TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM

**TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

**KHOA CÔNG NGHỆ THÔNG TIN**



**BÁO CÁO CUỐI KÌ MÔN**

**AN TOÀN MẠNG KHÔNG DÂY VÀ DI ĐỘNG**

**XÂY DỰNG HỆ THỐNG MẠNG KHÔNG DÂY CHO DOANH NGHIỆP EPIC BEAUTY SPA AND CLINIC VÀ CHO GIA ĐÌNH**

*Người hướng dẫn*: **TS. BÙI QUY ANH**

*Người thực hiện*: **NGUYỄN THỊ HỒNG HƯƠNG – 51800284**

Lớp **:** **18050402**

Khoá  **: 22**

**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**



**BÁO CÁO CUỐI KÌ MÔN**

**AN TOÀN MẠNG KHÔNG DÂY VÀ DI ĐỘNG**

**XÂY DỰNG HỆ THỐNG MẠNG KHÔNG DÂY CHO DOANH NGHIỆP EPIC BEAUTY SPA AND CLINIC VÀ CHO GIA ĐÌNH**

Người hướng dẫn: **TS. BÙI QUY ANH**

Người thực hiện: **NGUYỄN THỊ HỒNG HƯƠNG – 51800284**

Lớp **: 18050402**

Khoá  **: 22, 23**

**THÀNH PHỐ HỒ CHÍ MINH, NĂM 2021**

LỜI CẢM ƠN

Em xin chân thành cảm ơn TS Bùi Quy Anh đã cung cấp những kiến thức vô cùng quý báu về môn học. Trong suốt quá trình giảng dạy, thầy đã luôn tận tâm và nhiệt tình chỉ bảo, truyền đạt những thông tin bổ ích giúp em rất nhiều để có thể tiến hành thực hiện bài báo cáo này.

Sau khoảng thời gian học tập, với những kiến thức em đã tiếp thu được từ thầy song vẫn còn mặt hạn chế từ phía kiến thức cũng như kĩ năng thực hành của chính bản thân nên bài báo cáo này không thể tránh khỏi sai và thiếu sót.

Một lần nữa em xin cảm ơn thầy và mong nhận được những đóng góp quý giá từ thầy để bài báo cáo được chỉnh chu và hoàn thiện hơn nữa.

*TP. Hồ Chí Minh, ngày 13 tháng 08 năm 2021*

*Tác giả*

*(ký tên và ghi rõ họ tên)*

*Nguyễn Thị Hồng Hương*

**ĐỒ ÁN ĐƯỢC HOÀN THÀNH**

**TẠI TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

Tôi xin cam đoan đây là công trình nghiên cứu của riêng tôi và được sự hướng dẫn khoa học của TS Bùi Quy 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 báo cáo 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 báo cáo 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 13 tháng 08 năm 2021*

*Tác giả*

*(ký tên và ghi rõ họ tên)*

*Nguyễn Thị Hồng Hương*

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

Ngày nay, mạng không dây trở thành như cầu gần như tất yếu cho người dùng công nghệ nói chung. Đối với các công ty – doanh nghiệp, nhân viên ngoài việc sử dụng máy tính nội bộ nơi làm việc còn sử dụng các thiết bị không dây khác để phục vụ cho công việc như máy tính bảng, laptop, điện thoại thông minh, … Để đáp ứng cho nhu cầu cơ động, thuận tiện cho người dùng, tối đa hóa khả năng truy cập nội bộ và Internet cũng như năng suất làm việc, bài báo cáo này sẽ tiến hành xây dựng giải pháp mạng không dây phù hợp cho một doanh nghiệp với những tiêu chí an toàn cho người dùng. Tiến hành phân tích khảo sát từ những yêu cầu thực tế của khách hàng để đưa ra giải pháp hợp lý và sử dụng công nghệ Wireless LAN – công nghệ truyền thông không dây áp dụng cho mạng cục bộ tại doanh nghiệp, các thiết bị trong mạng WLAN sẽ giao tiếp qua Wi-Fi. Đưa ra những giới thiệu chung về mạng không dây với các chuẩn của WLAN IEEE 802.11, các mô hình mối đe dọa, các dịch vụ bảo mật trong hệ thống mạng không dây và dịch vụ bảo mật 802.1x. Ngoài ra, trong báo cáo còn nhắc đến kiến trúc Hot Spot dành riêng cho bảo mật Wi-Fi.

Bài báo cáo gồm có ba chương:

CHƯƠNG 1 – CƠ SỞ LÝ THUYẾT: Trình bày những cơ sở lý thuyết liên quan đến bảo mật trong hệ thống mạng không dây và di động.

CHƯƠNG 2 – THỰC HÀNH: Phân tích và đánh giá yêu cầu của khách hàng để tiến hành xây dựng hệ thống mạng không dây phù hợp.

CHƯƠNG 3 – DEMO: Xây dựng chương trình demo minh họa hệ thống mạng không dây trong doanh nghiệp và trong gia đình.

MỤC LỤC

[LỜI CẢM ƠN i](#_Toc79756827)

[PHẦN XÁC NHẬN VÀ ĐÁNH GIÁ CỦA GIẢNG VIÊN iii](#_Toc79756828)

[TÓM TẮT iv](#_Toc79756829)

[MỤC LỤC 1](#_Toc79756830)

[DANH MỤC CÁC BẢNG BIỂU, HÌNH VẼ, ĐỒ THỊ 4](#_Toc79756831)

[CHƯƠNG 1 – CƠ SỞ LÝ THUYẾT 5](#_Toc79756832)

[1.1 Các chuẩn WLAN IEEE 802.11 5](#_Toc79756833)

[1.1.1 Chuẩn 802.11a 5](#_Toc79756834)

[1.1.2 Chuẩn 802.11b 5](#_Toc79756835)

[1.1.3 Chuẩn 802.11g 6](#_Toc79756836)

[1.1.4 Chuẩn 802.11n 6](#_Toc79756837)

[1.1.5 So sánh các chuẩn WLAN IEEE 802.11 7](#_Toc79756838)

[1.2 Các mô hình de dọa trong hệ thống viễn thông 8](#_Toc79756839)

[1.2.1 Mô hình liên lạc tối thiểu 8](#_Toc79756840)

[1.2.2 Mô hình liên lạc với hệ thống viễn thông 9](#_Toc79756841)

[1.2.3 Mô hình đe dọa cho hệ thống viễn thông và các bên tham gia 9](#_Toc79756842)

[1.3 Các dịch vụ bảo mật 10](#_Toc79756843)

[1.4 Kiến trúc Hot Spot 11](#_Toc79756844)

[1.4.1 Tổng quan về kiến trúc Hot Spot 11](#_Toc79756845)

[1.4.2 Tổng quan về công nghệ Captive Portal 12](#_Toc79756846)

[1.4.2.1 Redirection 13](#_Toc79756847)

[1.4.2.2 Authorization 13](#_Toc79756848)

[1.4.2.3 Connection 13](#_Toc79756849)

[1.4.2.4 Disconnection 13](#_Toc79756850)

[1.5 Giao thức bảo mật 802.1x 14](#_Toc79756851)

[1.5.1 Kiến trúc 802.1x 14](#_Toc79756852)

[1.5.2 Thủ tục xác thực 15](#_Toc79756853)

[CHƯƠNG 2 – THỰC HÀNH 17](#_Toc79756854)

[2.1 Khảo sát doanh nghiệp 17](#_Toc79756855)

[2.2 Yêu cầu khách hàng 17](#_Toc79756856)

