=281ms TTL=46
Reply from 171.64.64.64: bytes=100 time=296ms TTL=46

Ping statistics for 171.64.64.64:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 271ms, Maximum = 296ms, Average = 282ms
```

```
C:\Users\priyavmehta>ping -n 10 -l 500 cs.stanford.edu

Pinging cs.stanford.edu [171.64.64.64] with 500 bytes of data:
Reply from 171.64.64.64: bytes=500 time=285ms TTL=46
Reply from 171.64.64.64: bytes=500 time=278ms TTL=46
Reply from 171.64.64.64: bytes=500 time=281ms TTL=46
Reply from 171.64.64.64: bytes=500 time=283ms TTL=46
Reply from 171.64.64.64: bytes=500 time=285ms TTL=46
Reply from 171.64.64.64: bytes=500 time=290ms TTL=46
Reply from 171.64.64.64: bytes=500 time=283ms TTL=46
Reply from 171.64.64.64: bytes=500 time=283ms TTL=46
Reply from 171.64.64.64: bytes=500 time=284ms TTL=46
Reply from 171.64.64.64: bytes=500 time=281ms TTL=46

Ping statistics for 171.64.64.64:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 278ms, Maximum = 290ms, Average = 283ms
```

```
C:\Users\priyavmehta>ping -n 10 -l 1000 cs.stanford.edu

Pinging cs.stanford.edu [171.64.64.64] with 1000 bytes of data:
Reply from 171.64.64.64: bytes=1000 time=292ms TTL=46
Reply from 171.64.64.64: bytes=1000 time=275ms TTL=46
Reply from 171.64.64.64: bytes=1000 time=285ms TTL=46
Reply from 171.64.64.64: bytes=1000 time=286ms TTL=46
Reply from 171.64.64.64: bytes=1000 time=281ms TTL=46
Reply from 171.64.64.64: bytes=1000 time=293ms TTL=46
Reply from 171.64.64.64: bytes=1000 time=282ms TTL=46
Reply from 171.64.64.64: bytes=1000 time=282ms TTL=46
Reply from 171.64.64.64: bytes=1000 time=286ms TTL=46
Reply from 171.64.64.64: bytes=1000 time=286ms TTL=46

Ping statistics for 171.64.64.64:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 275ms, Maximum = 293ms, Average = 284ms
```

```
C:\Users\priyavmehta>ping -n 10 -l 1400 cs.stanford.edu

Pinging cs.stanford.edu [171.64.64.64] with 1400 bytes of data:
Reply from 171.64.64.64: bytes=1400 time=286ms TTL=46
Reply from 171.64.64.64: bytes=1400 time=289ms TTL=46
Reply from 171.64.64.64: bytes=1400 time=283ms TTL=46
Reply from 171.64.64.64: bytes=1400 time=284ms TTL=46
Reply from 171.64.64.64: bytes=1400 time=290ms TTL=46
Reply from 171.64.64.64: bytes=1400 time=296ms TTL=46
Reply from 171.64.64.64: bytes=1400 time=290ms TTL=46
Reply from 171.64.64.64: bytes=1400 time=291ms TTL=46
Reply from 171.64.64.64: bytes=1400 time=287ms TTL=46
Reply from 171.64.64.64: bytes=1400 time=293ms TTL=46

Ping statistics for 171.64.64.64:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 283ms, Maximum = 296ms, Average = 288ms
```

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?

Round-trip time (RTT) is the duration in milliseconds (ms) it takes for a network request to go from a starting point to a destination and back again to the starting point. RTT is an important metric in determining the health of a connection on a local network or the larger Internet, and is commonly utilised by network administrators to diagnose the speed and reliability of network connections. Delay may differ slightly, depending on the location of the specific pair of communicating endpoints. Engineers usually report both the maximum and average delay, and they divide the delay into several parts:

- 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.

  A certain minimum level of delay is experienced by signals due to the time it takes to transmit a packet serially through a link. This delay is extended by more variable

levels of delay due to network congestion. IP network delays can range from a few milliseconds to several hundred milliseconds. [8]

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 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's

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).

Command Prompt

```
Microsoft Windows [Version 10.0.18362.959]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\priyavmehta>ping www.uw.edu

Pinging www.washington.edu [128.95.155.197] with 32 bytes of data:
Reply from 128.95.155.197: bytes=32 time=330ms TTL=44
Reply from 128.95.155.197: bytes=32 time=503ms TTL=44
Reply from 128.95.155.197: bytes=32 time=313ms TTL=44
Reply from 128.95.155.197: bytes=32 time=335ms TTL=44

Ping statistics for 128.95.155.197:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 313ms, Maximum = 503ms, Average = 370ms
```

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

Pinging www-production-1113102805.us-west-2.elb.amazonaws.com [2600:1f14:436:7800:4110:c28c:3c8b:7aa5] with 32 bytes of data:
Reply from 2600:1f14:436:7800:4110:c28c:3c8b:7aa5: time=944ms
Reply from 2600:1f14:436:7800:4110:c28c:3c8b:7aa5: time=446ms
Reply from 2600:1f14:436:7800:4110:c28c:3c8b:7aa5: time=930ms
Reply from 2600:1f14:436:7800:4110:c28c:3c8b:7aa5: time=408ms

Ping statistics for 2600:1f14:436:7800:4110:c28c:3c8b:7aa5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 408ms, Maximum = 944ms, Average = 682ms
```

```
C:\Users\priyavmehta>ping www.uchicago.edu

Pinging wsee2.elb.uchicago.edu [54.89.29.50] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 54.89.29.50:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

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

Pinging www.ox.ac.uk [151.101.194.133] with 32 bytes of data:
Reply from 151.101.194.133: bytes=32 time=169ms TTL=53
Reply from 151.101.194.133: bytes=32 time=131ms TTL=53
Reply from 151.101.194.133: bytes=32 time=137ms TTL=53
Reply from 151.101.194.133: bytes=32 time=146ms TTL=53

Ping statistics for 151.101.194.133:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 131ms, Maximum = 169ms, Average = 145ms
```

```
C:\Users\priyavmehta>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),
```

Interesting Observations : RTT is different for different hosts.

