CS 342 Assignment

Name : **Naman Goyal**
Roll No : **180123029**
Branch : **Mathematics and Computing**

Q.1)

(a) To specify no. of echo requests Option ‘**-c**’ command is been send with ping command.

(b) To set time interval between 2 consecutive ping request Option ‘**-i**’ command is used.

(c) Options ‘**-l**’ or ‘**-f**’ can be used to send ECHO_REQUESTS packets to the destination one after another without waiting for the reply.

(d) Option ‘**-s**’ can be used to set the ECHO_REQUEST packet size in bytes. There is an addition of ICMP header = 8 bytes and IP headers = 20 bytes with the packet also.

So when the packet size is set to 32 bytes, the total packet size would become 32+8+20 = **60 bytes**.

Q.2)

(a) Avg RTT’s :

-> Six of the hosts chosen are Myntra.com, Google.com, Amazon.in, Apple.com, Oracle.com, Samsung.com.

-> Packet losses and Avg RTT observed are given in the below table:

Host Address	**IP Address**	**Location**	**Avg. RTT 1 (ms) at 9 am**	**Avg. RTT 2 (ms) at 3 pm**	**Avg. RTT 3 (ms) at 7 pm**	**Total Avg. (ms)**
Myntra.com	195.95.193.54	USA	78.566 (0%)	83.705 (0%)	85.985 (0%)	73.752
Google.com	64.233.177.113	Atlanta	38.269 (0%)	35.115 (0%)	46.879 (0%)	40.087
Amazon.in	52.95.120.67	Ireland	97.482 (0%)	102.383 (0%)	98.128 (0%)	99.331
Apple.com	17.172.224.47	USA	89.112 (12%)	75.289 (10%)	98.121 (10%)	87.508
Oracle.com	137.254.120.50	USA	47.565 (0%)	54.272 (0%)	58.458 (0%)	53.431
Samsung.com	211.45.27.231	South Korea	98.731 (10%)	103.225 (8%)	127.543 (10%)	109.833

Generally we can see that server close to the client device faces a relatively lower latency as compared to far away ones and similarly we have in the above ones in the table. But we have seen that RTT’s are weakly correltaed to the geographical location factor because packet switching between two locals is very significant.

(b) Packet loss variations :

Yes, we can observe more than 0% packet losses in the case of Apple.com and Samsung.com. One of the reasons may be lost of the packet in between the client and the server. Also might be there is some difference in the rates of processing and receiving of the packets which leads to packet losses. There can be another reasons also like Link Congestion in which the data packet failed to rech their final destination.

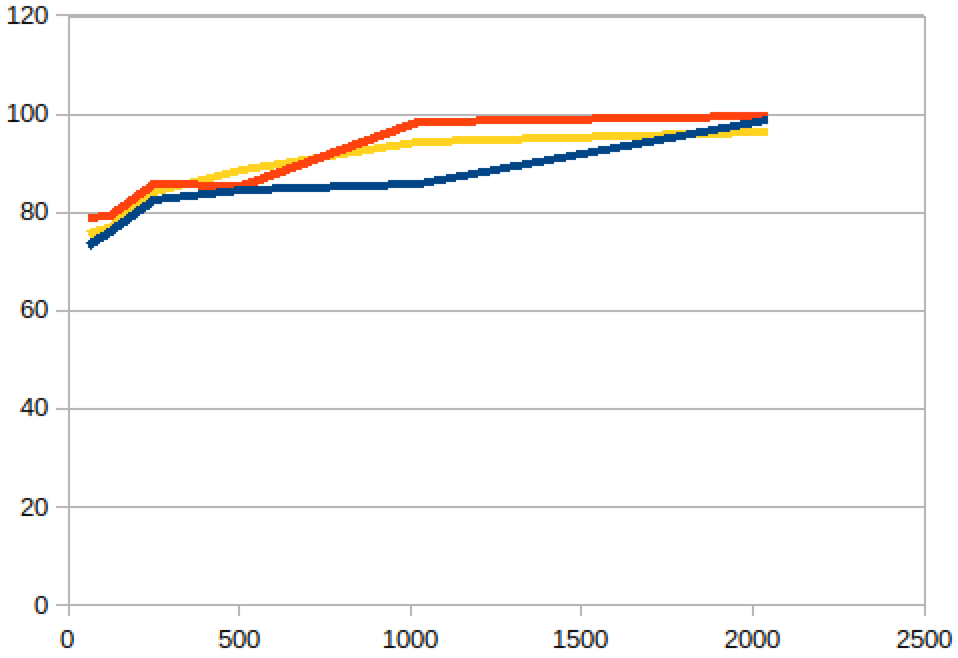
(c) Time of delay :

During some hours of the day the ping will be more because the ISP can handle only a constant number of requests per second. So the different sizes will have difference in ping values.

