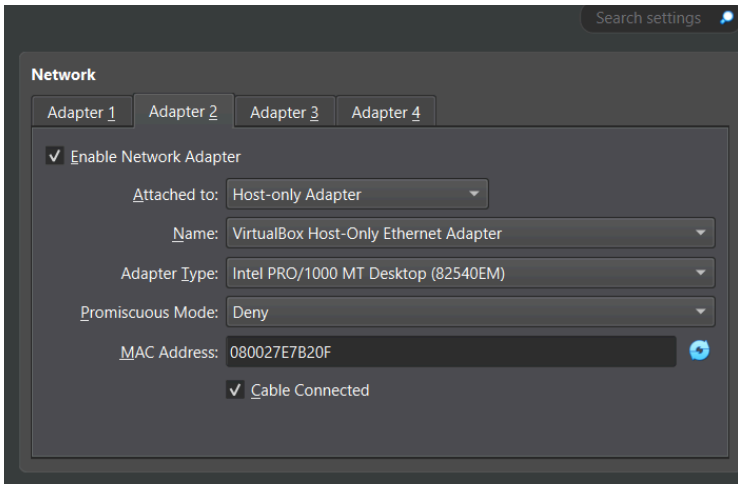
CSE 232: Programming Assignment 3
Using Linux iptables
By: Subham Maurya, 2022510

Q1)

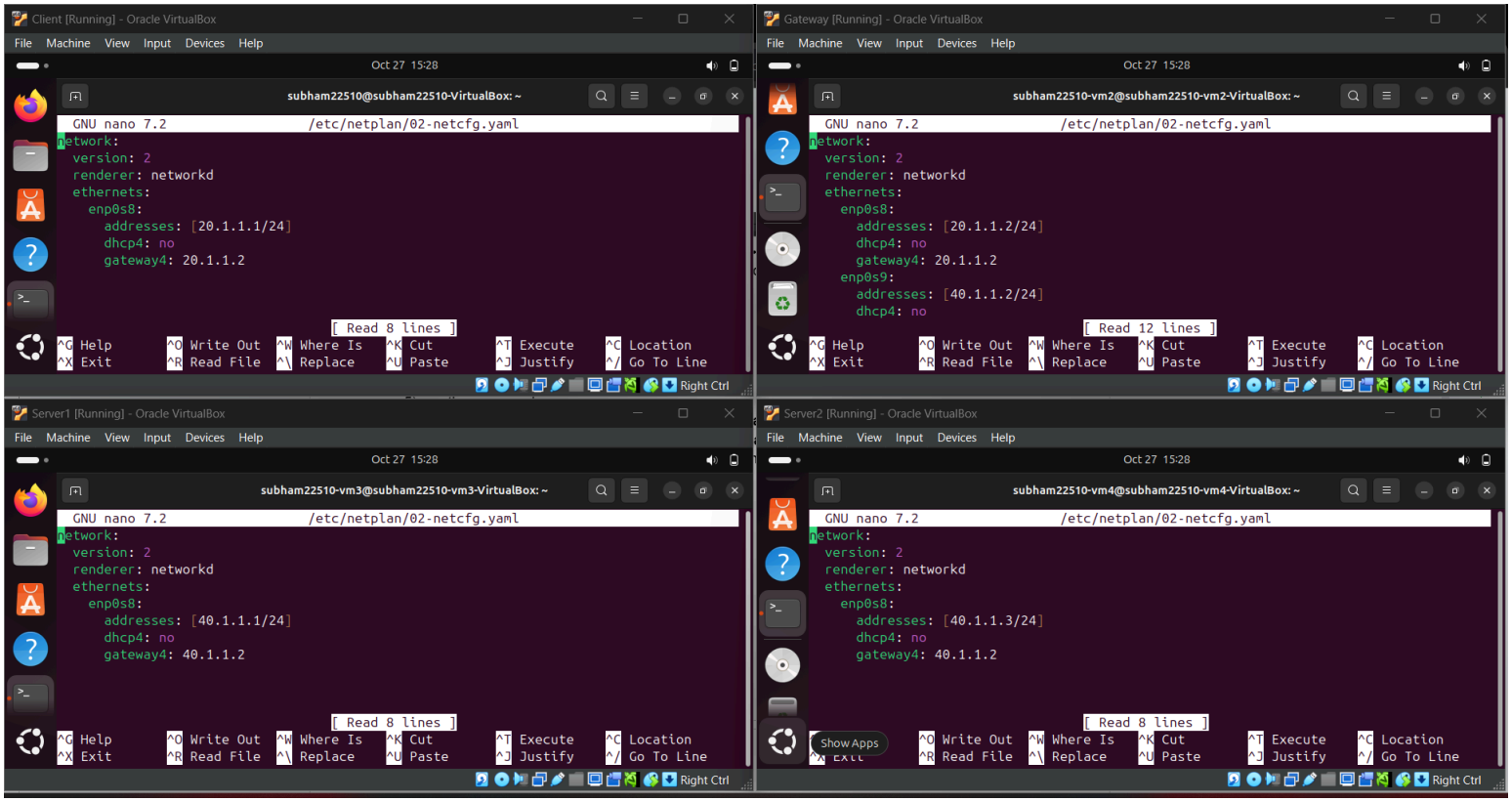
Steps to setup the environment:

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:

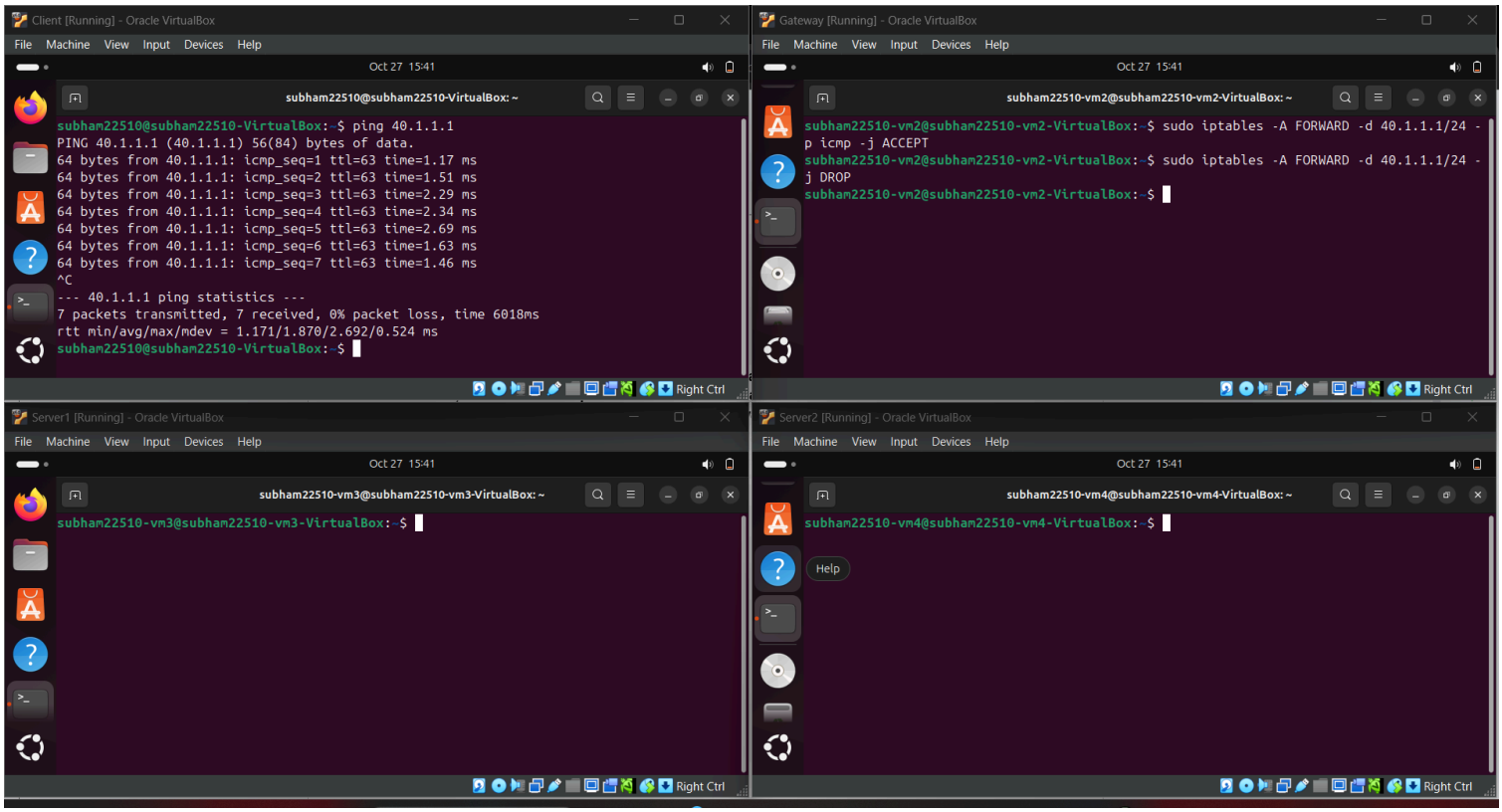
i) on client: **sudo ip route add 40.1.1.0/24 via 20.1.1.2**

