CS 349 Assignment 1 Manan Gupta - 170101035

Question 1

a) **-c** option is used for specifying the count of ECHO_REQUESTS to be sent
For example :- ***ping -c 4 10.19.6.44***.
This command will send 4 ECHO_REQUESTS to the given address

b) **-i** option is used for specifying the time interval between two successive ECHO_REQUESTS
For example :- ***ping -i 0.5 10.19.6.44***.
This command will send ECHO_REQUESTS after every 0.5 seconds.

c)
- **-l** option is used for specifying the number of packets to be sent not waiting for a reply
For example :- ***ping -l 3 10.19.6.44***.
This command will send 3 ECHO_REQUESTS right at the beginning.
- The limit for sending such requests for a normal user is **3**.

d)
- **-s** option is used for specifying the number of data bytes in a packet
For example :- ***ping -s 32 10.19.6.44***.
This command will send packets having 32 data bytes.
- The total packet size will be **60 bytes** as 8 bytes of IMCP header and 20 bytes IP header are added.

Question 2

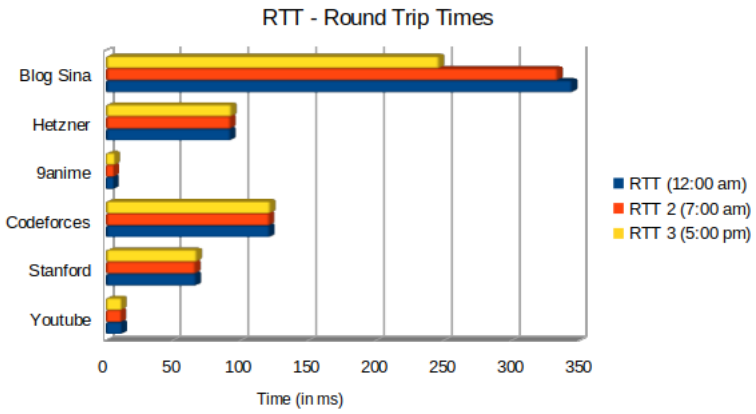
The server is located in New Jersey USA.
*Time when the readings are taken are **12:00 am, 7:00 am, 5:00 pm. (Indian Standard Time)***

Host Name	IP Address	Location	Latency 1	Latency 2	Latency 3	Avg RTT
youtube.com	172.217.7.174	California, USA	12.074 ms	11.640 ms	11.914 ms	11.876 ms
web.stanford.edu	171.67.215.200	Virginia, USA	66.963 ms	66.454 ms	67.507 ms	66.974 ms
codeforces.com	81.27.240.126	Peterburg, Russia	121.442 ms	121.139 ms	121.896 ms	121.492 ms
9anime.ru	104.27.157.26	Illinois, USA	6.032 ms	6.105 ms	6.805 ms	6.314 ms
hetzner.com	78.47.166.55	Bavaria, Germany	92.498 ms	92.486 ms	93.160 ms	92.714 ms
blogx.sina.com.cn	49.7.37.126	Beijing, China	344.783 ms	334.069 ms	246.561 ms	308.471 ms

Table 1: Round Trip Times for 6 hosts at 3 different times

Size of Packet	64B	128B	256B	512B	1024B	2048B
Latency 1	66.963 ms	67.057 ms	67.327 ms	67.201 ms	67.419 ms	78.836 ms
Latency 2	66.454 ms	66.503 ms	66.656 ms	67.006 ms	67.582 ms	78.299 ms
Latency 3	67.507 ms	67.496 ms	67.531 ms	67.986 ms	68.004 ms	79.383 ms

