

**ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH**  
**TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN**



**BÁO CÁO**

**Lab 4. WIFI SECURITY**

**Họ và tên: Nguyễn Bửu Thạch**

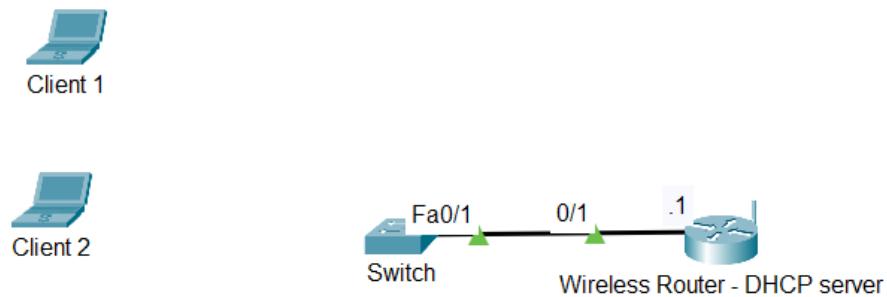
**MSSV:20120576**

**Môn học: An ninh máy tính**

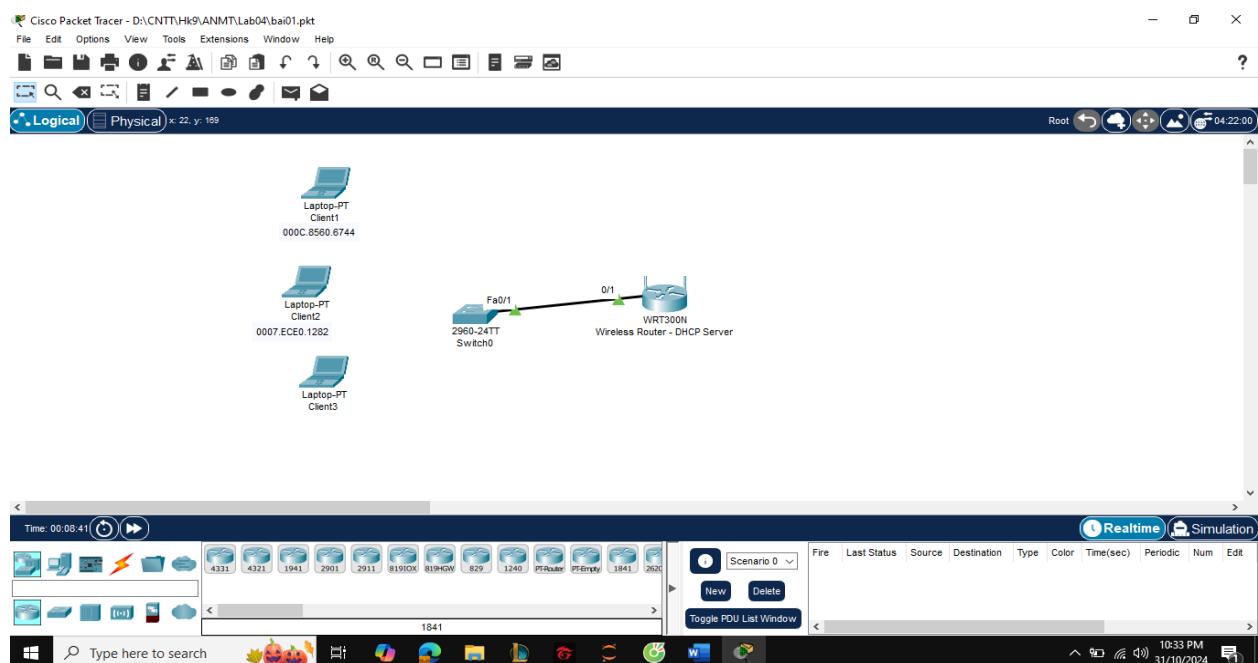
Thành phố Hồ Chí Minh-2024

### 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



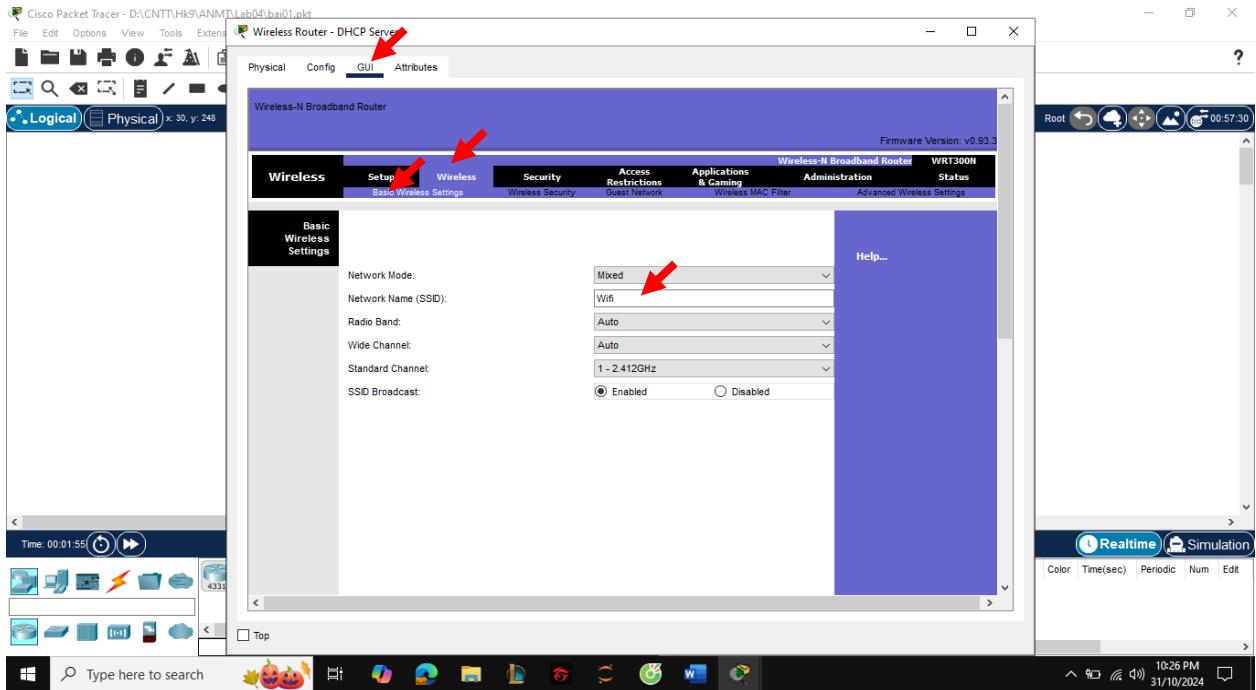
#### Yêu cầu:

- Cấu hình AP – tên SSID SV tự cho
- Cấu hình AP làm DHCP server, các thông số IP cấp phát
  - o Network: 192.168.1.0/24
  - o 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)

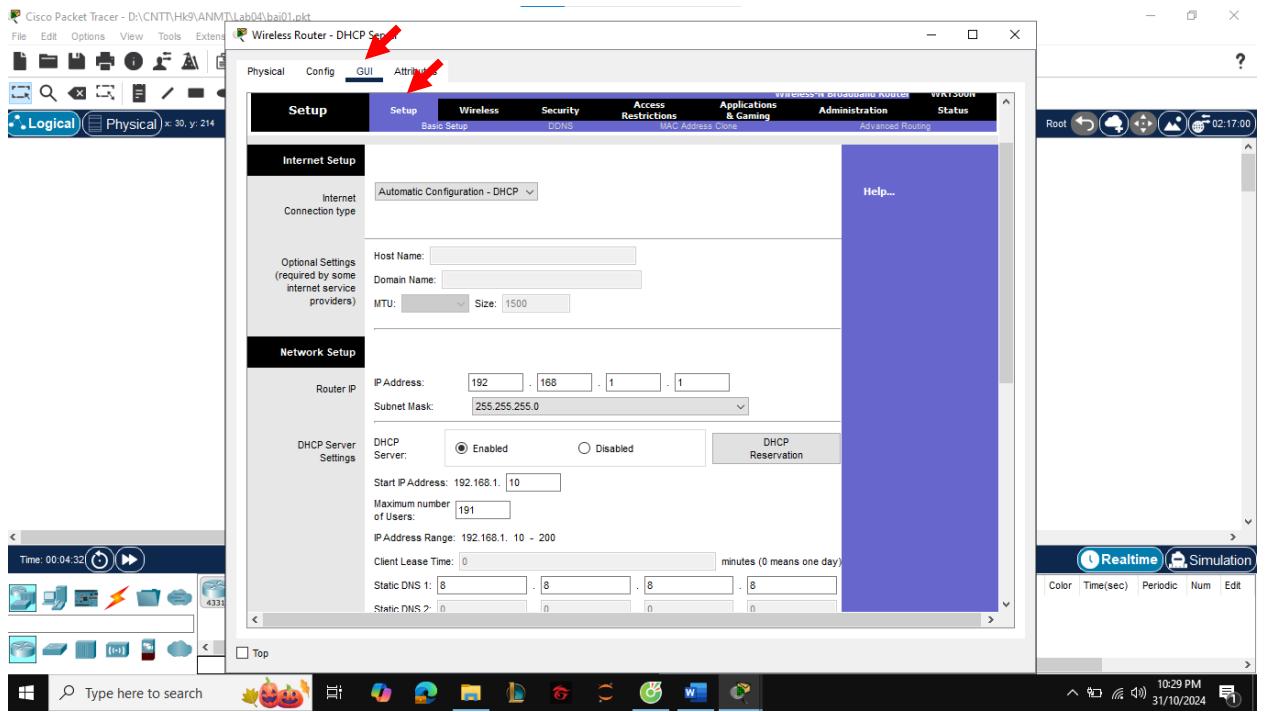
### Các bước thực hiện:

- Cấu hình AP – tên SSID SV tự cho



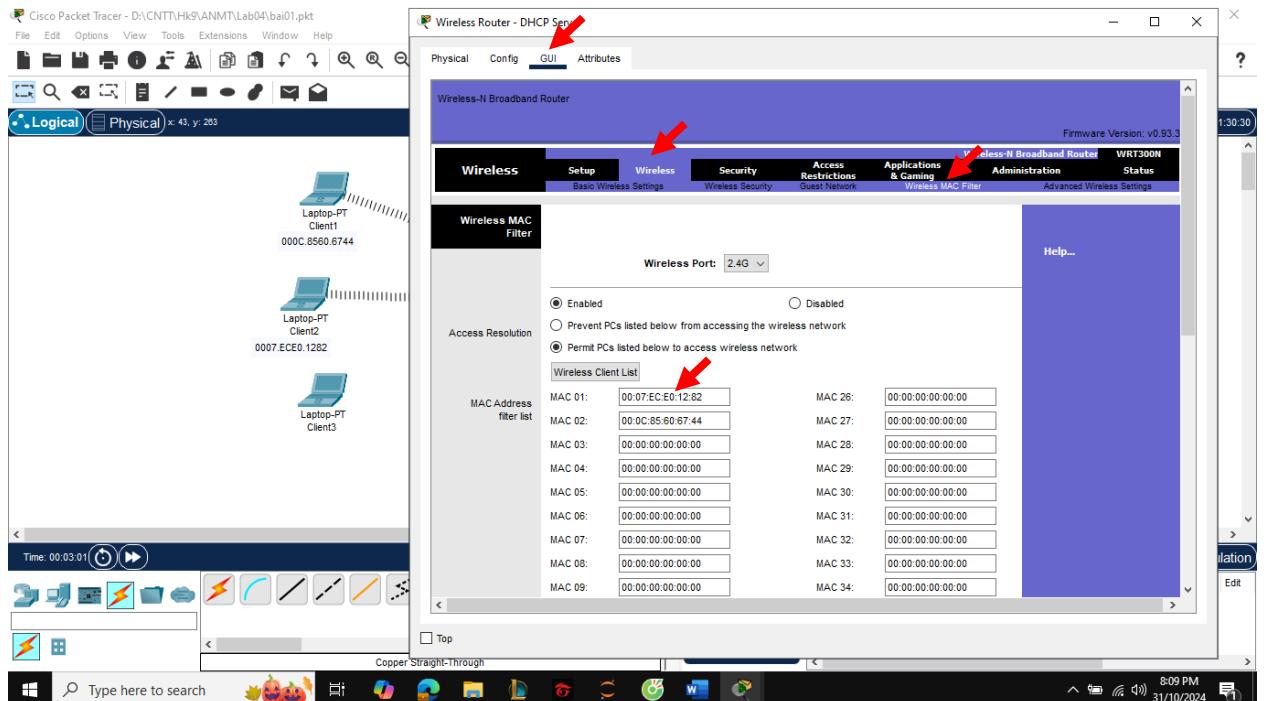
- Cấu hình AP làm DHCP server, các thông số IP cấp phát
  - Network: 192.168.1.0/24
  - IP range 192.168.1.10 – 192.168.1.200
  - Default gateway: 192.168.1.1
  - DNS: 8.8.8.8

Thực hiện như bên dưới và nhập các thông số IP cấp phát. Rồi nhấn chọn Save Settings:



- Cấu hình AP chỉ cho phép máy Client 1 và Client 2 sử dụng mạng WiFi (MAC filtering)

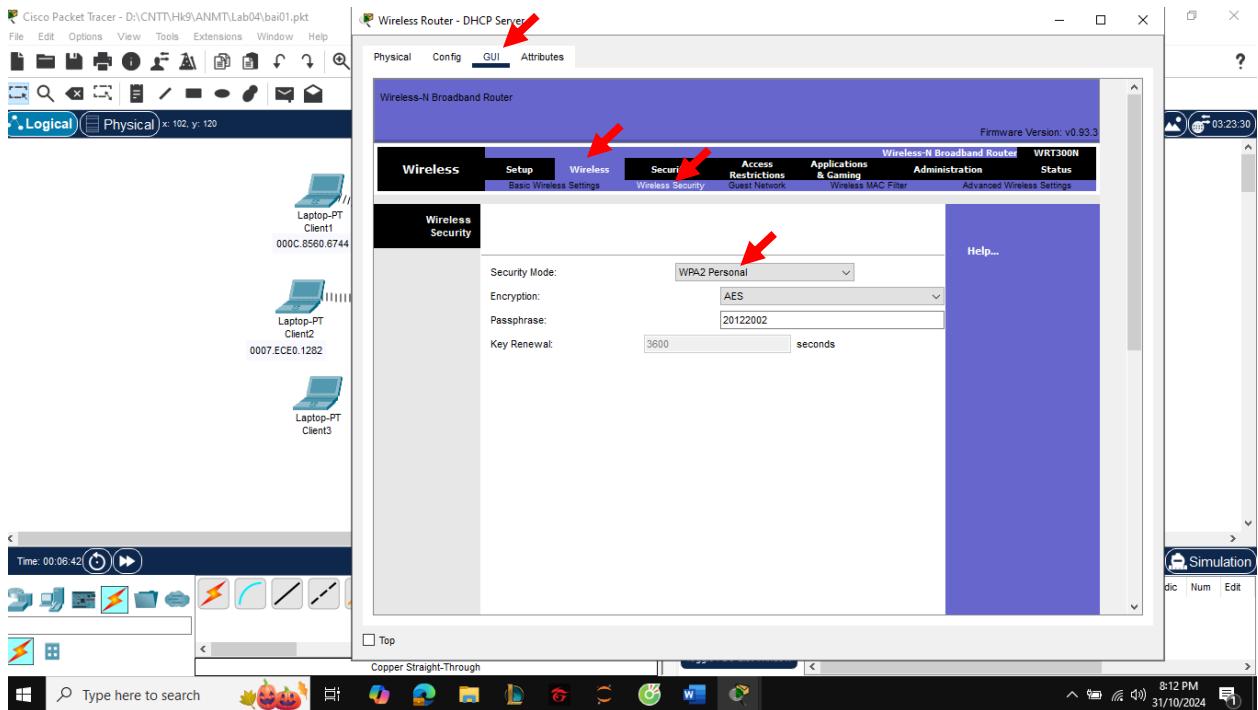
Thực hiện các bước như bên dưới. Sau đó nhập địa chỉ MAC của Client1 và Client2 . Cuối cùng nhấn Save Settings



