TRƯỜNG ĐẠI HỌC SÀI GÒN
KHOA CÔNG NGHỆ THÔNG TIN
BỘ MÔN KỸ THUẬT MÁY TÍNH

TÀI LIỆU
HỆ THỐNG BÀI THỰC HÀNH
MÔN MẠNG MÁY TÍNH

Biên soạn: Thạc sỹ LƯƠNG MINH HUẤN

Năm 2020

MỤC LỤC

LỜI NÓI ĐẦU

Tài liệu thực hành mạng máy tính được biên soạn với mong muốn giúp sinh viên và giảng viên của khoa công nghệ thông tin, trường đại học Sài Gòn, có một tài liệu thống nhất trong việc học thực hành mạng máy tính. Giúp các bạn sinh viên sau khi học ngoài việc nắm bắt các kiến thức lý thuyết về mạng máy tính trong lớp lý thuyết, thì sinh viên còn có thể có các kiến thức thực hành về mạng máy tính như cấu hình các thiết bị mạng: router, switch,… Ngoài ra, sinh viên cũng có thể sử dụng phần mềm wireshark đê bắt và tìm hiểu gói tin trên mạng.

Trong quá trình biên soạn, tác giả có sử dụng các tài liệu tham khảo của chương trình đào tạo CCNA của VNPRO, những hướng dẫn kỹ thuật ở các trang web trên internet, giáo trình môn cấu hình thiết bị mạng Cisco của trường cao đẳng kỹ thuật Cao Thắng, tài liệu thí nghiệm môn học kỹ thuật truyền số liệu của học viện quân sự. Sau đó, căn cứ theo đề cương chương trình của trường đại học Sài Gòn mà biên soạn cho phù hợp.

Trong quá trình biên soạn, dù đã rất cố gắng nhưng chắc sẽ khó tránh được những thiếu sót. Rất mong muốn quý thầy cô và các bạn sinh viên khi sử dụng tài liệu có thể phản hồi để tác giả có thể chỉnh sửa cho tài liệu ngày một tốt hơn và dể hiểu hơn với các bạn sinh viên.

Xin chân thành cảm ơn!

BÀI 1: GIỚI THIỆU ROUTER – CẤU HÌNH ROUTER

I. Hướng dẫn thực hiện

1. Giới thiệu router – phần mềm Cisco Packet Tracer

Router là loại thiết bị dùng để lựa chọn đường đi tốt nhất cho các gói tin hướng ra mạng bên ngoài. Ngoài ra, router còn dùng để ghép nối các mạng cục bộ lại với nhau thành mạng rộng. Router là một thiết bị quan trọng trong hệ thống mạng ngày nay. Router hoạt động ở tầng thứ network trong mô hình OSI.

Trong việc thực hành cấu hình router, người ta sử dụng các phần mềm mô phỏng thiết bị giả lập như Cisco Packet Tracer, Boson netsim, GNS3,… Trong phần tài liệu thực hành này sẽ sử dụng phần mềm Cisco Packet Tracer để mô phỏng các thiết bị cấu hình trong hệ thống mạng máy tính.

Packet Tracer là một phần mềm giả lập mạng dùng trong học tập sử dụng các thiết bị mạng (router/switch) của Cisco. Phần mềm được hãng Cisco cung cấp miễn phí cho các trường lớp, sinh viên đang giảng dạy và theo học chương trình mạng của Cisco. Sản phẩm cung cấp một công cụ để nghiên cứu các nguyên tắc cơ bản của mạng và các kỹ năng làm việc với hệ thống Cisco.

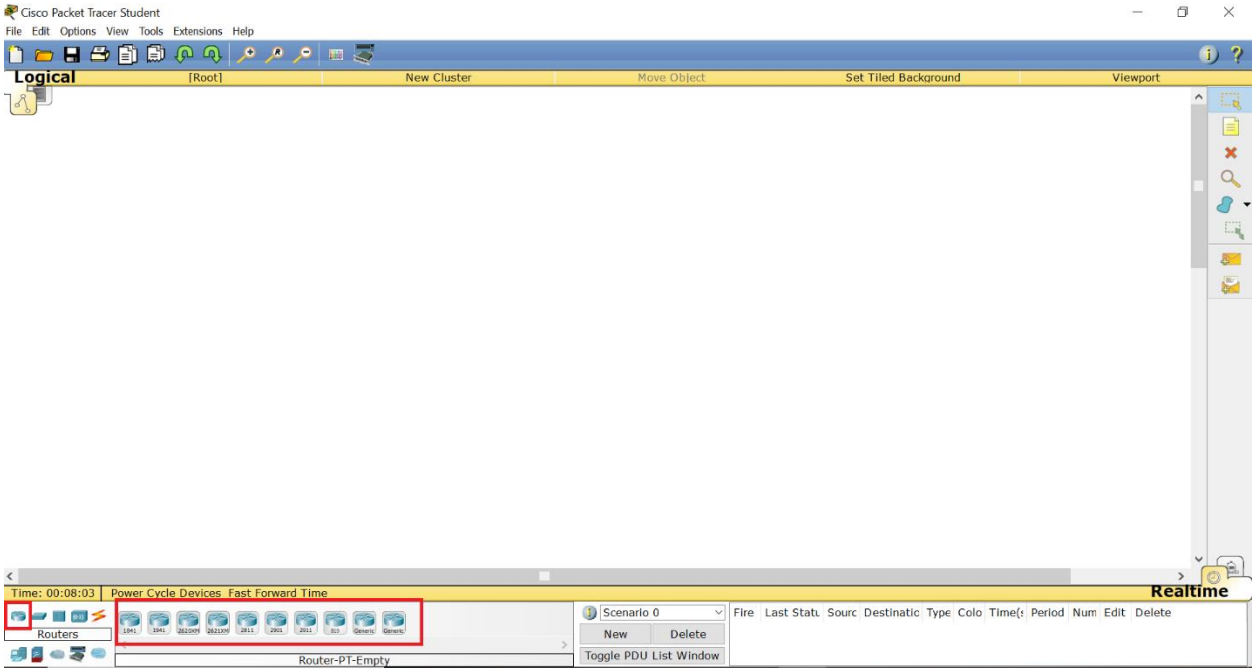
Cấu hình đòi hỏi để cài đặt Cisco Packet Tracer:

- CPU: Intel Pentium 300 MHz trở lên
- OS: Microsoft Windows 2000, Windows XP, Vista Home Basic, Vista Home Premium, Win 7, Win 10, Fedora 7, or Ubuntu 7.10
- RAM: 96 MB
- Ổ cứng: còn trống hơn 250 MB
- Độ phân giải màn hình: 800 x 600 hoặc cao hơn
- Macromedia Flash Player >= 6.0
- Font chữ Unicode

Để cài đặt phần mềm ta có thể đăng ký và download từ trang chủ của cisco: https://www.netacad.com. Phần mềm được cung cấp miễn phí.

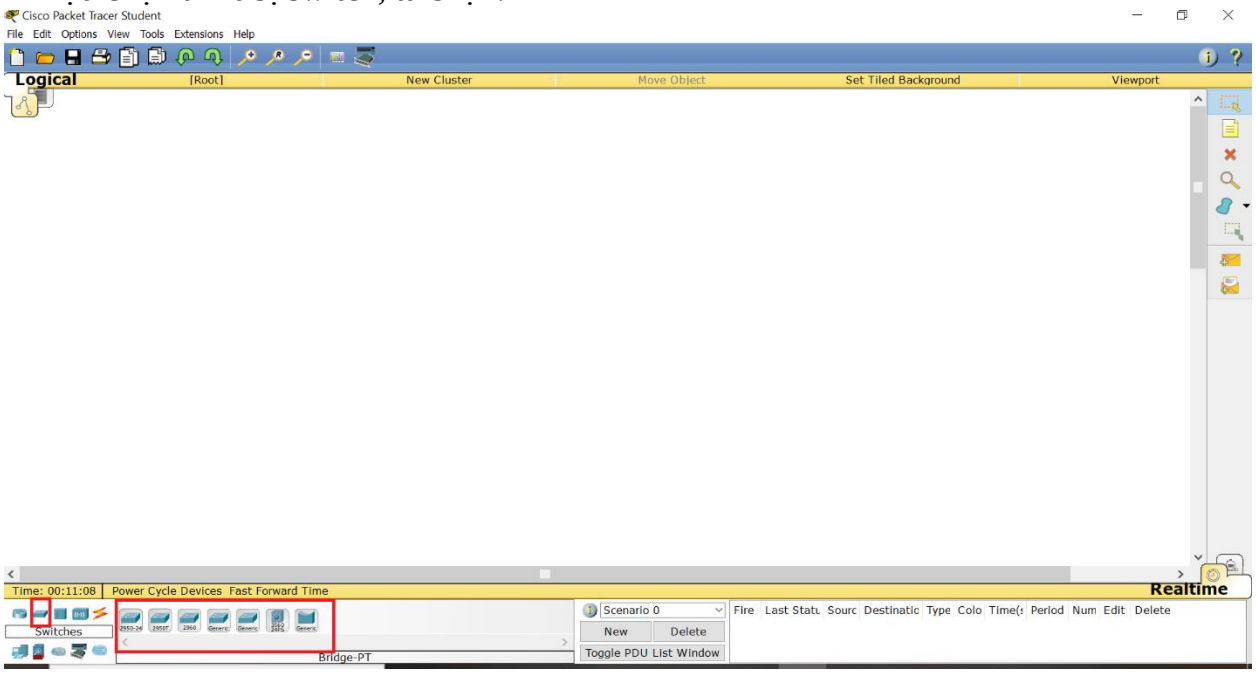
Sau khi cài đặt ta chạy chương trình Cisco Packet Tracer.

Để lựa chọn các thiết bị router, ta chọn mục router trên phần mềm.

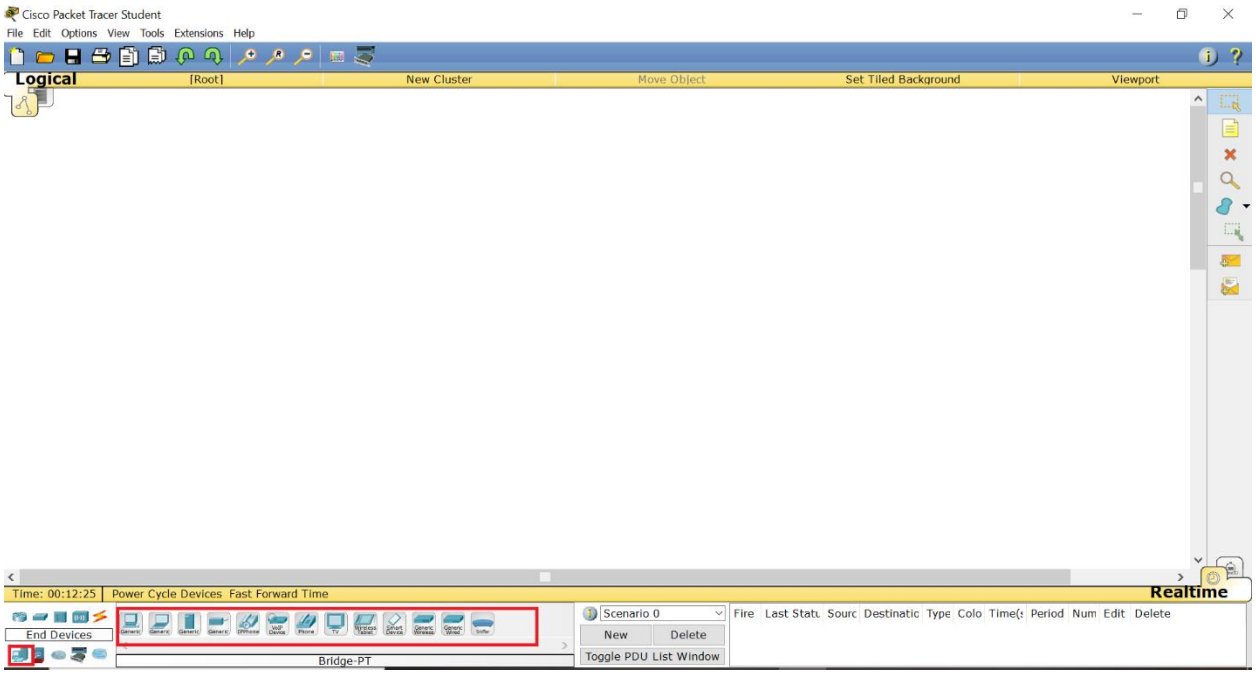


Hình ảnh phần mềm Packet Tracer

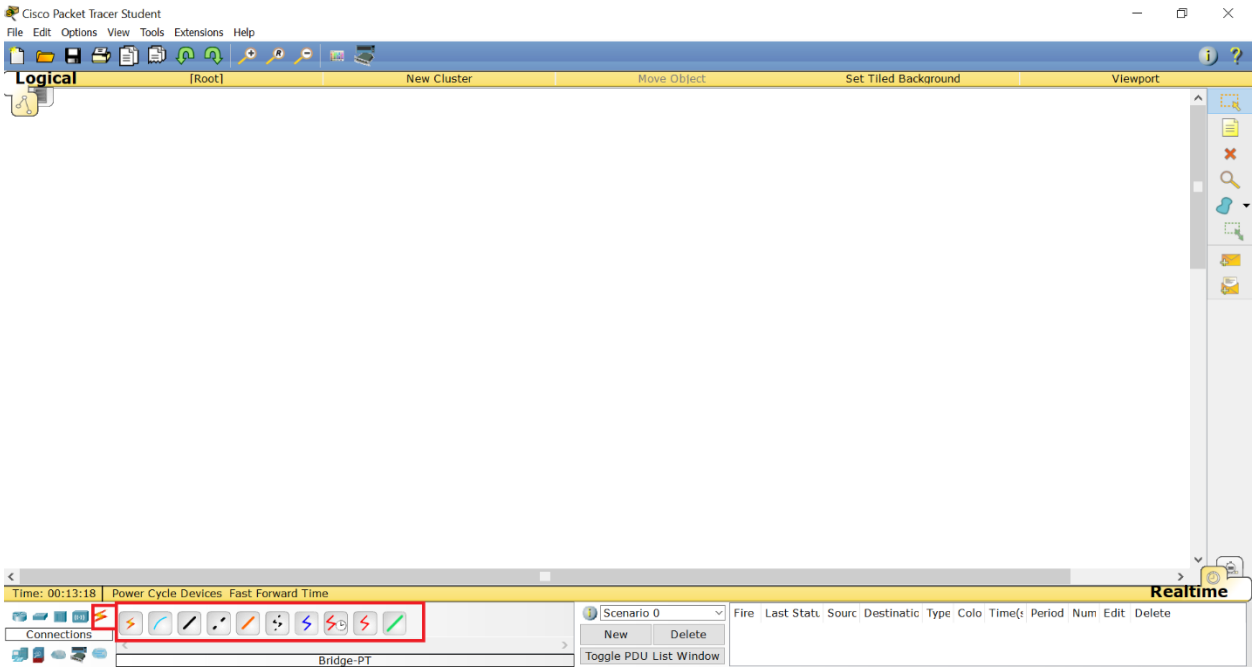
Để lựa chọn thiết bị switch, ta chọn:



Để lựa chọn các loại thiết bị về máy tính, ta chọn:



Để lựa chọn cách kết nối, ta chọn:



2. Các câu lệnh căn bản trên router

a) Các mode của router:

Khi ta khởi động router, dấu nhắc đợi lệnh của router có dạng:

Router> đang ở dạng user mode

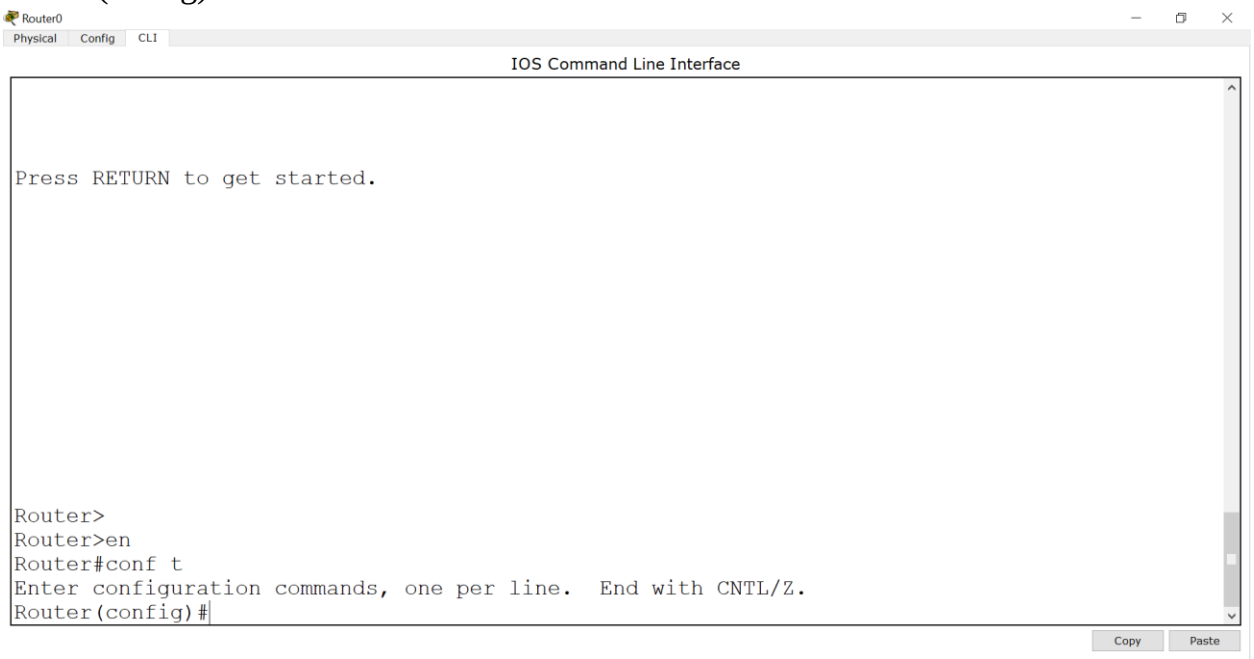
Để quan sát các lệnh được phép sử dụng ở user mode, ta gõ dấu chấm hỏi (?) và Enter

Router> **?**

Để vào Privileged mode, ta dùng lệnh:

Router> ***enable***

Router# đang ở privileged mode
Để quan sát các lệnh được phép sử dụng ở privileged mode, ta gõ dấu chấm hỏi (?) và Enter
Router# **?**
Để vào chế độ cấu hình, ta dùng lệnh:
Router#**config terminal**
Router(config)# đang ở dạng config mode
Để quan sát các lệnh được phép sử dụng ở config mode, ta gõ dấu chấm hỏi (?) và Enter
Router(config)#**?**



b) Một số thao tác cơ bản trên router

Đặt password cho router

Vì lý do bảo mật, ta sẽ đặt mật khẩu cho các mode cấu hình. Điều này có nghĩa là mỗi khi đăng nhập vào một mode thì IOS sẽ yêu cầu chúng ta nhập vào password.
Nếu password đúng thì mới có thể vào mode này.
Chúng ta sẽ thực thi việc đặt password cho:

- Console
- Enable mode

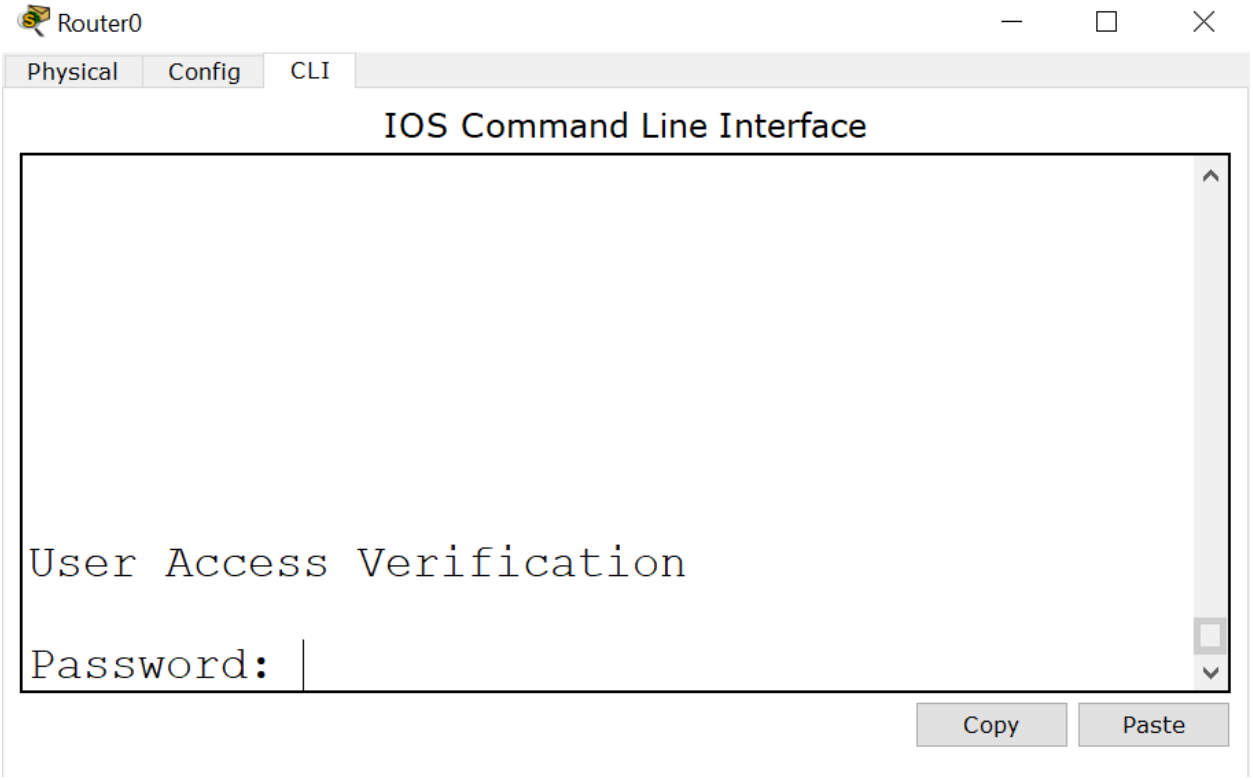
Đặt password cho cổng console (console password)

Ý nghĩa: Trước khi vào user mode, IOS sẽ yêu cầu nhập password để kiểm tra.

Thực hiện:

Router> enable
Router# configure terminal
Router(config)# line console 0 //chọn cổng console được kết nối đến router.
Router(config-line)# password cisco //Pass được đặt là cisco
Router(config-line)# login

Router(config-line)# exit



Hình ảnh kết quả

Đặt password cho enable mode

Ý nghĩa: Trước khi chuyển vào chế độ privileged mode, phải nhập password:

Thực hiện

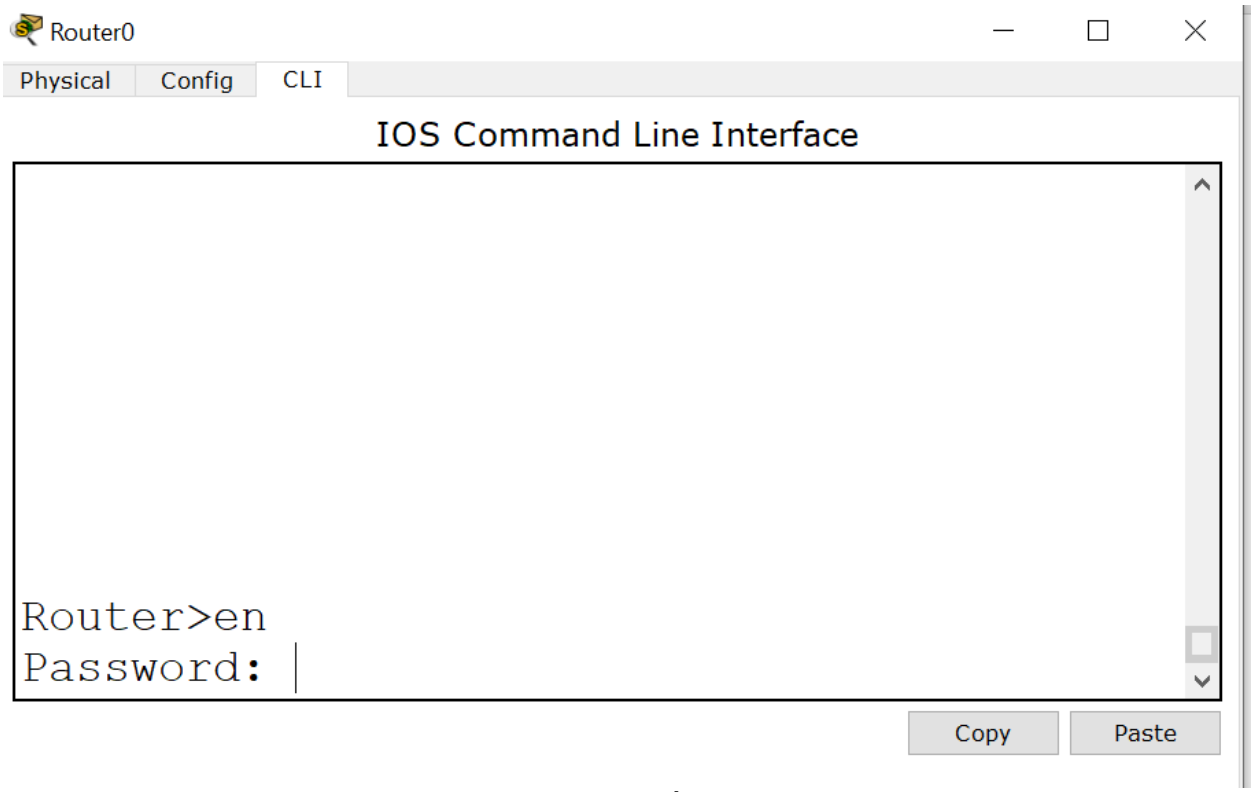
Router(config)# enable password cisco

Hoặc

Router(config)# enable secret cisco

Chú ý:

Nếu sử dụng cả hai câu lệnh này, thì password của câu lệnh thứ 2 (enable secret) mạnh hơn, có nghĩa là nó sẽ được sử dụng.



Hình ảnh kết quả

Câu lệnh mã hóa password:
Router(config)# service password-encryption
Câu lệnh tắt mã hóa password:
Router(config)# no service password-encryption
Đặt tên cho router:
Ý nghĩa: đặt tên cho router. Mỗi Router có thể gán một cái tên, cấu hình để gán tên cho router như sau.
Thực hiện
Router(config)# hostname hostname
Ví dụ:
Router(config)# hostname SAIGON
SAIGON(config)#
Đặt banner cho router:
Ý nghĩa: Khi đăng nhập vào router, sẽ xuất hiện dòng thông báo này.
Thực hiện:
Router(config)# banner motd # text message #
Ví dụ:
Router(config)#banner motd # Hãy nhập Password #

Hình ảnh sau khi thiết lập banner

Đặt địa chỉ IP cho interface

Ý nghĩa: mỗi cổng (interface) của router phải mang một địa chỉ IP để giao tiếp với các thiết bị. Do đó, ta phải thiết lập IP cho các cổng của router.

Thực hiện:

Đặt địa chỉ IP cho cổng Fast Ethernet (thông thường, đây là cổng để kết nối giữa router và switch hoặc router và PC). Mỗi cổng sẽ được đặt tên riêng. Tùy theo thiết bị mà mỗi cổng sẽ có tên khác, thông thường các cổng sẽ có tên là: fastether0/0, fastethernet0/1, ….

Router(config)# interface fastethernet0/0 //Gọi tên cổng cần cấu hình
Router(config-if)#ip address 192.168.1.1 255.255.255.0 //Đặt IP và subnet mask
Router(config-if)#no shutdown //Khởi động cổng.

Đặt địa chỉ IP cho cổng serial (thông thường, đây là cổng để kết nối giữa router và router). Mỗi cổng sẽ được đặt theo tên riêng. Tùy theo thiết bị mà mỗi cổng sẽ có tên khác, thông thường, các cổng sẽ có tên là: seria; 0/0, serial 0/1,…

Router(config)# interface serial 0/0 //Gọi tên cổng cần cấu hình
Router(config-if)#ip address 192.168.1.1 255.255.255.0 //Đặt IP và subnet mask
Router(config-if)#clock rate 64000 //Thiết lập xung nhịp giữa các router
Router(config-if)#no shutdown //Khởi động cổng

Đặt lời mô tả cho interface (Interface Description)

Ý nghĩa: đặt lời mô tả cho interface, chú thích trong việc quản trị các thiết bị sau này.

Thực hiện

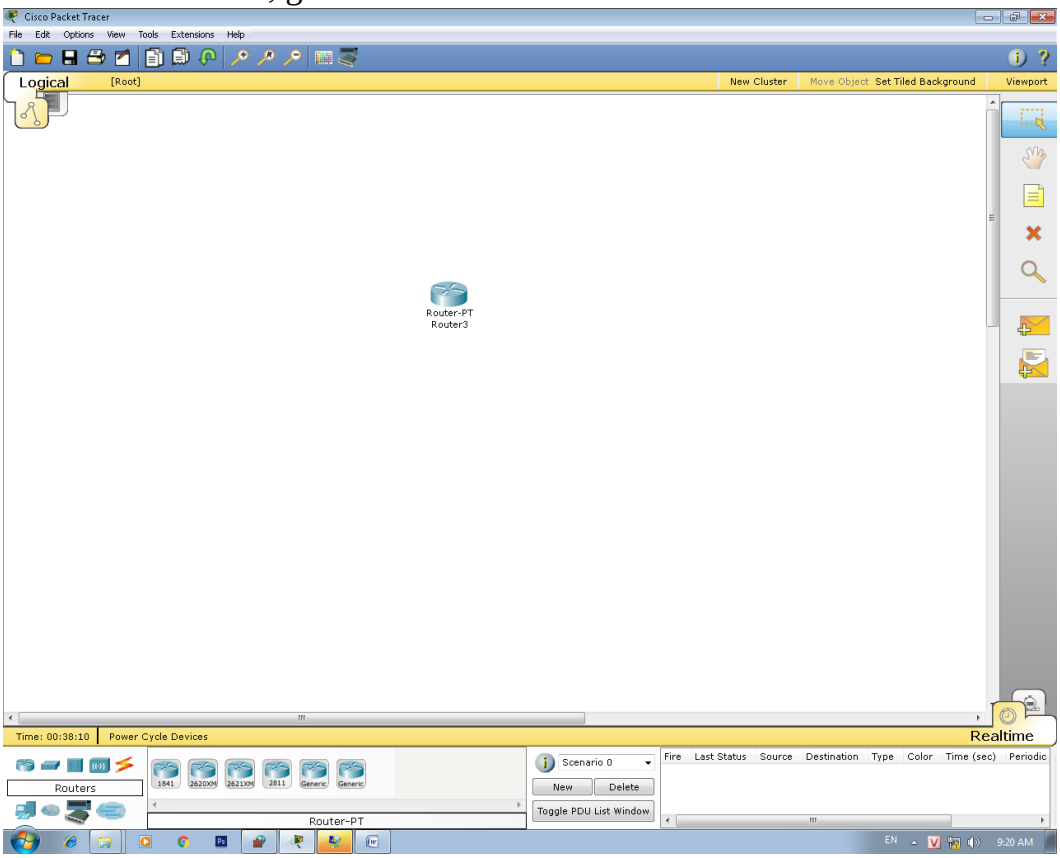
Router(config)#interface interface

Router(config-if)#description lời mô tả cho interface
Ví dụ:
Router(config)#interface fa0/0
Router(config-if)#description Kết nối với LAN Sales
Một số câu lệnh xem thông tin:
Router#show ip route: Xem bảng định tuyến
Router#Show version: Xem cấu hình thanh ghi
Router#Show flash: Xem thông tin hệ điều hành (.bin)
Router#Show history: Xem tất cả lệnh trong bộ nhớ(buffer)
Router#Show ip interface brief
Router#Show cdp: Xem thông tin CDP
Router#ping : Kiễm tra kết nối
Router#Show running-config // hiển thị cấu hình in RAM
Router#Show start-config //hiển thị cấu hình in NVRAM

II. Bài tập thực hành:

Bài 1:

Trên Packet Tracer, gán 1 router.

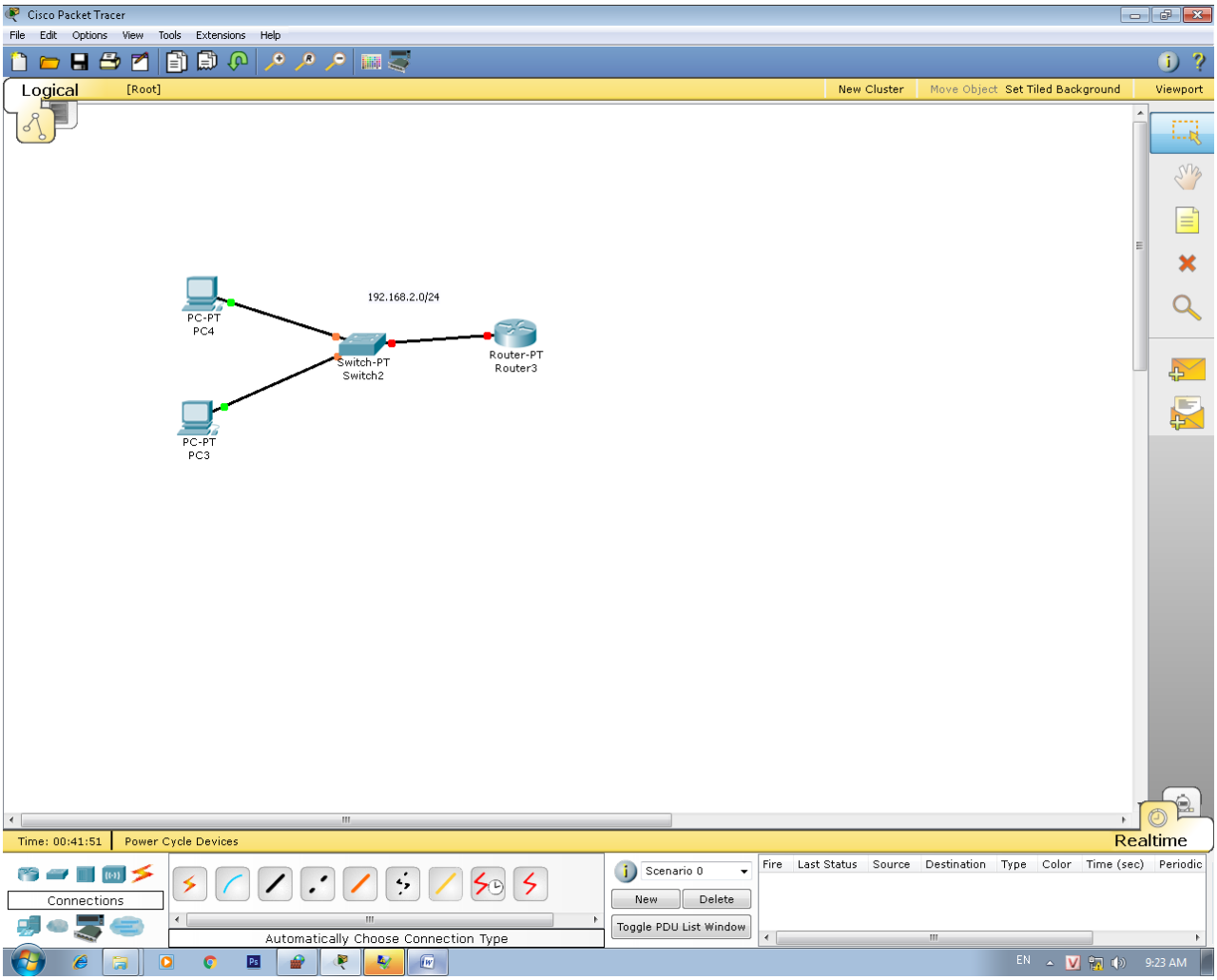


Yêu cầu :
Đặt Password cho cổng console.

Đặt password cho cổng privelled mode với enable password.
Đặt password cho cổng privelled mode với enable secret.
Vô hiệu hóa password dạng enable secret.
Tất cả password phải lưu dưới dạng mã hóa.
Đổi tên router thành SaiGon.
Đặt banner là “Day la router SaiGon”.

