

# Thiết kế & triển khai mạng IP

Bài thực hành số 1: Kết nối liên mạng (version 3.0)

## Mục lục

1	Chuẩn bị môi trường .....	2
2	Tạo máy ảo kết nối Internet qua máy host .....	2
3	Tạo mạng LAN kết nối Internet qua máy R1.....	4
3.1	Cấu hình máy ảo R1 thành NAT router của mạng LAN01.....	4
3.2	Tạo máy trạm A, B .....	5
3.3	Sử dụng netplan để cấu hình thông số mạng.....	6
4	Tạo các mạng LAN kết nối Internet qua router R1, R2, R3.....	7
4.1	Tạo thêm các mạng LAN và router R2, R3 .....	7
4.2	Tạo thêm máy trạm X kết nối vào LAN3 .....	10
5	Phân tích giao thức với các công cụ hỗ trợ .....	11
5.1	Xem gói tin tại các kết nối mạng.....	12
5.2	Phân tích các gói tin ICMP của lệnh tracepath .....	13
5.3	Theo dõi gói tin được xử lý NAT .....	13
5.4	Tạo các kịch bản ping destination unreachable và time out .....	14

# 1 Chuẩn bị môi trường

Tham khảo: <https://users.soict.hust.edu.vn/hoangph/textbook/apdxA01-1.html>

1. Download & cài đặt Virtualbox
2. Download ISO image hệ điều hành Ubuntu Server 18.04: <https://ubuntu.com/download/server>

# 2 Tạo máy ảo kết nối Internet qua máy host

Sơ đồ mạng:

[máy ảo R1] <=====> [máy host] <=====> [Internet]

1. Thiết lập thông số chung:

## General

Basic	Advanced	Description	Disk Encryption
Name: R1			
Type: Linux			
Version: Other Linux (64-bit)			

2. Thiết lập cấu hình CPU & memory phù hợp với máy host. **Tối thiểu 1G RAM**
3. Thiết lập kết nối mạng: Adapter 1: Enable, Attached to: NAT. Các Adapter khác thiết lập không kết nối (Not attached).

## Network

Adapter 1	Adapter 2	Adapter 3	Adapter 4
<input checked="" type="checkbox"/> Enable Network Adapter			
Attached to: NAT			
Name:			
Advanced			
Adapter Type: Intel PRO/1000 MT Desktop (82540EM)			
Promiscuous Mode: Deny			
MAC Address: 0800270B0101			
<input checked="" type="checkbox"/> Cable Connected			
Port Forwarding			

## Network

Adapter 1	Adapter 2	Adapter 3	Adapter 4
<input checked="" type="checkbox"/> Enable Network Adapter			
Attached to: Not attached			
Name:			
Advanced			
Adapter Type: Intel PRO/1000 MT Desktop (82540EM)			
Promiscuous Mode: Deny			
MAC Address: 080027650102			
<input checked="" type="checkbox"/> Cable Connected			

4. Chỉnh sửa 2 byte cuối của các MAC address để dễ quản lý. Byte #1 là ký hiệu router (01, 02, 03, v.v..) và byte số 2 là ký hiệu network trong router (01,02,03,04):

Adapter 1: xx:xx:xx:xx:xx:0101

Adapter 2: xx:xx:xx:xx:xx:0102

Adapter 3: xx:xx:xx:xx:xx:0103

Adapter 4: xx:xx:xx:xx:xx:0104

- Thiết lập bộ nhớ ngoài: Storage, CDROM = file ISO ubuntu server 18.04
- Khởi động máy ảo
- Chọn menu “Install or upgrade an existing system”
- Cài đặt hệ điều hành Ubuntu Server vào máy ảo với các thông số mặc định
- Reboot R1, login root
- Kiểm tra cấu hình mạng. Dựa vào 2 byte cuối của MAC address, có thể xác định được kết nối mạng (enp0s3, enp0s8, v.v..) tương ứng với kết nối mạng vật lý nào (Adapter 1, Adapter 2, v.v..)

```
hp@R1:~$ ifconfig -a
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::a00:27ff:fe0b:101 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:0b:01:01 txqueuelen 1000 (Ethernet)
    RX packets 75 bytes 23627 (23.6 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 106 bytes 26171 (26.1 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s8: flags=4098<BROADCAST,MULTICAST> mtu 1500
    ether 08:00:27:65:01:02 txqueuelen 1000 (Ethernet)
    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

enp0s9: flags=4098<BROADCAST,MULTICAST> mtu 1500
    ether 08:00:27:2f:01:03 txqueuelen 1000 (Ethernet)
```

- Kiểm tra địa chỉ MAC để xác định kết nối nào là Adapter 1 (đang được cấu hình NAT để có thể kết nối Internet) - giả sử là *enp0s3*. Kiểm tra địa chỉ IP của *enp0s3*, nếu chưa có địa chỉ IP thì thực hiện yêu cầu gán địa chỉ IP động:

```
R1:~$ sudo dhclient -s enp0s3
R1:~$ ifconfig enp0s3
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::a00:27ff:fe0b:101 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:0b:01:01 txqueuelen 1000 (Ethernet)
    RX packets 75 bytes 23627 (23.6 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 106 bytes 26171 (26.1 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

- Kiểm tra kết nối R1 ra Internet:

```
R1~$ 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=63 time=36.0 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=63 time=36.3 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=63 time=36.6 ms
```

- Cài đặt trình soạn thảo *nano* (nếu chưa có) để làm việc với các file cấu hình:

```
R1~$ sudo apt-get install nano
Reading package lists... Done
Building dependency tree
Reading state information... Done
nano is already the newest version (4.8-1ubuntu1).
nano set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 25 not upgraded.
```

- Tìm hiểu cách lưu cấu hình vào các file config *netplan* để khởi động máy không cần cấu hình lại  
<https://vitux.com/how-to-configure-networking-with-netplan-on-ubuntu>

### 3 Tạo mạng LAN kết nối Internet qua máy R1

Sơ đồ mạng:

[máy A], [máy B] <= = LAN01: 192.168.1.0/24 ==> [R1] <= = = = => [Internet]

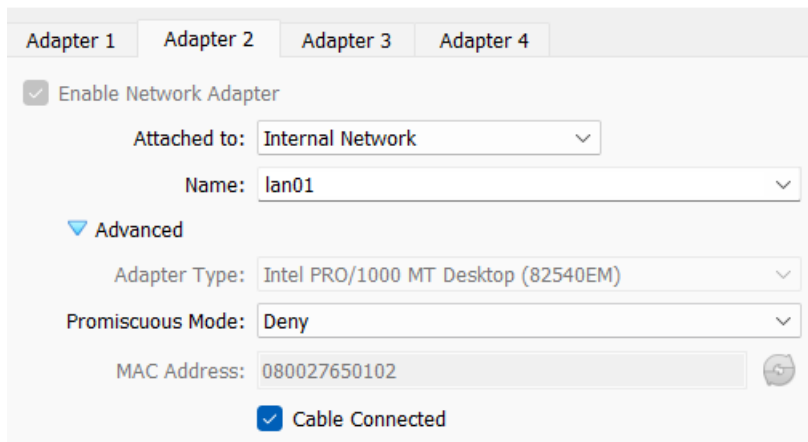
Hướng dẫn chi tiết: <https://users.soict.hust.edu.vn/hoangph/textbook/ch01-1.html>

#### 3.1 Cấu hình máy ảo R1 thành NAT router của mạng LAN01

Để các máy trong mạng ảo có thể sử dụng R1 như một Gateway đi ra Internet, R1 cần có khả năng routing với NAT (giống như máy host hỗ trợ R1 khi kết nối Internet). Các bước cần thực hiện để bật chức năng NAT routing trong R1:

1. Cấu hình kết nối mạng: Adapter 2, Attached to: Internal Network, Name: lan01

##### Network



2. Kiểm tra MAC address để xác định các kết nối mạng tương ứng với các Adapter 1 (kết nối NAT) & Adapter 2 (kết nối Internal network: lan01). Giả sử là *enp0s3* và *enp0s8*
3. Thiết lập cấu hình địa chỉ IP cho *enp0s8*:

```
hp@R1:~$ sudo ifconfig enp0s8 192.168.1.1/24
hp@R1:~$ ifconfig enp0s8
enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.1 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::a00:27ff:fe65:102 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:65:01:02 txqueuelen 1000 (Ethernet)
```

4. Kiểm tra và bật chế độ IP forward trong linux kernel (chuyển từ server mode sang routing mode):

```
hp@R1:~$ sudo sysctl net.ipv4.ip_forward
net.ipv4.ip_forward = 0
hp@R1:~$ sudo sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
```

5. Kiểm tra bảng routing của R1. Dòng default gateway (0.0.0.0) mô tả tất cả các gói tin khi cần xử lý ở R1 mà không xác định được luật forwarding trong routing table thì sẽ áp dụng luật default. Mặc định chuyển đến gateway 10.0.2.2 (là máy host) theo kết nối *enp0s3*.

```
hp@R1:~$ route -n
Kernel IP routing table
Destination    Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0        10.0.2.2       0.0.0.0         UG    100    0      0 enp0s3
10.0.2.0       0.0.0.0       255.255.255.0   U      0      0      0 enp0s3
10.0.2.2       0.0.0.0       255.255.255.255 UH     100    0      0 enp0s3
192.168.1.0    0.0.0.0       255.255.255.0   U      0      0      0 enp0s8
```

- Kiểm tra các luật iptables, bật luật *masquerade* tại vị trí POSTROUTING trên kết nối *enp0s3* để cho phép router R1 hoạt động chế độ NAT. Sau khi bật luật này, tất cả các gói tin IP khi đi ra khỏi kết nối *enp0s3* sẽ được áp dụng cơ chế NAT (thay địa chỉ IP source bằng địa chỉ IP mặt ngoài của *enp0s3*):

```
hp@R1:~$ sudo iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination

hp@R1:~$ sudo iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE
hp@R1:~$ sudo iptables -L -n -t nat -v
Chain PREROUTING (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target     prot opt in     out     source            destination

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target     prot opt in     out     source            destination

Chain OUTPUT (policy ACCEPT 4 packets, 301 bytes)
pkts bytes target     prot opt in     out     source            destination

Chain POSTROUTING (policy ACCEPT 4 packets, 301 bytes)
pkts bytes target     prot opt in     out     source            destination
  0      0 MASQUERADE all  --  *      enp0s3  0.0.0.0/0         0.0.0.0/0
```

### 3.2 Tạo máy trạm A, B

- Tạo máy ảo A, B & cài đặt hệ điều hành Ubuntu Server như với máy ảo R1, hoặc dùng chức năng “clone” từ R1 để tạo máy ảo A, B (nhanh hơn).
- Kết nối máy ảo vào mạng *lan01* (là mạng đã nối với R1): Adapter 1, Attached to: Internal Network, Name: *lan01*. Các Adapter khác để ở chế độ không kết nối (Not attached)

#### Network

Adapter 1 Adapter 2 Adapter 3 Adapter 4

☒ Enable Network Adapter

Attached to: Internal Network

Name: lan01

Advanced

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Deny

MAC Address: 080027E30A01

☒ Cable Connected

- Đổi địa chỉ MAC trong các máy A và B theo qui tắc byte cuối là 0A01, 0A02, v.v..
- Khởi động máy A, B và kiểm tra các kết nối mạng bằng địa chỉ MAC. Xác định kết nối tương ứng với Adapter 1 (đã nối vào *lan01*):

```
hp@pc01:~$ ifconfig -a
enp0s3: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether 08:00:27:e3:0a:01 txqueuelen 1000 (Ethernet)
    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

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet6 fe80::a00:27ff:fe8a:a02 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:8a:0a:02 txqueuelen 1000 (Ethernet)
```

5. Thiết lập cấu hình địa chỉ IP cho *enp0s3* theo *lan01* (192.168.1.0) và *ping* kiểm tra kết nối giữa máy A với R1

