ASSIGNMENT

Aditya vardhan Gara

CS 349 **170101003**

Question 1:

A) ping -c <no. of echoes> IP/host

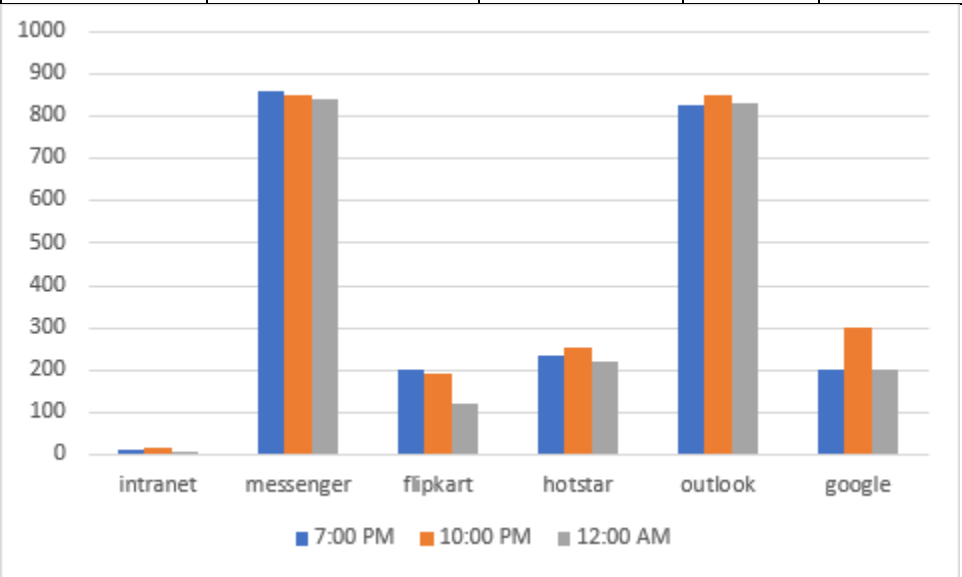
B) ping -i <intervel> IP/host

C) ping -I IP/host (normal users can send upto 3 such requests)

D) ping -s <pack size> IP/host (32+8<ICMP>+20<IP>=60GB)

Question 2:

Host	IP	Location	7 PM	10 PM	0 AM	Avg. loss %
Intranet	172.17.0.23	IIT G	12.2	13.1	7.1	0
Messenger	157.240.22.19	USA	861.4	850.1	840.4	4
flipkart	163.53.78.128	Bangalore	200.6	190.3	120.4	0
hotstar	99.84.224.39	USA	233.4	251.3	220.7	0
outlook	40.97.161.50	USA	826.4	851.2	830.1	0
Google	216.58.196.206	USA	234.1	300.1	200.1	0



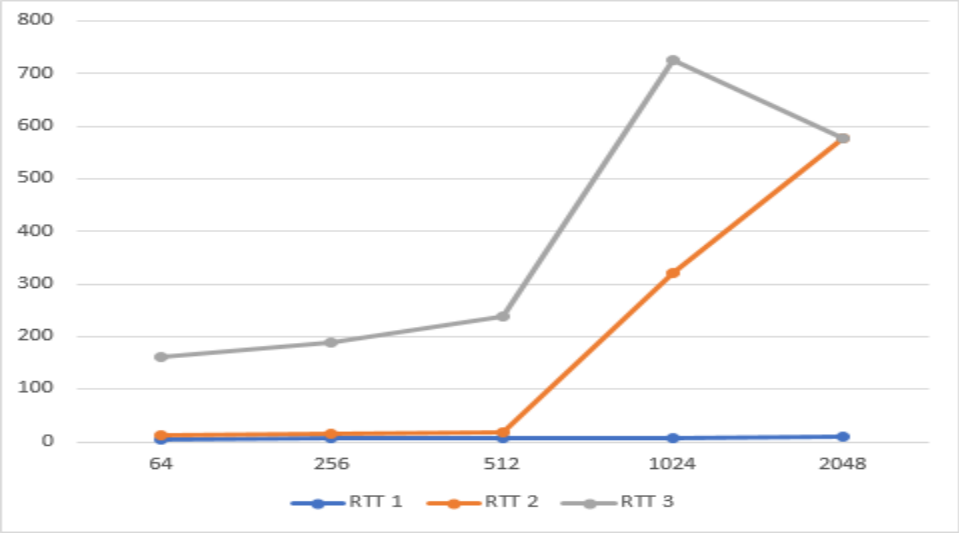
Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination. Packet loss is either caused by errors in data transmission, typically across wireless networks, network congestion. Packet loss is measured as a percentage of packets lost with respect to packets sent. I got 100% packet loss when I ping google.com with packet size 2048bytes. The destination server dropped all the ping ICMP packets.

