CS349 NETWORKS LAB ASSIGNMENT 1

PARTHA PRATIM MALAKAR

170101043

Question 1.

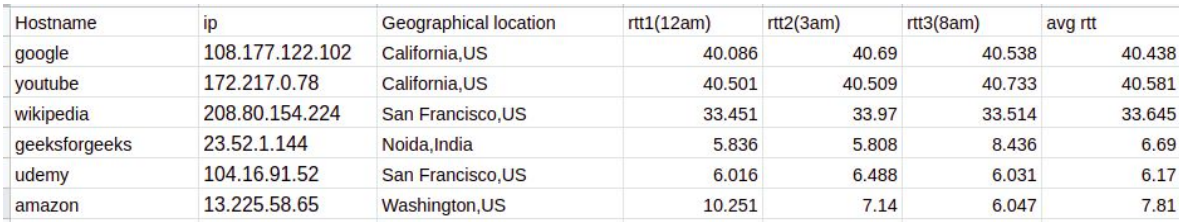
a)The option required is “-c”.(ping -c <number> <ip>)

b)The option required is “-i”.(ping -i <time> <ip>)

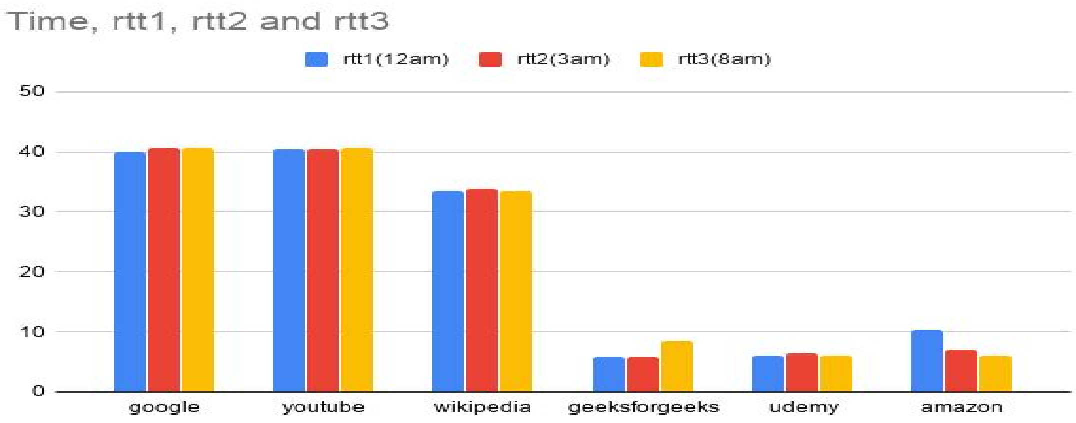
c)The option is “-l”.(ping -l 3 <ip>)(*3 is the maximum number of packet that can be sent to the without waiting for a reply*)

d)The option required is “-s”.(ping -s <size> <ip>)

Question 2.



Hostname	ip	Geographical location	rtt1(12am)	rtt2(3am)	rtt3(8am)	avg rtt
google	108.177.122.102	California,US	40.086	40.69	40.538	40.438
youtube	172.217.0.78	California,US	40.501	40.509	40.733	40.581
wikipedia	208.80.154.224	San Francisco,US	33.451	33.97	33.514	33.645
geeksforgeeks	23.52.1.144	Noida,India	5.836	5.808	8.436	6.69
udemy	104.16.91.52	San Francisco,US	6.016	6.488	6.031	6.17
amazon	13.225.58.65	Washington,US	10.251	7.14	6.047	7.81

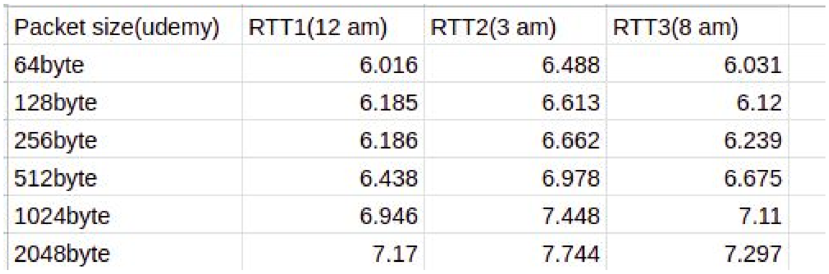


RTT and geographical distance:Though geography by itself cannot provide any information about many performance characteristics like bandwidth, congestion along a path, the linearized distance of a path does enforce a minimum delay along a path (propagation delay along a path).Therefore there is a weakly positive correlation between distance and RTT.There are a number of reasons for this. For example, an increased hop count. The packets have to go through more routers, at each router there may be a processing and propagation delay.

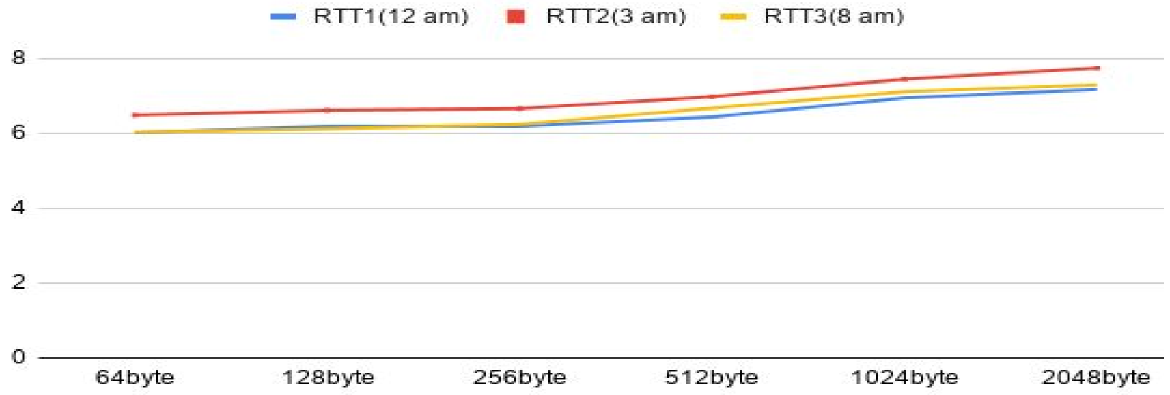
RTT vs daytime:RTT value is different in daytime for different website.This happens mainly due to network congestion.

