CS342 : ASSIGNMENT 1

NAME : NAYANIKA GHOSH
ROLL : 200123036

1.a. The option required to specify the number of echo requests to send with ping command is **-c**. For example, ping -c 6 google.com

1.b. The option required to set time interval (in seconds), rather than the default one second interval, between two successive ping ECHO_REQUESTs is **-i**. For example,
ping -i 5 127.0.0.1

1.c. i) The command to send ECHO_REQUEST packets to the destination one after   another

without waiting for a reply is **-l**. For example, ping -l preload <destination>

ii) The limit for sending such ECHO_REQUEST packets by
normal users (not superuser) is 3.

1.d. i) The command to set the ECHO_REQUEST packet size (in bytes) is **-s**.

ii) If the PacketSize is set to 32 bytes, the total packet size is 60 bytes for IPv4 header(due to 8 bytes of ICMP header and 20 bytes of IP header).

2.

Host Name	Time of Day	Average RTT	Packet Loss	Location	Distance
Whatsapp	1.12 am	124.464 ms	0%	California,USA	12,285 km
Whatsapp	2.58 pm	162.510 ms	4%	California,USA	12,285 km
Whatsapp	8:52 pm	123.600	0%	California,USA	12,285 km
Microsoft Teams	1.24 am	194.260 ms	0%	Redmond,USA	11,126 km
Microsoft Teams	3.01 pm	140.878 ms	0%	Redmond,USA	11,126 km
Microsoft Teams	8:53 pm	236.072 ms	4%	Redmond,USA	11,126 km
Outlook	1.25 am	173.953 ms	0%	Redmond,USA	11,126 km
Outlook	3.10 pm	116.470 ms	0%	Redmond,USA	11,126 km
Outlook	8:54 pm	149.444 ms	0%	Redmond,USA	11,126 km
Amazon Prime Video	1.30 am	113.919 ms	0%	Seattle,USA	11,124 km
Amazon Prime Video	3.13 pm	136.515 ms	0%	Seattle,USA	11,124 km
Amazon Prime Video	8:55 pm	108.796 ms	0%	Seattle,USA	11,124 km
Twitter	1.35 am	199.461 ms	0%	San Francisco,USA	12,054 km
Twitter	3.22 pm	131.558 ms	0%	San Francisco,USA	12,054 km
Twitter	8:58 pm	183.446 ms	4%	San Francisco,USA	12,054 km
Gmail	1.36 pm	125.389 ms	0%	California,USA	12,285 km

Gmail	.30 pm	150.649 ms	0%	California,USA	12,285 km
Gmail	8:59 pm	129.595 ms	4%	California,USA	12,285 km

Packet loss of more than 0% was observed due to heavy network traffic.Some packets might have been lost or got dropped due to packet collision.

There is **weak correlation** between ping latency and geographical distance as observed.

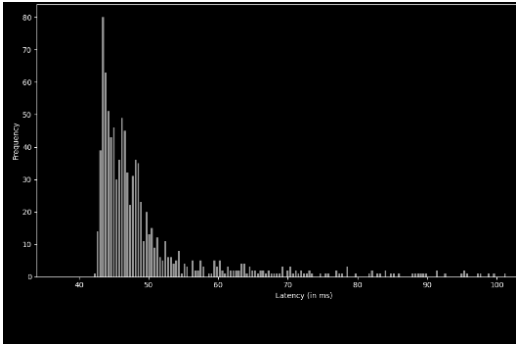**Host chosen for pinging with different data size packets: - *Gmail***

PING LATENCY VS SIZE PACKETS
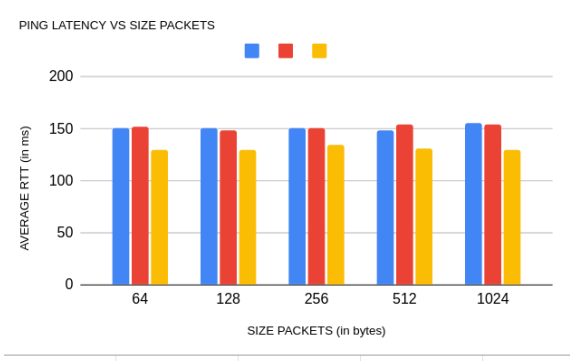
3.a) The IP address chosen is 104.44.11.4.

