



LAB WEEK 2: NAT, Port Forwarding & Routing

NGUYEN CONG LUC

nguyencongluc.82@gmail.com

[Luc Nguyen | LinkedIn](#)

0329206845

MỤC LỤC

<i>MỤC TIÊU</i>	3
<i>Phần 1. NAT</i>	5
1.1 Yêu cầu	5
1.2 Cấu hình IP LAN để 2 VM thông nhau, VM2 ping ra được internet	5
1.2.1 Cấu hình IP cho VM1	6
1.2.2 Cấu hình IP cho VM2	7
1.3 Cấu hình NAT Masquerade trên VM1	9
1.3.1 Bật tính năng IP Forwarding	9
1.3.2 Cấu hình NAT với iptables trên VM1	10
1.4 Lưu iptables để không mất khi reboot	10
<i>Phần 2. Port Forwarding</i>	11
2.1 Yêu cầu	11
2.2 Cấu hình Port Forwarding trên VM1:	11
2.3 Tùy chỉnh SSH config ở 2 VM:	11
2.3.1 SSH config ở VM1	11
2.3.2 SSH config ở VM2	12
2.3.3 Thực hiện SSH từ client vào VM2 qua IP WAN VM1	13
<i>Phần 3. Routing</i>	14
3.1 Yêu cầu	14
3.2 Cấu hình VM2 và VM3 để cho network của VM4 và VM1 có thể ping thấy nhau	15
3.2.1 Cấu hình Static Routing trên VM1 và VM2	16
3.2.2 Cấu hình Static Routing trên VM3 và VM4	18
3.2.3 Thực hiện ping từ VM1 sang VM4 và ngược lại	20
3.2.4 Reboot lại VM2 và VM3 thì hệ thống vẫn hoạt động bình thường (sau khi vào OS)	20

MỤC TIÊU

Week2: Nắm vững kỹ thuật NAT, Port Forwarding & Routing.

Phần 1: NAT.

Mỗi bạn tạo 2 VM:

VM1: 1/1/20/vmbr0/vmbr1

- IP WAN: 45.122.223.122
- IP LAN: 10.0.x.1/24

VM2: 1/1/20/vmbr0

- IP LAN: 10.0.x.2/24 - GW: 10.0.x.1

x: Là số cuối trong IP card mạng ra net(ens18) của VM1 (192.168.186.x)

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.

Phần 2: Port Forwarding.

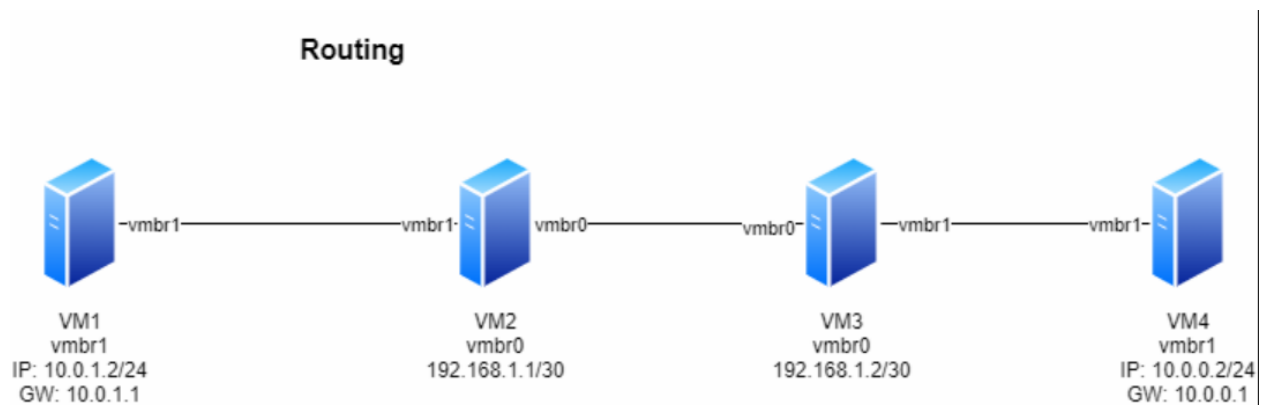
Yêu cầu:

- Cấu hình port forwarding trên VM1 để khi SSH vào IP WAN của VM1 port 2223 thì có thể truy cập được SSH được thẳng vào VM2.

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)
- IP các máy không cần giống ảnh



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).

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.x.1/24

VM2: 1/1/20/vmbr1

- IP LAN: 10.0.x.2/24 - GW: 10.0.x.1

Giá trị x của các bạn như sau:

- Lấy theo giá trị cuối của IP card mạng 1 ra Internet ví dụ 192.168.186.21 thì x là 21.

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.

Phần 2: Port Forwarding.

Yêu cầu:

- Cấu hình port forwarding trên VM1 để khi SSH vào IP WAN của VM1 port 2223 thì có thể truy cập được SSH được thẳng vào VM2.

