Answer 1)

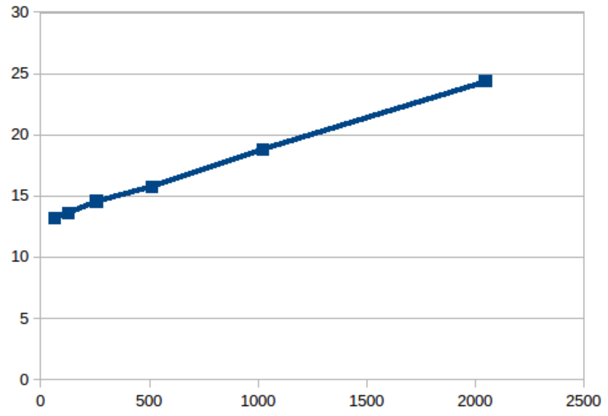
- ping -c count
- ping -i wait
- ping -l count , 3
- ping -s PacketSize , 92 bytes (ICMP header 28 bytes)

Answer 2)

- I encountered 0 packet loss while performing the experiment. Packet loss is typically caused by network congestion. When content arrives for a sustained period at a given router or network segment at a rate greater than it is possible to send through, there is no other option than to drop packets.It can also be caused by a number of other factors that can corrupt or lose packets in transit, such as radio signals that are too weak due to distance or multi-path fading, faulty networking hardware, or faulty network drivers.
-

IP	Location	10AM	1PM	10PM	Avg
104.16.109.208	Arizona ,US	76.061	91.875	85.680	84.539
95.211.185.133	Netherlands	331.955	358.695	247.127	312.592
113.13.101.208	China	281.58	319.45	211.86	270.96
164.100.58.217	India	226.65	319.45	211.86	252.65
139.59.80.215	India	218.768	218.242	216.443	217.817

- It can be clearly seen that the server which is close to the host i.e. in US have faster pings which is obvious as the distance is less. Also it can be seen that the ping to netherlands is slower than India and China even after less distance due to fact that more than geographical location it is the network distance that matters.
- Also there is no unique trend in the times but it is definitely seen that there is some significant slowness at some points in the day.This can be attributed to the fact that at those times the servers are loaded with requests leading to slower response time.



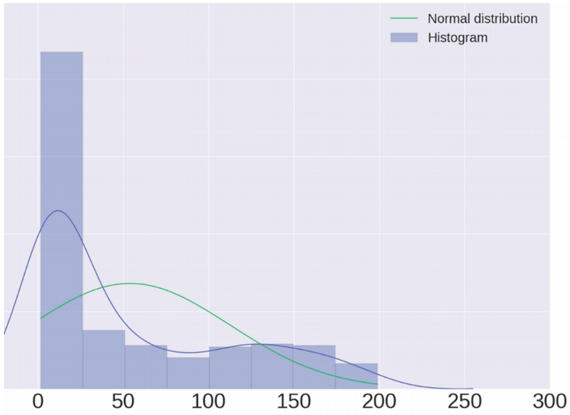
- Experiment is performed with the packet sizes 64,128,256,512,1024 and 2048 on X axis and RTT on Y axis.
- It can be easily seen as the packet size increases the RTT increases.
- Also there is sharp increase in RTT after 1500 because we need to send two packets.
- Also again in the experiment different RTT were seen at different times of the day due to the fact that servers have different loads at different times of the day.

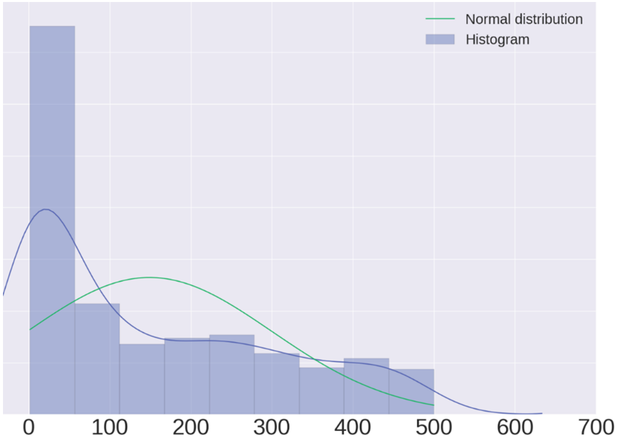
Answer 3) Ip address chosen is 202.141.80.14