Table 2: Round Trip Times for 1 host at 6 different packet sizes

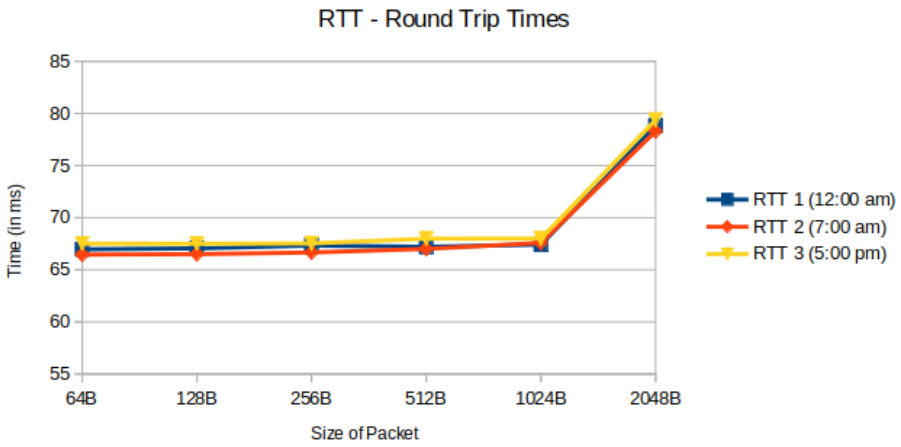


a) **RELATION BETWEEN RTT AND DISTANCE:-** From the observations, we can conclude that RTT and geographical distance are **weakly correlated**. The relationship can be explained by an **increased number of hops** required and **increased propagation delay**. As the distance increases so does the propagation delay. Also, with more distance, more hops are required between nodes which also add **processing delay** at each node. The relationship is weak as RTT also depends on network traffic and server capacity.

b) **PACKET LOSS :-** I did not encounter any case where the packet loss was greater than **0%**. There can be packet loss if there is **congestion in the network.** Also, ICMP packets have low priority, so in case of congestion, they have a higher chance of being dropped.

c) **RELATION BETWEEN RTT AND TIME OF DAY:-** The lowest RTT on average was observed around **5:00 pm IST**, which translates to **6:30 am in the USA** where the server is located. The difference is due to varying **congestion** in the network at different times. Also in case different paths are followed then queueing and processing delay might also be different. The order for increasing average RTT is 5:00 pm, 7:00 am, 12:00 am. Hence we can conclude that network traffic is high at 12:00 am IST (1:30 pm USA).

d)



RELATION BETWEEN RTT AND SIZE OF PACKET:- It can be seen from the graph that the Round Trip Times(RTT) does not change much for smaller than equal to 1024 Bytes. After that there is a sudden noticeable jump in the RTT. This can be explained by the fact that **Maximum Transmission Unit** is 1500 Bytes by default. Smaller packets are padded to make 1500 Bytes. 2048B size packet is split into two parts. Hence RTT is almost the same for smaller than 1500 Bytes packets and increases for 2048 B packet as more packets are transmitted increasing the **transmission delay**.

Question 3

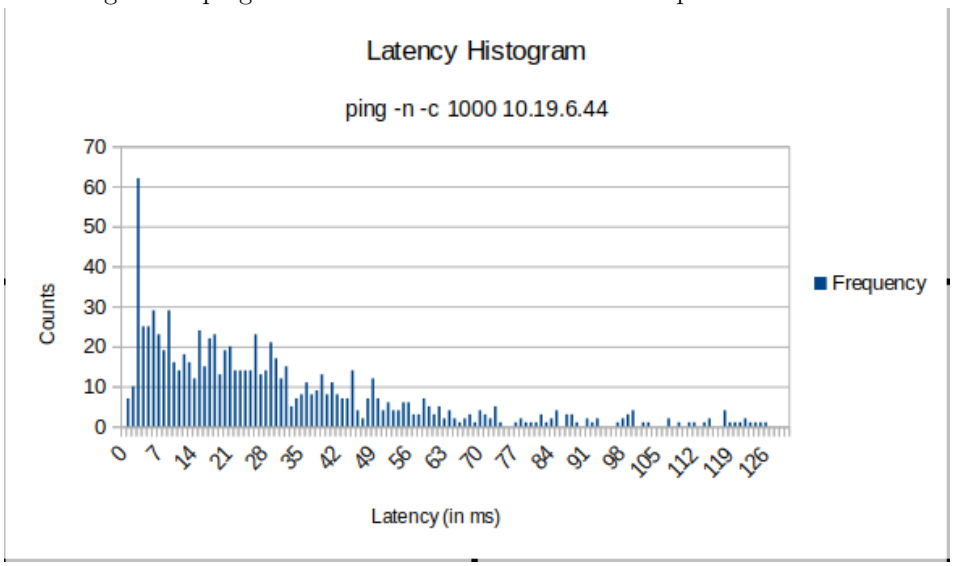
a)

