CS 349 Assignment 1

Harit Gupta (170123020)

Q1 Ping

a. Option **-c** command is used to denote no of echo requests to send with 'ping' command. Ex: ping -c 4 www.facebook.com

b. Option **'-i'** command is used to set time interval (in seconds) between two consecutive ping requests. Ex : ping -i 2 www.facebook.com

c. Option '-l' command is used to send ECHO_REQUEST packets to the destination one after another without waiting for a reply. The limit for sending such packets by a normal user is 3. We can send more packets using sudo control. *Ex:* ping -l 3 www.facebook.com
Also, option '-f' command can be used to flood the requests one after the other without waiting for a response.

d. Option '-s' command is used to set the ECHO_REQUEST packet size (in bytes). But, actual size of packet is larger than what the user specify, due to addition of ICMP header(8 bytes) and IP headers(20 bytes). So, if the packet size is set to 32 bytes, the total packet size sent would be 32+8+20 = 60 bytes.
Ex: ping -s 32 www.facebook.com

Q2 : Variation in RTT (Round Trip Time) due to changing factors

- ❏ Six hosts were used which are mentioned in the table below
- ❏ Reading were taken at 3 time slots i.e 9 am, 3 pm and 9 pm
- ❏ Packet Loss is mentioned in parenthesis alongside with RTT in the table.

Host Address	IP Address	Location	Avg. RTT 1 (ms) at 9 am	Avg. RTT 1 (ms) at 3 pm	Avg. RTT 1 (ms) at 9 pm	Total Avg, RTT (ms)
amazon.in	54.239.33.92	Dublin	40.927 (0%)	41.181 (0%)	42.481 (0%)	41.529
glodls.to	104.27.188.5	Texas	14.981 (0%)	13.518(0%)	13.491 (0%)	13.996
subscene.com	104.27.181.8	Texas	14.185(0%)	19.253(0%)	13.744(0%)	15.727
codeforces.com	81.27.240.126	Russia	48.214(8%)	47.796(4%)	47.036(0%)	47.682
reddit.com	151.101.193.140	California	8.296(3%)	7.357(0%)	7.927(2%)	7.86
flipkart.com	163.53.78.128	India	169.164(0%)	168.862(0%)	181.083(0%)	173.036

➢ **Packet Size:** As packet size increases, the latency also increases. Also over a certain size, the latency rapidly increases. This is because of the concept of the *Maximum Transmission Unit(MTU).* The most common MTU size is 1500 bytes, that is if packet size is less than 1500 bytes, it will be sent as a single packet else it will be broken into frames to fit in buffer of the reciever,thus increasing latency.

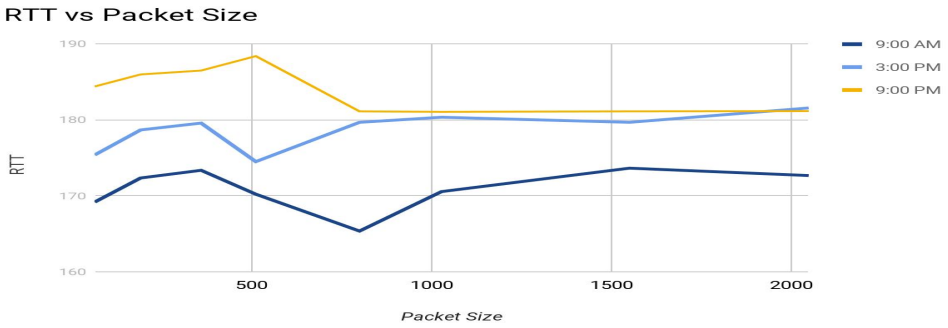
➢ **Time of the day:** The Internet Service Provider(ISP) gateway can handle only a constant number of requests per second. So, there's a increase in ping time during certain hours of the day(generally evening/night) as more users are active at that time. During a certain hour, no of hosts will be different in different countries due to different time zones in countries which can be seen in the table as well.