Bài 2 :

Cho mô hình :

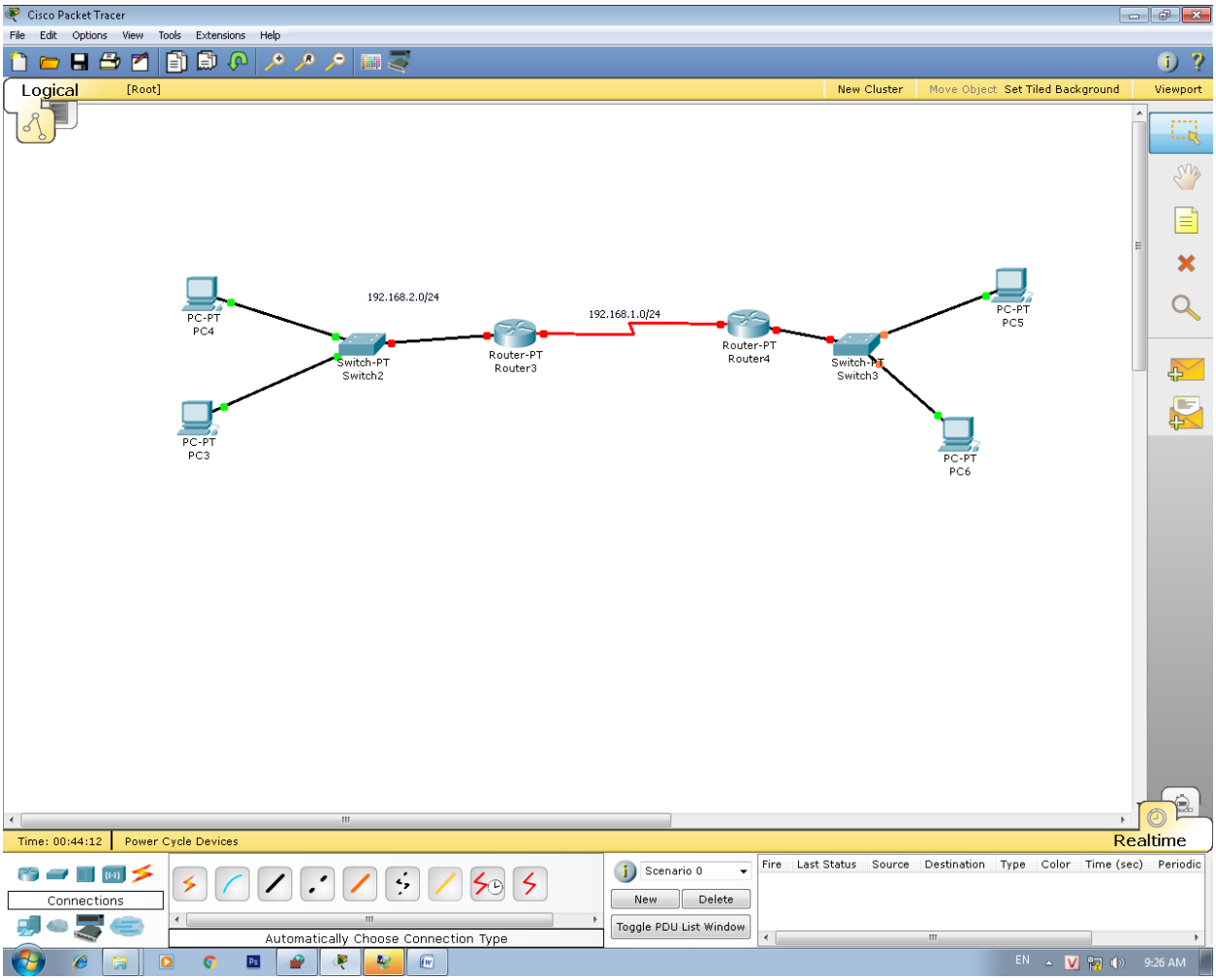


Yêu cầu:

Thiết lập password ở console, privelled mode.
Đổi tên router là SaiGon.
Đặt banner là : “Router SAIGON’
Gán địa chỉ IP cho phù hợp với mô hình.
Kiểm tra kết nối giữa router và PC.

Bài 3 :

Cho mô hình :

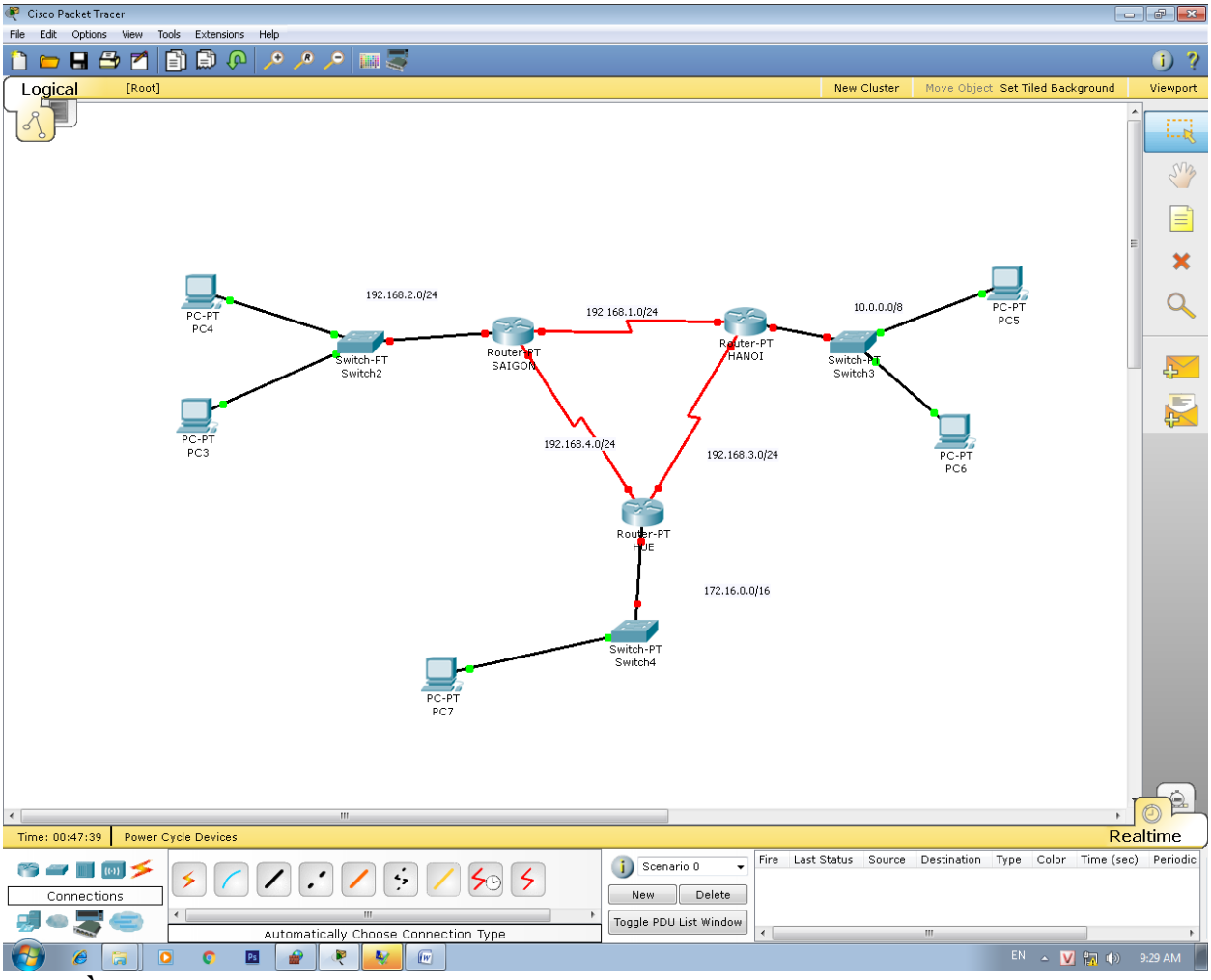


Yêu cầu:

Thiết lập password ở console, privelled mode.
Đổi tên một router là SaiGon.
Đặt banner là : “Router SAIGON’
Gán địa chỉ IP cho phù hợp với mô hình.
Kiểm tra kết nối giữa router và PC.
Đổi tên router còn lại là CanTho.
Đặt banner là : “Router CANTHO’
Gán địa chỉ IP cho phù hợp với mô hình.
Kiểm tra kết nối giữa router và PC.

Bài 4 :

Cho mô hình :



Yêu cầu:

Thực hiện mô hình trên. Gán địa chỉ IP cho các router theo mô hình. Yêu cầu các router phải có password ở console và privelled mode, và phải có banner thông báo (password và banner thông báo sinh viên tự đặt).

BÀI 2: CẤU HÌNH ROUTER CĂN BẢN

I. Hướng dẫn thực hiện

Lưu trữ file cấu hình

Ý nghĩa: khi thực hiện cấu hình router, các câu lệnh cấu hình sẽ được lưu trữ trên RAM, do đó, khi tắt máy các cấu hình này sẽ bị mất. Để lưu trữ những cấu hình đã thực hiện ta phải lưu trữ các cấu hình này xuống NVRAM.

Thực hiện:

Router#copy running-config startup-config

Ví dụ:

```
SaiGon#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SaiGon#
%SYS-5-CONFIG_I: Configured from console by console
```

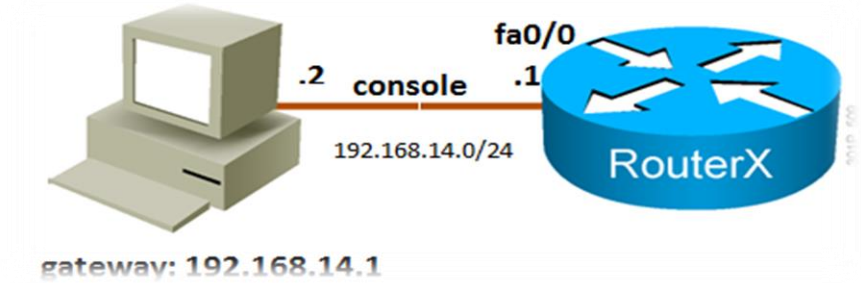
Lưu trữ IOS cho router.

Ý nghĩa: các router cũng có hệ điều hành IOS để điều khiển và quản lý các thiết bị hoạt động. Do đó, cũng có thể xảy ra tình huống mất hay hư hỏng IOS dẫn đến router không thể hoạt động, hoặc hoạt động sai. Để tránh tình huống này, người ta sẽ lưu trữ bản sao IOS của router, để khi có vấn đề sẽ lấy ra để phục hồi.

Để thực hiện được việc này, người ta sẽ dùng một server lưu trữ gọi là TFTP server để lưu trữ IOS cho router, và sẽ backup IOS này khi cần.

Thực hiện:

Để thực hiện được, ta phải có 1 TFTP server kết nối vào router.



Sau khi đã thiết lập IP cho router và TFTP server, ta bắt đầu lưu trữ IOS của router vào TFTP server.

Router#show version *//xem phiên bản IOS của router*
Router#show flash *//xem thông tin lưu trữ của router*
Router#copy flash tftp *//copy IOS từ flash sang tftp server*
//source filename: *.bin(IOS) 192.168.14.2
//Address or name of remote host[]? Address tftp server
//Destination filename *.bin ; //Mở tftp server lên

Ví dụ:

```
SaiGon#show version
Cisco Internetwork Operating System Software
IOS (tm) PT1000 Software (PT1000-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang
Image text-base: 0x8000808C, data-base: 0x80A1FECC

ROM: System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.
ROM: PT1000 Software (PT1000-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)

System returned to ROM by reload
System image file is "flash:pt1000-i-mz.122-28.bin"

PT 1001 (PTSC2005) processor (revision 0x200) with 60416K/5120K bytes of memory
.
Processor board ID PT0123 (0123)
PT2005 processor: part number 0, mask 01
Bridging software.
X.25 software, Version 3.0.0.
4 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
```

Lưu ý file pt1000-i-mz.122-28.bin

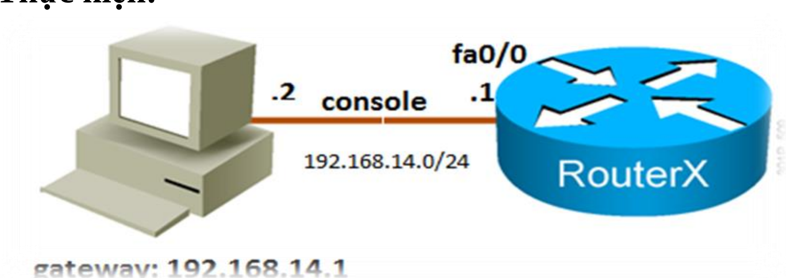
```
SaiGon#copy flash tftp:
Source filename []? pt1000-i-mz.122-28.bin
Address or name of remote host []? 192.168.1.10
Destination filename [pt1000-i-mz.122-28.bin]?

Writing pt1000-i-
mz.122-28.bin....!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 5571584 bytes]

5571584 bytes copied in 3.088 secs (413412 bytes/sec)
SaiGon#
```

Tới đây ta đã thực hiện thành công việc copy file IOS vào TFTP server.

Backup lại IOS từ TFTP server vào router.

Ý nghĩa: trong trường hợp router bị lỗi, ta có thể sử dụng TFTP server đã có lưu trữ file IOS của router trước đây, sau đó ta sẽ backup vào router.

Thực hiện:



PC chạy TFTP server nối với Router trong cùng mạng LAN. IOS image mới sẽ chứa trong PC và sẽ truyền qua Cisco Router bằng giao thức TFTP. PC hoạt động như TFTP server, router sẽ là TFTP client.

Sau khi đã xác định TFTP server đã gắn IP để kết nối đến router. File IOS đã sẵn sàng để chép. Giả sử rằng, IOS của router đã hư hỏng hoàn toàn. Ta thực hiện các câu lệnh sau:

```
Rommon> FE_PORT=0
Rommon> IP_ADDRESS=10.0.0.1
Rommon> IP_SUBNET_MASK=255.0.0.0
Rommon> DEFAULT_GATEWAY=10.0.0.2
Rommon> TFTP_SERVER=10.0.0.2
Rommon> TFTP_FILE=c2600-is-mz.113-3.0.3.0.bin
Rommon> sync
Rommon> tftpdnld
Rommon> dir flash:
Rommon> reset
```

Sau khi reset lại, IOS của router đã được chép lại, và sẵn sàng hoạt động bình thường.

Khôi phục mật khẩu cho router.

Ý nghĩa: trong một số tình huống ta mất mật khẩu để đăng nhập vào router, do đó, để lấy lại mật khẩu của router ta phải thực hiện khôi phục mật khẩu cho router như sau:

Thực hiện:

Thao tác trực tiếp trên Router.

Quá trình khởi động của Router đã được định trước. Sau quá trình POST và nạp hệ điều hành IOS, router sẽ nạp cấu hình hoạt động trong NVRAM. Các cấu hình này không chỉ chứa thông tin giao thức định tuyến, địa chỉ mà còn chứa mật khẩu của Router.

Mật khẩu được phục hồi bằng cách bỏ qua nội dung file cấu hình (Configuration file) trong NVRAM trong quá trình khởi động.

Việc bỏ qua cấu hình được thực hiện bằng cách sửa đổi nội dung thanh ghi cấu hình *(configuration register)* router.

Lúc này: Router sẽ không cấu hình chứa mật khẩu cần phục hồi.

Khi đã vào được router, người dùng có thể xem mật khẩu trong NVRAM và có thể sử dụng, xóa hay thay đổi chúng.

Thực hiện sửa đổi nội dung thanh ghi cấu hình: **0x2102 -> 0x2142**

Việc phục hồi mật khẩu(Password Recovery) khác nhau đối với các dòng router.

Để thực hiện được, ta thực hiện các bước sau:

- Tắt router và bật lại(Turn off / Turn on)
- Bấm tổ hợp (Ctrl + Break)

//Màn hình thông báo dung lượng bộ nhớ Ram của router hoặc 15 giây sau khi Turn on

- Router vào monitor mode, thực hiện lệnh:
  Rommon 1>confreg 0x2142

Rommon 2>reset

// Router sẽ nhắc phải reset lại để thay đổi có tác dụng, sau khi khởi động sẽ không bị đòi hỏi pass, do router không load từ NVRAM vào RAM

Sau khi thực hiện các bước trên, ta sẽ đặt password lại cho router và lưu xuống file NVRAM

Router#copy start run
Router#show run *//xem password hoặc đặt pass mới*
Router#copy run start *//lưu lại cấu hình*

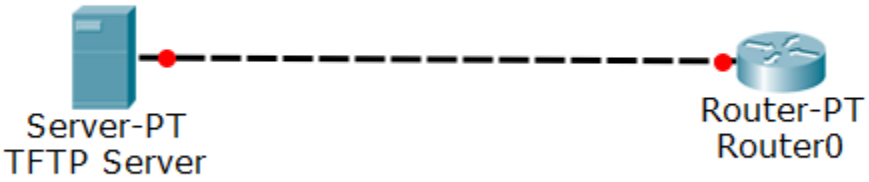
Thay đổi thanh ghi:

- Xem cấu hình thanh ghi hiện tại:
  Router#show version *//configuration register is 0x2142*
- Thay đổi thanh ghi:
  Router#confg terminal
  Router(config)#config-register 0x2102
  Router(config)#exit

Sau khi thực hiện xong, ta chỉ cần reset lại router lần nửa, sau đó sẽ sử dụng password đã đặt trước đó.

II. Bài tập thực hành:

Bài 1: Cho mô hình



Với mô hình như trên, hãy tự đặt IP cho router và TFTP server. Hãy thực hiện các việc sau:

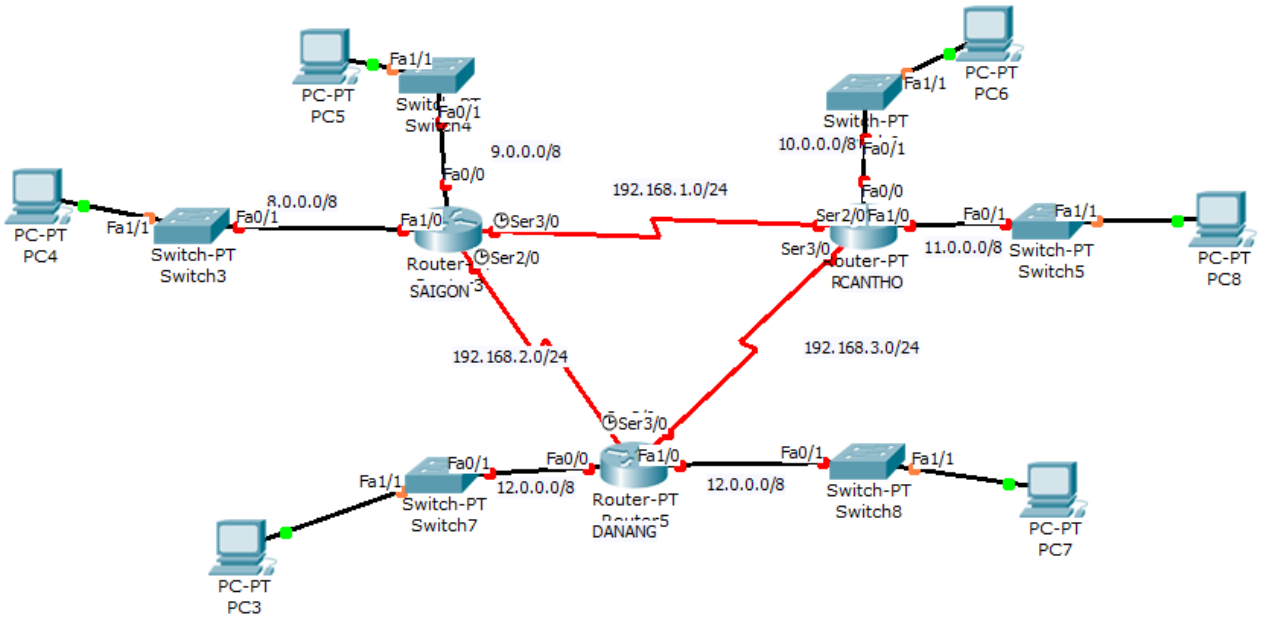
Thiết lập dịch vụ trên TFTP Server.

Cấu hình trên router, chép IOS sang TFTP server.

Thực hiện delete flash trên router.

Cấu hình chép IOS từ TFTP server sang Router.

Bài 2



Yêu cầu :

Đặt tên của các router theo như mô hình trên.

Đặt banner “Day la router <<tên router>>” cho các router trên.

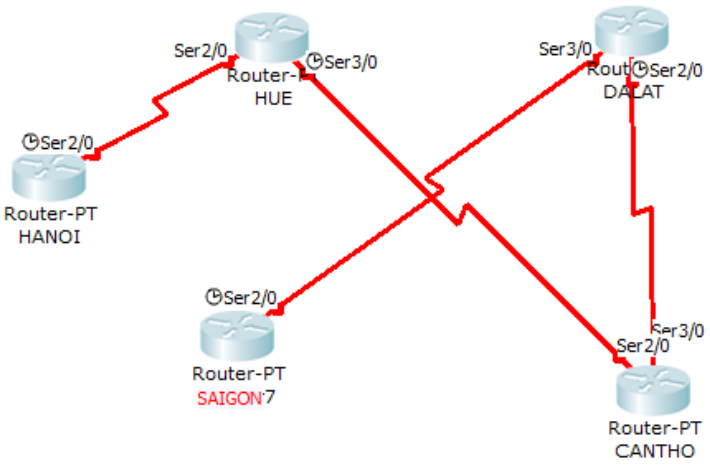
Đặt Pass cho enable mode và console mode cho các router trên.

Thực hiện mã hóa password cho các pass đã đặt.

Đặt IP cho các interfaces tương ứng với mô hình.

Kiểm tra sự liên thông của các router.

Bài 3 : Cho mô hình :



Yêu cầu :

Sinh viên tự thêm địa chỉ IP vào mô hình.
Đặt tên của các router theo như mô hình trên.
Đặt banner "Day la router <<tên router>>" cho các router trên.
Đặt Pass cho enable mode và console mode cho các router trên.
Thực hiện mã hóa password cho các pass đã đặt.
Đặt IP cho các interfaces tương ứng với mô hình.
Kiểm tra sự liên thông của các router.

BÀI 3: CẤU HÌNH ĐỊNH TUYẾN TĨNH TRÊN ROUTER

I. Hướng dẫn thực hiện

1. Khái niệm về định tuyến:

Định tuyến là chức năng của router giúp xác định quá trình tìm đường đi cho các gói tin từ nguồn tới đích thông qua hệ thống mạng.

Các loại định tuyến: Chia làm 2 loại

- Định tuyến tĩnh: do người quản trị quy định đường đi của gói tin.
- Định tuyến động: do thuật toán cấu hình quy định đường đi của gói tin.

Ưu điểm của định tuyến tĩnh:

- Router không phải thực hiện các thuật toán định tuyến, do đó không tiêu tốn tài nguyên để xử lý.
- Thông tin sẽ đi theo con đường mà người quản trị đã cấu hình, làm tăng tính bảo mật của thông tin truyền trên mạng.
- Định tuyến tĩnh thích hợp cho các mạng nhỏ, ít có sự thay đổi trong topo mạng.

Nhược điểm của định tuyến tĩnh:

- Router không có khả năng tự cập nhật các thông tin về đường đi khi có sự thay đổi trong mạng. Do đó không thích hợp sử dụng khi sử dụng cho hệ thống mạng lớn.

2. Cách cấu hình định tuyến tĩnh:

Để cấu hình định tuyến tĩnh, ta phải cấu hình hoàn tất IP cho các interface của router. Sau đó, căn cứ theo sơ đồ mạng mà thiết lập cấu hình với câu lệnh như sau:

Cấu hình: dùng lệnh ip route. Cấu trúc như sau:

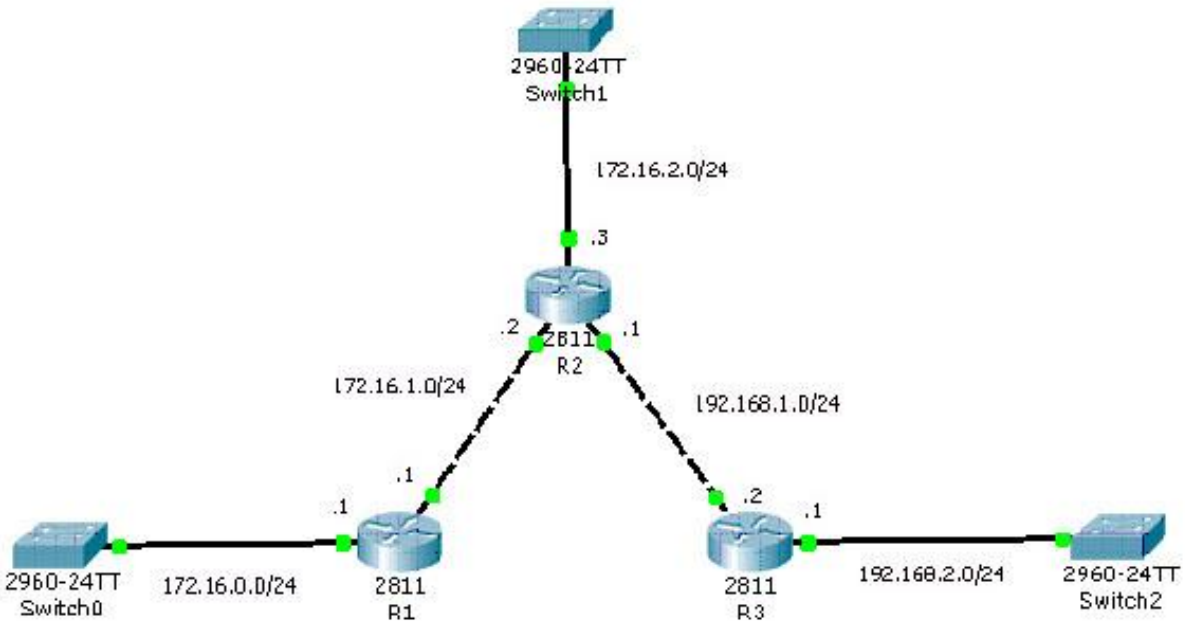
Router(config)#ip route [network-address] [subnet-mask] [next-hop]

Với:

[network-address]: địa chỉ của mạng đích
[subnet-mask]: subnet mask của mạng đích
[next-hop]: là địa chỉ IP của cổng phải đi qua để đến mạng đích

3. Ví dụ minh họa:

Giả sử có sơ đồ mạng như sau:



Giả sử rằng, ta đã cấu hình hoàn tất các địa chỉ IP cho các interface của các router đúng theo mô hình. Khi đó, ta cấu hình định tuyến tĩnh như sau:

Trên R1:

R1(config)#ip route 172.16.2.0 255.255.255.0 172.16.1.2
R1(config)#ip route 192.168.1.0 255.255.255.0 172.16.1.2
R1(config)#ip route 192.168.2.0 255.255.255.0 172.16.1.2

Trên R2:

R2(config)#ip route 172.16.0.0 255.255.255.0 172.16.1.1
R2(config)#ip route 192.168.2.0 255.255.255.0 192.168.1.2

Trên R3:

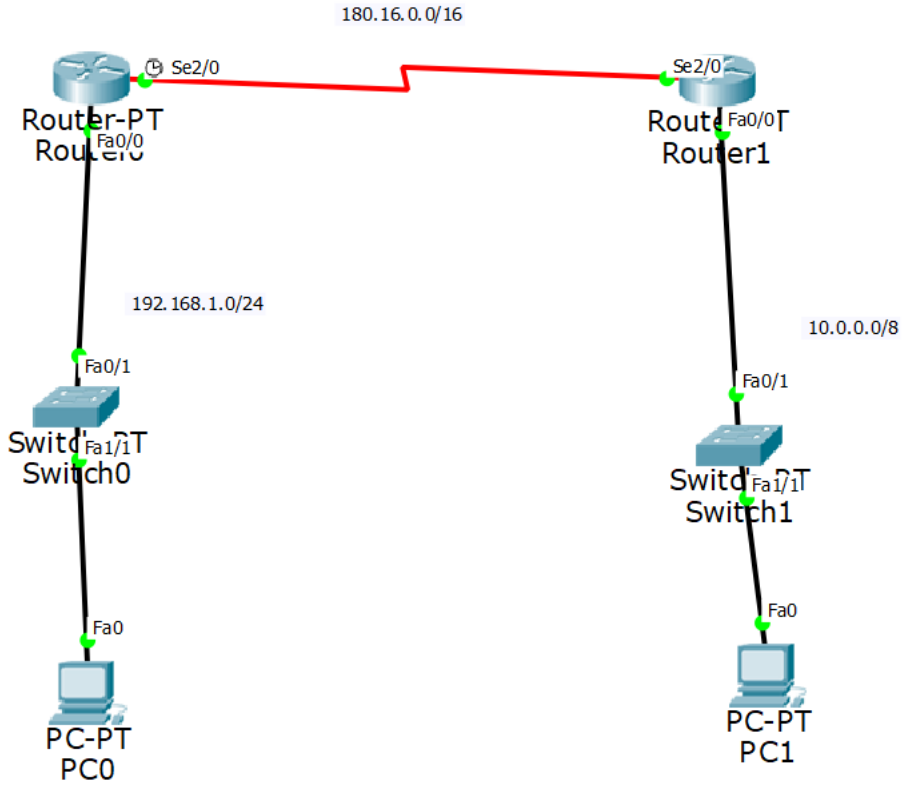
R3(config)#ip route 172.16.0.0 255.255.255.0 192.168.1.1
R3(config)#ip route 172.16.1.0 255.255.255.0 192.168.1.1
R3(config)#ip route 172.16.2.0 255.255.255.0 192.168.1.1

Sau khi thực hiện cấu hình chỉ các đường cần thiết cho từng router, router sẽ có thể giao tiếp với các đường mạng mà nó đã được hướng đến.

II. Bài tập thực hành:

Bài 1:

Cho sơ đồ sau:



Hãy cấu hình các địa chỉ như trong hình. Thực hiện cấu hình sao cho PC0 có thể ping đến PC1.

Để thực hiện điều này, ta phải thực hiện định tuyến. Ở đây, ta sẽ dùng định tuyến tĩnh.

Câu lệnh thực hiện định tuyến tĩnh:

Router(config)#ip route <địa chỉ mạng cần đến> <subnetmask của mạng này> <cổng interface cần đến>.

Ví dụ: trong mô hình trên, tại router bên tay trái, ta phải cấu hình chỉ đường đến lớp 10.0.0.0/8. Lớp này nằm bên trong của Router1.

Router(config)#ip route 10.0.0.0 255.0.0.0 180.16.0.2

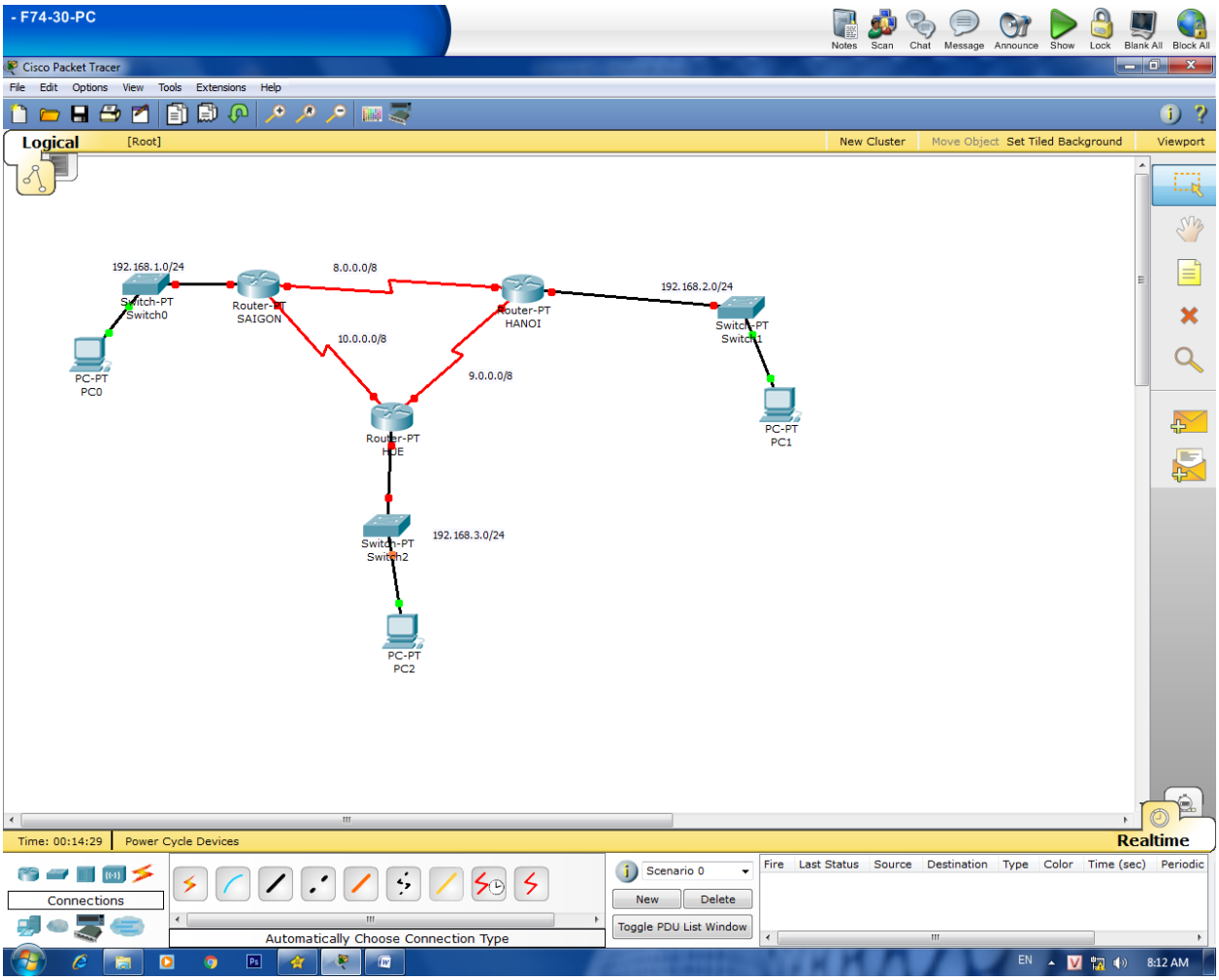
Ngược lại, tại router bên phải, ta cũng cấu hình chỉ đường đến lớp 192.168.1.0, lớp này nằm bên trong của router0.

Router(config)#ip route 192.168.1.0 255.255.255.0 180.16.0.1

Lưu ý: giả sử rằng cổng ser2/0 của router bên trái là 180.16.0.1/16 và cổng ser2/0 của router bên phải là 180.16.0.2/16.

Bài 2:

Cho mô hình như sau:

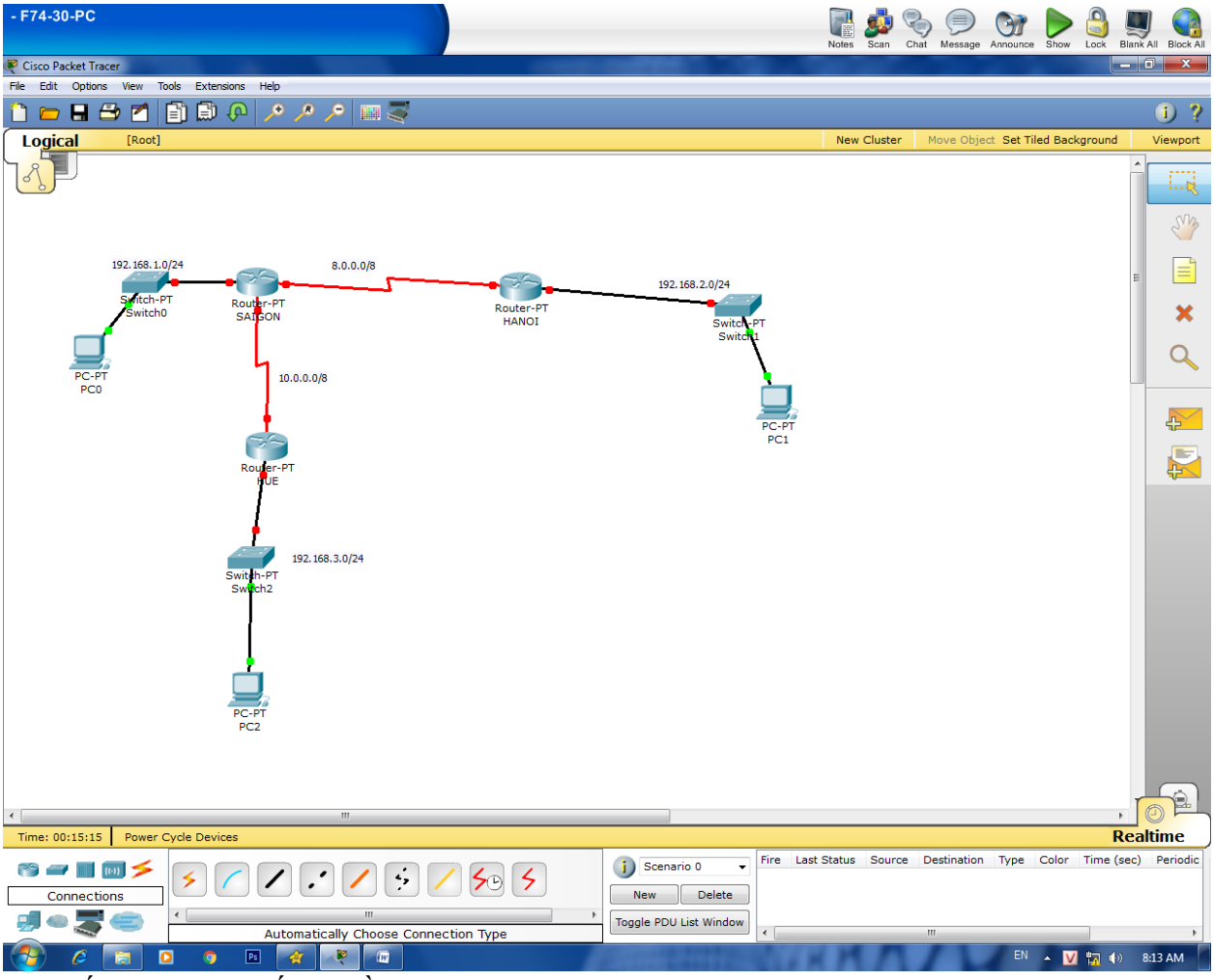


Hãy cấu hình hoàn tất sơ đồ trên.

