CS-349
NETWORKS LAB

ASSIGNMENT 1

ANUBHAV TYAGI
170101009

January 20, 2020

Q1.

(a) **-c** is the option used to specify the number of echo requests to send with *ping* command.
Command : ping -c [**number**] ⟨**host_address**⟩

(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.
Command : ping -i [**number**] ⟨**host_address**⟩

(c) **-l** is the option to send ECHO_REQUEST packets one after another without waiting for a reply. For a normal user, the limit for sending such ECHO_REQUEST packets is **3**.
Command : ping -l [**number**] ⟨**host_address**⟩

(d) **-s** is the option used to specify the ECHO_REQUEST packet size (in bytes).
If the packet size is set to 32 bytes, then the total packet size will be **60 bytes** [32 bytes (Packet Size) + 8 bytes (ICMP Header Size) + 20 bytes (IP Header)].
Command : ping -s [**size**] ⟨**host_address**⟩

Q2.

The following readings were recorded at 0830 hrs, 1400 hrs and 1930 hrs

Destination Host Address	IP Address	Location	Avg RTT (0830 hrs) (ms)	Avg RTT (1400 hrs) (ms)	Avg RTT (1930 hrs) (ms)	Overall Avg RTT (ms)
ox.ac.uk	129.67.242.155	England	453.642	500.076	421.678	458.465
msu.ru	188.44.50.103	Russia	512.777	548.614	464.168	508.519
iitd.ac.in	103.27.9.20	India	160.733	196.008	287.318	214.686
harvard.edu	23.185.0.1	USA	293.223	227.001	237.512	252.578
sydney.edu.au	129.78.5.8	Australia	530.681	463.465	399.720	464.622
www.tsinghua.edu.cn	166.111.4.100	China	753.655	715.697	626.862	698.738

Packet loss was observed to be 0% in all cases. However congestion and high traffic in the network may result in packet loss.

RTT v/s Distance : From the above table, we can conclude that there exists a **weak positive correlation** between geographical distance and RTT due to factors such as number of hops, propagation delay. Larger the distance, generally more are the number of routers the packet has to pass through and hence greater the processing delay.

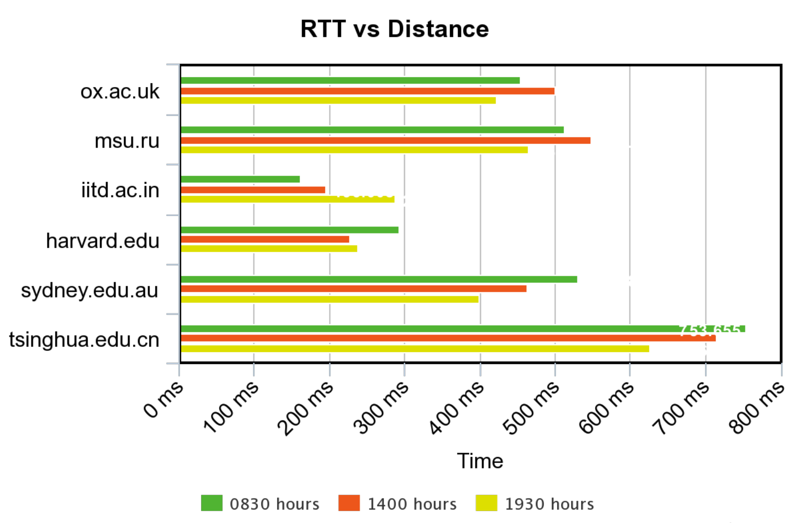


Figure 1: RTT vs Distance

The following experiment was carried by pinging **iitg.ac.in**

Size (in bytes)	64	128	256	512	1024	2048
Avg RTT (0830 hrs) (ms)	0.430	0.591	0.470	0.601	0.741	0.883
Avg RTT (1400 hrs) (ms)	0.399	0.422	0.483	0.594	0.786	0.910
Avg RTT (1930 hrs) (ms)	0.368	0.459	0.454	0.518	0.700	0.817

RTT v/s Size : From the above table, we can conclude that there exists a **positive correlation** between packet size and RTT. This is because larger the packet size, greater is the transmission delay. Also there is not much difference in RTT upto 1024 bytes because mtu (Maximum Transfer Unit) is 1500 bytes. Any packet greater than mtu gets split into multiple packets and hence have greater RTT.

