**EXPERIMENT 2**

**NAME: Vishal Shashikant Salvi UID: 2019230069**

**CLASS: TE COMPS BATCH: C**

CEL 51, DCCN, Monsoon 2020

Lab 2: Basic Network Utilities

**Aim:** To study 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 [1]:**

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 response 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>

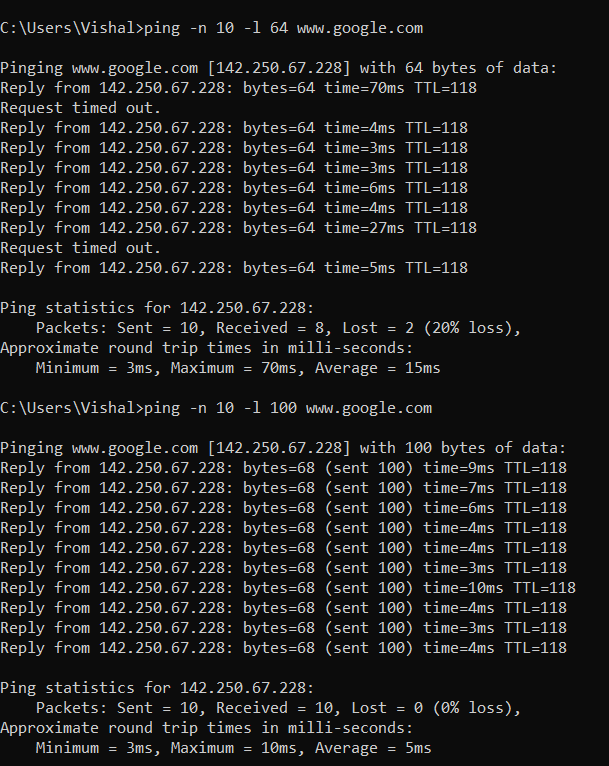
The default number of ICMP packets to send is either infinite (in Linux and Mac OS) or 4 (in Windows). The default packet size is either 64 bytes (in Linux) or 32 bytes (in Windows). You can specify either a hostname (e.g., spit.ac.in) or an IP address.

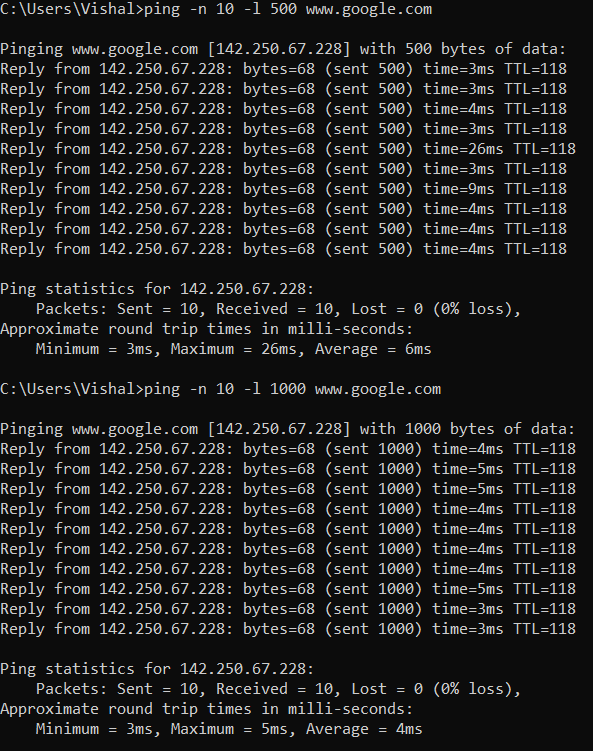
To save the output from ping to a file, include a greater than symbol and a file name at the end of the command. For example:

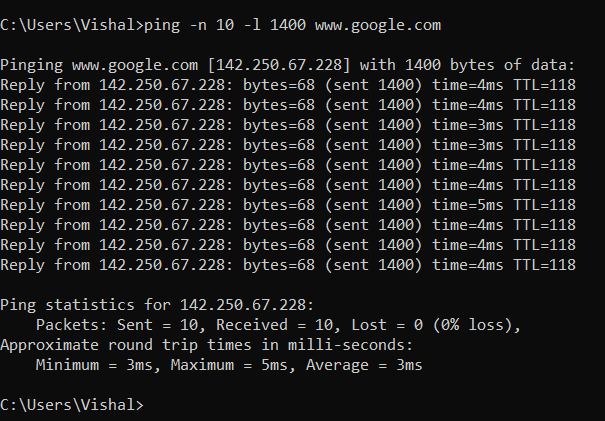
ping -c 10 google.com > ping\_c10\_s64\_google.log

**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







**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?

Yes.

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

Transmission Delay = Data size / bandwidth = (L/B) second

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

Propagation delay = distance/transmission speed = d/s

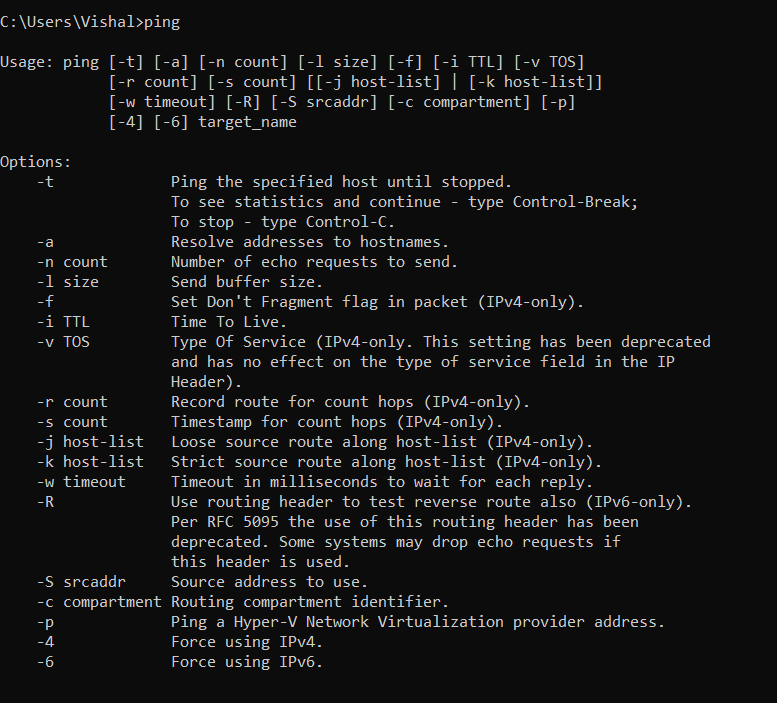
**Queuing Delay :**  
Queuing delay is the time a job waits in a queue until it can be executed. It depends on congestion. It is the time difference between when the packet arrived Destination and when the packet data was processed or executed. It may be caused by mainly three reasons i.e. originating switches, intermediate switches or call receiver servicing switches.