The packet loss for the command **ping -c 1000 -n 104.44.11.4** is 1.1% and that for the command **ping -c 1000 -p ff00 104.44.11.4** is 3.8%.
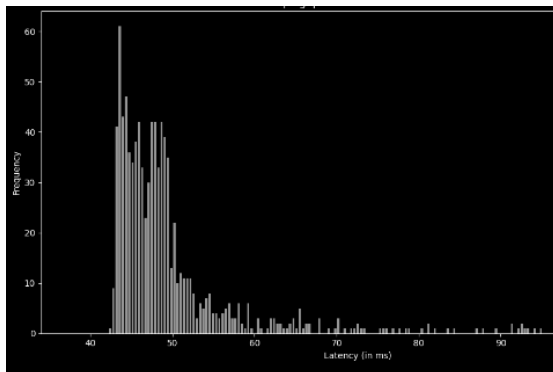
b)

Latency	ping -c 1000 -n 104.44.11.4	ping -c 1000 -p ff00 104.44.11.4
Minimum	42.4 ms	42.5 ms
Maximum	820 ms	821 ms
Mean	57.61 ms	58.04 ms
Median	46.7ms	47.7 ms

c) Graphs of PING LATENCY vs FREQUENCY :-

i) For ping -c 1000 -n 104.44.11.4 :-

ii) For ping -c 1000 -p ff00 104.44.11.4 :-

d) If we use the ping with -p flag, the statistical quantities are more than those in case of -n flag.When -n flag is used, no DNS resolution occurs. So, the mean latency is lower in the case of -n flag.

4. a)

There are 3 network interfaces on my machine :- **enp3s0**, **lo** and **wlp0s20f3**.

b) The following options can be provided with the ifconfig command :-

  i) **-a** :- It shows all the available interfaces.

  ii) **-s** :- It shows a brief list,not in detail.

  iii) **-v** :- It runs the command in verbose mode.

  iv) **[-]arp** :- It controls the use of ARP protocol on an interface.

c)

The following fields are shown in the output :-

 i) **Destination** :- It specifies the destination network.

 ii) **Gateway** :- It defines the gateway for the mentioned network.

 iii) **Genmask** :- It shows the netmask on the network.

iv) **Flags** :-The U flag shows that the route is up.The G flag shows that the route is to the gateway.

v) **Metric** :- It is the distance to target.

vi) **Ref** :- It is the number of references to the route.

vii) **Iface** :- It gives the network interface name.

d) The following options can be provided with the route command :-

i) **-n** :- It shows the routing table in numeric form.

ii) **-Cn** :- It shows the kernel's routing cache information.

iii) **-ee** :- It shows all the parameters from the routing line.

iv) **-e** :- It makes the route command use netstat format to show the routing table.

```
nayanika@nayanika-Inspiron-3501:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.150.32.1     0.0.0.0         UG    600    0        0 wlp0s20f3
10.150.32.0     0.0.0.0         255.255.240.0   U     600    0        0 wlp0s20f3
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 wlp0s20f3
nayanika@nayanika-Inspiron-3501:~$ route -Cn
Kernel IP routing cache
Source          Destination     Gateway         Flags Metric Ref    Use Iface
nayanika@nayanika-Inspiron-3501:~$ route -ee
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface    MSS   Window irtt
default         _gateway        0.0.0.0         UG    600    0        0 wlp0s2   0     0      0
10.150.32.0     0.0.0.0         255.255.240.0   U     600    0        0 wlp0s2   0     0      0
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 wlp0s2   0     0      0
nayanika@nayanika-Inspiron-3501:~$ route -e
Kernel IP routing table
Destination     Gateway         Genmask         Flags  MSS Window  irtt Iface
default         _gateway        0.0.0.0         UG       0 0          0 wlp0s20f3
10.150.32.0     0.0.0.0         255.255.240.0   U        0 0          0 wlp0s20f3
link-local      0.0.0.0         255.255.0.0     U        0 0          0 wlp0s20f3
nayanika@nayanika-Inspiron-3501:~$
```

