TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM

**TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

**KHOA CÔNG NGHỆ THÔNG TIN**



**ĐỒ ÁN CUỐI KÌ MÔN AN TOÀN MẠNG KHÔNG DÂY VÀ DI ĐỘNG**

**Xây dựng hệ thống mạng cho công ty doanh nghiệp cà phê Trung Nguyên**

*Người hướng dẫn*: **TS BÙI QUY ANH**

*Người thực hiện*: **NGUYỄN TRƯỜNG KHƯƠNG DUY - 51800371**

Lớp **: 18050281**

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**



**ĐỒ ÁN CUỐI KÌ MÔN AN TOÀN MẠNG KHÔNG DÂY VÀ DI ĐỘNG**

**Xây Dựng Hệ Thống Mạng Không Dây Cho Doanh Nghiệp Cà Phê Trung Nguyên**

*Người hướng dẫn*: **TS BÙI QUY ANH**

*Người thực hiện*: **NGUYỄN TRƯỜNG KHƯƠNG DUY - 51800371**

Lớp **: 18050281**

Khoá  **: 22**

**THÀNH PHỐ HỒ CHÍ MINH, NĂM 2021**

LỜI CẢM ƠN

Em xin gửi lời cảm ơn đến Ban Giám Hiệu cùng toàn thể quý thầy cô khoa Công Nghệ Thông Tin, trường Đại Học Tôn Đức Thắng đã tạo điều kiện để em có thể hoàn thành được bài báo cáo này. Đặc biệt, em cũng muốn gửi lời cảm ơn sâu sắc nhất đến thầy Bùi Quy Anh vì đã giúp em mở mang thêm kiến thức cơ bản lẫn nâng cao về an ninh mạng không dây và di động. Tuy nhiên, do tình hình dịch bệnh căng thẳng cùng với những giới hạn về kiến thức và thời gian, bài báo cáo sẽ khó tránh khỏi những thiếu sót. Em mong có thể nhận được sự thông cảm, góp ý và chỉ dạy thêm của thầy.

**ĐỒ ÁN ĐƯỢC HOÀN THÀNH**

**TẠI TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

Tôi xin cam đoan đây là sản phẩm đồ án của riêng tôi và được sự hướng dẫn 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 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)*

*Nguyễn Trường Khương Duy*

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

Bài báo cáo gồm có 4 chương:

* Chương 1: Giới thiệu doanh nghiệp, đề xuất giải pháp và báo cáo chi phí
* Chương 2: Các lý thuyết liên quan đến hệ thống
* Chương 3: Mô hình đề xuất, mô tả các bước cấu hình mạng
* Chương 4: Nêu ra các kết quả đạt được khi hoàn thành mô hình hệ thống và các khó khăn lẫn hạn chế trong quá trình xây dựng hệ thống mạng

MỤC LỤC

[LỜI CẢM ƠN ii](#_Toc91892969)

[PHẦN XÁC NHẬN VÀ ĐÁNH GIÁ CỦA GIẢNG VIÊN iv](#_Toc91892970)

[TÓM TẮT v](#_Toc91892971)

[MỤC LỤC 1](#_Toc91892972)

[DANH MỤC CÁC BẢNG BIỂU, HÌNH VẼ, ĐỒ THỊ 6](#_Toc91892973)

[CHƯƠNG 1 – MÔ TẢ ĐỀ TÀI 7](#_Toc91892974)

[1.1. Giới thiệu tập đoàn cà phê Trung Nguyên 7](#_Toc91892975)

[1.2. Yêu cầu khách hàng 8](#_Toc91892976)

[1.3. Đề xuất hướng giải quyết 8](#_Toc91892977)

[1.4. Bảng giá chi phí 9](#_Toc91892978)

[CHƯƠNG 2 – CƠ SỞ LÝ THUYẾT 11](#_Toc91892979)

[2.1. Các thiết bị xây dựng mạng 11](#_Toc91892980)

[2.1.1. Router 11](#_Toc91892981)

[2.1.2. Access Point (AP) 11](#_Toc91892982)

[2.1.3. Switch 12](#_Toc91892983)

[2.1.4. Wireless LAN Controller (WLC) 13](#_Toc91892984)

[2.1.5. Light Weight Access Point (LWAPP) 14](#_Toc91892985)

[2.2. Khái niệm mạng máy tính 15](#_Toc91892986)

[2.2.1. Các mô hình mạng 15](#_Toc91892987)

[2.2.1.1 Mô hình mạng ngang hàng (Peer – to – Peer) 15](#_Toc91892988)

[2.2.1.2 Mô hình khách – chủ (Client – Server) 16](#_Toc91892989)

[2.2.1.3 Mô hình dựa trên nền Web 16](#_Toc91892990)

[2.3. Khái niệm mạng wifi 17](#_Toc91892991)

[2.3.1. Các chuẩn mạng không dây 17](#_Toc91892992)

[2.3.1.1. Chuẩn 802.11 17](#_Toc91892993)

[2.3.1.2. Chuẩn 802.11b 17](#_Toc91892994)

[2.3.1.3. Chuẩn 802.11a 17](#_Toc91892995)

[2.3.1.4. Chuẩn 802.11g 18](#_Toc91892996)

[2.3.1.5. Chuẩn 802.11n 18](#_Toc91892997)

[2.3.1.6. Chuẩn 802.11ac 18](#_Toc91892998)

[2.3.1.7. Chuẩn 802.11ad 18](#_Toc91892999)

[2.3.1.8. Chuẩn 802.11ax 18](#_Toc91893000)

[2.3.2. Các mô hình mạng không dây 19](#_Toc91893001)

[2.3.2.1. Independent Basic Service Set (IBSS) 19](#_Toc91893002)

[2.3.2.2. Basic Service Set (BSS) 20](#_Toc91893003)

[2.3.2.3. Distribution System (DS) 23](#_Toc91893004)

[2.3.2.4. Extended Service Set (ESS) 25](#_Toc91893005)

[2.3.2.5. Mesh Basic Service Set (MBSS) 26](#_Toc91893006)

[2.4. Khái niệm an toàn bảo mật không dây 27](#_Toc91893007)

[2.4.1. Các hình thức tấn công mạng WLAN 29](#_Toc91893008)

[2.4.1.1. Tấn công bằng phần mềm độc hại (Malware) 29](#_Toc91893009)

[2.4.1.2. Tấn công giả mạo (Phishing) 29](#_Toc91893010)

[2.4.1.3. Tấn công trung gian (Man in the middle) 30](#_Toc91893011)

[2.4.1.4. Tấn công từ chối dịch vụ (DoS và DDoS) 30](#_Toc91893012)

[2.4.1.5. Tấn công cơ sở dữ liệu (SQL Injection) 30](#_Toc91893013)

[2.4.1.6. Khai thác lỗ hổng Zero Day (Zero Day) 31](#_Toc91893014)

[2.4.2. Các phương pháp bảo mật cơ bản 31](#_Toc91893015)

[2.4.2.1. Kiểm soát truy cập 31](#_Toc91893016)

[2.4.2.2. Sử dụng tường lửa 31](#_Toc91893017)

[2.4.2.3. Hệ thống phát hiện xâm nhập mạng 31](#_Toc91893018)

[2.4.2.4. VPN (Virtual Private Network) 31](#_Toc91893019)

[2.4.2.5. Giám sát và phân tích mã độc 31](#_Toc91893020)

[2.4.2.6. Xây dựng các chính sách cần thiết 32](#_Toc91893021)

[2.4.3. Các giao thức bảo mật mạng 32](#_Toc91893022)

[2.4.3.1. Giao thức mạng SNMP 32](#_Toc91893023)

[2.4.3.2. Giao thức xác thực AAA 32](#_Toc91893024)

[2.4.3.3. Giao thức RADIUS 34](#_Toc91893025)

[CHƯƠNG 3 – MÔ HÌNH DEMO 36](#_Toc91893026)

[3.1. Mô hình luận lý 36](#_Toc91893027)

[3.2. Mô hình vật lý 36](#_Toc91893028)

[3.2.1. Bảng địa chỉ 37](#_Toc91893029)

[3.2.2. Thông tin VLAN 38](#_Toc91893030)

[3.2.3. Thông tin WLAN 39](#_Toc91893031)

[3.3. Cấu hình thiết bị 40](#_Toc91893032)

[3.3.1. Cấu hình Router R1 40](#_Toc91893033)

[3.3.1.1. Thiết lập bảo mật cho Router R1 40](#_Toc91893034)

[3.3.1.2. Cấp phát địa chỉ IP động (DHCP) 41](#_Toc91893035)

[3.3.1.3. Cấu hình xác thực trên R1 42](#_Toc91893036)

[3.3.1.4. Cấu hình giới hạn đăng nhập 44](#_Toc91893037)

[3.3.2. Sao lưu dữ liệu hệ thống lên Server 44](#_Toc91893038)

[3.3.3. Cấu hình WLC 48](#_Toc91893039)

[3.3.3.1. Tạo giao diện VLAN mới 48](#_Toc91893040)

[3.3.3.2. Cấu hình WLC sử dụng máy chủ RADIUS 53](#_Toc91893041)

[3.3.3.3. Tạo WLAN mới 54](#_Toc91893042)

[3.3.3.4. Cấu hình bảo mật WLAN 59](#_Toc91893043)

[3.3.3.5. Cấu hình DHCP cho Light Weight Access Point 62](#_Toc91893044)

[3.3.3.6. Cấu hình SNMP 66](#_Toc91893045)

[3.3.4. Cấu hình Store Router 68](#_Toc91893046)

[3.3.4.1. Kết nối tới Store Router 68](#_Toc91893047)

[3.3.4.2. Cấu hình bảo mật wifi 70](#_Toc91893048)

[3.3.4.3. Cấu hình bảo mật Store Router 72](#_Toc91893049)

[3.3.5. Cấu hình R0 73](#_Toc91893050)

[3.3.5.1. Cấu hình định tuyến tĩnh 73](#_Toc91893051)

[3.4. Kết quả chạy chương trình 74](#_Toc91893052)

[3.4.1. Bảo mật và DHCP trên R1 74](#_Toc91893053)

[3.4.2. Sử dụng cơ chế xác thực aaa và mã hoá mật khẩu 74](#_Toc91893054)

[3.4.3. Phân quyền tài khoản 76](#_Toc91893055)

[3.4.4. Thông tin WLAN trên WLC 76](#_Toc91893056)

