Name: Rishita Mote
UID: 2018130029
Batch B

Aim:- Introduction to some basic network monitoring/analysis tools.

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.

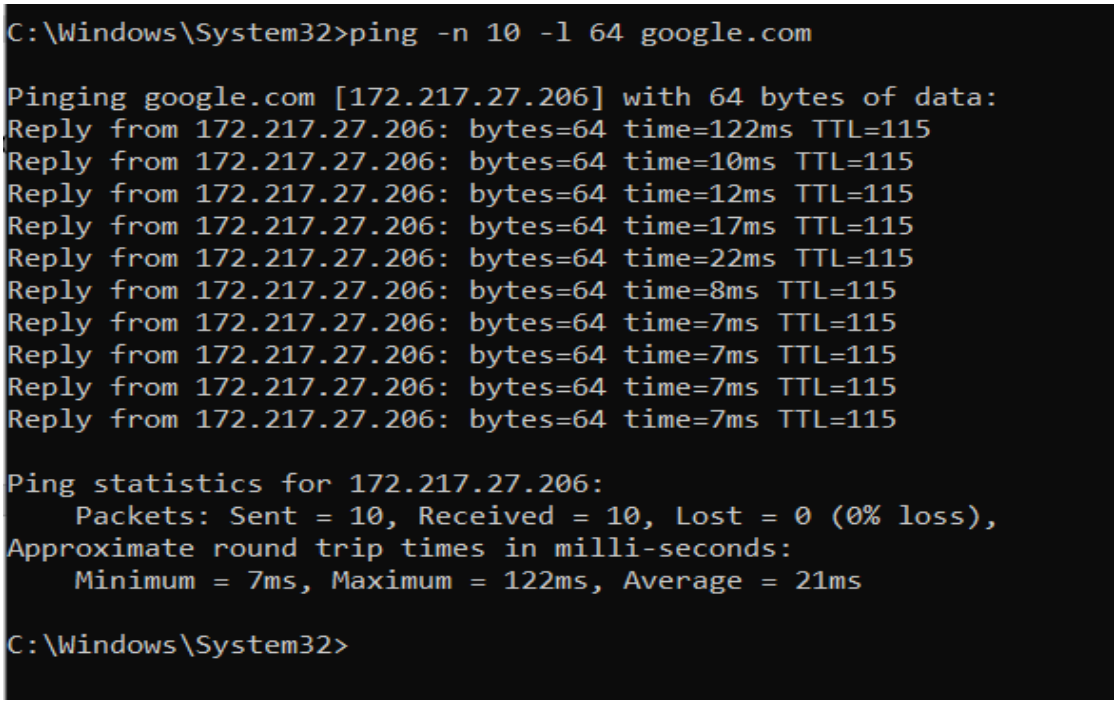
To save the output from ping to a file, include a greater than symbol and a file name at the end of the command. For example:

```
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

a) 64 bytes:



b) 100 bytes:

```
C:\Windows\System32>ping -n 10 -l 100 google.com

Pinging google.com [172.217.27.206] with 100 bytes of data:
Reply from 172.217.27.206: bytes=68 (sent 100) time=9ms TTL=115
Reply from 172.217.27.206: bytes=68 (sent 100) time=7ms TTL=115
Reply from 172.217.27.206: bytes=68 (sent 100) time=8ms TTL=115
Reply from 172.217.27.206: bytes=68 (sent 100) time=8ms TTL=115
Reply from 172.217.27.206: bytes=68 (sent 100) time=8ms TTL=115
Reply from 172.217.27.206: bytes=68 (sent 100) time=13ms TTL=115
Reply from 172.217.27.206: bytes=68 (sent 100) time=8ms TTL=115
Reply from 172.217.27.206: bytes=68 (sent 100) time=12ms TTL=115
Reply from 172.217.27.206: bytes=68 (sent 100) time=7ms TTL=115
Reply from 172.217.27.206: bytes=68 (sent 100) time=7ms TTL=115

Ping statistics for 172.217.27.206:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 13ms, Average = 8ms

C:\Windows\System32>
```

c) 500 Bytes:

```
C:\Windows\System32>ping -n 10 -l 500 google.com

Pinging google.com [172.217.27.206] with 500 bytes of data:
Reply from 172.217.27.206: bytes=68 (sent 500) time=55ms TTL=115
Reply from 172.217.27.206: bytes=68 (sent 500) time=60ms TTL=115
Reply from 172.217.27.206: bytes=68 (sent 500) time=7ms TTL=115
Reply from 172.217.27.206: bytes=68 (sent 500) time=8ms TTL=115
Reply from 172.217.27.206: bytes=68 (sent 500) time=14ms TTL=115
Reply from 172.217.27.206: bytes=68 (sent 500) time=16ms TTL=115
Reply from 172.217.27.206: bytes=68 (sent 500) time=8ms TTL=115
Reply from 172.217.27.206: bytes=68 (sent 500) time=8ms TTL=115
Reply from 172.217.27.206: bytes=68 (sent 500) time=8ms TTL=115
Reply from 172.217.27.206: bytes=68 (sent 500) time=9ms TTL=115

Ping statistics for 172.217.27.206:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 60ms, Average = 19ms
```

d) 1000 Bytes:

```
C:\Windows\System32>ping -n 10 -l 1000 google.com

Pinging google.com [172.217.27.206] with 1000 bytes of data:
Reply from 172.217.27.206: bytes=68 (sent 1000) time=10ms TTL=115
Reply from 172.217.27.206: bytes=68 (sent 1000) time=9ms TTL=115
Reply from 172.217.27.206: bytes=68 (sent 1000) time=8ms TTL=115
Reply from 172.217.27.206: bytes=68 (sent 1000) time=10ms TTL=115
Reply from 172.217.27.206: bytes=68 (sent 1000) time=101ms TTL=115
Reply from 172.217.27.206: bytes=68 (sent 1000) time=7ms TTL=115
Reply from 172.217.27.206: bytes=68 (sent 1000) time=7ms TTL=115
Reply from 172.217.27.206: bytes=68 (sent 1000) time=7ms TTL=115
Reply from 172.217.27.206: bytes=68 (sent 1000) time=8ms TTL=115
Reply from 172.217.27.206: bytes=68 (sent 1000) time=13ms TTL=115

Ping statistics for 172.217.27.206:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 101ms, Average = 18ms

C:\Windows\System32>
```

e) 1400 bytes:

```
C:\Windows\System32>ping -n 10 -l 1400 google.com

Pinging google.com [172.217.27.206] with 1400 bytes of data:
Reply from 172.217.27.206: bytes=68 (sent 1400) time=10ms TTL=115
Reply from 172.217.27.206: bytes=68 (sent 1400) time=9ms TTL=115
Reply from 172.217.27.206: bytes=68 (sent 1400) time=9ms TTL=115
Reply from 172.217.27.206: bytes=68 (sent 1400) time=20ms TTL=115
Reply from 172.217.27.206: bytes=68 (sent 1400) time=10ms TTL=115
Reply from 172.217.27.206: bytes=68 (sent 1400) time=7ms TTL=115
Reply from 172.217.27.206: bytes=68 (sent 1400) time=9ms TTL=115
Reply from 172.217.27.206: bytes=68 (sent 1400) time=9ms TTL=115
Reply from 172.217.27.206: bytes=68 (sent 1400) time=9ms TTL=115
Reply from 172.217.27.206: bytes=68 (sent 1400) time=7ms TTL=115

Ping statistics for 172.217.27.206:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 20ms, Average = 9ms

C:\Windows\System32>
```

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:

   1) Yes, the average RTT varies between different hosts.
   2) Propagation delay is the time taken by the last bit of the packet to reach the destination. It depends on distance and velocity. Since the distance will change depending on where the server of the hostname is located, hence RTT for different hosts will be affected by propagation delay.

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:

   1. Yes, RTT varies with different packet sizes.
   2. Transmission delay is the time taken to transmit a packet from the host to the transmission medium. It depends on packet size and bandwidth. Since we are using different packet sizes , RTT for different packet sizes will be affected by transmission delay.
   3. will be affected by queueing delay due to network congestion.

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).

Answer:

1) **uw.edu**

```
C:\Windows\System32>ping -n 4 -l 32 uw.edu

Pinging uw.edu [128.95.155.135] with 32 bytes of data:
Reply from 128.95.155.135: bytes=32 time=308ms TTL=45
Reply from 128.95.155.135: bytes=32 time=239ms TTL=45
Reply from 128.95.155.135: bytes=32 time=308ms TTL=45
Reply from 128.95.155.135: bytes=32 time=240ms TTL=45