[2.3 Đề xuất hướng giải quyết 17](#_Toc79756857)

[2.4 Giá thành dự kiến cho hệ thống mạng 19](#_Toc79756858)

[CHƯƠNG 3 – DEMO 20](#_Toc79756859)

[3.1 Mô hình demo 20](#_Toc79756860)

[3.2 Bảng địa chỉ 20](#_Toc79756861)

[3.3 Cấu hình chương trình 22](#_Toc79756862)

[3.3.1 Cấu hình hạ tầng mạng 22](#_Toc79756863)

[3.3.2 Cấu hình định tuyến cho mạng doanh nghiệp 27](#_Toc79756864)

[3.3.3 Định cấu hình mạng wifi cho gia đình 41](#_Toc79756865)

[3.4 Chạy chương trình demo 45](#_Toc79756866)

[3.4.1 Mạng gia đình 45](#_Toc79756867)

[3.4.2 Mạng doanh nghiệp 46](#_Toc79756868)

[CHƯƠNG 4 – KẾT LUẬN 48](#_Toc79756869)

**DANH MỤC KÍ HIỆU VÀ CHỮ VIẾT TẮT**

**CÁC CHỮ VIẾT TẮT**

AP Access Point

CCK Complementary Code Keying

DHCP Dynamic Host Configuration Protocol

DSSS Direct Sequence Spread Spectrum

EAP Extensible Authentication Protocol

EAPOL Extensible Authentication Protocol over LAN

FHSS Frequency Hoping Spread Spectrum

GHz Gigahertz

HTTP Hypertext Transfer Protocol

HTTPS Hypertext Transfer Protocol Secure

IEEE Institute of Electrical and Electronic Engineers

IP Internet Protocol

LAN Local Area Network

m Meter

MAC Medium Access Control

Mbps Megabits per second

MHz Megahertz

MIMO Multiple Input Multiple Output

OFDM Orthogonal Frequency Division Multiplexing

SNMP Simple Network Management Protocol

SSID Server Set Identifier

TLS Transport Layer Security

RADIUS Remote Authentication Dial-In User Service

Wi-Fi Wireless Fidelity

WLAN Wireless Local Area Network

WLC Wireless LAN Controller

DANH MỤC CÁC BẢNG BIỂU, HÌNH VẼ, ĐỒ THỊ

**DANH MỤC HÌNH**

[Hình 1.1 Công nghệ MIMO với m kênh phát và n kênh thu 6](#_Toc79755995)

[Hình 1.2 Mô hình liên lạc tối thiểu 8](#_Toc79755996)

[Hình 1.3 Mô hình liên lạc với hệ thống viễn thông 9](#_Toc79755997)

[Hình 1.4 Mô hình đe dọa cho hệ thống viễn thông và các bên tham gia 10](#_Toc79755998)

[Hình 1.5 Captive Portal 12](#_Toc79755999)

[Hình 1.6 Mô hình kiến trúc 802.1x 14](#_Toc79756000)

[Hình 1.7 Thủ tục xác thực 802.1x 15](#_Toc79756001)

[Hình 3.1 Mô hình demo hệ thống mạng không dây cho gia đình và doanh nghiệp 20](#_Toc79756002)

**DANH MỤC BẢNG**

[Bảng 1.1 Bảng so sánh các chuẩn WLAN 802.11 8](#_Toc79755257)

[Bảng 2.1 Bảng giá thiết bị dự kiến cho hệ thống mạng doanh nghiệp 19](#_Toc79755258)

[Bảng 3.1 Bảng thông tin địa chỉ của hệ thống 21](#_Toc79755259)

[Bảng 3.2 Bảng thông tin WLAN 22](#_Toc79755260)

CHƯƠNG 1 – CƠ SỞ LÝ THUYẾT

1.1 Các chuẩn WLAN IEEE 802.11

Viện kỹ sư điện và điện tử IEEE đã đưa ra chuẩn mạng cục bộ không dây WLAN đầu tiên vào năm 1997 gọi là 802.11. Chuẩn này dùng công nghệ trải phổ trực tiếp DSSS (Direct Sequence Spread Spectrum), trải phổ nhảy tần FHSS (Frequency Hoping Spread Spectrum) và hồng ngoại (Infrared).

Đa số các hệ thống mạng WLAN sử dụng công nghệ trải phổ, một kỹ thuật tần số vô tuyến mà trước đây được phát triển bởi quân đội trong các hệ thống truyền thông tin cậy, an toàn, bảo mật và trọng yếu. Chuẩn 802.11 mô tả hệ thống trải phổ sử dụng tần số từ 2.4 GHz đến 2.485 GHz, tốc độ truyền dữ liệu tối đa là 2 Mbps.

1.1.1 Chuẩn 802.11a

Vào năm 1999, đặc điểm kỹ thuật cơ bản của 802.11 được cải tiến với phiên bản mới 802.11a. Sử dụng tần số 5 GHz với tốc độ truyền dữ liệu 54 Mbps. Chuẩn 802.11a sử dụng kỹ thuật trải phổ theo phương pháp đa phân chia tần số trực giao OFDM (Orthogonal Frequency Division Multiplexing), kỹ thuật này với tốc độ truyền dữ liệu nhanh hơn nhiều. Chuẩn 802.11a thường chỉ được sử dụng trong các mạng doanh nghiệp tuy nhiên với tần số cao, các tín hiệu 802.11a gặp nhiều khó khăn khi xuyên tường các vật cản khác.

1.1.2 Chuẩn 802.11b

Chuẩn 802.11b được xuất bản cùng năm với 802.11a, sử dụng kỹ thuật điều chế khoá mã bù CCK (Complementary Code Keying) và công nghệ trải phổ trực tiếp DSSS. Chuẩn này hỗ trợ băng thông lên đến 11 Mbps và hoạt động ở tần số 2.4 GHz. Các thiết bị 802.11b có thể bị xuyên nhiễu từ các thiết bị điện thoại không dây hoặc các thiết bị có cùng tần số là 2.4 GHz. Tuy nhiên, nếu được lắp đặt ở khoảng cách hợp lý thì sẽ dễ dàng tránh được nhiễu.