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:

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

Phần 1. NAT

1.1 Yêu cầu

Tạo 2 VM:

VM1: 1/1/20/vmbr0/vmbr1 (Dùng lại server ở Lab1)

- IP WAN: liên hệ leader để được cấp IP (IP WAN ở lab 1)
- IP LAN: 10.0.25.1/24

VM2: 1/1/20/vmbr1

- IP LAN: 10.0.25.2/24 - GW: 10.0.25.1

Yêu cầu:

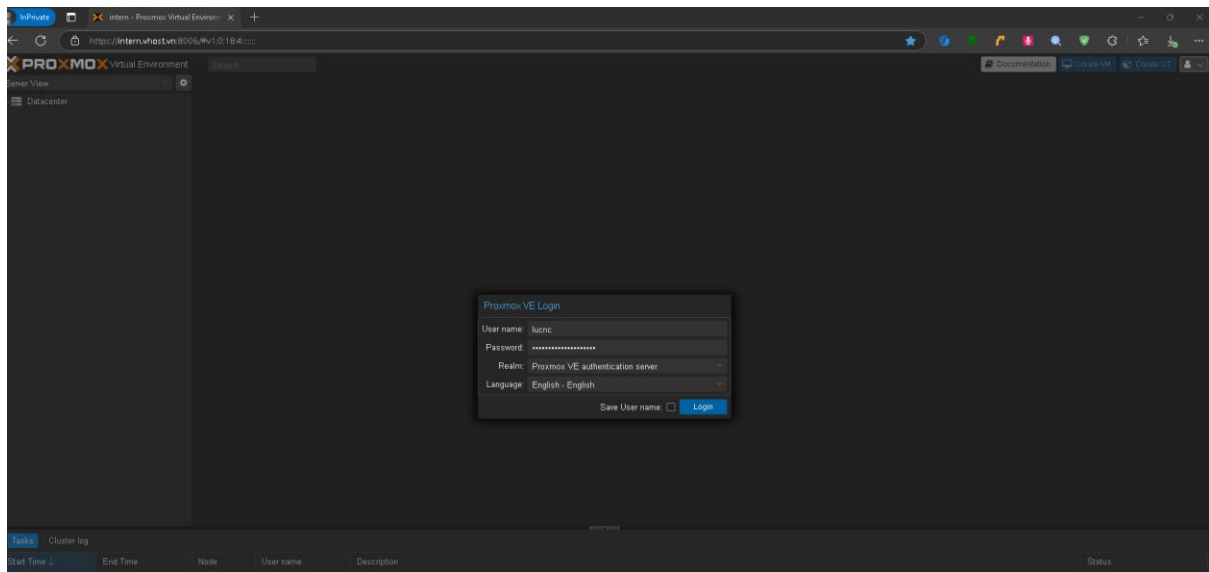
- Sử dụng iptables cấu hình VM1 NAT masquerade để VM2 có thể đi ra internet được thông qua VM1.
- Reboot VM1 và sau khi boot vào OS thì VM2 vẫn có thể đi ra internet được thông qua VM1.

(VM1 cần có 2 IP để mô phỏng một cấu trúc mạng có nhiều lớp, với một mạng nội bộ riêng biệt cho các máy ảo và một mạng kết nối internet.

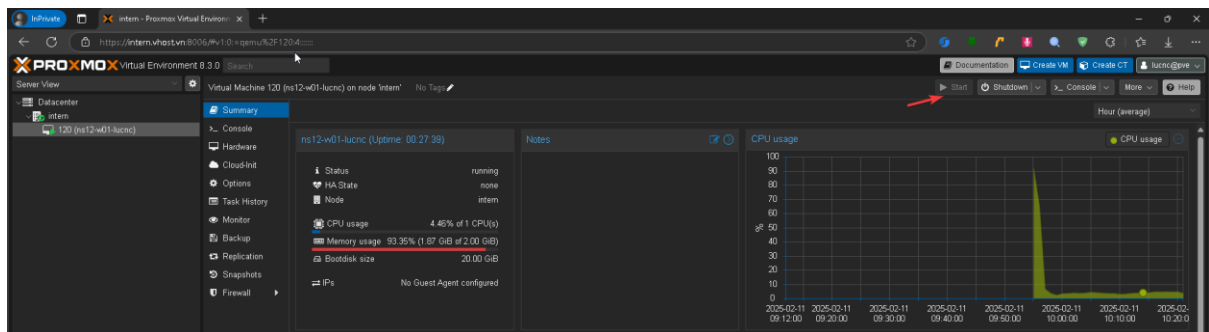
Việc tạo thêm IP 10.0.25.1 giúp dễ dàng quản lý và bảo mật, Cách ly các mạng giữa các máy ảo với mạng ngoài)

1.2 Cấu hình IP LAN để 2 VM thông nhau, VM2 ping ra được internet

- Truy cập server vHost triển khai trên Proxmox tại link: <https://intern.vhost.vn:8006/> và dùng tài khoản mật khẩu lưu tại keepass

