BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC QUẢN LÝ VÀ CÔNG NGHỆ HẢI PHÒNG

ĐỒ ÁN TỐT NGHIỆP

NGÀNH ĐIỆN TỬ TRUYỀN THÔNG

Sinh viên : Lê Bá Duy

Giảng viên hướng dẫn : ThS. Phạm Văn Thắng

HẢI PHÒNG - 2024

BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC QUẢN LÝ VÀ CÔNG NGHỆ HẢI PHÒNG

XÂY DỰNG SMART WIFI MAKETING PHỤC VỤ ỦY BAN NHÂN DÂN QUẬN HỒNG BÀNG - THÀNH PHỐ HẢI PHÒNG

ĐỒ ÁN TỐT NGHIỆP HỆ ĐẠI HỌC CHÍNH QUY

NGHÀNH ĐIỆN TỬ TRUYỀN THÔNG

Sinh viên : Lê Bá Duy

Giảng viên hướng dẫn : ThS. Phạm Văn Thắng

HẢI PHÒNG – 2024

BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC QUẢN LÝ VÀ CÔNG NGHỆ HẢI PHÒNG

NHIỆM VỤ ĐỀ TÀI TỐT NGHIỆP

Sinh viên: Lê Bá Duy – MSV: 2113103023

Lớp: DTL2501 – Ngành Điện Tử Truyền Thông

Tên đề tài: Xây Dựng Smart Wifi Maketing Phục Vụ Ủy Ban Nhân Dân Quận Hồng Bàng - Thành Phố Hải Phòng

NHIỆM VỤ ĐỀ TÀI

1. Nội dung và các yêu cầu cần giải quyết trong nhiệm vụ đề tài tốt nghiệp :

……

……

……

……

……

……

2. Các số liệu cần thiết để thiết kế tình toán xây dựng hệ thống :

……

……

……

……

……

……

3. Địa điểm triển khai nâng cấp hệ thống :

……

……

……

……

CÁC CÁN BỘ HƯỚNG DẪN ĐỀ TÀI TỐT NGHIỆP

Họ và tên: Phạm Văn Thắng

Học hàm, học vị: Thạc sĩ

Cơ quan công tác: Trường Đại học Quản lý và Công nghệ Hải Phòng

Nội dung hướng dẫn: Xây dựng smart wifi marketting UBND Quận Hồng Bàng - Thành Phố Hải Phòng

Đề tài tốt nghiệp được giao ngày ….. tháng ….. năm 2024

Yêu cầu phải hoàn thành xong trước ngày…..tháng ….năm 2024

Đã nhận nhiệm vụ Đ.T.T.N	Đã giao nhiệm vụ Đ.T.T.N
Sinh Viên	Cán bộ hướng dẫn Đ.T.T.N
Lê Bá Duy	ThS. Phạm Văn Thắng

Hải Phòng, ngày……tháng…. năm 2024

TRƯỞNG KHOA

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

Độc Lập - Tự Do - Hạnh Phúc

PHIẾU NHẬN XÉT CỦA GIẢNG VIÊN HƯỚNG DẪN TỐT NGHIỆP

Họ và tên giảng viên:

Đơn vị công tác : Trường Đại học Quản lý và Công nghệ Hải Phòng

Họ và tên sinh viên : Lê Bá Duy

Chuyên ngành : Điện tử truyền thông

Nội dung hướng dẫn: Toàn bộ đề tài

1. Tinh thần thái độ của sinh viên trong quá trình làm đề tài tốt nghiệp

……

……

……

2. Đánh giá chất lượng của Đ.T.T.N (so với yêu cầu đã đề ra trong nhiệm vụ Đ.T.T.N, trên các mặt về lý luận thực tiễn, tính toán số liệu…)

……

……

……

3. Ý kiến của giảng viên hướng dẫn tốt nghiệp

Được bảo vệ ☐ Không được bảo vệ ☐ Điểm hướng dẫn ☐

Hải phòng, ngày ……tháng ……năm 2024

Giảng viên hướng dẫn

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

Độc Lập - Tự Do - Hạnh Phúc

NHẬN XÉT ĐÁNH GIÁ CỦA GIẢNG VIÊN CHẤM PHẢN BIỆN

Họ và tên giảng viên: …….

Đơn vị công tác: …….

Họ và tên sinh viên: ……. Chuyên ngành: …….

Đề tài tốt nghiệp: ……

……

1. Phần nhận xét của giảng viên chấm phản biện

……

……

……

2. Những mặt còn hạn chế

……

……

……..

3. Ý kiến của giảng viên chấm phản biện

Được bảo vệ ☐ Không được bảo vệ ☐ Điểm phản biện ☐

Hải phòng, ngày……tháng ……năm 2024

Giảng viên chấm phản biện

MỤC LỤC

DANH MỤC BẢNG

DANH MỤC HÌNH

LỜI MỞ ĐẦU

Wireless LAN là một trong những công nghệ truyền thông không dây được áp dụng cho mạng cục bộ. Sự ra đời của nó đã khắc phục những hạn chế mà mạng nối dây không thể giải quyết được, và là giải pháp cho su thế phát triển của công nghệ truyền thông hiện đại. Nói như vậy để thấy được những lợi ích to lớn mà Wireless LAN mang lại, tuy nhiên nó không phải là giải pháp thay thế toàn bộ cho các mạng LAN nối dây truyền thống.

Dựa trên chuẩn IEEE 802.1 mạng Wireless LAN đã đi đến sự thống nhất và trở thành mạng công nghiệp, từ đó được áp dụng trong rất nhiều lĩnh vực, từ lĩnh vực trong sóc sức khoẻ, bán lẻ, sản xuất, lưu kho, đến các trường học. Nghành công nghiệp này đã kiếm lợi từ các thiết bị đầu cuối và các máy tính notebook để truyền thông tin thời gian thực đến các trung tâm tập trung để xử lý. Ngày nay, mạng Wireless LAN đang được đón nhận rộng rãi như một kết nối đa chức năng từ các doanh nghiệp. Lợi ích của thị trường ngày càng tăng.

Thêm vào đó, mạng Wireless LAN cũng có thể đóng vai trò như một mạng quảng bá nội dung theo mục đích người dùng mang lại nhiều hiểu quả trong việc khai thác.

Wifi marketing -với sự phát triển bùng nổ của công nghệ và nhất là Internet. Ngày có càng nhiều doanh nghiệp/công ty sử dụng phương tiện Internet làm công cụ chính để quảng cáo. Nó giúp thương hiệu đến gần hơn với người dùng. Đặc biệt khi chúng kết hợp với những mạng xã hội lớn như: Facebook, instagram... Ngày nay marketing trên Internet đã trở thành xu hướng toàn cầu tất yếu.

Do đó tôi đã chọn đề tài nghiên cứu " thiết kế hệ thống wifi maketing lắp đặt tại tòa nhà hành chính quận Hồng Bàng " .

Trong phạm vi khóa luận tôi sẽ trình bày một cái nhìn tổng quan về WLAN, lịch sử phát triển, chuẩn thực hiện, một số đặc tính kỹ thuật, các khuyến cáo về bảo mật, đặc biệt phương pháp bảo mật xác thực bàng Radius sever để từ đó giới thiệu về hệ thống Wifi maketing

Chương 1: TỔNG QUAN VỀ MẠNG KHÔNG DÂY

1.1. Các khái niệm về mạng không dây

Mạng LAN không dây viết tắt là WLAN (Wireless Local Area Network), là một mạng dùng để kết nối hai hay nhiều máy tính với nhau mà không sử dụng dây dẫn. WLAN dùng công nghệ trải phổ, sử dụng sóng vô tuyến cho phép truyền thông giữa các thiết bị trong một vùng nào đó còn được gọi là Basic Service Set. Nó giúp cho người sử dụng có thể di chuyển trong một vùng bao phủ rộng mà vẫn kết nối được với mạng.

Công nghệ WLAN lần đầu tiên xuất hiện vào cuối năm 1990, khi những nhà sản xuất giới thiệu những sản phẩm hoạt động trong băng tần 900Mhz. Những giải pháp này (không được thống nhất giữa các nhà sản xuất) cung cấp tốc độ truyền dữ liệu 1Mbps, thấp hơn nhiều so với tốc độ 10Mbps của hầu hết các mạng sử dụng cáp hiện thời.

Năm 1992, những nhà sản xuất bắt đầu bán những sản phẩm WLAN sử dụng băng tần 2.4Ghz. Mặc dầu những sản phẩm này đã có tốc độ truyền dữ liệu cao hơn nhưng chúng vẫn là những giải pháp riêng của mỗi nhà sản xuất không được công bố rộng rãi. Sự cần thiết cho việc hoạt động thống nhất giữa các thiết bị ở những dãy tần số khác nhau dẫn đến một số tổ chức bắt đầu phát triển ra những chuẩn mạng không dây chung.

Năm 1997, Institute of Electrical and Electronics Engineers (IEEE) đã phê chuẩn sự ra đời của chuẩn 802.11, và cũng được biết với tên gọi WI-FI (Wireless Fidelity) cho các mạng WLAN. Chuẩn 802.11 hỗ trợ ba phương pháp truyền tín hiệu, trong đó có bao gồm phương pháp truyền tín hiệu vô tuyến ở tần số 2.4Ghz.

Năm 1999, IEEE thông qua hai sự bổ sung cho chuẩn 802.11 là các chuẩn 802.11a và 802.11b (định nghĩa ra những phương pháp truyền tín hiệu). Và những thiết bị WLAN dựa trên chuẩn 802.11b đã nhanh chóng trở thành công nghệ không dây vượt trội. Các thiết bị WLAN 802.11b truyền phát ở tần số 2.4Ghz, cung cấp tốc độ truyền dữ liệu có thể lên tới 11Mbps. IEEE 802.11b được tạo ra

nhằm cung cấp những đặc điểm về tính hiệu dụng, thông lượng (throughput) và bảo mật để so sánh với mạng có dây.

Năm 2003, IEEE công bố thêm một sự cải tiến là chuẩn 802.11g mà có thể truyền nhận thông tin ở cả hai dãy tần 2.4Ghz và 5Ghz và có thể nâng tốc độ truyền dữ liệu lên đến 54Mbps. Thêm vào đó, những sản phẩm áp dụng 802.11g cũng có thể tương thích ngược với các thiết bị chuẩn 802.11b. Hiện nay chuẩn 802.11g đã đạt đến tốc độ 108Mbps-300Mbps.

Ưu điểm của mạng không dây

- **Sự tiện lợi:** Mạng không dây cũng như hệ thống mạng thông thường. Nó cho phép người dùng truy xuất tài nguyên mạng ở bất kỳ nơi đâu trong khu vực được triển khai (nhà hay văn phòng). Với sự gia tăng số người sử dụng máy tính xách tay (laptop), đó là một điều rất thuận lợi.
- **Khả năng di động:** Với sự phát triển của các mạng không dây công cộng, người dùng có thể truy cập Internet ở bất cứ đâu. Chẳng hạn ở các quán Cafe, người dùng có thể truy cập Internet không dây miễn phí.
- **Hiệu quả:** Người dùng có thể duy trì kết nối mạng khi họ đi từ nơi này đến nơi khác.
- **Triển khai**: Việc thiết lập hệ thống mạng không dây ban đầu chỉ cần ít nhất 1 access point. Với mạng dùng cáp, phải tốn thêm chi phí và có thể gặp khó khăn trong việc triển khai hệ thống cáp ở nhiều nơi trong tòa nhà.
- **Khả năng mở rộng:** Mạng không dây có thể đáp ứng tức thì khi gia tăng số lượng người dùng. Với hệ thống mạng dùng cáp cần phải gắn thêm cáp.

Nhược điểm của mạng không dây

Công nghệ mạng LAN không dây, ngoài rất nhiều sự tiện lợi và những ưu điểm được đề cập ở trên thì cũng có các nhược điểm. Trong một số trường hợp mạng LAN không dây có thể không như mong muốn vì một số lý do. Hầu hết chúng phải làm việc với những giới hạn vốn có của công nghệ.

- **Bảo mật:** Môi trường kết nối không dây là không khí nên khả năng bị tấn công của người dùng là rất cao.

- **Phạm vi:** Một mạng chuẩn 802.11g với các thiết bị chuẩn chỉ có thể hoạt động tốt trong phạm vi vài chục mét. Nó phù hợp trong 1 căn nhà, nhưngvới một tòa nhà lớn thì không đáp ứng được nhu cầu. Để đáp ứng cần phải mua thêm Repeater hay access point, dẫn đến chi phí gia tăng.
- **Độ tin cậy:** Vì sử dụng sóng vô tuyến để truyền thông nên việc bị nhiễu, tín hiệu bị giảm do tác động của các thiết bị khác (lò vi sóng,…) là không tránh khỏi. Làm giảm đáng kể hiệu quả hoạt động của mạng.
- **Tốc độ:** Tốc độ của mạng không dây (1- 125 Mbps) rất chậm so với mạng sử dụng cáp (100 Mbps đến hàng Gbps)

1.2. Các chuẩn thông dụng của WLAN

Hiện nay tiêu chuẩn chính cho Wireless là một họ giao thức truyền tin qua mạng không dây IEEE 802.11. Do việc nghiên cứu và đưa ra ứng dụng rất gần nhau nên có một số giao thức đã thành chuẩn của thế giới, một số khác vẫn còn đang tranh cãi và một số còn đang dự thảo. Một số chuẩn thông dụng như: 802.11b (cải tiến từ 802.11), 802.11a, 802.11g, 802.11n.

1.2.1. Chuẩn IEEE 802.11b

Chuẩn này được đưa ra vào năm 1999, nó cải tiến từ chuẩn 802.11.

- ✓ Cũng hoạt động ở dải tần 2,4 Ghz nhưng chỉ sử dụng trải phổ trực tiếp DSSS.
- ✓ Tốc độ tại Access Point có thể lên tới 11Mbps (802.11b), 22Mbps (802.11b+).
- ✓ Các sản phẩm theo chuẩn 802.11b được kiểm tra và thử nghiệm bởi hiệp hội các công ty Ethernet không dây (WECA) và được biết đến như là hiệp hội Wi-Fi, những sản phẩm Wireless được WiFi kiểm tra nếu đạt thì sẽ mang nhãn hiệu này.
- ✓ Hiện nay IEEE 802.11b là một chuẩn được sử dụng rộng rãi nhất cho Wireless LAN. Vì dải tần số 2,4Ghz là dải tần số ISM (Industrial, Scientific and Medical: dải tần vô tuyến dành cho công nghiệp, khoa học và y học, không cần xin phép) cũng được sử dụng cho các chuẩn mạng không dây khác như là: Bluetooth và HomeRF, hai chuẩn này không được phổ biến như là 801.11. Bluetooth được thiết kế sử dụng cho thiết bị không dây mà không phải là Wireless LAN, nó được dùng cho mạng cá nhân PAN(Personal Area

Network). Như vậy Wireless LAN sử dụng chuẩn 802.11b và các thiết bị Bluetooth hoạt động trong cùng một dải băng tần.

