TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM

**TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

**KHOA CÔNG NGHỆ THÔNG TIN**



**BÁO CÁO MÔN HỌC**

**WIRELESS AND MOBILE NETWORK SECURITY**

**Tên chủ đề**

**Xây Dựng Hệ Thống Mạng Không Dây Cho Công Ty TTN**

Người hướng dẫn: Ts Bùi Quy Anh

Người thực hiện: Trần Thảo Nguyên - 51801001

Lớp: 18050401

Khoá: 22

**THÀNH PHỐ HỒ CHÍ MINH, NĂM 2021**

LỜI CẢM ƠN

Em xin chân thành gửi lời cảm ơn đến thầy Bùi Quy Anh đã tận tình giảng dạy và giải đáp những thắc mắc cho sinh viên chúng em, mặc dù tình hình dịch bệnh đã gây ảnh hưởng ít nhiều đến chất lượng giảng dạy nhưng thầy đã rất nhiệt tình qua các bài giảng online giúp em có cơ sở vững chắc về lý thuyết cũng như các bài lab thực hành. Qua bài báo cáo cuối môn này giúp em tổng kết những kiến thức về môn học cũng như áp dụng những kiến thức đó như thế nào. Có thể kiến thức của em còn hạn hẹp và còn nhiều sai sót mong thầy góp ý để em có thể hoàn thiện hơn.

Em xin chân thành cảm ơn thầy.

**BÁO CÁO ĐƯỢC HOÀN THÀNH**

**TẠI TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

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

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

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

*TP. Hồ Chí Minh, ngày 21 tháng 12 năm 2021*

*Tác giả*



*Trần Thảo Nguyên*

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

Với sự phát triển rộng lớn của công nghệ hiện nay, đặc biệt là sự tăng trưởng mạnh mẽ của internet và các dịch vụ trực tuyến. Mạng không dây là một trong những lựa chọn hàng đầu của mọi người dùng cá nhân cũng như các tổ chức trên toàn cầu. Qua đề tài xây hệ thống mạng không dây cho doanh nghiệp cụ thể là một công ty có quy mô gồm 4 phòng ban được thiết kế demo trên phần mềm Packet Tracer. Em đã xây dựng hệ thống mạng cho mỗi phòng ban của công ty sử dụng một mạng WLAN riêng và cả mạng WLAN dung chung cùng với cấu hình cài đặt bảo mật cho mỗi WLAN. Em cấu hình các máy khách cụ thể là các thiết bị của người dùng có thể kết nối mạng không dây và có thể giao tiếp với nhau và với internet và để đảm bảo bảo mật em bảo mật mạng WLAN bằng WPA-2 802.1x/Enterprise và WPA-2 PSK/Personal. Thông qua cấu hình WLC để sử dụng RADIUS server doanh nghiệp để xác thực người dùng cũng như quản lý tập trung các access point.

MỤC LỤC

[LỜI CẢM ƠN ii](#_Toc91508838)

[PHẦN XÁC NHẬN VÀ ĐÁNH GIÁ CỦA GIẢNG VIÊN iv](#_Toc91508839)

[TÓM TẮT v](#_Toc91508840)

[MỤC LỤC 1](#_Toc91508841)

[MỤC CÁC BẢNG BIỂU, HÌNH VẼ 3](#_Toc91508842)

[CHƯƠNG 1 – MÔ TẢ ĐỀ TÀI 6](#_Toc91508843)

[1.1 Yêu cầu khách hàng 6](#_Toc91508844)

[1.2 Đề xuất hướng giải quyết 6](#_Toc91508845)

[CHƯƠNG 2 – CƠ SỞ LÝ THUYẾT 7](#_Toc91508846)

[2.1 Các khái niệm cơ bản 7](#_Toc91508847)

[2.1.1 Khái niệm mạng máy tính 7](#_Toc91508848)

[2.1.2 Khái niệm mạng không dây 7](#_Toc91508849)

[2.1.2.1 Các mô hình mạng không dây 7](#_Toc91508850)

[2.1.2.2 Các chuẩn mạng không dây 8](#_Toc91508851)

[2.1.3 Khái niệm an toàn bảo mật không dây 9](#_Toc91508852)

[2.1.3.1 Các hình thức tấn công mạng WLAN 9](#_Toc91508853)

[2.1.3.2 Các phương pháp bảo mật cơ bản trong WLAN 10](#_Toc91508854)

[2.2 Các thiết bị dây dựng mạng 11](#_Toc91508855)

[2.2.1 Router 11](#_Toc91508856)

[2.2.2 Switch 12](#_Toc91508857)

[2.2.3 Thiết bị phát wifi 12](#_Toc91508858)

[2.2.4 Máy chủ 12](#_Toc91508859)

[2.2.5 Cáp mạng 12](#_Toc91508860)

[2.2.6 Thiết bị máy khách 12](#_Toc91508861)

[CHƯƠNG 3 – MÔ HÌNH DEMO 13](#_Toc91508862)

[3.1 Mô hình đề xuất 13](#_Toc91508863)

[3.1.1 Bảng địa chỉ 13](#_Toc91508864)

[3.1.1 Bảng thông tin WLAN 15](#_Toc91508865)

[3.2 Cấu hình các thiết bị 16](#_Toc91508866)

[3.2.1 Trên router R1 16](#_Toc91508867)

[3.2.2 Trên switch core SW1 18](#_Toc91508868)

[3.2.2 Trên Radius Server 20](#_Toc91508869)

[3.2.4 Trên WLC TTN-Company 21](#_Toc91508870)

[3.2.5 Trên các thiết bị máy khách 39](#_Toc91508871)

[3.2.6 Cấu hình ngoài Internet 49](#_Toc91508872)

[3.3 Kết quả chạy chương trình 54](#_Toc91508873)

[3.3.1 Kiểm tra kết nối giữa các thiết bị với nhau. 54](#_Toc91508874)

[3.3.2 Kiểm tra kết nối giữa các thiết bị đến Web Server 56](#_Toc91508875)

[CHƯƠNG 4 – KẾT LUẬN 60](#_Toc91508876)

[TÀI LIỆU THAM KHẢO 61](#_Toc91508877)

MỤC CÁC BẢNG BIỂU, HÌNH VẼ

**DANH MỤC HÌNH**

[Hình 3.1: Mô hình đề xuất 13](#_Toc91507256)

[Hình 3.2: Cấu hình địa chỉ IP cho router R1 16](#_Toc91507257)

[Hình 3.3: Cấu hình tạo DHCP cho router R1 17](#_Toc91507258)

[Hình 3.4: Các Vlan đã tạo trên SW1 18](#_Toc91507259)

[Hình 3.5: Cấu hình trunk trên SW1 19](#_Toc91507260)

[Hình 3.6: Cấu hình AAA trên Radius Server 20](#_Toc91507261)

[Hình 3.7: Thông tin về WLC 21](#_Toc91507262)

[Hình 3.8: Giao diện chính của WLC 27](#_Toc91507263)

[Hình 3.9: Các interface đã khởi tạo trên WLC 30](#_Toc91507264)

[Hình 3.10: Các WLAN đã khởi tạo trên WLC 36](#_Toc91507265)

[Hình 3.11: Tạo các group cho Access Point 38](#_Toc91507266)

[Hình 3.12: Cài đặt địa chỉ IP cho router R0 49](#_Toc91507267)

[Hình 3.13: Cấu hình IP route 50](#_Toc91507268)

[Hình 3.14: Đặt địa chỉ cho Web Server 51](#_Toc91507269)

[Hình 3.15: Đặt địa chỉ cho DNS Server 52](#_Toc91507270)

[Hình 3.16: Cấu hình phân giải tên miền cho Web Server 53](#_Toc91507271)

[Hình 3.17: Kiểm tra kết nối giữa 2 máy dùng mạng riêng của phòng kỹ thuật 54](#_Toc91507272)

[Hình 3.18: Kiểm tra kết nối giữa 2 máy dùng mạng chung cho khách 54](#_Toc91507273)

[Hình 3.19: Kiểm tra kết nối giữa máy phòng kỹ thuật và máy phòng kế toán 55](#_Toc91507274)

[Hình 3.20: Kiểm tra kết nối giữa máy phòng kinh doanh và máy phòng lễ tân 55](#_Toc91507275)

[Hình 3.21: Kiểm tra kết nối giữa máy phòng kinh doanh và máy phòng kế toán 55](#_Toc91507276)

[Hình 3.21: Kết nối máy từ phòng kỹ thuật đến Web Server 56](#_Toc91507277)

[Hình 3.22: Kết nối máy từ phòng kế toán đến Web Server 57](#_Toc91507278)

[Hình 3.22: Kết nối máy từ phòng kinh doanh đến Web Server 58](#_Toc91507279)

[Hình 3.23: Kết nối máy từ phòng lễ tân đến Web Server 59](#_Toc91507280)

**DANH MỤC BẢNG**

[Bảng 1.1: Danh sách thiết bị cần lắp đặt 5](#_Toc91460035)

[Bảng 3.1: Bảng địa chỉ 13](#_Toc91460036)

[Bảng 3.2: Bảng thông tin WLAN 13](#_Toc91460037)

**DANH MỤC KÍ HIỆU VÀ CHỮ VIẾT TẮT**

**CÁC CHỮ VIẾT TẮT**

AP: Access Point

WLC: Wireless LAN Controller

WLAN: Wireless LAN

IEEE: Institute of Electrical and Electronics Engineers

CHƯƠNG 1 – MÔ TẢ ĐỀ TÀI

Đề tài về thiết kế mô hình mạng không dây cho công ty TTN gồm 4 phòng ban.

1.1 Yêu cầu khách hàng

Mỗi phòng ban có đều có access point có thể phát wifi sử dụng cho riêng cho nhân viên mỗi phòng ban và cả wifi có thể dùng chung cho cả khách, bảo mật cho mỗi mạng WLAN phải cao nhất và mức chi phí hợp lý.

1.2 Đề xuất hướng giải quyết

|  |  |  |
| --- | --- | --- |
| **Thiết bị** | **Số lượng** | **Giá thành**  **(đồng)** |
| Router  (ISR 4331) | 2 | 46.300.000 x 2 |
| Switch core  (3650 - 24PS) | 1 | 33.000.000 |
| Máy chủ Server | 3 | 30.000.000 x 3 |
| WLC  (WLC – 3504) | 1 | 50.000.000 |
| Access point  (3702i) | 4 | 4.000.000 x 4 |
| Tiền công lắp đặt | | 10.000.000 |
| Tổng chi phí | | 281.600.000 |

Bảng 1.1: Danh sách thiết bị cần lắp đặt

CHƯƠNG 2 – CƠ SỞ LÝ THUYẾT

2.1 Các khái niệm cơ bản

2.1.1 Khái niệm mạng máy tính

Mạng máy tính là sự kết hợp các máy tính với nhau thông qua các thiết bị kết nối mạng trong môi trường truyền dẫn thông qua các giao thức theo một cấu trúc mà các máy tính có thể giao tiếp với nhau như việc chia sẻ tập tin, xem và chỉnh sửa các tập tin trên các máy,... Các thiết bị chuyên dụng như router, switch và access point tạo thành cở sở trong mạng máy tính.

Với các phạm vi khác nhau thông thường có thể phân loại mạng máy tính cơ bản như sau:

1. LAN (Local Area Network) là mạng cục bộ, thường được dùng trong mô hình mạng máy tính phạm vi hẹp (khoảng vài trăm mét) như một cơ quan, tổ chức. Môi trường truyền thong có tốc độ kết nối cao.

2. WAN(Wide Area Network) là mạng diện rộng gộp các LAN kết nối lại với nhau phạm vi kết nối có thể nội bộ quốc gia, hay giữa các quốc gia trên thế giới.

3. GAN (Golbal Area Network) là các WAN kết nối với nhau, pham vi kết nối giữa các châu lục với nhau.

2.1.2 Khái niệm mạng không dây

Mạng không dây hay còn gọi là mạng WLAN, hiện nay có thể nói internet là không thể thiếu trong đời sống chúng ta. Mạng không dây là mạng kết nối các thiết bị có khả thu phát song, không sử dụng đường truyền vật lý mà sử dụng song vô tuyến được truyền dẫn thông qua các trạm thu phát sóng

2.1.2.1 Các mô hình mạng không dây

Có 3 mô hình mạng không dây cơ bản như sau:

1. Mô hình mạng không dây độc lập IBSSs: Cấu trúc mô hình mạng độc lập gồm các máy tính kết nối mạng tập trung lại thành một không gian nhỏ để hình thành các kết nối, các máy tính có thể giao tiếp với nhau mà không cần phải quản trị mạng.
2. Mô hình mạng không dây cơ sở BSSs: Cấu trúc mô hình mạng cơ sở bao gồm các điểm truy cập là các Access Point đóng vai trò điều khiển lưu lượng tới mạng. Các thiết bị di động không giao tiếp trực tiếp với nhau mà giao tiếp với các Access Point.
3. Mô hình mạng không dây mở rộng ESSs: Mô hình mở rộng kết hợp các BSSs nơi các Access Point giao tiếp với nhau để chuyển lưu lượng từ một BSS này đến một BSS khác nhằm bảo đảm sự ổng định trong quá trình kết nối các trạm BSS.

2.1.2.2 Các chuẩn mạng không dây

1. Chuẩn WiFi 802.11: Là chuẩn đầu tiên của WLAN được  IEEE (Institute of Electrical and Electronics Engineers) ra mắt năm 1997, chuẩn 802.11 chỉ hỗ trợ băng tần cực đại tối ta 2Mbps, ngày nay chuẩn này không được sử dụng trong sản suất nữa.
2. Chuẩn WiFi 802.11b: Được IEEE mở rộng từ chuẩn 802.11 vào năm 1999, chuẩn 802.11b hỗ trợ băng thông lên đến 11Mbps và sử dụng tần số tín hiệu vô tuyến với tần số 2.4 GHz. Một bất lợi của chuẩn 802.11b là khi các thiết bị áp dụng chuẩn này dễ bị nhiễu khi ở cùng các thiết bị có cùng dải tần cần lắp đặt các thiết bị cách xa nhau để hạn chế hiện tượng này.
3. Chuẩn WiFi 802.11a: Cùng ra mắt năm 1999. Chuẩn 802.11a thích hợp sư dụng trọng các mạng doanh nghiệp, nó hỗ trợ băng thông lên đến 54 Mbps và dải tần 5Ghz. Chuẩn 802.11a có tốc độ nhanh và kiểm soát được hiện tượng nhiễu ổn định nhưng nó có giá thành khá đắt đỏ.
4. Chuẩn WiFi 802.11g : Chuẩn 802.11g ra mắt vào năm 2003 được đánh giá cao trên thị trường, nó hỗ trợ băng thông lên đến 54Mbps và có dải tần 2.4 Ghz và tương thích với các chuẩn 802.11b. Chuẩn 802.11g có tốc độ rất nhanh, phạm vi tín hiệu tốt và vẫn có hiện tượng nhiễu từ những thiết bị có cùng tần số.
5. Chuẩn WiFi 802.11n: Chuẩn 802.11n được phê chuẩn năm 2009 với sự hỗ trợ băng thông lến đến 600 Mpbs nó cung cấp phạm vi tốt hơn những chuẩn WiFi trước đó và khả năng chống nhiễu tốt, những giá thành đắt đỏ.

2.1.3 Khái niệm an toàn bảo mật không dây

Mạng không dây kết nối trong môi trường không khí nên khả năng bị kẻ xấu tấn công rất cao.

2.1.3.1 Các hình thức tấn công mạng WLAN

Một số hình thức tân công trong hệ thống mạng không dây được đề cập sau đây:

1. Giả mạo Access Point: Hình thức tấn công này chỉ đến những Access Point được tạo ra một hay cố tình hay vô tình làm ảnh hưởng đến hệ thống mạng, ngoài những sự cố do cài đặt cấu hình thì những kẻ tấn công có thể lợi dụng nó bằng cắc thiết lập các sao chép tất cả các cấu hình của AP chính thống như SSID, địa chỉ MAC,..vv. Khi người dùng vô tình kết nối tới AP giả mạo thì kẻ xấu có thể đánh cắp thông, sử dụng hệ thống mạng để tấn công đối tượng khác.
2. Tấn công yêu cầu xác thực lại: Kẻ tấn công chèn các frame yêu cầu xác thực lại vào mạng WLAN bằng cách giả mạo địa chỉ MAC nguồn và đích lần lượt của Access Point và các người dùng. Người dùng trong mạng không dây khi nhận được frame yêu cầu xác thực lại sẽ chủ quan mà nghĩ rằng chúng do AP gửi đến. Thông thường người dùng sẽ kết nối lại để sử dụng dịch vụ, kẻ tấn công sẽ tiếp tục gửi các gói yêu cầu xác thực cho người dùng.
3. Tấn công dựa trên sự cảm nhận sóng mang vật lý: Hình thức tấn công này là khi kẻ tấn công lợi dụng giao thức chống đụng độ CSMA/CA, tức là nó sẽ làm cho tất cả người dùng nghĩ rằng lúc nào trong mạng cũng có một máy tính đang truyền thông. Điều này làm cho các máy tính khác luôn luôn ở trạng thái chờ đợi kẻ tấn công ấy truyền dữ liệu xong và dẫn đến tình trạng ngẽn trong mạng.
4. Tấn công ngắt kết nối: Hình thức tấn công này khá giống với hình thức tấn công yêu cầu xác thực lại, khi kẻ tấn công xác định mục tiêu hắn sẽ gửi disassociation frame bằng cách giả mạo địa chỉ MAC nguồn và đích đến AP và các máy khách tương ứng. Các máy khách sẽ nhận các frame này và nghĩ rằng frame hủy kết nối đến từ AP. Đồng thời kẻ tấn công cũng gửi disasociation frame đến AP. Sau khi đã ngắt kết nối với một máy khách, kẻ tấn công thực tiếp tục với các máy khác làm cho chúng tự động ngắt kết nối đến AP.

