LAB WEEK 2:

NAT, Port Forwarding & Routing

DO NGOC TUAN DUY

MỤC LỤC

Week 2: Nắm vững kỹ thuật NAT, Port Forwarding & Routing.

Phần 1: NAT.

Mỗi bạn tạo 2 VM:

VM1: 1/1/20/vmbr0/vmbr1

- IP WAN: liên hệ leader để được cấp IP
- IP LAN: 10.0.0.1/24

VM2: 1/1/20/vmbr1

- IP LAN: 10.0.0.2/24 - GW: 10.0.0.1

Yêu cầu:

- Sử dụng iptables cấu hình VM1 NAT masquerade để VM2 có thể đi ra internet được thông qua VM1.
- Reboot VM1 và sau khi boot vào OS thì VM2 vẫn có thể đi ra internet được thông qua VM1.

1. Sử dụng iptables cấu hình VM1 NAT masquerade để VM2 có thể đi ra internet được thông qua VM1.

Cấu hình card mạng của VM1

```
# This is the network config written by 'subiquity'
network:
  version: 2
  renderer: networkd
  ethernets:
      ens18:
          dhcp4: no
          addresses:
            - 192.168.1.121/24
          nameservers:
           addresses:
            - 8.8.8.8
            - 8.8.4.4
          routes:
            - to: default
              via: 192.168.1.1
      ens19:
          dhcp4: no
          addresses:
            - 10.0.25.1/24
```

Cấu hình card mạng của VM2

```
 GNU nano 6.2                                  /etc/netplan/00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  version: 2
  renderer: networkd
  ethernets:
      ens18:
          dhcp4: no
          addresses:
            - 10.0.25.2/24
          nameservers:
              addresses:
                - 8.8.8.8
                - 8.8.4.4
          routes:
            - to: default
              via: 10.0.25.1
```

2. Lưu iptables để sau reboot vẫn còn

sudo apt install iptables-persistent -y

sudo netfilter-persistent save

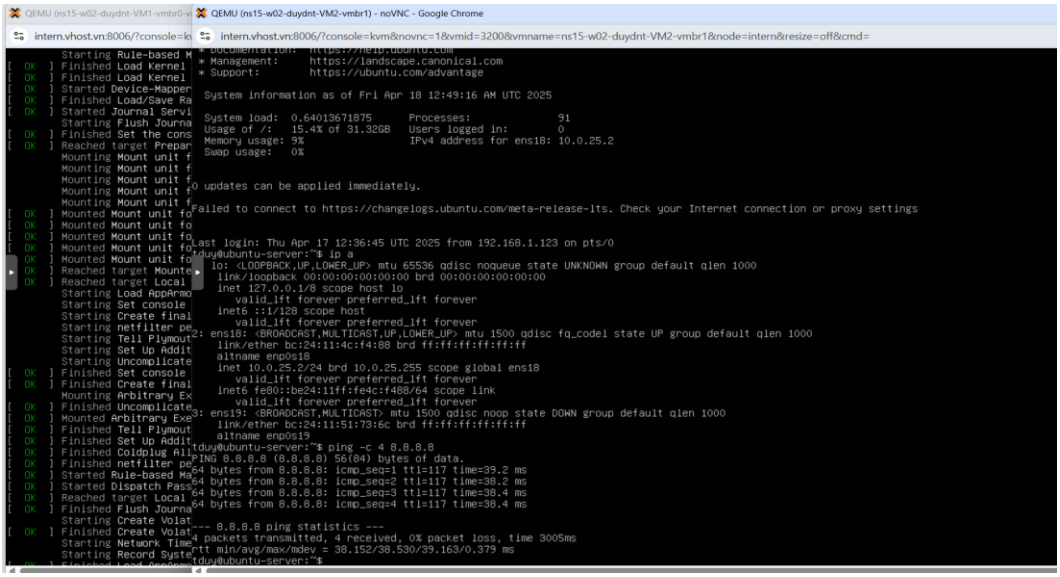
```
tduy@ubuntu-server:~$ sudo netfilter-persistent sav
run-parts: executing /usr/share/netfilter-persistent/plugins.d/15-ip4tables save
run-parts: executing /usr/share/netfilter-persistent/plugins.d/25-ip6tables save
```

