CS342: ASSIGNMENT 1

RITWIK GANGULY – 180101067

Answer 1:

Note: Use of <> suggest it's not part of the syntax, instead it's used to denote that the variable inside <> is to be replaced by the user-defined value.

a) *ping -c <count>* : The value of count specifies the number of requests to be sent.

b) *ping -i <interval>* : The value of interval specifies the time interval in seconds between two successive ping ECHO_REQUESTs.

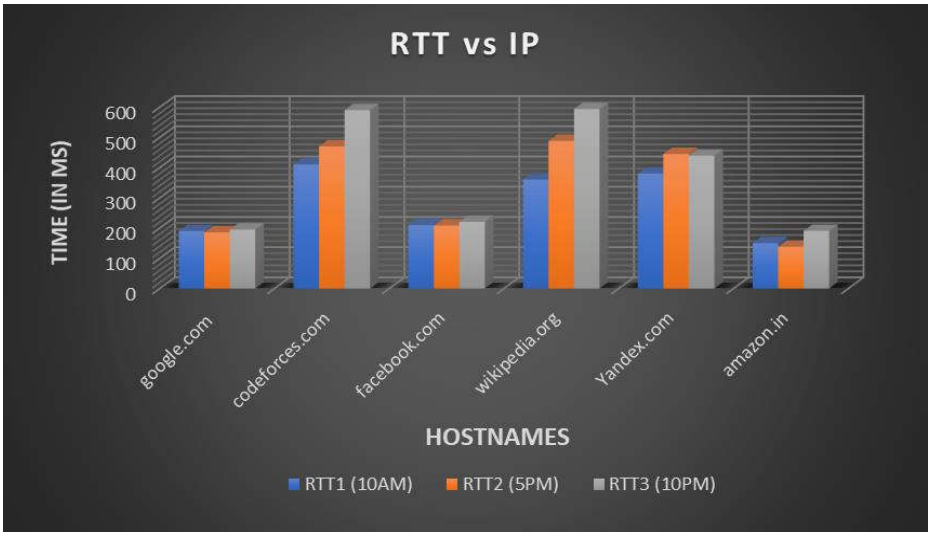
c) *ping -l <hostname> :* ping sends that many packets not waiting for a reply. The limit for sending such packets by normal users is 3. We can also specify the -f option with zero-time interval (flood ping), which sends ICMP packets as fast as possible without waiting for replies.

d) *ping -s <size>* : The value of size denotes the packet size to be sent.
The packet is added with 20 bytes IP header and 8 bytes Internet Control Message Protocol (ICMP) header. If payload size is 32 bytes, then total packet size = 32+28= 60 bytes.

Answer 2:

a) Note: All RTT are in milliseconds.

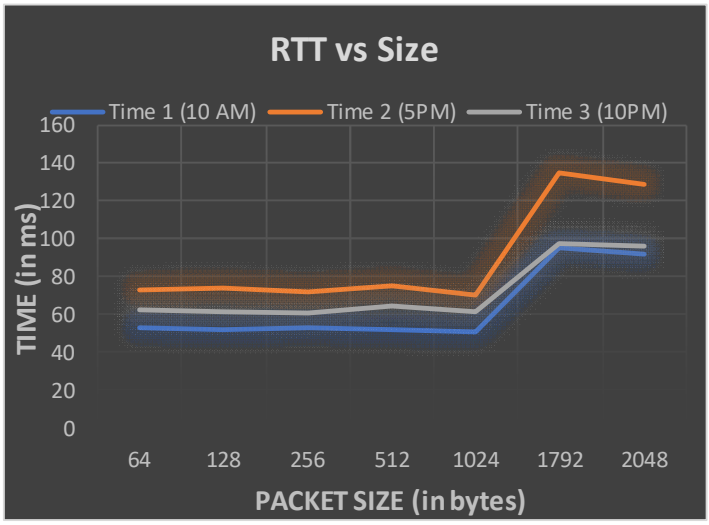
HOST	IP ADDRESS	LOCATION	RTT1 (10AM)	RTT2 (5PM)	RTT3 (10PM)	AVG. RTT
google.com	172.217.7.174	California, USA	190.2	185.9	195.2	190.4
codeforces.com	81.27.240.126	Moscow, Russia	410.6	470.2	590.5	490.4
facebook.com	157.240.23.35	Chennai, India	210.1	208.5	220.9	213.2
wikipedia.org	103.102.166.224	New York, USA	360.9	488.4	594.2	481.2
Yandex.com	231.180.204.62	Russia	380.5	445.2	440.1	421.9
amazon.in	54.239.33.92	Bangalore, India	150.2	138.2	190.8	159.7