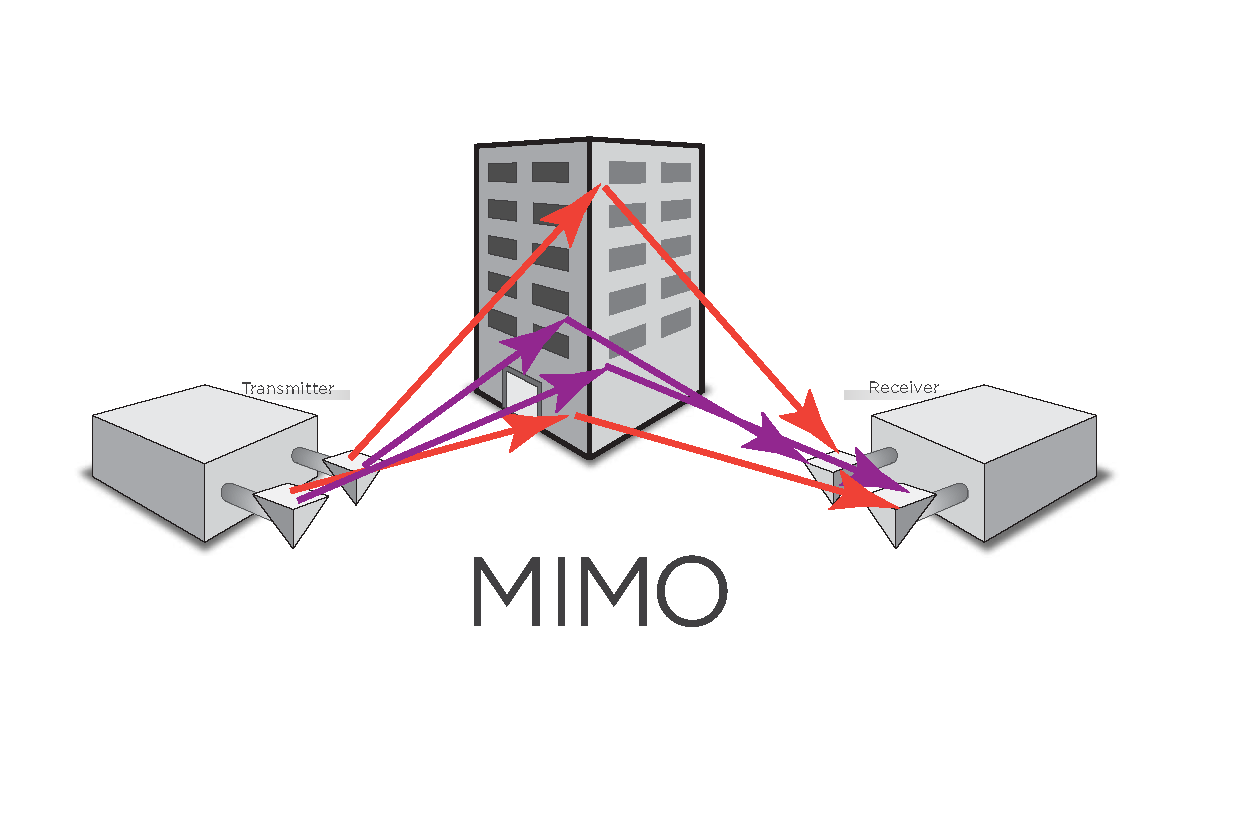
1.1.3 Chuẩn 802.11g

Vào tháng 6 năm 2003, IEEE đã phát hành một chuẩn mới có khả năng tương thích với chuẩn 802.11b. Chuẩn 802.11g sử dụng kỹ thuật OFDM và cho phép tốc độ truyền tương tự 802.11a với tối đa 54 Mbps nhưng lại dùng tần số 2.4 GHz giống với chuẩn 802.11b.

1.1.4 Chuẩn 802.11n

Chuẩn 802.11n hoạt động ở cả tần số 2.4 và 5 GHz với tốc độ truyền có thể lên đến 600 Mbps. Đây là chuẩn được thiết kế bằng cách tận dụng nhiều tín hiệu không dây và anten với việc sử dụng công nghệ MIMO (Multiple Input Multiple Output), công nghệ Channel Bonding, công nghệ Frame Aggregation. Theo đặc tả kỹ thuật được phê duyệt, MIMO là công nghệ bắt buộc phải có trong các sản phẩm 802.11n và thường được dùng chung với kỹ thuật OFDM.

MIMO sử dụng một số máy phát và một số máy thu cùng một lúc. Bằng cách ghép kênh trong không gian, các luồng dữ liệu được phân mảnh và truyền như các đơn vị riêng lẻ qua cùng một kênh. Từ các luồng này, người nhận sẽ hợp nhất thông điệp bằng cách sử dụng một thuật toán phức tạp.



Hình 1. Công nghệ MIMO với m kênh phát và n kênh thu

(Nguồn: [Internet](https://www.google.com.vn/search?tbm=isch&q=c%C3%B4ng%20ngh%E1%BB%87%20MIMO#imgrc=CknC9jD8ImPbIM))

Với công nghệ Channel Bonding sẽ kết hợp hai kênh 20 MHz thành một kênh 40 MHz duy nhất để tăng tốc độ truyền. Khối lượng truyền có thể được tăng lên bằng cách kết hợp các khung riêng lẻ thành các gói dữ liệu lớn hơn và giảm số lượng khung tổng thể và cả tổng chi phí của chúng.

1.1.5 So sánh các chuẩn WLAN IEEE 802.11

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Chuẩn IEEE** | **Năm phát hành** | **Tần số** | **Tốc độ truyền** | **Phạm vi trong nhà (m) ~** | **Phạm vi ngoài trời (m) ~** | **Kỹ thuật** | **Ưu điểm** | **Nhược điểm** |
| **802.11a** | 1999 | 5 GHz | 54 Mbps | 35m | 120m | OFDM | Tốc độ nhanh, với tần số tránh bị nhiễu bởi các thiết bị khác. | Phạm vi hẹp, không xuyên qua được vật cản. |
| **802.11b** | 1999 | 2.4 GHz | 11 Mbps | 38m | 140m | DSSS | Phạm vi phủ sóng tốt. | Tốc độ truyền thấp, dễ bị nhiễu bởi các thiết bị có cùng tần số. |
| **802.11g** | 2003 | 2.4 GHz | 54 Mbps | 38m | 140m | OFDM,  DSSS | Tốc độ nhanh, phạm vi phủ sóng tốt. | Dễ bị nhiễu bởi các thiết bị có cùng tần số. |
| **802.11n** | 2009 | 2.4/ 5 GHz | 600 Mbps | 70m | 250m | OFDM | Tốc độ nhanh nhất, vùng phủ sóng tốt nhất, khả năng chịu đựng tốt từ việc xuyên nhiễu. | Sử dụng nhiều tín hiệu có thể gây nhiễu với các mạng 802.11b/g ở gần. |

Bảng 1. Bảng so sánh các chuẩn WLAN 802.11

1.2 Các mô hình de dọa trong hệ thống viễn thông

1.2.1 Mô hình liên lạc tối thiểu

Mô hình mối đe dọa truyền thống với một kênh giao tiếp dựa trên mô hình liên lạc tối thiểu gồm có tối thiểu liên quan đến hai người tham gia là Bob và Alice và một kênh liên lạc.

A picture containing text, electronics, screenshot

Description automatically generated

Hình 1. Mô hình liên lạc tối thiểu

(Nguồn: Wireless and Mobile Network Security, p.56)

Mô hình này thường giả định mối quan hệ tin cậy ban đầu giữa Bob và Alice. Mô hình này thường được sử dụng trong mật mã học, vì nó hạn chế hiệu quả các cuộc tấn công chống lại kênh giao tiếp giữa Alice và Bob. Trong bối cảnh của các hệ thống viễn thông, mô hình này là không thấu đáo hết mọi khía cạnh vì các yếu tố và lỗ hỏng bảo mật khác hiện diện.

1.2.2 Mô hình liên lạc với hệ thống viễn thông

Mô hình liên lạc với hệ thống viễn thông được mô tả đầy đủ hơn, phân biệt giữa hai bên giao tiếp là Alice và Bob và ít nhất một cơ sở hạ tầng viễn thông và quyền hạn của nó được vượt quá kênh giao tiếp. Và thẩm quyền này là của một tác nhân thứ ba gọi là nhà cung cấp viễn thông.

Diagram

Description automatically generated

Hình 1. Mô hình liên lạc với hệ thống viễn thông

(Nguồn: Wireless and Mobile Network Security, p.57)

Sự xuất hiện của tác nhân thứ ba như vậy làm tăng độ phức tạp cho hệ thống, cho vào các giao diện và các lỗ hỏng mới và có thể yêu cầu một chuỗi tin cậy phức tạp hơn. Chính vì thế mà mở rộng phạm vi các mối đe dọa có thể xảy ra.

