LỜI CẢM ƠN

Trước tiên em xin gửi lời cảm ơn sâu sắc tới thầy, TS. Hồ Văn Canh, đã tận tình hướng dẫn,giúp đỡ em trong suốt quá trình thực hiện đề tài. Để đề tài của em hoàn thành đúng thời hạn.

Em xin cảm ơn các thầy, cô khoa Công nghệ thông tin, trường Đại học Dân Lập Hải Phòng đã trang bị cho chúng em những kiến thức quý báu trong quá trình học tập, và tạo điều kiện giúp đỡ để em làm tốt nghiệp tốt nhất trong thời gian vừa qua.

Em xin cảm ơn các thầy cô trong trường Đại học Dân Lập Hải Phòng đã trang bị cho chúng em nhứng tri thức quý báu giúp chúng em đủ hành trang bước vào đời.

Cảm ơn tất cả các bạn khoa công nghệ thông tin đã giúp đỡ và đồng hành với tôi trong suốt thời gian qua!

MỤC LỤC

LỜI MỞ ĐẦU

Sự tiến bộ của nền khoa học công nghệ thông tin đã góp phần làm cho đời sống xã hội ngày càng phong phú. Nó mang lại siêu lợi nhuận cho nền kinh tế của mỗi quốc gia và toàn cầu, đồng thời mang lại nền văn minh cho nhân loại chưa từng có từ trước đến nay. Việt Nam là một nước đang trên đà phát triển và hội nhập, những ảnh hưởng tích cực và hệ quả ưu việt do công nghệ thông tin mang lại cho nền kinh tế và đời sống xã hội khoảng vài chục năm gần đây đã chứng minh điều này.

Hệ thống mạng không dây WLAN là một phát triển vượt bậc của ngành công nghệ thông tin. Hiện nay nó là sự lựa chọn tối ưu nhất bởi cùng một lúc có thể kết nối máy in, Internet và các thiết bị máy tính khác mà không cần dây cáp truyền dẫn. Nhờ đó mà ta giảm thiểu được số lượng dây chạy trong phòng, từ phòng này sang phòng khác. Số lượng dây không đáng kể nên không làm thay đổi cảnh quan, thẩm mĩ nơi ở và nơi làm việc, hội họp.Hệ thống liên lạc không dây hiện nay không chỉ còn bị giới hạn trong truyền thông tiếng nói mà nó mở rộng ra nhiều dịch vụ khác như hệ thống điện thoại 3G. Ngoài chức năng điện thoại, người sử dụng có thể sử dụng nó như một thiết bị giải trí, truy cập internet, kiểm tra tài khoản...Ngoài ra mạng LAN không dây còn rất nhiều tiện lợi khác đó là sự mềm dẻo, dễ thay thế bảo trì, dễ dàng mở rộng hệ thống…

Các chuẩn mạng không dây tuy mới đưa ra nhưng đã nhanh chóng trở lên phổ biến trong hệ thống mạng kết nối sử dụng dây hiện nay. Hiện nay, mạng không dây thực sự đi vào cuộc sống . Chỉ cần một laptop, PDA hoặc một phương tiện truy cập mạng không dây bất kỳ, bạn có thể truy cập vào mạng ở bất cứ nơi đâu, trên cơ quan, trong nhà, ngoài đường , trong quán cafe…bất cứ nới đâu nằm trong phạm vi phủ sóng của WLAN.

Trong nội dung đề tài nay, em xin trình bày những hiểu biết về WLAN như là một giới thiệu về một công nghệ mới đang được triển khai rộng rãi hiện nay.

Nộ dung đề tài gồm 3 chương:

Chương 1 : Giới thiệu tổng quan về WLAN

Chương 2: Các vấn đề kĩ thuật

Chương 3: Bảo mật cho WLAN

Trong quá trình làm, do điều kiện thời gian và trình độ có hạn, điều kiện tiếp xúc với thiết bị còn ít, do đó không tránh khỏi một số sai sót.Vì vậy mong thầy cô và các bạn đóng góp ý kiến để em có thể hoàn thiện hơn tài liệu này, em xin chân thành cảm ơn.

CHƯƠNG 1: GIỚI THIỆU TỔNG QUAN VỀ WIRELESS LAN

1.1. Tổng quan

Kỹ thuật liên lạc không dây thực sự trở thành một hiện tượng bùng nổ của khoa học kĩ thuật trên toàn thế giới. Chỉ riêng tại Mỹ, số lượng thống kê cho thấy từ năm 1987 đến 1993 số lượng điện thoại di động (cellular phone) đã tăng từ 1 triệu cái lên 10 triệu cái, hiệu suất bán thiết bị có thể lên tới 180.000 cái/tháng. Ở Thụy Điển, theo số lượng thống kê năm 90, cứ 10 người dân thì có một người sử dụng điện thoại di động. Kỹ thuật này ngày càng trở thành một phương tiện liên lạc hữu hiệu với sự ra đời của vệ tinh. Ngày nay, liên lạc không dây đã trở thành một phương tiện không thể thiếu của con người.

Các công nghệ và sản phẩm dung cho kết nối mạng máy tính không cần dây dẫn thực sự mới được chú ý vào cuối những năm 90 của thế kỷ 20. Khả năng di chuyển linh hoạt trong mạng LAN không dây (WLAN) cho phép nhân viên có thể tận dụng thời gian và không gian làm việc tại bất kỳ đâu trong phạm vi bán kính cho phép, họ không phải gắn cứng vào chiếc máy PC nữa, vì thế nâng cao hiệu suất làm việc. Do đó, việc phát triển WLAN đã trở thành một mục tiêu hàng đầu của công ty máy tính, nhằm giúp các doanh nghiệp cũng như người dùng riêng lẻ có được những tiện lợi tối đa trong công việc.

Được phê chuẩn của IEEEb 802.11 vào năm 1999, đến nay WLAN đã trở lên phát triển mạnh trên thế giới, tuy nhiên ở một số nước mà nền công nghệ thông tin đanh phát triển như ở Việt Nam hiện nay thì WLAN vẫn còn là một công nghệ khá mới mẻ cần được nghiên cứu và đầu tư thích đáng

Hình 1.1: Vị trí của WLAN trong mô hình hệ thống mạng

Khái niệm mạng WLAN

Mạng WLAN (WIRELESS LOCAL AREA NETWORK–WLAN) là một hệ thống truyền thông số liệu linh hoạt được thực hiện trên sự mở rộng của mạng LAN hữu tuyến. WLAN gồm các thiết bị được nối lại với nhau có khả năng giao tiếp thông qua sóng RADIO hay tia hồng ngoại trên cơ sở sử dụng các giao thức chuẩn riêng của mạng không dây thay vì các đường truyền dẫn bằng dây.