5. a) The **netstat** command is a networking tool used for troubleshooting and configuration and as a monitoring tool for connections over the network. It is used for incoming and outgoing connections, routing tables, port listening, and usage statistics.

b) To show all the established TCP connections,run the following command:- **netstat -at**

The following fields are shown in the output :-

i) Proto :- It mentions the protocol used by the socket(tcp/udp/raw).

ii) Recv-Q :- It gives the count of bytes not copied by the user program connected to this socket.

iii) Send-Q :- It gives the count of bytes not acknowledged by the remote host.

iv) Local Address :- It gives the address and port number of the local socket.

v) Foreign Address :- It gives the address and port number of the remote socket.

vi) State :- It specifies the state of the socket.

```
nayanika@nayanika-Inspiron-3501:~$ 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 nayanika-Inspiron:54470 69.174.120.105:https    ESTABLISHED
tcp        0      0 nayanika-Inspiron:52982 ec2-52-20-174-233:https ESTABLISHED
tcp        0      0 nayanika-Inspiron:57464 ec2-52-16-236-137:https ESTABLISHED
tcp        0      0 nayanika-Inspiron:60066 151.139.105.12:https    TIME_WAIT
tcp        0      0 nayanika-Inspiron:41120 8.159.244.35.bc.g:https ESTABLISHED
tcp        0      0 nayanika-Inspiron:59908 23.106.127.35:https     ESTABLISHED
tcp        0      0 nayanika-Inspiron:40920 123.208.120.34.bc:https ESTABLISHED
tcp        0      0 nayanika-Inspiron:52870 103.231.98.193:https    ESTABLISHED
tcp        0      0 nayanika-Inspiron:53036 ec2-52-36-69-167.:https ESTABLISHED
tcp        0      0 nayanika-Inspiron:40128 server-52-84-12-5:https TIME_WAIT
tcp        0      0 nayanika-Inspiron:56048 ec2-52-0-137-185.:https ESTABLISHED
tcp        0      0 nayanika-Inspiron:45136 ec2-54-179-182-81:https ESTABLISHED
tcp        0      0 nayanika-Inspiron:57508 72.251.249.14:https     ESTABLISHED
tcp        0      0 nayanika-Inspiron:44744 117.18.237.29:http      ESTABLISHED
tcp        0      0 nayanika-Inspiron:51760 server-65-8-72-71:https TIME_WAIT
tcp        0      0 nayanika-Inspiron:57464 69.173.158.65:https     TIME_WAIT
tcp        0      0 nayanika-Inspiron:41524 _gateway:domain         ESTABLISHED
tcp        0      0 nayanika-Inspiron:46242 maa05s06-in-f2.1e:https TIME_WAIT
tcp        0      0 nayanika-Inspiron:33482 104.18.18.126:https     ESTABLISHED
tcp        0      0 nayanika-Inspiron:57462 ec2-52-16-236-137:https TIME_WAIT
tcp        0      0 nayanika-Inspiron:54472 69.174.120.105:https    ESTABLISHED
tcp        0      0 nayanika-Inspiron:47276 srv-us-ca-14.buys:https ESTABLISHED
tcp        0      0 nayanika-Inspiron:47934 maa03s28-in-f14.1:https ESTABLISHED
tcp        0      0 nayanika-Inspiron:36476 maa03s31-in-f14.1:https ESTABLISHED
tcp        0      0 nayanika-Inspiron:57468 69.173.158.65:https     TIME_WAIT
tcp        0      0 nayanika-Inspiron:49774 maa05s12-in-f2.1e:https ESTABLISHED
tcp        0      0 nayanika-Inspiron:57314 162.247.241.14:https    ESTABLISHED
tcp        0      0 nayanika-Inspiron:35990 ec2-3-90-121-113.:https ESTABLISHED
tcp        0      0 nayanika-Inspiron:57466 69.173.158.65:https     TIME_WAIT
tcp6       0      0 ip6-localhost:ipp       [::]:*                  LISTEN
tcp6       0      0 nayanika-Inspiron:37584 maa03s45-in-x02.1:https ESTABLISHED
tcp6       0      0 nayanika-Inspiron:43098 maa03s34-in-x03.1e:http ESTABLISHED
tcp6       0      0 nayanika-Inspiron:40302 2602:803:c006:158:https TIME_WAIT
tcp6       0      0 nayanika-Inspiron:41568 whatsapp-cdn6-shv:https ESTABLISHED
tcp6       0      0 nayanika-Inspiron:59416 2a02:fa8:c411:11::https ESTABLISHED
tcp6       0      0 nayanika-Inspiron:52304 maa03s46-in-x02.1:https ESTABLISHED
tcp6       0      0 nayanika-Inspiron:40306 2602:803:c006:158:https TIME_WAIT
tcp6       0      0 nayanika-Inspiron:44074 maa05s21-in-x02.1:https ESTABLISHED
tcp6       0      0 nayanika-Inspiron:40304 2602:803:c006:158:https TIME_WAIT
tcp6       0      0 nayanika-Inspiron:56164 maa05s17-in-x04.1:https ESTABLISHED
tcp6       0      0 nayanika-Inspiron:59798 maa05s24-in-x0a.1:https ESTABLISHED
tcp6       0      0 nayanika-Inspiron:41724 maa05s06-in-x02.1:https ESTABLISHED
nayanika@nayanika-Inspiron-3501:~$
```

