TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM

**TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

**KHOA CÔNG NGHỆ THÔNG TIN**



**BÁO CÁO CUỐI KỲ MÔN HỌC**

**WIRELESS AND MOBILE NETWORK SECURITY**

**Xây Dựng Hệ Thống Mạng Không Dây Và Thực Hiện Bảo Mật Cho Công ty Viễn thông Mobifone**

*Người hướng dẫn*: **THẦY BÙI QUY ANH**

*Người thực hiện*: **NGUYỄN MINH TÂN – 51900830**

**NGUYỄN HOÀNG MINH KHÔI – 51900809**

**NGUYỄN PHÚC DUY KHANG – 51900801**

Lớp **: 19050402**

Khoá  **: 23**

**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 KỲ MÔN HỌC**

**WIRELESS AND MOBILE NETWORK SECURITY**

**Xây Dựng Hệ Thống Mạng Không Dây Và Thực Hiện Bảo Mật Cho Công ty Viễn thông Mobifone**

Người hướng dẫn: **THẦY BÙI QUY ANH**

Người thực hiện: **NGUYỄN MINH TÂN**

**NGUYỄN HOÀNG MINH KHÔI**

**NGUYỄN PHÚC DUY KHANG**

Lớp **: 19050402**

Khoá  **: 23**

**THÀNH PHỐ HỒ CHÍ MINH, NĂM 2021**

LỜI CẢM ƠN

Chúng em xin chân thành cảm ơn thầy Bùi Quy Anh đã dạy cho chúng em nhiều kiến thức quan trọng và kinh nghiệm làm bài báo cáo này. Vì đây là môn học quan trọng liên quan dến chuyên ngành cũng như liên quan đến công việc sau này nên nhờ sự giảng dạy và hỗ trợ nhiệt tình của thầy đã giúp nhóm em hoàn thành tốt môn học.

Chúng em cũng xin cảm ơn nhà trường đã hỗ trợ chúng em điều kiện tốt đề hoàn thành môn học mặc dù hiện giờ tình hình dịch bệnh vẫn đang căng thẳng.

Chúng em xin kính chúc thầy có nhiều sức khỏe và thành công hơn trong công việc của mình.

**ĐỒ ÁN ĐƯỢC HOÀN THÀNH**

**TẠI TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

Chúng em xin cam đoan đây là sản phẩm đồ án của riêng chúng em và được sự hướng dẫn của Thầy 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 chúng em 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 Minh Tân*

*Nguyễn Hoàng Minh Khôi*

*Nguyễn Phúc Duy Khang*

PHẦN XÁC NHẬN VÀ ĐÁNH GIÁ CỦA GIẢNG VIÊN

**Phần xác nhận của GV hướng dẫn**

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

Tp. Hồ Chí Minh, ngày tháng năm

(kí và ghi họ tên)

**Phần đánh giá của GV chấm bài**

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

Tp. Hồ Chí Minh, ngày tháng năm

(kí và ghi họ tên)

TÓM TẮT

Trong cuộc cách mạng công nghiệp 4.0, mạng Internet đóng một vai trò rất quan trọng và mạng không dây cũng nằm trong đó. Sự ra đời của mạng không dây đã khắc phục các hạn chế tồn đọng của mạng có dây và hiện đang dần thay thế cho mạng có dây. Tuy nhiên mạng có dây vẫn có một vài ưu điểm mà mạng không dây vẫn không thể làm được. Cho nên việc kết hợp giữa mạng có dây và mạng không dây sẽ mang đến một giải pháp tối ưu cho các công ty, tập đoàn,...

Dựa trên chuẩn IEEE 802.11 mạng không dây được áp dụng cho nhiều lĩnh vực như: sản xuất, thương mại, chăm sóc sức khỏe và được sử dụng nhiều ở các trường đại học. Hiện nay, mạng WLAN đang được đón nhận rộng rãi như một kết nối đa năng từ các doanh nghiệp.

Do vậy, chúng em đã chọn để tài “Xây dựng hệ thống mạng không dây và thực hiện bảo mật cho Công ty Viễn thông Mobifone”. Nhằm giúp mọi người hiểu rõ hơn về mạng không dây và cụ thể hơn là mạng WLAN và các vấn đề liên quan đến mạng WLAN. Ngoài ra chúng em còn thực hiện việc tạo ra mạng WLAN mới và sử dụng các chuẩn bảo mật WPA2 Personal và WPA2 Enterprise để bảo mật cho mạng không dây.

MỤC LỤC

[LỜI CẢM ƠN i](#_Toc91965998)

[PHẦN XÁC NHẬN VÀ ĐÁNH GIÁ CỦA GIẢNG VIÊN iii](#_Toc91965999)

[TÓM TẮT iv](#_Toc91966000)

[MỤC LỤC 1](#_Toc91966001)

[DANH MỤC KÍ HIỆU VÀ CHỮ VIẾT TẮT 5](#_Toc91966002)

[DANH MỤC CÁC BẢNG BIỂU, HÌNH VẼ, ĐỒ THỊ 7](#_Toc91966003)

[I. MÔ TẢ ĐỀ TÀI 11](#_Toc91966004)

[1.1. Yêu cầu của khách hàng 11](#_Toc91966005)

[1.2. Đề xuất hướng giải quyết 12](#_Toc91966006)

[II. CƠ SỞ LÝ THUYẾT 15](#_Toc91966007)

[2.1. Các khái niệm cơ bản 15](#_Toc91966008)

[2.1.1. Khái niệm mạng máy tính 15](#_Toc91966009)

[2.1.2. Khái niệm mạng WiFi 15](#_Toc91966010)

[2.1.3. Khái niệm VLAN 16](#_Toc91966011)

[2.1.4. Khái niệm Định tuyến động OSPF 16](#_Toc91966012)

[2.1.5. Khái niệm DHCP 17](#_Toc91966013)

[2.2. Mạng không dây 18](#_Toc91966014)

[2.2.1. Khái niệm 18](#_Toc91966015)

[2.2.2. Phân loại mạng không dây 19](#_Toc91966016)

[2.3. Mạng WLAN 19](#_Toc91966017)

[2.3.1. Giới thiệu về mạng WLAN 19](#_Toc91966018)

[2.3.2. Khái niệm 23](#_Toc91966019)

[2.3.3. Nguyên lý hoạt động của mạng WLAN 24](#_Toc91966020)

[2.3.4. Các chuẩn phổ biến của mạng WLAN 25](#_Toc91966021)

[2.3.5. Ưu điểm và nhược điểm của mạng WLAN 26](#_Toc91966022)

[2.3.6. Ứng dụng của mạng WLAN 27](#_Toc91966023)

[2.3.7. Các thiết bị cơ bản được sử dụng trong mạng WLAN 30](#_Toc91966024)

[2.4. Thiết lập Dịch vụ 802.11 cho mạng WLAN 32](#_Toc91966025)

[2.4.1. IBSS 33](#_Toc91966026)

[2.4.2. Chế độ cơ sở hạ tầng 34](#_Toc91966027)

[2.4.3. Chế độ AP 40](#_Toc91966028)

[2.5. Bảo mật mạng WLAN 44](#_Toc91966029)

[2.5.1. Khái niệm 44](#_Toc91966030)

[2.5.2. Một số hình thức tấn công qua mạng không dây thường gặp 44](#_Toc91966031)

[2.5.3. Một số giải pháp để đề phòng các cuộc tấn công mạng 46](#_Toc91966032)

[2.5.4. Các phương pháp để bảo mật mạng WLAN để ngăn ngừa các truy cập trái phép 47](#_Toc91966033)

[2.5.5. Các biện pháp để bảo mật mạng WLAN cho từng đối tượng 50](#_Toc91966034)

[2.6. Các thiết bị mạng khác: 51](#_Toc91966035)

[2.6.1. Bộ định tuyến(Router) 51](#_Toc91966036)

[2.6.2. Switch 51](#_Toc91966037)

[2.6.3. Switch layer 3 51](#_Toc91966038)

[2.6.4. WLC (Wireless LAN Controller) 52](#_Toc91966039)

[III. MÔ HÌNH DEMO 53](#_Toc91966040)

[3.1. Mô hình đề xuất 53](#_Toc91966041)

[3.1.1. Mô hình 53](#_Toc91966042)

[3.1.2. Bảng địa chỉ IP 57](#_Toc91966043)

[3.1.3. Bảng thông tin kết nối port trong hệ thống 60](#_Toc91966044)

[3.1.4. Bảng thiết kế thông tin vlan 63](#_Toc91966045)

[3.1.5. Bảng thông tin 63](#_Toc91966046)

[3.2. Cấu hình trên các thiết bị 64](#_Toc91966047)

[3.2.1. Máy chủ web 64](#_Toc91966048)

[3.2.2. Máy chủ DNS 65](#_Toc91966049)

[3.2.3. Máy chủ mail 66](#_Toc91966050)

[3.2.4. RADIUS Server 67](#_Toc91966051)

[3.2.5. Router ISP 68](#_Toc91966052)

[3.2.6. Cấu hình Cloud 70](#_Toc91966053)

[3.2.7. Cấu hình router Mobifone 70](#_Toc91966054)

[3.2.8. MLS 72](#_Toc91966055)

[3.2.9. Switch tầng 1 79](#_Toc91966056)

[3.2.10. Switch Tầng 2 80](#_Toc91966057)

[3.2.11. Switch Tầng 3 82](#_Toc91966058)

[3.2.12. Cấu hình WRTang1 83](#_Toc91966059)

[3.2.13. Cấu hình WLC tầng 2 85](#_Toc91966060)

[3.2.14. Cấu hình AP Tầng 2 KV1 95](#_Toc91966061)

[3.2.15. Cấu hình AP Tầng 2 KV2 96](#_Toc91966062)

[3.2.16. Cấu hình WLC Tầng 3 96](#_Toc91966063)

[3.2.17. Cấu hình cho Access Point Tang 3 Personal và Access Point Tang 3 Enterprise 99](#_Toc91966064)

[3.3. Kết quả chạy chương trình 99](#_Toc91966065)

[3.3.1. PCTang1 99](#_Toc91966066)

[3.3.2. LaptopTang1 100](#_Toc91966067)

[3.3.3. LaptopTang1KD 101](#_Toc91966068)

[3.3.4. TabletTang1KD 102](#_Toc91966069)

[3.3.5. SmartphoneTang1KD 104](#_Toc91966070)

[3.3.6. LaptopTang2\_KV1 105](#_Toc91966071)

[3.3.7. LaptopTang2\_KV2 106](#_Toc91966072)

[3.3.8. LaptopTang3\_Per 107](#_Toc91966073)

[3.3.9. LaptopTang3\_Ent 108](#_Toc91966074)

[IV. Kết luận 109](#_Toc91966075)

[TÀI LIỆU THAM KHẢO 110](#_Toc91966076)

[Tiếng Việt 110](#_Toc91966077)

[Tiếng Anh 110](#_Toc91966078)

DANH MỤC KÍ HIỆU VÀ CHỮ VIẾT TẮT

**CÁC KÝ HIỆU**

Mbps: Megabit trên giây

m: mét

**CÁC CHỮ VIẾT TẮT**

DSL: Digital Subcriber Line (Đường thuê bao số)

SSID: Service Set Identifier (Tên chính của mạng WLAN)

CAPWAP: Control And Provisioning of Wireless Access Points (Kiểm soát và cung cấp các điểm truy cập không dây)

WLC: Wireless LAN Controller (Bộ kiểm soát mạng WLAN)

AP: Access Point (Điểm truy cập mạng)

ADSL: Asymmetric Digital Subscriber Line (đường dây thuê bao số bất đối xứng)

IBSS: Independent Basic Service Set (mạng ad-hoc)

BSS: Base Station Subsystem (Hệ thống trạm gốc)

BSSID: Basic Service Set Identifier (Dịch vụ cơ bản thiết lập định danh)

MAC: Media Access Control (Địa chỉ MAC)

WEP: Wired Equivalent Privacy (chuẩn bảo mật cơ bản nhất của mạng không dây)

TKIP: Temporal Key Integrity Protocol (giao thức mã hóa cũ được giới thiệu với WPA để thay thế mã hóa WEP rất không an toàn vào thời điểm đó.)

MIC: Message Integrity Check (đảm bảo cho dữ liệu không bị giả mạo)

WPA: Wireless Application Protocol (chuẩn bảo mật mạng không dây)

DANH MỤC CÁC BẢNG BIỂU, HÌNH VẼ, ĐỒ THỊ

**DANH MỤC HÌNH**

[Hình 2.1. Mạng máy tính 15](#_Toc91966079)

[Hình 2.2. 20](#_Toc91966080)

[Hình 2.3. 21](#_Toc91966081)

[Hình 2.4. 22](#_Toc91966082)

[Hình 2.5. 22](#_Toc91966083)

[Hình 2.6. AP 31](#_Toc91966084)

[Hình 2.7. Router AP 31](#_Toc91966085)

[Hình 2.8. Card mạng không dây 32](#_Toc91966086)

[Hinh 2.9. Bridge không dây 32](#_Toc91966087)

[Hình 2.10. IBSS 34](#_Toc91966088)

[Hình 2.11. BSS 34](#_Toc91966089)

[Hình 2.12. BSS(tt) 35](#_Toc91966090)

[Hình 2.13. BSS(tt) 36](#_Toc91966091)

[Hình 2.14. DS 37](#_Toc91966092)

[Hình 2.15. DS(tt) 37](#_Toc91966093)

[Hình 2.16. ESS 39](#_Toc91966094)

[Hình 2.17. MBSS 40](#_Toc91966095)

[Hình 2.18. Bộ lặp 41](#_Toc91966096)

[Hình 2.19. Cầu nối dành cho Làm việc nhóm 42](#_Toc91966097)

[Hình 2.20. Cầu nối dành cho Ngoài trời 43](#_Toc91966098)

[Hình 2.21. Cầu nối dành cho Ngoài trời(tt) 44](#_Toc91966099)

[Hình 3.1.1. Mô hình luận lý tổng quát 53](#_Toc91966100)

[Hình 3.1.2. Chi tiết mô hình luận lý Internet ISP 54](#_Toc91966101)

[Hình 3.1.3. Mô hình luận lý Modem, Router Mobifone và MLSMobifone 54](#_Toc91966102)

[Hình 3.1.4. Chi tiết mô hình luận lý tầng 1 55](#_Toc91966103)

[Hình 3.1.5. Chi tiết mô hình luận lý tầng 2 55](#_Toc91966104)

[Hình 3.1.6. Chi tiết mô hình luận lý tầng 3 55](#_Toc91966105)

[Hình 3.1.7. Mô hình vật lý tổng quát 56](#_Toc91966106)

[Hình 3.1.8. Chi tiết mô hình vật lý tầng 1 56](#_Toc91966107)

[Hình 3.1.9. Chi tiết mô hình vật lý tầng 2 56](#_Toc91966108)

[Hình 3.1.10. Chi tiết mô hình vật lý tầng 3 57](#_Toc91966109)

[Hình 3.1.11. Chi tiết phòng Server 57](#_Toc91966110)

[Hình 3.2.1. Cấu hình máy chủ web 65](#_Toc91966111)

[Hình 3.2.2. Cấu hình dịch vụ web 65](#_Toc91966112)

[Hình 3.2.3. Cấu hình máy chủ DNS 66](#_Toc91966113)

[Hình 3.2.4. Cấu hình dịch vụ DNS 66](#_Toc91966114)

[Hình 3.2.5. Cấu hình cho máy chủ mail 67](#_Toc91966115)

[Hình 3.2.6. Thêm tên người dùng vào máy chủ mail 67](#_Toc91966116)

[Hình 3.2.8. Cấu hình dịch vụ cho RADIUS Server 68](#_Toc91966117)

[Hình 3.2.9. Cấu hình cho cloud 70](#_Toc91966118)

[Hình 3.2.10. Cấu hình cơ bản cho WRTang1 84](#_Toc91966119)

[Hình 3.2.11. Cấu hình SSID cho WRTang1 84](#_Toc91966120)

[Hình 3.2.12. Đặt mật khẩu cho cho WRTang1 85](#_Toc91966121)

[Hình 3.2.13. Cấu hình địa chỉ cho WLC Tang 2 85](#_Toc91966122)

[Hình 3.2.14. Cấu hình địa chỉ cho Laptop1 86](#_Toc91966123)

[Hình 3.2.15. Trang đăng ký cho WLC Tang 2 87](#_Toc91966124)

[Hình 3.2.17. Trang đăng ký tên mạng và mật khẩu cho WLC Tang 2 88](#_Toc91966125)

[Hình 3.2.18. Trang nhập địa chỉ IP ảo cho WLC Tang 2 88](#_Toc91966126)

[Hình 3.2.19. Kết quả đăng ký cho WLC Tang 2 89](#_Toc91966127)

[Hình 3.2.20. Kết quả đăng ký cho WLC Tang 2 (tiếp theo) 89](#_Toc91966128)

[Hình 3.2.21. Trang đăng nhập của WLC Tang 2. 90](#_Toc91966129)

[Hình 3.2.22. Tạo thêm mạng WLAN cho WLC Tang 2 91](#_Toc91966130)

[Hình 3.2.23. Chọn Enabled và nhấn vào nút Apply để lưu lại 91](#_Toc91966131)

[Hình 3.2.24. Tạo AP group mới cho WLC Tang 2 92](#_Toc91966132)

[Hình 3.2.25. Kết quả tạo AP groups cho WLC Tang 2 93](#_Toc91966133)

[Hình 3.2.26. Thêm mạng WLANTang2 vào nhóm WLANTang2KV1 93](#_Toc91966134)

[Hình 3.2.27. Thêm AP Access Point Tang 2 KV1 vào nhóm WLANTang2KV1 94](#_Toc91966135)

[Hình 3.2.28. Thêm mạng WLANTang2KV2 vào nhóm WLANTang2KV2 94](#_Toc91966136)

[Hình 3.2.30. Gắn power adapter cho Access Point Tang 2 KV1. 96](#_Toc91966137)

[Hình 3.2.31. Cấu hình địa chỉ cho Access Point Tang 2 KV1. 96](#_Toc91966138)

[Hình 3.2.32. Cấu hình WPA2 Enterprise 97](#_Toc91966139)

[Hình 3.2.33. Cấu hình WPA2 Enterprise (tiếp theo) 97](#_Toc91966140)

[Hình 3.2.34. Cấu hình WPA2 Enterprise (tiếp theo) 98](#_Toc91966141)

[Hình 3.2.35. Cấu hình WPA2 Enterprise (tiếp theo) 98](#_Toc91966142)

[Hình 3.2.36. Cấu hình WPA2 Enterprise (tiếp theo) 99](#_Toc91966143)

[Hình 3.3.1. PCTang1 kết nối đến trang web mobifone.com.vn 100](#_Toc91966144)

[Hình 3.3.2. PCTang1 gửi và nhận mail đến LaptopTang1 100](#_Toc91966145)

[Hình 3.3.3. LaptopTang1 kết nối đến trang web mobifone.com.vn 101](#_Toc91966146)

[Hình 3.3.4. LaptopTang1 gửi và nhận mail đến PCTang1 101](#_Toc91966147)

[Hình 3.3.5. LaptopTang1KD kết nối đến trang web mobifone.com.vn 102](#_Toc91966148)

[Hình 3.3.6. LaptopTang1KD gửi và nhận mail đến SmartphoneTang1KD và TabletTang1KD 102](#_Toc91966149)

[Hình 3.3.7. TabletTang1KD kết nối đến trang web mobifone.com.vn 103](#_Toc91966150)

[Hình 3.3.8. TabletTang1KD gửi và nhận mail đến SmartphoneTang1KD và LaptopTang1KD 103](#_Toc91966151)

[Hình 3.3.9. SmartphoneTang1KD kết nối đến trang web mobifone.com.vn 104](#_Toc91966152)

[Hình 3.3.8. SmartphoneTang1KD gửi và nhận mail đến TabletTang1KD và LaptopTang1KD 104](#_Toc91966153)

[Hình 3.3.9. LaptopTang2\_KV1 kết nối đến trang web mobifone.com.vn 105](#_Toc91966154)

[Hình 3.3.10. LaptopTang2\_KV1 gửi và nhận mail đến các thiết bị có kết nối vào điểm truy cập mạng 105](#_Toc91966155)

[Hình 3.3.11. LaptopTang2\_KV2 kết nối đến trang web mobifone.com.vn 106](#_Toc91966156)

[Hình 3.3.12. LaptopTang2\_KV2 gửi và nhận mail đến các thiết bị có kết nối vào điểm truy cập mạng 106](#_Toc91966157)

[Hình 3.3.11. LaptopTang3\_Per kết nối đến trang web mobifone.com.vn 107](#_Toc91966158)

[Hình 3.3.14. LaptopTang3\_Per gửi và nhận mail đến các thiết bị có kết nối vào điểm truy cập mạng 107](#_Toc91966159)

[Hình 3.3.15. LaptopTang3\_Per kết nối đến trang web mobifone.com.vn 108](#_Toc91966160)

[Hình 3.3.16. LaptopTang3\_Ent gửi và nhận mail đến các thiết bị có kết nối vào điểm truy cập mạng 108](#_Toc91966161)

**DANH MỤC BẢNG**

[Bảng 1.1. Số lượng và giá tiền của các thiết bị mạng 14](#_Toc91966162)

[Bảng 3.1.1. Bảng địa chỉ IP 60](#_Toc91966163)

[Bảng 3.1.2. Bảng thông tin kết nối cổng trong hệ thống 63](#_Toc91966164)

[Bảng 3.1.3. Bảng thông tin vlan trong hệ thống 63](#_Toc91966165)

[Bảng 3.1.4. Bảng thông tin trong hệ thống 64](#_Toc91966166)

1. MÔ TẢ ĐỀ TÀI
   1. Yêu cầu của khách hàng

Thiết kế và xây dựng hệ thống mạng không dây dành cho chi nhánh công ty Mobifone ở Vũng Tàu. Chi nhánh này có tòa nhà gồm có 5 tầng, diện tích tòa nhà là 300 mét vuông, Ở mỗi tầng sẽ có cùng 1 yêu cầu là tính bảo mật cao và có thể kết nối Internet ở bất kỳ vị trí nào ở mỗi tầng bên trong tòa nhà. Ngoài ra các thiết bị kết nối mạng có thể truy cập vào trang web của công ty là **mobifone.com.vn** và thực hiện việc gửi và nhận mail thông qua địa chỉ **@mobifone.com.** Tuy nhiên ở mỗi tầng sẽ có các yêu cầu khác nhau.

* Tầng 1: sẽ có các yêu cầu về mạng Wifi, mạng LAN, có tối đa 40 user kết nối vào mạng và sử dụng các thiết bị: switch, Wireless Router, Camera, Cửa thông minh. Tầng 1 sẽ có quầy Dịch vụ để sử dụng các máy tính hoặc laptop kết nối với mạng LAN. Phòng Bảo vệ sử dụng Camera, các thiết bị không dây và cửa thông minh, phòng khách sẽ cho phép khách hàng sử dụng mạng wifi.
* Tầng 2: sẽ có các yêu cầu về mạng WLAN có bảo mật WPA2 Personal, mạng LAN, có tối đa là 30 user sẽ kết nối với mạng và sẽ sử dụng các thiết bị switch, Access Point, Camera, WLC, Laptop, Cửa thông minh. Tầng 2 sẽ có phòng Nhân viên khu vực 1 sẽ sử dụng AP Tang 2 KV1, cửa thông minh và phòng Nhân viên khu vực 2 sử dụng AP Tang 2 KV2. Ngoài ra còn có Nhà kho có máy tính để quản lý.
* Tầng 3: sẽ có các yêu cầu về mạng WLAN có bảo mật WPA2 Personal và WPA2 Enterprise, có tối đa là 25 user sẽ kết nối với mạng và sẽ sử dụng các thiết bị switch, Access Point, Camera, WLC, Laptop, Cửa thông minh. Tầng 3 sẽ có phòng Quản lý NS sẽ sử dụng AP Tang 3 Enterprise, cửa thông minh, camera và phòng Giám đốc sử dụng AP Tang 3 Personal và cửa thông minh.
* Tầng 4 sẽ có yêu cầu giống như tầng 2.
* Tầng 5 sẽ có yêu cầu giống như tầng 5.

Chi phí mà chi nhánh dành cho việc thiết kế, xây dựng mạng là 300 triệu VND.

* 1. Đề xuất hướng giải quyết

Với các yêu cầu trên của khách hàng, chúng em sẽ thiết kế và xây dựng hệ thống mạng gồm 3 tầng và 1 phòng server có các dịch phụ cơ bản của công ty như truy cập vào trang web của công ty là mobifone.com.vn, gửi và nhận mail cũng như thiết kế có tính thông minh nhờ IoT Server. Khách hàng yêu có mạng không dây tộc đô cao cũng như kết nối được ở bất cứ đâu trong tòa nhà thì nhóm em sẽ đề xuất mạng WLAN kết hợp với mạng LAN đã có trước đây. Mạng WLAN sẽ cấu hình bảo mật WPA2 Personal và WPA2 Enterprise để đảm bảo độ bảo mật cao và tốc độ xử lý nhanh. Chúng em đã chọn ra các thiết bị sẽ cấu hình cho công ty và đây là bảng số lượng và giá tiền của các thiết bị.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **STT** | **Tên thiết bị** | **Giá** | **Số lượng** | **Tổng tiền** |
| 1 | **Wireless Controller 2500 CISCO AIR-CT2504-5-K9** | 22.423.500 | 4 | 89.692.000 |
| 2 | Unifi EdgeRouter X SFP | 1.892.000 | 2 | 3.785.000 |
| 3 | Router Wifi Tp-Link Archer | 1.129.000 | 1 | 1.129.000 |
| 4 | Wifi Access Point GWN7605 | 2.250.000 | 4 | 9.000.000 |
| 5 | Gigabit PoE TP-Link TL-SG1008MP | 2.000.000 | 7 | 14.000.000 |
| 6 | Máy chủ server pos – Mini PC Intel NUC N5095 | 6.850.000 | 5 | 34.250.000 |
| 7 | Camera IP Dome Hikvision ds-2cd2121g0-i | 1.350.000 | 3 | 4.050.000 |
| 8 | Dây cáp mạng CAT5e,24AWG,lõi đồng | 1,683,000 | 10 | 16.830.000 |
| 9 | Tiền công |  |  | 50.000.000 |
| **Tổng cộng:** 222.736.000 VND | | | | |

Bảng 1.1. Số lượng và giá tiền của các thiết bị mạng

1. CƠ SỞ LÝ THUYẾT
   1. Các khái niệm cơ bản
      1. Khái niệm mạng máy tính

**Mạng máy tính** là mạng viễn thông kỹ thuật số, nó cho phép các nút mạng chia sẻ tài nguyên. Trong mạng máy tính, các thiết bị máy tính trao đổi dữ liệu hoặc thông tin với nhau bằng các liên kết dữ liệu giữa các nút. Các liên kết dữ liệu này được thiết lập qua cáp mạng hoặc cáp quang hoặc các mạng không dây như Wi-Fi.

Các thiết bị trong mạng máy tính có nhiệm vụ khởi động, định tuyến và chấm dứt việc gửi hoặc nhận dữ liệu được gọi là các nút mạng. Các nút này thường được xác định bởi địa chỉ mạng và có thể bao gồm các host như: Laptop, Smartphone hoặc máy chủ.

Mạng máy tính hỗ trợ các ứng dụng và dịch vụ như truy cập vào World Wide Web, video và âm thanh kỹ thuật số, sử dụng dịch vụ mail, ứng dụng nhắn tin như Messenger, Zalo, Telegram,.. dịch vụ máy in và máy fax, dịch vụ lưu trữ đám mây như Google Drive, OneDrive, DropBox,... và nhiều ứng dụng và dịch vụ khác.