- Cấu hình WPA2-personal (password SV tự cho)

Thực hiện các bước như hình . Rồi nhấn chọn Save Settings

- Trong Security Mode, chọn WPA2-Personal
- Trong Passphrase, nhập mật khẩu để khởi tạo (20122002)

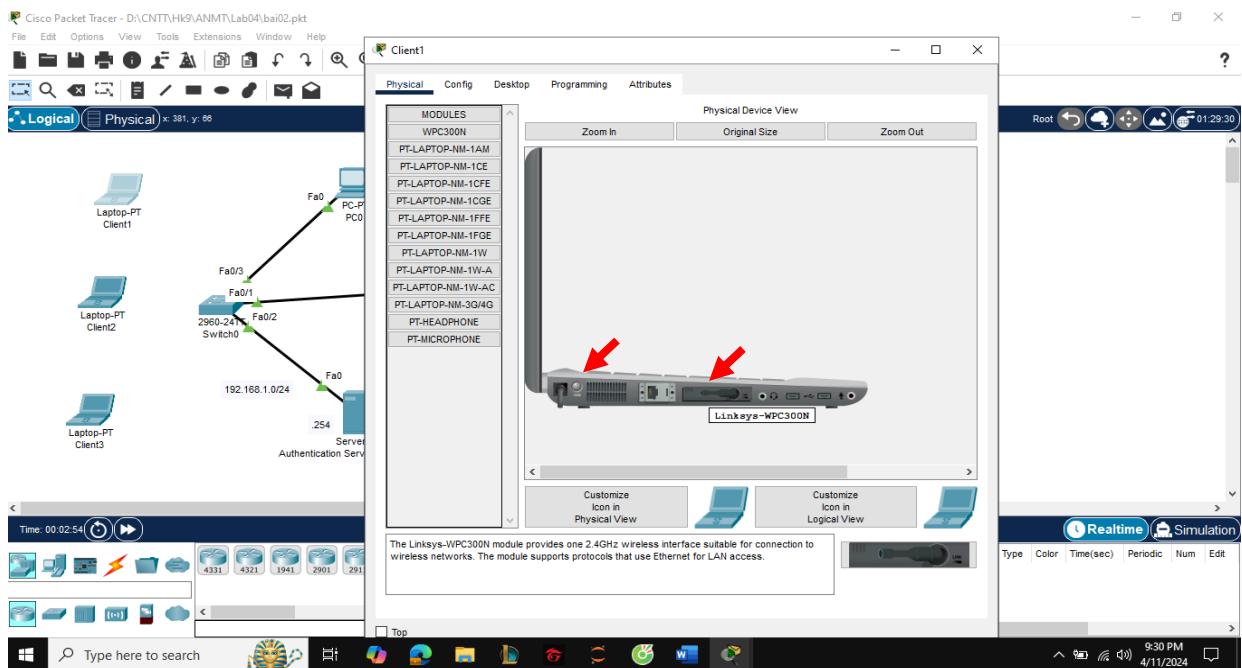


### Cách thức kiểm tra:

#### Trước khi kiểm tra. Ta cần thực hiện bước sau:

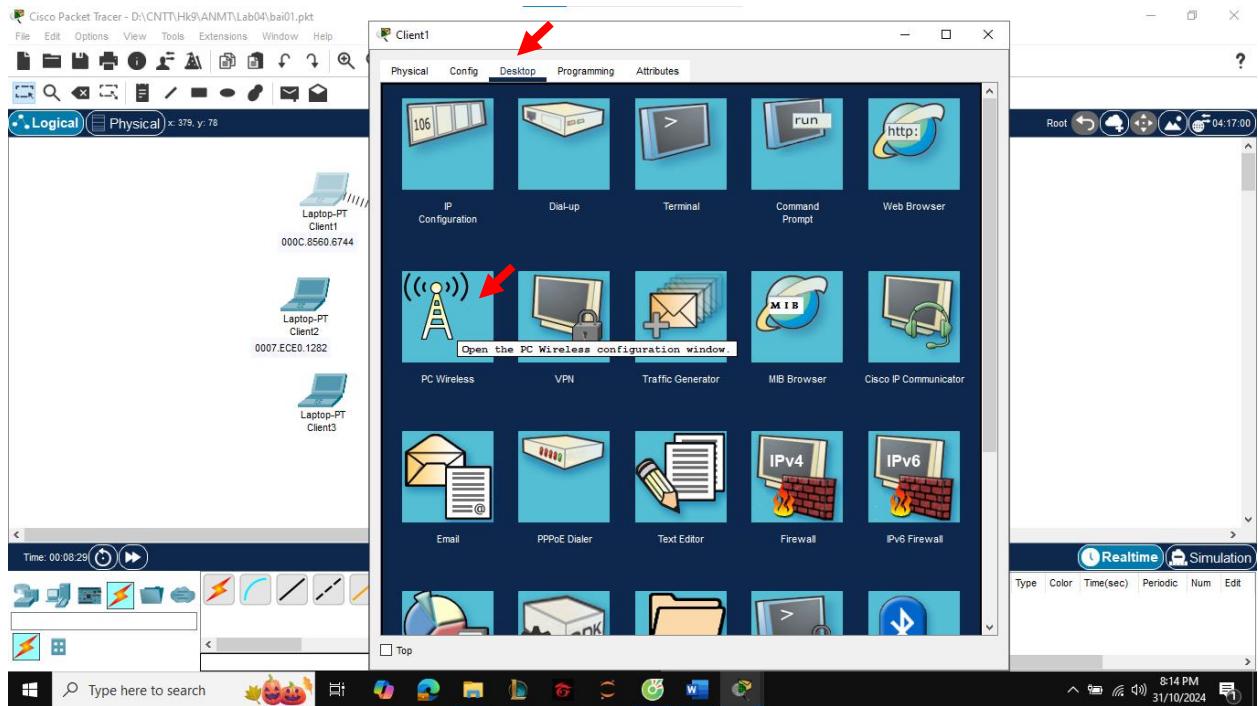
Thay đổi MODULES của 3 client thành WPC300N để hỗ trợ kết nối với mạng không dây

Bằng cách tắt nguồn của client. Sau đó đổi MODULES phù hợp. Rồi bật nguồn trở lại

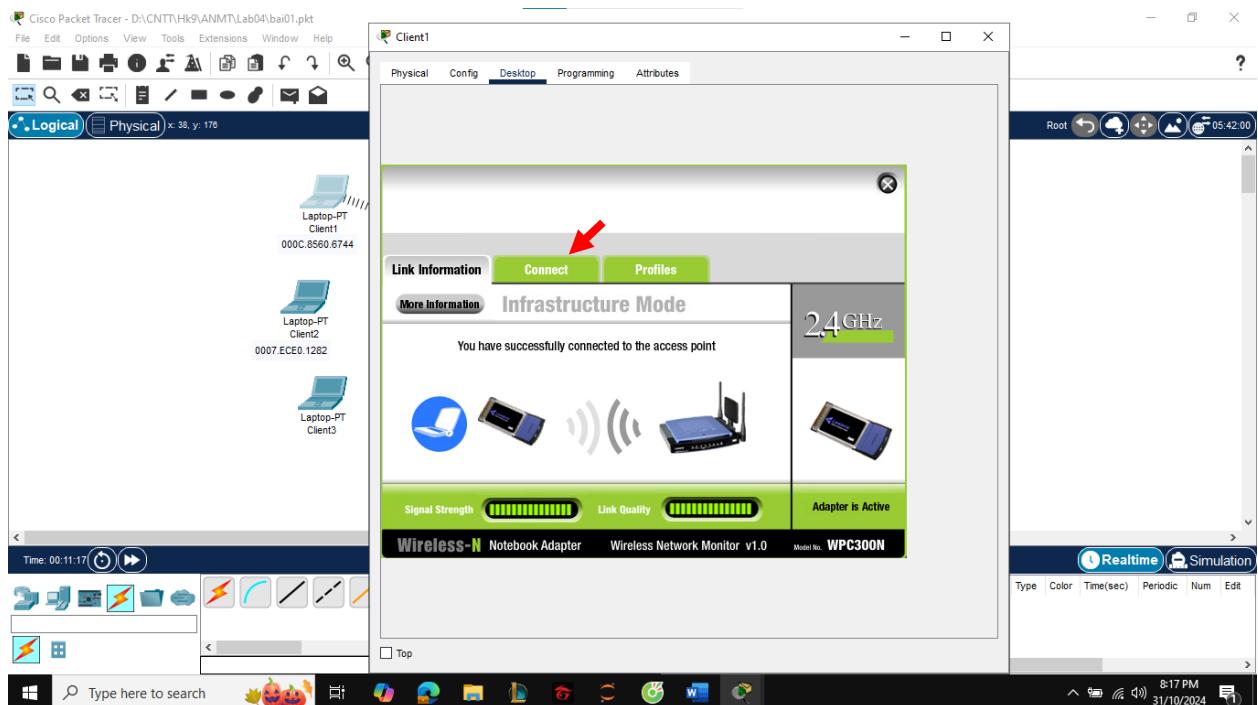


## Thực hiện kiểm tra kết quả:

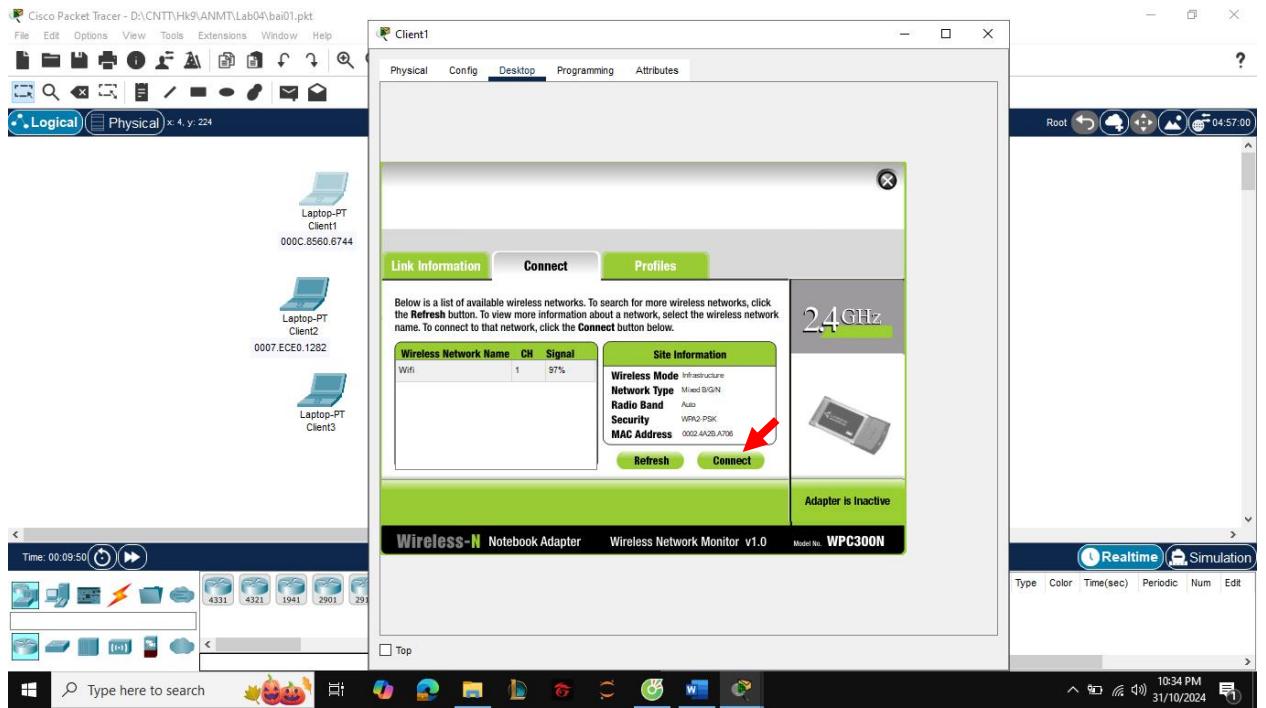
B1: Chọn client. Sau đó chọn Desktop và nhấn chọn PC Wireless



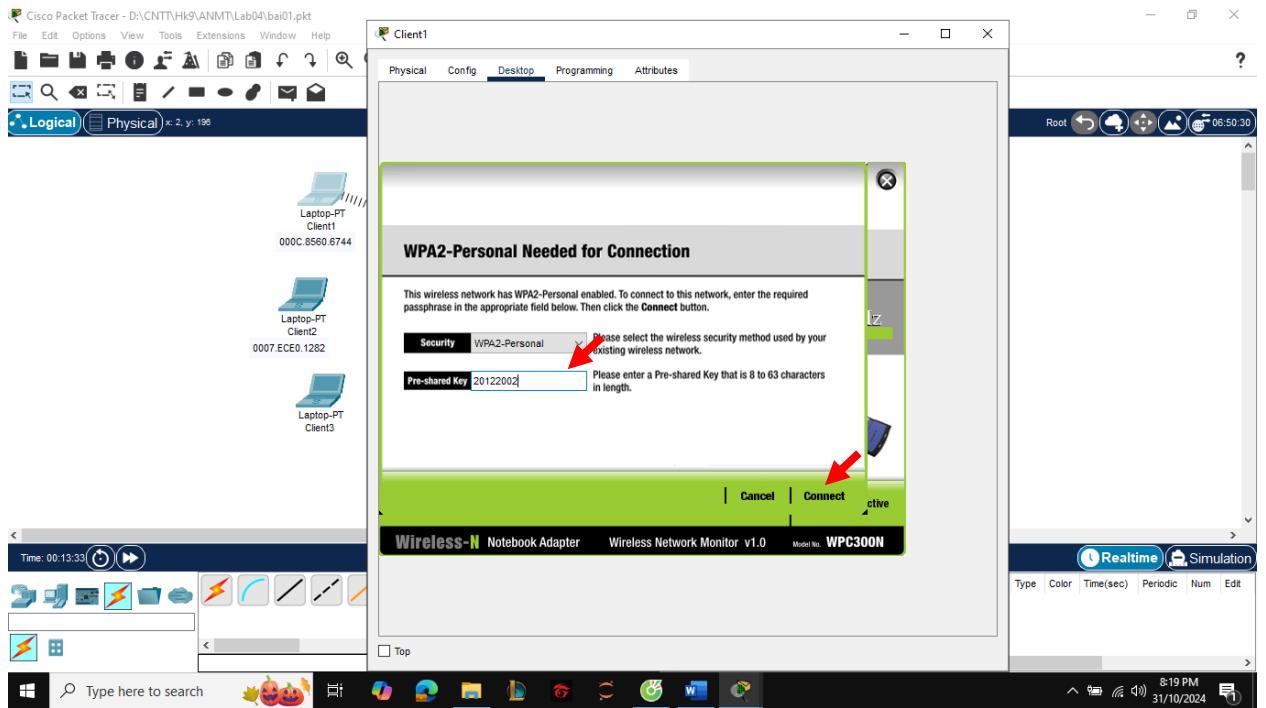
B2: Chọn Connect.