NAT Masquerade (ens18 là interface WAN, ens19 là interfacce LAN)

sudo iptables -t nat -A POSTROUTING -o ens18 -j MASQUERADE

```
tduy@ubuntu-server:~$ sudo iptables -t nat -A POSTROUTING -o ens18 -j MASQUERADE
tduy@ubuntu-server:~$ sudo iptables -A FORWARD -i ens19 -o ens18 -j ACCEPT
tduy@ubuntu-server:~$ sudo iptables -A FORWARD -i ens18 -o ens19 -m state --state RELATED,ESTABLISHED -j ACCEPT
tduy@ubuntu-server:~$ sudo netfilter-persistent save
run-parts: executing /usr/share/netfilter-persistent/plugins.d/15-ip4tables save
run-parts: executing /usr/share/netfilter-persistent/plugins.d/25-ip6tables save
```

3. Reboot VM1 và sau khi boot vào OS thì VM2 vẫn có thể đi ra internet được thông qua VM1



4. Cho phép forward từ LAN sang WAN

sudo iptables -A FORWARD -i ens19 -o ens18 -j ACCEPT

sudo iptables -A FORWARD -i ens18 -o $ens19 -m state --state ESTABLISHED,RELATED -j ACCEPT

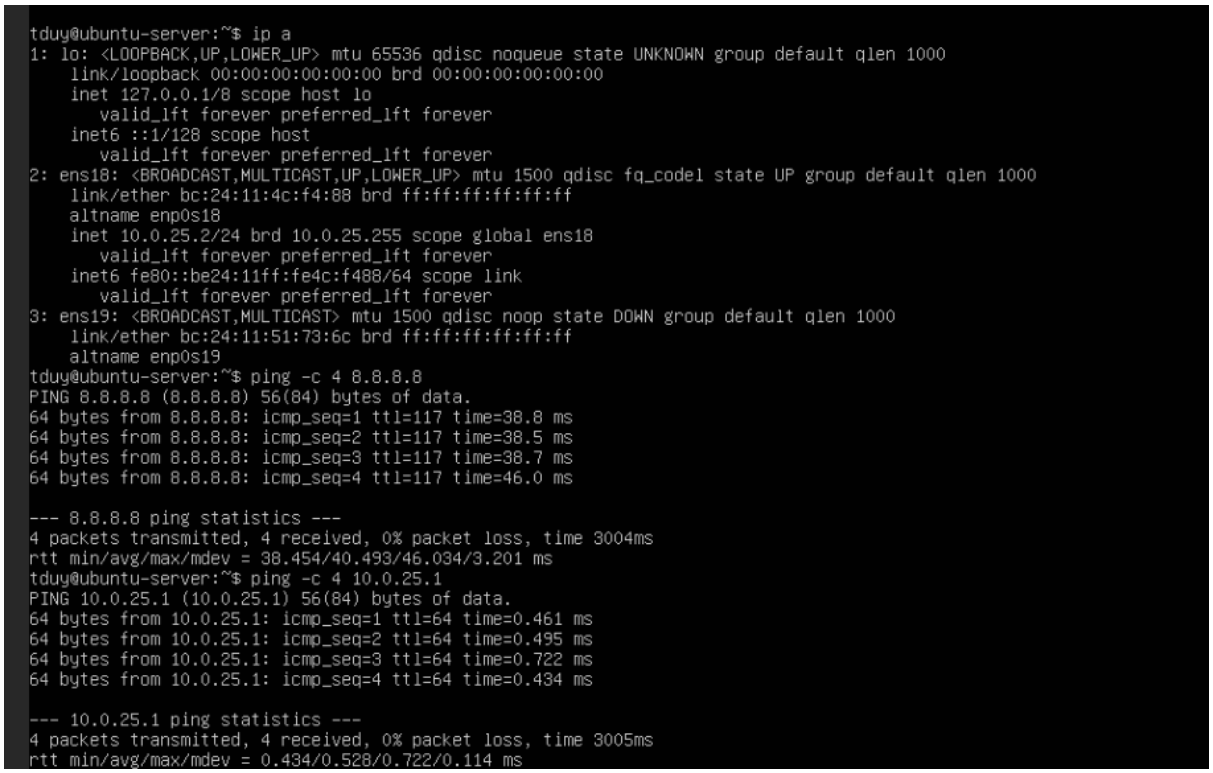
Lấy VM1 ping ra internet và ping được VM2

```
tduy@ubuntu-server:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:58:21:da brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet 192.168.1.121/24 brd 192.168.1.255 scope global ens18
       valid_lft forever preferred_lft forever
    inet6 fe80::be24:11ff:fe58:21da/64 scope link
       valid_lft forever preferred_lft forever
3: ens19: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:3d:08:36 brd ff:ff:ff:ff:ff:ff
    altname enp0s19
    inet 10.0.25.1/24 brd 10.0.25.255 scope global ens19
       valid_lft forever preferred_lft forever
    inet6 fe80::be24:11ff:fe3d:836/64 scope link
       valid_lft forever preferred_lft forever
tduy@ubuntu-server:~$ ping -c 4 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=118 time=38.9 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=118 time=39.2 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=118 time=38.1 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=118 time=41.6 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 38.137/39.468/41.593/1.288 ms
tduy@ubuntu-server:~$ ping -c 4 10.0.25.2
PING 10.0.25.2 (10.0.25.2) 56(84) bytes of data.
64 bytes from 10.0.25.2: icmp_seq=1 ttl=64 time=0.648 ms
64 bytes from 10.0.25.2: icmp_seq=2 ttl=64 time=0.445 ms
64 bytes from 10.0.25.2: icmp_seq=3 ttl=64 time=0.617 ms
64 bytes from 10.0.25.2: icmp_seq=4 ttl=64 time=0.782 ms

--- 10.0.25.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 0.445/0.623/0.782/0.120 ms
```

