**Lab 7. Network Infrastructure Security**

**Submission:**

You will compose a lab report that documents each step you take, including screenshots to illustrate the effects of commands you type, and describing your observations. Simply attaching code without any explanation will not receive credits

**Câu 1. Port Security**

Bằng cách giới hạn và kiểm soát các thiết bị gắn vào Switch có thể hạn chế nhiều tấn công trong LAN như:

* Kẻ tấn công dùng công cụ để quét lấy hết IP từ DHCP server
* Kiểm soát các thiết bị người dùng cố định, các server kết nối đến Switch (tránh sự thay đổi tự do trong quá trình vận hành hệ thống)

#### Topology

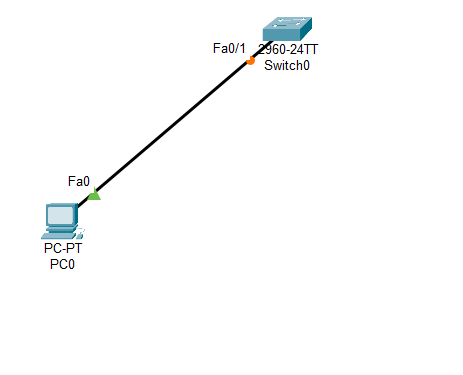


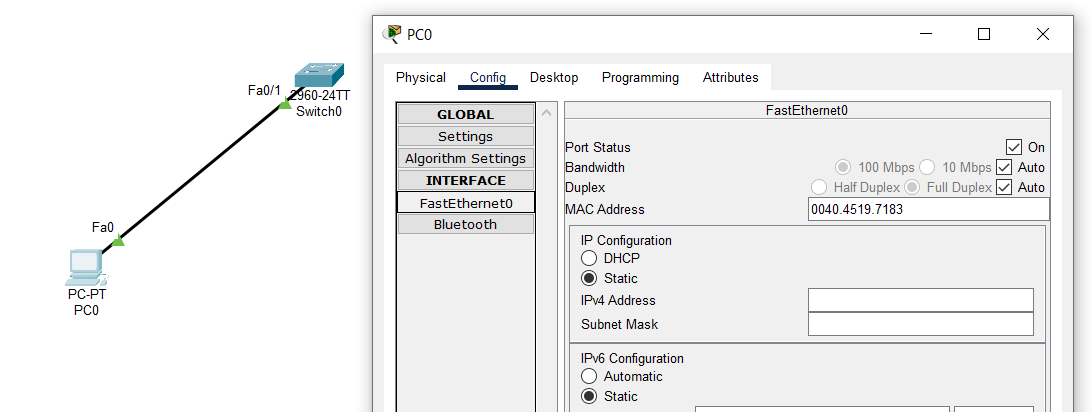
#### Yêu cầu

1. Chỉ có client với địa chỉ MAC: 00-40-45-19-71-83 được sử dụng port fa0/1 trên Switch (tùy vào PC, SV có thể dùng địa chỉ MAC khác).

2. Các client khác gắn vào port fa0/1, port fa0/1 sẽ bị shutdown

3. port fa0/1 sẽ khôi phục lại sau 30 giây.





#### Cấu hình

1. Cấu hình port security. Chỉ có client với địa chỉ MAC: 00-40-45-19-71-83 được sử dụng port fa0/1 trên Switch.

Switch(config)#interface fa0/1

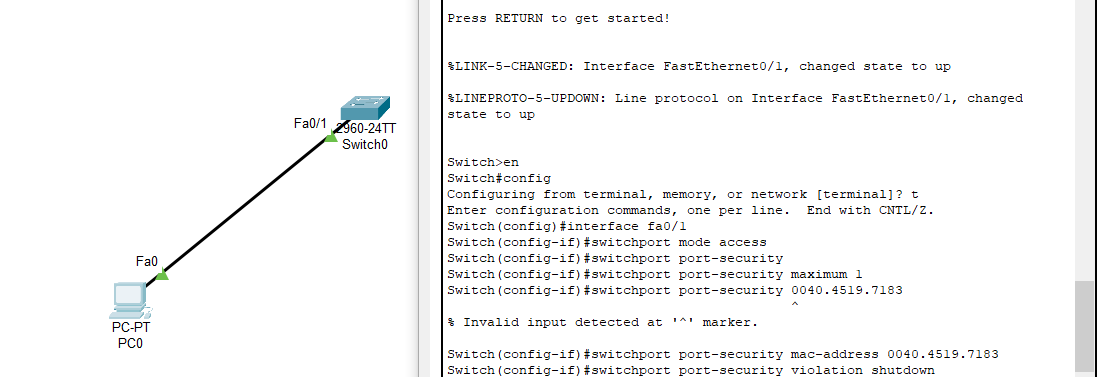
Switch(config-if)#switchport mode access

