Sweta Snigdha
2022527

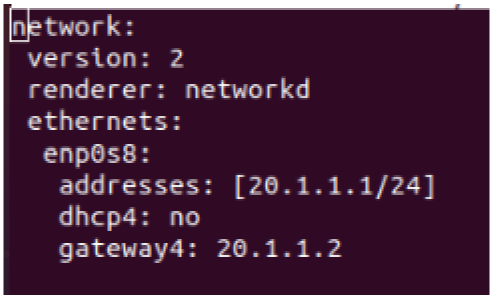
CN Assignment 3

Q1.a

<u>sweta_vm1 (Client):</u>
Interface: enp0s8
IP Address: 20.1.1.1/24

Commands:

```
sudo ip link set enp0s8 up
sudo nano /etc/netplan/02-netcfg.yaml
sudo netplan apply
sudo reboot
sudo ip route add 40.1.1.0/24 via 20.1.1.2
```

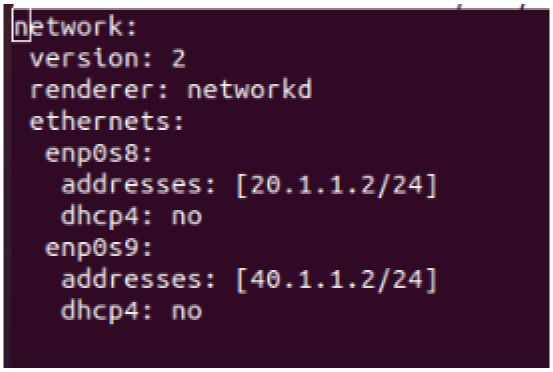


```
network:
 version: 2
 renderer: networkd
 ethernets:
  enp0s8:
   addresses: [20.1.1.1/24]
   dhcp4: no
   gateway4: 20.1.1.2
```

<u>sweta_vm2 (Gateway):</u>
Interface 1: enp0s8 (Client side)
IP Address: 20.1.1.2/24
Interface 2: enp0s9 (Server side)
IP Address: 40.1.1.2/24

Commands:

```
sudo ip link set enp0s8 up
sudo ip link set enp0s9 up
sudo nano /etc/netplan/02-netcfg.yaml
sudo netplan apply
sudo reboot
```

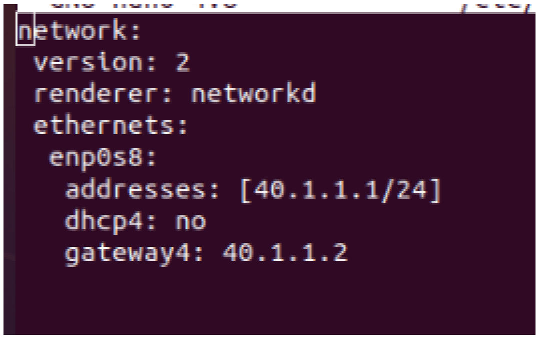


```
network:
 version: 2
 renderer: networkd
 ethernets:
  enp0s8:
   addresses: [20.1.1.2/24]
   dhcp4: no
  enp0s9:
   addresses: [40.1.1.2/24]
   dhcp4: no
```

<u>sweta_vm3 (Server 1):</u>
Interface: enp0s8
IP Address: 40.1.1.1/24

Commands:

```
sudo ip link set enp0s8 up
sudo nano /etc/netplan/02-netcfg.yaml
sudo netplan apply
sudo reboot
sudo ip route add 20.1.1.0/24 via 40.1.1.2
```

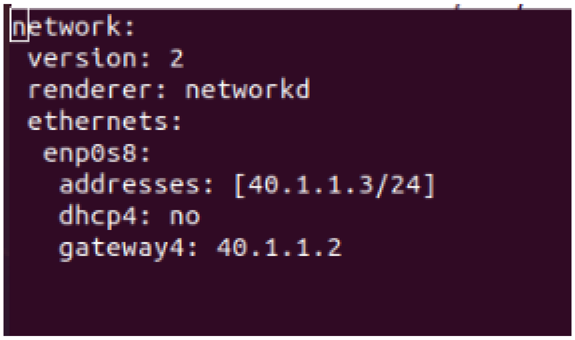


```
network:
 version: 2
 renderer: networkd
 ethernets:
  enp0s8:
   addresses: [40.1.1.1/24]
   dhcp4: no
   gateway4: 40.1.1.2
```

<u>sweta_vm4 (Server 2):</u>
Interface: enp0s8
IP Address: 40.1.1.3/24

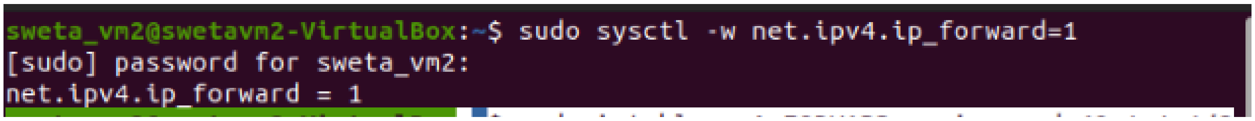
Commands:

```
sudo ip link set enp0s8 up
sudo nano /etc/netplan/02-netcfg.yaml
sudo netplan apply
sudo reboot
sudo ip route add 20.1.1.0/24 via 40.1.1.2
```



```
network:
 version: 2
 renderer: networkd
 ethernets:
  enp0s8:
   addresses: [40.1.1.3/24]
   dhcp4: no
   gateway4: 40.1.1.2
```

Q1.b

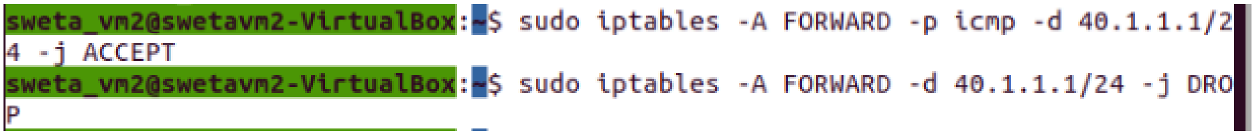


```
sweta_vm2@swetavm2-VirtualBox:~$ sudo sysctl -w net.ipv4.ip_forward=1
[sudo] password for sweta_vm2:
net.ipv4.ip_forward = 1
```

Commands:
sudo sysctl -w net.ipv4.ip_forward=1
sudo ip route add 20.1.1.0/24 via 20.1.1.2
sudo ip route add 40.1.1.0/24 via 40.1.1.2

By enabling IP forwarding on sweta_vm2 and configuring forwarding rules with iptables, traffic from the client (sweta_vm1) can be forwarded to either server (sweta_vm3 or sweta_vm4) based on the routing rules. Traffic from sweta_vm1 should now be forwarded to the respective server based on the destination IP.