Hãy thực hiện định tuyến tĩnh để cấu hình sao cho tất cả các PC và router có thể ping thấy nhau.

Bài 3:

Cho mô hình như sau:

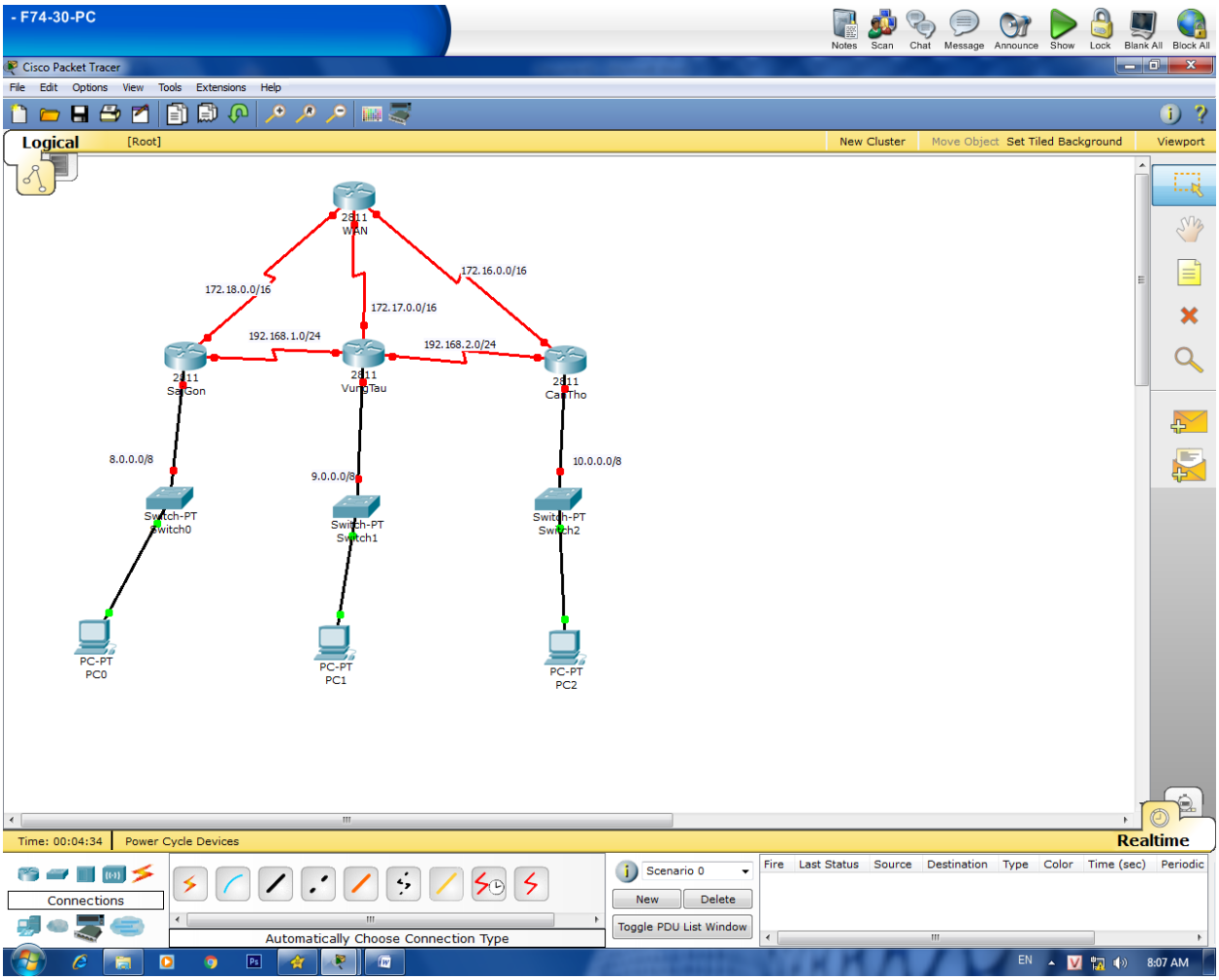


Hãy cấu hình hoàn tất sơ đồ trên.

Hãy thực hiện định tuyến tĩnh để cấu hình sao cho tất cả các PC và router có thể ping thấy nhau.

Bài 4:

Cho mô hình như sau:



Hãy cấu hình hoàn tất sơ đồ trên.

Hãy thực hiện định tuyến tĩnh để cấu hình sao cho tất cả các PC và router có thể ping thấy nhau.

BÀI 4: CẤU HÌNH ĐỊNH TUYẾN TĨNH – DEFAULT ROUTE

I. Hướng dẫn thực hiện

1. Khái niệm default route – đường mặc định:

Đường mặc định là đường mà router sẽ sử dụng trong trường hợp không tìm thấy đường đi nào phù hợp trong bảng định tuyến để đi tới đích.

Trong một số trường hợp, router được đặt ở các biên của hệ thống mạng (nghĩa là router chỉ có 1 con đường để kết nối đến các router khác), ta sẽ áp dụng cách thức định tuyến đường mặc định cho router.

2. Cách cấu hình đường mặc định:

Ta cấu hình tương tự như với cấu hình định tuyến tĩnh.

Câu lệnh:

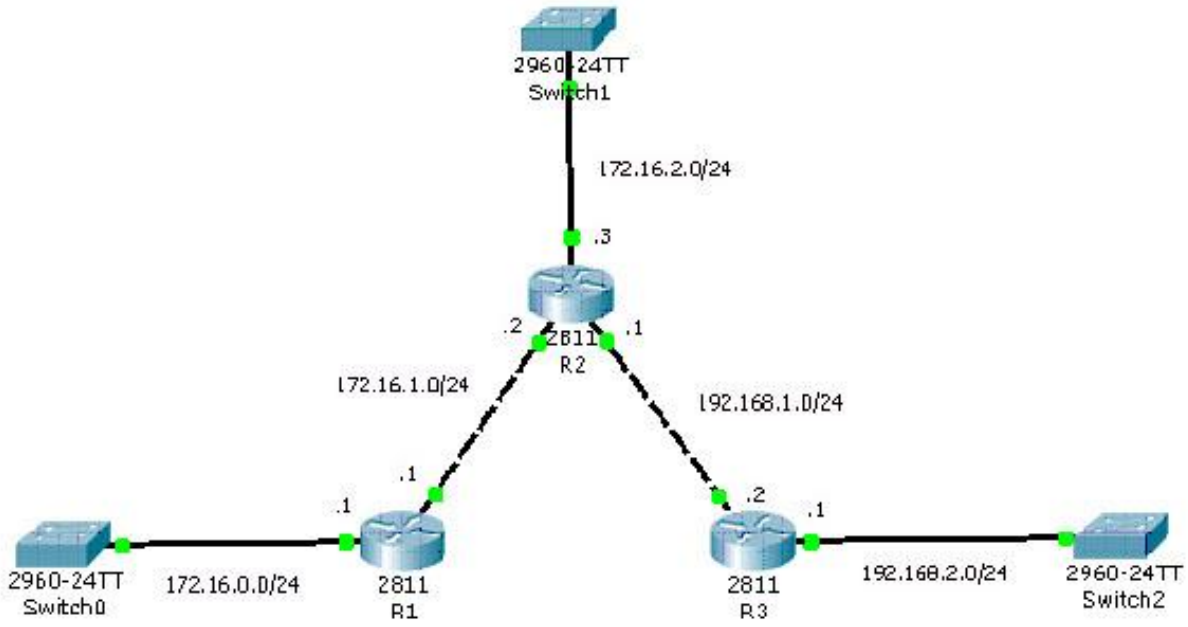
Router(config)#ip route 0.0.0.0.0.0.0.0 [next-hop]

Trong đó:

- Địa chỉ mạng đích và subnet mask đều là 0.0.0.0 đại diện cho các đường mạng không xác định.
- [next-hop]: là địa chỉ của router kế tiếp mà gói tin sẽ đi đến.

3. Ví dụ minh họa:

Giả sử có sơ đồ mạng như sau:



Giả sử rằng, ta đã cấu hình hoàn tất các địa chỉ IP cho các interface của các router đúng theo mô hình. Khi đó, ta cấu hình định tuyến tĩnh kết hợp với đường mặc định như sau:

Trên R1:

R1(config)#ip route 0.0.0.0.0.0.0.0 172.16.1.2

Trên R2:

R2(config)#ip route 172.16.0.0 255.255.255.0 172.16.1.1

R2(config)#ip route 192.168.2.0 255.255.255.0 192.168.1.2

Trên R3:

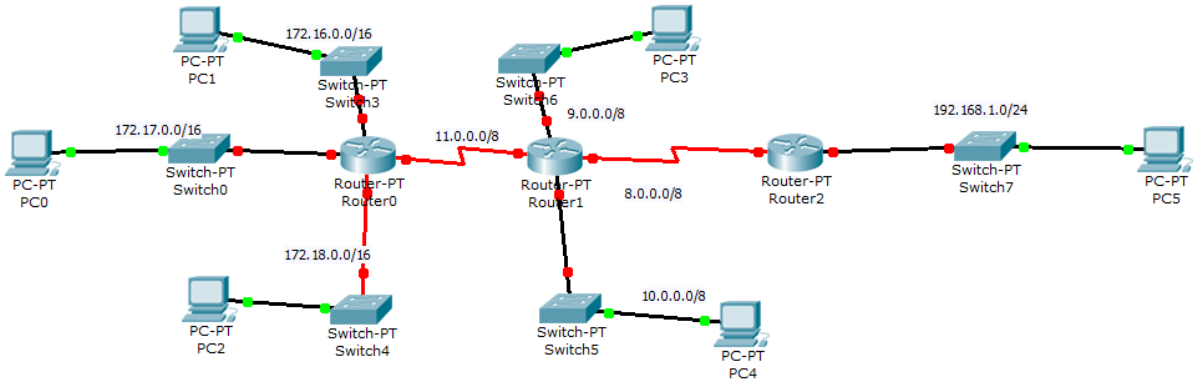
R3(config)#ip route 0.0.0.0.0.0.0.0 192.168.1.1

Trong trường hợp này, ta thấy câu lệnh cấu hình trên R1 và R3 ít hơn hẳn so với cấu hình sử dụng định tuyến tĩnh thông thường.

II. Bài tập thực hành:

Bài 1:

Cho mô hình như sau:



Yêu cầu:

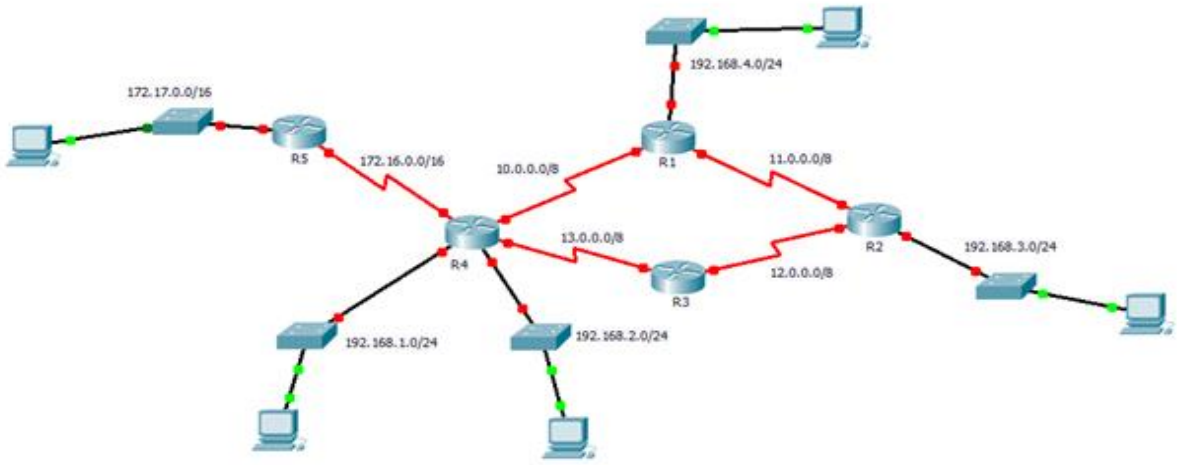
Hãy cấu hình cho các thiết bị theo như trong hình.

Hãy cấu hình định tuyến tĩnh trên router0 và router1 trỏ đến tất cả lớp mạng bên trong của 2 bên.

Trên router2 và router0, hãy cấu hình đường mặc định trỏ về router1.

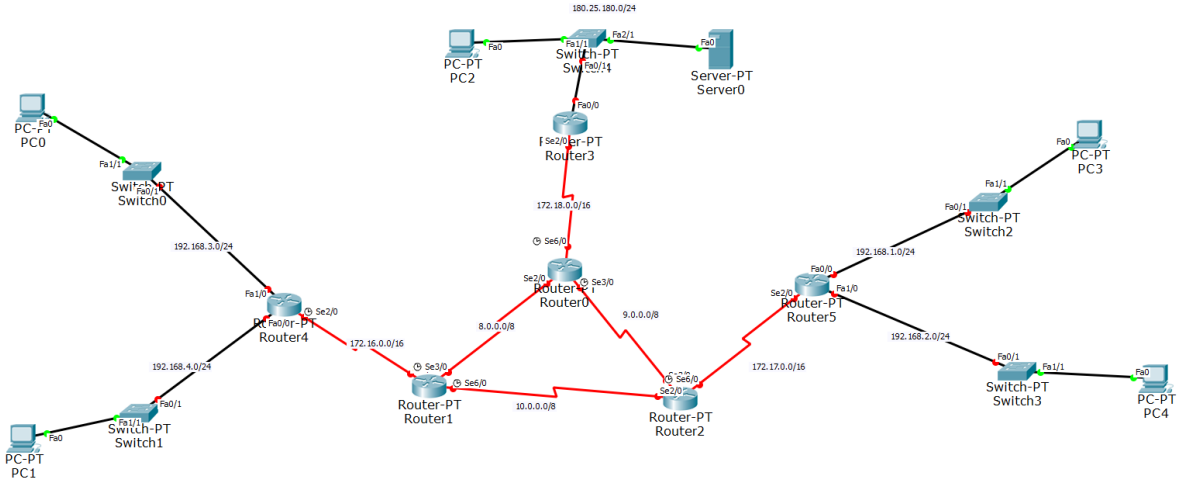
Trên router1, hãy cấu hình định tuyến tĩnh trỏ về đường mạng 192.168.1.0/24.

Bài 2:
Cho mô hình:



Yêu cầu:
Hãy cấu hình các thiết bị như trong mô hình.
Hãy cấu hình tên router theo như mô hình trên.
Hãy cấu hình định tuyến tĩnh trên R1, R2, R3, R4 trỏ về tất cả các lớp bên trong của các router này.
Cấu hình đường mặc định cho R5 trỏ về R4.
Cấu hình R4 trỏ về lớp mạng bên trong của R5 (172.17.0.0/16).

Bài 3:
Cho mô hình sau:



Yêu cầu:
Hãy cấu hình các thiết bị như mô hình trên.

Hãy cấu hình định tuyến tĩnh trỏ về tất cả các đường mạng trên router0, router1, router2. Hãy cấu hình đường mặc định cho router3, router4, router5 trỏ về các router tương ứng trong mô hình trên.

BÀI 5: CẤU HÌNH ĐỊNH TUYẾN ĐỘNG – GIAO THỨC RIP

I. Hướng dẫn thực hiện

1. Khái niệm định tuyến động:

Trong phương pháp định tuyến động, các router sẽ tự xây dựng nên bảng định tuyến nhờ vào các giao thức định tuyến được cài đặt trong router.

Phân loại: chia làm 3 loại

- Distance Vector: các giao thức sẽ dùng thuật toán distance-vector để xây dựng bảng định tuyến. Các giao thức thuộc loại này là RIPv1, RIPv2, IGRP…
- Link State: các giao thức sẽ trao đổi các gói LSA để xây dựng bảng định tuyến. Các giao thức thuộc loại này là OSPF, IS-IS…
- Hybrid: là sự kết hợp của 2 loại trên, giao thức thuộc loại này là EIGRP.

Ưu điểm của định tuyến động:

- Đường đi đến đích có tính linh hoạt khi có sự thay đổi trong kiến trúc và lưu lượng mạng.
- Phù hợp với các mạng lớn, thường xuyên có sự thay đổi trong mô hình mạng.

Nhược điểm của định tuyến động:

- Tiêu tốn tài nguyên của router để thực hiện các xử lý, tính toán các thuật toán định tuyến.
- Đòi hỏi khả năng cấu hình các giao thức của người quản trị

2. Khái niệm giao thức định tuyến động RIP

RIP (Routing Information Protocol) là giao thức cổng nội được thiết kế để sử dụng trong các hệ thống tự trị nhỏ.

RIP là giao thức định tuyến động theo vector khoảng cách, sử dụng thuật toán Bellman-Ford để xây dựng nên bảng định tuyến.

Giao thức RIP chạy trên UDP port 520. Tất cả các gói tin RIP được đóng gói trong 1 RIP segment với source port và destination port là 520.

Cơ chế hoạt động của RIP

- Khi vừa khởi động, các router RIP sẽ broadcast các gói tin Request trong mạng và lắng nghe phản hồi.
- Khi một router nhận được gói Request, nó sẽ gửi trả lại toàn bộ bảng định tuyến của nó bằng multicast.
- Sau khi nhận được bảng định tuyến
    - Nếu nó nhận được 1 route đã tồn tại trong bảng định tuyến của nó, nó sẽ xem xét chỉ số hop của route vừa nhận được, nếu chỉ số hop nhận được thấp hơn hop trong bảng định tuyến, nó sẽ cập nhật thông tin route đó vào bảng định tuyến của nó.
    - Nếu nó nhận được một route mới, nó sẽ cập nhật route đó vào bảng định tuyến của nó.

Metric của RIP (cách tính giá trị đường đi của RIP): dựa trên số lượng router mà gói tin đi qua, điều này có nghĩa rằng, đường đi tốt nhất của RIP là đường đi qua ít router nhất. Tổng số lượng router tối đa mà một gói tin được giao thức định tuyến RIP cho đi qua là 15 router. Nếu đi quá 15 router mà vẫn chưa đến đích thì gói tin sẽ bị hủy. Chính vì lý do này mà giao thức RIP không được sử dụng nhiều trong các hệ thống mạng lớn.

3. Cách thức cấu hình:

Để cấu hình 1 router chạy giao thức RIP, ta dùng lệnh router rip, tiếp theo là danh sách các mạng kết nối trực tiếp với nó.

Lưu ý: nếu như cấu hình định tuyến tĩnh là cấu hình địa chỉ mạng đích nối mà router cần đến thì cấu hình RIP là cấu hình các đường mạng nối trực tiếp với nó. Giao thức RIP sẽ dùng thông tin này để gửi đến các router khác nhằm mục đích tìm kiếm đường đi tốt nhất.

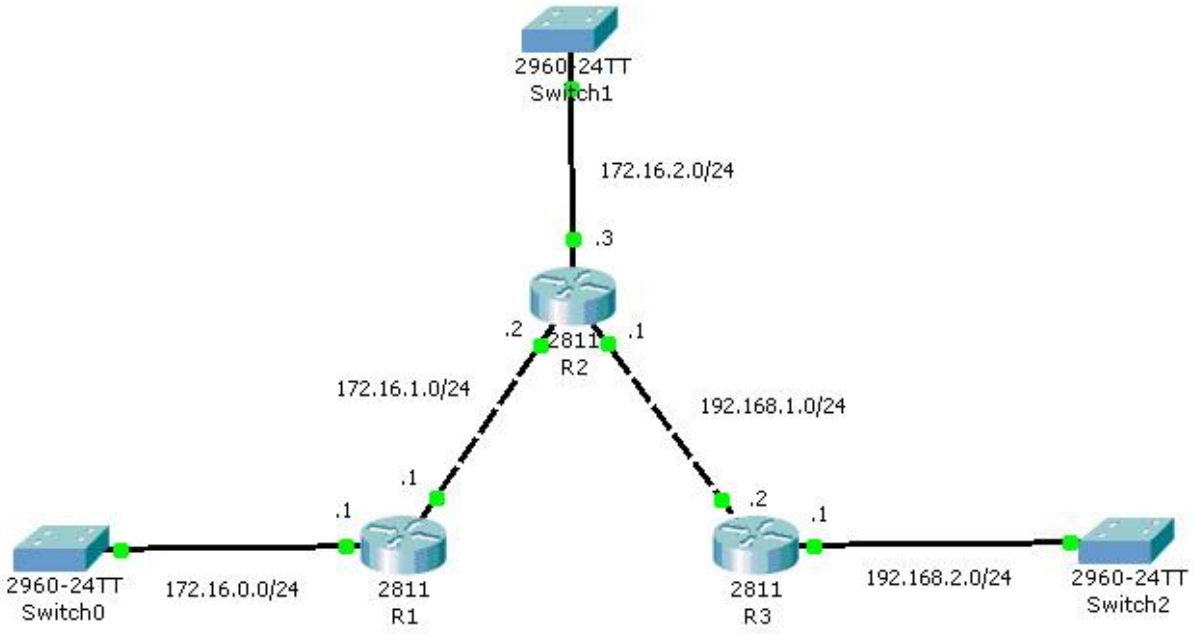
Câu lệnh:

Router(config)#router rip

Router(config-router)#network <địa chỉ các đường mạng kết nối trực tiếp>

4. Ví dụ minh họa

Giả sử ta có mô hình mạng như bên dưới.



Cấu hình trên R1:

R1(config)#router rip

R1(config-router)#network 172.16.0.0

R1(config-router)#network 172.16.1.0

Cấu hình trên R2:

R2(config)#router rip

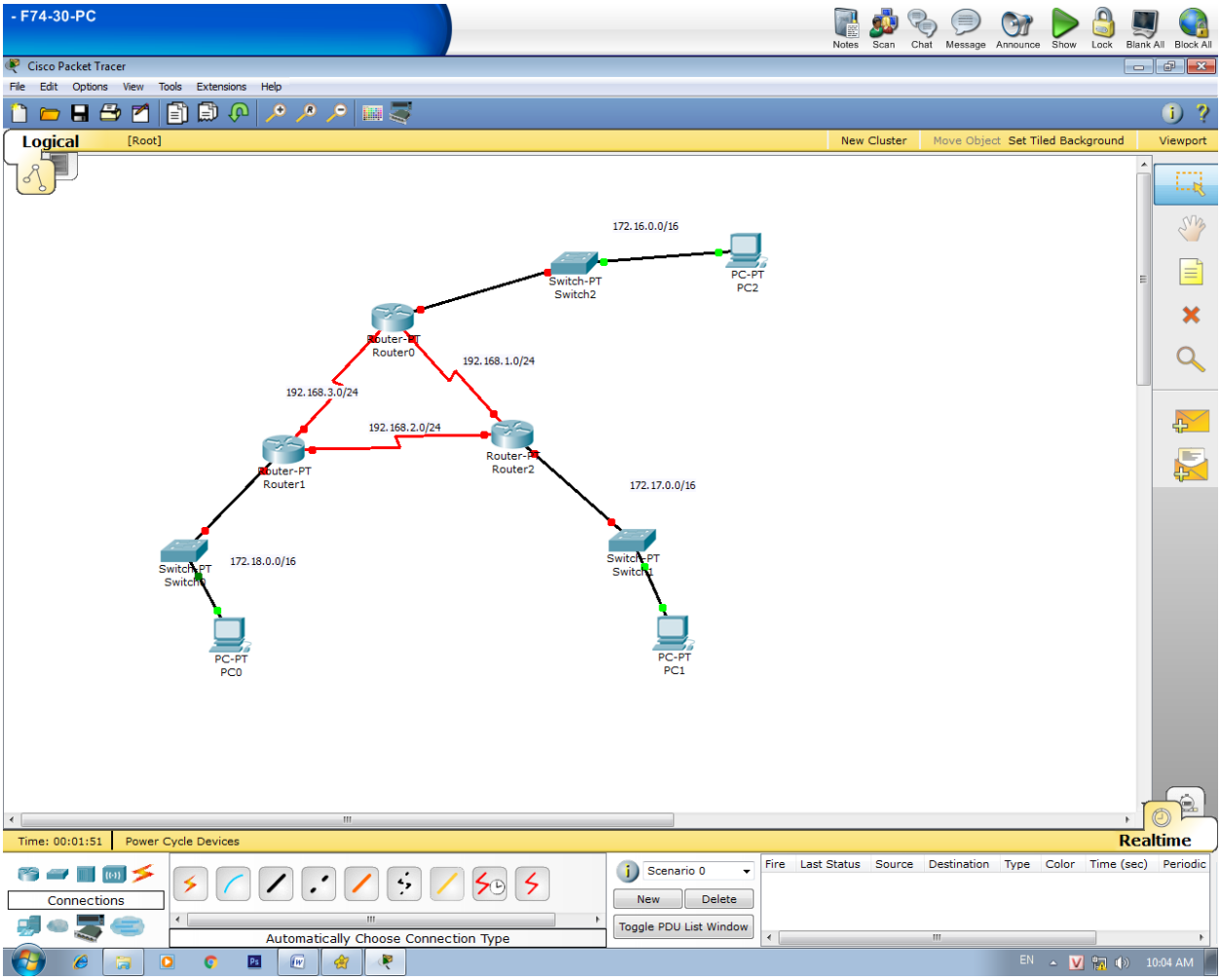
R2(config-router)#network 172.16.0.0

R2(config-router)#network 172.16.2.0
R2(config-router)#network 192.168.1.0
Cấu hình trên R3:
R3(config)#router rip
R3(config-router)#network 192.168.1.0
R3(config-router)#network 192.168.2.0

II. Bài tập thực hành:

Bài 1:

Cho mô hình sau :

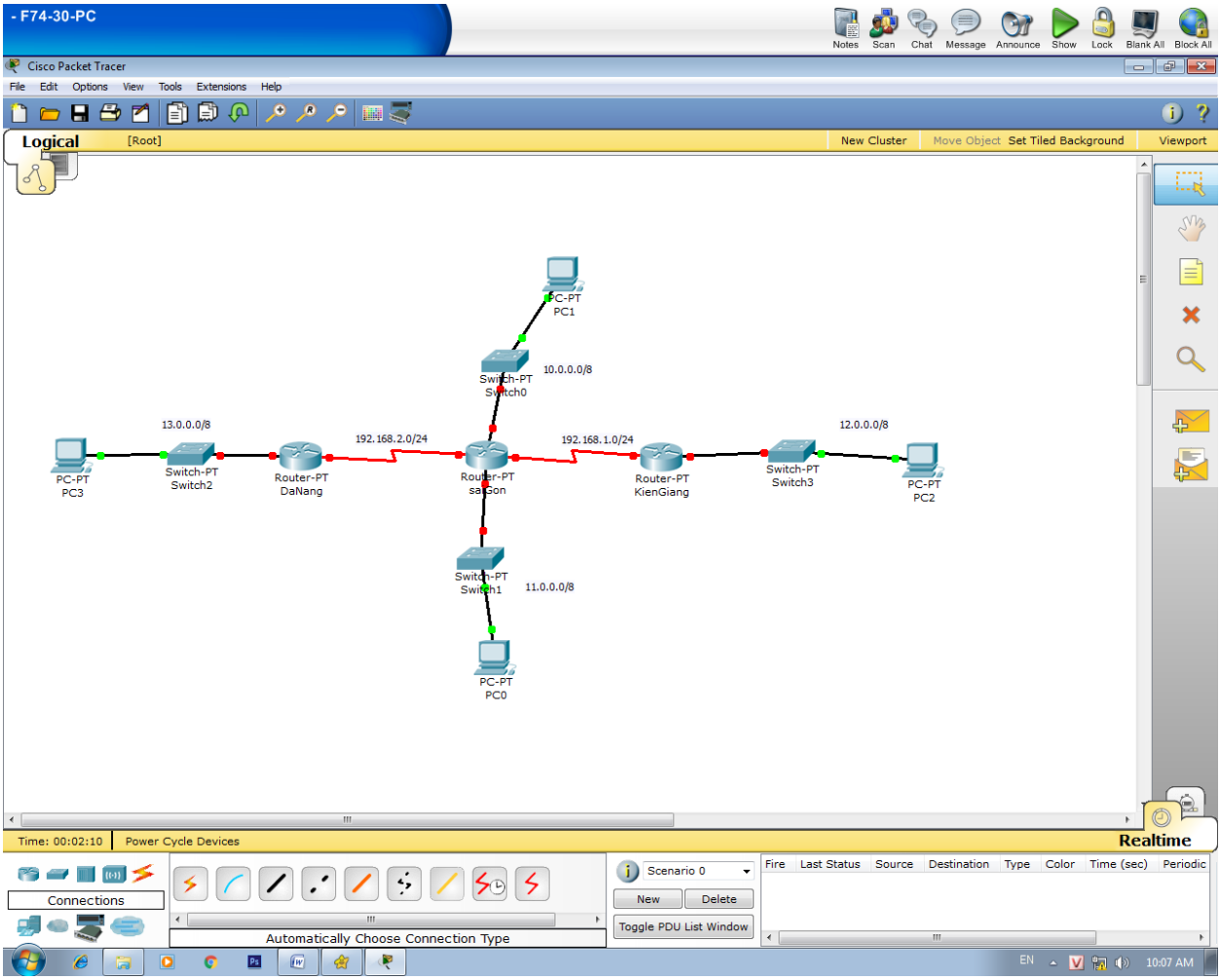


Yêu cầu:

Hãy cấu hình hoàn tất sơ đồ trên.
Dùng RIP để cấu hình định tuyến cho tất cả router trên.

Bài 2 :

Cho sơ đồ sau :

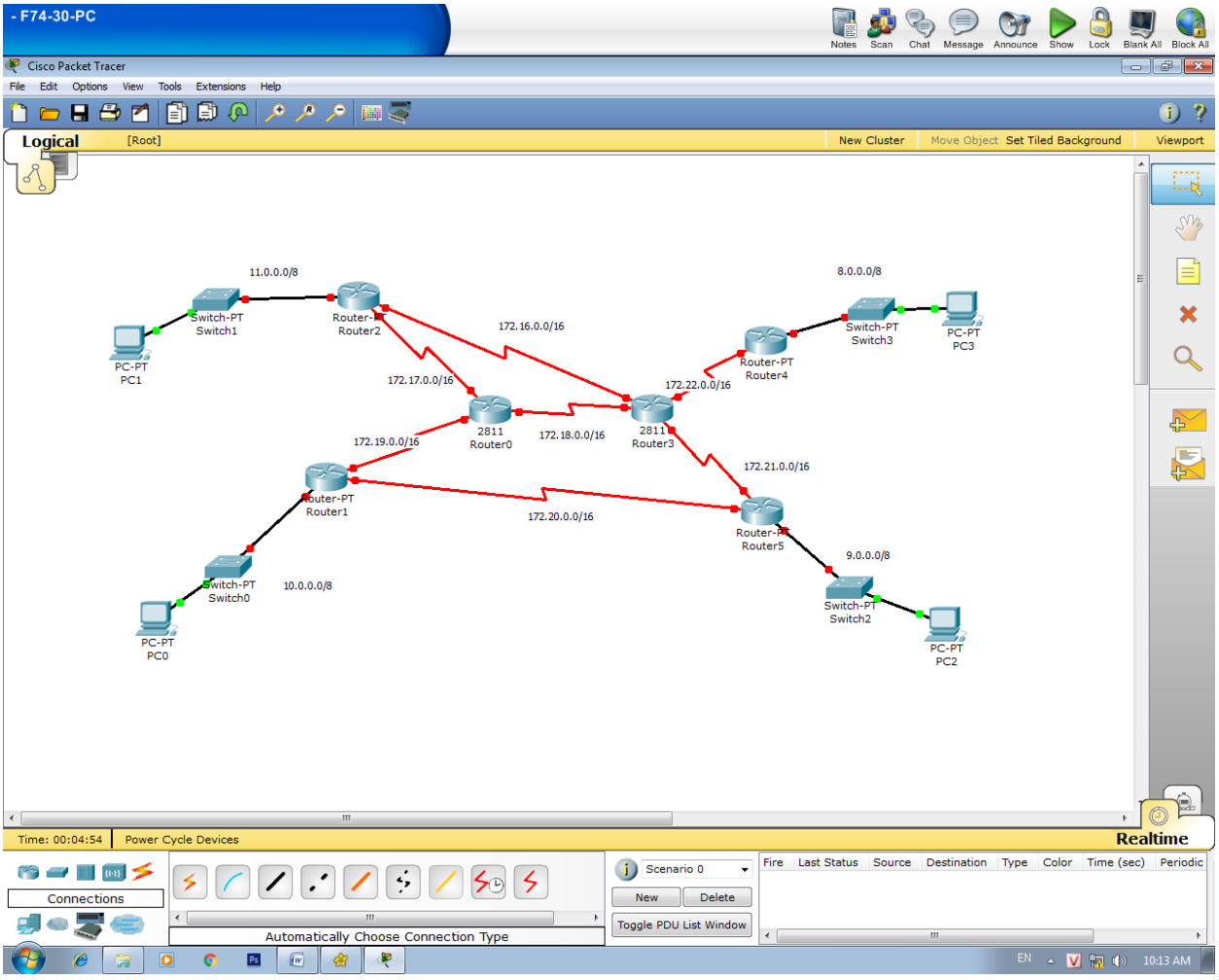


Yêu cầu:

Hãy cấu hình hoàn tất sơ đồ trên.

Dùng RIP để cấu hình định tuyến cho tất cả router trên.

