Thiết kế & triển khai mạng IP

Bài thực hành số 1: Kết nối liên mạng

1 Chuẩn bị môi trường

Hướng dẫn chi tiết: https://users.soict.hust.edu.vn/hoangph/textbook/apdxA01-1.html

1. Download & cài đặt Virtualbox
2. Download ISO image hệ điều hành CentOS 6.8 minimal
   https://users.soict.hust.edu.vn/hoangph/files/CentOS-6.8-x86_64-minimal.iso

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 CentOS 6.8 minimal
5. Khởi động máy ảo
6. Chọn menu "Install or upgrade an existing system"
7. Cài đặt hệ điều hành CentOS vào máy ảo với các thông số mặc định
8. Reboot R1, login root
9. Kiểm tra cấu hình mạng:
   > *ifconfig -a*
10. Kiểm tra các thông số kết nối mạng eth0, so sánh địa chỉ MAC của eth0 với địa chỉ MAC của Adapter 1 trong Virtualbox
11. Kiểm tra địa chỉ IP của eth0
12. Gán địa chỉ IP động:
    > *dhclient -s eth0*
13. Kiểm tra kết nối R1 ra Internet:
    > *ping 8.8.8.8*
14. Cài đặt trình soạn thảo nano để làm việc với các file cấu hình:
    > *yum install nano*
15. Tìm hiểu cách lưu cấu hình vào các file config để khởi động máy không cần cấu hình lại

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:

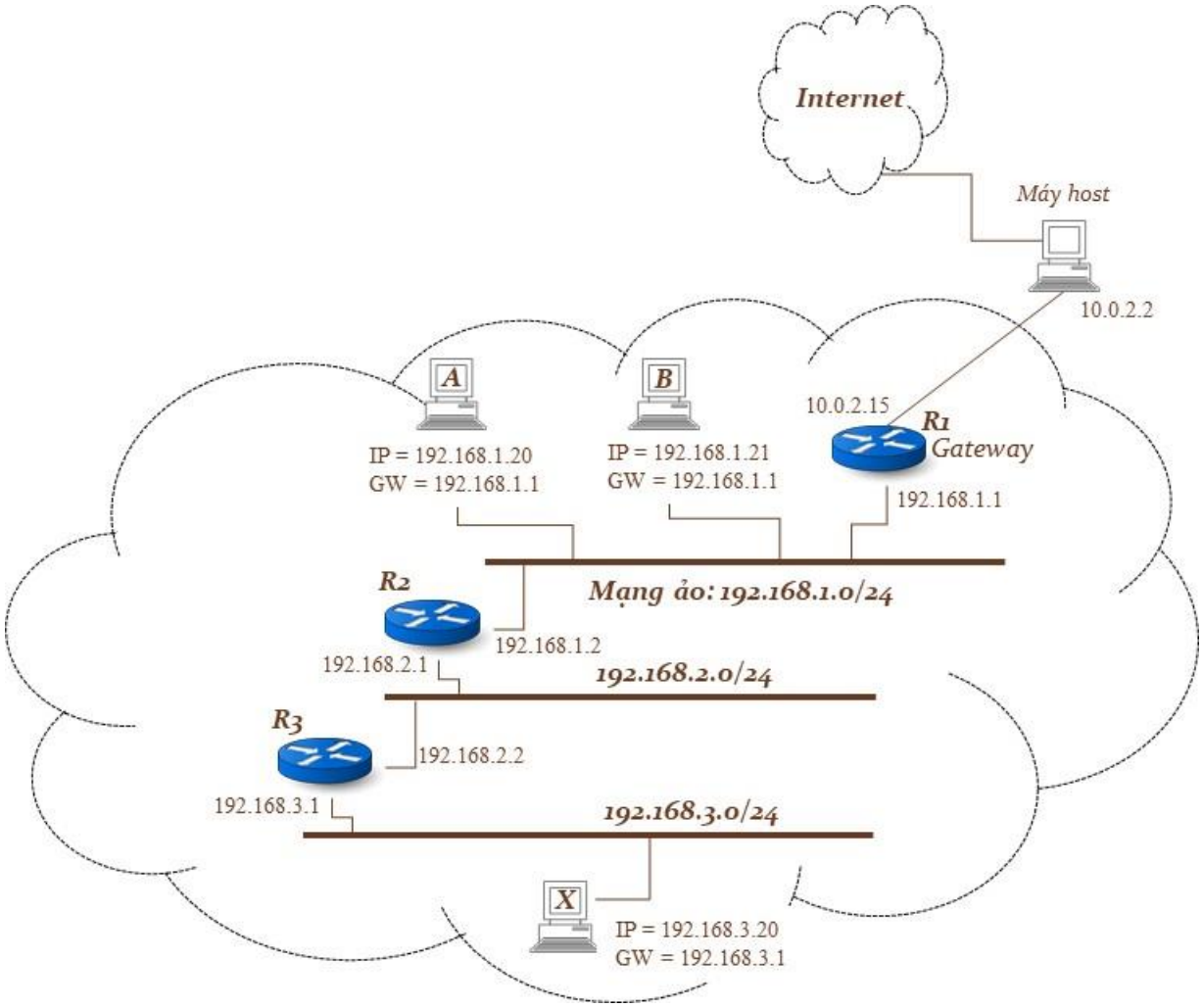
1. Shutdown R1
2. Thêm kết nối mạng: Adapter 2, Enable, Attached to: Internal Network, Name: LAN01
3. Khởi động R1 & login root
4. Kiểm tra các kết nối mạng eth0 và eth1 tương ứng với các Adapter 1 & Adapter 2
5. Thiết lập cấu hình địa chỉ IP cho eth1:
   > *ifconfig eth1 192.168.1.1/24*
6. Bật chế độ IP forward (routing mode):
   > *sysctl -w net.ipv4.ip_forward=1*
7. Tắt luật tường lửa mặc định (iptables):
   > *iptables -D FORWARD -j REJECT --reject-with icmp-host-prohibited*
8. Kiểm tra luật tường lửa:
   > *iptables -L -n*
9. Thiếp lập NAT routing cho R1:
   > *iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE*
   (lưu ý tham số *-o eth0:* chọn đúng kết nối mạng *eth0* là output – kết nối ra phía mạng bên ngoài)
10. 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 CentOS 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 eth0 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:
   > *tracepath 8.8.8.8*

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 defalt 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. Xóa luật cấm ICMP khi routing (nếu có):
   > iptables -D FORWARD <#số thứ tự của luật>
4. Bật luật log gói tin ngay sau bước routing:
   > iptables -t mangle -A FORWARD -j LOG
5. Xem log các gói tin đi qua router:
   > tail -f /var/log/message
6. Xem log & lọc hiển thị riêng gói tin ICMP:
   > tail -f /var/log/message | grep ICMP

5.2 Phân tích các gói tin ICMP của lệnh tracepath

1. Tại máy A, thực hiện *tracepath* đến máy X:
   A> tracepath 192.168.3.20
   . . . .
   . . . .
2. Xem log & lọc hiển thị riêng gói tin ICMP trên R2 & R3:
   > tail -f /var/log/message | 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 ~~den~~ 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 den -net 192.168.1.0/24 gw 192.168.2.1