1.2.3 Mô hình đe dọa cho hệ thống viễn thông và các bên tham gia

Mô hình này sẽ xuất hiện một kẻ tân công gọi là Eve có thể tấn công một trong các bên giao tiếp bằng cách sử dụng các lỗ hỏng trong phần mềm và các biện pháp bảo mật mà bên giao tiếp bị Eve tấn công sử dụng. Nói một cách chính xác, mối đe dọa này không liên quan đến hệ thống viễn thông. Tuy nhiên thì thiết bị đầu cuối có giao diện kết nối với hệ thống viễn thông do đó dễ bị tấn công hơn.

Diagram

Description automatically generated

Hình 1. Mô hình đe dọa cho hệ thống viễn thông và các bên tham gia

(Nguồn: Wireless and Mobile Network Security, p.59)

Eve có thể tấn công kênh liên lạc liên kết Alice với hệ thống viễn thông. Eve có thể tấn công chống lại các kênh tồn tại trong hệ thống viễn thông. Để làm được điều này, Eve cố gắng giả dạng hợp pháp để thu hút Alice hoặc Bob sử dụng dịch vụ của mình để thu thập thông tin liên lạc giữa Bob và Alice và thao túng luồng dữ liệu của hai bên. Sự xâm nhập vào cơ sở hạ tầng cho phép thực hiện cuộc tấn công “man-in-the-middle”.

1.3 Các dịch vụ bảo mật

Theo chuẩn X.800, dịch vụ bảo mật là một dịch vụ được cung cấp bởi một lớp giao thức giao tiếp với các hệ thống mở đảm bảo sự bảo mật đầy đủ cho hệ thống hoặc cho việc truyền tải dữ liệu. Sau đây là các dịch vụ bảo mật:

* Tính sẵn sàng: Tài sản có thể truy cập và sử dụng được theo yêu cầu của tổ chức được ủy quyền.
* Kiểm soát truy cập: Ngăn chặn việc sử dụng trái phép tài nguyên, bao gồm cả ngăn chặn việc truy cập trái phép vào tài nguyên hệ thống. Việc sử dụng tài nguyên phải đảm bảo rằng ai có quyền được truy cập, truy cập dưới những điều kiện gì và họ được phép làm cái gì.
* Toàn vẹn dữ liệu: Dữ liệu không bị thay đổi và phá hủy một cách trái phép. Đảm bảo rằng dữ liệu nhận được chính xác là những gì đã gửi.
* Xác thực nguồn gốc dữ liệu: Đảm bảo nguồn dữ liệu nhận được là từ người gửi hợp lệ đã được xác nhận quyền sỡ hữu.
* Xác thực thực thể ngang hàng: chứng thực rằng một thực thể ngang hàng trong một liên kết là một thực thể đã được xác nhận, hợp lệ. Ví dụ như có hai người trao đổi thông tin với nhau thì hai người đó phải được xác nhận danh tính và có vai trò là ngang nhau.
* Tính bí mật: Đảm bảo tài sản, thông tin không được cung cấp và tiết lộ cho các cá nhân, thực thể hoặc các tiến trình bất hợp pháp.
* Phát hiện việc phát lại: bao gồm một thực thể để phát hiện rằng dữ liệu đã nhận được bị trùng lặp với lần trao đổi trước đó. Một số dữ liệu có thể đã được gửi một cách an toàn bởi một thực thể hợp pháp, nhưng chúng có thể bị sao chép và gửi lại vào cùng một chỗ nhận. Dữ liệu vẫn xác thực nhưng chúng đã được xử lý trước đó. Chính vì thế, cần phát hiện việc phát lại để tránh dữ liệu ấy được xử lý nhiều lần.
* Tính không thể chối cãi: đảm bảo rằng một bên giao dịch không thể phủ nhận việc họ đã giao dịch với các bên khác.

1.4 Kiến trúc Hot Spot

1.4.1 Tổng quan về kiến trúc Hot Spot

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 Intranet của họ nhờ vào kết nối không dây.

Kiến trúc Hot Spot dựa trên công nghệ “captive portal”. Công nghệ này được tạo ra nhờ vào việc triển khai các mạng không dây công cộng. Kiểm soát truy cập và xác thực được thực hiện nhờ vào captive portal.

Kiểm soát truy cập của Captive Portal dựa trên địa chỉ IP hoặc địa chỉ MAC. Kiến trúc Hot Spot dựa trên điểm truy cập Wi-Fi mở không có mã hóa hay tính toàn vẹn dữ liệu trên mạng không dây, dẫn đến việc dễ dàng nghe trộm thông tin liên lạc dữ liệu và có thể giả mạo địa chỉ IP/ MAC. Về cơ bản, cơ chế bảo vệ chính của Hot Spot là sử dụng tường lửa thực thi chính sách bảo mật giữa mạng không dây và Internet.

1.4.2 Tổng quan về công nghệ Captive Portal

Captive portal bao gồm:

* Tường lửa dựa trên các quy tắc động
* Một Web server
* Một khung xác thực và cơ sở dữ liệu
* Diagram

  Description automatically generatedMột khung thanh toán (tùy chọn)

Hình 1. Captive Portal

(Nguồn: Wireless and Mobile Network Security, p.132)

Quá trình hoạt động gồm có:

* Redirection
* Authorization
* Connection
* Disconnection

1.4.2.1 Redirection

Khi một máy tính liên kết tới điểm truy cập Wi-Fi mở, trước tiên nó sẽ thương lượng yêu cầu cấp phát địa chỉ DHCP. Máy khách không dây sẽ được chuyển đến máy chủ Web bất cứ lúc nào mà người dùng đó yêu cầu truy cập Internet. Việc chuyển hướng này được thực hiện nhờ vào mã trạng thái HTTP 302 (chuyển hướng tạm thời) – mã mà được hiểu một cách chính xác bởi trình duyệt Web phổ biến. Captive Portal sẽ chuyển hướng kết nối tới máy chủ Web HTTPS để xác thực máy chủ Web bằng cách sử dụng mật mã công khai và sử dụng giao thức TLS (Transport Layer Security). Trang Web được đưa ra là trang thông tin của nhà cung cấp dịch vụ mà người dùng sẽ luôn được chuyển hướng cho đến khi người dùng đó xác thực thành công đến Hot Spot.

1.4.2.2 Authorization

Khi người tự xác thực với Captive Portal bằng cách cung cấp username/ password hợp lệ hoặc là mã thông báo hợp lệ), khung xác thực sau đó sẽ cho phép người dùng giao tiếp với Internet bằng cách định cấu hình động bộ quy tắc được áp dụng trên tường lửa. Hầu hết các Captive Portal chỉ dựa vào địa chỉ IP để cấp quyền cho người dùng trên tường lửa, trong khi một số cổng khác cũng có thể sử dụng địa chỉ MAC để ngăn chặn các cuộc tấn công giả mạo vào địa chỉ MAC.

1.4.2.3 Connection

Khi tường lửa đã cấu hình các quy tắc mới đặt ra cho người dùng xác thực, các chính sách bảo mật mẫu (áp dụng bởi nhà cung cấp) được thực thi và về cơ bản người dùng bây giờ có thể truy cập Internet.

1.4.2.4 Disconnection

Người dùng có thể kết thúc phiên truy cập với Captive Portal bằng cách gửi đăng xuất qua một trang Web cụ thể trên Captive Portal. Ngoài ra, hầu hết các kiến trúc Hot Spot sử dụng các kỹ thuật khác để phát hiện xem người dùng có rời khỏi hay không.

