CS342 Assignment :1

Question 1:

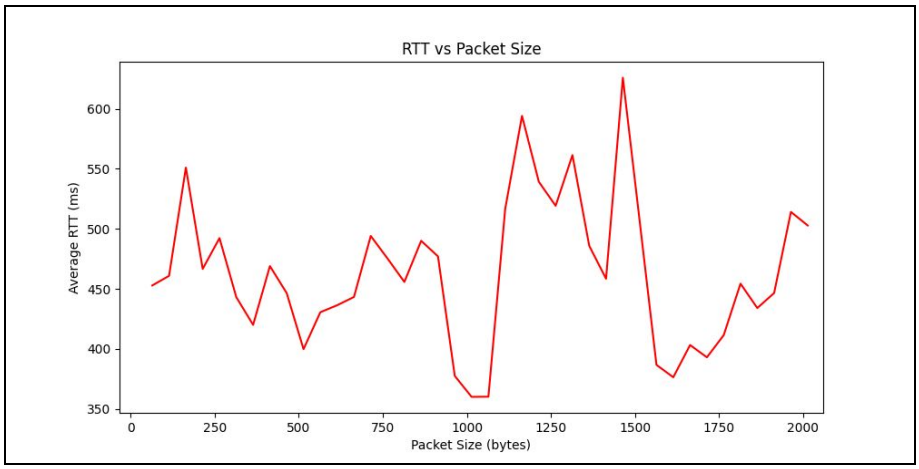
a)ping -c ***count*** **:** ping -c 7 172.16.114.174
b)ping -i ***intervaltime*** : ping -i 3 172.16.114.174
c)ping -l ***count_of_preload_packets*** : ping -l 2 172.16.114.174
A maximum of 3 echo_requests can be sent by a normal user
d)ping -s ***size_of_packet*** : tping -s 1000 172.16.114.174
Total size is specified size plus 8 bytes for ICMP header
Total size = header size + payload size

Question 2:

No.	Hosts	Average RTT			Place
		15:00 hours	19:00 hours	23:00 hours	
1	https://www.gov.sg/	1861.761 ms	88.216	81.422	Singapore(6,311.5 km)
2	www.youtube.com	102.008	101.989	95.514	Dallas,USA (13,357 km)
3	https://www.stuff.co.nz/	1755.489	219.368	660.408	New Zealand (12828 km)
4	www.geeksforgeeks.org	99.046	137.667	94.492	India
5	www.euronews.com	414.021	61.948	158.506	Lyon,Europe(6,299 km)
6	www.yahoo.co.jp	390.575	239.516	354.272	Japan (6,183 km)

No, **RTT does not have an explicit relation with geographical distance**. For instance, an IP address in Europe has less RTT than the one in Japan. RTT is only impacted by the number of routers the datagram has to go through.

b)The first host **https://www.gov.sg/**, suffered a 4% packet loss when pinged at 15:00 hours and 19:00 hours. **www.youtube.com** suffered a 4% packet loss at 19:00 hours. This loss might be caused by **errors in data transmission, typically across wireless networks, or network congestion.**
c) Host : 172.16.114.174



d)

- **RTT vs Packet Size**: Packet size does not impact RTT up until 1024 bytes because the default size of mtu(maximum transmission unit) is 1500 bytes. After 1500, the packets are broken down and transmitted in separate frames, which explains the increased RTT.
- **RTT vs Time:** RTT is impacted by the different congestion in the network at different times of the day.Late during the night when congestion is less, higher RTT was observed.

Question 3:

IP address : 174.16.114.174

a) **Packet Loss Rate :**

1)ping -n <IPAddress> : 1% packet loss

2)ping -p ff00 <IPAddress> : 0% packet loss

b) 1) ping -n <IPAddress>

Min Latency = 352 ms

Max Latency = 16028 ms

Mean Latency = 2913.414 ms

Median Latency = 1780 ms

2) ping -p ff00 <IPAddress>

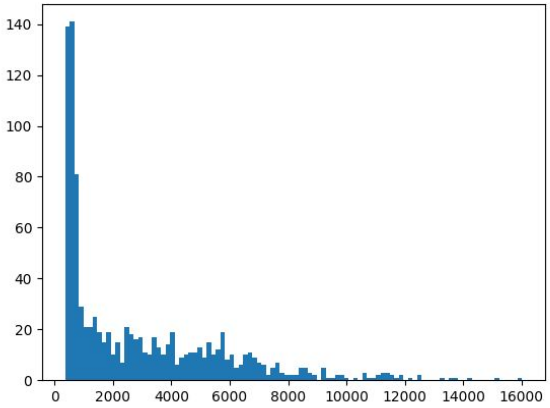
Min Latency = 87.0 ms

Max Latency = 573 ms

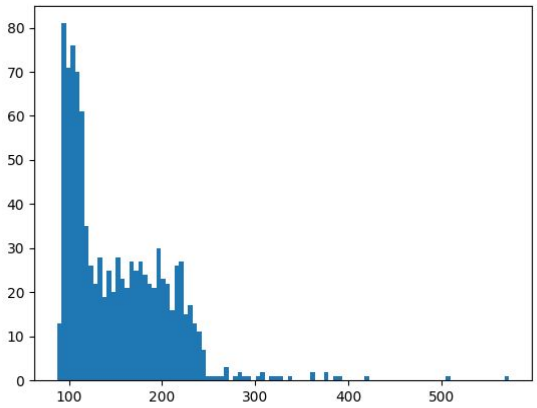
Mean Latency = 152.7779 ms

Median Latency = 140 ms

c)



Distribution for ping -n <IPAddress>



Distribution for ping -p ff00 <IPAddress>

d)

- ➔ The latency distribution of the commands is normal.
- ➔ The first command has higher mean and lower variance when compared to ping -p ff00.

Question 4 :

a) **ifconfig command :** This command is used to configure system's kernel-resident network interfaces and displays related statistics

eno1 : The network interface representing Ethernet connection

Lo: A virtual network device called as the loopback interface used for debugging locally

Output Explanation :

As shown in the above output, the active network interfaces in my system are eno1(ethernet), lo(localhost), and wlo1(wi-fi).

- ➔ **UP**: UP represents that the network interface is configured to be enabled
- ➔ **BROADCAST**:Broadcast represents that the interface is ready to handle broadcast packets
- ➔ **MULTICAST:**Multicast represents that the interface is ready to handle multicast packets
- ➔ **RUNNING:** Running indicates that the interface is operational to accept data
- ➔ **MTU**:Mtu indicates the Maximum Interface Unit for which the interface is configured and provides a limit on the size of the ethernet frame(1500 being the default value)
- ➔ **Broadcast address**: Broadcast address of the network associated with the interface
- ➔ **inet address**: IPv4 address assigned to the interface
- ➔ **inet6** : IPv6 address assigned to the interface
- ➔ **Netmask** :
- ➔ **RX packets**: number of packets received via the interface
- ➔ **RX errors**: number of damaged packets received
- ➔ **RX overruns:** number of received packets that experienced data overruns

- **RX dropped**: number of dropped packets due to reception errors.TX packets: number of packets transmitted via the interface
- **Frame:**
- **TX errors:** number of packets that incurred transmission error
- **TX dropped:** The number of dropped transmitted packets due to transmission errors.
- **TX overruns:** The number of transmitted packets that experienced data overruns.
- **TX carriers:** The number received packets that experienced loss of carriers.
- **TX collisions:** number of transmitted packets that experienced Ethernet collisions.
- **Txqueuelen:** The field provides information about the configured length of the transmission queue.
- **RX bytes:** total bytes received over this interface.
- **TX bytes:** total bytes transmitted over this interface.

b) Commands that can be used with ifconfig command :

- **mtu N :** The user uses this parameter to set the Maximum Transfer Unit(MTU)
- **up :** This option is used to activate the driver for the given interface(Ifconfig interface up)
- **down :** This option is used to deactivate the driver for the given interface(ifconfig interface down)
- **-v :** Run the command in verbose mode – log more details about execution.(ifconfig -v)

c) The route command displays the computer's routing table.The **route command** distinguishes between **routes** to hosts and **routes** to networks by interpreting the network address of the Destination variable, which can be specified either by symbolic name or numeric address. Output of Route command :

