CSE 232: Programming Assignment 3

Using Linux iptables

Due date: Oct 27, 2024

Total: 21 points

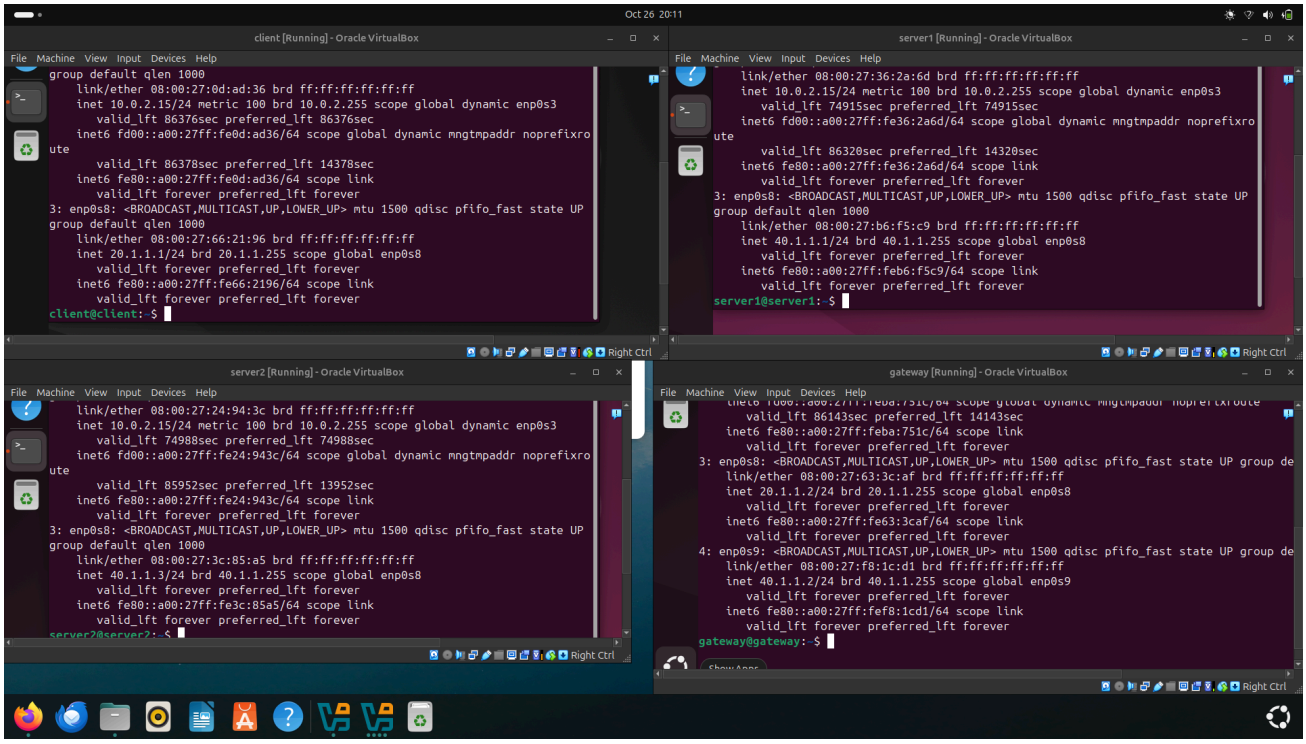
Ans 1

(a)

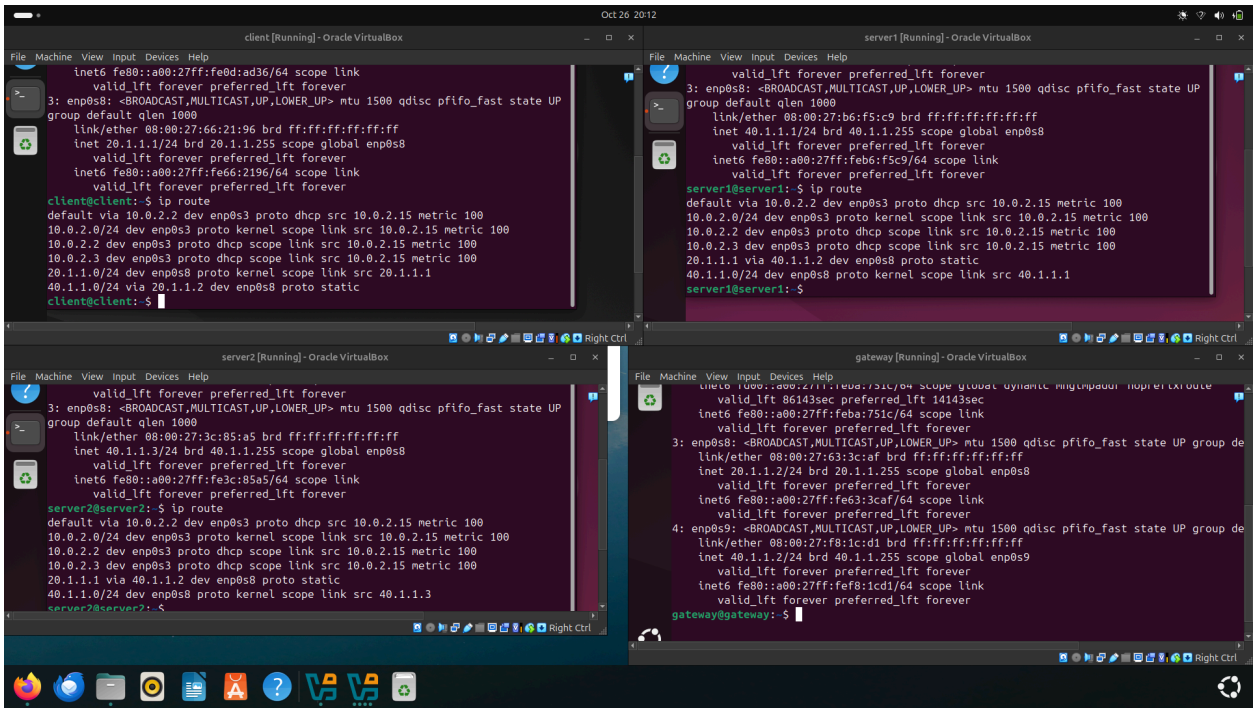
Set IPs for each VM as shown in the image:

- **Client: `20.1.1.1/24` with default route to `20.1.1.2`.**
- **Gateway VM: `20.1.1.2/24` on `enp0s8` (client side) and `40.1.1.2/24` on `enp0s9` (server side).**
- **Server 1: `40.1.1.1/24` with default route to `40.1.1.2`.**
- **Server 2: `40.1.1.3/24` with default route to `40.1.1.2`.**

Network Interface with desired IP Address.



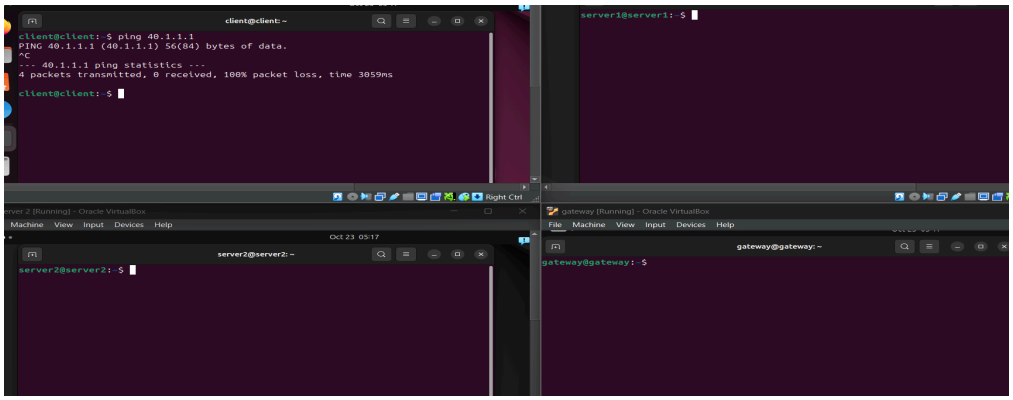
Routes for All VMs.



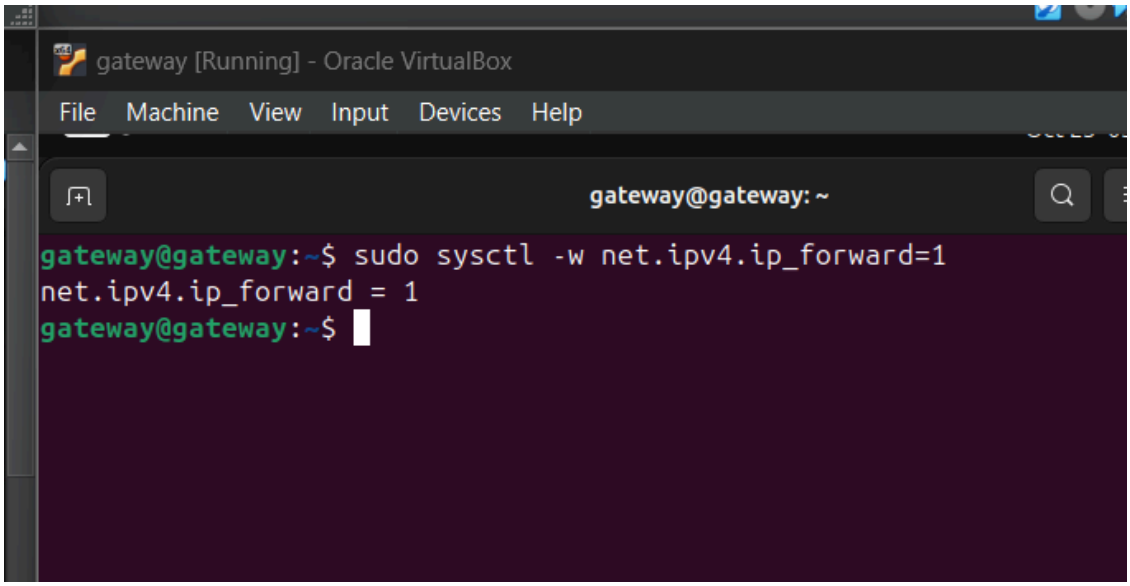
(b)

Stage 1: Attempt to Ping Server Before Enabling Forwarding

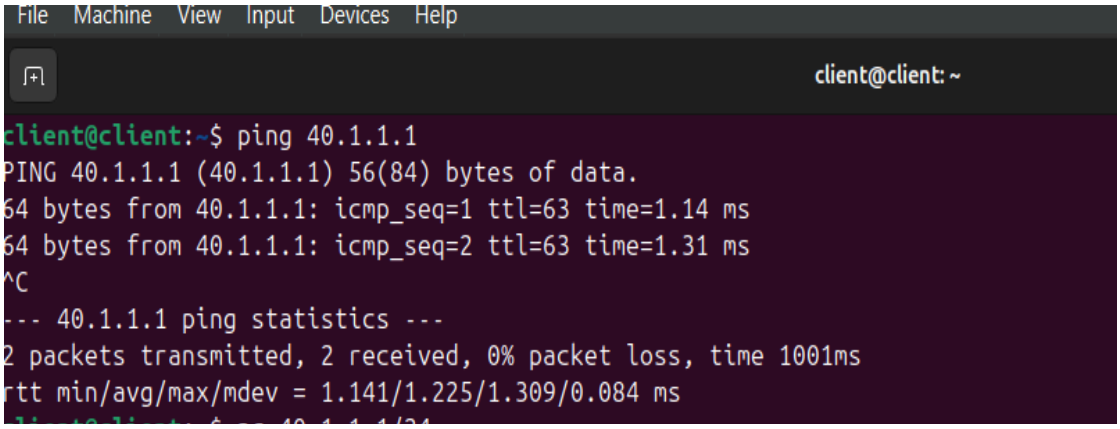
- **In this stage, client cannot reach Server 1 before IP forwarding is configured on the gateway**