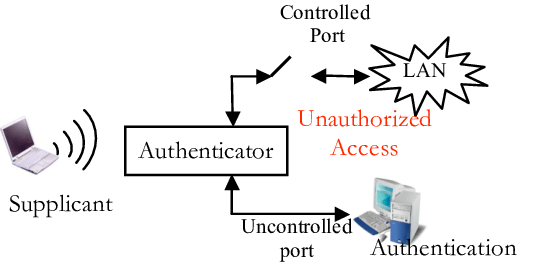
1.5 Giao thức bảo mật 802.1x

802.1x là chuẩn được chỉ định xác thực người dùng và quản lý khóa mật mã cho mạng nội bộ nói chung. Một máy chủ xác thực là cần thiết để đảm nhận quyền kiểm soát truy cập tổng thể của toàn bộ mạng. Một máy khách không được xác thực thành công sẽ bị từ chối bởi điểm truy cập AP của mạng không dây.

1.5.1 Kiến trúc 802.1x

Có 3 thành phần chính cho 802.1x:

* Bộ hỗ trợ hoặc là máy khách 802.1x: đây là thiết bị đầu cuối muốn sử dụng các tài nguyên được cung cấp bởi một mạng truyền thông.
* Bộ xác thực hoặc bộ điều khiển: hệ thống này kiểm soát một cổng để truy cập mạng. Nó có thể là bộ chuyển mạch của mạng có dây hoặc là điểm truy cập AP trong mạng không dây.
* Máy chủ xác thực, thường là RADIUS Server: chịu tránh nhiệm thực hiện quá trình xác thực máy khách 802.1x. Trong giai đoạn này, bộ xác thực không thúc đẩy cuộc đàm thoại giữa hai thực thể mà hoạt động như một cuộc chuyển tiếp thụ động đơn giản.



Hình 1. Mô hình kiến trúc 802.1x

([Nguồn: 802.1x architecture, ResearchGate](https://www.researchgate.net/figure/IEEE-8021x-architecture_fig3_236867998))

1.5.2 Thủ tục xác thực

Trong mạng không dây, giao thức EAP được sử dụng giữa trạm và máy chủ xác thực thông qua một AP. Đầu tiên nó được đóng gói trong các khung EAPOL, sau đó là định tuyến trong giao thức RADIUS vì nó được truyền qua IP.

Diagram

Description automatically generated

Hình 1. Thủ tục xác thực 802.1x

(Nguồn: Wireless and Mobile Network Security, p.249)

Việc đưa một thiết bị đầu cuối không dây trong môi trường 802.1x xảy ra cơ bản như sau:

* Xác thực trạm trước, sau đó kết nối với một điểm truy cập AP được xác định bằng SSID.
* Để bắt đầu xác thực, trạm phát sóng một khung EAPOL-START 30 giây một lần.
* AP gửi một thông điệp REQUEST.IDENTITY-EAP tới máy khách 802.1x, từ đó tạo ra phản hồi EAP-RESPONSE.IDENTITY có chứa danh tính (EAP-ID) của thiết bị đầu cuối không dây.
* Từ tham số này, AP sẽ suy ra địa chỉ IP của máy chủ xác thực và gửi đến máy chủ này thông báo EAP-RESPONSE.IDENTITY được gói gọn trong một yêu cầu RADIUS.
* Các yêu cầu và phản hồi của thông điệp EAP được trao đổi giữa máy chủ RADIUS và máy khách 802.1x. AP chỉ đóng vai trò chuyển tiếp thụ động.
* Máy chủ RADIUS cho biết quy trình này thành công hay thất bại thông qua một thông báo EAP-SUCCESS hoặc EAP-FAILURE.
* Cuối quá trình xác thực, thông báo RADIUS ACCESS-ACCEPT gây ra sự chuyển đổi trạng thái của cổng để được ủy quyền. Thông báo RADIUS ACCESS-REJECT buộc các cổng có liên quan đến trạng thái trái phép. Một cổng giữ nguyên trạng thái hiện tại của nó trong phiên xác thực.
* Trong trường hợp xác thực thành công, máy khách và máy chủ xác thực 802.1x sẽ tính toán một khóa phiên gọi là Unicast Key.
* AP sẽ chọn một khóa mã hóa gọi là Global Key cho liên kết bảo mật với máy khách 802.1x. Sau đó được mã hóa và được ký bằng khóa phiên nhận từ máy chủ RADIUS và gửi đến máy khách 802.1x trong khung EAPOL-KEY.

CHƯƠNG 2 – THỰC HÀNH

2.1 Khảo sát doanh nghiệp

Công ty cổ phần EPIC BEAUTY SPA AND CLINIC có trụ sở chính tại 556, đường 3 Tháng 2, Phường 8, Quận 10. Đây là công ty spa với các dịch vụ chăm sóc sức khỏe và kinh doanh những mỹ phẩm làm đẹp. Tòa nhà gồm có:

* Tầng hầm: nơi gửi xe.
* Tầng 1: nơi trưng bày các mỹ phẩm, hàng hóa chăm sóc làm đẹp như sữa rửa mặt, kem chống nắng, tinh chất serum, … với một quầy giao dịch với khách hàng để thanh toán.
* Tầng 2: nơi làm việc vận hành công ty gồm có phòng giám đốc, phòng nhân viên hội đồng, phòng kinh doanh, phòng dịch vụ chăm sóc khách hàng.
* Tầng 3,4: là spa chăm sóc các dịch vụ sức khỏe làm đẹp gồm có phòng chờ cho các khách hàng và có một quầy tư vấn khách hàng.

2.2 Yêu cầu khách hàng

Triển khai một hệ thống mạng không dây kết nối các máy tính làm việc chia sẻ dữ liệu đảm bảo an toàn bảo mật trong hệ thống mạng. Lắp đặt mạng không dây sao cho khách hàng có thể truy cập internet trong lúc chờ đợi dịch vụ chăm sóc. Đảm bảo các phòng ban cũng truy cập được internet với tốc độ cao. Thiết kế đảm bảo tính thẩm mỹ, dễ lắp đặt và bảo trì. Lắp đặt mạng Wifi cho gia đình có thể truy cập Internet.

2.3 Đề xuất hướng giải quyết

Về mạng doanh nghiệp, xây dựng hệ thống mạng WLAN cho công ty sử dụng một switch tổng kết nối tới các bị có dây vào và dùng Host PC Admin để vận hành. Sử dụng thiết bị quản lý mạng không dây tập trung (Wireless LAN Controller) và các thiết bị phát sóng mạng Wi-Fi với các điểm truy cập AP – Access Point kết nối tập trung về thiết bị Wireless Controller để giám sát và quản lý. Giúp cho người dùng không cần phải cấu hình trên từng thiết bị AP khi có bất kỳ thay đổi.

Người quản trị truy cập vào thiết bị WLC tiến hành cài đặt hoặc thay đổi cho hệ thống và WLC sẽ tự động thực hiện chính xác những cài đặt hay thay đổi từ người dùng tới các thiết bị AP trong cùng hệ thống. Xây dựng hệ thống mạng phân chia quyền truy cập kết nối dành riêng cho khách hàng đến làm dịch vụ. Tách biệt với lớp mạng dành cho nhân viên cũng như ngăn chặn kết nối vào hệ thống nội bộ riêng tư của doanh nghiệp. Phân chia mỗi AP là một phòng ban riêng, tách biệt nhau gồm có 3 AP tương ứng với 3 phòng ban là Sale, phòng Spa và phòng hội đồng Council với một AP dành riêng cho khách hàng đến EPIC.

