BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC QUẢN LÝ VÀ CÔNG NGHỆ HẢI PHÒNG

ĐỒ ÁN TỐT NGHIỆP

NGÀNH : CÔNG NGHỆ THÔNG TIN

Sinh viên : VŨ ĐỨC HIẾU

Giảng viên hướng dẫn: NGUYỄN NHƯ CHIẾN

NGUYỄN THỊ XUÂN HƯƠNG

HẢI PHÒNG – 2022

BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC QUẢN LÝ VÀ CÔNG NGHỆ HẢI PHÒNG

TÌM HIỂU, PHÂN TÍCH VÀ ĐỀ XUẤT GIẢI PHÁP BẢO MẬT KHI TRIỂN KHAI MẠNG WLAN SỬ DỤNG GIAO THỨC WPA3

ĐỒ ÁN TỐT NGHIỆP ĐẠI HỌC HỆ CHÍNH QUY

NGÀNH: CÔNG NGHỆ THÔNG TIN

Sinh viên : VŨ ĐỨC HIẾU

Giảng viên hướng dẫn: NGUYỄN NHƯ CHIẾN

NGUYỄN THỊ XUÂN HƯƠNG

HẢI PHÒNG – 2022

BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC QUẢN LÝ VÀ CÔNG NGHỆ HẢI PHÒNG

NHIỆM VỤ ĐỀ TÀI TỐT NGHIỆP

Sinh viên : Vũ Đức Hiếu **Mã SV** : 1812111010

Lớp : CT2201M **Ngành** : Công nghệ thông tin

Tên đề tài: Tìm hiểu, phân tích và đề xuất giải pháp bảo mật khi triển khai mạng WLAN sử dụng giao thức WPA3

CÁN BỘ HƯỚNG DẪN ĐỀ TÀI TỐT NGHIỆP

Họ và tên :

Học hàm, học vị :

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

Nội dung hướng dẫn:

Đề tài tốt nghiệp được giao ngày 04 tháng 04 năm 2022

Yêu cầu phải hoàn thành xong trước ngày 24 tháng 06 năm 2022

Đã nhận nhiệm vụ ĐTTN	Đã giao nhiệm vụ ĐTTN
Sinh viên	*Giảng viên hướng dẫn*

Hải Phòng, ngày tháng năm 2022

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:

Họ và tên sinh viên: Ngành: Công nghệ thông tin

Nội dung hướng dẫn:

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

……..…....

……..……

……..……

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

……..……

……..……

……..……

……..……

……..……

3. Ý kiến của giảng viên hướng dẫn tốt nghiệp

Đạt ☐ Không đạt ☐ Điểm:……

Hải Phòng, ngày.....tháng 07 năm 2022

Giảng viên hướng dẫn

(Ký và ghi rõ họ tên)

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

PHIẾU NHẬN XÉT CỦA GIẢNG VIÊN CHẤM PHẢN BIỆN

Họ và tên giảng viên: .....

Đơn vị công tác: .....

Họ và tên sinh viên: Ngành: Công nghệ thông tin

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:.....

Hải Phòng, ngày.....tháng 07 năm 2022

Giảng viên chấm phản biện

(Ký và ghi rõ họ tên)

MỤC LỤC

DANH MỤC HÌNH VẼ

DANH MỤC BẢNG BIỂU

DANH MỤC CHỮ VIẾT TẮT

TỪ VIẾT TẮT	TÊN VIẾT ĐẦY ĐỦ	TIẾNG VIỆT
AP	Access Point	Điểm truy cập
AES	Advanced Encryption Standard	Chuẩn Mã hóa Cấp cao
HTTP	Hyper text transfer protocol	Giao thức truyền siêu văn bản
HTTPS	Hyper text transfer protocol secure	Giao thức truyền siêu văn bản an toàn
IV	Initializtion Vector	Vector khởi tạo
KRACK	Key Reinstallation Attack	Tấn công cài đặt lại khóa
OFDM	Orthogonal Frequency Division Multiplexing	Ghép kênh phân chia theo tần số trực giao
PMF	Protection Management Frames	Khung quản lý bảo vệ
PSK	Pre-Shared Key	Khóa chia sẻ trước
TKIP	Temporal Key In tegrity Protocol	Giao thức toàn vẹn khóa tạm thời
VPN	Virtual private network	Mạng riêng ảo
WPS	Wifi Protected Setup	Thiết lập Wi-Fi được bảo vệ
WEP	Wired Equivalent Privacy	Quyền riêng tư tương đương có dây
WLAN	Wireless local area network	Mạng lưới không dây khu vực địa phương
WPA	Wifi protected access	Quyền truy cập bằng Wi-Fi

LỜI NÓI ĐẦU

Công nghệ không dây là một phương pháp chuyển giao từ điểm này đến điểm khác sử dụng sóng vô tuyến. Mạng không dây ngày nay bắt nguồn từ nhiều giai đoạn phát triển của thông tin vô tuyến, những ứng dụng điện báo và radio. Mặc dù một vài phát minh xuất hiện từ năm 1899, nhưng sự phát triển nổi bật đạt được vào kỷ nguyên của công nghệ điện tử và chịu ảnh hưởng lớn của nền kinh tế hiện đại, cũng như các khám phá trong lĩnh vực vật lý. Cho đến nay, mạng không dây đã đạt được những bước phát triển đáng kể. Tại một số nước có nền công nghệ thông tin phát triển, mạng không dây thực sự đi vào cuộc sống. Chỉ cần một laptop hoặc một phương tiện truy nhập mạng không dây bất kỳ, chúng ta có thể truy nhập vào mạng ở bất cứ nơi đâu, trên cơ quan, trong nhà, ngoài đường, trong quán cafe, trên máy bay…, bất cứ nơi đâu nằm trong phạm vi phủ sóng của WLAN. Tuy nhiên chính sự hỗ trợ truy nhập công cộng, các phương tiện truy nhập lại đa dạng, đơn giản, cũng như phức tạp, kích cỡ cũng có nhiều loại, đã đem lại sự đau đầu cho các nhà quản trị trong vấn đề bảo mật. Làm thế nào để tích hợp được các biện pháp bảo mật vào các phương tiện truy nhập, mà vẫn đảm bảo những tiện ích như nhỏ gọn, giá thành, hoặc vẫn đảm bảo hỗ trợ truy cập công cộng.

Nhưng chính sự hỗ trợ truy nhập công cộng với các phương tiện truy nhập đơn giản cũng như phức tạp đã đem lại nhiều rắc rối cho các nhà quản trị trong việc bảo mật thông tin. Vấn đề tích hợp các biện pháp bảo mật vào các phương tiện truy nhập nhưng vẫn đảm bảo những tiện ích và việc hỗ trợ truy cập công cộng là vấn đề rất đáng quan tâm. Vì vậy mà đã có nhiều giao thức bảo mật dữ liệu được ra đời như; WEP, WPA1, WPA2. Dựa trên chuẩn IEEE 802.11 nhưng đều chưa mang lại sự an toàn cao cho người dùng.

Các hệ thống mạng WLAN thường được triển khai theo mô hình hệ thống mở không cài đặt cơ chế kiểm soát truy cập, cũng như bảo mật cho Access Point để giúp người dùng dễ dàng truy cập, mặc dù thiết bị đó có hỗ trợ các giao thức bảo vệ thông tin theo bộ tiêu chuẩn IEEE 802.11: WEP, WPA, WPA2 hoặc cao hơn.

Tuy nhiên lỗ hổng lớn nhất trong bộ giáp của WPA vẫn còn tồn tại trong

những giao thức trước đó. Mặc dù để thâm nhập được vào mạng lưới được bảo vệ bởi WPA/WPA2 bằng lỗ hổng trên cần tới 2-14 giờ hoạt động liên tục của một máy tính hiện đại, đây vẫn là một mối lo tiềm tàng. Ngày 25/6/2018, Wifi Alliance - tổ chức quản lý công nghệ Wifi đã tuyên bố chính thức phát hành WPA3. Đây là chuẩn WPA mới nhất, công nghệ xác thực người dùng cho các kết nối Wifi. WPA3 hiện đang là lựa chọn bảo mật tùy chọn cho các thiết bị mới nhưng nó sẽ hoạt động trên tất cả các thiết bị đáp ứng được chuẩn này trong những năm tới.

Qua quá trình học tập và nghiên cứu tại trường, dưới góc độ là sinh viên năm cuối và kết hợp sự định hướng hướng dẫn của thầy giáo Nguyễn Như Chiến em đã quyết định chọn đề tài: "*Tìm hiểu, phân tích và đề xuất giải pháp bảo mật khi triển khai mạng WLAN sử dụng giao thức WPA3*" làm đồ án tốt nghiệp của mình.

LỜI CẢM ƠN

Đồ án tốt nghiệp này đạt kết quả là do nhận được sự hỗ trợ, giúp đỡ của nhiều cơ quan, tổ chức, cá nhân. Với tình cảm sâu sắc, chân thành, cho phép em được bày tỏ lòng biết ơn sâu sắc đến tất cả các cá nhân và cơ quan đã tạo điều kiện giúp đỡ trong quá trình học tập và nghiên cứu đồ án.

Trước hết em xin gửi tới các Thầy Cô khoa Công nghệ thông tin trường Đại học Quản lý và Công nghệ Hải phòng lời chào trân trọng, lời chúc sức khỏe và lời cảm ơn sâu sắc. Với sự quan tâm, dạy dỗ, chỉ bảo tận tình chu đáo của Thầy Cô, đến nay em đã có thể hoàn thành đồ án tốt nghiệp với đề tài *"Tìm hiểu, phân tích và đề xuất giải pháp bảo mật khi triển khai mạng WLAN sử dụng giao thức WPA3"*. Đặc biệt em xin gửi lời cảm ơn chân thành nhất tới thầy giáo – ThS. Nguyễn Như Chiến đã quan tâm giúp đỡ, hướng dẫn em hoàn thành tốt đề tài này trong thời gian qua.

Em xin bày tỏ lòng biết ơn đến lãnh đạo Trường Đại học Quản lý và Công nghệ Hải Phòng, Khoa Công nghệ thông tin, các Phòng ban chức năng đã trực tiếp và gián tiếp giúp đỡ tôi trong suốt quá trình học tập và nghiên cứu đề tài.

Không thể không nhắc tới sự giúp đỡ nhiệt tình của đơn vị đã tạo điều kiện thuận lợi nhất cho tôi tìm hiểu nghiệp vụ cũng như các chứng từ để làm tài liệu phục vụ cho đề tài.

Với điều kiện thời gian cũng như kinh nghiệm còn hạn chế của một sinh viên, đồ án tốt nghiệp này không thể tránh được những thiếu sót. Em rất mong nhận được sự chỉ bảo, đóng góp ý kiến của các thầy cô để em có điều kiện bổ sung, nâng cao ý thức của mình, phục vụ tốt hơn công tác thực tế sau này.

Em xin chân thành cảm ơn!

Hải Phòng ngày… tháng… năm 2022

Sinh viên

CHƯƠNG 1

TỔNG QUAN MẠNG KHÔNG DÂY VÀ VẤN ĐỀ BẢO ĐẢM AN TOÀN MẠNG KHÔNG DÂY

1.1. Tổng quan về WLAN

1.1.1. Lịch sử hình thành và phát triển.

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 dù 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.

1.1.2. Ưu điểm của WLAN

- 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.

- 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.

1.1.3. Nhược điểm của WLAN

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, nhưng với một tòa nhà lớn thì không đáp ứng được nhu cầu. Để đáp ứng cần phải mua thêm Repeater hay access point,

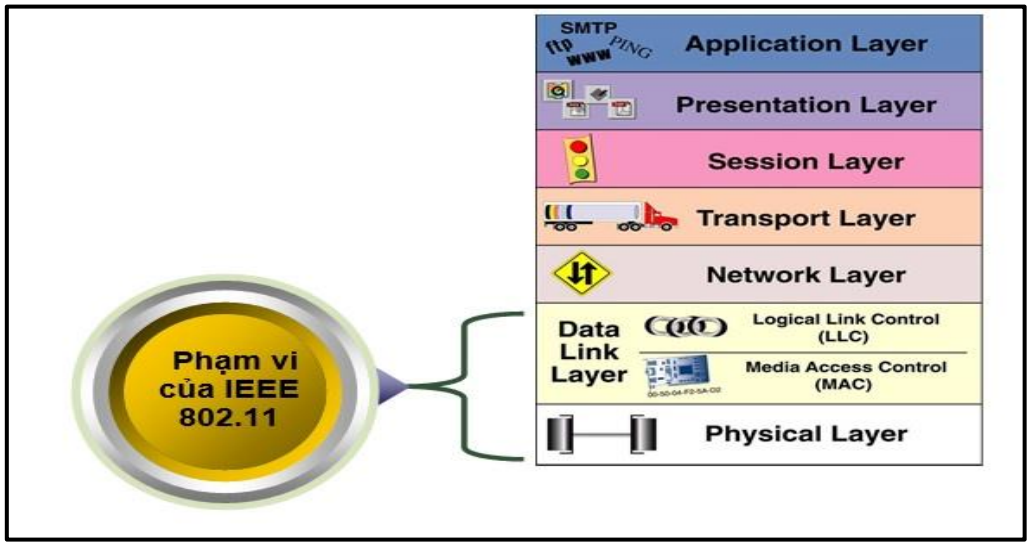
dẫn đến chi phí gia tăng.

- 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.



Hình 1.1: Phạm vi của WLAN trong mô hình OSI

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.

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

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

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).

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

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

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.

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

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

1.2.4. Chuẩn IEEE 802.11n

Hình 1.2: Logo Wi-fi

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.

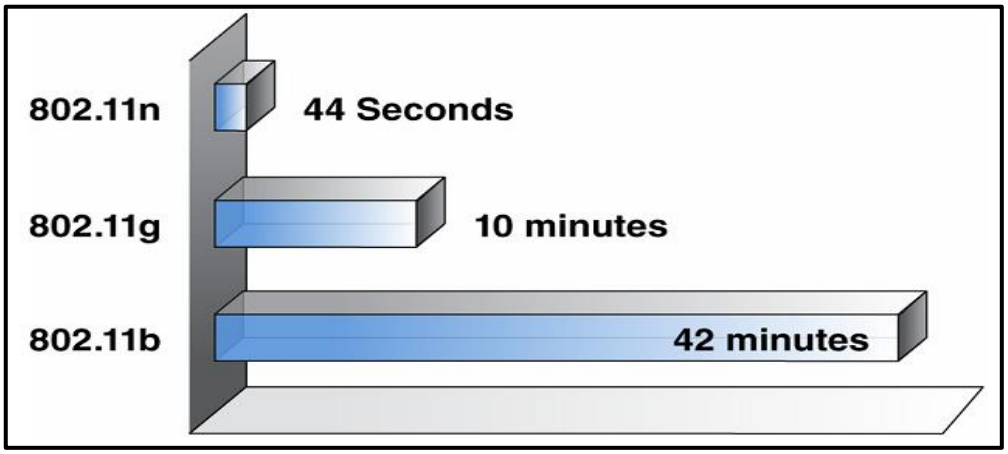
Winston Sun, giám đốc công nghệ của công ty không dây Atheros Communications, nhận xét, một thiết bị tương thích 802.11n có thể truy cập các điểm hotspot với tốc độ 150 MB/giây với khoảng cách lý tưởng dưới 6m, khả năng liên kết càng giảm khi người dùng ở cách xa điểm truy cập đó.

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 .

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

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



Hình 1.3: Tốc độ truyền tải so với các chuẩn khác

1.2.5. So sánh các chuẩn IEEE 802.11x

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.wifi.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.

- IEEE 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 giai 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 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.

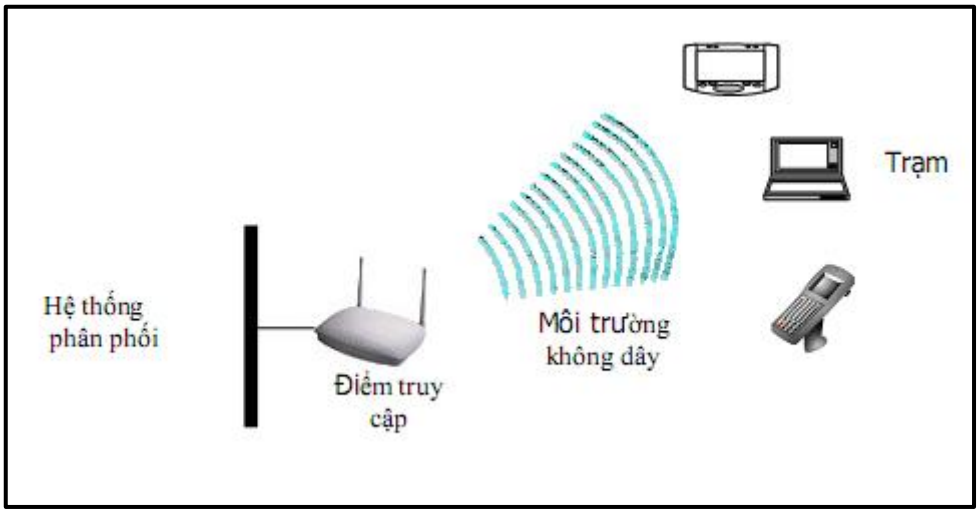
Tuy chuẩn IEEE 802.11n chưa được thông qua nhưng khá nhiều nhà sản xuất thiết bị đã dựa trên bản thảo của chuẩn này để tạo ra những cái gọi là chuẩn G+ hoặc SuperG với tốc độ thông thường là gấp đôi giới hạn của IEEE 802.11g. Các thiết bị này tương thích ngược với IEEE 802.11b/g rất tốt nhưng tất nhiên 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.