Stage 2: Enable Forwarding and Successfully Ping Server



- **On the gateway, enable IP forwarding and configure `iptables` to allow traffic forwarding, as shown below:**



Ans 2
(a)

(a) Block All Traffic Except Ping to Server (40.1.1.1/24)

1. **Set up iptables to allow only ICMP (ping) traffic and block everything else to the `40.1.1.0/24` network:**

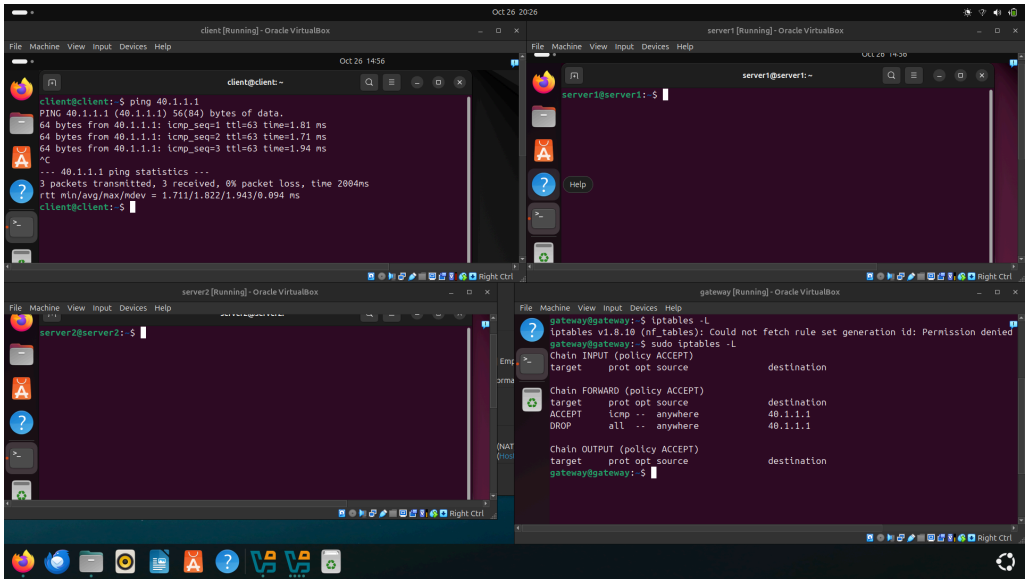
```
root@gateway: /home/gateway
gateway@gateway:/$ sudo iptables -A FORWARD -p icmp -d 40.1.1.1 -j ACCEPT
gateway@gateway:/$ sudo iptables -A FORWARD -d 40.1.1.1 -j DROP
gateway@gateway:/$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
ACCEPT     icmp --  anywhere             40.1.1.1
DROP       all  --  anywhere             40.1.1.1

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
gateway@gateway:/$
```

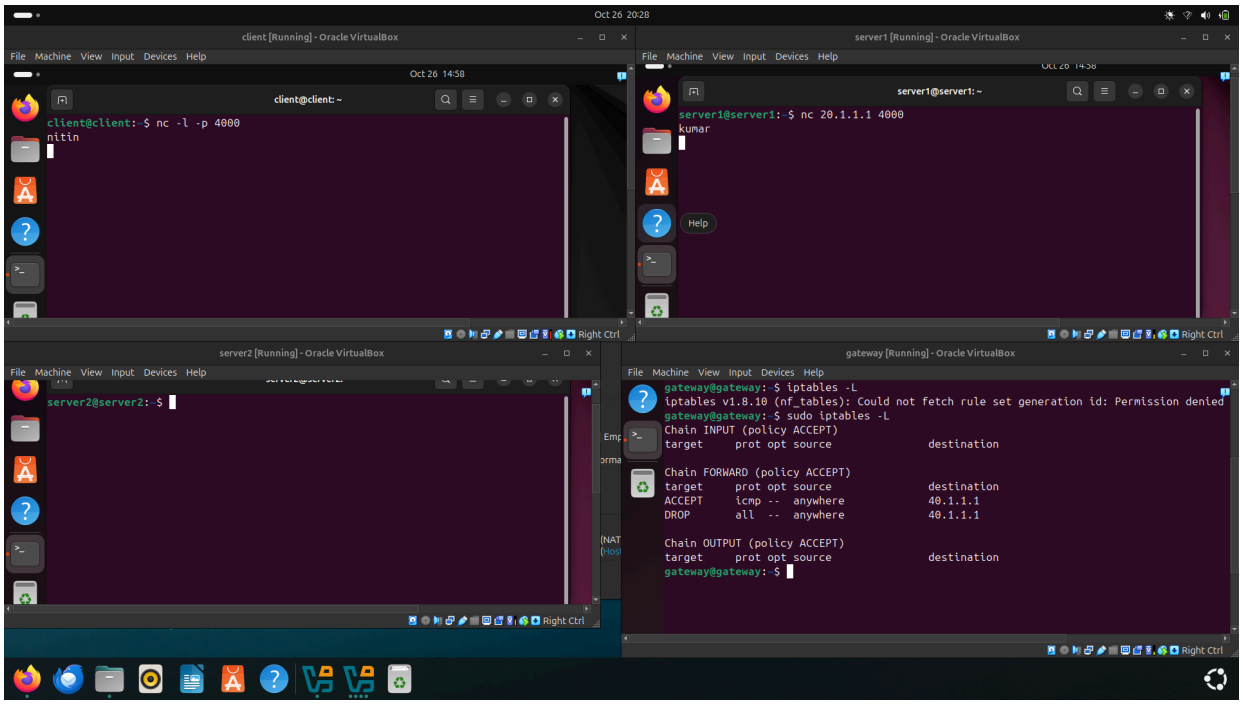
PROOF 1:

Showing ping working well in IMAGE GIVE BELOW:



PROOF 2:

Showing dropping tcp packets in IMAGE GIVE BELOW:



(b) Block Only TCP Traffic from 20.1.1.1/24

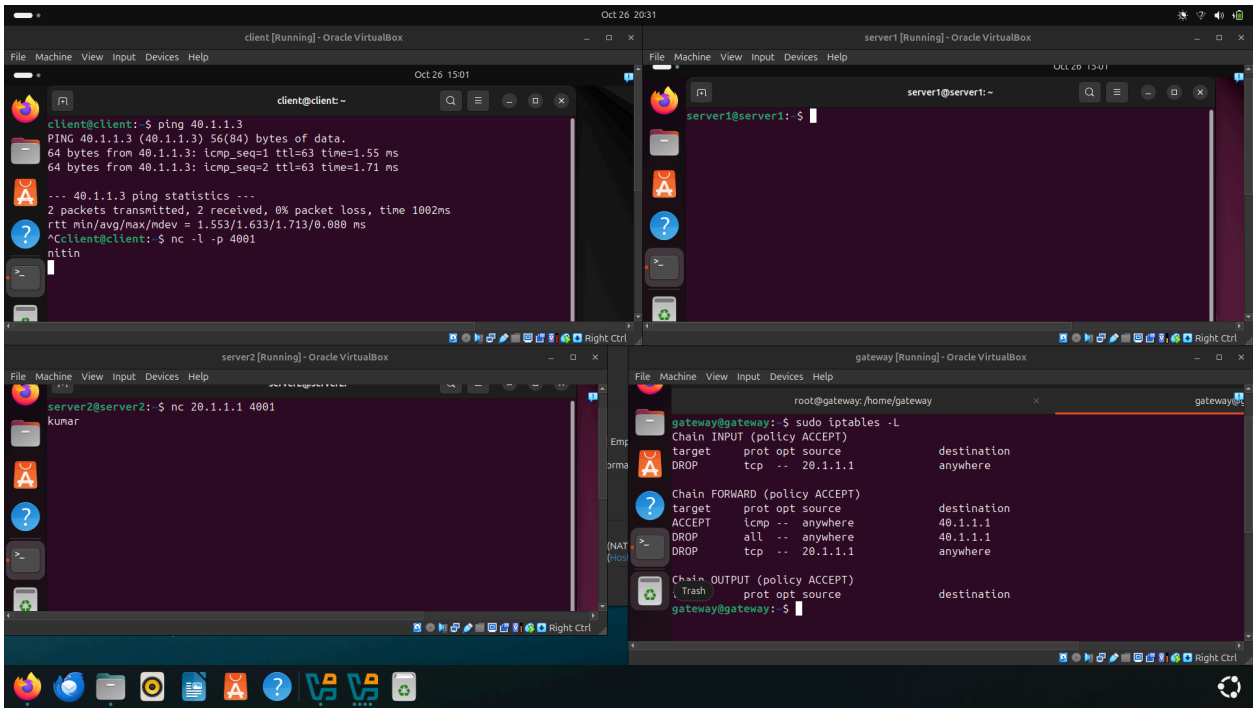
1. **Set up iptables to block only TCP traffic originating from the `20.1.1.0/24` network:**

```
target     prot opt source               destination
gateway@gateway:/$ sudo iptables -A INPUT -p tcp -s 20.1.1.1 -j DROP
gateway@gateway:/$ sudo iptables -A FORWARD -p tcp -s 20.1.1.1 -j DROP
gateway@gateway:/$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  20.1.1.1             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
ACCEPT     icmp --  anywhere             40.1.1.1
DROP       all  --  anywhere             40.1.1.1
DROP       tcp  --  20.1.1.1             anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
gateway@gateway:/$
```

