NAME: AISHWARYA GHAIWAT
CLASS : TE COMPS
BATCH : A
ROLL NO:13
UID NO: 2018130012

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>

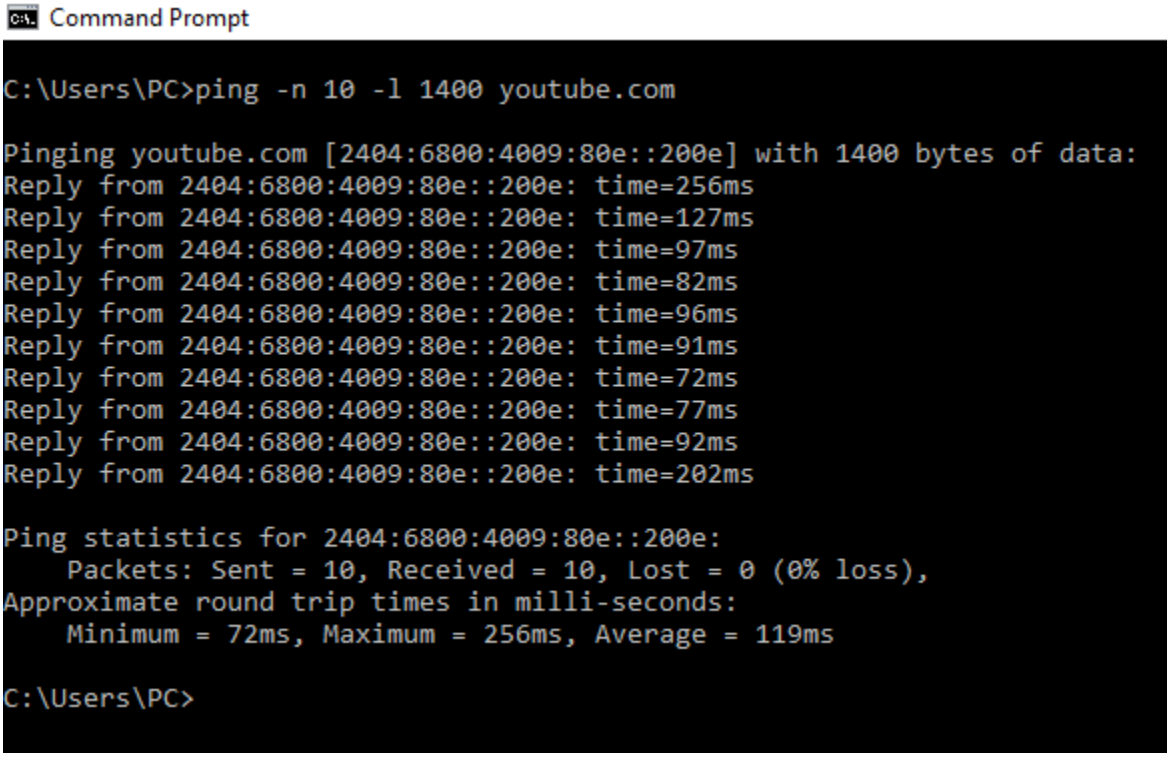
The default number of ICMP packets to send is either infinite (in Linux and Mac OS) or 4 (in Windows). The default packet size is either 64 bytes (in Linux) or 32 bytes (in Windows). You can specify either a hostname (e.g., spit.ac.in) or an IP address.

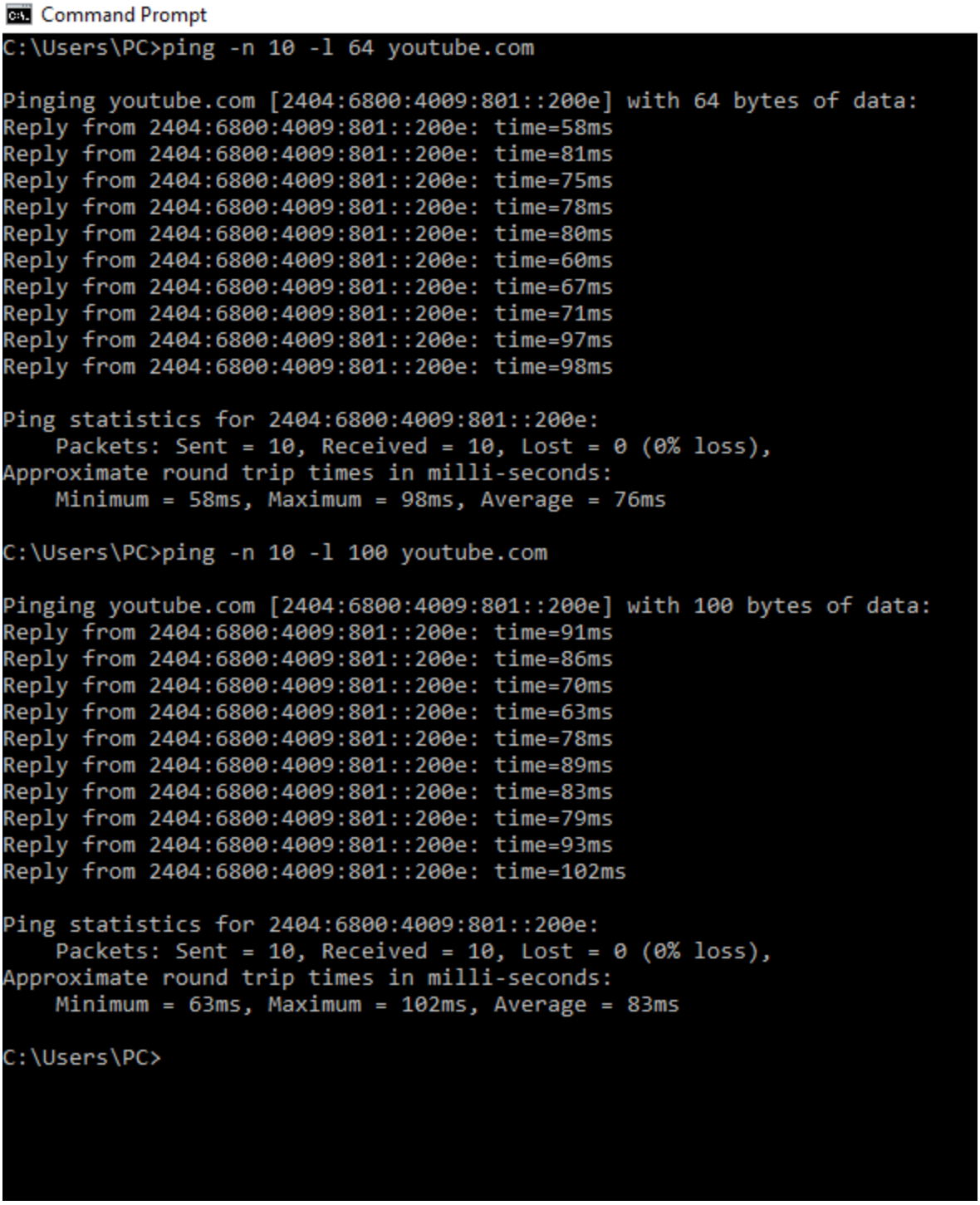
To save the output from ping to a file, include a greater than symbol and a file name at the end of the command. For example:

ping -c 10 google.com > ping_c10_s64_google.log

EXPERIMENTS WITH PING

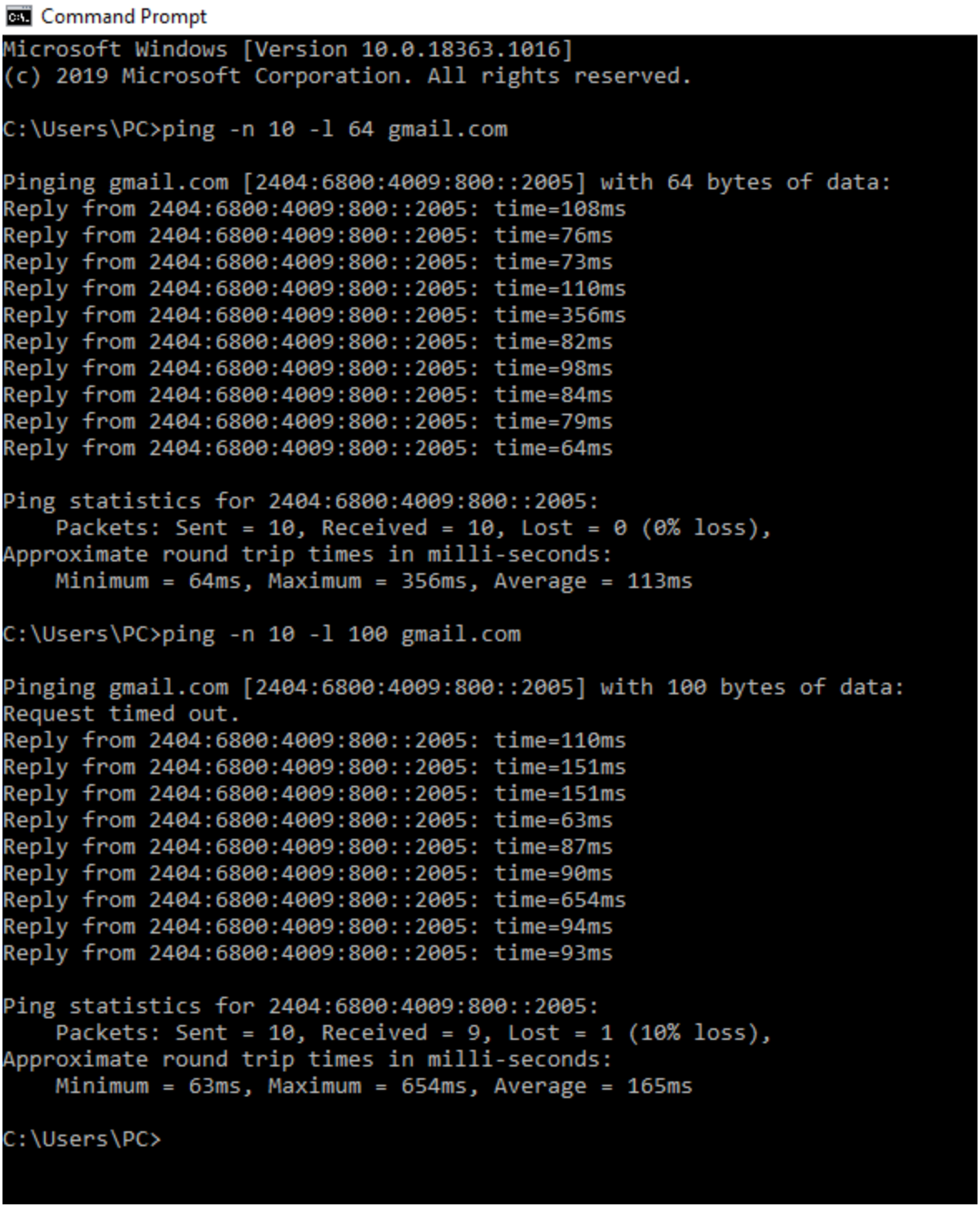
1. Ping the any hosts 10 times (i.e., packet count is 10) with a packet size of 64 bytes, 100 bytes, 500 bytes, 1000 bytes, 1400 bytes