Factors affecting RTT :-

RTT w.r.t distance: Larger the distance longer it takes to propagate the packets (propagation delay increases).It also causes increase in the number of nodes in between (processing delay increases). It is a weak relation because it also depends on network traffic, server capacities and others.

RTT w.r.t packet size: It is observed that as packet size increases the RTT also increases. But the trends are not actually same. Some deviations occur at size around 1536 Bytes. Sudden peak is observed at 1536 bytes.

size	64	256	512	1024	2048
RTT 1	6.124	6.753	7.805	8.384	10.356
RTT 2	5.815	8.099	10.147	313.7	567.425
RTT 3	150.106	175.387	221.345	405.908	100% loss

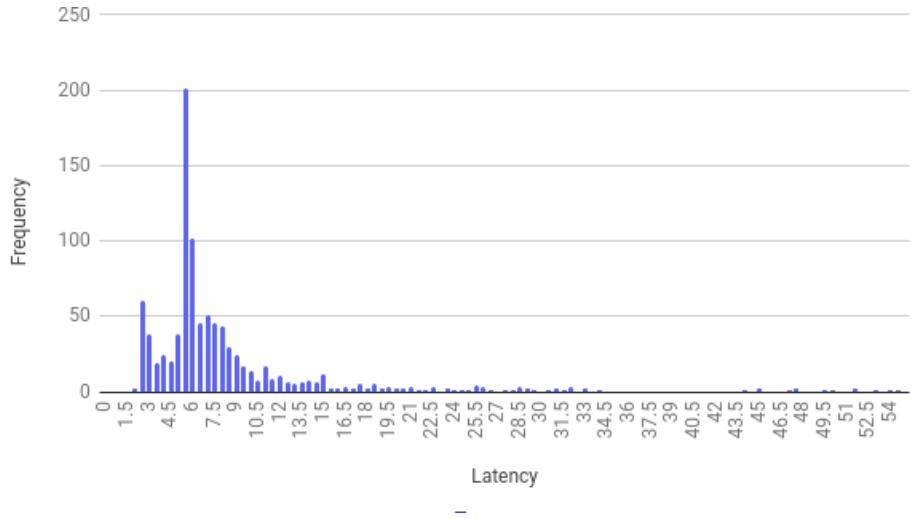


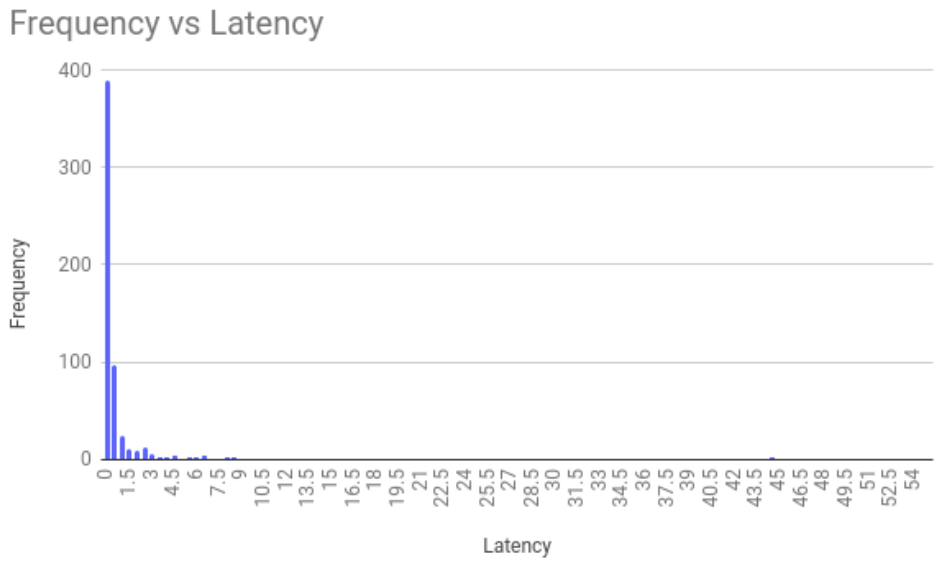
RTT w.r.t time: RTT also depends on the time because the more the congestion in network the more the time taken for RTT. RTT is high in the peak hours of network usage and comparitively lesser in the others which can be depicted from the above table.