Size	**64**	**128**	**256**	**512**	**1024**	**2048**
Avg. RTT 1	73.132	75.711	82.448	84.264	98.685	83.765
Avg. RTT 2	78.541	79.125	85.549	85.222	98.127	99.487
Avg. RTT 3	75.201	76.655	84.027	88.215	94.213	96.233

(d) Size of packets :

As the packet size increases, the expected one is that latency will also increase and we find that the above statement in the above table as well. We have different transmission unit in case of sizes of packets that is when the size is below 1500 bytes they will be transmitted in a single frame and above 1500 they will be transmitted in multiple frames.

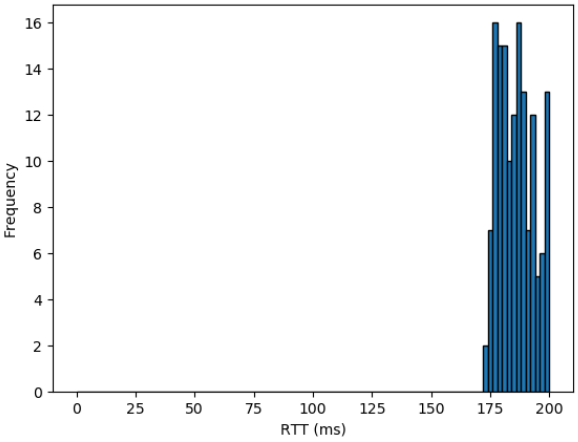


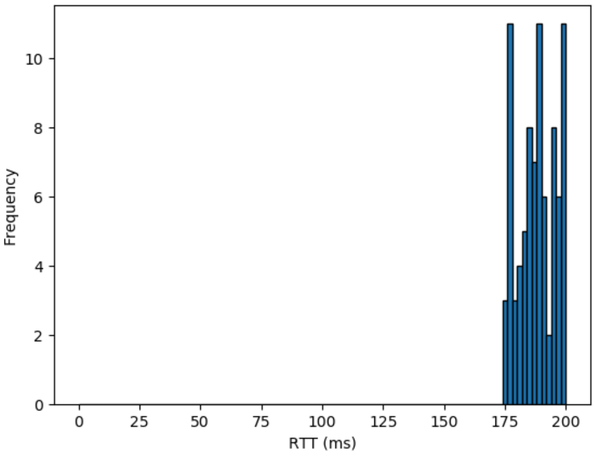
Q.3) Scenarios of Pings :

Linux Terminal Command	Packets Sent	Packets Receive d	Packet Loss (%)	Minimum Latency	Maximum Latency	Mean Latency	Average Latency
Ping -n -c1000 -i0.2 52.95.154.0	1000	996	0.4	0.181 ms	0.302 ms	0.202 ms	0.241
Ping -p ff00 -c1000 -i0.2 52.95.154.0	1000	984	1.6	0.204 ms	0.382 ms	0.258 ms	0.293 ms

-> The two cases were very having the same obejctive but the difference lies in the functionality that is "-n" symbolizes that no attempt will be made to lookup for host addresses, that making it little faster than a normal ping. That's we can even observe in the above table that 1st case is having a lesser latency than that of 2nd case. "-p" is used to pad bytes to fill out the packets with are been used further of retreiving data problems in the network. For eg "-p ff00" with pad the data with 1111111100000000. Problems are with the time then hence causing more latency and as we have seen in the table it is more in the second case one, that leads a little higher percentage loss in packets