c) The command **netstat -r** shows the kernel routing information.

```
nayanika@nayanika-Inspiron-3501:~$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         _gateway        0.0.0.0         UG        0 0          0 wlp0s20f3
link-local      0.0.0.0         255.255.0.0     U         0 0          0 wlp0s20f3
192.168.43.0    0.0.0.0         255.255.255.0   U         0 0          0 wlp0s20f3
nayanika@nayanika-Inspiron-3501:~$
```

The following fields are shown in the output :-
i) Destination :- It specifies the destination network.
ii) Gateway :- It defines the gateway for the mentioned network.
iii) Genmask :- It shows the netmask on the network.
iv) Flags:-The U flag shows that the route is up.The G flag shows that the route is to a gateway.
v) MSS :- Its full form is **Maximum Segment Size.** It gives the size of the largest datagram the kernel will create for transmission through this route.
vi) Window :- It gives the maximum data the system will take in one burst of transfer from a remote host.
vii) irtt :- Its full form is **initial round trip time**. It ensures that the data is reliably transferred between hosts by retransmitting a datagram if it is lost.
vii) Iface :- It gives the network interface name.

d) The option of netstat that can be used to display the status of all the network interfaces is **-i**. There are 3 interfaces in my laptop :- **enp3s0**, **lo** and **wlp0s20f**.

```
nayanika@nayanika-Inspiron-3501:~$ netstat -i
Kernel Interface table
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
enp3s0     1500       0      0      0 0             0      0      0      0 BMU
lo        65536   50125      0      0 0         50125      0      0      0 LRU
wlp0s20f   1500  247604      0    406 0        198238      0      0      0 BMRU
nayanika@nayanika-Inspiron-3501:~$
```

e) Th option of netstat that is used to show the statistics of all UDP connections is **-su.**

```
nayanika@nayanika-Inspiron-3501:~$ netstat -su
IcmpMsg:
    InType0: 50
    InType3: 208
    InType8: 2
    OutType3: 201
    OutType8: 100
Udp:
    65361 packets received
    107 packets to unknown port received
    0 packet receive errors
    61496 packets sent
    0 receive buffer errors
    0 send buffer errors
    IgnoredMulti: 484
UdpLite:
IpExt:
    InMcastPkts: 3152
    OutMcastPkts: 253
    InBcastPkts: 488
    OutBcastPkts: 3
    InOctets: 60980602
    OutOctets: 59094699
    InMcastOctets: 560413
    OutMcastOctets: 35153
    InBcastOctets: 51171
    OutBcastOctets: 234
    InNoECTPkts: 188663
MPTcpExt:
nayanika@nayanika-Inspiron-3501:~$
```

f) The loopback interface identifies the device. Interfaces might be removed or addresses changed based on network topology changes but the loopback address never changes.

