CN Assignment-3

Name: Manan Aggarwal
Roll Number: 2022273

Q1. (A) The setup for the assignment is as follows:
4 VMs were made on VirtualBox with the configuration: 1 core, 512 MB RAM, 20 GB HDD, Debian (64-bit), these were named: client, gateway, server1, server2
2 Host only networks were made within VirtualBox, one for the ip range 20.1.1.0/24 and another for the ip range 40.1.1.0/24 with DHCP off, named VirtualBox Host-Only Ethernet Adapter and VirtualBox Host-Only Ethernet Adapter #2

Client was connected to the VirtualBox Host-Only Ethernet Adapter. (enp0s3)
Gateway has 2 interfaces, with one connected to VirtualBox Host-Only Ethernet Adapter (enp0s3) and another one to VirtualBox Host-Only Ethernet Adapter #2 (enp0s8)
Server1 was connected to VirtualBox Host-Only Ethernet Adapter #2 (enp0s8)
Server2 was also connected to VirtualBox Host-Only Ethernet Adapter #2 (enp0s8)

The interfaces were set up within the virtual machines with the following configurations at /etc/network/interfaces file and then rebooted.

Client:

```
client@client:~$ cat /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug enp0s3
iface enp0s3 inet static
 address 20.1.1.1
 netmask 255.255.255.0
 gateway 20.1.1.2
# This is an autoconfigured IPv6 interface
iface enp0s3 inet6 auto
client@client:~$ _
```

```
client@client:~$ /sbin/ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 20.1.1.1  netmask 255.255.255.0  broadcast 20.1.1.255
        inet6 fe80::a00:27ff:fe1b:5643  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:1b:56:43  txqueuelen 1000  (Ethernet)
        RX packets 992  bytes 107394 (104.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1935  bytes 166076 (162.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

client@client:~$ _
```

Gateway:

```
gateway@gateway:~$ cat /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug enp0s3
iface enp0s3 inet static
 address 20.1.1.2
 netmask 255.255.255.0
# This is an autoconfigured IPv6 interface
iface enp0s3 inet6 auto

allow-hotplug enp0s8
iface enp0s8 inet static
 address 40.1.1.2
 netmask 255.255.255.0

iface enp0s8 inet6 auto
gateway@gateway:~$
```

```
gateway@gateway:~$ /sbin/ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 20.1.1.2  netmask 255.255.255.0  broadcast 20.1.1.255
        inet6 fe80::a00:27ff:fea5:bd5  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:a5:0b:d5  txqueuelen 1000  (Ethernet)
        RX packets 1945  bytes 167124 (163.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1000  bytes 108128 (105.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 40.1.1.2  netmask 255.255.255.0  broadcast 40.1.1.255
        inet6 fe80::a00:27ff:fe83:1c85  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:83:1c:85  txqueuelen 1000  (Ethernet)
        RX packets 3845  bytes 329064 (321.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2002  bytes 215756 (210.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Server1:

```
server1@server1:~$ cat /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug enp0s3
iface enp0s3 inet static
 address 40.1.1.1
 netmask 255.255.255.0
 gateway 40.1.1.2
# This is an autoconfigured IPv6 interface
iface enp0s3 inet6 auto
server1@server1:~$
```

```
server1@server1:~$ /sbin/ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 40.1.1.1  netmask 255.255.255.0  broadcast 40.1.1.255
        inet6 fe80::a00:27ff:fe5d:5a15  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:5d:5a:15  txqueuelen 1000  (Ethernet)
        RX packets 1010  bytes 108522 (105.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1933  bytes 165184 (161.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

server1@server1:~$ _
```

Server2:

```
server2@server2:~$ cat /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug enp0s3
iface enp0s3 inet static
 address 40.1.1.3
 netmask 255.255.255.0
 gateway 40.1.1.2
# This is an autoconfigured IPv6 interface
iface enp0s3 inet6 auto
server2@server2:~$ _
```

```
server2@server2:~$ /sbin/ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 40.1.1.3  netmask 255.255.255.0  broadcast 40.1.1.255
        inet6 fe80::a00:27ff:fedc:8f0b  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:dc:8f:0b  txqueuelen 1000  (Ethernet)
        RX packets 1010  bytes 108868 (106.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1972  bytes 169188 (165.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

server2@server2:~$
```

(B) Even Though everything was correctly setup, when I tried pinging server1 from the client it resulted in 100% packet loss

```
client@client:~$ ping 40.1.1.1 -c 10
PING 40.1.1.1 (40.1.1.1) 56(84) bytes of data.

