Computers Systems Lab-Assignment 1

Group 1

Name	Roll Number
Prahil Bhowmik	**234101037**
Manpreet Singh Saluja	**234101029**
Prateek Kamble	**234101039**
Manish Joshi	**234101027**

1)

a) ping -c count, count echo requests to be

b) ping -i t, t second wait between two consecutive ping requests

c) ping -l ,maximum 3 allowed

d) ping -s x, ping request of size x, for packet of size 40kb total sent is 40+8=48byte

2)

SERVER NAME	PING TIME	AVG RTT(MS)	PACKET LOSS(%)
WWW.GOOGLE.COM	1:00	410.882	0
	3:00	132.934	0
	7:00	154.049	0
WWW.WIKIPEDIA.ORG	1:00	154.576	0
	3:00	138.943	0
	7:00	270.374	0
WWW.GODADDY.COM	1:00	415.525	0
	3:00	203.334	0
	7:00	103.407	0
WWW.DREAMH0ST.COM	1:00	102.165	0
	3:00	205.813	0
	7:00	184.300	0

PacketLoss: It could be due to inadequate signal strength at destination , network congestion,etc.Although in our experiment we did not observe any packet loss.

RTT and Geographic Distance Relation : RTT is directly proportional to geographical distance. Physical distance affects RTT because the further away the host is from the source, the longer it takes to receive a response. So, one method to reduce RTT is moving the two communication endpoints closer together.

Relation of RTT and packet size:

Host used is 209.85.202.138 GOOGLE.COM server in CALIFORNIA US.

Size:	64B	128B	256B	512B	1024B	2048B

RTT:	99.990	138.440	175.965	467.332	467.332	No packet recieved

On increasing the size of packet by a factor of 2 , increase in RTT is observed until 2048 B , at 2048 B no packet is received.

3)

a) You can use the **ifconfig** command to assign an address to a network interface and to configure or display the current network interface configuration information.

Terms in ouput of ifconfig commands are following:

- **inet addr**: IPv4 address assigned to the interface.
- **Inet6 addr**: IPv6 address assigned to the interface.
- **Net Mask**: Network mask associated with the interface.
- **UP**: This flag indicates that the network interface is configured to be enabled.
- **RX**: Related to received packets.
- **TX**: Related to transmitted packets

b) Options with ifconfig

Option	Description	Syntax
-a	Display all interfaces, including those that are down	ifconfig -a
-s	Display a short list instead of details	ifconfig -s
-v	Run th command in verbose mode	ifconfig -v
up	Activates the driver for given interface	ifconfig interface up
Down	Deactivate the driver for given interface	ifconfig interface down

Mtu N	Set the Maximum Transfer Unit	ifconfig interface mtusize size

c) ROUTE: Route manipulates the kernel's IP routing tables. Its primary use is to set up static
routes to specific hosts or networks via an interface after it has been configured with the
ifconfig program. When the add or del options are used, route modifies the routing tables.

OUTPUT:

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.
Flags: Possible flags include
U (route is up),H (target is a host), G (use gateway), R (reinstate route for dynamic routing),
D (dynamically installed by daemon or redirect), M (modified from routing daemon or
redirect), A (installed by addrconf), C (cache entry), ! (reject route)

d) Options in route command :

a) route -n : To display routing table in full numeric form

```
manishjoshi@manishjoshi-VirtualBox:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.0.2.2        0.0.0.0         UG    100    0        0 enp0s3
10.0.2.0        0.0.0.0         255.255.255.0   U     100    0        0 enp0s3
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 enp0s3
manishjoshi@manishjoshi-VirtualBox:~$
```

b) To add a default gateway.

sudo route add default gw 169.254.0.0

```
manishjoshi@manishjoshi-VirtualBox:~$ sudo route add default gw 169.254.0.0
manishjoshi@manishjoshi-VirtualBox:~$
```

c) To reject routing to a particular host

sudo route add -host 192.168.1.51 reject

```
manishjoshi@manishjoshi-VirtualBox:~$ sudo route add -host 192.168.1.51 reject
manishjoshi@manishjoshi-VirtualBox:~$
```

d) To get details of the kernel/IP routing table using ip command

```
manishjoshi@manishjoshi-VirtualBox:~$ ip route
default via 169.254.0.0 dev enp0s3
default via 10.0.2.2 dev enp0s3 proto dhcp metric 20100
10.0.2.0/24 dev enp0s3 proto kernel scope link src 10.0.2.15 metric 100
169.254.0.0/16 dev enp0s3 scope link metric 1000
unreachable 192.168.1.51 scope host
manishjoshi@manishjoshi-VirtualBox:~$
```

4) a)

The netstat command is a network utility tool used to display information about network connections, routing tables, interface statistics, masquerade connections, and other network-related information on a computer. The name "netstat" stands for "network statistics."

When you run the netstat command, it provides a list of active network connections, listening ports, and various network-related statistics. This information can be helpful for troubleshooting network issues, monitoring network activities, and understanding the current state of network connections on a system.

b)

sudo netstat | grep "ESTABLISHED"

