

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 cho
doanh nghiệp THL**

Người hướng dẫn: TS. BÙI QUY ANH

Người thực hiện: HUỲNH HỮU HIỆP – 51800677

Lớp : 18050402

Khoa : 22

THÀNH PHỐ HỒ CHÍ MINH, NĂM 2020

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 cho
doanh nghiệp THL**

Người hướng dẫn: TS. **BÙI QUY ANH**
Người thực hiện: **HUỲNH HỮU HIỆP**
Lớp : **18050402**
Khoá : **22**

THÀNH PHỐ HỒ CHÍ MINH, NĂM 2020

LỜI CẢM ƠN

Lời đầu tiên tôi chân thành cảm ơn giảng viên hướng dẫn của tôi là thầy Bùi Quy Anh. Người đã hướng dẫn trên lớp và truyền đạt khá nhiều kiến thức bổ ích cho tôi trong suốt quá trình học tập cũng như giải đáp tất cả các thắc mắc mà tôi gặp phải. Và hơn thế nữa thầy còn là người cung cấp cho tôi nguồn tài liệu bổ ích cho chúng tôi. Từ đó, đó là nguồn kiến thức để tôi có thể nắm vững và đọc thêm một số tài liệu mà thầy cung cấp để có thể hoàn thành bài báo cáo như ngày hôm nay một cách hoàn thiện nhất. Do kiến thức còn hạn chế và cũng như không tránh khỏi những sai sót, qua đây tôi mong thầy có những ý kiến, đánh giá của thầy để bài báo cáo có thể hoàn thiện hơn.

Em chân thành cảm ơn!

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

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

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

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

TP. Hồ Chí Minh, ngày tháng năm

Tác giả

(ký tên và ghi rõ họ tên)

Huỳnh Hữu Hiệp

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

Hiện nay với sự phát triển ngày càng lớn mạnh và nhanh chóng của công nghệ thông tin mà ở đây là mạng không dây là rất quan trọng thì việc triển khai hệ thống mạng không dây trong doanh nghiệp là một việc cực kỳ cần thiết để sử dụng trong nội bộ doanh nghiệp và sử dụng Internet trong doanh nghiệp. Nhưng đi đôi với đó là một số rủi ro mà chúng ta có thể gặp phải về độ bảo mật, an toàn của hệ thống thì chúng ta cần một số thiết lập cơ bản cũng như nâng cao để đảm bảo an toàn và doanh nghiệp hoạt động tốt nhất. Qua đó, bài báo cáo hôm nay sẽ trình bày ý tưởng để thiết kế một mạng không dây cho doanh nghiệp THL nhằm áp dụng thực tế cho doanh nghiệp. Để làm rõ vấn đề thì bài báo sẽ trình bày ngắn gọn trong bốn phần. Gồm: Phần đầu tiên sẽ là giới thiệu doanh nghiệp, về cách thức hoạt động cũng như yêu cầu về lắp đặt của công ty từ đó sẽ đề xuất hướng giải quyết tối ưu cho doanh nghiệp. Phần hai sẽ trình bày cơ bản về các khái niệm như mạng máy tính, wifi, sự phát triển của thế hệ mạng và các giao thức được sử dụng hiện nay, bên cạnh đó trình bày các mối đe dọa dành cho hệ thống cũng như các cách thức phòng tránh nhằm giảm rủi ro, từ đó đề xuất các thiết bị cần dùng và giá thành dự đoán cần lắp đặt. Phần ba sẽ demo cơ bản về mô hình sẽ lắp đặt cho doanh nghiệp bao gồm: Bảng thông tin địa chỉ cũng như thông tin WLAN để tạo kết nối cần thiết và thực hiện cấu hình cần thiết cho các thiết bị có trong hệ thống và thực hiện kiểm tra kết quả chạy chương trình. Phần bốn sẽ kết luận về các vấn đề của việc triển khai mô hình mạng không dây cho doanh nghiệp THL.

MỤC LỤC

LỜI CẢM ƠN	i
PHẦN XÁC NHẬN VÀ ĐÁNH GIÁ CỦA GIẢNG VIÊN	iii
TÓM TẮT	iv
MỤC LỤC.....	1
DANH MỤC CÁC BẢNG BIẾU, HÌNH VẼ, ĐỒ THỊ	6
CHƯƠNG 1 – MÔ TẢ ĐỀ TÀI.....	13
1.1 Thông tin cơ bản về doanh nghiệp.....	13
1.2 Yêu cầu từ khách hàng.....	13
1.3 Đề xuất hướng giải quyết.....	14
CHƯƠNG 2 – CƠ SỞ LÝ THUYẾT	16
2.1 Các khái niệm cơ bản.....	16
2.1.1 Khái niệm mạng máy tính	16
2.1.1.1 Khái niệm	16
2.1.1.2 Các loại mạng phô biến	17
2.1.2 Khái niệm mạng wifi	21
2.1.3 Các mô hình mạng wifi	23
2.1.4 Các chuẩn wifi cơ bản	26
2.1.5 Thế hệ mạng 1G, 2G, 3G, 4G, 5G	30
2.1.5.1 Mạng di động thế hệ đầu tiên – 1G	30
2.1.5.2 Thế hệ mạng 2G	32
2.1.5.3 Thế hệ mạng 3G	34
2.1.5.4 Thế hệ mạng 4G	37
2.1.5.5 Thế hệ mạng 5G	38
2.1.5.6 So sánh các thế hệ mạng.....	40
2.1.6 Khái niệm an toàn bảo mật không dây	40
2.1.6.1 Các lỗ hổng chủ yếu trong hệ thống viễn thông.....	40

2.1.6.2	Các hình thức tấn công WLAN	44
2.1.6.3	Kiến trúc Hot Spot và các hoạt động khác	49
2.1.6.4	Các giao thức AAA để kiểm soát quyền truy cập vào mạng riêng	53
2.1.6.5	Các phương pháp bảo mật không dây	56
2.2	Các thiết bị dùng trong hệ thống mạng	62
2.2.1	Các thiết bị chủ yếu dùng trong hệ thống	63
2.2.2	Bảng giá tham khảo các thiết bị được sử dụng trong xây dựng mô hình DEMO	65
CHƯƠNG 3 – MÔ HÌNH DEMO		67
3.1	Mô hình đề xuất	67
3.1.1	Bảng địa chỉ	67
3.1.2	Bảng thông tin WLAN	69
3.1.3	Mô hình đề xuất	69
3.2	Cấu hình các thiết bị	70
3.2.1	Thiết lập IP cho DNS Server, Web Server, RADIUS Server.....	70
3.2.2	Thiết lập IP cho Enterprise PC	72
3.2.3	Thiết lập IP cho Wireless LAN Controller (WLC).	73
3.2.4	Cấu hình thiết bị Multilayer Switch.	73
3.2.5	Cấu hình thiết bị Router 1.	75
3.2.6	Cấu hình thiết bị Router 0.	76
3.2.7	Cấu hình thiết bị Wireless LAN Controller.....	78
3.2.7.1	Cấu hình các giao diện VLAN.	78
3.2.7.2	Cấu hình DHCP Scope cho mạng quản lý không dây....	82
3.2.7.3	Cấu hình WLC với các địa chỉ server bên ngoài.....	84
3.2.7.4	Tạo các mạng WLANs	87
3.2.7.5	Tạo AP Group	95

3.2.8 Kết nối các thiết bị các nhân ở doanh nghiệp THL với mạng WLAN.....	97
3.2.8.1 Phòng Lê Tân	97
3.2.8.2 Phòng Họp	102
3.2.8.3 Phòng Giám Đốc	105
3.2.8.4 Phòng Kinh Doanh	111
3.2.8.5 Phòng Marketing	114
3.2.8.6 Phòng tài chính	117
3.2.9 Cấu hình thiết bị Home Wireless Router tại nhà.....	120
3.3 Kết quả chạy chương trình.....	127
3.3.1 Kiểm tra kết nối thiết bị của doanh nghiệp với internet	127
3.3.2 Kiểm tra kết nối thiết bị gia đình với internet	134
3.3.3 Gửi email giữa các phòng doanh nghiệp	136
CHƯƠNG 4 – KẾT LUẬN.....	138

DANH MỤC KÍ HIỆU VÀ CHỮ VIẾT TẮT

CÁC KÝ HIỆU

CÁC CHỮ VIẾT TẮT

LAN	Local Area Network (Mạng cục bộ)
MAN	Metropolitan Area Network (Mạng đô thị)
WAN	Wide Area Network (Mạng diện rộng)
WLAN	Wireless Local Area Network (Mạng không dây cục bộ)
Wifi	Wireless Fidelity (Mạng không dây)
IEEE	Institute of Electrical and Electronics Engineers (Hội kỹ sư Điện và Điện tử)
THL	Doanh nghiệp Tường Hiệp Luân
P2P	Peer to Peer (Mô hình mạng ngang hàng)
IBSSs	Independent Basis Service Set (Mô hình mạng độc lập)
BSS	Basic Service Sets (Mô hình mạng cơ bản)
AP	Access Point
ESS	Extend Service Set (Hệ thống chuyển mạch điện tử)
MIMO	Multiple In, Multiple Out
TDMA	Time Division Multile Access (Đa truy nhập phân chia theo thời gian)
CDMA	Code Division Multile Access (Đa truy nhập phân chia theo mã)
GSM	Global System for Mobile Communications (Hệ thống giao tiếp di động toàn cầu)
MAC	Media Access Control (Kiểm soát phương tiện truyền thông)
IP	Internet Protocol (Kiểm soát truy cập mạng)
DoS	Denial of Service Attack (Tấn công từ chối dịch vụ)
CKA	Compromised Key Attack (Tấn công phá mã khóa)

DHCP	Dynamic Host Configuration Protocol (Kiểm soát cấu hình máy chủ tự động)
OSI	Open Systems Interconnection Reference Model (Mô hình tham chiếu kết nối các hệ thống mở)
UDP	User Datagram Protocol
TCP	Transmission Control Protocol
WPA	Wi-Fi Protected Access (Giao thức trong mạng an ninh)
WPA2	Wi-Fi Protected Access (Giao thức trong mạng an ninh)
WEP	Wired Equivalent Privacy (Thuật toán bảo mật)
EAP	Email AntiSpam Protection (Chống spam bằng công nghệ AL)
WLC	Wisconsin Lutheran College
VPN	Virtual Protocol Network (Mạng riêng ảo)
SNMP	Simple Network Management Protocol (Quản lý kiểm soát mạng đơn giản)
PSK	Pre-Shared Key (Chia sẻ khóa bí mật)
AAA	Authentication, Authorization, Accounting

DANH MỤC CÁC BẢNG BIỂU, HÌNH VẼ, ĐỒ THỊ

DANH MỤC HÌNH

Hình 2. 1: Tổng quan về mạng máy tính.....	16
Hình 2. 2: Mô hình mạng nganh hàng.	17
Hình 2. 3: Mô hình khách – chủ (client – server).	18
Hình 2. 4: Mô hình mạng LAN.....	19
Hình 2. 5: Mô hình mạng WAN.....	20
Hình 2. 6: Mô hình mạng MAN.....	21
Hình 2. 7: Mô hình mạng wifi.....	22
Hình 2. 8: Mô hình mạng độc lập.	24
Hình 2. 9: Mô hình mạng cơ sở.....	25
Hình 2. 10: Mô hình mạng mở rộng.	26
Hình 2. 11: Bảng thông tin tổng hợp về mạng wifi.	27
Hình 2. 12: Những thiết bị sử dụng 1G đầu tiên.....	31
Hình 2. 13: Các thiết bị sử dụng mạng 2G.....	34
Hình 2. 14: Thẻ hệ mạng 3G xuất hiện.	37
Hình 2. 15: SIM 4G bắt đầu được sử dụng.	38
Hình 2. 16: Mạng 5G được sử dụng rộng rãi.	40
Hình 2. 17: Sự phát triển các thẻ hệ mạng.	40
Hình 2. 18: Kênh liên lạc giữa 2 người Alice và Bob.....	41
Hình 2. 19: Mô hình phân biệt giữa hai bên giao tiếp	42
Hình 2. 20: Mô hình chống lại cuộc tấn công từ attacker.	44
Hình 2. 21: Các cuộc tấn công nội bộ.	45
Hình 2. 22: Các cuộc tấn công phá mã khóa.....	47
Hình 2. 23: Kiến trúc Hot Spot.	50
Hình 2. 24: Các hoạt động trong kiến trúc của Hot Spot.	51
Hình 2. 25: Các hoạt động trong kiến trúc của Hot Spot.	51

Hình 2. 26: Các hoạt động trong kiến trúc của Hot Spot	52
Hình 2. 27: Kiến trúc AAA	53
Hình 2. 28: Thay đổi tên mạng SSID	58
Hình 2. 29: Thay đổi tên người dùng và mật khẩu	59
Hình 2. 30: Sử dụng mã hóa khác nhau để tăng cường bảo mật	60
Hình 2. 31: Chọn mật khẩu đủ mạnh để bảo mật tốt hơn	60
Hình 2. 32: Sử dụng VPN để bảo mật	61
Hình 2. 33: Quản lý firmware của bộ định tuyến	62
Hình 2. 34: Tắt các quản lý không cần thiết	62
Hình 2. 35: Các thiết cơ bản được sử dụng	65
Hình 2. 59: Giao diện kết quả tạo thành công Scope Name management	84
Hình 3. 1: Mô hình đề xuất cho doanh nghiệp	70
Hình 3. 2: Giao diện địa chỉ DNS Server	71
Hình 3. 3: Giao diện địa chỉ Web Server	71
Hình 3. 4: Giao diện địa chỉ RADIUS Server	72
Hình 3. 5: Giao diện địa chỉ Enterprise PC	72
Hình 3. 6: Giao diện địa chỉ WLC	73
Hình 3. 7: Câu lệnh tạo các vlan trên multilayer switch	73
Hình 3. 8: Kết quả sau khi tạo các vlan trên multilayer switch	74
Hình 3. 9: Câu lệnh cấu hình trunk cho các cổng trên multilayer switch	74
Hình 3. 10: Câu lệnh cấu hình địa chỉ IP cho các cổng của router 1	75
Hình 3. 11: Câu lệnh cấu hình các cổng ảo trên router 1	75
Hình 3. 12: Câu lệnh cấu hình DHCP pool trên router 1	76
Hình 3. 13: Câu lệnh cấu hình địa chỉ IP cho các cổng của router 0	77
Hình 3. 14: Câu lệnh cấu hình định tuyến tĩnh trên router 0	77
Hình 3. 15: Câu lệnh cấu hình DHCP pool trên router 0	78

Hình 3. 16: Giao diện đăng nhập vào bộ điều khiển WLC.....	79
Hình 3. 17: Giao diện các thao tác tạo mạng VLAN.	80
Hình 3. 18: Giao diện điền thông tin tạo WLAN 10.....	80
Hình 3. 19: Giao diện cấu hình địa chỉ cho WLAN 10.....	81
Hình 3. 20: Giao diện kết quả tạo thành công các WLAN.	82
Hình 3. 21: Giao diện các thao tác tạo DHCP Scope.....	83
Hình 3. 22: Giao diện điền thông tin tạo DHCP Scope.	83
Hình 3. 23: Giao diện cấu hình địa chỉ cho management.	84
Hình 3. 24: Giao diện các thao tác tạo RADIUS Server.....	85
Hình 3. 25: Giao diện cấu hình thông tin cho RADIUS Server.....	85
Hình 3. 26: Kết quả kết quả tạo thành công RADIUS Server.	86
Hình 3. 27: Giao diện các thao tác tạo SNMP Trap Receiver.	86
Hình 3. 28: Giao diện cấu hình thông tin SNMP Trap Receiver.	87
Hình 3. 29: Giao diện kết quả tạo thành công SNMP Trap Receiver.	87
Hình 3. 30: Giao diện các thao tác tạo mạng WLAN 6.	88
Hình 3. 31: Giao diện cấu hình thông tin cho WLAN 6.	88
Hình 3. 32: Giao diện cấu hình thông tin ở tab General cho WLAN 6.	89
Hình 3. 33: Giao diện cấu hình Security cho Layer 2 cho WLAN 6.	89
Hình 3. 34: Giao diện cấu hình Authentication Key Management ở Layer 2 cho WLAN 6.	90
Hình 3. 35: Giao diện cấu hình Advanced cho WLAN 6.	91
Hình 3. 36: Giao diện các thao tác tạo mạng WLAN 1.	92
Hình 3. 37: Giao diện cấu hình thông tin cho WLAN 1.	92
Hình 3. 38: Giao diện cấu hình thông tin ở tab General cho WLAN 1.	93
Hình 3. 39: Giao diện cấu hình Security cho Layer 2 cho WLAN 1.	93
Hình 3. 40: Giao diện cấu hình Secutity cho AAA Servers cho WLAN 1.....	94
Hình 3. 41: Giao diện cấu hình Advanced cho WLAN 1.	94

Hình 3. 42: Giao diện cấu hình thành công tạo các WLAN 1, 2, 3, 4, 5, 6	95
Hình 3. 43: Giao diện các thao tác tạo AP Groups cho phòng lễ tân.....	95
Hình 3. 44: Giao diện chọn cấu hình WLANs cho thiết bị Access Point phòng lễ tân.	96
Hình 3. 45: Giao diện cấu hình APs cho thiết bị Access Point phòng lễ tân	96
Hình 3. 46: Giao diện sau khi tạo thành công các AP Groups cho các phòng.	97
Hình 3. 47: Giao diện các bước vào PC Wireless của PC_LETAN.	98
Hình 3. 48: Giao diện chọn LeTan để kết nối cho PC_LETAN.	99
Hình 3. 49: Giao diện chọn Security và điền mật khẩu kết nối cho PC_LETAN.	100
Hình 3. 50: Giao diện các thao tác vào Wireless0 của Guest Tablet PC.	101
Hình 3. 51: Giao diện cấu hình thông tin để kết nối cho Guest Tablet PC.....	101
Hình 3. 52: Kết quả sau khi kết nối thành công các thiết bị cá nhân ở phòng lễ tân... <td>102</td>	102
Hình 3. 53: Giao diện các bước vào PC Wireless của laptop NhanVien6.....	103
Hình 3. 54: Giao diện chọn Edit để cấu hình kết nối cho laptop NhanVien6.....	103
Hình 3. 55: Giao diện chọn PhongHop để kết nối cho laptop NhanVien6.	104
Hình 3. 56: Giao diện chọn Security cho laptop NhanVien6.	104
Hình 3. 57: Giao diện điền thông tin để kết nối cho laptop NhanVien6.....	105
Hình 3. 58: Kết quả sau khi kết nối thành công các thiết bị cá nhân ở phòng họp.....	105
Hình 3. 59: Giao diện các bước vào PC Wireless của laptop GIAMDOC.	106
Hình 3. 60: Giao diện chọn Edit để cấu hình kết nối cho laptop GIAMDOC.	107
Hình 3. 61: Giao diện chọn GiamDoc để kết nối cho laptop GIAMDOC.....	107
Hình 3. 62: Giao diện chọn Security cho laptop GIAMDOC.....	108
Hình 3. 63: Giao diện điền thông tin để kết nối cho laptop GIAMDOC.....	109
Hình 3. 64: Giao diện các thao tác vào Wireless0 của laptop GIAMDOC.	110
Hình 3. 65: Giao diện cấu hình thông tin để kết nối cho laptop GIAMDOC	110
Hình 3. 66: Kết quả sau khi kết nối thành công các thiết bị cá nhân ở phòng giám đốc.	
	111
Hình 3. 67: Giao diện các bước vào PC Wireless của laptop PC_KD.....	111

Hình 3. 68: Giao diện chọn Edit để cấu hình kết nối cho PC_KD.	112
Hình 3. 69: Giao diện chọn KinhDoanh để kết nối cho PC_KD.	112
Hình 3. 70: Giao diện chọn Security cho PC_KD.	113
Hình 3. 71: Giao diện điền thông tin để kết nối cho PC_KD.	113
Hình 3. 72: Kết quả sau khi kết nối thành công các thiết bị cá nhân ở phòng kinh doanh.	114
Hình 3. 73: Giao diện các bước vào PC Wireless của laptop NhanVien 3.	114
Hình 3. 74: Giao diện chọn Edit để cấu hình kết nối cho laptop NhanVien 3.	115
Hình 3. 75: Giao diện chọn Marketing để kết nối cho laptop NhanVien 3.	115
Hình 3. 76: Giao diện chọn Security cho laptop NhanVien 3.	116
Hình 3. 77: Giao diện điền thông tin để kết nối cho laptop NhanVien 3.	116
Hình 3. 78: Kết quả sau khi kết nối thành công các thiết bị cá nhân ở phòng marketing.	117
Hình 3. 79: Giao diện các bước vào PC Wireless của PC_TC.	117
Hình 3. 80: Giao diện chọn Edit để cấu hình kết nối cho PC_TC.	118
Hình 3. 81: Giao diện chọn TaiChinh để kết nối cho PC_TC.	118
Hình 3. 82: Giao diện chọn Security cho PC_TC.	119
Hình 3. 83: Giao diện điền thông tin để kết nối cho PC_TC.	119
Hình 3. 84: Kết quả sau khi kết nối thành công các thiết bị cá nhân ở phòng tài chính.	120
Hình 3. 85: Đăng nhập vào Home Wireless Router.	120
Hình 3. 86: Thay đổi địa chỉ để phù hợp.	121
Hình 3. 87: Các địa chỉ cần thiết cho thiết lập.	122
Hình 3. 88: Các cài đặt cho Wireless.	122
Hình 3. 89: Chọn chế độ bảo mật, mã hóa phù hợp.	123
Hình 3. 90: Giao diện các bước vào PC Wireless của Home Laptop.	124
Hình 3. 91: Giao diện chọn GiaDinh để kết nối cho Home Laptop.	124

Hình 3. 92: Giao diện chọn Security và điền mật khẩu kết nối cho Home Laptop.	125
Hình 3. 93: Giao diện các thao tác vào Wireless0 của Home Tablet PC.....	125
Hình 3. 94: Giao diện cấu hình thông tin để kết nối cho Home Tablet PC	126
Hình 3. 95: Giao diện kết nối thành công các thiết bị các nhân trong gia đình.	126
Hình 3. 96: Kết quả ping thành công của PC _ LETAN.....	127
Hình 3. 97: Kết quả ping thành công của Guest Smartphone.	127
Hình 3. 98: Kết quả ping thành công từ thiết bị phòng lễ tân đến url Web Server.....	128
Hình 3. 99: Kết quả ping thành công của PC _ TC.....	128
Hình 3. 100: Kết quả ping thành công của NhanVien5.	129
Hình 3. 101: Kết quả ping thành công từ thiết bị phòng tài chính đến url Web Server.	129

Hình 3. 102: Kết quả ping thành công của NhanVien3.	130
Hình 3. 103: Kết quả ping thành công từ thiết bị phòng marketing đến url Web Server.	130

Hình 3. 104: Kết quả ping thành công của PC _ KD.....	131
Hình 3. 105: Kết quả ping thành công của NhanVien1.	131
Hình 3. 106: Kết quả ping thành công từ thiết bị phòng tài chính đến url Web Server.	132

Hình 3. 107: Kết quả ping thành công của THUKY.....	132
Hình 3. 108: Kết quả ping thành công của GIAMDOC.....	133
Hình 3. 109: Kết quả ping thành công từ thiết bị phòng giám đốc đến url Web Server.	133

Hình 3. 110: Kết quả ping thành công của NhanVien6.	134
Hình 3. 111: Kết quả ping thành công từ thiết bị phòng họp đến url Web Server.	134
Hình 3. 112: Kết quả ping thành công của Home Admin.....	135
Hình 3. 113: Kết quả ping thành công của Home Laptop.....	135
Hình 3. 114: Kết quả ping thành công của Home Smartphone.	136

Hình 3. 115: Kết quả ping thành công từ thiết bị gia đình đến url Web Server.	136
Hình 3. 116: Giao diện gửi email từ giám đốc đến nhân viên.	137
Hình 3. 117: Giao diện email nhân viên phòng marketing nhận được từ giám đốc. ...	137

DANH MỤC BẢNG

Bảng 2. 1: Bảng giá các thiết bị sử dụng trong hệ thống.	66
Bảng 3. 1: Bảng địa chỉ được sử dụng trong hệ thống.	68
Bảng 3. 2: Bảng thông tin WLAN.	69

CHƯƠNG 1 – MÔ TẢ ĐỀ TÀI

1.1 Thông tin cơ bản về doanh nghiệp

Doanh nghiệp THL là một doanh nghiệp cơ bản mới được thành lập chưa lâu và chuẩn bị đi vào hoạt động chính thức tại Quận 7. Để đáp ứng nhu cầu về trao đổi, liên lạc thông tin cũng như hoạt động trong doanh nghiệp nhanh chóng thì doanh nghiệp cần tiến hành thiết kế mạng nội bộ cho doanh nghiệp. Cấu trúc trong doanh nghiệp đưa ra là một tòa nhà để thi công lắp đặt gồm các phòng ban như sau:

- Phòng họp chính: đáp ứng nhu cầu cho cùng lúc trên 10 thiết bị.
- Phòng giám đốc: đáp ứng nhu cầu cho 3 thiết bị.
- Phòng kinh doanh: đáp ứng nhu cầu cho 5 thiết bị.
- Phòng Marketing: đáp ứng nhu cầu cho 5 thiết bị.
- Phòng lễ tân: đáp ứng nhu cầu cho 5 thiết bị.
- Phòng tài chính: đáp ứng nhu cầu cho 3 thiết bị.

1.2 Yêu cầu từ khách hàng

Để đáp ứng nhu cầu cho công ty. Công ty đưa ra yêu cầu xây dựng hệ thống mạng wifi đáp ứng được các yếu tố như sau:

- Về thi công, lắp đặt:
 - + Thực hiện nhanh chóng, tiết kiệm tối đa chi phí, hệ thống nhìn đơn giản nhưng hiệu quả cao.

- + Có thể mở rộng, chỉnh sửa thay đổi khi cần thiết.
- Về kĩ thuật: Cần đáp ứng các tiêu chí sau:
 - + Các thiết bị kết nối ổn định, đường truyền tốt, tránh gặp các sự cố bất ngờ.
 - + Giao tiếp trong doanh nghiệp thông qua email của doanh nghiệp để thực hiện trao đổi thông tin trong quá trình làm việc.
 - + Các máy tính trong doanh nghiệp có thể giao tiếp được với nhau để trao đổi thông tin.
 - + Chức năng bảo mật cao, đảm bảo cho dữ liệu đảm bảo tính bí mật, tránh mất mát dữ liệu.
 - + Cấu hình Mail Sever với tên miền riêng cho công ty. Xây dựng kết nối an toàn từ xa. Truy cập và quản lý điều hành công ty từ xa.

1.3 Đề xuất hướng giải quyết

Để giải quyết đúng theo yêu cầu của khách hàng thì cần thiết kế:

Về thi công lắp đặt:

- Lựa chọn các thiết bị có khả năng kết nối tốt phù hợp với doanh nghiệp.
- Chi phí phù hợp với yêu cầu doanh nghiệp.
- Lắp đặt đơn giản nhưng hiệu quả mang lại cao.
- Có thể chỉnh sửa thay đổi và mở rộng về sau nếu cần thiết.

Về cấu trúc mạng như sau:

- Mỗi nhân viên trong từng phòng ban sẽ được cấp tài khoản người dùng và mật khẩu riêng biệt để truy cập vào hệ thống của doanh nghiệp.
- Thực hiện chia các AP theo từng phòng ban khác nhau dựa trên sự quản lý của WLC, mỗi AP có nhiệm vụ chỉ cung cấp internet cho phòng đó nhằm đảm bảo kết nối.
- Ở các phòng như: Phòng Hợp, Phòng Giám Đốc, Phòng Kinh Doanh, Phòng Tài Chính, Phòng Marketing sẽ sử dụng cơ chế xác thực WPA2 – Enterprise để đảm bảo tính bí mật trong doanh nghiệp.
- Ở phòng Lễ Tân sẽ sử dụng cơ chế xác thực WPA2 – Personal do tính bảo mật thấp hơn so với các phòng ban khác.

CHƯƠNG 2 – CƠ SỞ LÝ THUYẾT

2.1 Các khái niệm cơ bản

2.1.1 Khái niệm mạng máy tính

2.1.1.1 Khái niệm

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

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



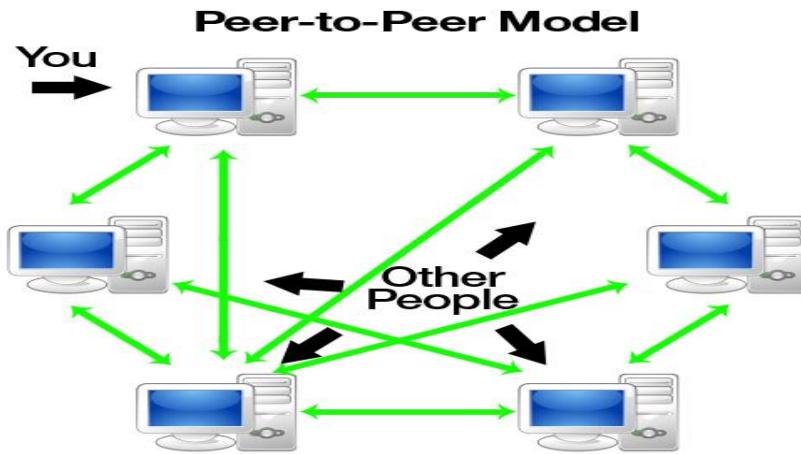
Hình 2. 1: Tổng quan về mạng máy tính.

2.1.1.2 Các loại mạng phổ biến

- ❖ Phân loại theo chức năng

- + Mô hình mạng ngang hàng (Peer – to – Peer)

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



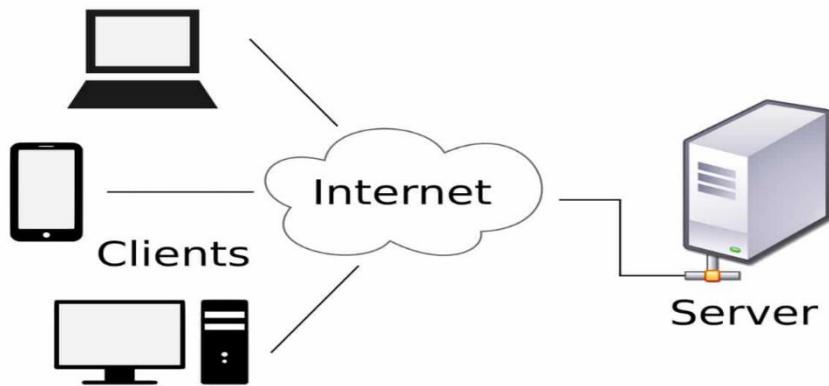
Hình 2. 2: Mô hình mạng ngang hàng.

- + Mô hình khách – chủ (Client – Server)

Trong mô hình này, một hoặc vài máy sẽ được chọn để đảm nhận việc quản lý và cung cấp tài nguyên (chương trình, dữ liệu, thiết bị,...) được gọi là máy chủ (Server), các máy khác sử dụng tài nguyên này được gọi là máy khách (Client).

Máy chủ là máy tính đảm bảo việc phục vụ các máy khách bằng cách điều khiển việc phân phối tài nguyên nằm trong mạng với mục đích sử dụng chung. Máy khách là máy sử dụng tài nguyên do máy chủ cung cấp.

Mô hình khách – chủ có ưu điểm là dữ liệu được quản lý tập trung, bảo mật tốt, thích hợp với các mạng trung bình và lớn.



Hình 2. 3: Mô hình khách – chủ (client – server).

+ Mô hình dựa trên nền Web

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

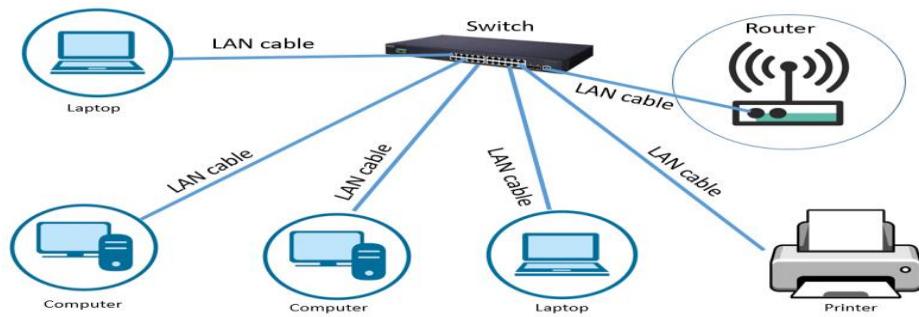
 Phân loại theo mạng máy tính

+ Mạng cục bộ (LAN: Local Area Network)

LAN là mạng kết nối các máy tính bên trong một vùng diện tích địa lý tương đối nhỏ, chẳng hạn như trong một phòng, một tòa nhà, một xí nghiệp, một trường học,...

Mạng LAN có các đặc điểm sau :

- Băng thông lớn để có khả năng chạy các ứng dụng trực tuyến như xem phim, giải trí, hội thảo qua mạng.
- Kích thước mạng bị giới hạn bởi thiết bị.
- Chi phí thiết kế, lắp đặt mạng LAN rẻ.
- Quản trị đơn giản.



Local Area Network

Hình 2. 4: Mô hình mạng LAN.

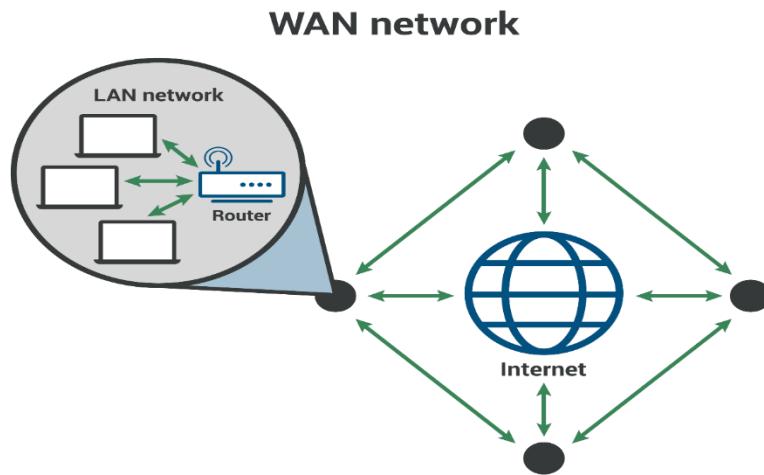
+ Mạng diện rộng (WAN: Wide Area Network)

WAN có phạm vi bao phủ một vùng rộng lớn, có thể là quốc gia, lục địa hay toàn cầu. Mạng WAN thường là mạng của các công ty đa quốc gia hay toàn cầu. Mạng WAN lớn nhất hiện nay là mạng Internet. Mạng WAN là tập hợp của nhiều mạng LAN và MAN được nối lại với nhau thông qua các phương tiện như vệ tinh, sóng vi ba, cáp quang, điện thoại....

Mạng WAN có các đặc điểm sau :

- Băng thông thấp, dễ mất kết nối, thường chỉ phù hợp với các ứng dụng online như e-mail, ftp, web....

- Phạm vi hoạt động không giới hạn.
- Do kết nối nhiều LAN và MAN với nhau nên mạng rất phức tạp và các tổ chức toàn cầu phải đứng ra quy định và quản lý.
- Chi phí cho các thiết bị và công nghệ WAN rất đắt Chú ý là việc phân biệt mạng thuộc loại LAN, MAN hay WAN chủ yếu dựa trên khoảng cách vật lý và chỉ mang tính chất ước lẻ.



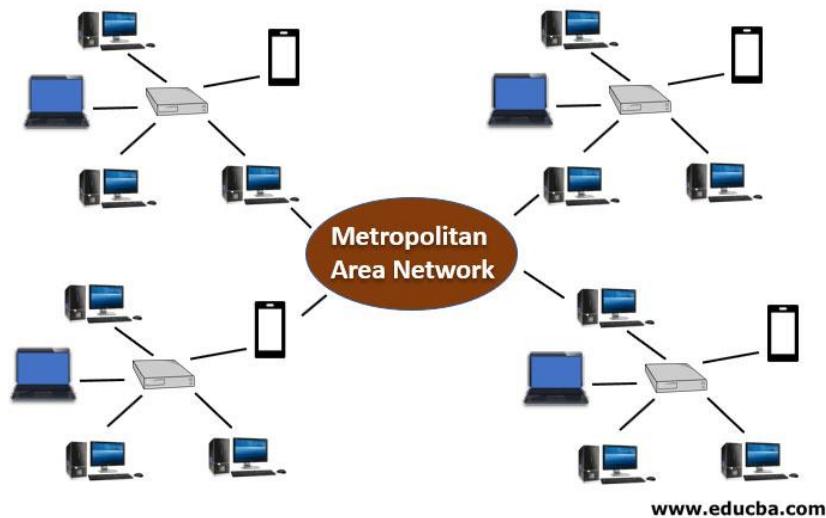
Hình 2. 5: Mô hình mạng WAN.