Bài 3 :

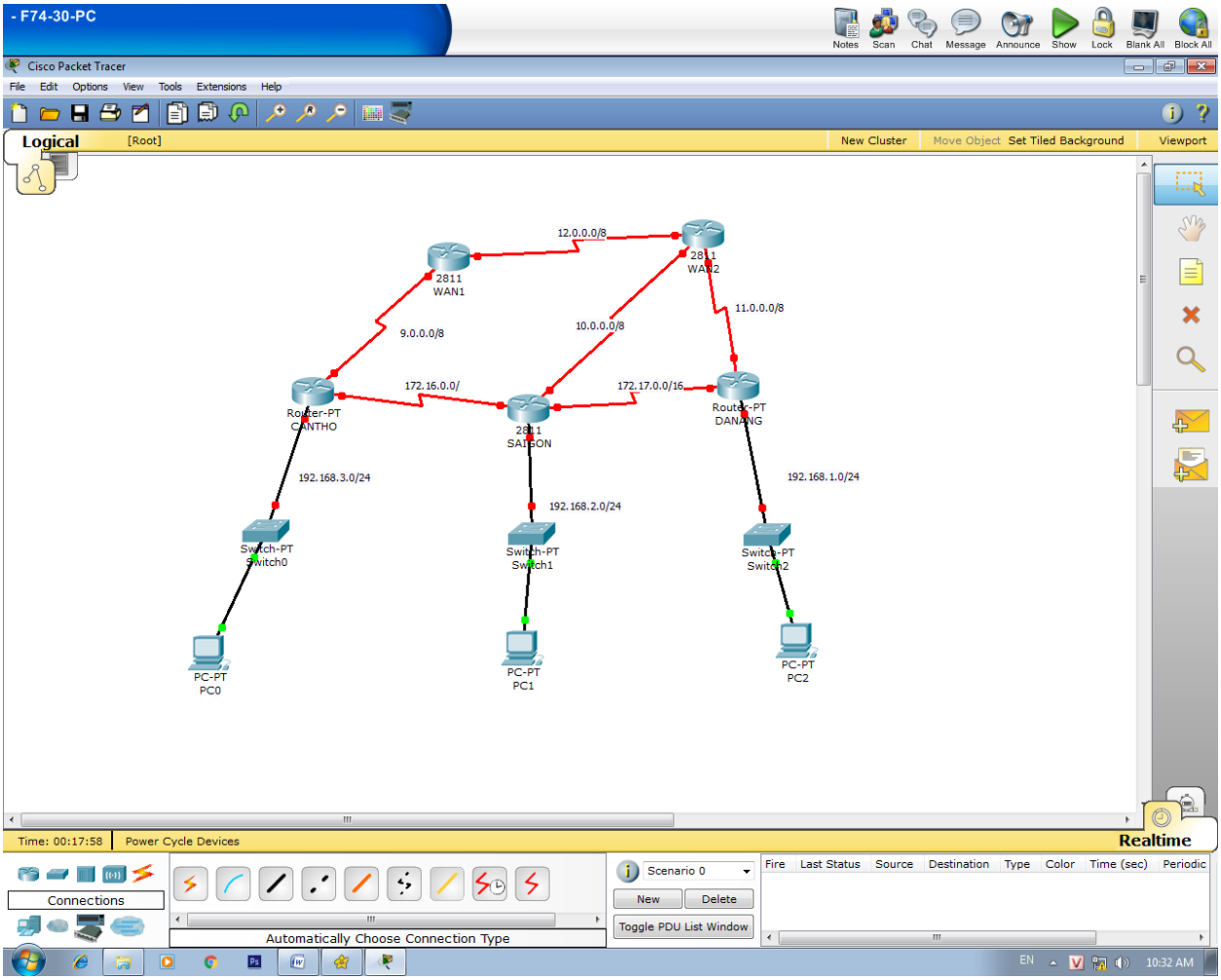


Yêu cầu:

Hãy cấu hình hoàn tất sơ đồ trên.

Dùng RIP để cấu hình định tuyến cho tất cả router trên.

Bài 4:



Yêu cầu:

Hãy cấu hình hoàn tất sơ đồ trên.

Hãy thực hiện định tuyến tĩnh theo yêu cầu sau :

- Khi lớp mạng 192.168.3.0 gửi tin qua lớp 192.168.2.0 và 192.168.1.0 bắt buộc phải đi qua lớp 172.16.0.0.
- Khi lớp mạng 192.168.2.0 gửi tin qua lớp 192.168.3.0 bắt buộc phải đi qua lớp 172.16.0.0, gửi tin qua lớp 192.168.1.0 bắt buộc phải đi qua lớp 172.17.0.0
- Khi lớp mạng 192.168.1.0 gửi tin qua lớp 192.168.2.0 và 192.168.3.0 bắt buộc phải đi qua lớp 172.17.0.0
- Từ router CANTHO, muốn đi ra các lớp khác ngoài miêu tả ở trên phải đi mặc định qua WAN1.

Hãy cấu hình định tuyến RIP cho các router trong mô hình trên.

Lưu ý: dùng câu lệnh traceroute để kiểm tra các gói tin đi theo đúng yêu cầu đặt ra ở trên.

BÀI 6: CẤU HÌNH ĐỊNH TUYẾN ĐỘNG RIP – DEFAULT ROUTE

I. Hướng dẫn thực hiện

Câu lệnh cấu hình định tuyến tĩnh:

Router(config)#ip route [network-address] [subnet-mask] [next-hop]

Với:

[network-address]: địa chỉ của mạng đích

[subnet-mask]: subnet mask của mạng đích

[next-hop]: là địa chỉ IP của cổng phải đi qua để đến mạng đích

Câu lệnh cấu hình đường mặc định:

Router(config)#ip route 0.0.0.0.0.0.0.0 [next-hop]

Trong đó:

- Địa chỉ mạng đích và subnet mask đều là 0.0.0.0 đại diện cho các đường mạng không xác định.
- [next-hop]: là địa chỉ của router kế tiếp mà gói tin sẽ đi đến.

Câu lệnh cấu hình định tuyến RIP

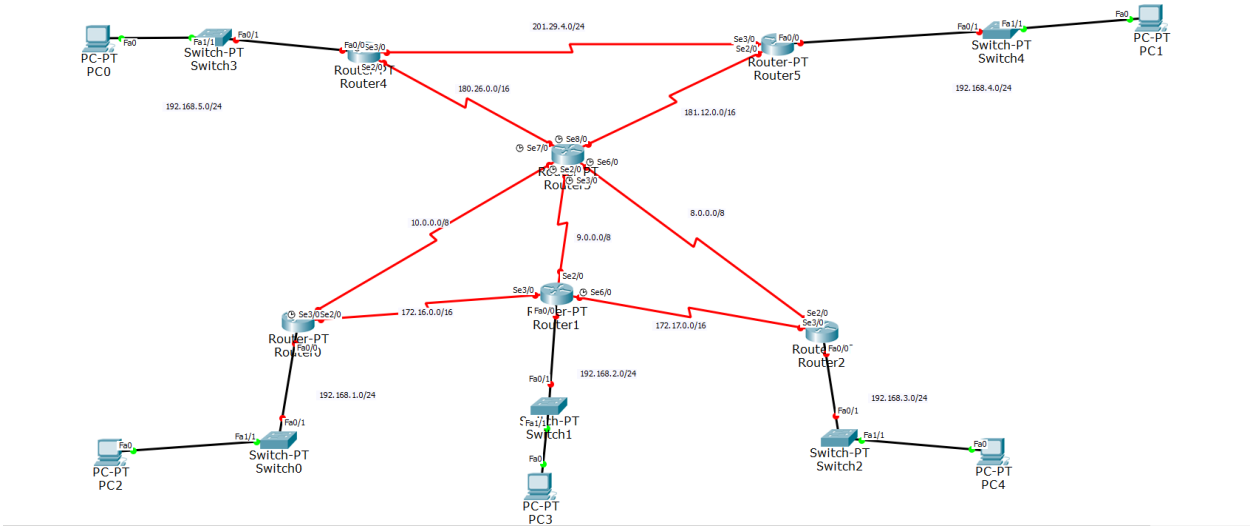
Router(config)#router rip

Router(config-router)#network <địa chỉ các đường mạng kết nối trực tiếp>

II. Bài tập thực hành:

Bài 1:

Cho mô hình sau:



Yêu cầu:

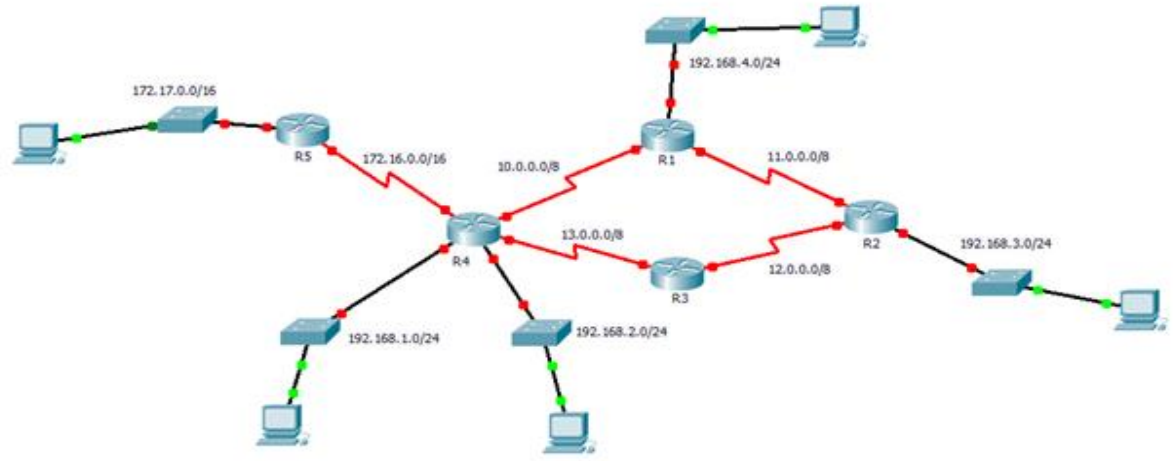
Hãy cấu hình cho router0, Router1, Router2 trỏ default route về Router3.

Cấu hình định tuyến tĩnh cho các lớp mạng 192.168.1.0/24, 192.168.2.0/24 và 192.168.3.0/24 để các tuyến đường này có thể giao tiếp với nhau.

Cấu hình định tuyến RIP cho các router.

Bài 2:

Cho mô hình:



Yêu cầu:

Cấu hình các thiết bị như mô hình trên.

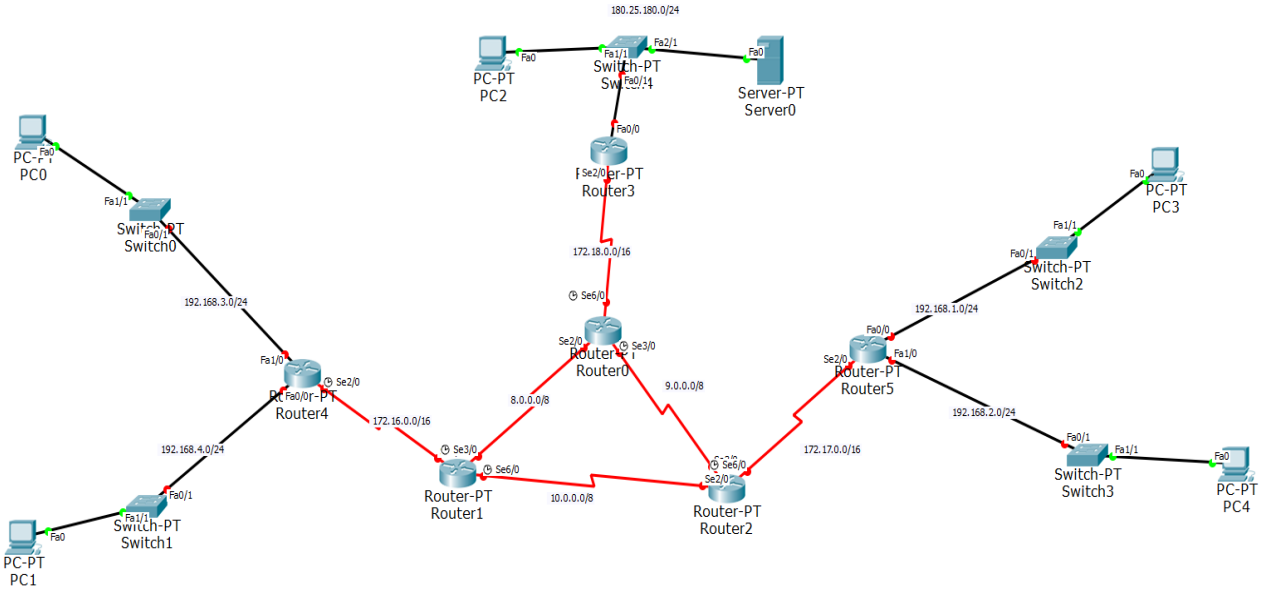
Hãy cấu hình R5 trỏ default route về R4.

Cấu hình định tuyến tĩnh từ R4 trỏ về R5.

Cấu hình RIP cho các router, trừ R5.

Bài 3:

Cho mô hình:



Yêu cầu:

Hãy cấu hình các thiết bị như trên mô hình:

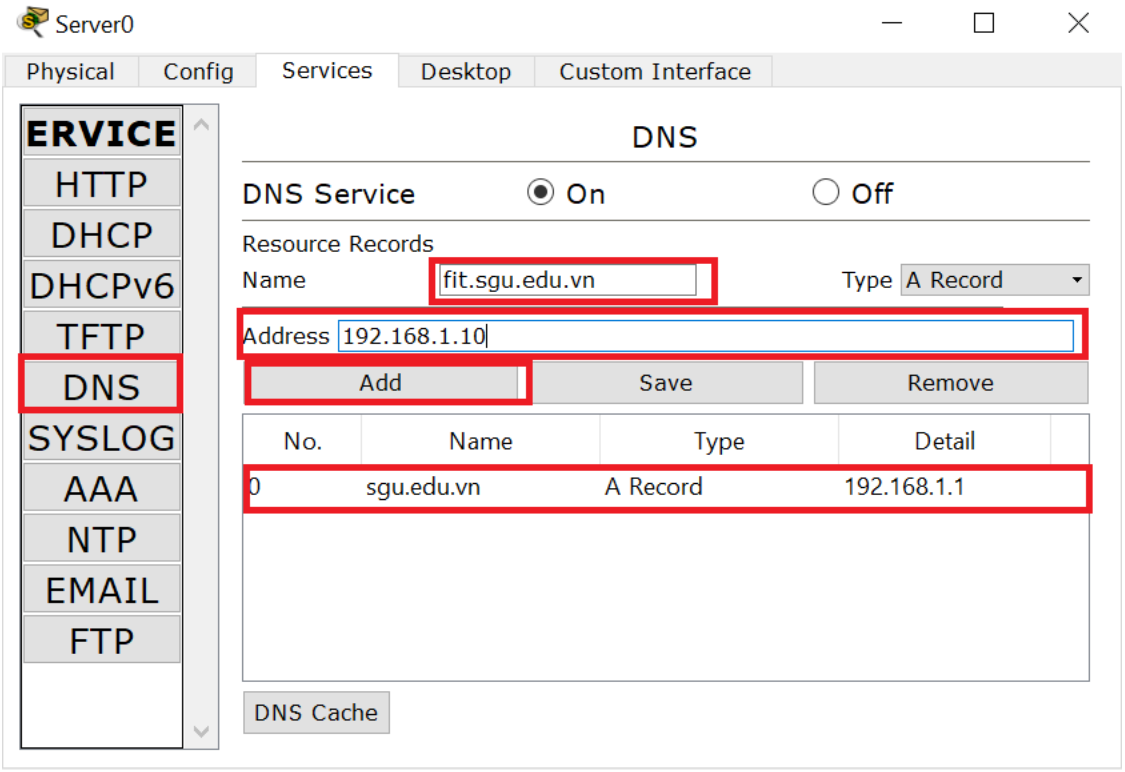
Hãy cấu hình default route cho Router3 trỏ về Router0.

Cấu hình IP route cho router0 trỏ về router3.

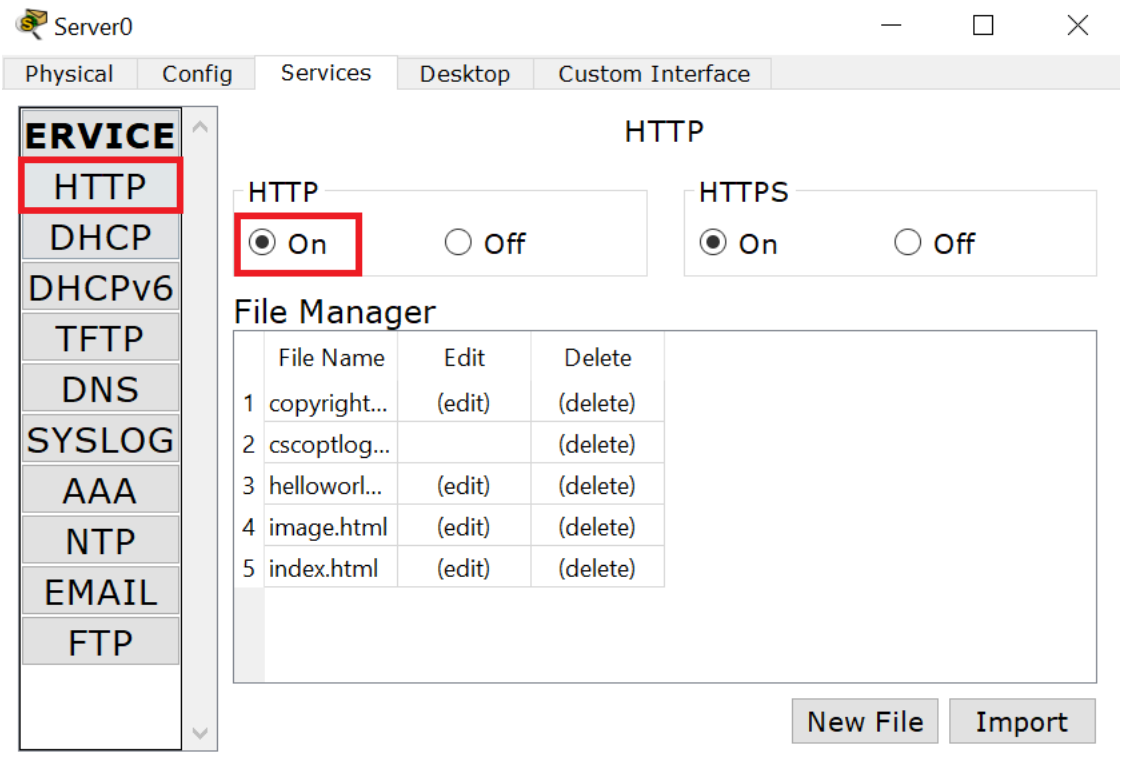
Cấu hình RIP cho các router, trừ router3.

Cấu hình Server có thể phân giải DNS và làm web server.

Lưu ý: để cấu hình server, ta chọn server và chọn service, để cấu hình DNS, ta chọn như hình bên dưới:



Ta chọn tên miền và địa chỉ tương ứng, sau khi nhấn nút add, ta sẽ có địa chỉ IP tương ứng với tên domain.
Đối với việc cấu hình web server, ta chọn services, nhấn chọn HTTP, chọn on.


Server0
Physical
Config
Services
Desktop
Custom Interface
ERVICE
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
HTTP
HTTP
On
Off
HTTPS
On
Off
File Manager
File Name
Edit
Delete
1 copyright... (edit) (delete)
2 cscoptlog... (delete)
3 helloworl... (edit) (delete)
4 image.html (edit) (delete)
5 index.html (edit) (delete)
New File
Import

BÀI 7: CẤU HÌNH ĐỊNH TUYẾN ĐỘNG OSPF

I. Hướng dẫn thực hiện

1. Khái niệm giao thức định tuyến động OSPF

Giao thức OSPF (Open Shortest Path First) được phát triển bởi tổ chức Internet Engineering Task Force (IETF) để thay thế giao thức RIP.

Đây là giao thức dựa trên thuật toán link-state, triển khai dựa trên các chuẩn mở.

Phiên bản 2 của giao thức này đã được đặc tả trong RFC 2328 vào năm 1998, dành cho IPv4.

Phiên bản 3 dành cho Ipv6 được đặc tả trong RFC 5340 vào năm 2008, dành cho IPv6.

OSPF có khả năng mở rộng cao và không bị giới hạn 15 hop count như RIP.

Các đặc điểm của giao thức OSPF:

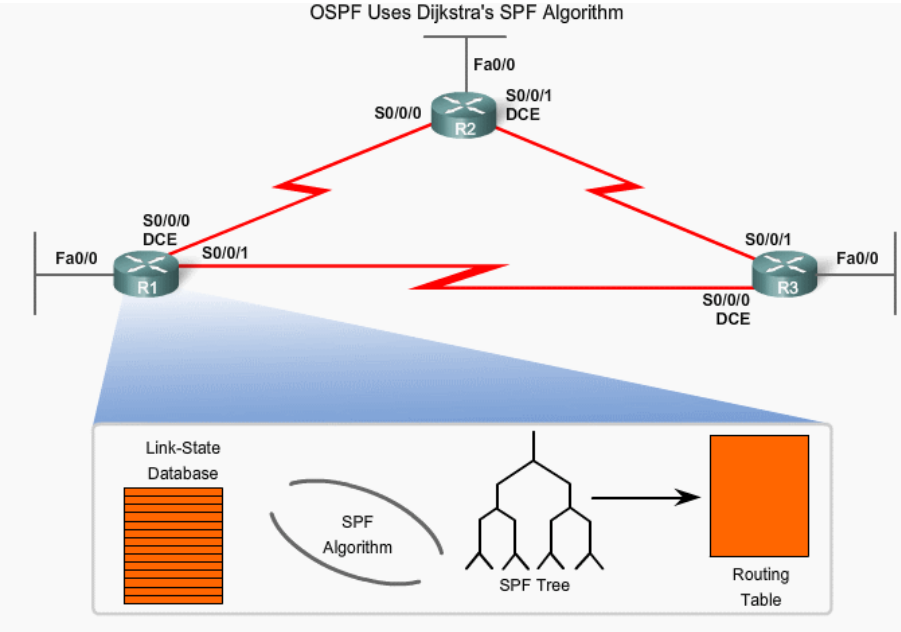
- Tốc độ hội tụ nhanh: Với giao thức OSPF thì thời gian hội tụ nhanh hơn vì nó chỉ gửi đi các thay đổi về topo mạng, giao thức RIP cần đến vài phút để hội tụ vì toàn bộ bảng định tuyến đến các router kết nối với nó.
- Hỗ trợ mặt nạ mạng con VLSM (Variable length subnet mask).
- Hỗ trợ các mạng có kích thước lớn: với giao thức RIP, nếu 1 mạng nằm cách xa quá 15 router thì sẽ không thể đến được. Đều này làm cho mạng sử dụng RIP có kích thước nhỏ. Với OSPF thì kích thước của mạng không bị hạn chế.
- Đường đi hiệu quả, linh hoạt: OSPF chọn đường đi dựa vào chỉ số COST, đây là metric dựa trên băng thông đường truyền.
- Hỗ trợ xác thực
- Tiết kiệm được băng thông: Cứ định kỳ 30 giây, RIP sẽ quảng bá toàn bộ bảng định tuyến tới tất cả hàng xóm. Điều này sẽ chiếm dụng băng thông của đường truyền 1 cách vô ích nếu như trong mạng không có bất kì sự thay đổi nào. Trong khi đó, OSPF phát multicast một cập nhật định tuyến có kích thuớc tối thiểu và chỉ gửi cập nhật khi có thay đổi về tôpô mạng.

Cơ chế hoạt động của OSPF:

OSPF có thể hoạt động trong vòng 6 bước như sau:

- Bước 1: Các OSPF router sẽ gửi các gói tin Hello ra tất cả các OSPF router khác trong mạng. Nếu 2 router sau khi trao đổi gói Hello và thoả thuận một số thông số chúng sẽ trở thành hàng xóm. Đồng thời thông qua gói tin Hello, OSPF cũng sẽ bầu ra DR và BDR nếu như đây là mạng quảng bá.
- Bước 2: Hình thành mối quan hệ tin cậy (Adjacency) với một vài router hàng xóm hoặc với DR. OSPF định nghĩa ra một số loại network và một số loại router. Sự thiết lập một adjacency được xác định bởi loại router trao đổi Hello và loại network mà Hello trao đổi qua.
- Bước 3: Mỗi router gửi các LSA (Link State Advertisement) để mô tả trạng thái kết nối qua tất cả adjacency. Có rất nhiều loại thông tin cho nên OSPF cũng định nghĩa nhiều loại LSA

- Bước 4: Khi 1 router nhận một LSA từ router hàng xóm, nó sẽ cập nhật vào link state database và gửi một copy của LSA tới tất cả router hàng xóm khác của nó
- Bước 5: Bằng cách gửi tràn ngập các LSA ra toàn bộ các router trong một area, tất cả router sẽ xây dựng chính xác link state database.
- Bước 6: Khi database được hoàn tất, mỗi router sử dụng thuật toán Dijkstra's Shortest Path First (SPF) để xây dựng nên SPF tree



Metric của OSPF (cách tính giá trị đường đi tốt nhất của OSPF):
Giá trị cơ sở để giao thức OSPF lựa chọn đường đi là COST. Giá trị COST càng nhỏ thì càng tốt và được tính theo công thức:

108/ bandwidth

Băng thông mặc định là 108 Mbps, giá trị này có thể thay đổi nhờ lệnh

Auto-cost reference-bandwidth

COST của 1 tuyến đường là giá trị tích lũy từ 1 router đến router kế tiếp cho tới khi đến đích.
Do đã khắc phục được tình trạng gói tin chỉ di chuyển qua 15 router của giao thức RIP, nên giao thức OSPF thường được cấu hình trong hệ thống mạng lớn.

2. Cách thức cấu hình:

Để cấu hình được giao thức OSPF, ta cũng phải đảm bảo các router đã cấu hình xong IP cho các interfaces, và đảm bảo các router giao tiếp trực tiếp với nhau phải kết nối được. Câu lệnh cấu hình OSPF như sau.
Để cấu hình một router sử dụng giao thức OSPF, ta dùng lệnh:
Router(config)#router ospf process_id

- *Process_id* là một chỉ số cục bộ trên router.

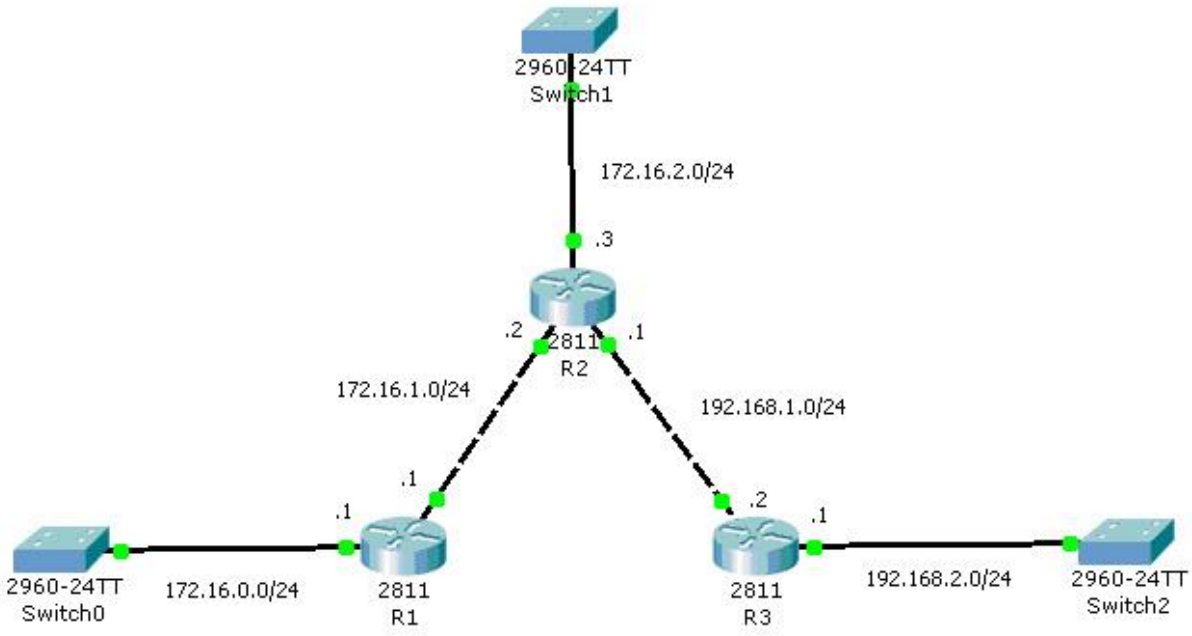
Sau đó liệt kê các mạng kết nối với nó.

Router(config-config)#network major_network wildcard area area_id

- *Area_id* là chỉ số dùng để nhóm các router vào cùng một area, các router này cùng chia sẻ hiểu biết về các đường học được trong miền OSPF .

3. Ví dụ minh họa:

Giả sử ta có sơ đồ mạng như sau:



Ta sẽ tiến hành cấu hình giao thức OSPF với process_id trên các router là 1, area_id là 100

Trên R1:

R1(config)#router ospf 1

R1(config-router)#network 172.16.0.0 0.0.0.255 area 100

R1(config-router)#network 172.16.1.0 0.0.0.255 area 100

Trên R2:

R2(config)#router ospf 1

R2(config-router)#network 172.16.1.0 0.0.0.255 area 100

R2(config-router)#network 172.16.2.0 0.0.0.255 area 100

R2(config-router)#network 192.168.1.0 0.0.0.255 area 100

Trên R3:

R3(config-if)#router ospf 1

R3(config-router)#network 192.168.1.0 0.0.0.255 area 100

R3(config-router)#network 192.168.2.0 0.0.0.255 area 100

Trong tình huống cấu hình trên, ta lưu ý rằng, các địa chỉ mạng liệt kê là những địa chỉ mạng kết nối trực tiếp với router.

Giá trị wildcast được tính bằng cách: 255.255.255.255 – subnetmask. Ví dụ: subnet mask của lớp mạng 192.168.1.0 là 255.255.255.0, do đó, 255.255.255.255 – 255.255.255.0 ta sẽ có: 0.0.0.255.

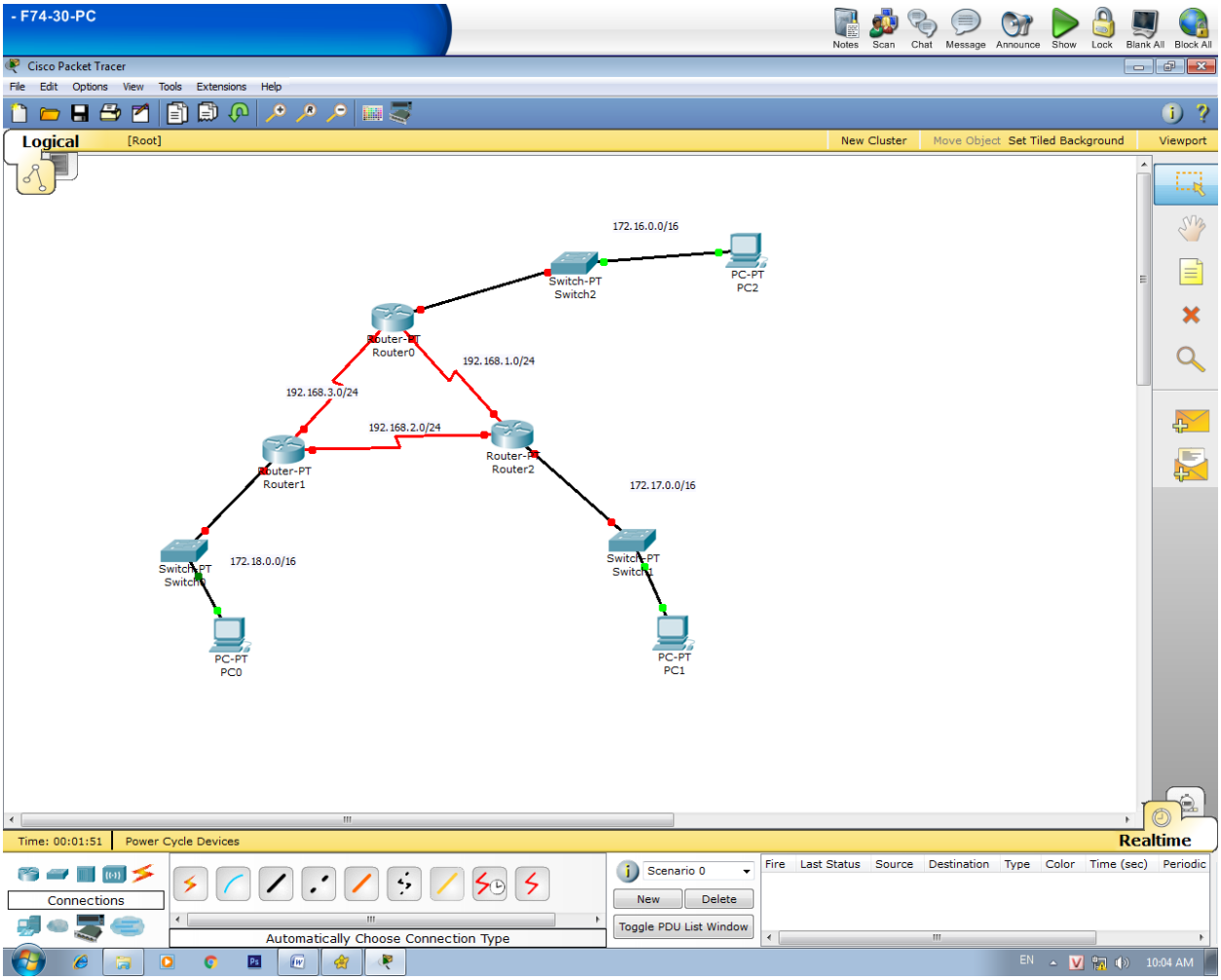
Các router muốn trao đổi thông tin định tuyến với nhau phải có chung 1 area. Nếu khác area các router sẽ không thể trao đổi gói tin định tuyến với nhau được.

Chỉ số process id của các router có thể giống, hoặc cũng có thể khác. Điều này chỉ ảnh hưởng khi chúng ta thực hiện redistribute cho các router trên area khác nhau (sẽ được trình bày trong bài sau).

II. Bài tập thực hành:

Bài 1 :

Cho mô hình sau :



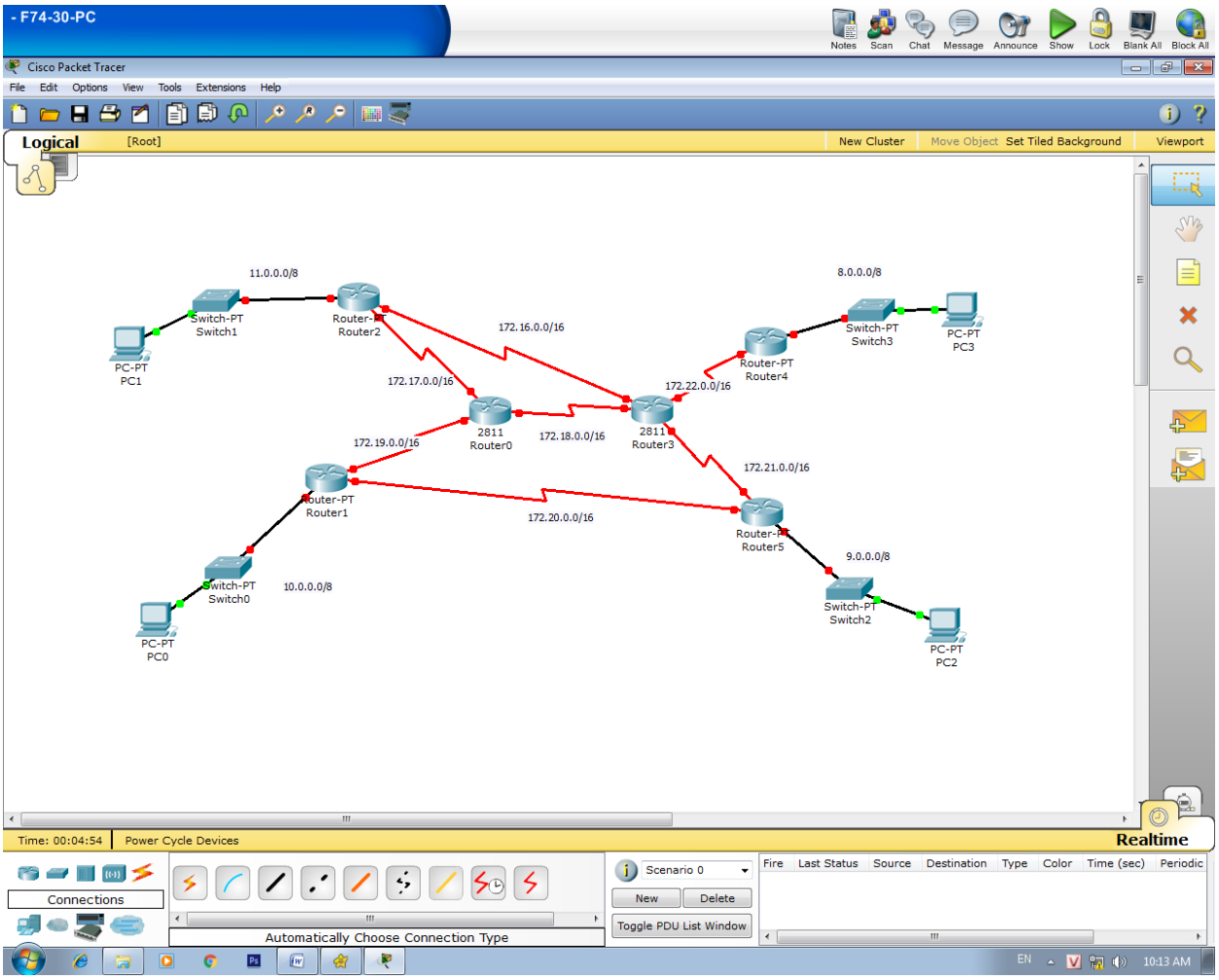
Yêu cầu:

Hãy cấu hình các thiết bị như mô hình trên.

