Name : TrushaTalati
UID: 2018130054
Batch : D

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

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

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

Some Basic command line Networking utilities

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

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

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

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

The syntax in Windows
is:

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

The default number of ICMP packets to send is either infinite (in Linux and Mac OS) or 4 (in Windows). The default packet size is either 64 bytes (in Linux) or 32 bytes (in Windows). You can specify either a hostname (e.g., spit.ac.in) or an IP address.
To save the output from ping to a file, include a greater than symbol and a file name at the end of the command. For example:

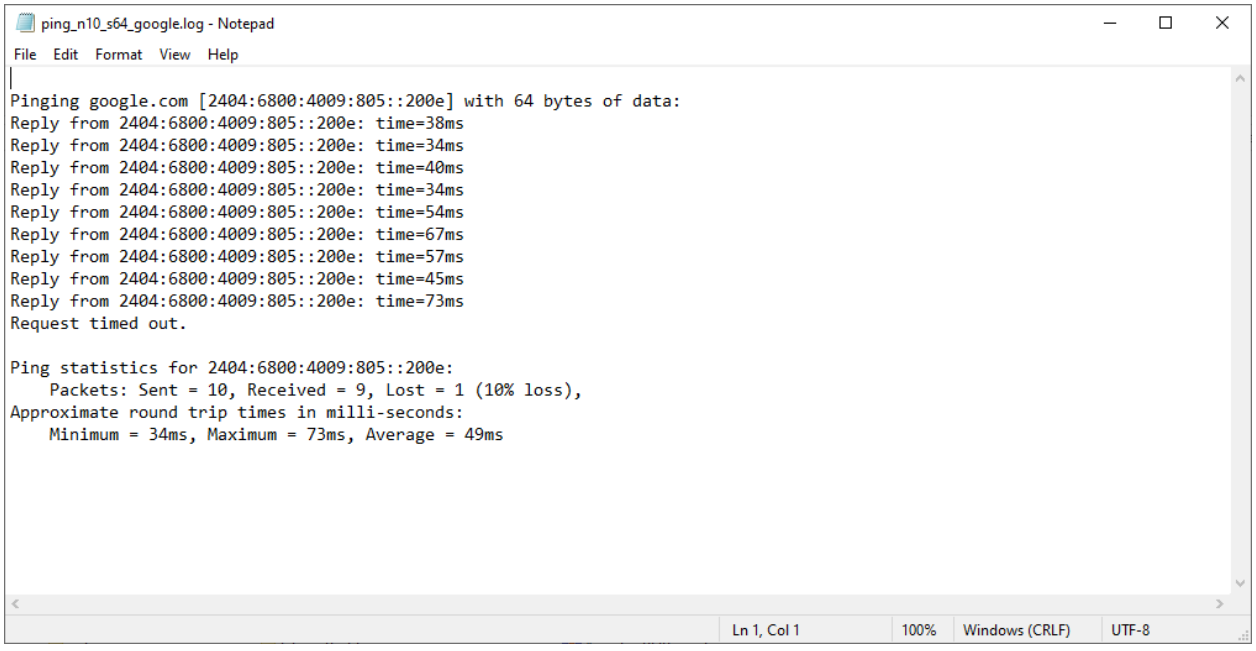
ping -c 10 google.com > ping_c10_s64_google.log

EXPERIMENTS WITH PING

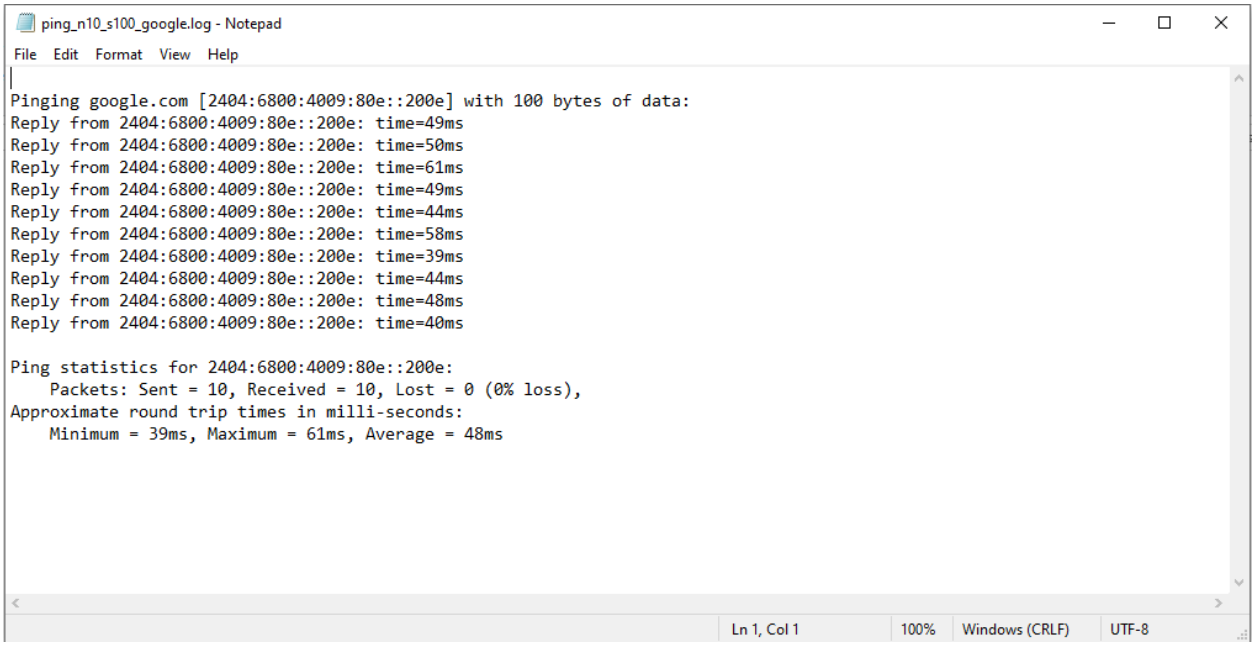
1. Ping the any hosts 10 times (i.e., packet count is 10) with a packet size of 64 bytes, 100 bytes, 500 bytes, 1000 bytes, 1400 bytes