Command Prompt
C:\Users\PC>ping -n 10 -l 64 youtube.com
Pinging youtube.com [2404:6800:4009:801::200e] with 64 bytes of data:
Reply from 2404:6800:4009:801::200e: time=58ms
Reply from 2404:6800:4009:801::200e: time=81ms
Reply from 2404:6800:4009:801::200e: time=75ms
Reply from 2404:6800:4009:801::200e: time=78ms
Reply from 2404:6800:4009:801::200e: time=80ms
Reply from 2404:6800:4009:801::200e: time=60ms
Reply from 2404:6800:4009:801::200e: time=67ms
Reply from 2404:6800:4009:801::200e: time=71ms
Reply from 2404:6800:4009:801::200e: time=97ms
Reply from 2404:6800:4009:801::200e: time=98ms
Ping statistics for 2404:6800:4009:801::200e:
Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 58ms, Maximum = 98ms, Average = 76ms
C:\Users\PC>ping -n 10 -l 100 youtube.com
Pinging youtube.com [2404:6800:4009:801::200e] with 100 bytes of data:
Reply from 2404:6800:4009:801::200e: time=91ms
Reply from 2404:6800:4009:801::200e: time=86ms
Reply from 2404:6800:4009:801::200e: time=70ms
Reply from 2404:6800:4009:801::200e: time=63ms
Reply from 2404:6800:4009:801::200e: time=78ms
Reply from 2404:6800:4009:801::200e: time=89ms
Reply from 2404:6800:4009:801::200e: time=83ms
Reply from 2404:6800:4009:801::200e: time=79ms
Reply from 2404:6800:4009:801::200e: time=93ms
Reply from 2404:6800:4009:801::200e: time=102ms
Ping statistics for 2404:6800:4009:801::200e:
Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 63ms, Maximum = 102ms, Average = 83ms
C:\Users\PC>

Command Prompt

```
C:\Users\PC>ping -n 10 -l 500 gmail.com

Pinging gmail.com [2404:6800:4009:802::2005] with 500 bytes of data:
Reply from 2404:6800:4009:802::2005: time=83ms
Reply from 2404:6800:4009:802::2005: time=70ms
Request timed out.
Reply from 2404:6800:4009:802::2005: time=79ms
Reply from 2404:6800:4009:802::2005: time=65ms
Reply from 2404:6800:4009:802::2005: time=85ms
Reply from 2404:6800:4009:802::2005: time=80ms
Reply from 2404:6800:4009:802::2005: time=122ms
Reply from 2404:6800:4009:802::2005: time=77ms
Reply from 2404:6800:4009:802::2005: time=94ms

Ping statistics for 2404:6800:4009:802::2005:
    Packets: Sent = 10, Received = 9, Lost = 1 (10% loss),
Approximate round trip times in milli-seconds:
    Minimum = 65ms, Maximum = 122ms, Average = 83ms

C:\Users\PC>ping -n 10 -l 1000 gmail.com

Pinging gmail.com [2404:6800:4009:802::2005] with 1000 bytes of data:
Reply from 2404:6800:4009:802::2005: time=70ms
Reply from 2404:6800:4009:802::2005: time=85ms
Reply from 2404:6800:4009:802::2005: time=66ms
Request timed out.
Reply from 2404:6800:4009:802::2005: time=95ms
Reply from 2404:6800:4009:802::2005: time=84ms
Reply from 2404:6800:4009:802::2005: time=78ms
Reply from 2404:6800:4009:802::2005: time=82ms
Reply from 2404:6800:4009:802::2005: time=100ms
Reply from 2404:6800:4009:802::2005: time=69ms

Ping statistics for 2404:6800:4009:802::2005:
    Packets: Sent = 10, Received = 9, Lost = 1 (10% loss),
Approximate round trip times in milli-seconds:
    Minimum = 66ms, Maximum = 100ms, Average = 81ms

C:\Users\PC>
```



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?

Ans : 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. Round-trip time (RTT) is the duration in milliseconds (ms) it takes for a network request to go from a starting point to a destination and back again to the starting point. RTT is an important metric in determining the health of a connection on a local network or the larger Internet, and is commonly utilized by network administrators to diagnose the speed and reliability of connections.

Yes ,It does vary between different hosts as in above example the average RTT was calculated

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

1. RTT increases with increase in packet size. There would be increased latency for increased packet size due to transmission delay, queuing delay and propagation delay.
    i. List of factors affecting RTT:
        1. **The nature of the transmission medium** - the way in which connections are made affects how fast the connection moves; connections made over optical fibre will behave differently than connections made over copper. Likewise, a connection made over a wireless frequency will behave differently than that of a satellite communication.
        2. **Local area network (LAN) traffic** - the amount of traffic on the local area network can bottleneck a connection before it ever reaches the larger Internet. For example, if many users are using streaming video service simultaneously, round-trip time may be inhibited even though the external network has excess capacity and is functioning normally.
        3. **Server response time** – the amount of time it takes a server to process and respond to a request is a potential bottleneck in network latency. When a server is overwhelmed with requests, such as during a DDoS attack, its ability to respond efficiently can be inhibited, resulting in increased RTT.
        4. **Node count and congestion** – depending on the path that a connection takes across the Internet, it may be routed or "hop" through a different number of intermediate nodes. Generally speaking, the greater the number of nodes a connection touches the slower it will be. A node may also experience network congestion

from other network traffic, which will slow down the connection and increase RTT.

5. **Physical distance** – although a connection optimized by a CDN can often reduce the number of hops required to reach a destination, there is no way of getting around the limitation imposed by the speed of light; the distance between a start and end point is a limiting factor in network connectivity that can only be reduced by moving content closer to the requesting users. To overcome this obstacle, a CDN will cache content closer to the requesting users, thereby reducing RTT.

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).

Ans:

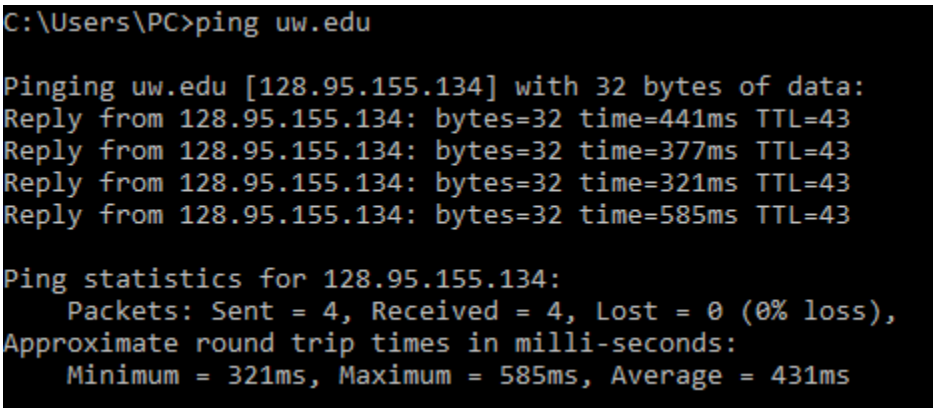
The length a signal has to travel correlates with the time taken for a request to reach a server and a response to reach a user.

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.

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.

RTT typically increases when a network is congested with high levels of traffic. Conversely, low traffic times can result in decreased RTT.

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



```
C:\Users\PC>ping cornell.edu

Pinging cornell.edu [128.253.173.247] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 128.253.173.247:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
C:\Users\PC>ping berkeley.edu

Pinging berkeley.edu [35.163.72.93] with 32 bytes of data:
Reply from 35.163.72.93: bytes=32 time=360ms TTL=37
Reply from 35.163.72.93: bytes=32 time=658ms TTL=37
Reply from 35.163.72.93: bytes=32 time=343ms TTL=37
Reply from 35.163.72.93: bytes=32 time=302ms TTL=37

Ping statistics for 35.163.72.93:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 302ms, Maximum = 658ms, Average = 415ms
```

```
C:\Users\PC>ping 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:\Users\PC>ping 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=65ms TTL=53
Reply from 151.101.66.133: bytes=32 time=195ms TTL=53
Reply from 151.101.66.133: bytes=32 time=165ms TTL=53
Reply from 151.101.66.133: bytes=32 time=70ms TTL=53

Ping statistics for 151.101.66.133:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 65ms, Maximum = 195ms, Average = 123ms
```

```
C:\Users\PC>ping u-tokyo.ac.jp
Ping request could not find host u-tokyo.ac.jp. Please check the name and try again.

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

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>

```
C:\Users\PC>nslookup wikipedia.com
Server:  UnKnown
Address:  192.168.43.1

Non-authoritative answer:
Name:    wikipedia.com
Addresses:  2001:df2:e500:ed1a::3
          103.102.166.226
```

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!!!.)

Command Prompt

```
C:\Users\PC>ipconfig /?