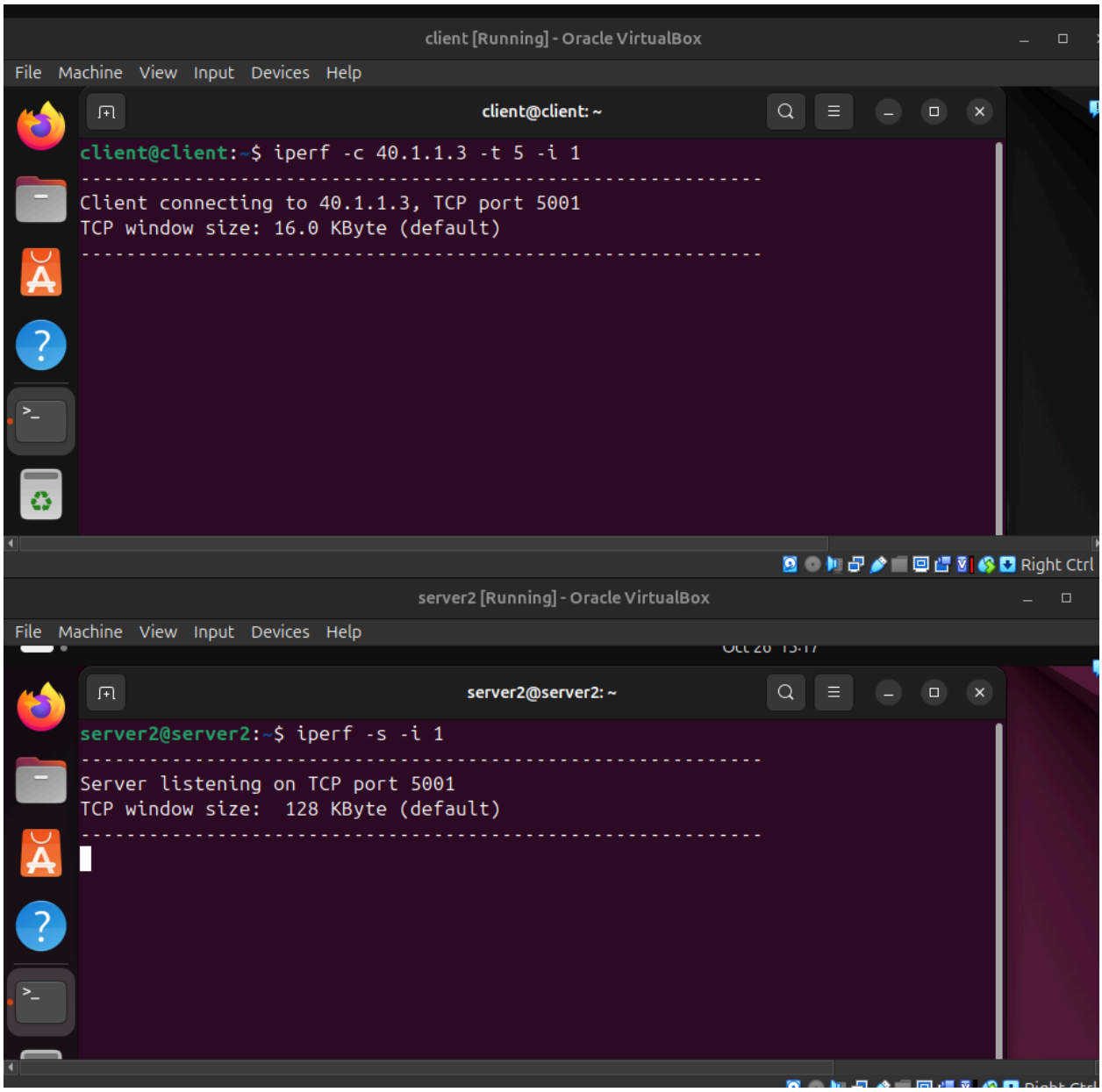
Proof:

- 

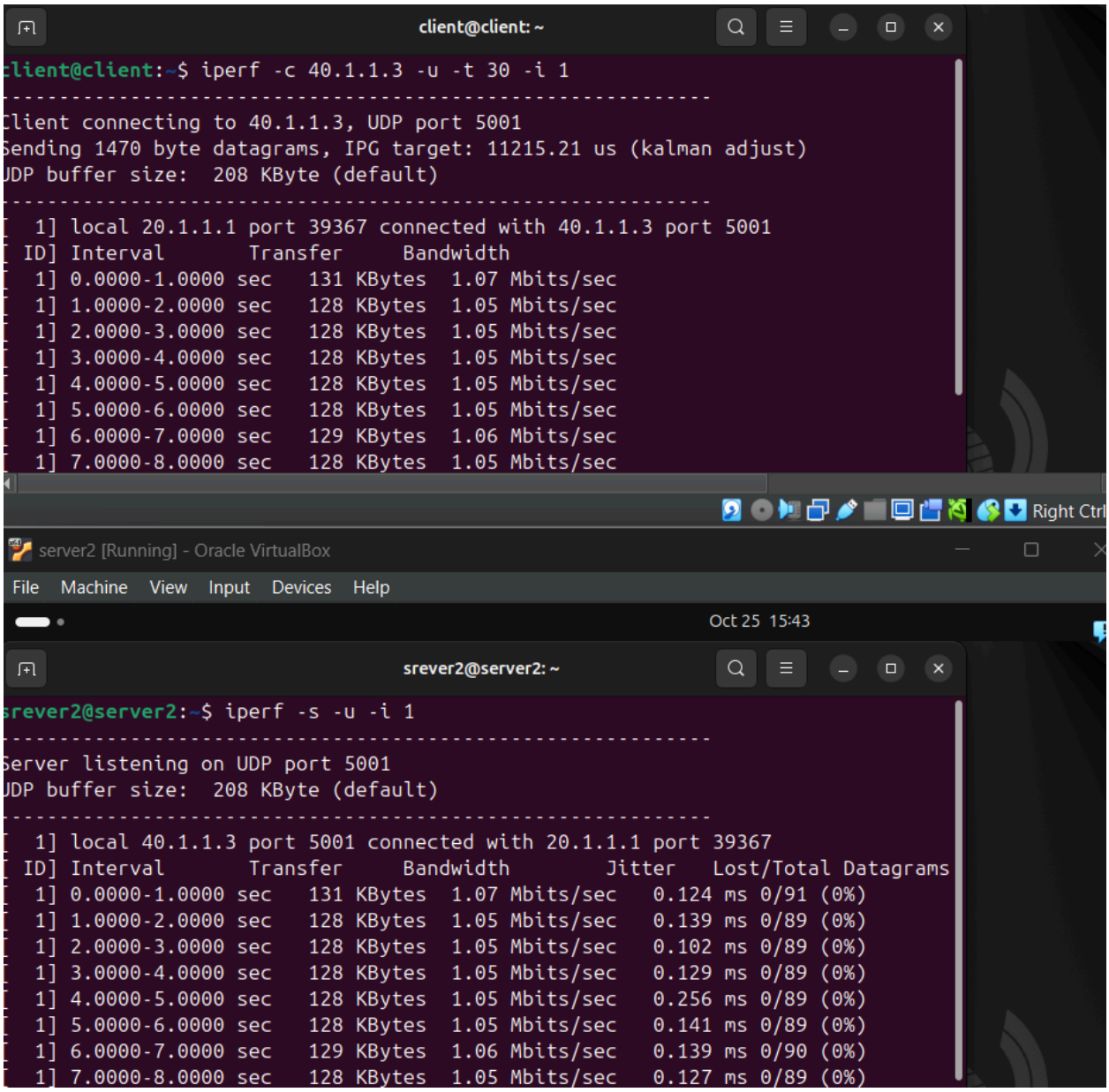
Ans 3

(a) Using iperf tools to test the tcp and udp bandwidth between 20.1.1.1/24 and 40.1.1.3/24

because tcp packets from client machine is blocked therefore the connection not established



as there is no restriction on udp packets from client therefore connection is established


client@client: ~
lient@client:~$ iperf -c 40.1.1.3 -u -t 30 -i 1
lient connecting to 40.1.1.3, UDP port 5001
ending 1470 byte datagrams, IPG target: 11215.21 us (kalman adjust)
DP buffer size: 208 KByte (default)
1] local 20.1.1.1 port 39367 connected with 40.1.1.3 port 5001
ID] Interval Transfer Bandwidth
1] 0.0000-1.0000 sec 131 KBytes 1.07 Mbits/sec
1] 1.0000-2.0000 sec 128 KBytes 1.05 Mbits/sec
1] 2.0000-3.0000 sec 128 KBytes 1.05 Mbits/sec
1] 3.0000-4.0000 sec 128 KBytes 1.05 Mbits/sec
1] 4.0000-5.0000 sec 128 KBytes 1.05 Mbits/sec
1] 5.0000-6.0000 sec 128 KBytes 1.05 Mbits/sec
1] 6.0000-7.0000 sec 129 KBytes 1.06 Mbits/sec
1] 7.0000-8.0000 sec 128 KBytes 1.05 Mbits/sec
Right Ctrl
server2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Oct 25 15:43
srever2@server2: ~
srever2@server2:~$ iperf -s -u -i 1
erver listening on UDP port 5001
DP buffer size: 208 KByte (default)
1] local 40.1.1.3 port 5001 connected with 20.1.1.1 port 39367
ID] Interval Transfer Bandwidth Jitter Lost/Total Datagrams
1] 0.0000-1.0000 sec 131 KBytes 1.07 Mbits/sec 0.124 ms 0/91 (0%)
1] 1.0000-2.0000 sec 128 KBytes 1.05 Mbits/sec 0.139 ms 0/89 (0%)
1] 2.0000-3.0000 sec 128 KBytes 1.05 Mbits/sec 0.102 ms 0/89 (0%)
1] 3.0000-4.0000 sec 128 KBytes 1.05 Mbits/sec 0.129 ms 0/89 (0%)
1] 4.0000-5.0000 sec 128 KBytes 1.05 Mbits/sec 0.256 ms 0/89 (0%)
1] 5.0000-6.0000 sec 128 KBytes 1.05 Mbits/sec 0.141 ms 0/89 (0%)
1] 6.0000-7.0000 sec 129 KBytes 1.06 Mbits/sec 0.139 ms 0/90 (0%)
1] 7.0000-8.0000 sec 128 KBytes 1.05 Mbits/sec 0.127 ms 0/89 (0%)

(b)

```
client@client:~$ ping 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=2.51 ms
64 bytes from 40.1.1.1: icmp_seq=2 ttl=63 time=1.74 ms
64 bytes from 40.1.1.1: icmp_seq=3 ttl=63 time=1.69 ms
64 bytes from 40.1.1.1: icmp_seq=4 ttl=63 time=1.81 ms
64 bytes from 40.1.1.1: icmp_seq=5 ttl=63 time=1.86 ms
64 bytes from 40.1.1.1: icmp_seq=6 ttl=63 time=1.55 ms
^C
--- 40.1.1.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5008ms
rtt min/avg/max/mdev = 1.546/1.857/2.506/0.306 ms
```

```
client@client:~$ ping 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=1.31 ms
64 bytes from 40.1.1.3: icmp_seq=2 ttl=63 time=1.20 ms
64 bytes from 40.1.1.3: icmp_seq=3 ttl=63 time=1.20 ms
64 bytes from 40.1.1.3: icmp_seq=4 ttl=63 time=1.03 ms
64 bytes from 40.1.1.3: icmp_seq=5 ttl=63 time=1.67 ms
^C
--- 40.1.1.3 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 1.030/1.281/1.668/0.212 ms
client@client:~$
```