Mạng máy tính nổi tiếng nhất là Internet.



Hình 2.1. Mạng máy tính

* + 1. Khái niệm mạng WiFi

WiFi là viết tắt của **Wireless Fidelity** là hệ thống truy cập internet không dây. Loại sóng vô tuyến này tương tự như sóng điện thoại, truyền hình và radio. WiFi là công nghệ mạng cho phép bạn kết nối không dây với Internet.

Wifi là công cụ kết nối không thể thiếu trên điện thoại, laptop, máy tính bảng và một số thiết bị thông minh khác như smartwatch, smartTV.

* + 1. Khái niệm VLAN

VLAN là viết tắt của Virtual Local Area Network hay còn gọi là mạng LAN ảo. Một VLAN được định nghĩa là một nhóm logic các thiết bị mạng và được thiết lập dựa trên các yếu tố như chức năng, bộ phận, ứng dụng… của công ty. Về mặt kỹ thuật, VLAN là một miền quảng bá được tạo bởi các switch. Bình thường thì router đóng vai trò tạo ra miền quảng bá. Đối với VLAN, switch có thể tạo ra miền quảng bá.

Cấu hình vlan ở switch:

vlan số...

name nhập tên vlan

int range f0/5-24 (chọn port f0/5 đến 24)

switchport mode access

swichport access vlan số vlan

* + 1. Khái niệm Định tuyến động OSPF

Giao thức định tuyến OSPF là một giao thức định tuyến cho các mạng Giao thức Internet. Nó sử dụng thuật toán định tuyến trạng thái liên kết và nằm trong nhóm các giao thức cổng nội bộ, hoạt động trong một hệ thống tự trị duy nhất.

Nó sử dụng thuật toán Dijkstra, còn được gọi là thuật toán đường đi ngắn nhất.

Một mạng OSPF có thể được cấu trúc hoặc chia nhỏ thành các khu vực định tuyến để đơn giản hóa việc quản trị và tối ưu hóa lưu lượng và sử dụng tài nguyên. Các khu vực được xác định bằng các số 32 bit, được thể hiện đơn giản bằng số thập phân hoặc thường bằng ký hiệu dấu chấm-thập phân được sử dụng cho địa chỉ [IPv4](https://vi.wikipedia.org/wiki/IPv4). Theo quy ước, vùng 0 (không) hoặc 0.0.0.0, đại diện cho vùng lõi hoặc đường trục của mạng OSPF. Trong khi danh tính của các khu vực khác có thể được lựa chọn theo ý muốn; quản trị viên thường chọn địa chỉ [IP](https://vi.wikipedia.org/wiki/Internet_Protocol) của [bộ định tuyến](https://vi.wikipedia.org/wiki/B%E1%BB%99_%C4%91%E1%BB%8Bnh_tuy%E1%BA%BFn) chính trong một khu vực làm định danh khu vực.

Định tuyến OSPF được cấu hình như sau:

Router ospf 1

Network địa chỉ mạng 0.255.255.255 area 0

* + 1. Khái niệm DHCP

DHCP (Dynamic Host Configuration Protocol hay Giao thức cấu hình host động) là một giao thức được sử dụng để cung cấp quản lý nhanh chóng, tự động và tập trung cho việc phân phối [địa chỉ IP](https://quantrimang.com/dia-chi-ip-la-gi-143625) trong mạng. DHCP cũng được sử dụng để cấu hình đúng subnet mask, cổng mặc định và thông tin về [DNS server](https://quantrimang.com/top-10-public-dns-server-tot-nhat-ban-nen-biet-121278) trên thiết bị.

Cấu hình DHCP pool cho vlan:

ip dhcp excluded-address địa chỉ đầu địa chỉ cuối

ip dhcp pool vlan...

network địa chỉ mạng subnet mask

default-router địa chỉ default gateway

dns-server địa chỉ DNS

* 1. Mạng không dây
     1. Khái niệm

Mạng không dây là mạng máy tính mà ở đó nó sử dụng kết nối dữ liệu không dây giữa các nút mạng.

Kết nối mạng không dây là một phương pháp mà các hộ gia đình, mạng viễn thông và các cơ sở kinh doanh tránh lãng phí tiền bạc, công sức khi đưa dây cáp khắp tòa nhà hoặc ví dụ như một kết nối giữa các vị trí thiết bị khác nhau. Mạng viễn thông quản trị thường được thực hiện và quản lý bằng cách sử dụng liên lạc vô tuyến. Việc triển khai này diễn ra ở mức (lớp) vật lý của cấu trúc mạng mô hình OSI.

Ví dụ về mạng không dây bao gồm mạng điện thoại di động, mạng cục bộ không dây (WLAN), mạng cảm biến không dây, mạng truyền thông vệ tinh và mạng vi sóng ở mặt đất.

Mạng không dây thường được triển khai trong môi trường và điều kiện sau đây:

* Môi trường có địa hình phức tạp, khó khăn cho đi dây mạng được như núi, đồi, đảo,...
* Các tòa nhà, cơ quan, công ty mà không thể nối được dây mạng hoặc có người dùng thường xuyên di chuyển như: khách sạn, cửa hàng điện thoại, nhà hàng,..
* Những nơi phục vụ internet công cộng như: nhà ga, bệnh viện, sân bay, ngân hàng,...
  + 1. Phân loại mạng không dây

Dựa trên phạm vi phủ sóng, ta có thể phân loại mạng không dây thành các loại mạng sau đây:

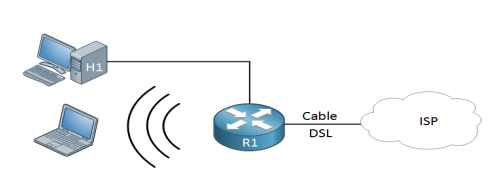
* Mạng WWAN (Wireless Wide Area Network) theo chuẩn 802.20
* Mạng WMAN (Wireless Metropolitan Area Network) theo chuẩn 802.16
* Mạng WLAN (Wireless Local Area Network) theo chuẩn 802.11
* Mạng WPAN (Wireless Personal Area Network) theo chuẩn 802.15
  1. Mạng WLAN
     1. Giới thiệu về mạng WLAN

Hiện nay, các thiết bị không dây có nhiều hơn các thiết bị có dây. Khoảng 10 năm trước về trước, khi mà hầu hết các văn phòng chỉ có máy tính để bàn và các thiết bị mạng khác như là máy in. Tất cả những thứ này đều được kết nối với dây điện. Hiện nay, rất nhiều người dùng có một cái máy tính xách tay, điện thoại thông minh và máy tính bảng. Đó là ba thiết bị không dây dành cho từng người dùng trong kỷ nguyên công nghệ. Tốc độ không dây đã tăng lên một cách đáng kể so với lúc trước, càng ngày tiến gần hơn đến tốc độ không dây Gigabit.

IEEE sử dụng chuẩn 802.11 cho tất cả các giao thức mà nó có liên quan đến chuẩn không dây. Hầu hết chúng ta trước đây đã từng được thấy hay được nghe về các chuẩn 802.11a, 802.11b, 802.11g, 802.11n và/ hoặc 802.11ac. Chúng ta cũng có Liên minh Wi-Fi mà ở đó nó giúp đỡ chúng ta trong việc quảng bá mạng không dây. Ví dụ, IEEE đã mô tả về tính xác thực và mã hóa trong chuẩn 802.11i của họ. Liên minh Wi-Fi có WEP, WPA, và WPA2 trên chuẩn này. Những cái tên này dễ dàng làm việc hơn khi mà nó đề cập đến 802.11i.

* **Mạng LAN Không dây SOHO (SOHO : Văn phòng nhỏ/ Văn phòng ở Nhà)**

Bộ định tuyến của bạn ở nhà có thể có các khả năng giống như một bộ định tuyến sau đây:

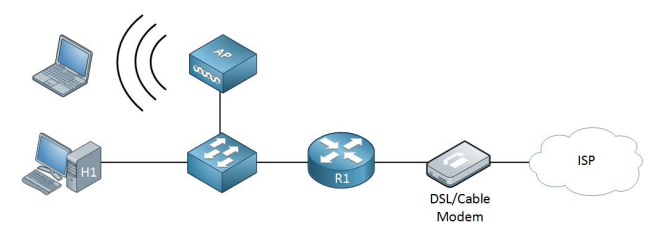


Hình 2.2.

Nó được kết nối đến ISP (Nhà cung cấp Dịch vụ Mạng) của bạn thông qua dây cáp hoặc DSL, hoặc cũng có lẽ là dây cáp quang. Nó có nhiều cổng Ethernet để kết nối máy tính của bạn và nó có ăn ten cho những người thích dùng mạng không dây. Trong thực tế, các thành phần này đều được xây dựng lại thành một thiết bị:

* Bộ Chuyển mạch Ethernet
* Điểm Truy cập Không dây
* (Cáp hoặc Modem DSL)
* Bộ định tuyến

Nếu bạn muốn tách mọi thứ ra, thì nó sẽ nhìn giống như thế này:



Hình 2.3.

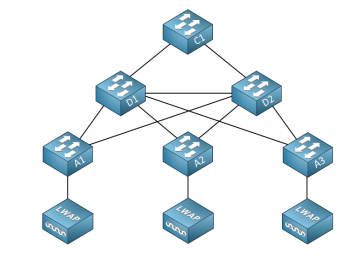
Trong một mạng nhỏ như thế này, Điểm truy cập tự làm mọi việc. Chúng ta gọi một điểm truy cập tự động này. Nó sử dụng giao thức 802.11 để giao tiếp với các máy khách không dây và sử dụng Ethernet ở phía mạng LAN.

* **Mạng LAN Không dây dành cho Doanh nghiệp**

Khi chúng ta nhìn vào các mạng Doanh nghiệp rộng lớn, một điểm truy cập thôi là sẽ không đủ. Tưởng tượng rằng một mạng với hàng trăm hoặc hàng ngàn người dùng. Khi bạn đi bộ xung quanh văn phòng, bạn không muốn mất kết nối mỗi khi điện thoại của bạn thay đổi từ điểm truy cập này sang điểm truy cập khác. Bạn muốn có một kết nối không dây ổn định, mỗi khi mà bạn đi. Chuyển đổi liền mạch từ một điểm truy cập này đến điểm truy cập khác được gọi là chuyển vùng.

Một điểm truy cập đơn cũng có băng thông giới hạn. Nếu bạn có một phòng họp mặt với 100 người dùng một điểm truy cập đơn có thể không cung cấp đủ băng thông cho mọi người.

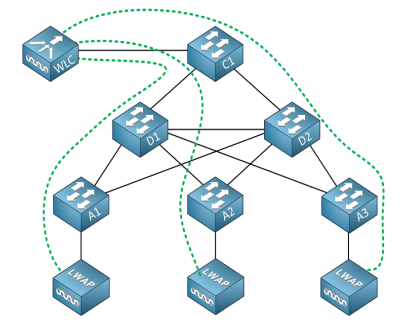
Khi mà chúng tôi sử dụng mạng không dây cho các người dùng của chúng tôi, nó phải gần với người dùng của chúng tôi. Đó là lý do tại sao bạn sẽ tìm thấy điểm truy cập trên lớp truy cập của mạng của bạn, giống như các máy tính và các máy in:



Hình 2.4.

Tuy nhiên vẫn còn có một vấn đề. Giả định bạn được kết nối đến một điểm truy cập và bạn bắt đầu đi bộ xung quanh văn phòng, điện thoại của bạn sẽ chuyển đến điểm truy cập khác. Làm thế nào để điểm truy cập thứ hai biết rằng bạn đã được xác thực vào mạng? Bạn có thể xác thực lại nhưng điều đó sẽ phá hủy kết nối của bạn ... không phải là một ý tưởng tốt.

Để giải quyết vấn đề này, chúng ta sẽ làm việc với bộ điều khiển mạng LAN không dây.



Hình 2.5.

Tất cả các công việc quản lý được di chuyển từ các điểm truy cập sang bộ điều khiển mạng LAN không dây. Nó đảm bảo việc xác thực, chuyển vùng, tạo ra mạng không dây mới,.... Các điểm truy cập chỉ chịu trách nhiệm cho việc chuyển tiếp lưu lượng, chúng tôi gọi là các LWAPs (Điểm Truy cập Khối lượng Nhẹ).

Để làm được điều này, tất cả lưu lượng phải được gửi từ các điểm truy cập đến bộ điều khiển mạng LAN không dây. Điều này được thực hiện bởi các đường hầm được gọi là CAPWAP (Trình Điều khiển và Cấp phép của các Điểm Truy cập Không dây). Các đường gạch chấm màu xanh lá cây là các đường hầm CAPWAP giữa các Điểm Truy cập và WLC.

Hiện tại, chúng ta có một mạng không dây lớn. Nếu bạn tạo ra một mạng không dây mới (SSID) thì nó sẽ được đẩy vào tất cả các điểm truy cập. Chuyển vùng cũng không thành vấn đề khi mà tất cả lưu lượng được chuyển tiếp đến WLC.

* + 1. Khái niệm

Mạng WLAN là mạng máy tính không dây mà ở đó nó liên kết hai hoặc nhiều thiết bị bằng cách sử dụng phương thức giao tiếp không dây để tạo thành mạng cục bộ (LAN) trong khu vực giới hạn diện tích như nhà riêng, trường học, cơ quan, công ty, xí nghiệp,... và nó đang dần thay thế cho kết nối có dây. Nó cung cấp cho người dùng kết nối Internet khi di chuyển xung quanh khu vực có kết nối mạng. Thông qua cổng mặc định, người dùng có thể kết nối đến Internet khắp nơi trên thế giới.

WLAN truyền tín hiệu trong bán kính khoảng vài trăm mét, và nó sử dụng băng tần 2,4 GHz hoặc 5 GHz.

Tùy vào chuẩn kết nối IEEE 802.11a/b/g/n/ac mà mạng WLAN sẽ có các phạm vi phủ sóng trong nhà hoặc ngoài trời khác nhau và nó sẽ có tốc độ khác nhau. Ví dụ với chuẩn 802.11a sẽ có tốc độ khoảng 2Mbps nhưng chuẩn 802.11.ac sẽ cung cấp tốc độ khoảng 866 Mbps.

* + 1. Nguyên lý hoạt động của mạng WLAN

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

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

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

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

* + 1. Các chuẩn phổ biến của mạng WLAN

Có các chuẩn phổ biến như sau:

* 802.11: Đây là tiêu chuẩn sơ khai nhất của mạng WLAN. Nó được ra mắt vào tháng 6 năm 1997. Nó sử dụng dải tần 2.4GHz và chỉ cung cấp tốc độ là 2Mbps. Phạm vi phát sóng trong nhà và ngoài trời của nó lần lượt là 20m và 100m. Hiện nay chuẩn này rất ít được sử dụng
* 802.11a: Tiêu chuẩn này được ra mắt vào tháng 9 năm 1999. Nó sử dụng dải tần 5Ghz giúp cho tốc độ nó tăng lên đến 54Mbps. Tuy nhiên phạm vi trong nhà và ngoài trời của nó lần lượt là 35m và 120m cho nên nó khá ngắn nếu so với chuẩn 802.11b. Tóm lại chuẩn này cung cấp tốc độ cao tuy nhiên phạm vi lại không xa lắm.
* 802.11b: Tiêu chuẩn này được ra mắt vào tháng 9 năm 1999 (cùng thời gian ra mắt so với chuẩn 802.11a). Nó sử dụng dải tần 2.4Ghz cho nên tốc độ của nó chỉ là 11Mbps. Tuy nhiên phạm vi trong nhà và ngoài trời của nó lần lượt là 38m và 140m cho nên nó sẽ xa hơn nếu so với chuẩn 802.11a. Tóm lại chuẩn này cung cấp tốc độ thấp tuy nhiên phạm vi lại xa hơn chuẩn a.
* 802.11g: Tiêu chuẩn này được ra mắt vào tháng 6 năm 2003. Nó là sự kết hợp giữa tốc độ cao của chuẩn 802.11a và phạm vi phủ sóng rộng của chuẩn 802.11b. Tốc độ của nó là 54Mbps và phạm vi trong nhà và ngoài trời lần lượt là 38m và 140m. Tuy nhiên giá của chuẩn này sẽ cao hơn 2 chuẩn trước.
* 802.11n: Tiêu chuẩn này được ra mắt vào tháng 10 năm 2009. Nó có 2 tần số và với mỗi tần số, tốc độ dữ liệu sẽ có khác biệt. Tuy nhiên, phạm vi phát sóng của 2 tần số này là như nhau (70m nếu ở trong nhà và 250m nếu ở ngoài trời). Với tần số 2.4GHz, nó sẽ cung cấp tốc độ là 72.2Mbps và 5Ghz là 150Mbps.
* 802.11ac: Tiêu chuẩn này được ra mắt vào tháng 12 năm 2012. Nó sử dụng dải tần 5GHz và nó cung cấp tốc độ khoảng 866Mbps.
  + 1. Ưu điểm và nhược điểm của mạng WLAN
* **Ưu điểm:**

Mạng không dây không sử dụng cáp để kết nối, chúng sử dụng sóng Radio. Ưu thế của mạng không dây là khả năng di động và sự tiện lợi cho người dùng khi họ không bị hạn chế về không gian và vị trí kết nối. Chỉ cần họ ở trong vùng phủ sóng của mạng WLAN. Mạng WLAN có các ưu điểm sau:

* Khả năng di động và sự tiện lợi khi cho phép người dùng kết nối không quan trọng là họ đang ở đâu, chỉ cần họ ở trong vùng phủ sóng.
* Không bị hạn chế về không gian và vị trí kết nối.
* Dễ lắp đặt và triển khai.
* Tiết kiệm thời gian, công sức, tiền bạc cho việc lắp đặt dây cáp mạng.
* Không ảnh hưởng đến thẩm mỹ của tòa nhà.
* Giảm chi phí bảo trì, bảo dưỡng hệ thống khi không cần phải thay dây cáp mạng nếu gặp sự cố vât lý.
* **Nhược điểm:**
* Dễ bị nhiễu sóng, mất sóng nếu đặt cục phát sóng không đúng vị trí

Mạng không dây rất dễ bị nhiễu do nó sử dụng sóng radio và rất dễ bị nhầm lẫn do lò vi sóng cũng sử dụng bước sóng có tần số giống mạng, vấn đề thứ hai là dễ mất sóng do tín hiệu không dây khó truyền qua các bề mặt bê tông,

* Dễ gặp các vấn đề liên quan đến bảo mật

Mạng không dây sẽ kém an toàn hơn nếu so với mạng có dây bởi vì bất kỳ thiết bị không dây nào cũng có thể cố gắng kết nối với mạng WLAN. Vì vậy nếu lo lắng về vấn đề bảo mật thì biện pháp duy nhất chỉ có thể là hạn chế truy cập vào mạng. Điều này thường được thực hiện bằng cách sử dụng xác thực không dây như WEP hoặc WPA, mã hóa thông tin liên lạc.

* Tốc độ không nhanh nếu so sánh với mạng có dây (cáp quang)
  + 1. Ứng dụng của mạng WLAN
* **Cung cấp khả năng truy cập mạng một cách dễ dàng, linh hoạt, thuận tiện.**

Cho phép người dùng có thể sử dụng các thiết bị truy cập mạng không dây như Smartphone, Laptop, Máy tính bảng,... để truy cập mạng tại mọi vị trí có phủ sóng WLAN.

* **Mở rộng mạng**

Cho phép mở rộng mạng tại các khu vực có vị trí đặc biệt, ví dụ: các khu vực không thể đi dây cáp, không được thay đổi kết cấu của tòa nhà, địa hình hiểm trở…v.v.

* **Kết nối mạng giữa các tòa nhà cách xa nhau**

Để kết nối mạng giữa các tòa nhà cách xa nhau, có thể kết nối bằng cáp (chôn dưới lòng đất, hoặc treo trên các cột trụ), giải pháp này rất tốn kém và khó thi công vì đường đi của cáp có thể liên quan tới nhiều thứ khác nhau; có giải pháp khác là thuê đường truyền riêng từ các công ty điện thoại, giải pháp này chi phí cao, do phải trả phí hàng tháng.

Giải pháp thứ 3 cho trường hợp này là sử dụng WLAN, bằng cách cài đặt cầu nối không dây (wireless bridge) tại mỗi tòa nhà. Có thể sử dụng mô hình kết nối điểm tới điểm (point – to – point) hoặc điểm tới đa điểm (point – to – multipoint).

* **Cung cấp dịch vụ truy cập mạng không dây**

Nhà cung cấp dịch vụ internet không dây (WISP – wireless internet service provider) là 1 nhà cung cấp dịch vụ internet dựa trên công nghệ không dây. Với người sử dụng ở những khu vực đặc biệt, việc triển khai lắp đặt đường dây kết nối internet khó khăn, chí phí cao, hoặc không thể thực hiện, thì giải pháp mạng không dây là lựa chọn tốt nhất cho họ.

WISP có thể hoàn toàn sử dụng công nghệ IEEE 802.11 hoặc WiMAX (IEEE 802.16) hoặc kết hợp giữa WiMAX và IEEE 802.11

* **Sử dụng cho văn phòng quy mô nhỏ (SOHO – small office/home office)**

Đối với các văn phòng có quy mô nhỏ, với khoảng 10 đến 15 máy tính, ví dụ: văn phòng luật sư, một trung tâm tư vấn xây dựng, cửa hàng in ấn,…v.v. có thể chỉ cần sử dụng 1 wireless router để thiết lập hệ thống mạng cho toàn văn phòng với chi phí thấp, triển khai nhanh.

Nếu sử dụng wireless router có kèm chức năng của 1 modem ADSL (ví dụ Linksys WRT54G) có thể cung cấp 2 dịch vụ cùng 1 lúc: kết nối các máy trong mạng nội bộ với nhau và cung cấp đường truy cập internet cho cả văn phòng.

* **Sử dụng trong tình huống cần thiết lập mạng trong thời gian ngắn**

Trong các tình huống đặc biệt, cần hệ thống mạng để làm việc trong thời gian ngắn, thiết lập đơn giản, nhanh chóng, ví dụ: văn phòng của công trường xây dựng, văn phòng điều hành khắc phục hậu quả trong vùng bị thiên tai …v.v. Mạng không dây là 1 lựa chọn tốt.

Có thể sử dụng thiết bị vừa có chứng năng của 1 access point vừa hỗ trợ kết nối WAN, giúp kết nối các máy tính nội bộ với nhau và kết nối internet, ví dụ dòng thiết bị SonicWALL.

* **Sử dụng trong trường học**

Với hệ thống WLAN các giáo viên có thể làm việc ở mọi vị trí, không bị bó buộc vào bàn làm việc cố định, giáo viên có thể khai thác các tài nguyên từ internet từ máy labtop mà không cần phải sử dụng đến cáp kết nối. Sinh viên có thể truy cập mạng internet và intranet để tham khảo các tài liệu, học tập, nộp bài và thực hiện kiểm tra qua mạng.

* **Sử dụng trong các nhà máy, nhà kho**

Với môi trường này, khi triển khai WLAN, chúng ta cần phải khảo sát kĩ, để tránh các vấn đề liên quan đến nhiễu sóng, mất tín hiệu do các thiết bị trong nhà kho hoặc nhà máy gây ra.

* **Sử dụng trong bệnh viện**

Sử dụng WLAN giúp các bác sĩ có thể nhanh chóng xác định được thông tin về các bệnh nhân cũng như các thông tin về y học thông qua kết nối mạng intranet và internet bằng các thiết bị truy cập WLAN. Vấn đề quan trọng hàng đầu trong hệ thống WLAN tại bệnh viện là phải đảm bảo thông tin được bảo mật do có thể sẽ hacker trà trộn vào để đánh cắp thông tin.

* **Cung cấp khả năng truy cập mạng ở nơi công cộng**

Ở nơi công cộng như quán cà phê, sân bay, bến xe, …có thể thiết lập các điểm phát sóng WLAN (gọi là các Wi-Fi hotspot) cho mọi người truy cập internet có thu phí hoặc miễn phí.

* + 1. Các thiết bị cơ bản được sử dụng trong mạng WLAN
* **Điểm truy cập mạng không dây(Access Point)**

Điểm truy cập mạng không dây AP (Access Point) tạo ra các vùng phủ sóng, nối các nút di động tới các cơ sở hạ tầng LAN. Các điểm truy cập này không chỉ cung cấp trao đổi thông tin với các mạng có dây mà còn lọc lưu lượng và thực hiện chức năng cầu nối với các tiêu chuẩn khác. Các điểm truy cập trao đổi với nhau qua mạng hữu tuyến để quản lí các nút di động.



Hình 2.6. AP

* **Router điểm truy cập**

Một “AP router” là một thiết bị kết hợp các chức năng của một Access Point và một router. Khi là Access Point, nó truyền dữ liệu giữa các trạm không dây và một mạng hữu tuyến cũng như là giữa các trạm không dây. Khi là router, nó hoạt động như là điểm liên kết giữa hai hay nhiều mạng độc lập, hoặc giữa một mạng bên trong và một mạng bên ngoài.



Hình 2.7. Router AP

* **Card mạng không dây**

Card mạng không dây giúp giao tiếp của máy tính với mạng không dây bằng cách điều chế tín hiệu dữ liệu với chuỗi trải phổ và thực hiện một giao thức truy nhập cảm ứng sóng mạng.



Hình 2.8. Card mạng không dây

* **Bridge không dây**

WBridge (Bridge không dây) tương tự như các điểm truy cập không dây trừ trường hợp chúng được sử dụng cho các kênh bên ngoài. WBridge được thiết kế để nối các mạng với nhau, đặc biệt trong các toà nhà có khoảng cách xa tới 32 km. WBridge có thể lọc lưu lượng và đảm bảo rằng các hệ thống mạng không dây được kết nối tốt mà không bị mất lưu lượng cần thiết.



Hinh 2.9. Bridge không dây

* 1. Thiết lập Dịch vụ 802.11 cho mạng WLAN

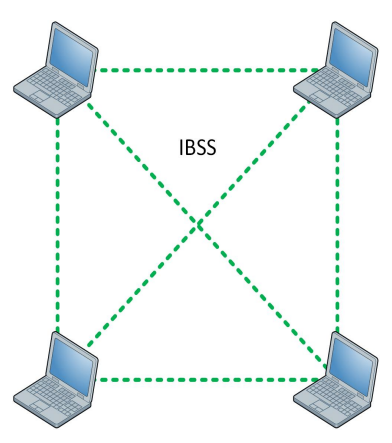
Giống như các mạng có dây, các mạng không dây có những cấu trúc liên kết vật lý và logic khác nhau. Tiêu chuẩn 802.11 mô tả các bộ dịch vụ khác nhau. Một bộ dịch vụ mô tả làm thế nào để một nhóm các thiết bị không dây giao tiếp với nhau.

Từng bộ dịch vụ sử dụng Bộ định danh Dịch vụ Giống nhau (SSID). SSID là cái tên “thân quen” của mạng không dây. Nó là tên mạng không dây mà bạn nhìn thấy khi bạn nhìn vào các mạng không dây khả dụng trên thiết bị không dây của bạn.

* + 1. IBSS

Với một Bộ Dịch vụ Độc lập Cơ bản (IBSS), hai hoặc nhiều thiết bị không dây kết nối trực tiếp mà không cần một điểm truy cập (AP). Chúng ta cũng gọi nó là một mạng ad hoc. Một trong các thiết bị phải bắt đầu và quảng cáo một SSID, việc này tương đồng với việc Điểm Truy cập sẽ làm những gì. Sau đó các thiết bị khác có thể kết nối vào mạng.