Switch(config-if)#switchport port-security

*(Switch(config-if)#switchport port-security mac-address 0040.4519.7183)*

Switch(config-if)#switchport port-security maximum 1

Switch(config-if)#switchport port-security mac-address sticky

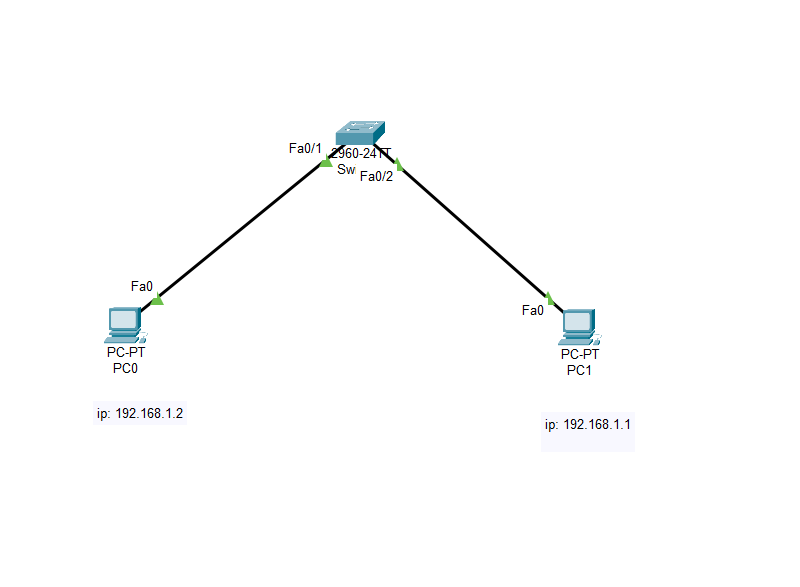


2. Các client khác gắn vào port fa0/1, port fa0/1 sẽ bị shutdown

Switch(config)#interface fa0/1

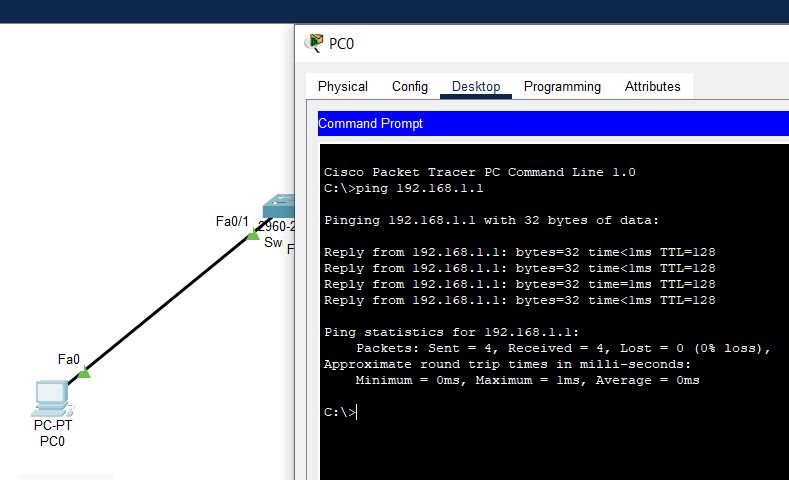
Switch(config-if)#switchport port-security violation shutdown

\_ Tạo thêm một máy PC1 có IP là 192.168.1.1 để kiểm tra

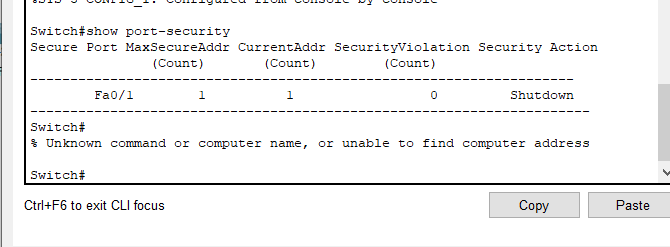




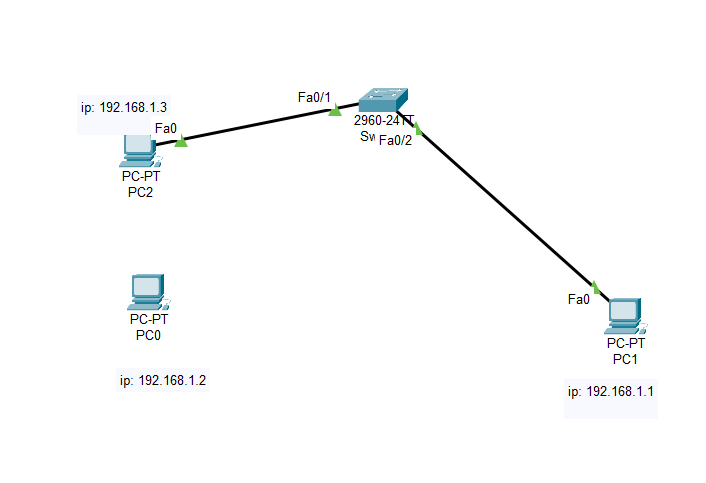
\_ Máy PC0 kết nối được với PC1 có IP là 192.168.1.1



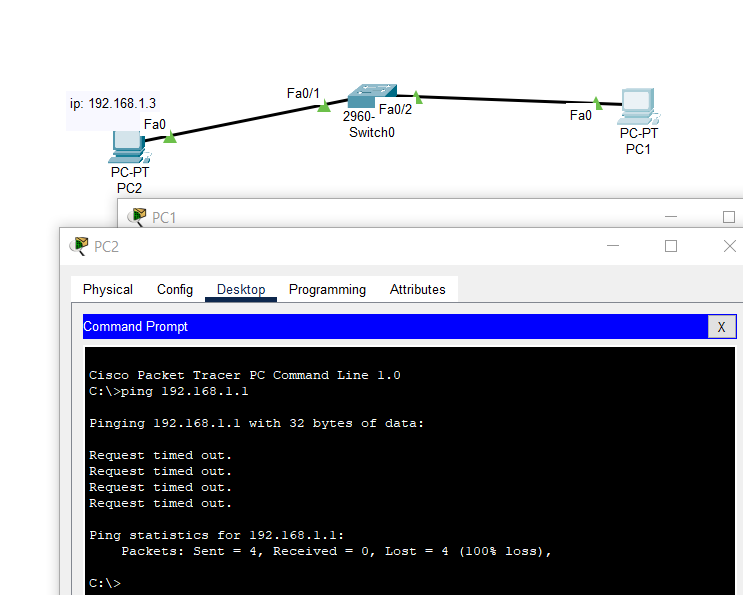
Cổng Fa0/1 của Switch đã được cấu hình: cho phép 1 địa chỉ, và hiện tại có một địa chỉ đã kết nối, chưa máy nào vi phạm, nếu vi phạm xảy ra sẽ shutdown



\_ Tạo thêm máy PC2 có IP là 192.168.1.3, xoá dây nối từ PC0 đến cổng Fa0/1 của Switch, và nối PC2 đến cổng Fa0/1 của Switch.