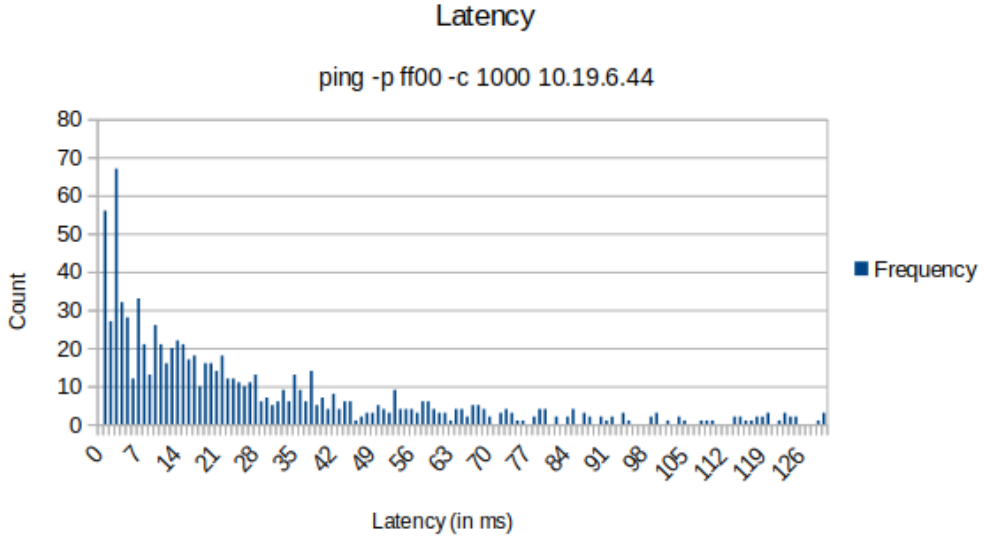
Command	Packets Sent	Packets Recieved	Packets Loss Rate
ping -n -c 1000 10.19.6.44	1000	1000	0%
ping -p ff00 -c 1000 10.19.6.44	1000	999	0.1%

b)

Command	Min Latency	Max Latency	Mean Latency	Median Latency
ping -n -c 1000 10.19.6.44	0.635ms	1078ms	54.5094ms	37.8ms
ping -p ff00 -c 1000 10.19.6.44	0.641ms	1895ms	61.8816ms	30.9ms

c) The histogram of ping latencies for both the commands is plotted





From the histogram it is apparent that both the curves follow **Normal Distribution**.

The mean latency is lower in the first command (that uses -n) as it makes no attempts to lookup symbolic names for host addresses and hence it is faster. Another difference between the two commands is that the second one (using -p ff00) is filled with 1111111100000000, therefore, has lower transitions in the signal that is sent. This is useful in checking data-dependent problems in the network. Since there are low transitions in the signal, clocking might become an issue especially for encodings that do do not use biphase encoding or scrambling techniques. Therefore it can be observed that the second command has a higher packet loss rate.