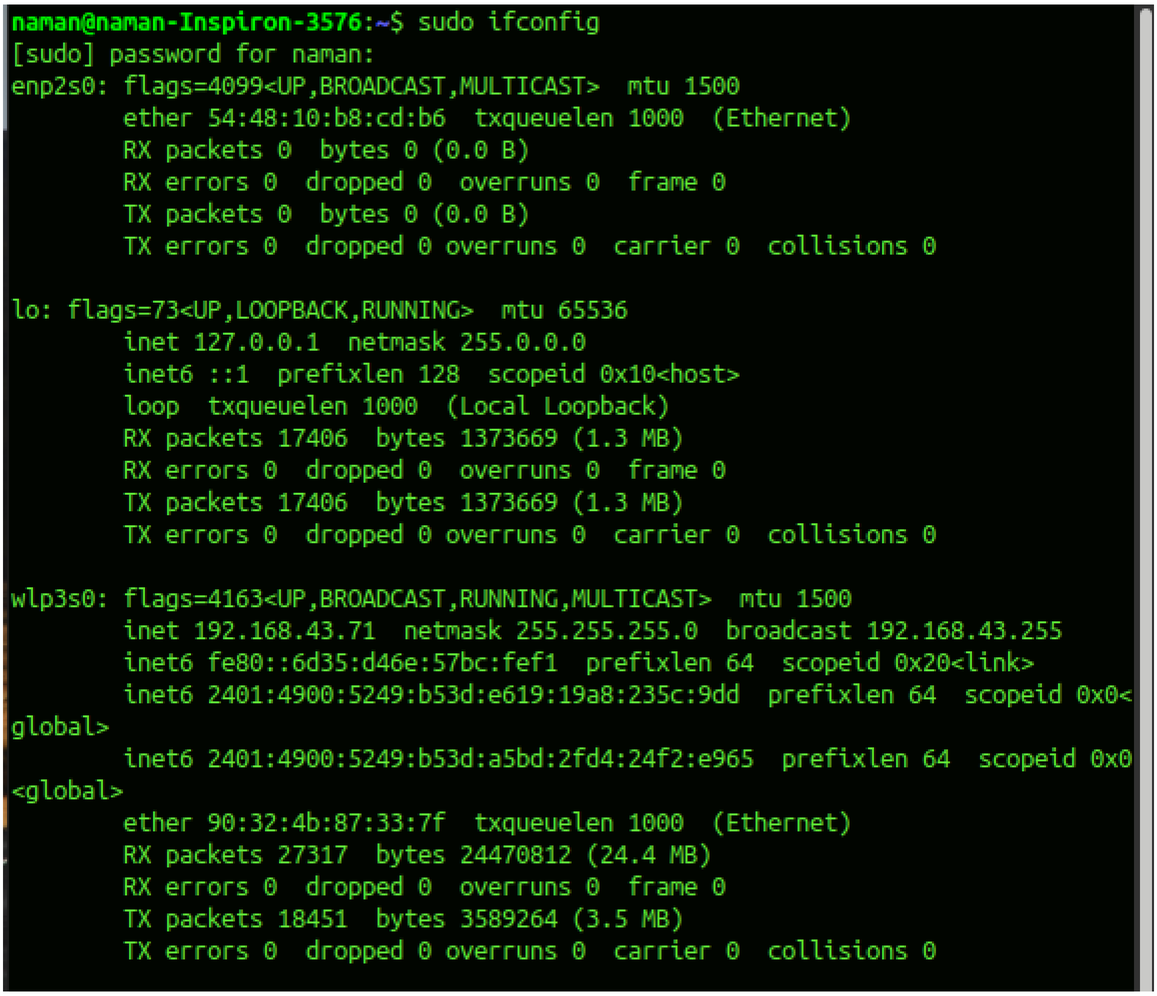
Graph I: ping -n -c1000 -i0.2 52.95.154.0
Graph II : ping -p ff00 -c1000 -i0.2 52.95.154.0





Q.4)

The command '**ifconfig**' shows details of the network interfaces that are up and running in the computer.