Vì PC2 đã vi phạm nên cổng Fa0/1 sẽ shutdown, làm cho PC2 không thể kết nối với PC1.



3. port fa0/1 sẽ khôi phục lại sau 30 giây *(các lệnh sau không hỗ trợ trên phần mềm giả lập Packet Tracer – SV không cần làm chức năng này)*

Switch(config)#errdisable detect cause all

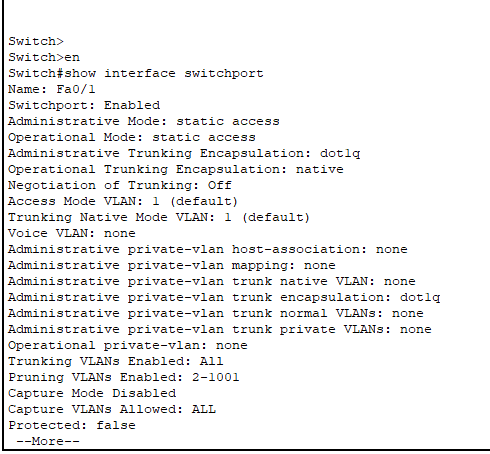
Switch(config)#errdisable recovery cause all

Switch(config)#errdisable recovery interval 30

#### Kiểm tra cấu hình

*show interface switchport*

*show port-security interface*

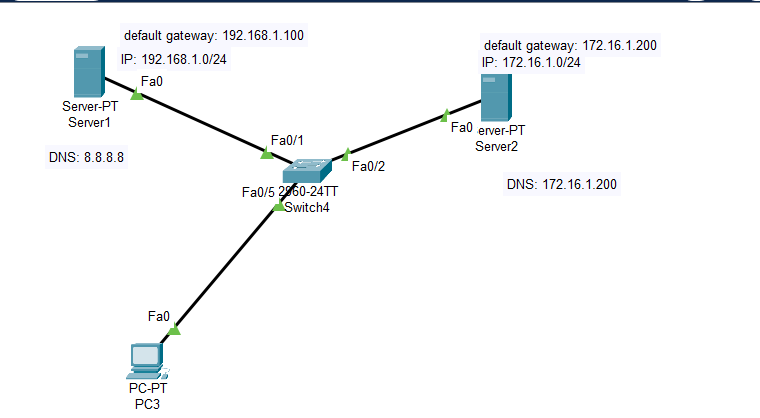


**Câu 2. DHCP snooping**

Chống giả các DHCP server trong hệ thống, chỉ cho phép các client xin IP từ DHCP Server thật *(sử dụng phần mềm giả lập Packet Tracer hoặc EVE)*

#### Topology





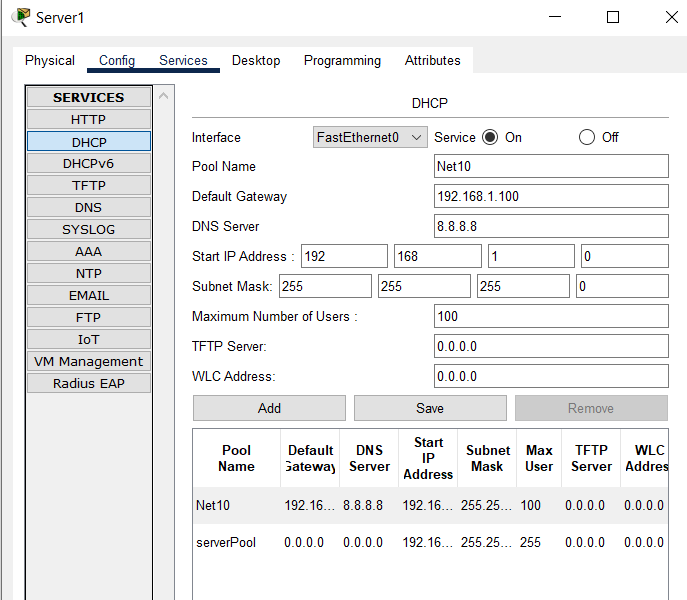
Yêu cầu

1. Cấu hình DHCP Server.

DHCP Server1: Cấp dãy địa chỉ IP : 192.168.1.0/24

Defaul Gateway : 192.168.1.100

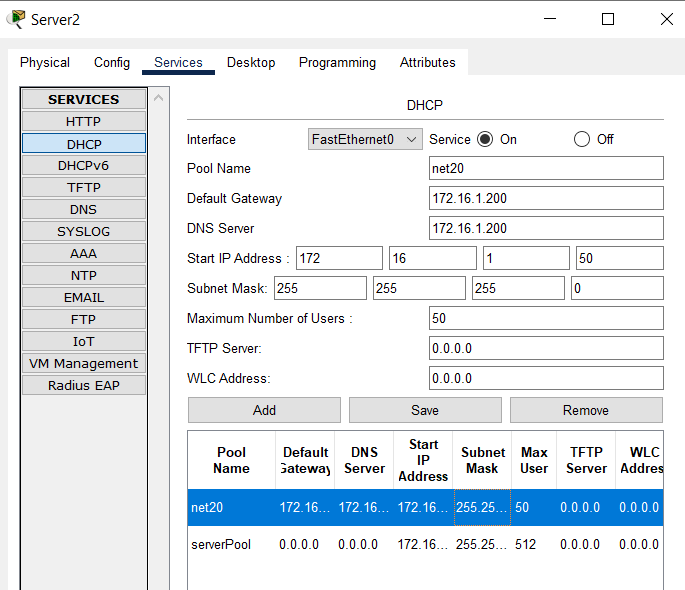
DNS: 8.8.8.8



DHCP Server2: Cấp dãy địa chỉ IP : 172.16.1.0/24

Defaul Gateway : 172.16.1.200

DNS: 172.16.1.200



2. Cấu hình DHCP snooping trên Switch, so cho các client chỉ xin địa chỉ IP từ DHCP trên DHCP Server1.

Cấu hình DHCP snooping trên Switch, so cho các client chỉ xin địa chỉ IP từ DHCP trên DHCP Server 1.