RTT v/s Time of Day : From the above tables, we can conclude that RTT is realted to time of day. RTT is observed to be higher when there is congestion and high traffic in the network. Hence RTT is higher during peak hours od the day.

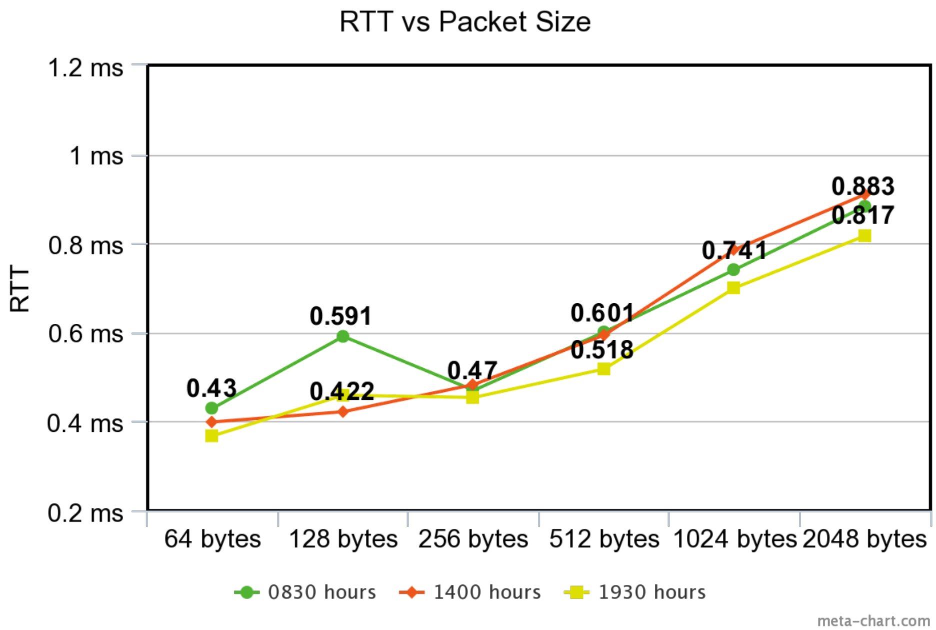


Figure 2: RTT vs Packet Size

Q3.

(a) IP Address : **172.17.0.23** Domain Name : **iitg.ernet.in**

Command	Packets Transmitted	Packets Recieved	Packet Loss Rate
ping -c 1000 -n 172.17.0.23	1000	1000	0%
ping -c 1000 -p ff00 172.17.0.23	1000	1000	0%

(b)

Command	Maximum Latency (ms)	Minimum Latency (ms)	Mean Latency (ms)	Median Latency (ms)
ping -c 1000 -n 172.17.0.23	3.550	0.172	0.383	0.357
ping -c 1000 -p ff00 172.17.0.23	3.100	0.194	0.389	0.353