- 0 percent packet loss for command 1 and 0.7 percent packet loss for command 2.
-

	Min	Max	Avg	Median
Command - 1	1.6	776.43	53.95	22.1
Command - 2	1.48	1012.32	149.13	92.1

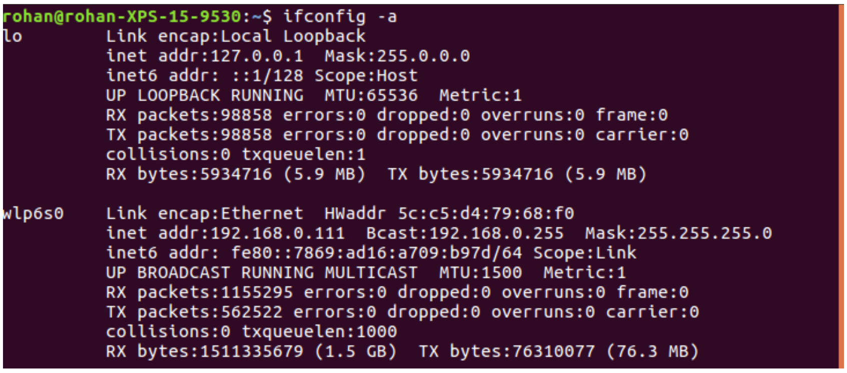
- The graph shows distribution of ping time in milliseconds. The graph on the left shows the distribution of command -1 while on the right shows the distribution of command -2.





- Repeating the experiiment many times , I observed that max/avg/median ping latencies for command-2 are large, i.e. ping with command-2 are slower. Also more packet loss happens with this pattern. There is a two fold reason to this :-
  Firstly in command 1 due to -n there is no reverse dns lookup and thus it has to be faster.
  Secondly it is easy to synchronize data with more no of transitions and thus command-2 which has only one tranisiton has more packet loss due to less synchronization.

Answer 4) Output of ifconifg command



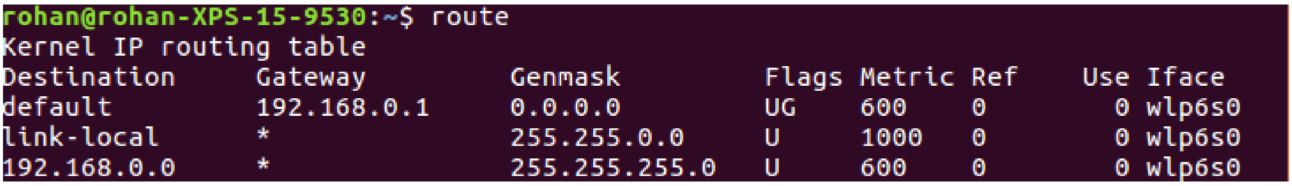
```
rohan@rohan-XPS-15-9530:~$ ifconfig -a
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:98858 errors:0 dropped:0 overruns:0 frame:0
          TX packets:98858 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:5934716 (5.9 MB)  TX bytes:5934716 (5.9 MB)

wlp6s0    Link encap:Ethernet  HWaddr 5c:c5:d4:79:68:f0
          inet addr:192.168.0.111  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::7869:ad16:a709:b97d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1155295 errors:0 dropped:0 overruns:0 frame:0
          TX packets:562522 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1511335679 (1.5 GB)  TX bytes:76310077 (76.3 MB)
```

- **wlp6s0** - It denotes the driver name and the unit number
- **Hwaddr** - shows the 48 bit Hex address of the device
- **inet addr** - shows the ipv4 address of the interface
- **inet6 addr** - shows the ipv6 address of the interface where fe80 denotes the subnet(/64) and 7869:ad16:a709:b97d denotes the host part. Link means that scope of the ip is on the link. Can't be used outside. Global means can be used anywhere.
- **ipv4 addr –** 192.168.0.11 is ipv4 address of the machine , Bcast 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 ie 192.168.0(24bits) is the subnet whereas 111 is the host part.
- **UP**(indicates kernel modules related to ethernet interface have been loaded) , **braodcast**(is able to) , **multicast**(supported) , **Running** (currently running).
- **MTU –** maximum transfer units in bytes
- **Metric –** used for priority in routing indicates distance
- **Rx packets – no of packets received , Tx packets – no of packets transmitted**
  errors(crc errorpackets).**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.

