CS349 NETWORKS LAB ASSIGNMENT – 1

NAME – SUNNY KUMAR **ROLL NO** – 170101068

1) ***Internet Ping commands:***

a) **'-c'** is the option required to specify the number of echo requests to send with ping command, i.e. **ping -c <no. of packets> IP**.

b) **'-i '** is the option required to set time interval (in seconds), rather than the default one second interval, between two successive ping ECHO_REQUESTs, i.e. **ping -i <time interval> IP**.

c) **'-l'** is used to send ECHO_REQUEST packets to the destination one after another without waiting for a reply, i.e. **ping -l <preload> IP**. Normal users can send maximum **3** such ECHO_REQUEST packets, i.e. preload<=3. Only super user may select preload more than 3.

d) **'-s'** is used to set ECHO_REQUEST packet size, i.e. **ping -s <size> IP**. If the packetsize is set to 32 bytes, the total packet size would be 40 bytes.

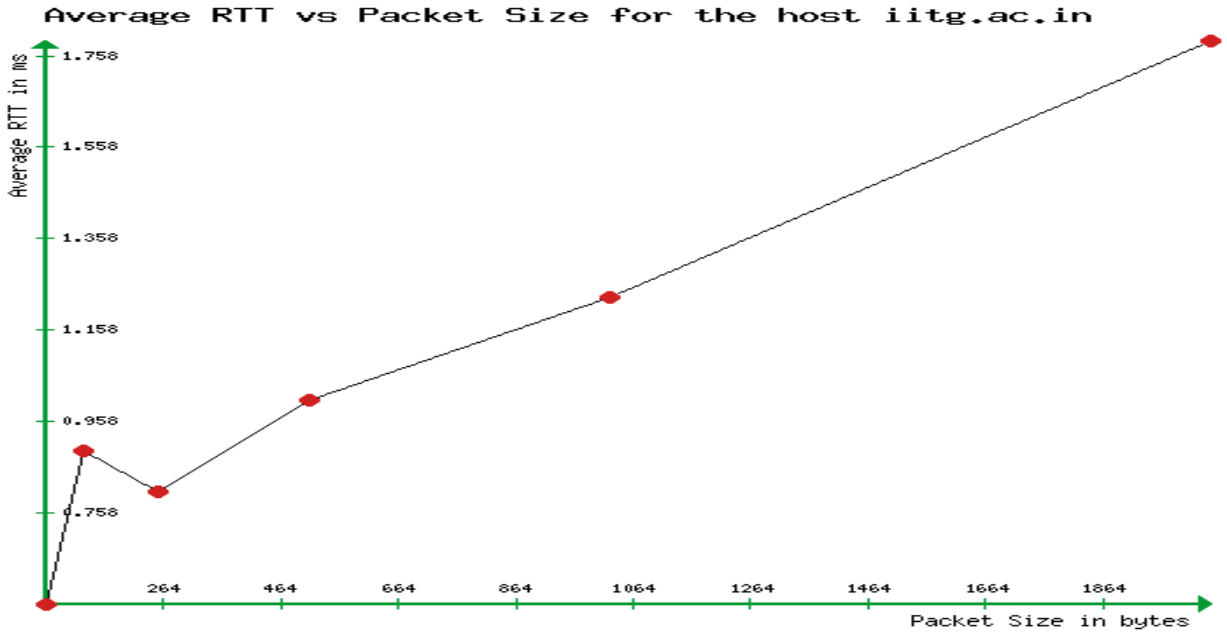
2) ***Ping Experiment:***

- The readings are taken at 10:00 am, 12:00 pm and 4:00 pm respectively.
- **' iitg.ac.in '** is chosen for experimenting with packets of size from 64 bytes to 2048 bytes.
- The following table shows average RTT (in ms) at three different time:

Host name	Location	10:00 am	12:00 pm	4:00 pm	AVG (in ms)
iitg.ac.in	India	0.608	0.575	0.609	0.597
youtube.com	USA	114.441	100.773	94.189	103.134
facebook.com	USA	117.981	97.434	95.297	103.57
geeksforgeeks.com	Germany	435.898	480.930	444.612	453.813
flipkart.com	India	206.099	145.764	156.079	169.314
cricbuzz.com	USA	110.601	160.898	116.945	129.481