[3.4.5. Giao diện VLAN trên WLC 76](#_Toc91893057)

[3.4.6. Thông tin Server dùng để xác thực 77](#_Toc91893058)

[3.4.7. Thông tin SNMP 77](#_Toc91893059)

[3.4.8. Thông tin các LAP đã được nhận bởi WLC 77](#_Toc91893060)

[3.4.9. Thông tin backup trên Server 78](#_Toc91893061)

[3.4.10. Kết nối đến web server 78](#_Toc91893062)

[3.4.11. Cấp phát IP động 80](#_Toc91893063)

[3.4.12. Ping từ nội bộ ra ngoài và server 80](#_Toc91893064)

[CHƯƠNG 4 – KẾT LUẬN 82](#_Toc91893065)

**DANH MỤC CHỮ VIẾT TẮT**

LWAPP - Lightweight Access Point Protocol

LAP - Lightweight Access Point

AP – Access Point

DHCP - Dynamic Host Configuration Protocol

WLAN - Wireless local area network

VLAN - Virtual local area network

WLC - Wireless LAN controller

RADIUS - Remote Authentication Dial-In User Service

VPN - Virtual Private Network

DSL - Digital Subcriber Line

ISP - Internet Service Provider

DANH MỤC CÁC BẢNG BIỂU, HÌNH VẼ, ĐỒ THỊ

**DANH MỤC HÌNH**

[Hình 1.1 Logo Cà phê Trung Nguyên 7](#_Toc91889629)

[Hình 2.1 Router 10](#_Toc91888205)

[Hình 2.2 Access Point 11](#_Toc91888206)

[Hình 2.3 Switch GS308P 12](#_Toc91888207)

[Hình 2.4 Wireless LAN Controller 13](#_Toc91888208)

[Hình 2.5 Light Weight Access Point 14](#_Toc91888209)

[Hình 2.6 Mô hình mạng ngang hàng 15](#_Toc91888210)

[Hình 2.7 Mô hình khách – chủ 15](#_Toc91888211)

[Hình 2.8 Mô hình IBSS (Independent Basic Service Set) 19](#_Toc91888212)

[Hình 2.9 Mô hình BSS (Basic Service Set) 20](#_Toc91888213)

[Hình 2.10 BSS trong các toà nhà 21](#_Toc91888214)

[Hình 2.11 Lưu lượng từ client bắt buộc phải đi qua AP 22](#_Toc91888215)

[Hình 2.12 Mô hình DS (Distribution System) giữa không dây và có dây 23](#_Toc91888216)

[Hình 2.13 Mô hình DS cho mạng có dây 23](#_Toc91888217)

[Hình 2.14 Mô hình ESS (Extended Service Set) 25](#_Toc91888218)

[Hình 2.15 Mô hình MBSS (Mesh Basic Service Set) 26](#_Toc91888219)

[Hình 2.16 Các mục tiêu bảo mật chính 28](#_Toc91888220)

[Hình 3.1 Các chuẩn wifi 18](#_Toc91885713)

CHƯƠNG 1 – MÔ TẢ ĐỀ TÀI

* 1. Giới thiệu tập đoàn cà phê Trung Nguyên



Hình 1.1 Logo Cà phê Trung Nguyên

Tập đoàn Trung Nguyên là một doanh nghiệp hoạt động trong các lĩnh vực sản xuất, chế biến, kinh doanh cà phê; nhượng quyền thương hiệu; dịch vụ phân phối, bán lẻ hiện đại và du lịch. Cà phê Trung Nguyên là một trong những thương hiệu nổi tiếng hàng đầu tại Việt Nam và đang có mặt tại hơn 60 quốc gia trên thế giới.

Trung Nguyên E-Coffee là chuỗi cửa hàng bán lẻ thế giới cà phê của Tập đoàn Trung Nguyên Legend – nơi hội tụ tinh hoa của 3 nền văn minh cà phê: Ottoman – Roman – Thiền được ra mắt từ tháng 8/2019.

Ngay từ khi ra đời, Trung Nguyên E-Coffee nhanh chóng tạo nên một làn sóng bùng nổ nhượng quyền mạnh mẽ, trở thành sự lựa chọn số 1 của hơn 1.000 đối tác và hiện diện trên toàn quốc. Trung Nguyên E-Coffee được xem là một giải pháp tối ưu cho cộng đồng kinh doanh, khởi nghiệp với cà phê, từ nhân viên văn phòng, chủ cửa tiệm tạp hoá – quán cà phê truyền thống, sinh viên, các công ty trong lĩnh vực nhượng quyền, ẩm thực, du lịch, vận tải, bản lẻ… đều có thể tham gia hợp tác.

Không chỉ sở hữu thiết kế linh hoạt cho mọi địa điểm, Trung Nguyên E-Coffee còn có chính sách hợp tác tối đa lợi ích nhất cho tất cả các đối tác từ chính sách gói hợp tác đến các chương trình hỗ trợ đào tạo, tư vấn, vận hành… Hơn nữa, với hệ sản phẩm đặc biệt gồm hơn 100 sản phẩm cà phê năng lượng tuyệt ngon và công cụ dụng cụ pha chế thưởng thức theo ba nền văn minh cà phê – sách quý đổi đời – bánh mì thực dưỡng, Trung Nguyên E-Coffee tạo nên một thế giới cà phê thu nhỏ, đáp ứng cho những người yêu cà phê có thể trải nghiệm đầy đủ các gói sản phẩm thưởng lãm tại nhà, văn phòng, hàng quán…

* 1. Yêu cầu khách hàng

Xây dựng hệ thống mạng có dây và không dây cho 1 chi nhánh ở TP.Hồ Chí Minh gồm có 4 phòng ban là: Quản lý chi nhánh, quản lý nhân sự, kế toán, marketing. Chi nhánh rộng 150m gồm có 4 tầng. Tầng 1 dùng cho mareting, tầng 2 là kế toán, tầng 3 là quản lý nhân sự và tầng 4 là quản lý chi nhánh. Quản lý chi nhánh có đặc quyền cao nhất và truy cập được tất cả mọi thứ. Quy mô công ty khoảng 100 nhân viên các phòng ban. Mỗi phòng ban gồm có 20 nhân viên, 1 máy in. Các phòng ban chỉ có thể truy cập lẫn nhau thông qua máy tính nội bộ và không thể kết nối đến các phòng ban khác trừ quản lý chi nhánh, mỗi phòng ban đều có 1 mật khẩu và đặc quyền riêng.

* 1. Đề xuất hướng giải quyết

Mỗi phòng ban sẽ có 1 switch, 1 PC, 1 LAP 1 máy in. Tất cả thiết bị sẽ được cấu hình IP tự động. Người dùng chỉ có thể truy cập vào wifi của phòng ban tương ứng. Ví dụ: marketing thì chỉ có thể truy cập vào wifi của ban marketing. Công ty sẽ có 1 server dùng để xác thực và backup dữ liệu khi cần thiết. Bên cạnh chi nhánh sẽ có 1 quán caffee nhỏ sử dụng 1 router wifi và 1 PC dùng cho thu ngân. Để đảm bảo an toàn, mạng không dây và router đều được cấu hình bảo mật.

* 1. Bảng giá chi phí

**Bảng tính toán chi phí thiết bị cần thiết để xây dựng hệ thống mạng**

*Lưu ý: Giá của các thiết bị chỉ mang tính chất tham khảo, có thể tăng hoặc giảm tuỳ vào nhu cầu và tình hình lúc triển khai. Giá được cập nhật vào ngày 31/12/2021*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **STT** | **Tên thiết bị** | **SL** | **Giá/thiết bị (đ)** | **Tổng tiền** |
| 1 | Router Cisco ISR4331/K9 | 2 | 46.300.000 | 92.600.000 |
| 2 | Switch Cisco WS-C2960-24TC-S | 5 | 8.623.000 | 43.115.000 |
| 3 | Switch Cisco WS-C3560-24TS-S | 1 | 42.280.000 | 42.280.000 |
| 4 | Cisco 3702I-C-K9 | 4 | 12.700.000 | 50.800.000 |
| 5 | Router wifi AC2350 Xiaomi | 1 | 1.290.000 | 1.290.000 |
| 6 | PC HP All in One 200 Pro G4 | 6 | 13.799.000 | 82.794.000 |
| 7 | Máy in HP Neverstop Laser 1000w Wifi | 4 | 3.090.000 | 12.360.000 |
| 8 | Cisco 3504 Wireless Controller AIR-CT3504-K9 | 1 | 58.750.000 | 58.750.000 |
| 9 | SERVER Tower SSN T440 | 3 | 37.704.000 | 113.112.000 |
| **Tổng cộng** | | | | **9 tỷ 2** |

**Bảng tính toán chi phí lắp đặt và duy trì hệ thống mạng**

*Lưu ý: Giá cước wifi sẽ được thu hàng tháng với số tiền đó cho đến khi kết thúc hợp đồng. Chi phí xây dựng và triển khai chính thức có thể tăng hoặc giảm tuỳ theo yêu cầu và tình hình triển khai*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **STT** | **Tên thiết bị** | **SL** | **Giá/thiết bị (đ)** | **Tổng tiền (đ)** |
| 1 | Đầu Mạng RJ45 Dintek UTP Cat.5e 1501-88052 (100 đầu) | 1 | 280.000 | 280.000 |
| 2 | Monoprice 102376 3-Feet 24AWG Cat6 500MHz Crossover Ethernet Bare Copper Network Cable, Red (102376) | 4 | 12.000 | 48.000 |
| 3 | CAB-SS-V35MT | 1 | 2.000.000 | 2.000.000 |
| 4 | Dây mạng 25m | 5 | 75.000 | 375.000 |
| 5 | Gói cước SUPERNET 5 viettel | 1 | 430.000/tháng | 430.000 |
| 6 | Công lắp đặt thiết bị  (10% tiền thiết bị) | 1 | 90.000.000 | 90.000.000 |
| **Tổng cộng** | | | | **93.133.000** |

CHƯƠNG 2 – CƠ SỞ LÝ THUYẾT

* 1. Các thiết bị xây dựng mạng
     1. Router

Router (thiết bị định tuyến hoặc bộ định tuyến) là [thiết bị mạng](https://www.thegioididong.com/thiet-bi-mang" \t "_blank) dùng để chuyển các gói dữ liệu đến các thiết bị đầu cuối. Nói một cách dễ hiểu, Router là một thiết bị để chia sẻ Internet tới nhiều các thiết bị khác trong cùng lớp mạng.