(c) The distribution for both the curves resemble **Normal Distribution**

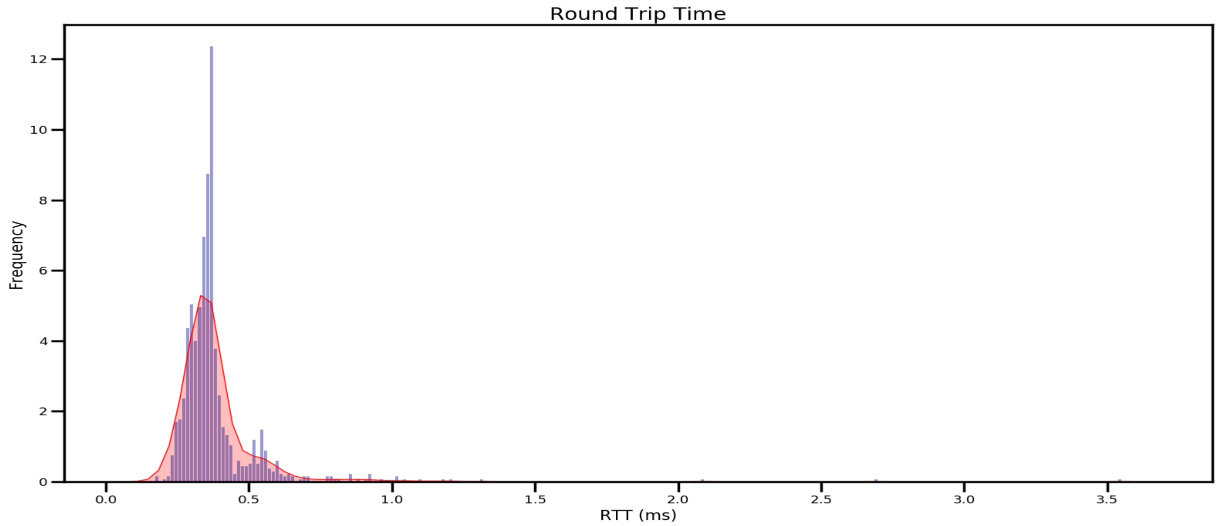


Figure 3: ping -c 1000 -n 172.17.0.23

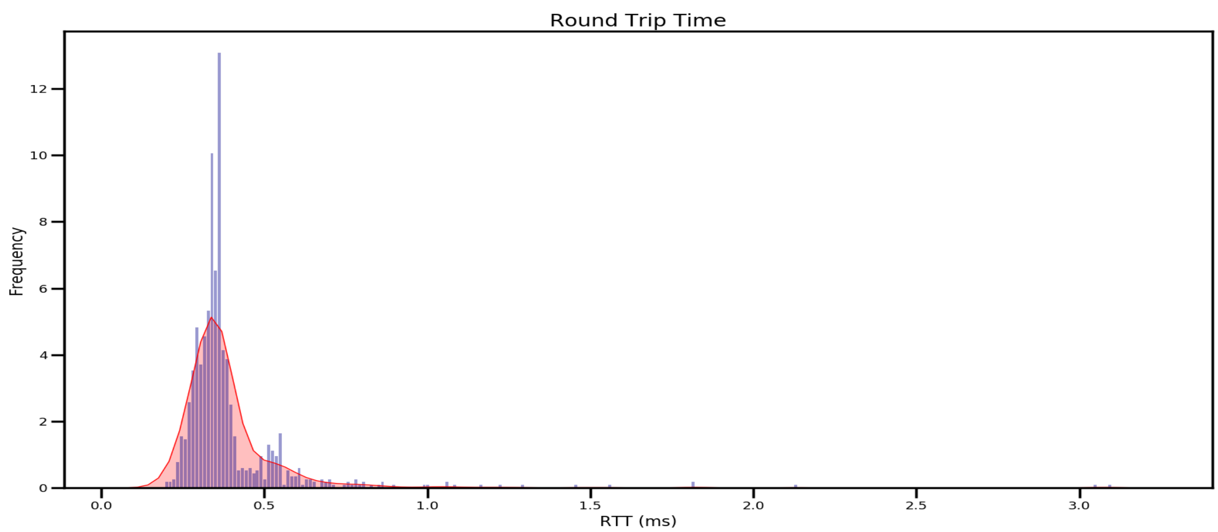


Figure 4: ping -c 1000 -p ff00 172.17.0.23

(d) The two scenarios set up to be very similar except two aspects. First is that **mean latency** in case of **ping -n** is smaller than that in case of **ping -p ff00**. This is because in case of **ping -n** no attempt will be made to lookup symbolic names for host addresses. Hence it saves a DNS query to translate domain name to an IP address. Second is that **packet loss rate** in case of **ping -p ff00** will be higher than that in case of **ping -n**. This is because *ping -p ff00* will fill the packet with *1111111100000000*. Since there is only one transition present (from 1 to 0), the clocks are more likely to go out of synchronisation and hence justifies for greater packet loss.