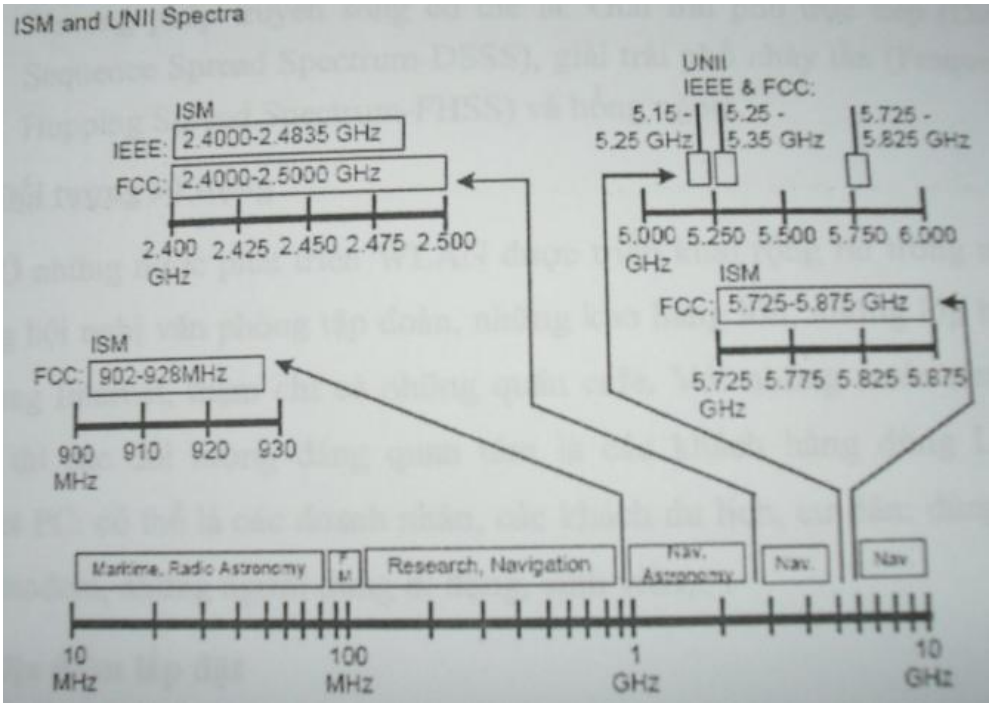
1.2. Công nghệ sử dụng

Hầu hết tất cả các công nghệ từ computer đến non-computer đều có những chuẩn riêng quy định cho chúng WLAN cũng không phải là ngoại lệ. Có 2 tổ chức lớn và uy tín của Mỹ hiện nay cùng đưa ra các chuẩn cho WLAN. Đó là FCC (Federal Communication Commission) và IEEE

(Institute of Electrical and Electronics Engineers). Họ quy định ra khoảng tần số mà các thiết bị WLAN được phép sử dụng. Có 2 loại khoảng tần số:

❖ ISM (Industrial, Scientifi, and Medical): tần số dùng cho ISM được quy đinh là: 902 MHz, 2.4 GHz và 5.8 GHz và độ rộng thay đổi có thể từ 26 MHz tới 150 MHz.

❖ UNII (Unlicensed National Information Infrastructure): Các băng sóng đều nằm trong dải 5GHz và độ rộng băng thay đổi là 100 MHz



Hình 1.2: Phân bổ tần số ISM và UNII

Hiện nay, các chuẩn do IEEE được sử dụng phổ biến nhất để dùng làm chuẩn cho các hãng sản xuất thiết bị WLAN. Chuẩn cho WLAN được IEEE đặt tên là IEEE 802.11. 802.11 quy định cách thứ hoạt động của mạng không dây, các kỹ thuật truyền, tốc độ và băng thông của mỗi phương pháp truyền.

Các chuẩn của WLAN được IEEE quy định trong 802.11: "WLAN là một công nghệ Internet không dây tốc độ cao theo chuẩn 802.11 IEEE"

Kích thước phủ sóng mỗi HOSTPOT : < 300m.

Tần số: Tần số sử dụng phổ biến: 802.11b, 2,4GHz (giải IMS), công suất phát : = 100mW, độ rộng băng thông 22MHz.

Tốc độ : 11Mbps với chuẩn 802.11b.

Bảo mật: WEP (Wired Equivalent Privacy)

Hệ quản lý: Radius (Remote Authentication Dial _ In User Service)

Phương pháp truyền sóng có thể là: Giải trải phổ trực tiếp (Direct Sequence Spread Spectrum-DSSS), giải trải phổ nhảy tần (Frequency Hopping Spread Spectrum-FHSS) và hồng ngoại.

1.3. Đối tượng sử dụng

Ở những nước phát triển WLAN được triển khai rộng rãi trong những phòng hội nghị văn phòng tập đoàn, những kho hàng lớn, những lớp học có sử dụng Internet, thậm chí cả những quán cafe. Với những nước như Việt Nam thì những đối tượng đáng quan tâm là khách hàng dùng Laptop, Pocket PC: có thể là các doanh nhân, các khách du lịch, cư dân: dùng PC + card modem, những người dùng di động, sinh viên…

Hệ thống thông tin doanh nghiệp: Các nhà quản lý mạng có thể di chuyển nhân viên lập ra các văn phòng tạm thời hoặc cài đặt máy in và nhiều thiết bị khác mà không ảnh hưởng bởi chi phí và tính phức tạp của mạng có dây.

Du lịch: Khách sạn và các điểm du lịch có thể xử lý thông tin đặt phòng yêu cầu dịch vụ hoặc thông tin hành lý của khách hàng.

Giáo dục: Sinh viên và giảng viên có thể liên lạc với nhau từ bất kỳ vị trí nào trong khuôn viên đại học để trao đổi hoặc tải về các bài giang có sẵn trên mạng. Mạng WLAN còn giảm thiểu nhu cầu sử dụng phòng thực hành máy tính của sinh viên.

Thông tin sản phẩm: Các nhân viên chịu trách nhiệm về xuất kho có thể cập nhật và trao đổi các thông tin của sản phẩm.

Y tế: Y tá có thể trao đổi các thông tin về liệu pháp chữa bệnh và bệnh nhân.

1.4. Địa điểm lắp đặt

Tại các khu tập trung đông người như: Các văn phòng, tòa nhà, trường đại học, sân bay, nhà ga, sân vận động, khu triển lãm, khách sạn , siêu thị, khu dân cư…

1.5. Khả năng ứng dụng tại Việt Nam

Việt Nam là một nước công nghệ thông tin đạng trên đà phát triển nhanh chóng, vì vậy tiềm năng khai thác là rất lớn. Hơn thế trong những năm vừa qua và những năm tới, Việt Nam là điểm đến của các nhà đầu tư, các khách du lịch nước ngoài. Các khách quốc tế, du lịch có Laptop cắm card để nối mạng WLAN, hoặc Laptop đời mới dùng công nghệ chip Centrino hoặc Duo Core là đối tượng người

dùng. (theo boingo: năm 2005 90% Laptop có sẵn tính năng kết nối mạng WLAN mà không cần đến card riêng, ở Mỹ 27 triệu trên tổng số 36 triệu doanh nhân có máy tính xách tay).Dân cư nằm trong vùng HOSTPOT dùng card chuyên dụng (dưới 100 USD) là đối tượng của nhà đầu tư. Nếu có những chính sách đầu tư giảm giá thích hợp, thì đối tượng sinh viên ở các trường đại học sử dụng Laptop, PC, PDA, Pocket PC là đối tượng tiềm năng cần quan tâm, cần phát triển số điểm HOSTPOT, giảm giá cước, có chiến **dịch xúc tiến, tiếp thị.**

1.6. Ưu và nhược điểm của mạng WLAN

1.6.1. Ưu điểm

Sự tiện lợi: Mạng không dây cũng như hệ thống mạng thông thường. Nó ***cho phép người dùng truy xuất tài nguyên mạng ở bất kỳ nơi đâu trong khu vực được triển khai***(nhà hay văn phòng). Với sự gia tăng số người sử dụng máy tính xách tay(laptop), đó là một điều rất thuận lợi. (bên trong vùng phủ sóng Radio các nút mạng các thể truyền thông không giới hạn xa hơn).

Khả năng di động: Với sự phát triển của các mạng không dây công cộng, ***người dùng có thể truy cập Internet ở bất cứ đâu.*** Chẳng hạn ở các quán Cafe, người dùng có thể truy cập Internet không dây miễn phí.

Hiệu quả: Người dùng có thể duy trì kết nối mạng khi họ đi từ nơi này đến nơi

Triển khai: Việc thiết lập hệ thống mạng không dây ban đầu ***chỉ cần ít nhất 1 access point***. Với mạng dùng cáp, phải tốn thêm chi phí và có thể gặp khó khăn trong việc triển khai hệ thống cáp ở nhiều nơi trong tòa nhà.

