



## 2. Định tuyến động và Access Control List

THỰC HÀNH QUẢN TRỊ MẠNG VÀ HỆ THỐNG – v3.2024

**PHỤC VỤ MỤC ĐÍCH GIÁO DỤC**  
FOR EDUCATIONAL PURPOSE ONLY

### A. GIỚI THIỆU TỔNG QUAN

#### 1. Mục tiêu

Mục tiêu của bài thực hành này là hiểu được cơ chế trao đổi thông tin định tuyến giữa các router. Thực hiện các thao tác cấu hình, quan sát và giải quyết các vấn đề định tuyến động sử dụng giao thức RIP (Routing Information Protocol) và OSPF (Open Shortest Path First).

Ngoài ra, sẽ tìm hiểu cách thức để giới hạn truy cập từ / đến các tài nguyên và đối tượng sử dụng danh sách điều khiển truy cập (ACL – Access Control List).

#### 2. Môi trường và thiết bị thực hành

Thực hành trên thiết bị mạng vật lý và trên công cụ mô phỏng Cisco Packet Tracer.

## B. NỘI DUNG THỰC HÀNH

### 1. Lý thuyết về định tuyến động

Sinh viên trả lời các câu hỏi sau trước khi thực hiện phần thực hành

1. Sự khác nhau giữa Classful và Classless.
2. Ý nghĩa của câu lệnh `no auto-summary` khi cấu hình RIP. Có bắt buộc phải sử dụng câu lệnh này hay không? Chuyện gì sẽ xảy ra khi cấu hình RIPv2 mà không sử dụng lệnh này?
3. Các ký hiệu C, L và R (thể hiện trong Hình 1) có ý nghĩa gì?
4. Đề xuất một danh sách ACL để chặn tất cả các host trong lớp mạng 192.168.10.0/24 truy cập Internet khi sử dụng giao thức HTTP/HTTPS.

```
R1# show ip route | begin Gateway
Gateway of last resort is not set

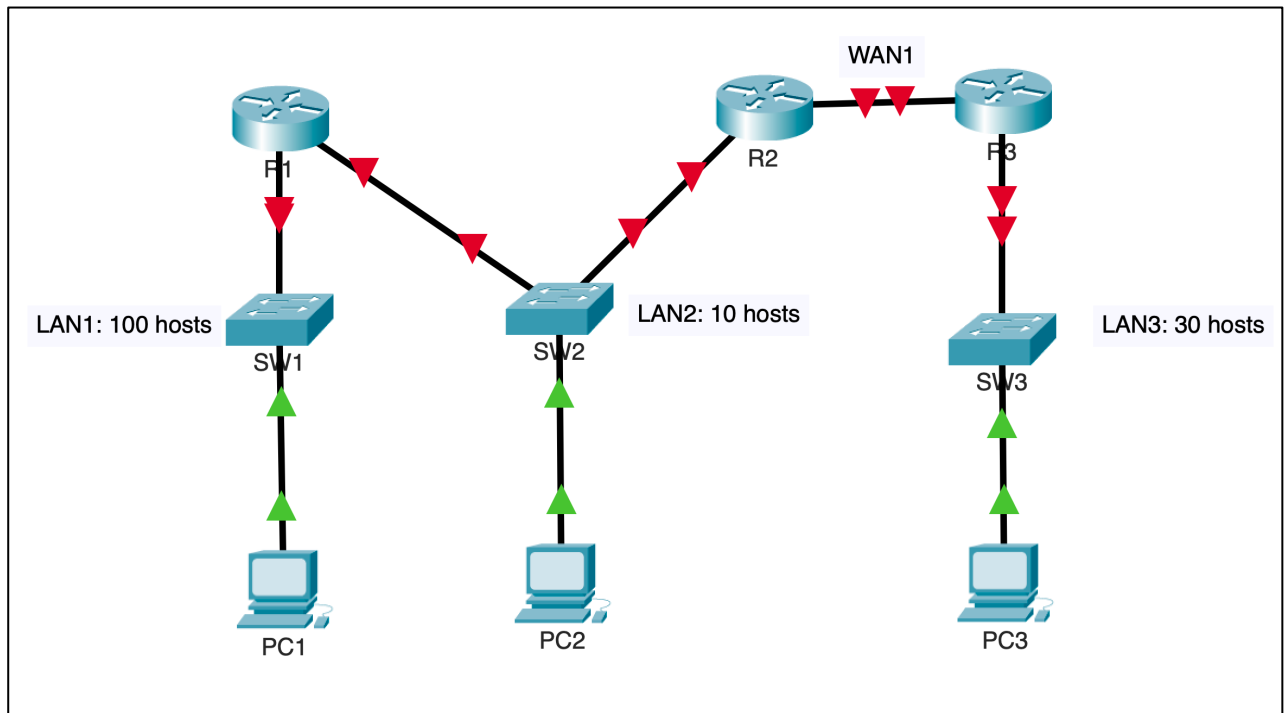
    192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
    192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/24 is directly connected, Serial0/0/0
L       192.168.2.1/32 is directly connected, Serial0/0/0
R       192.168.3.0/24 [120/1] via 192.168.2.2, 00:00:24, Serial0/0/0
R       192.168.4.0/24 [120/1] via 192.168.2.2, 00:00:24, Serial0/0/0
R       192.168.5.0/24 [120/2] via 192.168.2.2, 00:00:24, Serial0/0/0
R1#
```