```
hp@pc01:~$ sudo ifconfig enp0s3 192.168.1.20/24
hp@pc01:~$ ifconfig enp0s3
enp0s3: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 192.168.1.20 netmask 255.255.255.0 broadcast 192.168.1.255
    ether 08:00:27:e3:0a:01 txqueuelen 1000 (Ethernet)
    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

hp@pc01:~$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=4.40 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=1.40 ms
```

6. Thiết lập default gateway là R1 và *ping* ra Internet:

```
hp@pc01:~$ sudo route add default gw 192.168.1.1
hp@pc01:~$ route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
0.0.0.0 192.168.1.1 0.0.0.0 UG 0 0 0 enp0s3
192.168.1.0 0.0.0.0 255.255.255.0 U 0 0 0 enp0s3
hp@pc01:~$ 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=2 ttl=112 time=38.4 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=112 time=41.3 ms
```

7. Kiểm tra đường đi của gói tin IP khi kết nối Internet, thấy đi qua R1 và máy host:

```
hp@pc01:~$ tracepath -n 8.8.8.8
1?: [LOCALHOST] pmtu 1500
1: 192.168.1.1 2.305ms
1: 192.168.1.1 2.245ms
2: 10.0.2.2 3.893ms
```

### 3.3 Sử dụng netplan để cấu hình thông số mạng

Các cấu hình địa chỉ IP cũng như bảng routing được cấu hình như bên trên sẽ bị hủy bỏ khi khởi động lại router hoặc máy PC. Netplan cung cấp phương pháp lưu lại các cấu hình này và tự động thiết lập lại khi khởi động hệ thống.

```
hp@pc01:~$ sudo nano /etc/netplan/00-installer-config.yaml
network:
  ethernets:
    enp0s3:
      dhcp4: false
      addresses:
        - 192.168.1.20/24
      routes:
        - to: default
          via: 192.168.1.1

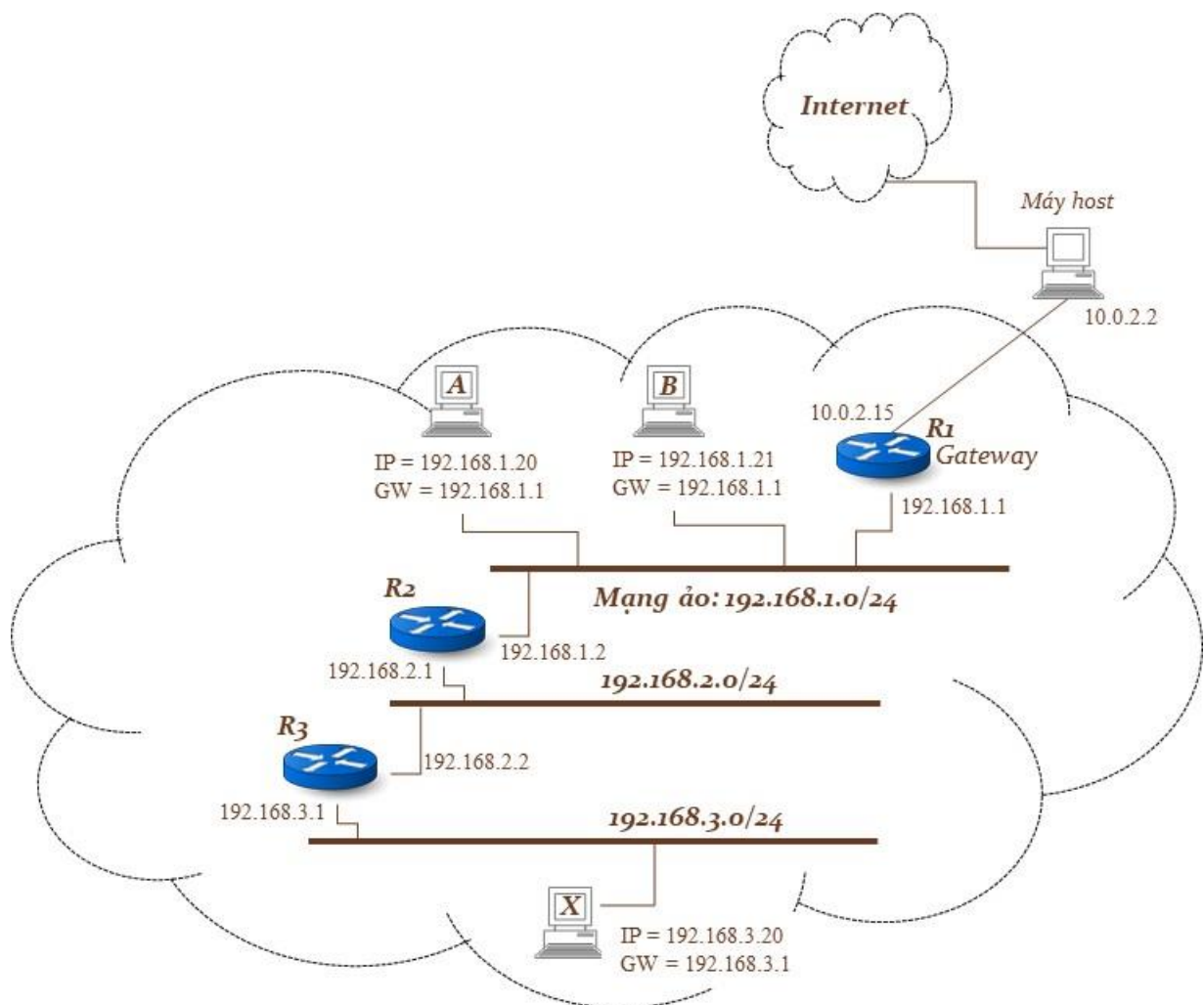
hp@pc01:~$ sudo netplan apply
hp@pc01:~$ ifconfig enp0s3
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.20 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::a00:27ff:fee3:a01 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:e3:0a:01 txqueuelen 1000 (Ethernet)
    RX packets 12 bytes 1942 (1.9 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 89 bytes 27268 (27.2 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

