

CSE 232: Programming Assignment 3

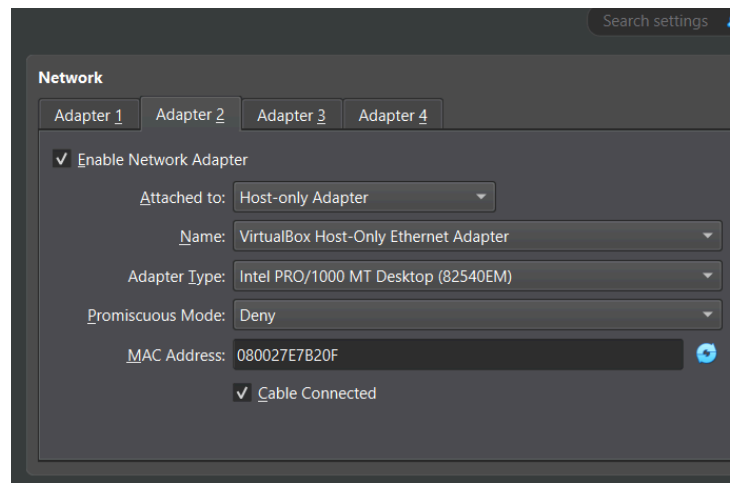
Using Linux iptables

By: **Subham Maurya, 2022510**

Q1)

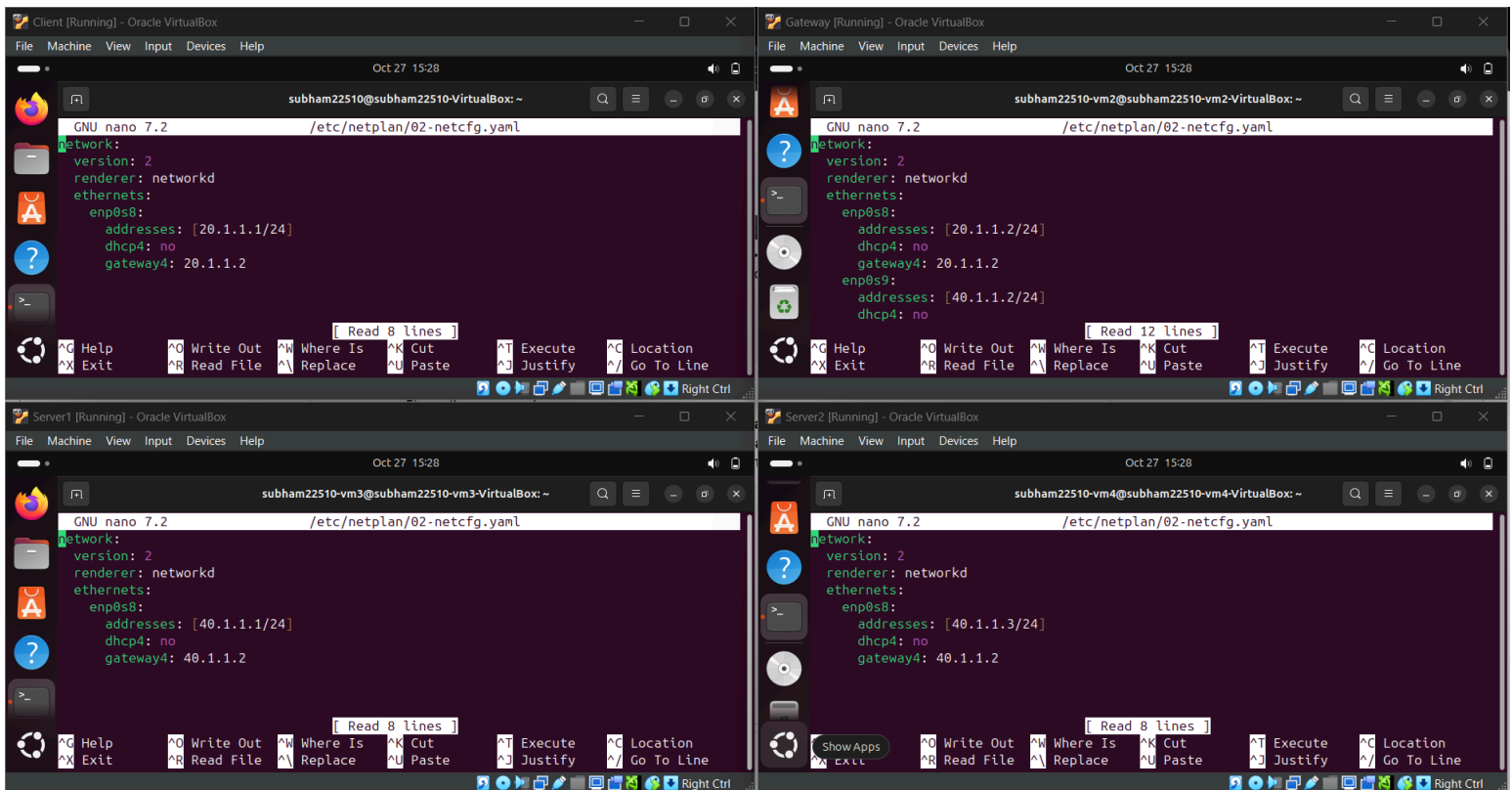
Steps to setup the environment:

