

Thiết kế & triển khai mạng IP

Bài thực hành số 1: Kết nối liên mạng

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.....	3
3.1	Cấu hình máy ảo R1 thành NAT router của mạng LAN01	3
3.2	Tạo máy trạm A, B.....	3
3.3	Sử dụng netplan để cấu hình sẵn thông số mạng	4
4	Tạo các mạng LAN kết nối Internet qua router R1, R2, R3	4
4.1	Tạo thêm các mạng LAN và router R2, R3	4
4.2	Tạo thêm máy trạm X kết nối vào LAN3	5
5	Phân tích giao thức với công cụ <i>iptables</i>	6
5.1	Bật log để xem các gói tin đi qua router R1, R2, R3	6
5.2	Phân tích các gói tin ICMP của lệnh <i>tracpath</i>	7
5.3	Tạo các kịch bản ping destination unreachable và time out	7

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: Name = R1
2. Thiết lập cấu hình CPU & memory phù hợp với máy host
3. Thiết lập kết nối mạng: Adapter 1, Enable, Attached to: NAT
4. Thiết lập bộ nhớ ngoài: Storage, CDROM = file ISO ubuntu server 18.04
5. Khởi động máy ảo
6. Chọn menu "Install or upgrade an existing system"
7. Cài đặt hệ điều hành Ubuntu Server vào máy ảo với các thông số mặc định
8. Reboot R1, login root
9. Kiểm tra cấu hình mạng:

```
R1:~$ ifconfig -a
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet6 fe80::a00:27ff:fe87:c4c prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:87:0c:4c txqueuelen 1000 (Ethernet)
    RX packets 1016 bytes 965159 (965.1 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 414 bytes 46358 (46.3 KB)
    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 116 bytes 9456 (9.4 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 116 bytes 9456 (9.4 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

10. Kiểm tra các thông số kết nối mạng *enp0s3*, so sánh địa chỉ MAC của *enp0s3* với địa chỉ MAC của Adapter 1 trong Virtualbox
11. 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:fe87:c4c prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:87:0c:4c txqueuelen 1000 (Ethernet)
    RX packets 1023 bytes 966839 (966.8 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 421 bytes 47422 (47.4 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

12. 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
```

13. 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.
```

14. 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. Shutdown R1
2. Thêm kết nối mạng: Adapter 2, Enable, Attached to: Internal Network, Name: LAN01
3. Khởi động R1 & login root
4. Kiểm tra các kết nối mạng *enp0s3* và *enp0s8* tương ứng với các Adapter 1 & Adapter 2
5. Thiết lập cấu hình địa chỉ IP cho *enp0s8*:
> *ifconfig enp0s8 192.168.1.1/24*
6. Bật chế độ IP forward (routing mode):
> *sysctl -w net.ipv4.ip_forward=1*
7. Kiểm tra các luật iptables (nếu muốn xem luật của bảng nào thì cần thêm tham số -t):
> *iptables -L -n*
8. Thiết lập NAT routing (luật MASQUERADE) cho R1:
> *iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE*
(lưu ý tham số -o *enp0s3*: chọn đúng kết nối mạng *enp0s3* là output – kết nối ra phía mạng bên ngoài)
9. Kiểm tra luật NAT:
> *iptables -t nat -L -v*

3.2 Tạo máy trạm A, B

1. Tạo máy ảo & cài đặt hệ điều hành Ubuntu Server như với máy ảo R, hoặc dùng chức năng “clone” từ R để tạo A, B (nhanh hơn). Chú ý nếu dùng clone thì cần thay đổi địa chỉ MAC của các Network Adapter.