Possible reasons are :

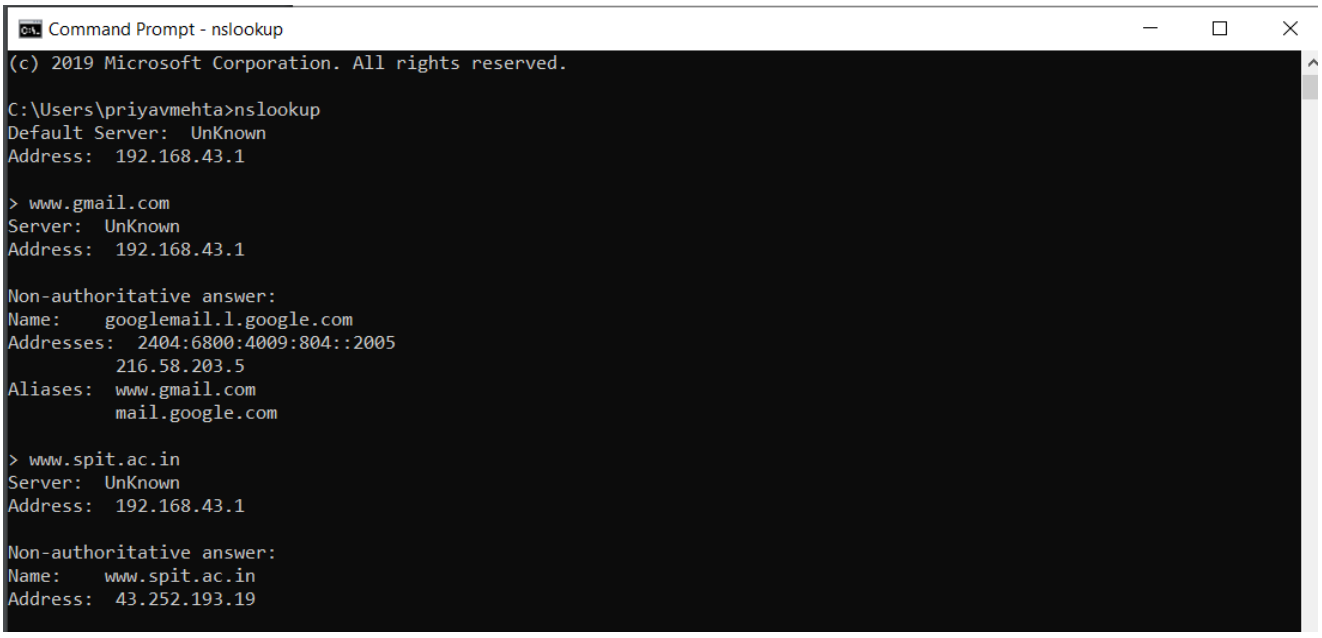
The nature of the transmission medium - the way in which connections are made affects how fast the connection moves; connections made over optical fiber will behave differently than connections made over copper. Likewise, a connection made over a wireless frequency will behave differently than that of a satellite communication. [9]

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. [9]

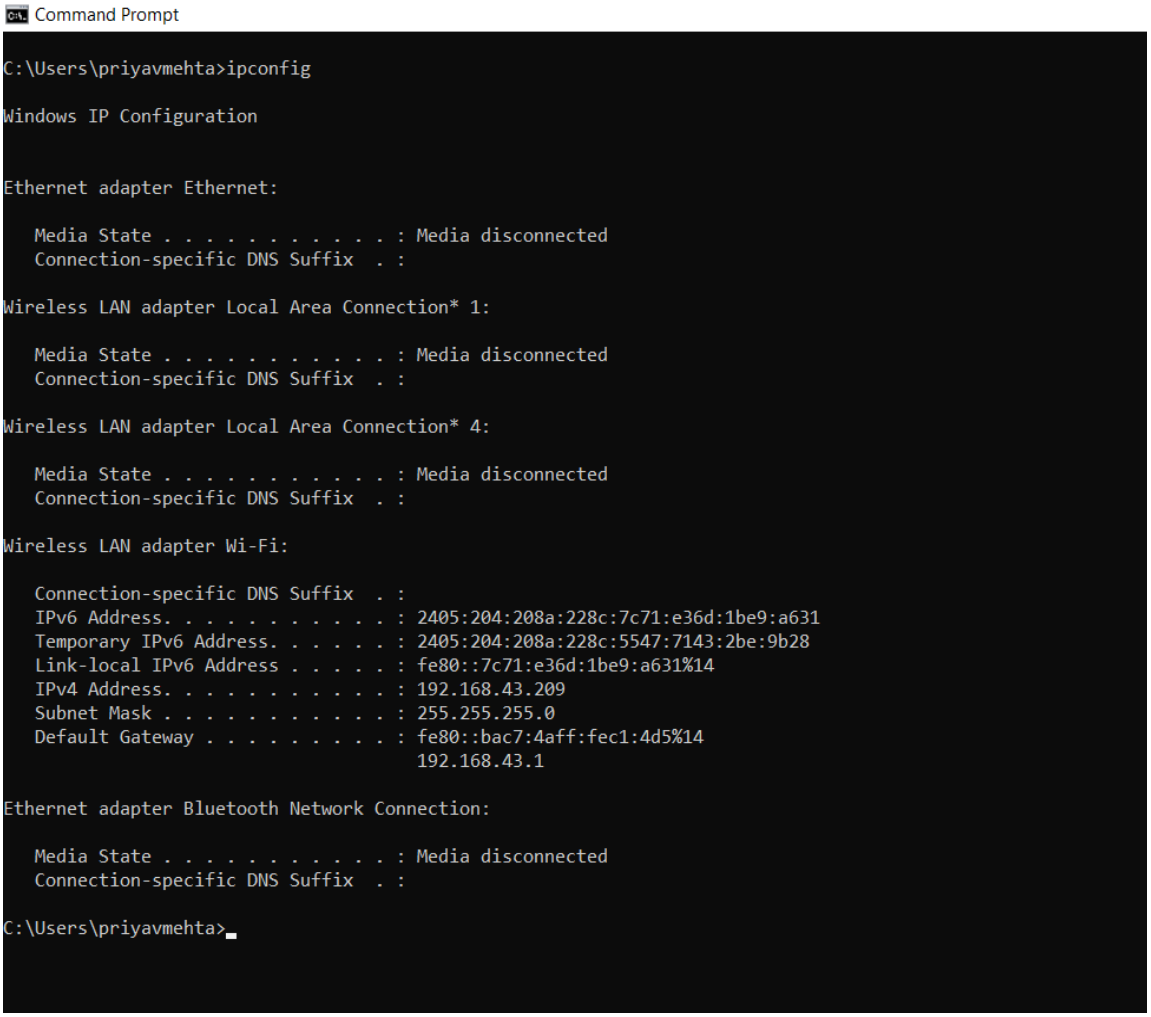
Local area network (LAN) traffic - the amount of traffic on the local area network can bottleneck a connection before it ever reaches the larger Internet. For example, if many users are using streaming video service simultaneously, round-trip time may be inhibited even though the external network has excess capacity and is functioning normally. [9]