➢ **Packet Loss:** There exists a packet loss of more than 0% in the case of some websites. It is primarily due to network congestion and flow control. Flow control refers to when packets are sent at a faster rate than the nodes can process. It occurs when one or more packets of data traveling across a computer fail to reach their destination IP. Also,there might be some faultly hardware which can cause some packets to be lost.

➢ **Geographical Location:** If someone is using a server closer to the client device, the latency would be less rather in the case where the server would be far because distance is less, so it should take less time.However, this correlation is not clearly observable due to a variety of factors. Firstly, the speed of

servicing requests and responding with a packet depends on the host server's efficiency and architecture. Hence RTTs measured are weakly correlated with the geographical distance of the hosts.

Size(Bytes)	**64**	**192**	**360**	**512**	**800**	**1028**	**1550**	**2048**
Avg. RTT (9 am)	169.164	168.983	169.804	170.207	169.380	169.294	169.499	170.212
Avg. RTT (3 pm)	168.862	169.022	170.045	168.940	169.043	170.351	169.961	169.193
Avg. RTT (9 pm)	181.083	181.054	181.371	181.105	181.105	181.037	181.105	181.136



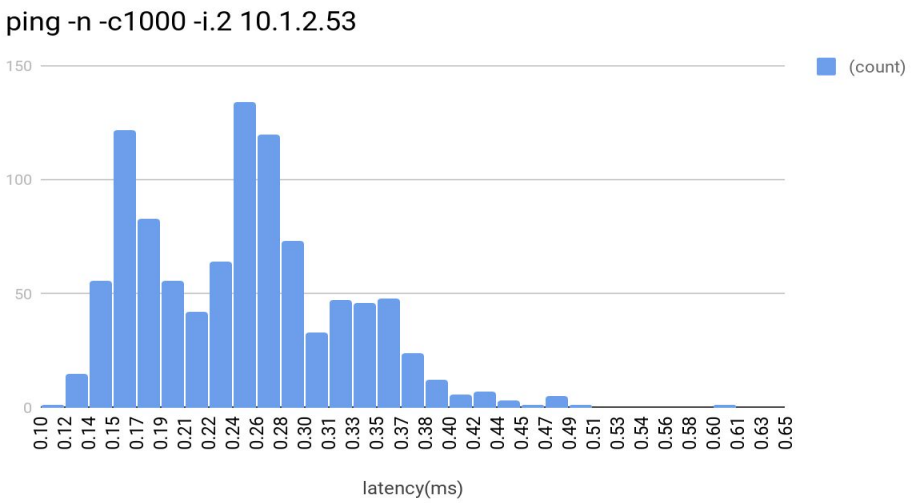
Q3) **Ping command Options**

Command	Packets transmitted	Packets received	Packet Loss	Min latency (ms)	Max latency (ms)	Avg. latency (ms)
ping -n -c1000 -i.2 10.1.2.53	1000	1000	0%	0.117	0.602	0.248
ping -p ff00 -c1000 -i0.2 10.1.2.53	1000	994	0.6%	0.190	17.185	0.444

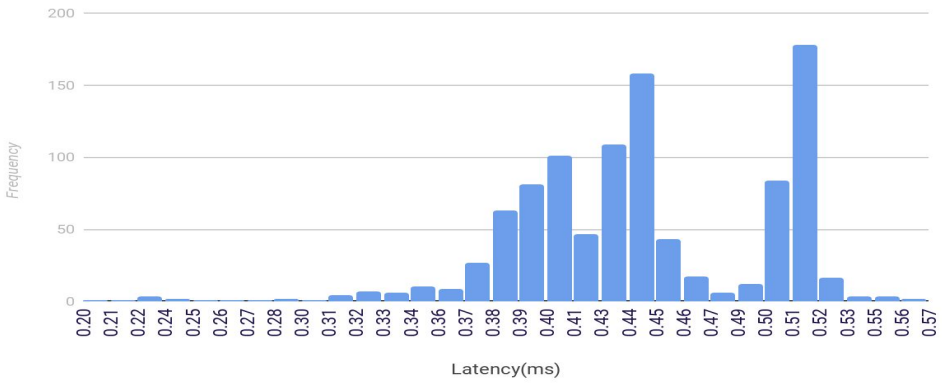
a)Packet Loss: Packet loss for the first command was 0.5%, while for the second command, it was 1%.