ii) on servers: **sudo ip route add 20.1.1.0/24 via 40.1.1.2**

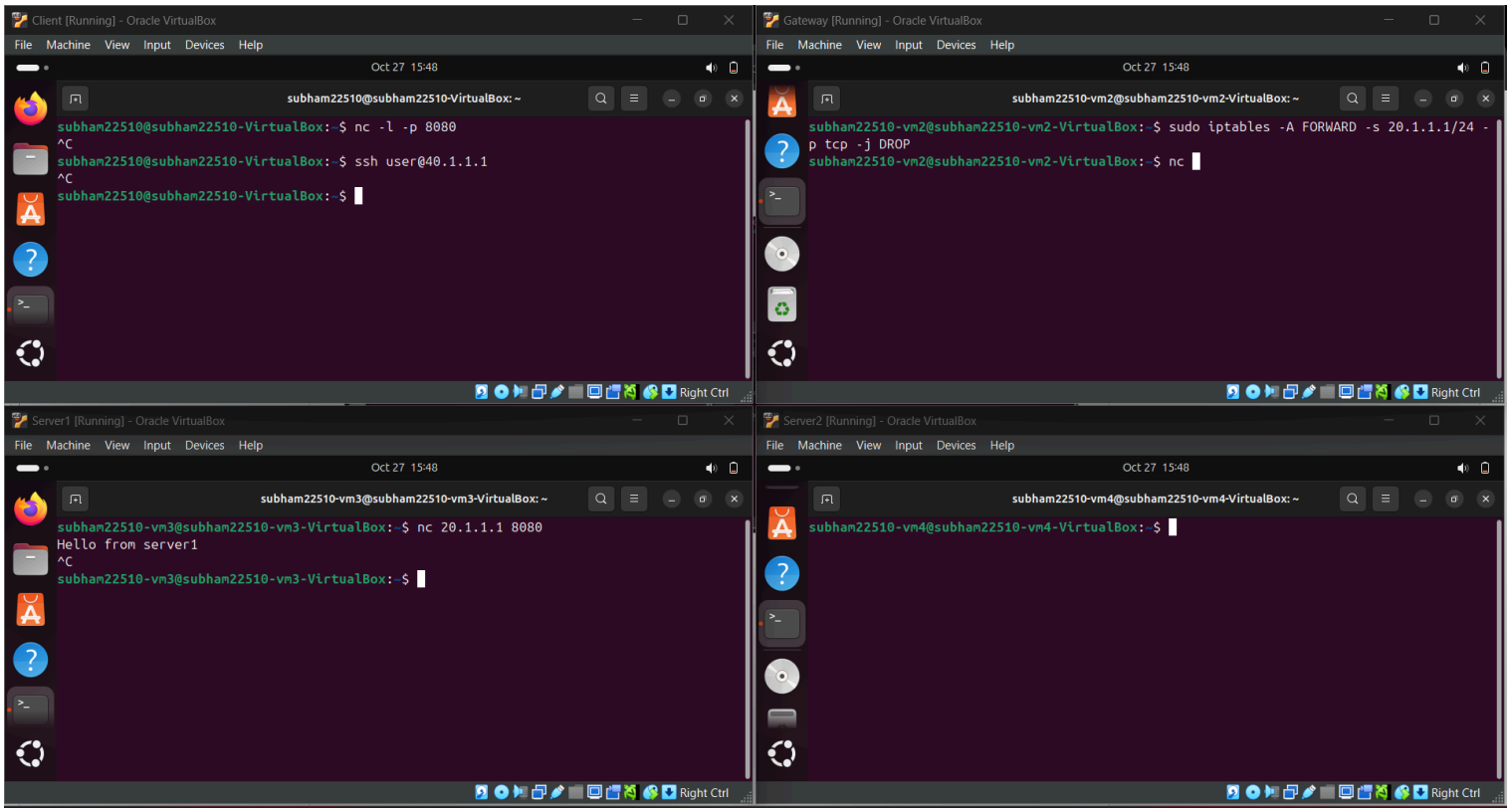
iii) on client: **sudo sysctl -w net.ipv4.ip_forward=1**