Physical distance between two hosts is defined as the length of the great circle arc connecting their locations on the surface of the Earth. Minimum RTT is two times of the propagation delay on the link. And propagation delay depends on the distance between hosts and speed of propagation. Hence RTT directly depends on the distance.[6]

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



ipconfig — 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!!!.)



Ethernet adapter Ethernet : Gives the information whether the system is connected with the wired ethernet connection

Wireless LAN adapter : Wireless local area network adapters are add-on devices that enable you to connect to wireless networks like at the office or hotel. These adapters can be added to either desktop or laptop computers, so long as the hardware and software are compatible.[1]

Wireless LAN adapter Wi-fi : Shows the Wi-fi connection in the system.

IPv6 Address : An **Internet Protocol Version 6 address** (IPv6 address) is a numerical label that is used to identify a network interface of a computer or a network node participating in an IPv6 computer network and for locating it in the network. IPv6 addresses have a size of 128 bits [2]

Temporary IPv6 Address : An IPv6 **temporary address** includes a randomly generated 64-bit number as the interface ID, instead of an interface's MAC address. You can use temporary addresses for any interfaces on an IPv6 node that you want to keep anonymous.[3]

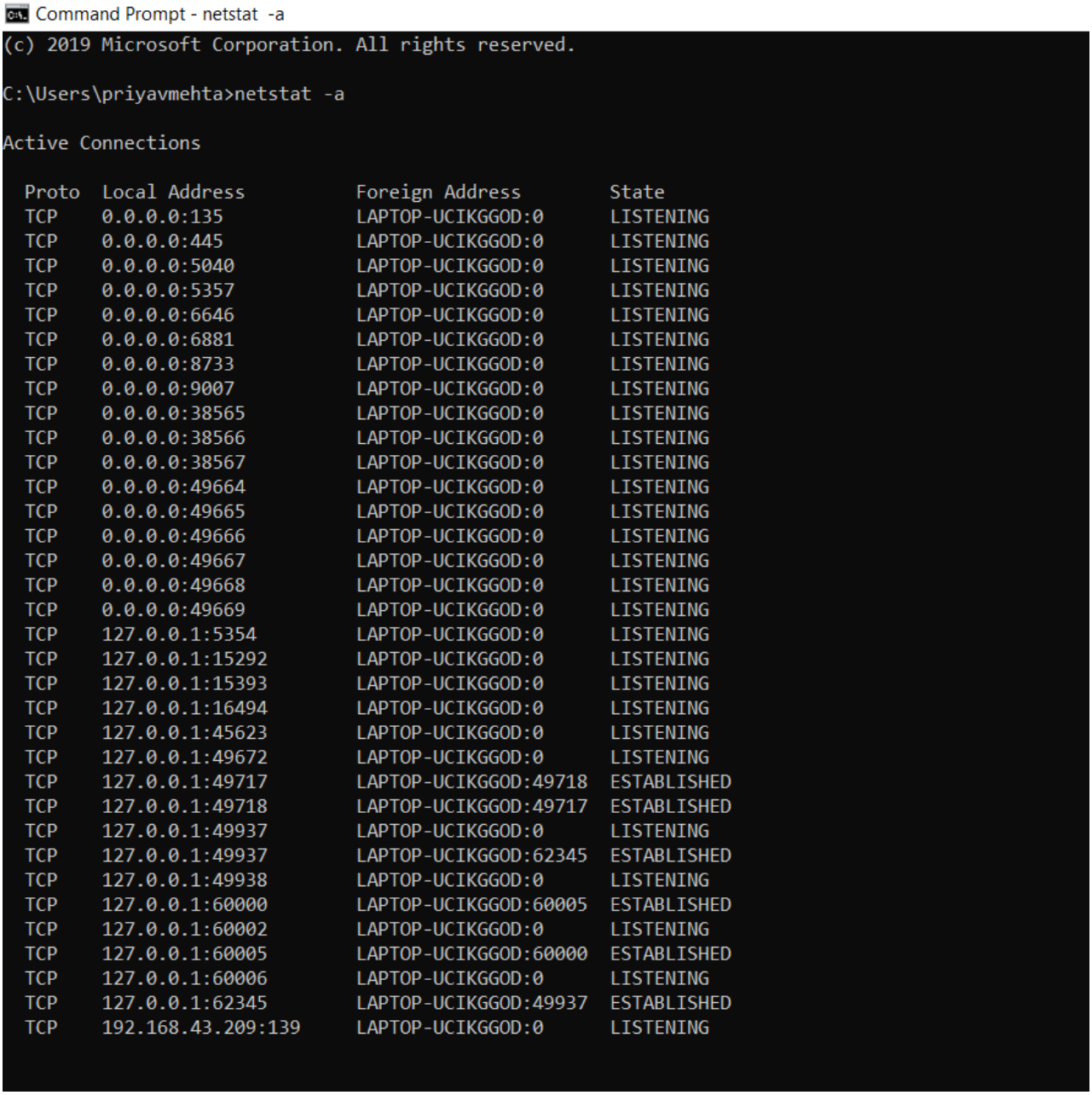
Link-local IPv6 Address : A link-local address is an IPv6 unicast address that can be automatically configured on any interface using the link-local prefix FE80::/10 (1111 1110 10) and the interface identifier in the modified EUI-64 format.[4]

IPv4 Address : The IP address being used by the network connection.