Router WiFi giúp biến mạng có dây thành không dây giúp kết nối các thiết bị di động với nhau dễ dàng hơn. Giúp nhiều người trong nhà cùng sử dụng được mạng Internet đồng thời mà không bị giới hạn như mạng có dây. Ngoài ra khi kết nối có dây cũng làm cho nhà bạn trở nên gọn gàng hơn nữa.



Hình 2.1 Router

* + 1. Access Point (AP)

AP là một thiết bị tạo ra một mạng không dây cục bộ, hoặc WLAN, thường trong một văn phòng hoặc tòa nhà lớn. Một điểm truy cập access point là một trạm truyền và nhận dữ liệu. Có thể gọi chúng là bộ thu phát wifi.

Một điểm truy cập Access Point kết nối người dùng với những người dùng khác trong cùng một mạng. Ngoài ra chúng còn đóng vai trò là điểm kết nối giữa mạng WLAN và mạng dây cố định. Trong một khu vực mạng được xác định thì mỗi điểm truy cập Access Point có thể phục vụ nhiều người dùng. Nếu khi mọi người di chuyển ra ngoài phạm vi của một điểm truy cập, thì chúng sẽ tự động được chuyển sang điểm tiếp theo.

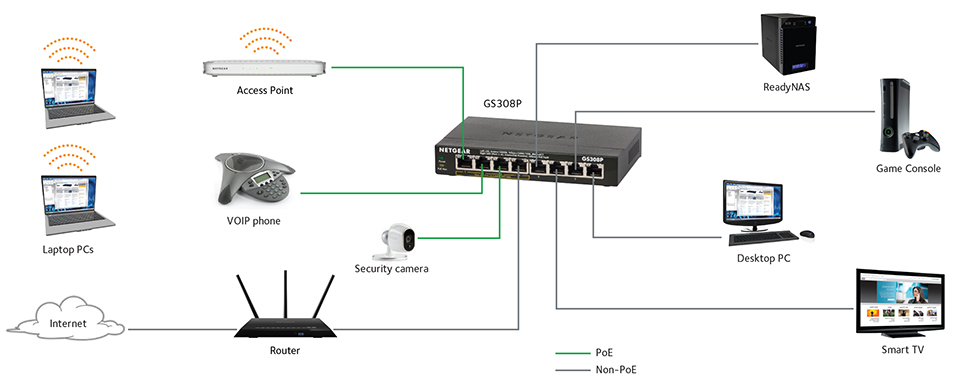


Hình 2.2 Access Point

* + 1. Switch

Switch là một thiết bị chuyển mạch tối quan trọng trong mạng, dùng để kết nối các đoạn mạng với nhau theo mô hình hình sao (Star). Trong mô hình này, switch đóng vai trò trung tâm và tất cả các thiết bị vệ tinh khác kể cả máy tính đều được kết nối về đây, từ đó định tuyến tạo đường nối tạm trung chuyển dữ liệu đi. Ngoài ra, Switch được hỗ trợ công nghệ Full Duplex dùng để mở rộng băng thông của đường truyền, điều mà các thiết bị khác không làm được.

Có thể hiểu đơn giản thiết bị chuyển mạch Switch giống như cảnh sát giao thông phân luồng dữ liệu của một mạng cục bộ. Nó có khả năng chọn đường dẫn để quyết định chuyển frame (đơn vị của tầng liên kết dữ liệu) nên [mạng LAN](https://www.totolink.vn/article/151-lan-la-gi-tong-quan-kien-thuc-ve-lan-ma-ban-nen-biet.html) hoạt động hiệu quả hơn. Switch có khả năng nhận dạng máy được kết nối với nó nhờ cách đọc địa chỉ MAC nguồn trong frame nó nhận được. Khi hai máy trong mạng liên lạc với nhau, chính Switch sẽ tạo mạch ảo giữa hai cổng tương ứng mà không làm ảnh hưởng đến lưu thông trên các cổng khác.



Hình 2.3 Switch GS308P

* + 1. Wireless LAN Controller (WLC)
* WLC trong mô hình mạng có chức năng quản lý, thống nhất các AP lại với nhau. Một WLC có thể quản lý 6-300 AP, trên mỗi AP có thể gán đế 15 mạng WLAN và hỗ trợ tối đa 512 VLAN. AP và WLC giao tiếp với nhau bằng giao thức LWAPP được cung cấp bởi radio resource management (RRM).
* RRM có thể giám sát nguồn tài nguyên vô tuyến, thực hiện phân bổ các kênh, phát hiện và tránh nhiễu và cung cấp việc kiểm soát năng lượng trong việc truyền thông tin động (TPC). Ngoài ra, WLC có thể điều chỉnh để khắc phục các lổ hỏng vùng phủ sóng LWAPP làm việc ở 2 chế độ:
  + Chế độ vận chuyển LWAPP layer 2
  + Chế độ vận chuyển LWAPP layer 3



Hình 2.4 Wireless LAN Controller

* + 1. Light Weight Access Point (LWAPP)

Giao thức điểm truy cập nhẹ (LWAPP) là tên của giao thức có thể điều khiển nhiều điểm truy cập không dây Wi-Fi cùng một lúc. Điều này có thể làm giảm lượng thời gian dành cho việc định cấu hình, giám sát hoặc khắc phục sự cố của một mạng lớn. Hệ thống cũng sẽ cho phép quản trị viên mạng phân tích chặt chẽ mạng. Hệ thống này được cài đặt trong một máy chủ trung tâm thu thập dữ liệu từ các thiết bị RF từ các thương hiệu và cài đặt khác nhau. Máy chủ có thể ra lệnh cho một nhóm thiết bị được chọn áp dụng đồng thời các cài đặt đã cho.



Hình 2.5 Light Weight Access Point

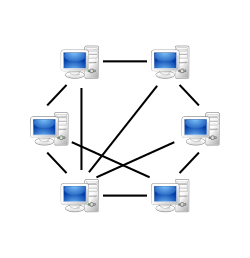
* 1. Khái niệm mạng máy tính

Mạng máy tính là một hệ thống gồm nhiều máy tính và các thiết bị được kết nối với nhau bởi đường truyền vật lý theo một kiến trúc (Network Architecture) nào đó nhằm thu thập, trao đổi dữ liệu và chia sẽ tài nguyên cho nhiều người sử dụng. Các máy tính được kết nối với nhau có thể trong cùng một phòng, một tòa nhà, một thành phố hoặc trên phạm vi toàn cầu. Mạng máy tính bao gồm ba thành phần chính:

* Các máy tính.
* Các thiết bị mạng đảm bảo kết nối các máy tính với nhau.
* Phần mềm cho phép thực hiện việc trao đổi thông tin giữa các máy tính.
  + 1. ****Các mô hình mạng****

**2.2.1.1 Mô hình mạng ngang hàng (Peer – to – Peer)**

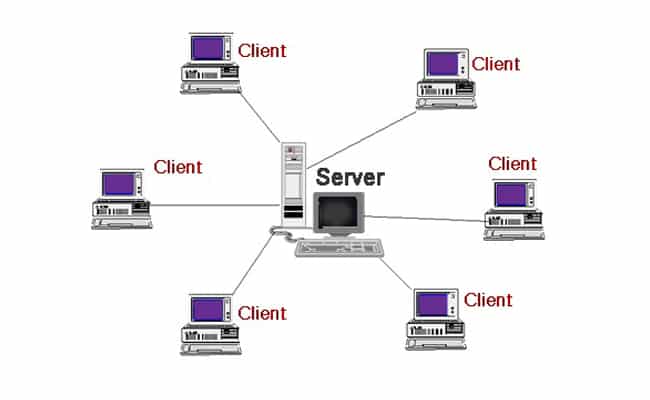
Trong mô hình này, tất cả các máy tính tham gia đều có vai trò giống nhau. Mỗi máy vừa có thể cung cấp trực tiếp tài nguyên của mình cho các máy khác, vừa có thể sử dụng trực tiếp tài nguyên của các máy khác trong mạng. Mô hình này chỉ thích hợp với mạng có quy mô nhỏ, tài nguyên được quản lý phân tán và chế độ bảo mật kém.



Hình 2.6 **Mô hình mạng ngang hàng**

**2.2.1.2 Mô hình khách – chủ (Client – Server)**

Trong mô hình này, một hoặc vài máy sẽ được chọn để đảm nhận việc quản lý và cung cấp tài nguyên (chương trình, dữ liệu, thiết bị,…) được gọi là máy chủ (Server), các máy khác sử dụng tài nguyên này được gọi là máy khách (Client). Máy chủ là máy tính đảm bảo việc phục vụ các máy khách bằng cách điều khiển việc phân phối tài nguyên nằm trong mạng với mục đích sử dụng chung. Máy khách là máy sử dụng tài nguyên do máy chủ cung cấp. Mô hình khách – chủ có ưu điểm là dữ liệu được quản lý tập trung, bảo mật tốt, thích hợp với các mạng trung bình và lớn.



Hình 2.7 **Mô hình khách – chủ**

**2.2.1.3 Mô hình dựa trên nền Web**

Ngày nay, do sự phát triển của Internet nên có rất nhiều công ty và cá nhân sử dụng Internet như một mạng “xương sống” và kết nối với mọi người trên toàn cầu. Mạng trên phạm vi Internet được gọi là mạng liên kết nối và ngày càng trở nên phổ biến. Người dùng chỉ cần trình duyệt Web và một kết nối Internet để chia sẻ các tập tin, tải các ứng dụng, xem video hoặc tham gia học tập trực tuyến.

* 1. Khái niệm mạng wifi

Là một mạng máy tính sử dụng các kết nối dữ liệu không dây giữa các nút mạng bằng cách sử dụng [sóng radio](https://vi.wikipedia.org/wiki/Radio) làm [sóng truyền dẫn](https://vi.wikipedia.org/w/index.php?title=S%C3%B3ng_truy%E1%BB%81n_d%E1%BA%ABn&action=edit&redlink=1" \o "Sóng truyền dẫn (trang chưa được viết)) hay [tầng vật lý](https://vi.wikipedia.org/wiki/T%E1%BA%A7ng_v%E1%BA%ADt_l%C3%BD" \o "Tầng vật lý). 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](https://vi.wikipedia.org/wiki/Internet_t%E1%BA%A1i_Vi%E1%BB%87t_Nam) 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](https://vi.wikipedia.org/wiki/OSI).