RTT vs Packet size:RTT value increases with packet size.So there is a weakly positive correlation.

Host udemy.com

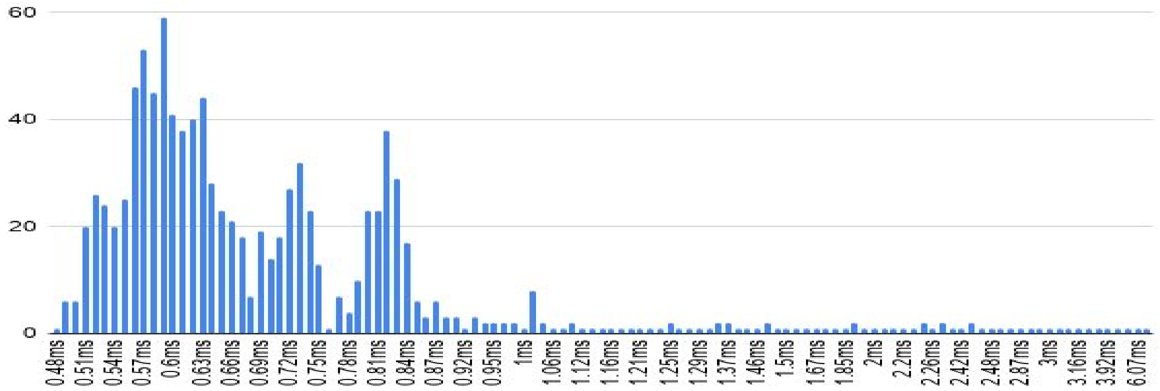


Packet size(udemy)	RTT1(12 am)	RTT2(3 am)	RTT3(8 am)
64byte	6.016	6.488	6.031
128byte	6.185	6.613	6.12
256byte	6.186	6.662	6.239
512byte	6.438	6.978	6.675
1024byte	6.946	7.448	7.11
2048byte	7.17	7.744	7.297



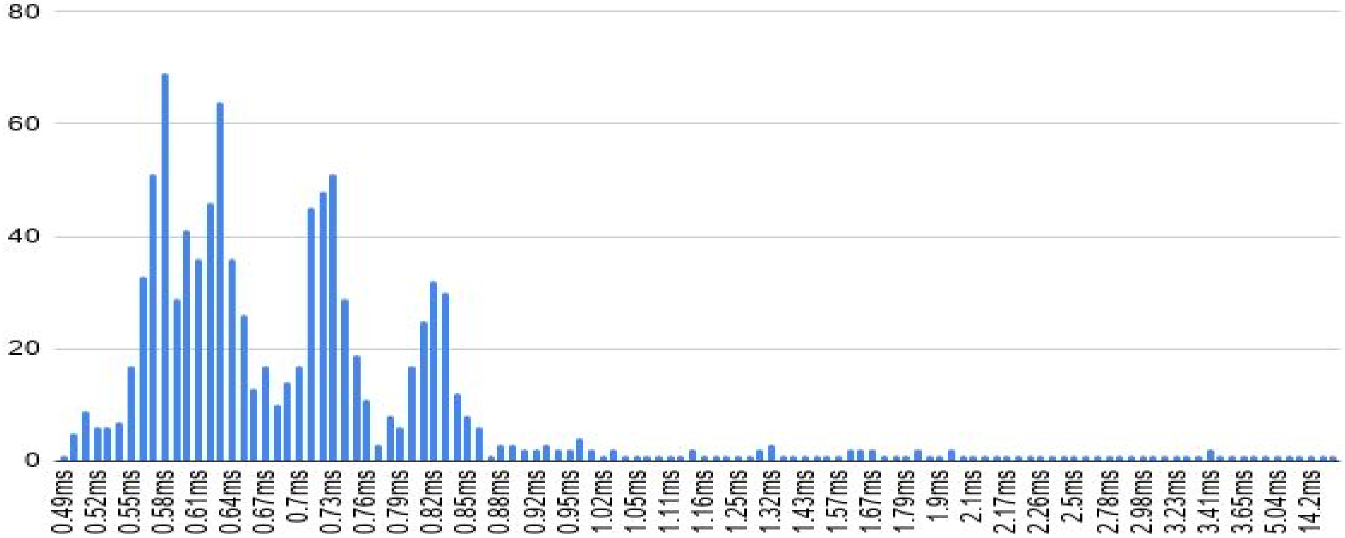
<u>Question 3.</u>

Command: ping -n -c 1000 10.19.4.1, Packet loss:0%, minimum latency=0.482,average latency=0.767,maximum latency=6.140, median latency=0.477 *(all in ms)*