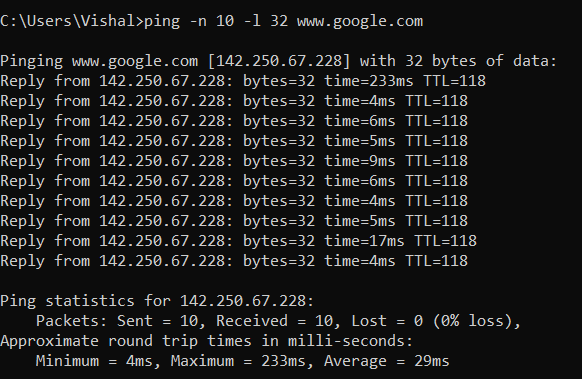
* Distance – The length a signal has to travel correlates with the time taken for a request to reach a server and a response to reach a browser.
* Transmission medium – The medium used to route a signal (e.g., copper wire, fiber optic cables) can impact how quickly a request is received by a server and routed back to a user.
* Number of network hops – 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.
* Traffic levels – RTT typically increases when a network is congested with high levels of traffic. Conversely, low traffic times can result in decreased RTT.

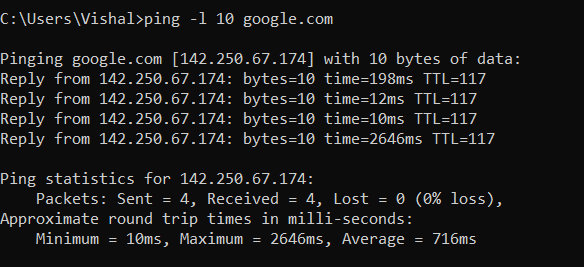
Server response time – The time taken for a target server to respond to a request depends on its processing capacity, the number of requests being handled and the nature of the request (i.e., how much server-side work is required). A longer server response time increases RTT.

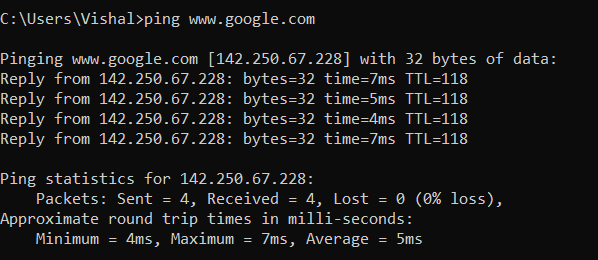
1. Does the average RTT vary with different packet sizes? What aspects of latency (transmit, propagation, and queueing delay) might impact this and why?

Yes ,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.

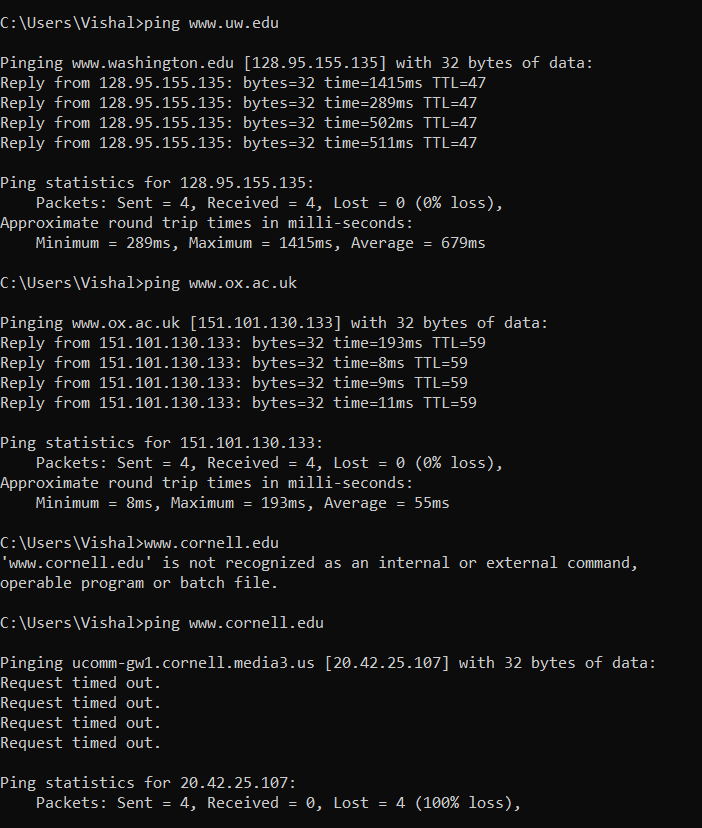


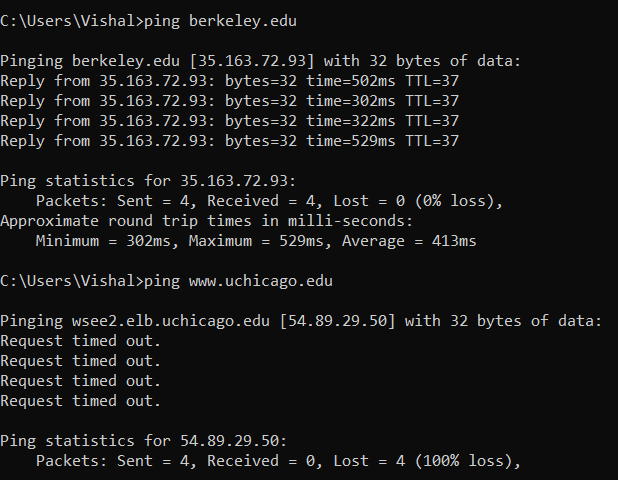






**Exercise 1:** Experiment with ping to find the round trip times to a variety of destinations. Write up any interesting observations, including in particular how the round trip time compares to the physical distance. Here are few places from who to get replies: www.uw.edu, www.cornell.edu, berkeley.edu, www.uchicago.edu, www.ox.ac.uk (England), www.u-tokyo.ac.jp (Japan).





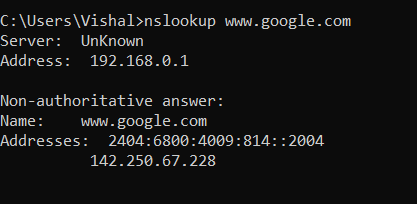
Round-trip time (RTT) is the duration, measured in milliseconds, from when a browser sends a request to when it receives a response from a server. It’s a key performance metric for web applications and one of the main factors, along with Time to First Byte (TTFB), when measuring [page load time](https://www.imperva.com/learn/performance/page-load-time/) and [network latency](https://www.imperva.com/learn/performance/latency/).

RTT is typically measured using a ping a command-line tool that bounces a request off a server and calculates the time taken to reach a user device. Actual RTT may be higher than that measured by the ping due to server throttling and network congestion.

From the above ping command on various site, it is clear that the sites in USA take more Round Trip Time than the ones in UK. So, it is clear that RTT increases with distance.