Q2)

a).



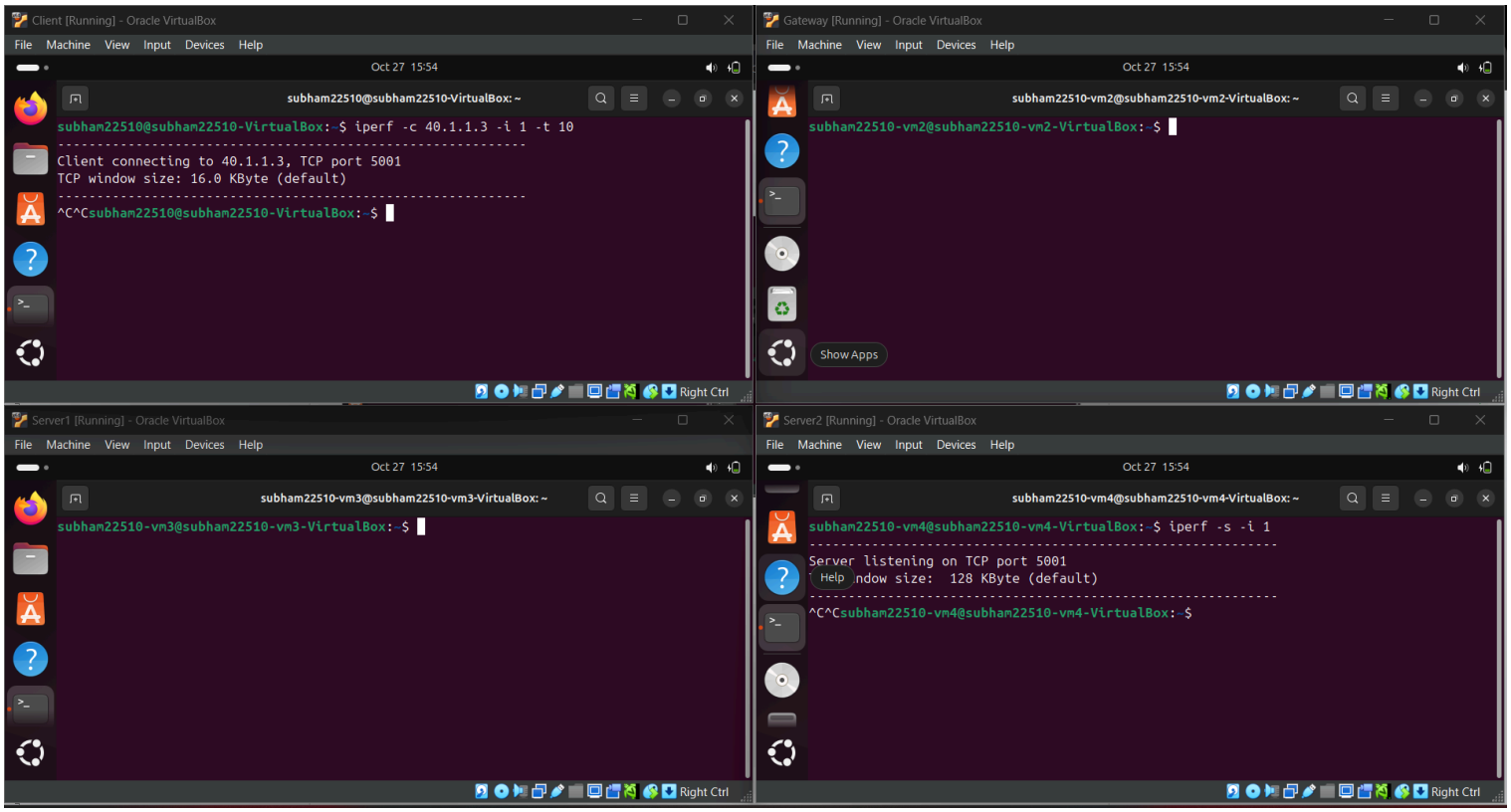
b).