Từ VM2 thì có thể ping được VM1 và internet



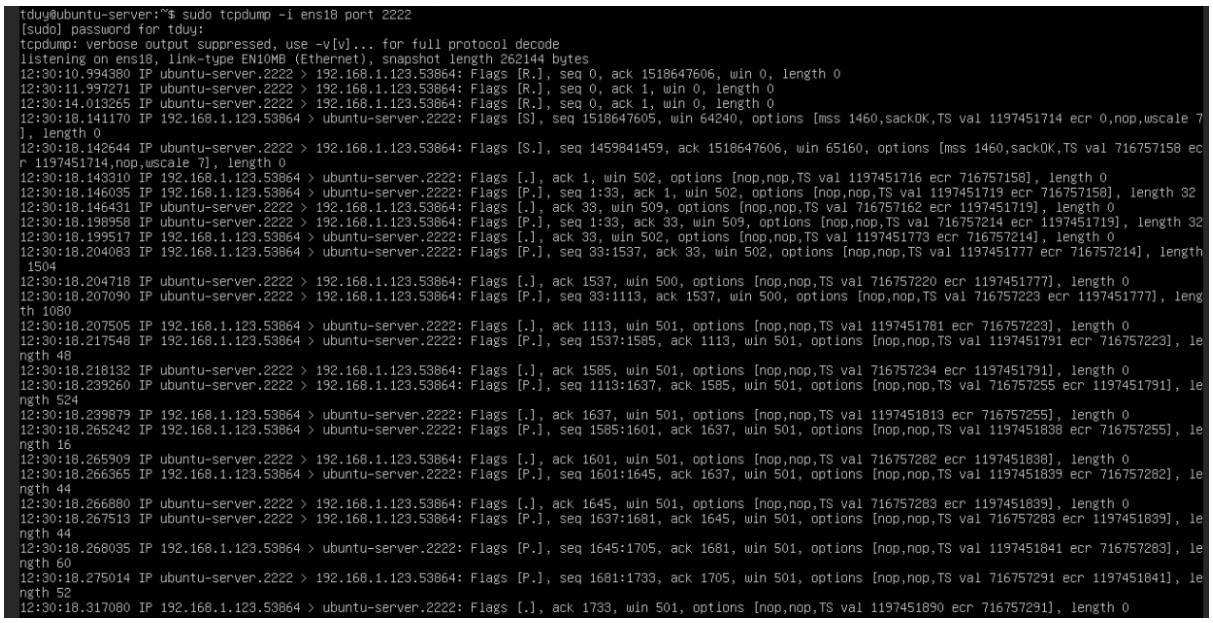
Phần 2: Port Forwarding.