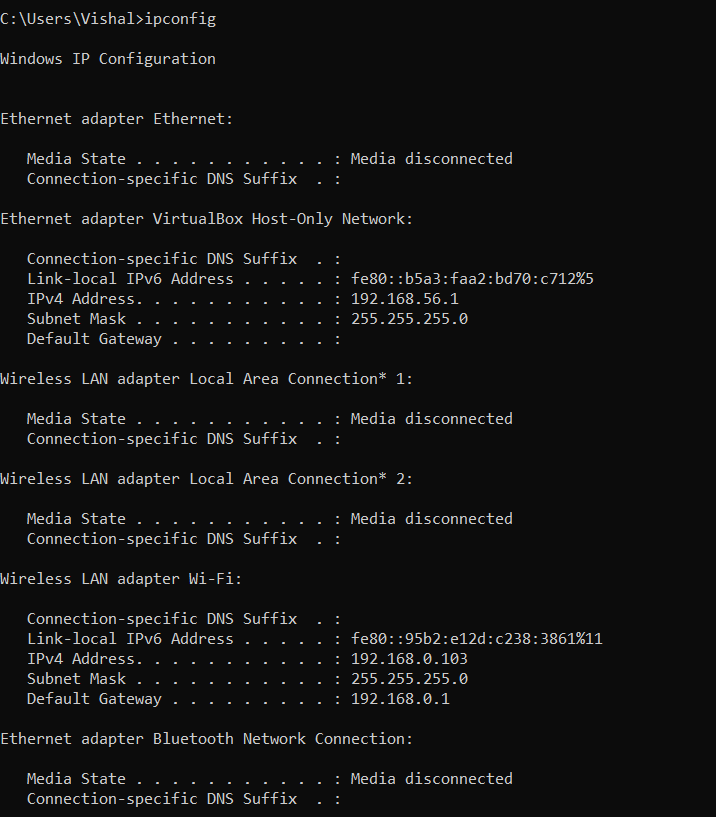
**Nslookup**

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



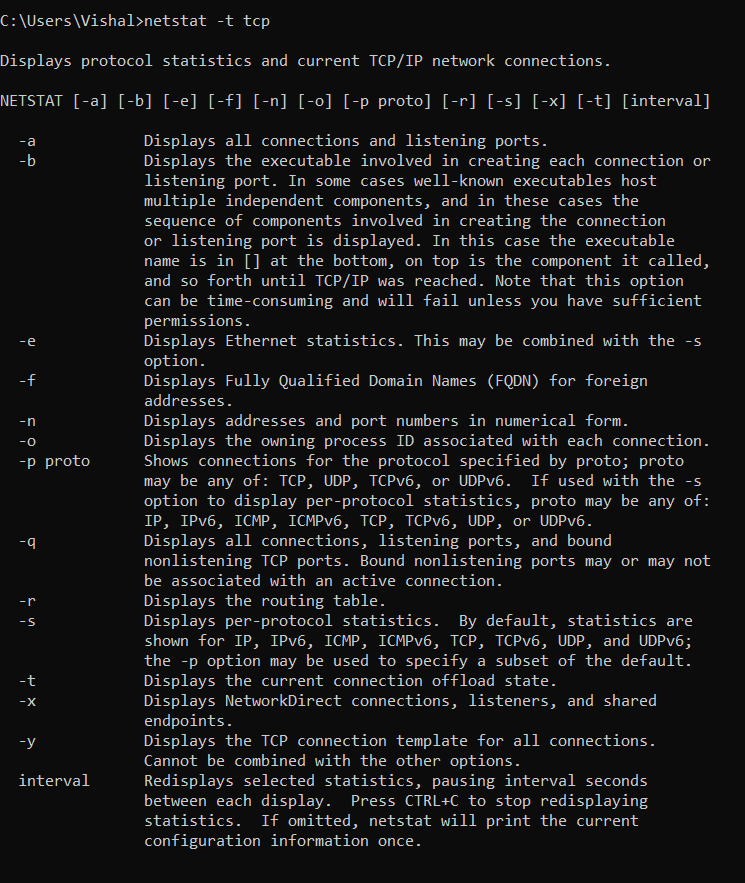
**Ifconfig**

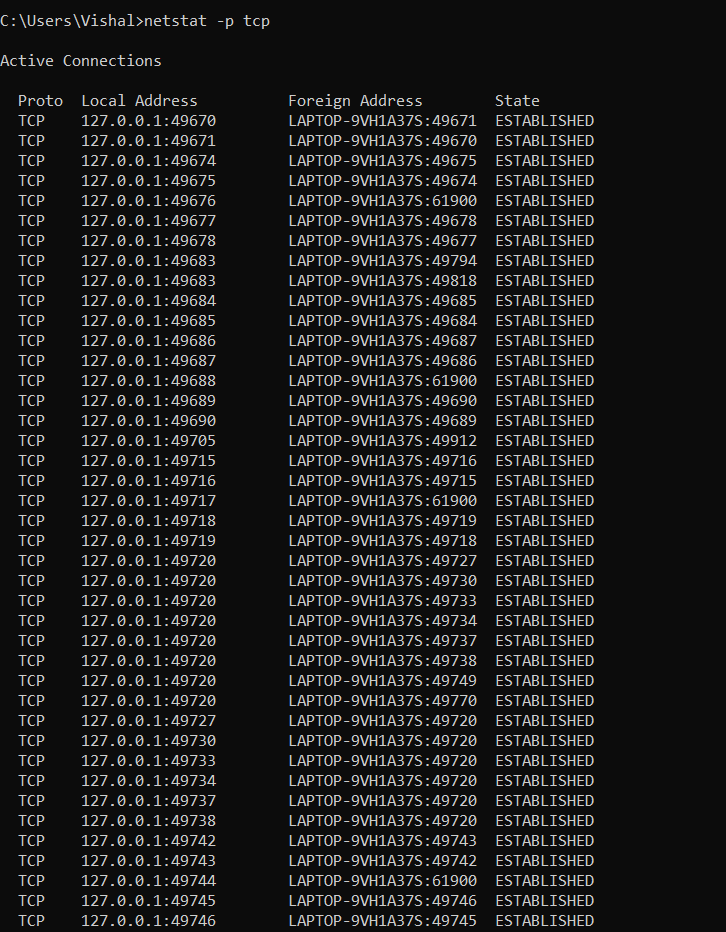
You used ifconfig in the previous lab. When used with no parameters, ifconfig reports some information about the computer's network interfaces. This usually includes lo which stands for localhost; it can be used for communication between programs running on the same computer. Linux often has an interface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