Ping statistics for 128.95.155.135:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 239ms, Maximum = 308ms, Average = 273ms

C:\Windows\System32>
```

2) **Berkeley.edu:**

```
C:\Windows\System32>ping -n 4 -l 32 berkeley.edu

Pinging berkeley.edu [35.163.72.93] with 32 bytes of data:
Reply from 35.163.72.93: bytes=32 time=315ms TTL=36
Reply from 35.163.72.93: bytes=32 time=247ms TTL=36
Reply from 35.163.72.93: bytes=32 time=247ms TTL=36
Reply from 35.163.72.93: bytes=32 time=345ms TTL=36

Ping statistics for 35.163.72.93:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 247ms, Maximum = 345ms, Average = 288ms

C:\Windows\System32>
```

3) Uchicago.edu:

```
C:\Windows\System32>ping -n 4 -l 32 uchicago.edu

Pinging uchicago.edu [34.200.129.209] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 34.200.129.209:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Windows\System32>
```

4) Ox.ac.uk:

```
C:\Windows\System32>ping -n 4 -l 32 ox.ac.uk

Pinging ox.ac.uk [151.101.66.133] with 32 bytes of data:
Reply from 151.101.66.133: bytes=32 time=74ms TTL=55
Reply from 151.101.66.133: bytes=32 time=7ms TTL=55
Reply from 151.101.66.133: bytes=32 time=42ms TTL=55
Reply from 151.101.66.133: bytes=32 time=8ms TTL=55

Ping statistics for 151.101.66.133:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 74ms, Average = 32ms

C:\Windows\System32>
```

5) Yahoo.co.jp:

```
C:\Windows\System32>ping -n 4 -l 32 yahoo.co.jp

Pinging yahoo.co.jp [182.22.59.229] with 32 bytes of data:
Reply from 182.22.59.229: bytes=32 time=203ms TTL=42
Reply from 182.22.59.229: bytes=32 time=316ms TTL=42
Reply from 182.22.59.229: bytes=32 time=138ms TTL=42
Reply from 182.22.59.229: bytes=32 time=213ms TTL=42

Ping statistics for 182.22.59.229:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 138ms, Maximum = 316ms, Average = 217ms
```

Observations:

1) The RTT depends on the distance between the source and destination of the network requests.
2) The RTT is more for the universities located in US than UK because distance for US is more than UK from India.

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>

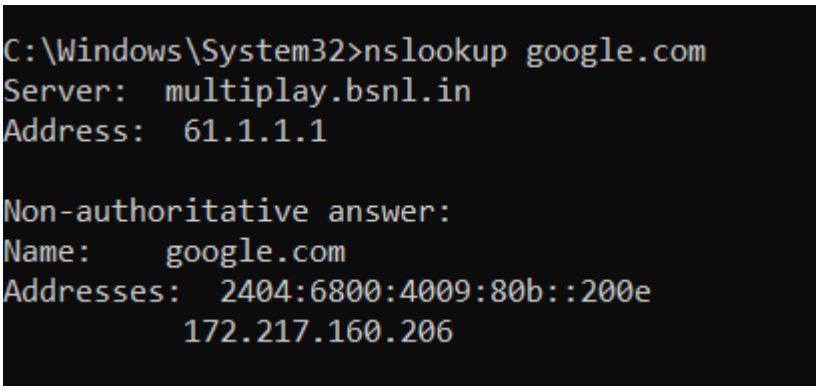
Answer:

1) Yahoo.com:

```
C:\Windows\System32>nslookup yahoo.com
Server:  multiplay.bsnl.in
Address:  61.1.1.1

Non-authoritative answer:
Name:    yahoo.com
Addresses:  2001:4998:124:1507::f000
          2001:4998:44:3507::8000
          2001:4998:124:1507::f001
          2001:4998:24:120d::1:1
          2001:4998:44:3507::8001
          2001:4998:24:120d::1:0
          74.6.143.26
          98.137.11.164
          74.6.143.25
          98.137.11.163
          74.6.231.21
          74.6.231.20
```

2) Google.com:



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!!!.)