+ Mạng đô thị (MAN: Metropolitan Area Network)

Gần giống như mạng LAN nhưng giới hạn kích thước của nó là một thành phố hay một quốc gia. Mạng MAN kết nối các mạng LAN lại với nhau thông qua môi trường truyền dẫn và các phương thức truyền thông khác nhau.

Mạng MAN có các đặc điểm sau :

- Băng thông ở mức trung bình,đủ để phục vụ các ứng dụng cấp thành phố hay quốc gia như chính phủ điện tử,thương mại điện tử,các ứng dụng của các ngân hàng...
- Do MAN kết nối nhiều LAN nên việc quản trị sẽ gặp khó khăn hơn,đồng thời độ phức tạp cũng tăng theo.
- Chi phí các thiết bị MAN tương đối đắt tiền.



Hình 2. 6: Mô hình mạng MAN.

2.1.2 Khái niệm mạng wifi

Khái niệm

WiFi là viết tắt của Wireless Fidelity là công nghệ mạng cho phép bạn kết nối không dây với Internet. Nó còn được gọi là 802.11, là tiêu chuẩn IEEE của mạng cục bộ không dây (WLAN).

Mạng WiFi hoạt động ở dải tần số 2.4GHz và 5GHz không li-xăng (unlicensed), có nghĩa là mạng này không gây nhiễu cho những mạng không dây lân cận khác hoạt động trên cùng các tần số (hoặc băng thông) đó.



Hình 2. 7: Mô hình mạng wifi.

Cách thức hoạt động

Mạng WiFi hiện đại hoạt động giống như kết nối mạng cục bộ Ethernet có dây (LAN). Sự khác biệt duy nhất là chúng sử dụng các tần số phổ không li-xăng để truyền dữ liệu trong khoảng cách ngắn với tốc độ cao, giống như băng thông rộng di động đối với điện thoại cầm tay.

Tiêu chuẩn WiFi được phát triển bởi Hội Kỹ sư Điện và Điện tử (IEEE) để cung cấp khả năng truy cập không dây trong khu vực cục bộ, thường là trong nhà hoặc tòa nhà văn phòng.

Để WiFi hoạt động, phải có một điểm truy cập (trạm gốc) có kết nối có dây để kết nối các thiết bị WiFi. Các thiết bị WiFi giao tiếp với điểm truy cập bằng tín hiệu tần số vô tuyến (RF), giống như điện thoại không dây.

 **Ưu, nhược điểm**

+ **Ưu điểm**

Ưu điểm của kết nối WiFi là tính tiện dụng, và đơn giản gọn nhẹ so với kết nối trực tiếp bằng cable truyền thông qua cổng RJ45. Người sử dụng có thể truy cập ở bất cứ vị trí nào trong vùng bán kính phủ sóng mà tại đó Router WiFi làm trung tâm. Ưu điểm thứ hai của mạng sử dụng WiFi là dễ dàng sửa đổi và nâng cấp, người sử dụng có thể tăng băng thông truy cập, tăng số lượng người sử dụng mà không cần nâng cấp thêm Router hay dây cáp như các kết nối bằng dây vật lý. Tính thuận tiện: người truy cập có thể duy trì kết nối kể cả khi đang di chuyển, một ví dụ cụ thể là các Router WiFi đặc lắp trên các xe khách đường dài. Bên cạnh đó, tính bảo mật của mạng WiFi tương đối cao.

+ **Nhược điểm**

Bên cạnh những ưu điểm, mạng WiFi cũng tồn tại nhiều nhược điểm chưa thể khắc phục như: phạm vi kết nối của mạng WiFi tới thiết bị có giới hạn, đi càng xa router kết nối càng yếu dần đi. Giải pháp cho vấn đề này là trang bị thêm các Repeater hoặc Access point. Tuy nhiên, gặp nhiều khó khăn do giá thành cao. Nhược điểm tiếp theo của mạng WiFi là về vấn đề băng thông, càng nhiều người kết nối vào mạng thì tốc độ truy cập giảm rõ rệt.

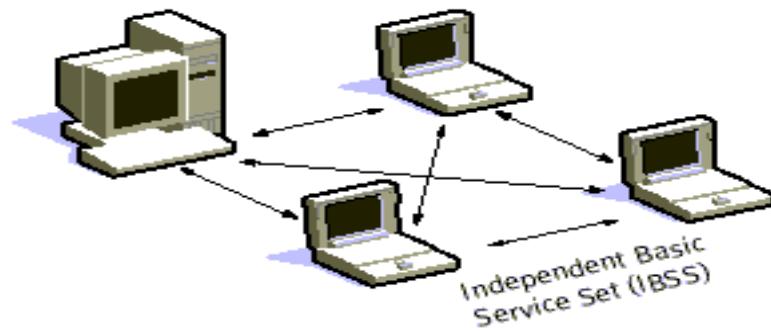
2.1.3 Các mô hình mạng wifi

 **Mô hình mạng độc lập (Ad-hoc)**

Mạng IBSSs (Independent Basic Service Set) hay còn gọi là mạng ad-hoc, trong mô hình mạng ad-hoc các client liên lạc trực tiếp với nhau mà không cần thông qua AP nhưng phải ở trong phạm vi cho phép.

Các nút di động (máy tính có hỗ trợ card mạng không dây) tập trung lại trong một không gian nhỏ để hình thành nên kết nối ngang cáp (peer-to-peer) giữa chúng. Các nút di động có card mạng wireless là chúng có thể trao đổi thông tin trực tiếp với nhau, không cần phải quản trị mạng. Mô hình mạng nhỏ nhất trong chuẩn 802.11 là 2 máy client liên lạc trực tiếp với nhau.

Mô hình mạng Ad-hoc này có nhược điểm lớn về vùng phủ sóng bị giới hạn, mọi người sử dụng đều phải nghe được lẫn nhau.



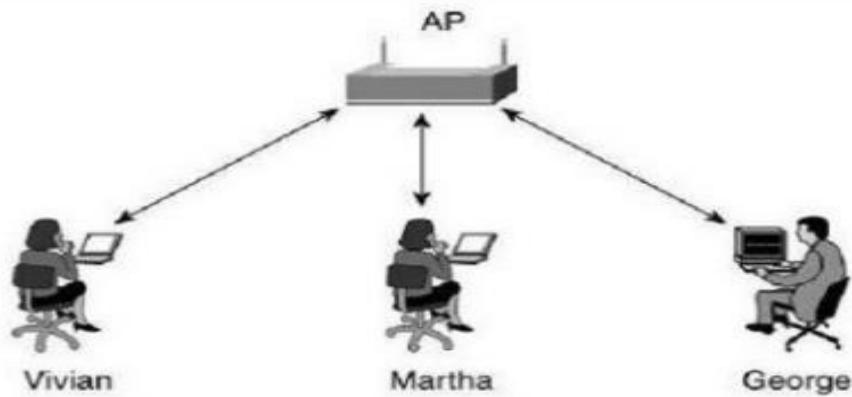
Hình 2. 8: Mô hình mạng độc lập.

Mô hình mạng cơ sở

The Basic Service Sets (BSS) là một topology nền tảng của mạng 802.11. Các thiết bị giao tiếp tạo nên một BSS với một AP duy nhất với một hoặc nhiều client.

BSS bao gồm các điểm truy nhập AP (Access Point) gắn với mạng đường trực huu tuyen và giao tiếp với các thiết bị di động trong vùng phủ sóng của một cell. AP

đóng vai trò điều khiển cell và điều khiển lưu lượng tới mạng. Các thiết bị di động không giao tiếp trực tiếp với nhau mà giao tiếp với các AP. Các cell có thể chồng lấn lên nhau khoảng 10-15 % cho phép các trạm di động có thể di chuyển mà không bị mất kết nối vô tuyến và cung cấp vùng phủ sóng với chi phí thấp nhất. Các trạm di động sẽ chọn AP tốt nhất để kết nối. Một điểm truy nhập nằm ở trung tâm có thể điều khiển và phân phối truy nhập cho các nút tranh chấp, cung cấp truy nhập phù hợp với mạng đường trực, xác định các địa chỉ và các mức ưu tiên, giám sát lưu lượng mạng, quản lý chuyển đi các gói và duy trì theo dõi cấu hình mạng.

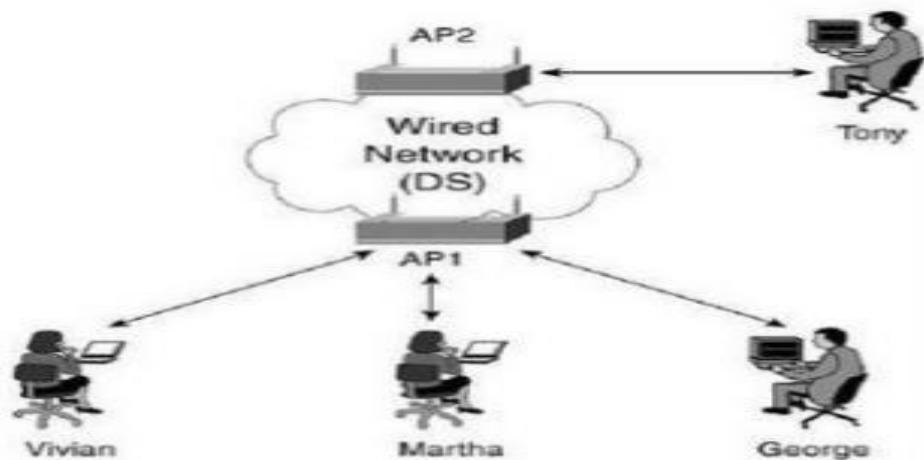


Hình 2. 9: Mô hình mạng cơ sở.

Mô hình mạng mở rộng

Mạng 802.11 mở rộng phạm vi di động tới một phạm vi bất kì thông qua ESS. Trong khi một BSS được coi là nền tảng của mạng 802.11, một mô hình mạng mở rộng ESS của mạng 802.11 sẽ tương tự như là một tòa nhà được xây dựng bằng đá. Một ESS là một tập hợp các BSSs nơi mà các Access Point giao tiếp với nhau để chuyển lưu lượng từ một BSS này đến một BSS khác để làm cho việc di chuyển dễ dàng của các trạm giữa các BSS. Access Point thực hiện việc giao tiếp thông qua hệ thống phân phối. Hệ thống phân phối là một lớp mỏng trong mỗi Access Point mà nó xác định đích đến cho một lưu lượng được nhận từ một BSS. Hệ thống phân phối được tiếp sóng trở lại một đích trong

cùng một BSS, chuyển tiếp trên hệ thống phân phối tới một Access Point khác, hoặc gởi tới một mạng có dây tới đích không nằm trong ESS. Các thông tin nhận bởi Access Point từ hệ thống phân phối được truyền tới BSS sẽ được nhận bởi trạm đích.



Hình 2. 10: Mô hình mạng mở rộng.

2.1.4 Các chuẩn wifi cơ bản

Chuẩn wifi do một tổ chức công nghệ IEEE (Institute of Electrical and Electronics Engineers) định nghĩa nên. Dùng để thống nhất một chuẩn chung cho nhiều giao thức kỹ thuật khác nhau và nó sử dụng một hệ thống số nhằm phân loại chúng, 4 chuẩn thông dụng của WiFi hiện nay là 802.11a/b/g/n.

								
Giao thức 802.11	Ngày ra đời	Dải tần (GHz)	Độ rộng kênh	Tốc độ dữ liệu mỗi luồng (Mbps)	Số luồng cho phép	Điều chế	Phạm vi trong nhà (m)	Phạm vi ngoài trời (m)
	Jun-97	2.4	20	2	1	DSSS, FHSS	20	100
	Sep-99	5	20	54	1	OFDM	35	120
	Sep-99	2.4	20	11	1	DSSS	38	140
	Jun-03	2.4	20	54	1	OFDM, DSSS	38	140
	Oct-09	2.4/5	20	72.2	4	OFDM	70	250
			40	150			70	250
	Dec-12	5	80/160	866	8	OFDM		

Hình 2. 11: Bảng thông tin tổng hợp về mạng wifi.

Chuẩn IEEE 802.11

- Được tổ chức IEEE giới thiệu đầu tiên vào năm 1997.
- Hỗ trợ cho băng thông tối đa là 2Mbps.
- Sử dụng tần số vô tuyến 2.4 GHz.
- Nhược điểm : số lượng băng thông quá thấp, dẫn đến việc khó khăn trong việc truyền tải dữ liệu.

Chuẩn IEEE 802.11a

- Được tạo đồng thời với chuẩn 802.11b. Tuy nhiên chuẩn 802.11a không được sử dụng rộng rãi vì giá thành cao hơn và vì sự sử dụng phổ biến và nhanh chóng của chuẩn 802.11b.

- Thích hợp cho các mô hình mạng doanh nghiệp.
- Hỗ trợ băng thông tối đa lên đến 54 Mbps.
- Sử dụng tần số vô tuyến là 5GHz.
- Ưu điểm: tốc độ cao, tần số 5GHz tránh được tình trạng nhiễu từ các thiết bị khác.
- Nhược điểm: giá thành tương đối cao, phạm vi hoạt động hẹp và dễ bị che khuất.

 Chuẩn IEEE 802.11b

- Được phát triển từ chuẩn 802.11 sơ khai. Vào 7/1999, tổ chức IEEE đã cho ra đời một chuẩn mới đó là 802.11b.
- Hỗ trợ băng thông tối đa 11Mbps và có sự tương quan với Ethernet truyền thống.
- Sử dụng tần số vô tuyến là 2.4 GHz giống như chuẩn 802.11
- Thích hợp cho các mạng gia đình
- Giá thành tương đối rẻ, tín hiệu tương đối tốt trong phạm vi cho phép.
- Nhược điểm: Tốc độ băng thông vẫn còn rất thấp, dễ xảy ra hiện tượng nhiễu do có nhiều thiết bị sử dụng dải tần 2.4 GHz này như: điện thoại không dây, lò vi sóng,...

 Chuẩn IEEE 802.11g

- Được ra mắt vào khoảng năm 2002-2003. Là sự kết hợp giữa 2 chuẩn 802.11a và 802.11b.
- Hỗ trợ băng thông tối đa là 54Mbps
- Sử dụng tần số 2.4GHz
- Ưu điểm: tốc độ cao, phạm vi tín hiệu hoạt động lớn và tốt hơn, ít bị che khuất
- Nhược điểm: giá thành tương đối cao so với 802.11b, các thiết bị sử dụng chuẩn này có thể bị nhiễu từ các thiết bị sử dụng cùng tần số 2.4GHz.

Chuẩn IEEE 802.11n

- Được ra đời vào khoảng năm 2009, nhằm cải thiện cho chuẩn 802.11g với tổng số băng thông được hỗ trợ bằng cách tận dụng các tín hiệu không dây và anten (Công nghệ MIMO).
- MIMO: sử dụng nhiều ăng-ten thông minh để xử lý các luồng dữ liệu lớn thay vì 1 ăng-ten đơn như các công nghệ khác bằng kỹ thuật ghép kênh và phân chia không gian.
- Hỗ trợ băng thông tối đa là 100Mbps .
- Hoạt động trên 2 dải tần 2.4GHz và 5GHz.
- Tương thích với các thiết bị sử dụng chuẩn 802.11g
- Ưu điểm: tốc độ nhanh, phạm vi hoạt động tín hiệu tốt, các khả năng chống nhiễu tốt từ các thiết bị khác sử dụng cùng băng tần.
- Nhược điểm: giá thành tương đối cao

 Chuẩn IEEE 802.11ac

- Được mở rộng từ chuẩn 802.11n
- Hỗ trợ băng thông tối thiểu là 1Gbps. Đối với 1 liên kết lẻ tối thiểu là: 500Mbps.
- Hoạt động ở tần số 5GHz
- Sử dụng công nghệ MIMO như chuẩn 802.11n (lên đến 8 luồng dữ liệu). Ngoài ra còn có thể sử dụng được cho các kênh có băng thông rộng RF (160MHz, 80Mhz).

 Chuẩn IEEE 802.11 ad

- Hỗ trợ băng thông lên đến 70Gbps
- Hoạt động ở dải tần 60GHz (Chịu sự hấp thu của khí Oxy trong không khí, vì vậy sóng vô tuyến có thể ảnh hưởng vì lý do này. Chỉ thích hợp cho các kết nối mạng point to point, các ứng dụng sử dụng anten hướng sóng cao).

2.1.5 Thẻ hệ mạng 1G, 2G, 3G, 4G, 5G

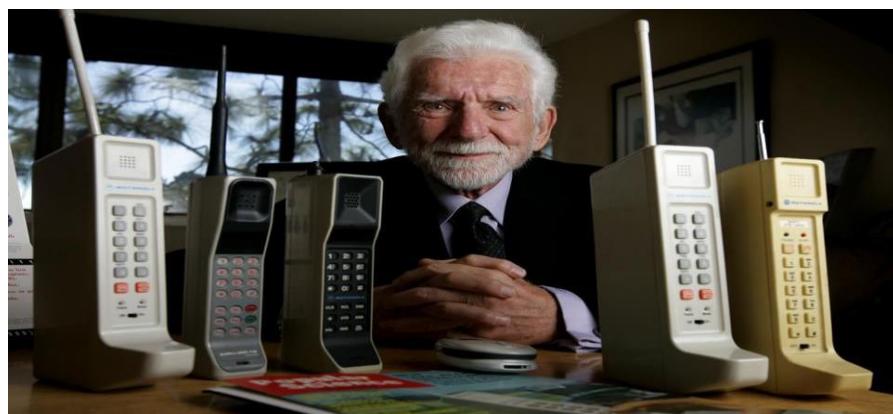
2.1.5.1 Mạng di động thẻ hệ đầu tiên – 1G

1G Là mạng thông tin di động không dây sơ khai đầu tiên trên thế giới. Nó là hệ thống giao tiếp thông tin qua kết nối tín hiệu analog được giới thiệu lần đầu tiên vào những năm đầu thập niên 80s. Nó sử dụng các ăng-ten thu phát sóng gắn ngoài, kết nối theo tín hiệu analog tới các trạm thu phát sóng và nhận tín hiệu xử lý thoại thông qua các module gắn trong máy di động. Chính vì thế mà các thẻ hệ máy di động đầu tiên trên thế

giới có kích thước khá to và cồng kềnh do tích hợp cùng lúc 2 module thu tín hiệu và phát tín hiệu như trên.

Mặc dù là thế hệ mạng di động đầu tiên với tần số chỉ từ 150MHz nhưng mạng 1G cũng phân ra khá nhiều chuẩn kết nối theo từng phân vùng riêng trên thế giới: NMT (Nordic Mobile Telephone) là chuẩn dành cho các nước Bắc Âu và Nga; AMPS (Advanced Mobile Phone System) tại Hoa Kỳ; TACS (Total Access Communications System) tại Anh; JTACS tại Nhật; C-Netz tại Tây Đức; Radiocom 2000 tại Pháp; RTMI tại Ý.

Hệ thống mạng di động 1G hoàn thiện đầu tiên là Nordic Mobile Telephone (NMT), được sử dụng ở các nước Bắc Âu, Thụy Sĩ, Hà Lan, Đông Âu và Nga. Những hệ thống mạng 1G khác bao gồm Advanced Mobile Phone System (AMPS) được sử dụng ở Bắc Mỹ và Úc, TACS (otal Access Communications System) tại Vương quốc Anh, C-450 ở Tây Đức, Bồ Đào Nha và Nam Phi, Radiocom 2000 ở Pháp, TMA ở Tây Ban Nha và RTMI ở Ý. Ở Nhật Bản có nhiều hệ thống mạng 1G. Ba tiêu chuẩn, TZ-801, TZ-802, và TZ-803 được phát triển bởi NTT (Nippon Telegraph và Telephone Corporation), trong khi một hệ thống cạnh tranh của công ty Daini Denden Planning, Inc. (DDI) sử dụng tiêu chuẩn JTACS (Japan Total Access Communications System).



Hình 2. 12: Những thiết bị sử dụng 1G đầu tiên.

2.1.5.2 Thế hệ mạng 2G

Đây chính là thế hệ mạng di động thứ 2 với tên gọi đầy đủ là: “hệ thống thông tin di động toàn cầu“. Mạng 2G có tên tiếng anh là Global System for Mobile Communications hay còn gọi là GSM. Mạng 2G có khả năng phủ sóng rộng khắp, làm cho những chiếc điện thoại có thể được sử dụng ở nhiều nơi trên thế giới. GSM gồm nhiều các trạm thu phát sóng để những điện thoại di động có thể kết nối mạng qua việc tìm kiếm các trạm thu phát gần nhất.

Ba tính năng vượt trội của mạng 2G so với 2 công nghệ tiền nhiệm là 0G và 1G là:

- Gọi thoại với tín hiệu được mã hóa dưới dạng tín hiệu kĩ thuật số (digital encrypted).
- Sử dụng hiệu quả hơn phô tần số vô tuyến cho phép nhiều người dùng hơn trên mỗi dải tần.
- Cung cấp dịch vụ dữ liệu cho di động, bắt đầu với tin nhắn văn bản SMS.

Khi mạng 2G xuất hiện, chất lượng cuộc gọi được cải thiện đáng kể, tín hiệu và tốc độ cũng tốt hơn rất nhiều so với thế hệ trước đó. Thời gian và chi phí được tiết kiệm khi mã hóa dữ liệu theo dạng kĩ thuật số. Những thiết bị được thiết kế nhỏ gọn và nhẹ hơn, ngoài ra chúng còn có thể thực hiện tin nhắn dạng SMS.

Những modem truyền thông trong công nghiệp như F2103 cũng sử dụng công nghệ mạng 2G này để thực hiện truyền tải dữ liệu. Nói chung mạng 2G có những tác động khá lớn tới ngành thông tin liên lạc và truyền tải dữ liệu.

Mạng 2G chia làm 2 nhánh chính: nền TDMA (Time Division Multiple Access) và nền CDMA cùng nhiều dạng kết nối mạng tùy theo yêu cầu sử dụng từ thiết bị cũng như hạ tầng từng phân vùng quốc gia:

- GSM (TDMA-based), khởi nguồn áp dụng tại Phần Lan và sau đó trở thành chuẩn phổ biến trên toàn 6 Châu lục. Và hiện nay vẫn đang được sử dụng bởi hơn 80% nhà cung cấp mạng di động toàn cầu.
- CDMA2000 – tần số 450 MHZ cũng là nền tảng di động tương tự GSM nói trên nhưng nó lại dựa trên nền CDMA và hiện cũng đang được cung cấp bởi 60 nhà mạng GSM trên toàn thế giới.
- IS-95 hay còn gọi là cdmaOne, (nền tảng CDMA) được sử dụng rộng rãi tại Hoa Kỳ và một số nước Châu Á và chiếm gần 17% các mạng toàn cầu. Tuy nhiên, tính đến thời điểm này thì có khoảng 12 nhà mạng đang chuyển dịch dần từ chuẩn mạng này sang GSM (tương tự như HT Mobile tại Việt Nam vừa qua) tại: Mexico, Ấn Độ, Úc và Hàn Quốc.
- PDC (nền tảng TDMA) tại Japan
- iDEN (nền tảng TDMA) sử dụng bởi Nextel tại Hoa Kỳ và Telus Mobility tại Canada.
- IS-136 hay còn gọi là D-AMPS, (nền tảng TDMA) là chuẩn kết nối phổ biến nhất tính đến thời điểm này và đã có 7c cung cấp hầu hết tại các nước trên thế giới cũng như Hoa Kỳ.



Hình 2. 13: Các thiết bị sử dụng mạng 2G.

2.1.5.3 Thế hệ mạng 3G

Mạng di động Thế hệ thứ 3 của chuẩn công nghệ điện thoại di động chính là mạng 3G Third-generation technology, cho phép truyền cả dữ liệu thoại như nghe gọi, nhắn tin và dữ liệu ngoài thoại như gửi mail, tải dữ liệu, hình ảnh. Nhờ có mạng 3G ta có thể truy cập Internet cho cả thuê bao cố định hay di chuyển ở các tốc độ khác nhau. hầu hết các smartphone hiện nay đều hỗ trợ công nghệ 3G. Hiện nay công nghệ 3G được xây dựng với 4 chuẩn chính: W-CDMA, CDMA2000, TD-CDMA, TD-SCDMA.

Mạng 3G cải thiện chất lượng cuộc gọi, tín hiệu, tốc độ cao hơn hẳn so với mạng 2G. Ta có thể truy cập Internet tốc độ cao ngay khi đang di chuyển, truy cập thế giới nội dung đa phương tiện: nhạc, phim, hình ảnh chất lượng cao. Người dùng có thể trò chuyện mọi nơi với chi phí rẻ hơn rất nhiều qua các ứng dụng hỗ trợ như: zalo, Viber, Line,...

Trong số các dịch vụ của 3G, Cuộc gọi video được phát triển mạnh nhất. Giá dịch vụ cho công nghệ 3G rất đắt tại nhiều quốc gia, nơi mà các cuộc bán đầu giá tiền số mang lại hàng tỷ Euro cho các chính phủ. Bởi vì chi phí cho bản quyền về các tiền số phải trang

trải trong nhiều năm trước khi các thu nhập từ mạng 3G đem lại, nên một khối lượng vốn đầu tư không lồ là cần thiết để xây dựng mạng 3G. Nhiều nhà cung cấp dịch vụ viễn thông đã roi vào khó khăn về tài chính và điều này đã làm chậm trễ việc triển khai mạng 3G tại nhiều nước ngoại trừ Nhật Bản và Hàn Quốc, nơi yêu cầu về bản quyền tần số được bỏ qua do phát triển hạ tầng cơ sở IT quốc gia được đặt lên làm vấn đề ưu tiên nhất. Và cũng chính Nhật Bản là nước đầu tiên đưa 3G vào khai thác thương mại một cách rộng rãi, tiên phong bởi nhà mạng NTT DoCoMo. Tính đến năm 2005, khoảng 40% các thuê bao tại Nhật Bản là thuê bao 3G, và mạng 2G đang dần dần đi vào lãng quên trong tiềm thức công nghệ tại Nhật Bản.

Công nghệ 3G cũng được nhắc đến như là một chuẩn IMT-2000 của Tổ chức Viễn thông Thế giới (ITU). Ban đầu 3G được dự kiến là một chuẩn thống nhất trên thế giới, nhưng trên thực tế, thế giới 3G đã bị chia thành 4 phần riêng biệt:

- W-CDMA: Tiêu chuẩn W-CDMA là nền tảng của chuẩn UMTS (Universal Mobile Telecommunication System), dựa trên kỹ thuật CDMA trải phổ dãy trực tiếp, trước đây gọi là UTRA FDD, được xem như là giải pháp thích hợp với các nhà khai thác dịch vụ di động (Mobile network operator) sử dụng GSM, tập trung chủ yếu ở châu Âu và một phần châu Á (trong đó có Việt Nam). UMTS được tiêu chuẩn hóa bởi tổ chức 3GPP, cũng là tổ chức chịu trách nhiệm định nghĩa chuẩn cho GSM, GPRS và EDGE.
- CDMA: Một chuẩn 3G quan trọng khác là CDMA2000, là thế hệ kế tiếp của các chuẩn 2G CDMA và IS-95. Các đề xuất của CDMA2000 nằm bên ngoài khuôn khổ GSM tại Mỹ, Nhật Bản và Hàn Quốc. CDMA2000 được quản lý bởi 3GPP2, là tổ chức độc lập với 3GPP. Có nhiều công nghệ truyền thông khác nhau được sử dụng trong CDMA2000 bao gồm 1xRTT,

CDMA2000-1xEV-DO và 1xEV-DV. CDMA 2000 cung cấp tốc độ dữ liệu từ 144 kbit/s tới trên 3 Mbit/s. Chuẩn này đã được chấp nhận bởi ITU.

- TD-CDMA: Chuẩn TD-CDMA, viết tắt từ Time-division-CDMA, trước đây gọi là UTRA TDD, là một chuẩn dựa trên kỹ thuật song công phân chia theo thời gian (Time-division duplex). Đây là một chuẩn thương mại áp dụng hồn hợp của TDMA và CDMA nhằm cung cấp chất lượng dịch vụ tốt hơn cho truyền thông đa phương tiện trong cả truyền dữ liệu lõi âm thanh, hình ảnh. Chuẩn TD-CDMA và W-CDMA đều là những nền tảng của UMTS, tiêu chuẩn hóa bởi 3GPP, vì vậy chúng có thể cung cấp cùng loại của các kênh khi có thể. Các giao thức của UMTS là HSDPA/HSUPA cải tiến cũng được thực hiện theo chuẩn TD-CDMA.
- TD-SCDMA: Chuẩn được ít biết đến hơn là TD-SCDMA (Time Division Synchronous Code Division Multiple Access) đang được phát triển tại Trung Quốc bởi các công ty Datang và Siemens, nhằm mục đích như là một giải pháp thay thế cho W-CDMA. Nó thường xuyên bị nhầm lẫn với chuẩn TD-CDMA. Cũng giống như TD-CDMA, chuẩn này dựa trên nền tảng UMTS-TDD hoặc IMT 2000 Time-Division (IMT-TD). Tuy nhiên, nếu như TD-CDMA hình thành từ giao thức mang cũng mang tên TD-CDMA, thì TD-SCDMA phát triển dựa trên giao thức của S-CDMA.

Mạng di động 3.5G: là hệ thống mạng di động truyền tải tốc độ cao HSDPA (High Speed Downlink Packet Access), phát triển từ 3G và hiện đang được 166 nhà mạng tại 75 nước đưa vào cung cấp cho người dùng. Nó được kết hợp từ 2 công nghệ kết nối không dây hiện đại HSPA và HSUPA, cho phép tốc độ truyền dẫn lên đến 7.2Mbps.



Hình 2. 14: Thế hệ mạng 3G xuất hiện.

2.1.5.4 Thế hệ mạng 4G

Mạng thông tin di động 4G Hay còn có thể viết là 4-G, là công nghệ truyền thông không dây thế hệ thứ tư, cho phép truyền tải dữ liệu với tốc độ tối đa trong điều kiện lý tưởng lên tới 1 – 1,5 Gbit/s. Cách đây không lâu thì một nhóm gồm 26 công ty trong đó có Vodafone (Anh), Siemens (Đức), Alcatel (Pháp), NEC và DoCoMo (Nhật Bản), đã ký thỏa thuận cùng nhau phát triển một tiêu chí cao cấp cho ĐTDĐ, một thế hệ thứ 4 trong kết nối di động – đó chính là nền tảng cho kết nối 4G sắp tới đây.

Mạng 4G hiện đang được sử dụng phổ biến và hội tụ rất nhiều ưu điểm khiến người dùng hài lòng. Dưới đây là những ưu điểm nổi bật nhất của mạng di động 4G.

- Tốc độ mạng 4G đạt mức rất ấn tượng khi trong điều kiện lý tưởng, tốc độ tải của công nghệ mạng này khi di chuyển lên đến 100 Mbps và đạt xấp xỉ 1Gbps nếu đứng yên.
- Công suất và hiệu suất hoạt động của mạng di động 4G cực kỳ cao khi một trạm phát 4G có thể phục vụ cùng lúc khoảng 300-400 người dùng. Mạng

4G hỗ trợ các chương trình mã hóa nhanh hơn, nén được nhiều dữ liệu bit hơn so với mạng 3G.

- Nhờ tốc độ truyền dữ liệu cao nên mạng 4G hỗ trợ các phần mềm chạy mượt mà hơn, người dùng được xem video chất lượng cao Full HD và 4K.



Hình 2. 15: SIM 4G bắt đầu được sử dụng.

2.1.5.5 Thẻ hệ mạng 5G

Giống như những gì chúng ta hình dung, 5G nhanh hơn 4G. Hiện tại, mạng 5G mới được lên kế hoạch hoạt động trong dải tần số cao của băng tần không dây – nó nằm giữa 30 GHz và 300 GHz, hay còn được gọi là băng tần bước sóng milimet. Đối với các thiết bị di động, 5G sẽ giúp sửa chữa rất nhiều vấn đề của 4G và các công nghệ không dây hiện tại. Nó sẽ được thiết kế để hỗ trợ đồng thời nhiều người dùng và thiết bị hơn (theo thông số kỹ thuật ITU mỗi cell 5G sẽ hỗ trợ cho 1 triệu thiết bị trên diện tích 1 km²), với tốc độ cao hơn cả 4G. Việc tốc độ dữ liệu của bạn bị chậm đi khi đang ở một sự kiện đông người sẽ chỉ còn là quá khứ.

Hiện cả ba nhà mạng lớn tại Việt Nam gồm Viettel, VinaPhone, MobiFone đều đã triển khai mạng 5G tại Hà Nội, TP Hồ Chí Minh và một số tỉnh, thành phố khác. Với

tốc độ cao hơn 10 lần so với 4G hiện tại, 5G được kỳ vọng sẽ giải quyết các bài toán khó hơn về mạng dữ liệu, mang tới những trải nghiệm tốc độ nhanh hơn.

Mạng 5G sẽ có mặt chính thức tại Việt Nam vào khoảng giữa năm 2021 sau khi cả ba nhà mạng hoàn tất việc thử nghiệm và cấp phép hoạt động của Bộ Thông Tin và Truyền Thông.

Hiện tại, theo thông tin được ghi nhận thì cuộc gọi đầu tiên được thử nghiệm trên đường truyền 5G đã tiến hành từ ngày 10/5/2019. Đến 20/8/2020 thì Bộ Thông Tin và Truyền Thông công bố sẽ quy hoạch băng tần 24.25 – 27.5 để phục vụ cho việc kết nối và sử dụng mạng 5G tại nước ta.

Hơn nữa, Bộ Thông Tin và Truyền Thông đã duyệt qua giấy phép thử nghiệm dịch vụ mạng 5G Việt Nam cho hai nhà mạng là Viettel và MobiFone.

Cụ thể, Viettel có quyền sử dụng các đoạn băng tần từ 2.500MHz đến 2.600MHz, từ 3.700MHz đến 3.800MHz và băng tần từ 27.100MHz đến 27.500MHz. Ngoài ra, quy mô thử nghiệm của nhà mạng này được kéo dài đến 30/6/2021 tại 140 địa điểm ở Hà Nội.

Trong khi đó, MobiFone sẽ bắt đầu thương mại viễn thông mạng 5G tại TP. Hồ Chí Minh với 50 địa điểm đặt trạm BTS và giấy phép thử nghiệm của nhà mạng này cũng kéo dài đến ngày 30/6/2021.

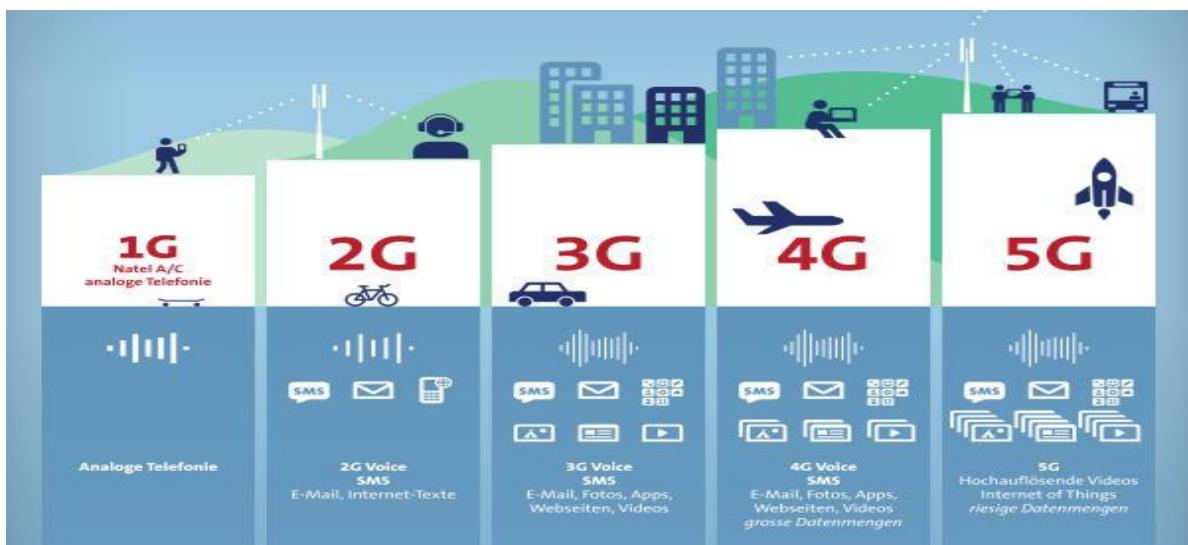
VinaPhone cũng đã sớm thử nghiệm 5G từ tháng 4/2020 và công bố kế hoạch cung cấp thương mại 5G thử nghiệm vào cuối tháng 11. Nhà mạng VinaPhone còn cho hay tốc độ tải xuống dữ liệu bằng mạng 5G do hãng cung cấp sẽ đạt tốc độ tối đa 2.2Gbps và độ trễ xấp xỉ 0%, đây là con số tuyệt vời đáng trông chờ.