Question 3:

command	Packets sent	Packets Received	Packet Loss Rate	Minimum Latency	Max	Mean	Median
-n	1000	998	0.2%	2.508	186.423	8.399	5.267
-p ff00	1000	990	1%	2.619	262.321	8.209	5.014

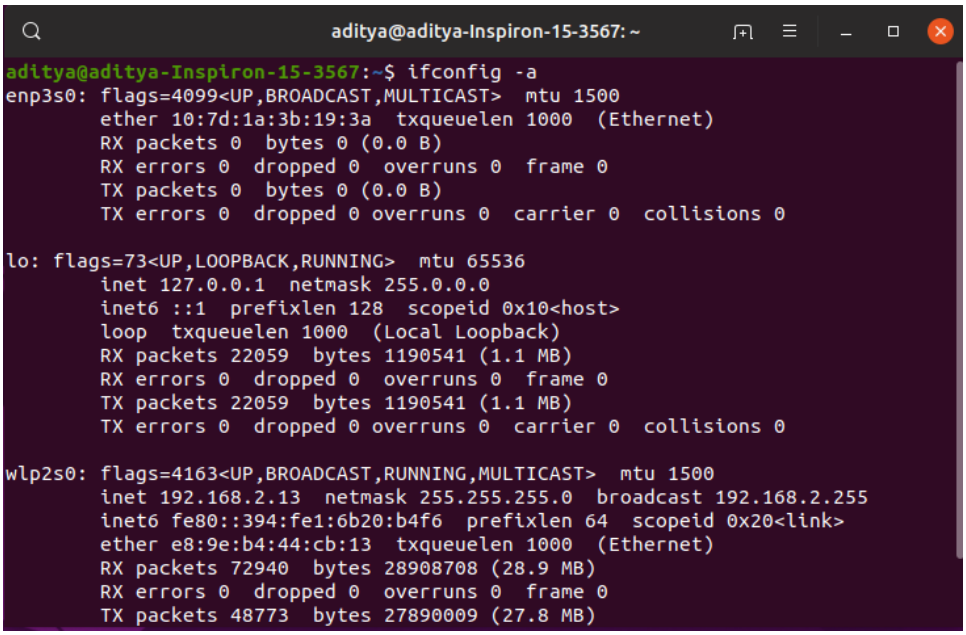
Based on below graph it resembles normal distribution. When '-n' is used there is no look is made up symbolic for host address so it will be little faster. when is ff00 is added then it causes synchronisation problems and thats why packets loss rate is high.


250
200
150
100
50
0
Frequency
0
1.5
3
4.5
6
7.5
9
10.5
12
13.5
15
16.5
18
19.5
21
22.5
24
25.5
27
28.5
30
31.5
33
34.5
36
37.5
39
40.5
42
43.5
45
46.5
48
49.5
51
52.5
54
Latency


Frequency vs Latency
400
300
200
100
0
Frequency
0
1.5
3
4.5
6
7.5
9
10.5
12
13.5
15
16.5
18
19.5
21
22.5
24
25.5
27
28.5
30
31.5
33
34.5
36
37.5
39
40.5
42
43.5
45
46.5
48
49.5
51
52.5
54
Latency

Question 4:

A)



wlp7so - It denotes the driver name and the unit number

inet - shows the ipv4 address of the interface

inet6 - shows the ipv6 address of the interface where fe80 denotes the subnet(/64) and 8b65:b265:7247:21ad denotes the host part. Link means that scope of the ip is on the link. Cant be used outside. Global means can be used any where.

Ipv4 - 192.168.0.2 is ipv4 address of the machine , broadcast shows the broadcast address for the local network (if you want to send to everyone on the network), Netmask shows that it is a class C 24 bit netmask i.e 192.168.0(24bits) is the subnet whereas 2 is the host part.