1) use 4 VMs and enable the adapter 2 in all along with an additional adapter 3 in gateway.



2). Use “**ip a**” to find and “**ip link set <interface name> up**” command to activate the adapters.

3). Use “**sudo nano /etc/netplan/02-netcfg.yaml**” to edit and add the network adapter information along with their gateway.



4). After doing this use the commands on all 4 VMs::

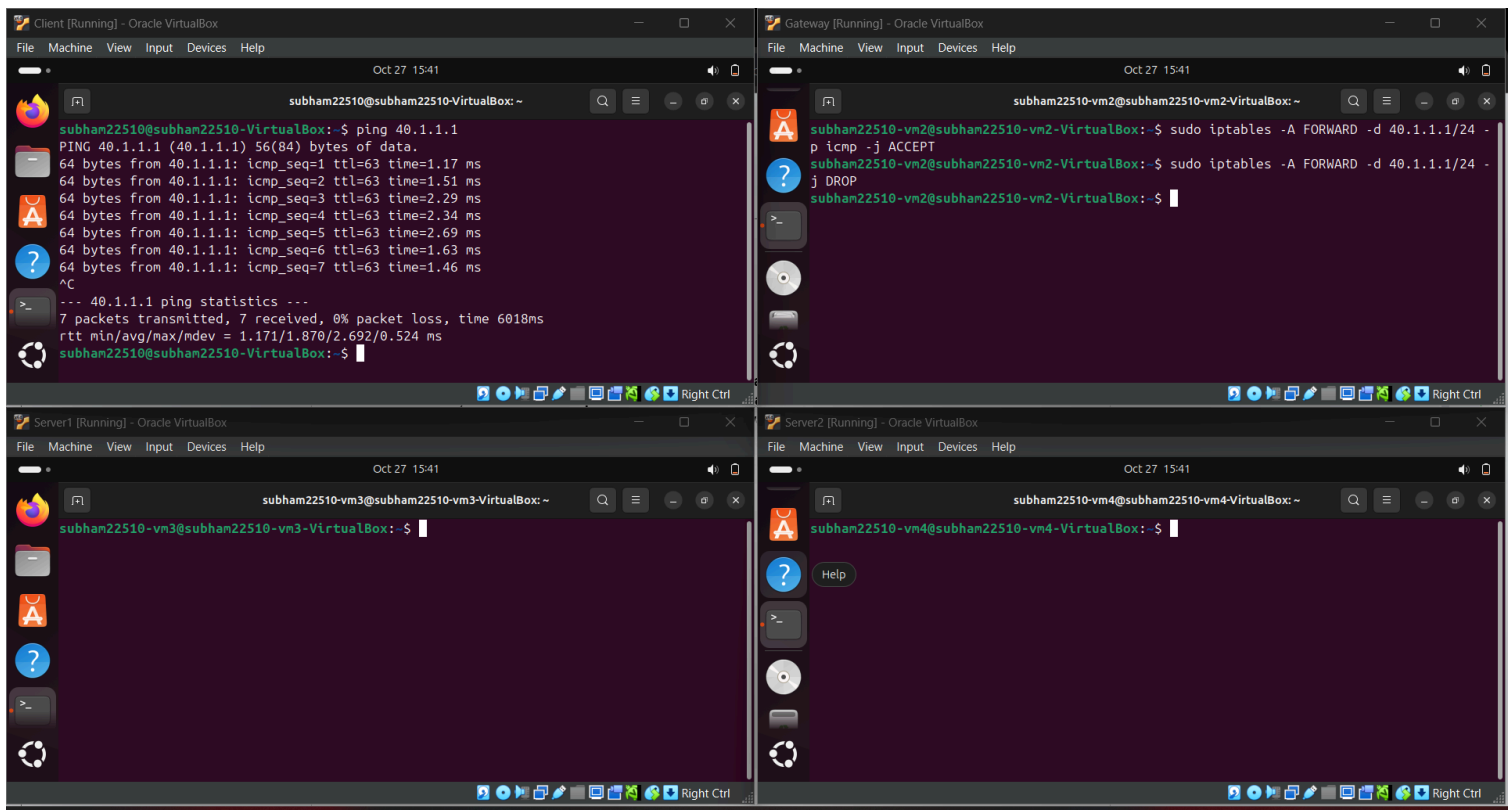
- **sudo netplan apply**
- **sudo reboot**