- **Destination** : The destination network or destination host.
- **Gateway** : The gateway address
- **Genmask** : The netmask for the destination network, which is 255.255.255.255 for a host destination and 0.0.0.0 for the default route
- **Flags** : Possible flags include :
  - U : (route is up)
  - H : (target is a host)
  - G: (use gateway)
- **Metric** : The distance to the target usually measured in hops.
- **Ref** : Number of references to this route
- **Use** : Count of lookups for the route. Depending on the use of -F and -C this will be either route cache misses (-F) or hits (-C).
- **Iface** : Interface to which packets of this route will be sent.

d) Commands that can be used with route command :

- **route add default gw <gateway>** : To add a default gateway.This assigns a gateway address on which all packets that do not belong to the network are forwarded.
- **route del default** : to delete the default gateway
- **route add -host <host address/network address> reject** : This will reject routing to the particular host or network. This can be tested by pinging the network. 'Network unreachable" will be displayed.
- **route -Cn** : lists routing cache information

Execution :

```
drishti@morty:~$ sudo route add default gw 192.168.13.10
[sudo] password for drishti:
drishti@morty:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    0      0        0 ppp0
default         _gateway        0.0.0.0         UG    0      0        0 ppp0
default         _gateway        0.0.0.0         UG    0      0        0 wlo1
default         _gateway        0.0.0.0         UG    0      0        0 ppp0
default         _gateway        0.0.0.0         UG    0      0        0 ppp0
default         _gateway        0.0.0.0         UG    0      0        0 wlo1
default         _gateway        0.0.0.0         UG    0      0        0 wlo1
default         _gateway        0.0.0.0         UG    0      0        0 ppp0
default         _gateway        0.0.0.0         UG    20600  0        0 wlo1
10.0.0.0        morty           255.0.0.0       UG    0      0        0 ppp0
agnigarh.iitg.a _gateway        255.255.255.255 UGH   0      0        0 wlo1
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 wlo1
172.16.0.0      morty           255.252.0.0     UG    0      0        0 ppp0
192.168.0.0     morty           255.255.0.0     UG    0      0        0 ppp0
192.168.43.0    0.0.0.0         255.255.255.0   U     600    0        0 wlo1
drishti@morty:~$ sudo route del default
drishti@morty:~$ sudo route add -host 192.168.43 reject
drishti@morty:~$ route -Cn
Kernel IP routing cache
Source          Destination     Gateway         Flags Metric Ref    Use Iface
```

Question : 5

a)**Netstat command** : The **netstat command** (network-statistics) generates and displays network status and protocol statistics. You can display the status of TCP and UDP endpoints in table format, routing table information, and interface information.

b)**netstat -at | grep ESTABLISHED**

```
drishti@morty:~$ netstat -at | grep ESTA
tcp        0      0 morty:36477             52.114.15.54:https      ESTABLISHED
tcp        0      0 morty:50030             ec2-54-85-120-133:https ESTABLISHED
tcp        0      0 morty:36523             52.114.15.54:https      ESTABLISHED
tcp        0      0 morty:57084             13.88.28.53:https       ESTABLISHED
tcp        0      0 morty:60882             agnigarh.iitg.ac.:10443 ESTABLISHED
tcp        0      0 morty:39620             aeab55d76dd13c9bb:https ESTABLISHED
tcp        0      0 morty:60208             ip-185-184-8-30.r:https ESTABLISHED
tcp        0      0 morty:45004             maa03s26-in-f3.1e:https ESTABLISHED
tcp        0      0 morty:33426             52.114.14.120:https     ESTABLISHED
tcp        0      0 morty:34016             104.24.114.179:https    ESTABLISHED
tcp        0      0 morty:58684             stackoverflow.com:https ESTABLISHED
```

c)**Output of netstat -r :**

Displays the routing table. Almost all computers and network devices connected to the Internet use routing tables to compute the next hop for a packet. The routing table stores the routes (and in some cases, metrics associated with those routes) to particular network destinations. This information contains the topology of the network immediately around it.

```
drishti@morty:~$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         _gateway        0.0.0.0         UG        0 0          0 wlo1
10.0.0.0        morty           255.0.0.0       UG        0 0          0 ppp0
agnigarh.iitg.a _gateway        255.255.255.255 UGH       0 0          0 wlo1
link-local      0.0.0.0         255.255.0.0     U         0 0          0 wlo1
172.16.0.0      morty           255.252.0.0     UG        0 0          0 ppp0
192.168.0.0     morty           255.255.0.0     UG        0 0          0 ppp0
192.168.225.0   0.0.0.0         255.255.255.0   U         0 0          0 wlo1
```