2.1.3.2 Các phương pháp bảo mật cơ bản trong WLAN

1. Bảo mật bằng WEP (Wired Equivalent Privacy): Một trong những giao thức bảo mật đầu tiên của WiFi được phát hành năm 1997, nghĩa là bảo mật tương đương có dây. WEP mã hóa dữ liệu của người dùng để những người khác không được thông tin trong các gói. WEP cung cấp bảo mật cho dữ liệu trên mạng không dây qua phương thức mã hóa sử dụng thuật toán đối xứng RC4, được Ron Rivest - thuộc hãng RSA Security Inc nổi tiếng - phát triển. Thuật toán RC4 cho phép chiều dài của khóa thay đổi và có thể lên đến 256 bit. Tuy nhiên, WEP không an toàn Cách sử dụng giá trị IV là nguồn gốc của đa số các vấn đề với WEP. Do giá trị IV được truyền đi ở dạng không mã hóa và đặt trong header của gói dữ liệu 802.11 nên bất cứ ai "tóm được" dữ liệu trên mạng đều có thể thấy được. Những giải pháp tối ưu cho WEP có thể gia tăng mức độ bảo mật như: Sử dụng khóa WEP có độ dài 128 bit, sử dụng các công cụ theo dõi số liệu trên đường truyền, … để khắc phục những điểm yếu của WEP, IEEE đã phát triển những chuẩn bảo mật cao hơn như WPA và WPA2.
2. Bảo mật bằng WPA (Wifi Protected Access): IEEE đã tạo ra một nhóm làm việc 802.11i hoạt động để tạo ra một mô hình bảo mật toàn diện nhằm cung cấp mã hóa và xác thực AES 128-bit để bảo vệ dữ liệu Mô-đun WPA kết hợp một số công nghệ để giải quyết lỗ hổng của hệ thống WEP 802.11. Do đó, WPA cung cấp khả năng xác thực người dùng mạnh mẽ bằng cách sử dụng tiêu chuẩn 802.1x (xác thực lẫn nhau và đóng gói dữ liệu được truyền giữa các thiết bị khách không dây, điểm truy cập và máy chủ) và Giao thức xác thực mở rộng (EAP).
3. Bảo mật bằng chuẩn 802.11i (WPA2): Với tiêu chuẩn 802.11i, toàn bộ chuỗi mô-đun bảo mật (đăng nhập, ủy quyền, xác thực và mã hóa dữ liệu) trở nên bảo vệ hiệu quả và đáng tin cậy hơn chống lại các cuộc tấn công có chủ đích và không có chủ đích. WPA2 cho phép quản trị viên mạng Wi-Fi chuyển từ các vấn đề bảo mật sang hoạt động và quản lý thiết bị. Chuẩn 802.11r là một sửa đổi của chuẩn 802.11i. Tiêu chuẩn này đã được phê chuẩn vào tháng 7 năm 2008. Công nghệ của tiêu chuẩn chuyển giao các phân cấp chính một cách nhanh chóng và đáng tin cậy hơn, dựa trên công nghệ Handoff, khi người dùng di chuyển giữa các điểm truy cập. Chuẩn 802.11r hoàn toàn tương thích với các chuẩn WiFi 802.11a / b / g / n. Ngoài ra còn có chuẩn 802.11w, được thiết kế để nâng cao cơ chế bảo mật dựa trên chuẩn 802.11i. Tiêu chuẩn này được thiết kế để bảo vệ các gói điều khiển. Chuẩn 802.11i và 802.11w là cơ chế bảo vệ mạng WiFi của chuẩn 802.11n.

2.2 Các thiết bị dây dựng mạng

2.2.1 Router

Router hay còn gọi là bộ định tuyến là thiết bị mạng có chức năng chuyển tiếp gói dữ liệu giữa các mạng máy tính. Gói dữ liệu sẽ được gửi đi trên Internet chuyển tiếp từ router này đến router khác thông qua các mạng nhỏ, kết nối với nhau cho đến khi gói dữ liệu đến được đích. Router thực hiện nhiệm bằng cách gán địa chỉ IP cục bộ cho mỗi thiết trị trên mạng.

2.2.2 Switch

Switch là thiết bị chuyển mạch dùng để kết nối các mạng theo mô hình sao, đóng vai vai trò trung tâm phân phối các gói tin trong mạng. Switch gồm các loại phổ biến là switch layer 2 và switch layer 3.

2.2.3 Thiết bị phát wifi

Thiết bị phát wifi là các Access point hay router wireless đóng vai trò thu phát tín hiệu wifi cho các thiết bị client như máy tính, điện thoại, …

Access point có nhiệm vụ kết nối nhiều máy tính trong LAN có thể coi là 1 thiết bị chuyển mạch như switch.

2.2.4 Máy chủ

Thiết bị có kết nối mạng có IP tĩnh có tính năng xử lý cao trên nó được cài đặt các dịch như web, dns, mail, … phục vụ cho các máy tính, thiết bị khác truy cập để yêu cầu dịch vụ.

2.2.5 Cáp mạng

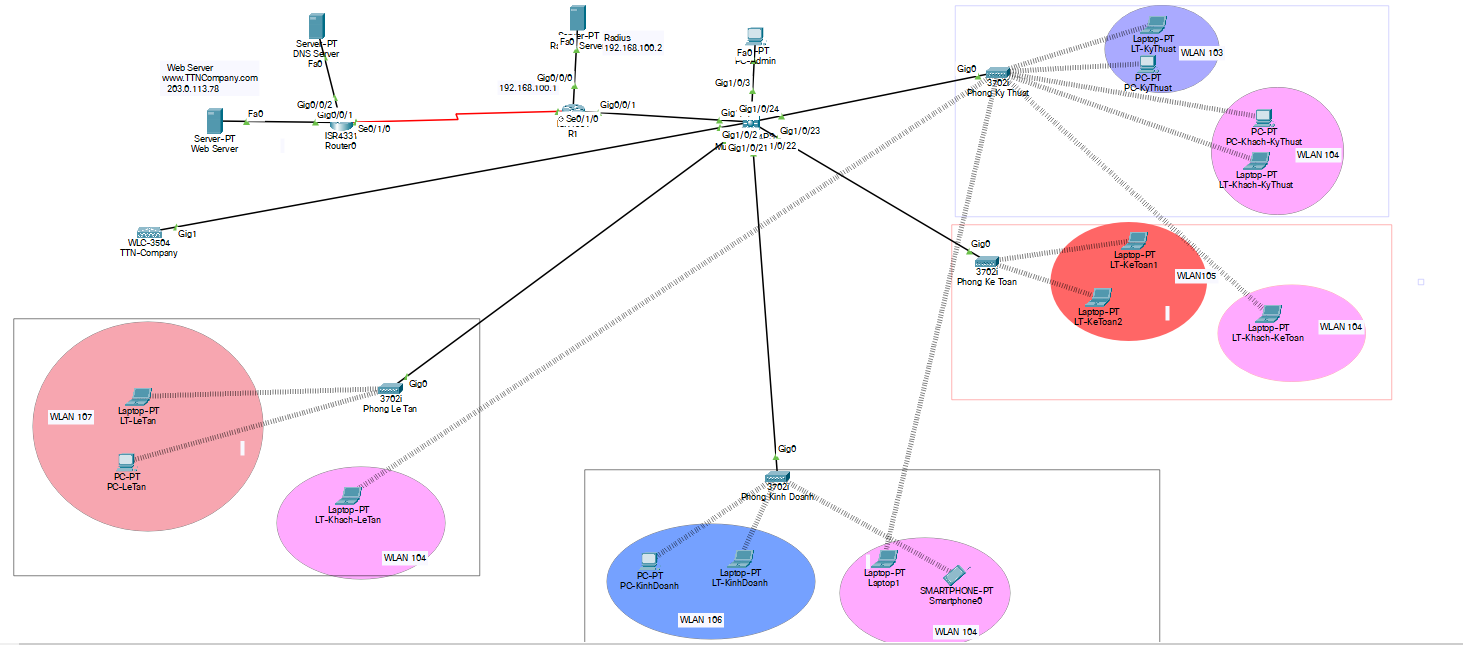
Cáp mạng là loại cáp dùng để sử dụng để kết nối các thiết bị mạng lại với nhau.

2.2.6 Thiết bị máy khách

Như các máy tính để bàn hay laptop, điện thoại, …

CHƯƠNG 3 – MÔ HÌNH DEMO

3.1 Mô hình đề xuất



Hình 3.1: Mô hình đề xuất

3.1.1 Bảng địa chỉ

|  |  |  |
| --- | --- | --- |
| Thiết bị | Interface | Địa chỉ IP |
| R1 | G0/0/0 | 192.168.100.1/24 |
| G0/0/1.103 | 192.168.103.1/24 |
| G0/0/1.104 | 192.168.104.1/24 |
| G0/0/1.105 | 192.168.105.1/24 |
| G0/0/1.106 | 192.168.106.1/24 |
| G0/0/1.107 | 192.168.107.1/24 |
| G0/0/1.200 | 192.168.200.1/24 |
| S0/1/0 | 10.20.30.2/24 |
| SW1 | VLAN200 |  |
| Phong Ky Thuat | G0 | DHCP |
| Phong Ke Toan | G0 | DHCP |
| Phong Kinh Doanh | G0 | DHCP |
| Phong Le Tan | G0 | DHCP |
| WLC TTN-Company | Management | 192.168.200.254/24 |
| RADIUS Server | NIC | 192.168.100.2 |
| PC-Admin | NIC | DHCP |
| Web Server | NIC | 203.0.113.78/24 |
| DNS Server | NIC | 10.100.100.254 |
| Router0 | G0/0/0 | 10.100.200.1/24 |
| G0/0/1 | 203.0.113.1/24 |
| G0/0/2 | 10.100.100.1/24 |
| S0/1/0 | 10.20.30.1/24 |
| LT-KyThuat | Wireless | DHCP |
| PC-KyThuat | Wireless | DHCP |
| PC-Khach-KyThuat | Wireless | DHCP |
| LT-Khach-KyThuat | Wireless | DHCP |
| LT-KeToan1 | Wireless | DHCP |
| LT-KeToan2 | Wireless | DHCP |
| LT-Khach-KeToan | Wireless | DHCP |
| PC-KinhDoanh | Wireless | DHCP |
| LT-KinhDoanh | Wireless | DHCP |
| Laptop1 | Wireless | DHCP |
| Smartphone | Wireless | DHCP |
| LT-LeTan | Wireless | DHCP |
| PC-LeTan | Wireless | DHCP |
| LT-Khach-LeTan | Wireless | DHCP |

Bảng 3.1: Bảng địa chỉ

3.1.1 Bảng thông tin WLAN

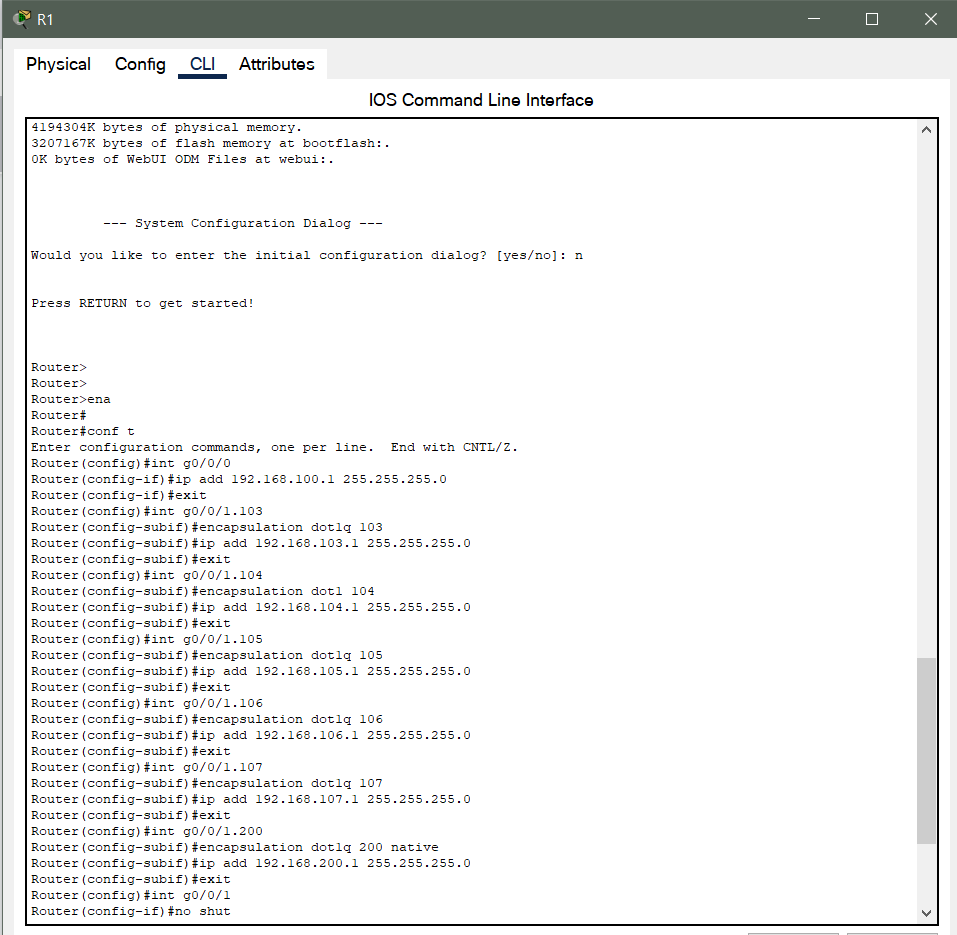
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| WLAN | SSID | Xác thực | Username | Password |
| KyThuat\_103 | KyThuat\_103 | WPA-2 802.1x/Enterprise | KyThuat | KyThuatPass |
| KeToan\_105 | KeToan\_105 | WPA-2 802.1x/Enterprise | KeToan | KeToanPass |
| KinhDoanh\_106 | KinhDoanh\_106 | WPA-2 802.1x/Enterprise | KinhDoanh | KinhDoanhPass |
| LeTan\_107 | LeTan\_107 | WPA-2 802.1x/Enterprise | LeTan | LeTanPass |
| Guest\_104 | Guest\_104 | WPA-2 PSK/Personal | N/A | GuestPass |

Bảng 3.2: Bảng thông tin WLAN

3.2 Cấu hình các thiết bị

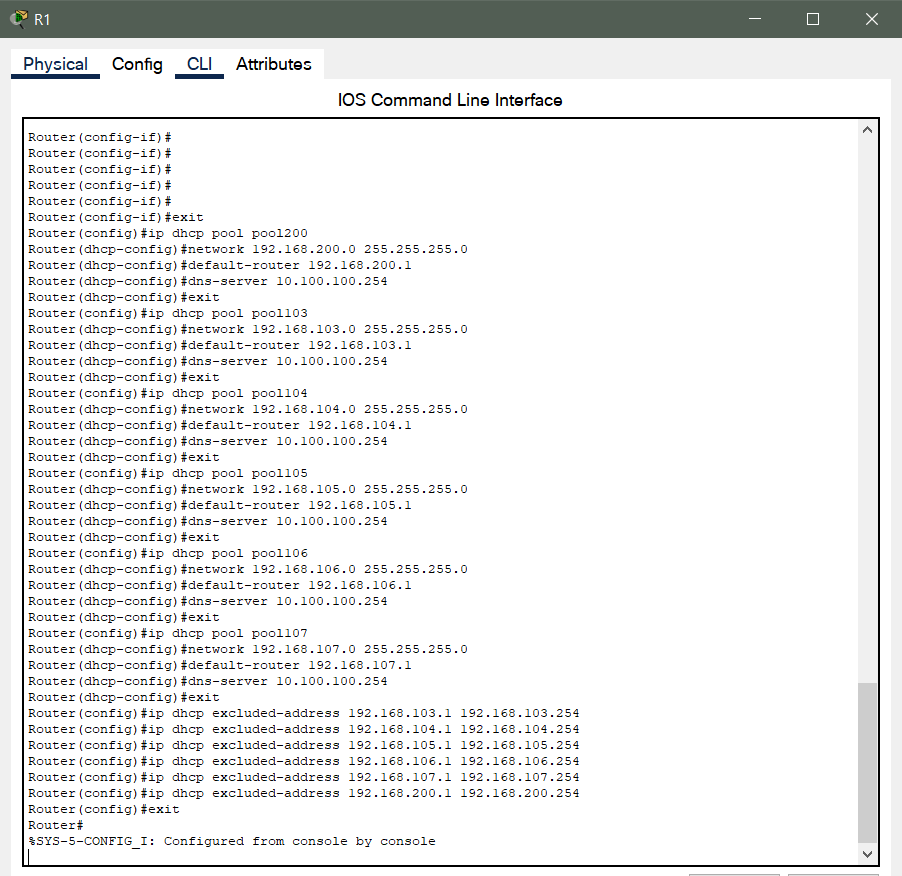
3.2.1 Trên router R1

* Cấu hình các địa chỉ IP cho cổng interface theo bảng địa chỉ đã đề cập.