Proto Recv-Q Send-Q Local Address Foreign Address State

tcp 0 0 debian:36074 maa05s26-in-f1.1e:https ESTABLISHED

tcp 0 0 debian:58136 76.237.120.34.bc.:https ESTABLISHED

tcp 0 0 debian:41878 181.214.120.34.bc:https ESTABLISHED

tcp 0 0 debian:47058 maa03s45-in-f6.1e:https ESTABLISHED

tcp 0 0 debian:51896 93.243.107.34.bc.:https ESTABLISHED

tcp 0 0 debian:34534 maa03s46-in-f3.1e:https ESTABLISHED

tcp 0 0 debian:50126 maa03s39-in-f3.1e:https ESTABLISHED

tcp 0 0 debian:35302 maa03s28-in-f10.1:https ESTABLISHED

tcp 0 0 debian:60914 104.208.16.90:https ESTABLISHED

tcp 0 0 debian:57304 maa03s47-in-f14.1:https ESTABLISHED

tcp 0 0 debian:33746 maa03s26-in-f3.1e:https ESTABLISHED

tcp 0 0 debian:55996 maa05s15-in-f22.1:https ESTABLISHED

tcp 0 0 debian:47350 maa05s18-in-f2.1e:https ESTABLISHED

tcp 0 0 debian:38282 sa-in-f84.1e100.n:https ESTABLISHED

tcp 0 0 debian:47358 maa05s18-in-f2.1e:https ESTABLISHED

tcp 0 0 debian:41906 maa03s39-in-f3.1e1:http ESTABLISHED

tcp 0 0 debian:55714 maa05s13-in-f14.1:https ESTABLISHED

tcp 0 0 debian:43590 maa05s26-in-f2.1e:https ESTABLISHED

tcp 0 0 debian:49978 maa05s22-in-f14.1:https ESTABLISHED

tcp 0 0 debian:48562 102.115.120.34.bc:https ESTABLISHED

tcp 0 0 debian:60114 180.149.61.136:http ESTABLISHED

tcp 0 0 debian:39274 maa03s37-in-f2.1e:https ESTABLISHED

tcp 0 0 debian:38574 maa05s26-in-f2.1e:https ESTABLISHED

tcp 0 0 debian:36354 maa03s41-in-f14.1:https ESTABLISHED

tcp 0 0 debian:50124 maa03s39-in-f3.1e:https ESTABLISHED

tcp 0 0 debian:60106 180.149.61.136:http ESTABLISHED

udp 0 0 debian:bootpc 172.17.1.1:bootps ESTABLISHED

Proto: This column displays the protocol used, which is typically TCP for established connections.

Recv-Q and Send-Q: These columns represent the size of the receive and send queues, respectively. They indicate the amount of data waiting to be sent or received.

Local Address: This column shows the local IP address and port number for the connection.

Foreign Address: This column shows the remote (or foreign) IP address and port number to which the local system is connected.

State: This column indicates the current state of the connection. For established connections, it should be "ESTABLISHED."

c)

The netstat -r command is used to display the kernel routing table.This table contains information about the network routes that the system uses to forward packets.

Destination: This column shows the destination network or host. It represents the destination IP address or network for the route.

Gateway: If a specific route requires forwarding through a gateway (router), this column displays the IP address of that gateway. If the destination is on a directly connected network, this field may show an asterisk (*) or the word "link#".

Genmask (Netmask): This column indicates the netmask associated with the destination.

Flags: Flags provide additional information about the route. Common flags include:

U (Up): Indicates that the route is active.

G (Gateway): Denotes that the route requires a gateway.

H (Host): Specifies that the destination is a host (a specific IP address).

D (Dynamic): Indicates a dynamically created route.

MSS (Maximum Segment Size): The Maximum Segment Size is the maximum amount of data that can be sent in a single TCP segment. It is negotiated during the TCP handshake between two devices. MSS is typically specified in bytes.

Window: In the context of TCP (Transmission Control Protocol), the "Window" refers to the TCP window size. It represents the amount of data (in bytes) that a sender can transmit before receiving an acknowledgment from the receiver. It plays a crucial role in flow control to prevent congestion.

irtt (Initial Round-Trip Time): This term represents the initial round-trip time, which is the time it takes for a packet to travel from the source to the destination and back. It is an important parameter in TCP connections and is used for estimating the retransmission timeout.

Iface (Interface): This column likely represents the network interface through which the corresponding connection is established.

Iface (Interface): This column displays the network interface through which the routing entry is accessible. It specifies the outgoing interface for the route.

d)

netstat -i

This command provides a list of network interfaces along with information about their status, such as bytes and packets transmitted and received.

The number of interfaces are 3

e)

sudo netstat -su

IcmpMsg:

InType0: 66

InType3: 133

InType8: 7

InType11: 31

OutType0: 7

OutType3: 127

OutType8: 91

Udp:

306295 packets received

127 packets to unknown port received

7809 packet receive errors

14606 packets sent

7809 receive buffer errors

0 send buffer errors

IgnoredMulti: 17816

UdpLite:

IpExt:

InMcastPkts: 184763

OutMcastPkts: 103

InBcastPkts: 17824

InOctets: 213636385

OutOctets: 6851891

InMcastOctets: 32962888

OutMcastOctets: 11465

InBcastOctets: 3245892

InNoECTPkts: 360597

InECT0Pkts: 18

MPTcpExt:

f)

The loopback device is a special, virtual network interface that your computer uses to communicate with itself. It is used mainly for diagnostics and troubleshooting, and to connect to servers running on the local machine.

The loopback interface does not represent any actual hardware, but exists so applications running on your computer can always connect to servers on the same machine.

5)

Traceroute is a network diagnostic tool used to trace the route that packets of data take from one destination to another across a network. It provides valuable information about the path that data packets follow, including the number of hops, the round-trip time for each hop, and the IP addresses of the routers or devices along the way.

//10:00 AM friday

traceroute google.com

traceroute to google.com (142.251.42.78), 30 hops max, 60 byte packets

1 _gateway (192.168.0.1) 1.433 ms 1.360 ms 2.472 ms

2 10.12.0.254 (10.12.0.254) 5.357 ms 5.349 ms 5.551 ms

3 172.17.0.1 (172.17.0.1) 4.713 ms 4.685 ms 4.690 ms

4 192.168.193.1 (192.168.193.1) 4.796 ms 4.834 ms 4.893 ms

5 14.139.196.17 (14.139.196.17) 5.707 ms 5.677 ms 5.649 ms

6 10.119.254.241 (10.119.254.241) 5.620 ms 2.532 ms 2.468 ms

7 * * *

8 * * *

9 10.119.73.122 (10.119.73.122) 43.855 ms 43.826 ms 43.798 ms

10 72.14.213.20 (72.14.213.20) 66.775 ms 68.809 ms 68.781 ms

11 * * *

12 74.125.242.129 (74.125.242.129) 87.460 ms 108.170.253.97 (108.170.253.97) 65.627 ms 142.251.55.220 (142.251.55.220) 67.540 ms

13 108.170.253.105 (108.170.253.105) 81.455 ms 74.125.242.138 (74.125.242.138) 90.684 ms 74.125.242.139 (74.125.242.139) 70.681 ms

14 142.250.212.0 (142.250.212.0) 77.730 ms 76.574 ms 99.179 ms

15 108.170.248.161 (108.170.248.161) 99.690 ms 142.250.238.206 (142.250.238.206) 79.338 ms 74.872 ms

16 142.251.69.103 (142.251.69.103) 71.156 ms 108.170.248.161 (108.170.248.161) 81.374 ms 142.251.69.105 (142.251.69.105) 70.193 ms