Q2.a



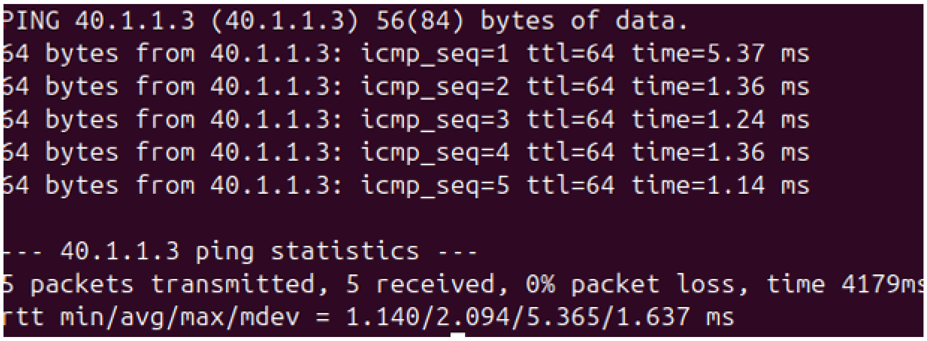
```
sweta_vm2@swetavm2-VirtualBox:~$ sudo iptables -A FORWARD -p icmp -d 40.1.1.1/2
4 -j ACCEPT
sweta_vm2@swetavm2-VirtualBox:~$ sudo iptables -A FORWARD -d 40.1.1.1/24 -j DRO
P
```

Commands:
sudo iptables -A FORWARD -p icmp -d 40.1.1.1 -j ACCEPT
sudo iptables -A FORWARD -d 40.1.1.1/24 -j DROP

By setting up an iptables rule to allow only ICMP traffic (ping) and dropping all other traffic to 40.1.1.1/24, we ensure that no other protocols, such as TCP or UDP, can reach Server 1. This is useful for restricting communication while still allowing network monitoring through ping.

-A FORWARD specifies the rule applies to packets being forwarded by the gateway.
-p icmp specifies the rule applies to ICMP packets (used by ping).
-d 40.1.1.1/24 -j ACCEPT allows the traffic to Server 1.
Another rule, -d 40.1.1.1/24 -j DROP, drops all other traffic.

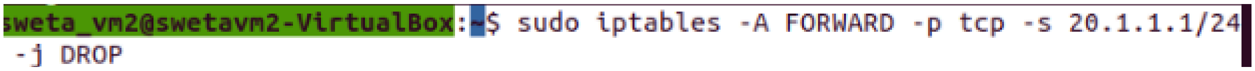
Testing ping: ping -c 5 40.1.1.3



```
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=64 time=5.37 ms
64 bytes from 40.1.1.3: icmp_seq=2 ttl=64 time=1.36 ms
64 bytes from 40.1.1.3: icmp_seq=3 ttl=64 time=1.24 ms
64 bytes from 40.1.1.3: icmp_seq=4 ttl=64 time=1.36 ms
64 bytes from 40.1.1.3: icmp_seq=5 ttl=64 time=1.14 ms

--- 40.1.1.3 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4179ms
rtt min/avg/max/mdev = 1.140/2.094/5.365/1.637 ms
```

There is 0% packet loss, showing the ping is not blocked.

Q2.b



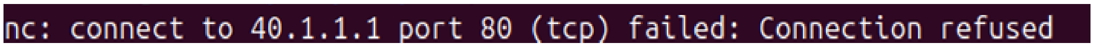
```
sweta_vm2@swetavm2-VirtualBox:~$ sudo iptables -A FORWARD -p tcp -s 20.1.1.1/24
 -j DROP
```

Command: sudo iptables -A FORWARD -p tcp-s 20.1.1.1/24 -j DROP

The rule will block TCP traffic initiated by the client (20.1.1.1/24). This filters out any TCP connection attempts from VM1, while other types of traffic, like UDP or ICMP, can still pass through.

-s 20.1.1.1/24 specifies the source IP (VM1).
-p tcp applies to TCP traffic only.
-j DROP ensures that TCP packets from the client are dropped.

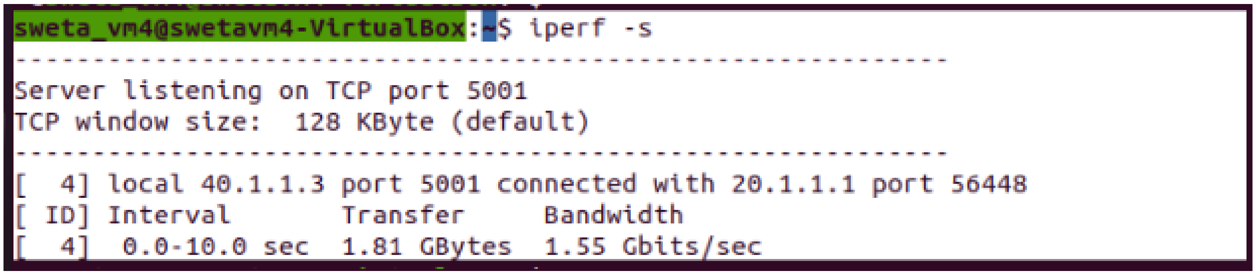
Tcp connection testing: nc -vz 40.1.1.1 80