Đảm bảo các thiết bị hỗ trợ các chuẩn bảo mật không dây thế hệ mới nhất, cung cấp khả năng kết nối vào mạng với độ ổn định cao nhất. Quản lý và giám sát được hành vi người dùng, thiết lập quyền truy cập tài nguyên mạng theo từng quyền tương ứng.

Các thiết bị dự kiến sử dụng gồm có:

* Wireless LAN Controller: WLC là bộ điều khiển mạng LAN không dây quản lý và thống nhất các điểm truy cập mạng AP lại với nhau. Thiết bị WLC có cấu hình là giao diện web-browser, đơn giản hóa việc truy cập và theo dõi các tham số về địa IP, địa chỉ MAC của tất cả các AP trong hệ thống, liệt kê các thiết bị mạng đang online/ offline của người quản trị trên một giao diện. Người dùng muốn truy cập vào mạng không dây sẽ được xác thực qua chuỗi username và password.
* Access Point: Mỗi một AP sẽ tương ứng với một phòng ban, tức là chỉ dành riêng cho một vùng mạng nội bộ ứng với từng phòng.
* RADIUS Server: Sử dụng RADIUS Server quản lý các username và password để có toàn quyền kiểm soát ai có thể kết nối và ai không được phép truy cập vào mạng của mình. Cho phép duy trì profile người dùng trong cơ sở dữ liệu trung tâm. Việc này giúp quản lý bảo mật tốt hơn.
* Switch: Dùng để kết nối các thiết bị có dây lại với nhau.
* Router: Cung cấp các cổng mặc định vào các mạng khác và Internet.

Về mạng gia đình, dùng thiết bị Cable Modem để kết nối giao tiếp với mạng lưới của nhà cung cấp dịch vụ Internet thông qua hệ thống cáp nối đồng trục, giúp kết nối Internet cho Router Wifi.

2.4 Giá thành dự kiến cho hệ thống mạng

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Thiết bị** | **Mô tả** | **Số lượng** | **Đơn giá** | **Thành tiền** |
| Switch S1 | Switch CISCO Catalyst 3560 24PS-S | 1 | 36.800.000 | 36.800.000 |
| Router EPIC | Router CISCO ISR4331/K9 | 1 | 32.000.000 | 32.000.000 |
| WLC | CISCO 3504 Wireless Controller AIR CT3504-K9 | 1 | 58.750.000 | 58.750.000 |
| Access Point | CISCO 3702I-C-K9 | 4 | 12.700.000 | 279.400.000 |
| Router Wifi | CISCO CVR100W | 1 | 1.490.000 | 1.490.000 |
| Tổng dự kiến: | | | | 408.440.000 |

Bảng 2. Bảng giá thiết bị dự kiến cho hệ thống mạng doanh nghiệp

CHƯƠNG 3 – DEMO

Diagram

Description automatically generated3.1 Mô hình demo

Hình 3. Mô hình demo hệ thống mạng không dây cho gia đình và doanh nghiệp

3.2 Bảng địa chỉ

|  |  |  |
| --- | --- | --- |
| **Thiết bị** | **Interface** | **Địa chỉ IP** |
| **Home Router** | Internet | DHCP |
| LAN | 192.168.50.1/24 |
| **EPIC** | G0/0/1 | 10.6.0.1/24 |
| G0/0/0.10 | 192.168.10.1/24 |
| G0/0/0.20 | 192.168.20.1/24 |
| G0/0/0.30 | 192.168.30.1/24 |
| G0/0/0.40 | 192.168.40.1/24 |
| G0/0/0.99 | 192.168.99.1/24 |
| **SALE** | G0 | DHCP |
| **SPA** | G0 | DHCP |
| **COUNCIL** | G0 | DHCP |
| **GUEST** | G0 | DHCP |
| **WLC** | Management | 192.168.99.254/24 |
| **RADIUS Server** | NIC | 10.6.0.254/24 |
| **Tablet NV1** | Wireless0 | DHCP |
| **NV1** | Wireless0 | DHCP |
| **NV2** | Wireless0 | DHCP |
| **NV3** | Wireless0 | DHCP |
| **NV4** | Wireless0 | DHCP |
| **NV5** | Wireless0 | DHCP |
| **NV6** | Wireless0 | DHCP |
| **NV7** | Wireless0 | DHCP |
| **NV8** | Wireless0 | DHCP |
| **NV9** | Wireless0 | DHCP |
| **KH1** | Wireless0 | DHCP |
| **KH2** | Wireless0 | DHCP |
| **KH3** | Wireless0 | DHCP |
| **WEB Server** | NIC | 209.165.201.2/24 |
| **Enterprise Admin** | NIC | 192.168.99.253/24 |
| **Me1** | Wireless0 | DHCP |
| **Me2** | Wireless0 | DHCP |
| **Me3** | Wireless0 | DHCP |
| **SamSung** | Wireless0 | DHCP |

Bảng 3. Bảng thông tin địa chỉ của hệ thống

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **WLAN** | **SSID** | **Authentication** | **Username** | **Password** |
| Home Network | HomeEpic | WPA2-Personal | N/A | EpicHome123 |
| Wireless VLAN 10 | EPIC-SALE | WPA2-Enterprise | userWLAN10 | userW10pass |
| Wireless VLAN 20 | EPCI-SPA | WPA2-Enterprise | userWLAN20 | userW20pass |
| Wireless VLAN 30 | EPIC-COUNCIL | WPA2-Enterprise | userWLAN30 | userW30pass |
| Wireless VLAN 40 | EPIC-GUEST | WPA2-Personal | N/A | Epicbeautyspa1 |

Bảng 3. Bảng thông tin WLAN

3.3 Cấu hình chương trình

3.3.1 Cấu hình hạ tầng mạng

* Router EPIC:

Router>enable

Router#configure terminal

Router(config)#int G0/0/1

Router(config-if)#ip add 10.6.0.1 255.255.255.0

Router(config-if)#no shut

Router(config-if)#exit

Router(config)#int G0/0/0

Router(config-if)#no shut

Router(config-if)#int G0/0/0.10

Router(config-subif)#encapsulation dot1q 10

Router(config-subif)#ip add 192.168.10.1 255.255.255.0

Router(config-if)#int G0/0/0.20

Router(config-subif)#encapsulation dot1q 20

Router(config-subif)#ip add 192.168.20.1 255.255.255.0

Router(config-if)#int G0/0/0.30

Router(config-subif)#encapsulation dot1q 30

Router(config-subif)#ip add 192.168.30.1 255.255.255.0

Router(config-if)#int G0/0/0.99

Router(config-subif)#encapsulation dot1q 99 native

Router(config-subif)#ip add 192.168.10.1 255.255.255.0

* Switch S1:

Switch>en

Switch#conf t

Switch#(config)#vlan 10

Switch#(config-vlan)#name SALE

Switch#(config-vlan)#vlan 20

Switch#(config-vlan)#name SPA

Switch#(config-vlan)#vlan 30

Switch#(config-vlan)#name COUNCIL

Switch#(config-vlan)#vlan 40

Switch#(config-vlan)#name GUEST

Switch#(config-vlan)#vlan 99

Switch#(config-vlan)#name ManagementNative

Switch#(config-vlan)#exit

Switch(config)#int F0/1

Switch(config-if)#switchport trunk encapsulation dot1q

Switch(config-if)#swichport mode trunk

Switch(config-if)#switchport trunk native vlan 99

Switch#(config-if)#exit

Switch(config)#int F0/2

Switch(config-if)#switchport trunk encapsulation dot1q

Switch(config-if)#swichport mode trunk

Switch(config-if)#switchport trunk native vlan 99

Switch#(config-if)#exit

Switch(config)#int range F0/21-24

Switch(config-if-range)#switchport trunk encapsulation dot1q

Switch(config-if-range)#swichport mode trunk

Switch(config-if-range)#switchport trunk native vlan 99

Switch(config)#int F0/20

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 99

* Cấu hình DHCP:

Router(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.100

Router(config)#ip dhcp excluded-address 192.168.20.1 192.168.20.100

Router(config)#ip dhcp excluded-address 192.168.30.1 192.168.30.100

Router(config)#ip dhcp excluded-address 192.168.40.1 192.168.40.100

Router(config)#ip dhcp pool WLAN10

Router(dhcp-config)#network 192.168.10.0 255.255.255.0

Router(dhcp-config)#default-router 192.168.10.1

Router(dhcp-config)#dns-server 209.165.201.2

Router(dhcp-config)#ip dhcp pool WLAN20

Router(dhcp-config)#network 192.168.20.0 255.255.255.0

Router(dhcp-config)#default-router 192.168.20.1

Router(dhcp-config)#dns-server 209.165.201.2

Router(dhcp-config)#ip dhcp pool WLAN30

Router(dhcp-config)#network 192.168.30.0 255.255.255.0

Router(dhcp-config)#default-router 192.168.30.1

Router(dhcp-config)#dns-server 209.165.201.2

Router(dhcp-config)#ip dhcp pool WLAN40

Router(dhcp-config)#network 192.168.40.0 255.255.255.0

Router(dhcp-config)#default-router 192.168.40.1

Router(dhcp-config)#dns-server 209.165.201.2

* Graphical user interface, application

  Description automatically generatedTạo tài khoản cho admin để quản lý WLAN với username là **admin** và mật khẩu là **Cisco123**:
* Cấu hình địa chỉ IP cho WLC là 192.168.99.254/24 rồi lưu cấu hình:

Graphical user interface, application

Description automatically generated

* Tại router **Internet** cấu hình cấp DHCP cho router **Home Wireless**:

Router>enable

Router#configure terminal

Router(config)#interface G0/0/0

Router(config-if)#ip add 10.100.200.1 255.255.255.0

Router(config-if)#no shut

Router(config-if)#exit

Router(config)#ip dhcp pool homewifi

Router(dhcp-config)#network 10.100.200.0 255.255.255.0

Router(dhcp-config)#default-router 10.100.200.1

3.3.2 Cấu hình định tuyến cho mạng doanh nghiệp

**Bước 1: Cấu hình giao diện VLAN**

1. Từ **Enterprise Admin**, điều hướng đến giao diện quản lý **WLC** thông qua trình duyệt web. Đăng nhập vào WLC với tên đăng nhập là **admin** và mật khẩu là **Cisco123**.

* Tại Enterprise Admin, Desktop🡪Web Browser, nhập <https://192.168.99.254>

Graphical user interface, text, application

Description automatically generated

1. Định cấu hình cho mạng **WLAN 20**:

* Name: WLAN 20
* VLAN Identifier: 20
* Port number: 1
* Interface IP Address: 192.168.20.254
* Netmask: 255.255.255.0
* Gateway: 192.168.20.1
* Graphical user interface, text, application

  Description automatically generatedPrimary DHCP Server: 192.168.20.1

Graphical user interface

Description automatically generated

Tương tự, tạo WLAN 10:

Định cấu hình cho mạng **WLAN 10**:

* Name: WLAN 10
* VLAN Identifier: 10
* Port number: 1
* Interface IP Address: 192.168.10.254
* Nesmask: 255.255.255.0
* Gateway: 192.168.10.1
* Primary DHCP Server: 192.168.10.1

**WLAN 30**:

* Name: WLAN 30
* VLAN Identifier: 30
* Port number: 1
* Interface IP Address: 192.168.30.254
* Nesmask: 255.255.255.0
* Gateway: 192.168.30.1
* Primary DHCP Server: 192.168.30.1

**WLAN 40**:

* Name: WLAN 40
* VLAN Identifier: 40
* Port number: 1
* Interface IP Address: 192.168.40.254
* Nesmask: 255.255.255.0
* Gateway: 192.168.40.1
* Primary DHCP Server: 192.168.40.1

**Bước 2: Định cấu hình phạm vi DHCP cho mạng quản lý không dây.**

Tại **Controller**, chọn mục **Internal DHCP Server🡪DHCP Scope🡪 New**:

* Scope Name: management
* Pool Start Address: 192.168.99.100
* Pool End Address: 192.168.99.115
* Network: 192.168.99.0
* Netmask: 255.255.255.0
* Default Router: 192.168.99.1

Graphical user interface

Description automatically generatedGraphical user interface, text, application, email

Description automatically generated

**Bước 3: Định cấu hình WLC với địa chỉ máy chủ bên ngoài**

1. Cấu hình thông tin máy chủ RADIUS:

* Server Index:1
* Server Address:10.6.0.254
* Shared Secret: RadiusPW

Tại mục **Security**, chọn **New**, cấu hình theo thông tin trên sau đó **Apply**:

Graphical user interface, text, application, email

Description automatically generated

1. Định cấu hình WLC để gửi thông tin nhật ký đến máy chủ SNMP.

* Community name: WLAN
* IP address: 10.6.0.254

Tại mục **Management🡪SNMP🡪Trap Receivers🡪New**:

Graphical user interface

Description automatically generated

**Bước 4: Tạo các mạng WLAN**

1. **WLAN 40**

Profile name: Wireless VLAN 40

WLAN SSID: EPIC-SPA-GUEST

ID: 4

Interface: WLAN 40

Security: WPA2-PSK

Passphrase: Epicbeautyspa1

Trong tab **Advanced**, hãy chuyển đến phần **FlexConnect** section. Bật tính năng Chuyển mạch **FlexConnect Local** và **FlexConnect Local Auth**.

* Tại **WLANs**, chọn **Create New**, cấu hình theo yêu cầu:

Graphical user interface, application, email

Description automatically generatedGraphical user interface, text

Description automatically generated

Graphical user interface, text, application, email

Description automatically generatedGraphical user interface

Description automatically generated

Graphical user interface, text, email, website

Description automatically generated

1. **WLAN 20**

Profile name: Wireless VLAN 20

WLAN SSID: EPIC-SPA

ID: 3

Interface: WLAN 20

Security: 802.1x - WPA2-Enterprise

Graphical user interface

Description automatically generatedĐịnh cấu hình WLAN sử sụng máy chủ RADIUS để xác thực. Trong tab **Advanced**, hãy chuyển đến phần **FlexConnect** section. Bật tính năng Chuyển mạch **FlexConnect Local** và **FlexConnect Local Auth**.

Graphical user interface, application

Description automatically generated

Graphical user interface

Description automatically generated

Graphical user interface

Description automatically generatedGraphical user interface

Description automatically generated

Tương tự cho các WLAN 10, 30.