Khả năng mở rộng: Mạng không dây có thể ***đáp ứng tức thì khi gia tăng số lượng người dùng.*** Dễ lắp đặt, triển khai và mở rộng (khi thêm máy không ảnh hưởng đến hệ thống), ít sử dụng các kết nối có dây do đó loại bỏ được sự rườm rà của việc đi cáp, đặc biệt thuận tiện với những điểm khó đi dây, tiết kiệm được thời gian lắp đặt dây cáp và không làm thay đổi thẩm mỹ kiến trúc toà nhà. Đồng nghĩa với việc ít phát sinh nhiều vấn đề cho người dùng và quản trị hệ thống. Do đó làm giảm chi phí bảo trì bảo dưỡng hệ thống nhờ khả năng dễ thay thế khi xảy ra sự cố.

Tính mạnh mẽ:

Mạng WLAN tránh được những thảm hoạ như động đất, người dùng lôi kéo. Sự phát triển mạnh mẽ và phổ biến rộng rãi của mạng không dây hiện đang là một động lực lớn thúc đẩy một làn sóng đổi mới trên Internet. Công nghệ không dây có mặt ở khắp mọi nơi.

1.6.2. Nhược điểm của mạng WLAN

Bảo mật: Môi trường kết nối không dây là không khí nên ***khả năng bị tấn công cuả người dùng là rất cao.*** Thêm vào nữa, giao diện sóng radio làm cho việc nghe trộm trong WLAN dễ hơn nhiều trong mạng khác.

Phạm vi: Một mạng chuẩn 802.11g với các thiết bị chuẩn ***chỉ có thể hoạt động tốt trong phạm vi vài chục mét.*** Nó phù hợp trong 1 căn nhà, nhưngvới một tòa nhà lớn thì không đáp ứng được nhu cầu. Để đáp ứng cần phải mua thêm Repeater hay access point, dẫn đến chi phí gia tăng.

Độ tin cậy(nhiễu): Vì sử dụng sóng vô tuyến để truyền thông nên ***việc bị nhiễu, tín hiệu bị giảm*** do tác động của các thiết bị khác(lò vi sóng,….) là không tránh khỏi. Làm giảm đáng kể hiệu quả hoạt động của mạng.

Tốc độ: Tốc độ của mạng không dây (1- 125 Mbps) ***rất chậm so với mạng sử dụng cáp***(100Mbps đến hàng Gbps).

CHƯƠNG 2: CÁC VẤN ĐỀ VỀ KĨ THUẬT

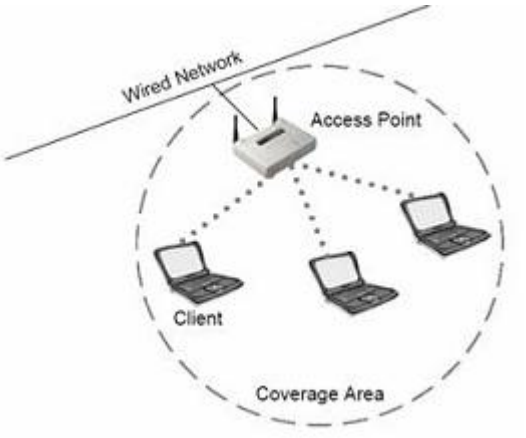
2.1. Tổng quan

WLAN là một công nghệ truy cập mạng băng thông rộng không dây theo chuẩn 802.11 của IEEE. 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 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 .

Tiêu chuẩn IEEE 802.11 định nghĩa cả 2 kiểu cơ sở hạ tầng, với số lượng tối thiểu các điểm truy nhập trung tâm tới một mạng hưu tuyến, và một chế độ là peer-to-peer, trong đó một tập hợp những đài vô tuyến liên lạc trực tiếp với nhau mà không cần một điểm truy nhập trung tâm hoặc mạng vô tuyến nào. Sự hấp dẫn của WLAN là tính linh hoạt của chúng. Chúng có thể mở rộng truy cập tới các mạng cục bộ, như Intranet, cũng như hỗ trợ sự truy nhập băng rộng tới Internet tại các điểm truy cập. WLAN có thể cung cấp kết nối không dây nhanh chóng và dễ dàng tới các máy tính, các máy móc hay các hệ thống trong một khu vực, nơi mà các hệ thống cơ sở hạ tầng truyền thông cố định không tồn tại hoặc nơi mà truy nhập như vậy là không cho phép. Người dùng có thể là cố định hoặc di động hoặc thậm chí có thể đang ngồi trên một phương tiện chuyển động. Một vài hình vẽ sau sẽ đưa ra một cái nhìn tổng quát về khả năng ứng dụng của WLAN:

Vai trò truy cập (Access role).

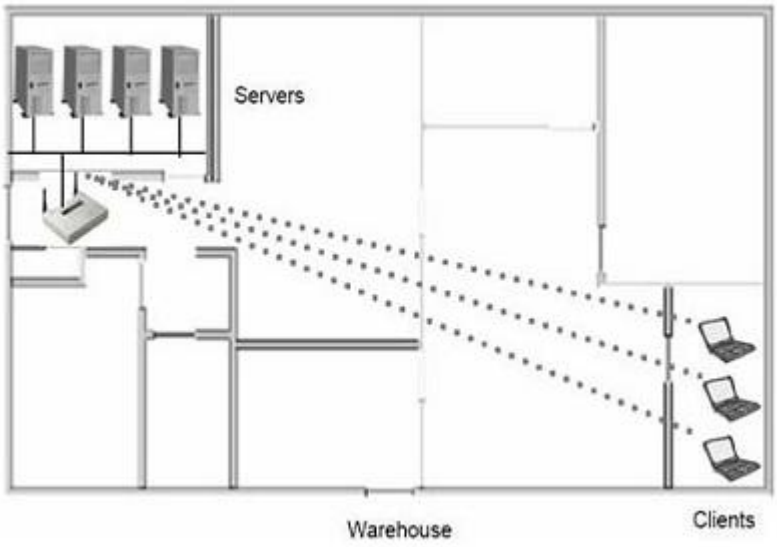
WLAN cung cấp giải pháp cho một vấn đề khá khó đó là: khả năng di động.Các WLAN nhanh,rẻ, và có mặt khắp mọi nơi.



Hình 2.1: Khả năng truy nhập

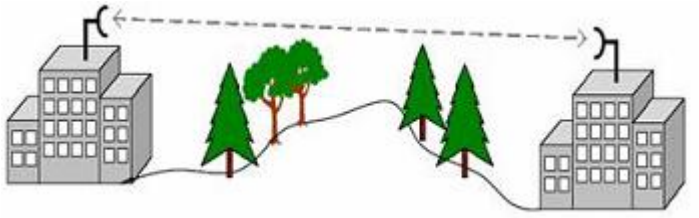
Về khả năng truy cập mạng trong các tòa nhà, nhà kho, bến bãi mà không gặp phải vấn đề tốn kém và phức tạp trong việc đi dây. Hay cũng chính là khả năng mở rộng mạng:

Các mạng không dây có thể được xem như một phần mở rộng của một mạng có dây. Khi muốn mở rộng một mạng hiện tại, nếu cài đặt thêm đường cáp thì sẽ rất tốn kém. Hay trong những tòa nhà lớn, có thể cài đặt cáp quang nhưng như thế sẽ yêu cầu nhiều thời gian và tiền bạc. Các WLAN có thể thực thi một cách dễ dàng hơn.