Average RTT vs Location: We can infer from the graph that there exists a weakly positive correlation between the geographic distance of the servers and the Round-Trip Time (RTT). There can be numerous reasons like number of hops, propagation delay etc. which affect this correlation. With increasing distance, it usually takes more time to reach destination since there are more nodes involved in between. However, the correlation is weak because distance isn't the sole determining factor for RTT.

b) Some servers like Google and Facebook gave a packet loss of 4-8% in the 5pm slot however, mostly all the hosts gave 0% packet loss. This might be due to severe congestion in network during the busy 5pm slot or overloaded nodes in a path.

c)

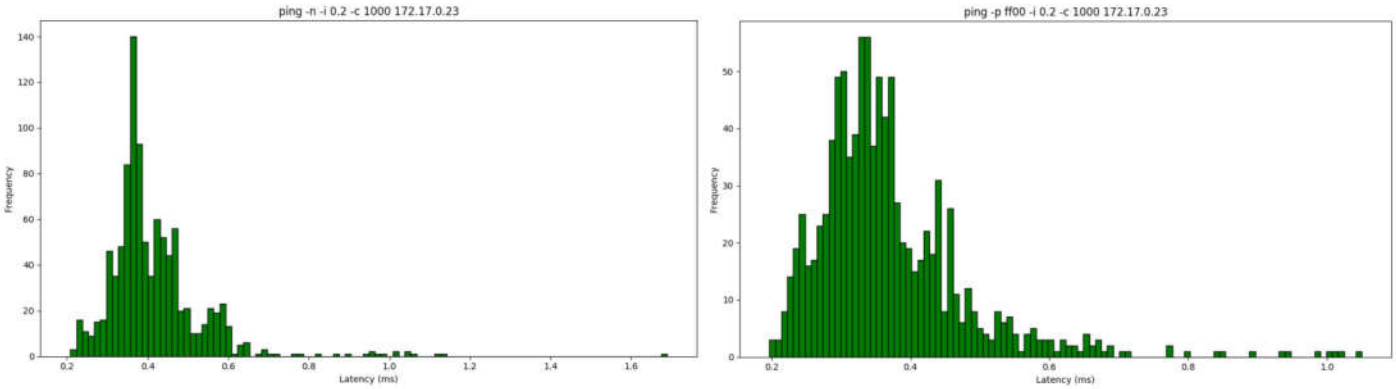


d) Average RTT vs Time: I could infer no strong relation between the two since all the servers have different locations. However, I noticed that for most servers, evening time pings were more. This can be credited to more usage of the servers during that period of time. It also depends on individual host audience as well. Example: Codeforces had a contest from 8:05pm-10:05pm due to which we see a spike in RTT at 10pm.

Average RTT vs Packet Size: From the graph, it can be reasonably inferred that RTT is similar for all sizes till 1024 bytes. Then it almost doubles up for 2048 bytes. This can be attributed to the fact that Maximum Transmission Unit is 1500 bytes. So, for sizes bigger than 1500 bytes, the packet is broken down into two frames of size 1500 bytes each, as a result of which RTT increases.