5) Finally use the commands:

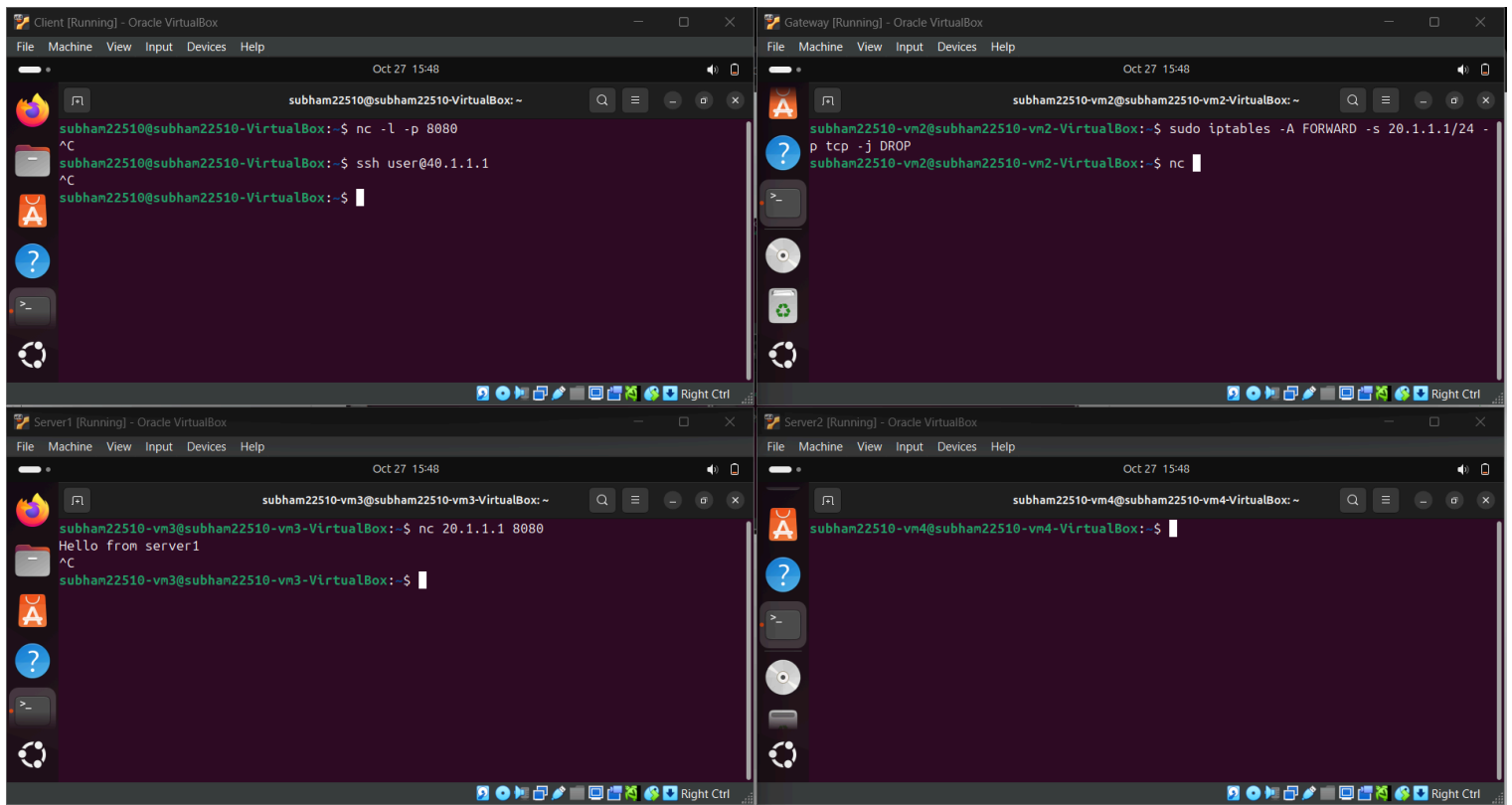
- i) on client: **sudo ip route add 40.1.1.0/24 via 20.1.1.2**
- ii) on servers: **sudo ip route add 20.1.1.0/24 via 40.1.1.2**
- iii) on client: **sudo sysctl -w net.ipv4.ip_forward=1**

Q2)

a).