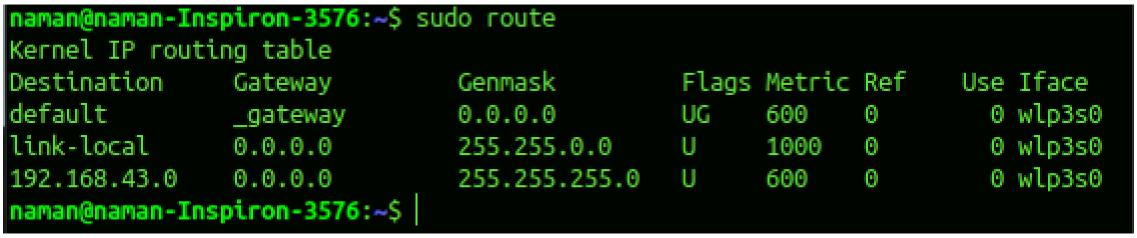
```
naman@naman-Inspiron-3576:~$ sudo ifconfig
[sudo] password for naman:
enp2s0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 54:48:10:b8:cd:b6  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

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 17406  bytes 1373669 (1.3 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 17406  bytes 1373669 (1.3 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp3s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.43.71  netmask 255.255.255.0  broadcast 192.168.43.255
        inet6 fe80::6d35:d46e:57bc:fef1  prefixlen 64  scopeid 0x20<link>
        inet6 2401:4900:5249:b53d:e619:19a8:235c:9dd  prefixlen 64  scopeid 0x0<
global>
        inet6 2401:4900:5249:b53d:a5bd:2fd4:24f2:e965  prefixlen 64  scopeid 0x0
<global>
        ether 90:32:4b:87:33:7f  txqueuelen 1000  (Ethernet)
        RX packets 27317  bytes 24470812 (24.4 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 18451  bytes 3589264 (3.5 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

->My machine has a wireless interface and a loopback interface (lo).
->The output of the ifconfig command is as follows:
1.) Inet Addr : Indicating IPv4 and IPv6 addresses.
2.) Bcast : Networks enabled broadcast addresses.
3.) Mask : Network Mask required to extract network and host address from IP address.
4.) UP : Indicator to show that kernel modules related to Ethernet interface has been loaded.
5.) BroadCast : Denoting that broadcasting is been supported.
6.) Running : Data can be accepted.
7.) MultiCast : Denoting that multicasting is been supported.
8.) NoTrailers : Indicator that trailer encapsulation is disbaled.
9.) MTU : Denoting the size of each packet received by Ethernet card. Default value 1500/
10.) RX/TX Packets : Total number of packets received and transmitted.
11.) Collisions : Number of packets colliding due to network congestion.
12.) Txqueuelen : Length of transmit queue of the device.
13.) RX/TX Bytes : Total amount of data passed through Ethernet interface.

->Options provided with ifconfig commands :
1.) -a : Displays al interfaces available.
2.) Up : For activation.
3.) Down : For shutting down.

4.) Mtu n : Sets the Maximum Transmission Unit of an interface.
5.) Address : IP address assigned to interface.

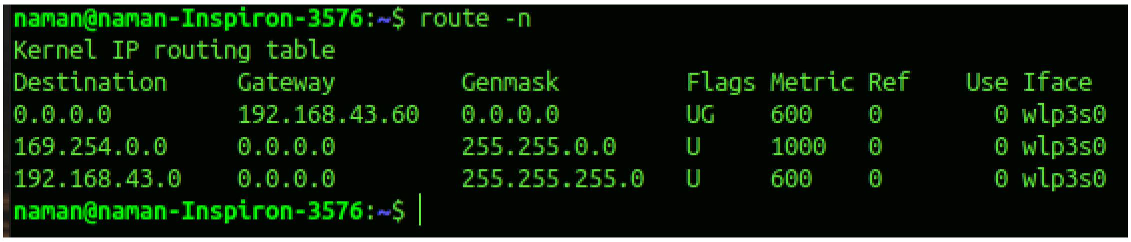
->The command '**route**' shows the routing table of the device.



```
naman@naman-Inspiron-3576:~$ sudo route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    600    0        0 wlp3s0
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 wlp3s0
192.168.43.0    0.0.0.0         255.255.255.0   U     600    0        0 wlp3s0
naman@naman-Inspiron-3576:~$ 
```

->My computer has 3 wireless networks connected to it.

->The output of the route commands are :
1.) Destination : destination host.
2.) Gateway : It is the gateway address.
3.) Genmask : Netmask for the destination net.
4.) Flags : U is for route up and G for using gateway.
5.) Metric : Distance to the target.
6.) Ref : Number of refernces to this route.
7.) Use : Lookups count for the route.
8.) Iface : Interface to which packets for this roue will be sent.

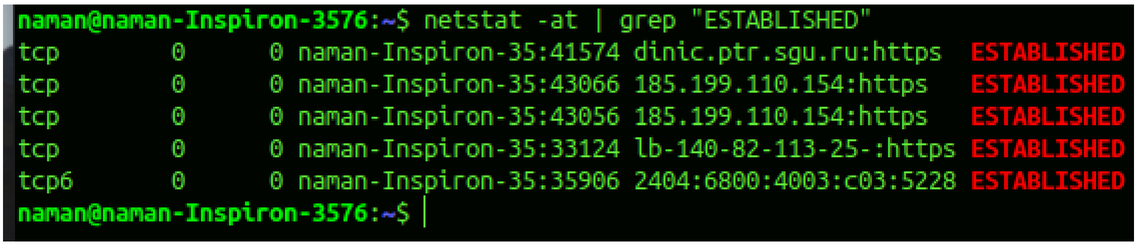