Q4.

(a) Ifconfig is used to configure the kernel-resident network interfaces. It is used at boot time to set up interfaces as necessary. After that,it is usually only needed when debugging or when system tuning is needed.

```
anu@tyagi619:~$ ifconfig
enp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.19.7.25  netmask 255.255.252.0  broadcast 10.19.7.255
        inet6 fe80::d681:c8a0:aa19:79d2  prefixlen 64  scopeid 0x20<link>
        ether 54:e1:ad:36:5c:dd  txqueuelen 1000  (Ethernet)
        RX packets 1430842  bytes 1819661298 (1.8 GB)
        RX errors 0  dropped 4  overruns 0  frame 0
        TX packets 326767  bytes 30581277 (30.5 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 4817  bytes 428075 (428.0 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4817  bytes 428075 (428.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp3s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.19.5.31  netmask 255.255.252.0  broadcast 10.19.7.255
        inet6 fe80::2340:4ec2:7065:b3f9  prefixlen 64  scopeid 0x20<link>
        ether 34:f6:4b:e4:1b:32  txqueuelen 1000  (Ethernet)
        RX packets 8344  bytes 5285959 (5.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3692  bytes 638376 (638.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figure 5: ifconfig Output

enp2s0 (ethernet interface) and lo (loopback interface) are the interface names.**flags** displays the status of the interface, including any flags currently associated with the interface. **BROADCAST** indicates that the interface supports IPv4 broadcasts. **RUNNING** indicates that the system is transmitting packets through the interface. **MULTICAST** shows that the interface supports multicast transmissions. **mtu 1500** shows that the interface has a maximum transfer size of 1500 octets. **inet and inet6** displays the IPv4 and IPv6 address that is assigned to the interface respectively. **netmask** displays the IPv4 netmask of the interface. **broadcast** denotes the broadcast address. **ether** shows the interface's ethernet layer address (or MAC Address). **txqueuelen** denotes the length of the transmit queue for the device. **RX Packets and TX Packets** show the total number of packets transmitted and recieved respectively.**RX bytes and TX bytes** indicate the total amount of data that has passed ethernet interface either way. **collisions** indicates if the packets are colliding while traversing the network (Value greater than 0 indicate packets are colliding).

(b) **-a** displays all the interfaces which are currently available, even if they are down. **up** causes the driver for the interface to be activated. **down** causes the driver for the interface to be shut down. **mtu N** sets the Maximum Transfer Unit (MTU) of an interface to N octets. **add addr/prefixlen** adds IPv6 addres to an interface.

(c) Route is used to show/manipulate routing table.

```
anu@tyagi619:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    100    0        0 enp2s0
10.19.4.0       0.0.0.0         255.255.252.0   U     100    0        0 enp2s0
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 enp2s0
```

Figure 6: route Output

Destination shows the destination network or destination host. **Gateway** shows the gateway address or '*' if none is set. **Genmask** shows the netmask for the destination net; '255.255.255.255' for a host destination and '0.0.0.0' for the default route. Possible **flags** include: **U** (route is up), **H** (target is a host), **G** (use gateway), **R** (reinstate route for dynamic routing), **D** (dynamically installed by daemon or redirect), **M** (modified from routing daemon or redirect), **A** (installed by addrconf), **C** (cache entry),**!** (reject route). **Metric** shows the distance to the target (counted in hops). **Ref** indicates the number of references to this route. **Use** displays count of number of lookups for the route. **Iface** shows the interface to which packets for this route will be sent.

(d) **-n** shows numerical addresses instead of trying to determine symbolic host names. **-C** lists the kernel's routing cache information. **-F** lists the kernel's FIB (Forwarding Information Base) routing table. **-A <ins>family</ins>** uses the specified address family (eg: inet).