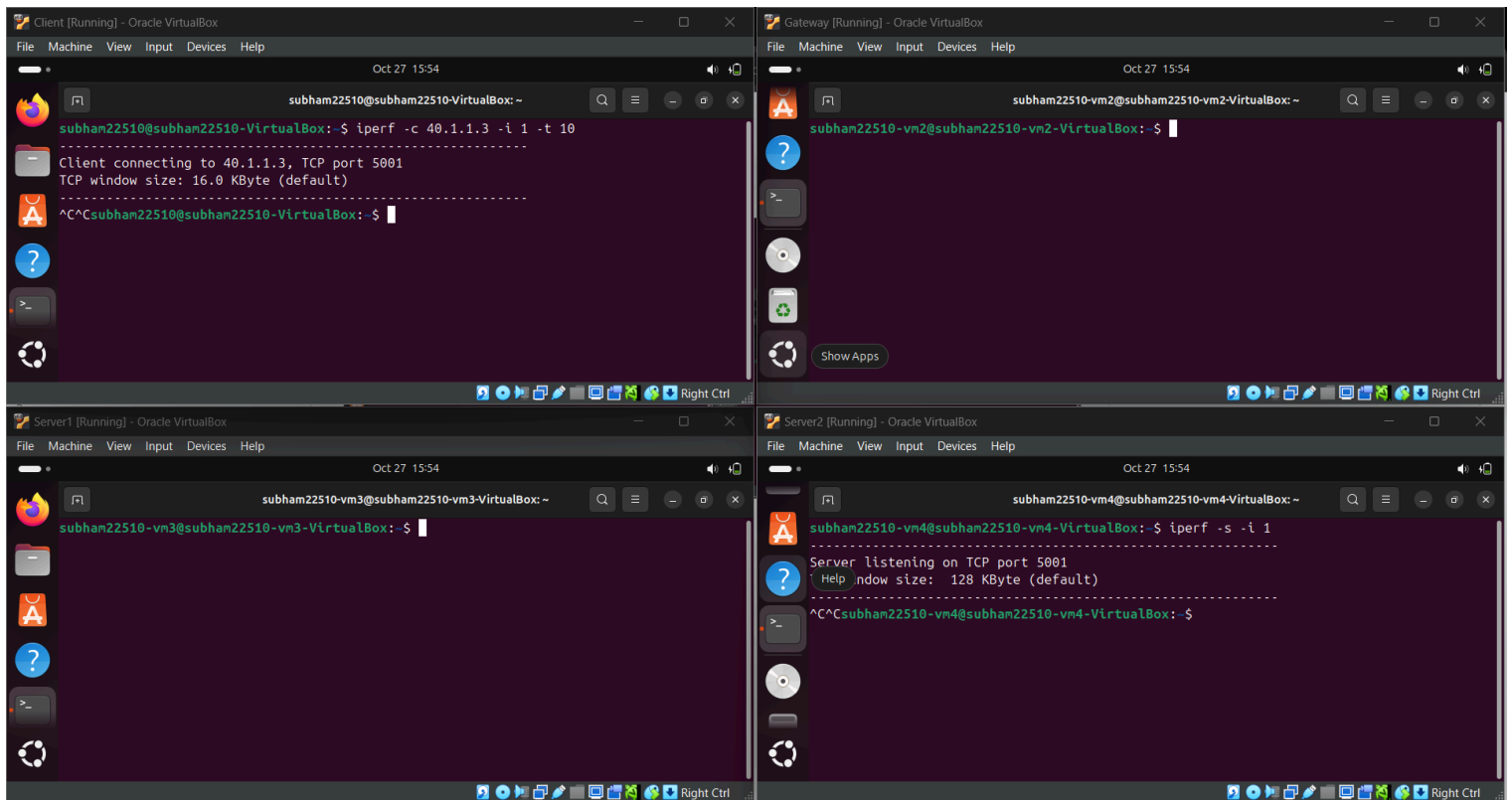
b).



Q3)

a).