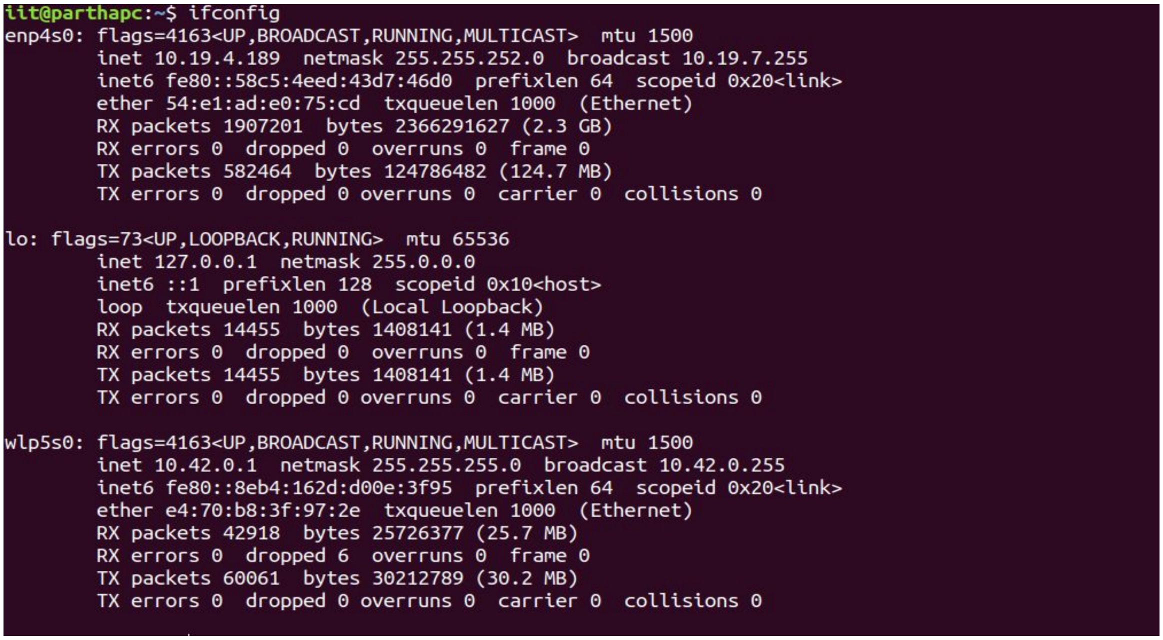
command:ping -p ff00 -c 1000 10.19.4.1

Packet loss:0%, minimum latency=0.496,average latency=0.846,maximum latency=27.445, median latency=1.170 *(all in ms)*



Both the graph have the shape of normal distribution. Minimum, Average,maximum,median latency are higher in second case.*ping -p* is use to specify up to 16 ``pad'' bytes to fill out the packet.Therefore -p ff will cause the sent packet to be filled with all ones which causes high latency.

Question 4.

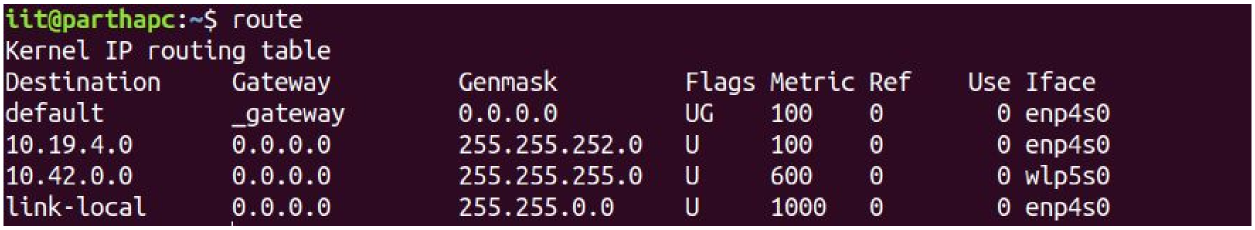


```
iit@parthapc:~$ ifconfig
enp4s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.19.4.189  netmask 255.255.252.0  broadcast 10.19.7.255
        inet6 fe80::58c5:4eed:43d7:46d0  prefixlen 64  scopeid 0x20<link>
        ether 54:e1:ad:e0:75:cd  txqueuelen 1000  (Ethernet)
        RX packets 1907201  bytes 2366291627 (2.3 GB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 582464  bytes 124786482 (124.7 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 14455  bytes 1408141 (1.4 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 14455  bytes 1408141 (1.4 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp5s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.42.0.1  netmask 255.255.255.0  broadcast 10.42.0.255
        inet6 fe80::8eb4:162d:d00e:3f95  prefixlen 64  scopeid 0x20<link>
        ether e4:70:b8:3f:97:2e  txqueuelen 1000  (Ethernet)
        RX packets 42918  bytes 25726377 (25.7 MB)
        RX errors 0  dropped 6  overruns 0  frame 0
        TX packets 60061  bytes 30212789 (30.2 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

ifconfig displays displays information about all network interfaces currently in operation. ***enp4s0*** is the ethernet(wired) interface. ***lo*** is the loopback interface . ***wlp5s0*** is the wireless ethernet interface***.mtu***(maximum transfer unit) is the maximum size of datagrams that can be processed by the interface ***.inet*** is the ipv4 address. ***inet6*** is the ipv6 address . ***netmask*** is the subnet mask to be used by the interface. ***broadcast*** address is usually made up from the network number by setting all bits of the host part***.prefixlen*** (Prefix length) specifies the number of bits in the IP address that are to be used as the subnet mask.For ipv4 the prefix length must be less than or equal to 32 bits. For an IPv6 address, the prefix length must be less than or equal to 128 bits. The default value of the prefix length for an IPv6 address is 64 bits. ***scopied*** the scope in Linux is an indicator of the distance to the destination network.Scopied *Host* A route has host scope when it leads to a destination address on the local host. Scopied *Link* A route has link scope when it leads to a destination address on the local network.*Universe* A route has universe scope when it leads to addresses more than one hop away***.ethe***r shows the hardware address or MAC address. ***TX*** gives the total number of packet transmitted.***TX byte*** total amount of data transmitted***.RX*** packets gives the total number of received packet.***RX bytes*** gives total data receive.The txqueuelen parameter of an interface limits the number of packets in the transmission queue in the interface's device driver.Its default value is 1000.***UP*** is a flag which marks an interface ``up'', i.e. accessible to the IP layer. This option is implied when an address is given on the command line.***BROADCAST*** shows that interface supports broadcast.***RUNNING*** Indicates that the system is transmitting packets through the interface.***MULTICAST*** indicates that the interface supports multicast transmissions.

b) ifconfig <interface name> up:This option is used to activate the driver for the given interface
ifconfig <interface name> down:This option is used to deactivate the driver for the given interface
ifconfig -s:Display a short list, instead of details.
ifconfig -a : This option is used to display all the interfaces available, even if they are down.

c)



