TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM

**TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

**KHOA CÔNG NGHỆ THÔNG TIN**



**BÀI BÁO CÁO CUỐI KỲ MÔN  
AN TOÀN MẠNG KHÔNG DÂY VÀ DI ĐỘNG**

**TÌM HIỂU VÀ XÂY DỰNG HỆ THỐNG MẠNG KHÔNG DÂY CHO   
SIÊU THI ĐIỆN MÁY XANH**

*Người hướng dẫn:* **ThS. BÙI QUI ANH**

*Người thực hiện*: **ĐẶNG THÀNH CHÍ – 51800964**

**TRẦN QUỐC TÂM – 51800721**

**TRẦN VŨ LUÂN – 51900815**

**THÀNH PHỐ HỒ CHÍ MINH, NĂM 2021**

TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM

**TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

**KHOA CÔNG NGHỆ THÔNG TIN**



**BÀI BÁO CÁO CUỐI KỲ MÔN  
AN TOÀN MẠNG KHÔNG DÂY VÀ DI ĐỘNG**

**TÌM HIỂU VÀ XÂY DỰNG HỆ THỐNG MẠNG KHÔNG DÂY CHO   
SIÊU THI ĐIỆN MÁY XANH**

*Người hướng dẫn:* **ThS. BÙI QUI ANH**

*Người thực hiện*: **ĐẶNG THÀNH CHÍ – 51800964**

**TRẦN QUỐC TÂM – 51800721**

**TRẦN VŨ LUÂN – 51900815**

**THÀNH PHỐ HỒ CHÍ MINH, NĂM 2021**

# LỜI CẢM ƠN

Chúng em xin gởi lời cảm ơn đến với giảng viên Bùi Quy Anh, giảng viên lý thuyết kiêm người hướng dẫn em trong quá trình làm báo cáo môn An toàn mạng không dây và di động.

Nhờ có sự dẫn dắt từ thầy trong thời gian qua mà chúng em đã có được rất nhiều kiến thức bổ ích về môn học này. Xin cảm ơn thầy đã hỗ trợ để em có thể hoàn thành bài báo cáo này.

Do còn ít kinh nghiệm nên bài báo cáo đôi chỗ vẫn còn sai sót, chúng em mong có được sự góp ý của thầy để chúng em có thể hoàn thiện hơn nữa khả năng viết báo cáo của mình sau này.Một lần nữa, chúng Em xin chân thành cảm ơn.

ĐỒ ÁN ĐƯỢC HOÀN THÀNH  
TẠI TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG

Chúng tôi xin cam đoan đây là sản phẩm đồ án của riêng chúng tôi và được sự hướng dẫn của giảng viên Bùi Qui Anh;. Các nội dung nghiên cứu, kết quả trong đề tài này là trung thực và chưa công bố dưới bất kỳ hình thức nào trước đây. Những số liệu trong các bảng biểu phục vụ cho việc phân tích, nhận xét, đánh giá được chính tác giả thu thập từ các nguồn khác nhau có ghi rõ trong phần tài liệu tham khảo.

Ngoài ra, trong đồ án còn sử dụng một số nhận xét, đánh giá cũng như số liệu của các tác giả khác, cơ quan tổ chức khác đều có trích dẫn và chú thích nguồn gốc.

**Nếu phát hiện có bất kỳ sự gian lận nào tôi xin hoàn toàn chịu trách nhiệm về nội dung đồ án của mình.** Trường đại học Tôn Đức Thắng không liên quan đến những vi phạm tác quyền, bản quyền do tôi gây ra trong quá trình thực hiện (nếu có).

*TP. Hồ Chí Minh, ngày tháng năm*

*Tác giả*

*(ký tên và ghi rõ họ tên)*

*Đặng Thành Chí*

*Trần Vũ Luân*

*Trần Quốc Tâm*

# PHẦN XÁC NHẬN VÀ ĐÁNH GIÁ CỦA GIẢNG VIÊN

Phần xác nhận của GV hướng dẫn

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Tp. Hồ Chí Minh, ngày tháng năm

(kí và ghi họ tên)

Phần đánh giá của GV chấm bài

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Tp. Hồ Chí Minh, ngày tháng năm

(kí và ghi họ tên)

# TÓM TẮT

Trong thời đại công nghệ số đang ngày càng phát triển mạnh mẽ như hiện nay thì việc ứng dụng công nghệ thông tin vào cuộc sống hằng ngày dần không còn xa lạ gì với mọi người. Bởi vì công nghệ là một công cụ giúp quản lý kiểm soát một cách chính xác cao, tổ chức hiệu quả và dễ dàng tiếp cận, giảm thời gian làm việc. Từ những gì mà công nghệ thông tin có thể đem lại cho mọi người thì cũng đồng nghĩa với việc mạng không dây đang dần trở thành một thứ không thể thiếu trong các hoạt động của cá nhân người dùng và doanh nghiệp. Ngày nay bất cứ một doanh nghiệp hay cá nhân nào cũng đều muốn ứng dụng công nghệ thông tin vào hoạt động quản lý, đặc biệt là quản lý thông tin trong nội bộ. Có rất nhiều dạng thông tin cần quản lý chẳng hạn như thông tin về các văn bản mật (file hồ sơ thầu, kế hoạch định hướng phát triển), thông tin về dữ liệu kế toán hay thông tin về các sản phẩm trí tuệ như phần mềm hoặc bản thiết kế sản phẩm. Nếu những thông tin này lọt ra ngoài doanh nghiệp nhẹ thì mất tiền chi phí cho sản phẩm, nặng thì mất uy tín với khách hàng. Điều tồi tệ này càng trở nên trầm trọng hơn khi doanh nghiệp không có đủ nhân lực công nghệ thông tin để thực hiện.

Báo cáo xây dựng mạng không dây cho siêu thị điện máy xanh gồm có 4 chương: chương 1 sẽ giới thiệu về cơ sở lý thuyết gồm những khái niệm cơ bản; các chuẩn Wifi, IEEE hiện nay; các kỹ thuật tấn công mạng không dây cũng như cách ngăn chặn chúng. Chương 2 sẽ mô tả đề tài, chi tiết sẽ là giới thiệu về doanh nghiệp siêu thị điện máy xanh; yêu cầu của khách hàng dành cho doanh nghiệp và đề xuất hướng giải quyết các vấn đề cũng như cập nhật các thiết bị cần thiết cho việc xây dựng hệ thống. Chương 3 sẽ giới về mô hình demo sẽ được xây dựng cho doanh nghiệp. Chương 4 kết luận lại xem đã đạt được và những hạn chế còn gặp phải trong khi làm bài báo cáo

# MỤC LỤC

[LỜI CẢM ƠN i](#_Toc91926294)

[PHẦN XÁC NHẬN VÀ ĐÁNH GIÁ CỦA GIẢNG VIÊN iii](#_Toc91926295)

[TÓM TẮT iv](#_Toc91926296)

[MỤC LỤC 1](#_Toc91926297)

[DANH MỤC KÍ HIỆU VÀ CHỮ VIẾT TẮT 3](#_Toc91926298)

[DANH MỤC CÁC BẢNG BIỂU, HÌNH VẼ, ĐỒ THỊ 4](#_Toc91926299)

[CHƯƠNG 1 - CƠ SỞ LÝ THUYẾT 6](#_Toc91926300)

[1.1 Các khái niệm cơ bản 6](#_Toc91926301)

[1.1.1 Mạng không dây 6](#_Toc91926302)

[1.1.1.1 Khái niệm 6](#_Toc91926303)

[1.1.1.2 Phân loại mạng không dây 6](#_Toc91926304)

[1.1.1.3 Nguyên lý hoạt động của mạng không dây 8](#_Toc91926305)

[1.1.2 Khái niệm mạng di động 9](#_Toc91926306)

[1.1.3 Mạng Wifi 9](#_Toc91926307)

[1.1.3.1 Khái niệm 9](#_Toc91926308)

[1.1.3.2 Mạng wifi hoạt động như thế nào? 9](#_Toc91926309)

[1.1.3.3 Điểm truy cập không dây là gì? 10](#_Toc91926310)

[1.1.3.4 Mobile Hotspot là gì? 10](#_Toc91926311)

[1.1.3.5 Điểm phát sóng Wifi hotspot là gì? 10](#_Toc91926312)

[1.1.3.6 Kiến trúc Hotspot là gì? 10](#_Toc91926313)

[1.1.4 Tổng quan về AAA 11](#_Toc91926314)

[1.1.4.1 Giao thức AAA trong bảo mật và điều khiền truy cập mở rộng trong mạng 12](#_Toc91926315)

[1.1.4.2 Giao thức bảo mật sử dụng cho dịch vụ AAA 12](#_Toc91926316)

[1.1.4.3 TACACS là gì? 13](#_Toc91926317)

[1.1.4.4 Tổng quan về RADIUS 14](#_Toc91926318)

[1.1.4.5 Ứng dụng RADIUS 15](#_Toc91926319)

[1.1.5 Một số chuẩn kết nối hiện nay 15](#_Toc91926320)

[1.1.6 Tổng quan về WEP và WPA. 19](#_Toc91926321)

[1.2 Các hình thức tấn công mạng không dây 20](#_Toc91926322)

[1.2.1 Những rủi ro khi sử dụng mạng không dây 21](#_Toc91926323)

[1.2.2 Các dạng tấn công mạng không dây phổ biến 21](#_Toc91926324)

[1.3 Các phương pháp bảo mật cơ bản 23](#_Toc91926325)

[CHƯƠNG 2 - MÔ TẢ ĐỀ TÀI 27](#_Toc91926326)

[2.1 Yêu cầu thiết kế 27](#_Toc91926327)

[2.1.1 Giới thiệu doanh nghiệp 27](#_Toc91926328)

[2.1.2 Yêu cầu của khách hàng 28](#_Toc91926329)

[2.1.3 Đề xuất hướng giải quyết 28](#_Toc91926330)

[2.2 Thiết kế mô hình 28](#_Toc91926331)

[2.2.1 Cấu trúc hệ thống mạng: 28](#_Toc91926332)

[2.2.2 Chi phí dự tính 29](#_Toc91926333)

[CHƯƠNG 3 - DEMO 30](#_Toc91926334)

[3.1 Mô hình mạng 30](#_Toc91926335)

[3.2 Thông tin cấu hình 31](#_Toc91926336)

[3.3 Kiểm tra kết nối 52](#_Toc91926337)

[CHƯƠNG 4 - KẾT LUẬN 59](#_Toc91926338)

[TÀI LIỆU THAM KHẢO 60](#_Toc91926339)

[BẢNG PHÂN CHIA CÔNG VIỆC 61](#_Toc91926340)

# DANH MỤC KÍ HIỆU VÀ CHỮ VIẾT TẮT

**CÁC CHỮ VIẾT TẮT**

WPAN Wireless Personal Area Network

WLAN Wireless Local Area Network

WMAN Wireless Metropolitan Area Network

WWAN Wireless Wide Area Network

PDA Personal Digital Assistants

ACL Asynchronous Connectionless Links

AAA Authentication Authorization Audit

DHCP Dynamic Host Configuration Protocol

SSID Service Set Identifier

IEEE Institute of Electrical and Electronics Engineers

TACACS Terminal Access Controller Access Control System

RADIUS Remote Authentication Dial-In User Service

RAS Remote Access Switch

CHAP Challenge Handshake Authentication Protocol

EAP Extensible Authenti-cation Protocol

MAC Media Access Control

AP Access Point

WPA Wi-Fi Protected Access

# DANH MỤC CÁC BẢNG BIỂU, HÌNH VẼ, ĐỒ THỊ

**DANH MỤC BẢNG**

[Bảng 1.1 So sánh IEEE 802.15.1; IEEE 802.15.3 và IEEE 802.15.4 19](#_Toc91926452)

[Bảng 2.1 Bảng chi phí dự tính cho các thiết bị 29](#_Toc91926453)

[Bảng 3.1 Bảng địa chỉ IP 31](#_Toc91926454)

[Bảng 3.2 Bảng thông tin WLAN 31](#_Toc91926455)

**DANH MỤC HÌNH**

[Hình 1.1 Lịch sử phát triển của chuẩn IEEE 802.11 16](#_Toc91926410)

[Hình 1.2 Mô tả thông số của các chuẩn IEEE 802.11 17](#_Toc91926411)

[Hình 1.3 VPN 26](#_Toc91926412)

[Hình 1.4 Tắt quản lý từ xa/ dịch vụ không cần thiết 27](#_Toc91926413)

[Hình 2.1 Logo Điện máy Xanh 28](#_Toc91926414)

[Hình 3.1 Mô hình mạng 30](#_Toc91926415)

[Hình 3.2 cấu hình R1 in (1) 32](#_Toc91926416)

[Hình 3.3 cấu hình R1 in (2) 33](#_Toc91926417)

[Hình 3.4 cấu hình R2 out (1) 34](#_Toc91926418)

[Hình 3.5 cấu hình R2 out (2) 35](#_Toc91926419)

[Hình 3.6 Cấu hình MLSwitch (1) 36](#_Toc91926420)

[Hình 3.7 Cấu hình MLSwitch (1) 37](#_Toc91926421)

[Hình 3.8 Cấu hình MLSwitch (3) 38](#_Toc91926422)

[Hình 3.9 Tạo tài khoản cho WLC (1) 39](#_Toc91926423)

[Hình 3.10 Tạo tài khoản cho WLC (2) 40](#_Toc91926424)

[Hình 3.11 Tạo tài khoản cho WLC (3) 41](#_Toc91926425)

[Hình 3.12 Tạo tài khoản cho WLC (4) 42](#_Toc91926426)

[Hình 3.13 Tab WLANs trong WLC 43](#_Toc91926427)

[Hình 3.14 cấu hình WLAN 103 (1) 43](#_Toc91926428)

[Hình 3.15 cấu hình WLAN 103 (2) 44](#_Toc91926429)

[Hình 3.16 cấu hình WLAN 103 (3) 44](#_Toc91926430)

[Hình 3.17 cấu hình WLAN 103 (4) 45](#_Toc91926431)

[Hình 3.18 cấu hình WLAN 104 (1) 46](#_Toc91926432)

[Hình 3.19 cấu hình WLAN 104 (2) 47](#_Toc91926433)

[Hình 3.20 cấu hình WLAN 104 (3) 48](#_Toc91926434)

[Hình 3.21 tab CONTROLLER 48](#_Toc91926435)

[Hình 3.22 Cấu hình WLAN 103 trong tab CONTROLLER 49](#_Toc91926436)

[Hình 3.23 Cấu hình WLAN 104 trong tab CONTROLLER 50](#_Toc91926437)

[Hình 3.24 cấu hình cho DNS server 51](#_Toc91926438)

[Hình 3.25 cấu hình cho RADIUS server 51](#_Toc91926439)

[Hình 3.26 IP Configuration của PC Admin 52](#_Toc91926440)

[Hình 3.27 cấu hình nhận WLAN103 với user1 52](#_Toc91926441)

[Hình 3.28 IP Configuration của NhanVien: user1 53](#_Toc91926442)

[Hình 3.29 cấu hình nhận WLAN103 với user2 53](#_Toc91926443)

[Hình 3.30 IP Configuration của NhanVien: user2 54](#_Toc91926444)

[Hình 3.31 cấu hình nhận WLAN104 với NhanVien lam them 1 54](#_Toc91926445)

[Hình 3.32 IP Configuration của NhanVien lam them 1 55](#_Toc91926446)

[Hình 3.33 cấu hình nhận WLAN104 với NhanVien lam them 2 55](#_Toc91926447)

[Hình 3.34 IP Configuration của NhanVien lam them 2 56](#_Toc91926448)

[Hình 3.35 cấu hình chọn mạng SSID DienMay cho máy khách 56](#_Toc91926449)

[Hình 3.36 IP Configuration của các khách hàng 57](#_Toc91926450)

[Hình 3.37 Truy cập đến WEB server từ domain được cấu hình ở DNS server 58](#_Toc91926451)

# CƠ SỞ LÝ THUYẾT

## Các khái niệm cơ bản

### Mạng không dây

#### Khái niệm

Mạng không dây là mạng kết nối các thiết bị có khả năng thu phát sóng (như máy vi tính có gắn Adapter buy modafinil không dây, PDA, …) lại với nhau. Không sử dụng dây dẫn mà sử dụng song vô tuyến được truyền dẫn trong không gian thông qua các trạm thu/phát sóng.

Một mạng không dây là một mạng máy tính sử dụng các kết nối dữ liệu không dây giữa các nút mạng. Mạng không dây được ưa thích bởi các hộ gia đình, các doanh nghiệp hay các cơ sở kinh doanh vừa và lớn có nhu cầu kết nối internet nhưng không thông qua quá nhiều cáp chuyển đổi. Các mạng không dây được quản lý bởi hệ thống truyền thông vô tuyến của các nhà mạng. Những hệ thống này thường được đặt tập trung hoặc rời rạc tại những cơ sở lưu trữ của các nhà mạng. Cấu trúc mạng thường được sử dụng là cấu trúc OSI.

Một số ví dụ về mạng không dây như: mạng wifi, mạng 3G, mạng điện thoại di động, mạng bluetooth, mạng nội bộ không dây (WLAN), mạng cảm biến không dây, mạng truyền thông vệ tinh và mạng sóng mặt đất.

Để dữ liệu hoặc thông tin được phân phối mạng không dây sử dụng sóng điện từ. Mạng không dây được sử dụng rộng rãi cho mạng máy tính hoặc khoảng cách ngắn vài mét với thiết bị bluetooth hoặc khoảng cách xa bằng vệ tinh. Hai mạng không dây phổ biến hiện nay là wifi và bluetooth.

#### Phân loại mạng không dây

Dựa theo độ rộng phủ song của mạng không dây mà người ta đã chia mạng này thành 4 loại là WPAN, WLAN, WMAN và WWAN.

* **Mạng WPAN – Wireless Personal Area Network**

Đây là một trong bốn loại mạng không dây có độ phủ sóng khá xa, khoảng 20m. Mạng WPAN được sử dụng cho một các nhân trong một không gian không lớn. Hiệu suất của mạng WPAN được xếp vào loại trung bình, với tốc độ dữ liệu lên đến 2 Mbps. WPAN được sử dụng trong các thiết bị như điện thoại thông minh, máy tính xách tay và PDA, ...

Những điểm ưu tiên mà WPAN sở hữu là tiêu thụ điện năng thấp, tính năng động cao cho phép người dùng truy cập thông tin ở mọi nếu đang ở trong phạm vi phủ sóng của mạng, thiết lập dễ dàng, nhanh chóng, linh hoạt, chi phí rẻ và có nhiều liên kết cấu trúc mạng (nếu cần).

* **Mạng cục bộ WLAN – Wireless Local Area Network**

WLAN hoặc mạng cục bộ không dây thường được sử dụng trong các công nghệ như điểm phát sóng và Wifi. Người dùng có thể sử dụng để giữ kết nối mà không cần dây mạng. Vì thế, máy tính xách tay hoặc thiết bị kết nối của người dùng được trang bị mạng cục bộ không dây này có thể di chuyển xung quanh tòa nhà và luôn kết nối ngay cả khi không có dây cáp. Mạng WLAN có khả năng phủ sóng khá rộng, tuy nhiên chi phí lắp đặt WLAN khá cao. Hạn chế của WLAN là độ trễ tương đối lớn, dung lượng mạng gặp khó khăn trong phổ tần hoặc không thể mở rộng dải tần.

* **Mạng không dây đô thị WMAN – Wireless Metropolitan Area Network.**

Mạng không dây này thường được sử dụng để kết nối các cơ sở khác nhau từ một trường đại học, các khối bệnh viện khác nhau và các tòa nhà văn phòng. Bản thân mạng dựa vào ánh sáng hồng ngoại mạnh hoặc sóng vô tuyến để truyền dữ liệu. Mạng WMAN này nằm giữa WWAN và WLAN.