1.3. Cấu trúc và các mô hình WLAN

1.3.1. Cấu trúc cơ bản của WirelessLAN



Hình 1.4: Cấu trúc WLAN

Có 4 thành phần chính trong các loại mạng sử dụng chuẩn 802.11:

- Hệ thống phân phối (DS _ Distribution System)

- Điểm truy cập (Access Point)

- Tầng liên lạc vô tuyến (Wireless Medium)

-Trạm (Stations)

a. Hệ thống phân phối (DS _ Distribution System)

- Thiết bị logic của 802.11 được dùng để nối các khung tới đích của chúng: Bao gồm kết nối giữa động cơ và môi trường DS (ví dụ như mạng xương sống).

- 802.11 không xác định bất kỳ công nghệ nhất định nào đối với DS.

- Hầu hết trong các ứng dụng quảng cáo, Ethernet được dùng như là môi trường DS - Trong ngôn ngữ của 802.11, xương sống Ethernet là môi trường hệ thống phân phối. Tuy nhiên, không có nghĩa nó hoàn toàn là DS.

b. Điểm truy cập (Access Points)

- Chức năng chính của AP là mở rộng mạng. Nó có khả năng chuyển đổi các frame dữ liệu trong 802.11 thành các frame thông dụng để có thể sử dụng trong các mạng khác.

- AP có chức năng cầu nối giữa không dây thành có dây.

c. Tầng liên lạc vô tuyến (Wireless Medium)

Chuẩn 802.11 sử dụng tầng liên lạc vô tuyến để chuyển đổi các frame dữ liệu giữa các máy trạm với nhau.

d. Trạm (Stations)

Các máy trạm là các thiết bị vi tính có hỗ trợ kết nối vô tuyến như: Máy tính xách tay, PDA, Palm, Desktop …

1.3.2. Các thiết bị hạ tầng mạng không dây

- Điểm truy cập: AP (Access Point)

Cung cấp cho các máy khách (client) một điểm truy cập vào mạng "Nơi mà các máy tính dùng wireless có thể vào mạng nội bộ của công ty". AP là một thiết bị song công (Full duplex) có mức độ thông minh tương đương với một chuyển mạch Ethernet phức tạp (Switch).

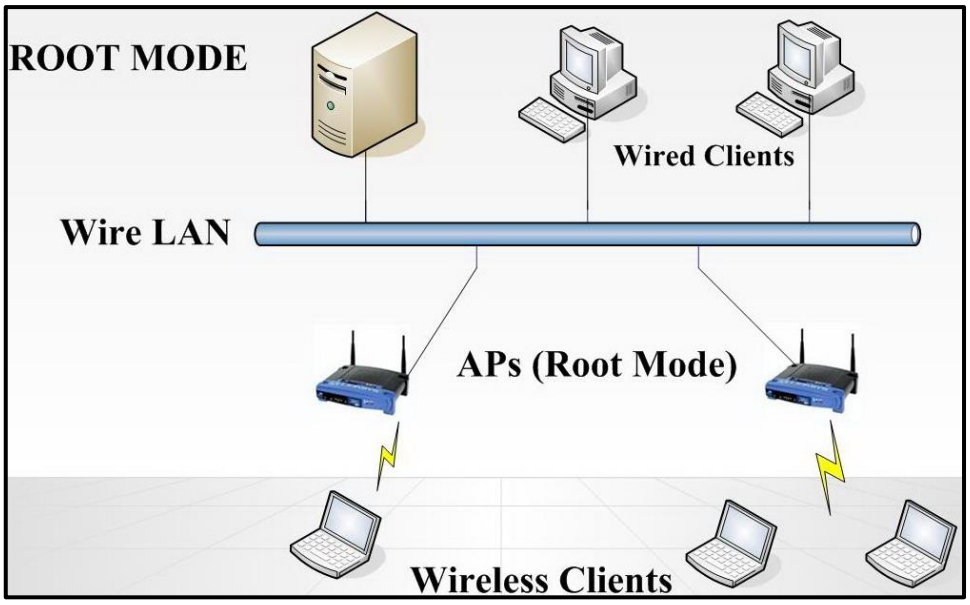
Hình 1.5: Access Points

- Các chế độ hoạt động của AP

AP có thể giao tiếp với các máy không dây, với mạng có dây truyền thống và với các AP khác. Có 3 Mode hoạt động chính của AP:

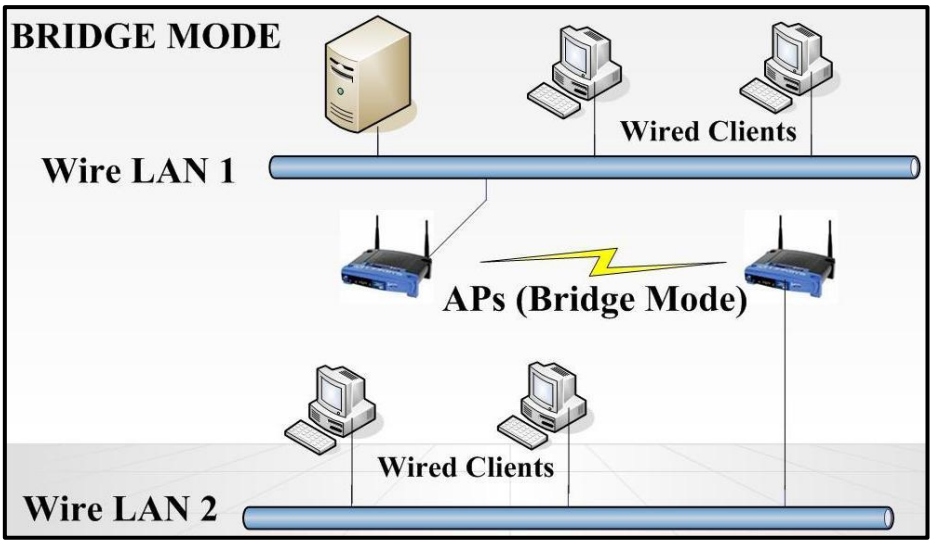
+ Chế độ gốc (Root mode): Root mode được sử dụng khi AP được kết nối với mạng backbone có dây thông qua giao diện có dây (thường là Ethernet) của nó. Hầu hết các AP sẽ hỗ trợ các mode khác ngoài root mode, tuy nhiên root mode là cấu hình mặc định. Khi một AP được kết nối với phân đoạn có dây thông qua cổng

Ethernet của nó, nó sẽ được cấu hình để hoạt động trong root mode. Khi ở trong root mode, các AP được kết nối với cùng một hệ thống phân phối có dây có thể nói chuyện được với nhau thông qua phân đoạn có dây. Các client không dây có thể giao tiếp với các client không dây khác nằm trong những cell (ô tế bào, hay vùng phủ sóng của AP) khác nhau thông qua AP tương ứng mà chúng kết nối vào, sau đó các AP này sẽ giao tiếp với nhau thông qua phân đoạn có dây, như ví dụ trong hình dưới đây.



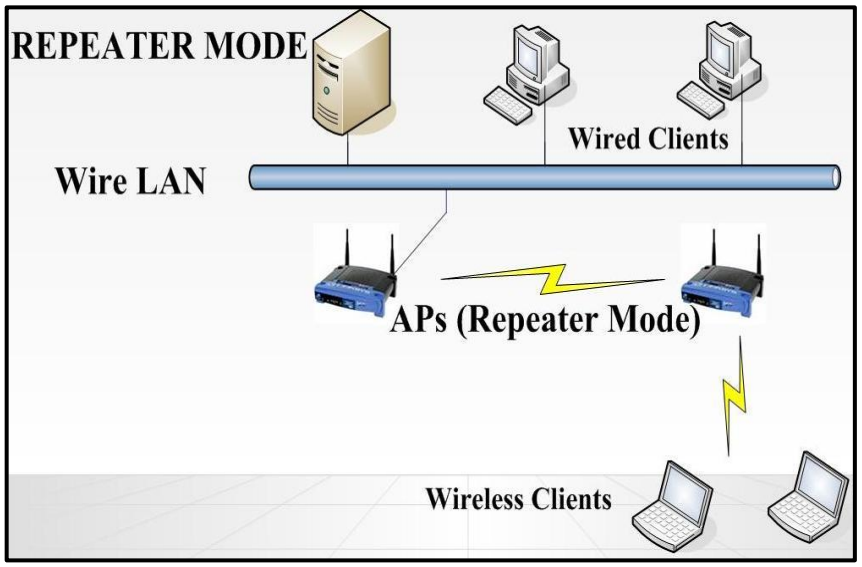
Hình 1.6: root mode

+ Chế độ cầu nối (bridge Mode): Trong Bridge mode, AP hoạt động hoàn toàn giống với một cầu nối không dây. AP sẽ trở thành một cầu nối không dây khi được cấu hình theo cách này. Chỉ một số ít các AP trên thị trường có hỗ trợ chức năng Bridge, điều này sẽ làm cho thiết bị có giá cao hơn đáng kể. Chúng ta sẽ giải thích một cách ngắn gọn cầu nối không dây hoạt động như thế nào, từ hình 1.7 Client không kết nối với cầu nối, nhưng thay vào đó, cầu nối được sử dụng để kết nối 2 hoặc nhiều đoạn mạng có dây lại với nhau bằng kết nối không dây.



Hình 1.7: BRIDGE MODE

+ Chế độ lặp(repeater mode): AP có khả năng cung cấp một đường kết nối không dây upstream vào mạng có dây thay vì một kết nối có dây bình thường. Một AP hoạt động như là một root AP và AP còn lại hoạt động như là một Repeater không dây. AP trong repeater mode kết nối với các client như là một AP và kết nối với upstream AP như là một client.



Hình 1.8: REPEATER MODE

- Các thiết bị máy khách trong WLAN

Là những thiết bị WLAN được các máy khách sử dụng để kết nối vào WLAN.

a. Card PCI Wireless:

Là thành phần phổ biến nhất trong WLAN. Dùng để kết nối các máy khách vào hệ thống mạng không dây. Được cắm vào khe PCI trên máy tính. Loại này được sử dụng phổ biến cho các máy tính để bàn(desktop) kết nối vào mạng không dây.

Hình 1.9: Card PCI Wireless

b. Card PCMCIA Wireless:

Trước đây được sử dụng trong các máy tính xách tay(laptop) và cácthiết bị hỗ trợ cá nhân số PDA(Personal Digital Associasion). Hiện nay nhờ sự phát triển của công nghệ nên PCMCIA wireless ít được sử dụng vì máy tính xách tay và PDA,…. đều được tích hợp sẵn Card Wireless bên trong thiết bị.

Hình 1.10: Card PCMCIA Wireless

c. Card USB Wireless:

Loại rất được ưu chuộng hiện nay dành cho các thiết bị kết nối vào mạng không dây vì tính năng di động và nhỏ gọn . Có chức năng tương tự như Card PCI Wireless, nhưng hỗ trợ chuẩn cắm là USB (Universal Serial Bus). Có thể tháo lắp nhanh chóng (không cần phải cắm cố định như Card PCI Wireless) và hỗ trợ cắm khi máy tính đang hoạt động.

Hình 1.11: Card USB Wireless

1.3.3. Các mô hình WLAN

Mạng 802.11 linh hoạt về thiết kế, gồm 3 mô hình mạng sau:

- Mô hình mạng độc lập (IBSSs) hay còn gọi là mạng Ad hoc.

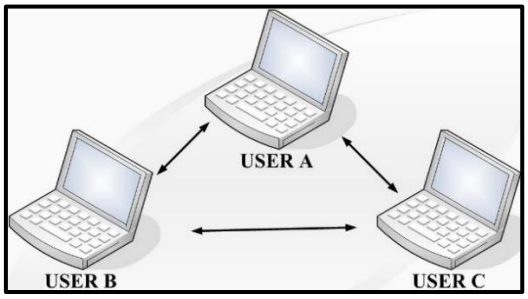
- Mô hình mạng cơ sở (BSSs).

- Mô hình mạng mở rộng (ESSs).

a) Mô hình mạng AD HOC (Independent Basic Service Sets (IBSSs))

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 cấp (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. Vì các mạng ad-hoc này có thể thực hiện nhanh và dễ dàng nên chúng thường được thiết lập mà không cần một công cụ hay kỹ năng đặc biệt nào vì vậy nó rất thích hợp để sử dụng trong các hội nghị thương mại hoặc trong các nhóm làm việc tạm thời. Tuy nhiên chúng có thể có những nhược điểm về

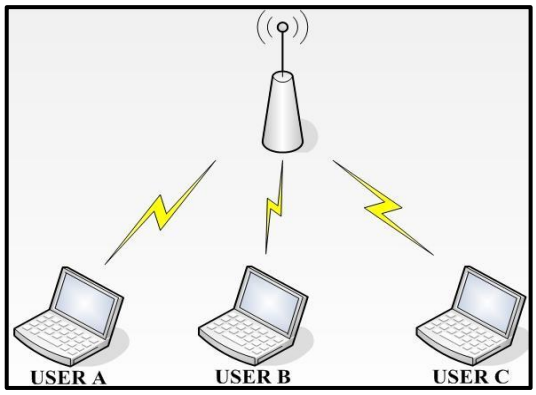
vùng phủ sóng bị giới hạn, mọi người sử dụng đều phải nghe được lẫn nhau.



Hình 1.12: Mô hình mạng AD HOC

b) Mô hình mạng cơ sở (Basic service sets (BSSs))

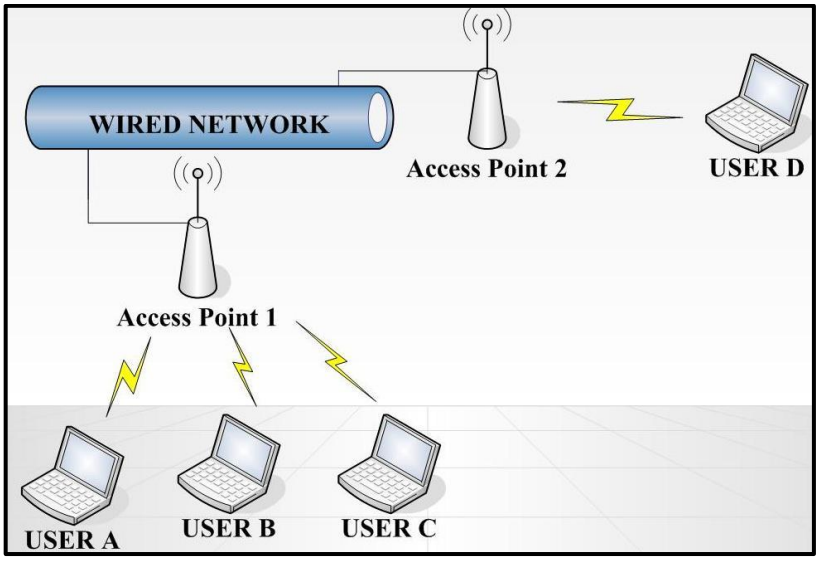
Bao gồm các điểm truy nhập AP (Access Point) gắn với mạng đường trục hữu tuyến và giao tiếp với các thiết bị di động trong vùng phủ sóng của một cell. AP đóng vai trò điều khiển cell và điều khiển lưu lượng tới mạng. Các thiết bị di động không giao tiếp trực tiếp với nhau mà giao tiếp với các AP. Các 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 trục, ấn 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. Tuy nhiên giao thức đa truy nhập tập trung không cho phép các nút di động truyền trực tiếp tới nút khác nằm trong cùng vùng với điểm truy nhập như trong cấu hình mạng WLAN độc lập. Trong trường hợp này, mỗi gói sẽ phải được phát đi 2 lần (từ nút phát gốc và sau đó là điểm truy nhập) trước khi nó tới nút đích, quá trình này sẽ làm giảm hiệu quả truyền dẫn và tăng trễ truyền dẫn.



Hình 1.13: Mô hình mạng cơ sở

c) Mô hình mạng mở rộng (Extended Service Set (ESSs))

Mạng 802.11 mở rộng phạm vi di động tới một phạm vi bất kì thông qua ESS. Một ESSs 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 gửi 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 1.14: Mô hình mạng mở rộng

1.4. Thực trạng về bảo mật WLAN hiện nay

Nếu con số thống kê đúng thì cứ 5 người dùng mạng không dây tại nhà có đến 4 người không kích hoạt bất kỳ chế độ bảo mật nào. Mặc định, các nhà sản xuất tắt chế độ bảo mật để cho việc thiết lập ban đầu được dễ dàng, khi sử dụng bạn phải mở lại. Tuy nhiên, chúng ta cần phải cẩn thận khi kích hoạt tính năng bảo mật, dưới đây là một số sai lầm thường gặp phải.

- Sai lầm 1: Không thay đổi mật khẩu của nhà sản xuất. Khi lần đầu tiên cài đặt router không dây, chúng ta rất dễ quên thay đổi mật khẩu mặc định của nhà sản xuất. Nếu không thay đổi, có thể người khác sẽ dùng mật khẩu mặc định truy cập vào *Router* và thay đổi các thiết lập để thoải mái truy cập vào mạng. Kinh nghiệm: Luôn thay mật khẩu mặc định.

- Sai lầm 2: Không kích hoạt tính năng mã hóa. Nếu không kích hoạt tính năng mã hóa, chúng ta sẽ quảng bá mật khẩu và e-mail của mình đến bất cứ ai trong tầm phủ sóng, người khác có thể cố tình dùng các phầm mềm nghe lén miễn phí như AirSnort (airsnort.shmoo.com) để lấy thông tin rồi phân tích dữ liệu. Kinh nghiệm: Hãy bật chế độ mã hóa kẻo người khác có thể đọc được e-mail của chúng ta.

- Sai lầm 3: Không kiểm tra chế độ bảo mật. Chúng ta mua một *AccessPoint*, kết nối Internet băng rộng, lắp cả máy in vào, rồi có thể mua thêm nhiều thiết bị không dây khác nữa. Có thể vào một ngày nào đó, máy in sẽ tự động in hết giấy bởi vì chúng ta không thiết lập các tính năng bảo mật. Kinh nghiệm: Đừng cho rằng mạng của chúng ta đã an toàn. Hãy nhờ những người am hiểu kiểm tra hộ.

