CS-349 | NETWORKS LAB | ASSIGNMENT-1
VAKUL GUPTA | 170101076

QUESTION-1 : PING COMMAND OPTIONS

a) **'-c'** option is required to specify the number of echo requests to send with ping.
Example: '**ping -c 5 172.17.0.23**' will send **5 ICMP ECHO_REQUESTS** to the specified address.

b) **Option 'i'** can be used to set the time interval (in seconds) between two successive ping ECHO_REQUESTS.Example: '**ping -i 8 172.17.0.23**' will send ICMP ECHO_REQUESTS to the specified address every 8 seconds.

c) **Option 'l'** can be used to send ECHO_REQUEST packets to the destination one after another without waiting for a reply. The **limit** for sending such ECHO_REQUEST packets by normal users is **3**. Alternatively, **'-f' option** will flood the target with ICMP ECHO_REQUESTS without waiting for a reply. Normal users can send requests with **minimum time interval of 0.2 seconds**.

d) **Option 's'** can be used to set the ECHO_REQUEST packet size. Example: '**ping -s 56 172.17.0.23**' will send ICMP ECHO_REQUESTS to the specified address with 56 bytes of ICMP_DATA.The actual packet size is bigger than what is given due to the addition of the **ICMP header(8 Bytes) and IP Headers(20 Bytes)**.Hence, total packet size will be **32+8+20=60 bytes** if packet size is set as **32 bytes.**

QUESTION-2 : FACTORS AFFECTING RTT AND % PACKET LOSS

The six different hosts used for the experiment were :- 1.) flipkart.in, 2.) hackerearth.com, 3.) google.com, 4.) facebook.com, 5.) yahoo.com, 6.) baidu.com

Packet Loss is mentioned in brackets along with the average RTTs.

Time slots chosen for the experiment were 2pm, 8pm & 2am.

The laptop was connected via a hotspot provided by the mobile data (Jio).

Destination Host Address	IP Address	Host Location	Avg. RTT-1 (ms) | 2pm	Avg. RTT-2 (ms) | 8pm	Avg. RTT-3 (ms) | 2am	Total Avg. RTT (ms)	Total Avg.% Packet Loss
flipkart.in	163.53.78.87	Benguluru,India	284.543(0%)	317.006(0%)	212.234(0%)	271.261	0%
hackerearth.com	54.254.164.171	Singapore	No RTT	No RTT	No RTT	No RTT	100%
google.com	172.217.5.100	California, USA	502.675(0%)	564.321(0%)	583.664(0%)	550.22	0%
facebook.com	157.240.22.35	California, USA	497.865(0%)	520.471(12%)	524.571(0%)	514.303	4%
yahoo.com	72.30.35.10	New York, USA	454.917(0%)	412.657(0%)	498.192(0%)	455.255	0%
baidu.com	39.156.69.79	Beijing, China	812.472(0%)	904.768(0%)	811.452(0%)	842.897	0%

REASONS FOR PACKET LOSS GREATER THAN ZERO% :-

There were two cases where packet loss greater than zero% was observed i.e. 12% loss in facebook.com at 8pm & 100% loss in hackerearth.com at all times.The reason for the 100% packet loss could be restrictions imposed on the source IP address that can be accessed. Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination, which can be because the firewall is blocking.Other reasons for partial packet loss are mainly network congestion or or target IP address might not have any network device connected with it.

GEOGRAPHICAL DISTANCE:-

I have observed that the RTTs for above hosts are weakly correlated with geographic distance of host as packet travels with speed of light between two hops. It Is strongly correlated with number of hops to the host because processing delay adds up by waiting in queue of hop.The reason for the weak correlation is that latency time also depends on various other factors like 'bandwidth of network', 'contention ratio', 'load at server' and 'traffic in the network'.e.g. "Traffic in the network" can vary based on the popularity of a website.