--- 40.1.1.1 ping statistics ---
10 packets transmitted, 0 received, 100% packet loss, time 9203ms

client@client:~$ _
```

This was setup by enabling ipv4 forwarding on the gateway machine

```
sudo sysctl -w net.ipv4.ip_forward=1
```

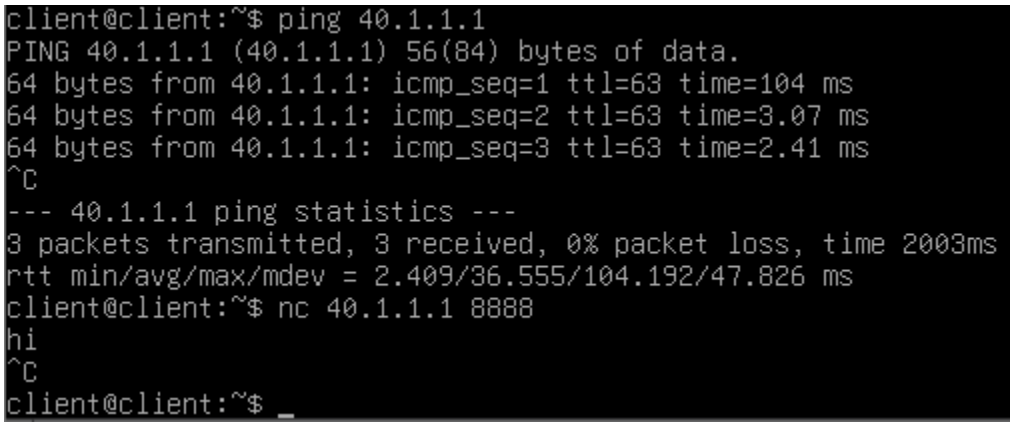
```
client@client:~$ ping 40.1.1.1 -c 10
PING 40.1.1.1 (40.1.1.1) 56(84) bytes of data.
64 bytes from 40.1.1.1: icmp_seq=1 ttl=63 time=104 ms
64 bytes from 40.1.1.1: icmp_seq=2 ttl=63 time=2.23 ms
64 bytes from 40.1.1.1: icmp_seq=3 ttl=63 time=2.72 ms
64 bytes from 40.1.1.1: icmp_seq=4 ttl=63 time=2.70 ms
64 bytes from 40.1.1.1: icmp_seq=5 ttl=63 time=3.23 ms
64 bytes from 40.1.1.1: icmp_seq=6 ttl=63 time=2.21 ms
64 bytes from 40.1.1.1: icmp_seq=7 ttl=63 time=4.35 ms
64 bytes from 40.1.1.1: icmp_seq=8 ttl=63 time=2.47 ms
64 bytes from 40.1.1.1: icmp_seq=9 ttl=63 time=2.35 ms
64 bytes from 40.1.1.1: icmp_seq=10 ttl=63 time=2.21 ms

--- 40.1.1.1 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9013ms
rtt min/avg/max/mdev = 2.209/12.891/104.442/30.523 ms
client@client:~$ _
```

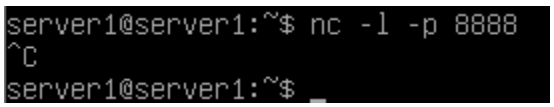
Running the above command fixed the issue, and i was able to successfully ping server1

Q2. (A) In order to drop all packets except ping packets (which are icmp-echo packets source), I first added an iptable rule to forward icmp echo-request and icmp echo-reply packets then drop all the remaining packets

```
sudo iptables -A FORWARD -d 40.1.1.1 -p icmp --icmp-type echo-request -j
ACCEPT
sudo iptables -A FORWARD -s 40.1.1.1 -p icmp --icmp-type echo-reply -j
ACCEPT
sudo iptables -A FORWARD -d 40.1.1.1 -j DROP
```

This allowed me to ping server1 but be unable to connect to it through netcat

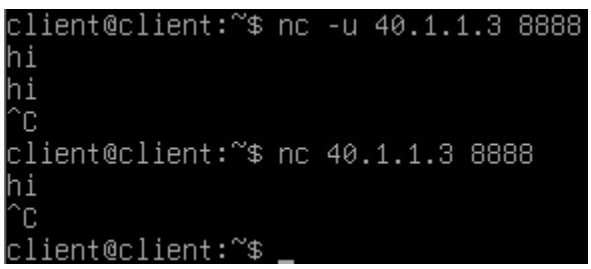


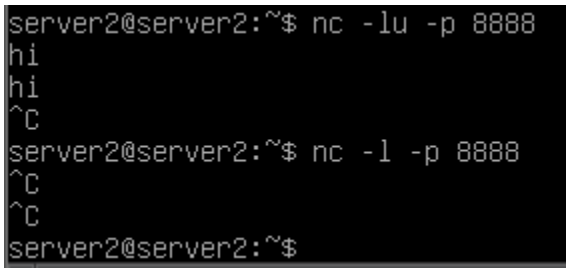


(B) In order to drop only the tcp packets from source address 20.1.1.1, i ran