- **RX/TX bytes** is the number of bytes received/sent.

Output of route command



```
rohan@rohan-XPS-15-9530:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         192.168.0.1     0.0.0.0         UG    600    0        0 wlp6s0
link-local      *               255.255.0.0     U     1000   0        0 wlp6s0
192.168.0.0     *               255.255.255.0   U     600    0        0 wlp6s0
```

- **Destination** : The destination network or destination host.
- **Gateway** : The gateway address or â€™*â€™ if none set.
- **Genmask** : The netmask for the 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, but may be needed by routing daemons.
- **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.
- a **link-local address** is a network address that is valid only for communications within the network segment (link) or the broadcast domain that the host is connected to. So these addresses are directly forwarded to the interface without need of the gateway.

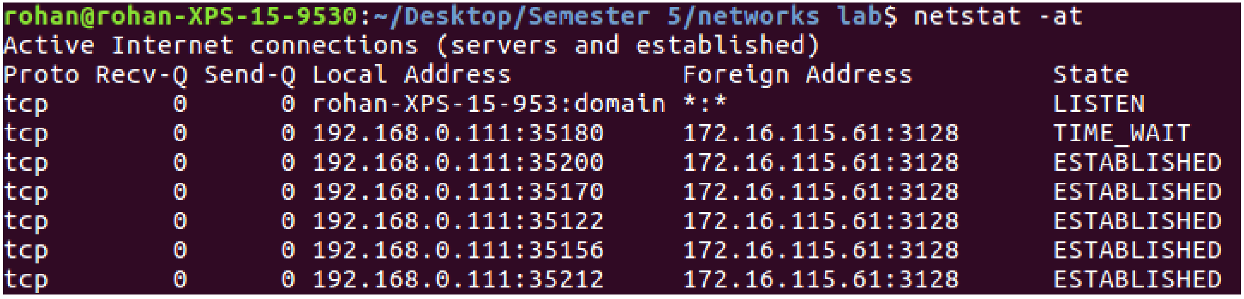
Route Options

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

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

Answer 5)

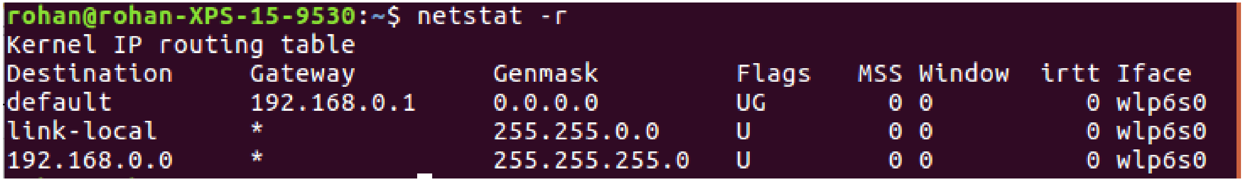
- Netstat is a networking utility that has multiple usages. It can print network connections, routing tables, interface statistics, masquerade connections, and multicast memberships depending on the first flag passed.
- It is used to display the status of TCP, SCTP, and UDP endpoints in table format. It can also display routing table information and interface information.
- **Netstat -at** where a stands for all listing all ports and t for TCP



```
rohan@rohan-XPS-15-9530:~/Desktop/Semester 5/networks lab$ netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 rohan-XPS-15-953:domain *:*                     LISTEN
tcp        0      0 192.168.0.111:35180     172.16.115.61:3128      TIME_WAIT
tcp        0      0 192.168.0.111:35200     172.16.115.61:3128      ESTABLISHED
tcp        0      0 192.168.0.111:35170     172.16.115.61:3128      ESTABLISHED
tcp        0      0 192.168.0.111:35122     172.16.115.61:3128      ESTABLISHED
tcp        0      0 192.168.0.111:35156     172.16.115.61:3128      ESTABLISHED
tcp        0      0 192.168.0.111:35212     172.16.115.61:3128      ESTABLISHED
```