PACKET SIZE :-

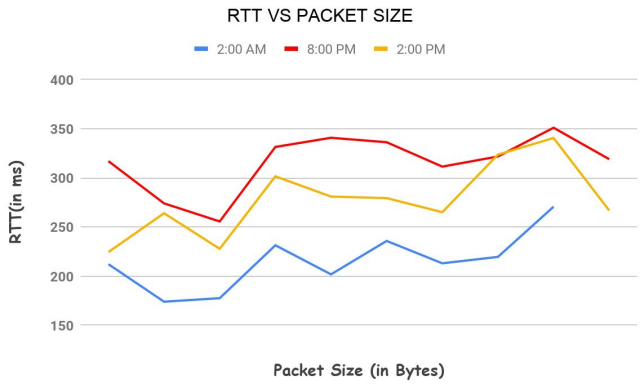
Every router and switch along the path has to receive the entire packet/frame before it can forward it. The latency introduced at each point thus equals the speed of the inbound link in bps divided by the frame size in bits. Larger frames = increased latency. For large packet size, the buffer at the immediate router gets filled up quickly hence losing packets.

TIME OF THE DAY:-

Time influence on RTT measurements can be understood as different hours correspond to different busy working hours of different continents. Higher RTTs are measured when it is daytime in Asia and the United States. It may be because of network traffic is busier, as more users are online.Although, there is no reason for a clear, visible pattern between latency and time of the day due to different time zones in different parts of the world.Though, lowest avg. RTTs were observed at 2am IST, as host location of flipkart.in is located in Karnataka(Indian Origin) itself, since traffic must be close to minimum at that particular time slot.

Readings with different packet sizes have been taken with flipkart.in as host:-

Packet Size (bytes)	64	128	256	512	768	1024	1280	1536	1792	2048
Avg. RTT-1 (ms) | 2pm	284.543	264.062	227.87	301.56	280.97	279.43	265.11	323.67	340.56	266.78
Avg. RTT-2 (ms) | 8pm	317.006	274.062	255.68	331.45	340.78	336.25	311.45	321.76	350.98	318.98
Avg. RTT-3 (ms) | 2am	212.234	174.062	177.662	231.45	201.881	235.87	213.11	219.65	270.672	238.76



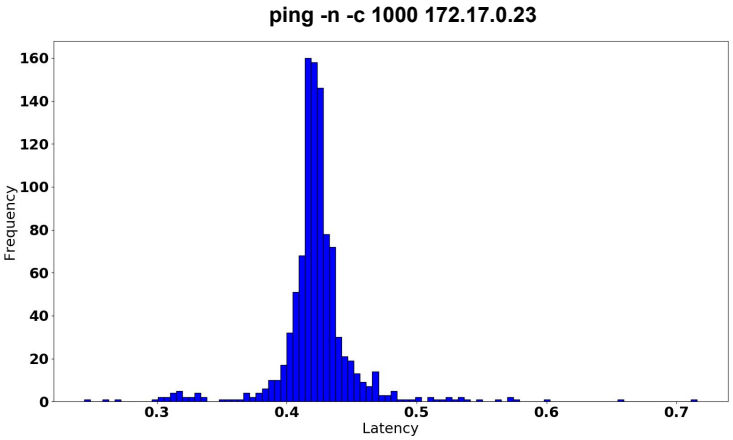
QUESTION-3 : ANALYSIS OF RTT DUE TO CHANGE IN PARAMETERS OF PING COMMAND

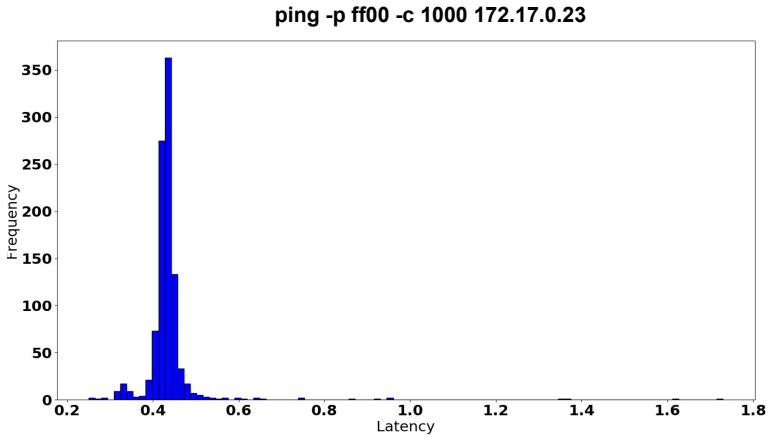
"172.17.0.23", the ip address of intranet.iitg.ernet.in was used for the following experiment:-