Subnet Mask : The specific section of the network to which a computer is connected.[5]

Default-Gateway : The router or switch that the network connection goes through.[5]

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`).

traceroute_iitb.ac.in - Notepad

File Edit Format View Help

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

  1     4 ms     4 ms   751 ms  192.168.43.1
  2     *        *        *     Request timed out.
  3  1012 ms   202 ms    44 ms  10.71.16.18
  4   595 ms    41 ms   162 ms  192.168.69.160
  5   109 ms   171 ms    31 ms  192.168.69.159
  6   446 ms   168 ms   204 ms  172.16.80.109
  7   314 ms   247 ms   203 ms  172.17.119.4
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13   364 ms    46 ms    38 ms  115.110.206.73.static-Mumbai.vsnl.net.in [115.110.206.73]
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16   151 ms   384 ms   388 ms  115.110.234.170.static.Mumbai.vsnl.net.in [115.110.234.170]
 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.
```

traceroute_mscs.mu.edu - Notepad

File Edit Format View Help

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

  1   575 ms   409 ms     4 ms  192.168.43.1
  2     *        *        *     Request timed out.
  3    36 ms   109 ms   203 ms  10.71.16.18
  4   867 ms   470 ms    84 ms  192.168.69.162
  5   220 ms    64 ms   138 ms  192.168.69.163
  6   155 ms   311 ms   234 ms  172.16.80.107
  7   169 ms   140 ms    63 ms  172.17.119.4
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11   715 ms   438 ms   165 ms  103.198.140.58
 12   173 ms   150 ms   140 ms  103.198.140.56
 13   382 ms   179 ms   143 ms  103.198.140.56
 14   146 ms   295 ms   225 ms  hurricane.mrs.franceix.net [37.49.232.13]
 15   212 ms   359 ms   152 ms  100ge4-2.core1.par2.he.net [184.105.222.21]
 16   246 ms   220 ms   415 ms  100ge14-1.core1.nyc4.he.net [184.105.81.77]
 17   373 ms   317 ms     *     100ge9-1.core2.chi1.he.net [184.105.223.161]
 18     *        *        *     Request timed out.
 19   370 ms   409 ms   614 ms  r-222wwash-isp-ae6-3926.wiscnet.net [140.189.8.126]
 20   497 ms   349 ms   613 ms  r-milwaukeeci-809-isp-ae3-0.wiscnet.net [140.189.8.230]
 21   633 ms   613 ms   395 ms  MarquetteUniv.site.wiscnet.net [216.56.1.202]
 22   626 ms   558 ms   453 ms  134.48.10.26
 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.
```

traceroute_www.cs.grinnell.edu - Notepad

File Edit Format View Help

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

  1   151 ms     5 ms     5 ms  192.168.43.1
  2     *        *        *     Request timed out.
  3   234 ms   203 ms   204 ms  10.71.16.18
  4   617 ms   205 ms    66 ms  192.168.69.164
  5   113 ms    36 ms    30 ms  192.168.69.165
  6   382 ms    32 ms    31 ms  172.16.80.111
  7   100 ms   142 ms    91 ms  172.17.119.4
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11    98 ms    42 ms   161 ms  103.198.140.58
 12   187 ms  1207 ms   208 ms  103.198.140.56
 13   219 ms   204 ms   203 ms  103.198.140.56
 14   218 ms   238 ms   349 ms  hurricane.mrs.franceix.net [37.49.232.13]
 15   391 ms   407 ms   290 ms  100ge4-2.core1.par2.he.net [184.105.222.21]
 16   270 ms   362 ms   408 ms  100ge14-1.core1.nyc4.he.net [184.105.81.77]
 17   276 ms   295 ms   467 ms  100ge2-1.core2.chi1.he.net [184.104.193.173]
 18   283 ms   611 ms   613 ms  100ge14-2.core1.msp1.he.net [184.105.223.178]
 19   429 ms   408 ms   245 ms  aureon-network-services-inc.e0-26.switch1.msp1.he.net [216.66.77.218]
 20   470 ms   408 ms   561 ms  peer-as5056.br02.msp1.tfbnw.net [157.240.76.37]
 21   786 ms   409 ms   263 ms  167.142.58.40
 22   481 ms   411 ms   406 ms  67.224.64.62
 23   355 ms   408 ms   613 ms  grinnellcollege1.desm.netins.net [167.142.65.43]
 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.
```

traceroute_csail.mit.edu - Notepad

File Edit Format View Help

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

  1     4 ms     4 ms     5 ms  192.168.43.1
  2     *        *        *     Request timed out.
  3   148 ms    39 ms   162 ms  10.71.16.18
  4   137 ms   244 ms   203 ms  192.168.69.164
  5   213 ms    34 ms   168 ms  192.168.69.165
  6    44 ms    35 ms   103 ms  172.16.80.113
  7    38 ms   109 ms    42 ms  172.17.119.4
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13   122 ms   203 ms   177 ms  49.45.4.251
 14   363 ms   409 ms   408 ms  49.45.4.103
 15   302 ms   260 ms   382 ms  103.198.140.89
 16   323 ms   273 ms   268 ms  4.7.26.61
 17     *        *        *     Request timed out.
 18   326 ms   618 ms   323 ms  MASSACHUSET.bear1.Boston1.Level3.net [4.53.48.98]
 19   455 ms   639 ms   341 ms  dmz-rtr-1-external-rtr-1.mit.edu [18.0.161.17]
 20   500 ms   617 ms   405 ms  dmz-rtr-2-dmz-rtr-1-2.mit.edu [18.0.162.6]
 21   369 ms   630 ms   574 ms  mitnet.core-1-ext.csail.mit.edu [18.4.7.65]
 22     *        *     1286 ms  core-1-ext.bdr.csail.mit.edu [128.30.13.26]
 23   408 ms   613 ms   409 ms  bdr.core-1.csail.mit.edu [128.30.0.246]
 24   427 ms   420 ms   364 ms  inquir-3ld.csail.mit.edu [128.30.2.109]

Trace complete.
```