Yêu cầu:

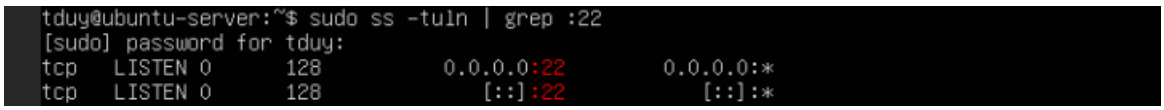
- Cấu hình port forwarding trên VM1 để khi SSH vào IP WAN của VM1(192.168.1.121) port 2222 thì có thể truy cập được SSH được thẳng vào VM2.

1. Cấu hình port forwarding trên VM1

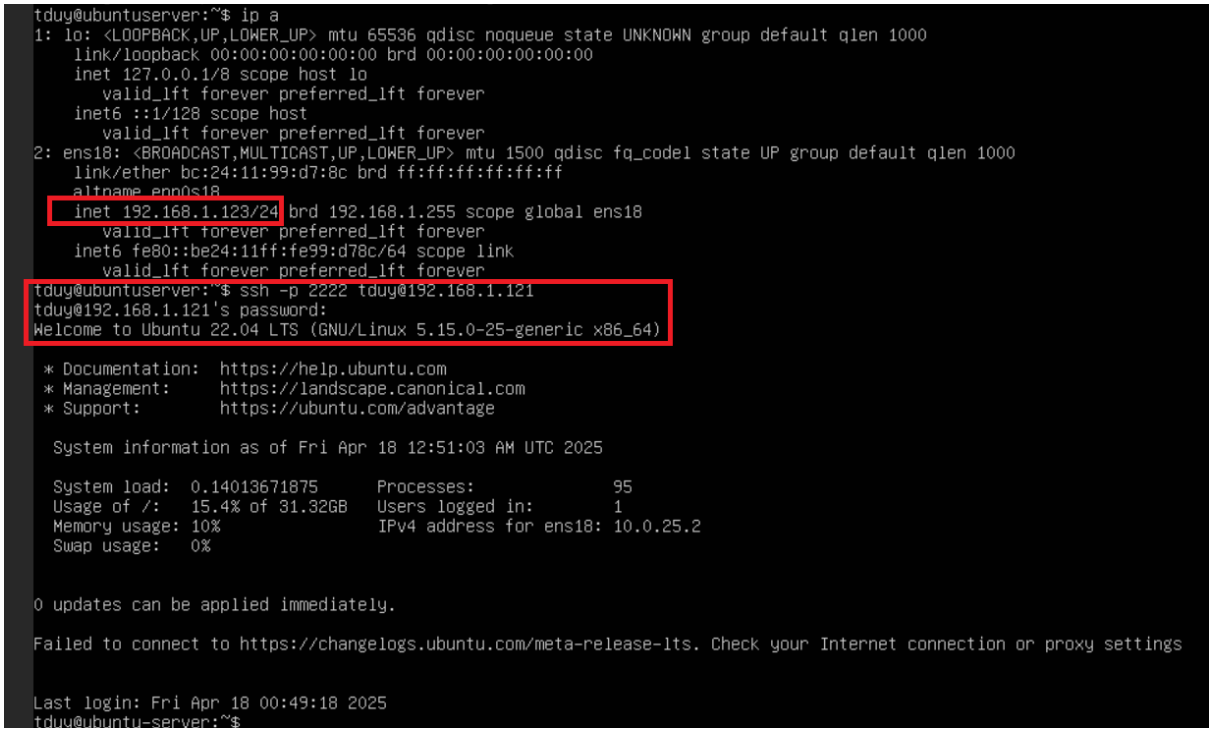
2. Dò thử trên VM1 cổng 2222 IP WAN đã có packet chưa