Hình 3.2: Cấu hình địa chỉ IP cho router R1

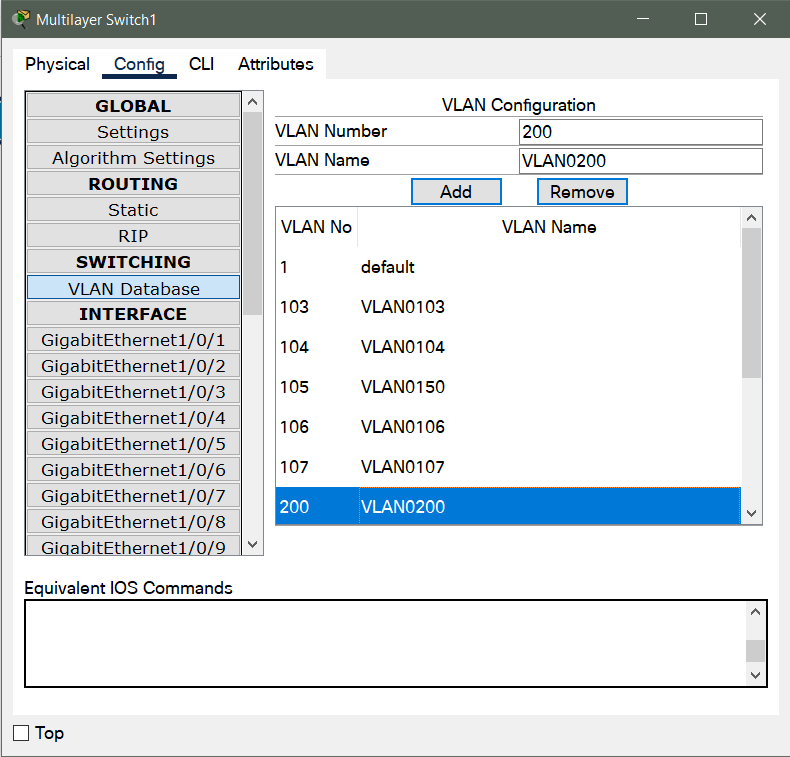
* Cấu hình DHCP trên router R1



Hình 3.3: Cấu hình tạo DHCP cho router R1

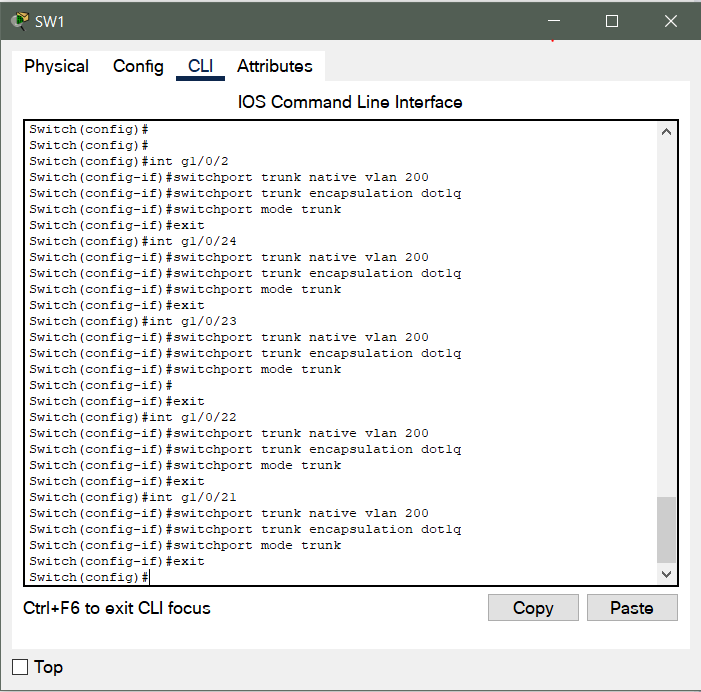
3.2.2 Trên switch core SW1

* Tạo các VLAN



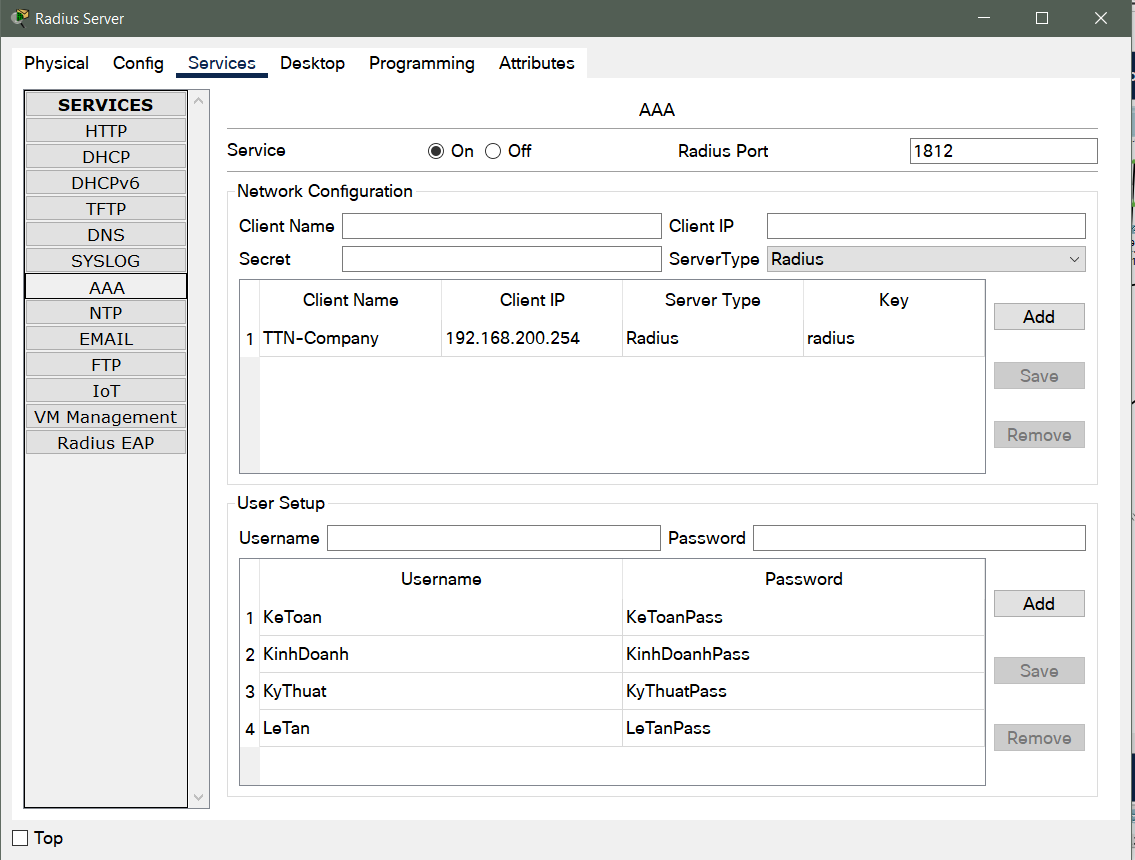
Hình 3.4: Các Vlan đã tạo trên SW1

* Cấu hình trunk qua các cổng mà Access Point kết nối tới SW1



Hình 3.5: Cấu hình trunk trên SW1

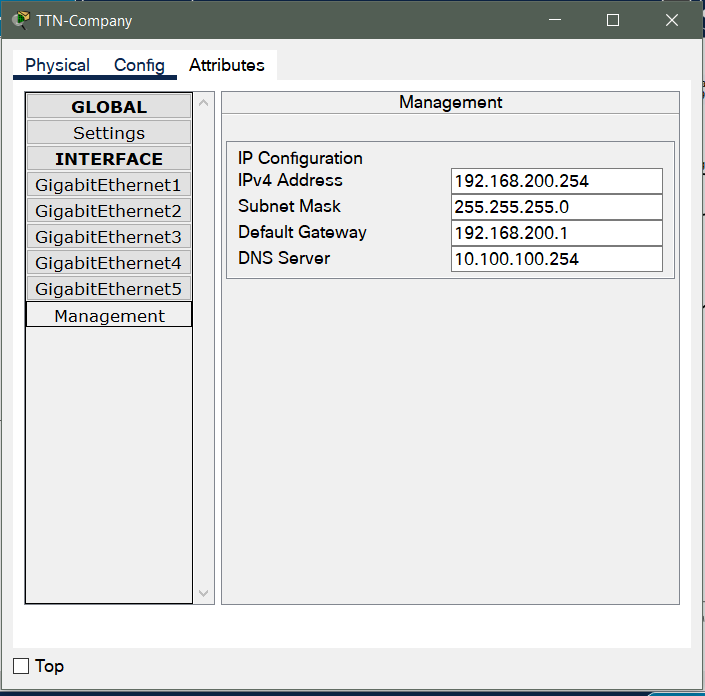
3.2.2 Trên Radius Server



Hình 3.6: Cấu hình AAA trên Radius Server

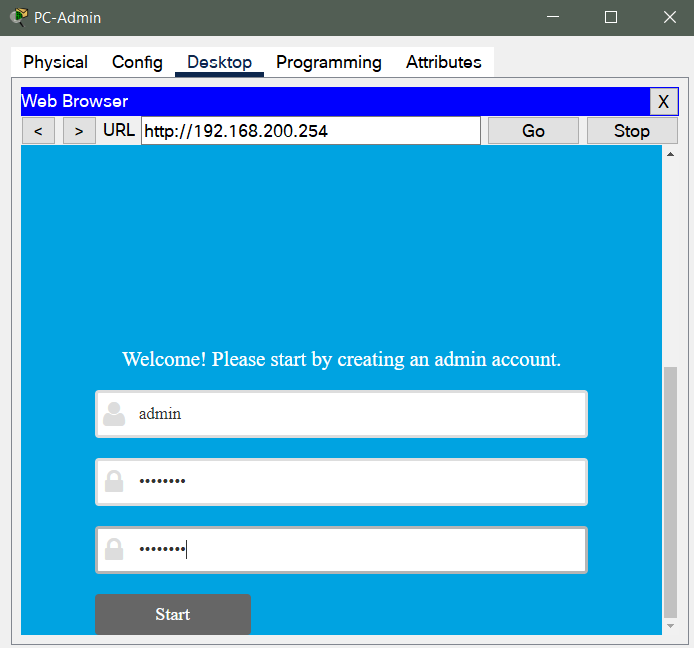
3.2.4 Trên WLC TTN-Company

* Cài đặt địa chỉ IP cho WLC theo bảng địa chỉ

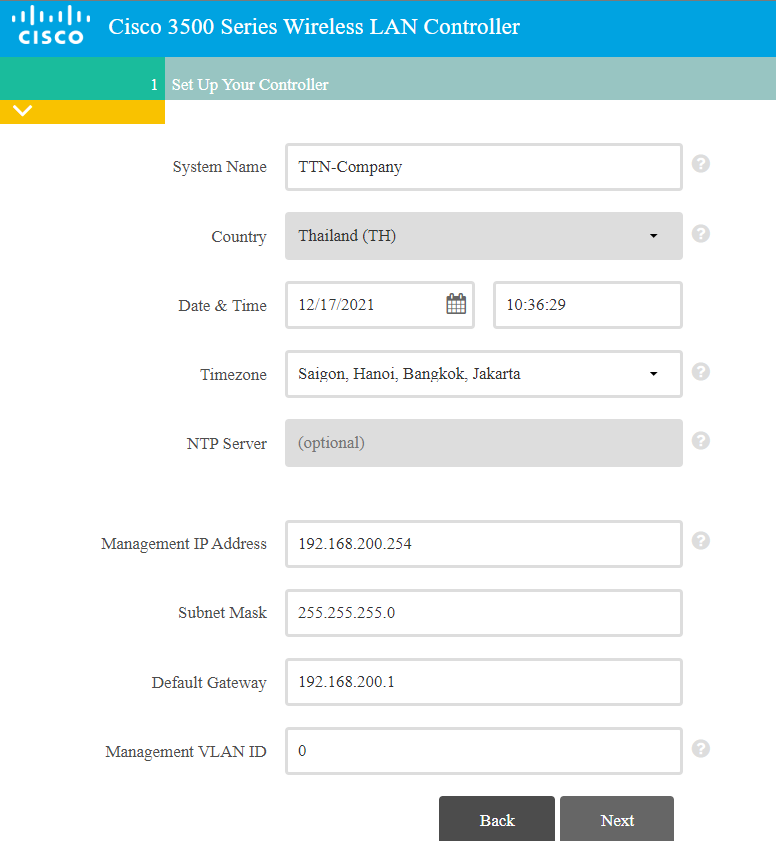


Hình 3.7: Thông tin về WLC

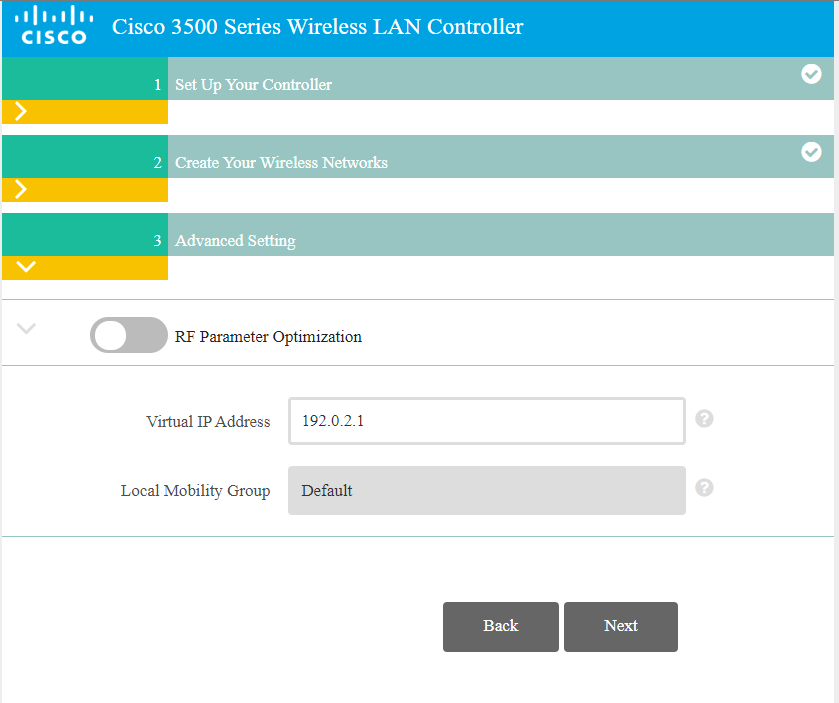
* **Cài đặt cấu hình WLC**
* Truy cập vào Web Browser trong tab Desktop của máy tính PC-Admin và gõ địa chỉ <http://192.168.200.254>
* Giao diện sau sẽ xuất hiện để bắt đầu khởi tạo WLC, nhập vào username và password theo sau: admin/Cisco123



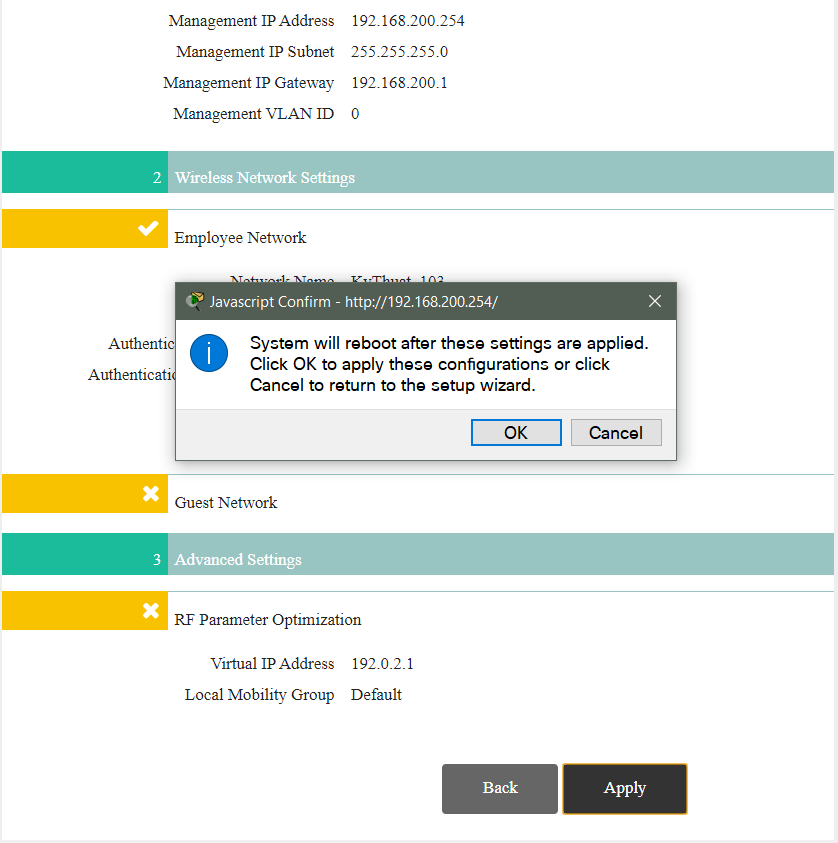
* Cấu hình tên và địa chỉ theo bảng địa chỉ, sau đó nhấn Next