traceroute_cs.stanford.edu - Notepad

File Edit Format View Help

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

  1     3 ms   119 ms     3 ms  192.168.43.1
  2     *        *        *     Request timed out.
  3   168 ms   204 ms   127 ms  10.71.16.18
  4   219 ms   204 ms    32 ms  192.168.69.160
  5   407 ms   203 ms    48 ms  192.168.69.159
  6   217 ms   204 ms   204 ms  172.16.80.107
  7   210 ms   373 ms   239 ms  172.17.119.4
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11    79 ms    25 ms    29 ms  103.198.140.174
 12   533 ms   149 ms   147 ms  103.198.140.27
 13   144 ms   141 ms   149 ms  103.198.140.27
 14   511 ms   163 ms   163 ms  hurricane.mrs.franceix.net [37.49.232.13]
 15   175 ms   163 ms   171 ms  100ge4-2.core1.par2.he.net [184.105.222.21]
 16   241 ms   230 ms   312 ms  100ge10-2.core1.ash1.he.net [184.105.213.173]
 17   303 ms   280 ms   289 ms  100ge7-2.core1.pao1.he.net [184.105.222.41]
 18   406 ms   409 ms   409 ms  stanford-university.100gigabitethernet5-1.core1.pao1.he.net [184.105.177.238]
 19   346 ms   319 ms   328 ms  csee-west-rtr-vl3.SUNet [171.66.255.140]
 20   277 ms   309 ms   333 ms  CS.stanford.edu [171.64.64.64]

Trace complete.
```

traceroute_cs.manchester.ac.uk - Notepad

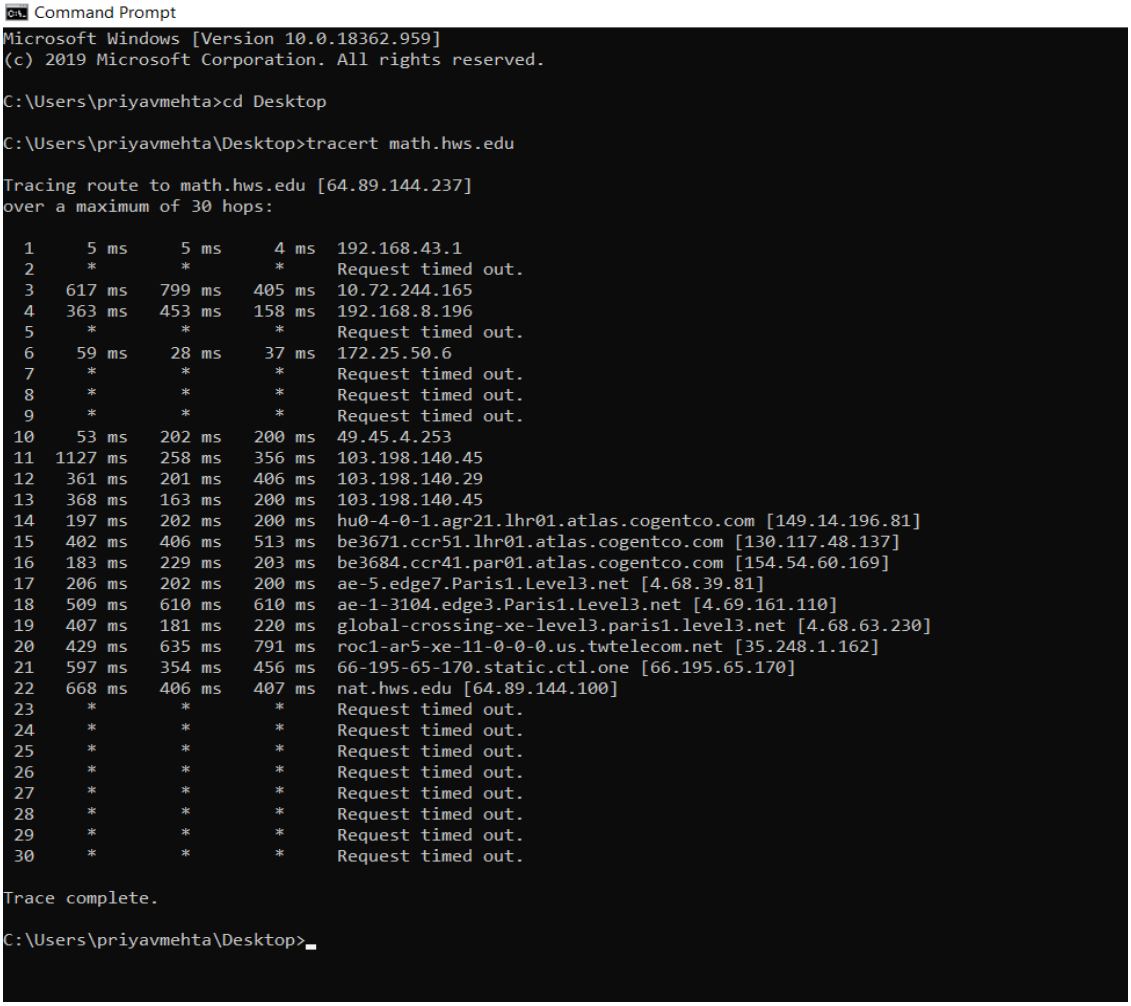
File Edit Format View Help

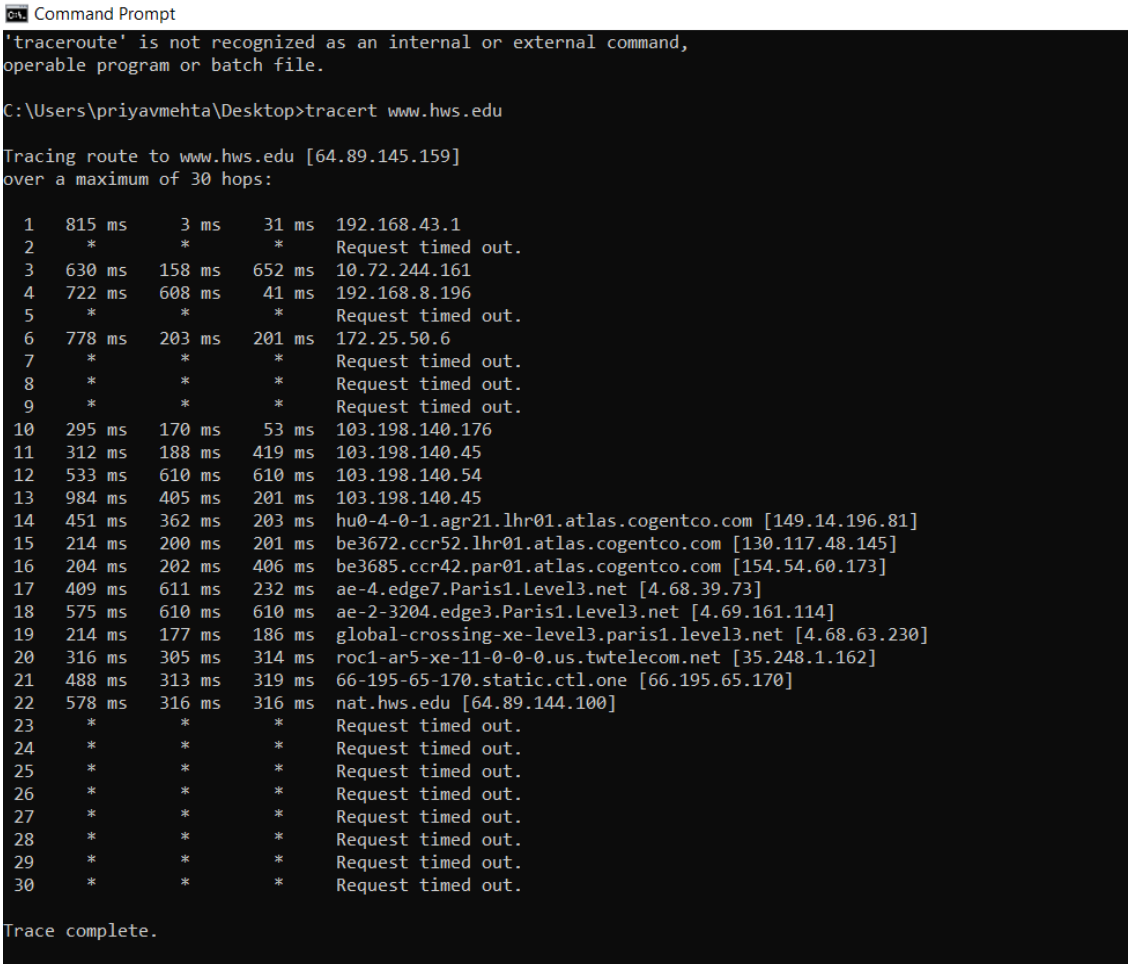
```
Tracing route to cs.manchester.ac.uk [130.88.101.49]
over a maximum of 30 hops:

  1     4 ms     3 ms    12 ms  192.168.43.1
  2     *        *        *     Request timed out.
  3    68 ms   323 ms   202 ms  10.71.16.18
  4    42 ms    40 ms    39 ms  192.168.69.158
  5   110 ms   372 ms  1054 ms  192.168.69.161
  6   128 ms    67 ms   182 ms  172.16.80.113
  7   976 ms   458 ms   362 ms  172.17.119.4
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11   435 ms   566 ms   249 ms  103.198.140.174
 12   468 ms   411 ms   408 ms  103.198.140.45
 13   435 ms   750 ms   634 ms  103.198.140.27
 14  1116 ms     *      317 ms  103.198.140.107
 15   465 ms   412 ms   417 ms  103.198.140.45
 16   624 ms   205 ms   204 ms  hu0-4-0-1.agr21.lhr01.atlas.cogentco.com [149.14.196.81]
 17   440 ms   581 ms   220 ms  be3671.ccr51.lhr01.atlas.cogentco.com [130.117.48.137]
 18   479 ms   578 ms   613 ms  be3684.ccr41.par01.atlas.cogentco.com [154.54.60.169]
 19   224 ms   203 ms   408 ms  prs-b2-link.telia.net [213.155.141.226]
 20   189 ms   190 ms   377 ms  prs-bb3-link.telia.net [62.115.122.4]
 21   489 ms   612 ms   204 ms  ldn-bb3-link.telia.net [62.115.134.93]
 22   425 ms   391 ms   220 ms  ldn-b7-link.telia.net [62.115.138.151]
 23   441 ms   204 ms   408 ms  jisc-ic-345130-ldn-b7.c.telia.net [62.115.175.107]
 24   429 ms   613 ms   409 ms  ae24.londtt-sbr1.ja.net [146.97.35.193]
 25   225 ms   204 ms   203 ms  ae28.londtw-sbr2.ja.net [146.97.33.62]
 26   222 ms   408 ms   204 ms  ae31.lowdss-sbr1.ja.net [146.97.33.29]
 27   431 ms   204 ms   204 ms  ae29.leedaq-sbr2.ja.net [146.97.33.49]
 28   223 ms   408 ms   613 ms  ae25.presab-rbr1.ja.net [146.97.38.46]
 29   427 ms   239 ms   373 ms  ae28.mancrh-rbr1.ja.net [146.97.78.69]
 30     *        *        *     Request timed out.

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.