Hình 1: Ví dụ bảng thông tin định tuyến

### 2. Định tuyến động và ACL đơn giản

*Lưu ý: Nội dung phần này được thiết kế để thực hiện trên thiết bị thật*

Trong yêu cầu này, sinh viên sẽ tìm hiểu và thực hiện cấu hình một mô hình mạng nhỏ sử dụng giao thức định tuyến động và áp dụng danh sách kiểm soát truy cập (Access Control List – ACL).



Hình 2: Mô hình mạng được sử dụng cho yêu cầu 2

Nhóm được cấp lớp mạng **192.168.10.0/24** (với X là số thứ tự nhóm)

### Yêu cầu thực hiện

1. Quy hoạch IP để cấp cho các vùng mạng tương ứng trong mô hình. Sau đó điền thông tin mạng con theo mẫu Bảng 1 (khuyến khích sử dụng phương pháp VLSM để chia mạng con)
2. Đặt hostname cho tất cả các thiết bị tương ứng trong mô hình.
3. Đặt Banner Motd "**Warning: Authorized Access Only on Rx**" (với Rx là tên của Router) trên tất cả router.
4. Đặt địa chỉ IP và subnet mask trên tất cả các cổng tương ứng thiết bị. Điền thông tin theo mẫu Bảng 2 .
5. Cấu hình định tuyến động trên tất cả các Router sử dụng giao thức RIPv2.

*Sinh viên cần đảm bảo tất cả các thiết bị có thể giao tiếp với nhau (có thể sử dụng lệnh ping) trước khi thực hiện các phần bên dưới.*

6. Bật cấu hình từ xa Telnet trên R2.
7. Chặn tất cả các lưu lượng truy cập đến LAN3 từ PC2.
8. Các thiết bị trong VLAN3, chỉ cho phép các thiết bị có địa chỉ IP chẵn (octet cuối cùng trong địa chỉ IP mang giá trị chẵn) truy cập vào LAN1.

9. Chỉ cho phép các thiết bị trong LAN1 có thể sử dụng giao thức Telnet để cấu hình từ xa R2.

*Lưu ý: Thường xuyên sao lưu Running-configuration vào Startup-configuration để tránh tình trạng bị mất thông tin cấu hình khi thiết bị vô tình bị tắt / khởi động lại.*