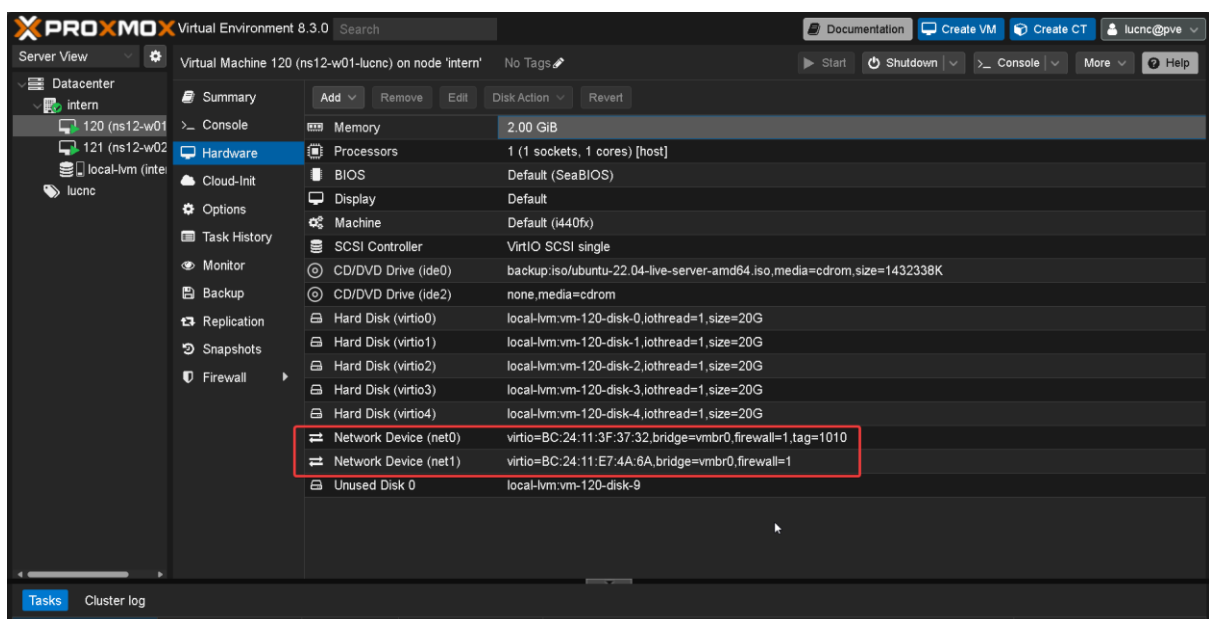


- Start Virtual Machine at dashboard



1.2.1 Cấu hình IP cho VM1

- Chuẩn bị các card mạng:



- Chỉnh sửa file cấu hình mạng trên VM1:

`sudo nano /etc/netplan/00-installer-config.yaml`

- Thêm cấu hình IP cho interface ens19

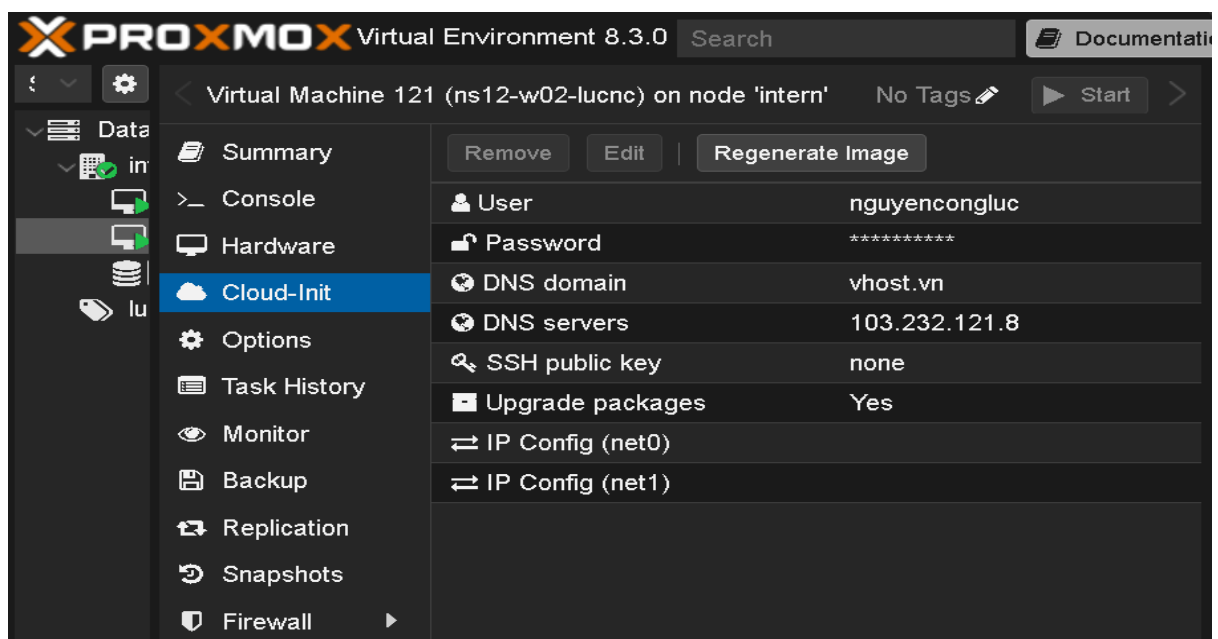
```
GNU nano 6.2
# This is the network config written by 'subiquity'
network:
  version: 2
  renderer: networkd
  ethernets:
    ens18:
      dhcp4: no
      addresses:
        - 192.168.186.25/24
      # routes:
      #   - to: default
      #     via: 192.168.186.1
      gateway4: 192.168.186.1
      # routes:
      #   - to: 10.0.26.0/24
      #     via: 192.168.186.26
      gateway4: 192.168.186.1
      nameservers:
        addresses:
          - 8.8.8.8
          - 8.8.4.4
    ens19:
      dhcp4: no
      addresses:
        - 10.0.25.1/24
```

- Xác nhận lại cấu hình: `sudo netplan apply`

```
nguyencongluc@ubuntu-server:~$ sudo netplan apply
```

1.2.2 Cấu hình IP cho VM2

- Set user và password cho VM2 ở Cloud-Init:



The screenshot shows the Proxmox Virtual Environment 8.3.0 interface. The main panel displays the configuration for Virtual Machine 121 (ns12-w02-lucnc) on node 'intern'. The 'Cloud-Init' tab is selected, showing the following settings:

Field	Value
User	nguyencongluc
Password	*****
DNS domain	vhost.vn
DNS servers	103.232.121.8
SSH public key	none
Upgrade packages	Yes
IP Config (net0)	
IP Config (net1)	

- Trong giao diện chính chạy lệnh để xem tên file cấu hình mạng: ls /etc/netplan

```
nguyencongluc@ns12-w02-lucnc:~$ ls /etc/netplan
50-cloud-init.yaml
```

- Mở file cấu hình mạng trên VM2: sudo nano /etc/netplan/50-cloud-init.yaml:

Và chỉnh sửa thành ảnh dưới(gateway phải trở về VM1)

```
GNU nano 6.2 /etc/netplan/50-cloud-init.yaml
network:
  version: 2
  ethernets:
    eth0:
      addresses:
        - 10.0.25.2/24
#      dhcp6: true
      match:
        macaddress: bc:24:11:c4:80:e3
      nameservers:
        addresses:
          - 103.232.121.8
        search:
          - vhost.vn
      #routes:
      #- to: default
      #   via: 10.0.1.1
      gateway4: 10.0.25.1
#      routes:
#        - to: 10.0.26.0/24
#          via: 10.0.25.1
```

- Xác nhận cấu hình: sudo netplan apply

```
nguyencongluc@ns12-w02-lucnc:~$ sudo netplan apply
nguyencongluc@ns12-w02-lucnc:~$
```

-Thử ping thành công từ VM2 về gateway-VM1 thành công

```
nguyencongluc@ns12-w02-lucnc:~$ ping 10.0.25.1
PING 10.0.25.1 (10.0.25.1) 56(84) bytes of data.
64 bytes from 10.0.25.1: icmp_seq=1 ttl=64 time=0.805 ms
64 bytes from 10.0.25.1: icmp_seq=2 ttl=64 time=0.493 ms
```


- Ping ngược lại từ gateway-VM1 sang VM2

```
root@ubuntu-server:~# ping 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=0.593 ms
64 bytes from 10.0.25.2: icmp_seq=2 ttl=64 time=0.569 ms
64 bytes from 10.0.25.2: icmp_seq=3 ttl=64 time=0.606 ms
```

- Ping từ gateway-VM2 sang internet thành công

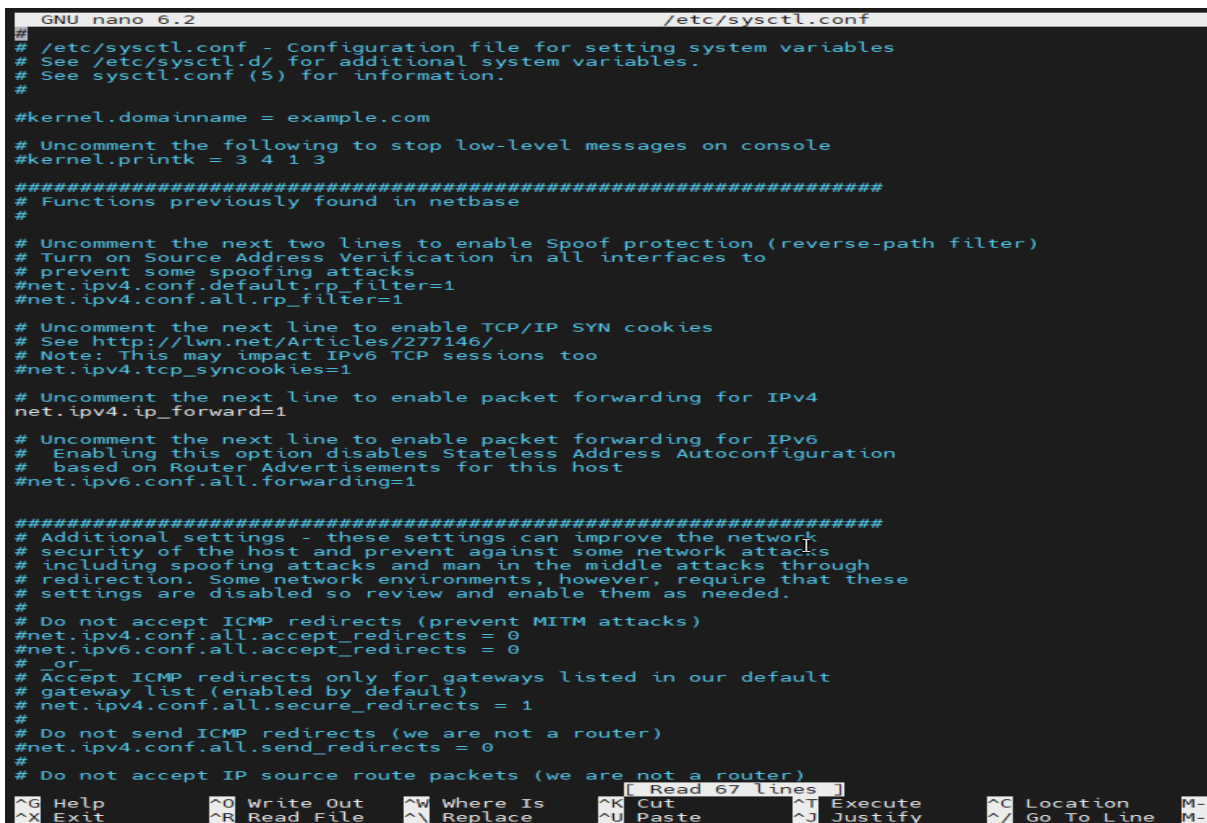
```
nguyencongluc@ns12-w02-lucnc:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=114 time=59.4 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=114 time=57.5 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=114 time=58.8 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=114 time=57.6 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 57.465/58.312/59.400/0.808 ms
```