Bảng 1.1 Một số thông số kỹ thuật của chuẩn IEEE 802.11b

Release Date	Op. Frequency	Data Rate (Typ)	Data Rate (Max)	Range (Indoor)
October 1999	2.4 GHz	4.5 Mbit/s	11 Mbit/s	~35 m

1.2.2 Chuẩn IEEE 802.11a

- ✓ Đây là một chuẩn được cấp phép ở dải băng tần mới. Nó hoạt động ở dải tần số 5 Ghz sử dụng phương thức điều chế ghép kênh theo vùng tần số vuông góc (OFDM). Phương thức điều chế này làm tăng tốc độ trên mỗi kênh (từ 11Mbps/1kênh lên 54 Mbps/1 kênh).
- ✓ Có thể sử dụng đến 8 Access Point (truyền trên 8 kênh Non-overlapping,kênh không chồng lấn phổ), đặc điểm này ở dải tần 2,4Ghz chỉ có thể sử dụng 3 Access Point (truyền trên 3 kênh Non – overlapping).
- ✓ Hỗ trợ đồng thời nhiều người sử dụng với tốc độ cao mà ít bị xung đột.
- ✓ Các sản phẩm của theo chuẩn IEEE 802.11a không tương thích với các sản phẩm theo chuẩn IEEE 802.11 và 802.11b vì chúng hoạt động ở các dải tần số khác nhau. Tuy nhiên các nhà sản xuất chipset đang cố gắng đưa loại chipset hoạt động ở cả 2 chế độ theo hai chuẩn 802.11a và 802.11b. Sự phối hợp này được biết đến với tên WiFi5 (WiFi cho công nghệ 5Gbps).

Bảng 1.2 Một số thông số kỹ thuật của chuẩn IEEE 802.11a

Release Date	Op. Frequency	Data Rate (Typ)	Data Rate (Max)	Range (Indoor)
October 1999	5 GHz	23 Mbit/s	54 Mbit/s	~35 m

1.2.3 Chuẩn IEEE 802.11g

- ➢ Bản dự thảo của tiêu chuẩn này được đưa ra vào tháng 10 – 2002.

- Sử dụng dải tần 2,4 Ghz, tốc độ truyền lên đến 54Mbps.
- Phương thức điều chế: Có thể dùng một trong 2 phương thức
  - Dùng OFDM (giống với 802.11a) tốc độ truyền lên tới 54Mbps.
  - Dùng trải phổ trực tiếp DSSS tốc độ bị giới hạn ở 11 Mbps.
- Tương thích ngược với chuẩn 802.11b.
- Bị hạn chế về số kênh truyền.

Bảng 1.3 Một số thông số kỹ thuật của chuẩn IEEE 802.11g

Release Date	Op. Frequency	Data Rate (Typ)	Data Rate (Max)	Range (Indoor)
June 2003	2.4 GHz	23 Mbit/s	54 Mbit/s	~35 m

1.2.4 Chuẩn IEEE 802.11n

Chuẩn 802.11n đang được xúc tiến để đạt tốc độ 100 Mb/giây, nhanh gấp 5 lần chuẩn 802.11g và cho phép thiết bị kết nối hoạt động với khoảng cách xa hơn các mạng Wi-Fi hiện hành.

Winston Sun, giám đốc công nghệ của công ty không dây Atheros Communications, nhận xét, một thiết bị tương thích 802.11n có thể truy cập các điểm hotspot với tốc độ 150 MB/giây với khoảng cách lý tưởng dưới 6m, khả năng liên kết càng giảm khi người dùng ở cách xa điểm truy cập đó.

802.11n chưa thể sớm trở thành chuẩn Wi-Fi thế hệ mới vì một số mạng Wi-Fi không thuộc thông số 802.11n cũng được giới thiệu. Theo Sun, các chuẩn Wi-Fi mới được ra mắt có thể tự động dò tần sóng thích hợp để kết nối Internet. Chính vì thế, thiết bị hỗ trợ 802.11n không thể "độc chiếm" phổ Wi-Fi và phải "nhường" sóng cho các mạng kết nối khác.

Ông Sun cho biết, tốc độ truy cập Wi-Fi giảm tỷ lệ nghịch với khoảng cách từ thiết bị tới hotspot vẫn cho phép các máy cầm tay, như iTV của Apple stream được các đoạn video clip nhưng không thể stream video nén có độ nét cao .

Bảng 1.4 Một số thông số kỹ thuật của chuẩn IEEE 802.11n

Release Date	Op. Frequency	Data Rate (Typ)	Data Rate (Max)	Range (In-door)
June 2009 (est.)	5 GHz and/or 2.4 GHz	74 Mbit/s	300 Mbit/s (2 streams)	~70 m

1.2.4 Chuẩn IEEE 802.11ac

Wi-Fi 802.11ac, hay còn được biết đến với tên gọi Wi-Fi 5, là một tiêu chuẩn truyền thông không dây thuộc họ các tiêu chuẩn IEEE 802.11, được thiết kế để cung cấp hiệu suất truyền dữ liệu cao và khả năng xử lý tốt hơn so với các tiêu chuẩn trước đó. Dưới đây là một số đặc điểm chính của Wi-Fi 802.11ac:

Tốc Độ Truyền Dữ Liệu Cao: Wi-Fi 802.11ac mang lại tốc độ truyền dữ liệu đáng kể, có thể lên đến vài gigabit mỗi giây. Điều này giúp cải thiện trải nghiệm người dùng khi sử dụng các ứng dụng đòi hỏi băng thông cao như video HD, trò chơi trực tuyến, và truyền dữ liệu lớn.

Khả Năng Hoạt Động ở Tần Số 5GHz: Wi-Fi 802.11ac thường hoạt động ở dải tần 5GHz, mang lại sự linh hoạt và giảm tình trạng nhiễu sóng từ các thiết bị hoạt động ở dải tần 2.4GHz. Điều này giúp tối ưu hóa chất lượng kết nối và tăng cường hiệu suất mạng.

Kỹ Thuật MIMO (Multiple Input Multiple Output): Wi-Fi 802.11ac thường sử dụng kỹ thuật MIMO để tăng cường khả năng truyền và nhận dữ liệu. Các thiết bị hỗ trợ MIMO có thể sử dụng nhiều anten để truyền và nhận dữ liệu đồng thời, làm tăng tốc độ truyền dữ liệu và cải thiện khả năng đối phó với nhiễu sóng.

Beamforming: Wi-Fi 802.11ac thường hỗ trợ kỹ thuật beamforming, cho phép router hoặc access point tập trung tín hiệu sóng Wi-Fi vào các thiết bị cụ thể, thay vì phát sóng một cách đồng đều. Điều này giúp tăng cường độ ổ định và phạm vi kết nối.

Tính Tương Thích Ngược: Mặc dù là một tiêu chuẩn mới, nhưng Wi-Fi 802.11ac vẫn có tính tương thích ngược với các thiết bị sử dụng các tiêu chuẩn

Wi-Fi trước đó như 802.11n và 802.11g, giúp người dùng chuyển đổi mà không mất kết nối.

Wi-Fi 802.11ac đã đóng góp quan trọng vào sự phát triển của mạng không dây, đáp ứng nhu cầu ngày càng cao về băng thông và hiệu suất trong môi trường số hóa ngày nay. Đối với người dùng và doanh nghiệp, sự nâng cấp lên Wi-Fi 802.11ac mang lại trải nghiệm mạng tốt hơn và khả năng đáp ứng đa dạng các yêu cầu kết nối.

1.2.5 Chuẩn IEEE 802.11ax

EEE 802.11ax, còn được biết đến với tên gọi Wi-Fi 6, là một tiêu chuẩn truyền thông không dây mới nhất trong họ các tiêu chuẩn IEEE 802.11, được thiết kế để đáp ứng nhu cầu ngày càng tăng về kết nối không dây chất lượng cao trong môi trường đa thiết bị và mật độ cao. Dưới đây là những đặc điểm chính của IEEE 802.11ax:

Tăng Cường Hiệu Suất: Một trong những mục tiêu chính của IEEE 802.11ax là tăng cường hiệu suất mạng không dây. Tiêu chuẩn này mang lại tốc độ truyền dữ liệu tăng lên đáng kể so với các tiêu chuẩn trước đó, hỗ trợ người dùng trong việc sử dụng các ứng dụng đòi hỏi băng thông lớn như video 4K, trò chơi trực tuyến và truyền dữ liệu nặng.

Khả Năng Xử Lý Đa Thiết Bị (OFDMA): 802.11ax sử dụng kỹ thuật Orthogonal Frequency Division Multiple Access (OFDMA) để tối ưu hóa sự sử dụng băng thông và xử lý đồng thời nhiều thiết bị. Điều này giúp cải thiện khả năng đáp ứng với môi trường có nhiều thiết bị kết nối đồng thời.

Tính Tiết Kiệm Năng Lượng (Target Wake Time - TWT): IEEE 802.11ax đưa ra một khía cạnh quan trọng là tính tiết kiệm năng lượng thông qua kỹ thuật Target Wake Time (TWT). TWT cho phép thiết bị thông báo trước về thời gian mà nó sẽ "thức dậy" để truyền dữ liệu, giúp giảm tiêu tốn năng lượng và kéo dài thời gian pin của thiết bị di động.

Beamforming và MU-MIMO Cải Tiến: IEEE 802.11ax tiếp tục hỗ trợ kỹ thuật beamforming để tập trung tín hiệu Wi-Fi vào các thiết bị cụ thể, cũng như

Multiple User-Multiple Input Multiple Output (MU-MIMO) để cải thiện khả năng truyền dữ liệu đồng thời.

Tính Tương Thích Ngược: Mặc dù là một tiêu chuẩn mới, nhưng IEEE 802.11ax vẫn có tính tương thích ngược với các tiêu chuẩn Wi-Fi trước đó. Điều này có nghĩa là nó có thể hoạt động cùng các thiết bị sử dụng Wi-Fi 5 (802.11ac) và Wi-Fi 4 (802.11n).

IEEE 802.11ax đã đánh dấu một bước tiến lớn trong sự phát triển của mạng không dây, đặc biệt là trong bối cảnh của môi trường đa thiết bị và ứng dụng đòi hỏi băng thông cao ngày nay. Với Wi-Fi 6, người dùng có cơ hội trải nghiệm một mạng không dây nhanh chóng, hiệu quả và linh hoạt hơn bao giờ hết.

1.2.6 So sánh các chuẩn kết nối

Wi-Fi còn có tên gọi khác là IEEE 802.11 (hay ngắn gọn là 802.11) cũng chính là nhóm các tiêu chuẩn kỹ thuật của công nghệ kết nối này do liên minh Wi-Fi (Wi-Fi Alliance: www.wi-fi.org) quy định. Hiện tồn tại các xác thực sau được đưa ra bởi Wi-Fi Alliance:

Bảng 1.5 So sánh các chuẩn IEEE 802.11x

Chuẩn	**Phân loại**	**Tính năng chính** **Định nghĩa**	**Chú thích**
IEEE 802.11	Kết nối	Tần số: 2,4 GHz Tốc độ tối đa: 2 mbps Tầm hoạt động: không xác định	Chuẩn lý thuyết
IEEE 802.11a	Kết nối	Tần số: 5 GHz Tốc độ tối đa: 54 mbps Tầm hoạt động: 25-75 m	Xem thêm 802.11d và 802.11h
IEEE 801.11b	Kết nối	Tần số: 2,4 GHz Tốc độ tối đa: 11 mbps Tầm hoạt động: 35-100 m	Tương thích với 802.11g

IEEE 802.11g	Kết nối	Tần số: 2,4 GHz Tốc độ tối đa: 54 mbps Tầm hoạt động: 25-75 m	Tương thích ngược với 802.11b, xem thêm 802.11d và 802.11h
IEEE 8021.11n	Kết nối	Tần số: 2,4 GHz Tốc độ tối đa: 540 mbps Tầm hoạt động: 50-125 m	Tương thích ngược với 802.11b/g Dự kiến sẽ được thông qua vào tháng 11/2008
IEEE 802.11d	Tính năng bổ sung	Bật tính năng thay đổi tầng MAC để phù hợp với các yêu cầu ở những quốc gia khác nhau	Hỗ trợ bởi một số thiết bị 802.11a và 802.11a/g
IEEE 802.11h	Tính năng bổ sung	Chọn tần số động (dynamic frequency selection: DFS) và điều khiển truyền năng lượng (transmit power control: TPC) để hạn chế việc xung đột với các thiết bị dùng tần số 5 GHz khác	Hỗ trợ bởi một số thiết bị 802.11a và 802.11a/g
WPA Enterprise	Bảo mật	Sử dụng xác thực 802.1x với chế độ mã hóa TKIP và một máy chủ xác thực	Xem thêm WPA2 Enterprise
WPA Personal	Bảo mật	Sử dụng khóa chia sẻ với mã hóa TKIP	Xem thêm WPA2 Personal

WPA2 Enterprise	Bảo mật	Nâng cấp của WPA Enterprise với việc dùng mã hóa AES	Dựa trên 802.11i
WPA2 Personal	Bảo mật	Nâng cấp của WPA Personal với việc dùng mã hóa AES	Dựa trên 802.11i
EAP-TLS	Bảo mật	Extensible Authentication Protocol Transport Layer Security	Sử dụng cho WPA Enterprise
EAP-TTLS/MSCHAPv2	Bảo mật	EAP-Tunneled TLS/Microsoft Challenge Authentication Handshake Protocol	Sử dụng cho WPA/WPA2 Enterprise
EAP-SIM	Bảo mật	Một phiên bản của EAP cho các dịch vụ điện thoại di động nền GSM	Sử dụng cho WPA/WPA2 Enterprise
WMM	Multimedia	Xác thực cho VoIP để quy định cách thức ưu tiên băng thông cho giọng nói hoặc video	Một thành phần của bản thảo 802.11e WLAN Quality of Service

IEEE 802.11 chưa từng được ứng dụng thực tế và chỉ được xem là bước đệm để hình thành nên kỷ nguyên Wi-Fi. Trên thực tế, cả 24 kí tự theo sau 802.11 đều được lên kế hoạch sử dụng bởi Wi-Fi Alliance. Như ở bảng trên, các IEEE 802.11 được phân loại thành nhiều nhóm, trong đó hầu như người dùng chỉ biết và quan tâm đến tiêu chuẩn phân loại theo tính chất kết nối (IEEE 802.11a/b/g/n...).

Một số IEEE 802.11 ít phổ biến khác:

- IEEE 802.11c: các thủ tục quy định cách thức bắt cầu giữa các mạng Wi-Fi. Tiêu chuẩn này thường đi cặp với 802.11d.
- IEEE 802.11e: đưa QoS (Quality of Service) vào Wi-Fi, qua đó sắp đặt thứ tự ưu tiên cho các gói tin, đặc biệt quan trọng trong trường hợp băng thông bị giới hạn hoặc quá tải.
- IEEE 802.11F: giao thức truy cập nội ở Access Point, là một mở rộng cho IEEE 802.11. Tiêu chuẩn này cho phép các Access Point có thể "nói chuyện" với nhau, từ đó đưa vào các tính năng hữu ích như cân bằng tải, mở rộng vùng phủ sóng Wi-Fi...
- IEEE 802.11h: những bổ sung cho 802.11a để quản lý dải tần 5 GHz nhằm tương thích với các yêu cầu kỹ thuật ở châu Âu.
- IEEE 802.11i: những bổ sung về bảo mật. Chỉ những thiết bị IEEE 802.11g mới nhất mới bổ sung khả năng bảo mật này. Chuẩn này trên thực tế được tách ra từ IEEE 802.11e. WPA là một trong những thành phần được mô tả trong 802.11i ở dạng bản thảo, và khi 802.11i được thông qua thì chuyển thành WPA2 (với các tính chất được mô tả ở bảng trên).
- IEEE 802.11j: những bổ sung để tương thích điều kiện kỹ thuật ở Nhật Bản.
- IEEE 802.11k: những tiêu chuẩn trong việc quản lí tài nguyên sóng radio. Chuẩn này dự kiến sẽ hoàn tất và được đệ trình thành chuẩn chính thức trong năm nay.
- IEEE 802.11p: hình thức kết nối mở rộng sử dụng trên các phương tiện giao thông (vd: sử dụng Wi-Fi trên xe buýt, xe cứu thương...). Dự kiến sẽ được phổ biến vào năm 2009.
- IEEE 802.11r: mở rộng của IEEE 802.11d, cho phép nâng cấp khả năng chuyển vùng.
- IEEE 802.11T: đây chính là tiêu chuẩn WMM như mô tả ở bảng trên.
- IEE 802.11u: quy định cách thức tương tác với các thiết bị không tương thích 802 (chẳng hạn các mạng điện thoại di động).
- IEEE 802.11w: là nâng cấp của các tiêu chuẩn bảo mật được mô tả ở IEEE 802.11i, hiện chỉ trong giải đoạn khởi đầu.