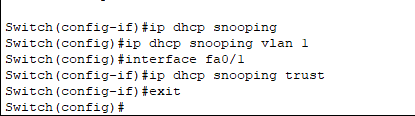
Switch(config)#ip dhcp snooping

Switch(config)#ip dhcp snooping vlan 1

Switch(config)#interface fa0/2 (nối với DHCP thật)

Switch(config-if)#ip dhcp snooping trust

Switch(config-if)#exit



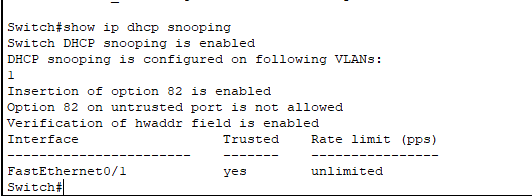
#### Kiểm tra cấu hình

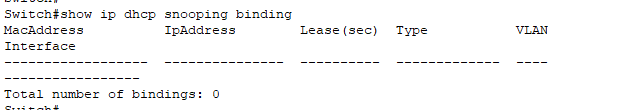
*show ip dhcp snooping*

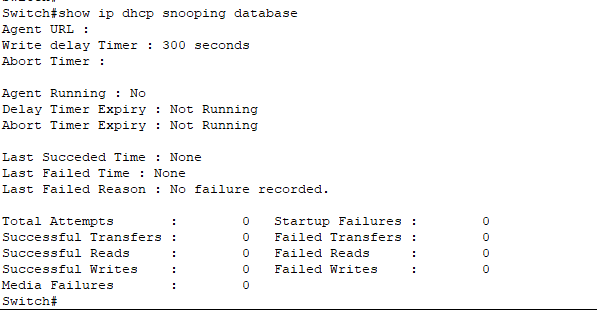
*show ip dhcp snooping binding*

*show ip dhcp snooping database*

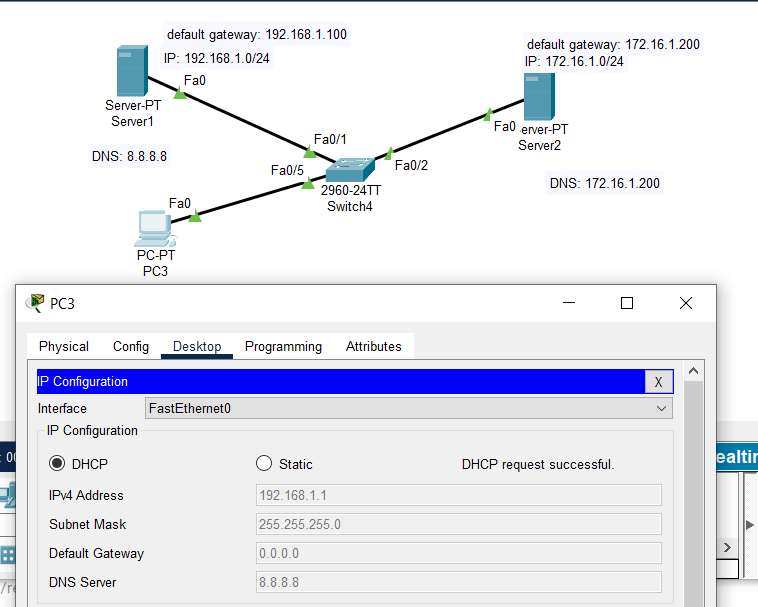
*show ip source binding*







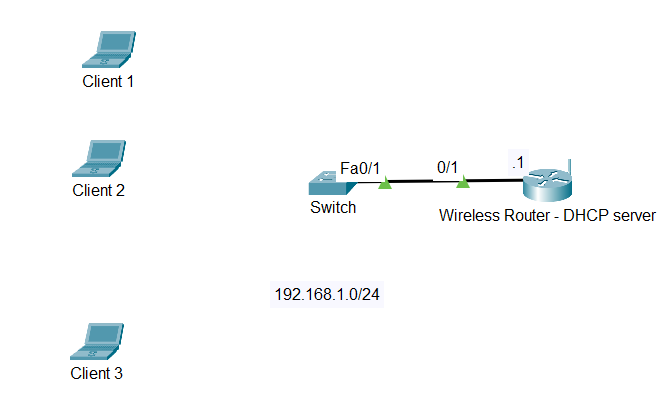
Máy PC3 đã nhận được IP: 192.168.1.1 do Server1 cấp.