Những ví dụ điển hình về mạng không dây là: mạng wifi, mạng 3G, mạng điện thoại di động, mạng bluetooth, mạng nội bộ không dây ([WLAN](https://vi.wikipedia.org/wiki/WLAN)), mạng cảm biến không dây, mạng truyền thông vệ tinh và mạng sóng mặt đất. Dưới đây là các mô hình mạng không dây

* + 1. Các chuẩn mạng không dây
       1. **Chuẩn 802.11**

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.**

* + - 1. **Chuẩn 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.

* + - 1. **Chuẩn 802.11a**

Song song với quá trình hình thành chuẩn b, 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.

* + - 1. **Chuẩn 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.**

* + - 1. **Chuẩn 802.11n**

Ra mắt năm 2009 và là chuẩn phổ biến nhất hiện nay nhờ sự vượt trội hơn so với chuẩn b và 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.

* + - 1. Chuẩn 802.11ac

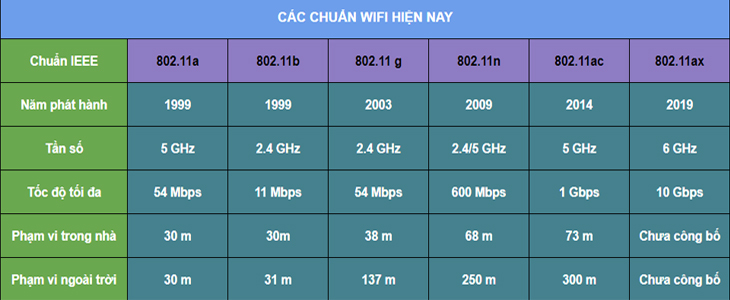
Là chuẩn được IEEE giới thiệu vào đầu năm 2013, hoạt động ở băng tầng 5 GHz. Chuẩn ac có thể mang đến cho người dùng trải nghiệm tốc độ cao nhất lên đến 1730 Mpbs. Do vấn đề giá thành cao nên các thiết bị phát tín hiệu cho chuẩn này chưa phổ biến dẫn đến các thiết bị này sẽ bị hạn chế sự tối ưu do thiết bị phát.

* + - 1. Chuẩn 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.

* + - 1. Chuẩn 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 3.1 Các chuẩn wifi

* + 1. Các mô hình mạng không dây
       1. Independent Basic Service Set (IBSS)

Với Independent Basic Service Set (IBSS), hai hoặc nhiều thiết bị không dây kết nối trực tiếp mà không cần điểm truy cập (AP). Chúng tôi cũng gọi đây là mạng đặc biệt. Một trong các thiết bị phải khởi động và quảng bá SSID, tương tự như những gì một AP sẽ làm. Các thiết bị khác sau đó có thể tham gia mạng tuy nhiên IBSS không phải là một giải pháp phổ biến.

A picture containing text, computer, computer, indoor

Description automatically generated

Hình 2.8 Mô hình IBSS (Independent Basic Service Set)

* + - 1. Basic Service Set (BSS)

Với Bộ dịch vụ cơ bản (BSS), các máy khách không dây kết nối với mạng không dây thông qua một AP. BSS là thứ chúng tôi sử dụng cho hầu hết các mạng không dây. Ý tưởng đằng sau BSS là AP chịu trách nhiệm về mạng không dây.

Mỗi client không dây quảng bá khả năng của mình cho AP và AP cấp hoặc từ chối quyền tham gia mạng. BSS sử dụng kênh duy nhất cho tất cả các giao tiếp. AP và không dây của client sử dụng cùng một kênh để truyền và nhận.

Diagram

Description automatically generated

Hình 2.9 Mô hình BSS (Basic Service Set)

SSID là tên "đẹp" của mạng không dây và nó không nhất thiết phải là duy nhất. AP cũng quảng bá Mã nhận dạng nhóm dịch vụ cơ bản (BSSID). Đây là địa chỉ MAC của đài AP, một địa chỉ duy nhất xác định AP. Tất cả các client không dây phải kết nối với AP. Điều này có nghĩa là phạm vi tín hiệu của AP xác định kích thước của BSS và được gọi là Khu vực Dịch vụ Cơ bản (BSA).

Trong hình trên, BSA là một vòng tròn đẹp. Trường hợp này có thể xảy ra nếu bạn cài đặt AP của mình ở đâu đó giữa đồng cỏ mà không có gì xung quanh AP. Trong một tòa nhà, BSA có thể trông giống như thế này:

Diagram

Description automatically generated

Hình 2.10 BSS trong các toà nhà

Khi một thiết bị không dây muốn tham gia BSS, nó sẽ gửi một yêu cầu liên kết đến AP. AP cho phép hoặc từ chối yêu cầu. Khi thiết bị không dây đã tham gia BSS, chúng tôi gọi nó là client không dây hoặc trạm 802.11 (STA).

Tất cả lưu lượng từ một máy khách không dây phải đi qua AP ngay cả khi nó được dành cho một client không dây khác.

Diagram

Description automatically generated

Hình 2.11 Lưu lượng từ client bắt buộc phải đi qua AP

Mọi thứ đều phải thông qua AP vì AP là điểm quản lý trung tâm của chúng tôi và nó giới hạn quy mô của BSS. Dải tín hiệu của AP xác định ranh giới của BSS.

* + - 1. Distribution System (DS)

BSS là một mạng độc lập với một AP duy nhất. Trong các hình trên, không có kết nối với mạng có dây.

Tuy nhiên, hầu hết các mạng không dây là một phần mở rộng của mạng có dây. Một AP hỗ trợ cả kết nối có dây và không dây. Tiêu chuẩn 802.11 gọi mạng có dây ngược dòng là sự phân phối hệ thống (DS).

AP làm cầu nối giữa các khung Ethernet L2 có dây và không dây, cho phép lưu lượng truyền từ mạng có dây sang mạng không dây và ngược lại.

Diagram

Description automatically generated

Hình 2.12 Mô hình DS (Distribution System) giữa không dây và có dây

Chúng tôi cũng có thể làm điều này với VLAN. AP kết nối với bộ chuyển mạch với 802.1Q trunk. Mỗi SSID ánh xạ tới một VLAN khác nhau:

Diagram

Description automatically generated

Hình 2.13 Mô hình DS cho mạng có dây

Mỗi mạng không dây có một BSSID duy nhất. BSSID dựa trên địa chỉ MAC, vì vậy hầu hết các nhà cung cấp (bao gồm cả Cisco) tăng chữ số cuối cùng của địa chỉ MAC để tạo ra một BSSID duy nhất.

Mặc dù chúng ta có nhiều mạng không dây, nhưng tất cả chúng đều sử dụng phần cứng, băng tầng và kênh cơ bản giống nhau. Nếu bạn có một AP với nhiều băng tầng, thì bạn có thể chỉ định mạng không dây cho các băng tầng khác nhau. Ví dụ: bạn có thể sử dụng một mạng không dây trên băng tầng 2,4 GHz và một mạng khác trên băng tầng 5 GHz.

* + - 1. Extended Service Set (ESS)

Một BSS sử dụng một AP duy nhất. Điều này có thể không đủ vì hai lý do:

* Phạm vi phủ sóng: Một tín hiệu của AP không thể bao phủ toàn bộ tầng hoặc tòa nhà. Bạn cần nhiều AP nếu bạn muốn mạng không dây ở mọi nơi.
* Băng thông: Một AP sử dụng một kênh duy nhất và không dây là bán song công. Bạn càng có nhiều máy khách không dây hoạt động, thông lượng của bạn sẽ càng thấp. Điều này cũng phụ thuộc vào tốc độ dữ liệu mà bạn hỗ trợ. Một ứng dụng khách không dây nằm trên biên giới BSA của bạn vẫn có thể truy cập AP, nhưng chỉ có thể sử dụng tốc độ dữ liệu thấp. Một máy khách không dây đặt gần AP có thể sử dụng tốc độ dữ liệu cao. Máy khách không dây ở xa sẽ yêu cầu nhiều "thời gian phát sóng" hơn, giảm băng thông cho mọi người.

Để tạo một mạng không dây lớn hơn, chúng tôi sử dụng nhiều AP và kết nối tất cả chúng với mạng có dây. Các AP làm việc cùng nhau để tạo ra một mạng không dây lớn trải dài toàn bộ một tầng hoặc tòa nhà. Người dùng chỉ nhìn thấy một SSID duy nhất, vì vậy họ sẽ không nhận thấy liệu chúng tôi sử dụng một hay nhiều AP. Mỗi AP sử dụng một BSSID khác nhau, do đó, đằng sau hậu trường, client không dây thấy nhiều AP mà nó có thể kết nối. Chúng tôi gọi cấu trúc liên kết này với nhiều AP là Bộ dịch vụ mở rộng (ESS).

Diagram

Description automatically generated

Hình 2.14 Mô hình ESS (Extended Service Set)

Các AP hoạt động cùng nhau. Ví dụ: nếu bạn kết hợp với một AP và bạn đi bộ xung quanh tòa nhà, bạn sẽ không ngắt kết nối. Máy khách không dây sẽ tự động “nhảy” từ AP này sang AP khác. Chúng tôi gọi đây là chuyển vùng. Để làm cho trải nghiệm này trở nên liền mạch, chúng ta cần có sự chồng chéo giữa các AP. Mỗi AP cung cấp BSS riêng và sử dụng một kênh khác nhau để ngăn nhiễu giữa các AP

* + - 1. Mesh Basic Service Set (MBSS)

Nếu bạn muốn cung cấp mạng không dây cho một khu vực rộng lớn, chẳng hạn như một thành phố, thì việc kết nối từng AP với mạng có dây là điều không dễ dàng.

Thay vào đó, bạn có thể xây dựng một mạng lưới, còn được gọi là Bộ Dịch vụ Cơ bản Mesh (MBSS). Với mạng lưới, chúng tôi kết nối lưu lượng truy cập không dây từ AP này sang AP khác. Các AP dạng lưới thường có nhiều băng tầng. Một băng tầng dành cho lưu lượng truy cập backhaul của mạng lưới giữa các AP; băng tầng khác là để duy trì một BSS cho các máy khách không dây trên một kênh khác.