Các chuẩn IEEE 802.11F và 802.11T được viết hoa chữ cái cuối cùng để phân biệt đây là hai chuẩn dựa trên các tài liệu độc lập, thay vì là sự mở rộng / nâng cấp của 802.11, và do đó chúng có thể được ứng dụng vào các môi trường khác 802.11 (chẳng hạn WiMAX – 802.16).

Trong khi đó 802.11x sẽ không được dùng như một tiêu chuẩn độc lập mà sẽ bỏ trống để trỏ đến các chuẩn kết nối IEEE 802.11 bất kì. Nói cách khác, 802.11 có ý nghĩa là "mạng cục bộ không dây", và 802.11x mang ý nghĩa "mạng cục bộ không dây theo hình thức kết nối nào đấy (a/b/g/n)".

Hình thức bảo mật cơ bản nhất ở mạng Wi-Fi là WEP là một phần của bản IEEE 802.11 "gốc".

Bạn dễ dàng tạo một mạng Wi-Fi với lẫn lộn các thiết bị theo chuẩn IEEE 802.11b với IEEE 802.11g. Tất nhiên là tốc độ và khoảng cách hiệu dụng sẽ là của IEEE 802.11b. Một trở ngại với các mạng IEEE 802.11b/g và có lẽ là cả n là việc sử dụng tần số 2,4 GHz, vốn đã quá "chật chội" khi đó cũng là tần số hoạt động của máy bộ đàm, tai nghe và loa không dây... Tệ hơn nữa, các lò viba cũng sử dụng tần số này, và công suất quá lớn của chúng có thể gây ra các vấn đề về nhiễu loạn và giao thoa.

Tuy chuẩn IEEE 802.11n chưa được thông qua nhưng khá nhiều nhà sản xuất thiết bị đã dựa trên bản thảo của chuẩn này để tạo ra những cái gọi là chuẩn G+ hoặc SuperG với tốc độ thông thường là gấp đôi giới hạn của IEEE 802.11g. Các thiết bị này tương thích ngược với IEEE 802.11b/g rất tốt nhưng tất nhiên là ở mức tốc độ giới hạn. Bên cạnh đó, bạn phải dùng các thiết bị (card mạng, router, access point...) từ cùng nhà sản xuất.

Khi chuẩn IEEE 802.11n được thông qua, các nốt kết nối theo chuẩn b/g vẫn được hưởng lợi khá nhiều từ khoảng cách kết nối nếu Access Point là chuẩn n.

Cần lưu ý, bất kể tốc độ kết nối Wi-Fi là bao nhiêu thì tốc độ "ra net" của bạn cũng chỉ giới hạn ở mức khoảng 2 mbps (tốc độ kết nối Internet). Với môi trường Internet công cộng (quán cafe Wi-Fi, thư viện...), ắt hẳn lợi thế tốc độ truyền file trong mạng cục bộ xem như không tồn tại.

1.2.2. Các thiết bị cơ bản và ứng dụng của hệ thống WLAN:

1.3.1 Các thiết bị cơ bản:

a) Card mạng không dây (Wireless NIC):

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

Hình 1.1: Card mạng không dây

b) Các điểm truy cập (Access Point):

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

Hình1.2: Access Point

c) Bridge không dây (Wbridge):

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

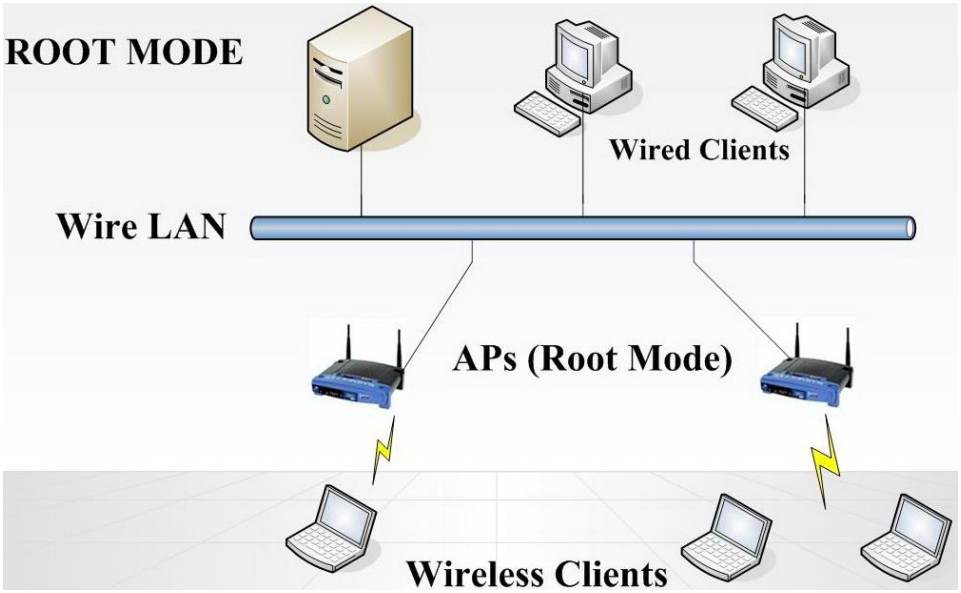
d) Các router điểm truy cập (Access Point Router):

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

1.3.2 Các ứng dụng của hệ thống WLAN:

a) Vai trò truy cập (Access Role):

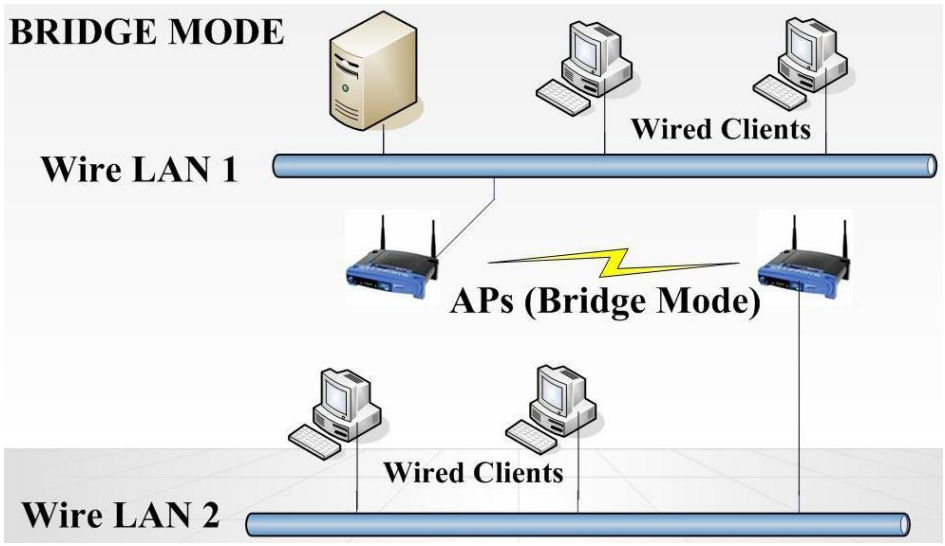
WLAN hầu như được triển khai ở lớp access, nghĩa là chúng được sử dụng ở một điểm truy cập vào mạng có dây thông thường. Các WLAN là các mạng ở lớp data-link như tất cả những phương pháp truy cập khác. Vì tốc độ thấp nên WLAN ít được triển khai ở core và distribution.



Hình 1.3: Access Role

b) Mở rộng mạng (Network Extention):

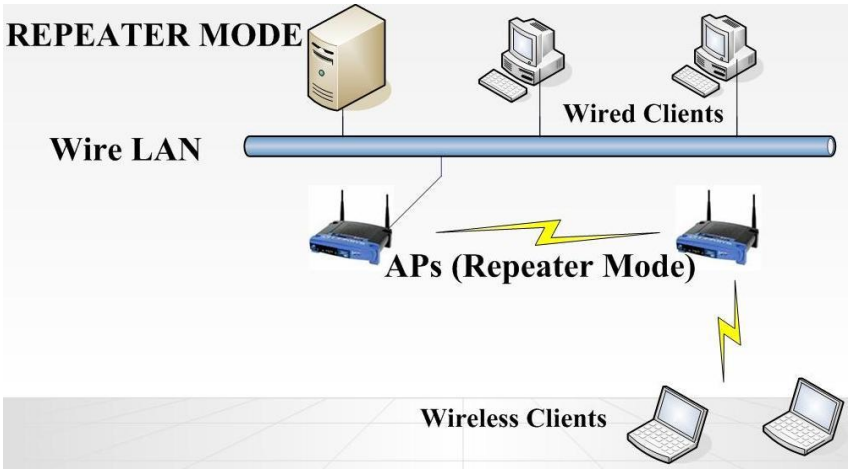
Các mạng không dây có thể được xem như một phần mở rộng của một mạng có dây. Khi muốn mở rộng một mạng hiện tại, nếu cài đặt thêm đường cáp thì sẽ rất tốn kém. Các WLAN có thể được thực thi một cách dễ dàng, vì ít phải cài đặt cáp trong mạng không dây.



Hình 1.4: Mở rộng mạng

c) Văn phòng nhỏ - Văn phòng gia đình (Small Office-Home Office):

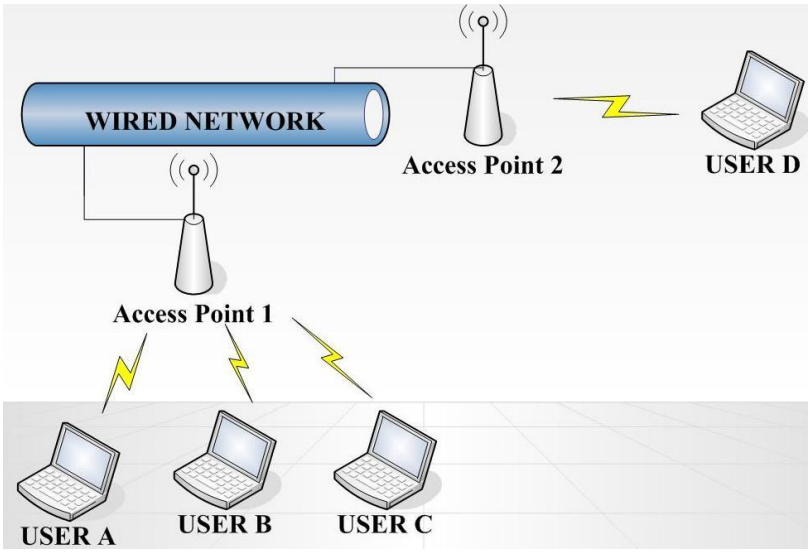
Các thiết bị wireless SOHO thì rất có ích khi người dùng muốn chia sẻ một kết nối Internet với các doang nghiệp nhỏ, văn phòng nhỏ…



Hình 1.5: SOHO Wireless LAN

d) Văn phòng di động (Mobile Offices):

Các văn phòng di động cho phép người dùng có thể di chuyển đến một vị trí khác một cách dễ dàng. Các kết nối WLAN từ toà nhà chính ra các lớp học di động cho phép các kết nối một cách lịnh hoạt với chi phí có thể chấp nhận được.



Hình 1.6: Mobile office

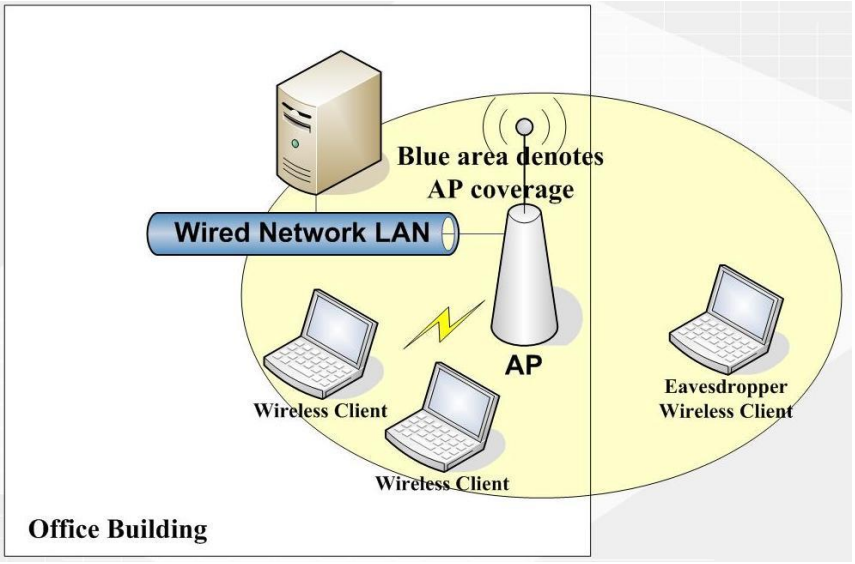
Các giải pháp bảo mật trong mạng wifi

1.4.1 Tầm quan trọng của các giải pháp bảo mật trong mạng WLAN

Để kết nối tới một mạng LAN hữu tuyến ta cần phải truy cập theo đường truyền bằng dây cáp, phải kết nối một PC vào một cổng mạng. Với mạng không dây ta chỉ cần có máy của ta trong vùng sóng bao phủ của mạng không dây. Điều khiển cho mạng có dây là đơn giản: đường truyền bằng cáp thông thường được đi

trong các tòa nhà cao tầng và các port không sử dụng có thể làm cho nó disable bằng các ứng dụng quản lý. Các mạng không dây (hay vô tuyến) sử dụng sóng vô tuyến xuyên qua vật liệu của các tòa nhà và như vậy sự bao phủ là không giới hạn ở bên trong một tòa nhà. Sóng vô tuyến có thể xuất hiện trên đường phố, từ các trạm phát từ các mạng LAN này, và như vậy ai đó có thể truy cập nhờ thiết bị thích hợp. Do đó mạng không dây của một công ty cũng có thể bị truy cập từ bên ngoài tòa nhà công ty của họ.

Với giá thành xây dựng một hệ thống mạng WLAN giảm, ngày càng có nhiều công ty sử dụng. Điều này sẽ không thể tránh khỏi việc Hacker chuyển sang tấn công và khai thác các điểm yếu trên nền tảng mạng sử dụng chuẩn 802.11. Những công cụ Sniffers cho phép tóm được các gói tin giao tiếp trên mạng, họ có thể phân tích và lấy đi những thông tin quan trọng của chúng ta.