Một IBSS không phải là một giải pháp phổ biến. Bạn có thể sử dụng nó nếu bạn muốn chuyển các tập tin của bạn giữa hai hoặc nhiều máy tính xách tay, điện thoại thông minh, hoặc máy tính bảng mà không cần phải kết nối đến mạng không dây mà một Điểm Truy cập cung cấp.



Hình 2.10. IBSS

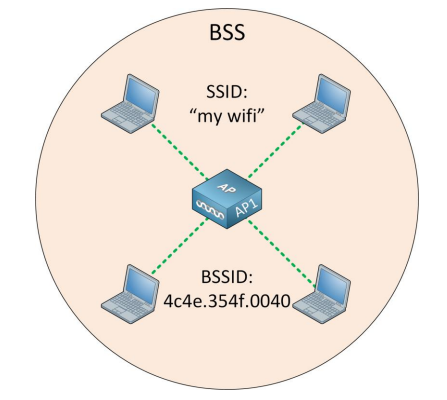
* + 1. Chế độ cơ sở hạ tầng

Với chế độ cơ sở hạ tầng, chúng tôi kết nối tất cả các thiết bị không dây đến một thiết bị trung tâm, Điểm Truy cập. Tất cả dữ liệu đi qua Điểm Truy cập. Tiêu chuẩn 802.11 mô tả các bộ dịch vụ khác nhau. Hãy cùng nhau tìm hiểu:

* **Bộ Dịch vụ Cơ bản (BSS)**

Với một Bộ Dịch vụ Cơ bản (BSS), các máy khách không dây kết nối vào một mạng không dây thông qua một Điểm Truy cập. Một BSS là những gì mà chúng ta sử dụng cho hầu hết các mạng không dây. Ý tưởng đằng sau một BSS là Điểm Truy cập mà ở đó nó đóng vai trò là mạng không dây.

Mỗi máy khách không dây quảng cáo các khả năng của nó đến Điểm Truy cập, và Điểm Truy cập cấp phép hoặc từ chối quyền tham gia vào mạng. BSS sử dụng một kênh đơn cho tất cả giao tiếp. Điểm Truy cập và các máy khách không dây của nó sử dụng cùng kênh để chuyển giao và nhận.

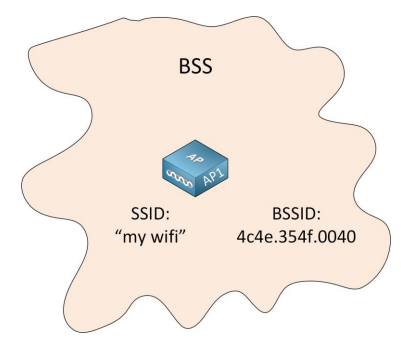


Hình 2.11. BSS

SSID là một cái tên “tốt” cho mạng không dây, và nó không phải là duy nhất.

Điểm Truy cập cũng quảng cáo Bộ Dịch vụ Định danh Cơ bản (BSSID). Đây là địa chỉ MAC của sóng AP, một địa chỉ duy nhất mà ở đó nó định danh cho Điểm Truy cập. Toàn bộ máy khách không dây phải kết nối đến Điểm Truy cập. Điều này có nghĩa là phạm vi tín hiệu của Điểm Truy cập xác định ra kích thước của BSS. Chúng tôi gọi nó là Khu vực Dịch vụ Cơ bản (BSA).

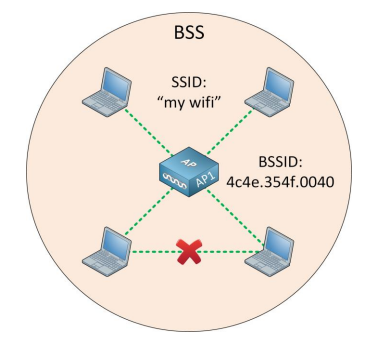
Trong hình phía trên, BSA là một vòng tròn tuyệt đẹp. Điều này có lẽ là trường hợp nếu bạn cài đặt Điểm Truy cập của bạn ở nơi nào đó ở giữa của một vùng trống mà không có gì xung quanh Điểm Truy cập. Trong một tòa nhà, BSA có thể giống như thế này nhiều hơn:



Hình 2.12. BSS(tt)

Khi một thiết bị không dây muốn tham gia vào BSS, nó gửi một yêu cầu liên kết đến Điểm Truy cập. Điểm Truy cập cho phép hoặc từ chối yêu cầu. Khi thiết bị không dây đã được tham gia vào BSS, chúng tôi gọi nó là một máy khách không dây hoặc trạm 802.11 (STA).

Tất cả lưu lượng từ một máy khách phải đi qua Điểm Truy cập thậm chí nếu điểm cuối của nó đến máy khách không dây khác.



Hình 2.13. BSS(tt)

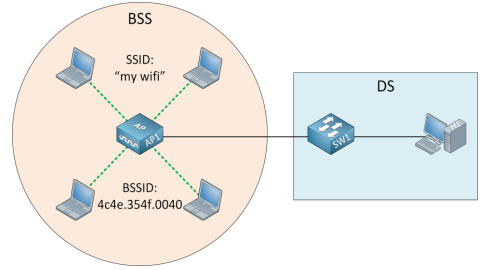
Mọi thứ phải đi qua Điểm Truy cập bởi vì Điểm Truy cập của chúng ta là điểm trung tâm của việc quản lý, và nó giới hạn kích thước của BSS. Phạm vi tín hiệu của Điểm Truy cập xác định ra ranh giới của BSS.

* **Hệ thống Phân phối (DS)**

Một BSS là một mạng đơn lẻ với một Điểm Truy cập đơn. Trong hình phía trên, không có kết nối với một mạng có dây.

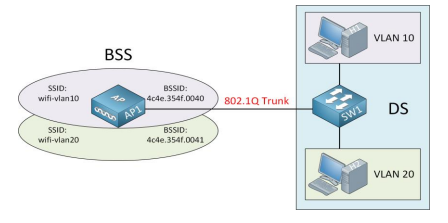
Hầu hết các mạng không dây, tuy nhiên, có một tiện ích của mạng có dây. Một Điểm Truy cập hỗ trợ cả hai loại kết nối: kết nối có dây và kết nối không dây. Tiêu chuẩn 802.11 gọi mạng có dây ngược luồng là hệ thống phân phối (DS).

Cầu nối điểm Truy cập kết nối các khung Ethernet Lớp 2 không dây và có dây, cho phép lưu thông di chuyển từ mạng có dây đến mạng không dây và ngược lại.



Hình 2.14. DS

Chúng ta cũng có thể làm điều này với các mạng VLAN. Điểm Truy cập kết nối thiết bị chuyển mạch mạng với một trunk 802.1Q. Mỗi SSID ánh xạ đến một VLAN khác nhau:



Hình 2.15. DS(tt)

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

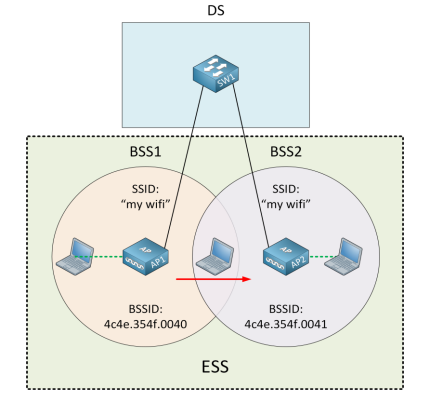
Mặc dù chúng ta có đa mạng không dây, tất cả chúng cùng sử dụng phần cứng nằm dưới, sóng radio, và các kênh. Nếu bạn có một Điểm Truy cập với đa sóng radio, thì nó có khả năng gán mạng không dây vào sóng radio khác. Ví dụ, bạn có thể sử dụng một mạng không dây trên sóng radio 2.4GHz và một mạng khác trên sóng 5 GHz.

* **Bộ Dịch vụ Mở rộng (ESS)**

Một BSS sử dụng một Điểm Truy cập đơn. Điều này có lẽ sẽ không đủ bởi vì hai lý do:

* Phủ sóng: Tín hiệu của một Điểm Truy cập đơn không thể bao phủ toàn bộ một tầng hoặc tòa nhà. Bạn cần nhiều Điểm Truy cập nếu bạn muốn sóng không dây ở khắp nơi.
* Băng thông: Một Điểm Truy cập sử dụng một kênh đơn, và không dây thì dùng chuẩn bán song công. Bạn có càng nhiều máy khách không dây hoạt động, thì thông lượng của bạn sẽ càng thấp. Điều này cũng phụ thuộc vào tốc độ dữ liệu mà bạn hỗ trợ. Một máy khách không dây trong cùng khu vực với BSA của bạn có lẽ vẫn có khả năng chạm tới Điểm Truy cập, nhưng chỉ có thể dùng tốc độ dữ liệu chậm. Một máy khách không dây mà ở gần với Điểm Truy cập có thể sử dụng tốc độ dữ liệu cao. Máy khách không dây ở xa sẽ nhận “thời gian phát sóng”, giảm băng thông cho các máy khách truy cập vào mạng.

Để tạo ra một mạng không dây rộng hơn, chúng ta sử dụng nhiều Điểm Truy cập và kết nối toàn bộ chúng vào mạng có dây. Các Điểm Truy cập làm việc cùng nhau để tạo ra một mạng không dây rộng mà ở đó nó mở rộng toàn bộ một tầng lầu hoặc tòa nhà. Người dùng chỉ nhìn thấy một SSID đơn, vì vậy sau đó, máy khách không dây nhìn thấy nhiều Điểm Truy cập, nó có thể kết nối đến. Chúng ta gọi cấu trúc liên kết này với nhiều Điểm Truy cập, là một Bộ Dịch vụ Mở rộng (ESS).



Hình 2.16. ESS

Các Điểm Truy cập làm việc cùng nhau. Ví dụ, nếu bạn liên kết với một Điểm Truy cập và bạn đi xung quanh tòa nhà, bạn sẽ không bị mất kết nối. Máy khách không dây sẽ tự động “nhảy” từ một Điểm Truy cập này sang Điểm Truy cập khác. Chúng tôi gọi đó là chuyển vùng. Để tận hưởng được trải nghiệm liền mạch, chúng ta cần một sự chồng chéo giữa các Điểm Truy cập.

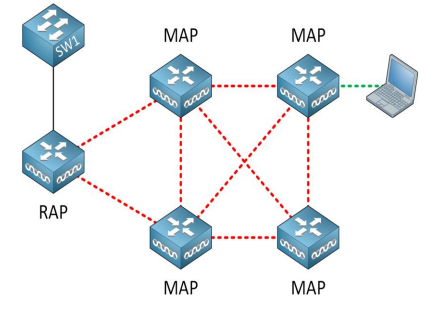
Mỗi Điểm Truy cập đề nghị BSS của chúng sử dụng một kênh khác để ngăn ngừa can thiệp giữa các Điểm Truy cập.

* **Bộ Dịch vụ Mesh Cơ bản (MBSS)**

Nếu bạn muốn cung cấp một mạng không dây cho một khu vực rộng lớn, như là một thành phố, thì nó không dễ để kết nối giữa các Điểm Truy cập thành một mạng có dây.

Thay vì đó, bạn có thể xây dựng một mạng lưới, cũng được biết như là một Bộ Dịch vụ Lưới Cơ bản (MBSS). Với một mạng lưới, chúng tôi làm cầu nối lưu lượng không dây từ một Điểm Truy cập này sang đến Điểm Truy cập khác. Các Điểm Truy cập Lưới thường có nhiều sóng radio. Một sóng radio dùng cho lưu lượng sửa chữa lại của mạng lưới giữa các Điểm Truy cập; sóng khác thì duy trì một BSS cho các máy khách không dây trên kênh khác.

Ít nhất một Điểm Truy cập được kết nối vào mạng có dây; chúng tôi gọi nó là Điểm Truy cập Gốc (RAP). Các Điểm Truy cập khác là các Điểm Truy cập Lưới (MAP) và chỉ được kết nối khi sửa lại không dây.



Hình 2.17. MBSS

Có nhiều đường dẫn cho một MAP để truy cập đến mạng có dây thông qua RAP, vì vậy chúng ta cần một giao thức mà ở đó nó tìm thấy đường dẫn không có vòng lặp tốt nhất. Tương đồng với việc làm thế nào mà cây mở rộng làm việc trong lớp 2 hoặc các giao thức định tuyến ở lớp 3, có các giải pháp không dây khác nhau. IEEE có tiêu chuẩn 802.11s cho các mạng lưới. Các bên cung cấp thỉnh thoảng cũng sử dụng các giải pháp độc quyền. Ví dụ, Cisco có Giao thức Đường dẫn Không dây Thích nghi (AWPP).

Các Điểm Truy cập Cisco hỗ trợ cả hai mạng trong nhà và ngoài trời.

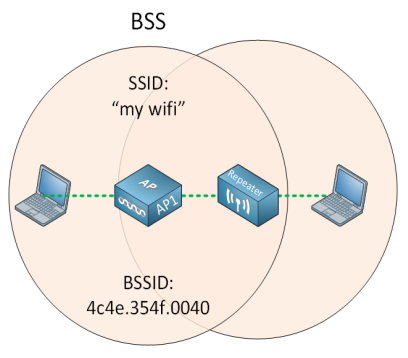
* + 1. Chế độ AP

Cho đến nay, chúng ta chỉ nói về các bộ dịch vụ. Một số Điểm Truy cập cũng hỗ trợ các chế độ không cấu trúc khác nhau. Tôi sẽ giải thích các chế độ Điểm Truy cập thông thường bên dưới.

* **Bộ lặp**

Nếu bạn cần bao phủ một khu vực rộng lớn với mạng không dây của bạn, bạn thường sử dụng ESS. Một ESS, tuy nhiên, yêu cầu các kết nối có dây. Nếu nó không có thể kết nối đến Điểm Truy cập của bạn với một dây, bạn có thể cấu hình một Điểm Truy cập trong chế độ bộ lặp.

Một bộ lặp không dây nhận một tín hiệu và chuyển giao lại nó. Điều này cho phép các thiết bị không dây mà ở đó nó không đủ gần Điểm Truy cập có thể tham gia vào mạng.



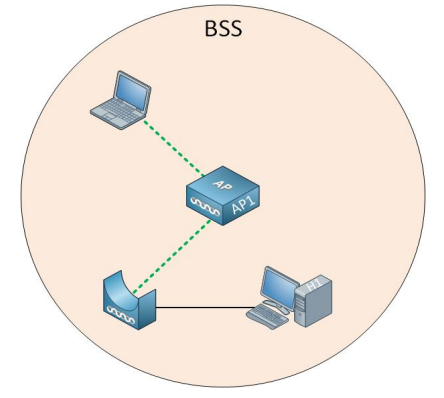
Hình 2.18. Bộ lặp

Nó bắt buộc phải chồng lên nhau giữa các ô kích thước của Điểm Truy cập và bộ lặp. Để có hiệu suất tối ưu, nó nên trong khoảng 50%. Nếu bộ lặp có một sóng radio đơn, thì nó sẽ nhận và truyền trên cùng tín hiệu với Điểm Truy cập. Trong trường hợp này, Điểm Truy cập cũng sẽ nhận được tín hiệu được chuyển lại. Khi mà không dây là bán song công, thêm một bộ lặp sẽ giảm thông lượng khả dụng của bạn khoảng 50%.

Để làm việc này xung quanh, nhiều bộ lặp có hai hoặc nhiều sóng radios. Chúng nhận một kênh (giống với Điểm Truy cập) và chuyển lại trên kênh khác.

* **Cầu nối dành cho Làm việc nhóm**

Sẽ như thế nào nếu bạn có một thiết bị có dây mà ở đó nó cần kết nối đến một thiết bị không dây nhưng không có một sóng radio? Ví dụ, các máy in cũ, các máy tính, hoặc các hệ thống điểm bán hàng (PoS). Trong trường hợp này, bạn có thể sử dụng một cầu nối làm việc nhóm (WGB). WGB có một kết nối có dây, bạn kết nối đến thiết bị có dây và một kết nối không dây, nó đóng vai trò như là một máy khách không dây của một BSS.



Hình 2.19. Cầu nối dành cho Làm việc nhóm

Có hai loại WGB:

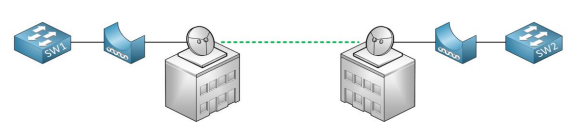
* Cầu nối làm việc nhóm chung (uWGB): WGB Chung chỉ hỗ trợ một máy khách có dây đơn. Điều này dựa trên tiêu chuẩn 802.11.
* Cầu nối Làm việc nhóm (WGB): WGB (hoặc Chế độ Cầu nối Làm việc nhóm) là một tiện ích độc quyền của Cisco cho tiêu chuẩn 802.11 và hỗ trợ cho nhiều máy khách có dây.
* **Cầu nối dành cho Ngoài trời**

Sẽ thế nào nếu bạn muốn kết nối hai tòa nhà, nhưng không có cáp giữa cả hai, và bạn không muốn sử dụng một mạng WAN? Bạn có thể sử dụng một cầu nối không dây ngoài trời. Bạn có thể cấu hình hai Điểm Truy cập để tạo ra một cầu nối không dây giữa hai mạng LAN trong một khoảng cách dài. Không dây làm cầu nối giữa hai tòa nhà, và thậm chí có khả năng là giữa hai thành phố.

Có hai tùy chọn:

* Điểm đến điểm
* Điểm đến đa điểm

Hãy bắt đầu với kết nối điểm đến điểm:

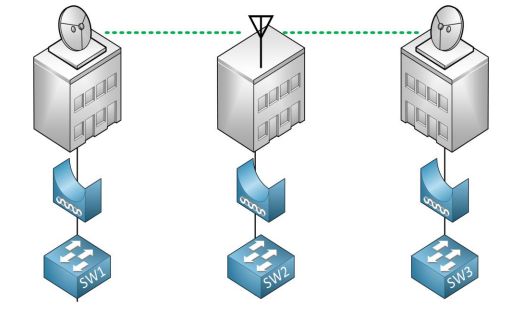


Hình 2.20. Cầu nối dành cho Ngoài trời

Chúng tôi có hai tòa nhà, mỗi tòa có một mạng LAN. Các Điểm Truy cập đang trong chế độ cầu nối và sử dụng ăn ten có hướng ở cả hai để tập trung tín hiệu ở một hướng, đối với Điểm Truy cập thì nó ở phía khác.

Nếu bạn thắc mắc khoảng cách tối đa của một cầu nối không dây thì có thể có: Ghi nhận liên kết wifi dài nhất là từ CISAR (Trung tâm Ý cho các Hoạt động Radio). Nó dài 304 km (khoảng 188 dặm).

Nếu bạn muốn làm cầu nối cho nhiều hơn hai mạng LAN, bạn có thể sử dụng một cầu nối điểm đến đa điểm:



Hình 2.21. Cầu nối dành cho Ngoài trời(tt)

Mạng LAN 1 và 3 sử dụng các Điểm Truy cập với các ăn ten có hướng. Mạng LAN2 ở giữa sử dụng một ăn ten đa hướng mà từ đó tín hiệu được chuyển tiếp bằng nhau ở cả hai hướng.

* 1. Bảo mật mạng WLAN
     1. Khái niệm

Bảo mật là vấn đề hết sức quan trọng đối với người dùng trong thời đại 4.0 và đặc biệt là các hệ thống mạng (LAN, WLAN…). Khi sử dụng mạng không dây, chúng ta chỉ cần có thiết bị có khả năng kết nối mạng và nằm trong vùng sóng là có thể truy cập được cho nên vấn đề bảo mật mạng không dây là cực kỳ quan trọng đối với người sử dụng mạng.

Bảo mật là vấn đề rất quan trọng và đặc biệt rất được sự quan tâm của tất cả mọi người, đặc biệt là các công ty, tập đoàn lớn.

* + 1. Một số hình thức tấn công qua mạng không dây thường gặp
* **Tấn công xác thực:**

Tấn công xác thực (Deauthentication attack), tin tặc sẽ sử dụng một nút giả mạo để tìm ra địa chỉ của AP đang điều khiển mạng. Khi tin tặc có được địa chỉ của AP, chúng sẽ gửi quảng bá các bản tin không chứng thực ra toàn mạng khiến cho các nút trong mạng dừng trao đổi tin với mạng. Sau đó tất cả các nút đó sẽ cố kết nối lại, chứng thực lại và liên kết lại với AP. Quá trình này lặp lại liên tục khiến cho mạng rơi vào tình trạng bị dừng hoạt động.

* **Giả mạo AP:**

Giả mạo AP là kiểu tấn công “man in the middle” cổ điển. Đây là kiểu tấn công mà tin tặc đứng ở giữa và trộm lưu lượng truyền giữa 2 nút. Kiểu tấn công này rất mạnh vì tin tặc có thể trộm tất cả lưu lượng đi qua mạng. Tin tặc tạo ra một AP thu hút nhiều sự lựa chọn hơn AP chính thống. AP giả này có thể được thiết lập bằng cách sao chép tất cả các cấu hình của AP chính thống đó là: SSID, địa chỉ MAC v.v…

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

Tần số là một trong những nhược điểm bảo mật trong mạng không dây. Mức độ nguy hiểm thay đổi phụ thuộc vào giao diện của lớp vật lý. Có một vài tham số quyết định sự chịu đựng của mạng là: năng lượng máy phát, độ nhạy của máy thu, tần số RF, băng thông và sự định hướng của anten.

* **Giả mạo địa chỉ MAC:**

Địa chỉ MAC là một cách để ngăn người dùng bất hợp pháp gia nhập vào mạng. Giá trị được mã hoá phần cứng là không thay đổi nhưng giá trị đưa ra phần sụn của phần cứng lại thay đổi được. Có nhiều chương trình sử dụng cho các hệ điều hành khác nhau có thể thay đổi được địa chỉ MAC được đưa ra trong bộ điều hợp mạng.

* **Tấn công từ chối dịch vụ (DDoS):**

Đây là hình thức tấn công làm cho các mạng không dây không thể phục vụ được người dùng, từ chối dịch vụ với những người dùng hợp pháp. Trong mạng có dây có các hình thức tấn công từ chối dịch vụ DoS (Denial of Service) phổ biến như Ping of Death, SYN Flooding. Mạng không dây, một kẻ tấn công có thể tạo ra các sóng có cùng tần số với tần số truyền tín hiệu để gây nhiễu cho đường truyền.

* **WEP Cracking:**

WEP rất dễ bị tấn công vì các khoá mật mã của nó là không thay đổi. WEP là giao thức an ninh Wireless đầu tiên. Ban đầu WEP dùng khoá mã 40-bit, nhưng về sau nó mở rộng lên tới 104-bit. Tuy nhiên về sau những nhà nghiên cứu đã thành công khi bẻ khóa WEP 104-bit trong hai phút bằng máy tính chạy chip Pentium-M loại cũ.

Bây giờ mã hoá WEP 104-bit có thể bị bẻ gẫy một cách dễ dàng, vì thế chuẩn này sẽ không còn tồn tại được lâu nữa do độ an toàn kém. Hiện nay, đa số các thiết bị không dây hỗ trợ WEP với 3 chiều dài khóa: 40bit, 64bit, 128bit.

* + 1. Một số giải pháp để đề phòng các cuộc tấn công mạng
* **WEP Cracking:**

Sử dụng mạng ảo VPN hay các cơ chế xác thực hiện nay cho phép bảo vệ chống lại chống lại quá trình bẻ gãy WEP. AES là một giải pháp mã hoá tiên tiến không có các điểm yếu như ở WEP.

* **Giả mạo địa chỉ MAC**

Có thể ngăn ngừa giả mạo địa chỉ MAC bằng cách sử dụng các cơ chế xác thực như 802.1x hay mạng ảo VPN.

* **Giả mạo AP**

Có thể được ngăn ngừa bằng cách sử dụng VPN hoặc các cơ chế xác thực khác.

* **Tấn công từ chối dịch vụ (DDoS)**

Nâng cao bảo mật mạng, thường xuyên kiểm tra quá trình bảo mật, có máy chủ dự phòng, nhận biết trước các dấu hiệu của cuộc tấn công trước khi nó xảy ra, giới hạn phát sóng mạng, tận dụng các dịch vụ đám mây.

* + 1. Các phương pháp để bảo mật mạng WLAN để ngăn ngừa các truy cập trái phép
* **Lọc địa chỉ MAC:**

Thông thường, một máy tính chỉ có một địa chỉ MAC (Media Access Control) tương ứng với một card mạng gồm 12 chữ số thập lục phân. Địa chỉ MAC là phần “ngầm” của thiết bị phần cứng và được gửi tự động tới điểm truy cập Wi-Fi mỗi khi thiết bị kết nối vào mạng. Sử dụng trình quản lý cấu hình của điểm truy cập (Access Point - AP), bạn có thể lập được một danh sách thiết bị an toàn (được phép truy xuất vào mạng) hay danh sách thiết bị không được phép truy xuất vào mạng (black list – danh sách đen). Nếu bộ lọc địa chỉ MAC được kích hoạt, AP chỉ cho phép các thiết bị trong danh sách an toàn được kết nối vào mạng và cấm tất cả thiết bị trong danh sách đen truy xuất vào mạng, ngay cả khi bạn có khóa kết nối, bất kể bạn đang sử dụng giao thức kết nối nào.

* **Sử dụng tường lửa**:

Tường lửa Internet là một trong các công cụ có thể giúp ngăn chặn các cá nhân không quen biết trên Internet tìm cách truy nhập được vào máy tính của bạn.

Tường lửa có hai loại, phần mềm hoặc phần cứng, nó có tác dụng như một bức tường để bảo vệ và lọc những kẻ xấu mong muốn truy cập vào thiết bị của bạn thông qua Internet. Quản lý bảo mật CSM (Content Security Management) cho ứng dụng tán gẫu IM (MSN, YM!, ICQ…) chia sẻ ngang hàng P2P (SoulSeek, eDonkey, BitTorrent…) và lọc nội dung URL/Web.

* Lọc gói tin IP thông qua chính sách lọc gói.
* Chống lại DoS/DdoS.
* Phòng chống mạo danh địa chỉ IP.
* Thông báo bằng E-Mail và ghi nhật ký thông qua phần mềm Syslog.
* Gán IP cố định theo địa chỉ MAC.
* **Sử dụng VPN (Mạng riêng ảo):**

VPN Server với 32 kênh đồng thời theo 2 dạng: Remote Dial-In User và LAN-to-LAN.

* Mã hóa: AES, MPPE và Hardware-Based DES/2DES.
* Định danh : MD5, SHA-1.
* Cơ chế mã hóa và xác thực IKE : khóa chia sẻ và chữ ký điện tử.
* Hỗ trợ kết nối LAN-to-LAN, Teleworker-to-LAN.
* Dead Peer Detection (DPD): Phát hiện đường không hoạt động.
* Hỗ trợ VPN Pass-Through.
* Cơ chế VPN dự phòng (VPN Bakup).
* **WPA**

WPA (Wi-Fi Protected Access) là chuẩn bảo mật được phát triển để thay thế WEP do mã hóa WEP đã lỗi thời và dễ dàng bị phá vỡ.

WPA có nhiều cải tiến so với WEP như hỗ trợ TKIP (Temporal Key Integrity Protocol) để ngăn chặn việc đánh cắp các gói tin truyền trong wifi và MIC (Message Integrity Check) nhằm đảm bảo dữ liệu không bị giả mạo. Tuy vậy, WAP vẫn còn tồn đọng một vài lỗ hổng từ WEP.

* **WPA2**

**WPA2** là chuẩn bảo mật thay thế cho WPA kể từ năm 2006. WPA2 còn thay thế TKIP bằng **giao thức CCMP** (Counter Mode Cipher Block Chaining Message Authentication Code Protocol).