17 142.251.69.105 (142.251.69.105) 70.413 ms bom12s21-in-f14.1e100.net (142.251.42.78) 81.746 ms 83.874 ms

traceroute youtube.com

traceroute to youtube.com (142.250.67.206), 30 hops max, 60 byte packets

1 _gateway (192.168.0.1) 0.938 ms 0.870 ms 1.529 ms

2 10.12.0.254 (10.12.0.254) 4.700 ms 4.747 ms 4.721 ms

3 172.17.0.1 (172.17.0.1) 4.262 ms 4.398 ms 4.369 ms

4 192.168.193.1 (192.168.193.1) 4.106 ms 4.078 ms 4.047 ms

5 14.139.196.17 (14.139.196.17) 5.023 ms 4.992 ms 4.963 ms

6 10.119.254.241 (10.119.254.241) 4.939 ms 1.680 ms 1.622 ms

7 * * *

8 * * *

9 10.119.73.122 (10.119.73.122) 43.220 ms 42.045 ms 43.408 ms

10 72.14.213.20 (72.14.213.20) 65.286 ms 72.14.195.128 (72.14.195.128) 66.455 ms 72.14.213.20 (72.14.213.20) 65.503 ms

11 * * *

12 74.125.242.129 (74.125.242.129) 85.334 ms 142.251.55.232 (142.251.55.232) 80.183 ms 108.170.253.97 (108.170.253.97) 66.297 ms

13 108.170.253.106 (108.170.253.106) 60.720 ms 74.125.242.155 (74.125.242.155) 84.066 ms 74.125.242.131 (74.125.242.131) 78.697 ms

14 172.253.72.137 (172.253.72.137) 66.937 ms 142.250.238.206 (142.250.238.206) 81.881 ms 142.250.212.4 (142.250.212.4) 67.180 ms

15 142.250.212.0 (142.250.212.0) 76.369 ms 108.170.248.177 (108.170.248.177) 57.583 ms 56.322 ms

16 . 108.170.248.177 (108.170.248.177) 55.645 ms 108.170.248.161 (108.170.248.161) 75.865 ms 75.594 ms

17 142.250.235.9 (142.250.235.9) 70.377 ms 66.319 ms 69.797 ms

18 bom12s08-in-f14.1e100.net (142.250.67.206) 63.272 ms 69.126 ms 63.756 ms

traceroute facebook.com

traceroute to facebook.com (163.70.143.35), 30 hops max, 60 byte packets

1 _gateway (192.168.0.1) 2.076 ms 2.005 ms 1.973 ms

2 10.12.0.254 (10.12.0.254) 16.630 ms 16.600 ms 16.620 ms

3 172.17.0.1 (172.17.0.1) 5.217 ms 5.258 ms 5.229 ms

4 192.168.193.1 (192.168.193.1) 5.200 ms 5.338 ms 5.310 ms

5 14.139.196.17 (14.139.196.17) 6.563 ms 6.531 ms 6.503 ms

6 10.119.254.241 (10.119.254.241) 6.476 ms 6.044 ms 6.026 ms

7 10.177.31.1 (10.177.31.1) 73.242 ms 75.534 ms 73.482 ms

8 10.255.237.21 (10.255.237.21) 60.865 ms 60.475 ms 61.403 ms

9 10.255.238.166 (10.255.238.166) 74.649 ms 76.472 ms 73.711 ms

10 10.152.7.38 (10.152.7.38) 65.202 ms 64.895 ms 10.152.7.214 (10.152.7.214) 77.188 ms

11 ae2.pr02.bom1.tfbnw.net (157.240.66.204) 65.536 ms ae1.pr01.bom1.tfbnw.net (157.240.68.238) 66.011 ms 65.961 ms

12 po105.psw04.bom2.tfbnw.net (129.134.33.197) 72.618 ms po106.psw04.bom2.tfbnw.net (129.134.33.205) 77.851 ms 77.520 ms

13 157.240.38.151 (157.240.38.151) 64.727 ms 157.240.38.255 (157.240.38.255) 82.074 ms 173.252.67.11 (173.252.67.11) 66.381 ms

14 edge-star-mini-shv-01-bom2.facebook.com (163.70.143.35) 59.342 ms 59.713 ms 60.187 ms

traceroute instagram.com

traceroute to instagram.com (163.70.143.174), 30 hops max, 60 byte packets

1 _gateway (192.168.0.1) 5.985 ms 6.481 ms 6.452 ms

2 10.12.0.254 (10.12.0.254) 10.184 ms 10.156 ms 10.127 ms

3 172.17.0.1 (172.17.0.1) 10.097 ms 10.072 ms 10.046 ms

4 192.168.193.1 (192.168.193.1) 10.018 ms 9.991 ms 9.966 ms

5 14.139.196.17 (14.139.196.17) 10.570 ms 10.544 ms 10.519 ms

6 10.119.254.241 (10.119.254.241) 10.493 ms 1.860 ms 15.805 ms

7 10.177.31.1 (10.177.31.1) 82.184 ms 82.174 ms 82.166 ms

8 10.255.237.21 (10.255.237.21) 67.295 ms 67.287 ms 67.280 ms

9 10.255.238.166 (10.255.238.166) 81.982 ms 81.974 ms 82.112 ms

10 10.152.7.38 (10.152.7.38) 69.008 ms 10.152.7.214 (10.152.7.214) 84.507 ms 84.662 ms

11 ae1.pr01.bom1.tfbnw.net (157.240.68.238) 75.906 ms 75.898 ms ae2.pr02.bom1.tfbnw.net (157.240.66.204) 75.875 ms

12 po106.psw01.bom2.tfbnw.net (129.134.33.199) 66.124 ms po106.psw03.bom2.tfbnw.net (129.134.33.203) 77.226 ms po105.psw03.bom2.tfbnw.net (129.134.33.195) 68.988 ms

13 173.252.67.29 (173.252.67.29) 87.096 ms 173.252.67.141 (173.252.67.141) 70.428 ms 173.252.67.135 (173.252.67.135) 74.706 ms