Hình 1.7: mô hình bảo mật mạng không dây

1.2.3. Các kiểu mã hóa bảo mật trong mạng WLAN

1.4.2.1 WEP

WEP (Wired Equivalent Privacy) có nghĩa là bảo mật không dây tương đương với có dây. Thực ra, WEP đã đưa cả xác thực người dùng và đảm bảo an toàn dữ liệu vào cùng một phương thức không an toàn. WEP sử dụng một khoá mã hoá không thay đổi có độ dài 64 bit hoặc 128 bit, (nhưng trừ đi 24 bit sử dụng cho vector khởi tạo khoá mã hoá, nên độ dài khoá chỉ còn 40 bit hoặc 104 bit)

được sử dụng để xác thực các thiết bị được phép truy cập vào trong mạng và cũng được sử dụng để mã hoá truyền dữ liệu.

Rất đơn giản, các khoá mã hoá này dễ dàng bị "bẻ gãy" bởi thuật toán brute-force và kiểu tấn công thử lỗi (trial-and-error). Các phần mềm miễn phí như Airsnort hoặc WEPCrack sẽ cho phép hacker có thể phá vỡ khoá mã hoá nếu họ thu thập đủ từ 5 đến 10 triệu gói tin trên một mạng không dây. Với những khoá mã hoá 128 bit cũng không khá hơn: 24 bit cho khởi tạo mã hoá nên chỉ có 104 bit được sử dụng để mã hoá, và cách thức cũng giống như mã hoá có độ dài 64 bit nên mã hoá 128 bit cũng dễ dàng bị bẻ khoá. Ngoài ra, những điểm yếu trong những vector khởi tạo khoá mã hoá giúp cho hacker có thể tìm ra mật khẩu nhanh hơn với ít gói thông tin hơn rất nhiều.

Không dự đoán được những lỗi trong khoá mã hoá, WEP có thể được tạo ra cách bảo mật mạnh mẽ hơn nếu sử dụng một giao thức xác thực mà cung cấp mỗi khoá mã hoá mới cho mỗi phiên làm việc. Khoá mã hoá sẽ thay đổi trên mỗi phiên làm việc. Điều này sẽ gây khó khăn hơn cho hacker thu thập đủ các gói dữ liệu cần thiết để có thể bẽ gãy khoá bảo mật.

1.4.2.2 TKIP

Là giải pháp của IEEE được phát triển năm 2004. Là một nâng cấp cho WEP nhằm vá những vấn đề bảo mật trong cài đặt mã dòng RC4 trong WEP. TKIP dùng hàm băm (hashing) IV để chống lại việc giả mạo gói tin, nó cũng cung cấp phương thức để kiểm tra tính toàn vẹn của thông điệp MIC (message integrity check) để đảm bảo tính chính xác của gói tin. TKIP sử dụng khóa động bằng cách đặt cho mỗi frame một chuỗi số riêng để chống lại dạng tấn công giả mạo.

1.4.2.3 AES

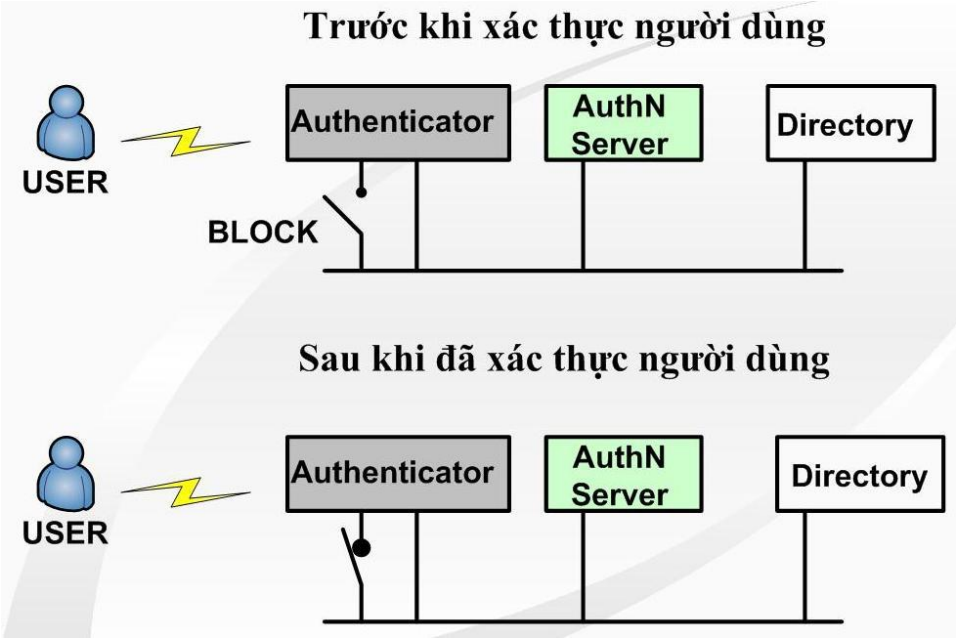
Trong mật mã học, AES (viết tắt của từ tiếng Anh: Advanced Encryption Standard, hay Tiêu chuẩn mã hóa tiên tiến) là một thuật toán mã hóa khối được chính phủ Hoa kỳ áp dụng làm tiêu chuẩn mã hóa. Giống như tiêu chuẩn tiền nhiệm DES, AES được kỳ vọng áp dụng trên phạm vi thế giới và đã được nghiên cứu rất kỹ lưỡng. AES được chấp thuận làm tiêu chuẩn liên bang bởi Viện tiêu

chuẩn và công nghệ quốc gia Hoa kỳ (NIST) sau một quá trình tiêu chuẩn hóa kéo dài 5 năm.

Thuật toán được thiết kế bởi hai nhà mật mã học người Bỉ: Joan Daemen và Vincent Rijmen (lấy tên chung là "Rijndael" khi tham gia cuộc thi thiết kế AES). Rijndael được phát âm là "Rhine dahl" theo phiên âm quốc tế (IPA: [ɹaindal]).

1.4.2.4 802.11x và EAP

802.1x là chuẩn đặc tả cho việc truy cập dựa trên cổng (port-based) được định nghĩa bởi IEEE. Hoạt động trên cả môi trường có dây truyền thống và không dây. Việc điều khiển truy cập được thực hiện bằng cách: Khi một người dùng cố gắng kết nối vào hệ thống mạng, kết nối của người dùng sẽ được đặt ở trạng thái bị chặn (blocking) và chờ cho việc kiểm tra định danh người dùng hoàn tất.



Hình 1. 8: Mô tả xác thực 802.1x

EAP là phương thức xác thực bao gồm yêu cầu định danh người dùng (password, cetificate,…), giao thức được sử dụng (MD5, TLS_Transport Layer Security, OTP_ One Time Password,…) hỗ trợ tự động sinh khóa và xác thực lẫn nhau.

Quá trình chứng thực 802.1x-EAP như sau:

Wireless client muốn liên kết với một AP trong mạng.

1. AP sẽ chặn lại tất cả các thông tin của client cho tới khi client log on vào mạng, khi đó Client yêu cầu liên kết tới AP

2. AP đáp lại yêu cầu liên kết với một yêu cầu nhận dạng EAP

3. Client gửi đáp lại yêu cầu nhận dạng EAP cho AP

4. Thông tin đáp lại yêu cầu nhận dạng EAP của client được chuyển tới Server chứng thực

5. Server chứng thực gửi một yêu cầu cho phép tới AP

6. AP chuyển yêu cầu cho phép tới client

7. Client gửi trả lời sự cấp phép EAP tới AP

8. AP chuyển sự trả lời đó tới Server chứng thực

9. Server chứng thực gửi một thông báo thành công EAP tới AP

10. AP chuyển thông báo thành công tới client và đặt cổng của client trong chế độ forward.

1.4.2.5 WPA (WI-FI PROTECTED ACCESS)

WEP được xây dựng để bảo vệ một mạng không dây tránh bị nghe trộm. Nhưng nhanh chóng sau đó người ta phát hiện ra nhiều lổ hỏng ở công nghệ này. Do đó, công nghệ mới có tên gọi WPA (Wi-Fi Protected Access) ra đời, khắc phục được nhiều nhược điểm của WEP.

Trong những cải tiến quan trọng nhất của WPA là sử dụng hàm thay đổi khoá TKIP. WPA cũng sử dụng thuật toán RC4 như WEP, nhưng mã hoá đầy đủ 128 bit. Và một đặc điểm khác là WPA thay đổi khoá cho mỗi gói tin. Các công cụ thu thập các gói tin để phá khoá mã hoá đều không thể thực hiện được với WPA. Bởi WPA thay đổi khoá liên tục nên hacker không bao giờ thu thập đủ dữ liệu mẫu để tìm ra mật khẩu.

Không những thế, WPA còn bao gồm kiểm tra tính toàn vẹn của thông tin (Message Integrity Check). Vì vậy, dữ liệu không thể bị thay đổi trong khi đang ở trên đường truyền. WPA có sẵn 2 lựa chọn: WPA Personal và WPA Enterprise. Cả 2 lựa chọn đều sử dụng giao thức TKIP, và sự khác biệt chỉ là khoá khởi tạo mã hóa lúc đầu. WPA Personal thích hợp cho gia đình và mạng văn phòng nhỏ, khoá khởi tạo sẽ được sử dụng tại các điểm truy cập và thiết bị máy trạm. Trong

khi đó, WPA cho doanh nghiệp cần một máy chủ xác thực và 802.1x để cung cấp các khoá khởi tạo cho mỗi phiên làm việc.

Lưu ý:

Có một lỗ hổng trong WPA và lỗi này chỉ xảy ra với WPA Personal. Khi mà sử dụng hàm thay đổi khoá TKIP được sử dụng để tạo ra các khoá mã hoá bị phát hiện, nếu hacker có thể đoán được khoá khởi tạo hoặc một phần của mật khẩu, họ có thể xác định được toàn bộ mật khẩu, do đó có thể giải mã được dữ liệu. Tuy nhiên, lỗ hổng này cũng sẽ bị loại bỏ bằng cách sử dụng những khoá khởi tạo không dễ đoán (đừng sử dụng những từ như "P@SSWORD" để làm mật khẩu).

Điều này cũng có nghĩa rằng kỹ thuật TKIP của WPA chỉ là giải pháp tạm thời, chưa cung cấp một phương thức bảo mật cao nhất. WPA chỉ thích hợp với những công ty mà không truyền dữ liệu "mật" về những thương mại, hay các thông tin nhạy cảm... WPA cũng thích hợp với những hoạt động hàng ngày và mang tính thử nghiệm công nghệ.

1.4.2.6 WPA2

Một giải pháp về lâu dài là sử dụng 802.11i tương đương với WPA2, được chứng nhận bởi Wi-Fi Alliance. Chuẩn này sử dụng thuật toán mã hoá mạnh mẽ và được gọi là Chuẩn mã hoá nâng cao AES. AES sử dụng thuật toán mã hoá đối xứng theo khối Rijndael, sử dụng khối mã hoá 128 bit, và 192 bit hoặc 256 bit. Để đánh giá chuẩn mã hoá này, Viện nghiên cứu quốc gia về Chuẩn và Công nghệ của Mỹ, NIST (National Institute of Standards and Technology), đã thông qua thuật toán mã đối xứng này.

Lưu ý:

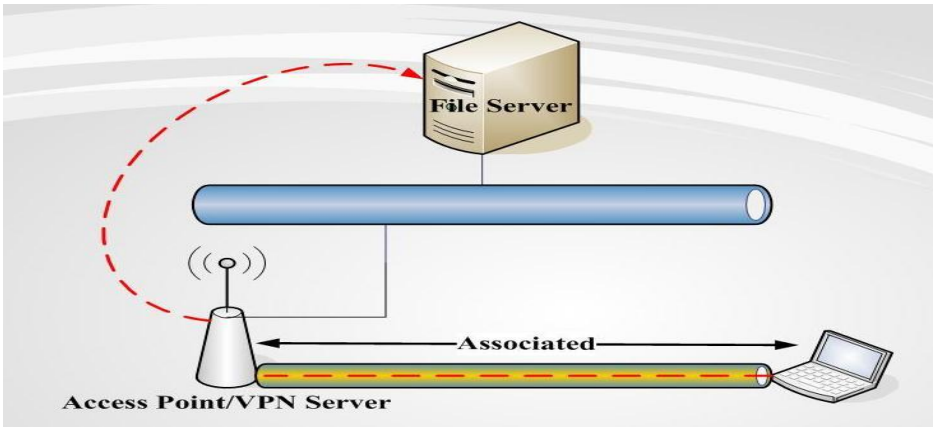
Chuẩn mã hoá này được sử dụng cho các cơ quan chính phủ Mỹ để bảo vệ các thông tin nhạy cảm.

Trong khi AES được xem như là bảo mật tốt hơn rất nhiều so với WEP 128 bit hoặc 168 bit DES (Digital Encryption Standard). Để đảm bảo về mặt hiệu năng, quá trình mã hoá cần được thực hiện trong các thiết bị phần cứng như tích hợp vào chip. Tuy nhiên, rất ít người sử dụng mạng không dây quan tâm tới vấn

đề này. Hơn nữa, hầu hết các thiết bị cầm tay Wi-Fi và máy quét mã vạch đều không tương thích với chuẩn 802.11i.

1.4.2.7 WLAN VPN

Mạng riêng ảo VPN bảo vệ mạng WLAN bằng cách tạo ra một kênh che chắn dữ liệu khỏi các truy cập trái phép. VPN tạo ra một tin cậy cao thông qua việc sử dụng một cơ chế bảo mật như IPSec (Internet Protocol Security). IPSec dùng các thuật toán mạnh như Data Encryption Standard (DES) và Triple DES (3DES) để mã hóa dữ liệu và dùng các thuật toán khác để xác thực gói dữ liệu. IPSec cũng sử dụng thẻ xác nhận số để xác nhận khóa mã (public key). Khi được sử dụng trên mạng WLAN, cổng kết nối của VPN đảm nhận việc xác thực, đóng gói và mã hóa.