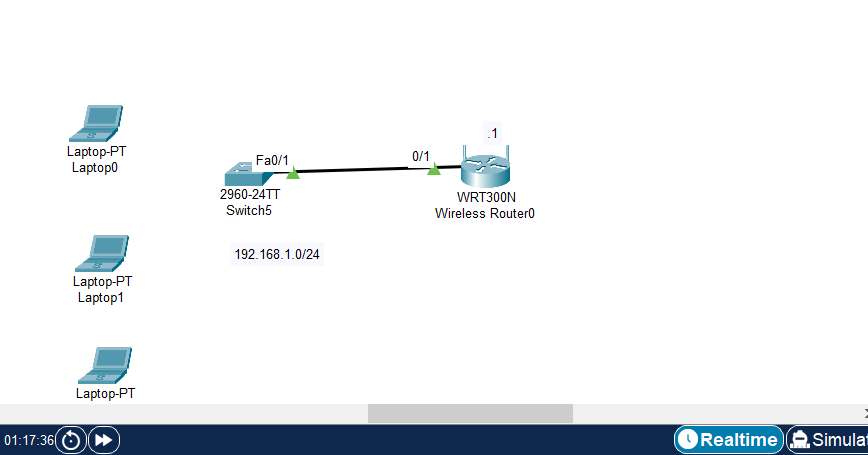
* 

**Câu 3. Wifi Security**

1. **Cấu hình WiFi cơ bản**

* MAC filtering
* WPA2 – Personal

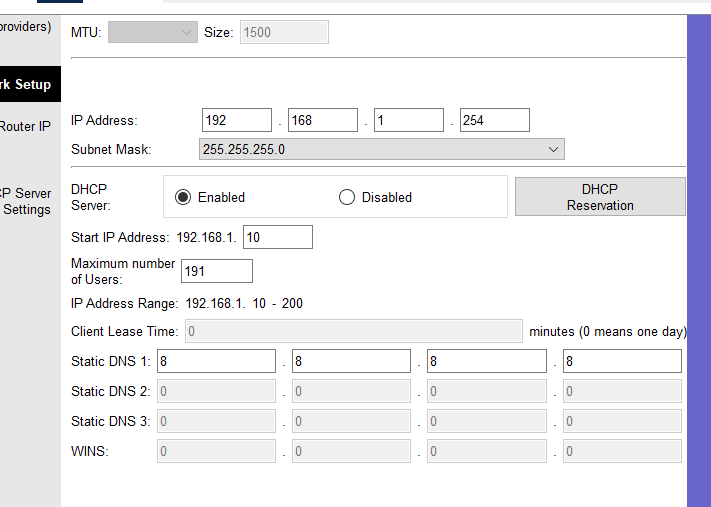


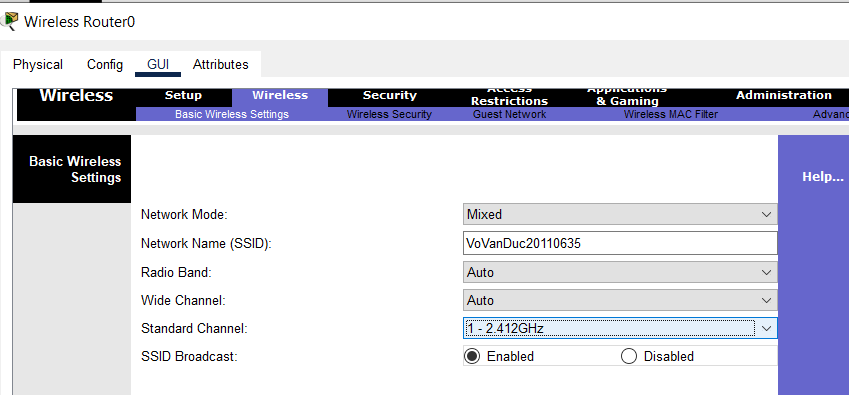


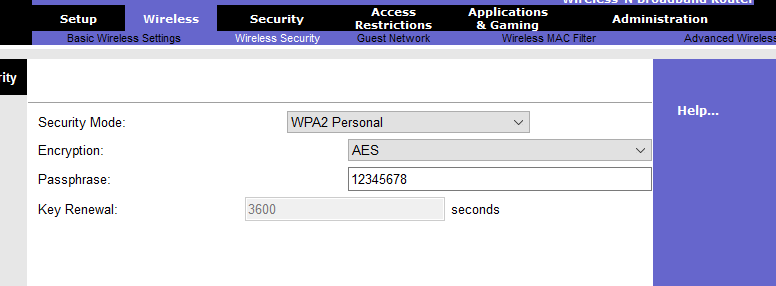
* AP có IP 192.168.1.1/24
* Mạng nội bộ được hoạch định với IP: 192.168.1.0/24