Answer 3:

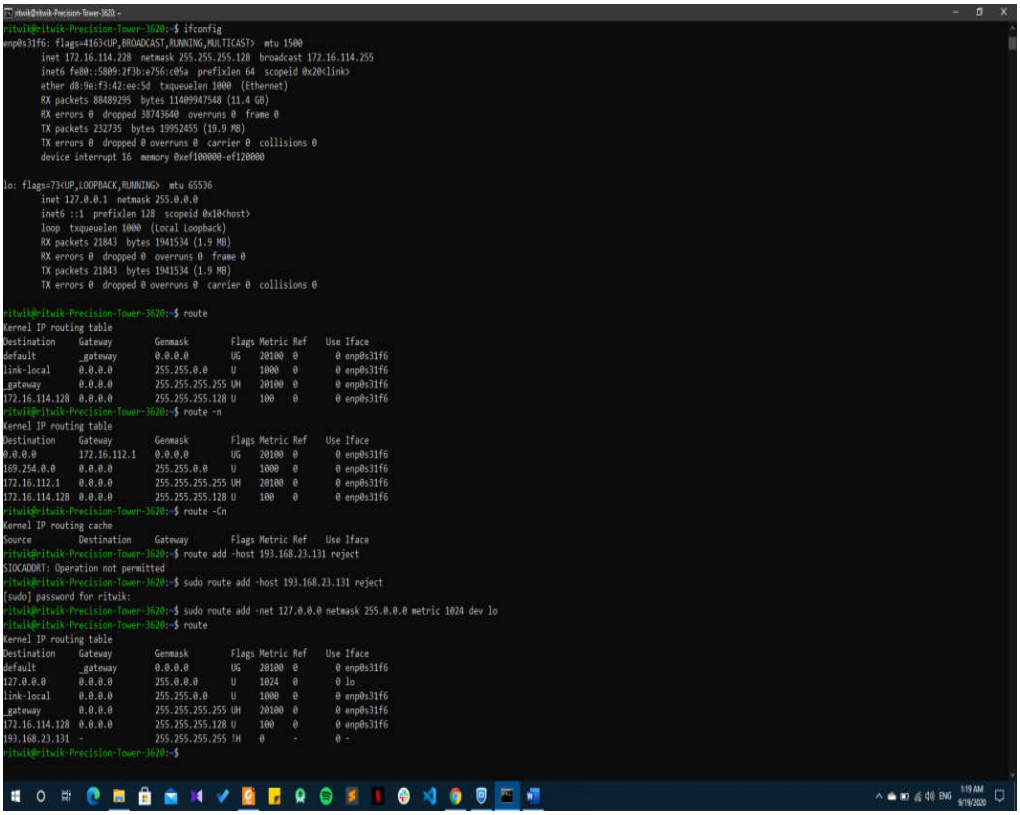
Command	Packets transmitted	Packets received	Min Latency (ms)	Max Latency (ms)	Avg. Latency (ms)	Median latency (ms)
ping -n -i 0.2 -c 1000 172.17.0.23	1000	1000 (0% loss)	0.244	14.043	0.344	0.433
ping -p ff00 -i 0.2 -c 1000 172.17.0.23	1000	995 (0.5% loss)	0.164	7.817	0.378	0.492



'-n' specifies that no attempt will be made to lookup symbolic names for host addresses. Hence, it is faster than normal ping. So, the mean latency is higher in the second case than the mean latency in the first case.

'-p' is used to pad bytes to fill out the packets that are sent which is useful for diagnosing data-dependent problems in a network. '-p ff00' will cause the packet to be padded with the pattern 1111 1111 0000 0000. Due to 1-bit transition in the bit pattern, the clocks will go out of synchronization at both sender and receiver end resulting in higher packet loss than the first case.