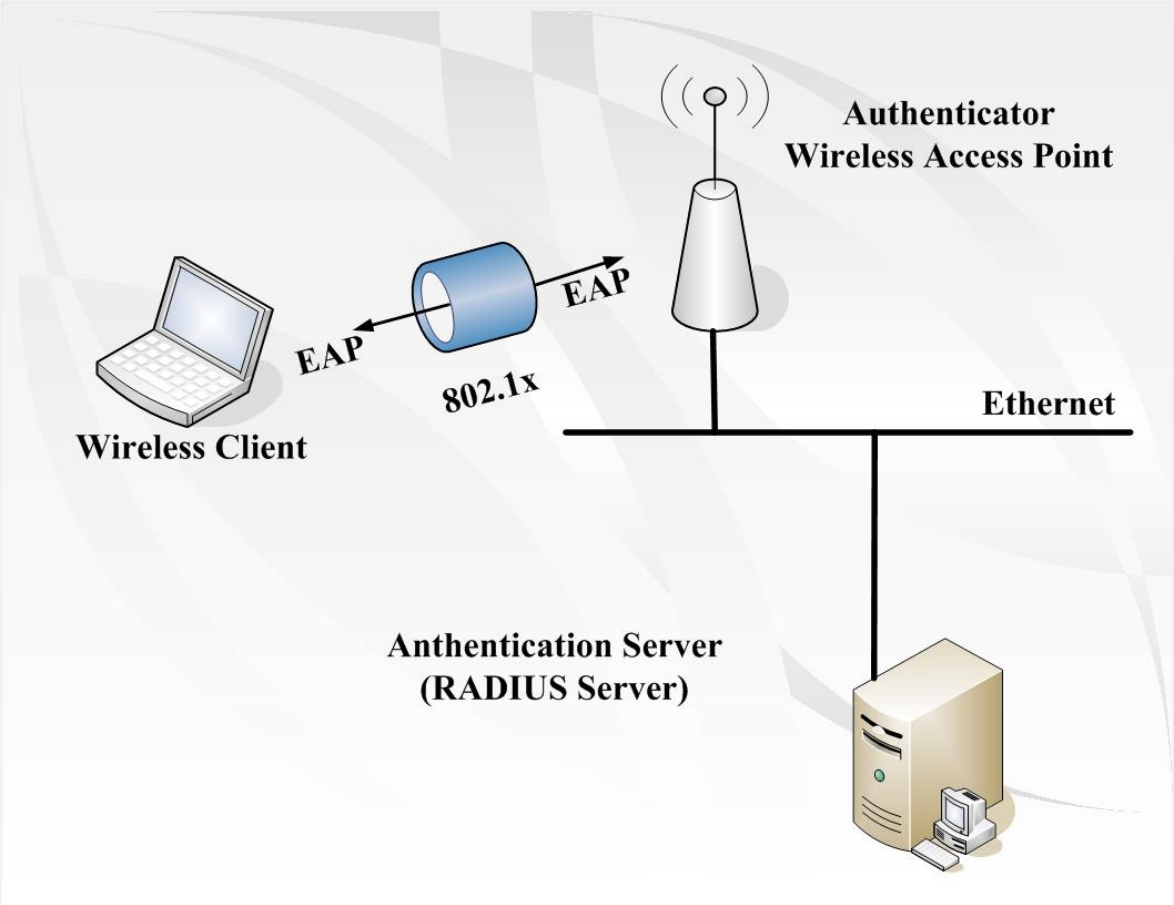


Hình1. 9: Mô tả xác thực qua VPN

Chương 2: HỆ THỐNG SMART WIFI MAKETING TẠI UBND QUẬN HỒNG BÀNG

2.1 Bảo mật WLAN bằng xác thực Radius Sever

2.1.1 Tổng quan hệ thống



Hình 2.1: Mô tả xác thực qua radiu sever

Việc bảo mật WLAN sử dụng chuẩn 802.1x kết hợp với xác thực người dùng trên Access Point (AP). Một máy chủ thực hiện việc xác thực trên nền tảng RADIUS có thể là một giải pháp tốt cung cấp xác thực cho chuẩn 802.1x.

Trong phần này này tôi sẽ giới thiệu cách thức làm việc của RADIUS và vì sao phải cần máy chủ RADIUS để hỗ trợ việc xác thực cho WLAN.

2.1.2 Xác thực, cấp phép , kiểm tra

Giao thức Remote Authentication Dial In User Service (RADIUS) được định nghĩa trong RFC 2865 như sau: Với khả năng cung cấp xác thực tập trung, cấp phép và điều khiển truy cập (Authentication, Authorization, và Accounting –

AAA) cho các phiên làm việc với SLIP và PPP Dial-up – như việc cung cấp xác thực của các nhà cung cấp dịch vụ Internet (ISP) đều dựa trên giao thức này để xác thực người dùng khi họ truy cập Internet.

Nó cần thiết trong tất cả các Network Access Server (NAS) để làm việc với danh sách các username và password cho việc cấp phép, RADIUS Access-Request sẽ chuyển các thông tin tới một Authentication Server, thông thường nó là một AAA Server (AAA – Authentication, Authoriztion, và Accounting). Trong kiến trúc của hệ thống nó tạo ra khả năng tập trung các dữ liệu, thông tin của người dùng, các điều kiện truy cập trên một điểm duy nhất (single point), trong khi có khả năng cung cấp cho một hệ thống lớn, cung cấp giải pháp NASs.

Khi một user kết nối, NAS sẽ gửi một message dạng RADIUS Access-Request tới máy chủ AAA Server, chuyển các thông tin như username và password, thông qua một port xác định, NAS identify, và một message Authenticator.

Sau khi nhận được các thông tin máy chủ AAA sử dụng các gói tin được cung cấp như NAS identify, và Authenticator thẩm định lại việc NAS đó có được phép gửi các yêu cầu đó không. Nếu có khả năng, máy chủ AAA sẽ tìm kiểm tra thông tin username và password mà người dùng yêu cầu truy cập trong cơ sở dữ lệu. Nếu quá trình kiểm tra là đúng thì nó sẽ mang một thông tin trong Access-Request quyết định quá trình truy cập của user đó là được chấp nhận.

Khi quá trình xác thực bắt đầu được sử dụng, máy chủ AAA có thể sẽ trả về một RADIUS Access-Challenge mang một số ngẫu nhiên. NAS sẽ chuyển thông tin đến người dùng từ xa (với ví dụ này sử dụng CHAP). Khi đó người dùng sẽ phải trả lời đúng các yêu cầu xác nhận (trong ví dụ này, đưa ra lời đề nghị mã hoá password), sau đó NAS sẽ chuyển tới máy chủ AAA một message RADIUS Access-Request.

Nếu máy chủ AAA sau khi kiểm tra các thông tin của người dùng hoàn toàn thoả mãn sẽ cho phép sử dụng dịch vụ, nó sẽ trả về một message dạng RADIUS Access-Accept. Nếu không thoả mãn máy chủ AAA sẽ trả về một tin RADIUS Access-Reject và NAS sẽ ngắt kết nối với user.

Khi một gói tin Access-Accept được nhận và RADIUS Accounting đã được thiết lập, NAS sẽ gửi mộtgói tin RADIUS Accounting-Request (Start) tới máy chủ AAA. Máy chủ sẽ thêm các thông tin vào file Log của nó, với việc NAS sẽ cho phép phiên làm việc với user bắt đầu khi nào, và kết thúc khi nào, RADIUS Accouting làm nhiệm vụ ghi lại quá trình xác thực của user vào hệ thống, khi kết thúc phiên làm việc NAS sẽ gửi một thông tin RADIUS Accounting-Request (Stop).

2.1.3 Sự bảo mật và tính mở rộng

Tất cả các message của RADIUS đều được đóng gói bởi UDP datagrams, nó bao gồm các thông tin như: message type, sequence number, length, Authenticator, và một loạt các Attribute-Value.

Authenticator: Tác dụng của Authenticator là cung cấp một chế độ bảo mật. NAS và AAA Server sử dụng Authenticator để hiểu được các thông tin đã được mã hóa của nhau như mật khẩu chẳng hạn. Authenticator cũng giúp NAS phát hiện sự giả mạo của gói tin RADIUS Responses. Cuối cùng, Authenticator được sử dụng làm cho để biễn password thành một dạng nào đó, ngăn chặn việc làm lộ mật khẩu của người dùng trong các message RADIUS.

Authenticator gửi Access-Request trong một số ngẫu nhiên. MD5 sẽ băm (hash) số ngẫu nhiên đó thành một dạng riêng là OR’ed cho mật khẩu của người dùng và gửi trong Access-Request User-Password. Toàn bộ RADIUS response sau đó được MD5 băm (hash) với cùng thông số bảo mật của Authenticator, và các thông số response khác.

Authenticator giúp cho quá trình giao tiếp giữa NAS và máy chủ AAA được bảo mật nhưng nếu kẻ tấn công tóm được cả hai gói tin RADIUS Access-Request và Access-Response thì có thể thực hiện "dictionary attack" để phân tích việc đóng gói này. Trong điều kiện thực tế để việc giải mã khó khăn bạn cần phải sử dụng những thông số dài hơn, toàn bộ vấn đề có khả năng nguy hại cho quá trình truyền tải này được miêu tả rất kỹ trong RFC 3580.

Attribute-Value Pairs: Thông tin được mang bởi RADIUS được miêu tả trong một dạng Attribute-Value, để hỗ trợ cho nhiều công nghệ khác nhau, và

nhiều phương thức xác thực khác nhau. Một chuẩn được định nghĩa trong Attribute-Value pairs (cặp đôi), bao gồm User-Name, User-Password, NAS-IPAddress, NAS-Port, Service-Type. Các nhà sản xuất (vendors) cũng có thể định nghĩa Attribute-Value pairs để mang các thông tin của mình như Vendor-Specific toàn bộ ví dụ này được miêu tả trong RFC 2548 - Định nghĩ Microsoft *Attribute-Vlue pair trong* MS-CHAP.

Thêm vào đó, rất nhiều chuẩn Attribute-Value pairs được định nghĩa trong nhiều năm để hỗ trợ Extensible Authentication Protocol (EAP), một dạng khác cũ hơn của nó là PAP và CHAP dial-up protocol. Bạn có thể tìm thấy trong tài liệu RFC 3579 cho phiên bản mới nhất của RADIUS hỗ trợ EAP. Trong phần này sẽ nói rất rõ về hỗ trợ xác thực cho WLAN, từ khi chuẩn EAP được sử dụng cho 802.1x Port Access Control để cho phép xác thực từ bên ngoài cho wireless.

2.1.4 Áp dụng cho WLan

Trong một mạng Wireless sử dụng 802.1x Port Access Control, các máy trạm sử dụng wireless với vai trò Remote User và Wireless Access Point làm việc như một Network Access Server (NAS). Để thay thế cho việc kết nối đến NAS với dial-up như giao thức PPP, wireless station kết nối đến Access Point bằng việc sử dụng giao thức 802.11.

Một quá trình được thực hiện, wireless station gửi một message EAP-Start tới Access Point. Access Point sẽ yêu cầu station nhận dạng và chuyển các thông tin đó tới một AAA Server với thông tin là RADIUS Access-Request User-Name attribute.

Máy chủ AAA và wireless station hoàn thành quá trình bằng việc chuyển các thông tin RADIUS Access-Challenge và Access-Request qua Access Point. Được quyết định bởi phía trên là một dạng EAP, thông tin này được chuyển trong một đường hầm được mã hoá TLS (Encypted TLS Tunnel).

Nếu máy chủ AAA gửi một message Access-Accept, Access Point và wireless station sẽ hoàn thành quá trình kết nối và thực hiện phiên làm việc với việc sử dụng WEP hay TKIP để mã hoá dữ liệu. Và tại điểm đó, Access Point sẽ không

cấm cổng và wireless station có thể gửi và nhận dữ liệu từ hệ thống mạng một cách bình thường.

Cần lưu ý là mã hoá dữ liệu từ wireless station tới Access Point khác với quá trình mã hoá từ Access Point tới máy chủ AAA Server (RADIUS Server).

Nếu máy chủ AAA gửi một message Access-Reject, Access Point sẽ ngắt kết nối tới station. Station có thể cố gắng thử lại quá tình xác thực, nhưng Access Point sẽ cấm station này không gửi được các gói tin tới các Access Point ở gần đó. Chú ý là station này hoàn toàn có khả năng nghe được các dữ liệu được truyền đi từ các stations khác – Trên thực tế dữ liệu được truyền qua sóng radio và đó là câu trả lời tại sao bạn phải mã hoá dữ liệu khi truyền trong mạng không dây.

2.1.5 Các Tùy Chọn bổ sung

Một vấn đề đầu tiên bạn phải hiểu vai trò của RADIUS trong quá trình xác thực của WLAN, bạn phải thiết lập một máy chủ AAA hỗ trợ interaction.

Nếu bạn có một máy chủ AAA trong mạng gọi là RADIUS, nó đã sẵn sàng để hỗ trợ xác thực cho chuẩn 802.1x và cho phép chọn lựa các dạng EAP. Nếu đã có bạn chuyển tiếp đến bước tiếp theo là làm thế nào để thiết lập tính năng này.

Nếu bạn có một RADIUS – AAA Server không hỗ trợ 802.1x, hoặc không hỗ trợ các dạng EAP, bạn có thể lựa chọn bằng cách cập nhật các phiên bản phần mềm mới hơn cho server, hay bạn có thể cài đặt một máy chủ mới. Nếu bạn cài đặt một máy chủ AAA hỗ trợ xác thực cho chuẩn 802.1x, bạn có thể sử dụng tính năng RADIUS proxy để thiết lập một chuỗi các máy chủ, cùng chia sẻ chung một cơ sở dữ liệu tập trung, RADIUS proxy có thể sử dụng để chuyển các yêu cầu xác thực tới máy chủ có khả năng xác thực qua chuẩn 802.1x.

Nếu bạn không có một RADIUS – là máy chủ AAA, bạn cần thiết phải cài đặt một máy chủ cho quá trình xác thực của WLAN, lựa chọn cài đặt này là một công việc thú vị.

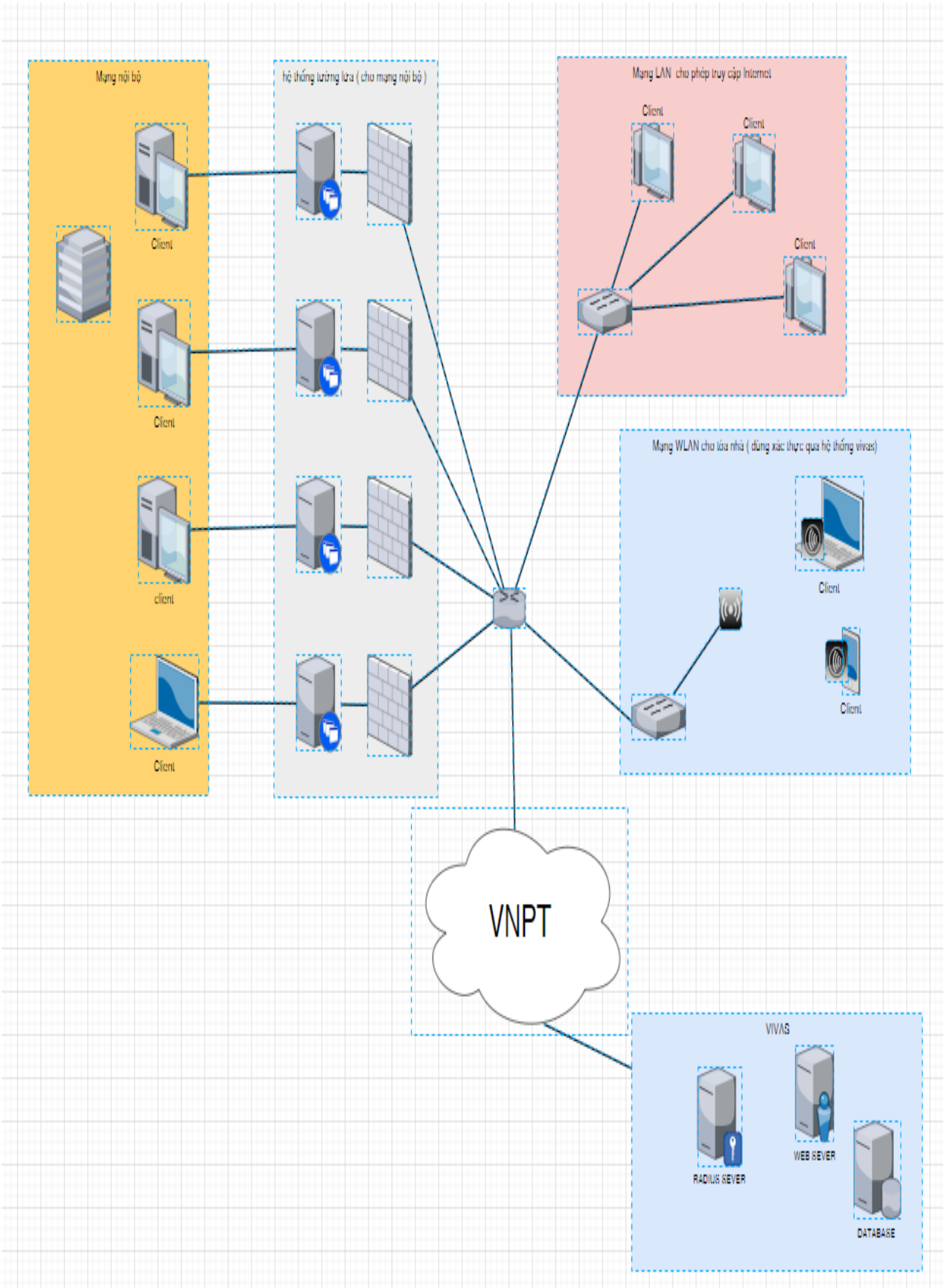
Với cơ sở tập trung - Giải pháp sử dụng RADIUS cho mạng WLAN là rất quan trọng bởi nếu một hệ thống mạng của bạn có rất nhiều Access Point việc cấu hình để bảo mật hệ thống này là rất khó nếu quản lý riêng biệt, người dùng có thể xác thực từ nhiều Access Point khác nhau và điều đó là không bảo mật.