B3: Chọn Connect bên dưới :

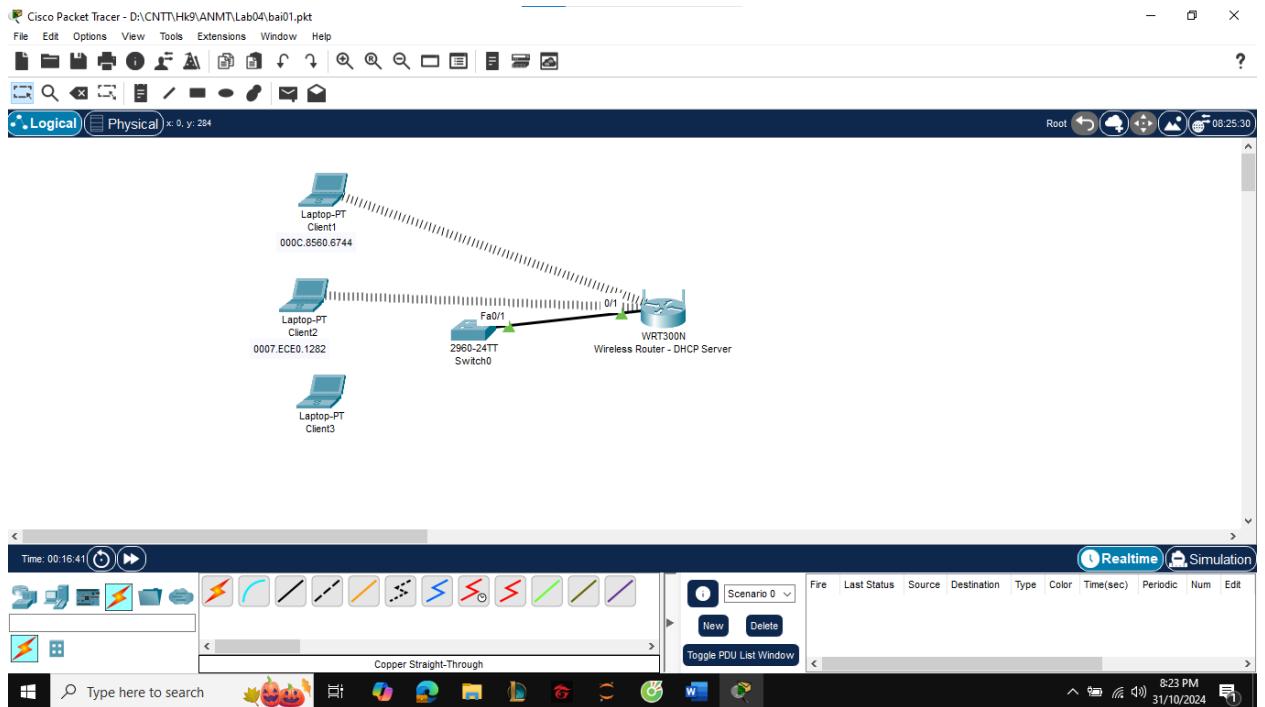


#### B4: Nhập password . Rồi nhấn Connect

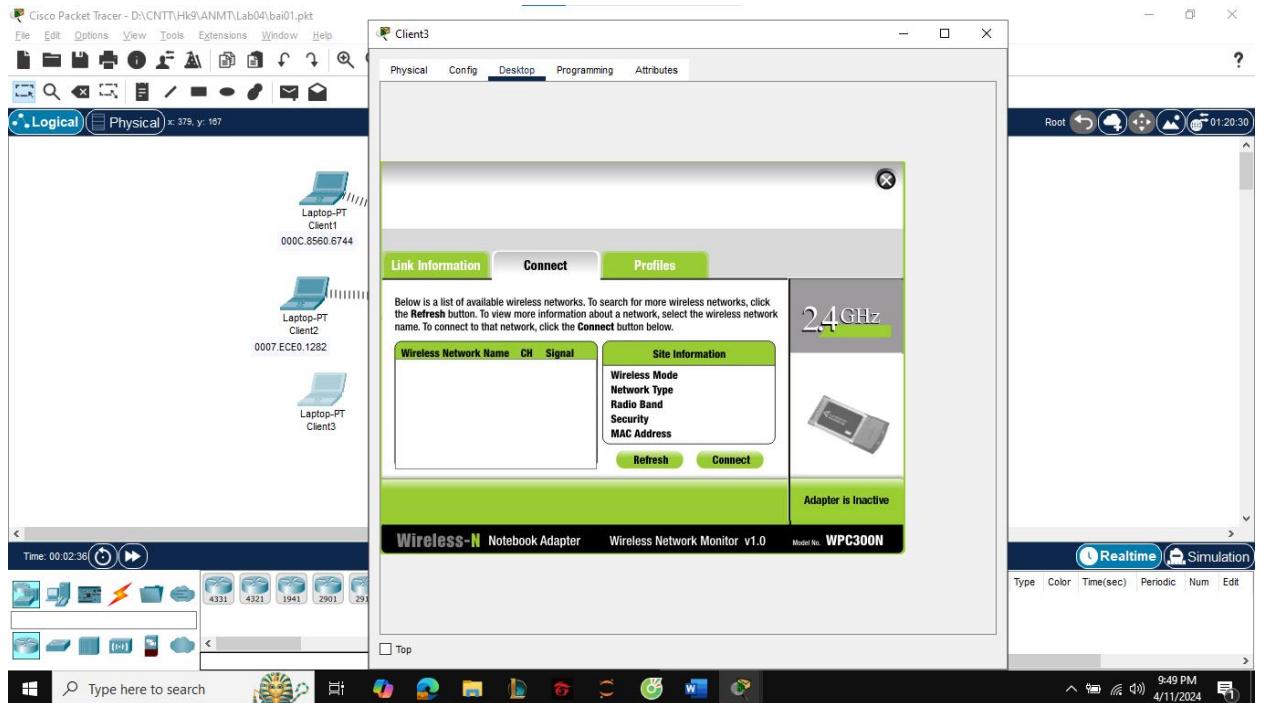


Làm tương tự với Client2

## Kết quả:

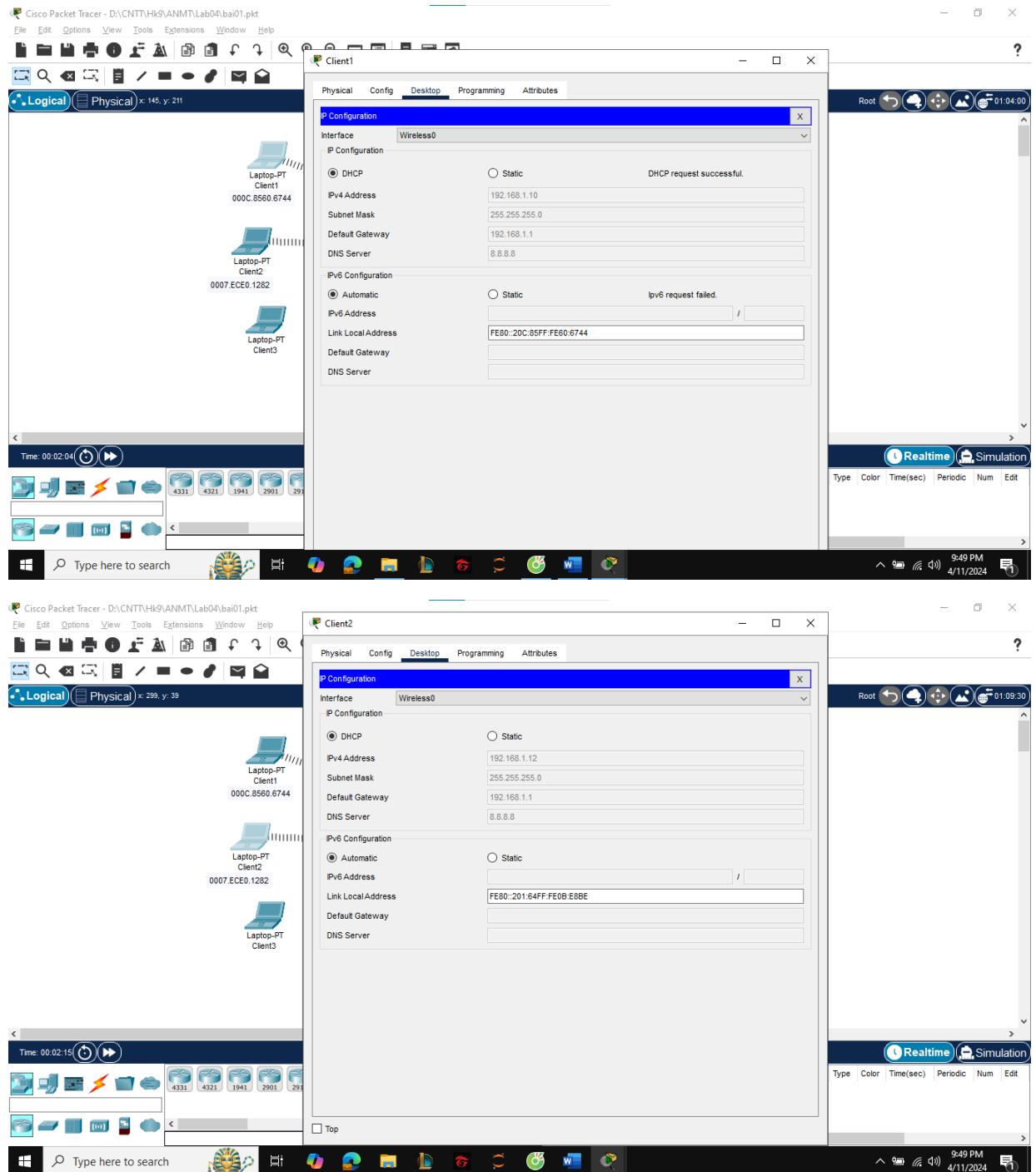


⇒ Chỉ máy Client 1 và Client 2 sử dụng mạng WiFi

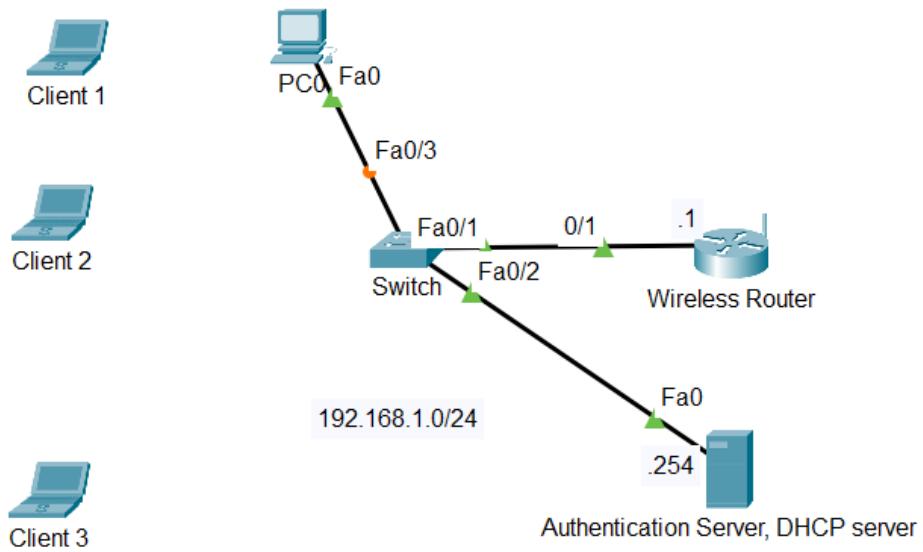


⇒ Vì chỉ cho phép Client 1 và Client 2 sử dụng mạng WiFi nên ở Client3 sẽ không tìm thấy WiFi để kết nối.