Answer 4:



```
ritwik@ritwik-Precision-Tower-3620:~$ ifconfig
enp0s31f6: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.114.228  netmask 255.255.255.128  broadcast 172.16.114.255
        inet6 fe80::5809:2f3b:e756:c05a  prefixlen 64  scopeid 0x20<link>
        ether d8:9e:f3:42:ee:5d  txqueuelen 1000  (Ethernet)
        RX packets 88489295  bytes 11409947548 (11.4 GB)
        RX errors 0  dropped 38743640  overruns 0  frame 0
        TX packets 232735  bytes 19952455 (19.9 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 16  memory 0xef100000-ef120000

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 21843  bytes 1941534 (1.9 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 21843  bytes 1941534 (1.9 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ritwik@ritwik-Precision-Tower-3620:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    20100  0        0 enp0s31f6
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 enp0s31f6
_gateway        0.0.0.0         255.255.255.255 UH    20100  0        0 enp0s31f6
172.16.114.128  0.0.0.0         255.255.255.128 U     100    0        0 enp0s31f6
ritwik@ritwik-Precision-Tower-3620:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         172.16.112.1    0.0.0.0         UG    20100  0        0 enp0s31f6
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 enp0s31f6
172.16.112.1    0.0.0.0         255.255.255.255 UH    20100  0        0 enp0s31f6
172.16.114.128  0.0.0.0         255.255.255.128 U     100    0        0 enp0s31f6
ritwik@ritwik-Precision-Tower-3620:~$ route -Cn
Kernel IP routing cache
Source          Destination     Gateway         Flags Metric Ref    Use Iface
ritwik@ritwik-Precision-Tower-3620:~$ route add -host 193.168.23.131 reject
SIOCADDRT: Operation not permitted
ritwik@ritwik-Precision-Tower-3620:~$ sudo route add -host 193.168.23.131 reject
[sudo] password for ritwik:
ritwik@ritwik-Precision-Tower-3620:~$ sudo route add -net 127.0.0.0 netmask 255.0.0.0 metric 1024 dev lo
ritwik@ritwik-Precision-Tower-3620:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    20100  0        0 enp0s31f6
127.0.0.0       0.0.0.0         255.0.0.0       U     1024   0        0 lo
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 enp0s31f6
_gateway        0.0.0.0         255.255.255.255 UH    20100  0        0 enp0s31f6
172.16.114.128  0.0.0.0         255.255.255.128 U     100    0        0 enp0s31f6
193.168.23.131  -               255.255.255.255 !H    0      -        0 -
ritwik@ritwik-Precision-Tower-3620:~$
```

a) **Ifconfig** stands for Interface Configuration. It is used to view and change the configuration of the network interfaces on our system.
In the ifconfig output report:
Link encap: Refers to interface type
HWaddr: Refers to unique MAC address of the ethernet card.
Inet and Bcast: Refer to IP and broadcast addresses respectively.
Up: indicates that the ethernet modules are loaded.
Broadcast: denotes broadcasting is supported.
Running means ready for acceptance of data