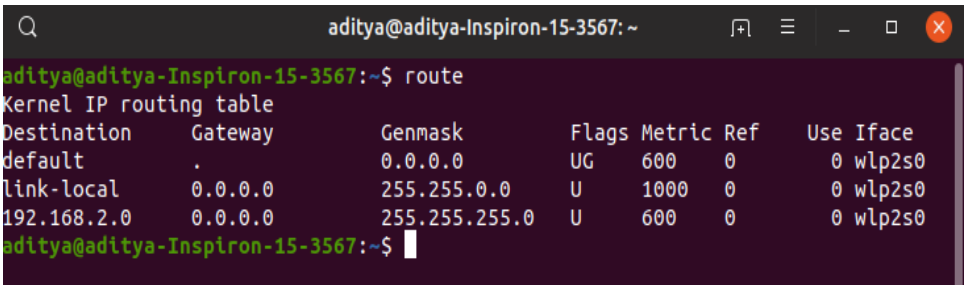
MTU - maximum transfer units in bytes.

Rx packets – no of packets received **, Tx packets –** no of packets transmitted errors(crc error packets). **dropped packets** (packets received but not destined for machine). frame counts only misaligned frames, it means frames with a length not divisible by 8. **Overruns** counts that times when there is fifo overruns, caused by the rate at which the buffer gets full and the kernel isn't able to empty it.carrier is a carrier related error (ie. duplex mismatch). **Collisions** is the number of collisions that occurred. **Txqueuelen** is the size of the transmit queue of the NIC.

B)

1. **ifconfig -a** : display all interfaces which are currently available, even if down.
2. **ifconfig -s** : display a short list.
3. **ifconfig -v** : be some more verbose for some error conditions.
4. **ifconfig[name of interface][up] :** this cause corresponding interface to active.
5. **ifconfig[name of interface][down] :** this cause corresponding interface to shut down

C)



Destination : Destination network or host.

Gateway : The gateway address.

Genmask : The netmask for destination net; 255.255.255.255 for a host destination and 0.0.0.0 for the default route.If we specify only the destination network(last 8 bits 0), then 255.255.255.0 is used as netmask.

Flags : Possible flags include. U (route is up) ; G (use gateway).

Metric : The distance to the target(usually counted in hops). It is not used by recent kernels.

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

Ref : Number of references to this route. **Use :** Count of lookups for the route.

Link-local : It is a network address that is valid only for communications with the network segment(link)or the broadcast that the host is connected to.So these addresses are directly forwarded to the interface without need of the gateway.

Route Options

- ✓ **-A <fly>** use the fly addresses(ipv4,ipv6 etc).
- ✓ **-F** operate on the kernel's FIB(Forwarding Information Base) rounding table. This is default.
- ✓ **-C** operates on the kernel's routing table.
- ✓ **-v** select verbose.
- ✓ **-n** show numeric pics instead of default,link-local etc.
- ✓ **-e** use netsat format to display.
- ✓ **del/add** delete or add new route(specify addr, dateway, interface, netmask, type(nrt/host)).

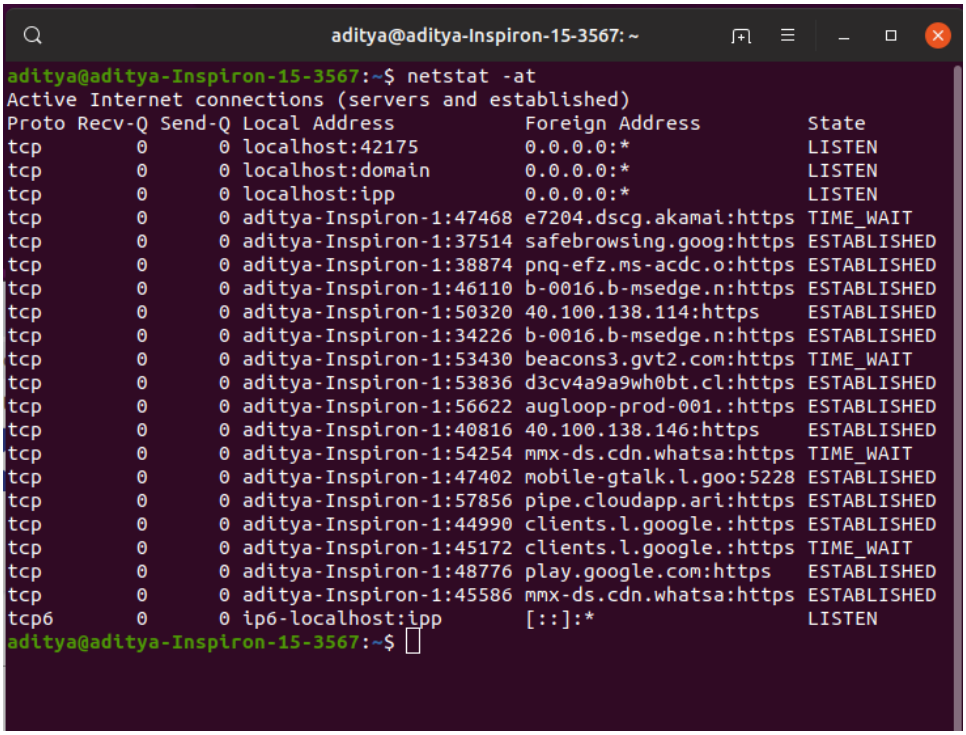
Add<target ip><type>netmask<NM>gw<gateway>metric<M>,dev<device>

