TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN – ĐHQG_HCM
KHOA CÔNG NGHỆ THÔNG TIN

An ninh máy tính

Lab 4

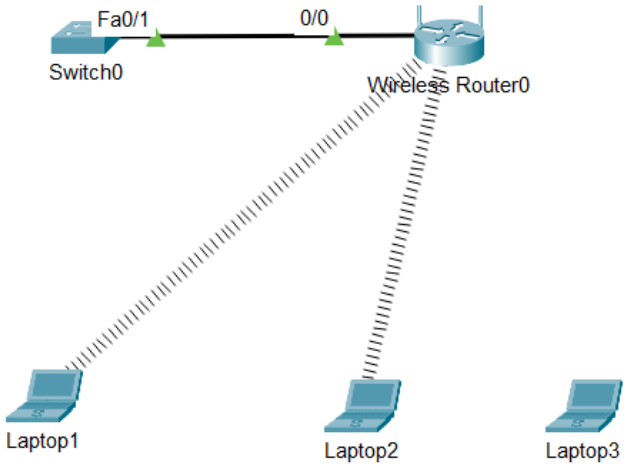
Giảng viên: **Huỳnh Nguyên Chính**
Nguyễn Văn Quang Huy
Ngô Đình Hy

MSSV	**Họ và tên**
20120083	Nguyễn Trọng Hiếu

Mục lục

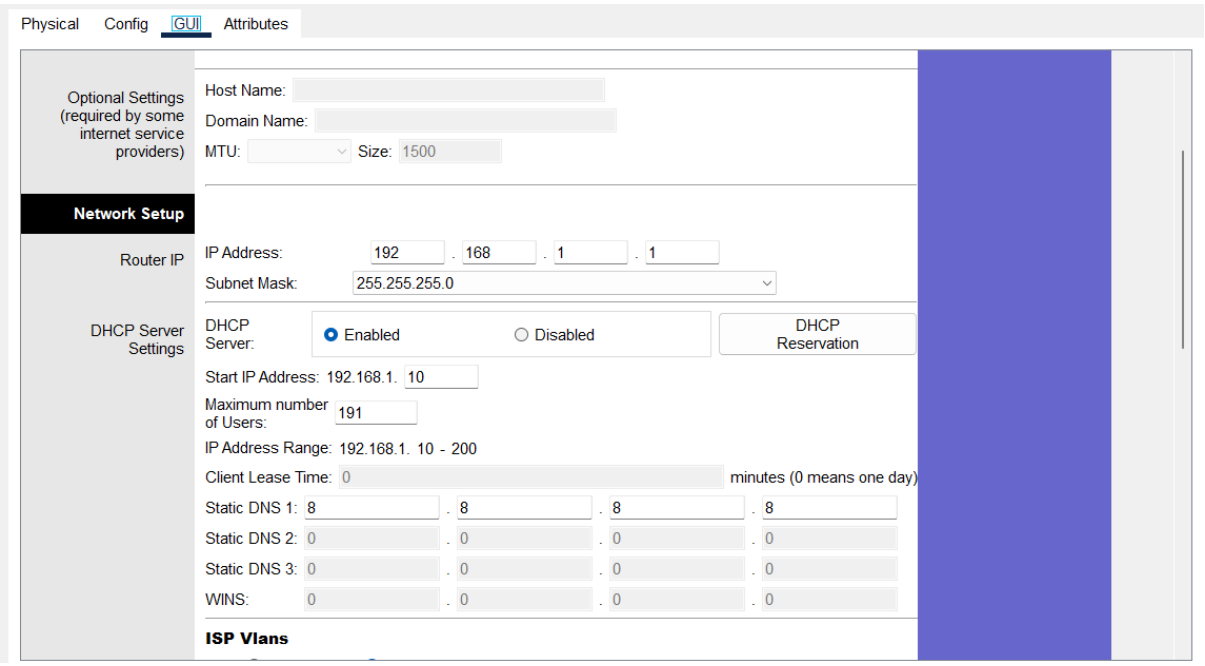
1. Cấu hình wifi cơ bản

Mô hình xây dựng:

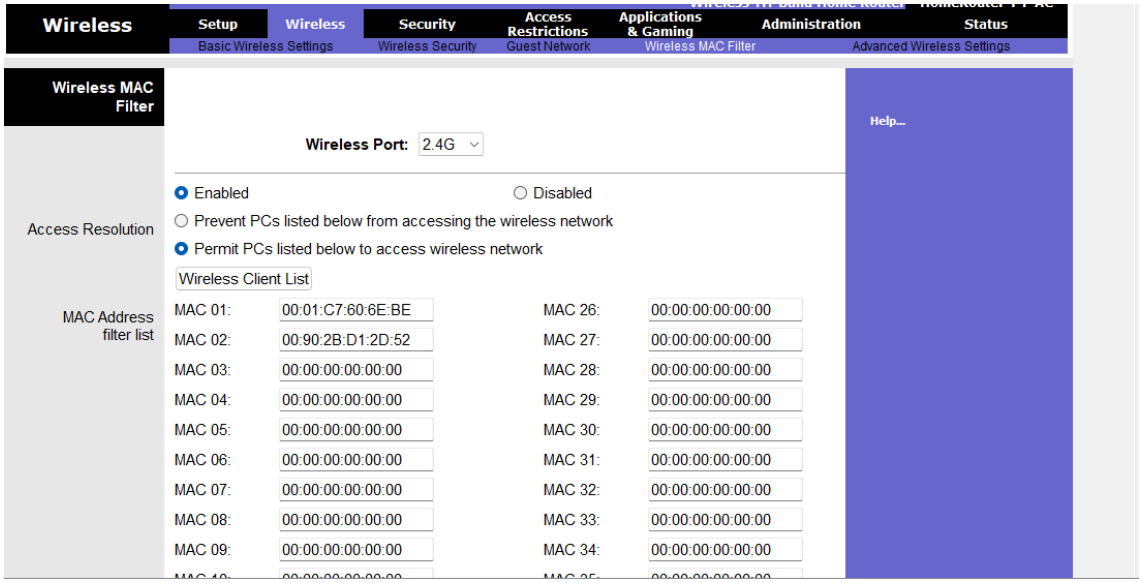


Hình 1: Mô hình MAC filtering

Cấu hình trên router:



Hình 2: Thông tin địa chỉ IP

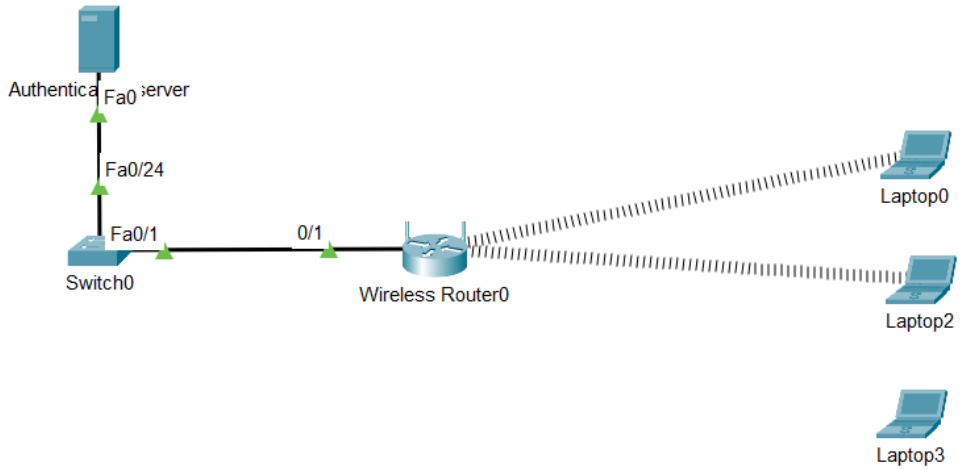


Hình 3: Cấu hình MAC filtering

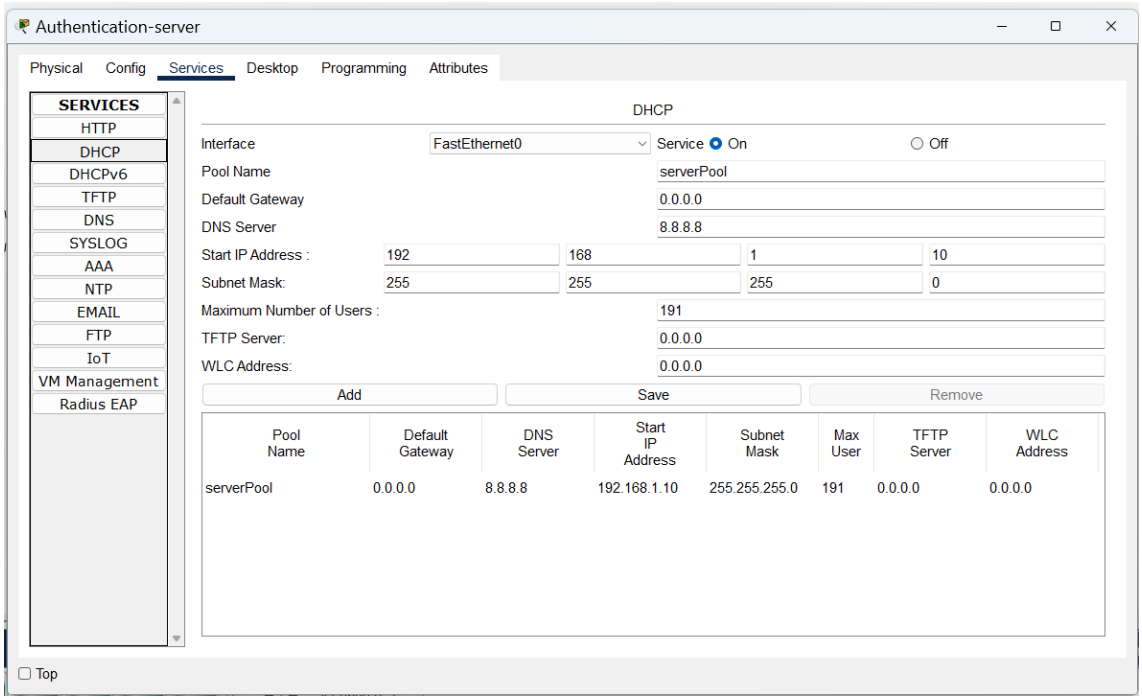
Lưu ý: Các thông tin cụ thể về địa chỉ của máy client cũng như cấu hình đều được lưu trong file ***bai1.pkt***