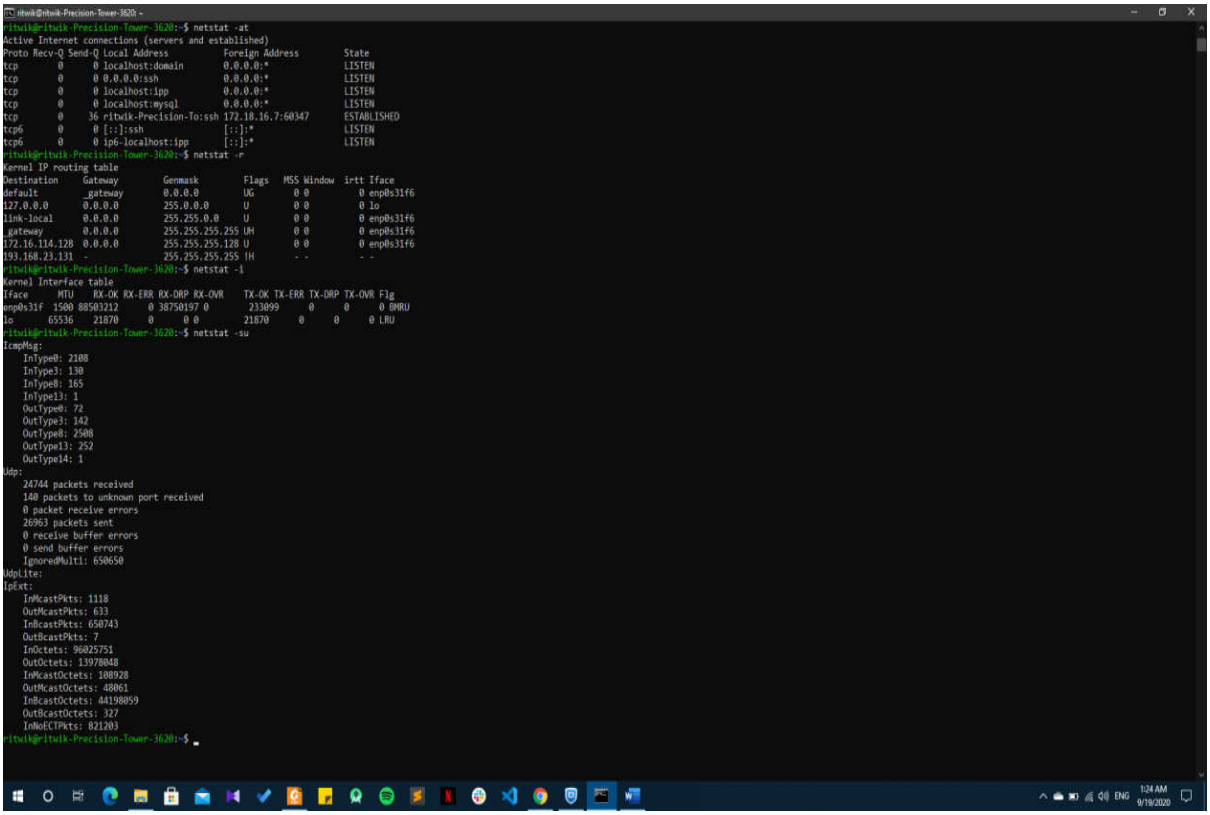
Multicast: refers to source able to send packets to multiple machines.
RX and TX packets: refer to received and transmitted packets respectively.
RX and TX bytes: refer to the total data passed through ethernet in both directions.
Collisions: Refer to the degree of network congestion.
Txqueuele: denotes length of transmit queue.
Metric: denotes the priority of device.
MTU (Maximum Transmission Unit): Size of each packet received by the ethernet card.

b) Four options that can be used with the ifconfig command are:
mtu N: Set packet size for transmission.
Multicast: Set this flag to the interface to allow multiple transmissions
-a: Displays all interfaces which are currently available, even if down.
add addr: To add an IPv6 address to an interface.

c) **Route command** is used to show/manipulate the IP routing table. It is primarily used to set up static routes to specific hosts or networks via an interface. **Destination** column identifies the destination network. The **Gateway** column identifies the gateway for the specified network. The **Genmask** column shows the netmask for the network. The **Flags** may be U (Up route) and G (Gateway route). **Metric** refers to the number of hops to the destination. **Ref** is the number of references to this route. **Iface** column shows the network interface (Ethernet or wireless ethernet).

d) **del/add** can be used to delete/add routes. **-n** to show numeric addresses instead of symbolic names. **-Cn** for routing cache information such that Kernel maintains a routing cache table to route the packets faster.
Block access to a single host: We can block access to a particular host or network by rejecting routes to it. Given below is an example of blocking access to host with the IP address 193.168.23.131. Example:
route add -host 193.168.23.131 reject

Answer 5:



a) Netstat (Network Statistics) command displays various network related information such as network connections, routing tables, interface statistics, masquerade connections, multicast memberships etc.

b) *netstat -at | egrep "ESTABLISHED"* is the required command. **Proto** indicates the protocol used. **Recv-Q** and **Send-Q** refers to the data queued to be received and sent respectively. **Local address** specifies Address and port number of the local end of the socket. **Foreign address** specifies Address and port number of the remote end of the socket. **State** refers to the state of the socket out of predefined values set.

c) It shows the Kernel Routing Table of the Machine. **Destination** column indicates the pattern that the destination of a packet is compared to. The **Gateway** column refers to the location where a packet is to be sent on the matching destination. The **Genmask** column identifies the subnet by indicating the bit count from the start of IP address. The **Flags** column describe the route - G(gateway), U(up), H