14 instagram-p42-shv-01-bom2.fbcdn.net (163.70.143.174) 63.199 ms 82.195 ms 61.135 ms

sudo traceroute flipkart.com

traceroute to flipkart.com (103.243.32.90), 30 hops max, 60 byte packets

1 _gateway (192.168.0.1) 2.846 ms 2.800 ms 3.005 ms

2 10.12.0.254 (10.12.0.254) 6.821 ms 6.814 ms 6.808 ms

3 172.17.0.1 (172.17.0.1) 6.255 ms 6.247 ms 6.238 ms

4 192.168.193.1 (192.168.193.1) 6.213 ms 6.363 ms 6.355 ms

5 14.139.196.17 (14.139.196.17) 7.264 ms 9.514 ms 9.506 ms

6 10.119.254.241 (10.119.254.241) 7.367 ms 2.510 ms 6.903 ms

7 * * *

8 * * *

9 10.119.73.122 (10.119.73.122) 43.202 ms 42.935 ms 45.972 ms

10 115.247.85.129 (115.247.85.129) 68.024 ms 68.016 ms 71.711 ms

11 * * *

12 * * *

13 * * *

14 * * *

15 * * *

16 * * *

17 * * *

18 * * *

19 * * *

20 * * *

21 * * *

22 * * *

23 * * *

24 * * *

25 * * *

26 * * *

27 * * *

28 * * *

29 * * *

30 * * *

traceroute amazon.com

traceroute to amazon.com (52.94.236.248), 30 hops max, 60 byte packets

1 _gateway (192.168.0.1) 1.564 ms 1.511 ms 1.494 ms

2 10.12.0.254 (10.12.0.254) 5.477 ms 5.463 ms 5.449 ms

3 172.17.0.1 (172.17.0.1) 4.875 ms 4.863 ms 4.848 ms

4 192.168.193.1 (192.168.193.1) 4.827 ms 4.813 ms 4.800 ms

5 14.139.196.17 (14.139.196.17) 5.350 ms 5.336 ms 5.323 ms

6 10.119.254.241 (10.119.254.241) 5.309 ms 2.298 ms 2.253 ms

7 * * *

8 * * *

9 10.119.73.122 (10.119.73.122) 44.336 ms 44.459 ms 44.847 ms

10 115.247.85.129 (115.247.85.129) 71.793 ms 71.768 ms 71.741 ms

11 * * *

12 * * *

13 * * *

14 * * *

15 * * *

16 * * *

17 * * *

18 * * *

19 * * *

20 * * *

21 * * *

22 * * *

23 * * *

24 * * *

25 * * *

26 * * *

27 * * *

28 * * *

29 * * *

30 * * *

// at 3:00 PM on friday

sudo traceroute google.com

[sudo] password for pratik:

traceroute to google.com (142.251.42.78), 30 hops max, 60 byte packets

1 _gateway (192.168.0.1) 1.254 ms 1.476 ms 1.465 ms

2 10.12.0.254 (10.12.0.254) 5.451 ms 5.512 ms 5.686 ms

3 172.17.0.1 (172.17.0.1) 4.915 ms 4.906 ms 4.898 ms

4 192.168.193.1 (192.168.193.1) 5.179 ms 5.170 ms 5.182 ms

5 14.139.196.17 (14.139.196.17) 6.233 ms 6.226 ms 6.218 ms

6 10.119.254.241 (10.119.254.241) 6.211 ms 4.008 ms 6.006 ms

7 * * *

8 * * *

9 10.119.73.122 (10.119.73.122) 52.784 ms 53.042 ms 52.700 ms

10 72.14.213.20 (72.14.213.20) 95.892 ms 72.14.195.128 (72.14.195.128) 66.538 ms 66.866 ms

11 * * *

12 74.125.242.129 (74.125.242.129) 90.021 ms 216.239.54.158 (216.239.54.158) 73.306 ms 209.85.142.246 (209.85.142.246) 83.396 ms

13 74.125.242.147 (74.125.242.147) 78.299 ms 108.170.253.105 (108.170.253.105) 84.948 ms 74.125.242.139 (74.125.242.139) 82.701 ms

14 142.250.212.0 (142.250.212.0) 99.286 ms 142.250.238.182 (142.250.238.182) 83.719 ms 142.250.212.0 (142.250.212.0) 95.369 ms

15 72.14.232.34 (72.14.232.34) 83.861 ms 172.253.68.121 (172.253.68.121) 69.110 ms 108.170.248.177 (108.170.248.177) 71.879 ms

16 108.170.248.161 (108.170.248.161) 88.501 ms 142.251.69.105 (142.251.69.105) 100.127 ms 108.170.248.177 (108.170.248.177) 66.309 ms

17 bom12s21-in-f14.1e100.net (142.251.42.78) 92.102 ms 142.251.69.103 (142.251.69.103) 83.279 ms bom12s21-in-f14.1e100.net (142.251.42.78) 90.732 ms

traceroute amazon.com

traceroute to amazon.com (52.94.236.248), 30 hops max, 60 byte packets

1 _gateway (192.168.0.1) 0.959 ms 1.187 ms 1.157 ms

2 * * *

3 172.17.0.1 (172.17.0.1) 2.942 ms 2.951 ms 2.922 ms

4 192.168.193.1 (192.168.193.1) 2.912 ms 3.040 ms 5.423 ms

5 14.139.196.17 (14.139.196.17) 5.641 ms 5.617 ms 5.591 ms

6 10.119.254.241 (10.119.254.241) 5.819 ms 3.976 ms 3.806 ms

7 * * *

8 * * *

9 10.119.73.122 (10.119.73.122) 53.709 ms 53.685 ms 53.659 ms

10 115.247.85.129 (115.247.85.129) 68.004 ms 68.317 ms 66.009 ms

11 * * *

12 * * *

13 * * *

14 * * *

15 * * *

16 * * *

17 * * *

18 * * *

19 * * *

20 * * *

21 * * *

22 * * *

23 * * *

24 * * *

25 * * *

26 * * *

27 * * *

28 * * *

29 * * *

30 * * *

traceroute facebook.com

traceroute to facebook.com (163.70.143.35), 30 hops max, 60 byte packets

1 _gateway (192.168.0.1) 1.419 ms 1.344 ms 1.312 ms

2 10.12.0.254 (10.12.0.254) 5.331 ms 5.299 ms 5.270 ms

3 172.17.0.1 (172.17.0.1) 4.198 ms 4.302 ms 4.215 ms

4 192.168.193.1 (192.168.193.1) 4.177 ms 4.186 ms 4.157 ms

5 14.139.196.17 (14.139.196.17) 5.274 ms 5.244 ms 5.216 ms

6 10.119.254.241 (10.119.254.241) 5.189 ms 2.247 ms 5.076 ms

7 10.177.31.1 (10.177.31.1) 75.080 ms 80.156 ms 80.099 ms

8 10.255.237.21 (10.255.237.21) 66.084 ms 64.296 ms 66.220 ms

9 10.255.238.166 (10.255.238.166) 79.991 ms 77.225 ms 79.938 ms

10 10.152.7.214 (10.152.7.214) 90.992 ms 10.152.7.38 (10.152.7.38) 66.481 ms 10.152.7.214 (10.152.7.214) 92.892 ms