**Kiểm tra địa chỉ IP của client do AP cấp phát**



## 2. (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:**

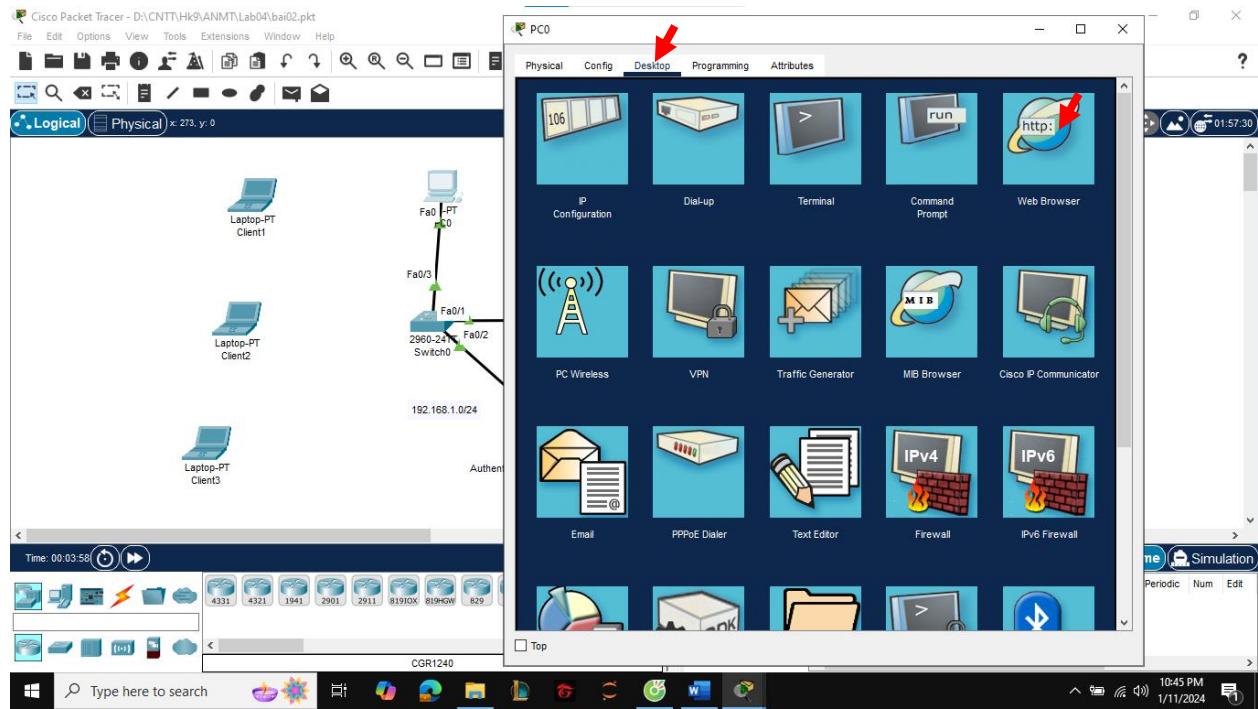
- Cấu hình AP – tên SSID SV tự cho
- Cấu hình Authentication Server (Radius server), tạo account để chứng thực người dùng Wifi
- AP đóng vai trò là Authenticator (dùng WPA2-Enterprise)
- Authentication Server cũng đóng vai trò là DHCP server cấp phép IP động cho các client trong mạng. Các thông số IP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

### **Các bước thực hiện:**

- Cấu hình AP – tên SSID SV tự cho

Chúng ta sẽ cấu hình AP sử dụng PC Web Brower

## B1: Chọn PC0

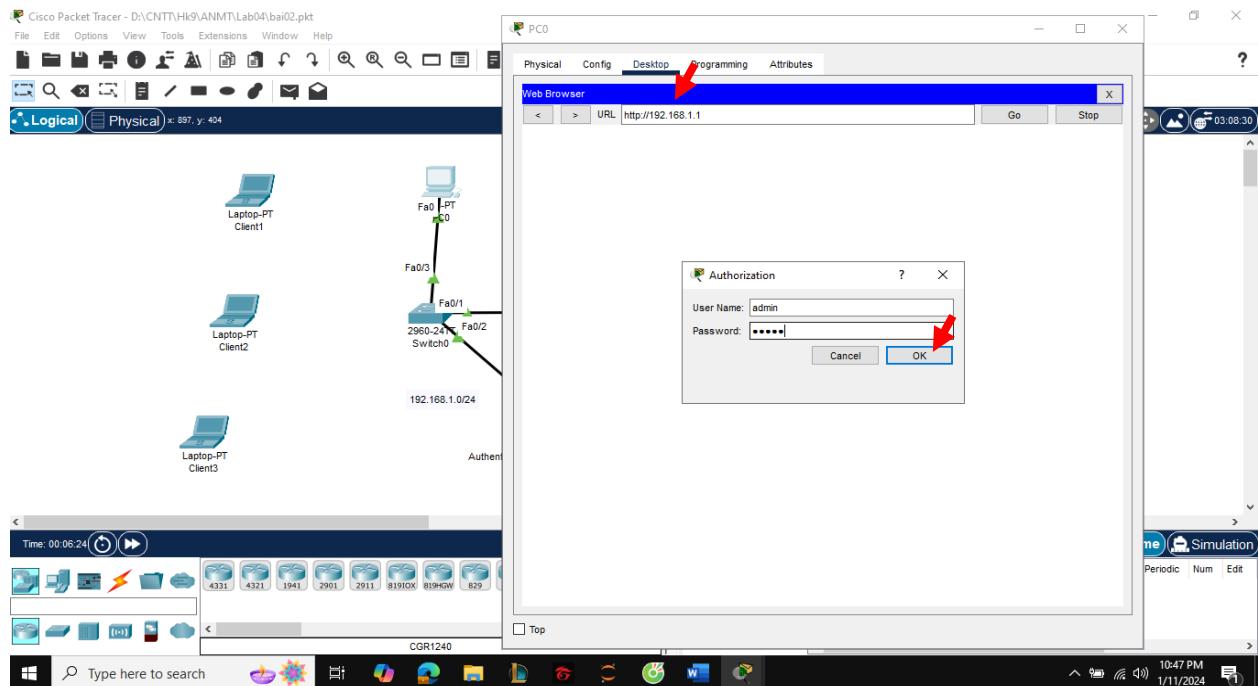


B2: Nhập URL: 192.168.1.1

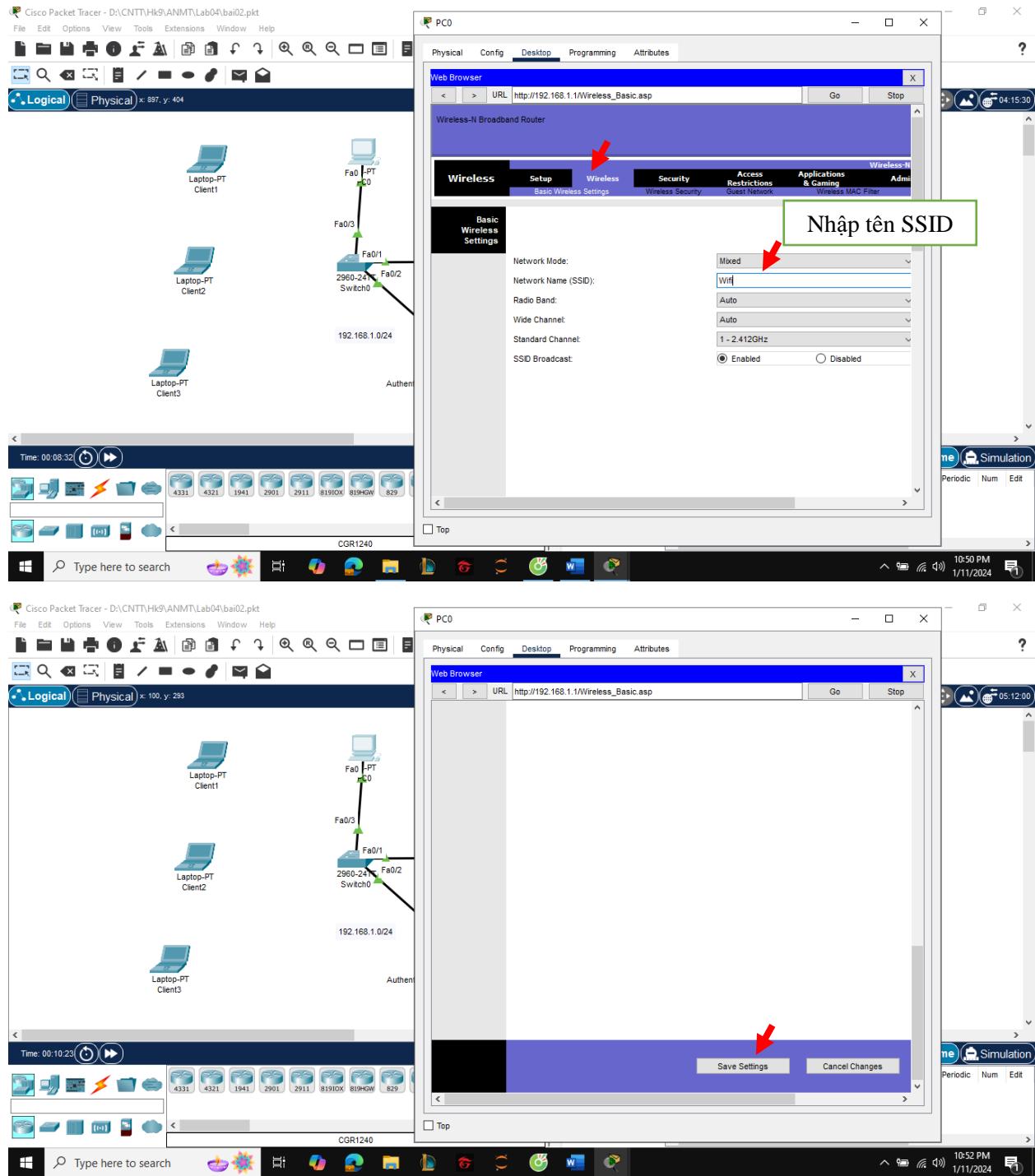
User Name: admin

Password: admin

Nhấn OK



B3: Cấu hình AP – Tên SSID



- Cấu hình Authentication Server (Radius server), tạo account để chứng thực người dùng Wifi

Các bước thực hiện:

- Service: Tick chọn On
- Network Configuration: Cấu hình mạng
  - + Client Name : Tên SSID đã đặt ở trên (Wifi)
  - + Client IP: Địa chỉ IP của AP (192.168.1.1)

+ Secret: Nhập khoá bí mật (thach)

Sau đó nhấn Add

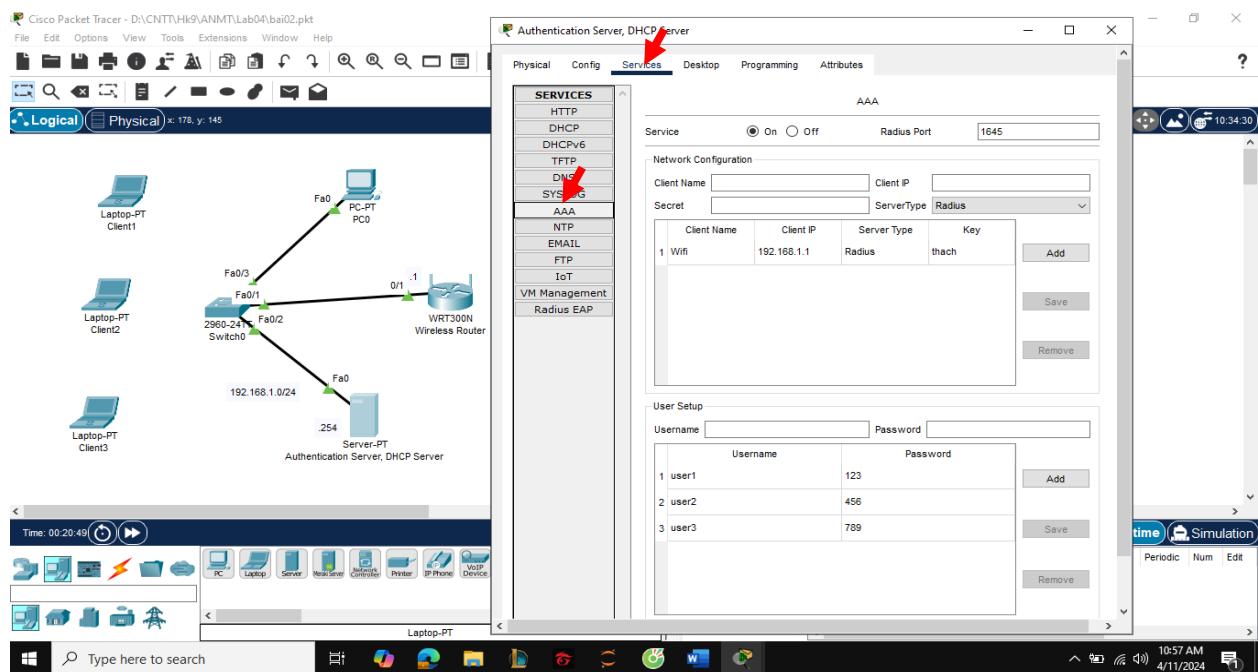
- User Setup: Tạo account chứng thực người dùng Wifi

+ User Name: Nhập tên account

+ Password : Nhập mật khẩu

Sau đó nhấn Add

Ở đây ta tạo 3 account



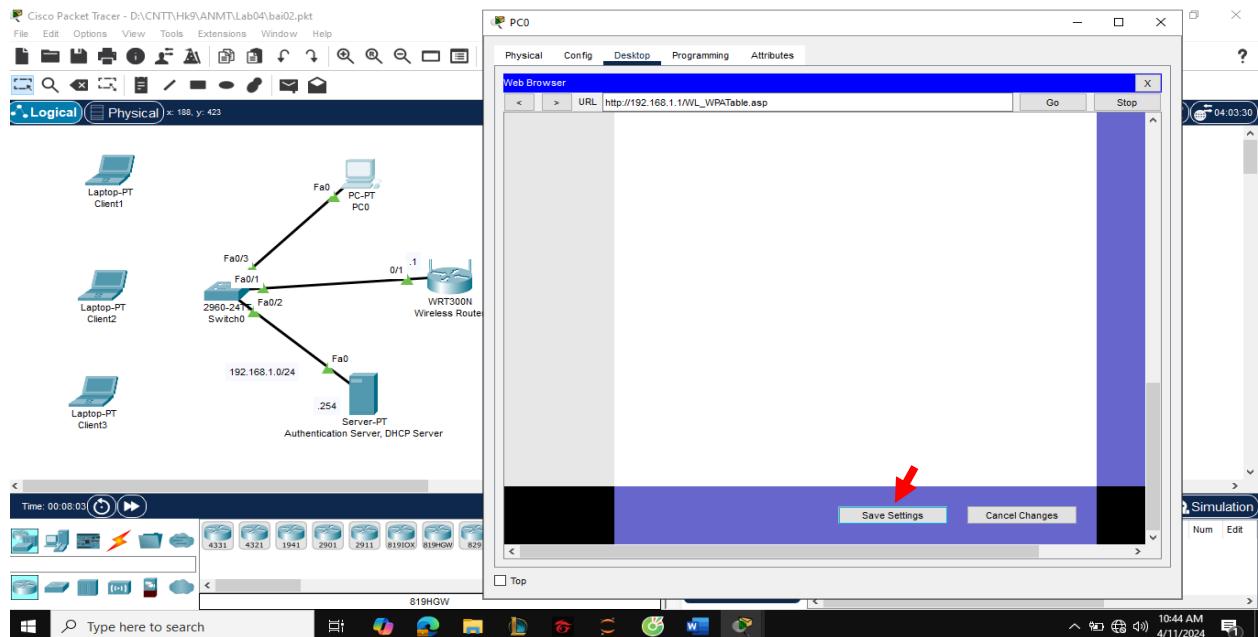
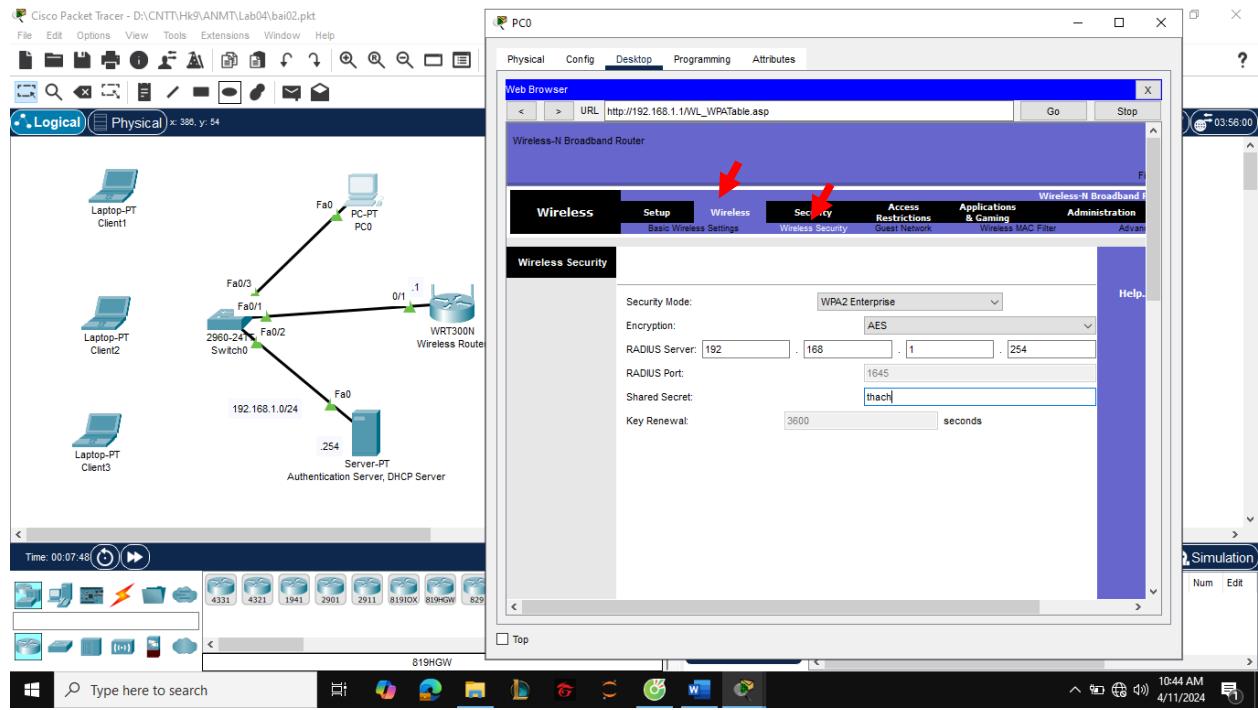
- AP đóng vai trò là Authenticator (dùng WPA2-Enterprise)