6. A **traceroute** tool is used to track the path which a packet follows from source to destination. It also displays the time taken between the intermediate routers.

a)

Time	Whatsapp	MS Teams	Outlook	Twitter	Prime Video	Gmail
3 am	30	29	30	30	28	30
4pm	30	29	30	30	28	30
9pm	30	29	30	30	28	30

The hop which are common to all the hosts is 192.168.43.1. The MS Teams and the Outlook have 104.44.66.1, 104.44.233.1 and 104.44.33.39 in common.

b) The route to the same host might change at different times of the day as the packets can be redirected to the nodes with less congestion during high traffic periods. The destination host may also use multiple servers to receive the packets.

c) traceroute uses UDP packets.If the hosts on the path block the ICMP/UDP packets,they don't respond but send data to the next hops. If a hop prints *** ,it denotes that the router at that hop can't respond to the type of packet used for traceroute.These nodes are set up to prevent DoS attacks which are generated using UDP/ICMP packets.Due to huge traffic, the nodes are disabled for receiving these packets.

d) It is possible to find the route to certain hosts which fail to respond with ping experiment as traceroute gives a wide range of protocols like ICMP echo request,TCP SYN and UDP packets but ping uses only ICMP echo requests.Traceroute searches for the ICMP Time exceeded packet and not the ICMP Reply Packet.

7. a) To show the full ARP table, we have to run the following command :- **arp -a**
There are 5 columns in the ARP table :-
  i) **Address** :- It gives the IP address of the machine.
  ii) **HWType** :- It gives the type of the Ethernet device used by the machine.
  iii) **HWaddress** :- It gives the MAC address of the network connection.
  iv) **Flags Mask:**- It states if the address is extracted manually,user-defined or incomplete.
  v) **IFace** :- It gives the network interface name.
 b) To add an entry in the arp table, run this :- **arp -s <IP_address> <MAC_address>**
To delete an entry from the arp table, run this :- **arp -d <IP_address>**
c) The command that determines how long the entries in the cache of the ARP module of the kernel remain valid and when they get deleted from the cache is **"arp timeout"**.
 Eg., **arp timeout 800.** Static entries remain in the arp table forever and are never timed out.
d) If two IP addresses map to the same Ethernet address, neither computer can communicate properly as the network becomes confused by the duplicate IP address.

8. For the LAN subnet 172.18.2.0/15

Time	2 am	3 am	4 pm	5 pm	9 pm	10 pm
No.of hosts online	27	29	37	28	27	29

NUMBER OF ACTIVE HOSTS
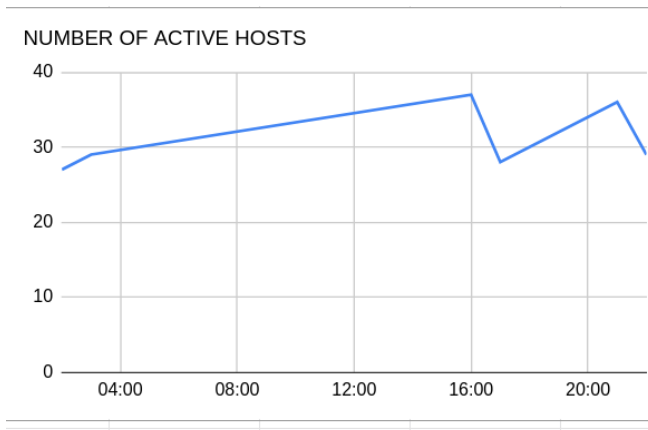
9. a) nslookup host_name
   b) nslookup IP_address
   c) nslookup -querytype=mx domain_name