- **Packet loss:** In my experiment, no cases of packet loss but in general packet loss can be greater than 0% because of network congestion and traffic. Some packets may collide with other packets and in the network and result in packet loss.
- **Geographic Distance:** There is a weakly correlation between the Geographic distance and RTT. They are correlated because of factors like increased no. of nodes and increased propagation delay. Larger the distance, longer it takes for a packet to propagate but RTT is affected by many other dominating factors also such as network traffic or server capacity.
- **Time**: From the above table, we can say that RTT varies with time of the day for different hosts with different perspective.
- The following table shows how RTT (ms) varies with packet size (bytes) for ' **iitg.ac.in** ':

Packet size	64	128	256	512	1024	2048
Avg RTT	0.558	0.892	0.804	1.005	1.228	1.792



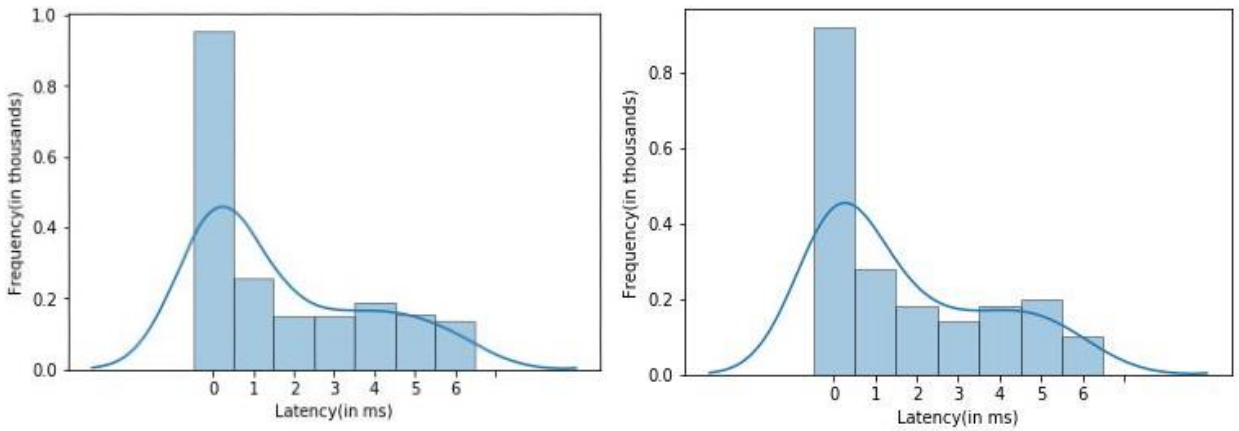
- **Packet Size:** With increase in Packet size, here we can see avg RTT value increases. From 64 bytes to 128 bytes it increases significantly but decreases a little bit from 128 to 256 but after then it increases significantly.

3) 2 Ping command experiment:

a) **Packet loss** for command **ping –n –c 1000 172.17.1.1** is **0.003%** and packet loss for command **ping –p ff00 –c 1000 172.17.1.1** is **0.006%**.

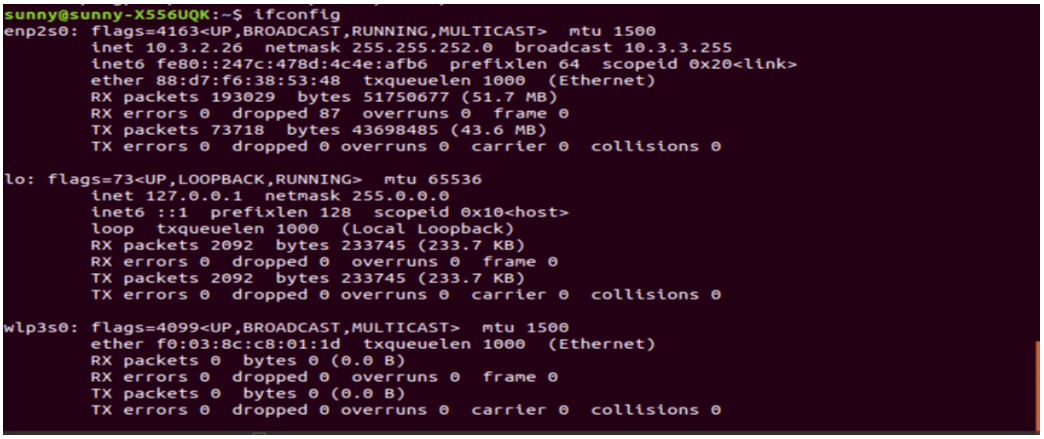
b) **Minimum, maximum, mean** and **median** latency of the pings that succeeded for command **ping –n –c 1000 172.17.1.1** (in ms) are **0.242, 6.679, 2.063** and **1.981**. **Minimum, maximum, mean** and **median** latency of the pings that succeeded for command **ping –p ff00 –c 1000 172.17.1.1** (in ms) are **0.263, 8.670, 2.141** and **2.001**.