1.3 Cấu hình NAT Masquerade trên VM1

1.3.1 Bật tính năng IP Forwarding

- Cách 1(Khuyên dùng): chỉnh sửa file cấu hình: `sudo nano /etc/sysctl.conf`

Bật dòng `net.ipv4.ip_forward = 1`



```
GNU nano 6.2 /etc/sysctl.conf
# /etc/sysctl.conf - Configuration file for setting system variables
# See /etc/sysctl.d/ for additional system variables.
# See sysctl.conf (5) for information.
#
#kernel.domainname = example.com
# Uncomment the following to stop low-level messages on console
#kernel.printk = 3 4 1 3
#####
# Functions previously found in netbase
#
# Uncomment the next two lines to enable Spoof protection (reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1
#
# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1
#
# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1
#
# Uncomment the next line to enable packet forwarding for IPv6
# Enabling this option disables Stateless Address Autoconfiguration
# based on Router Advertisements for this host
#net.ipv6.conf.all.forwarding=1
#####
# Additional settings - these settings can improve the network
# security of the host and prevent against some network attacks
# including spoofing attacks and man in the middle attacks through
# redirection. Some network environments, however, require that these
# settings are disabled so review and enable them as needed.
#
# Do not accept ICMP redirects (prevent MITM attacks)
#net.ipv4.conf.all.accept_redirects = 0
#net.ipv6.conf.all.accept_redirects = 0
#_or_
# Accept ICMP redirects only for gateways listed in our default
# gateway list (enabled by default)
# net.ipv4.conf.all.secure_redirects = 1
#
# Do not send ICMP redirects (we are not a router)
#net.ipv4.conf.all.send_redirects = 0
#
# Do not accept IP source route packets (we are not a router)
```

- Cách 2(Cẩn thận khi dùng vì có thể tạo thêm lệnh lặp): Thêm `net.ipv4.ip_forward = 1` với lệnh: `echo "net.ipv4.ip_forward = 1" | sudo tee -a /etc/sysctl.conf`

- Xác nhận thay đổi: `sudo sysctl -p`

```
nguyencongluc@ubuntu-server:~$ sudo sysctl -p
net.ipv4.ip_forward = 1
```

1.3.2 Cấu hình NAT với iptables trên VM1

- Download iptables nếu chưa có:

`sudo apt install iptables-persistent -y`

```
root@ubuntu-server:~# apt install iptables-persistent -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
iptables-persistent is already the newest version (1.0.16).
0 upgraded, 0 newly installed, 0 to remove and 285 not upgraded.
```

- Xem tất cả các rule iptables: `sudo iptables -L -v -n`

- Nếu tồn tại dùng các lệnh sau để xóa:

- + Xóa tất cả các rules trong bảng filter: `sudo iptables -F`

- + Xóa tất cả các rules trong bảng nat: `sudo iptables -t nat -F`

- + Xóa tất cả các rules trong bảng mangle: `sudo iptables -t mangle -F`

- + Xóa tất cả các rules trong bảng raw: `sudo iptables -t raw -F`

- Thêm rule NAT

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

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

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

```
nguyencongluc@ubuntu-server:~$ sudo iptables -t nat -A POSTROUTING -o ens18 -j MASQUERADE
nguyencongluc@ubuntu-server:~$ sudo iptables -A FORWARD -i ens19 -o ens18 -j ACCEPT
nguyencongluc@ubuntu-server:~$ sudo iptables -A FORWARD -i ens18 -o ens19 -m state --state RELATED,ESTABLISHED -j ACCEPT
```

- Lệnh 1 (MASQUERADE): Cho phép các máy trong mạng nội bộ sử dụng địa chỉ IP của VM1 để truy cập internet.

- Lệnh 2 (FORWARD từ LAN ra WAN): Cho phép các gói tin từ mạng nội bộ (LAN) đi ra internet (WAN).

- Lệnh 3 (FORWARD từ WAN về LAN): Cho phép các gói tin phản hồi từ internet trở về các máy trong mạng nội bộ.

1.4 Lưu iptables để không mất khi reboot

- Sử dụng lệnh:

`iptables-save > /etc/iptables/rules.v4`

```
root@ubuntu-server:~# iptables-save > /etc/iptables/rules.v4
```

Phần 2. Port Forwarding

2.1 Yêu cầu

Yêu cầu: Cấu hình port forwarding trên VM1 để khi SSH vào IP WAN của VM1 port 2223 thì có thể truy cập được SSH được thẳng vào VM2.

2.2 Cấu hình Port Forwarding trên VM1:

- Sử dụng iptables để chuyển tiếp port 2223 trên VM1 đến port 22 trên VM2 bằng các lệnh sau:

```
iptables -t nat -A PREROUTING -p tcp --dport 2223 -j DNAT --to-destination 10.0.25.2:22
```

```
iptables -t nat -A POSTROUTING -p tcp -d 10.0.25.2 --dport 22 -j MASQUERADE
```

```
iptables -A FORWARD -p tcp -d 10.0.25.2 --dport 22 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
```

```
root@ubuntu-server:~# iptables -t nat -A PREROUTING -p tcp --dport 2223 -j DNAT --to-destination 10.0.25.2:22
root@ubuntu-server:~# iptables -t nat -A POSTROUTING -p tcp -d 10.0.25.2 --dport 22 -j MASQUERADE
root@ubuntu-server:~# iptables -A FORWARD -p tcp -d 10.0.25.2 --dport 22 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
```

Lệnh 1: Chuyển tiếp gói tin TCP đến cổng 2222 sang địa chỉ 10.0.0.2 và cổng 22.

Lệnh 2: Thay đổi địa chỉ IP nguồn của gói tin đến 10.0.0.2 trên cổng 22 để phù hợp với địa chỉ IP của thiết bị gửi.

Lệnh 3: Cho phép gói tin TCP mới, đã thiết lập hoặc liên quan đến 10.0.0.2 trên cổng 22 được chuyển tiếp.