```
iit@parthapc:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    100    0        0 enp4s0
10.19.4.0       0.0.0.0         255.255.252.0   U     100    0        0 enp4s0
10.42.0.0       0.0.0.0         255.255.255.0   U     600    0        0 wlp5s0
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 enp4s0
```

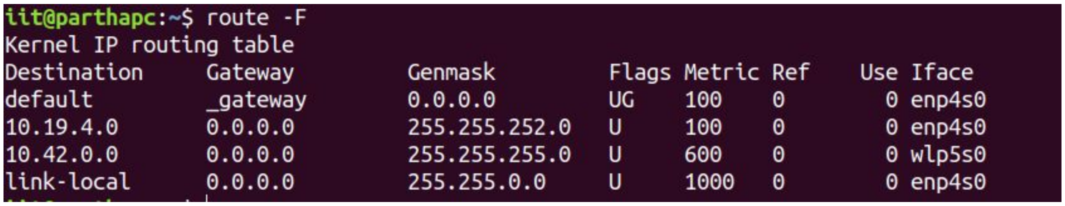
route command displays the routing table.***Destination*** indicates the destination network.***Gateway*** indicates gateway for the network.***Genmask*** indicates netmask.***Flags*** :the ***U*** indicate UP and the ***G*** indicate gateway used for the route.***MSS*** indicates the default Maximum Segment Size(MSS) for TCP connections for this route.Iface means network interface.***Ref*** indicates the number of references to the route.***Metric*** assigns an integer cost metric (that ranges from 1 to 9999) which you can use to calculate the fastest, most reliable, and least expensive routes.default route is used when no specific route can be determined for a given Internet Protocol (IP) destination address. Genmask for default destination is 0.0.0.0 .Gateway 0.0.0.0 means destination is in same network.***Iface*** indicates interface.

d) route -n :use numeric address instead of names.

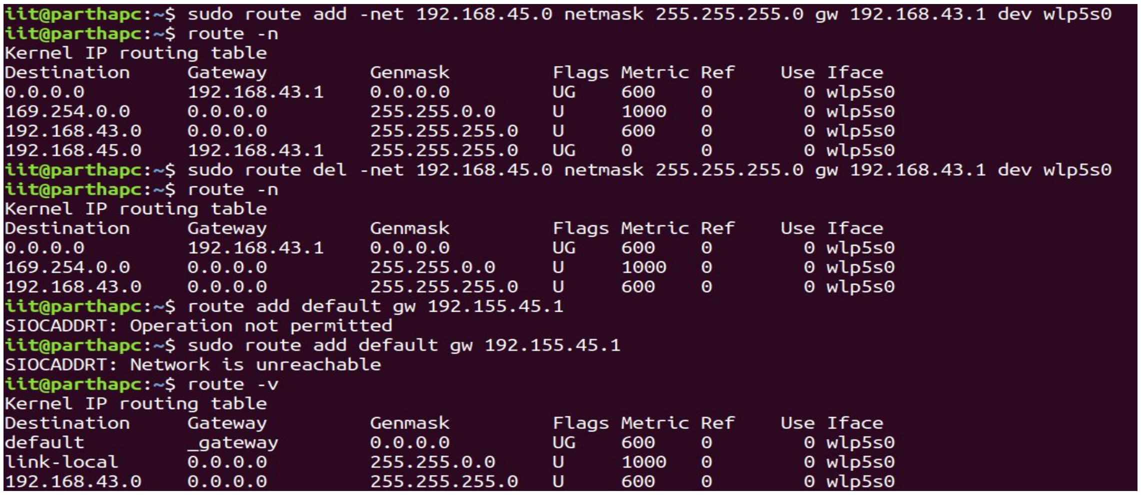
route add -net <network_address> gw <gateway> <interface_name> : to indicate the destination network we want to join

route del -net <network_address> gw <gateway> <interface_name> : to delete a destination network from the routing table

route -F :operate on the kernel's FIB (Forwarding Information Base) routing table.



