Using Labsetup 2.0

```
seed@ubuntu-s-1vcpu-2gb-nyc1-01:~$ dockps
c1dd56178ffc  host1-192.168.60.5
0d48f77e2d65  host2-192.168.60.6
e76b6462572f  host3-192.168.60.7
2d7a40d43a9c  hostA-10.9.0.5
b3d323aa865a  seed-router
```

Section4
4A
Before running the iptables, verify we can ping and telnet to seed-router from HostA:

```
root@2d7a40d43a9c:/# ping 10.9.0.11
PING 10.9.0.11 (10.9.0.11) 56(84) bytes of data.
64 bytes from 10.9.0.11: icmp_seq=1 ttl=64 time=0.119 ms
64 bytes from 10.9.0.11: icmp_seq=2 ttl=64 time=0.090 ms
64 bytes from 10.9.0.11: icmp_seq=3 ttl=64 time=0.117 ms
^C
```

```
root@2d7a40d43a9c:/# telnet 10.9.0.11
Trying 10.9.0.11...
Connected to 10.9.0.11.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
b3d323aa865a login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-107-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
```

Add rules suggested in Lab description on seed-router.

```
root@b3d323aa865a:/# iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
root@b3d323aa865a:/# iptables -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT
root@b3d323aa865a:/# v
bash: v: command not found
root@b3d323aa865a:/# iptables -P OUTPUT DROP
root@b3d323aa865a:/# iptables -P INPUT DROP
```

From 10.9.0.5, ping and telnet to seed-router again, we can see that ping works, telnet does not work.

```
root@2d7a40d43a9c:/# ping 10.9.0.11
PING 10.9.0.11 (10.9.0.11) 56(84) bytes of data.
64 bytes from 10.9.0.11: icmp_seq=1 ttl=64 time=0.124 ms
64 bytes from 10.9.0.11: icmp_seq=2 ttl=64 time=0.086 ms
^C
--- 10.9.0.11 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1014ms
rtt min/avg/max/mdev = 0.086/0.105/0.124/0.019 ms
root@2d7a40d43a9c:/# telnet 10.9.0.11
Trying 10.9.0.11...
^C
root@2d7a40d43a9c:/#
```

Explanation:
iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
Specifies INPUT packets with icmp protocol should be accepted.

iptables -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT
Specifies OUTPUT packets with icmp protocol should be accepted.

iptables -P OUTPUT DROP
By default, drop output packets

iptables -P INPUT DROP
By default, drop input packets

That's why ping works(icmp protocol), but telnet fails(tcp protocol).

4B

```
root@b3d323aa865a:/# iptables -A FORWARD -i eth0 -p icmp --icmp-type echo-request -j DROP
```

1. Outside hosts cannot ping internal hosts.

```
rtt min/avg/max/mdev = 0.099/0.125/0.151/0.026 ms
root@2d7a40d43a9c:/# ping 192.168.60.5
PING 192.168.60.5 (192.168.60.5) 56(84) bytes of data.
^C
--- 192.168.60.5 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2049ms

root@2d7a40d43a9c:/#
```

2. Outside hosts can ping the router.

```
root@2d7a40d43a9c:/# ping 10.9.0.11
PING 10.9.0.11 (10.9.0.11) 56(84) bytes of data.
64 bytes from 10.9.0.11: icmp_seq=1 ttl=64 time=0.151 ms
64 bytes from 10.9.0.11: icmp_seq=2 ttl=64 time=0.099 ms
^C
```

3. Internal hosts can ping outside hosts

```
root@c1dd56178ffc:/# ping 10.9.0.5
PING 10.9.0.5 (10.9.0.5) 56(84) bytes of data.
64 bytes from 10.9.0.5: icmp_seq=1 ttl=63 time=0.148 ms
64 bytes from 10.9.0.5: icmp_seq=2 ttl=63 time=0.109 ms
64 bytes from 10.9.0.5: icmp_seq=3 ttl=63 time=0.091 ms
64 bytes from 10.9.0.5: icmp_seq=4 ttl=63 time=0.147 ms
^C
--- 10.9.0.5 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3075ms
rtt min/avg/max/mdev = 0.091/0.123/0.148/0.024 ms
root@c1dd56178ffc:/#
```

To satisfy **requirement 4,** add the following rule:

```
root@b3d323aa865a:/# iptables -A FORWARD -i eth0 -p icmp --icmp-type echo-request -j DROP
```