Command	Packets Transmitted	Packets Received	Packet Loss	Minimum Latency (ms)	Maximum Latency (ms)	Avg. Latency (ms)	Median Latency (ms)
ping -n -c 1000 172.17.0.23	1000	1000	0%	0.244	5.374	0.431	0.179
ping -p ff00 -c 1000 172.17.0.23	1000	996	0.4%	0.250	2.186	0.440	0.114

a) Packet Loss for the first command was 0%, while for the second it was 0.4%
b) Min,Max,Avg, & Med Latencies of both the commands are shown in the above table.
c) The graphs are shown below:-
d) OBSERVATION:-

'-n' specifies that no attempt will be made to reverse lookup the ip address.
'-p' on the other hand, is used to specify a pattern for the content of the ping packet.
In the second case, we are sending pattern **1111111100000000**. Sending continuous 1s and 0s is always an error prone task and synchronization issue come into the picture. This requires resending of same packets. This results in high latency. Also in the first case, no attempt will be made to look up symbolic names for host address. So it is likely that case 2 is more likely to have more RTT. Both of the above supports that second case have more RTT than the first case.





QUESTION-4 : IFCONFIG AND ROUTE COMMANDS

Ifconfig:- It stands for "Interface Configuration". It is a utility for Linux machines to configure, assign, add, delete, control and query network interface in Unix/Linux machine.

Explanation of ifconfig output :-

- **inet addr** : IPv4 address assigned to the interface.
- **Bcast**: denotes the broadcast address for the current network
- **Mask** : the network mask which decides the potential size of your network
- **Up**: network interface is configured to be enabled.
- **Broadcast** : Ethernet device supports broadcasting which is a necessary characteristic to obtain an IP address via DHCP.
- **Multicast**: Interface is configured to handle multicast packets. It allows a source to send a packet to multiple machines.
- **Running** : Indicates that the network interface is operational and is ready to accept the data.
- **MTU** : Maximum Transmission Unit is a link layer characteristic which provides limit on the size of the Ethernet frame. 1500 is the default value for all Ethernet de
- **METRIC** : Interface metric is used to compute the cost of a route. It tells the OS which interface a packet should be forwarded to, when multiple interfaces could be used to reach destination.
- **RX/TX packets** : The total number of packets received and transmitted respectively.
- **RX/TX bytes** : The total amount of data that has passed through the Ethernet interface.
- **Interrupt** : Network interface card is using the interrupt number 9. This is usually set by the system.
- **Collisions** : The number of transmitted packets that experienced Ethernet collisions. A nonzero value of this field indicates the possibility of network congestion.

```
vakul@vakul-G7-7588:~/SEMESTER-6/Networks_Lab$ ifconfig
enp59s0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether d8:d0:90:03:5f:a3  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
        device interrupt 17

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 16442  bytes 1581758 (1.5 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 16442  bytes 1581758 (1.5 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp0s20f3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.43.86  netmask 255.255.255.0  broadcast 192.168.43.255
        inet6 2409:4065:1a:f8fc:87c5:1bd2:27e0:8786  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::9f5e:6452:e5de:5447  prefixlen 64  scopeid 0x20<link>
        inet6 2409:4065:1a:f8fc:fd4a:c7f2:e64:b82  prefixlen 64  scopeid 0x0<global>
        ether 98:2c:bc:fc:ad:be  txqueuelen 1000  (Ethernet)
        RX packets 703434  bytes 208786697 (208.7 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 158066  bytes 45561938 (45.5 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Txqueuelen: The field provides the information about the configured length of transmission queue.

Options provided with the ifconfig command:-

Running ifconfig with no options will display the configuration of all active interfaces.

-a : display all interfaces available. (both active and inactive)

-s : display a short list.

-v : more verbose for some error conditions.

interface : The name of the interface.This is usually a driver name followed by a unit number, eg. eth0.

To change the settings of the existing interfaces, following after type options can be used:-

- **up** : This flag causes the interface to be activated.
- **down** : This flag causes the driver for this interface to be shut down.
- **metric N** : This parameter sets the interface metric.
- **mtu N** : This parameter sets the Maximum Transfer Unit (MTU) of an interface.
- **dstaddr addr** : Set the remote IP address for a point-to-point link.
- **netmask addr** : Set the IP network mask for this interface.
- **address** : The IP address to be assigned to this interface.

ROUTE COMMAND:-