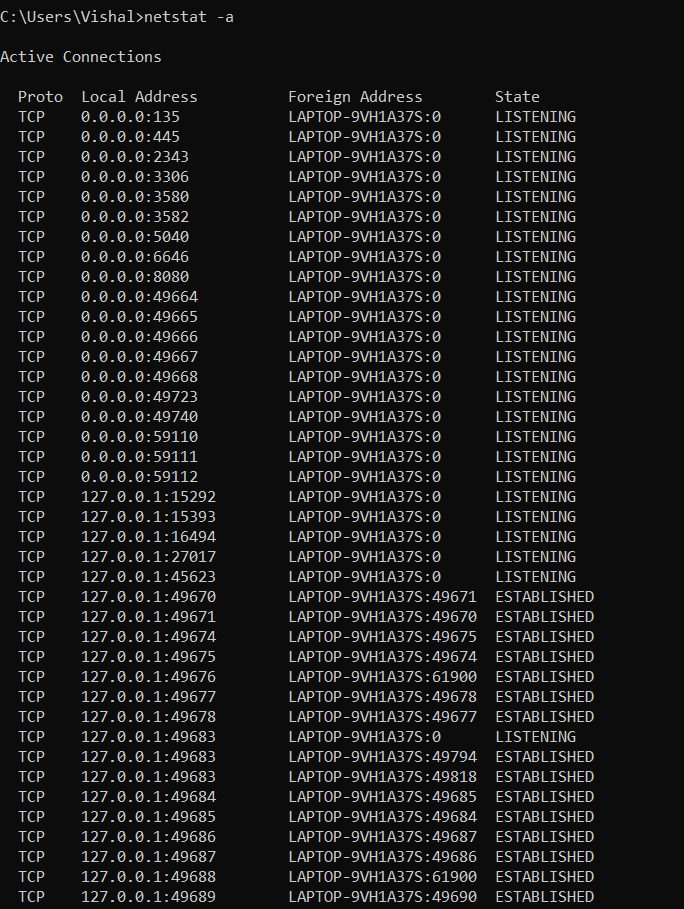


**Netstat**

The netstat command gives information about network connections. I often use netstat -t -n which lists currently open TCP connections (that's the "-t" option) by IP address rather than domain name (that's the "-n" option). Add the option "-l" (lower case ell) to list listening sockets, that is sockets that have been opened by server programs to wait for connection requests from clients: netstat -t -n -l. (On Mac, use netstat -p tcp to list tcp connections, and add "-a" to include listening sockets in the list.)







**telnet**

Telnet is an old program for remote login. It's not used so much for that any more, since it has no security features. But basically, all it does is open a connection to a server and allow server and client to send lines of plain text to each other. It can be used to check that it's possible to connect to a server and, if the server communicates in plain text, even to interact with the server by hand. Since the Web uses a plain text protocol, you can use telnet to connect to a web client and play the part of the web browser. I will suggest that you to do this with your own web server when you write it, but you might want to try it now. When you use telnet in this way, you need to specify both the host and the port number to which you want to connect: telnet <host> <port>. For example, to connect to the web server on www.spit.ac.in: telnet spit.ac.in 80.

**Tracert**

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)

**EXPERIMENTS WITH TRACEROUTE**

From your machine traceroute to the following hosts:

1. ee.iitb.ac.in

2. mscs.mu.edu

3. www.cs.grinnell.edu

4. csail.mit.edu

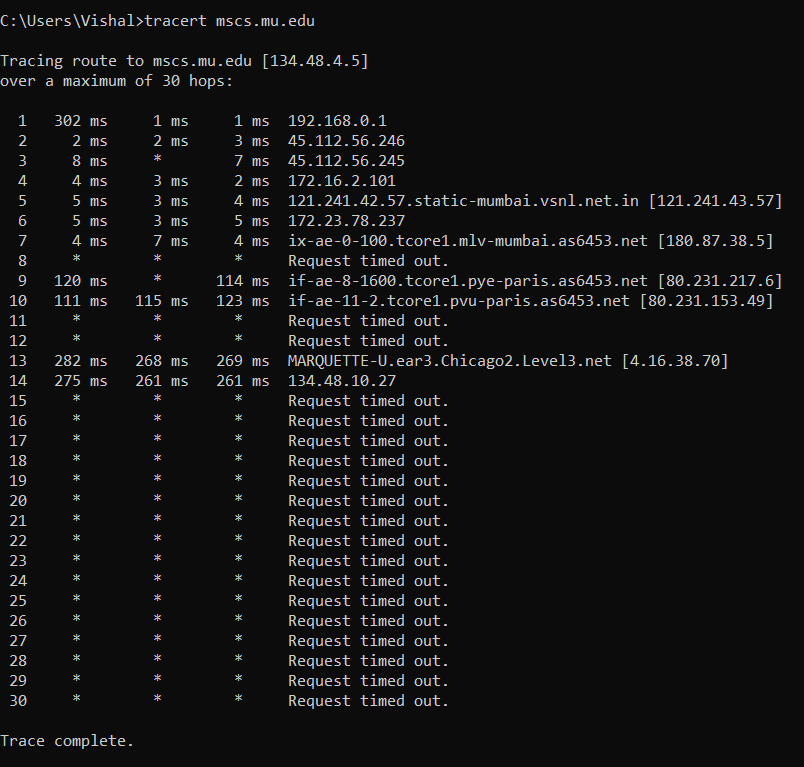
5. cs.stanford.edu

6. cs.manchester.ac.uk

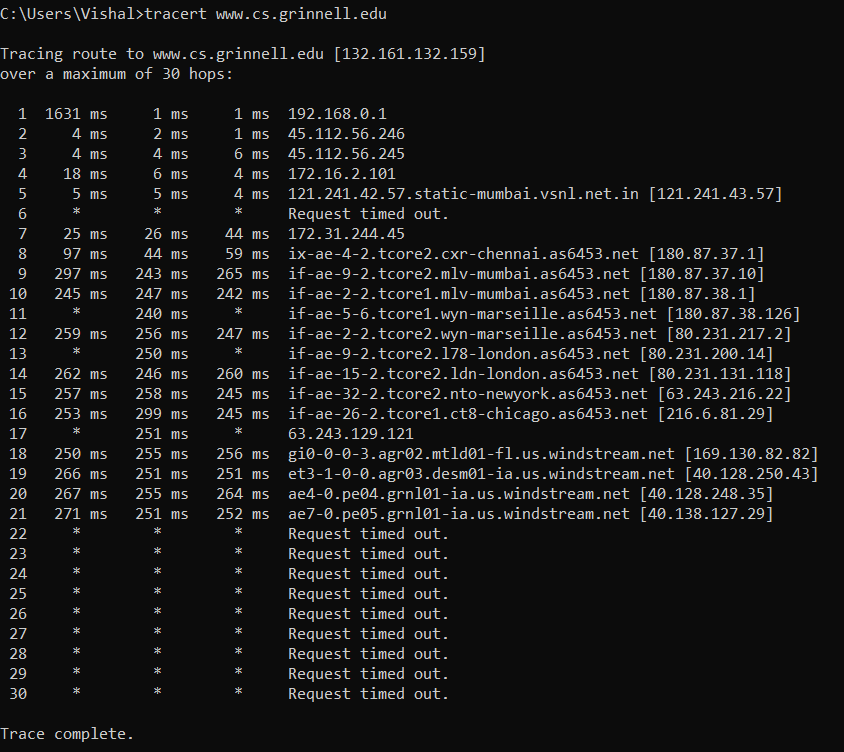
Store the output of each traceroute command in a separate file named traceroute\_HOSTNAME.log, replacing HOSTNAME with the hostname for end-host you pinged

