BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI

LUẬN VĂN THẠC SĨ KHOA HỌC

NGHIÊN CỨU VẤN ĐỀ AN TOÀN MẠNG CỤC BỘ KHÔNG DÂY

NGÀNH: XỬ LÝ THÔNG TIN VÀ TRUYỀN THÔNG.
MÃ SỐ:

PHẠM THỊ THANH THỦY

Người hướng dẫn khoa học: TS. PHẠM HUY HOÀNG

HÀ NỘI 2006

MỤC LỤC

DANH MỤC CÁC TỪ VIẾT TẮT

STT	Từ viết tắt	Tên đầy đủ
1	AES	Advanced Encryption Standard
2	AP	Access Point
3	BSS	Basic Service Set
4	DCF	Distributed Coordination Function
5	EAP	Extensible Authentication Protocol
6	ESS	Extended Service Set
7	HCF	Hybrid Coordination Function
8	IBSS	Independent Basic Service Set
9	IDS	Intrusion Detection System
10	IEEE	Institute of Electrical and Electronics Engineers
11	IPsec	Internet Protocol Security
12	ISM	Industrial Scientific and Medical
13	MAC	Media Access Control
14	NIC	Network Interface Card
15	PBCC	Packet Binary Convolution Coding
16	PCF	Point Coordination Function
17	PKI	Public Key Infrastructure
18	PSK	Pre-sharing Key
19	RADIUS	Remote Authentication Dial-In User Service
20	TKIP	Temporal Key Integrity Protocol
21	UNII	Unlicense National Information Infrastructure
22	VPN	Virtual Private Network
23	WEP	Wired Equivalent Privacy
24	WLAN	Wireless Local Area Network
25	WPA	Wi-Fi Protected Access

DANH MỤC CÁC BẢNG

DANH MỤC CÁC HÌNH VẼ

MỞ ĐẦU

Sự phát triển bùng nổ của mạng không dây trong những năm qua gợi cho chúng ta nhớ đến sự phát triển nhanh chóng của Internet trong thập kỷ qua. Điều đó chứng tỏ những tiện ích nổi trội mà công nghệ mạng không dây đem đến. Chỉ trong một thời gian ngắn, mạng không dây đã trở nên phổ biến, nhờ giá giảm, các chuẩn mới nhanh hơn và dịch vụ Internet băng rộng phổ biến ở mọi nơi. Giờ đây, chuyển sang dùng mạng không dây đã rẻ và dễ dàng hơn trước nhiều, đồng thời các thiết bị mới nhất cũng đủ nhanh để đáp ứng các tác vụ nặng nề như truyền các tập tin dung lượng lớn, xem phim, nghe nhạc trực tuyến qua mạng...

Xu hướng kết nối mạng LAN không dây (WLAN – Wireless Local Area Network) ngày càng trở nên phổ biến trong các cấu trúc mạng hiện nay. LAN không dây hiện đang làm thay đổi những cấu trúc mạng hiện hành một cách nhanh chóng. Nhờ việc ngày càng có nhiều những thiết bị điện toán di động như máy tính xách tay, thiết bị xử lý cá nhân PDA (Personal Digital Assistant).., cộng với việc người sử dụng luôn lo lắng đến những phiền toái khi kết nối mạng LAN bằng cáp mạng thông thường.

Công nghệ không dây có mặt ở khắp mọi nơi, với bất cứ ứng dụng hay dịch vụ nào liên quan đến vận chuyển dữ liệu sẽ đều có một giải pháp không dây, phổ biến là ở những điểm công cộng như sân bay, nhà ga.., mạng không dây còn chứng tỏ những tiện ích nổi bật của nó khi ứng dụng trong lĩnh vực y tế và giáo dục. Đối với riêng lĩnh vực giáo dục, hệ thống mạng cục bộ không dây đã được triển khai rộng khắp ở các trường đại học trên thế giới bởi những lợi ích về mặt giáo dục cũng như những ưu điểm khi lắp đặt.

Sự phát triển nhanh chóng của những mạng cục bộ không dây là minh chứng cho thấy những lợi ích đi kèm của công nghệ này, Tuy nhiên, hiện nay hầu hết những triển khai không giây về cơ bản là không an toàn. Việc triển khai một môi trường không dây về cơ bản không khó. Việc triển khai một môi

trường không dây đáp ứng những yêu cầu an toàn, và tối thiểu hoá rủi ro thì lại không dễ. Có thể thực hiện được điều đó nhưng đòi hỏi việc lập kế hoạch chắc chắn và một cam kết giải quyết một số vấn đề vận hành, thực thi và kiến trúc quan trọng.

Trong một tương lai gần, việc nghiên cứu và áp dụng công nghệ mạng cục bộ không dây cho các trường đại học ở Việt Nam là hoàn toàn có khả năng thực hiện được. Với mục đích đi sâu tìm hiểu công nghệ mạng cục bộ không dây, những giải pháp an ninh cho mạng để trong một tương lai không xa có thể triển khai công nghệ mạng cục bộ không dây tại tại các trường đại học công an nhân dân, nội dung của luận văn tập trung nghiên cứu về mạng cục bộ không dây và an toàn mạng cục bộ không dây, chuẩn IEEE 802.11.

Luận văn gồm 4 chương:

Chương 1: Mạng cục bộ không dây WLAN – Những vấn đề tổng quan.

Chương 2: An toàn mạng cục bộ không dây – Những nguy cơ và và giải pháp.

Chương 3: Một số biện pháp an toàn WLAN thông dụng.

Chương 4: Triển khai WLAN an toàn trong môi trường giáo dục.

Vấn đề luận văn đề cập còn khá mới mẻ, chính vì thế không tránh khỏi có những sai sót, rất mong nhận được sự đóng góp ý kiến của các thầy cô giáo và các bạn đồng nghiệp.

Tôi xin chân thành cảm ơn **Tiến sỹ Phạm Huy Hoàng** cùng các thầy cô giáo trong khoa Công nghệ thông tin-đại học Bách Khoa Hà Nội đã giúp đỡ tôi trong quá trình học tập và hoàn thành luận văn này.

CHƯƠNG 1. MẠNG CỤC BỘ KHÔNG DÂY WLAN– NHỮNG VẤN ĐỀ TỔNG QUAN

1.1. Tổng quan mạng cục bộ không dây họ 802.11

Được IEEE 802.11 phê chuẩn vào năm 1999, đến nay WLAN đã được phát triển mạnh trên thế giới. Ở những nước phát triển, WLAN được triển khai rộng rãi ở những khu đông người như các văn phòng, toà nhà, trường đại học, sân bay, thư viện, nhà ga, sân vận động, khu triển lãm, khách sạn, siêu thị, khu dân cư..

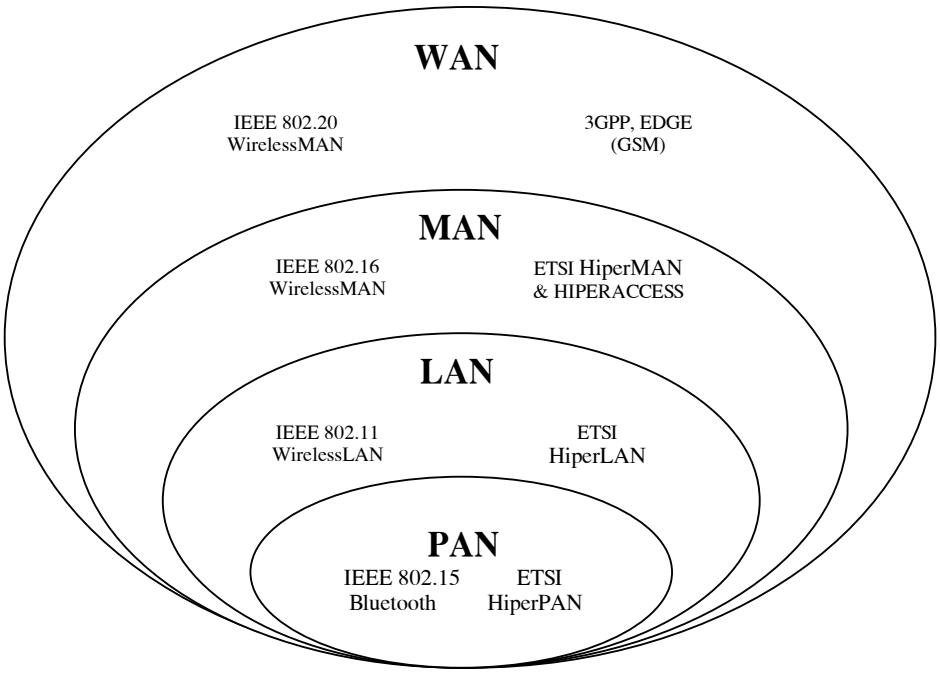
WLAN là một công nghệ truy cập mạng băng rộng không dây, được phát triển với mục đích ban đầu là một sản phẩm phục vụ gia đình và văn phòng để kết nối các máy tính cá nhân mà không cần dây, nó cho phép trao đổi dữ liệu qua sóng radio với tốc độ rất nhanh, là cơ hội để cung cấp đường truy cập Internet băng thông rộng ngày càng nhiều ở các địa điểm công cộng như sân bay, cửa hàng cafe, nhà ga, các trung tâm thương mại hay trung tâm báo chí...

Có 3 kiểu mạng không dây cơ bản được phân loại phụ thuộc vào phạm vi phủ sóng của chúng:

- ***Mạng dùng riêng không dây - WPAN (Wireless Personal Area Network)***: được biết đến là Bluetooth và IR (Infrared), hai công nghệ được ứng dụng phổ biến trong các loại điện thoại di động.

- ***Mạng cục bộ không dây - WLAN (Wireless Local Area Network)***: trong đó có 802.11, HiberLAN và một số công nghệ khác.

- ***Mạng diện rộng không dây - WWAN (Wireless Wide Area Network)***: bao gồm các công nghệ như 2G, 3G, cellular, CDPD (Cellular Digital Packet Data), GSM (Global System and Mobile Communication)..



Hình 1.1: Các loại mạng không dây

Mạng diện rộng không dây là một dạng của mạng không dây. Công nghệ mạng này sử dụng là công nghệ mạng tế bào như GPRS, CDMA, GSM, CDPD, Mobitex để truyền dữ liệu. Những công nghệ tế bào được đưa ra theo phạm vi vùng, quốc gia, hoặc thậm chí toàn cầu và được cung cấp bởi những nhà cung cấp dịch vụ không dây. Có hai phương tiện cơ bản một mạng di động có thể sử dụng để truyền dữ liệu, đó là những mạng dữ liệu chuyển mạch gói (GPRS, CDPD) hoặc những kết nối quay số chuyển mạch vòng.

Mạng đô thị không dây cho phép truy cập mạng băng rộng thông qua những ăngten ngoài. Những trạm thuê bao truyền thông với những trạm cơ sở được kết nối tới một mạng lõi. Mạng này là một giải pháp thay thế tốt cho những mạng có dây cố định và việc xây dựng nó đơn giản và không tốn kém.

Chuẩn 802.16 là một chuẩn nổi tiếng cho mạng đô thị không dây. Chuẩn này sử dụng những giải tần từ 10 đến 66 GHz. Chuẩn này hỗ trợ topo mạng điểm tới đa điểm, sử dụng công nghệ phân chia tần số và phân chia thời gian cùng với chất lượng dịch vụ QoS. Với QoS cho phép gửi âm thanh, video

và dữ liệu với những mức ưu tiên khác nhau. Tốc độ truyền phụ thuộc vào khoảng cách truyền nhưng xét về mặt lý thuyết thì tốc độ tối đa khoảng 70 Mbít/s. Ngoài ra còn có chuẩn 802.16a sử dụng dải tần từ 2 đến 11 GHz và cũng hỗ trợ những mạng lưới thay cho kiến trúc mạng điểm tới đa điểm, cho phép những trạm thuê bao truyền thông với những thuê bao khác hơn là truyền thông trực tiếp với trạm cơ sở.

Mạng cục bộ không dây kết nối hai hay nhiều máy tính mà không sử dụng dây cáp mạng. Nó cũng tương tự như một LAN có dây nhưng có một giao diện không dây. WLAN sử dụng công nghệ trải phổ dựa trên những sóng vô tuyến để thực hiện truyền thông giữa các thiết bị trong một phạm vi diện tích giới hạn, được gọi là tập dịch vụ cơ sở (BSS – Basic Service Set). Nó cho phép người sử dụng có thể di chuyển trong một diện tích phủ sóng rộng mà vẫn có thể kết nối tới mạng. Công nghệ mạng cục bộ không dây ngày càng trở nên phổ dụng, đặc biệt với sự phát triển nhanh chóng của các thiết bị cầm tay kích thước nhỏ như PDA, máy tính bỏ túi..

Mạng dùng riêng không dây sử dụng công nghệ cho phép truyền thông trong phạm vi khoảng 10 m – một phạm vi rất ngắn, một trong những công nghệ như vậy là Bluetooth, được sử dụng như là cơ sở cho một chuẩn mới IEEE 802.15.

Một khái niệm then chốt trong công nghệ WPAN đó là plugging in. Trong trường hợp lý tưởng, khi bất kỳ hai thiết bị được trang bị WPAN nào đặt gần nhau (cách nhau trong phạm vi vài mét) hoặc trong phạm vi một vài km từ một máy chủ trung tâm, chúng có thể truyền thông với nhau như thể được kết nối bằng cáp. Đặc tính quan trọng khác đó là khả năng của mỗi thiết bị khoá các thiết bị khác, ngăn ngừa nhiễu hay truy cập thông tin không được quyền. Tần số hoạt động của mạng này là 2.4 GHz.

1.1.1. Kiến trúc mạng WLAN

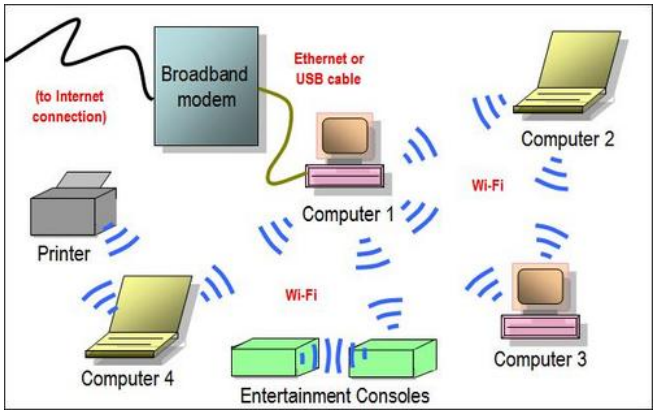
IEEE 802.11 hỗ trợ 3 topo mạng cơ bản cho WLAN:

- Tập dịch vụ cơ bản độc lập - IBSS (Independent Basic Service Set).
- Tập dịch vụ cơ bản – BSS (Basic Service Set).
- Tập dịch vụ mở rộng – ESS (Extended Service Set).

Chuẩn 802.11 định nghĩa hai mô hình:

- Chế độ tự do (ad hoc) hay IBSS.
- Chế độ cơ sở hạ tầng (Infrastructure).

Về mặt logic cấu hình tự do ad hoc tương tự như một mạng văn phòng điểm tới điểm mà trong đó không có nút nào đóng vai trò như một máy chủ. IBSS WLAN gồm một số nút hay những trạm không dây truyền thông trực tiếp với nhau. Nhìn chung, những thực thi dạng ad hoc có phạm vi hoạt động không lớn và không được kết nối tới bất kỳ mạng diện rộng nào.

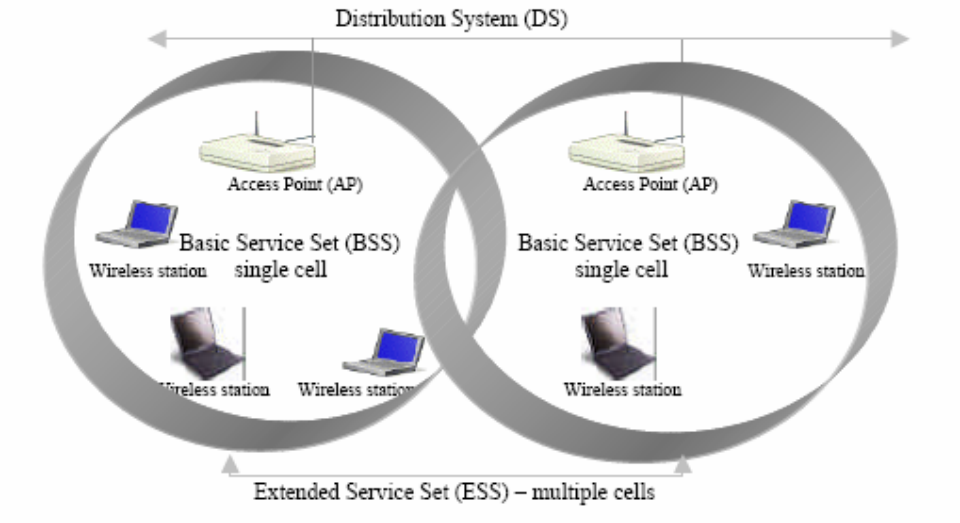


Hình 1.2: Ví dụ mạng ad hoc

Sử dụng chế độ cơ sở hạ tầng, mạng không dây bao gồm ít nhất một AP kết nối tới cơ sở hạ tầng có dây và một tập những trạm cuối không dây. Cấu hình này được gọi là BSS. Bởi vì hầu hết các WLAN liên hợp yêu cầu truy cập tới LAN có dây cho những dịch vụ (những máy chủ file, những máy in, những kết nối Internet), chúng sẽ hoạt động ở chế độ cơ sở hạ tầng và dựa vào một AP hoạt động như là một máy chủ logic cho một tế bào hay một kênh WLAN đơn. Việc truyền thông giữa hai nút A và B, thực chất là từ nút A tới AP và sau

đó từ AP tới nút B. AP có vai trò như cầu nối và kết nối nhiều tế bào hoặc kênh WLAN, và để kết nối những tế bào WLAN tới một LAN có dây.

Một ESS là một tập gồm hai hay nhiều BSS hình thành một mạng con duy nhất. Những cấu hình ESS gồm nhiều tế bào BSS có thể được liên kết bởi nhiều mạng xương sống có dây hoặc không dây. IEEE 802.11 hỗ trợ những cấu hình ESS trong đó nhiều tế bào sử dụng cùng kênh, và sử dụng những kênh khác nhau để thúc đẩy thông lượng tập hợp.



Hình 1.3: Những topo BSS và ESS IEEE 802.11

1.1.2. Các thành phần của WLAN

Kiến trúc WLAN cơ bản gồm:

- Những AP.

- Những card giao diện mạng (NIC- network interface cards) hay còn gọi là những card mạng client cho những client không dây.

- Ăngten là một thành phần quan trọng của WLAN, chịu trách nhiệm phát tán tín hiệu đã qua điều chế để cho các thành phần không dây có thể thu được tín hiệu.

- Những cầu không dây và những repeater cung cấp kết nối giữa nhiều LAN (hữu tuyến và vô tuyến) ở tầng MAC.

Mạng WLAN xí nghiệp bao gồm những thành phần sau:

- Máy chủ xác thực, cấp quyền, và kiểm tra (máy chủ AAA-authentication, authorization, accounting server), máy chủ quản lý mạng (NMS - network management server).

- Những switch và router "cảnh báo không dây".

Bảng sau mô tả các thành phần của WLAN:

Các thành phần WLAN	**Mô tả**
AP (Access Point)	Thành phần cơ bản của cơ sở hạ tầng WLAN cung cấp cho các client điểm truy cập tới mạng không dây. Nó là một thiết bị tầng 2 làm việc như là một giao diện giữa mạng hữu tuyến và mạng không dây, điều khiển truy cập môi trường sử dụng RTS/CTS (bắt tay 4 chiều) [1]. AP hoạt động ở cả dải tần 2.4 GHz và 5 GHz phụ thuộc vào chuẩn 802.11 được triển khai, và sử dụng những kỹ thuật điều chế chuẩn 802.11. AP chịu trách nhiệm thông báo cho client không dây về sự sẵn sàng của nó, và xác thực/kết hợp những client không dây tới một WLAN. Ngoài ra, AP phối hợp sử dụng những tài nguyên hữu tuyến và chức năng roam [2] như tái kết hợp. AP có thể được cấu hình theo 3 chế độ: chế độ gốc (root), cầu (bridge) và chuyển tiếp (repeater). Có nhiều loại AP từ một radio đến nhiều radio (phụ thuộc vào các kỹ thuật 802.11).
NIC hay Client adapter	Được sử dụng bởi những nút người dùng cuối như những PC, laptop hay PDA kết nối tới một WLAN. NIC chịu trách nhiệm quyét phạm vi tần số cho kết nối và sau đó kết hợp tới một AP hay client không dây. Những card vô tuyến chỉ được sản xuất ở hai dạng vật lý: PCMCIA và

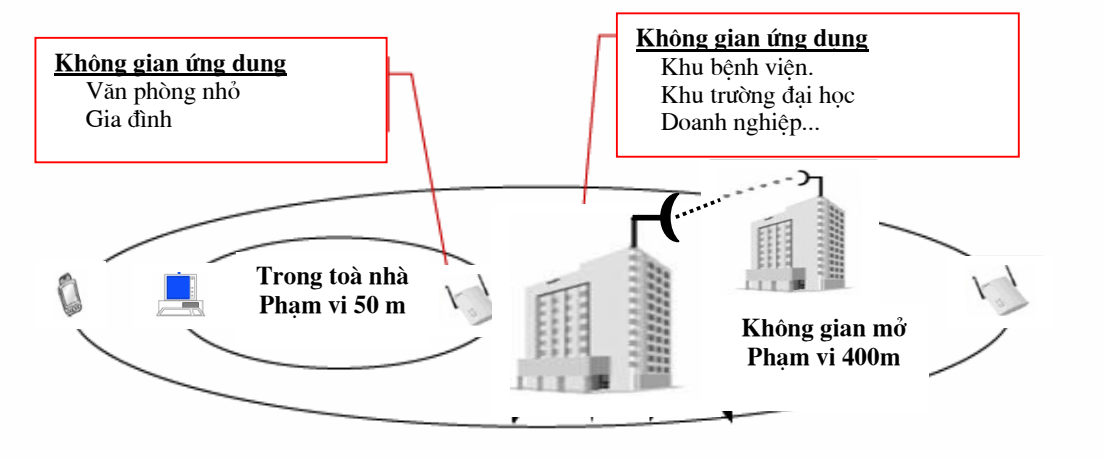
	Compact Flash (CF). Những card vô tuyến được kết nối tới adapter như PCI, ISA và USB.
Bridge và Workgroup Bridge (WGB)	Những bridge không dây và những repeater cung cấp kết nối giữa nhiều LAN (hữu tuyến và vô tuyến) ở tầng MAC. Bridge được sử dụng để cung cấp kết nối từ toà nhà này sang toà nhà khác, và có phạm vi bao trùm dài hơn AP. Một Workgroup Bridge (WGB) là một bridge phạm vi nhỏ hơn chỉ chịu trách nhiệm hỗ trợ một số lượng giới hạn những client không dây. Hoạt động ở kiến trúc mạng tầng 2, và cung cấp phân đoạn những khung dữ liệu.
Ăngten	Chịu trách nhiệm phát tán tín hiệu đã qua điều chế qua không khí để cho các thành phần không dây có thể thu phát. Một ăngten là một thiết bị chuyển những tín hiệu RF tần số cao từ một cable thành những sóng truyền trong không khí. Ăngten được triển khai trên các AP, bridge, và client (thông qua một NIC hay client adapter), và được phân thành 3 loại chung: định hướng toàn phần (Omni-directional), bán định hướng (semi-directional), và định hướng cao (highly directional). Mỗi một loại ăngten RF có những đặc trưng RF khác nhau (thành phần truyền, nhận, công suất truyền..).
Máy chủ AAA	Được biết đến nhiều hơn như là một máy chủ RADIUS (Remote Authentication Dial-In User Service), một máy chủ AAA sử dụng giao thức RADIUS [3] để cung cấp những dịch vụ xác thực, cấp quyền, và kiểm tra trong một WLAN cho những cơ sở hạ tầng doanh nghiệp. Đơn giản, một máy chủ RADIUS là một cơ sở dữ liệu dựa trên

	cơ sở máy tính, nó so sánh những username và password để cho phép truy cập tới một mạng không dây. Những máy chủ AAA có thể cung cấp nhiều chức năng từ cung cấp các mức quyền khác nhau tới những người sử dụng quản trị, thông qua chính sách như LAN ảo (VLAN – Virtual LAN) [4] và SSID [5] cho những client, tới việc tạo những khoá mã hoá động cho những người sử dụng WLAN. Ngoài ra, một máy chủ AAA có thể cung cấp những dịch vụ như thu bắt điểm bắt đầu/kết thúc của một phiên tới việc cung cấp dữ liệu thống kê trên một lượng tài nguyên (thời gian, những gói tin, những byte..) được sử dụng trong phiên.
Những máy chủ quản lý mạng NMS (Network Management Servers)	NMS có thể cung cấp một phạm vi rộng lớn những dịch vụ hỗ trợ quản lý mạng WLAN lớn gồm an toàn, tin cậy và hiệu năng. Hỗ trợ NMS nên bao gồm quản lý cấu hình, quản lý ứng dụng, báo cáo và xu hướng hoạt động. Để quản lý những mạng WLAN xí nghiệp lớn, những dịch vụ NMS cũng nên bao gồm những khả năng báo cáo kết hợp client, và những công cụ để quản lý phổ RF và dò những AP giả mạo [6].
Switch và Router "cảnh báo không dây"	Những switch và router "cảnh báo không dây" cung cấp những dịch vụ tích hợp tầng 2 và 3 giữa những thành phần WLAN truyền thống và những thành phần mạng hữu tuyến, quản lý và tính mở tăng cường của những mạng WLAN.

Bảng 1.1: Mô tả các thành phần WLAN

1.1.3. Phạm vi phủ sóng

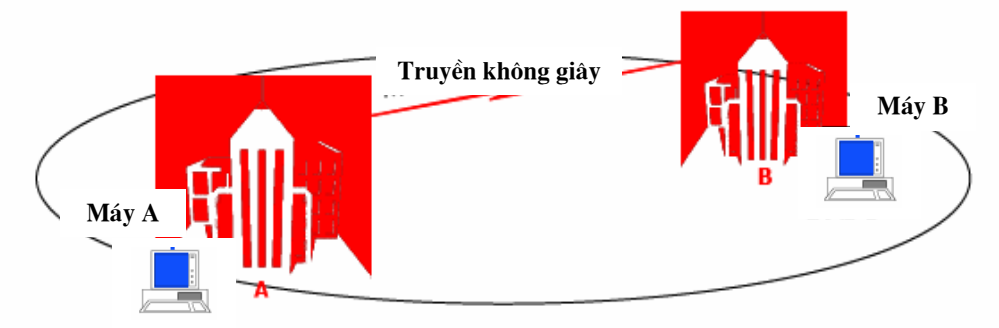
Phạm vi phủ sóng tin cậy cho 802.11 phụ thuộc vào nhiều yếu tố, bao gồm tốc độ truyền dữ liệu, công suất, các nguồn gây nhiễu vô tuyến, vùng vật lý và những đặc tính, nguồn, kết nối, và sử dụng ăngten. Phạm vi phủ sóng lý thuyết là từ 29 m (cho 11 Mbps) trong phạm vi văn phòng kín tới 485m (cho 1 Mpbs) trong khu vực mở. Tuy nhiên, theo kinh nghiệm, phạm vi cơ bản cho kết nối của thiết bị 802.11 là xấp xỉ 50 m ở phạm vi trong nhà. Phạm vi 400 m, khiến cho WLAN trở nên lý tưởng cho nhiều ứng dụng ở những khu trường sở. Quan trọng là sử dụng ăngten đặc biệt có thể tăng phạm vi phủ sóng lên nhiều dặm.



Hình 1.4: Phạm vi phủ sóng điển hình của WLAN 802.11

AP cũng có chức năng cầu nối. Cầu nối liên kết hai hay nhiều mạng lại với nhau và cho phép chúng truyền thông với nhau. Cầu nối liên quan tới cả cấu hình điểm - điểm hoặc đa điểm. Trong kiến trúc điểm - điểm, hai LAN được kết nối với nhau thông qua AP tương ứng của LAN đó. Trong cầu đa điểm, một mạng con trên một LAN được kết nối tới nhiều mạng con khác trên một LAN khác thông qua mỗi AP của mạng con đó. Ví dụ, nếu một máy tính trên một mạng con A cần kết nối tới những máy tính trên mạng con B, C, D, thì AP của mạng con A sẽ kết nối tới AP tương ứng của mạng con B, C, D.

Chúng ta có thể sử dụng chức năng cầu nối để liên kết các LAN giữa các toà nhà khác nhau thuộc một khu. Thiết bị AP cầu nối thường được đặt ở trên nóc toà nhà để thu sóng ăng ten được nhiều nhất. Khoảng cách cơ bản mà một AP có thể kết nối không dây tới AP khác thông qua phương tiện cầu nối là xấp xỉ 2 dặm. Khoảng cách này có thể thay đổi phụ thuộc vào nhiều yếu tố bao gồm bộ phận thu nhận cụ thể được sử dụng. Hình dưới dây minh hoạ cầu điểm điểm giữa 2 LAN.



Hình 1.5: Cầu nối Access Point

1.1.4. Băng tần sử dụng

Đề cập đến băng tần sử dụng cho WLAN, chúng ta gặp hai thuật ngữ khá quen thuộc là thuật ngữ "băng tần ISM (Industrial, Scientific and Medical)" và "băng tần U-NII (Unlicense National Information Infrastructure)". Khi tìm hiểu về hai thuật ngữ này sẽ phần nào giải thích được vì sao hầu hết các nước hiện nay không thu phí sử dụng tần số khi phát triển Wi-Fi cũng như các mạng truy cập không dây khác sử dụng những băng tần trên.

1.1.4.1. Băng tần ISM

Các thiết bị khi sử dụng băng tần này bao gồm cả Wi-Fi đều phải tuân thủ các quy định về bảo vệ các dịch vụ viễn thông khác và chấp nhận nhiễu từ các thiết bị cùng hoạt động trong băng tần ISM (Industrial Scientific Medical).

Trong thực tế, các quy định cụ thể về sử dụng các ứng dụng ở băng tần ISM cũng rất khác nhau ở các nước:

Công suất cực đại	Vùng địa lý
1000 mW	Mỹ
100 Mw (EIRP)	Châu Âu
10 Mw/mhZ	Nhật Bản

Bảng 1.2: Quy định công suất phát ở một số nước sử dụng băng tần ISM 2.4 GHz

Trong các quy định hiện hành, Việt Nam chưa có các quy định cụ thể về sử dụng băng tần ISM, ngoài một số tiêu chuẩn đã ban hành về điện thoại kéo dài, yêu cầu về tương thích điện từ..

1.1.4.2. Băng tần UNII

Chúng ta không thấy thuật ngữ băng tần UNII (Unlicensed National Information Infrastructure) trong thể lệ thông tin vô tuyến thế giới, điều này cũng dễ hiểu vì thuật ngữ này được sử dụng trong dự án phát triển hạ tầng thông tin quốc gia Mỹ. Năm 1995, để phục vụ dự án hạ tầng thông tin quốc gia về phát triển cung cấp Internet tốc độ cao đến trường học và cộng đồng của chính phủ Mỹ, FCC đã phân bổ thêm hai đoạn băng tần (5.1 GHz-5.35 GHz; 5.725 GHz-5.825 GHz) bổ sung cho băng tần ISM ở băng tần 5 GHz (5.725-5.825 GHz). Cũng do đặc điểm này mà việc phát triển dịch vụ truy nhập không dây băng rộng đều hướng tới phát triển sử dụng băng tần 5 GHz với các lý do chính sau:

- Băng tần ISM 2.4 GHz với độ rộng băng thông 100 MHz đã trở nên quá chật hẹp trước sự phát triển của hàng loạt ứng dụng như Wi-Fi, Bluetooth, thiết bị cá nhân không dây, thiết bị điều khiển,..

- Băng tần ISM 5 GHz được bổ sung thêm băng tần UNII trở nên đủ rộng để triển khai dịch vụ truy nhập băng rộng không dây.

- Băng tần UNII được dành riêng cho phát triển WLAN với các điều kiện như ISM nhưng không bị gây nhiễu từ các thiết bị ISM khác.

Tuy nhiên, việc sử dụng băng tần này sẽ gặp bất lợi nếu không được công nhận trên phạm vi toàn cầu. Để giải quyết vấn đề này, ITU-R đã thông qua một nghị quyết về phát triển dịch vụ truy nhập vô tuyến không dây ở băng

tần 5GHz gồm: 5.150-5.250; 5.250-5.350; 5.470-5.725 MHz, trong đó 100 MHz đầu tiên (5.150-5.250 MHz) chỉ giới hạn sử dụng ở phạm vi trong nhà.

1.1.5. Các chuẩn chính trong họ 802.11

1.1.5.1. Chuẩn 802.11

Áp dụng cho WLAN và cung cấp tốc độ truyền từ 1 đến 2 Mbps trong dải tần 2.4 GHz sử dụng trải phổ trượt tần số FHSS (frequency-hopping spread spectrum) và trải phổ chuỗi trực tiếp DSSS (direct-sequence spread spectrum).

1.1.5.2. Chuẩn 802.11b

Có tốc độ truyền 11 Mbps ở dải tần ISM 2.4 GHz chuẩn Wi-Fi. 802.11b là phiên bản sửa đổi của 802.11. Tuy nhiên 802.11b hay còn gọi là Wi-Fi về mặt lý thuyết thì tốc độ là 11 Mbps nhưng trên thực tế chỉ đạt 7 Mbps do những vấn đề đồng bộ, overhead ACK (Acknowledge).

1.1.5.3. Chuẩn 802.11a

802.11a hoạt động ở dải tần 5 GHz. Do tần số hoạt động cao hơn so với 802.11b nên 802.11a có phạm vi phủ sóng nhỏ hơn. Nó cố gắng giải quyết vấn đề khoảng cách bằng cách sử dụng nguồn nhiều hơn và những sơ đồ mã hoá dữ liệu hiệu quả hơn. Ưu điểm chính của nó là tốc độ: phổ của 802.11a được chia thành 8 phân đoạn mạng con hay còn gọi là 8 kênh, mỗi kênh khoảng 20 MHz. Mỗi kênh này phụ trách một số lượng những nút mạng. Những kênh được tạo 52 sóng mang, mỗi sóng mang là 300 kHz, và có thể đạt tốc độ tối đa là 54 Mbps. 802.11a dựa trên một sơ đồ điều chế OFDM. Hệ thống RF hoạt động ở những dải tần UNII 5.15-5.25, 5.25-5.35 và 5.725-5.825 GHz. Hệ thống OFDM (Orthogonal frequency-division multiplexing) cung cấp 8 tốc độ dữ liệu khác nhau từ 6 đến 54 Mbps. Nó sử dụng những sơ đồ điều chế BPSK (binary phase-shift keying), QPSK (Quadrature Phase-shift Keying), 16-QAM (Quadtrative Amplitude Modulation) và 64-QAM cùng với mã sửa lỗi. 802.11a không tương thích với 802.11b.

1.1.5.4. Chuẩn 802.11g

Bản phác thảo đầu tiên của 802.11g được thông qua vào tháng 11 năm 2001 sau một tranh cãi lâu dài và căng thẳng của những người ủng hộ PBCC (packet binary convolution coding) và OFDM. 802.11g là sự mở rộng tốc độ cho chuẩn 802.11b, với tốc độ lên đến 54 Mbps ở dải tần 2.4 GHz. 802.11g dựa trên các kỹ thuật CCK (**C**omplementary **C**ode **K**eying), OFDM và PBCC (packet binary convolution coding).