Hình 2. 16: Mạng 5G được sử dụng rộng rãi.

2.1.5.6 So sánh các thế hệ mạng

Các công nghệ mạng được sử dụng qua các thế hệ mạng khác nhau:



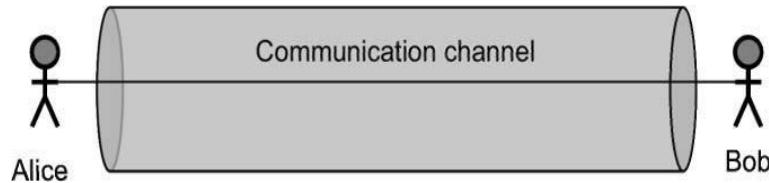
Hình 2. 17: Sự phát triển các thế hệ mạng.

2.1.6 Khái niệm an toàn bảo mật không dây

2.1.6.1 Các lỗ hỏng chủ yếu trong hệ thống viễn thông

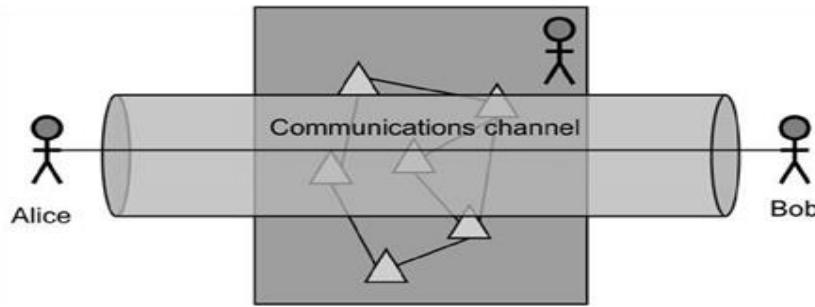
Các mô hình mối đe dọa trước tiên mô tả hệ thống, tất cả các tác nhân trong hệ thống này và vị trí của chúng trong hệ thống (ví dụ: liên kết, nút). Sau đó, mô hình mối đe dọa giới thiệu kẻ tấn công trong hệ thống và thể hiện năng lực của kẻ tấn công, tức là vị trí cấu trúc liên kết trong hệ thống, tài nguyên, khả năng truy cập, v.v.

Mô hình mối đe dọa truyền thông đối với một kênh liên lạc dựa trên mô hình giao tiếp tối thiểu tối giản liên quan đến hai người tham gia được gọi là Alice và Bob, và một kênh liên lạc (xem Hình 1.18).



Hình 2. 18: Kênh liên lạc giữa 2 người Alice và Bob

Mô hình này thường giả định mối quan hệ tin cậy ban đầu giữa Alice và Bob. Nó thường được sử dụng trong mật mã, vì nó hạn chế hiệu quả các cuộc tấn công có thể xảy ra đối với các cuộc tấn công chống lại kênh liên lạc giữa Alice và Bob. Tuy nhiên, trong bối cảnh của các hệ thống viễn thông, mô hình này không phải là đầy đủ, vì các yếu tố và lỗ hổng bảo mật khác hiện diện. Hình 1.19 giới thiệu một mô hình thích hợp hơn, phân biệt giữa hai bên giao tiếp (Alice và Bob) và ít nhất một cơ sở hạ tầng viễn thông và quyền hạn của nó được vượt qua kênh giao tiếp. Nói chung người có thẩm quyền này không phải là Alice hay Bob mà là một bên thứ ba thực sự.



Hình 2. 19: Mô hình phân biệt giữa hai bên giao tiếp

Sự xuất hiện của một bên thứ ba như vậy làm tăng độ phức tạp của hệ thống, giới thiệu các giao diện và lỗ hổng mới và có thể yêu cầu một chuỗi tin cậy phức tạp hơn. Do đó, nó mở rộng phạm vi các mối đe dọa có thể xảy ra.

Mô hình tin cậy của có thể có các dạng rất khác nhau, nhưng trên thực tế, chúng ta giả sử một trong những điều sau:

- Alice và Bob tin tưởng lẫn nhau về cách thức liên lạc dự kiến, và cả hai đều tin tưởng hệ thống viễn thông đã sử dụng cung cấp chính xác các dịch vụ (mạng riêng).
- Alice và Bob tin tưởng lẫn nhau, nhưng không tin tưởng vào cơ sở hạ tầng chéo (mạng công cộng).
- Alice và Bob tin tưởng vào cơ sở hạ tầng viễn thông nhưng không tin tưởng lẫn nhau, họ sẽ sử dụng cơ sở hạ tầng như một bên thứ ba đáng tin cậy (TTP) để thiết lập một mối quan hệ tin cậy mới.

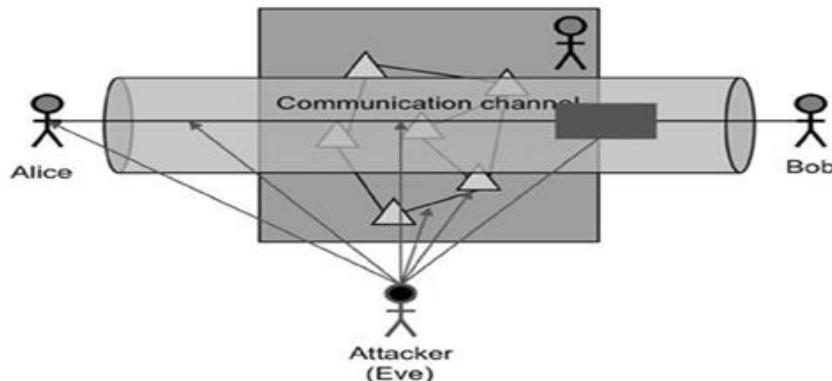
Trình bày từ trái sang phải các mối đe dọa điển hình chống lại các tác nhân và các bộ phận của mô hình này. Trong phần sau, kẻ tấn công được ký hiệu là Eve:

- Eve có thể tấn công một trong các bên giao tiếp (ví dụ như Alice) bằng cách sử dụng các lỗ hổng trong phần mềm và các biện pháp bảo vệ mà

Alice sử dụng. Nói một cách chính xác, mối đe dọa này không liên quan đến hệ thống viễn thông. Tuy nhiên, thiết bị đầu cuối có giao diện kết nối với hệ thống viễn thông là một thực thể mở hơn và do đó dễ bị tấn công hơn. Thông thường, các cuộc tấn công có thể xảy ra do các lỗ hổng trong thiết bị đầu cuối và khả năng hiển thị của thiết bị đầu cuối liên quan đến dịch vụ viễn thông. Một ví dụ điển hình là việc thực thi mã độc hại trên nền tảng được Alice sử dụng thông qua vi-rút hoặc do tràn bộ đệm tiếp nhận.

- Ngoài ra, Eve có thể tấn công kênh liên lạc liên kết Alice với hệ thống viễn thông. Cuộc tấn công này có thể là không xâm nhập (đọc dữ liệu được trao đổi) hoặc xâm nhập (sửa đổi dữ liệu đã trao đổi, đưa dữ liệu vào, phát lại dữ liệu cũ). Khả năng xảy ra một cuộc tấn công như vậy phụ thuộc vào kênh. Ví dụ: một kênh không dây có khả năng dễ bị người thứ ba nghe thu động hơn so với cáp mạng, vốn thường ít nhất yêu cầu quyền truy cập vật lý vào phương tiện.
- Một cuộc tấn công có thể xảy ra khác chống lại kênh tồn tại trong hệ thống viễn thông. Để làm được điều này, thông thường cần phải có một hình thức truy cập vào hệ thống viễn thông. Nếu Eve không phải là chủ sở hữu của hệ thống, Eve có thể cố gắng giả dạng như một phần hợp pháp của cơ sở hạ tầng để thu hút Alice (hoặc Bob) sử dụng dịch vụ của nó. Trong một số trường hợp, Eve có thể có quyền truy cập vật lý vào các kênh liên lạc tạo thành một phần của hệ thống hoặc sử dụng các lỗ hổng của hệ thống để truy cập vào các thành phần của hệ thống. Các hình thức truy cập này có thể cho phép Eve thu thập thông tin về liên lạc giữa Alice và Bob và điều khiển luồng dữ liệu giữa hai người.

- Sự xâm nhập vào cơ sở hạ tầng cho phép thực hiện các cuộc tấn công "người ở giữa". Trong trường hợp này, Eve định vị như một điểm giao nhau giữa Alice (hoặc Bob) và cơ sở hạ tầng sao cho tất cả các liên lạc của Alice (hoặc Bob) với cơ sở hạ tầng đi qua đêm giao thửa. Nếu không có xác thực đáng tin cậy và lẫn nhau (tức là xác minh danh tính) giữa Alice (hoặc Bob) và cơ sở hạ tầng, Alice và cơ sở hạ tầng không thể tìm thấy loại xâm nhập này. Tuy nhiên, các cuộc tấn công "người ở giữa" cũng có thể xảy ra nếu Eve có thể chiếm đoạt danh tính của đối thủ giao tiếp. Để chống lại các cuộc tấn công này, xác thực lẫn nhau và đáng tin cậy giữa Alice và Bob trở nên cần thiết.



Hình 2. 20: Mô hình chống lại cuộc tấn công từ attacker.

2.1.6.2 Các hình thức tấn công WLAN

Tấn công bị động (Passive attack)

Trong một cuộc tấn công bị động, các hacker sẽ kiểm soát traffic không được mã hóa và tìm kiếm mật khẩu không được mã hóa (Clear Text password), các thông tin nhạy cảm có thể được sử dụng trong các kiểu tấn công khác. Các cuộc tấn công bị động bao gồm phân tích traffic, giám sát các cuộc giao tiếp không được bảo vệ, giải mã các traffic mã hóa yếu, và thu thập các thông tin xác thực như mật khẩu.

Các cuộc tấn công chặn bắt thông tin hệ thống mạng cho phép kẻ tấn công có thể xem xét các hành động tiếp theo. Kết quả của các cuộc tấn công bị động là các thông tin hoặc file dữ liệu sẽ bị rơi vào tay kẻ tấn công mà người dùng không hề hay biết.

Tấn công nội bộ (Insider attack)

Các cuộc tấn công nội bộ (insider attack) liên quan đến người ở trong cuộc, chẳng hạn như một nhân viên nào đó "bất mãn" với công ty của mình,...các cuộc tấn công hệ thống mạng nội bộ có thể gây hại hoặc vô hại.

Người trong cuộc có ý nghe trộm, ăn cắp hoặc phá hoại thông tin, sử dụng các thông tin một cách gian lận hoặc truy cập trái phép các thông tin.



Hình 2. 21: Các cuộc tấn công nội bộ.

Tấn công Phishing

Trong các cuộc tấn công phising, các hacker sẽ tạo ra một trang web giả trông “giống hệt” như các trang web phổ biến. Trong các phần tấn công phising, các hacker sẽ gửi một email để người dùng click vào đó và điều hướng đến trang web giả mạo. Khi

người dùng đăng nhập thông tin tài khoản của họ, các hacker sẽ lưu lại tên người dùng và mật khẩu đó lại.

Tấn công từ chối dịch vụ (denial of service attack)

Không giống như các cuộc tấn công mật khẩu (Password attack), các cuộc tấn công từ chối dịch vụ (denial of service attack) ngăn chặn việc sử dụng máy tính của bạn hoặc hệ thống mạng theo cách thông thường bằng valid users.

Sau khi tấn công, truy cập hệ thống mạng của bạn, các hacker có thể:

- Chặn traffic.

- Gửi các dữ liệu không hợp lý tới các ứng dụng hoặc các dịch vụ mạng, dẫn đến việc thông báo chấm dứt hoặc các hành vi bất thường trên các ứng dụng hoặc dịch vụ này.

- Lỗi tràn bộ nhớ đệm.

Tấn công phá mã khóa (Compromised-Key Attack)

Mã khóa ở đây là mã bí mật hoặc các con số quan trọng để “giải mã” các thông tin bảo mật. Mặc dù rất khó để có thể tấn công phá một mã khóa, nhưng với các hacker thì điều này là có thể. Sau khi các hacker có được một mã khóa, mã khóa này sẽ được gọi là mã khóa gây hại.

Hacker sử dụng mã khóa gây hại này để giành quyền truy cập các thông tin liên lạc mà không cần phải gửi hoặc nhận các giao thức tấn công. Với các mã khóa gây hại, các hacker có thể giải mã hoặc sửa đổi dữ liệu.



Hình 2. 22: Các cuộc tấn công phá mã khóa.

Tấn công trực tiếp

Những cuộc tấn công trực tiếp thông thường được sử dụng trong giai đoạn đầu để chiếm quyền truy nhập bên trong. Một phương pháp tấn công cổ điển là dò tìm tên người sử dụng và mật khẩu. Đây là phương pháp đơn giản, dễ thực hiện và không đòi hỏi một điều kiện đặc biệt nào để bắt đầu. Khi tấn công có thể sử dụng những thông tin như tên người dùng, ngày sinh, địa chỉ, số nhà vv.. để đoán mật khẩu. Trong trường hợp có được danh sách người sử dụng và những thông tin về môi trường làm việc, có một chương trình tự động hóa về việc dò tìm mật khẩu này.

Một chương trình có thể dễ dàng lấy được từ Internet để giải các mật khẩu đã mã hoá của hệ thống unix có tên là crack, có khả năng thử các tổ hợp các từ trong một từ điển lớn, theo những quy tắc do người dùng tự định nghĩa. Trong một số trường hợp, khả năng thành công của phương pháp này có thể lên tới 30%.

Phương pháp sử dụng các lỗi của chương trình ứng dụng và bản thân hệ điều hành đã được sử dụng từ những vụ tấn công đầu tiên và vẫn được tiếp tục để chiếm quyền truy

nhập. Trong một số trường hợp phương pháp này cho phép kẻ tấn công có được quyền của người quản trị hệ thống (root hay administrator).

Hai ví dụ thường xuyên được đưa ra để minh họa cho phương pháp này là ví dụ với chương trình sendmail và chương trình rlogin của hệ điều hành UNIX.

Sendmail là một chương trình phức tạp, với mã nguồn bao gồm hàng ngàn dòng lệnh của ngôn ngữ C. Sendmail được chạy với quyền ưu tiên của người quản trị hệ thống, do chương trình phải có quyền ghi vào hộp thư của những người sử dụng máy. Và Sendmail trực tiếp nhận các yêu cầu về thư tín trên mạng bên ngoài. Đây chính là những yếu tố làm cho sendmail trở thành một nguồn cung cấp những lỗ hổng về bảo mật để truy nhập hệ thống.

Rlogin cho phép người sử dụng từ một máy trên mạng truy nhập từ xa vào một máy khác sử dụng tài nguyên của máy này. Trong quá trình nhận tên và mật khẩu của người sử dụng, rlogin không kiểm tra độ dài của dòng nhập, do đó kẻ tấn công có thể đưa vào một xâu đã được tính toán trước để ghi đè lên mã chương trình của rlogin, qua đó chiếm được quyền truy nhập.

Tấn công vào yếu tố con người

Kẻ tấn công có thể liên lạc với một người quản trị hệ thống, giả làm một người sử dụng để yêu cầu thay đổi mật khẩu, thay đổi quyền truy nhập của mình đối với hệ thống, hoặc thậm chí thay đổi một số cấu hình của hệ thống để thực hiện các phương pháp tấn công khác.

Với kiểu tấn công này không một thiết bị nào có thể ngăn chặn một cách hữu hiệu, và chỉ có một cách giáo dục người sử dụng mạng nội bộ về những yêu cầu bảo mật để đề cao cảnh giác với những hiện tượng đáng nghi.

Nói chung yếu tố con người là một điểm yếu trong bất kỳ một hệ thống bảo vệ nào, và chỉ có sự giáo dục cộng với tinh thần hợp tác từ phía người sử dụng có thể nâng cao được độ an toàn của hệ thống bảo vệ.

Các hình thức tấn công khác

Ngoài ra còn các hình thức tấn công phổ biến khác như: Tấn công rác rưởi (Distributed attack), Tấn công mật khẩu (Password attack), Buffer overflow (lỗi tràn bộ đệm), Tấn công theo kiểu Man-in-the-Middle Attack,..vv.

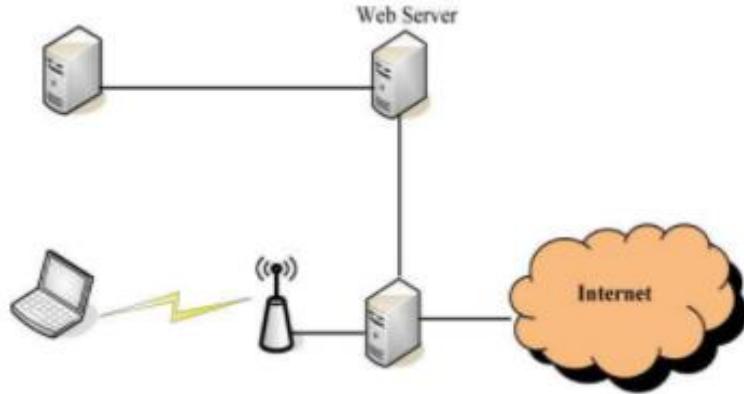
2.1.6.3 Kiến trúc Hot Spot và các hoạt động khác

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

Kiến trúc Hot Spot dựa trên công nghệ "cổng cố định". Công nghệ gần đây này được tạo ra nhờ vào việc triển khai các mạng không dây công cộng, ngay cả khi ý tưởng đầu tiên sau điều này cũng có thể áp dụng cho mạng có dây. Kiểm soát truy cập và xác thực được thực hiện nhờ cổng cố định.

Cổng cố định trong kiến trúc Hot Spot bao gồm:

- Tường lửa dựa trên quy tắc động
- Máy chủ Web
- Khung xác thực và cơ sở dữ liệu
- Khung thanh toán (tùy chọn)



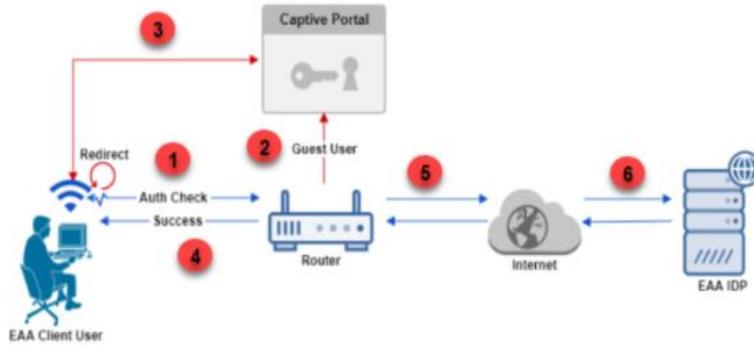
Hình 2. 23: Kiến trúc Hot Spot.

Các hoạt động của kiến trúc Hot Spot bao gồm:

- Chuyển hướng (Redirection)
 - Ủy quyền (Authorization)
 - Kết nối (Connection)
- [1] Ngắt kết nối (Disconnection)

 Chuyển hướng (Redirection)

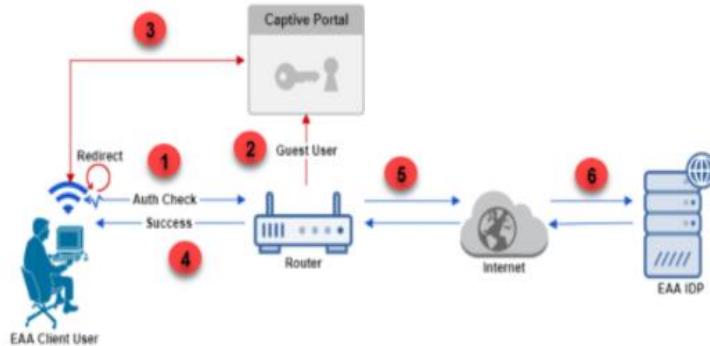
Khi một máy tính kết hợp với điểm truy cập Wi-Fi “Mở”, trước hết nó sẽ thương lượng hợp đồng thuê DHCP. Máy khách không dây sẽ được chuyển hướng đến máy chủ Web bất cứ khi nào anh ta yêu cầu truy cập Internet.



Hình 2. 24: Các hoạt động trong kiến trúc của Hot Spot.

✚ Ủy quyền (Authorization)

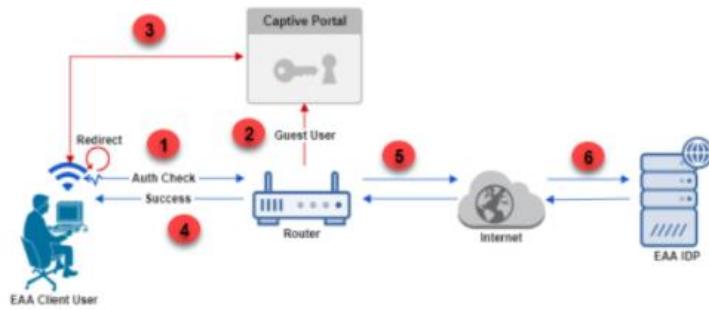
Khi người dùng tự xác thực với cổng bị khóa (bằng cách cung cấp tên người dùng / mật khẩu hợp lệ hoặc mã thông báo hợp lệ), khung xác thực sau đó sẽ cho phép người dùng giao tiếp với Internet bằng cách định cấu hình động bộ quy tắc được áp dụng trên tường lửa.



Hình 2. 25: Các hoạt động trong kiến trúc của Hot Spot.

✚ Kết nối (Connection)

Khi tường lửa đã định cấu hình bộ quy tắc mới cho người dùng được xác thực, chính sách bảo mật mẫu (do nhà cung cấp áp dụng) sẽ được thực thi và về cơ bản người dùng hiện có quyền truy cập Internet.



Hình 2. 26: Các hoạt động trong kiến trúc của Hot Spot.

Ngắt kết nối (Disconnection)

Người dùng có thể đóng kết nối với cổng bị khóa bằng cách gửi đăng xuất qua một trang Web cụ thể trên cổng bị khóa.

Ngoài ra, hầu hết các kiến trúc điểm nóng sử dụng các kỹ thuật khác để phát hiện xem người dùng có rời khỏi kiến trúc hay không (ví dụ: bằng cách gửi các đầu dò ARP hoặc quan sát sự gia hạn DHCP).

Về phân tích bảo mật:

Kiểm soát truy cập của cổng bị khóa dựa trên địa chỉ IP và / hoặc MAC.

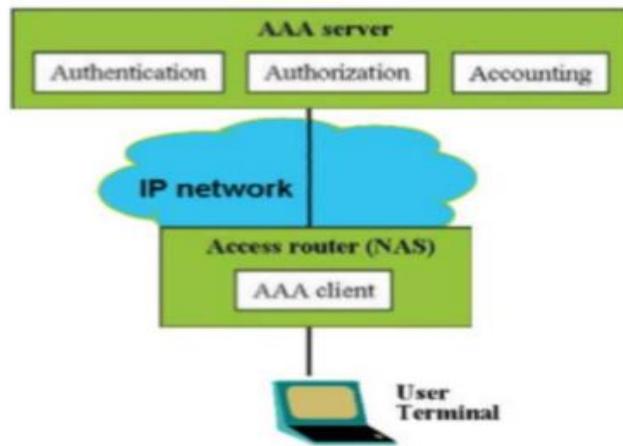
Kiến trúc điểm phát sóng dựa trên các điểm truy cập Wi-Fi “mở” không có mã hóa hoặc tính toàn vẹn dữ liệu trên mạng không dây.

Về cơ bản, cơ chế bảo vệ chính đạt được bởi điểm nóng là tường lửa điểm vào thực thi chính sách bảo mật giữa mạng không dây và Internet.

Ngoài ra, nếu kiến trúc điểm nóng không có bất kỳ mối tương quan nào giữa địa chỉ IP và MAC, thì sẽ khó phát hiện ra vấn đề. Nếu kiến trúc điểm nóng sử dụng cơ chế lọc MAC, sẽ không thể vượt qua các bộ lọc này chỉ bằng cách giả mạo IP.

2.1.6.4 Các giao thức AAA để kiểm soát quyền truy cập vào mạng riêng

❖ Giới thiệu về AAA



Hình 2. 27: Kiến trúc AAA.

AAA cho phép nhà quản trị mạng biết được các thông tin quan trọng về tình hình cũng như mức độ an toàn trong mạng. Gồm:

- + Authentication: cung cấp việc xác thực người dùng nhằm bảo đảm có thể nhận dạng đúng người dùng.
- + Authorization: Một khi đã nhận dạng người dùng, ta có thể giới hạn thẩm quyền mà người dùng có thể làm.
- + Accounting: Khi người dùng sử dụng mạng, ta cũng có thể giám sát tất cả những gì mà họ làm.

AAA với ba phần xác thực (authentication), cấp quyền (authorization), tính cước (accounting) là các phần riêng biệt mà ta có thể sử dụng trong dịch vụ mạng, cần thiết để mở rộng và bảo mật mạng.

AAA có thể dùng để tập hợp thông tin từ nhiều thiết bị trên mạng. Ta có thể bật các dịch vụ AAA trên router, switch, firewall, các thiết bị VPN, server, ...

Các giao thức sử dụng trong dịch vụ AAA

- TACACS

TACACS là giao thức sử dụng giao thức hướng kết nối (connection-oriented) là TCP trên port 49.

TACACS có các ưu điểm sau:

- + Với khả năng nhận gói reset (RST) trong TCP, một thiết bị có thể lập tức báo cho đầu cuối khác biết rằng đã có hỏng hóc trong quá trình truyền.
- + TCP là giao thức mở rộng vì có khả năng xây dựng cơ chế phục hồi lỗi. Nó có thể tương thích để phát triển cũng như làm tắc nghẽn mạng với việc sử dụng sequence number để truyền lại.
- + Toàn bộ payload được mã hóa với TACACS+ bằng cách sử dụng một khóa bí mật chung (shared secret key). TACACS+ đánh dấu một trường trong header để xác định xem thử có mã hóa hay không.
- + TACACS+ mã hóa toàn bộ gói bằng việc sử dụng khóa bí mật chung nhưng bỏ qua header TACACS chuẩn. Cùng với header là một trường xác định body có được mã hóa hay không. Thường thì trong toàn bộ thao tác, body của một gói được mã hóa hoàn toàn để truyền thông an toàn.

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

+ TACACS+ hỗ trợ nhiều giao thức.

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

+ Phương pháp thứ nhất là tạo một mức phân quyền (privilege) với một số câu lệnh giới hạn và user đã xác thực bởi router và TACACS server rồi thì sẽ được cấp cho mức đặc quyền xác định nói trên.

+ Phương pháp thứ hai đó là tạo một danh sách các dòng lệnh xác định trên TACACS+ server để cho phép một user hay một nhóm sử dụng.

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

- RADIUS

RADIUS là giao thức dựa theo mô hình client-server.

Nó dùng giao thức UDP. RADIUS server thường chạy trên máy tính.

Client là các dạng thiết bị có thể truyền thông tin đến RADIUS server được chỉ định trước và sau đó đóng vai trò phục đáp mà nó trả về.

Giao tiếp giữa client và RADIUS server được xác thực thông qua việc sử dụng khóa bí mật chung không được truyền qua mạng.

Một số ưu điểm của RADIUS là:

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

2.1.6.5 Các phương pháp bảo mật không dây

Bảo mật trong 802.1x

Tiêu chuẩn 802.1x xác định truy cập mạng điều khiển dựa trên các cổng. Chức năng của nó là xác thực và ủy quyền thiết bị được gắn vào cổng của mạng cục bộ.

IEEE 802.1X là một cách để xác thực theo người dùng hoặc mỗi thiết bị cho mạng LAN Ethernet có dây hoặc không dây (và có khả năng là các sơ đồ mạng khác trong gia đình IEEE 802). Ban đầu nó được thiết kế và triển khai cho các mạng Ethernet có dây và sau đó được nhóm làm việc của IEEE 802.11 (LAN không dây) chấp nhận, như một phần của phụ lục bảo mật 802.11i cho 802.11, để phục vụ như một phương thức xác thực cho mỗi người dùng hoặc mỗi thiết bị cho các mạng 802.11.

Khi bạn sử dụng xác thực 802.1X trên mạng WPA hoặc WPA2, bạn vẫn đang sử dụng thuật toán bảo mật và thuật toán bảo mật thông tin của WPA hoặc WPA2. Đó là, trong trường hợp của WPA, bạn vẫn đang sử dụng TKIP làm mật mã bảo mật và MICHAEL làm kiểm tra tính toàn vẹn tin nhắn của bạn. Trong trường hợp WPA2, bạn đang sử dụng AES-CCMP, đây vừa là mật mã bảo mật cũng như kiểm tra tính toàn vẹn của tin nhắn.

Sự khác biệt khi bạn đang sử dụng 802.1X là bạn không sử dụng Khóa chia sẻ trước toàn mạng (PSK) trên toàn mạng nữa. Vì bạn không sử dụng một PSK duy nhất cho tất cả các thiết bị, lưu lượng của mỗi thiết bị sẽ an toàn hơn. Với PSK, nếu bạn biết PSK và nắm bắt tay khi thiết bị tham gia mạng, bạn có thể giải mã tất cả lưu lượng truy cập của thiết bị đó. Nhưng với 802.1X, quy trình xác thực sẽ tạo tài liệu khóa được sử dụng một cách an toàn để tạo Khóa cặp chính (PMK) duy nhất cho kết nối, do đó không có cách nào để một người dùng giải mã lưu lượng người dùng khác.

802.1X dựa trên EAP, Giao thức xác thực mở rộng ban đầu được phát triển cho PPP và vẫn được sử dụng rộng rãi trong các giải pháp VPN sử dụng PPP bên trong đường hầm được mã hóa (LT2P-over-IPSec, PPTP, v.v.). Trên thực tế, 802.1X thường được gọi là "EAP qua mạng LAN" hoặc "EAPoL".

EAP cung cấp một cơ chế chung để vận chuyển các thông điệp xác thực (yêu cầu xác thực, thách thức, phản hồi, thông báo thành công, v.v.) mà không cần lớp EAP phải biết chi tiết về phương thức xác thực cụ thể đang được sử dụng. Có một số "loại EAP" khác nhau (cơ chế xác thực được thiết kế để cắm vào EAP) để thực hiện xác thực thông qua tên người dùng và mật khẩu, chứng chỉ, thẻ mã thông báo, v.v.

Do lịch sử của EAP với PPP và VPN, nó luôn dễ dàng được chuyển đến RADIUS. Do đó, nó là điển hình (nhưng không bắt buộc về mặt kỹ thuật) đối với các AP 802.11 hỗ trợ 802.1X để chứa máy khách RADIUS. Do đó, các AP thường không biết tên người dùng hoặc mật khẩu của ai hoặc thậm chí cách xử lý các loại xác thực EAP khác nhau, họ chỉ biết cách nhận một tin nhắn EAP chung từ 802.1X và chuyển nó thành tin nhắn RADIUS và chuyển tiếp nó đến máy chủ RADIUS. Vì vậy, AP chỉ là một ống dẫn để xác thực, và không phải là một bên của nó. Các điểm cuối thực sự của xác thực thường là máy khách không dây và máy chủ RADIUS (hoặc một số máy chủ xác thực ngược dòng mà máy chủ RADIUS chuyển đến).

WEP

WEP (Wired Equivalent Privacy) nghĩa là bảo mật tương đương với mạng có dây (Wired LAN). Khái niệm này là một phần trong chuẩn IEEE 802.11. Theo định nghĩa, WEP được thiết kế để đảm bảo tính bảo mật cho mạng không dây đạt mức độ như mạng nối cáp truyền thống. Đối với mạng LAN (định nghĩa theo chuẩn IEEE 802.3), bảo mật dữ liệu trên đường truyền đối với các tấn công bên ngoài được đảm bảo qua biện pháp giới hạn vật lý, tức là hacker không thể truy xuất trực tiếp đến hệ thống đường truyền cáp. Do đó chuẩn 802.3 không đặt ra vấn đề mã hóa dữ liệu để chống lại các truy cập trái phép. Đối với chuẩn 802.11, vấn đề mã hóa dữ liệu được ưu tiên hàng đầu do đặc tính của mạng không dây là không thể giới hạn về mặt vật lý truy cập đến đường truyền, bất cứ ai trong vùng phủ sóng đều có thể truy cập dữ liệu nếu không được bảo vệ.

Thay đổi tên mạng (SSID)

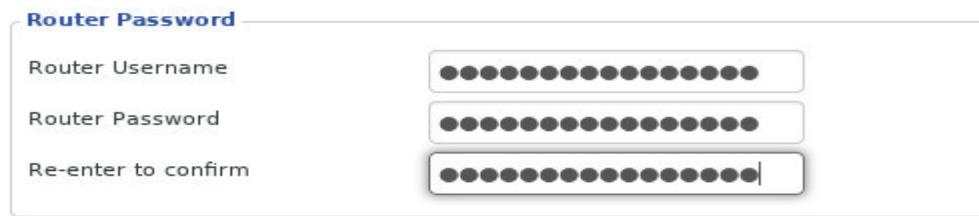
Thay đổi tên mạng (SSID) là cách bảo mật wifi thường được nhiều gia đình áp dụng bởi cách làm khá đơn giản. Bạn nên thay đổi tên mạng mặc định để tránh trường hợp kẻ tấn công biết được SSID mặc định. Bạn hãy hình dung là, mỗi sản phẩm wifi khi sản xuất ra đều có bộ định tuyến (router) và ISP. Nếu kẻ tấn công tìm ra được bộ định tuyến Router và vào được tên mạng SSID của bạn thì họ sẽ rất dễ dàng tấn công. Do đó việc thay đổi tên mạng SSID là rất cần thiết để đảm bảo an toàn khi truy cập internet bằng mạng không dây.



Hình 2. 28: Thay đổi tên mạng SSID.

Thay đổi tên người dùng và mật khẩu

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



Hình 2. 29: Thay đổi tên người dùng và mật khẩu.

Sử dụng mã hóa mạnh để bảo mật wifi

Nhiều người cho rằng mạng wifi không cần mã hóa. Tuy nhiên đây là một suy nghĩ sai lầm. Nếu bạn chưa dùng mã hóa cho mạng wifi thì những kẻ tấn công rất dễ hack wifi nhà bạn. Để mã hóa bảo mật wifi bạn có thể chọn “WPA2 Personal” cho mạng nhà mình. Nếu được bạn hãy thiết lập phiên bản mã hóa doanh nghiệp. Những cách thiết lập phiên bản doanh nghiệp khá phức tạp. Bạn cũng cần lưu ý, đối với thuật toán mã hóa bạn nên chọn AES và không nên dùng TKIP. Bởi AES sẽ cung cấp mã hóa mạnh khó tấn công hơn TKIP.



Hình 2. 30: Sử dụng mã hóa khác nhau để tăng cường bảo mật.

Chọn mật khẩu mạnh

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



Hình 2. 31: Chọn mật khẩu đủ mạnh để bảo mật tốt hơn.

Vô hiệu hóa mạng khách

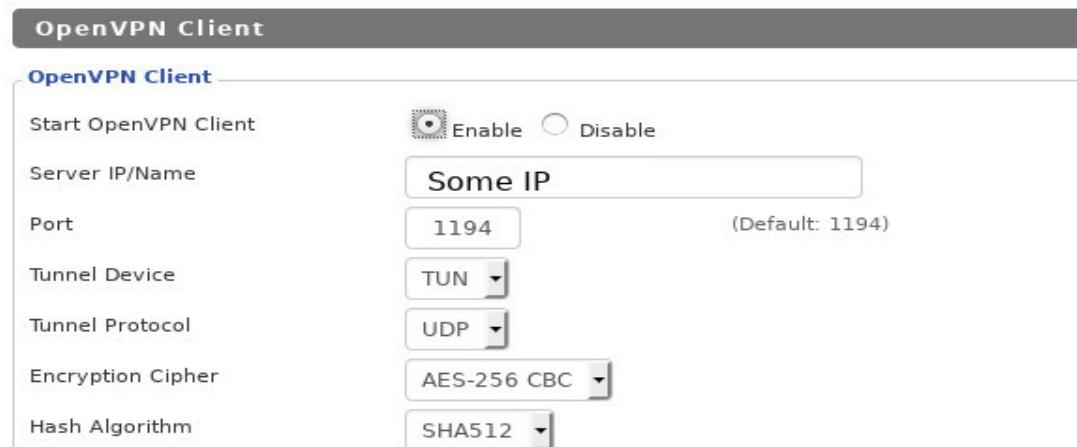
Vô hiệu hóa mạng khách cũng là cách bảo mật mạng không dây an toàn cho gia đình bạn. Nhiều gia đình để mạng wifi chế độ mở giúp ai cũng có thể kết nối wifi mà không cần mật khẩu. Tuy nhiên cách để mạng khách mở như này rất nguy hiểm. Tốt nhất là bạn nên vô hiệu hóa mạng khách bằng một dãy mật khẩu riêng.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

Bật tường lửa để bảo mật wifi

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

⊕ Sử dụng VPN

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



Hình 2. 32: Sử dụng VPN để bảo mật.