**(e.g., traceroute\_ee.iitb.ac.in.log).**

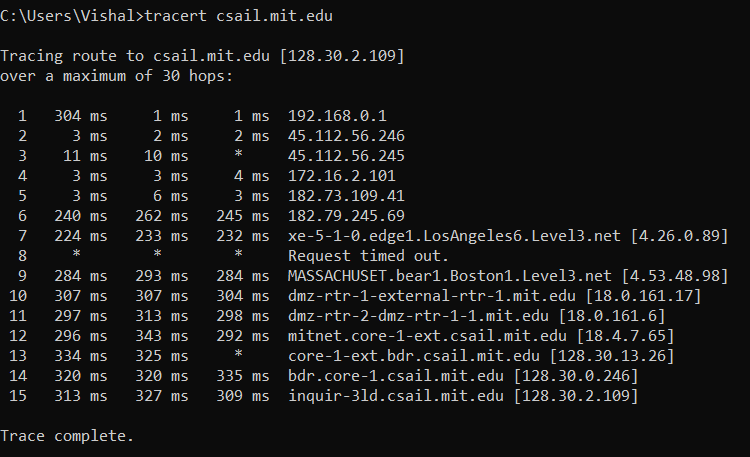
**mscs.mu.edu**



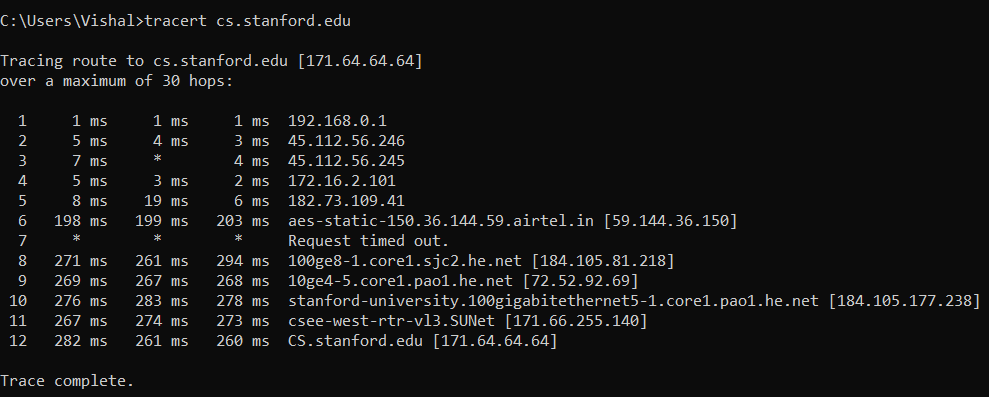
**www.cs.grinnell.edu**



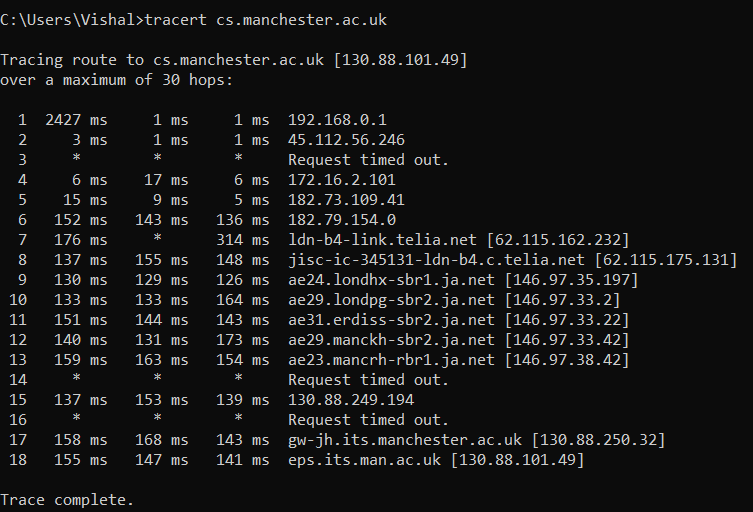
**csail.mit.edu**

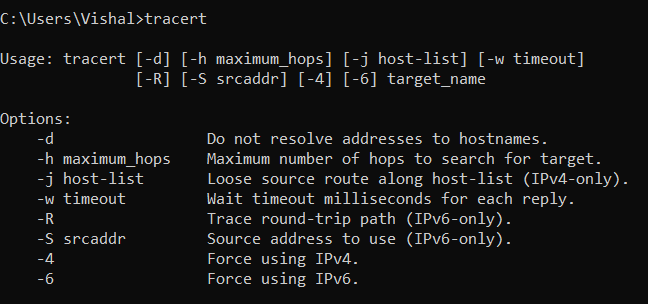


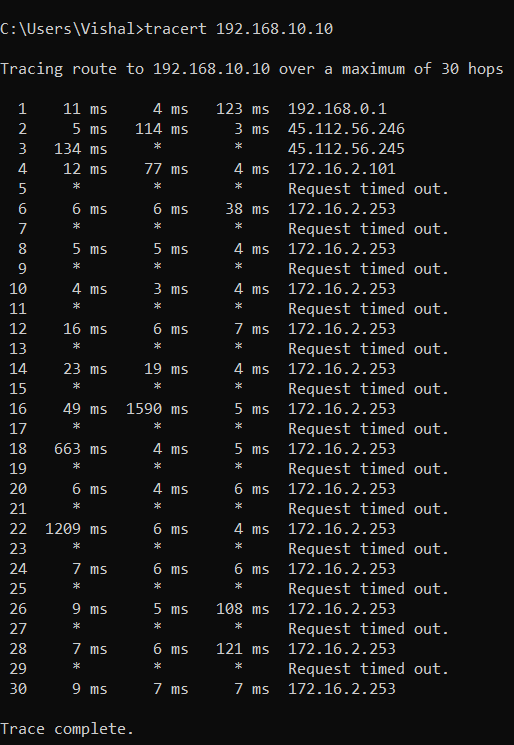