- ➔ **Destination** : The destination network or destination host.
- ➔ **Gateway** : The gateway address or '*' 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.
- ➔ **irtt** : initial round trip time
- ➔ **Flags** :
  - ◆ U : route is up
  - ◆ G : use gateway
  - ◆ H : Target is a host
- ➔ **MSS window** : minimum segment size for TCP connection

d) **Status of all networks** : netstat -i
Count of all networks : `netstat -i | tail -n +3 |wc -l`

e) **For all udp connection stats** : netstat -asu

```
drishti@morty:~$ netstat -asu
IcmpMsg:
    InType3: 4
    OutType3: 4
Udp:
    653 packets received
    4 packets to unknown port received
    0 packet receive errors
    550 packets sent
    0 receive buffer errors
    0 send buffer errors
UdpLite:
IpExt:
    InMcastPkts: 89
    OutMcastPkts: 99
    InBcastPkts: 7
    OutBcastPkts: 7
    InOctets: 2656449
    OutOctets: 1795548
    InMcastOctets: 8435
    OutMcastOctets: 12649
    InBcastOctets: 327
    OutBcastOctets: 327
    InNoECTPkts: 6028
```

f) **lo is a loopback device**. It acts as a virtual network device that is on all systems, even when not connected to any network.The IP address of 127.0.0.1 and can be used to locally access network services. Running a web server for debugging/testing locally will route it through this device to the address 127.0.0.1

Question 6 :

a) **Traceroute** is a network diagnostic tool used to track in real-time the pathway taken by a packet on an IP network from source to destination, reporting the IP addresses of all the routers it pinged in between. Traceroute also records the time taken for each hop the packet makes during its route to the destination.Traceroute is a useful tool for determining the response delays and routing loops present in a network pathway across packet switched nodes. It also helps to locate any points of failure encountered while en route to a certain destination.

b)

No.	Hosts	Hops		
		13:00	**20:00**	**2:00**
1	https://www.gov.sg/	22	13	21
2	www.youtube.com	16	13	15
3	https://www.stuff.co.nz/	23	17	14
4	www.geeksforgeeks.org	13	8	13
5	www.euronews.com	21	21	21
6	www.yahoo.co.jp	26	24	23

The blue-highlighted routes are common to all the hosts.

192.168.1.1 : IP address of the first router. Common as all hosts will first jump to this address.

```
drishti@morty:~$ traceroute -I www.yahoo.co.jp
traceroute to edge12.g.yimg.jp (182.22.25.252), 64 hops max
  1   192.168.1.1  3.890ms  109.923ms  2.094ms
  2   192.168.27.237  212.376ms  257.570ms  150.384ms
  3   192.168.27.45  32.737ms  29.828ms  40.108ms
drishti@morty:~$ traceroute -I www.youtube.com
traceroute to youtube-ui.l.google.com (172.217.160.142), 64 hops max
  1   192.168.1.1  1.723ms  1.441ms  1.642ms
  2   192.168.27.237  82.789ms  523.170ms  87.492ms
  3   192.168.27.41  29.789ms  34.276ms  16.400ms
```

c) Yes the route does change at different times of the day, as and when different routers experience network congestion, and other routers may come in to balance the traffic.

d) Some devices do not decrement the TTL of packets passing through them, so they will not show up in traceroutes.

e) the `ping` utility relies on the ICMP protocol which is sometimes blocked at the network firewall or the firewall on the device itself. The most common reason why network admins block ICMP is to prevent "scanning" of the network which they consider to be a security concern. The `traceroute` utility on Linux uses UDP, a completely different protocol, which in this case in not blocked by the network admins. UDP has a variety of uses and blocking this would cause many things to be unusable on a network. The type of ICMP 'control message' needed by `ping` is a subset of a protocol which means blocking that type of ICMP packet causes less problems on a network and is therefore more likely to be blocked than UDP.