⊕ Tắt WPS

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

⊕ Quản lý firmware của bộ định tuyến

Bộ định tuyến wifi thường có một hệ điều hành tương tự như máy tính vậy. Nhưng hệ điều hành này không thể tự update của bản cập nhật bảo mật mạng không dây như

một chiếc máy tính. Một số bộ định tuyến có thể update các bản cập nhật firmware từ trên mạng. Còn các trường hợp khác thì bạn phải tải các bản cập nhật xuống rồi lại tải lên bộ định tuyến từ máy tính để cập nhật cho wifi. Lời khuyên cho bạn là vài ba tháng nên update bản cập nhật cho wifi định kỳ để đảm bảo tính bảo mật cho wifi.



Hình 2. 33: Quản lý firmware của bộ định tuyến.

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

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



Hình 2. 34: Tắt các quản lý không cần thiết.

2.2 Các thiết bị dùng trong hệ thống mạng

2.2.1 Các thiết bị chủ yếu dùng trong hệ thống

+ Router : Bộ định tuyến, thiết bị định tuyến hay tiếng Anh router (tiếng Anh-Mỹ: raotor, tiếng Anh-Anh: rutor) là một thiết bị mạng máy tính dùng để chuyển các gói dữ liệu qua một liên mạng và đến các đầu cuối, thông qua một tiến trình được gọi là định tuyến. Định tuyến xảy ra ở tầng 3 tầng mạng của mô hình OSI 7 tầng.

+ Switch: Bộ chuyển mạch hay thiết bị chuyển mạch là một thiết bị dùng để kết nối các đoạn mạng với nhau theo mô hình mạng hình sao. Theo mô hình này, switch đóng vai trò là thiết bị trung tâm, tất cả các máy tính đều được nối về đây. Switch làm việc như một Bridge nhiều cổng

+ WLC: Bộ điều khiển mạng LAN không dây được sử dụng kết hợp với Giao thức điểm truy cập hạng nhẹ để quản lý các điểm truy cập trọng lượng nhẹ với số lượng lớn bởi quản trị viên mạng hoặc trung tâm điều hành mạng. Bộ điều khiển LAN không dây là một phần của Mặt phẳng dữ liệu trong Mô hình không dây của Cisco.

+ Bộ chia HUB: Hub là gì ? (Hay còn có thể nói là bộ chia mạng là gì?). Khi nói về mạng máy tính thì HUB là một phần không thể thiếu, vì nó là một thiết bị mạng cơ bản, có khả năng kết nối nhiều máy tính hay nhiều thiết điện tử với nhau. Thông thường một HUB thì có 4 đến 24 cổng nên chúng còn được gọi là bộ chia mạng. HUB là trung tâm kết nối các thiết bị trong hệ thống mạng, dùng để kết nối mạng LAN vì chúng có khá nhiều cổng giúp thực hiện công việc đó dễ dàng hơn. Có nghĩa là dữ liệu được truyền đến một cổng và nó sẽ sao chép ra và chuyển đến các cổng khác tương tự như vậy, giúp các cổng khác nhận dạng được các thông tin đó. Tóm lại HUB đóng vai trò như một kết nối của nó đến với tất cả thiết bị mạng. Nhưng HUB không phân biệt được cổng sẽ thực hiện nhiệm vụ gửi đến nên nó dành chuyển đến tất cả các cổng, để đảm bảo rằng nó đã truyền hết thông tin đi theo dự tính.

+ Modem: Modem (viết tắt của Modulator and Demodulator – Bộ điều giải) là một thiết bị điều chế tín hiệu tương tự để mã hóa dữ liệu số, và giải điều chế tín hiệu mạng để giải mã tín hiệu số. Giải thích một cách dễ hiểu hơn thì modem biến đổi thông tin kỹ thuật số từ các thiết bị kết nối mạng (máy tính, điện thoại) thành tín hiệu analog có thể truyền qua dây dẫn, và ngược lại, modem dịch các tín hiệu analog thành dữ liệu số mà những thiết bị như máy tính có thể hiểu được.

+ Gateway: Gateway là một nút mạng được sử dụng trong viễn thông nhằm kết nối hai mạng có giao thức truyền thông khác nhau có thể giao tiếp được với nhau. Gateway có vai trò xử lý đầu vào và ra của mạng vì tất cả dữ liệu phải đi qua hoặc giao tiếp với gateway trước khi được định tuyến. Trong hầu hết các mạng IP, lưu lượng duy nhất không đi qua gateway là lưu lượng truyền giữa các nút trên cùng một phân đoạn mạng cục bộ (LAN). Thuật ngữ default gateway hoặc network gateway cũng có thể được sử dụng để mô tả khái niệm trên.

+ Bộ lặp Repeater: Bộ lặp là một thiết bị điện tử có hai cổng: cổng vào và cổng ra. Nó có chức năng bù suy hao tín hiệu bằng cách chuyển tiếp tất cả các tín hiệu điện đến từ cổng vào tới cổng ra sau khi đã khuếch đại. Bộ lặp được sử dụng, được tích hợp trong đa số các hệ thống viễn thông.

+ Cầu nối Bridge: Bridge còn được gọi là cầu nối, là một thiết bị lưu trữ / chuyển tiếp kết nối hai mạng LAN, nó có thể chia một mạng LAN lớn thành nhiều đoạn mạng hoặc kết nối hai hay nhiều mạng LAN thành một mạng LAN logic. Tất cả người dùng của có thể truy cập vào máy chủ. Cách phổ biến nhất để mở rộng mạng LAN là sử dụng cầu nối

+ Máy chủ (Server) là một máy tính được kết nối với mạng máy tính hoặc Internet, có IP tĩnh, có năng lực xử lý cao. Trên đó người ta cài đặt các phần mềm để phục vụ cho các máy tính khác truy cập để yêu cầu cung cấp các dịch vụ và tài nguyên. Và nó được

sử dụng cho nhu cầu lưu trữ và xử lý dữ liệu trong một mạng máy tính hoặc trên môi trường Internet. Máy chủ là nền tảng của mọi dịch vụ trên Internet, bất kỳ một dịch vụ nào trên Internet như Website, ứng dụng, trò chơi,... muốn vận hành cũng đều phải thông qua một máy chủ nào đó. Theo chức năng, máy chủ được chia thành các loại sau: Database servers, File servers, Mail servers, Print servers, Web servers, Game servers, Application servers.

+ Access Point là một thiết bị có khả năng tạo ra WLAN, hay còn gọi là mạng không dây cục bộ. Access Point thường được dùng tại môi trường công sở, nhà hàng, tiệc cưới hay các tòa nhà lớn nhằm tạo ra không gian sử dụng mạng rộng rãi mà không làm suy giảm tốc độ của mạng. Ngoài ra, Access Point còn khả năng chuyển đổi mạng có dây thành mạng không dây, từ đây mà các thiết bị có thể dễ dàng kết nối được. Có thể hiểu Access Point là một loại thiết bị thu phát WiFi. Tuy nhiên, không vì thế mà tính bảo mật trên không gian mạng bị suy giảm theo, điều này giúp bạn có thể yên tâm sử dụng thiết bị.



Hình 2. 35: Các thiết cơ bản được sử dụng.

2.2.2 *Bảng giá tham khảo các thiết bị được sử dụng trong xây dựng mô hình DEMO*

Tên thiết bị	Loại	Số lượng	Đơn giá
Router	ISR4331-K9	2	$34\ 110\ 000 \times 2 = 68\ 220\ 000$
Multilayer Switch	WS-C3650-24PS-S	1	45 557 100
Wireless LAN controller	AIR-CT2504-5-K9		12 690 000
Light Weight Access Point	AIR-CAP3702I-C-K9	6	$5\ 000\ 000 \times 6 = 30\ 000\ 000$
Server	Dell PowerEdge T40 (Standard)	3	$17\ 460\ 000 \times 3 = 52\ 380\ 000$
PC văn phòng	Dell Inspiron Desktops 3881 42IN380006	4	$10\ 000\ 000 \times 4 = 40\ 000\ 000$
Printer	HP LaserJet Pro MFP M135w 4ZB83A	4	$3\ 690\ 000 \times 4 = 14\ 760\ 000$

Bảng 2. 1: Bảng giá các thiết bị sử dụng trong hệ thống.

CHƯƠNG 3 – MÔ HÌNH DEMO

3.1 Mô hình đề xuất

3.1.1 Bảng địa chỉ

Device	Interface	IP Address
R0	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
R1	G0/0/1	172.31.1.1/24
	G0/0/0.10	192.168.10.1/24
	G0/0/0.20	192.168.20.1/24
	G0/0/0.30	192.168.30.1/24
	G0/0/0.40	192.168.40.1/24
	G0/0/0.50	192.168.50.1/24
	G0/0/0.60	192.168.60.1/24
	G0/0/0.200	192.168.200.1/24
	S0/1/0	10.20.30.2/30
Home Wireless Router	Internet	DHCP
	LAN	192.168.0.1/24
Mul_Sw	VLAN 200	192.168.200.100/24
WLC	Management	192.168.200.254/24

RADIUS Server	NIC	172.31.1.254/24
Web Server	NIC	203.0.113.78/24
DNS Server	NIC	10.100.100.254/24
ADMIN Enterprise	NIC	192.168.200.199/24
Enterprise PC	NIC	192.168.200.200/24
LAP.LETAN, LAP.GIAMDOC, LAP.TAICHINH, LAP.MARKETING, LAP.KINHDOANH, LAP.PHONGHOP	G0	DHCP
Home Admin	NIC	DHCP
PC.LETAN, PC.TC, PC.KD	Wireless0	DHCP
GIAMDOC, THUKY, Home Laptop, NhanVien1, NhanVien2, NhanVien3, NhanVien4, NhanVien5, NhanVien6, NhanVien7	Wireless0	DHCP
Home TabletPC, Guest Tablet PC	Wireless0	DHCP
Home Smartphone, Guest Smartphone, NhanVien Smartphone	Wireless0	DHCP
Printer_TC, Printer_Marketing, Printer_KD	Wireless0	DHCP

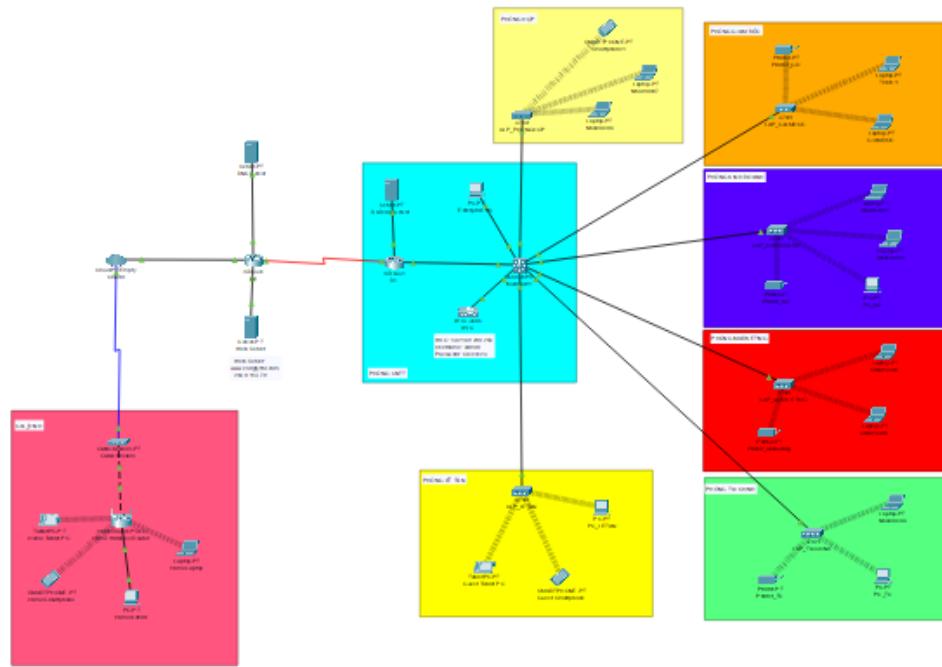
Bảng 3. 1: Bảng địa chỉ được sử dụng trong hệ thống.

3.1.2 Bảng thông tin WLAN

WLAN	SSID	Authentication	Username	Password
Mang gia dinh	GiaDinh	WPA2 – Personal	N/A	giadinh123
WLAN VLAN 1	PhongHop	WPA2 – Enterprise	phonghop	phonghop123
WLAN VLAN 2	GiamDoc	WPA2 – Enterprise	giamdoc	giamdoc123
WLAN VLAN 3	KinhDoanh	WPA2 – Enterprise	kinhdoanh	kinhdoanh123
WLAN VLAN 4	Marketing	WPA2 – Enterprise	marketing	marketing123
WLAN VLAN 5	TaiChinh	WPA2 – Enterprise	taichinh	taichinh123
WLAN VLAN 6	LeTan	WPA2 – Personal	N/A	letan123

Bảng 3. 2: Bảng thông tin WLAN.

3.1.3 Mô hình đề xuất

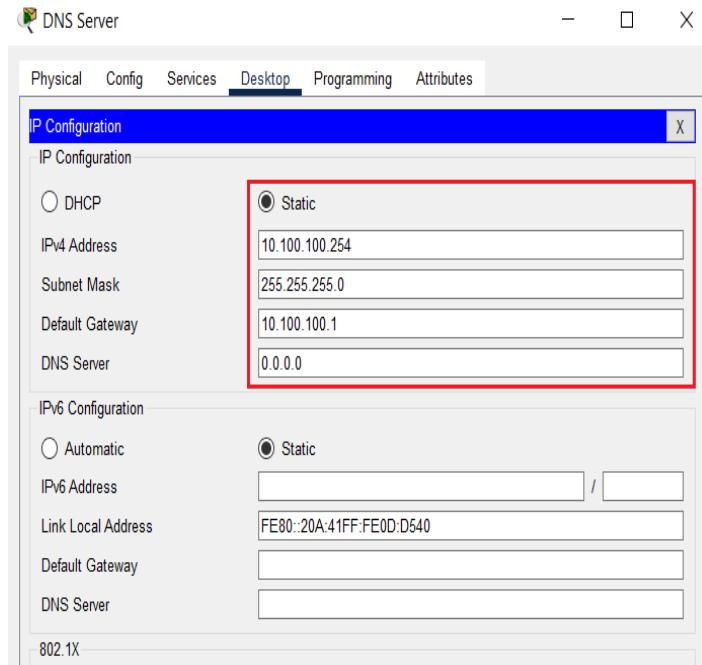


Hình 3. 1: Mô hình đề xuất cho doanh nghiệp.

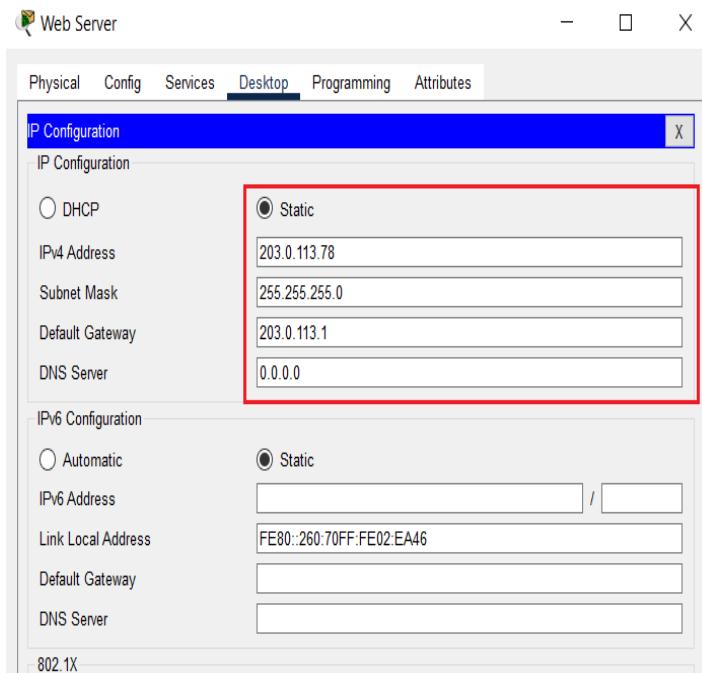
3.2 Cấu hình các thiết bị

3.2.1 Thiết lập IP cho DNS Server, Web Server, RADIUS Server.

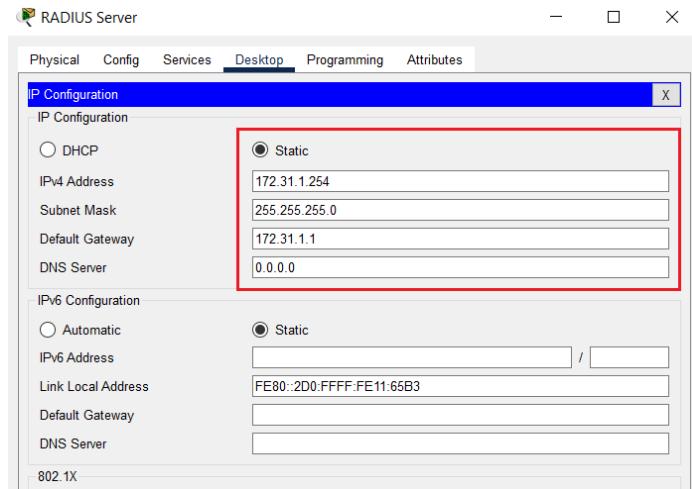
Vào các thiết bị DNS Server, Web Server, RADIUS Server. Chọn tab Desktop, chọn IP Configuration. Nhập địa chỉ tương ứng trong bảng địa chỉ.



Hình 3. 2: Giao diện địa chỉ DNS Server.



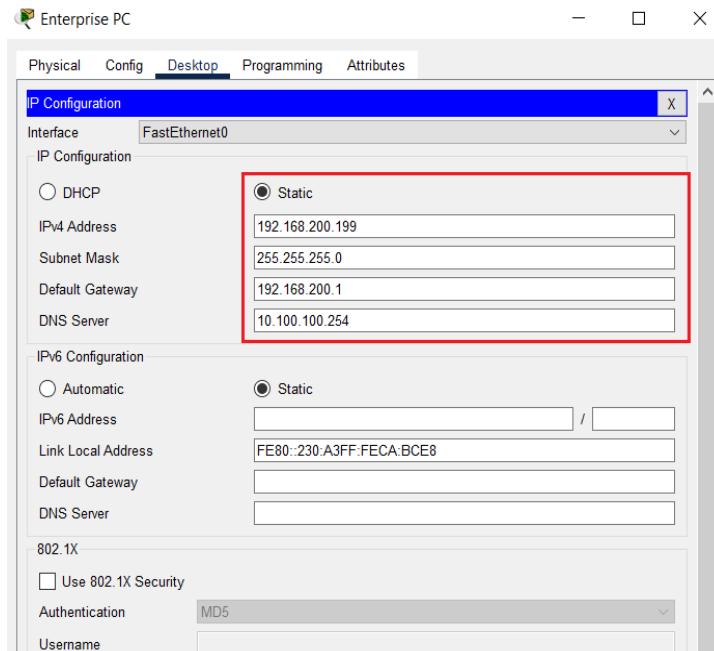
Hình 3. 3: Giao diện địa chỉ Web Server.



Hình 3. 4: Giao diện địa chỉ RADIUS Server.

3.2.2 Thiết lập IP cho Enterprise PC.

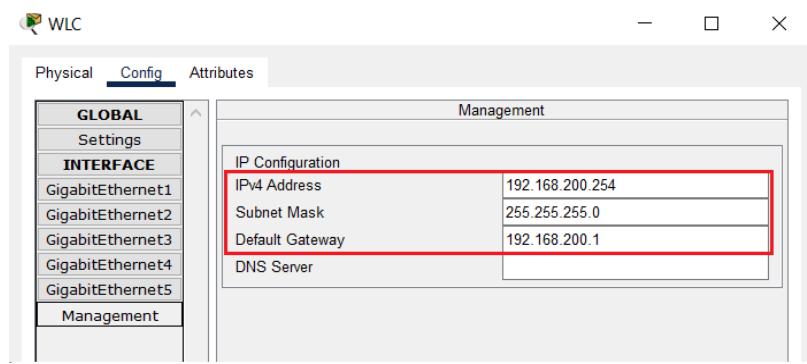
Vào các thiết bị Enterprise PC. Chọn tab Desktop, chọn IP Configuration. Nhập địa chỉ tương ứng trong bảng địa chỉ.



Hình 3. 5: Giao diện địa chỉ Enterprise PC.

3.2.3 Thiết lập IP cho Wireless LAN Controller (WLC).

Vào thiết bị WLC, chọn tab config, chọn management. Đặt IP cho thiết bị.



Hình 3. 6: Giao diện địa chỉ WLC.

3.2.4 Cấu hình thiết bị Multilayer Switch.

Tạo vlan: Cấu hình tạo các **vlan 10, 20, 30, 40, 50, 60, 200** trên multilayer switch để kết nối đến phòng ban của doanh nghiệp THL.

The screenshot shows the Multi SW CLI interface. The command line shows the configuration of multiple VLANs. A red box highlights the configuration commands for VLANs 10 through 60 and 200. The commands are:

```

Multi-SW>
Multi-SW>
Multi-SW>ena
Multi-SW#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Multi-SW(config)#vlan 10
Multi-SW(config-vlan)#name GianDoc
Multi-SW(config-vlan)#ex
Multi-SW(config)#vlan 20
Multi-SW(config-vlan)#name KinhDoanh
Multi-SW(config-vlan)#ex
Multi-SW(config)#vlan 30
Multi-SW(config-vlan)#name Marketing
Multi-SW(config-vlan)#ex
Multi-SW(config)#vlan 40
Multi-SW(config-vlan)#name TaiChinh
Multi-SW(config-vlan)#ex
Multi-SW(config)#vlan 50
Multi-SW(config-vlan)#name LeTan
Multi-SW(config-vlan)#ex
Multi-SW(config)#vlan 60
Multi-SW(config-vlan)#name PhongHop
Multi-SW(config-vlan)#ex
Multi-SW(config)#vlan 200
Multi-SW(config-vlan)#name wireless_management
Multi-SW(config-vlan)#ex
Multi-SW(config)#ex
Multi-SW#
%SYS-5-CONFIG_I: Configured from console by console

```

Hình 3. 7: Câu lệnh tạo các vlan trên multilayer switch.

Hình 3. 8: Kết quả sau khi tạo các vlan trên multilayer switch.

Cấu hình Trunk để sử dụng nhiều vlan trên multilayer switch. Cổng **g1/0/2-7** kết từ multilayer switch đến các thiết bị Light Weight Access Point của phòng doanh nghiệp. Cổng **g1/0/23-24** lân lượt kết nối đến thiết bị WLC và R1. Cổng g1/0/1 kết nối Enterprise PC.

Hình 3.9: Câu lệnh cấu hình trunk cho các cổng trên multilayer switch.

3.2.5 Cấu hình thiết bị Router 1.

Cấu hình địa chỉ IP cho cổng **g0/0/1** kết nối đến RADIUS server và cổng **Se0/1/0** kết nối đến router 0.

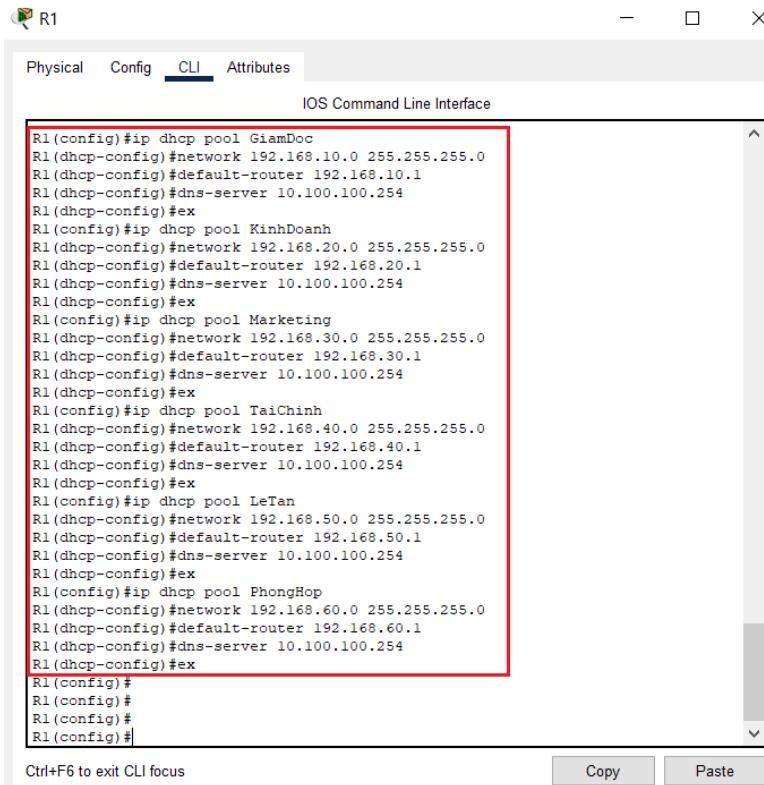
Hình 3. 10: Câu lệnh cấu hình địa chỉ IP cho các cổng của router 1.

Tạo các cổng ảo g0/0/0.10, g0/0/0.20, g0/0/0.30, g0/0/0.40, g0/0/0.50, g0/0/0.60.

R1>
R1>ena
R1>conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface g0/0/0.10
R1(config-subif)#encapsulation dot1Q 10
R1(config-subif)#ip address 192.168.10.1 255.255.255.0
R1(config-subif)#exit
R1(config)#interface g0/0/0.20
R1(config-subif)#encapsulation dot1Q 20
R1(config-subif)#ip address 192.168.20.1 255.255.255.0
R1(config-subif)#exit
R1(config)#interface g0/0/0.30
R1(config-subif)#encapsulation dot1Q 30
R1(config-subif)#ip address 192.168.30.1 255.255.255.0
R1(config-subif)#exit
R1(config)#interface g0/0/0.40
R1(config-subif)#encapsulation dot1Q 40
R1(config-subif)#ip address 192.168.40.1 255.255.255.0
R1(config-subif)#exit
R1(config)#interface g0/0/0.50
R1(config-subif)#encapsulation dot1Q 50
R1(config-subif)#ip address 192.168.50.1 255.255.255.0
R1(config-subif)#exit
R1(config)#interface g0/0/0.60
R1(config-subif)#encapsulation dot1Q 60
R1(config-subif)#ip address 192.168.50.1 255.255.255.0
% 192.168.50.0 overlaps with GigabitEthernet0/0/0.50
R1(config-subif)#ip address 192.168.60.1 255.255.255.0
R1(config-subif)#exit
R1(config)#interface g0/0/0.70
R1(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0.70, changed state to up

Hình 3. 11: Câu lệnh cấu hình các cổng ảo trên router 1.

Cấu hình DHCP pool để cấp phát IP cho mạng **192.168.10.0/24**, **192.168.20.0/24**, **192.168.30.0/24**, **192.168.40.0/24**, **192.168.50.0/24**, **192.168.60.0/24**.



```

R1(config)#ip dhcp pool GiamDoc
R1(dhcp-config)#network 192.168.10.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.10.1
R1(dhcp-config)#dns-server 10.100.100.254
R1(dhcp-config)#ex
R1(config)#ip dhcp pool KinhDoanh
R1(dhcp-config)#network 192.168.20.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.20.1
R1(dhcp-config)#dns-server 10.100.100.254
R1(dhcp-config)#ex
R1(config)#ip dhcp pool Marketing
R1(dhcp-config)#network 192.168.30.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.30.1
R1(dhcp-config)#dns-server 10.100.100.254
R1(dhcp-config)#ex
R1(config)#ip dhcp pool TaiChinh
R1(dhcp-config)#network 192.168.40.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.40.1
R1(dhcp-config)#dns-server 10.100.100.254
R1(dhcp-config)#ex
R1(config)#ip dhcp pool LeTan
R1(dhcp-config)#network 192.168.50.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.50.1
R1(dhcp-config)#dns-server 10.100.100.254
R1(dhcp-config)#ex
R1(config)#ip dhcp pool PhongHop
R1(dhcp-config)#network 192.168.60.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.60.1
R1(dhcp-config)#dns-server 10.100.100.254
R1(dhcp-config)#ex
R1(config)#
R1(config)#
R1(config)#
R1(config)#

```

Hình 3. 12: Câu lệnh cấu hình DHCP pool trên router 1.

3.2.6 Cấu hình thiết bị Router 0.

Cấu hình địa chỉ IP cho cổng **g0/0/0** kết nối đến Cloud, cổng **g0/0/1** kết nối đến Web server, cổng **g0/0/2** kết nối đến DNS server và cổng **se0/1/0** kết nối đến router 1.

```

R0>ena
R0#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R0(config)#interface g0/0/0
R0(config-if)#ip address 10.100.200.1 255.255.255.0
R0(config-if)#no shutdown
R0(config-if)#ex
R0(config)#interface g0/0/1
R0(config-if)#ip address 203.0.113.1 255.255.255.0
R0(config-if)#no shutdown
R0(config-if)#ex
R0(config)#interface g0/0/2
R0(config-if)#ip address 10.100.100.1 255.255.255.0
R0(config-if)#no shutdown
R0(config-if)#ex
R0(config)#interface se0/1/0
R0(config-if)#ip address 10.20.30.1 255.255.255.0
R0(config-if)#ex
R0(config)#ex
R0#
%SYS-5-CONFIG_I: Configured from console by console
R0#
R0#
R0#
R0#
R0#
R0#

```

Ctrl+F6 to exit CLI focus Copy Paste

Hình 3. 13: Câu lệnh cấu hình địa chỉ IP cho các cổng của router 0.

Cấu hình định tuyến tĩnh để router thực hiện chuyển gói dữ liệu tới địa chỉ mạng đích dựa vào địa chỉ IP đích của gói dữ liệu.

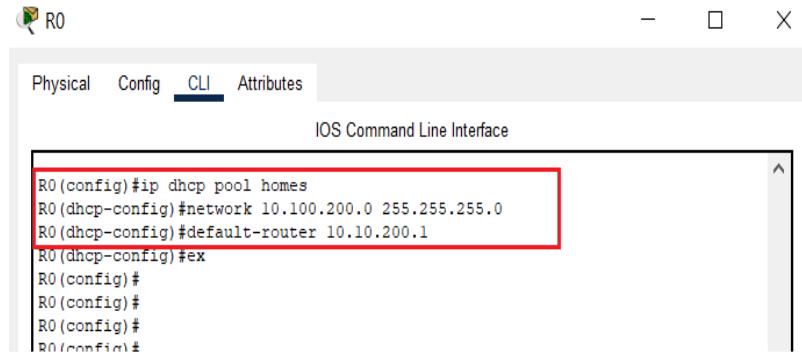
```

R0#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R0(config)#
R0(config)#ip route 192.168.10.0 255.255.255.0 10.20.30.2
R0(config)#ip route 192.168.20.0 255.255.255.0 10.20.30.2
R0(config)#ip route 192.168.30.0 255.255.255.0 10.20.30.2
R0(config)#ip route 192.168.40.0 255.255.255.0 10.20.30.2
R0(config)#ip route 192.168.50.0 255.255.255.0 10.20.30.2
R0(config)#ip route 192.168.200.0 255.255.255.0 10.20.30.2
R0(config)#ip route 192.168.60.0 255.255.255.0 10.20.30.2
R0(config)#
R0(config)#
R0(config)#
R0(config)#
R0(config)#
R0(config)#
R0(config)#

```

Hình 3. 14: Câu lệnh cấu hình định tuyến tĩnh trên router 0.

Cấu hình DHCP pool để cấp phát IP cho mạng **10.100.200.0/24**.



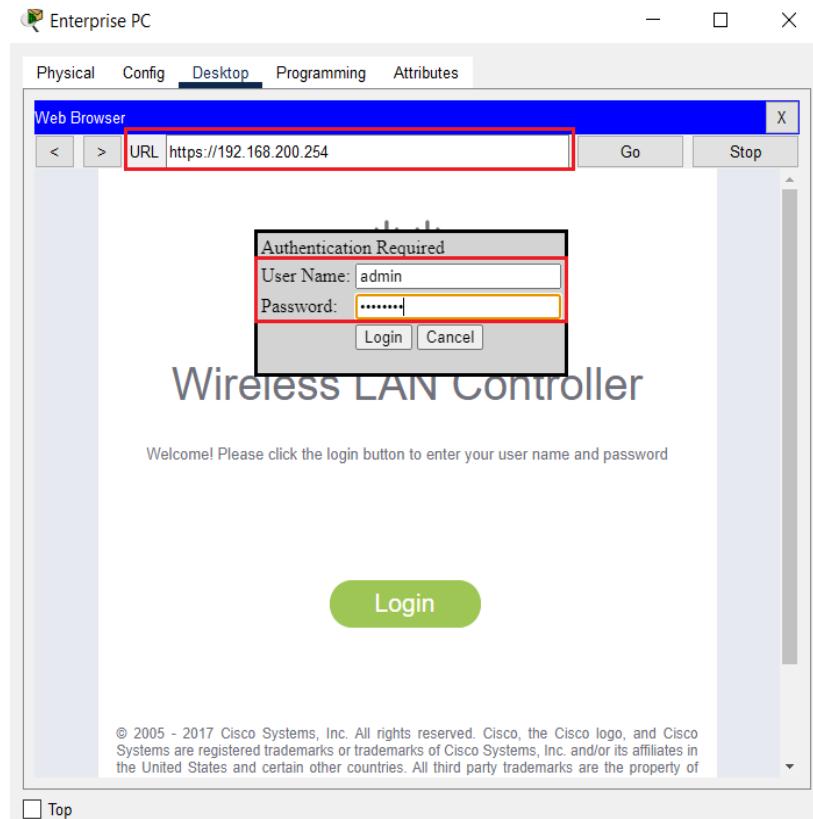
```
R0(config)#ip dhcp pool homes
R0(dhcp-config)#network 10.100.200.0 255.255.255.0
R0(dhcp-config)#default-router 10.10.200.1
R0(dhcp-config)#ex
R0(config)#
R0(config)#
R0(config)#
R0(config)#
R0(config)#
```

Hình 3. 15: Câu lệnh cấu hình DHCP pool trên router 0.

3.2.7 Cấu hình thiết bị Wireless LAN Controller.

3.2.7.1 Cấu hình các giao diện VLAN.

Bước 1: Từ Enterprise PC, điều hướng đến giao diện quản lý WLC qua trình duyệt web. Để đăng nhập vào WLC, chọn thiết bị Enterprise PC, chọn tab Desktop, Chọn Web Browser. Nhập địa chỉ url **<https://192.168.200.254>**, sử dụng **admin** làm tên người dùng và **Cisco123** làm mật khẩu.



Hình 3. 16: Giao diện đăng nhập vào bộ điều khiển WLC.

Bước 2: Tạo và cấu hình giao diện cho mạng WLAN 10, 20, 30, 40, 50, 60. Đầu tiên chúng ta sẽ tạo WLAN 10. Vào Controller, chọn Interfaces, chọn New...