Question 4

a) **Inet** denotes the IP address of the machine, for **lo** it is the localhost. **broadcast** shows the broadcast address that is the address required to broadcast on the network connected through the interface of the machine. **Netmask** is used to divide IP address into subnets and specify the available hosts. Netmask defines how large a network is. **inet 6** refers to the IPv6 address.**UP** indicates that the server is configured to be enabled and **RUNNING** indicates that it is operational to accept data. **Multicast** indicates that the network can handle multicast packets. **MTU** (maximum transmission unit) is a link layer characteristic which provides the limit on the size of the ethernet frame. If an IP datagram is larger than the MTU then it is broken down into smaller pieces till each piece is in the range itself.The default value of MTU is 1500. **ether** shows the MAC address of the machine. **RX packets, Bytes** refer to the number of packets and bytes received respectively. **RX errors** refer to the number of damages packets received. **RX dropped** is the number of packets that were dropped. **RX frame** is the number of packets that experienced frame errors. similarly, **TX Packets** refers to the number of packets transmitted, **TX errors** refers to the number of packets that experienced errors. **txqueuelen** refers to the length of the transmission queue. **LOOPBACK** means that the interface is local loopback related.

```
manan:~$ sudo ifconfig
enp9s0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 54:e1:ad:41:dd:cc  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

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 12924  bytes 1303431 (1.3 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 12924  bytes 1303431 (1.3 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

virbr0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 192.168.122.1  netmask 255.255.255.0  broadcast 192.168.122.255
        ether 52:54:00:d1:de:77  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp8s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.43.116  netmask 255.255.255.0  broadcast 192.168.43.255
        inet6 2409:4065:282:391:823:bbec:ecd:4cc4  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::b18c:fb18:3611:a77b  prefixlen 64  scopeid 0x20<link>
        inet6 2409:4065:282:391:bfd0:68f7:8b8e:8f8f  prefixlen 64  scopeid 0x0<global>
        ether ac:ed:5c:52:3e:06  txqueuelen 1000  (Ethernet)
        RX packets 497256  bytes 368135965 (368.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 255839  bytes 57245118 (57.2 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

b) The options that can be applied with ifconfig interface are -

- **-a** it displays all the interfaces even if they are down
- **-s** it displays a short list
- **-v** it displays more verbose errors
- **mtu N** sets the MTU of an interface
- **down** causes the interface driver to be shut down

c)

```
manan:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    20600  0        0 wlp8s0
10.19.4.0       0.0.0.0         255.255.252.0   U     600    0        0 wlp8s0
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 virbr0
192.168.122.0   0.0.0.0         255.255.255.0   U     0      0        0 virbr0
```

The **route** command is used to show the routing table of the device. The attached image shows the route command run locally. The **Destination** column shows the destination host or network. The **genmask** column represents the netmask of the network. The **gateway** column shows the gateway of the network. An asterisk in the field implies that no forwarding gateway is needed. **Iface** shows the network interfaces to which packets of this route will be sent. **Metric** is the distance of the target usually counted in hops. **G** flag means that the specified gateway should be used while the **U** flag shows that the network is up. **Ref** is the number of references to the route.

d) The options that can be applied with route are -

- **-n** it shows numerical IP addresses instead of determining symbolic host names
- **-F** it displays kernels FIB routing information
- **-ee** shows extra columns (MSS and Window) in the output
- **-v** to select verbose option
- **-A** to specify the address family
- **del** to delete a route

```
manan:~$ route -n -v -A inet -F
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.19.4.1       0.0.0.0         UG    20600  0        0 wlp8s0
10.19.4.0       0.0.0.0         255.255.252.0   U     600    0        0 wlp8s0
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 virbr0
192.168.122.0   0.0.0.0         255.255.255.0   U     0      0        0 virbr0
manan:~$ route -ee
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface    MSS   Window irtt
default         _gateway        0.0.0.0         UG    20600  0        0 wlp8s0   0     0      0
10.19.4.0       0.0.0.0         255.255.252.0   U     600    0        0 wlp8s0   0     0      0
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 virbr0   0     0      0
192.168.122.0   0.0.0.0         255.255.255.0   U     0      0        0 virbr0   0     0      0
```

Question 5

a) **Netstat** is used to **print network connections, routing tables, interface statistics, masquerade connections, and multicast memberships**. It is one of the most basic command-line network utility tools and prints information about the Linux networking subsystem. It can be used for **performance measurement** and also to **find faults** in the network.

b) **netstat -at** is used to show all established TCP connections.
The **Proto** column shows us whether the protocol is TCP or UDP. The amount of data in queue to be sent and read is shown by **Send-Q** and **Recv-Q** respectively. The **Local Address** and **Foreign Address** columns show the hosts and ports the listed sockets are connected to. The local end is the machine on which netstat is run, and the foreign end is the other computer. The **State** shows in which state the socket is in. eg - **LISTEN** (wait for some external computer to contact us) and **ESTABLISHED** (ready for communication).