Question 5:

A) **Netstat** is a networking utility that has multiple usages. It can print network connections, routing tables, interface statistics, masquerade connections and multicast memberships depending on the first flag passed. It is used to display the status of TCP, SCTP and UDP endpoints in table.

B) **netsat -at** is used for listing all TCP ports.

‘**a**’ stands for listing all ports and **’t’** stands for TCP. Therefore, - **at** gives all the TCP connections.



Fields in netstat table are:

Proto column shown gives the name of the protocol being used by the particular connection.

Recv-Q is the count of bytes not copied by the user program connected to this socket.

Send-Q is the count of bytes not acknowledged by the remote host.

Local Address is the IP address of the local computer and the port number being used for this particular connection appear in the Local Address column.

Foreign Address column contains the address of the remote computer and the port number being used for particular connection.

State

CLOSED - Indicate that the server has received an ACK signal from the client and the connection is closed

CLOSE_WAIT -The remote end has shut down, waiting for the socket to close.

ESTABLISHED -The socket has an established connection.

LISTENING -Indicates that the server is ready to accept a connection.

C) **netstat -r** shows the routing table.

The fields are same as the output of the route command explained above. The extra fields are :-

MSS : Default maximum segment size for TCP connections over this route.

Window : Default window size for TCP connections over this route.

irtt : Initial RTT(Round trip time). The kernel uses this to guess about the best TCP protocol parameters without waiting on (possibly slow) answers.

D) **netstat -i** can be used to display the status of all the active network interfaces.

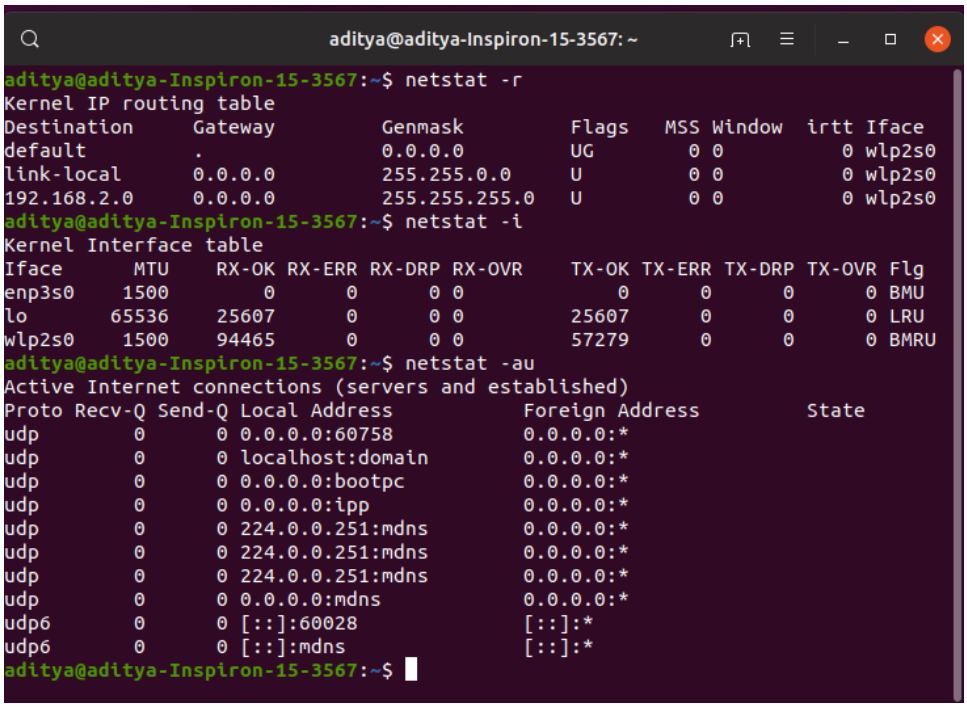
My system has 3 interfaces as shown in the above picture, The MTU and Met fields show the current MTU and metric values for that interface.The RX and TX columns show how many packets have been received or transmitted.