11 ae1.pr01.bom1.tfbnw.net (157.240.68.238) 75.746 ms ae2.pr02.bom1.tfbnw.net (157.240.66.204) 106.731 ms 106.892 ms

12 po105.psw02.bom2.tfbnw.net (129.134.33.193) 82.569 ms po105.psw01.bom2.tfbnw.net (129.134.33.191) 75.231 ms po106.psw01.bom2.tfbnw.net (129.134.33.199) 72.112 ms

13 173.252.67.83 (173.252.67.83) 81.545 ms 173.252.67.151 (173.252.67.151) 64.575 ms 173.252.67.191 (173.252.67.191) 76.513 ms

14 edge-star-mini-shv-01-bom2.facebook.com (163.70.143.35) 63.842 ms 63.788 ms 60.904 ms

traceroute instagram.com

traceroute to instagram.com (163.70.143.174), 30 hops max, 60 byte packets

1 _gateway (192.168.0.1) 0.697 ms 3.803 ms 3.771 ms

2 10.12.0.254 (10.12.0.254) 11.413 ms 11.384 ms 11.356 ms

3 172.17.0.1 (172.17.0.1) 4.830 ms 4.801 ms 4.770 ms

4 192.168.193.1 (192.168.193.1) 4.727 ms 4.854 ms 4.824 ms

5 14.139.196.17 (14.139.196.17) 5.362 ms 5.329 ms 5.301 ms

6 10.119.254.241 (10.119.254.241) 5.272 ms 3.708 ms 4.196 ms

7 10.177.31.1 (10.177.31.1) 75.473 ms 75.443 ms 73.920 ms

8 10.255.237.21 (10.255.237.21) 59.946 ms 61.900 ms 62.225 ms

9 10.255.238.166 (10.255.238.166) 75.235 ms 72.827 ms 76.338 ms

10 10.152.7.38 (10.152.7.38) 63.513 ms 10.152.7.214 (10.152.7.214) 88.928 ms 10.152.7.38 (10.152.7.38) 62.826 ms

11 ae1.pr01.bom1.tfbnw.net (157.240.68.238) 72.643 ms ae2.pr02.bom1.tfbnw.net (157.240.66.204) 80.032 ms ae1.pr01.bom1.tfbnw.net (157.240.68.238) 73.983 ms

12 po105.psw02.bom2.tfbnw.net (129.134.33.193) 85.666 ms po105.psw01.bom2.tfbnw.net (129.134.33.191) 75.027 ms po105.psw02.bom2.tfbnw.net (129.134.33.193) 74.720 ms

13 157.240.39.7 (157.240.39.7) 65.827 ms 157.240.38.227 (157.240.38.227) 62.824 ms 157.240.38.123 (157.240.38.123) 81.490 ms

14 instagram-p42-shv-01-bom2.fbcdn.net (163.70.143.174) 63.343 ms 83.004 ms 61.179 ms

traceroute flipkart.com

traceroute to flipkart.com (103.243.32.90), 30 hops max, 60 byte packets

1 _gateway (192.168.0.1) 0.849 ms 1.038 ms 1.009 ms

2 10.12.0.254 (10.12.0.254) 13.438 ms 13.511 ms 13.588 ms

3 172.17.0.1 (172.17.0.1) 4.496 ms 4.461 ms 4.453 ms

4 192.168.193.1 (192.168.193.1) 4.441 ms 4.431 ms 4.422 ms

5 14.139.196.17 (14.139.196.17) 5.962 ms 5.952 ms 5.942 ms

6 10.119.254.241 (10.119.254.241) 5.933 ms 4.594 ms 4.790 ms

7 * * *

8 * * *

9 10.119.73.122 (10.119.73.122) 51.988 ms 51.979 ms 53.301 ms

10 115.247.85.129 (115.247.85.129) 69.271 ms 71.589 ms 67.082 ms

11 * * *

12 * * *

13 * * *

14 * * *

15 * * *

16 * * *

17 * * *

18 * * *

19 * * *

20 * * *

21 * * *

22 * * *

23 * * *

24 * * *

25 * * *

26 * * *

27 * * *

28 * * *

29 * * *

30 * * *

traceroute youtube.com

traceroute to youtube.com (142.250.76.206), 30 hops max, 60 byte packets

1 _gateway (192.168.0.1) 3.555 ms 4.705 ms 4.676 ms

2 10.12.0.254 (10.12.0.254) 10.664 ms 10.637 ms 10.611 ms

3 172.17.0.1 (172.17.0.1) 7.235 ms 7.210 ms 7.182 ms

4 192.168.193.1 (192.168.193.1) 7.147 ms 7.122 ms 7.090 ms

5 14.139.196.17 (14.139.196.17) 12.933 ms 12.902 ms 12.863 ms

6 10.119.254.241 (10.119.254.241) 16.412 ms 1.887 ms 4.086 ms

7 * * *

8 * * *

9 10.119.73.122 (10.119.73.122) 50.753 ms 50.888 ms 53.196 ms

10 72.14.195.128 (72.14.195.128) 65.862 ms 72.14.213.20 (72.14.213.20) 77.169 ms 72.14.195.128 (72.14.195.128) 67.504 ms

11 * * *

12 216.239.54.158 (216.239.54.158) 70.156 ms 74.125.242.129 (74.125.242.129) 104.261 ms 104.418 ms

13 74.125.242.130 (74.125.242.130) 99.336 ms 74.125.242.138 (74.125.242.138) 112.727 ms 108.170.253.105 (108.170.253.105) 94.034 ms

14 64.233.174.3 (64.233.174.3) 91.813 ms 142.250.238.206 (142.250.238.206) 75.341 ms 142.250.56.38 (142.250.56.38) 68.303 ms

15 108.170.248.177 (108.170.248.177) 68.233 ms 142.250.238.206 (142.250.238.206) 75.807 ms 108.170.248.177 (108.170.248.177) 70.381 ms

16 108.170.248.161 (108.170.248.161) 96.624 ms 142.250.208.149 (142.250.208.149) 71.122 ms 108.170.248.177 (108.170.248.177) 72.299 ms

17 142.250.208.149 (142.250.208.149) 72.701 ms bom12s10-in-f14.1e100.net (142.250.76.206) 99.806 ms 142.250.208.149 (142.250.208.149) 70.012 ms

b)

Network Congestion:

During peak hours, network congestion may occur as more users access the network. Routers might dynamically adjust the routing paths to avoid congested links, leading to changes in the optimal route.

Dynamic Routing Protocols:

Networks often use dynamic routing protocols (e.g., OSPF, BGP) to adapt to changing network conditions. These protocols allow routers to exchange information and dynamically choose the best paths based on factors like link quality and traffic load.