```
naman@naman-Inspiron-3576:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.43.60   0.0.0.0         UG    600    0        0 wlp3s0
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 wlp3s0
192.168.43.0    0.0.0.0         255.255.255.0   U     600    0        0 wlp3s0
naman@naman-Inspiron-3576:~$ 
```

-> Options provideed with route command :
1.) Del : Delete a route.
2.) Add : Add a route.
3.) Target : Destination Target.
4.) -net : Target is a new network.
5.) -host : Target is the host.

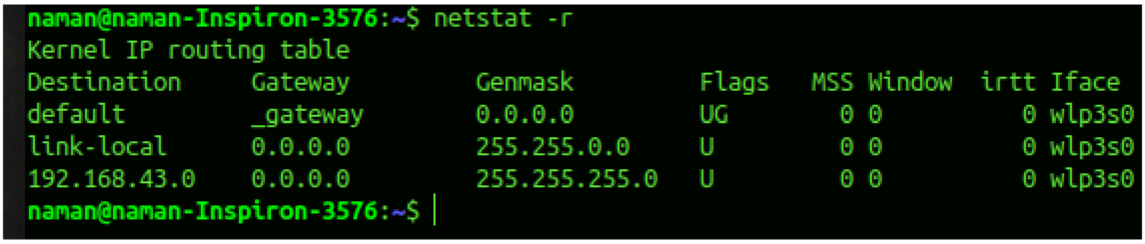
Q.5)

->'**Netstat**' or netwok statistics is a command-line tool for monitoring newtork connections which are incoming as well as outgoing.
-> Basic network debugging tool which gives information about ports and their connections.



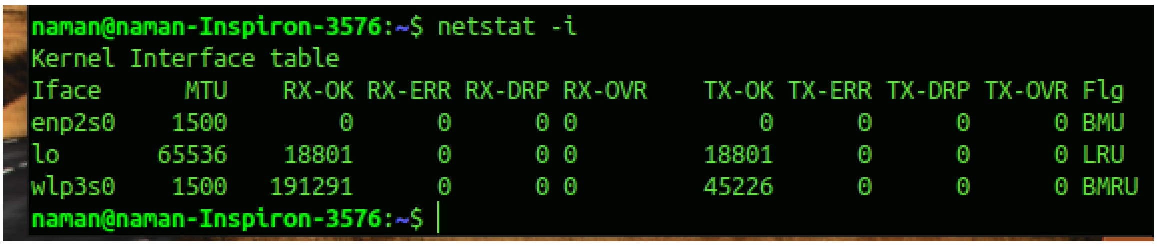
```
naman@naman-Inspiron-3576:~$ netstat -at | grep "ESTABLISHED"
tcp        0      0 naman-Inspiron-35:41574 dinic.ptr.sgu.ru:https  ESTABLISHED
tcp        0      0 naman-Inspiron-35:43066 185.199.110.154:https   ESTABLISHED
tcp        0      0 naman-Inspiron-35:43056 185.199.110.154:https   ESTABLISHED
tcp        0      0 naman-Inspiron-35:33124 lb-140-82-113-25-:https ESTABLISHED
tcp6       0      0 naman-Inspiron-35:35906 2404:6800:4003:c03:5228 ESTABLISHED
naman@naman-Inspiron-3576:~$ |
```