Ưu điểm của mạn WMAN là các máy chủ văn phòng tại trung tâm, có thể được sử dụng để làm trung tâm dữ liệu từ các văn phòng chi nhánh. Thông tin có thể được phổ biến nhanh chóng, rộng rãi và có ý nghĩa hơn. Sau đó, các giao dịch có thể được thực hiện trong thời gian thực và giao tiếp giữa các văn phòng có thể sử dụng email để hội nghị truyền hình.

* **Mạng diện rộng WWAN – Wireless Wide Area Network**

Loại mạng không dây này có khả năng tiếp cận một khu vực rộng hơn WLAN. WWAN có khả năng phủ sóng toàn quốc, với tầng cơ sở được cung cấp bởi các nhà cung cấp dịch vụ không dây với chi phí sử dụng hàng tháng. Mạng WWAN cũng được sử dụng để cung cấp di động kết nối với Internet, với mức phủ sóng rộng cho các kỹ thuật viên thực hiện hoặc những người đi công tác. Ví dụ như di động hệ thống được sử dụng trong mạng này là EDGE, 3G, 4G, GSM, CDMA, HSDPA và GPRS.

#### Nguyên lý hoạt động của mạng không dây

Mạng WLAN sử dụng sóng điện từ (vô tuyến và tia hồng ngoại) để truyền thông tin từ điểm này sang điểm khác mà không dựa vào bất kỳ kết nối vật lý nào. Các sóng vô tuyến thường là các sóng mang vô tuyến bởi vì chúng thực hiện chức năng phân phát năng lượng đơn giản tới máy thu ở xa.

Dữ liệu truyền được chồng lên trên sóng mang vô tuyến để nó được nhận lại đúng ở máy thu. Đó là sự điều biến sóng mang theo thông tin được truyền. Một khi dữ liệu được chồng (được điều chế) lên trên sóng mang vô tuyến, thì tín hiệu vô tuyến chiếm nhiều hơn một tần số đơn, vì tần số hoặc tốc độ truyền theo bit của thông tin biến điệu được thêm vào sóng mang. Nhiều sóng mang vô tuyến tồn tại trong cùng không gian tại cùng một thời điểm mà không nhiễu với nhau nếu chúng được truyền trên các tần số vô tuyến khác nhau.

Để nhận dữ liệu, máy thu vô tuyến bắt sóng (hoặc chọn) một tần số vô tuyến xác định trong khi loại bỏ tất cả các tín hiệu vô tuyến khác trên các tần số khác. Trong một cấu hình mạng WLAN tiêu biểu, một thiết bị thu phát, được gọi một điểm truy cập (AP – access point), nối tới mạng nối dây từ một vị trí cố định sử dugj cáp Ethernet chuẩn. Điểm truy cập (access point) nhận, lưu vào bộ nhớ đệm, và truyền dữ liệu giữa mạng WLAN và cơ sở hạn tầng mạng nối dây.

Một điểm truy cập đơn hỗ trợ một nhóm nhỏ người sử dụng và vận hành bên trong một phạm vi vài mét tới hàng chục mét. Điểm truy cập (hoặc anten được gắn tới nó) thông thường được gắn trên cao nhưng thực tế được gắn bất cứ nơi đâu miễn là khoảng vô tuyến cần thu được. Các người dùng đầu cuối truy cập mạng WLAN thông qua các card giao tiếp mạng WLAN mà được thực hiện như các card PC trong các máy tính để bàn, hoặc các thiết bị tích hợp hoàn toàn bên trong các máy tính cầm tay. Các card giao tiếp mạng WLAN cung cấp một giao diện giữa hệ điều hành mạng (NOS) và sóng trời (qua một anten). Bản chất của kết nối không dây là trong suốt với NOS.

### Khái niệm mạng di động

Mạng di động (Cellular Network) là một mạng vô tuyến bao gồm một số lượng các tế bào vô tuyến (radio cell), được phục vụ bởi một máy phát (transmitter) cố định được gọi là các trạm gốc (cell site hoặc base station). Các tế bào vô tuyến này được dùng để phủ các vùng khác nhau với mục đích cung cấp vùng phủ sóng trên một diện rộng hơn gấp rất nhiều lần so với một tế bào. Mạng các tế bào vốn dĩ không đối xứng với một tập hợp các trạm thu phát vô tuyến chính cố định, mỗi trạm phục vụ một tế bào và một tập các trạm thu phát phân tán (thường là di động nhưng không phải lúc nào cũng như vậy) cung cấp dịch vụ cho người sử dụng.

### Mạng Wifi

#### Khái niệm

Wi-Fi là công nghệ mạng không dây cho phép các thiết bị như máy tính (máy tính xách tay và máy tính để bàn), thiết bị di động (điện thoại thông minh và thiết bị đeo được) và các thiết bị khác (máy in và máy quay video) giao tiếp với Internet. Wifi cho phép các thiết bị này - và nhiều thiết bị khác - trao đổi thông tin với nhau, tạo ra một mạng.

Kết nối Internet xảy ra thông qua bộ định tuyến không dây. Khi người dùng truy cập Wi-Fi, người dùng đó đang kết nối với bộ định tuyến không dây cho phép các thiết bị tương thích với Wi-Fi của bạn giao tiếp với Internet.

#### Mạng wifi hoạt động như thế nào?

Mạng WiFi hoặc mạng không dây sử dụng sóng vô tuyến để trao đổi thông tin giữa các thiết bị. Các sóng vô tuyến này được truyền trên tần số 2,4 GHz hoặc 5 GHz. Tần số phụ thuộc vào chuẩn 802.11 mà thiết bị sử dụng. Công nghệ tương tự được sử dụng cho điện thoại di động.

Các thiết bị sẽ không cần sử dụng bất kì loại cáp nào để kết nối với Internet mà thay vào đó người dùng sẽ sử dụng Wifi chỉ với ăng – ten (được ẩn bên trong thiết bị). Vì tín hiệu Wifi được truyền qua không khi nên bất kì người dùng nào sử dụng thiết bị có thể kết nối Wifi đều có thể kết nối được mạng wifi này.

Về mặt kỹ thuật, tiêu chuẩn IEEE 802.11 xác định các giao thức cho phép giao tiếp với các thiết bị không dây hỗ trợ Wi-Fi hiện tại, bao gồm bộ định tuyến không dây và điểm truy cập không dây. Các điểm truy cập không dây hỗ trợ các tiêu chuẩn IEEE khác nhau. Mỗi tiêu chuẩn là một sửa đổi đã được phê chuẩn theo thời gian. Các tiêu chuẩn hoạt động trên các tần số khác nhau, cung cấp băng thông khác nhau và hỗ trợ số lượng kênh khác nhau.

#### Điểm truy cập không dây là gì?

Điểm truy cập không dây (Access Point) cho phép các thiết bị không dây kết nối với mạng không dây. Có mạng không dây giúp dễ dàng đưa các thiết bị mới lên mạng và hỗ trợ linh hoạt cho nhân viên di động.

#### Mobile Hotspot là gì?

Điểm phát sóng di động (Mobile Hotspot) là một tính năng phổ biến trên điện thoại thông minh có cả kết nối có kết nối liên kết và kết nối không kết nối. Khi bật điểm phát sóng di động của điện thoại, thiết bị của người dùng sẽ chia sẻ kết nối mạng không dây của mình với các thiết bị khác có thể truy cập Internet.

#### Điểm phát sóng Wifi hotspot là gì?

Điểm phát sóng Wi-Fi hotspot là điểm phát sóng di động thu được thông qua nhà cung cấp dịch vụ điện thoại di động. Đó là một thiết bị nhỏ sử dụng tháp di động phát tín hiệu băng thông rộng 3G hoặc 4G tốc độ cao. Nhiều thiết bị, như iPad và máy tính xách tay, sau đó có thể kết nối không dây với thiết bị, từ đó kết nối liền mạch với Internet ở bất cứ nơi nào mà người dùng đến.

#### Kiến trúc Hotspot là gì?

Hot Spot là các mạng Wi-Fi chuyên dụng thường được triển khai tại các sân bay và nhà ga giúp người dùng có cơ hội kết nối Internet hoặc mạng nội bộ của họ nhờ kết nối không dây.

### Tổng quan về AAA

AAA là một framework (bộ khung) được thiết kế thông minh dùng để kiểm soát truy cập trên hệ thống thông tin. AAA cho phép nhà quản trị mạng biết được các thông tin quan trọng về tình hình cũng như mức độ an toàn trong mạng. Giao thức này cung cấp việc xác thực (authentication) người dùng nhằm bảo đảm có thể nhận dạng đúng người dùng. Một khi đã nhận dạng người dùng, nhà phát triển sẽ có thể giới hạn thẩm quyền (authorization) mà người dùng có thể làm. Khi người dùng sử dụng mạng, các quản trị viên này cũng có thể giám sát tất cả những gì mà họ làm. AAA được chia làm ba dịch vụ với xác thực (authentication), cấp quyền (authorization), tính cước (accounting) là các phần riêng biệt mà ta có thể sử dụng trong dịch vụ mạng, cần thiết để mở rộng và bảo mật mạng. AAA có thể dùng để tập hợp thông tin từ nhiều thiết bị trên mạng. Có thể bật các dịch vụ AAA trên router, switch, firewall, các thiết bị VPN, server, …

Để hiểu hơn về các dịch vụ của giao thức AAA, dưới đây sẽ là tìm hiểu sự khác nhau của ba phần này và cách thức chúng làm việc như thể nào.

* **Xác thực (Authentication)**

Xác thực dùng để nhận dạng (identify) người dùng. Trong suốt quá trình xác thực, username và password của người dùng được kiểm tra và đối chiếu với cơ sở dữ liệu lưu trong AAA Server. Tất nhiên, tùy thuộc vào giao thức mà AAA hỗ trợ mã hóa đến đâu, ít nhất thì cũng mã hóa username và password.

Sau khi xác thực thành công thì người dùng đó có thể truy cập được vào mạng. Tiến trình này chỉ là một trong các thành phần để điều khiển người dùng với AAA. Một khi username và password được chấp nhận, AAA có thể dùng để định nghĩa thẩm quyền mà người dùng được phép làm trong hệ thống.

* **Thẩm quyền (Authorization)**

Authorization cho phép nhà quản trị điều khiển việc cấp quyền trong một khoảng thời gian, hay trên từng thiết bị, từng nhóm, từng người dùng cụ thể hay trên từng giao thức. AAA cho phép nhà quản trị tạo ra các thuộc tính mô tả các chức năng của người dùng được phép làm. Do đó, người dùng phải được xác thực trước khi cấp quyền cho người đó. AAA Authorization làm việc giống như một tập các thuộc tính mô tả những gì mà người dùng đã được xác thực có thể có. Những thuộc tính xác thực được so sánh với cơ sở dữ liệu của người dùng, sau đó kết quả sẽ được trả về nhằm xác định khả năng và giới hạn thẩm quyền của người dùng đó. Điều này yêu cầu cơ sở dữ liệu phải giao tiếp liên tục với AAA server trong suốt quá trình kết nối đến thiết bị truy cập từ xa (RAS).

* **Tính cước (Accounting)**

Accounting hay tính cước sẽ cho phép nhà quản trị có thể thu thập thông tin như thời gian bắt đầu, thời gian kết thúc người dùng truy cập vào hệ thống, các câu lệnh đã thực thi, thống kê lưu lượng, việc sử dụng tài nguyên và sau đó lưu trữ thông tin trong hệ thống cơ sở dữ liệu quan hệ. Nói cách khác, accounting cho phép giám sát dịch vụ và tài nguyên được người dùng sử dụng. Điểm chính trong Accounting đó là cho phép người quản trị giám sát tích cực và tiên đoán được dịch vụ và việc sử dụng tài nguyên. Thông tin này có thể được dùng để tính cước khách hàng, quản lý mạng, kiểm toán sổ sách.

#### Giao thức AAA trong bảo mật và điều khiền truy cập mở rộng trong mạng

Ngày nay, các nhà quản trị mạng phải chịu trách nhiệm điều khiển việc truy cập và giám sát thông tin mà người dùng đang thao tác. Điều đó là hết sức cần thiết vì chúng ảnh hưởng rất nhiều đến việc thành công hay thất bại của bất kì doanh nghiệp nào. Với mục đích đó, giao thức AAA là giải pháp tốt nhất để giám sát những gì mà người dùng đầu cuối có thể thao tác với mạng. Với giao thức này các nhà quản trị mạng có thể xác thực (Authentication) người dùng, cấp quyền (Authorization) cho người dùng và tập hợp được thông tin như thời gian bắt đầu hay kết thúc của người dùng (Accounting). Chính vì lẽ đó mà có thể thấy được vấn đề bảo mật luôn được đặt lên hàng đầu trong bất kì lĩnh vực nào.

#### Giao thức bảo mật sử dụng cho dịch vụ AAA

Trong dịch vụ AAA có hai giao thức bảo mật là TACACS (Terminal Access Controller Access Control System) và RADIUS (Remote Authentication Dial-In User Service). Cả hai giao thức này đều có phiên bản và thuốc tính riêng như phiên bản riêng của TACACS là TACACS+ (một phiên bản hoàn toàn tương thích với TACACS). RADIUS tương tự như giao thức TACACS, cũng có sự mở rộng khi cho phép khách hàng thêm thông tin xác định được mang bởi RADIUS. TACACS và RADIUS được dùng từ một thiết bị như server truy cập mạng (NAS) đến AAA server. Để dễ hiểu hơn về việc một cuộc gọi từ xa thì đầu tiên người dùng gọi từ PC đến NAS. Tiếp đến, sau khi NAS nhận được cuộc gọi, NAS sẽ hỏi thông tin để xác thực người dùng. TIếp tục, từ PC đến NAS, giao thức sử dụng PPP (Point-to-Point Protocol là một giao thức liên kết dữ liệu, thường được dùng để thiết lập một kết nối trực tiếp giữa 2 nút mạng), và một giao thức như là CHAP (Challenge Handshake Authentication Protocol (CHAP) là một phương pháp chứng thực được sử dụng nhiều trong giao thức PPP. CHAP xác nhận người dùng sử dụng cơ chế three-way hand shake - bắt tay 3 bước) hay PAP (Password Authentication Protocol là phương pháp chứng thực đơn giản của giao thức PPP) được dùng để truyền thông xác thực. Và cuối cung, NAS sẽ truyền thông tin truyền thông tin đến AAA Server để xác thực. Thông tin được truyền đó đều được vận chuyển bởi giao thức TACACS và RADIUS.

#### TACACS là gì?

TACACS là giao thức được chuẩn hóa sử dụng giao thức hướng kết nối (connection-oriented) là TCP trên port 49. Giao thức TACACS có các ưu điểm sau:

TCP (Transmission Control Protocol) là giao thức mở rộng vì có khả năng xây dựng cơ chế phục hồi lỗi. Giao thức có thể tương thích để phát triển cũng như làm tắc nghẽn mạng với việc sử dụng sequence number để truyền lại.

Với khả năng nhận gói reset (RST) trong TCP, một thiết bị có thể lập tức báo cho đầu cuối khác biết rằng đã có hỏng hóc trong quá trình truyền.

TCP là giao thức mở rộng vì có khả năng xây dựng cơ chế phục hồi lỗi. Nó có thể tương thích để phát triển cũng như làm tắc nghẽn mạng với việc sử dụng sequence number để truyền lại.

Toàn bộ payload được mã hóa với phiên bản mở rộng TACACS+ bằng cách sử dụng một khóa bí mật chung (shared secret key). TACACS+ đánh dấu một trường trong header để xác định xem thử có mã hóa hay không.

Phiên bản mở rộng TACACS+ mã hóa toàn bộ gói bằng việc sử dụng khóa bí mật chung nhưng bỏ qua header TACACS chuẩn. Cùng với header là một trường xác định body có được mã hóa hay không. Thường thì trong toàn bộ thao tác, body của một gói được mã hóa hoàn toàn để truyền thông an toàn.

TACACS+ được chia làm ba phần: xác thực (authentication), cấp quyền (authorization) và tính cước (accounting). Với cách tiếp cận theo module, ta có thể sử dụng các dạng khác của xác thực và vẫn sử dụng TACACS+ để cấp quyền và tính cước. Chẳng hạn như, việc sử dụng phương thức xác thực Kerberos cùng với việc cấp quyền và tính cước bằng TACACS+ là rất phổ biến.

TACACS+ hỗ trợ nhiều giao thức.

Với TACACS+, ta có thể dùng hai phương pháp để điều khiển việc cấp quyền thực thi các dòng lệnh của một user hay một nhóm nhiều user:

* Phương pháp thứ nhất là tạo một mức phân quyền (privilege) với một số câu lệnh giới hạn và user đã xác thực bởi router và TACACS server rồi thì sẽ được cấp cho mức đặc quyền xác định nói trên.
* Phương pháp thứ hai đó là tạo một danh sách các dòng lệnh xác định trên TACACS+ server để cho phép một user hay một nhóm sử dụng.

TACACS thường được dùng trong môi trường enterprise. Nó có nhiều ưu điểm và làm việc tốt đáp ứng yêu cầu quản lý mạng hàng ngày.

#### Tổng quan về RADIUS

RADIUS là giao thức bảo mật mạng dựa theo mô hình client-server. Giao thức này dùng giao thức UDP (User Datagram Protocol). RADIUS server thường chạy trên máy tính. Client là các dạng thiết bị có thể truyền thông tin đến RADIUS server được chỉ định trước và sau đó đóng vai trò phản hồi thông tin trả về. Giao tiếp giữa client và RADIUS server được xác thực thông qua việc sử dụng khóa bí mật chung không được truyền qua mạng.

Một số ưu điểm của RADIUS là:

* RADIUS có phần overhead ít hơn so với TACACS vì nó sử dụng UDP, trong phần overhead không có địa chỉ đích, port đích.
* Với cách thức phân phối dạng source code, RADIUS là dạng giao thức hoàn toàn mở rộng. Người dùng có thể thay đổi nó để làm việc với bất kì hệ thống bảo mật hiện có.
* RADIUS yêu cầu chức năng tính cước (accounting) mở rộng.

Nhược điểm của giao thức RADIUS:

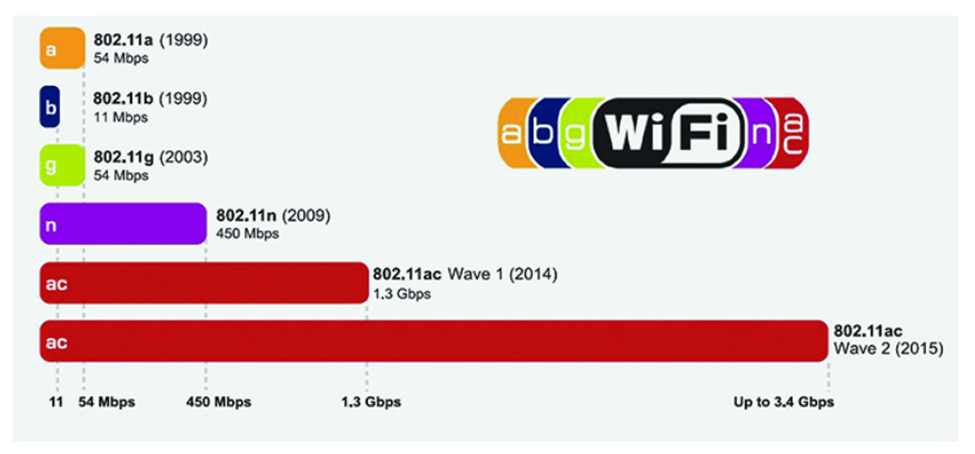
* Chỉ mã hóa mật khẩu trong gói access - request
* Không hỗ trợ truy cập ARA, Net Bios Frame Protocol Control Protocol, NASI X.25
* Không cho phép người dùng thực thi các dòng lệnh trên thiết bị định tuyến.