b)Ping Latency Statistics: Given in above table

c) Histograms of both the cases are shown below



ping -p ff00 -c1000 -i0.2 172.16.115.35



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) Ifconfig and Routing

A)

```
harit@thunderbolt: ~

harit@thunderbolt:~$ ifconfig
enp3s0f1  Link encap:Ethernet  HWaddr 98:29:a6:3f:44:bc
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:1304 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1304 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:214110 (214.1 KB)  TX bytes:214110 (214.1 KB)

wlp2s0    Link encap:Ethernet  HWaddr f8:28:19:bd:be:39
          inet addr:10.150.34.161  Bcast:10.150.39.255  Mask:255.255.248.0
          inet6 addr: fe80::49d1:b6fb:e986:53e0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:213234 errors:0 dropped:1 overruns:0 frame:0
          TX packets:64542 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:118372543 (118.3 MB)  TX bytes:17908806 (17.9 MB)
```

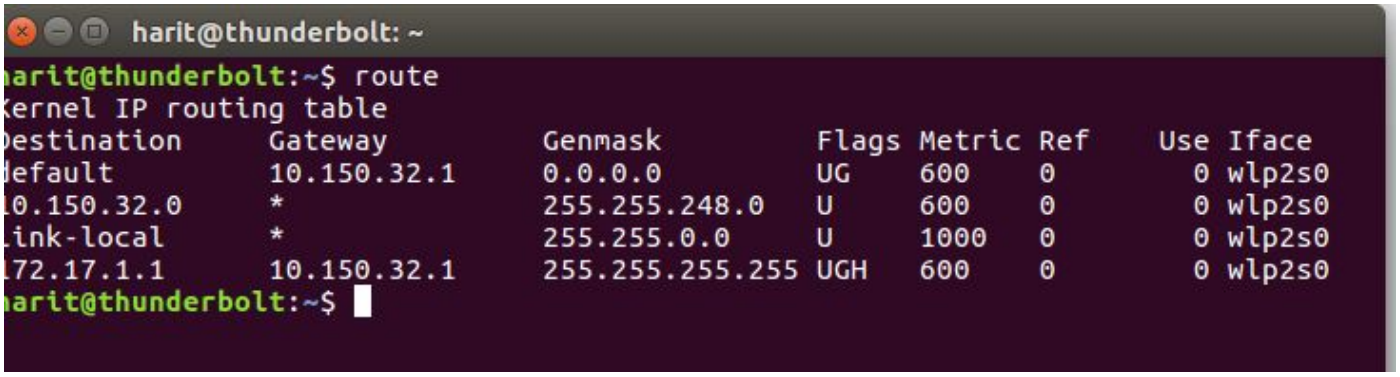
Ifconfig Explanation:

- ❏ Link encap:Ethernet : This represents the frame type associated with this interface. In our case it is Ethernet.
- ❏ HWaddr : the hardware address of the ethernet interface also known as MAC address. It is of 48 bits. First three octets represents the manufacturer id and the last three represents the serial number assigned to the device by the manufacturer.
- ❏ 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 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.
- ❏ **COLLISIONS**: Shows the number of packets that are colliding due to network congestion.
- ❏ **TXQUEUELN**: Denotes the length of the transmit queue of the device.

B) Options provided with ifconfig command:

- **-a**: Displays all interfaces which are currently available, even if down
- **-s :** Display a short list, instead of details
- **up :** This option is used to activate the driver for the given interface.
- **down :** This option is used to deactivate the driver for the given interface.
- **Address:** The IP address to be assigned to this interface.