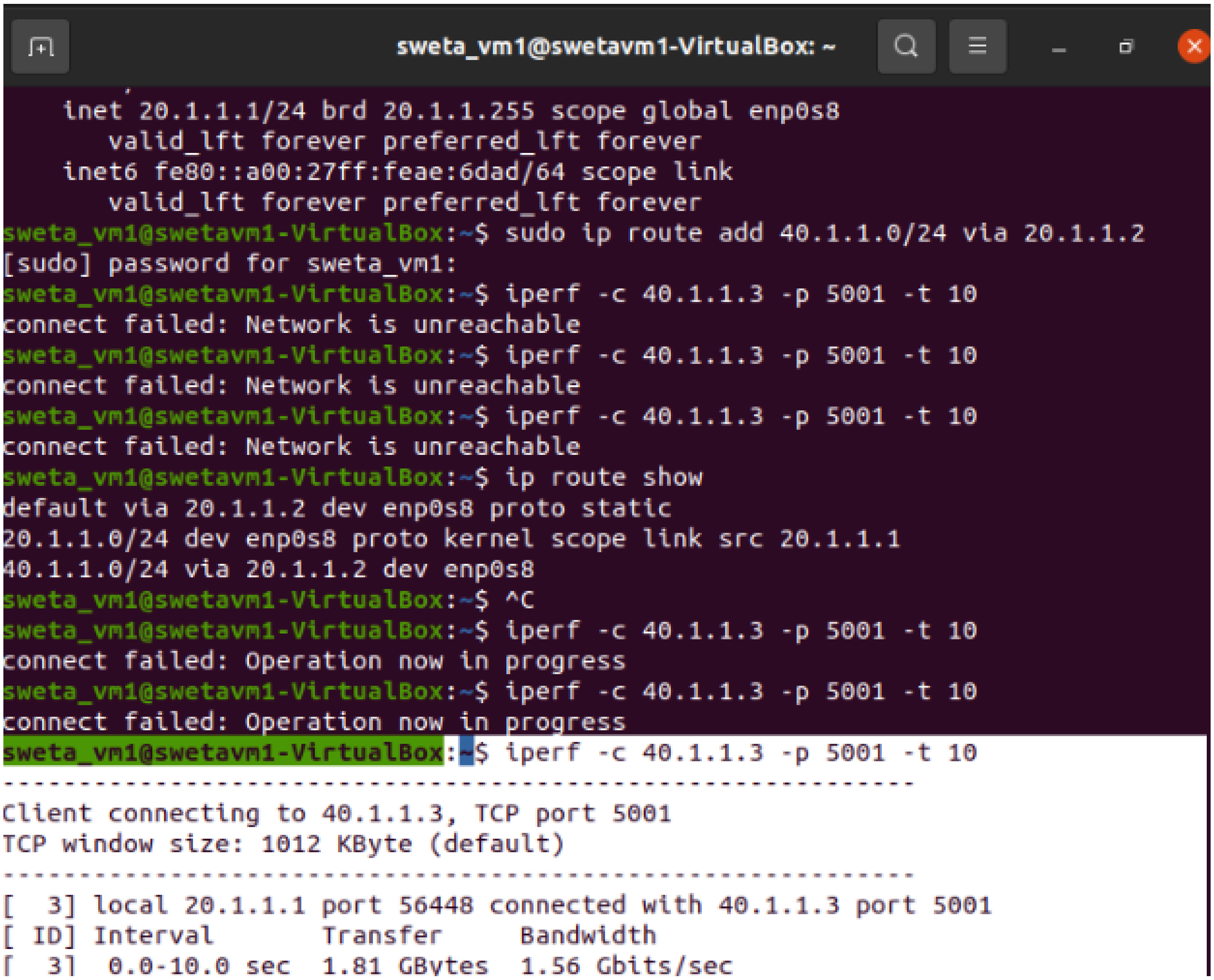
```
nc: connect to 40.1.1.1 port 80 (tcp) failed: Connection refused
```

Q3.a

TCP:



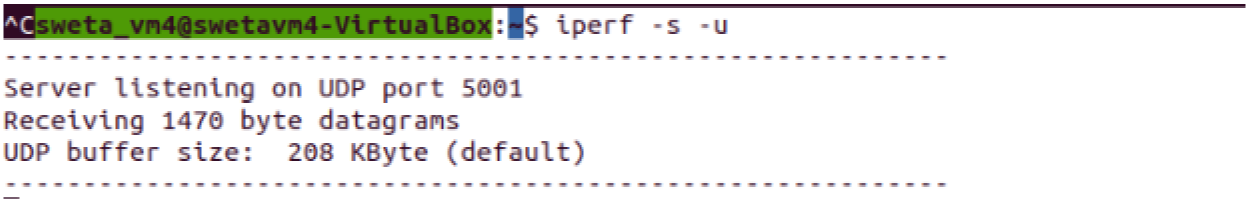
```
sweta_vm4@swetavm4-VirtualBox:~$ iperf -s
------------------------------------------------------------
Server listening on TCP port 5001
TCP window size:  128 KByte (default)
------------------------------------------------------------
[  4] local 40.1.1.3 port 5001 connected with 20.1.1.1 port 56448
[ ID] Interval       Transfer     Bandwidth
[  4]  0.0-10.0 sec  1.81 GBytes  1.55 Gbits/sec
```