1.1.5.5. Chuẩn 802.11e

802.11e được đưa ra để hỗ trợ cho QoS. Mục đích là tăng cường MAC 802.11 hiện tại để mở rộng hỗ trợ cho những ứng dụng LAN với những yêu cầu QoS, để cung cấp những cải thiện về an toàn, và về những khả năng và hiệu quả của giao thức. Những tăng cường này, kết hợp với những cải tiến hiện tại ở tầng vật lý từ 802.11a và 802.11b, sẽ làm tăng hiệu năng tổng thể của hệ thống, và mở rộng không gian ứng dụng cho 802.11. Ví dụ, những ứng dụng bao gồm truyền thoại, audio và video qua những mạng không dây 802.11, hội nghị video, những ứng dụng an toàn tăng cường, và những ứng dụng truy cập di động

1.2. Cơ chế truy nhập môi trường tầng MAC 802.11

Tầng MAC 802.11 chịu trách nhiệm quản lý và duy trì truyền thông giữa những thực thể WLAN (những AP, những client không dây-những card giao diện mạng NIC Network Interface Card, và những hệ phân tán). WLAN 802.11 gồm một tập những dịch vụ cần thiết được thực thi bởi những thực thể WLAN để phối hợp truy cập tới những kênh vô tuyến chia sẻ, truyền dữ liệu, xác thực và những chức năng quan trọng khác. Những dịch vụ đạt được bằng cách truyền tin giữa các thực thể được sắp xếp trong những khung. Bảng sau đây đưa ra một số dịch vụ 802.11 quan trọng được thực thi trong tầng MAC.

Dịch vụ	Mô tả	Nhóm	Kiểu
Xác thực	Qúa trình thiết lập xác minh client trước khi một client không dây kết hợp với một AP. Máy chủ xác thực phải thoả mãn rằng nó thực sự là client không dây được quyền. Mục đích là cung cấp điểu khiển truy cập tương ứng với LAN hữu tuyến.	SS (station service-Dịch vụ trạm)	Yêu cầu.
Giải xác thực	Qúa trình ngắt một xác thực đang có.	SS	Khai báo.
Kết hợp	Qúa trình thiết lập liên kết không dây giữa client không dây và AP. Được thực hiện sau khi một xác thực, một kết hợp phải diễn ra trước khi những khung dữ liệu có thể được truyền. Một client không dây chỉ được kết hợp với một AP.	SS và DSS (Distributed system service-Dịch vụ phân tán) [7].	Yêu cầu.
Giải kết hợp	Qúa trình ngắt một kết hợp giữa một client không dây và một AP.	SS và DSS	Yêu cầu.
Tái kết hợp	Qúa trình cung cấp một khả năng roam cho client không dây. Cho phép một client không dây di chuyển từ một AP này sang một AP khác trong cùng một ESS.	DSS	Yêu cầu.
Tin cậy	Cung cấp khả năng bảo vệ thông tin trước những thực thể không được quyền. Dịch vụ này chỉ được cung cấp cho những khung dữ liệu.	SS (DSS cho nguyên liệu khoá)	Yêu cầu.

Phân tán	Qúa trình phát những tin (những khung MAC) trên một DS (Distributed system).	DSS	Yêu cầu.
Tích hợp	Qúa trình kết nối một WLAN với một LAN phụ trợ. Đơn giản, nó thực hiện việc dịch những khung 802.11 thành những khung có thể chuyển qua mạng khác, và ngược lại	DSS	Yêu cầu.
Phát dữ liệu	Qúa trình phát dữ liệu giữa những điểm truy cập dịch vụ MAC, với sao chép và sắp xếp lại những khung ở mức tối thiểu.	SS	Yêu cầu.

Bảng 1.3: Những dịch vụ thiết yếu tầng MAC 802.11

Có hai cách để cung cấp truy cập môi trường tới một kênh vô tuyến, như được định nghĩa trong chuẩn 802.11, trước khi một khung có thể được truyền: chức năng phối hợp phân tán DCF (Distributed Coordination Function) và chức năng phối hợp điểm PCF (Point Coordination Function)

1.2.1. Phương pháp truy cập cơ sở - chức năng phối hợp phân tán DCF

Cơ chế truy cập cơ sở, hay còn gọi là chức năng phối hợp phân tán DCF (Distributed Coordination Function), về cơ bản là một cơ chế đa truy cập cảm nhận sóng mang dò va đập CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance).

Một giao thức CSMA làm việc như sau: một trạm muốn truyền thì trước tiên nó cảm ứng môi trường, nếu như môi trường bận, khi đó trạm này sẽ hoãn việc truyền lại ở một thời điểm sau đó, nếu như môi trường được cảm nhận là rỗi, khi đó trạm sẽ được truyền.

Những loại giao thức này rất hiệu quả khi môi trường không chịu tải nặng, bởi vì nó cho phép các trạm truyền với trễ tối thiểu. Tuy nhiên, luôn có cơ hội để các trạm truyền cùng lúc (va đập xảy ra), do các trạm đều cảm nhận môi trường rỗi và thực hiện truyền cùng lúc.

Những tình huống va đập này phải được xác định, do đó tầng MAC có thể truyền lại các gói tin bởi chính nó chứ không phải bởi những tầng cao hơn, sẽ gây ra trễ đáng kể. Trong Ethernet va đập có thể được nhận ra bởi các trạm truyền sẽ đi đến một pha truyền lại dựa trên cơ sở một thuật toán backoff ngẫu nhiên hàm mũ (Exponential random backoff algorithm) [8]. Trong khi những cơ chế dò va đập là một ý tưởng tốt đối với LAN hữu tuyến thì chúng lại không thể thực hiện được trên một môi trường LAN không dây. Để giải quyết vấn đề này, 802.11 sử dụng một cơ chế tránh va đập (Collision Avoidance) kết hợp với sơ đồ thừa nhận xác thực, như sau:

Một trạm muốn truyền sẽ cảm ứng môi trường, nếu môi trường bận khi đó nó sẽ trễ truyền lại. Nếu như môi trường rỗi trong một khoảng thời gian cụ thể (được gọi là DIFS - Distributed Inter Frame Space, trong chuẩn) khi đó trạm này được phép truyền, trạm nhận sẽ kiểm tra CRC (cyclic redundancy check) của gói tin nhận được và gửi một gói tin thừa nhận (ACK - Acknowledgement packet). Việc nhận thừa nhận này sẽ chứng tỏ rằng không có va đập xảy ra. Nếu như bên gửi không nhận được thông tin thừa nhận thì khi đó nó sẽ truyền lại đoạn tin này cho đến khi nó nhận được thông tin từ phía bên nhận hoặc bỏ qua sau một số lần truyền lại nhất định.

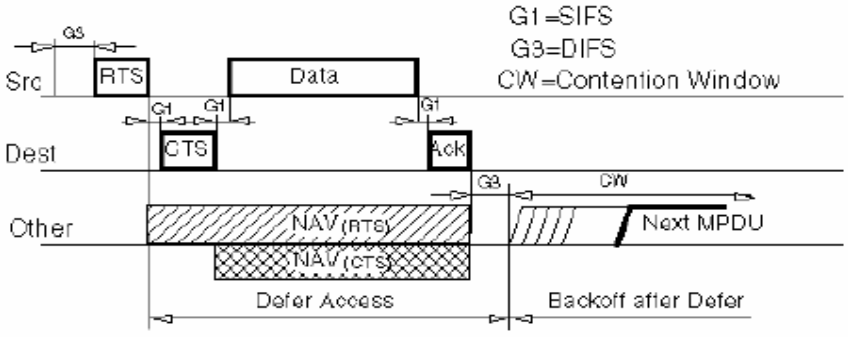
Để giảm khả năng hai trạm va đập do không nghe được nhau, chuẩn này định nghĩa một cơ chế cảm nhận sóng mang ảo như sau: Một trạm muốn truyền một gói tin trước tiên sẽ truyền một gói điều khiển ngắn được gọi là RTS (Request to Send – yêu cầu gửi), gồm nguồn, đích và thời gian truyền tiếp theo (ví dụ như gói tin và ACK tương ứng), trạm đích sẽ trả lời (nếu như môi trường rỗi) bằng một gói điều khiển trả lời gọi là CTR (Clear to Send –

sẵn sàng gửi), gồm thông tin thời gian truyền tương tự. Tất cả các trạm nhận RTS hay CTS sẽ thiết lập chỉ báo cảm nhận sóng mang ảo của chúng (được gọi là NAV – Network Assign Vector), trong một khoảng thời gian nhất định, và sẽ sử dụng thông tin này cùng với cảm nhận sóng mang vật lý (Physical Carrier Sense) khi cảm nhận môi trường.

Cơ chế này giảm khả năng xuất hiện một va đập trên vùng nhận bằng một trạm "ẩn" [9] trước bộ phận truyền, tới một khoảng thời gian ngắn của quá trình truyền RTS, do trạm này sẽ lắng nghe CTS và "dự trữ " môi trường khi bận cho đến cuối quá trình giao tác. Thông tin thời gian trên RTS cũng bảo vệ vùng truyền khỏi những va đập trong quá trình ACK (bởi những trạm ngoài phạm vi trạm báo nhận).

Cũng cần lưu ý rằng do thực tế RTS và CTS là những khung ngắn, nó cũng giảm overhead của những va đập, bởi những khung này được thừa nhận nhanh hơn nếu như toàn bộ gói tin đã được truyền, (điều này hoàn toàn đúng nếu như gói tin lớn hơn đáng kể so với RTS), do vậy chuẩn này cho phép những gói tin ngắn được truyền mà không cần giao tác RTS/CTS , và quá trình này được điều khiển trên mỗi trạm bằng một tham số gọi là ngưỡng RTS - RTSThreshold).

Biểu đồ sau đây thể hiện một giao tác giữa hai trạm A và B, và thiết lập NAV của các trạm láng giềng.



Hình 1.6: Trạng thái NAV kết hợp với cảm nhận sóng mang vật lý để chỉ ra trạng thái bận của môi trường.

1.2.2. Phương pháp điều khiển truy nhập môi trường: chức năng phối hợp điểm PCF

MAC 802.11 định nghĩa một chức năng phối hợp khác gọi là chức năng phối hợp điểm PCF (Point Coordination Function); chỉ có ở chế độ "cơ sở hạ tầng", ở đó các trạm được kết nối tới mạng thông qua một AP.

Kỹ thuật này dựa vào một nút trung tâm, thường là một AP để truyền thông với một nút đang lắng nghe, để xem xem môi trường truyền có rỗi hay không. Bởi vì hầu hết các AP có những topo bus logic, (chúng là những mạch chia sẻ) khi đó chỉ một tin có thể được xử lý ở một thời điểm (nó là một hệ thống dựa trên cơ sở tranh chấp), và do vậy yêu cầu một kỹ thuật điều khiển truy cập môi trường.

PCF đơn giản sử dụng AP như là một hệ thống điều khiển trong MAC không dây.

Chế độ này không bắt buộc, chỉ có một vài AP hay các adapter Wi-Fi thực thi nó. Các AP gửi những khung báo hiệu (Beacon frame) ở những khoảng thời gian nhất định (thường sau mỗi 0.1 giây). Giữa những khung báo hiệu này, PCF định nghĩa hai chu kỳ: chu kỳ không tranh chấp CFP (Contention Free Period) và chu kỳ tranh chấp CP (Contention Period). Trong CP, DFC được sử dụng. Trong CFP, AP gửi các gói tin dò không tranh chấp CF-Poll tới mỗi trạm, ở từng thời điểm, để trao cho chúng quyền gửi một gói tin. AP là một bộ phối hợp. Điều này cho phép quản lý QoS tối hơn. Tuy nhiên, PCF cũng có những giới hạn (ví dụ, nó không định nghĩa các lớp lưu lượng).

1.2.3. Phương pháp điều khiển truy nhập môi trường – chức năng phối hợp lai HCF.

Chuẩn IEEE 802.11e tăng cường DCF và PCF thông qua một chức năng phối hợp mới gọi là chức năng phối hợp lai HCF (Hybrid Coordination Function). Trong HCF có hai phương pháp truy cập kênh: HCCA – truy cập

kênh được điều khiển HCF (HCF Controlled Channel Access) và truy cập kênh DCF tăng cường EDCA (Enhanced DCF Channel Access) [7]. Cả HCCA và EDCA đều định nghĩa các lớp lưu lượng TC (Traffic Classes). Ví dụ, thư điện tử có thể được gán cho một mức ưu tiên thấp, và VoWIP (Voice over Wireless IP) có thể được gán cho một mức ưu tiên cao.

Với EDCA, lưu lượng ưu tiên cao có cơ hội được gửi cao hơn lưu lượng ưu tiên thấp: một trạm với lưu lượng ưu tiên cao đợi ít hơn trước khi nó gửi gói tin của nó, hơn là một trạm với lưu lượng ưu tiên thấp. Ngoài ra, mỗi mức ưu tiên được gán một cơ hội truyền TXOP (Transmit Opportunity). Một TXOP là một khoảng thời gian giới hạn trong suốt quá trình một trạm có thể gửi càng nhiều khung càng tốt (khi thời gian của những lần truyền không vượt quá thời gian tối đa của TXOP). Nếu như một khung là quá lớn để được truyền trong một TXOP duy nhất thì nó nên được phân thành những khung nhỏ hơn. Việc sử dụng TXOP sẽ làm giảm vấn đề các trạm tốc độ thấp giành một khối lượng thời gian kênh quá nhiều trong MAC DCF 802.11.

HCCA làm việc giống nhiều như PCF: khoảng cách giữa hai khung báo hiệu được chia thành hai giai đoạn, CFP và CP. Trong giai đoạn CFP, HC còn được gọi là AP điều khiển truy cập môi trường. Trong giai đoạn CP, tất cả các trạm thực hiện chức năng trong EDAC (Error Detection and Correction). Sự khác nhau chính so với PCF đó là các lớp lưu lượng được xác định. Cũng vậy, HC có thể phối hợp lưu lượng theo bất kỳ kiểu nào nó chọn. Hơn nữa, các trạm đưa thông tin về những độ dài của những hàng đợi của chúng cho mỗi lớp lưu lượng. HC có thể sử dụng thông tin này để trao quyền ưu tiên cho một trạm so với trạm khác. Điểm khác nhau nữa là các trạm được trao một TXOP có thể gửi nhiều gói tin trong một hàng, trong một khoảng thời gian cho trước được lựa chọn bởi HC. Trong giai đoạn CP, HC cho phép các trạm gửi dữ liệu bằng cách gửi những khung CF-Poll.

HCCA thường được xem như là chức năng phối hợp tiên tiến nhất và phức tạp nhất. Với HCCA, QoS có thể được cấu hình với độ chính xác lớn nhất. Các trạm tăng cường QoS có khả năng yêu cầu những tham số truyền cụ thể (tốc độ dữ liệu..) cho phép những ứng dụng tiên tiến như VoIP và Video làm việc hiệu quả hơn trên một mạng Wi-Fi.

1.3. Các kỹ thuật tầng vật lý 802.11

Chuẩn IEEE802.11 tập trung trên hai tầng đáy của mô hình OSI: Tầng vật lý và tầng liên kết dữ liệu. Tầng vật lý cung cấp truyền các bít thông qua một mạng không dây. IEEE 802.11 định nghĩa nhiều kỹ thuật vật lý để truyền dữ liệu sử dụng một WLAN:

- Truyền hồng ngoại IR (Diffused Infrared).
- Trải phổ trượt tần số FHSS (frequency hopping spread spectrum).
- Trải phổ chuỗi trực tiếp DSSS (direct sequence spread spectrum).
- Đa phân chia tần số trực giao OFDM (orthogonal frequency division multiplexing).

Những giải pháp dựa trên cơ sở RF (tần số vô tuyến radio frequency) là công nghệ truyền thống cho truyền dữ liệu qua những WLAN. Ngược lại, những giải pháp dựa trên cơ sở IR không tạo ra nhiều quan tâm như một công nghệ, và các nhà sản xuất chưa sản xuất những sản phẩm tương thích 802.11 IR. IR đưa ra những tốc độ truyền cao hơn những hệ thống dựa trên cơ sở RF, tuy nhiên những giới hạn về khoảng cách cản trở việc sử dụng nó như là một chuẩn tầng vật lý WLAN.

Công nghệ trải phổ sử dụng tần số vô tuyến RF để truyền dữ liệu qua một WLAN gồm: FHSS, DSSS và OFDM. Trải phổ lấy những tín hiệu số và mở rộng nó khiến cho nó xuất hiện giống hơn với nhiễu nền ngẫu nhiên (độ rộng dải thông và nguồn đỉnh thấp). Điều này khiến cho một tín hiệu trải phổ khó dò hơn, càng giống nhiễu nhiều hơn thì càng khó chặn bắt và giải mã nếu như không có thiết bị phù hợp. Công nghệ này sử dụng nhiều phương pháp

điều chế bao gồm các phiên bản tạo khoá dịch pha khác nhau (PSK - phase shift keying), điều chế biên độ cầu phương QAM (Quadrature amplitude modulation), tạo khoá mã bổ sung CCK (complementary code keying).

1.3.1. Trải phổ chuỗi trực tiếp DSSS

DSSS là công nghệ trải phổ được lựa chọn bởi IEEE 802.11, và được sử dụng rộng rãi với những thiết bị 802.11b. Một tín hiệu dữ liệu được kết hợp với một chuỗi bít tốc độ dữ liệu cao hơn, được biết đến như là một mã chipping (chipping code) hay processing gain, chuyển mỗi bít dữ liệu người sử dụng thành một loạt những thành phần bít dư thừa (được gọi là những chip). DSSS làm việc bằng cách chia dải tần 2.4 GHz thành 11 kênh có độ rộng 22 MHz, và sử dụng một tần số mang 1 MHz cho truyền dữ liệu. Dữ liệu được trải và được truyền qua một trong số những kênh 22 MHz này mà không trượt sang những kênh khác, tác dụng tạo nhiễu trên kênh đưa ra. Bằng việc kết hợp các chip và trải tín hiệu trên những kênh 22 MHz, DSSS cung cấp một cơ chế cho kiểm tra lỗi và chức năng sửa lỗi để khôi phục dữ liệu. Những tần số trung tâm cho mỗi kênh là những phần 5 MHz, tạo ra những kênh chồng nhau. Chỉ có tối đa 3 kênh không chồng nhau có thể được đồng thời định vị (kênh 1, 6 và 11) mà không cần giảm dải thông. DSSS được sử dụng ban đầu với những thiết bị 802.11b. FCC quản lý DSSS ở Mỹ. Ở châu Âu, ETSI (European Standard Organizations and Regulations) quản lý công nghệ DSSS.

1.3.2. Đa phân chia tần số trực giao OFDM.

OFDM không phải là một công nghệ trải phổ, mà là một kỹ thuật điều chế đa phân chia tần số có thể truyền khối lượng lớn dữ liệu số qua sóng vô tuyến. OFDM làm việc bằng cách tách tín hiệu số thành những tín hiệu con phân biệt được truyền đồng thời một cách tách biệt ở những tần số khác nhau qua một mạng không dây. Một tín hiệu số được chia theo 48 tần số mang con tách biệt trong một kênh 20 MHz tạo ra những tốc độ truyền lên đến 54 Mbps. OFDM rất hiệu quả khi truyền dữ liệu ở tốc độ cao, và tối thiểu hoá khối

lượng đàm thoại chéo (crosstalk) trong những lần truyền tín hiệu. Ngoài việc được triển khai như là những chuẩn WLAN 802.11a và 802.11g, OFDM được lựa chọn để sử dụng với những công nghệ 802.16 và WiMax.

Ngoài ra, tầng vật lý 802.11 IEEE được chia thành hai tầng con: giao thức hội tụ tầng vật lý PLCP (Physical Layer Convergence Protocol), và phụ thuộc môi trường vật lý PMD (Physical Medium Dependent). PLCP chịu trách nhiệm chuẩn bị những khung 802.11 (tín hiệu) cho việc truyền. Nó định hướng PMD, chịu trách nhiệm chính cho việc mã hoá, để truyền và nhận những tín hiệu, và thay đổi những kênh vô tuyến trong số những chức năng khác.

CHƯƠNG 2. AN TOÀN MẠNG WLAN – NGUY CƠ VÀ GIẢI PHÁP

2.1. Những cơ chế an toàn mạng WLAN

Những truyền thông không dây đưa ra nhiều ích lợi như tính cơ động, sản phẩm không dây được sản xuất ngày càng nhiều, và chi phí cài đặt thấp hơn. Tuy nhiên, thách thức về vấn đề an toàn WLAN vẫn là một cản trở lớn khi triển khai nó. Các tổ chức mong muốn rằng một triển khai WLAN của họ phải giảm thiểu nguy cơ bất an toàn trước khi nhìn thấy những lợi ích mà nó đem lại. Ngoài những nguy cơ đi kèm đã xuất hiện trong những mạng hữu tuyến [10], còn có thêm những nguy cơ khác vốn có trong công nghệ không dây bởi bản chất kết nối không dây của nó, và một số nguy cơ mới không xuất hiện trong những mạng hữu tuyến.

Bước đầu tiên giải quyết tính phức tạp của an toàn mạng không dây là xem xét những cơ chế an toàn cơ sở, và những cơ chế sẵn có cho những triển khai không dây. Những cơ chế an toàn cơ sở, trong thế giới không dây, kế thừa những khả năng chung về sự tin cậy, tính toàn vẹn, khả năng sẵn sàng, xác thực, cấp quyền, và điều khiển truy cập. Những cơ chế cung cấp phương tiện thông qua những công nghệ, những giao thức, và những thực thi để đạt được cơ chế an toàn cơ sở. Một số những cơ chế khoá quan trọng triển khai trong mạng không dây gồm những giao thức mã hoá, những chữ ký số, và quản lý khoá. An toàn, cho mọi mục đích cụ thể, là sự kết hợp của những xử lý, những thủ tục, và những hệ thống được sử dụng để đạt đến những cơ chế an toàn cơ sở. Bảng sau đây mô tả những cơ chế an toàn cơ sở và những cơ chế cho những triển khai không dây.

Những cơ chế quản lý khoá và cơ chế an toàn cơ sở	Định nghĩa	Cơ chế
Độ tin cậy	Khả năng bảo vệ thông tin trước những thực thể không được quyền. Khả năng gửi/nhận dữ liệu mà không để lộ bất kỳ thông tin nào cho những thực thể không được quyền trong quá trình truyền dữ liệu.	Mã hoá (đối xứng và không đối xứng).
Toàn vẹn	Khả năng bảo vệ nội dung dữ liệu trước những biến đổi không được quyền. Khả năng gửi/nhận dữ liệu mà những thực thể không được quyền không thể thay đổi bất kỳ phần dữ liệu được trao đổi nào.	Những chữ ký số (sử dụng những hàm băm một chiều) [11].
Tính sẵn sàng	Khả năng cho bên gửi/nhận dữ liệu không bị ngắt quãng. Đảm bảo dữ liệu hoặc hệ thống có thể truy cập/sẵn sàng khi cần.	Những công nghệ phòng thủ để dò/bảo vệ trước những tấn công từ chối dịch vụ DoS.
Xác thực	Khả năng hợp thức hoá xác minh của bên gửi/nhận thông tin.	802.1x, RADIUS, PAP/CHAP, MS-CHAP..
Cấp quyền	Thường đi theo thủ tục xác thực, và thiết lập những gì mà	802.1x (dựa trên cơ sở xác thực), nhiều mức và

	những khả năng và thông tin một người sử dụng có thể truy cập.	nhiều giao thức.
Điều khiển truy cập	Khả năng đảm bảo người sử dụng chỉ nhìn thấy thông tin họ được cấp quyền đối với chúng.	Dựa trên cơ sở xác thực, mã hoá.
Mã hoá	Khả năng biến đổi dữ liệu (hay bản rõ) thành những byte vô nghĩa (bản mã) dựa trên cơ sở thuật toán nào đó.	WEP, CKIP,TKIP, AES.
Giải mã	Khả năng biến đổi những byte vô nghĩa (bản mã) trở lại dữ liệu có nghĩa (bản rõ).	WEP, CKIP, TKIP, AES
Quản lý khoá	Phương pháp và khả năng tạo, lưu trữ, và phân phối khoá.	

Bảng 2.1: Những cơ chế và kỹ thuật an toàn cơ sở

2.1.1. Độ tin cậy

Mục đích của tin cậy (Confidentiality) là bảo vệ thông tin trong quá trình truyền trước những thực thể không được quyền. Mã hoá là một cơ chế then chốt để đạt được độ tin cậy. Đơn giản, mã hoá là một phương tiện để mã hoá dữ liệu, sử dụng mật mã để đạt tính riêng tư của dữ liệu trong quá trình truyền, và nó trở nên vô nghĩa đối với những người nhận không được quyền. Bằng cách biến đổi dữ liệu thành một dạng không dễ hiểu, mã hoá cố gắng ngăn ngừa việc lộ lọt thông tin trước những người không được quyền. Trong thế giới không dây, mục đích này là để ngăn ngừa những tên trộm thông tin sử dụng các công cụ chặn bắt gói tin truyền và sau đó tiến hành phân tích chúng. Do vậy, thuật toán phải đạt đến độ tin cậy trong khoảng thời gian nhất định.

Qúa trình mã hoá dữ liệu sử dụng một thuật toán, hay khoá. Có hai loại khoá sử dụng để mã hoá: khoá đối xứng và khoá công khai. Trong thế giới không dây, phương pháp được ưa chuộng hơn cho độ tin cậy dữ liệu là những thuật toán khoá đối xứng. Nó sử dụng một khoá chung và thuật toán mật mã giống nhau cho mã hoá và giải mã dữ liệu. Thuật toán khoá đối xứng sử dụng một trong số hai phương pháp khác nhau để mã hoá và giải mã dữ liệu: những mã khối (block cipher) [12] và những mã dòng (stream cipher) [13]. Những triển khai WLAN ban đầu sử dụng phương pháp mã khối. Nhìn chung, những phương pháp mã khối là phù hợp hơn cho mã hoá dựa trên cơ sở phần mềm. Những thuật toán khoá đối xứng mới hơn triển khai phương pháp mã dòng. Mã dòng hiệu quả hơn cho mã hoá dựa trên cơ sở phần cứng. Ngoài ra, mã dòng vốn được xem là an toàn hơn những mã khối. Ngược lại, những mã khối biến đổi những khối tin giống nhau thành những khối bản mã giống nhau khi sử dụng một khoá cố định, cho phép những thực thể không được quyền có thể xoá, chèn, hoặc dùng lại bản mã, và dẫn tới tấn công tìm kiếm bản mã để đối chiếu phù hợp với bản mã thật. Những mã dòng triển khai một hàm nhớ mã hoá một dòng dữ liệu (thường là một ký tự hoặc byte dữ liệu) theo một hàm khoá thay đổi theo thời gian để ngăn ngừa việc xoá, chèn hay dùng lại bản mã, và tìm kiếm bản mã.

Mã hoá công khai sử dụng một cặp khoá để mã hoá và giải mã dữ liệu: một khoá công khai và một khoá bí mật. Nó có thể sử dụng cùng thuật toán hoặc một thuật toán khác nhau. Mã hoá công khai hiếm khi được sử dụng cho độ tin cậy dữ liệu. Thuật toán khoá công khai thường được sử dụng trong những ứng dụng liên quan đến xác thực bên gửi tin sử dụng những chữ ký số và quản lý khoá, và trao đổi những khoá đối xứng.

2.1.2. Tính toàn vẹn

Tính toàn vẹn (Integrity) cung cấp phương tiện để dò xem dữ liệu có bị giả mạo hay không. Việc triển khai những cơ chế toàn vẹn mạnh nhằm mục

đích cung cấp độ tin cậy rằng dữ liệu đến hoặc đang tồn tại trên mạng là tin cậy. Một chữ ký số là cơ chế ưa dùng để đạt tính toàn vẹn. Đơn giản, một chữ ký số là một digest tin được mã hoá hoặc băm và được gắn vào tài liệu. Một chữ ký số sử dụng một thuật toán mã hoá khoá công khai để khẳng định xác minh bên gửi và mã hoá băm của một tin, và một thuật toán hàm băm an toàn một chiều để đảm bảo tính toàn vẹn của tài liệu.

2.1.3. Xác thực

Xác thực (Authentication) là khả năng hợp thức hoá những xác minh của một người sử dụng, dịch vụ hoặc thiết bị dựa trên những tiêu chí được xác định trước. Do bản chất quảng bá của WLAN đã có nhiều phương pháp xác thực được xây dựng để ngăn ngừa truy cập không được quyền tới những tài nguyên mạng bởi một người sử dụng hoặc thiết bị. Xác thực là quá trình xác định xem người sử dụng thiết bị hay dịch vụ được quyền cố gắng giành quyền truy cập tới mạng có đúng là thực thể được quền hay không. Trong thế giới không dây, những chuẩn 802.11 không quan tâm đến người sử dụng, mà chỉ xác thực một trạm hay thiết bị không dây. Những hệ thống xác thực có thể đơn giản là mật khẩu-tên đến những giao thức thách thức-đáp ứng. Họ 802.11 định nghĩa hai dịch vụ xác thực cơ bản: phương pháp xác thực mở và phương pháp xác thực chia sẻ khoá. Có hai cơ chế khác cũng thường được dùng cho xác thực: SSID (Service Set Identifier), và địa chỉ MAC (Media Access Control).

2.1.3.1. Xác thực mở và những lỗ hổng

Phương pháp xác thực mở không triển khai mật mã. Nó là một thuật toán xác thực không, có nghĩa là AP sẽ cấp bất kỳ yêu cầu nào cho xác thực thiết bị. Một trạm không dây có thể truy cập mạng không dây mà không cần bất kỳ xác thực xác minh nào. Nếu như một trạm không dây (client không dây) có thể tìm thấy và truyền thông với AP, nó sẽ được phép gia nhập mạng không dây. Cơ chế an toàn duy nhất được triển khai cho xác thực mở là SSID

của AP. Nếu như mã hoá WEP không được triển khai, một thiết bị chỉ cần biết SSID của AP sẽ có thể giành quyền truy cập tới mạng. Nếu như mã hoá WEP được thiết lập trên AP, thiết bị này sẽ không thể truyền hoặc nhận dữ liệu từ AP nếu như không có một khoá WEP đúng. Năm 1997, xác thực 802.11 thiên về kết nối, và cho phép các thiết bị truy cập nhanh chóng tới những mạng không dây. Xác thực mở cung cấp kết nối đơn giản và dễ dàng tới một mạng không dây, và được sử dụng cho một WLAN công cộng.

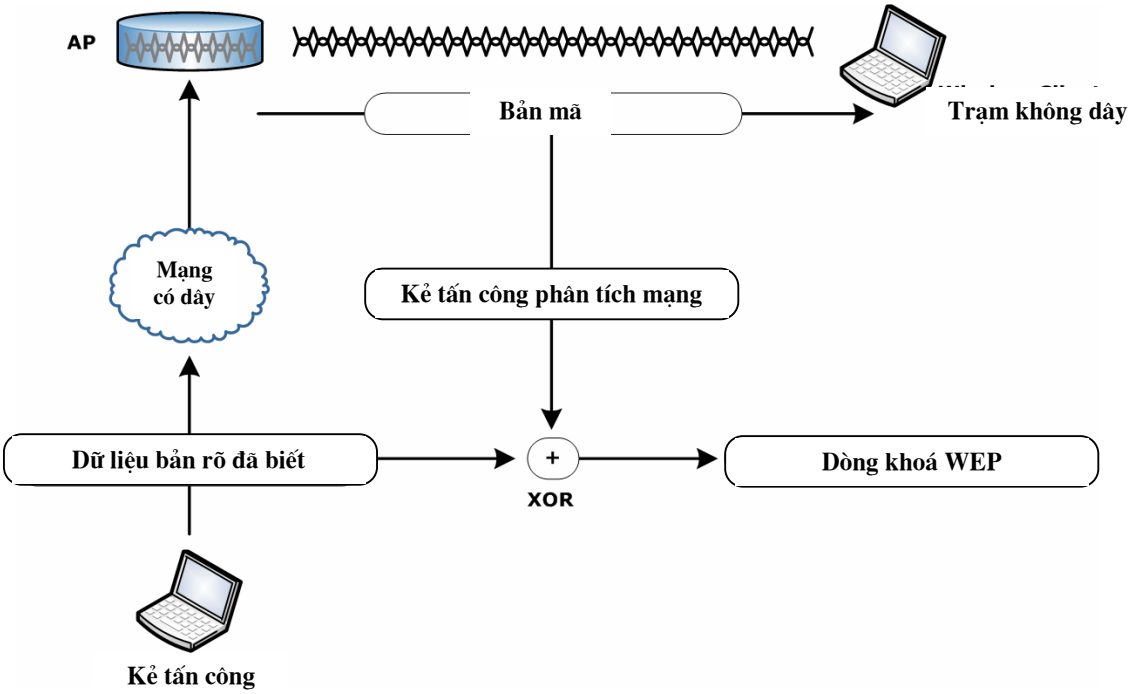
Không có cách nào để AP có thể xác định xem một client không dây có hợp lệ hay không nếu dùng xác thực mở. Điều này có thể tạo ra nguy cơ an toàn đáng kể nếu như xác thực mở được triển khai mà không thực thi mã hoá WEP. Tuy nhiên, WEP đã bị phá và không còn là một giải pháp an toàn WLAN có thể dùng được [14].

2.1.3.2. Xác thực khoá chia sẻ và những lỗ hổng

Sử dụng xác thực khoá chia sẻ được xem là một trong số những phương pháp xác thực an toàn hơn trong một môi trường WLAN. Nó sử dụng một kỹ thuật mật mã cho xác thực, và dựa trên cơ sở một giao thức thách thức-đáp ứng. Xác thực khoá chia sẻ yêu cầu một khoá WEP tĩnh được cấu hình bởi một client không dây. AP gửi một thách thức ngẫu nhiên dưới dạng bản rõ tới một client không dây. Nếu như client không dây này biết khoá chia sẻ, nó sẽ mã hoá thách thức và gửi kết quả trở lại AP. AP sẽ chỉ cho phép truy cập nếu như giá trị được giải mã (kết quả do client không dây tính toán) giống như thách thức ngẫu nhiên được truyền bởi AP.

Có nhiều vấn đề cơ bản đi kèm với xác thực chia sẻ khoá. Trước tiên, nó không cung cấp xác thực lẫn nhau, tuy nhiên chỉ đơn thuần thiết lập chứng minh rằng cả hai bên (AP và client không dây) chia sẻ cùng một bí mật. Thứ hai, phương pháp xác thực khoá chia sẻ phụ thuộc vào cơ sở hạ tầng WEP đã được chứng minh là không an toàn. Thứ 3, quá trình thách thức-đáp ứng được giải thích ở trên là lỗ hổng cho tấn công man-in-the-middle. Một kẻ trộm có

thể bắt được cả thách thức bản rõ và đáp ứng bản mã chỉ bằng cách phân tích mạng với một công cụ phân tích giao thức, và xác định được dòng khoá.



Hình 2.1: Tấn công bản rõ đã biết

2.1.3.3. Xác thực địa chỉ MAC và những lỗ hổng

Chính sách của AP cũng có thể căn cứ vào truy cập của nó trên địa chỉ MAC của client, ở đó việc xác thực địa chỉ MAC là phù hợp với bảng địa chỉ MAC hợp lệ của AP. Lọc địa chỉ MAC không được chỉ ra trong 802.11. Tuy nhiên, nhiều nhà sản xuất hỗ trợ phương pháp xác thực này. Lọc địa chỉ MAC cung cấp tầng an toàn khác để ngăn cản những thiết bị không được quyền truy cập mạng, và gia cố thêm cho xác thực mở và xác thực khoá chia sẻ được cung cấp bởi họ chuẩn 802.11.

2.1.4. Tính sẵn sàng

Yêu cầu một WLAN luôn sẵn sàng đối với những người truy cập được quyền khi cần thiết. Đó là khả năng nhận và gửi dữ liệu mà không bị ngắt quãng những dịch vụ. Những tấn công kiểu từ chối dịch vụ DoS là một mối đe doạ cho tính sẵn sàng mạng. Các tổ chức phải triển khai những cơ chế phòng

thủ để dò và bảo vệ trước các dạng khác nhau của tấn công DoS để đảm bảo luôn đạt được tính sẵn sàng mạng.

2.1.5. Điều khiển truy cập

Điều khiển truy cập là khả năng đảm bảo những người sử dụng chỉ nhìn thấy thông tin mà họ được quyền nhìn. Những thực thể (username, địa chỉ MAC,..) sử dụng những xác minh như những mật khẩu, và những khoá chia sẻ để thiết lập xác minh, được xác thực bởi những hệ thống AAA (RADIUS, LDAP,..). Nó sử dụng những giao thức xác thực 802.1x hoặc những giao thức tương tự (EAP, LEAP, PEAP,..) để trao đổi những xác minh và thiết lập những bắt tay đáp ứng/thách thức.