```
C:\Windows\System32>ipconfig

Windows IP Configuration


Unknown adapter WSSVPNTap0901:

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

Ethernet adapter Ethernet:

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

Unknown adapter Local Area Connection 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* 10:

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

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::34fc:7e91:7221:8a50%13
   IPv4 Address. . . . . . . . . . . : 192.168.1.6
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Ethernet adapter Bluetooth Network Connection:

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

C:\Windows\System32>
```

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.)

```
C:\Windows\System32>netstat -t -n

Active Connections

  Proto  Local Address          Foreign Address        State           Offload State

  TCP    127.0.0.1:5939         127.0.0.1:58774        ESTABLISHED     InHost
  TCP    127.0.0.1:58774        127.0.0.1:5939         ESTABLISHED     InHost
  TCP    127.0.0.1:58793        127.0.0.1:58794        ESTABLISHED     InHost
  TCP    127.0.0.1:58794        127.0.0.1:58793        ESTABLISHED     InHost
  TCP    127.0.0.1:58829        127.0.0.1:58830        ESTABLISHED     InHost
  TCP    127.0.0.1:58830        127.0.0.1:58829        ESTABLISHED     InHost
  TCP    127.0.0.1:58834        127.0.0.1:58845        ESTABLISHED     InHost
  TCP    127.0.0.1:58845        127.0.0.1:58834        ESTABLISHED     InHost
  TCP    127.0.0.1:65434        127.0.0.1:65435        ESTABLISHED     InHost
  TCP    127.0.0.1:65435        127.0.0.1:65434        ESTABLISHED     InHost
  TCP    192.168.1.6:58769      169.38.74.8:80         ESTABLISHED     InHost
  TCP    192.168.1.6:58770      169.38.74.8:80         ESTABLISHED     InHost
  TCP    192.168.1.6:58778      52.139.250.253:443     ESTABLISHED     InHost
  TCP    192.168.1.6:58799      5.62.54.73:80          ESTABLISHED     InHost
  TCP    192.168.1.6:58808      52.139.250.253:443     ESTABLISHED     InHost
  TCP    192.168.1.6:58818      142.250.4.188:5228     ESTABLISHED     InHost
  TCP    192.168.1.6:59276      5.45.58.214:80         ESTABLISHED     InHost
  TCP    192.168.1.6:60711      52.11.231.199:443      ESTABLISHED     InHost
  TCP    192.168.1.6:60731      52.11.231.199:443      ESTABLISHED     InHost
  TCP    192.168.1.6:62631      52.97.186.98:443       ESTABLISHED     InHost
  TCP    192.168.1.6:63156      204.79.197.200:443     TIME_WAIT       InHost
  TCP    192.168.1.6:63158      40.100.141.162:443     TIME_WAIT       InHost
  TCP    192.168.1.6:63159      85.113.152.44:49160    ESTABLISHED     InHost
  TCP    192.168.1.6:63161      161.69.226.16:443      ESTABLISHED     InHost
  TCP    192.168.1.6:63166      204.79.197.222:443     TIME_WAIT       InHost
  TCP    192.168.1.6:63188      52.203.253.231:443     ESTABLISHED     InHost
  TCP    192.168.1.6:63208      37.153.12.146:21703    ESTABLISHED     InHost
  TCP    192.168.1.6:63212      204.79.197.200:443     ESTABLISHED     InHost
  TCP    192.168.1.6:63215      40.100.141.162:443     ESTABLISHED     InHost
  TCP    192.168.1.6:63218      220.161.5.50:8586      ESTABLISHED     InHost
  TCP    192.168.1.6:63219      13.107.246.254:443     ESTABLISHED     InHost
  TCP    192.168.1.6:63220      13.107.42.254:443      ESTABLISHED     InHost
  TCP    192.168.1.6:63221      13.107.4.254:443       ESTABLISHED     InHost
  TCP    192.168.1.6:63222      204.79.197.222:443     ESTABLISHED     InHost
  TCP    192.168.1.6:63234      51.116.232.21:443      ESTABLISHED     InHost
  TCP    192.168.1.6:63235      117.18.232.200:443     ESTABLISHED     InHost
  TCP    192.168.1.6:63249      51.15.232.45:6890      ESTABLISHED     InHost
  TCP    192.168.1.6:63254      159.69.121.155:6890    ESTABLISHED     InHost
  TCP    192.168.1.6:63258      183.87.198.127:6890    ESTABLISHED     InHost
  TCP    192.168.1.6:63260      45.123.161.155:59221   ESTABLISHED     InHost
  TCP    192.168.1.6:63261      45.249.72.166:63198    ESTABLISHED     InHost
  TCP    192.168.1.6:63264      40.90.22.192:443       ESTABLISHED     InHost
  TCP    192.168.1.6:63265      20.44.239.154:443      TIME_WAIT       InHost
```