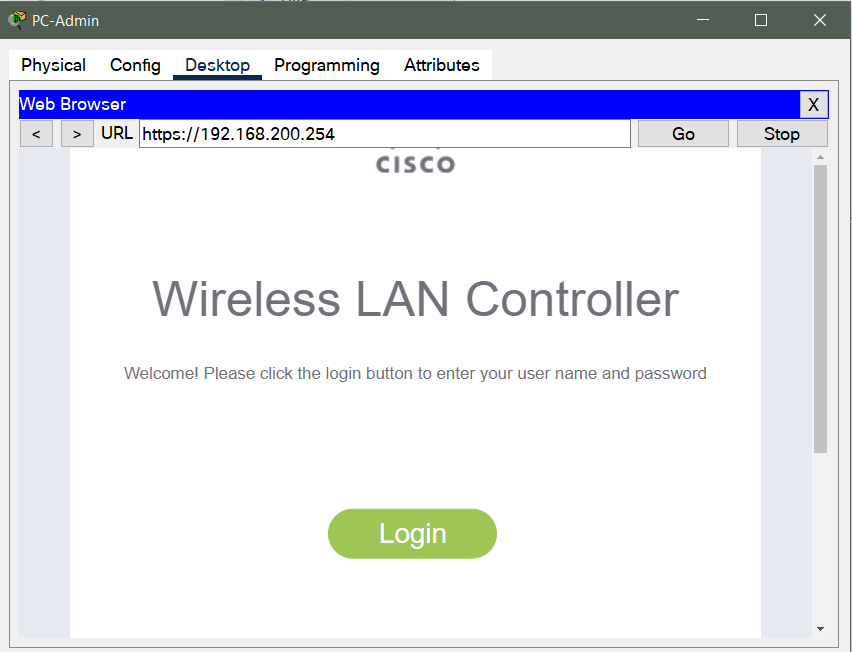
* Tiếp tục nhấn Next



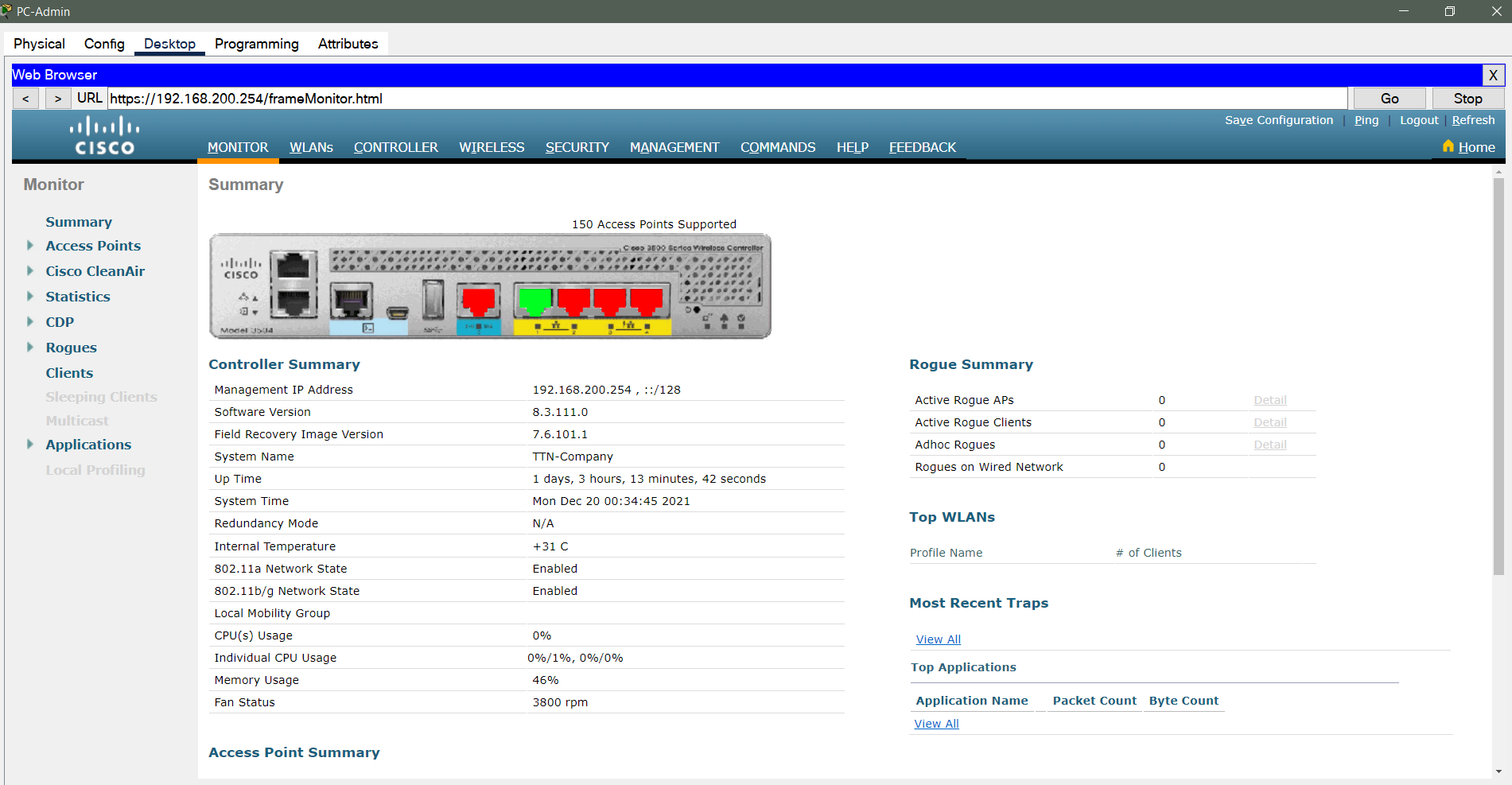
* Nhấn Apply 🡪 OK



* Truy cập lại vào Web Browser trong tab Desktop của máy tính PC-Admin và gõ địa chỉ <https://192.168.200.254>, giao diện đăng nhập vào WLC sẽ xuất hiện

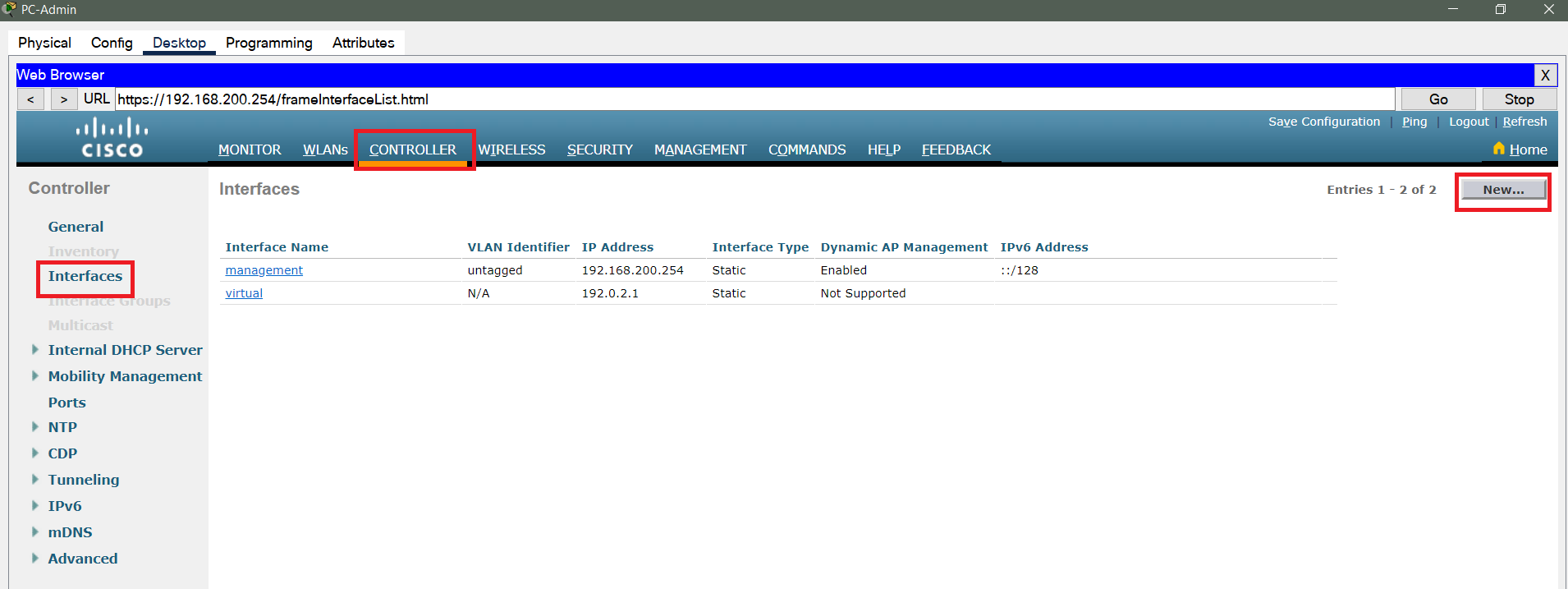


* Đăng nhập vào bằng username và password đã khởi tạo lúc ban đầu

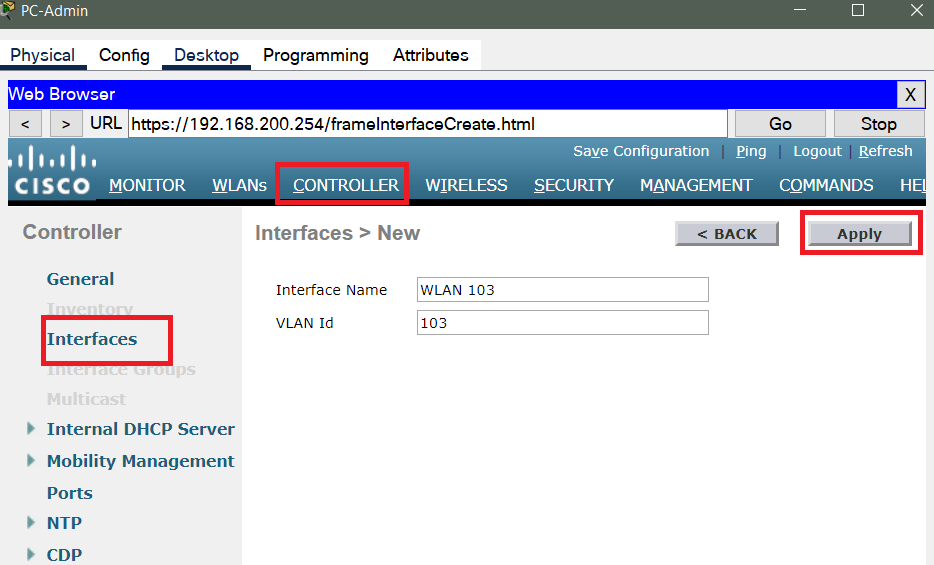


Hình 3.8: Giao diện chính của WLC

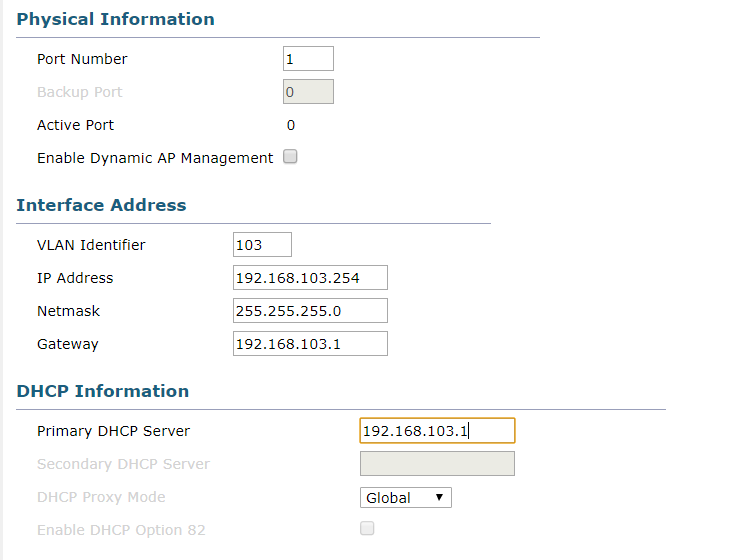
* **Tạo interface trên WLC**
  + Vào tab CONTROLLER 🡪 Interfaces 🡪 New…



* Tạo interface WLAN 103

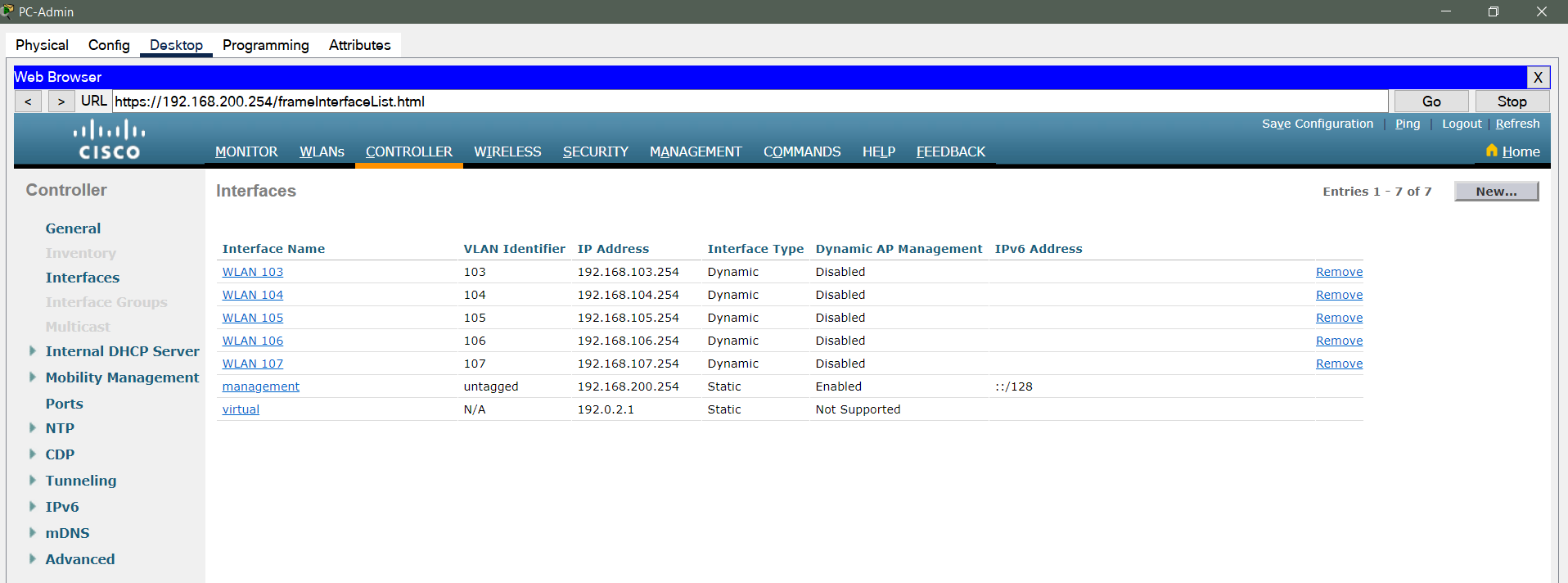


* Cấu hình địa chỉ cho interface, chọn Port Number là 1, và các địa chỉ theo bảng địa chỉ



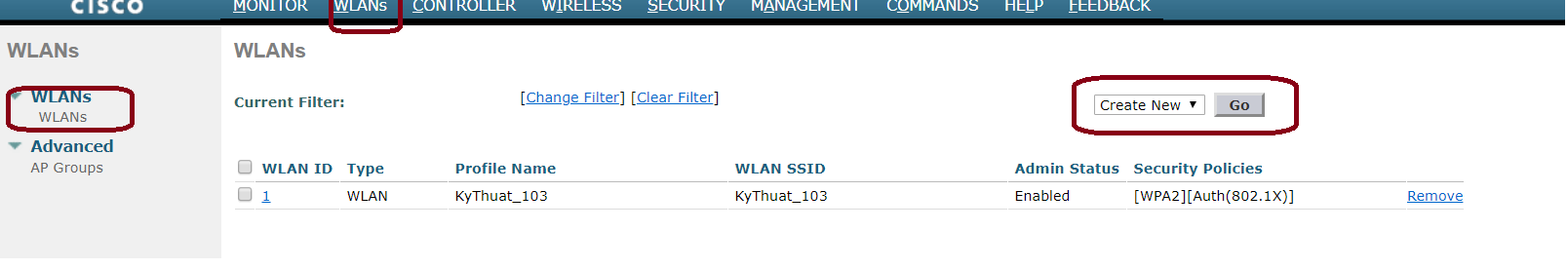


* Tiếp tục tạo các interface khác.

