Question 1:

a) ping -c <count> <IP address>
b) ping -i <time> <IP address>
c) ping -l <preload> <IP address>, limit for normal users is 3
d) ping -s <packet size> <IP address>, Total packet size=40 bytes (32(payload)+8(ICMP headers)). If we consider the size of IP Address also, then the answer will be 60 bytes.

Question 2:

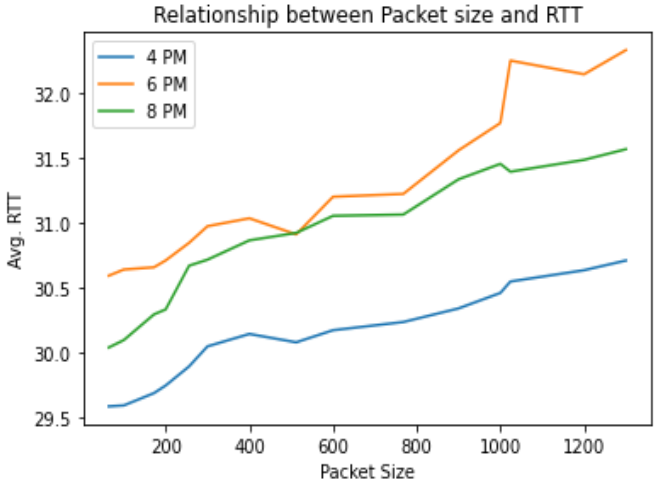
Hosts chosen: 1) www.google.com 2)www.samikshasachdeva26.github.io 3) www.youtube.com

4) www.goldmansachs.com 5) www.facebook.com 6) www.linkedin.com

Host IP address	Location of the host	4 PM IST (RTT & % loss)	6 PM IST (RTT & % loss)	8 PM IST (RTT & % loss)	Average RTT (in ms)	Distance of host (in kms)	%age Packet loss
172.217.166.238	Google, United States	17.887 ms, 0%	18.130 ms, 0%	17.990 ms, 0%	18.030	12619	0
185.199.111.153	San Francisco, United States	58.463 ms, 0%	59.121 ms, 0%	59.002 ms, 0%	58.861	12698	0
172.217.167.14	Delhi, India	21.009 ms, 0%	20.998 ms, 0%	21.316 ms, 0%	21.107	298.3	0
204.74.99.100	San Mateo, United States	106.670 ms, 8%	106.798 ms, 10%	107.536 ms, 9.6%	107.001	12723	9.2
157.240.198.35	Menlo Park, United States	29.301 ms, 12%	29.632 ms, 14%	30.638 ms, 12.7%	29.857	12351	12.9
108.174.10.10	San Jose, United States	273.436 ms, 0%	275.625 m, 0%	274.837 ms, 0%	274.633	12371	0

a. RTTs for above hosts are weakly correlated to the geographical distance. More than the geographical distance, it's the network distance that matters. It is because the packet travels with speed of light between two hops and RTT strongly depends on the number of hops to the host because main latency comes by waiting in a queue of hops.

b. The packet loss percentage is non-zero in the 5th host i.e. 157.240.198.35. The main reason behind packet loss is usually 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.



c. I have used Facebook which is the 5th host in the table, i.e. 157.240.198.35 to analyse the relationship between packet size and RTT.

d. **Relation between Packet Size & RTT:** It can be observed from the graph that as packet size increases, the RTT also increases (with some exceptions in between). Every router and switch along the path has to receive the entire packet before it can forward it. The latency introduced at each point thus equals the speed of the inbound link in bps divided by the frame size in bits.Therefore, larger packets result in increased latency.
Relation between time of the day & RTT: We get different RTT at different times of the day simply because of different traffic or load on the server at different times of the day. It is because an ISP gateway can handle a constant number of requests per second. So when there is more traffic, the number of requests exceeds than those that can be handled by the ISP. So

some of them are pushed into the gateway queue, resulting in a delay in response and finally an increase in RTT.