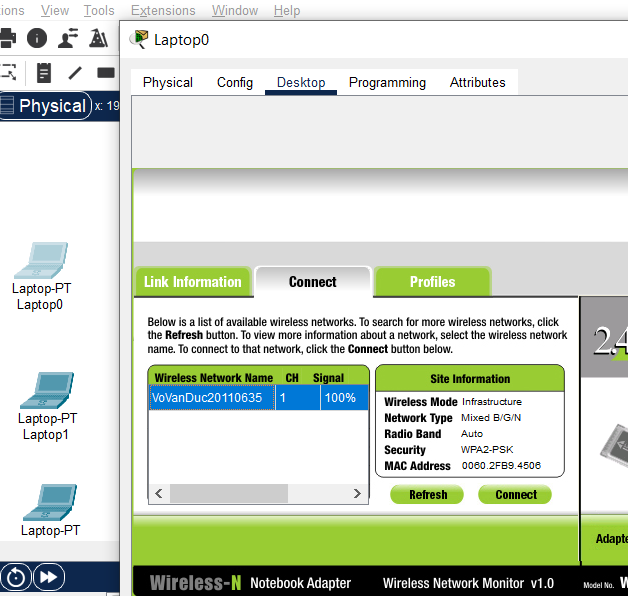
**Yêu cầu:**

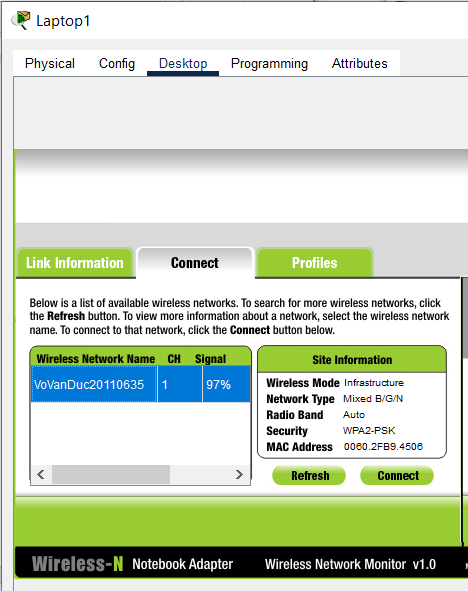
* Cấu hình AP – tên SSID SV tự cho
* Cấu hình AP làm DHCP server, các thông số IP cấp phát
  + Network: 192.168.1.0/24
  + IP range 192.168.1.10 – 192.168.1.200
  + Default gateway: 192.168.1.1
  + DNS: 8.8.8.8
* Cấu hình AP chỉ cho phép máy Client 1 và Client 2 sử dụng mạng WiFi (MAC filtering)
* Cấu hình WPA2-personal (password SV tự cho)

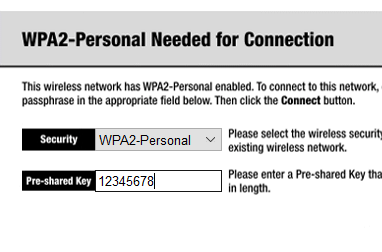


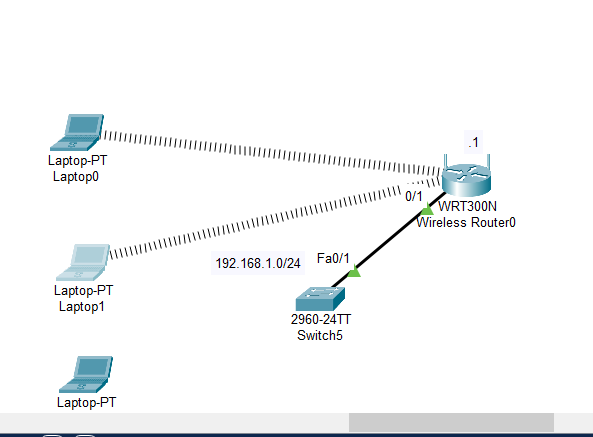


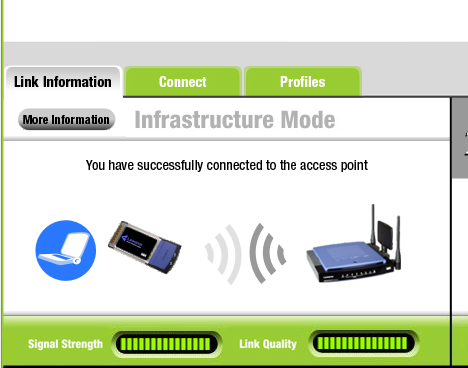




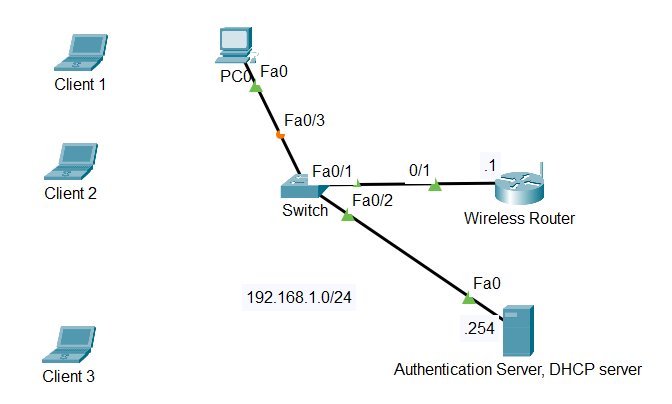








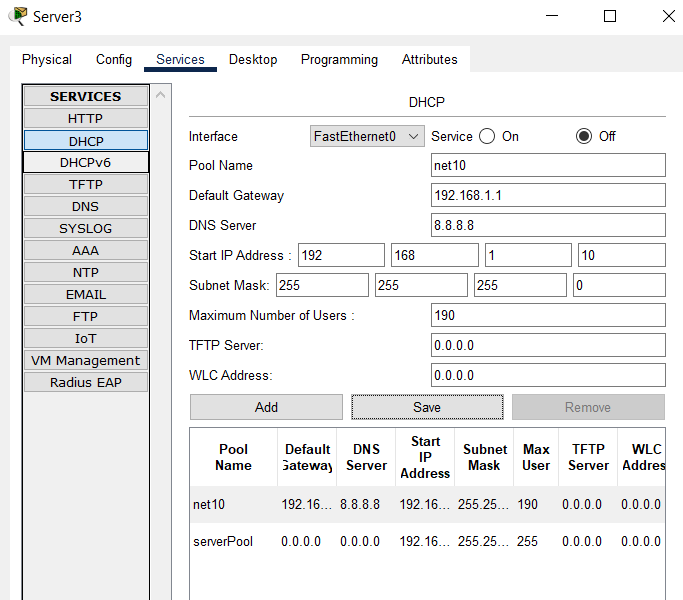
1. **Cấu hình chứng thực người dùng WiFi dùng Radius Server**