Name: **WLAN 10/ 20/ 30/ 40/ 50/ 60**

VLAN Identifier: **10/ 20/ 30/ 40/ 50/ 60**

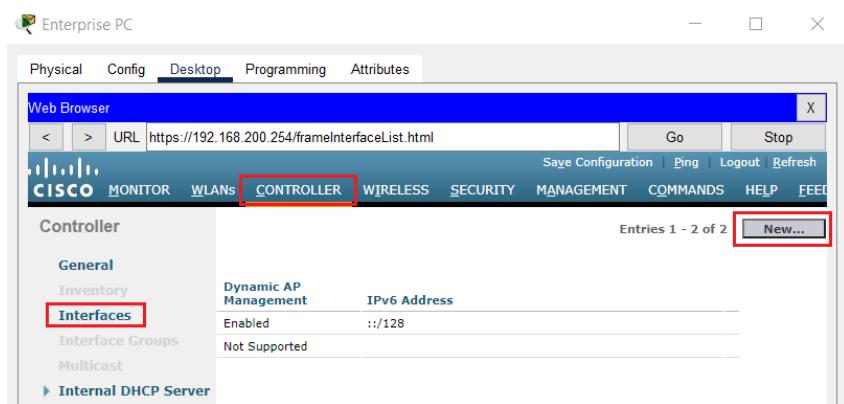
Port Number: **1**

Interface IP Address: **192.168.10.254/ 192.168.20.254/ 192.168.30.254/ 192.168.40.254/ 192.168.50.254/ 192.168.60.254**

Netmask: **255.255.255.0**

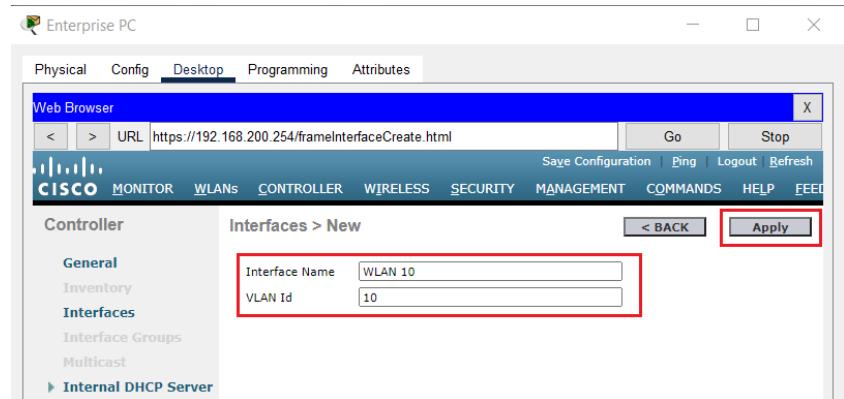
Gateway: **192.168.10.1/ 192.168.20.1/ 192.168.30.1/ 192.168.40.1/ 192.168.50.1/ 192.168.60.1**

Primary DHCP Server: **192.168.10.1/ 192.168.20.1/ 192.168.30.1/ 192.168.40.1/ 192.168.50.1/ 192.168.60.1**



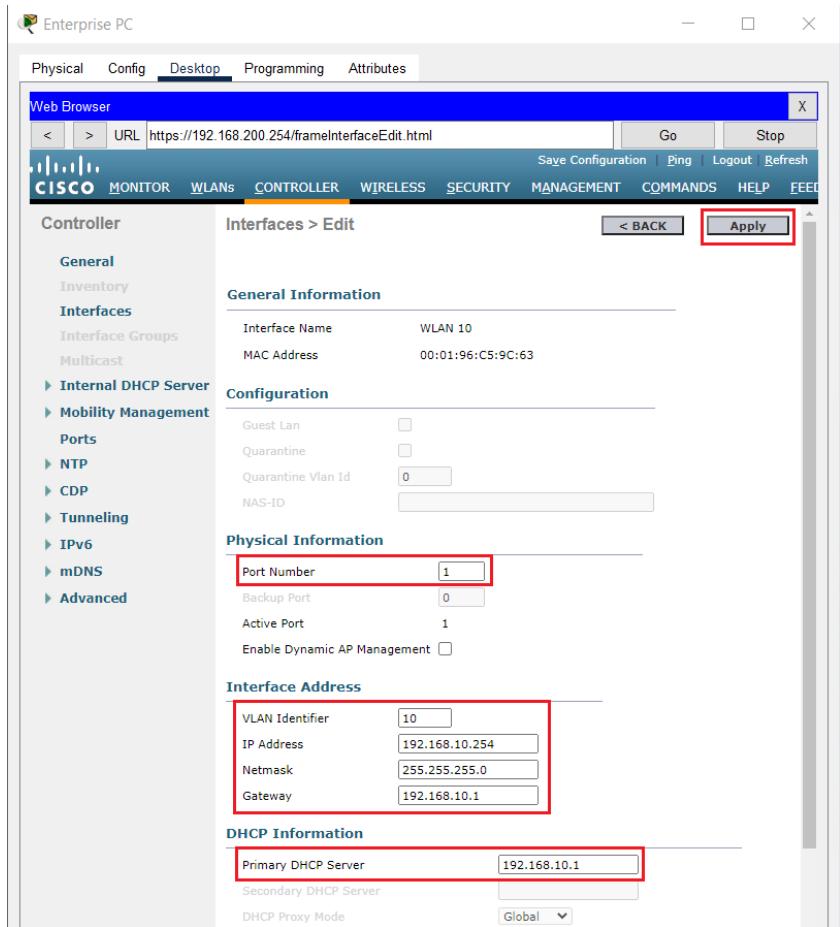
Hình 3. 17: Giao diện các thao tác tạo mạng VLAN.

Bước 3: Điền thông tin Interface Name và VLAN Id rồi ấn Apply.



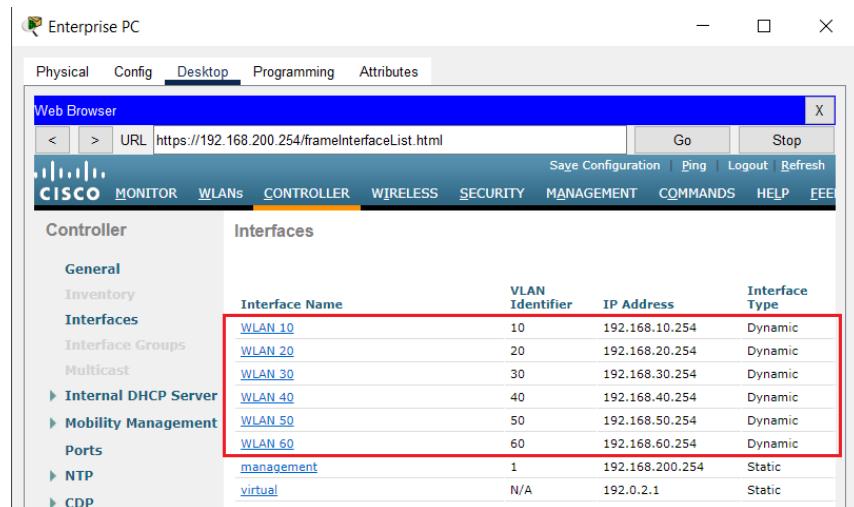
Hình 3. 18: Giao diện điền thông tin tạo WLAN 10.

Bước 4: Điền thông tin địa chỉ cho Port Number, IP Address, Netmask, Gateway, Primary DHCP Server. Ấn Apply.



Hình 3. 19: Giao diện cấu hình địa chỉ cho WLAN 10.

Bước 5: Làm tương tự với **WLAN 20, 30, 40, 50, 60** với địa chỉ tương ứng.



Hình 3. 20: Giao diện kết quả tạo thành công các WLAN.

3.2.7.2 Cấu hình DHCP Scope cho mạng quản lý không dây.

Scope Name: **management**

Pool Start Address: **192.168.200.235**

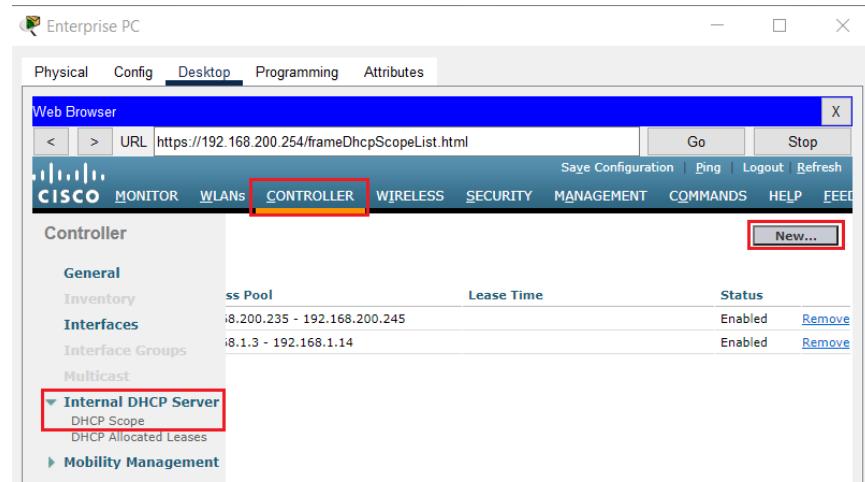
Pool End Address: **192.168.200.245**

Network: **192.168.200.0**

Netmask: **255.255.255.0**

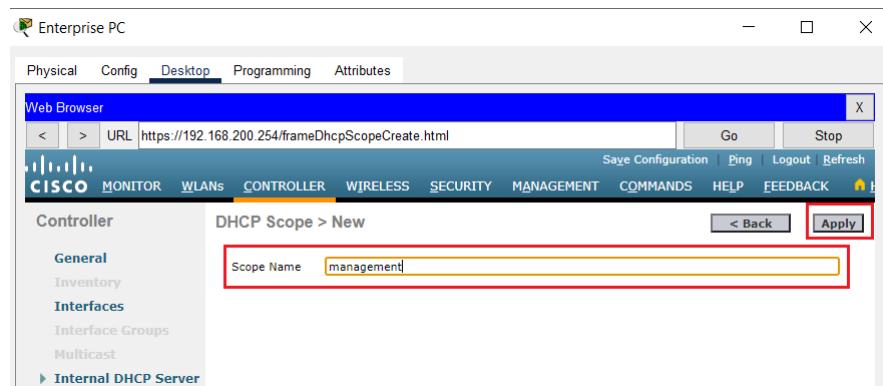
Default Routers: **192.168.200.1**

Bước 1: Vào Controller, chọn DHCP Scope trong Internal DHCP Server, chọn New...



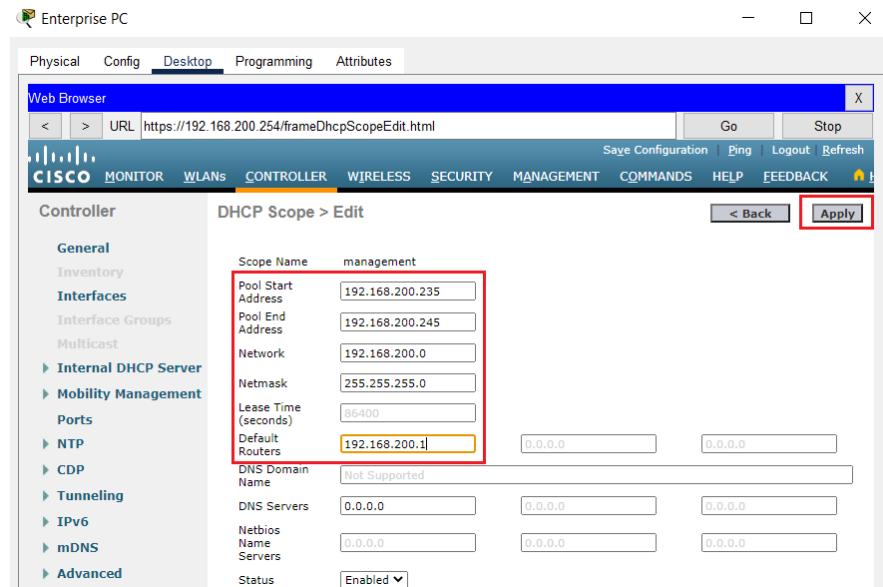
Hình 3. 21: Giao diện các thao tác tạo DHCP Scope.

Bước 2: Điền thông tin Scope Name và ấn Apply.

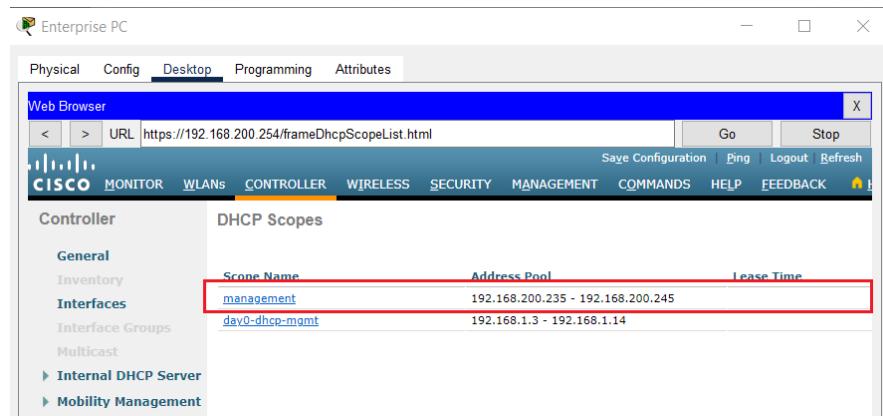


Hình 3. 22: Giao diện điền thông tin tạo DHCP Scope.

Bước 3: Điền thông tin địa chỉ cho Pool Start Address, Pool End Address, Network, Netmask, Default Routers. Ấn Apply.



Hình 3. 23: Giao diện cấu hình địa chỉ cho management.



Hình 2. 36: Giao diện kết quả tạo thành công Scope Name management.

3.2.7.3 Cấu hình WLC với các địa chỉ server bên ngoài.

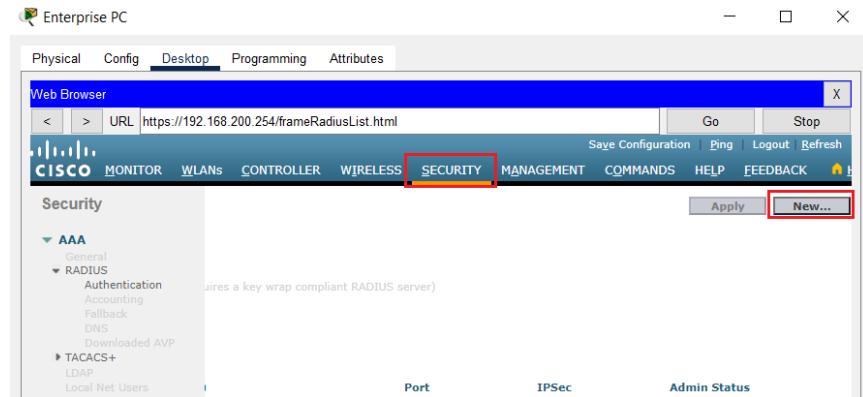
Bước 1: Cấu hình thông tin RADIUS Server.

Server Index: 1

Server Address: 172.31.1.254

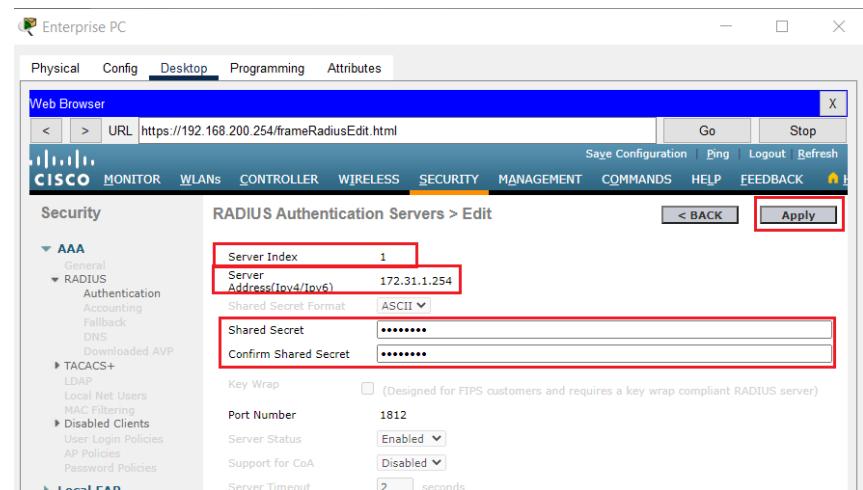
Shared Secret: Cisco123

+ Vào Security, chọn New...

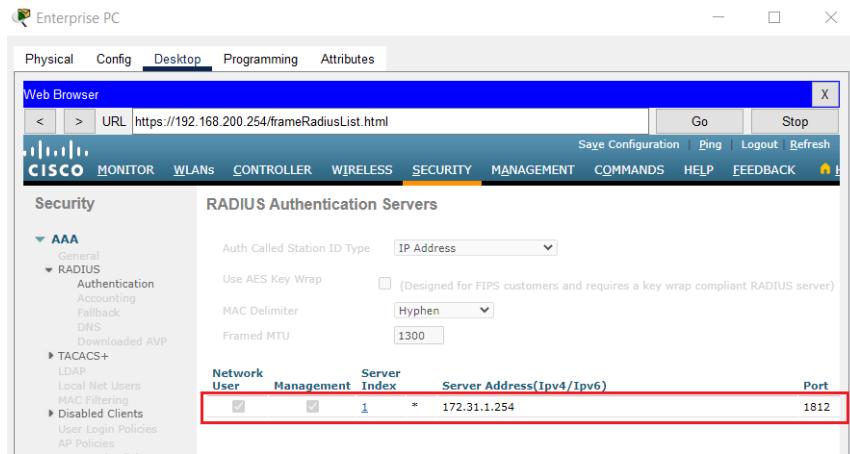


Hình 3. 24: Giao diện các thao tác tạo RADIUS Server.

+ Điền thông tin Server Index, Server Address, Shared Secret, Comfirm Shared Secret. Ấn Apply.



Hình 3. 25: Giao diện cấu hình thông tin cho RADIUS Server.



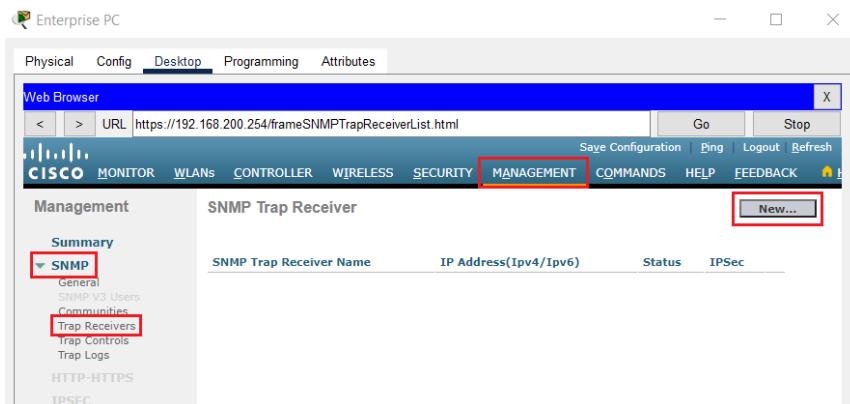
Hình 3. 26: Kết quả tạo thành công RADIUS Server.

Bước 2: Cấu hình WLC để gửi thông tin nhật ký đến SNMP Server.

Community Name: WLAN

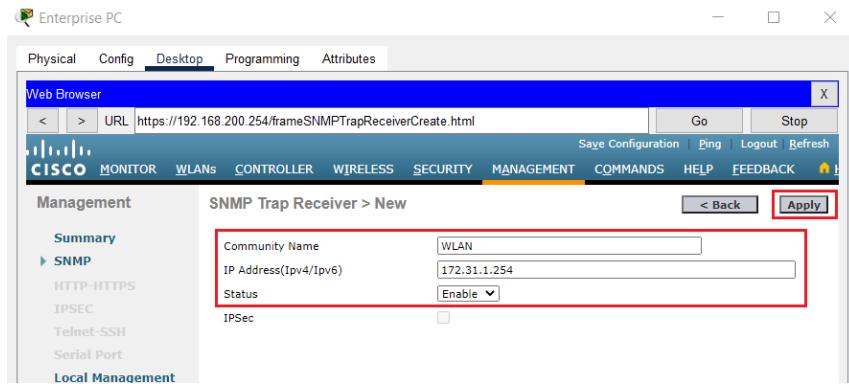
IP Address: 172.31.1.254

+ Vào Management, chọn Trap Receiver trong SNMP, chọn New...

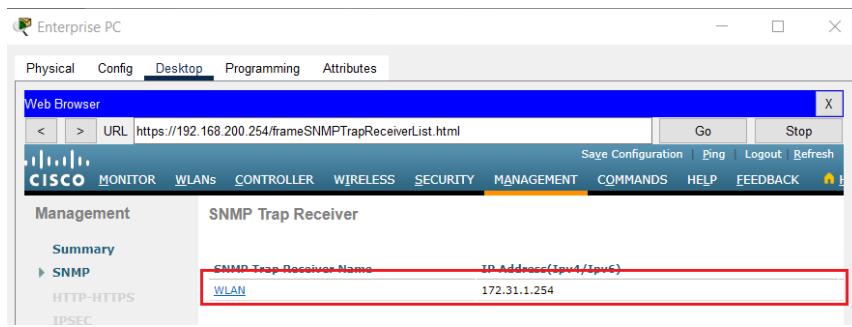


Hình 3. 27: Giao diện các thao tác tạo SNMP Trap Receiver.

+ Diền các thông tin rồi ấn Apply.



Hình 3. 28: Giao diện cấu hình thông tin SNMP Trap Receiver.



Hình 3. 29: Giao diện kết quả tạo thành công SNMP Trap Receiver.

3.2.7.4 Tạo các mạng WLANs

Bước 1: Tạo WLAN 6 cấu hình Security: PSK – WPA2-Personal

Profile Name: **LeTan**

WLAN SSID: **LeTan**

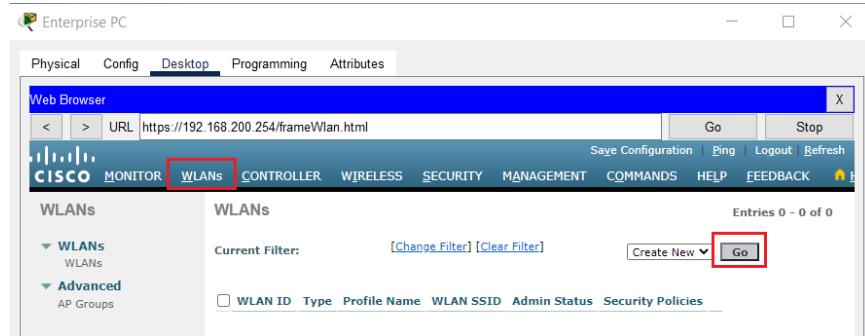
ID: **6**

Interface: **WLAN 6**

Security: **WPA2-PSK**

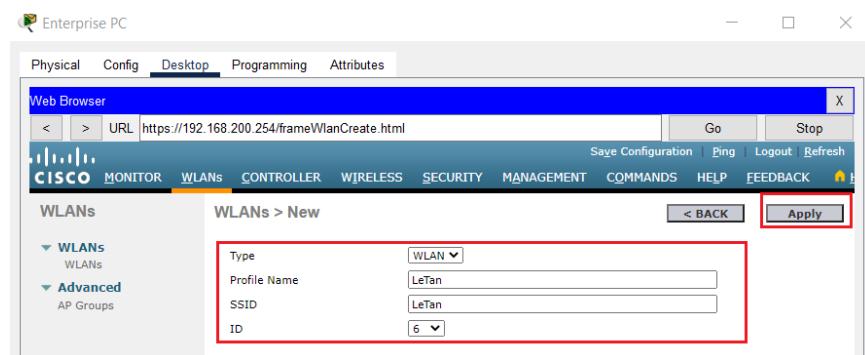
Passphrase: **Cisco123**

+ Chọn WLANs, chọn Go để tạo.



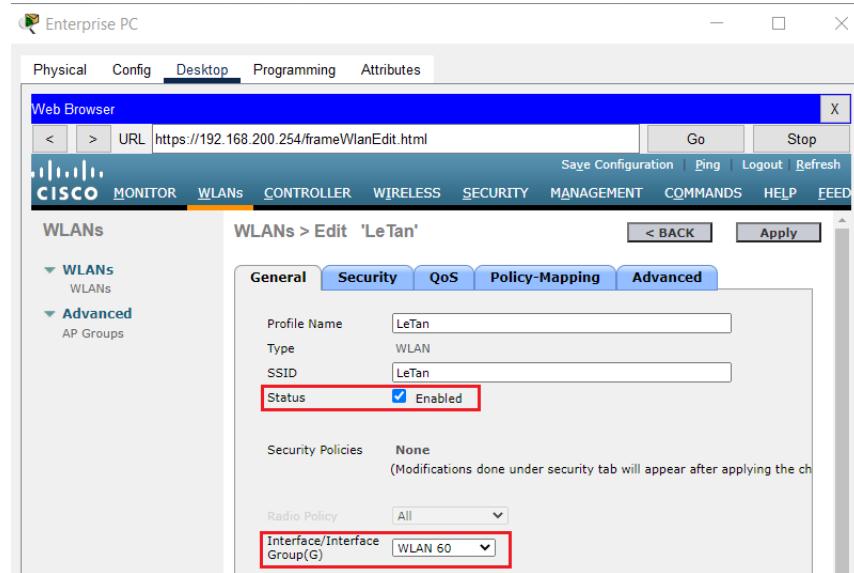
Hình 3. 30: Giao diện các thao tác tạo mạng WLAN 6.

+ Điền thông tin profile name, SSID, ID. Chọn Apply.



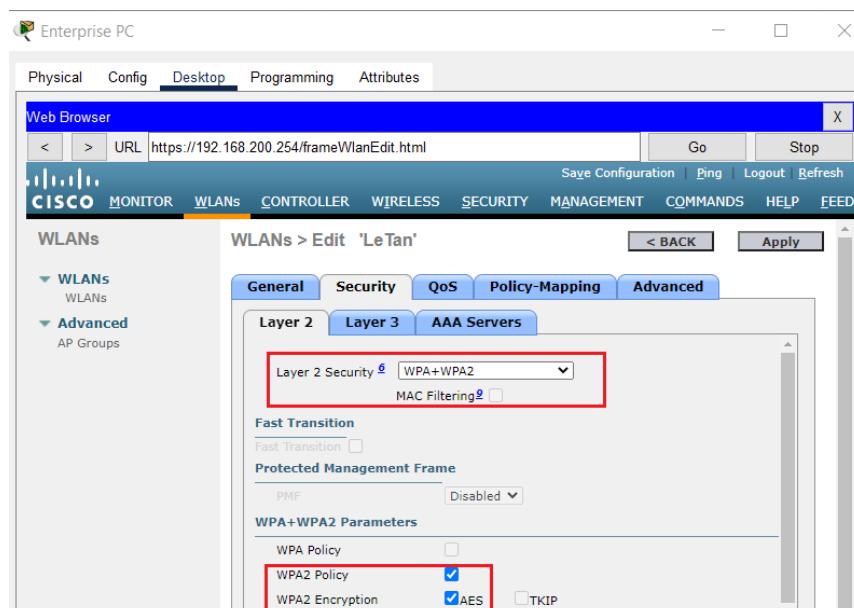
Hình 3. 31: Giao diện cấu hình thông tin cho WLAN 6.

+ Ở tab General, Bật **Enable** cho status, Interface/Interfaces Group
chọn **VLAN 60**.



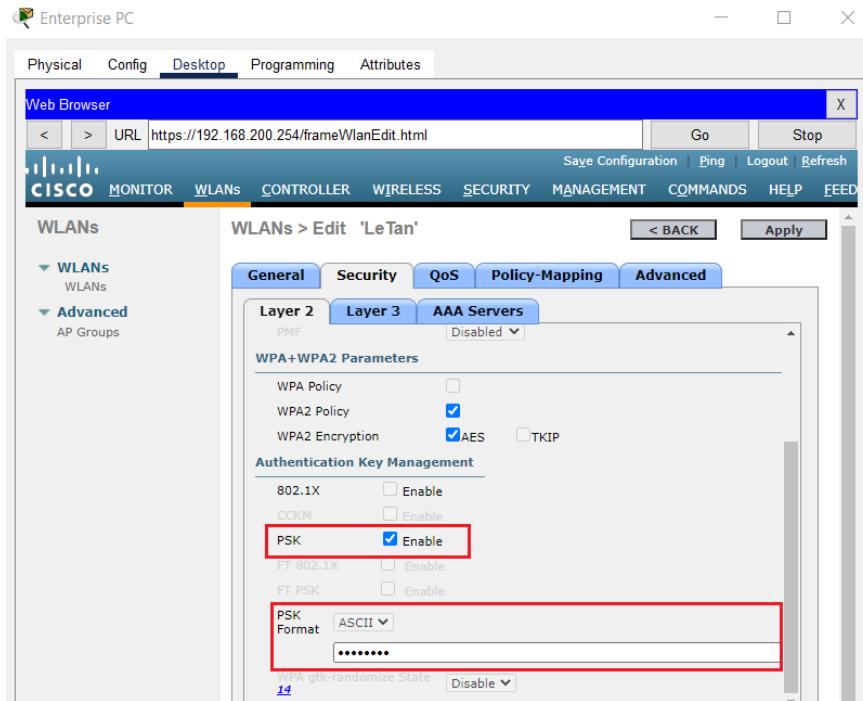
Hình 3. 32: Giao diện cấu hình thông tin ở tab General cho WLAN 6.

+ Chọn tab Security, ở Layer 2 chọn **WPA + WPA2**, tích chọn **WPA2 Policy**.



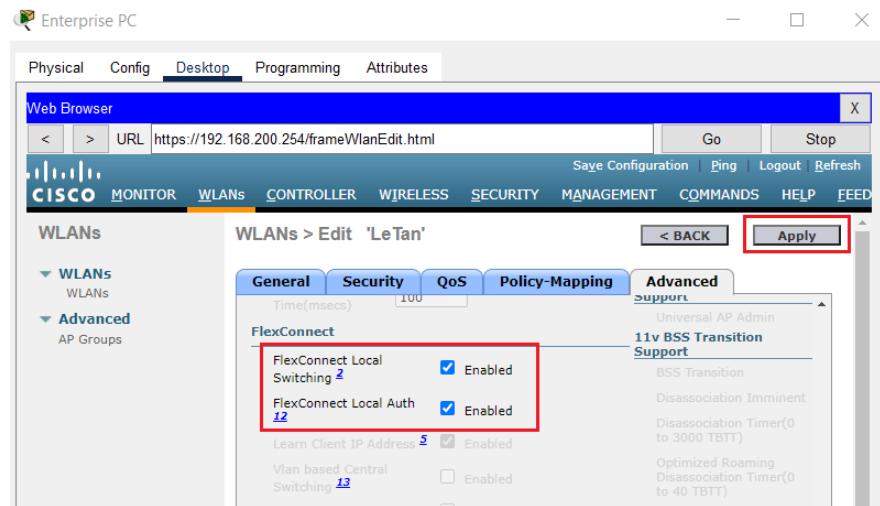
Hình 3. 33: Giao diện cấu hình Security cho Layer 2 cho WLAN 6.

+ Kéo xuống Authentication Key Management, Tích chọn **PSK**, và điền mật khẩu **Cisco123** cho PSK Format.



Hình 3. 34: Giao diện cấu hình Authentication Key Management ở Layer 2 cho WLAN 6.

+ Chọn tab Advanced, kéo xuống FlexConnect, tích chọn **FlexConnect Local Switching** và **FlexConnect Local Auth**. Chọn Apply.



Hình 3. 35: Giao diện cấu hình Advanced cho WLAN 6.

Bước 2: Tạo WLAN 1, 2, 3, 4, 5 cấu hình Security: 802.1x – WPA2 Enterprise

Profile Name: **PhongHop, GiamDoc, KinhDoanh, Marketing, TaiChinh**

WLAN SSID: **PhongHop, GiamDoc, KinhDoanh, Marketing, TaiChinh**

Interface: **WLAN 1/ 2/ 3/ 4/ 5**

ID: **1/ 2/ 3/ 4/ 5**

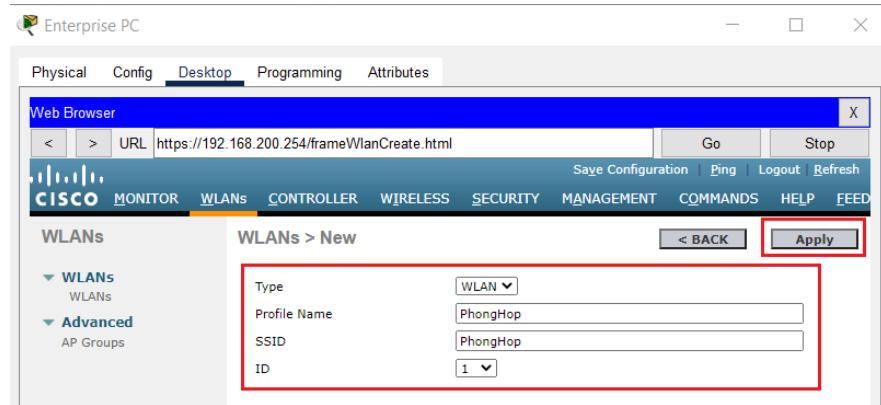
Security: **802.1x - WPA2-Enterprise**

Cấu hình mạng WLAN sử dụng RADIUS Server để xác thực.

+ Chọn WLANS, chọn Go để tạo.

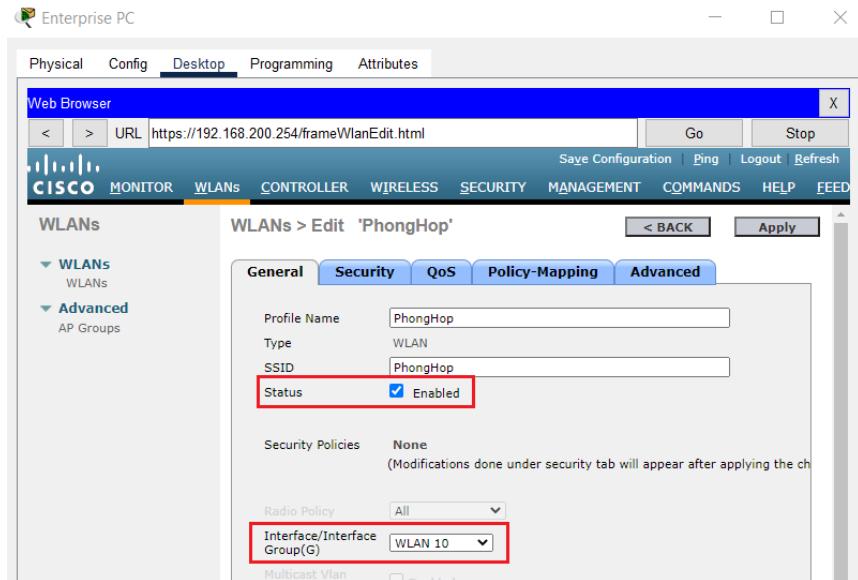


Hình 3. 36: Giao diện các thao tác tạo mạng WLAN 1.



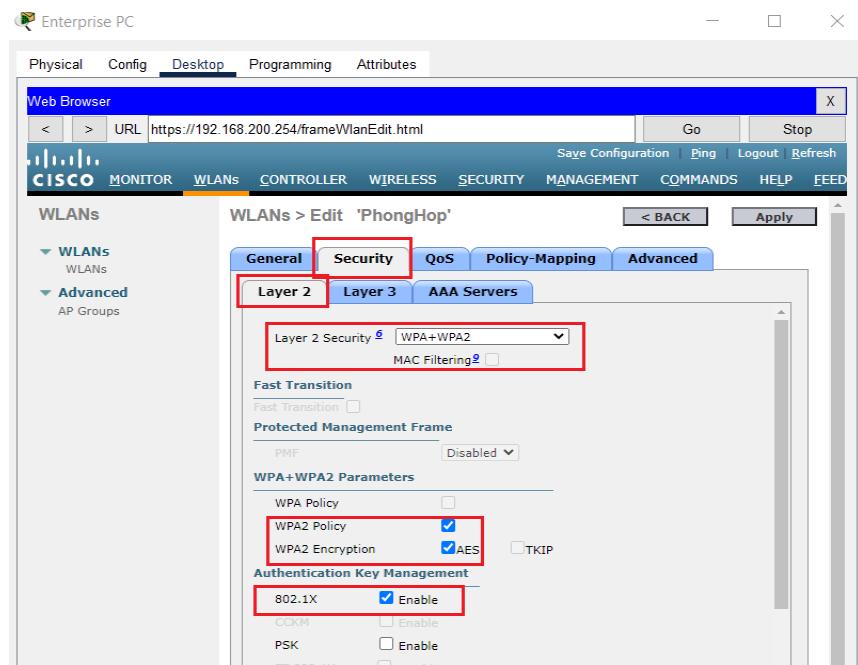
Hình 3. 37: Giao diện cấu hình thông tin cho WLAN 1.

+ Điền thông tin profile name, SSID, ID. Chọn Apply.