Khi sử dụng RADIUS cho WLAN mang lại khả năng tiện lợi rất cao, xác thực cho toàn bộ hệ thống nhiều Access Point, … cung cấp các giải pháp thông minh hơn.

2.2. Hệ thống smart wifi marketing được triển khai ở tòa nhà UBND quận Hồng Bàng

2.2.1 Sơ đồ cầu trúc mạng hiện có ở tòa nhà

Tòa nhà ủy ban nhân dân quận Hồng bàng là một tòa nhà có cấu trúc 7 tầng, bao gồm nhiều phòng chức năng phục vụ các phòng ban chuyên trách khác nhau. Do đó việc thiết lập hệ thống wifi ở mỗi vị trí khu vực là khác nhau. Từ nhu cầu có chung ta sẽ có sơ đồ khối tổng quát cho cấu trúc mạng ở toàn nhà.



Hình 2.1: Cấu trúc mạng tại tòa nhà UBND quận Hồng Bàng

Dựa vào sơ đồ này chúng ta có thể thấy được, cấu trúc mạng sẽ được phân ra làm các vùng như sau :

Vùng mạng nội bộ : Phục vụ các máy tính có yêu cầu bảo mật cao (khối đảng ủy, khối kế toán ….) chỉ có mạng kết nối có dây

Vụng mạng Lan có truy cập internet : Phục vụ các máy tính có tính bảo mật thấp hơn, có nhu cầu kết nối ra bên ngoài internet, không thể kết nối với các máy tính trong vùng mạng nội bộ .

Vùng mạng Wlan : phục vụ các thiết bị cá nhân có kết nối wifi kết nối ra ngoài, không thể kết nối với mạng nội bộ và phải xác thực bằng radius sever. Dịch vụ này được cung cấp bởi công ty vivas

2.2.2 Giới thiệu VIVAS

Thành viên của VNPT Technology, thuộc tập đoàn Bưu chính Viễn thông Việt Nam (VNPT)

Đơn vị sở hữu các giải pháp công nghệ: CDN, SDP, Wifi Platform, OTT, TVOD, AI & Data Analytics

Cạnh tranh bằng chất lượng dịch vụ với đội ngũ trẻ năng động, tâm huyết và hỗ trợ tức thời 24/7, mang đến cho khách hàng sự hài lòng với mức chi phí hợp lý nhất.

Kinh nghiệm PTSP tích hợp, cung cấp nền tảng và vận hành cho VNPT, trong đó giải pháp Wifi tích hợp với thiết bị của VNPT Technology trong các dự án Wifi

Marketing tại HN, QN, BN, TPHCM, BRVT,… Ngoài thị trường VNPT, VIVAS là đơn vị cung cấp giải pháp marketing (Wifi Marketing, Mobile Marketing,…) cho KHDN chuỗi lớn như Agribank, PNJ, Coopmart, Lotte Mart, Vua Nệm, Guardian, LUG, … giúp tăng độ nhận diện thương hiệu và tăng trưởng kinh doanh.

Hơn 10 năm kinh nghiệm trong lĩnh vực quảng cáo trên di động và cung cấp giải pháp cho doanh nghiệp SMEs và đa quốc gia (hơn 1000 khách hàng và đại lý)

2.2.3 Wifi maketig là gì ?

WiFi Marketing là hình thức sử dụng wifi như một phương tiện phục vụ cho việc tiếp thị, truyền thông và quảng bá thương hiệu, sản phẩm, dịch vụ của Doanh nghiệp

WiFi Marketing cho phép Doanh nghiệp triển khai chương trình marketing và chăm sóc khách hàng qua nhiều định dạng: Hình ảnh, Video, Game… và có khả năng tương tác cao đến một số lượng khách hàng lớn

Wifi Marketing cũng là một kênh truyền thông vô cùng hiểu quả với khối chính quyền, do tính dễ tiếp cân với người sử dụng

Mục đích

▪ Tạo dấu ấn về thương hiệu trong tâm trí khách hàng

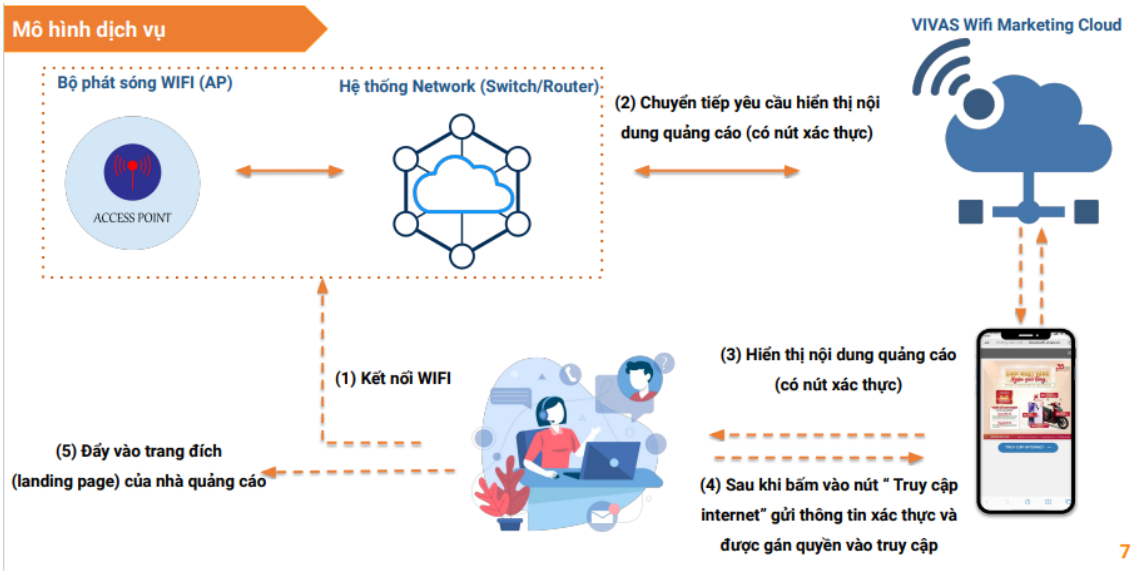
▪ Lôi cuốn, thu hút thêm khách hàng

▪ Quảng cáo cho sản phẩm, dịch vụ

▪ Thu nhập thông tin khách hàng để phục vụ công tác chăm sóc, tiếp thị hậu bán hang

▪ Tuyên truyền chính sách, hỗ trợ hướng dẫn công dân

Hệ thống vivas sủ dụng xác thực qua sever Radius được VIVAS xây dựng sẵn



Hình 2.3: Mô tả dịch vụ của VIVAS

2.2.4 Quy trình sử dụng

Hình 2.4: Mô tả quy trình sử dụng

- ✓ Khách hàng kết nối Wifi miễn phí trên thiết bị di động, tablet, laptop
- ✓ Hệ thống dẫn tới trang captive portal đã được thiết lập
- ✓ Điều kiện truy cập: Xem quảng cáo (banner/video, …) hoặc Thực hiện khảo sát/ Nhập thông tin,...
- ✓ Truy cập Wifi miễn phí

2.2.5 Hướng dẫn thiết lập thiết bị

Thiết bị được đề xuất dùng cho hệ thống này sẽ có như sau

Thiết bị định tuyến : Mikrotik 750rbg

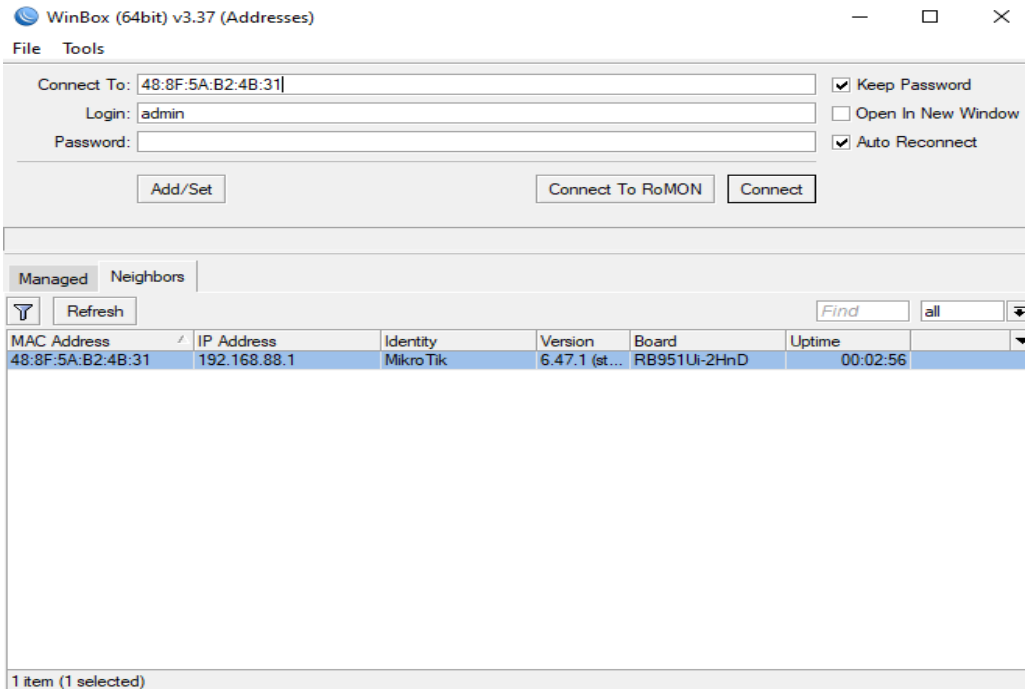
Thiết bị phát wifi : Ruijie reyee RAP- 2200E

Các bước cài đặt được thực hiện như sau

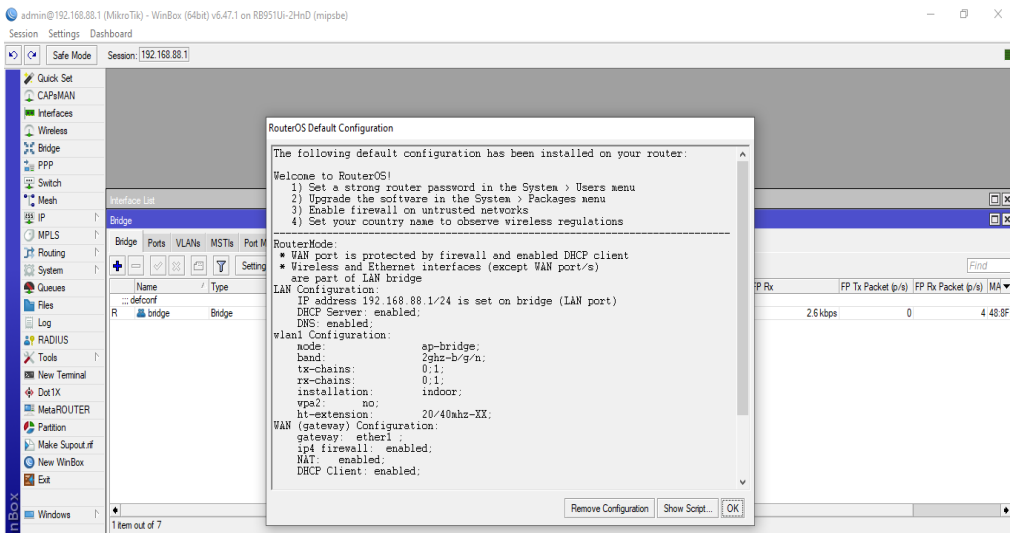
Đăng nhập vào winbox

Download phần mềm winbox từ địa chỉ:https://mikrotik.com/download

Trên giao diện WinBox sẽ hiển thị địa chỉ MAC port kết nối như hình dưới sau đó Connect vào giao diện config

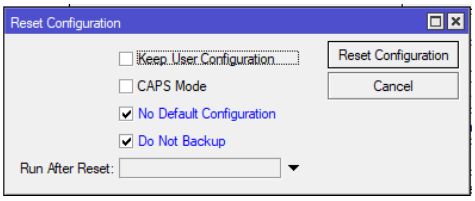


- Giao diện cấu hình của WinBox hiển thị như hình



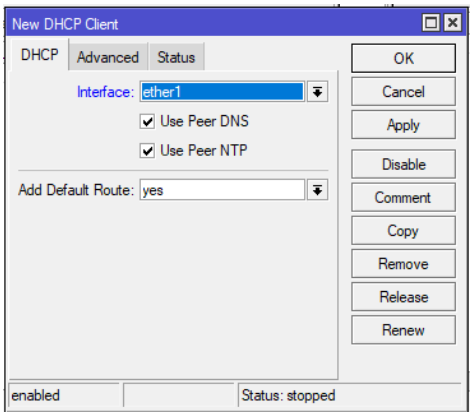
1. **Reset router Mikrotik về cấu hình mặc định, config DHCP Client, thực hiện Nat Interface Ether1 ra Internet**

B1: Reset router không giữ cấu hình mặc định: System → Reset Configuration → Tích chọn các checkbox

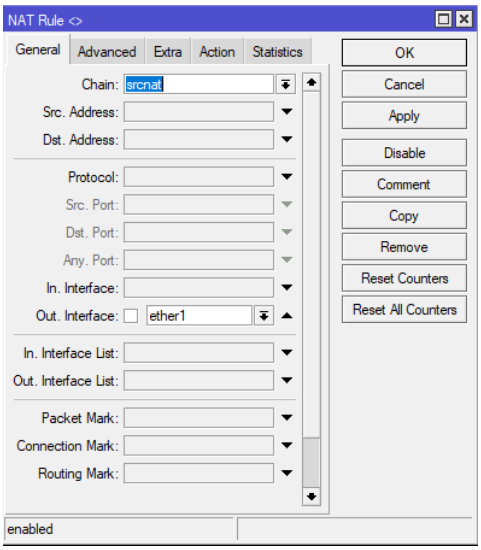


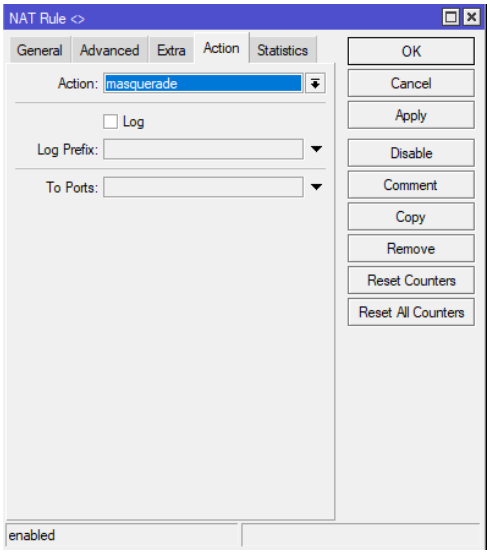
B2: Cắm đường kết nối internet vào port ether1