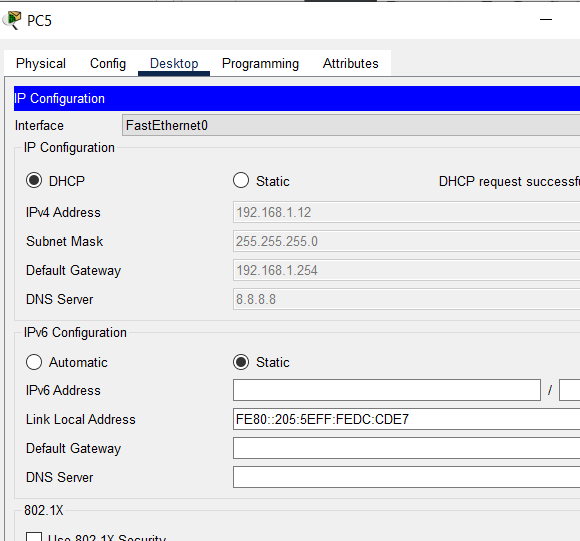


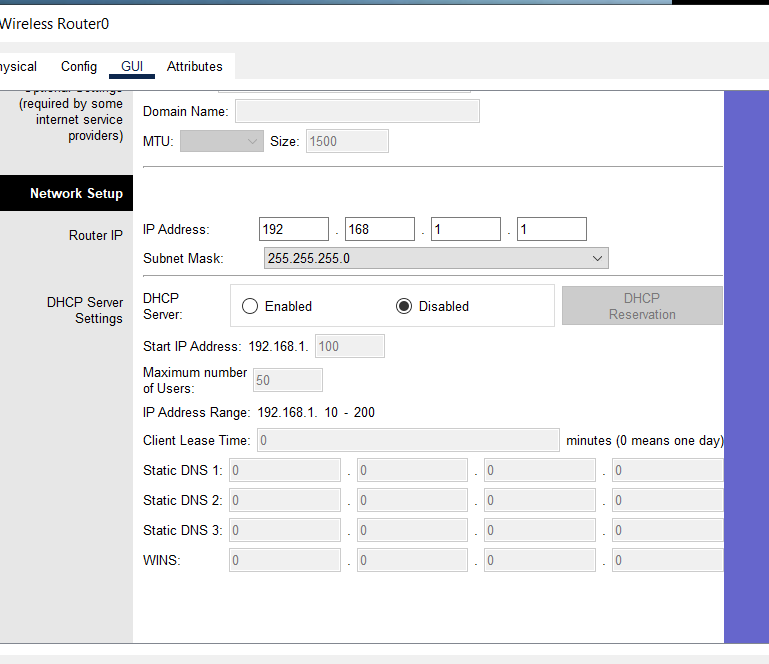
* AP có IP 192.168.1.1/24
* Mạng nội bộ được hoạch định với IP: 192.168.1.0/24

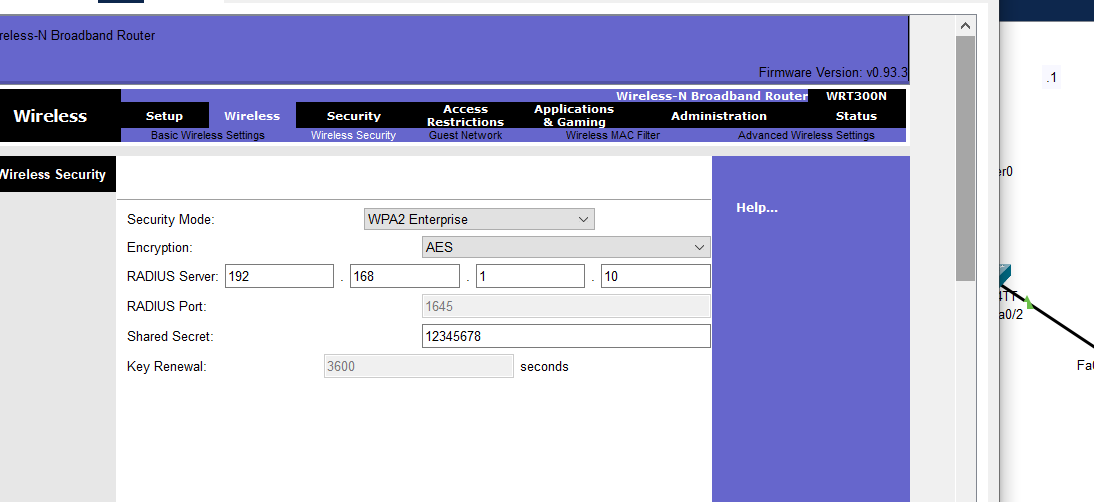
**Yêu cầu:**

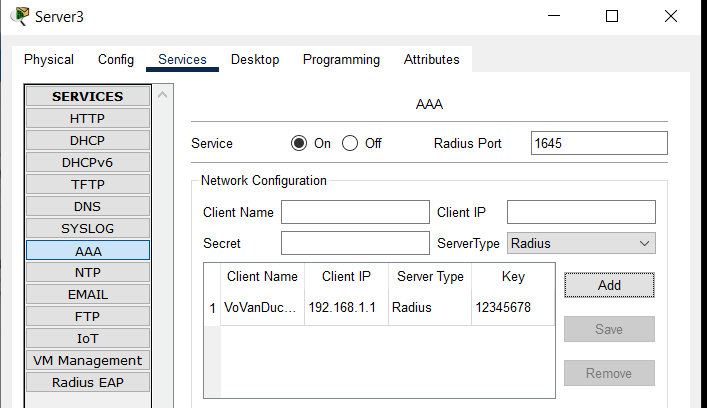
* Cấu hình AP – tên SSID SV tự cho
* Cấu hình Authentication Server (Radius server), tạo account để chứng thực người dùng Wifi
* AP đóng vai trò là Authenticator (dùng WPA2-Enterprise)
* Authentication Server cũng đóng vai trò là DHCP server cấp pháp IP động cho các client trong mạng. Các thông số IP cấp phát như sau:
  + Network: 192.168.1.0/24
  + IP range 192.168.1.10 – 192.168.1.200
  + Default gateway: 192.168.1.1
  + DNS: 8.8.8.8