- Sai lầm 4: Quá tích cực với các thiết lập bảo mật. Mỗi *Wireless Card/ Thẻ mạng không dây* đều có một địa chỉ phần cứng (địa chỉ MAC) mà AP có thể dùng để kiểm soát những máy tính nào được phép nối vào mạng. Khi bật chế độ lọc địa chỉ MAC, có khả năng chúng ta sẽ quên thêm địa chỉ MAC của máy tính chúng ta đang sử dụng vào danh sách, như thế chúng ta sẽ tự cô lập chính mình, tương tự như bỏ chìa khóa trong xe hơi rồi chốt cửa lại. Kinh nghiệm: Phải kiểm tra cẩn thận khi thiết lập tính năng bảo mật.

- Sai lầm 5: Cho phép mọi người truy cập. Có thể chúng ta là người đầu tiên có mạng không dây và muốn 'khoe' bằng cách đặt tên mạng là 'truy cập thoải mái' chẳng hạn. Hàng xóm của mình có thể dùng kết nối này để tải rất nhiều phim ảnh chẳng hạn và mạng sẽ chạy chậm hơn so với lúc trước. Kinh nghiệm: Mạng không dây giúp chia sẻ kết nối Internet dễ dàng, tuy nhiên, đừng bỏ ngỏ vì sẽ có người lạm dụng.

1.5. Một số hình thức tấn công xâm nhập phổ biến

1.5.1. Tấn công không qua chứng thực

- Tấn công không qua chứng thực (Deauthentication attack) là sự khai thác gần như hoàn hảo lỗi nhận dạng trong mạng 802.11. Trong mạng 802.11 khi một nút mới gia nhập vào mạng nó sẽ phải đi qua quá trình xác nhận cũng như các quá trình có liên quan khác rồi sau đó mới được phép truy cập vào mạng. Bất kỳ các nút ở vị trí nào cũng có thể gia nhập vào mạng bằng việc sử dụng khoá chia sẻ tại vị trí nút đó để biết được mật khẩu của mạng. Sau quá trình xác nhận, các nút sẽ đi tới các quá trình có liên quan để có thể trao đổi dữ liệu và quảng bá trong toàn mạng. Trong suốt quá trình chứng thực chỉ có một vài bản tin dữ liệu, quản lý và điều khiển là được chấp nhận. Một trong các bản tin đó mang lại cho các nút khả năng đòi hỏi không qua chứng thực từ mỗi nút khác. Bản tin đó được sử dụng khi một nút muốn chuyển giữa hai mạng không dây khác nhau. Ví dụ nếu trong cùng một vùng tồn tại nhiều hơn một mạng không dây thì nút đó sẽ sử dụng bản tin này. Khi một nút nhận được bản tin "không qua chứng thực" này nó sẽ tự động rời khỏi mạng và quay trở lại trạng thái gốc ban đầu của nó.

- Trong tấn công không qua chứng thực, tin tặc sẽ sử dụng một nút giả mạo để tìm ra địa chỉ của AP đang điều khiển mạng. Không quá khó để tìm ra địa chỉ của AP bởi nó không được bảo vệ bởi thuật toán mã hoá, địa chỉ của chúng có thể được tìm thấy nếu chúng ta lắng nghe lưu lượng giữa AP và các nút khác. Khi tin tặc có được địa chỉ của AP, chúng sẽ gửi quảng bá các bản tin không chứng thực ra toàn mạng khiến cho các nút trong mạng ngay lập tức dừng trao đổi tin với mạng. Sau

đó tất cả các nút đó sẽ cố kết nối lại, chứng thực lại và liên kết lại với AP tuy nhiên do việc truyền các bản tin không qua chứng thực được lặp lại liên tục khiến cho mạng rơi vào tình trạng bị dừng hoạt động.

1.5.2. Tấn công giả mạo AP

- Giả mạo AP là kiểu tấn công “man in the middle" cổ điển. Đây là kiểu tấn công mà Attacker đứng ở giữa và trộm lưu lượng truyền giữa 2 nút. Kiểu tấn công này rất mạnh vì attacker có thể lấy đi tất cả lưu lượng đi qua mạng. Rất khó khăn để tạo một cuộc tấn công "man in the middle" trong mạng có dây bởi vì kiểu tấn công này yêu cầu truy cập thực sự đến đường truyền. Trong mạng không dây thì lại rất dễ bị tấn công kiểu này. Attacker cần phải tạo ra một AP thu hút nhiều sự lựa chọn hơn AP chính thống. AP giả này có thể được thiết lập bằng cách sao chép tất cả các cấu hình của AP chính thống đó là: SSID, địa chỉ MAC,... Bước tiếp theo là làm cho nạn nhân thực hiện kết nối tới AP giả. Cách thứ nhất là đợi cho người dùng tự kết nối. Cách thứ hai là gây ra một cuộc tấn công từ chối dịch vụ DoS trong AP chính thống do vậy người dùng sẽ phải kết nối lại với AP giả. Trong mạng 802.11 sự lựa chọn AP được thực hiện bởi cường độ của tín hiệu nhận. Điều duy nhất attacker phải thực hiện là chắc chắn rằng AP của mình có cường độ tín hiệu mạnh hơn cả. Để có được điều đó attacker phải đặt AP của mình gần nạn nhân hơn là AP chính thống hoặc sử dụng kỹ thuật anten định hướng. Sau khi nạn nhân kết nối tới AP giả, nạn nhân vẫn hoạt động như bình thường do vậy nếu nạn nhân kết nối đến một AP chính thống khác thì dữ liệu của nạn nhân đều đi qua AP giả. Attacker sẽ sử dụng các tiện ích để ghi lại mật khẩu của nạn nhân khi trao đổi với Web Server. Như vậy, attacker sẽ có được tất cả những gì anh ta muốn để đăng nhập vào mạng chính thống. Kiểu tấn công này tồn tại là do trong 802.11 không yêu cầu chứng thực 2 hướng giữa AP và nút AP phát quảng bá ra toàn mạng. Điều này rất dễ bị attacker nghe trộm và do vậy attacker có thể lấy được tất cả các thông tin mà chúng cần. Các nút trong mạng sử dụng WEP để chứng thực chúng với AP nhưng WEP cũng có những lỗ hổng có thể khai thác. Một attacker có thể nghe trộm thông tin và sử dụng bộ phân tích mã hóa để trộm mật khẩu của người dùng.

1.5.3. Tấn công từ chối dịch vụ (DoS/DDoS)

- DoS tên đầy đủ tiếng Anh là Denial of Service, dịch ra tiếng Việt là từ chối dịch vụ. Tấn công từ chối dịch vụ DoS là cuộc tấn công nhằm làm sập một máy chủ hoặc mạng, khiến người dùng khác không thể truy cập vào máy chủ/mạng đó. Kẻ tấn công thực hiện điều này bằng cách "tuồn" ồ ạt traffic hoặc gửi thông tin có thể kích hoạt sự cố đến máy chủ, hệ thống hoặc mạng mục tiêu, từ đó khiến người dùng hợp pháp (nhân viên, thành viên, chủ tài khoản) không thể truy cập dịch vụ, tài nguyên họ mong đợi. Nạn nhân của tấn công DoS thường là máy chủ web của các tổ chức cao cấp như ngân hàng, doanh nghiệp thương mại, công ty truyền thông, các trang báo, mạng xã hội... Ví dụ, khi bạn nhập vào URL của một website vào trình duyệt, lúc đó bạn đang gửi một yêu cầu đến máy chủ của trang này để xem. Máy chủ chỉ có thể xử lý một số yêu cầu nhất định trong một khoảng thời gian, vì vậy nếu kẻ tấn công gửi ồ ạt nhiều yêu cầu đến máy chủ sẽ làm nó bị quá tải và yêu cầu của bạn không được xử lý. Đây là kiểu “từ chối dịch vụ” vì nó làm cho bạn không thể truy cập đến trang đó.

- DDoS (Distributed Denial of Service), nghĩa tiếng Việt là từ chối dịch vụ phân tán. Tấn công DDoS là nỗ lực làm sập một dịch vụ trực tuyến bằng cách làm tràn ngập nó với traffic từ nhiều nguồn. Khi DDoS, kẻ tấn công có thể sử dụng máy tính của bạn để tấn công vào các máy tính khác. Bằng cách lợi dụng những lỗ hổng về bảo mật cũng như sự không hiểu biết, kẻ này có thể giành quyền điều khiển máy tính của bạn. Sau đó chúng sử dụng máy tính của bạn để gửi số lượng lớn dữ liệu đến một website hoặc gửi thư rác đến địa chỉ email nào đó. Đây là kiểu tấn công phân tán vì kẻ tấn công sử dụng nhiều máy tính, bao gồm có cả máy tính của bạn để thực hiện tấn công Dos.

1.6. Nâng cao độ an toàn WLAN

1.6.1. Lọc SSID

- Lọc SSID: thường được sử dụng trong các điều khiển truy cập cơ bản. Trong đó, SSID của client phải khớp với SSID của AP để có thể xác thực và kết nối với

tập dịch vụ.

- Lọc SSID SSID Filtering là một phương pháp lọc chỉ được dùng cho hầu hết các điều khiển truy nhập. SSID của một trạm WLAN phải khớp với SSID trên AP hoặc của các trạm khác để chứng thực và liên kết Client để thiết lập dịch vụ. Nhiều AP có khả năng lấy các SSID của các khung thông tin dẫn đường beacon frame. Trong trường hợp này client phải so khớp SSID để liên kết với AP. Lọc SSID được coi là một phương pháp không tin cậy trong việc hạn chế những người sử dụng trái phép của một WLAN. Một vài lỗi chung do người sử dụng WLAN tạo ra khi thực hiện SSID là sử dụng SSID mặc định. Sự thiết lập này là một cách khác để đưa ra thông tin về WLAN của mạng. Nó đủ đơn giản để sử dụng một bộ phân tích mạng để lấy địa chỉ MAC khởi nguồn từ AP. Cách tốt nhất để khắc phục lỗi này là: Luôn luôn thay đổi SSID mặc định. Sử dụng SSID như những phương tiện bảo mật mạng WLAN, SSID phải được người dùng thay đổi trong việc thiết lập cấu hình để vào mạng. Nó nên được sử dụng như một phương tiện để phân đoạn mạng chứ không phải để bảo mật, vì thế hãy luôn coi SSID chỉ như một cái tên mạng. Không cần thiết quảng bá các SSID Nếu AP của mạng có khả năng chuyển SSID từ các thông tin dẫn đường và các thông tin phản hồi để kiểm tra thì hãy cấu hình chúng theo cách đó. Cấu hình này ngăn cản những người nghe vô tình khỏi việc gây rối hoặc sử dụng WLAN.

1.6.2. Lọc địa chỉ MAC

- Lọc địa chỉ MAC: là chức năng tồn tại trong hầu hết các AP. Nếu client có địa chỉ MAC không nằm trong danh sách lọc địa chỉ MAC của AP thì AP sẽ ngăn chặn không cho phép client đó kết nối vào mạng.

- Cách thức lọc địa chỉ MAC hoạt động

+ Trên một mạng không dây thông thường, bất kỳ thiết bị nào có thông tin đăng nhập thích hợp (biết SSID và mật khẩu) có thể xác thực với bộ định tuyến và tham gia mạng, nhận địa chỉ IP và truy cập internet và mọi tài nguyên được chia sẻ.

+ Lọc địa chỉ MAC thêm một lớp bổ sung cho quá trình này. Trước khi cho phép bất kỳ thiết bị nào tham gia vào mạng, router sẽ kiểm tra địa chỉ MAC của thiết bị dựa vào danh sách các địa chỉ được chấp thuận. Nếu địa chỉ của khách hàng khớp với một địa chỉ trên danh sách của bộ định tuyến, quyền truy cập được cấp như bình thường; nếu không, nó bị chặn tham gia.

- Cách cấu hình lọc địa chỉ MAC

+ Để thiết lập lọc MAC trên bộ định tuyến, quản trị viên phải định cấu hình danh sách các thiết bị sẽ được phép tham gia. Địa chỉ vật lý của mỗi thiết bị được phê duyệt phải được tìm thấy và sau đó các địa chỉ đó cần được nhập vào bộ định tuyến và tùy chọn lọc địa chỉ MAC được bật.

+ Hầu hết các bộ định tuyến cho phép bạn xem địa chỉ MAC của các thiết bị được kết nối từ bảng điều khiển dành cho quản trị viên. Nếu không, bạn có thể sử dụng hệ điều hành của bạn để làm điều đó. Khi bạn đã có danh sách địa chỉ MAC, hãy vào cài đặt của bộ định tuyến và đặt chúng vào vị trí thích hợp của chúng.

1.6.3. Lọc giao thức

- Lọc giao thức: được sử dụng trong các mạng WLAN không dây để lọc các gói đi qua mạng dựa trên các giao thức từ lớp 2 đến lớp 7.

- Trong nhiều trường hợp, các nhà sản xuất làm các bộ lọc giao thức có thể định hình độc lập cho cả những đoạn mạng hữu tuyến và vô tuyến của AP.

- Ví dụ một tình huống, trong đó một nhóm cầu nối không dây được đặt trên một remote building trong một mạng WLAN của một trường đại học kết nối tới AP của tòa nhà kỹ thuật trung tâm. Vì tất cả những người sử dụng trong remote building chia sẻ băng thông 5 Mbps giữa những tòa nhà này, nên một số lượng đáng kể các điều khiển trên các sử dụng này phải được thực hiện. Nếu các kết nối này được cài đặt với mục đích truy nhập internet đặc biệt của người sử dụng, thì bộ lọc giao thức sẽ loại trừ tất cả các giao thức, ngoại trừ SMTP, POP3, HTTP, HTTPS, FTP…

1.6.4. Tắt bỏ tính năng WPS

- WPS là tính năng thiết lập kết nối mạng WIFI giữa các thiết bị thu và thiết bị phát, mà không cần phải đăng nhập mật khẩu WIFI. WPS được viết tắt là WIFI Protected Setup, là một tiêu chuẩn mới cho việc thiết lập mạng không dây dễ dàng so với cách thủ công trước đây và an toàn. WPS wifi là công nghệ hiện đại khá mới trên các thiết bị hiện nay, nhưng tính năng vô cùng tiện lợi, sử dụng nhanh chóng cho người dùng. WPS sinh ra nhằm hỗ trợ kết nối WIFI giữa các thiết bị khác nhau.

- WPS cũng mang đến một rủi ro bảo mật khá nghiêm trọng mà bạn không thể tránh được. Khi WPS được bật, tin tặc có thể đoán mật khẩu router nhiều lần cho đến khi chúng tìm được mật khẩu đúng. Nếu bạn chưa thực hiện các bước để cải thiện bảo mật router, router có thể đặc biệt dễ bị tấn công. Khi tin tặc có mật khẩu, chúng sẽ có quyền truy cập vào kết nối Internet, sử dụng cho bất cứ thứ gì chúng muốn, cho đến khi bạn reset lại mật khẩu của router. Nếu muốn sử dụng WPS, bạn nên cân nhắc giữa lượng thời gian có thể tiết kiệm được so với những rắc rối tiềm ẩn, nếu một cuộc tấn công vào router của bạn thành công.

1.6.5. Loại bỏ việc hỗ trợ băng tầng 2.4Ghz

- Nó có băng thông thấp hơn mạng 5 GHz.

- Các thiết bị như điện thoại không dây và lò vi sóng sử dụng sóng vô tuyến 2,4 GHz giống như bộ định tuyến không dây. Nếu bạn có các thiết bị như vậy ở nhà, chúng có thể gây nhiễu sóng vô tuyến từ bộ định tuyến, khiến băng thông của mạng bị giảm.

- Nhiều thiết bị hỗ trợ tần số này để có nhiều tắc nghẽn hơn trong tần số này có thể gây ra vấn đề với băng thông

1.6.6. Sử dụng chuẩn bảo mật WPA2/WPA3

- WPA2 mang đến một bản nâng cấp bảo mật và mã hóa khác, đáng chú ý nhất là việc giới thiệu Advanced Encryption Standard (AES) cho các mạng WiFi

tiêu dùng. AES mạnh hơn đáng kể so với RC4 (vì RC4 đã từng bị "bẻ khóa" nhiều lần) và là tiêu chuẩn bảo mật được áp dụng cho nhiều dịch vụ trực tuyến tại thời điểm hiện tại.

- WPA2 cũng giới thiệu Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (Chế độ mã hóa truy cập với giao thức mã xác thực thông báo chuỗi khối), gọi tắt là CCMP, để thay thế TKIP dễ bị tấn công hiện nay.

- Bảo vệ mật khẩu đáng tin cậy

+ WPA3-Enterprise được kéo dài mã hóa thành 192bit (mã hóa 128bit ở chế độ WPA3-Personal) để tăng cường độ mạnh của mật khẩu. Nó bảo vệ chống lại các mật khẩu yếu có thể bị bẻ khóa tương đối dễ dàng thông qua việc đoán.

- Bảo vệ các thiết bị mạng của bạn

+ WPA3 thay thế Khóa chia sẻ trước WPA2 (WPA2 Pre-Shared Key - PSK) bằng Xác thực đồng thời - Simultaneous Authentication of Equals (SAE) để tránh các cuộc tấn công cài đặt lại khóa như KRACK khét tiếng. Nó sẽ giữ an toàn cho các thiết bị mạng của bạn trong khi kết nối với điểm truy cập không dây. tấn công từ điển ngoại tuyến.

