Assignment 1
Name: Tanvi Ohri, Roll No.: 170123051

Q1. a) Option required: 'c'. Example: ping -c 10 facebook.com sends 10 echo requests with ping.
b) Option required: 'i'. Example: ping -i 10 facebook.com sets the time interval to 10 seconds.
c) Option required: 'l'. Limit for sending such packets by normal users is 3.
Alternate Solution: Set time interval between packets to 0 using 'i'. Example: ping -i 0 yahoo.com.
d) Option required: 's'. Example: ping -s 32 facebook.com sets the packet size to 32 bytes.
Total Packet Size= 8 bytes (ICMP header) + 20 bytes (IP header) + 32 bytes (PacketSize) = 60 bytes

Q2. Internet Connection Used: USB tethering through Airtel's Mobile Network

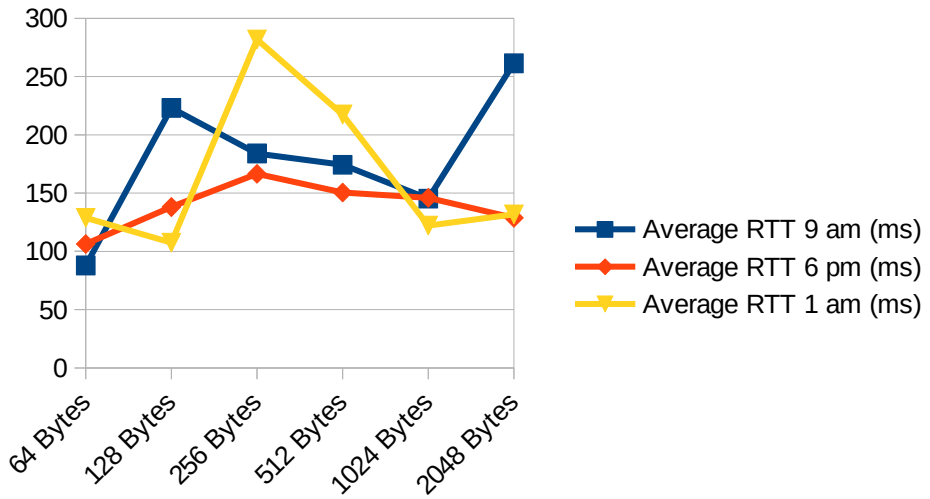
Host Address	IP Address	Geographical Location	Average RTT 9 am (ms)	Average RTT 6 pm (ms)	Average RTT 1 am (ms)	Average RTT
facebook.com	157.240.22.35	California, USA	188.015	146.494	102.585	145.698
myntra.com	104.101.101.38	Brussels, Belgium	132.997	124.937	340.299	199.411
yahoo.com	98.138.219.231	New York, USA	314.950	348.452	289.828	317.743
amazon.in	52.95.120.67	Dublin, Ireland	250.895	276.559	246.205	257.886
flipkart.com	163.53.78.128	Karnataka, India	125.250	138.717	89.794	117.92
news.com.au	23.2.76.132	Virginia, USA	95.241	132.101	114.849	114.064

In my observations, there were no cases with packet loss greater than 0%. Generally, some packet loss may occur due to faulty hardware, network congestion, limit on packet size accepted by the destination server or an unresponsive server.

In general, it is expected that average RTT will increase with increasing distance because number of hops and intermediae nodes increases, thus increasing processing and propagation time. However, from the collected data, this is not visible clearly. This happens because some destination servers might be more efficient in processing and responding than others, thus decreasing their latency, while some might be more busy than others, thus increasing their latency.

Host Chosen: news.com.au

Packet Size (Bytes) / Time	64	128	256	512	1024	2048
Average RTT 9 am (ms)	87.851	223.115	184.050	174.395	145.247	261.436
Average RTT 6 pm (ms)	106.352	138.060	166.595	150.450	145.905	128.730
Average RTT 1 am (ms)	128.740	107.440	281.849	217.430	122.159	131.780



Analysis of Packet Size & RTTs: MTU is the size of the largest Protocol Data Unit (PDU) that can be sent in a packet-based network. The default value (used here) is 1500 bytes. For packet sizes smaller than MTU, no specific pattern is observed. Packets which are larger than the MTU usually have higher RTTs, this is because these packets are split into multiple packets, while those that are smaller than MTU transmit without splitting.