```
  TCP    192.168.1.6:63222      204.79.197.222:443     ESTABLISHED     InHost
  TCP    192.168.1.6:63234      51.116.232.21:443      ESTABLISHED     InHost
  TCP    192.168.1.6:63235      117.18.232.200:443     ESTABLISHED     InHost
  TCP    192.168.1.6:63249      51.15.232.45:6890      ESTABLISHED     InHost
  TCP    192.168.1.6:63254      159.69.121.155:6890    ESTABLISHED     InHost
  TCP    192.168.1.6:63258      183.87.198.127:6890    ESTABLISHED     InHost
  TCP    192.168.1.6:63260      45.123.161.155:59221   ESTABLISHED     InHost
  TCP    192.168.1.6:63261      45.249.72.166:63198    ESTABLISHED     InHost
  TCP    192.168.1.6:63264      40.90.22.192:443       ESTABLISHED     InHost
  TCP    192.168.1.6:63265      20.44.239.154:443      TIME_WAIT       InHost
  TCP    192.168.1.6:63266      20.44.239.154:443      TIME_WAIT       InHost
  TCP    192.168.1.6:63267      20.44.239.154:443      TIME_WAIT       InHost
  TCP    192.168.1.6:63268      20.190.3.175:443       TIME_WAIT       InHost
  TCP    192.168.1.6:63271      45.249.73.238:16332    ESTABLISHED     InHost
  TCP    192.168.1.6:63272      52.114.7.36:443        TIME_WAIT       InHost
  TCP    192.168.1.6:63273      52.230.220.159:443     TIME_WAIT       InHost
  TCP    192.168.1.6:63274      183.87.197.5:54314     SYN_SENT        InHost
  TCP    192.168.1.6:63275      52.114.7.36:443        TIME_WAIT       InHost
  TCP    192.168.1.6:63276      111.221.29.40:443      ESTABLISHED     InHost

C:\Windows\System32>
```

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).

Answer:

1) **csail.mit.edu:**

```
C:\Windows\System32>tracert csail.mit.edu

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

  1    74 ms     1 ms     2 ms  192.168.1.1
  2     4 ms     8 ms     6 ms  117.212.240.1
  3     3 ms     2 ms     4 ms  218.248.164.97
  4    41 ms     3 ms     3 ms  218.248.164.114
  5     *        7 ms     7 ms  218.248.235.197
  6     6 ms     *        *     218.248.235.134
  7     5 ms     5 ms     5 ms  115.114.89.149.static-Mumbai.vsnl.net.in [115.114.89.149]
  8     6 ms     5 ms    10 ms  172.23.78.233
  9    10 ms    45 ms    10 ms  ix-ae-0-100.tcore1.mlv-mumbai.as6453.net [180.87.38.5]
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13   246 ms   276 ms   301 ms  if-ae-18-2.tcore1.nto-newyork.as6453.net [80.231.131.73]
 14   248 ms   309 ms   246 ms  if-ae-9-2.tcore1.n75-newyork.as6453.net [63.243.128.122]
 15   286 ms   250 ms   244 ms  66.110.96.150
 16   253 ms   384 ms   252 ms  be-10390-cr02.newyork.ny.ibone.comcast.net [68.86.83.89]
 17   278 ms   245 ms   245 ms  be-1402-cs04.newyork.ny.ibone.comcast.net [96.110.38.45]
 18   256 ms   364 ms   251 ms  96.110.42.14
 19   260 ms   341 ms   305 ms  ae0-0-eg-bstpmall74w.boston.ma.boston.comcast.net [68.86.238.34]
 20   247 ms   240 ms   241 ms  50-201-57-174-static.hfc.comcastbusiness.net [50.201.57.174]
 21   272 ms   248 ms   248 ms  dmz-rtr-1-external-rtr-3.mit.edu [18.0.161.13]
 22   256 ms   245 ms   290 ms  dmz-rtr-2-dmz-rtr-1-1.mit.edu [18.0.161.6]
 23   276 ms   253 ms   248 ms  mitnet.core-1-ext.csail.mit.edu [18.4.7.65]
 24     *        *        *     Request timed out.
 25   336 ms   255 ms   255 ms  bdr.core-1.csail.mit.edu [128.30.0.246]
 26   247 ms   253 ms   247 ms  inquir-3ld.csail.mit.edu [128.30.2.109]