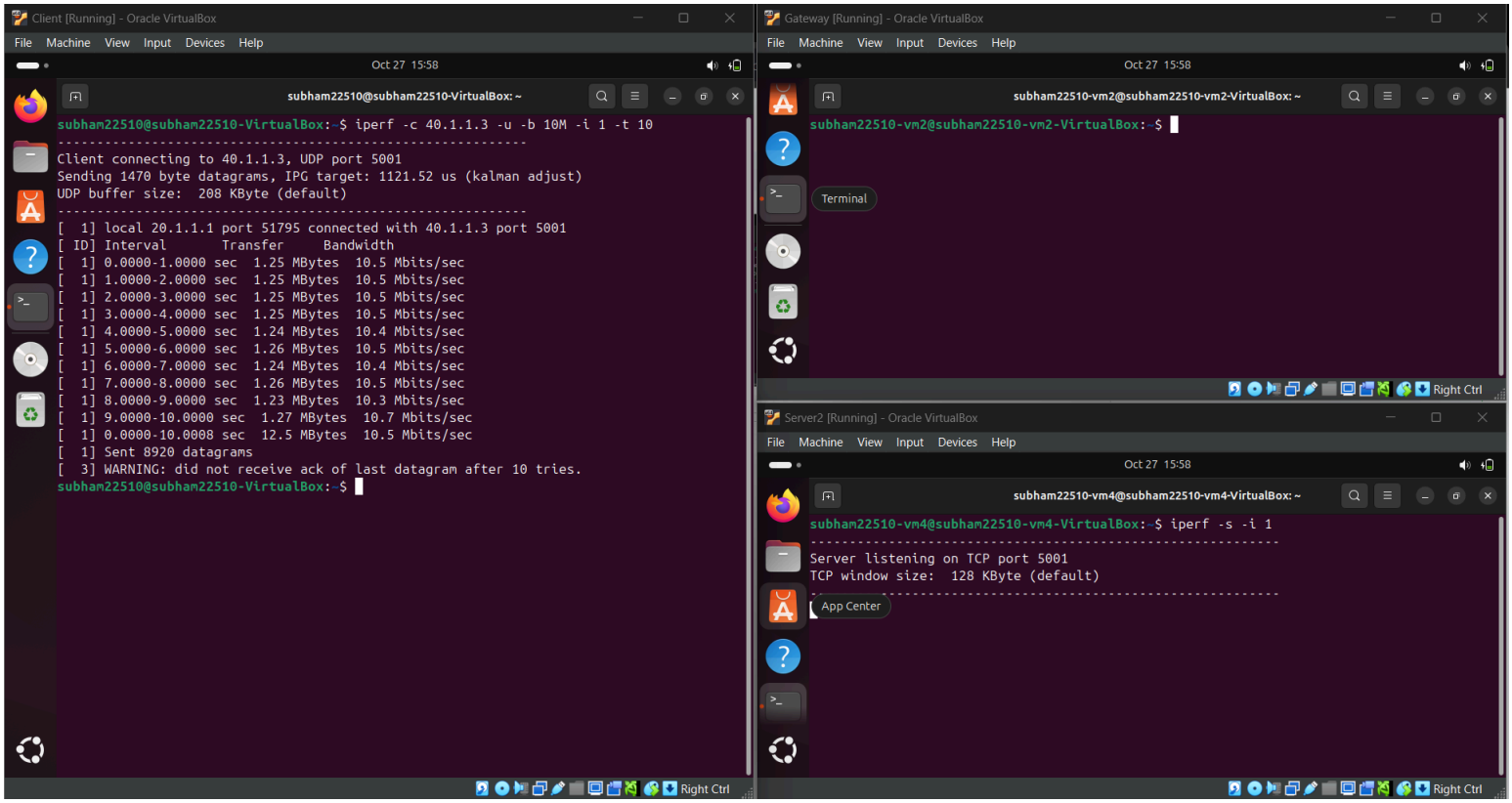
Q3)