Khi được xác thực, một hệ thống AAA cấp quyền và kiểm soát truy cập tới những tài nguyên mạng cho người sử dụng. Những cơ chế an toàn điều khiển truy cập dựa trên cơ sở xác thực, và nhận biết về khoá WEP trước khi truy cập và cấp quyền.

2.1.6. Mã hoá/Giải mã

Mã hoá là cơ chế để đạt độ tin cậy. Đó là khả năng biến bản rõ thành những byte vô nghĩa, được gọi là bản mã, dựa trên cơ sở 3 thuật toán 802.11 cơ bản: WEP, TKIP và AES (CCMP). Giải mã là quá trình ngược lại. Đó là khả năng biến đổi những byte vô nghĩa (bản mã) thành dữ liệu có nghĩa (hay bản rõ). Đơn giản, những kỹ thuật mã hoá cung cấp 3 mục tiêu an toàn chính cho một WLAN: tin cậy, toàn vẹn tin và hỗ trợ xác thực, cấp quyền và quá trình điều khiển truy cập.

2.1.7. Quản lý khoá

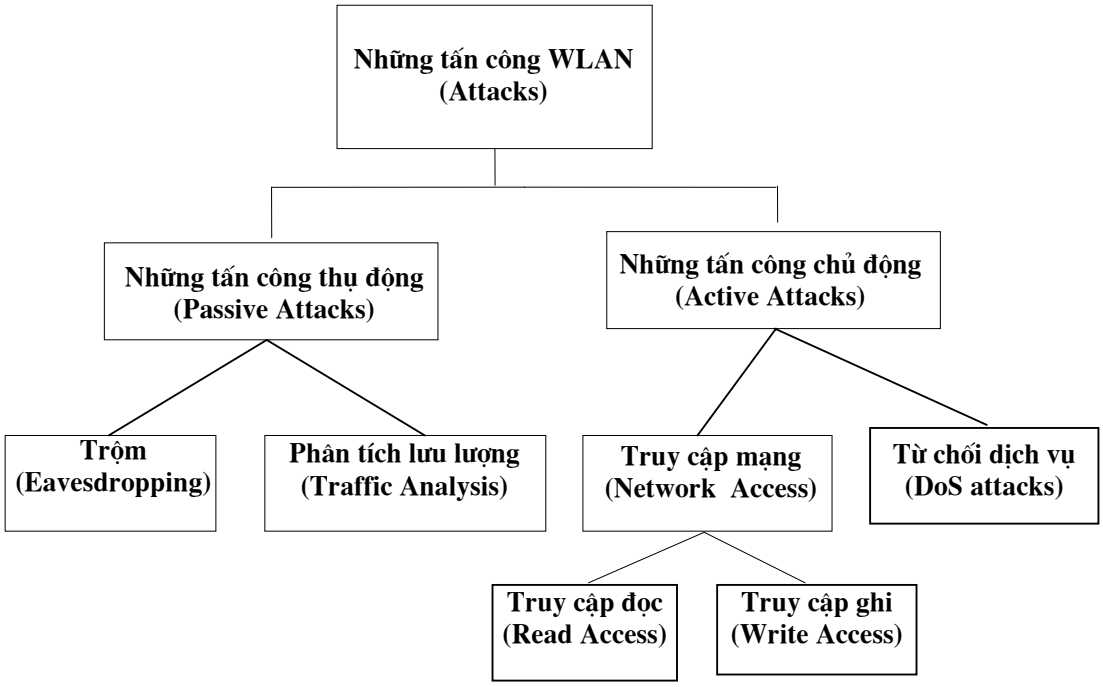
Quản lý khoá là quá trình phân phối khoá để hỗ trợ mã hoá, giải mã, và xác thực lẫn nhau. Nó là quá trình tạo, lưu trữ, phân phối, và cung cấp bảo vệ khoá tổng thể. Một khoá là một mã số. Được sử dụng để mã hoá, giải mã và ký thông tin. Độ dài khoá và sức mạnh của khoá là hai yếu tố quan trọng liên quan đến vấn đề quản lý khoá. Sức mạnh khoá là khả năng không bị giải mã

của mã số, và thường được tính bằng thời gian, nỗ lực và những tài nguyên yêu cầu để phá khoá. Độ dài khoá là số lượng bít trong khoá. Khoá càng dài thì càng khó phá khoá bằng tấn công bắt ép thô bạo (brute force attack). Tuy nhiên, phải có một sự cân bằng giữa chi phí khoá và giá trị thông tin mà khoá đó bảo vệ. Khoá càng dài thì yêu cầu càng nhiều overhead và giải thông, và càng đắt đỏ hơn về mặt tính toán để mã hoá và giải mã. Có hai kiểu khoá: khoá công khai, và khoá chia sẻ hay khoá bí mật. Với khoá công khai, tất cả mọi người đều biết, với khoá chia sẻ chỉ được biết bởi bên nhận tin. Với WEP khoá được phân phối bằng tay, và là duy nhất cho mạng. Với chuẩn IEEE 802.11i (những giao thức WPA/WPA2), khoá được phân phối tự động, và là duy nhất cho một gói tin, phiên và người sử dụng.

2.2. Những mối đe doạ an toàn WLAN và những lỗ hổng an toàn

WLAN dễ dàng bị tấn công và truy cập không được quyền hơn môi trường mạng LAN hữu tuyến. Khó có thể ngăn cản được truy cập tới một mạng không dây, bởi vì WLAN làm việc qua môi trường không khí. Bất kỳ ai đều có thể chặn bắt và truyền những tín hiệu không dây nếu như họ đang ở trong vùng phủ sóng và có những công cụ tốt để thực hiện điều đó. Điều này khiến cho an toàn không dây trở thành một thách thức thực sự. Nhiều tài liệu về những tấn công lên mạng không dây 802.11 đã được công bố nhằm cảnh báo những tổ chức về các nguy cơ an toàn cần được xem xét. Hậu quả của một tấn công có thể dẫn đến những phá huỷ cho một tổ chức như mất mát thông tin độc quyền, mất mát dịch vụ mạng, tốn kém chi phí phục hồi.

Hình sau đây đưa ra phân loại chung những tấn công an toàn mạng WLAN.



Hình 2.2: Phân loại chung những tấn công an toàn WLAN

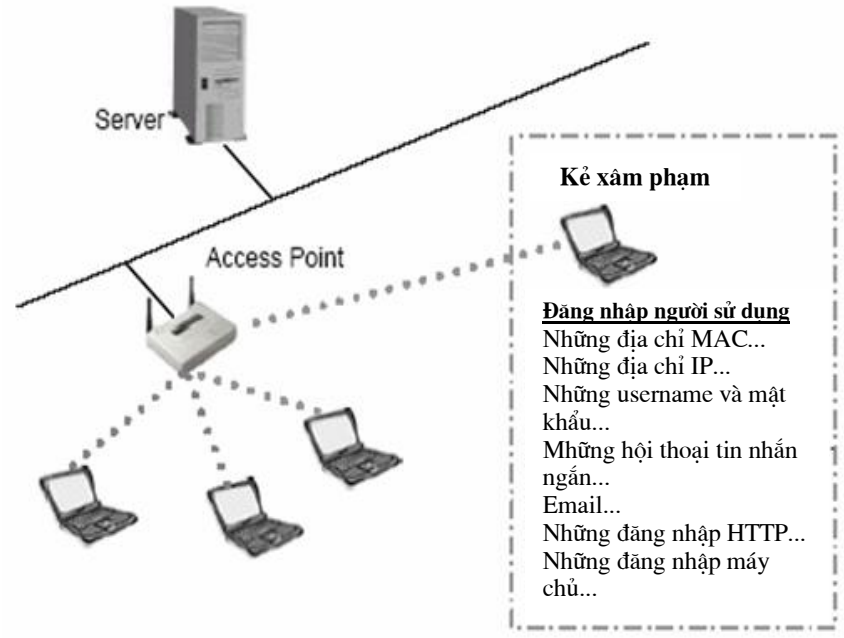
Có hai kiểu tấn công an toàn: thụ động và bị động. Những tấn công thụ động gồm truy cập không được quyền tới một mạng vì mục đích trộm hay phân tích lưu lượng, và không biến đổi nội dung của nó. Một tấn công chủ động là một truy cập không được quyền tới một mạng vì mục đích thực hiện những thay đổi tới một tin, dòng dữ liệu, hoặc file, hoặc ngắt quãng những chức năng của một dịch vụ mạng. Có nhiều lý do giải thích tại sao một kẻ tấn công có thể nhằm vào một mạng không dây hay một tổ chức. Tuy nhiên, 3 mục tiêu chính của một kẻ tấn công nhằm ngắt quãng những hoạt động mạng thông thường của một tổ chức bằng cách từ chối dịch vụ DoS, giành quyền đọc, hoặc giành quyền ghi. Hành động của một tấn công thường bắt đầu với giai đoạn thăm dò, tiếp theo là một tấn công chủ động để giành quyền truy cập mạng hoặc DoS.

2.2.1. Tấn công thụ động (passive attack)

Thường một tấn công có hai giai đoạn thực hiện. Giai đoạn đầu tiên được gọi là giai đoạn thăm dò, thực hiện một cách thụ động. Trong giai đoạn thăm dò, một kẻ tấn công phải khám phá một mạng mục tiêu, và sau đó tìm ra nhiều thông tin hơn về mạng. Hai phương pháp được triển khai để thực hiện tấn công thụ động: trộm, và phân tích lưu lượng.

- Trộm: Trộm có lẽ là phương pháp đơn giản nhất, tuy nhiên, nó vẫn có hiệu quả đối với WLAN. Tấn công bị động như một cuộc nghe trộm mà không phát hiện được sự có mặt của người nghe trộm (hacker) trên hoặc gần mạng khi hacker không thực sự kết nối tới AP để lắng nghe các gói tin truyền qua phân đoạn mạng không dây, sử dụng thiết bị ứng dụng nào đó để lấy thông tin của WLAN từ một khoảng cách với một ăngten hướng tính.

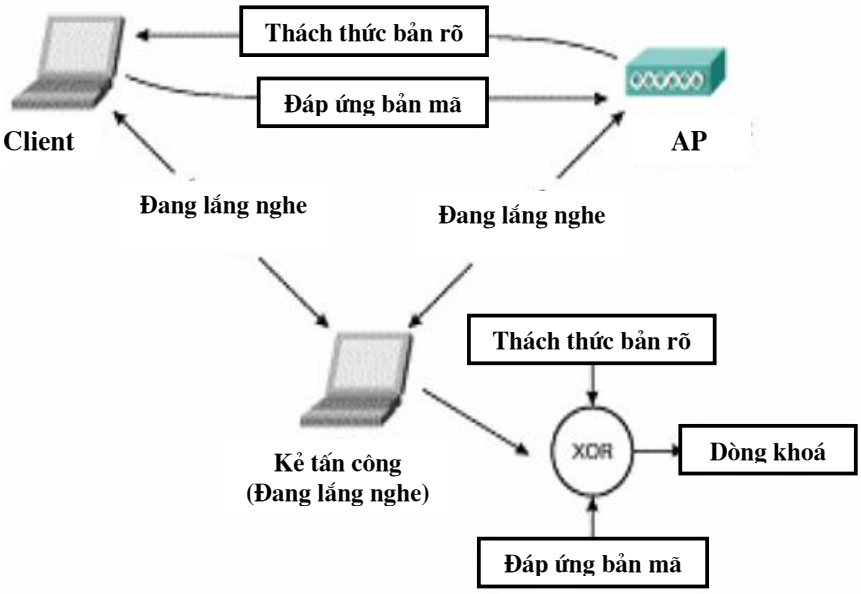
- ***Phân tích đường truyền*** – Kẻ tấn công, theo một cách tinh vi hơn, thu thông tin nhờ theo dõi những cuộc truyền giữa các bên truyền tin. Một lượng thông tin đáng kể đạt được trong luồng tin giữa những bên truyền tin.



Hình 2.3: Tấn công bị động

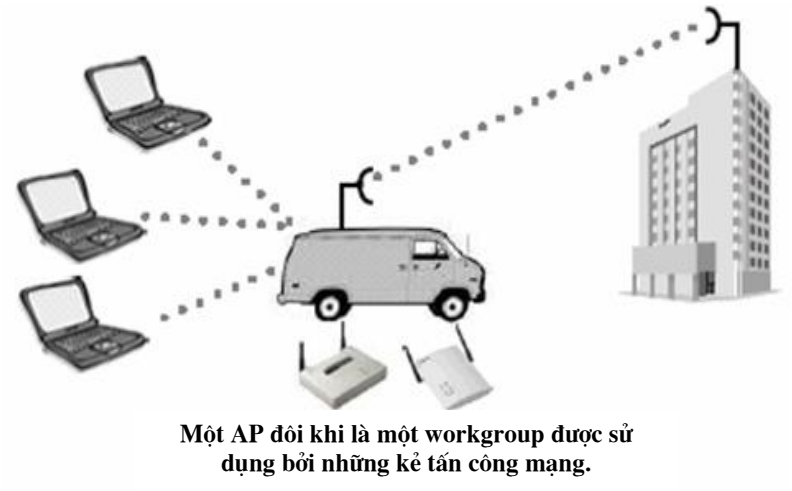
Phương pháp này cho phép hacker giữ khoảng cách thuận lợi không để bị phát hiện, nghe và thu nhặt thông tin quý giá.

Trong thế giới không dây, những công cụ phân tích mạng là những phương tiện hiệu quả nhất để có thể tìm ra những gì đang xảy ra trên một mạng. Phân tích mạng có thể thực hiện hai chức năng then chốt: chặn bắt gói tin và phân tích gói tin. Việc phân tích một gói tin cho phép một kẻ tấn công xác định những khả năng gì có trên một mạng, và có thể cung cấp tất cả những loại thông tin tin cậy để khai thác một tổ chức. Với việc chặn bắt gói tin, một kẻ tấn công có thể khôi phục những khoá WEP trong vòng vài phút, tạo khả năng đọc tất cả dữ liệu truyền giữa client và AP không dây.



Hình 2.4: Qúa trình lấy khoá WEP

Có nhiều công cụ phân tích mạng sẵn có. Một kỹ thuật được sử dụng trong quá trình thăm dò là War Driving. War Driving là quá trình điều tra những mạng không dây bằng cách sử dụng một xe ô tô (tấn công theo kiểu thu hút Man-in-the-Middle).



Hình 2.5: Tấn công MitM (Man-in-the-middle)

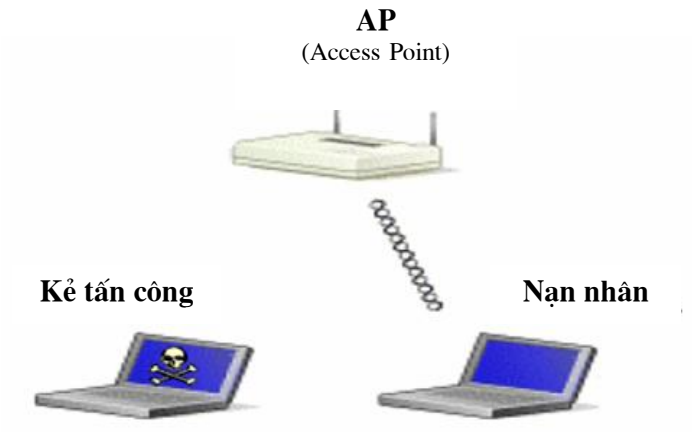
Kiểu tấn công man-in-the-middle là một tình trạng mà trong đó một cá nhân sử dụng một AP để chiếm đoạt sự điều khiển của một node di động bằng cách gửi những tín hiệu mạnh hơn những tín hiệu hợp pháp mà AP đang gửi tới những node đó, Sau đó node di động kết hợp với AP trái phép này, để gửi các dữ liệu của người xâm nhập, có thể là các thông tin nhạy cảm.

Để các client liên kết với AP trái phép thì công suất của AP đó phải cao hơn nhiều của các AP khác trong khu vực và đôi khi phải là nguyên nhân tích cực cho các user truy nhập tới. Việc mất kết nối với AP hợp pháp có thể như là một việc tình cờ trong quá trình vào mạng, và một vài client sẽ kết nối tới AP trái phép một cách ngẫu nhiên.

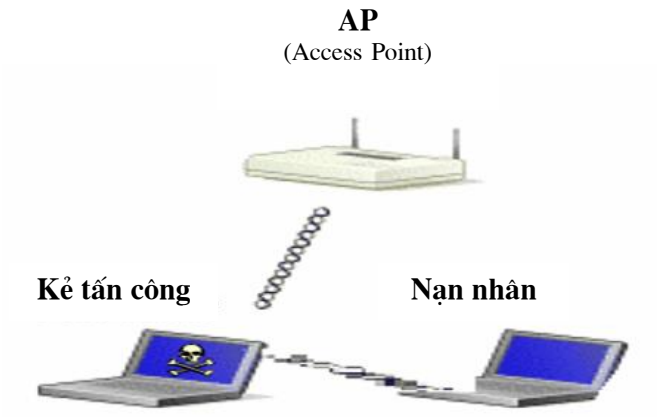
Người thực hiện tấn công man-in-the-middle trước tiên phải biết SSID mà client sử dụng, và phải biết khoá WEP của mạng, nếu nó đang được sử dụng.

Kết nối ngược (hướng về phía mạng lõi) từ AP trái phép được điều khiển thông qua một thiết bị client như là PC card hoặc workgroup bridge. Nhiều khi tấn công man-in-the-middle được sắp đặt sử dụng một laptop với hai card PCMCIA. Phần mềm AP chạy trên một laptop mà ở đó một PC card được sử dụng như là một AP và PC card thứ hai được dùng để kết nối laptop

tới gần AP hợp pháp. Kiểu cấu hình này biến laptop thành một tấn công man-in-the-middle vận hành giữa client và AP hợp pháp. Một hacker theo kiểu tấn công man-in-the-middle có thể lấy được các thông tin có giá trị bằng cách chạy một chương tình phân tích mạng trên laptop trong trường hợp này.



Hình 2.6: Trước cuộc tấn công



Hình 2.7: và sau cuộc tấn công

Một điều đặc biệt với kiểu tấn công này là người sử dụng không thể phát hiện ra được cuộc tấn công, và lượng thông tin thu nhặt được nhờ tấn công kiểu này là giới hạn, nó bằng lượng thông tin thủ phạm lấy được trong khi còn trên mạng mà không bị phát hiện.

Biện pháp tốt nhất để ngăn ngừa loại tấn công này là bảo mật lớp vật lý.

Có những ứng dụng có khả năng lấy mật khẩu từ các Site HTT, email, các instant messenger, các phiên FTP, các phiên telnet được gửi dưới dạng text không được mã hoá. Có những ứng dụng khác có thể lấy mật khẩu trên những phân đoạn mạng không dây giữa Client và Server cho mục đích truy cập mạng.

Xem xét tác động nếu một hacker tìm được cách truy nhập tới một domain của người sử dụng, hacker đó sẽ đăng nhập vào domain của người sử dụng và gây hậu quả nghiêm trọng trên mạng. Tất nhiên, việc đó là do hacker thực hiện, nhưng người dùng phải trực tiếp chịu trách nhiệm, và gánh chịu mọi hậu quả.

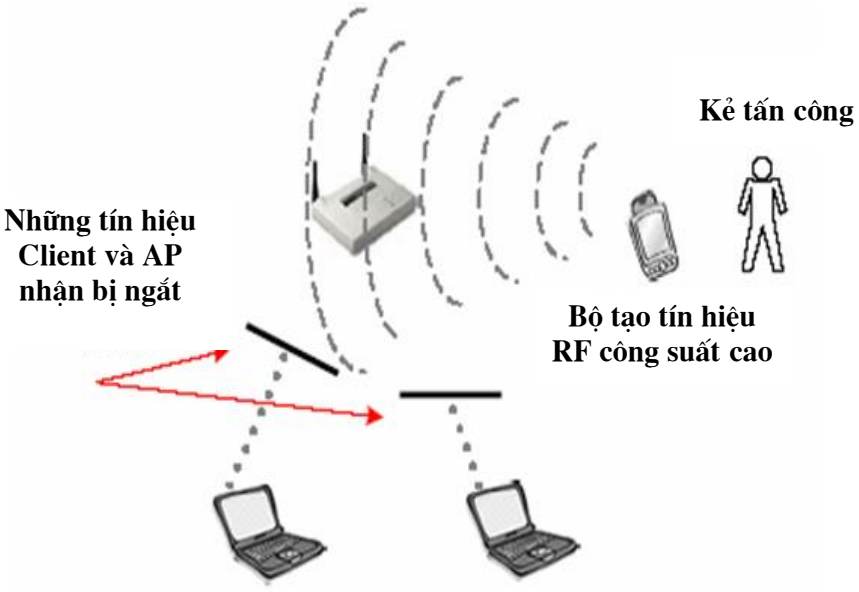
Một tình huống khác trong đó mật khẩu HTTP hoặc email bị lấy trên những phân đoạn mạng không dây, và sau đó được hacker sử dụng với mục đích truy nhập tới WLAN.

2.2.2. Tấn công chủ động

Một kẻ tấn công chủ động có thể giả mạo một người sử dụng hợp pháp và giành những quyền lợi bất hợp pháp nhất định, giám sát những lần truyền một cách thụ động và sau đó truyền lại những tin như là một người sử dụng hợp pháp (tấn công dùng lại - replay), hoặc biến đổi những tin hợp pháp.

Những tấn công DoS có thể là sự phá huỷ thiết bị vật lý, ngắt quãng những dịch vụ mạng nhất định, ngăn cản hoặc cấm sử dụng thông thường các khả năng mạng của một tổ chức, hoặc là một tấn công được thiết kế để sử dụng tất cả dải thông của một mạng. Những tấn công DoS có thể ngắt quãng những dịch vụ đối với một người sử dụng cụ thể hoặc đối với toàn mạng. Một kẻ tấn công có thể thiết lập một AP giả mạo và kết hợp những người sử dụng tới một mạng giả mạo. Trong thế giới không dây, những tấn công DoS khó giải quyết hơn bởi vì nó dễ dàng truy cập tới mạng hơn. Sau đây là một số hiện tượng đi kèm với DoS:

- Triển khai thiết bị nghẽn radio: Ví dụ tấn công theo kiểu chèn ép (jamming attack): là một kỹ thuật sử dụng đơn giản để đóng mạng của bạn. Tương tự như việc kẻ phá hoại sắp đặt một sự từ chối dịch vụ một cách áp đảo, sự tấn công nhằm vào Web server, vì vậy một WLAN có thể ngừng làm việc vì một tín hiệu RF áp đảo. Tính hiệu RF đó có thể vô tình hoặc cố ý, và tín hiệu có thể di chuyển hoặc cố định. Khi một hacker thực hiện một cuộc tấn công jamming có chủ ý, hacker có thể sử dụng thiết bị WLAN nhưng có nhiều khả năng hơn là hacker sẽ dùng một máy phát tín hiệu RF công suất cao hoặc máy tạo sóng quyết.



Hình 2.8: Tấn công theo kiểu chèn ép.

Để loại bỏ kiểu tấn công này, yêu cầu trước hết là tìm được nguồn phát tín hiệu RF đó, bằng cách phân tích phổ.

Khi jamming gây ra bởi một nguồn cố định, không chủ ý, như một tháp truyền thông hoặc các hệ thống hợp pháp khác, thì người quản trị mạng WLAN có thể phải xem xét đến việc sử dụng bộ thiết đặt các tần số khác nhau. Ví dụ, nếu một admin có trách nhiệm thiết kế và cài đặt một mạng RF trong một khu phòng rộng, phức tạp, thì người đó cần phải xem xét một cách

kỹ càng theo thứ tự. Nếu nguồn giao thoa là một điện thoại, hoặc các thiết bị làm việc ở dải tần 2.4 GHz, thì admin có thể sử dụng thiết bị ở dải tần UNII, 5GHz, thay vì dải tần 802.11b, 2.4 GHz và chia sẻ dải tần ISM 2.4 GHz với các thiết bị khác.

Sự jamming không chủ ý xảy ra với mọi thiết bị dùng chung dải tần 2.4 GHz. Jamming không phải là sự đe doạ nghiêm trọng vì jamming không thể được thực hiện phổ biến bởi hacker do vấn đề giá cả của thiết bị, nó quá đắt trong khi hacker chỉ tạm thời vô hiệu hóa mạng.

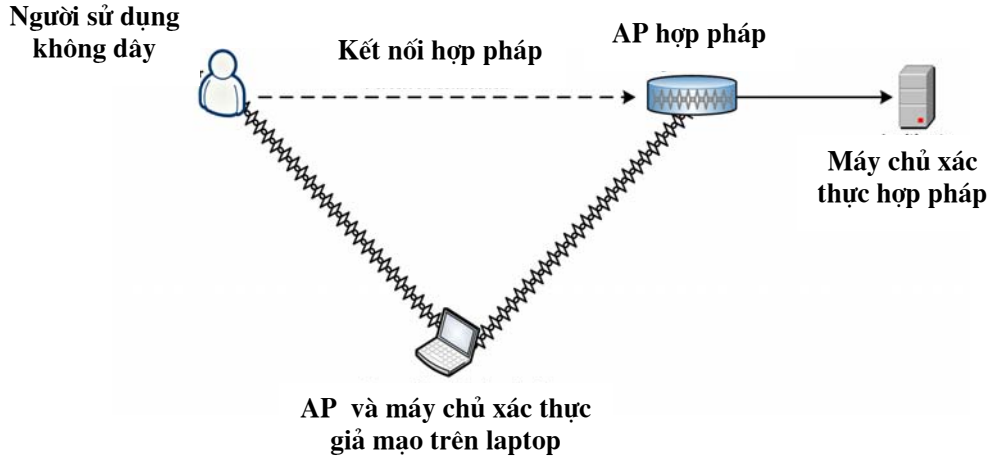
- Làm đầy dải thông mạng bằng những khung truyền liên tục.

- Thực hiện những tấn công giải kết hợp/tái kết hợp.

- Tiến hành truyền những tấn công khoảng thời gian bằng cách cấu hình trường thời gian truyền tối đa với tốc độ 30 gói tin trên một giây.

- Làm đầy những bảng AP bằng cách ngập lụt những kết hợp.

- Thiết lập một AP giả mạo và kết hợp những người sử dụng tới một mạng giả mạo để thiết lập một tấn công man-in-the-middle.



Hình 2.9: Tấn công MitM sử dụng một AP giả mạo

Những tấn công chủ động có thể được thực hiện bằng phương tiện giành quyền truy cập mạng để có những khả năng đọc và ghi. Mục đích cho những tấn công truy cập mạng là giành quyền truy cập tới những tài nguyên mạng

hoặc để chặn bắt và giải mã dữ liệu (nếu mã hoá). Truy cập đọc là khả năng của một kẻ tấn công chặn bắt và đọc lưu lượng từ một mạng, cung cấp khả năng đưa ra những tấn công lên mã hoá, xác thực, và những phương pháp bảo vệ khác. Khi một kẻ tấn công có khả năng khám phá một mạng mục tiêu thông qua việc thăm dò, và chặn bắt lưu lượng được mã hoá hay không được mã hoá bằng một phương tiện phân tích mạng, kẻ tấn công có thể giành được nguyên liệu khoá và khôi phục những khoá mã hoá. Việc lộ những khoá mã hoá có thể tạo khả năng cho một kẻ tấn công truy cập hoàn toàn tới mạng mục tiêu. Truy cập viết là khả năng gửi lưu lượng tới một thực thể mạng. Sau đây là một số mục đích của một kẻ tấn công với truy cập viết và đọc mạng:

- Khôi phục những khoá mã hoá.

- Khôi phục những dòng khoá được tạo ra bởi những khoá mã hoá.

- Chèn thêm những gói dữ liệu: Viết dữ liệu được mã hoá bằng cách dùng lại dòng khoá chặn bắt được.

- Mã hoá dữ liệu bằng khoá và chèn dữ liệu lên mạng.

- Cài đặt phần mềm gián điệp trên một client không dây và có khả năng đọc những kết quả.

- Thiết lập một AP giả mạo và kiểm soát những tham số mạng (như những khoá mã hoá chẳng hạn).

- Bỏ qua những sơ đồ xác thực:

+ Bằng cách triển khai giả mạo địa chỉ MAC để tránh lọc địa chỉ MAC.

+ Bằng cách triển khai xác thực khoá chia sẻ bỏ qua những tấn công.

+ Bằng cách thực hiện những tấn công từ điển LEAP nếu như sử dụng 802.1x cho xác thực.

+ Bằng cách thực hiện những tấn công MitM PEAP nếu như mạng đang sử dụng 802.1x cho xác thực.

- Cài đặt mã gây hại lên một client không dây.

WLAN được thực hiện với những khung gọi là những khung báo hiệu (beacon) được truyền và phục vụ như những cơ chế khám phá chính cho những client không dây để dò AP trong một BSS. Điều này để lộ tín hiệu cho bất kỳ ai có khả năng lắng nghe và ở trong phạm vi phủ sóng WLAN. Nếu như một WLAN có thể được đặt trong một văn phòng ở đó những tín hiệu vô tuyến không thể thoát ra được, khi đó nguy cơ truy cập không được quyền bị tối thiểu hoá. Bởi vì điều này không phải lúc nào cũng là một giải pháp có thể thực hiện, những giải pháp an toàn khác phải được triển khai như kiểm soát truy cập mạnh và công nghệ mã hoá. Những kỹ thuật dùng để giành quyền truy cập không được quyền tới một WLAN là những vấn đề an toàn được biết đến. Nhiều những vấn đề an toàn WLAN gần đây đã được sửa đổi với những triển khai công nghệ trong chuẩn 802.11i. Bảng sau đây đưa ra những tấn công an toàn đã biết được triển khai chống lại WLAN.

Tấn công	**Mô tả**	**Mục tiêu**	**Những giải pháp cho bảo vệ**
Những tấn công DoS	Ngắt quãng những dịch vụ mạng	Những dịch vụ mạng	Lọc MAC, những tường lửa (có dây), IDS (có dây), kiến trúc DMZ, 802.11i.
Giải kết hợp và tái kết hợp (tấn công DoS)	Khai thác bản chất không xác thực của những khung quản lý 802.11. Do thiếu xác thực mạnh, một client không dây có thể giả mạo giải kết hợp hoặc tái kết hợp một tin, do đó ngắt quãng những dịch vụ mạng. Do một AP phải kết hợp với một client không dây trước khi lưu	Những dịch vụ mạng.	Yêu cầu xác thực mạnh những khung quản lý và điều khiển. 802.11i hiện tại không ngăn ngừa được những tấn công này.

	lượng có thể được truyền nên một kẻ tấn công có thể duy trì hiệu quả một hoặc nhiều trạm khỏi việc truyền bằng cách gửi liên tục những khung giải kết hợp. Có nhiều thực thi được biết đến về kiểu tấn công này.		
Trường thời gian truyền (Transit Duration Field)- tấn công DoS.	Dựa trên cơ sở trường thời gian truyền của khung 802.11 công bố tới những nút khác một khung sẽ kéo dài trong bao lâu. Nếu như một dòng gói tin do một kẻ tấn công gửi thì trường thời gian truyền sẽ thiết lập đến mức tối đa của nó ($1/30^{th}$ của giây) điều này ngăn chặn những trạm khác truyền trong khoảng thời gian đó, xâm chiếm mạng một cách hiệu quả.	Những dịch vụ mạng.	Logic trong những card NIC không dây bỏ qua trường thời gian truyền. Yêu cầu xác thực mạnh những khung điều khiển và quản lý. 802.11i hiện nay không ngăn ngừa được những tấn công kiểu này.
Những tấn công xác thực	Khai thác những phương pháp xác thực để giành quyền truy cập mạng.	Truy cập mạng	Xác thực dựa trên cơ sở 802.1x và EAP.
Xác thực chia sẻ khoá	Cơ chế xác thực lẫn nhau có lỗ hổng, dựa trên cơ sở một giao thức đáp ứng-thách thức. Trong quá trình xác thực chia sẻ khoá, mỗi bên đáp ứng một thách thức bằng một tin được mã hoá	Truy cập mạng.	Xác thực khoá mở hay xác thực dựa trên cơ sở EAP.

	chứng minh nhận biết của nó về khoá WEP. Một kẻ tấn công có thể đơn giản thực hiện XOR tin thách thức và đáp ứng và xác định một phần của dòng khoá để tạo ra một đáp ứng xác thực thành công trong tương lai.		
Gỉa mạo địa chỉ MAC	Việc phân tích mạng có thể dò ra được địa chỉ MAC hợp lệ có thể được sử dụng với những driver card 802.11 nhất định để giả mạo địa chỉ MAC và giành quyền truy cập mạng.	Truy cập mạng	802.11i (TKIP và CCMP) hay VPN.
Man-in-the-middle	Một kẻ tấn công có khả năng chặn bắt/giải mã những khung trong quá trình kết hợp để cung cấp thông tin then chốt. Với thông tin này, một kẻ tấn công có thể cài đặt một AP giả mạo để buộc client không dây phải tái kết hợp với AP giả mạo. Điều này cho phép kẻ tấn công có thể truy cập tới tất cả dữ liệu được truyền giữa client và máy chủ. Lưu ý client không dây và máy chủ tin rằng chúng đang kết nối trực tiếp với nhau, và	Truy cập mạng.	An toàn vật lý, 802.1x hay VPN.

	không phải AP giả mạo hay MitM.		
Những tấn công từ điển (phá mật khẩu)	Một kẻ tấn công có thể tập hợp những trao đổi thách thức và đáp ứng từ những giao thức dựa trên cơ sở mật khẩu, với khả năng xác định kết hợp tên đăng nhập-mật khẩu. Sử dụng những công cụ nguồn mở dựa trên cơ sở từ điển gồm hàng trăm nghìn từ/cụm từ, và một máy tính offline để xoay vòng qua mỗi kết hợp tên-mật khẩu có thể, thông tin đăng nhập có thể bị lộ. Khi bị lộ, một kẻ tấn công có những quyền và đặc ân của người sử dụng đó.	Truy cập mạng.	Chính sách mật khẩu mạnh, 802.1x và VPN.
Tấn công bản rõ đã biết (Khôi phục dòng khoá WEP).	Một kẻ tấn công có thể khôi phục những dòng khoá mà một khoá có thể tạo ra được gọi là một tấn công bản rõ đã biết. Một kẻ tấn công gửi dữ liệu qua một mạng hữu tuyến tới một client không dây, và chặn bắt dữ liệu được mã hoá từ AP đang được gửi tới cho client không dây. Khi bắt được, một kẻ tấn công có thể áp dụng	Truy cập mạng	WPA và 802.11i.

	phép toán XOR trên bản rõ và dữ liệu chặn bắt được (bản mã) để xác định dòng khoá. Một kẻ tấn công sẽ có thể giải mã bất kỳ lưu lượng nào được sử dụng bởi khoá WEP đó, khi một từ điển được thiết lập cho tất cả 15 triệu dòng khoá.		
Những va đập IV (khôi phục dòng khoá WEP).	Một phương pháp khôi phục dòng khoá WEP bằng cách chờ một va đập (những dòng khoá được lặp lại). Một kẻ tấn công có thể tập hợp những va đập IV và thông qua những kỹ thuật mật mã để khám phá dữ liệu và những dòng khoá. Khi khám phá được, một kẻ tấn công có thể xây dựng một từ điển dòng khoá.	Truy cập mạng.	WPA và 802.11i.
Phá WEP (Những tấn công khôi phục khoá WEP).	Một kẻ tấn công có thể khôi phục những khoá mã hoá bằng cách sử dụng một công cụ phân tích để tập hợp từ 5 đến 10 triệu gói tin. Bằng việc sử dụng những công cụ như WEPcrack hay Airsnort [15], một kẻ tấn công có thể xác định được những khoá mã hoá trong một	Truy cập mạng.	WPA và 802.11i.

	vài phút và giành quyền đọc/ghi dữ liệu được mã hoá.		
Chèn lưu lượng (khôi phục khoá WEP)	Sau khi khôi phục một dòng khoá, một kẻ tấn công có khả năng chèn thêm những gói tin bằng cách sử dụng lại IV.	Truy cập mạng.	WPA và 802.11i (thuật toán MIC), Cisco có những cơ chế được thực thi để từ chối bất kỳ những IV nào bị lặp lại.
Tấn công bít lật (Biến đổi tin)	Lật bít dựa vào sự yếu kém của ICV (Integrity Check Vector-Vectơ kiểm tra tính toàn vẹn), bởi vì nó có thể được tính toán lại thậm chí dưới dạng được mã hoá. Một kẻ tấn công có thể lấy một tin, lập những bít bất kỳ trong vị trí dữ liệu của khung (những gói tin tầng cao hơn), tính toán lại một ICV hợp lý, sau đó truyền lại tin và được xem là hợp lệ. ICV sẽ được đẩy qua một AP hoặc client không dây, tuy nhiên CRC sẽ bị từ chối ở tầng 3 (router), tạo ra một tin lỗi bản rõ, kẻ tấn công có thể phân tích tin lỗi này và dò ra dòng khoá.	Truy cập mạng.	WPA và 802.11i (thuật toán MIC).
Tấn công dùng lại	Xuất phát từ việc khôi phục lại những dòng khoá từ một khoá	Truy cập mạng	WPA và 802.11i (thuật toán MIC, TSC trong

IV	WEP, một kẻ tấn công có thể phát triển dòng khóa bằng cách sử dụng cùng cặp khoá IV/WEP như khung quan sát được.Việc sử dụng lại cặp khoá IV/WEP này có thể tạo ra một dòng khoá đủ lớn để phá hoại một mạng.		TKIP, và PN trong CCMP).
PEAP MitM	Một kẻ tấn công có thể thiết lập một AP và AS giả mạo để ăn trộm những xác minh của một client nếu như một trong số hai nguyên tắc cho PEAP bị vi phạm. Trước tiên, client phải hợp thức hoá xác minh máy chủ, và không có khả năng vượt qua những xác minh máy chủ không hợp lệ. Thứ hai, những xác minh xác thực PEAP bên trong phải được cấu hình để chạy bên ngoài một phiên được bảo vệ. Nếu như vậy, một kẻ tấn công có thể ăn trộm những xác minh để đưa ra một phiên xác thực PEAP thành công. Lưu ý EAP-TTLS nhạy bén với tấn công MitM.	Truy cập mạng.	PEAP v2.
Tấn công	Khai thác việc sử dụng MS-	Truy cập	Chính sách mật khẩu

từ điển trên LEAP	CHAPv2 (một dạng không được mã hoá dùng cho xác thực) trong giao thức LEAP Cisco. Một kẻ tấn công có thể thực hiện những tấn công từ điển offline từ thông tin thách thức/đáp ứng phân tích được từ xác thực LEAP, và đối chiếu với kết hợp mật khẩu-tên đăng nhập. Khi đối chiếu phù hợp, một kẻ tấn công có thể đóng giả là một client không dây sử dụng phương pháp xác thực LEAP. Những công cụ như là asleap cung cấp phương tiện để đưa ra tấn công kiểu này.	mạng.	mạnh.
Cướp phiên	Khả năng của một kẻ tấn công định hướng lại lưu lượng mạng từ một người sử dụng cuối hợp pháp. Được gọi là cướp phiên, một kẻ tấn công phải có khả năng phân tích lưu lượng mạng, và chèn thông tin. Được thực hiện bằng cách thiết lập một AP giả mạo, với những client không dây không ngờ tới cố gắng xác thực nó.	Truy cập mạng.	802.11i, 802.1x và VPN.
Những AP	Những AP không được quyền	Truy cập	Chính sách kết hợp, an

giả mạo	trong một mạng, một AP giả mạo được sử dụng bởi những kẻ tấn công để giành quyền truy cập tới mạng thông qua những tấn công MitM.	mạng.	toàn vật lý và SWAN (Cisco Structured Wireless-Aware Network).