```
iit@parthapc:~$ route -F
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    100    0        0 enp4s0
10.19.4.0       0.0.0.0         255.255.252.0   U     100    0        0 enp4s0
10.42.0.0       0.0.0.0         255.255.255.0   U     600    0        0 wlp5s0
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 enp4s0
```

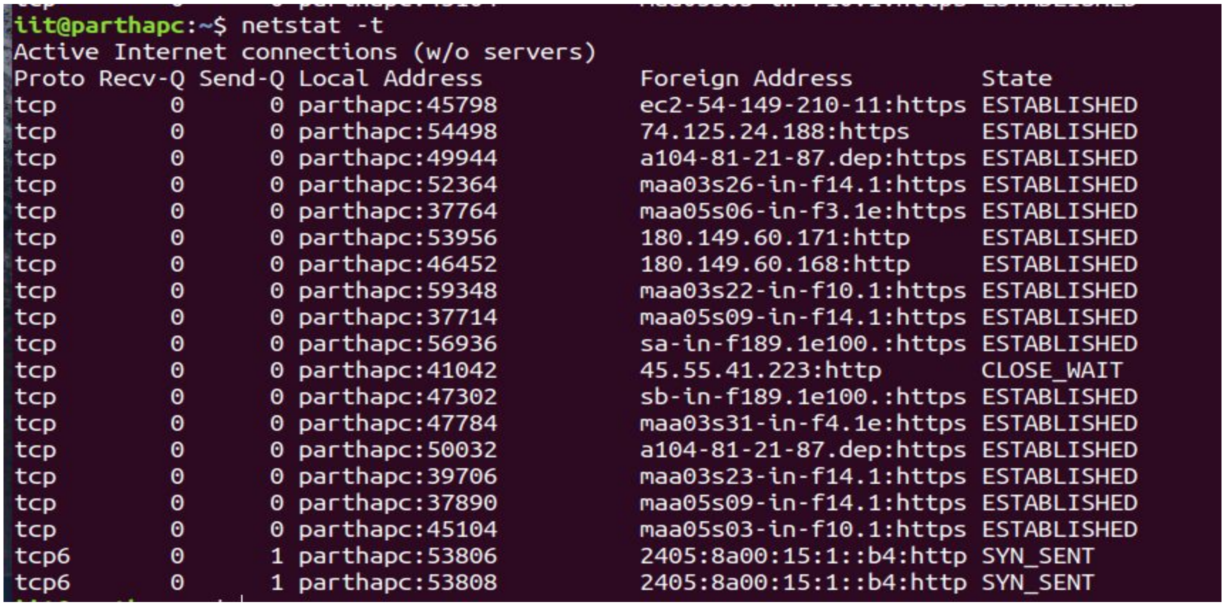


```
iit@parthapc:~$ sudo route add -net 192.168.45.0 netmask 255.255.255.0 gw 192.168.43.1 dev wlp5s0
iit@parthapc:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.43.1    0.0.0.0         UG    600    0        0 wlp5s0
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 wlp5s0
192.168.43.0    0.0.0.0         255.255.255.0   U     600    0        0 wlp5s0
192.168.45.0    192.168.43.1    255.255.255.0   UG    0      0        0 wlp5s0
iit@parthapc:~$ sudo route del -net 192.168.45.0 netmask 255.255.255.0 gw 192.168.43.1 dev wlp5s0
iit@parthapc:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.43.1    0.0.0.0         UG    600    0        0 wlp5s0
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 wlp5s0
192.168.43.0    0.0.0.0         255.255.255.0   U     600    0        0 wlp5s0
iit@parthapc:~$ route add default gw 192.155.45.1
SIOCADDRT: Operation not permitted
iit@parthapc:~$ sudo route add default gw 192.155.45.1
SIOCADDRT: Network is unreachable
iit@parthapc:~$ route -v
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    600    0        0 wlp5s0
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 wlp5s0
192.168.43.0    0.0.0.0         255.255.255.0   U     600    0        0 wlp5s0
```

Question 5.

a)The netstat command used for getting routing table information,network connections,interface statistics etc.

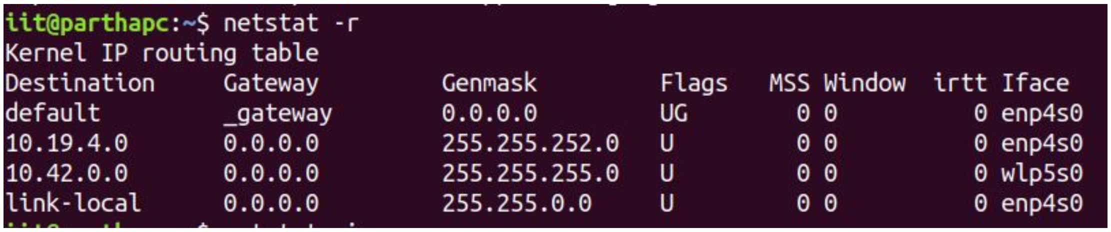
b)