Analysis of Time of the Day & RTTs: The RTT values depend on the network traffic at the destinations. So, latencies are expected to be different at different times of the day. No clear correlation is visible in the collected data because the geographical locations have different time zones.

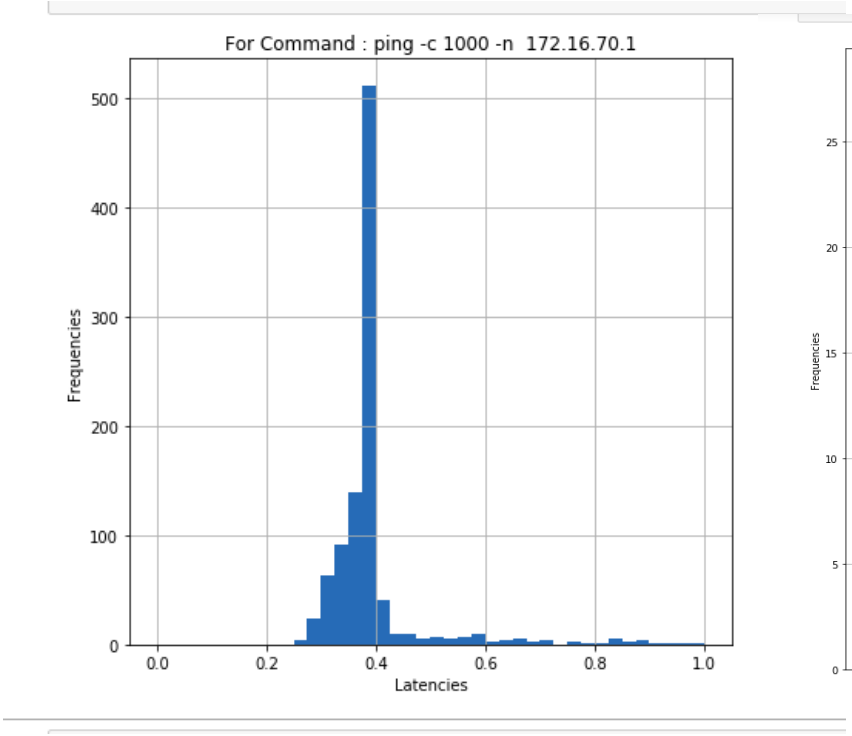
Q3.

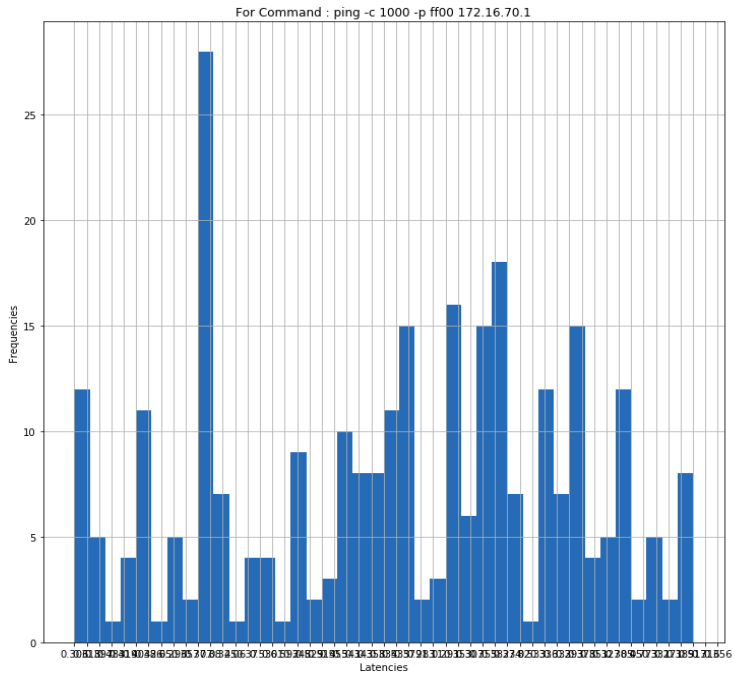
a. Packet loss for both the commands came out to be 0%.

b.