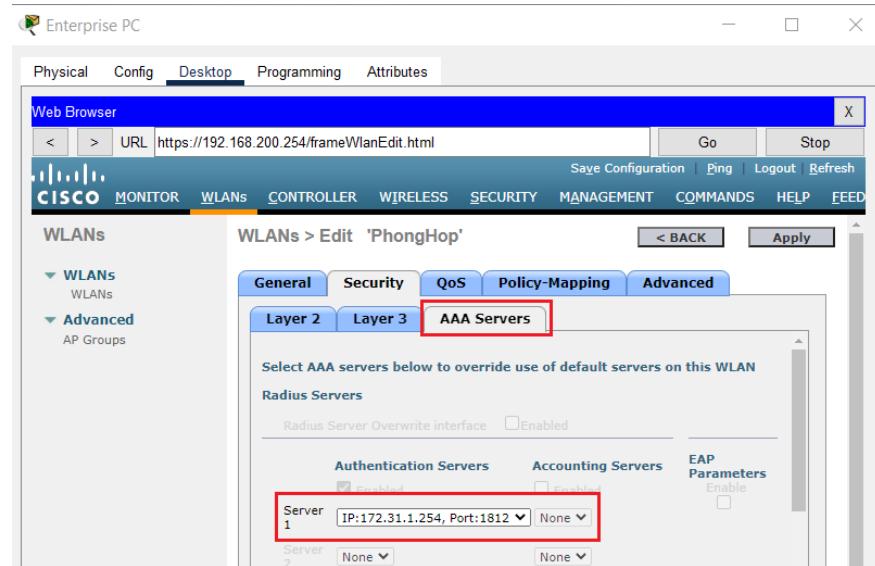
Hình 3. 38: Giao diện cấu hình thông tin ở tab General cho WLAN 1.

+ Chọn tab Security, ở Layer 2 chọn **WPA + WPA2**, tích chọn **WPA2 Policy** và **802.1X**.



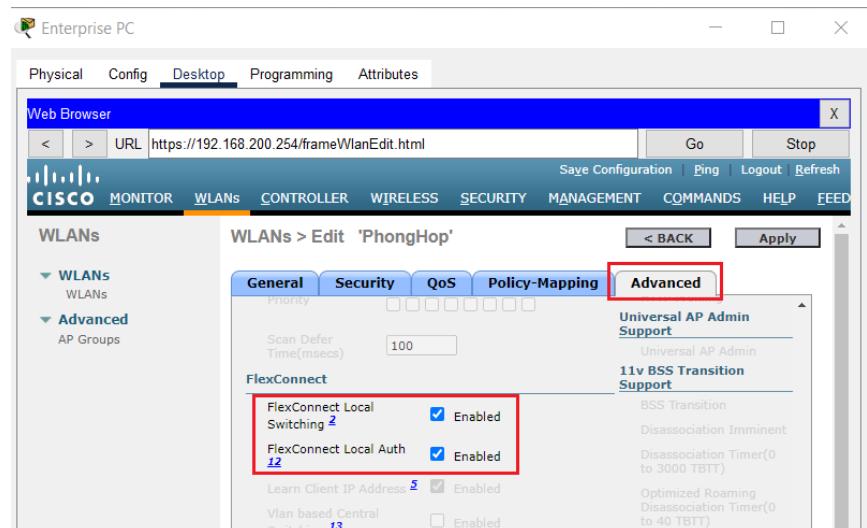
Hình 3. 39: Giao diện cấu hình Security cho Layer 2 cho WLAN 1.

+ Qua AAA Servers, ở Server 1 chọn IP: 172.31.1.254, Port: 1812.



Hình 3. 40: Giao diện cấu hình Secutity cho AAA Servers cho WLAN 1.

+ Chọn tab Advanced, kéo xuống FlexConnect, tích chọn **FlexConnect Local Switching** và **FlexConnect Local Auth**. Chọn Apply.



Hình 3. 41: Giao diện cấu hình Advanced cho WLAN 1.

+ Làm tương tự theo WLAN 1, chúng ta sẽ tạo ra các mạng WLAN 2, 3, 4, 5.

WLAN ID	Type	Profile Name	WLAN SSID
1	WLAN	PhongHop	PhongHop
2	WLAN	GiamDoc	GiamDoc
3	WLAN	KinhDoanh	KinhDoanh
4	WLAN	Marketing	Marketing
5	WLAN	TaiChinh	TaiChinh
6	WLAN	LeTan	LeTan

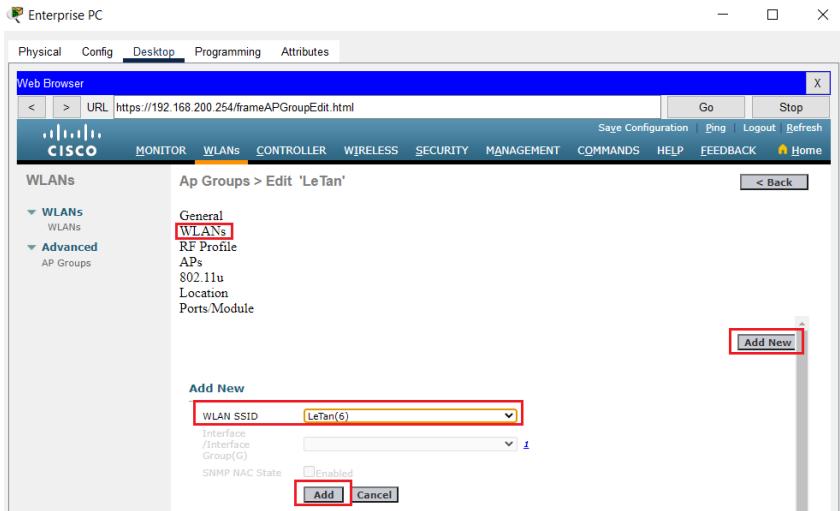
Hình 3. 42: Giao diện cấu hình thành công tạo các WLAN 1, 2, 3, 4, 5, 6.

3.2.7.5 Tạo AP Group

Bước 1: Vào WLANs > chọn AP Groups > chọn Add Group. Ở AP Group Name điền LeTan.

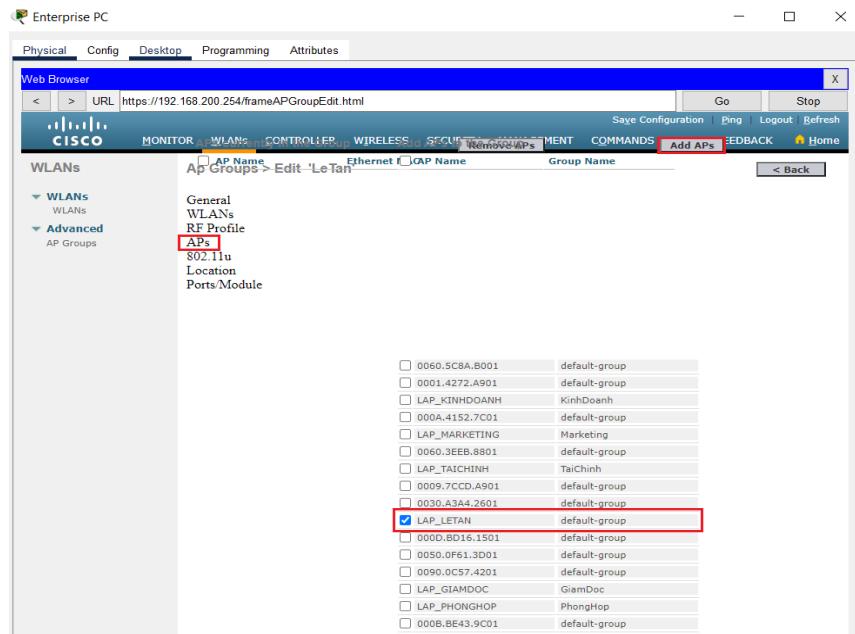
Hình 3. 43: Giao diện các thao tác tạo AP Groups cho phòng lễ tân

Bước 2: Vào phần WLANs, chọn Add New. Ở WLAN SSID chọn LeTan. Chọn Add để thêm.



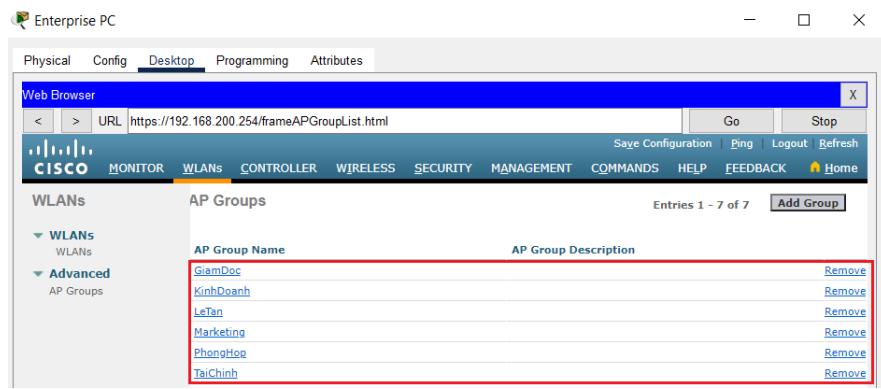
Hình 3. 44: Giao diện chọn cấu hình WLANs cho thiết bị Access Point phòng lẽ tân.

Bước 3: Vào phần APs, tích chọn AP _ LETAN. Ấn Add APs để thiết bị Access Point ở phòng lẽ tân sẽ cho phép truy cập mạng lẽ tân.



Hình 3. 45: Giao diện cấu hình APs cho thiết bị Access Point phòng lẽ tân

Bước 4: Đổi với các AP Group cho các phòng giám đốc, kinh doanh, marketing, tài chính làm tương tự như các bước trên tạo cho phòng lẽ tân.



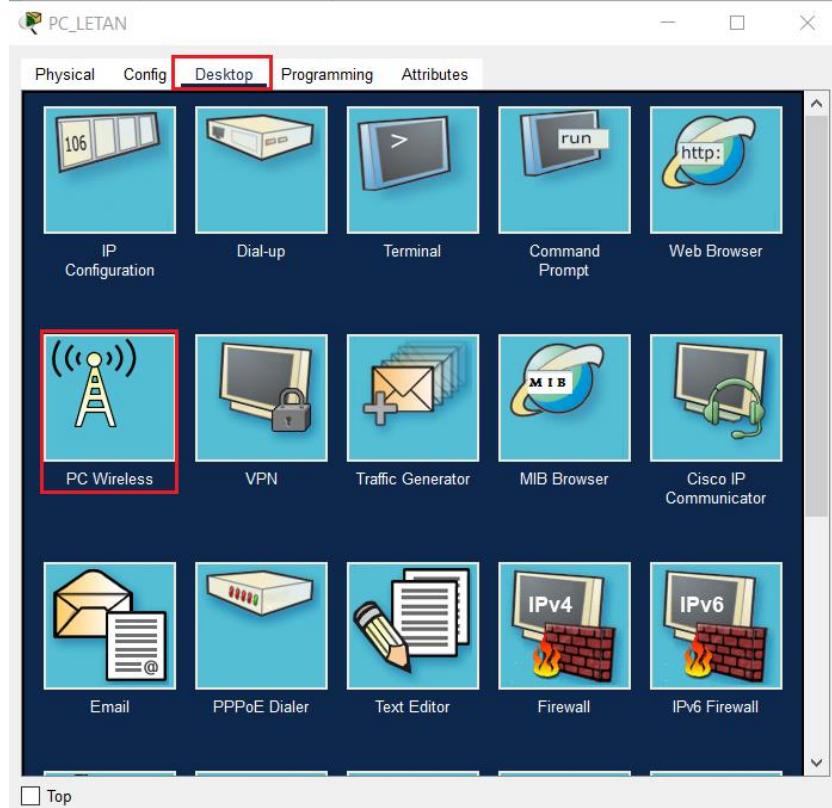
Hình 3. 46: Giao diện sau khi tạo thành công các AP Groups cho các phòng.

3.2.8 *Kết nối các thiết bị các nhân ở doanh nghiệp THL với mạng WLAN*

3.2.8.1 Phòng Lê Tân

Bước 1: Đổi với PC_LETAN.

+ Mở thiết bị PC_LETAN, chọn tab Desktop, mở ứng dụng PC Wireless.



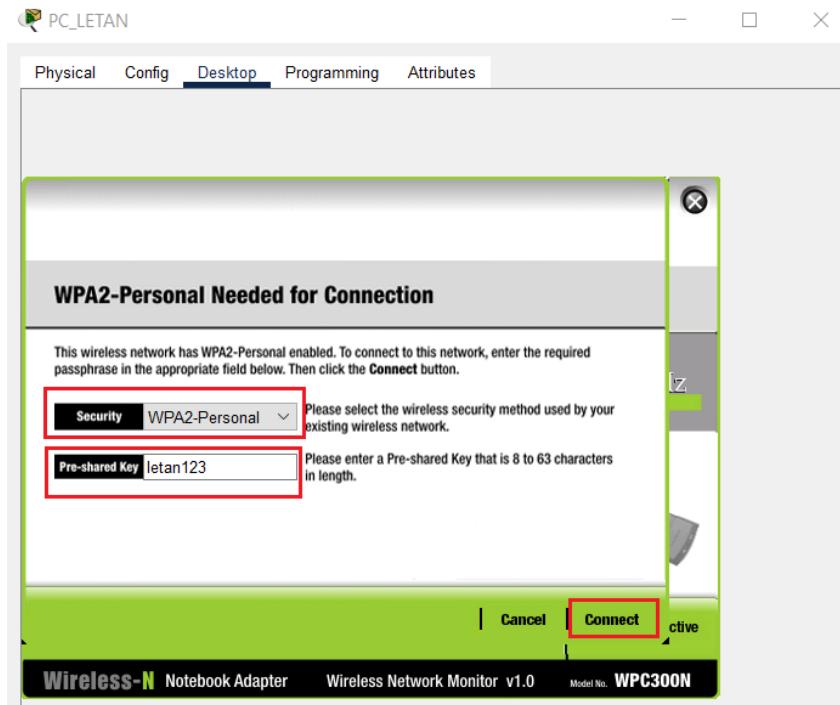
Hình 3. 47: Giao diện các bước vào PC Wireless của PC _LETAN.

+ Chọn tab Connect, ấn Refresh, chọn **LeTan** rồi chọn Connect.



Hình 3. 48: Giao diện chọn LeTan để kết nối cho PC_LETAN.

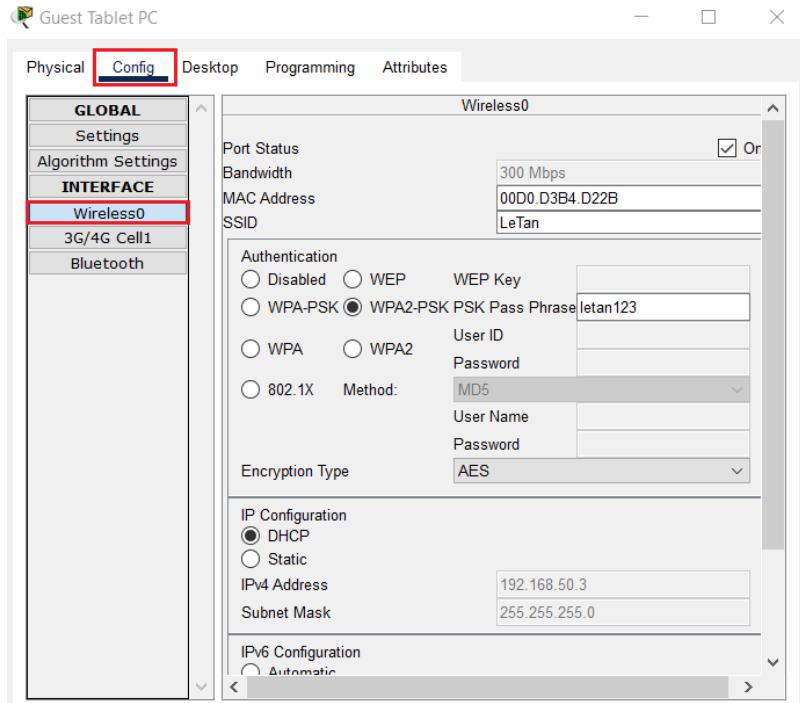
+ Chọn **WPA2-Personal** ở Security, điền mật khẩu **Cisco123** vào Pre-shared Key và chọn Connect.



Hình 3. 49: Giao diện chọn Security và điền mật khẩu kết nối cho PC _LETAN.

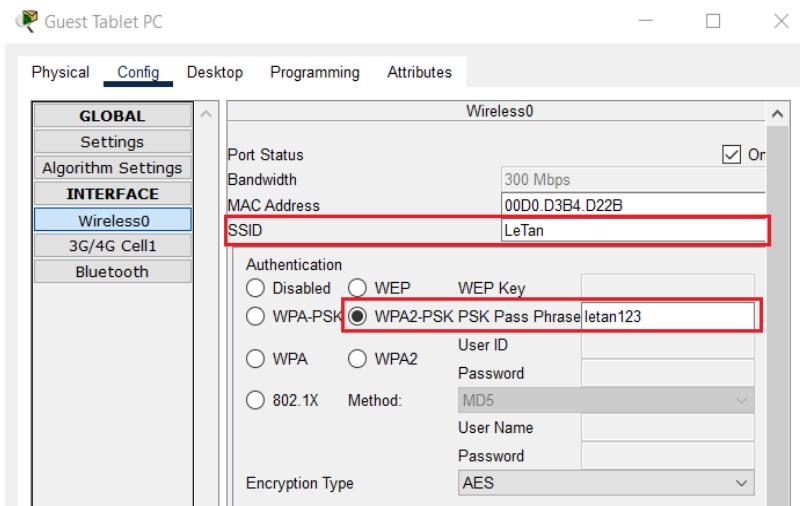
Bước 2: Đổi với Guest Tablet PC.

- + Vào Guest Tablet PC chọn Config, ở phần Interface chọn Wireless0.



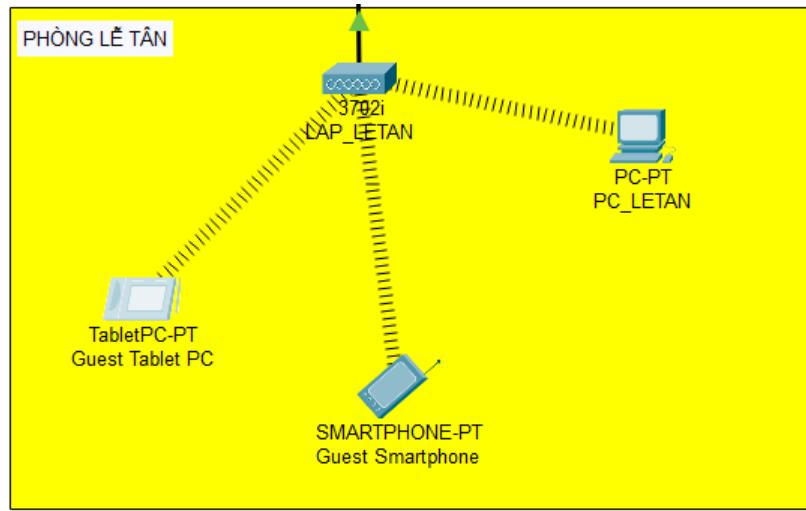
Hình 3. 50: Giao diện các thao tác vào Wireless0 của Guest Tablet PC.

+ Điền SSID, chọn **WPA2-PSK**, điền mật khẩu vào PSK Pass Phrase. Sau đó tắt Guest Tablet PC.



Hình 3. 51: Giao diện cấu hình thông tin để kết nối cho Guest Tablet PC.

Bước 3: Đổi với Guest Smartphone làm tương tự như Guest Tablet PC.

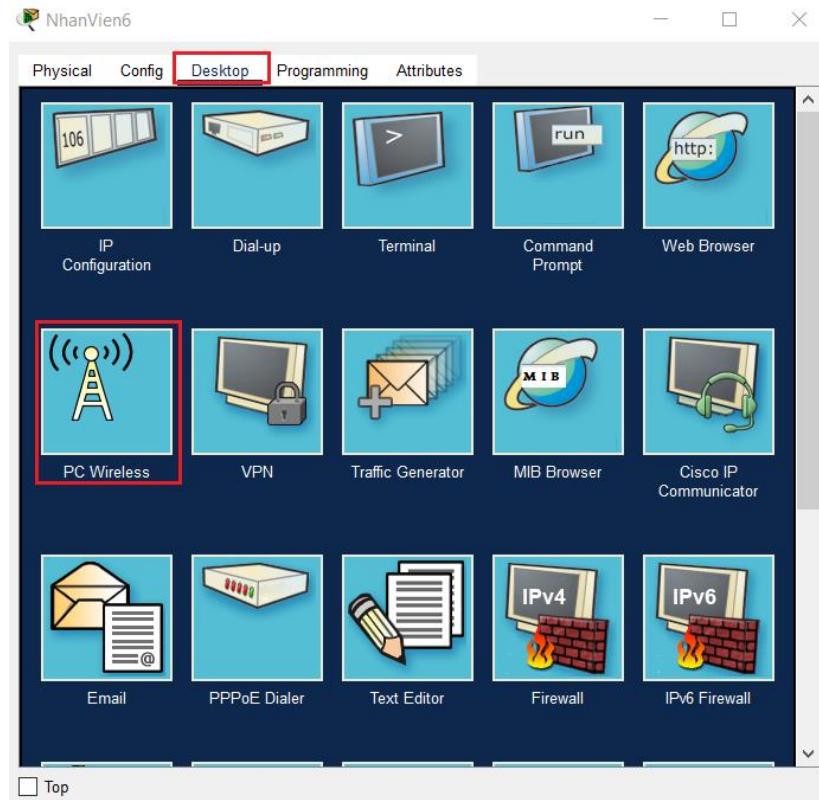


Hình 3. 52: Kết quả sau khi kết nối thành công các thiết bị cá nhân ở phòng lễ tân.

3.2.8.2 Phòng Họp

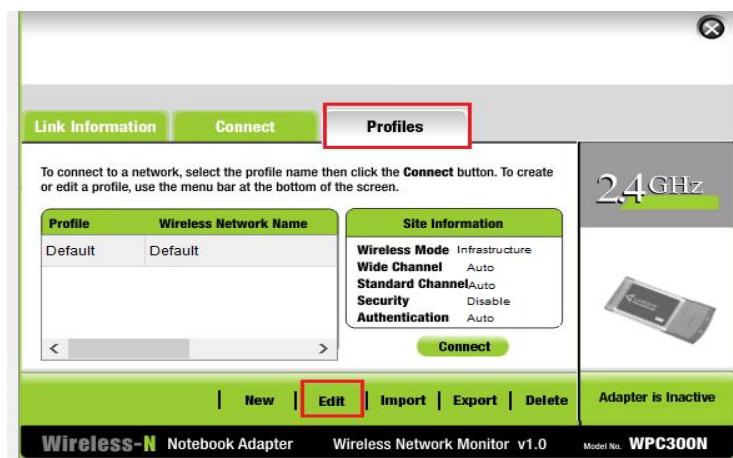
Bước 1: Đổi với laptop NhanVien6.

- + Mở thiết bị laptop NhanVien6, chọn tab Desktop, mở ứng dụng PC Wireless.



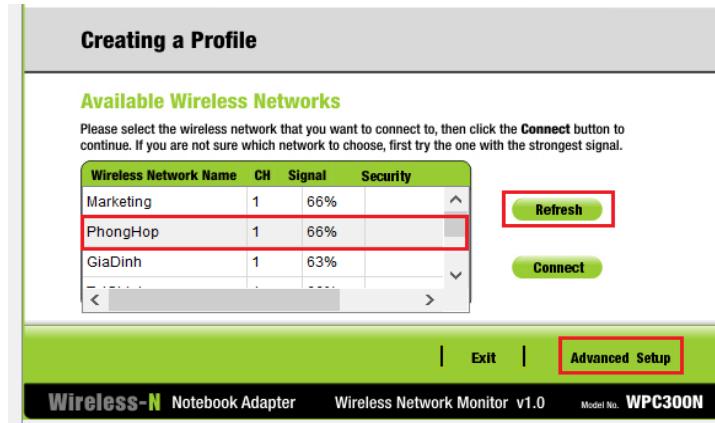
Hình 3. 53: Giao diện các bước vào PC Wireless của laptop NhanVien6

+ Chọn tab Profiles, chọn Edit.



Hình 3. 54: Giao diện chọn Edit để cấu hình kết nối cho laptop NhanVien6.

+ Ấn Refresh, Chọn **PhongHop**, chọn Advanced Setup.



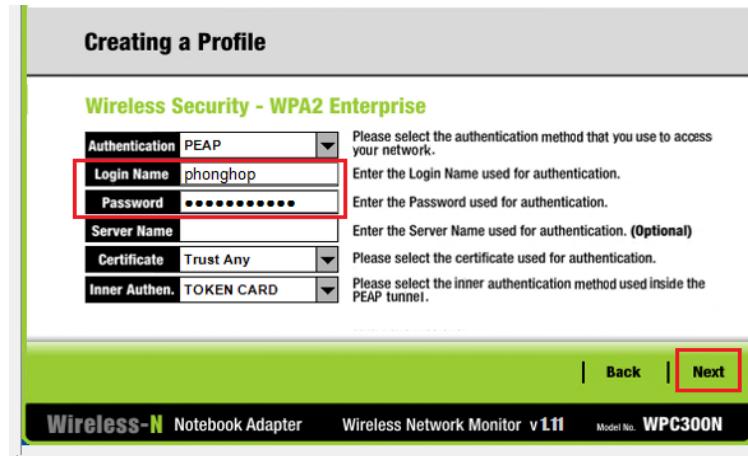
Hình 3. 55: Giao diện chọn PhongHop để kết nối cho laptop NhanVien6.

+ Chọn Next cho đến Wireless Security. Ở Security chọn **WPA2-Enterprise**. Chọn Next.



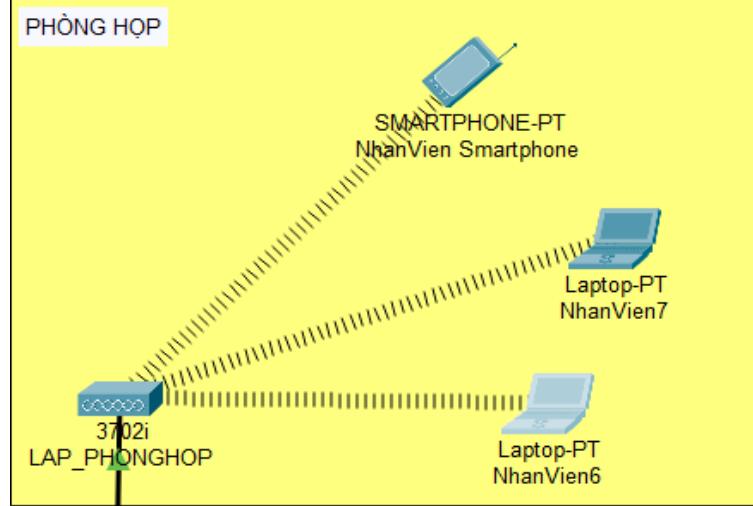
Hình 3. 56: Giao diện chọn Security cho laptop NhanVien6.

+ Điền Login Name và Password rồi chọn Next. Sau đó chọn Save và chọn Connect to Nextwork.



Hình 3. 57: Giao diện điền thông tin để kết nối cho laptop NhanVien6.

Bước 2: Đối với laptop NhanVien7 làm tương tự như laptop NhanVien6 ở bước 1. Đối với NhanVien Smartphone làm tương tự như Guest Tablet PC ở phòng lễ tân nhưng Authentication chọn WPA2 và điền User ID và Password.

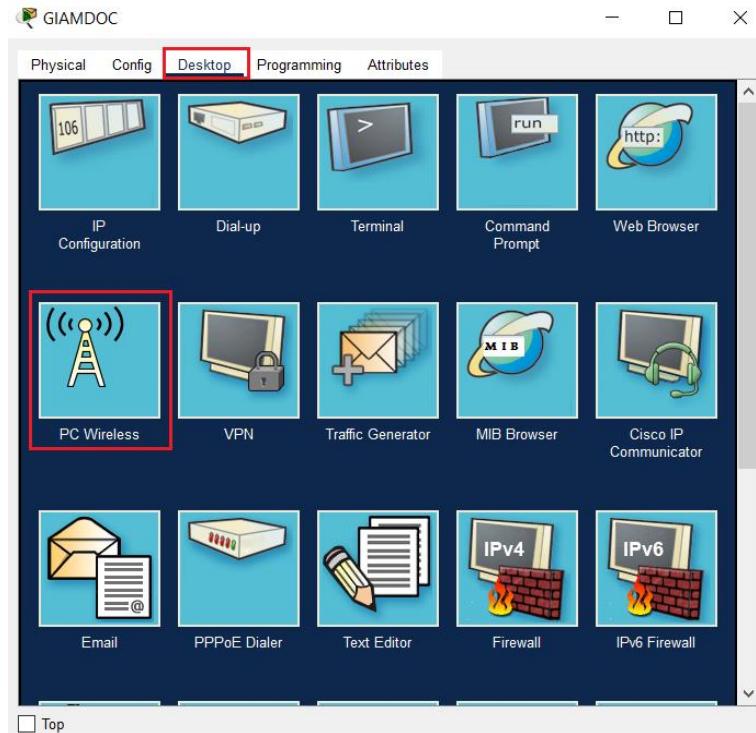


Hình 3. 58: Kết quả sau khi kết nối thành công các thiết bị cá nhân ở phòng họp.

3.2.8.3 Phòng Giám Đốc

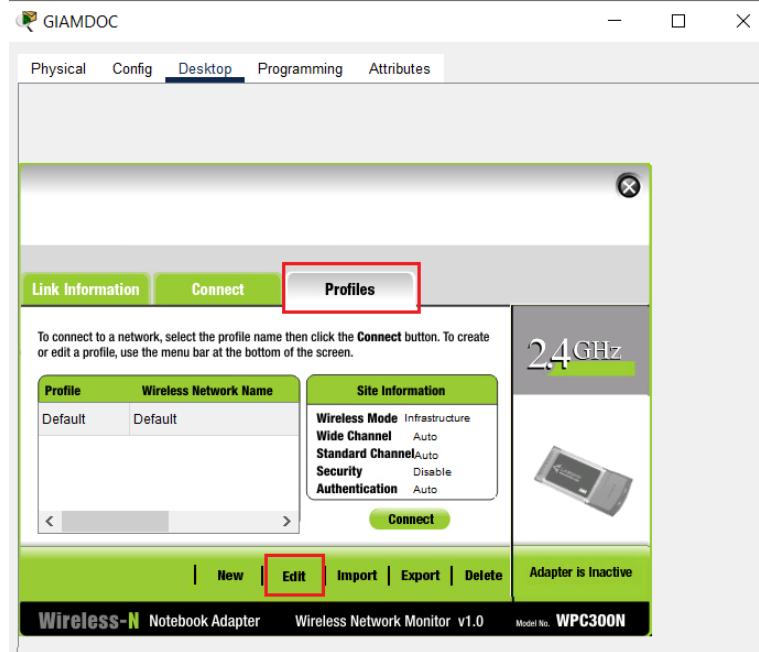
Bước 1: Đối với laptop GIAMDOC.

- + Mở thiết bị laptop GIAMDOC, chọn tab Desktop, mở ứng dụng PC Wireless.



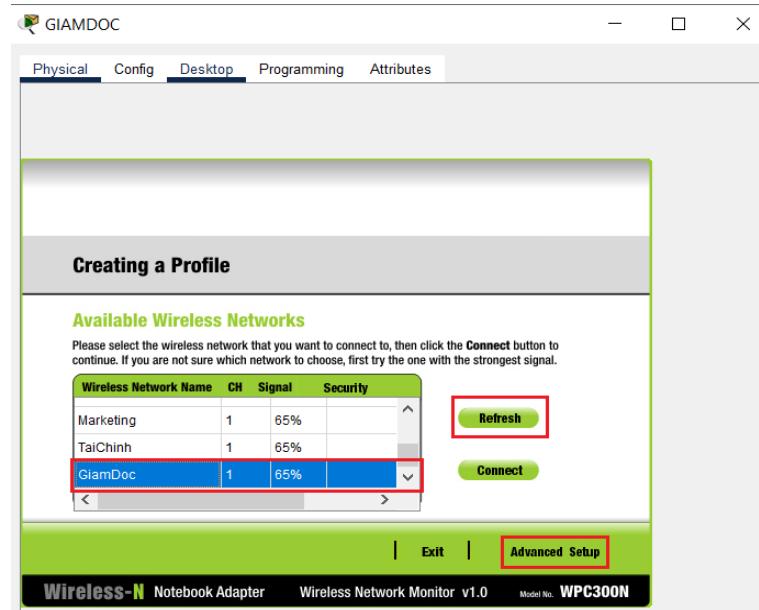
Hình 3. 59: Giao diện các bước vào PC Wireless của laptop GIAMDOC.

- + Chọn tab Profiles, chọn Edit.



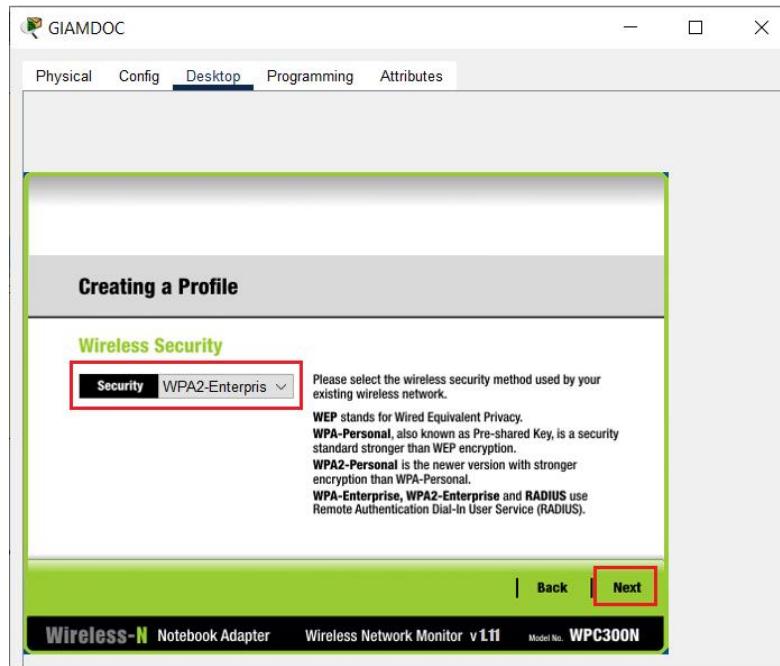
Hình 3. 60: Giao diện chọn Edit để cấu hình kết nối cho laptop GIAMDOC.

+ Án Refresh, Chọn **GiamDoc**, chọn Advanced Setup.



Hình 3. 61: Giao diện chọn GiamDoc để kết nối cho laptop GIAMDOC.

+ Chọn Next cho đến Wireless Security. Ở Security chọn **WPA2-Enterprise**. Chọn Next.



Hình 3. 62: Giao diện chọn Security cho laptop GIAMDOC.

+ Điền Login Name và Password rồi chọn Next. Sau đó chọn Save và chọn Connect to Nextwork.

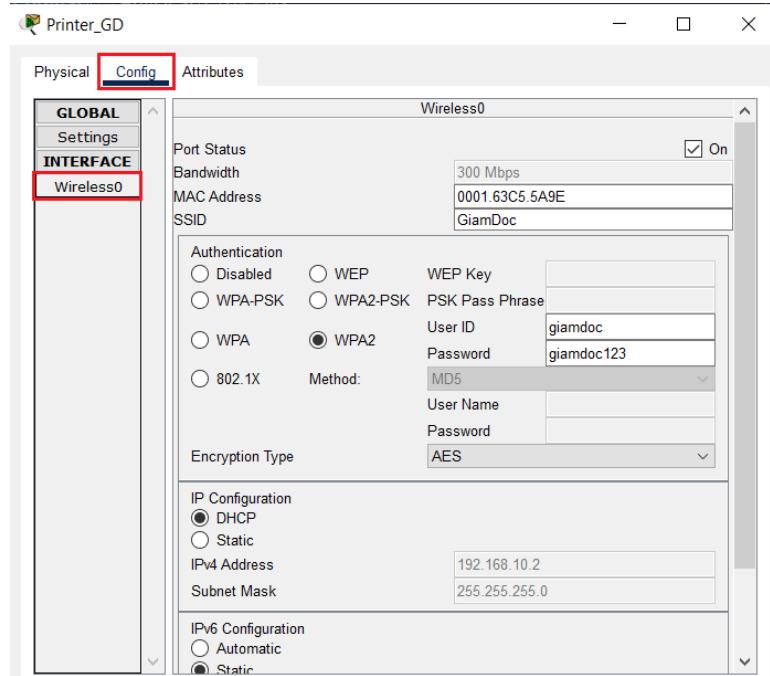


Hình 3. 63: Giao diện điền thông tin để kết nối cho laptop GIAMDOC.

Bước 2: Đổi với laptop THUKY làm tương tự như laptop GIAMDOC.