```
vakul@vakul-G7-7588:~/SEMESTER-6/Networks_Lab$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    600    0        0 wlp0s20f3
10.19.2.0       0.0.0.0         255.255.254.0   U     600    0        0 wlp0s20f3
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 wlp0s20f3
```

- **Destination** : The destination network or destination host.
- **Gateway** : The gateway address or '*' if none set.
- **Genmask** : The netmask for the destination net.
- **Flags** : U (route is up) G (use gateway)
- **Metric** : The distance to the target (usually counted in hops). It is not used by recent kernels.
- **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.

Some of the relevant options of route used are:

- **-n** : show numerical addresses instead of trying to determine the symbolic host names.
- **-v** : select verbose operation.
- **-ee** : will generate a very long line with all parameters from the routing table.
- **del** : delete a route
- **add** : add new route

```
vakul@vakul-G7-7588:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.19.2.1       0.0.0.0         UG    20100  0        0 enp59s0
10.19.2.0       0.0.0.0         255.255.254.0   U     100    0        0 enp59s0
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 enp59s0
vakul@vakul-G7-7588:~$ route -v
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    20100  0        0 enp59s0
10.19.2.0       0.0.0.0         255.255.254.0   U     100    0        0 enp59s0
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 enp59s0
vakul@vakul-G7-7588:~$ route -ee
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface    MSS   Window irtt
default         _gateway        0.0.0.0         UG    20100  0        0 enp59s   0     0      0
10.19.2.0       0.0.0.0         255.255.254.0   U     100    0        0 enp59s   0     0      0
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 enp59s   0     0      0
```

QUESTION-5 : NETSTAT COMMAND:-

a) Netstat (network statistics) is a command line tool for monitoring network connections both incoming and outgoing as well as viewing routing tables, interface statistics etc.

USES :-

- It is used for finding problems in the network, to determine the amount of traffic on the network as a performance measurement.
- It helps the network administrators to keep an eye on the invalid or suspicious network connections.
- It can show you which programs are active on your network right now.

b) '**netstat -at | grep -e ESTABLISHED**' command should be used to show all the established TCP connections. **The fields are:-**

- **Proto**: The name of the protocol (tcp, udp, raw) used by the socket which is tcp in this case.
- **Recv-Q**: The counts of bytes not copied by the user program connected to this socket.
- **Send-Q**: The count of bytes yet to be acknowledged by the remote host.
- **Local address**: Address and port number of the local end of socket.
- **Foreign Address**: Address and port number of the remote end of the socket.
- **State**: The state of the socket connected in between the Local Address and Foreign Address. These states represent the three-way handshake communication system that TCP uses.