Command	Packets transmitted,received	Packet Loss %age	Min RTT (ms)	Max RTT (ms)	Average RTT (ms)	Median RTT (ms)	Total Time (ms)
ping -n -c 1000 172.16.70.1 > list1.csv	1000,1000	0	0.251	15.537	0.483	0.3835	1021462
ping -p ff00 -c 1000 172.16.70.1 > list2.csv	1000,1000	0	0.244	23.069	0.639	0.364	1020143

c.





d. In the 2nd case, the mean latency is much higher than the 1st. That is, the -n ping is faster than the normal ping, this happens because the -n option does not allow any attempt to reverse lookup the IP address.
In my case there was no packet loss in either case. However, generally, a higher packet loss is expected in the 2nd case. This is because of clock synchronization troubles. Option ‘p’ is used to specify the ping packet pattern. Here, the sent packet is filled with the pattern 11111100000000. As it has only 1 bit transition for diagnosing the problems, it will cause troubles with clock synchronisation.

Q4.

a.

-Left Margin: Names of network interfaces

-What different flags indicate:

1. UP: Kernel modules related to the interface have been loaded.
2. BROADCAST: Interface is configured to handle broadcast packets, essential to obtain IP address via DHCP.
3. RUNNING: Interface is ready to accept data.
4. MULTICAST: Interface supports multicasting which allows a source to send one packet to multiple destinations, provided they are watching out for that packet.

```
tanvi@tanvi-HP-Notebook:~$ ifconfig
enp7s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.16.0.12  netmask 255.255.192.0  broadcast 10.16.63.255
        inet6 fe80::725a:fff:febf:6ff8  prefixlen 64  scopeid 0x20<link>
        ether 70:5a:0f:bf:6f:f8  txqueuelen 1000  (Ethernet)
        RX packets 217831  bytes 91525270 (91.5 MB)
        RX errors 0  dropped 901  overruns 0  frame 0
        TX packets 74457  bytes 10550128 (10.5 MB)
        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 12251  bytes 1206183 (1.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 12251  bytes 1206183 (1.2 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

tanvi@tanvi-HP-Notebook:~$
```

-inet address: IPv4/IPv6 addresses of the interface

-Netmask: Network mask associated with the interface.

- Broadcast: Broadcast address of the network associated with the interface.
- txqueuelen: provides the information about the configured length of transmission queue.
- RX packets: number of packets received, RX errors:number of damaged packets received, dropped: number of dropped packets due to reception errors, overruns: number of received packets that experienced data overruns,frame: number received packets that experienced frame errors.
- TX Packets: number of packets transmitted, TX errors: number of packets that experienced transmission error, dropped: number of dropped transmitted packets due to transmission errors, overruns: number of transmitted packets that experienced data overruns, carriers: number of received packets that experienced loss of carriers, collisions: number of transmitted packets that experienced Ethernet collisions. High value indiactes network congestion.

b.

1. add addr/prefixlen : used to add an IPv6 address to an interface. Syntax: ifconfig interface add addr/prefixlen

2. del addr/prefixlen : used to remove an IPv6 address to an interface. Syntax: ifconfig interface del addr/prefixlen

3. -a : used to display all the interfaces available, even if they are down. Syntax: ifconfig -a

4. -s : Display a short list, instead of details. Syntax: ifconfig -s

c. -Destination : The destination network or host.

-Gateway : The gateway address or * if none set.

-Genmask : The netmask for the destination net;

For Host destination-> 255.255.255.255,

For Default Route -> 0.0.0.0

```
tanvi@tanvi-HP-Notebook:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    100    0        0 enp0s20u3
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 enp0s20u3
192.168.42.0    0.0.0.0         255.255.255.0   U     100    0        0 enp0s20u3
tanvi@tanvi-HP-Notebook:~$
```

-What different flags indicate :

1. U: route is up 2. G: use gateway

-Metric : The distance to the target. Usually measured as number of hops.

-Ref : Number of references to this route.

-Use : Count of lookups for the route.