-> The above command ‘**netstat -at**’ is used to show all TCP established connections.
It has some components:
1.) Proto : Tells whether the socket is TCP or UDP.
2.) Local and Foreign Address : Hosts that the sockets are connected to. Local end tells about the computer on which netstat is running and foreign is about the other end of the connection.
3.) Recv-Q and Send-Q : Tells about the remaining data left in queue that has to processed or you can say receive or send to the destination.
4.) State : Tells the current state of the listed sockets.



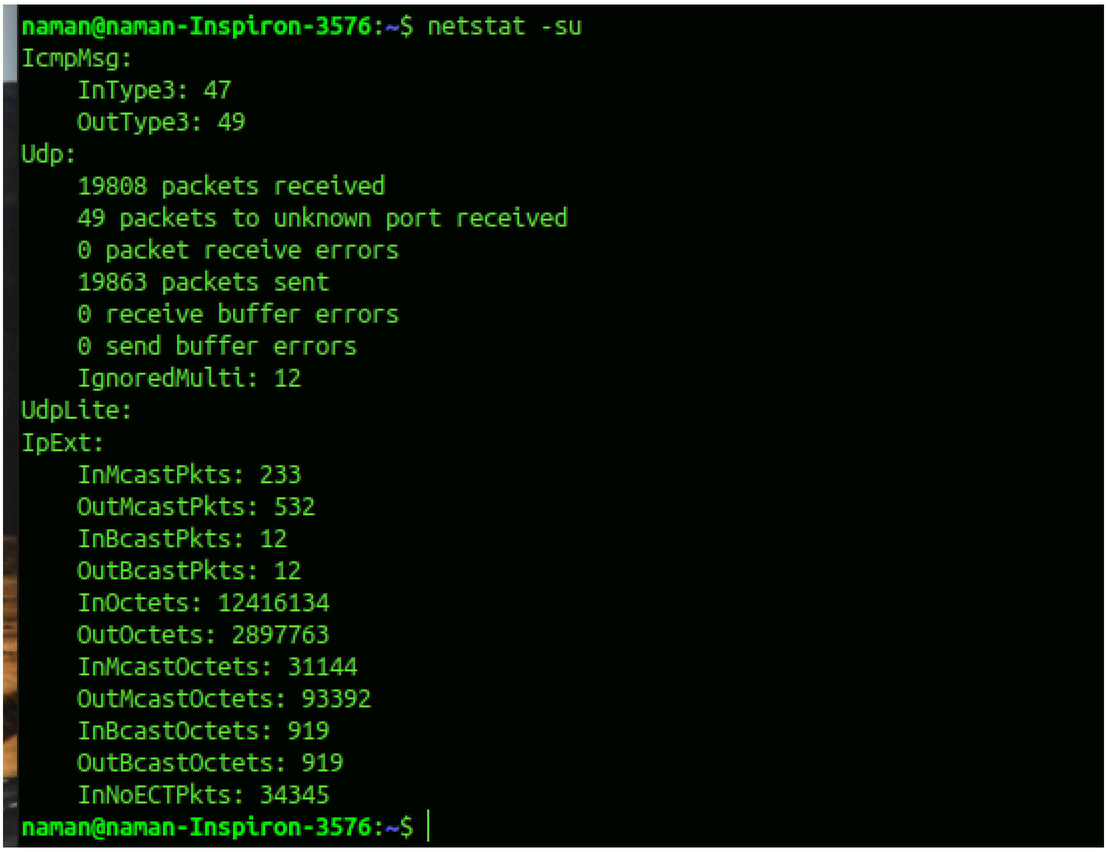
```
naman@naman-Inspiron-3576:~$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         _gateway        0.0.0.0         UG        0 0          0 wlp3s0
link-local      0.0.0.0         255.255.0.0     U         0 0          0 wlp3s0
192.168.43.0    0.0.0.0         255.255.255.0   U         0 0          0 wlp3s0
naman@naman-Inspiron-3576:~$ |
```

->The above command ‘**netstat -r**’ is used to display the kernel routing table.
-> Similar output to ‘route’ command.
->Desciption of the components:
1.) MSS : list the values of Maximum Segment Size. TCP parameter and used to split packets.
2.) WINDOW : Shows the window size that means the no of TCP packets which can be sent before atleast one of them can be allowed.
3) IRTT : Initail Round Trip time.