```
sudo iptables -A FORWARD -s 20.1.1.1 -p tcp -j DROP
```

This resulted in the following:





Since all the packets were being dropped where destination is server1, I decided to test the configuration on server2. Even Though the UDP connection went through and transferred data, the TCP connection did not go through and blocked the data

Q3 (A) To run iperf on the server I ran

```
iperf -s
iperf -u -s
```

To test TCP and UDP connections I ran:

```
iperf -c 40.1.1.3
iperf -u -c 40.1.1.3
```

```
server2@server2:~$ iperf -s
------------------------------------------------------------
Server listening on TCP port 5001
TCP window size:  128 KByte (default)
------------------------------------------------------------
^Cserver2@server2:~$
```

```
client@client:~$ iperf -c 40.1.1.3
------------------------------------------------------------
Client connecting to 40.1.1.3, TCP port 5001
TCP window size: 16.0 KByte (default)
------------------------------------------------------------
^C^Cclient@client:~$
```

```
server2@server2:~$ iperf -u -s
------------------------------------------------------------
Server listening on UDP port 5001
UDP buffer size:  208 KByte (default)
------------------------------------------------------------
[  1] local 40.1.1.3 port 5001 connected with 20.1.1.1 port 43919
[ ID] Interval       Transfer     Bandwidth        Jitter   Lost/Total Datagrams
[  1] 0.0000-10.0152 sec  1.25 MBytes  1.05 Mbits/sec   0.352 ms 0/895 (0%)
^Cserver2@server2:~$ _
```

```
client@client:~$ iperf -u -c 40.1.1.3
------------------------------------------------------------
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)
------------------------------------------------------------
[  1] local 20.1.1.1 port 43919 connected with 40.1.1.3 port 5001
[ ID] Interval       Transfer     Bandwidth
[  1] 0.0000-10.0158 sec  1.25 MBytes  1.05 Mbits/sec
[  1] Sent 896 datagrams
[  1] Server Report:
[ ID] Interval       Transfer     Bandwidth        Jitter   Lost/Total Datagrams
[  1] 0.0000-10.0152 sec  1.25 MBytes  1.05 Mbits/sec   0.351 ms 0/895 (0%)
client@client:~$
```

From the configuration of Q2 we had blocked all the TCP traffic from 20.1.1.1 therefore iperf could not establish a TCP connection and hence did not give any output. Incase of UDP the connection was successful and we got a data transfer rate of 1.05 Mbits/sec

(B) I used ping to check the RTT from 20.1.1.1 to 40.1.1.1 and 40.1.1.3

```
ping 40.1.1.1
ping 40.1.1.3
```

(i)

```
client@client:~$ ping 40.1.1.1 -c 10
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=104 ms
64 bytes from 40.1.1.1: icmp_seq=2 ttl=63 time=2.47 ms
64 bytes from 40.1.1.1: icmp_seq=3 ttl=63 time=2.94 ms
64 bytes from 40.1.1.1: icmp_seq=4 ttl=63 time=3.12 ms
64 bytes from 40.1.1.1: icmp_seq=5 ttl=63 time=3.04 ms
64 bytes from 40.1.1.1: icmp_seq=6 ttl=63 time=2.09 ms
64 bytes from 40.1.1.1: icmp_seq=7 ttl=63 time=3.07 ms
64 bytes from 40.1.1.1: icmp_seq=8 ttl=63 time=3.14 ms
64 bytes from 40.1.1.1: icmp_seq=9 ttl=63 time=2.80 ms
64 bytes from 40.1.1.1: icmp_seq=10 ttl=63 time=3.28 ms

--- 40.1.1.1 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9015ms
rtt min/avg/max/mdev = 2.094/12.955/103.597/30.215 ms
```

Min RTT = 2.094 ms
Max RTT = 103.597 ms
Avg RTT = 12.955 ms

(ii)