-Iface : Interface to which packets for this route will be sent

```
tanvi@tanvi-HP-Notebook:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.42.129  0.0.0.0         UG    100    0        0 enp0s20u3
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 enp0s20u3
192.168.42.0    0.0.0.0         255.255.255.0   U     100    0        0 enp0s20u3
tanvi@tanvi-HP-Notebook:~$ route -e
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         _gateway        0.0.0.0         UG        0 0          0 enp0s20u3
link-local      0.0.0.0         255.255.0.0     U         0 0          0 enp0s20u3
192.168.42.0    0.0.0.0         255.255.255.0   U         0 0          0 enp0s20u3
tanvi@tanvi-HP-Notebook:~$
```

d.

1. -n: show numerical addresses instead of trying to determine symbolic hostnames. This is useful if you are trying to determine why the route to your nameserver has vanished.

2. -e: use netstat(8)-format for displaying the routing table.

3. del: delete a route

4. add: add a new route

5. gw: route packets via a gateway.

```
tanvi@tanvi-HP-Notebook:~$ sudo route del default
tanvi@tanvi-HP-Notebook:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 enp0s20u3
192.168.42.0    0.0.0.0         255.255.255.0   U     100    0        0 enp0s20u3
tanvi@tanvi-HP-Notebook:~$ sudo route add default gw 192.168.42.110
tanvi@tanvi-HP-Notebook:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.42.110  0.0.0.0         UG    0      0        0 enp0s20u3
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 enp0s20u3
192.168.42.0    0.0.0.0         255.255.255.0   U     100    0        0 enp0s20u3
```

Q5.

a. netstat (network statistics) is a command-line tool that displays network connections (both incoming and outgoing), routing tables, and a number of network interface statistics.

```
tanvi@tanvi-HP-Notebook:~$ netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN
tcp        0      0 tanvi-HP-Notebook:36732 server-13-33-169-:https ESTABLISHED
tcp        0      0 tanvi-HP-Notebook:35736 180.149.60.168:http     ESTABLISHED
tcp        0      0 tanvi-HP-Notebook:54854 maa05s02-in-f10.1:https ESTABLISHED
tcp        0      0 tanvi-HP-Notebook:39376 maa05s04-in-f3.1e1:http TIME_WAIT
tcp        0      0 tanvi-HP-Notebook:36376 maa03s21-in-f2.1e:https ESTABLISHED
tcp        0      0 tanvi-HP-Notebook:54856 maa05s02-in-f10.1:https ESTABLISHED
tcp        0      0 tanvi-HP-Notebook:57142 104.25.58.103:https     ESTABLISHED
tcp        0      0 tanvi-HP-Notebook:58106 maa05s02-in-f14.1:https ESTABLISHED
tcp        0      0 tanvi-HP-Notebook:52326 maa03s26-in-f14.1:https ESTABLISHED
tcp        0      0 tanvi-HP-Notebook:44512 maa03s28-in-f10.1:https ESTABLISHED
tcp        0      0 tanvi-HP-Notebook:58100 maa05s02-in-f14.1:https ESTABLISHED
tcp        0      0 tanvi-HP-Notebook:51926 maa03s29-in-f10.1:https ESTABLISHED
tcp        0      0 tanvi-HP-Notebook:49140 maa05s02-in-f4.1e:https ESTABLISHED
tcp        0      0 tanvi-HP-Notebook:33610 104.25.57.103:https     ESTABLISHED
tcp        0      0 tanvi-HP-Notebook:49270 maa05s02-in-f4.1e:https TIME_WAIT
tcp        0      0 tanvi-HP-Notebook:56724 maa03s20-in-f3.1e:https ESTABLISHED
tcp        0      0 tanvi-HP-Notebook:39460 maa05s04-in-f3.1e1:http TIME_WAIT
tcp        0      0 tanvi-HP-Notebook:44510 maa03s28-in-f10.1:https ESTABLISHED
tcp        0      0 tanvi-HP-Notebook:50148 117.18.237.29:http      ESTABLISHED
tcp        0      0 tanvi-HP-Notebook:39456 maa05s04-in-f3.1e1:http TIME_WAIT
tcp        0      0 tanvi-HP-Notebook:41890 maa03s20-in-f14.1:https ESTABLISHED
tcp        0      0 tanvi-HP-Notebook:39790 maa05s10-in-f3.1e:https ESTABLISHED
tcp        0      0 tanvi-HP-Notebook:59966 104.27.176.254:https    ESTABLISHED
tcp        0      0 tanvi-HP-Notebook:37362 maa05s09-in-f1.1e:https TIME_WAIT
tcp        0      0 tanvi-HP-Notebook:46228 maa05s01-in-f18.1:https ESTABLISHED
tcp        0      0 tanvi-HP-Notebook:39596 maa05s05-in-f8.1e:https ESTABLISHED
tcp        0      0 tanvi-HP-Notebook:38844 maa03s20-in-f6.1e:https ESTABLISHED
tcp        0      0 tanvi-HP-Notebook:51954 maa03s29-in-f10.1:https ESTABLISHED
tcp        0      0 tanvi-HP-Notebook:47956 maa05s03-in-f3.1e:https TIME_WAIT
tcp        0      0 tanvi-HP-Notebook:33632 maa03s22-in-f1.1e:https ESTABLISHED
tcp        0      0 tanvi-HP-Notebook:56168 maa05s03-in-f10.1:https ESTABLISHED
tcp        0      0 tanvi-HP-Notebook:51670 maa05s10-in-f18.1:https ESTABLISHED
tcp        0      0 tanvi-HP-Notebook:34020 maa05s09-in-f3.1e:https ESTABLISHED
```