Bảng 2.2: Những tấn công an toàn không dây

2.3. Các biện pháp đảm bảo an toàn WLAN

Chúng ta có thể giảm thiểu nguy cơ cho WLAN bằng cách áp dụng các biện pháp đối phó nhằm giải quyết những mối hiểm hoạ và những lỗ hổng cụ thể. Những biện pháp quản lý kết hợp với các biện pháp kỹ thuật và vận hành có thể hiệu quả trong việc giảm thiểu những nguy cơ đi kèm với WLAN.

2.3.1. Các biện pháp quản lý

Các biện pháp quản lý để đảm bảo an toàn cho những mạng không dây bắt đầu bằng một chính sách an toàn tổng thể. Một chính sách an toàn là nền tảng mà nhờ đó những biện pháp đối phó khác – biện pháp kỹ thuật và vận hành - được hợp lý hoá và được thực thi. Một chính sách an toàn WLAN có thể thực hiện như sau:

- Xác minh người có thể sử dụng công nghệ WLAN trong một cơ quan.
- Xác minh xem có yêu cầu truy cập Internet không.
- Mô tả người có thể cài đặt các AP và những thiết bị không dây khác.
- Cung cấp những giới hạn về vị trí và an toàn vật lý cho các AP.
- Mô tả loại thông tin có thể được gửi qua những liên kết không dây.
- Mô tả những điều kiện mà các thiết bị không dây phải tuân thủ.
- Xác định những thiết đặt an toàn chuẩn cho các AP.
- Mô tả những giới hạn mà thiết bị không dây có thể được sử dụng như thế nào, như vị trí chẳng hạn.
- Mô tả cấu hình phần cứng và phần mềm của tất cả các thiết bị không dây.

- Cung cấp những hướng dẫn thông báo những mất mát thiết bị không dây và những sự cố an toàn.

- Cung cấp những hướng dẫn cho việc bảo vệ những client không dây để giảm thiểu vấn đề trộm.

- Cung cấp những hướng dẫn về sử dụng mật mã và quản lý khoá.

- Xác định tần số và phạm vi của những đánh giá an toàn để điều chỉnh AP.

Các cơ quan cũng nên lưu ý đào tạo nhân sự biết sử dụng công nghệ không dây. Những người quản trị mạng cần nhận thức đầy đủ về những nguy cơ an ninh của WLAN và những thiết bị của nó để từ đó có những biện pháp đối phó. Cuối cùng, biện pháp quan trọng nhất là người sử dụng phải được đào tạo và nhận thức được những nguy cơ an toàn cũng như về công nghệ WLAN.

2.3.2. Các biện pháp vận hành

An toàn vật lý là một bước cơ bản nhất mà chỉ những người sử dụng được quyền mới có thể truy cập tới thiết bị máy tính không dây. An toàn vật lý bao gồm những biện pháp như những kiểm soát truy cập, xác minh cá nhân, và những bảo vệ biên giới bên ngoài. Giống như những tiện ích an toàn cho những mạng có dây, những tiện ích hỗ trợ mạng không dây cần những kiểm soát truy cập vật lý. Ví dụ, xác minh ảnh, những thiết bị đọc dấu hiệu card, hoặc những thiết bị sinh trắc học có thể được sử dụng để giảm thiểu nguy cơ an toàn. Những hệ thống sinh trắc học cho những truy cập vật lý gồm quýet dấu vân tay, quýet tròng mắt, quýet võng mạc, nhận dạng giọng nói, chữ ký, nhận dạng khuôn mặt. Bảo vệ biên giới bên ngoài cơ quan gồm khoá cửa, cài đặt camera theo dõi.

Điều quan trọng cần phải tính đến phạm vi phủ sóng của AP khi quyết định vị trí đặt trong môi trường WLAN. Nếu như phạm vi này vượt quá những biên giới vật lý của những bức tường toà nhà văn phòng, thì phần vượt thêm này sẽ tạo ra một lỗ hổng an toàn. Một cá nhân ở bên ngoài toà nhà, có thể

gián điệp những truyền thông mạng bằng cách sử dụng một thiết bị không dây thu chặn những tín hiệu tần số vô tuyến. Một xem xét tương tự áp dụng cho việc thực thi những cầu nối giữa các toà nhà. Lý tưởng, các AP nên được đặt trong phạm vi một toà nhà do đó phạm vi này không thể vượt quá chu vi vật lý của toà nhà và không cho phép người không được quyền gián điệp gần chu vi đó. Các cơ quan nên sử dụng những công cụ điều tra vùng để đo đạc phạm vi phủ sóng của những thiết bị AP, cả bên trong lẫn bên ngoài toà nhà nơi có mạng không dây. Ngoài ra, các cơ quan cũng nên sử dụng các công cụ đánh giá an toàn không dây (ví dụ như đánh giá lỗ hổng) và hướng dẫn ghi chép nhật ký an toàn.

Các công cụ điều tra vùng sẵn có để đo đạc và đảm bảo an toàn vùng phủ sóng AP. Những công cụ này, một số nhà sản xuất có bán kèm với những sản phẩm của mình, đo cường độ tín hiệu nhận được từ các AP. Những đo đạc này có thể được sử dụng để chỉ ra vùng phủ sóng. Tuy nhiên, những nhà quản trị an toàn nên sử dụng thận trọng khi thông dịch kết quả bởi vì mỗi nhà sản xuất thông dịch cường độ tín hiệu nhận được khác nhau. Một số nhà sản xuất AP cũng đưa ra những kiểm soát mức nguồn và từ đó là phạm vi phủ sóng AP. Điều này thật hữu ích nếu như phạm vi phủ sóng yêu cầu không vượt quá, bởi vì, ví dụ, toà nhà hay căn phòng trong đó có truy cập tới mạng không dây cần phải đủ nhỏ. Kiểm soát phạm vi phủ sóng cho những toà nhà hay gian phòng nhỏ hơn này có thể giúp ngăn ngừa những tín hiệu không giây vượt ra ngoài không gian mở rộng phạm vi vùng phủ sóng dự kiến. Các cơ quan nên sử dụng thêm những ăngten định hướng để kiểm soát sự phát xạ tín hiệu. Tuy nhiên, những ăngten định hướng này không bảo vệ những kết nối mạng; chúng chỉ đơn thuần giúp kiểm soát phạm vi phủ sóng nhờ việc giới hạn sự phát tán tín hiệu.

Mặc dù việc chỉ ra phạm vi phủ sóng có thể tạo thuận lợi liên quan đến an toàn, tuy nhiên nó không được xem là một giải pháp tuyệt đối. Luôn có khả

năng có một cá nhân sử dụng một ăngten mạnh để gián điệp lưu lượng mạng không dây. Phải thừa nhận rằng chỉ thông qua sử dụng các biện pháp mật mã mạnh mới có thể giải quyết tốt vấn đề an toàn.

2.3.3. Các biện pháp kỹ thuật

Các biện pháp kỹ thuật liên quan đến việc sử dụng các giải pháp phần cứng và phần mềm để giúp đảm bảo an toàn cho môi trường không dây. Các biện pháp phần mềm bao gồm cấu hình AP hoàn chỉnh (ví dụ các thiết lập an toàn và vận hành cho một AP), những sửa chữa và năng cấp phần mềm, xác thực những hệ thống dò xâm nhập IDS (Intrusion Detection System), và mã hoá.. Các giải pháp phần cứng bao gồm smart card, mạng riêng ảo VPN, cơ sở hạ tầng khoá công khai (PKI), và sinh trắc học..

2.3.3.1. Các giải pháp phần mềm

Các biện pháp kỹ thuật liên quan đến phần mềm bao gồm cấu hình hoàn chỉnh cho các AP, phần mềm cập nhật thường xuyên, thực thi xác thực và những giải pháp IDS, thực thi việc kiểm tra an toàn, và sử dụng mật mã hiệu quả.

*** Cấu hình AP**

Những nhà quản trị mạng cần cấu hình AP phù hợp với những chính sách và những yêu cầu an ninh được thiết lập. Cấu hình hoàn chỉnh những mật khẩu quản trị, các thiết đặt mật mã, chức năng khởi tạo, chức năng kết nối mạng tự động. Danh sách điều khiển truy cập MAC Ethernet, các khoá chia sẻ, và các tác tử giao thức quản lý mạng đơn giản (tác tử SNMP - Simple Network Management Protocol) sẽ giúp loại bỏ nhiều lỗ hổng vốn có trong một cấu hình ngầm định phần mềm của nhà sản xuất.

- Cập nhật những mật khẩu ngầm định: mỗi một thiết bị WLAN đều đi kèm với những thiết lập ngầm định của chính nó, một số trong chúng vốn chứa những lỗ hổng an toàn. Mật khẩu của nhà quản trị là một ví dụ điển hình. Ở một số AP, cấu hình ngầm định của nhà sản xuất không yêu cầu mật khẩu

ví dụ để trống trường mật khẩu). Những người sử dụng không được quyền có thể dễ dàng giành quyền truy cập tới thiết bị kết nối không dây nếu không có bảo vệ mật khẩu. Những nhà quản trị mạng nên thay đổi những thiết lập ngầm định để phù hợp với chính sách an toàn của công ty, dùng mật khẩu quản trị mạnh (mật khẩu có độ dài ít nhất là 8 ký tự). Một biện pháp thay thế xác thực mật khẩu là xác thực hai nhân tố. Một dạng của xác thực hai nhân tố đó là sử dụng một thuật toán khoá đối xứng để tạo ra một mã mới trong mỗi phút. Mã này là một mã sử dụng một lần đi kèm với số xác minh cá nhân (PIN) dùng để xác thực. Một ví dụ khác của xác thực hai nhân tố đó là cặp smart card của người sử dụng và số Pin của người sử dụng đó. Loại xác thực này yêu cầu một thiết bị phần cứng đọc smart card hoặc một máy chủ xác thực PIN. Nhiều các sản phẩm thương mại có khả năng này. Tuy nhiên, việc sử dụng một bộ tạo mật khẩu tự động hoặc cơ chế xác thực hai nhân tố có thể không đáng đầu tư, phụ thuộc vào những yêu cầu an toàn của một cơ quan, số lượng người sử dụng, và những giới hạn về ngân sách. Đưa ra nhu cầu đảm bảo những chính sách và xác thực mật khẩu tốt, điều quan trọng cần lưu ý tầm quan trọng mang tính tiêu chí của việc đảm bảo rằng giao diện quản lý có bảo vệ mật mã hoàn hảo để ngăn ngừa việc lộ mật khẩu thông qua giao diện quản lý. Một số cơ chế hiện có có thể được triển khai để đảm bảo chắc chắn rằng truy cập được mã hoá bảo vệ những "bí mật tiêu chí đó" trong quá trình truyền. SSH (Secure Shell) [16] và SSL (secure sockets layer) [17] là hai cơ chế như vậy.

- Thiết lập những cài đặt mã hoá hoàn chỉnh: những cài đặt mã hoá nên được thiết lập với mã hoá mạnh nhất sẵn có trong sản phẩm, phụ thuộc vào yêu cầu an toàn của cơ quan. Thông thường, các AP chỉ có một vài thiết đặt mã hoá sẵn có: không, khoá chia sẻ 40 bít, và khoá chia sẻ 104 bít. Chúng ta không cần phải lo lắng về khả năng của bộ xử lý máy tính khi lập kế hoạch sử dụng mã hoá với những khoá mã dài hơn. Tuy nhiên cần lưu ý rằng một số tấn công chống lại WEP tạo ra những kết quả có hại cho kích cỡ khoá. Điều quan

trọng cần lưu ý những sản phẩm sử dụng những khoá 128 bít sẽ không hoạt động được với những sản phẩm sử dụng những khoá 104 bít.

- Kiểm soát chức năng xác lập lại: chức năng xác lập lại đặt ra một vấn đề cụ thể bởi vì nó cho phép một cá nhân phủ nhận bất kỳ thiết lập an toàn nào mà những nhà quản trị đã cấu hình trong AP. Nó thực hiện điều này bằng cách chuyển AP về những thiết lập ngầm định của nhà sản xuất. Những thiết lập ngầm định này thường không yêu cầu một mật khẩu quản trị, và có thể vô hiệu hoá chức năng mã hoá. Một cá nhân có thể xác lập lại cấu hình cho những thiết lập ngầm định đơn giản bằng cách chèn thêm một vật nhọn như là một cái bút chẳng hạn vào trong lỗ xác lập lại và ấn vào đó. Nếu như một người sử dụng có dã tâm giành quyền truy cập vật lý tới thiết bị, cá nhân đó có thể khai thác đặc điểm xác lập lại và xoá bỏ bất kỳ thiết lập an toàn nào trên thiết bị. Chức năng xác lập lại, nếu được cấu hình để xoá bỏ thông tin vận hành cơ bản như địa chỉ IP hay các khoá, có thể tạo ra một tấn công từ chối dịch vụ mạng, bởi vì những AP có thể không hoạt động nếu không có những thiết lập này. Những kiểm soát truy cập vật lý ngăn ngừa người sử dụng không được quyền thực hiện xác lập lại AP có thể giảm bớt những mối nguy. Các cơ quan có thể dò những mối nguy bằng cách thực hiện những kiểm tra an toàn thường xuyên. Ngoài ra, xác lập lại có thể được thực hiện từ xa qua giao diện quản lý trên một số sản phẩm.Vì lý do này, cần phải có quản trị mật khẩu hoàn chỉnh và mã hoá trên giao diện quản lý.

- Sử dụng chức năng MAC ACL (MAC Access Lists): một địa chỉ MAC là một địa chỉ phần cứng xác minh duy nhất cho mỗi máy tính (hoặc thiết bị đi kèm) trên một mạng. Những mạng sử dụng địa chỉ MAC giúp quy định những truyền thông giữa những NIC máy tính khác nhau trên cùng một subnet mạng. Nhiều nhà sản xuất sản phẩm 802.11 cung cấp những khả năng cho việc giới hạn truy cập tới WLAN dựa trên cơ sở những ACL MAC được lưu trữ và phân phối trong nhiều AP. MAC ACL cấp phát hoặc từ chối truy cập tới một máy

tính sử dụng một danh sách những cấp phép được thiết kế bởi địa chỉ MAC. Tuy nhiên, MAC ACL Ethernet không mô tả một cơ chế phòng thủ mạnh. Bởi vì những địa chỉ MAC được truyền dưới dạng rõ từ một NIC không dây tới một AP, MAC này có thể dễ dàng bị lấy trộm. Những người sử dụng ác tâm có thể giả mạo một địa chỉ MAC bằng cách thay đổi địa thỉ MAC thực trên máy tính của họ thành một địa chỉ MAC có quyền truy cập tới mạng không dây. Biện pháp đối phó này có thể cung cấp mức an toàn nào đó; tuy nhiên, người sử dụng nên thận trọng khi sử dụng. Nó có thể có hiệu quả chống lại trộm không có chủ đích nhưng sẽ không hiệu quả chống lại những kẻ thù có dã tâm. Người sử dụng có thể coi biện pháp này như là một phần của chiến lược phòng thủ sâu tổng thể - bổ sung thêm những cấp độ an toàn để giảm bớt nguy cơ. Trong một mạng cỡ vừa đến cỡ lớn, gánh nặng của việc thiết lập và duy trì những MAC ACL có thể vượt quá giá trị của biện pháp đối phó an toàn. Ngoài ra, hầu hết các sản phẩm chỉ hỗ trợ một số giới hạn những địa chỉ MAC trong MAC ACL. Khối lượng danh sách truy cập có thể không đầy đủ cho những mạng vừa đến lớn.

- Thay đổi SSID (service set identifier): SSID của AP phải được thay đổi từ ngầm định nhà máy. Những giá trị ngầm định của SSID được sử dụng bởi nhiều nhà sản xuất WLAN 802.11 đã được công bố. Những giá trị ngầm định nên được thay đổi để ngăn chặn những truy cập dễ dàng. Mặc dù một đối phương được trang bị có thể thu được tham số xác thực qua giao diện không dây, nên thay đổi nó để ngăn ngừa những cố gắng kết nối mạng không dây của đối phương.

- Tối đa khoảng cách báo hiệu (Beacon Interval): Chuẩn 802.11 chỉ ra việc sử dụng các khung báo hiệu (Beacon) để công bố sự tồn tại của một mạng không dây. Những beacon được truyền từ những AP ở những khoảng thời gian nhất định và cho phép một trạm client xác minh và tuân thủ những tham số cấu hình để gia nhập vào mạng không dây. AP có thể được cấu hình để triệt

bỏ việc truyền những khung Beacon và trường SSID bắt buộc của nó. Tuy nhiên, độ dài khoảng thời gian có thể được thiết lập tới giá trị cao nhất. Trong khi việc cải thiện an toàn là phụ, nó không gây thêm khó khăn cho việc tìm một mạng một cách bị động, bởi vì AP đơn giản hơn và SSID không được truyền thường xuyên. Việc sử dụng một khoảng Beacon dài hơn buộc đối phương phải thực hiện những gì được xem như là sử dụng "quýet động" những tin thăm dò (Probe) với một SSID cụ thể. Do vậy, ở những nơi có thể, những mạng không dây nên được cấu hình với khoảng cách beacon dài nhất.

- Vô hiệu hoá tính năng SSID quảng bá: SSID là một phần xác thực đôi khi được xem như là "tên mạng" và thường là một chuỗi ký tự ASCII đơn giản (0 đến 32 byte), trường hợp byte không là một trường hợp đặc biệt được gọi là SSID quảng bá (broadcast SSID). SSID được sử dụng để chỉ định một xác thực cho mạng không dây. Các client muốn gia nhập mạng phải có một SSID. Một client không dây có thể xác định tất cả các mạng trong một vùng bằng việc quýet động những AP có sử dụng những tin yêu cầu thăm dò (Probe Request) truyền với một SSID không. SSID quảng bá thăm dò các nút một trả lời thăm dò (Probe Response) từ tất cả những mạng 802.11 trong vùng. Việc vô hiệu hoá đặc tính SSID quảng bá trong những AP khiến nó bỏ qua tin từ client và thực hiện quýet động (thăm dò bằng một SSID cụ thể).

- Thay đổi khoá mật mã ngầm định: nhà sản xuất có thể cung cấp một hoặc nhiều khoá để tạo khả năng xác thực khoá chia sẻ giữa thiết bị muốn giành quyền truy cập tới mạng và AP. Việc sử dụng thiết lập khoá chia sẻ ngầm định hình thành một lỗ hổng an ninh bởi vì nhiều nhà sản xuất sử dụng những khoá chia sẻ giống nhau trong những thiết lập của họ. Một người sử dụng ác tâm có thể biết khoá chia sẻ ngầm định và sử dụng nó để giành quyền truy cập tới mạng. Việc thay đổi thiết lập khoá chia sẻ ngầm định bằng khoá khác sẽ giảm bớt nguy cơ. Ví dụ, khoá chia sẻ có thể thay đổi thành 954617 thay bằng việc sử dụng một khoá chia sẻ ngầm định của nhà máy là 111111.

Dù ở cấp độ an toàn nào đi chăng nữa, các cơ quan nên thay đổi khoá chia sẻ từ thiết lập ngầm định bởi vì nó dễ dàng bị tìm ra. Nhìn chung, các cơ quan nên chọn những khoá có độ dài lớn nhất (ví dụ 104 bít). Cuối cùng, một nguyên tắc thường được chấp nhận cho việc quản lý khoá hoàn hảo đó là việc thay đổi những khoá mật mã thường xuyên và khi có những thay đổi cá nhân.

- Sử dụng SNMP: một số AP không dây sử dụng những tác tử SNMP, cho phép những công cụ quản lý mạng giám sát tình trạng của những AP không dây và các client không dây. Hai phiên bản đầu tiên của SNMP là SNMPv1 và SNMPv2 chỉ hỗ trợ xác thực bình thường dựa trên cơ sở những chuỗi bản rõ và kết quả về cơ bản là không an toàn. Nếu như trên mạng không yêu cầu SNMP thì cơ quan nên đơn giản vô hiệu hoá SNMP. Nếu như một cơ quan phải sử dụng một phiên bản của SNMP bên cạnh phiên bản 3, thì họ phải thừa nhận và chấp nhận những nguy cơ. Nhận thức thông thường rằng chuỗi SNMP ngầm định mà các tác tử SNMP thường sử dụng là từ "công khai" với những quyền được gán "đọc" hoặc "đọc và ghi". Việc sử dụng chuỗi ngầm định được biết đến này sẽ tạo ra những lỗ hổng cho những thiết bị. Nếu như một người sử dụng không được quyền giành quyền truy cập và có những quyền đọc/ghi, thì người sử dụng đó có thể ghi dữ liệu tới AP, kết quả tạo ra một lỗ hổng toàn vẹn dữ liệu. Các cơ quan yêu cầu SNMP nên thay đổi chuỗi ngầm định thường xuyên khi cần, để tạo chuỗi an toàn. Những đặc quyền nên được thiết lập để "chỉ đọc" nếu như đó chỉ là truy cập một người sử dụng yêu cầu. Những bao gói tin SNMPv1 và SNMPv2 chỉ hỗ trợ xác thực tầm thường dựa trên cơ sở những chuỗi bản rõ và kết quả về cơ bản là không an toàn và không được giới thiệu. Các cơ quan nên sử dụng SNMPv3.

- Thay đổi kênh ngầm định: Một quan tâm khác không được khai thác trực tiếp đó là kênh ngầm định. Những nhà sản xuất thường sử dụng những kênh ngầm định trong những AP của họ. Nếu như hai hay nhiều AP được đặt gần nhau nhưng ở những mạng khác nhau, một tấn công từ chối dịch vụ có thể

được tạo ra từ nhiễu sóng vô tuyến giữa hai AP này. Các cơ quan chịu nhiễu vô tuyến cần xác định xem liệu một hoặc nhiều AP gần nhau đang sử dụng cùng kênh hoặc một kênh trong vòng 5 kênh của chính chúng và sau đó chọn một kênh trong một phạm vi khác. Ví dụ, kênh 1, 6, 11 có thể được sử dụng đồng thời bởi những AP gần nhau không nhiễu lẫn nhau. Các cơ quan phải thực hiện một điều tra vùng để tìm ra bất kỳ nguồn gây nhiễu sóng vô tuyến nào. Đều tra vùng nên tạo ra một bản báo cáo dự kiến về những vị trí đặt AP, xác định vùng phủ sóng và gán những kênh vô tuyến cho mỗi AP.

- Sử dụng DHCP (Dynamic Host Configuration Protocol): Những kết nối mạng tự động liên quan đến việc sử dụng một máy chủ DHCP. Máy chủ DHCP tự động gán những địa chỉ IP cho những thiết bị đi kèm với một AP. Ví dụ, một máy chủ DHCP được sử dụng để quản lý những địa chỉ TCP/IP cho các máy trạm client. Sau khi thiết lập các địa chỉ IP, máy chủ DHCP tự động gán những địa chỉ này cho các máy trạm khi cần. Máy chủ này gán cho thiết bị một địa chỉ IP động khi những thiết lập mã hoá tương thích với WLAN. Mối đe doạ với DHCP đó là một người sử dụng ác ý có thể dễ dàng giành quyền truy cập mạng thông qua việc sử dụng một máy tính có card không dây. Bởi vì một máy chủ DHCP sẽ không cần thiết biết những thiết bị không dây nào có quyền truy cập, máy chủ sẽ tự động gán cho máy tính một địa chỉ IP hợp lệ. Việc giảm bớt nguy cơ liên quan đến việc vô hiệu hoá DHCP và sử dụng những địa chỉ IP tĩnh cho mạng không dây nếu khả thi.

Phương pháp an toàn này, giống như biện pháp đối phó MAC ACL, chỉ có thể dùng được cho những mạng nhỏ. Việc gán địa chỉ IP tĩnh cũng sẽ phủ nhận một số ưu điểm chính của các mạng không dây, như roaming và thiết lập mạng tự do. Giải pháp khác là thực thi tường lửa của mạng có dây, sử dụng những AP với những tường lửa kết hợp. Giải pháp này sẽ bổ sung thêm tầng bảo vệ cho toàn mạng. Tất cả những người sử dụng nên đánh giá nhu cầu DHCP dựa vào kích cỡ mạng của họ.

*** Những cập nhật và nâng cấp phần mềm**

Những nhà sản xuất thường cố gắng sửa chữa những lỗ hổng an toàn phần mềm khi phát hiện ra chúng. Những sửa chữa này được thực hiện dưới dạng những nâng cấp và sửa chữa an toàn. Những nhà quản trị mạng cần kiểm tra thường xuyên với nhà sản xuất để xem liệu những nâng cấp và sửa chữa an toàn có sẵn sàng không và áp dụng chúng khi cần. Cũng vậy, nhiều nhà sản xuất có những danh sách thư điện tử "cảnh báo an toàn"để đưa ra lời khuyên cho những khách hàng về những lỗ hổng và những tấn công an toàn mới. Những nhà quản trị mạng nên cập nhật những cảnh báo tiêu chí này. Cuối cùng, những nhà quản trị mạng có thể kiểm tra bằng cơ sở dữ liệu lỗ hổng NIST ICAT, liệt kê tất cả những lỗ hổng được biết đến trong phần cứng và phần mềm đang được thực hiện.

Một ví dụ về nâng cấp phần mềm là tăng cường an toàn WEP với an toàn RSA. Tháng 11/2001, tổ chức an toàn RSA đã phát triển một kỹ thuật xử lý những lỗ hổng an toàn được tìm thấy trong WEP [18]. Tăng cường này, được xem như là "fast packet keying", tạo ra một khoá duy nhất để mã hoá mỗi gói mạng trên WLAN. Giải pháp Fast Packet Keying sử dụng một kỹ thuật băm tạo một cách nhanh chóng trên mỗi khoá gói. IEEE đã thông qua kỹ thuật fast packet keying như là một kỹ thuật cố định cho giao thức 802.11. Các nhà sản xuất đã bắt đầu áp dụng kỹ thuật này cho những sản phẩm không dây mới và đã phát triển những sửa chữa phần mềm cho nhiều sản phẩm đang có. Các cơ quan nên kiểm tra xem những nâng cấp phần mềm đã sẵn có cho những sản phẩm mà họ đã mua chưa.

Một ví dụ nâng cấp phần mềm khác đó là WPA (Wi-Fi Protected Acess). WPA, được phát triển bởi WiFi Alliance, là một giải pháp an toàn tạm thời không đòi hỏi một nâng cấp phần cứng trong thiết bị 802.11 hiện có. WPA không phải là một giải pháp hoàn hảo mà là một giải pháp tạm thời - để giải quyết một số vấn đề với WEP. WPA gồm hai phần chính:

+ 801.1x.

+ TKIP (Temporal Key Integrity Protocol).

Kiểm soát quyền truy cập dựa trên cơ sở 802.1x cung cấp một khung cho phép sử dụng những giao thức xác thực tầng cao. Nó cũng tạo thuận lợi cho việc sử dụng những khoá phiên-bởi vì những khoá mật mã nên thay đổi thường xuyên. TKIP bao gồm 4 thuật toán mới tăng cường an toàn cho 802.11. TKIP mở rộng không gian véctơ khởi tạo, cho phép xây dựng khoá trên mỗi gói tin, cung cấp tính toàn vẹn mật mã, và cung cấp nguồn khoá và phân phối khoá. TKIP, thông qua những thuật toán này, cung cấp bảo vệ chống lại nhiều tấn công an toàn được đề cập ở trên, gồm những tấn công replay và những tấn công lên tính toàn vẹn dữ liệu. Ngoài ra, nó giải quyết nhu cầu thay đổi khoá. Mục đích của WPA là đem đến giải pháp an toàn dựa trên cơ sở chuẩn thay thế WEP trong khi IEEE 802.11 Task Group i đủ thời gian hoàn chỉnh chuẩn an toàn 802.11i (RSN), một sửa đổi đối với chuẩn WLAN hiện tại. RSN cũng gồm chuẩn mã hoá tăng cường AES cho ta độ tin cậy và tính toàn vẹn. Giải pháp RSN sẽ đòi hỏi những thay thế phần cứng.

*** Xác thực**

Nhìn chung, những giải pháp xác thực hiệu quả là một cách tin cậy cho phép chỉ những người sử dụng được quyền mới có thể truy cập tới mạng. Những giải pháp xác thực bao gồm việc sử dụng username và mật khẩu; smart card, sinh trắc học, hay PKI; hoặc kết hợp của những giải pháp đó (ví dụ smart card với PKI). Khi dựa vào username và mật khẩu cho xác thực, quan trọng là phải có những chính sách xác định độ dài mật khẩu tối thiểu, những ký tự mật khẩu yêu cầu, và thời hạn mật khẩu. Thẻ thông minh (Smart card), sinh trắc học, và PKI cho những đòi hỏi riêng của chính nó.

Tất cả các cơ quan nên thực thi một chính sách mật khẩu mạnh, tập trung vào mức độ an toàn của những hoạt động của họ. Những mật khẩu mạnh đơn giản là một phép đo cơ bản trong bất kỳ môi trường nào. Các cơ quan

cũng nên xem xét những cơ chế xác thực khác (ví dụ như smart card với PKI). Những cơ chế này có thể kết hợp vào một giải pháp WLAN để tăng cường an toàn cho hệ thống. Tuy nhiên, những người sử dụng nên cẩn trọng để hiểu một cách đầy đủ vấn đề an toàn được quy định bởi xác thực tăng cường. Nó không phải là một giải pháp để giải quyết mọi vấn đề. Ví dụ một mật khẩu mạnh được sử dụng cho những tham số truy cập lên một NIC không có tác dụng giải quyết những vấn đề với mật mã WEP.

*** Những tường lửa cá nhân**

Các tài nguyên trên những mạng không dây có nguy cơ bị tấn công cao hơn bởi vì chúng thường không có mức độ bảo vệ tương tự như những tài nguyên nội bộ. Tường lửa cá nhân cho phép chống chọi với một số những tấn công nhất định. Tường lửa cá nhân là những giải pháp dựa trên cơ sở phần mềm được cài vào máy của client và được quản lý ở tại client đó và ở cả trung tâm. Những phiên bản do client quản lý là phù hợp nhất cho người sử dụng bởi vì họ có thể tự cấu hình tường lửa và có thể không tuân theo bất kỳ những hướng dẫn an toàn cụ thể nào. Những giải pháp quản lý trung tâm cung cấp mức độ bảo vệ lớn hơn bởi những phòng công nghệ thông tin cấu hình và quản lý chúng từ xa. Các giải pháp quản lý trung tâm cho phép những tổ chức thay đổi tường lửa của client để chống lại những lỗ hổng an toàn đã biết và để duy trì một chính sách an toàn cố định cho tất cả những người sử dụng từ xa. Một số những sản phẩm cũng có những khả năng VPN và kiểm tra. Mặc dù tường lửa cá nhân đưa ra biện pháp bảo vệ nào đó, nhưng chúng không bảo vệ được trước những dạng tấn công tiên tiến. Phụ thuộc vào yêu cầu an toàn, các cơ quan vẫn có thể cần thêm những tầng bảo vệ. Người sử dụng truy cập vào những mạng công cộng ở các sân bay hay các trung tâm hội nghị chẳng hạn, nên sử dụng một tường lửa cá nhân. Những tường lửa cá nhân cũng cung cấp thêm biện pháp bảo vệ chống lại những AP giả mạo có thể dễ dàng cài đặt trong những nơi công cộng như thế.

*** Hệ thống dò tấn công IDS**

Một hệ thống dò tấn công IDS là một công cụ hiệu quả để xác định liệu những người sử dụng không được quyền đang cố gắng truy cập, đã truy cập, hoặc đã xâm nhập vào mạng. IDS dùng cho những WLAN có thể là IDS dựa trên cơ sở máy chủ, dựa trên cơ sở mạng hoặc kết hợp các đặc điểm của IDS dựa trên cơ sở máy chủ và dựa trên cơ sở mạng. Một IDS dựa trên cơ sở máy chủ bổ sung một tầng mục tiêu an toàn tới những hệ thống quan trọng hoặc những hệ thống có lỗ hổng. Một tác tử dựa trên cơ sở máy chủ được cài đặt trên một hệ thống cá nhân (ví dụ, một máy chủ cơ sở dữ liệu) và theo dõi những vết kiểm tra và những đăng nhập hệ thống có hành vi khả nghi, như những cố gắng đăng nhập lặp đi lặp lại nhưng thất bại hoặc những thay đổi tới những cấp phép file. Tác tử cũng có thể triển khai một tổng kiểm tra ở những khoảng thời gian cách đều nhau để tìm kiếm những thay đổi tới những file hệ thống. Trong một số trường hợp, một tác tử có thể ngăn cản một tấn công lên một hệ thống, mặc dù một chức năng đầu tiên của tác tử máy chủ là đăng nhập và phân tích những sự kiện và gửi những cảnh báo. Một IDS dựa trên cơ sở mạng giám sát lưu lượng mạng LAN (hoặc một segment LAN), từng gói tin, trong thời gian thực (hoặc càng gần thời gian thực càng tốt) để xác định xem liệu lưu lượng có thích nghi với những dấu hiệu tấn công được xác định trước (những hành động phù hợp với những kiểu tấn công được biết). Ví dụ, tấn công từ chối dịch vụ TearDrop gửi những gói tin được chia thành nhiều đoạn dưới dạng đổ xô vào hệ thống mục tiêu. Giám sát mạng sẽ công nhận những gói tin phù hợp với đối tượng này và hành động như đang phá huỷ phiên mạng, gửi một thư điện tử cảnh báo tới nhà quản trị, hoặc hành động khác được chỉ định. Những hệ thống dựa trên cơ sở máy chủ có ưu điểm hơn so với IDS dựa trên cơ sở mạng khi những liên kết mã hoá - ví dụ những phiên Web SSL hay những liên kết trên VPN - được kết hợp. Do tác tử cư trú trên chính thành phần này, nên hệ thống dựa trên cơ sở máy chủ có thể kiểm tra dữ liệu

sau khi nó được giải mã. Ngược lại, một IDS dựa trên cơ sở mạng không thể giải mã dữ liệu, do đó, lưu lượng mạng được mã hoá được thông qua mà không cần điều tra.