3. Máy VM2 cũng đang lắng nghe trên port 22 mà port forwarding đã ánh xạ từ port 2222



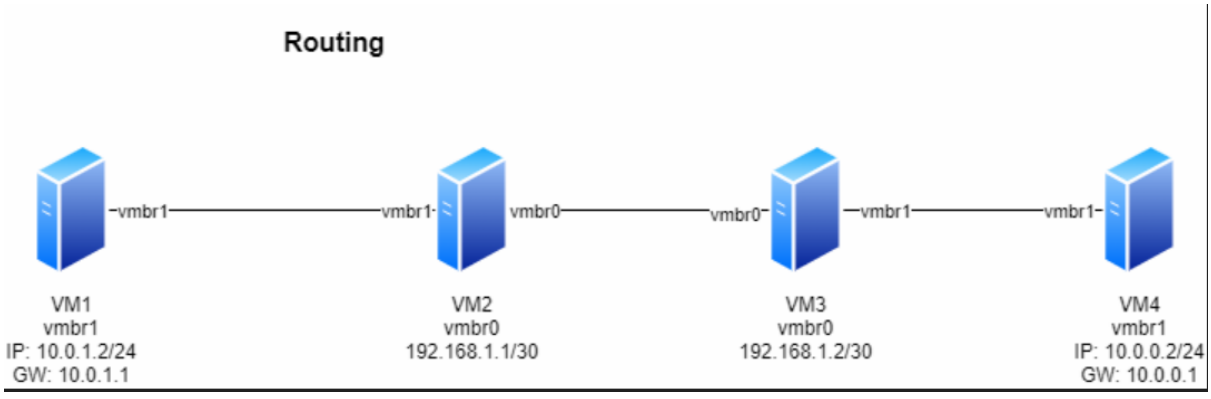
4. **Kết quả đã thành công ssh từ máy client có IP là 192.168.1.123 sang máy 192.168.1.123**



Phần 3: Routing.

Môi trường: đề tài yêu cầu 2 bạn làm chung 1 bài lab. Mỗi bạn được cấp 2 VM và cấu hình mạng như hình sau:

- Bạn 1: VM2 (có vmbr0 và vmbr1) và VM1 (only vmbr1)
- Bạn 2: VM3 (có vmbr0 và vmbr1) và VM4 (only vmbr1)



Yêu cầu:

- Cấu hình VM2 và VM3 để cho network của VM4 và VM1 có thể ping thấy nhau.
- Reboot lại VM2 và VM3 thì hệ thống vẫn hoạt động bình thường (sau khi vào OS).

Cấu hình các máy VM

VM1

- IP: 10.0.25.2
- GW: 10.0.25.1

VM2

- IP WAN: 192.168.1.121
- IP LAN: 10.0.25.1

VM3

- IP WAN: 192.168.1.81
- IP LAN: 10.0.0.1

VM4

- IP: 10.0.0.2
- GW: 10.0.0.1

1. Bật IP Forwarding trên máy VM2

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

Ghi vào file hệ thống

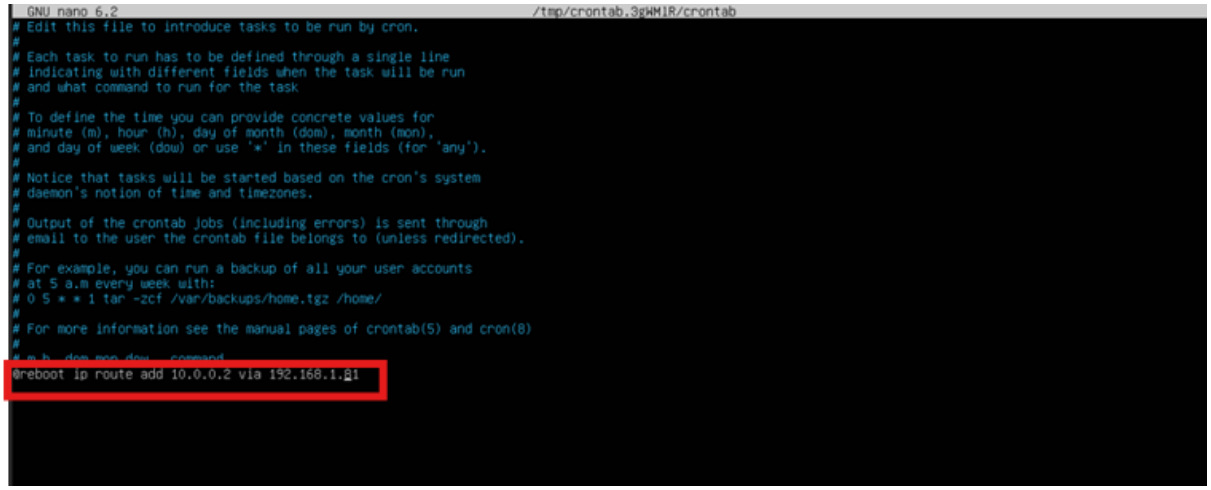
```
169  sudo echo "net.ipv4.ip_forward=1" >> sudo /etc/sysctl.conf
```