Output:

RTT (avg) = 49ms

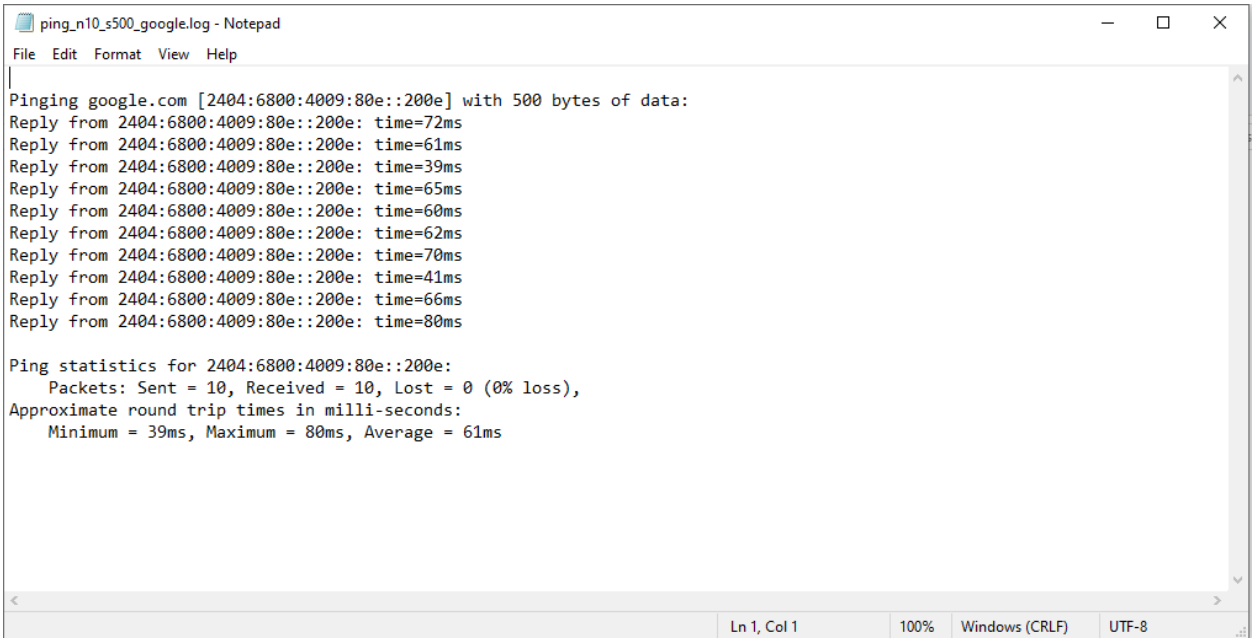


2.



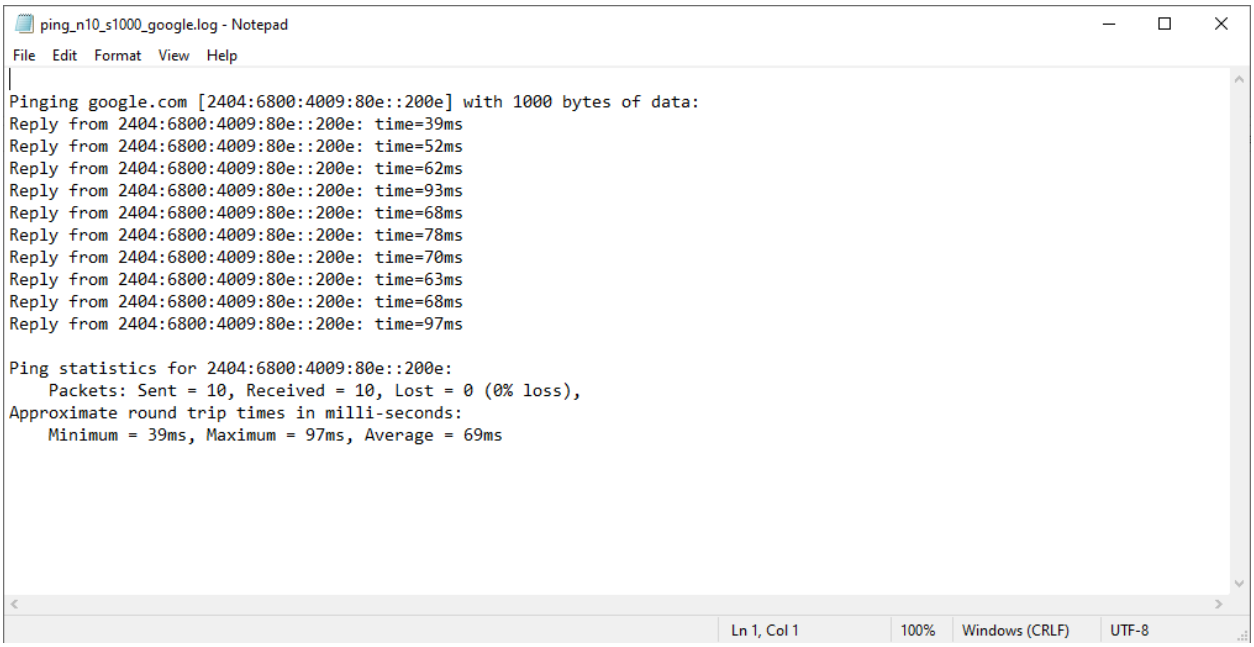
RTT (avg) = 48ms

3.