CCMP là một giao thức truyền dữ liệu và kiểm soát tính truyền dữ liệu thống nhất để **bảo đảm cả tính bảo mật và nguyên vẹn** của dữ liệu được truyền đi. Hiện nay, phần lớn bộ định tuyến wifi đều sử dụng WPA2.

* **WPA3**

**WPA3**là chuẩn bảo mật wifi **mới nhất**hiện nay và được áp dụng trên một số bộ định tuyến sản xuất trong năm 2019. WPA3 được nâng cấp tối ưu hơn so với chuẩn bảo mật WPA2.

WPA3 mang đến khả năng bảo mật trên các **mạng wifi công cộng**, ngăn chặn việc hacker có thể xem trộm hay đánh cắp thông tin khi bạn kết nối với wifi công cộng như ở sân bay, ngân hàng,...

Với chuẩn bảo mật WPA3, hacker **khó có thể đoán mật khẩu wifi** của bạn, đồng thời **ngăn chặn hacker giải mã lưu lượng** ngay cả khi họ đã từng biết mật khẩu của wifi.

* + 1. Các biện pháp để bảo mật mạng WLAN cho từng đối tượng
* **Đối với các công ty, tập đoàn lớn:** nên sử dụng phương pháp mạnh nhất là chứng thực theo mô hình khóa công khai kết hợp với mã hóa WPA2.
* **Đối với các cơ quan có quy môt trung bình:** thì nên kết hợp nhiều phương thức bảo mật. Ngoài ra, nên tách mạng Wifi ra thành một vùng riêng và quy định để hạn chế tối đa truy cập không cần thiết từ mạng Wifi. Khi áp dụng các biện pháp này, có thể thầy rằng độ an ninh của hệ thống giờ sẽ phụ thuộc vào việc đảm bảo tính bí mật của khóa. Như vậy, yếu tố con người sẽ quyết định mức độ an ninh của hệ thống.
* **Đối với các hệ thống mạng Wifi tại gia đình:** chúng ta nên kết hợp đồng thời biện pháp chứng thực và mã hóa, chẳng hạn áp dụng lọc địa chỉ MAC với mã hóa dùng WPA2. Do sử dụng trong nội bộ gia đình, vấn đề quản lý khóa WPA2 sẽ đơn giản đi rất nhiều và giải pháp này là phù hợp.
* **Tại những nơi công cộng:** Khi sử dụng Wifi tại những nơi ngoài cơ quan, ví dụ như tại các quán café Wifi, sân bay… do các hệ thống này thường không áp dụng các biện pháp đảm bảo an ninh và bạn không thể can thiệp để thay đổi điều này, nên chúng ta phải tự lo cho chính mình bằng một biện pháp: dùng firewall cá nhân để ngăn chặn tối đa những truy nhập bất hợp pháp vào máy, thông tin gửi đi phải được đặt mật khẩu, khi kết nối về hệ thống của cơ quan nhất thiết phải sử dụng mã hóa VPN và đặc biệt bạn cần phải cập nhật đầy đủ các bản vá lỗi cho những phần mềm được sử dụng trên máy, nếu không thì tất cả các biện pháp trên cũng trở nên vô nghĩa.
  1. Các thiết bị mạng khác:
     1. Bộ định tuyến(Router)

Bộ định tuyến là thiết bị nối mạng để chuyển tiếp các gói dữ liệu trong mạng máy tính. Nó có chức năng định hướng lưu lượng trên Internet. Một thiết bị định tuyến router được kết nối với hai hoặc nhiều dòng dữ liệu từ các mạng khác nhau. Khi một gói dữ liệu đến trên một trong các dòng, router đọc thông tin địa chỉ mạng trong gói để xác định đích đến cuối cùng. Sau đó, sử dụng thông tin trong bảng định tuyến hoặc chính sách định tuyến của nó, nó sẽ hướng gói dữ liệu đến mạng tiếp theo trên hành trình của nó.

* + 1. Switch

Switch là một thiết bị chuyển mạch quan trọng trong mạng, nó 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.

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.

* + 1. Switch layer 3

Switch layer 3 đảm bảo được nhiều tính năng hơn layer 2 nên chúng có giá trên thị trường cao hơn. Bởi chúng có khả năng thực hiện các tính năng của một switch. Cụ thể là nó có thể lưu được bảng cập nhật địa chỉ MAC của thiết bị kết nối. Bên cạnh đó nó có thêm bảng định tuyến của một Router. Nên đôi lúc bạn bắt gặp một thiết bị switch như là một router nhưng không có cổng kết nối Wan với nhau.

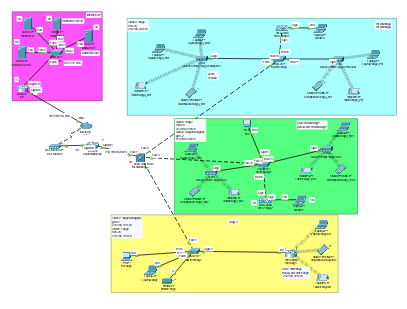
Tuy nhiên không có cổng kết nối WAN nhưng nó thể hiện mình là router tốc độ cao và có chức năng định tuyến như Router để có thể liên thông với các mạng con hoặc VLANs. Và đồng thời đảm bảo định tuyến giữa chúng cùng hệ thống hoạt động ổn định hơn mà không cần đến sự trợ giúp của thiết bị định tuyến Router. Nhờ có tính năng như trên, nên Switch Layer 3 có khả năng xử lý vượt trội hơn so với Switch L2.

* + 1. WLC (Wireless LAN Controller)

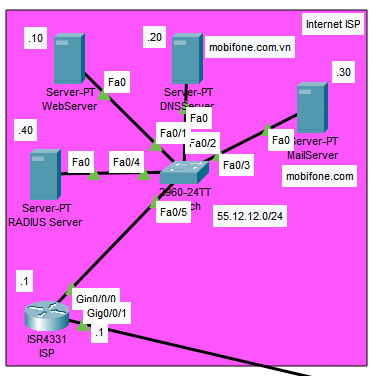
WLC có chức năng quản lý, thống nhất các AP lại với nhau. Một WLC có thể quản lý 6-300 AP, trên mỗi AP có thể gán đến 15 mạng WLAN và hỗ trợ tối đa 512 VLAN. AP và WLC giao tiếp với nhau bằng giao thức LWAPP được cung cấp bởi radio resource management (RRM).

1. MÔ HÌNH DEMO
   1. Mô hình đề xuất
      1. Mô hình

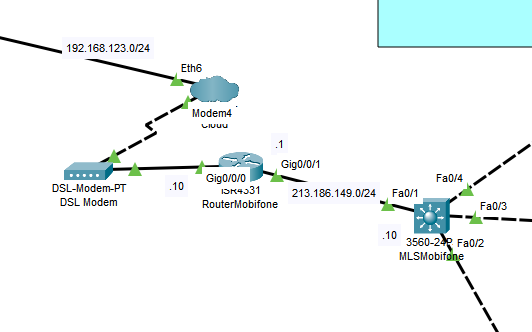
* **Mô hình luận lý**



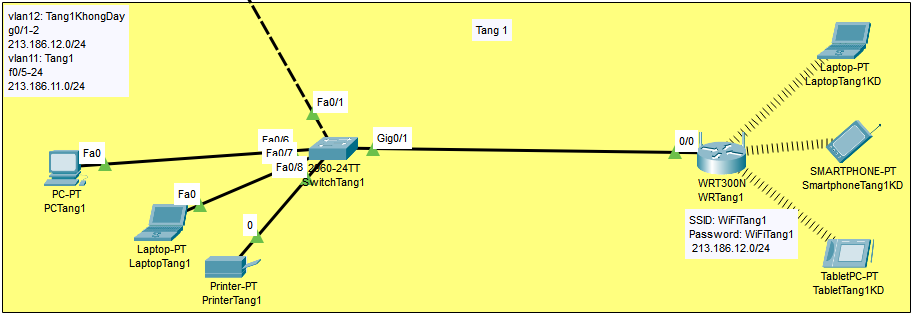
Hình 3.1.1. Mô hình luận lý tổng quát



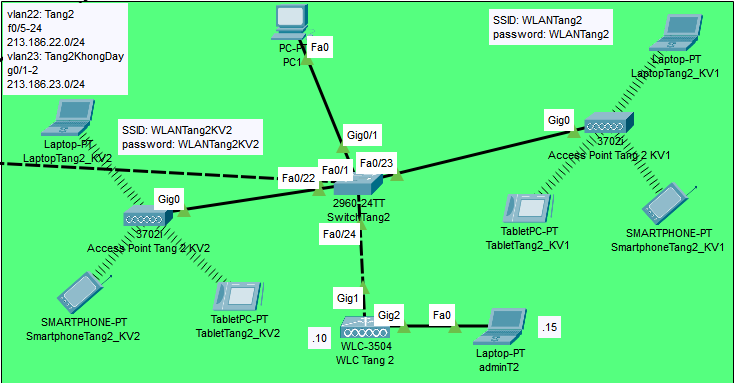
Hình 3.1.2. Chi tiết mô hình luận lý Internet ISP



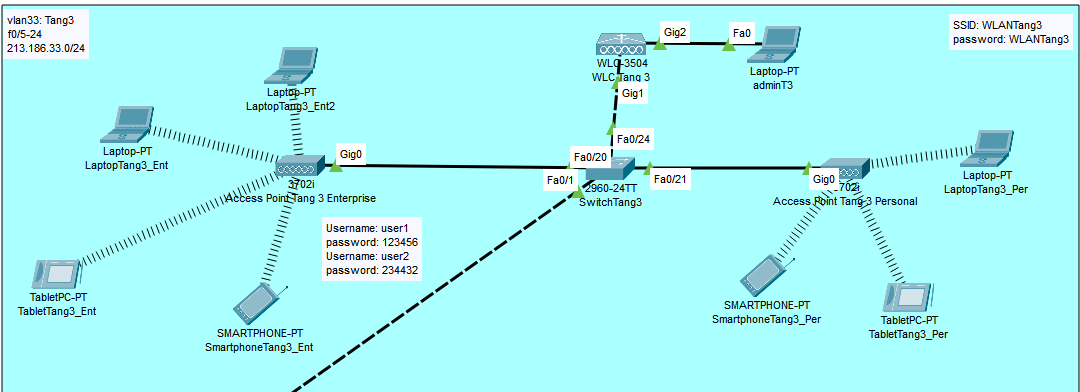
Hình 3.1.3. Mô hình luận lý Modem, Router Mobifone và MLSMobifone



Hình 3.1.4. Chi tiết mô hình luận lý tầng 1

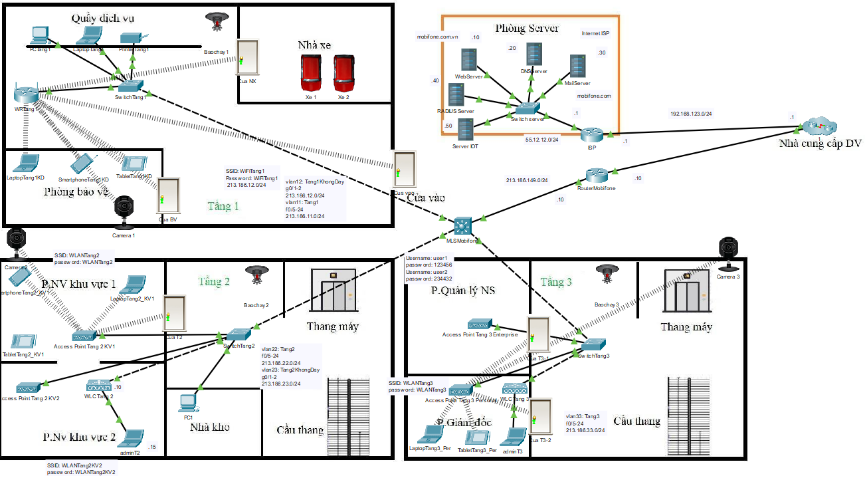


Hình 3.1.5. Chi tiết mô hình luận lý tầng 2

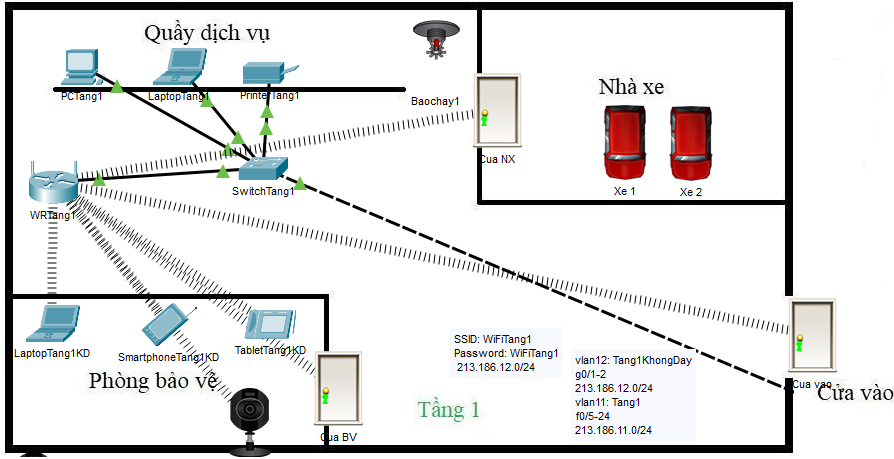


Hình 3.1.6. Chi tiết mô hình luận lý tầng 3

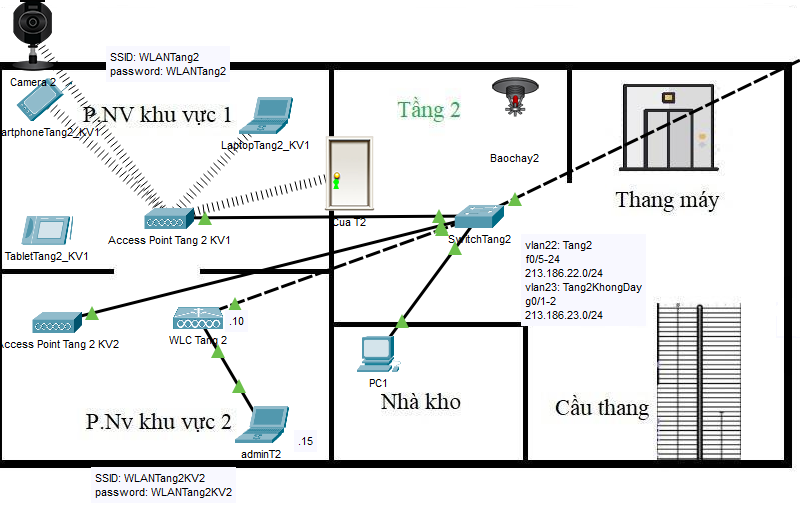
* **Mô hình vật lý**



Hình 3.1.7. Mô hình vật lý tổng quát



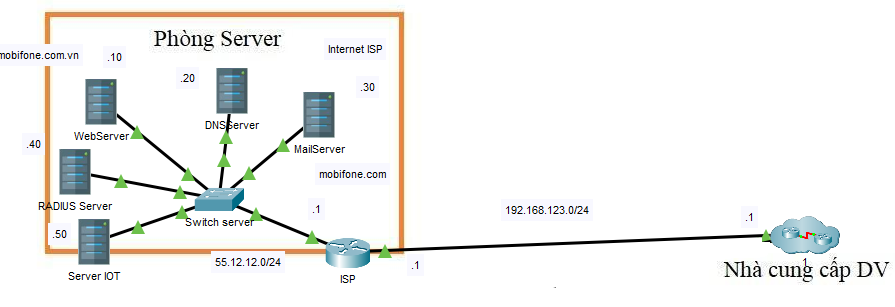
Hình 3.1.8. Chi tiết mô hình vật lý tầng 1



Hình 3.1.9. Chi tiết mô hình vật lý tầng 2



Hình 3.1.10. Chi tiết mô hình vật lý tầng 3



Hình 3.1.11. Chi tiết phòng Server

* + 1. Bảng địa chỉ IP

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Interface** | **VLAN** | **IP Address** | **Subnet mask** | **Default gateway** |
| Web Server | Fa0 | N/A | 55.12.12.10 | 255.255.255.0 | 55.12.12.1 |
| DNS Server | Fa0 | N/A | 55.12.12.20 | 255.255.255.0 | 55.12.12.1 |
| Mail Server | Fa0 | N/A | 55.12.12.30 | 255.255.255.0 | 55.12.12.1 |
| RADIUS Server | Fa0 | N/A | 55.12.12.40 | 255.255.255.0 | 55.12.12.1 |
| ISP | Gig0/0/0 | N/A | 55.12.12.1 | 255.255.255.0 | N/A |
| Gig0/0/1 | N/A | 192.168.123.1 | 255.255.255.0 | N/A |
| Router Mobifone | Gig0/0/0 | N/A | 192.168.123.10 | 255.255.255.0 | N/A |
| Gig0/0/1 | N/A | 213.186.149.1 | 255.255.255.0 | N/A |
| MLS Mobifone | Fa0/1 | N/A | 213.186.149.10 | 255.255.255.0 | N/A |
| Fa0/2 |  | DHCP Assigned | DHCP Assigned | DHCP Assigned |
| Fa0/3 |  | DHCP Assigned | DHCP Assigned | DHCP Assigned |
| Fa0/4 |  | DHCP Assigned | DHCP Assigned | DHCP Assigned |
| SwitchTang1 | Fa0/6 | 11 | DHCP Assigned | DHCP Assigned | DHCP Assigned |
| Fa0/7 | DHCP Assigned | DHCP Assigned | DHCP Assigned |
| Fa0/7 | DHCP Assigned | DHCP Assigned | DHCP Assigned |
| Gig0/1 | 12 | DHCP Assigned | DHCP Assigned | DHCP Assigned |
| SwitchTang2 | Fa0/24 | 22 | 213.186.22.10 | 255.255.255.0 | 213.186.22.1 |
| Fa0/23 | DHCP Assigned | DHCP Assigned | DHCP Assigned |
| Fa0/22 | DHCP Assigned | DHCP Assigned | DHCP Assigned |
| Gig0/1 | 23 | DHCP Assigned | DHCP Assigned | DHCP Assigned |
| SwitchTang3 | Fa0/24 | 33 | 213.186.33.10 | 255.255.255.0 | 213.186.33.1 |
| Fa0/20 | DHCP Assigned | DHCP Assigned | DHCP Assigned |
| Fa0/21 | DHCP Assigned | DHCP Assigned | DHCP Assigned |

Bảng 3.1.1. Bảng địa chỉ IP

* + 1. Bảng thông tin kết nối port trong hệ thống

|  |  |  |  |
| --- | --- | --- | --- |
| **From Source to Destination Device** | **Source Interface** | **Destination Interface** | **Trunking/ VLAN** |
| Web Server to Switch | Fa0 | Fa0/1 |  |
| DNS Server to Switch | Fa0 | Fa0/2 |
| Mail Server to Switch | Fa0 | Fa0/3 |
| RADIUS Server to Switch | Fa0 | Fa0/4 |
| Switch to Router ISP | Fa0/5 | Gig0/0/0 |
| ISP to Cloud | Gig0/0/1 | Eth6 |
| Cloud to DSL Modem | Modem4 | Port 0 |
| DSL Modem to Router Mobifone | Port 1 | Gig0/0/0 |
| Router Mobifone to MLS Mobifone | Gig0/0/1 | Fa0/1 |
| MLS Mobifone to SwitchTang1 | Fa0/2 | Fa0/1 | Trunking |
| MLS Mobifone to SwitchTang2 | Fa0/3 | Fa0/1 |
| MLS Mobifone to SwitchTang3 | Fa0/4 | Fa0/1 |
| SwitchTang1 to PCTang1 | Fa0/6 | Fa0 | Vlan 11 |
| SwitchTang1 to LaptopTang1 | Fa0/7 | Fa0 |
| SwitchTang1 to PrinterTang1 | Fa0/8 | Fa0 |
| SwitchTang1 to WRTang1 | Gig0/1 | Internet | Vlan 12 |
| SwitchTang2 to WLC Tang 2 | Fa0/24 | Gig1 | Vlan 22 |
| SwitchTang2 to AP Tang2 KV1 | Fa0/23 | Gig0 |
| SwitchTang2 to AP Tang2 KV2 | Fa0/22 | Gig0 |
| WLC Tang 2 to adminT2 | Gig2 | Fa0 |
| SwitchTang2 to PC1 | Gig0/1 | Fa0 | Vlan 23 |
| SwitchTang 3 to WLC Tang 3 | Fa0/24 | Gig1 | Vlan 33 |
| SwitchTang 3 to AP Tang 3 Personal | Fa0/21 | Gig0 |
| SwitchTang 3 to AP Tang 3 Enterprise | Fa0/20 | Gig0 |
| WLC Tang 3 to adminT3 | Gig0/2 | Fa0 |

Bảng 3.1.2. Bảng thông tin kết nối cổng trong hệ thống

* + 1. Bảng thiết kế thông tin vlan

|  |  |  |  |
| --- | --- | --- | --- |
| **VLAN Name** | **VLAN Number** | **Subnet** | **Default Gateway** |
| Tang1 | 11 | 213.186.11.0/24 | 213.186.11.1 |
| Tang1KhongDay | 12 | 213.186.12.0/24 | 213.186.12.1 |
| Tang2 | 22 | 213.186.22.0/24 | 213.186.22.1 |
| Tang2KhongDay | 23 | 213.186.23.0/24 | 213.186.23.1 |
| Tang3 | 33 | 213.186.33.0/24 | 213.186.33.1 |

Bảng 3.1.3. Bảng thông tin vlan trong hệ thống

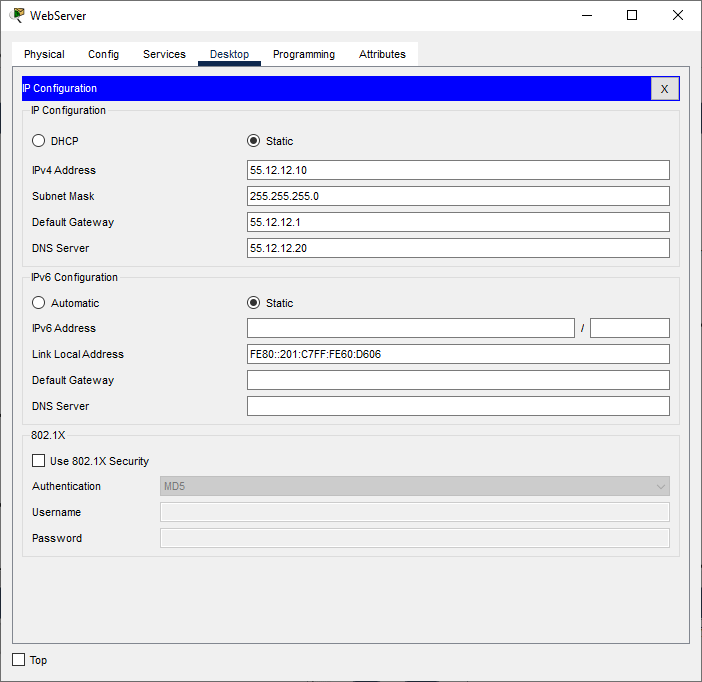
* + 1. Bảng thông tin

|  |  |  |
| --- | --- | --- |
| **Device** | **Username** | **Password** |
| RADIUS Server | WLC Tang 3 | WLCTang3 |
| WRTang1 | WiFiTang1 | WiFiTang1 |
| Access Point Tang 2 KV1 | WLANTang2 | WLANTang2 |
| WLANTang2KV2 | WLANTang2KV2 |
| WLC Tang 2 | adminT2 | adminT2 |
| Access Point Tang 3 Personal | WLANTang3 | WLANTang3 |
| Access Point Tang 3 Enterprise | user1 | 123456 |
| user2 | 234432 |
| WLC Tang 3 | adminT3 | adminT3 |

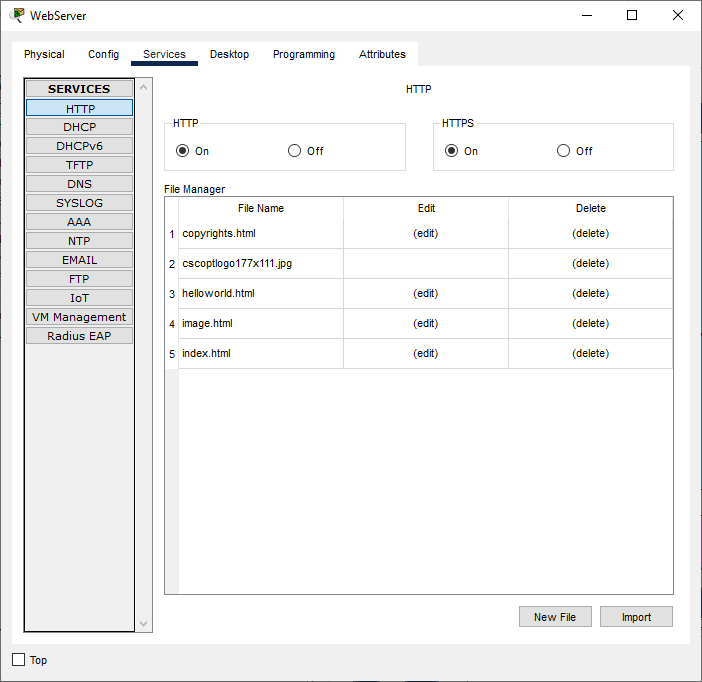
Bảng 3.1.4. Bảng thông tin trong hệ thống

* 1. Cấu hình trên các thiết bị
     1. Máy chủ web

Cấu hình địa chỉ IP, subnet mask, default gateway và DNS Server cho máy chủ web.



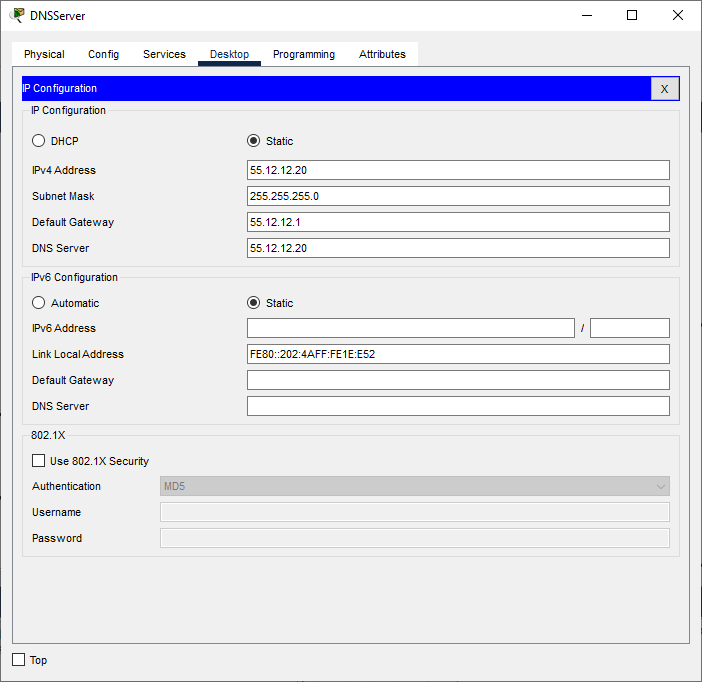
Hình 3.2.1. Cấu hình máy chủ web



Hình 3.2.2. Cấu hình dịch vụ web

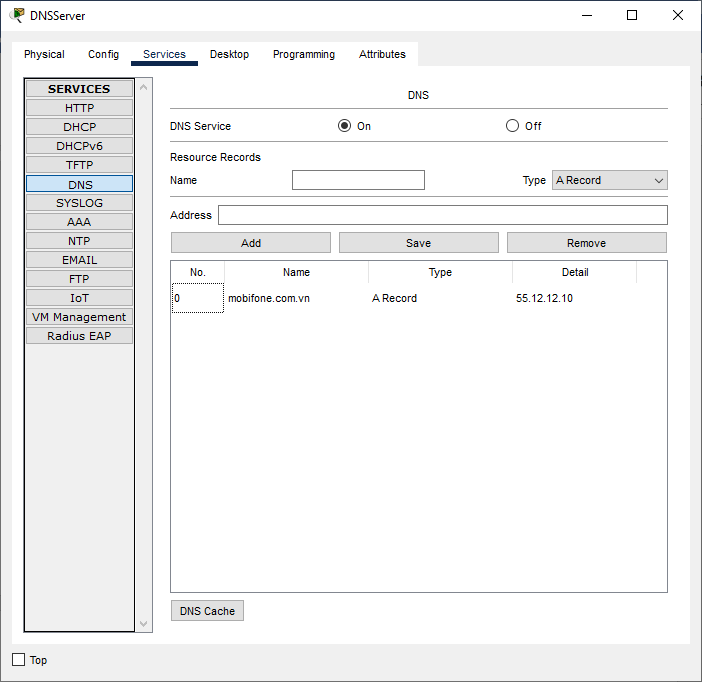
* + 1. Máy chủ DNS

Cấu hình địa chỉ IP, subnet mask, default gateway và DNS Server cho máy chủ DNS.