Ít nhất một AP được kết nối với mạng có dây; chúng tôi gọi đây là Root AP (RAP). Các AP khác là Mesh AP (MAP) và chỉ được kết nối thông qua backhaul không dây.

Diagram

Description automatically generated

Hình 2.15 Mô hình MBSS (Mesh Basic Service Set)

Có nhiều đường dẫn để MAP đến được mạng có dây thông qua RAP, vì vậy chúng ta cần một giao thức tìm ra đường dẫn không có vòng lặp tốt nhất. Tương tự như cách thức hoạt động của cây bao trùm đối với L2 hoặc các giao thức định tuyến cho L3, có các giải pháp không dây khác nhau. IEEE có tiêu chuẩn 802.11s cho mạng lưới. Các nhà cung cấp đôi khi cũng sử dụng các giải pháp độc quyền. Ví dụ: Cisco có Giao thức đường dẫn không dây thích ứng (AWPP). Các AP của Cisco hỗ trợ cả mạng lưới trong nhà và ngoài trời.

* 1. Khái niệm an toàn bảo mật không dây

Bảo mật máy tính là bảo vệ hệ thống thông tin tự động nhằm đạt được các mục tiêu là duy trì tính toàn vẹn, tính sẵn sàng và tính bảo mật của tài nguyên hệ thống thông tin (gồm phần cứng, phần mềm, dữ liệu/thông tin người dùng,...)

Có 3 mục tiêu chính (CIA) để hệ thống được an toàn là:

* Confidentiality (tính bí mật):
  + Bảo mật dữ liệu: Đảm bảo rằng thông tin bí mật không tiết lộ cho các cá nhân trái phép
  + Quyền riêng tư: Đảm bảo rằng cá nhân kiểm soát hoặc ảnh hưởng đến những gì thông tin có thể được thu thập và lưu trữ
* Integrity (tính toàn vẹn):
  + Tính toàn vẹn dữ liệu: Đảm bảo rằng thông tin và chương trình được thay đổi chỉ theo một cách cụ thể và được ủy quyền
  + Tính toàn vẹn hệ thống: Đảm bảo rằng một hệ thống thực hiện các hoạt động của nó một cách chính xác
* Availability (tính sẵn sàng): Đảm bảo rằng hệ thống hoạt động nhanh chóng và dịch vụ không bị từ chối đối với người dùng được ủy quyền

Diagram

Description automatically generated

Hình 2.16 Các mục tiêu bảo mật chính

Ngoài ra còn có các mục tiêu khác như:

* Authenticity (Tính xác thực): Đảm bảo thông tin người gửi hợp pháp
* Accountability (Tính giải trình): Tạo ra yêu cầu đối với các hành động của một thực thể phải được theo dõi duy nhất đối với cá nhân đó để hỗ trợ việc không từ chối, bảo vệ, cách ly lỗi, v.v. Ví dụ: chữ ký điện tử, sao kê
  + 1. Các hình thức tấn công mạng WLAN
       1. Tấn công bằng phần mềm độc hại (Malware)

Một trong những hình thức tấn công mạng điển hình nhất những năm gần đây là hình thức tấn công bằng phần mềm độc hại (malware). Các phần mềm độc hại này bao gồm: mã độc tống tiền (ransomeware), phần mềm gián điệp (spyware), virus và worm (phần mềm độc hại có khả năng lây lan với tốc độ chóng mặt). Các tin tặc thường khai thác các lỗ hổng bảo mật để cài đặt malware nhằm xâm nhập và tấn công hệ thống.

Một số hậu quả do malware gây ra:

* Chặn người dùng truy cập vào các file hoặc folder nhất định
* Theo dõi hành động của người dùng và đánh cắp dữ liệu
* Làm hỏng phần cứng và làm ngưng trệ hoạt động
  + - 1. Tấn công giả mạo (Phishing)

Phishing Attack là hình thức tấn công trong đó tin tặc giả mạo thành một tổ chức hoặc cá nhân uy tín để lấy lòng tin của người dùng. Từ đó, chúng đánh cắp các dữ liệu nhạy cảm như tài khoản ngân hàng, thẻ tín dụng…

Các cuộc tấn công giả mạo thường được thực hiện qua email. Cụ thể, người dùng sẽ nhận được email giả mạo một tổ chức/ cá nhân uy tín với thông điệp vô cùng khẩn thiết. Thông điệp này yêu cầu người dùng click vào đường link tin tặc tạo ra. Nếu click vào, người dùng sẽ được chuyển đến một website giả mạo và được yêu cầu đăng nhập. Khi đó, tin tặc sẽ có được thông tin đăng nhập và dữ liệu nhạy cảm khác của người dùng.

Mục đích của tấn công Phishing thường là đánh cắp dữ liệu như thông tin thẻ tín dụng, mật khẩu. Đôi khi, tấn công phishing là để lừa người dùng cài đặt malware vào thiết bị. Lúc này, phishing là một công đoạn trong cuộc tấn công malware.

* + - 1. Tấn công trung gian (Man in the middle)

Tấn công trung gian là hình thức tin tặc xen vào giữa phiên giao dịch hay giao tiếp giữa hai đối tượng. Khi đã xâm nhập thành công, chúng có thể theo dõi được mọi hành vi của người dùng. Tệ hơn, chúng có thể đánh cắp được toàn bộ dữ liệu trong phiên giao dịch đó. Tấn công trung gian dễ xảy ra khi nạn nhân truy cập vào một mạng wifi không an toàn.

* + - 1. Tấn công từ chối dịch vụ (DoS và DDoS)

DoS (Denial of Service) là hình thức tấn công mà tin tặc đánh sập một hệ thống hoặc máy chủ tạm thời bằng cách tạo ra một lượng traffic khổng lồ ở cùng một thời điểm khiến cho hệ thống bị quá tải. Khi đó, người dùng không thể truy cập vào mạng trong thời gian tin tặc tấn công.

[DDoS (Distributed Denial of Service)](https://securitybox.vn/1353/12-loai-tan-cong-ddos-tan-cong-tu-choi-dich-vu-ddos/) là hình thức biến thể của DoS. Theo đó, tin tặc sử dụng một mạng lưới các máy tính để tấn công. Sự nguy hiểm thể hiện ở chỗ chính các máy tính thuộc mạng lưới máy tính trên cũng không biết bản thân đang bị lợi dụng làm công cụ tấn công.

Hình thức tấn công DDoS chủ yếu nhắm vào các mục tiêu như: website, máy chủ trò chơi, máy chủ DNS… làm chậm, gián đoạn hoặc đánh sập hệ thống. Theo dự đoán của các cơ quan bảo mật, tần suất của tấn công DDoS sẽ ngày càng gia tăng. Nười dùng nên đặc biệt cẩn trọng.

* + - 1. Tấn công cơ sở dữ liệu (SQL Injection)

SQL Injection là hình thức tấn công trong đó tin tặc chèn một đoạn mã độc hại vào server sử dụng ngôn ngữ SQL để đánh cắp những dữ liệu quan trọng.

Hậu quả lớn nhất của SQL Injection là làm lộ dữ liệu trong database. Đây là điều đặc biệt tối kỵ bởi chúng sẽ ảnh hưởng nặng nề đến uy tín của doanh nghiệp. Khi khách hàng mất niềm tin vào doanh nghiệp, khả năng cao họ sẽ sử dụng dịch vụ của bên khác. Doanh số giảm sút là hậu quả dễ thấy đầu tiên mà doanh nghiệp phải gánh chịu.

* + - 1. Khai thác lỗ hổng Zero Day (Zero Day)

Lỗ hổng Zero Day là các lỗ hổng bảo mật chưa được các nhà phát triển phần mềm biết tới. Vì vậy, chưa có bản vá chính thức cho các lỗ hổng này. Nói cách khác, các vụ tấn công Zero Day xảy ra một cách bất ngờ mà các nhà phát triển phần mềm không thể dự liệu trước. Đó là lý do hậu quả của các vụ tấn công Zero Day thường vô cùng nặng nề.

* + 1. Các phương pháp bảo mật cơ bản
       1. Kiểm soát truy cập

Kiểm soát truy cập hạn chế đối tượng truy cập vào các tài nguyên của doanh nghiệp bằng việc kiểm tra thông tin người truy cập bằng một số phương pháp: đăng nhập bằng tài khoản/mật khẩu được cung cấp, nhận diện gương mặt hoặc dấu vân tay,...

* + - 1. Sử dụng tường lửa

Tường lửa là công cụ giúp doanh nghiệp ngăn chặn những cố gắng xâm nhập của người ngoài tổ chức, tạo rào chắn giữa mạng nội bộ và một mạng khác (Internet,...), theo dõi, quản lý lưu lượng truy cập và ngăn chặn ngay khi xuất hiện dấu hiệu đáng ngờ.

* + - 1. Hệ thống phát hiện xâm nhập mạng

Hệ thống phát hiện xâm nhập (IDS) có khả năng theo dõi, phân tích và đánh giá những hoạt động diễn ra trên mạng, sau khi phát hiện hành vi khả nghi sẽ lập tức truyền tín hiệu thông báo đến người quản trị.

* + - 1. VPN (Virtual Private Network)

[VPN](https://vi.wikipedia.org/wiki/M%E1%BA%A1ng_ri%C3%AAng_%E1%BA%A3o) là mạng riêng ảo dùng để kết nối các máy tính một cách an toàn và bảo mật tới [hệ thống mạng](https://vi.wikipedia.org/wiki/H%E1%BB%87_th%E1%BB%91ng_m%E1%BA%A1ng) của doanh nghiệp thông qua [Internet](https://vi.wikipedia.org/wiki/Internet).

* + - 1. Giám sát và phân tích mã độc

Giám xác và phân tích mã độc giúp xác định các loại [mã độc](https://vi.wikipedia.org/wiki/Ph%E1%BA%A7n_m%E1%BB%81m_%C3%A1c_%C3%BD" \o "Phần mềm ác ý) đang hiện hữu trên hệ thống hoặc mã độc được gửi đến doanh nghiệp thông qua các [thư rác](https://vi.wikipedia.org/wiki/Th%C6%B0_r%C3%A1c" \o "Thư rác). Từ đó, doanh nghiệp có thể cô lập và ngăn chặn những liên kết có chứa [mã độc](https://vi.wikipedia.org/wiki/Ph%E1%BA%A7n_m%E1%BB%81m_%C3%A1c_%C3%BD" \o "Phần mềm ác ý) xâm hại hệ thống doanh nghiệp.