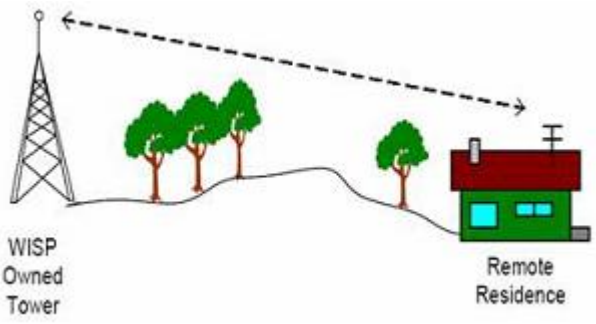
Hình 2.2: Khả năng truy cập mạng mà không phải đi dây

Về khả năng đơn giản hóa việc kết nối mạng giữ hai tòa nhà mà giữa chúng là địa hình phức tạp không thi công đối với mạng thông thường.(với các loại anten không dây phù hợp và trong một khoảng cách cho phép)



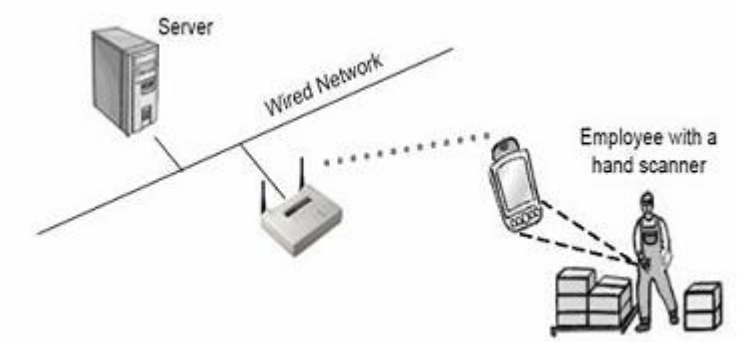
Hình 2.3:Tiện lợi trong việc xây dựng mạng trên miền núi

hay các khu vực có địa hình lòng giếng vẫn có thể truy cập mạng bình thường như các nơi khác.



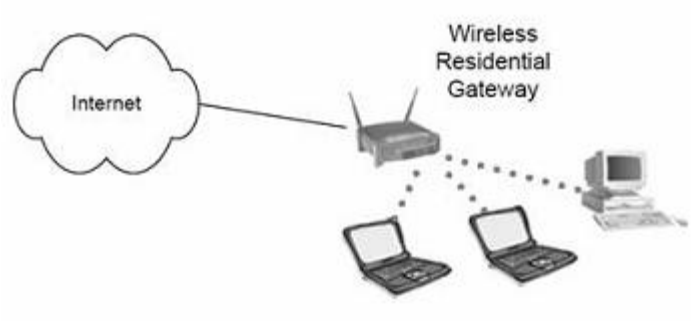
Hình 2.4: Tại nơi có địa hình lòng chảo

Và sự tiện lợi trong việc truy cập mạng mà vẫn có thể di chuyển (nghĩa là di chuyển từ khu vực không dây này sang khu vực không dây khác mà không bị mất kết nối, giống như điện thoại di động, người dùng có thể di chuyển giữa các vùng khác nhau. Trong một tổ chức lớn, khi phạm vi phủ sóng của wireless rộng thì việc roaming khá quan trọng vì người dùng có thể vẫn giữ kết nối khi họ ra ngoài)



Hình 2.5:Khả năng truy cập trong khi di chuyển

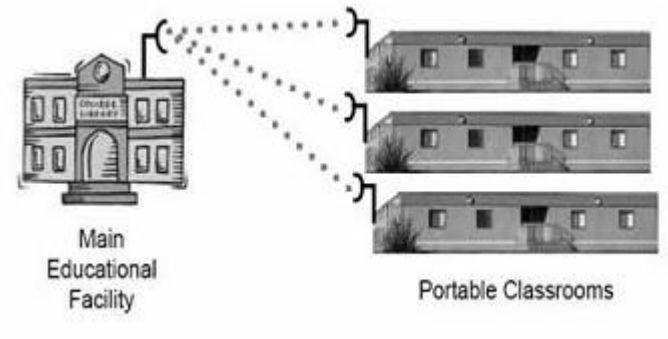
Từ các văn phòng , nhà riêng (Trong một số doanh nghiệp chỉ có một vài người dùng và họ muốn trao đổi thông tin giữa những người dùng và chỉ có một đường ra Internet. Với những ứng dụng này, thì một wireless LAN là rất đơn giản và hiệu quả.)



Hình 2.6: Truy cập từ các văn phòng, nhà riêng

Đến các văn phòng di động (Mobile Ofices),các khu lớn hơn như các trường đạii học, các khu chung cư đều có thể truy cập mạng với tốc độ cao và quá trình thiết lập đơn giản. (như tình trạng thiêu các văn phòng làm trụ sở ở các công ty hiện nay, hay vì tình trạng quá tải của các lớp học, nhiều trường hiện nay đang sử dụng lớp học di động. Để có thể mở rộng mạng máy tính ra những tòa nhà tạm thời, nếu sử dụng cáp thì rất tốn chi phí. Các kết nối WLAN từ tòa nhà chính ra các lớp học di động cho phép các kết nối một cách linh hoạt với chi phí có thể chấp nhận được)

A school with mobile classrooms



Hình 2.7: Truy cập từ các trường đại học

2.2. Các tính năng của WLAN 802.11

WLAN là công nghệ thuộc lớp truy nhập, về bản chất là một mạng LAN có cơ chế tránh xung đột CSMA/CA.

IEEE 802.11 gồm có các chuẩn:

- **802.11a:** 5,6 GHz, 54 Mbps, Sử dụng phương pháp điều chế OFDM

(Orthogonal Frequency Division Multiplexing), hoạt động ở dải tần 5,6GHz, tốc độ truyền dữ liệu lên tới 54 Mbps, hiện chuẩn này đang được một số hãng đầu tư để hy vọng chiếm lĩnh thị trường thay cho chuẩn 802.11b.

- **802.11b:** 2,4 GHz, 11 Mbps, DSSS đây là một chuẩn khá phổ biến, nó hoạt động ở dải tần 2.4GHz, là dải tần ISM (Industrial, Scientific and Medical). Ở Mỹ, thiết bị hoạt động ở dải tần này không phải đăng kí. Tốc độ truyền dữ liệu có thể lên đến 11Mbps. Wi-Fi là tên gọi của các dòng sản phẩm tương thích với chuẩn 802.11b và được đảm bảo bởi tổ chức WECA (Wireless Ethernet Compatibility Alliance).

- **802.**11c: hỗ trợ các khung thông tin của 802.11.

- **802.**11d: cũng hỗ trợ các khung thông tin của 802.11 nhưng tuân theo những chuẩn mới.

- **802.**11e: nâng cao QoS ở lớp MAC.

- **802.**11f: Inter Access Point Protocol

- **802.**11g: (2.4GHz, 54Mbps, OFDM): tăng cường sử dụng dải tần 2.4GHz, nó là phiên bản nâng cấp của 802.11b, được thông qua bởi IEEE, tốc độ truyền có thể lên tới 54Mbps nhưng chỉ truyền được giữa những đối tượng nằm trong khoảng cách ngắn. Hiện nay chuẩn 802.11g đã đạt đến tốc độ 108Mbps-300Mbps.

- **802.**11h: có thêm tính năng lựa chọn kênh động. Dynamic Channel Selection (DCS) và điều khiển công suất truyền dẫn (Transmit Power Control).

- **802.**11x: một chuẩn mới được cập nhật và thực hiện, nó cung cấp việc điều khiển truy cập mạng trên cổng cơ sở. Mặc dù lúc đầu IEEE thiết kế 802.1x cho thông tin hữu tuyến, nhưng đã được áp dụng cho các WLAN để cung cấp cho vài sự bảo mật cần thiết. Lợi ích chính của 802.1x đối với WLANs là nó cung cấp sự chứng thực lẫn nhau giữa một network và một client của nó.