**cs.stanford.edu**

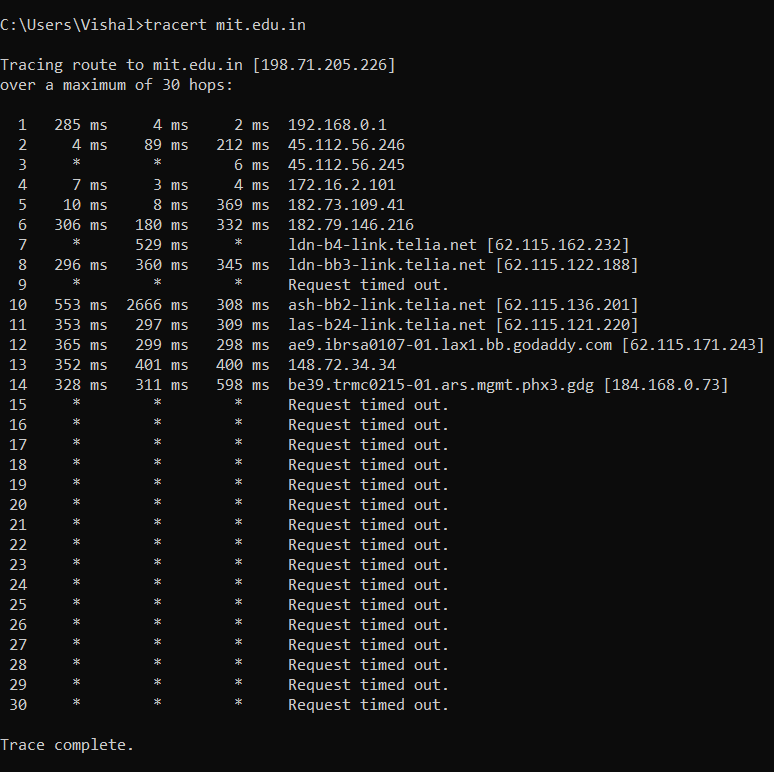


**cs.manchester.ac.uk**

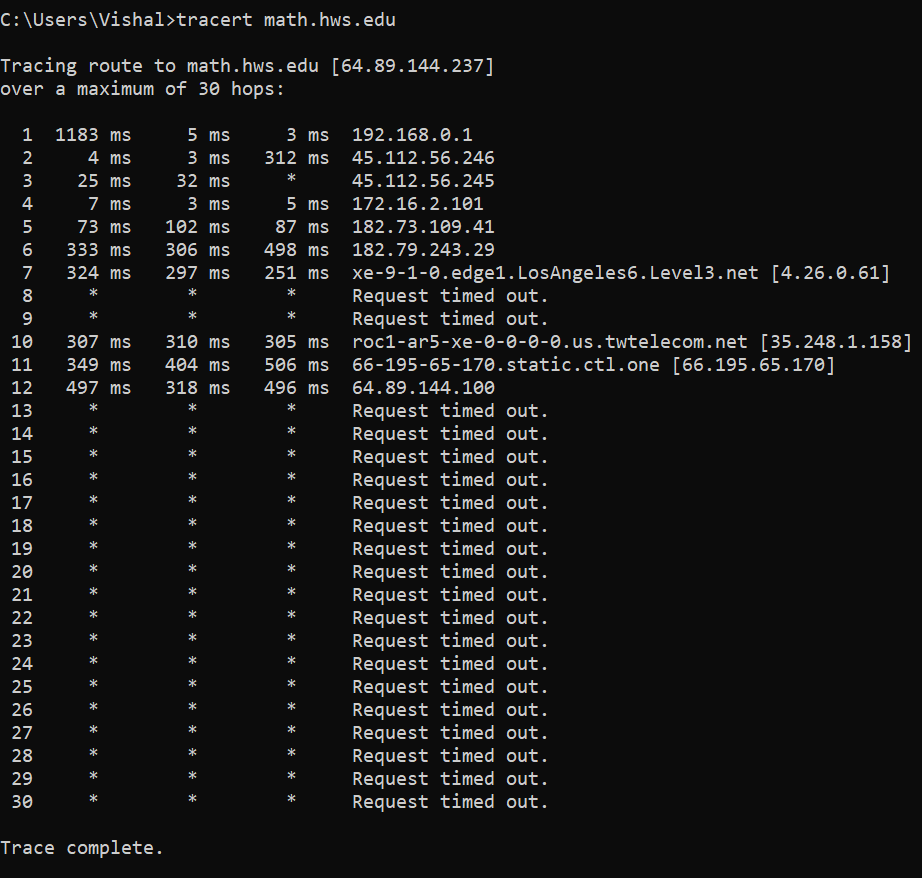


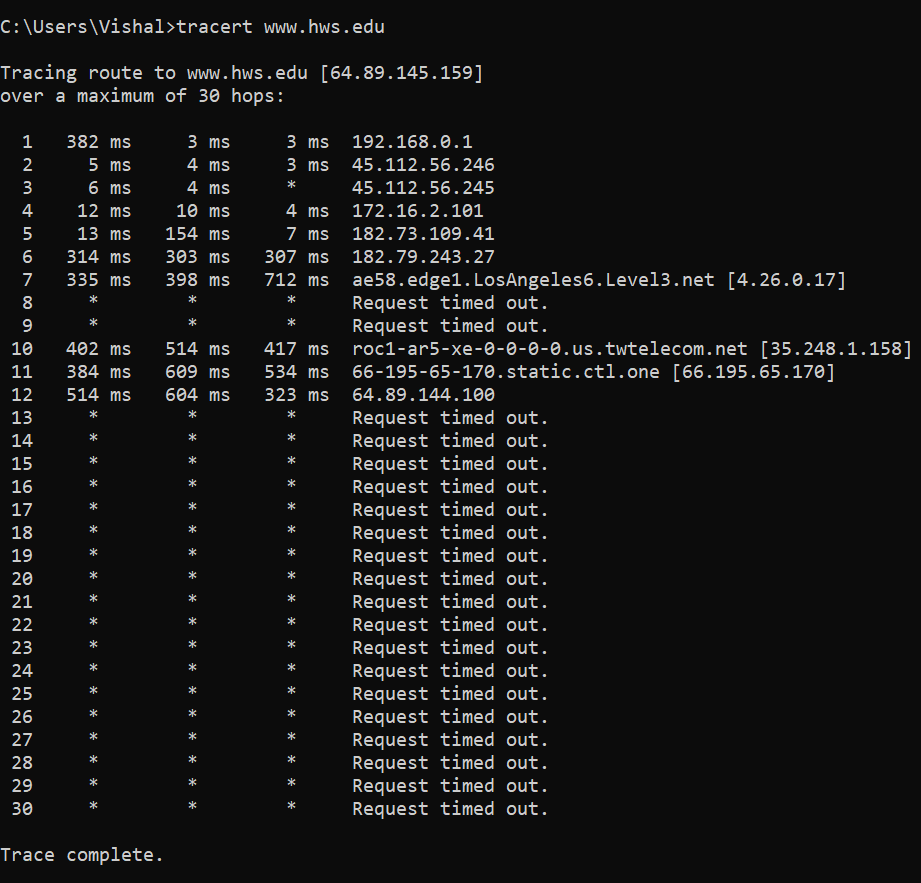






**Exercise 2:** Use traceroute to trace the route from your computer to math.hws.edu and to www.hws.edu. Explain the difference in the results.