2. Cấu hình chứng thực người dùng Wifi dùng Radius Server

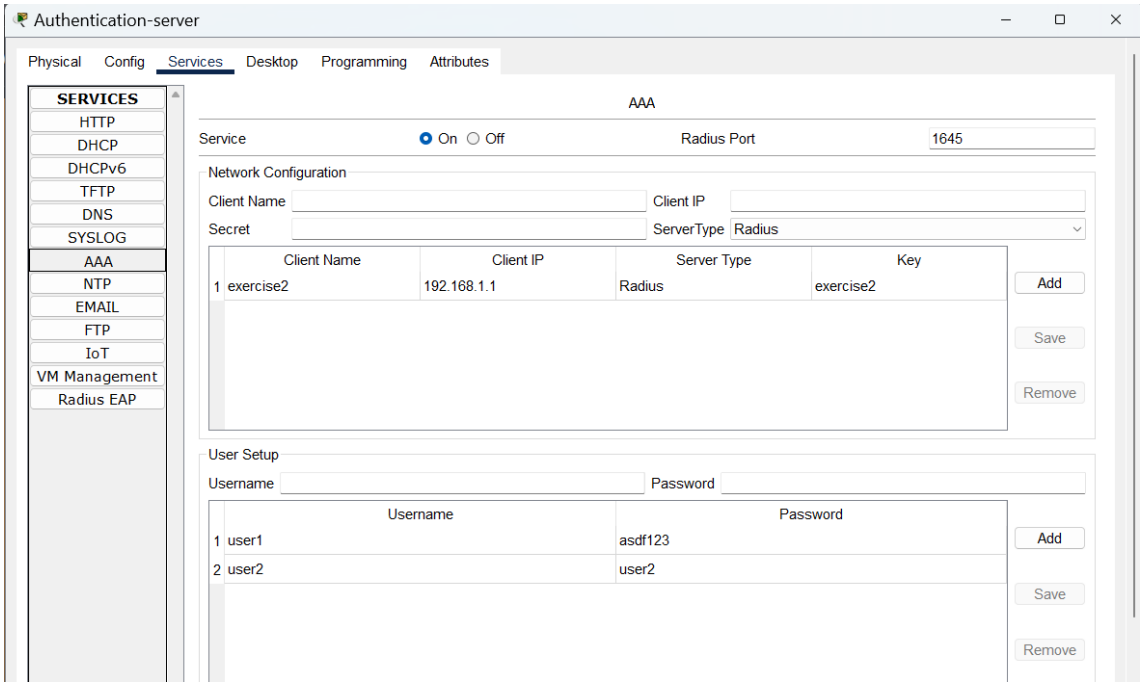
Mô hình xây dựng



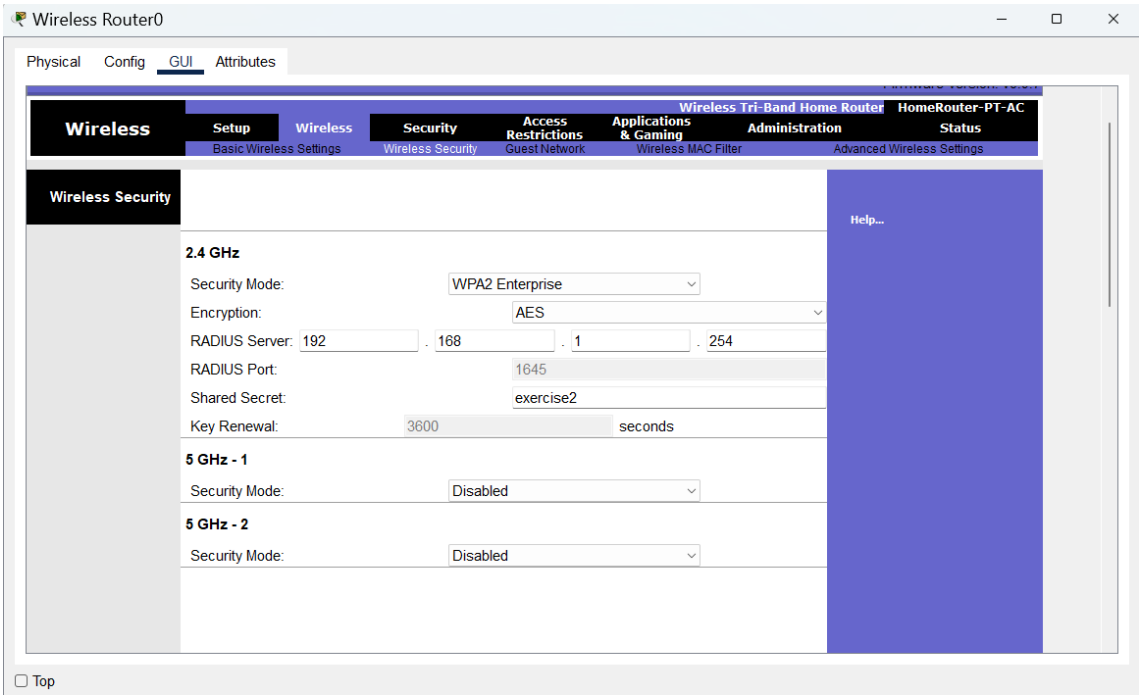
Hình 4: Mô hình cho câu 2



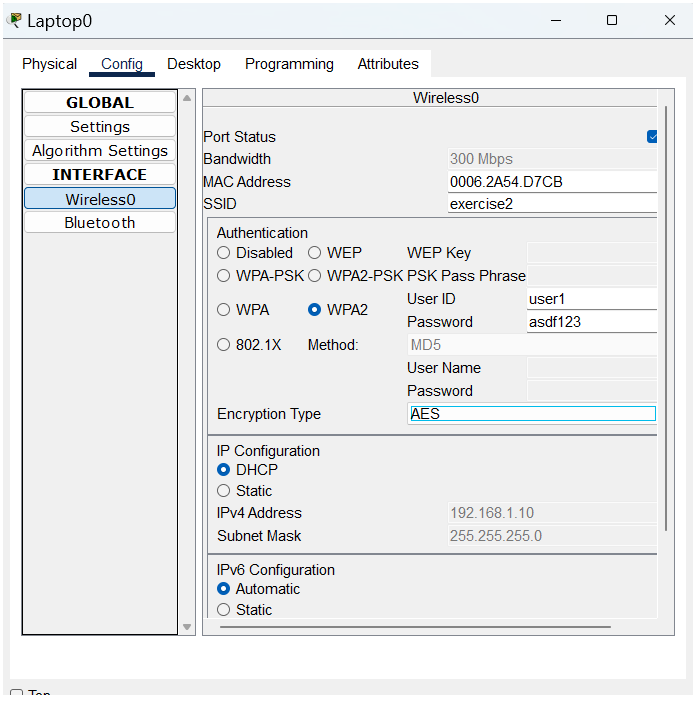
Hình 5: Cấu hình dhcp trên Authentication-server



Hình 6: Cấu hình Radius server trên Authentication-server



Hình 7: Thêm ip của radius-server trên Wireless router gui



Hình 8: Cấu hình wireless trên laptop để bắt được wifi

Lưu ý: Các thông tin cụ thể về địa chỉ của máy client cũng như cấu hình đều được lưu trong file ***bai2.pkt***

3. Tấn công wifi

Kịch bản: truy cập mạng wifi có cấu hình MAC filtering với các tool support như: nmap, airmon-ng, … (được tích hợp sẵn trong hệ điều hành kali linux).

Khái niệm:

- ***Media Access Control (MAC) address*** là một chuỗi 48-bits độc nhất gắn liền với một network in terface để định danh thiết bị.
- ***Router wifi***: đa số đều hỗ trợ MAC Whitelist/Blacklist. Bằng các danh sách này, người quản trị có thể xác định các địa chỉ MAC truy cập hoặc chặn truy cập vô wifi.

Bẻ khóa wifi cơ bản [1]

Bước 1: Cài các tool cần thiết – dùng luôn hệ điều hành kali-linux để tiết kiệm thời gian cài.

Bước 2: Sử dụng các tool cần thiết để handshake password hash.

Bước 3: Tiến hành giải mã hash password để tìm được wifi password