TCP connection:



UCP Connection:

The image displays three separate Oracle VM VirtualBox windows, each containing a terminal window. The first window, titled 'Client [Running] - Oracle VirtualBox', shows a terminal session where a client connects to 40.1.1.3 on UDP port 5001. The output shows a successful connection with a transfer of 12.5 MBytes and a bandwidth of 10.5 Mbits/sec. The second window, titled 'Gateway [Running] - Oracle VirtualBox', shows a terminal session where a server listens on TCP port 5001. The output shows the server is listening on TCP port 5001 with a window size of 128 KByte. The third window, titled 'Server2 [Running] - Oracle VirtualBox', shows a terminal session where a client connects to 40.1.1.3 on TCP port 5001. The output shows a successful connection with a transfer of 12.5 MBytes and a bandwidth of 10.5 Mbits/sec.

b).

(i).

```
subham22510@subham22510-VirtualBox:~$ ping -c 10 40.1.1.1
PING 40.1.1.1 (40.1.1.1) 56(84) bytes of data.
64 bytes from 40.1.1.1: icmp_seq=1 ttl=63 time=1.88 ms
64 bytes from 40.1.1.1: icmp_seq=2 ttl=63 time=1.09 ms
64 bytes from 40.1.1.1: icmp_seq=3 ttl=63 time=2.50 ms
64 bytes from 40.1.1.1: icmp_seq=4 ttl=63 time=3.56 ms
64 bytes from 40.1.1.1: icmp_seq=5 ttl=63 time=2.87 ms
64 bytes from 40.1.1.1: icmp_seq=6 ttl=63 time=1.02 ms
64 bytes from 40.1.1.1: icmp_seq=7 ttl=63 time=1.12 ms
64 bytes from 40.1.1.1: icmp_seq=8 ttl=63 time=1.34 ms
64 bytes from 40.1.1.1: icmp_seq=9 ttl=63 time=2.62 ms
64 bytes from 40.1.1.1: icmp_seq=10 ttl=63 time=2.01 ms

--- 40.1.1.1 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9019ms
rtt min/avg/max/mdev = 1.015/1.999/3.559/0.827 ms
```

(ii).

```
subham22510@subham22510-VirtualBox:~$ ping -c 10 40.1.1.3
PING 40.1.1.3 (40.1.1.3) 56(84) bytes of data.
64 bytes from 40.1.1.3: icmp_seq=1 ttl=63 time=1.99 ms
64 bytes from 40.1.1.3: icmp_seq=2 ttl=63 time=1.91 ms
64 bytes from 40.1.1.3: icmp_seq=3 ttl=63 time=2.53 ms
64 bytes from 40.1.1.3: icmp_seq=4 ttl=63 time=2.25 ms
64 bytes from 40.1.1.3: icmp_seq=5 ttl=63 time=2.90 ms
64 bytes from 40.1.1.3: icmp_seq=6 ttl=63 time=2.65 ms
64 bytes from 40.1.1.3: icmp_seq=7 ttl=63 time=2.77 ms
64 bytes from 40.1.1.3: icmp_seq=8 ttl=63 time=1.43 ms
64 bytes from 40.1.1.3: icmp_seq=9 ttl=63 time=2.35 ms
64 bytes from 40.1.1.3: icmp_seq=10 ttl=63 time=2.52 ms

--- 40.1.1.3 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9042ms
rtt min/avg/max/mdev = 1.425/2.329/2.903/0.426 ms
```

(iii). Yes, there is very small difference between (i) and (ii) that indicates RTT time for (i) is less than (ii) because the iptables for gateway have two forwarding commands, one for accepting icmp ping request and second for dropping/blocking all other traffic for server1. Hence when a ping command is issued for server1 then it takes only the one iteration of iptables to allow that command to move forward while for server2 it takes complete two iterations of the iptables to move forward which eventually increases its RTT by very small amount.

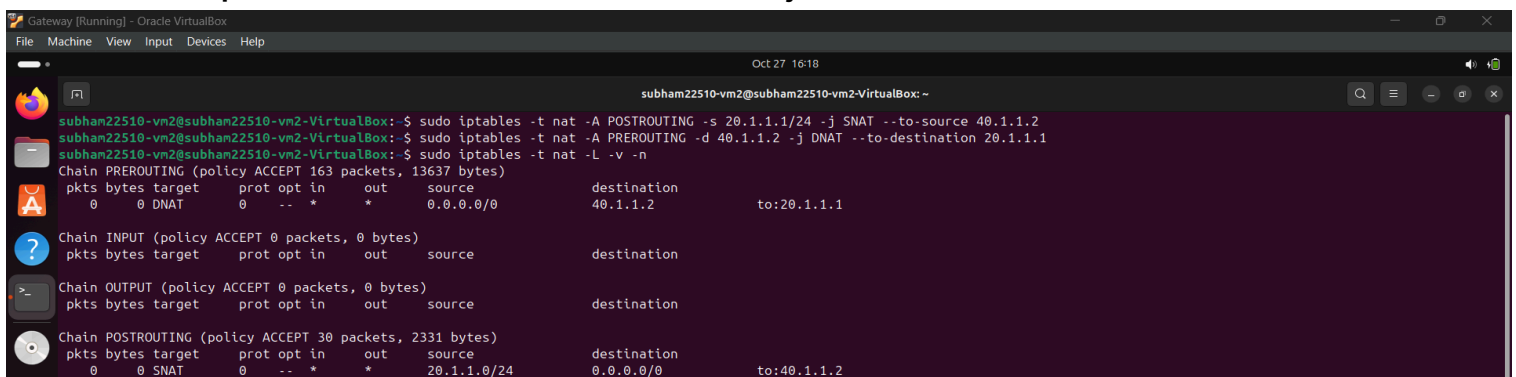
Q4).

