Name : Prathamesh Bagekari
Branch : TE Computer
Batch : A
UID : 2018130002

Lab 2
Basic Network Utilities

Command : ping

Description : **PING (Packet Internet Groper)** command is used to check the network connectivity between host and server/host. This command takes as input the IP address or the URL and sends a data packet to the specified address with the message “PING” and gets a response from the server/host this time is recorded which is called **latency**. Fast ping low latency means faster connection. Ping uses **ICMP(Internet Control Message Protocol)** to send an **ICMP echo message** to the specified host if that host is available then it sends an **ICMP reply message**. Ping is generally measured in **millisecond** every modern operating system has this ping pre-installed.

Experiments :

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.

Solution :

(1) *ping -n 10 -l 64 google.com*

```
C:\Windows\system32>ping -n 10 -l 64 google.com

Pinging google.com [216.58.203.46] with 64 bytes of data:
Reply from 216.58.203.46: bytes=64 time=3ms TTL=120
Reply from 216.58.203.46: bytes=64 time=3ms TTL=120
Reply from 216.58.203.46: bytes=64 time=3ms TTL=120
Reply from 216.58.203.46: bytes=64 time=3ms TTL=120
Reply from 216.58.203.46: bytes=64 time=3ms TTL=120
Reply from 216.58.203.46: bytes=64 time=3ms TTL=120
Reply from 216.58.203.46: bytes=64 time=3ms TTL=120
Reply from 216.58.203.46: bytes=64 time=2ms TTL=120
Reply from 216.58.203.46: bytes=64 time=2ms TTL=120
Reply from 216.58.203.46: bytes=64 time=3ms TTL=120

Ping statistics for 216.58.203.46:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms
```

(2) *ping -n 10 -l 100 www.uw.edu*

```
C:\Users\prath\Documents>ping -n 10 -l 100 www.uw.edu

Pinging www.washington.edu [128.95.155.134] with 100 bytes of data:
Reply from 128.95.155.134: bytes=100 time=239ms TTL=48
Reply from 128.95.155.134: bytes=100 time=239ms TTL=48
Reply from 128.95.155.134: bytes=100 time=239ms TTL=48
Reply from 128.95.155.134: bytes=100 time=240ms TTL=48
Reply from 128.95.155.134: bytes=100 time=239ms TTL=48
Reply from 128.95.155.134: bytes=100 time=239ms TTL=48
Reply from 128.95.155.134: bytes=100 time=239ms TTL=48
Reply from 128.95.155.134: bytes=100 time=240ms TTL=48
Reply from 128.95.155.134: bytes=100 time=239ms TTL=48
Reply from 128.95.155.134: bytes=100 time=240ms TTL=48

Ping statistics for 128.95.155.134:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 239ms, Maximum = 240ms, Average = 239ms
```

(3) *ping -n 10 -l 500 berkeley.edu*

```
C:\Users\prath\Documents>ping -n 10 -l 500 berkeley.edu

Pinging berkeley.edu [35.163.72.93] with 500 bytes of data:
Reply from 35.163.72.93: bytes=500 time=268ms TTL=34
Reply from 35.163.72.93: bytes=500 time=267ms TTL=34
Reply from 35.163.72.93: bytes=500 time=267ms TTL=34
Reply from 35.163.72.93: bytes=500 time=267ms TTL=34
Reply from 35.163.72.93: bytes=500 time=270ms TTL=34
Reply from 35.163.72.93: bytes=500 time=267ms TTL=34
Reply from 35.163.72.93: bytes=500 time=269ms TTL=34
Reply from 35.163.72.93: bytes=500 time=272ms TTL=34
Reply from 35.163.72.93: bytes=500 time=267ms TTL=34
Reply from 35.163.72.93: bytes=500 time=267ms TTL=34

Ping statistics for 35.163.72.93:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 267ms, Maximum = 272ms, Average = 268ms
```

(4) *ping -n 10 -l 1000 www.ox.ac.uk*

```
C:\Windows\system32>ping -n 10 -l 1000 www.ox.ac.uk

Pinging www.ox.ac.uk [151.101.130.133] with 1000 bytes of data:
Reply from 151.101.130.133: bytes=1000 time=5ms TTL=60
Reply from 151.101.130.133: bytes=1000 time=6ms TTL=60
Reply from 151.101.130.133: bytes=1000 time=5ms TTL=60
Reply from 151.101.130.133: bytes=1000 time=5ms TTL=60
Reply from 151.101.130.133: bytes=1000 time=5ms TTL=60
Reply from 151.101.130.133: bytes=1000 time=5ms TTL=60
Reply from 151.101.130.133: bytes=1000 time=5ms TTL=60
Reply from 151.101.130.133: bytes=1000 time=5ms TTL=60
Reply from 151.101.130.133: bytes=1000 time=7ms TTL=60
Reply from 151.101.130.133: bytes=1000 time=5ms TTL=60

Ping statistics for 151.101.130.133:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 7ms, Average = 5ms
```

(5) *ping -n 10 -l 1400 www.mozilla.org*

```
C:\Windows\system32>ping -n 10 -l 1400 www.mozilla.org

Pinging www.mozilla.org.cdn.cloudflare.net [104.18.164.34] with 1400 bytes of data:
Reply from 104.18.164.34: bytes=1400 time=9ms TTL=60
Reply from 104.18.164.34: bytes=1400 time=7ms TTL=60
Reply from 104.18.164.34: bytes=1400 time=8ms TTL=60
Reply from 104.18.164.34: bytes=1400 time=8ms TTL=60
Reply from 104.18.164.34: bytes=1400 time=14ms TTL=60
Reply from 104.18.164.34: bytes=1400 time=10ms TTL=60
Reply from 104.18.164.34: bytes=1400 time=8ms TTL=60
Reply from 104.18.164.34: bytes=1400 time=8ms TTL=60
Reply from 104.18.164.34: bytes=1400 time=9ms TTL=60
Reply from 104.18.164.34: bytes=1400 time=9ms TTL=60

Ping statistics for 104.18.164.34:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 14ms, Average = 9ms
```