E) **netstat -au** is used to show the statistics of all UDP connections.

F) **Loopback Interface:**
The loopback device is a special, virtual network interface that your computer uses to communicate with itself. It is used mainly for diagnostics and troubleshooting, and to connect to servers running on the local machine.

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. Whereas interfaces might be removed or addresses changed based on network topology changes, the loopback interface address never changes and is always up if the device is up.
- ✓ **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.



Question 6:

A) The readings are taken at 1:00PM, 7:00PM, 0:00AM(IST) respectively:

	INTRANET	FACEBOOK	AMAZON	FLIPKART	YOUTUBE	GOOGLE
Hop count #1	3	10	12	11	13	13
Hop count #2	3	10	12	11	13	13
Hop count #3	3	10	12	11	13	13

The obvious common host is **192.168.2.1** (my static ip) and **10.9.0.254** (my machine) which are same in all 6 hosts 172.16.85.229 and 103.198.140.54 is same all host expect intranet and facebook.com. Hops are common because of the reason that routes to these destinations pass through the same internet circles and hence overlap.

B) Because of changes of network traffic route to the hosts changes at different times of the day.The load balancing is done to reduce the load of congested path.

C) Sometimes, traceroute might not find a complete path to some host. Some servers/hosts along the path may have not been configured to respond to the ICMP Traffic or may have set up firewalls which block the ICMP Traffic. However, they still send the data to the next hop as there are results that follow. Many network providers disable ICMP traffic if their network is under heavy load.

It is possible to find the route to certain hosts which fail to respond with ping experiment. The ping and traceroute both use the ICMP Packets but there working is different. Ping is straight ICMP from point A to point B, that traverses networks via routing rules and expects a ICMP Reply from the host. Most probably the server is blocking the reply. On the other hand, Traceroute sends packets with TTL values that gradually increase from packet to packet. Routers decrement TTL values of packets by one and discard packets whose TTL value has reached zero, returning the ICMP error (ICMP Time Exceeded). Traceroute looks for the ICMP Time exceeded packet and not the ICMP Reply Packet, and that is why it might be possible.

Question 7:

A) ARP is the adress resolution protocol. To see the complete arp table we can use command: **arp -a**

Fields of arp command are: Adress(shows the IP), HWtype(type of network connection ether/wifi), HWare adress of device, flags, mask, Interface.

B) To add entry to arp table we use arp –s IP MACadress and to delete we use arp –d IP MACadress.

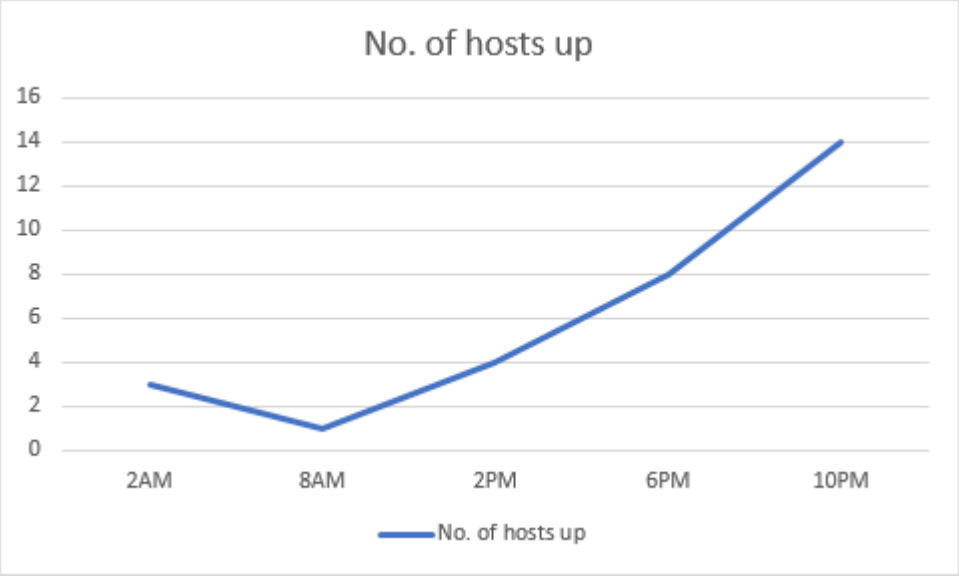
C)Entries stay cached in the ARP table for 60 seconds. A trial & error method to discover the timeout value is to add a temporary entry in the arp table and keep on checking the arp table after fixed intervals of time (say 5 seconds). The time after which it disappears is approximately the required cache timeout. For a better approximation, decrease the interval length. Alternatively, one can use binary search also for finding the cache time, for e.g. – Add a temporary entry in ARP and check after 5000ms. If then entry has been deleted, then add the entry again and check after 2500ms. Continue in Binary sense to find the cache time.