```
manan:~$ netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 manan-Lenovo-ide:domain 0.0.0.0:*               LISTEN
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:ssh             0.0.0.0:*               LISTEN
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN
tcp        0      0 manan-Lenovo-idea:50126 kliqyl174.htmalk.:https ESTABLISHED
tcp        0      0 manan-Lenovo-idea:50236 kliqyl174.htmalk.:https ESTABLISHED
tcp        0      0 manan-Lenovo-idea:50234 kliqyl174.htmalk.:https ESTABLISHED
tcp        0      0 manan-Lenovo-idea:50084 kliqyl174.htmalk.:https ESTABLISHED
tcp        0      0 manan-Lenovo-idea:49872 kliqyl174.htmalk.:https ESTABLISHED
tcp      164      0 manan-Lenovo-idea:60784 10.19.6.44:netbios-ssn  ESTABLISHED
tcp        0      0 manan-Lenovo-idea:58596 10.19.7.181:netbios-ssn ESTABLISHED
tcp        0      0 manan-Lenovo-idea:50054 kliqyl174.htmalk.:https ESTABLISHED
tcp        0      0 manan-Lenovo-idea:50238 kliqyl174.htmalk.:https ESTABLISHED
tcp        0      0 manan-Lenovo-idea:55052 ec2-52-43-230-97.:https ESTABLISHED
tcp        8      0 manan-Lenovo-idea:52994 10.19.5.193:netbios-ssn ESTABLISHED
tcp        0      0 manan-Lenovo-idea:49352 kliqyl174.htmalk.:https ESTABLISHED
tcp        0      0 manan-Lenovo-idea:50078 kliqyl174.htmalk.:https ESTABLISHED
tcp        0      0 manan-Lenovo-idea:50202 kliqyl174.htmalk.:https ESTABLISHED
tcp6       0      0 [::]:ssh                [::]:*                  LISTEN
```

c) **netstat -r** shows the kernel routing table. The **Destination** column shows the destination host or network. The **genmask** column represents the netmask of the network. The **gateway** column shows the gateway of the network. **Iface** shows the network interfaces to which packets of this route will be sent. **G** flag means that the specified gateway should be used while the **U** flag shows that the network is up. **Ref** is the number of references to the route. The **MSS(Maximum Segment Size)** is the size of the largest datagram the kernel can construct for transmission via this route. The **Window** is the maximum amount of data the system can accept in a single burst from a remote host. The acronym **irtt** is the initial round trip time. 0 in MSS and Window represents no changes from commonly used values.

```
manan:~$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         _gateway        0.0.0.0         UG        0 0          0 wlp8s0
10.19.4.0       0.0.0.0         255.255.252.0   U         0 0          0 wlp8s0
link-local      0.0.0.0         255.255.0.0     U         0 0          0 virbr0
192.168.122.0   0.0.0.0         255.255.255.0   U         0 0          0 virbr0
```

d)