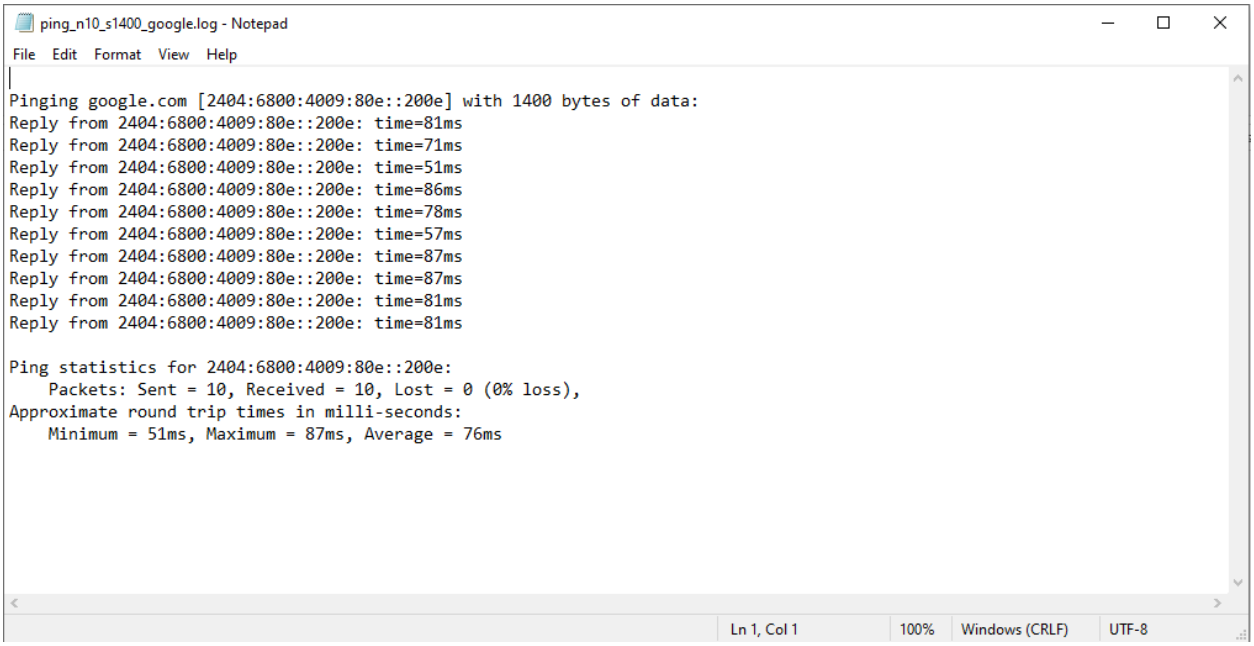
RTT (avg) = 61ms

4 .



RTT (avg) = 69ms

5 .



RTT(avg) = 76ms

Observations : 1 .Server may be different for different packet sizes.
2. It seems RTT seems to be increasing with increase in packet size when pinged to the same IP address .

Q UESTIONS A BOUT L ATENCY 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 :-

Round-trip time (RTT) is the duration, measured in milliseconds, from when a browser sends a request to when it receives a response from a server.

Latency = Propagation + Transmit + Queue

Transmission Delay :

Time taken to put a packet onto the link. In other words, it is simply time required to put data bits on the wire/communication medium. It depends on the length of the packet and the bandwidth of the network.

Transmit = Size/Bandwidth

Propagation delay :

Time taken by the first bit to travel from sender to receiver end of the link. In other words, it is simply the time required for bits to reach the destination from the start point. Factors on which Propagation delay depends are Distance and propagation speed.

Propagation = Distance/SpeedOfLight

Queuing Delay :

Queuing delay is the time a job waits in a queue until it can be executed. It depends on congestion. It is the time difference between when the packet arrived Destination and when the packet data was processed or executed. It may be caused by mainly three reasons i.e. originating switches, intermediate switches or call receiver servicing switches.
Average Queuing delay = (N-1)L/(2*R)
where N = no. of packets
L=size of packet
R=bandwidth

Processing Delay :

Processing delay is the time it takes routers to process the packet header. Processing of packets helps in detecting bit-level errors that occur during transmission of a packet to the destination. Processing delays in high-speed routers are typically on the order of microseconds or less.In simple words, it is just the time taken to process packets.

So yes , Average RTT does vary between different hosts due to queuing delay as we can see.This can mostly be due to propagation Delay as it depends on distance and due to Queuing delay as the packet may be in a queue . Thus various aspects of latency contribute to rtt being varied between hosts .

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 varies with different packet sizes even if we ping to the same host. This is because of the **Transmission delay** and the **Queueing delay** which depend on the size of the packets as explained above .

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).

Output : -

```
C:\Users\trusha>ping www.uw.edu

Pinging www.washington.edu [128.95.155.134] with 32 bytes of data:
Reply from 128.95.155.134: bytes=32 time=386ms TTL=43
Reply from 128.95.155.134: bytes=32 time=335ms TTL=43
Reply from 128.95.155.134: bytes=32 time=644ms TTL=43
Reply from 128.95.155.134: bytes=32 time=562ms TTL=43

Ping statistics for 128.95.155.134:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 335ms, Maximum = 644ms, Average = 481ms

C:\Users\trusha>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\trusha>ping 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=378ms TTL=36
Reply from 35.163.72.93: bytes=32 time=657ms TTL=36
Reply from 35.163.72.93: bytes=32 time=596ms 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 = 315ms, Maximum = 657ms, Average = 486ms
```