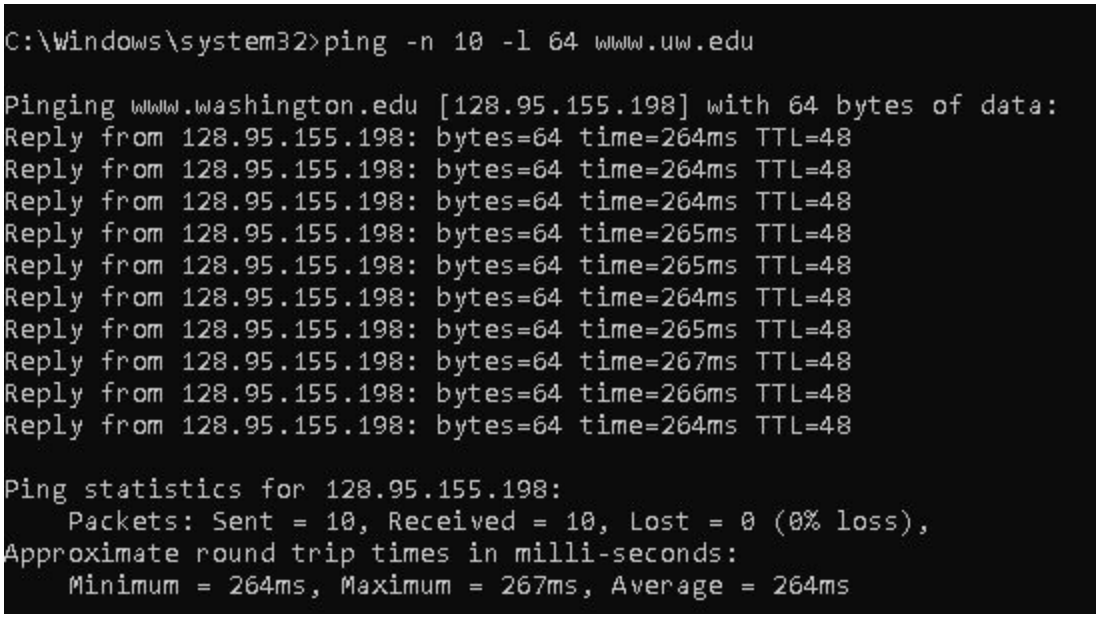
Questions on Latency :

1. Does the average RTT vary between different hosts? What aspects of latency (transmit, propagation, and queueing delay) might impact this and why?

```
C:\Windows\system32>ping -n 10 -l 64 google.com

Pinging google.com [216.58.203.46] with 64 bytes of data:
Reply from 216.58.203.46: bytes=64 time=3ms TTL=120
Reply from 216.58.203.46: bytes=64 time=3ms TTL=120
Reply from 216.58.203.46: bytes=64 time=3ms TTL=120
Reply from 216.58.203.46: bytes=64 time=3ms TTL=120
Reply from 216.58.203.46: bytes=64 time=3ms TTL=120
Reply from 216.58.203.46: bytes=64 time=3ms TTL=120
Reply from 216.58.203.46: bytes=64 time=3ms TTL=120
Reply from 216.58.203.46: bytes=64 time=2ms TTL=120
Reply from 216.58.203.46: bytes=64 time=2ms TTL=120
Reply from 216.58.203.46: bytes=64 time=3ms TTL=120

Ping statistics for 216.58.203.46:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms
```



From the above figures, we can clearly conclude that the RTT is dependent on the host on which the 'ping' command is used. **Transmission delay** is the time taken to put a packet onto a link or simply, the time required to put data bits on the wire/communication medium. It depends on the **size of the packet** and the **bandwidth of the network**. Since the hosts are the only parameters changed, there is no transmission delay in the two cases. **Propagation delay** is the time taken by the first bit to travel from sender to receiver end of the link or 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**. So, there exists a propagation delay in the two cases. **Queueing delay** is the time difference between when the packet arrived at its destination and when the packet data was processed or executed. It depends on the **number of packets, size of the packet** and **bandwidth** of the network. Since all the parameters are non-varying in both cases, there is hardly any queueing 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?

```
C:\Windows\system32>ping -n 10 -l 64 google.com

Pinging google.com [172.217.166.46] with 64 bytes of data:
Reply from 172.217.166.46: bytes=64 time=3ms TTL=120
Reply from 172.217.166.46: bytes=64 time=3ms TTL=120
Reply from 172.217.166.46: bytes=64 time=3ms TTL=120
Reply from 172.217.166.46: bytes=64 time=7ms TTL=120
Reply from 172.217.166.46: bytes=64 time=5ms TTL=120
Reply from 172.217.166.46: bytes=64 time=3ms TTL=120
Reply from 172.217.166.46: bytes=64 time=4ms TTL=120
Reply from 172.217.166.46: bytes=64 time=3ms TTL=120
Reply from 172.217.166.46: bytes=64 time=3ms TTL=120
Reply from 172.217.166.46: bytes=64 time=3ms TTL=120

Ping statistics for 172.217.166.46:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 7ms, Average = 3ms
```

```
C:\Windows\system32>ping -n 10 -l 100 google.com

Pinging google.com [172.217.166.46] with 100 bytes of data:
Reply from 172.217.166.46: bytes=68 (sent 100) time=5ms TTL=120
Reply from 172.217.166.46: bytes=68 (sent 100) time=3ms TTL=120
Reply from 172.217.166.46: bytes=68 (sent 100) time=4ms TTL=120
Reply from 172.217.166.46: bytes=68 (sent 100) time=3ms TTL=120
Reply from 172.217.166.46: bytes=68 (sent 100) time=5ms TTL=120
Reply from 172.217.166.46: bytes=68 (sent 100) time=3ms TTL=120
Reply from 172.217.166.46: bytes=68 (sent 100) time=3ms TTL=120
Reply from 172.217.166.46: bytes=68 (sent 100) time=9ms TTL=120
Reply from 172.217.166.46: bytes=68 (sent 100) time=3ms TTL=120
Reply from 172.217.166.46: bytes=68 (sent 100) time=49ms TTL=120

Ping statistics for 172.217.166.46:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 49ms, Average = 8ms
```

From the above images, we can say that the Round Trip Time is impacted due to the difference in the size of the packets. This is because of the **Transmission delay** and the **Queueing delay** which depend on the size of the packets.