Hình 3.2.3. Cấu hình máy chủ DNS

Cấu hình dịch vụ cho máy chủ DNS bằng cách thêm tên trang web mobifone.com.vn.



Hình 3.2.4. Cấu hình dịch vụ DNS

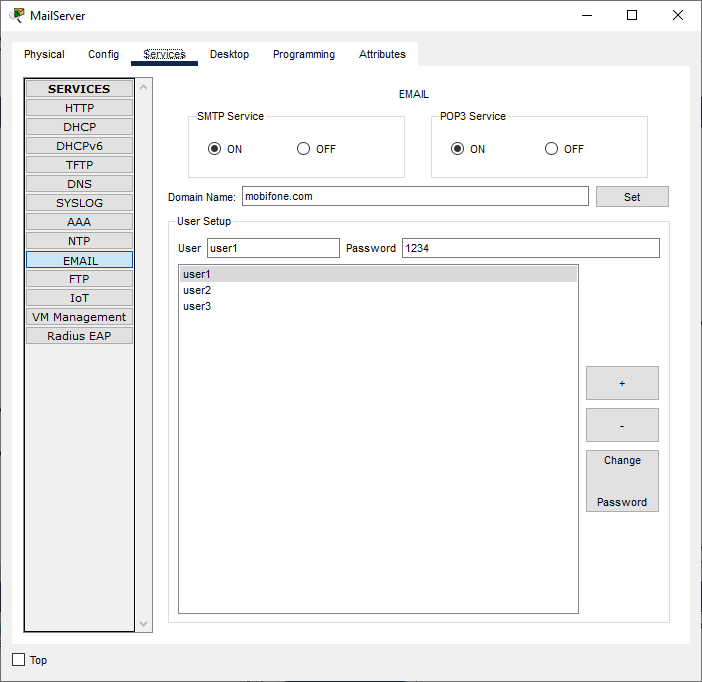
* + 1. Máy chủ mail

Cấu hình địa chỉ IP, subnet mask, default gateway và DNS Server cho máy chủ mail.



Hình 3.2.5. Cấu hình cho máy chủ mail

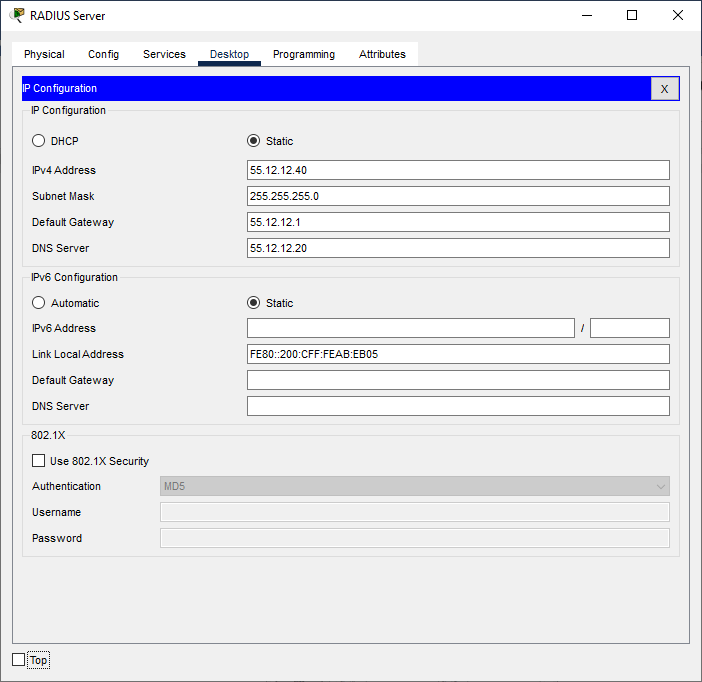
Thêm tên người dùng vào máy chủ mail.



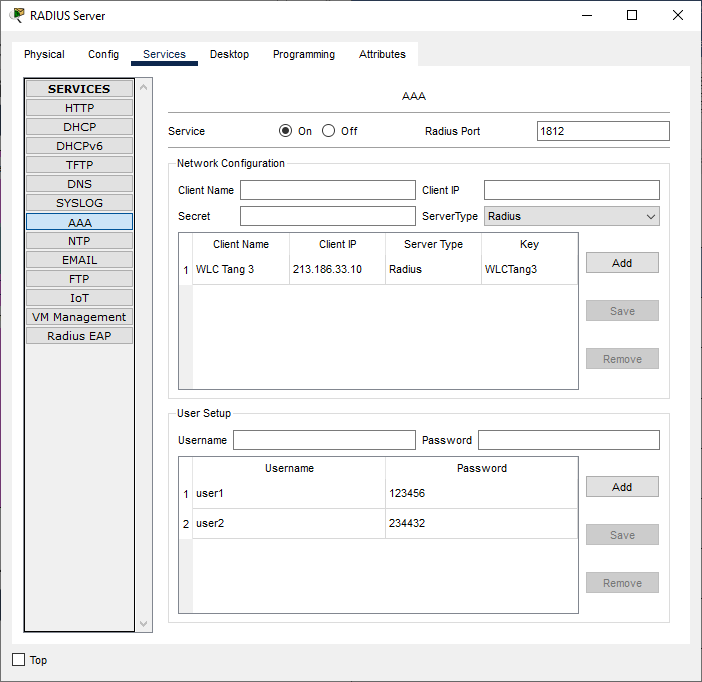
Hình 3.2.6. Thêm tên người dùng vào máy chủ mail

* + 1. RADIUS Server

Cấu hình các thông tin cơ bản



Hình 3.2.7. Cấu hình cơ bản cho RADIUS Server

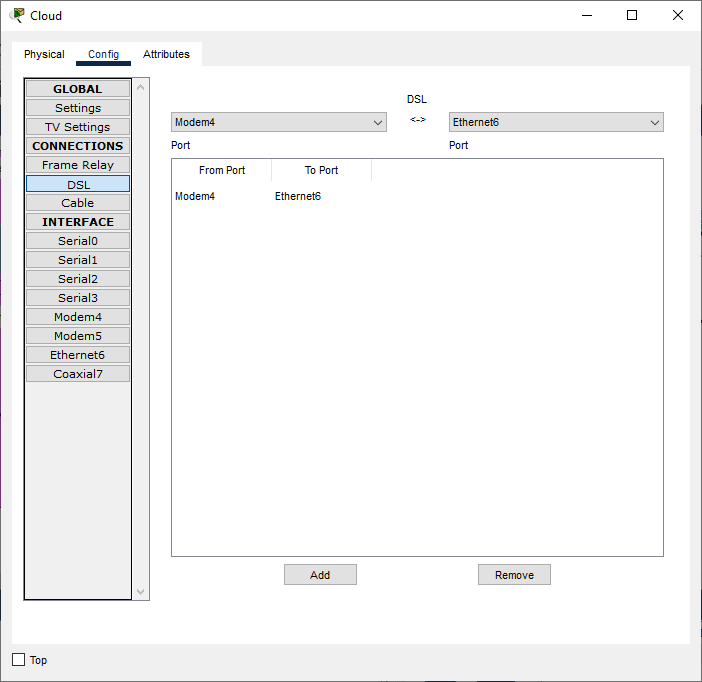


Hình 3.2.8. Cấu hình dịch vụ cho RADIUS Server

* + 1. Router ISP

|  |
| --- |
| Router>ena  Router#conf t  Router(config)#hostname ISP  ISP(config)#int g0/0/0  ISP(config-if)#ip address 55.12.12.1 255.255.255.0  ISP(config-if)#no shutdown  ISP(config-if)#int g0/0/1  ISP(config-if)#ip address 192.168.123.1 255.255.255.0  ISP(config-if)#no shutdown  ISP(config-if)#exit  ISP(config)#ip routing  ISP(config)#router ospf 1  ISP(config-router)#network 55.12.12.0 0.255.255.255 area 0  ISP(config-router)#network 192.168.123.0 0.255.255.255 area 0  ISP(config-router)#exit  ISP(config)#end  ISP#  ISP#copy running-config startup-config  Destination filename [startup-config]?  Building configuration...  [OK]  ISP# |

* + 1. Cấu hình Cloud



Hình 3.2.9. Cấu hình cho cloud

* + 1. Cấu hình router Mobifone

|  |
| --- |
| Router>ena  Router#conf t  Router(config)#host RouterMobifone  RouterMobifone(config)#int g0/0/0  RouterMobifone(config-if)#ip address 192.168.123.10 255.255.255.0  RouterMobifone(config-if)#no shutdown  RouterMobifone(config-if)#int g0/0/1  RouterMobifone(config-if)#ip address 213.186.149.1 255.255.255.0  RouterMobifone(config-if)#no shutdown  RouterMobifone(config-if)#exit  RouterMobifone(config)#ip routing  RouterMobifone(config)#router ospf 1  RouterMobifone(config-router)#network 192.168.123.0 0.255.255.255 area 0  RouterMobifone(config-router)#network 213.186.149.0 0.255.255.255 area 0  RouterMobifone(config-router)#end  RouterMobifone#cop run sta  Destination filename [startup-config]?  Building configuration...  [OK]  RouterMobifone# |

* + 1. MLS

|  |
| --- |
| Switch>ena  Switch#conf t  Enter configuration commands, one per line. End with CNTL/Z.  Switch(config)#hostname MLSMobifone  MLSMobifone(config)#int f0/1  MLSMobifone(config-if)#no switchport  MLSMobifone(config-if)#  MLSMobifone(config-if)#ip address 213.186.149.10 255.255.255.0  MLSMobifone(config-if)#no shutdown  MLSMobifone(config-if)#exit  MLSMobifone(config)#ip routing  MLSMobifone(config)#router ospf 1  MLSMobifone(config-router)#network 213.186.149.0 0.255.255.255 area 0  MLSMobifone(config-router)#end  MLSMobifone#conf t  MLSMobifone(config)#vlan 11  MLSMobifone(config-vlan)#name Tang1  MLSMobifone(config-vlan)#vlan 12  MLSMobifone(config-vlan)#name Tang1KhongDay  MLSMobifone(config-vlan)#int vlan 11  MLSMobifone(config-if)#ip address 213.186.11.1 255.255.255.0  MLSMobifone(config-if)#no shutdown  MLSMobifone(config-if)#int vlan 12  MLSMobifone(config-if)#ip address 213.186.12.1 255.255.255.0  MLSMobifone(config-if)#no shutdown  MLSMobifone(config-if)#ex  MLSMobifone(config)#ip dhcp excluded-address 213.186.11.1 213.186.11.15  MLSMobifone(config)#ip dhcp pool vlan11  MLSMobifone(dhcp-config)#network 213.186.11.0 255.255.255.0  MLSMobifone(dhcp-config)#default-router 213.186.11.1  MLSMobifone(dhcp-config)#dns-server 55.10.10.20  MLSMobifone(dhcp-config)#exit  MLSMobifone(config)#ip dhcp excluded-address 213.186.12.1 213.186.12.15  MLSMobifone(config)#ip dhcp pool vlan12  MLSMobifone(dhcp-config)#network 213.186.12.0 255.255.255.0  MLSMobifone(dhcp-config)#default-router 213.186.12.1  MLSMobifone(dhcp-config)#dns-server 55.10.10.20  MLSMobifone(dhcp-config)#exi  MLSMobifone(config)#  MLSMobifone(config)#router ospf 1  MLSMobifone(config-router)#network 213.186.11.0 0.255.255.255 area 0  MLSMobifone(config-router)#network 213.186.12.0 0.255.255.255 area 0  MLSMobifone(config-router)#  LSMobifone(config-router)#ex  MLSMobifone(config)#  MLSMobifone(config)#ex  MLSMobifone#  %SYS-5-CONFIG\_I: Configured from console by console  MLSMobifone#copy run sta  Destination filename [startup-config]?  Building configuration...  [OK]  MLSMobifone#  MLSMobifone#conf t  MLSMobifone(config)#vlan 22  MLSMobifone(config-vlan)#name Tang2  MLSMobifone(config-vlan)#vlan 23  MLSMobifone(config-vlan)#name Tang2KhongDay  MLSMobifone(config-vlan)#ex  MLSMobifone(config)#int vlan 22  MLSMobifone(config-if)#ip address 213.186.22.1 255.255.255.0  MLSMobifone(config-if)#no shutdown  MLSMobifone(config-if)#int vlan 23  MLSMobifone(config-if)#ip address 213.186.23.1 255.255.255.0  MLSMobifone(config-if)#no shutdown  MLSMobifone(config-if)#e  MLSMobifone(config)#ip dhcp excluded-address 213.186.22.1 213.186.22.15  MLSMobifone(config)#ip dhcp pool vlan22  MLSMobifone(dhcp-config)#network 213.186.22.0 255.255.255.0  MLSMobifone(dhcp-config)#default-router 213.186.22.1  MLSMobifone(dhcp-config)#dns-server 55.12.12.20  MLSMobifone(dhcp-config)#ex  MLSMobifone(config)#ip dhcp excluded-address 213.186.23.1 213.186.23.15  MLSMobifone(config)#ip dhcp pool vlan23  MLSMobifone(dhcp-config)#network 213.186.23.0 255.255.255.0  MLSMobifone(dhcp-config)#default-router 213.186.23.1  MLSMobifone(dhcp-config)#dns-server 55.12.12.20  MLSMobifone(dhcp-config)#ex  MLSMobifone(config)#router ospf 1  MLSMobifone(config-router)#network 213.186.22.0 0.255.255.255 area 0  MLSMobifone(config-router)#network 213.186.23.0 0.255.255.255 area 0  MLSMobifone(config-router)#end  MLSMobifone#  MLSMobifone#cop run sta  Destination filename [startup-config]?  Building configuration...  [OK]  MLSMobifone#  MLSMobifone>ena  MLSMobifone#conf t  MLSMobifone(config)#vlan 33  MLSMobifone(config-vlan)#name Tang3  MLSMobifone(config-vlan)#ex  MLSMobifone(config)#int vlan 33  MLSMobifone(config-if)#  MLSMobifone(config-if)#ip address 213.186.33.1 255.255.255.0  MLSMobifone(config-if)#no shutdown  MLSMobifone(config-if)#ex  MLSMobifone(config)#ip dhcp excluded-address 213.186.33.1 213.186.33.15  MLSMobifone(config)#ip dhcp pool vlan33  MLSMobifone(dhcp-config)#network 213.186.33.0 255.255.255.0  MLSMobifone(dhcp-config)#default-router 213.186.33.1  MLSMobifone(dhcp-config)#dns-server 55.12.12.20  MLSMobifone(dhcp-config)#ex  MLSMobifone(config)#router ospf 1  MLSMobifone(config-router)#network 213.186.33.0 0.255.255.255 area 0  MLSMobifone(config-router)#ex  MLSMobifone(config)#end  MLSMobifone#cop run sta  Destination filename [startup-config]?  Building configuration...  [OK]  MLSMobifone#  MLSMobifone# |

* + 1. Switch tầng 1

|  |
| --- |
| Switch>ena  Switch#conf t  Switch(config)#host Tang1  Tang1(config)#vlan 11  Tang1(config-vlan)#name Tang1  Tang1(config-vlan)#vlan 12  Tang1(config-vlan)#name Tang1KhongDay  Tang1(config-vlan)#ex  Tang1(config)#int f0/1  Tang1(config-if)#swi mod tru  Tang1(config-if)#  Tang1(config-if)#ex  Tang1(config)#int ran f0/5-24  Tang1(config-if-range)#swi mod acc  Tang1(config-if-range)#swi acc vla 11  Tang1(config-if-range)#int ran g0/1-2  Tang1(config-if-range)#swi mod acc  Tang1(config-if-range)#swi acc vla 12  Tang1(config-if-range)#ex  Tang1(config)#end  Tang1#  Tang1#cop run sta  Destination filename [startup-config]?  Building configuration...  [OK]  Tang1#  Tang1# |

* + 1. Switch Tầng 2

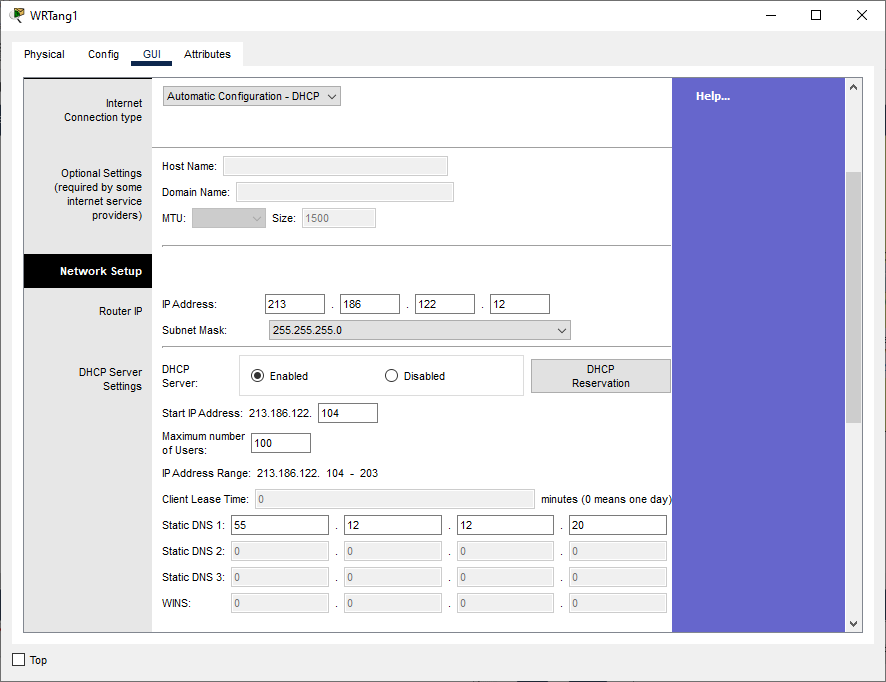
|  |
| --- |
| Switch>ena  Switch#conf t  Switch (config)#host Tang2  Tang2(config)#vlan 22  Tang2(config-vlan)#name Tang2  Tang2(config-vlan)#vlan 23  Tang2(config-vlan)#name Tang2KhongDay  Tang2(config-vlan)#ex  Tang2(config)#int f0/1  Tang2(config-if)#swi mod tru  Tang2(config-if)#int ran f0/5-24  Tang2(config-if-range)#swi mod acc  Tang2(config-if-range)#swi acc vlan 22  Tang2(config-if-range)#int ran g0/1-2  Tang2(config-if-range)#swi mod acc  Tang2(config-if-range)#swi acc vlan 23  Tang2(config-if-range)#end  Tang2#  Tang2#cop run sta  Destination filename [startup-config]?  Building configuration...  [OK]  Tang2# |

* + 1. Switch Tầng 3

|  |
| --- |
| Switch>ena  Switch#conf t  Switch (config)#host Tang3  Tang3(config)#vlan 33  Tang3(config-vlan)#name Tang3  Tang3(config-vlan)#ex  Tang3(config)#int f0/1  Tang3(config-if)#swi mod tru  Tang3(config-if)#int ran f0/5-24  Tang3(config-if-range)#swi mod acc  Tang3(config-if-range)#swi acc vlan 33  Tang3(config-if-range)#end  Tang3#  Tang3#cop run sta  Destination filename [startup-config]?  Building configuration...  [OK]  Tang3# |

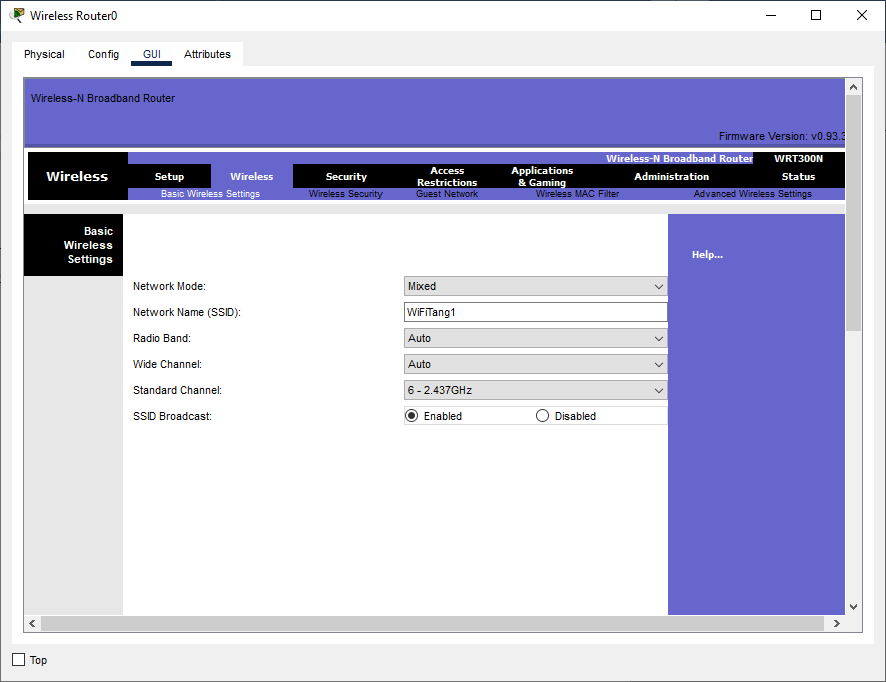
* + 1. Cấu hình WRTang1

Chọn loại kết nối Internet là DHCP, nhập địa chỉ IP và chọn subnet mask, sau đó chọn địa chỉ IP bắt đầu là 213.186.122.104 và giới hạn số lượng máy là 100. Sau đó nhập địa chỉ DNS. Sau đó, kéo xuống dưới nhấn vào Save Settings để lưu lại cấu hình.



Hình 3.2.10. Cấu hình cơ bản cho WRTang1

Nhấn vào mục Wireless, Nhập SSID là **WiFiTang1** và chọn Kênh số **6**, sau đó kéo xuống dưới nhấn vào Save Settings để lưu lại cấu hình.



Hình 3.2.11. Cấu hình SSID cho WRTang1

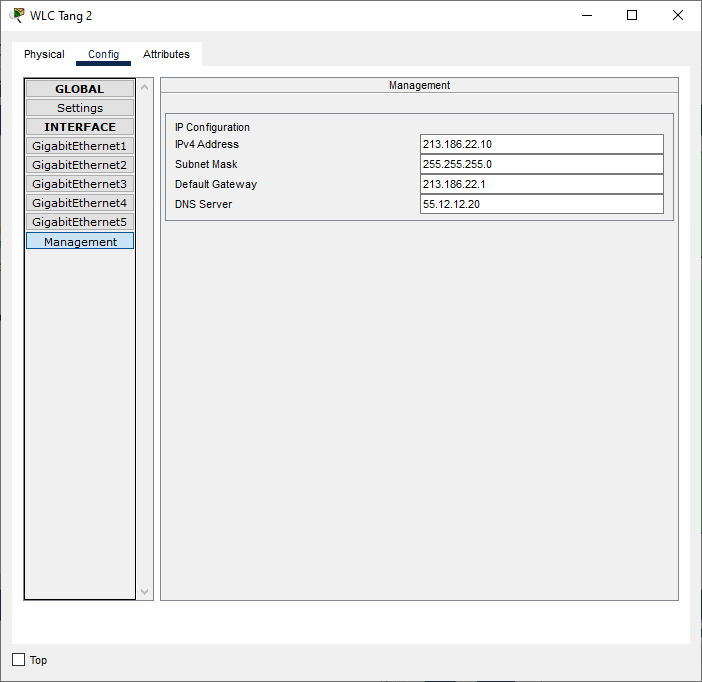
Nhấn vào Wireless Security và chọn Security Mode là WPA2 Personal. Nhập mật khẩu là WiFiTang1 và kéo xuống dưới nhấn vào Save Settings để lưu lại cấu hình.



Hình 3.2.12. Đặt mật khẩu cho cho WRTang1

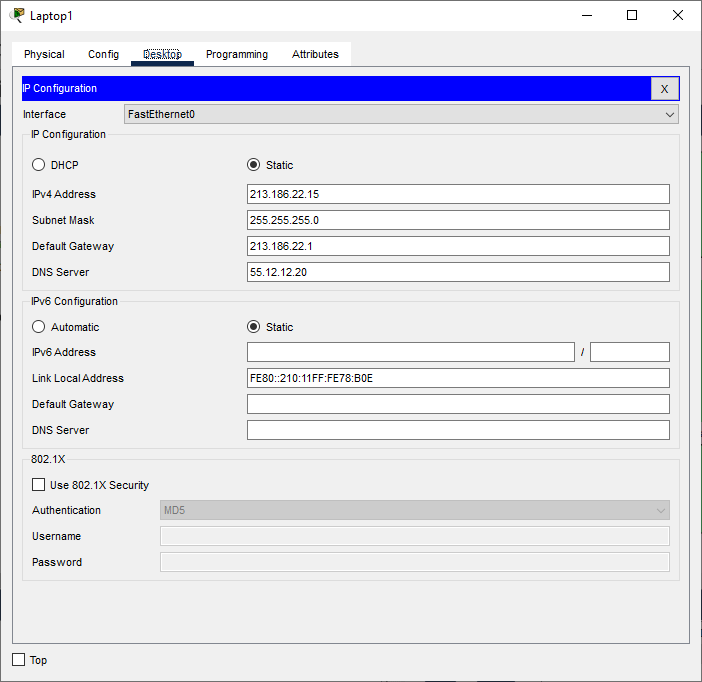
* + 1. Cấu hình WLC tầng 2

Nhấn vào WLC Tang 2 và chọn tab Config. Chọn phần Management và nhập các thông tin có trong bảng địa chỉ.