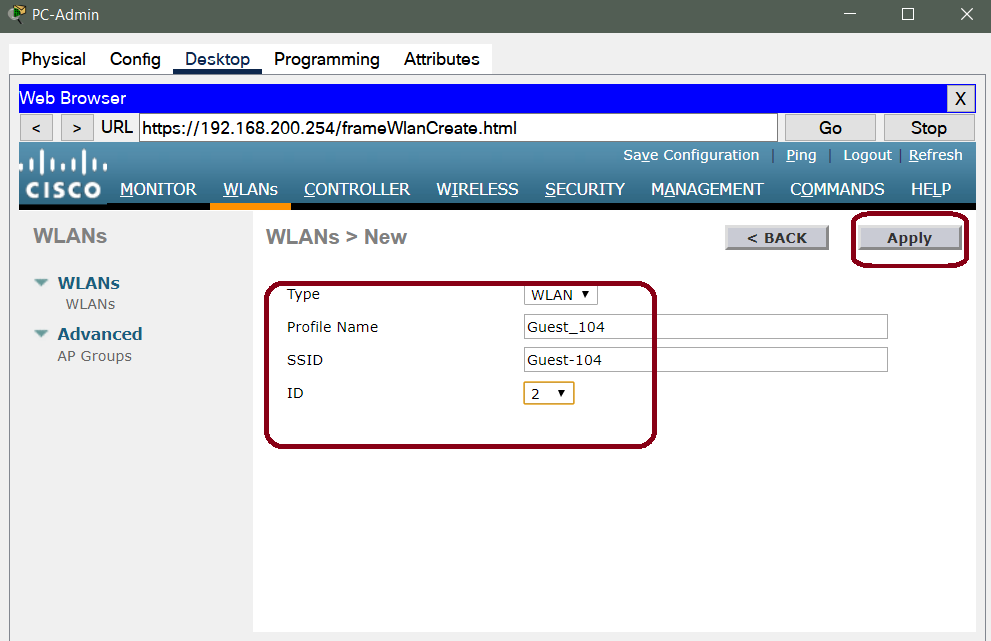


Hình 3.9: Các interface đã khởi tạo trên WLC

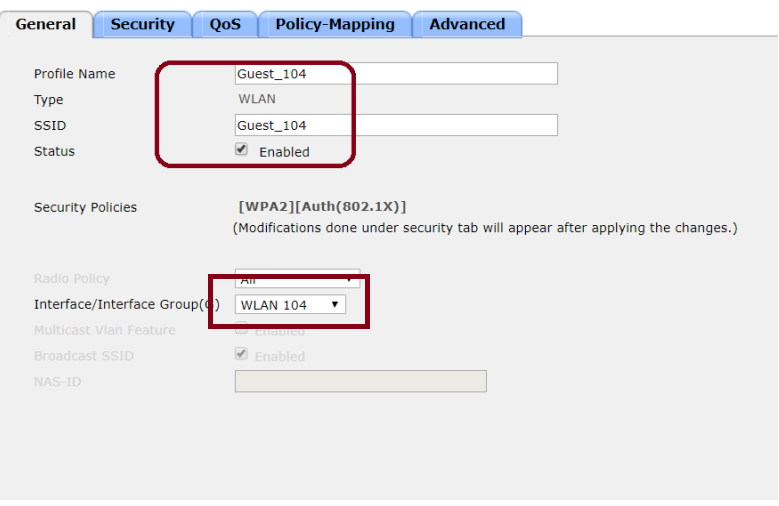
* **Tạo WLAN và cài đặt bảo mật**
  + Thực hiện tạo WLAN cho khách sử dụng : GUEST\_104 và cài đặt bảo mật WPA2-PSK/Personal
    - Vào tab WLANs sau đó chọn Create New --> GO



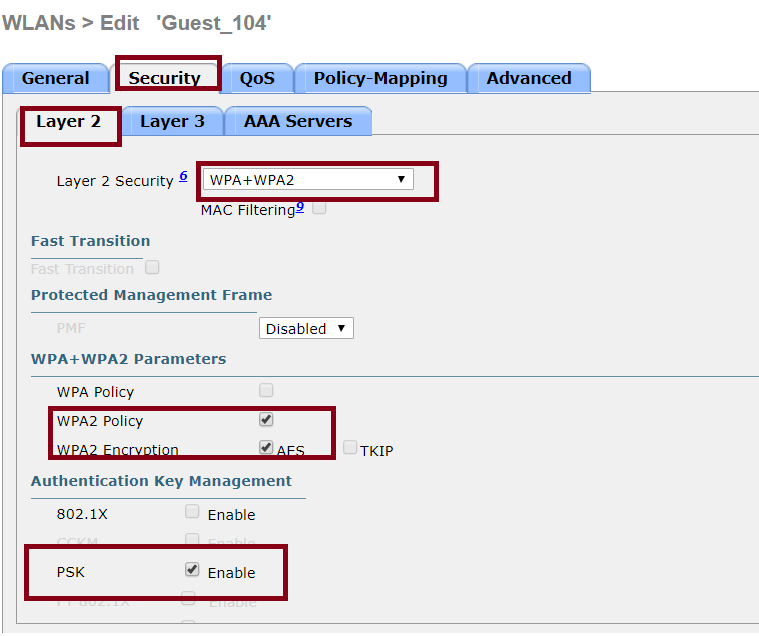
* + - Điền vào Profile Name và SSID sau đó Apply

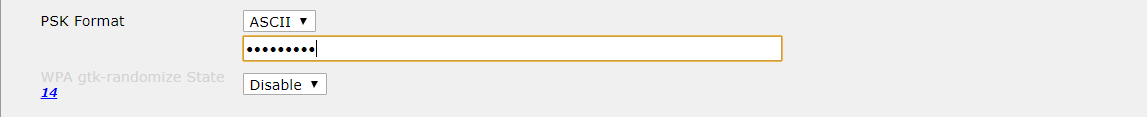


* + - Tiếp tục cấu hình: Kích hoạt WLAN bằng cách tích vào ô Enable và chọn interface cho WLAN

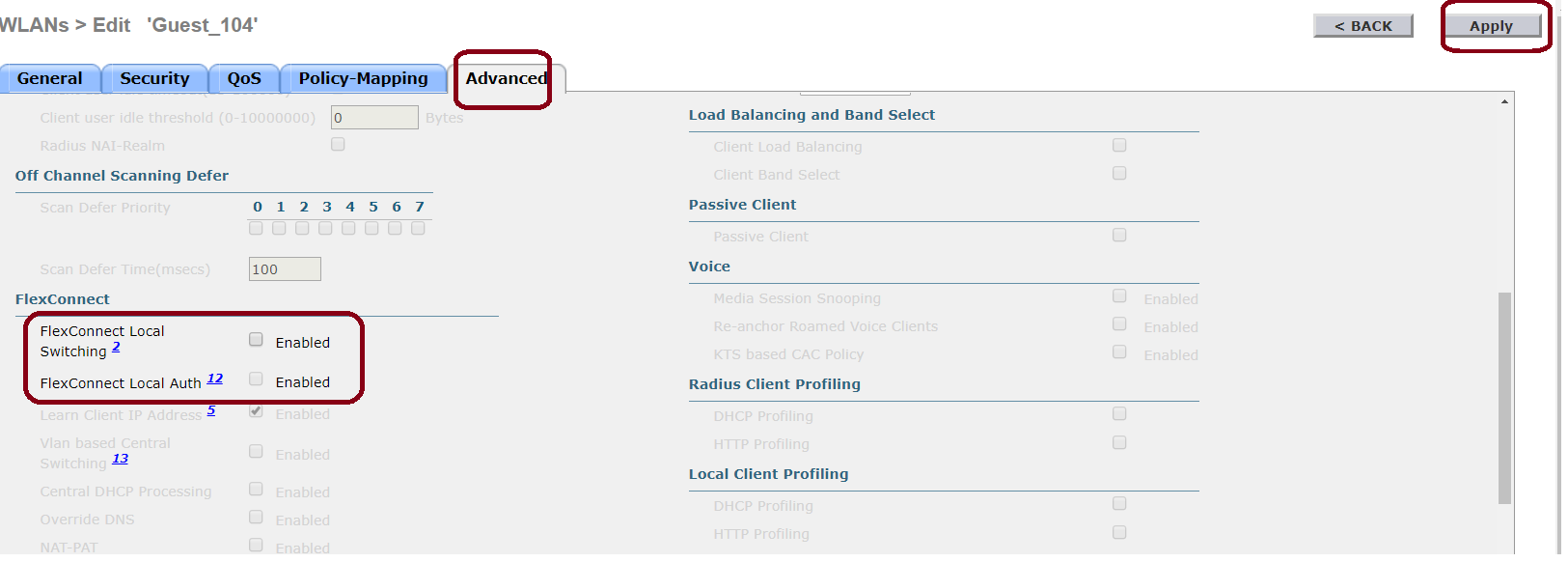


* + - Qua tab Security ở tab Layer 2 chọn WPA + WP2, sau đó tích vào WP2 Policy rồi tích vào ô PSK. Sau đó điền mật khẩu trong ô PSK format ở đây điền GuestPass.

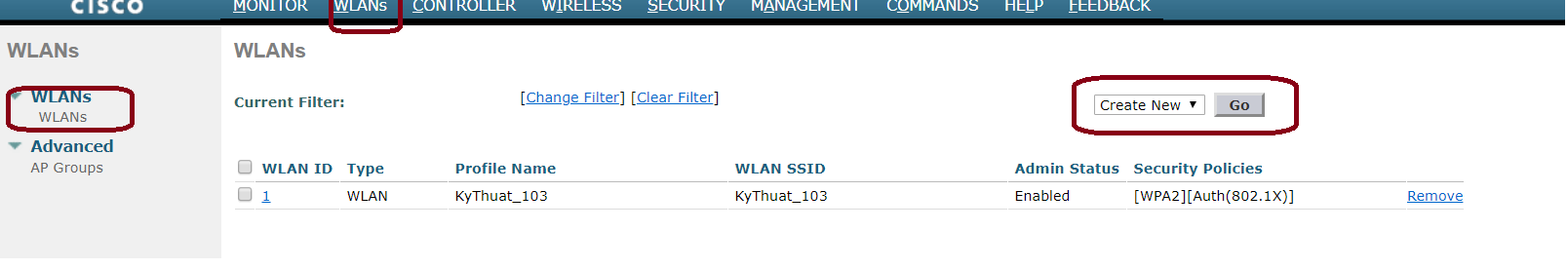




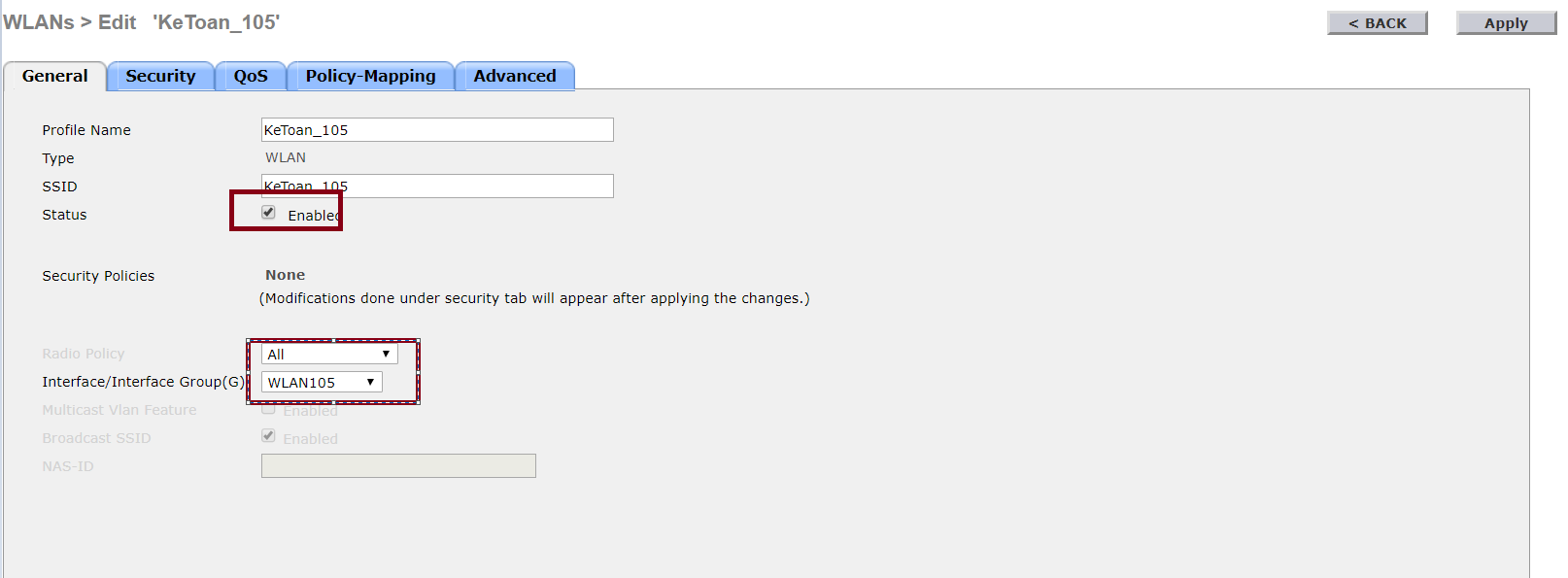
* + - Qua tab Advanced cuộn xuống dưới và tích vào 2 ô FlexConnect Local Switching và FlexConnect Local Auth sau đó nhấn Apply



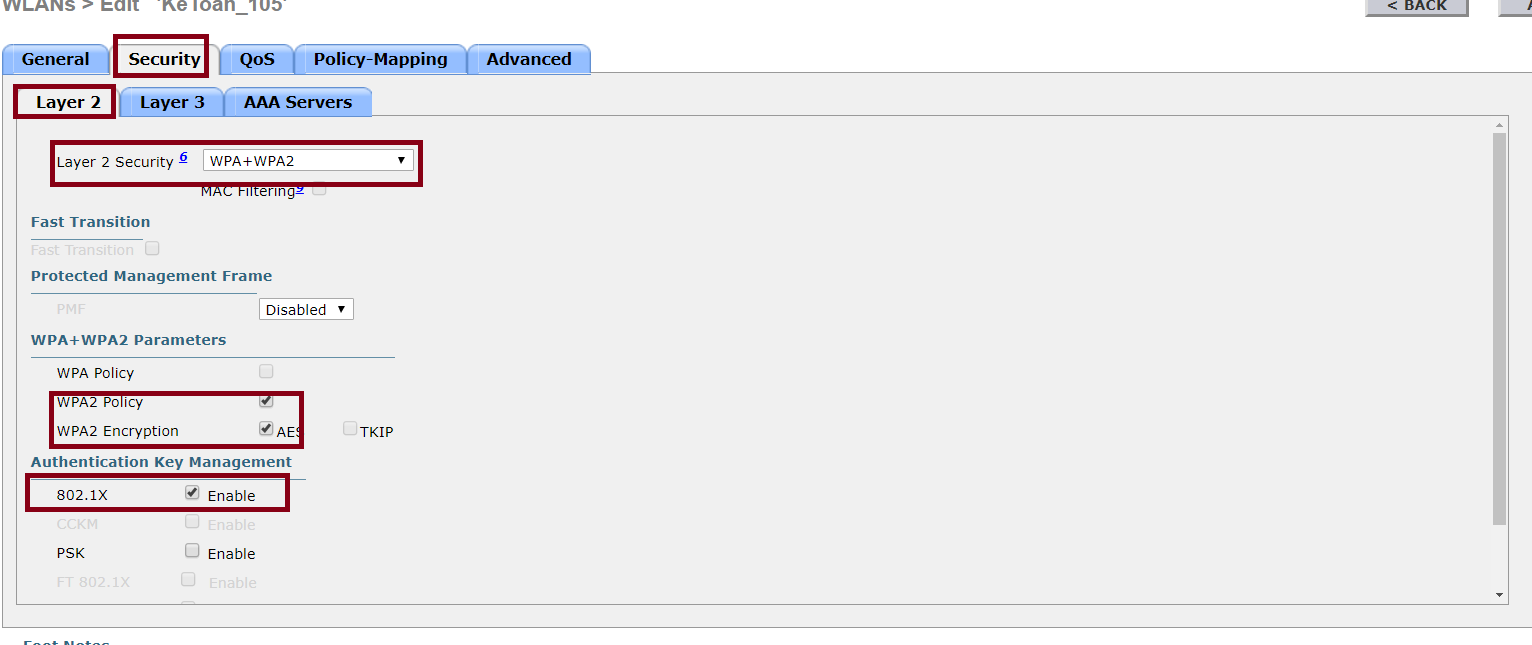
* Tạo WLAN giành riêng cho 1 phòng ban và cài đặt bảo mật WPA-2 802.1x/Enterprise, ví dụL Phòng kế toán: KeToan\_105
* Vào tab WLANs sau đó chọn Create New --> GO



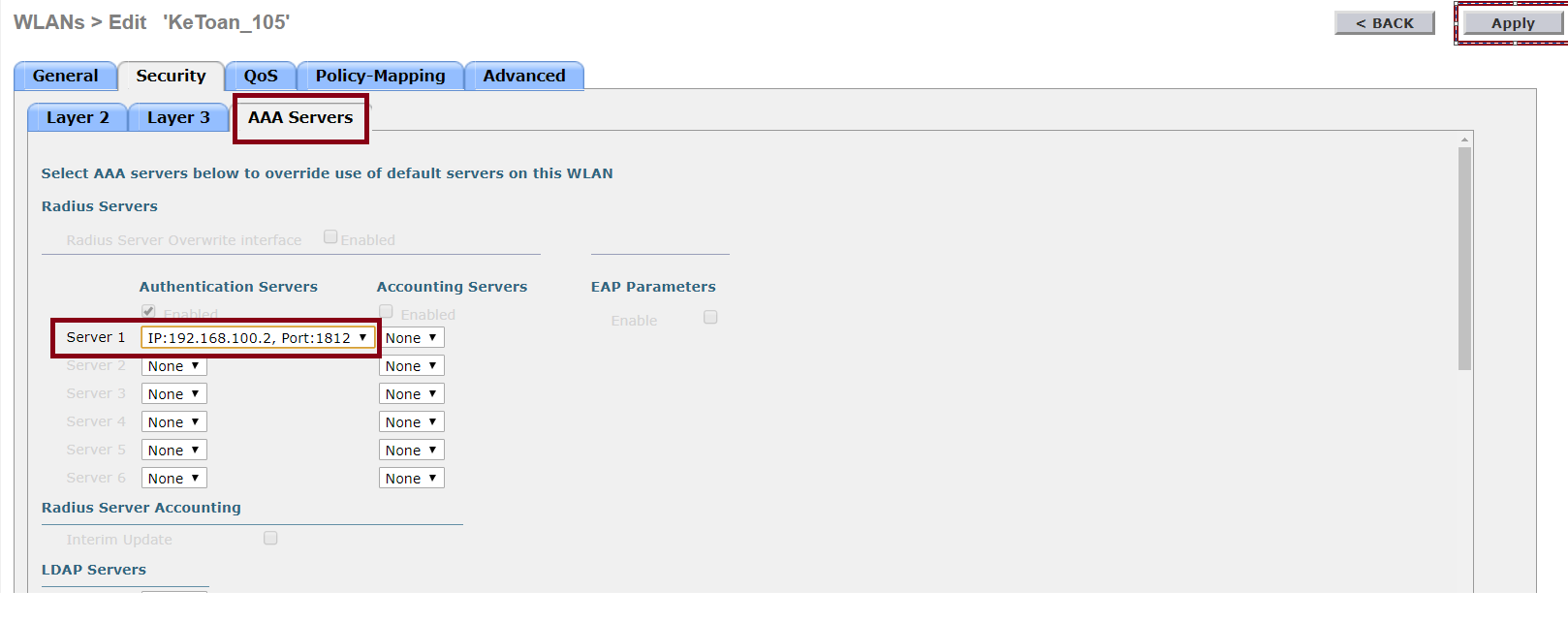
* Bước 2: Kích hoạt WLAN và chọn Interface tương thích