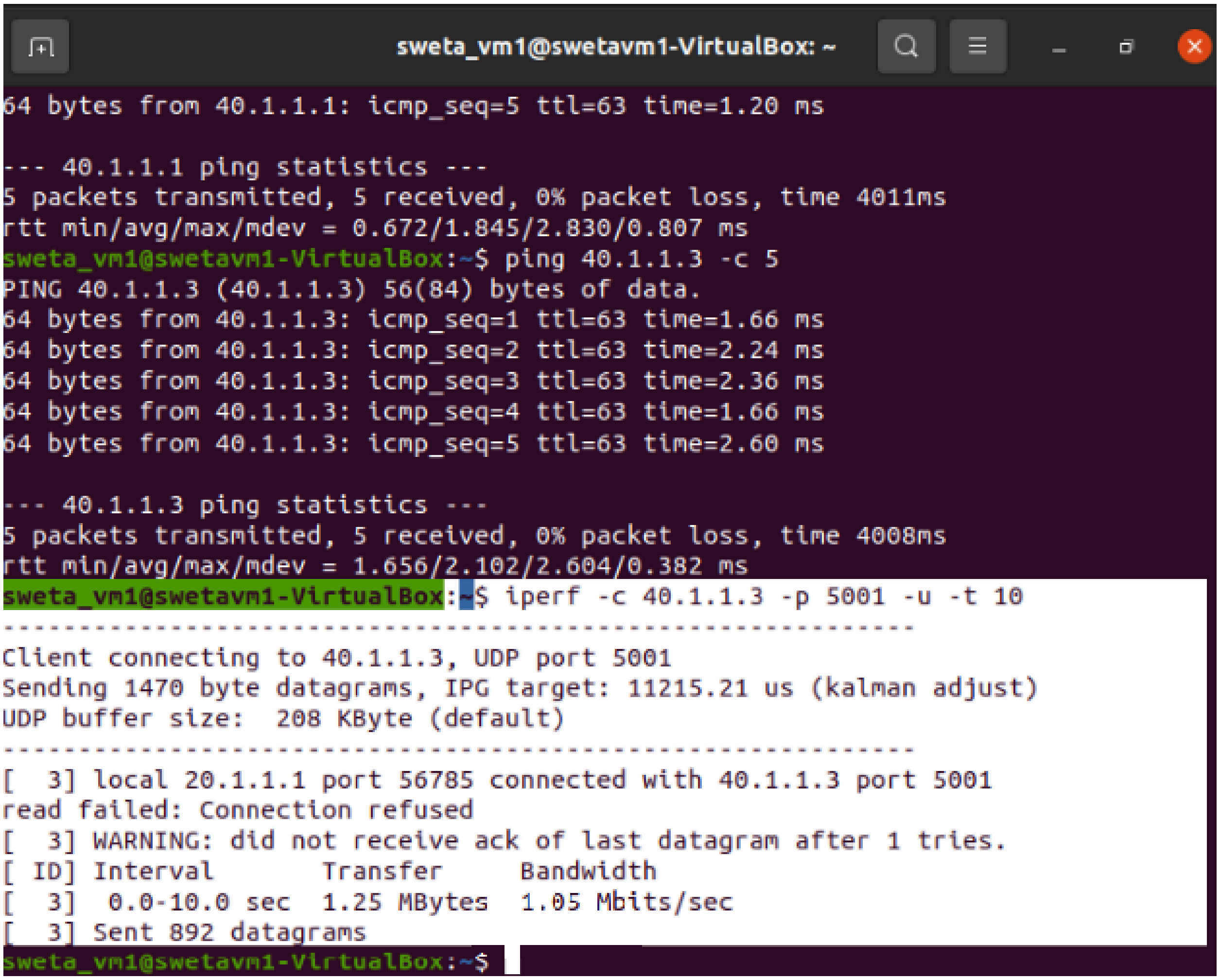
```
    inet 20.1.1.1/24 brd 20.1.1.255 scope global enp0s8
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:feae:6dad/64 scope link
       valid_lft forever preferred_lft forever
sweta_vm1@swetavm1-VirtualBox:~$ sudo ip route add 40.1.1.0/24 via 20.1.1.2
[sudo] password for sweta_vm1:
sweta_vm1@swetavm1-VirtualBox:~$ iperf -c 40.1.1.3 -p 5001 -t 10
connect failed: Network is unreachable
sweta_vm1@swetavm1-VirtualBox:~$ iperf -c 40.1.1.3 -p 5001 -t 10
connect failed: Network is unreachable
sweta_vm1@swetavm1-VirtualBox:~$ iperf -c 40.1.1.3 -p 5001 -t 10
connect failed: Network is unreachable
sweta_vm1@swetavm1-VirtualBox:~$ ip route show
default via 20.1.1.2 dev enp0s8 proto static
20.1.1.0/24 dev enp0s8 proto kernel scope link src 20.1.1.1
40.1.1.0/24 via 20.1.1.2 dev enp0s8
sweta_vm1@swetavm1-VirtualBox:~$ ^C
sweta_vm1@swetavm1-VirtualBox:~$ iperf -c 40.1.1.3 -p 5001 -t 10
connect failed: Operation now in progress
sweta_vm1@swetavm1-VirtualBox:~$ iperf -c 40.1.1.3 -p 5001 -t 10
connect failed: Operation now in progress
sweta_vm1@swetavm1-VirtualBox:~$ iperf -c 40.1.1.3 -p 5001 -t 10
------------------------------------------------------------
Client connecting to 40.1.1.3, TCP port 5001
TCP window size: 1012 KByte (default)
------------------------------------------------------------
[  3] local 20.1.1.1 port 56448 connected with 40.1.1.3 port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0-10.0 sec  1.81 GBytes  1.56 Gbits/sec
```

The server is listening on TCP port 5001. We test TCP bandwidth on IP address 40.1.1.3 & port 5001 for 10 seconds

UDP:



```
^Csweta_vm4@swetavm4-VirtualBox:~$ iperf -s -u
------------------------------------------------------------
Server listening on UDP port 5001
Receiving 1470 byte datagrams
UDP buffer size:  208 KByte (default)
------------------------------------------------------------
_
```

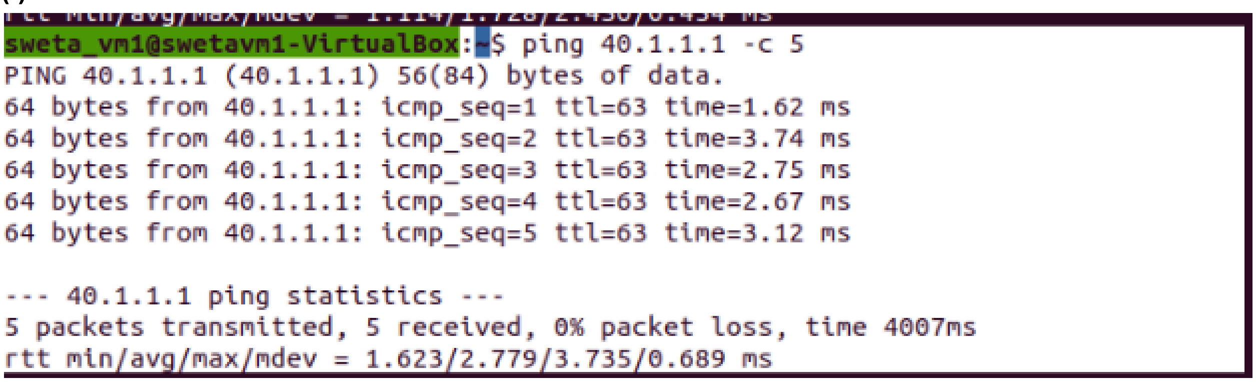


```
64 bytes from 40.1.1.1: icmp_seq=5 ttl=63 time=1.20 ms

--- 40.1.1.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4011ms
rtt min/avg/max/mdev = 0.672/1.845/2.830/0.807 ms
sweta_vm1@swetavm1-VirtualBox:~$ ping 40.1.1.3 -c 5
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=1.66 ms
64 bytes from 40.1.1.3: icmp_seq=2 ttl=63 time=2.24 ms
64 bytes from 40.1.1.3: icmp_seq=3 ttl=63 time=2.36 ms
64 bytes from 40.1.1.3: icmp_seq=4 ttl=63 time=1.66 ms
64 bytes from 40.1.1.3: icmp_seq=5 ttl=63 time=2.60 ms

--- 40.1.1.3 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4008ms
rtt min/avg/max/mdev = 1.656/2.102/2.604/0.382 ms
sweta_vm1@swetavm1-VirtualBox:~$ iperf -c 40.1.1.3 -p 5001 -u -t 10
------------------------------------------------------------
Client connecting to 40.1.1.3, UDP port 5001
Sending 1470 byte datagrams, IPG target: 11215.21 us (kalman adjust)
UDP buffer size:  208 KByte (default)
------------------------------------------------------------
[  3] local 20.1.1.1 port 56785 connected with 40.1.1.3 port 5001
read failed: Connection refused
[  3] WARNING: did not receive ack of last datagram after 1 tries.
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0-10.0 sec  1.25 MBytes  1.05 Mbits/sec
[  3] Sent 892 datagrams
sweta_vm1@swetavm1-VirtualBox:~$
```