Telent from outside host to inside host does not work

```
root@2d7a40d43a9c:/# telnet 192.168.60.5
Trying 192.168.60.5...
^C
root@2d7a40d43a9c:/#
```

Telnet from inside host to outside host:

```
root@c1dd56178ffc:/# telnet 10.9.0.5
Trying 10.9.0.5...
^C
root@c1dd56178ffc:/#
```

4C
Before we add rules, check outside hosts can telnet to all internal hosts.

```
root@2d7a40d43a9c:/# telnet 192.168.60.5
Trying 192.168.60.5...
Connected to 192.168.60.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
c1dd56178ffc login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-107-generic x86_64)
```

```
root@2d7a40d43a9c:/# telnet 192.168.60.6
Trying 192.168.60.6...
Connected to 192.168.60.6.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
0d48f77e2d65 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-107-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
```

```
root@2d7a40d43a9c:/# telnet 192.168.60.7
Trying 192.168.60.7...
Connected to 192.168.60.7.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
e76b6462572f login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-107-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
```

Inside hosts can access outside hosts:

```
bash: telent: command not found
root@c1dd56178ffc:/# telnet 10.9.0.5
Trying 10.9.0.5...
^C
root@c1dd56178ffc:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
2d7a40d43a9c login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-107-generic x86_64)
```

On seed-router, set up the rules

```
root@b3d323aa865a:/# iptables -A FORWARD -i eth0 -d 192.168.60.5 -p tcp --dport 23 -j ACCEPT
```

```
root@b3d323aa865a:/# iptables -A FORWARD -i eth1 -s 192.168.60.5 -p tcp --sport 23 -j ACCEPT
```

```
root@b3d323aa865a:/# iptables -P FORWARD DROP
```

Ip tables looks like below:

```
root@b3d323aa865a:/# iptables -t filter -L -n --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination

Chain FORWARD (policy DROP)
num  target     prot opt source               destination
1    ACCEPT     tcp  --  0.0.0.0/0            192.168.60.5         tcp dpt:23
2    ACCEPT     tcp  --  192.168.60.5         0.0.0.0/0            tcp spt:23

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
```

1. All the internal hosts run a telnet server (listening to port 23). Outside hosts can only access the telnet server on 192.168.60.5, not the other internal hosts.

```
^C
seed@2d7a40d43a9c:~$ telnet 192.168.60.5
Trying 192.168.60.5...
Connected to 192.168.60.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
c1dd56178ffc login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-107-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Thu Apr 21 00:15:35 UTC 2022 from 10.9.0.5 on pts/2
```

2. Outside hosts cannot access other internal servers

```
Last login: Thu Apr 21 00:30:22 UTC 2022 fro
seed@2d7a40d43a9c:~$ telent 192.168.60.6
-bash: telent: command not found
seed@2d7a40d43a9c:~$ telnet 192.168.60.6
Trying 192.168.60.6...
^C
seed@2d7a40d43a9c:~$ telnet 192.168.60.7
Trying 192.168.60.7...
^C
```

3. Internal hosts can access all the internal servers.
On host2-192.168.60.6

```
root@0d48f77e2d65:/# telnet 192.168.60.7
Trying 192.168.60.7...
Connected to 192.168.60.7.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
e76b6462572f login:
```

```
root@0d48f77e2d65:/# telnet 192.168.60.5
Trying 192.168.60.5...
Connected to 192.168.60.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
c1dd56178ffc login:
```

On host1-192.168.60.5:

```
root@c1dd56178ffc:/# telnet 192.168.60.7
Trying 192.168.60.7...
Connected to 192.168.60.7.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
e76b6462572f login:
```

```
root@c1dd56178ffc:/# telnet 192.168.60.6
Trying 192.168.60.6...
Connected to 192.168.60.6.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
0d48f77e2d65 login:
```

On host3-192.168.60.7:

```
root@e76b6462572f:/# telnet 192.168.60.5
Trying 192.168.60.5...
Connected to 192.168.60.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
c1dd56178ffc login:
```

```
root@e76b6462572f:/# telnet 192.168.60.6
Trying 192.168.60.6...
Connected to 192.168.60.6.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
0d48f77e2d65 login:
```

4. Internal hosts cannot access external servers.

```
root@c1dd56178ffc:/# telnet 10.9.0.5
Trying 10.9.0.5...
^C
root@c1dd56178ffc:/#
```