```
iit@parthapc:~$ netstat -t
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 parthapc:45798          ec2-54-149-210-11:https ESTABLISHED
tcp        0      0 parthapc:54498          74.125.24.188:https     ESTABLISHED
tcp        0      0 parthapc:49944          a104-81-21-87.dep:https ESTABLISHED
tcp        0      0 parthapc:52364          maa03s26-in-f14.1:https ESTABLISHED
tcp        0      0 parthapc:37764          maa05s06-in-f3.1e:https ESTABLISHED
tcp        0      0 parthapc:53956          180.149.60.171:http     ESTABLISHED
tcp        0      0 parthapc:46452          180.149.60.168:http     ESTABLISHED
tcp        0      0 parthapc:59348          maa03s22-in-f10.1:https ESTABLISHED
tcp        0      0 parthapc:37714          maa05s09-in-f14.1:https ESTABLISHED
tcp        0      0 parthapc:56936          sa-in-f189.1e100.:https ESTABLISHED
tcp        0      0 parthapc:41042          45.55.41.223:http       CLOSE_WAIT
tcp        0      0 parthapc:47302          sb-in-f189.1e100.:https ESTABLISHED
tcp        0      0 parthapc:47784          maa03s31-in-f4.1e:https ESTABLISHED
tcp        0      0 parthapc:50032          a104-81-21-87.dep:https ESTABLISHED
tcp        0      0 parthapc:39706          maa03s23-in-f14.1:https ESTABLISHED
tcp        0      0 parthapc:37890          maa05s09-in-f14.1:https ESTABLISHED
tcp        0      0 parthapc:45104          maa05s03-in-f10.1:https ESTABLISHED
tcp6       0      1 parthapc:53806          2405:8a00:15:1::b4:http SYN_SENT
tcp6       0      1 parthapc:53808          2405:8a00:15:1::b4:http SYN_SENT
```

Proto shows which protocol is used .***Recv-Q*** and ***Send-Q*** how much data is in the queue for that socket waiting to be read or send.***Local address*** is the IP address(or the hostname) of the local computer and the port number being used.***Foreign Address*** is the IP address and port number of the remote computer to which the socket is connected.The ***State*** column tells in which state the listed sockets are. “*LISTEN*” State means waiting for some external computer to contact us. “*ESTABLISHED*” state means ready for communication. “*CLOSE WAIT”* state means that the foreign or remote machine has already closed the connection, but that the local program somehow hasn’t followed suit.

c)

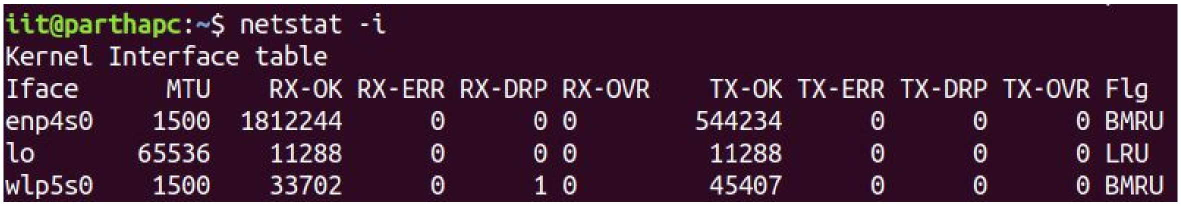


```
iit@parthapc:~$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         _gateway        0.0.0.0         UG        0 0          0 enp4s0
10.19.4.0       0.0.0.0         255.255.252.0   U         0 0          0 enp4s0
10.42.0.0       0.0.0.0         255.255.255.0   U         0 0          0 wlp5s0
link-local      0.0.0.0         255.255.0.0     U         0 0          0 enp4s0
```

netstat -r shows kernel IP routing table.

Destination column gives the destination of the packet.***Gateway*** indicates the gateway of the network. ***Genmask*** is the subnet mask.***Flags*** shows which flags are currently applied.*U* means up.*G* means gateway used.***MSS*** means maximum segment size.Its value 0 meaning no splitting of packet.***Window*** column gives the option of altering a TCP parameter.***irtt*** column stands for initial round trip time and used the kernel to guess about the best TCP parameters without waiting for slow replies.***Iface*** parameter indicates interface.

d)

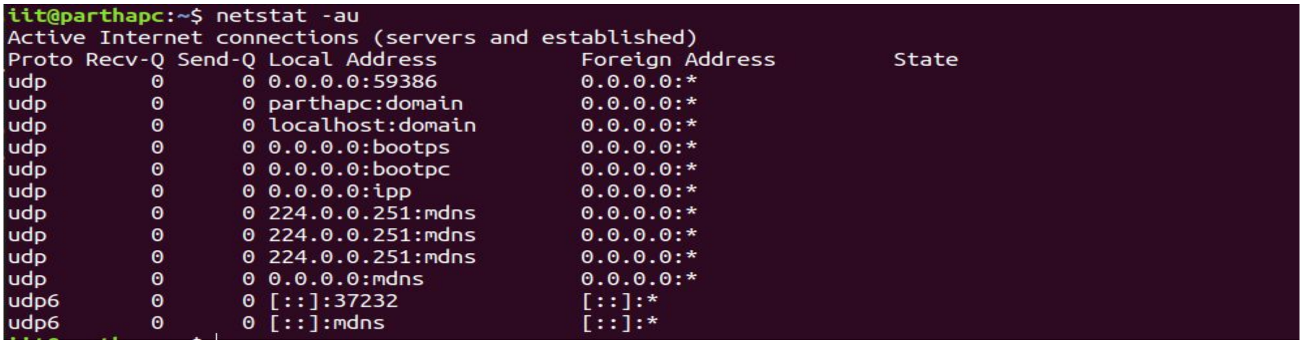


```
iit@parthapc:~$ netstat -i
Kernel Interface table
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
enp4s0    1500  1812244      0      0 0        544234      0      0      0 BMRU
lo       65536    11288      0      0 0         11288      0      0      0 LRU
wlp5s0    1500    33702      0      1 0         45407      0      0      0 BMRU
```

Total number of interface in my computer is 3.

Iface indicates interface***.MTU*** indicates maximum transfer unit.***flag*** column B means broadcast capability,***M*** means multicast capability,***L*** means loopback interface

e) netstat -au for udp connection

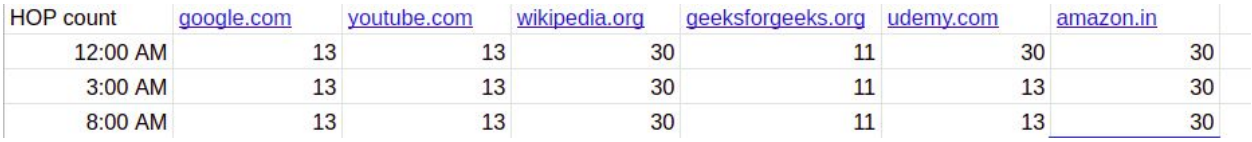