```
vakul@vakul-G7-7588:~/SEMESTER-6/Networks_Lab$ netstat -at | grep -e ESTABLISHED
tcp        0      0 vakul-G7-7588:48496     180.149.60.168:https    ESTABLISHED
tcp        0      0 vakul-G7-7588:42550     172.217.194.188:5228    ESTABLISHED
tcp        0      0 vakul-G7-7588:43440     sb-in-f189.1e100.:https ESTABLISHED
tcp        0      0 vakul-G7-7588:42142     maa05s09-in-f14.1:https ESTABLISHED
tcp        0      0 vakul-G7-7588:40936     maa05s06-in-f3.1e:https ESTABLISHED
tcp        0      0 vakul-G7-7588:46904     maa03s23-in-f206.:https ESTABLISHED
tcp        0      0 vakul-G7-7588:48494     180.149.60.168:https    ESTABLISHED
tcp        0      0 vakul-G7-7588:41454     maa03s22-in-f170.:https ESTABLISHED
tcp        0      0 vakul-G7-7588:58694     a118-214-44-253.d:https ESTABLISHED
tcp        0      0 vakul-G7-7588:49646     ec2-34-214-229-24:https ESTABLISHED
tcp        0      0 vakul-G7-7588:41372     3.67.98.34.bc.goo:https ESTABLISHED
tcp        0      0 vakul-G7-7588:38638     124.124.201.159:https   ESTABLISHED
tcp        0      0 vakul-G7-7588:40320     maa05s06-in-f2.1e:https ESTABLISHED
tcp        0      0 vakul-G7-7588:42088     maa03s31-in-f14.1:https ESTABLISHED
```

c) '**netstat -r**' command is used to list the kernel routing table.

```
vakul@vakul-G7-7588:~/SEMESTER-6/Networks_Lab$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         _gateway        0.0.0.0         UG        0 0          0 enp59s0
10.19.2.0       0.0.0.0         255.255.254.0   U         0 0          0 enp59s0
link-local      0.0.0.0         255.255.0.0     U         0 0          0 enp59s0
```

- **The "Destination" column** indicates the pattern that the destination of a packet is compared to.
- **The "Gateway" column** tells the computer where to send a packet that matches the destination of the same line. An asterisk (*) here means "send locally", because the destination is supposed to be on the same network.
- **The "Genmask" column** is the subnet mask that is used for the connection
- **The "Flags" column** shows which flags apply to the current line. "U" means Up (active line),"G" means line uses a Gateway.
- **The "MSS" column** lists the value of the Maximum Segment Size for this line. Nowadays, most computers have no problems with the most commonly used maximum packet sizes, so this column usually has the value of 0, meaning "no changes".
- **The "Window" column** is like the MSS column in that it gives the opon of altering a TCP parameter. In this case that parameter is the default window size, which indicates how many TCP packets can be sent before at least one of them has to be acknowledged. Like the MSS, this field is usually 0, meaning "no changes".
- **The "irtt" column** stands for Initial Round Trip Time and may be used by the kernel to guess about the best TCP parameters without waiting for slow replies. In practice, it's not used much, so 0 here.
- **The "Iface" column** tells which network interface should be used for sending packets that match the destination.

d) "**netstat -i**" can be used to display the status of all network interfaces & "**netstat –i | wc -l**" gives the number of network interfaces. My laptop has 2 interfaces **i.e. "lo" and "enp59s0"**, which I found from the above command.

e) "**netstat -su**" is used to show the statistics of all UDP connections.

```
vakul@vakul-G7-7588:~/SEMESTER-6/Networks_Lab$ netstat -su
IcmpMsg:
    InType0: 14842
    InType3: 177
    InType8: 5
    InType11: 179
    OutType0: 5
    OutType3: 6071
    OutType8: 15328
Udp:
    1787342 packets received
    6107 packets to unknown port received
    0 packet receive errors
    41760 packets sent
    0 receive buffer errors
    7 send buffer errors
    IgnoredMulti: 265591
UdpLite:
IpExt:
    InTruncatedPkts: 10
    InMcastPkts: 438376
    OutMcastPkts: 2813
    InBcastPkts: 266202
    OutBcastPkts: 84
    InOctets: 553327342
    OutOctets: 93104167
    InMcastOctets: 25567535
    OutMcastOctets: 491075
    InBcastOctets: 26495576
    OutBcastOctets: 5457
    InNoECTPkts: 1374143
```

f) **Loopback Interface:** The loopback device is a virtual network interface that computer uses to communicate with itself. It is used for diagnostics and troubleshooting, and to connect to servers running on local machine. If we ping the virtual address of the machine then it loopbacks till keyboard interrupt is given.