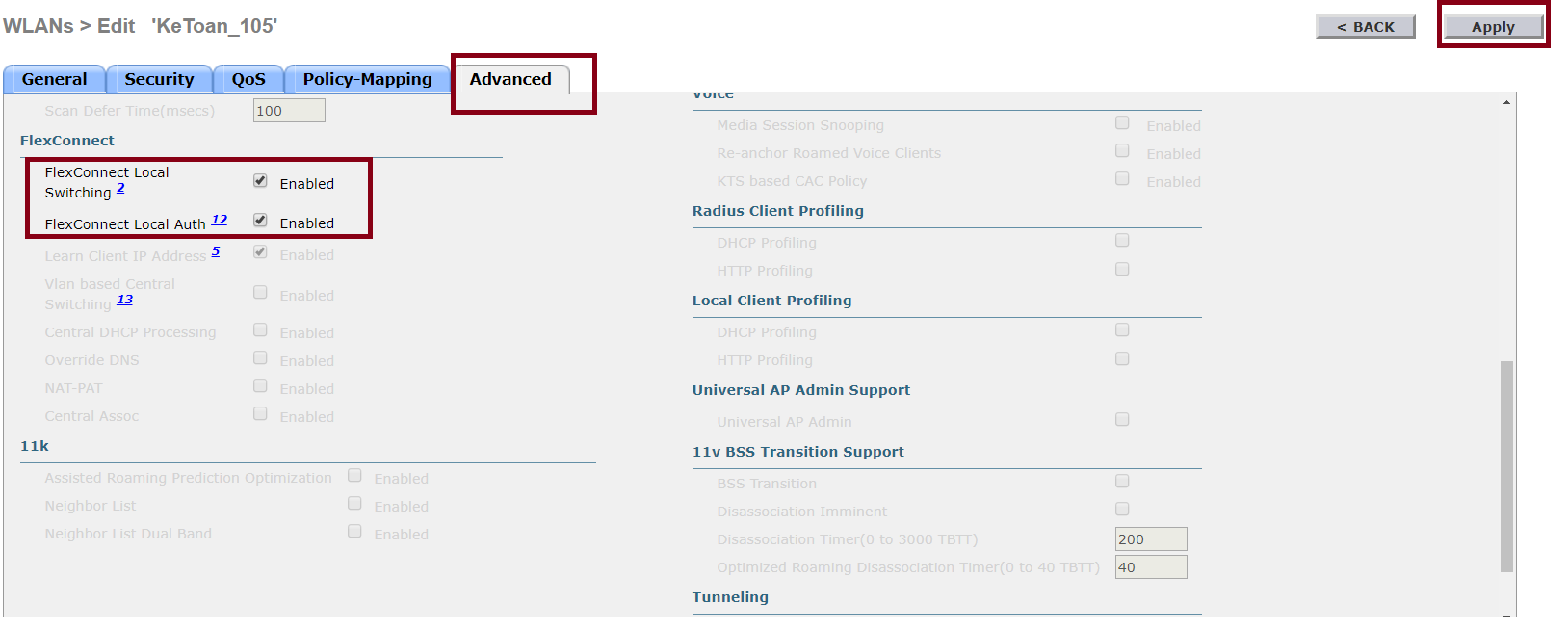
* Qua tab Security để cài đặt bảo mật, Ở tab layer 2 chon WPA+WPA2 sau đó tích vào ô WP2 Policy và bật chuẩn 802.1X



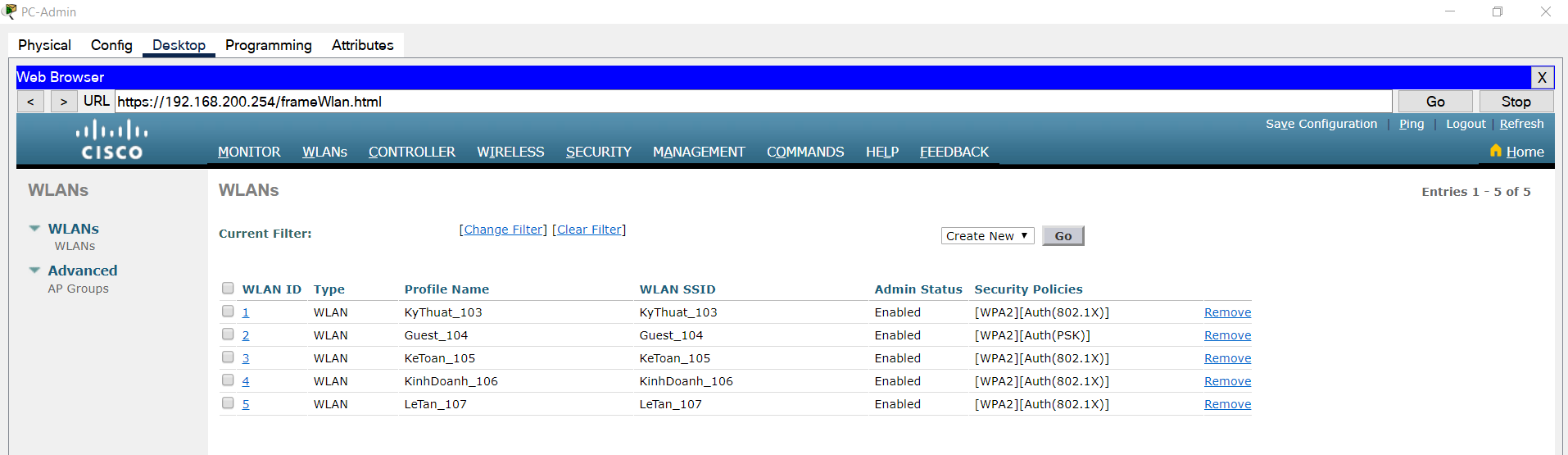
* Qua tab AAA Server  Chọn server đã cài đặt Radius Server



* Qua tab Advanced cuộn xuống dưới và tích vào 2 ô FlexConnect Local Switching và FlexConnect Local Auth sau đó nhấn Apply

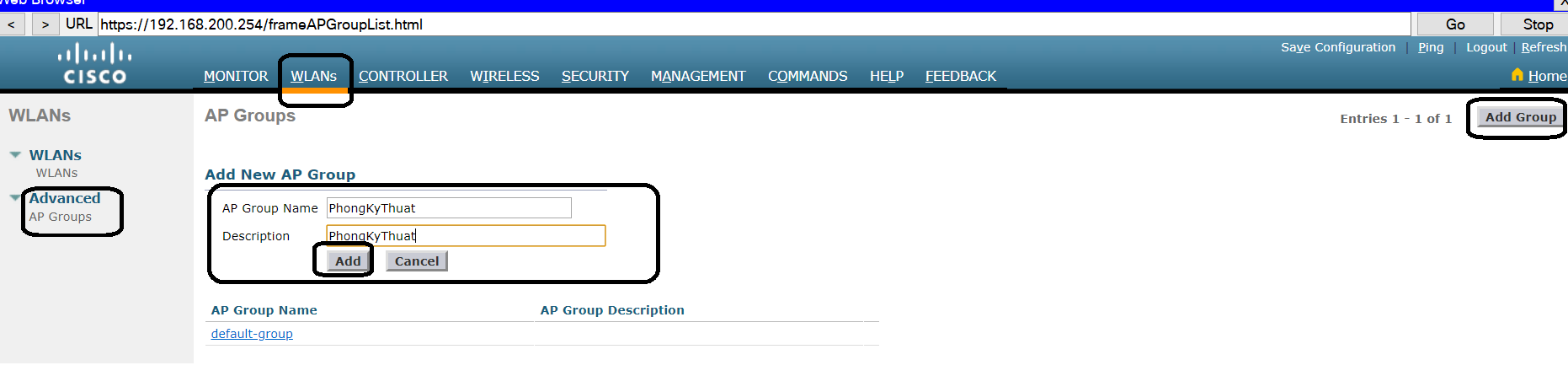


* Thực hiện tạo các WLAN cho các phòng ban còn lại.



Hình 3.10: Các WLAN đã khởi tạo trên WLC

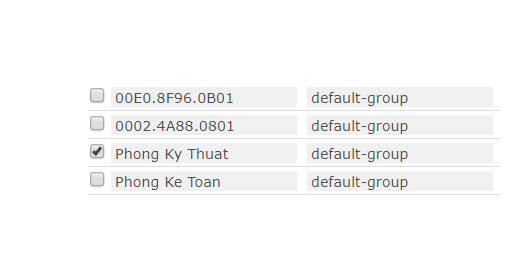
* **Add Group cho các Access Point chỉ cung cấp những mạng riêng**
* Vào giao diện chính WLC 🡪 WLANs 🡪 Advanced 🡪 Ap Groups 🡪Add Group



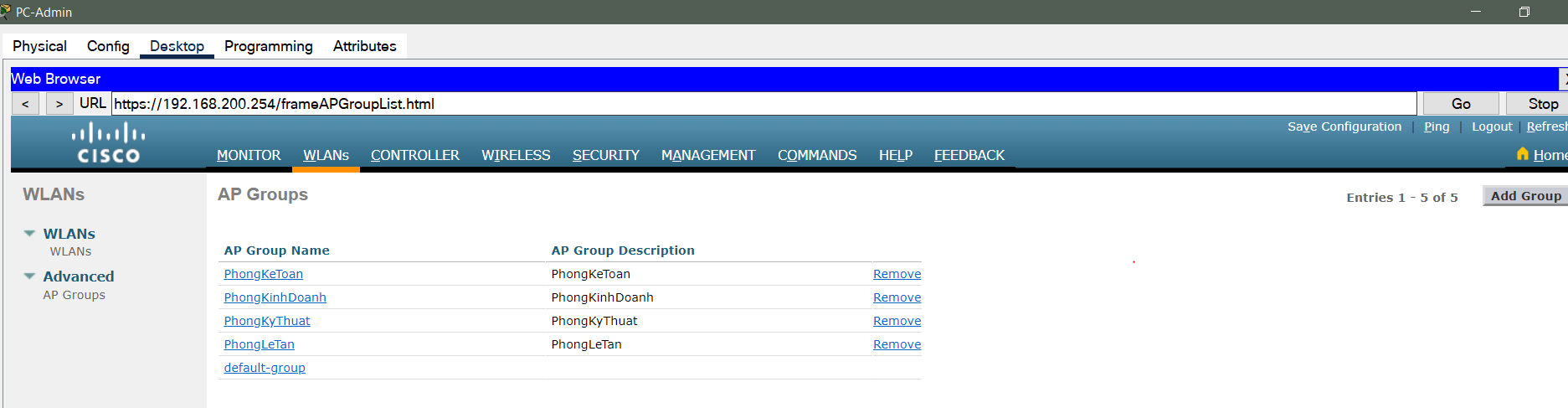
* Add những WLAN SSID vào group ở đây t đã add KyThuat\_103 và Guest\_104



* Chọn Access Point



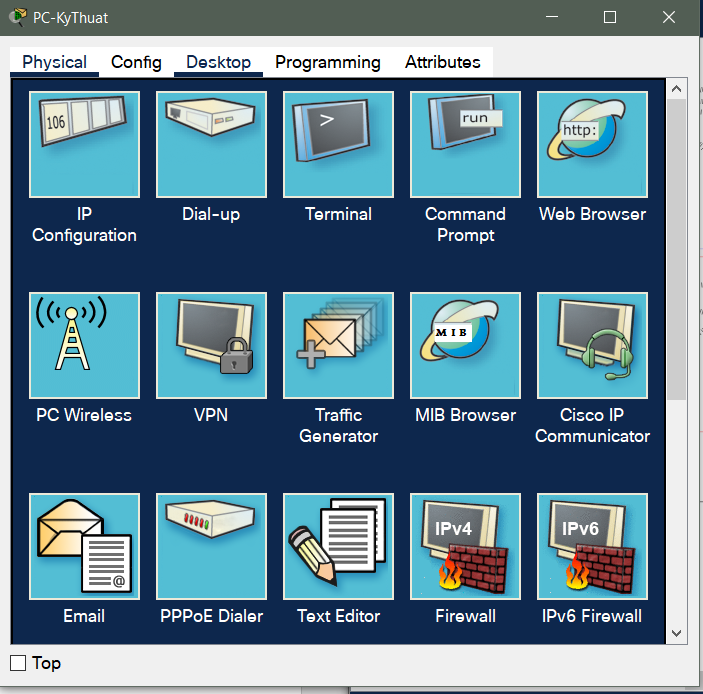
Tương tự các tạo group cho các phòng ban khác :



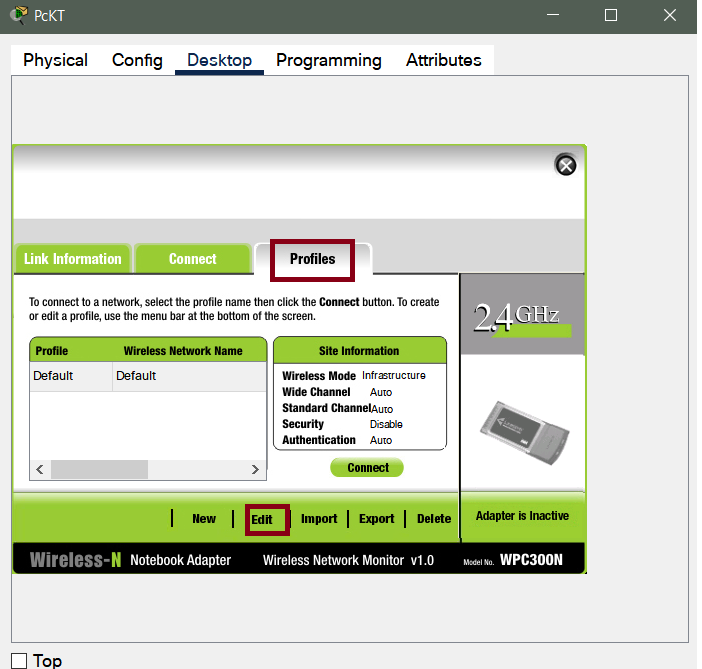
Hình 3.11: Tạo các group cho Access Point

3.2.5 Trên các thiết bị máy khách

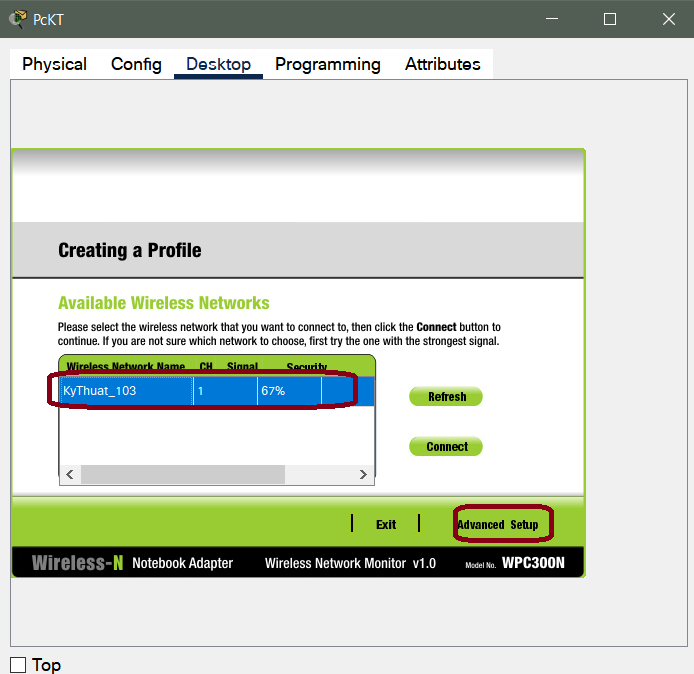
* Với Access Point Phong Ky Thuat
* Kết nối máy tính Pc-KyThuat dùng mạng chỉ giành riêng cho phòng kỹ thuật.
* Vào tab Desktop trên máy tính 🡪 PC Wireless