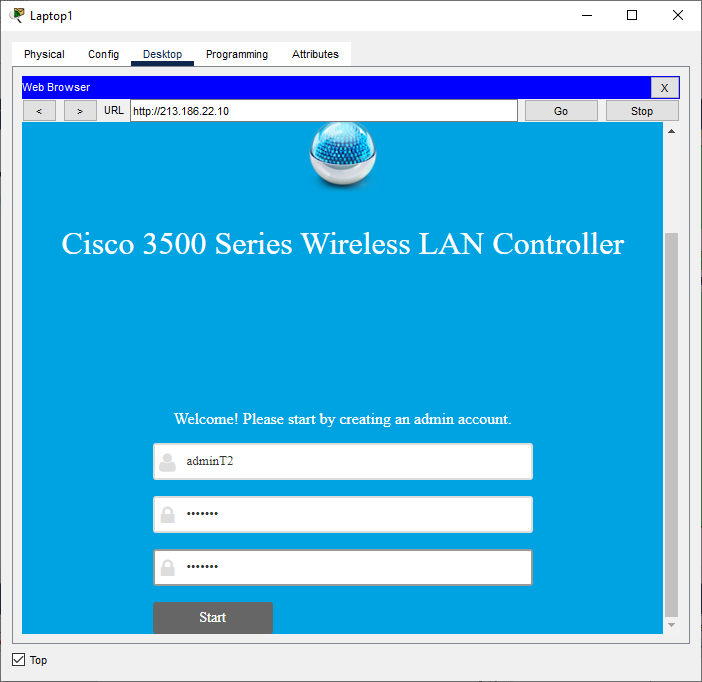
Hình 3.2.13. Cấu hình địa chỉ cho WLC Tang 2

Nhập địa chỉ cho Laptop1 để sử dụng nó để kết nối đến WLC.



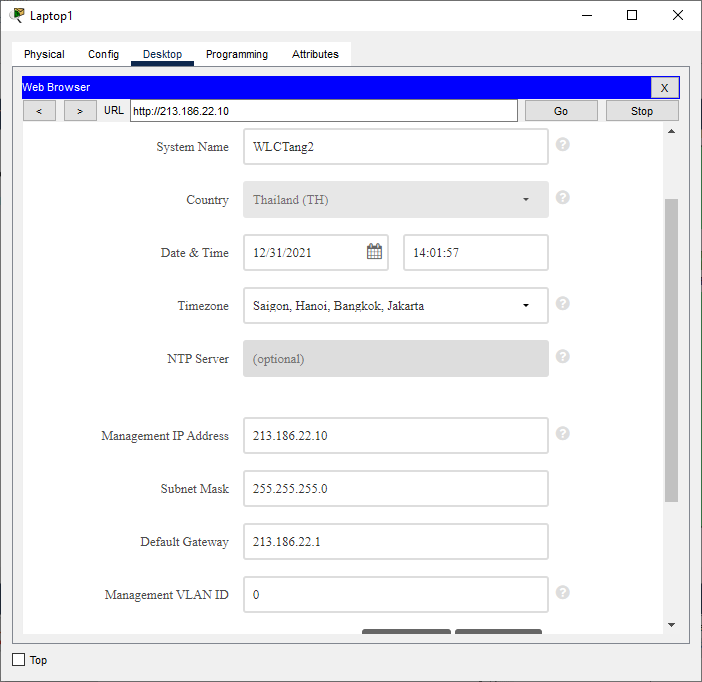
Hình 3.2.14. Cấu hình địa chỉ cho Laptop1

Ở Laptop1, mở trình duyệt và nhập địa chỉ **213.186.22.10**. Chờ một tí để trình duyệt hiển trị trang đăng ký cho WLC. Nhập **adminT2** cho username và password.



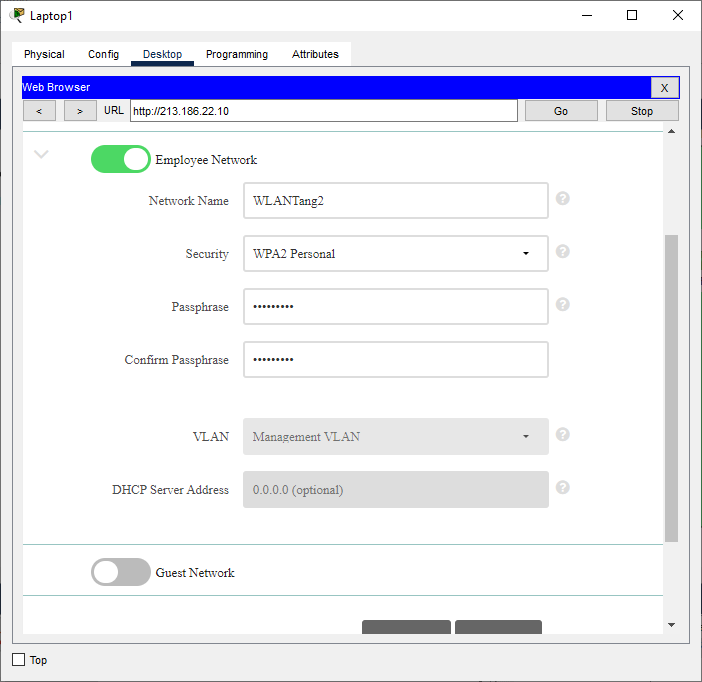
Hình 3.2.15. Trang đăng ký cho WLC Tang 2

Điền các thông tin vào chỗ trống bao gồm **WLCTang2** cho System Name, 213.186.22.10 cho mục **địa chỉ IP**, 255.255.255.0 cho **subnet mask**, 213.186.22.1 cho **default gateway,** và sau đó nhấn vào nút **Next**.



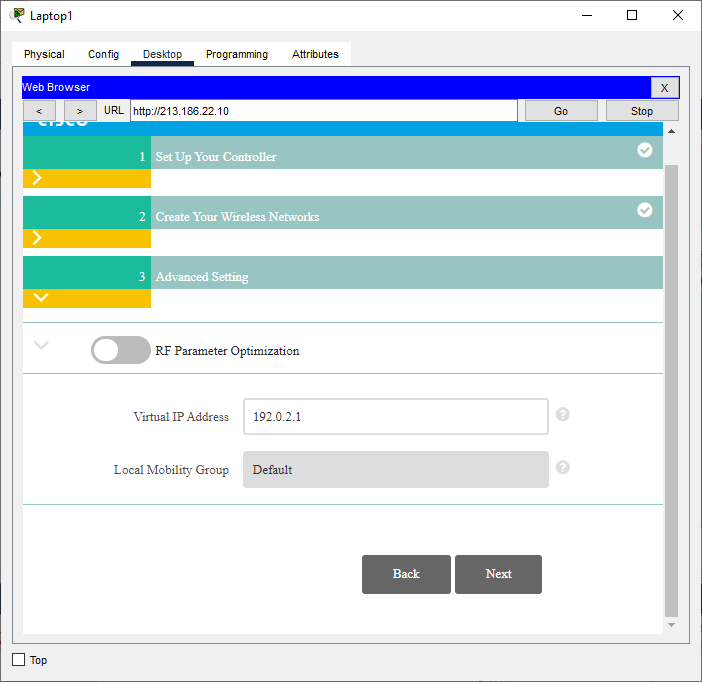
Hình 3.2.16. Trang đăng ký tên và địa chỉ cho WLC Tang 2

Nhập Network Name là **WLANTang2** và chọn Security là WPA2 Personal. Nhập mật khẩu là **WLANTang2**, giữ nguyên các tùy chọn còn lại và nhấn vào nút **Next.**



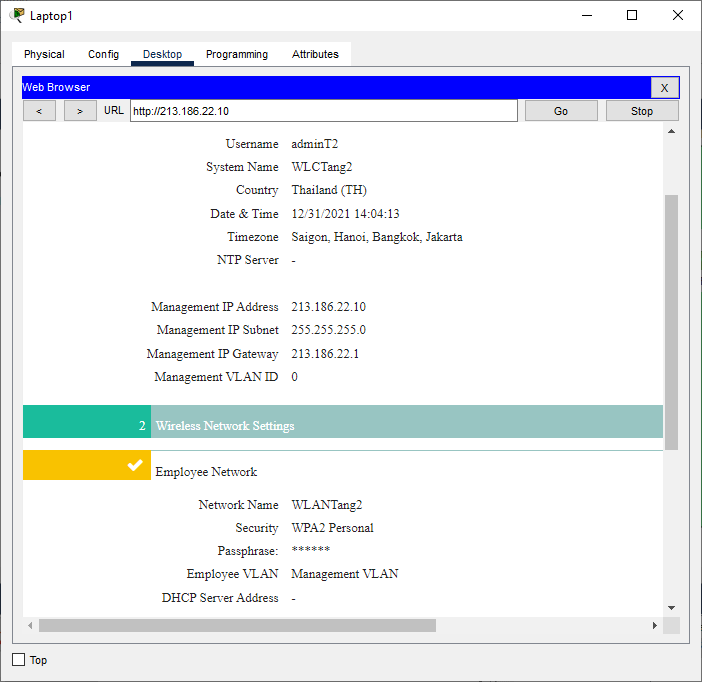
Hình 3.2.17. Trang đăng ký tên mạng và mật khẩu cho WLC Tang 2

Ở trang này, chúng ta giữ nguyên tùy chọn và nhấn vào **Next** để tiếp tục.

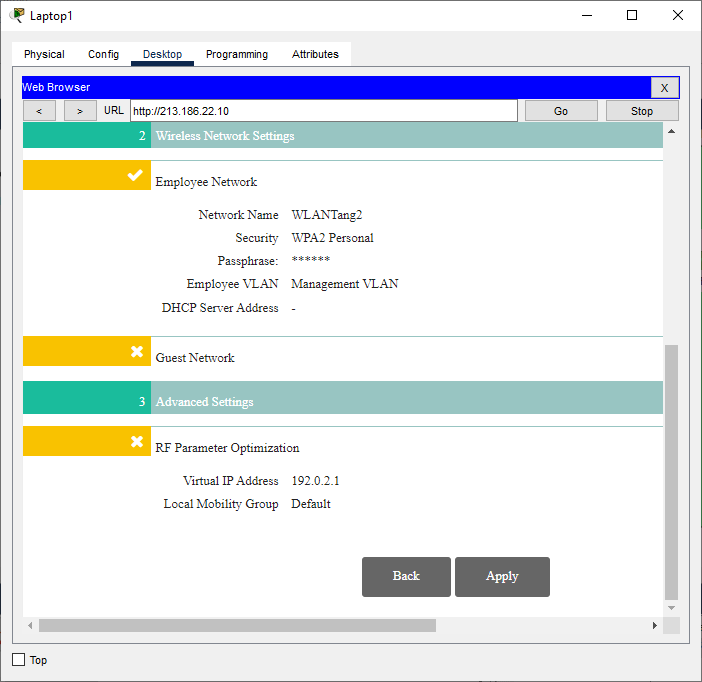


Hình 3.2.18. Trang nhập địa chỉ IP ảo cho WLC Tang 2

Lúc này trang đăng ký WLC sẽ hiển thị thông tin mà chúng ta đã đăng ký trước đó. Nhấn **Apply** để hoàn tất đăng ký và nhấn vào nút **X** để thoát khỏi trình duyệt.

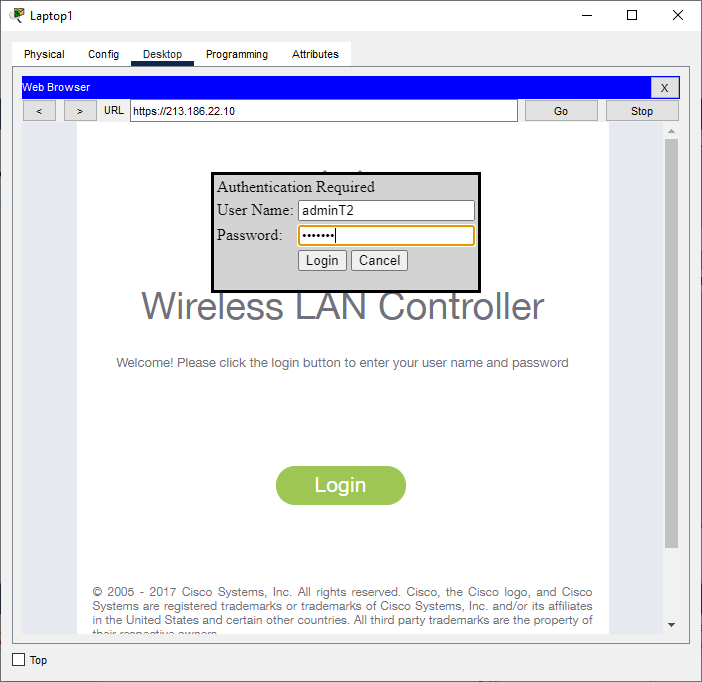


Hình 3.2.19. Kết quả đăng ký cho WLC Tang 2



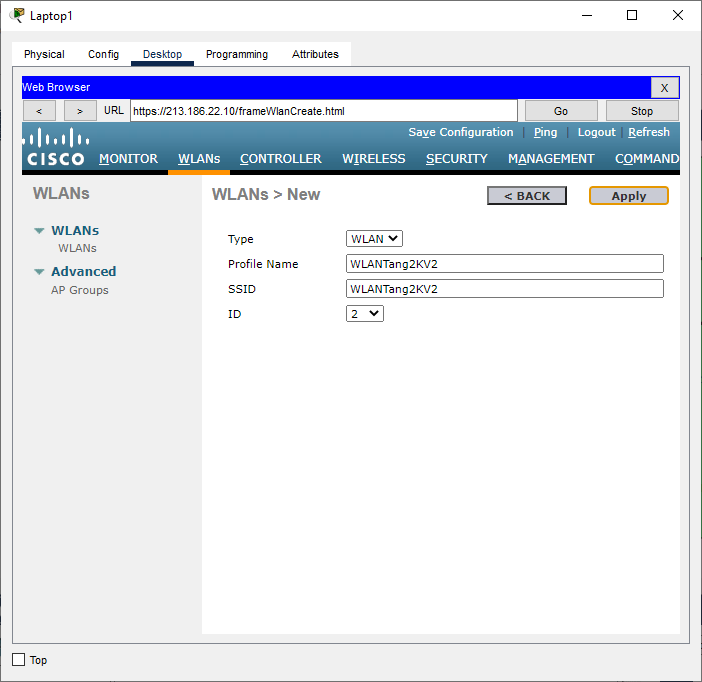
Hình 3.2.20. Kết quả đăng ký cho WLC Tang 2 (tiếp theo)

Vào trình duyệt của Laptop1, nhập địa chỉ IP là **213.186.22.10** và chọn phương thức https để tiếp tục. Lúc này trang đăng nhập sẽ xuất hiện, nhấn vào nút **Login** và nhập User Name và Password lần lượt là **adminT2** và **adminT2.**



Hình 3.2.21. Trang đăng nhập của WLC Tang 2.

Chọn tab WLANs, chọn Create News và nhấn vào nút Go. Nhập Profile Name và SSID là **WLANTang2KV2**. Nhấn vào **Apply** để lưu lại.



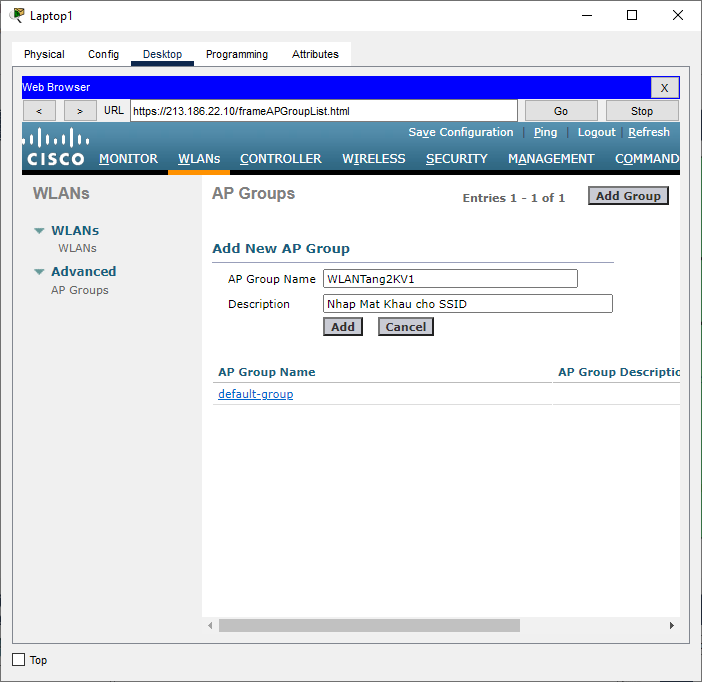
Hình 3.2.22. Tạo thêm mạng WLAN cho WLC Tang 2

Ở mục General, nút vào nút **Enabled** để kích hoạt mạng WLAN vừa mới tạo. Nhấn vào nút **Apply** để lưu lại cấu hình.



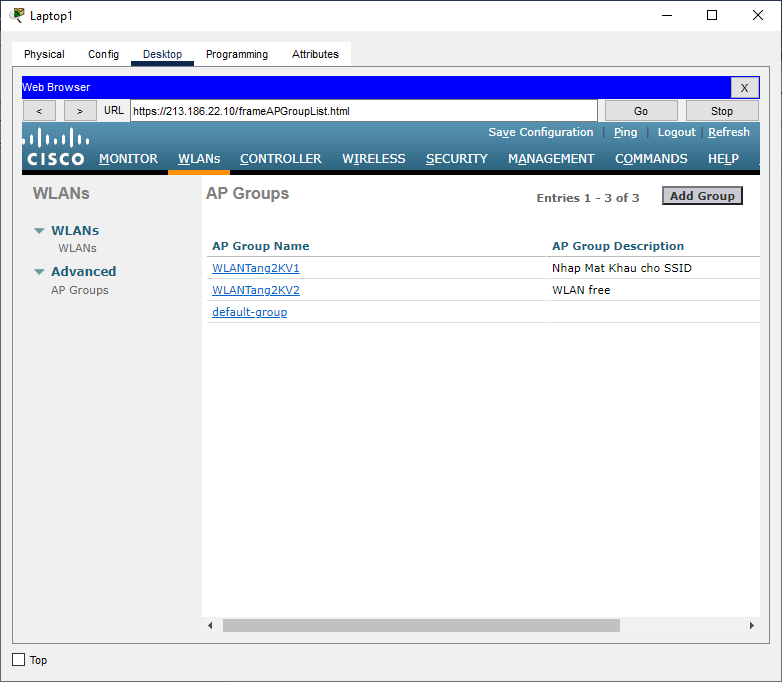
Hình 3.2.23. Chọn Enabled và nhấn vào nút Apply để lưu lại

Tạo Nhóm AP mới bằng cách nhấn vào tab WLANs và chọn AP Groups. Nhập WLANTang2KV1 và Nhap mat khau cho SSID cho mục AP Group Name và Description, sau đó nhấn vào nút **Add**.



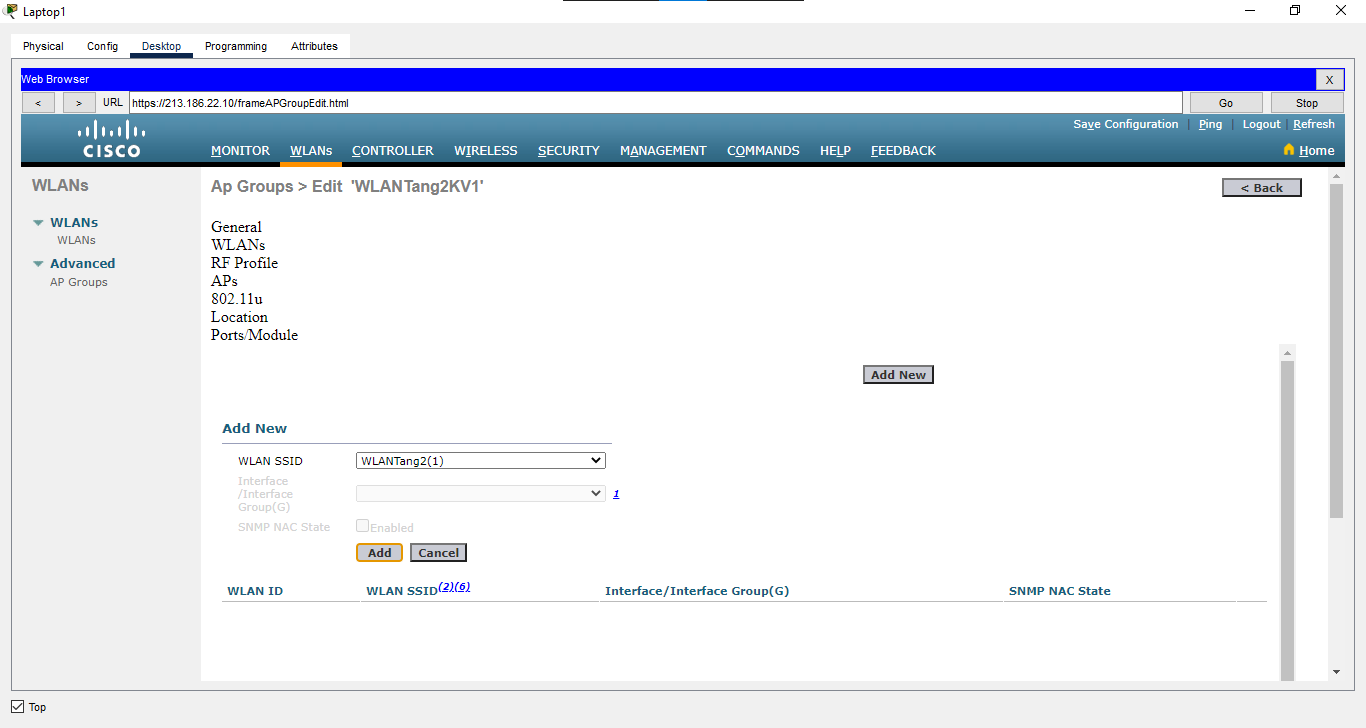
Hình 3.2.24. Tạo AP group mới cho WLC Tang 2

Làm theo các bước tương tự như ở trên cho **WLANTang2KV2**, ta có kết quả sau khi tạo nhóm:



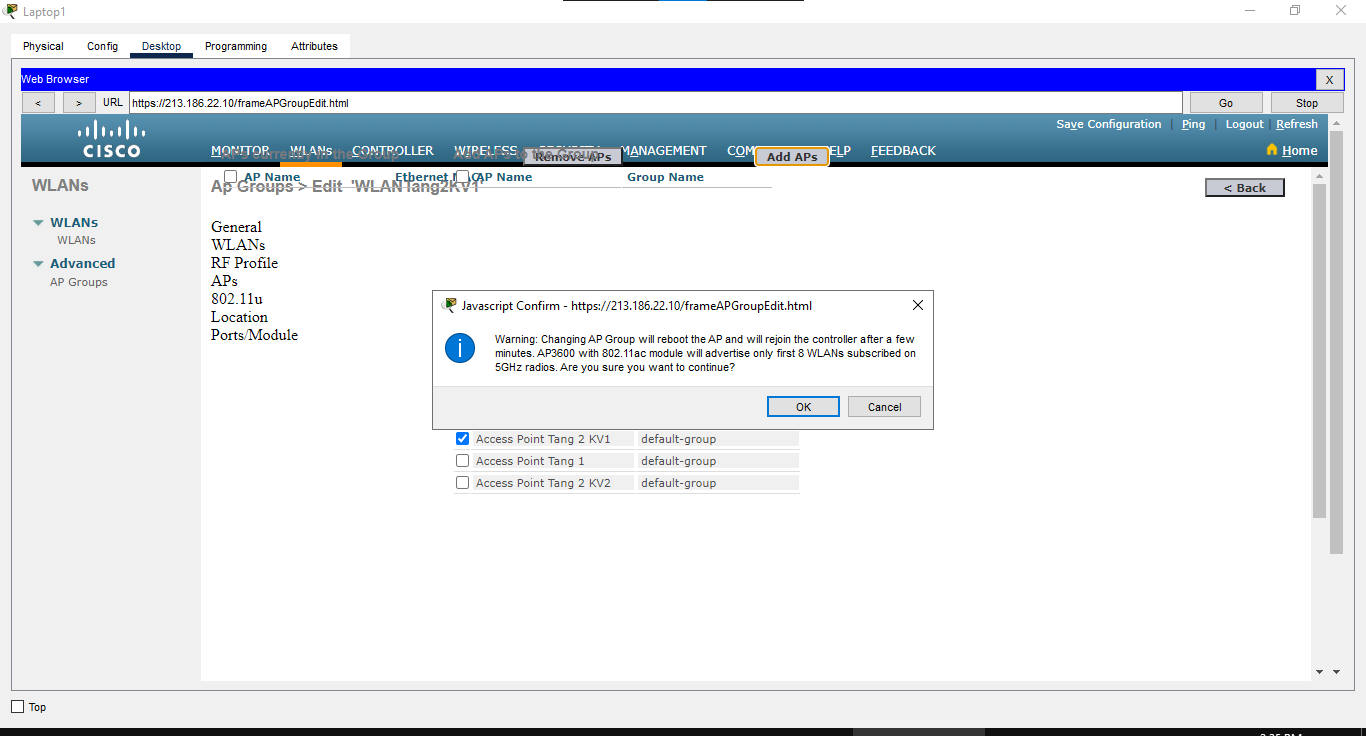
Hình 3.2.25. Kết quả tạo AP groups cho WLC Tang 2

Ở mục AP Groups, nhấn vào **WLANTang2KV1** và chọn mục WLANs, nhấn vào nút **Add New**, chọn WLAN SSID là **WLANTang2** và nhấn nút **Add**



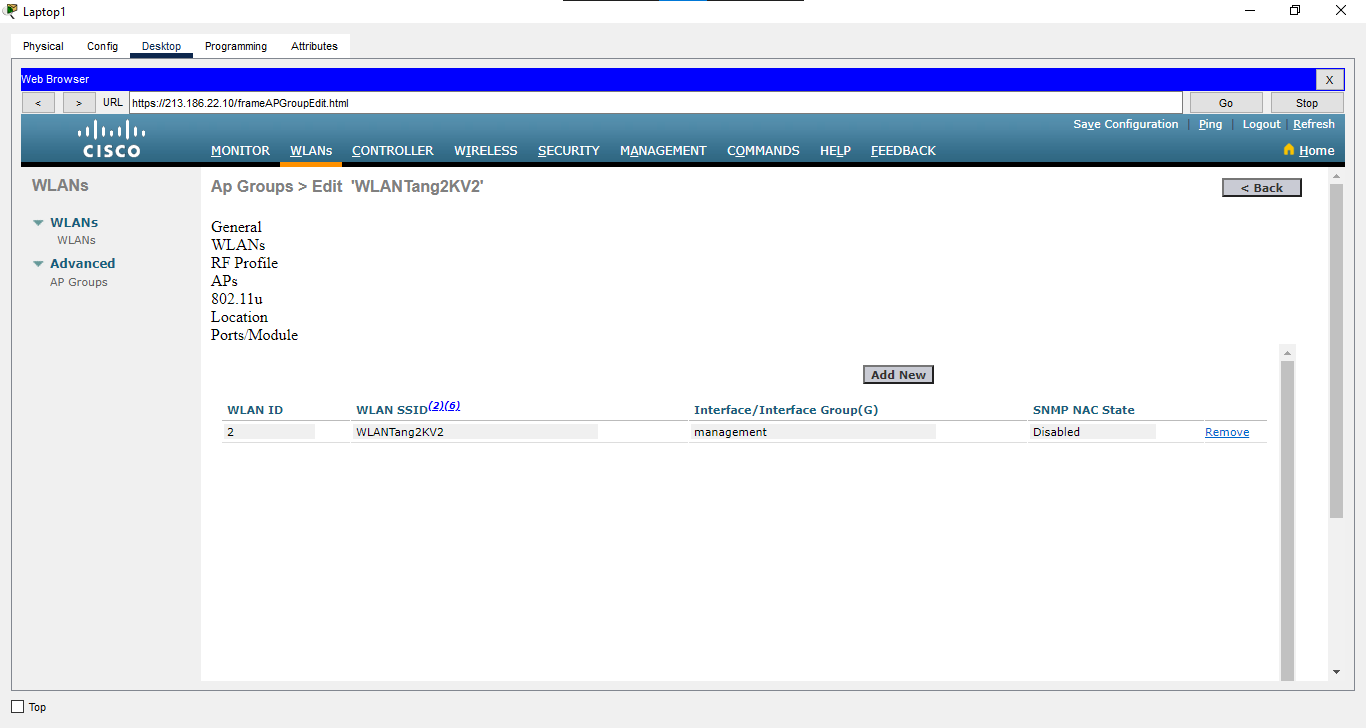
Hình 3.2.26. Thêm mạng WLANTang2 vào nhóm WLANTang2KV1

Tiếp tục nhấn vào mục **APs** và chọn **Access Point Tang 2 KV1** và nhấn vào nút **Add APs**, lúc này sẽ hiện lên thông báo, nhấn vào OK để lưu lại.