USAGE:
    ipconfig [/allcompartments] [/? | /all |
                                 /renew [adapter] | /release [adapter] |
                                 /renew6 [adapter] | /release6 [adapter] |
                                 /flushdns | /displaydns | /registerdns |
                                 /showclassid adapter |
                                 /setclassid adapter [classid] |
                                 /showclassid6 adapter |
                                 /setclassid6 adapter [classid] ]

where
    adapter             Connection name
                       (wildcard characters * and ? allowed, see examples)

    Options:
       /?               Display this help message
       /all             Display full configuration information.
       /release         Release the IPv4 address for the specified adapter.
       /release6        Release the IPv6 address for the specified adapter.
       /renew           Renew the IPv4 address for the specified adapter.
       /renew6          Renew the IPv6 address for the specified adapter.
       /flushdns        Purges the DNS Resolver cache.
       /registerdns     Refreshes all DHCP leases and re-registers DNS names
       /displaydns      Display the contents of the DNS Resolver Cache.
       /showclassid     Displays all the dhcp class IDs allowed for adapter.
       /setclassid      Modifies the dhcp class id.
       /showclassid6    Displays all the IPv6 DHCP class IDs allowed for adapter.
       /setclassid6     Modifies the IPv6 DHCP class id.


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
```

```
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

C:\Users\PC>
```

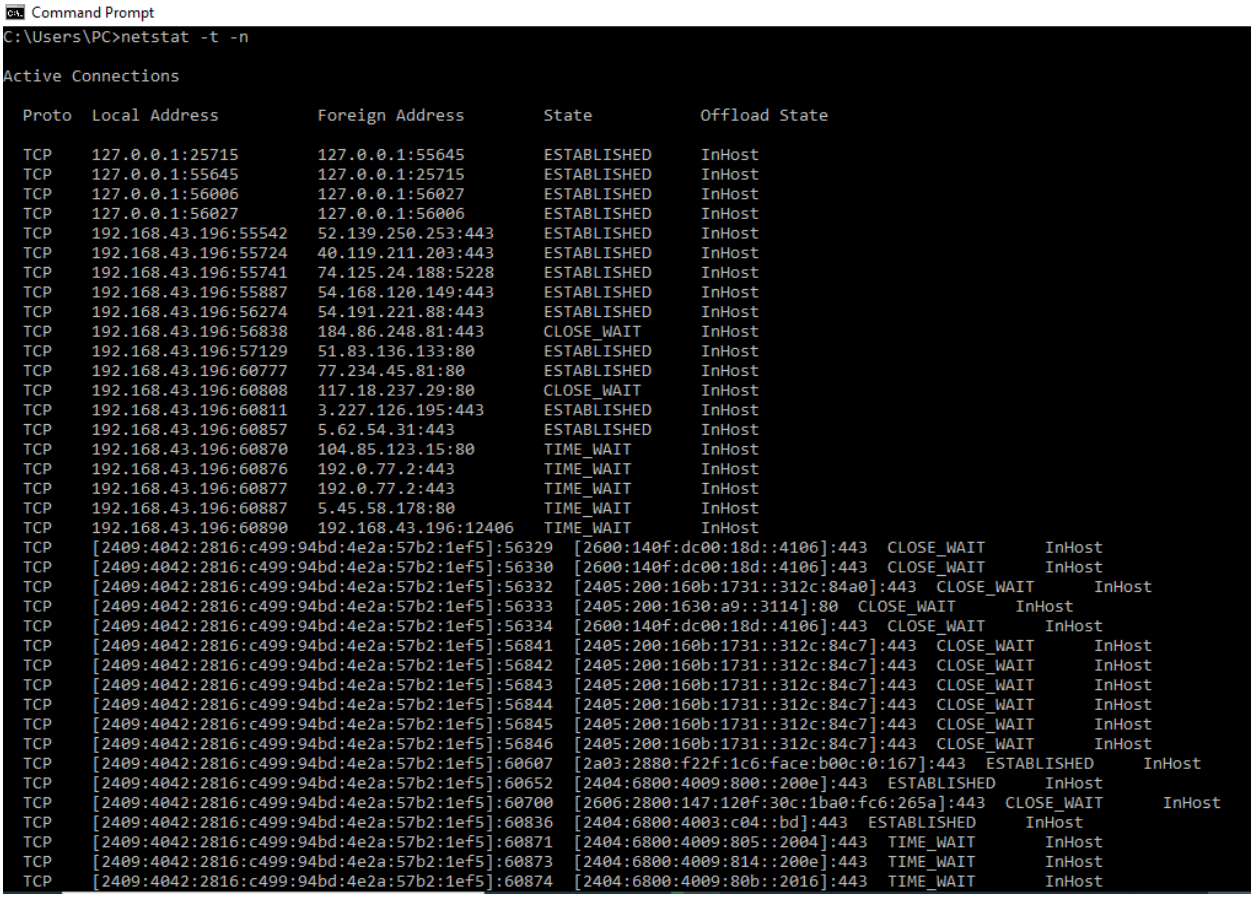
netstat — The netstat command gives information about network connections. I often use netstat -t -n which lists currently open TCP connections (that's the "-t" option) by IP address rather than domain name (that's the "-n" option). Add the option "-l" (lower case ell) to list listening sockets, that 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.)

Command Prompt

```
C:\Users\PC>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:25715        DESKTOP-BM64VDV:55645  ESTABLISHED
  TCP    127.0.0.1:55645        DESKTOP-BM64VDV:25715  ESTABLISHED
  TCP    127.0.0.1:56006        DESKTOP-BM64VDV:56027  ESTABLISHED
  TCP    127.0.0.1:56027        DESKTOP-BM64VDV:56006  ESTABLISHED
  TCP    192.168.43.196:55542   52.139.250.253:https   ESTABLISHED
  TCP    192.168.43.196:55724   40.119.211.203:https   ESTABLISHED
  TCP    192.168.43.196:55741   74.125.24.188:5228     ESTABLISHED
  TCP    192.168.43.196:55887   ec2-54-168-120-149:https  ESTABLISHED
  TCP    192.168.43.196:56274   ec2-54-191-221-88:https  ESTABLISHED
  TCP    192.168.43.196:56838   a184-86-248-81:https   CLOSE_WAIT
  TCP    192.168.43.196:57129   ip133:http             ESTABLISHED
  TCP    192.168.43.196:60777   fra02-014:http         ESTABLISHED
  TCP    192.168.43.196:60808   117.18.237.29:http     CLOSE_WAIT
  TCP    192.168.43.196:60811   ec2-3-227-126-195:https  ESTABLISHED
  TCP    192.168.43.196:60857   5.62.54.31:https       ESTABLISHED
  TCP    192.168.43.196:60867   160:https              TIME_WAIT
  TCP    192.168.43.196:60869   20.44.239.154:https    TIME_WAIT
  TCP    192.168.43.196:60870   a104-85-123-15:http    TIME_WAIT
  TCP    192.168.43.196:60876   i1:https               TIME_WAIT
  TCP    192.168.43.196:60877   i1:https               TIME_WAIT
  TCP    192.168.43.196:60887   r-178-58-45-5:http     FIN_WAIT_1
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:56329  g2600-140f-dc00-018d-0000-0000-0000-4106:https  CLOSE_WAIT
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:56330  g2600-140f-dc00-018d-0000-0000-0000-4106:https  CLOSE_WAIT
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:56332  [2405:200:160b:1731::312c:84a0]:https  CLOSE_WAIT
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:56333  [2405:200:1630:a9::3114]:http  CLOSE_WAIT
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:56334  g2600-140f-dc00-018d-0000-0000-0000-4106:https  CLOSE_WAIT
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:56841  [2405:200:160b:1731::312c:84c7]:https  CLOSE_WAIT
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:56842  [2405:200:160b:1731::312c:84c7]:https  CLOSE_WAIT
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:56843  [2405:200:160b:1731::312c:84c7]:https  CLOSE_WAIT
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:56844  [2405:200:160b:1731::312c:84c7]:https  CLOSE_WAIT
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:56845  [2405:200:160b:1731::312c:84c7]:https  CLOSE_WAIT
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:56846  [2405:200:160b:1731::312c:84c7]:https  CLOSE_WAIT
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60607  whatsapp-cdn6-shv-02-bom1:https  ESTABLISHED
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60652  bom07s15-in-x0e:https  ESTABLISHED
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60700  [2606:2800:147:120f:30c:1ba0:fc6:265a]:https  CLOSE_WAIT
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60836  [2404:6800:4003:c04::bd]:https  ESTABLISHED
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60858  bom05s11-in-x0e:https  TIME_WAIT
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60860  bom07s24-in-x0e:https  TIME_WAIT
```

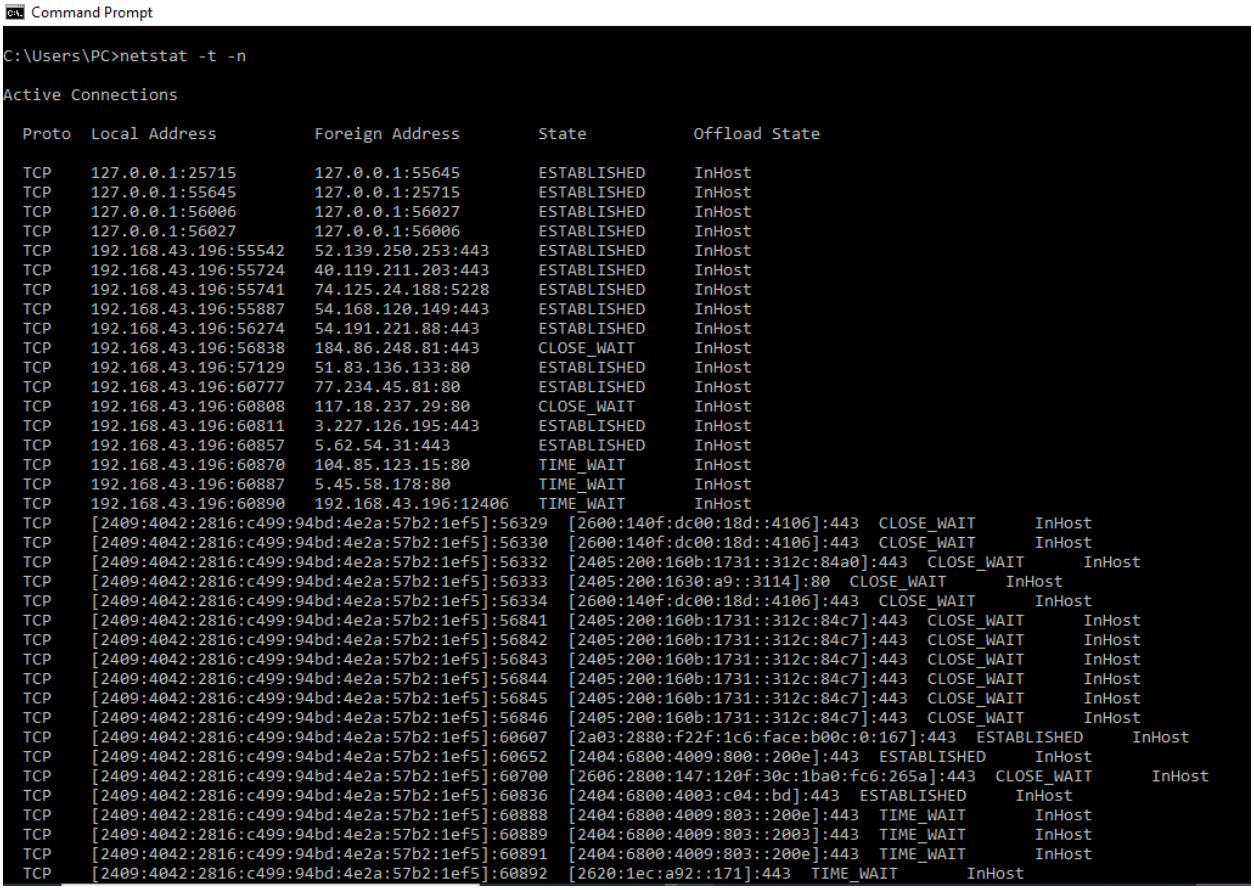
Command Prompt