Exercise :

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.

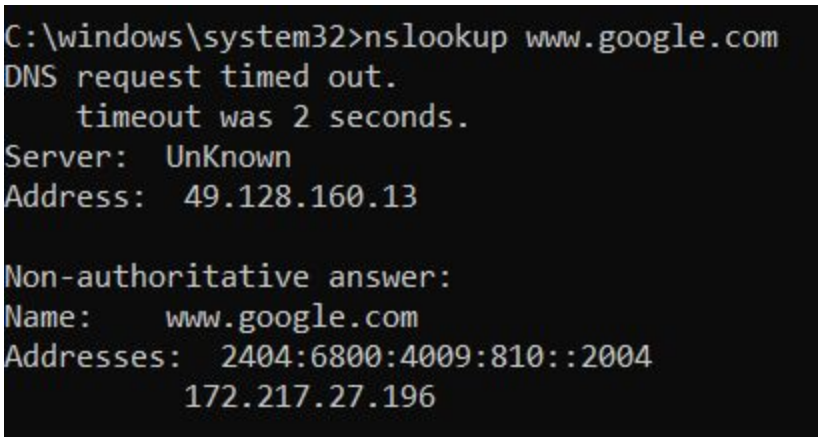
From the images shown above, the following observations can be made :

(1) The length a signal has to travel correlates with the time taken for a request to reach a server.
(2) 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.
(3) Intermediate routers or servers take time to process a signal, increasing RTT. The more hops a signal has to travel through, the higher the RTT.
(4) RTT typically increases when a network is congested with high levels of traffic. Conversely, low traffic times can result in decreased RTT.
(5) 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.

Command : nslookup

Description : 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>

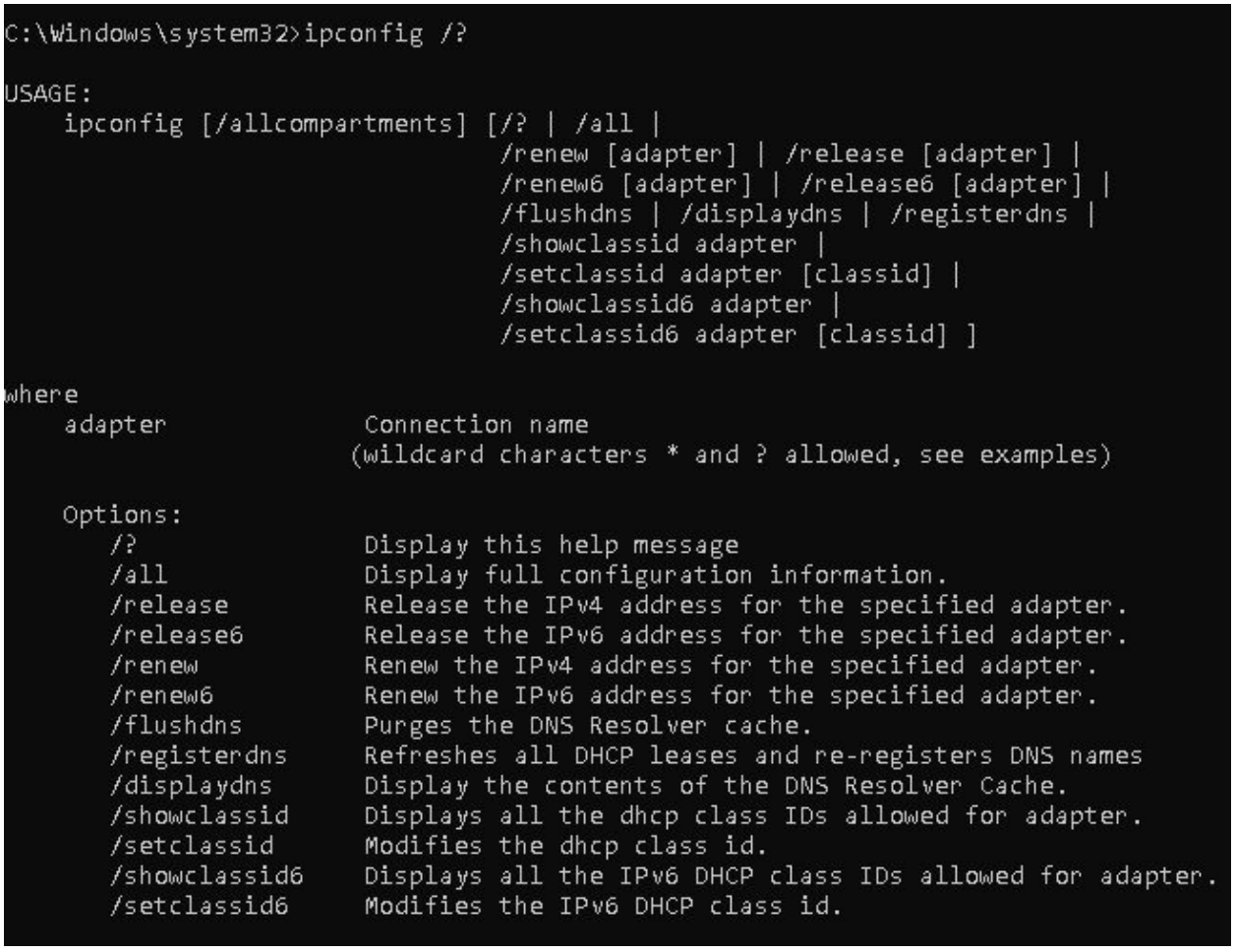
Screenshot :



Command : ipconfig

Description : 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.