**giải dựa trên word list – Danh sách các password thường được dùng*

Cách thức bỏ qua MAC filtering [1]

Bước 1: Tiến hành dò cấc giá trị MAC cho phép kết nối vào mạng bằng tool.

Bước 2: Gán một trong các giá trị MAC được liệt kê ra từ ***Bước 1*** vào wireless card của máy và tiến hành reconnect.

- ***Phân tích*** [2]

Ứng dụng của MAC filtering trong mạng máy tính

Kiểm soát truy cập: Lọc địa chỉ MAC có thể được sử dụng để hạn chế quyền truy cập vào mạng bằng cách chỉ cho phép các thiết bị có địa chỉ MAC được ủy quyền kết nối. Điều này có thể giúp ngăn chặn truy cập không ủy quyền vào mạng và cải thiện bảo mật mạng.

Hỗ trợ phụ huynh quản lý con nhỏ: Lọc địa chỉ MAC có thể được sử dụng bởi phụ huynh để hạn chế quyền truy cập vào internet của con cái bằng cách chỉ cho phép những thiết bị cụ thể được kết nối vào mạng.

Chính sách BYOD: Lọc địa chỉ MAC có thể được sử dụng để triển khai các chính sách Mang Theo Thiết Bị Cá Nhân (BYOD) trong tổ chức. Bằng cách chỉ cho phép các thiết bị được ủy quyền kết nối vào mạng, tổ chức có thể đảm bảo chỉ có những thiết bị được chấp nhận mới được sử dụng để truy cập tài nguyên doanh nghiệp.

Truy cập cho thiết bị lạ (khách): Lọc địa chỉ MAC có thể được sử dụng để cung cấp quyền truy cập cho khách vào mạng bằng cách chỉ cho phép những thiết bị cụ thể được kết nối. Điều này có thể giúp cải thiện bảo mật và ngăn chặn truy cập không ủy quyền vào mạng.