The server is listening on UDP port 5001. We test UDP bandwidth on IP address 40.1.1.3 & port 5001 for 10 seconds

Q3.b

(i)

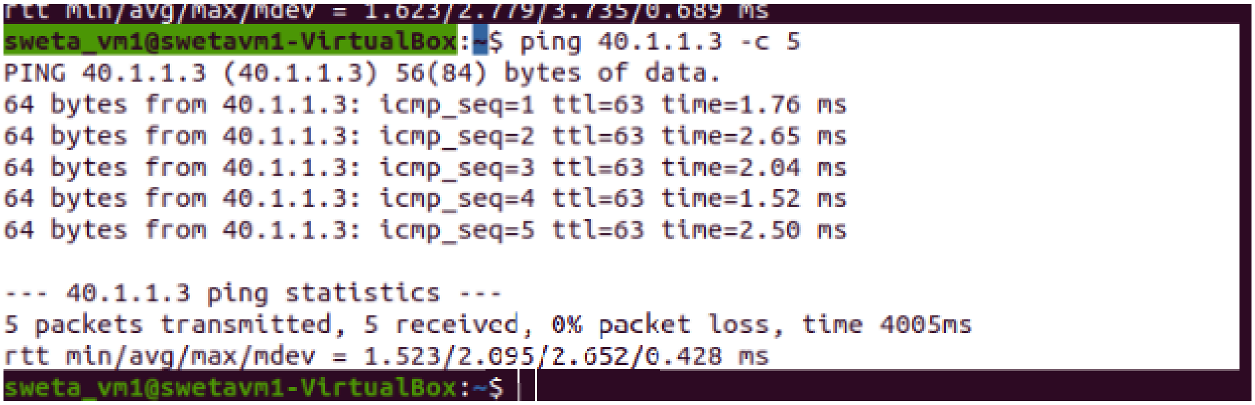


```
rtt min/avg/max/mdev = 1.114/1.728/2.430/0.434 ms
sweta_vm1@swetavm1-VirtualBox:~$ ping 40.1.1.1 -c 5
PING 40.1.1.1 (40.1.1.1) 56(84) bytes of data.
64 bytes from 40.1.1.1: icmp_seq=1 ttl=63 time=1.62 ms
64 bytes from 40.1.1.1: icmp_seq=2 ttl=63 time=3.74 ms
64 bytes from 40.1.1.1: icmp_seq=3 ttl=63 time=2.75 ms
64 bytes from 40.1.1.1: icmp_seq=4 ttl=63 time=2.67 ms
64 bytes from 40.1.1.1: icmp_seq=5 ttl=63 time=3.12 ms

--- 40.1.1.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 1.623/2.779/3.735/0.689 ms
```

Min rtt = 1.623 ms

Avg rtt = 2.779 ms
Max rtt = 3.735 ms

(ii)



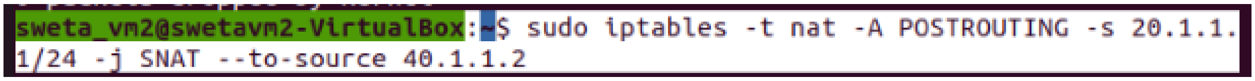
```
rtt min/avg/max/mdev = 1.623/2.779/3.735/0.689 ms
sweta_vm1@swetavm1-VirtualBox:~$ ping 40.1.1.3 -c 5
PING 40.1.1.3 (40.1.1.3) 56(84) bytes of data.
64 bytes from 40.1.1.3: icmp_seq=1 ttl=63 time=1.76 ms
64 bytes from 40.1.1.3: icmp_seq=2 ttl=63 time=2.65 ms
64 bytes from 40.1.1.3: icmp_seq=3 ttl=63 time=2.04 ms
64 bytes from 40.1.1.3: icmp_seq=4 ttl=63 time=1.52 ms
64 bytes from 40.1.1.3: icmp_seq=5 ttl=63 time=2.50 ms

--- 40.1.1.3 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 1.523/2.095/2.652/0.428 ms
sweta_vm1@swetavm1-VirtualBox:~$
```

Min rtt = 1.523 ms
Avg rtt = 2.095 ms
Max rtt = 2.652 ms

(iii)

Round-trip Time for 20.1.1.1/24 to 40.1.1.1/24 has higher minimum, average, and maximum values. This could be because of network congestion, higher latency or more server load compared to 40.1.1.3/24.

Q4.a



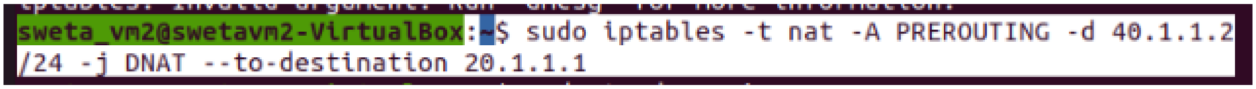
```
sweta_vm2@swetavm2-VirtualBox:~$ sudo iptables -t nat -A POSTROUTING -s 20.1.1.
1/24 -j SNAT --to-source 40.1.1.2
```

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

NAT allows the gateway to rewrite the source IP address of packets as they pass through. This makes it look like the traffic is originating from the gateway instead of the client.

-t nat specifies that we’re modifying the NAT table.
POSTROUTING modifies packets after the routing decision has been made.
--to-source 40.1.1.2 rewrites the source IP to 40.1.1.2.

Q4.b



```
iptables: Invalid argument. Run `dmesg' for more information.
sweta_vm2@swetavm2-VirtualBox:~$ sudo iptables -t nat -A PREROUTING -d 40.1.1.2
/24 -j DNAT --to-destination 20.1.1.1
```