B3: Cấu hình DHCP Client: IP→DHCP → config DHCP Client như hình



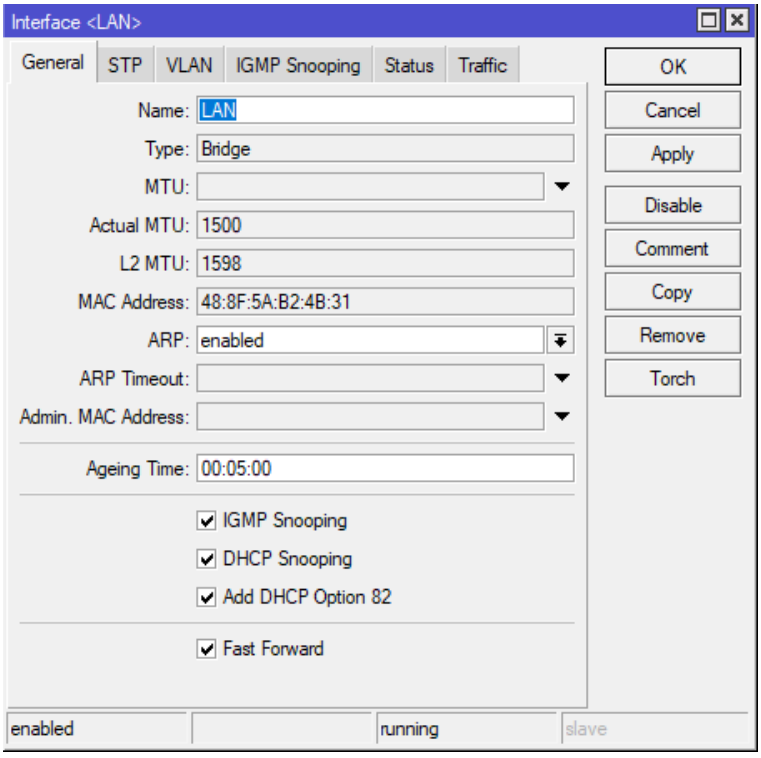
B4: Thực hiện NAT các port còn lại ra internet qua port ether1: IP → Firewall → NAT config như hình dưới



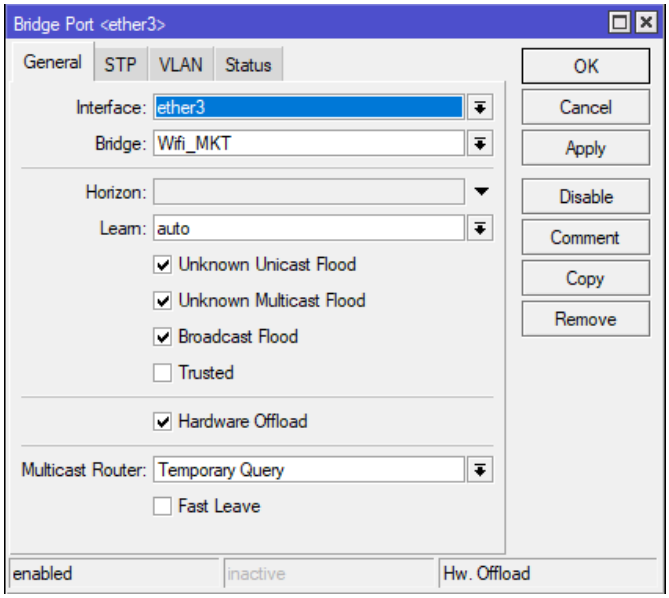


2. Tạo Bridge và add port vào bridge tương ứng

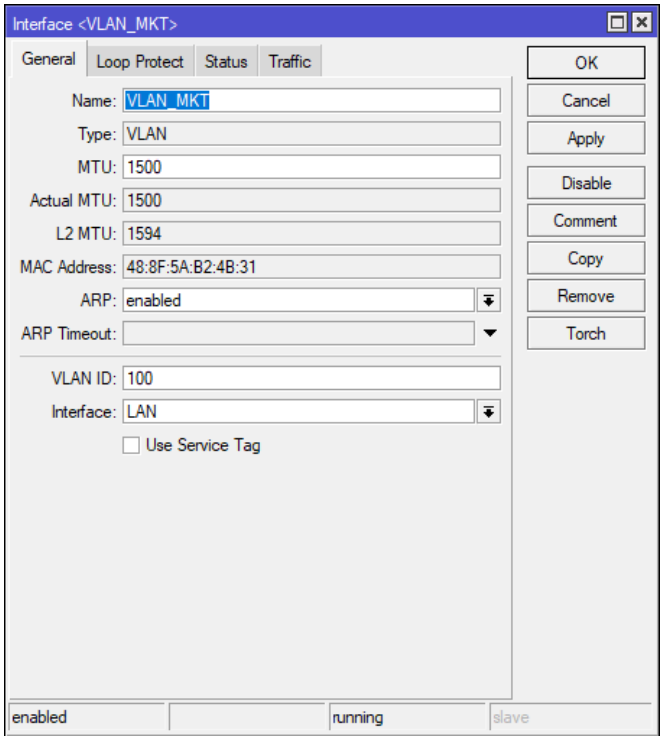
B1: Tạo Bridge: Bridge → Add → config như hình



B2: Thêm các port vào bridge : Bridge → Port → Add → Interface (Thêm port vào Bridge ngoại trừ ether1)

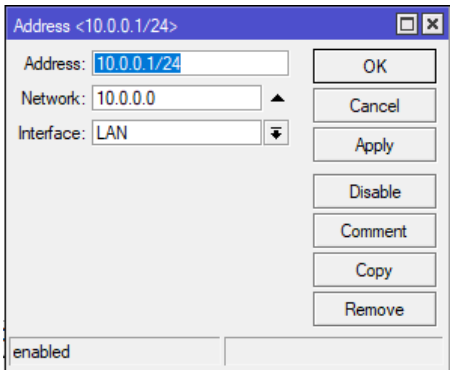


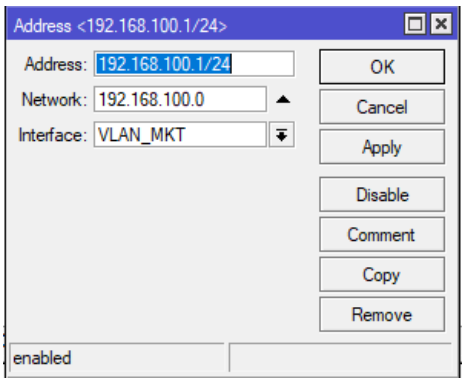
B3: Tạo Vlan trên Bridge: Interfaces→ chuột phải vào Bridge → Add → VLAN_MKT (VLAN ID: 100)



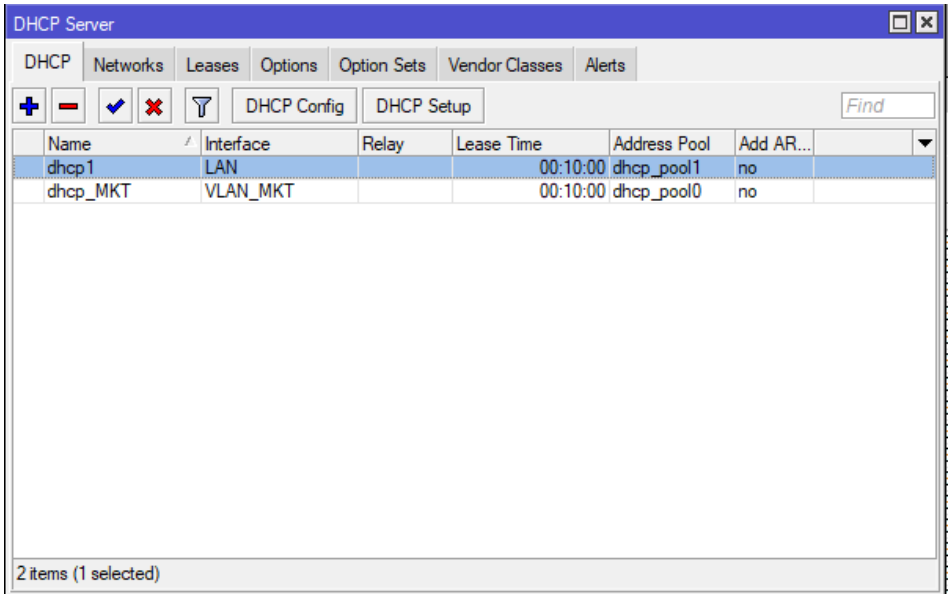
3. **Tạo địa chỉ IP và gán DHCP Server cho Bridge và VLAN_MKT**

B1: Tạo địa chỉ IP cho Bridge và VLAN_MKT : IP → Addressess → Add



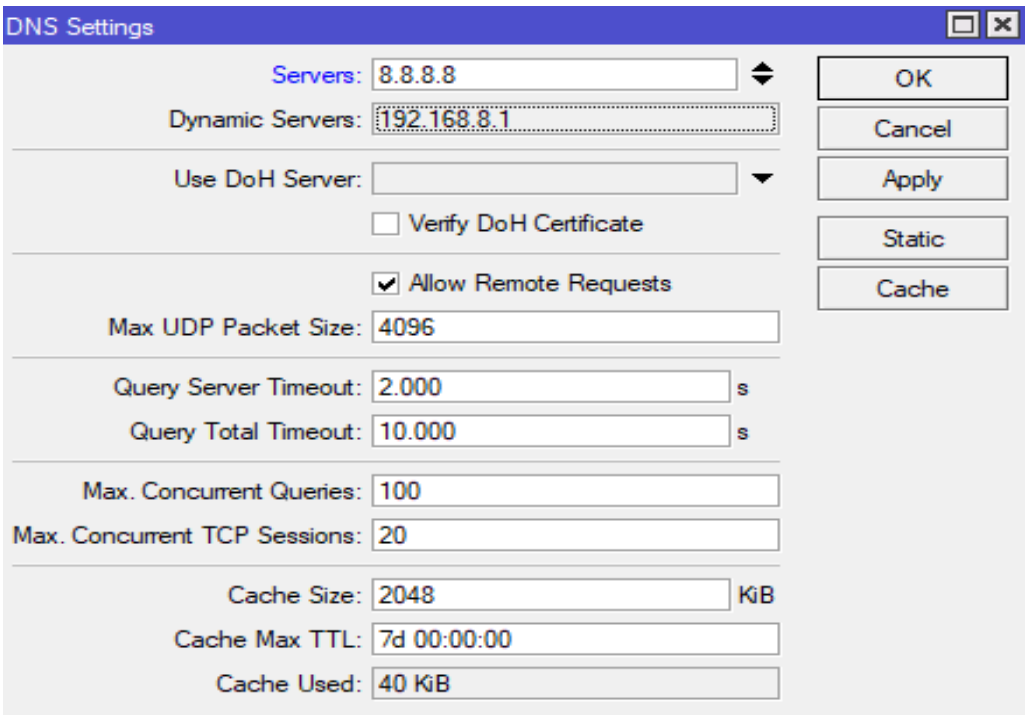


B2: Tạo DHCP server cho Bridge và VLAN : IP →DHCP Server → DHCP setup → chọn Bridge và VLAN muốn cấp phát DHCP → Next



4. Config DNS, Radius, Hotspot cho Router Mikrotik

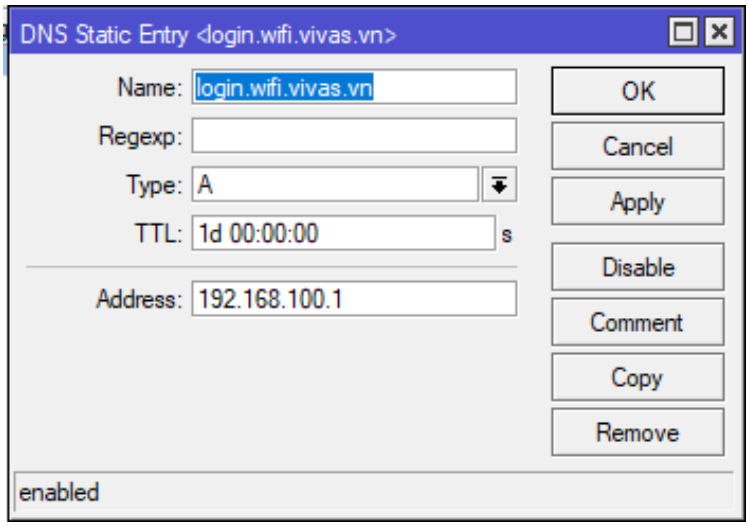
B1: Khai báo DNS: IP → DNS → Servers: nhập 8.8.8.8



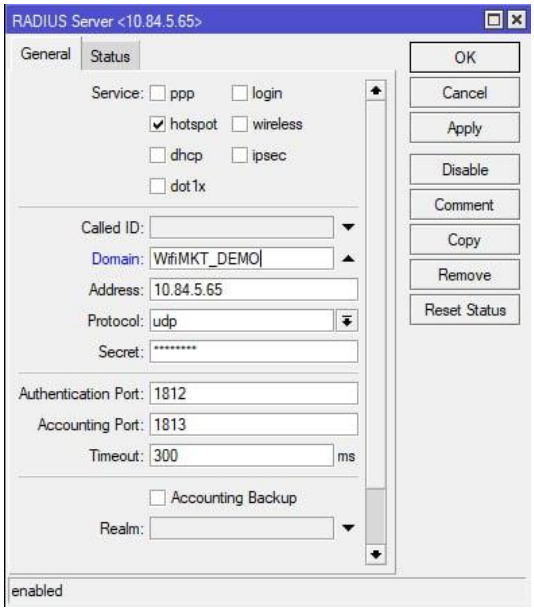
B2: Tại tab Static → khai báo domain

Name: login.wifi.vivas.vn

Address: Nhập địa chỉ VLAN cấp WifiMarketing



B3: Cấu hình RADIUS: RADIUS→ Add → Config thông tin như hình

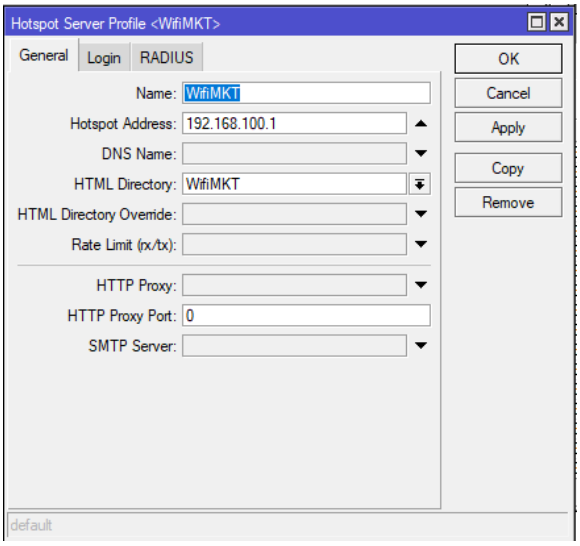


- Domain: Nhập tên Domain
- Address: **103.31.127.188**
- Secret: **068e022a**
- Các port mặc định.