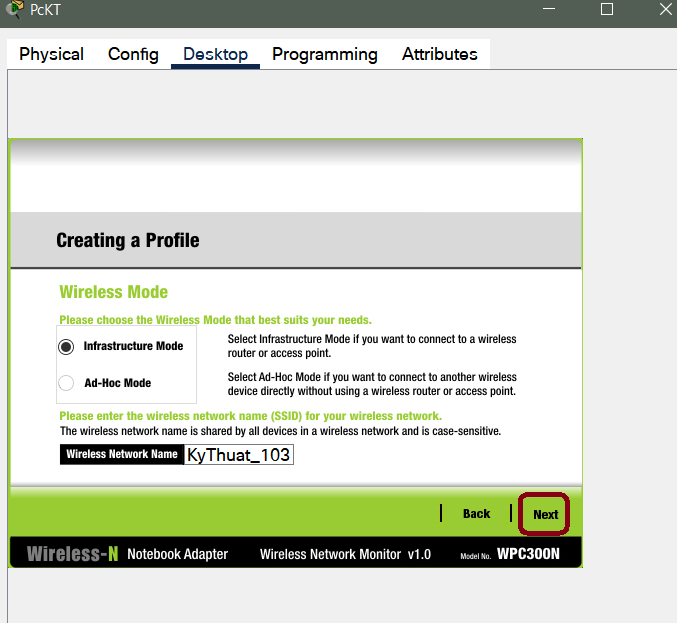
* Chọn Desktop🡪Profiles 🡪 Edit



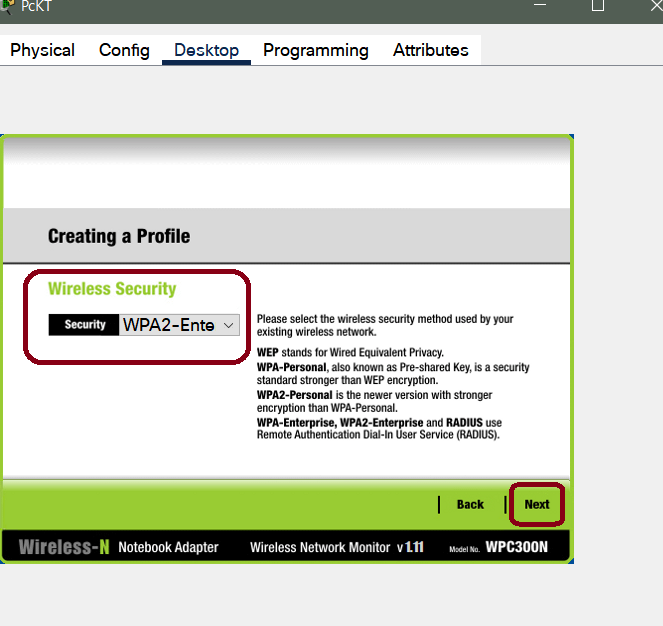
* Chọn vào KyThuat\_103 🡪 Advanced Setup



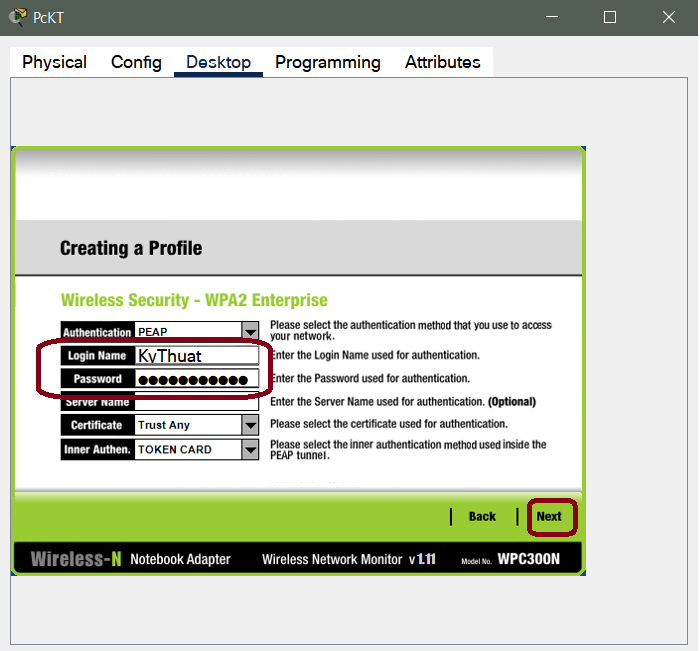
* Nhấn Next



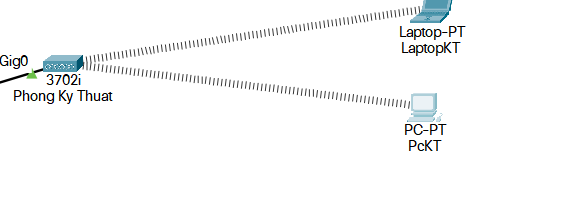
* Chọn chuẩn bảo mật WPA2-Enterpirse 🡪 Next



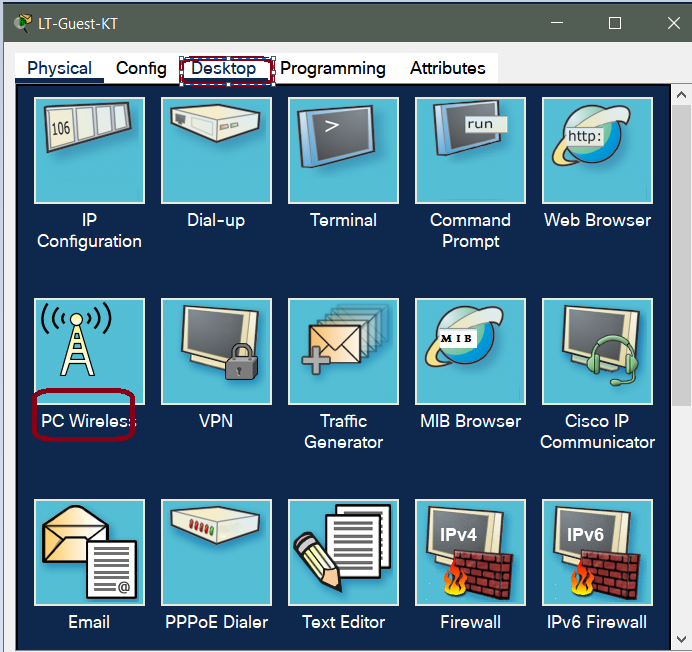
* Nhập vào Login Name/Password: KyThuat/KyThuatPasss🡪Next



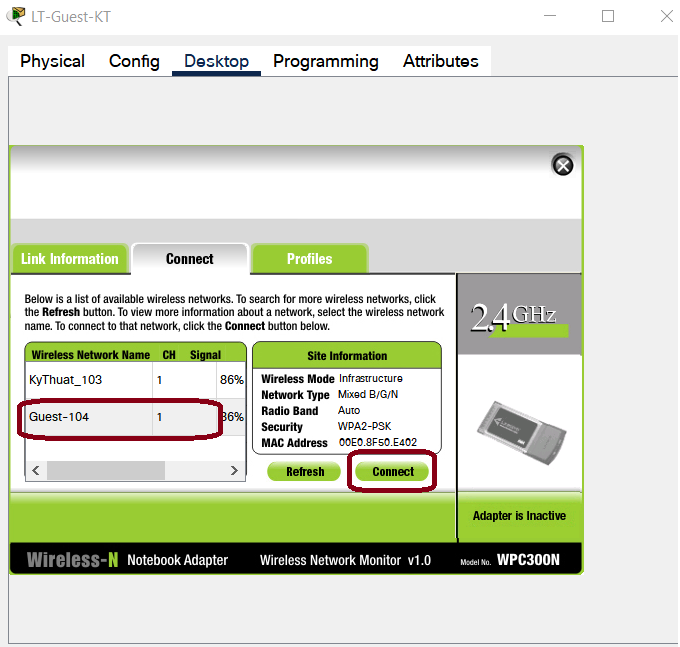
Máy tính đã kết nối được với Access point Phong Ky Thuat



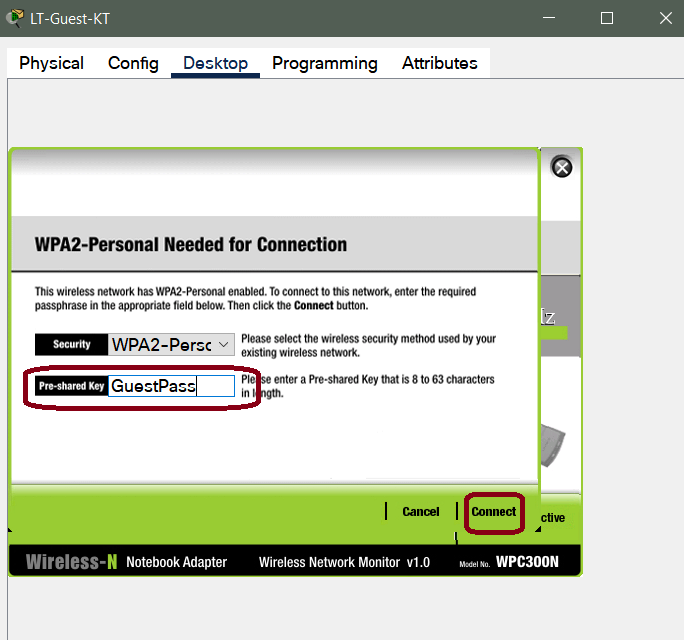
* Kết nối thiết bị dùng mạng sử dụng cho khách
* Vào thiết bị  Desktop  PC Wireless



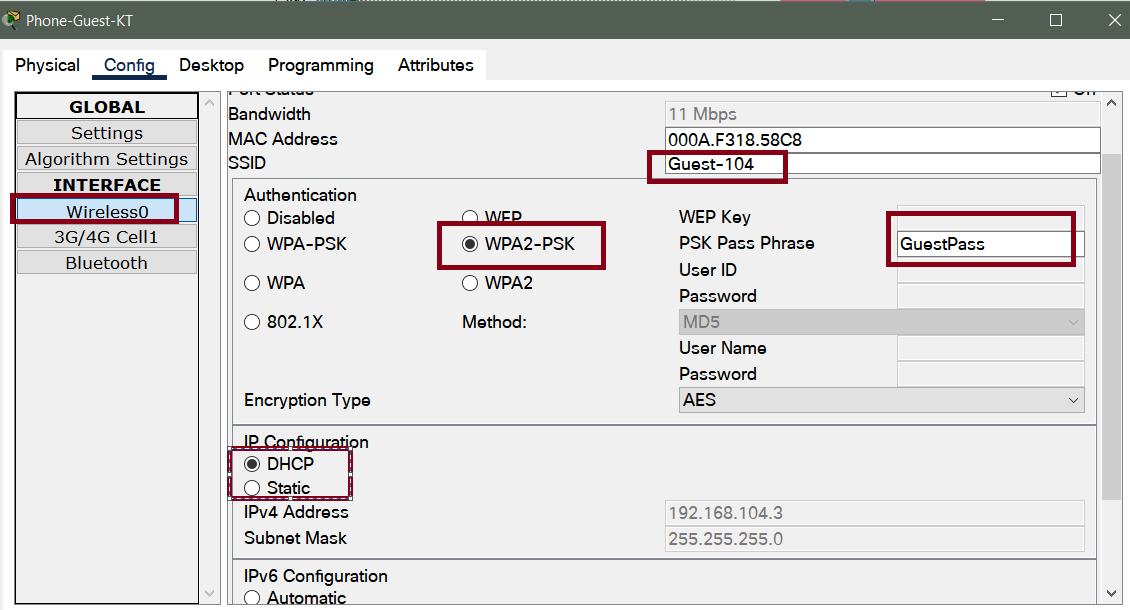
* Vào tab Connect  Chọn Guest-104  Connect



* Nhập mật khẩu khi cài đặt bảo mật GuestPass Connect

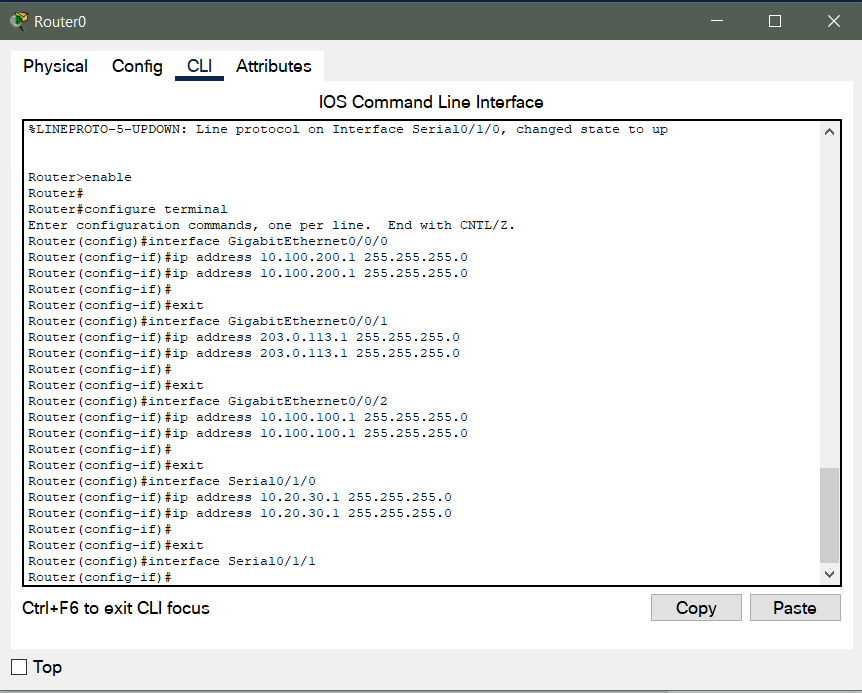


* Đối với thiết bị smartphone khi kết nối : Vào tab Config  Wireless  Điền SSID của WLAN ở đây điền Guest-104, tiếp thep chọn chuẩn bảo mật ở đây chọn WP2-PSK và nhập mật khẩu vào ô PSK Pass Phrase sau đó chọn lại thiết lập DHCP để thiết bị được cấp địa chỉ Ip.



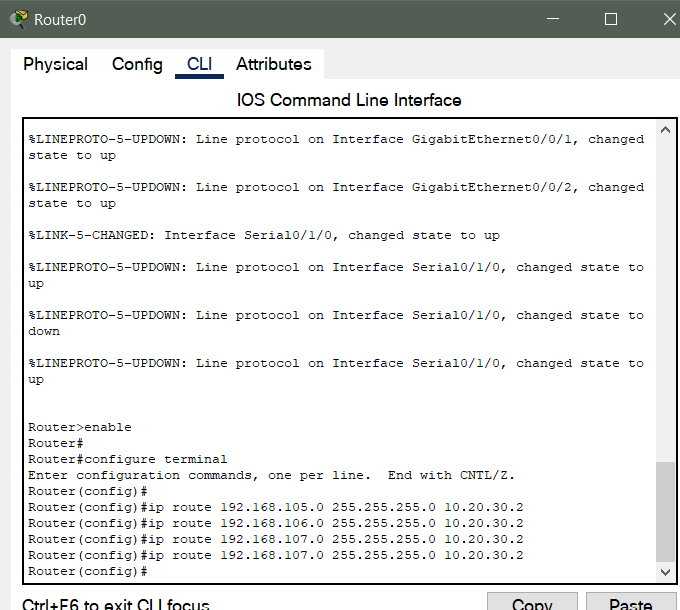
3.2.6 Cấu ***hình*** ngoài Internet

* **Cấu hình router 0**
* **Đặt địa chỉ IP như bảng địa chỉ đã cung cấp**



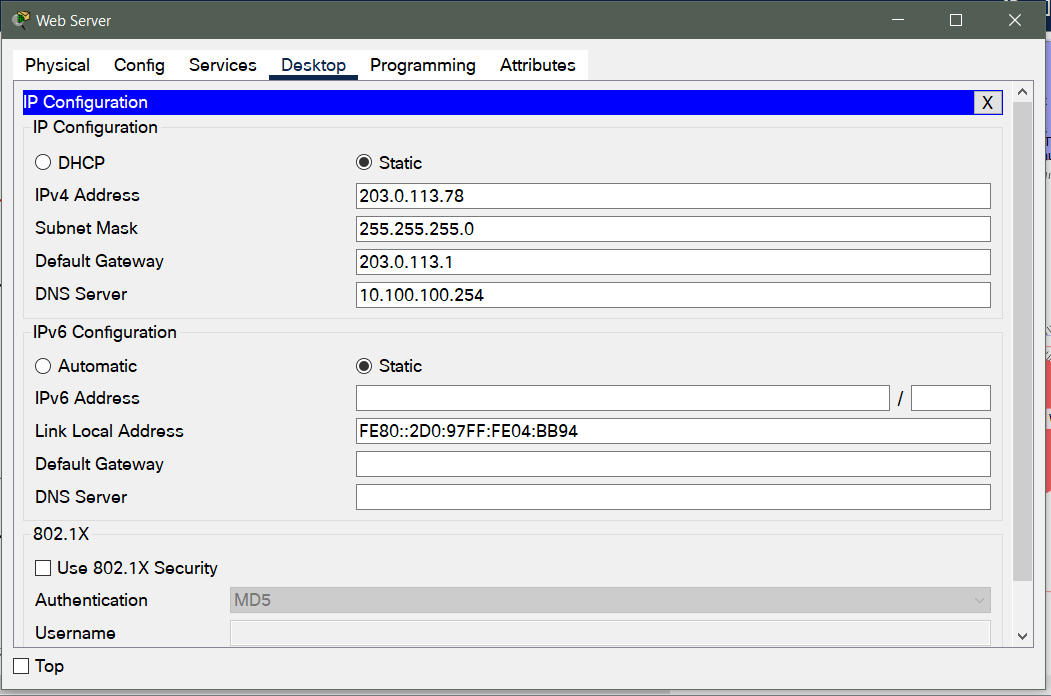
Hình 3.12: Cài đặt địa chỉ IP cho router R0