a).

TCP connection:



UCP Connection:



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.

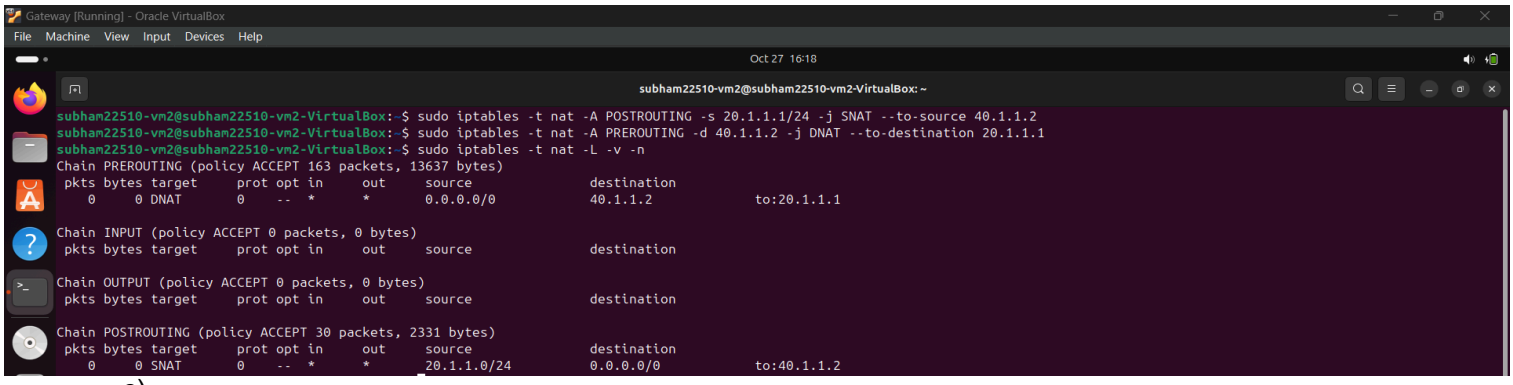
Q4).