Công nghệ IDS trên những mạng có dây có thể có những giới hạn sau đây nếu được sử dụng để bảo vệ những mạng không dây.

- Bộ cảm biến IDS dựa trên cơ sở mạng có thể được đặt trên mạng có dây đằng sau AP không dây sẽ không dò những tấn công định hướng từ một client không dây tới một client không dây khác (ví dụ điểm-điểm) trên cùng một mạng con. AP không dây liên kết lưu lượng trực tiếp giữa các client không dây. Lưu lượng này không gia nhập vào mạng có dây, nó được mã hoá WEP, và những bộ cảm biến IDS mạng có dây không có một cơ hội nào để thu được những gói tin bản rõ. Kết quả, một đối phương kết nối thành công tới một client không dây không được quyền tới mạng này có thể thực hiện việc khôi phục và tấn công chống lại những máy chủ không dây khác mà không cần dò bởi bộ cảm biến IDS dựa trên cơ sở mạng. Trong trường hợp này, dữ liệu trên những client không dây khác sẽ gặp nguy hiểm và thông tin được tập hợp từ những client khác có thể được sử dụng để tạo ra một tấn công lên mạng có dây.

- Những bộ cảm biến IDS trên mạng có dây thường sẽ không dò những cố gắng tới một client hợp pháp từ mạng không dây và sẽ không dò kết hợp của một client không dây không được quyền với mạng không dây. Tắc nghẽn, ngập lụt và những tấn công từ chối dịch vụ khác chống lại những thiết bị không dây sử dụng những kỹ thuật tầng liên kết dữ liệu và kỹ thuật vật lý mà bộ cảm biến IDS không nhìn thấy ở một mức gói tin và thường sẽ không phá bỏ được trên mạng có dây.

- Công nghệ IDS cho những mạng có dây thường chỉ dò những tấn công khi những gói tin được dò ở những máy chủ trên mạng có dây từ một client không dây. Ở điểm đó, mạng không dây đã được kết hợp, và nguy cơ tới mạng

có dây là sắp xảy ra. Một mục tiêu quan trọng là dò và gửi một cảnh báo lên hoạt động không dây không được quyền trước khi nó ảnh hưởng tới mạng có dây.

- Công nghệ IDS trên những mạng có dây sẽ không xác minh vị trí vật lý của những AP giả mạo trong toà nhà. Những AP giả mạo này có thể hành động như những điểm vào cho truy cập không dây không được quyền từ những vị trí từ xa..

- Công nghệ IDS sẽ không dò một thiết bị không dây được quyền truyền thông peer to peer với một thiết bị không dây không được quyền. Trường hợp này có thể tạo ra một cầu nối vào trong mạng có dây bằng cách cho phép đối phương kết nối tới một thiết bị không dây đang hoạt động trong chế độ "tự do". Chế độ tự do cho phép một thiết bị không dây được sử dụng để tiếp sóng lưu lượng tới mạng đó và tạo ra một số tấn công tiềm ẩn.

Việc mở rộng một mạng có dây bằng cách kết nối một hoặc nhiều mạng không dây thường mở rộng vành đai an toàn của mạng này và tạo ra nguy cơ không thể được giải quyết bởi những thiết bị dò tấn công hiện có trên mạng có dây. Các cơ quan muốn mở rộng chức năng mạng bằng cách bổ sung thêm một mạng không dây nên kiểm tra kiến trúc IDS hiện có và xem xét những giải pháp bổ sung để giải quyết những nguy cơ được đề cập ở trên. Các cơ quan nên xem xét thực thi một giải pháp IDS không dây nhằm cung cấp những khả năng sau:

- Xác minh vị trí vật lý của những thiết bị không dây trong phạm vi toà nhà.

- Dò những truyền thông peer to peer không được quyền trong mạng không dây mà không thấy trong mạng có dây.

- Phân tích những truyền thông không dây và giám sát không gian tần số vô tuyến 802.11 và việc tạo một cảnh báo đối với việc dò những thay đổi

cấu hình không được quyền đối với những thiết bị không dây vi phạm chính sách an toàn.

- Dò flooding trước khi chúng xâm nhập thành công vào mạng không dây.

- Cung cấp những đặc tính giám sát và quản lý với những tích hợp tiềm năng vào trong phần mềm thông báo và giám sát IDS hiện có để tạo ra một cái nhìn vững chắc về tình trạng an toàn mạng không dây và có dây.

Các cơ quan yêu cầu những mức độ an toàn cao nên xem xét việc triển khai một IDS bởi vì nó cung cấp một tầng an toàn bổ sung. Các cơ quan hiện triển khai IDS nên xem xét việc bổ sung những khả năng trên để bổ sung cho những khả năng hiện có của chúng. Việc triển khai IDS đương nhiên tốn phí và nên được xem xét nếu phù hợp về tài chính. Ngoài ra, đối với chi phí của chính hệ thống, một IDS yêu cầu cá nhân có kinh nghiệm giám sát và trả lời những sự kiện IDS và cung cấp quản trị chung cho cơ sở dữ liệu và những thành phần ID. Các cơ quan cũng nên xem xét sử dụng một động cơ liên quan, nhận được những sự kiện an toàn thời gian thực chuẩn từ những bộ cảm biến khác nhau, như IDS, tường lửa, và những hệ thống chống vi rút. Những động cơ tương quan kết hợp trong thời gian thực và phân tích nhiều mối đe doạ. Những mối đe doạ này có thể bao gồm nhiều lớp tấn công, như những tấn công từ chối dịch vụ phân tán DDoS (Distributed DoS).

*** Mã hoá**

Như đã đề cập trước đó, các AP thường chỉ có 3 thiết đặt mã hoá sẵn có: không, khoá chia sẻ 40 bít và 104 bít. Thiết đặt không thể hiện nguy cơ nghiêm trọng nhất bởi vì dữ liệu không được mã hóa truyền trên mạng có thể dễ dàng bị thu chặn, đọc và bị thay đổi nội dung. Một khoá chia sẻ 40 bít sẽ mã hoá dữ liệu truyền thông trên mạng, nhưng vẫn có nguy cơ không an toàn. Mã hoá 40 bít đã bị phá bởi thám mã bắt ép thô bạo sử dụng một máy tính đồ hoạ cao cấp và thậm chí là những máy tính thấp cấp. Nhìn chung, mã hoá 104

bít an toàn hơn mã hoá 40 bít bởi vì sự khác nhau về kích cỡ không gian khoá mật mã. Mặc dù điều này không đúng với WEP 802.11 bởi vì nó có thiết kế mật mã nghèo nàn sử dụng những vectơ khởi tạo.

*** Những đánh giá an toàn**

Những đánh giá an toàn, hoặc những kiểm tra, là một công cụ quan trọng kiểm tra tình hình an toàn của mạng WLAN và xác định hành động sửa chữa nhằm đảm bảo rằng nó vẫn an toàn. Điều quan trọng đối với các cơ quan đó là thực hiện kiểm tra thường xuyên sử dụng những phân tích mạng không dây và những công cụ khác. Một bộ phân tích, đôi khi được gọi là một bộ giám sát mạng là một công cụ hiệu quả để thực hiện những kiểm tra an toàn và xử lý những vấn đề mạng không dây. Những nhà quản trị an toàn và những nhà kiểm tra an toàn có thể sử dụng những bộ phân tích mạng để xác định xem liệu những sản phẩm đang truyền chính xác và trên những kênh đúng. Những nhà quản trị mạng nên kiểm tra định kỳ trong không gian toà nhà văn phòng để phát hiện những AP giả mạo và những truy cập không được quyền khác. Các cơ quan cũng có thể xem xét việc sử dụng đối tượng thứ 3 độc lập để thực hiện những kiểm tra an ninh. Những cố vấn an toàn đối tượng thứ 3 độc lập thường là những lỗ hổng an toàn được cập nhật nhiều hơn, được đào tạo tốt hơn về những giải pháp an toàn, và được trang bị để đạt được tính an toàn cho mạng không dây. Một kiểm tra đối tượng thứ 3 độc lập, có thể bao gồm việc kiểm tra sự thâm nhập, sẽ giúp một cơ quan đảm bảo chắc rằng WLAN của nó tương thích với những thủ tục và những chính sách an toàn đã được thiết lập và hệ thống đó được cập nhật với những sửa chữa và nâng cấp phần mềm mới nhất.

2.2.3.2. Các giải pháp phần cứng

Các biện pháp đối phó phần cứng để giảm bớt nguy cơ WLAN gồm thực thi những smart card, mạng riêng ảo VPN, PKI, sinh trắc học, và những giải pháp phần cứng khác.

*** Smart card**

Smart card có thể bổ sung thêm mức độ an toàn, mặc dù chúng cũng bổ sung thêm sự phức tạp. Các cơ quan có thể sử dụng smart card kết hợp với username và mật khẩu. Xác thực người sử dụng và thông tin khác được lưu trữ trên những card này và thường yêu cầu người sử dụng chỉ cần nhớ một số PIN. Smart card cũng có thể cầm tay; người sử dụng có thể truy cập an toàn mạng của họ ở những vị trí khác nhau. Giống như giải pháp xác thực phần mềm, những thiết bị chống nhiễu có thể được tích hợp vào một giải pháp WLAN để tăng cường an toàn cho hệ thống. Người sử dụng nên hiểu một cách đầy đủ vấn đề an toàn được cung cấp bởi giải pháp smart card.

*** Cơ sở hạ tầng khoá công khai PKI (Public Key Infrastructure)**

PKI cung cấp khung và những dịch vụ cho việc tạo, sản xuất, phân phối, kiểm soát và tính toán những xác minh khoá công khai. Nó cung cấp những ứng dụng với mã hoá và xác thực an toàn cho những giao dịch mạng cũng như tính toàn vẹn dữ liệu và không thừa nhận, sử dụng những xác minh khoá công khai để thực thi những tác vụ đó. WLAN có thể kết hợp PKI cho xác thực và an toàn những giao dịch mạng. Những nhà sản xuất đối tượng thứ 3, ví dụ, cung cấp PKI không dây, những máy thu phát không dây, smart card kết hợp với WLAN.

Người sử dụng yêu cầu những mức an toàn cao nên chú ý tới PKI. Nó cung cấp xác thực mạnh thông qua xác minh người sử dụng, có thể được sử dụng với an toàn mức ứng dụng, để ký và mã hoá tin. Smart card thậm chí cung cấp tiện ích lớn hơn bởi vì những xác minh được kết hợp vào card. Smart card phục vụ như là một phương tiện an toàn và lưu những uỷ nhiệm mật mã. Người sử dụng yêu cầu những mức an toàn thấp, cần phải xem xét cẩn thận tính phức tạp và chi phí cho việc thực thi và quản trị một PKI trước khi sử dụng giải pháp này.

*** Sinh trắc học**

Những thiết bị sinh trắc học gồm những máy quýet dấu vân tay, máy quýet quang (gồm máy quýet tròng mắt và võng mạc), máy quýet nhận dạng khuôn mặt và máy quýet nhận dạng giọng nói. Sinh trắc học cung cấp một tầng bảo vệ bổ sung khi được sử dụng độc lập hoặc cùng với những giải pháp an toàn khác. Ví dụ, đối với những cơ quan cần những mức an toàn cao, sinh trắc học có thể được kết hợp với những smart card không dây hoặc những máy tính xách tay không dây và những thiết bị không dây khác và được sử dụng thay cho username và mật khẩu để truy cập tới mạng không dây. Ngoài ra, sinh trắc học có thể kết hợp với những giải pháp VPN để cung cấp tính xác thực và tính tin cậy dữ liệu.

2.2.4. Những chuẩn và những công nghệ an toàn WLAN tiên tiến hiện nay

Tổ chức IEEE hiện nay đang làm việc theo 3 nhóm tách rời với mục đích cải thiện an toàn WLAN. Nhóm thứ nhất liên quan đến IEEE 802.11 TGi đã đưa ra những thay đổi quan trọng đối với chuẩn 802.11 IEEE hiện tại như là một giải pháp an toàn lâu dài. TGi xác định những mã bổ sung dựa trên cơ sở AES. Giải pháp dựa trên cơ sở AES sẽ cung cấp một biện pháp an toàn mạnh cho tương lai tuy nhiên sẽ yêu cầu những thay đổi về giao thức và phần cứng. Hiện tại TGi đã thiết kế những yêu cầu để giải quyết nhiều vấn đề trong WEP bao gồm ngăn ngừa những giả mạo và dò những tấn công dùng lại.

Nhóm thứ hai cải thiện an toàn cho WLAN bằng giải pháp ngắn hạn TGi-WPA (WiFi Protected Acess)-để giải quyết những vấn đề của WEP. Nhóm này định nghĩa giao thức TKIP (Temporal Key Integrity) dùng để giải quyết những vấn đề an toàn trong WEP mà không yêu cầu những thay đổi phần cứng - chỉ yêu cầu những thay đổi driver phần mềm. Nhóm thứ 3 giới thiệu một chuẩn mới, IEEE 802.11x-2001, một khung chung cho truy cập mạng dựa trên cơ sở cổng và phân phối khoá, được thông qua vào tháng 6 năm

2001. Bằng việc xác định một bao gói của EAP (được xác định trong RFC 2284) qua môi trường 802 IEEE, IEEE 802.1x cho phép AP và trạm xác thực lẫn nhau .

Vì 801.1x IEEE ban đầu được pháp triển cho sử dụng với những LAN 802 IEEE, không phải cho sử dụng với WLAN, chuẩn phác thảo 802.11i IEEE xác định những khả năng bổ sung yêu cầu cho thực thi an toàn của 802.1x IEEE trên những mạng 802.11. Những khả năng này bao gồm yêu cầu sử dụng một phương pháp EAP hỗ trợ xác thực lẫn nhau, quản lý khoá, và chống lại tấn công từ điển. Ngoài ra, 802.1i xác định hệ đẳng cấp cho việc sử dụng những mã TKIP và AES và một bắt tay quản lý khoá "bốn chiều" được sử dụng để đảm bảo chắc chắn rằng trạm được xác thực cho AP và một máy thủ xác thực back – end.

IEEE 802.1x có thể được thực hiện toàn bộ trên AP (bằng việc cung cấp hỗ trợ một hoặc nhiều phương pháp EAP trong AP), hoặc nó có thể sử dụng một máy chủ xác thực backend. Chuẩn 802.1x IEEE hỗ trợ những giao thức xác thực như RADIUS, Diameter [19], và Kerberos [20], RADIUS được mô tả trong RFC 2865-2869, và RFC 3162, cho phép xác thực, cấp quyền, và kiểm tra những thiết bị máy chủ truy cập mạng NAS (Network Access Server), gồm quay số, xDSL, và 802.11.

Chuẩn 802.1x có thể được thực hiện với nhiều kiểu EAP (Extensible Authentication Protocol) khác nhau, gồm EAP-MD5 (Extensible Authentication Protocol-Message Digest 5) (được xác định trong RFC 2284 và chỉ hỗ trợ xác thực một chiều không có trao đổi khoá) cho những LAN Ethernet và EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) (được xác định trong RFC 2716, hỗ trợ tái kết nối nhanh, xác thực lẫn nhau và quản lý khoá thông qua chứng thực số). Hiện nay một thế hệ mới của các phương pháp EAP đang được pháp triển ở IETF, tập trung giải quyết những vấn đề xác thực và quản lý khoá không dây. Những phương pháp này

hỗ trợ những đặc tính an toàn bổ sung như bảo vệ mật mã truyền tin EAP, bảo vệ xác minh, thương thuyết mã hoá an toàn, tạo những phương pháp EAP khác nhau.

CHƯƠNG 3. MỘT SỐ BIỆN PHÁP AN TOÀN WLAN THÔNG DỤNG

3.1. Đánh giá chung về các biện pháp an toàn WLAN

Công nghệ WLAN lần đầu tiên xuất hiện vào giữa những năm 1980 khi ECC (Federal Communications Commission) cho phép sử dụng phổ tần số vô tuyến (RF-Radio Frequency) trong WLAN. Vào năm 1990, IEEE (Institute of Electrical and Electronics Engineers) xây dựng một nhóm làm việc để phát triển một chuẩn không dây với mục đích cung cấp cho công nghệ mạng cục bộ không dây tương tự như Ethernet có dây (802.3). Nhóm làm việc này tập trung vào việc phát triển một chuẩn chung cho thiết bị và các mạng vô tuyến làm việc ở dải tần 2.4 GHz, với tốc độ truy cập 1 và 2 Mbps. Vào tháng 6/1997, IEEE đã công bố chuẩn không dây mô tả những hoạt động cho WLAN, được biết đến là 802.11. 802.11 là chuẩn cơ bản cho WLAN. Chuẩn mới này định nghĩa những chức năng và những công nghệ sau cho WLAN:

- Kiến trúc WLAN.

- Những dịch vụ tầng MAC như kết hợp, tái kết hợp, xác thực và riêng tư, những định dạng khung, những chức năng tín hiệu..

- Thuật toán WEP.

Tháng 9/1999, IEEE thông qua 802.11b cung cấp kiến trúc, những đặc tính và dịch vụ cơ bản tương tự như 802.11, tuy nhiên nó cải tiến chuẩn 802.11 bằng việc bổ sung thêm những tốc độ dữ liệu cao hơn (5.5 và 11 Mbps) và kết nối mạnh hơn. Chuẩn 802.11b thiết lập những hoạt động trong phạm vi tần số không cấp phép 2.4-2.5 GHz sử dụng công nghệ trải phổ chuỗi trực tiếp DSSS (direct sequence spread-spectrum).

Cuối năm 2001, 802.11a được thông qua và đã cải tiến tốc độ truyền lên đến 54 Mbps, hoạt động ở dải tần cấp phép 5GHz, và sử dụng công nghệ đa phân chia theo tần số trực giao OFDM để giảm nhiễu. Đây là một sự thay đổi công nghệ ấn tượng so với 802.11b cung cấp tốc độ truyền dữ liệu nhanh ở

phạm vi tần số cao hơn không dễ bị nhiễu từ các thiết bị khác. Tuy nhiên, chuẩn 802.11a có phạm vi hoạt động giảm hơn so với 802.11b.

Vào năm 2003, IEEE công bố 802.11g sửa đổi lần thứ 4 cung cấp tốc độ truyền dữ liệu cao hơn lên đến 54 Mbps (tương tự như 802.11a), hoạt động ở dải tần không cấp phép 2.4 GHz. Nó cung cấp tương thích trở lại với 802.11b, bằng việc vẫn hỗ trợ điều chế CCK (complimentary code key). 802.11g cung cấp tốc độ cao hơn, và triển khai những công nghệ OFDM như 802.11a, tuy nhiên ở những dải tần 2.4 GHz ở đó phạm vi hoạt động không bị tổn hại (như 802.11b).

Những chuẩn IEEE đề cập ở trên (802.11a, 802.11b, 802.11g) phục vụ như những chuẩn chính trong thế giới mạng không giây. Tuy nhiên, có những chuẩn khác liên quan đến việc thúc đẩy chức năng chung của giao thức 802.11. Hai chuẩn quan trọng giải quyết trực tiếp những giới hạn an toàn trong những giao thức 802.11 là chuẩn 802.11i và 802.1x. IEEE TGi đã phát triển chuẩn 802.11i, công bố năm 2004, cung cấp những giải pháp ngắn hạn và lâu dài cho an toàn WLAN để đảm bảo độ tin cậy thông tin và toàn vẹn thông tin. TGi đã phát triển TKIP (Temporal Key Integrity Protocol) như là một giải pháp ngắn hạn, được biết đến là WPA, để giải quyết những vấn đề tồn tại với WEP và hỗ trợ những hệ thống kế thừa. Nó gồm 3 giao thức: một thuật toán xác thực tin mật mã, một thuật toán trộn khoá, và một tăng cường cho IV. Giải pháp lâu dài được xác định trong 802.11i là giao thức CCMP (Counter Mode/CBC-MAC Protocol) dựa trên cơ sở AES (Advanced Encryption Standard) được công bố mới. CCMP là một giải thuật mạnh không tương thích với phần cứng vận hành theo WEP trước đó, do vậy sẽ yêu cầu những thay đổi giao thức và phần cứng mới. Giao thức AES (CCMP) cung cấp cho WLAN khả năng mã hoá và toàn vẹn tin mạnh hơn TKIP. Nó cũng bảo vệ trước những tấn công dùng lại. Tương lai của những triển khai WLAN hướng theo CCMP như là một chuẩn tương thích được chấp nhận.

Công nghệ 802.1x lúc đầu được phát triển để hỗ trợ những LAN 802, và được bao hàm trong chuẩn 802.11i để cung cấp những tăng cường an toàn tầng MAC. 802.1x là một thuật toán xác thực cổng cung cấp một khung ở tầng liên kết cho phép nhiều thuật toán xác thực hoạt động qua nó. Nó sử dụng giao thức xác thực tăng cường EAP (Extensible Authentication Protocol) để trao đổi thông tin xác thực với một máy chủ xác thực nhằm hợp thức hoá những xác minh của họ, và hỗ trợ xác thực lẫn nhau và quản lý khoá mạnh.

Trong những WLAN, khung 802.1x bao gồm 3 thực thể: client, bộ phận xác thực (AP) và bộ phận máy chủ xác thực hay AS (RADIUS). Giao thức 802.1x là một xử lý xác thực truyền thông end to end giữa client và AS, với AP phục vụ như ống dẫn cho những tin xác thực. Client và AP truyền thông bằng giao thức EAPOL (EAP encapsulation over LAN (EAPOL). AP và AS truyền thông thông qua RADIUS. Lưu ý rằng giao thức 802.1x hỗ trợ nhiều giao thức xác thực khác nhau ngoài RADIUS như Diameter, và Kerberos. 802.1x có thể được thực thi với những kiểu EAP khác nhau.

Chuẩn 802.11i ban đầu đưa ra một phương pháp ngắn hạn tăng cường an toàn cho WLAN đó là WPA (Wi-Fi Protected Access). WPA được phát triển bởi Wi-Fi Alliance. WPA giúp giải quyết những vấn đề an toàn yếu kém trong WEP. Giải pháp WPA yêu cầu những cập nhật phần mềm (không yêu cầu phần cứng). WPA sử dụng TKIP với MIC (Message Integrity Check) cho mã hoá. Nó cung cấp xác thực lẫn nhau bằng cách sử dụng công nghệ khoá chia sẻ trước PSK (pre-shared key) và xác thực 802.1x/EAP. Trong môi trường doanh nghiệp lớn, WPA cung cấp một mức độ tin cậy cao và xác thực cho tất cả những người sử dụng không dây khi được triển khai với một máy chủ RADIUS và cơ sở dữ liệu. WPA đưa ra hai lớp xác minh: một WPA doanh nghiệp và một WPA cá nhân.

Wi-Fi Alliance công bố WPA2 vào tháng 9 năm 2004, kết hợp với thực thi đầy đủ của 802.11i. WPA2 cung cấp những sửa đổi chính về những cơ chế

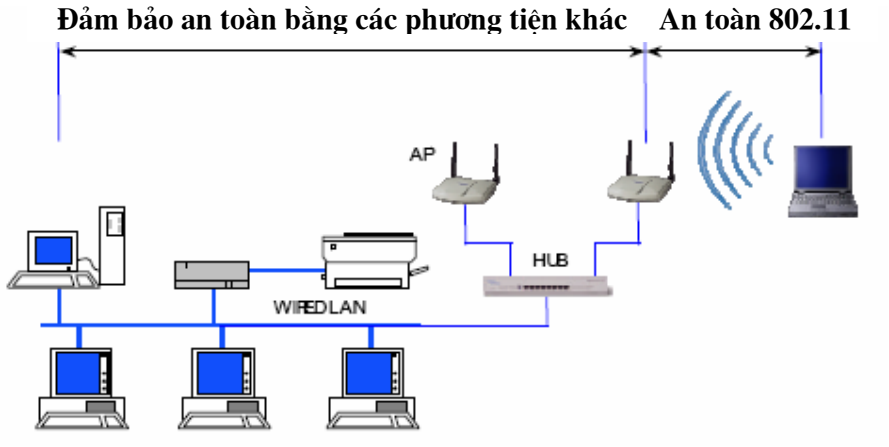
quản lý khoá, mã hoá và tiền xác thực. WPA2 khác WPA ở chỗ nó cung cấp một cơ chế mã hoá mạnh hơn thông qua CCMP sử dụng chuẩn mã hoá AES. Nó tương tự như WPA ở chỗ nó vẫn sử dụng 802.1x và EAP cho xác thực. Tương tự như WPA, WPA2 đưa ra hai chế độ hoạt động: một chế độ cá nhân và một chế độ doanh nghiệp. WPA2 cũng tạo những khoá phiên mới trên mỗi kết hợp. Điều này cung cấp một lợi ích an toàn bổ sung bằng cách đưa ra những khoá mã hoá mới, duy nhất cho một client cụ thể, và tránh dùng lại khoá. WPA2 không giải quyết bất kỳ những lỗ hổng nào trong WPA, tuy nhiên, nó cung cấp một giải pháp an toàn AES tạo điều kiện cho các cơ quan chính phủ hay các tập đoàn có thể triển khai WLAN. Những sản phẩm xác minh WPA2 tương thích trở lại với WPA. Việc cập nhật WPA2 có thể yêu cầu những cập nhật phần cứng mới do nó triển khai AES.

3.2. Biện pháp an toàn WEP

WLAN vốn không phải là một mạng an toàn, tuy nhiên ngay cả với LAN hữu tuyến, nếu chúng ta không có biện pháp bảo mật tốt thì nó cũng không bao giờ an toàn. Chìa khoá mở ra sự an toàn cho WLAN và giữ nó được an toàn là sự thực hiện và quản lý nó. Đào tạo người quản trị một cách căn bản, trên những công nghệ tiên tiến là cách quan trọng để tạo sự an toàn cho WLAN. Phần này, sẽ đề cập đến biện pháp bảo mật theo chuẩn 802.11 đã biết, WEP (Wired Equivalent Privacy). Bản thân WEP không phải là ngôn ngữ bảo mật duy nhất, một mình WEP không thể đảm bảo an toàn tuyệt đối cho WLAN. Vì vậy, cần xem xét tại sao có sự hạn chế trong bảo mật của WEP, phạm vi ứng dụng của WEP, và các biện pháp khắc phục.

3.2.1. Cơ chế an toàn WEP

Những dịch vụ an toàn trong chuẩn 802.11 được quy định phần lớn bởi giao thức WEP để bảo vệ dữ liệu ở mức liên kết trong quá trình truyền không dây giữa các client và AP. WEP không cung cấp an toàn end to end, mà chỉ an toàn cho phần liên kết không dây như minh hoạ ở hình dưới đây:

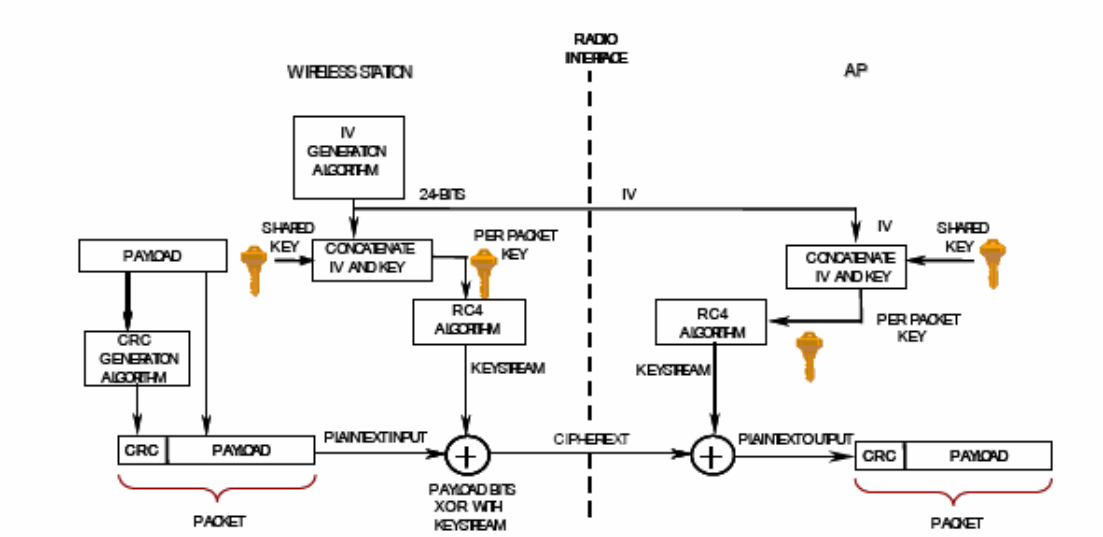


Hình 3.1: An toàn không dây 802.11 trong mạng cơ bản

WEP là một giao thức mã hoá được dùng để xác thực người sử dụng và mã hoá payload dữ liệu qua một môi trường không dây. WEP dự kiến cung cấp những mục đích an toàn: tin cậy, toàn vẹn dữ liệu, và điều khiển truy cập, để đảm bảo một môi trường không dây cũng an toàn như Ethernet hữu tuyến. Những người thực hiện WLAN ban đầu tin rằng họ có thể thực thi đơn giản WEP, và có một mạng không dây hoàn toàn an toàn. Những nhà sản xuất nhanh chóng nhận ra rằng WEP không phải là một giải pháp hoàn toàn an toàn, tuy nhiên ở thời điểm đó công nghệ WLAN đã trở nên thông dụng (thị trường gia đình và SOHO-Small Office and Home), trước khi vấn đề này được công bố rộng khắp.

Để ngăn chặn việc lộ những gói tin trong quá trình truyền (độ tin cậy), WEP sử dụng thuật toán RC4 [21], một mật mã đối xứng, tạo ra một dòng khoá có độ dài bằng độ dài dữ liệu. RC4 không được thiết kế cho sử dụng lại với cùng khoá. Để giải quyết lỗ hổng này, một vectơ khởi tạo IV (initialization vector) 24 bít được bổ sung thêm vào và đã làm thay đổi giá trị khoá cho mỗi gói tin. Qúa trình mã hoá WEP bắt đầu bằng một IV được tạo, sau đó kết hợp với khoá WEP thông qua thuật toán RC4 để tạo một giá trị mầm WEP. Gía trị mầm WEP này được chạy qua một bộ tạo số giả ngẫu nhiên để tạo một dòng mã, sau đó cho qua phép toán XOR với tin rõ/ICV. Kết quả là bản mã WEP

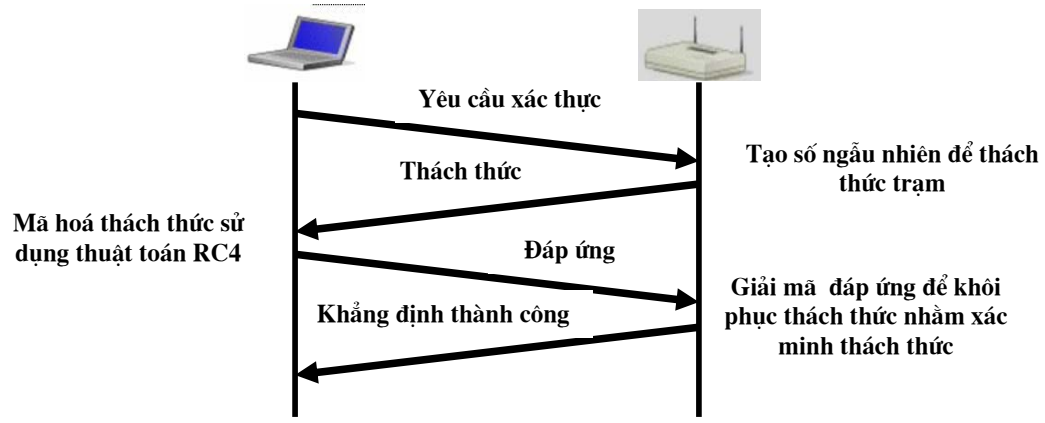
được gắn kèm với IV (trong bản rõ), và khoá này dùng để định hình tin sẽ được truyền. Việc tăng IV và gửi nó dưới dạng rõ cho phép một kẻ tấn công khôi phục một dòng khoá RC4, và thực hiện những tấn công như thâm nhập lưu lượng, dùng lại và biến đổi tin, tấn công dựa trên cơ sở từ điển, và tấn công phá khoá WEP.



Hình 3.2: Tính riêng tư WEP sử dụng thuật toán RC4

Để ngăn chặn biến đổi những gói tin trong quá trình truyền (toàn vẹn dữ liệu), WEP sử dụng vectơ kiểm tra tính toàn vẹn ICV (Integrity Check Vector), được biết đến như là một tổng kiểm tra (checksum) không an toàn. Bản rõ được gửi thông qua một thuật toán kiểm tra tính toàn vẹn CRC 32, tạo ra một ICV, được đính kèm với bản rõ. ICV có trong payload được mã hoá (bản mã). Sự yếu kém của ICV, cho phép một kẻ tấn công thực hiện một tấn công lật bít. Một kẻ tấn công có thể lấy một tin, lật những bít ngẫu nhiên nào đó trong vị trí dữ liệu của khung (những gói tin tầng cao hơn), tính toán lại một ICV thích hợp, và sau đó truyền lại một tin hợp lệ.

WEP sử dụng cơ chế xác thực khoá chia sẻ để điều khiển truy cập. Dựa trên cơ sở một giao thức thách thức-đáp ứng.



Hình 3.3: Sơ đồ xác thực WEP

Xác thực khoá chia sẻ yêu cầu một khoá WEP tĩnh được cấu hình bởi một client không dây. Qúa trình này bắt đầu bằng việc AP gửi một thách thức ngẫu nhiên dưới dạng bản rõ tới một client không dây. Nếu như client không dây biết khoá chia sẻ, nó mã hoá thách thức và gửi kết quả trở lại cho AP. AP chỉ cho phép truy cập nếu như giá trị được giải mã (kết quả được tính toán bởi client không dây) giống với thách thức ngẫu nhiên được truyền bởi AP. Phương pháp xác thực khoá chia sẻ có lỗ hổng, và để lộ những bít của dòng khoá. Nó không cung cấp xác thực lẫn nhau, mà chỉ đơn thuần thiết lập chứng minh rằng cả hai bên (AP và client không dây) chia sẻ cùng khoá bí mật. Nó phụ thuộc vào cơ sở hạ tầng WEP được xem là không an toàn. Thách thức-đáp ứng một chiều là lỗ hổng trước một tấn công man-in-the-middle. Một tên trộm có thể chặn bắt cả văn bản thách thức dưới dạng bản rõ và đáp ứng dưới dạng bản mã chỉ bằng cách phân tích mạng với một công cụ phân tích giao thức, và xác định dòng khoá.

Việc quản lý khoá WEP là một vấn đề an toàn nghiêm trọng khác trong giao thức WEP. Vấn đề quản lý khoá không được hỗ trợ, không cung cấp trao đổi khoá mã hoá tự động giữa client không dây và AP. Điều này có nghĩa là những khoá WEP phải được cấu hình bằng tay (những khoá tĩnh), và được

thay đổi thường xuyên để duy trì an toàn hiệu quả. Trong môi trường xí nghiệp lớn, công việc này quả là rất mệt mỏi, tốn kém và hầu như là một nhiệm vụ không thể thực hiện được.