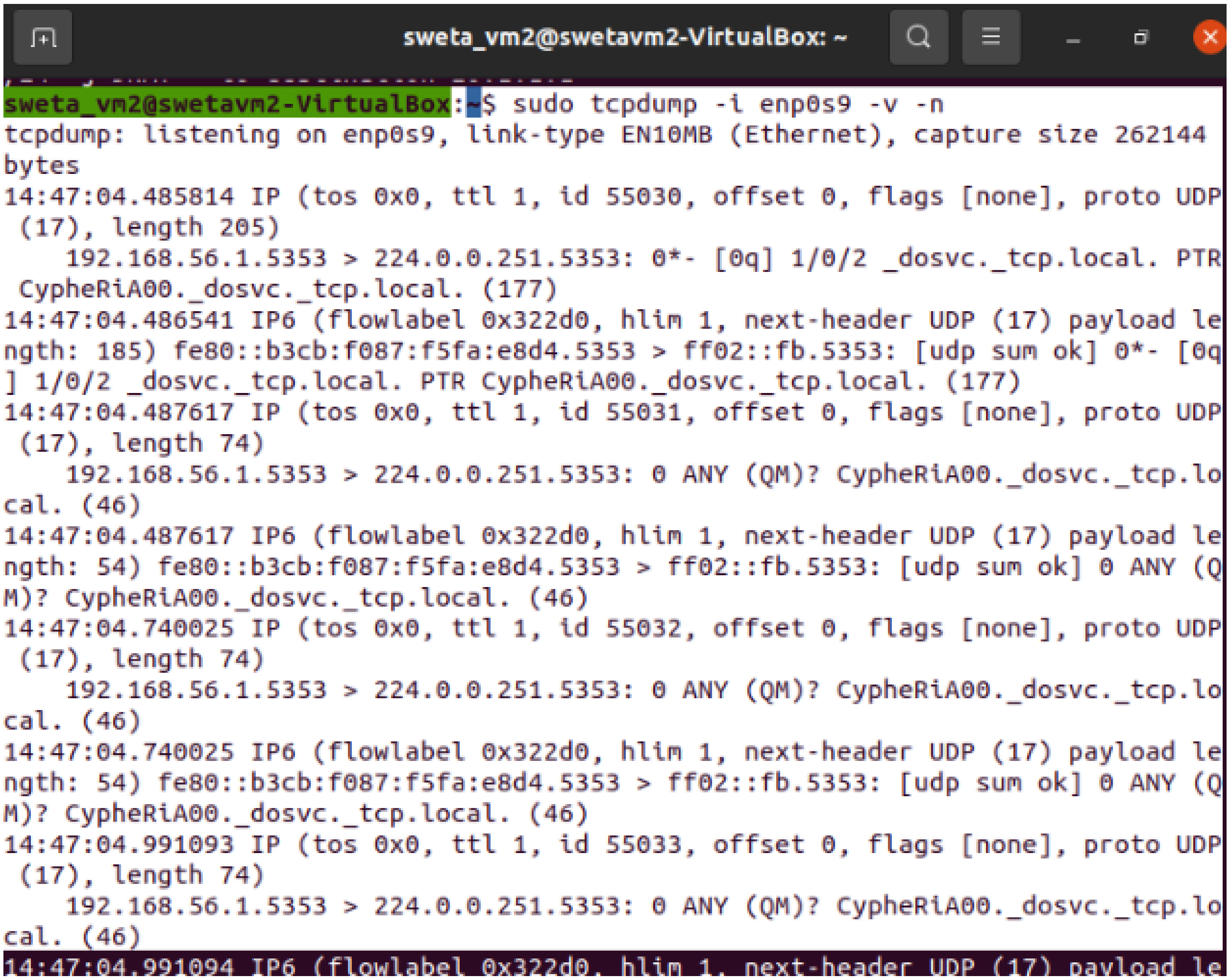
Command: sudo iptables -t nat -A PREROUTING -d 40.1.1.2 -j DNAT --to-destination 20.1.1.1

When the server responds, the gateway needs to rewrite the destination IP back to the client’s original IP (20.1.1.1) so that the response reaches client(sweta_vm1).

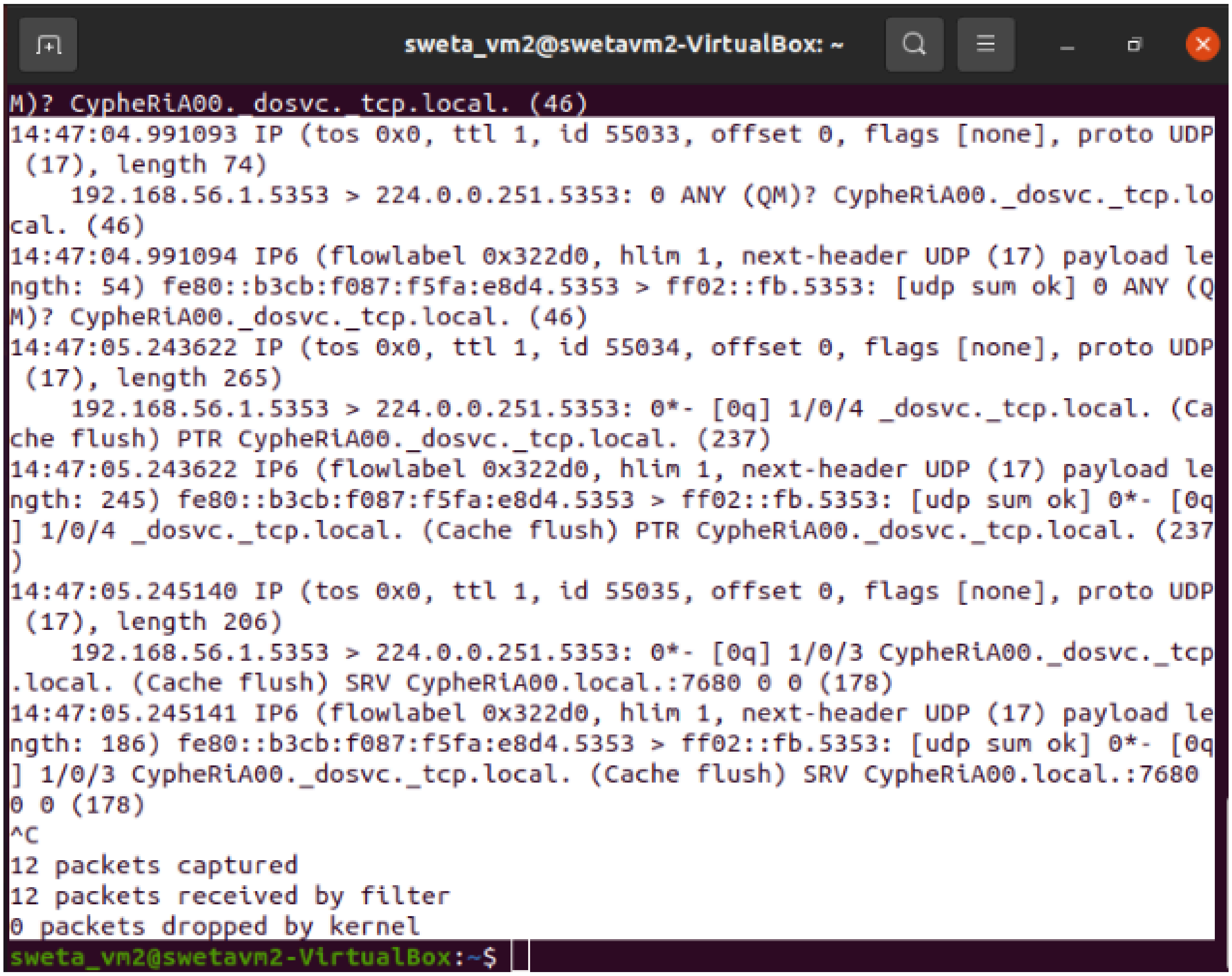
PREROUTING modifies packets before the routing decision.
--to-destination 20.1.1.1 rewrites the destination IP.