```
client@client:~$ ping 40.1.1.3 -c 10
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=102 ms
64 bytes from 40.1.1.3: icmp_seq=2 ttl=63 time=2.29 ms
64 bytes from 40.1.1.3: icmp_seq=3 ttl=63 time=2.66 ms
64 bytes from 40.1.1.3: icmp_seq=4 ttl=63 time=2.02 ms
64 bytes from 40.1.1.3: icmp_seq=5 ttl=63 time=1.70 ms
64 bytes from 40.1.1.3: icmp_seq=6 ttl=63 time=3.51 ms
64 bytes from 40.1.1.3: icmp_seq=7 ttl=63 time=2.78 ms
64 bytes from 40.1.1.3: icmp_seq=8 ttl=63 time=2.66 ms
64 bytes from 40.1.1.3: icmp_seq=9 ttl=63 time=3.22 ms
64 bytes from 40.1.1.3: icmp_seq=10 ttl=63 time=2.25 ms

--- 40.1.1.3 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9018ms
rtt min/avg/max/mdev = 1.704/12.545/102.365/29.944 ms
```

Min RTT = 1.704 ms
Max RTT = 102.365 ms
Avg RTT = 12.545 ms

(iii) There is not much difference between the RTTs of 40.1.1.1 and 40.1.1.3 from the client. Server2 has slightly lower Avg RTT from that of Server1. This might be attributed to the fact that we are applying more iptables filters on 40.1.1.1 than 40.1.1.3

Q4 The previous config was result by flushing the iptable using

```
sudo iptables -F
```

(A) To change the SNAT source to 40.1.1.2 for the packets which come from 20.1.1.1

```
sudo iptables -t nat -A POSTROUTING -s 20.1.1.1 -j SNAT --to-source
40.1.1.2
```

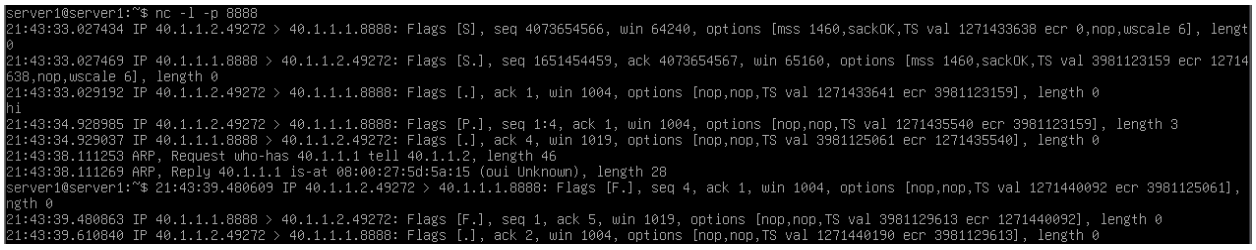
(B) To change the DNAT destination to 20.1.1.1 for the packets which have destination as 20.1.1.2

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

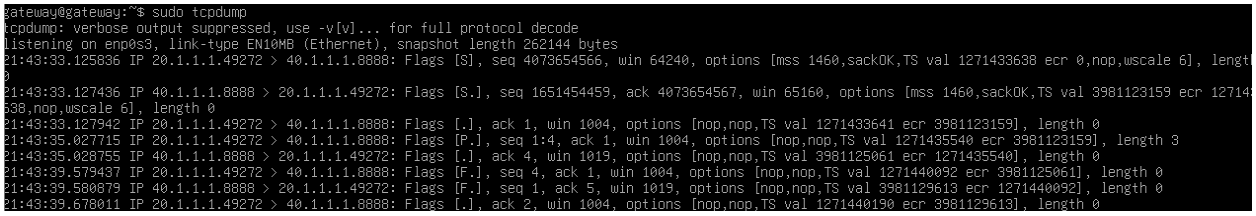
(C) I ran tcpdump on client, gateway and server1 in background and then connected client and server1 through netcat

```
sudo tcpdump &
```

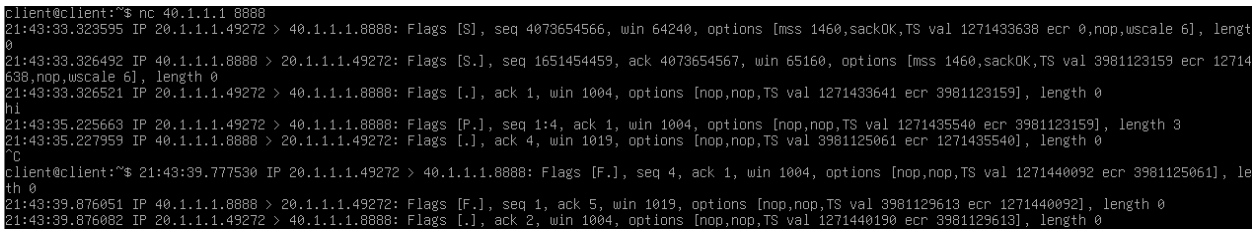
Server1:



Gateway:



Client:



All the requests received on server1 had source IP as 40.1.1.2 and the requests received on client had destination ip as 20.1.1.1 indicating that the NAT was successfully set up

Q5 (A) in question 3 it was seen that server2 has slightly lower RTT than that of server1