- Lưu cấu hình 4

để sau khi reboot, cấu hình vẫn được áp dụng:

```
iptables-save > /etc/iptables/rules.v4
```

```
root@ubuntu-server:~# iptables-save > /etc/iptables/rules.v4
```

2.3 Tùy chỉnh SSH config ở 2 VM:

2.3.1 SSH config ở VM1

- Giữ nguyên nội dung file config VM1 ở lab 1: `sudo nano /etc/ssh/sshd_config`

PubkeyAuthentication yes

PasswordAuthentication no

ChallengeResponseAuthentication no

2.3.2 SSH config ở VM2

- Trong file cấu hình SSH của VM2 sửa lại như sau:

+ chạy lệnh `sudo nano /etc/ssh/sshd_config`

+ sửa hoặc thêm nếu chưa tồn tại:

`PubkeyAuthentication yes`

`ChallengeResponseAuthentication no`

`PasswordAuthentication no` (Đảm bảo dòng này ở cuối file)

```
GNU nano 6.2 /etc/ssh/sshd_config
#VersionAddendum none

# no default banner path
#Banner none

# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

# override default of no subsystems
Subsystem sftp /usr/lib/openssh/sftp-server

# Example of overriding settings on a per-user basis
#Match User anoncvs
#       X11Forwarding no
#       AllowTcpForwarding no
#       PermitTTY no
#       ForceCommand cvs server
ChallengeResponseAuthentication no
PasswordAuthentication no
```

- Reset lại service để nhận cấu hình mới:

`sudo systemctl restart sshd`

```
nguyencongluc@ns12-w02-lucnc:~$ sudo systemctl restart sshd
```

- Download public key và thêm vào nơi lưu trữ server với lệnh

`sudo curl -s`

`https://raw.githubusercontent.com/lucskyost/vHost/refs/heads/main/authorized_keys >>`

`~/.ssh/authorized_keys`

- Kiểm tra lại: `sudo cat ~/.ssh/authorized_keys`

```
nguyencongluc@ns12-w02-lucnc:~$ cat ~/.ssh/authorized_keys
#nguyencongluc.82@gmail.com
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCDem4ZafOr+/nAWYDCMEyYDdo6G2A8OhjMgt9DTjy7Na1x8FP
osptxhiiPXpt1EU390lPkQzIxhuom9D4h+8gYTngOGXafRsZW/OIFoAQRieb+DgJPlntiyCYVj8UpC6C14Nm+t
/3FzmsaqCz6oOrgQWFxQhNs/OLFrwVZ2UdCoIPXPwgV6IgsKXwRasvXQNSm5g7sXZ21eKB1+6++M2H3sdNg72u
2euvmmkOzR8T9FHV9G/Db8LypbXsk2PVtGNaoQJdkA3430I63QUm3BcoOZ1Hb0BdcAv1AiDpLs518LrPW7pU2zT
3T5BfT4OFTBkqydM4E3I1bc9faAYfC1Iifx7GM3SiEamNUdWBf6qdjc+VKzTFBap3x600M9haehEGXLFsABNkzh
gvRyErC63+Jh1PdCo11K0EmSXxIzWN2bUL0HJE/JYxVgCP11G07q2Q/YtgoXuvMRR63Xw8Lo2/JwAv+BdzjdU
FOz2hdGuryxMoRPLYCemxqArL5Ypbt/Q+uuVZthjtTpcotk8oY0ThvsiylabPKqAuWikzUY/g7gAutqfdyl8Up
fA3gXt/GpFJi8z42e4xulNpHY8Su6m9Kb90P6UANcPWYXnvULTH4vFwwIQYNTry+S+BoY3zgg8/NfpcbRAIGH2
h17dWTnnzIXsKpG1KosrT6b9SlUGOfEUXQ== nguyencongluc.82@gmail.com
```

- Gán quyền để đảm file chứa key được toàn quyền truy cập

`chmod 700 ~/.ssh`

`chmod 600 ~/.ssh/authorized_keys`

```
nguyencongluc@ns12-w02-lucnc:~$ chmod 700 ~/.ssh
nguyencongluc@ns12-w02-lucnc:~$ chmod 600 ~/.ssh/authorized_keys
```

2.3.3 Thực hiện SSH từ client vào VM2 qua IP WAN VM1

- Dùng CMD của window để SSH vào VM2 với public key, qua port 2223 và IP WAN của VM1 bằng lệnh:

```
ssh -i "C:\Users\Nguyen Cong Luc\.ssh\id_rsa" -p 2223 nguyencongluc@45.122.223.121
```

```
C:\Users\Nguyen Cong Luc>ssh -i "C:\Users\Nguyen Cong Luc\.ssh\id_rsa" -p 2223 nguyencongluc@45.122.223.121
The authenticity of host '[45.122.223.121]:2223 ([45.122.223.121]:2223)' can't be established.
ED25519 key fingerprint is SHA256:ME+2Sjn38YDz9Kh90lVITJOzmmOWYPwngIKRmpMti4g.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[45.122.223.121]:2223' (ED25519) to the list of known hosts.
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 5.15.0-131-generic x86_64)

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

System information as of Fri Feb 21 07:40:52 UTC 2025

System load:  0.02               Processes:    97
Usage of /:   12.8% of 19.40GB   Users logged in: 1
Memory usage: 6%                IPv4 address for eth0: 10.0.25.2
Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

New release '24.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

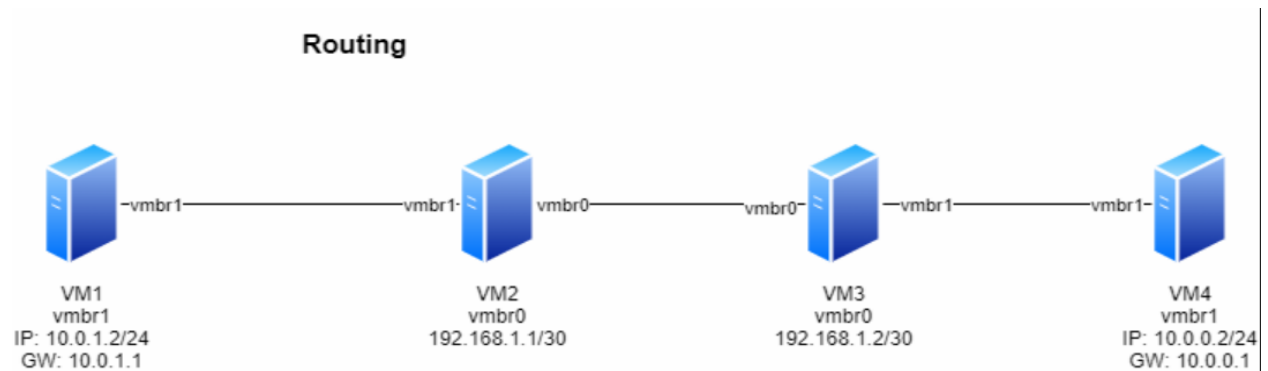
Last login: Fri Feb 21 07:38:55 2025 from 10.0.25.1
nguyencongluc@ns12-w02-lucnc:~$ |
```