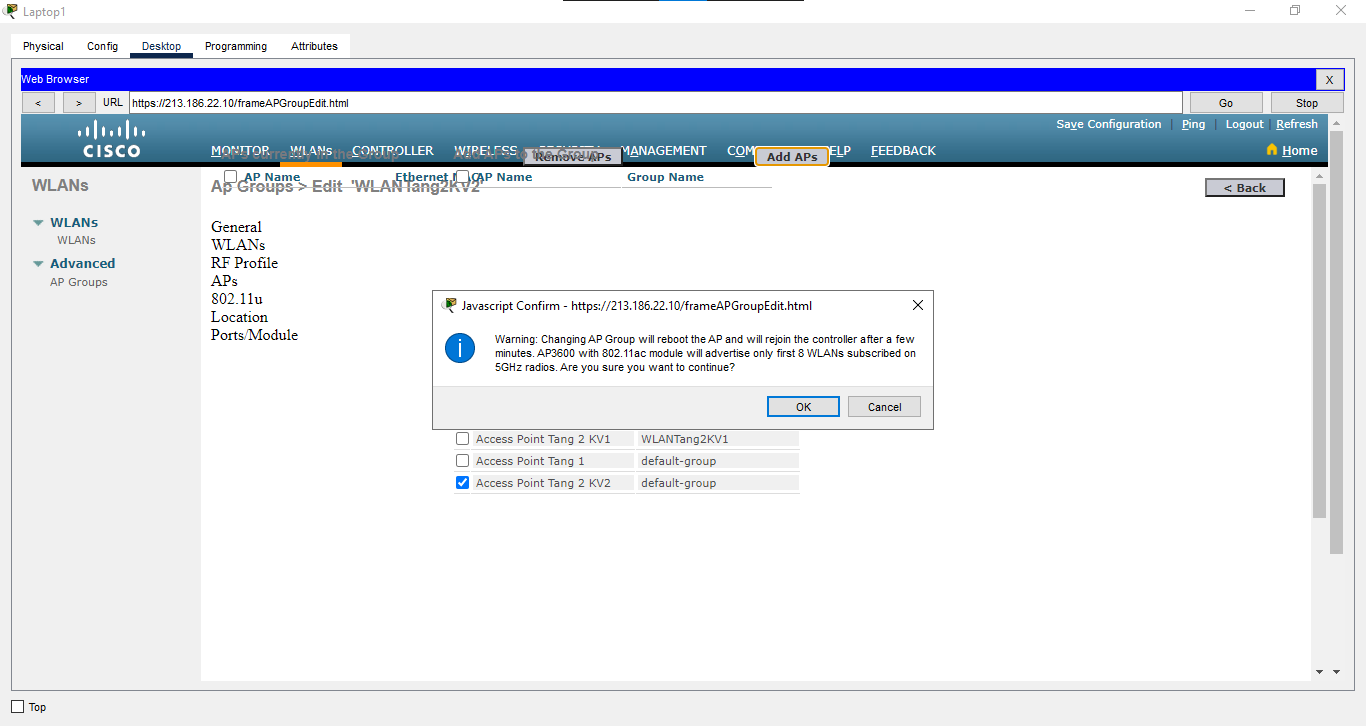


Hình 3.2.27. Thêm AP Access Point Tang 2 KV1 vào nhóm WLANTang2KV1

Làm theo các bước tương tự cho nhóm WLANTang2KV2. Ta có kết quả như sau:



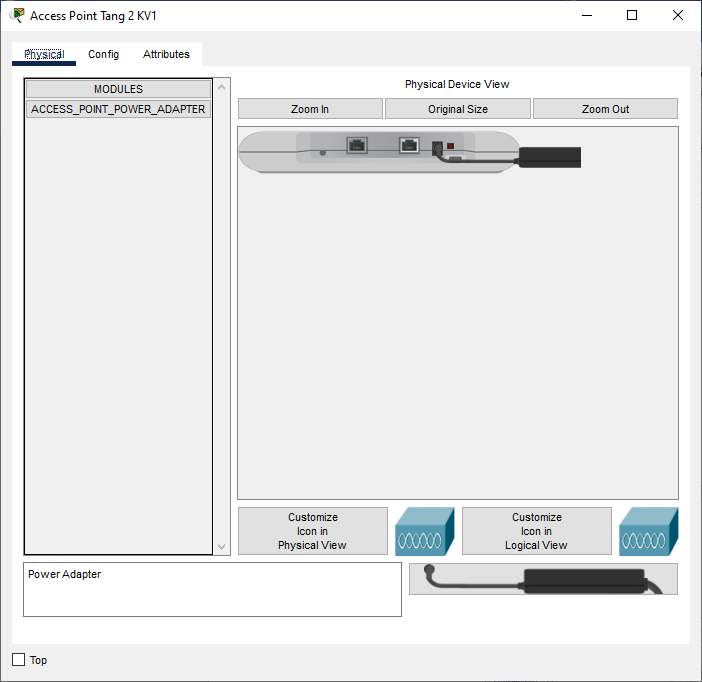
Hình 3.2.28. Thêm mạng WLANTang2KV2 vào nhóm WLANTang2KV2



Hình 3.2.29. Thêm AP Access Point Tang 2 KV2 vào nhóm WLANTang2KV2

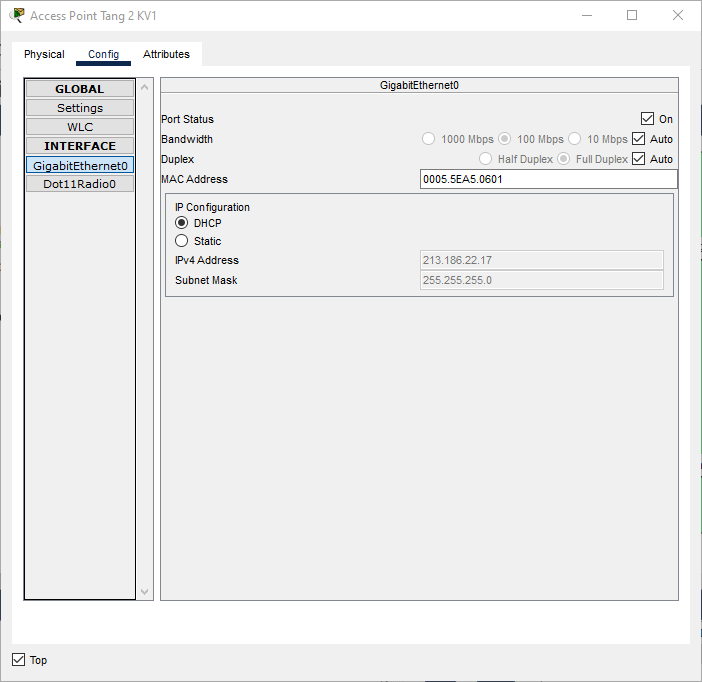
* + 1. Cấu hình AP Tầng 2 KV1

Nhấn vào tab Physical và kéo power adapter vào cái lỗ bên trái nút màu đỏ.



Hình 3.2.30. Gắn power adapter cho Access Point Tang 2 KV1.

Ở tab config, nhấn vào GigabitEthernet0 và nhấn vào DHCP.



Hình 3.2.31. Cấu hình địa chỉ cho Access Point Tang 2 KV1.

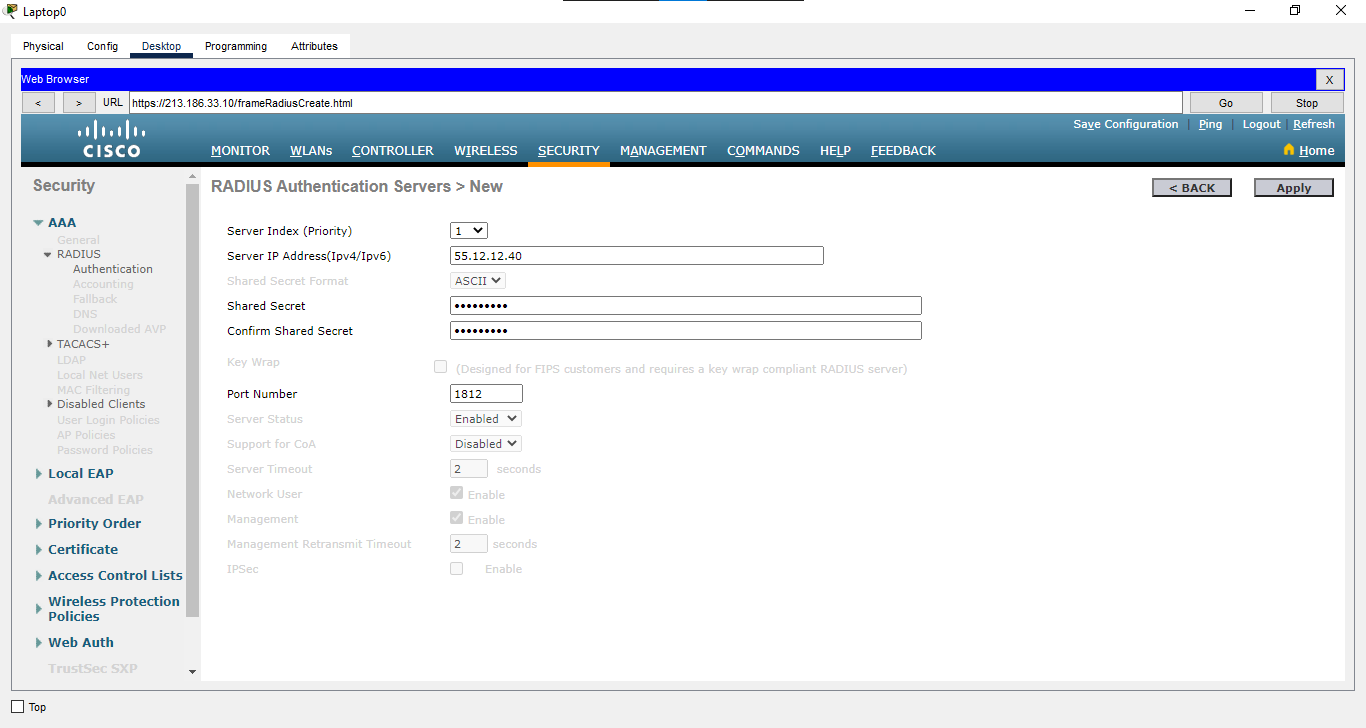
* + 1. Cấu hình AP Tầng 2 KV2

Thực hiện các bước cấu hình tương tự như AP Tầng 2 KV1 ở tab Physical và tab Config.

* + 1. Cấu hình WLC Tầng 3

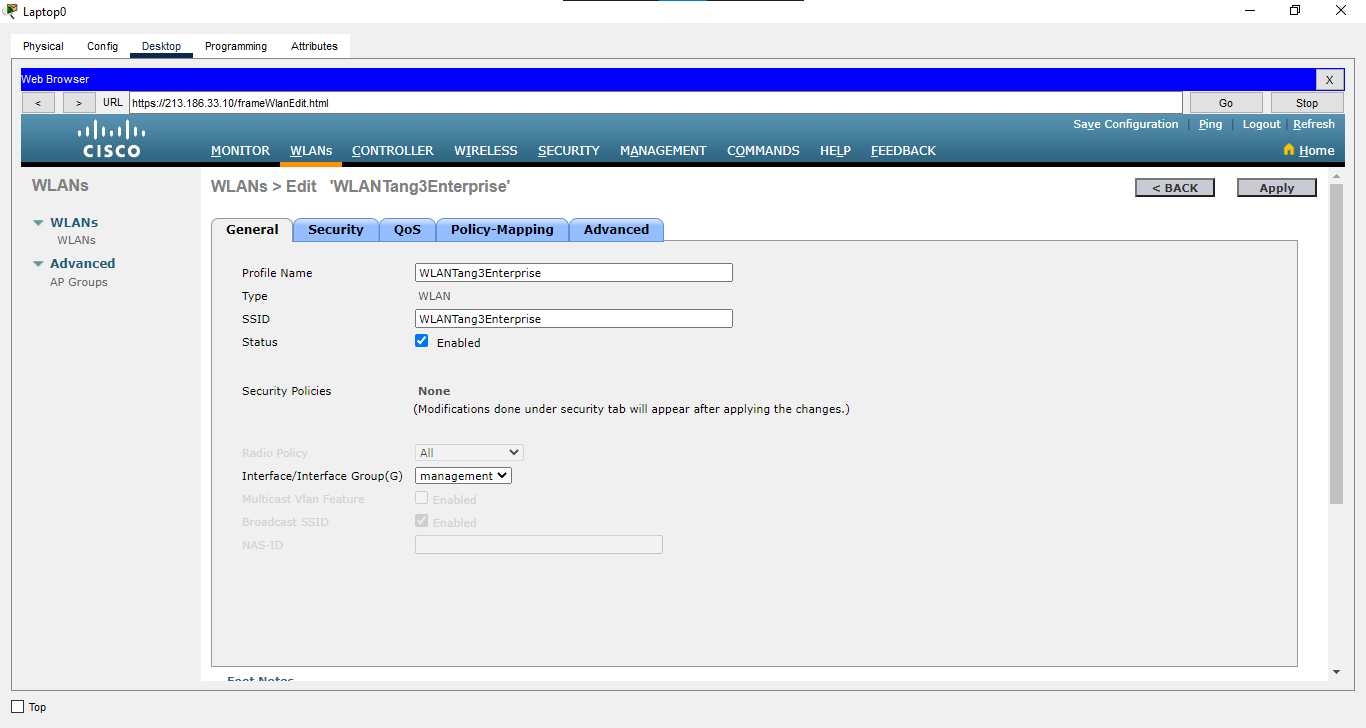
Các bước đăng ký thông tin, tạo WLAN sử dụng chuẩn WPA2 Personal, tạo và thêm groups AP thì tương tự như ở tầng 2 nên em tạm bỏ qua. Tới bước tạo WLAN sử dụng chuẩn WPA2 Enterprise.

Chọn tab Security và nhấn vào nút New. Nhập địa chỉ IP của máy chủ và mật khẩu có trong bảng thông tin.



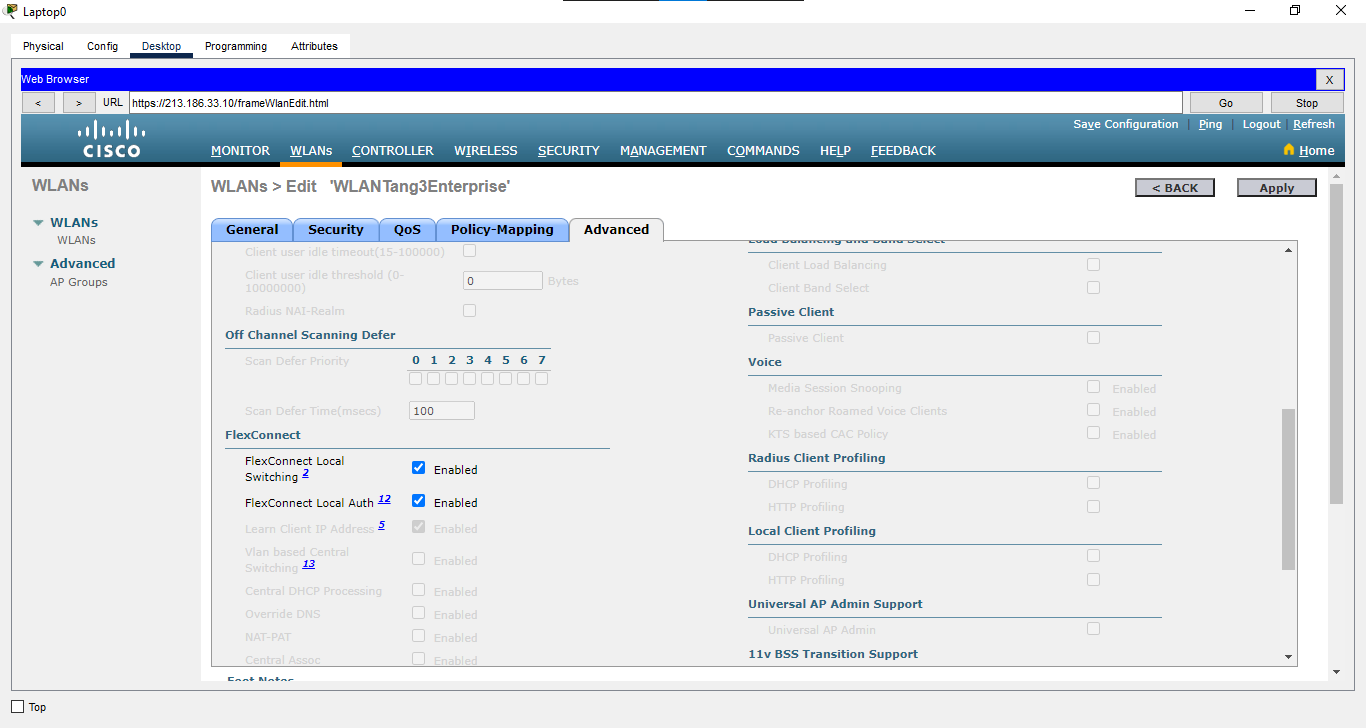
Hình 3.2.32. Cấu hình WPA2 Enterprise

Điền Profile Name và SSID lần lượt là **WLANTang3Enterprise.** Nhấn nút **Enabled** để kích hoạt mạng WLAN này.



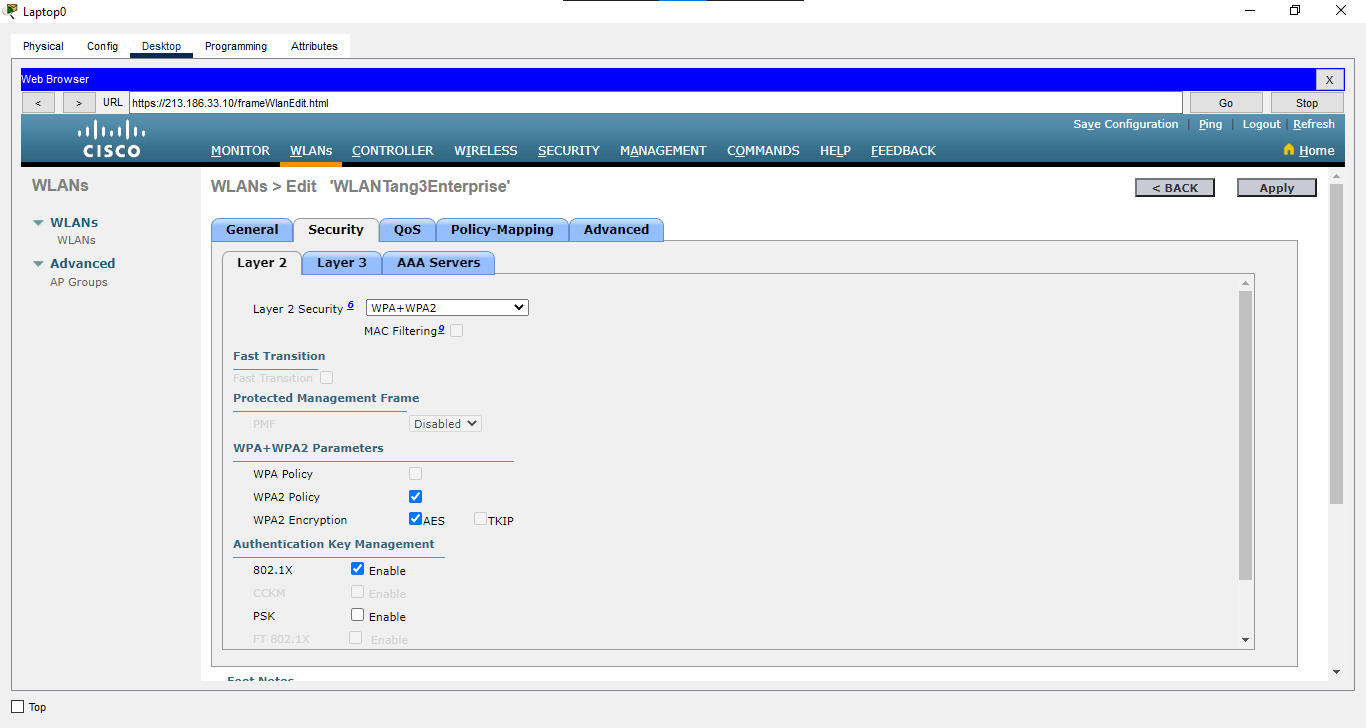
Hình 3.2.33. Cấu hình WPA2 Enterprise (tiếp theo)

Chuyển qua tab Advanced, kéo xuống dưới và đánh dấu tích ở 2 mục của FlexConnect.



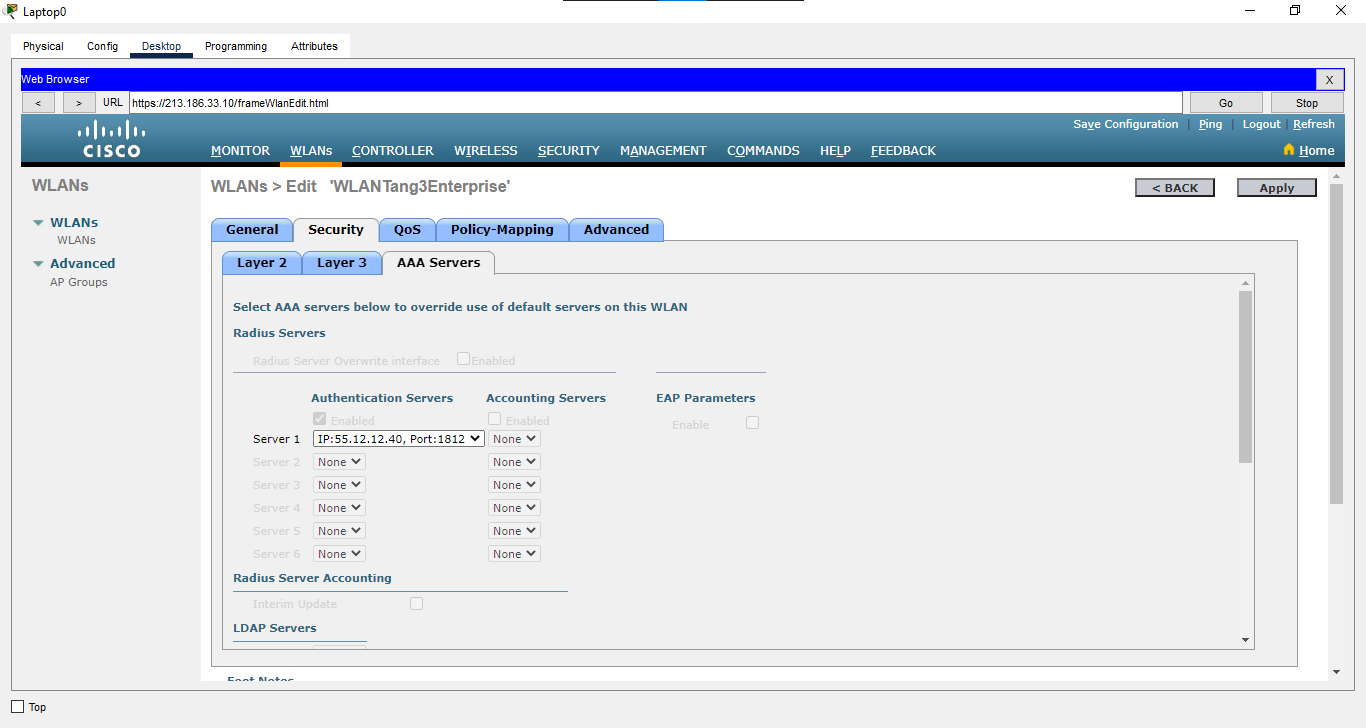
Hình 3.2.34. Cấu hình WPA2 Enterprise (tiếp theo)

Ở tab Security, chọn Layer 2 và chọn WPA+WPA2 cho Layer 2 Security. Nhấn vào nút Enabled ở 802.1X.



Hình 3.2.35. Cấu hình WPA2 Enterprise (tiếp theo)

Nhấn vào tab AAA Server và Chọn IP và cổng cho Server 1 và nhấn vào Apply để lưu lại cấu hình.



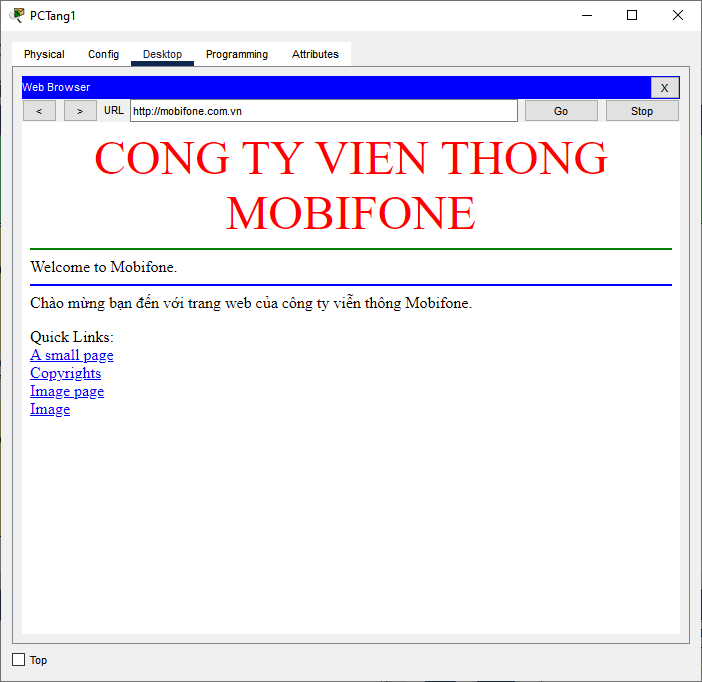
Hình 3.2.36. Cấu hình WPA2 Enterprise (tiếp theo)

* + 1. Cấu hình cho Access Point Tang 3 Personal và Access Point Tang 3 Enterprise

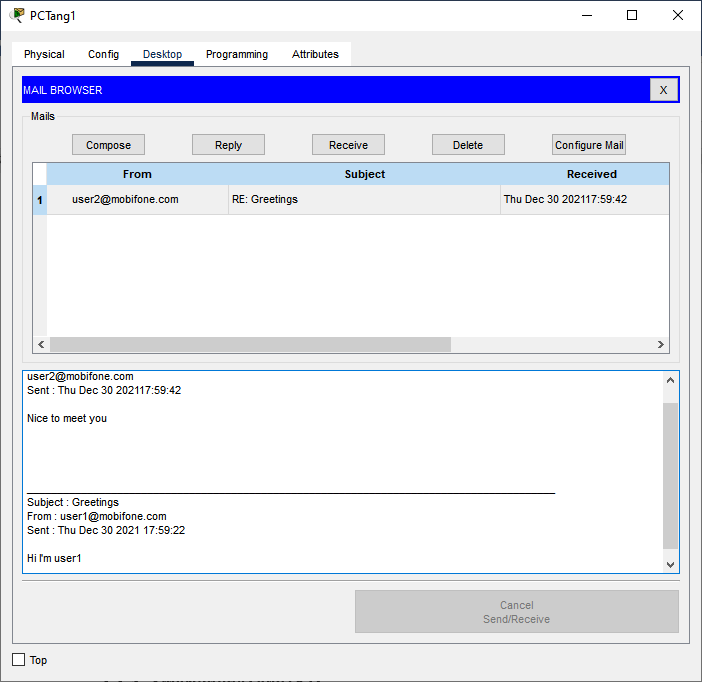
Thực hiện tương tự như cấu hình cho AP ở tầng 2.