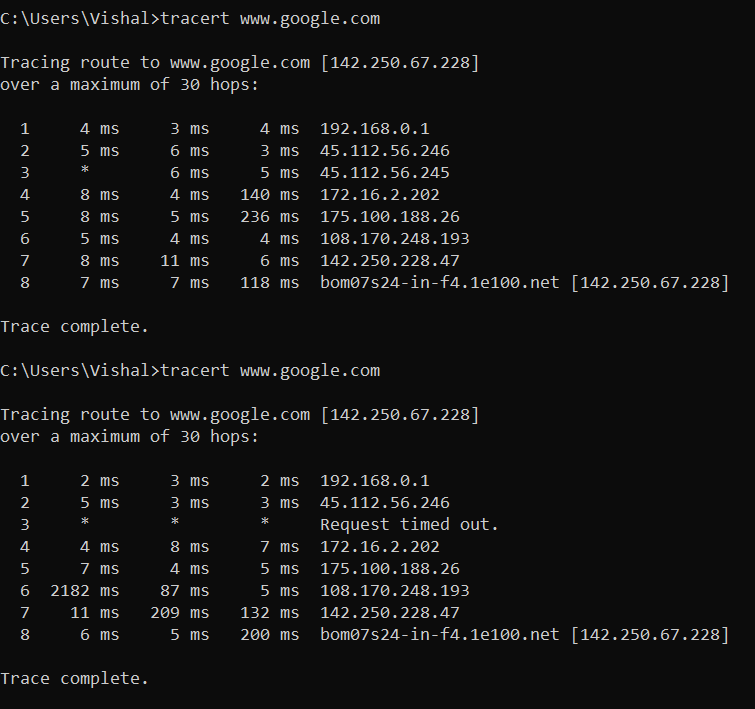




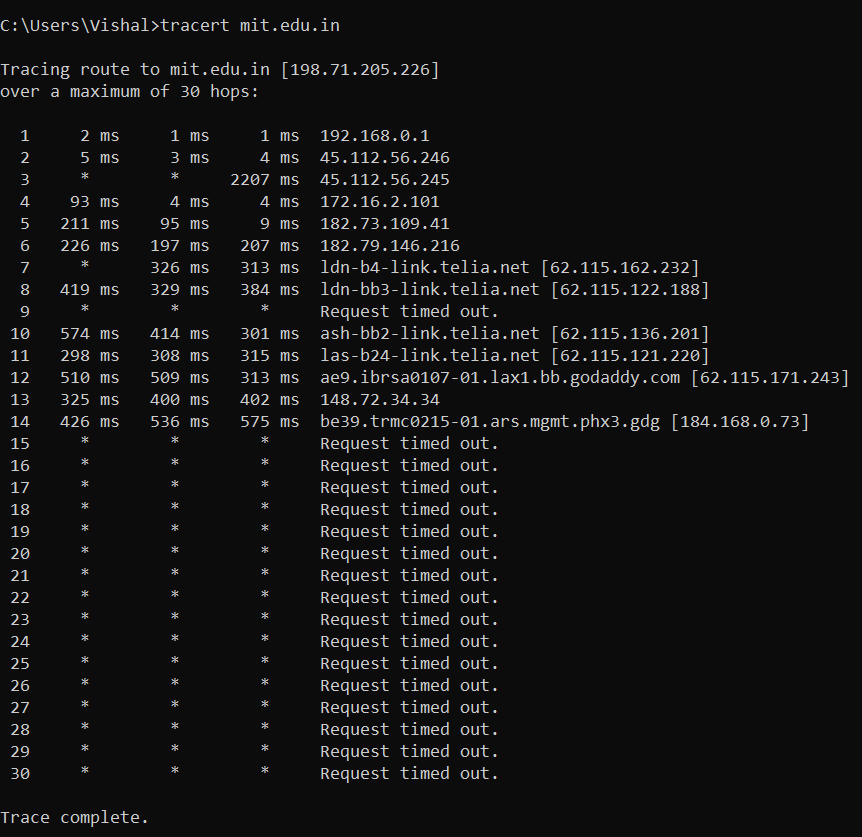
The only difference is that from 1st hop time taken by the packet is different but the end

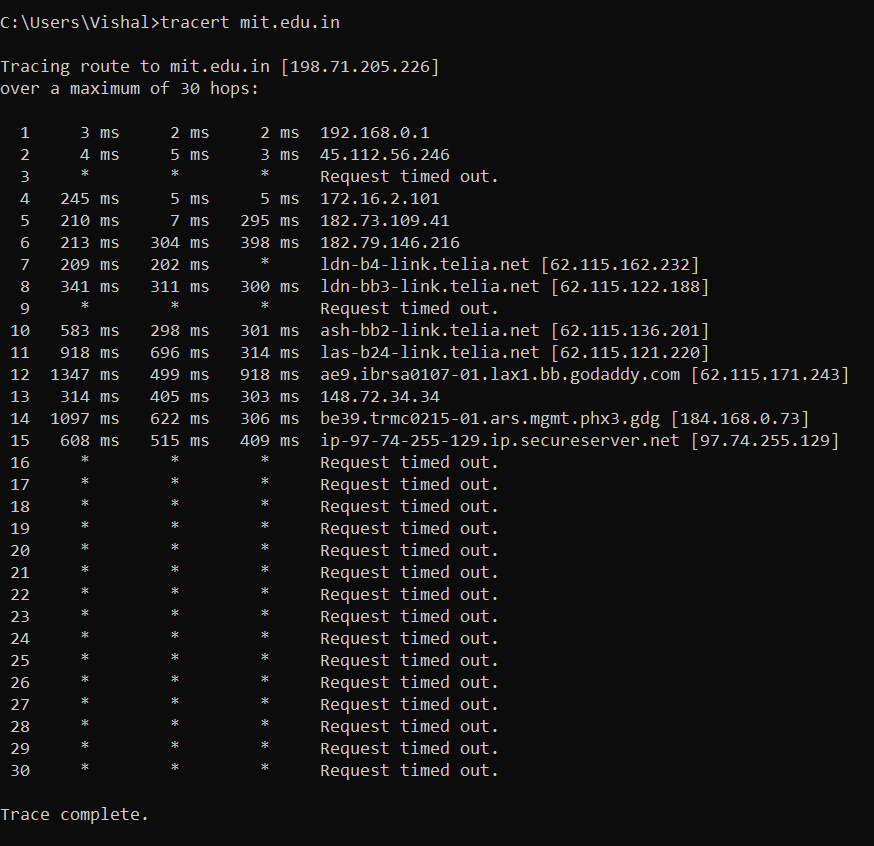
result is the same.

**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.



It is true that 2 packets sent from the same source to the same destination do not necessarily follow the same path through the net. As seen in the above image the first one takes 8 hops and the second one takes 8 hops to reach the destination but at 3rd hop there is request time out otherwise result will be same.





**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, it is true that some part of path common for host that I traceroute. When packet sent from the same source to the same destination do not necessarily follow the same path through the net. Some of take more hope than other one. As I see in mit.edu.in first packet takes 14 hopes to reach where as other one take 15.

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?

If the distance between source and destination 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.

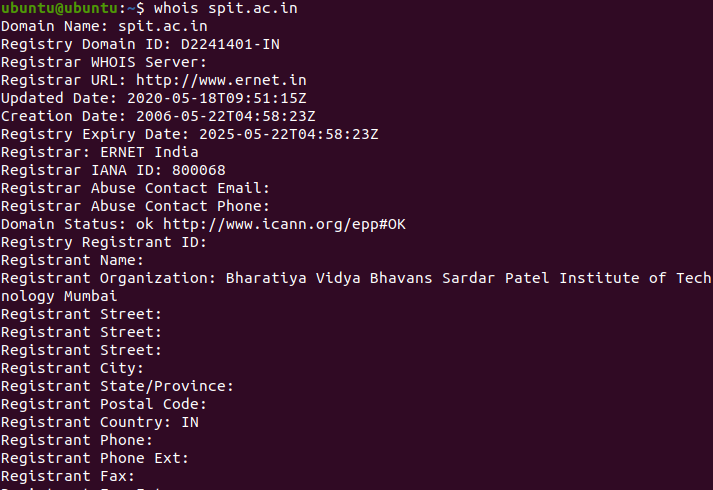
3. Is there a relationship between the number of nodes that show up in the traceroute and latency of the host (from your ping results above)? Does the same relationship hold for all hosts?