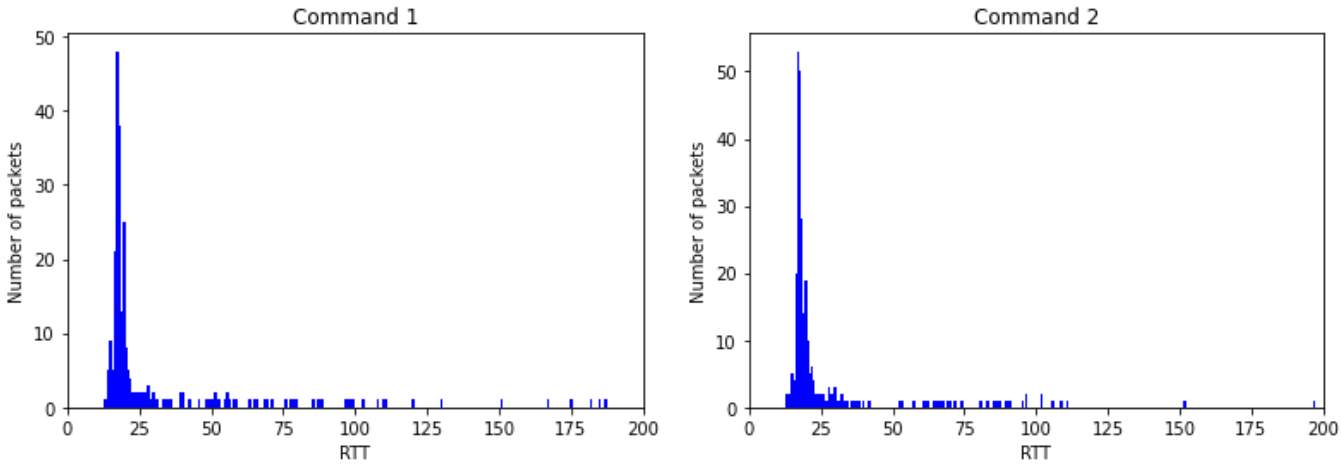
Question 3:

a. **0.8%** packet loss for command 1 and **4.1%** packet loss for command 2.

b.

Command	Min latency	Max latency	Mean latency	Median latency
Command 1	13.358 ms	772.931 ms	24.151 ms	18.0 ms
Command 2	13.115 ms	1194.422 ms	28.057 ms	18.0 ms

c.



d.

I observed that in case of command 2, the ping latencies were larger. Moreover, the packet loss was also more in case of command 2. It is because, in the first case there is no reverse dns lookup making it faster. Also, command 2 has only one transition resulting in less synchronisation and more packet loss and high latency.

Question 4:

a. The output of **ifconfig** command:

```
samiksha@LAPTOP-8LQIR856:/mnt/c/Users/HP$ ifconfig
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 1500
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0xfe<compat,link,site,host>
        loop  (Local Loopback)
        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

wifi0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.100.28  netmask 255.255.255.0  broadcast 192.168.100.255
        inet6 fe80::21bb:4dd5:5370:3e84  prefixlen 64  scopeid 0xfd<compat,link,site,host>
        ether e0:9d:31:d6:6c:e9  (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
```

This command is used to view and change the configuration of the network interfaces on your system. If no arguments are given, ifconfig displays the status of the currently active interfaces. The output of running ifconfig is described below:-

- **MTU** is the short form for Maximum Transmission Unit is the size of each packet received by the Ethernet card. The value of MTU for all Ethernet devices by default is set to 1500.
- **RX and TX Packets** are the number of packets received and transmitted through the interface respectively. The number of bytes corresponding to each are also specified. The number of packets dropped , overrun , collided , or had error transmitting while receiving or transmitting is also mentioned for both RX and TX packets.
- **Inet addr and inet6 addr** are the IPV4 and IPV6 address assigned when the machine is connected to the network.
- **Bcast** denotes the Broadcast Address (address at which all devices connected to the network are enabled to receive datagrams).
- **Mask** is the network mask which we passed using the netmask option. This is required to extract the network address and host address from the IP address.
- **Flags** denote the status of the interface and its facilities. Example, the UP flag indicates an active interface. Running flag indicates that the interface is ready to accept data. Broadcast flag indicates that a broadcast address has been set. Multicast flag indicates that the interface supports multicasting, i.e., it allows a source to send a packet to multiple machines if the machines are watching out for that packet.

b. Options that can be used with ifconfig:

-v : Verbose mode; display additional information for certain error conditions.