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

Pinging wsee2.elb.uchicago.edu [34.225.113.202] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 34.225.113.202:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\trusha>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=38ms TTL=52
Reply from 151.101.194.133: bytes=32 time=92ms TTL=52
Reply from 151.101.194.133: bytes=32 time=56ms TTL=52
Reply from 151.101.194.133: bytes=32 time=39ms TTL=52

Ping statistics for 151.101.194.133:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 38ms, Maximum = 92ms, Average = 56ms

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

Observation :

Factors affecting RTT :

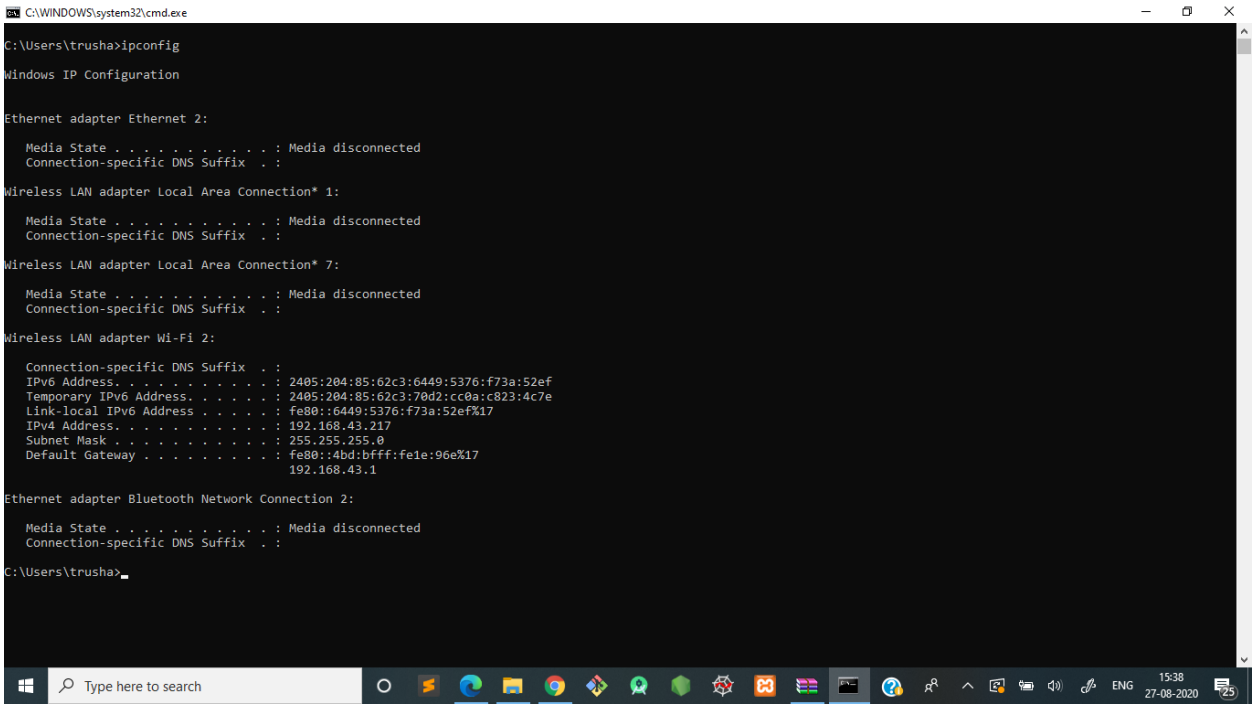
● **Distance** – The length a signal has to travel correlates with the time taken for a request to reach a server and a response to reach a browser.

● **Transmission medium** – The medium used to route a signal (e.g., copper wire, fiber optic cables) can impact how quickly a request is received by a server and routed back to a user.

● **Server response time** – The time taken for a target server to respond to a request depends on its processing capacity, the number of requests being handled and the nature of the request (i.e., how much server-side work is required). A longer server response time increases RTT

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

ifconfig — You used ifconfig in the previous lab. When used with no parameters, ifconfig reports some information about the computer's network interfaces. This usually includes lo which stands for localhost; it can be used for communication between programs running on the same computer. Linux often has an interface named eth0, which is the first ethernet card. The information is different on Mac OS and Linux, but includes the IP or "inet" address and ethernet or "hardware" address for an ethernet card. On Linux, you get the number of packets received (RX) and sent (TX), as well as the number of bytes transmitted and received. (A better place to monitor network bytes on our Linux computers is in the GUI program System Monitor, if it is installed!!!.)



Windows :-

Displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. Used without parameters, ipconfig displays Internet Protocol version 4 (IPv4) and IPv6 addresses, subnet mask, and default gateway for all adapters.

- This command is most useful on computers that are configured to obtain an IP address automatically. This enables users to determine which TCP/IP configuration values have been configured by DHCP, Automatic Private IP Addressing (APIPA), or an alternate configuration.
- If the name you supply for *adapter* contains any spaces, use quotation marks around the adapter name (for example, "adapter name").
- For adapter names, ipconfig supports the use of the asterisk (*) wildcard character to specify either adapters with names that begin with a specified string or adapters with names that contain a specified string. For example, Local* matches all adapters that start with the string Local and *Con* matches all adapters that contain the string Con.

Some parameters :

/all Displays the full TCP/IP configuration for all adapters. Adapters can represent physical interfaces, such as installed network adapters, or logical interfaces, such as dial-up connections.

/displaydns Displays the contents of the DNS client resolver cache, which includes both entries preloaded from the local Hosts file and any recently obtained resource records for name queries resolved by the computer. The DNS Client service uses this information to resolve frequently queried names quickly, before querying its configured DNS servers.

/flushdns Flushes and resets the contents of the DNS client resolver cache. During DNS troubleshooting, you can use this procedure to discard negative cache entries from the cache, as well as any other entries that have been added dynamically.