* + - 1. Xây dựng các chính sách cần thiết

Các cuộc tấn công mạng xuất hiện chủ yếu là do ý thức và sự thiếu hiểu biết của người dùng khi truy cập vào các trang không chính thống hoặc tải những phần mềm không rõ nguồn gốc. Biện pháp cần thiết nhất là phải tuyên truyền, ra những chính sách hợp lý để ngăn người dùng không tiết lộ các thông tin nội bộ và nâng cao cảnh giác đối với những thông tin lừa đảo

* + 1. Các giao thức bảo mật mạng
       1. Giao thức mạng SNMP

SNMP là viết tắt của từ Simple Network Monitoring Protocol (tiếng Việt gọi là Giao thức giám sát mạng đơn giản). Nó là một giao thức để truyền thông tin quản lý trong mạng, đặc biệt là sử dụng trong mạng LAN, tùy thuộc vào phiên bản đã chọn. Tính hữu ích của nó trong quản trị mạng đến từ thực tế là nó cho phép thu thập thông tin về các thiết bị kết nối mạng theo cách chuẩn hóa trên nhiều loại phần cứng và phần mềm.

Hầu như không có quản trị viên mạng nào từ bỏ SNMP. Thay vào đó, hầu hết họ đều tin tưởng vào nó vì gần như tất cả các loại thiết bị từ nhiều nhà sản xuất khác nhau đều hỗ trợ SNMP, giúp họ giám sát toàn diện nhờ công nghệ SNMP.

* + - 1. Giao thức xác thực AAA

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. Nó cung cấp việc xác thực (authentication) người dùng nhằm bảo đảm có thể nhận dạng đúng người dùng, đúng họ và tên nhân viên, đúng phòng ban. Một khi đã nhận dạng người dùng, ta có thể giới hạn phân quyền (authorization) mà người dùng có thể tương tác vào hệ thống. Khi người dùng sử dụng mạng, ta cũng có thể giám sát tất cả những gì mà họ làm. AAA với ba thành phần xác thực (authentication), phân 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.

* Xác thực người dùng (Authentication user):

Xác thực dùng để định danh, nhận dạng (identify user) 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 hoặc external database. Tất nhiên, tùy thuộc vào giao thức mà AAA hỗ trợ mã hóa đến đâu, ít nhất thì cũng mã hóa username và password. Xác thực sẽ xác định người dùng là ai.

Ví dụ: Người dùng có username và mật khẩu trong hệ thống, sẽ là hợp lệ và được xác thực thành công với hệ thống. 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 phân quyền mà người dùng được phép làm trong hệ thống.

* Phân quyền người dùng (Authorization user)

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. Ví dụ: 1 người dùng là nhân viên thuộc phòng nhân sự, truy cập vào hệ thống, sẽ được phân quyền theo chúc năng của phòng nhân sự, người dùng là khách của công ty, sẽ được phân quyền tối thiểu để truy cập internet, không truy cập vào tài nguyên hệ thống được. Những thuộc tính này được so sánh với thông tin chứa trong cơ sở dữ liệu của người dùng đó và kết quả được AAA trả về để xác định khả năng cũng như giới hạn thực tế của người 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.

* Tính cước người dùng (Accounting user):

Accounting 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.

Ví dụ: thống kê cho thấy người dùng đã truy cập vào web server với số lượng bao nhiêu lần, thời gian truy cập vào server là bao lâu. Điểm chính trong Accounting đó là cho phép người quản trị giám sát tích cực và dự đoán được dịch vụ và việc sử dụng tài nguyên. Thông tin này có thể được dùng để thời gian truy cập của khách hàng, quản lý mạng, kiểm toán trong các chính sách bảo mật của công ty.

* + - 1. Giao thức RADIUS

Remote Authentication Dial-In User Service (RADIUS) là một [giao thức](https://vi.wikipedia.org/wiki/Giao_th%E1%BB%A9c_truy%E1%BB%81n_th%C3%B4ng" \o "Giao thức truyền thông) mạng, hoạt động trên cổng mặc định là [UDP](https://vi.wikipedia.org/wiki/UDP) 1812  cung cấp quản lý xác thực tập trung (Authentication), phân quyền (Authorization) và tính cước (Accounting) (AAA) cho người dùng kết nối và sử dụng dịch vụ mạng. RADIUS được Livingston Enterprises, Inc. phát triển vào năm 1991 dưới dạng giao thức tính cước và xác thực truy cập, sau đó được đưa vào các tiêu chuẩn của [Internet Engineering Task Force](https://vi.wikipedia.org/wiki/Internet_Engineering_Task_Force) (IETF).

RADIUS rất phổ biến, được sử dụng rộng rãi, nó thường được các [nhà cung cấp dịch vụ Internet](https://vi.wikipedia.org/wiki/Nh%C3%A0_cung_c%E1%BA%A5p_d%E1%BB%8Bch_v%E1%BB%A5_Internet" \o "Nhà cung cấp dịch vụ Internet) (ISP) và doanh nghiệp sử dụng để quản lý truy cập [Internet](https://vi.wikipedia.org/wiki/Internet) hoặc [mạng](https://vi.wikipedia.org/wiki/M%E1%BA%A1ng_m%C3%A1y_t%C3%ADnh) nội bộ, [mạng không dây](https://vi.wikipedia.org/wiki/M%E1%BA%A1ng_kh%C3%B4ng_d%C3%A2y) và dịch vụ email tích hợp. Các mạng này có thể kết hợp [modem](https://vi.wikipedia.org/wiki/Modem), [đường dây thuê bao kỹ thuật số](https://vi.wikipedia.org/wiki/DSL" \o "DSL) ([DSL](https://vi.wikipedia.org/wiki/DSL)), [điểm truy cập](https://vi.wikipedia.org/wiki/%C4%90i%E1%BB%83m_truy_c%E1%BA%ADp_kh%C3%B4ng_d%C3%A2y" \o "Điểm truy cập không dây), [mạng riêng ảo](https://vi.wikipedia.org/wiki/M%E1%BA%A1ng_ri%C3%AAng_%E1%BA%A3o) (VPN), cổng mạng, [máy chủ web](https://vi.wikipedia.org/wiki/M%C3%A1y_ch%E1%BB%A7_web" \o "Máy chủ web), v.v.

RADIUS là giao thức [máy khách / máy chủ](https://vi.wikipedia.org/wiki/Client-server" \o "Client-server) chạy trên [lớp ứng dụng](https://vi.wikipedia.org/wiki/T%E1%BA%A7ng_%E1%BB%A9ng_d%E1%BB%A5ng" \o "Tầng ứng dụng) (Application Layer) và có thể sử dụng [TCP](https://vi.wikipedia.org/wiki/TCP) hoặc [UDP](https://vi.wikipedia.org/wiki/UDP) làm [phương thức vận chuyển](https://vi.wikipedia.org/wiki/T%E1%BA%A7ng_giao_v%E1%BA%ADn" \o "Tầng giao vận). RADIUS thường là lựa chọn đầu cuối cho xác thực 802.1X

CHƯƠNG 3 – MÔ HÌNH DEMO

* 1. Mô hình luận lý

A picture containing diagram

Description automatically generated

* 1. Mô hình vật lý

A picture containing text, computer

Description automatically generated

* + 1. Bảng địa chỉ

|  |  |  |
| --- | --- | --- |
| **Device** | **Interface** | **IP Address** |
| R1 | Se0/1/0 | 192.168.0.2/24 |
| G0.0.1 | 10.6.0.254 |
| G0/0/1.10 | 192.168.10.1/24 |
| G0/0/1.20 | 192.168.20.1/24 |
| G0/0/1.30 | 192.168.30.1/24 |
| G0/0/1.40 | 192.168.40.1/24 |
| G0/0/1.100 | 192.168.100.1/24 |
| R0 | G0/0/0 | 203.0.113.1/24 |
| G0/0/1 | 10.10.200.1/24 |
| Store Router | Internet | DHCP |
| LAN | 192.168.5.254/24 |
| RADIUS Server | F0 | 10.6.0.254 |
| Web Server | F0 | 203.0.113.5/24 |
| DNS Server | F0 | 203.0.113.10/24 |
| S0 | G0/1 | Trunk |
| F0/1-5 |
| G0/2 | VLAN 100 |
| WLC | Management | 192.168.100.254/24 |
| S1 | F0/1-2 | Trunk |
| F0/3 | VLAN 10 |
| F0/4 | Trunk |
| S2 | F0/1-2 | Trunk |
| F0/3 | VLAN 20 |
| F0/4 | Trunk |
| S3 | F0/1-2 | Trunk |
| F0/3 | VLAN 30 |
| F0/4 | Trunk |
| S4 | F0/1-2 | Trunk |
| F0/3 | VLAN 40 |
| F0/4 | Trunk |
| LAP-1 | G0 | DHCP |
| LAP-2 | G0 | DHCP |
| LAP-3 | G0 | DHCP |
| LAP-4 | G0 | DHCP |
| Management-1 | F0 | DHCP |
| Management-2 | F0 | DHCP |
| Management-3 | F0 | DHCP |
| Management-4 | F0 | DHCP |
| Thu Ngan | F0 | DHCP |
| User1 - User8 | Wireless | DHCP |

* + 1. Thông tin VLAN

|  |  |  |
| --- | --- | --- |
| **ID** | **Name** | **IP Address** |
| 10 | MARKETING | 192.168.10.0/24 |
| 20 | NHANSU | 192.168.20.0/24 |
| 30 | KETOAN | 192.168.30.0/24 |
| 40 | QUANLY | 192.168.40.0/24 |
| 100 | WLAN-Manage | 192.168.100.0/24 |

* + 1. Thông tin WLAN

|  |  |  |
| --- | --- | --- |
| **SSID** | **Username** | **Password** |
| marketing | marketing | 123 |
| nhansu | nhansu | 123 |
| ketoan | ketoan | 123 |
| quanly | quanly | 123 |
| Trung Nguyen Coffee | ---- | trungnguyen |

* 1. Cấu hình thiết bị

*Để đẩy nhanh quá trình cấu hình, những thao tác dưới đây dùng 2 Laptop tên là IT Management và IT Management 2 và 1 PC tên Admin PC. Bạn có thể thấy nó trong phần End Device và chọn Laptop-PT. Nối dây Console vào cổng RS 232 của Laptop tới cổng Console trên thiết bị cần cấu hình. Còn PC thì đã được cấu hình sẵn*