hp@pc01:~$ route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
0.0.0.0 192.168.1.1 0.0.0.0 UG 0 0 0 enp0s3
192.168.1.0 0.0.0.0 255.255.255.0 U 0 0 0 enp0s3
```

Tham khảo các file cấu hình netplan ở đây: <https://netplan.io/examples>

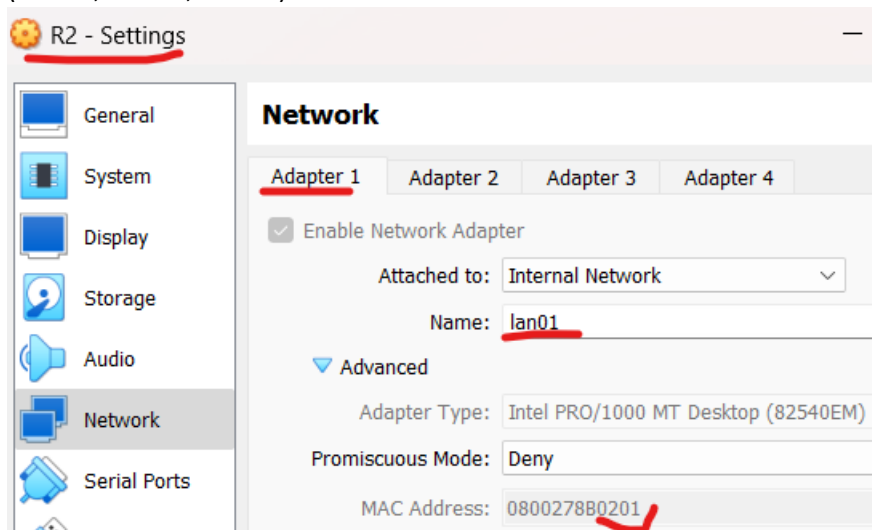
## 4 Tạo các mạng LAN kết nối Internet qua router R1, R2, R3

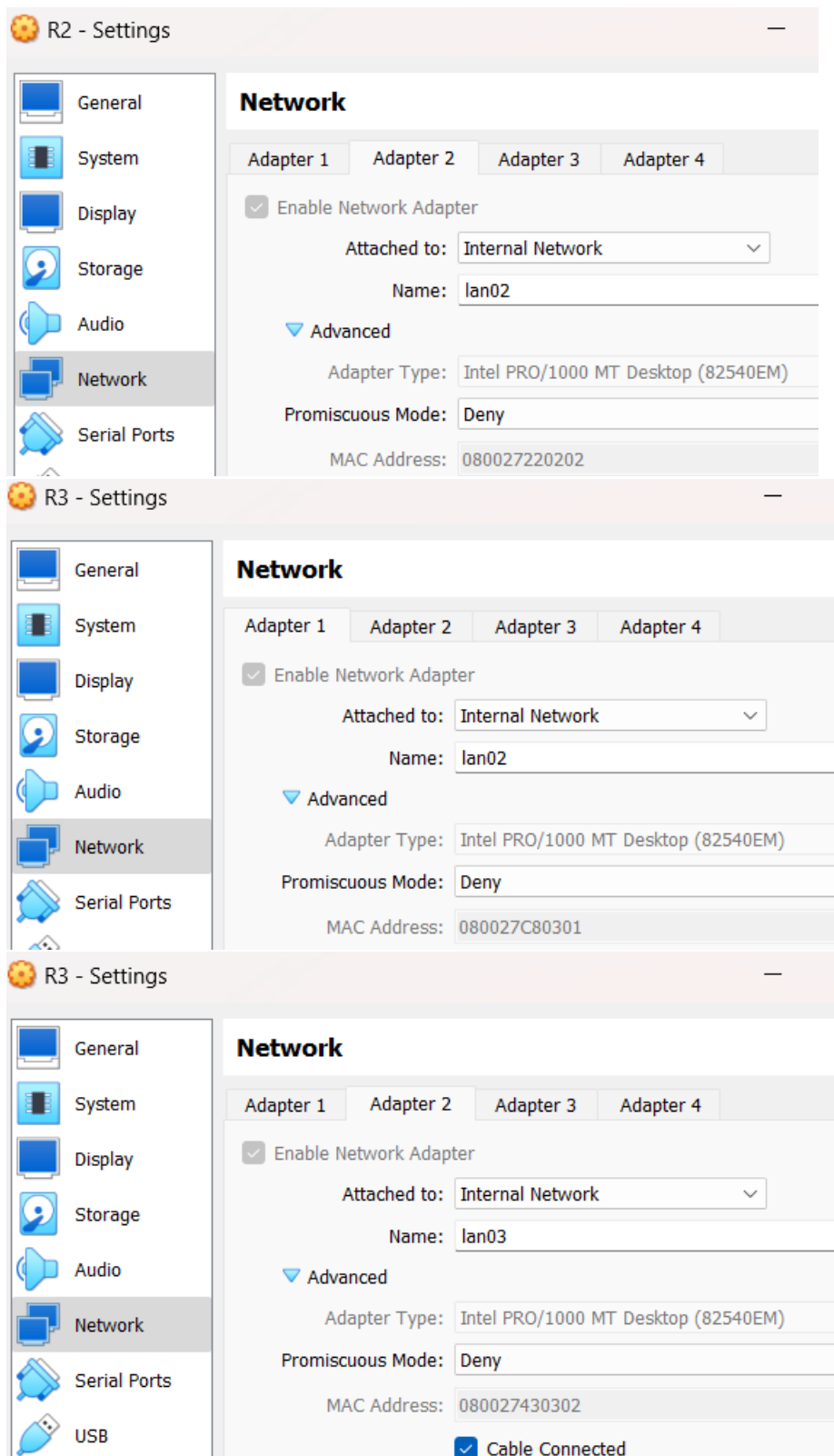
Sơ đồ mạng:



### 4.1 Tạo thêm các mạng LAN và router R2, R3

1. Clone R2 & R3 từ R1. Đặt lại các địa chỉ MAC của kết nối mạng các router theo đúng qui tắc dễ nhớ (R2: xx:xx:xx:xx:xx:0201 / xx:xx:xx:xx:xx:0202 / v.v..)
2. Router R2, R3, thiết lập 2 kết nối mạng kiểu Internal Network và lần lượt kết nối vào các mạng tương ứng (LAN01, LAN02, LAN03)





### 3. Cấu hình IP và route table trên R1

4. 