c) The left graph is for command ping –n <IP> and other is for ping -p ff00 <IP>.



d) The min/max/avg/median latencies are greater for second command. First, there is no attempt made to lookup symbolic names for host addresses when using '-n', hence it is faster. Second, -p ff00' will cause the sent packet to be filled with the pattern **1111111100000000** and this will cause problems with the synchronisation of the clocks since only one transition is present in the padding from 1 to 0. Hence, we observe more packet loss in second case.

4) Ifconfig and route commands:

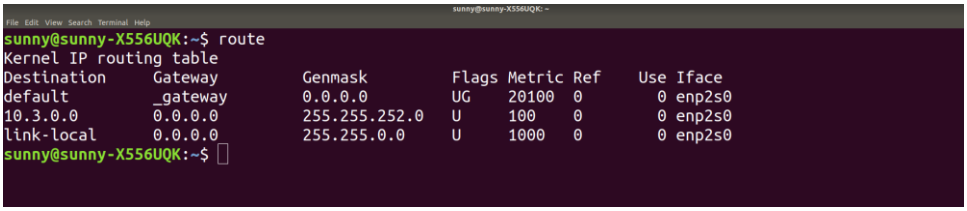


a) The command **'ifconfig'** display all the **active** network interfaces details. In my machine, I got the output as shown in figure. My machine has a wired ethernet interface ***enp2s0***, a loopback interface ***lo*** that the system uses to communicate with itself and a wireless interface ***wlp3s0***. ***Inet and Inet6***: indicates the machine IPv4 and IPv6 address associated with the network interface. ***UP***: This flag indicates that the kernel modules related to the ethernet interface has been loaded. ***BROADCAST***: denotes that the ethernet device supports broadcasting – a necessary characteristic to obtain IP address via DHCP. ***RUNNING***: The interface is ready to accept data. ***MULTICAST***: indicates that the ethernet device supports multicasting. ***MTU***: (Maximum Transmission Unit) The size of each packet received by the ethernet card. ***RX and TX packets***: total number of packets received and transmitted respectively. ***RX and TX bytes***: These indicate the total amount of data that has passed through the Ethernet interface either way. ***Collisions***: The value of this field should ideally be 0. If it has a value greater than 0, it could mean that the packets are colliding while traversing your network – a sure sign of network congestion. ***Txqueuelen***: denotes the length of the transmit queue of the device. ***TX and RX errors***: The number of packets that experienced transmission error and the number of damaged packets received respectively. ***RX and TX dropped***: The number of dropped packets due to reception errors and transmission errors respectively. ***RX overruns and frame***: The number of received packets that experienced data overruns and frame errors respectively. ***TX overruns***: The number of transmitted packets that experienced data overruns. ***TX carriers***: The number of received packets that experienced loss of carriers.

b) **Options provided with ifconfig command**:

- **'-a'** is used to display information of all active or inactive network interfaces.
- Using interface name (enp2s0) as an argument with 'ifconfig' command will display details of specific network interface.
- The **'up'** or **'ifup'** flag with interface name (enp2s0) activates a network interface, if it is not in active state and allowing to send and receive information. For example, 'ifconfig enp2s0 up' will activate enp2s0 interface.
- The **'down'** or **'ifdown'** flag with interface name (enp2s0) deactivates the specified network interface. For example, 'ifconfig enp2s0 down' will activate enp2s0 interface.
- **'-s'** is used to display a short list, instead of details.

c) **route command**:



The **'route'** command by default will show the details of the kernel routing table entries. ***Destination***: This field represents IP address of the destination. ***Gateway***: This identifies the defined gateway for the specified network. The 0.0.0.0 means that the network is locally connected on that interface and no more hops are needed to get it. ***Genmask***: It shows the netmask for the network. ***Iface***: It shows network interface. ***G flag***: It specified gateway should be used for this route. ***U flag***: It means the route is up. ***Metric***: The distance to the target (usually counted in hops). ***Ref***: Number of references to this route. ***Use***: Count of lookups for the route.

d) **Options provided with route command:**

- **'-n'** is used to display numerical IP address.
- **'-C'** is used to list the kernel's routing cache information.
- **'-v'** specifies verbose mode and prints additional details.
- **'-e'** specifies other more information.
- **'add'** to add a route, **'-net'** specifies that the target is a network and **'-host'** indicates that the destination parameter should be interpreted as a host.