Ta cấu hình AP bằng PC Web Brower

Các bước thực hiện như bên dưới:

- Security Mode: Chọn WPA2-Enterprise
- RADIUS Server: Địa chỉ IP của Authentication Server (192.168.1.254)
- Shared Secret: Khoá bí mật đã được tạo ở trên (thach)

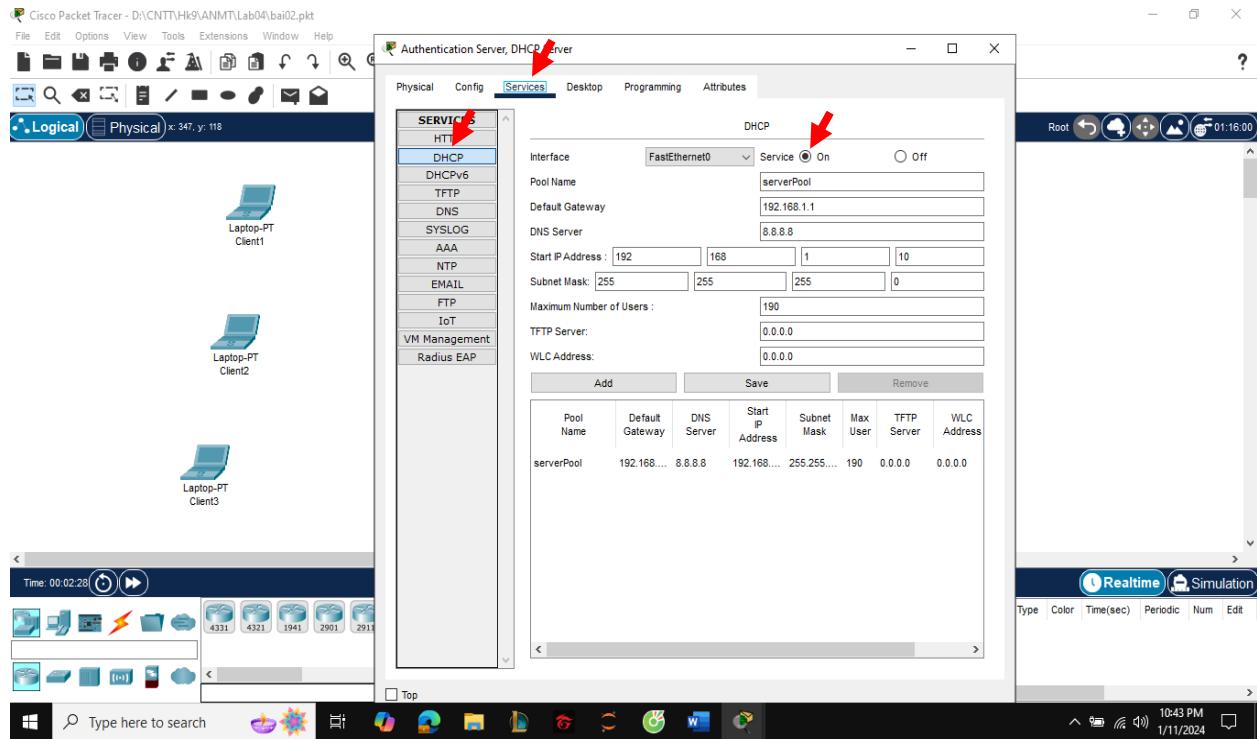
Sau đó Save Settings



- Authentication Server cũng đóng vai trò là DHCP server cấp phép IP động cho các client trong mạng. Các thông số IP cấp phát như sau:
  - o Network: 192.168.1.0/24
  - o IP range 192.168.1.10 – 192.168.1.200
  - o Default gateway: 192.168.1.1
  - o DNS: 8.8.8.8

Nhập các thông số IP cấp phát như ở trên:

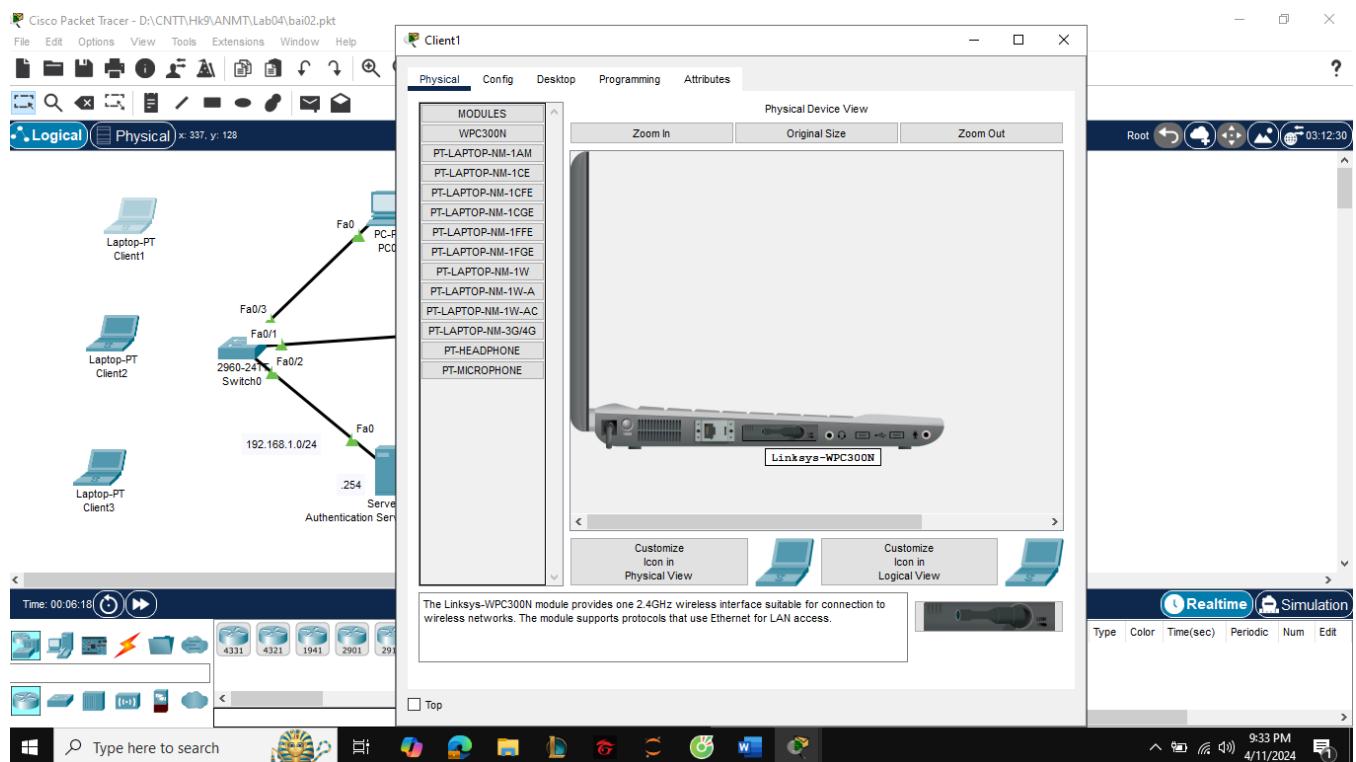
Sau đó nhấn Add



## Kiểm tra kết quả:

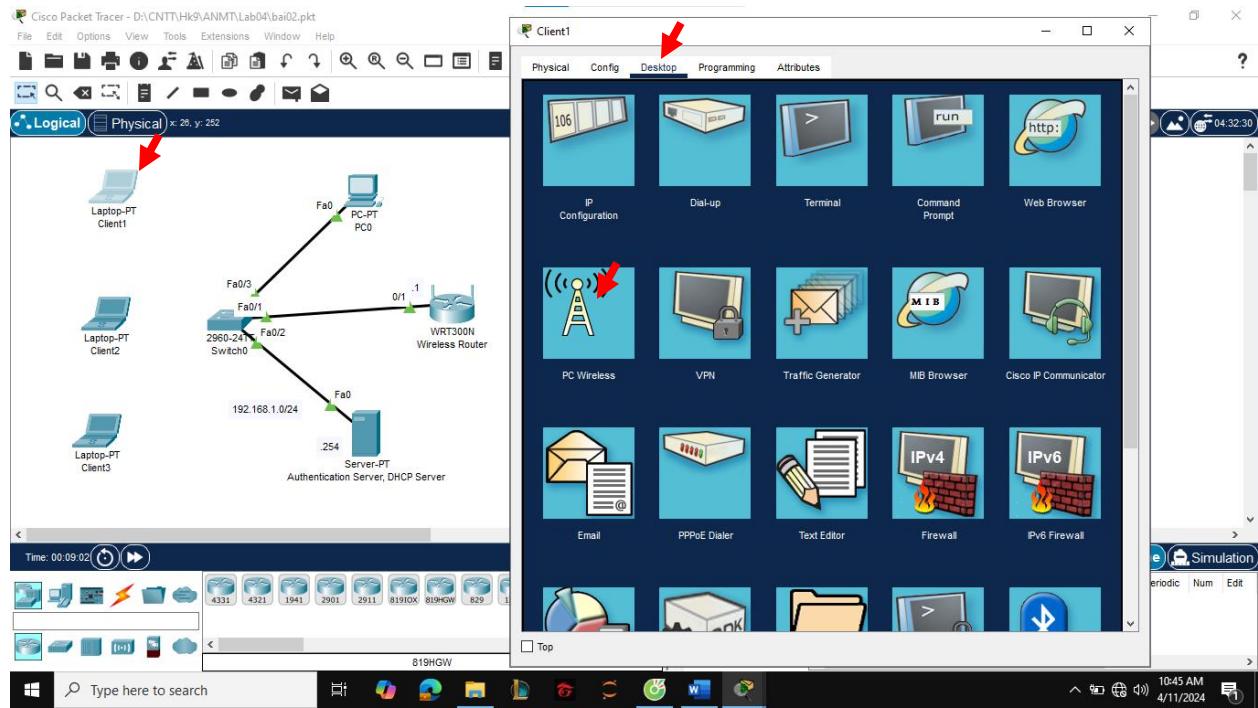
**Trước khi ta kiểm tra. Ta cần thực hiện bước sau:**

Thay đổi MODULES của 3 client thành WPC300N để hỗ trợ kết nối với mạng không dây  
Bằng cách tắt nguồn của client. Sau đó đổi MODULES phù hợp. Rồi bật nguồn trở lại