- Kết nối an toàn hơn trên khu vực công cộng

+ Cho dù kẻ tấn công có được khóa mã hóa lưu lượng, thật khó để tính toán mức sử dụng lưu lượng và dữ liệu được truyền bằng WPA3-Personal. SAE mang lại lợi ích của bảo mật chuyển tiếp (forward-secrecy) và bảo mật dữ liệu hơn nhiều so với mạng mở. WPA3 cũng cung cấp các khung quản lý được bảo vệ (Protected management frames - PMF) để tránh nghe lén và giả mạo từ khu vực công cộng.

1.6.7. Thay đổi thông tin đăng nhập mặc định

- Người dùng cần thay đổi tên người dùng và mật khẩu của người dùng quản trị mạng. Những kẻ tấn công biết được tên và mật khẩu mặc định và họ sẽ thử những thứ đó trước.

- Lưu ý, thay đổi tên người dùng quản trị thành một cái gì đó hơi khó đoán.

Mật khẩu phải là một cụm mật mã. Điều đó có nghĩa là nó phải là một cụm từ chứa ít nhất một hoặc nhiều từ không có nghĩa. Ngoài ra cũng nên sử dụng chữ viết hoa, số, và một vài ký tự đặc biệt.

- Ngay cả khi mật khẩu Wi-Fi của bạn cực kỳ mạnh, bạn cũng cần phải thay đổi nó nếu thấy những dấu hiệu đầu tiên của việc bị trộm mật khẩu Wi-Fi. Giống như bất kỳ mật khẩu nào, bạn nên thường xuyên thay đổi để tăng tính bảo mật bằng những cụm từ mới vài tháng một lần.

Chương 2

GIAO THỨC BẢO MẬT WPA3

2.1. Tổng quan về giao thức WPA3

WPA là từ viết tắt cho Wi-Fi Protected Access, nó là một chứng chỉ bảo mật do Wi-Fi Alliance tạo ra để bảo vệ các kết nối không dây. Bạn có thể hiểu đơn giản rằng WPA là một bộ quy tắc được thiết kế để giúp bảo vệ bộ định tuyến Wi-Fi nhà mình, các thiết bị mà nó kết nối tới cùng những dữ liệu được truyền đi. Nhờ vào một lớp liên lạc trung gian, hai thiết bị đầu và cuối sẽ không cần phải biết được các thông tin "bí mật" của nhau.

WPA2 đang là chuẩn bảo mật được sử dụng ở nước ta hiện tại. Nó được ra mắt vào năm 2004 và là một bước cải tiến lớn so với những gì mà chúng ta phải sử dụng trước đó, song nó đã dần bộc lộ những điểm lỗi thời sau 14 năm hoạt động. Do đó, WPA3 được ra đời để giúp khắc phục những yếu điểm cần được thay thế của phiên bản tiền nhiệm.

Giao thức bảo mật mới cung cấp một số cải tiến lớn cho các thiết bị có hỗ trợ Wi-Fi về cấu hình, xác thực và tăng cường mã hóa, khiến hacker khó tấn công WiFi hoặc rình mò mạng của bạn hơn. Wi-Fi Alliance đã giới thiệu hai loại của giao thức bảo mật mới nhất - WPA3-Personal và WPA3-Enterprise - cho các mạng không dây cá nhân, doanh nghiệp và IoT.

2.1.1. WPA3-Personal cung cấp mã hóa an toàn và cá nhân hơn

WPA3 cung cấp các cải tiến cho mã hóa Wi-Fi chung, nhờ Xác thực đồng thời (SAE) thay thế phương thức xác thực Khóa trước chia sẻ (PSK) được sử dụng trong các phiên bản WPA trước. Điều này cho phép chức năng bảo mật tốt hơn vì vậy các mạng WPA3-Personal với một cụm mật khẩu đơn giản nhưng không đơn giản để tin tặc bẻ khóa bằng cách sử dụng các nỗ lực bẻ khóa ngoài trang web, vũ phu, dựa trên từ điển như với WPA/WPA2. Tất nhiên, mọi người vẫn sẽ dễ dàng đoán được mật khẩu rất đơn giản khi họ cố kết nối trực tiếp với Wi-Fi bằng thiết

bị, nhưng đó là một phương pháp bẻ khóa ít thực tế hơn.

Mã hóa với WPA3-Personal được cá nhân hóa nhiều hơn. Người dùng trên mạng WPA3-Personal không thể rình mò lưu lượng WPA3-Personal của người khác, ngay cả khi người dùng có mật khẩu Wi-Fi và được kết nối thành công. Hơn nữa, nếu người ngoài xác định mật khẩu, không thể thụ động quan sát một trao đổi và xác định các khóa phiên, cung cấp bảo mật chuyển tiếp của lưu lượng mạng. Thêm vào đó, họ không thể giải mã bất kỳ dữ liệu nào được ghi lại trước khi bẻ khóa.

Wi-Fi Easy Connect là một tính năng tùy chọn được công bố gần đây có vẻ như sẽ xuất hiện với nhiều thiết bị WPA3-Personal, có thể thay thế hoặc được sử dụng cùng với tính năng Thiết lập bảo vệ Wi-Fi (WPS) đi kèm với WPA/WPA2. WiFi Easy Connect đang được thiết kế để giúp kết nối các thiết bị IoT và màn hình không hiển thị với Wi-Fi dễ dàng hơn. Điều này có thể bao gồm một phương thức nút tương tự như WPS, nhưng cũng có thể thêm các phương thức bổ sung, như quét mã QR của thiết bị từ điện thoại thông minh để kết nối thiết bị một cách an toàn.

2.1.2. WPA3-Enterprise nhắm mục tiêu Wi-Fi quy mô lớn

Đối với WPA3-Enterprise, có bảo mật 192bit tùy chọn được thêm vào để bảo vệ tốt hơn. Đây có thể là một tính năng được hoan nghênh cho các tổ chức chính phủ, các tập đoàn lớn và các môi trường rất nhạy cảm khác. Tuy nhiên, tùy thuộc vào việc triển khai máy chủ RADIUS cụ thể, chế độ bảo mật 192bit trong WPA3-Enterprise có thể yêu cầu các bản cập nhật liên quan đến thành phần máy chủ EAP của máy chủ RADIUS.

Một số bộ thuật toán mật mã trong EAP được sử dụng với WPA3-Enterprise:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384: ECDHE và ECDSA sử dụng số nguyên tố 384-bit

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384: ECDHE sử dụng số

nguyên tố 384-bit; số module RSA ≥ 3072-bit

- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384: số module RSA ≥ 3072-bit và DHE ≥ 3072-bit.

2.2. Sự khác biệt giữa giao thức WPA3 và các giao thức khác

2.2.1. WEP (Wired Equivalent Privacy)

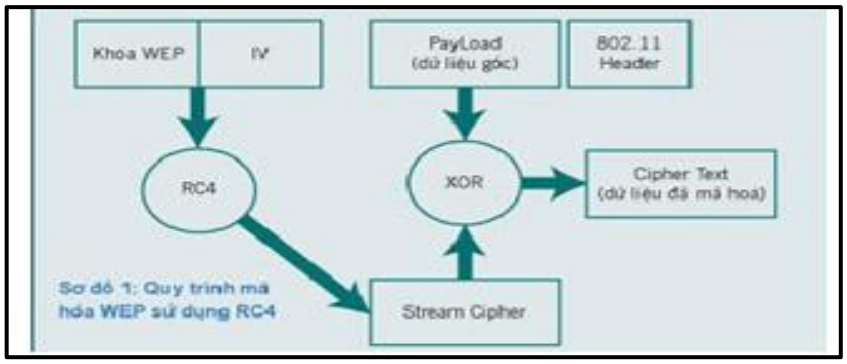
Chuẩn Wired Epuivalent Privacy (WEP) được tạo ra để cung cấp cho các mạng không dây các tính năng an toàn và bảo mật tương tự như các mạng có dây. WEP được định nghĩa là cơ chế mật mã tùy chọn được sử dụng để cung cấp bảo mật dữ liệu tương đương với tính bảo mật của môi trường mạng cục bộ có dây (LAN). Ý tưởng cơ bản về cách thức WEP được tạo ra và mục đích ban đầu của nó nhằm đáp ứng các mục tiêu và giải quyết ba nguyên lý bảo mật thông tin: bảo mật, tính khả dụng và tính toàn vẹn.

- Mục tiêu cơ bản của WEP là ngăn chặn nghe lén, đảm bảo tính bí mật.

- Mục tiêu thứ hai là cho phép truy cập được ủy quyền vào mạng không dây, đảm bảo tính khả dụng.

- Mục tiêu thứ ba là ngăn chặn sự can thiệp của bất kỳ giao tiếp không dây nào, đảm bảo tính toàn vẹn.

Giao thức WEP dựa trên mật mã dòng RC4 của RSA Securities. Mật mã này được áp dụng cho phần thân của mỗi khung và CRC. Có hai mức WEP thường có sẵn: một mức dựa trên khóa mã hóa 40 bit và vectơ khởi tạo 24 bit, tương đường 64 bit; và một dựa trên khóa mã hóa 104 bit và vectơ khởi tạo 24 bit, tương đương 128 bit.



Hình 2.1: Quy trình mã hóa WEP sử dụng RC4

Do WEP sử dụng RC4, một thuật toán sử dụng phương thức mã hóa dòng, nên cần một cơ chế đảm bảo hai dữ liệu giống nhau sẽ không cho kết quả giống nhau sau khi được mã hóa hai lần khác nhau. Đây là một yếu tố quan trọng trong vấn đề mã hóa dữ liệu nhằm hạn chế khả năng suy đoán khóa của hacker. Để đạt mục đích trên, một giá trị (Initializtion Vector) được sử dụng để cộng thêm với khóa nhằm tạo ra khóa khác nhau mỗi lần mã hóa. IV là một giá trị có chiều dài 24 bit và được chuẩn IEEE 802.11 đề nghị (không bắt buộc) phải thay đổi theo từng gói dữ liệu. Vì máy gửi tạo ra IV không theo định luật hay tiêu chuẩn, IV bắt buộc phải được gửi đến máy nhận ở dạng không mã hóa. Máy nhận sẽ sử dụng giá trị IV và khóa để giải mã gói dữ liệu.

Cách sử dụng giá trị IV là nguồn gốc của đa số các vấn đề với WEP. Do giá trị IV được truyền đi ở dạng không mã hóa và đặt trong header của gói dữ liệu 802.11 nên bất cứ ai thu được dữ liệu trên mạng đều có thể thấy được. Với độ dài 24 bit, giá trị của IV dao động trong khoảng 16.777.216 trường hợp. Những chuyên gia bảo mật tại đại học Califonia-Berkeley đã phát hiện ra là khi cùng giá trị IV được sử dụng với cùng khóa trên một gói dữ liệu mã hóa (khái niệm này được gọi nôm na là va chạm IV), hacker có thể bắt gói dữ liệu và tìm ra được khóa WEP. Thêm vào đó, ba nhà phân tích mã hóa Fluhrer, Mantin và Shamir (FMS) đã vạch ra một phương pháp phát hiện và sử dụng những IV lỗi nhằm tìm ra khóa WEP.

Thêm vào đó, một trong những mối nguy hiểm lớn nhất là những cách tấn

công dùng hai phương pháp nêu trên đều mang tính chất thụ động. Có nghĩa là kẻ tấn công chỉ cần thu nhận các gói dữ liệu trên đường truyền mà không cần liên lạc với Access Point. Điều này khiến khả năng phát hiện các tấn công tìm khóa WEP đầy khó khăn và gần như không thể phát hiện được.

Để gia tăng mức độ bảo mật cho WEP và gây khó khăn cho hacker, các biện pháp sau được đề nghị:

- Sử dụng khóa WEP có độ dài 128 bit: thường các thiết bị WEP cho phép cấu hình khóa ở ba đội dài: 40 bit, 64 bit, 128 bit. Sử dụng khóa với độ dài 128 bit gia tăng số lượng gói dữ liệu hacker cần phải có để phân tích IV, gây khó khăn và kéo dài thời gian giải mã khóa WEP.

- Thực thi chính sách thay đổi khóa WEP định kỳ: Do WEP không hỗ trợ phương thức thay đổi khóa tự động nên sự thay đổi khóa định kỳ sẽ gây khó khăn cho người sử dụng. Tuy nhiên, nếu không đổi khóa WEP thường xuyên thì cũng nên thực hiện ít nhất một lần trong tháng hoặc khi nghi ngờ có khả năng bị lộ khóa.

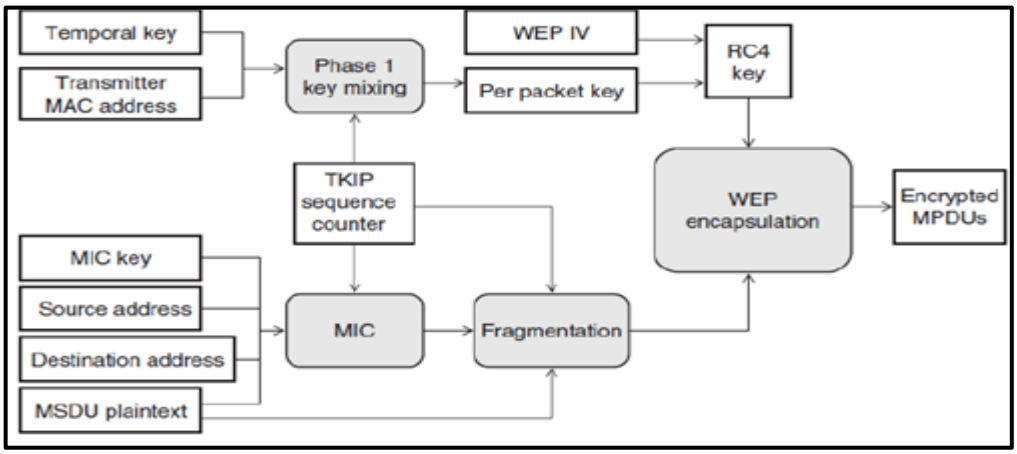
- Sử dụng các công cụ theo dõi số liệu thống kê dữ liệu trên đường truyền không dây: Do các công cụ dò khóa WEP cần bắt được số lượng lớn gói dữ liệu và hacker có thể phải sử dụng các công cụ phát sinh dữ liệu nên sự đột biến về lưu lượng dữ liệu có thể là dấu hiệu của một cuộc tấn công WEP, đánh động người quản trị mạng phát hiện và áp dụng các biện pháp phòng chống kịp thời.

2.2.2. WPA (WI-FI Protected Access)

Truy cập Wi-Fi được bảo vệ (WPA), người kế thừa nối tiếp WEP, là một giao thức bảo mật chuẩn IEEE 802.11i. WPA được tạo bởi Wi-Fi Alliance như một giải pháp tạm thời để thay thế WEP trước khi chuẩn 802.11i sẵn sàng. WPA cải thiện đáng kể quá trình mã hóa của WEP và thêm cơ chế xác thực người dùng cụ thể. Trong WPA người dùng có thể được xác thực thông qua một máy chủ xác thực IEEE 802.1X(thường là một máy chủ RADIUS) hoặc thông qua một điểm truy cập với một mật khẩu trong chế độ khóa chia sẻ trước (PSK). WPA cũng cung cấp các nâng cấp phần mềm để thực hiện khả năng tương tác với các card mạng cũ và các

điểm truy cập.

WPA sử dụng mật mã dòng RC4 với khóa 128 bit và mã hóa 48 bit trong mã hóa. RC4 vẫn được sử dụng, vì nó tương thích với phần cứng cũ. Ngoài ra, WPA còn giới thiệu một giao thức bảo mật quan trọng mới, giao thức toàn vẹn khóa tạm thời (TKIP), khóa được tự động thay đổi trong suốt phiên làm việc. Kết quả là việc lặp lại các khóa làm việc giống nhau được ngăn chặn. TKIP sử dụng một trình tự sắp xếp gói tin và chức năng trộn hai pha cho mỗi gói tin. Trình tự sắp xếp gói tin có nghĩa là mọi khóa mã hóa được liên kết với một số thứ tự. Điều này ngăn chặn các cuộc tấn công phát lại hiệu quả. Chức năng trộn gói tin sẽ lấy số thứ tự này cùng với khóa WPA cơ sở và địa chỉ MAC của máy phát làm đầu vào và xuất ra một khóa WPA mới cho mỗi gói. Khóa WPA mới này sau đó được dử dụng cùng với IV để tạo khóa WPA sử dụng mật mã dòng RC4 với khóa 128 bit và mã hóa 48 bit trong mã hóa.



Hình 2.2: Quy trình trộn và mã hóa của TKIP

TKIP cũng tăng cường tính toàn vẹn của các gói tin bằng cách thêm trường kiểm tra tích hợp tin nhắn (MIC) để bảo vệ chống lại các giả mạo. Giá trị của MIC được tính toán bằng thuật toán mã hóa được gọi là Michael. Michael sử dụng khóa 64 bit và chia các gói thành các khối 32 bit. Sau đó, xử lý từng khối 32 bit thành hai thanh ghi 32 bit, nghĩa là xác thực 64 bit. Michael cũng cung cấp một tính năng bổ sung, tức là một cơ chế đối phó đặc biệt, phát hiện bất kỳ nỗ lực nào để phá vỡ TKIP và kết quả là chặn liện lạc với kẻ tấn công. WPA có hai tùy chọn để xác thực

người dùng. Tùy chọn đầu tiên, máy chủ xác thực, được gọi là WPA-Enterprise. WPA-Enterprise sử dụng giao thức xác thực mở rộng (EAP) cùng với xác thực lẫn nhau để người dùng không dây vô tình tham gia vào mạng giả mạo. EAP không phải là một cơ chế xác thực thực tế mà là một khung xác thực, cung cấp một số chức năng phổ biến và một cuộc đàm phán về cơ chế xác thực mong muốn. Máy chủ xác thực hoạt động theo nguyên tắc sau:

- Máy chủ xác thực chấp nhận thông tin đăng nhập của người dùng.