Dùng OSPF để cấu hình định tuyến cho tất cả router trên với process id là 1 và area là 100.

Bài 2:

Cho mô hình như sau:

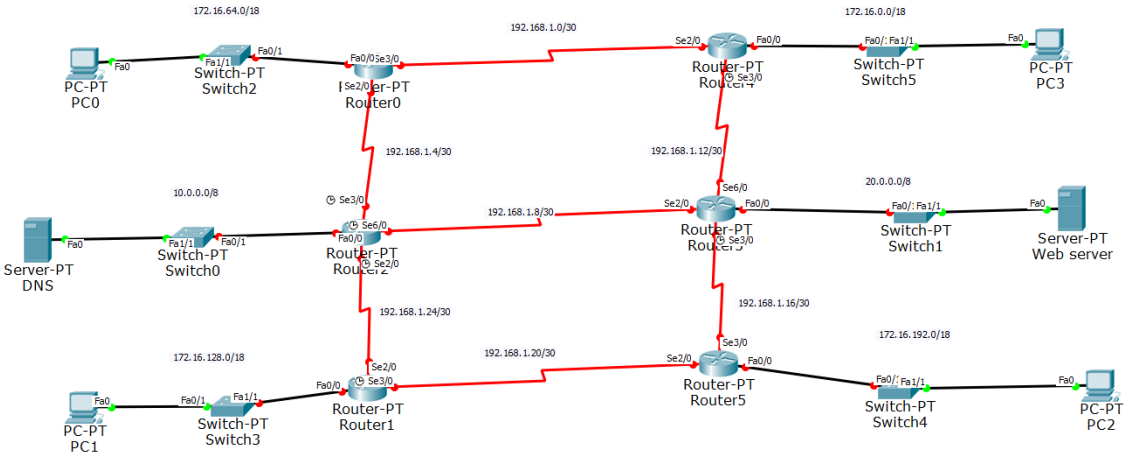


Yêu cầu:

Hãy cấu hình các thiết bị như mô hình trên.

Dùng OSPF để cấu hình định tuyến cho tất cả router trên với process id là 1 và area là 100.

Bài 3:



Yêu cầu:

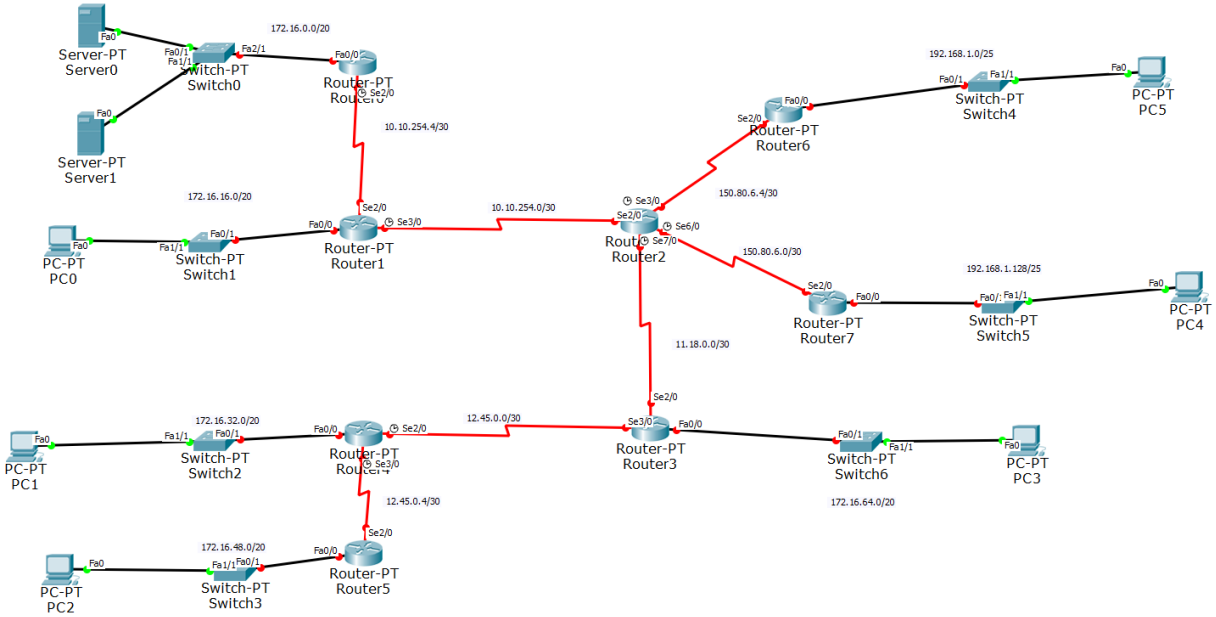
Hãy cấu hình hoàn tất các thiết bị như mô hình trên.

Hãy cấu hình định tuyến với OSPF cho các router trên. Cấu hình DSN với tên miền là it.com và trỏ về web server để truy cập website.

Lưu ý: hãy tự lựa chọn process id và area cho giao thức OSPF.

Bài 4:

Cho sơ đồ sau:



Yêu cầu:

Hãy cấu hình định tuyến với OSPF để các thiết bị giao tiếp với nhau (process id và area tùy chọn). Hãy cấu hình cho các server để các máy có thể gửi thư cho nhau.

BÀI 8: CẤU HÌNH ĐỊNH TUYẾN ĐỘNG OSPF ĐA VÙNG

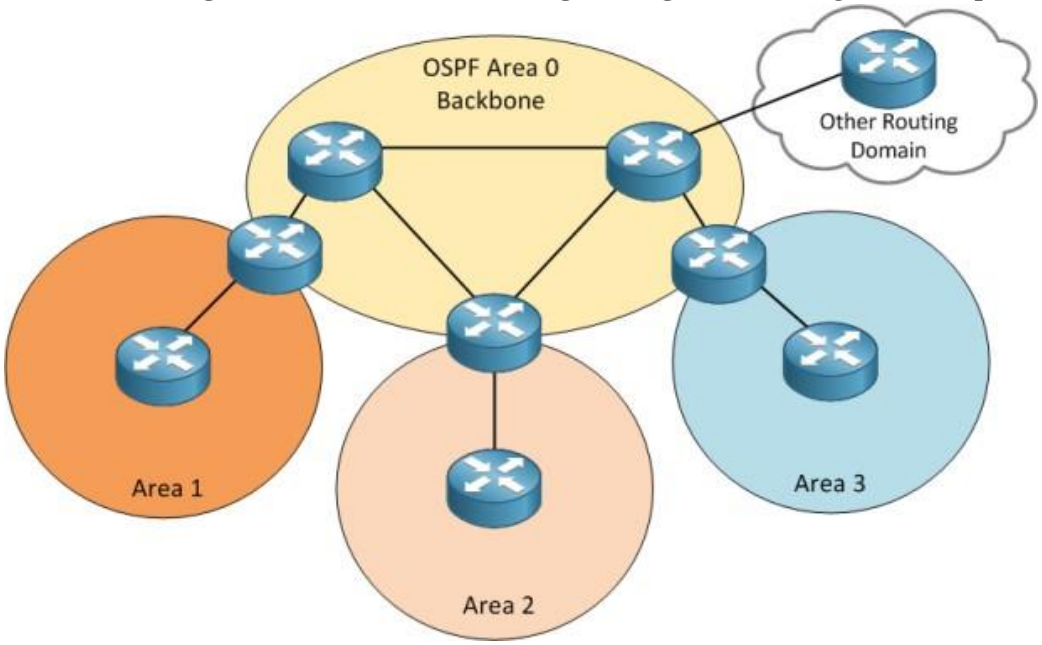
I. Hướng dẫn thực hiện

1. Khái niệm OSPF đa vùng

Khi quy mô hệ thống mạng nhỏ, ta có thể cấu hình OSPF đơn vùng (single area) để có thể đơn giản hóa việc quản trị. Tuy nghiên, khi kích thước mạng lớn hoặc trong môi trường mạng thường xuyên có sự thay đổi, việc sử dụng OSPF đơn vùng sẽ nảy sinh các nhược điểm sau:

- Kích thước bảng định tuyến trên mỗi Router lớn khi mạng lớn.
- Cơ sở dữ liệu về cấu trúc toàn mạng của mỗi Router cũng vì thế phình to ra.
- Các Router phải gồng mình thực hiện nhiều lần tính toán đường đi tốt nhất bằng thuật toán SPF gây tiêu tốn tài nguyên bộ nhớ và tài nguyên xử lý.

Để giải quyết hạn chế của OSPF đơn vùng, người ta chia mạng lớn thành các phần nhỏ hơn gọi là các Area, đây gọi là kiến trúc phân cấp OSPF. Nó cho phép Router trong mỗi vùng duy trì cơ sở dữ liệu riêng của vùng đó và tóm lược cơ sở dữ liệu của các vùng khác. Đảm bảo được tính kết nối giữa các Area và các mạng bên ngoài hệ thống là độc lập với nhau.



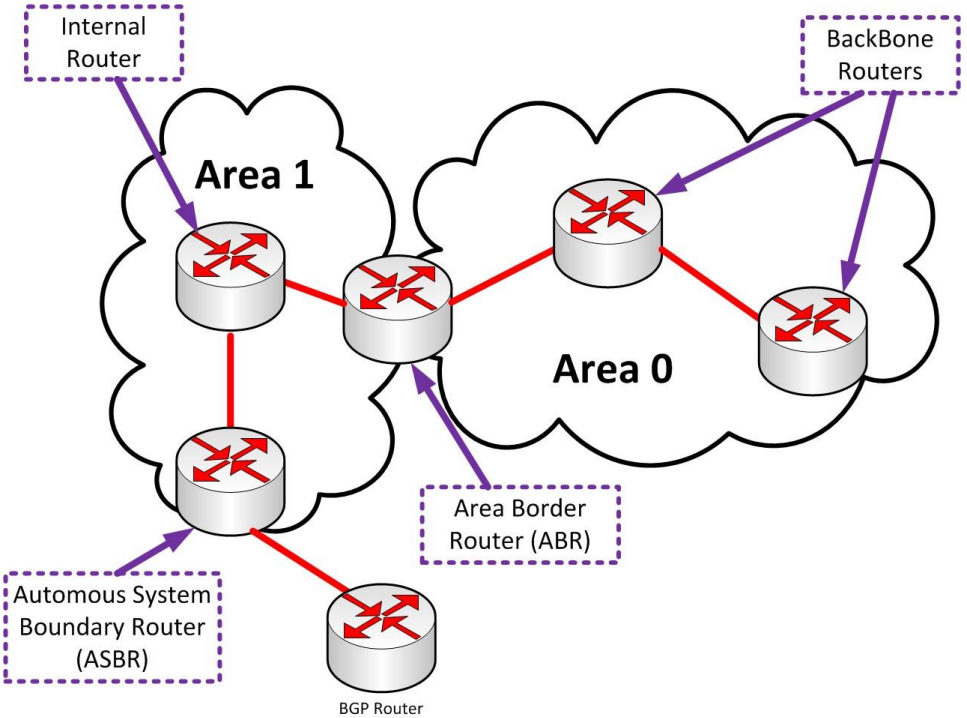
Lợi ích của việc sử dụng OSPF đa vùng:

- Các Router bên trong một Area chỉ cần quan tâm đến Link-State Database của Area chứa nó, không cần quan tâm đến toàn mạng. Giảm chi phí bộ nhớ.
- Bảng định tuyến của Router biên sẽ ngắn gọn hơn vì ta có thể tóm tắt (sumary) các địa chỉ mạng theo khu vực.
- Giảm tần suất sử dụng thuật toán SPF. Các Router trong một Area chỉ phải tính toán lại khi có sự thay đổi của mạng bên trong Area của chúng khi có sự thay đổi.
- Các Router chỉ gửi các gói Link-State Update cho các Router khác trong vùng của nó khi có sự thay đổi. Giảm các gói LSU trên toàn mạng.

Phân loại các loại router trong OSPF

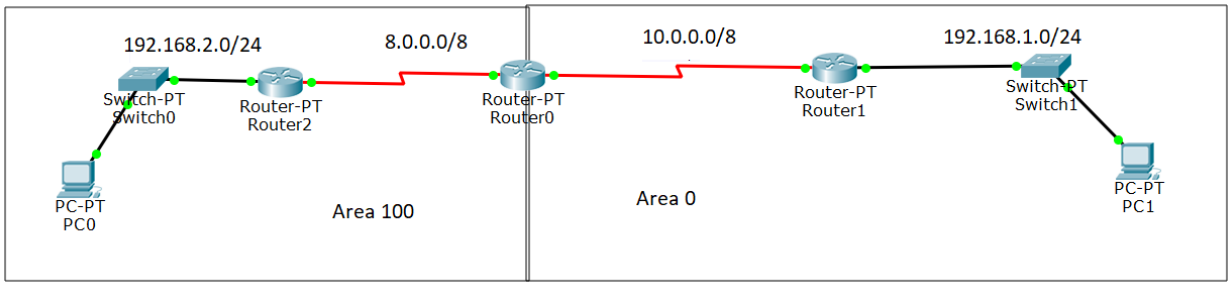
Các router trong OSPF được phân thành 4 loại router sau:

- Internal Routers (IRs): Hay còn gọi là Router nội vùng, là các Router kết nối trực tiếp với nhau thuộc cùng một Area của OSPF. Loại Router này chỉ có một Link-State Database do nó chỉ thuộc về một Area.
- Area Border Routers (ABRs): Còn gọi là Router biên, là các Router kết nối đến nhiều Area của OSPF. Trong một mạng có thể có nhiều Router biên. Bởi vì nằm giữa các Area nên nó có nhiều Link-State Database. Với mỗi Area mà Router biên kết nối đến, Router biên sẽ có 1 database về mạng đó (đã được tóm tắt) để gửi về Backbone-Area và phân phối tới các Area khác. Router biên nằm giữa một hoặc nhiều Area và kết nối trực tiếp đến Backbone-Area cũng được xem là thành viên của Backbone-Area và là thành viên của Area mà nó kết nối đến. Nói cách khác, một Router nếu muốn trở thành Router biên phải kết nối trực tiếp đến Backbone-Area và là thành viên của Area khác.
- Autonomous System Boundary Routers (ASBRs): Là Router kết nối đến một hoặc nhiều AS khác, hoặc kết nối với các mạng khác có giao thức định tuyến khác không phải OSPF.
- Backbone Routers (BRs): Là Router chỉ thuộc Backbone-Area, không kết nối với Area khác.



2. Cách thức cấu hình:

Giả sử ta có mô hình như sau:



Trong mô hình trên, router0 và router2 thuộc về định tuyến OSPF sử dụng area 100. Router0 và router1 thuộc về định tuyến OSPF sử dụng area 0.

Area 0 là đường backbone, mọi khu vực để có thể giao tiếp với nhau phải thông qua đường backbone này. Có nghĩa là phải kết nối về Area 0.

Giả sử rằng, địa chỉ IP trên các router đã cấu hình hoàn tất. Giờ ta sẽ thực hiện cấu hình OSPF đa phân vùng cho mô hình trên.

Trên Router2

Router2(config)#router ospf 1
Router2(config-router)#network 192.168.2.0 0.0.0.255 area 100
Router2(config-router)#network 8.0.0.0 0.255.255.255 area 100

Trên Router0

Router0(config)#router ospf 1
Router0(config-router)#network 8.0.0.0 0.255.255.255 area 100
Router0(config-router)#network 10.0.0.0 0.255.255.255 area 0

Trên Router1

Router1(config)#router ospf 1
Router1(config-router)#network 192.168.1.0 0.0.0.255 area 0
Router1(config-router)#network 10.0.0.0 0.255.255.255 area 0

Như vậy, ta cấu hình cho các interface theo đúng area như mô hình.

Sau khi thực hiện xong, các gói tin đã có thể giao tiếp xuyên qua các khu vực nhờ kết nối đến đường backbone.

```
Router#sho ip rou
Router#sho ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    8.0.0.0/8 is directly connected, Serial2/0
O IA 10.0.0.0/8 [110/128] via 8.0.0.2, 00:00:47, Serial2/0
O IA 192.168.1.0/24 [110/129] via 8.0.0.2, 00:00:22, Serial2/0
C    192.168.2.0/24 is directly connected, FastEthernet0/0
Router#
```

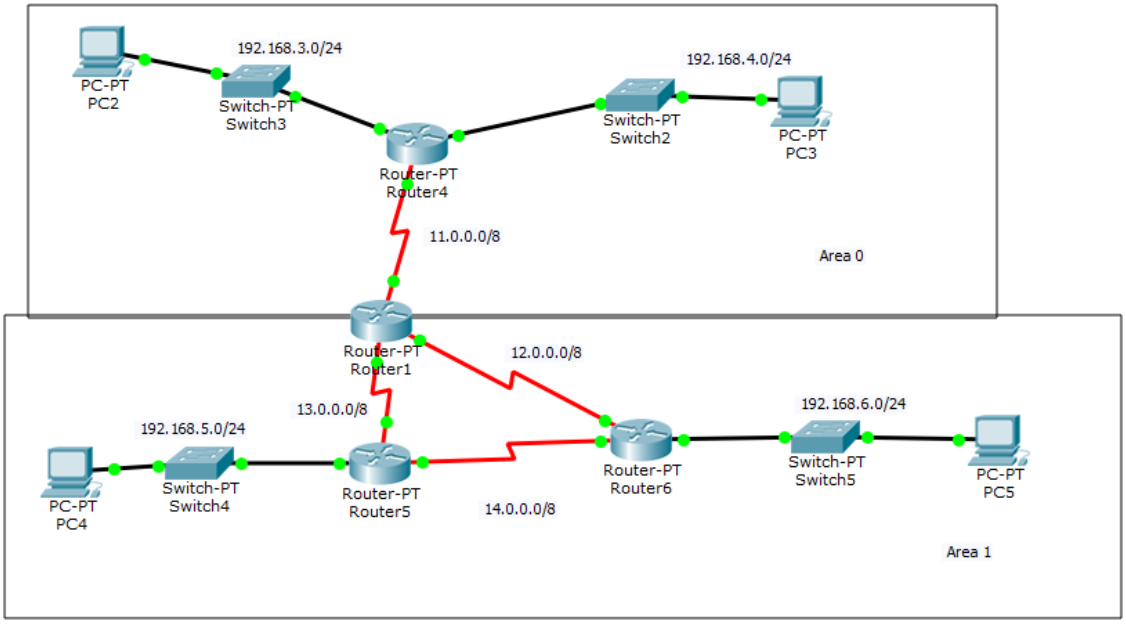
Kết quả khi show ip route trên router2

Ta thấy trong kết quả khi show ip route của router2 ở hình trên, ta thấy đường 192.168.1.0/24 và 10.0.0.0/8 thuộc về area 0. Do đó, bảng định tuyến có thêm thông tin IA. Đến đây, các gói tin trên router khác area có thể liên lạc với nhau thông qua cấu hình kết nối đến backbone.

II. Bài tập thực hành:

Bài 1:

Cho mô hình sau:



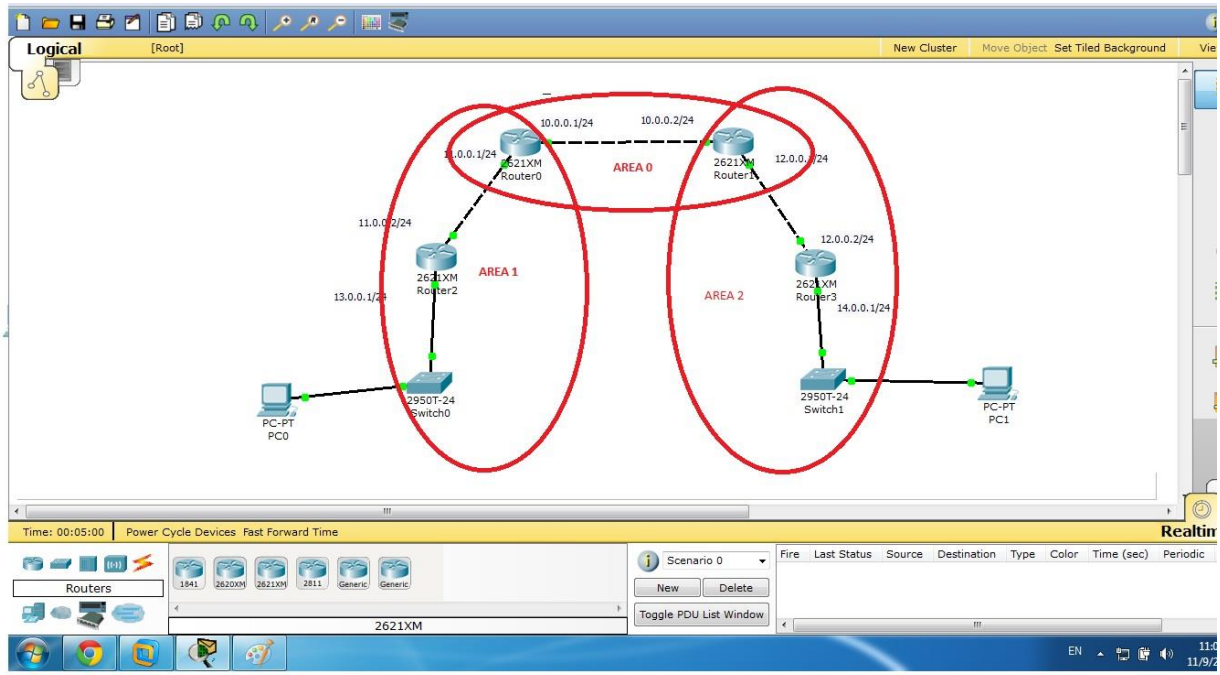
Yêu cầu:

Hãy cấu hình các thiết bị hoàn chỉnh theo mô hình trên.

Dùng OSPF để thực hiện cấu hình các area như trong sơ đồ.

Bài 2:

Cho mô hình sau:



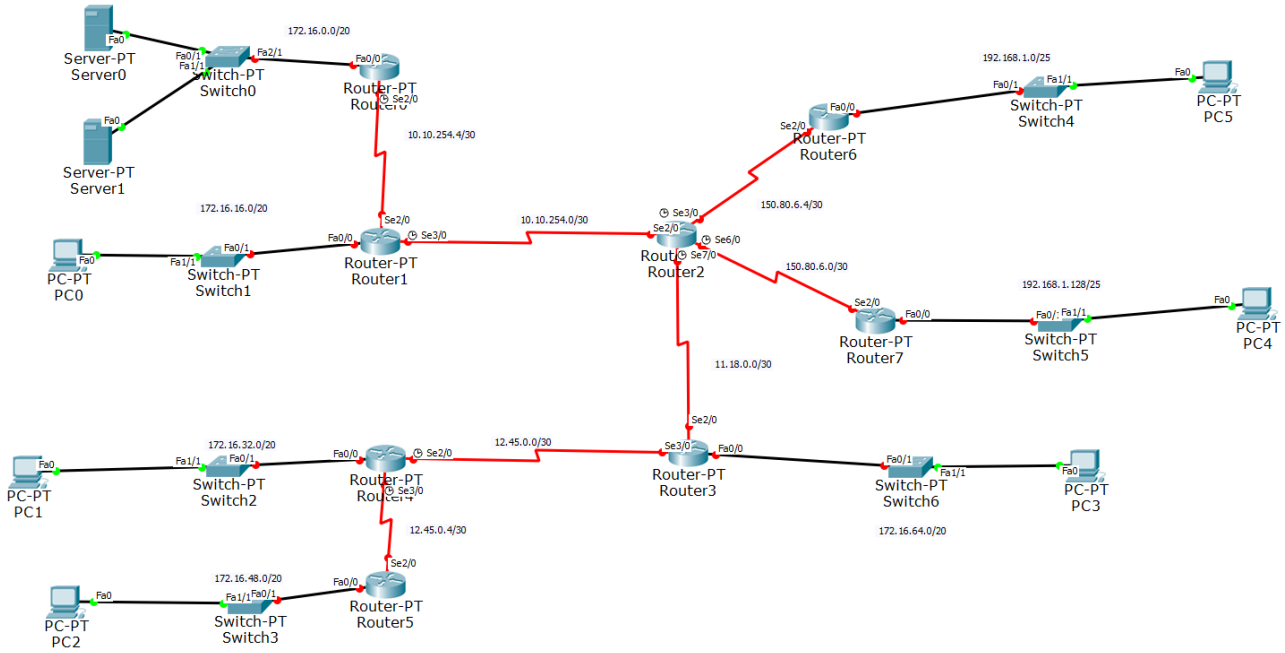
Yêu cầu:

Hãy cấu hình các thiết bị hoàn chỉnh theo mô hình trên.

Dùng OSPF để thực hiện cấu hình các area như trong sơ đồ.

Bài 3:

Cho mô hình sau:



Yêu cầu:

Hãy cấu hình định tuyến với OSPF để các thiết bị giao tiếp với nhau. Hãy cấu hình cho các server để các máy có thể gửi thư cho nhau.

Lưu ý: căn cứ theo mô hình tự phân chia vùng area để phân nhỏ lớp mạng ra nhằm dể quản lý.

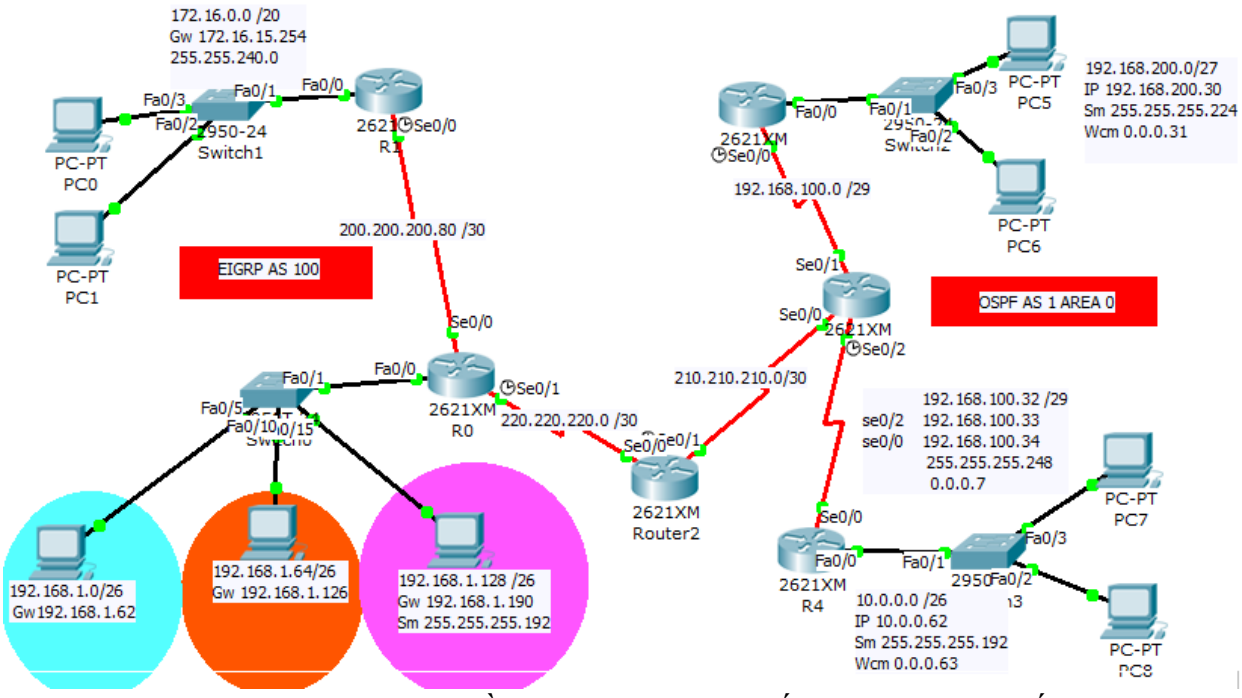
BÀI 9: REDISTRIBUTE OSPF – RIP – STATIC ROUTE

I. Hướng dẫn thực hiện

1. Giới thiệu Redistribute

Trên thực tế, đối với các hệ thống mạng lớn, luôn có sự tồn tại nhiều giao thức định tuyến khác nhau. Trên hệ thống mạng đó, có thể có sự hiện của giao thức RIP, OSPF, hay cũng có thể là static route (định tuyến tĩnh). Để các router có thể giao tiếp với nhau dù khác giao thức định tuyến, ta phải thực hiện cấu hình redistribute để kết nối các router sử dụng các giao thức định tuyến khác nhau.

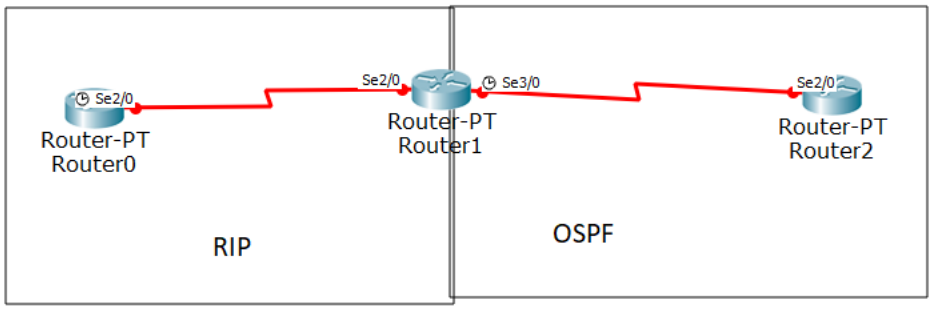
Redistribute là một phương pháp phân phối một Route được học từ giao thức định tuyến này vào một giao thức định tuyến khác. Redistribute thường được thực hiện trên Router giao tiếp giữa hai giao thức định tuyến khác nhau hay còn gọi là Router biên dịch ASBR (Boundary Router).



Hình minh họa có nhiều giao thức định tuyến trong một hệ thống

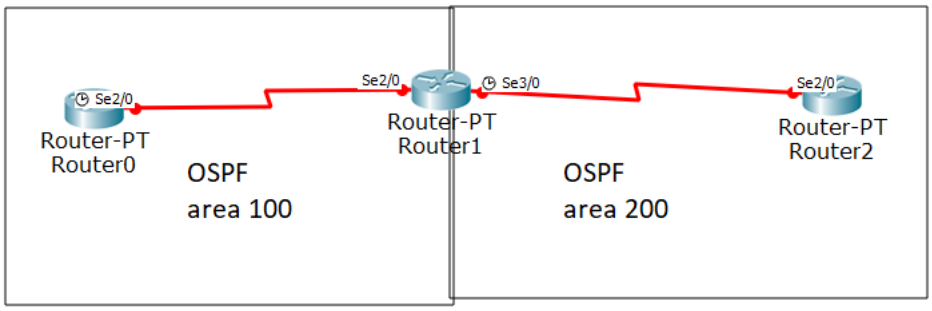
2. Cách thức cấu hình:

Redistribute giữa RIP và OSPF



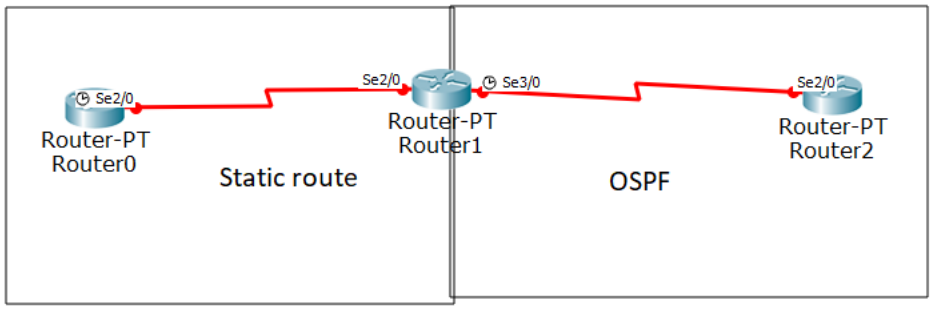
Giả sử rằng đã cấu hình định tuyến cho các router theo mô hình trên (giả sử cấu hình OSPF với process id là 1). Để thực hiện redistribute, ta cấu hình ở router nằm ở nơi giao giữa 2 giao thức định tuyến, trong tình huống này là router1. Ta cấu hình như sau:
Trên router1
Router1(config)#router rip
Router1(config)#redistribute ospf 1metric 5
Router1(config)#exit
Router1(config)#router ospf 1
Router1(config)#redistribute rip subnets

Redistribute giữa 2 OSPF khác area



Giả sử rằng đã cấu hình định tuyến cho các router theo mô hình trên (giả sử cấu hình OSPF với process id là 1 cho area 100 và 2 cho area 200). Trong tình huống này, do 2 giao thức OSPF không kết nối đến area 0 (đường backbone) nên không thể chuyển tiếp gói tin cho nhau được. Do đó, ta phải thực hiện cấu hình redistribute trong tình huống này. Để thực hiện redistribute, ta phải cấu hình ở router trung gian giữa 2 area, trong tình huống này là router1. Ta cấu hình như sau**:**
Trên router1
Router1(config)#router ospf 1
Router1(config)#redistribute ospf 2 subnets
Router1(config)#exit
Router1(config)#router ospf 2
Router1(config)#redistribute ospf 1 subnets

Redistribute giữa ospf và static route



Giả sử rằng đã cấu hình định tuyến cho các router theo mô hình trên (giả sử cấu hình OSPF với process id là 1). Trong tình huống này, để các thiết bị sử dụng định tuyến theo giao thức OSPF và static route có thể giao tiếp gói tin với nhau, ta phải cấu hình redistribute. Để thực hiện redistribute, ta chọn cấu hình ở router trung gian giữa 2 giao thức, trong tình huống này, ta chọn router1. Ta cấu hình như sau:

Trên router1

Router1(config)#router ospf 1

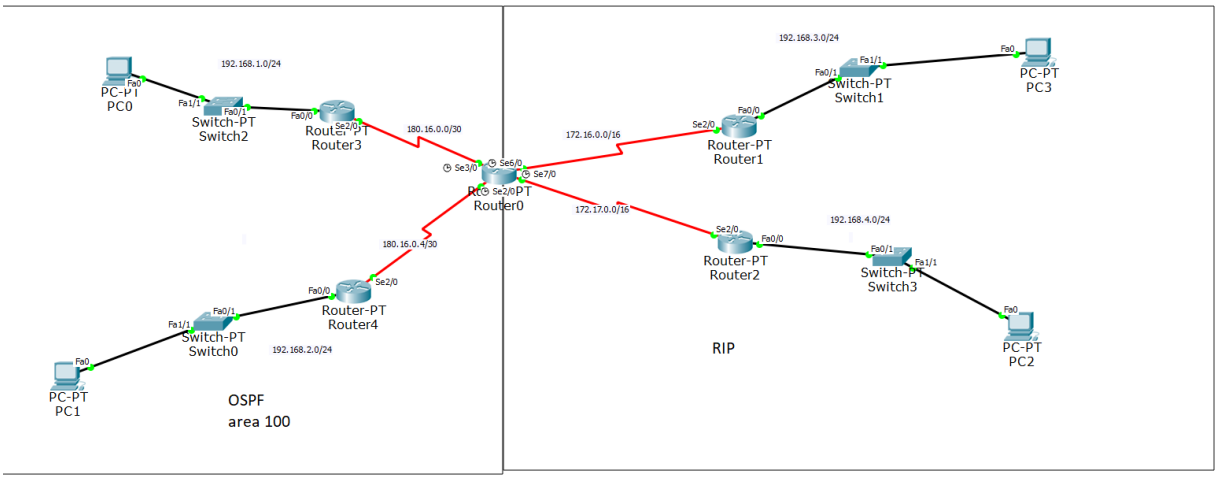
Router1(config)#redistribute connected subnets

Router1(config)#redistribute static subnets

II. Bài tập thực hành:

Bài 1:

Cho mô hình:

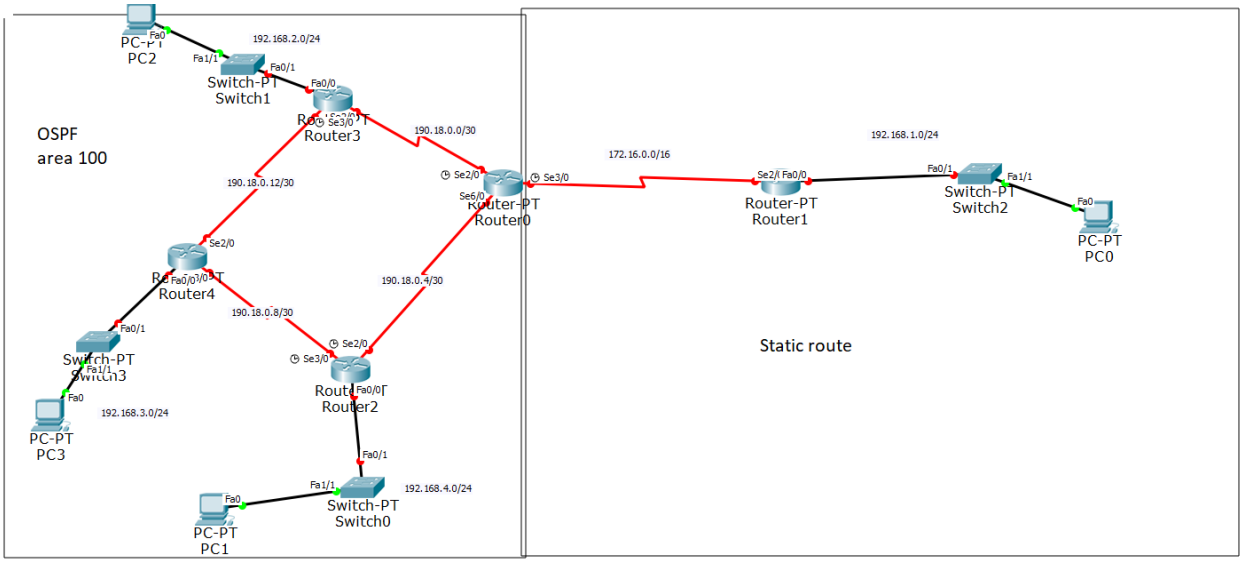


Yêu cầu:

Hãy cấu hình các router theo mô hình trên, cấu hình định tuyến cho RIP và OSPF theo sơ đồ trên. Sau đó, hãy thực hiện cấu hình Redistribute trên Router0.