```
anu@tyagi619:~$ route -n -A inet -C
Kernel IP routing cache
Source          Destination     Gateway         Flags Metric Ref    Use Iface
anu@tyagi619:~$ route -n -A inet -F
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.19.4.1       0.0.0.0         UG    20100  0        0 enp2s0
10.19.4.0       0.0.0.0         255.255.252.0   U     100    0        0 enp2s0
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 enp2s0
```

Figure 7: Various route options

Q5.

(a) **Netstat** prints information about the Linux networking subsystem including network connections, routing tables, interface statistics, masquerade connections, and multicast memberships.

(b) *netstat* **-at** is used to show all established TCP connections.

```
anu@tyagi619:~$ 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 0.0.0.0:postgresql      0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:https           0.0.0.0:*               LISTEN
tcp        0      0 localhost:6379          0.0.0.0:*               LISTEN
tcp        0      0 anu-Lenovo-ideapa:39032 maa03s31-in-f14.1:https ESTABLISHED
tcp        0      0 anu-Lenovo-ideapa:37062 sb-in-f188.1e100.n:5228 ESTABLISHED
tcp        0      0 anu-Lenovo-ideapa:39438 stackoverflow.com:https ESTABLISHED
tcp        0      0 anu-Lenovo-ideapa:41788 maa05s04-in-f3.1e:https ESTABLISHED
tcp        0      0 anu-Lenovo-ideapa:49986 maa03s23-in-f206.:https ESTABLISHED
tcp        0      0 anu-Lenovo-ideapa:45372 maa05s06-in-f3.1e:https ESTABLISHED
tcp        0      0 anu-Lenovo-ideapa:60906 sa-in-f189.1e100.:https ESTABLISHED
tcp        0      0 anu-Lenovo-ideapa:39016 maa03s31-in-f14.1:https ESTABLISHED
tcp        0      0 anu-Lenovo-ideapa:60416 maa05s09-in-f14.1:https ESTABLISHED
tcp        0      0 anu-Lenovo-ideapa:47784 instagram-p3-shv-:https ESTABLISHED
tcp6       0      0 ip6-localhost:ipp       [::]:*                  LISTEN
tcp6       0      0 [::]:postgresql         [::]:*                  LISTEN
tcp6       0      0 [::]:https              [::]:*                  LISTEN
tcp6       0      0 ip6-localhost:6379      [::]:*                  LISTEN
```

Figure 8: netstat -at Output

The fields of the output are as follows: **Proto** tells the protocol used by the socket, **Recv-Q**, in case of *ESTABLISHED Socket* shows the count of bytes not copied by the user program connected to this socket and in case of *LISTENING Socket* contains the current syn backlog, **SEND-Q** in case of *ESTABLISHED Socket* shows the count of bytes not acknowledged by the remote host and in case of *LISTENING Socket* contains the maximum size of the syn backlog,**Local Address** shows the address and port number of the local end of the socket, **Foreign Address** shows the address and port number of the remote end of the socket, **State** shows the status of the socket (Eg: LISTEN, ESTABLISHED, CLOSE, UNKNOWN, SYN_SET, SYN_RECV, FIN_WAIT1, FIN_WAIT2, TIME_WAIT, CLOSE_WAIT, LAST_ACK, CLOSING).

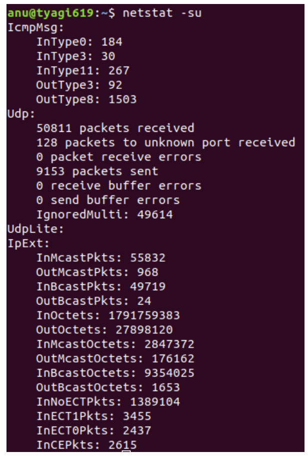
(c) **netstart -r** shows the **kernal routing table**.The fields of the output are as follows:
Destination shows the destination network or destination host. **Gateway** shows the gateway address or '*' if none is set. **Genmask** shows the netmask for the destination net. Possible **flags** include: **U** (route is up), **H** (target is a host), **G** (use gateway), **R** (reinstate route for dynamic routing), **D** (dynamically installed by daemon or redirect), **M** (modified from routing daemon or redirect), **A** (installed by addrconf), **C** (cache entry),**!** (reject route). **Metric** shows the distance to the target (counted in hops). **Ref** indicates the number of references to this route. **Use** displays count of number of lookups for the route. **Iface** shows the interface to which packets for this route will be sent. **MSS** shows default maximum segment size for TCP connections over this route. **Window** shows default window size for TCP connections over this route. **irtt** shows initial round trip time.