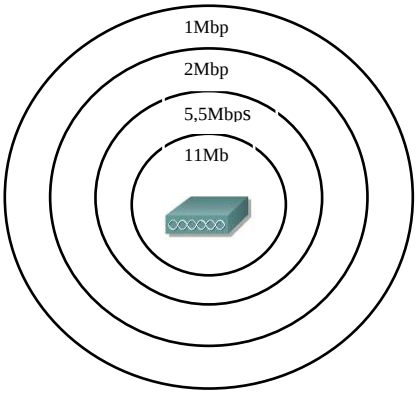
- **802.**11i: nâng cao khả năng an ninh bảo mật lớp MAC, chuẩn này đang được hoàn thiện, nó sẽ là một nền tảng vững chắc cho các chuẩn WLAN sau này. Nó cung cấp nhiều dịch vụ bảo mật hơn cho WLAN 802.11 bởi những vấn đề định vị gắn liền với cả sự điều khiển phương tiện truy nhập, Media Access Control (MAC), lẫn những lớp vật lý của mạng Wireless. Những kiểu chứng thực dựa trên nền tảng là 802.1x và giao thức chứng thực có thể mở rộng Extensible Authentication Protocol (EAP), mà vẫn cho phép các nhà cung cấp tạo ra một vài khả năng chứng thực khác. Trong thời gian sau 802.11i có thể cung cấp một sự thống nhất để sử dụng những tiêu chuẩn mã hóa tiên tiến (Advanced Encryption Standard - AES) cho những dịch vụ mã hóa của nó, nhưng nó vẫn tương thích với thuật toán RC4.

- **802.**11j: là chuẩn thống nhất toàn cầu cho các tiêu chuẩn: IEEE, ETSI, HiperLAN2, ARIB, HiSWANa.

Với các chuẩn 802.11, thì chuẩn 802.11b và 802.11g hoạt động ở dải tần 2.4GHz, tuy nhiên dải tần ISM là dải tần số hoạt động không cần cấp phép, do đó có thể bị giao thoa đáng kể với các phương tiện như xe cấp cứu, ôtô cảnh sát, xe taxi, cũng như từ những người dùng khác và nhiều thiết bị gia đình và văn phòng hoạt động

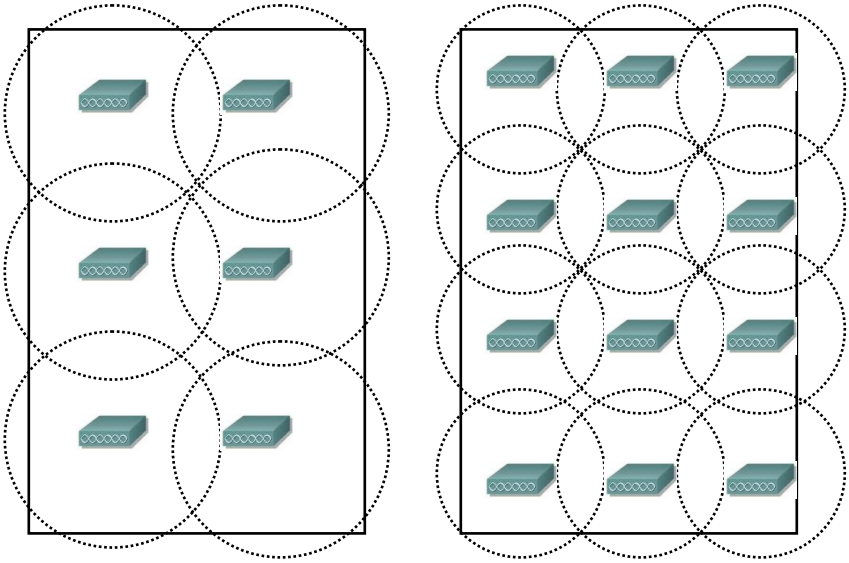
trong băng ISM. Vì lẽ đó, chuẩn 802.11a được đưa ra. Nhưng tất cả các chuẩn khác lại sử dụng dải 2.4GHz, do đó khả năng tương thích ngược lại là một vấn đề.

802.11a: có những ưu điểm nổi bật như tốc độ truyền dữ liệu nhanh hơn, trong khi 802.11b chỉ cung cấp 3 kênh độc lập thì 802.11a mặc dù khu vực phủ sóng nhỏ hơn, lại có thể cung cấp tới 12 kênh. Những băng thông phụ thêm này có ý nghĩa rất quan trọng trong việc chống nhiễu sóng khi thiết kế mạng với dung lượng tối đa. Một điểm yếu của 802.11a là dải phủ sóng hẹp, do chuẩn này sử dụng dải tần 5GHz (tần số càng cao thì dải truyền tín hiệu càng ngắn).



Hình 2.8: Sự liên quan giữa tốc độ và bán kính phủ sóng

Tốc độ truyền dữ liệu thấp hơn thì phạm vi hoạt động của AP rộng hơn, do đó việc lựa chọn giữa tốc độ truyền và phạm vi hoạt động cần phải cân nhắc, khi đó ảnh hưởng trực tiếp tới việc bố trí các AP.



Hình 2.9: Sự liên quan giữa tốc độ và số lượng AP

Xét trong cùng phạm vi phủ sóng, thì nếu yêu cầu tốc độ là 2Mbps thì chỉ cần bố trí 6 AP, trong khi với tốc độ truyền yêu cầu là 5Mbps thì để phạm vi phủ sóng bao hết khu vực trên thì cần gấp đôi số AP, 12 AP (h.vẽ).

Khái niệm In-door và Out-door: In-door là khái niệm dùng vô tuyến trong phạm vi không gian nhỏ, như trong một tòa nhà. Out-door là khái niệm dùng vô tuyến trong phạm vi không gian lớn hơn. Với WLAN thì bán kính đến các thiết bị đầu cuối phía khách hàng (CPE- Customer Premises Equipment) mà nó quản lý có thể từ 5÷40 km. Với khoảng cách nhỏ hơn 1km thì thậm chí CPE không cần trong tầm nhìn thẳng với AP. CPE là thiết bị truyền thông cá nhân dùng để kết nối với mạng trong một tổ chức. Thiết bị CPE bao gồm các thiết bị PBX (Private Branch Exchange), các đường điện thoại, hệ thống khóa, các thiết bị fax, modem, thiết bị xử lý tiếng nói, và thiết bị truyền video.

2.3. Điều khiển xung đột:

WLAN sử dụng sóng radio làm phương tiện truyền dẫn, tuy nhiên, môi trường truyền sóng cũng là một môi trường có tính chất chia sẻ (shared medium). Do đó, nó cũng phải có các cơ chế để triệt tiêu các xung đột giữa các thiết bị trong mạng khi chúng truyền/ nhận dữ liệu giống như các mạng hữu tuyến trước đó đã gặp phải. Các mạng sử dụng dây dẫn sử dụng cơ chế CSMA/CD (Carrier Sense Multi Access/ Collission Avoidence) để hạn chế tránh các xung đột.

Điểm khác biệt lớn nhất giữa CSMA/CD và CSMA/CA đó là: các thiết bi sử dụng CSMA/CD chỉ dò xung đột và tránh các xung đột bằng cách không truyền dữ liệu khi mạng xảy ra xung đột mà đợi cho đến khi hết xung đột mới truyền, còn CSMA/CA thì khác, nó có khả nằng ngăn ngừa các xung đột và sử dụng các tín hiệu positive acknowledgement (ACK) thay vì phải đứng ra phân xử việc sử dụng đường truyền khi có xung đột như CSMA/CD. Cách thứ hoạt động của ACK cũng khá đơn giản. Khi một trạm wireless gửi đi một gói tin, trạm nhận sẽ gửi lại một ACK sau khi đã nhận được hết gói tin. Nếu trạm gốc không nhận được gói tin ACK đó, nó sẽ coi như là đã xảy ra xung đột, gói tin đã bị mất và nó sẽ gửi lại gói tin đó.Điều này có thể khiến cho các tín hiệu điều khiển chiếm tới 50% băng thông của mạng (với chuẩn 802.11b có băng thông 11Mbps thì nó chiếm khoảng 5-5,5Mbps) nhưng chúng có thể giúp cho hệ thống ngăn ngừa được các xung đột. Với CSMA/CD,lượng băng thông chỉ chiếm khoảng 30%. Nhưng nếu xảy ra xung đột thì mạng sử dụng CSMA/CD có thể bị chiếm tới 70% băng thông trong khi CSMA/CA chỉ bị chiếm khoảng 50-55% băng thông mà thôi.