Command Prompt
Microsoft Windows [Version 10.0.18362.959]
(c) 2019 Microsoft Corporation. All rights reserved.
C:\Users\priyavmehta>cd Desktop
C:\Users\priyavmehta\Desktop>tracert math.hws.edu
Tracing route to math.hws.edu [64.89.144.237]
over a maximum of 30 hops:
1 5 ms 5 ms 4 ms 192.168.43.1
2 * * * Request timed out.
3 617 ms 799 ms 405 ms 10.72.244.165
4 363 ms 453 ms 158 ms 192.168.8.196
5 * * * Request timed out.
6 59 ms 28 ms 37 ms 172.25.50.6
7 * * * Request timed out.
8 * * * Request timed out.
9 * * * Request timed out.
10 53 ms 202 ms 200 ms 49.45.4.253
11 1127 ms 258 ms 356 ms 103.198.140.45
12 361 ms 201 ms 406 ms 103.198.140.29
13 368 ms 163 ms 200 ms 103.198.140.45
14 197 ms 202 ms 200 ms hu0-4-0-1.agr21.lhr01.atlas.cogentco.com [149.14.196.81]
15 402 ms 406 ms 513 ms be3671.ccr51.lhr01.atlas.cogentco.com [130.117.48.137]
16 183 ms 229 ms 203 ms be3684.ccr41.par01.atlas.cogentco.com [154.54.60.169]
17 206 ms 202 ms 200 ms ae-5.edge7.Paris1.Level3.net [4.68.39.81]
18 509 ms 610 ms 610 ms ae-1-3104.edge3.Paris1.Level3.net [4.69.161.110]
19 407 ms 181 ms 220 ms global-crossing-xe-level3.paris1.level3.net [4.68.63.230]
20 429 ms 635 ms 791 ms roc1-ar5-xe-11-0-0-0.us.twtelecom.net [35.248.1.162]
21 597 ms 354 ms 456 ms 66-195-65-170.static.ctl.one [66.195.65.170]
22 668 ms 406 ms 407 ms nat.hws.edu [64.89.144.100]
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\priyavmehta\Desktop>



Some hops are same for both routes and some are different. Overall paths are hence different for both.

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.

Command Prompt

```
Microsoft Windows [Version 10.0.18362.959]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\priyavmehta>tracert www.hws.edu

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

  1    57 ms   539 ms     4 ms  192.168.43.1
  2     *        *        *     Request timed out.
  3   208 ms   346 ms   220 ms  10.71.5.29
  4   168 ms    54 ms   334 ms  192.168.70.221
  5    40 ms    58 ms    57 ms  192.168.70.216
  6     *        *        *     Request timed out.
  7  1526 ms   156 ms   201 ms  172.25.50.7
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11    49 ms     *      156 ms  103.198.140.174
 12   314 ms   201 ms   201 ms  103.198.140.45
 13   359 ms   406 ms   201 ms  103.198.140.56
 14   193 ms   211 ms   192 ms  103.198.140.107
 15   424 ms   169 ms   405 ms  103.198.140.45
 16   402 ms   206 ms   201 ms  hu0-4-0-1.agr21.lhr01.atlas.cogentco.com [149.14.196.81]
 17   211 ms   193 ms   201 ms  be3672.ccr52.lhr01.atlas.cogentco.com [130.117.48.145]
 18   205 ms   561 ms   201 ms  be3488.ccr42.lon13.atlas.cogentco.com [154.54.60.13]
 19   172 ms   181 ms   147 ms  be2869.ccr22.lon01.atlas.cogentco.com [154.54.57.162]
 20     *        *        *     Request timed out.
 21   891 ms   202 ms   239 ms  ae-117-3503.edge3.London15.Level3.net [4.69.167.82]
 22   244 ms   201 ms   203 ms  ae-117-3503.edge3.London15.Level3.net [4.69.167.82]
 23   209 ms   201 ms   201 ms  ae4.ar8.lon15.Level3.net [4.68.111.254]
 24   616 ms   406 ms   406 ms  roc1-ar5-xe-11-0-0-0.us.twtelecom.net [35.248.1.162]
 25   409 ms   410 ms   402 ms  66-195-65-170.static.ctl.one [66.195.65.170]
 26   413 ms   406 ms   406 ms  64.89.144.100
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.

C:\Users\priyavmehta>
```

Command Prompt

```
Control-C
^C
C:\Users\priyavmehta>tracert math.hws.edu

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

  1   405 ms   959 ms   223 ms  192.168.43.1
  2     *        *        *     Request timed out.
  3   794 ms   647 ms   610 ms  10.71.5.29
  4    63 ms    47 ms   215 ms  192.168.70.221
  5   235 ms   200 ms   202 ms  192.168.70.216
  6     *        *        *     Request timed out.
  7    58 ms    36 ms    39 ms  172.25.50.7
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11   220 ms   201 ms   198 ms  103.198.140.58
 12  1027 ms   554 ms   201 ms  103.198.140.45
 13   205 ms   213 ms   189 ms  103.198.140.56
 14   197 ms   200 ms   201 ms  103.198.140.107
 15   434 ms  1409 ms   206 ms  103.198.140.45
 16   249 ms   366 ms   406 ms  hu0-4-0-1.agr21.lhr01.atlas.cogentco.com [149.14.196.81]
 17   409 ms   201 ms   201 ms  be3671.ccr51.lhr01.atlas.cogentco.com [130.117.48.137]
 18   358 ms   816 ms   264 ms  be3487.ccr41.lon13.atlas.cogentco.com [154.54.60.5]
 19   372 ms   201 ms   201 ms  be2868.ccr21.lon01.atlas.cogentco.com [154.54.57.154]
 20     *        *        *     Request timed out.
 21   548 ms   402 ms   206 ms  ae-115-3501.edge3.London15.Level3.net [4.69.167.74]
 22   214 ms   201 ms   201 ms  ae-115-3501.edge3.London15.Level3.net [4.69.167.74]
 23   565 ms   201 ms   201 ms  ae4.ar8.lon15.Level3.net [4.68.111.254]
 24   422 ms   436 ms   370 ms  roc1-ar5-xe-11-0-0-0.us.twtelecom.net [35.248.1.162]
 25   360 ms   407 ms   320 ms  66-195-65-170.static.ctl.one [66.195.65.170]
 26   368 ms   343 ms   401 ms  64.89.144.100
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.

C:\Users\priyavmehta>
```