a). Use this command on gateway:

“sudo iptables -t nat -A POSTROUTING -s 20.1.1.1/24 -j SNAT --to-source 40.1.1.2”

b). Use this command on gateway:

“sudo iptables -t nat -A PREROUTING -d 40.1.1.2 -j DNAT --to-destination 20.1.1.1”



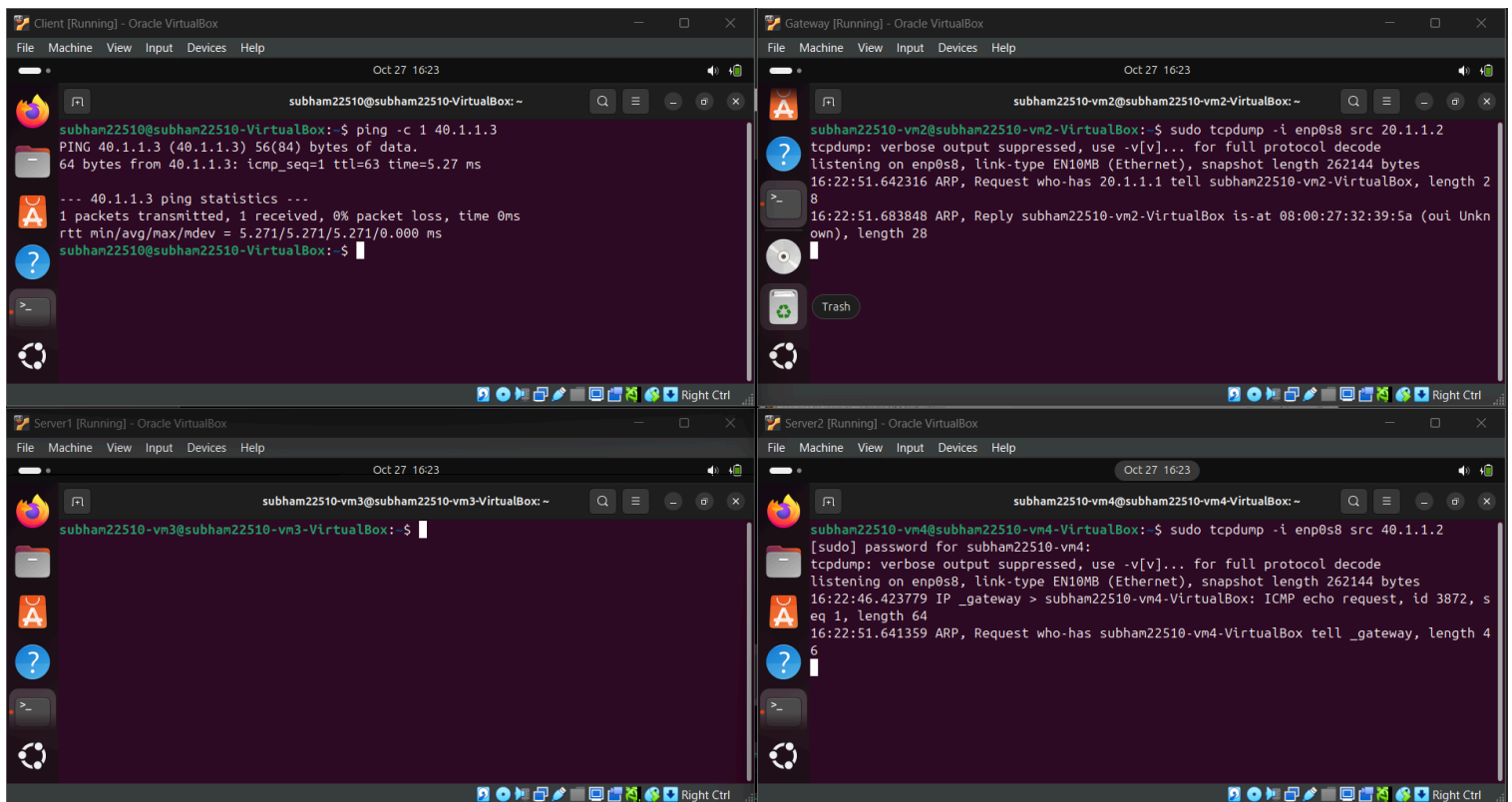
```
subham22510-vm2@subham22510-vm2-VirtualBox: ~  
subham22510-vm2@subham22510-vm2-VirtualBox:~$ sudo iptables -t nat -A POSTROUTING -s 20.1.1.1/24 -j SNAT --to-source 40.1.1.2  
subham22510-vm2@subham22510-vm2-VirtualBox:~$ sudo iptables -t nat -A PREROUTING -d 40.1.1.2 -j DNAT --to-destination 20.1.1.1  
subham22510-vm2@subham22510-vm2-VirtualBox:~$ sudo iptables -t nat -L -v -n  
Chain PREROUTING (policy ACCEPT 163 packets, 13637 bytes)  
pkts bytes target prot opt in out source destination  
0 0 DNAT 0 -- * * 0.0.0.0/0 40.1.1.2 to:20.1.1.1  
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)  
pkts bytes target prot opt in out source destination  
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)  
pkts bytes target prot opt in out source destination  
Chain POSTROUTING (policy ACCEPT 30 packets, 2331 bytes)  
pkts bytes target prot opt in out source destination  
0 0 SNAT 0 -- * * 20.1.1.0/24 0.0.0.0/0 to:40.1.1.2
```