C) Output of Route Command:

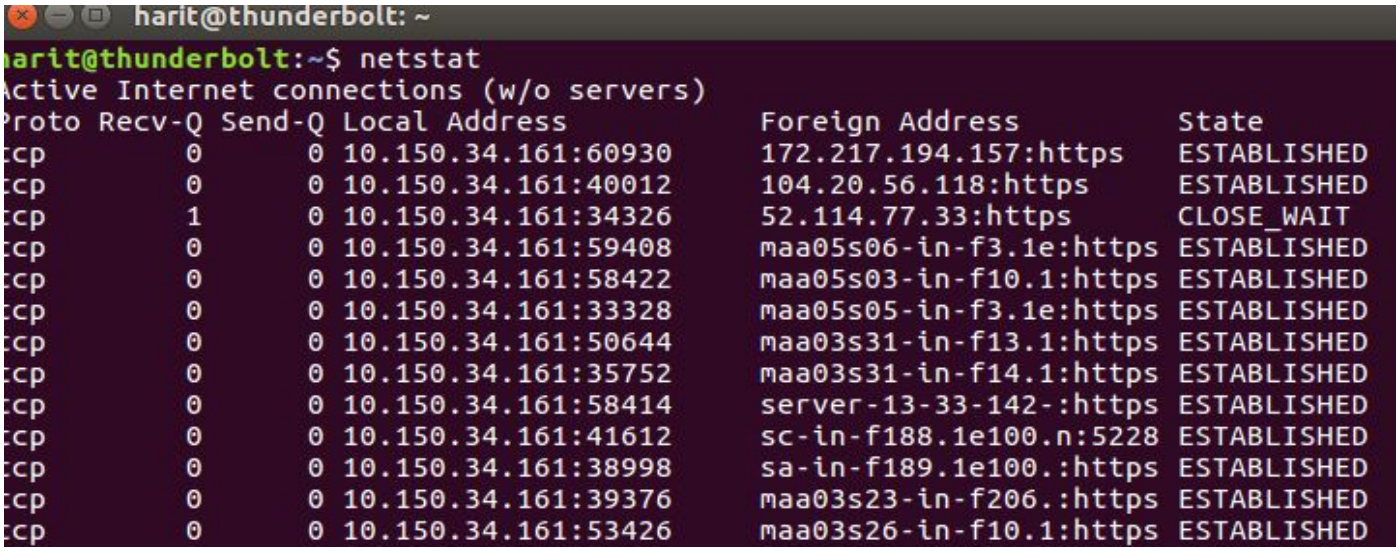


Explanation of Route :
DESTINATION: The destination network or destination host. **GATEWAY**: The gateway address or '*' if none set. **GENMASK**: The netmask for the destination net. **FLAGS**: U: route is up and G: use gateway.**METRIC**: The 'distance' to the target(counted in hops).**REF**: Number of references to this route. **USE**: count of lookups for the route. **IFACE**: Interface to which packets for this route will be sent.
D)Options provided with route command:
DEL: Delete a route **ADD**: Add a route **TARGET**: The destination network or host **-net**: Target is a network **-host**: Target is a host **-n:** Show numerical addresses instead of symbolic hostnames.

5) Netstat Command

a) **netstat** ("network statistics") is a **command**-line tool that displays network connections (both incoming and outgoing), routing tables, and many network interface (network interface controller or software-defined network interface) and network protocol statistics.

b) Netstat **-at comman**d is used to show all the TCP established connections.
Explanation:



Proto: Tells socket is TCP or UDP
Local and Foreign Address: Tells to which hosts and ports the listed sockets are connected
Recv-Q and Send-Q: Tells how much data is in the queue for that socket waiting to be read(Recv-Q) or sent(Send-Q)
State: Tells in which state the listed sockets are.

c) Netstat -r command is used to display the kernel routing table i.e it nearly shows the same output as route command does.

```
harit@thunderbolt:~$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         10.150.32.1     0.0.0.0         UG        0 0          0 wlp2s0
10.150.32.0     *               255.255.248.0   U         0 0          0 wlp2s0
link-local      *               255.255.0.0     U         0 0          0 wlp2s0
172.17.1.1      10.150.32.1     255.255.255.255 UGH       0 0          0 wlp2s0
```