Trace complete.
```

2) cs.stanfor.edu:

```
C:\Windows\System32>tracert cs.stanford.edu

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

  1    72 ms     1 ms     1 ms  192.168.1.1
  2     7 ms     4 ms     7 ms  117.212.240.1
  3     3 ms     3 ms     3 ms  218.248.164.97
  4     3 ms     5 ms     3 ms  218.248.164.114
  5     7 ms     8 ms     9 ms  218.248.235.197
  6     *        *        7 ms  218.248.235.198
  7     5 ms    40 ms    10 ms  115.114.89.149.static-Mumbai.vsnl.net.in [115.114.89.149]
  8     5 ms     6 ms     5 ms  172.23.78.233
  9    28 ms    28 ms    29 ms  172.31.244.45
 10    32 ms    31 ms    42 ms  ix-ae-4-2.tcore2.cxr-chennai.as6453.net [180.87.37.1]
 11   301 ms   266 ms   234 ms  if-ae-10-4.tcore2.svw-singapore.as6453.net [180.87.67.16]
 12   298 ms   257 ms   242 ms  if-ae-7-2.tcore2.lvw-losangeles.as6453.net [180.87.15.26]
 13   570 ms   286 ms   234 ms  if-ae-2-2.tcore1.lvw-losangeles.as6453.net [66.110.59.1]
 14   347 ms   258 ms   346 ms  las-b24-link.telia.net [80.239.128.214]
 15   262 ms   262 ms   262 ms  palo-b24-link.telia.net [62.115.119.90]
 16   284 ms   361 ms   263 ms  palo-b1-link.telia.net [62.115.122.169]
 17   248 ms   313 ms   304 ms  hurricane-ic-308019-palo-b1.c.telia.net [80.239.167.174]
 18   294 ms   271 ms   272 ms  stanford-university.100gigabitethernet5-1.core1.pao1.he.net [184.105.177.238]
 19   310 ms   241 ms   239 ms  csee-west-rtr-vl3.SUNet [171.66.255.140]
 20   253 ms   262 ms   272 ms  CS.stanford.edu [171.64.64.64]

Trace complete.
```

3) cs.manchester.ac.uk:

```
C:\Windows\System32>tracert cs.manchester.ac.uk

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

  1   292 ms     2 ms     1 ms  192.168.1.1
  2     4 ms     3 ms     2 ms  117.212.240.1
  3     2 ms     3 ms     2 ms  218.248.164.97
  4     5 ms     4 ms     7 ms  218.248.164.114
  5     *        *        6 ms  218.248.235.197
  6     *        *       17 ms  218.248.235.198
  7     5 ms     5 ms     5 ms  115.114.89.149.static-Mumbai.vsnl.net.in [115.114.89.149]
  8     7 ms     8 ms     6 ms  172.23.78.233
  9    10 ms     9 ms     9 ms  ix-ae-0-100.tcore1.mlv-mumbai.as6453.net [180.87.38.5]
 10     *        *      223 ms  if-ae-29-8.tcore1.wyn-marseille.as6453.net [80.231.217.110]
 11   161 ms   161 ms   240 ms  if-ae-21-2.tcore1.pye-paris.as6453.net [80.231.154.208]
 12   180 ms   166 ms   164 ms  if-ae-11-2.tcore1.pvu-paris.as6453.net [80.231.153.49]
 13     *        *      172 ms  80.231.153.66
 14     *        *      182 ms  ae-1-9.bear1.Manchesteruk1.Level3.net [4.69.167.38]
 15   176 ms   258 ms   210 ms  JANET.bear1.Manchester1.Level3.net [212.187.174.238]
 16   180 ms   251 ms   200 ms  ae22.manckh-sbr2.ja.net [146.97.35.189]
 17   183 ms   178 ms   178 ms  ae23.mancrh-rbr1.ja.net [146.97.38.42]
 18     *        *        *     Request timed out.
 19   249 ms   202 ms   177 ms  130.88.249.194
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22   184 ms   183 ms   198 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.