Những khoá WEP tĩnh tạo ra một lỗ hổng an toàn nghiêm trọng khác trong giao thức WEP, nhiều người sử dụng WLAN chia sẻ khoá giống nhau trong một thời gian dài. Trước hết, một khoá WEP có thể bị lộ nếu như một máy tính laptop bị mất trộm, khiến cho tất cả những thành phần không dây khác chia sẻ cùng lỗ hổng khoá đó. Thứ hai, một khối lượng lớn dữ liệu lưu lượng trở nên sẵn sàng trước một tên trộm thông tin để khôi phục những dòng khoá và thực hiện những tấn công chủ động, đặc biệt trong môi trường lớn chia sẻ cùng khoá WEP.

WEP cung cấp những mức độ mã hoá khác nhau từ 40 đến 152 bít. Logic phổ biến chung đó là càng nhiều bít thì càng an toàn hơn, bởi vì một khoá mã hoá dài hơn sẽ khó phá hơn. Điều này không đúng với WEP. Nguồn gốc yếu kém ở đây không phải là độ dài khoá, mà là IV 24 bít. Một kẻ tấn công không có lý do gì thực hiện một tấn công bắt ép thô bạo, khi nó quá dễ dàng khai thác IV bằng những phương tiện khác.

3.2.2. ICV giá trị kiểm tra tính toàn vẹn

Thuật toán RC4 không thực sự thích hợp cho WEP, nó không đủ để làm phương pháp bảo mật duy nhất cho mạng 802.11. Cả hai loại 64 bít và 128 bít đều có cùng vectơ khởi tạo, IV (Initialization Vector) là 24 bít. Vectơ khởi tạo bằng một chuỗi các số 0, sau đó tăng thêm 1 sau mỗi gói được gửi. Với một mạng hoạt động liên tục, thì sự khảo sát chỉ ra rằng, chuỗi mã này có thể sẽ bị tràn trong vòng nửa ngày, vì thế vectơ khởi tạo cần được khởi động lại ít nhất mỗi lần một ngày, tức là các bít lại trở về 0. Khi WEP được sử dụng, IV được truyền mà không được mã hoá cùng với một gói được mã hoá. Việc phải khởi động lại và truyền không được mã hoá là nguyên nhân cho một vài kiểu tấn công sau:

- Tấn công chủ động để chèn gói tin mới: Một trạm di động không được phép có thể chèn các gói tin vào mạng, không cần giải mã.

- Tấn công chủ động để giải mã thông tin: dựa vào sự đánh lừa điểm truy nhập.

- Tấn công nhờ vào từ điển tấn công được xây dựng: sau khi thu thập đủ thông tin, chìa khoá WEP có thể bị crack bằng các công cụ phần mềm miễn phí. Khi khoá WEP bị crack, việc giải mã các gói thời gian thực có thể thực hiện bằng cách nghe các gói truyền, sử dụng chìa khoá WEP.

- Tấn công bị động để giải mã thông tin: sử dụng phương pháp phân tích thống kê để giải mã dữ liệu của WEP.

3.2.3. Tại sao WEP được lựa chọn

WEP không được an toàn, vậy tại sao WEP lại được lựa chọn và đưa vào chuẩn 802.11.

Chuẩn 802.11 đưa ra các tiêu chuẩn bảo mật, đó là:

- Có thể xuất khẩu.
- Đủ mạnh.
- Khả năng tương thích.
- Khả năng ước tính được.
- Tuỳ chọn, không bắt buộc.

WEP hội tụ đủ các yếu tố này, khi được đưa vào để thực hiện, WEP dự định hỗ trợ bảo mật với mục đích đảm bảo tin cậy, điều khiển truy nhập, và toàn vẹn dữ liệu. Người ta thấy rằng, WEP không phải là giải pháp bảo mật đầy đủ cho WLAN, tuy nhiên các thiết bị không dây đều được hỗ trợ khả năng dùng WEP, và điều đặc biệt là họ có thể bổ sung các biện pháp an toàn cho WEP. Mỗi nhà sản xuất có thể sử dụng WEP với các cách khác nhau. Như chuẩn Wi-Fi của WECA chỉ sử dụng từ khoá WEP 40 bít, một vài hãng sản xuất lựa chọn cách tăng cường cho WEP, một vài hãng khác lại sử dụng một chuẩn mới như 802.1X với EAP hoặc VPN.

3.2.4. Khoá WEP

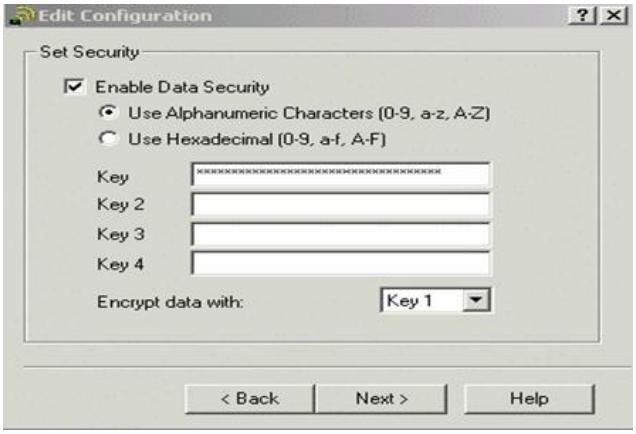
Vấn đề cốt lõi của WEP đó là khoá WEP. Khoá WEP là một chuỗi ký tự chữ cái và số, được sử dụng với hai mục đích cho WLAN:

- Dùng để xác định sự cho phép của một trạm.
- Dùng để mã hoá dữ liệu.

Khi một client sử dụng WEP cố gắng thực hiện một xác thực và liên kết tới một AP. AP sẽ xác thực xem client có chìa khoá xác thực hay không, nếu có, nghĩa là client phải có một từ khóa là một phần của khoá WEP, khoá WEP này phải khớp với kết nối cuối cùng của WLAN.

Một nhà quản trị mạng có thể thực hiện phân phối khoá WEP bằng tay hoặc bằng một phương pháp tiên tiến khác. Hệ thống phân phối khoá WEP có thể đơn giản như thực hiện khoá tĩnh, hoặc tiên tiến như sử dụng Server quản lý khoá mã tập trung. Hệ thống WEP càng tiên tiến, càng ngăn chặn được khả năng bị phá hoại.

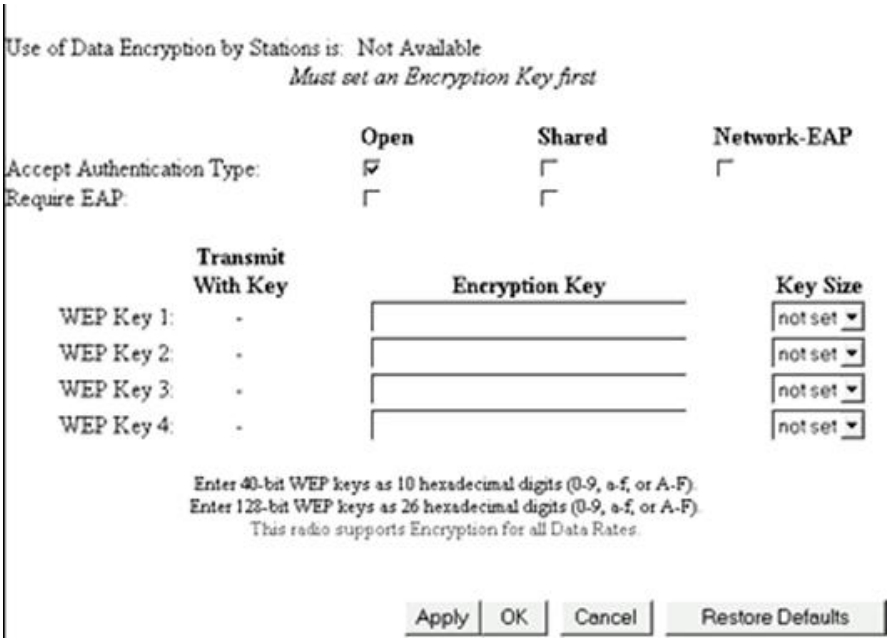
Khoá WEP tồn tại hai loại, 64 bít và 128 bít, mà đôi khi thấy viết là 40 bít và 104 bít. Lý do vì cả hai loại khoá WEP này đều dùng chung một vectơ khởi tạo IV 24 bít và một từ khoá bí mật 40 bít hoặc 104 bít. Việc nhập khoá WEP vào client hoặc các thiết bị phụ thuộc như là bridge hoặc AP rất đơn giản. Nó được cấu hình như hình vẽ sau:



Hình 3.4: Giao diện nhập khoá WEP

Hầu hết các client và AP có thể đưa ra đồng thời 4 khoá WEP, nhằm hỗ trợ phân đoạn mạng. Ví dụ, nếu hỗ trợ một mạng có 100 trạm: đưa ra 4 khoá WEP thay vì một có thể phân số người dùng ra làm 4 nhóm riêng biệt, mỗi nhóm 25 người, nếu một WEP bị mất thì chỉ phải thay đổi 25 trạm và một đến hai AP thay vì phải thay trên toàn bộ mạng.

Một lý do khác khi dùng nhiều khoá WEP là nếu một card tích hợp cả khoá 64 bít và khoá 128 bít thì nó có thể dùng phương án tối ưu nhất, đồng thời nếu hỗ trợ 128 bít thì cũng có thể làm việc được với khoá 64 bít.



Hình 3.5: Sự hỗ trợ sử dụng nhiều khoá WEP

Theo chuẩn 802.1, khoá WEP sử dụng là khoá WEP tĩnh. Nếu chọn WEP tĩnh bạn phải tự gán một WEP tĩnh cho một AP hoặc client liên kết với nó. Khoá WEP này sẽ không bao giờ thay đổi. Nó có thể là một phương pháp bảo mật căn bản, đơn giản, thích hợp cho những WLAN nhỏ, nhưng không thích hợp với những mạng WLAN quy mô lớn hơn. Nếu chỉ sử dụng WEP tĩnh thì rất dễ dẫn đến sự mất an toàn. Trong trường hợp một người nào đó làm mất card mạng WLAN của họ, card mạng đó chứa chương trình cơ sở có thể

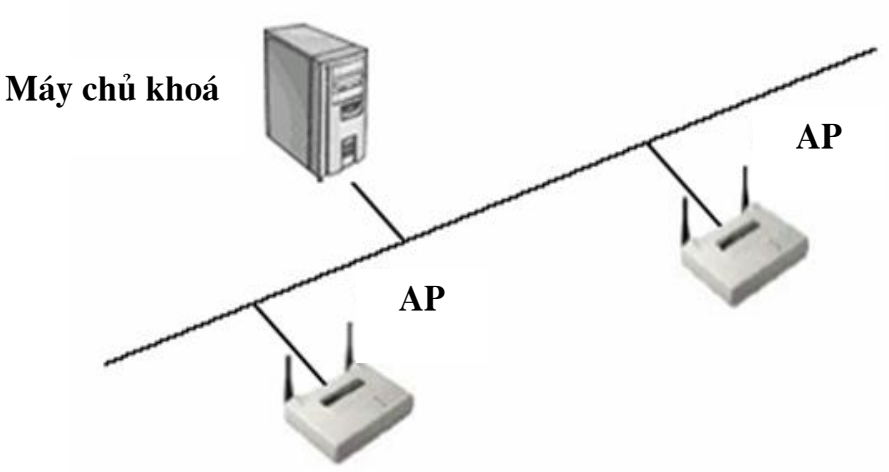
truy nhập vào WLAN đó cho tới khi khoá WEP tĩnh của WLAN đó được thay đổi.

3.2.5. Máy chủ quản lý khoá mã tập trung

Với những mạng WLAN quy mô lớn sử dụng WEP như một phương pháp bảo mật căn bản, máy chủ quản lý khoá mã tập trung nên được sử dụng vì lý do sau:

- Quản lý sinh khoá tập trung.
- Quản lý phân phối khoá tập trung.
- Thay đổi khoá thường xuyên.
- Giảm bớt công việc cho nhà quản lý.

Thông thường, khi sử dụng WEP, những khoá mã được tạo bởi người quản trị thường được nhập bằng tay vào trong các trạm và các AP. Khi sử dụng máy chủ quản lý khoá mã tập trung, một quá trình tự động giữa các trạm, AP và máy chủ quản lý sẽ thực hiện phân phối các khoá WEP. Hình sau mô tả cách thiết lập một hệ thống như vậy.



Hình 3.6: Cấu hình quản lý khoá mã tập trung

Máy chủ quản lý khoá mã tập trung cho phép sinh khoá trên mỗi gói, mỗi phiên, hoặc các phương pháp khác, phụ thuộc vào sự thực hiện của các nhà sản xuất.

Phân phối khoá WEP trên mỗi gói tin, mỗi khoá WEP mới sẽ được gán vào phần cuối của các kết nối cho mỗi gói được gửi, trong khi đó, phân phối khoá WEP trên mỗi phiên sử dụng một khoá mới cho mỗi một phiên mới giữa các nút (node).

3.2.6. Cách sử dụng WEP

Khi WEP được khởi tạo, dữ liệu phần tải (payload) của mỗi gói được gửi, sử dụng WEP, đã được mã hoá; tuy nhiên, phần header của mỗi gói, bao gồm địa chỉ MAC, không được mã hoá, tất cả thông tin lớp 3 bao gồm địa chỉ nguồn và địa chỉ đích được mã hoá bởi WEP [22].

Khi một AP gửi ra ngoài những thông tin đường dẫn của nó trên một WLAN đang sử dụng WEP, những thông tin này không được mã hoá. Thông tin dẫn đường không bao gồm bất cứ thông tin nào của lớp 3.

Khi các gói được gửi đi sử dụng mã hoá WEP, những gói này phải được giải mã. Qúa trình giải mã chiếm các chu kỳ của CPU, nó làm giảm đáng kể thông lượng trên WLAN. Một vài nhà sản xuất tích hợp các CPU trên các AP của họ cho mục đích mã hoá và giải mã WEP. Nhiều nhà sản xuất lại tích hợp cả mã hoá và giải mã trên một phần mềm và sử dụng cùng CPU được dùng cho quản lý AP, chuyển tiếp gói. Nhờ tích hợp WEP trong phần cứng, một AP có thể duy trì thông lượng 5 Mbps hoặc nhiều hơn. Tuy nhiên, sự bất lợi của giải pháp này là giá thành của AP tăng lên hơn so với AP thông thường.

WEP có thể được thực hiện như một phương pháp bảo mật căn bản, nhưng các nhà quản trị mạng cần nắm bắt những điểm yếu của WEP và cách khắc phục chúng. Mỗi nhà cung cấp sử dụng WEP có thể khác nhau, vì vậy gây trở ngại cho việc sử dụng phần cứng của nhiều nhà cung cấp.

Để khắc phục những yếu điểm của WEP, chuẩn mã hoá tiên tiến AES (Advanced Encryption Standard) đang được công nhận như là một sự thay thế thích hợp cho thuật toán RC4. AES sử dụng thuật toán RINE-dale với những loại khoá sau:

- 128 bít.
- 192 bít.
- 256 bít.

AES được xem như là một phương pháp không thể crack bởi hầu hết người viết mật mã, và NIST (National Institute of Standards and Technology) đã chọn AES cho FIPS (Federal Information Processing Standard). Như một phần cải tiến cho chuẩn 802.11, 802.11i được xem xét để sử dụng AES trong WEP phiên bản 2.

AES sẽ được thực hiện trong phần vi chương trình và các phần mềm bởi các nhà cung cấp. Chương trình cơ sở trong AP và trong Client (card vô tuyến PCMCIA) sẽ phải được nâng cấp để hỗ trợ AES. Phần mềm trạm khách (các driver và các tiện ích máy khách) sẽ hỗ trợ cấu hình AES cùng với khoá mật.

3.3. Lọc (Filtering)

Lọc là một cơ chế bảo mật căn bản có thể dùng để bổ sung cho WEP hoặc AES. Lọc theo nghĩa đen là chặn những gì không mong muốn và cho qua những gì mong muốn. Lọc làm việc giống như một danh sách truy nhập trên router: bằng cách xác định các tham số mà các trạm phải gán vào để truy cập mạng. Với WLAN việc đó có nghĩa là xác định xem các máy trạm là ai và phải cấu hình như thế nào. Có 3 loại lọc căn bản có thể thực hiện trên WLAN:

- Lọc SSID.
- Lọc địa chỉ MAC.
- Lọc giao thức.

3.3.1. Lọc SSID

Lọc SSID (SSID Filtering) là một phương pháp lọc sơ đẳng, và chỉ nên dùng cho hầu hết các điều khiển truy nhập. SSID (Service Set Identifier) là một thuật ngữ khác cho tên mạng, SSID của một trạm WLAN phải khớp với SSID trên AP (chế độ cơ sở – Infrastructure mode) hoặc của các trạm khác (chế độ tự do-Ad-hoc mode) để chứng thực và liên kết client nhằm thiết lập

dịch vụ. Vì SSID được phát quảng bá trong các bản tin dẫn đường mà các AP hoặc các trạm gửi ra, nên dễ dàng tìm ra SSID của một mạng sử dụng một bộ phân tích mạng (Sniffer). Nhiều AP có khả năng lấy các SSID của các khung thông tin báo hiệu (beacon frame). Trong trường hợp này, client phải so khớp với SSID để liên kết với AP. Khi một hệ thống được cấu hình theo kiểu này, nó được gọi là hệ thống đóng (closed system). Lọc SSID được coi là một phương pháp không tin cậy trong việc hạn chế những người sử dụng trái phép một WLAN.

Một vài loại AP có khả năng gỡ bỏ SSID từ những thông tin dẫn đường hoặc các thông tin kiểm tra. Trong trường hợp này, để gia nhập dịch vụ một trạm phải có SSID được cấu hình bằng tay khi thiết đặt cấu hình driver.

Một số lỗi chung do người sử dụng WLAN tạo ra khi thực hiện SSID, đó là:

- Sử dụng SSID mặc định: sự thiết lập này là một cách khác để đưa ra thông tin về WLAN của bạn. Nó đủ đơn giản sử dụng một bộ phân tích mạng để lấy địa chỉ MAC khởi nguồn từ AP, sau đó xem MAC trong bảng OUI của IEEE, bảng này liệt kê các tiền tố địa chỉ MAC khác nhau ứng với các nhà sản xuất. Cách tốt nhất khắc phục lỗi này là thay đổi SSID mặc định thường xuyên.

- Làm cho SSID có gì đó liên quan đến công ty của bạn: Loại thiết lập này là một mạo hiểm về bảo mật vì nó làm đơn giản hoá quá trình một hacker tìm thấy vị trí vật lý của công ty. Khi tìm kiếm WLAN trong đó một người quản trị sử dụng SSID có tên liên quan đến công ty hoặc tổ chức, việc tìm thấy WLAN sẽ rất dễ dàng. Do vậy luôn sử dụng SSID không liên quan đến công ty.

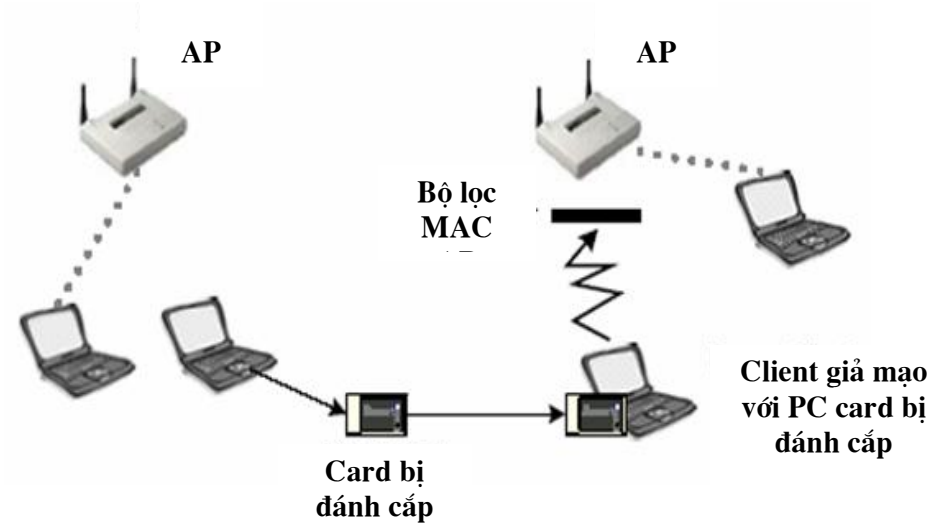
- Sử dụng SSID như những phương tiện bảo mật mạng WLAN: SSID phải được người sử dụng thay đổi khi thiết lập cấu hình để vào mạng. Nó nên

được sử dụng như một phương tiện phân đoạn mạng chứ không phải để bảo mật, vì thế hãy luôn coi SSID như một tên mạng.

- Không cần thiết quảng bá SSID: Nếu AP của bạn 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 trộm vô tình khỏi việc gây rối hoặc sử dụng WLAN của bạn.

3.3.2. Lọc địa chỉ MAC

WLAN có thể lọc dựa vào địa chỉ MAC của các trạm khách. Hầu hết các AP, thậm chí cả AP rẻ tiền, đều có chức năng lọc MAC. Những người quản trị mạng có thể biên tập, phân phối và bảo trì một danh sách những địa chỉ MAC được phép và lập trình chúng vào các AP. Nếu một card PC hoặc những Client khác với một địa chỉ MAC không có trong danh sách địa chỉ MAC của AP, nó sẽ không thể đến được điểm truy nhập đó.



Hình 3.7: Lọc địa chỉ MAC

Tất nhiên, việc lập trình các địa chỉ MAC của các Client trong mạng WLAN vào các AP trên một mạng rộng thì không thực tế. Bộ lọc MAC có thể được thực hiện trên vài máy chủ RADIUS thay vì trên mỗi điểm truy nhập. Các cấu hình này làm cho lọc MAC là một giải pháp an toàn, và do đó có khả năng được lựa chọn nhiều hơn. Việc nhập địa chỉ MAC cùng với thông tin xác

định người sử dụng vào RADIUS khá đơn giản, có thể phải được chấp nhận bằng bất kỳ giá nào, là một giải pháp tốt. Máy chủ RADIUS thường trỏ đến các nguồn chứng thực khác, vì vậy các nguồn chứng thực khác phải được hỗ trợ bộ lọc MAC.

Bộ lọc MAC có thể làm việc tốt trong chế độ ngược lại. Xét một ví dụ, một người làm thuê bỏ việc và mang theo cả card mạng WLAN của họ. Card WLAN này nắm giữ cả khoá WEP và bộ lọc MAC, vì thế không thể để họ còn quyền sử dụng. Khi đó người quản trị mạng có thể loại bỏ địa chỉ MAC của máy khách đó ra khỏi danh sách cho phép.

Mặc dù lọc MAC có vẻ là một phương pháp bảo mật tốt, chúng vẫn dễ bị ảnh hưởng bởi những thâm nhập sau:

- Trộm card PC trong đó có bộ lọc MAC của AP.

- Thăm dò WLAN sau đó giả mạo địa chỉ MAC để thâm nhập vào mạng.

Với những mạng gia đình hoặc những mạng văn phòng nhỏ, với ít trạm khách, việc dùng bộ lọc MAC là một giải pháp bảo mật hiệu quả, vì không một hacker thông minh nào lại tốn hàng giờ để truy nhập vào một mạng có giá trị sử dụng thấp.

Địa chỉ MAC của Client WLAN thường được phát quảng bá bởi các AP và Bridge, ngay cả khi sử dụng WEP. Vì thế một hacker có thể nghe được lưu lượng trên mạng và nhanh chóng tìm thấy hầu hết các địa chỉ MAC . Để một bộ phân tích mạng thấy được địa chỉ MAC của một trạm, trạm đó phải truyền một khung qua đoạn mạng không dây, đây chính là cơ sở dẫn đến việc xây dựng một phương pháp bảo mật mạng, tạo đường hầm trong VPN, sẽ được đề cập ở phần sau.

Một vài card PC không dây cho phép thay đổi địa chỉ MAC của họ thông qua phần mềm hoặc thậm chí qua cách thay đổi cấu hình hệ thống. Một hacker có danh sách các địa chỉ MAC, có thể dễ dàng thay đổi địa chỉ MAC

của card PC để phù hợp với một card PC trên mạng của bạn, và do đó truy nhập tới toàn bộ mạng không dây của bạn.

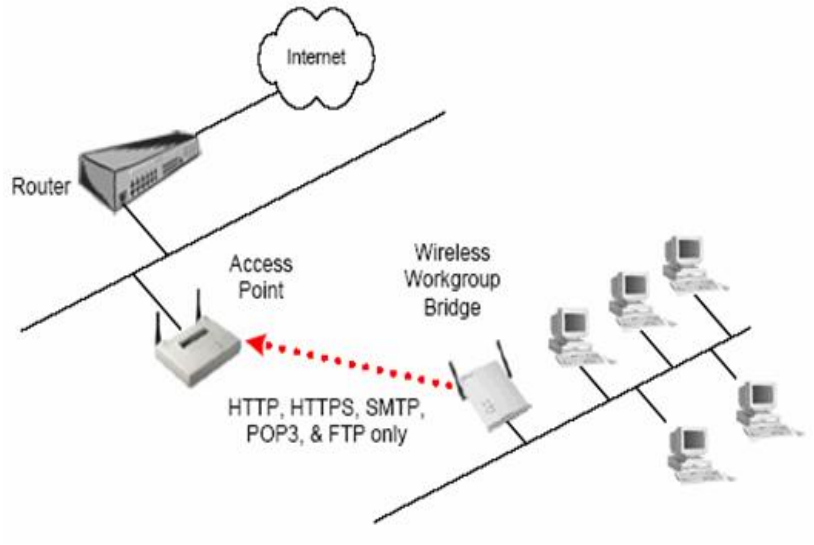
Do hai trạm với cùng địa chỉ MAC không thể đồng thời cùng tồn tại trên một WLAN, hacker phải tìm một địa chỉ MAC của trạm mà hiện thời không có trên mạng. Chính trong thời gian trạm di động hoặc máy tính xách tay không có trên mạng là thời gian hacker có thể truy nhập vào mạng tốt nhất.

Lọc MAC nên được sử dụng khi khả thi, nhưng không phải là cơ chế bảo mật duy nhất trên máy của bạn.

3.3.3. Lọc giao thức

Một WLAN có thể lọc các gói đi qua mạng dựa trên các giao thức lớp 2-7. Trong nhiều trường hợp, các nhà sản xuất làm các bộ lọc giao thức có thể định hình độc lập cho cả những đoạn trạm 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 toà nhà kỹ thuật trung tâm. Vì tất cả những người sử dụng trong remote building chia sẻ băng thông 5 Mbps giữa những toà 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...



Hình 3.8: Lọc giao thức

3.4. Bảo vệ WLAN với xác thực và mã hoá dữ liệu 802.1x

Bảo vệ WLAN liên quan đến 3 yếu tố chính:

- Xác thực người (hoặc thiết bị) kết nối tới mạng do vậy bạn có một mức độ tin cậy cao để biết ai hay cái gì đang cố gắng kết nối tới mạng của bạn.

- Cấp quyền cho cá nhân hay thiết bị sử dụng WLAN do đó bạn kiểm soát được ai có quyền truy cập tới nó.

- Bảo vệ dữ liệu được truyền trên mạng do đó mạng an toàn trước việc nghe trộm và biến đổi không được phép.

Bạn có thể yêu cầu một chức năng kiểm định ngoài những vấn đề trên, mặc dù kiểm định về cơ bản là một phương tiện kiểm tra và củng cố cho những yếu tố trên.

3.4.1. Xác thực và cấp quyền mạng

Như đã đề cập ở trên an toàn WEP tĩnh dựa vào một khoá (hay mật khẩu) bí mật được chia sẻ để xác thực tới WLAN. Bất kỳ ai có khoá bí mật có thể truy cập tới WLAN. Chuẩn WEP ban đầu không cung cấp một phương pháp nào cho việc tự động cập nhật hay phân phối những khoá này, do vậy

việc thay đổi khoá thường xuyên rất khó. Những thiếu sót mật mã trong WEP đồng nghĩa với việc một kẻ tấn công có thể phá những khoá WEP tĩnh bằng những công cụ đơn giản.

Để cung cấp một giải pháp xác thực và cấp quyền mạnh hơn, một số nhà sản xuất đưa ra một khung an toàn WLAN sử dụng giao thức 802.1x. 802.1x là một chuẩn IEEE cho xác thực truy cập tới một mạng và cho quản lý khoá sử dụng để bảo vệ lưu lượng. Việc sử dụng nó không chỉ giới hạn cho những mạng không dây; nó cũng được thực thi trong nhiều chuyển mạch LAN hữu tuyến đầu trên.

Giao thức 802.1x liên quan đến người sử dụng mạng. Một thiết bị truy cập mạng (hay một cổng) như một AP không dây chẳng hạn, và một dịch vụ xác thực và cấp quyền dưới dạng một máy chủ RADIUS (Remote Authentication Dia-In User Service). Máy chủ RADIUS thực hiện công việc xác thực những chứng minh của người sử dụng và cấp quyền truy cập cho người sử dụng WLAN.

802.1x dựa trên một giao thức IETF gọi là giao thức xác thực tăng cường (EAP-Extensive Authetication Protocol) [23] để mang tải hội thoại xác thực giữa client và máy chủ RADIUS (được tiếp sóng bởi AP). EAP nhìn chung là một giao thức dùng cho xác thực hỗ trợ nhiều phương pháp xác thực, dựa trên cơ sở những mật khẩu, những xác minh số, hay những kiểu xác minh khác. Những phương pháp này có thể sử dụng những giao thức xác thực khác nhau như Kerberos, TLS (Transport Layer Security), và MS-CHAP (Microsoft Chanllenge Handshake Authentication Protocol) sử dụng một trong những kiểu xác thực như xác thực mật khẩu, xác thực mã thông báo mật khẩu một lần hay xác thực sinh trắc học. Mặc dù bất kỳ phương pháp EAP nào, về mặt lý thuyết, có thể được sử dụng với 802.x, tuy nhiên không phải tất cả đều phù hợp cho sử dụng với WLAN; đặc biệt, phương pháp được sử dụng phải phù hợp cho một môi trường không được bảo vệ và có thể tạo những khoá mã hoá.

Những phương pháp EAP cơ bản trong sử dụng cho những WLAN là EAP-TLS, PEAP (Protected EAP), TTLS (Tunneled TLS), và LEAP (Lightweight EAP).

3.4.1.1. EAP TLS

EAP – TLS (Extensible Authentication Protocol - Transport Layer Security) là một chuẩn IEFT (RFC 2716) và có lẽ được hỗ trợ rộng rãi nhất, trên cả những client và máy chủ RADIUS. Nó sử dụng xác thực khoá công khai để xác thực cả client không dây và máy chủ RADIUS bằng cách thiết lập một phiên TLS được mã hoá giữa client và RADIUS.

3.4.1.2. PEAP

PEAP (Protected EAP) là một phương pháp xác thực hai giai đoạn. Giai đoạn đầu thiết lập một phiên TLS tới máy chủ và cho phép client xác thực máy chủ sử dụng xác minh số của máy chủ. Giai đoạn thứ hai yêu cầu một phương pháp EAP thứ hai nằm bên trong phiên PEAP để xác thực client với máy chủ RADIUS. Điều này cho phép PEAP sử dụng các phương pháp xác thực client khác nhau bao gồm những mật khẩu với giao thức MS-CHAP phiên bản 2 và những xác minh sử dụng EAP-TLS bên trong PEAP. Những kiểu EAP như MS-CHAP v2 không đủ an toàn để sử dụng mà không có bảo vệ PEAP bởi vì chúng có thể là lỗ hổng trước những tấn công từ điển offline.

3.4.1.3. TTLS

TTLS (Tunneled Transport Layer Security) là giao thức hai giai đoạn tương tự như PEAP sử dụng một phiên TLS để bảo vệ một xác thực client đi qua đường hầm. Ngoài những phương pháp EAP đường hầm, TTLS cũng có thể sử dụng những phiên bản của những giao thức xác thực không phải EAP như CHAP, MS-CHAP, và những phương pháp khác.

3..4.1.4. LEAP

LEAP (Cisco Lightweight EAP) là một phương pháp EAP độc quyền được phát triển bởi Cisco, sử dụng những mật khẩu để xác thực các client.

Mặc dù thông dụng, LEAP chỉ làm việc với phần cứng và phần mềm do Cisco sản xuất và một số nhà sản xuất khác. LEAP cũng có nhiều những lỗ hổng an ninh được công bố như sự nhạy cảm với những tấn công từ điển offline (có thể cho phép kẻ tấn công tìm ra mật khẩu người sử dụng) và những tấn công man-in-the-middle. Trong một môi trường miền, LEAP chỉ có thể xác thực người sử dụng WLAN, chứ không phải máy tính. Không có xác thực máy tính, những chính sách nhóm máy sẽ không được thực hiện đúng, những thiết lập cài đặt phần mềm, những hiện trạng roaming, và những mã đăng nhập, tất cả có thể thất bại, và người sử dụng sẽ không thể thay đổi những mật khẩu được gia hạn.

Có nhiều giải pháp an toàn WLAN sử dụng 802.1x với những phương pháp EAP khác. Một số trong những phương pháp EAP này, như EAP-MD5, có sự yếu kém an toàn đáng kể khi sử dụng trong một môi trường WLAN và không nên sử dụng nó. Có những phương pháp khác hỗ trợ sử dụng những mã báo hiệu mật khẩu một lần và những giao thức xác thực khác như Kerberos.

3.4.2. Bảo vệ dữ liệu WLAN

Xác thực và truy cập mạng 802.1x chỉ là một phần của phương pháp này. Thành phần quan trọng khác là bảo vệ lưu lượng mạng không dây.

Những thiếu sót trong mã hoá dữ liệu WEP được mô tả ở trên có thể được cải thiện nếu như WEP tĩnh được bổ sung thêm một phương pháp cập nhật tự động những khoá mã hoá định kỳ. Những công cụ dùng cho phá WEP tĩnh cần tập hợp giữa một và 10 triệu gói tin được mã hoá cùng khoá. Do những khoá WEP tĩnh thường vẫn không thay đổi trong nhiều tuần hoặc nhiều tháng nên một kẻ tấn công nào đó rất dễ tập hợp lượng dữ liệu này. Do tất cả các máy tính trên một WLAN chia sẻ cùng khoá tĩnh, nên những lần truyền dữ liệu từ tất cả các máy tính trên WLAN có thể được thu vén lại để giúp phá khoá.

Việc sử dụng một giải pháp dựa trên cơ sở 802.1x cho phép những khoá mã hoá được thay đổi thường xuyên. Giống như quá trình xác thực an toàn 802.1x, phương pháp EAP tạo một khoá mã duy nhất cho mỗi client. Để ngăn ngừa những tấn công phá khoá WEP, máy chủ RADIUS thường xuyên thực hiện tạo những khoá mã hoá mới. Điều này cho phép thuật toán mã hoá WEP (được thấy trong hầu hết những phần cứng WLAN hiện nay) được sử dụng theo một cách an toàn hơn nhiều.

3.4.3. Ưu điểm của 802.1x với bảo vệ dữ liệu WLAN

Lợi ích chính của giải pháp 802.1x:

- An toàn cao: nó là một sơ đồ xác thực an toàn cao bởi vì nó có thể sử dụng những xác minh client hay những mật khẩu và tên người sử dụng.

- Mã hoá mạnh hơn: nó cho phép mã hoá tăng cường dữ liệu mạng.

- Trong suốt: nó cung cấp xác thực và kết nối trong suốt tới WLAN.

- Xác thực người sử dụng và máy tính: nó cho phép xác thực tách biệt người sử dụng và máy tính. Xác thực tách biệt máy tính cho phép máy tính được quản lý thậm chí khi không có người sử dụng nào đăng nhập vào.

- Chi phí thấp: chi phí cho phần cứng mạng thấp.

- Hiệu năng cao: do mã hoá được thực hiện trong phần cứng WLAN chứ không phải ở CPU máy tính client, việc mã hoá WLAN không có tác động nào lên mức độ hiệu năng của máy tính client.