* + 1. Cấu hình Router R1
       1. Thiết lập bảo mật cho Router R1
* Mật khẩu console

A screenshot of a computer

Description automatically generated

* Mật khẩu enable

Graphical user interface, application

Description automatically generated

* Mã hoá mật khẩu console và enable

Graphical user interface, application

Description automatically generated

* Thiết lập chống trôi dòng lệnh và tự động đăng xuất sau 2 phút (120 giây)

Graphical user interface, text, application

Description automatically generated

* Phân giải tên miền

Graphical user interface, text, application

Description automatically generated

* + - 1. Cấp phát địa chỉ IP động (DHCP)

Graphical user interface, text

Description automatically generated

* + - 1. Cấu hình xác thực trên R1
* Cấu hình xác thực bằng username và password

Graphical user interface, text

Description automatically generated

* Phân quyền xác thực
  + Tạo cơ chế xác thực aaa với tên là TrungNguyenLocal

Graphical user interface

Description automatically generated

* + Áp dụng cơ chế xác thực aaa

Graphical user interface, text, application

Description automatically generated

* + Phân quyền đối với mật khẩu

Graphical user interface, text, application, chat or text message

Description automatically generated

Text

Description automatically generated

* + - 1. Cấu hình giới hạn đăng nhập

Cho phép user đăng nhập 3 lần trong 60 giây. Nếu đăng nhập sai quá 3 lần thì phải đợi 60 giây

Graphical user interface, text, application

Description automatically generated

* + 1. Sao lưu dữ liệu hệ thống lên Server
* Lưu hệ điều hành của Router R0 lên TFTP và FTP Server
  + TFTP

Text

Description automatically generated

* + FTP

Text

Description automatically generated

* Chép hệ điều hành từ TFTP và FTP Server vào flash của Router
  + TFTP

Graphical user interface, text

Description automatically generated

* + FTP

Text

Description automatically generated

* Lưu cấu hình của thiết bị lên TFTP và FTP Server
  + TFTP

Text

Description automatically generated

* + FTP

Graphical user interface, text

Description automatically generated

* Chép cấu hình vào thiết bị từ TFTP và FTP Server
  + TFTP

Text

Description automatically generated

* + FTP

Text

Description automatically generated

* + 1. Cấu hình WLC
       1. Tạo giao diện VLAN mới

Mỗi mạng WLAN yêu cầu một giao diện ảo trên WLC. Các giao diện này được gọi là giao diện động. Giao diện ảo được gán một ID VLAN và lưu lượng truy cập sử dụng giao diện này sẽ được gắn thẻ là lưu lượng truy cập VLAN. Đây là lý do tại sao kết nối giữa các AP, WLC và bộ định tuyến qua cổng trunk. Để lưu lượng từ nhiều mạng WLAN được vận chuyển qua mạng, lưu lượng cho các VLAN mạng WLAN phải được trunk.

1. Mở trình duyệt từ màn hình của IT Management 2. Kết nối với địa chỉ IP của WLC thông qua HTTPS.

Graphical user interface, text, application

Description automatically generated

1. Nhập User name **admin** và Password **Admin123**. Sau đó chọn Login

Graphical user interface, text, application

Description automatically generated

1. Nhấp vào Controller và sau đó nhấp vào Interfaces từ menu bên trái. Bạn sẽ thấy giao diện ảo mặc định và giao diện quản lý mà bạn được kết nối

A screenshot of a computer

Description automatically generated

1. Nhấp vào nút **New** ở góc trên bên phải của trang.

A screenshot of a computer

Description automatically generated

1. Nhập tên của giao diện mới. Chúng tôi sẽ gọi nó là **WLAN-10**. Định cấu hình ID VLAN là **10**. Đây là VLAN sẽ mang lưu lượng truy cập cho mạng WLAN mà chúng ta tạo sau này. Nhấp vào **Apply**. Điều này dẫn đến màn hình cấu hình cho giao diện VLAN.

Graphical user interface

Description automatically generated

1. Cấu hình như sau
   * Port Number: 1
   * IP Address: 192.168.10.254
   * Netmask: 255.255.255.0
   * Gateway: 192.168.10.1
   * Primary DHCP server: 192.168.10.1

Graphical user interface, text, application

Description automatically generated

1. Hãy đảm bảo rằng đã nhấn vào Apply để thực hiện các thay đổi của bạn và nhấp vào OK nếu xuất hiện thông điệp cảnh báo. Nhấp vào Save Configuration để cấu hình của bạn sẽ có hiệu lực khi WLC khởi động lại.

Graphical user interface, text, application

Description automatically generated

1. Làm tương tự các bước trên với 3 WLAN còn lại

Graphical user interface

Description automatically generated

* + - 1. Cấu hình WLC sử dụng máy chủ RADIUS

WPA2-Enterprise sử dụng máy chủ RADIUS bên ngoài để xác thực người dùng WLAN. Các tài khoản người dùng cá nhân với tên người dùng và mật khẩu duy nhất có thể được định cấu hình trên máy chủ RADIUS. Trước khi WLC có thể sử dụng các dịch vụ của máy chủ RADIUS, WLC phải được định cấu hình với địa chỉ máy chủ.

* 1. Chọn menu **Security** và chọn **New** để tạo máy chủ RADIUS

Graphical user interface, text, application, email

Description automatically generated

* 1. Nhập địa chỉ RADIUS Server vào **Server IP Address**. Máy chủ RADIUS sẽ xác thực WLC trước khi cho phép WLC truy cập thông tin tài khoản người dùng trên máy chủ. Điều này yêu cầu một giá trị shared secret. Sử dụng **admin**. Xác nhận shared secret và nhấn **Apply**.

Graphical user interface, text, application, email

Description automatically generated

* + - 1. Tạo WLAN mới

1. Nhấp vào mục nhập **WLANs** trong thanh menu. Tìm hộp thả xuống ở góc trên bên phải của màn hình mạng WLAN. Nó sẽ thông báo **Create New**. Nhấp vào **Go** để tạo một mạng WLAN mới.

Graphical user interface, website

Description automatically generated

1. Nhập **profile name** của mạng WLAN mới. Sử dụng profile name là **Nhan Su**. Gán một SSID của **Ban Nhan Su** cho mạng WLAN. Thay đổi ID thả xuống 2. Máy chủ sẽ cần sử dụng SSID này để tham gia mạng. Khi bạn hoàn tất, hãy nhấp vào **Apply** để chấp nhận cài đặt của bạn. Lưu ý: ID là một giá trị tùy ý được sử dụng làm nhãn cho mạng WLAN. Trong trường hợp này, chúng tôi đã định cấu hình nó là 2 để phù hợp với VLAN 20 cho mạng WLAN. Nó có thể là bất kỳ giá trị có sẵn nào.

Graphical user interface, website

Description automatically generated

1. Bây giờ mạng WLAN đã được tạo, bạn có thể cấu hình các tính năng của mạng. Nhấp vào **Enabled** để làm cho mạng WLAN hoạt động. Việc vô tình bỏ qua bước này là một sai lầm phổ biến

Graphical user interface, application

Description automatically generated

1. Chọn giao diện VLAN sẽ được sử dụng cho mạng WLAN mới. WLC sẽ sử dụng giao diện này cho lưu lượng người dùng trên mạng. Nhấp vào hộp thả xuống của **Interface/Interface Group (G)**. Chọn WLAN-20 mà chúng tôi đã tạo ở Bước 1.

Graphical user interface, text, application, email

Description automatically generated

1. Chuyển đến tab **Advanced**. Di chuyển đến phần **FlexConnect** của giao diện. Nhấp để bật **FlexConnect Local Switching** và **FlexConnect Local Auth.** Cuối cùng, nhấn vào **Apply** để kích hoạt WLAN

Graphical user interface, text, application, email

Description automatically generated

1. Làm tương tự với 3 WLAN còn lại ta được danh sách như sau:

Graphical user interface, website

Description automatically generated

* + - 1. Cấu hình bảo mật WLAN

Thay vì WPA2-PSK, chúng tôi sẽ định cấu hình WLAN mới để sử dụng WPA2-Enterprise.

1. Bấm vào ID WLAN của mạng WLAN mới tạo để tiếp tục định cấu hình nó, nếu cần.
2. Nhấp vào tab Security. Trong tab Layer 2, chọn WPA + WPA2 từ hộp thả xuống.

Graphical user interface

Description automatically generated

1. Trong WPA+WPA2 Parameters, hãy bật WPA2 Policy. Nhấp vào 802.1X trong **Authentication Key Management**. Điều này yêu cầu WLC sử dụng giao thức 802.1X để xác thực người dùng bên ngoài.

Graphical user interface, application

Description automatically generated

1. Nhấp vào tab **AAA Servers**. Mở menu thả xuống bên cạnh **Server 1** trong cột **Authentication Servers** và chọn máy chủ mà chúng tôi đã định cấu hình ở Bước 2. Cuối cùng, nhấn vào **Apply** để áp dụng cài đặt

Graphical user interface

Description automatically generated

* + - 1. Cấu hình DHCP cho Light Weight Access Point

WLC cung cấp máy chủ DHCP nội bộ của riêng mình. Cisco khuyến nghị rằng máy chủ WLAN DHCP không được sử dụng cho các dịch vụ DHCP khối lượng lớn, chẳng hạn như các dịch vụ WLAN của người dùng lớn hơn yêu cầu.

Tuy nhiên, trong các mạng nhỏ hơn, máy chủ DHCP có thể được sử dụng để cung cấp địa chỉ IP cho các LAP được kết nối với mạng quản lý có dây. Trong bước này, chúng tôi sẽ cấu hình phạm vi DHCP trên WLC và sử dụng nó để giải quyết các LAP.

1. Bấm vào menu **Controller** rồi bấm vào **Interfaces**.

A screenshot of a computer

Description automatically generated

1. Chọn management và ghi chú lại các thông tin địa chỉ của nó
2. Chúng tôi muốn WLC sử dụng máy chủ DHCP của riêng nó để cung cấp địa chỉ cho các thiết bị trên mạng quản lý không dây, chẳng hạn như các AP nhẹ. Vì lý do này, hãy nhập địa chỉ IP của WLC management làm địa chỉ **primary DHCP server**. Kéo màn hình lên trên và nhấn vào **Apply**. Nhấp chuột **OK** để xác nhận bất kỳ thông báo cảnh báo nào xuất hiện.