❖ **CSMA/CA (Carrier Sense Multi Access/ Collission Avoidence)**

Một trạm không dây muốn truyền khung, đầu tiên nó sẽ nghe trên môi trường không dây để xác đinh hiện có trạm nào đang truyền hay không (nhạy cảm sóng mang). Nếu môi trường này hiện đang bị chiếm, trạm không dây tính toán một khoảng trễ lặp lại ngẫu nhiên. Ngay sau khi thời gian trễ đó trôi qua, trạm không dây lại nghe xem liệu có trạm nào đang truyền hay không. Bằng cách tạo ra thời gian trễ ngẫu nhiên, nhiều trạm đang muốn truyền tin sẽ không cố gắng truyền lại tại cùng một thời điểm (tránh xung đột). Những va chạm có thể xảy ra và không

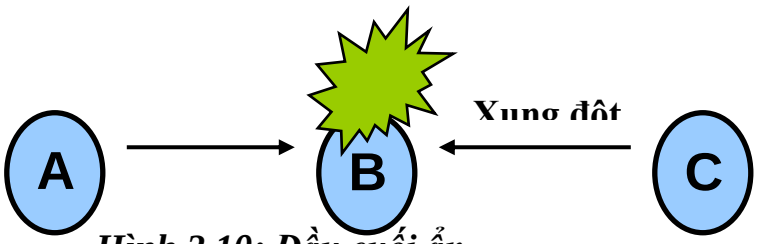
giống như Ethernet, chúng không thể bị phát hiện bởi các node truyền dẫn. Do đó, 802.11b dùng giao thức Request To Send (RTS)/ Clear To Send (CTS) với tín hiệu Acknowlegment (ACK) để đảm bảo rằng một khung nào đó đã được gửi và nhận thành công.

Các yếu tố quan trọng:

- Đợi yên lặng
- Rồi "nói"
- "Nghe" trong khi "noi"
- Hệ thống sẽ làm gì nếu có hai thiết bị cùng "lên tiếng"? Tạm dừng
- Lặp lại quá trình

Trong cơ chế CSMA/CA ta cần quan tâm đến hai vấn đề là đầu cuối ẩn (Hidden Termial) và đầu cuối hiện (Exposed Terminal).

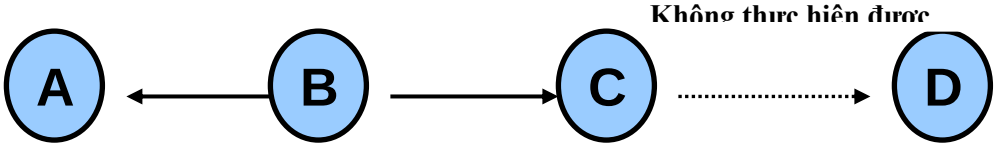
❖ **Đầu cuối ẩn**



Hình 2.10: Đầu cuối ẩn

- A nói chuyện với B
- C cảm nhận đường truyền
- C không nghe thấy A do C nằm ngoài vùng phủ sóng của A
- C quyết định nói chuyện với B
- Tại B xảy ra xung đột.

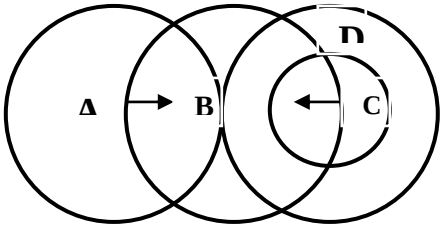
❖ **Đầu cuối hiện:**



Hình 2.11: Đầu cuối hiện

- B nói chuyện với A
- C muốn nói chuyện với D
- C cảm nhận kênh truyền và thấy nó đang bận
- C giữ im lặng (trong khi nó hoàn toàn có thể nói chuyện với D)

❖ **Giải quyết vấn đề đầu cuối ẩn :**



Hình 2.12: Giải quyết vấn đề đầu cuối ẩn

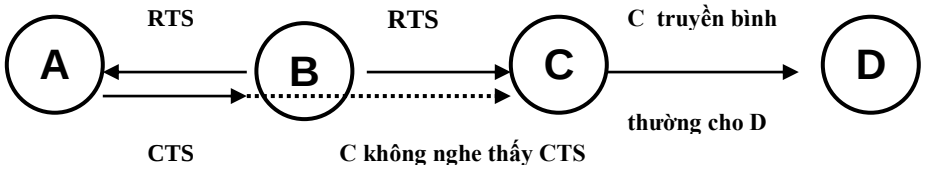
- A gửi RTS cho B
- B gửi lại CTS cho A nếu nó sẵn sàng nhận
- C nghe thấy CTS
- C không nói chuyện với B và chờ đợi
- A gửi dữ liệu thành công cho B

Trong trường hợp này nếu C muốn nói chuyện với D thì nó hoàn toàn có thể giảm công suất cho phù hợp.

Vấn đề đặt ra là C phải chờ bao lâu thì mới nói chuyện được với B:

Trong RTS mà A gửi cho B có chứa độ dài của DATA mà nó muốn gửi. B chứa thông tin chiều dài này trong gói CTS mà nó gửi lại A C, khi "nghe" thấy gói CTS sẽ biết được chiều dài gói dữ liệu và sử dung nó để đặt thời gian kìm hãm sự truyền.

❖ **Giải quyết vấn đề đầu cuối hiện :**



Hình 2.13 : Giải quyết vấn đề đầu cuối hiện

- B gửi RTS cho A (bao trùm cả C)
- A gửi lại CTS cho B (nếu A rỗi)
- C không thể nghe thấy CTS của A
- C coi rằng A hoặc " chết" hoặc ngoài phạm vi
- C nói chuyện bình thường với D

Tuy nhiên còn có vấn đề xảy ra :

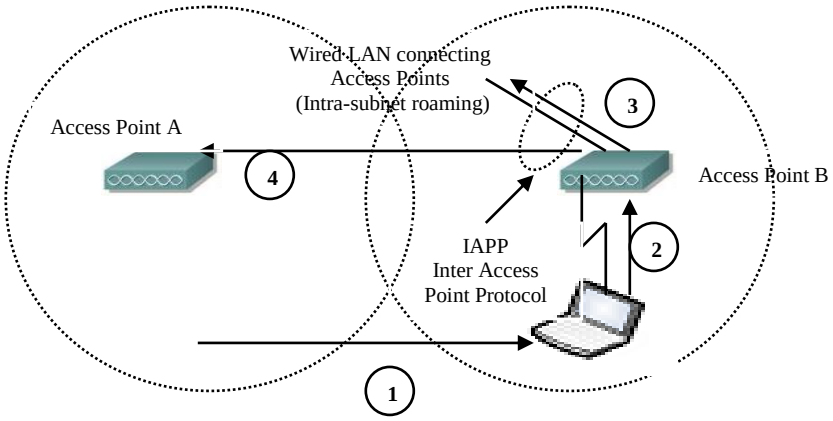
Gói RTS có thể xung đột, ví dụ: C và A cùng nhận thấy có thể truyền cho B và cùng gửi RTS cho B, tại B sẽ có xung đột, nhưng xung đột này không nghiêm trọng như xung đột gói DATA bởi chiều dài gói RTS thường nhỏ hơn nhiều DATA. Tuy nhiên những gói CTS có thể gây giao thoa, nếu kích thước của gói RTS/CTS như của DATA thì điều này rất đáng quan tâm. Vấn đề này được khắc phục bằng cách tạo ra một khoảng thời gian trễ lặp lại ngẫu nhiên (như trên đã trình bày).