```
iit@parthapc:~$ netstat -au
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 0.0.0.0:59386           0.0.0.0:*
udp        0      0 parthapc:domain         0.0.0.0:*
udp        0      0 localhost:domain        0.0.0.0:*
udp        0      0 0.0.0.0:bootps          0.0.0.0:*
udp        0      0 0.0.0.0:bootpc          0.0.0.0:*
udp        0      0 0.0.0.0:ipp             0.0.0.0:*
udp        0      0 224.0.0.251:mdns        0.0.0.0:*
udp        0      0 224.0.0.251:mdns        0.0.0.0:*
udp        0      0 224.0.0.251:mdns        0.0.0.0:*
udp        0      0 0.0.0.0:mdns            0.0.0.0:*
udp6       0      0 [::]:37232              [::]:*
udp6       0      0 [::]:mdns               [::]:*
```

f) Loopback interface :The loopback interface is useful because it is an interface with an IP address which never goes down.The loopback device is a special, virtual network interface that your computer uses to communicate with itself.Thus it can be used to identify the device. It is used mainly for diagnostics and troubleshooting, and to connect to servers running on the local machine. The most commonly used IP address on the loopback network is 127.0.0.1 for IPv4 . The standard domain name for the address is localhost.The loopback address is used by protocols such as OSPF to determine protocol-specific properties for the device or network.

Question 6.

a)



HOP count	google.com	youtube.com	wikipedia.org	geeksforgeeks.org	udemy.com	amazon.in
12:00 AM	13	13	30	11	30	30
3:00 AM	13	13	30	11	13	30
8:00 AM	13	13	30	11	13	30

common hub for all routes…

_gateway (10.19.4.1)
172.17.0.50 (172.17.0.50)
172.17.0.1 (172.17.0.1)
192.168.193.1 (192.168.193.1)
14.139.196.17 (14.139.196.17)
10.119.254.241 (10.119.254.241

For google and youtube 2 more are common

10.177.31.21 , 10.255.238.205

b)When a router receives a packet, its only job is to send it to the next hop as soon as possible.Therefore it looks for the less traffic path around it for load balancing.So a router may send a packet to a different hob in different route even if the destination is same.

c)traceroute use ICMP or UDP .But some routers/firewall don't let icmp echo pass trough . Firewall blocks the UDP ports.In Most cases the blocking of packet is due security reason.Therefore the packet lost.

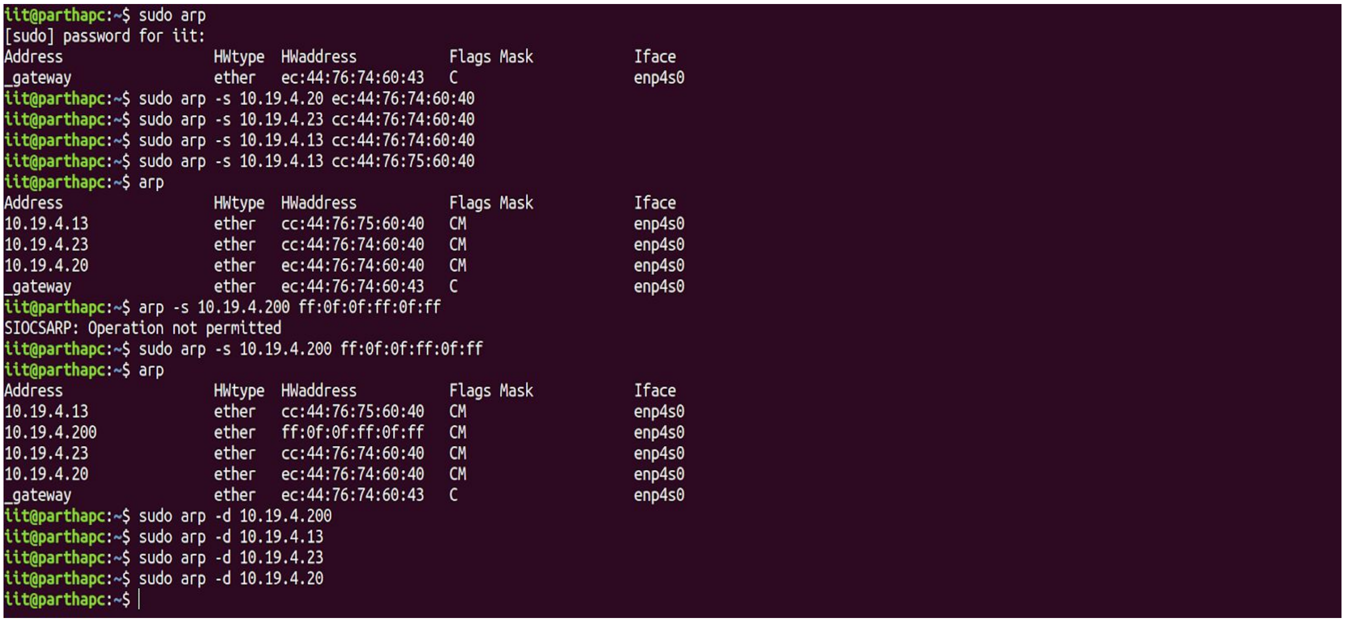
d)Though ping and Traceroute uses ICMP protocol ,they are not exactly same.Their working mechanisms are different.Ping uses ICMP “echo request” and traceroute uses ICMP “time exceeded” packets.Some router may allow ICMP “time exceeded” packets but not those ping “echo request” packets.Therefore if in a route those router/firewall present,ping will not work but traceroute will work.