Section 6

Without the second rule:

```
root@2d7a40d43a9c:/# ping 192.168.60.5
PING 192.168.60.5 (192.168.60.5) 56(84) bytes of data.
64 bytes from 192.168.60.5: icmp_seq=1 ttl=63 time=0.094 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=63 time=0.119 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=63 time=0.151 ms
64 bytes from 192.168.60.5: icmp_seq=4 ttl=63 time=0.107 ms
64 bytes from 192.168.60.5: icmp_seq=5 ttl=63 time=0.119 ms
64 bytes from 192.168.60.5: icmp_seq=6 ttl=63 time=0.106 ms
64 bytes from 192.168.60.5: icmp_seq=7 ttl=63 time=0.107 ms
64 bytes from 192.168.60.5: icmp_seq=8 ttl=63 time=0.106 ms
64 bytes from 192.168.60.5: icmp_seq=9 ttl=63 time=0.115 ms
64 bytes from 192.168.60.5: icmp_seq=10 ttl=63 time=0.162 ms
64 bytes from 192.168.60.5: icmp_seq=11 ttl=63 time=0.107 ms
64 bytes from 192.168.60.5: icmp_seq=12 ttl=63 time=0.117 ms
64 bytes from 192.168.60.5: icmp_seq=13 ttl=63 time=0.127 ms
64 bytes from 192.168.60.5: icmp_seq=14 ttl=63 time=0.106 ms
64 bytes from 192.168.60.5: icmp_seq=15 ttl=63 time=0.144 ms
64 bytes from 192.168.60.5: icmp_seq=16 ttl=63 time=0.106 ms
64 bytes from 192.168.60.5: icmp_seq=17 ttl=63 time=0.120 ms
64 bytes from 192.168.60.5: icmp_seq=18 ttl=63 time=0.101 ms
64 bytes from 192.168.60.5: icmp_seq=19 ttl=63 time=0.125 ms
64 bytes from 192.168.60.5: icmp_seq=20 ttl=63 time=0.105 ms
64 bytes from 192.168.60.5: icmp_seq=21 ttl=63 time=0.146 ms
```

With the second rule:

```
--- 192.168.60.5 ping statistics ---
21 packets transmitted, 21 received, 0% packet loss, time 20470ms
rtt min/avg/max/mdev = 0.094/0.118/0.162/0.017 ms
root@2d7a40d43a9c:/# ping 192.168.60.5
PING 192.168.60.5 (192.168.60.5) 56(84) bytes of data.
64 bytes from 192.168.60.5: icmp_seq=1 ttl=63 time=0.098 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=63 time=0.141 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=63 time=0.147 ms
64 bytes from 192.168.60.5: icmp_seq=4 ttl=63 time=0.111 ms
64 bytes from 192.168.60.5: icmp_seq=5 ttl=63 time=0.124 ms
64 bytes from 192.168.60.5: icmp_seq=7 ttl=63 time=0.109 ms
64 bytes from 192.168.60.5: icmp_seq=13 ttl=63 time=0.122 ms
64 bytes from 192.168.60.5: icmp_seq=19 ttl=63 time=0.140 ms
64 bytes from 192.168.60.5: icmp_seq=25 ttl=63 time=0.113 ms
64 bytes from 192.168.60.5: icmp_seq=31 ttl=63 time=0.104 ms
64 bytes from 192.168.60.5: icmp_seq=37 ttl=63 time=0.108 ms
64 bytes from 192.168.60.5: icmp_seq=43 ttl=63 time=0.107 ms
64 bytes from 192.168.60.5: icmp_seq=48 ttl=63 time=0.107 ms
64 bytes from 192.168.60.5: icmp_seq=54 ttl=63 time=0.109 ms
64 bytes from 192.168.60.5: icmp_seq=60 ttl=63 time=0.111 ms
^C
```

The second rule is necessary. When number of packets reaches 5, the first rule for 10/minute applies, meaning that we can only forward packets every 6 seconds(10/minute). On second rule we set the policy DROP to drop the unnecessary packets from 10.9.0.5 to 192.168.60.5 by default. Without the second rule, we can receive all the ICMP reply packets as usual.