The **“Destination”** column indicates the pattern that the destination of a packet is compared to. When a packet has to be sent over the network, this table is examined top to bottom, and the first line with a matching destination is then used to determine where to send the packet. 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 tells how many bits from the start of the ip address are used to identify the subnet from the ip address. The **“Flags”** column shows which flags apply to the current table line. “U” means Up, indicating that this is an active line. “G” means this line uses a Gateway. The “MSS” column lists the value of the Maximum Segment Size for this line. The MSS is a TCP parameter and is used to split packets when the destination has indicated that it somehow can’t handle larger ones. The “Window” column shows the window size, which indicates how many TCP packets can be sent before at least one of them has to be ACKnowledged. 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. The “Iface” column tells which network interface should be used for sending packets that match the destination.

d) netstat -i command is used to display the status of all network interfaces.

```
Kernel Interface table
Iface   MTU Met   RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
enp3s0f1   1500 0          0      0      0 0          0      0      0      0 BMU
lo        65536 0       1602      0      0 0       1602      0      0      0 LRU
wlp2s0     1500 0     284411      0      1 0      81771      0      0      0 BMRU
harit@thunderbolt:~$
```

e) netstat -su is used to showing the statistics of all UDP connections.

```
IcmpMsg:
    InType3: 172
    OutType3: 177
    OutType8: 4
Udp:
    14878 packets received
    177 packets to unknown port received.
    35 packet receive errors
    5021 packets sent
    RcvbufErrors: 35
    SndbufErrors: 2
    IgnoredMulti: 6927
UdpLite:
IpExt:
    InMcastPkts: 40
    OutMcastPkts: 254
    InBcastPkts: 6939
    OutBcastPkts: 22
    InOctets: 114043469
    OutOctets: 27034266
    InMcastOctets: 4687
    OutMcastOctets: 46955
    InBcastOctets: 1541908
    OutBcastOctets: 1164
    InNoECTPkts: 162721
    InECT0Pkts: 3
harit@thunderbolt:~$
```

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. When a network interface is disconnected--for example, when an Ethernet port is unplugged or Wi-Fi is turned off or not associated with an access point--no communication on that interface is possible, not even communication between your computer and itself. 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. This is important for troubleshooting.

Q6) Traceroute Experiment

- The six hosts used for the experiment are the same as used in Question 2
- Readings were taken at three times of a day: 9 am, 3 pm and 9 pm;

a)

Time of the Day	amazon.in	glodls.to	subscene.com	codeforces.com	reddit.com	flipkart.com
9 AM	30(incomplete)	12	12	20	9	11
3 PM	30(incomplete)	12	12	20	8	11
9 PM	30(incomplete)	10	27	19	9	11

a) Common hops with respect to my machine were 172.17.0.1 ,192.168.193,

b) It is possible to avoid network congestion.As as host might be in a different datacenter which means different physical locations, so the route to the same host might be different. For example, at 3 PM(163.53.78.128) flipkart.com have a different destination server address, while at 9 PM (163.53.78.87)it has a different address.

c) Sometimes, tracerouter doesn't provide the complete path. This happens mainly due to existence of a firewall which is setup to block such packets so as to maintain security.Moreover,some routers silently drop packets with expired TTLs.

d) Yes, it is possible. ping is straight ICMP from point A to point B, that traverses networks via routing rules. Tracert works very different, even though it uses ICMP. Traceroute works quite differently and 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 to the ICMP echo request from the host along the way, but a time exceeded message from that host - so even though it is using ICMP, it is using it in a very different way.