Question 7:

a)The full output of the arp table can be seen with : arp -a

```
drishti@drishti-HP-EliteDesk-800-G2-TWR:~$ arp -a
? (172.16.114.218) at a0:8c:fd:e4:57:62 [ether] on eno1
? (172.16.112.66) at 00:03:0f:1a:fc:38 [ether] on eno1
? (172.16.114.200) at a0:8c:fd:de:50:a3 [ether] on eno1
? (172.16.114.236) at a0:8c:fd:e4:57:cb [ether] on eno1
? (172.16.114.153) at a0:8c:fd:e6:92:74 [ether] on eno1
_gateway (172.16.112.1) at 38:22:d6:0c:ef:99 [ether] on eno1
? (172.16.114.143) at d8:9e:f3:3c:6c:4a [ether] on eno1
```

- ➔ The first column of the format: 172.16.114.176 indicates the **IP address**
- ➔ The second column of the format a0:8c:fd:de:f1:2b indicates the **Hardware address**
- ➔ The third column of the format [ether] indicates the **hardware type** (ethernet in this case)
- ➔ The fourth column of the format eno1 indicates the type of **network interface** (ethernet in this case)

b) i) To delete an entry use: arp -d IP address
ii)To add an entry use: **arp -s' IP address' -i 'Network Interface' 'Hardware Address'**

1) arp -s 172.16.114.12 -i eno1 00:03:0f:1a:fc:33
2) arp -s 172.16.114.13 -i eno1 00:03:0f:1a:fc:34

```
? (172.16.114.12) at 00:03:0f:1a:fc:33 [ether] PERM on eno1
? (172.16.114.200) at a0:8c:fd:e4:57:cb [ether] PERM on eno1
? (172.16.114.139) at a0:8c:fd:e3:d9:49 [ether] on eno1
? (172.16.112.51) at 00:03:0f:1b:60:bc [ether] on eno1
? (172.16.114.185) at a0:8c:fd:e6:cd:62 [ether] on eno1
? (172.16.112.33) at 00:03:0f:1d:ab:58 [ether] on eno1
? (172.16.114.175) at a0:8c:fd:de:f1:3a [ether] on eno1
? (172.16.114.221) at a0:8c:fd:e6:91:fb [ether] on eno1
? (172.16.114.156) at a0:8c:fd:e6:cd:2e [ether] on eno1
? (172.16.117.213) at b0:7f:b9:48:5f:dc [ether] on eno1
? (172.16.114.176) at <incomplete> on eno1
? (172.16.114.166) at a0:8c:fd:de:f1:2b [ether] on eno1
```

c)No there cannot exist an entry from a different subnet.

d) **Delete command** : sudo arp -d 172.16.114.200
Add command : sudo arp -s 172.16.114.200 -i eno1 a0:8c:fd:e4:57:cb
Both these addresses were displayed in the arp table with the same Ethernet address.
But the result of pinging the deleted address was as below :

```
? (172.16.114.200) at a0:8c:fd:e4:57:cb [ether] PERM on eno1
? (172.16.112.66) at 00:03:0f:1a:fc:38 [ether] on eno1
? (172.16.114.236) at a0:8c:fd:e4:57:cb [ether] on eno1
drishti@drishti-HP-EliteDesk-800-G2-TWR:~$ ping -c 5 172.16.114.200
PING 172.16.114.200 (172.16.114.200) 56(84) bytes of data.

--- 172.16.114.200 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4083ms
```

We cannot ping the address because the MAC address of the IP address has been forcefully modified in the arp table. And PING sends echo_requests to the IP address after matching it with its MAC address from the arp table. Because the entry was modified, PING command cannot send echo_requests to the correct MAC address.

Question : 8

a)Command : sudo nmap -sn 172.16.114.174/25

b) Command to check firewall : **sudo nmap -sA -T4 <ip address>**

c)

Time	Number of PC's on
00:00	80
02:00	81
11:00	80
16:00	78
21:00	78
23:00	80