- Máy chủ xác thực sử dụng 802.1X và EAP để tạo khóa chính duy nhất

- 802.1X phân phối khóa cho AP và máy khách

- TKIP thiết lập một hệ thống phân cấp và quản lý khóa bằng cách sử dụng khóa chính. Nói cách khác, các khóa mã dùng để mã hóa mọi gói dữ liệu được tạo ra từ khóa chính.

Tùy chọn thứ hai, chế độ PSK, được gọi là WPA-Personal. WPA-Personal được thiết kế cho các mạng gia đình và văn phòng nhỏ, không thể trang bị máy chủ xác thực. Trong chế độ này, người dùng xác thực với Access Point(AP) bằng cụm mật khẩu từ 8-63 ký tự ASCII hoặc 64 chữ số thập lục phân. Nếu các ký tự ASII được chọn, hàm băm sẽ giảm nó từ các bit 504(63 ký tự*8bit/ký tự) thành 256 bit. Cụm mật khẩu có thể được lưu trữ và tự động được sử dụng trên máy tính của người dùng trong hầu hết các hệ điều hành. Chế độ PSK cũng sử dụng chức năng dẫn xuất khóa PBKDF2, sử dụng một quá trình lặp đi lặp lại của hàm băm mật mã vào cụm mật khẩu. Kết quả là mật khẩu mạnh hơn và an toàn hơn được tạo ra. Tuy nhiên việc chọn một mật khẩu yếu vẫn có thể dẫn đến một cuộc tấn công mật khẩu.

2.2.3. WPA 2 (WI-FI Protected Access 2)

WPA2 dựa trên chuẩn IEEE 802.11i. Ngoài thuật toán TKIP , MIC và Michael, nó còn cung cấp một thuật toán CCMP dựa trên mật mã khối AES mới, để thay thế mật mã dòng RC4 cũ. Giống như TKIP, CCMP sử dụng IV 48 bit làm số thứ tự để phát hiện phát lại. Nhưng thay vì mỗi chức năng dẫn xuất khóa gói,

CCMP sử dụng khóa AES duy nhất để bảo vệ tính bảo mật và tính toàn vẹn của thông điệp.

Trong WPA2, AES được định nghĩa trong cơ chế chuỗi mã khối truy cập (CCM) và hỗ trợ Bộ dịch vụ cơ bản độc lập (IBSS), cho phép bảo mật giữa các máy trạm làm việc trong chế độ ad-hoc. WPA2 cũng cung cấp khả năng tương tác giữa máy trạm WPA và WPA2, cho phép chuyển đổi theo thứ tự từ WPA sang WPA2 mà không ảnh hưởng đến bảo mật. Các tính năng mới khác trong WPA2 được giảm thời gian trong quá trình trao đổi xác thực, lưu trữ khóa, khi chuyển vùng giữa các điểm truy cập và trao đổi xác thực trước khi chuyển vùng. Mối quan hệ giữa WPA2, WPA và WEP được trình bày trong bảng:

Bảng 2.1: So sánh WEP, WPA và WPA2

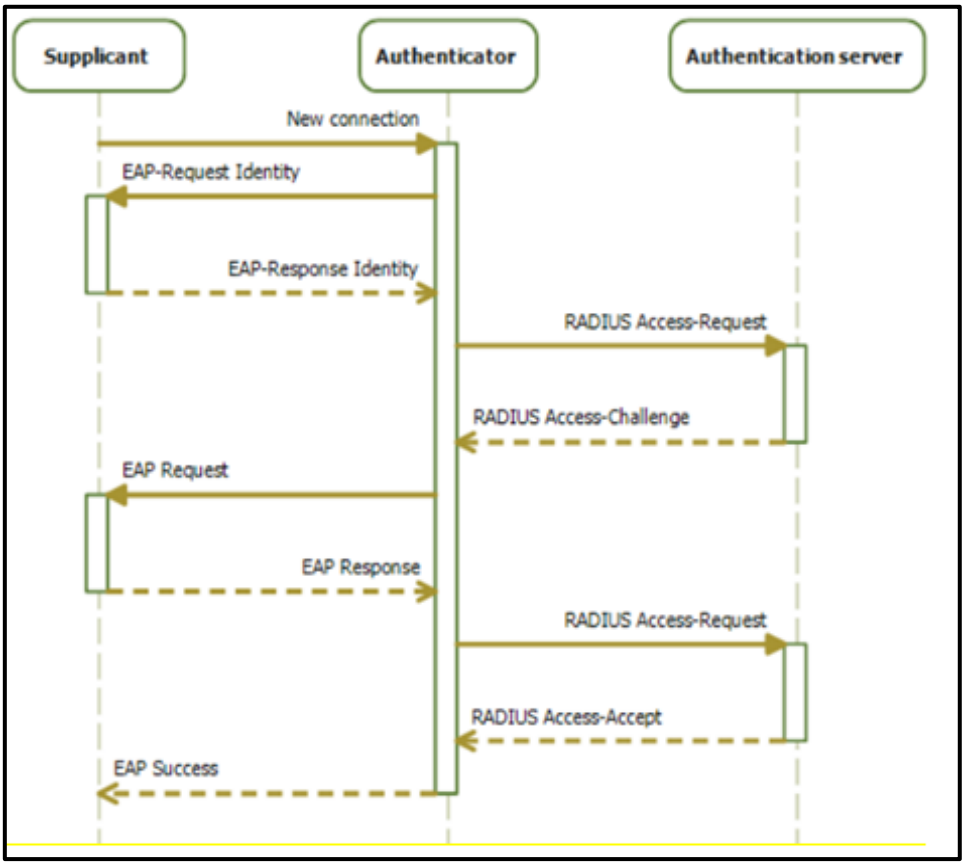
	WEP	WPA	WPA2
Encryption cip.	RC4	RC4	AES
Key sizes	40/104 bit	128 bit	128 bit
IV size	24 bit	48 bit	48 bit
Per-packet key	Key + IV	TKIP mix.fc.	CCM
Data integrity	CRC-32	Michael	CCM
Replay detection	None	IV seq.	IV seq.
Key mng.	None	802.1X	802.1X

Một trong những thay đổi chính được giới thiệu với tiêu chuẩn WPA2 là sự tách biệt xác thực người dùng khỏi việc thực thi quyền riêng tư và tính toàn vẹn của thông điệp, qua đó cung cấp một kiến trúc bảo mật mạnh mẽ và mở phù hợp với mạng gia đình hoặc mạng công ty. WPA2 cung cấp 2 chế độ xác thực:

- Chế độ Personal: Xác thực ở chế độ Personal, WPA2 không yêu cầu máy chủ xác thực và được thực hiện giữa máy khách và AP, nó tạo một PSK 256 bit từ một cụm từ văn bản thuần (từ 8 đến 63 ký tự). PSK kết hợp với Bộ nhận dạng dịch vụ và độ dài SSID tạo thành cơ sở toán học cho ra khóa chính kép (PMK) sẽ được sử dụng sau này trong tạo khóa.

- Chế độ Enterprise: Xác thực trong chế độ Enterprise dựa trên tiêu chuẩn

xác thực IEEE 802.1X. Các thành phần chính là clien trong mạng, xác thực AP cung cấp điều khiển truy cập và máy chủ xác thực (RADIUS) đưa ra các quyết định ủy quyền. Xác thực AP chia mỗi cổng ảo thành hai cổng một cho dịch vụ và cổng kia để xác thực, tạo nên PAE (Port Access Entity). PAE xác thực luôn được mở để cho phép các khung xác thực thông qua, trong khi dịch vụ PAE chỉ mở khi xác thực thành công bởi máy chủ RADIUS. Trình hỗ trợ và trình xác thực giao tiếp sử dụng lớp 2 EAPoL (EAP qua LAN), chuyển đổi các thông báo EAPoL thành các tin nhắn RADIUS và sau đó chuyển tiếp chúng tới máy chủ RADIUS. Máy chủ xác thực (RADIUS), phải tương thích với các loại EAP của người bổ trợ, nhận và xử lý yêu cầu xác thực. Một khi quá trình xác thực hoàn tất, người thẩm định và người xác thực có một Master Key (MK) bí mật như trong hình:



Hình 2.3: Xác thực 802.1X

2.2.4. WPA 3 (WI-FI Protected Access 3)

WPA3 yêu cầu áp dụng Khung quản lý được bảo vệ, giúp bảo vệ chống lại

việc nghe trộm và giả mạo. Nó cũng tiêu chuẩn hóa bộ mật mã 128 bit và không cho phép các giao thức bảo mật lỗi thời. WPA3 Enterprise có mã hóa bảo mật 192 bit tùy chọn và IV 48 bit để bảo vệ cao hơn đối với dữ liệu nhạy cảm của công ty, tài chính và chính phủ. WPA3 Personal sử dụng CCMP-128 và AES-128.

WPA3 giải quyết lỗ hổng KRACK của WPA2 bằng kiểu bắt tay mật mã an toàn hơn, thay thế kiểu bắt tay bốn chiều PSK bằng Xác thực đồng thời bằng (SAE), một phiên bản của kiểu bắt tay chuồn chuồn của Lực lượng đặc nhiệm kỹ thuật Internet trong đó máy khách hoặc AP có thể bắt đầu liên hệ. Sau đó, mỗi thiết bị sẽ truyền thông tin xác thực của nó trong một tin nhắn rời rạc, một lần, thay vì trong một cuộc trò chuyện nhiều phần, cho và nhận. Điều quan trọng, SAE cũng loại bỏ việc sử dụng lại các khóa mã hóa, yêu cầu mã mới với mọi tương tác. Nếu không có giao tiếp mở giữa AP và ứng dụng khách hoặc sử dụng lại khóa mã hóa, tội phạm mạng không thể dễ dàng nghe trộm hoặc tự đưa chúng vào một cuộc trao đổi.

SAE giới hạn người dùng trong các nỗ lực xác thực tại chỗ, đang hoạt động, gắn cờ cho bất kỳ ai đã vượt quá một số lần đoán mật khẩu nhất định. Khả năng này sẽ làm cho mạng Wi-Fi điển hình có khả năng chống lại các cuộc tấn công từ điển ngoại tuyến tốt hơn. Bằng cách yêu cầu một cụm mật khẩu mã hóa mới cho mỗi kết nối, SAE cũng cho phép một tính năng được gọi là bí mật chuyển tiếp , nhằm mục đích ngăn những kẻ tấn công bẻ khóa mật mã sử dụng nó để giải mã dữ liệu mà chúng đã bắt và lưu trước đó.

* Sự khác biệt của giao thức WPA3 với các giao thức:

- WPA dễ bị tấn công: Mặc dù sở hữu tính năng mã hóa khóa công khai mạnh và sử dụng WPA-PSK 256 bit (Pre Shared Key), WPA vẫn còn một số lỗ hổng "thừa hưởng" từ tiêu chuẩn WEP cũ (cả hai đều có chung tiêu chuẩn mã hóa luồng dễ bị tấn công, RC4).

Các lỗ hổng tập trung vào việc giới thiệu Temporal Key Integrity Protocol (TKIP).

Bản thân TKIP là một bước tiến lớn, vì nó sử dụng hệ thống key trên mỗi gói để bảo vệ từng gói dữ liệu được gửi giữa các thiết bị. Thật không may, việc triển khai TKIP WPA phải tính đến cả các thiết bị WEP cũ.

Hệ thống TKIP WPA mới đã "tái chế" một số khía cạnh của hệ thống WEP dễ bị tấn công và tất nhiên, những lỗ hổng tương tự đó cũng đã xuất hiện trong tiêu chuẩn mới.

WPA2 thay thế WPA: WPA2 chính thức thay thế WPA vào năm 2006. Nhưng dù sao WPA đã từng có một thời gian ngắn là "đỉnh cao" của mã hóa WiFi.

WPA2 mang đến một bản nâng cấp bảo mật và mã hóa khác, đáng chú ý nhất là việc giới thiệu Advanced Encryption Standard (AES) cho các mạng WiFi tiêu dùng. AES mạnh hơn đáng kể so với RC4 (vì RC4 đã từng bị "bẻ khóa" nhiều lần) và là tiêu chuẩn bảo mật được áp dụng cho nhiều dịch vụ trực tuyến tại thời điểm hiện tại.

WPA2 cũng giới thiệu Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (Chế độ mã hóa truy cập với giao thức mã xác thực thông báo chuỗi khối), gọi tắt là CCMP, để thay thế TKIP dễ bị tấn công hiện nay.

TKIP vẫn là một phần của tiêu chuẩn WPA2, cũng như cung cấp chức năng cho các thiết bị chỉ có WPA.

Tấn công KRACK WPA2: Cuộc tấn công KRACK là lỗ hổng đầu tiên được tìm thấy trong WPA2. Key Reinstallation Attack (KRACK) là một cuộc tấn công trực tiếp vào giao thức WPA2 và không may làm suy yếu mọi kết nối WiFi bằng WPA2. Về cơ bản, KRACK làm suy yếu khía cạnh quan trọng trong quy trình bắt tay 4 bước của WPA2, cho phép tin tặc chặn và thao túng việc tạo khóa mã hóa mới trong quy trình kết nối an toàn.

Nhưng ngay cả khi KRACK có sức sát thương mạnh đến vậy, thì khả năng ai đó sử dụng công cụ này để tấn công mạng gia đình cũng rất mong manh.

WPA3: Sự đáp trả của WiFi Alliance. WPA3 ra đời hơi muộn nhưng cung

cấp bảo mật cao hơn nhiều. Chẳng hạn, WPA3-Personal cung cấp mã hóa cho người dùng ngay cả khi tin tặc đã "bẻ khóa" mật khẩu sau khi kết nối với mạng.

Hơn nữa, WPA3 yêu cầu tất cả các kết nối sử dụng Protected Management Frames (PMF). PMF về cơ bản tăng cường bảo vệ quyền riêng tư, với các cơ chế bảo mật bổ sung để bảo mật dữ liệu.

Chuẩn AES 128 bit vẫn được giữ nguyên cho WPA3 (một minh chứng cho tính bảo mật "trường tồn" của nó). Tuy nhiên, các kết nối WPA3-Enterprise vẫn cần có AES 198bit. Người dùng WPA3-Personal cũng sẽ có tùy chọn sử dụng AES 198bit cường độ cao.

2.3. Sự an toàn và cần thiết của giao thức bảo mật WPA3

WPA3 là thế hệ bảo mật WiFi tiếp theo. Bảo vệ Wi-Fi khỏi tin tặc là một trong những nhiệm vụ quan trọng nhất trong an ninh mạng. Đó là lý do tại sao sự xuất hiện của giao thức bảo mật không dây thế hệ tiếp theo WPA3 đáng được bạn quan tâm: Nó không chỉ giúp giữ cho các kết nối Wi-Fi an toàn hơn mà còn giúp bạn tránh khỏi những thiếu sót về bảo mật của chính mình.

Đây là những gì nó cung cấp:

- Mật khẩu bảo vệ:

Bắt đầu với cách WPA3 sẽ bảo vệ bạn tại nhà. Cụ thể, nó sẽ giảm thiểu thiệt hại có thể xuất phát từ mật khẩu lười biếng của bạn.

Một điểm yếu cơ bản của WPA2, giao thức bảo mật không dây hiện tại có từ năm 2004, là nó cho phép tin tặc triển khai một cuộc tấn công từ điển ngoại tuyến để đoán mật khẩu của bạn. Kẻ tấn công có thể chụp bao nhiêu bức ảnh mà chúng muốn khi đoán thông tin đăng nhập của bạn mà không ở trên cùng một mạng, xem xét toàn bộ từ điển và hơn thế nữa theo thứ tự tương đối ngắn.

WPA3 sẽ bảo vệ khỏi các cuộc tấn công từ điển bằng cách triển khai một giao thức trao đổi khóa mới. WPA2 đã sử dụng kiểu bắt tay bốn chiều không hoàn hảo giữa máy khách và điểm truy cập để kích hoạt các kết nối được mã hóa; đó là những gì đằng sau lỗ hổng KRACK khét tiếng ảnh hưởng đến cơ bản mọi thiết bị được kết nối. WPA3 sẽ loại

bỏ điều đó để chuyển sang chế độ bắt tay Xác thực Bình đẳng an toàn hơn và được kiểm tra rộng rãi. Đồng thời.

Tuy nhiên, lợi ích khác đi kèm trong trường hợp mật khẩu của bạn bị xâm phạm. Với sự bắt tay mới này, WPA3 hỗ trợ bảo mật chuyển tiếp, có nghĩa là bất kỳ lưu lượng truy cập nào đi qua chuyển đổi của bạn trước khi người ngoài có quyền truy cập sẽ vẫn được mã hóa. Với WPA2, họ cũng có thể giải mã lưu lượng cũ.

- Kết nối an toàn hơn:

Khi WPA2 xuất hiện vào năm 2004, Internet of Things vẫn chưa trở thành bất cứ thứ gì gần với nỗi kinh hoàng về bảo mật vốn là dấu ấn ngày nay của nó. Do đó, không có gì ngạc nhiên khi WPA2 không đưa ra cách hợp lý nào để kết nối các thiết bị này một cách an toàn với mạng Wi-Fi hiện có. Và trên thực tế, phương pháp chủ yếu mà quá trình đó xảy ra ngày nay Wi-Fi Protected Setup đã có các lỗ hổng bảo mật được biết đến từ năm 2011. WPA3 cung cấp một bản sửa lỗi.

Wi-Fi Easy Connect, như Wi-Fi Alliance gọi nó, giúp việc đưa các thiết bị không dây không có (hoặc hạn chế) vào mạng của bạn dễ dàng hơn. Khi được bật, bạn chỉ cần sử dụng điện thoại thông minh để quét mã QR trên bộ định tuyến, sau đó quét mã QR trên máy in hoặc loa hoặc thiết bị IoT khác của bạn và bạn đã thiết lập chúng được kết nối an toàn. Với phương pháp mã QR, bạn đang sử dụng mã hóa dựa trên khóa công khai cho các thiết bị tích hợp hiện hầu hết thiếu phương pháp đơn giản, an toàn để làm như vậy.