```
vakul@vakul-G7-7588:~/SEMESTER-6/Networks_Lab$ ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.032 ms
^C
--- 127.0.0.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.032/0.032/0.032/0.000 ms
```

QUESTION-6 : TRACEROUTE TOOL:-

The six different hosts used for the experiment were :- 1.) flipkart.in, 2.) hackerearth.com, 3.) google.com, 4.) facebook.com, 5.) yahoo.com, 6.) baidu.com
Time slots chosen for the experiment were 2pm, 8pm & 2am.
The laptop was connected via a hotspot provided by the mobile data (Jio).

Time of the Day	flipkart.in	hackerearth.com	google.com	facebook.com	yahoo.com	baidu.com
2AM	14	28(Trace Aborted)	13	25	17	28
2PM	15	28(Trace Aborted)	14	24	18	28
8PM	15	28(Trace Aborted)	14	25	17	29

a) **'192.168.43.194'** and **'10.72.35.2'** are the 2 most common hops found for every host.These are most probably the hops dedicated to the mobile data that I am using (Jio in this case), so the packets must pass through them leading to further hops.

b) The destination address of the '**baidu.com**' comes out to '**180.76.146.53'** and **'180.76.193.10'** at times 2PM and 8PM respectively.This may be because destination host utilizes multiple Internet servers to handle incoming requests, so it shows different IP addresses. Also, due to different network traffic at these times and so, load balancing comes into play, where some requests are redirected to a different server, thus reducing network congestion.

c) In one case i.e. '**hackerearth.com**' , traceroute didn't provide the complete path in my experiment. The primary reason could be existence of firewall which is configured to block these packets or a secondary (very unlikely though) reason could be that router is dropping packets going through it. This is usually caused by three reasons either the router is overloaded, the router having a software or physical failure or the router is configured to do so (null route/black holes).

d) **Yes, it is possible to find the route to certain hosts which fail to respond with ping experiment.** Ping works on straight ICMP (Internet Control Message Protocol). Traceroute works very different from ping even though it uses ICMP. Traceroute works by targeting the final hop, but liming the TTL (Time To Live) 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 to the ICMP echo request from the host along the way, but a time exceeded message from the host. There are some hops, which don't give an ICMP echo reply so we don't get a reply for ping request but we are able to trace the route.

QUESTION-7 : ARP TABLE:-

a) ARP table can be seen using the 'arp' or 'arp -v' command. The output of arp command:-

```
vakul@vakul-G7-7588:~/SEMESTER-6/Networks_Lab$ arp -v
Address                  HWtype  HWaddress           Flags Mask            Iface
_gateway                 ether   ec:44:76:74:60:42   C                     enp59s0
10.19.3.185              ether   f8:ca:b8:61:12:39   C                     enp59s0
10.19.3.110              ether   0c:80:63:16:c9:52   C                     enp59s0
Entries: 3      Skipped: 0      Found: 3
```

The fields are:-

- **Address column** of the table shows the IP address of the machine connected to a network
- **Hwtype** specifies the type of hardware.
- **Hwaddress column** shows the mac address corresponding the particular entry in the table.
- **ARP cache entries** may be marked with the following **flags**: C(complete), M(permanent).
- **Interface** shows the network interface type for the corresponding entry.

b) Add entry : **sudo arp –s ip_addrress HWaddress**
Delete entry: **sudo arp –d ip_address**
Change entry: just add entry, it will overwrite the existing ip address's corresponding details.
Four entries are added:-