5) netstat command:

a) 'netstat' command is used to list out all the network (socket) connections on a system. It lists out all the tcp, udp socket connections and the Unix socket connections.

b) Command used to show all the tcp established connections is:
netstat –at | grep ESTABLISHED

```
sunny@sunny-X556UQK:~$ netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:mysql         0.0.0.0:*               LISTEN
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN
tcp        0      0 sunny-X556UQK:39362     a23-32-178-29.dep:https ESTABLISHED
tcp        0      0 sunny-X556UQK:48702     maa05s10-in-f2.1e:https ESTABLISHED
tcp        0      0 sunny-X556UQK:48696     maa05s10-in-f2.1e:https ESTABLISHED
tcp        0      0 sunny-X556UQK:45612     lga15s49-in-f3.1e:https ESTABLISHED
tcp        0      0 sunny-X556UQK:50118     maa05s04-in-f3.1e:https ESTABLISHED
tcp        0      0 sunny-X556UQK:46880     a104-80-51-143.de:https ESTABLISHED
tcp        0      0 sunny-X556UQK:43708     ec2-54-244-31-189:https ESTABLISHED
tcp        0      0 sunny-X556UQK:48700     maa05s10-in-f2.1e:https ESTABLISHED
tcp        0      0 sunny-X556UQK:58772     maa05s09-in-f14.1:https ESTABLISHED
tcp        0      0 sunny-X556UQK:42730     maa03s26-in-f14.1:https ESTABLISHED
tcp        0      0 sunny-X556UQK:50584     40.100.140.226:https    ESTABLISHED
tcp        0      0 sunny-X556UQK:53698     a104-81-21-87.dep:https TIME_WAIT
tcp        0      0 sunny-X556UQK:58888     104.20.33.107:https     ESTABLISHED
tcp        0      0 sunny-X556UQK:40352     ec2-13-235-224-15:https ESTABLISHED
tcp        0      0 sunny-X556UQK:36062     52.109.124.38:https     ESTABLISHED
tcp        0      0 sunny-X556UQK:32808     52.114.158.102:https    ESTABLISHED
tcp        0      0 sunny-X556UQK:41094     maa03s26-in-f10.1:https ESTABLISHED
tcp        0      0 sunny-X556UQK:53560     sa-in-f188.1e100.n:5228 ESTABLISHED
tcp        0      0 sunny-X556UQK:37314     maa05s06-in-f3.1e:https ESTABLISHED
tcp        0      0 sunny-X556UQK:34786     maa03s31-in-f14.1:https ESTABLISHED
tcp        0      0 sunny-X556UQK:34004     maa03s20-in-f14.1:https ESTABLISHED
tcp        0      0 sunny-X556UQK:37358     maa03s31-in-f13.1:https ESTABLISHED
tcp        0      0 sunny-X556UQK:52640     13.107.6.171:https      ESTABLISHED
tcp        0      0 sunny-X556UQK:39484     maa03s29-in-f6.1e:https ESTABLISHED
tcp        1      0 sunny-X556UQK:39704     maa05s09-in-f16.1e:http CLOSE_WAIT
tcp        0      0 sunny-X556UQK:49658     13.107.6.171:https      ESTABLISHED
tcp        0      0 sunny-X556UQK:33994     40.100.138.18:https     ESTABLISHED
tcp        0      0 sunny-X556UQK:34600     maa03s20-in-f1.1e:https ESTABLISHED
tcp        0      0 sunny-X556UQK:41586     maa05s03-in-f2.1e:https ESTABLISHED
tcp        0      0 sunny-X556UQK:39048     sa-in-f189.1e100.:https ESTABLISHED
tcp        1      0 sunny-X556UQK:39706     maa05s09-in-f16.1e:http CLOSE_WAIT
tcp6       0      0 ip6-localhost:ipp       [::]:*                  LISTEN
sunny@sunny-X556UQK:~$
```

'netstat -at' command will give all tcp connections as shown in figure. ***Proto***: It tells us if the socket listed is TCP or UDP. ***Recv-Q and Send-Q:*** It tell us how much data is in the queue for that socket, waiting to be read (Recv-Q) or sent (Send-Q). ***Local Address and Foreign Address***: It tell which hosts and ports the listed sockets are connected. The local end is always on the computer on which netstat is running and the foreign end is about the other computer. ***State***: tells in which state the listed sockets are.