Screenshots :

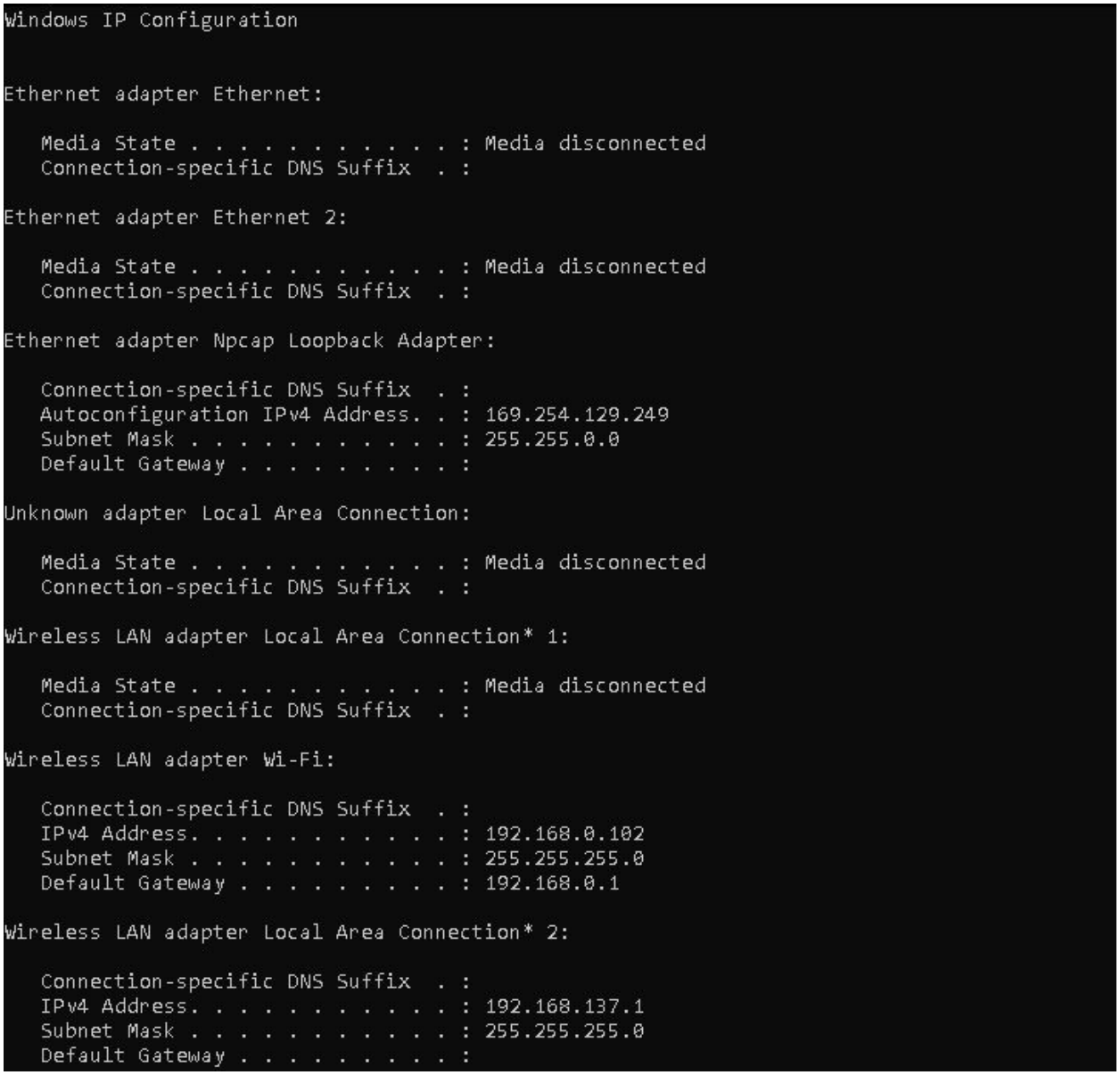


```
The default is to display only the IP address, subnet mask and
default gateway for each adapter bound to TCP/IP.

For Release and Renew, if no adapter name is specified, then the IP address
leases for all adapters bound to TCP/IP will be released or renewed.

For Setclassid and Setclassid6, if no ClassId is specified, then the ClassId is removed.

Examples:
    > ipconfig                      ... Show information
    > ipconfig /all                 ... Show detailed information
    > ipconfig /renew               ... renew all adapters
    > ipconfig /renew EL*           ... renew any connection that has its
                                        name starting with EL
    > ipconfig /release *Con*       ... release all matching connections,
                                        eg. "Wired Ethernet Connection 1" or
                                            "Wired Ethernet Connection 2"
    > ipconfig /allcompartments     ... Show information about all
                                        compartments
    > ipconfig /allcompartments /all ... Show detailed information about all
                                        compartments
```



Command : netstat

Description : 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.)

Screenshots :

```
C:\windows\system32>netstat -t -n

Active Connections

  Proto  Local Address          Foreign Address        State           Offload State

  TCP    127.0.0.1:56792        127.0.0.1:61266        ESTABLISHED     InHost
  TCP    127.0.0.1:61254        127.0.0.1:65001        ESTABLISHED     InHost
  TCP    127.0.0.1:61266        127.0.0.1:56792        ESTABLISHED     InHost
  TCP    127.0.0.1:65001        127.0.0.1:61254        ESTABLISHED     InHost
  TCP    192.168.0.102:60421    23.221.52.163:443      CLOSE_WAIT      InHost
  TCP    192.168.0.102:60422    23.221.52.163:443      CLOSE_WAIT      InHost
  TCP    192.168.0.102:60423    23.221.52.163:443      CLOSE_WAIT      InHost
  TCP    192.168.0.102:60424    23.217.53.10:443       CLOSE_WAIT      InHost
  TCP    192.168.0.102:60436    23.221.52.163:443      CLOSE_WAIT      InHost
  TCP    192.168.0.102:61282    40.119.211.203:443     ESTABLISHED     InHost
  TCP    192.168.0.102:61287    142.250.67.238:443     ESTABLISHED     InHost
  TCP    192.168.0.102:61307    54.191.221.88:443      ESTABLISHED     InHost
  TCP    192.168.0.102:61308    54.191.221.88:443      ESTABLISHED     InHost
  TCP    192.168.0.102:61310    54.191.221.88:443      ESTABLISHED     InHost
  TCP    192.168.0.102:61317    54.191.221.88:443      ESTABLISHED     InHost
  TCP    192.168.0.102:61333    172.217.160.206:443    ESTABLISHED     InHost
  TCP    192.168.0.102:61335    216.58.199.138:443     TIME_WAIT       InHost
  TCP    192.168.0.102:61337    13.107.6.171:443       ESTABLISHED     InHost
  TCP    192.168.0.102:61338    13.107.21.200:443      ESTABLISHED     InHost
  TCP    192.168.0.102:61339    184.30.63.124:80       ESTABLISHED     InHost
  TCP    192.168.0.102:61340    13.107.136.254:443     ESTABLISHED     InHost
  TCP    192.168.0.102:61341    117.18.232.200:443     ESTABLISHED     InHost
  TCP    192.168.0.102:61342    13.107.4.254:443       ESTABLISHED     InHost
  TCP    192.168.0.102:61343    161.69.226.18:443      TIME_WAIT       InHost
  TCP    192.168.0.102:61344    204.79.197.222:443     ESTABLISHED     InHost
```