b. Option required: at
Output Fields Explained:
-Proto: tell us if the socket listed is TCP or UDP-
-Recv-Q and Send-Q: tell us how much data is in the queue for that socket, waiting to be read and sent respectively
-Local Address and Foreign Address: tell to which hosts & ports the listed sockets are connected. Local: Computer on which the netstat command is run, that is my system, Foreign: Other computer on the network.
-State: tells in which state the listed sockets are. "LISTEN" means wait for some external computer to contact you, "ESTABLISHED" means ready for communication and "TIME_WAIT" means the foreign or remote machine has already closed the connection, but that the local program has failed to follow.

c. netstat -r lists the current entries in the routing table of the system.
Output Fields Explained:
-Destination : the pattern that the destination of a packet is matched to. When a packet has to be sent over the network, column entries are scanned starting from the top, and the first line with a matching destination is then used further.
-Gateway : tells the computer where to send a packet that matches the destination of the same line.
-Genmask : tells how many bits from the start of the ip address are used to identify the subnet from the ip address.
-What different flags indicate :
1. U: this is an active line. 2. G: line uses a gateway
-MSS : value of the Maximum Segment Size for this line.

```
tanvi@tanvi-HP-Notebook:~$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         _gateway        0.0.0.0         UG        0 0          0 enp7s0
10.16.0.0       0.0.0.0         255.255.192.0   U         0 0          0 enp7s0
link-local      0.0.0.0         255.255.0.0     U         0 0          0 enp7s0
```

-Window: window size, or number of TCP packets that can be sent before at least one of them has to be acknowledged.
-irtt: Initial Round Trip Time
-Iface: tells which network interface should be used for sending packets that match the destination.

d. Option required: i
Number of Interfaces on my system: 2

```
tanvi@tanvi-HP-Notebook:~$ netstat -i
Kernel Interface table
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
enp7s0    1500    47682      0    324 0          14697      0      0      0 BMRU
lo       65536     3982      0      0 0           3982      0      0      0 LRU
```

e. Option required: su

```
tanvi@tanvi-HP-Notebook:~$ netstat -su
IcmpMsg:
    InType3: 45
    OutType3: 47
Udp:
    7288 packets received
    47 packets to unknown port received
    0 packet receive errors
    4505 packets sent
    0 receive buffer errors
    0 send buffer errors
    IgnoredMulti: 4982
UdpLite:
IpExt:
    InMcastPkts: 3084
    OutMcastPkts: 164
    InBcastPkts: 5099
    OutBcastPkts: 1
    InOctets: 19372267
    OutOctets: 2328699
    InMcastOctets: 238278
    OutMcastOctets: 18028
    InBcastOctets: 591429
    OutBcastOctets: 65
    InNoECTPkts: 33355
```