Phần 3. Routing

3.1 Yêu cầu

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).

3.2 Cấu hình VM2 và VM3 để cho network của VM4 và VM1 có thể ping thấy nhau

- Bật IP forwarding ở 2 máy:

Bật IP forwarding

echo 1 > /proc/sys/net/ipv4/ip_forward

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

- Hoặc sudo nano /etc/sysctl.conf

Chỉnh net.ipv4.ip_forward=1

```
GNU nano 6.2
#
# /etc/sysctl.conf - Configuration file for setting system vari
# See /etc/sysctl.d/ for additional system variables.
# See sysctl.conf (5) for information.
#
#kernel.domainname = example.com
# Uncomment the following to stop low-level messages on console
#kernel.printk = 3 4 1 3
#####
# Functions previously found in netbase
#
# Uncomment the next two lines to enable Spoof protection (reve
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1
# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1
# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1
# Uncomment the next line to enable packet forwarding for IPv6
```

- Check ip forward: sysctl -p

```
root@ubuntu-server:~# sysctl -p
net.ipv4.ip_forward = 1
```

3.2.1 Cấu hình Static Routing trên VM1 và VM2

- Set định tuyến route cho VM2: `sudo nano /etc/netplan/00-installer-config.yaml`

```
network:
  ethernet:
    ens18:
      dhcp4: no
      addresses:
        - 192.168.186.25/24
      #
      # routes:
      #   - to: default
      #     via: 192.168.186.1
      gateway4: 192.168.186.1
      routes:
        - to: 10.0.26.0/24
          via: 192.168.186.26
      #
      gateway4: 192.168.186.1
      nameservers:
        addresses:
          - 8.8.8.8
          - 8.8.4.4
    ens19:
      dhcp4: no
      addresses:
        - 10.0.25.1/24
  version: 2
```

- Check IP VM 2:

+ ens18: 192.168.186.25/24 (kết nối với VM3)

+ ens19: 10.0.25.1/24 (Kết nối với VM1)

```
nguyencongluc@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:24:11:3f:37:32 brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet 192.168.186.25/24 brd 192.168.186.255 scope global ens18
        valid_lft forever preferred_lft forever
    inet6 fe80::be24:11ff:fe3f:3732/64 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:e7:4a:6a 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:fee7:4a6a/64 scope link
        valid_lft forever preferred_lft forever
```

- Kiểm tra định tuyến route VM2

```
nguyencongluc@ubuntu-server:~$ ip route
default via 192.168.186.1 dev ens18 proto static
10.0.25.0/24 dev ens19 proto kernel scope link src 10.0.25.1
10.0.26.0/24 via 192.168.186.26 dev ens18 proto static
192.168.186.0/24 dev ens18 proto kernel scope link src 192.168.186.25
```


- Set định tuyến route cho VM1: `sudo nano /etc/netplan/50-cloud-init.yaml`

```
network:
  version: 2
  ethernets:
    eth0:
      addresses:
        - 10.0.25.2/24
      match:
        macaddress: bc:24:11:c4:80:e3
      nameservers:
        addresses:
          - 103.232.121.8
        search:
          - vhost.vn
      #routes:
      #- to: default
      #   via: 10.0.1.1
      gateway4: 10.0.25.1
      routes:
        - to: 10.0.26.0/24
          via: 10.0.25.1
      set-name: eth0
```

- Check IP của VM1:

+ eth0: 10.0.25.2 (kết nối với VM2)

```
nguyencongluc@ns12-w02-lucnc:~$ 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: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:c4:80:e3 brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet 10.0.25.2/24 brd 10.0.25.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::be24:11ff:fec4:80e3/64 scope link
        valid_lft forever preferred_lft forever
```

- Kiểm tra định tuyến route VM1

```
nguyencongluc@ns12-w02-lucnc:~$ ip route
default via 10.0.25.1 dev eth0 proto static
10.0.25.0/24 dev eth0 proto kernel scope link src 10.0.25.2
10.0.26.0/24 via 10.0.25.1 dev eth0 proto static
```

3.2.2 Cấu hình Static Routing trên VM3 và VM4

- Set định tuyến route cho VM3: `sudo nano /etc/netplan/00-installer-config.yaml`

```
network:
  version: 2
  renderer: networkd
  ethernets:
    ens18:
      dhcp4: false
      addresses:
        - 192.168.186.26/24
      gateway4: 192.168.186.1
      nameservers:
        addresses:
          - 8.8.8.8
          - 8.8.4.4
      routes:
        - to: 10.0.25.0/24
          via: 192.168.186.25
    ens19:
      dhcp4: false
      addresses:
        - 10.0.26.1/24
```

- Check IP của VM3:

+ ens18: 192.168.186.26/24 (kết nối với VM2)