Graphical user interface, application

Description automatically generated

1. Trong menu bên trái, mở rộng phần **Internal DHCP Server** và nhấn vào **DHCP Scope.** Sau đó nhấn **New...** để tạo phạm vi DHCP

Graphical user interface, website

Description automatically generated

1. Đặt tên là **Wired Management**. Bạn sẽ định cấu hình phạm vi DHCP này để cung cấp địa chỉ cho mạng cơ sở hạ tầng. Sau đó, nhấn **Apply** để tạo

Graphical user interface, text

Description automatically generated

1. Bấm vào phạm vi mới trong bảng Phạm vi DHCP để định cấu hình thông tin địa chỉ cho phạm vi. Nhập thông tin sau.

* Pool Start Address: 192.168.100.240
* Pool End Address: 192.168.100.249
* Status: Enabled
* Cung cấp các giá trị cho Network, Netmask, và Default Routers từ thông tin bạn thu thập được ở đầu.

Graphical user interface, website

Description automatically generated

1. Nhấp vào **Apply** để kích hoạt cấu hình. Nhấp vào **Save Configuration** ở góc trên bên phải của giao diện WLC để lưu công việc của bạn để nó khả dụng khi WLC khởi động lại. Máy chủ DHCP nội bộ bây giờ sẽ cung cấp địa chỉ cho LAP-1 sau một khoảng thời gian ngắn. Khi các LAP có địa chỉ IP, đường hầm CAPWAP sẽ được thiết lập và các LAP sẽ có thể cung cấp quyền truy cập vào các mạng WLAN. Nếu bạn di chuyển chuột qua LAP trong cấu trúc liên kết, bạn sẽ thấy địa chỉ IP của nó, trạng thái của đường hầm CAPWAP và mạng WLAN mà các LAP đang cung cấp quyền truy cập

Graphical user interface, website

Description automatically generated

* + - 1. Cấu hình SNMP

1. Nhấp vào menu **Management** trong WLC GUI và mở rộng mục nhập cho **SNMP** trong menu bên trái. Chọn **Trap Receivers** và chọn **New...**

Graphical user interface, text, application, email

Description automatically generated

1. Nhập Community Name là **TrungNguyen\_SNMP** và địa chỉ IP của máy chủ là **192.168.1.4**. Sau đó, nhấn **Apply** để áp dụng cài đặt

Graphical user interface, email, website

Description automatically generated

* + 1. Cấu hình Store Router
       1. Kết nối tới Store Router
* Trong tab Desktop của Thu Ngan chọn Web Browser.
* Nhập địa chỉ 192.168.5.254 trên thanh url để mở web cấu hình của router không dây
* Nhập **admin** vào username và password. Sau đó nhấn **OK**

Graphical user interface

Description automatically generated

* Dưới tiêu đề **Setup**, trong trang **Basic Setup**, ở phần **Network Setup**. Cấu hình theo thông tin sau:
  + IP Address: 192.168.5.254
  + Subnet Mask: 255.255.255.0
  + Start IP Address: 192.168.5.2
  + Static DNS 1: 203.0.113.10

Graphical user interface, application

Description automatically generated

* Cuối cùng, kéo trang xuống và chọn **Save Setting** để lưu cấu hình. Lưu ý: Nếu bạn nhận được thông báo Request Timeout, hãy đóng cửa sổ Admin và đợi màu cam tròn biến thành hình tam giác màu xanh lá cây. Nhấp vào nút tua nhanh để làm cho việc này diễn ra nhanh hơn.

Graphical user interface

Description automatically generated with medium confidence

* + - 1. Cấu hình bảo mật wifi
* Cấu hình SSID của Store Router

1. Chuyển sang Wireless > Basic Wireless Settings.
2. Đổi tên mạng (SSID) thành Trung Nguyen Coffee chỉ cho **2.4GHz**.
3. Đổi Standard Channel sang 6 - 2.437GHz.
4. Đối với hoạt động này, hãy tắt cả hai tần số 5 GHz. Giữ nguyên phần còn lại của cài đặt.
5. Cuộn xuống cuối cửa sổ và chọn **Save Setting**

Graphical user interface

Description automatically generated

* Cấu hình bảo mật mạng

Trong bước này, bạn sẽ cấu hình cài đặt bảo mật không dây bằng chế độ bảo mật WPA2 với mã hóa và cụm mật khẩu.

1. Chuyển tới Wireless > Wireless Security.
2. Dưới tiêu đề 2.4GHz chọn WPA2 Personal đối với phần **Security Mode**.
3. Ở phần **Encryption**, giữ lại cài đặt mặc định AES
4. Ở phần **Passphrase**, nhập trungnguyen để làm mật khẩu
5. Chọn **Save Setting**
6. Xác nhận tất cả cài đặt trong Basic Wireless Settings và Wireless Security đều chính xác và được lưu

Graphical user interface, application

Description automatically generated

* + - 1. Cấu hình bảo mật Store Router
* Thay đổi mật khẩu đăng nhập

1. Chuyển tới Administration > Management ở thanh tiêu đề và thay đổi mật khẩu ở phần Router Password thành **Admin123**
2. Nhập lại mật khẩu ở phần Re-enter to confirm
3. Kéo xuống dưới cùng màn hình và chọn Save Settings
4. Dùng tài khoản là admin với mật khẩu mới thay đổi là Admin123 khi được nhắc đăng nhập vào mạng không dây bộ định tuyến. Nhấn OK để tiếp tục.
5. Chọn Continue và di chuyển đến bước tiếp theo

Graphical user interface, application

Description automatically generated

Graphical user interface, text

Description automatically generated

Graphical user interface

Description automatically generated

* + 1. Cấu hình R0
       1. Cấu hình định tuyến tĩnh

Để có thể kết nối được các server bên ngoài, bạn phải cấu hình định tuyến tĩnh

Graphical user interface, application

Description automatically generated

* 1. Kết quả chạy chương trình
     1. Bảo mật và DHCP trên R1

Graphical user interface, text

Description automatically generated

* + 1. Sử dụng cơ chế xác thực aaa và mã hoá mật khẩu

Text

Description automatically generated

Graphical user interface, text

Description automatically generated

* + 1. Phân quyền tài khoản

Graphical user interface, text, application

Description automatically generated

* + 1. Thông tin WLAN trên WLC

Graphical user interface, application

Description automatically generated

* + 1. Giao diện VLAN trên WLC

Graphical user interface

Description automatically generated with medium confidence

* + 1. Thông tin Server dùng để xác thực

Graphical user interface

Description automatically generated

* + 1. Thông tin SNMP

Graphical user interface, application

Description automatically generated

* + 1. Thông tin các LAP đã được nhận bởi WLC

A screenshot of a computer

Description automatically generated

* + 1. Thông tin backup trên Server

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface

Description automatically generated

* + 1. Kết nối đến web server

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

* + 1. Cấp phát IP động

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

* + 1. Ping từ nội bộ ra ngoài và server

Graphical user interface, text

Description automatically generated

CHƯƠNG 4 – KẾT LUẬN

* Những kết quả đạt được khi hoàn thành

Nhìn chung, mô hình hệ thống mạng của em đã được hoàn thành. Toàn bộ hệ thống đều được xây dựng và thiết kế trên nền tảng Cisco Packet Tracer. Các thiết bị đều có thể hoạt động bình thường và thực hiện được các yêu cầu cơ bản như: các máy ping được lẫn nhau, kết nối được tới web server, phân giải tên miền, upload/download file từ Server và cấp phát IP động,.... Ngoài những thứ cơ bản ra, những thứ nâng cao về về bảo mật cũng được hoàn thành như: bảo mật trên Router, áp dụng cơ chế xác thực trên RADIUS Server, bảo mật wifi,...

* Những khó khăn, hạn chế trong mô hình

Khó khăn: Do là thiết kế cả 1 hệ thống mạng lớn nên chỉ cần “sai 1 li là đi 1 dặm”. Những khó khăn ban đầu xuất hiện như thiết bị không thể kết nối đến các LAP, không nhận được DHCP, không kết nối ra bên ngoài, lỗi cấu hình,... Có những lỗi lớn liên quan đến thiết bị thì phải cấu hình lại trên thiết bị mới hoặc nghiêm trọng hơn là phải thay mới toàn bộ hệ thống. Qua những lần thay mới toàn bộ hệ thống và đúc kết kinh nghiệm qua các mô hình trước thì em đã cho ra được 1 mô hình hệ thống hoàn thiện như trên.

Hạn chế: Mô hình hệ thống mạng do được xây dựng trên giả lập nên khó tránh khỏi việc không đáp ứng đủ các thiết bị cần thiết hoặc chưa hỗ trợ các tính năng

**TÀI LIỆU THAM KHẢO**

|  |  |
| --- | --- |
| [1] | "wikipedia," 30 12 2021. [Online]. Available: https://vi.wikipedia.org/wiki/B%E1%BA%A3o\_m%E1%BA%ADt\_m%E1%BA%A1ng. |
| [2] | "vietsunshine," 30 12 2021. [Online]. Available: https://www.vietsunshine.com.vn/2021/04/28/kiem-soat-truy-cap-mang-nac-bao-mat-mang-va-iot/. |
| [3] | "securitybox," 30 12 2021. [Online]. Available: https://securitybox.vn/3126/top-6-hinh-thuc-tan-cong-mang-pho-bien-nhat/. |
| [4] | "licensesoft," 30 12 2021. [Online]. Available: https://licensesoft.vn/snmp-la-gi.htm. |
| [5] | "dienmayxanh," 30 12 2021. [Online]. Available: https://www.dienmayxanh.com/kinh-nghiem-hay/wifi-la-gi-596329. |
| [6] | "vnpro," 30 12 2021. [Online]. Available: https://vnpro.vn/thu-vien/giao-thuc-chung-thuc-va-phan-quyen-truy-cap-mang-aaa-3141.html. |
| [7] | "youtube," 30 12 2021. [Online]. Available: https://www.youtube.com/watch?v=iDHR78QSnus. |
| [8] | "youtube," 30 12 2021. [Online]. Available: https://www.youtube.com/watch?v=RaRdteeIu4U. |
| [9] | H. Science/Lavoisier, Wireless and Mobile Network Security, United States: Great Britain, 2009. |