Question 7.

a) ARP stands address resolution protocol is used to map MAC address (or hardware address) to an IP address.***Address*** Column indicates the destination IP and ***Hwaddress*** indicates MAC address corresponding to the ip.***HWtype*** indicate the hardware type.***C*** Flag indicate Complete entry.***M*** indicate permanent entry.***P*** flag indicate published entry .

c)The default arp cache timeout can be found by the command **cat /proc/sys/ipv4/neigh/default/gc_stale_time**.Its 60 for my PC.If we want to check the timeout value by trial and error what we"ll do is ,take a time interval,add a dummy entry and check for some interval and after that we will get to know the approximate value ,like +/- 10 seconds.

b)



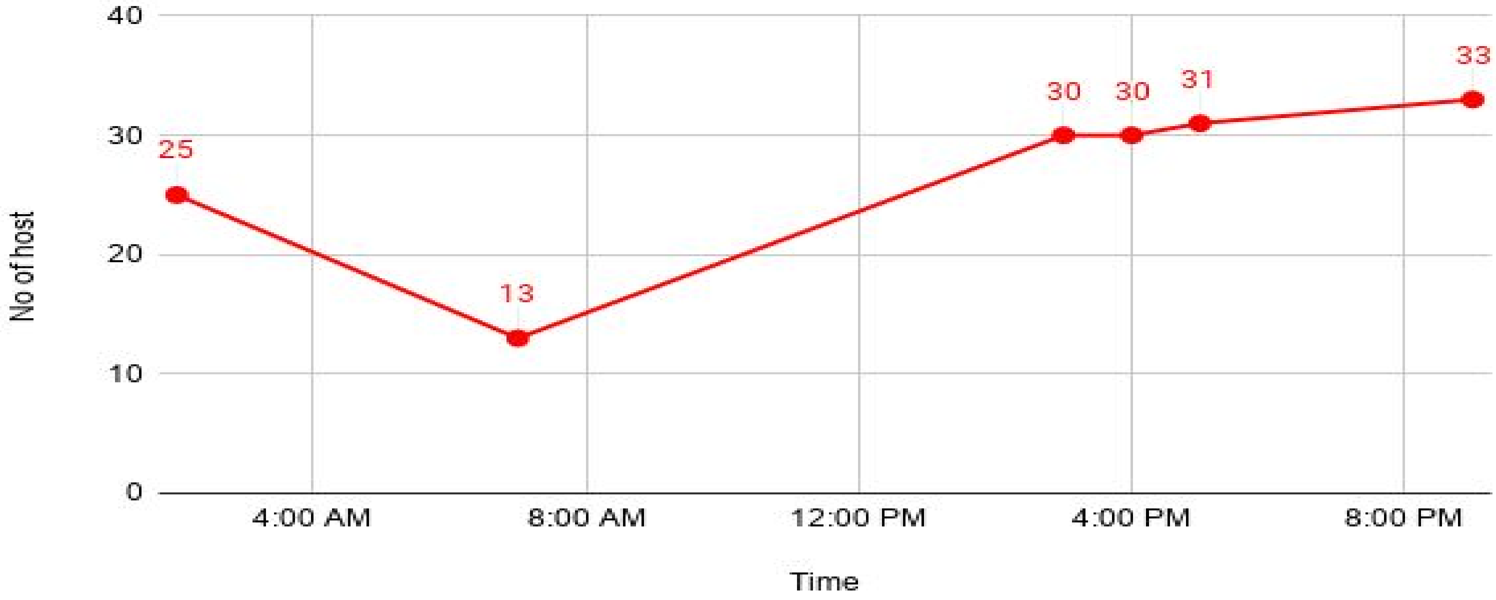
```
iit@parthapc:~$ sudo arp
[sudo] password for iit:
Address                  HWtype  HWaddress           Flags Mask            Iface
_gateway                 ether   ec:44:76:74:60:43   C                     enp4s0
iit@parthapc:~$ sudo arp -s 10.19.4.20 ec:44:76:74:60:40
iit@parthapc:~$ sudo arp -s 10.19.4.23 cc:44:76:74:60:40
iit@parthapc:~$ sudo arp -s 10.19.4.13 cc:44:76:74:60:40
iit@parthapc:~$ sudo arp -s 10.19.4.13 cc:44:76:75:60:40
iit@parthapc:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.19.4.13               ether   cc:44:76:75:60:40   CM                    enp4s0
10.19.4.23               ether   cc:44:76:74:60:40   CM                    enp4s0
10.19.4.20               ether   ec:44:76:74:60:40   CM                    enp4s0
_gateway                 ether   ec:44:76:74:60:43   C                     enp4s0
iit@parthapc:~$ arp -s 10.19.4.200 ff:0f:0f:ff:0f:ff
SIOCSARP: Operation not permitted
iit@parthapc:~$ sudo arp -s 10.19.4.200 ff:0f:0f:ff:0f:ff
iit@parthapc:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.19.4.13               ether   cc:44:76:75:60:40   CM                    enp4s0
10.19.4.200              ether   ff:0f:0f:ff:0f:ff   CM                    enp4s0
10.19.4.23               ether   cc:44:76:74:60:40   CM                    enp4s0
10.19.4.20               ether   ec:44:76:74:60:40   CM                    enp4s0
_gateway                 ether   ec:44:76:74:60:43   C                     enp4s0
iit@parthapc:~$ sudo arp -d 10.19.4.200
iit@parthapc:~$ sudo arp -d 10.19.4.13
iit@parthapc:~$ sudo arp -d 10.19.4.23
iit@parthapc:~$ sudo arp -d 10.19.4.20
iit@parthapc:~$ |
```

d)

Question8

nmap -n -sP 10.19.7.1/22

No of host vs. Time


No of host
4:00 AM
8:00 AM
12:00 PM
4:00 PM
8:00 PM
Time