Command : telnet

Description : 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 the 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 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: telnet <host> <port>. For example, to connect to the web server on www.spit.ac.in: telnet spit.ac.in 80

Screenshots :

A blank command prompt screen appears showing that the connection is established.

Command : tracert

Description : The **tracert** diagnostic utility determines the route to a destination by sending **Internet Control Message Protocol (ICMP) echo packets** to the destination. In these packets, traceroute uses varying IP Time-To-Live (TTL) values. Because each router along the path is required to decrement the packet's TTL by at least 1 before forwarding the packet, the TTL is effectively a **hop counter**. When the TTL on a packet reaches zero (0), the router sends an ICMP "Time Exceeded" message back to the source computer.

Experiment :

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).

Screenshots :

```
C:\Users\prath\Documents>tracert mscs.mu.edu > traceroute_mscs.mu.edu.log

C:\Users\prath\Documents>type traceroute_mscs.mu.edu.log

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

  1     4 ms     1 ms     1 ms  192.168.0.1
  2     3 ms     1 ms     2 ms  43-252-100-182.dhcp-mumbai.wnet.net.in [43.252.100.182]
  3     3 ms     2 ms     2 ms  43-252-100-161.dhcp-mumbai.wnet.net.in [43.252.100.161]
  4     2 ms     3 ms     3 ms  49.128.160-61.static-mumbai.wnet.net.in [49.128.160.61]
  5     4 ms     4 ms     4 ms  nsg-static-013.115.72.182.airtel.in [182.72.115.13]
  6   197 ms   197 ms   199 ms  182.79.222.233
  7   198 ms   200 ms   198 ms  core1.nyc4.he.net [198.32.118.57]
  8   221 ms   221 ms     *     100ge2-1.core2.chi1.he.net [184.104.193.173]
  9     *        *        *     Request timed out.
 10   215 ms   214 ms   214 ms  r-222wwash-isp-ae6-3926.wiscnet.net [140.189.8.126]
 11   225 ms   223 ms   223 ms  r-milwaukeeci-809-isp-ae3-0.wiscnet.net [140.189.8.230]
 12   222 ms   222 ms   221 ms  MarquetteUniv.site.wiscnet.net [216.56.1.202]
 13   213 ms   212 ms   212 ms  134.48.10.26
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.

C:\Users\prath\Documents>tracert ee.iitb.ac.in
Unable to resolve target system name ee.iitb.ac.in.
```

```
C:\Users\prath\Documents>tracert www.cs.grinnell.edu > traceroute_www.cs.grinnell.edu.log

C:\Users\prath\Documents>type traceroute_www.cs.grinnell.edu.log

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

  1     1 ms     1 ms     1 ms  192.168.0.1
  2     2 ms     2 ms     5 ms  43-252-100-182.dhcp-mumbai.wnet.net.in [43.252.100.182]
  3     3 ms     2 ms     2 ms  43-252-100-161.dhcp-mumbai.wnet.net.in [43.252.100.161]
  4     3 ms     2 ms     2 ms  49.128.160-61.static-mumbai.wnet.net.in [49.128.160.61]
  5     4 ms     3 ms     4 ms  nsg-static-013.115.72.182.airtel.in [182.72.115.13]
  6   194 ms   196 ms   195 ms  116.119.52.165
  7   195 ms   194 ms   209 ms  core1.nyc4.he.net [198.32.118.57]
  8   215 ms     *      220 ms  100ge9-1.core2.chi1.he.net [184.105.223.161]
  9   225 ms   225 ms   225 ms  100ge14-2.core1.msp1.he.net [184.105.223.178]
 10   245 ms   245 ms   249 ms  aureon-network-services-inc.e0-26.switch1.msp1.he.net [216.66.77.218]
 11   229 ms   229 ms   229 ms  17.1.137.57
 12   232 ms   231 ms   231 ms  173.215.28.193
 13     *      233 ms   232 ms  ins-kc3-lo0.kmrr.netins.net [167.142.66.74]
 14   231 ms   232 ms   233 ms  167.142.58.42
 15   231 ms   232 ms   231 ms  167.142.67.141
 16   224 ms   224 ms   225 ms  grinnellcollege1.desm.netins.net [167.142.65.43]
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.
```

```
C:\Users\prath\Documents>tracert csail.mit.edu > traceroute_csail.mit.edu.log

C:\Users\prath\Documents>type traceroute_csail.mit.edu.log