2. Cấu hình route đặt đường mặc định để thêm vào bảng định tuyến để máy tính có thể gửi gói tin đến địa chỉ IP 10.0.0.2 thông qua cổng (gateway) 192.168.1.81

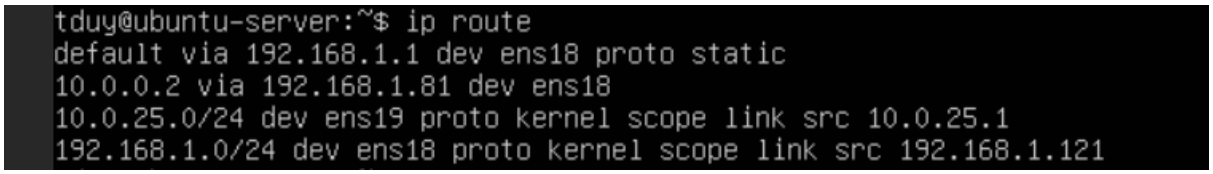
```
170  sudo ip route add 10.0.0.2/24 via 192.168.1.81
171  sudo ip route add 10.0.0.2 via 192.168.1.81
```

3. Để route tồn tại sau khi reboot, thêm vào crontab dùng sudo crontab -e

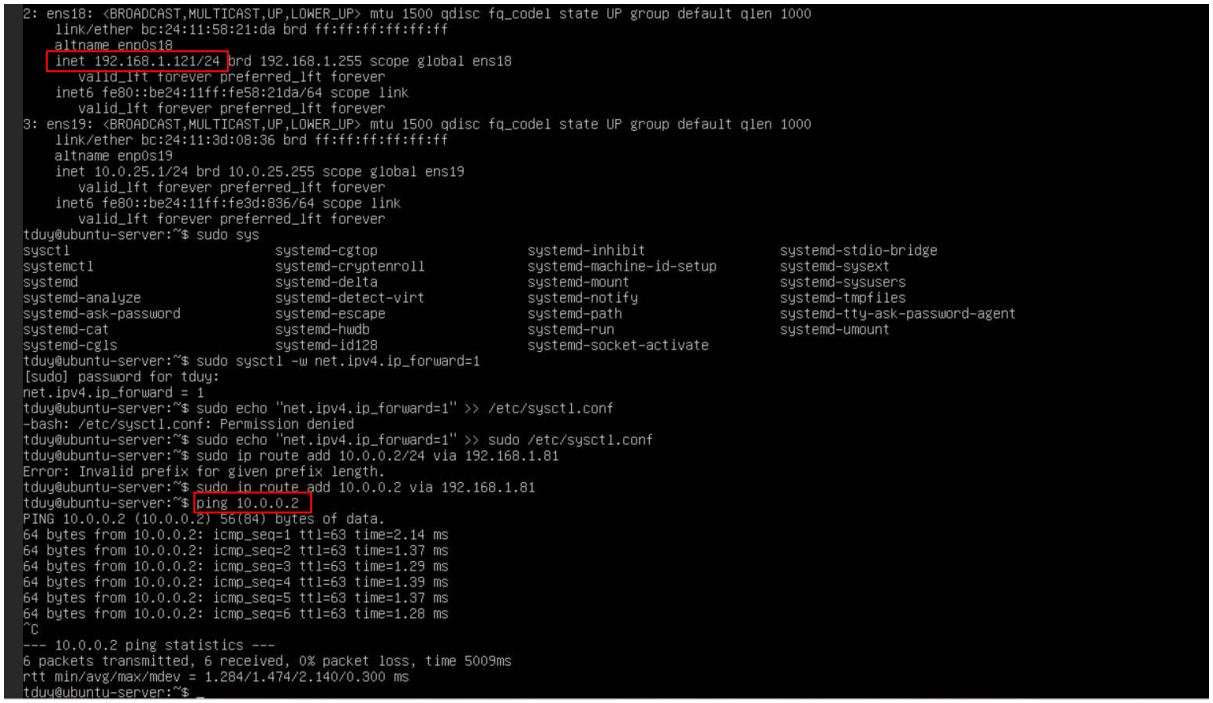
@reboot ip root add 10.0.0.2 via 192.168.1.81