Q4.c

Tcpdump of ping from client to server: sudo tcpdump -i enp0s9 -v -n



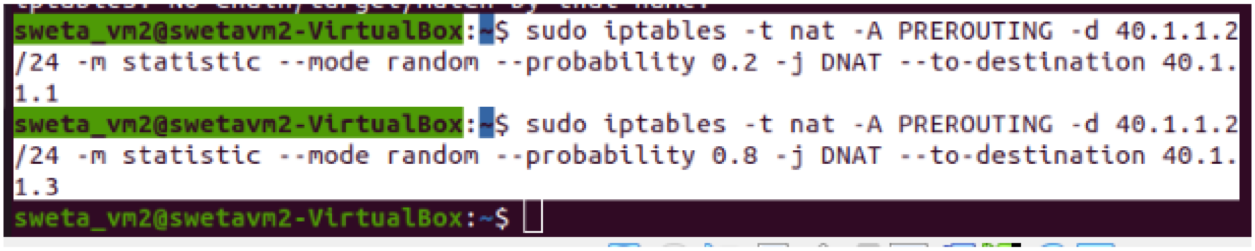
```
sweta_vm2@swetavm2-VirtualBox:~$ sudo tcpdump -i enp0s9 -v -n
tcpdump: listening on enp0s9, link-type EN10MB (Ethernet), capture size 262144
bytes
14:47:04.485814 IP (tos 0x0, ttl 1, id 55030, offset 0, flags [none], proto UDP
 (17), length 205)
    192.168.56.1.5353 > 224.0.0.251.5353: 0*- [0q] 1/0/2 _dosvc._tcp.local. PTR
 CypheRiA00._dosvc._tcp.local. (177)
14:47:04.486541 IP6 (flowlabel 0x322d0, hlim 1, next-header UDP (17) payload le
ngth: 185) fe80::b3cb:f087:f5fa:e8d4.5353 > ff02::fb.5353: [udp sum ok] 0*- [0q
] 1/0/2 _dosvc._tcp.local. PTR CypheRiA00._dosvc._tcp.local. (177)
14:47:04.487617 IP (tos 0x0, ttl 1, id 55031, offset 0, flags [none], proto UDP
 (17), length 74)
    192.168.56.1.5353 > 224.0.0.251.5353: 0 ANY (QM)? CypheRiA00._dosvc._tcp.lo
cal. (46)
14:47:04.487617 IP6 (flowlabel 0x322d0, hlim 1, next-header UDP (17) payload le
ngth: 54) fe80::b3cb:f087:f5fa:e8d4.5353 > ff02::fb.5353: [udp sum ok] 0 ANY (Q
M)? CypheRiA00._dosvc._tcp.local. (46)
14:47:04.740025 IP (tos 0x0, ttl 1, id 55032, offset 0, flags [none], proto UDP
 (17), length 74)
    192.168.56.1.5353 > 224.0.0.251.5353: 0 ANY (QM)? CypheRiA00._dosvc._tcp.lo
cal. (46)
14:47:04.740025 IP6 (flowlabel 0x322d0, hlim 1, next-header UDP (17) payload le
ngth: 54) fe80::b3cb:f087:f5fa:e8d4.5353 > ff02::fb.5353: [udp sum ok] 0 ANY (Q
M)? CypheRiA00._dosvc._tcp.local. (46)
14:47:04.991093 IP (tos 0x0, ttl 1, id 55033, offset 0, flags [none], proto UDP
 (17), length 74)
    192.168.56.1.5353 > 224.0.0.251.5353: 0 ANY (QM)? CypheRiA00._dosvc._tcp.lo
cal. (46)
14:47:04.991094 IP6 (flowlabel 0x322d0, hlim 1, next-header UDP (17) payload le
```



```
M)? CypheRiA00._dosvc._tcp.local. (46)
14:47:04.991093 IP (tos 0x0, ttl 1, id 55033, offset 0, flags [none], proto UDP
 (17), length 74)
    192.168.56.1.5353 > 224.0.0.251.5353: 0 ANY (QM)? CypheRiA00._dosvc._tcp.lo
cal. (46)
14:47:04.991094 IP6 (flowlabel 0x322d0, hlim 1, next-header UDP (17) payload le
ngth: 54) fe80::b3cb:f087:f5fa:e8d4.5353 > ff02::fb.5353: [udp sum ok] 0 ANY (Q
M)? CypheRiA00._dosvc._tcp.local. (46)
14:47:05.243622 IP (tos 0x0, ttl 1, id 55034, offset 0, flags [none], proto UDP
 (17), length 265)
    192.168.56.1.5353 > 224.0.0.251.5353: 0*- [0q] 1/0/4 _dosvc._tcp.local. (Ca
che flush) PTR CypheRiA00._dosvc._tcp.local. (237)
14:47:05.243622 IP6 (flowlabel 0x322d0, hlim 1, next-header UDP (17) payload le
ngth: 245) fe80::b3cb:f087:f5fa:e8d4.5353 > ff02::fb.5353: [udp sum ok] 0*- [0q
] 1/0/4 _dosvc._tcp.local. (Cache flush) PTR CypheRiA00._dosvc._tcp.local. (237
)
14:47:05.245140 IP (tos 0x0, ttl 1, id 55035, offset 0, flags [none], proto UDP
 (17), length 206)
    192.168.56.1.5353 > 224.0.0.251.5353: 0*- [0q] 1/0/3 CypheRiA00._dosvc._tcp
.local. (Cache flush) SRV CypheRiA00.local.:7680 0 0 (178)
14:47:05.245141 IP6 (flowlabel 0x322d0, hlim 1, next-header UDP (17) payload le
ngth: 186) fe80::b3cb:f087:f5fa:e8d4.5353 > ff02::fb.5353: [udp sum ok] 0*- [0q
] 1/0/3 CypheRiA00._dosvc._tcp.local. (Cache flush) SRV CypheRiA00.local.:7680
0 0 (178)
^C
12 packets captured
12 packets received by filter
0 packets dropped by kernel
sweta_vm2@swetavm2-VirtualBox:~$
```

Q5.a

As observed in Q3.b, 20.1.1.1/24 to 40.1.1.3/24 connection has lower RTT. So we assign the higher probability(80 %) to 40.1.1.3/24 server.