* 1. Kết quả chạy chương trình
     1. PCTang1

PCTang1 có thể truy cập vào trang web mobifone.com.vn và thực hiện gửi và nhận mail với LaptopTang1.



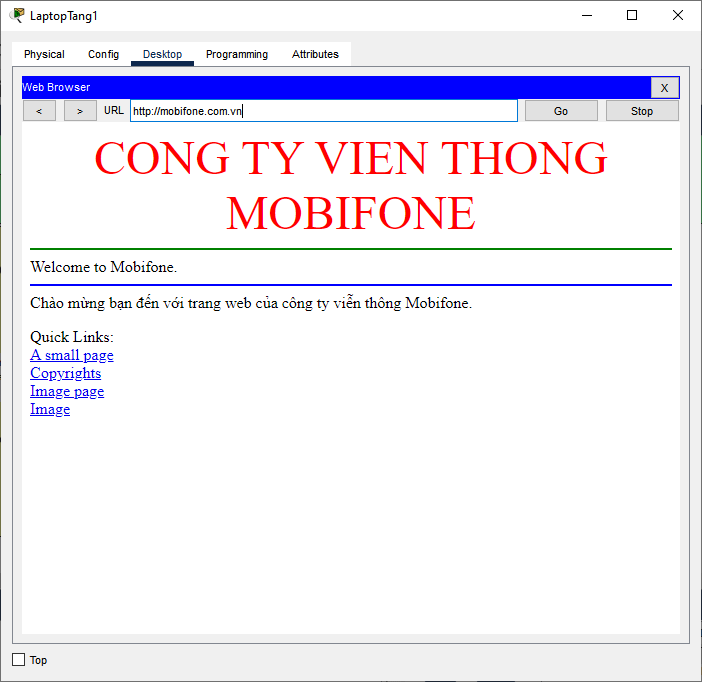
Hình 3.3.1. PCTang1 kết nối đến trang web mobifone.com.vn



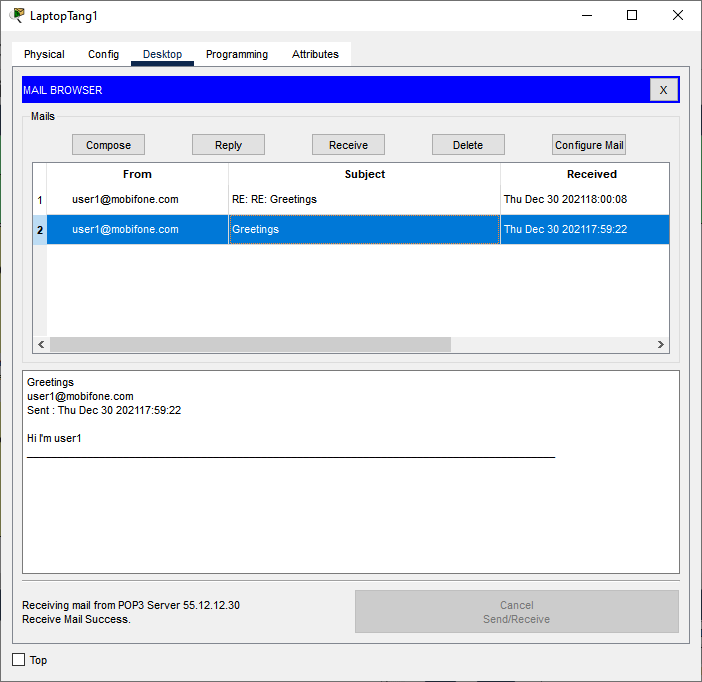
Hình 3.3.2. PCTang1 gửi và nhận mail đến LaptopTang1

* + 1. LaptopTang1

LaptopTang1 có thể truy cập vào trang web mobifone.com.vn và thực hiện gửi và nhận mail với PCTang1.



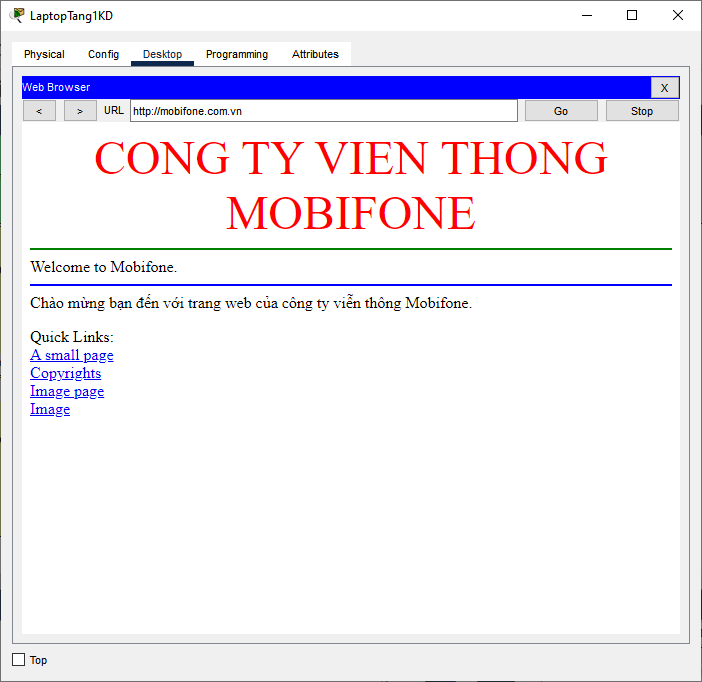
Hình 3.3.3. LaptopTang1 kết nối đến trang web mobifone.com.vn



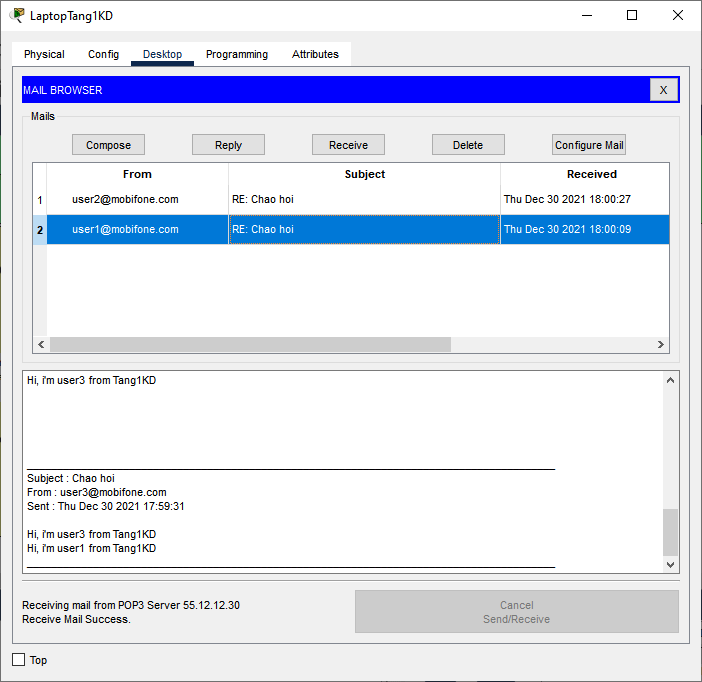
Hình 3.3.4. LaptopTang1 gửi và nhận mail đến PCTang1

* + 1. LaptopTang1KD

LaptopTang1KD có thể truy cập vào trang web mobifone.com.vn và thực hiện gửi và nhận mail với SmartphoneTang1KD và TabletTang1KD.



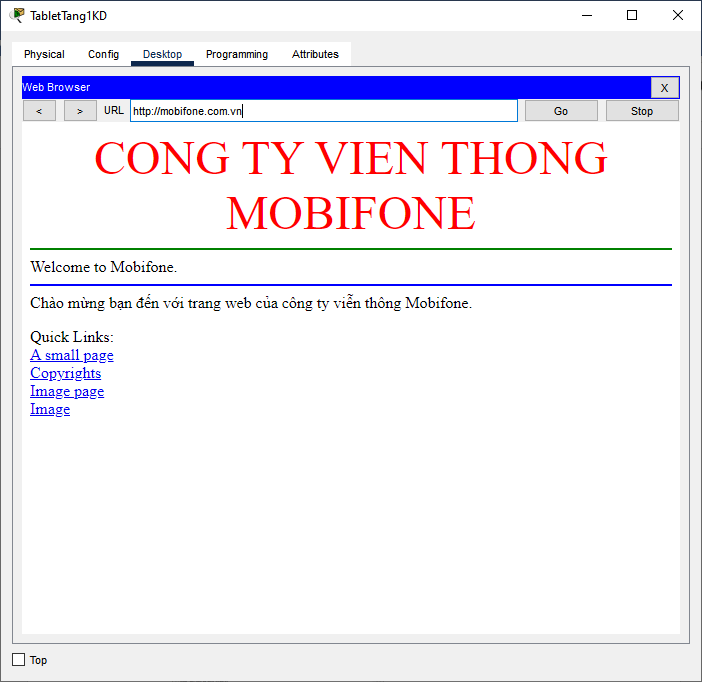
Hình 3.3.5. LaptopTang1KD kết nối đến trang web mobifone.com.vn



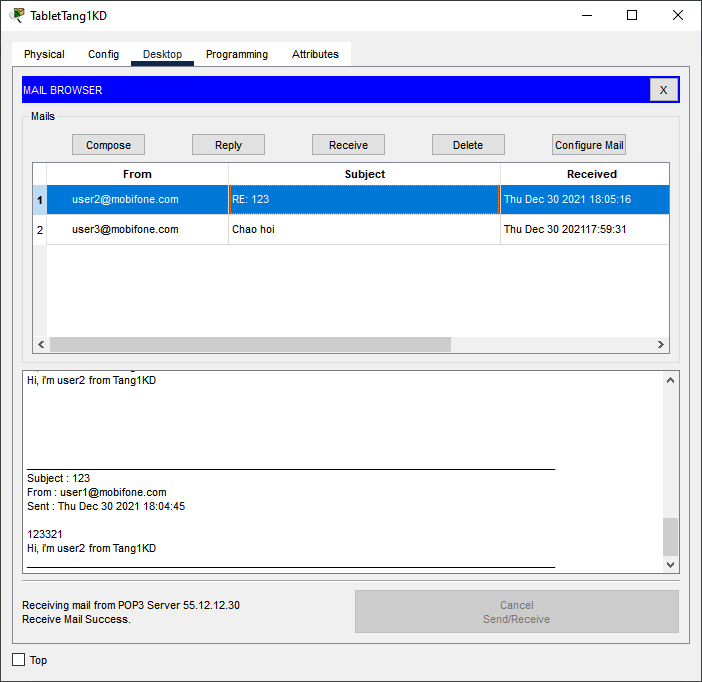
Hình 3.3.6. LaptopTang1KD gửi và nhận mail đến SmartphoneTang1KD và TabletTang1KD

* + 1. TabletTang1KD

TabletTang1KD có thể truy cập vào trang web mobifone.com.vn và thực hiện gửi và nhận mail với SmartphoneTang1KD và LaptopTang1KD.



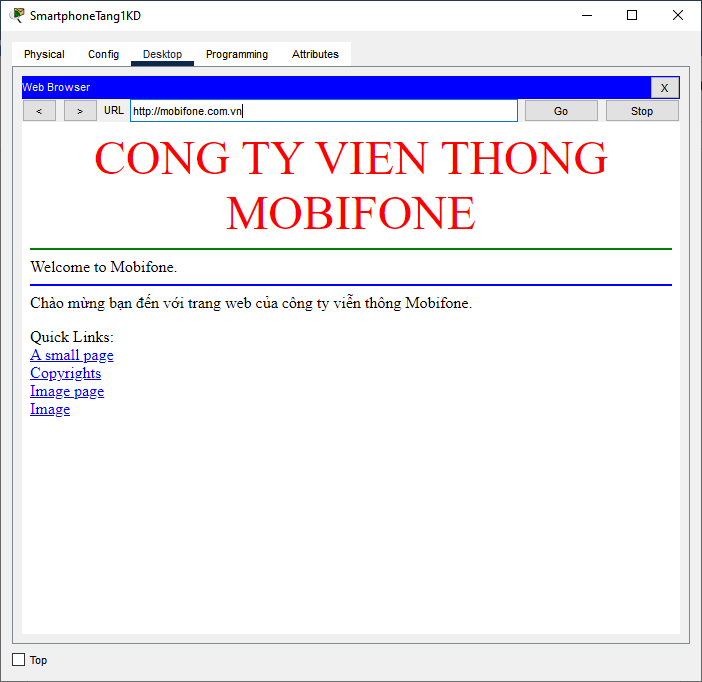
Hình 3.3.7. TabletTang1KD kết nối đến trang web mobifone.com.vn



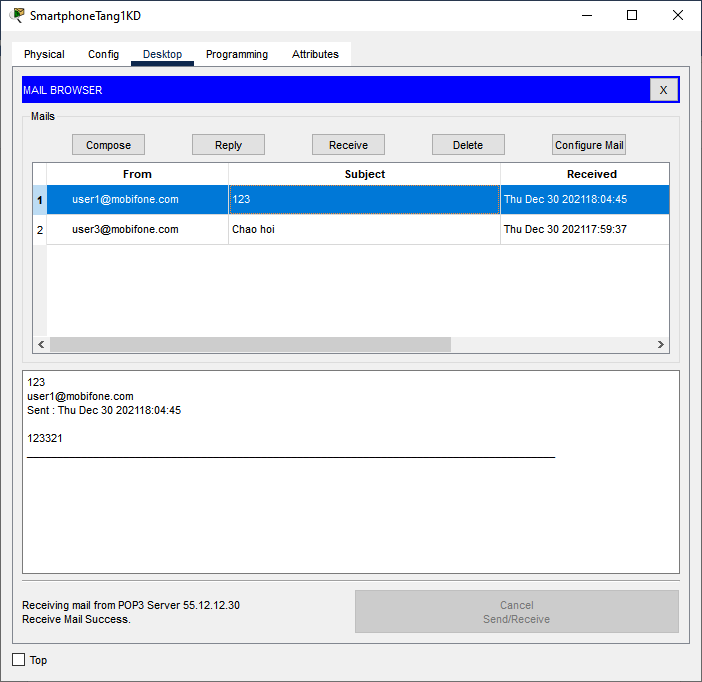
Hình 3.3.8. TabletTang1KD gửi và nhận mail đến SmartphoneTang1KD và LaptopTang1KD

* + 1. SmartphoneTang1KD

SmartphoneTang1KD có thể truy cập vào trang web mobifone.com.vn và thực hiện gửi và nhận mail với TabletTang1KD và LaptopTang1KD.



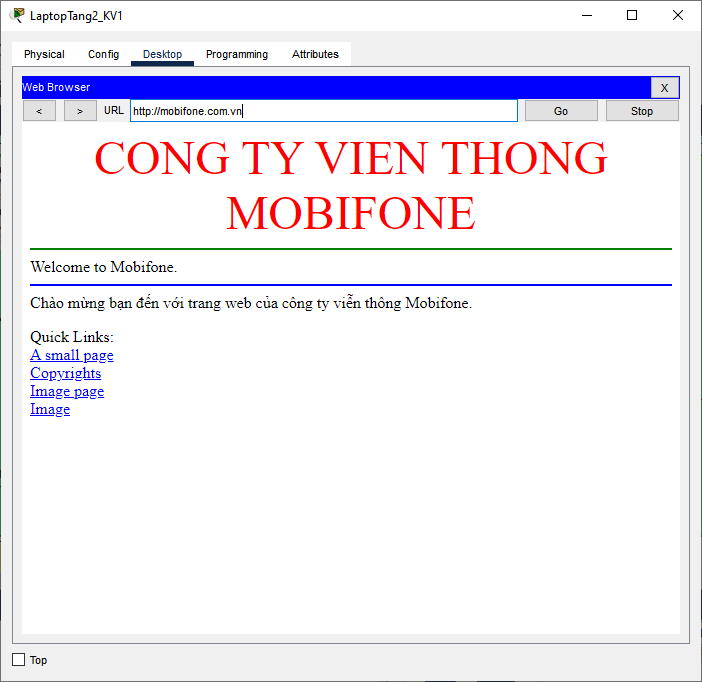
Hình 3.3.9. SmartphoneTang1KD kết nối đến trang web mobifone.com.vn



Hình 3.3.8. SmartphoneTang1KD gửi và nhận mail đến TabletTang1KD và LaptopTang1KD

* + 1. LaptopTang2\_KV1

Có thể kết nối đến trang web mobifone.com.vn và thực hiện gửi và nhận mail



Hình 3.3.9. LaptopTang2\_KV1 kết nối đến trang web mobifone.com.vn



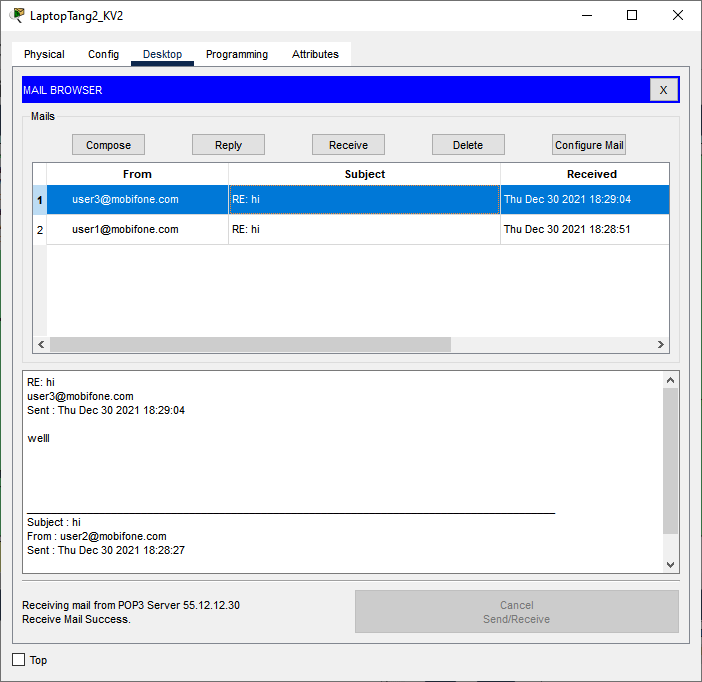
Hình 3.3.10. LaptopTang2\_KV1 gửi và nhận mail đến các thiết bị có kết nối vào điểm truy cập mạng

* + 1. LaptopTang2\_KV2

Có thể kết nối đến trang web mobifone.com.vn và thực hiện gửi và nhận mail, và các thiết bị mạng có kết nối đến AP Tang 2 KV1 cũng tương tự như vậy.



Hình 3.3.11. LaptopTang2\_KV2 kết nối đến trang web mobifone.com.vn



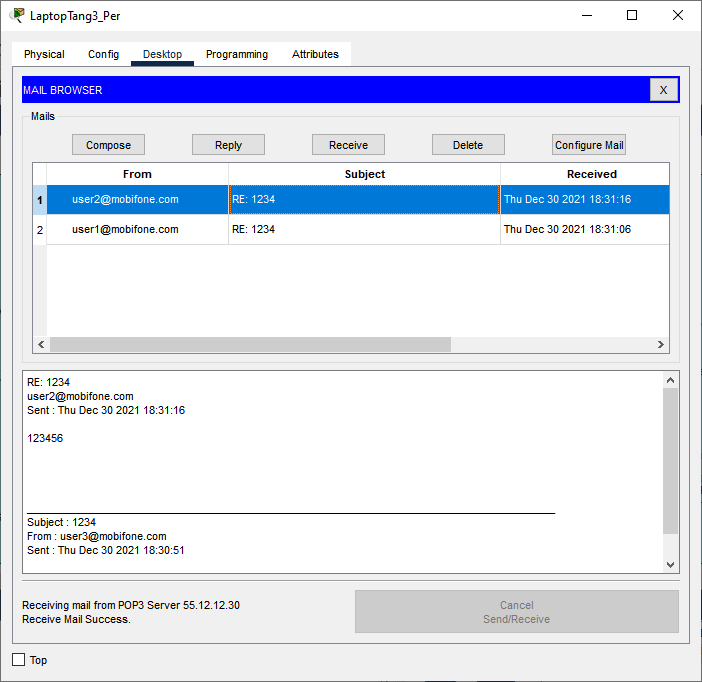
Hình 3.3.12. LaptopTang2\_KV2 gửi và nhận mail đến các thiết bị có kết nối vào điểm truy cập mạng

* + 1. LaptopTang3\_Per

Có thể kết nối đến trang web mobifone.com.vn và thực hiện gửi và nhận mail, và các thiết bị mạng kết nối đến AP Tang 3 Personal cũng tương tự như vậy.



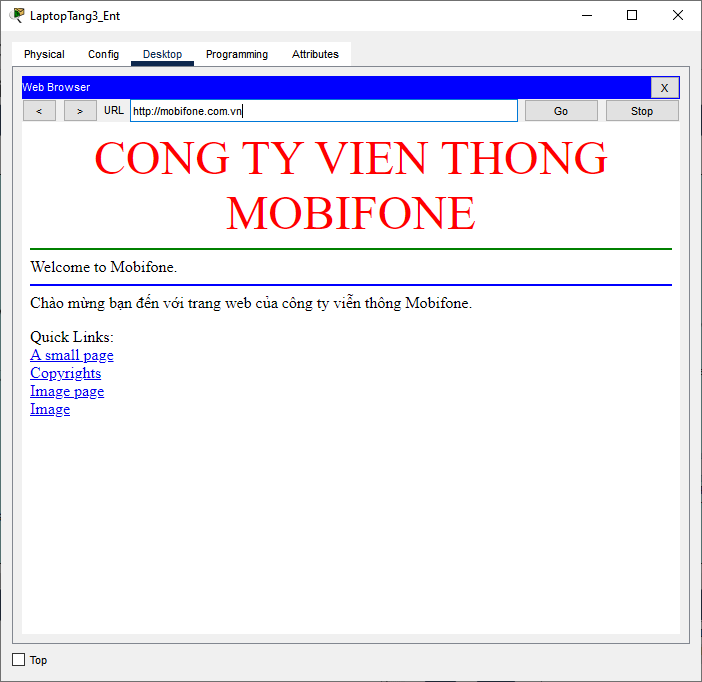
Hình 3.3.11. LaptopTang3\_Per kết nối đến trang web mobifone.com.vn



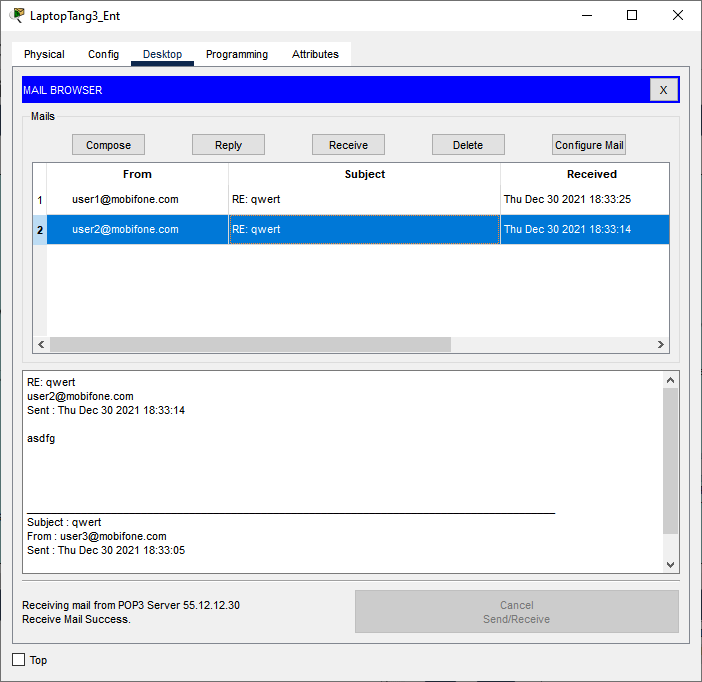
Hình 3.3.14. LaptopTang3\_Per gửi và nhận mail đến các thiết bị có kết nối vào điểm truy cập mạng

* + 1. LaptopTang3\_Ent

Có thể kết nối đến trang web mobifone.com.vn và thực hiện gửi và nhận mail, và các thiết bị mạng kết nối đến AP Tang 3 Enterprise cũng tương tự như vậy.



Hình 3.3.15. LaptopTang3\_Per kết nối đến trang web mobifone.com.vn



Hình 3.3.16. LaptopTang3\_Ent gửi và nhận mail đến các thiết bị có kết nối vào điểm truy cập mạng

1. Kết luận

Tổng kết, sau khi tìm hiểu về cách hoạt động của mạng WLAN cũng như đã hiểu về yêu cầu của khách hàng, nhóm em đã xây dựng được một hệ thống mạng 3 tầng với 1 phòng server trong bài chúng em đã thiết lập mạng WLAN sử dụng phương thức bảo mật WPA2 presonal và WPA2 Enterprise, tạo DHCP pool, cấu hình định tuyến động OSPF, web-server, mail-server, DNS-server, RADIUS server cũng như thêm vào các thiết bị IOT cũng như quản lý chúng qua web phù hợp với những điều trên và sau khi thực hiện xong mô hình mạng thì em cũng hiểu thêm về những khó khăn trong việc xây dựng hoàn chỉnh một mô hình mạng WLAN cũng như cách cấu hình chúng. Trong bài chúng em chỉ làm được tầm 80% so với kế hoạch đề ra từ trước do nhiều vần đề phát sinh trong lúc làm vì vậy chúng em mong thầy có đánh giá nhận xét khách quan để chúng em có thể sửa chữa cũng như chuẩn bị tốt hơn cho các môn học sau cũng như công việc sau này.

TÀI LIỆU THAM KHẢO

Tiếng Việt

1. <https://vi.wikipedia.org/wiki/M%E1%BA%A1ng_m%C3%A1y_t%C3%ADnh>
2. <https://quantrimang.com/wifi-la-gi-120057>
3. <https://www.dienmayxanh.com/kinh-nghiem-hay/wifi-la-gi-596329>
4. <https://bkaii.com.vn/tin-tuc/308-nguyen-li-hoat-dong-cua-mang-khong-day>
5. <http://legiacong.blogspot.com/2012/03/wireless-network3cac-ung-dung-cua-wlan.html>
6. <https://www.dienmayxanh.com/kinh-nghiem-hay/wep-wpa-wpa2-la-gi-dau-la-chuan-bao-mat-wifi-tot-n-1215377>
7. <https://netsystem.vn/router-la-gi-bo-dinh-tuyen-router-hoat-dong-nhu-nao/>
8. <https://www.totolink.vn/article/85-switch-la-gi-cong-dung-cua-thiet-bi-chuyen-mach.html>
9. <https://www.totolink.vn/article/158-so-sanh-su-khac-nhau-giua-switch-layer-2-va-switch-layer-3.html>
10. <https://quantrimang.com/vlan-la-gi-lam-the-nao-de-cau-hinh-mot-vlan-tren-switch-cisco-64830>
11. https://quantrimang.com/dhcp-giao-thuc-cau-hinh-host-dong-la-gi-149708

Tiếng Anh

1. <https://en.wikipedia.org/wiki/Wireless_network>
2. <https://en.wikipedia.org/wiki/Wireless_LAN>
3. <https://phoenixnap.com/blog/prevent-ddos-attacks>
4. Lab 5. Configure a Basic WLAN on the WLC
5. Lab 6. Configure a WPA2 Enterprise WLAN on the WLC