Bài 2:

Cho mô hình:



Yêu cầu:

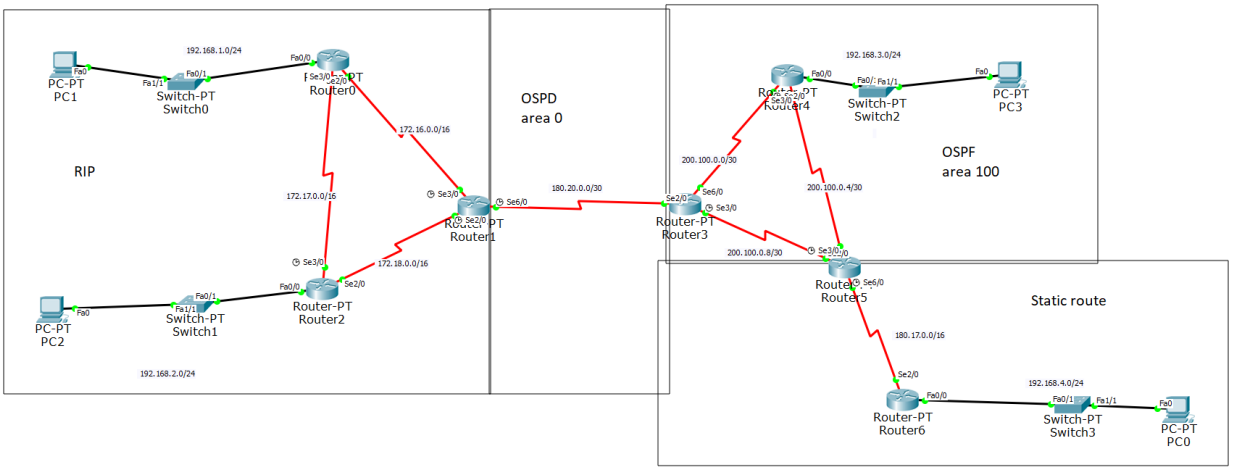
Hãy cấu hình theo sơ đồ trên, thực hiện cấu hình định tuyến với OSPF theo như mô hình.

Cấu hình default route trỏ về router0, trên router0 cấu hình static route chỉ về lớp 192.168.1.0/24.

Cấu hình redistribute cho static route.

Bài 3:

Cho sơ đồ:



Yêu cầu:

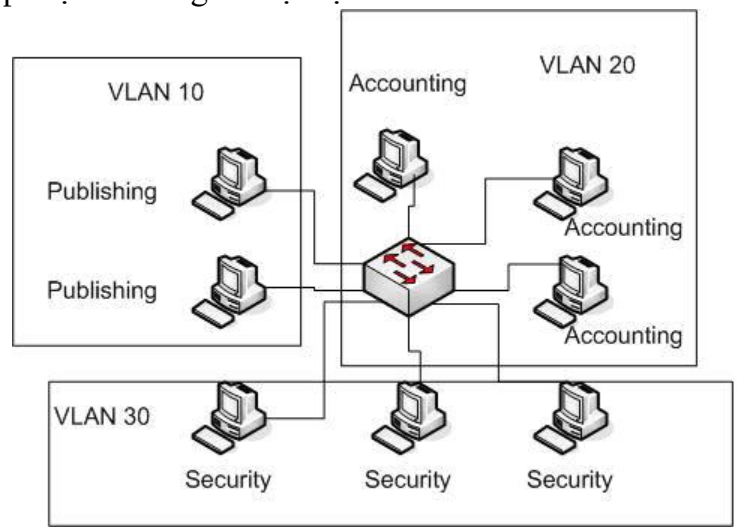
Hãy cấu hình theo sơ đồ trên. Thực hiện định tuyến và redistribute cho sơ đồ trên.

BÀI 10: CẤU HÌNH VLAN

I. Hướng dẫn thực hiện

1. Giới thiệu VLAN

VLAN (Virtual Local Area Network) là mạng LAN ảo, đây là kỹ thuật cho phép tạo ra các mạng LAN độc lập một cách logic được tạo ra trên 1 switch.



Chia nhiều VLAN trên cùng 1 switch

Các loại VLAN: có 3 loại mạng VLAN

- Port-based VLAN: là cách cấu hình VLAN đơn giản và phổ biến. Mỗi cổng của switch gán với một VLAN xác định (mặc định là VLAN 1). Do đó mỗi host gắn vào cổng đó đều thuộc một VLAN nào đó.
- MAC Address Based VLAN: mỗi địa chỉ MAC được đánh dấu với một VLAN xác định. Cách cấu hình này ít được sử dụng do sự bất tiện trong quản lý.
- Protocol Based VLAN: cách cấu hình gần giống như MAC Address Based, nhưng sử dụng một địa chỉ logic hay địa chỉ IP thay cho địa chỉ MAC.

Lợi ích của việc chia VLAN:

- Tiết kiệm được băng thông của mạng: khi 1 gói tin được quảng bá, nó sẽ chỉ truyền trong 1 mạng VLAN, không truyền đến các VLAN khác nên giảm được lưu lượng quảng bá, tiết kiệm được băng thông đường truyền
- Tăng khả năng bảo mật: các VLAN khác nhau không thể truy cập vào nhau, trừ khi được định tuyến.
- Dễ dàng thêm hay bớt máy tính vào VLAN: Việc thêm một máy tính vào VLAN rất đơn giản, chỉ cần cấu hình cổng cho máy đó vào VLAN mong muốn.
- Tiết kiệm chi phí thiết bị, khai thác tối đa số port trên switch.
- Giúp mạng có tính linh động cao: việc chia VLAN giúp có thể dễ dàng di chuyển, thêm bớt các thiết bị, chỉ cần cấu hình lại các cổng switch và đặt chúng vào các VLAN theo yêu cầu.

Tuy nhiên, việc thực hiện VLAN vẫn còn tồn tại các nhược điểm như sau:

- Hiện nay, các chuẩn chính thức của VLAN được tổ chức IEEE 802.1g soạn thảo chưa được phê chuẩn, mặc dù chuẩn này được hỗ trợ bởi nhiều nhà cung cấp. Do đó, các thiết lập và cấu hình VLAN phụ thuộc vào nhà sản xuất thiết bị.

Để tiến hành **cấu hình VLAN trên Switch**, người dùng cần thực hiện một trình tự kỹ thuật với các bước làm khác nhau. Quy trình cấu hình VLAN thường được tiến hành tuần tự như sau:

- Bước 1: Xác định các VLAN cần được cấu hình bên trên Switch.
- Bước 2: Tiến hành kết nối các thiết bị qua cổng interface đã chuẩn bị kỹ lưỡng.
- Bước 3: Thực hiện cấu hình VLAN trên Switch theo thứ tự từ trên xuống

2. Cách thức cấu hình

Trên switch, mỗi VLAN được đại diện bởi 1 chỉ số (Number) và tên (Name). Để thực hiện chia VLAN, ta cần một số lệnh sau:

Tạo ra một VLAN có chỉ số là vlan_number

Switch(config)#vlan vlan_number

Đặt tên cho VLAN

Switch(config-vlan)#name vlan_name

Xóa một VLAN có số vlan_number

Switch(config)#no vlan vlan_number

Hiển thị danh sách các VLAN trên switch

Switch>show vlan

Chọn và gán 1 cổng vào VLAN có chỉ số vlan_number

Switch(config)#interface fa0/0

Switch(config)#switchport access vlan vlan_number

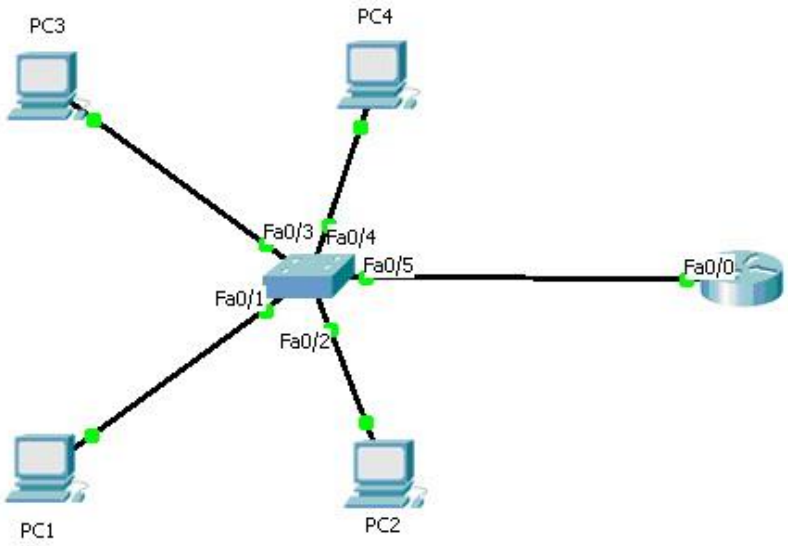
Để chọn 1 nhóm cổng, giả sử từ fa0/1 đến fa0/10 và gán vào VLAN

Switch(config)#interface range fa0/1 – fa0/10

Switch(config)#switchport access vlan vlan_number

3. Ví dụ minh họa

Cho sơ đồ mạng sau:



Cấu hình PC1 và PC2 thuộc VLAN số 10, tên ketoan
Cấu hình PC3 và PC4 thuộc VLAN số 20, tên nhansu
Trên switch ta cấu hình như sau:
Switch>en
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Tạo VLAN có tên nhansu, chỉ số 10
Switch(config)#vlan 10
Switch(config-vlan)#name ketoan
Tạo VLAN có tên ketoan, chỉ số 20
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name nhansu
Gán interface fa0/1 và fa0/2 vào VLAN nhansu, chỉ số 10
Switch(config-vlan)#interface range fa0/1-fa0/2
Switch(config-if-range)#switchport access vlan 10
Gán interface fa0/3 và fa0/4 vào VLAN ketoan, chỉ số 20
Switch(config-vlan)#interface range fa0/3-fa0/4
Switch(config-if-range)#switchport access vlan 20

Kết nối switch đã chia VLAN vào router

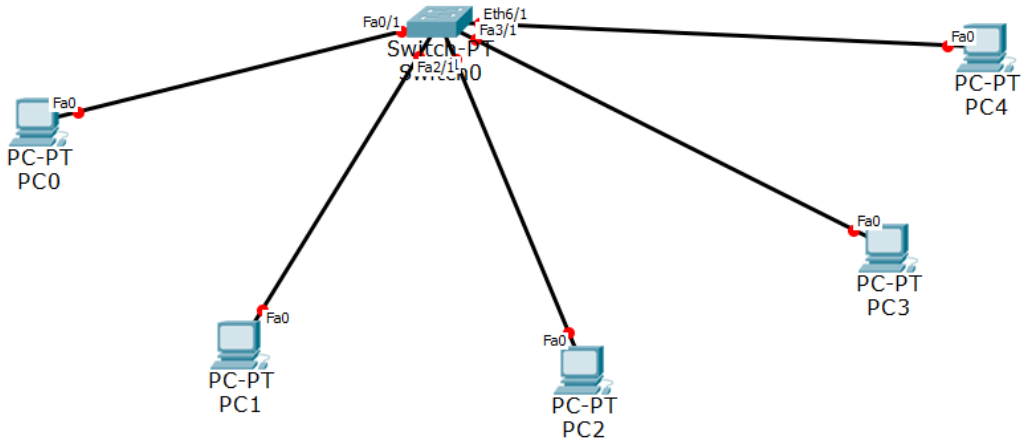
Khi nối switch đã chia VLAN vào router, để router nhận biết các VLAN, ta cần cấu hình sub interface cho router.
Trên router kết nối đến switch, ta dùng câu lệnh:
Router(config)#interface f0/0.<số sub interface>
Router(config-subif)# encapsulation dot1Q <khai báo chỉ số VLAN>
Router(config-subif)#<khai báo IP>

Ví dụ:
R1(config)#interface f0/0.1
R1(config-subif)#encapsulation dot1Q 10 //giả sử kết nối đến VLAN ketoan ở trên
R1(config-subif)#ip address 192.168.1.254 255.255.255.0 //khai báo IP
R1(config)#interface f0/0.2
R1(config-subif)#encapsulation dot1Q 20 //giả sử kết nối đến VLAN nhansu ở trên
R1(config-subif)#ip address 192.168.2.254 255.255.255.0 //khai báo IP
R1(config)#interface f0/0
R1(config-if)#no shutdown
Sau khi đã thực hiện xong, trên switch, tại cổng kết nối đến router, ta phải thực hiện:
Switch(config)#interface fastethernet0/5 //cổng kết nối trực tiếp đến router
Switch(config-if)#switchport mode trunk

II. Bài tập thực hành:

Bài 1:

Cho mô hình:

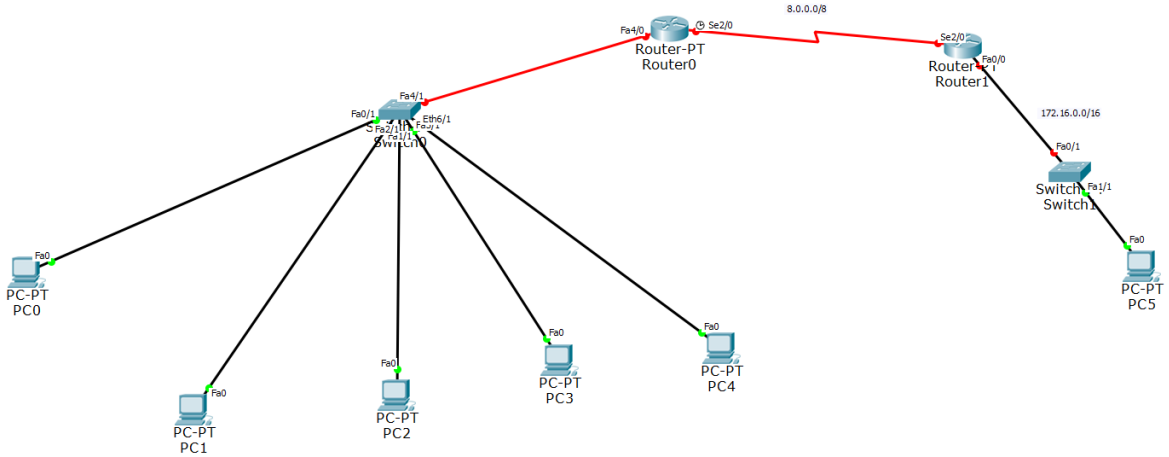


Yêu cầu:

Hãy cấu hình VLAN như sau:
Cấu hình VLAN kế toán: cho các máy PC0 và PC3 thuộc VLAN này, lớp địa chỉ sử dụng là: 192.168.1.0/24
Cấu hình VLAN kỹ thuật: cho các máy PC1 và PC2 thuộc VLAN này, lớp địa chỉ sử dụng là: 192.168.2.0/24.
Cấu hình VLAN quản lý: cho máy PC4 thuộc VLAN này, lớp địa chỉ sử dụng là: 192.168.3.0/24.

Bài 2:

Cho mô hình như sau:



Yêu cầu:

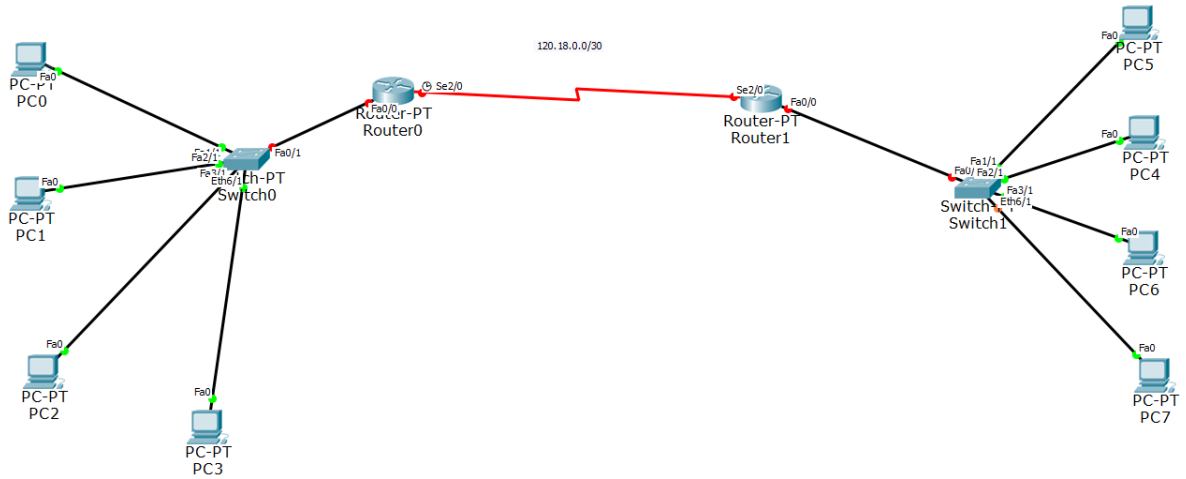
Dựa trên bài 1, hãy cấu hình sub interface tương ứng cho Router0.

Hãy cấu hình hoàn chỉnh mô hình và thực hiện định tuyến trên router để các thiết bị có thể giao tiếp lẫn nhau, có thể lựa chọn bất kỳ giao thức định tuyến nào đã học để thiết lập định tuyến.

Lưu ý: đối với Router0, phải cấu hình định tuyến cho tất cả các đường mạng của sub interface gắn trên Router0.

Bài 3:

Cho mô hình sau:



Yêu cầu:

Bên phía switch0, hãy cấu hình VLAN như sau:

VLAN1: cho máy PC0, PC1: địa chỉ: 192.168.1.0/24

VLAN2: cho máy PC2, PC3: địa chỉ: 192.168.2.0/24
Bên phía switch1, hãy cấu hình VLAN như sau:
VLAN3: cho máy PC5, PC7: địa chỉ: 192.168.3.0/24
VLAN4: cho máy PC4, PC6: địa chỉ: 192.168.4.0/24.
Hãy gán địa chỉ sub interface tương ứng cho router, sau đó cấu hình định tuyến để các máy có thể giao tiếp với nhau, có thể lựa chọn bất kỳ giao thức định tuyến nào đã học để thực hiện việc định tuyến này.

BÀI 11: CẤU HÌNH VLAN – VTP – TRUNKING

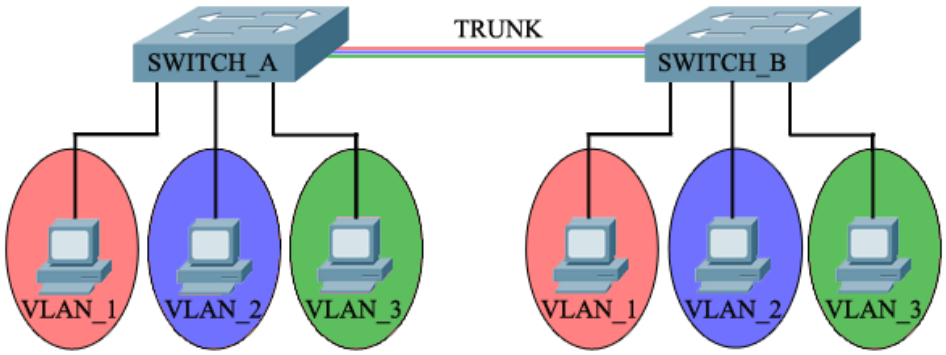
I. Hướng dẫn thực hiện

1. Khái niệm trunking

Các Host cùng một VLAN trên 2 hoặc nhiều Switch muốn đi đến nhau thì giữa các Switch này phải có một hoặc nhiều đường đấu nối với nhau.

Giả sử hệ thống có quá nhiều VLAN. Giữa các VLAN trên các Switch có quá nhiều đường đấu nối là không hợp lý. Nên cần có một giải pháp chỉ cần một đường kết nối mà vẫn đảm bảo tính thông suốt của các VLAN.

Đường đấu nối này gọi là đường trunk. Lúc này Switch chỉ cần dành ra một đường kết nối để thông suốt các VLAN trên các Switch lại với nhau.



2. Khái niệm VTP

VTP (Vlan Trunking Protocol) là giao thức hoạt động ở tầng liên kết dữ liệu trong mô hình OSI. VTP giúp cho việc cấu hình VLAN luôn đồng nhất khi thêm, xóa, sửa thông tin về VLAN trong hệ thống mạng.

VTP mode và đặc điểm các mode:

- Server : switch hoạt động ở mode này có toàn quyền quyết định tạo, xóa, sửa thông tin VLAN. Đồng bộ thông tin VLAN từ các Switch khác, Forward thông tin VLAN đến các Switch khác.
- Client: switch hoạt động ở mode này không được thay đổi thông tin VLAN mà chỉ nhận thông tin VLAN từ Server. Đồng bộ thông tin VLAN từ switch khác và forward thông tin VLAN.
- Transparent: switch hoạt động ở mode này không tiến hành tiếp nhận thông tin VLAN. Nó vẫn nhận được thông tin VLAN từ các Switch khác nhưng không tiến hành đồng bộ thông tin VLAN. Có thể tạo, xóa, sửa VLAN độc lập trên nó. Không gửi thông tin VLAN của bản thân cho các Switch khác nhưng nó có thể forward thông tin VLAN nhận được đến các Switch khác.

Lưu ý: tài liệu sẽ nhấn mạnh hướng dẫn về VTP server và VTP client.

3. Cách thức cấu hình:

Cấu hình trunking giữa 2 switch để các VLAN có thể giao tiếp với nhau:

Trên 2 switch cần cấu hình trunking phải có các VLAN giống nhau để có thể giao tiếp với nhau. Khi đó, ta cấu hình đường trunking như sau:

Ta chọn cổng nối giữa 2 switch.

Switch(config)#int fa0/1 //cổng nối giữa 2 switch.

Switch(config-if)#switchport mode trunk

Sau khi cấu hình 2 câu lệnh trên, những VLAN giống nhau dù nằm khác switch vẫn có thể giao tiếp với nhau.

Cấu hình VTP:

Cho phép các Switch tự đồng bộ cấu hình VLAN, ta phải cấu hình VTP. Khi đó, các VLAN của switch nắm mode server sẽ chuyển xuống switch nắm mode client. Lưu ý: phải cấu hình đường trunk như phần trên trước khi thực hiện các bước bên dưới.

Ta cần cấu hình các bước như sau:

Khai báo domain-name cho switch khi tham gia VTP:

Switch(config)#vtp domain [domain-name]

Khai báo password cho VTP, các switch cùng password mới đồng bộ VTP với nhau:

Switch(config)#vtp password [password]

Chọn mode hoạt động cho switch:

Switch(config)#vtp mode {server | client | transparent}

Kiểm tra VTP:

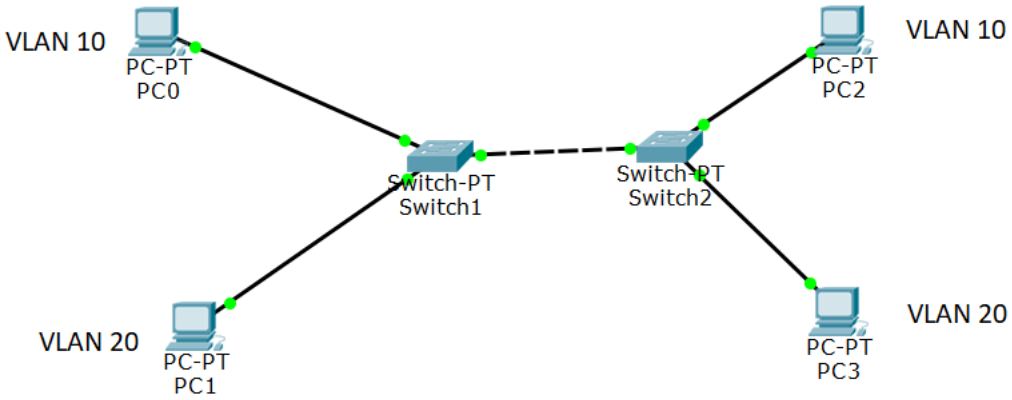
Switch#show vtp status

Switch#show vtp password

4. Ví dụ minh họa

Cấu hình trunking:

Cho mô hình như sau:



Giả sử trên Switch1 và Switch2 đều cấu hình VLAN 10 có tên là VLAN1, VLAN20 có tên là VLAN2. Sau khi cấu hình gán port cho các PC vào đúng VLAN theo yêu cầu, ta sẽ cấu hình trên switch1 và switch2 để thực hiện trunking như sau:

Trên switch1

Switch(config)#int fa0/1 //cổng kết nối đến switch2

Switch(config-if)#switchport mode trunk

Trên switch2

Switch(config)#int fa0/1 //cổng kết nối đến switch1

Switch(config-if)#switchport mode trunk

Sau khi thực hiện câu lệnh trên. Gán IP cho các PC như sau:

PC0: 192.168.1.1/24

PC1: 192.168.1.2/24

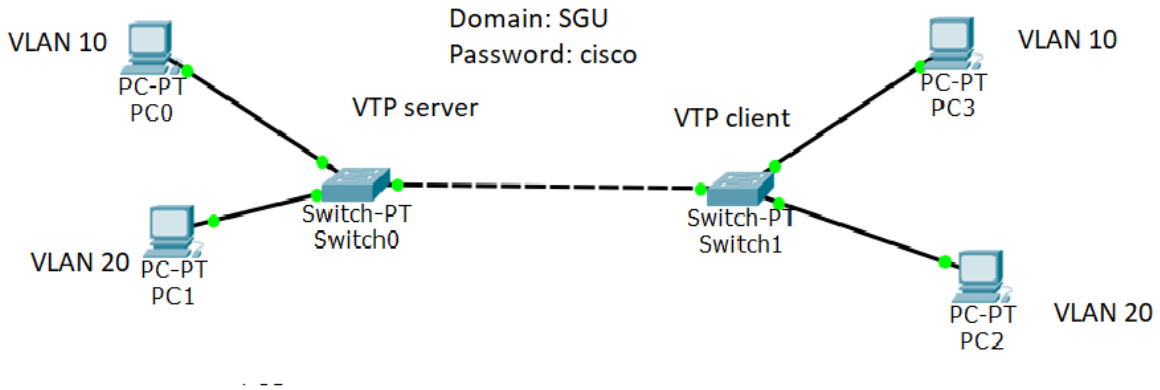
PC2: 192.168.1.3/24

PC3: 192.168.1.4/24

Khi đó, dù chung lớp mạng nhưng chỉ có PC0 và PC2 có thể ping thấy nhau vì chung VLAN 10, tương tự PC1 và PC3 có thể ping thấy nhau vì chung VLAN 20.

Cấu hình VTP server – client

Cho mô hình sau:



Trên switch0, ta sẽ cấu hình VLAN 10, VLAN 20. Sau đó, cấu hình VTP server, với domain và password trên mô hình. Bên switch1, ta sẽ cấu hình VTP client, với domain và password giống như bên server. Lưu ý: domain phải giống nhau thì giữa 2 switch mới có thể trao đổi thông tin cấu hình VLAN. Sau khi thực hiện xong, trên switch1 dù không cấu hình VLAN 10 và VLAN 20 nhưng cũng sẽ có các thông tin cấu hình này để đưa PC tương ứng vào.

Để thực hiện, giả sử rằng VLAN 10 và VLAN 20 đã cấu hình hoàn chỉnh.

Trên switch1

Switch(config)#int fa0/1 //cổng kết nối đến switch2
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#vtp domain SGU
Switch(config)#vtp password cisco
Switch(config)#vtp mode server

Trên switch2

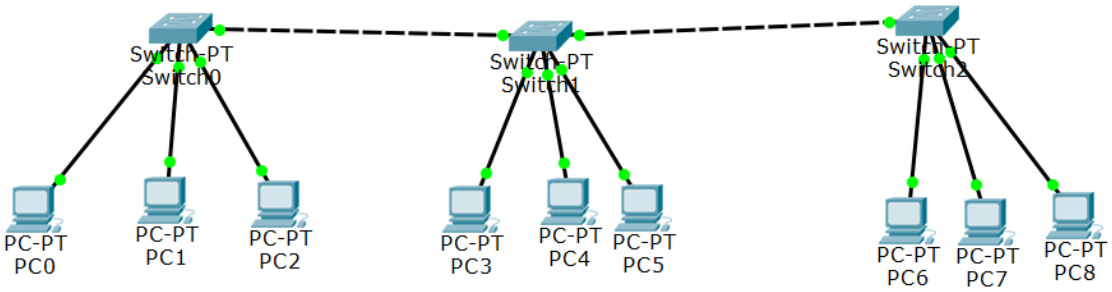
Switch(config)#int fa0/1 //cổng kết nối đến switch1
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#vtp domain SGU
Switch(config)#vtp password cisco
Switch(config)#vtp mode client

Sau khi cấu hình hoàn chỉnh, trên switch2, đã có thông tin cấu hình của VLAN10 và VLAN 20. Hãy gán PC tương ứng vào và ping kiểm tra.

II. Bài tập thực hành

Bài 1

Cho mô hình như sau:



Yêu cầu:

Trên cả 3 switch hãy cấu hình các VLAN như sau:

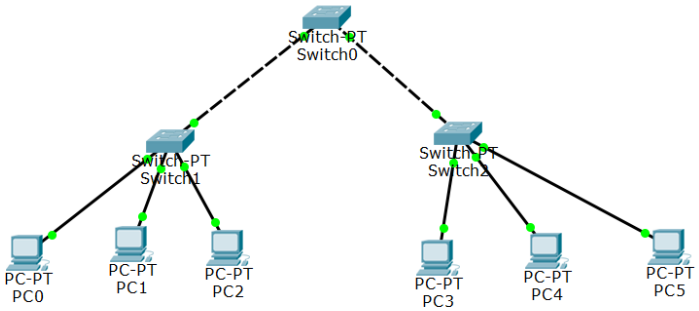
- VLAN 10: name IT
- VLAN 20: name Nhansu
- VLAN 30: name Quanly

Sau khi đã cấu hình xong VLAN, hãy gắn port cho các PC vào VLAN.

Thực hiện cấu hình trunking để các PC cùng VLAN nằm trên các switch khác nhau có thể ping thấy nhau.

Bài 2:

Cho mô hình như sau:



Yêu cầu:

Trên switch0, hãy cấu hình các VLAN như sau:

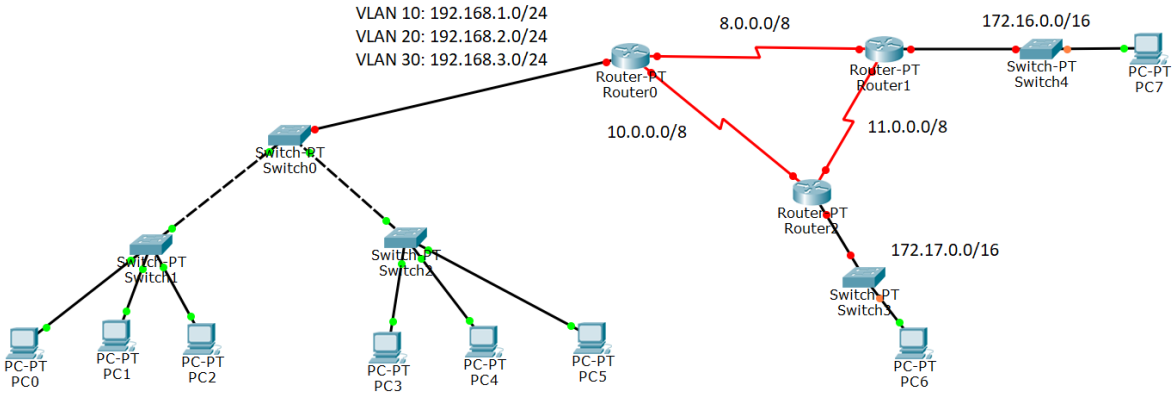
- VLAN 10: name IT
- VLAN 20: name Nhansu
- VLAN 30: name Quanly

Sau đó, cấu hình switch0 là VTP mode server, 2 switch còn lại là vtp mode client. Domain và password tùy chọn.

Trên switch1 và switch2 sau khi đã đồng bộ thông tin cấu hình VLAN, hãy cấu hình gắn các port tương ứng cho các PC. Kiểm tra kết nối giữa các PC này.

Bài 3:

Cho mô hình sau:



Yêu cầu:

Hãy cấu hình VLAN như yêu cầu ở bài 2.

Các PC thuộc VLAN phải mang IP theo như mô hình trên.

Lựa chọn một giao thức định tuyến, hãy thực hiện cấu hình định tuyến trên router để tất cả thiết bị trong hệ thống mạng có thể giao tiếp với nhau.

BÀI 12: NAT

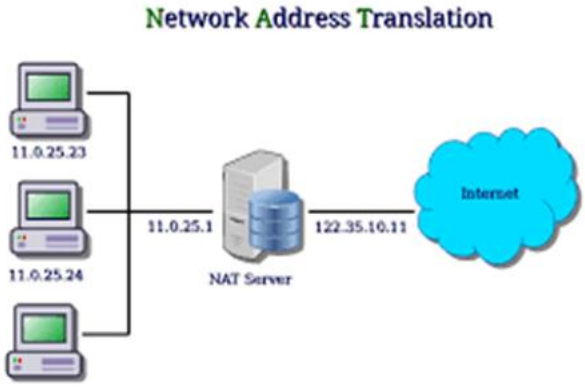
I. Hướng dẫn thực hiện

1. Khái niệm NAT

NAT (Network Address Translation) là một chức năng của router, cho phép dịch địa chỉ này sang địa chỉ IP khác, thông thường được dùng để chuyển IP Private sang địa chỉ IP Public với mục đích tiết kiệm không gian địa chỉ IP.

Trong môi trường Workgroup, các máy liên hệ với nhau thông qua địa chỉ IP do chúng ta cấu hình bằng tay hoặc do DHCP Server cấp phát, đây là IP cục bộ (Local IP)

Khi cả hệ thống kết nối ra ngoài Internet thông qua 1 router ADSL, nó sẽ dịch từ các địa chỉ IP local sang địa chỉ IP Public do IPS cung cấp cho bạn bằng dịch vụ DHCP hoặc IP tĩnh làm IP Public của bạn.



Các dạng NAT:

Có 2 dạng NAT: NAT cứng và NAT mềm:

- NAT cứng là NAT thông qua router. Ưu điểm của phương pháp này là tiết kiệm chi phí, nhưng nhược điểm là NAT sẽ chiếm dụng RAM và CPU của router. Do đó không nên dùng NAT cứng khi trong mạng có nhiều máy.
- NAT mềm là sử dụng NAT Server. NAT Server có thể là 1 máy chủ chạy hệ điều hành mạng như Windows Server 2003 hoặc Windows Server 2008. Do RAM và tốc độ CPU của NAT Server mạnh hơn nhiều so với router nên quá trình NAT sẽ nhanh hơn.