```
  TCP    192.168.43.196:60808   117.18.237.29:http     CLOSE_WAIT
  TCP    192.168.43.196:60811   ec2-3-227-126-195:https  ESTABLISHED
  TCP    192.168.43.196:60857   5.62.54.31:https       ESTABLISHED
  TCP    192.168.43.196:60867   160:https              TIME_WAIT
  TCP    192.168.43.196:60869   20.44.239.154:https    TIME_WAIT
  TCP    192.168.43.196:60870   a104-85-123-15:http    TIME_WAIT
  TCP    192.168.43.196:60876   i1:https               TIME_WAIT
  TCP    192.168.43.196:60877   i1:https               TIME_WAIT
  TCP    192.168.43.196:60887   r-178-58-45-5:http     FIN_WAIT_1
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:56329  g2600-140f-dc00-018d-0000-0000-0000-4106:https  CLOSE_WAIT
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:56330  g2600-140f-dc00-018d-0000-0000-0000-4106:https  CLOSE_WAIT
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:56332  [2405:200:160b:1731::312c:84a0]:https  CLOSE_WAIT
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:56333  [2405:200:1630:a9::3114]:http  CLOSE_WAIT
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:56334  g2600-140f-dc00-018d-0000-0000-0000-4106:https  CLOSE_WAIT
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:56841  [2405:200:160b:1731::312c:84c7]:https  CLOSE_WAIT
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:56842  [2405:200:160b:1731::312c:84c7]:https  CLOSE_WAIT
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:56843  [2405:200:160b:1731::312c:84c7]:https  CLOSE_WAIT
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:56844  [2405:200:160b:1731::312c:84c7]:https  CLOSE_WAIT
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:56845  [2405:200:160b:1731::312c:84c7]:https  CLOSE_WAIT
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:56846  [2405:200:160b:1731::312c:84c7]:https  CLOSE_WAIT
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60607  whatsapp-cdn6-shv-02-bom1:https  ESTABLISHED
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60652  bom07s15-in-x0e:https  ESTABLISHED
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60700  [2606:2800:147:120f:30c:1ba0:fc6:265a]:https  CLOSE_WAIT
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60836  [2404:6800:4003:c04::bd]:https  ESTABLISHED
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60858  bom05s11-in-x0e:https  TIME_WAIT
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60860  bom07s24-in-x0e:https  TIME_WAIT
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60862  bom07s24-in-x0e:https  TIME_WAIT
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60863  bom05s09-in-x04:https  TIME_WAIT
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60864  bom07s12-in-x0a:https  TIME_WAIT
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60865  bom07s12-in-x0a:https  TIME_WAIT
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60866  bom07s10-in-x0e:https  TIME_WAIT
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60868  [2620:1ec:a92::171]:https  TIME_WAIT
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60871  bom05s09-in-x04:https  TIME_WAIT
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60873  bom07s24-in-x0e:https  TIME_WAIT
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60874  bom07s16-in-x16:https  TIME_WAIT
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60875  upload-lb:https        TIME_WAIT
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60878  bom05s09-in-x04:https  TIME_WAIT
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60879  bom07s24-in-x0e:https  TIME_WAIT
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60880  bom07s10-in-x0e:https  TIME_WAIT
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60881  [2620:1ec:a92::171]:https  TIME_WAIT
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60882  bom05s09-in-x04:https  TIME_WAIT
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60884  bom07s24-in-x0e:https  TIME_WAIT
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60885  [2606:4700:8d7c:b510:bfde:30:c180:a667]:https  TIME_WAIT
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60886  bom07s10-in-x0e:https  TIME_WAIT
```

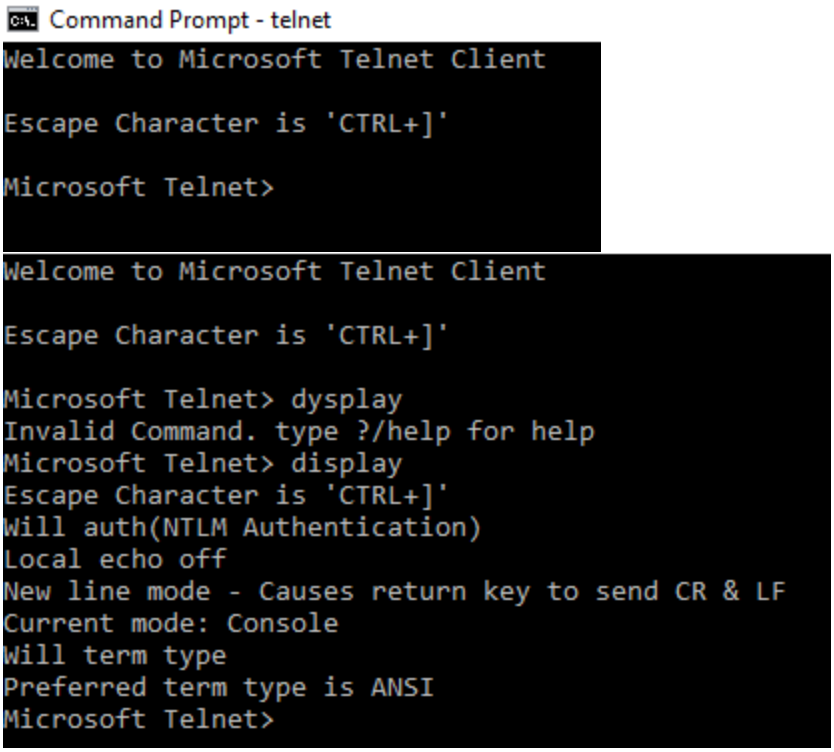

Command Prompt
C:\Users\PC>netstat -t -n
Active Connections
Proto Local Address Foreign Address State Offload State
TCP 127.0.0.1:25715 127.0.0.1:55645 ESTABLISHED InHost
TCP 127.0.0.1:55645 127.0.0.1:25715 ESTABLISHED InHost
TCP 127.0.0.1:56006 127.0.0.1:56027 ESTABLISHED InHost
TCP 127.0.0.1:56027 127.0.0.1:56006 ESTABLISHED InHost
TCP 192.168.43.196:55542 52.139.250.253:443 ESTABLISHED InHost
TCP 192.168.43.196:55724 40.119.211.203:443 ESTABLISHED InHost
TCP 192.168.43.196:55741 74.125.24.188:5228 ESTABLISHED InHost
TCP 192.168.43.196:55887 54.168.120.149:443 ESTABLISHED InHost
TCP 192.168.43.196:56274 54.191.221.88:443 ESTABLISHED InHost
TCP 192.168.43.196:56838 184.86.248.81:443 CLOSE_WAIT InHost
TCP 192.168.43.196:57129 51.83.136.133:80 ESTABLISHED InHost
TCP 192.168.43.196:60777 77.234.45.81:80 ESTABLISHED InHost
TCP 192.168.43.196:60808 117.18.237.29:80 CLOSE_WAIT InHost
TCP 192.168.43.196:60811 3.227.126.195:443 ESTABLISHED InHost
TCP 192.168.43.196:60857 5.62.54.31:443 ESTABLISHED InHost
TCP 192.168.43.196:60870 104.85.123.15:80 TIME_WAIT InHost
TCP 192.168.43.196:60876 192.0.77.2:443 TIME_WAIT InHost
TCP 192.168.43.196:60877 192.0.77.2:443 TIME_WAIT InHost
TCP 192.168.43.196:60887 5.45.58.178:80 TIME_WAIT InHost
TCP 192.168.43.196:60890 192.168.43.196:12406 TIME_WAIT InHost
TCP [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:56329 [2600:140f:dc00:18d::4106]:443 CLOSE_WAIT InHost
TCP [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:56330 [2600:140f:dc00:18d::4106]:443 CLOSE_WAIT InHost
TCP [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:56332 [2405:200:160b:1731::312c:84a0]:443 CLOSE_WAIT InHost
TCP [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:56333 [2405:200:1630:a9::3114]:80 CLOSE_WAIT InHost
TCP [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:56334 [2600:140f:dc00:18d::4106]:443 CLOSE_WAIT InHost
TCP [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:56841 [2405:200:160b:1731::312c:84c7]:443 CLOSE_WAIT InHost
TCP [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:56842 [2405:200:160b:1731::312c:84c7]:443 CLOSE_WAIT InHost
TCP [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:56843 [2405:200:160b:1731::312c:84c7]:443 CLOSE_WAIT InHost
TCP [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:56844 [2405:200:160b:1731::312c:84c7]:443 CLOSE_WAIT InHost
TCP [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:56845 [2405:200:160b:1731::312c:84c7]:443 CLOSE_WAIT InHost
TCP [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:56846 [2405:200:160b:1731::312c:84c7]:443 CLOSE_WAIT InHost
TCP [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60607 [2a03:2880:f22f:1c6:face:b00c:0:167]:443 ESTABLISHED InHost
TCP [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60652 [2404:6800:4009:800::200e]:443 ESTABLISHED InHost
TCP [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60700 [2606:2800:147:120f:30c:1ba0:fc6:265a]:443 CLOSE_WAIT InHost
TCP [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60836 [2404:6800:4003:c04::bd]:443 ESTABLISHED InHost
TCP [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60871 [2404:6800:4009:805::2004]:443 TIME_WAIT InHost
TCP [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60873 [2404:6800:4009:814::200e]:443 TIME_WAIT InHost
TCP [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60874 [2404:6800:4009:80b::2016]:443 TIME_WAIT InHost

Command Prompt