```
vakul@vakul-G7-7588:~/SEMESTER-6/Networks_Lab$ arp -v
Address                  HWtype  HWaddress           Flags Mask            Iface
10.19.2.211              ether   54:e1:ad:dd:fe:0e   C                     enp59s0
_gateway                 ether   ec:44:76:74:60:42   C                     enp59s0
10.19.3.112              ether   00:0c:29:c0:94:bf   CM                    enp59s0
10.19.3.110              ether   0c:80:63:16:c9:52   C                     enp59s0
Entries: 4      Skipped: 0      Found: 4
vakul@vakul-G7-7588:~/SEMESTER-6/Networks_Lab$ sudo arp -s 10.19.3.113 00:0c:29:c0:94:bf
vakul@vakul-G7-7588:~/SEMESTER-6/Networks_Lab$ sudo arp -s 10.19.3.114 00:0c:29:c0:94:bf
vakul@vakul-G7-7588:~/SEMESTER-6/Networks_Lab$ sudo arp -s 10.19.3.115 00:0c:29:c0:94:bf
vakul@vakul-G7-7588:~/SEMESTER-6/Networks_Lab$ sudo arp -s 10.19.3.116 00:0c:29:c0:94:bf
vakul@vakul-G7-7588:~/SEMESTER-6/Networks_Lab$ arp -v
Address                  HWtype  HWaddress           Flags Mask            Iface
10.19.3.113              ether   00:0c:29:c0:94:bf   CM                    enp59s0
10.19.3.116              ether   00:0c:29:c0:94:bf   CM                    enp59s0
10.19.3.114              ether   00:0c:29:c0:94:bf   CM                    enp59s0
10.19.3.115              ether   00:0c:29:c0:94:bf   CM                    enp59s0
10.19.2.211              ether   54:e1:ad:dd:fe:0e   C                     enp59s0
_gateway                 ether   ec:44:76:74:60:42   C                     enp59s0
10.19.3.112              ether   00:0c:29:c0:94:bf   CM                    enp59s0
10.19.3.110              ether   0c:80:63:16:c9:52   C                     enp59s0
Entries: 8      Skipped: 0      Found: 8
```

c) Trial And Error method to find the timeout:

An approach similar to the binary search can be used to get the desired value. Connect the machine to a new network and then after every 5 mins, check if the entry in table is updated. Let the entry be updated in the ith check. This means that the cache was refreshed between the(i-1)th and the ith check. Now disconnect from this network and wait for (i-1)*5 minutes + 2min + 30 sec. If the entry still exist at this time that means that the cache is cleared after this me and before (5*i) minutes. Apply this approach iteratively to get the result.

It comes out that in my system dynamic entries stay cached for 60 seconds (can be checked in the file "/proc/sys/net/ipv4/neigh/default/gc_stale_me") while static entries stay for about 4 hours in the arp table.

d) **Yes, a single ethernet card can have multiple IP's assigned to it, this process is known as IP aliasing.**

With this, one node on a network can have multiple connections to a network, each serving a different purpose. In a lot of scenarios, multiple IP addresses are used such as when a single server hosts multiple domain names, when we use two operating systems simultaneously one background and another as virtual machine we use different two different ip addresses to communicate among them, even though the MAC address is same(MAC address of our machine). If IP's with same MAC address are on different subnet then there is no problem in packet routing as each router's table contains single ip with a specific MAC. But if IP's with same MAC are on the same subnet (be it on the same machine or different machines), there will be conflict as router will not know to which ip it has to route as ARP table contains many IP's with same MAC hence less correct transmission.

QUESTION-8 : NMAP:-

- **Nmap (*Network Mapper*)** is a free and open-source network scanner used to discover hosts and services on a computer network by sending packets and analyzing the responses.Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services those hosts are offering, what operating systems they are running, etc.
- The command used for the analysis is **nmap -n -sP 10.19.3.3/22** scanning 1024 IP addresses in the Lohit hostel.
- As we can observe that the maximum number of hosts are up during the time interval of 7pm to 11pm, as most people are often engaged in work in that time period. Also, after 2am, number of hosts decrease gradually.There is slight dip in the number of hosts during 1pm to 5pm as most people are attending classes/labs.The graph depicting the same is shown below:-