Các phương pháp NAT

Có 3 dạng NAT thường dùng là Static NAT, Dynamic NAT và NAT Overload

- Static NAT là phương pháp NAT mà địa chỉ ánh xạ và địa chỉ được ánh xạ được xác định rõ ràng. Static NAT hữu ích trong trường hợp những host cần có địa chỉ IP cố định như những mail server, web server…
- Dynamic NAT
    - Khi trong mạng có nhiều host, việc cấu hình Static NAT là bất khả thi, lúc đó ta sẽ dùng đến phương pháp Dynamic NAT.

- Dynamic NAT được thiết kế để ánh xạ một địa chỉ IP này sang một địa chỉ IP khác một cách tự động. Người ta sẽ định nghĩa 1 dãy các địa chỉ IP public dùng để gán cho các host bên trong mạng kết nối với nó.

- NAT Overload
  - NAT Overload là một dạng của Dynamic NAT, nó thực hiện ánh xạ nhiều địa chỉ private thành một địa chỉ public (many – to – one) bằng cách sử dụng các chỉ số port khác nhau để phân biệt từng chuyển dịch. NAT Overload còn có tên gọi là PAT (Port Address Translation).
  - PAT sử dụng số port nguồn cùng với địa chỉ IP riêng bên trong để phân biệt khi chuyển đổi. Số port được mã hóa 16 bit, do đó có tới 65536 địa chỉ nội bộ có thể được chuyển đổi sang một địa chỉ công cộng.

2. Cách thức cấu hình:

Static NAT – NAT tĩnh: đây là loại NAT mà người quản trị phải cấu hình địa chỉ chuyển đổi bằng tay cho quá trình NAT. Thông thường, được áp dụng cho các trường hợp NAT các máy server.

Các lệnh cấu hình Static NAT

Router(config)#ip nat inside // xác định 1 interface là kết nối vào mạng bên trong
Router(config)#ip nat outside // xác định 1 interface là kết nối ra mạng bên ngoài
Router(config)#ip nat inside source static local_ip global_ip // xác định địa chỉ bên trong và địa chỉ bên ngoài, local_ip là địa chỉ bên trong, global_ip là địa chỉ bên ngoài.

Các lệnh cấu hình Dynamic NAT

Đầu tiên ta cần định nghĩa vùng mạng sẽ được NAT bằng lệnh
Router(config)#access-list list_number permit network_address wildcard
Sau đó ta xác định vùng IP public (pool) sẽ được sử dụng
Router(config)#ip nat pool pool_name start_ip end_ip netmask
Cho phép các địa chỉ private được dịch thành địa chỉ public
Router(config)#ip nat inside source list list_number pool pool_name
Sau đó xác định các interface kết nối vào bên trong và interface kết nối ra bên ngoài bằng các lệnh Router(config)#ip nat inside và Router(config)#ip nat outside

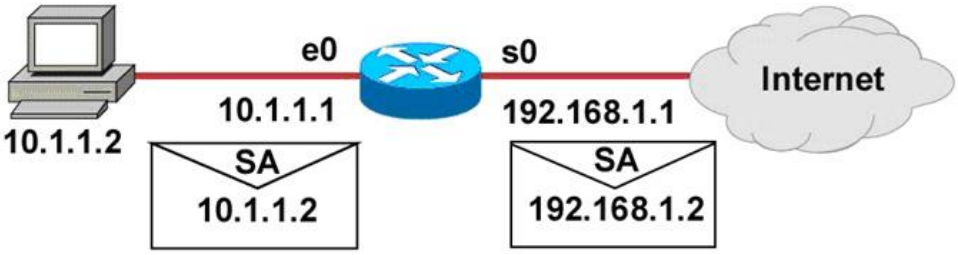
Lệnh cấu hình NAT Overload – NAT PAT

Cấu hình Overload NAT cũng tương tự như cấu hình Dynamic NAT, ở bước xác định quan hệ chuyển đổi, ta thêm từ khóa overload vào cuối câu lệnh.
Router(config)#ip nat inside source list list-number pool pool_name overload

3. Ví dụ minh họa

Minh họa static NAT – NAT tĩnh

Ta có mô hình:




```
interface s0
ip address 192.168.1.1 255.255.255.0
ip nat outside
!
interface e0
ip address 10.1.1.1 255.255.255.0
ip nat inside
!
ip nat inside source static 10.1.1.2 192.168.1.2
```

ICND20GR_282

Giả sử ta có host kết nối với internet qua 1 router, host này có địa chỉ IP tĩnh là 10.1.1.2, ta muốn cấu hình static NAT để khi ra ngoài, nó có địa chỉ IP là 192.168.1.2, ta sẽ tiến hành như sau:

Gán địa chỉ IP, chỉ định interface e0 là inside

Router(config)#interface e0

Router(config-if)#ip address 10.1.1.1 255.255.255.0

Router(config-if)#ip nat inside

Gán địa chỉ IP, chỉ định interface s0 là outside

Router(config-if)#interface s0

Router(config-if)#ip address 192.168.1.1 255.255.255.0

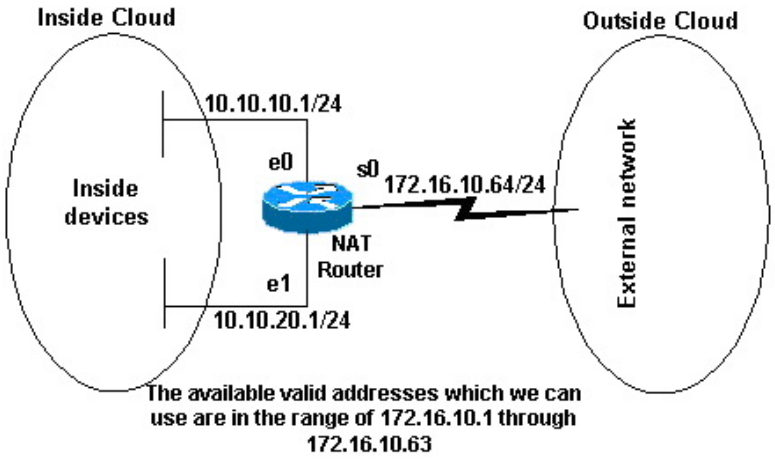
Router(config-if)#ip nat outside

Xác định quan hệ chuyển đổi:

Router(config)#ip nat inside source static 10.1.1.2 192.168.1.2

Minh họa Dynamic NAT

Ta có mô hình:

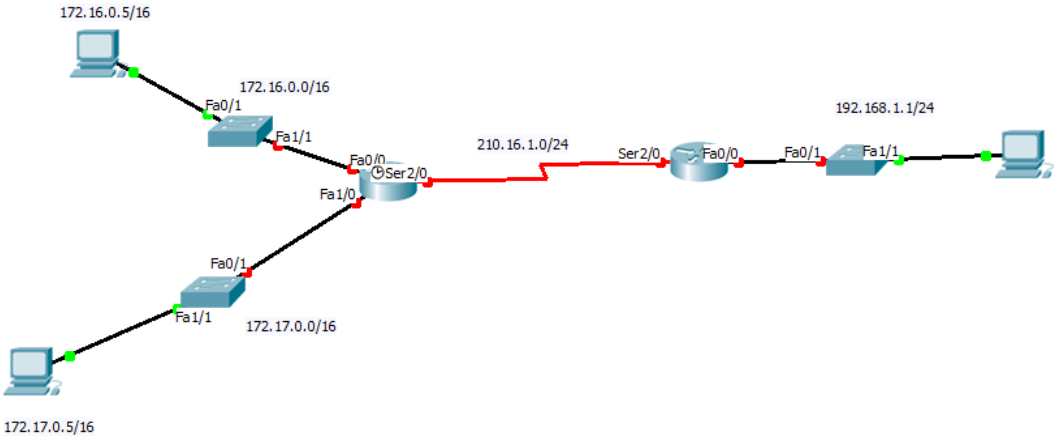


Giả sử ta có hai vùng bên trong ta có hai mạng 10.10.10.0/24 và 10.10.20.0/24, ta cần NAT ra ngoài với vùng IP Public là [172.16.10.1 – 172.16.10.63], ta sẽ cấu hình như sau:
Định nghĩa vùng mạng sẽ được NAT, danh sách này sẽ mang chỉ số 1
Router(config)#access-list 1 permit 10.10.10.0 0.0.0.255
Router(config)#access-list 1 permit 10.10.20.0 0.0.0.255
Sau đó xác định vùng IP Public, ta sẽ đặt tên vùng này là pool1
Router(config)#ip nat pool pool1 172.16.10.1 172.16.10.63 netmask 255.255.255.0
Cho phép các địa chỉ private được NAT thành địa chỉ public
Router(config)#ip nat inside source list 1 pool pool1
Lưu ý: nếu ta cấu hình Dynamic overload thì cũng làm giống như Dynamic NAT, tuy nhiên tại bước cuối cùng, khi cho phép các địa chỉ private được NAT thành địa chỉ public, ta phải thêm vào câu lệnh overload.
Router(config)#ip nat inside source list 1 pool pool1 overload

II. Bài tập thực hành

Bài 1:

Cho sơ đồ sau:



Yêu cầu:

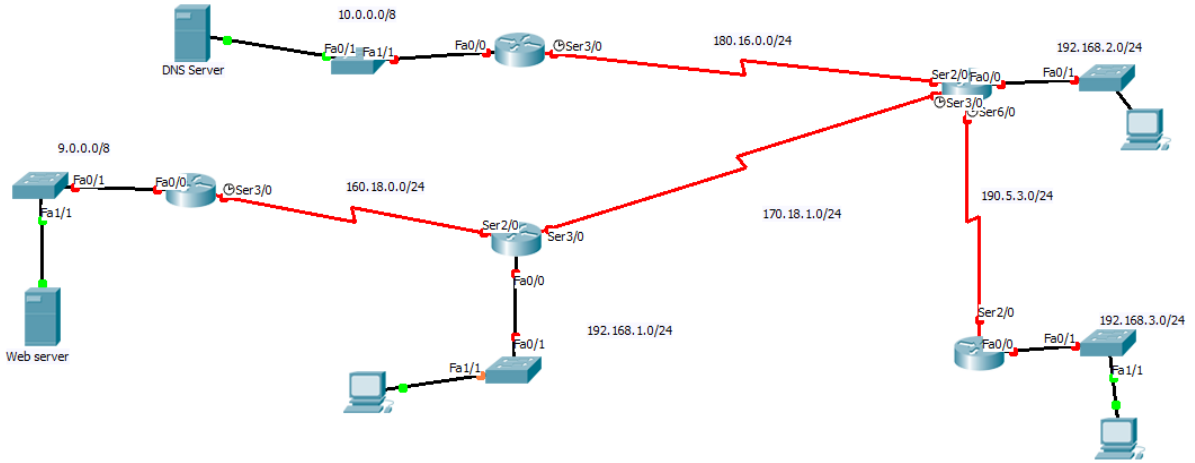
Hãy cấu hình gán địa chỉ cho các thiết bị giống như mô hình trên.

Hãy cấu hình định tuyến tĩnh cho 2 router để có thể giao tiếp giữa lớp 210.16.1.0/16 và 192.168.1.0/24. Tuy nhiên, sẽ không cấu hình định tuyến vào 2 lớp 172.16.0.0/16 và 172.17.0.0/16.

Hãy cấu hình static NAT cho 172.16.0.5/16 thành 210.16.1.10/24 và 172.17.0.5/16 thành 210.16.1.20/24.

Bài 2:

Cho sơ đồ sau:



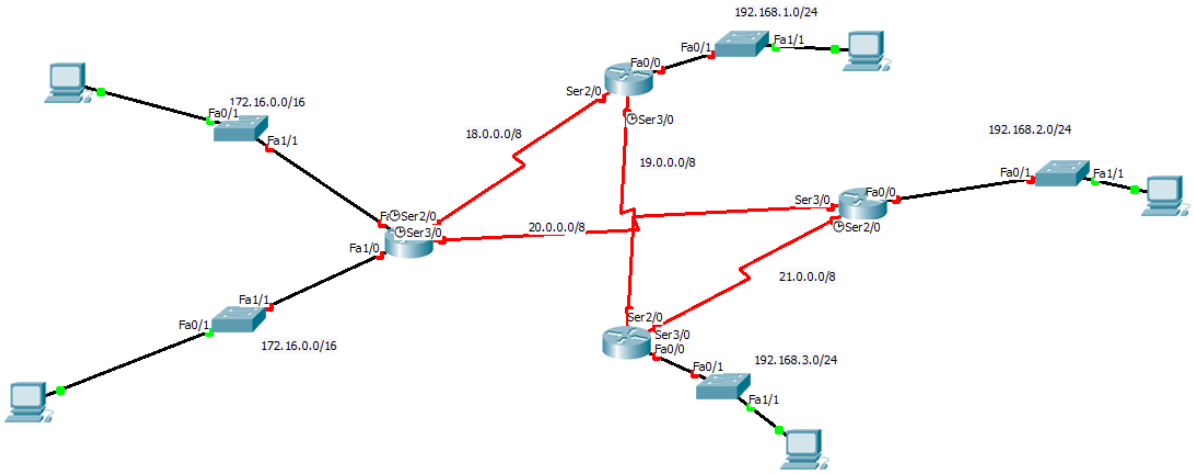
Yêu cầu:

Hãy cấu hình địa chỉ và định tuyến OSPF cho các router trên. Tuy nhiên, không cấu hình cho 2 lớp 10.0.0.0/8 và 9.0.0.0/8.

Hãy cấu hình NAT cho DNS server ra ngoài sẽ mang địa chỉ là 180.16.0.10/24 và Web server ra ngoài sẽ mang địa chỉ 160.18.0.10/24.

Bài 3:

Cho mô hình sau:



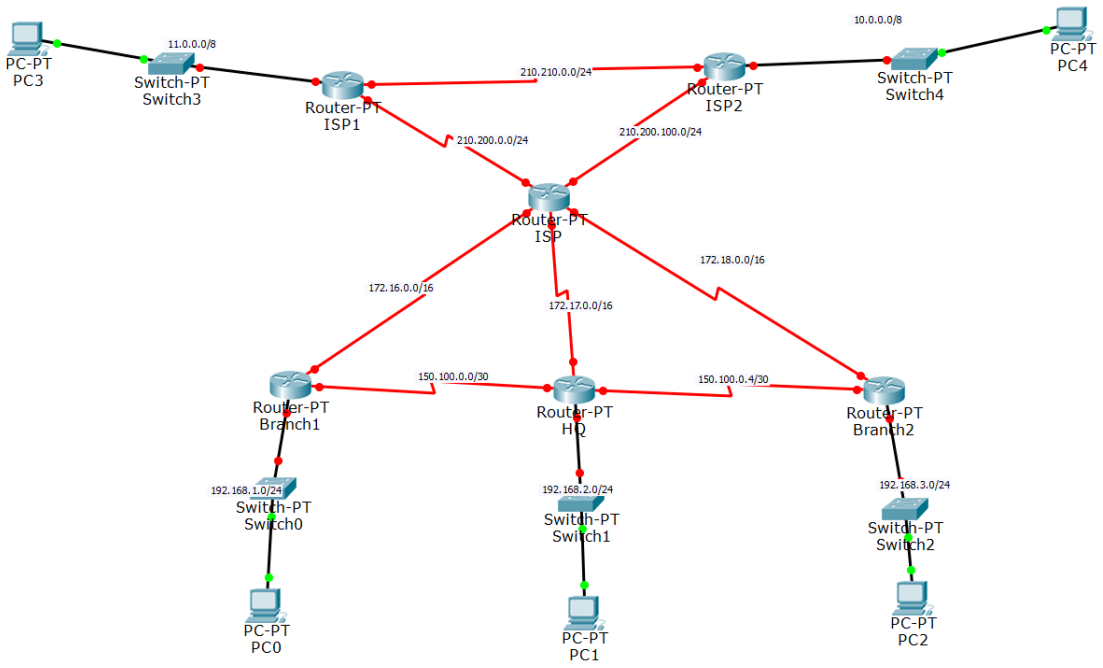
Yêu cầu:

Hãy cấu hình OSPF cho các router. Không cấu hình định tuyến cho các đường mạng nối vào các PC.

Hãy cấu hình Dynamic NAT cho các router có chứa PC, để các PC có thể ra ngoài đường mạng bên ngoài.

Lưu ý: tự lựa chọn dãy IP bên ngoài.

Bài 4:
Cho mô hình như sau:



Yêu cầu:

Hãy cấu hình định tuyến tĩnh cho các đường mạng 192.168.1.0/24, 192.168.2.0/24, 192.168.3.0/24 có thể giao tiếp với nhau.

Hãy cấu hình định tuyến RIP với ISP, ISP1, ISP2 trên các đường 210.200.0.0/24, 210.200.100.0/24, 210.210.0.0/24, 10.0.0.0/8, 11.0.0.0/8.

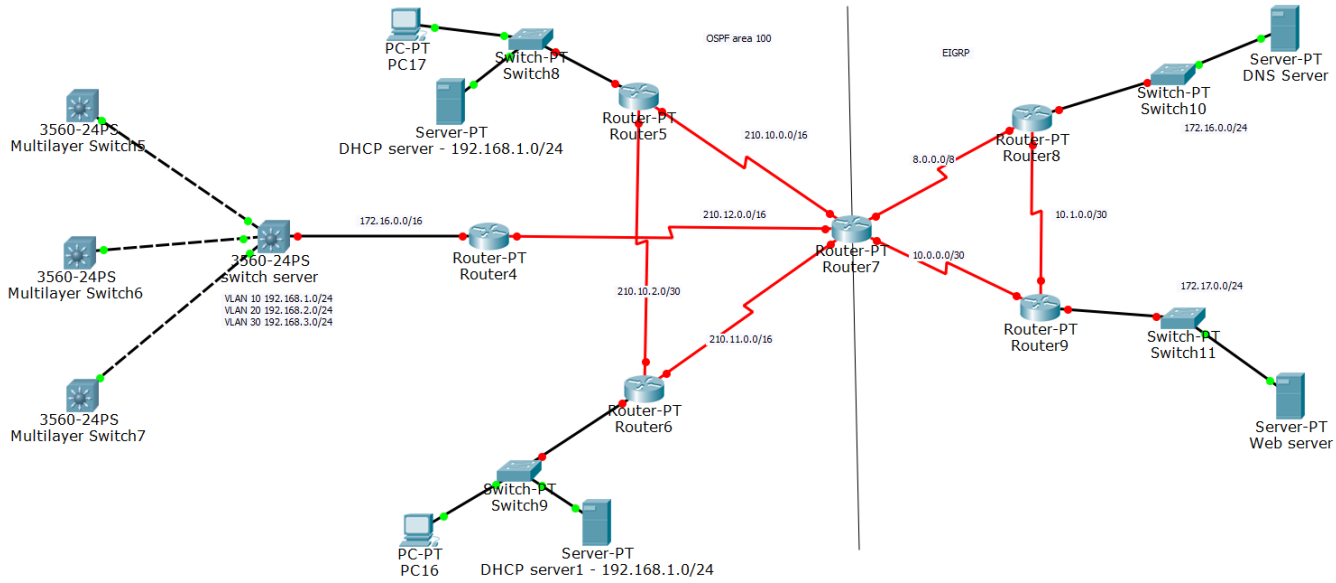
Hãy cấu hình NAT Overload từ lớp mạng 192.168.1.0/24 sang 172.16.0.0/16. 192.168.2.0/24 sang 172.17.0.0/24. 192.168.3.0/24 sang 172.18.0.0/16.

BÀI 13: BÀI TẬP TỔNG HỢP

Sinh viên hãy áp dụng các kiến thức đã học trong các bài tập trước để thực hiện các bài tập tổng hợp sau đây.

Bài 1:

Cho mô hình:



Yêu cầu:

Hãy cấu hình địa chỉ IP theo mô hình trên.

Hãy cấu hình định tuyến giữa các router, tuy nhiên không được cấu hình vào các mạng bên trong (những mạng nối với switch).

Hãy cấu hình VLAN theo dạng server và client. Sau đó, hãy đưa PC vào các port tương ứng ở các switch mang mode client.

Hãy cấu hình NAT như sau:

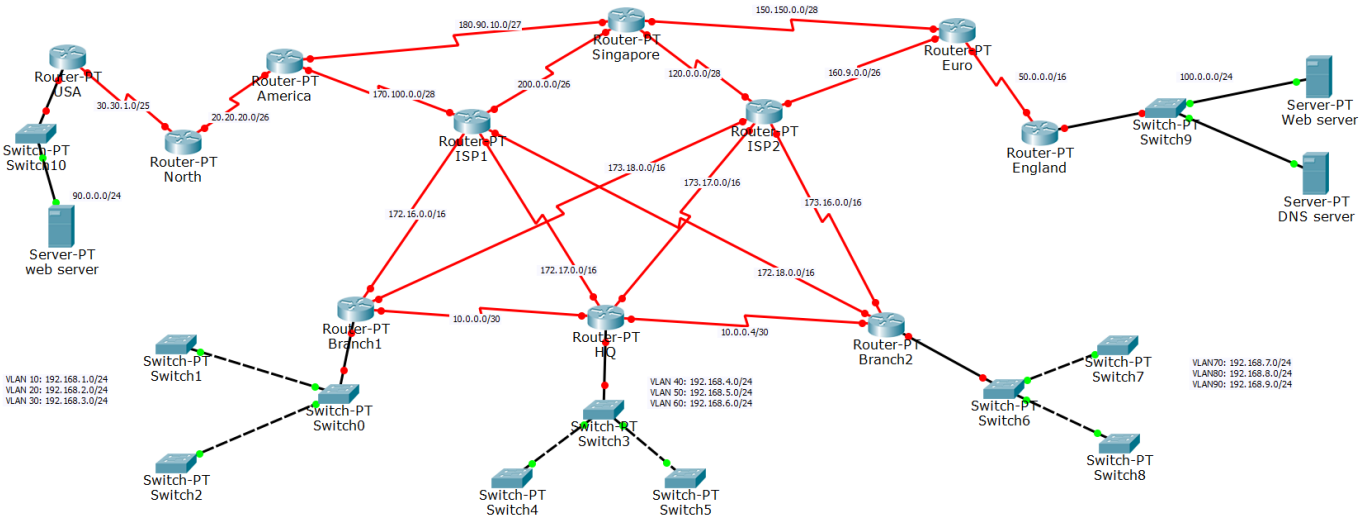
- Router 4 cấu hình Dynamic NAT cho các lớp mạng bên trong.
  - VLAN 10: sẽ mang địa chỉ: 172.16.1.1/16 – 172.16.1.200/16
  - VLAN 20: sẽ mang địa chỉ: 172.16.2.1/16 – 172.16.2.200/16
  - VLAN 30: sẽ mang địa chỉ: 172.16.3.1/16 – 172.16.3.200/16
- Router 5 và Router 6 cấu hình NAT overload. Với Pool tự chọn.
- Router 8 và Router 9 cấu hình static NAT với địa chỉ ra tự chọn.

Hãy gán địa chỉ DNS lên các PC để các máy có thể truy cập website do server cung cấp.

Hãy thực hiện redistribute cho các router trên.

Bài 2:

Cho mô hình sau:



Yêu cầu:

Các switch0, switch3, switch6 là switch dưới dạng VTP server. Hãy cấu hình cho các switch còn lại đang kết nối với 3 switch trên là VTP client. Hãy cấu hình VLAN theo như mô hình. Tự đưa các PC vào để kiểm tra.

Hãy cấu hình định tuyến tĩnh trên Branch1, HQ, Branch2 để VLAN10, VLAN 40, VLAN70 có thể giao tiếp với nhau. Các VLAN khác không được giao tiếp.

Trên Branch1, hãy cấu hình NAT overload:

- VLAN10, VLAN20 đi ra bằng đường 172.16.0.0/16
- VLAN30 đi ra bằng đường 173.18.0.0/16.

Trên HQ, hãy cấu hình NAT overload:

- VLAN40, VLAN50 đi ra bằng đường 172.17.0.0/16.
- VLAN60 đi ra bằng đường 173.17.0.0/16

Trên Branch2, hãy cấu hình NAT overload:

- VLAN70 đi ra bằng đường 173.16.0.0/16
- VLAN80, VLAN90 đi ra bằng đường 172.18.0.0/16.

Giữa ISP2, Singapore và Euro định tuyến bằng EIGRP.

Giữa ISP1, America và Singapore định tuyến bằng OSPF area 100.

Giữa Euro và England định tuyến bằng RIP.

Giữa America, North và USA định tuyến bằng OSPF area 200.

Hãy thực hiện Redistribute cho các lớp mạng.

Hãy cấu hình các server tương ứng.

BÀI 14: WIRESHARK

I. Hướng dẫn thực hiện

1. Giới thiệu wireshark

Wireshark là phần mềm phân tích gói tin, được sử dụng để khắc phục sự cố mạng, phân tích mạng, xây dựng giao thức và ứng dụng mạng, sử dụng trong đào tạo. Trước năm 2006, Wireshark có tên là Ethereal.

Wireshark còn được gọi là một bộ phân tích gói mạng (network packet analyzer). Một network packet analyzer sẽ cố gắng nắm bắt các network packets và cố gắng hiển thị dữ liệu gói đó càng chi tiết càng tốt.

Một network packet analyzer được sử dụng như một thiết bị đo lường, dùng để kiểm tra những gì đang xảy ra bên trong cáp mạng (network cable), không khác gì chức năng của một vôn kế được thợ điện sử dụng để kiểm tra những gì đang xảy ra bên trong cáp điện.

Trước đây, các công cụ này thường hoặc là rất tốn kém, hoặc độc quyền, hoặc cả hai. Tuy nhiên, với sự ra đời của Wireshark, tất cả những điều đó đã thay đổi.

Wireshark có lẽ là một trong những phần mềm phân tích gói mã nguồn mở tốt nhất hiện nay (open source packet analyzer).

Mục đích của wireshark:

Sử dụng Wireshark nhằm các mục đích sau:

- Network administrators sử dụng Wireshark để khắc phục sự cố mạng.
- Các kỹ sư Network security sử dụng Wireshark để kiểm tra các vấn đề bảo mật.
- Các kỹ sư QA sử dụng Wireshark để xác minh các network applications.
- Các developers sử dụng Wireshark để gỡ lỗi triển khai giao thức.
- Mọi người sử dụng Wireshark để học internals giao thức mạng.
- Không chỉ các tình huống trên, Wireshark cũng có thể hữu ích trong nhiều tình huống khác nữa.

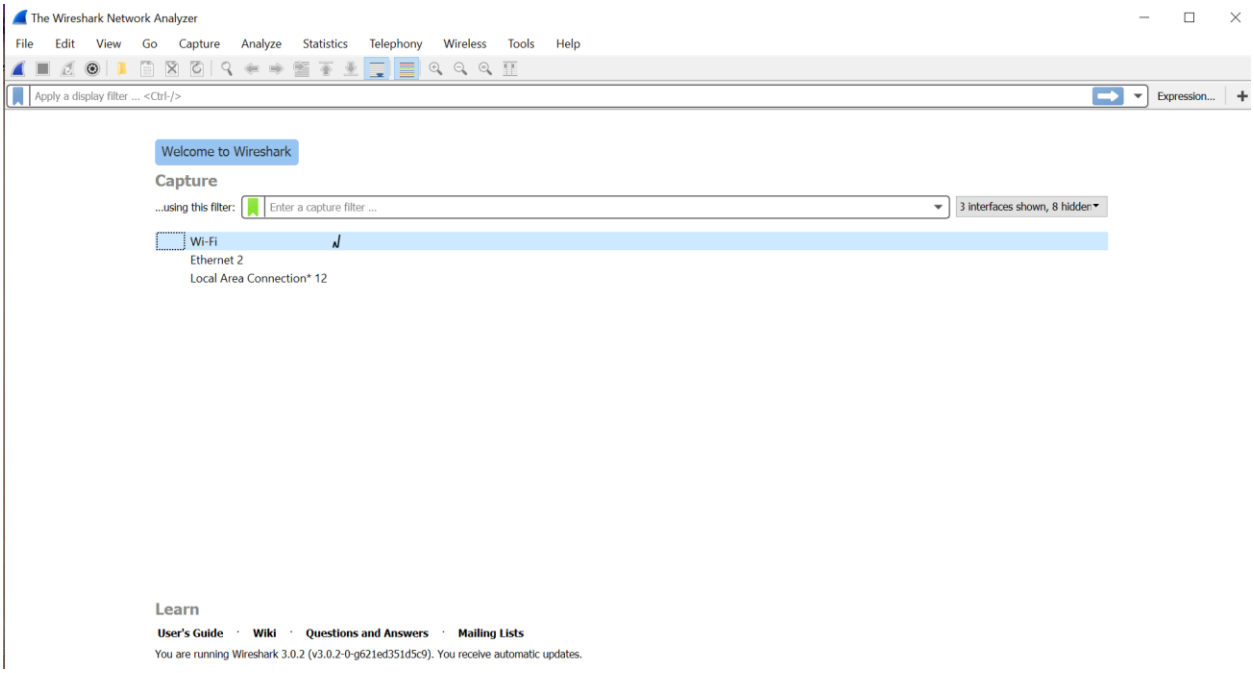
Wireshark không phải là một hệ thống phát hiện xâm nhập (IDS). Nó sẽ không cảnh báo khi ai đó làm những điều không được phép trên mạng. Tuy nhiên, nếu có gì đó không ổn, Wireshark có thể cho ta biết những gì đang diễn ra.

Wireshark sẽ không thao túng mọi thứ trên mạng, nó sẽ chỉ thực hiện việc "đo" hay bắt các gói tin trên mạng một cách chi tiết nhất.

2. Cài đặt và sử dụng wireshark

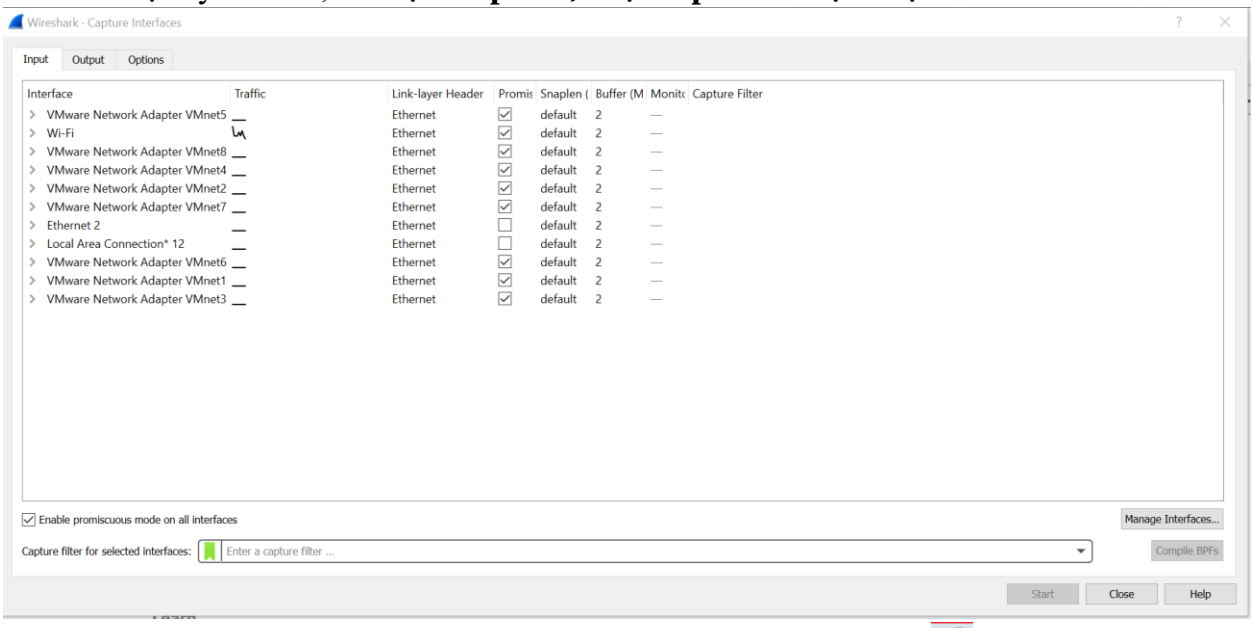
Để sử dụng wireshark, ta phải download phần mềm wireshark từ trang chủ: https://www.wireshark.org/#download. Sau đó, tùy theo hệ điều hành của máy tính mà ta chọn phiên bản phù hợp.

Sau khi hoàn thành cài đặt, ta có màn hình hiển thị phần mềm wireshark như sau:

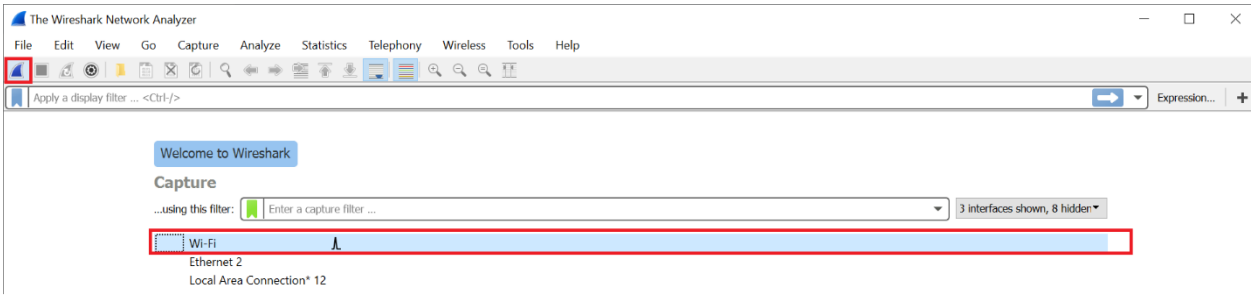


Để bắt đầu cho wireshark bắt gói tin, ta click vào card mạng đang kết nối với internet, ở hình trên ta thấy có 2 loại card mạng: wi-fi, ethernet2. Tùy theo máy tính đang kết nối bằng wifi hay kết nối có dây mà ta chọn card tương ứng. Ví dụ trong tình huống này, ta chọn card wifi, sau khi ta chọn card, ta sẽ thấy xuất hiện các mô tả kết nối hình sóng trên màn hình. Đó là những gói tin đang giao tiếp trên mạng mà card đang quản lý.

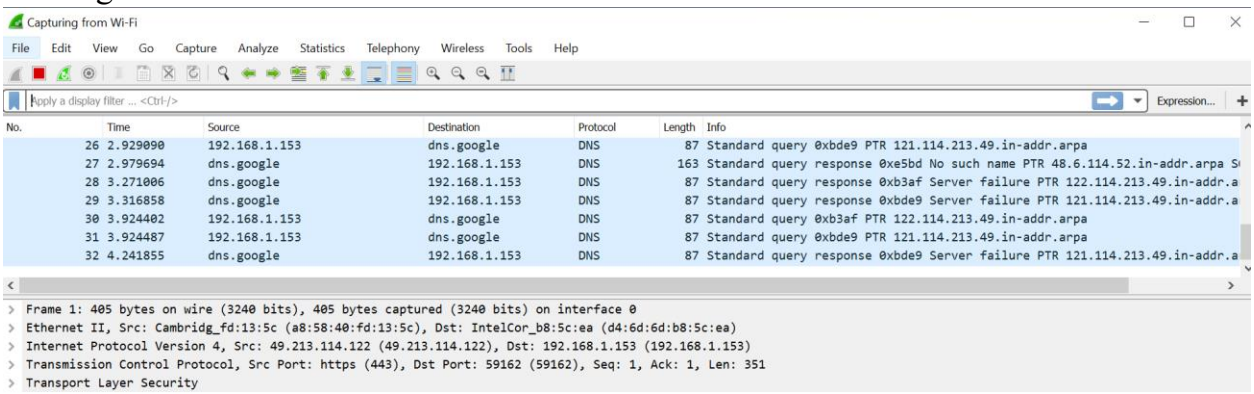
Để hiển thị đầy đủ hơn, ta chọn **Capture,** chọn **Option** để lựa chọn chi tiết hơn.