Proto Under the Proto column, you'll find the name of the protocol being used by this particular connection. The protocol will be either TCP or UDP.
Recv-Q The count of bytes not copied by the user program connected to this socket.
Send-Q The count of bytes not acknowledged by the remote host.
Local address 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 The Foreign Address column contains the IP address of the remote computer and the port number being used for this particular connection.
State
CLOSED - Indicates 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

- **netstat -r** shows the routing table



```
rohan@rohan-XPS-15-9530:~$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         192.168.0.1     0.0.0.0         UG        0 0          0 wlp6s0
link-local      *               255.255.0.0     U         0 0          0 wlp6s0
192.168.0.0     *               255.255.255.0   U         0 0          0 wlp6s0
```

The fields are same as the output of the command route explained in question 3.
The extra fields are as follows :-
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.

- **netstat -i** can be used to display the all the active network interfaces. The output is same as ifconfig of ques 3.
- As displayed in the output above, I have 2 network interfaces on my desktop, wlp6so the ethernet interface and lo the loopback.
- **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.

Answer 6)

-

	104.16.109.208	95.211.185.133	113.13.101.208	164.100.58.217	139.59.80.215
Hop-1	4	10	12	15	11
Hop-2	4	10	12	15	10
Hop-3	4	10	11	14	11

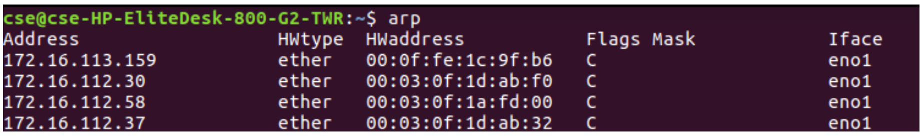
- The obvious common hop found was 207.86.208.17 and 207.88.13.122 which is the ip address of the site I used for the trace and I am guessing some immediate server next to the main server. Also I found the ip 213.248.81.237 and 216.6.87.1 common between 2 of the traces. This is a common occurrence as network circles are common and the routes can pass through similar servers.

- The time of the day also affects the hops as due to congestion different paths are chosen for routing.Redirection and load balancing are common practices due to which all this happens.

- The reason could be attributed to the fact that a firewall upstream is blocking the UDP packets. Also sometimes the networks block disable ICMP traffic when the network is under high load.
- Yes it is possible as working of both trace and ping are different.Ping works as a straight ICMP from source to destination, that involves sending a request and waiting for a reply in ICMP format. If the server is blocking and we don’t get a reply ping does not work. On the other hand trace works by targetting 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 is ICMP time exceeded message from the host which is very different from ICMP ECHO_RESPONSE.

Answer 7)

- arp table is displayed using **arp** command



```
cse@cse-HP-EliteDesk-800-G2-TWR:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
172.16.113.159           ether   00:0f:fe:1c:9f:b6   C                     eno1
172.16.112.30            ether   00:03:0f:1d:ab:f0   C                     eno1
172.16.112.58            ether   00:03:0f:1a:fd:00   C                     eno1
172.16.112.37            ether   00:03:0f:1d:ab:32   C                     eno1
```

Address IP/resolved name of the host
HWtype H/W address type, defaults to Ethernet. ash, netrom, dlci and irda also available.
HWaddress Actual H/W address entry

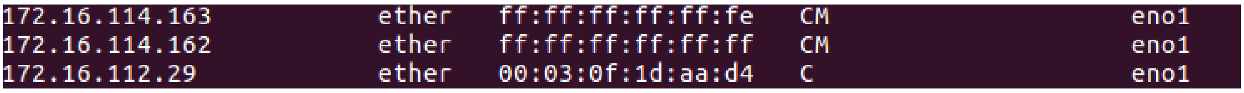
Flags ARP flags. Complete entries in the ARP cache will be marked with the C flag, permanent entries with M and published entries with P flag

Mask Netmask

Iface The network interface the host was found on

- **arp -s ip_address hw_address**
  The above command can be used to set up a new permanent ARP cache table entry.To insert a temporary entry without a M flag use the following command
  arp -s ip_address hw_address temp

  arp -d ip_address
  The above command is used to delete an entry from the ARP table.