c) **'netstat -r'** list the current entries in the routing table of my machine.

```
File  Edit  View  Search  Terminal  Help
sunny@sunny-X556UQK:~$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         _gateway        0.0.0.0         UG        0 0          0 enp2s0
10.3.0.0        0.0.0.0         255.255.252.0   U         0 0          0 enp2s0
link-local      0.0.0.0         255.255.0.0     U         0 0          0 enp2s0
sunny@sunny-X556UQK:~$
```

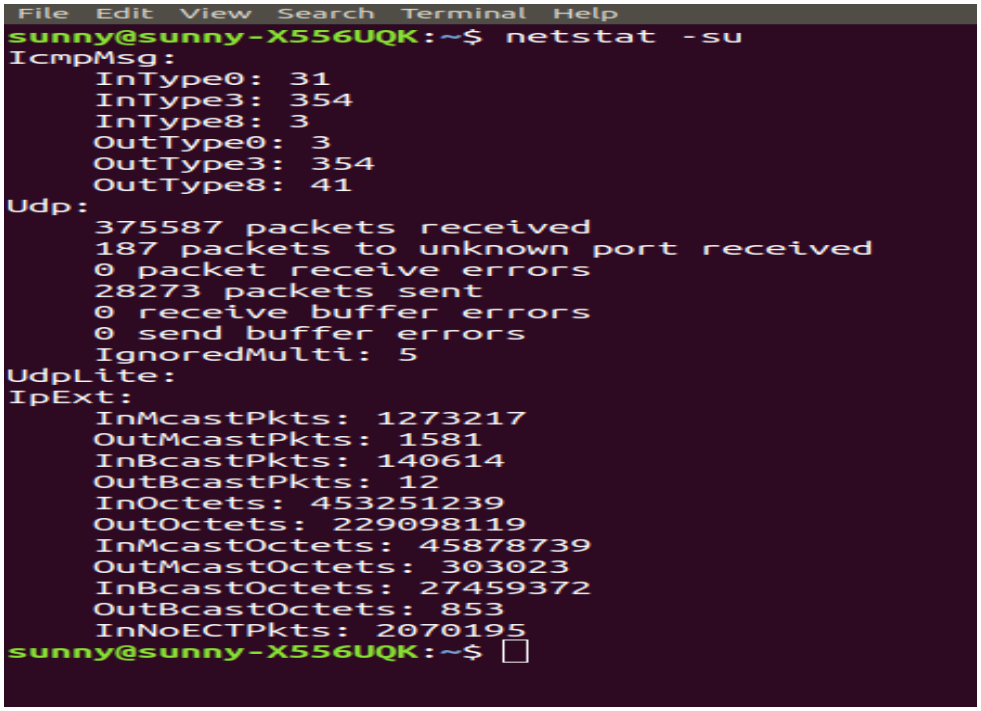
Destination: indicates the pattern that the destination of a packet is compared to. ***Gateway***: tells the computer where to send a packet that matches the destination of the same line. ***Genmask***: tells how many bits

from the start of the IP address are used to identify the subnet. As a rule of thumb, it is 255 for any non-zero part of the destination and 0 for parts of the destination that are 0. ***Flags***: shows which flags apply to current table line. 'U' means up, indicating active line. 'G' means this line uses a gateway. ***MSS***: lists the value of the Maximum Segment Size for this line. ***Window***: It is like the MSS column in that it gives the option of altering a TCP parameter. ***Irtt***: stands for initial round trip time. ***Iface***: tells which network interface.

d) The option used to display the status of all network interfaces is **'-i'**. The number of interfaces in my computer is **3**, i.e. enp2s0, lo, wlp3s0.

e) To show statistics of all UDP connections, **'-su'** is used and output is shown in below figure.

f) 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. It is used for device identification, routing information and packet filtering. The most commonly used IP address on the loopback network is 127.0.0.1 for IPv4 and ::1 for IPv6. The standard domain name for the address is localhost.