```
  TCP    192.168.43.196:55741   74.125.24.188:5228     ESTABLISHED     InHost
  TCP    192.168.43.196:55887   54.168.120.149:443     ESTABLISHED     InHost
  TCP    192.168.43.196:56274   54.191.221.88:443      ESTABLISHED     InHost
  TCP    192.168.43.196:56838   184.86.248.81:443      CLOSE_WAIT      InHost
  TCP    192.168.43.196:57129   51.83.136.133:80       ESTABLISHED     InHost
  TCP    192.168.43.196:60777   77.234.45.81:80        ESTABLISHED     InHost
  TCP    192.168.43.196:60808   117.18.237.29:80       CLOSE_WAIT      InHost
  TCP    192.168.43.196:60811   3.227.126.195:443      ESTABLISHED     InHost
  TCP    192.168.43.196:60857   5.62.54.31:443         ESTABLISHED     InHost
  TCP    192.168.43.196:60870   104.85.123.15:80       TIME_WAIT       InHost
  TCP    192.168.43.196:60876   192.0.77.2:443         TIME_WAIT       InHost
  TCP    192.168.43.196:60877   192.0.77.2:443         TIME_WAIT       InHost
  TCP    192.168.43.196:60887   5.45.58.178:80         TIME_WAIT       InHost
  TCP    192.168.43.196:60890   192.168.43.196:12406   TIME_WAIT       InHost
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:56329  [2600:140f:dc00:18d::4106]:443  CLOSE_WAIT      InHost
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:56330  [2600:140f:dc00:18d::4106]:443  CLOSE_WAIT      InHost
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:56332  [2405:200:160b:1731::312c:84a0]:443  CLOSE_WAIT      InHost
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:56333  [2405:200:1630:a9::3114]:80  CLOSE_WAIT      InHost
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:56334  [2600:140f:dc00:18d::4106]:443  CLOSE_WAIT      InHost
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:56841  [2405:200:160b:1731::312c:84c7]:443  CLOSE_WAIT      InHost
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:56842  [2405:200:160b:1731::312c:84c7]:443  CLOSE_WAIT      InHost
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:56843  [2405:200:160b:1731::312c:84c7]:443  CLOSE_WAIT      InHost
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:56844  [2405:200:160b:1731::312c:84c7]:443  CLOSE_WAIT      InHost
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:56845  [2405:200:160b:1731::312c:84c7]:443  CLOSE_WAIT      InHost
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:56846  [2405:200:160b:1731::312c:84c7]:443  CLOSE_WAIT      InHost
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60607  [2a03:2880:f22f:1c6:face:b00c:0:167]:443  ESTABLISHED     InHost
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60652  [2404:6800:4009:800::200e]:443  ESTABLISHED     InHost
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60700  [2606:2800:147:120f:30c:1ba0:fc6:265a]:443  CLOSE_WAIT      InHost
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60836  [2404:6800:4003:c04::bd]:443  ESTABLISHED     InHost
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60871  [2404:6800:4009:805::2004]:443  TIME_WAIT       InHost
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60873  [2404:6800:4009:814::200e]:443  TIME_WAIT       InHost
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60874  [2404:6800:4009:80b::2016]:443  TIME_WAIT       InHost
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60875  [2001:df2:e500:ed1a::2:b]:443  TIME_WAIT       InHost
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60878  [2404:6800:4009:805::2004]:443  TIME_WAIT       InHost
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60879  [2404:6800:4009:814::200e]:443  TIME_WAIT       InHost
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60880  [2404:6800:4009:801::200e]:443  TIME_WAIT       InHost
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60881  [2620:1ec:a92::171]:443  TIME_WAIT       InHost
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60882  [2404:6800:4009:805::2004]:443  TIME_WAIT       InHost
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60884  [2404:6800:4009:814::200e]:443  TIME_WAIT       InHost
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60885  [2606:4700:8d7c:b510:bfde:30:c180:a667]:443  TIME_WAIT       InHost
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60886  [2404:6800:4009:801::200e]:443  TIME_WAIT       InHost
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60888  [2404:6800:4009:803::200e]:443  TIME_WAIT       InHost
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60889  [2404:6800:4009:803::2003]:443  TIME_WAIT       InHost
  TCP    [2409:4042:2816:c499:94bd:4e2a:57b2:1ef5]:60891  [2404:6800:4009:803::200e]:443  TIME_WAIT       InHost
```



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

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

2. mscs.mu.edu

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

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

  1     2 ms     2 ms     2 ms  192.168.43.1
  2     *        *        *     Request timed out.
  3    52 ms    46 ms    46 ms  10.72.218.138
  4    51 ms    50 ms    37 ms  172.25.101.187
  5    57 ms    69 ms    68 ms  172.25.101.190
  6    54 ms    60 ms    51 ms  172.17.120.7
  7    43 ms    93 ms    76 ms  172.17.120.73
  8    65 ms    62 ms    74 ms  172.16.92.147
  9   114 ms    88 ms    49 ms  172.16.24.30
 10    64 ms    76 ms    66 ms  172.16.2.48
 11   173 ms   173 ms   184 ms  103.198.140.54
 12   182 ms   161 ms   203 ms  103.198.140.54
 13   182 ms   202 ms   188 ms  hurricane-electric.telecity2.nl-ix.net [193.239.116.14]
 14   201 ms   194 ms   196 ms  100ge8-1.core1.lon3.he.net [184.104.193.193]
 15   184 ms   197 ms   196 ms  100ge14-1.core1.lon2.he.net [184.105.64.237]
 16   537 ms   318 ms   246 ms  100ge13-2.core1.nyc4.he.net [72.52.92.166]
 17   293 ms   268 ms     *     100ge2-1.core2.chi1.he.net [184.104.193.173]
 18     *        *        *     Request timed out.
 19   292 ms   284 ms   286 ms  r-222wwash-isp-ae6-3926.wiscnet.net [140.189.8.126]
 20   294 ms   278 ms   298 ms  r-milwaukeeci-809-isp-ae3-0.wiscnet.net [140.189.8.230]
 21   293 ms   266 ms   287 ms  MarquetteUniv.site.wiscnet.net [216.56.1.202]
 22   296 ms   268 ms   263 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.
```