Section 7

Nth mode:
On seed-router, add the rules suggested by Lab description first:

```
root@b3d323aa865a:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode nth --every 3 --packet 0 -j DNAT --to-destination 192.168.60.5:8080
root@b3d323aa865a:/#
```

On 10.9.0.5:

```
root@2d7a40d43a9c:/# echo hello | nc -u 10.9.0.11 8080
```

We can see on 198.162.60.5, the UPD packet is received

```
root@c1dd56178ffc:/# nc -luk 8080
hello
```

Add more rules. Explanation: we are adding rules so that the packets are sent to 192.168.60.6 for the first packet of remaining every 2 packets, and packets are sent to 192.168.60.7 for the first packet of remaining 1 packet.

```
root@b3d323aa865a:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode nth --every 3 --packet 0 -j DNAT --to-destination 192.168.60.5:8080
root@b3d323aa865a:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode nth --every 2 --packet 0 -j DNAT --to-destination 192.168.60.6:8080
root@b3d323aa865a:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode nth --every 1 --packet 0 -j DNAT --to-destination 192.168.60.7:8080
root@b3d323aa865a:/# iptables -t nat -L -n
```

On nat table:

```
root@b3d323aa865a:/# iptables -t nat -L -n
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination
DNAT       udp  --  0.0.0.0/0            0.0.0.0/0            udp dpt:8080 statistic mode nth every 3 to:192.168.60.5:8080
DNAT       udp  --  0.0.0.0/0            0.0.0.0/0            udp dpt:8080 statistic mode nth every 2 to:192.168.60.6:8080
DNAT       udp  --  0.0.0.0/0            0.0.0.0/0            udp dpt:8080 statistic mode nth every 1 to:192.168.60.7:8080
```

On 10.9.0.5:

```
root@2d7a40d43a9c:/# echo "hello1" | nc -u 10.9.0.11 8080
```

On 192.168.60.5, we can see hello1 printed

```
root@c1dd56178ffc:/# nc -luk 8080
hello
hello1
```

No other outputs on other two internal services.

On 10.9.0.5:

```
root@2d7a40d43a9c:/# echo "hello2" | nc -u 10.9.0.11 8080
```

On 192.168.60.6, we can see hello2 printed

```
seed@ubuntu-s-1vcpu-2gb-nyc1-01:~$ docksh 0d
root@0d48f77e2d65:/# nc -luk 8080
hello2
```

No other outputs on other two internal services.

On 10.9.0.5:

```
root@2d7a40d43a9c:/# echo "hello3" | nc -u 10.9.0.11 8080
```

On 192.168.60.7, we can see hello3 printed

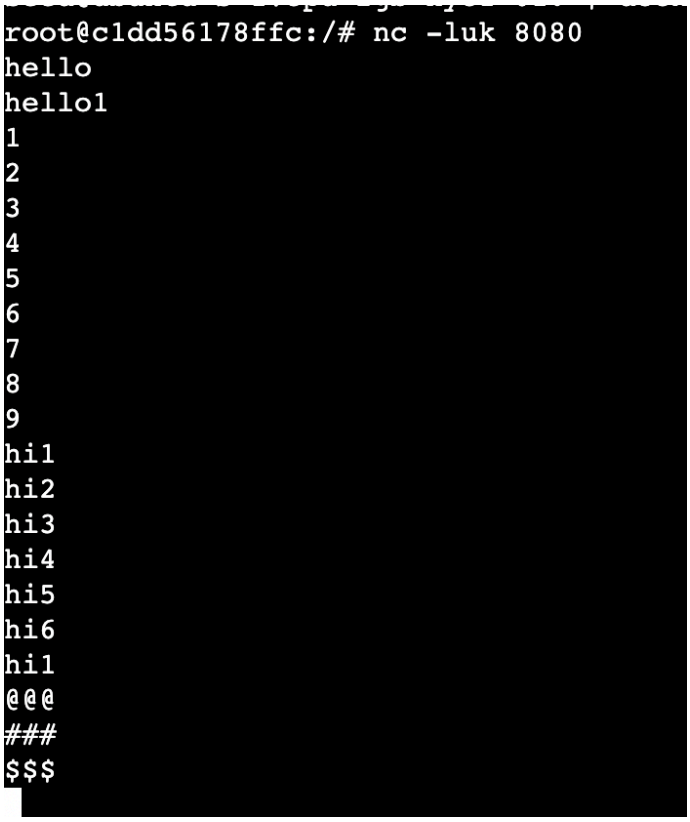
```
root@e76b6462572f:/# nc -luk 8080
hello3
```

No other outputs on other two internal services.