```
manan:~$ netstat -i
Kernel Interface table
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
enp9s0    1500        0      0      0 0             0      0      0      0 BMU
lo       65536    19971      0      0 0         19971      0      0      0 LRU
virbr0    1500        0      0      0 0             0      0      0      0 BMU
wlp8s0    1500   914886      0      0 0        405006      0      0      0 BMRU
```

netstat -i is used to show the status of all the interfaces of the machine. **There are 4 interfaces on my computer.**
The **Iface** column contains the name of the interface for which the statistics are shown. **MTU** is the value of Maximum Transmission Unit. **RX, TX** values represent the number of packets received and sent by the interface so far. **OK, ERR, DRP** and **OVR** stand for 'correctly received', 'received but with incorrect checksum', 'dropped because receive buffer was too full' and 'dropped because the kernel couldnt get to it in time' respectively. Flags **B, M, L, U, R** stand for broadcast capability, multicast capability, loopback interface, up and running respectively.

e) **netstat -asu** shows the statistics of all the UDP connections. The table fields are already described above.

```
manan:~$ netstat -asu
IcmpMsg:
    InType0: 4177
    InType3: 133
    OutType3: 167
    OutType8: 4460
Udp:
    106374 packets received
    103 packets to unknown port received
    0 packet receive errors
    31457 packets sent
    0 receive buffer errors
    0 send buffer errors
    IgnoredMulti: 86364
UdpLite:
IpExt:
    InNoRoutes: 145
    InMcastPkts: 36250
    OutMcastPkts: 5184
    InBcastPkts: 86620
    OutBcastPkts: 117
    InOctets: 655986934
    OutOctets: 81481450
    InMcastOctets: 2937393
    OutMcastOctets: 597496
    InBcastOctets: 13773726
    OutBcastOctets: 8771
    InNoECTPkts: 831224
```

f) The **loopback** device/interface is a special, virtual network interface that the computer uses to communicate with itself. It is used for troubleshooting and diagnostics, and also to connect to servers running on the local machine. Consider the situation when a network interface is disconnected, then no communication on the interface is possible, not even the communication between the computer and itself. Loopback interface handles this problem by allowing applications running on the computer to connect to the servers on the same machine. It does not actually represent any hardware. For IPv4, the loopback interface is assigned all the IPs in the 127.0.0.0/8 address block (i.e.127.0.0.1 through 127.255.255.254).

Question 6

*Time when the readings are taken are **12:00 am, 7:00 am, 5:00 pm. (Indian Standard Time)***

	Youtube	Stanford	Codeforces	9anime	Hetzner	Sina Blog
Hop Count 1	8	12	9	6	9	11
Hop Count 2	8	12	9	6	9	11
Hop Count 3	8	12	9	6	9	11

Table 3: Round Trip Times for 6 hosts at 3 different times

a) The obvious common hop is the source of the packets. *213.239.252.241* is a common hop for all. *213.239.245.237* is a common hop for Stanford, Codeforces, 9anime and Hetzner. *213.239.224.242* is a common hop between Codeforces and 9anime. Hops are common because the routes to the given destinations pass through some common internet circles and therefore overlap.

b) Route to the same host might change during different times of the day due to **failure** on an intermediate path or because of **congestion** in that path. **Load balancing** is done to reduce the load of the congested path and therefore packets are redirected to routes having lower traffic. However, I did not experience any change in the path during the day.

c) Sometimes *traceroute* is unable to find the complete path to some hosts. This may happen because some servers/hosts on the route might not be configured to respond to the ICMP packet. Alternately, **firewalls** might also be setup that prevents responses and block ICMP traffic. It may also occur due to the **loss of packets** sent by the intermediate hosts.

d) Yes, it is possible to find the route to certain hosts which fail to respond with ping experiment because both of them use different techniques. *Ping* sends a packet to the specified address and expects a reply, relying on the **reply packet**. On the other hand, *traceroute* works by sending packets with **TTL** (Time To Live) values that gradually increase from packet to packet. Routers decrement TTL values of packets by unit amount, discarding the ones which have reached 0 value, returning ICMP error. Thus *traceroute* relies on **time exceeded packet**. Therefore the scenario can occur if the host blocks ICMP responses or has a firewall that does so.

Question 7

a)