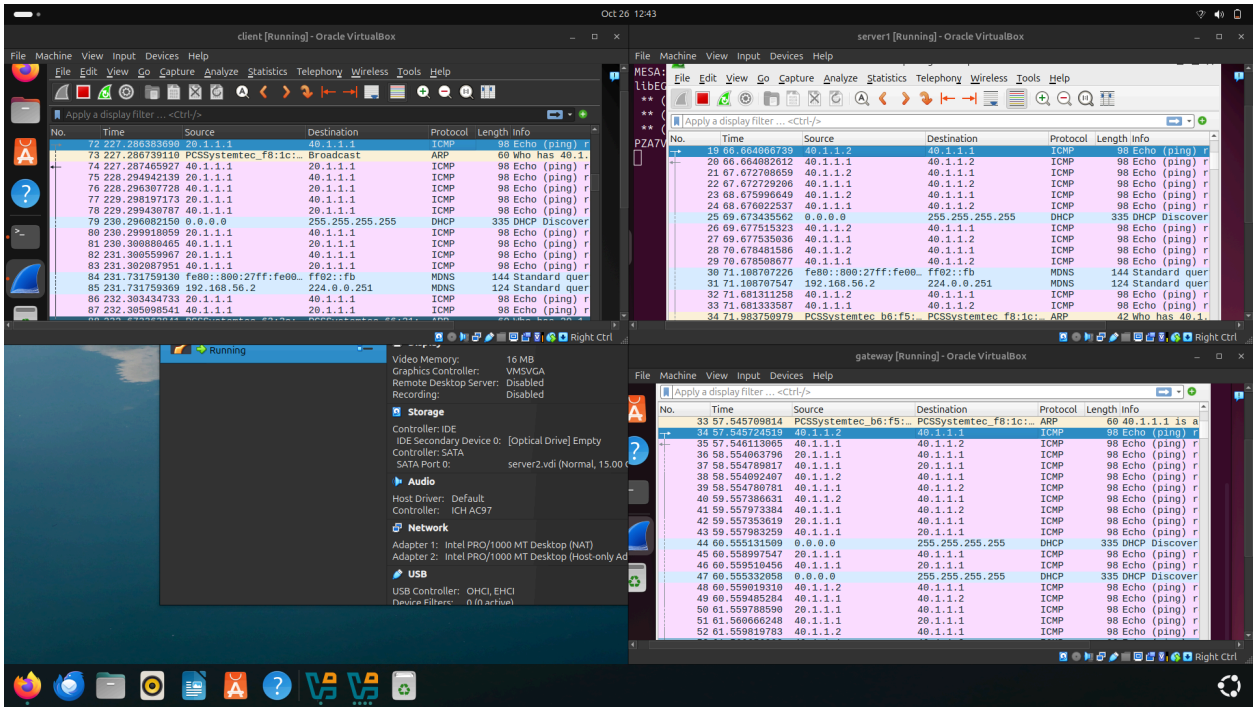
There is a clear difference between rtt in 40.1.1.1 and 40.1.1.3 because on the gateway there are processings going on for the 40.1.1.1 destination packets. Hence rtt for 40.1.1.3 is lower than 40.1.1.1 .

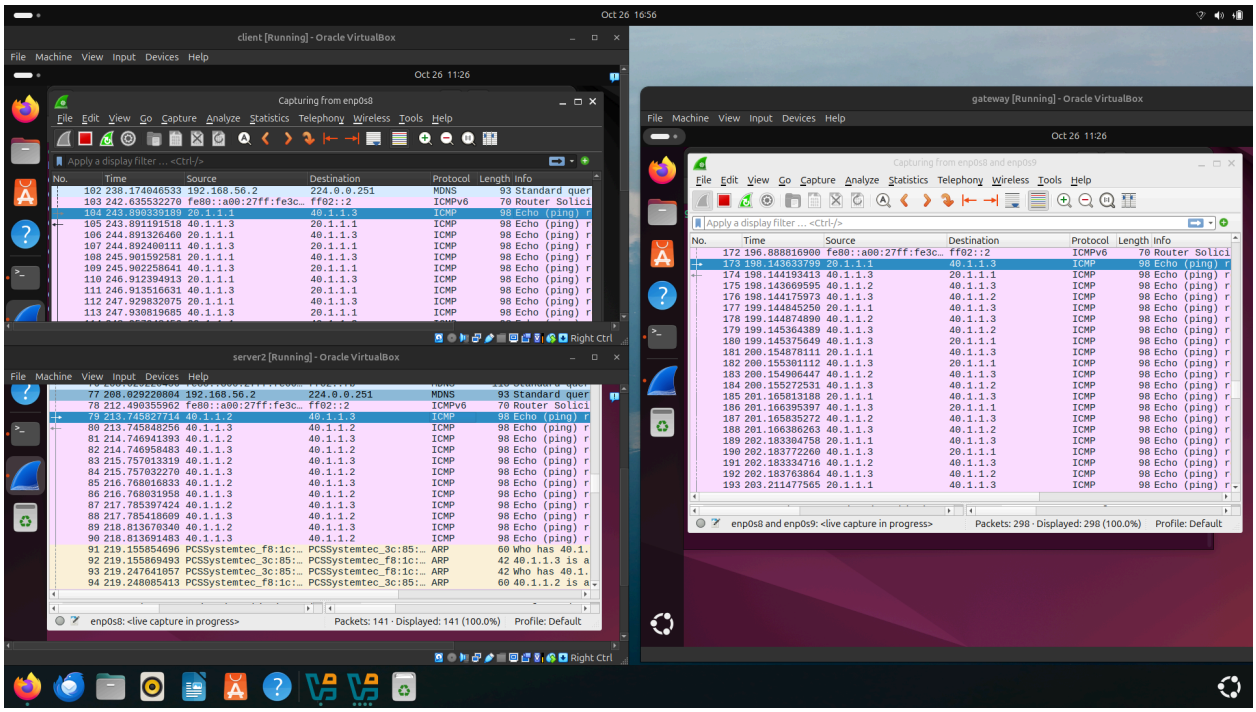
Q.4. Network address translation at the gateway VM **[4]**