Để bắt đầu bắt gói tin, ta chọn biểu tượng **Start capturing packet** 

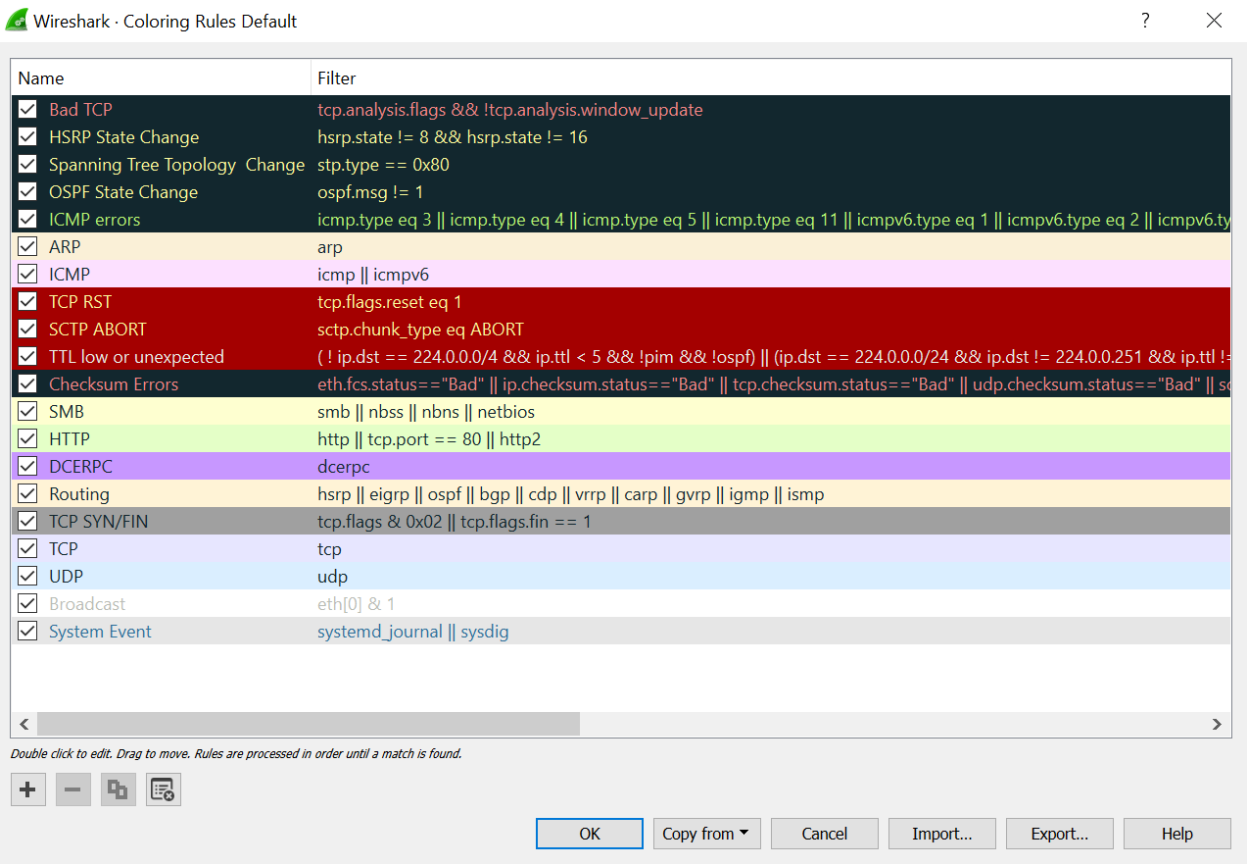


Sau khi bắt đầu bắt gói tin, wireshark sẽ bắt đầu bắt và hiển thị các gói tin đi qua card mà nó đang kiểm soát.

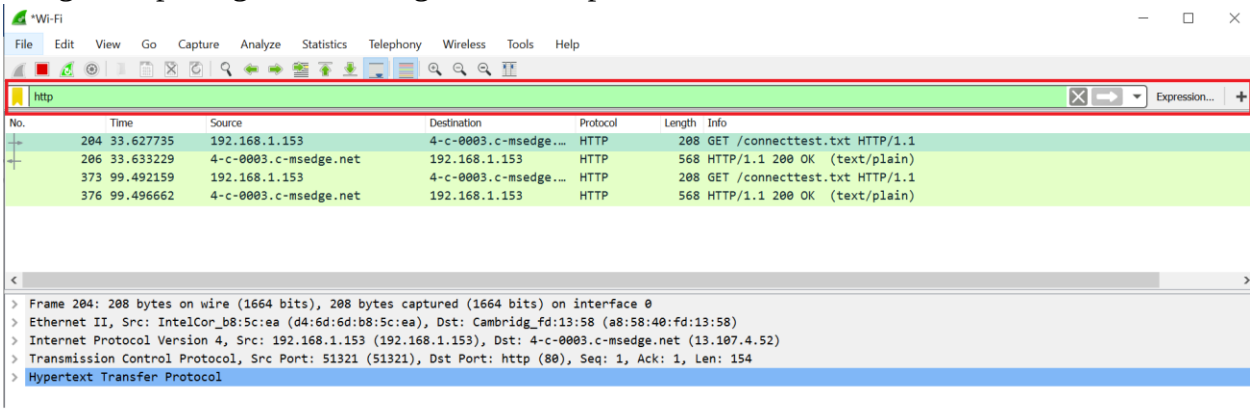


Nếu muốn dừng việc bắt gói tin, ta nhấn nút stop 

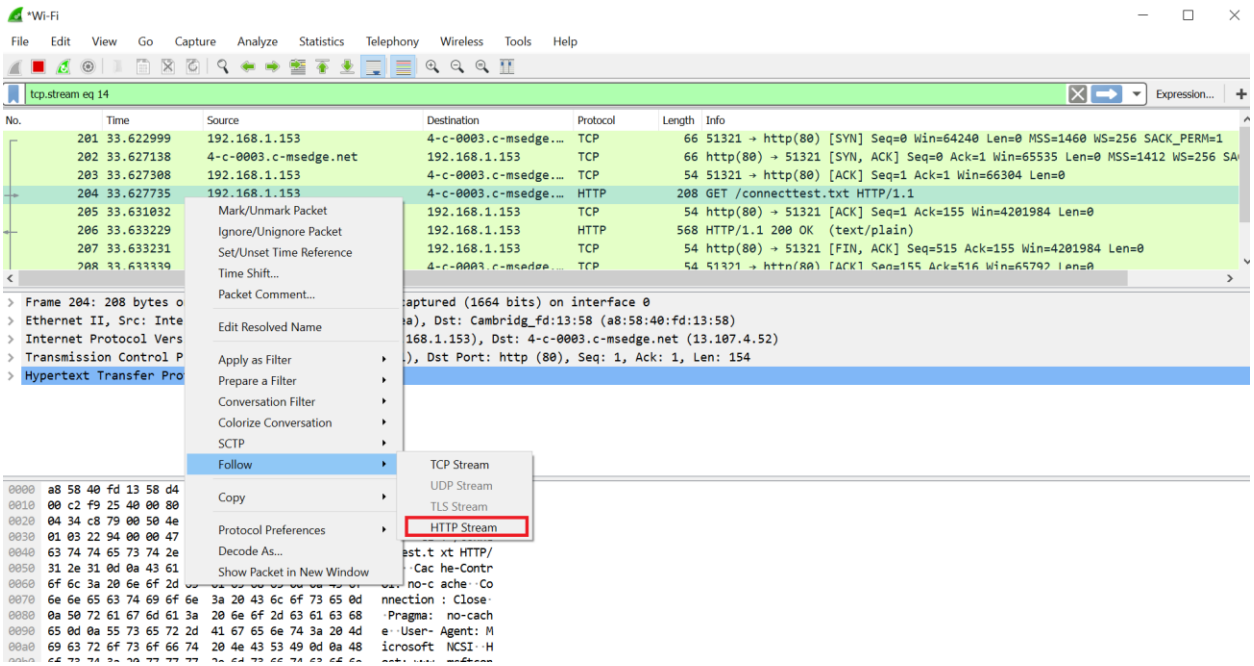
Các packet trong wireshark sẽ được hiển thị bởi các màu khác nhau, để hiển thị ý nghĩa của nó, ta chọn **View,** chọn **coloring rules…**



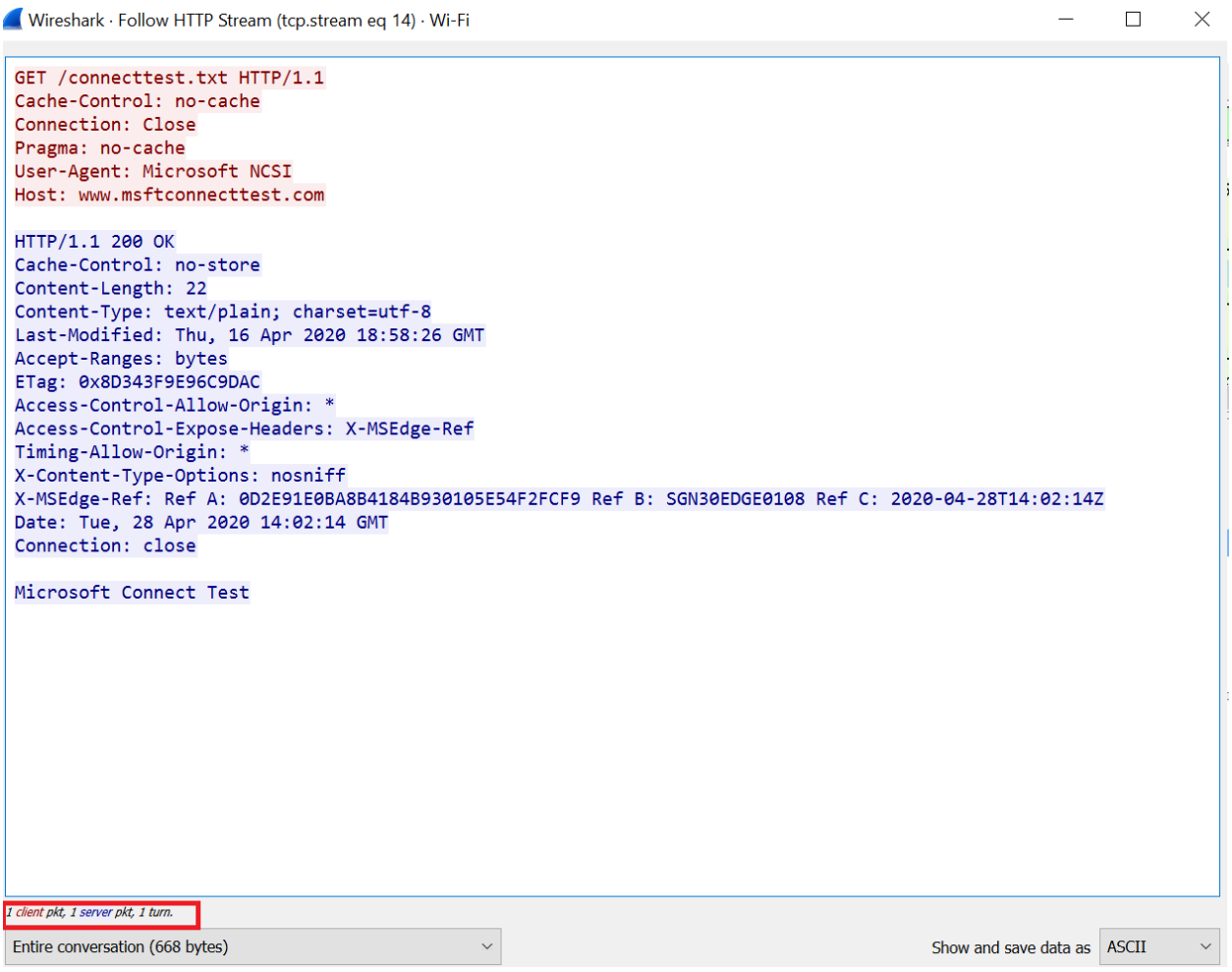
Ở đây, ta thấy các gói tin trong wireshark lướt liên tục trên màn hình hiển thị, để lọc bớt những thông tin cần tìm, ta sẽ nhập từ khóa cần lọc vào ô lọc để tìm. Ví dụ ở đây ta sẽ lọc các gói tin phân giải web với giao thức http.



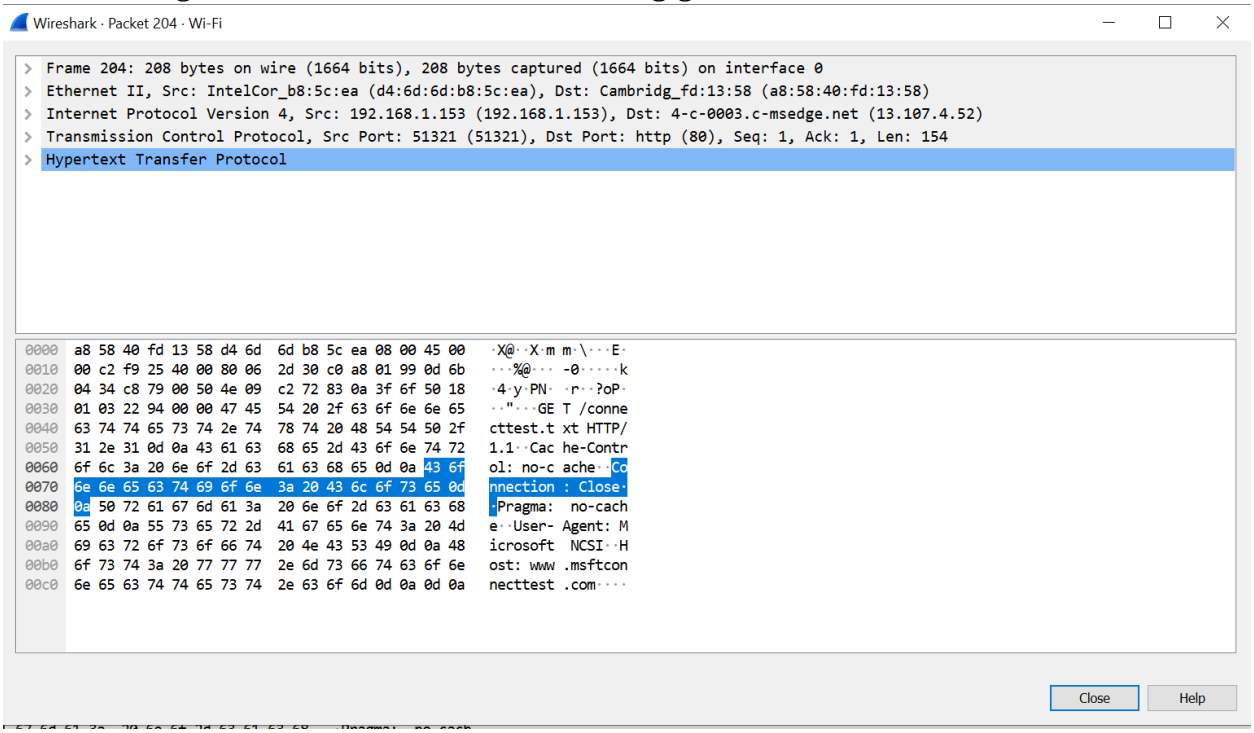
Sau khi lọc, chỉ có những gói tin liên quan đến từ khóa cần lọc được hiển thị. Tại các từ gói hiển thị, để kiểm tra các thông tin gửi nhận giữa client và server, ta có thể click phải vào từng gói tin, sau đó, chọn **follow**, chọn **HTTP stream.**


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 14
No. Time Source Destination Protocol Length Info
201 33.622999 192.168.1.153 4-c-0003.c-msedge.... TCP 66 51321 → http(80) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
202 33.627138 4-c-0003.c-msedge.net 192.168.1.153 TCP 66 http(80) → 51321 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 WS=256
203 33.627308 192.168.1.153 4-c-0003.c-msedge.... TCP 54 51321 → http(80) [ACK] Seq=1 Ack=1 Win=66304 Len=0
204 33.627735 192.168.1.153 4-c-0003.c-msedge.... HTTP 208 GET /connecttest.txt HTTP/1.1
205 33.631032 192.168.1.153 TCP 54 http(80) → 51321 [ACK] Seq=1 Ack=155 Win=4201984 Len=0
206 33.633229 192.168.1.153 HTTP 568 HTTP/1.1 200 OK (text/plain)
207 33.633231 192.168.1.153 TCP 54 http(80) → 51321 [FIN, ACK] Seq=515 Ack=155 Win=4201984 Len=0
Mark/Unmark Packet
Ignore/Unignore Packet
Set/Unset Time Reference
Time Shift...
Packet Comment...
Edit Resolved Name
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
TCP Stream
UDP Stream
TLS Stream
HTTP Stream

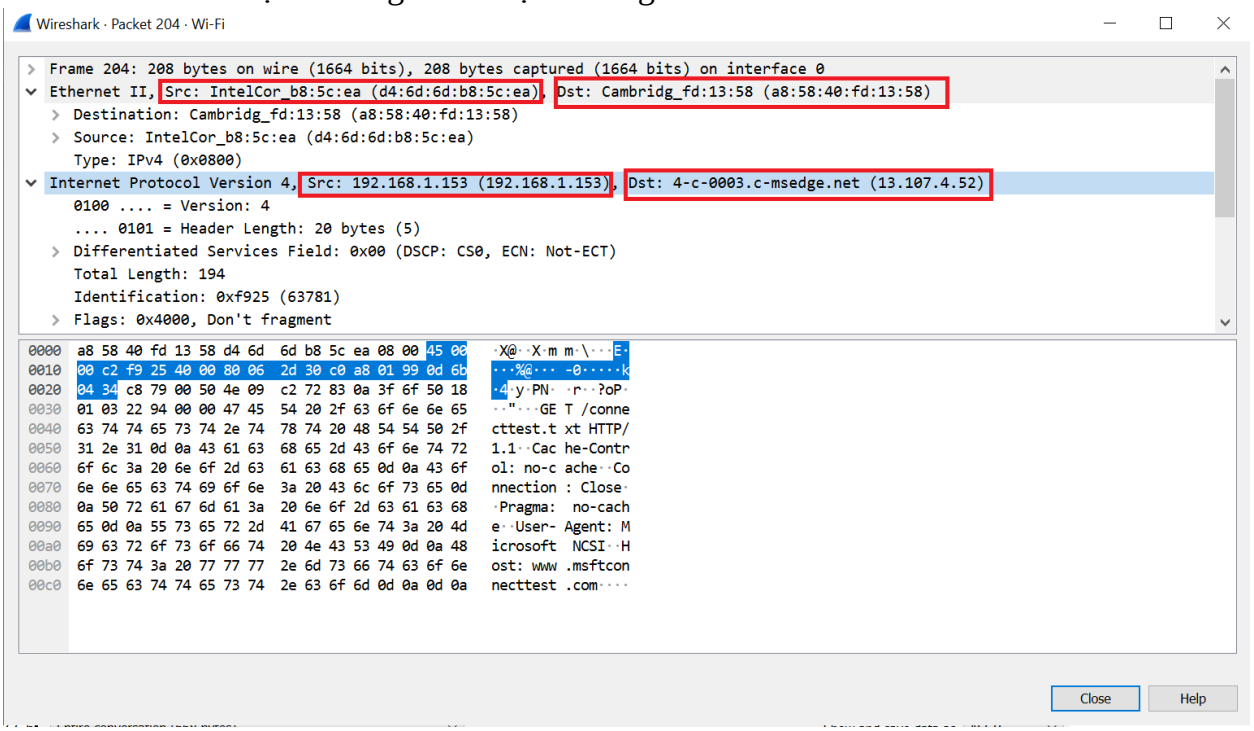
Kết quả sẽ là:


Wireshark · Follow HTTP Stream (tcp.stream eq 14) · Wi-Fi
GET /connecttest.txt HTTP/1.1
Cache-Control: no-cache
Connection: Close
Pragma: no-cache
User-Agent: Microsoft NCSI
Host: www.msftconnecttest.com
HTTP/1.1 200 OK
Cache-Control: no-store
Content-Length: 22
Content-Type: text/plain; charset=utf-8
Last-Modified: Thu, 16 Apr 2020 18:58:26 GMT
Accept-Ranges: bytes
ETag: 0x8D343F9E96C9DAC
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: X-MSEdge-Ref
Timing-Allow-Origin: *
X-Content-Type-Options: nosniff
X-MSEdge-Ref: Ref A: 0D2E91E0BA8B4184B930105E54F2FCF9 Ref B: SGN30EDGE0108 Ref C: 2020-04-28T14:02:14Z
Date: Tue, 28 Apr 2020 14:02:14 GMT
Connection: close
Microsoft Connect Test
1 client pkt, 1 server pkt, 1 turn.
Entire conversation (668 bytes)
Show and save data as
ASCII

Ta để ý dòng được tô trong khung, đó là tổng số gói tin giao tiếp giữa client và server. Để kiểm tra gói tin cụ thể hơn, ta click vào từng gói tin muốn kiểm tra.

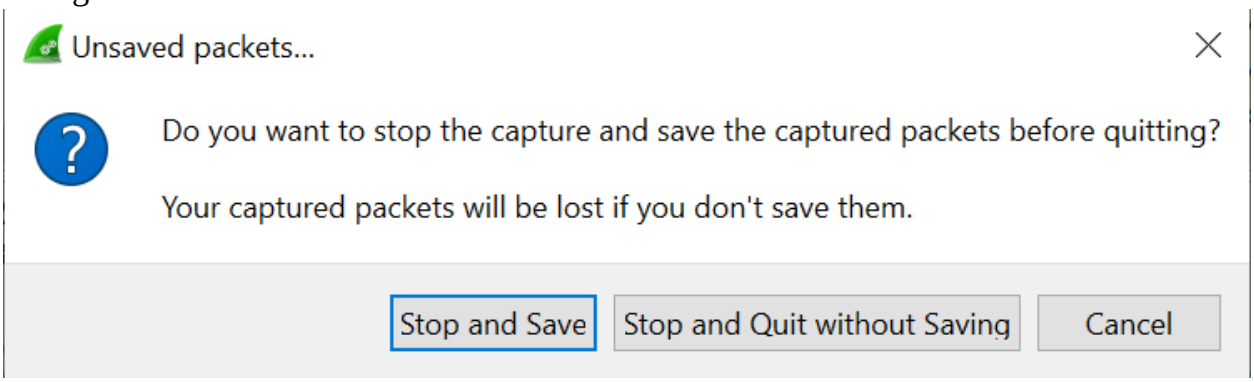


Trong tình huống trên, ta có thể xem địa chỉ MAC của máy gửi và máy nhận ở dòng Ethernet II. Xem địa chỉ IP gửi và nhận ở dòng Internet Protocol.



Đây là các thao tác cơ bản trong quản lý phần mềm wireshark, nếu ta muốn tắt phần mềm wireshark, khi click vào biểu tượng tắt phần mềm, phần mềm sẽ hỏi ta có lưu lại các gói

mà chúng ta đang bắt để phân tích hay không. Tùy theo nhu cầu mà ta sẽ lựa chọn lưu hay không.



3. Ví dụ minh họa

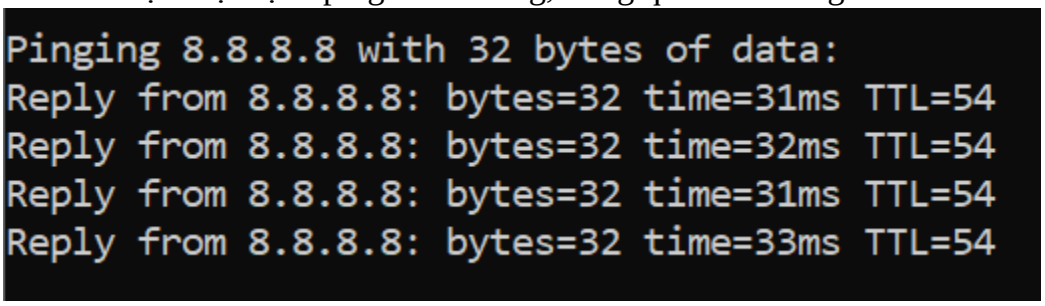
Ví dụ: bắt gói tin khi thực hiện ping đến 8.8.8.8

Máy tính phải được kết nối vào mạng.

Chạy chương trình wireshark và thiết lập card mạng phù hợp.

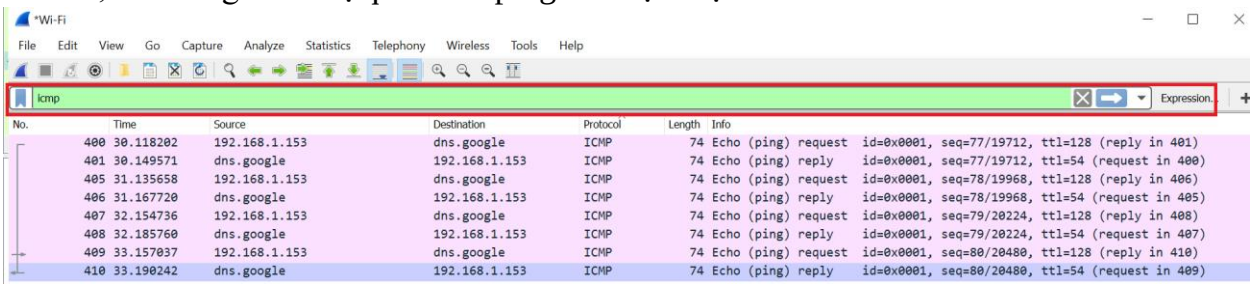
Thực hiện lệnh ping 8.8.8.8 trên comman prompt.

Sau khi thực hiện lệnh ping thành công, dừng quá trình bắt gói trên wireshark.

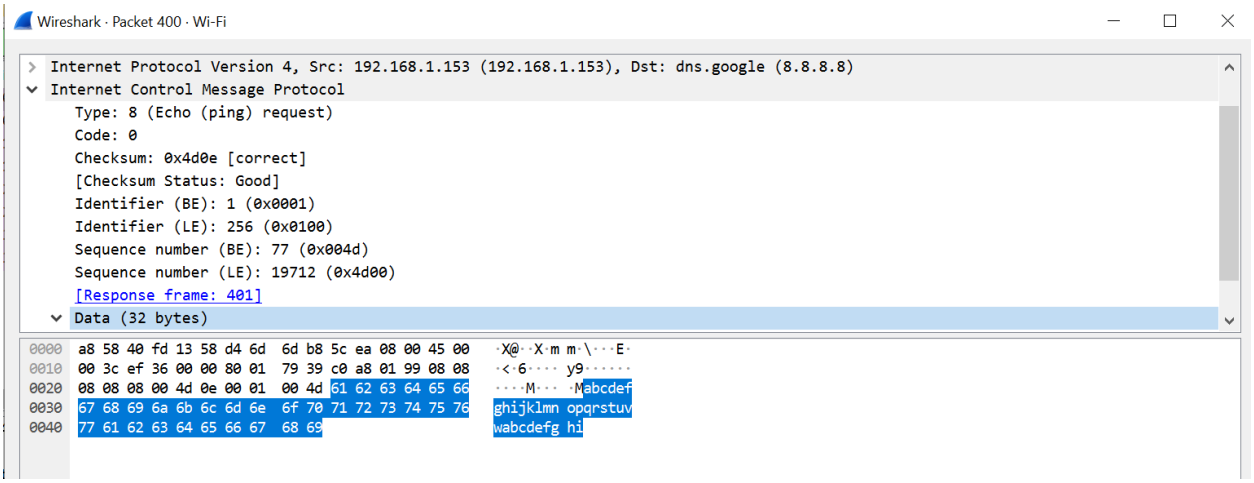


Trên wireshark, tại mục filter, ta nhập giao thức của câu lệnh ping là giao thức icmp.

Khi đó, các dòng hiển thị quá trình ping sẽ được hiện ra.



Khi click vào chi tiết của từng gói tin, ta sẽ thấy thông tin của gói icmp.



Ở đây, ta thấy nội dung của gói tin này là các ký tự từ a đến z. Trong tình huống này, các ký tự không có mã hóa, tuy nhiên, thông thường các ký tự khi gửi dữ liệu sẽ được mã hóa, cho nên ta sẽ không dễ dàng nhìn thấy nội dung các gói tin như ví dụ ở trên.

II. Bài tập thực hành

Bài 1:

Bắt gói tin khi truy cập website với wireshark. Hãy thực hiện theo các yêu cầu sau.
Cài đặt wireshark lên máy tính.
Đảm bảo máy tính kết nối với internet.
Chạy wireshark, cho phép wireshark bắt gói tin.
Mở trình duyệt, truy cập vào một trang web bất kỳ.
Sau khi truy cập trang web, mở wireshark, nhấn nút stop để ngưng quá trình bắt gói tin.
Hãy xác định các thông tin như sau:

- Cho biết địa chỉ IP của trang web đó là gì?
- Cho biết MAC address của web server là gì?
- Hãy cho biết tên của web server là gì?
- Hãy cho biết có những giao thức nào tham gia khi truy cập vào trang web trên.

Bài 2:

Bắt gói tin khi yêu cầu xin cấp phát DHCP.
Hãy cài đặt và cho chạy phần mềm wireshark.
Trên máy tính hãy dùng câu lệnh *ipconfig /release* và *ipconfig /renew* trên command prompt.
Sau đó, hãy stop wireshark, sau khi đã xin cấp phát IP thành công.
Trên mục filter, hãy nhập bootp, đây là gói tin của giao thức DHCP.
Hãy cho biết:

- Quá trình gửi nhận giữa server và client bao gồm bao nhiêu bước?
- Những bước đó tên gì?
- Quá trình cụ thể bao gồm các gói tin gì được gửi đi.
- Hãy phân tích cụ thể từng gói tin đã bắt.

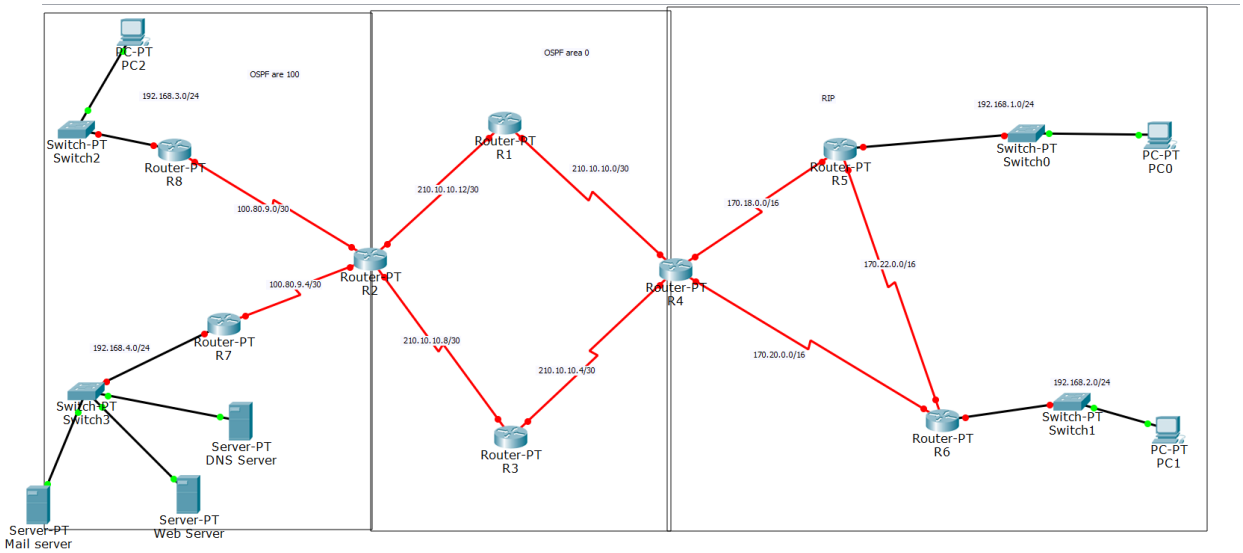
BÀI 15: ÔN TẬP KIỂM TRA

Một số bài kiểm tra mẫu cho thực hành mạng máy tính.

Bài 1:

Yêu cầu thời gian làm bài trong vòng 45 phút.

Cho sơ đồ sau:



Hãy gán các thiết bị theo như sơ đồ.

Hãy đặt tên cho các router theo như sơ đồ (2 điểm)

Hãy cấu hình IP tương ứng cho cổng theo như sơ đồ (3 điểm).

Hãy cấu hình định tuyến RIP cho các router R4, R5, R6 với các cổng tương ứng của sơ đồ (1 điểm).

Hãy cấu hình định tuyến OSPF với area 0 cho router R1, R2, R3, R4 với các cổng tương ứng của sơ đồ (1 điểm).

Hãy cấu hình định tuyến OSPF với area 100 cho router R2, R7, R8 với các cổng tương ứng của sơ đồ (1 điểm).

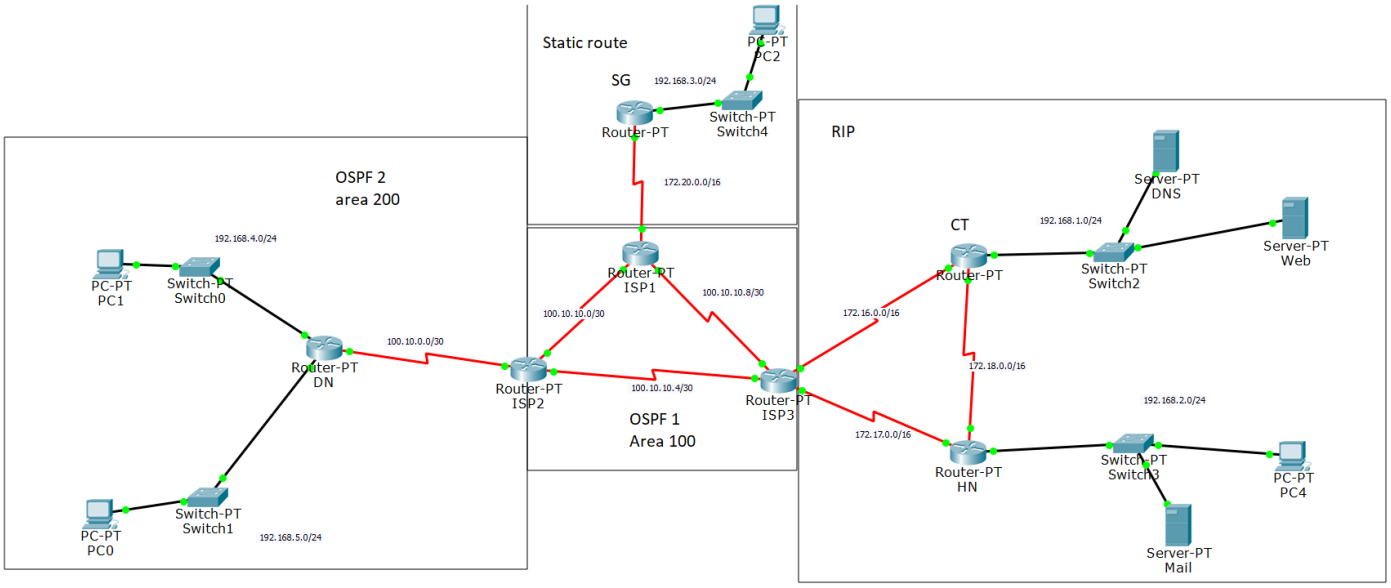
Hãy cấu hình Redistribute cho các router để các thiết bị có thể giao tiếp với nhau. (1 điểm).

Hãy cấu hình các server như sau: DNS server: 192.168.4.10, web server: tương ứng tên miền sgu.edu.vn 192.168.4.15, mail server tương ứng tên miền mail-sgu.edu.vn 192.168.4.20. Các PC phải truy cập được websites và mail. (1 điểm).

Bài 2:

Yêu cầu làm bài trong vòng 45 phút.

Cho sơ đồ mạng như sau:



Hãy thực hiện các công việc như sau:

1. Hãy cấu hình tên của các router như trên sơ đồ. (1đ)
2. Hãy cấu hình IP cho các router và các thiết bị mạng (3 đ)
3. Hãy cấu hình định tuyến RIP cho router ISP3, CT, HN theo sơ đồ (1đ)
4. Hãy cấu hình định tuyến OSPF với process id 2, area 200 cho router ISP2, DN theo sơ đồ (1đ)
5. Hãy cấu hình định tuyến OSPF với process id 1, area 100 cho router ISP1, ISP2, ISP3 theo sơ đồ (1đ)
6. Hãy cấu hình định tuyến tĩnh cho router ISP1, trỏ về đường mạng 192.168.3.0/24 theo sơ đồ, trên router SG, cấu hình default route trỏ về ISP1. (1đ)
7. Hãy cấu hình Redistribute cho các router biên (1đ)
8. Hãy cấu hình các thiết bị: DNS, Web, Mail. (1đ)

HẾT