3. www.cs.grinnell.edu

```
C:\Users\PC>tracert www.cs.grinnell.edu

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

  1     1 ms     1 ms     1 ms  192.168.43.1
  2     *        *        *     Request timed out.
  3    46 ms    43 ms    63 ms  10.72.216.10
  4    35 ms    50 ms    40 ms  172.25.101.191
  5    43 ms    65 ms    56 ms  172.25.101.190
  6     *       57 ms    54 ms  172.17.120.7
  7    37 ms    45 ms    48 ms  172.17.120.73
  8    60 ms    99 ms    90 ms  172.26.40.5
  9    63 ms    76 ms    63 ms  172.16.24.8
 10    90 ms    79 ms    65 ms  172.16.2.46
 11   172 ms   169 ms   181 ms  103.198.140.29
 12   160 ms   157 ms   178 ms  103.198.140.29
 13   170 ms   179 ms   179 ms  hurricane-electric.telecity2.nl-ix.net [193.239.116.14]
 14   180 ms   191 ms   187 ms  100ge8-1.core1.lon3.he.net [184.104.193.193]
 15     *      189 ms   189 ms  100ge14-1.core1.lon2.he.net [184.105.64.237]
 16     *      341 ms   326 ms  100ge13-2.core1.nyc4.he.net [72.52.92.166]
 17     *      520 ms   278 ms  100ge9-1.core2.chi1.he.net [184.105.223.161]
 18   294 ms   279 ms   274 ms  100ge14-2.core1.msp1.he.net [184.105.223.178]
 19   304 ms   304 ms   297 ms  aureon-network-services-inc.e0-26.switch1.msp1.he.net [216.66.77.218]
 20   325 ms   303 ms   302 ms  peer-as5056.br02.msp1.tfbnw.net [157.240.76.37]
 21   288 ms   287 ms   295 ms  167.142.58.40
 22   289 ms   333 ms   287 ms  67.224.64.62
 23   291 ms   296 ms   306 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.
```

4. csail.mit.edu

```
C:\Users\PC>tracert csail.mit.edu

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

  1     2 ms     3 ms     2 ms  192.168.43.1
  2     *        *        *     Request timed out.
  3    57 ms    53 ms    75 ms  10.72.216.10
  4    46 ms    55 ms    57 ms  172.25.101.189
  5    55 ms    53 ms    46 ms  172.25.101.188
  6    62 ms    56 ms    56 ms  172.17.120.7
  7    60 ms    62 ms    50 ms  172.17.120.73
  8    77 ms    77 ms    75 ms  172.16.92.145
  9   112 ms     *       60 ms  172.16.24.8
 10    79 ms    66 ms    78 ms  172.16.2.46
 11    87 ms    79 ms    93 ms  172.25.41.167
 12    70 ms    75 ms    75 ms  49.45.4.251
 13   298 ms   297 ms   292 ms  49.45.4.103
 14   298 ms   291 ms   286 ms  49.45.4.86
 15   310 ms   301 ms   294 ms  4.7.26.61
 16     *        *        *     Request timed out.
 17   371 ms   358 ms   477 ms  MASSACHUSET.bear1.Boston1.Level3.net [4.53.48.98]
 18   352 ms   364 ms   356 ms  dmz-rtr-1-external-rtr-1.mit.edu [18.0.161.17]
 19   362 ms   350 ms   359 ms  dmz-rtr-2-dmz-rtr-1-1.mit.edu [18.0.161.6]
 20   351 ms   362 ms   364 ms  mitnet.core-1-ext.csail.mit.edu [18.4.7.65]
 21     *        *        *     Request timed out.
 22   354 ms   354 ms   366 ms  bdr.core-1.csail.mit.edu [128.30.0.246]
 23   364 ms     *        *     inquir-3ld.csail.mit.edu [128.30.2.109]
 24   351 ms   396 ms   365 ms  inquir-3ld.csail.mit.edu [128.30.2.109]

Trace complete.
```

5. cs.stanford.edu

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

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

  1     2 ms     2 ms     3 ms  192.168.43.1
  2     *        *        *     Request timed out.
  3    55 ms    56 ms    46 ms  10.72.216.10
  4    57 ms    66 ms    56 ms  172.25.101.185
  5    87 ms    42 ms    50 ms  172.25.101.188
  6    42 ms    46 ms    51 ms  172.17.120.7
  7    57 ms    57 ms    66 ms  172.17.120.77
  8    63 ms    57 ms    78 ms  172.26.40.5
  9   112 ms   136 ms    84 ms  172.16.24.10
 10    73 ms    66 ms    74 ms  172.16.2.46
 11   184 ms   196 ms   182 ms  103.198.140.54
 12   189 ms   192 ms   186 ms  103.198.140.54
 13   228 ms   190 ms   188 ms  hurricane-electric.telecity2.nl-ix.net [193.239.116.14]
 14   205 ms   205 ms   206 ms  100ge8-1.core1.lon3.he.net [184.104.193.193]
 15   202 ms   200 ms   199 ms  100ge14-1.core1.lon2.he.net [184.105.64.237]
 16   265 ms   256 ms   332 ms  100ge13-2.core1.nyc4.he.net [72.52.92.166]
 17   310 ms   368 ms     *     100ge8-1.core1.sjc2.he.net [184.105.81.218]
 18   303 ms   327 ms   339 ms  100ge1-1.core1.pao1.he.net [72.52.92.158]
 19   339 ms   321 ms   318 ms  stanford-university.100gigabitethernet5-1.core1.pao1.he.net [184.105.177.238]
 20   327 ms   349 ms   327 ms  csee-west-rtr-vl3.SUNet [171.66.255.140]
 21   340 ms   336 ms   320 ms  CS.stanford.edu [171.64.64.64]

Trace complete.
```

6. cs.manchester.ac.uk

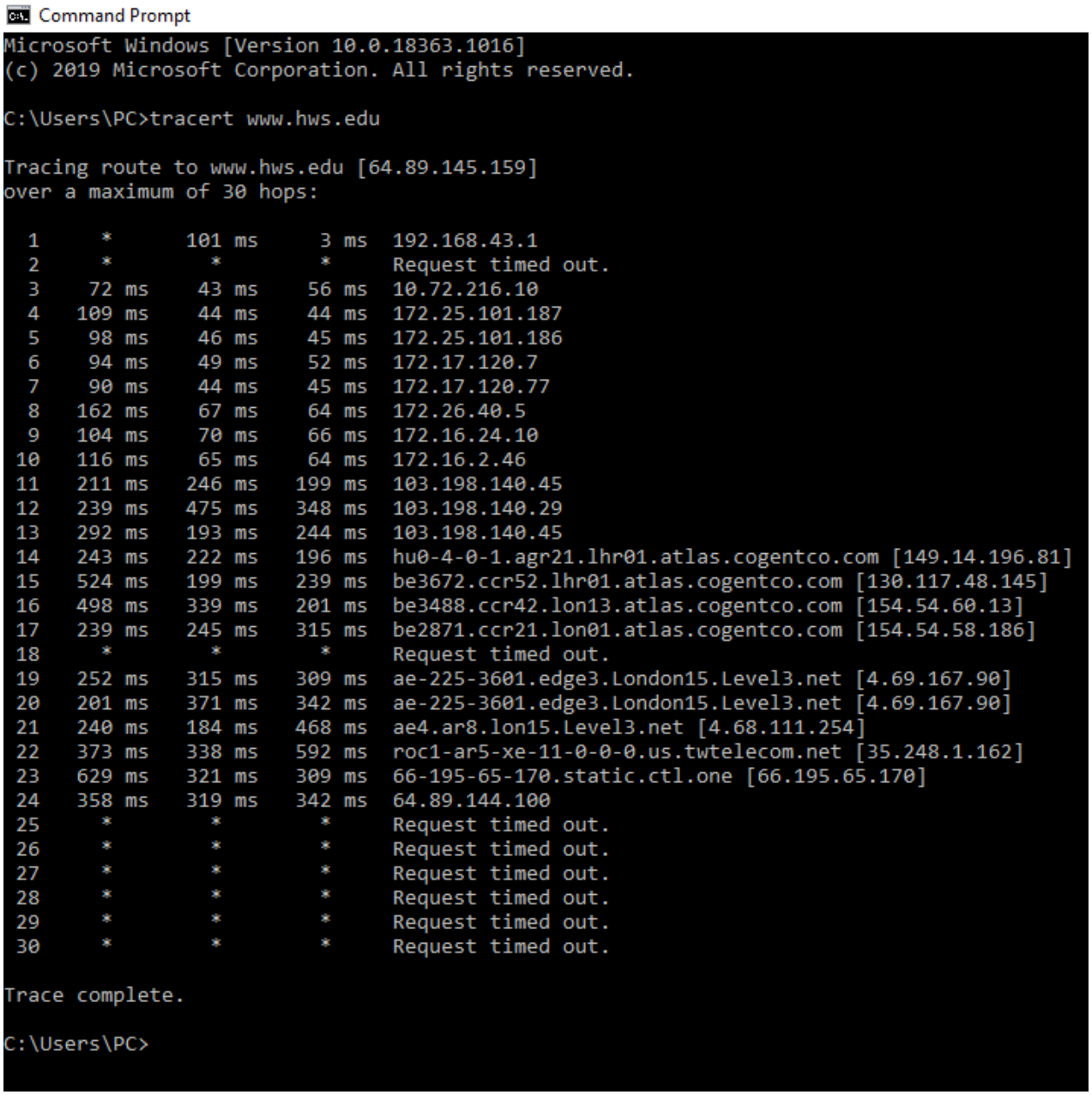
```
C:\Users\PC>tracert cs.manchester.ac.uk

