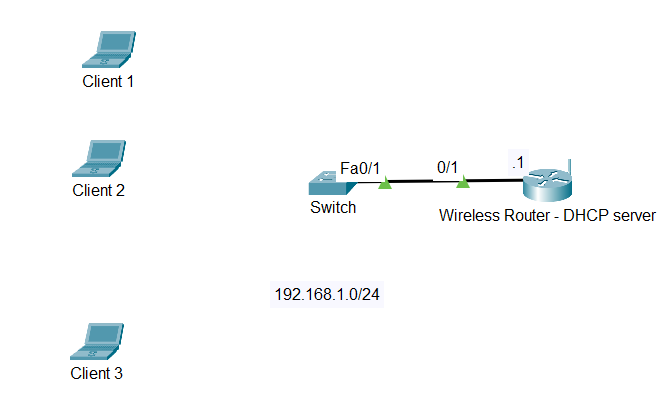
**Lab 4. WIFI SECURITY**

*SV thực hiện và trình bày theo từng kịch bản (có mô tả tình huống, cách thức thực hiện, cách thức kiểm tra kết quả) dựa trên các yêu cầu cơ bản như sau:*

1. ***(3 điểm)* Cấu hình WiFi cơ bản**

* MAC filtering
* WPA2 – Personal

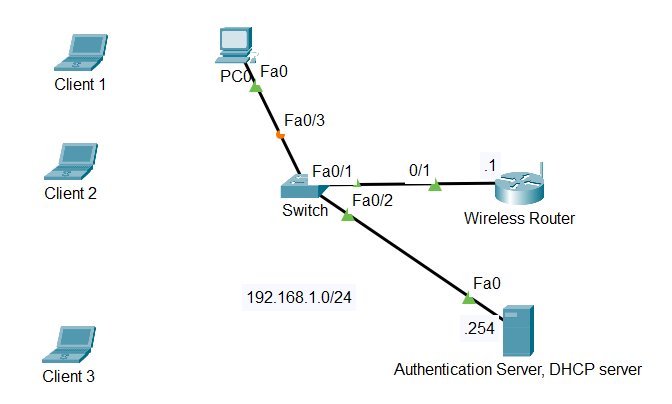


* AP có IP 192.168.1.1/24
* Mạng nội bộ được hoạch định với IP: 192.168.1.0/24

**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. ***(3 điểm)* 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

**3) *(4 điểm)* Tấn công mạng WiFi**

Chọn 1 kịch bản tấn công mạng WiFi. Phân tích & đưa ra giải pháp phòng chống.

Ví dụ:

* Tìm cách vào được mạng WiFi (trường hợp mạng WiFi chỉ cho phép các máy có địa chỉ MAC cho trước)
* Đã ở trong mạng WiFi, tấn công Man-in-the-Middle
* …..