- 

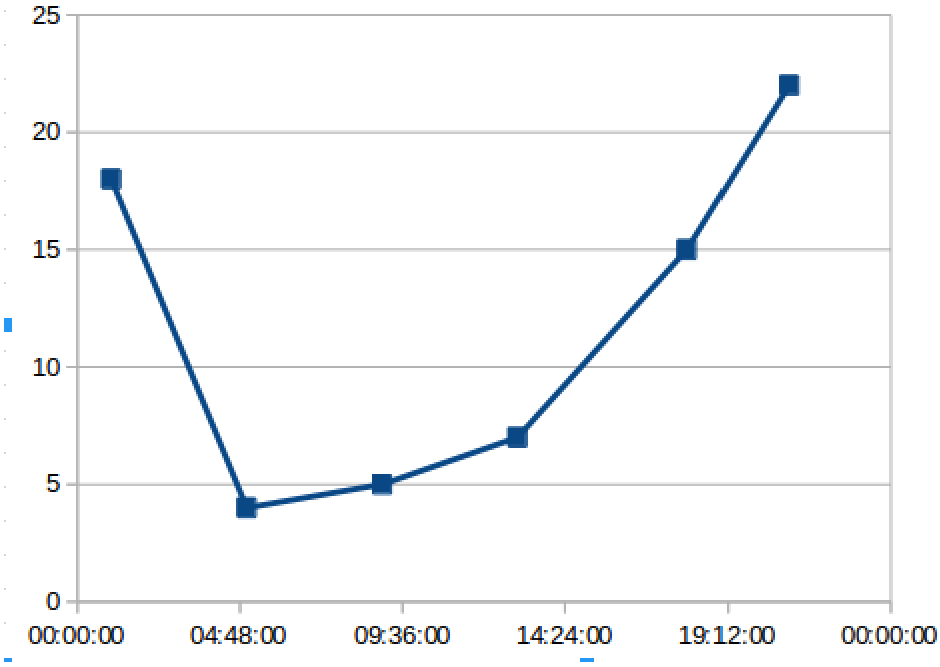
```
172.16.114.163          ether   ff:ff:ff:ff:ff:fe   CM                    eno1
172.16.114.162          ether   ff:ff:ff:ff:ff:ff   CM                    eno1
172.16.112.29           ether   00:03:0f:1d:aa:d4   C                     eno1
```

- 1) We can get the default arp cache timeout in the file "/proc/sys/net/ipv4/neigh/default/gc_stale_time". In my computer it is set as 60, which means timeout = 60 seconds.

  2) Another way is that we can randomly guess a number, and increase the system time by that value. If the entries have got cleared then we can half this value otherwise we double the value (Like binary search).

- I did the following to get the answer. I added a new ip address with a hwaddress already present in the arp table where the ip address belonged to the same subnet and then tried to ping the new ip address which worked properly. On taking the new ip address in a different subnet there is no response from the server. Hence pinging in the same subnet happens through MAC addresses and having 2 ips mapped to same MAC in the same subnet does not matter as the MAC address never leave the subnet. On the other hand having different ip addresses with the same MAC address in different subnets leads to lot of conflicts as switches can't learn properly and hence should be avoided.

Answer 8) I used the following command **nmap 10.10.2.0-25** which denotes the ip addresses of the rooms in my hostel lobby.



Observation – I woke up at 5:00 AM which shows the bottom in the graph as everybody is sleeping at that time.Peaks come around 9:00 PM and 1:00 AM which are the common before dinner and post dinner free times. Also around 9:00 AM and 4:00 PM we see very less activity as the institute net is switched off and people are in labs or in classes.