f. The loopback device is a special, virtual network interface that the system uses to communicate with itself. It is used mainly for diagnostics & troubleshooting, & to connect to servers running on the local machine. The loopback interface does not represent any actual hardware, but exists so applications running on your computer can always connect to servers on the same machine. The loopback device is sometimes used as purely a diagnostic tool. But it is also helpful when a server offering a resource you need is running on the system itself. For example, if we run a web server, we have all our web documents and could examine them file by file. On running netstat -ie or ifconfig, the details of lo interface (loopback interface) can be seen as shown below.

```
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 4471  bytes 381922 (381.9 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4471  bytes 381922 (381.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Q6. Traceroute is a network tool used to determine the "path" packets take from one IP address to another. It provides the hostname, IP address, and the response time to a ping

a.

Time/Host	facebook.com	myntra.com	yahoo.com	amazon.in	flipkart.com	news.com.au
10 am	13	31 (!H)	19	19	19	19 (!H)
6 pm	13	64 (incomplete)	18	64 (incomplete)	64 (incomplete)	64 (incomplete)
11 pm	13	64(incomplete)	24	43 (!H)	41 (!H)	64 (incomplete)

!H means means that the machine received ICMP message "destination host unreachable".
Common Hops: 10.16.0.254 (Subansiri Hostel Gateway), 172.17.0.1, 192.168.193.1, 14.139.196.17, 10.119.254.241

b. The destination server address for yahoo.com is different at times 10 am (98.137.246.7), 6 pm (98.138.219.231) and 11 pm (98.137.246.8). This maybe because of different network traffic at different times. Hence, some load balancing takes place, where some requests are redirected to a different server, thus reducing network congestion.

c. Traceroute may not find a complete path to some host. For example, in the incomplete and !H cases. This is because some servers are not configured to respond to ICMP traffic or may have firewalls set up that block this traffic. Organizations do this to keep their internal network topology protected.

d. Yes, is is possible. This is because ping sends an ICMP segment from source to destination, that traverses networks via routing rules and expects an ICMP reply from the host. Traceroute does not expect an ICMP reply from the server. Traceroute works by targeting the final hop, but limiting the TTL and waiting for a time exceeded message, and then increasing it by one for the next iteration. Therefore, the response it gets is not an ICMP echo reply from the host, but a time exceeded message from that host.

Q7. a. Command used for displaying full arp table is “arp”.