-s : Display a short list in a format identical to the command netstat -i.

-a : Display information for all network interfaces, even if they are down.

up : This flag causes the interface to be activated.

down : This flag causes the driver for this interface to be shut down.

mtu N : sets the maximum transfer unit of an interface (limit the maximum packet size).

c. Route command manipulates and displays the system's IP routing tables. Output Explanation:

- **Destination** : The destination network or destination host.
- **Gateway** : It points to the gateway through which network can be reached (* if none set)
- **Genmask** : It is the netmask for the destination net; The value is 255.255.255.255 for a host destination and 0.0.0.0 for the default route.
- **Flags** : These are status indicators. Flag U denote that the route is up, Flag G signifies that the route is to a gateway. Flag H signifies that route is to a host i.e. the dest. is a complete host address.
- **Metric** : The Metric indicates the associated cost of using the indicated route. This is useful for determining the efficiency of a certain route from two points in a network.
- **Ref** : Indicates the number of references to this route.
- **Use** : Indicates the count of lookups for the route.
- **Iface**: Interface to which packets for this route will be sent.

d.

```
amiksha@LAPTOP-8LQIR856:/mnt/c/Users/HP$ route -n
ernel IP routing table
estination     Gateway         Genmask         Flags Metric Ref    Use Iface
27.0.0.0       0.0.0.0         255.0.0.0       U     256    0        0 lo
27.0.0.1       0.0.0.0         255.255.255.255 U     256    0        0 lo
27.255.255.255 0.0.0.0         255.255.255.255 U     256    0        0 lo
24.0.0.0       0.0.0.0         240.0.0.0       U     256    0        0 lo
55.255.255.255 0.0.0.0         255.255.255.255 U     256    0        0 lo
24.0.0.0       0.0.0.0         240.0.0.0       U     256    0        0 wifi0
55.255.255.255 0.0.0.0         255.255.255.255 U     256    0        0 wifi0
.0.0.0         192.168.100.1   255.255.255.255 U     0      0        0 wifi0
92.168.100.255 0.0.0.0         255.255.255.255 U     0      0        0 wifi0
92.168.100.0   0.0.0.0         255.255.255.0   U     0      0        0 wifi0
92.168.100.28  0.0.0.0         255.255.255.255 U     0      0        0 wifi0
amiksha@LAPTOP-8LQIR856:/mnt/c/Users/HP$ route -e
ernel IP routing table
estination     Gateway         Genmask         Flags   MSS Window  irtt Iface
27.0.0.0       0.0.0.0         255.0.0.0       U         0 0          0 lo
27.0.0.1       0.0.0.0         255.255.255.255 U         0 0          0 lo
27.255.255.255 0.0.0.0         255.255.255.255 U         0 0          0 lo
24.0.0.0       0.0.0.0         240.0.0.0       U         0 0          0 lo
55.255.255.255 0.0.0.0         255.255.255.255 U         0 0          0 lo
24.0.0.0       0.0.0.0         240.0.0.0       U         0 0          0 wifi0
55.255.255.255 0.0.0.0         255.255.255.255 U         0 0          0 wifi0
.0.0.0         192.168.100.1   255.255.255.255 U         0 0          0 wifi0
92.168.100.255 0.0.0.0         255.255.255.255 U         0 0          0 wifi0
92.168.100.0   0.0.0.0         255.255.255.0   U         0 0          0 wifi0
```

Various options along with route command are (screenshot is attached above):

1. **-n**: show numerical addresses instead of trying to determine symbolic hostnames.
2. **-e**: use netstat-format for displaying the routing table.
3. **add**: add a new route. While adding a new route, -net specifies the destination network and netmask specifies the Genmask.
4. **del**: While deleting a route, -net specifies destination network to be deleted and netmask specifies the Genmask.