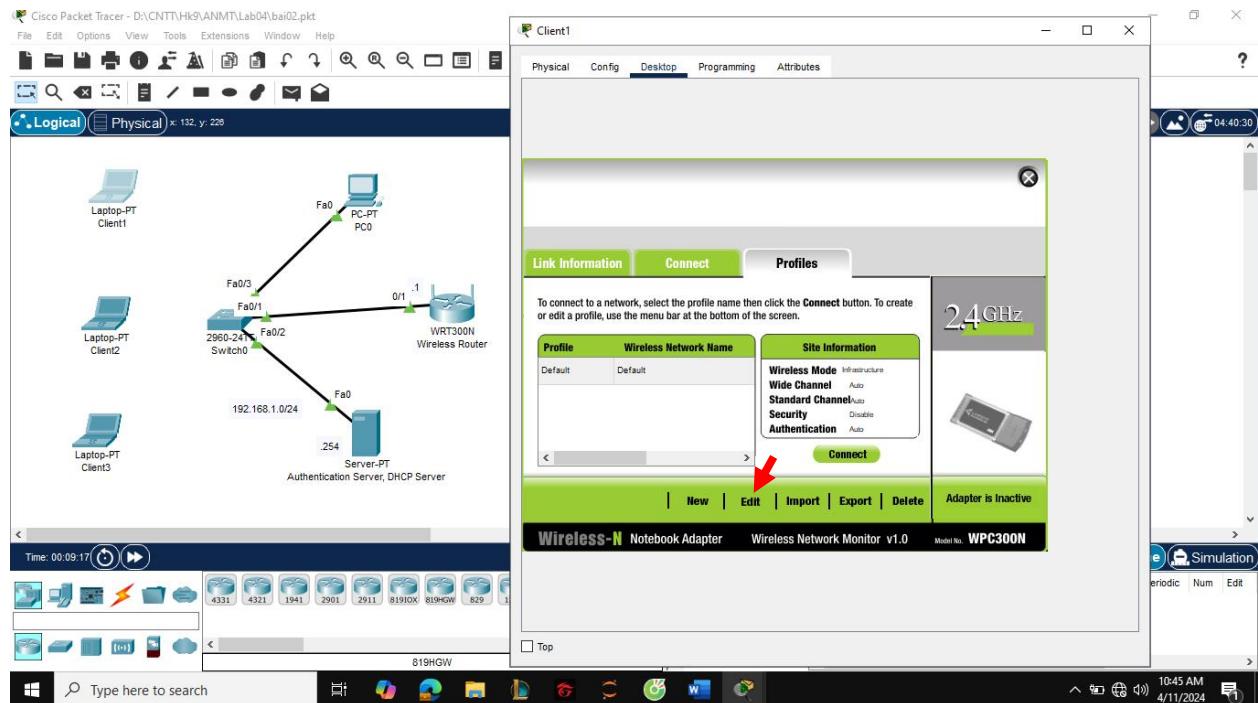


## Thực hiện kiểm tra kết quả:

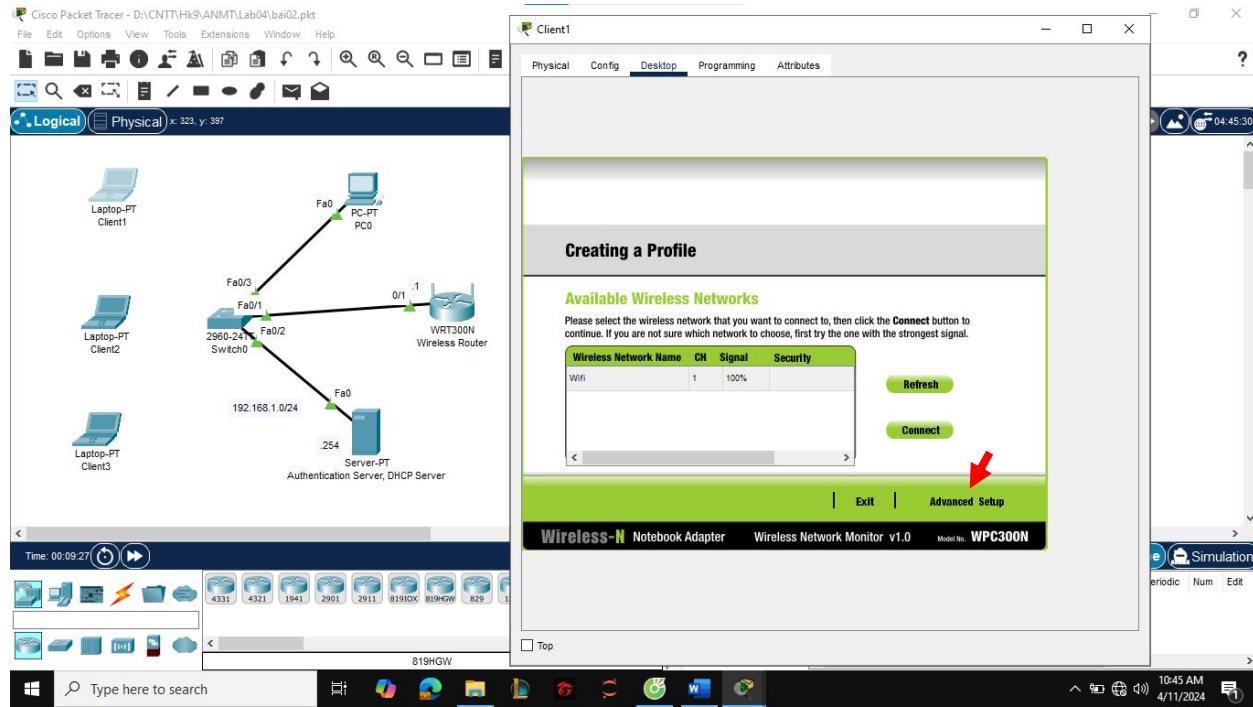
B1: Chọn Client1 . Chọn Desktop, sau đó nhấn chọn PC Wireless