Xu hướng đó cũng diễn ra với Wi-Fi Enhanced Open, mà Wi-Fi Alliance đã trình bày chi tiết vài tuần trước đó. Có thể bạn đã nghe nói rằng bạn nên tránh thực hiện bất kỳ thao tác duyệt hoặc nhập dữ liệu nhạy cảm nào trên các mạng Wi-Fi công cộng. Đó là bởi vì với WPA2, bất kỳ ai trên cùng một mạng công cộng với bạn đều có thể quan sát hoạt động của bạn và nhắm mục tiêu bạn bằng các hành vi xâm nhập như tấn công man-in-the-middle hoặc đánh hơi lưu lượng truy cập. Trên WPA3? Không nhiều lắm.

Khi bạn đăng nhập vào Wi-Fi WPA3 bằng thiết bị WPA3, kết nối của bạn sẽ tự động được mã hóa mà không cần thêm thông tin đăng nhập. Nó làm như vậy bằng cách sử dụng một tiêu chuẩn đã được thiết lập gọi là mã hóa không dây cơ hội.

Cũng như các biện pháp bảo vệ bằng mật khẩu, mã hóa mở rộng của WPA3 cho các mạng công cộng cũng giúp người dùng Wi-Fi an toàn trước lỗ hổng bảo mật mà họ có thể không nhận ra là tồn tại ngay từ đầu. Trên thực tế, nếu có bất cứ điều gì nó có thể khiến người dùng Wi-Fi cảm thấy quá an toàn.

2.4. Một số tấn công lên giao thức WPA3

2.4.1. Tấn công dựa trên cảm nhận sóng mang lớp vật lý

Ta có thể hiểu nôm na là: Kẻ tất công lợi dụng giao thức chống đụng độ CSMA/CA, tức là nó sẽ làm cho tất cả người dùng nghĩ rằng lúc nào trong mạng cũng có 1 máy tính đang truyền thông. Điều này làm cho các máy tính khác luôn luôn ở trạng thái chờ đợi kẻ tấn công ấy truyền dữ liệu xong dẫn đến tình trạng nghẽn trong mạng.

Tần số là một nhược điểm bảo mật trong mạng không dây. Mức độ nguy hiểm thay đổi phụ thuộc vào giao diện của lớp vật lý. Có một vài tham số quyết định sự chịu đựng của mạng là: năng lượng máy phát, độ nhạy của máy thu, tần số RF (Radio Frequency), băng thông và sự định hướng của anten. Trong 802.11 sử dụng thuật toán đa truy cập cảm nhận sóng mang (CSMA) để tránh va chạm. CSMA là một thành phần của lớp MAC. CSMA được sử dụng để chắc chắn rằng sẽ không có va chạm dữ liệu trên đường truyền. Kiểu tấn công này không sử dụng tạp âm để tạo ra lỗi cho mạng nhưng nó sẽ lợi dụng chính chuẩn đó. Có nhiều cách để khai thác giao thức cảm nhận sóng mang vật lý. Cách đơn giản là làm cho các nút trong mạng đều tin tưởng rằng có một nút đang truyền tin tại thời điểm hiện tại. Cách dễ nhất đạt được điều này là tạo ra một nút giả mạo để truyền tin một cách liên tục. Một cách khác là sử dụng bộ tạo tín hiệu RF. Một cách tấn công tinh vi hơn là làm cho card mạng chuyển vào chế độ kiểm tra mà ở đó nó truyền đi liên tiếp một mẫu kiểm tra. Tất cả các nút trong phạm vi của một nút giả là rất nhạy với sóng mang và trong khi có một nút đang truyền thì sẽ không có nút nào được truyền.

2.4.2. Tấn công kênh bên dựa trên thời gian

Với WPA3, đối thủ có thể khôi phục mật khẩu của mạng Wi-Fi được coi là không khả thi. Thật không may, các nhà nghiên cứu đã phát hiện ra rằng số lần AP cần để phản hồi các khung cam kết có thể rò rỉ thông tin về mật khẩu. Khi AP sử dụng các nhóm bảo mật dựa trên các đường cong elip NIST, tất cả các thiết bị WPA3 được yêu cầu hỗ trợ, không có thông tin về thời gian nào bị rò rỉ. Tuy nhiên, khi AP hỗ trợ các đường cong

Brainpool hoặc nhóm bảo mật nhân số modulo một số nguyên tố (nhóm MODP), thời gian phản hồi phụ thuộc vào mật khẩu được sử dụng. Một kẻ thù có thể lạm dụng thông tin này để thực hiện một cuộc tấn công từ điển, bằng cách mô phỏng AP sẽ mất bao nhiêu thời gian để AP xử lý từng mật khẩu và so sánh thông tin này với thời gian quan sát được. Các nhà nghiên cứu nhận xét rằng trái với một số tuyên bố, Dragonfly thực sự được thiết kế để hỗ trợ các nhóm bảo mật nhân (MODP). Rốt cuộc, biến thể Dragonfly được sử dụng trong TLS-PWD bao gồm một thay đổi nhỏ để các nhóm MODP này có thể được sử dụng một cách an toàn. Thật không may, những thay đổi đó không được đưa vào biến thể Dragonfly được sử dụng trong WPA3.

2.4.3. Tấn công kênh bên dựa trên bộ nhớ cache

Khi tấn công có thể quan sát các mẫu truy cập bộ nhớ trên thiết bị của nạn nhân thì nó sẽ xây dựng khung cam kết của cái bắt tay Dragonfly, các mẫu truy cập bộ nhớ này sẽ tiết lộ thông tin về mật khẩu đang được sử dụng. Quan sát các mẫu này là có thể biết nếu đối phương kiểm soát bất kỳ ứng dụng nào trên thiết bị của nạn nhân và thậm chí có thể khi đối phương kiểm soát mã JavaScript (ngôn ngữ lập trình thông dịch- được dịch lúc chạy) trong trình duyệt của nạn nhân. Các mẫu bị rò rỉ có thể được sử dụng để thực hiện một cuộc tấn công từ điển, bằng cách mô phỏng các mẫu truy cập bộ nhớ được liên kết với mật khẩu đã đoán và so sánh nó với các mẫu truy cập được đo. Các nhà nghiên cứu tin rằng các giao thức hiện đại sẽ cung cấp những hướng dẫn rõ ràng về cách ngăn chặn các mẫu truy cập bộ nhớ bị rò rỉ thông tin bí mật. Do đó, các nhà nghiên cứu coi đây là một lỗ hổng trong đặc điểm kỹ thuật bắt tay Dragonfly của WPA3.

2.4.4. Tấn công từ chối dịch vụ

Thiết bị khởi tạo bắt tay Dragonfly bắt đầu bằng cách gửi khung cam kết. Xử lý khung này và tạo ra một câu trả lời là mất thời gian về mặt tính toán, đặc biệt là nếu việc bảo vệ chống lại các cuộc tấn công kênh bên (đã biết) được thực hiện. Mặc dù WPA3 chứa phương thức trao đổi cookie để ngăn kẻ tấn công giả mạo các khung cam kết sử dụng địa chỉ MAC giả, nhưng việc bỏ qua là chuyện nhỏ. Do đó, kẻ tấn công có thể làm quá tải Điểm truy cập (AP) bằng cách tạo ra ít nhất 16 khung cam kết giả mạo mỗi giây. Cuộc tấn công tiêu thụ tài nguyên này gây ra việc sử dụng CPU cao trên AP, làm cạn kiệt pin, ngăn chặn hoặc trì hoãn các thiết bị khác kết nối với AP bằng WPA3 và cũng có thể

ngăn chặn hoặc làm chậm chức năng khác của AP.

Mặc dù cuộc tấn công có thể được giảm thiểu bằng cách xử lý khung cam kết trong luồng nền có mức độ ưu tiên thấp, các biến thể của cuộc tấn công vẫn có thể xảy ra. Tùy thuộc vào sự bảo vệ chính xác mà các nhà cung cấp thực hiện, vẫn có thể kích hoạt mức sử dụng CPU cao trên AP hoặc có thể ngăn chặn hoặc trì hoãn các thiết bị khác kết nối với AP bằng WPA3.

2.4.5. Tấn công yêu cầu xác thực lại

Kẻ tấn công xác định mục tiêu tấn công là các người dùng trong mạng wireless và các kết nối của họ (Access Point đến các kết nối của nó).

Chèn các frame yêu cầu xác thực lại vào mạng WLAN bằng cách giả mạo địa chỉ MAC nguồn và đích lần lượt của Access Point và các người dùng.

Người dùng wireless khi nhận được frame yêu cầu xác thực lại thì nghĩ rằng chúng do Access Point gửi đến.

Sau khi ngắt được một người dùng ra khỏi dịch vụ không dây, kẻ tấn công tiếp tục thực hiện tương tự đối với các người dùng còn lại.

Thông thường người dùng sẽ kết nối lại để phục hồi dịch vụ, nhưng kẻ tấn công đã nhanh chóng tiếp tục gửi các gói yêu cầu xác thực lại cho người dùng.

2.4.6. Tấn công ngắt kết nối

- Kẻ tấn công xác định mục tiêu (wireless clients) và mối liên kết giữa AP với các clients.

- Kẻ tấn công gửi disassociation frame bằng cách giả mạo Source và Destination MAC đến AP và các client tương ứng.

- Client sẽ nhận các frame này và nghĩ rằng frame hủy kết nối đến từ AP. Đồng thời kẻ tấn công cũng gửi disassociation frame đến AP.

- Sau khi đã ngắt kết nối của một client, kẻ tấn công tiếp tục thực hiện tương tự với các client còn lại làm cho các client tự động ngắt kết nối với AP.

- Khi các clients bị ngắt kết nối sẽ thực hiện kết nối lại với AP ngay lập tức. Kẻ tấn công tiếp tục gửi disassociation frame đến AP và clients.

- Có thể ta sẽ rất dễ nhầm lẫn giữa 2 kiểu tấn công: Disassociation flood attack và De-authentication Flood Attack.

Giống nhau : Về hình thức tấn công, có thể cho rằng chúng giống nhau vì nó giống như một đại bác 2 nòng, vừa tấn công Access Point vừa tấn công Clients. Và quan trọng hơn hết, chúng "nã pháo" liên tục.

Khác nhau:

De-authentication Flood Attack: Yêu cầu cả AP và client gửi lại frame xác thực xác thực failed.

Disassociation flood attack : Gửi disassociation frame làm cho AP và client tin tưởng rằng kết nối giữa chúng đã bị ngắt.

2.5. Một số công cụ phục vụ tấn công giao thức WPA3

Các công cụ có thể được sử dụng để tấn công WPA3 nhằm mục đích nghiên cứu thử nghiệm và công bố công khai trên Github.

- Dragonslayer: thực hiện các cuộc tấn công đường cong không hợp lệ đối với máy khách và máy chủ EAP-pwd. Các cuộc tấn công này bỏ qua xác thực: kẻ tấn công chỉ cần sở hữu tên người dùng hợp lệ.

- Dragondrain: công cụ này có thể được sử dụng để kiểm tra thời tiết hoặc mở rộng, Điểm truy cập dễ bị tấn công từ chối dịch vụ chống lại bắt tay SAE của WPA3.

- Dragontime: đây là một công cụ thử nghiệm để thực hiện các cuộc tấn công thời gian chống lại bắt tay SAE nếu MODP nhóm 22, 23 hoặc 24 được hỗ trợ. Lưu ý rằng hầu hết các triển khai WPA3 theo mặc định không cho phép các nhóm này.

- Dragonforce: đây là một công cụ thử nghiệm lấy thông tin được phục hồi từ các cuộc tấn công dựa trên bộ nhớ cache hoặc thời gian và thực hiện một cuộc tấn công phân vùng mật khẩu. Điều này tương tự như một cuộc tấn công từ điển.

Chương 3

GIẢI PHÁP VÀ THỬ NGHIỆM HỆ THỐNG MẠNG KHÔNG DÂY SỬ DỤNG GIAO THỨC BẢO MẬT WPA3

3.1. Giới thiệu về công ty CMC telecom

Thông tin công ty:

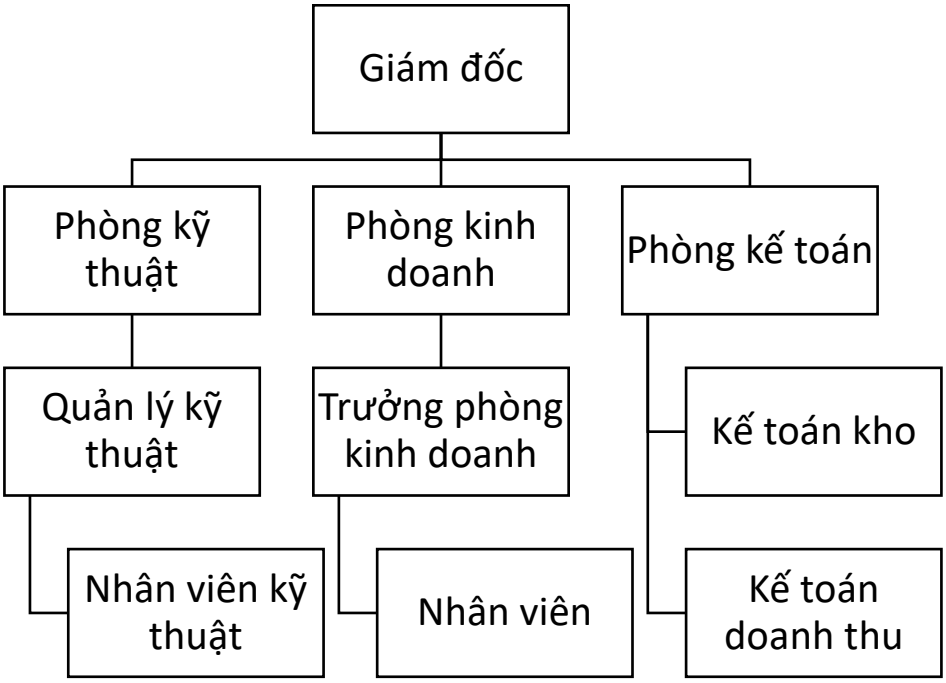
Tên	Công ty Cổ phần hạ tầng viễn thông CMC
Trụ sở chính	Tòa nhà CMC, phố Duy Tân, Quận Cầu Giấy, Thành phố Hà Nội
Chi nhánh	Phòng 710, tầng 7, tòa nhà TD Business Center, Lô 20A đường Lê Hồng Phong, Phường Đông Khê, Ngô Quyền, Hải Phòng.
Số điện thoại	1900 2010
Website	https://cmctelecom.vn
Năm thành lập	1993

CMC Telecom là doanh nghiệp hạ tầng viễn thông duy nhất của Việt Nam có cổ đông nước ngoài, tập đoàn TIME dotCom, tập đoàn viễn thông Top2 Malaysia. CMC Telecom sở hữu mạng đường trục CVCS (Cross Vietnam Cable System), tuyến cáp Việt Nam đầu tiên kết nối xuyên Đông Nam Á, kết nối trực tiếp với hạ tầng mạng viễn thông A-Grid, kết nối trực tiếp với 05 tuyến cáp quang biển quốc tế AAE1, APG, A-Grid, Unity và Faster. CMC Telecom sở hữu 03 Data Center tiêu chuẩn Tier III và là Data Center duy nhất tại Việt Nam sở hữu chứng chỉ bảo mật PCI – DSS, tiêu chuẩn an ninh thông tin bắt buộc phải có đối với các doanh nghiệp lưu trữ thẻ thanh toán.

Sau 10 năm phát triển, CMC Telecom được ICTNews và Hiệp hội Internet Việt Nam vinh doanh là 1 trong 5 doanh nghiệp viễn thông có ảnh hưởng lớn nhất tới Internet Việt Nam trong 1 thập kỷ (2007-2017) CMC Telecom hiện là đối tác vàng (Gold Partner) của Microsoft, là đối tác đầu tiên cung cấp dịch vụ Bảo mật Thuê ngoài

(MSS – Managed Security Service) của IBM và là đối tác công nghệ tiêu chuẩn của AWS, Amazon Web Service. CMC Telecom được Hiệp hội Tin học Thành phố Hồ Chí Minh (HCA) vinh danh là Nhà cung cấp dịch vụ điện toán đám mây hàng đầu Việt Nam. Liên tiếp năm 2017, 2018, CMC Telecom được Tạp chí APAC CIO Outlook (Mỹ) bình

chọn là Top 25 Nhà cung cấp dịch vụ hàng đầu châu Á – Thái Bình Dương và Tạp chí International Finance Magazine (Anh) bình chọn là Nhà cung cấp dịch vụ viễn thông cho Doanh nghiệp tốt nhất Việt Nam. Năm 2019, CMC Telecom là đại diện Việt Nam duy nhất được Tạp chí Telecom Asia (Tạp chí uy tín và lâu đời nhất của ngành Viễn thông Châu Á) vinh danh là top 3 Nhà cung cấp dịch vụ Data Center tốt nhất Châu Á.