1. **WLAN 10**

Profile name: Wireless VLAN 10

WLAN SSID: EPIC-SALE

ID: 2

Interface: WLAN 10

Security: 802.1x - WPA2-Enterprise

1. **WLAN 30**

Profile name: Wireless VLAN 30

WLAN SSID: EPIC-COUNCIL

ID: 5

Interface: WLAN 30

Security: 802.1x - WPA2-Enterprise

**Bước 5: Định cấu hình các host kết nối tới mạng WLAN**

1. Các máy tính ở phòng **Sale** kết nối tới **Wireless VLAN 10** với tên mạng là **EPIC-SALE**, username là **userWLAN10** và password là **userW10pass.**

* Vào **Desktop🡪PC Wirreless**, nhấn tab **Profile**, chọn **Edit**. Nhấn vào tên mạng không dây là **EPIC-SALE** và chọn **Advanced Setup:**

Graphical user interface, text, application

Description automatically generated

* Tại **Wireless Security** chọn **WPA2-Enterprise** và **Next:**

Graphical user interface, text, application

Description automatically generated

* Graphical user interface, text, application

  Description automatically generatedNhập **Login Name** là **userWLAN10** và mật khẩu là **userW10pass** sau đó lưu lại để hoàn thiện việc kết nối.

1. Các máy tính ở phòng **Spa** kết nối tới **Wireless VLAN 20** bằng thông tin đăng nhập trong bảng WLAN với login name là **userWLAN20**, mật khẩu là **userW20pass.**
2. Các máy tính ở phòng **Council** kết nối tới **Wireless VLAN 30** bằng thông tin đăng nhập trong bảng WLAN với login name là **userWLAN30**, mật khẩu là **userW30pass**.
3. Các thiết bị không dây của khách hàng kết nối tới **Wireless VLAN 40** với mật khẩu **Epicbeautyspa1**.

Graphical user interface, table

Description automatically generated

**Bước 6: Tiến hành tạo các Access Point Group để cho phép một AP là một mạng Wireless VLAN được kết nối.**

* Graphical user interface, text, application, email

  Description automatically generatedTại **WLANs**, mục **Advanced🡪AP Groups🡪Add Group**

3.3.3 Định cấu hình mạng wifi cho gia đình

**Bước 1: Cấu hình DHCP**

1. Mở GUI **Home Router** và thay đổi cài đặt IP và DHCP của bộ định tuyến với địa chỉ 192.168.50.1/24.
2. Cho phép bộ định tuyến cấp tối đa 20 địa chỉ.
3. Định cấu hình máy chủ DHCP bắt đầu bằng địa chỉ IP .10 của mạng LAN.
4. Định cấu hình giao diện **internet** của bộ định tuyến để nhận địa chỉ IP của nó qua DHCP.
5. Định cấu hình máy chủ DNS tĩnh thành địa chỉ 209.165.201.2

Graphical user interface, application

Description automatically generated

**Bước 2: Định cấu hình mạng LAN không dây**

1. Mạng sẽ sử dụng giao diện LAN không dây **2.4GHz**. Định cấu hình giao diện với SSID với network name là **HomeEpic.**
2. Sử dụng **channel 6**.

Graphical user interface, application

Description automatically generated

**Bước 3: Định cấu hình bảo mật.**

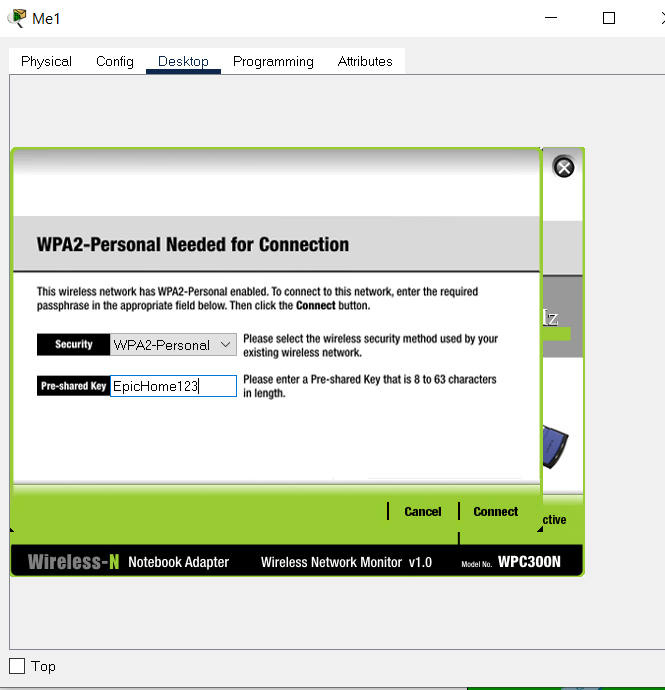
1. Graphical user interface

   Description automatically generatedĐịnh cấu hình bảo mật mạng LAN không dây. Sử dụng **WPA2 Personal** và mật khẩu là **EpicHome123**.
2. Graphical user interface, application

   Description automatically generatedSau đó tại tab **Administration**, thay đổi mật khẩu mặc định thành **EpicHome123.**

**Bước 4: Kết nối máy tính đến mạng**

* Graphical user interface, text, application

  Description automatically generatedMở Laptop chọn **Desktop🡪PC Wirreless**, tại tab **Connect** nhấn vào tên mạng **HomeSSID** để kết nối:
* Click **Connect** và nhập mật khẩu là **EpicHome123** để kết nối thành công.

3.4 Chạy chương trình demo

3.4.1 Mạng gia đình

Các máy có thể truy cập vào trang web trên server thành công:

* Graphical user interface, text, application

  Description automatically generatedLaptop Me1:
* Graphical user interface, text, application

  Description automatically generatedĐiện thoại SamSung:

3.4.2 Mạng doanh nghiệp

Các máy có thể truy cập vào trang web trên server thành công:

* Graphical user interface, text, application

  Description automatically generatedLaptop NV1 ở phòng Sale:
* Graphical user interface, text, application, email

  Description automatically generatedLaptop NV4 ở phòng Spa:
* Laptop NV7 ở phòng Council:

Graphical user interface, text, application, email

Description automatically generated

* Điện thoại KH1 của khách hàng:

Graphical user interface, text, application

Description automatically generated

CHƯƠNG 4 – KẾT LUẬN

Việc nghiên cứu một số vấn đề liên quan đến an toàn và bảo mật trong mạng không dây và di động đã giúp bản thân em phần nào hiểu rõ hơn về một hệ thống mạng không dây trong doanh nghiệp và trong gia đình. Tiến hành nghiên cứu và đề xuất giải pháp xây dựng mạng không dây cho doanh nghiệp là một việc cần thiết để đưa ra những quyết định hiện tại và làm cơ sở cho tương lai. Kết quả của bài báo cáo là những kiến thức mà em có được trong quá trình học tập và nghiên cứu, bên cạnh đó vẫn còn thiếu sót như chưa thể định giá những thiết bị cần cho hệ thống mạng. Qua bài báo cáo này rất mong nhận được những nhận xét quý giá từ thầy để bài báo cáo trở nên hoàn thiện hơn.

**TÀI LIỆU THAM KHẢO**

**Tiếng Việt**

[1] Bài giảng Mạng không dây, trường Đại học Công nghệ TPHCM – Khoa Công nghệ thông tin.

**Tiếng Anh**

[1] Slide Ch1B – Introduction to Mobile and Wireless Network, p.15.

[2] Wireless and Mobile Network Security, Hakima Chaouchi and Maryline Laurent-Maknavicius.

[3] Wireless Network Security, Wolfgang Osterhage.

[4] [IEEE 802.11n-2019, Wikipedia.](https://en.wikipedia.org/wiki/IEEE_802.11n-2009)

[5] [MIMO, Wikipedia.](https://en.wikipedia.org/wiki/MIMO)