Load Balancing:

Network administrators or automated systems may configure load balancing policies. Different routes may be selected at different times to distribute traffic evenly across multiple paths, optimizing network performance.

Time-of-Day Network Policies:

Some organizations implement time-of-day network policies that influence routing decisions. For example, specific routes might be preferred during business hours and different routes during non-peak hours to optimize performance or reduce costs.

Scheduled Maintenance:

Network maintenance activities, such as updates, patches, or hardware upgrades, may be scheduled during off-peak hours. During maintenance windows, routers may temporarily use alternative paths, leading to changes in the route.

Changing Network Topology:

The network topology itself might change due to various factors like the addition of new routers, modifications to network infrastructure, or changes in connectivity between network segments.

Security Policies:

Security measures, such as firewalls or intrusion prevention systems, may influence routing decisions based on the time of day. For instance, certain routes might be preferred during high-security periods.

Route Flapping:

Unstable network conditions or temporary link failures can result in route flapping, where routers repeatedly switch between different routes. This behavior may be more pronounced during certain times of the day.

c)

Firewall Blocking ICMP:

Reasoning: Many hosts and network devices are configured to block ICMP (Internet Control Message Protocol) packets, which are used by traceroute. Firewalls at the host or network level may discard or filter out ICMP packets, preventing traceroute from receiving responses.

Router Configuration:

Reasoning: Some routers are configured not to respond to ICMP requests or have ICMP rate limiting in place. In such cases, routers along the path may not provide the necessary responses to complete the traceroute.

Network Filtering Policies:

Reasoning: Certain networks may implement filtering policies that restrict or control the types of traffic allowed through. If ICMP traffic is selectively filtered, it can result in incomplete traceroute paths.

Load Balancers and Anycast:

Reasoning: In environments with load balancers or anycast configurations, multiple servers may share the same IP address. Traceroute may not follow the same path for each packet, leading to inconsistencies in the responses and potentially incomplete paths.

Host Unreachable:

Reasoning: If the destination host is down or unreachable, traceroute will not receive responses beyond the point of failure. This can occur due to network outages, server maintenance, or other issues affecting the host's accessibility.

Rate Limiting or ICMP Unresponsiveness:

Reasoning: Some hosts and routers may implement rate limiting for ICMP responses or may not respond to certain types of ICMP messages. Traceroute relies on ICMP Time Exceeded and ICMP Echo Reply messages, and if these are suppressed, the traceroute may not complete.

Policy-Based Routing:

Reasoning: Networks that implement policy-based routing may have different routing policies for different types of traffic. Traceroute packets may be subject to policies that lead them on different paths, resulting in incomplete traceroute paths.

Network Security Policies:

Reasoning: Security measures such as intrusion detection or prevention systems may affect the ability of traceroute to complete paths. These systems may interpret traceroute packets as potentially malicious and filter them out.

NAT (Network Address Translation):

Reasoning: In networks employing NAT, the IP address seen by traceroute may not accurately reflect the actual path to the destination. The NAT device may not respond to traceroute requests or may provide misleading information.

d)

Different Handling of ICMP Types:

While ping and traceroute both use ICMP, they serve different purposes. Ping relies on ICMP Echo Request and Echo Reply messages, while traceroute uses ICMP Time Exceeded and ICMP Echo Reply messages. Some hosts and routers may selectively respond to or ignore specific ICMP types.

Firewall Configuration:

Firewalls may be configured to allow certain ICMP types but block others. A host or network device might block ICMP Echo Requests (ping) for security reasons but still allow ICMP Time Exceeded messages generated by routers along the traceroute path.

Routing Policies:

Networks may implement policies that treat different types of ICMP traffic differently. While ICMP Echo Requests might be blocked, routers may still generate ICMP Time Exceeded messages, revealing information about the route.

Rate Limiting or Unresponsiveness to Ping:

Some hosts or routers may be configured to limit responses to ping requests due to security concerns or resource considerations. However, they may still respond to traceroute probes, allowing the identification of the path.

Different Network Paths:

The path taken by traceroute packets may differ from the path taken by ping packets. Network conditions, load balancing, and routing policies can result in different paths for different types of traffic.

Anycast Configurations:

Hosts or services configured with anycast may respond differently to ping requests than to traceroute probes. Anycast involves multiple servers sharing the same IP address, and the responses may depend on the specific server that receives the traffic.

Selective Configuration for Troubleshooting:

In some cases, hosts or routers may be selectively configured to respond to traceroute probes for troubleshooting purposes, even if they don't respond to ping requests.

Administrative Configuration:

Network administrators have the flexibility to configure routers and hosts to respond differently to various types of traffic. They may choose to allow traceroute responses for diagnostic purposes while blocking other types of ICMP traffic.

6) a)

command : sudo arp

Address:

This column typically contains the IP addresses (Internet addresses) associated with devices on the network.

HWtype (Hardware Type):

Indicates the type of network technology or hardware, often represented by a numeric code. Common values include Ethernet (1), ARP (Ethernet), etc.

HWaddress (Hardware Address or MAC Address):

Shows the MAC (Media Access Control) addresses corresponding to the IP addresses in the first column.

Flags:

This column includes various flags that provide additional information about the ARP entry. Common flags include "C" for complete entries and "M" for permanent (static) entries.

Mask:

If present, this column might display the subnet mask associated with the IP address.

b)

for adding new entries to the arp table we use the command

sudo arp -s ipaddress hardwareaddress

for deleting the entry we use the command

sudo arp -d ipaddress

sudo arp

Address HWtype HWaddress Flags Mask Iface

192.168.0.101 ether aa:bb:cc:dd:ee:ff CM wlp0s20f3

_gateway ether aa:bb:cc:dd:ee:ff C wlp0s20f3

sudo arp

Address HWtype HWaddress Flags Mask Iface

_gateway ether aa:bb:cc:dd:ee:ff C wlp0s20f3

sudo arp

Address HWtype HWaddress Flags Mask Iface

192.168.0.104 ether aa:bb:cc:dd:ee:ff CM wlp0s20f3

192.168.0.102 ether aa:bb:cc:dd:ee:ff CM wlp0s20f3

192.168.0.103 ether aa:bb:cc:dd:ee:ff CM wlp0s20f3

192.168.0.101 ether aa:bb:cc:dd:ee:ff CM wlp0s20f3

_gateway ether aa:bb:cc:dd:ee:ff C wlp0s20f3

c)

The validity and expiration of entries in the ARP (Address Resolution Protocol) cache are determined by a combination of factors, and the specific parameters might vary based on the operating system. In general, the following factors play a role in determining the timeout and deletion of ARP cache entries:

ARP Timeout:

ARP cache entries have a timeout associated with them. This timeout is the period for which an ARP entry remains valid. After this period, the entry may be considered stale and subject to removal.