Hình 3.1: Sơ đồ tổ chức công ty CMC telecom

Cơ quan công ty CMC telecom Đứng đầu là giám đốc

Đơn vị cấp dưới: Phòng kỹ thuật, phòng kinh doanh, kế toán trưởng

Phòng kỹ thuật gồm: Quản lý kỹ thuật, nhân viên kỹ thuật

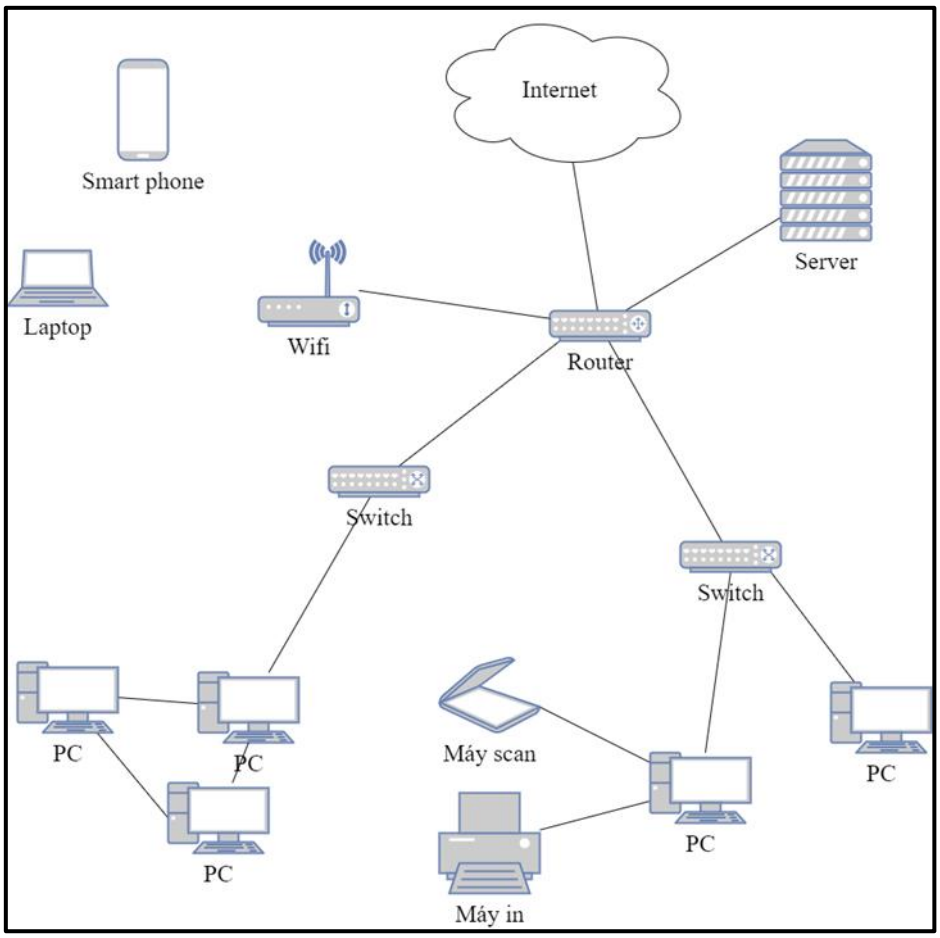
Phòng kinh doanh gồm: Trưởng phòng kinh doanh và nhân viên

Phòng kế toán gồm : Kế toán kho, kế toán doanh thu

3.2. Thực trạng tổ chức, sử dụng hệ thống công nghệ thông tin tại công ty

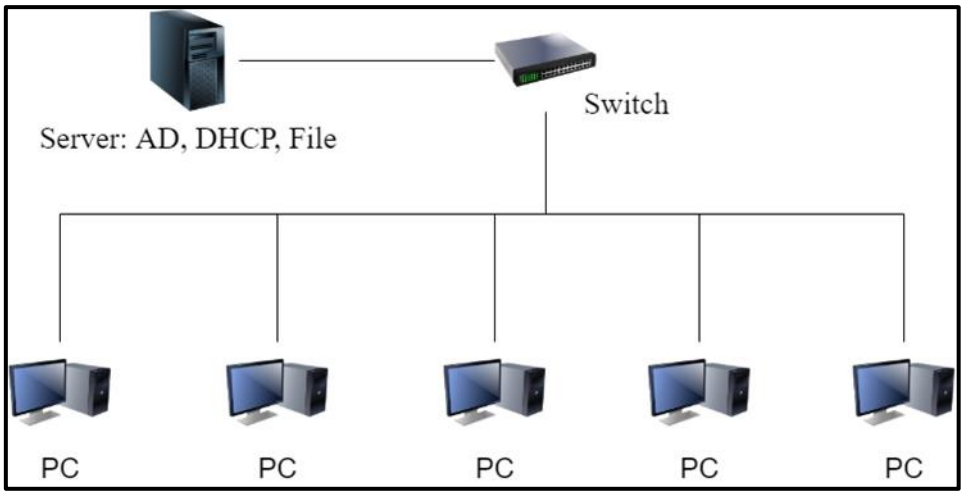
Hiện nay dịch vụ hệ thống thông tin nói chung và dịch vụ mạng không dây nói riêng đã và đang được sử dụng rất phổ biến ở mọi nơi, mọi lĩnh vực, ngành

nghề. Chính từ những tiện ích mà nó đem lại như: thuận tiện, nhanh chóng, hiệu quả, chi phí thấp nên đã được nhiều người dùng.



Hình 3.2: Hệ thống máy tính cho nhân viên sử dụng Internet

Hệ thống này dùng cho phòng kỹ thuật và phòng kinh doanh để tra cứu những nội dung trên mạng internet, kết nối với khác hàng. Đặc biệt còn dùng cho kết nối wifi, internet phục vụ cho cán bộ, nhân viên trong cơ quan tra cứu, tham khảo tài liệu phục vụ cho công tác chuyên môn và nâng cao trình độ chuyên môn, nghiệp vụ. Nhân viên muốn sử dụng tài liệu của công ty cần có tài khoản mạng nội bộ. Thực tế hiện nay những phòng, ban đang sử dụng hệ thống Wi-Fi với giao thức bảo mật phổ biến nhất hiện nay là WPA2, với giao thức bảo mật đã không còn được an toàn này thì rất rễ bị tấn công với các hình thức như ở Chương 2 đã nêu ra.



Hình 3.3: Mô hình hệ thống mạng máy tính phòng kế toán

Hệ thống mạng nội bộ này dùng cho phòng kế toán. Nên hệ thống này không kết nối với mạng internet bên ngoài mà chỉ phục vụ trong quá trình làm việc. Trên các máy tính đã được trang bị kết nối vào tên miền (domain) riêng cung cấp tài khoản đăng nhập (user/password) vào máy tính cho từng nhân viên. Các máy tính được cấp địa chỉ IP thông qua máy chủ DHCP. Trên các máy tính đã được cài đặt phần mềm diệt virus Bkav Endpoint. Các máy tính ở hệ thống này cũng không được bật chế độ tự động cập nhật hệ điều hành cho các máy.

3.3. Biện pháp bảo đảm an toàn thông tin công ty

Nâng cao nhận thức cho nhân viên về bảo đảm an toàn thông tin số, chủ động có biện pháp đấu tranh, phòng ngừa và tự giác chấp hành tốt các quy định của công ty.

- Về giải pháp kỹ thuật: Đã khuyến cáo tất cả nhân viên sử dụng các phần mềm bảo mật và diệt vi rút. Lắp đặt thiết bị tường lửa như là fotinet. Tuyệt đối không được sao chép các loại tài liệu mật khi chưa được phép của cấp có thẩm quyền, dùng máy tính chuyên ngành để truy cập mạng, sử dụng các thiết bị đã được kiểm định an toàn về bảo mật và sử sử dụng chuẩn bảo mật mạng không dây đang được sử dụng phổ biến hiện nay là WPA2… Ngoài ra cần sử dụng một số biện pháp nâng cao an toàn cho mạng Wifi như; tắt bỏ tính năng WPS trên Router, nếu có thể thì không sử dụng băng tần 2.4, thường xuyên thay đổi thông tin đăng

nhập mặc định cũng như mật khẩu, cập nhật phần mềm điều khiển theo định kỳ....

3.4. Đề xuất giải pháp sử dụng mạng không dây với chuẩn bảo mật WPA3

3.4.1. Các yêu cầu chung

Xuất phát từ thực tiễn yêu cầu nhiệm vụ của đơn vị đang sử dụng WPA2 với những lỗ hổng giao thức WPA2 từ lâu đã được coi là không an toàn do vấn đề bảo mật thông thường nên rất dễ bị tấn công.

Đặc biệt, WPA2 đã tồn tại lỗ hổng KRACK (Key Reinstallation Attack) cho phép tin tặc có khả năng đánh chặn và giải mã dữ liệu trên đường truyền Wi-Fi giữa máy tính và thiết bị phát Wifi. Với lỗ hỏng bảo mật này thì kẻ xấu nằm trong phạm vi phủ sóng wifi có thể lấy được thông tin gửi và nhận giữa các thiết bị truy cập trong chính wifi đó, kẻ xấu xẻ đánh cắp thông tin và thu thập dữ liệu người dùng, nghe lén và hack mật khẩu.

Em đã tìm hiểu giao thức bảo mật WPA3 để đề xuất giải pháp xây dựng thử nghiệm mạng hệ thống mạng không dây có sử dụng giao thức bảo mật WPA3 để tăng cường độ bảo mật phục vụ cho công tác của công ty.

Cung cấp một hệ thống mạng an toàn, ổn định đảm bảo được các hoạt động nghiên cứu công tác chuyên môn, chia sẻ dữ liệu, trao đổi thông tin và các nhu cầu sử dụng thông thường như lướt Web, video call, chat voice, giải trí…

- Đảm bảo mạng lưới Wi-Fi có bảo mật WPA3 được bao phủ tới tất cả các khu vực của công ty.

- Đảm bảo hạn chế nhiễu tối đa đối với sóng Wi-Fi.

- Mạng Wi-Fi sử dụng các thiết bị được tích hợp giao thức bảo mật WPA3 và các phương thức bảo mật khác được hỗ trợ.

- Có thể cung cấp được kết nối có dây nếu cần thiết đến các phòng tại các hệ thống camera.

- Hệ thống bảo đảm dễ dàng lắp đặt, dễ thay thế, tận dụng tối đa cơ sở hạ tầng sẵn có của cơ quan, dễ dàng mở rộng và đảm bảo được vẻ mỹ quan cho khu vực thi công.

3.4.2. Hệ thống mạng wifi sử dụng giao thức bảo mật WPA3

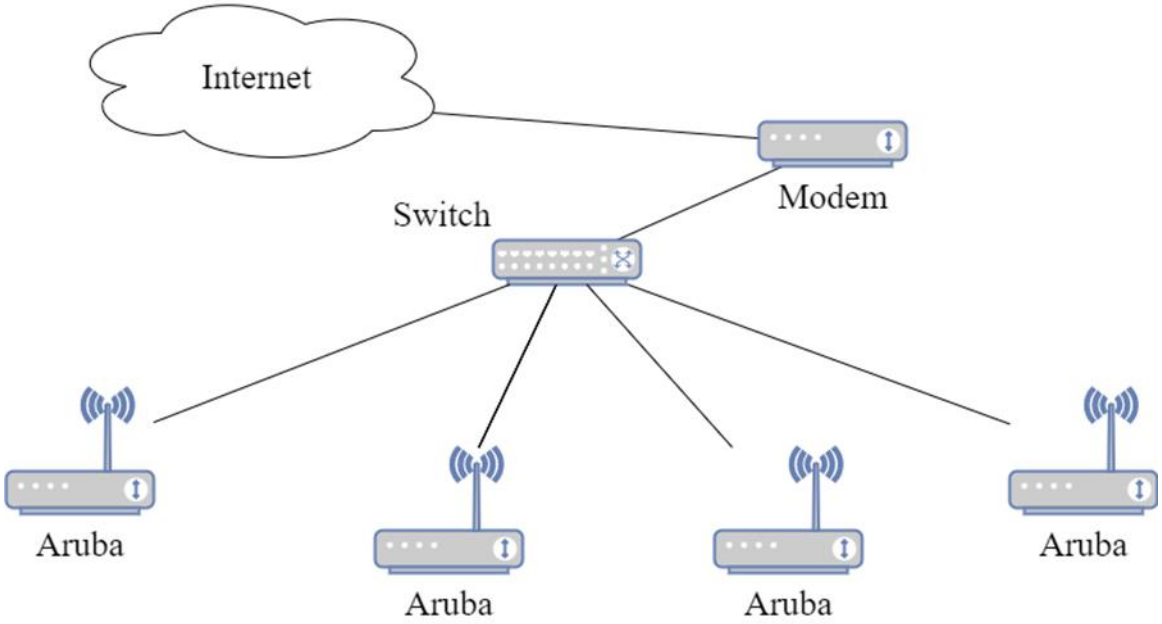
Yêu cầu tổ chức mạng Wifi sử dụng giao thức bảo mật WPA3 tại các phòng, ban:

- Các trưởng phòng và tất cả các nhân viên có nhu cầu liên lạc với nhau bằng máy tính cá nhân, Smart phone hay bất cứ thiết bị thông minh nào để trao đổi chuyên môn phục vụ cho công tác chuyên môn.

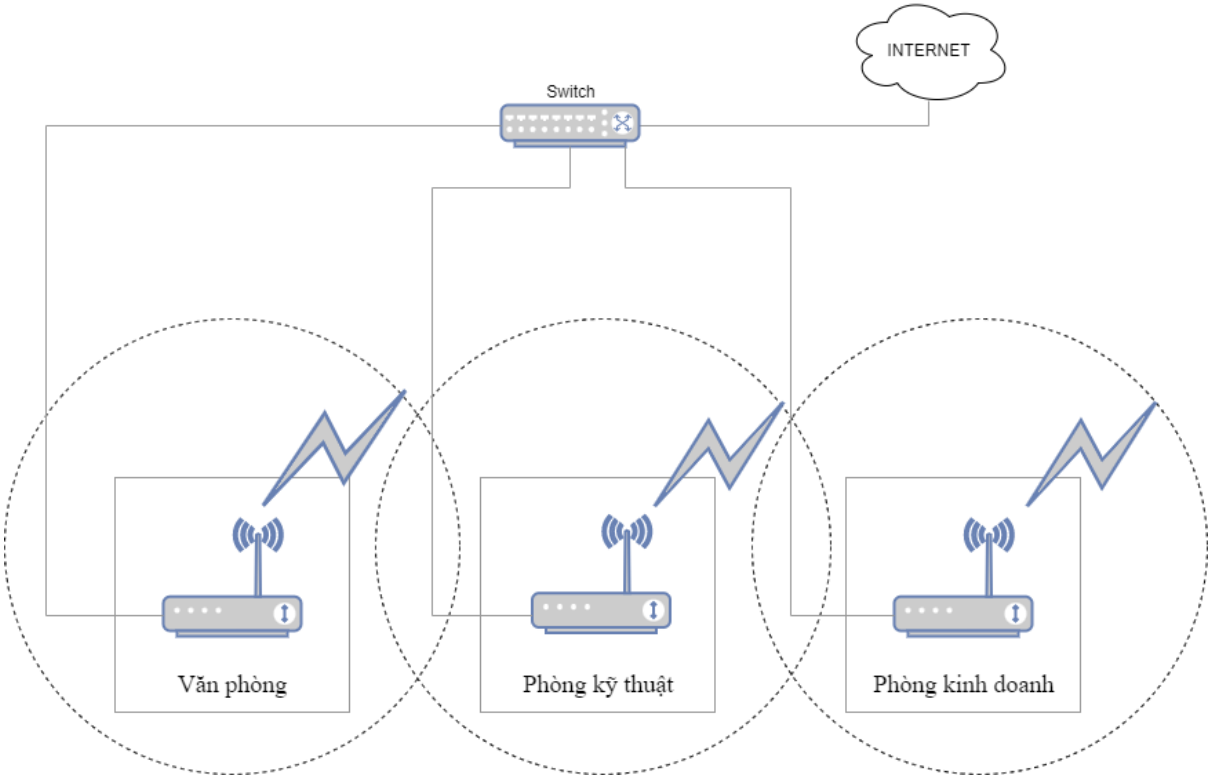
- Khi hệ thống phát triển cần mở rộng từ các phòng này sang các phòng khác qua một thiết bị kỹ thuật trung gian đều bảo đảm kết nối không dây có bảo mật WPA3.

- Đề xuất hệ thống Wifi tích hợp giao thức bảo mật WPA3 (khi hệ thống phát triển mở rộng sau này).

3.4.3. Sơ đồ lắp đặt hệ thống mạng wifi có bảo mật WPA3 tại công ty



Hình 3.4: Mô hình cơ bản



Hình 3.5: Mô hình lắp đặt

* Yêu cầu về thiết bị:

- Chọn thiết bị Router chịu tải cao

- Chọn các thiết bị Access point ốp trần hoặc tường chuẩn AX tốc độ cao hỗ trợ nhiều user, cổng PoE 1Gbps VLAN tăng tính bảo mật.