```
tanvi@tanvi-HP-Notebook:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
_gateway                 ether   4c:4e:35:97:1e:ef   C                     enp7s
0
```

-Address: IP address of the other workstation to which communication was established.
-Hwtype: type of the network interface through which the connection was established. HWaddress is the MAC address of the other system.
-Flags: denote how the entry has been added to the table. Here, learned by the system, C.
-Iface: gives the name of the network interface on the system.

b. arp -s <IP_address> <mac_address> can be used to add an entry to the ARP table permanently. To add a new entry temporarily, the word ‘temp’ is added after the command.
arp -d <IP_address> can be used to delete an entry from the ARP table.

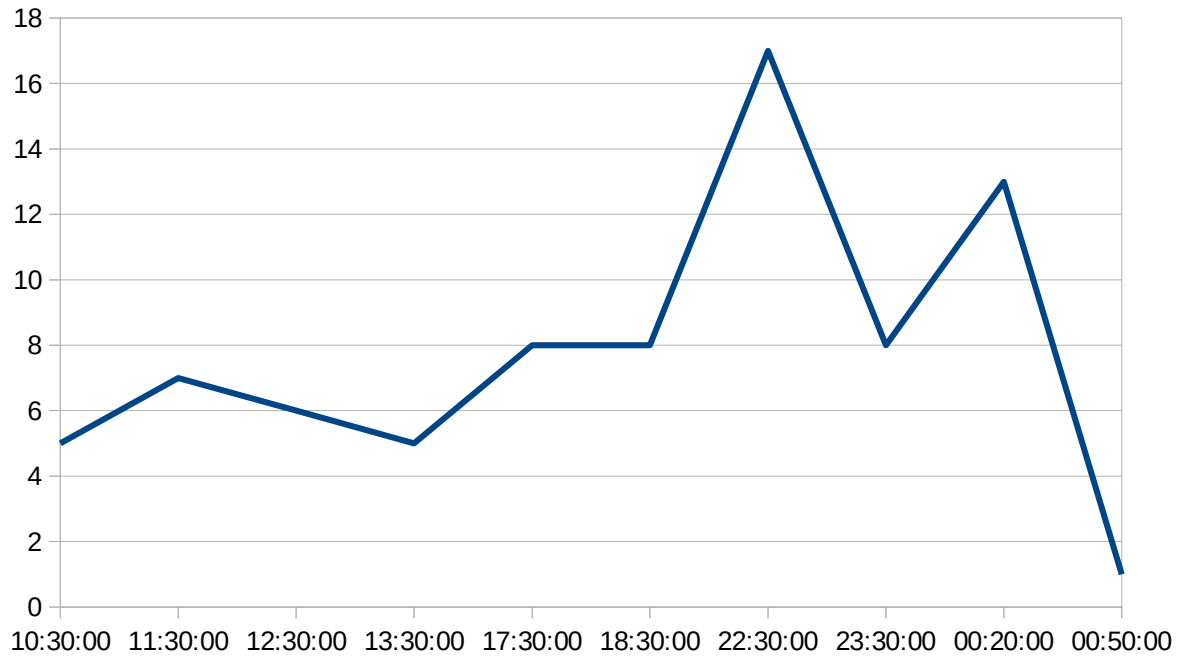
```
tanvi@tanvi-HP-Notebook:~$ sudo arp -s 10.16.00.17 4c:4e:35:97:1e:ef
tanvi@tanvi-HP-Notebook:~$ sudo arp -s 10.16.00.19 4c:4e:35:97:1e:ef
tanvi@tanvi-HP-Notebook:~$ sudo arp -s 10.16.00.20 4c:4e:35:97:1e:ef
tanvi@tanvi-HP-Notebook:~$ sudo arp -s 10.16.00.40 4c:4e:35:97:1e:ef
tanvi@tanvi-HP-Notebook:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.16.0.40               ether   4c:4e:35:97:1e:ef   CM                    enp7s0
10.16.0.20               ether   4c:4e:35:97:1e:ef   CM                    enp7s0
10.16.0.17               ether   4c:4e:35:97:1e:ef   CM                    enp7s0
_gateway                 ether   4c:4e:35:97:1e:ef   C                     enp7s0
10.16.0.19               ether   4c:4e:35:97:1e:ef   CM                    enp7s0
```

c.Parameters: the setting gc_stale_time affects how often the ARP cache is checked for stale entries. The value base_reachable_time_ms actually controls how long an ARP cache entry is valid. But each new ARP cache entry will actually receive a time to live value randomly set somewhere between base_reachable_time_ms / 2 and 3*base_reachable_time_ms / 2.
File /proc/sys/net/ipv4/neigh/default contains these values. On my PC, gc_stale_time is 60 seconds and base_reachable_time_ms is 30000 milliseconds.
Trial and Error method: Add a temporary entry in the table and check the table after fixed intervals of time. The time after which it is deleted is approximately the required cache timeout.

d. For two systems in the same subnet, the ARP table stores the respective MAC addresses, but if the destination system is on a different subnet, then the MAC address of the destination subnet router will be stored in the ARP table. So, for two destination systems on a different subnet than the source, the two IPs will have the same MAC Addresses. After reaching the destination router, the router is responsible for routing the message to the correct destination system.

Q8. LAN Subnet Address Used: 10.16.0.254/22 scans network of Subansiri Hostel.

Time	10:30 AM	11:30 AM	12:30 PM	1:30 PM	5:30 PM	6:30 PM	10:30 PM	11:30 PM	12:20 AM	12:50 AM
No. of Active Hosts	5	7	6	5	8	8	17	8	13	1



Analysis:

In the morning (during class/lab hours), number of hosts is low, this continues until lunch time. There is a peak around 5 to 11 pm when most people are in the hostel. There is a decline afterwards because of sleeping hours around 1 am.