Command Prompt

```
Microsoft Windows [Version 10.0.18362.959]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\priyavmehta>tracert www.hws.edu

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

  1   132 ms   436 ms   315 ms  192.168.43.1
  2     *        *        *     Request timed out.
  3   891 ms    47 ms   150 ms  10.71.5.29
  4    88 ms    81 ms   117 ms  192.168.70.217
  5   471 ms   202 ms   201 ms  192.168.70.216
  6     *        *        *     Request timed out.
  7   242 ms   252 ms   201 ms  172.25.50.7
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11   106 ms   166 ms   202 ms  103.198.140.174
 12   538 ms   203 ms   200 ms  103.198.140.45
 13   374 ms   368 ms   201 ms  103.198.140.56
 14   341 ms   201 ms   201 ms  103.198.140.107
 15   173 ms   147 ms   223 ms  103.198.140.45
 16   222 ms  1203 ms   444 ms  hu0-4-0-1.agr21.lhr01.atlas.cogentco.com [149.14.196.81]
 17   224 ms   228 ms   584 ms  be3672.ccr52.lhr01.atlas.cogentco.com [130.117.48.145]
 18   385 ms   406 ms   611 ms  be3488.ccr42.lon13.atlas.cogentco.com [154.54.60.13]
 19   207 ms   201 ms   420 ms  be2869.ccr22.lon01.atlas.cogentco.com [154.54.57.162]
 20     *        *        *     Request timed out.
 21   541 ms   406 ms   204 ms  ae-117-3503.edge3.London15.Level3.net [4.69.167.82]
 22   415 ms   406 ms   203 ms  ae-117-3503.edge3.London15.Level3.net [4.69.167.82]
 23   209 ms   236 ms   252 ms  ae4.ar8.lon15.Level3.net [4.68.111.254]
 24   468 ms   406 ms   406 ms  roc1-ar5-xe-11-0-0-0.us.twtelecom.net [35.248.1.162]
 25   415 ms   610 ms   611 ms  66-195-65-170.static.ctl.one [66.195.65.170]
 26   618 ms   611 ms   611 ms  64.89.144.100
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.

C:\Users\priyavmehta>
```

Command Prompt

```
Microsoft Windows [Version 10.0.18362.959]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\priyavmehta>tracert math.hws.edu

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

  1  1017 ms   426 ms   263 ms  192.168.43.1
  2     *        *        *     Request timed out.
  3   407 ms   511 ms   152 ms  10.71.5.13
  4   261 ms    97 ms   240 ms  192.168.70.221
  5   546 ms    69 ms   130 ms  192.168.70.216
  6     *        *        *     Request timed out.
  7   323 ms   201 ms   201 ms  172.25.50.7
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11   511 ms   240 ms   164 ms  103.198.140.58
 12   307 ms   611 ms   406 ms  103.198.140.45
 13   207 ms   202 ms   407 ms  103.198.140.56
 14   595 ms   260 ms   834 ms  103.198.140.107
 15   370 ms   201 ms   406 ms  103.198.140.45
 16   813 ms   410 ms   406 ms  hu0-4-0-1.agr21.lhr01.atlas.cogentco.com [149.14.196.81]
 17   617 ms   611 ms   201 ms  be3671.ccr51.lhr01.atlas.cogentco.com [130.117.48.137]
 18   212 ms   406 ms   611 ms  be3487.ccr41.lon13.atlas.cogentco.com [154.54.60.5]
 19   239 ms   171 ms   353 ms  be2868.ccr21.lon01.atlas.cogentco.com [154.54.57.154]
 20     *        *        *     Request timed out.
 21  1203 ms   780 ms   241 ms  ae-115-3501.edge3.London15.Level3.net [4.69.167.74]
 22   251 ms   407 ms   406 ms  ae-115-3501.edge3.London15.Level3.net [4.69.167.74]
 23   208 ms   201 ms   201 ms  ae4.ar8.lon15.Level3.net [4.68.111.254]
 24   408 ms   611 ms   816 ms  roc1-ar5-xe-11-0-0-0.us.twtelecom.net [35.248.1.162]
 25   411 ms   544 ms   677 ms  66-195-65-170.static.ctl.one [66.195.65.170]
 26   478 ms   406 ms   406 ms  64.89.144.100
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.

C:\Users\priyavmehta>
```

Some variations in paths and ip-addresses on different dates.

QUESTIONS ABOUT PATHS

Now look at the results you gathered and answer the following questions about the paths taken by your packets. Store your answers in a file named `traceroute.txt`.

1. Is any part of the path common for all hosts you tracerouted?

   Yes, the tracerouting follows a particular path from the user's IP address through the IP addresses of the ISP, the destination can be reached through different paths at different times.

2. Is there a relationship between the number of nodes that show up in the traceroute and the location of the host? If so, what is this relationship?

   There is no direct relationship between location and number of nodes. It depends on the physical interfaces as well. Sometimes larger the distance, larger the nodes, but not always true. Though the number of hops and number of machines/nodes have the following relationship.
   hops = machine - 1

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?

   Since the two hosts were of the same institution there were certain nodes that were common on running the tracert command. If the location of the host is farther away then generally it means more hops (more nodes/steps).

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

(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.

References :

1. https://smallbusiness.chron.com/wireless-lan-adapters-60680.html
2. https://en.wikipedia.org/wiki/IPv6_address#:~:text=An%20IPv6%20address%20is%20represented,0000%3A8a2e%3A0370%3A7334
3. https://docs.oracle.com/cd/E19253-01/816-4554/ipv6-config-tasks-102/index.html
4. https://www.cisco.com/c/en/us/support/docs/ip/ip-version-6-ipv6/113328-ipv6-lla.html
5. https://kstate.service-now.com/kb_view.do?sysparm_article=KB10532#:~:text=1)%20Click%20on%20Start%20%3E%20Accessories,connection%20information%20for%20the%20computer.
6. https://stackoverflow.com/questions/2043185/correlation-between-rtt-and-distance#:~:text=You%20mean%20physical%20distance%20in,travels%20at%20the%20light%20speed.
7. https://blog.stackpath.com/latency/
8. https://en.wikipedia.org/wiki/Transmission_time#:~:text=The%20round%2Dtrip%20time%20or,received%20at%20the%20same%20node.&text=Link%20roundtrip%20time%20%3D%202%20%C3%97,%C3%97%20propagation%20delay%20%2B%20processing%20delay
9. https://www.cloudflare.com/learning/cdn/glossary/round-trip-time-rtt/