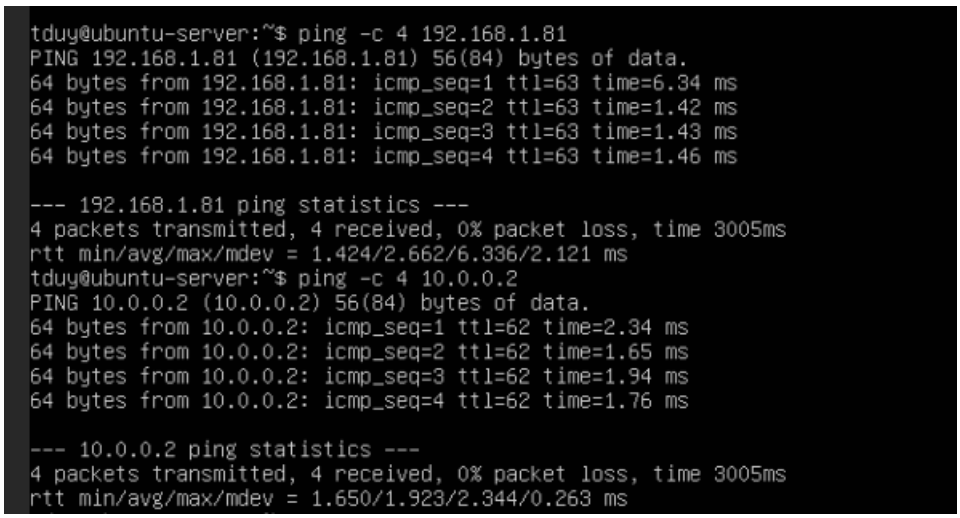
4. Sau khi cấu hình thì được kết quả



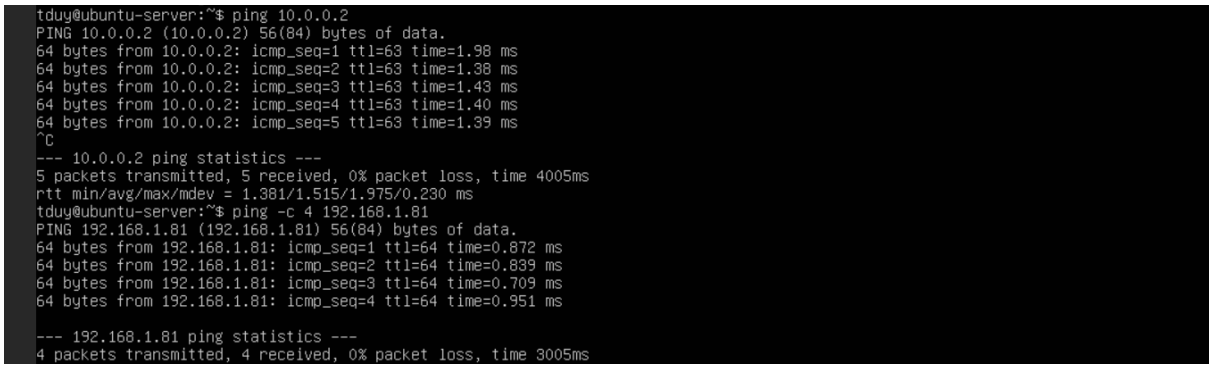
5. Kết quả dùng VM2(IP: 192.168.1.121) ping cho VM4 (IP: 10.0.0.2) thành công



6. Kết quả VM1 ping được tới VM3 và VM4 thành công



7. Kết quả VM2 ping tới VM3 và VM4 thành công



8. **Reboot lại VM2 thì hệ thống vẫn hoạt động bình thường (sau khi vào OS) do có cấu hình trong crontab**