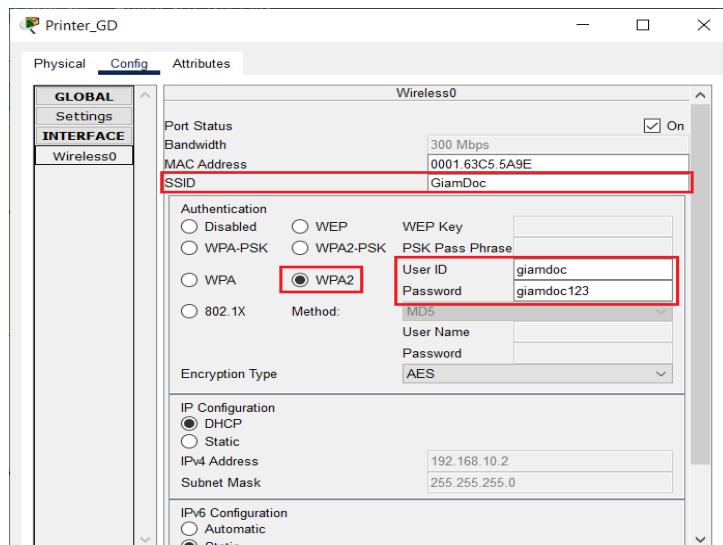
Bước 3: Đổi với máy in Printer_GD.

- + Vào máy in Printer_GD chọn Config, ở phần Interface chọn Wireless0.

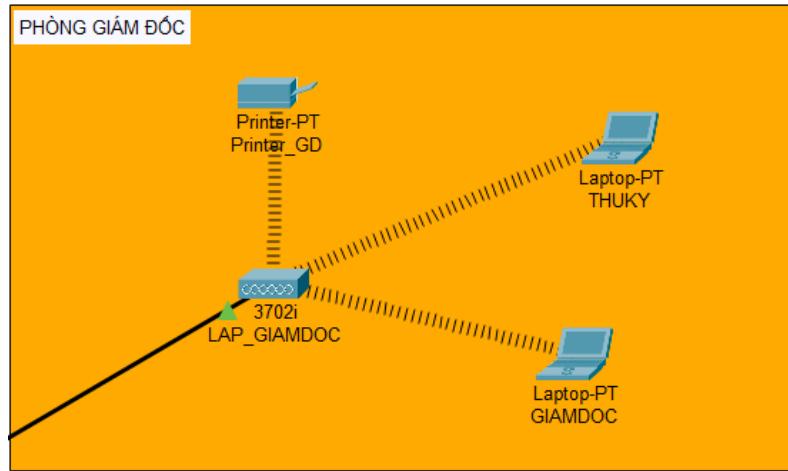


Hình 3. 64: Giao diện các thao tác vào Wireless0 của laptop GIAMDOC.

+ Điền SSID, chọn **WPA2**, điền mật khẩu vào PSK Pass Phrase. máy in Printer_GD.



Hình 3. 65: Giao diện cấu hình thông tin để kết nối cho laptop GIAMDOC

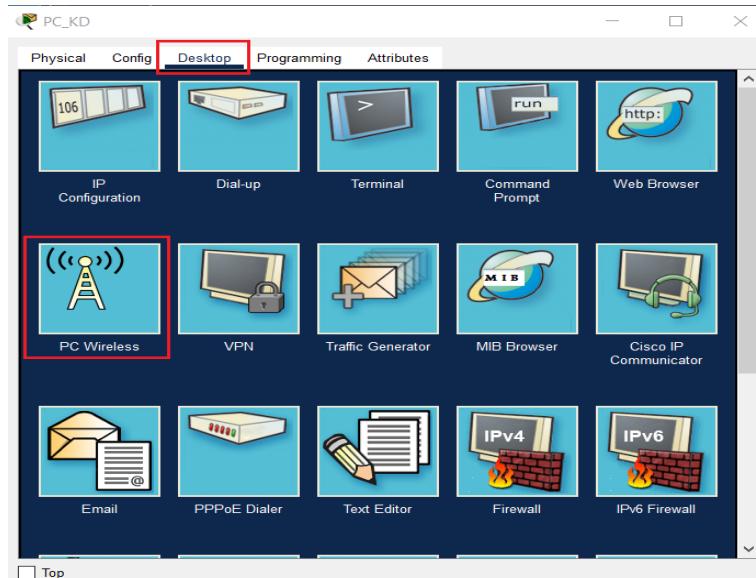


Hình 3. 66: Kết quả sau khi kết nối thành công các thiết bị cá nhân ở phòng giám đốc.

3.2.8.4 Phòng Kinh Doanh

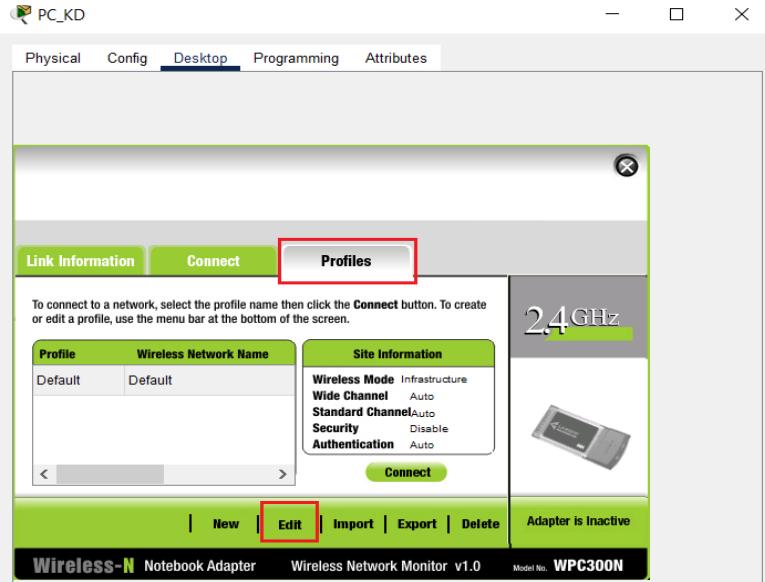
Bước 1: Đổi với PC_KD.

+ Mở thiết bị PC_KD, chọn tab Desktop, mở ứng dụng PC Wireless.



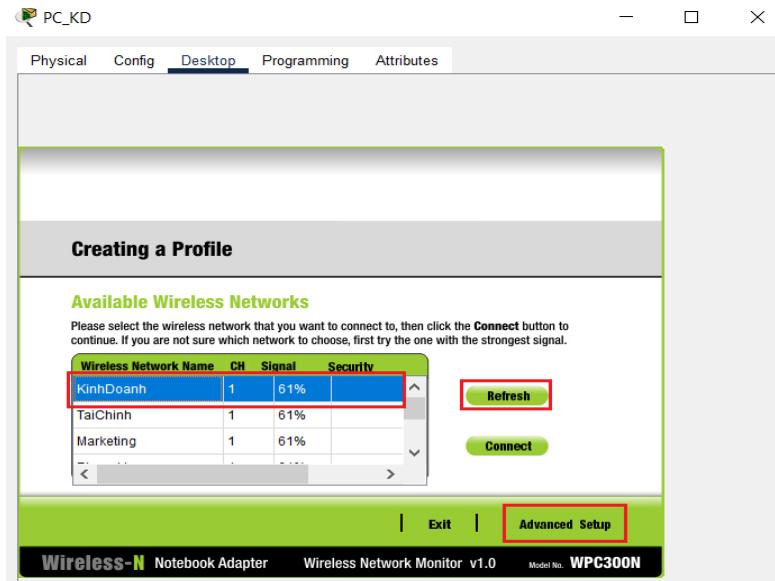
Hình 3. 67: Giao diện các bước vào PC Wireless của laptop PC_KD.

+ Chọn tab Profiles, chọn Edit.



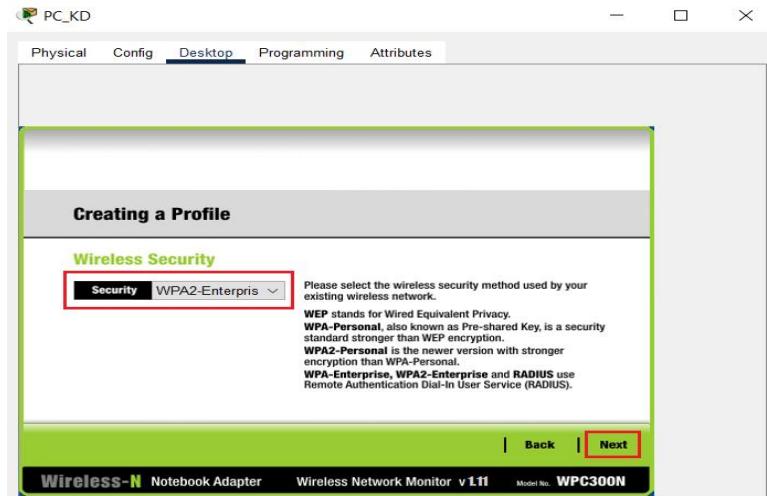
Hình 3. 68: Giao diện chọn Edit để cấu hình kết nối cho PC_KD.

+ Án Refresh, Chọn **KinhDoanh**, chọn Advanced Setup.



Hình 3. 69: Giao diện chọn KinhDoanh để kết nối cho PC_KD.

+ Chọn Next cho đến Wireless Security. Ở Security chọn **WPA2-Enterprise**. Chọn Next.



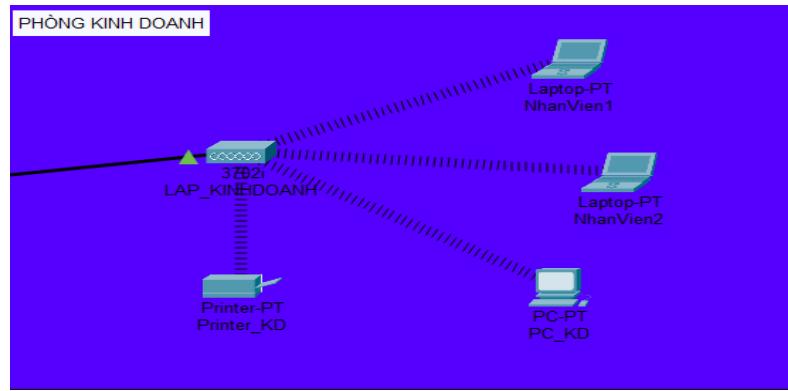
Hình 3. 70: Giao diện chọn Security cho PC_KD.

+ Điền Login Name và Password rồi chọn Next. Sau đó chọn Save và chọn Connect to Nextwork.



Hình 3. 71: Giao diện điền thông tin để kết nối cho PC_KD.

Bước 2: Đổi với laptop NhanVien1, NhanVien2 làm tương tự như PC_KD. Đổi với máy in Printer_KD làm tương tự như máy tin Printer_GD ở phòng giám đốc.

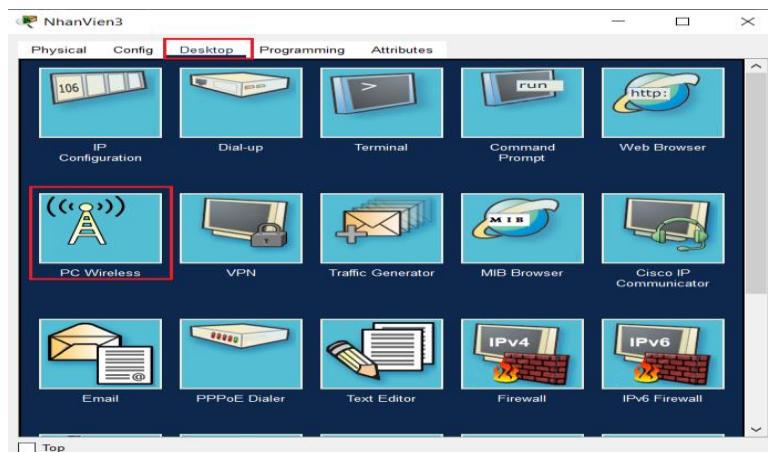


Hình 3. 72: Kết quả sau khi kết nối thành công các thiết bị cá nhân ở phòng kinh doanh.

3.2.8.5 Phòng Marketing

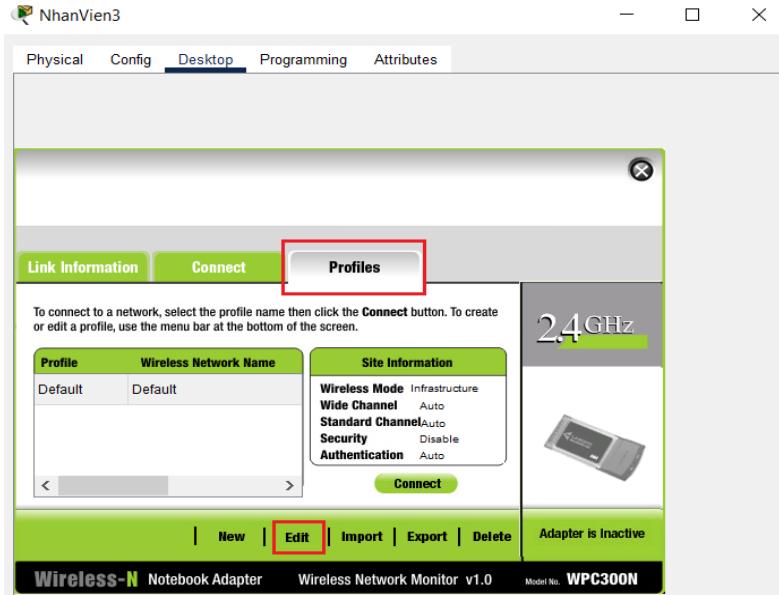
Bước 1: Đổi với laptop NhanVien 3.

+ Mở thiết bị laptop NhanVien 3, chọn tab Desktop, mở ứng dụng PC Wireless.



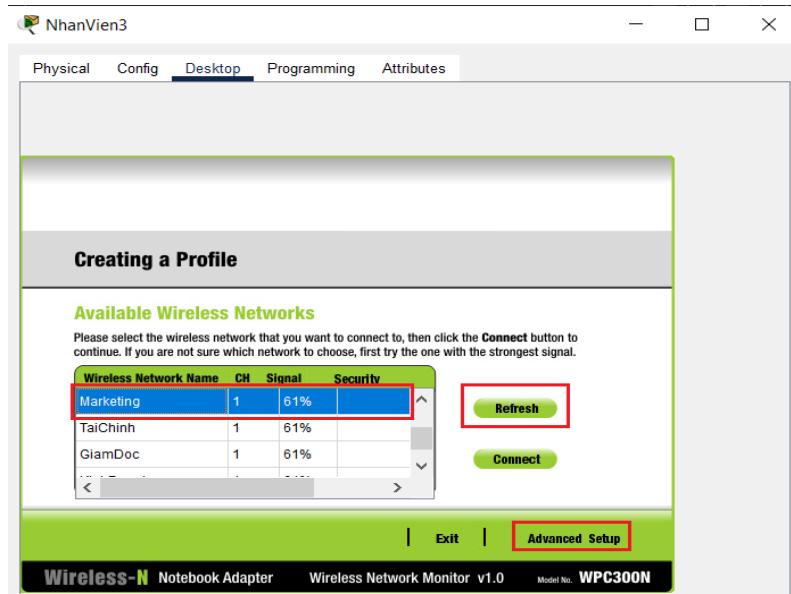
Hình 3. 73: Giao diện các bước vào PC Wireless của laptop NhanVien 3.

+ Chọn tab Profiles, chọn Edit.



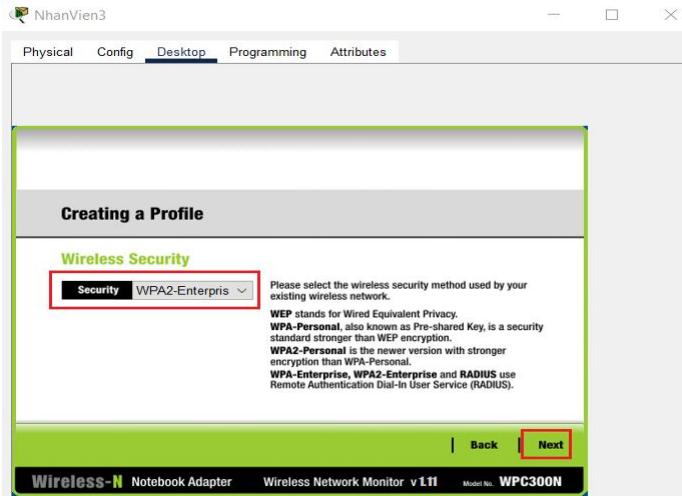
Hình 3. 74: Giao diện chọn Edit để cấu hình kết nối cho laptop NhanVien 3.

+ Án Refresh, Chọn Marketing, chọn Advanced Setup.



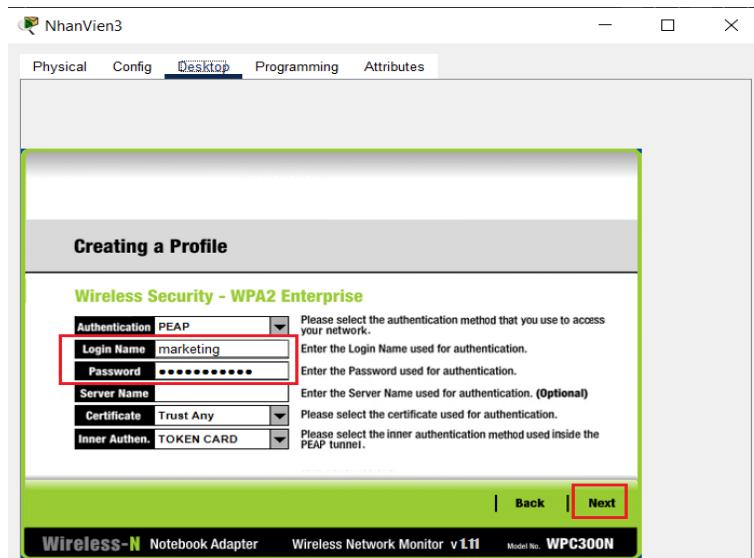
Hình 3. 75: Giao diện chọn Marketing để kết nối cho laptop NhanVien 3.

+ Chọn Next cho đến Wireless Security. Ở Security chọn **WPA2-Enterprise**. Chọn Next.



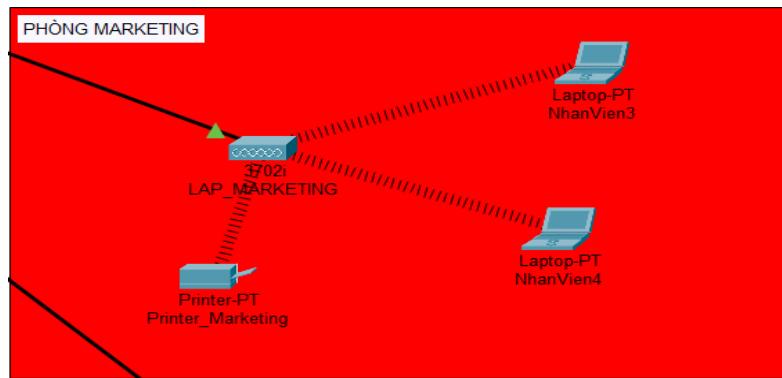
Hình 3. 76: Giao diện chọn Security cho laptop NhanVien 3.

+ Điền Login Name và Password rồi chọn Next. Sau đó chọn Save và chọn Connect to Nextwork.



Hình 3. 77: Giao diện điền thông tin để kết nối cho laptop NhanVien 3.

Bước 2: Đổi với laptop NhanVien4 làm tương tự như laptop NhanVien 3. Đổi với máy in Printer_Marketing làm tương tự như máy tin Printer_GD ở phòng giám đốc.

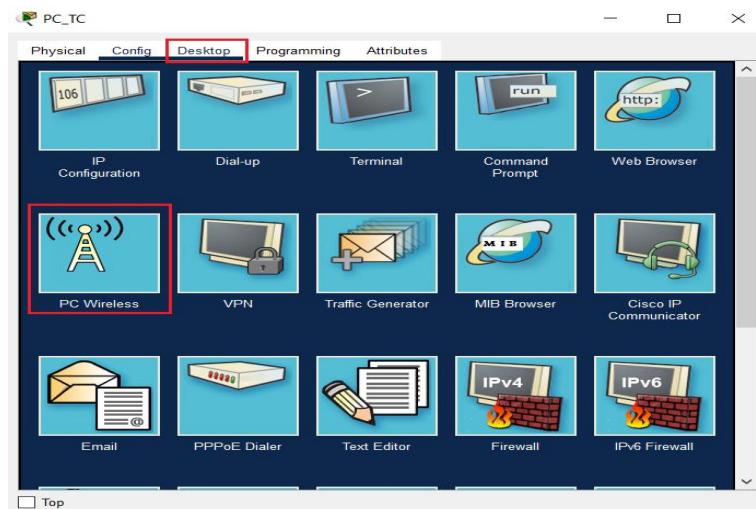


Hình 3. 78: Kết quả sau khi kết nối thành công các thiết bị cá nhân ở phòng marketing.

3.2.8.6 Phòng tài chính

Bước 1: Đổi với PC_TC.

+ Mở thiết bị PC_TC, chọn tab Desktop, mở ứng dụng PC Wireless.



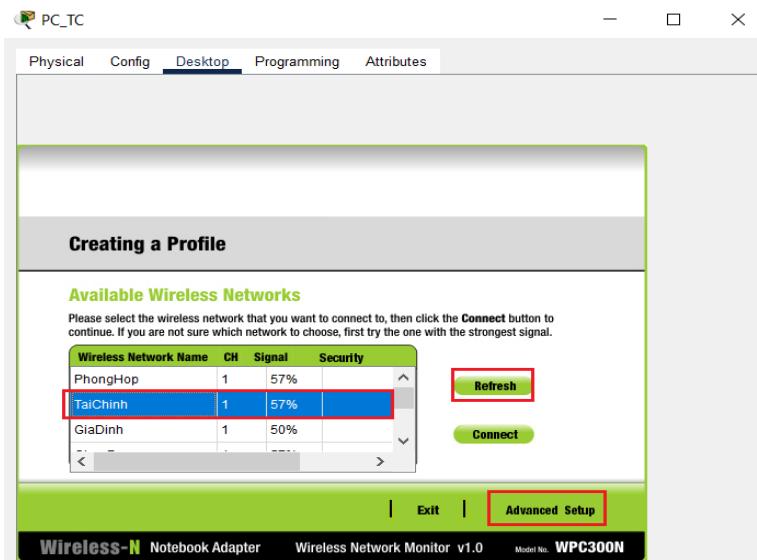
Hình 3. 79: Giao diện các bước vào PC Wireless của PC_TC.

+ Chọn tab Profiles, chọn Edit.



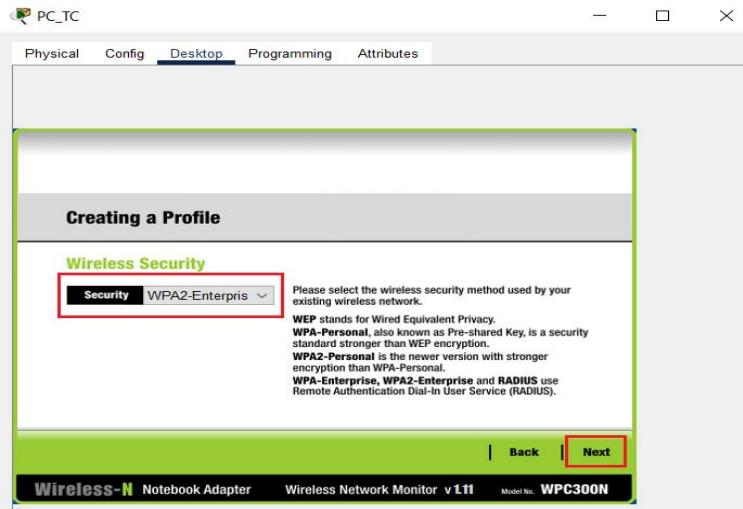
Hình 3. 80: Giao diện chọn Edit để cấu hình kết nối cho PC_TC.

+ Án Refresh, Chọn **TaiChinh**, chọn Advanced Setup.



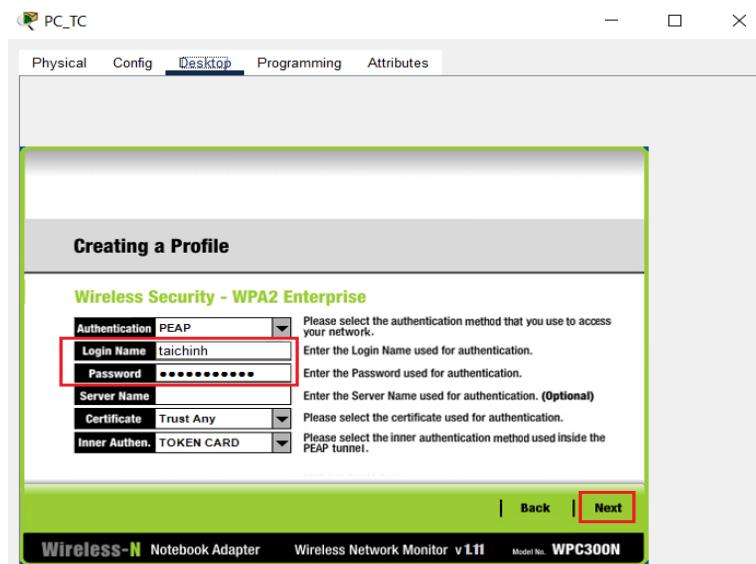
Hình 3. 81: Giao diện chọn TaiChinh để kết nối cho PC_TC.

+ Chọn Next cho đến Wireless Security. Ở Security chọn **WPA2-Enterprise**. Chọn Next.



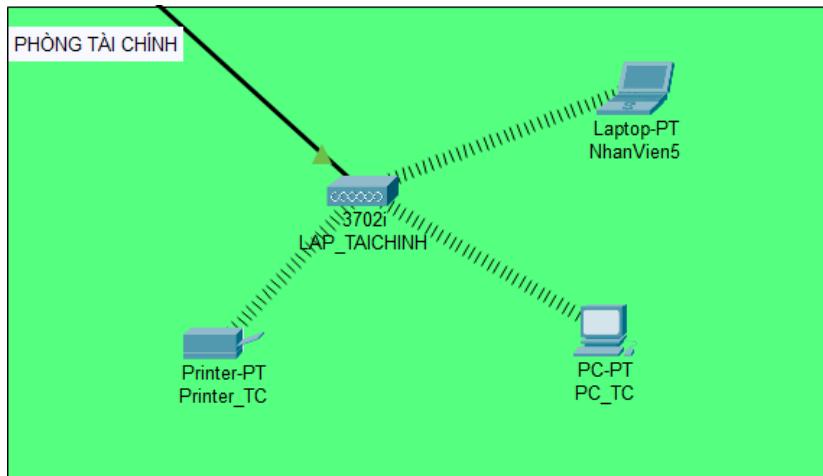
Hình 3. 82: Giao diện chọn Security cho PC_TC.

+ Điền Login Name và Password rồi chọn Next. Sau đó chọn Save và chọn Connect to Nextwork.



Hình 3. 83: Giao diện điền thông tin để kết nối cho PC_TC.

Bước 2: Đổi với laptop NhanVien5 làm tương tự như PC_TC. Đổi với máy in Printer_TC làm tương tự như máy tin Printer_GD ở phòng giám đốc.

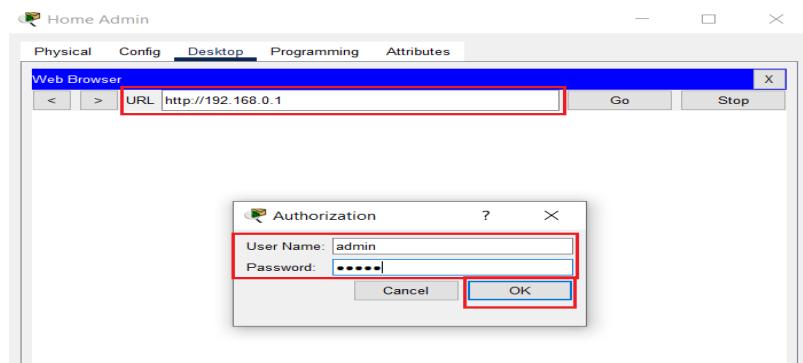


Hình 3. 84: Kết quả sau khi kết nối thành công các thiết bị cá nhân ở phòng tài chính.

3.2.9 Cấu hình thiết bị Home Wireless Router tại nhà.

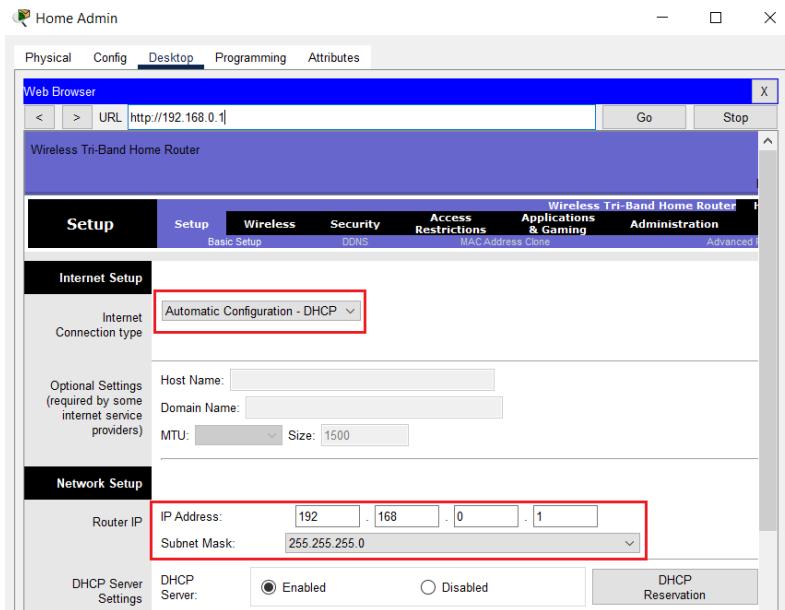
Bước 1: Thay đổi cài đặt DHCP.

- + Vào thiết bị Home Admin, chọn tab Desktop, chọn Web Browser. Đăng nhập vào thiết bị Home Wireless Router bằng địa chỉ url **192.168.0.1**.



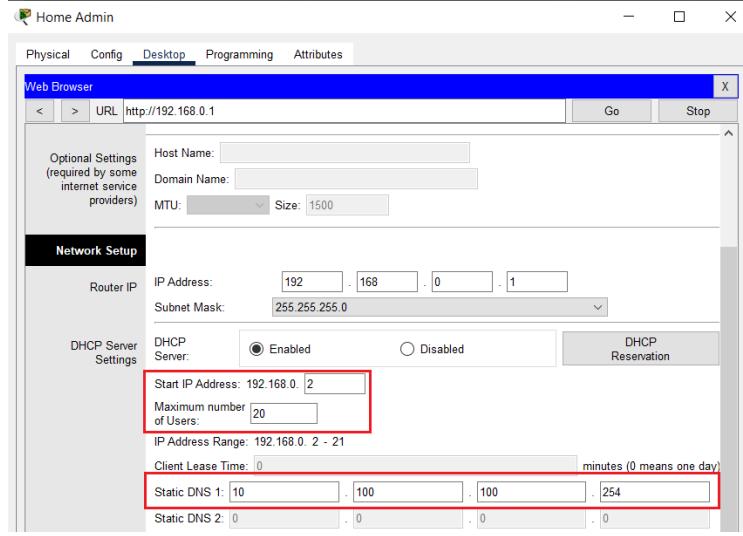
Hình 3. 85: Đăng nhập vào Home Wireless Router.

- + Trong Internet Setup, thay đổi phương pháp địa chỉ IP Internet thành **Automatic Configuration - DHCP** và trong Network Setup, thay đổi địa chỉ IP và Subnet Mask theo bảng địa chỉ.



Hình 3. 86: Thay đổi địa chỉ để phù hợp.

- + Cho phép bộ định tuyến cấp tối đa **20** địa chỉ và cấu hình DHCP server để bắt đầu bằng địa chỉ IP **.2** của mạng LAN. Cấu hình Static DNS server thành địa chỉ trong bảng địa chỉ.

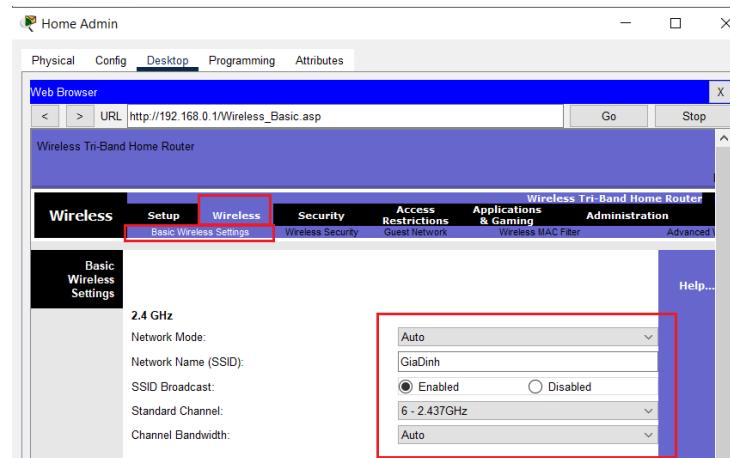


Hình 3. 87: Các địa chỉ cần thiết cho thiết lập.

+ Án **Save Settings** để lưu cấu hình.

Bước 2: Cấu hình mạng LAN không dây.

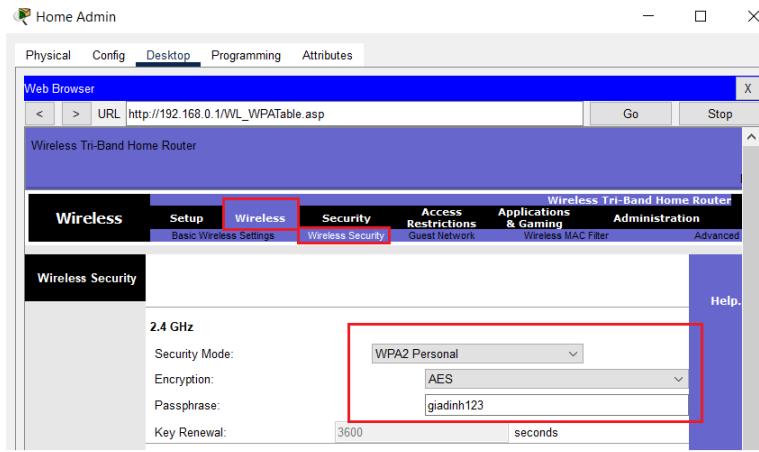
+ Diều hướng đến Wireless > Basic Wireless Settings. Ở tần số 2.4 GHz thay đổi Network Name (SSID) thành **GiaDinh**. Và sử dụng **Channel 6**. Tắt 2 tần số 5 GHz.



Hình 3. 88: Các cài đặt cho Wireless.

Bước 3: Cấu hình bảo mật.

- + Điều hướng đến Wireless > Wireless Security. Trong 2,4 GHz, chọn **WPA2 Personal** cho Chế độ bảo mật. Giữ AES làm mã hóa, nhập **Cisco123** làm mật khẩu.



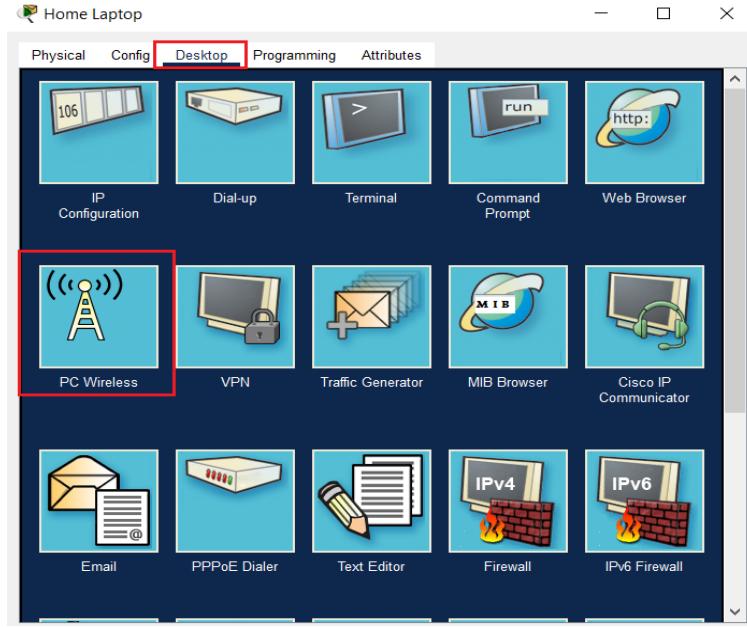
Hình 3. 89: Chọn chế độ bảo mật, mã hóa phù hợp.

- + Án **Save Settings** để lưu cấu hình.