(a) & (b) adding the DNAT and SNAT rules in iptables rules.

```
 GNU nano 7.2                                    iptablesrules.v4
:INPUT ACCEPT [666:130938]
:FORWARD ACCEPT [231:19086]
:OUTPUT ACCEPT [162:14595]
-A INPUT -s 20.1.1.1/32 -p tcp -j DROP
-A FORWARD -d 40.1.1.1/32 -p icmp -j ACCEPT
-A FORWARD -d 40.1.1.1/32 -j DROP
-A FORWARD -s 20.1.1.1/32 -p tcp -j DROP
COMMIT
# Completed on Sat Oct 26 14:47:45 2024
# Generated by iptables-save v1.8.10 (nf_tables) on Sat Oct 26 14:47:45 2024
*nat
:PREROUTING ACCEPT [38:3768]
:INPUT ACCEPT [37:3695]
:OUTPUT ACCEPT [75:5648]
:POSTROUTING ACCEPT [74:5575]
-A PREROUTING -d 40.1.1.0/24 -j DNAT --to-destination 20.1.1.1
#-A PREROUTING -d 20.1.1.2/32 -j DNAT --to-destination 40.1.1.3
#-A PREROUTING -d 20.1.1.2/32 -m statistic --mode random --probability 0.79999999
-A POSTROUTING -s 20.1.1.0/24 -j SNAT --to-source 40.1.1.2
COMMIT
```

(c)





Q.5. Load balancing at the gateway VM. Attach screenshots **[4]**

Ans

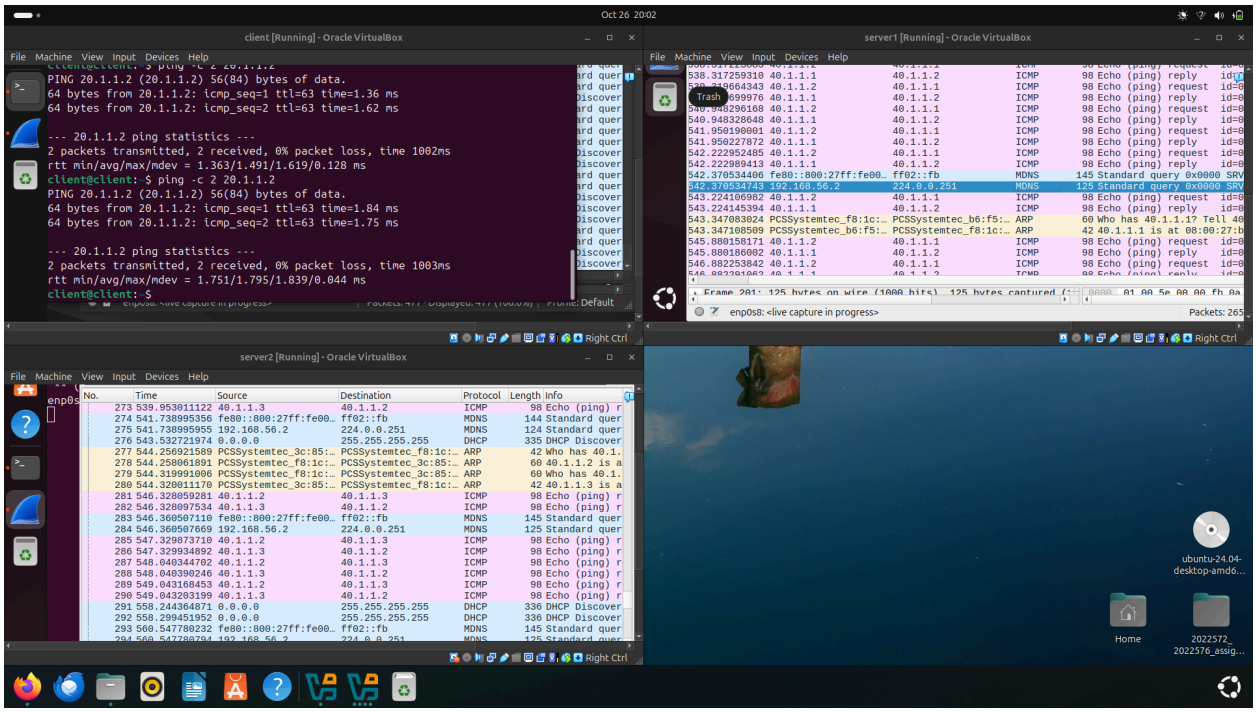
(a)

```
root@gateway:/home/gateway# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination
DNAT       all  --  anywhere             40.1.1.0/24          to:20.1.1.1
DNAT       all  --  anywhere             gateway              to:40.1.1.3
DNAT       all  --  anywhere             gateway              statistic mode random probability 0.79999999981 to:40.1.1.
1

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
SNAT       all  --  20.1.1.0/24          anywhere             to:40.1.1.2
root@gateway:/home/gateway#
```


client [Running] - Oracle VirtualBox
server1 [Running] - Oracle VirtualBox
server2 [Running] - Oracle VirtualBox
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=1.36 ms
64 bytes from 20.1.1.2: icmp_seq=2 ttl=63 time=1.62 ms
--- 20.1.1.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 1.363/1.491/1.619/0.128 ms
client@client: $ ping -c 2 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=1.84 ms
64 bytes from 20.1.1.2: icmp_seq=2 ttl=63 time=1.75 ms
--- 20.1.1.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1003ms
rtt min/avg/max/mdev = 1.751/1.795/1.839/0.044 ms
client@client:~$
Right Ctrl
enp0s8: <live capture in progress>
Packets: 265
ubuntu-24.04-desktop-amd6...
Home
2022572_2022576_assig...

(b)