/registerdns Initiates manual dynamic registration for the DNS names and IP addresses that are configured at a computer. You can use this parameter to troubleshoot a failed DNS name registration or resolve a dynamic update problem between a client and the DNS server without rebooting the client computer. The DNS settings in the advanced properties of the TCP/IP protocol determine which names are registered in DNS.

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.k

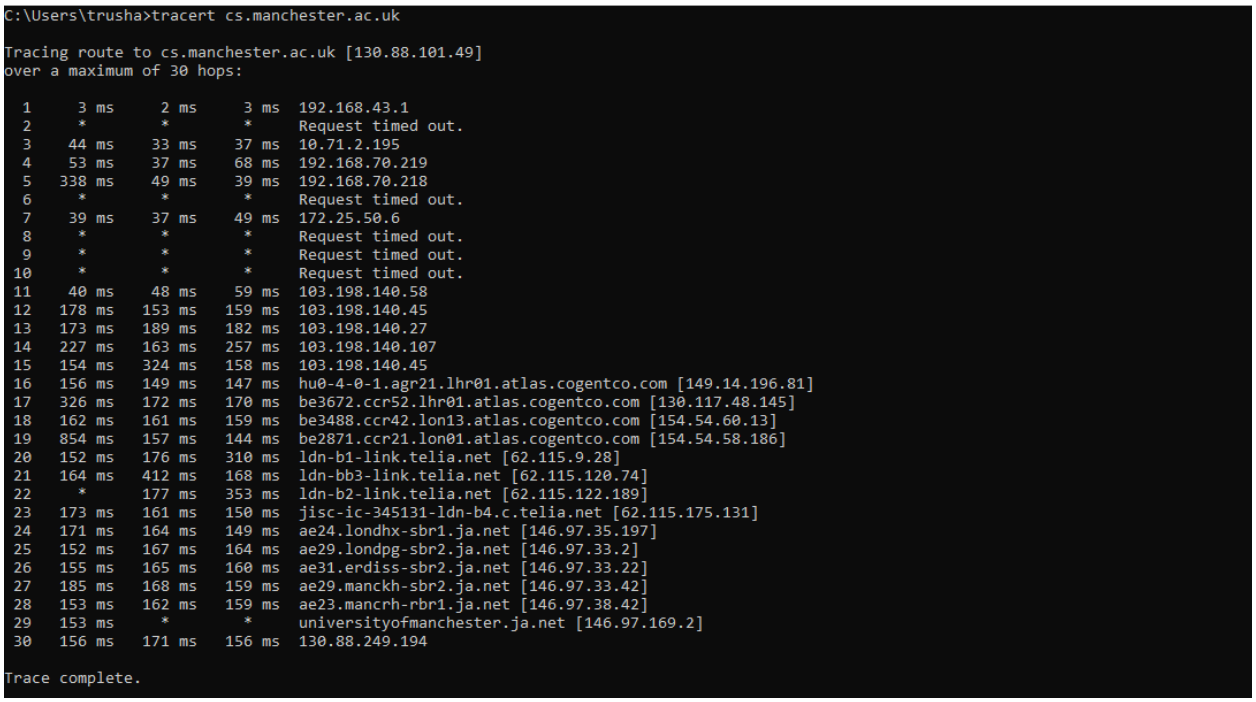
Store the output of each traceroute command in a separate file named traceroute_HOSTNAME.log , replacing HOSTNAME with the hostname for end-host you pinged (e.g., traceroute_ee.iitb.ac.in.log).

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

  1   146 ms     4 ms     4 ms  192.168.43.1
  2     *        *        *     Request timed out.
  3   593 ms   203 ms    96 ms  10.71.2.210
  4   128 ms    81 ms    99 ms  192.168.70.215
  5   320 ms   123 ms    76 ms  192.168.70.218
  6     *        *        *     Request timed out.
  7    83 ms    99 ms    98 ms  172.25.50.6
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11   152 ms   100 ms   166 ms  103.198.140.58
 12   176 ms   203 ms   216 ms  103.198.140.56
 13   148 ms   994 ms   197 ms  103.198.140.56
 14   315 ms   139 ms   164 ms  hurricane.mrs.franceix.net [37.49.232.13]
 15   197 ms   285 ms   200 ms  100ge4-2.core1.par2.he.net [184.105.222.21]
 16   413 ms   307 ms   408 ms  100ge14-1.core1.nyc4.he.net [184.105.81.77]
 17     *        *        *     Request timed out.
 18   510 ms   589 ms   534 ms  100ge14-2.core1.msp1.he.net [184.105.223.178]
 19     *      544 ms   403 ms  aureon-network-services-inc.e0-26.switch1.msp1.he.net [216.66.77.218]
 20   396 ms     *      444 ms  peer-as5056.br02.msp1.tfbnw.net [157.240.76.37]
 21   427 ms   332 ms   508 ms  167.142.58.40
 22   553 ms   313 ms   256 ms  167.142.219.32
 23   279 ms   533 ms   317 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.
```