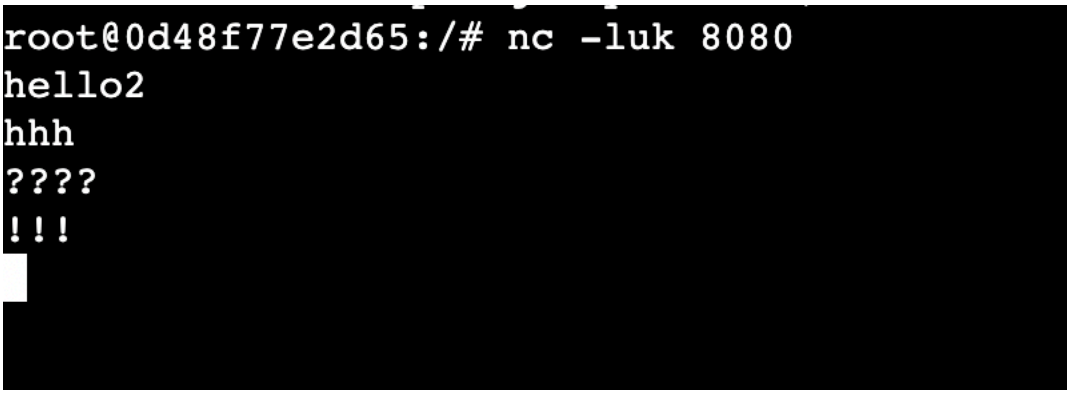
If we choose to echo dynamically on 10.9.0.5:

```
root@2d7a40d43a9c:/# nc -u 10.9.0.11 8080
1
2
3
4
5
6
7
8
9
hi1
hi2
hi3
hi4
hi5
hi6
hi1
hhh
????
!!!
12232
3432
@@@
###
$$$
```

On the three internal servers we see the following output:
On 192.168.68.5



On 192.168.60.6



On 192.168.60.7:

```
seed@ubuntu-s-1vcpu-2gb-nyc1-01:~$ docksh e7
root@e76b6462572f:/# nc -luk 8080
hello3
12232
3432
```

We can see the UDP servers follow the round-robin pattern to receive UDP packets

Random mode
Add those policies on seed-router.
Explanation: For every three packets, 1/3 probability to go to 192.168.60.5
For every remaining two packets, 0.5 probability to go to 192.168.60.5
For every remaining one packet, 1 probability to go to 192.168.60.7

```
root@b3d323aa865a:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode random --probability 0.33333 -j DNAT --to-destination 192.168.60.5:
8080
root@b3d323aa865a:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode random --probability 0.5 -j DNAT --to-destination 192.168.60.6:8080
root@b3d323aa865a:/# iptables -t nat -A PREROUTING -p udp --dport 8080 -m statistic --mode random --probability 1 -j DNAT --to-destination 192.168.60.7:8080
root@b3d323aa865a:/#
```

On 10.9.0.5, randomly echo some messages:

```
^C
seed@ubuntu-s-1vcpu-2gb-nyc1-01:~$ echo "111" | nc -u 10.9.0.11 8080
^C
seed@ubuntu-s-1vcpu-2gb-nyc1-01:~$ echo "222" | nc -u 10.9.0.11 8080
^C
seed@ubuntu-s-1vcpu-2gb-nyc1-01:~$ echo "333" | nc -u 10.9.0.11 8080
^C
seed@ubuntu-s-1vcpu-2gb-nyc1-01:~$ echo "444" | nc -u 10.9.0.11 8080
^C
seed@ubuntu-s-1vcpu-2gb-nyc1-01:~$ echo "555" | nc -u 10.9.0.11 8080
^C
seed@ubuntu-s-1vcpu-2gb-nyc1-01:~$ echo "666" | nc -u 10.9.0.11 8080
^C
seed@ubuntu-s-1vcpu-2gb-nyc1-01:~$ echo "777" | nc -u 10.9.0.11 8080
^C
seed@ubuntu-s-1vcpu-2gb-nyc1-01:~$ echo "888" | nc -u 10.9.0.11 8080
^C
seed@ubuntu-s-1vcpu-2gb-nyc1-01:~$ echo "999" | nc -u 10.9.0.11 8080
^C
seed@ubuntu-s-1vcpu-2gb-nyc1-01:~$
```

On the three servers, we can see the packets are received by the internal servers randomly.

```
^C
root@c1dd56178ffc:/# nc -luk 8080
333
444
555
888
999
```

```
root@0d48f77e2d65:/# nc -luk 8080
222
777
```

```
^C
root@e76b6462572f:/# nc -luk 8080
111
666
```