The timeout is usually set by the operating system and can be influenced by various parameters such as the ARP cache timeout setting.

ARP Cache Timeout Setting:

Many operating systems allow administrators to configure the ARP cache timeout setting. This setting determines how long an ARP entry remains valid before it is considered outdated.

On some systems, this setting might be configurable in seconds or milliseconds, and it typically defaults to a specific value.

ARP Probe and Announcement:

Some systems use ARP probes and announcements to verify the validity of ARP cache entries. An ARP probe is a mechanism where a device sends out ARP requests to verify if an IP address is still in use. If no response is received, the entry might be marked as stale.

ARP announcements are also used to refresh ARP caches. A device periodically announces its IP-MAC mapping to the network, ensuring that other devices update their ARP caches.

Network Activity:

ARP entries may also be influenced by network activity. If a device communicates with another device using a particular IP-MAC mapping, the ARP cache entry for that mapping may be refreshed.

Operating System Implementation:

Different operating systems may implement ARP cache management differently. Some systems might be more aggressive in removing stale entries, while others might have more lenient timeout settings.

Unpredictable Communication:

Hosts on the subnet may experience unpredictable communication issues. Traffic destined for either of the conflicting IP addresses may be sent to the device with the shared MAC address.

d)

ARP Resolution Confusion:

ARP (Address Resolution Protocol) is used to map IP addresses to MAC addresses. When a device needs to communicate with an IP address, it sends an ARP request to discover the corresponding MAC address. In the case of an IP address conflict, ARP resolution becomes ambiguous, as multiple IP addresses are associated with the same MAC address.

Network Disruptions:

Network disruptions and connectivity problems can occur. Devices may receive packets that they did not expect, leading to confusion and potential network instability.

Unreliable Routing:

Routers and switches may encounter difficulties in forwarding packets correctly. The presence of conflicting IP addresses can lead to incorrect routing decisions, affecting the overall reliability and performance of the network.

Duplicate IP Address Detection:

Some modern operating systems implement mechanisms for detecting duplicate IP addresses on the network. When a device detects a duplicate IP address, it may take action to resolve the conflict, such as sending warning messages or automatically disabling the network interface.

Intermittent Connectivity Issues:

Hosts with conflicting IP addresses may experience intermittent connectivity issues. The conflicting devices may intermittently lose

network connectivity, experience slow performance, or encounter other erratic behavior.

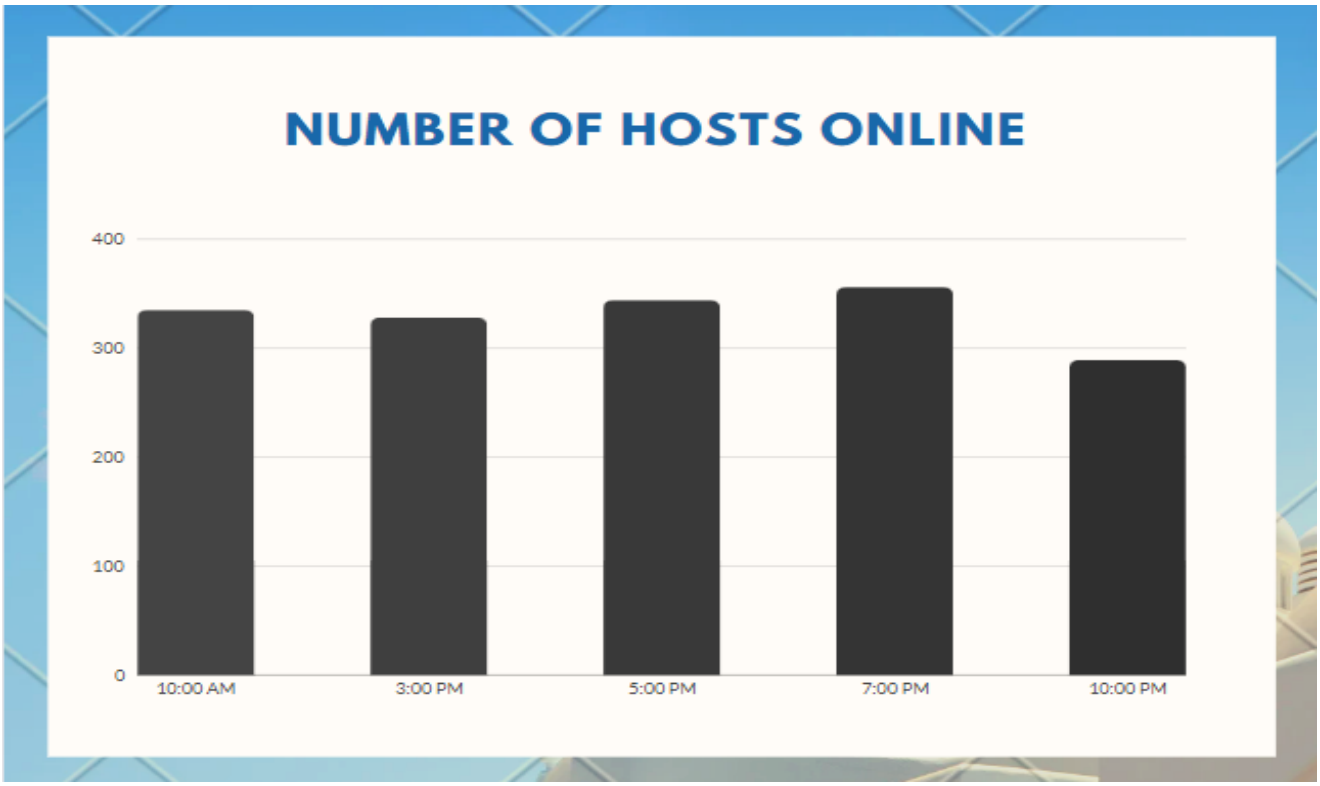
Troubleshooting Challenges:

Identifying the cause of network issues can be challenging because the conflict involves shared MAC addresses. Troubleshooting such problems may require careful examination of network configurations and ARP tables on affected devices.