#### Ứng dụng RADIUS

RADIUS được ứng dụng rộng rãi để quản lý và chứng thực người dùng một cách tập trung cho kết nối VPN, WLAN, ... Với việc tổ chức quản lý người dùng theo các OU, Group được phần quyền và áp dụng các chính sách thích hợp để đáp ứng như cầu bảo mật dữ liệu truyền đi trên mạng. RADIUS còn có chức năng Accounting nhằm kiểm soát người dùng một cách chặt chẽ theo dạng file log.

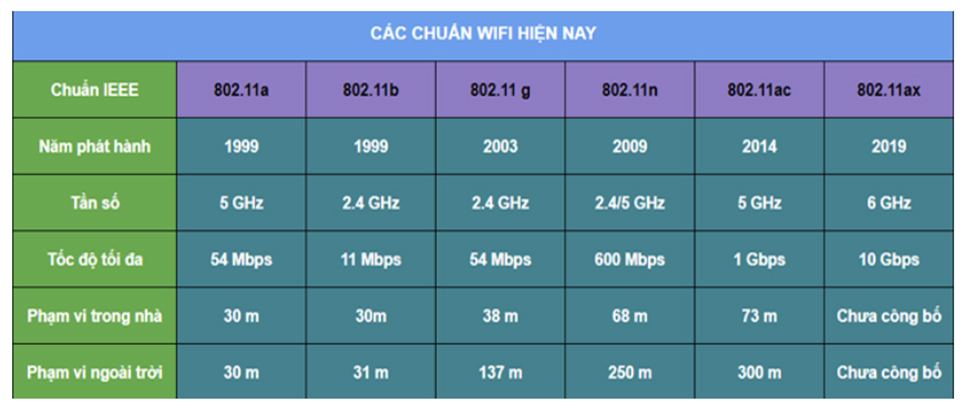
### Một số chuẩn kết nối hiện nay

Chuẩn WLAN IEEE 802.11



Hình 1.1 Lịch sử phát triển của chuẩn IEEE 802.11

* **Chuẩn wifi 802.11:** Vào năm 1997, IEEE giới thiệu chuẩn mạng không dây đầu tiên và đặt tên nó là 802.11. Khi đó, tốc độ hỗ trợ tối đa của mạng này chỉ là 2 Mbps với băng tầng 2.4GHz.
* **Chuẩn wifi 802.11b:** Vào tháng 7/1999, chuẩn 802.11b ra đời và hỗ trợ tốc độ lên đến 11Mbps. Chuẩn này cũng hoạt động tại băng tần 2.4GHz nên cũng rất dễ bị nhiễu từ các thiết bị điện tử khác.
* **Chuẩn wifi 802.11a:** Song song với quá trình hình thành chuẩn 802.11b, chuẩn 802.11a phát ở tần số cao hơn là 5GHz nhằm tránh bị nhiễu từ các thiết bị khác. Tốc độ xử lý của chuẩn đạt 54 Mbps tuy nhiên chuẩn này khó xuyên qua các vách tường và giá cả của nó hơi cao.
* **Chuẩn wifi 802.11g:** Chuẩn 802.11g có phần hơn so với chuẩn b, tuy nhiên nó cũng hoạt động ở tần số 2.4GHz nên vẫn dễ nhiễu. Chuẩn này có thể xử lý tốc độ lên tới 54 Mbps.
* **Chuẩn wifi 802.11n:** Ra mắt năm 2009 và là chuẩn phổ biến nhất hiện nay nhờ sự vượt trội hơn so với chuẩn b và chuẩn g. Chuẩn kết nối 802.11n hỗ trợ tốc độ tối đa lên đến 300Mbps, có thể hoạt động trên cả băng tần 2,4 GHz và 5 GHz. Chuẩn kết nối này đã và đang dần thay thế chuẩn 802.11g với, phạm vi phát sóng lớn hơn, tốc độ cao hơn và giá hợp lý.
* **Chuẩn wifi 802.11ac:** Đây là chuẩn được IEEE giới thiệu vào đầu năm 2013, hoạt động ở băng tầng 5 GHz. Chuẩn ac có thể mang đến cho người dùng trải nghiệm tốc độ cao nhất lên đến 1730 Mpbs. Do vấn đề giá thành cao nên các thiết bị phát tín hiệu cho chuẩn này chưa phổ biến dẫn đến các thiết bị này sẽ bị hạn chế sự tối ưu do thiết bị phát.
* **Chuẩn wifi 802.11ad:** Được giới thiệu năm 2014, chuẩn wifi 802.11ad được hỗ trợ băng thông lên đến 70 Gbps và hoạt động ở dải tần 60GHz. Nhược điểm của chuẩn này là sóng tín hiệu khó có thể xuyên qua các bức tường, đồng nghĩa với việc chỉ cần Router khuất khỏi tầm mắt, thiết bị sẽ không còn kết nối tới Wifi được nữa.
* **Chuẩn wifi 802.11ax:** Wi-Fi 6 là bản cập nhật mới nhất cho chuẩn mạng không dây. Wi-Fi 6 dựa trên tiêu chuẩn IEEE 802.11ax, với tốc độ nhanh hơn, dung lượng lớn hơn và hiệu suất năng lượng được cải thiện tốt hơn so với các kết nối không dây trước đây. Tên gọi mới Wifi 6 này sẽ chính thức được áp dụng từ năm 2019.



Hình 1.2 Mô tả thông số của các chuẩn IEEE 802.11

Chuẩn WPAN IEEE 802.15: WPAN 802.15 tập trung vào việc phát triển các tiêu chuẩn đồng thuận cho mạng khu vực cá nhân hoặc mạng không dây khoảng cách ngắn. Các WPAN này xử lý mạng không dây của các thiết bị máy tính di động như PC, thiết bị hỗ trợ kỹ thuật số cá nhân (PDAs), thiết bị ngoại vi, điện thoại di động, máy nhắn tin và thiết bị điện tử tiêu dùng, cho phép các thiết bị này giao tiếp và tương tác với nhau trong một phạm vi nhỏ. Ban đầu, tiêu chuẩn này được phát triển vào năm 1999 với mục đích cho phép giao tiếp trong khoảng cách ngắn. Tiêu chuẩn 802.15 được IEEE đề xuất nhằm chia các loại mạng WPAN theo tốc độ truyền, mức tiêu hao năng lượng, chất lượng dịch vụ, ... Cụ thể hơn thì chuẩn này được chia làm ba loại sau:

* IEEE 802.15.1: tiêu chuẩn nổi tiếng nhất là cơ sở của công nghệ Bluetooth.
* IEEE 802.15.3: định nghĩa công nghệ UWB.
* IEEE 802.15.4: cơ sở của đặc điểm kỹ thuật Zigbee. Mục đích của nhóm này là cung

So sánh các chuẩn WPAN IEEE 802.15:

* Chuẩn IEEE 802.15.1 – Bluetooth: có tốc độ trung bình, hiện nay vẫn được sử dụng rộng rãi.
* Chuẩn IEEE 802.15.3 – UWB: có tốc độ cao, dùng trong các ứng dụng đa phương tiện.
* Chuẩn IEEE 802.15.4 – Zigbee: có tốc độ thấp, được ứng dụng trong công nghiệp, y tế; nó đòi hỏi mức tiêu hao năng lượng thấp, không yêu cầu tốc độ truyền và chất lượng dịch vụ.

|  |  |  |  |
| --- | --- | --- | --- |
|  | IEEE 802.15.1  Bluetooth | IEEE 802.15.3  UWB | IEEE 802.15.4  Zigbee |
| Tầm hoạt động (m) | 1-3 | 1-10 | 1-100 |
| Số lượng nút mạng | 7 | 4000 | >64000 |
| Ứng dụng phổ biến | Web, mail | videoHD, 4K | Giám sát, điều khiển |
| Độ rộng băng tần (kB) | 250 | 500000 | 4-32 |
| Tốc độ truyền (Kbps) | 720 | 480000 | 20-250 |
| Dải tần hoạt động (Hz) | 2,4-2,8 | 3,1-10,6 | 0,868; 0,915; 2,45 |

Bảng 1.1 So sánh IEEE 802.15.1; IEEE 802.15.3 và IEEE 802.15.4

### Tổng quan về WEP và WPA.

* **WEP – Wired Equivalent Privacy**

WEP là giải pháp bảo mật đầu tiên được ứng dụng cho mạng không dây dựa trên tiêu chuẩn 802.11 dùng cho việc mã hóa dữ liệu trên mạng WLAN (Wireless LAN) cũng như mã hóa khóa chia sẽ (pre-shared key) dùng để xác thực các WLAn Client. WEP sử dụng khóa mã hóa RC4 có độ dài 64 bit hoặc 128 bit để mã hóa dữ liệu tại lớp 2 trong mô hình OSI. Tuy nhiên, trong 64 bit hay 128 bit này thì có 24 bit được dành cho việc tạo các giá trị Initialization Vector (IV). Tiến trình mà RC4 xử dụng các giá trị IV để tạo ra các khóa chia sẽ chính là điểm yếu của WEP và khiến cho nó có khả năng bị bẽ gãy. Trước đây việc chờ đợi để thu thập đủ các gói tín sẽ mất nhiều thời gian nhưng với các kỹ thuật gởi các yêu cầu giả mạo đến Access Point sẽ giúp cho hacker có thể nhanh chóng tổng hợp đủ dữ liệu và bẻ khóa WEP trong thời gian chưa đầy 5 phút. Một trong những công cụ thường được sử dụng cho dạng tấn công này là Backtrack 5.

Vì WEP là một thuật toán mã hóa yếu nên nó còn được gọi bằng tên Weak Encryption Protocol, tuy nhiên trên các hệ thống phần cứng cũ vẫn sử dụng WEP cho nên các router hay modem wifi ngày nay vẫn phải hỗ trợ giao thức này nhằm bảo đảm cho vấn đề tương thích.

* **WPA - Wifi Protected Access**

Đây là giải pháp bảo mật được phát triển để khắc phục những điểm yếu của WEP. WPA được Wi-fi Alliance xây dựng vào năm 2003, đây được xem là giải pháp thay thế cho WEP mà không cần phải có sự thay đổi về phần cứng, tuy nhiên những thay đổi này chỉ là một phần bổ sung của 802.11i. Có hai chế độ được sử dụng trong WPA là Personal và Enterprise nhưng chế độ thường dùng là WPA Personal hay còn gọi là WPA Preshared Key (PSK). Với WPA Personal hệ thống sử dụng một chuỗi ký tự ASCII để xác thực người dùng còn WPA Enterprise sử dụng hệ thống xác thực tập trung RADIUS, nếu như người dùng muốn triển khai hệ thống Wifi xác thực dựa trên thông tin tài khoản của người dùng trong Active Directory thì phải sử dụng chế độ này. Mặc dù WPA Enterprise an toàn và mạnh mẽ hơn so với WPA Personal nhưng do vấn đề triển khai phức tạp nên trong các hệ thống thông thường hay ứng dụng WPA Personal.

WPA sử dụng giao thức TKIP để mã hóa dữ liệu và xác thực người dùng (các máy tính của người sử dụng) cho cả hai trường hợp WPA Personal và WPA Enterprise, TKIP là viết tắt của Temporal Key Integrity Protocol (giao thức toàn vẹn khoá thời gian) có độ an toàn hơn RC4 rất nhiều. Để mã hóa một mạng với WPA Personal (hay PSK), người dùng cần cung cấp một mật khẩu có độ dài từ 8 đến 63 ký tự. Mật khẩu này sau đó sẽ được kết hợp với SSID thông qua thuật toán TKIP để tạo các khoá mã hoá duy nhất cho từng máy trạm không dây. Các khoá đã được mã hoá này được thay đổi thường xuyên giúp loại bỏ các điểm nhạy cảm mà WEP mang lại.

Vào năm 2004, Wi-Fi Alliance đã công bố đấy đủ tiêu chuẩn IEEE 802.11i với cơ chế xác thực WPA2 như một sợ mở rộng của WPA nhưng sử dụng giao thức mã hóa nâng cao AES, đây là một giao thức được xem như là “không thể bị bẻ khóa”, WPA2 có thể sử dụng kết hợp TKIP hay AES trong chế độ mixed mode security cho quá trình mà hóa dữ liệu. Cả WPA Personal và WPA2 Personal sử dụng một chuỗi chia sẽ trước gọi là passphare để xác thức WLAn Client, còn WPA Enterprise và WPA2 Enterprise xác thực WLAN client qua máy chủ RADIUS sử dụng chuẩn 802.1X/Extensible Authenti-cation Protocol (EAP).

## Các hình thức tấn công mạng không dây

Những chuẩn công nghệ IEEE đều tồn tại một lổ hỗng bảo mật lớn làm cho hệ thống mạng không dây trở nên thiếu an toàn hơn bất kì hệ thống mạng nào, đó là do cơ chế phát sóng vô tuyến dựa trên nền tảng truyền thông broadcast mà ở đó bất cứ máy tính nào cũng có thể nhận được tín hiệu của nhau, miễn là chúng cùng nằm trong một lớp mạng. Bên cạnh đó, công nghệ mã hóa và xác thực dựa trên WEP của các tiêu chuẩn trên đã được chứng minh là không an toàn, có thể bị hacker bẻ khóa và xâm nhập vào hệ thống trong vòng 15 phút.

### Những rủi ro khi sử dụng mạng không dây

Tổ chức an ninh mạng BKIS đã từng cảnh báo các hệ thống wifi ở nhà hay một số doanh nghiệp sử dụng các cấu hình mặc định cho hệ thống quản lý truy cập Wifi là WAP (Wireless Access Point), với các thông tin mặc định này thì hacker có thể dễ dàng đoán được mật khẩu quản trị của WAP và thay đổi các thông tin cấu hình dẫn đến những mục tiêu nguy hiểm hay chặn bắt thông tin nhạy cảm của người dùng thông qua phương pháp nghe lén. Vì thế cần có trách nhiệm thay đổi các cầu hình mặc định nhằm để nâng cao tính an toàn cho mạng không dây. Có một số giải pháp được áp dụng để có thể giải các quyết vấn đề trên như xác thực người dùng với WPA/WPA2 (tuyệt đối không sử dụng WEP), kiểm soát việc gia nhập hệ thống dựa trên địa chỉ MAC của thiết bị mạng hay sử dụng certificate cho quá trình xác thực, yêu cầu phài gia nhập domain mới kết nối được vào mạng wifi, …

### Các dạng tấn công mạng không dây phổ biến

* **Sniffing attack**

Đây là hình thức tấn công thông dụng trên mạng không dây (WLAN), Sniffing sẽ nghe lén và đánh cắp thông tin rất dễ tiến hành trên các hệ thống Access Point được cấu hình mặc định vì các gói tin sẽ được truyền theo cách thức không an toàn với cơ chế truyền broadcast mà không có biện pháp mã hóa nào. Vì thế, những mật khẩu và tài khoản của người dùng trong các giao thức như FTP, POP3, SMTP dễ dàng bị hacker đánh cắp. Các mạng WLAN được xác định thông qua tên của chúng là SSID, tên này được gởi dưới dạng không mã hóa trong các gói tin beacon, do đó hacker sẽ dễ dàng phát hiện được tên những hệ thống mạng WLAN. Mặc dù hầu hết các AP có khả năng cấu hình để ẩn các SSID nhằm hạn chế sự tấn công nhưng đây không hẳn là một chức năng đem đến sự an toàn cao, vì có khá nhiều công cụ có thể phát hiện ra các SSID thông qua những gói tin khác mà chúng bắt được trên mạng.

* **Snoofing attack**

Ở trường hợp này các hacker giả mạo làm một trạm phát sóng với thông tin cấu hình giống như các AP hợp lệ, nếu người dùng kết nối đến các Access Point (AP) spoofing này thì thông tin của họ sẽ hoàn toàn chuyển đến cho những kẻ tấn công. Ngày nay, trên các hệ thông máy tính MAC có chức năng cho phép một máy chia sẽ kết nối với những hệ thống MAC khác, điều này cũng có thể bị các kẻ tấn công lợi dụng để tạo ra các AP giả mạo. MAC spoofing là hình thức tấn công giải mạo địa chỉ MAC để vượt qua sự kiếm soát ở mức vật lý của Access Point. Ví dụ như khi AP xác thực các máy tính dựa trên địa chỉ vật lý của card mạng thì tin sẽ áp dụng hình thức giả mạo này.

* **Denial of Service (DoS):**

Denial of Service hay còn gọi là tấn công từ chối dịch vụ, đây là phương thức tấn công không loại trừ đối với bất kì hệ thống hay dịch vụ nào, kể cả các mạng không dây. Một trong những đặc trưng của hệ thống mạng không dây là có tần số sóng gần với các dãy sóng của thiết bị viba và các thiết bị cầm tay khác và kẻ tấn công có thể tận dụng điều này để làm nhiễu loạn môi trường của mạng không dây làm cho chúng không hoạt động được.

* **Rogue Access Point**

Access Point giả mạo (Rogue Access Point) là cụm từ được dùng để mô tả những AP được tạo ra một cách vô tình hoặc cố ý nhằm làm ảnh hưởng đến hệ thống mạng không dây hiện có. Có nhiều cách để phân loại các AP giả mạo. Trong đó, bốn loại AP giả mạo thường gặp trong mạng WLAN là:

* Access Point được cấu hình không hoàn chỉnh
* Access Point giả mạo từ các mạng WLAN lân cận
* Access Point giả mạo do kẻ tấn công tạo ra
* Access Point giả mạo được thiết lập bởi chính nhân viên của công ty
* De-authentication Flood Attack (tấn công yêu cầu xác thực lại)

De-authentication Flood Attack được tạo ra nhằm hướng đến các mục tiêu tấn công là người dùng đang kết nối và giao tiếp trong mạng không dây. Trong đó, người dùng sẽ nhận được các frame yêu cầu xác thực thông tin giả mạo địa chỉ MAC nguồn và đích từ kẻ tấn công. Khi đó, người dùng sẽ bị ngắt khỏi dịch vụ liên kết mạng WLAN và kẻ tấn công sẽ thực hiện các bước tương tự với những người dùng khác.

* **Fake Access Point**

Với Fake Access Point, kẻ tấn công sẽ gửi các gói beacon với địa chỉ vật lý (MAC) và SSID giả để tạo ra nhiều điểm truy cập giả lập. Quá trình này sẽ gây xáo trộn toàn bộ các phần mềm điều khiển card mạng không dây của người dùng trên hệ thống.

* **Tấn công dựa trên sự cảm nhận sóng mang lớp vật lý**

Với phương thức này, kẻ tấn công sẽ tìm cách tạo ra lỗi nghẽn mạng vì nhầm lẫn tín hiệu. Điều này có thể được thực hiện bằng hình thức tạo ra một nút giả truyền tin liên tục đồng thời sử dụng bộ tạo tín hiệu RF hoặc làm cho card mạng chuyển vào chế độ kiểm tra.

* **Tấn công ngắt kết nối (Disassociation flood attack)**

Với kỹ thuật tấn công này, đầu tiên kẻ tấn công xác định mục tiêu và mối liên kết giữa điểm truy cập với các clients. Sau đó sẽ gửi disassociation frame bằng cách giả mạo địa chỉ MAC nguồn và đích đến AP với các client tương ứng. Tiếp đến, Client sẽ nhận các frame này và nghĩ rằng frame hủy kết nối đến từ AP. Tiếp tục, kẻ tấn công tiếp tục thực hiện tương tự với các client còn lại làm cho các client tự động ngắt kết nối với AP. Và cuối cùng, khi bị ngắt kết nối, client sẽ thực hiện kết nối lại với AP ngay lập tức. Kẻ tấn công sẽ tiếp tục gửi disassociation frame đến AP và client.