+ ens19: 10.0.26.1/24 (Kết nối với VM4)

```
root@kiennt:/home/kiennt# 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:bf:7c:aa brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet 192.168.186.26/24 brd 192.168.186.255 scope global ens18
        valid_lft forever preferred_lft forever
    inet6 fe80::be24:11ff:febf:7caa/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:24:11:36:15:f2 brd ff:ff:ff:ff:ff:ff
    altname enp0s19
    inet 10.0.26.1/24 brd 10.0.26.255 scope global ens19
        valid_lft forever preferred_lft forever
    inet6 fe80::be24:11ff:fe36:15f2/64 scope link
        valid_lft forever preferred_lft forever
root@kiennt:/home/kiennt#
```

- Kiểm tra định tuyến route VM3

```
root@kiennt:/home/kiennt# ip route show
default via 192.168.186.1 dev ens18 proto static
10.0.26.0/24 dev ens19 proto kernel scope link src 10.0.26.1
192.168.186.0/24 dev ens18 proto kernel scope link src 192.168.186.26
root@kiennt:/home/kiennt# _
```

- Set định tuyến route VM4:

sudo nano /etc/netplan/00-installer-config.yaml

```
network:
  version: 2
  ethernets:
    eth0:
      addresses:
        - 10.0.26.2/24
      dhcp6: true
      gateway4: 10.0.26.1
      match:
        macaddress: bc:24:11:60:18:45
      nameservers:
        addresses:
          - 103.232.121.8
        search:
          - vhost.vn
      set-name: eth0
      routes:
        - to: 10.0.25.0/24
          via: 10.0.26.1
```

- Check IP của VM4:

+ eth0: 10.0.26.2 (kết nối với VM3)

```
root@ns12-w02-kiennt:/home/kiennt# 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: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:60:18:45 brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet 10.0.26.2/24 brd 10.0.26.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::be24:11ff:fe60:1845/64 scope link
        valid_lft forever preferred_lft forever
root@ns12-w02-kiennt:/home/kiennt# _
```

- Kiểm tra định tuyến route VM4

```
root@ns12-w02-kiennt:/home/kiennt# ip route show
default via 10.0.26.1 dev eth0 proto static
10.0.25.0/24 via 10.0.26.1 dev eth0 proto static
10.0.26.0/24 dev eth0 proto kernel scope link src 10.0.26.2
root@ns12-w02-kiennt:/home/kiennt#
```

3.2.3 Thực hiện ping từ VM1 sang VM4 và ngược lại

- Ping từ VM2 sang VM4

```
nguyencongluc@ubuntu-server:~$ ping 10.0.26.2
PING 10.0.26.2 (10.0.26.2) 56(84) bytes of data.
64 bytes from 10.0.26.2: icmp_seq=1 ttl=63 time=1.26 ms
64 bytes from 10.0.26.2: icmp_seq=2 ttl=63 time=1.18 ms
64 bytes from 10.0.26.2: icmp_seq=3 ttl=63 time=1.09 ms
```

- Ping từ VM1 sang VM4:

```
nguyencongluc@ns12-w02-lucnc:~$ ping 10.0.26.2
PING 10.0.26.2 (10.0.26.2) 56(84) bytes of data.
64 bytes from 10.0.26.2: icmp_seq=1 ttl=62 time=4.43 ms
64 bytes from 10.0.26.2: icmp_seq=2 ttl=62 time=1.83 ms
64 bytes from 10.0.26.2: icmp_seq=3 ttl=62 time=2.18 ms
```

- Ping từ VM3 sang VM1

```
root@kiennt:/home/kiennt# ping 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=63 time=2.43 ms
64 bytes from 10.0.25.2: icmp_seq=2 ttl=63 time=1.42 ms
64 bytes from 10.0.25.2: icmp_seq=3 ttl=63 time=1.63 ms
64 bytes from 10.0.25.2: icmp_seq=4 ttl=63 time=1.43 ms
64 bytes from 10.0.25.2: icmp_seq=5 ttl=63 time=1.41 ms
```

- Ping từ VM4 sang VM1

```
root@ns12-w02-kiennt:/home/kiennt# ping 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=62 time=3.48 ms
64 bytes from 10.0.25.2: icmp_seq=2 ttl=62 time=1.89 ms
64 bytes from 10.0.25.2: icmp_seq=3 ttl=62 time=2.01 ms
64 bytes from 10.0.25.2: icmp_seq=4 ttl=62 time=1.93 ms
64 bytes from 10.0.25.2: icmp_seq=5 ttl=62 time=1.71 ms
```

3.2.4 Reboot lại VM2 và VM3 thì hệ thống vẫn hoạt động bình thường (sau khi vào OS)

- Sau khi reboot VM2, VM3, thì VM1 và VM4 vẫn ping được với nhau

```
nguyencongluc@ns12-w02-lucnc:~$ ping 10.0.26.2
PING 10.0.26.2 (10.0.26.2) 56(84) bytes of data.
64 bytes from 10.0.26.2: icmp_seq=1 ttl=62 time=4.43 ms
64 bytes from 10.0.26.2: icmp_seq=2 ttl=62 time=1.83 ms
64 bytes from 10.0.26.2: icmp_seq=3 ttl=62 time=2.18 ms
```

```
root@ns12-w02-kiennt:/home/kiennt# ping 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=62 time=3.48 ms
64 bytes from 10.0.25.2: icmp_seq=2 ttl=62 time=1.89 ms
64 bytes from 10.0.25.2: icmp_seq=3 ttl=62 time=2.01 ms
64 bytes from 10.0.25.2: icmp_seq=4 ttl=62 time=1.93 ms
64 bytes from 10.0.25.2: icmp_seq=5 ttl=62 time=1.71 ms
```