```
naman@naman-Inspiron-3576:~$ netstat -i
Kernel Interface table
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
enp2s0    1500        0      0      0 0             0      0      0      0 BMU
lo       65536    18801      0      0 0         18801      0      0      0 LRU
wlp3s0    1500   191291      0      0 0         45226      0      0      0 BMRU
naman@naman-Inspiron-3576:~$ |
```

-> The above command ‘**netstat -i**’ is used to display the status of all network interfaces.
For example the above fig shows 3 interfaces.



```
naman@naman-Inspiron-3576:~$ netstat -su
IcmpMsg:
    InType3: 47
    OutType3: 49
Udp:
    19808 packets received
    49 packets to unknown port received
    0 packet receive errors
    19863 packets sent
    0 receive buffer errors
    0 send buffer errors
    IgnoredMulti: 12
UdpLite:
IpExt:
    InMcastPkts: 233
    OutMcastPkts: 532
    InBcastPkts: 12
    OutBcastPkts: 12
    InOctets: 12416134
    OutOctets: 2897763
    InMcastOctets: 31144
    OutMcastOctets: 93392
    InBcastOctets: 919
    OutBcastOctets: 919
    InNoECTPkts: 34345
naman@naman-Inspiron-3576:~$ 
```

-> The above command '**netstat -su**' is used to show the statistics of all UDP connections.

(f) Loopback Interface :

-> Virtual Interface.
-> It kind of a loop only where the packets are been returned which are sent to it.
->It is require to put a default route on a network interface as well.
-> Following functions are mainly performed:

-> **Device Identification :** Used to identify a device. There can be many ways but this method is being preferred.

-> **Routing Information :** It's address is being used ny protocols such as OSPF to determine protocal specific properties and it's a backbone for some commmands suchas ping mpls.

Q.6)

<u>Traceroute Experiment</u> :

-> This six hosts used are similar to used in Q2.

Day Time	Myntra.com	Google.com	Amazon.in	Apple.com	Oracle.com	Samsung.com
11 AM	15	5	29	10	13	17
3 PM	15	4	28	10	14	17
7 PM	16	4	29	5	3 (Incomplete)	19

(a)
-> A traceroute is a network tool used to show the route taken by packets across an IP network. It will show each hop sequentially, and total hops required.

(b)
-> The most common hops found are the IP Address : 164.51.192.1 and 180.178.193.21. These can be considered to be uptrends websites. Hops are common because that routes to these destinations pass through the same internet circles and hence they may overlap.

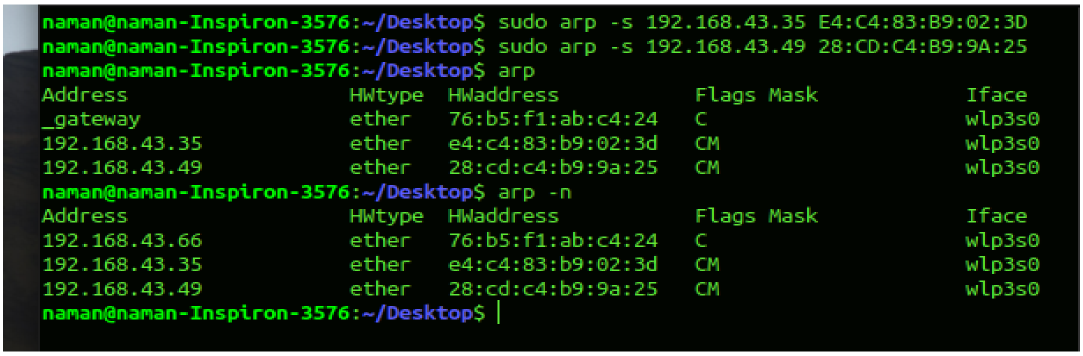
(c)
-> For the same company, it’s not guarranted that they are on same network and hence different pings and routes are been observed. They take path with the lowest traffic using load balancing.

(d)
->We can see from the above table that traceroute was unable to reach Oracle.com at 7pm because may be the servers be loaded to block ICMP/ ping for security reasons as it can lead to websites attacks as well such DDOS attack or kind of SQL injection. Many networks providers disbale ICMP traffic if their network is under very high load that it can handle.

(e)
-> Yes, it’s possible.There’s a ICMP segment between the source and destination by the ping, that traverses networks that expects ICMP reply from host. Server may be blocking the reply. Traceroute works by targeting the final hop, but limiting the TTL and waiting for the message for the TLE , increasing by one on next iteration. Thus ICMP reply was given to ICMP request, that’s why giving a Time limit exceeded message.

Q.7)
(a) :
-> ARP is the Address Resolution Protocol and it is required to match MAC Address to IP Address and vice-versa.
-> Command : arp

-> We have the following components related to it:
1.) Address : Cuurently connected IP address.
2.) Flags : M represents permanent entries and P represents published entries. Complete entry is been marked with C flag.
3.) HWType : MAC Address. Gives the value of the type of hardware used for local network transmission.
4.) Iface : Interface to which mapped address is mapped.
(b)
->Command to add the entry is ‘**sudo arp -s ip_address HWaddress**’ and to delete an entry is ‘**sudo arp -d ip_address**’.

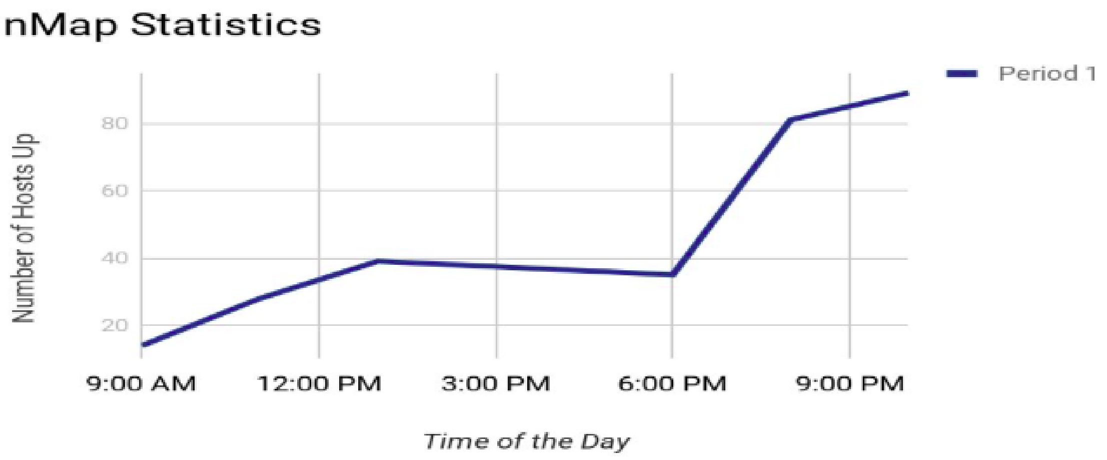