Mạng không dây: Lọc địa chỉ MAC có thể được sử dụng để bảo mật mạng không dây bằng cách chỉ cho phép các thiết bị được ủy quyền kết nối vào mạng. Điều này có thể giúp ngăn chặn truy cập không ủy quyền vào mạng và bảo vệ dữ liệu nhạy cảm.

Giám sát mạng: Lọc địa chỉ MAC có thể được sử dụng để giám sát lưu lượng mạng bằng cách chỉ cho phép những thiết bị cụ thể được kết nối và theo dõi hoạt động của chúng trên mạng.

Tuân thủ: Lọc địa chỉ MAC có thể được sử dụng để bắt buộc tuân thủ các chính sách và quy định về bảo mật bằng cách đảm bảo chỉ có những thiết bị được ủy quyền mới được phép kết nối vào mạng.

Quản lý lưu lượng: Lọc địa chỉ MAC có thể được sử dụng để quản lý lưu lượng mạng bằng cách hạn chế số lượng thiết bị được phép kết nối vào mạng tại bất kỳ thời điểm nào.

Khắc phục sự cố: Lọc địa chỉ MAC có thể được sử dụng để khắc phục sự cố về kết nối mạng bằng cách xác định các thiết bị không ủy quyền có thể gây ra vấn đề trên mạng.

Quản lý từ xa: Lọc địa chỉ MAC có thể được sử dụng để cung cấp khả năng quản lý từ xa cho các thiết bị mạng bằng cách chỉ cho phép những thiết bị cụ thể kết nối vào mạng và truy cập vào tài nguyên mạng.

Những hạn chế

Mặt hiệu quả: lọc địa chỉ MAC không phải là biện pháp an ninh hoàn toàn và có thể dễ dàng bị qua mặt bởi những hacker có kinh nghiệm có thể làm giả hoặc thay đổi địa chỉ MAC của họ. Ngoài ra, một số thiết bị có thể cho phép người dùng thay đổi địa chỉ MAC của mình, làm cho việc kiểm soát truy cập mạng trở nên khó khăn.

Vấn đề tương thích: Một số thiết bị có thể không tương thích với lọc địa chỉ MAC hoặc có thể gặp vấn đề khi kết nối vào mạng nếu địa chỉ MAC của chúng không được cấu hình đúng. Điều này có thể gây ra vấn đề về kết nối và có thể đòi hỏi thêm công việc khắc phục sự cố.

Tăng cường độ phức tạp quản lý mạng: Việc duy trì danh sách các địa chỉ MAC được phép có thể tốn thời gian và khó khăn để quản lý, đặc biệt là đối với các mạng lớn với nhiều thiết bị. Ngoài ra, việc xác định và loại bỏ các thiết bị không được ủy quyền khỏi mạng cũng có thể là một thách thức.

Do đó việc này có thể làm cho mạng ít an toàn hơn vì bây giờ hacker không cần phải bẻ khóa mật khẩu được mã hóa WPA2 của bạn nữa mà chỉ cần chú ý đến việc giả mạo địa chỉ MAC.

- ***Giải pháp phòng chống***

Kết hợp cả địa chỉ lọc đị chỉ MAC lẫn mã hóa mật khẩu bằng WPA2/3. Sử dụng các mật khẩu có độ phức tạp đủ cao giúp đáp ứng sự an toàn.

Một giải pháp tốt hơn để kiểm soát những người ngoại vi muốn kết nối vào mạng của bạn là sử dụng một mạng Wi-Fi cho khách. Điều này sẽ cho phép họ kết nối vào mạng của bạn, nhưng không cho phép họ nhìn thấy bất kỳ điều gì trên mạng nội trú của bạn. Bạn có thể mua một router giá rẻ và kết nối nó vào mạng của bạn với một mật khẩu và dãy địa chỉ IP riêng biệt để thực hiện điều này.

4. Tham khảo

[1] Phương pháp bẻ khóa wifi khi mac filtering enabled

[2] MAC Filtering in Computer Network - GeeksforGeeks