```
sudo iptables -A PREROUTING -t nat -d 20.1.1.2 -m statistic --mode random
--probability 0.2 -j DNAT --to-destination 40.1.1.1
sudo iptables -A PREROUTING -t nat -d 20.1.1.2 -j DNAT --to-destination
40.1.1.3
sudo iptables -A POSTROUTING -t nat -d 40.1.1.1 -j SNAT --to-source
40.1.1.2
```

```
sudo iptables -A POSTROUTING -t nat -d 40.1.1.3 -j SNAT --to-source
40.1.1.2
```

This ensures that 20% of the time the requests are sent to 40.1.1.1 and 80% the requests are sent to 40.1.1.3

(b) I manually ping 20.1.1.2 from the client 10 times

I also ran

```
sudo tcpdump icmp
```

On both the servers showed that 1 request went through server1 and 9 requests went through server2, this gives a 10% chance of requests going through server1, due to the sample size being small, if we increase the number of requests this would go up.

The reason for not directly pinging the gateway continuously with the -c flag is that when a ping request is sent the first packet has NEW as its state and after a response further packets are sent with state of ESTABLISHED, since the rules that we have made only correspond to NEW packets therefore all the subsequent requests would be sent to the server where the first request was sent (source)

Server1:

```
server1@server1:~$ sudo tcpdump icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
22:56:40.264395 IP 40.1.1.2 > 40.1.1.1: ICMP echo request, id 30709, seq 1, length 64
22:56:40.264425 IP 40.1.1.1 > 40.1.1.2: ICMP echo reply, id 30709, seq 1, length 64
```

Server2:

```
server2@server2:~$ sudo tcpdump icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
22:56:38.511354 IP 40.1.1.2 > 40.1.1.3: ICMP echo request, id 7654, seq 1, length 64
22:56:38.511396 IP 40.1.1.3 > 40.1.1.2: ICMP echo reply, id 7654, seq 1, length 64
22:56:39.054908 IP 40.1.1.2 > 40.1.1.3: ICMP echo request, id 31664, seq 1, length 64
22:56:39.054937 IP 40.1.1.3 > 40.1.1.2: ICMP echo reply, id 31664, seq 1, length 64
22:56:39.575983 IP 40.1.1.2 > 40.1.1.3: ICMP echo request, id 30524, seq 1, length 64
22:56:39.576011 IP 40.1.1.3 > 40.1.1.2: ICMP echo reply, id 30524, seq 1, length 64
22:56:40.127851 IP 40.1.1.2 > 40.1.1.3: ICMP echo request, id 58958, seq 1, length 64
22:56:40.127903 IP 40.1.1.3 > 40.1.1.2: ICMP echo reply, id 58958, seq 1, length 64
22:56:40.648077 IP 40.1.1.2 > 40.1.1.3: ICMP echo request, id 20484, seq 1, length 64
22:56:40.648110 IP 40.1.1.3 > 40.1.1.2: ICMP echo reply, id 20484, seq 1, length 64
22:56:41.776753 IP 40.1.1.2 > 40.1.1.3: ICMP echo request, id 37938, seq 1, length 64
22:56:41.776789 IP 40.1.1.3 > 40.1.1.2: ICMP echo reply, id 37938, seq 1, length 64
22:56:42.343931 IP 40.1.1.2 > 40.1.1.3: ICMP echo request, id 25887, seq 1, length 64
22:56:42.343968 IP 40.1.1.3 > 40.1.1.2: ICMP echo reply, id 25887, seq 1, length 64
22:56:42.879993 IP 40.1.1.2 > 40.1.1.3: ICMP echo request, id 42215, seq 1, length 64
22:56:42.880031 IP 40.1.1.3 > 40.1.1.2: ICMP echo reply, id 42215, seq 1, length 64
22:56:43.440660 IP 40.1.1.2 > 40.1.1.3: ICMP echo request, id 547, seq 1, length 64
22:56:43.440697 IP 40.1.1.3 > 40.1.1.2: ICMP echo reply, id 547, seq 1, length 64
```