## Các phương pháp bảo mật cơ bản

Ngày nay, hầu như doanh nghiệp, gia đình đều trang bị mạng không dây và cụ thể là wifi. Tuy nhiên vấn đề bảo mật mạng không dây chưa thực sự được quan tâm đúng đắn trong khi wifi rất dễ bị hacker và các đối tượng xấu trên internet xâm phạm. Vì môi trường kết nối của mạng không dây là không khí nên khả năng bị xâm nhập của người dùng cao hơn so với mạng có dây. Các kẻ tấn công có thể thực hiện hành vi nghe lén với các thiết bị sử dụng mạng wifi công cộng, dẫn đến việc bị lộ, lấy cắp thông tin nhạy cảm, mật khẩu, email, ... Chính vì lẽ đó mà các phương pháp bảo mật mạng không dây rất được người dùng quan tâm, chúng ta hay tìm hiểu một số phương pháp mạng bảo mật mạng không dây sau:

* **Thay đổi tên mạng (SSID)**

Đâu tiên, mỗi người dùng hay doanh nghiệp sau khi lắp đặt wifi thì tên mặc định của router sẽ dễ gây chú ý cho kẻ tấn công vì những kẻ này đều biết tên mạng mặc định mà các nhà sản xuất router và ISP thường sử dụng. Chính vì điều đó mà các nhân viên kỹ thuật sau khi lắp đặt wifi thường khuyến khích thay đổi tên mạng, nếu không thì hacker sẽ tìm ra loại router mà người dùng đang sử dụng và tấn công dễ dàng hơn vào mạng không dây wifi đó. Để tiến hành đổi tên mạng SSID có thể làm theo các bước đơn giản sau:

Bước 1: Nhập địa chỉ IP router của bạn vào thanh address trên bất kỳ trình duyệt nào.

Bước 2: Đăng nhập với tên và mật khẩu quản trị mạng (thường có trên thiết bị router).

Bước 3: Vào mục Cài đặt (settings)

Bước 4: Tìm đến mục Wireless Network Name (SSID)

Bước 5: Tiến hành đổi tên mạng

* **Sử dụng mã hóa mạnh để bảo mật wifi**

Đây là một trong những điều bắt buộc để bảo mật mạng không dây. Nếu bỏ qua việc này mọi hành động, thông tin trên thiết bị đều có thể bị xâm phạm bởi bất cứ ai. Phần lớn các bộ định tuyến wifi đều bị tắt tính năng mã hóa, đây là điều hết sức nguy hiểm. Không phải bất cứ chuẩn mã hóa nào đều cũng tốt như nhau, nếu như khả năng bảo mật của chúng đều ngang nhau thì các nhà phát triển sẽ không cần phải xây dựng các chuẩn mới. Vì thế cần nên lựa chọn các chuận mã hóa đủ tốt để có thể an tâm tham gia vào không gian mạng không dây.

Nếu như thiết bị hỗ trợ chuẩn mã hóa WPA2 thì hãy sử dụng ngay bởi vì đây là chuẩn bảo mật tốt nhất hiện nay. tiếp đến là WPA Personal hay WPA – PSK, đây là chuẩn không phải tốt nhất nhưng ít nhất nó tốt hơn chuẩn mã hóa WEP – chuẩn mã hóa rất dễ bị tấn công dễ dàng.

Cũng cần nên thiết lập phiên bản mã hóa doanh nghiệp. Những cách thiết lập phiên bản doanh nghiệp khá phức tạp. Đối với thuật toán mã hóa (WPA Algorithms) nên chọn AES và không nên dùng TKIP. Bởi AES sẽ cung cấp mã hóa mạnh khó tấn công hơn TKIP.

* **Thay đổi tên người dùng và mật khẩu**

Thay đổi tên người dùng và thay đổi mật khẩu cũng là cách để bảo mật wifi. Bởi thông thường các hacker sẽ thường thử tấn công mạng không dây của người dùng bằng tên người dùng và mật khẩu. Nếu không hack được thì chúng mới áp dụng cách tấn công khác. Điểu đặc biệt là các hacker này thường có công cụ để tra cứu dò ra mật khẩu cũng như tên người dùng rất nhanh. Do đó, không nên để mật khẩu quá đơn giản. Lời khuyên cho người dùng là hãy thay đổi tên người dùng và mật khẩu bằng một dãy ký tự khó đoán. Đồng thời người dùng cũng nên kết hợp chữ hoa chữ thường và các con số để tạo nên một dãy tên người dùng và mật khẩu vô nghĩa. Điều này sẽ khiến cho những kẻ tấn công khó dò ra được tên người dùng và mật khẩu hơn.

* **Sử dụng mật khẩu mạnh**

Cách bảo mật wifi đơn giản tiếp theo nên áp dụng là chọn mật khẩu mạnh cho wifi nhà mình. Một mật khẩu wifi mạnh cần đảm bảo một vài yếu tố về độ dài (độ dài lý tưởng là ít nhất 15 ký tự), dãy mật khẩu nên có các ký tự đặc biệt.

* **Vô hiệu hóa mạng khách**

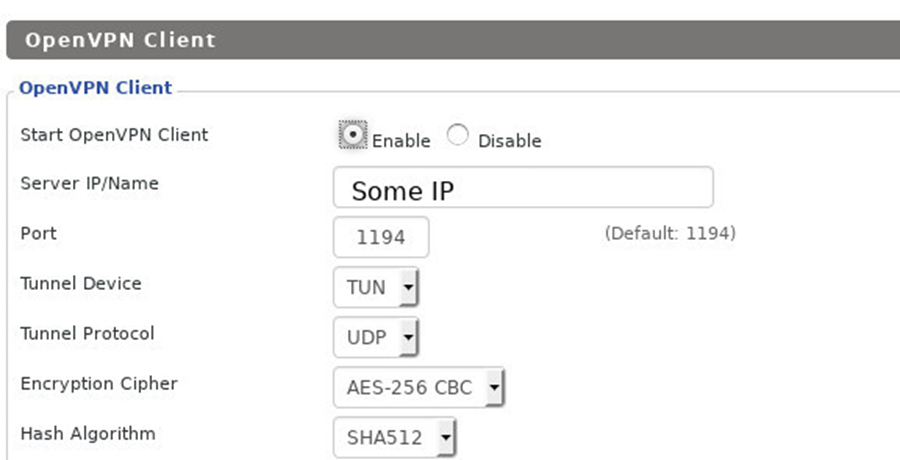
Vô hiệu hóa mạng khách cũng là cách bảo mật mạng không dây an toàn cho mạng gia đình. Nhiều gia đình để mạng wifi chế độ mở giúp bất kì ai cũng có thể kết nối wifi mà không cần mật khẩu. Tuy nhiên cách để mạng khách mở như này rất nguy hiểm. Tốt nhất là người dùng mạng không dây nên vô hiệu hóa mạng khách bằng một dãy mật khẩu riêng. Và sau khi họ rời đi hãy thay đổi mật khẩu wifi gia đình lại.

* **Bật tường lửa để bảo mật wifi**

Một số bộ định tuyến wifi sẽ được cài sẵn tường lửa. Để bảo mật mạng không dây người dùng nên bật tường lửa này lên. Tường lửa được ví như hàng phòng thủ giúp bảo vệ mạng không dây của mạng không dây của người dùng. Tường lửa có tác dụng quản lý và lọc tất cả các lưu lượng truy cập vào mạng wifi. Thậm chí nó có thể khóa, ngăn chặn các truy cập nguy hiểm cho mạng không dây.

* **Sử dụng VPN**

Ưu điểm khi sử dụng VPN là có thể ngăn chặn các kẻ tấn công vào mạng wifi của người dùng. Cách dùng VPN như sau, đầu tiên là kết nối wifi với máy chủ VPN. Sau đó kết nối wifi với internet. Các lưu lượng truy cập sẽ được quản lý thông qua VPN. Đặc biệt, VPN có thể ẩn danh một phần lưu lượng truy cập mạng. Điều này sẽ giúp bảo mật wifi tốt hơn.



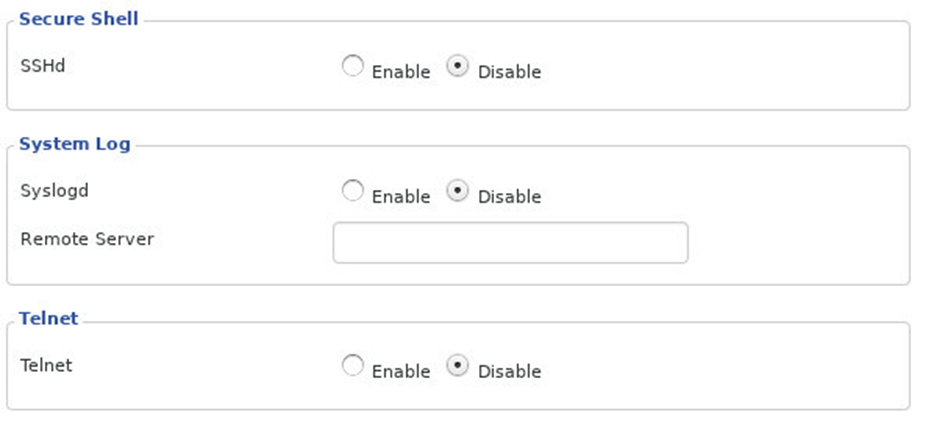
Hình 1.3 VPN

* **Tắt WPS**

WPS được hiểu là một hệ thống được kết nối với wifi đã được mã hóa mà không cần sử dụng mật khẩu. Nhược điểm của WPS là nó có thể tạo điều kiện cho những kẻ tấn công dễ dàng tấn công mạng không dây hơn. Do đó, hãy tắt WPS để đảm bảo an toàn tối đa cho mạng không dây của gia đình hoặc doanh nghiệp.

* **Tắt quản lý từ xa/ dịch vụ không cần thiết**

Một số bộ định tuyến cho phép quản lý từ xa. Điều này có thể sẽ giúp người dùng quản lý bộ định tuyến dễ dàng hơn. Nhưng nó cũng tiềm ẩn nhiều rủi ro và nguy hiểm cho mạng không dây nhà bạn. Bởi những kẻ tấn công hoàn toàn có thể truy cập vào giao diện quản lý bộ định tuyến và xâm nhập mạng không dây của người dùng. Do đó, để đảm bảo tính bảo mật wifi bạn nên tắt dịch vụ quản lý từ xa của bộ định tuyến.



Hình 1.4 Tắt quản lý từ xa/ dịch vụ không cần thiết

# MÔ TẢ ĐỀ TÀI

## Yêu cầu thiết kế

### Giới thiệu doanh nghiệp

Công ty Cổ phần Đầu tư Thế Giới Di Động (MWG) là nhà bán lẻ có trụ chính tại Việt Nam, được thành lập vào tháng 3 năm 2004 chuyên cung cấp các thiết bị gia dụng, điện tử uy tín với phương châm “đạo phục vụ khách hàng” cùng với đó là gần 1.000 siêu thị hiện diện tại 63 tỉnh thành trên khắp Việt Nam và cũng là chuỗi bán lẻ thiết bị di động có thị phần số 1 Việt Nam.



Hình 2.1 Logo Điện máy Xanh

### Yêu cầu của khách hàng

Công ty đang có nhu cầu mở cửa hàng mới nhằm tăng phạm vi kinh doanh, yêu cầu của khách hàng gồm có một mạng riêng dành cho nhân viên toàn thời gian và bán thời gian, một mạng dành cho khách mua hàng tại cửa hàng. Đảm bảo các bảo mật cần thiết để đảm bảo không bị rò rỉ dữ liệu ra bên ngoài, có thể truy cập mạng ở khắp mọi nơi trong phạm vi cửa hàng mà không lo bị ngắt kết nối, đảm bảo đường truyền mạng ổn định khi cửa hàng đang hoạt động.

### Đề xuất hướng giải quyết

Cần xây dựng 1 hệ thống mạng không dây quản lý nhân viên tách biệt với khách mua hàng tại cửa hàng. Đảm bảo việc vận hành hệ thống diễn ra suôn sẻ trong quá trình cửa hàng hoạt động, xây dựng chiến lược sao lưu và phục hồi dữ liệu cùng với đó khả năng nâng cấp hệ thống dễ dàng, không tốn nhiều thời gian, chi phí.

## Thiết kế mô hình

### Cấu trúc hệ thống mạng:

Khu vực khách hàng sẽ có một Access Point riêng để cấp mạng miễn phí cho khách hàng, khách hàng không cần mật khẩu mà chỉ cần truy cập vào SSID của mạng wifi

Có Access Point dùng giao thức Lightweight AP Protocol để phát 2 mạng Wifi (số lượng dự tính là 2 để có thể phát mạng đủ cả khu vực):

* Một mạng dành cho nhân viên công ty dùng RADIUS server để xác thực, có user và password riêng cho mỗi nhân viên
* Một mạng dành cho nhân viên làm thêm chỉ cần dùng password để có thể vào.

Một Multilayer Switch để Access Point kết nối vào và kết nối với Router công ty được đặt tại phòng kỹ thuật.

Hệ thống mạng sẽ được câú hình và kiếm soát bằng WLC ( Wireless Access Controller) và có một máy tính bàn để kết nối

Các thiệt bị kết nối với các mạng sẽ được cấp địa chỉ DHCP tự động cho từng mạng

Trong phần Demo chúng em chỉ dùng 2 thiết bị truy cập vào mạng dành cho nhân viên công ty, 2 thiết bị dành cho nhân viên làm thêm và 4 thiết bị khách hàng để test kết nối mạng

### Chi phí dự tính

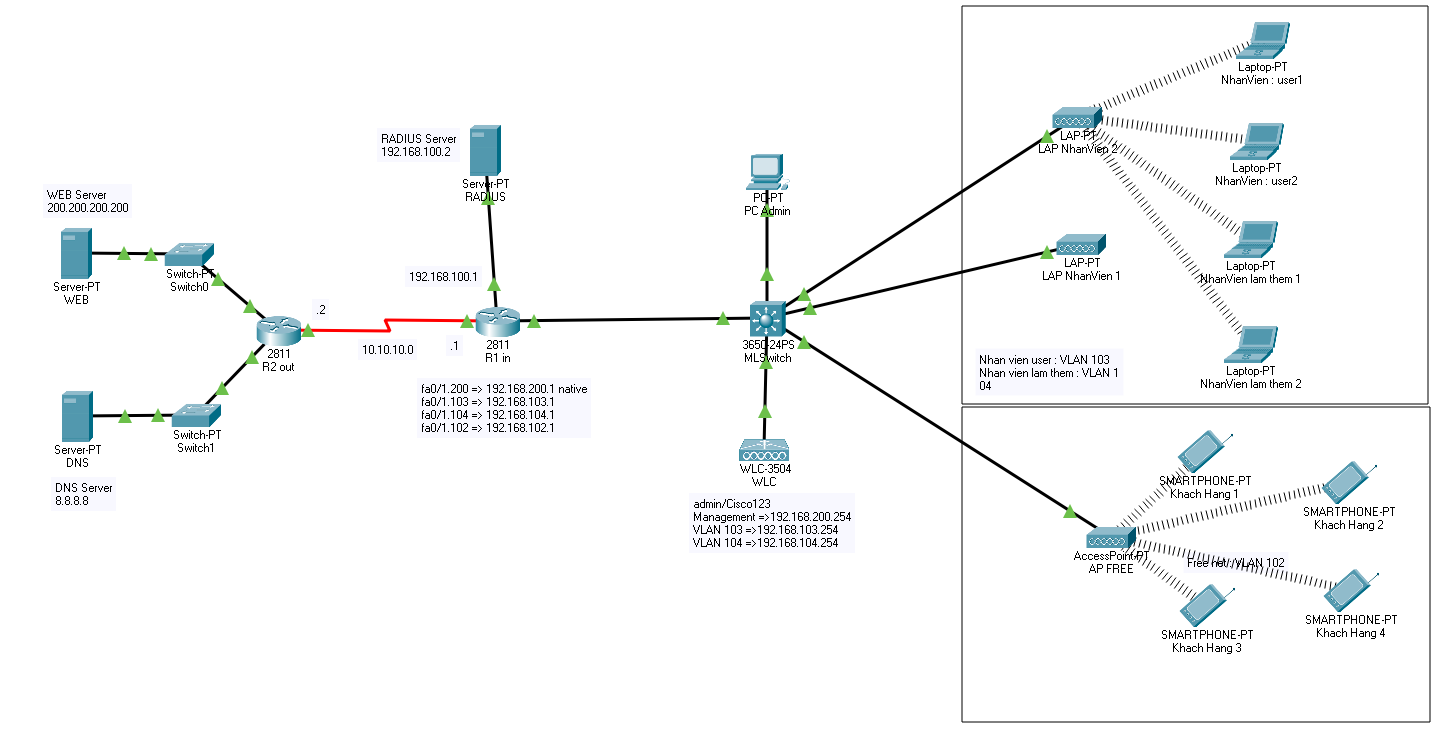
|  |  |  |
| --- | --- | --- |
| **Tên** | **Số lượng** | **Chi phí dự tính** |
| Radius server | 1 | 18,000,000đ |
| Access Point | 3 | 28,000,000đ |
| WLC | 1 | 12,000,000đ |
| MLSwitch | 1 | 8,000,000đ |
| Router | 1 | 33,500,000đ |
| PC admin | 1 | 10,000,000đ |
| **Tổng** | | 165,500,000đ |

Bảng 2.1 Bảng chi phí dự tính cho các thiết bị

Lưu ý:Chi phí dự tính có thể không chính xác chỉ có thể dùng để ước tính chi phí cần thiết để tạo nên mô hình mạng này

# DEMO

## Mô hình mạng



Hình 3.1 Mô hình mạng

Bảng địa chỉ:

|  |  |  |
| --- | --- | --- |
| **Device** | **Interface** | **IP address** |
| R1 in | f0/0 | 192.168.100.1/24 |
| f0/1.102 | 192.168.102.1/24 |
| f0/1.103 | 192.168.103.1/24 |
| f0/1.104 | 192.168.104.1/24 |
| f0/1.200 | 192.168.200.1/24 |
| s0/0/0 | 10.10.10.1/24 |
| MLSwitch | VLAN 200 |  |
| WLC | Management | 192.168.200.254/24 |
| PC Admin | NIC | DHCP |
| LAP NhanVien 1 | G0 | DHCP |
| LAP NhanVien 2 | G0 | DHCP |
| RADIUS | NIC | 192.168.100.2 |
| R2 out | f0/0 | 200.200.200.1 |
| f0/1 | 8.8.8.1 |
| s0/0/0 | 10.10.10.2 |
| WEB | NIC | 200.200.200.200 |
| DNS | NIC | 8.8.8.8 |
| Khach hang 1 | Wireless | DHCP |
| Khach hang 2 | Wireless | DHCP |
| Khach hang 3 | Wireless | DHCP |
| Khach hang 4 | Wireless | DHCP |
| NhanVien : user1 | Wireless | DHCP |
| NhanVien : user2 | Wireless | DHCP |
| NhanVien lam them 1 | Wireless | DHCP |
| NhanVien lam them 2 | Wireless | DHCP |

Bảng 3.1 Bảng địa chỉ IP

Bản thông tin WLAN:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **WLAN** | **SSID** | **Authentication** | **Username** | **Password** |
| WLAN 103 | WLAN\_103 | WPA-2 Enterprise | user1  user2 | user1  user2 |
| WLAN 104 | WLAN\_104 | WPA-2 Personal | N/A | abcd1234 |
| FREE | DienMay | disable | N/A | N/A |