```
anu@tyagi619:~$ 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
10.19.4.0       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
```

Figure 9: netstat -r output

(d) **-i** option of *netstat* is used to display the status of all network interfaces. The number of network interfaces on my computer is **3** (enp2s0 (Ethernet), lo (loopback), wlp3s0 (wireless lan)).

(e) **-su** is used to show statistics of all UDP connections.



```
anu@tyagi619:~$ netstat -su
IcmpMsg:
    InType0: 184
    InType3: 30
    InType11: 267
    OutType3: 92
    OutType8: 1503
Udp:
    50811 packets received
    128 packets to unknown port received
    0 packet receive errors
    9153 packets sent
    0 receive buffer errors
    0 send buffer errors
    IgnoredMulti: 49614
UdpLite:
IpExt:
    InMcastPkts: 55832
    OutMcastPkts: 968
    InBcastPkts: 49719
    OutBcastPkts: 24
    InOctets: 1791759383
    OutOctets: 27898120
    InMcastOctets: 2847372
    OutMcastOctets: 176162
    InBcastOctets: 9354025
    OutBcastOctets: 1653
    InNoECTPkts: 1389104
    InECT1Pkts: 3455
    InECT0Pkts: 2437
    InCEPkts: 2615
```

Figure 10: netstat -su Output

(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.

Q6.

Traceroute tracks the route packets taken from an IP network on their way to a given host.

(a) The following readings were recorded at 0830 hrs, 1400 hrs and 1730 hrs.

	ox.ac.uk	msu.ru	iitd.ac.in	harvard.edu	sydney.edu.au	tsinghua.edu.cn
Hop Count (0830 hrs)	32	26	22	12	19	33
Hop Count (1400 hrs)	32	26	22	12	19	33
Hop Count (1930 hrs)	32	26	22	12	19	33

The common hops among all traceroute found are - **192.168.43.234** and **172.25.11.85**. **10.72.163.19** and **172.16.85.235** are same for msu.ru and harvard.edu. **10.72.163.18** is same for ox.ac.uk and sydney.edu.au. **172.16.85.229** is same for sydney.edu.au and iitd.ac.in. **103.198.140.54** is same for msu.ru and www.tsinghua.edu.cn.

(b) The route to the host changes at different times of the day because the packets are redirected at nodes to take a route having less congestion or traffic. Since **congestion** in a network varies at different times of the day, the packet is routed to different paths in the network. Also failure in one part of network may result in different route to host.

(c) *Traceroute* may not find complete path to some hosts in the following cases: ICPM reply by intermediate host may be lost, destination host may not send ICPM reply or accept ICPM packet, and either destination host or sender may not be connected to the network.