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"

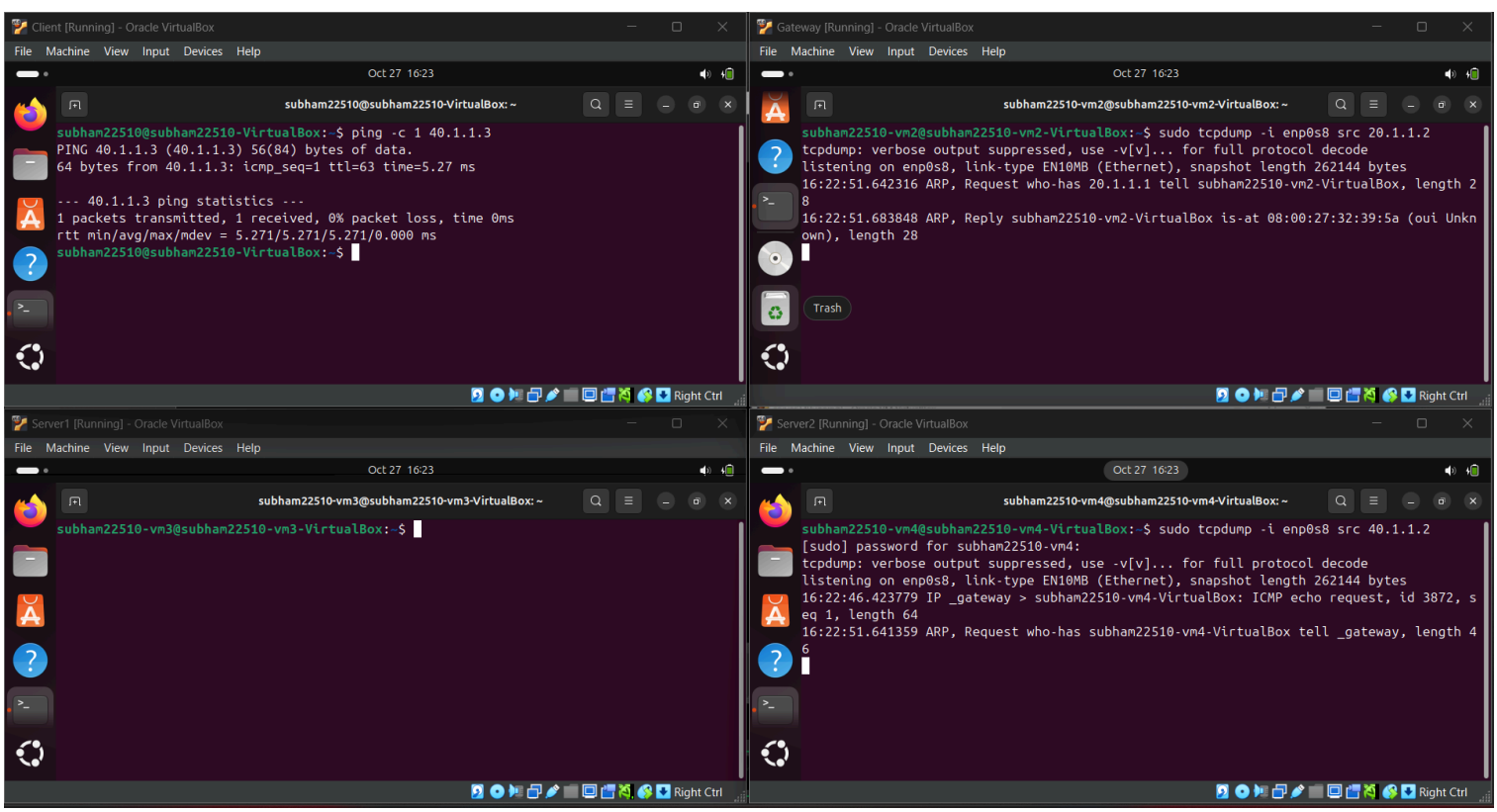


c).