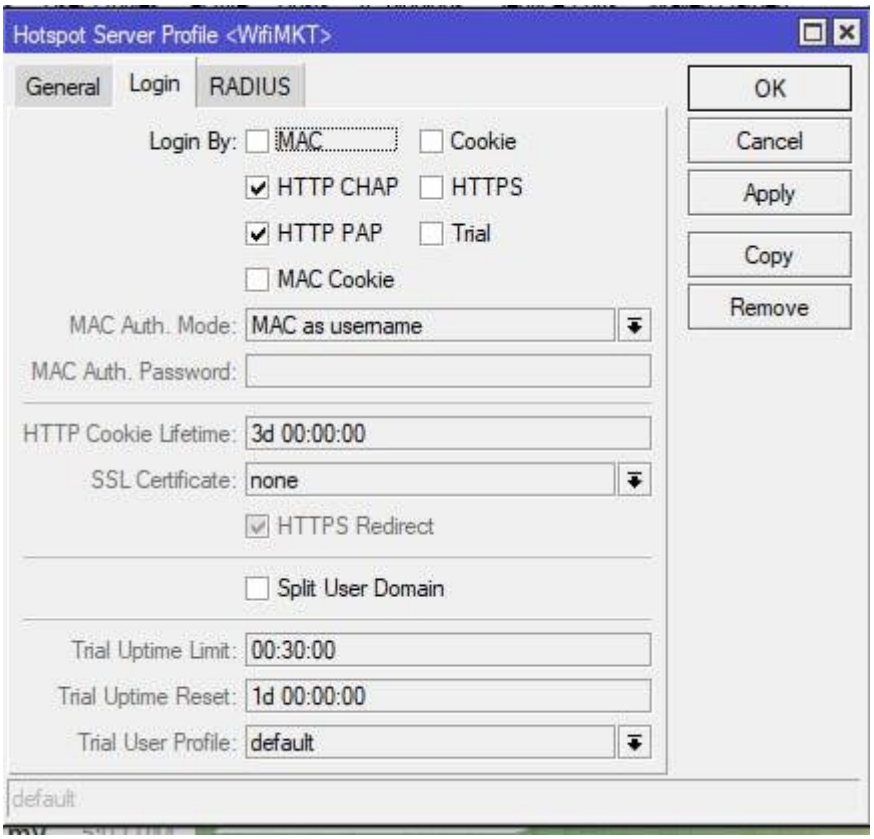
B4: Cấu hình IP -> Hotspot:

Tab Server Profiles → tab General

- Name: WifiMKT
- Hotspot Address: Địa chỉ của VLAN cấp WifiMarketing
- DNS Name:
- HTML Directory: tên thư mục chứa file login.html của Mikrotik (chứa link -> captive portal)

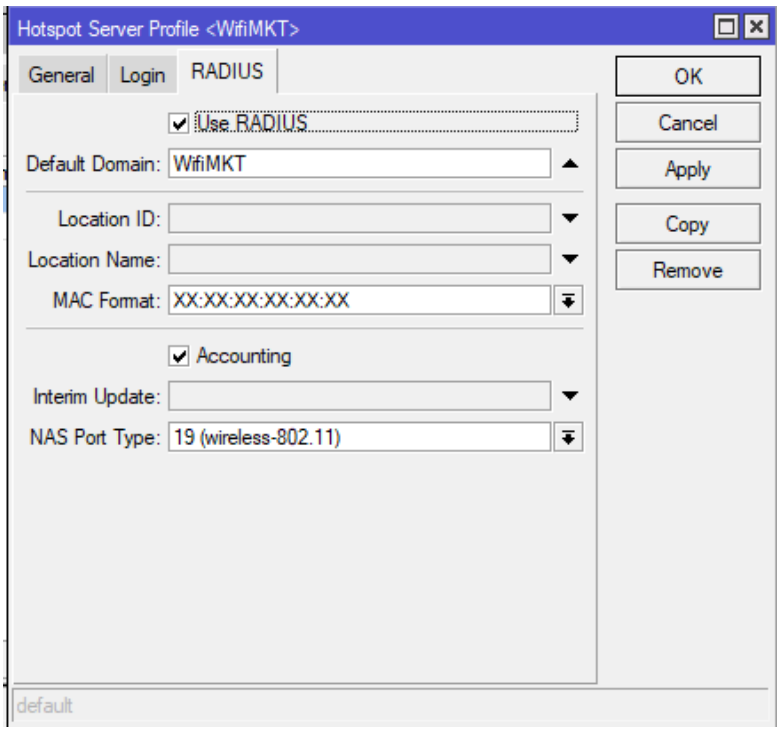


Tại tab Login cấu hình như hình

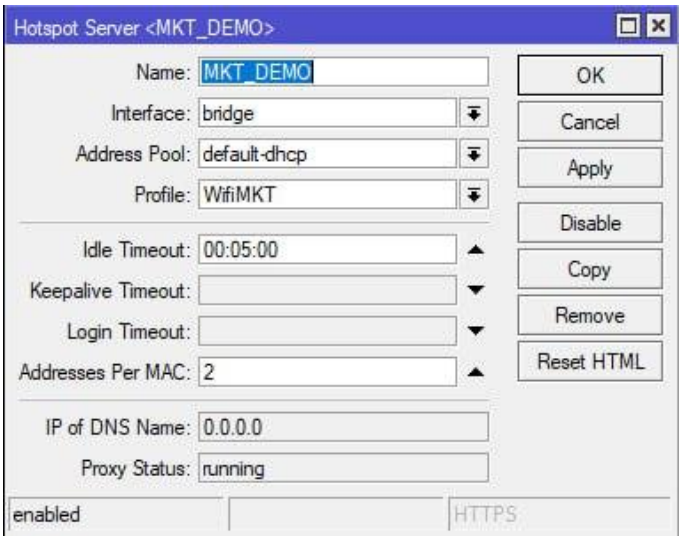


Tại tab RADIUS

- **Default domain**: nhập tên domain khai báo tại RADIUS



IP→ Hotspot → tab Servers →Add → Config như hình



Name: Đặt tùy ý

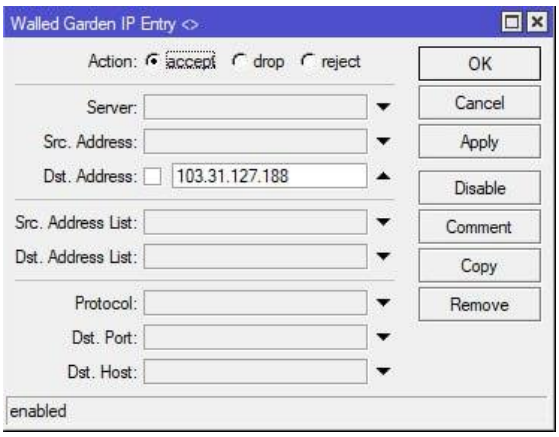
Interface: chọn VLAN cấp WifiMarketing

Address Pool: chọn DHCP tương ứng với VLAN

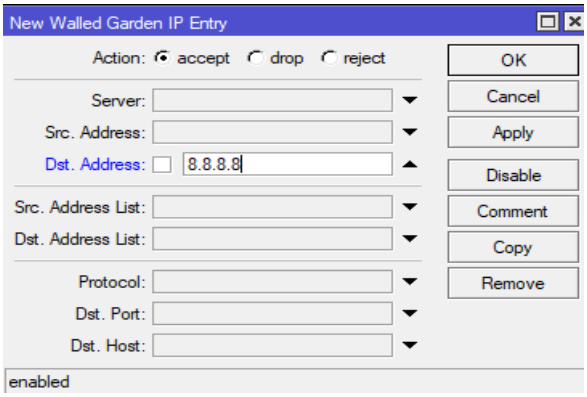
Profile: chọn Server Profiles vừa tạo (WifiMKT)

IP→ Hotspot → Walled Garden IP Entry → Add

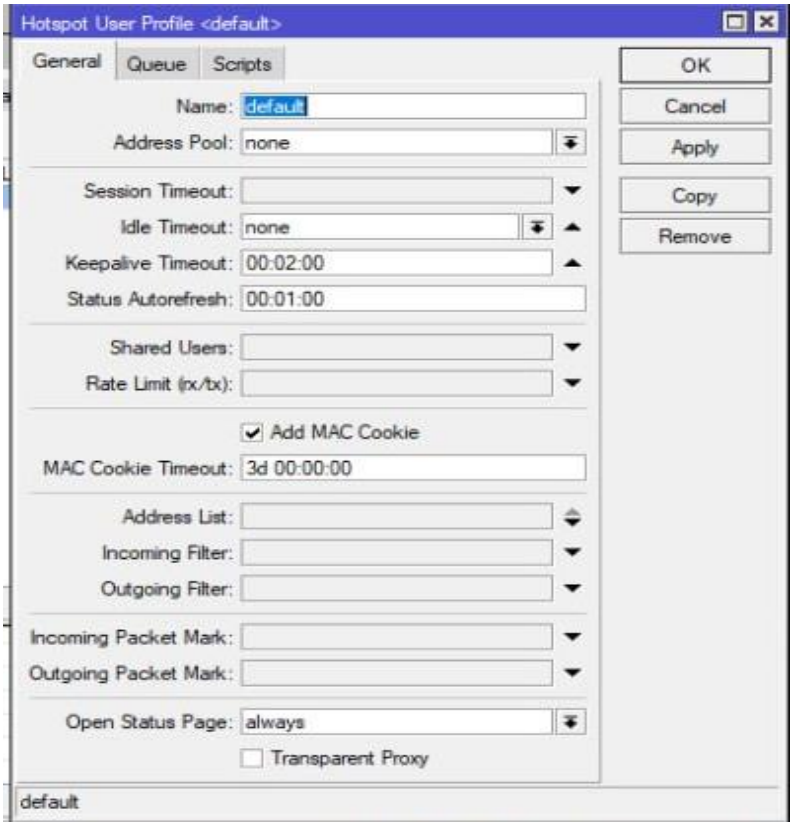
- Dst. Address: 103.31.127.188



- Nếu không phân giải được tên miền, tạo thêm 1 Entry với Dst. Address: 8.8.8.8



IP→ Hotspot → User Profiles → Sửa file default



Shared Users : đổi thành 1 → 0

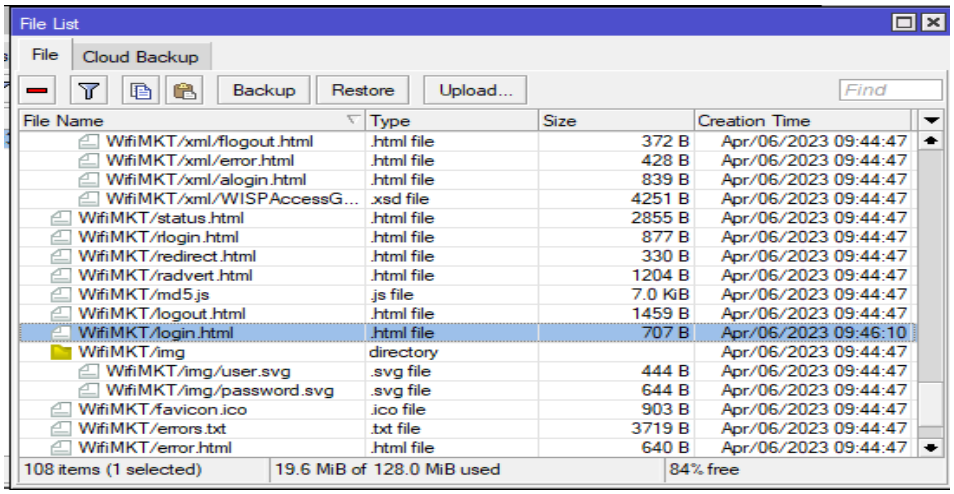
5. Chỉnh sửa file login.html và thêm vào HTML Directory :

B1: Sửa file login.html:

```
<html>
<head>
<title>Hidden Page</title>
<style>
   body {
      display: none;
   }
</style>
</head>
<form name="redirect" action="http://cloud.wifi-demo.vivas.vn/index.php" method="GET">
<input type="hidden" name="r" value="site/index">
<input type="hidden" name="device_id" value="ID_diemtruycap">
<input type="hidden" name="mac" value="MAC address E01">
<input type="hidden" name="t" value="sc">
</form>
<script language="JavaScript">
<!--
  document.redirect.submit();
//-->
</script></center>
</body>
</html>
```

device_id	ID của thiết bị AP GrandStream được cấp sau khi đăng ký điểm truy cập trên trang quản trị.
mac	MAC E01 phía sau thiết bị Mikrotik

B2: Kéo thả lại file login.html sau khi sửa vào HTML Directory khai báo tại Hotspot Server Profile



B3: Sửa file alogin.html trong HTML Directory

```
<!doctype html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0" />
  <meta http-equiv="refresh" content="2; url=$(link-redirect)">
  <meta http-equiv="pragma" content="no-cache">
  <meta http-equiv="expires" content="-1">
  <script>
    function startClock() {
      $(if popup == 'true')
      open('$(link-status)', 'hotspot_status', 'toolbar=0,location=0,directories=0,status=0,menubars=0,resizable=1,width=290,height=200');
    $(endif)
    location.href = unescape('$(link-redirect-esc)');
    }
  </script>
</head>
</html>
```

Sau khi cấu hình xong, các thiết bị muốn kết nối vào wifi sẽ hiện lên một trang portal có hình ành truyền thông và người dung sẽ phải xem hết thông tin và chọn kết nối internet để có thể vào mạng. như mô tả phía dưới.

Hình 2.5: Mô tả kết quả sau khi thực hiện

KẾT LUẬN

Thông qua việc tìm hiểu về mạng không dây đặc biệt là mạng cục bộ không dây, tôi đã có được các kiến thức về các chuẩn, cấu trúc mạng, các vấn đề bảo mật và khi triển khai hệ thống mạng cục bộ không dây. Việc phát triển mạng không dây thật sự đem lại hiệu quả với sự thuận lợi khi sử dụng các thiết bị có tính di động cao và vấn đề bảo mật được đặt lên hàng đầu.

Do vậy tôi đã chọn phương pháp xác thực RADIUS Server kết hợp với phương pháp mã hóa WPA2 nhằm đề xuất giải pháp bảo mật WLAN.

Và với việc sử dụng dịch vụ của một đối tác như VIVAS việc tạo và quản lý hệ thống mạng wifi đã đơn giản hơn rất nhiều. Đồng thời việc tích hợp thêm các thông tin quảng bá vào hệ thống cũng làm cho tăng tính hiệu quả của việc sử dụng mạng wifi

TÀI LIỆU THAM KHẢO

1. Nguyễn Huy Thành-NXB 2006 " Nghiên cứu lựu chọn công nghệ giải pháp xây dựng mạng MAN cáp quang, luận văn thạc sỹ, Học viện công nghệ bưu chính viễn thông"

2. Thạc sỹ Nguyễn Quý Minh Hiển, Đỗ Kim Bằng-NXB 2002 " Mạng viễn thông hệ sau"

3. Nhà xuất bản bưu điện-NXB 2005 " Công nghệ IP,WDW"