```
C:\Users\trusha>tracert mscs.mu.edu

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

  1    13 ms   164 ms     4 ms  192.168.43.1
  2     *        *        *     Request timed out.
  3   710 ms   100 ms   101 ms  10.71.2.195
  4   404 ms   223 ms   101 ms  192.168.70.221
  5   214 ms   304 ms   101 ms  192.168.70.216
  6     *        *        *     Request timed out.
  7   133 ms    99 ms    98 ms  172.25.50.6
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11    79 ms    45 ms    77 ms  103.198.140.58
 12   197 ms   199 ms   201 ms  103.198.140.27
 13   418 ms   308 ms   239 ms  103.198.140.27
 14   212 ms   201 ms   201 ms  hurricane.mrs.franceix.net [37.49.232.13]
 15   212 ms   204 ms   197 ms  100ge4-2.core1.par2.he.net [184.105.222.21]
 16     *        *      308 ms  100ge14-1.core1.nyc4.he.net [184.105.81.77]
 17   415 ms     *      339 ms  100ge2-1.core2.chi1.he.net [184.104.193.173]
 18     *        *        *     Request timed out.
 19   554 ms   505 ms   421 ms  r-222wwash-isp-ae6-3926.wiscnet.net [140.189.8.126]
 20   276 ms   380 ms   996 ms  r-milwaukeeci-809-isp-ae3-0.wiscnet.net [140.189.8.230]
 21   366 ms   251 ms   308 ms  MarquetteUniv.site.wiscnet.net [216.56.1.202]
 22   415 ms   305 ms   291 ms  134.48.10.27
 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\trusha>tracert csail.mit.edu

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

  1    73 ms     4 ms     4 ms  192.168.43.1
  2     *        *        *     Request timed out.
  3   145 ms    98 ms    99 ms  10.71.2.195
  4   102 ms    53 ms    44 ms  192.168.70.219
  5   157 ms   263 ms   317 ms  192.168.70.218
  6     *        *        *     Request timed out.
  7   118 ms    99 ms    99 ms  172.25.50.6
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15   366 ms   307 ms   268 ms  49.45.4.86
 16   292 ms   309 ms   356 ms  4.7.26.61
 17   457 ms     *        *     ae-2-3.bear1.Boston1.Level3.net [4.69.159.249]
 18   435 ms   371 ms   343 ms  MASSACHUSET.bear1.Boston1.Level3.net [4.53.48.98]
 19   380 ms   508 ms   357 ms  dmz-rtr-1-external-rtr-1.mit.edu [18.0.161.17]
 20   350 ms   443 ms   461 ms  dmz-rtr-2-dmz-rtr-1-2.mit.edu [18.0.162.6]
 21   347 ms   640 ms   840 ms  mitnet.core-1-ext.csail.mit.edu [18.4.7.65]
 22     *        *        *     Request timed out.
 23   556 ms   615 ms   713 ms  bdr.core-1.csail.mit.edu [128.30.0.246]
 24   416 ms   510 ms   714 ms  inquir-3ld.csail.mit.edu [128.30.2.109]

Trace complete.
```

```
C:\Users\trusha>tracert cs.stanford.edu

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

  1     7 ms     4 ms     4 ms  192.168.43.1
  2     *        *        *     Request timed out.
  3   138 ms   201 ms   173 ms  10.71.2.211
  4   190 ms   133 ms   101 ms  192.168.70.215
  5   228 ms    82 ms   197 ms  192.168.70.218
  6     *        *        *     Request timed out.
  7   130 ms    98 ms    99 ms  172.25.50.6
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11    38 ms    46 ms    55 ms  103.198.140.58
 12   172 ms   144 ms   151 ms  103.198.140.56
 13   143 ms   141 ms   141 ms  103.198.140.56
 14   152 ms   130 ms   142 ms  hurricane.mrs.franceix.net [37.49.232.13]
 15   200 ms   328 ms   316 ms  100ge4-2.core1.par2.he.net [184.105.222.21]
 16   260 ms   327 ms   236 ms  100ge10-2.core1.ash1.he.net [184.105.213.173]
 17   292 ms   546 ms   307 ms  100ge7-2.core1.pao1.he.net [184.105.222.41]
 18   303 ms   298 ms   291 ms  stanford-university.100gigabitethernet5-1.core1.pao1.he.net [184.105.177.238]
 19   360 ms   316 ms   279 ms  csee-west-rtr-vl3.SUNet [171.66.255.140]
 20   571 ms   316 ms   316 ms  CS.stanford.edu [171.64.64.64]

Trace complete.
```



```
C:\Users\trusha>tracert cs.manchester.ac.uk

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

  1     3 ms     2 ms     3 ms  192.168.43.1
  2     *        *        *     Request timed out.
  3    44 ms    33 ms    37 ms  10.71.2.195
  4    53 ms    37 ms    68 ms  192.168.70.219
  5   338 ms    49 ms    39 ms  192.168.70.218
  6     *        *        *     Request timed out.
  7    39 ms    37 ms    49 ms  172.25.50.6
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11    40 ms    48 ms    59 ms  103.198.140.58
 12   178 ms   153 ms   159 ms  103.198.140.45
 13   173 ms   189 ms   182 ms  103.198.140.27
 14   227 ms   163 ms   257 ms  103.198.140.107
 15   154 ms   324 ms   158 ms  103.198.140.45
 16   156 ms   149 ms   147 ms  hu0-4-0-1.agr21.lhr01.atlas.cogentco.com [149.14.196.81]
 17   326 ms   172 ms   170 ms  be3672.ccr52.lhr01.atlas.cogentco.com [130.117.48.145]
 18   162 ms   161 ms   159 ms  be3488.ccr42.lon13.atlas.cogentco.com [154.54.60.13]
 19   854 ms   157 ms   144 ms  be2871.ccr21.lon01.atlas.cogentco.com [154.54.58.186]
 20   152 ms   176 ms   310 ms  ldn-b1-link.telia.net [62.115.9.28]
 21   164 ms   412 ms   168 ms  ldn-bb3-link.telia.net [62.115.120.74]
 22     *      177 ms   353 ms  ldn-b2-link.telia.net [62.115.122.189]
 23   173 ms   161 ms   150 ms  jisc-ic-345131-ldn-b4.c.telia.net [62.115.175.131]
 24   171 ms   164 ms   149 ms  ae24.londhx-sbr1.ja.net [146.97.35.197]
 25   152 ms   167 ms   164 ms  ae29.londpg-sbr2.ja.net [146.97.33.2]
 26   155 ms   165 ms   160 ms  ae31.erdiss-sbr2.ja.net [146.97.33.22]
 27   185 ms   168 ms   159 ms  ae29.manckh-sbr2.ja.net [146.97.33.42]
 28   153 ms   162 ms   159 ms  ae23.mancrh-rbr1.ja.net [146.97.38.42]
 29   153 ms     *        *     universityofmanchester.ja.net [146.97.169.2]
 30   156 ms   171 ms   156 ms  130.88.249.194

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.