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

  1     2 ms     1 ms     2 ms  192.168.43.1
  2     *        *        *     Request timed out.
  3    54 ms    54 ms    54 ms  10.72.216.10
  4    40 ms    65 ms    43 ms  172.25.101.187
  5    57 ms    70 ms    43 ms  172.25.101.186
  6    46 ms    76 ms    48 ms  172.17.120.7
  7    49 ms    46 ms    45 ms  172.17.120.77
  8    74 ms    78 ms    65 ms  172.16.92.145
  9    65 ms     *       67 ms  172.16.24.10
 10    62 ms    76 ms     *     172.16.2.46
 11   205 ms   173 ms   187 ms  103.198.140.45
 12   196 ms   235 ms   197 ms  103.198.140.56
 13     *      220 ms   215 ms  103.198.140.107
 14   202 ms   215 ms   208 ms  103.198.140.45
 15   203 ms   186 ms   206 ms  hu0-4-0-1.agr21.lhr01.atlas.cogentco.com [149.14.196.81]
 16   207 ms   219 ms   214 ms  be3672.ccr52.lhr01.atlas.cogentco.com [130.117.48.145]
 17   208 ms   192 ms     *     be3488.ccr42.lon13.atlas.cogentco.com [154.54.60.13]
 18   192 ms   212 ms   200 ms  be2871.ccr21.lon01.atlas.cogentco.com [154.54.58.186]
 19   314 ms   196 ms   189 ms  ldn-b1-link.telia.net [62.115.9.28]
 20     *        *        *     Request timed out.
 21   185 ms     *        *     ldn-b2-link.telia.net [62.115.120.239]
 22   179 ms   195 ms   197 ms  jisc-ic-345131-ldn-b4.c.telia.net [62.115.175.131]
 23   198 ms   253 ms   200 ms  ae24.londhx-sbr1.ja.net [146.97.35.197]
 24   199 ms   197 ms   304 ms  ae29.londpg-sbr2.ja.net [146.97.33.2]
 25   189 ms   186 ms   199 ms  ae31.erdiss-sbr2.ja.net [146.97.33.22]
 26   189 ms   198 ms   217 ms  ae29.manckh-sbr2.ja.net [146.97.33.42]
 27   197 ms   199 ms   196 ms  ae23.mancrh-rbr1.ja.net [146.97.38.42]
 28     *        *        *     Request timed out.
 29   176 ms   202 ms   441 ms  130.88.249.194
 30     *        *        *     Request timed out.

Trace complete.
```

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).

Exercise 2: (Very short.) Use traceroute to trace the route from your computer to math.hws.edu and to www.hws.edu. Explain the difference in the results.

```
C:\Users\PC>tracert math.hws.edu

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

  1     3 ms     3 ms     2 ms  192.168.43.1
  2     *        *        *     Request timed out.
  3    59 ms    57 ms    46 ms  10.72.216.10
  4    59 ms    58 ms    51 ms  172.25.101.189
  5    52 ms    45 ms    86 ms  172.25.101.184
  6    57 ms    48 ms    58 ms  172.17.120.7
  7    59 ms    54 ms    48 ms  172.17.120.73
  8    77 ms    72 ms    77 ms  172.16.92.147
  9    97 ms    74 ms    63 ms  172.16.24.30
 10    64 ms    67 ms    71 ms  172.16.2.48
 11   322 ms   187 ms   186 ms  103.198.140.45
 12   212 ms   196 ms   203 ms  103.198.140.54
 13   183 ms   192 ms   182 ms  103.198.140.45
 14   235 ms   185 ms   192 ms  hu0-4-0-1.agr21.lhr01.atlas.cogentco.com [149.14.196.81]
 15   184 ms   198 ms   197 ms  be3672.ccr52.lhr01.atlas.cogentco.com [130.117.48.145]
 16   190 ms   171 ms   183 ms  be3488.ccr42.lon13.atlas.cogentco.com [154.54.60.13]
 17   194 ms   186 ms   196 ms  be2871.ccr21.lon01.atlas.cogentco.com [154.54.58.186]
 18     *        *        *     Request timed out.
 19   193 ms   218 ms     *     ae-228-3604.edge3.London15.Level3.net [4.69.167.102]
 20   185 ms   199 ms   185 ms  ae-228-3604.edge3.London15.Level3.net [4.69.167.102]
 21   186 ms   432 ms   185 ms  ae4.ar8.lon15.Level3.net [4.68.111.254]
 22   310 ms   341 ms   311 ms  roc1-ar5-xe-11-0-0-0.us.twtelecom.net [35.248.1.162]
 23   312 ms   339 ms   314 ms  66-195-65-170.static.ctl.one [66.195.65.170]
 24   307 ms   336 ms   306 ms  nat.hws.edu [64.89.144.100]
 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\PC>
```



. A URL with the www prefix is technically a subdomain, so it's possible that traces to demo.com and www.demo.com follow two very different paths.

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 and then math.hws.edu 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

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\PC>tracert cs.stanford.edu

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

  1     4 ms     4 ms     5 ms  192.168.43.1
  2     *        *        *     Request timed out.
  3   104 ms    60 ms     *     10.72.218.138
  4    83 ms    64 ms    50 ms  172.25.101.189
  5    70 ms     *       90 ms  172.25.101.188
  6   114 ms    59 ms    56 ms  172.17.120.7
  7    46 ms    50 ms    55 ms  172.17.120.77
  8   204 ms   106 ms    66 ms  172.16.92.147
  9   120 ms    81 ms    93 ms  172.16.24.32
 10   127 ms    74 ms    73 ms  172.16.2.48
 11   407 ms   182 ms   457 ms  103.198.140.29
 12   230 ms   193 ms   250 ms  103.198.140.29
 13   497 ms   326 ms   295 ms  hurricane-electric.telecity2.nl-ix.net [193.239.116.14]
 14   276 ms   337 ms   224 ms  100ge8-1.core1.lon3.he.net [184.104.193.193]
 15   337 ms   501 ms   316 ms  100ge14-1.core1.lon2.he.net [184.105.64.237]
 16   569 ms   320 ms   251 ms  100ge13-2.core1.nyc4.he.net [72.52.92.166]
 17   574 ms   316 ms   314 ms  100ge8-1.core1.sjc2.he.net [184.105.81.218]
 18   361 ms   525 ms   316 ms  10ge4-5.core1.pao1.he.net [72.52.92.69]
 19   574 ms   325 ms   317 ms  stanford-university.100gigabitethernet5-1.core1.pao1.he.net [184.105.177.238]
 20   548 ms   318 ms   312 ms  csee-west-rtr-vl3.SUNet [171.66.255.140]
 21   570 ms   316 ms   314 ms  CS.stanford.edu [171.64.64.64]

Trace complete.
```

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

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

  1     4 ms     2 ms     5 ms  192.168.43.1
  2     *        *        *     Request timed out.
  3    86 ms    44 ms    47 ms  10.72.218.138
  4   105 ms    56 ms    43 ms  172.25.101.189
  5   101 ms    44 ms    46 ms  172.25.101.188
  6   103 ms    48 ms    47 ms  172.17.120.7
  7   100 ms    46 ms    68 ms  172.17.120.77
  8    88 ms    51 ms    73 ms  172.16.92.147
  9   124 ms    85 ms    90 ms  172.16.24.32
 10   114 ms    82 ms    63 ms  172.16.2.48
 11   315 ms   303 ms   317 ms  103.198.140.29
 12   234 ms   321 ms   305 ms  103.198.140.29
 13   541 ms   315 ms   310 ms  hurricane-electric.telecity2.nl-ix.net [193.239.116.14]
 14   268 ms   315 ms   309 ms  100ge8-1.core1.lon3.he.net [184.104.193.193]
 15   252 ms   317 ms   310 ms  100ge14-1.core1.lon2.he.net [184.105.64.237]
 16   583 ms   317 ms   308 ms  100ge13-2.core1.nyc4.he.net [72.52.92.166]
 17   392 ms   501 ms   316 ms  100ge8-1.core1.sjc2.he.net [184.105.81.218]
 18   401 ms   488 ms   320 ms  10ge4-5.core1.pao1.he.net [72.52.92.69]
 19   580 ms   320 ms   634 ms  stanford-university.100gigabitethernet5-1.core1.pao1.he.net [184.105.177.238]
 20   327 ms   312 ms   577 ms  csee-west-rtr-vl3.SUNet [171.66.255.140]
 21   509 ms   323 ms   319 ms  CS.stanford.edu [171.64.64.64]

Trace complete.
```

QUESTIONS ABOUT PATHS

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

1. Is any part of the path common for all hosts you tracerouted?
Yes, a particular path is followed from the user's IP address through the IP addresses of the ISP and then the path depends on which access point is ready to respond

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?
Yes , there is a relationship between the number of nodes that show up in the traceroute and the location of the host because 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. It 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

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.

Command Prompt

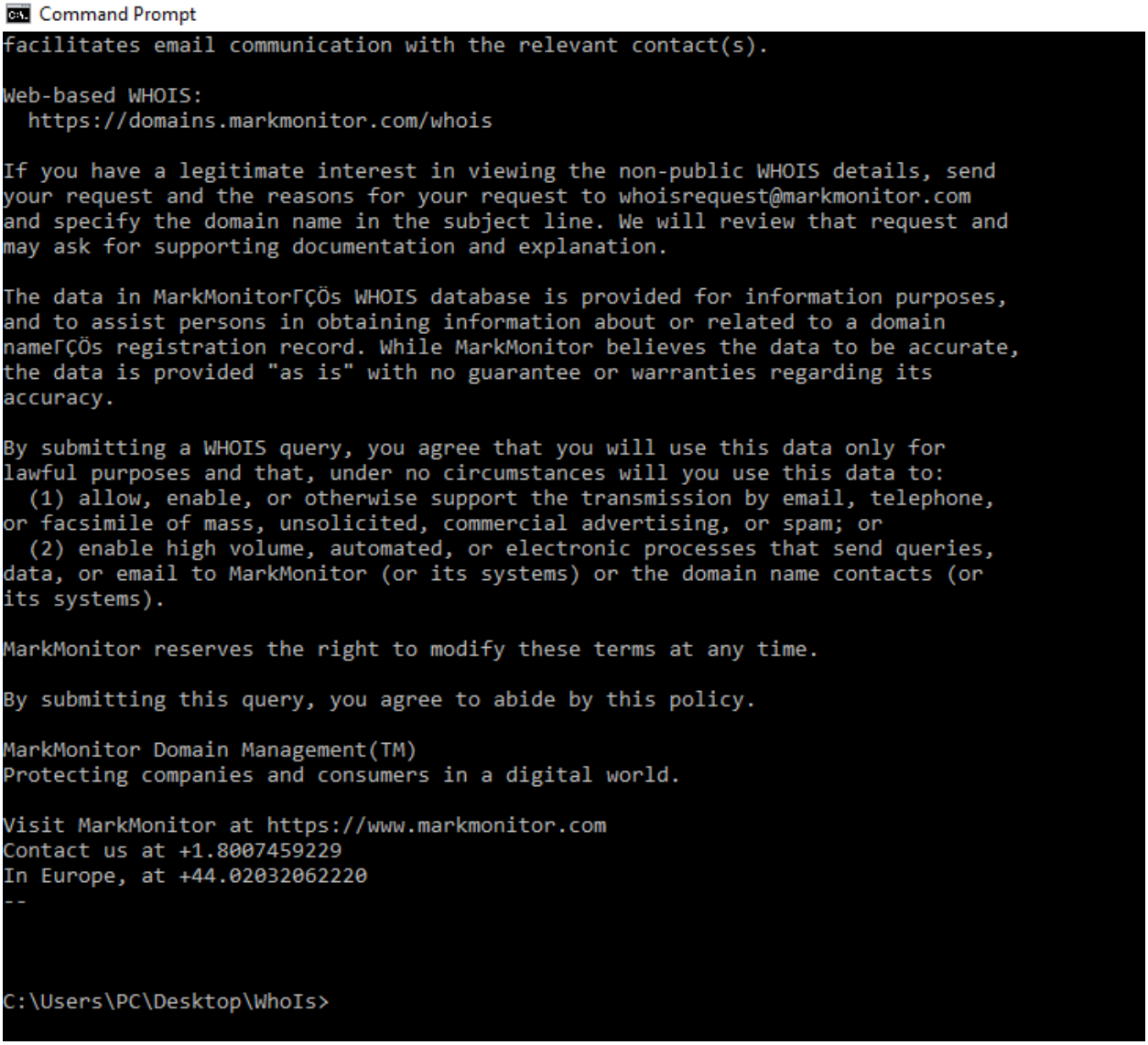
```
C:\Users\PC\Desktop>cd WhoIs