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

  1     1 ms     3 ms     1 ms  192.168.0.1
  2     2 ms     2 ms     2 ms  43-252-100-182.dhcp-mumbai.wnet.net.in [43.252.100.182]
  3     2 ms     2 ms     2 ms  43-252-100-161.dhcp-mumbai.wnet.net.in [43.252.100.161]
  4     2 ms     2 ms     2 ms  49.128.160-61.static-mumbai.wnet.net.in [49.128.160.61]
  5     3 ms     4 ms     4 ms  nsg-static-013.115.72.182.airtel.in [182.72.115.13]
  6     *        *        *     Request timed out.
  7   237 ms   234 ms   235 ms  xe-9-1-0.edge1.LosAngeles6.Level3.net [4.26.0.61]
  8     *      270 ms     *     ae-2-3.bear1.Boston1.Level3.net [4.69.159.249]
  9   255 ms   255 ms   255 ms  MASSACHUSET.bear1.Boston1.Level3.net [4.53.48.98]
 10   258 ms   258 ms   258 ms  dmz-rtr-1-external-rtr-1.mit.edu [18.0.161.17]
 11   261 ms   260 ms   261 ms  dmz-rtr-2-dmz-rtr-1-1.mit.edu [18.0.161.6]
 12   254 ms   254 ms   254 ms  mitnet.core-1-ext.csail.mit.edu [18.4.7.65]
 13   252 ms     *        *     core-1-ext.bdr.csail.mit.edu [128.30.13.26]
 14   255 ms   255 ms   255 ms  bdr.core-1.csail.mit.edu [128.30.0.246]
 15   270 ms   267 ms   266 ms  inquir-3ld.csail.mit.edu [128.30.2.109]

Trace complete.
```

```
C:\Users\prath\Documents>tracert cs.stanford.edu > traceroute_cs.stanford.edu.log

C:\Users\prath\Documents>type traceroute_cs.stanford.edu.log

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

  1     1 ms     1 ms     1 ms  192.168.0.1
  2     2 ms     2 ms     2 ms  43-252-100-182.dhcp-mumbai.wnet.net.in [43.252.100.182]
  3     2 ms     2 ms     5 ms  43-252-100-161.dhcp-mumbai.wnet.net.in [43.252.100.161]
  4     2 ms     2 ms     2 ms  49.128.160-61.static-mumbai.wnet.net.in [49.128.160.61]
  5     3 ms     3 ms     5 ms  nsg-static-013.115.72.182.airtel.in [182.72.115.13]
  6   203 ms   199 ms   200 ms  116.119.52.163
  7   195 ms   195 ms   195 ms  core1.nyc4.he.net [198.32.118.57]
  8   247 ms   247 ms     *     100ge8-1.core1.sjc2.he.net [184.105.81.218]
  9   248 ms   247 ms   247 ms  10ge4-5.core1.pao1.he.net [72.52.92.69]
 10   249 ms   248 ms   247 ms  stanford-university.100gigabitethernet5-1.core1.pao1.he.net [184.105.177.238]
 11   244 ms   243 ms   244 ms  csee-west-rtr-vl3.SUNet [171.66.255.140]
 12   248 ms   250 ms   248 ms  CS.stanford.edu [171.64.64.64]

Trace complete.
```

```
C:\Users\prath\Documents>tracert cs.manchester.ac.uk > traceroute_cs.manchester.ac.uk.log

C:\Users\prath\Documents>type traceroute_cs.manchester.ac.uk.log

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

  1     1 ms     1 ms     1 ms  192.168.0.1
  2     2 ms     2 ms     2 ms  43-252-100-182.dhcp-mumbai.wnet.net.in [43.252.100.182]
  3     2 ms     2 ms     2 ms  43-252-100-161.dhcp-mumbai.wnet.net.in [43.252.100.161]
  4     2 ms     2 ms     2 ms  49.128.160-61.static-mumbai.wnet.net.in [49.128.160.61]
  5     4 ms     3 ms     3 ms  nsg-static-013.115.72.182.airtel.in [182.72.115.13]
  6   148 ms   175 ms   140 ms  182.79.134.223
  7     *        *        *     Request timed out.
  8   138 ms   136 ms   136 ms  jisc-ic-345131-ldn-b4.c.telia.net [62.115.175.131]
  9   139 ms   139 ms   139 ms  ae24.londhx-sbr1.ja.net [146.97.35.197]
 10   140 ms   137 ms   136 ms  ae29.londpg-sbr2.ja.net [146.97.33.2]
 11   141 ms   143 ms   140 ms  ae31.erdiss-sbr2.ja.net [146.97.33.22]
 12   144 ms   143 ms   144 ms  ae29.manckh-sbr2.ja.net [146.97.33.42]
 13   143 ms   143 ms   145 ms  ae23.mancrh-rbr1.ja.net [146.97.38.42]
 14   142 ms     *        *     universityofmanchester.ja.net [146.97.169.2]
 15   142 ms   142 ms   142 ms  130.88.249.194
 16     *        *        *     Request timed out.
 17   143 ms   142 ms   142 ms  gw-jh.its.manchester.ac.uk [130.88.250.32]
 18   145 ms   147 ms   145 ms  eps.its.man.ac.uk [130.88.101.49]

Trace complete.
```