```
manan:~$ sudo arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.19.7.196              ether   54:e1:ad:e0:75:cd   C                     wlp8s0
169.254.147.187                  (incomplete)                              virbr0
_gateway                 ether   ec:44:76:74:60:43   C                     wlp8s0
10.19.5.1                ether   74:e6:e2:20:23:09   C                     wlp8s0
```

sudo arp command is used to show the full arp (**Address Resolution Protocol**) table on the machine. The table is used to translate IP address to destination address on physical network. **Address** field shows the IP address. **HWaddress** shows the corresponding MAC address. **Mask** shows the netmask. **Iface** shows the interface name. **HWtype** tells the hardware type. **C** flag represents complete entries. **M** flag represents permanent entries.

b) **sudo arp -s (ipAddress) (MACaddress)** command is used to add entries into the arp table.
sudo arp -d (ipAddress) command is used to delete entries into the arp table.
It is not possible to add static entries for other subnets therefore the first command fails and the subsequent ones work.

```
manan:~$ sudo arp -s 10.10.10.10 ff:ff:ff:00:00:00
SIOCSARP: Network is unreachable
manan:~$ sudo arp -s 10.19.5.10 ff:ff:ff:00:00:00
manan:~$ sudo arp -s 10.19.5.9 ff:ff:ff:00:00:01
manan:~$ sudo arp -s 10.19.5.8 ff:ff:ff:00:00:02
manan:~$ sudo arp -s 10.19.5.7 ff:ff:ff:00:00:03
manan:~$ sudo arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.19.5.7                ether   ff:ff:ff:00:00:03   CM                    wlp8s0
10.19.5.9                ether   ff:ff:ff:00:00:01   CM                    wlp8s0
10.19.7.196              ether   54:e1:ad:e0:75:cd   C                     wlp8s0
10.19.5.10               ether   ff:ff:ff:00:00:00   CM                    wlp8s0
169.254.147.187                  (incomplete)                              virbr0
_gateway                 ether   ec:44:76:74:60:43   C                     wlp8s0
10.19.5.1                ether   74:e6:e2:20:23:09   C                     wlp8s0
10.19.5.8                ether   ff:ff:ff:00:00:02   CM                    wlp8s0
```

c) **gc_stale_time** is the parameter that defines the amount of time the entries in the cache of the ARP module of the kernel remain valid. It can ve checked via the following command - **cat /proc/sys/net/ipv4/neigh/default/gc_stale_time**. The default value is **60 seconds**.
A **trial and error** method to find this time would be to add a temporary entry and check after a fixed interval of time whether the entry is deleted or not. The time interval of checking can then be reduced for higher precision. **Binary search** technique can also be used.

d) It can occur that two IP addresses are mapped to the same Ethernet address in the case when a router or gateway connects two or more subnet ranges. MAC addressed is used while communicating within the same subnet range. In the ARP table, the IP addresses of the devices in other subnet ranges are mapped to the MAC/ethernet address of the router/gateway connecting those two subnets. Hence the ARP table contains the same ethernet address for the two IPs. The packet from this machine is sent to this router/gateway which sends the packet further to the correct device.

One another situation that needs to be discussed here is that when two PCs with the same MAC address are connected within the same subnet mask. This situation howsoever unlikely is still possible. In such a situation the router will not send packets to either of the two IP's leading to a **100% packet loss** in case they are pinged.

Question 8

The following command is used. The analysis is done for **Lohit hostel**.

nmap -n -sP 10.19.4.1/22

subnet: 10.19.4.1
subnet mask: 255.255.252.0

	22:00:00	01:00:00	06:00:00	10:00:00	14:00:00	18:00:00
Hosts Up	37	29	10	18	19	31

Table 4: Number of Hosts up at different times

It is seen that most people are active during the night hours which seems consistent with the lifestyle of college students. The number of users decreases during early morning and then steadily rises till the evening.
It seems that the numbers are a little low given that 1024 IP addresses are pinged. It is so because the hosts using Windows are not detected due to firewall which destroys the sent ICMP packets.