C:\Users\PC\Desktop\WhoIs>whois -v google.com

Whois v1.21 - Domain information lookup
Copyright (C) 2005-2019 Mark Russinovich
Sysinternals - www.sysinternals.com

Connecting to COM.whois-servers.net...
Server COM.whois-servers.net returned the following for GOOGLE.COM

   Domain Name: GOOGLE.COM
   Registry Domain ID: 2138514_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2019-09-09T15:39:04Z
   Creation Date: 1997-09-15T04:00:00Z
   Registry Expiry Date: 2028-09-14T04:00:00Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
   Registrar Abuse Contact Phone: +1.2083895740
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Name Server: NS1.GOOGLE.COM
   Name Server: NS2.GOOGLE.COM
   Name Server: NS3.GOOGLE.COM
   Name Server: NS4.GOOGLE.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2020-08-16T20:55:38Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.
```

Command Prompt

```
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
operational stability.  VeriSign may restrict or terminate your access to the
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.


Connecting to whois.markmonitor.com...
Server whois.markmonitor.com returned the following for GOOGLE.COM

Domain Name: google.com
Registry Domain ID: 2138514_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2019-09-09T08:39:04-0700
Creation Date: 1997-09-15T00:00:00-0700
Registrar Registration Expiration Date: 2028-09-13T00:00:00-0700
```

Command Prompt

```
Creation Date: 1997-09-15T00:00:00-0700
Registrar Registration Expiration Date: 2028-09-13T00:00:00-0700
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895770
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
Domain Status: serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)
Domain Status: serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited)
Domain Status: serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited)
Registrant Organization: Google LLC
Registrant State/Province: CA
Registrant Country: US
Registrant Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com
Admin Organization: Google LLC
Admin State/Province: CA
Admin Country: US
Admin Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com
Tech Organization: Google LLC
Tech State/Province: CA
Tech Country: US
Tech Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com
Name Server: ns4.google.com
Name Server: ns1.google.com
Name Server: ns3.google.com
Name Server: ns2.google.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2020-08-16T13:47:03-0700 <<<

For more information on WHOIS status codes, please visit:
  https://www.icann.org/resources/pages/epp-status-codes

If you wish to contact this domainΓÇÖs Registrant, Administrative, or Technical
contact, and such email address is not visible above, you may do so via our web
form, pursuant to ICANNΓÇÖs Temporary Specification. To verify that you are not a
robot, please enter your email address to receive a link to a page that
facilitates email communication with the relevant contact(s).

Web-based WHOIS:
  https://domains.markmonitor.com/whois
```

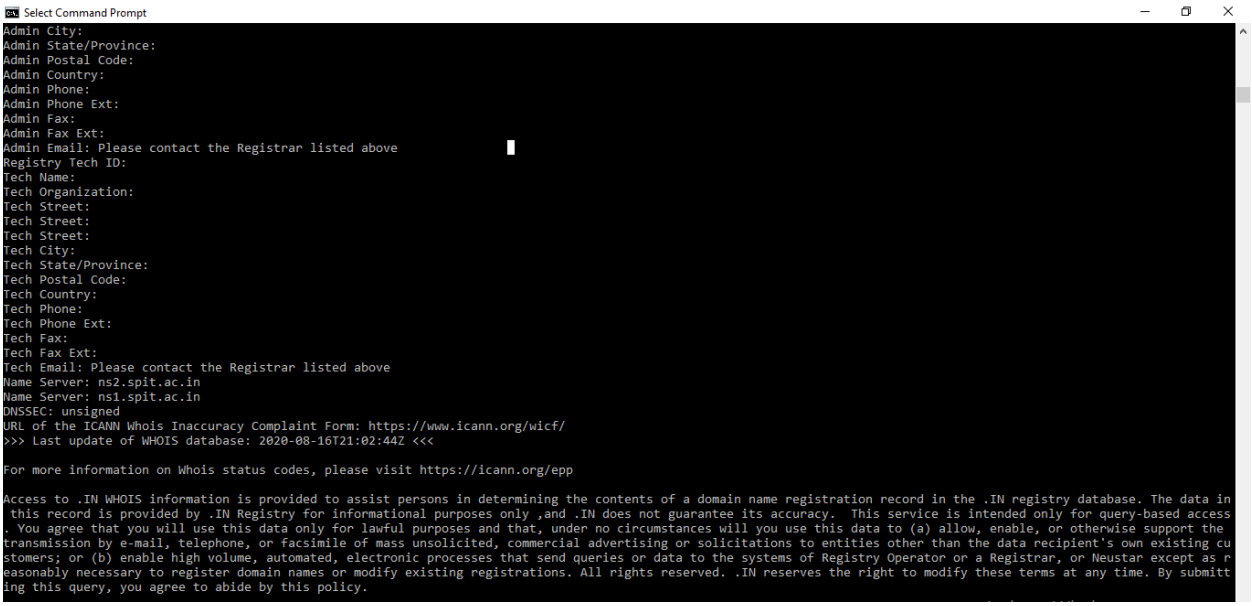


The whois command gives information about the domain name, the Registry Domain ID and some other details such as the details of the Registrar and the Registrant.,domain expiry date., the Registrant Organization , the Registrant State/Province and the Registrant Country .

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.

Command Prompt

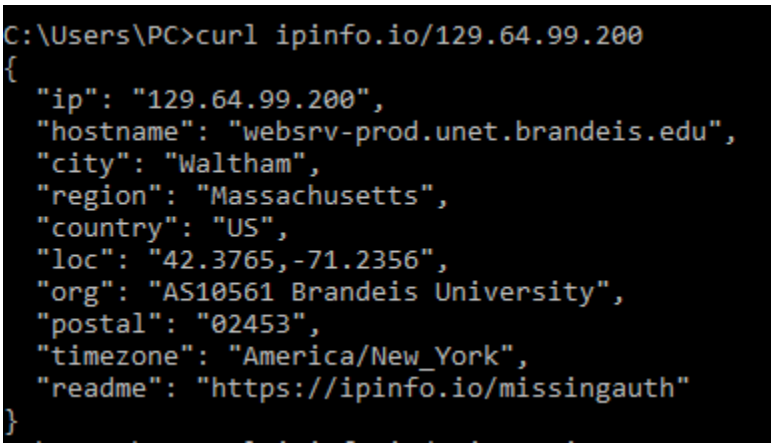
```
C:\Users\PC\Desktop\WhoIs>whois -v spit.ac.in

Whois v1.21 - Domain information lookup
Copyright (C) 2005-2019 Mark Russinovich
Sysinternals - www.sysinternals.com

Connecting to IN.whois-servers.net...
Server IN.whois-servers.net returned the following for SPIT.AC.IN

Domain Name: spit.ac.in
Registry Domain ID: D2241401-IN
Registrar WHOIS Server:
Registrar URL: http://www.ernet.in
Updated Date: 2020-05-18T09:51:15Z
Creation Date: 2006-05-22T04:58:23Z
Registry Expiry Date: 2025-05-22T04:58:23Z
Registrar: ERNET India
Registrar IANA ID: 800068
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: ok http://www.icann.org/epp#OK
Registry Registrant ID:
Registrant Name:
Registrant Organization: Bharatiya Vidya Bhavans Sardar Patel Institute of Technology Mumbai
Registrant Street:
Registrant Street:
Registrant Street:
Registrant City:
Registrant State/Province:
Registrant Postal Code:
Registrant Country: IN
Registrant Phone:
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: Please contact the Registrar listed above
Registry Admin ID:
Admin Name:
Admin Organization:
Admin Street:
Admin Street:
Admin Street:
Admin City:
```



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.)

Conclusion: 1. Learnt about some basic command line network utilities.
2. Learnt about Network Latency, RTT and the factors impacting RTT.