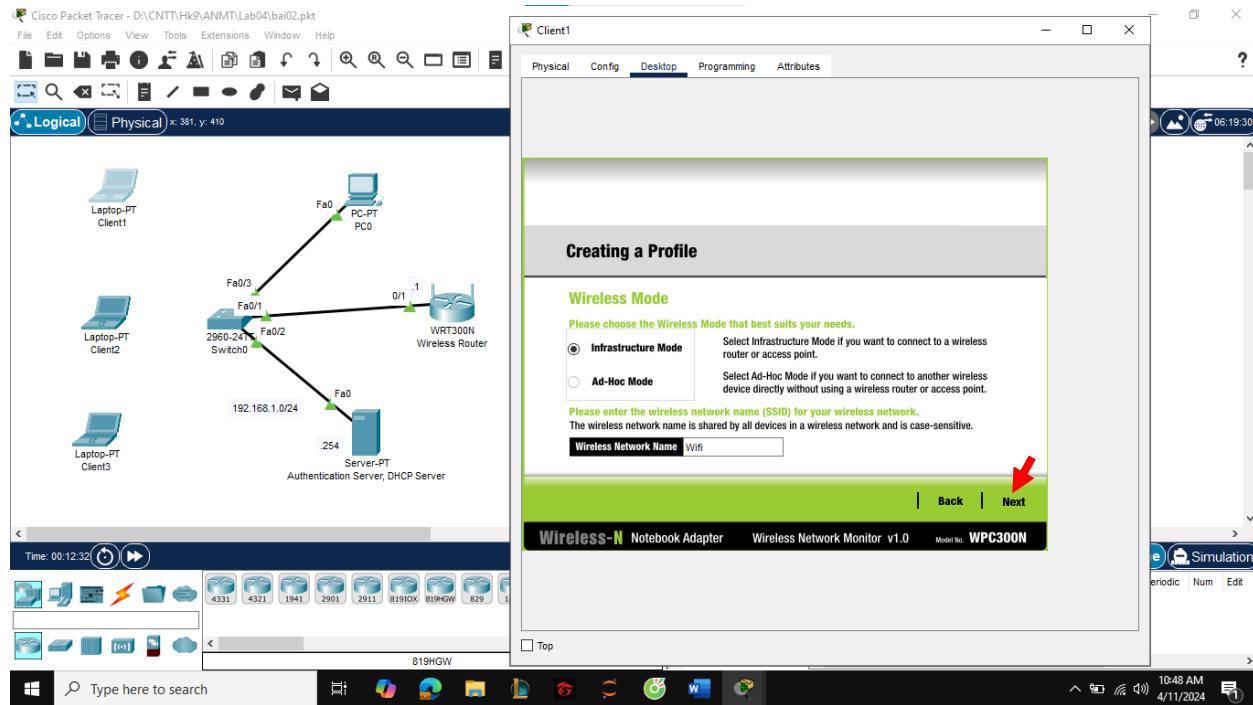
B2: Nhấn chọn Edit



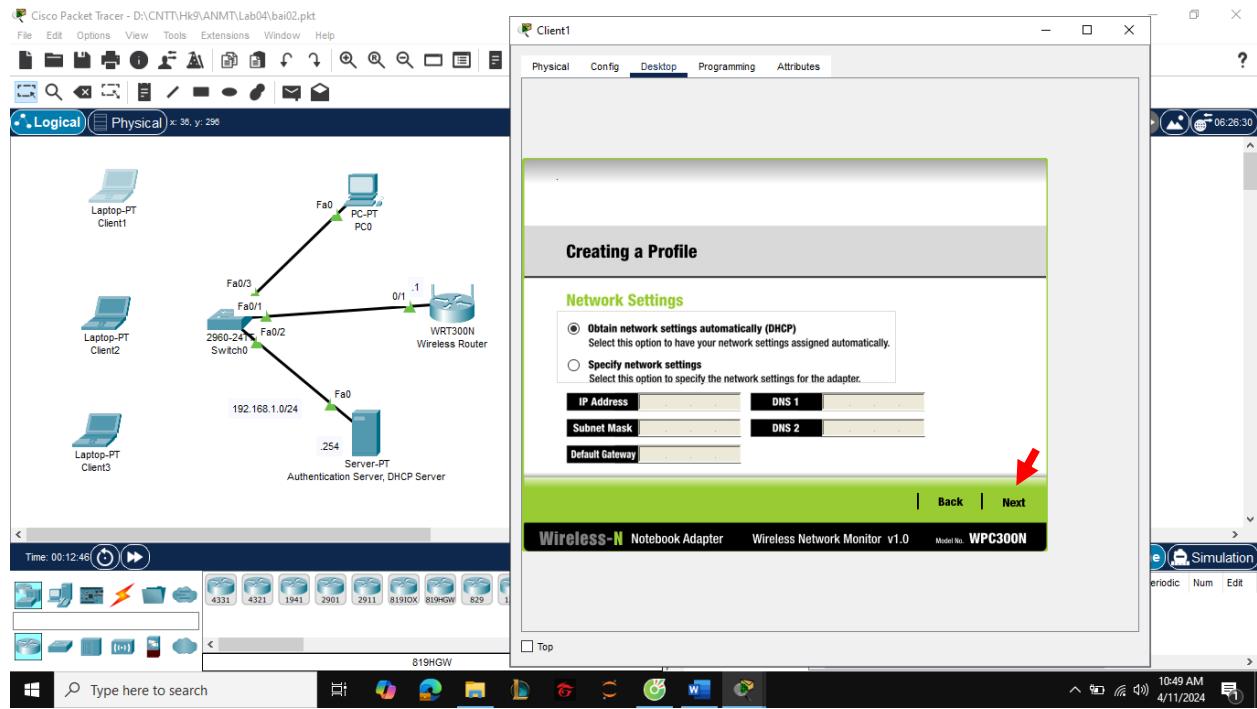
### B3: Nhấn chọn Advanced Setup



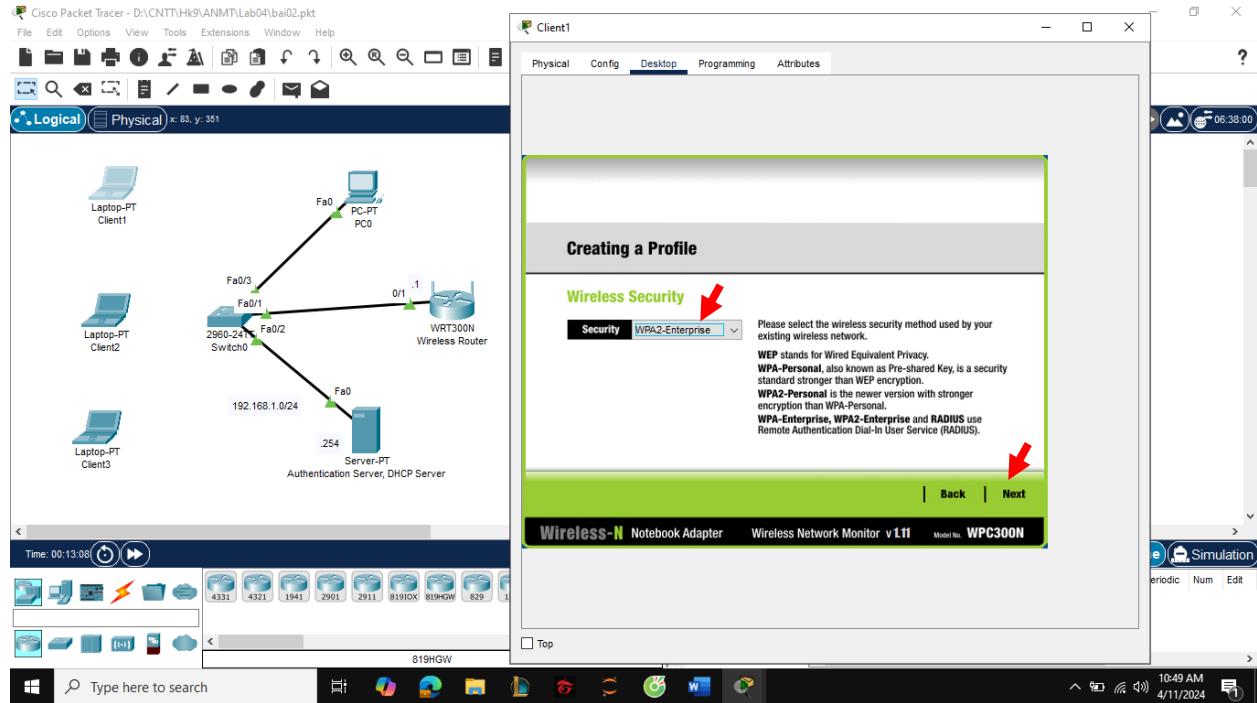
### B4: Nhấn chọn Next



## B5: Nhấn chọn Next



## B6: Trong Security, chọn WPA2-Enterprise. Sau đó nhấn chọn Next

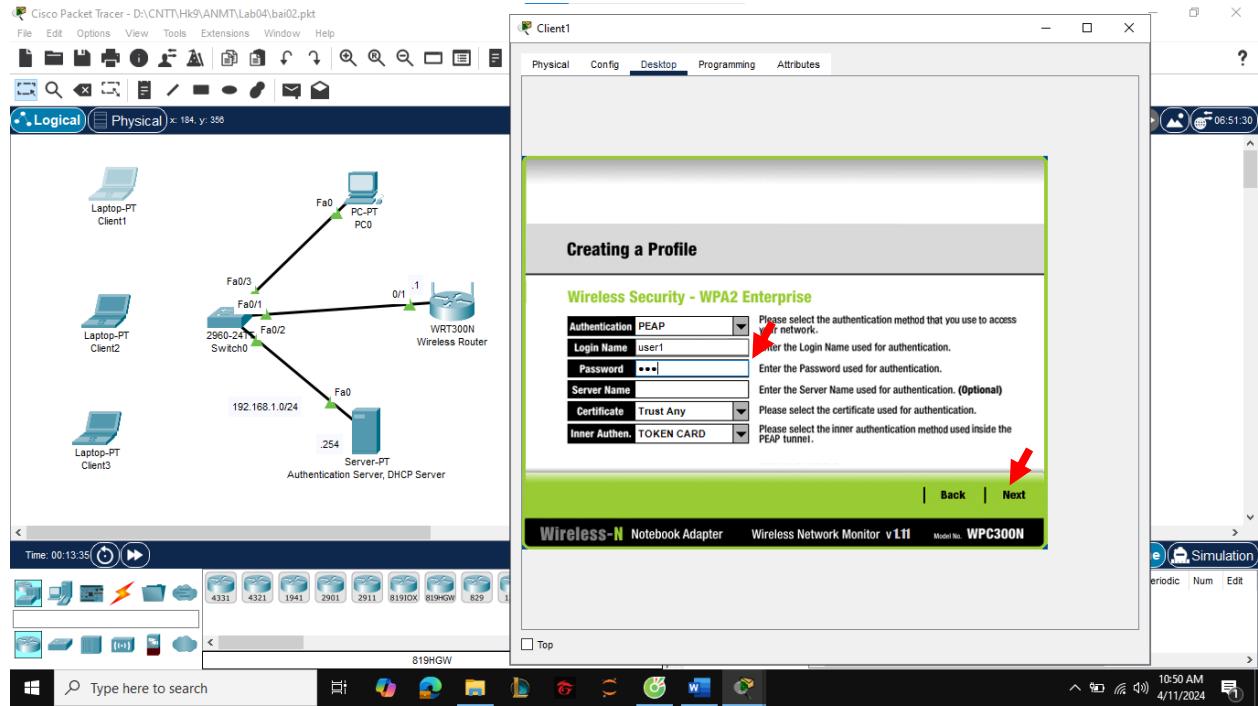


B7: Login Name và Password, nhập thông tin account đã được tạo ở trên

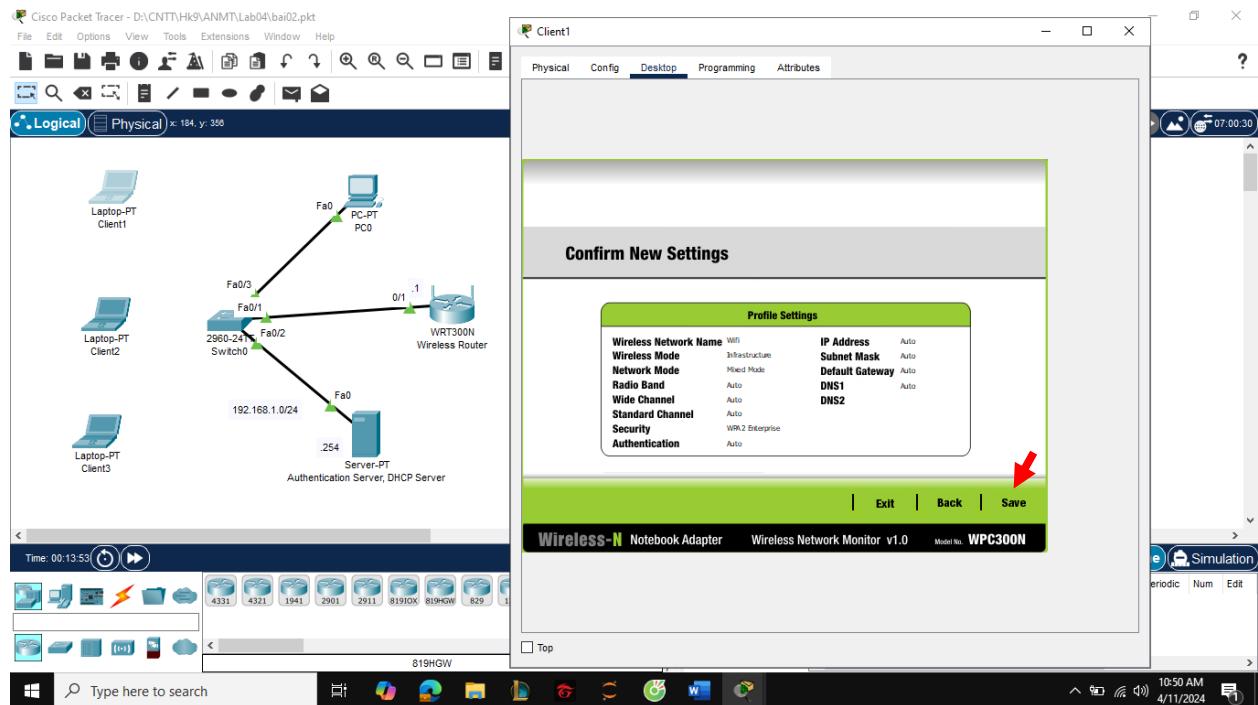
Login Name: user1

Password: 123

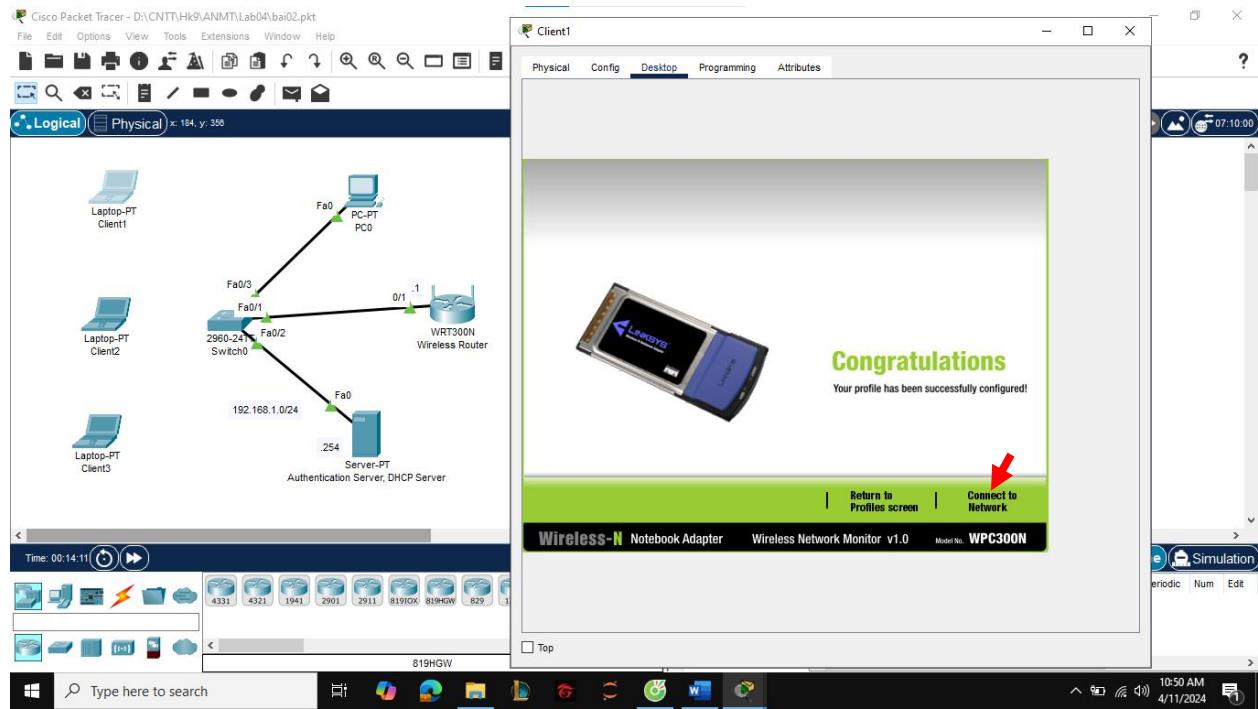
Nhấn chọn Next



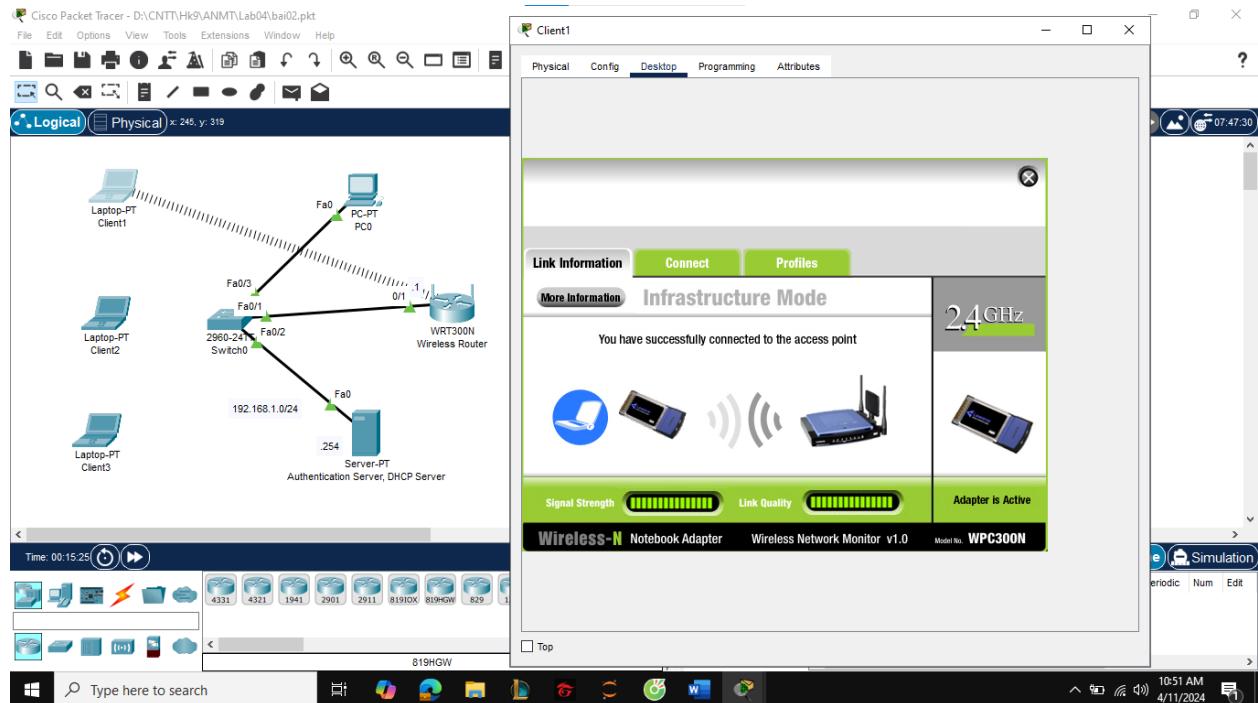
B8: Nhấn chọn Save



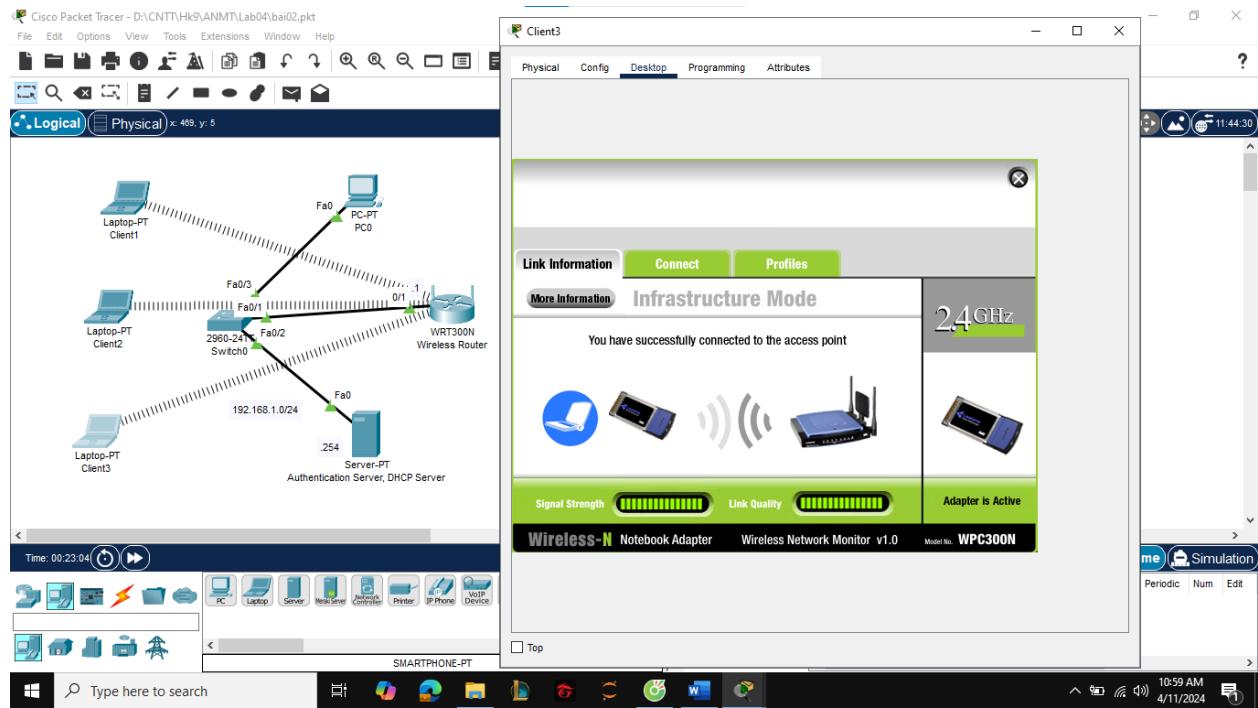
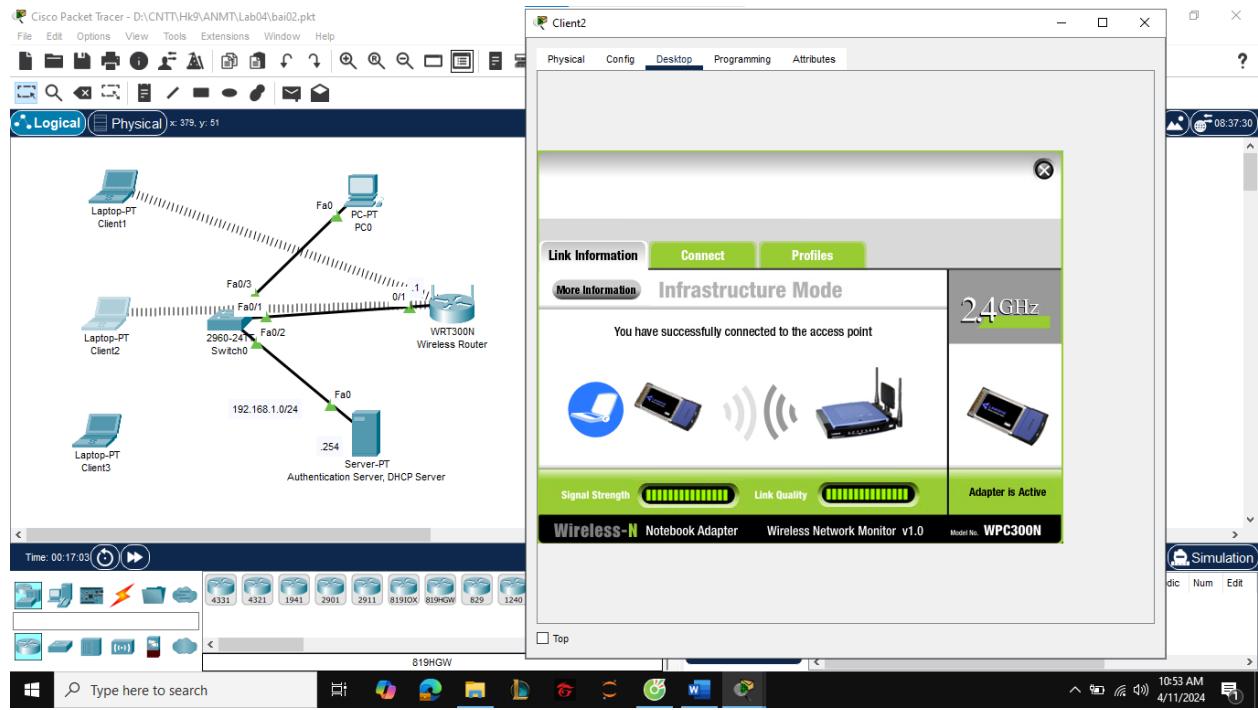
## B9: Nhấn chọn Connect to Network