```
hp@R1:~$ sudo ifconfig enp0s8 192.168.1.1/24
hp@R1:~$ ifconfig enp0s8
enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.1 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::a00:27ff:fe65:102 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:65:01:02 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 7 bytes 586 (586.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

hp@R1:~$ route -n
Kernel IP routing table
```



```

Destination      Gateway          Genmask          Flags Metric Ref    Use Iface
0.0.0.0           10.0.2.2         0.0.0.0          UG        100    0      0 enp0s3
10.0.2.0          0.0.0.0          255.255.255.0   U         0      0      0 enp0s3
10.0.2.2          0.0.0.0          255.255.255.255 UH        100    0      0 enp0s3
192.168.1.0       0.0.0.0          255.255.255.0   U         0      0      0 enp0s8
hp@R1:~$ sudo route add -net 192.168.2.0/24 gw 192.168.1.2
hp@R1:~$ sudo route add -net 192.168.3.0/24 gw 192.168.1.2
hp@R1:~$ route -n
Kernel IP routing table
Destination      Gateway          Genmask          Flags Metric Ref    Use Iface
0.0.0.0           10.0.2.2         0.0.0.0          UG        100    0      0 enp0s3
10.0.2.0          0.0.0.0          255.255.255.0   U         0      0      0 enp0s3
10.0.2.2          0.0.0.0          255.255.255.255 UH        100    0      0 enp0s3
192.168.1.0       0.0.0.0          255.255.255.0   U         0      0      0 enp0s8
192.168.2.0       192.168.1.2      255.255.255.0   UG         0      0      0 enp0s8
192.168.3.0       192.168.1.2      255.255.255.0   UG         0      0      0 enp0s8

```

## 5. Cấu hình network bvaf bảng routing trên R2, sử dụng netplan thay cho command line:

```

hp@R2:~$ sudo nano /etc/netplan/00-installer-config.yaml
network:
  ethernet:
    enp0s3:
      dhcp4: false
      addresses: [192.168.1.2/24]
      routes:
        - to: 0.0.0.0/0
          via: 192.168.1.1
    enp0s8:
      dhcp4: false
      addresses: [192.168.2.1/24]
      routes:
        - to: 192.168.3.0/24
          via: 192.168.2.2
hp@R2:~$ sudo netplan apply
hp@R2:~$ ifconfig enp0s3
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.2 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::a00:27ff:fe8b:201 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:8b:02:01 txqueuelen 1000 (Ethernet)
    RX packets 1 bytes 60 (60.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 59 bytes 4804 (4.8 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

hp@R2:~$ ifconfig enp0s8
enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.2.1 netmask 255.255.255.0 broadcast 192.168.2.255
    inet6 fe80::a00:27ff:fe22:202 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:22:02:02 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 54 bytes 4216 (4.2 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

hp@R2:~$ route -n
Kernel IP routing table
Destination      Gateway          Genmask          Flags Metric Ref    Use Iface
0.0.0.0           192.168.1.1      0.0.0.0          UG         0      0      0 enp0s3
192.168.1.0       0.0.0.0          255.255.255.0   U         0      0      0 enp0s3
192.168.2.0       0.0.0.0          255.255.255.0   U         0      0      0 enp0s8
192.168.3.0       192.168.2.2      255.255.255.0   UG         0      0      0 enp0s8

```

## 6. Cấu hình network bvaf bảng routing trên R3, sử dụng netplan thay cho command line:

```

hp@R3:~$ sudo nano /etc/netplan/00-installer-config.yaml
network:
  ethernet:
    enp0s3:
      dhcp4: false
      addresses: [192.168.2.2/24]
      routes:
        - to: 192.168.1.0/24
          via: 192.168.2.1
    enp0s8:
      dhcp4: false
      addresses: [192.168.3.1/24]
hp@R3:~$ ifconfig enp0s3
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500

```

```

inet 192.168.2.2 netmask 255.255.255.0 broadcast 192.168.2.255
inet6 fe80::a00:27ff:fec8:301 prefixlen 64 scopeid 0x20<link>
ether 08:00:27:c8:03:01 txqueuelen 1000 (Ethernet)
RX packets 5 bytes 376 (376.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 20 bytes 1618 (1.6 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

hp@R3:~$ ifconfig enp0s8
enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.3.1 netmask 255.255.255.0 broadcast 192.168.3.255
inet6 fe80::a00:27ff:fe43:302 prefixlen 64 scopeid 0x20<link>
ether 08:00:27:43:03:02 txqueuelen 1000 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 13 bytes 1046 (1.0 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

hp@R3:~$ route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
192.168.1.0 192.168.2.1 255.255.255.0 UG 0 0 0 enp0s3
192.168.2.0 0.0.0.0 255.255.255.0 U 0 0 0 enp0s3
192.168.3.0 0.0.0.0 255.255.255.0 U 0 0 0 enp0s8

```

## 7. Thiết lập chế độ routing cho R1, R2, R3:

```

hp@R1:~$ sudo sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
hp@R1:~$ sudo sysctl net.ipv4.ip_forward
net.ipv4.ip_forward = 1

hp@R2:~$ sudo sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
hp@R2:~$ sudo sysctl net.ipv4.ip_forward
net.ipv4.ip_forward = 1

hp@R3:~$ sudo sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
hp@R3:~$ sudo sysctl net.ipv4.ip_forward
net.ipv4.ip_forward = 1

```

## 8. Kiểm tra kết nối mạng từ máy PCA đến R3:

```

hp@pc01:~$ ping 192.168.3.1
PING 192.168.3.1 (192.168.3.1) 56(84) bytes of data.
From 192.168.1.1 icmp_seq=1 Redirect Host(New nexthop: 2.1.168.192)
64 bytes from 192.168.3.1: icmp_seq=1 ttl=63 time=4.08 ms
64 bytes from 192.168.3.1: icmp_seq=2 ttl=63 time=4.36 ms
64 bytes from 192.168.3.1: icmp_seq=3 ttl=63 time=3.65 ms

hp@pc01:~$ tracepath -n 192.168.3.1
 1?: [LOCALHOST] pmtu 1500
 1: 192.168.1.2 2.046ms
 1: 192.168.1.2 2.651ms
 2: 192.168.3.1 3.988ms reached
Resume: pmtu 1500 hops 2 back 2

```

## 4.2 Tạo thêm máy trạm X kết nối vào LAN3

1. Clone X từ máy A.
2. Thiết lập địa chỉ IP của X và default gateway là R3:

```

hp@pcX:~$ sudo nano /etc/netplan/00-installer-config.yaml
network:
  ethernets:
    enp0s3:
      dhcp4: false
      addresses:
        - 192.168.3.21/24
      routes:
        - to: default
          via: 192.168.3.1
hp@pcX:~$ sudo netplan apply
hp@pcX:~$ ifconfig enp0s3
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.3.21 netmask 255.255.255.0 broadcast 192.168.3.255
inet6 fe80::a00:27ff:fe88:f01 prefixlen 64 scopeid 0x20<link>

```

```

ether 08:00:27:88:0f:01 txqueuelen 1000 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 24 bytes 1896 (1.8 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

hp@pcX:~$ route -n
Kernel IP routing table
Destination      Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0          192.168.3.1    0.0.0.0         UG    0      0      0 enp0s3
192.168.3.0      0.0.0.0        255.255.255.0   U     0      0      0 enp0s3

```

### 3. Kiểm tra kết nối từ X đến A:

```

hp@pcX:~$ ping 192.168.1.20
PING 192.168.1.20 (192.168.1.20) 56(84) bytes of data.
64 bytes from 192.168.1.20: icmp_seq=1 ttl=61 time=10.6 ms
64 bytes from 192.168.1.20: icmp_seq=2 ttl=62 time=3.75 ms
64 bytes from 192.168.1.20: icmp_seq=3 ttl=62 time=3.79 ms
^C
--- 192.168.1.20 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2008ms
rtt min/avg/max/mdev = 3.748/6.056/10.629/3.233 ms
hp@pcX:~$ tracepath -n 192.168.1.20
  1?: [LOCALHOST] pmtu 1500
  1:  192.168.3.1 1.207ms
  1:  192.168.3.1 0.651ms
  2:  192.168.2.1 3.716ms
  3:  192.168.1.20 4.309ms reached
Resume: pmtu 1500 hops 3 back 3

```

### 4. Kiểm tra kết nối từ X ra Internet, thấy đang có lỗi. Hãy tìm cách xử lý:

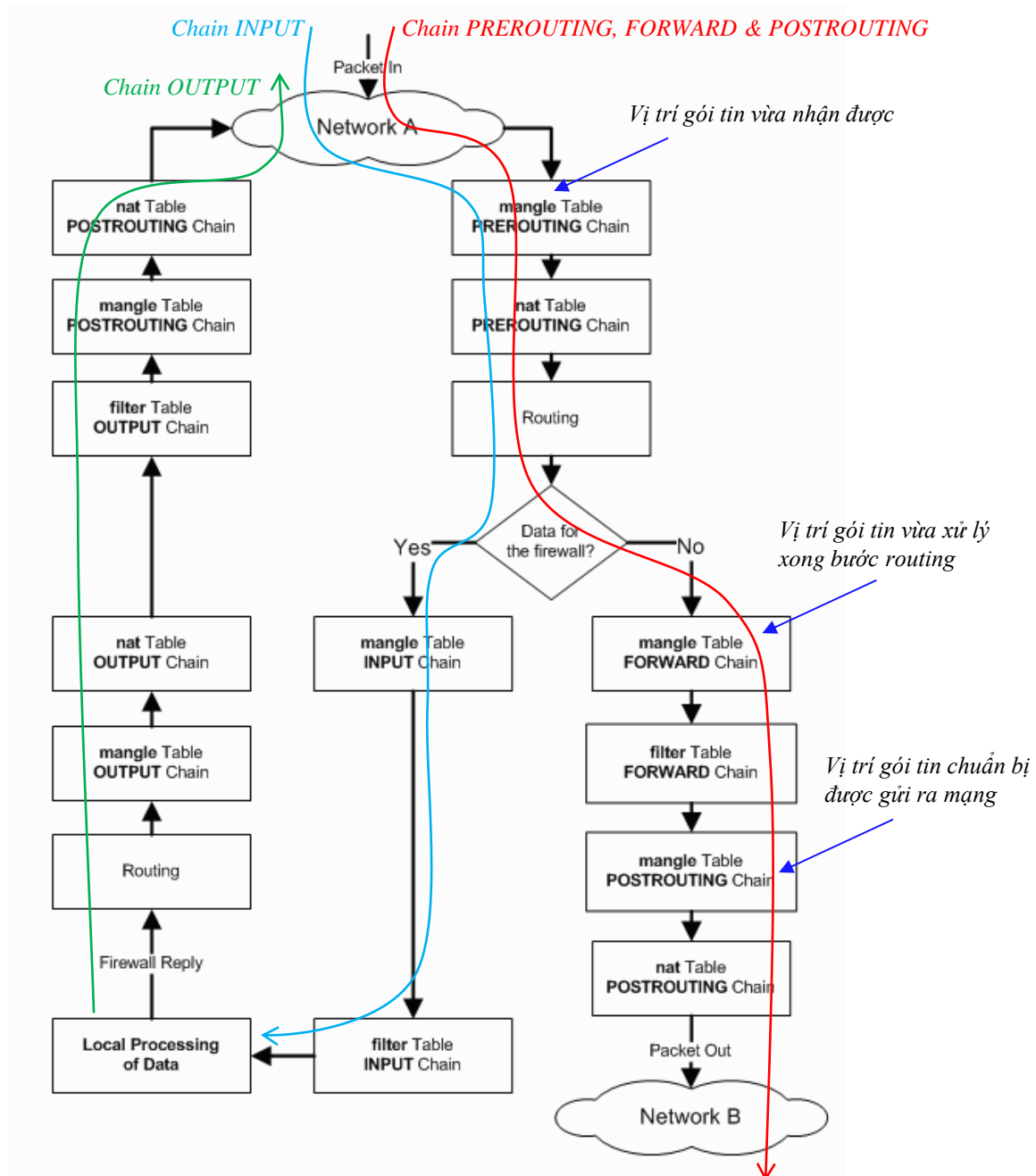
```