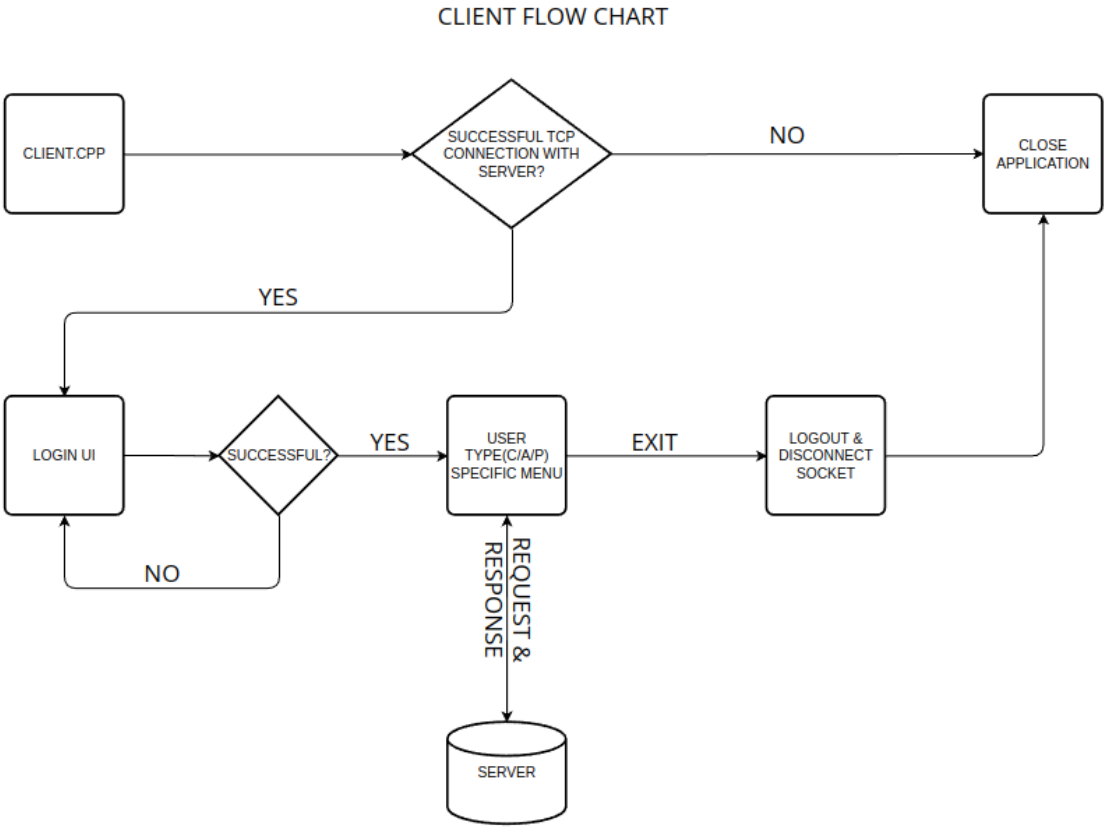
7)

- 10:00 AM → 335
- 3:00 PM → 328
- 5:00 PM → 344
- 7:00 PM → 356

- 10:00 PM → 289

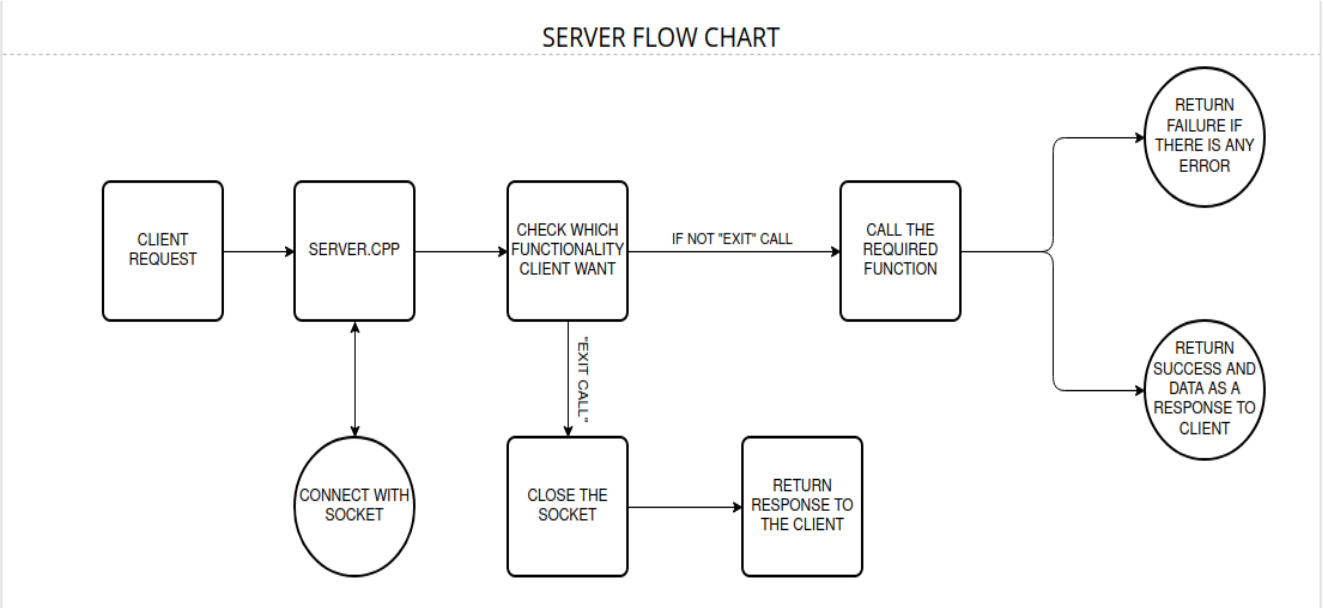


REPORT OF THE APPLICATION



CLIENT SIDE

- In client side we provide UI to the user to access the bank services.
- The **client.cpp** is the main program in client side.
- The **clientUtils.h** contains all the necessary functions to communicate with server (from establishing TCP connection to sending requests and receiving responses.



SERVER SIDE

- In server side we are maintaining the bussiness logic part and the database part of the application.
- There are three file in which we have written the bussiness logic code.

1. **admin.h** -> contain all the bussiness logic of admin like credit and debit balance of the customer.
2. **user.h** -> contain all the bussiness logic of customer like get available balance or mini statement.
3. **police.h** -> contain all the bussiness logic of police like get available balance of all the customer or get the mini statement of particular customer.

- There is also a **serverUtils.h** file which contain all the authentication part (LOGIN)

- **server.cpp** is the main file where the socket code is written, to accept the request of the client and provide the functionality according to the client type.