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

  1   282 ms     5 ms     4 ms  192.168.43.1
  2     *        *        *     Request timed out.
  3   462 ms    99 ms   201 ms  10.71.2.195
  4    82 ms   474 ms   715 ms  192.168.70.215
  5   106 ms    99 ms    99 ms  192.168.70.218
  6     *        *        *     Request timed out.
  7   155 ms   303 ms   627 ms  172.25.50.6
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11    53 ms    79 ms    98 ms  103.198.140.58
 12   195 ms   202 ms   201 ms  103.198.140.45
 13   413 ms   303 ms   303 ms  103.198.140.56
 14   303 ms   203 ms   300 ms  103.198.140.107
 15   272 ms   303 ms   201 ms  103.198.140.45
 16   217 ms   176 ms   275 ms  hu0-4-0-1.agr21.lhr01.atlas.cogentco.com [149.14.196.81]
 17   170 ms   280 ms   199 ms  be3672.ccr52.lhr01.atlas.cogentco.com [130.117.48.145]
 18   175 ms   167 ms   167 ms  be3488.ccr42.lon13.atlas.cogentco.com [154.54.60.13]
 19   189 ms   170 ms   401 ms  be2869.ccr22.lon01.atlas.cogentco.com [154.54.57.162]
 20     *        *        *     Request timed out.
 21   380 ms   351 ms   262 ms  ae-116-3502.edge3.London15.Level3.net [4.69.167.78]
 22   264 ms   197 ms   201 ms  ae-116-3502.edge3.London15.Level3.net [4.69.167.78]
 23   330 ms   180 ms   201 ms  ae4.ar8.lon15.Level3.net [4.68.111.254]
 24   376 ms   343 ms   308 ms  roc1-ar5-xe-11-0-0-0.us.twtelecom.net [35.248.1.162]
 25   493 ms   357 ms   455 ms  66-195-65-170.static.ctl.one [66.195.65.170]
 26   356 ms   304 ms   508 ms  64.89.144.100
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.
```

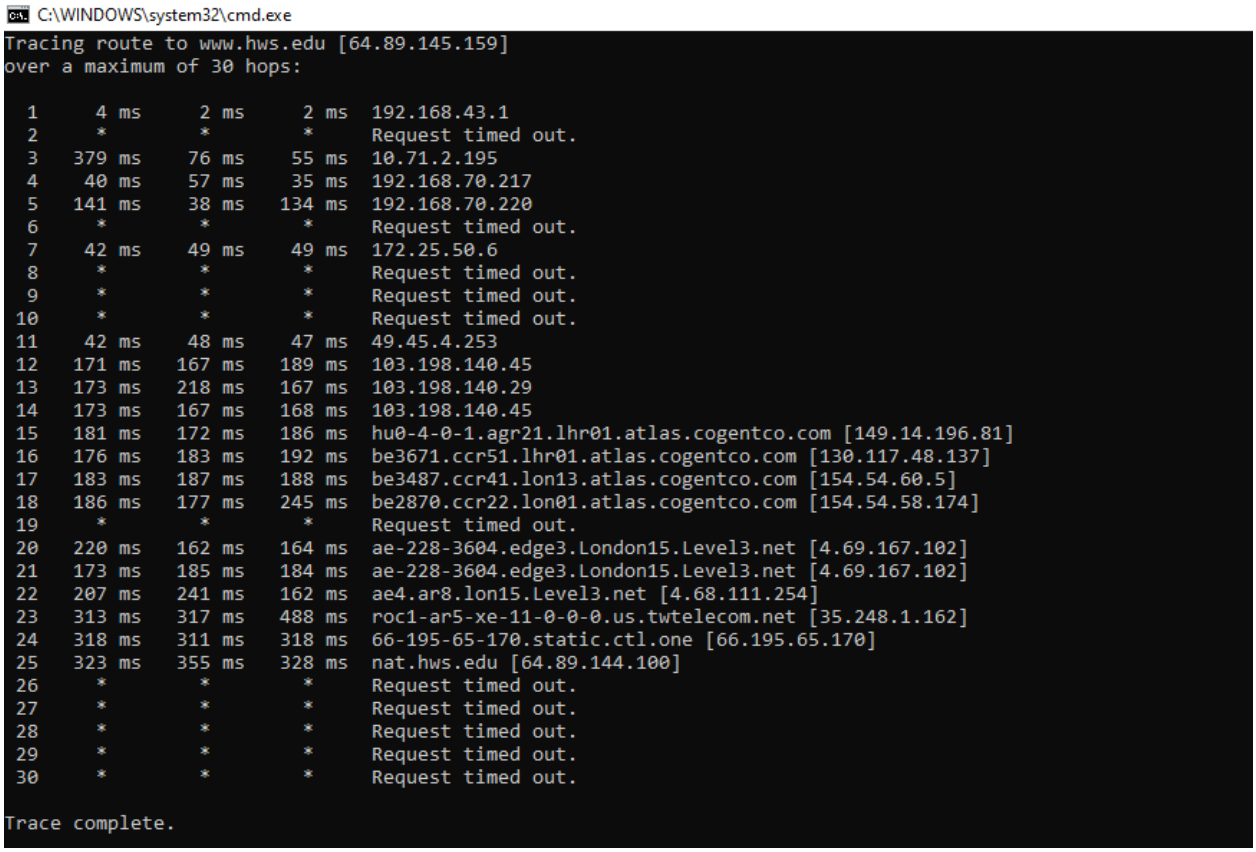
```
C:\Users\trusha>tracert www.hws.edu