Exercise 2 :

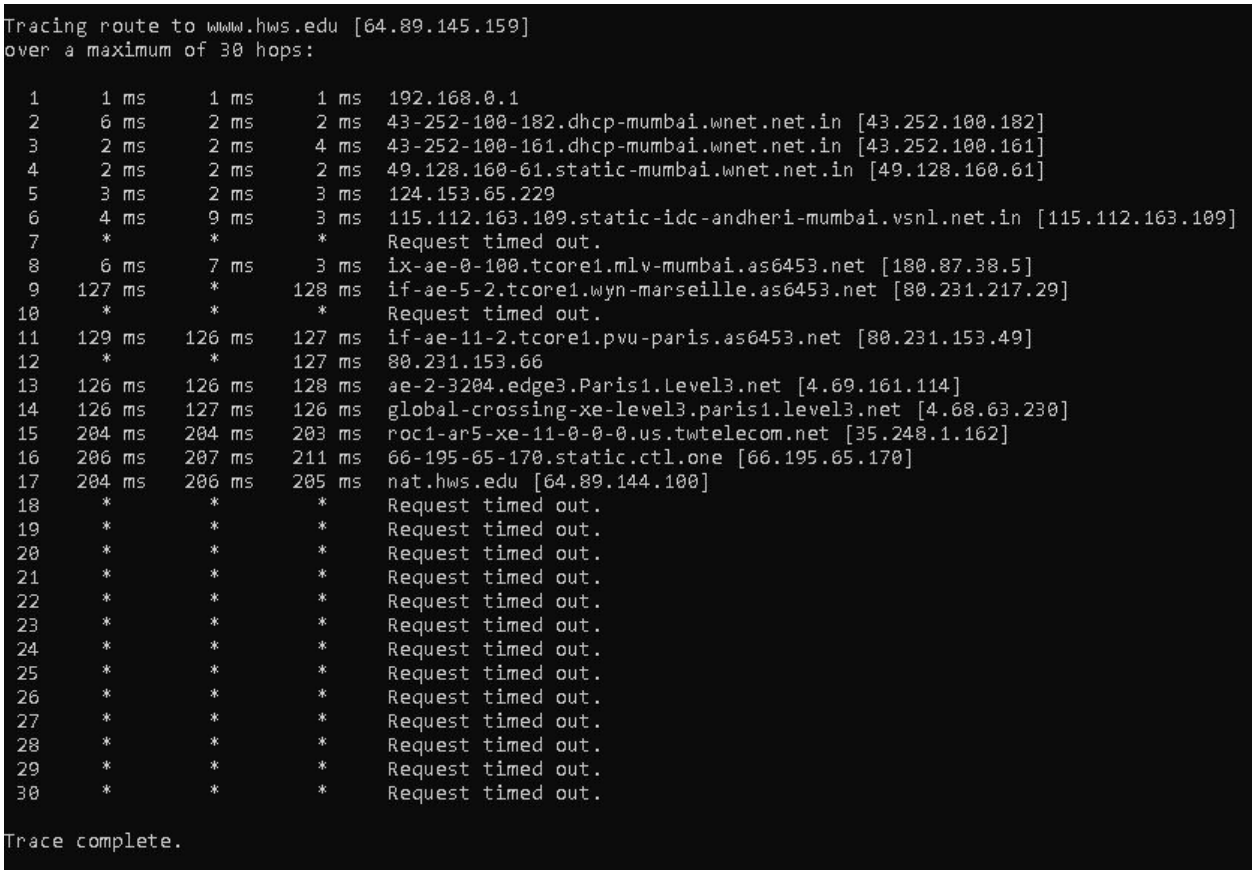
Use traceroute to trace the route from your computer to math.hws.edu and to www.hws.edu. Explain the difference in the results.

```
C:\Users\prath\Documents>tracert math.hws.edu && tracert www.hws.edu

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

  1     1 ms     1 ms     1 ms  192.168.0.1
  2     2 ms     1 ms     2 ms  43-252-100-182.dhcp-mumbai.wnet.net.in [43.252.100.182]
  3     2 ms     2 ms     3 ms  43-252-100-161.dhcp-mumbai.wnet.net.in [43.252.100.161]
  4     2 ms     2 ms     2 ms  49.128.160-61.static-mumbai.wnet.net.in [49.128.160.61]
  5     3 ms     5 ms     3 ms  nsg-static-013.115.72.182.airtel.in [182.72.115.13]
  6     *        *        *     Request timed out.
  7   239 ms   245 ms   238 ms  ae58.edge1.LosAngeles6.Level3.net [4.26.0.17]
  8     *      235 ms   235 ms  ae-1-51.ear3.LosAngeles1.Level3.net [4.69.206.225]
  9     *        *        *     Request timed out.
 10   257 ms   256 ms   256 ms  roc1-ar5-xe-0-0-0-0.us.twtelecom.net [35.248.1.158]
 11   263 ms   262 ms   262 ms  66-195-65-170.static.ctl.one [66.195.65.170]
 12   260 ms   260 ms   262 ms  nat.hws.edu [64.89.144.100]
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.
```



From the above images, the first row shows that the process of route tracing has started as the last column shows the Default Gateway of the user. The next three rows in both the cases are similar as the route is being traced starting from the ISP (Internet service provider) of the user. The next few rows, after which the tracing reaches the common IP address of **66.195.65.170** and then **nat.hws.edu [64.89.144.100],** clearly show that the route is completely different after crossing the ISP for both the cases. A domain name might have multiple IP addresses associated. If this is the case, multiple traces may access two or more IP addresses. This will yield trace paths that differ from one another, even if the origin and destinations are the same.

Domains may also use multiple servers for its subdomains. Tracing the path to the base domain might result in a completely different path when tracing to the subdomain. A URL with the **www** prefix is technically a subdomain, so it's possible that traces to **example.com** and **www.example.com** follow two very different paths.

Many domains use separate hosting for email. If you try to trace the domain, you'll get data for the website server, not the email server. This concept is popularly known as **Caveats** (Reference: https://network-tools.com/trace/).

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.

```
C:\Users\prath\Documents>tracert cs.stanford.edu > traceroute_cs.stanford.edu.log

C:\Users\prath\Documents>type traceroute_cs.stanford.edu.log

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

  1     1 ms     1 ms     1 ms  192.168.0.1
  2     2 ms     2 ms     2 ms  43-252-100-182.dhcp-mumbai.wnet.net.in [43.252.100.182]
  3     2 ms     2 ms     5 ms  43-252-100-161.dhcp-mumbai.wnet.net.in [43.252.100.161]
  4     2 ms     2 ms     2 ms  49.128.160-61.static-mumbai.wnet.net.in [49.128.160.61]
  5     3 ms     3 ms     5 ms  nsg-static-013.115.72.182.airtel.in [182.72.115.13]
  6   203 ms   199 ms   200 ms  116.119.52.163
  7   195 ms   195 ms   195 ms  core1.nyc4.he.net [198.32.118.57]
  8   247 ms   247 ms     *     100ge8-1.core1.sjc2.he.net [184.105.81.218]
  9   248 ms   247 ms   247 ms  10ge4-5.core1.pao1.he.net [72.52.92.69]
 10   249 ms   248 ms   247 ms  stanford-university.100gigabitethernet5-1.core1.pao1.he.net [184.105.177.238]
 11   244 ms   243 ms   244 ms  csee-west-rtr-vl3.SUNet [171.66.255.140]
 12   248 ms   250 ms   248 ms  CS.stanford.edu [171.64.64.64]

Trace complete.
```

```
C:\windows\system32>tracert cs.stanford.edu

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

  1    87 ms     1 ms     3 ms  192.168.0.1
  2     5 ms     4 ms     1 ms  43-252-100-182.dhcp-mumbai.wnet.net.in [43.252.100.182]
  3     5 ms     5 ms     2 ms  43-252-100-161.dhcp-mumbai.wnet.net.in [43.252.100.161]
  4     4 ms     4 ms     2 ms  49.128.160-61.static-mumbai.wnet.net.in [49.128.160.61]
  5     8 ms     6 ms     5 ms  nsg-static-013.115.72.182.airtel.in [182.72.115.13]
  6   326 ms   260 ms   266 ms  182.79.222.237
  7   241 ms   304 ms   194 ms  core1.nyc4.he.net [198.32.118.57]
  8     *        *      350 ms  100ge8-1.core1.sjc2.he.net [184.105.81.218]
  9   457 ms   302 ms   351 ms  100ge1-1.core1.pao1.he.net [72.52.92.158]
 10   406 ms  1205 ms   272 ms  stanford-university.100gigabitethernet5-1.core1.pao1.he.net [184.105.177.238]
 11   305 ms   297 ms   305 ms  csee-west-rtr-vl3.SUNet [171.66.255.140]
 12   274 ms   256 ms   360 ms  CS.stanford.edu [171.64.64.64]

Trace complete.
```