Q7) **a) Address Resolution Protocol** is a procedure for mapping a dynamic Internet Protocol address (IP address) to a permanent physical machine address in a local area network (LAN). **Address** is the IP Address of the other workstation to which communication was established. **HWtype** is the 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: manually added, M (as done in the screenshot), learned by the system, C by connecting to the host or 'published', M i.e told to the system by some other host than the one requested. **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, we can add the word 'temp' after the command.
arp -d <ip address> <mac address> can be used to delete an entry from the ARP table

```
harit@thunderbolt:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.150.33.185            ether   d4:6a:6a:5b:ca:25   C                     wlp2s0
10.150.33.143            ether   90:cd:b6:2c:78:55   C                     wlp2s0
10.150.32.1              ether   00:25:b4:d9:f7:c0   C                     wlp2s0
10.150.33.133            ether   bc:85:56:5f:6d:ef   C                     wlp2s0
10.150.34.31             ether   d4:3b:04:ed:ec:ca   C                     wlp2s0
10.150.34.120            ether   4c:34:88:be:1c:ac   C                     wlp2s0
10.150.34.43             ether   f8:28:19:59:9e:6f   C                     wlp2s0
10.150.33.159            ether   00:21:00:7c:2d:3f   C                     wlp2s0
```

```
harit@thunderbolt:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.1.2.12                ether   4c:4e:35:97:1e:ef   CM                    enp3s0f1
10.1.2.42                ether   4c:4e:35:97:1e:ef   CM                    enp3s0f1
10.1.1.74                ether   54:e1:ad:dd:fe:c9   C                     enp3s0f1
10.1.2.22                ether   4c:4e:35:97:1e:ef   CM                    enp3s0f1
10.1.0.254               ether   4c:4e:35:97:1e:ef   C                     enp3s0f1
harit@thunderbolt:~$ sudo arp -s 10.1.2.62 4c:4e:35:97:1e:ef
```

c) if you go into root directory and then to the following location, procs/sys/net/ipv4/neig

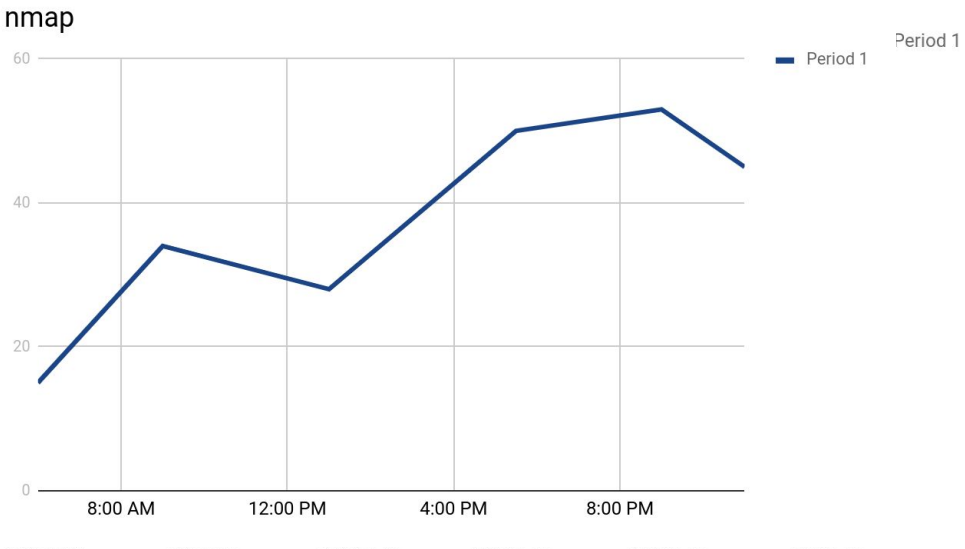
h/default/gc_stale_time ,you will find the arp value to be 60 seconds.

We can also find out the value of arp timeout manually by periodically checking the table and seeing if the value is deleted. That time will approximately be the cache timeout . We can also use binary search algo to improve efficiency
proc/sys/net/ipv4/neigh/default/gc_stale_time

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) NMAP

nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses.Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection. Nmap can adapt to network conditions including latency and congestion during a scan.



- The command used for the analysis is **nmap -n -sP 10.1.2.52/22** scanning 1024 IP addresses in the Kapili hostel.

A trend can be seen in the diagram as no of students increase before classes start (9 am) and decrease between class timings(1 Pm) and then again after classes are over (6 pm) and it increases around 9 pm,when students have come from various activities such as sport and then finally starts to decrease as night approaches as students sleep.