2. Thiết lập kết nối mạng: Adapter 1, Attached to: Internal Network, Name: LAN01
3. Khởi động máy A, B & login root
4. Kiểm tra kết nối mạng *enp0s3* tương ứng với các Adapter 1
5. Thiết lập cấu hình địa chỉ IP cho *eth1*:
> *ifconfig eth1 192.168.1.21/24*

6. Thiết lập default gateway:
> `route add default gw 192.168.1.1`
7. Kiểm tra kết nối ra Internet:
> `ping 8.8.8.8`
8. Kiểm tra các bước routing:
> `tracert 8.8.8.8`

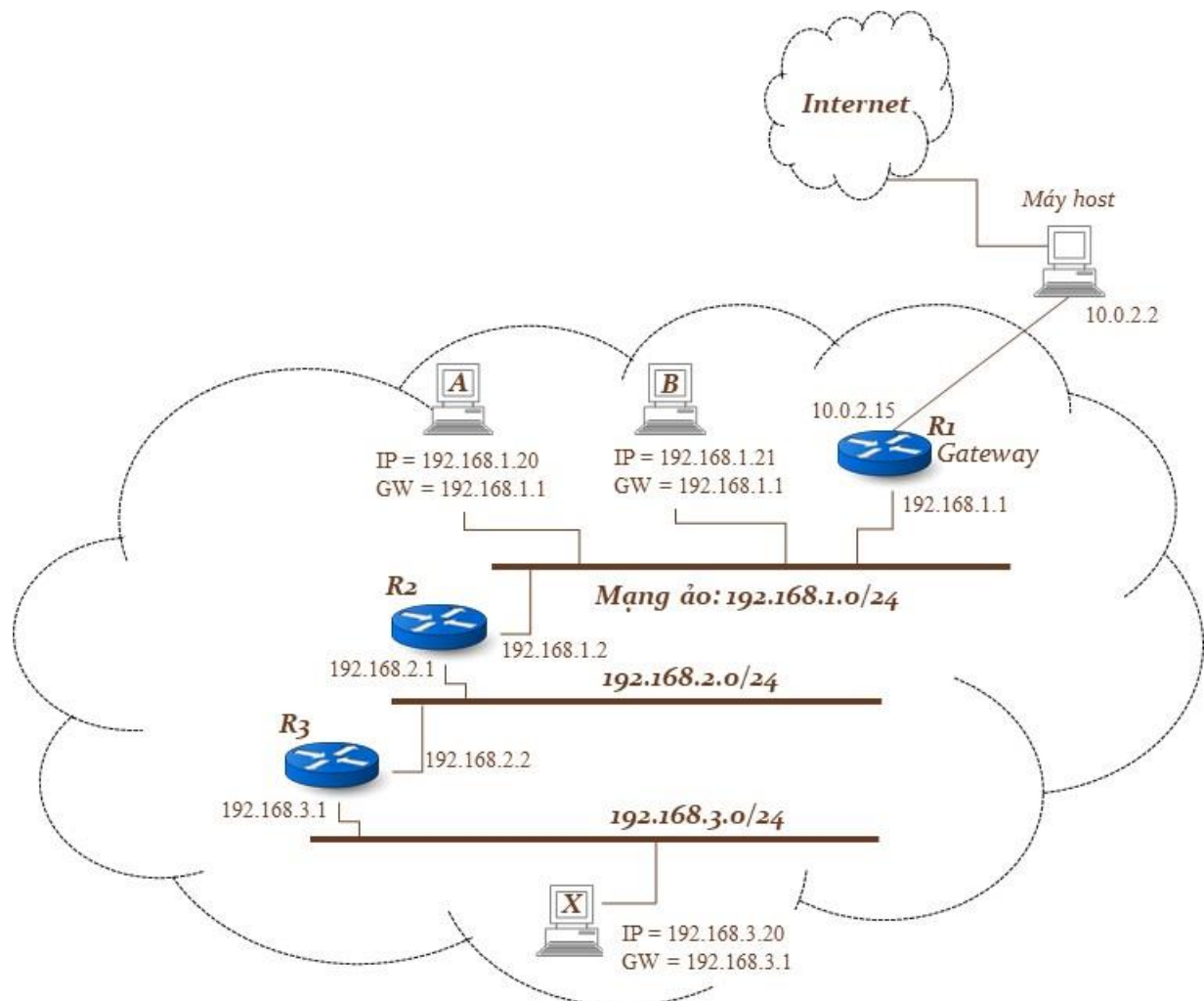
3.3 Sử dụng netplan để cấu hình sẵn thông số mạng

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 host. Netplan cung cấp phương pháp lưu lại các cấu hình này và tự động thiết lập lại khi khởi động hệ thống.