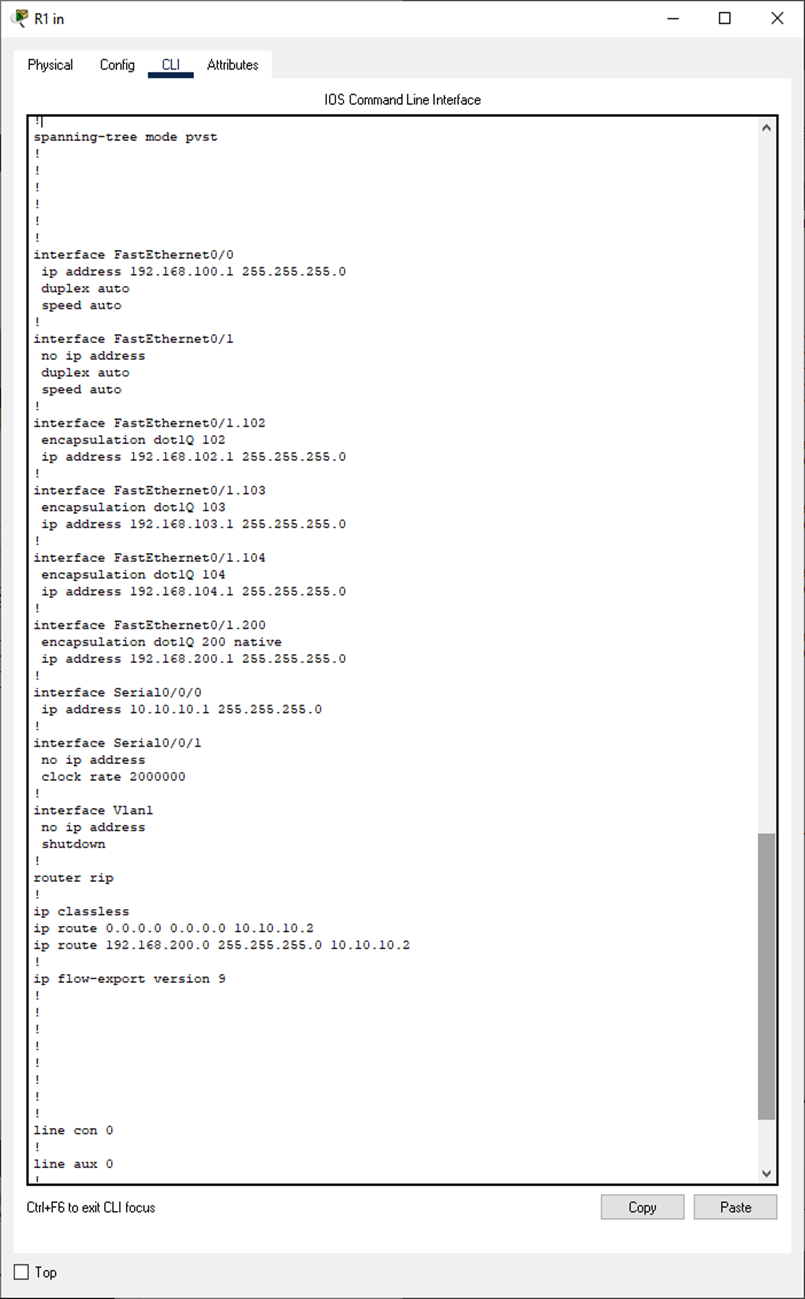
Bảng 3.2 Bảng thông tin WLAN

## Thông tin cấu hình

* Cấu hình R1 in

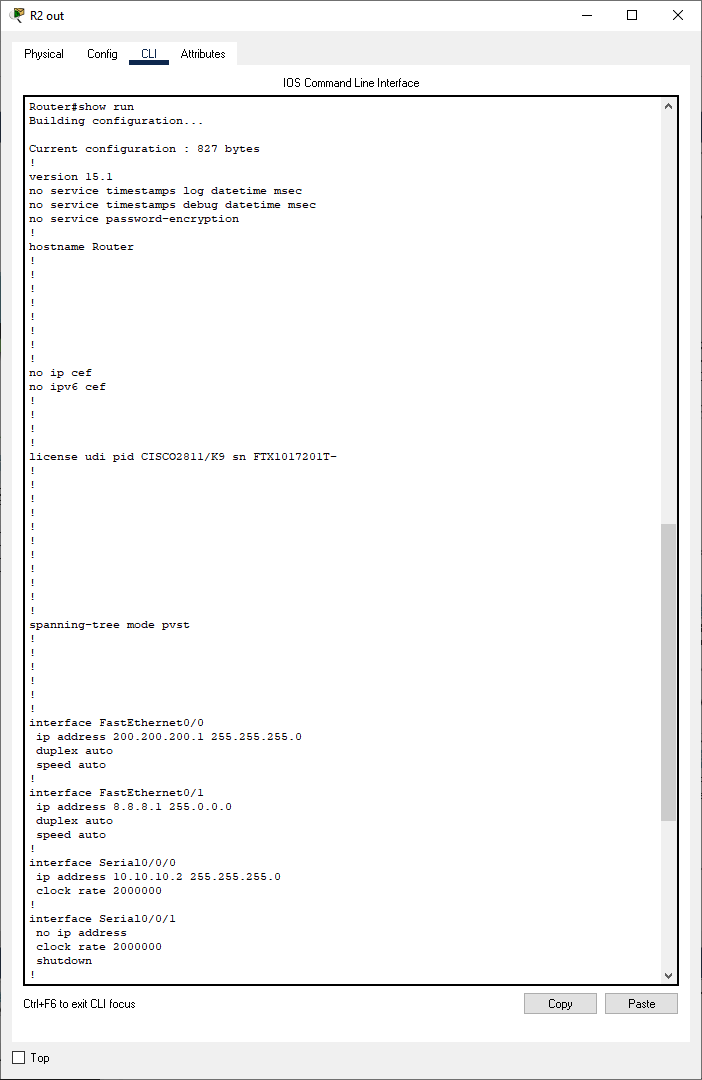


Hình 3.2 cấu hình R1 in (1)

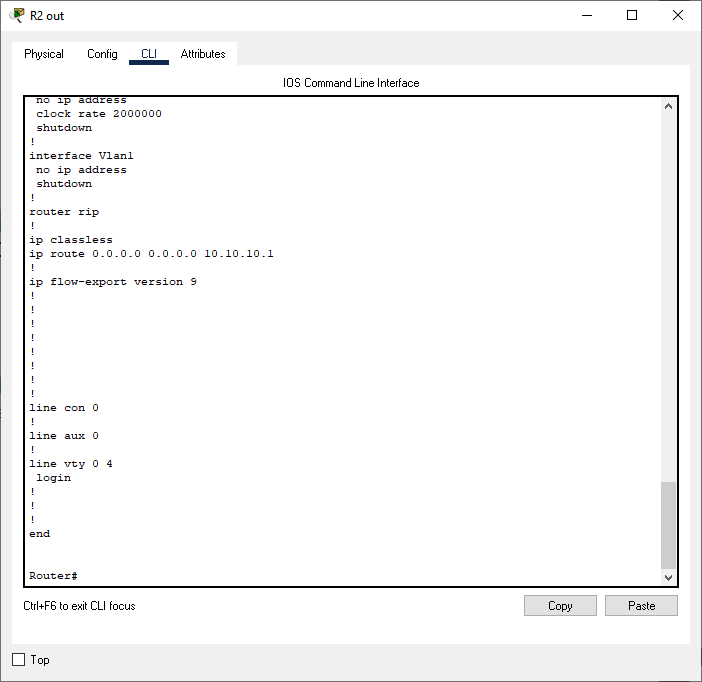


Hình 3.3 cấu hình R1 in (2)

* Cấu hình R2 out:



Hình 3.4 cấu hình R2 out (1)

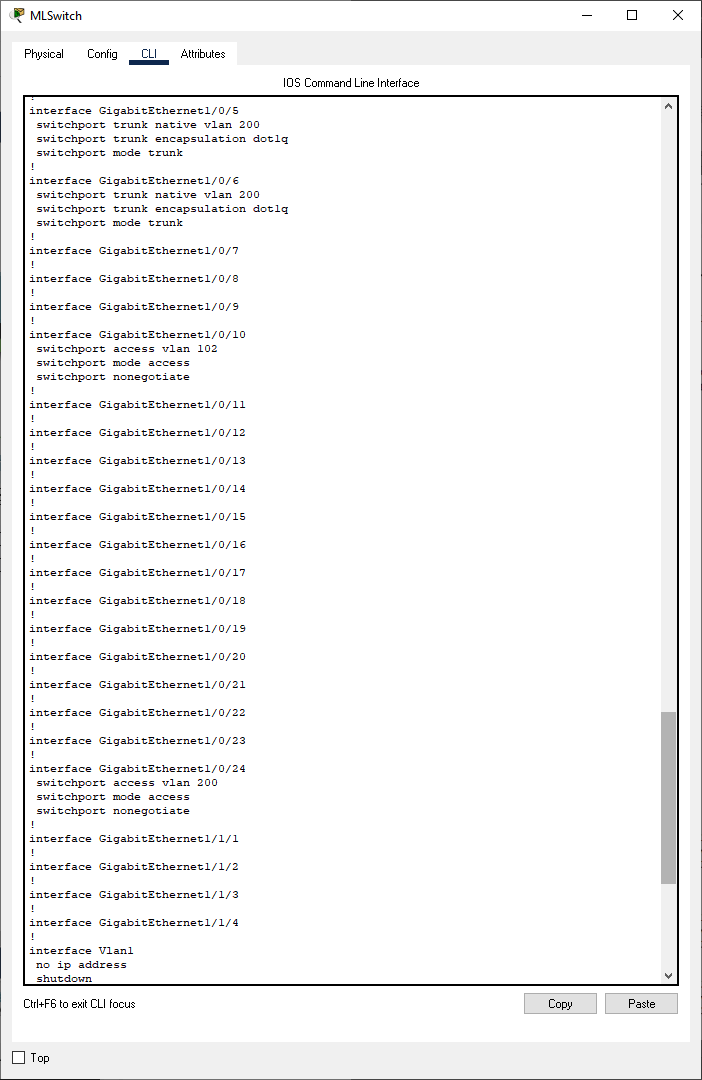


Hình 3.5 cấu hình R2 out (2)

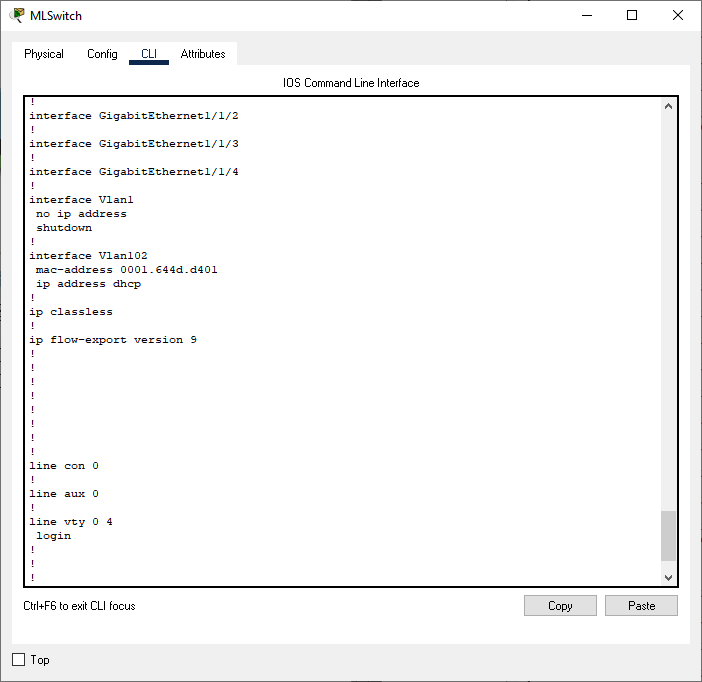
* Cấu hình MLSwitch



Hình 3.6 Cấu hình MLSwitch (1)



Hình 3.7 Cấu hình MLSwitch (1)



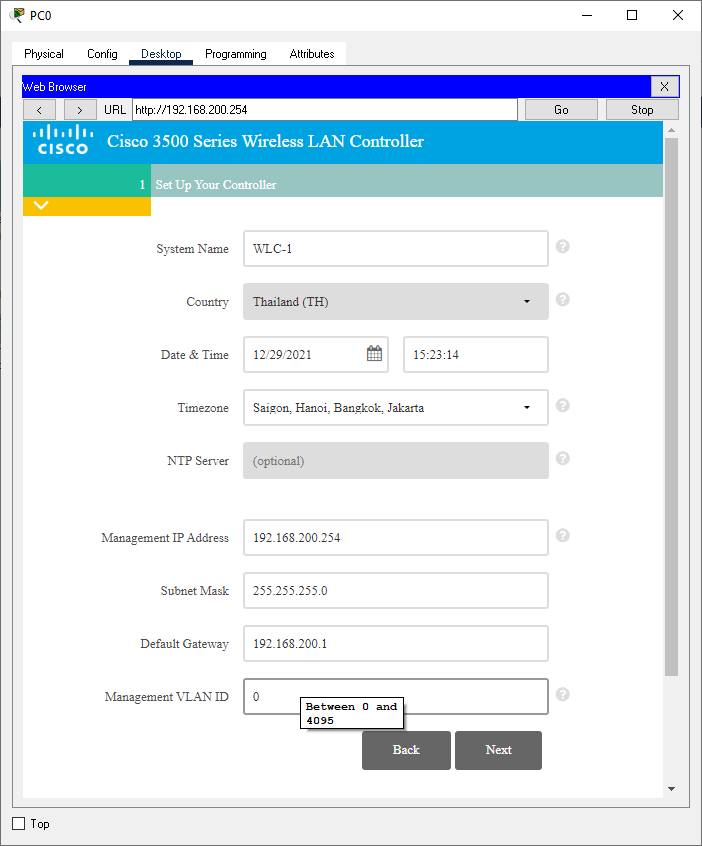
Hình 3.8 Cấu hình MLSwitch (3)

Cấu hình WLC từ PC admin. Đầu tiên ta phải tạo tài khoản admin cho WLC

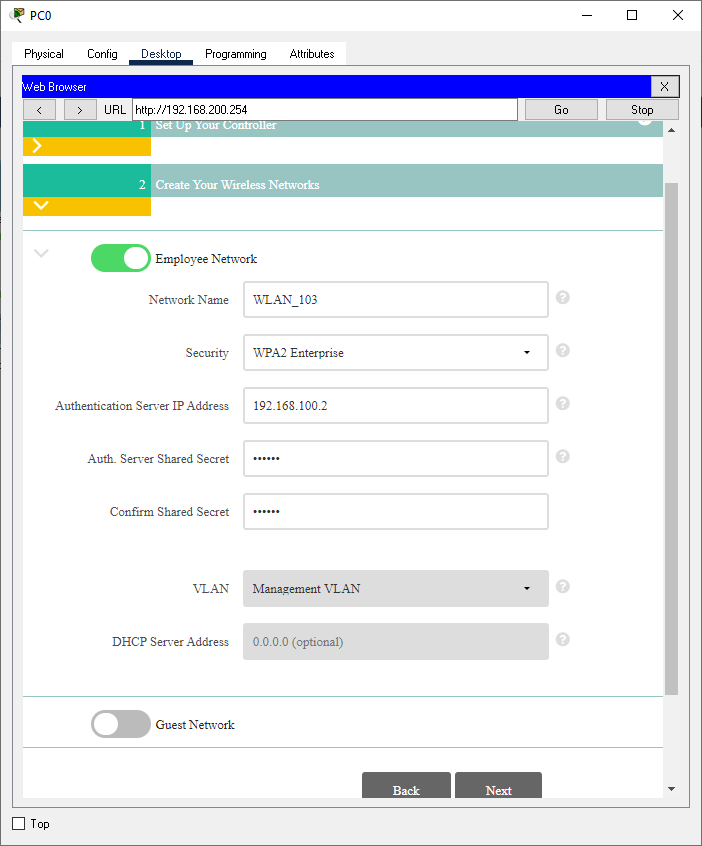
Truy cập vào địa chỉ http://192.168.200.254



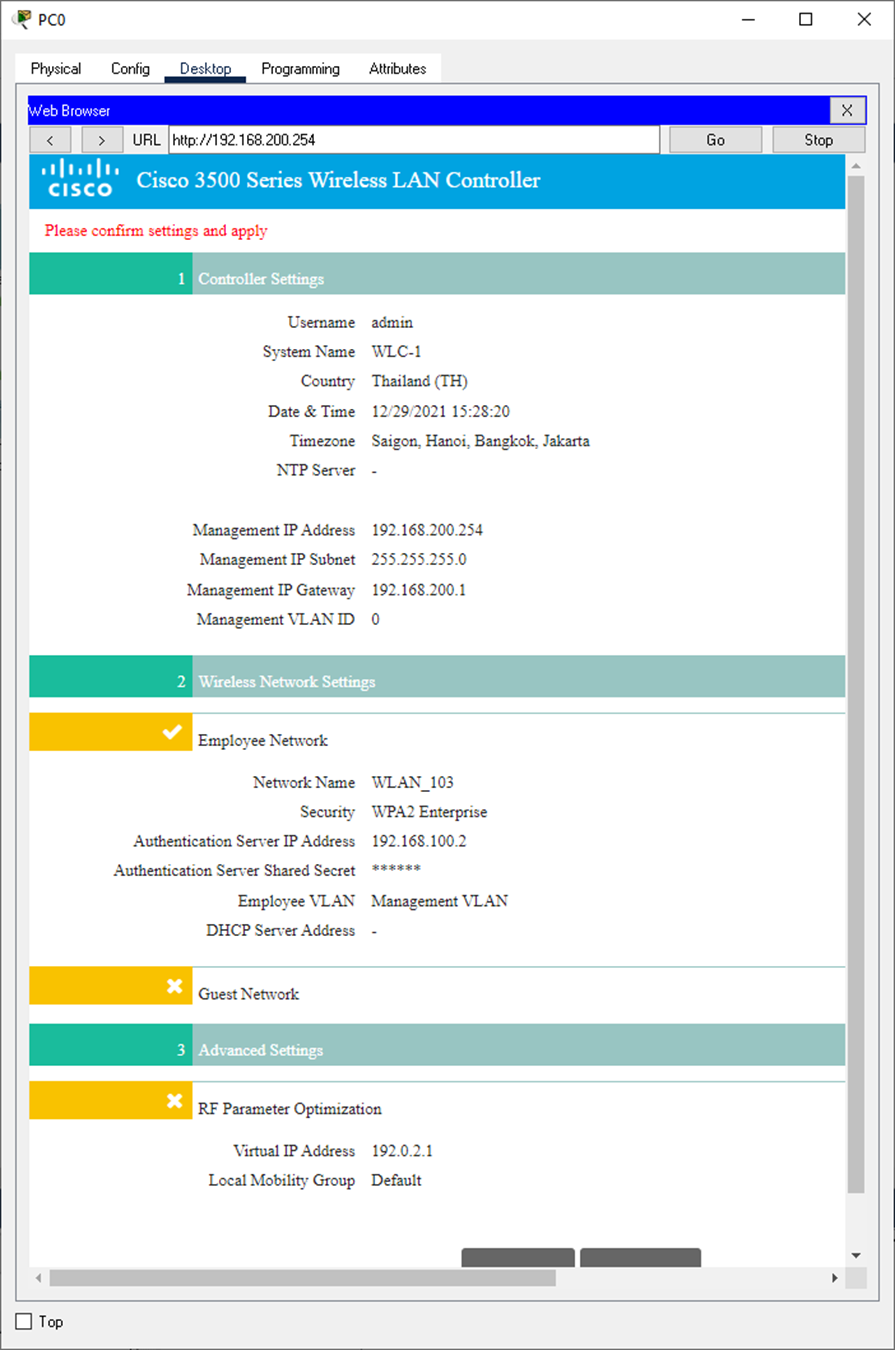
Hình 3.9 Tạo tài khoản cho WLC (1)



Hình 3.10 Tạo tài khoản cho WLC (2)