Chọn các thiết bị chuyển mạch cổng tốc độ 1Gbps hỗ trợ nhiều chế độ sử dụng riêng

3.4.4. Danh sách thiết bị

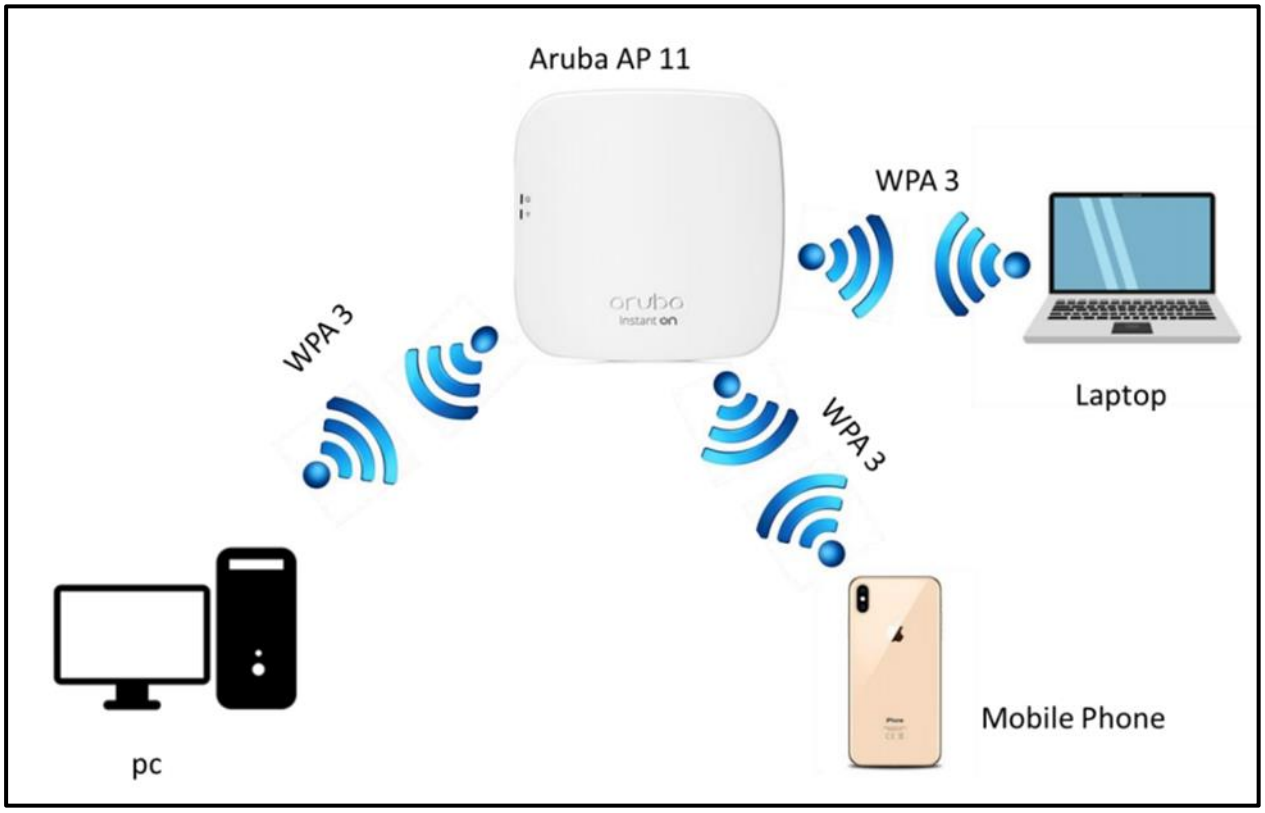
Sau khi nghiên cứu và khảo sát thực tiễn tại đơn vị và tham khảo ngoài thị trường hiện nay thì em đã chọn được các thiết bị phù hợp để lắp đặt tại đơn vị. Cụ thể sử dụng:

- 01 SWITCH dùng để chia sẻ các cổng sau khi nhận tín hiệu từ MODEM nhà mạng.

- Router có tích hợp giao thức bảo mật WPA3 để trang bị cho các Phòng, ban.

3.5. Triển khai cài đặt, thử nghiệm hệ thống

3.5.1. Mô hình thử nghiệm



Hình 3.6: Mô hình hệ thống thử nghiệm

Để giải quyết được bài toán này em sẽ sử dụng một chiếc Router Aruba Instant On AP11 làm điểm đầu để kết nối với Card mạng không dây wifi Asus PCE-AX 3000 và một chiếc điện thoại thông minh có tích hợp giao thức WPA3 làm điểm cuối và cần phải cấu hình cho từng thiết bị này

3.5.2. Cấu hình thiết bị AP hỗ trợ WPA3

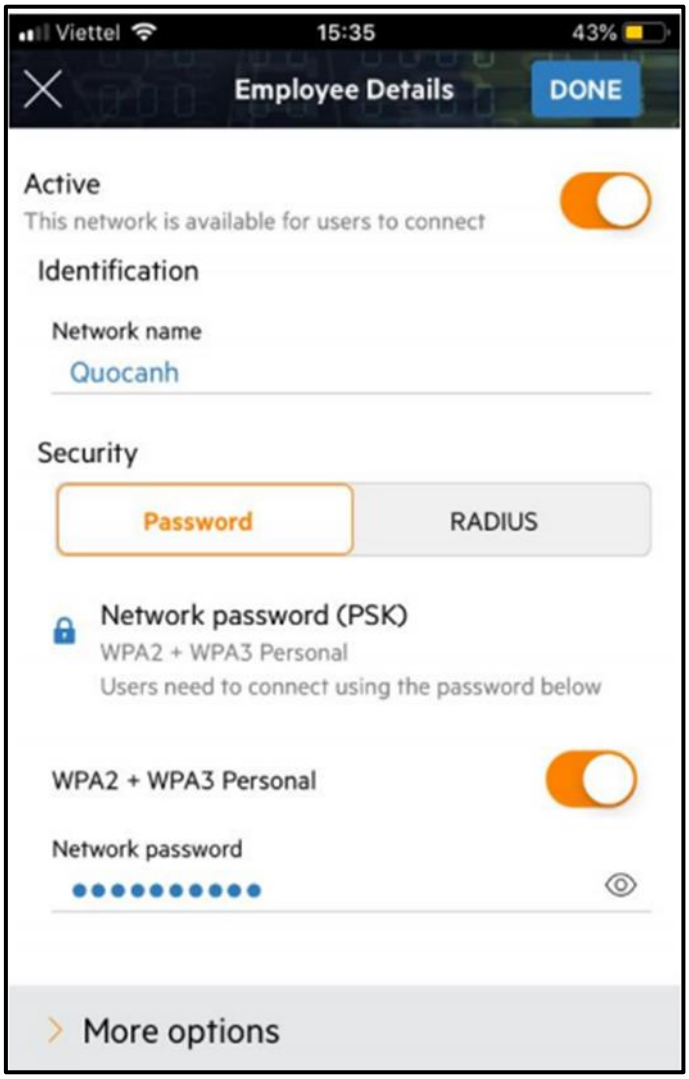
+ B1. Để cấu hình được cho AP này thì trước tiên cần cấp nguồn cho AP qua một cổng POE từ Adapter vào cổng ENET của AP, tiếp theo cấp mạng vào cổng LAN của Adapter như vậy là AP đã được cấp đủ cả mạng và nguồn.

+ B2. Đợi khoảng 10 đến 15 phút để cả 2 đèn báo sóng WIFI sáng màu hổ phách.

+ B3. Vào App Store tải Instant On.

+ B4. Khởi chạy ứng dụng và làm theo hướng dẫn.

Cụ thể: cần tạo một tài khoản GMAIL (có thể sử dụng chính tài khoản Gmail mà mình vẫn đang sử dụng) và sử dụng một mật khẩu 10 ký tự trở lên bao gồm nhiều kí tự đặc biệt bảo đảm độ bảo mật cao. Tiếp theo cần đặt tên cho thiết bị AP và tạo mật khẩu từ 10 ký tự trở lên không cần quá đặc biệt về ký tự, sau đó nhập số Serial của AP và chọn ngôn ngữ. Kết quả cuối cùng là:



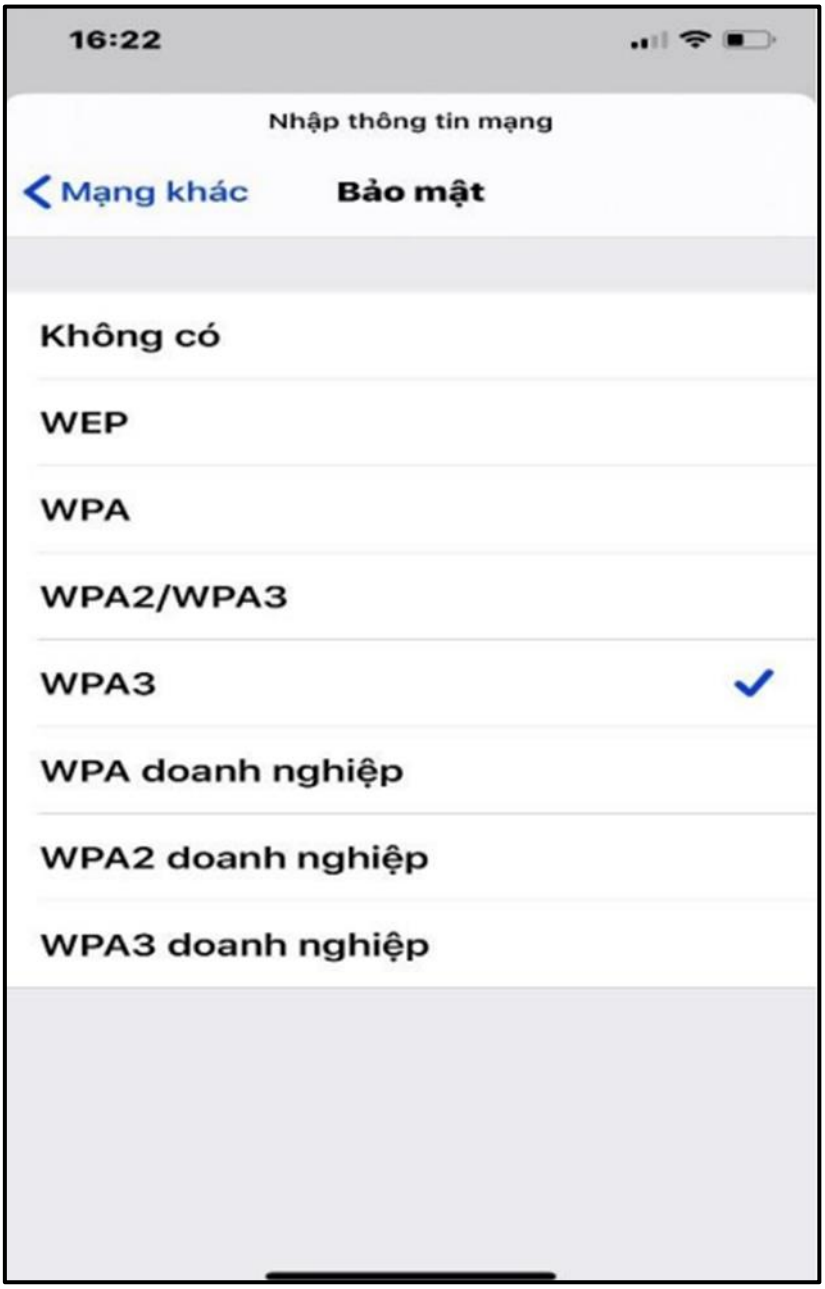
Hình 3.7 Kết quả cấu hình WPA3 cho AP

3.5.3. Cấu hình cho Mobile kết nối đến AP

Trong phần này, trình bày các bước chính để thực hiện kết nối thiết bị điện thoại di động có hỗ trợ WPA3 (Iphone 11 pro) kết nối đến AP.

+ B1: Vào chế độ “cài đặt” trên điện thoại sau đó vào “Wifi” sau khi cửa sổ

hiện lên vào mục “khác” đi đến phần “Bảo mật” và kết quả là:



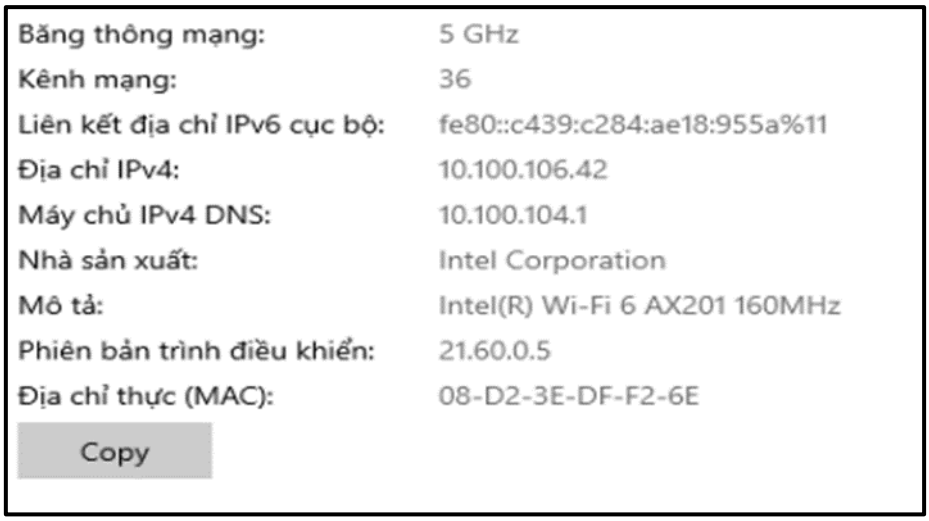
Hình 3.8: Cấu hình WPA3 cho Mobile

+ B2: Sau khi vào chế độ WPA3 xong thì tiến hành kết nối với AP bằng việc đăng nhập vào mạng WIFI đang phát nhập mật khẩu, như vậy đã kết nối thành công với điểm đầu bằng việc sử dụng giao thức WPA3.

Hình 3.9: Kết quả cấu hình WPA3 cho Mobile

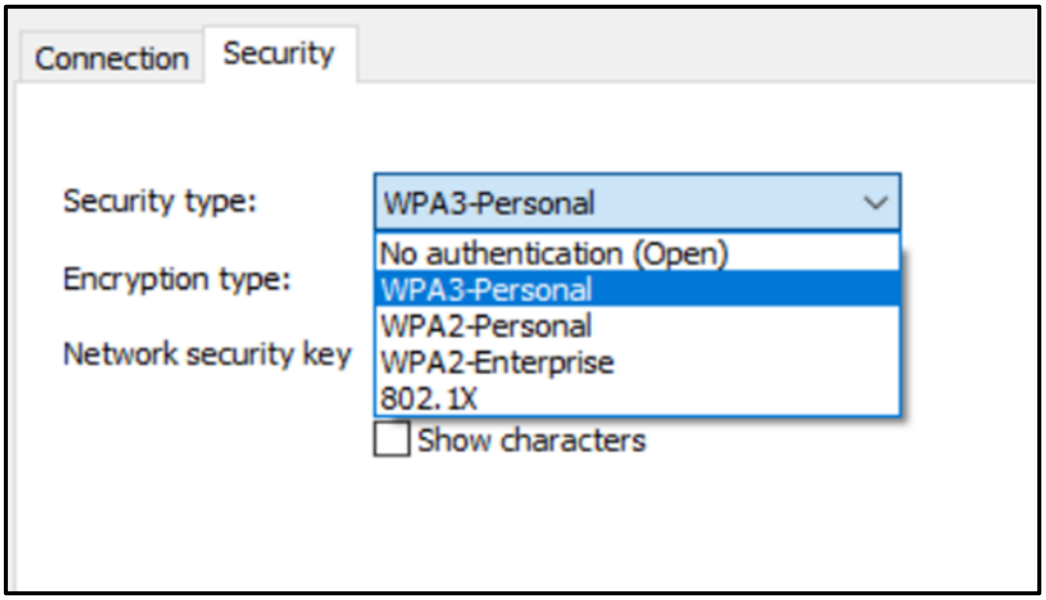
3.5.4. Cấu hình cho máy laptop kết nối đến AP

Để thực hiện kết nối không dây có bảo mật theo chuẩn WPA3 đến ta cần thực hiện kiểm tra các máy tính có hỗ trợ chuẩn kết nối WiFi có bảo mật WPA3 hay không bằng việc xem thuộc tính của card mạng không dây nếu thấy xuất hiện mục Wi- Fi 6 AX trong phần mô tả như hình dưới đây:



Hình 3.10: Thuộc tính card mạng theo chuẩn Wi-Fi 6

Chọn kết nối bảo mật đến AP theo chuẩn WPA3-Personal trong mục Security



Hình 3.11: Lựa chọn chuẩn giao thức WPA3-Personal

KẾT LUẬN

Đồ án với đề tài Tìm hiểu, phân tích và đề xuất giải pháp bảo mật khi triển khai mạng WLAN sử dụng giao thức WPA3 đã nêu ra được tổng quan về mạng không dây bao gồm: Lịch sử hình thành và phát triển mạng không dây, ưu nhược điểm, các chuẩn thông dụng của mạng WLAN, cấu trúc và mô hình WLAN, một số chuẩn bảo mật trong mạng WLAN.

Trình bày tổng quan về giao thức bảo mật WPA3, sự khác biệt giữa giao thức WPA3 với các giao thức khác. Một số tấn công vào các lỗ hổng mới nhất mà các nhà nghiên cứu bảo mật đã tìm ra trong thời gian vừa qua và những phương pháp bảo vệ. Bên cạnh đó cũng giải quyết vấn đề là khi nào thì giao thức WPA3 sẽ được tích hợp và sử dụng rộng rãi trên tất cả các thiết bị thông minh.

Trên cơ sở nghiên cứu lý thuyết về hệ thống thông tin mạng không dây và giao thức bảo mật WPA3. khảo sát nhu cầu, thực trạng sử dụng hệ thống thông tin mạng không dây tại đơn vị từ đó đề xuất giải pháp triển khai thử nghiệm và đánh giá hệ thống thông tin mạng không dây sử dụng giao thức bảo mật WPA3 như sau: chọn thiết bị tích hợp giao thức bảo mật WPA3 để lắp ráp vào mô hình bảo đảm đúng yêu cầu đã đặt ra và mang tính thẩm mỹ cao nhất. Tiến hành cấu hình các thiết bị đầu cuối và kết nối giữa các thiết bị lại với nhau. Sau khi hoàn thành thì tiến hành thử nghiệm nếu bảo đảm theo yêu cầu đặt ra thì tiến hành lắp ráp bảo đảm người dùng được sử dụng một mạng WIFI an toàn.

TÀI LIỆU THAM KHẢO

[1]. Nguyễn Đình Việt, bài giảng "Truyền số liệu và mạng máy tính'', chuyên ngành mạng và Truyền máy tính, Khoa CNTT, Trường Đại học Công nghệ, ĐHQGHN.

[2]. PGS TS. Trần Công Hùng, Quản trị và Bảo mật Mạng không dây.

[3]. Lê Tiến Liên, Minh Quân, "Hacking Wireless - Kỹ thuật thâm nhập mạng không dây", NXB Hồng Đức.

[4]. Chuẩn giao thức xác thực mạng WLAN sử dụng WPA3 google.com