c).

Gateway command: **“sudo tcpdump -i enp0s8 src 20.1.1.2”**

Server2 command: **“sudo tcpdump -i enp0s8 src 40.1.1.2”**

Client command: **“ping -c 1 40.1.1.3”**



```
subham22510@subham22510-VirtualBox:~$ ping -c 1 40.1.1.3  
PING 40.1.1.3 (40.1.1.3) 56(84) bytes of data:  
64 bytes from 40.1.1.3: icmp_seq=1 ttl=63 time=5.27 ms  
--- 40.1.1.3 ping statistics ---  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 5.271/5.271/5.271/0.000 ms  
subham22510@subham22510-VirtualBox:~$  
  
subham22510-vm2@subham22510-vm2-VirtualBox:~$ sudo tcpdump -i enp0s8 src 20.1.1.2  
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode  
listening on enp0s8, link-type EN10MB (Ethernet), snapshot length 262144 bytes  
16:22:51.642316 ARP, Request who-has 20.1.1.1 tell subham22510-vm2-VirtualBox, length 28  
16:22:51.683848 ARP, Reply subham22510-vm2-VirtualBox is-at 08:00:27:32:39:5a (oui Unknown), length 28  
  
subham22510-vm3@subham22510-vm3-VirtualBox:~$  
  
subham22510-vm4@subham22510-vm4-VirtualBox:~$ sudo tcpdump -i enp0s8 src 40.1.1.2  
[sudo] password for subham22510-vm4:  
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode  
listening on enp0s8, link-type EN10MB (Ethernet), snapshot length 262144 bytes  
16:22:46.423779 IP_gateway > subham22510-vm4-VirtualBox: ICMP echo request, id 3872, seq 1, length 64  
16:22:51.641359 ARP, Request who-has subham22510-vm4-VirtualBox tell IP_gateway, length 46
```

Q5)

a).

From the observation of Q3 part B, server 1 has low RTT and server 2 has high RTT.

Hence, we will use 0.8 probability with server 1 and 0.2 with server 2.

```
Gateway [Running] - Oracle VirtualBox
File Machine View Input Devices Help

Oct 27 16:42

subham22510-vm2@subham22510-vm2-VirtualBox: ~
subham22510-vm2@subham22510-vm2-VirtualBox:~$ sudo iptables -t nat -A PREROUTING -s 20.1.1.1/24 -m statistic --mode random --probability 0.8 -j DNAT --to-destination 40.1.1.1
subham22510-vm2@subham22510-vm2-VirtualBox:~$ sudo iptables -t nat -A PREROUTING -s 20.1.1.1/24 -j DNAT --to-destination 40.1.1.3
subham22510-vm2@subham22510-vm2-VirtualBox:~$ sudo iptables -t nat -L -v -n
Chain PREROUTING (policy ACCEPT 177 packets, 16452 bytes)
 pkts bytes target     prot opt in     out     source                   destination
    0      0 DNAT       tcp  --  *      *       20.1.1.0/24             0.0.0.0/0
    0      0 DNAT       tcp  --  *      *       20.1.1.0/24             0.0.0.0/0
                                statistic mode random probability 0.79999999981 to:40.1.1.1
                                to:40.1.1.3
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source                   destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source                   destination
Chain POSTROUTING (policy ACCEPT 44 packets, 3373 bytes)
 pkts bytes target     prot opt in     out     source                   destination
subham22510-vm2@subham22510-vm2-VirtualBox:~$
```