Answer:

The traceroute command, as the name implies, traces the route that packets takes to reach the host. It will show you how many hops it takes to reach the host and how long it took between each hop. This allows you to diagnose potential networking bottlenecks. [3]

a) For math.hws.edu:

```
C:\Windows\System32>tracert math.hws.edu

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

  1   308 ms     1 ms     1 ms  192.168.1.1
  2     7 ms     6 ms     7 ms  59.96.124.1
  3     4 ms     4 ms     3 ms  218.248.164.97
  4     3 ms     3 ms     5 ms  218.248.164.114
  5     6 ms     6 ms     6 ms  218.248.235.197
  6     *        *        *     Request timed out.
  7     5 ms     5 ms     6 ms  115.114.89.149.static-Mumbai.vsnl.net.in [115.114.89.149]
  8     *        7 ms     7 ms  172.23.78.233
  9     8 ms     7 ms     7 ms  ix-ae-0-100.tcore1.mlv-mumbai.as6453.net [180.87.38.5]
 10     *      132 ms     *     if-ae-5-2.tcore1.wyn-marseille.as6453.net [80.231.217.29]
 11   128 ms   130 ms   131 ms  if-ae-8-1600.tcore1.pye-paris.as6453.net [80.231.217.6]
 12   130 ms   130 ms   130 ms  if-ae-11-2.tcore1.pvu-paris.as6453.net [80.231.153.49]
 13     *        *      245 ms  80.231.153.66
 14   264 ms   232 ms   228 ms  ae-2-3204.edge3.Paris1.Level3.net [4.69.161.114]
 15   251 ms   263 ms   258 ms  global-crossing-xe-level3.paris1.level3.net [4.68.63.230]
 16   277 ms   276 ms   267 ms  roc1-ar5-xe-11-0-0-0.us.twtelecom.net [35.248.1.162]
 17   352 ms   260 ms   261 ms  66-195-65-170.static.ctl.one [66.195.65.170]
 18   269 ms   253 ms   252 ms  64.89.144.100
 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.
```

b) For www.hws.edu :

```
C:\Windows\System32>tracert www.hws.edu

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

  1   344 ms     2 ms     1 ms  192.168.1.1
  2     9 ms     5 ms     7 ms  59.96.124.1
  3     6 ms     6 ms     5 ms  218.248.164.97
  4     7 ms     3 ms     5 ms  218.248.164.114
  5     *        *        *     Request timed out.
  6     *       11 ms     *     218.248.235.198
  7     5 ms     5 ms     6 ms  115.114.89.149.static-Mumbai.vsnl.net.in [115.114.89.149]
  8     7 ms     6 ms     5 ms  172.23.78.233
  9     7 ms     7 ms     6 ms  ix-ae-0-100.tcore1.mlv-mumbai.as6453.net [180.87.38.5]
 10   130 ms   129 ms   129 ms  if-ae-5-2.tcore1.wyn-marseille.as6453.net [80.231.217.29]
 11     *        *        *     Request timed out.
 12   131 ms   130 ms   129 ms  if-ae-11-2.tcore1.pvu-paris.as6453.net [80.231.153.49]
 13     *        *        *     Request timed out.
 14   271 ms   265 ms   265 ms  ae-2-3204.edge3.Paris1.Level3.net [4.69.161.114]
 15   251 ms   259 ms   255 ms  global-crossing-xe-level3.paris1.level3.net [4.68.63.230]
 16   293 ms   281 ms   266 ms  roc1-ar5-xe-11-0-0-0.us.twtelecom.net [35.248.1.162]
 17   299 ms   297 ms   274 ms  66-195-65-170.static.ctl.one [66.195.65.170]
 18   299 ms   290 ms   260 ms  64.89.144.100
 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.
```

Observation: In math.hws.edu at 6th hop, request timed out but in www.hws.edu at 6th Hop it is 218.248.235.164.114.

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.