6) Traceroute command: Traceroute command in Linux prints the route that a packet takes to reach the host. This command is useful when you want to know about the route and about all hops that a packet takes.

a) The readings are taken at 10:00 am, 12:00 pm and 4:00 pm.

	iitg.ac.in	Youtube.com	Facebook.com	Geeksforgeeks.com	Flipkart.com	Cricbuzz.com
10:00 am	2	12	13	18(firewall)	10(firewall)	20
12:00 pm	2	12	13	18(firewall)	10(firewall)	21
4;00 pm	2	12	13	18(firewall)	10(firewall)	20

The obvious common hop is 10.3.0.254 and 172.17.0.1, 192.168.193.1 and 14.139.196.17 are also common in all except for iitg.ac.in.

b) Yes, in case of **cricbuzz.com** the route to host changed. This may be because destination host utilizes multiple internet servers to handle incoming requests. The packets are redirected by the nodes to take a route having less traffic.

c) In case of **geeksforgeeks.com** and **flipkart.com,** traceroute does not find the complete path. It is because **Firewall of that host might be blocking our IP**, or we need to **increase max hops** as packets might not reach to destination within fixed hops. Other reason may be packet loss between various routers in between the path.

d) Yes, 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 their 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.

*7) **ARP:***

a) The command **'arp'** shows the full ARP table of my machine. ARP stands for address resolution protocol and its main function is to resolve the IP address of a system to its mac address.

Address: IP address
HWtype: Hardware type, here is ethernet.
HWaddress: Hardware address. ***C flags***: denotes cache entry. ***Iface***: Network Interface.

```
File  Edit  View  Search  Terminal  Help
sunny@sunny-X556UQK:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.1.1              ether   00:1e:a6:fb:64:d0   C                     enp2s0
10.3.2.58                ether   10:7d:1a:37:d9:f3   CM                    enp2s0
10.3.2.30                ether   04:95:e6:7b:b1:d8   C                     enp2s0
10.3.2.31                ether   58:d5:6e:d1:3c:65   C                     enp2s0
_gateway                 ether   4c:4e:35:97:1e:ef   C                     enp2s0
sunny@sunny-X556UQK:~$ sudo arp -d 10.3.2.58
sunny@sunny-X556UQK:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.1.1              ether   00:1e:a6:fb:64:d0   C                     enp2s0
10.3.2.30                ether   04:95:e6:7b:b1:d8   C                     enp2s0
10.3.2.31                ether   58:d5:6e:d1:3c:65   C                     enp2s0
_gateway                 ether   4c:4e:35:97:1e:ef   C                     enp2s0
sunny@sunny-X556UQK:~$ sudo arp -s 10.3.2.58 10:7d:1a:37:d9:f3
sunny@sunny-X556UQK:~$ sudo arp -s 10.3.2.59 10:7d:1a:37:d9:f4
sunny@sunny-X556UQK:~$ sudo arp -s 10.3.2.60 10:7d:1a:37:d9:f5
sunny@sunny-X556UQK:~$ sudo arp -s 10.3.2.61 10:7d:1a:37:d9:f6
sunny@sunny-X556UQK:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.1.1              ether   00:1e:a6:fb:64:d0   C                     enp2s0
10.3.2.60                ether   10:7d:1a:37:d9:f5   CM                    enp2s0
10.3.2.61                ether   10:7d:1a:37:d9:f6   CM                    enp2s0
10.3.2.58                ether   10:7d:1a:37:d9:f3   CM                    enp2s0
10.3.2.30                ether   04:95:e6:7b:b1:d8   C                     enp2s0
10.3.2.59                ether   10:7d:1a:37:d9:f4   CM                    enp2s0
10.3.2.31                ether   58:d5:6e:d1:3c:65   C                     enp2s0
_gateway                 ether   4c:4e:35:97:1e:ef   C                     enp2s0
sunny@sunny-X556UQK:~$
```

b) To delete an entry - **'arp -d address'** and to add an entry - **'arp -s address hw_address'**. You need to run it as a root user (using sudo). I have added 4 entries of addresses 10.3.2.58, 10.3.2.59, 10.3.2.60, 10.3.2.61 as you can see in above figure.

c) The default timeout value varies according to machine. If the entry is no longer needed, then it will be deleted after that default time value. A trial and 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. The time after which it disappears (call finish time and its previous checking time called it previous time), then after adding again this entry and check for the time at average of time of previous and finish time and doing this. This will give approximate timeout value of the entries.

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 its routing table and sends the packet further to the correct device.

*8) **NMAP:*** The following command is used for this question. The IP used is of Siang hostel.

nmap –n –sP 10.3.0.254/22

From the adjacent graph, one can notice that the number of hosts online are low in the early morning around 10:00 am and from afternoon to evening it is neither decreasing so much nor increasing so much.