Tham khảo cách sử dụng 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.
2. Mỗi router R2, R3, thiết lập 2 kết nối mạng kiểu Internal Network
3. Kết nối các Network Adapter vào các mạng tương ứng (LAN01, LAN02, LAN03)
4. Cấu hình các bảng routing trên R1, R2, R3 để đi đến các mạng LAN1, LAN2, LAN3

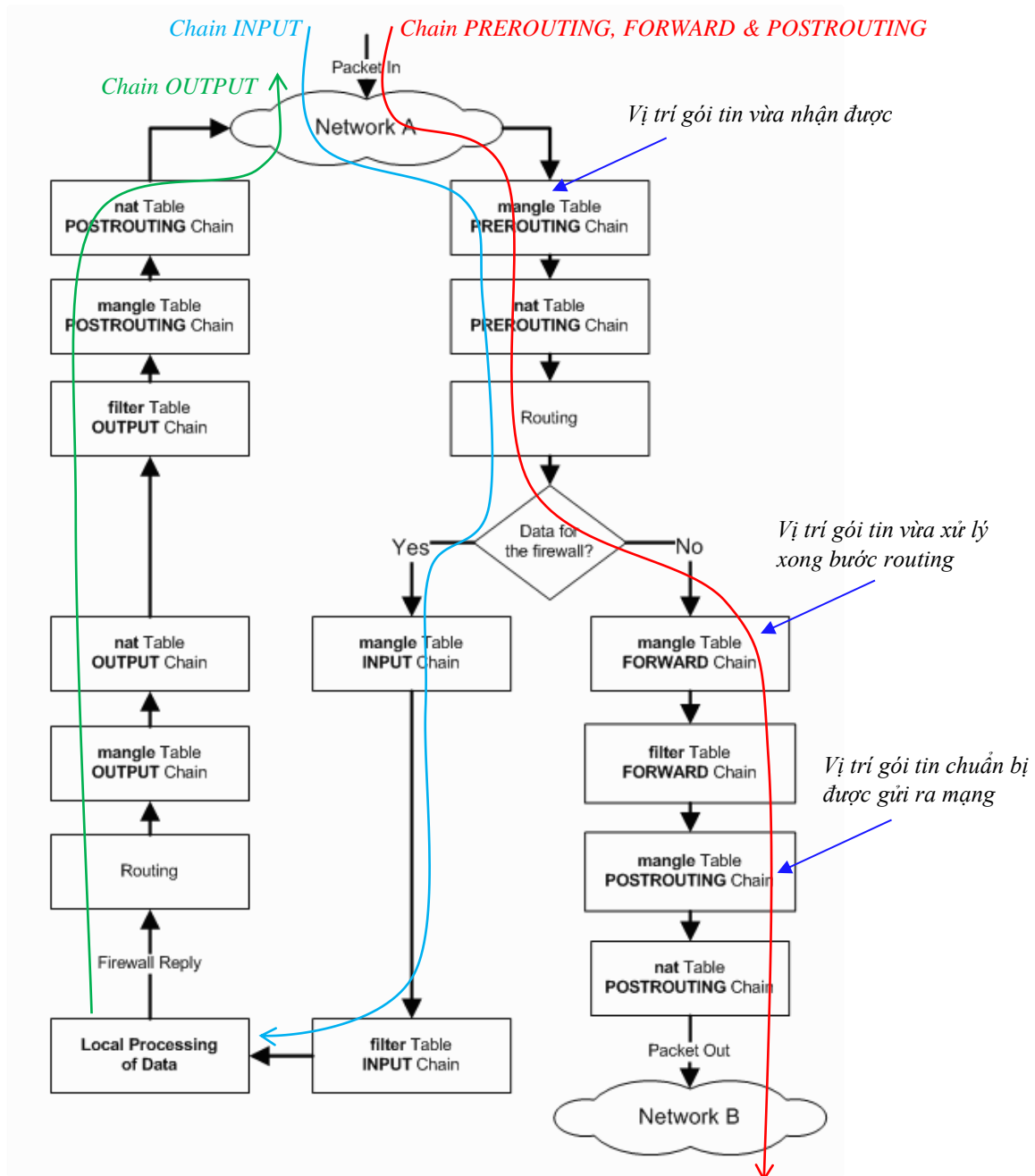
R1:

- *route add -net 192.168.2.0/24 gw 192.168.1.2*
 - *route add -net 192.168.3.0/24 gw 192.168.1.2*
- R2:
- *route add -net 192.168.3.0/24 gw 192.168.2.2*
- R3:
- *route add -net 192.168.1.0/24 gw 192.168.2.1*
5. Cấu hình default route trên R1 (đã có), R2, R3 để đi ra Internet
- R2:
- *route add default gw 192.168.1.1*
- R3:
- *route add default gw 192.168.2.1*
6. Bỏ cấu hình NAT routing trên R2, R3 (chỉ R1 cần NAT do phải nối Internet)
- Liệt kê tất cả các rule trong *iptables* với thông số cấu hình chi tiết
- > *iptables -S*
- Liệt kê theo các *chain*
- > *iptables -L*
- Liệt kê theo một bảng (nat)
- > *iptables -L -t nat*
- Liệt kê thêm số thứ tự
- > *iptables -L -t nat --line-numbers*
- Xóa rule theo số thứ tự trong *chain*
- > *iptables -D INPUT 3*
- Tham khảo: <https://www.digitalocean.com/community/tutorials/how-to-list-and-delete-iptables-firewall-rules>
7. Kiểm tra kết nối Internet từ R2, R3:
- > *ping 8.8.8.8*