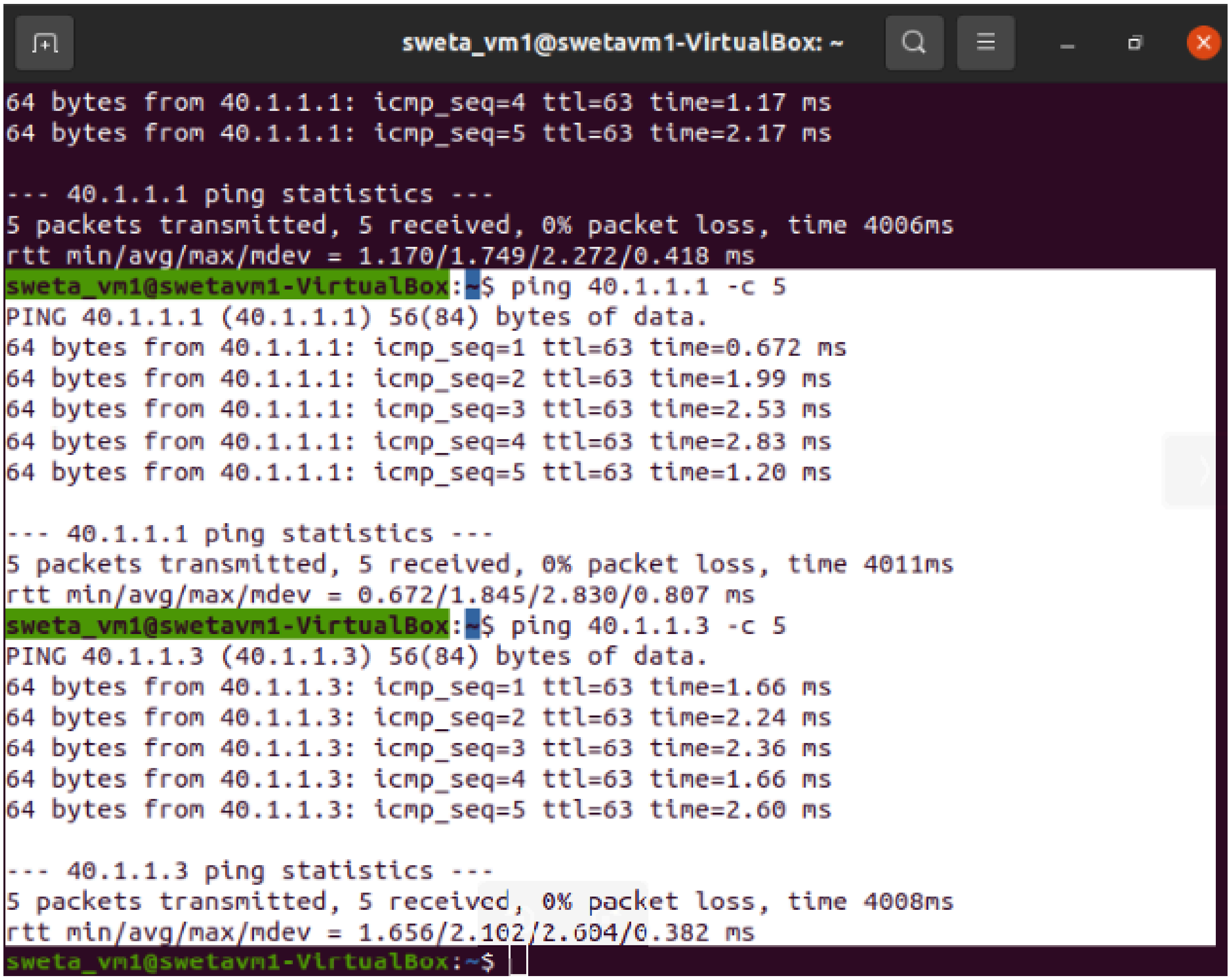


```
sweta_vm2@swetavm2-VirtualBox:~$ sudo iptables -t nat -A PREROUTING -d 40.1.1.2
/24 -m statistic --mode random --probability 0.2 -j DNAT --to-destination 40.1.
1.1
sweta_vm2@swetavm2-VirtualBox:~$ sudo iptables -t nat -A PREROUTING -d 40.1.1.2
/24 -m statistic --mode random --probability 0.8 -j DNAT --to-destination 40.1.
1.3
sweta_vm2@swetavm2-VirtualBox:~$
```

Commands:

```
sudo iptables -t nat -A PREROUTING -d 40.1.1.2/24 -m statistic --mode random --probability 0.2 -j DNAT --to-destination 40.1.1.1
sudo iptables -t nat -A PREROUTING -d 40.1.1.2/24 -m statistic --mode random --probability 0.8 -j DNAT --to-destination 40.1.1.3
```

Q5.b



```
64 bytes from 40.1.1.1: icmp_seq=4 ttl=63 time=1.17 ms
64 bytes from 40.1.1.1: icmp_seq=5 ttl=63 time=2.17 ms

--- 40.1.1.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 1.170/1.749/2.272/0.418 ms
sweta_vm1@swetavm1-VirtualBox:~$ ping 40.1.1.1 -c 5
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=0.672 ms
64 bytes from 40.1.1.1: icmp_seq=2 ttl=63 time=1.99 ms
64 bytes from 40.1.1.1: icmp_seq=3 ttl=63 time=2.53 ms
64 bytes from 40.1.1.1: icmp_seq=4 ttl=63 time=2.83 ms
64 bytes from 40.1.1.1: icmp_seq=5 ttl=63 time=1.20 ms

--- 40.1.1.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4011ms
rtt min/avg/max/mdev = 0.672/1.845/2.830/0.807 ms
sweta_vm1@swetavm1-VirtualBox:~$ ping 40.1.1.3 -c 5
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=1.66 ms
64 bytes from 40.1.1.3: icmp_seq=2 ttl=63 time=2.24 ms
64 bytes from 40.1.1.3: icmp_seq=3 ttl=63 time=2.36 ms
64 bytes from 40.1.1.3: icmp_seq=4 ttl=63 time=1.66 ms
64 bytes from 40.1.1.3: icmp_seq=5 ttl=63 time=2.60 ms

--- 40.1.1.3 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4008ms
rtt min/avg/max/mdev = 1.656/2.102/2.604/0.382 ms
sweta_vm1@swetavm1-VirtualBox:~$
```