Question 5:

a. Netstat is a command-line network utility tool that displays network connections for the TCP, routing tables, and several network interfaces. It is one of the most basic network debugging tools and is used to find problems in the network and to determine the amount of traffic on the network as a performance measurement by telling what ports are open and whether any programs are listening on ports.

b. **netstat -at** is used to show all TCP connections. We can use **netstat -at | grep "ESTABLISHED"** command to show only the ESTABLISHED TCP connections.

c. The output of the netstat -r command is as follows:

```
samiksha@LAPTOP-8LQIR856:/mnt/c/Users/HP$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
127.0.0.0       0.0.0.0         255.0.0.0       U         0 0          0 lo
127.0.0.1       0.0.0.0         255.255.255.255 U         0 0          0 lo
127.255.255.255 0.0.0.0         255.255.255.255 U         0 0          0 lo
224.0.0.0       0.0.0.0         240.0.0.0       U         0 0          0 lo
255.255.255.255 0.0.0.0         255.255.255.255 U         0 0          0 lo
224.0.0.0       0.0.0.0         240.0.0.0       U         0 0          0 wifi0
255.255.255.255 0.0.0.0         255.255.255.255 U         0 0          0 wifi0
0.0.0.0         192.168.100.1   255.255.255.255 U         0 0          0 wifi0
192.168.100.255 0.0.0.0         255.255.255.255 U         0 0          0 wifi0
192.168.100.0   0.0.0.0         255.255.255.0   U         0 0          0 wifi0
192.168.100.28  0.0.0.0         255.255.255.255 U         0 0          0 wifi0
```

netstat -r shows the kernel routing table of the machine. The output of the command is explained below:

1. **Destination**: It indicates the pattern that the destination of a packet is compared to. While sending a packet over the network, this table is examined in top-down fashion, and the first line that matches is the destination for the packet.
2. **Gateway**: It indicates where to send a packet that matches the destination of the same line. An asterisk means send the packet locally as the destination is on the same network.
3. **Genmask**: It is the netmask for the destination network. It tells the number of bits from the start of the IP address used to identify the subnet.
4. **Flags**: This column indicates which flags apply to the current table line. Flag U indicates that the route is up, Flag G signifies that the route is to a gateway. Moreover, Flag H signifies that the route is to a host which means that the destination is a complete host address.
5. **MSS**: Maximum Segment Size is the size of the 4 largest datagram that the kernel constructs for transmission via this route. It is a TCP parameter which is used to split packets when the destination cannot handle large packets.
6. **Window**: This column indicates the window size which denotes how many TCP packets can be sent before at least one of them has to be acknowledged.
7. **irtt**: Initial Round Trip Time is used by the kernel to guess about the best TCP parameters without waiting for slow replies.
8. **Iface**: it indicates which network interface should be used for sending packets that match the destination.

d. **netstat -i** is used to display the status of all network interfaces. As it can be seen in the image, **two network interfaces** are present on my system.

```
samiksha@LAPTOP-8LQIR856:/mnt/c/Users/HP$ netstat -i
Kernel Interface table
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
lo        1500        0      0      0 0             0      0      0      0 LRU
wifi0     1500        0      0      0 0             0      0      0      0 BMRU
```

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

f. The **loopback device** is a virtual network interface that the system uses to communicate with itself. It is not an actual hardware but helps the applications running on the machine to connect to servers on the same machine. The IPv4 address for accessing loopback interface is 127.0.0.1 . It is used majorly for diagnostics and troubleshooting, and to connect to servers running on the local machine. Apart from using it as a diagnostic tool, it is used when a server offering

a resource is running on the system itself. The **loopback interface** is shown in the screenshot of ifconfig command in the previous question under the **head lo**.

Question 6:

a. Traceroute is a network diagnostic tool used to track the pathway taken by a packet on an IP network from source to destination in real-time. It lists 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(denoted by an asterisk) encountered while enroute to a certain destination.

b.