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
- > *ifconfig ... 192.168.3.20/24*
3. Thiết lập default Gateway của X là R3
- > *route add default gw 192.168.3.1*
4. Kiểm tra kết nối từ X đến A, B và X ra Internet
- > *ping 192.168.3.1*
- > *ping 192.168.1.1*
- > *ping 8.8.8.8*

5 Phân tích giao thức với công cụ *iptables*



5.1 Bật log để xem các gói tin đi qua router R1, R2, R3

1. Bật công cụ iptables trên R1, R2 & R3:
> `service iptables start`
> `service iptables status`
2. Kiểm tra các luật hiện tại trong router:
> `iptables -L -line-number`
3. Bật luật log gói tin ngay sau bước routing. Các gói tin sẽ được log vào file log hệ thống (thông thường là `/var/log/syslog`):
> `iptables -t mangle -A FORWARD -j LOG`
4. Xem log các gói tin đi qua router:
> `tail -f /var/log/syslog`

5. Xem log & lọc hiển thị riêng gói tin ICMP:
`> tail -f /var/log/syslog | grep ICMP`

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

1. Tại máy A, thực hiện `tracpath` đến máy X:
`A> tracpath 192.168.3.20`
....
....
2. Xem log & lọc hiển thị riêng gói tin ICMP trên R2 & R3:
`> tail -f /var/log/syslog | grep ICMP`
 - Chú ý trường TTL của gói tin gửi đi từ A (bắt được tại R2 & R3) có giá trị tăng dần.
 - Chú ý gói tin ICMP trả về A từ các router R2 & R3

5.3 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`