(Single host), D(dynamic), M (set if entry was modified by an ICMP redirect message). The **MSS (Maximum Segment Size)** is the size of the largest datagram that will be used for the transmission by the kernel. The **Window** refers to the maximum amount of data accepted in single out from remote host. **IRTT** refers to initial round trip time. The **Iface** column refers to the network interface type.

d) *netstat -i* is the required command. Looking at the output, my device has 2 interfaces, namely **enp0s31f** and **lo**.

e) *netstat -su* is the required command.

f) The loopback device is a special, virtual network interface that the computer uses to communicate with itself. It is used mainly for diagnostics and troubleshooting, and to connect to servers running on the local machine. It can perform the following functions:
Device identification: The loopback interface is used to identify the device. While any interface address can be used to determine if the device is online, the loopback address is the preferred method. **Routing information:** The loopback address is used by protocols such as OSPF to determine protocol-specific properties for the device or network. Further, some commands such as ping mpls require a loopback address to function correctly. **Packet filtering:** Stateless firewall filters can be applied to the loopback address to filter packets originating from, or destined for, the Routing Engine.

Answer 6:

a) Traceroute is a network diagnostic tool used to track in real-time the pathway taken by a packet on an IP network from source to destination, reporting the IP addresses of all the routers it pinged in between. Traceroute also records the time taken for each hop the packet makes during its route to the destination.

Time Slot	google.com	codeforces.com	facebook.com	Wikipedia.org	Yandex.com	amazon.in
1 AM	9	18	9	9	14	11
11 AM	8	15	8	9	13	12
5 PM	9	14	8	9	13	12

b) The common IP I found in all the hops was the starting one, which obviously being the testing server's Ip. Apart from these, same hosts in nearby geographical locations seemed to have some intermediary IP same because of the fact that they might have the same internet circles for longer transmission distance.

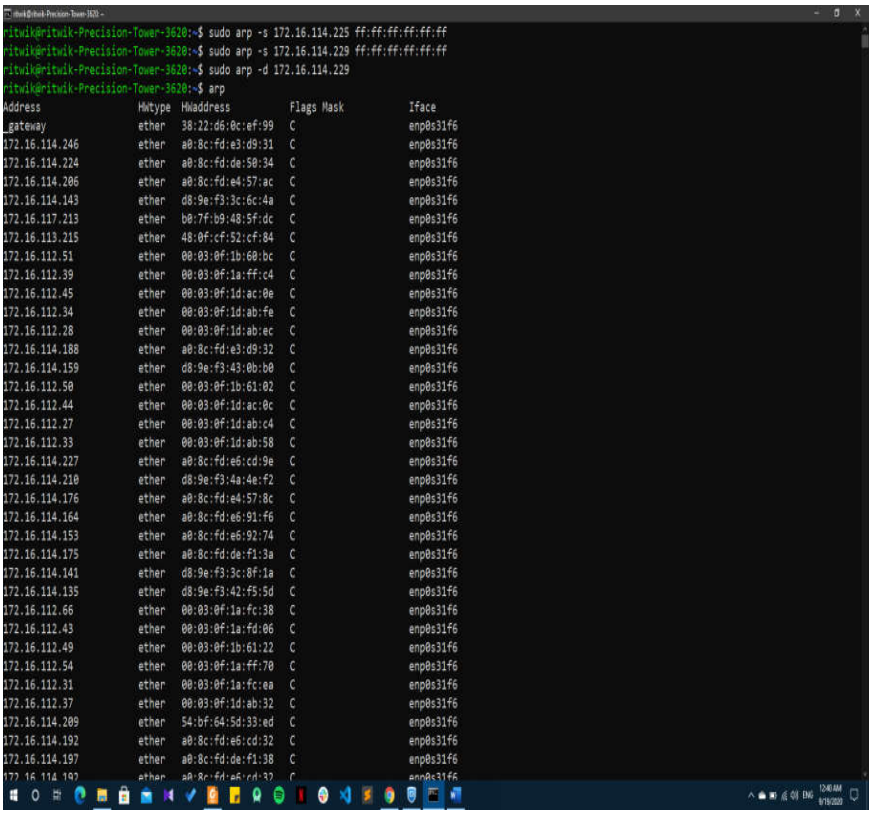
c) Yes. The route changed at different times because of the fact that network congestion is variable at all times during a day. Generally, packets are preferred to be sent through lower congestion node to increase efficiency and speed as a result of which route changes.