Ngoài những ưu điểm trên, giải pháp an toàn 802.1x cũng có một số vấn đề như:

- Mặc dù 802.1x gần như được chấp nhận trên toàn cầu, nhưng việc sử dụng những phương pháp EAP khác nhau có nghĩa là sự tương thích hoạt động không phải lúc nào cũng được đảm bảo.

- WPA vẫn còn khá mới mẻ và có thể không sẵn sàng trên những phần cứng cũ.

- RSN thế hệ mới (802.1i) sẽ được phê chuẩn và sẽ yêu cầu phát triển những cập nhật phần cứng và phần mềm.

3.5. WPA(Wi-Fi Protect Access) và 802.11i

Những vấn đề an toàn trong chuẩn 802.11 và WEP dẫn đến sự phát triển của chuẩn 802.11i. Vào tháng 10 năm 2003, Wi-Fi Alliance đã công bố WPA để giải quyết tất cả những lỗ hổng được biết đến trong WEP. Đây là một giải pháp tạm thời để khắc phục những lỗ hổng của chuẩn 802.11 ở thời điểm đó. Sự thúc đẩy phát triển WPA tập trung vào những lỗ hổng an toàn trong 802.11. WPA được thiết kế là một giải pháp mạnh, kinh tế làm việc với phần cứng cũ (những sản phẩm 802.11), và tương thich với chuẩn 802.11i. Đến năm 2004, tất cả các sản phẩm phải tích hợp WPA sẽ được xác nhận Wi-Fi.

WPA thực hiện những cải tiến chính đối với mã hoá, xác thực, toàn vẹn dữ liệu, quản lý khoá, và bổ sung một yếu tố xác định khả năng an toàn mạng. WPA đưa ra một công nghệ mã hoá mới, TKIP (Temporal Key Integrity Protocol) với kiểm tra tính toàn vẹn tin MIC (Message Integrity Check), để thay thế WEP và cung cấp tin cậy dữ liệu và toàn vẹn payload dữ liệu mạng. Wi-Fi Alliance thực thi xác thực lẫn nhau trong WPA bằng phương tiện xác thực IEEE 802.1x/EAP, cung cấp một xác thực mạnh giữa một client không dây và máy chủ xác thực thông qua một AP. Ngoài ra, WPA mở đường cho sử dụng phương pháp xác thực mở. Quản lý khoá, một trong những vấn đề lớn nhất trong 802.11, đã được giải quyết và thực thi trong 802.11i (và WPA) cung cấp một quá trình xác thực tách biệt để cho phép phân phối khoá. Yếu tố xác định an toàn mạng tích hợp những yếu tố thông tin WPA trong những khung 802.11 (báo hiệu, thăm dò, đáp ứng, và thách thức tái kết hợp) để xác định mã hoá và xác thực nào là phù hợp cho sử dụng.

3.5.1. Mã hoá TKIP trong WPA

TKIP được thiết kế để giải quyết những lỗ hổng của WEP, không cần thay thế phần cứng cũ. Vì lý do này, TKIP duy trì những cơ chế cơ bản của

WEP: IV, thuật toán RC4, và ICV. Tuy nhiên, sơ đồ mã hoá RC4 được tăng cường sử dụng một khoá trên mỗi gói tin 128 bít, và một IV 48 bít dài hơn. Không giống như WEP, TKIP mã hoá mỗi gói dữ liệu được gửi bằng khoá mã hoá duy nhất của chính nó. Những khoá này được tạo ra một cách tự động, cung cấp khả năng an toàn cao hơn chống lại những kẻ xâm phạm dựa vào việc dự đoán trước những khoá tĩnh trong WEP. Ngoài ra, WPA bao gồm một kiểm tra tính toàn vẹn tin MIC, được gọi là Michael, để ngăn chặn biến đổi tin.

Có ba giao thức kết hợp với TKIP: MIC (hay Michael), một thuật toán trộn khoá, và một tăng cường IV. Thuật toán đầu tiên, MIC, là một thuật toán toàn vẹn tin mật mã để ngăn chặn bất kỳ biến đổi nào tới một tin. Nó sử dụng một hàm băm thay cho tổng kiểm tra tuyến tính, giải quyết những lỗ hổng trong ICV. Thuật toán băm, được gọi là Michael, được thiết kế để đảm bảo nội dung của gói dữ liệu chỉ được gửi bởi những client không dây hợp pháp và không có sự biến đổi dữ liệu nào trong suốt quá trình truyền gói tin. Michael tạo ra hai từ 32 bít để tạo một băm 64 bít. Một băm được tính toán, sau đó được so sánh với cả bên nhận/truyền. Gía trị MIC phải phù hợp với dữ liệu sẽ được chấp nhận. Nếu không, gói tin này bị bỏ qua bởi vì nó được giả định rằng tính toàn vẹn gói tin đã bị gây hại, trừ phi những biện pháp đối phó được thực hiện. Trong trường hợp này, tất cả những lần truyền và thu nhận gói tin đều bị vô hiệu hoá, và tất cả các client không dây giải xác thực và những kết hợp mới bị dừng lại trong vòng 60 giây.

Giao thức thứ hai, TKIP thay thế IV 24 bít lỗ hổng bằng một bộ đếm chuỗi TKIP TSC (TKIP Sequence Counter) 48 bít để giải quyết những vấn đề sử dụng lại IV trong WEP. TSC là một bộ đếm 48 bít bắt đầu bằng 0 và tăng thêm 1 cho mỗi gói tin, cung cấp cho bên nhận phương tiện duy trì dấu vết của giá trị cao nhất cho mỗi địa chỉ MAC, để đảm bảo những gói tin đến theo chuỗi. Một gói tin bị bỏ qua nếu như giá trị TSC (gói TKIP) ít hơn hoặc bằng

với gói tin nó vừa nhận được, để ngăn chặn những tấn công dùng lại. Do giao thức đầu tiên tăng cường ICV và MIC, một kẻ tấn công cũng bị ngăn chặn trước thay đổi TSC và sử dụng nó để truyền lại một gói tin. TSC được sử dụng trong thuật toán giải mã, và nếu bị biến đổi với kết quả trong ICV và MIC không phù hợp gói tin này sẽ bị bỏ qua. Hàm TSC cho phép một chuỗi khoá không bao giờ bị dùng lại với cùng khoá. Giao thức này ngăn chặn một kẻ tấn công thực hiện một tấn công dùng lại, được biết đến là những tấn công bản rõ đã biết và những tấn công dựa trên cơ sở từ điển sau khi khôi phục một dòng khoá.

Giao thức thứ ba, TKIP tích hợp một hàm trộn khoá để đảm bảo những khoá mã hoá thay đổi trên cơ sở mỗi gói tin. Nó được thiết kế để bảo vệ khoá mã hoá tạm thời TEK (Temporal Encryption Key) 128 bít, một khóa cơ sở tạm thời được sử dụng để tạo những khoá dùng duy nhất trên mỗi gói tin. Thuật toán trộn khoá là một phép toán hai pha. Để đơn giản, TEK, được kết hợp với TSC và một địa chỉ nơi truyền TA (Transmitter Address) 48 bít để tạo một khoá duy nhất trên mỗi gói tin, mầm WEP 128 bít, được sử dụng với thuật toán WEP. Bộ đếm TSC, như đã nêu trước đó, tăng với mỗi gói tin, tạo ra mầm WEP thay đổi với mỗi gói tin. Kết quả, TKIP tạo ra những khoá duy nhất một cách tự động để mã hoá mỗi gói dữ liệu được truyền trong một phiên không dây, cung cấp xấp xỉ 280 nghìn tỉ những kết hợp khoá có thể sẽ được tạo ra cho mỗi gói tin.

3.5.2. Xác thực trong WPA

Trong WPA, xác thực lẫn nhau đạt được bằng khung 802.1x/EAP. Xác thực lẫn nhau giúp đảm bảo chỉ những người sử dụng được quyền mới có thể truy cập mạng. Nó là một quá trình khẳng định rằng một client không dây đang xác thực tới một máy chủ được quyền, và không phải với một AP giả mạo.

Qúa trình xác thực bắt đầu với một giao thức hỗ trợ EAP, client không dây liên lạc với một AP bằng một yêu cầu (kết hợp) sẽ được xác thực. Với điều khiển truy cập cổng 802.1x, một client không dây không được cấp quyền truy cập tới một AP cho đến khi nó được xác thực. AP đẩy yêu cầu này tới một máy chủ xác thực AS (Authentication server), ở đó AS yêu cầu người sử dụng đưa ra một mật khẩu hợp lệ (thông qua AP), và xác thực đáp ứng từ người sử dụng (nếu hợp lệ). Sau đó, một AP nhận được quyền từ AS, và mở một cổng để chấp nhận dữ liệu từ người sử dụng. Client không dây khi đó được phép gia nhập WLAN.

Khi được xác thực, client không dây và AS đồng thời tạo một PMK (Pairwise Master Key), như là một phần của quá trình xác thực lẫn nhau. Những khoá chủ này giống như phần gốc rễ của cây khoá cho ra những khoá truyền. PMK là một khoá chia sẻ được sử dụng bởi client không dây và AS để thương thuyết những khoá truyền sử dụng cho một phiên. Nó không phải là PMK, tuy nhiên những khoá truyền (những khoá PTK) được sử dụng trong những hàm mã hoá và băm. PMK không liên quan trực tiếp trong việc tạo những dòng khoá cho mã hoá, nó giúp ngăn chặn những khoá yếu. Khi khoá chia sẻ chủ được tạo, AS truyền khoá này tới AP thông qua giao thức RADIUS.

Cơ chế xác thực chia thành hai loại, bởi vì WPA phải giải quyết hai thị trường rất khác nhau: xí nghiệp và người dùng.

- Ở mức xí nghiệp: Cấp quyền, xác thực và kiểm định là những thành phần cần thiết để cung cấp một tài nguyên an toàn cho người sử dụng mức xí nghiệp. Sử dụng WPA để xác thực người sử dụng, thường thông qua một máy chủ RADIUS. Trong quá trình xác thực, người sử dụng nhận được một khoá cái (primary master key-PMK), khoá này sau đó được sử dụng để thiết lập thuật toán mã hoá được sử dụng bởi TKIP. Do PMK được sinh ra như là kết quả của quá trình xác thực, không cần những mật khẩu được lưu cục bộ.

Ngoài ra thông tin xác thực được đưa qua một kênh mã hoá để bảo vệ trước những kẻ nghe trộm.

- Mức người dùng: WPA không chỉ là một giải pháp mức xí nghiệp, nó cũng được dùng để đảm bảo an toàn cho những người sử dụng SOHO. Môi trường này không thực sự cần tới một máy chủ xác thực, do đó, WPA phải có một phương pháp nào đó để tạo PMK được sử dụng để khởi tạo quá trình mã hoá TKIP. Giải pháp này được tạo ra bằng cách sử dụng một mật khẩu được chia sẻ trước đã được cấu hình trước trong AP và tất cả các nút. Ở mức này WPA với chế độ khoá chia sẻ trước PSK (Pre-shared Key) dễ bị tấn công hơn khi sử dụng WPA ở mức xí nghiệp.

WPA-PSK trông có vẻ làm việc giống như WEP. Người sử dụng thiết lập AP bằng cách lựa chọn WPA-PSK và nhập một mật khẩu hay passphrase. Sau đó, anh ta thực hiện những thao tác tương tự trên thiết bị không dây, khởi động kết nối, và có thể lướt an toàn trên internet. WPA không chỉ bao gồm tất cả những thành phần và những rắc rối của WEP (như KSA, PRGA, XOR, và ICV), mà nó còn bổ sung thêm những thuật toán và những công nghệ khác như MD5, SHA-1, HMAC, PMK, PTK..

3.5.3. Quản lý khoá trong WPA

WPA kết hợp một hệ thống quản lý khoá và tạo khóa mạnh, kết hợp quá trình xác thực và những hàm toàn vẹn dữ liệu. Sử dụng giao thức 802.1x/EAP, một khoá chủ được tạo một cách tự động. Sau việc tạo PMK, quá trình trao đổi khoá được xem là quá trình bắt tay 4 chiều, và bắt tay GTK (Group Key). Bắt tay 4 chiều và GTK là những bắt tay an toàn được sử dụng để thiết lập và cài đặt những khoá truyền được sử dụng giữa một client không dây và một AP trong phiên, gồm những khoá mã hoá TKIP. Nó là một quá trình trao đổi 4 gói tin của những tin khoá EAPOL. Những gói khoá EAPOL 802.1x được sử dụng để phân phối những khoá trên mỗi phiên tới những client không dây đã được xác thực thành công. Phải lưu ý rằng những khoá truyền này là tạm thời, và

chỉ kéo dài khi một client không dây được kết hợp và xác thực tới một AP. WPA bổ sung một yếu tố xác định khả năng an toàn mạng trong những khung 802.11 để phân loại thông qua những nhân tố thông tin WPA (trong khung) phương pháp xác thực yêu cầu (802.1x hay khoá chia sẻ trước) và mã hoá phù hợp (WEP, TKIP, AES). Những yếu tố thông tin WPA sẵn có trong những khung sau: những khung báo hiệu (AP tới tất cả client trong BSS), đáp ứng thăm dò (AP tới client không dây), yêu cầu kết hợp (client tới AP) và các yêu cầu tái kết hợp. Client không dây sẽ lấy những thông tin này từ những yếu tố thông tin WPA để xác định phương pháp cấp quyền và mã hoá phù hợp.

3.5.4. Đánh giá chung về giải pháp an toàn WPA

WPA không phải là một giải pháp hoàn hảo, nó bộc lộ một số giới hạn, Trước hết, nó dễ bị những tấn công DoS. Như đã đề cập ở trên, giao thức TKIP triển khai hai biện pháp đối phó để hạn chế những yếu kém trong thuật toán Michael. Khi hai gói dữ liệu có lỗi MIC trong một chu kỳ 60 giây, một AP, giả sử đang chịu một tấn công chủ động, sẽ giải kết hợp tất cả client được kết hợp tới nó. Kết quả, kết nối mạng sẽ ngưng trong 60 giây. Tuy nhiên, một kẻ tấn công sẽ không thể tìm ra thông tin về những khoá mã hoá. Ngoài ra, 802.11i (gồm cả WPA) không giải quyết yếu kém an toàn bằng một vài giao thức EAP như LEAP và PEAP.

WPA thực thi an toàn WLAN hơn WEP. Hầu hết những lỗ hổng được đưa ra trong WEP đã được WPA xử lý, TKIP tăng đáng kể sức mạnh và độ phức tạp của mã hoá không dây, làm cho một kẻ tấn công thêm khó khăn khi muốn đột nhập vào một WLAN. Thông qua WPA, những biện pháp an toàn không dây được mở rộng gồm: kích cỡ khoá, số lượng khoá sử dụng bằng cách bổ sung thêm việc tạo khoá động trên mỗi gói tin, một mã hoá mạnh hơn (TKIP), tạo ra một cơ chế kiểm tra toàn vẹn và kết hợp xác thực lẫn nhau. WPA giải quyết và loại bỏ những tấn công thụ động và bị động được biết. MIC có thể dò ra bất kỳ những biến đổi tin nào, do đó loại bỏ những tấn công

như lật bít, dùng lại, quy nạp. Nhờ thuật toán trộn khoá TKIP, việc khôi phục những dòng khoá WEP là không thể thực hiện được. Những khôi phục khoá WEP dựa trên cơ sở từ điển cũng không thể thực hiện được, bởi vì kẻ tấn công không thể đoán thêm gì được nữa. Việc phá WEP cũng bị đánh bại bằng thuật toán trộn khoá TKIP. WPA cũng cung cấp trợ giúp cho việc dò những AP giả mạo.

Vậy cụ thể WPA giải quyết những yếu kém của WEP như thế nào?

- Vectơ khởi tạo yếu kém và những va đập

Gía trị vectơ khởi tạo được sử dụng để cung cấp cho mỗi gói tin một khoá duy nhất (vectơ khởi tạo cộng với một khoá chia sẻ trước). Khoá duy nhất này tạo ra một trở ngại nghiêm trọng cho bất kỳ một kẻ tấn công nào, đơn giản bởi vì mỗi gói tin phải được xử lý như là một mục tiêu duy nhất. Crack mật khẩu của một gói tin chỉ cung cấp truy cập tới gói tin đó mà thôi.
WEP sử dụng vectơ khởi tạo chỉ có 24 bít, do đó vectơ khởi tạo sau vài giờ sẽ bị lặp lại, tạo ra lỗ hổng được gọi là những va đập (collision), từ đó kẻ tấn công có thể dễ dàng giành quyền truy cập dữ liệu.

WPA khắc phục nhược điểm này của WEP bằng cách tăng kích cỡ vectơ khởi tạo lên 48 bít, cung cấp ít nhất 900 năm dùng mật khẩu không lặp lại, loại bỏ lỗ hổng va đập trong WEP.

WPA thay đổi giá trị vectơ khởi tạo. Mặc dù cũng sử dụng cùng thuật toán như WEP nhưng do kiểm soát được giá trị vectơ khởi tạo ở đầu vào thuật toán nên nó lấp được những lỗ hổng an toàn trong WEP. Ngoài ra, mật khẩu mới được thay đổi một cách tự động sau mỗi 10,000 gói tin.

- Gía trị kiểm tra tính toàn vẹn (ICV)

WEP sử dụng một giá trị kiểm tra tính toàn vẹn ICV (Integrity Check Value) để đảm bảo rằng những gói tin không bị sửa đổi trong suốt quá trình truyền. Gía trị kiểm tra tính toàn vẹn này không mấy an toàn. Để khắc phục nhược điểm này, WPA sử dụng thuật toán Michael, tạo ra một giá trị toàn vẹn

duy nhất, sử dụng những địa chỉ MAC của bên nhận và bên gửi. Tuy nhiên, Michael sử dụng một sơ đồ mã hoá đơn giản có thể bị phá bằng những tấn công kiểu bắt ép thô bạo. Để chống lại tấn công này, nếu như Michael dò ra nhiều hơn hai gói tin không hợp lệ trong vòng chưa đầy một phút, nó sẽ treo mạng trong một phút và khởi động lại tất cả các mật khẩu. Tuy nhiên, biện pháp này lại mở cửa cho những kẻ tấn công thực hiện một kiểu tấn công từ chối dịch vụ bằng cách chèn thêm những gói tin lỗi, tuy nhiên, để có thể thực hiện được điều này, kẻ tấn công trước hết phải trải qua nhiều tầng bảo vệ khác nhau.

- Giả mạo và dùng lại (Forgery and Replay)

WEP không có biện pháp bảo vệ chống lại những tấn công giả mạo hay dùng lại. Bất kỳ kẻ tấn công nào đều có thể chèn gói tin nào đó vào trong một mạng. Ngoài ra, một kẻ tấn công có thể sử dụng lại một gói tin thu được trong việc chèn thêm này. WPA chống lại những tấn công kiểu này thông qua một giá trị IV 48 bít.

Trước hết, IV được tạo ra sử dụng những địa chỉ MAC của card mạng gửi và một giá trị đếm chuỗi. Kỹ thuật này ngăn chặn những tấn công giả mạo bởi vì một kẻ tấn công phải biết MAC và những giá trị IV được mã hoá trong gói tin. Thứ hai, IV bao gồm một bộ đếm chuỗi. Khi một gói tin được nhận, gía trị đếm của nó phải nằm trong phạm vi chấp nhận được nếu không nó sẽ bị bỏ qua. Kết quả, những tấn công dùng lại sẽ không thể thực hiện được.

- Xác thực người sử dụng

WEP không đưa ra nhiều cách thức xác thực. Có thể thiết lập một hệ thống xác thực chia sẻ, tuy nhiên sử dụng phương pháp này mở ra những nguy cơ an toàn khác. Để giải quyết vấn đề này, WPA hỗ trợ xác thực thông qua giao thức xác thực tăng cường 802.1x qua LAN (EAPoL - Extensible Authentication Protocol over LAN), thường bằng một máy chủ RADIUS.

3.5.5. WPA2 (Wi-Fi Protect Access 2)

WPA2 được Wi-Fi Alliance công bố vào tháng 9 năm 2004. Nó dựa trên cơ sở phiên bản sửa đổi cuối cùng của chuẩn 802.11i. WPA2 là thế hệ thứ hai của an toàn WPA tích hợp cơ chế mã hoá tiên tiến hơn, sử dụng giao thức CCMP (Counter –Mode/CBC-MAC) được gọi là AES (Advanced Encryption Standard) [24]. Xác thực WPA2 vẫn sử dụng sơ đồ xác thực 802.1x/EAP được nêu trong WPA. Tuy nhiên, chuẩn 802.11i đầy đủ kết hợp EAP qua một giao thức LAN Ethernet (EAPOL) cho phép client xác thực trước với AP. Điều này được thực hiện bằng cách gửi một xác nhận client thông qua một LAN hữu tuyến, khiến dễ dàng hơn cho việc thực hiện roam giữa những AP và từ những môi trường hữu tuyến tới những môi trường không dây. Ngoài ra, WPA2 tương thích trở lại và tích hợp hoạt động với những sản phẩm được xác nhận Wi-Fi cho WPA.

CCMP dựa trên cơ sở AES mới được đưa ra đã nhận được sự xem xét đánh giá kỹ lưỡng của các chuyên gia mật mã trên toàn thế giới. AES đáp ứng những yêu cầu an toàn chính phủ Mỹ, và được chấp nhận như là một chuẩn mã hoá phù hợp. CCMP là một thuật toán mạnh không tương thích với phần cứng vận hành WEP trước đó và sẽ yêu cầu những thay đổi về giao thức và phần cứng. CCMP cung cấp mã hoá (độ tin cậy), toàn vẹn tin mạnh hơn TKIP, và cũng bảo vệ trước tấn công dùng lại. Tương lai của những triển khai WLAN dịch chuyển theo hướng dùng CCMP.

AES được NIST lựa chọn nhờ sức mạnh mật mã của nó, và tính dễ dàng thực hiện. Được tạo ra từ thuật toán Rijndael [25], AES là một mã hoá đơn giản sử dụng một tính toán hoán vị – thay thế. Nó được triển khai với cả phần cứng hoặc phần mềm, và yêu cầu rất ít bộ nhớ. AES là một kỹ thuật mã hoá khoá đối xứng sử dụng một phương pháp mã khối để mã hoá những bít dưới dạng khối bản rõ, được tính toán độc lập. Mỗi khối có kích cỡ 128 bít, và triển khai một khoá có độ dài 128 bít. AES hoạt động trên một mảng byte 4x4 được

gọi là một trạng thái. Với WPA2, có 10 vòng, và 4 giai đoạn tạo một vòng. Bốn giai đoạn này gồm:

- Những byte phụ (một phép thay thế phi tuyến)- mỗi byte được thay thế bằng byte khác theo một bảng đối chiếu.

- Dịch hàng (ShiftRows) - bước chuyển vị – mỗi hàng của trạng thái được dịch chuyển vòng tròn qua một số bước nhất định.

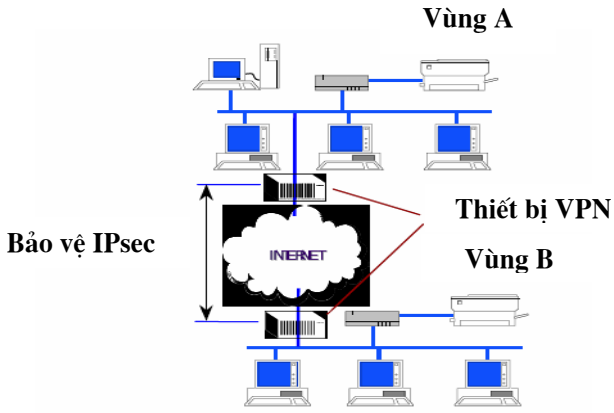
- Trộn cột (MixColumns) – một bước trộn – một phép trộn được thực hiện trên những cột của trạng thái, kết hợp 4 byte trong mỗi cột sử dụng một phép biến đổi tuyến tính.

- Cộng khoá vòng (AddRoundKey) – phép XOR – mỗi byte của trạng thái được kết hợp với một byte của vòng khoá phụ sử dụng phép XOR.

Cho đến năm 2005, vẫn chưa có tấn công thành công nào chống lại được AES. AES là một thuật toán mật mã cực kỳ an toàn. Vào tháng 4/2006, WPA2 sẽ mang tính bắt buộc với những sản phẩm không dây được xác nhận logo Wi-Fi.

3.6. Mạng riêng ảo VPN cho WLAN

Công nghệ mạng riêng ảo là công nghệ đang phát triển nhanh chóng cung cấp truyền dữ liệu an toàn trong những cơ sở hạ tầng mạng. VPN (Virtual Private Network) thường được sử dụng trong 3 trường hợp khác nhau: đối với truy cập người sử dụng từ xa, đối với kết nối LAN-to-LAN, và đối với Extranet. VPN triển khai những kỹ thuật mật mã để bảo vệ thông tin IP khi nó truyền từ một mạng sang mạng kế tiếp hoặc từ một vị trí tới vị trí kế tiếp. Dữ liệu bên trong "đường hầm" VPN được mã hoá và tách rời khỏi lưu lượng mạng khác. Một VPN cho kết nối site-to-site được minh hoạ ở hình dưới đây. Trong trường hợp này, lưu lượng truyền từ vùng A sang vùng B được bảo vệ khi nó di chuyển trong Internet.



Hình 3.9: Bảo vệ bằng VPN

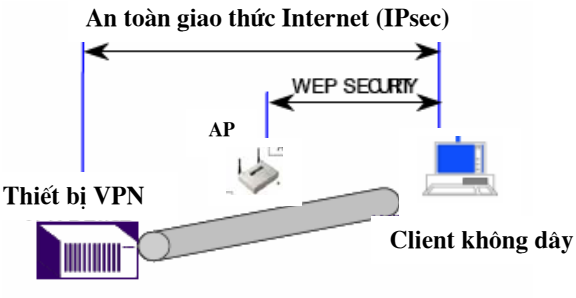
Hầu hết các VPN sử dụng ngày nay tận dụng bộ giao thức IPsec. IPsec được phát triển bởi IETF (Internet Engineering Task Force), là một khung của những chuẩn mở để đảm bảo truyền tin riêng qua những mạng IP. Nó cung cấp những kiểu bảo vệ sau:

- Độ tin cậy.
- Tính toàn ven.
- Xác thực nguồn gốc dữ liệu.
- Bảo vệ phân tích lưu lượng.

Tính toàn vẹn phi kết nối đảm bảo một tin nhận được không bị thay đổi so với tin gốc. Xác thực nguồn gốc dữ liệu đảm bảo tin nhận được gửi đi từ tác giả thực của nó chứ không phải bởi kẻ giả mạo nào khác. Bảo vệ dùng lại (replay) đảm bảo cùng một tin không được truyền nhiều lần và các tin không bị xáo trộn khi truyền. Độ tin cậy đảm bảo những người khác không thể đọc thông tin trong tin truyền. Bảo vệ phân tích lưu lượng đảm bảo gián điệp không thể xác định được người đang truyền tin hoặc tần số hay khối lượng truyền tin. Đầu ESP (Encapsulating Security Protocol) cung cấp tính riêng tư và bảo vệ chóng lại những thay đổi có ác ý, và header xác thực (AH-Authentification Header) bảo vệ chống lại sự thay đổi nhưng không cung cấp tính riêng tư. Giao thức IKE (Internet Key Exchange) [26] cho phép những

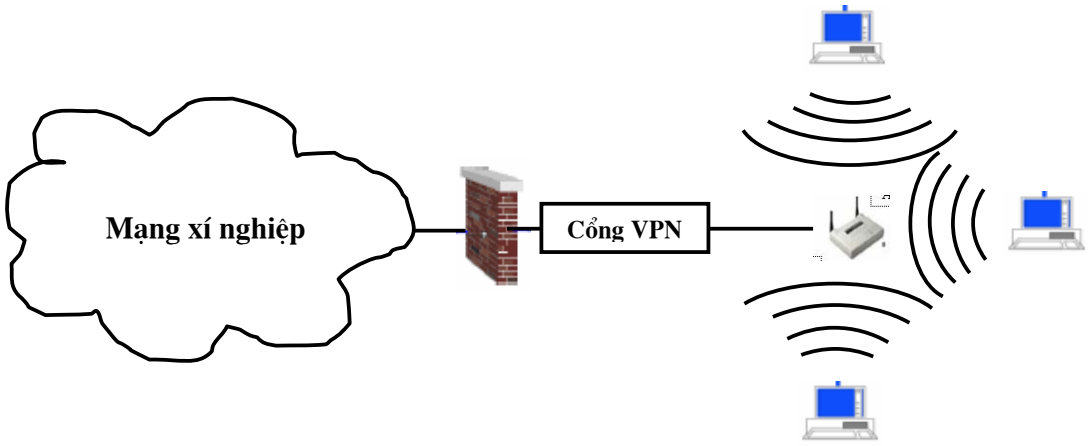
khoá mật và những tham số có liên quan tới những bảo vệ khác được trao đổi trước cho một cuộc truyền tin mà không cần có sự can thiệp của người sử dụng.

Việc sử dụng IPsec với WLAN được mô tả ở hình dưới đây:



Hình 3.10: An toàn VPN

Như minh hoạ ở trên, đường ống IPsec được cung cấp từ client không dây qua AP tới thiết bị VPN. Với IPsec, các dịch vụ an toàn được cung cấp ở tầng mạng của ngăn giao thức. Điều này có nghĩa tất cả những ứng dụng và những giao thức hoạt động trên tầng đó (ví dụ trên tầng 3) được bảo vệ bởi IPsec. Các dịch vụ an toàn IPsec là độc lập với an toàn xuất hiện ở tầng thứ 2, an toàn WEP. Với chiến lược phòng thủ sâu, thì nên có cả VPN và IPsec. Ở hình trên, VPN mã hoá dữ liệu được truyền tới và từ mạng có dây.



Hình 3.11: Bảo vệ WLAN bằng VPN

Hình trên minh hoạ một ví dụ khác về một mạng không dây với "vật phủ VPN". Như minh hoạ, với những thiết bị không dây được trang bị VPN, các client có thể kết nối an toàn tới mạng doanh nghiệp thông qua một cổng VPN. Các client không dây thiết lập những kết nối IPsec tới cổng VPN không dây-bổ sung cho hoặc thay thế WEP. Lưu ý rằng client không dây không cần phần cứng đặc biệt; nó chỉ cần được cung cấp với phần mềm client IPsec/VPN. Cổng VPN có thể sử dụng những khoá mật mã được chia sẻ trước hoặc những xác minh số (dựa trên cơ sở khoá công khai) cho xác thực thiết bị client không dây. Một tổ chức sử dụng những khoá chia sẻ trước cho một giải pháp VPN sẽ phải đối mặt với những vấn đề phân phối khoá tương tự như ở WEP. Ngoài ra, xác thực người sử dụng với một cổng mạng riêng ảo VPN có thể xuất hiện việc sử dụng dịch vụ người sử dụng quay số xác thực từ xa (RADIUS) hay những mật khẩu on time (OTP). Cổng mạng riêng ảo có thể hoặc không thể có một tường lửa trọn vẹn để giới hạn lưu lượng tới những vị trí nhất định trong mạng. Ngày nay, hầu hết các thiết bị VPN có tường lửa kết hợp cùng làm việc để bảo vệ toàn mạng khỏi truy cập không được quyền và dữ liệu người sử dụng truyền qua mạng. VPN và tường lửa kết hợp sẽ tiết kiệm chi phí và giảm gánh nặng quản trị. Ngoài ra, cổng VPN có thể hoặc không thể có khả năng tạo một nhật ký kiểm tra mọi hoạt động. Một dấu vết kiểm tra là một bản ghi theo thứ tự thời gian về các hoạt động của hệ thống để có thể khôi phục lại và kiểm tra chuỗi các môi trường và các hoạt động. Một nhà quản lý an toàn có thể sử dụng một vết kiểm tra trên cổng VPN để giám sát sự tuân thủ chính sách an toàn và hiểu được liệu chỉ có những người được quyền mới có quyền truy cập vào mạng không dây.

Cũng cần lưu ý rằng mặc dù phương pháp VPN tăng cường an toàn giao diện truyền trong môi trường không khí, tuy nhiên, phương pháp này không hoàn toàn giải quyết vấn đề an toàn cho mạng doanh nghiệp. Ví dụ, xác thực và cấp quyền cho những ứng dụng xí nghiệp không phải lúc nào cũng được

giải quyết bằng giải pháp an toàn này. Một số thiết bị VPN có thể sử dụng những chính sách người sử dụng cụ thể yêu cầu xác thực trước khi truy cập tới những ứng dụng mức xí nghiệp. Các cơ quan mong muốn tìm kiếm sự hỗ trợ trong việc phát triển một chiến lược an toàn mức xí nghiệp tổng thể.

Đối với những mạng cục bộ không dây khi những lỗ hổng của WEP tĩnh bị khám phá, VPN đã nhanh chóng được đưa ra như là một cách để đảm bảo an toàn dữ liệu truyền qua mạng WLAN. VPN là một giải pháp cực kỳ tốt để đảm bảo an toàn khi truyền dữ liệu trên một mạng có nhiều kẻ thù như Internet (mặc dù chất lượng của những thực thi VPN là không giống nhau). Tuy nhiên, nó không cần thiết là giải pháp tốt nhất để đảm bảo an toàn cho những WLAN nội bộ. Đối với loại ứng dụng này, một VPN đưa ra ít hơn hoặc không đưa ra tính chất an toàn bổ sung gì so với những giải pháp 802.1x trong khi đó lại làm tăng một cách đáng kể độ phức tạp và chi phí, giảm khả năng sử dụng.

Lưu ý: điều này không giống với việc sử dụng VPN để đảm bảo an toàn lưu lượng truyền qua những hotspots. Việc bảo vệ dữ liệu mạng của những người sử dụng kết nối qua những mạng từ xa là một sử dụng VPN hợp lý.

3.6.1. Những ưu điểm sử dụng VPN bảo vệ WLAN

- Hầu hết các tổ chức đã có một giải pháp VPN được triển khai do vậy những người sử dụng và nhân viên IT sẽ thấy quen với phương pháp này.

- Bảo vệ dữ liệu VPN thường sử dụng mã hoá phần mềm cho phép những thuật toán được thay đổi và cập nhật một cách dễ dàng hơn mã hoá dựa trên cơ sở phần cứng.

- Bạn có thể sử dụng phần cứng với chi phí thấp hơn bởi vì bảo vệ VPN là độc lập với phần cứng WLAN.

3.6.2. Nhược điểm sử dụng VPN

- VPN thiếu tính trong suốt người sử dụng. Những client VPN thường yêu cầu người sử dụng khởi tạo bằng tay một kết nối tới máy chủ VPN; do đó, kết nối này sẽ không bao giờ trong suốt như một kết nối hữu tuyến. Những client không phải Microsoft cũng có thể khởi động cho những xác minh đăng nhập tại kết nối ngoài mạng chuẩn hay đăng nhập miền. Nếu như VPN ngắt kết nối, do một tín hiệu WLAN nghèo nàn hay do người sử dụng roam giữa các AP, người sử dụng sẽ phải kết nối lại.

- Do kết nối VPN chỉ là khởi tạo người sử dụng, một máy tính giả mạo không đăng nhập sẽ không thể kết nối tới VPN. Do đó, một máy tính không thể bị quản lý từ xa hay bị theo dõi từ xa trừ khi một người sử dụng đã đăng nhập vào. Những thiết lập GPO (Group policy object) máy tính nhất định, như những mã khởi động và máy tính được gán phần mềm sẽ không bao giờ được áp dụng.

- Những hiện tượng roaming, những mã đăng nhập, và phần mềm được triển khai tới người sử dụng sử dụng GPO có thể không làm việc được như mong đợi. Trừ khi người sử dụng lựa chọn để đăng nhập sử dụng kết nối VPN từ khởi động đăng nhập Windows, máy tính sẽ không kết nối tới LAN liên hợp cho đến sau khi người sử dụng đã đăng nhập và khởi động kết nối VPN. Với một client VPN không phải Microsoft, không thể thực hiện một đăng nhập miền đầy đủ qua một kết nối VPN.

- Sự khởi đầu lại từ chế độ standby hay chế độ nghỉ không tự động thiết lập lại kết nối VPN; người sử dụng phải thực hiện điều này bằng tay.