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

  1    72 ms     4 ms     4 ms  192.168.43.1
  2     *        *        *     Request timed out.
  3   108 ms    99 ms   139 ms  10.71.2.195
  4   108 ms    99 ms    99 ms  192.168.70.217
  5   344 ms   480 ms   100 ms  192.168.70.220
  6     *        *        *     Request timed out.
  7   413 ms   101 ms    47 ms  172.25.50.6
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11   404 ms   100 ms   100 ms  103.198.140.58
 12   320 ms   293 ms   200 ms  103.198.140.45
 13   159 ms   167 ms   166 ms  103.198.140.27
 14   326 ms   166 ms   167 ms  103.198.140.107
 15   205 ms   203 ms   201 ms  103.198.140.45
 16   327 ms   469 ms   206 ms  hu0-4-0-1.agr21.lhr01.atlas.cogentco.com [149.14.196.81]
 17   166 ms   155 ms   183 ms  be3671.ccr51.lhr01.atlas.cogentco.com [130.117.48.137]
 18   210 ms   180 ms   201 ms  be3487.ccr41.lon13.atlas.cogentco.com [154.54.60.5]
 19   207 ms   201 ms   203 ms  be2870.ccr22.lon01.atlas.cogentco.com [154.54.58.174]
 20   215 ms   304 ms   201 ms  ae-7.edge7.London1.Level3.net [4.68.62.41]
 21   213 ms   201 ms   201 ms  ae-227-3603.edge3.London15.Level3.net [4.69.167.98]
 22   198 ms   477 ms   232 ms  ae-227-3603.edge3.London15.Level3.net [4.69.167.98]
 23   229 ms   201 ms   200 ms  ae4.ar8.lon15.Level3.net [4.68.111.254]
 24   311 ms   310 ms   399 ms  roc1-ar5-xe-11-0-0-0.us.twtelecom.net [35.248.1.162]
 25   397 ms   610 ms   403 ms  66-195-65-170.static.ctl.one [66.195.65.170]
 26   307 ms   610 ms   615 ms  64.89.144.100
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.
```

Exercise 3: Two packets sent from the same source to the same destination do not necessarily follow the same path through the net. Experiment with some sources that are fairly far away. Can you find cases where packets sent to the same destination follow different paths? How likely does it seem to be? What about when the packets are sent at very different times? Save some of the outputs from traceroute. (You can copy them from the Terminal window by highlighting and right-clicking, then paste into a text editor.) Come back sometime next week, try the same destinations again, and compare the results with the results from today. Report your observations .

20/08/2020:

```
C:\Users\trusha>tracert www.hws.edu

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

  1    72 ms     4 ms     4 ms  192.168.43.1
  2     *        *        *     Request timed out.
  3   108 ms    99 ms   139 ms  10.71.2.195
  4   108 ms    99 ms    99 ms  192.168.70.217
  5   344 ms   480 ms   100 ms  192.168.70.220
  6     *        *        *     Request timed out.
  7   413 ms   101 ms    47 ms  172.25.50.6
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11   404 ms   100 ms   100 ms  103.198.140.58
 12   320 ms   293 ms   200 ms  103.198.140.45
 13   159 ms   167 ms   166 ms  103.198.140.27
 14   326 ms   166 ms   167 ms  103.198.140.107
 15   205 ms   203 ms   201 ms  103.198.140.45
 16   327 ms   469 ms   206 ms  hu0-4-0-1.agr21.lhr01.atlas.cogentco.com [149.14.196.81]
 17   166 ms   155 ms   183 ms  be3671.ccr51.lhr01.atlas.cogentco.com [130.117.48.137]
 18   210 ms   180 ms   201 ms  be3487.ccr41.lon13.atlas.cogentco.com [154.54.60.5]
 19   207 ms   201 ms   203 ms  be2870.ccr22.lon01.atlas.cogentco.com [154.54.58.174]
 20   215 ms   304 ms   201 ms  ae-7.edge7.London1.Level3.net [4.68.62.41]
 21   213 ms   201 ms   201 ms  ae-227-3603.edge3.London15.Level3.net [4.69.167.98]
 22   198 ms   477 ms   232 ms  ae-227-3603.edge3.London15.Level3.net [4.69.167.98]
 23   229 ms   201 ms   200 ms  ae4.ar8.lon15.Level3.net [4.68.111.254]
 24   311 ms   310 ms   399 ms  roc1-ar5-xe-11-0-0-0.us.twtelecom.net [35.248.1.162]
 25   397 ms   610 ms   403 ms  66-195-65-170.static.ctl.one [66.195.65.170]
 26   307 ms   610 ms   615 ms  64.89.144.100
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.
```

27/08/2020 :



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 traceroute?

Answer :- Yes, the tracerouting follows a particular path from the user's IP address through the IP addresses of the ISP and then the path really depends on which access point is ready to respond and which access points or routers have firewalls configured for blocking the requests and accordingly, 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?

Answer :No , there is no relationship between the number of nodes that show up in 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 :-

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). 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).

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.

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 : Through this experiment, I understood and implemented commands for basic networking utilities.

Resources :-

1. https://www.imperva.com/learn/performance/round-trip-time-rtt/#:~:text=Round%2Dtrip%20time%20(RTT),load%20time%20and%20network%20latency.
2. https://www.geeksforgeeks.org/packet-switching-and-delays-in-computer-network/
3. https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/ipconfig