D) The scenario where two IP’s can map to same Ethernet Address is when a router or a gateway connects two or more subnet ranges. When communicating with machines on the same subnet range, MAC address is used for directing the packages. In the. ARP Table, the IP’s of the devices which are connected in the other subnet range have the ethernet address/MAC address as that of the Router or Gateway which connects the two subnet ranges. ARP table is referred to convert these IP addresses to the MAC address and packets are sent to it(router/gateway). The router then uses it’s routing table and sends the packet further to the correct device.

```
aditya@aditya-Precision-Tower-3620: ~
aditya@aditya-Precision-Tower-3620:~$ sudo arp -v
Address                  HWtype  HWaddress           Flags Mask            Iface
_gateway                 ether   38:22:d6:0c:ef:99   C                     enp0s31f6
Entries: 1      Skipped: 0      Found: 1
aditya@aditya-Precision-Tower-3620:~$ sudo arp -s 172.16.115.105 ff:ff:ff:00:00
aditya@aditya-Precision-Tower-3620:~$ sudo arp -s 172.16.115.104 ff:ff:ff:00:00
SIOCSARP: Network is unreachable
aditya@aditya-Precision-Tower-3620:~$ sudo arp -s 172.16.115.101 ff:ff:ff:00:00
SIOCSARP: Network is unreachable
aditya@aditya-Precision-Tower-3620:~$ sudo arp -s 172.16.115.102 ff:ff:ff:00:00
aditya@aditya-Precision-Tower-3620:~$ sudo arp -s 172.16.115.103 ff:ff:ff:00:00
aditya@aditya-Precision-Tower-3620:~$ sudo arp -s 172.16.115.104 ff:ff:ff:00:00
aditya@aditya-Precision-Tower-3620:~$ sudo arp -v
Address                  HWtype  HWaddress           Flags Mask            Iface
172.16.115.104           ether   ff:ff:ff:00:00:68   CM                    enp0s31f6
172.16.115.103           ether   ff:ff:ff:00:00:67   CM                    enp0s31f6
_gateway                 ether   38:22:d6:0c:ef:99   C                     enp0s31f6
172.16.115.102           ether   ff:ff:ff:00:00:66   CM                    enp0s31f6
Entries: 4      Skipped: 0      Found: 4
aditya@aditya-Precision-Tower-3620:~$ sudo arp -d 172.16.115.102
aditya@aditya-Precision-Tower-3620:~$ sudo arp -d 172.16.115.1032
172.16.115.1032: Unknown host
aditya@aditya-Precision-Tower-3620:~$ sudo arp -d 172.16.115.103
aditya@aditya-Precision-Tower-3620:~$ sudo arp -v
Address                  HWtype  HWaddress           Flags Mask            Iface
172.16.115.104           ether   ff:ff:ff:00:00:68   CM                    enp0s31f6
_gateway                         (incomplete)                              enp0s31f6
Entries: 2      Skipped: 0      Found: 2
aditya@aditya-Precision-Tower-3620:~$
```

Question 8:

Nmap can be considered as a prominent command which allows you to know the condition of a host. I ran nmap command on my lobby IP range and made a scenario of active hours.



We can see that the peaks in the graph are observed at 10PM and usage is dropped at class times in the morning and afternoon and also at late nights.