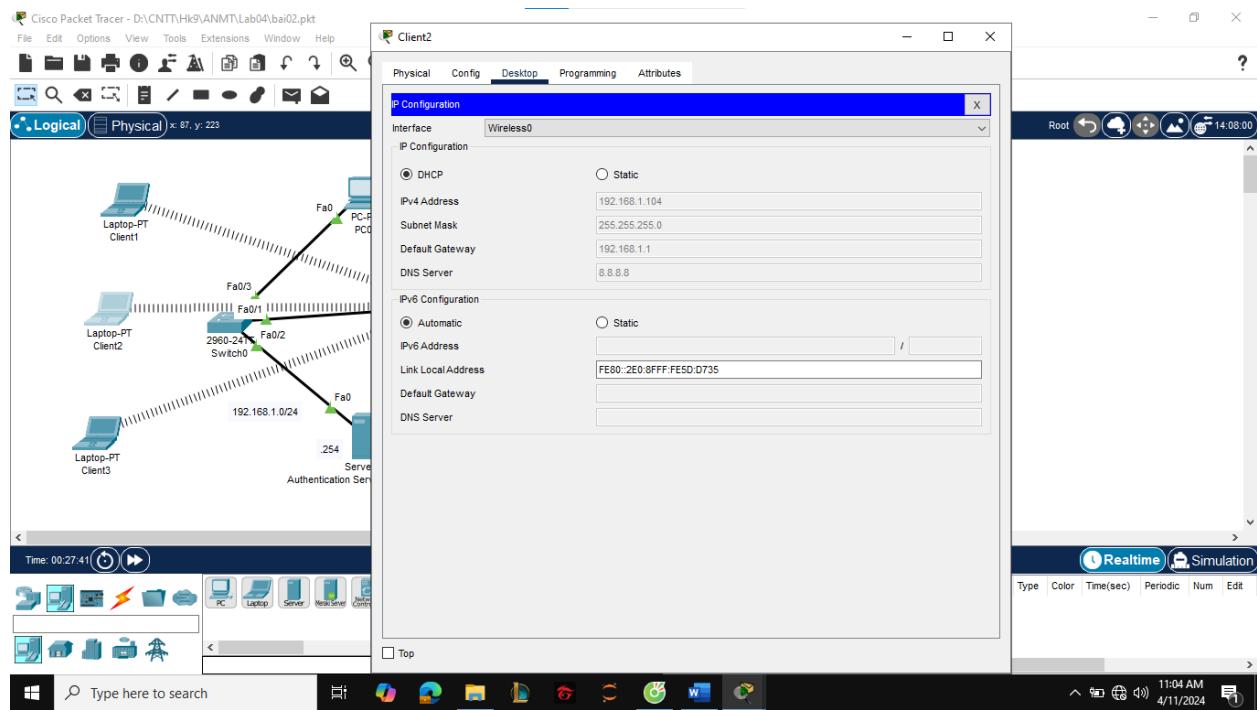
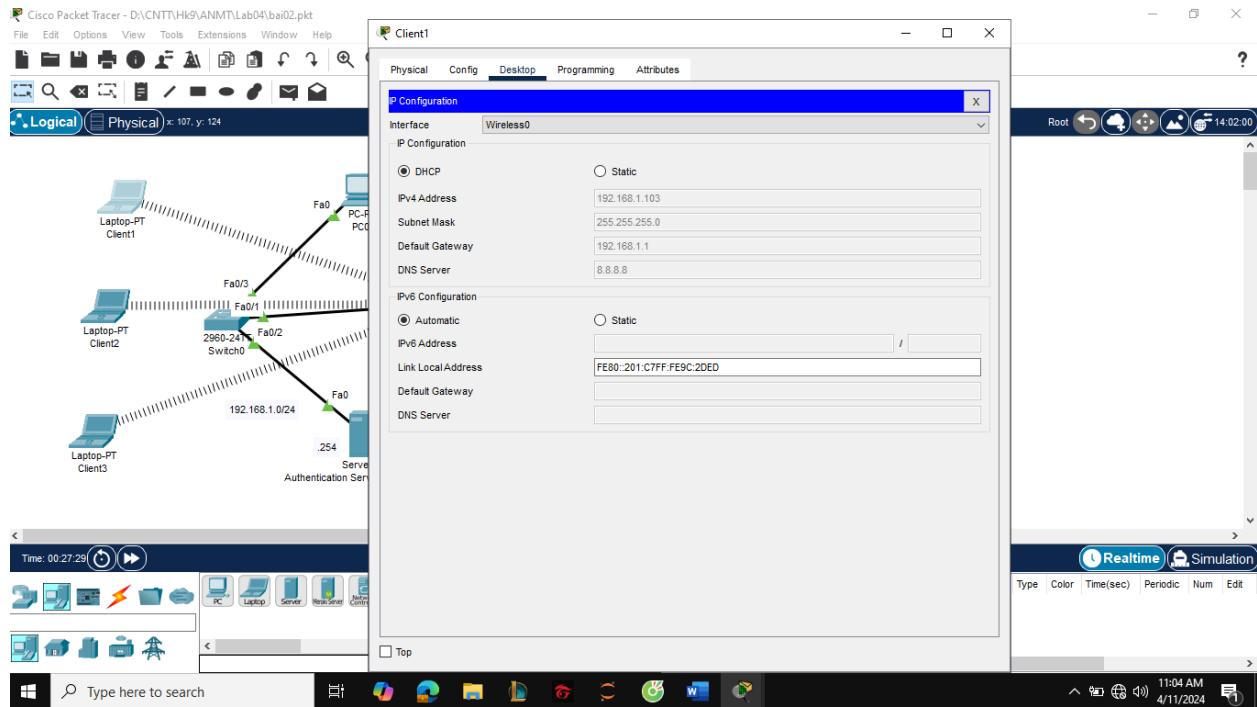
Kết quả sau khi đã xác thực người dùng wifi thành công

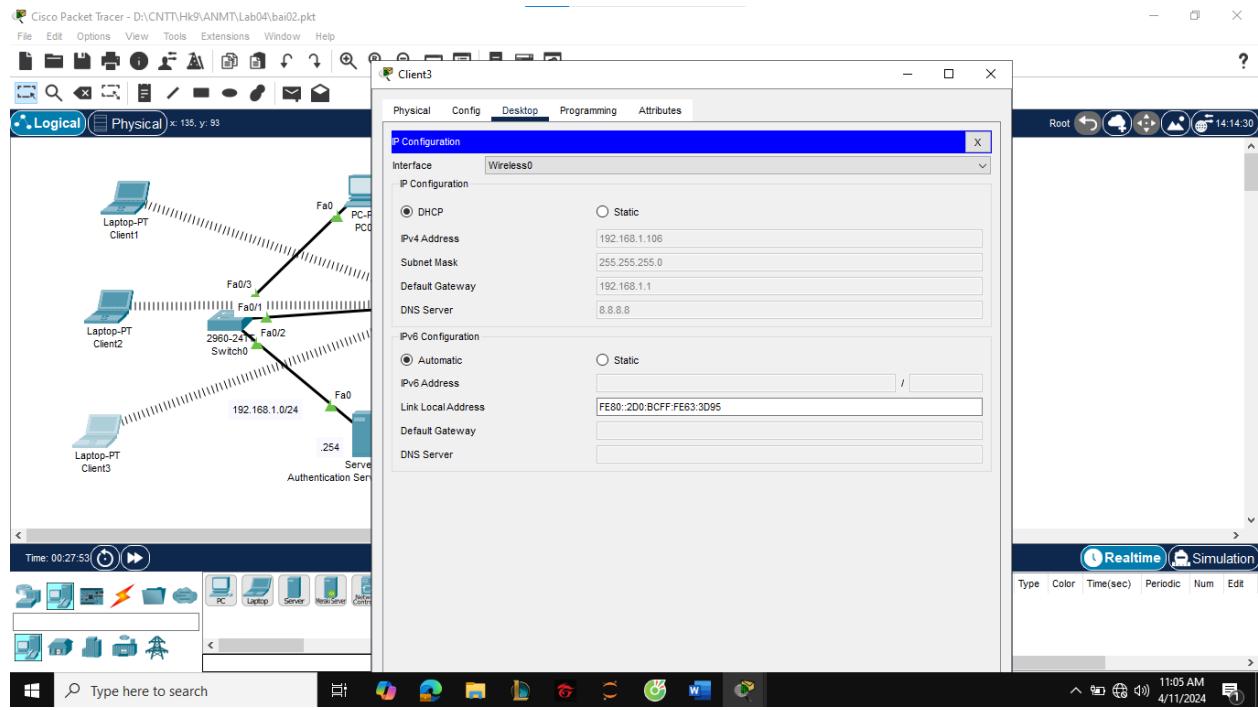


Làm tương tự với Client2, Client3



## Kiểm tra địa chỉ IP của các client được DHCP cấp phát IP động:





### 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
- .....

#### Kịch bản: Tấn công Evil Twin trên mạng WiFi công cộng

##### Mô tả:

Một cuộc tấn công Evil Twin diễn ra khi kẻ tấn công thiết lập một điểm truy cập Wi-Fi giả mạo có tên và cài đặt bảo mật tương tự như một mạng WiFi hợp lệ (thường là mạng WiFi công cộng hoặc mạng WiFi có nhiều người truy cập) với hy vọng rằng người dùng sẽ kết nối đến điểm truy cập này thay vì một điểm truy cập WiFi hợp lệ. Khi người dùng kết nối đến điểm truy cập này, tất cả dữ liệu họ chia sẻ với mạng sẽ đi qua một máy chủ do kẻ tấn công kiểm soát.

##### Các bước tấn công:

- **Bước 1: Tìm kiếm địa điểm phù hợp**

Kẻ tấn công thường tìm kiếm những địa điểm đông đúc có Wi-Fi miễn phí. Bao gồm các không gian như quán cà phê, thư viện hoặc sân bay, thường có nhiều điểm truy cập có cùng tên. Điều này giúp mạng giả của kẻ tấn công dễ dàng không bị phát hiện.

- **Bước 2: Thiết lập điểm truy cập WiFi**

Sau đó, kẻ tấn công sẽ ghi lại Mã định danh dịch vụ (SSID) của mạng hợp pháp và thiết lập một tài khoản mới có cùng SSID. Chúng có thể sử dụng hầu như bất kỳ thiết bị nào để thực hiện việc này, bao gồm điện thoại thông minh, máy tính xách tay, máy tính bảng hoặc bộ định tuyến di động. Các thiết bị được kết nối không thể phân biệt giữa mạng hợp lệ và mạng giả mạo.

- **Bước 3: Thuyết phục nạn nhân kết nối với Evil Twin Wi-Fi**

Kẻ tấn công có thể di chuyển gần hơn đến nạn nhân để tạo ra tín hiệu kết nối mạnh hơn so với các mạng hợp lệ. Điều này thuyết phục nạn nhân chọn mạng của chúng thay vì các mạng yếu hơn và buộc một số thiết bị tự động kết nối.

- **Bước 4: Thiết lập một cổng thông tin giả mạo**

Trước khi bạn có thể đăng nhập vào nhiều tài khoản Wi-Fi công cộng, bạn phải gửi dữ liệu trên một trang đăng nhập chung. Những kẻ tấn công Evil Twin đã thiết lập một bản sao của trang này, hy vọng sẽ lừa những nạn nhân tiết lộ thông tin đăng nhập của họ. Khi những kẻ tấn công có được thông tin đó, chúng có thể đăng nhập vào mạng và kiểm soát nó.

- **Bước 5: Đánh cắp dữ liệu của nạn nhân**

Bất kỳ ai đăng nhập đều kết nối thông qua kẻ tấn công. Đây là một cuộc tấn công man-in-the-middle cổ điển cho phép kẻ tấn công theo dõi hoạt động trực tuyến của nạn nhân. Giả sử người dùng đăng nhập vào bất kỳ tài khoản nào của họ. Trong trường hợp đó, kẻ tấn công có thể đánh cắp thông tin đăng nhập của họ - điều này đặc biệt nguy hiểm nếu nạn nhân sử dụng cùng một thông tin đăng nhập.

#### **Hậu quả:**

- Rò rỉ thông tin nhạy cảm: Khi kết nối vào mạng giả mạo, dữ liệu của người dùng có thể bị thu thập và sử dụng cho các mục đích xấu như ăn cắp thông tin tài khoản, mật khẩu, hoặc thông tin tài chính.
- Nguy cơ nhiễm mã độc: Kẻ tấn công có thể lợi dụng kết nối để cài đặt mã độc vào thiết bị của người dùng, từ đó thực hiện các cuộc tấn công sâu hơn hoặc giành quyền kiểm soát thiết bị.
- Đánh lừa người dùng truy cập vào các trang web lừa đảo: Kẻ tấn công có thể chuyển hướng người dùng tới các trang web giả mạo để thu thập thêm thông tin nhạy cảm hoặc lừa người dùng thực hiện các hành vi có hại.

#### **Giải pháp phòng chống:**

- Thiết lập VPN cho người dùng khi truy cập mạng công cộng:

- Sử dụng VPN (Virtual Private Network) để mã hóa toàn bộ dữ liệu trước khi nó rời khỏi thiết bị, từ đó bảo vệ người dùng trước các cuộc tấn công Man-in-the-Middle, ngay cả khi họ kết nối vào mạng Evil Twin.

- Cảnh giác với các mạng WiFi công cộng không yêu cầu mật khẩu hoặc có nhiều SSID giống nhau:
  - Người dùng nên cẩn thận khi kết nối vào các mạng WiFi công cộng, đặc biệt là những mạng không yêu cầu mật khẩu hoặc có tên SSID tương tự nhau. Nếu thấy một mạng công cộng với cùng tên nhưng không yêu cầu mật khẩu, đó có thể là dấu hiệu của một mạng Evil Twin.
- Xác thực điểm truy cập với quản trị viên mạng hoặc nhân viên tại nơi cung cấp WiFi:
  - Khi kết nối vào mạng WiFi tại nơi công cộng như quán cà phê, khách sạn, sân bay, người dùng nên kiểm tra và xác nhận tên mạng chính xác với nhân viên tại đó để tránh kết nối nhầm vào điểm truy cập giả mạo.
- Cấu hình thiết bị không tự động kết nối với mạng công cộng:
  - Người dùng nên tắt chế độ tự động kết nối với các mạng WiFi công cộng để tránh tình trạng thiết bị kết nối vào mạng Evil Twin.
- Sử dụng các phần mềm phát hiện tấn công mạng (IDS):
  - Các tổ chức có thể sử dụng Hệ thống phát hiện xâm nhập mạng (Network Intrusion Detection System - NIDS) để giám sát mạng WiFi của họ, phát hiện và cảnh báo khi có sự xuất hiện của các điểm truy cập giả mạo hoặc các hoạt động bất thường.