(d) It is possible to find partial intermediate path using *traceroute* even if *ping* fails. This is because in case of *ping* intermediate hosts only forward ICPM packets to destination host, and only destination host replies on recieving packet. Whereas in case of *traceroute* each intermediate host responds with an ICPM packet. So even if destination host is not accepting ICPM packets (or not replying), a partial path can be found.

Q7.

(a) **arp** is the command used to show full ARP Table for a machine. The following are the columns of ARP Table: **Address** lists the IPv4 address of network neighbour, **HWtype** shows the type of hardware device (like ethernet), **HWaddress** lists MAC address for the corresponding IPv4 address, **Iface** shows the interface name, **Mask** displays the netmask and **flags** show the status of each entry(C (Complete), M (Permanent), P (Published)).

(b) Adding or deleteing entries from ARP Table require sudo (root) access. **arp -s IP_Address MAC_address** is used to add entry to ARP Table. **arp -d IP_Address** is used to delete entry from ARP Table.

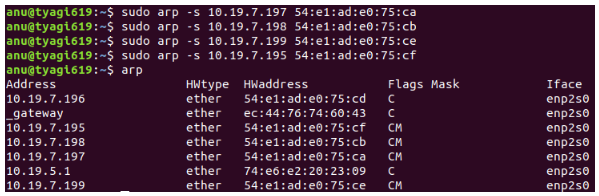


Figure 11: Adding entry to ARP Table

(c) The entries in the cache of the ARP module of the kernel remain valid for **60 seconds**.This can be observed from **cat /proc/sys/net/ipv4/neigh/default/gc_stale_time**. A *trial and error* method to discover the timeout values for the ARP cache entries is to add a temporary entry to ARP Table and check for the presence of entry in table after fixed intervals(say 6 seconds). The time at which entry disappears from the ARP Table is the cache timeout.

(d) If two IP addresses map to same Ethernet address then 100% packet loss will be observed when either of the IP address is pinged. To communicate with machines on the same subnet range, MAC address is used for sending the packages. In the ARP table ,the IPs of devices of other subnet ranges have the ethernet address of the router that connects those two subnets, ARP tables is referred and then packets are sent to the router which then uses its own routing table to send to the packet to destination device.

Q8.

The command used was **nmap -n -sP 10.19.4.0/22**. The hostel chosen for the experiment was **Lohit**. **Maximum** number of hosts were active around **2330 hours** and **minimum** number of hosts were active around **0530 hours**.

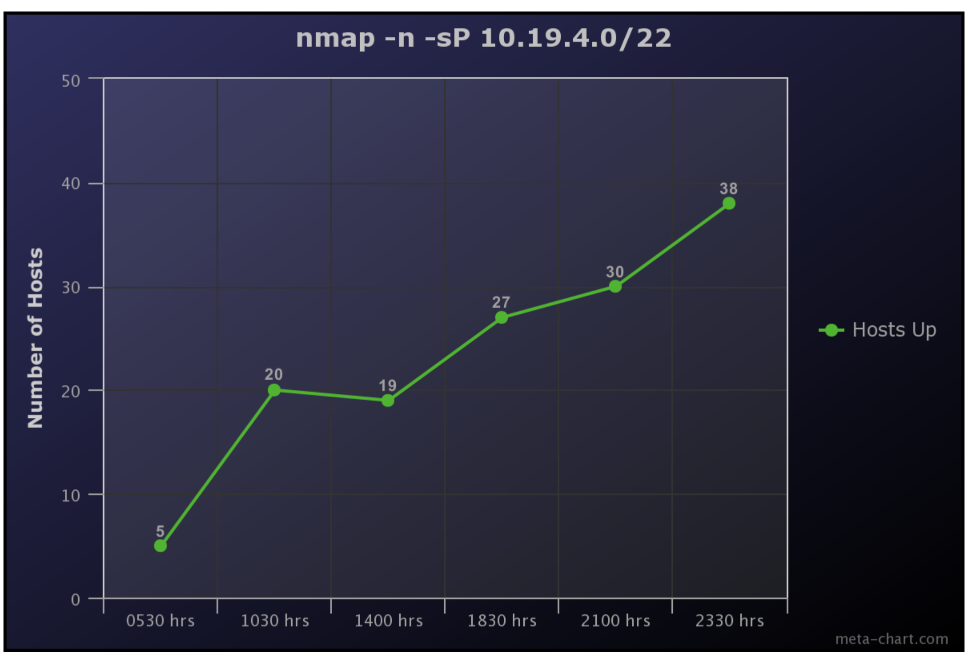


Figure 12: Number of active hosts using nmap