hp@pcX:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
From 192.168.3.1 icmp_seq=1 Destination Net Unreachable
From 192.168.3.1 icmp_seq=2 Destination Net Unreachable
From 192.168.3.1 icmp_seq=3 Destination Net Unreachable

```

## 5 Phân tích giao thức với các công cụ hỗ trợ

Có thể sử dụng *iptables* để tương tác với các gói tin khi đi qua vùng lỗi (Linux kernel). Ví dụ luật NAT xử lý gói tin IP tại điểm POSTROUTING, thay địa chỉ IP source bằng địa chỉ IP mặt ngoài của gateway. Ngoài ra, *tcpdump* cho phép bắt gói tin tại từng kết nối mạng.



## 5.1 Xem gói tin tại các kết nối mạng

1. Chạy lệnh `ping` kiểm tra kết nối giữa máy A và máy X:

```
hp@pcA:~$ ping 192.168.3.21
PING 192.168.3.21 (192.168.3.21) 56(84) bytes of data.
64 bytes from 192.168.3.21: icmp_seq=1 ttl=62 time=5.45 ms
64 bytes from 192.168.3.21: icmp_seq=2 ttl=62 time=4.23 ms
64 bytes from 192.168.3.21: icmp_seq=3 ttl=62 time=3.80 ms
```

2. Kiểm tra các gói tin đi qua R2, sẽ thấy gói ICMP Echo Request và Echo Reply gửi giữa máy A và máy X:

```
hp@R2:~$ sudo tcpdump -i enp0s3 -nv
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
03:29:17.139062 IP (tos 0x0, ttl 64, id 5756, offset 0, flags [DF], proto ICMP (1), length 84)
  192.168.1.20 > 192.168.3.21: ICMP echo request, id 12, seq 1, length 64
03:29:17.142632 IP (tos 0x0, ttl 62, id 43573, offset 0, flags [none], proto ICMP (1), length 84)
  192.168.3.21 > 192.168.1.20: ICMP echo reply, id 12, seq 1, length 64
03:29:18.142752 IP (tos 0x0, ttl 64, id 5944, offset 0, flags [DF], proto ICMP (1), length 84)
  192.168.1.20 > 192.168.3.21: ICMP echo request, id 12, seq 2, length 64
03:29:18.145472 IP (tos 0x0, ttl 62, id 43743, offset 0, flags [none], proto ICMP (1), length 84)
  192.168.3.21 > 192.168.1.20: ICMP echo reply, id 12, seq 2, length 64
03:29:19.144193 IP (tos 0x0, ttl 64, id 6170, offset 0, flags [DF], proto ICMP (1), length 84)
  192.168.1.20 > 192.168.3.21: ICMP echo request, id 12, seq 3, length 64
03:29:19.146745 IP (tos 0x0, ttl 62, id 43937, offset 0, flags [none], proto ICMP (1), length 84)
```

```

192.168.3.21 > 192.168.1.20: ICMP echo reply, id 12, seq 3, length 64
03:29:20.144434 IP (tos 0x0, ttl 64, id 6205, offset 0, flags [DF], proto ICMP (1), length 84)
192.168.1.20 > 192.168.3.21: ICMP echo request, id 12, seq 4, length 64
03:29:20.147442 IP (tos 0x0, ttl 62, id 43958, offset 0, flags [none], proto ICMP (1), length 84)
192.168.3.21 > 192.168.1.20: ICMP echo reply, id 12, seq 4, length 64

```

## 5.2 Phân tích các gói tin ICMP của lệnh `tracpath`

### 1. Tại máy X, thực hiện `tracpath` đến máy Google:

```

hp@pcX:~$ tracpath -n 8.8.8.8
1?: [LOCALHOST] pmtu 1500
1: 192.168.3.1 1.984ms
1: 192.168.3.1 2.236ms
2: 192.168.2.1 4.209ms
3: 192.168.1.1 6.276ms
4: 10.0.2.2 7.115ms

```

### 2. Xem các gói tin tại các kết nối mạng của R3 bằng `tcpdump`, chú ý trường TTL của các gói tin và *ICMP time exceeded*:

```

hp@R3:~$ sudo tcpdump -i enp0s3 -nv
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
03:44:13.017873 IP (tos 0x0, ttl 1, id 0, offset 0, flags [DF], proto UDP (17), length 1500)
192.168.3.21.51003 > 8.8.8.8.44446: UDP, length 1472
03:44:13.020605 IP (tos 0xc0, ttl 64, id 14076, offset 0, flags [none], proto ICMP (1), length 576)
192.168.2.1 > 192.168.3.21: ICMP time exceeded in-transit, length 556
IP (tos 0x0, ttl 1, id 0, offset 0, flags [DF], proto UDP (17), length 1500)
192.168.3.21.51003 > 8.8.8.8.44446: UDP, length 1472
03:44:13.022224 IP (tos 0x0, ttl 2, id 0, offset 0, flags [DF], proto UDP (17), length 1500)
192.168.3.21.51003 > 8.8.8.8.44447: UDP, length 1472
03:44:13.027239 IP (tos 0xc0, ttl 63, id 13507, offset 0, flags [none], proto ICMP (1), length 576)
192.168.1.1 > 192.168.3.21: ICMP time exceeded in-transit, length 556
IP (tos 0x0, ttl 1, id 0, offset 0, flags [DF], proto UDP (17), length 1500)
192.168.3.21.51003 > 8.8.8.8.44447: UDP, length 1472
03:44:13.030027 IP (tos 0x0, ttl 3, id 0, offset 0, flags [DF], proto UDP (17), length 1500)
192.168.3.21.51003 > 8.8.8.8.44448: UDP, length 1472
03:44:13.033999 IP (tos 0xc0, ttl 253, id 385, offset 0, flags [none], proto ICMP (1), length 56)
10.0.2.2 > 192.168.3.21: ICMP time exceeded in-transit, length 36
IP (tos 0x0, ttl 1, id 0, offset 0, flags [DF], proto UDP (17), length 1500)
192.168.3.21.51003 > 8.8.8.8.44448: UDP, length 1472
03:44:13.035542 IP (tos 0x0, ttl 4, id 0, offset 0, flags [DF], proto UDP (17), length 1500)
192.168.3.21.51003 > 8.8.8.8.44449: UDP, length 1472
03:44:14.039350 IP (tos 0x0, ttl 4, id 0, offset 0, flags [DF], proto UDP (17), length 1500)
192.168.3.21.51003 > 8.8.8.8.44450: UDP, length 1472

```

## 5.3 Theo dõi gói tin được xử lý NAT

### 1. `ping` từ máy X ra Internet:

```

hp@pcX:~$ 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=52 time=59.5 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=52 time=35.7 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=52 time=43.9 ms

```

### 2. Kiểm tra các gói tin đi qua R2, sẽ thấy gói ICMP Echo Request và Echo Reply gửi giữa máy X và máy 8.8.8.8:

```

hp@R2:~$ sudo tcpdump -i enp0s3 -nv
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
03:49:24.666191 IP (tos 0x0, ttl 62, id 1889, offset 0, flags [DF], proto ICMP (1), length 84)
192.168.3.21 > 8.8.8.8: ICMP echo request, id 19, seq 1, length 64
03:49:24.701565 IP (tos 0x22, ECT(0), ttl 54, id 389, offset 0, flags [none], proto ICMP (1), length 84)
8.8.8.8 > 192.168.3.21: ICMP echo reply, id 19, seq 1, length 64
03:49:25.668144 IP (tos 0x0, ttl 62, id 1940, offset 0, flags [DF], proto ICMP (1), length 84)
192.168.3.21 > 8.8.8.8: ICMP echo request, id 19, seq 2, length 64
03:49:25.710445 IP (tos 0x22, ECT(0), ttl 54, id 390, offset 0, flags [none], proto ICMP (1), length 84)
8.8.8.8 > 192.168.3.21: ICMP echo reply, id 19, seq 2, length 64

```

3. Kiểm tra các gói tin đi qua R1 ở kết nối NAT, sẽ thấy gói ICMP Echo Request và Echo Reply gửi với máy 8.8.8.8 nhưng địa chỉ IP nguồn được thay bằng địa chỉ mặt ngoài của R1:

```
hp@R1:~$ sudo tcpdump -i enp0s3 -nv
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
03:51:38.055258 IP (tos 0x0, ttl 61, id 19881, offset 0, flags [DF], proto ICMP (1), length 84)
    10.0.2.15 > 8.8.8.8: ICMP echo request, id 19, seq 148, length 64
03:51:38.082437 IP (tos 0x22,ECT(0), ttl 55, id 540, offset 0, flags [none], proto ICMP (1),
length 84)
    8.8.8.8 > 10.0.2.15: ICMP echo reply, id 19, seq 148, length 64
03:51:39.055728 IP (tos 0x0, ttl 61, id 19997, offset 0, flags [DF], proto ICMP (1), length 84)
    10.0.2.15 > 8.8.8.8: ICMP echo request, id 19, seq 149, length 64
03:51:39.083081 IP (tos 0x22,ECT(0), ttl 55, id 541, offset 0, flags [none], proto ICMP (1),
length 84)
    8.8.8.8 > 10.0.2.15: ICMP echo reply, id 19, seq 149, length 64
```

4. Tắt luật NAT trên router R1, sẽ không *ping* được từ máy X ra 8.8.8.8 nữa

```
hp@R1:~$ sudo iptables -L -t nat --line-number
Chain PREROUTING (policy ACCEPT)
num target      prot opt source                destination

Chain INPUT (policy ACCEPT)
num target      prot opt source                destination

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

Chain POSTROUTING (policy ACCEPT)
num target      prot opt source                destination
1 MASQUERADE all -- anywhere              anywhere
hp@R1:~$ sudo iptables -t nat -D POSTROUTING 1
hp@R1:~$ sudo iptables -L --line-number
Chain INPUT (policy ACCEPT)
num target      prot opt source                destination

Chain FORWARD (policy ACCEPT)
num target      prot opt source                destination

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

## 5.4 Tạo các kịch bản ping destination unreachable và time out

1. Ping từ A đến X:  
*A> ping 192.168.3.20*  
....  
....
2. Router R2 hoặc R3 nếu thiếu luật routing sẽ tạo ra gói tin ICMP thông báo cho A, lúc đó *ping* sẽ hiển thị kết quả “*destination unreachable*”:  
*R2> route -n*  
....  
....  
*R2> route del -net 192.168.3.0/24 gw 192.168.2.2*
3. Nếu router chuyển được gói tin ICMP của ping đến X nhưng gói tin trả về lại không đến được A thì lệnh *ping* sẽ hiển thị kết quả “*time out*”  
*R3> route -n*  
....  
....  
*R3> route del -net 192.168.1.0/24 gw 192.168.2.1*