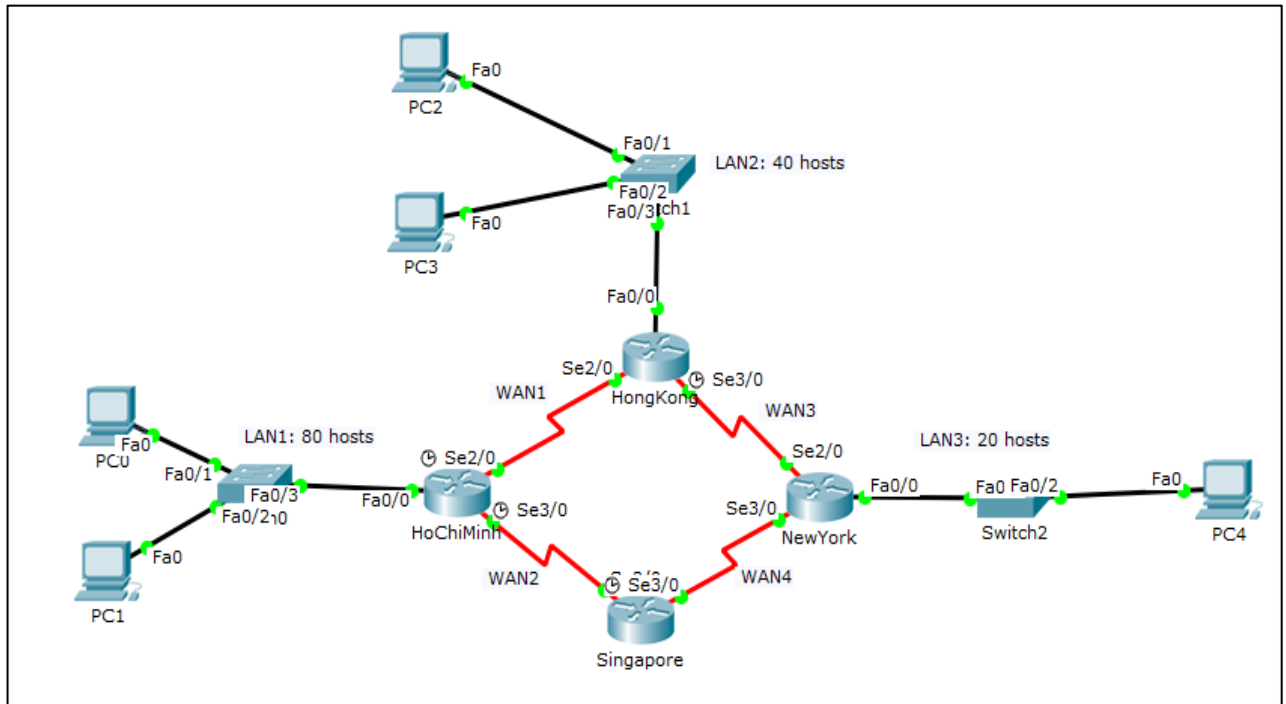
Bảng 1: Thông tin mạng con

| Subnet | Network Address/CIDR | First IP Address | Broadcast Address |
|--------|----------------------|------------------|-------------------|
| LAN1   |                      |                  |                   |
| LAN2   |                      |                  |                   |
| LAN3   |                      |                  |                   |
| WAN1   |                      |                  |                   |

Bảng 2: Thông tin địa chỉ IP cho các thiết bị

| Thiết bị | Interface | IPv4 Address | Subnet Mask | Default Gateway |
|----------|-----------|--------------|-------------|-----------------|
| R1       | G0/0/0    |              |             |                 |
|          | G0/0/1    |              |             |                 |
| R2       | G0/0/0    |              |             |                 |
|          | G0/0/1    |              |             |                 |
| R3       | G0/0/0    |              |             |                 |
|          | G0/0/1    |              |             |                 |
| PC1      | NIC       |              |             |                 |
| PC2      | NIC       |              |             |                 |
| PC3      | NIC       |              |             |                 |

### 3. Định tuyến động OSPF và ACL



Hình 3: Mô hình mạng cho yêu cầu 3

**Yêu cầu thực hiện:** Sử dụng lớp mạng được cấp **172.(16+X%16).0.0/16** (với X là số thứ tự của nhóm)

1. Thực hiện chia mạng con cho các vùng LAN và WAN từ lớp mạng được cấp. Điền thông tin mạng con theo mẫu Bảng 1. Sử dụng phương pháp VLSM.
2. Đặt hostname cho tất cả các thiết bị.
3. Đặt Banner Motd "Warning: Authorized Access Only on Router Rx" (với Rx là tên Router) trên tất cả Router.
4. Đặt địa chỉ IP cho tất cả các cổng của thiết bị. Điền thông tin vào bảng theo mẫu Bảng 2.
5. Cấu hình định tuyến động OSPF đến tất cả Router để tất cả các host trong mạng đều có thể giao tiếp với nhau. Sử dụng ProcessID=1 và Area=0.
6. Cấu hình ACL để không cho phép các thiết bị trong LAN1 truy cập đến LAN3.
7. Máy PC3 chỉ có thể truy cập đến LAN3 khi sử dụng giao thức FTP hoặc SSH.

*Thường xuyên sao lưu Running-configuration vào Startup-configuration để tránh tình trạng bị mất thông tin cấu hình khi thiết bị vô tình bị tắt hoặc khởi động lại.*

## C. YÊU CẦU NỘP BÀI

Sinh viên hoàn thành tất cả các yêu cầu tại phần B (nội dung thực hành). Thực hiện thêm các yêu cầu mở rộng, nâng cao sẽ có thêm điểm cộng. Khuyến khích sinh viên thực hiện bài thực hành theo nhóm 04 thành viên.

Khi nộp bài, sinh viên cần tuân thủ các quy định sau:

- Báo cáo chi tiết về quá trình thực hiện bằng định dạng docx (Word Document), sử dụng mẫu báo cáo được cung cấp tại Website môn học.
- Báo cáo có thể viết bằng ngôn ngữ tiếng Việt hoặc tiếng Anh. Tuy nhiên không trộn lẫn nhiều ngôn ngữ (ngoại trừ các cụm từ, từ khóa không thể dịch được).
- Đối với các **yêu cầu lập trình** (viết ứng dụng hoặc script), cần đính kèm tất cả mã nguồn và file thực thi (nếu có) khi nộp bài. Trong báo cáo cần giải thích chức năng của các khối mã nguồn quan trọng và ảnh chụp demo quá trình hoạt động.

Không sao chép báo cáo. Nếu phát hiện tình trạng sao chép của nhau (hoặc sử dụng báo cáo của sinh viên từ các khóa trước) để nộp bài sẽ không được chấp nhận.

**Lưu ý:** Nén file báo cáo và các file liên quan với định dạng **ZIP (.zip)**, đặt tên theo quy tắt sau:

*LabX-NhomX-MSSV1-MSS2-MSSV3.zip*