```
naman@naman-Inspiron-3576:~/Desktop$ sudo arp -s 192.168.43.35 E4:C4:83:B9:02:3D
naman@naman-Inspiron-3576:~/Desktop$ sudo arp -s 192.168.43.49 28:CD:C4:B9:9A:25
naman@naman-Inspiron-3576:~/Desktop$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
_gateway                 ether   76:b5:f1:ab:c4:24   C                     wlp3s0
192.168.43.35            ether   e4:c4:83:b9:02:3d   CM                    wlp3s0
192.168.43.49            ether   28:cd:c4:b9:9a:25   CM                    wlp3s0
naman@naman-Inspiron-3576:~/Desktop$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.43.66            ether   76:b5:f1:ab:c4:24   C                     wlp3s0
192.168.43.35            ether   e4:c4:83:b9:02:3d   CM                    wlp3s0
192.168.43.49            ether   28:cd:c4:b9:9a:25   CM                    wlp3s0
naman@naman-Inspiron-3576:~/Desktop$ |
```

(c)
->The time limit is set for ARP tables values that is 60 seconds stored in /proc / sys/ net/ ipv4 / neigh/ default/ gc_state_time.
-> Therefore a trial and error method is been used to add a temporary entry in the table. The time after which it’s deleted is the required cache timeout. One can use binary search also.
-> They temporary entry added is been checked after some fixed intervals of time.

(d)
->There may case when some router or a gateway are connected to 2 ot more subnet ranges that is maps to same Ethernet Address. When same subnet ranges are been addressed they are being directed using MAC Address. ARP Table is referred to convert those IP Addresses to the corresponding MAC address and packets are being delivered to the request. The router then continues with the requested packets.

Q.8)
-> **Nmap** or Network Mapper is used in network exploration and security auditing.
-> Rapidly scan large networks, working fine against single hosts.
-> ‘**nmap -sA 192.168.0.1**’ is the command used to detect the firewall settings.
-> The command used to scan my LAN network is ‘**nmap -sP 192.168.100.0/24**’. I run this command in my Local Network and found that no of users increases around 12pm and dip is been observed around 6 PM because children here go to play out. Their is a high increase at 9-10 pm beacuse many people are free at the time and work with their devices such as laptops.


nMap Statistics
Period 1
Number of Hosts Up
9:00 AM
12:00 PM
3:00 PM
6:00 PM
9:00 PM
Time of the Day