Gateway command: **"sudo tcpdump -i enp0s8 src 20.1.1.2"**

Server2 command: **"sudo tcpdump -i enp0s8 src 40.1.1.2"**

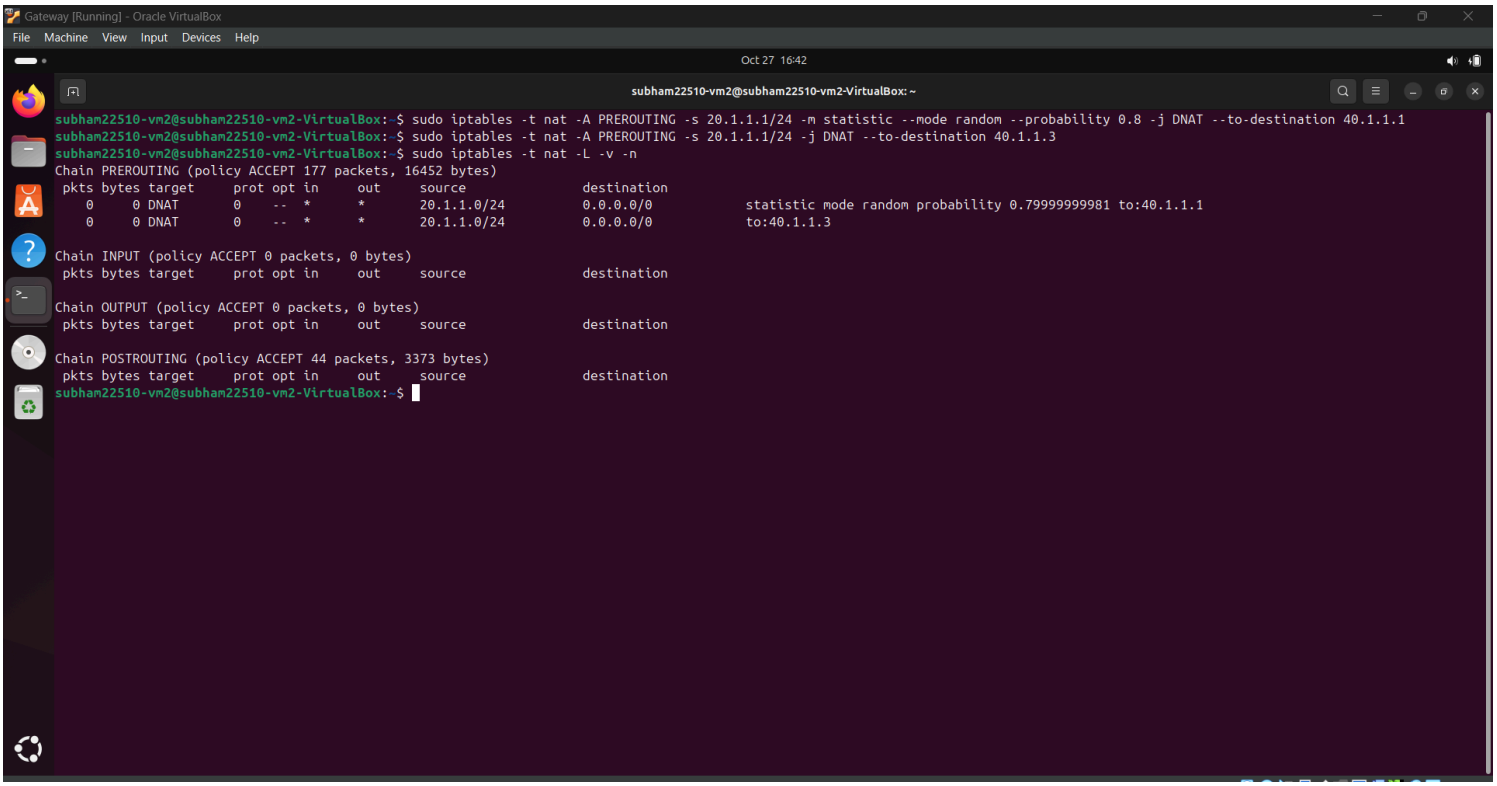
Client command: **"ping -c 1 40.1.1.3"**



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.



b).