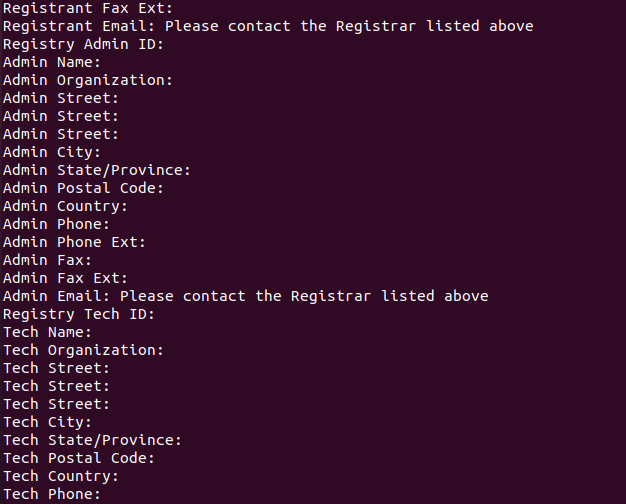
If the latency of the host causes the traceroute request to get timed out even after the conventional three tries then it keeps on sending the data packets until the host responds or upto certain hops. The same relationship may not hold for all hosts.

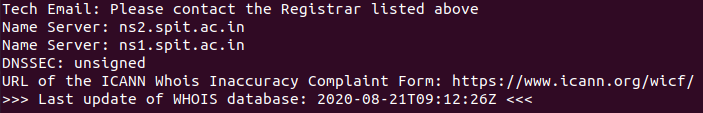
Whois — The whois command can give detailed information about domain names and IP addresses. If it is not installed on the computers then install it with command sudo apt-get install whois in. Whois can tell you what organization owns or is responsible for the name or address and where to contact them. It often includes a list of domain name servers for the organization.

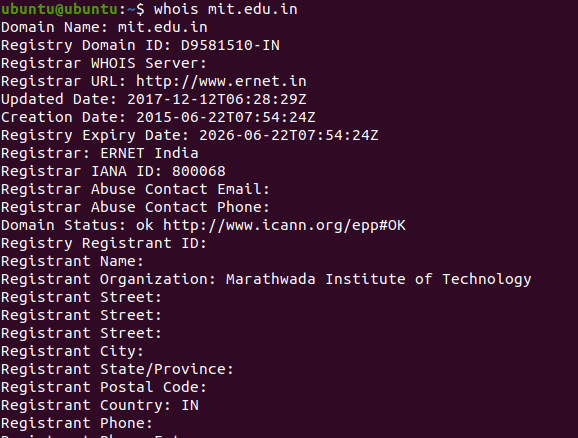
When using whois to look up a domain name, use the simple two-part network name, not an individual computer name (for example, whois spit.ac.in).

**Exercise 4:** 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.









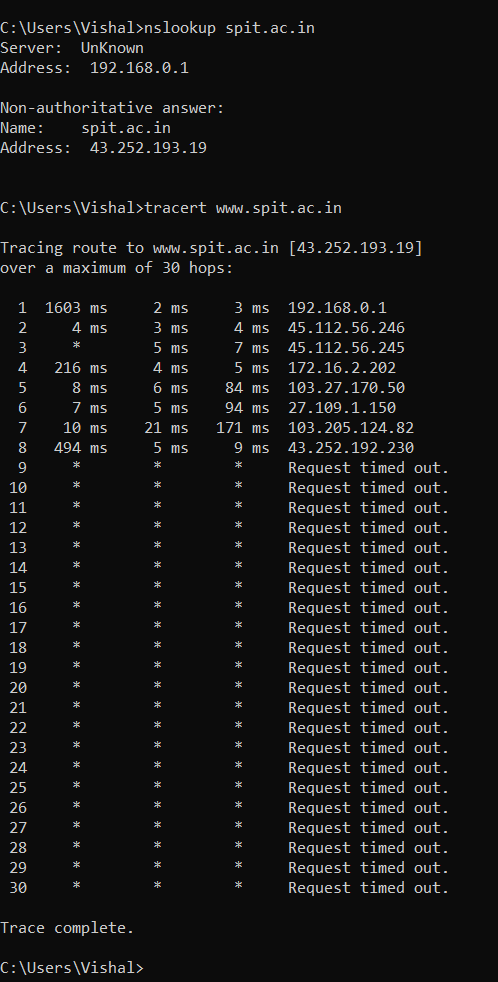
**Domain information**

This type of information contains the general details about the domain. It will consist of the

following fields.

* **Domain**: This field will give you the domain name which we are querying the WHOIS details.
* **Registrar:** This is the details of the registrar with whom the domain name is registered.
* **Registration Date:** This is the date when the domain name was first registered. With some whois lookup tools, it will be displayed as “Creation Date”.
* **Register Organization:** This is the name of the organisation.

**Exercise 5:** 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.



NAT is short for Network Address Translation. NAT is an Internet standard that enables a local-area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. Hence, we can see that the domain name spit.ac.in has a different IP address outside of SPIT than it does on campus.

Geolocation — A geolocation service tries to tell, approximately, where a given IP address is located physically. They can't be completely accurate—but they probably get at least the country right most of the time.

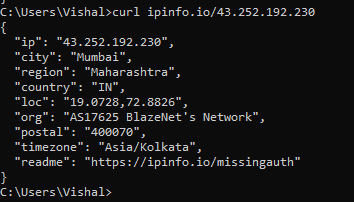
This geolocation program is not installed on our computers, but you can access one on the command line using the curl command, which can send HTTP requests and display the

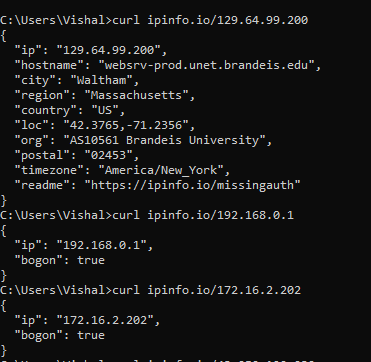
response. The following command uses curl to contact a public web service that will look up an IP address for you: curl ipinfo.io/<IP-address>. For a specific example:

curl ipinfo.io/129.64.99.200

(As you can see, you get back more than just the location.)

**Exercise 6:** Find a few IP addresses that are connected to the web server on spit.ac.in right now, and determine where those IP addresses are located. (I'm expecting that there will be several; if not, try again in a few minutes or sometime later.) Find one that is far from Geneva, NY. Explain how you did it.





You can access location of IP address 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:

cu**rl ipinfo.io/<IP-address>.**

**Reference:**

**1]Ping:**

<https://www.imperva.com/learn/performance/round-trip-time-rtt/>

**Conclusion:**

Thus, I studied as well as implemented basic networking commands and utilities like ping, nslookup, ifconfig, netstat, traceroute, whois in detail.