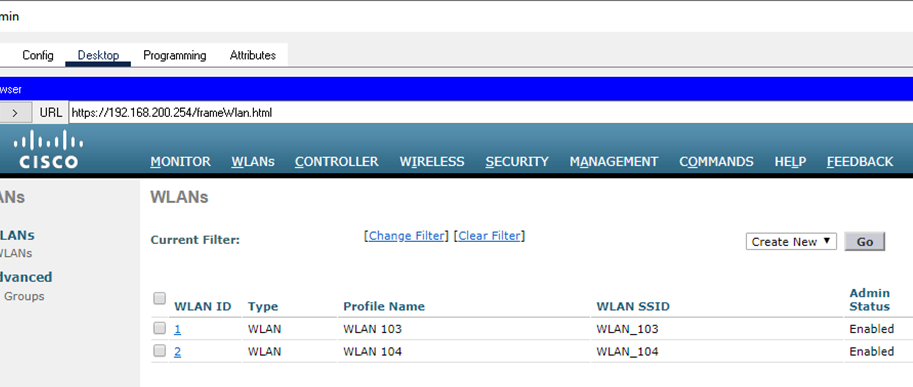
Hình 3.11 Tạo tài khoản cho WLC (3)



Hình 3.12 Tạo tài khoản cho WLC (4)

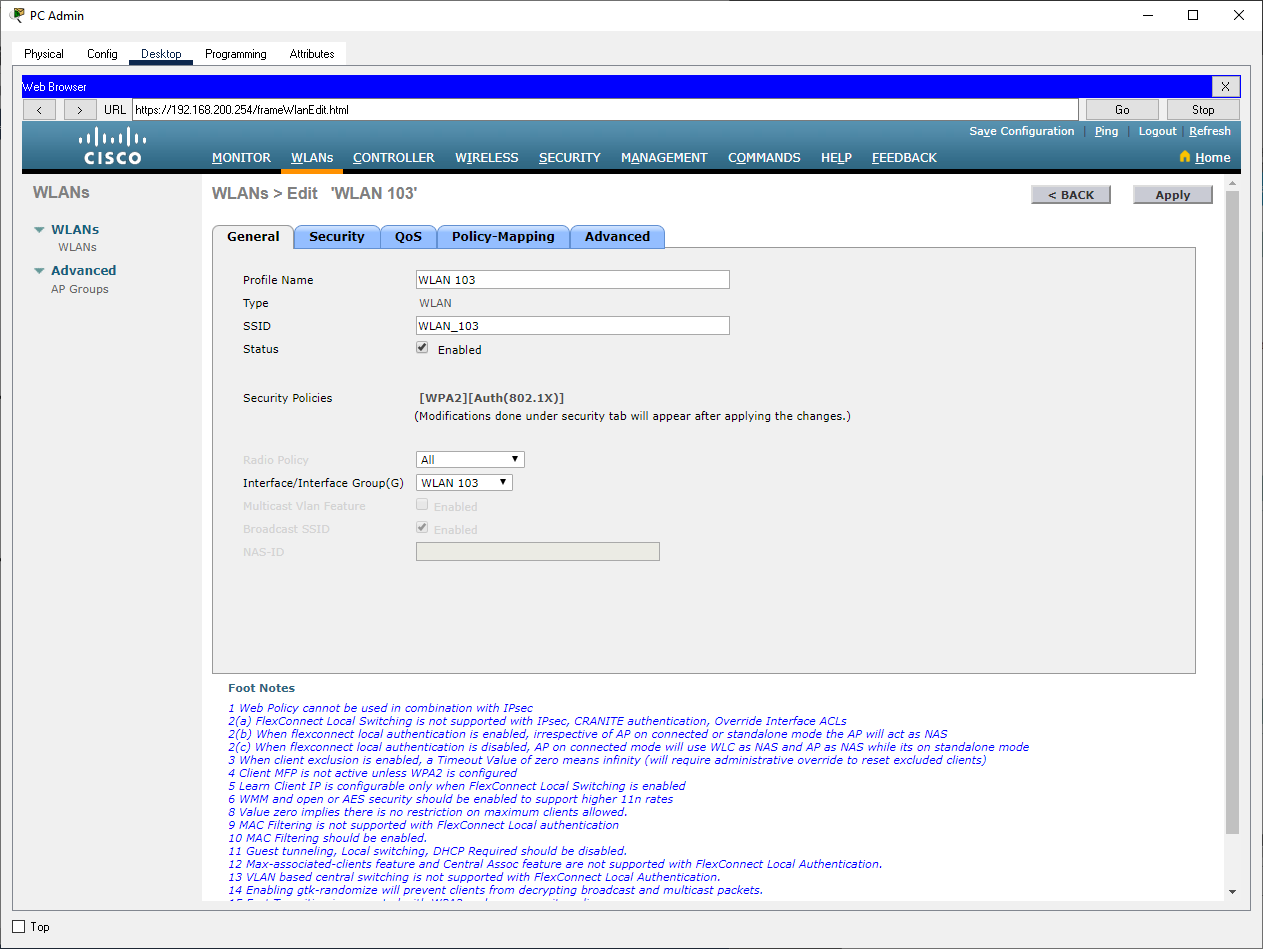
Sau khi tạo xong tài khoản thì vào trang https://192.168.200.254

Trong tab WLANs ta tạo thêm WLAN 104 và cấu hình cho cả 2 WLAN

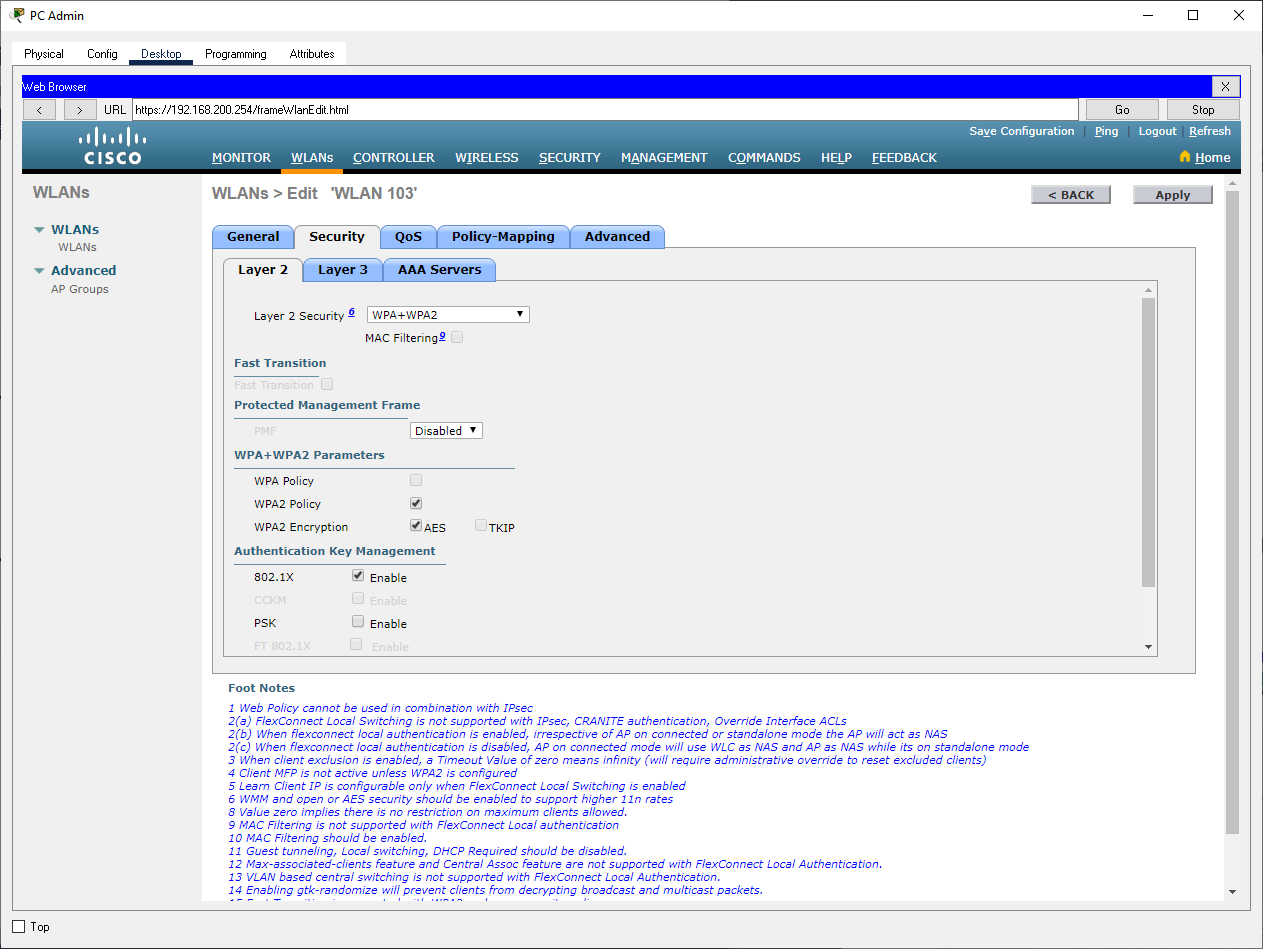


Hình 3.13 Tab WLANs trong WLC

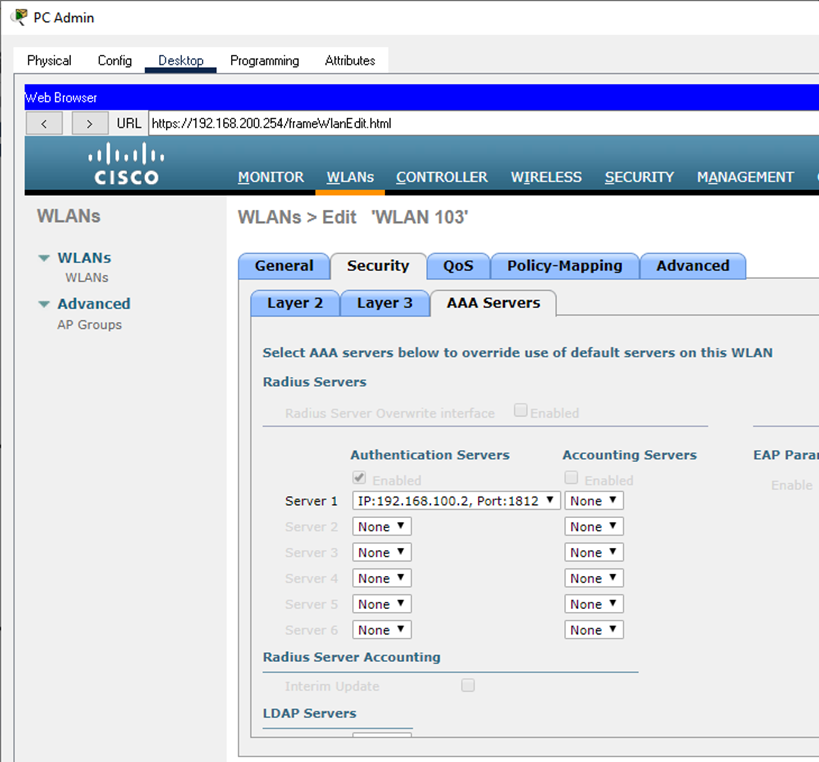
Cấu hình của WLAN 103 dùng máy chủ RADIUS dể xác thực



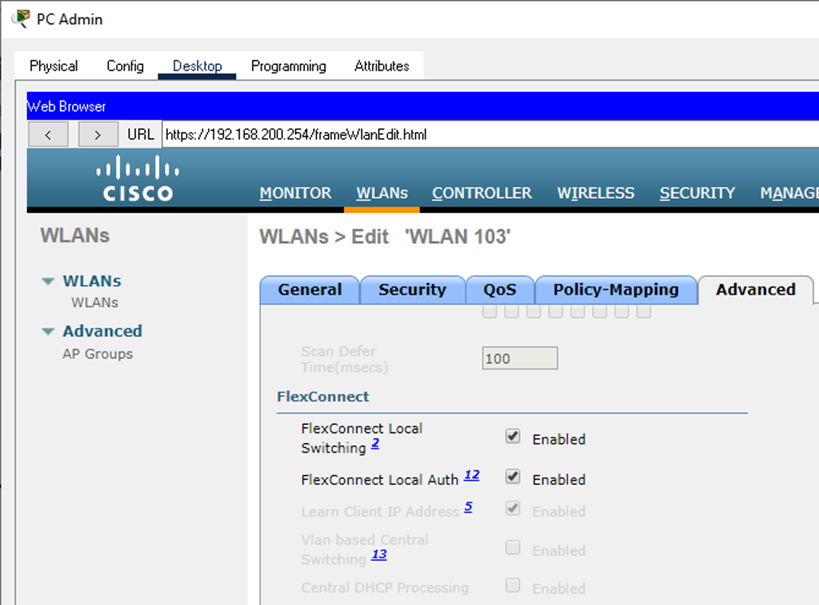
Hình 3.14 cấu hình WLAN 103 (1)



Hình 3.15 cấu hình WLAN 103 (2)

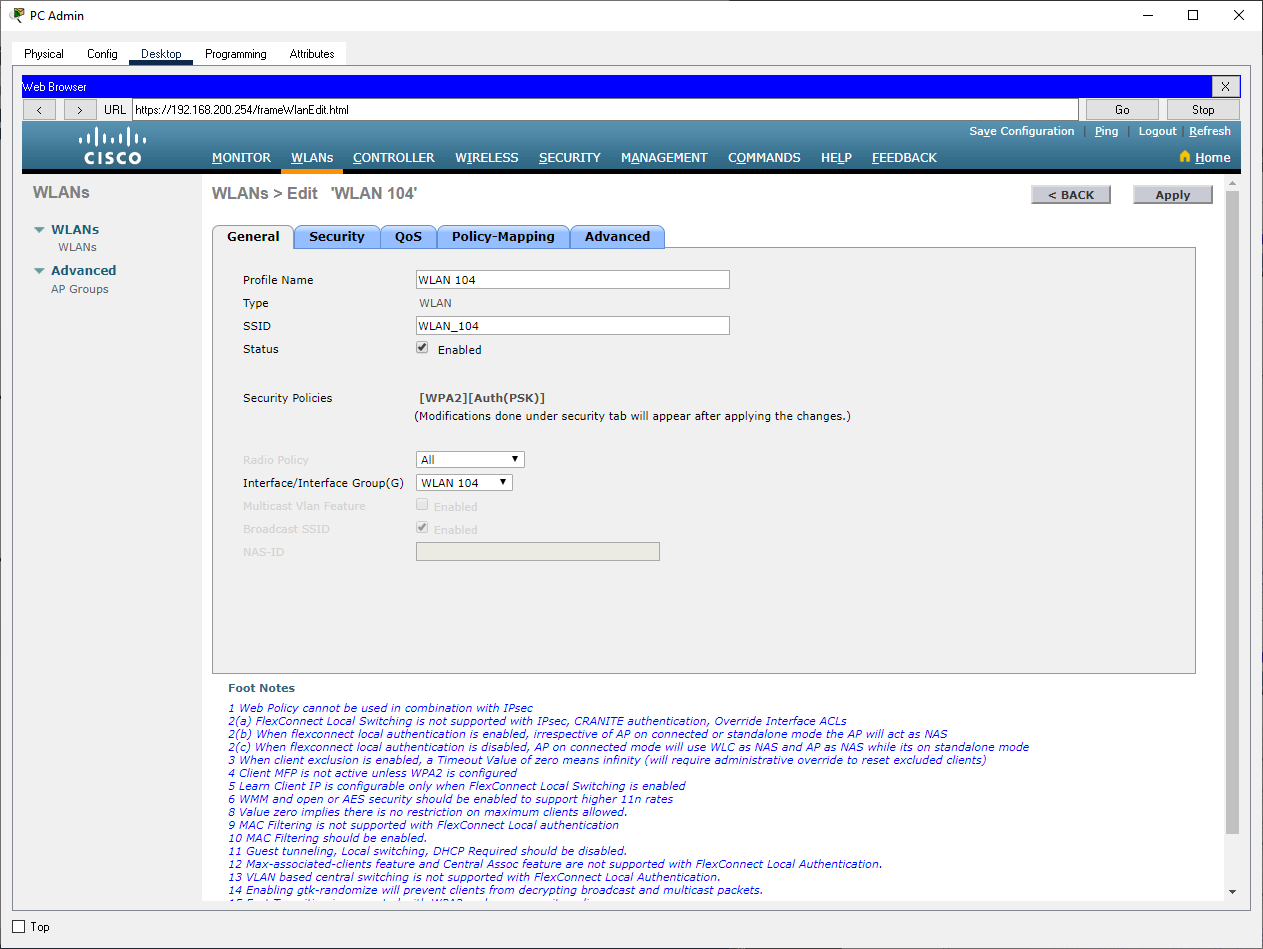


Hình 3.16 cấu hình WLAN 103 (3)

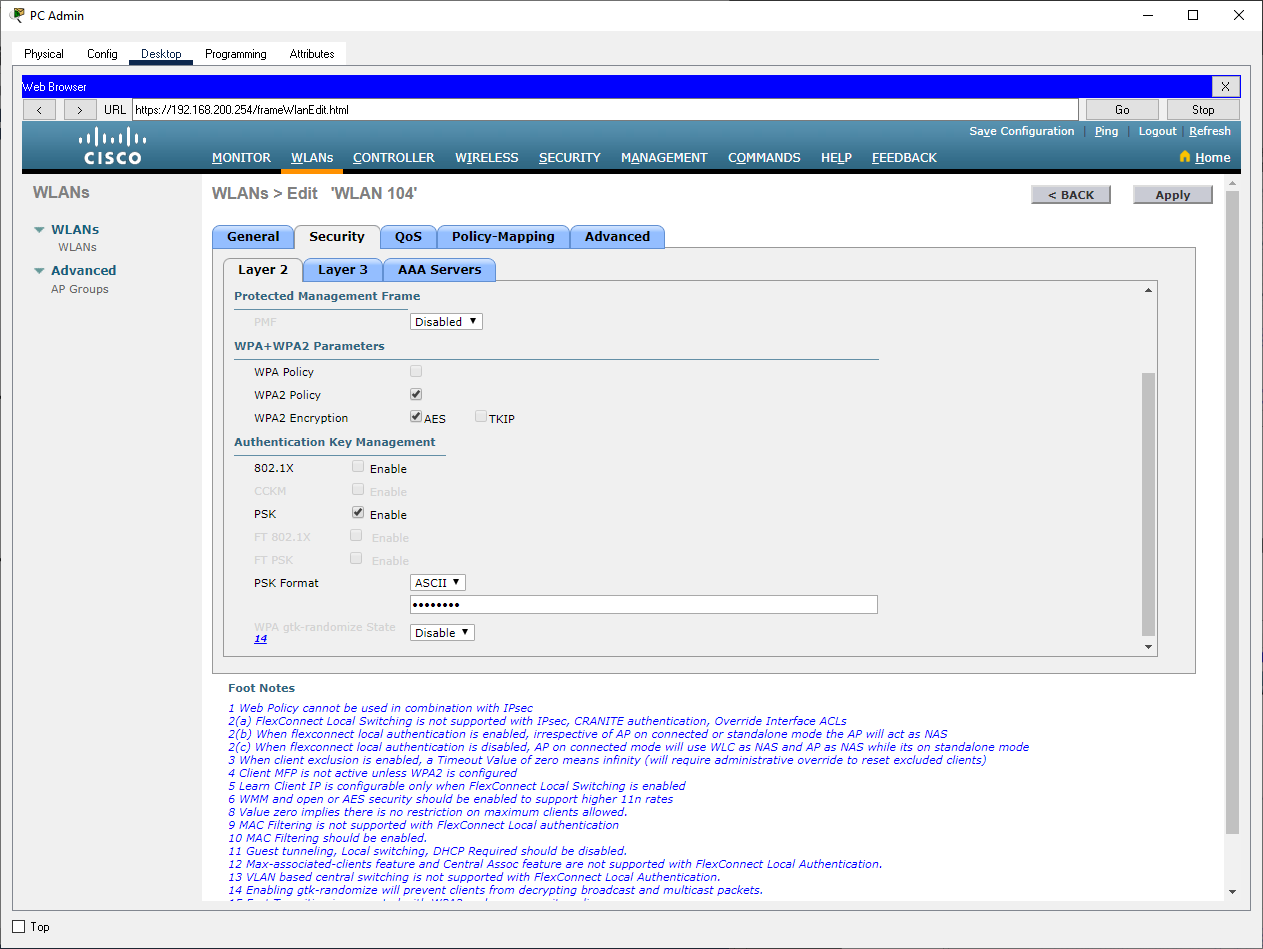


Hình 3.17 cấu hình WLAN 103 (4)