* Cấu hình định tuyến để liên thông giữa các mạng



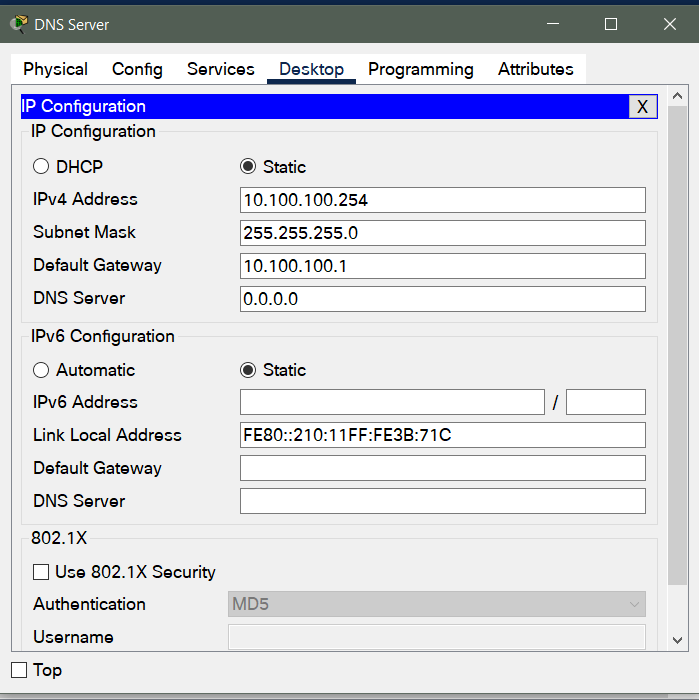
Hình 3.13: Cấu hình IP route

* Cấu hình Web Server

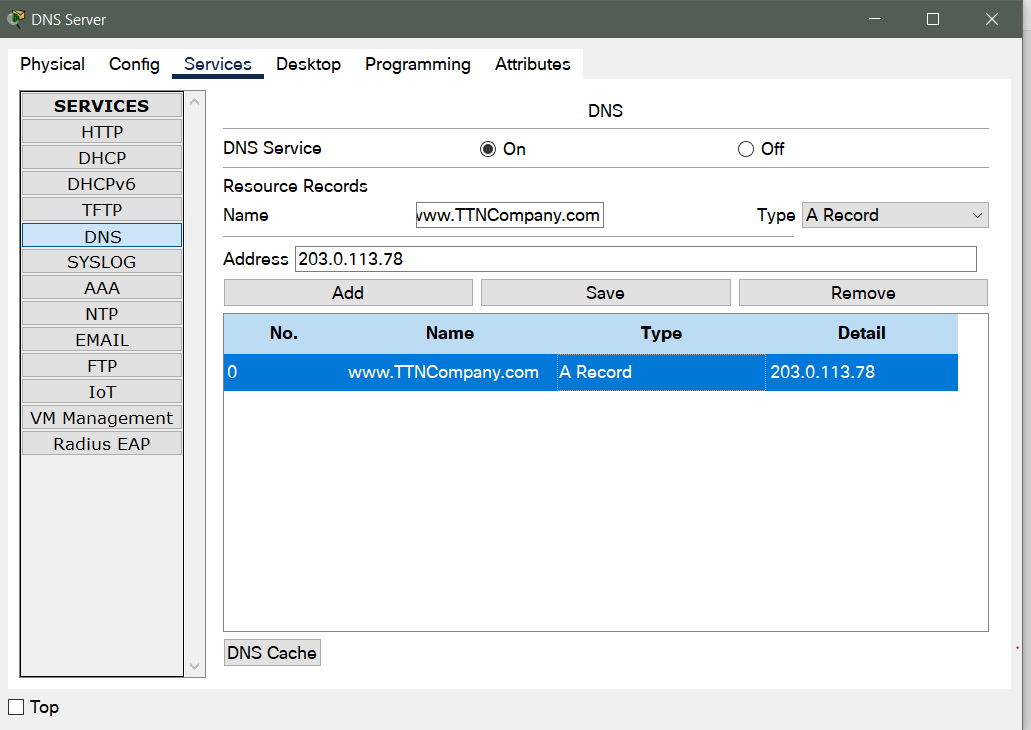


Hình 3.14: Đặt địa chỉ cho Web Server

* Cấu hình DNS Server



Hình 3.15: Đặt địa chỉ cho DNS Server



Hình 3.16: Cấu hình phân giải tên miền cho Web Server

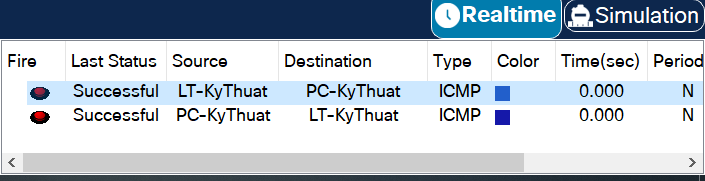
3.3 Kết quả chạy chương trình

3.3.1 Kiểm tra kết nối giữa các thiết bị với nhau.

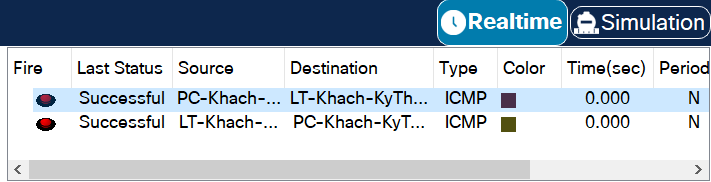
* Kiểm tra giữa các máy cùng phòng ban

Ví dụ: Như 2 máy kết nối trong mạng riêng của phòng kỹ thuật

Kiểm tra trên công cụ Packet Tracer

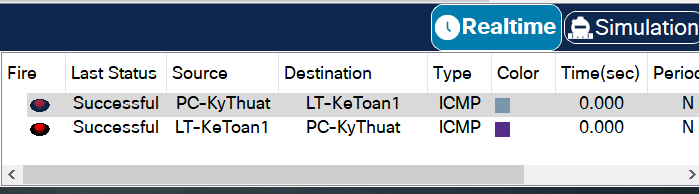


Hình 3.17: Kiểm tra kết nối giữa 2 máy dùng mạng riêng của phòng kỹ thuật

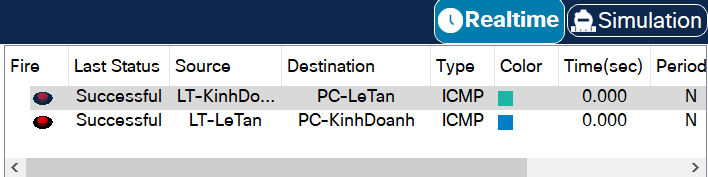


Hình 3.18: Kiểm tra kết nối giữa 2 máy dùng mạng chung cho khách

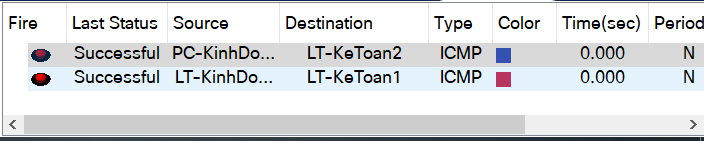
* Kiểm tra giữa các máy khác phòng ban



Hình 3.19: Kiểm tra kết nối giữa máy phòng kỹ thuật và máy phòng kế toán



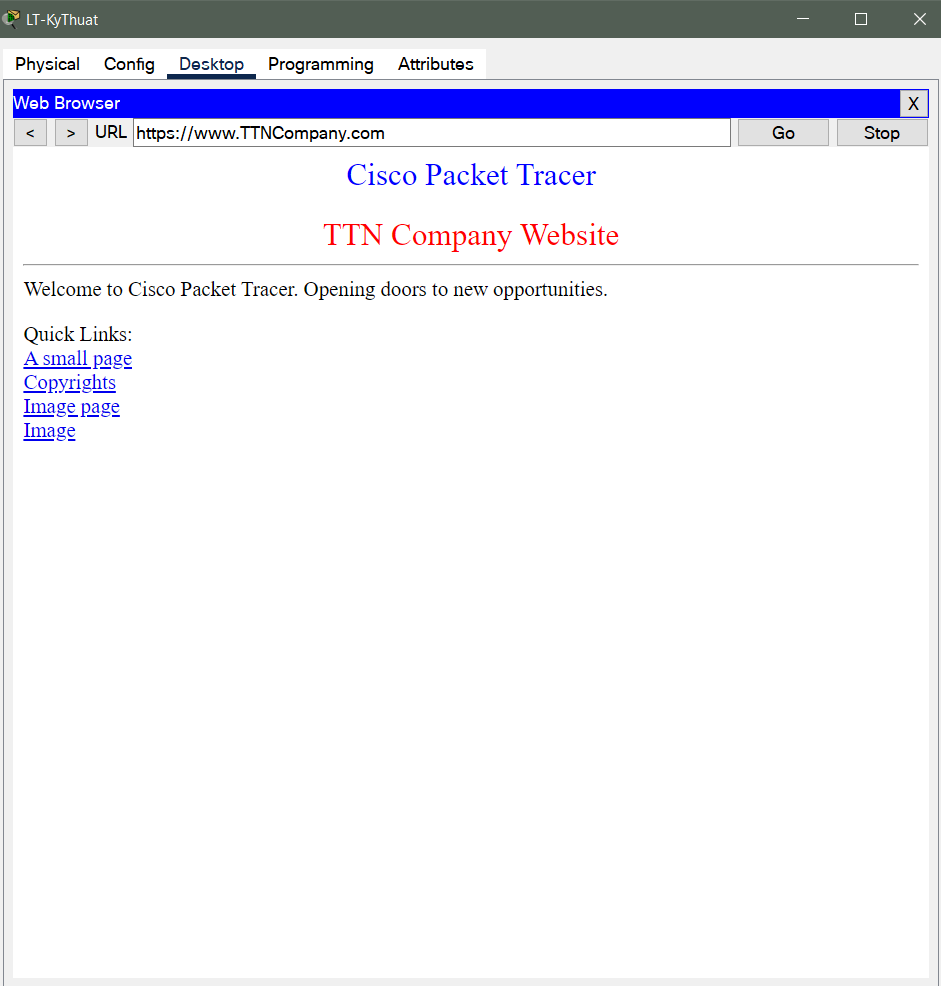
Hình 3.20: Kiểm tra kết nối giữa máy phòng kinh doanh và máy phòng lễ tân



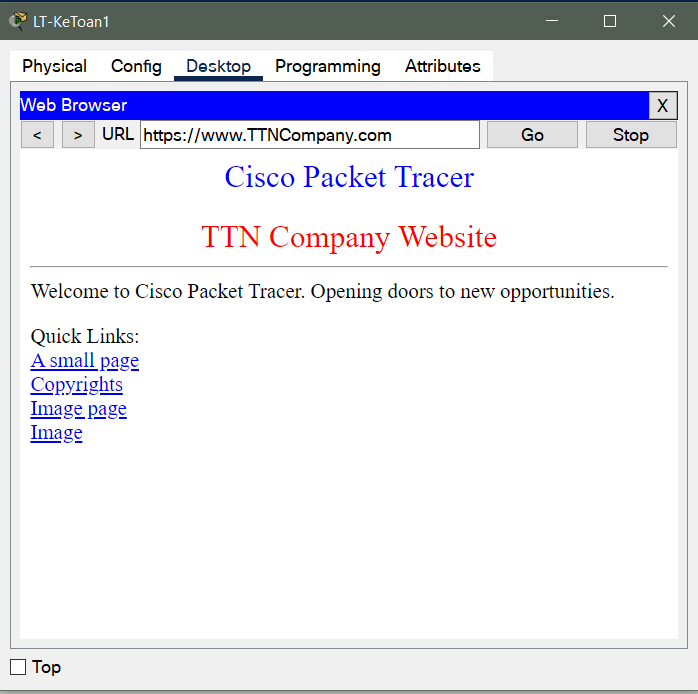
Hình 3.21: Kiểm tra kết nối giữa máy phòng kinh doanh và máy phòng kế toán

3.3.2 Kiểm tra kết nối giữa các thiết bị đến Web Server

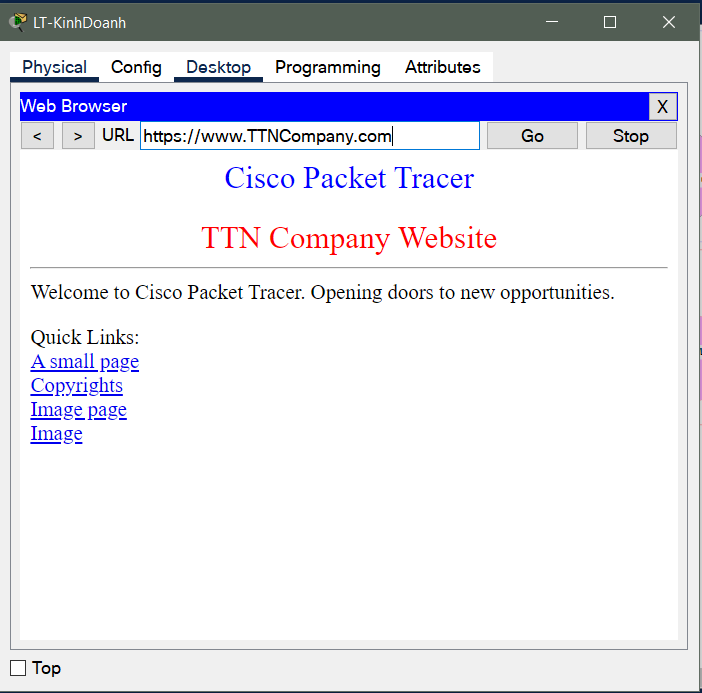
Ta truy cập vào Web Browser của các thiết bị và gõ tên miền của trang web https://[www.TTNCompany.com](http://www.TTNCompany.com)



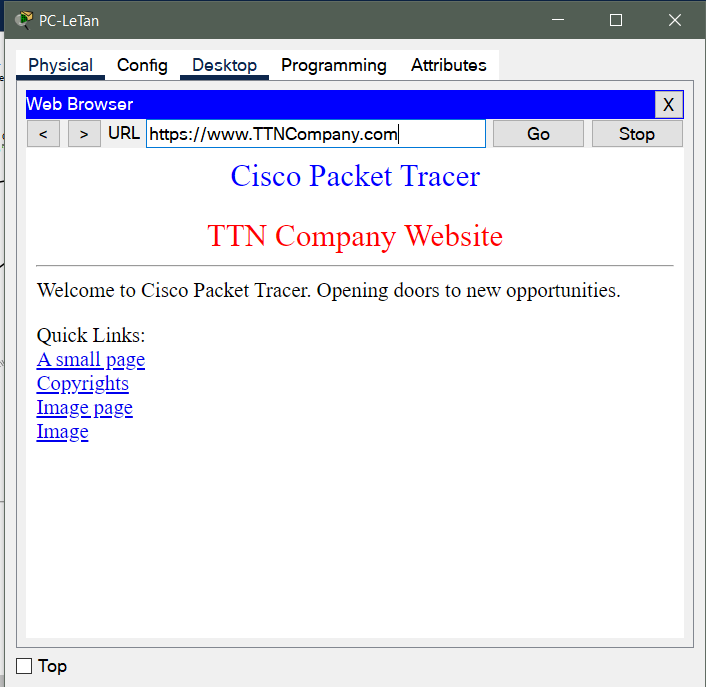
Hình 3.21: Kết nối máy từ phòng kỹ thuật đến Web Server



Hình 3.22: Kết nối máy từ phòng kế toán đến Web Server



Hình 3.22: Kết nối máy từ phòng kinh doanh đến Web Server



Hình 3.23: Kết nối máy từ phòng lễ tân đến Web Server

CHƯƠNG 4 – KẾT LUẬN

Qua bài báo cáo cuối môn, em đã tìm hiểu cách thức xây dựng một mạng không dây cho một doanh nghiệp là như thế nào từ khảo sát khách hàng, lên danh sách thiết bị, dự trù chi phí, thiết kế đề xuất mô hình củng cố các kiến thức cài đặt IP, cấu hình cho WLC kết nối cho các Access Point tạo WLAN và cài đặt bảo mật trên WLAN. Do mô hình còn hạn chế về mặt quy mô và ít bảo mật, nhưng cũng đã củng cố cho em phần nào về kiến thức có thể sau này áp dụng cho các mô hình doanh nghiệp có quy mô lớn hơn và yêu cầu cao hơn.

TÀI LIỆU THAM KHẢO

1. Mạng máy tính - Những thông tin cần biết để xây dựng hệ thống mạng hoàn chỉnh. (2018). Retrieved 20 December 2021, from <https://bizflycloud.vn/tin-tuc/he-thong-mang-la-gi-co-nhung-loai-mang-may-tinh-nao-20180309122116793.htm>
2. Nguyen, A. (2021). Tìm hiểu về bảo mật trong mạng không dây. Retrieved 20 December 2021, from <https://maiphuong.vn/blogs/kien-thuc/tim-hieu-ve-bao-mat-trong-mang-khong-day>
3. Thanh, C. (2020). Các chuẩn mạng không dây. Retrieved 20 December 2021, from <https://tamthanh.pro.vn/ho-tro/huong-dan/cac-chuan-mang-khong-day-1.html>
4. (2020). Retrieved 18 December 2021, from <https://www.youtube.com/watch?v=bN8Rh6-QjEY&ab_channel=ChristianAugustoRomeroGoyzueta>