Bước 4: Kết nối thiết bị cá nhân với mạng gia đình.

Đối với Home Laptop.

- + Mở thiết bị Home Laptop, chọn tab Desktop, mở ứng dụng PC Wireless.



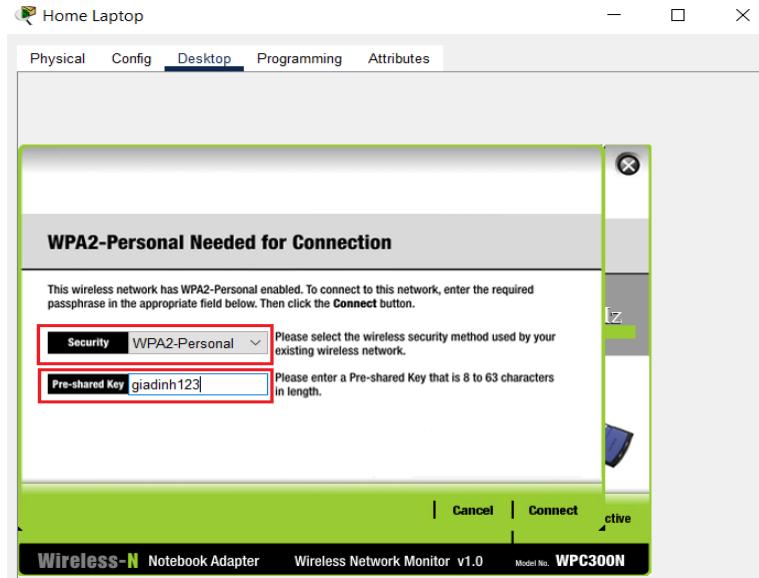
Hình 3. 90: Giao diện các bước vào PC Wireless của Home Laptop.

+ Chọn tab Connect, ấn Refresh, chọn **GiaDinh** rồi chọn Connect.



Hình 3. 91: Giao diện chọn GiaDinh để kết nối cho Home Laptop.

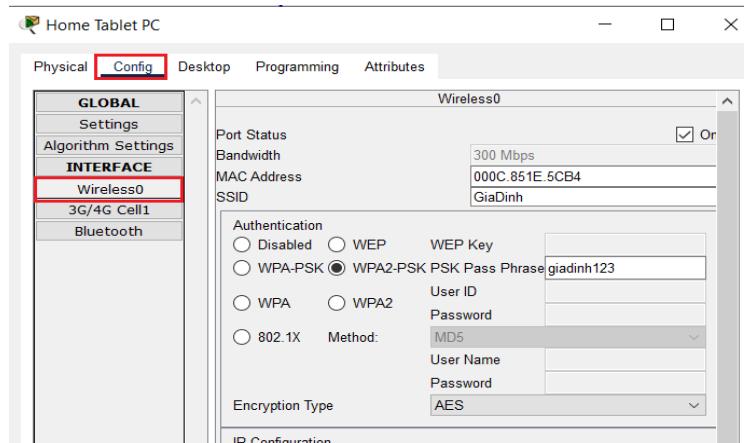
- + Chọn **WPA2-Personal** ở Security, điền mật khẩu **Cisco123** vào Pre-shared Key và chọn Connect.



Hình 3. 92: Giao diện chọn Security và điền mật khẩu kết nối cho Home Laptop.

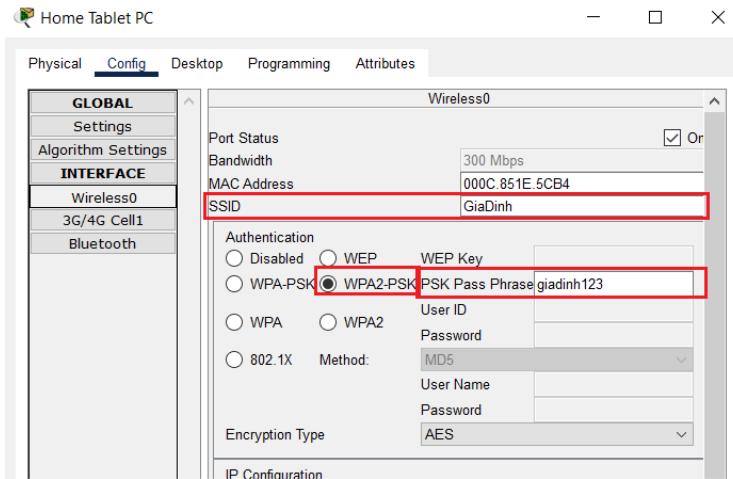
Đối với Home Tablet PC.

- + Vào Home Tablet PC chọn Config, ở phần Interface chọn Wireless0.



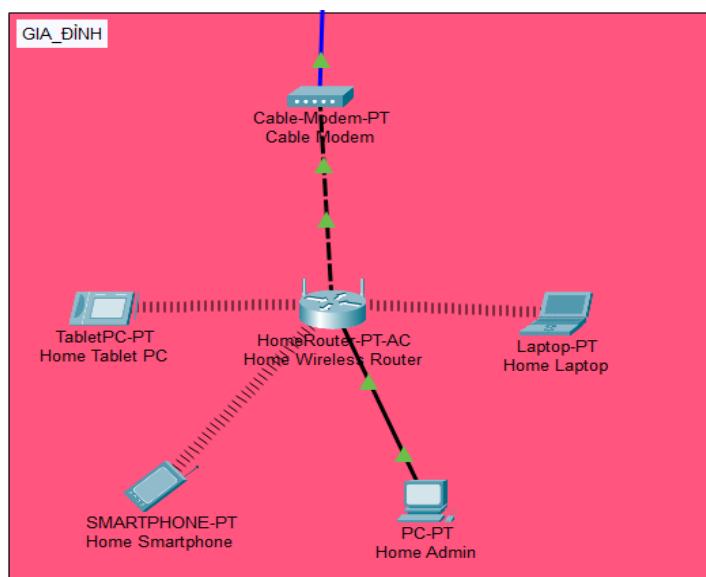
Hình 3. 93: Giao diện các thao tác vào Wireless0 của Home Tablet PC.

+ Điền SSID, chọn **WPA2-PSK**, điền mật khẩu vào PSK Pass Phrase. Sau đó tắt Home Tablet PC.



Hình 3. 94: Giao diện cấu hình thông tin để kết nối cho Home Tablet PC

Đối với Home Smartphone làm tương tự như Home Tablet PC.



Hình 3. 95: Giao diện kết nối thành công các thiết bị các nhân trong gia đình.

3.3 Kết quả chạy chương trình

3.3.1 Kiểm tra kết nối thiết bị của doanh nghiệp với internet.



Ping từ PC_{_}LETAN đến DNS Server và Web Server.

```

Cisco Packet Tracer PC Command Line 1.0
C:>ping 10.100.100.254

Pinging 10.100.100.254 with 32 bytes of data:

Request timed out.
Reply from 10.100.100.254: bytes=32 time=9ms TTL=126
Reply from 10.100.100.254: bytes=32 time=10ms TTL=126
Reply from 10.100.100.254: bytes=32 time=10ms TTL=126

Ping statistics for 10.100.100.254:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 9ms, Maximum = 10ms, Average = 9ms

C:>ping 203.0.113.78

Pinging 203.0.113.78 with 32 bytes of data:

Request timed out.
Reply from 203.0.113.78: bytes=32 time=24ms TTL=126
Reply from 203.0.113.78: bytes=32 time=8ms TTL=126
Reply from 203.0.113.78: bytes=32 time=11ms TTL=126

Ping statistics for 203.0.113.78:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 8ms, Maximum = 24ms, Average = 14ms

C:>

```

Hình 3. 96: Kết quả ping thành công của PC_{_}LETAN.

Ping từ Guest Smartphone đến DNS Server và Web Server.

```

Cisco Packet Tracer PC Command Line 1.0
C:>ping 10.100.100.254

Pinging 10.100.100.254 with 32 bytes of data:

Reply from 10.100.100.254: bytes=32 time=22ms TTL=126
Reply from 10.100.100.254: bytes=32 time=13ms TTL=126
Reply from 10.100.100.254: bytes=32 time=14ms TTL=126
Reply from 10.100.100.254: bytes=32 time=9ms TTL=126

Ping statistics for 10.100.100.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 9ms, Maximum = 22ms, Average = 14ms

C:>ping 203.0.113.78

Pinging 203.0.113.78 with 32 bytes of data:

Reply from 203.0.113.78: bytes=32 time=13ms TTL=126
Reply from 203.0.113.78: bytes=32 time=11ms TTL=126
Reply from 203.0.113.78: bytes=32 time=13ms TTL=126
Reply from 203.0.113.78: bytes=32 time=11ms TTL=126

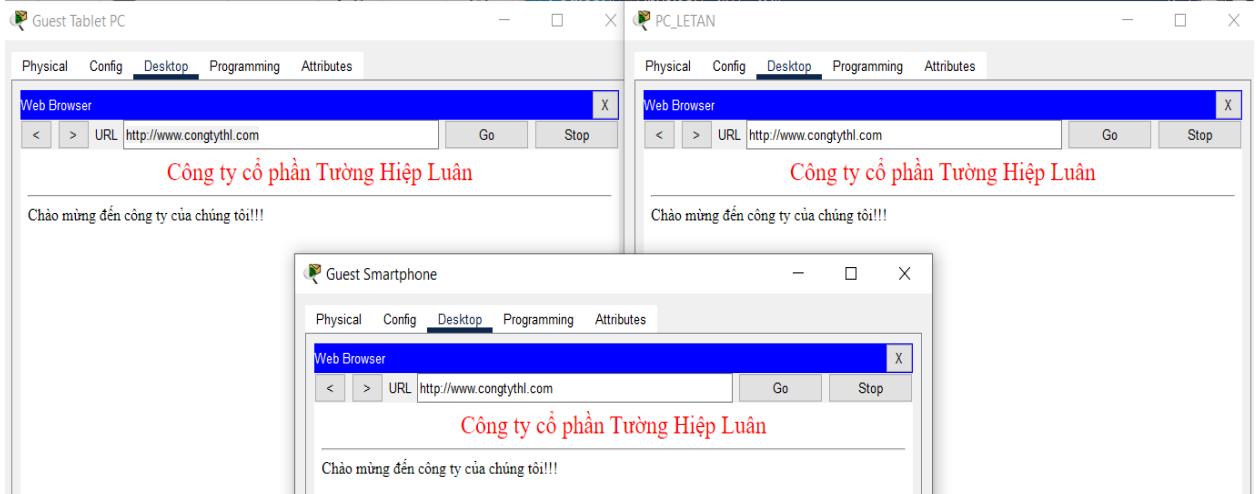
Ping statistics for 203.0.113.78:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 13ms, Average = 12ms

C:>

```

Hình 3. 97: Kết quả ping thành công của Guest Smartphone.

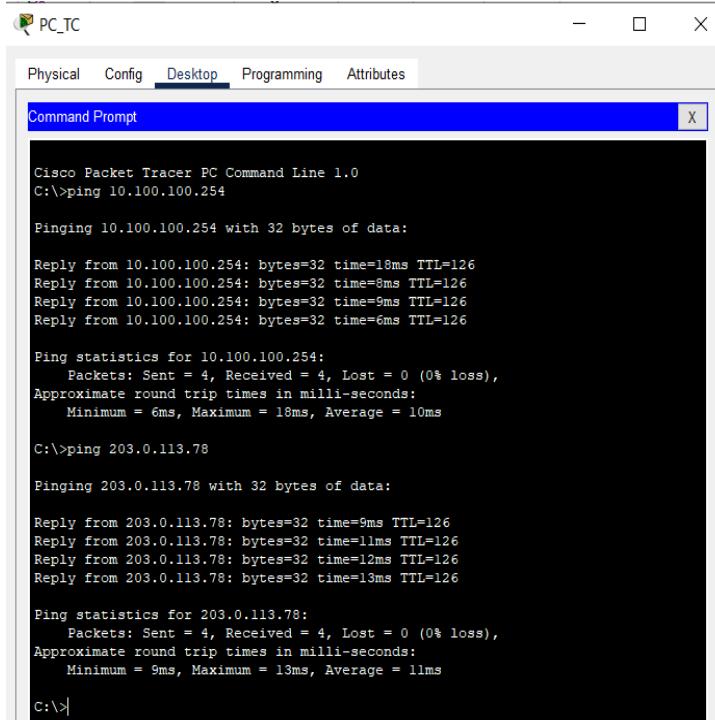
Kiểm tra kết nối bằng url từ PC_{_}LETAN, Guest Smartphone, Guest Tablet PC đến Web Server.



Hình 3. 98: Kết quả ping thành công từ thiết bị phòng lễ tân đến url Web Server.

Phòng tài chính

Ping từ PC_{_}TC đến DNS Server và Web Server.



```
Cisco Packet Tracer PC Command Line 1.0
C:>ping 10.100.100.254

Pinging 10.100.100.254 with 32 bytes of data:
Reply from 10.100.100.254: bytes=32 time=18ms TTL=126
Reply from 10.100.100.254: bytes=32 time=8ms TTL=126
Reply from 10.100.100.254: bytes=32 time=9ms TTL=126
Reply from 10.100.100.254: bytes=32 time=6ms TTL=126

Ping statistics for 10.100.100.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 6ms, Maximum = 18ms, Average = 10ms

C:>ping 203.0.113.78

Pinging 203.0.113.78 with 32 bytes of data:
Reply from 203.0.113.78: bytes=32 time=9ms TTL=126
Reply from 203.0.113.78: bytes=32 time=11ms TTL=126
Reply from 203.0.113.78: bytes=32 time=12ms TTL=126
Reply from 203.0.113.78: bytes=32 time=13ms TTL=126

Ping statistics for 203.0.113.78:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 9ms, Maximum = 13ms, Average = 11ms

C:>
```

Hình 3. 99: Kết quả ping thành công của PC_{_}TC.

Ping từ NhanVien5 đến DNS Server và Web Server.

```
C:\>ping 10.100.100.254
Pinging 10.100.100.254 with 32 bytes of data:
Reply from 10.100.100.254: bytes=32 time=9ms TTL=126
Reply from 10.100.100.254: bytes=32 time=8ms TTL=126
Reply from 10.100.100.254: bytes=32 time=11ms TTL=126
Reply from 10.100.100.254: bytes=32 time=14ms TTL=126

Ping statistics for 10.100.100.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 8ms, Maximum = 14ms, Average = 10ms

C:\>ping 203.0.113.78
Pinging 203.0.113.78 with 32 bytes of data:
Reply from 203.0.113.78: bytes=32 time=13ms TTL=126
Reply from 203.0.113.78: bytes=32 time=11ms TTL=126
Reply from 203.0.113.78: bytes=32 time=12ms TTL=126
Reply from 203.0.113.78: bytes=32 time=11ms TTL=126

Ping statistics for 203.0.113.78:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 13ms, Average = 11ms

C:\>
```

Hình 3. 100: Kết quả ping thành công của NhanVien5.

Kiểm tra kết nối bằng url từ PC_TC, Guest Smartphone, NhanVien5 đến Web Server.



Hình 3. 101: Kết quả ping thành công từ thiết bị phòng tài chính đến url Web Server.

Phòng marketing

Ping từ NhanVien3 đến DNS Server và Web Server.

```

Cisco Packet Tracer PC Command Line 1.0
C:>ping 10.100.100.254

Pinging 10.100.100.254 with 32 bytes of data:

Reply from 10.100.100.254: bytes=32 time=18ms TTL=126
Reply from 10.100.100.254: bytes=32 time=11ms TTL=126
Reply from 10.100.100.254: bytes=32 time=12ms TTL=126
Reply from 10.100.100.254: bytes=32 time=9ms TTL=126

Ping statistics for 10.100.100.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 9ms, Maximum = 18ms, Average = 12ms

C:>ping 203.0.113.78

Pinging 203.0.113.78 with 32 bytes of data:

Reply from 203.0.113.78: bytes=32 time=11ms TTL=126
Reply from 203.0.113.78: bytes=32 time=10ms TTL=126
Reply from 203.0.113.78: bytes=32 time=9ms TTL=126
Reply from 203.0.113.78: bytes=32 time=11ms TTL=126

Ping statistics for 203.0.113.78:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 9ms, Maximum = 11ms, Average = 10ms

C:>

```

Hình 3. 102: Kết quả ping thành công của NhanVien3.

Kiểm tra kết nối bằng url từ NhanVien3, NhanVien4 đến Web Server.



Hình 3. 103: Kết quả ping thành công từ thiết bị phòng marketing đến url Web Server.

Phòng kinh doanh

Ping từ PC_KD đến DNS Server và Web Server.

```

Cisco Packet Tracer PC Command Line 1.0
C:>ping 10.100.100.254

Pinging 10.100.100.254 with 32 bytes of data:

Reply from 10.100.100.254: bytes=32 time=19ms TTL=126
Reply from 10.100.100.254: bytes=32 time=11ms TTL=126
Reply from 10.100.100.254: bytes=32 time=12ms TTL=126
Reply from 10.100.100.254: bytes=32 time=26ms TTL=126

Ping statistics for 10.100.100.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 26ms, Average = 17ms

C:>ping 203.0.113.78

Pinging 203.0.113.78 with 32 bytes of data:

Reply from 203.0.113.78: bytes=32 time=11ms TTL=126
Reply from 203.0.113.78: bytes=32 time=12ms TTL=126
Reply from 203.0.113.78: bytes=32 time=11ms TTL=126
Reply from 203.0.113.78: bytes=32 time=5ms TTL=126

Ping statistics for 203.0.113.78:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 5ms, Maximum = 12ms, Average = 9ms

C:>

```

Hình 3. 104: Kết quả ping thành công của PC_KD.

Ping từ NhanVien1 đến DNS Server và Web Server.

```

Cisco Packet Tracer PC Command Line 1.0
C:>ping 10.100.100.254

Pinging 10.100.100.254 with 32 bytes of data:

Reply from 10.100.100.254: bytes=32 time=23ms TTL=126
Reply from 10.100.100.254: bytes=32 time=10ms TTL=126
Reply from 10.100.100.254: bytes=32 time=6ms TTL=126
Reply from 10.100.100.254: bytes=32 time=13ms TTL=126

Ping statistics for 10.100.100.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 6ms, Maximum = 23ms, Average = 13ms

C:>ping 203.0.113.78

Pinging 203.0.113.78 with 32 bytes of data:

Reply from 203.0.113.78: bytes=32 time=13ms TTL=126
Reply from 203.0.113.78: bytes=32 time=12ms TTL=126
Reply from 203.0.113.78: bytes=32 time=9ms TTL=126
Reply from 203.0.113.78: bytes=32 time=11ms TTL=126

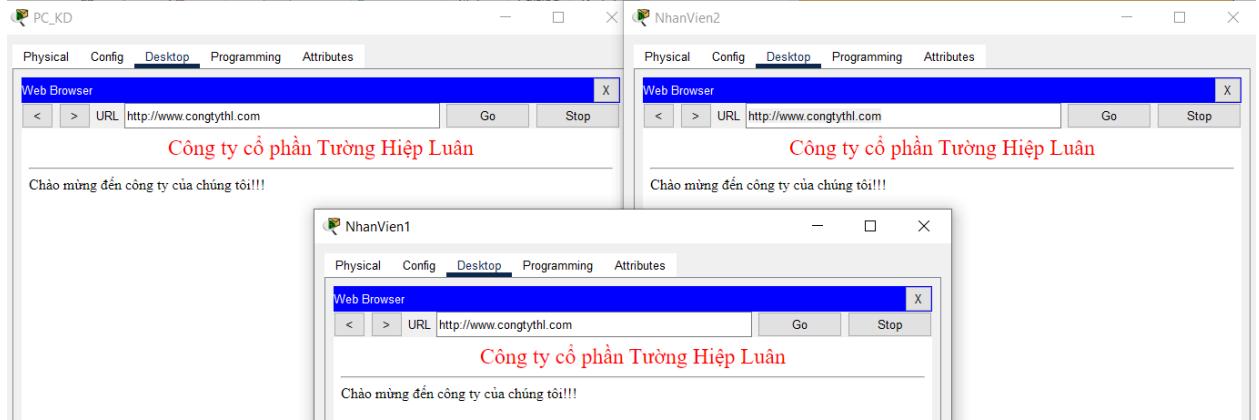
Ping statistics for 203.0.113.78:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 9ms, Maximum = 13ms, Average = 11ms

C:>

```

Hình 3. 105: Kết quả ping thành công của NhanVien1.

Kiểm tra kết nối bằng url từ PC_KD, NhanVien1, NhanVien2 đến Web Server.



Hình 3. 106: Kết quả ping thành công từ thiết bị phòng tài chính đến url Web Server.

Phòng giám đốc

Ping từ THUKY đến DNS Server và Web Server.

```
Cisco Packet Tracer PC Command Line 1.0
C:>ping 10.100.100.254

Pinging 10.100.100.254 with 32 bytes of data:
Reply from 10.100.100.254: bytes=32 time=23ms TTL=126
Reply from 10.100.100.254: bytes=32 time=14ms TTL=126
Reply from 10.100.100.254: bytes=32 time=11ms TTL=126
Reply from 10.100.100.254: bytes=32 time=9ms TTL=126

Ping statistics for 10.100.100.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 9ms, Maximum = 23ms, Average = 14ms

C:>ping 203.0.113.78

Pinging 203.0.113.78 with 32 bytes of data:
Reply from 203.0.113.78: bytes=32 time=13ms TTL=126
Reply from 203.0.113.78: bytes=32 time=13ms TTL=126
Reply from 203.0.113.78: bytes=32 time=8ms TTL=126
Reply from 203.0.113.78: bytes=32 time=7ms TTL=126

Ping statistics for 203.0.113.78:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 7ms, Maximum = 13ms, Average = 10ms

C:>
```

Hình 3. 107: Kết quả ping thành công của THUKY.

Ping từ GIAMDOC đến DNS Server và Web Server.

```

Cisco Packet Tracer PC Command Line 1.0
C:>ping 10.100.100.254

Pinging 10.100.100.254 with 32 bytes of data:

Reply from 10.100.100.254: bytes=32 time=33ms TTL=126
Reply from 10.100.100.254: bytes=32 time=10ms TTL=126
Reply from 10.100.100.254: bytes=32 time=5ms TTL=126
Reply from 10.100.100.254: bytes=32 time=10ms TTL=126

Ping statistics for 10.100.100.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 5ms, Maximum = 33ms, Average = 14ms

C:>ping 203.0.113.78

Pinging 203.0.113.78 with 32 bytes of data:

Reply from 203.0.113.78: bytes=32 time=20ms TTL=126
Reply from 203.0.113.78: bytes=32 time=15ms TTL=126
Reply from 203.0.113.78: bytes=32 time=12ms TTL=126
Reply from 203.0.113.78: bytes=32 time=7ms TTL=126

Ping statistics for 203.0.113.78:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 7ms, Maximum = 20ms, Average = 13ms

C:>

```

Hình 3. 108: Kết quả ping thành công của GIAMDOC.

Kiểm tra kết nối bằng url từ THUKY, GIAMDOC đến Web Server.



Hình 3. 109: Kết quả ping thành công từ thiết bị phòng giám đốc đến url Web Server.

Phòng họp

Ping từ NhanVien6 đến DNS Server và Web Server.

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.100.100.254

Pinging 10.100.100.254 with 32 bytes of data:

Reply from 10.100.100.254: bytes=32 time=19ms TTL=126
Reply from 10.100.100.254: bytes=32 time=10ms TTL=126
Reply from 10.100.100.254: bytes=32 time=9ms TTL=126
Reply from 10.100.100.254: bytes=32 time=6ms TTL=126

Ping statistics for 10.100.100.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 6ms, Maximum = 19ms, Average = 11ms

C:\>ping 203.0.113.78

Pinging 203.0.113.78 with 32 bytes of data:

Reply from 203.0.113.78: bytes=32 time=12ms TTL=126
Reply from 203.0.113.78: bytes=32 time=10ms TTL=126
Reply from 203.0.113.78: bytes=32 time=9ms TTL=126
Reply from 203.0.113.78: bytes=32 time=9ms TTL=126

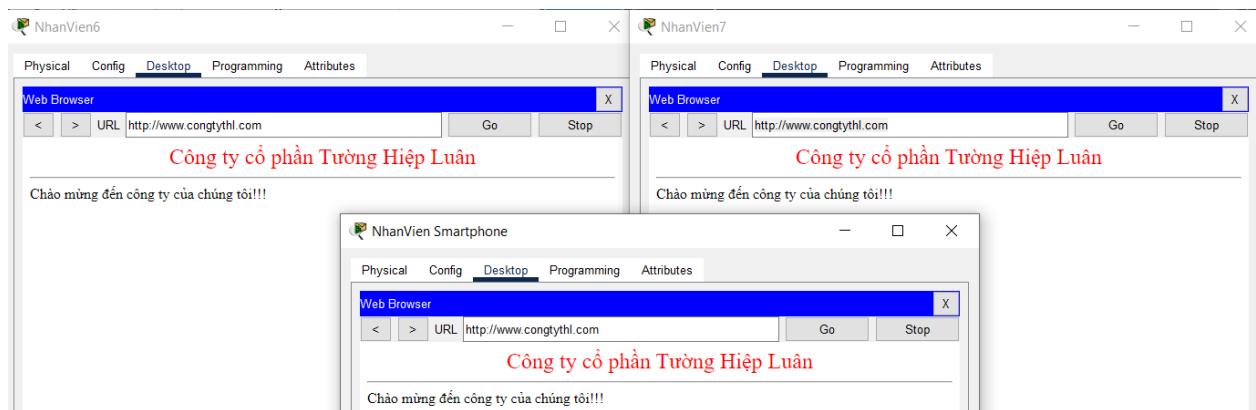
Ping statistics for 203.0.113.78:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 9ms, Maximum = 12ms, Average = 10ms

C:\>

```

Hình 3. 110: Kết quả ping thành công của NhanVien6.

Kiểm tra kết nối bằng url từ NhanVien6, NhanVien7, NhanVien Smartphone đến Web Server.



Hình 3. 111: Kết quả ping thành công từ thiết bị phòng họp đến url Web Server.

3.3.2 Kiểm tra kết nối thiết bị gia đình với internet.

Ping từ Home Admin đến DNS Server và Web Server.

```
C:\>ping 10.100.100.254

Pinging 10.100.100.254 with 32 bytes of data:

Reply from 10.100.100.254: bytes=32 time=8ms TTL=126
Reply from 10.100.100.254: bytes=32 time=6ms TTL=126
Reply from 10.100.100.254: bytes=32 time=4ms TTL=126
Reply from 10.100.100.254: bytes=32 time=4ms TTL=126

Ping statistics for 10.100.100.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 8ms, Average = 5ms

C:\>ping 203.0.113.78

Pinging 203.0.113.78 with 32 bytes of data:

Reply from 203.0.113.78: bytes=32 time=8ms TTL=126
Reply from 203.0.113.78: bytes=32 time=8ms TTL=126
Reply from 203.0.113.78: bytes=32 time=4ms TTL=126
Reply from 203.0.113.78: bytes=32 time=4ms TTL=126

Ping statistics for 203.0.113.78:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 8ms, Average = 6ms

C:\>
```

Hình 3. 112: Kết quả ping thành công của Home Admin.

Ping từ Home Laptop đến DNS Server và Web Server.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.100.100.254

Pinging 10.100.100.254 with 32 bytes of data:

Reply from 10.100.100.254: bytes=32 time=26ms TTL=126
Reply from 10.100.100.254: bytes=32 time=15ms TTL=126
Reply from 10.100.100.254: bytes=32 time=11ms TTL=126
Reply from 10.100.100.254: bytes=32 time=13ms TTL=126

Ping statistics for 10.100.100.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 26ms, Average = 16ms

C:\>ping 203.0.113.78

Pinging 203.0.113.78 with 32 bytes of data:

Reply from 203.0.113.78: bytes=32 time=15ms TTL=126
Reply from 203.0.113.78: bytes=32 time=17ms TTL=126
Reply from 203.0.113.78: bytes=32 time=13ms TTL=126
Reply from 203.0.113.78: bytes=32 time=15ms TTL=126

Ping statistics for 203.0.113.78:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 13ms, Maximum = 17ms, Average = 15ms

C:\>
```

Hình 3. 113: Kết quả ping thành công của Home Laptop.

Ping từ Home Smartphone đến DNS Server và Web Server.

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.100.100.254

Pinging 10.100.100.254 with 32 bytes of data:

Reply from 10.100.100.254: bytes=32 time=23ms TTL=126
Reply from 10.100.100.254: bytes=32 time=13ms TTL=126
Reply from 10.100.100.254: bytes=32 time=15ms TTL=126
Reply from 10.100.100.254: bytes=32 time=14ms TTL=126

Ping statistics for 10.100.100.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 13ms, Maximum = 23ms, Average = 16ms

C:\>ping 203.0.113.78

Pinging 203.0.113.78 with 32 bytes of data:

Reply from 203.0.113.78: bytes=32 time=9ms TTL=126
Reply from 203.0.113.78: bytes=32 time=11ms TTL=126
Reply from 203.0.113.78: bytes=32 time=13ms TTL=126
Reply from 203.0.113.78: bytes=32 time=18ms TTL=126

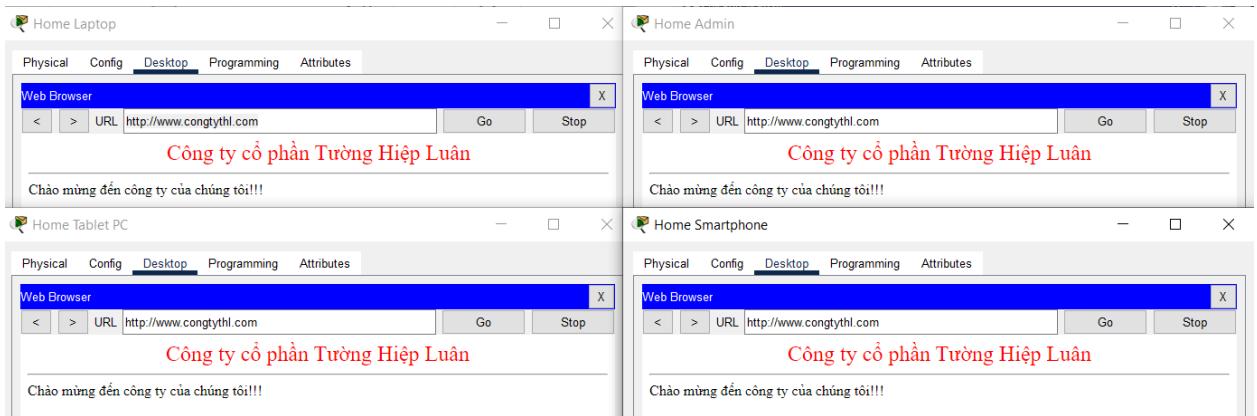
Ping statistics for 203.0.113.78:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 9ms, Maximum = 18ms, Average = 12ms

C:\>

```

Hình 3. 114: Kết quả ping thành công của Home Smartphone.

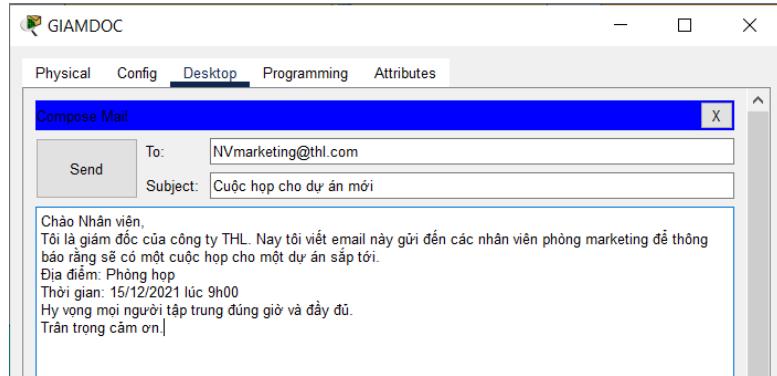
Kiểm tra kết nối bằng url từ Home Admin, Home Laptop, Home Smartphone, Home Tablet PC đến Web Server.



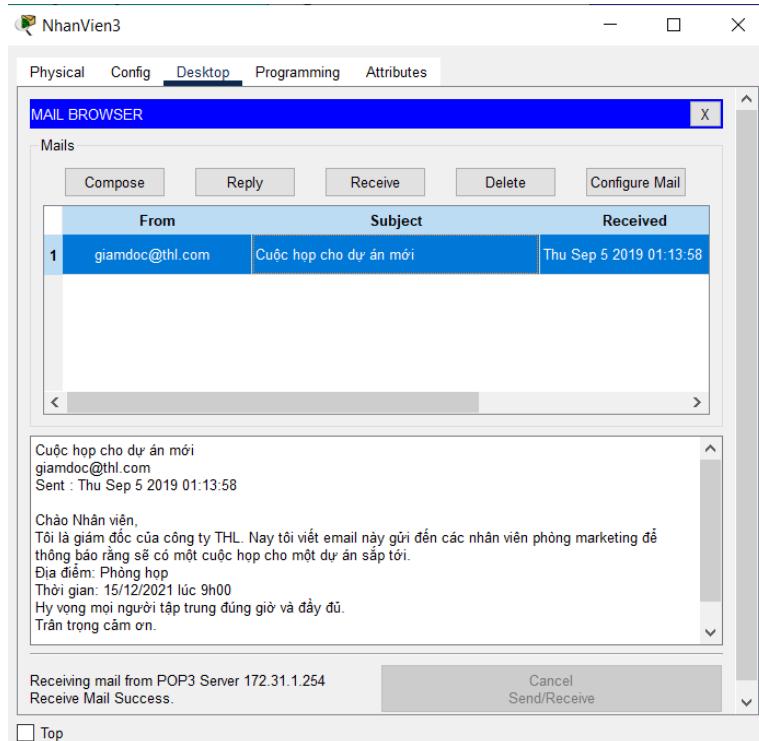
Hình 3. 115: Kết quả ping thành công từ thiết bị gia đình đến url Web Server.

3.3.3 Gửi email giữa các phòng doanh nghiệp

Gửi email từ phòng giám đốc đến nhân viên phòng marketing.



Hình 3. 116: Giao diện gửi email từ giám đốc đến nhân viên.



Hình 3. 117: Giao diện email nhân viên phòng marketing nhận được từ giám đốc.

CHƯƠNG 4 – KẾT LUẬN

Qua việc triển khai hệ thống mạng không dây nội bộ cho doanh nghiệp THL thì chúng ta có thể lắp đặt một hệ thống mạng cơ bản, nhanh chóng và thuận tiện theo mô hình hệ thống như trên. Sử dụng các AP khác nhau để chia thành các phòng khác nhau để sử dụng, áp dụng bảo mật WPA2-Enterprise cung cấp cả tên đăng nhập và mật khẩu để người dùng đăng nhập vào đối với các phòng quan trọng và áp dụng bảo mật WPA2-Personal đối với các phòng ít quan trọng hơn. Xác thực bằng Radius Sever từ xa để đảm bảo tính bảo mật. Các người dùng nội bộ trong công ty mới có thể truy cập vào mạng trong từng phòng và có thể giao tiếp với nhân viên khác trong nội bộ công ty mà không thể kết nối ra bên ngoài để đảm bảo an toàn cho công ty. Hệ thống về cơ bản đáp ứng đầy đủ yêu cầu công ty đưa ra nhưng vẫn có thể thay đổi chỉnh sửa cần thiết hay mở rộng quy mô thì vẫn có thể triển khai nhanh chóng, hệ thống vẫn đảm bảo tính bảo mật về dữ liệu và thông tin của công ty.

TÀI LIỆU THAM KHẢO

Tiếng Việt

- [1] <https://vnpro.vn/tin-tuc/cac-khai-niem-co-ban-cua-mang-may-tinh-1397.html> [Accessed 1 12 21].
- [2] <https://quantrimang.com/cac-kieu-tan-cong-mang-22> [Accessed 1 12 21].
- [3] <https://biettuot.info/lich-su-phat-trien-mang-di-dong-1g-2g-3g-4g-5g/> [Accessed 1 12 21].
- [4] <https://www.digistar.vn/gioi-thieu-cac-chuan-wifi/> [Accessed 2 12 21].
- [5] <https://www.totolink.vn/article/57-11-cach-bao-mat-mang-khong-day-cho-gia-dinh-ban.html> [Accessed 1 12 21].
- [6] <https://khs247.com/thiet-bi-mang/> [Accessed 2 12 21].

Tiếng Anh

- [1] Hakima Chaouchi, Maryline Laurnet-Maknavicius, Wireless and Mobile Network Security, London: Hermes Science/Lavoisier, 2007.
- [2] <https://qastack.vn/superuser/373453/8021x-what-exactly-is-it-regarding-wpa-and-eap> [Accessced 1 12 21]