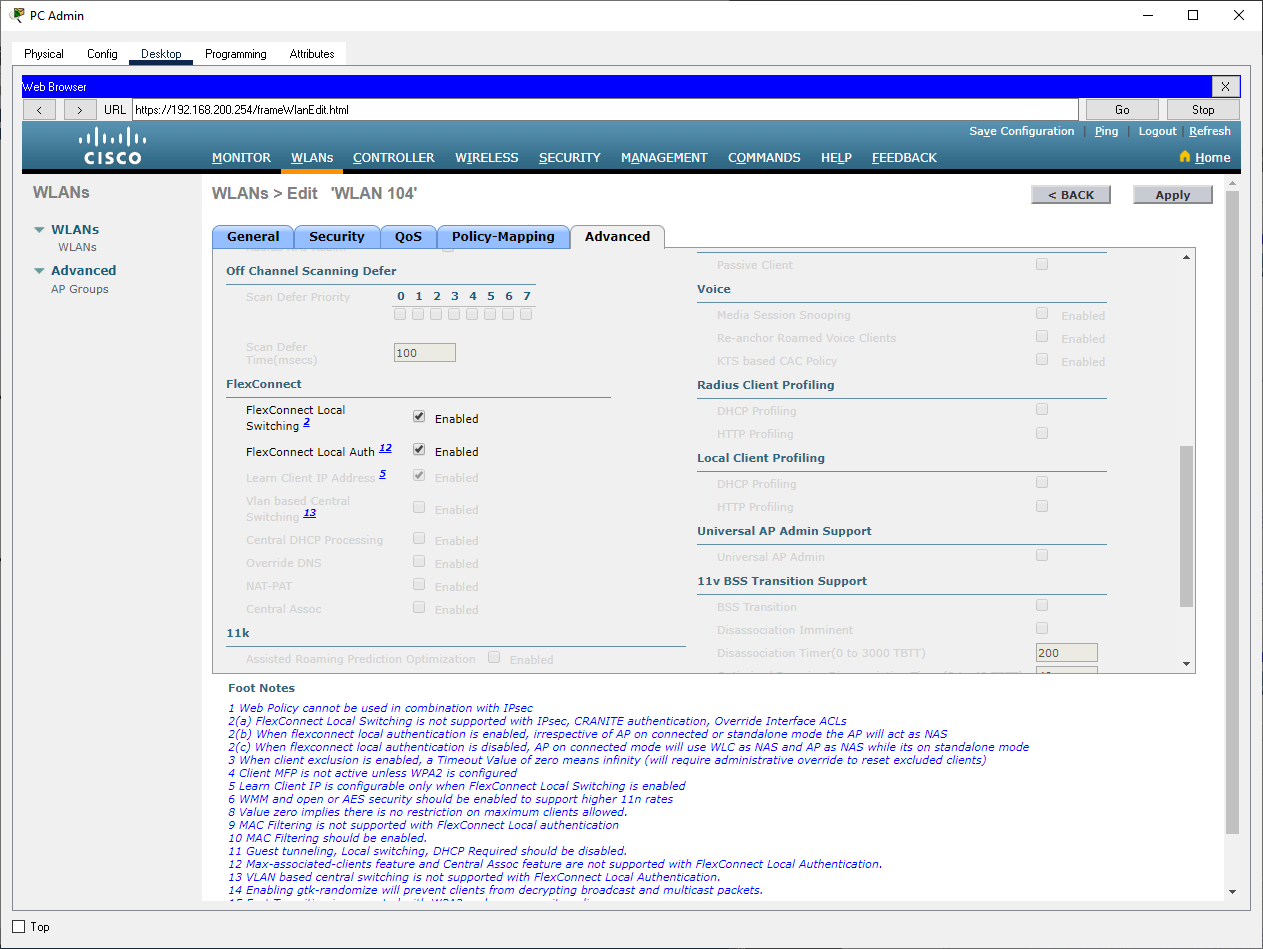
Cấu hình của WLAN 104 dùng Pre-Shared Key để xác thực người dùng



Hình 3.18 cấu hình WLAN 104 (1)

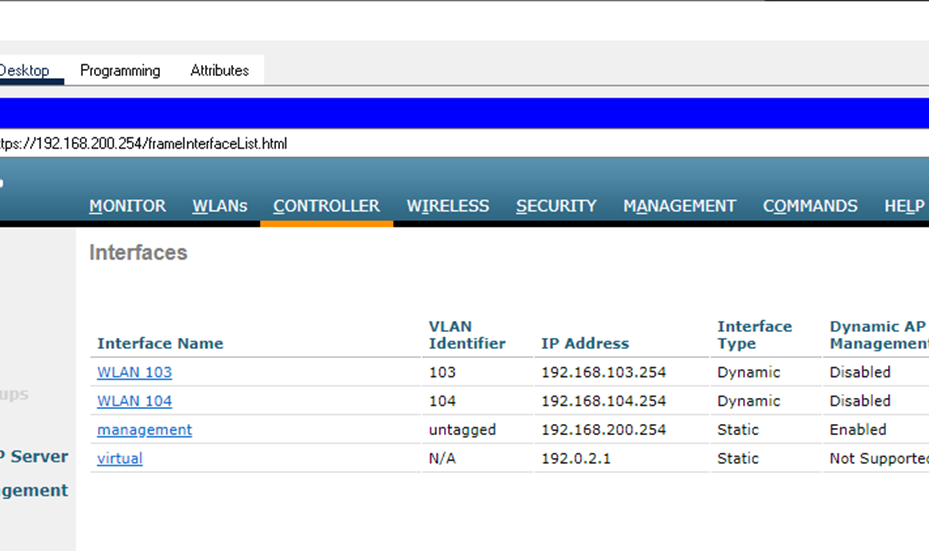


Hình 3.19 cấu hình WLAN 104 (2)



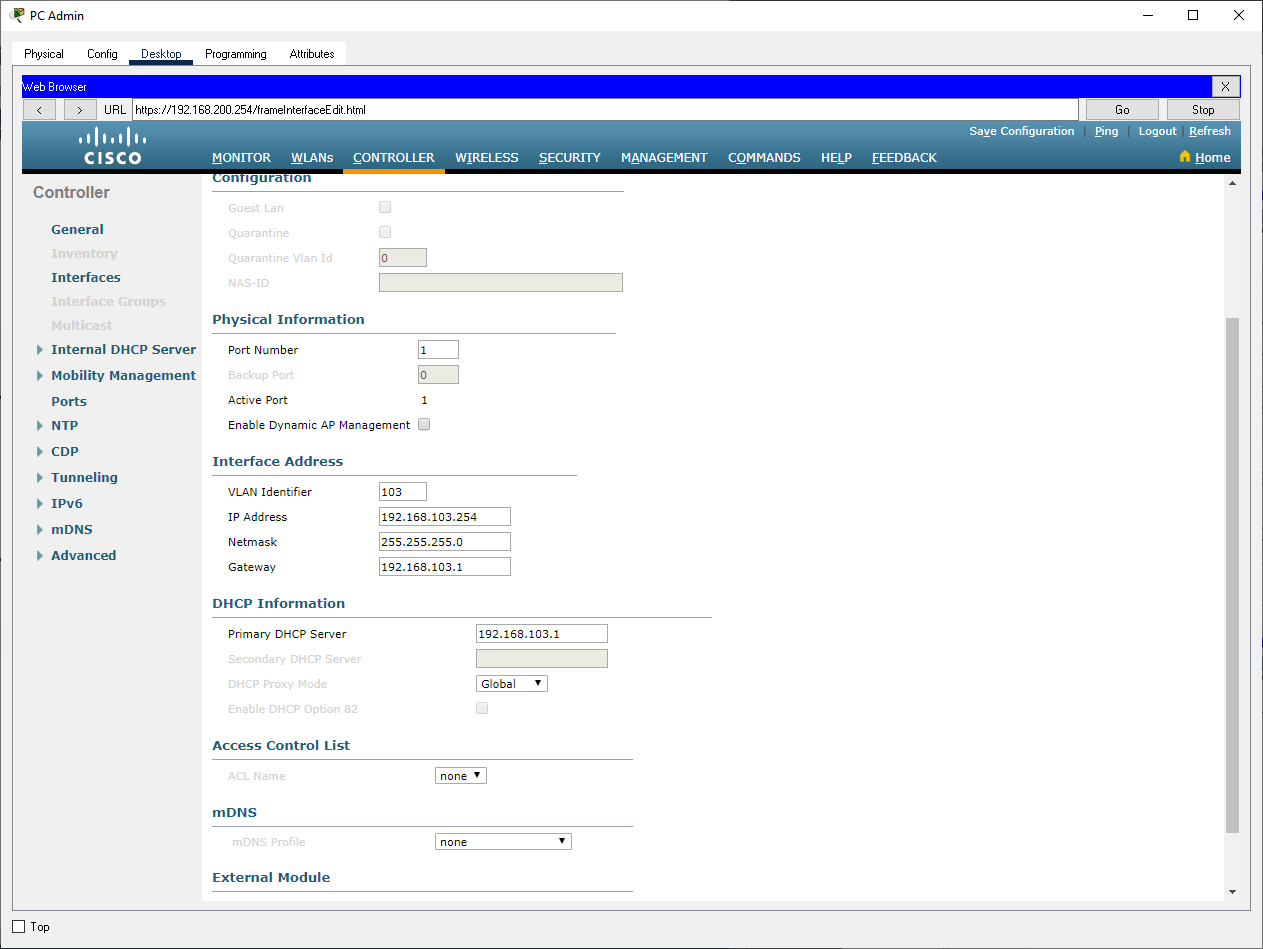
Hình 3.20 cấu hình WLAN 104 (3)

Trong tab CONTROLLER tạo hai Interface WLAN 103 và WLAN 104



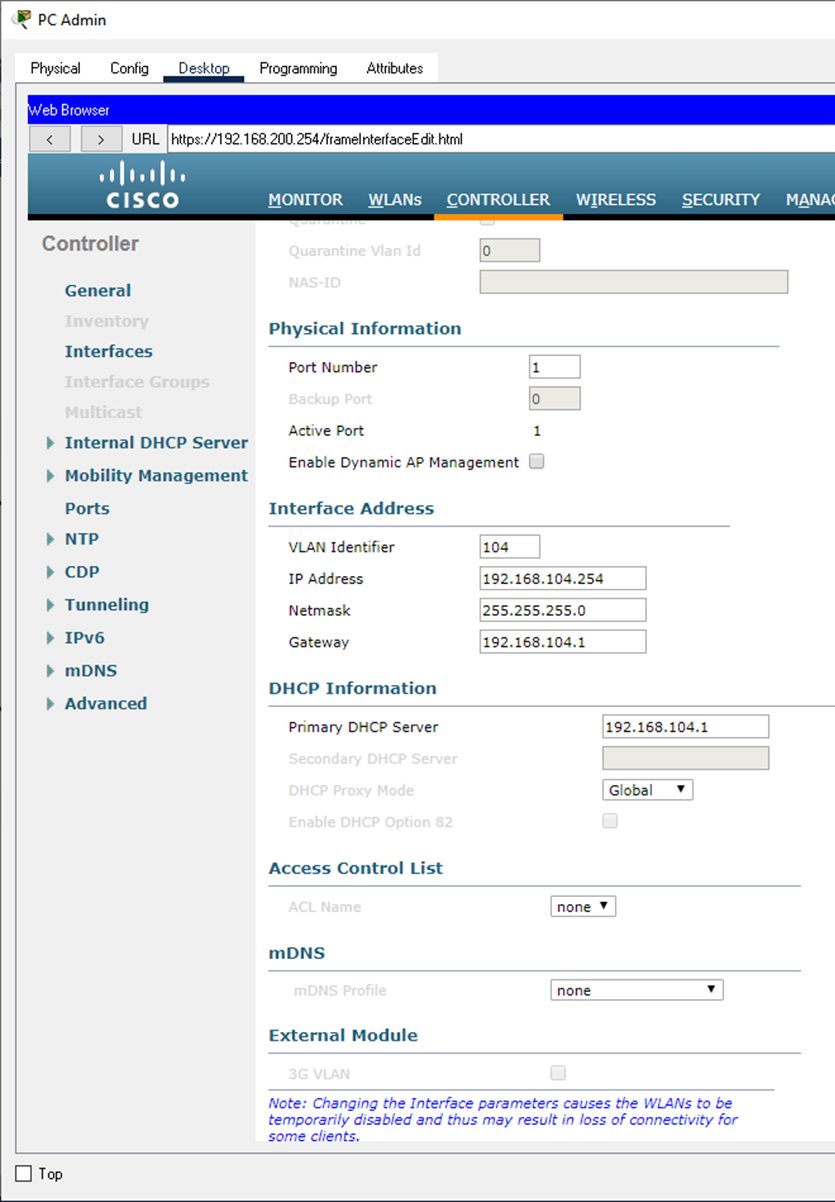
Hình 3.21 tab CONTROLLER

Cấu hình cho WLAN 103



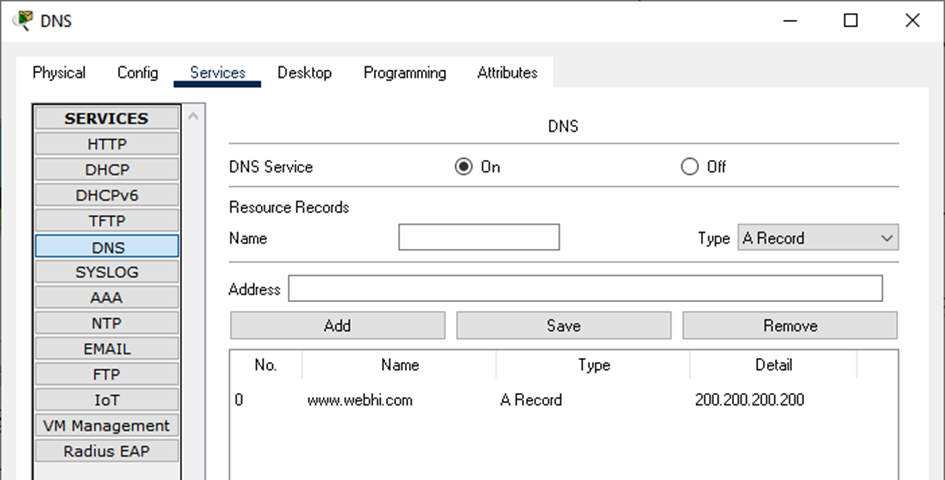
Hình 3.22 Cấu hình WLAN 103 trong tab CONTROLLER

Cấu hình cho WLAN 104



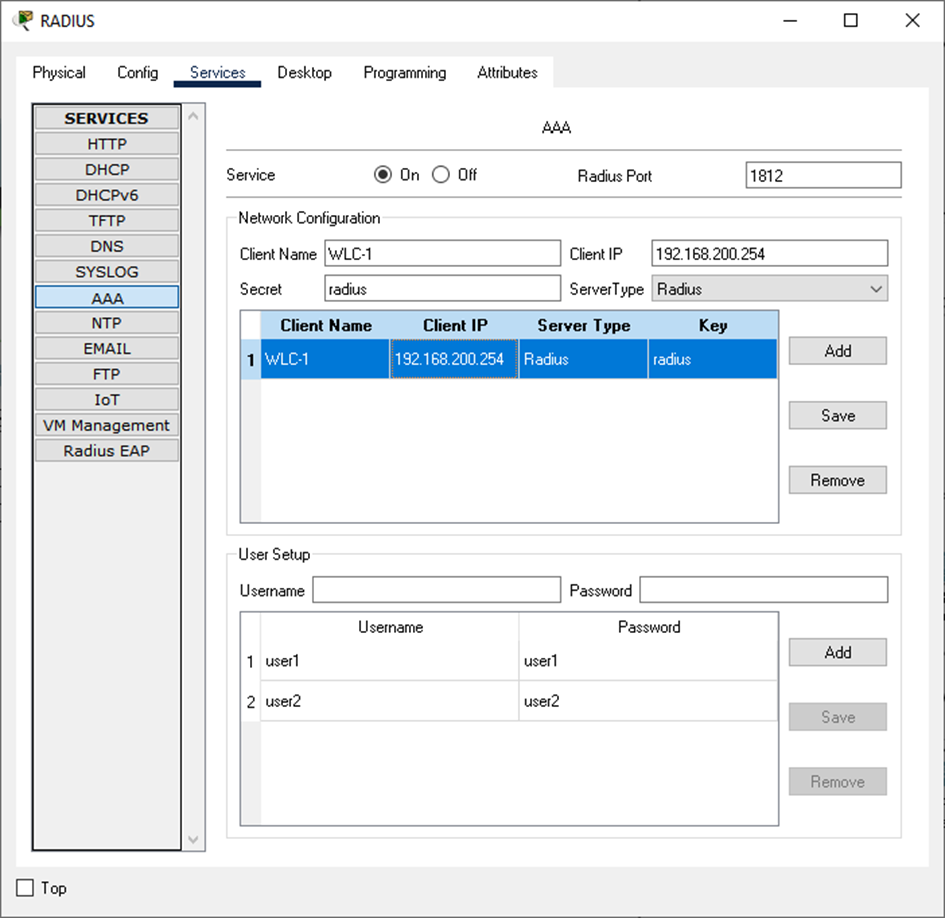
Hình 3.23 Cấu hình WLAN 104 trong tab CONTROLLER

Với DNS server, thêm Domain cho Web Server là “www.webhi.com”



Hình 3.24 cấu hình cho DNS server

Trong RADIUS Server ta cấu hình như sau:

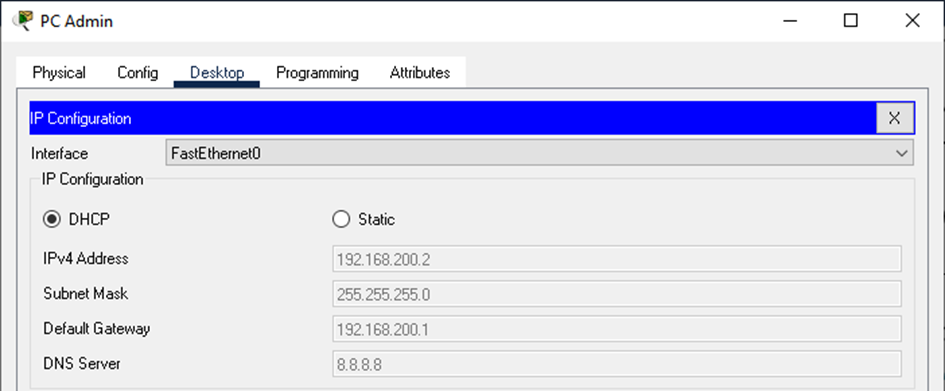


Hình 3.25 cấu hình cho RADIUS server

## Kiểm tra kết nối

Địa chỉ ip của các thiết bị nhận được khi chon DHCP

PC Admin:

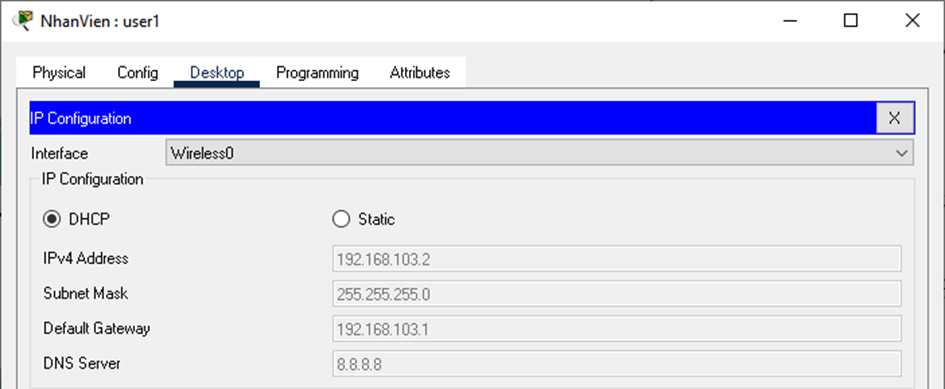


Hình 3.26 IP Configuration của PC Admin

NhanVien: user1

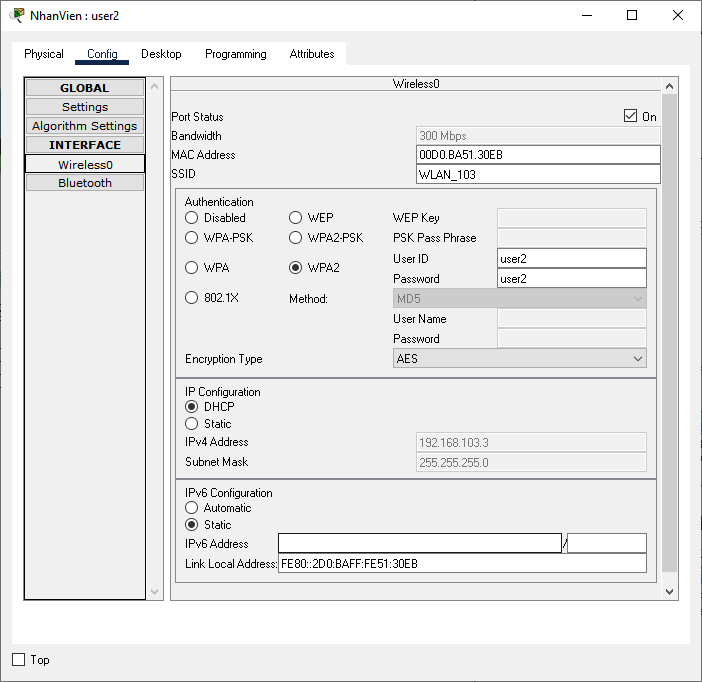


Hình 3.27 cấu hình nhận WLAN103 với user1

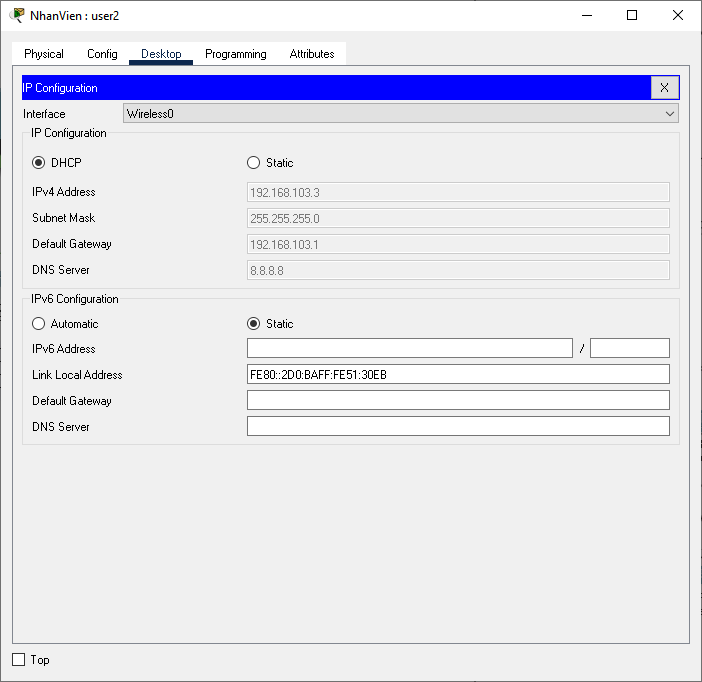


Hình 3.28 IP Configuration của NhanVien: user1

NhanVien: user2

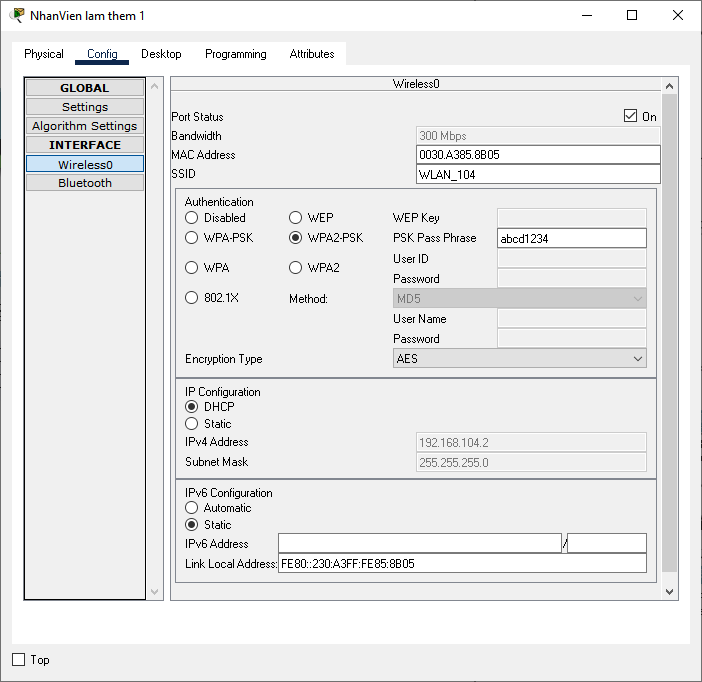


Hình 3.29 cấu hình nhận WLAN103 với user2

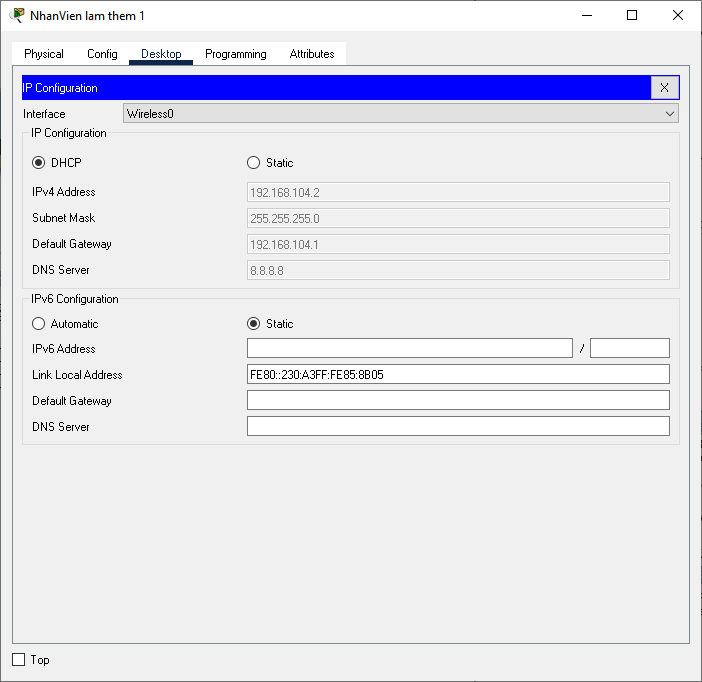


Hình 3.30 IP Configuration của NhanVien: user2

NhanVien lam them 1:

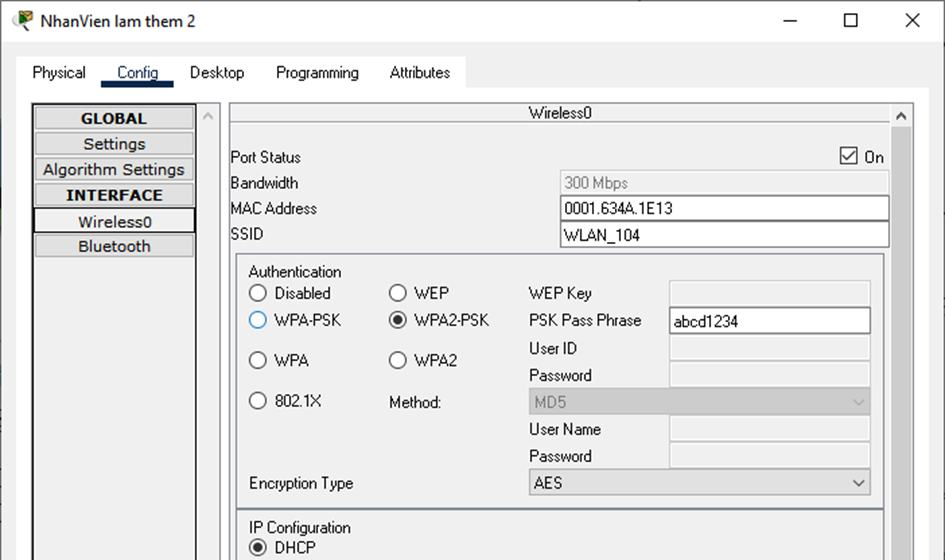


Hình 3.31 cấu hình nhận WLAN104 với NhanVien lam them 1

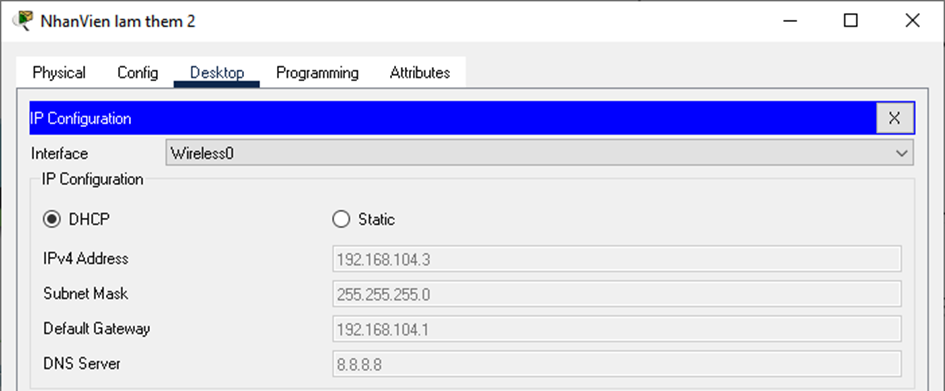


Hình 3.32 IP Configuration của NhanVien lam them 1

NhanVien lam them 2:

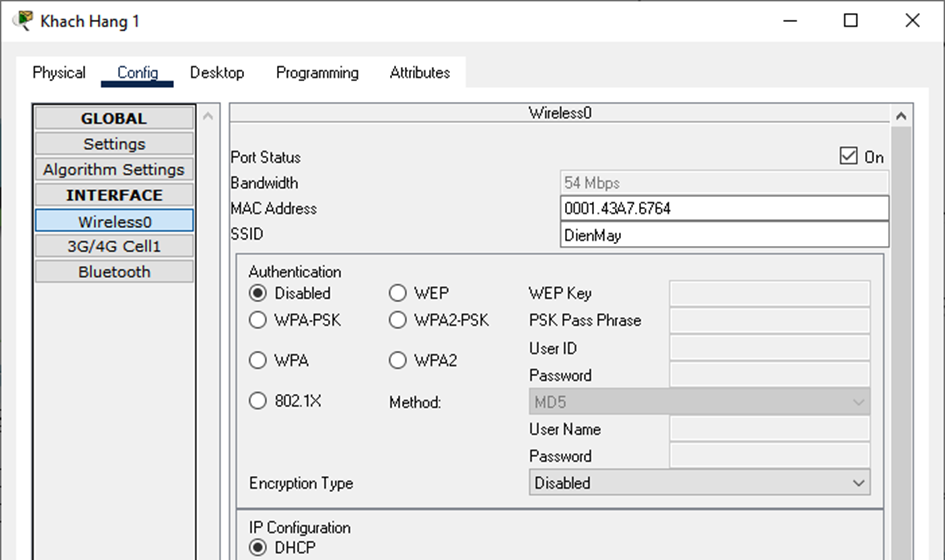


Hình 3.33 cấu hình nhận WLAN104 với NhanVien lam them 2

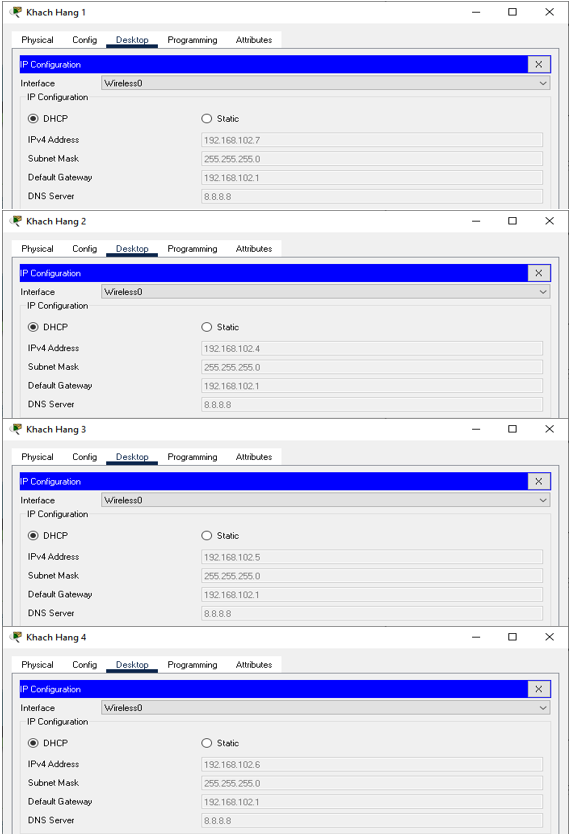


Hình 3.34 IP Configuration của NhanVien lam them 2

Các khách hàng truy cập vào mạng SSID: DienMay để truy cập mạng mà không cần mật khẩu

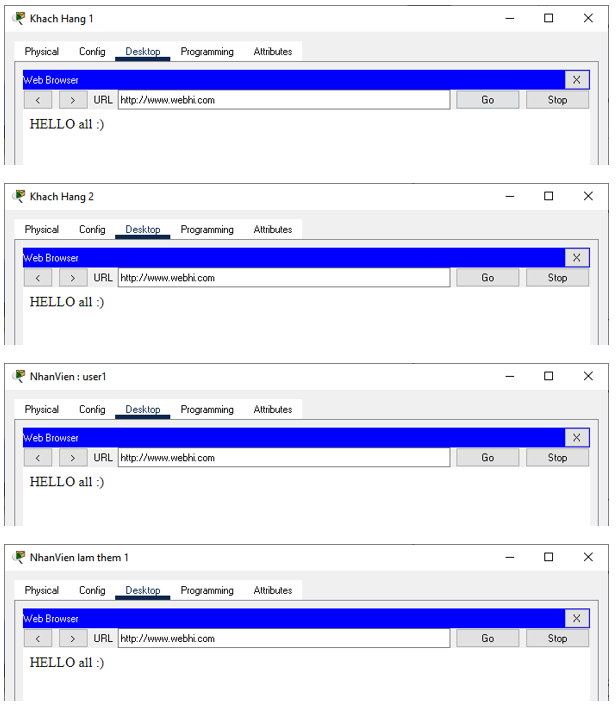


Hình 3.35 cấu hình chọn mạng SSID DienMay cho máy khách



Hình 3.36 IP Configuration của các khách hàng

Kiểm tra kết nối mạng của các thiết bị với mạng bên ngoài bằng cách truy cập vào trang web “http://www.webhi.com”



Hình 3.37 Truy cập đến WEB server từ domain được cấu hình ở DNS server

# KẾT LUẬN

Kết quả đạt được:

Xây dựng mạng cho siêu thị điện máy xanh căn bản đã hoàn thành được sơ bộ, đúng tiến trình, đáp ứng được các yêu cầu của khách hàng. Các thiết bị kết nối được với nhau, kết nối được với mạng WLAN. Dữ liệu được lưu trữ tập trung nên dễ bảo mật, backup, đồng bộ. Tài nguyên và dịch vụ được tập trung nên dễ quản lý và chia sẻ, phục vụ cho nhiều người dùng. Các hình thức tấn công cũng như các phương pháp bảo mật cơ bản được nêu rõ giúp khách hàng nắm bắt rõ hơn về mạng không dây để có thể giải quyết một số tình huống nhỏ khẩn cấp.

Hạn chế của chúng em là còn thiếu kiến thức nên chưa thể tìm hiểu hết và thật sự sâu của các mục trong chương 1 – Cơ sở lý thuyết. Tuy nhiên chúng em vẫn tự tin cung cấp đầy đủ những yêu cầu và truyền đạt những thông tin cần thiết cho người đọc có thể hiểu một cách dễ dàng nhất. Chúng em xin cam kết sau bài báo cáo này, chúng em sẽ tìm hiểu sâu hơn về mạng không dây, các phương thức bảo mật khi sử dụng web và hạn chế bị tấn công bởi các kỹ thuật tấn công. Từ những kiến thức của bài đồ án này, sẽ là những kiến thức quý báu và là nền tảng cho chúng em bước vào công việc sau này.

# TÀI LIỆU THAM KHẢO

1. <https://wiki.matbao.net/wlan-la-gi-nen-chon-giai-phap-bao-mat-nao-cho-wlan/>
2. <http://www.idz.vn/2016/04/cac-kieu-tan-cong-trong-mang-wlan.html>
3. <https://cvmtelecom.com/mang-khong-day-la-gi.html/>
4. https://vi.wikipedia.org/wiki/Mạng\_không\_dây
5. <https://www.daihockhonggiay.com/blogs/post/cong-nghe-mang-khong-day>
6. <https://vnpro.vn/thu-vien/so-luoc-ve-mang-khong-day-2270.html>
7. <https://vnpro.vn/thu-vien/mang-lan-ket-noi-voi-nhau-bang-nhung-thiet-bi-gi-2304.html>
8. <https://dichvudidong.vienthong.com.vn/tin-tuc/kien-thuc-co-ban-can-biet-ve-mang-di-dong.html>
9. <https://tamthanh.pro.vn/ho-tro/huong-dan/cac-chuan-mang-khong-day-1.html>
10. <https://thuthuat.taimienphi.vn/khai-niem-wifi-la-gi-cach-hoat-dong-ung-dung-wifi-trong-cuoc-song-22545n.aspx>
11. <https://www.dienmayxanh.com/kinh-nghiem-hay/wifi-la-gi-596329>
12. <http://luanvan.net.vn/luan-van/bao-cao-chuyen-de-mang-wpan-cac-chuan-ieee-802-15-va-cac-ung-dung-77558/>
13. <https://securitybox.vn/3126/top-6-hinh-thuc-tan-cong-mang-pho-bien-nhat/>
14. <https://congnghecit.com/de-tro-thanh-chuyen-gia-bao-mat-module15-tan-cong-tren-mang-khong-day.html>
15. <https://quantrimang.com/bao-mat-mang-khong-day-wifi-cho-doanh-nghiep-gia-dinh-179260>
16. <https://www.songhung.vn/tin-tuc/cach-bao-mat-mang-khong-day/>

# BẢNG PHÂN CHIA CÔNG VIỆC

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Đặng Thành Chí** | **Trần Vũ Luân** | **Trần Quốc Tâm** |
| Tìm tài liệu | Phần demo | Phần mô tả yêu cầu | Phần cơ sở lý thuyết |
| Thuyết trình | Phần demo | Phần mô tả yêu cầu | Phần cơ sở lý thuyết |
| Word Báo cáo | x |  | x |
| Slide thuyết trình |  | x | x |
| Mô hình demo | x | x |  |