d) In my observation, I had to change the tool once for getting a route because the server displayed the message "Couldn't reach destination because of firewall blocking". Firewall can block ICMP packets or in some cases hosts may not provide complete path is network congestion exceeds a specified limit.

e) Yes, the route might be possible. This is due to the fact that ping and traceroute differ in their fundamental working. Ping sends ICMP packets to the host and expects the reply. If the server blocks the reply, ping fails. But in the case of traceroute, packets are sent with TTL values that decrement with each passing router and when the value turns zero, it shows ICMP error (ICMP Time Exceeded). Thus, if TTL value stays greater than zero after reaching host, we can find a route.

Answer 7:

a) *arp* is the required command. Address refers to the IP address. HWtype signifies the network link protocol type. **HWaddress** refers to unique MAC address of the ethernet card. The **flags** indicate if the mac address has been learned, manually set, published (announced by another node than the requested) or is incomplete. **Mask** refers to the subnet mask. **Iface** refers to the specific type of interface.



b) *arp -s ipaddr mac_addr* is used to add new table entry. *arp -d address* is used to delete a specific entry.

c) Arp command works only on the IP in the same subnet. The packets follow different protocols if two IP addresses are on different subnets. It will search for the routing table for the destination network and send the packet to the router or default gateway. In such a situation, the arp table will be used in finding the hardware address of that specific router since the destination IP address had already been designated as unreachable, therefore the packet must be delivered to a router which will take care of it.

d) Ping command couldn't run on the modified node. This is because two types of conflicts might occur:

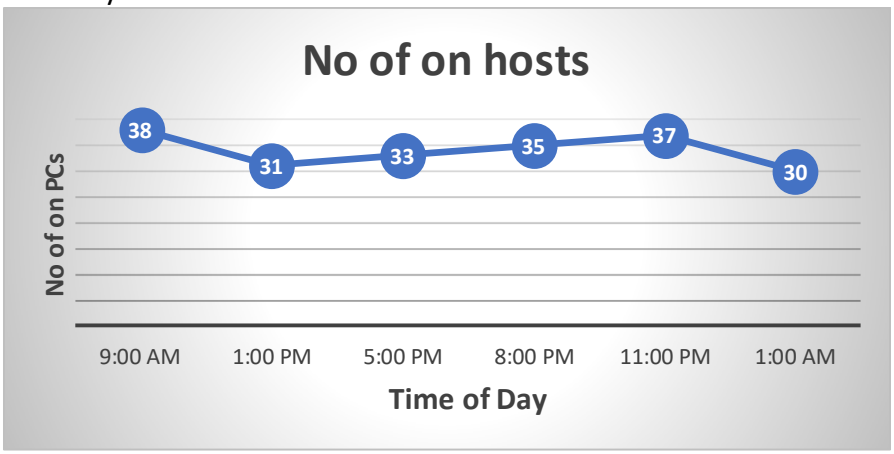
(I) IP Address conflict: Traffic will be forwarded based on ARP cache.

(II) MAC Address conflict: Either two nodes won't be able to communicate as arp broadcast will fail as source node will possess same MAC address as destination node; Or other nodes trying to send data to any of these conflicting MAC Address nodes will be contacted through switches. These two nodes will be sending data regularly; hence, switch will regularly update the table corresponding to this MAC address. This results in MAC address flapping and communication disruption.

Answer 8:

a) The command used for the analysis is nmap -n -sP 10.19.3.0/21 scanning 2048 IP addresses in the Lohit hostel.

b) *sudo nmap -sA 172.16.114.228 :* This command using root privileges will determine the firewall settings on my PC.



c) The trend is currently not visible properly because of suspension in classes and very few students in Campus. However, judging by the usual trend, we can guess that the number of hosts decreases during class hours while increases rapidly till midnight and then starts decreasing as people go to sleep.