b).

```
Client [Running] - Oracle VirtualBox
File Machine View Input Devices Help

Oct 27 16:47

subham22510@subham22510-VirtualBox: ~
subham22510@subham22510-VirtualBox:~$ ping -c 1 20.1.1.2
PING 20.1.1.2 (20.1.1.2) 56(84) bytes of data:
64 bytes from 20.1.1.2: icmp_seq=1 ttl=63 time=3.74 ms

--- 20.1.1.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/ndev = 3.735/3.735/3.735/0.000 ms
subham22510@subham22510-VirtualBox:~$ ping -c 1 20.1.1.2
PING 20.1.1.2 (20.1.1.2) 56(84) bytes of data:
64 bytes from 20.1.1.2: icmp_seq=1 ttl=63 time=3.02 ms

--- 20.1.1.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/ndev = 3.023/3.023/3.023/0.000 ms
subham22510@subham22510-VirtualBox:~$ ping -c 1 20.1.1.2
PING 20.1.1.2 (20.1.1.2) 56(84) bytes of data:
64 bytes from 20.1.1.2: icmp_seq=1 ttl=63 time=2.77 ms

--- 20.1.1.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/ndev = 2.770/2.770/2.770/0.000 ms
subham22510@subham22510-VirtualBox:~$ ping -c 1 20.1.1.2
PING 20.1.1.2 (20.1.1.2) 56(84) bytes of data:
64 bytes from 20.1.1.2: icmp_seq=1 ttl=63 time=2.66 ms

--- 20.1.1.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/ndev = 2.664/2.664/2.664/0.000 ms
subham22510@subham22510-VirtualBox:~$ ^C
subham22510@subham22510-VirtualBox:~$

Server1 [Running] - Oracle VirtualBox
File Machine View Input Devices Help

Oct 27 16:47

subham22510-vm3@subham22510-vm3-VirtualBox: ~
subham22510-vm3@subham22510-vm3-VirtualBox:~$ sudo tcpdump -i enp0s8 icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp0s8, link-type EN10MB (Ethernet), snapshot length 262144 bytes
16:46:51.113060 IP 20.1.1.1 > subham22510-vm3-VirtualBox: ICMP echo request, id 4047, s
eq 1, length 64
16:46:51.113104 IP subham22510-vm3-VirtualBox > 20.1.1.1: ICMP echo reply, id 4047, s
eq 1, length 64
16:46:54.120663 IP 20.1.1.1 > subham22510-vm3-VirtualBox: ICMP echo request, id 4049, s
eq 1, length 64
16:46:54.120694 IP subham22510-vm3-VirtualBox > 20.1.1.1: ICMP echo reply, id 4049, s
eq 1, length 64
16:46:55.344316 IP 20.1.1.1 > subham22510-vm3-VirtualBox: ICMP echo request, id 4050, s
eq 1, length 64
16:46:55.344341 IP subham22510-vm3-VirtualBox > 20.1.1.1: ICMP echo reply, id 4050, s
eq 1, length 64
^C
6 packets captured
6 packets received by filter
0 packets dropped by kernel
subham22510-vm3@subham22510-vm3-VirtualBox:~$

Server2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help

Oct 27 16:47

subham22510-vm4@subham22510-vm4-VirtualBox: ~
subham22510-vm4@subham22510-vm4-VirtualBox:~$ sudo tcpdump -i enp0s8 icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp0s8, link-type EN10MB (Ethernet), snapshot length 262144 bytes
16:46:52.858484 IP 20.1.1.1 > subham22510-vm4-VirtualBox: ICMP echo request, id 4048, s
eq 1, length 64
16:46:52.858520 IP subham22510-vm4-VirtualBox > 20.1.1.1: ICMP echo reply, id 4048, s
eq 1, length 64
^C
2 packets captured
2 packets received by filter
0 packets dropped by kernel
subham22510-vm4@subham22510-vm4-VirtualBox:~$
```