- Mặc dù dữ liệu bên trong đường hầm VPN được bảo vệ, VPN không đưa ra sự bảo vệ cho bản thân WLAN. Một kẻ tấn công vẫn có thể gia nhập vào WLAN và cố gắng thăm dò hay tấn công bất kỳ thiết bị nào được gắn tới WLAN.

- Những máy chủ VPN có thể trở thành một nút cổ chai. Tất cả client WLAN truy cập tới LAN liên hợp được chuyển qua máy chủ VPN. Những thiết bị VPN phục vụ một số lượng lớn những client từ xa tốc độ thấp; do vậy, hầu hết các cổng VPN sẽ không thể đối mặt với hàng chục hay hàng trăm client chạy ở tốc độ LAN tối đa.

- Chi phí cho việc bổ sung phần cứng và quản lý những thiết bị VPN chắc chắn cao hơn nhiều một giải pháp WLAN đơn thuần. Mỗi một vùng sẽ phải cần tới máy chủ VPN của chính nó ngoài những AP WLAN.

- Những phiên VPN thiên về ngắt kết nối khi những client roam giữa những AP. Mặc dù những ứng dụng sẽ thường phải chịu một ngắt kết nối tạm thời khi chuyển mạch những AP không dây, những phiên VPN sẽ thường xuyên bị phá vỡ, yêu cầu người sử dụng tái kết nối lại bằng tay.

- Chi phí của máy chủ VPN và những cấp phép phần mềm client, cũng như chi phí triển khai phần mềm, có thể là một vấn đề với những giải pháp VPN không phải là Microsoft. Bạn cũng có thể phải quan tâm tới tương thích phần mềm client VPN bởi những client không phải Microsoft thường thay thế chức năng Windows chính.

Nhiều nhà phân tích và nhà sản xuất cho rằng an toàn VPN thường tốt hơn an toàn WLAN. Mặc dù điều này là đúng cho WEP tĩnh, nhưng không hoàn toàn với những giải pháp dựa trên cơ sở EAP 802.1x. Những phương pháp xác thực VPN, cụ thể, thường kém an toàn hơn và không mạnh hơn. Ví dụ, những giải pháp WLAN được hỗ trợ bởi Microsoft sử dụng cùng phương pháp xác thực EAP giống như những phương pháp VPN của nó (EAP-TLS và MS-CHAP v2). Nhiều thực thi VPN, đặc biệt là những thực thi dựa trên cơ sở chế độ đường hầm IPsec, sử dụng xác thực khoá chia sẻ (một mật khẩu nhóm). Điều này tạo ra những lỗ hổng an toàn nghiêm trọng giống như WEP tĩnh.

Một VPN không làm điều gì để đảm bảo an toàn cho bản thân WLAN. Mặc dù dữ liệu bên trong những đường hầm VPN là an toàn, bất kỳ ai vẫn có thể xâm nhập vào WLAN và cố gắng tấn công những client hợp pháp và những thiết bị khác trên WLAN.

VPN phù hợp nhất để đảm bảo an toàn cho lưu lượng truyền qua những mạng công cộng, ở đó người sử dụng đang kết nối qua một kết nối băng thông rộng gia đình hoặc từ một hotspot không dây. Tuy nhiên, VPN chưa bao giờ được thiết kế để đảm bảo an toàn lưu lượng mạng trên những mạng bên trong. Đối với hầu hết các tổ chức, VPN trong vai trò của nó sẽ qúa cồng kềnh và hạn chế về mặt chức năng cho người sử dụng và quá đắt đỏ và phức tạp cho phòng IT để có thể duy trì nó. Trong những trường hợp ngoại lệ ở đó an toàn cao hơn cho một kết nối cụ thể hay kiểu lưu lượng cần thiết, điều này có thể được cung cấp bởi một đường hầm VPN hoặc chế độ vận tải IPsec ngoài bảo vệ WLAN đơn thuần.

CHƯƠNG 4: TRIỂN KHAI WLAN AN TOÀN TRONG MÔI TRƯỜNG GIÁO DỤC

4.1. Vai trò tiềm năng của WLAN trong giáo dục

Mạng cục bộ dựa trên công nghệ không dây sẽ đóng một phần quan trọng trong việc phát triển cơ sở hạ tầng công nghệ thông tin tại các trường cao đẳng và đại học trong một vài năm tới. Nó đặc biệt hữu ích đối với những môi trường giáo dục mong muốn mở rộng hệ thống mạng hiện hành của họ sang các khu vực mới xây dựng, bởi vì công nghệ WLAN chắc chắn sẽ là một cách thức hiệu quả nhất về chi phí cho việc mở rộng hệ thống mạng cũng như kéo theo nó là sự gia tăng đồng thời số lượng người sử dụng.

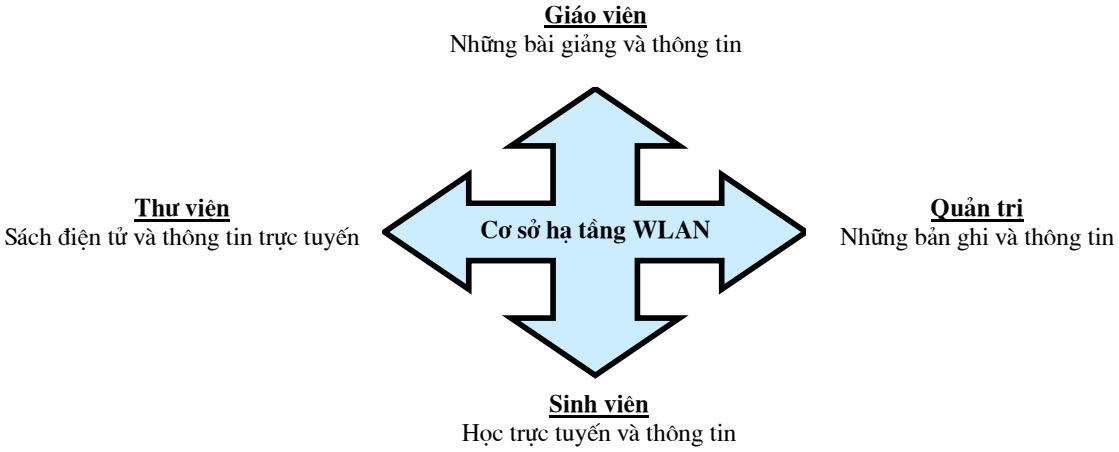
Ngoài những lợi ích về mặt kinh tế, WLAN cũng cung cấp cấp tính cơ động hơn so với LAN hữu tuyến vì những lý do sau:

Thứ nhất, WLAN cung cấp tính cơ động vật lý, bởi vì bất kỳ đâu trong không gian giáo dục người sử dụng làm việc, họ vẫn có thể sử dụng hệ thống mạng. Với một mạng hữu tuyến, điều này chỉ có thể thực hiện được bằng cách phải quyết định vị trí đặt máy tính và cài đặt những socket mạng tại nơi đó. Thường việc sử dụng không gian thay đổi theo thời gian, và khi đó, với triển khai hữu tuyến ta phải đặt lại đường cáp, còn đối với công nghệ không dây điều này không cần thiết, nó hoàn toàn có thể đáp ứng được trước những thay đổi đó.

Thứ hai, với một mạng hữu tuyến, số lượng tối đa người sử dụng phải được xác định khi không gian được lắp dây dẫn và số lượng phù hợp những socket mạng được cài đặt. Điều này đồng nghĩa với việc có quá nhiều socket mạng được cài đặt, dẫn đến tốn kém tiền bạc, và khi cầu vượt quá cung một số người sử dụng không thể sử dụng mạng. Với một mạng không dây, mặc dù hiệu năng mạng cũng sẽ giảm khi lượng sử dụng tăng, trừ khi có một nhu cầu rất cao tất cả người sử dụng cùng truy cập mạng.

Thứ ba, mạng không dây có thể đến với những nơi mà mạng hữu tuyến không thể đến được, như những phạm vi ngoài trời, do tín hiệu có thể bao trùm ở phạm vi hàng trăm mét từ các toà nhà.

Việc trang bị hệ thống mạng không dây ở khu trường đại học cho ta khả năng tương tác nhiều hơn giữa những giáo viên và những sinh viên. Họ có thể truy cập thông tin và những ứng dụng mạng dễ dàng hơn, ở bất kỳ đâu trong khuôn viên của trường. Ngoài ra, nó còn khuyến khích sử dụng những máy tính xách tay có trang bị công nghệ không dây của chính sinh viên, làm tăng khả năng học tập nghiên cứu của họ cũng như không gian học tập không bị gò bó trong lớp học mà vẫn đạt hiệu quả cao.



Hình 4.1: Truy cập thông tin có thể thực hiện bất kỳ đâu trong khuôn viên với công nghệ WLAN

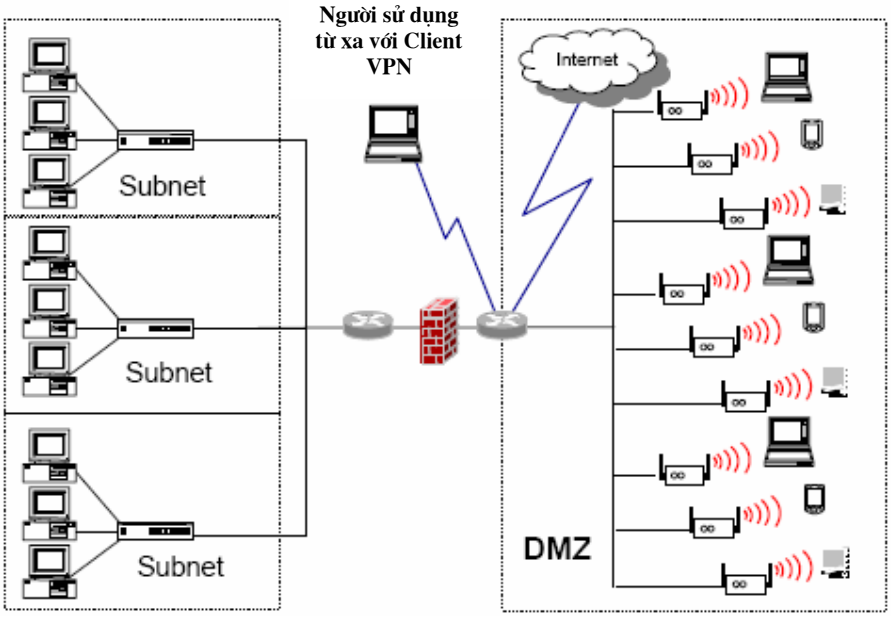
4.2. Lựa chọn giải pháp an toàn WLAN cho khu trường học

Ngoài những thuận lợi nêu trên của WLAN, cũng giống như với bất kỳ công nghệ mới nào khác, WLAN cũng có những vấn đề đi kèm với nó như khả năng đáp ứng trước những thay đổi nhanh chóng về những chuẩn công nghệ WLAN; vấn đề chia sẻ dải thông; và vấn đề an toàn.

An toàn là một vấn đề quan trọng trong WLAN, tuy nhiên không có nghĩa là không thể triển khai WLAN vì nó hổng hơn so với LAN hữu tuyến.

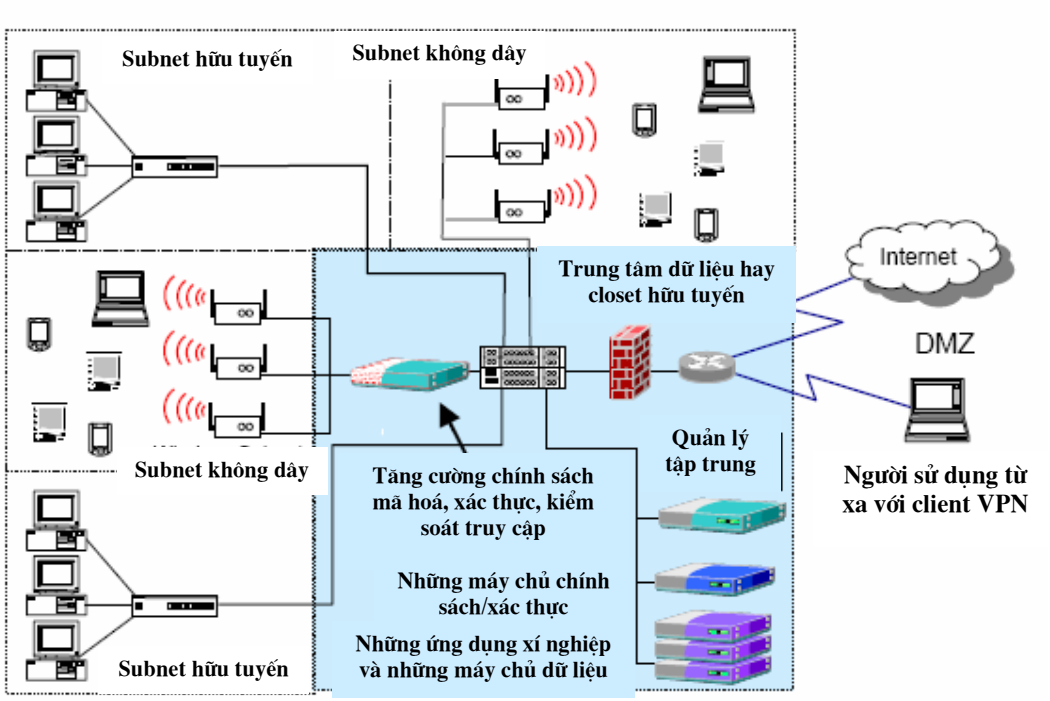
Bất kỳ mạng nào đều có những nguy cơ an toàn tiềm ẩn nếu như chúng ta không chú ý tới việc bảo vệ nó trước những tấn công. Đối với từng môi trường, mục đích sử dụng cụ thể, cần lựa chọn giải pháp an toàn phù hợp.

Trước đây, đối với những thiết kế WLAN cho một khu (campus) nào đó, không thể cung cấp roaming kết nối liên tục giữa những toà nhà, đặc biệt khi VPN được sử dụng để đảm bảo an toàn WLAN. Việc roaming giữa các toà nhà yêu cầu tương tác người sử dụng ở dạng treo và bắt đầu lại những ứng dụng khi họ di chuyển từ toà nhà này sang toà nhà khác. Chính vì thế, WLAN thường được xây dựng trên một subnet duy nhất.



Hình 4.2: Topo mạng WLAN truyền thống – tách rời những người sử dụng không dây sử dụng một subnet duy nhất.

Tuy nhiên, hiện nay chúng ta có thể thiết kế dịch vụ WLAN bao phủ toàn bộ khu nhà bằng hỗ trợ IP di động [27], một chuẩn sẽ cho phép roaming giữa các toà nhà.



Hình 4.3: Topo mạng WLAN với những phân đoạn mạng không dây và có dây đan xen, kết hợp chặt chẽ với những máy chủ chính sách và xác thực

Với sự phát triển của công nghệ WLAN trong giai đoạn hiện nay, sử dụng công nghệ VPN cho mã hoá mạnh giữa WLAN và mạng liên hợp cùng với triển khai xác thực để hỗ trợ kiểm soát truy cập sẽ cung cấp cho ta mức độ an toàn tốt nhất. Đây cũng chính là giải pháp được triển khai hầu hết ở các trường đại học trên thế giới có triển khai WLAN.

Những chuẩn an toàn WLAN đang nổi lên hiện nay, như TKIP và những chuẩn tương lai, như chuẩn mã hoá AES trong 802.11i sẽ là một giải pháp lâu dài để đảm bảo an toàn WLAN mà không cần đến mã hoá VPN.

4.3. Đề xuất thực thi WLAN an toàn tại trường kỹ thuật nghiệp vụ công an.

Hiện nay, mục đích triển khai WLAN tại trường kỹ thuật nghiệp vụ công an là mở rộng hệ thống mạng hữu tuyến hiện có sang các khu vực khác trong khuôn viên của Trường mà không cần phải thực hiện thiết kế và triển

khai đường cáp mạng. Sử dụng công nghệ WLAN sẽ giúp giảm bớt chi phí lắp đặt, mở ra khả năng nối mạng giữa những toà nhà hoặc giữa các tầng trong một toà nhà khó triển khai cáp, hoặc phải thực hiện những phá dỡ về xây dựng, kiến trúc..

Khi triển khai WLAN phải giải quyết hai vấn đề an toàn cơ bản , đó là:

- Xác thực (người sử dụng và thiết bị).
- Bảo mật thông tin trên đường truyền.

Triển khai WLAN với mục đích mở rộng hệ thống mạng LAN văn phòng và hệ thống mạng LAN thực tập chuyên ngành.

Đối với hệ thống mạng văn phòng có thể sử dụng những biện pháp an toàn WLAN cơ bản như đã đề cập ở trên như sử dụng WEP tĩnh, lọc.., hoặc có thể sử dụng giải pháp an toàn tốt hơn như WPA ở chế độ PSK.

Đối với hệ thống mạng thực tập chuyên ngành, do đặc thù, các biện pháp bảo vệ vật lý được chú ý hàng đầu để đảm bảo an toàn thiết bị mạng. Ngoài ra vấn đề bảo mật lưu lượng mạng (bảo mật thông tin truyền trong không khí) cũng là quan tâm chính khi triển khai WLAN cho mạng này. Sử dụng kỹ thuật mật mã mạnh để mã hoá thông tin truyền trên mạng là một biện pháp đảm bảo an toàn tốt nhất. Có thể sử dụng mật mã khoá đối xứng, với cơ sở hạ tầng khoá mã hoá/giải mã sẵn có, cung cấp cho bên truyền và bên nhận tin để thực hiện mã hoá/giải mã file truyền/nhận. Khi đó trên các client sẽ được cài đặt phần mềm mã hoá giải mã file.

Phần phụ lục sẽ trình bày một chương trình phần mềm minh hoạ mã hoá/giải mã file sử dụng mật mã khoá đối xứng.

KẾT LUẬN

Mạng WLAN sẽ là công nghệ mạng của tương lai. Tuy nhiên, do tính chất mở của mạng này, vấn đề an toàn cũng cần được đặt lên hàng đầu.

Hiện nay những công nghệ an toàn như WEP, lọc.. được xem là những công nghệ an toàn cơ sở, được triển khai cho WLAN từ thời kỳ bắt đầu của mạng này. Công nghệ mạng riêng ảo VPN và 802.1x được xem là công nghệ an toàn đang được áp dụng triển khai tại thời điểm hiện tại, và những công nghệ như 802.11i và WPA chính là sự lựa chọn của tương lai khi thực hiện triển khai WLAN. Tuy nhiên, việc lựa chọn công nghệ an toàn nào là phù hợp hoàn toàn phụ thuộc vào từng mục đích an toàn cụ thể. Đối với môi trường mạng yêu cầu tính bảo mật cao (như bảo mật thông tin quốc gia) thì cần lựa chọn giải pháp an toàn có sử dụng kỹ thuật mật mã và xác thực người dùng mạnh.

Qua tìm hiểu về mạng WLAN và những vấn đề an toàn cho mạng này tôi nhận thấy trong tương lai không xa, việc xây dựng dự án triển khai công nghệ WLAN an toàn cho trường đại học kỹ thuật công an nhân dân là hoàn toàn có thể thực hiện được. Đó cũng chính là một phần trong định hướng nghiên cứu tiếp theo của luận văn.

PHỤ LỤC CHƯƠNG TRÌNH MÃ HOÁ/GIẢI MÃ FILE

Chương trình mã hóa/giải mã File sử dụng kỹ thuật mã dòng đối xứng. File trước khi truyền được mã hóa bằng một khoá mật mã nhằm đảm bảo an toàn thông tin trên đường truyền. Tại nơi nhận, sẽ sử dụng khoá tương tự để giải mã. Chương trình hỗ trợ mã hoá file nén (Winzip); sử dụng phương pháp mật mã tăng cường MD5 và SHA để băm khoá, đảm bảo an toàn cao. Dưới đây là một số phần trong chương trình được xây dựng trên ngôn ngữ lập trình VB 6.0.

****

Phần mã hoá/giải mã dùng thuật toán mã dòng đối xứng

****

```
'Khởi tạo thuật toán
Public Sub RC4ini(Pwd As String)
Dim temp As Integer, Aini As Integer, bini As Integer
   'Lưu khoá trong mảng byte
   bini = 0
   For Aini = 0 To 255
      bini = bini + 1
      If bini > Len(Pwd) Then
         bini = 1
      End If
      kep(Aini) = Asc(Mid$(Pwd, bini, 1))
   Next Aini
   'Khởi tạo S-box
   For Aini = 0 To 255
      s(Aini) = Aini
   Next Aini
   bini = 0
```

```
    For Aini = 0 To 255
        bini = (bini + s(Aini) + kep(Aini)) Mod 256
        ' Swap( S(i),S(j) )
        temp = s(Aini)
        s(Aini) = s(bini)
        s(bini) = temp
    Next Aini
End Sub
'Chỉ sử dụng thủ tục này cho những text ngắn
Public Function EnDeCrypt(plaintxt As String) As String
Dim temp As Integer, rccounter As Long, i As Integer, j As Integer, k
As Integer
Dim TempArray() As Byte
Str2ByteArray plaintxt, TempArray
For rccounter = 1 To UBound(TempArray)
    i = (i + 1) Mod 256
    j = (j + s(i)) Mod 256
    ' Swap( S(i),S(j) )
    temp = s(i)
    s(i) = s(j)
    s(j) = temp
    'Tạo k byte khoá
    k = s((s(i) + s(j)) Mod 256)
    'Bytebảnrõ xor Bytekhoá
    TempArray(rccounter) = TempArray(rccounter) Xor k
Next rccounter
EnDeCrypt = StrConv(TempArray, vbUnicode)
End Function
```

```
'********** Thủ tục mã hoá/giải mã file **********
Private Sub EnDeCryptfile()
Dim eNr As Integer
Dim DNr As Integer
Dim Answer As Integer
Dim dCount As Double
Dim dRest As Double
Dim sTemp As String
Const CPY_BUFFER = 10240
On Error GoTo Error
'Thiết lập bộ đếm Set-Box về 0
i = 0: j = 0
If olefile = "" Then
path = SaveDialog(Me, "*.*", "Lua chon file de ma hoa/giai ma", App.path)
Else
path = olefile
End If
If path = "" Then
   txtpwd.SetFocus
   Exit Sub
End If
'In một text trạng thái
Form1.Caption = "Dang xu ly file"
'Disable the Mousepointer
MousePointer = vbHourglass
'Xoá màn hình
Form1.Refresh
```

```
        If Winzip And encrypt Then
           Call Zip
        End If
        eNr = FreeFile
        DNr = FreeFile + 1
        Open path For Binary As eNr
              If LOF(eNr) = 0 Then
           Close eNr
           GoTo Error
        End If
              If encrypt Then
        'Nếu như đã có file thì cảnh báo người sử dụng
           If FileExist(path + ".enc") Then
                    Answer = MsgBox("File " & path + ".enc da co - tiep tuc?",
vbYesNo, "Loi")
                    If Answer = vbYes Then
              SetAttr path + ".enc", vbArchive
           Else
              'Enable the Mousepointer
              MousePointer = vbDefault
              'Sẵn sàng!
              Form1.Caption = StatusCaption
              'Thiết lập Focus
              txtpwd.SetFocus
              Exit Sub
           End If
        End If
        Open path + ".enc" For Binary As DNr
```

```
            Else
            path = Left$(path, Len(path) - 4)
            'Nếu như đã có file này rồi thì cảnh báo người sử dụng
            If FileExist(path) Then
               Answer = MsgBox("File " & path + " da co - tiep tuc?", vbYesNo,
"Loi")
               If Answer = vbYes Then
                  SetAttr path, vbArchive
               Else
                  'Enable the Mousepointer
                  MousePointer = vbDefault
                  'Sẵn sàng!
                  Form1.Caption = StatusCaption
                  'Thiết lập Focus
                  txtpwd.SetFocus
                  Exit Sub
               End If
            End If
               Open path For Binary As DNr
         End If
         'Băm khoá (MD5 hoặc SHA)
         If Hash_Sel = "MD5" Then
            Call md5_hash_msg(txtpwd.Text)
            sign_msg = Trim(Str(Context.State(1))) + Trim(Str(Context.State(2)))
+ Trim(Str(Context.State(3))) + Trim(Str(Context.State(4)))
         Else 'Default Setting
            Call sha_hash_msg(txtpwd.Text)
```

```
            sign_msg = Trim(Str(bufA)) & Trim(Str(bufB)) & Trim(Str(bufC)) &
Trim(Str(bufD)) & Trim(Str(bufE))
        End If
        'Khởi tạo những S-Box chỉ một lần cho một file (với băm khoá)
        RC4ini (sign_msg)
        'Đọc file và mã hoá
        'Nếu như file lớn hơn 10Kb
        If LOF(eNr) > CPY_BUFFER Then
           sTemp = Space(CPY_BUFFER)
           dCount = Int(LOF(eNr) / CPY_BUFFER)
           dRest = LOF(eNr)
              For i = 1 To dCount
              Get eNr, , sTemp
              Put DNr, , EnDeCrypt(sTemp)
              dRest = dRest - CPY_BUFFER
           Next i
              sTemp = String(dRest, " ")
           Get eNr, , sTemp
           Put DNr, , EnDeCrypt(sTemp)
         'Nếu như file nhỏ hơn hoặc bằng 10 Kb
        ElseIf LOF(eNr) <= CPY_BUFFER And LOF(eNr) > 0 Then
           sTemp = Space(LOF(eNr))
           Get eNr, , sTemp
           Put DNr, , EnDeCrypt(sTemp)
        End If
        sTemp = Empty
        Close eNr
        Close DNr
```

```
        Close 1
        Close 2
        If FileExist(oldzipname) And encrypt Then Kill oldzipname
        'Tạo con trỏ chuột
        MousePointer = vbDefault
        'Sẵn sàng!
        Form1.Caption = StatusCaption
        'Thiết lập Focus
        txtpwd.SetFocus
        Error:
        End Sub
        Private Sub Zip()
        Dim zipname As String
        'Kiểm tra xem file đã được nén chưa
        If InStr(path, ".zip") > 0 Then GoTo Error
        If InStr(path, ".") > 0 Then
           'Xoá bổ sung mở rộng cũ .zip
           zipname = Chr(34) + Left$(path, Len(path) - 3) + "zip" + Chr(34) + "
"
           oldzipname = Left$(path, Len(path) - 3) + "zip"
        Else
              'Nếu như file không có bổ sung mở rộng .zip
           zipname = Chr(34) + zipname + ".zip" + Chr(34) + " "
           oldzipname = zipname + ".zip"
           'Kiểm tra xem đã có file nén chưa
           If FileExist(oldzipname) Then
              MsgBox "Da co mot file duoc nen: " + oldzipname, vbOKOnly,
"Loi!"
```

```
        GoTo Error
      End If
    End If
    'Khởi động Winzip
    ShellAndWait Winzippath + " " + zipname + Chr(34) + path + Chr(34)
    'Tên file nén
    'File để nén
    'Lưu đường dẫn mới bởi vì bây giờ muốn mã hoá file nén!
    If FileExist(oldzipname) Then
      path = oldzipname
    Else
      MsgBox "Khong the nen file...", vbOKOnly, "Loi!"
    End If
    Error:
    End Sub

    'Dùng cho Drag and Drop
    Private Sub Encryptb_OLEDragDrop(Data As DataObject, Effect As
Long, Button As Integer, Shift As Integer, x As Single, y As Single)
    Dim filecounter As Integer
    For filecounter = 1 To Data.Files.Count
      If (GetAttr(Data.Files.Item(filecounter)) And vbDirectory) = 0 Then
        olefile = Data.Files(filecounter)
        encrypt = True
        Call check
        End If
    Next
    End Sub
```

```
Private Sub Decrypt_OLEDragDrop(Data As DataObject, Effect As Long, Button As Integer, Shift As Integer, x As Single, y As Single)
Dim filecounter As Integer
For filecounter = 1 To Data.Files.Count
  If (GetAttr(Data.Files.Item(filecounter)) And vbDirectory) = 0 Then
    olefile = Data.Files(filecounter)
    encrypt = False
    Call check
    End If
Next
End Sub

Private Sub check()
'Kiểm tra lỗi
If txtpwd.Text = "" Then
  MsgBox "Ban can nhap khoa de ma hoa hoac giai ma", 0, "Loi!"
  txtpwd.SetFocus
  Exit Sub
ElseIf Len(txtpwd) < 8 Then
  MsgBox "Ban nen su dung khoa dai hon 7 ky tu!", 0, "Canh bao an toan"
End If
If Verify Then
  Ok.Visible = True
  Cancel.Visible = True
  temp = txtpwd
  txtpwd = ""
  txtpwd.SetFocus
```

```
   Form1.Caption = "Xac thuc khoa!"
Else
      Call EnDeCryptfile
End If
End Sub

'Dùng cho xác thực khoá
Private Sub Ok_Click()
If temp = txtpwd Then
   Ok.Visible = False
   Cancel.Visible = False
   Call EnDeCryptfile
Else
   Ok.Visible = False
   Cancel.Visible = False
   Form1.Caption = StatusCaption
   txtpwd = ""
   txtpwd.SetFocus
   Exit Sub
End If
Form1.Caption = StatusCaption
End Sub
```

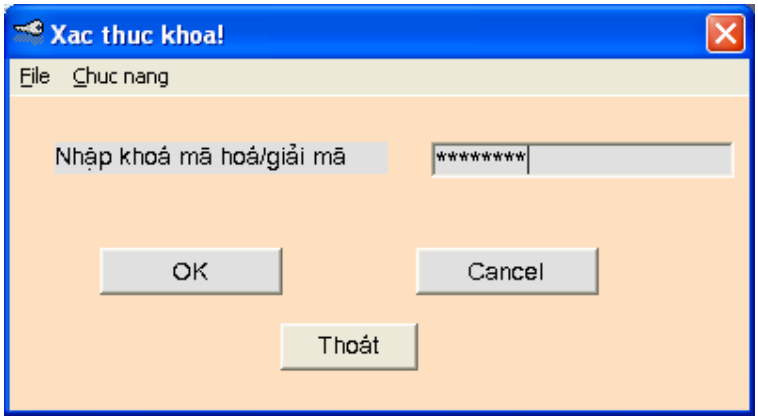
****

Thực hiện chương trình

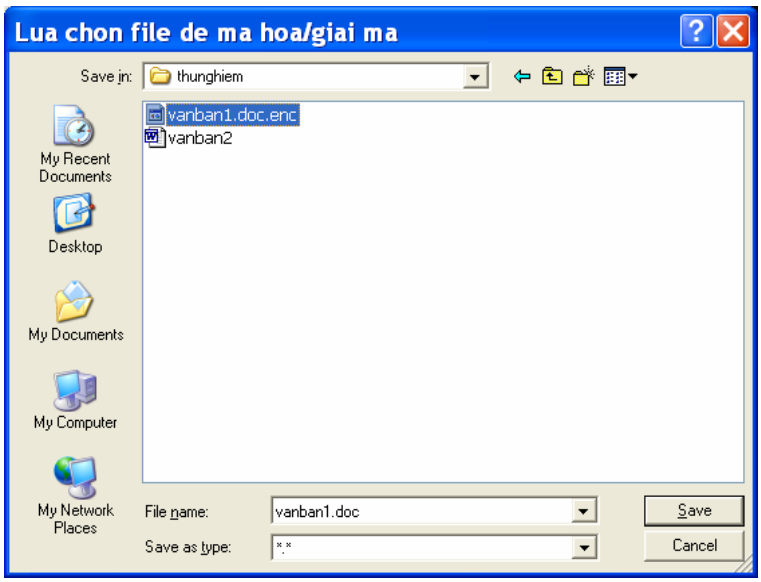
****

1. Nhập khoá mã hoá/giải mã

2. Thực hiện xác thực khoá mã hoá/giải mã (nếu chọn chức năng này)



3. Lựa chọn file để mã hoá/giải mã



TÀI LIỆU THAM KHẢO

[1]. Jim Geier (2002), *Improving WLAN Performance with RTS/CTS*, http://www.wi-fiplanet.com/tutorials/article.php/1445641.

[2]. Pejman Roshan Jonathan Leary (2003), *802.11 Wireless LAN Fundermentals*, Cisco Press.

[3]. MicrosoftTechnet (2002), *RADIUS Protocol Security and Best Practices*, http://www.microsoft.com/technet/prodtechnol/windows2000serv/maintain/security/radiussec.mspx#E2.

[4]. David Taylor (2000), *Intrusion Detection FAQ: Are there Vulnerabilites in VLAN Implementations? VLAN Security Test Report,* http://www.sans.org/resources/idfaq/vlan.php.

[5]. Jim Geier (2004), *What SSID is Right for You?,* http://www.wi-fiplanet.com/tutorials/article.php/3422271.

[6]. Sean Convery, Darrin Miller, Sri Sundaralingam (2003), *Wireless LAN Security in Depth*, Cisco SAFE White Paper.

[7]. Grace12 (2005), *Wireless LAN 802.11*, "Station Services", "Distribution System Services", http://wiki.ittoolbox.com/index.php/Topic:802.11,

[8]. Ilenia Tinnrello, Giuseppe Bianchi, Luca Scalia, "Performance Evaluation of Differentiated Access Mechanisms Effectiveness in 802.11 Network", University degli studi di Palermo, Dipartimento di Ingegneria Elettrica Viale delle scienze, 90128, Palemo, Italy.

[9]. Plamen Nedeltchev (2001), "The Hidden Station Challenge", *Wireless Local Area Networks and the 802.11 standard*, Felicia Brych, pp. 13-15.

[10]. NIST (1999), *An Introduction to Computer Security*, Special Publication 800-12.

[11]. Alfred J. Menezes, Paul C. VanOorschot, Scott A. Vanstore (2000), "Digital Signatures", *Handbook of Applied Cryptography, CRC Press*, pp. 425-489.

[12]. Alfred J. Menezes, Paul C. VanOorschot, Scott A. Vanstore (2000), "Block Cipher", *Handbook of Applied Cryptography, CRC Press*, pp. 223-283.

[13]. Alfred J. Menezes, Paul C. VanOorschot, Scott A. Vanstore (2000), "Stream Cipher", *Handbook of Applied Cryptography, CRC Press*, pp. 191-223.

[14]. William A. Arbaugh, Narendar Shankar, Y.C. Justin Wan (2001), *Your 802.11 Wireless Network has No Clothes,* Department of Computer Science, University of Maryland, College Park, Maryland 20742.

[15]. Anton T. Rager (2001), *WEPCrack, AirSnort*, http://wepcrack.sourceforge.net/.

[16]. Daniel J. Barrett, Richard E. Silverman, and Robert G. Byrnes (2005), *SSH: The Secure Shell (The Definitive Guide)*, O'Reilly.

[17]. http://www.verisign.com/ssl/ssl-information-center/how-ssl-security-works/index.html, *Secure Sockets Layer (SSL): How It Works*.

[18]. Third Wave Communications (2002), *RSA Security help create solution to secure WLAN*, Johannesburg, South Africa.

[19]. Mark Roy (2000), *Diameter extends remote authentication*, http://www.networkworld.com/news/tech/0131tech.html.

[20]. B.Clifford Neuman, Theodore Ts'o (1994), *Kerberos: An Authentication Service for Computer Networks*, IEEE Communications Magazine, Vol 32, Number 9, pages 33-38.

[21]. Scott Fluhrer, Itsik Mantin, Adi Shamir (2003), *Weaknesses in the Key Scheduling Algorithm of RC4*, Computer Science department, the Weizmann Institude, Rehovot 76100, Israel.

[22]. Sean Whalen (2002), *Analysis of WEP and RC4 Algorithm*, http://www.chocobospore.org.

[23]. B. Aboba (2004), *Extensible Authentication Protocol (EAP)*, Network Working Group, IETF.

[24]. Federal Information Standards Publication 197 (2001), *Announcing the Advanced Encryption Standard (AES),* National Institude of Standards and Technology.

[25]. Joan Daemen, Vincent Rijmen (1999), *AES Proposal Rijndael,* National Institude of Standards and Technology.

[26]. Angelos D. Keromytis (2000), *The IKE Protocol*, http://www.usenix.org/events/usenix2000/freenix/full_papers/hallqvist/hallqvist_html/node5.html.

[27]. Jim Geier (2003), *Mobile IP Enables WLAN Roaming*, http://www.wi-fiplanet.com/tutorials/article.php/2205821.