Questions :

(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 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?

A hop is limited only to a specific distance and also depends largely on the bandwidth and the traffic present on the network. If the distance between the location of the user and that of the destination url is more, then more hops will be required in order to reach the destination as more number of access points will be used for routing and the greater the number of access points involved, the greater are the chances of access points failing to respond and similarly for searching the alternative optimal path towards the destination.

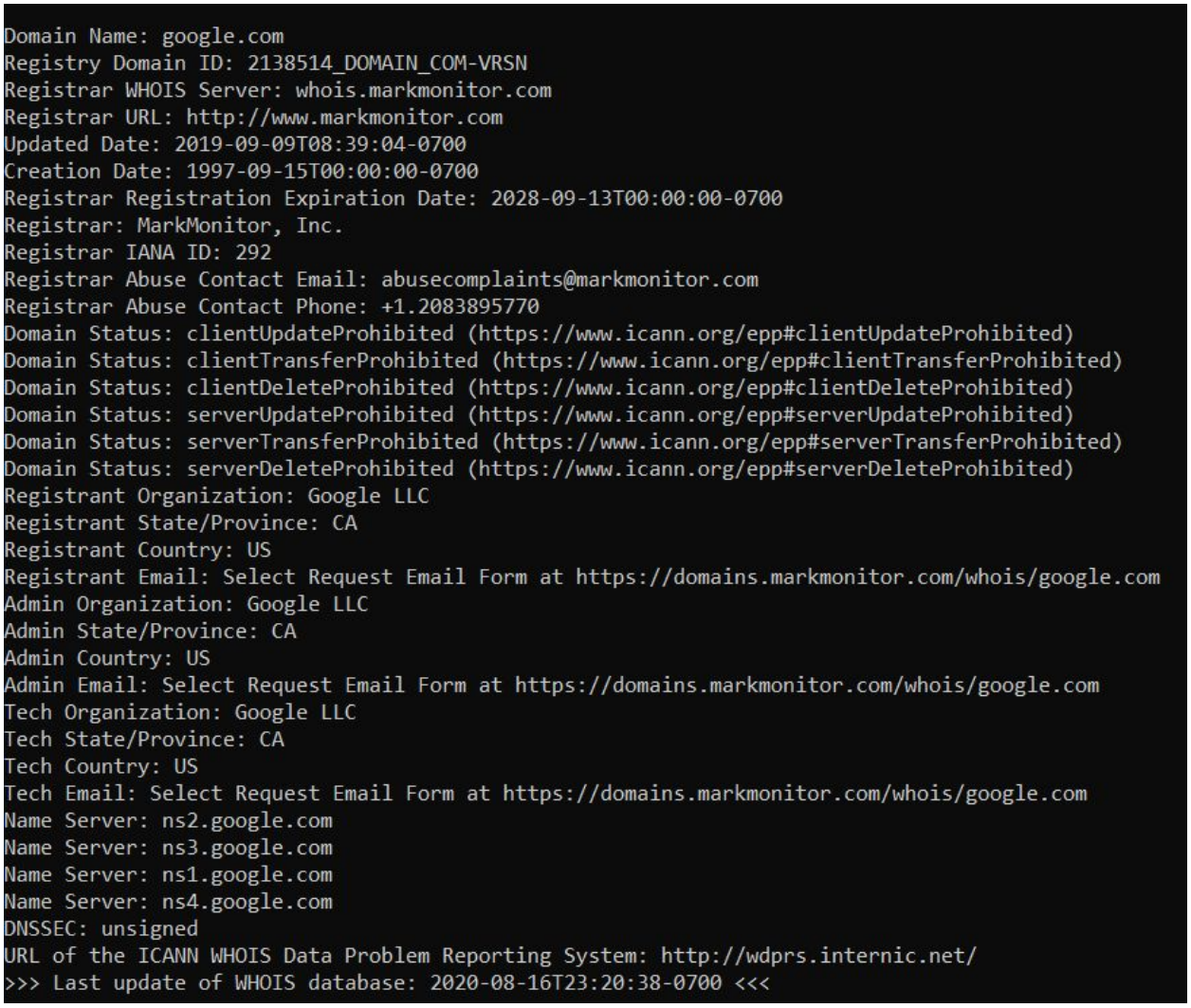
(3) Is there a relationship between the number of nodes that show up in the traceroute and latency of the host (from your ping results above)? Does the same relationship hold for all hosts?

If the latency of the host causes the traceroute request to get timed out even after the conventional three tries, then it keeps on sending the data packets until the host responds or upto a certain maximum hops. The same relationship may not hold for each host as it really depends on the time which the host takes to respond. If the host responds in the first request itself, the tracerouting stops with a success message.

Command : whois

Description : The **whois** command can give detailed information about the **domain names** and **IP addresses**.

Exercise 4 : 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.



As shown in the above image, the whois command gives information about the **domain name**, the **Registry Domain ID** and some other details such as the details of the **Registrar** and the **Registrant**. For example, in case of **google.com** (domain name), the **Registrant Organization** is **Google LLC**, the **Registrant State/Province** is **California** and the **Registrant Country** is the **United States**. It also provides the domain expiry date.