Answer: For cs.manchester.ac.uk:

```
C:\Windows\System32>tracert cs.manchester.ac.uk

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

  1   288 ms     3 ms     1 ms  192.168.1.1
  2     3 ms     5 ms     4 ms  59.96.124.1
  3     9 ms     5 ms    10 ms  218.248.164.97
  4     7 ms     7 ms     9 ms  218.248.164.122
  5     9 ms     *        *     218.248.235.133
  6     *        *        *     Request timed out.
  7    15 ms     6 ms     5 ms  115.114.89.149.static-Mumbai.vsnl.net.in [115.114.89.149]
  8     5 ms     5 ms     5 ms  172.23.78.233
  9     8 ms     7 ms     7 ms  ix-ae-0-100.tcore1.mlv-mumbai.as6453.net [180.87.38.5]
 10     *        *      134 ms  if-ae-5-2.tcore1.wyn-marseille.as6453.net [80.231.217.29]
 11   130 ms   129 ms   129 ms  if-ae-21-2.tcore1.pye-paris.as6453.net [80.231.154.208]
 12   135 ms   130 ms   130 ms  if-ae-11-2.tcore1.pvu-paris.as6453.net [80.231.153.49]
 13     *      280 ms   272 ms  80.231.153.66
 14     *        *        *     Request timed out.
 15   252 ms   230 ms   225 ms  212.187.174.238
 16   287 ms   290 ms   289 ms  ae22.manckh-sbr2.ja.net [146.97.35.189]
 17   250 ms   253 ms   242 ms  ae23.mancrh-rbr1.ja.net [146.97.38.42]
 18     *      274 ms     *     universityofmanchester.ja.net [146.97.169.2]
 19   286 ms   273 ms   278 ms  130.88.249.194
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22   290 ms   275 ms   249 ms  eps.its.man.ac.uk [130.88.101.49]

Trace complete.
```

```
C:\Windows\System32>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  192.168.1.1
  2     6 ms     4 ms     4 ms  59.96.124.1
  3     6 ms     6 ms     6 ms  218.248.164.97
  4     4 ms     4 ms     3 ms  218.248.164.122
  5     *        6 ms     *     218.248.235.197
  6     *        7 ms     *     218.248.235.134
  7     8 ms     6 ms     5 ms  115.114.89.149.static-Mumbai.vsnl.net.in [115.114.89.149]
  8    10 ms     9 ms     8 ms  172.23.78.233
  9     6 ms     7 ms     7 ms  ix-ae-0-100.tcore1.mlv-mumbai.as6453.net [180.87.38.5]
 10   129 ms   129 ms   130 ms  if-ae-5-2.tcore1.wyn-marseille.as6453.net [80.231.217.29]
 11     *      133 ms   130 ms  if-ae-21-2.tcore1.pye-paris.as6453.net [80.231.154.208]
 12   129 ms   131 ms   130 ms  if-ae-11-2.tcore1.pvu-paris.as6453.net [80.231.153.49]
 13     *        *      253 ms  80.231.153.66
 14     *        *        *     Request timed out.
 15   271 ms   265 ms   272 ms  JANET.bear1.Manchester1.Level3.net [212.187.174.238]
 16   266 ms   281 ms   290 ms  ae22.manckh-sbr2.ja.net [146.97.35.189]
 17   255 ms   277 ms   262 ms  ae23.mancrh-rbr1.ja.net [146.97.38.42]
 18     *        *        *     Request timed out.
 19   263 ms   289 ms   291 ms  130.88.249.194
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22   345 ms   329 ms   244 ms  eps.its.man.ac.uk [130.88.101.49]

Trace complete.
```

Observation: At 6th hop the second case the path is 218.228.235.197 whereas the first case it was Request Timed Out.

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: No, no part of the path is common.

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, there is no relation between the number of nodes that show up in the traceroute and the location of the host

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 can be propagation delay because of more number of nodes.

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.)

I used the command nslookup spit.ac.in. This gave me the outside IP address on my home computer.

```
C:\Windows\System32>nslookup spit.ac.in
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  61.1.1.1

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

```
C:\Windows\System32>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"
}
C:\Windows\System32>
```

CONCLUSION:

1) In this experiment, learned about the basic network utilities such as ping, traceroute, ipconfig, etc.
2) I learned about their implementation and variation in them depending upon different factors such as distance, packet size, etc.