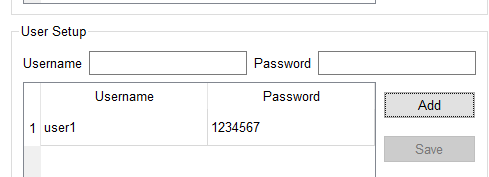


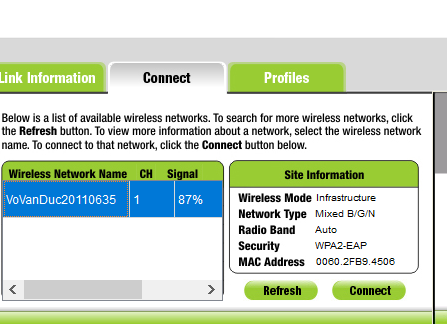


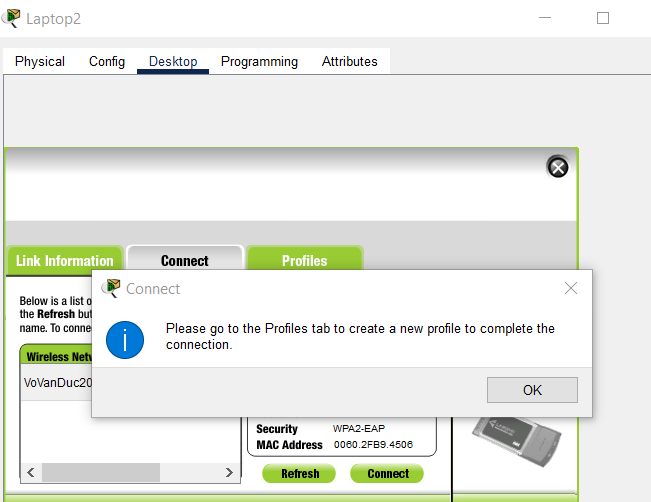


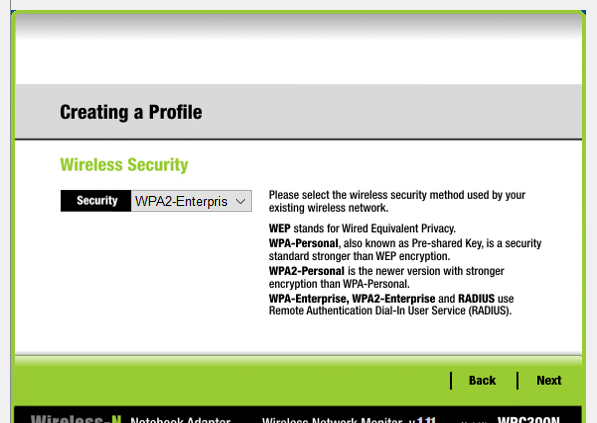


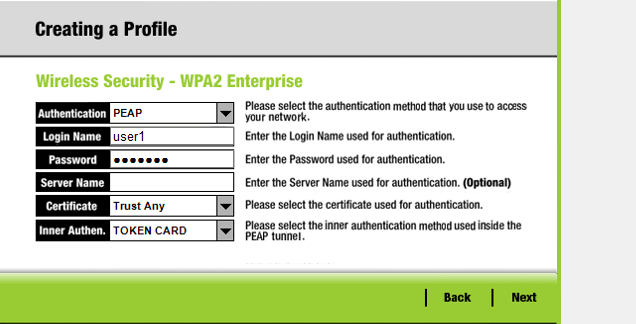


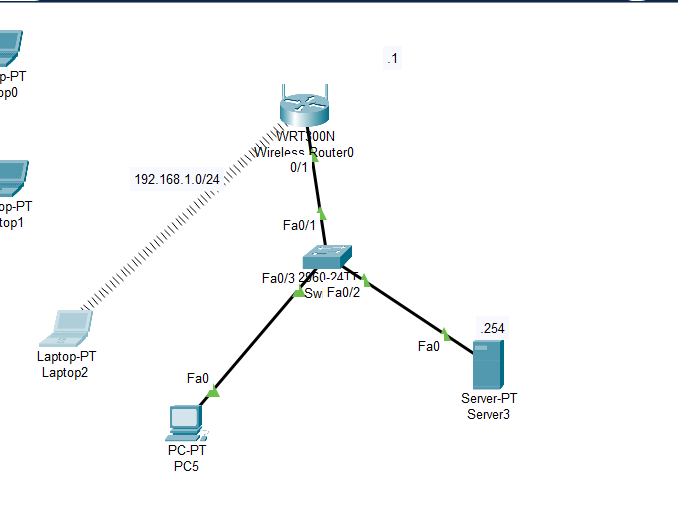












**Câu 3. Firewall**

* *Sinh viên tự chọn một Firewall dạng VMWare để thử nghiệm (Fortigate, Checkpoint,…)*

Topology



Thực hiện các rule:

* Cho phép các PC bên trong mạng nội bộ ra ngoài Internet
* Kiểm soát truy cập Web
* Kiểm soát port truy cập
* Kiểm soát ứng dụng truy cập
* Thực hiện các phương thức khác

SV có thể sử dụng các FW dạng VMWare: Fortigate, Checkpoint,…

**Câu 4. Snort-IDS**



* Cài đặt Snort
* Dùng một số công cụ tấn công và mô tả kết quả xử lý trên Snort

**Câu 5. Network Monitoring System**

* Thực hiện giám sát mạng với phần mềm PRTG
* Cấu hình chức năng giám sát performance (RAM, CPU), giám sát một số dịch vụ mạng (DHCP, Web,…), giám sát dung lượng đĩa trên Server
* Thiết lập ngưỡng cảnh báo