Time	Google	Samiksha's website	YouTube	Goldman Sachs	Facebook	LinkedIn
4 PM	18	12	28	54 incomplete	28	32
6 PM	18	12	28	56 incomplete	26	32
8 PM	18	12	28	54 incomplete	28	32

c. While going to goldmansachs.com server at 6 PM and facebook.com at 6 PM, the packets went through an additional router which was the only change in their path. The reason for this would most probably be some hardware failure on the path or network congestion. Migration of destination VM servers across data centres may also have caused a change in hop count. Variations in the amount of traffic that the different hops are experiencing as the packets transverse the network also results in different output. Another reason might be the fast switching technique which changes the routing table.

d. Incomplete tracing of route occurred in the case goldmansachs.com. Loss of ICMP/UDP reply packets from intermediate hosts or no reply from the host can be a reason for this. The reason can also be from the sender's side(sender timeout or ICMP/UDP packet not sent with incremental TTL value). Sometimes routers and servers have firewall enabled which either blocks the ICMP traffic or hides the IP Addresses of the hosts to be traced by traceroute. If none of the above problems is present, then there must be a fault in the router itself.

e. Yes, it is possible to find paths using traceroute in cases where ping fails. In ping, intermediate hosts forward the ICMP packets and the destination host replies, thus ping relies on the reply packet. Traceroute works by sending the packets of data with low survival time (Time to Live – TTL) which specifies how many hops the packet can survive before it is returned. Each intermediate host needs to respond with an ICMP/UDP packet. Hence, even if the destination host doesn't respond to ping, a partial path can always be found provided the given source is not blocked from receiving responses. Moreover, if you are not able to connect to a server, traceroute can be used to find the epicenter of the failure.

Question 7:

a. To see the full arp table, arp command is used. ARP table stores IP addresses and the corresponding MAC addresses of the hosts on the network. It can be used to find out the destination MAC address while sending packets to other hosts.
Explanation of the output:
- **Address** : It is the IP address of the connected host on the network.
- **HWtype** : It indicates whether the host has an ethernet interface.
- **HWaddress** : It is the corresponding MAC address.
- **Flags Mask**: They indicate if the mac address has been learned by the system by connecting to the host(denoted by C flag) or/and manually set(denoted by M flag).
- **Iface**: It denotes the interface connecting them.

b. **sudo arp –s <ip_address> <MAC_address>** command is used to add an entry.
sudo arp -d <ip_address> command is used to delete an entry.

c. ARP only works between devices in the same IP subnet. When a device with IP address X needs to send a packet to a device with IP address Y, the first thing it does is looking up its routing table to determine if IP address Y belongs to a subnet it can directly reach through its network interface and if it does, then devices X uses ARP to map IP address Y to a physical Ethernet address. But if the two IP Addresses are on different subnets it will look in its routing table for a route to the destination network, and then it will send its packet to the appropriate router. In some cases, devices on a subnet may respond on behalf of other devices outside the subnet, such as a gateway acting as an ARP proxy.

d. Forcefully replacing the ethernet address of an existing entry and pinging resulted in a 100% packet loss. This is because the ping command operates on layer 3(the network layer) while ARP operates on layer 2(the link layer). So, when you ping an IP address, the layer 3 header is built first and passed to layer 2. At layer 2, the PC checks its ARP table for the corresponding MAC address. The device sends out an ARP request to the destination MAC address. If one of the devices reading that frame has that IP address, then it sends out an ARP reply with a destination MAC address of the device that sent the ARP request and its own MAC address as the source MAC address. If the device reading the ARP request doesn't have the particular IP address in the request, then the requesting device does not receive a reply to its request. Because no reply comes to the system, ping connection timeout occurs eventually.

Question 8:

a. IP Address of my LAB PC is **172.16.70.50.** I have used **nmap -n -sP 172.16.70.50** command to check which PCs of my subnet are up.

b. I used **sudo nmap -sA -T4 172.16.70.50** command to detect firewall settings of my Lab PC.

c. Graph of **number of hosts online vs Time of the Day**. We can see that LAN has the maximum number of active hosts during the day hours i.e. (11 AM-PM) and number of active hosts start falling after 2 AM and are minimum in morning hours.

Time of the day	No. of hosts
8 AM	40
11 AM	72
2 PM	60
4 PM	78
8 PM	60
2 AM	61