2.4. Giải pháp Roaming cho WLAN

Vấn đề Roaming được đề cập đến khi một client của AP này di chuyển đến vùng phủ sóng của AP khác. Có hai loại Roaming cần giải quyết trong mạng WLAN: Đó là Roaming lớp 2 và Roaming lớp 3.

➢ **Roaming lớp 2 (Datalink layer):**

Roaming lớp 2 xảy ra trong trường hợp xảy ra sự si chuyển của client từ vùng phủ sóng của AP này sang vùng phủ sóng của AP khác.



Hình 2.14: Roaming ở lớp Datalink

Quá trình được tiến hành theo các sự kiện sau:

1. Một client di chuyển từ vùng phủ sóng của AP "A" sang vùng phủ sóng của AP "B", cả hai đều cùng subnet. Khi client di chuyển, quá trình Roaming giữa AP "A" và AP "B" bắt đầu được thực hiện. Client sẽ cảm nhận và so sánh cường độ sóng phát của AP, nếu lớn hơn khoảng 20% so với AP cũ thì nó sẽ tiến hành bắt tay với AP mới.

2. Client đó sẽ quét tất cả các kênh theo chuẩn 802.11 để lựa chọn AP thay thế. Trong trường hợp này, client này sẽ phát hiện ra nó đang nằm trong vùng phủ sóng của AP "B", do đó, nó sẽ bắt đầu thuwch hiện quá trình xác thực lại và kết hợp lại với AP " B", như nó đã từng thực hiện với AP "A".

3. AP "B" nó sẽ gửi một null MAC multicast với địa chỉ nguồn là địa chỉ MAC của client. Các thông tin này sẽ được cập nhật cho bảng địa chỉ (Content Addressable Memory - CAM) trong các chuyển mạch đường lên (upstream switche) và điều khiển traffic của LAN cho client thông qua B chứ không phải qua A nữa.

4. AP "B" gửi một MAC multicast sử dụng địa chỉ nguồn là địa chỉ của nó để thông báo với AP của client rằng nó đã bắt tay làm việc với client mà trước đó dang làm việc với AP "A". A nhận được gói tin multicast đó và thực hiện loại bỏ địa chỉ MAC của client đó ra khỏi bộ nhớ.

- **Roaming lớp 3**

Quá trình Roaming lớp 3 được thực hiện khi một client di chuyển từ subnet này sang một subnet khác. Quá trình Roaming lớp 3 sẽ được thực hiện tiếp theo sau quá trình Roaming lớp 2.

Sau khi đã thực hiện việc quảng bá rằng client đã nằm trong vùng phủ sóng của mình, đã ghi nhớ địa chỉ MAC của thiết bị, AP "B" sẽ sử dụng cơ chế đánh địa chỉ động (DHCP) để cung cấp một địa chỉ IP (lớp 3) mới cho thiết bị.

2.5. Sự định vị một WLAN

Một máy client muốn định vị một WLAN thì nó sẽ "nghe" trên mạng để tìm kiếm những vệt tin để lại bởi AP, các SSID hoặc các bản tin dẫn đường (Beacons). Quá trình này được gọi là quét, có hai loại quét là: quét chủ động và quét bị động.

- **Beacon:**

Viết đầy đủ là Beacon management frame, là các khung ngắn được gửi từ AP tới các máy trạm (Station) trong chế độ cơ sở, hoặc từ các trạm tới các trạm trong chế độ đặc biệt, để thiết lập và đồng bộ thông tin vô tuyến trên mạng WLAN. Trong bản tin dẫn đường chứa các thông tin phục vụ.

- **Sự đồng bộ:**

Khi các client nhận được bản tin dẫn đường, chúng sẽ đồng bộ đồng hồ của mình với đồng hồ AP.

- **Tập hợp các tham số của FH và DS:**

Chứa đựng các thông tin đặc biệt phục vụ cho công nghệ trải phổ: với hệ thống FHSS, các thông tin về thời gian nhảy và ngừng. Còn với DSSS, bản tin dẫn đường chứa các thông tin về kênh truyền.

- **Thông tin về SSID:**

Các trạm tìm trong bản tin dẫn đường thông tin SSID của mạng mà chúng muốn truy cập. Khi các thông tin này được tìm thấy, các trạm xem địa chỉ MAC của nơi

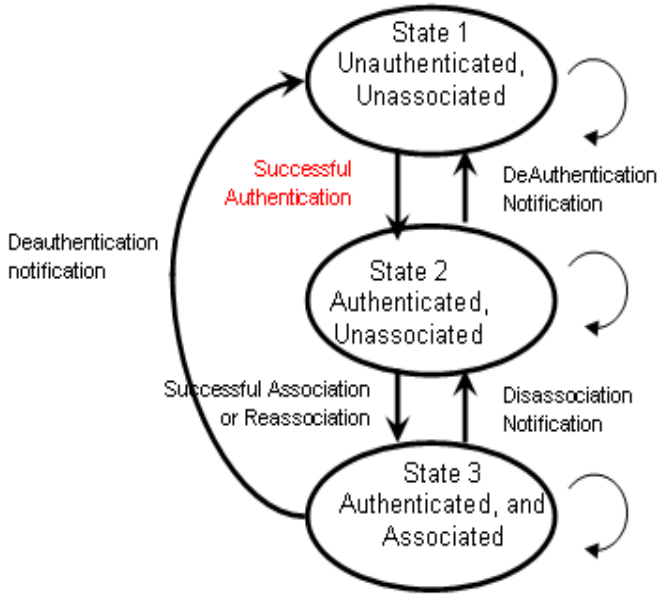
xuất phát bản tin dẫn đường và gửi yêu cầu chứng thực để liên kết với điểm truy nhập. Nếu một trạm được thiết lập để chấp nhận bất cứ SSID nào, trạm đó sẽ cố gắng truy cập đến mạng thông qua AP đầu tiên mà gửi bản tin dẫn đường hoặc thông qua AP có tín hiệu tốt nhất trong trường hợp có nhiều AP.

➢ **Chứng thực và liên kết:**

Quá trình này có ba trạng thái phân biệt:

1. Không chứng thực và không liên kết (Unauthenticated and unassociated).
2. Chứng thực và không liên kết (Authenticated and unassociated).
3. Chứng thực và liên kết (Authenticated and associated)

Theo sơ đồ sau:

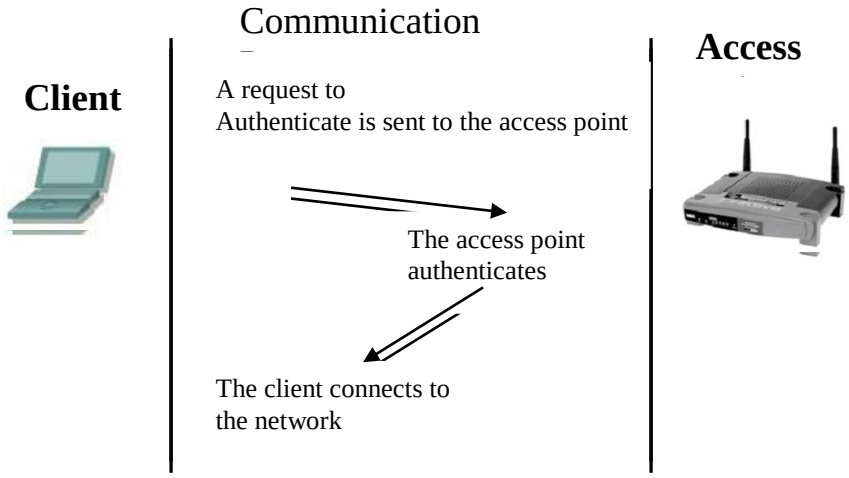


Hình 2.15: Qúa trình chứng thực và liên kết

❖ **Quá trình chứng thực hệ thống mở:**

Quá trình này thực hiện đơn giản theo hai bước sau:

1. Máy client gửi một yêu cầu liên kết tới AP
2. AP chứng thực máy khách và gửi một trả lời xác thực client được liên kết



Hình 2.16: Quá trình chứng thực hệ thống mở

Phương pháp này đơn giản và bảo mật hơn phương pháp chứng thực khóa chia sẻ. Phương pháp này được 802.11 cài đặt mặc định trong các thiết bị WLAN. Sử dụng phương pháp này một trạm có thể liên kết với bất cứ một AP nào sử dụng phương pháp chứng thực hệ thống mở khi nó có SSID đúng. SSID đó phải phù hợp trên cả AP và client trước khi client đó hoàn thành quá trình chứng thực. Quá trình chứng thực hệ thống mở dùng cho cả môi trường bảo mật và môi trường không bảo mật. Trong phương pháp này thi WEP chỉ được sử dụng để mã hóa dữ liệu, nếu có.

❖ **Chứng thực chia sẻ khóa:**

Phương pháp này bắt buộc phải dùng WEP.

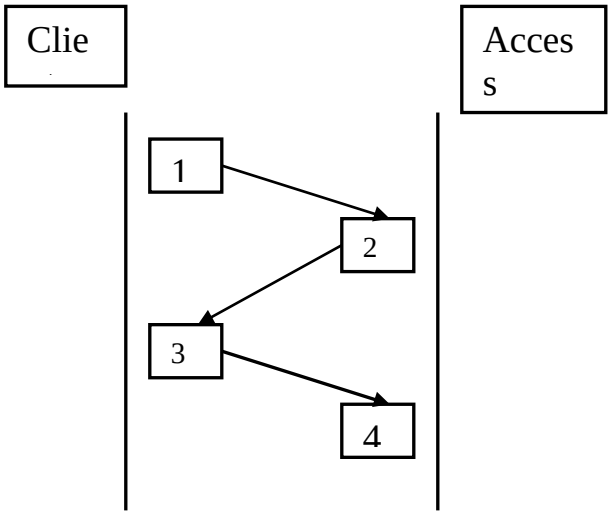
Một quá trình chứng thực khóa chia sẻ xảy ra theo các bước sau:

1. Một client gửi yêu cầu liên kết tới AP, bước này giống như chứng thực hệ thống mở.

2. AP gửi một đoạn văn bản ngẫu nhiên tới client, văn bản này chưa được mã hóa, và yêu cầu Client dùng chìa khóa WEP của nó để mã hóa.

3. Client mã hóa văn bản với chìa khóa WEP của nó và gửi văn bản đã được mã hóa đó đến AP.

4. AP sẽ thử giải mã văn bản đó, để xác định xem chìa khóa WEP của Client có hợp lệ không, nếu có thì nó gửi một trả lời cho phép, còn nếu không, thì nó trả lời bằng một thông báo không cho phép Client đó liên kết.



Hình 2.17: Quá trình chứng thực khóa chia sẻ

Nhìn qua thì phương pháp này có vẻ an toàn hơn phương pháp chứng thực hệ thống mở, nhưng nếu xem xét kỹ thì trong phương pháp này, chìa khóa Wep được dùng cho hai mục đích, để chứng thực và để mã hóa dữ liệu, đây chính là kẽ hở để hacker có cơ hội thâm nhập mạng. Hacker sẽ thu cả hai tín hiệu, văn bản chưa mã hóa do AP gửi và văn bản đã mã hóa, do Client gửi, và từ hai thông tin đó Hacker có thể giải mã ra

được chìa khóa WEP. Để đối phó với Hacker, người ta dùng 2 chìa khóa: một để xác thực và một chìa khóa khác để mã hóa.

2.6. Kỹ thuật điều chế

2.6.1. Kỹ thuật điều chế số SHIFT KEYING

Hiện nay có rất nhiều phương thức thực hiện điều chế số Shift Keying như: ASK, FSK, PSK…Quá trình điều chế được thực hiện bởi khóa chuyển (keying) giữa hai trạng thái (states), một cách lý thuyết thì một trạng thái sẽ là 0 còn một trạng thái sẽ là 1, (chuỗi 0/1 trước khi điều chế là chuỗi số đã được mã hóa đường truyền).

PSK đã được phát triển trong suốt thời kỳ đầu của chương trình phát triển vũ trụ và ngày nay được sử dụng rộng rãi trong các hệ thống thông tin quân sự và thương mại. Nó tạo ra xác xuất lỗi thấp nhất với mức tín hiệu thu cho trước khi đo một chu kỳ tín hiệu.

- **Nguyên lý cơ bản của điều chế PSK**

Dạng xung nhị phân coi như là đầu vào của bộ điều khiển PSK sẽ biến đổi về pha ở dạng tín hiệu ra thành một trạng thái xác định trước, và do đó tín hiệu ra được biểu thị bằng phương trình sau:

$$V_0(t) = E\sin\left[\varpi_0 t + \frac{2\pi(i-1)}{M}\right]$$

i= 1,2,…,M

M=2N, số lượng trạng thái pha cho phép

N= Số lượng các bit số liệu cần thiết để thiết kế trạng thái pha M

Nhìn chung thì có 3 kỹ thuật điều chế PSK: khi M=2 thì là BPSK, khi M=4 thì là QPSK và khi M=8 thì là 8(phi)-PSK.

Ở đây cần nghi nhớ rằng khi số lượng các trạng thái pha tăng lên thì tốc độ bit cũng tăng nhưng tốc độ boud vẫn giữ nguyên. Tuy nhiên muốn tăng tốc độ số

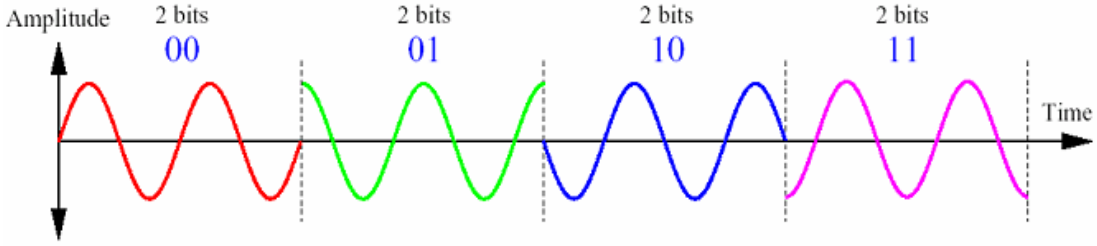
liệu thì phải trả giá. Nghĩa là, yêu cầu về S/N tăng lên để giữ nguyên được BER (tỷ lệ lỗi bit)

- **Khóa chuyển dịch pha (Phase Shifp Keying – PSK/Binary PSK):**

Đây là phương pháp thông dụng nhất, tín hiệu sóng mang được điều chế dựa vào chuỗi nhị phân, tín hiệu điều chế có biên độ không thay đổi và biến đổi giữa hai trạng thái 0^0 và 180^0, mỗi trạng thái của tín hiệu điều chế được gọi là symbol.

- **QPSK(Quardrature Phase Shift Keying):**

Ở phương pháp BPSK, mỗi symbol biểu diễn cho một bit nhị phân. Nếu mỗi symbol này biểu diễn hơn 1 bit, thì sẽ đạt được một tốc độ bit lớn hơn. Với QPSK sẽ gấp đôi số thông lượng dữ liệu của PSK với cùng một băng thông bằng cách mỗi symbol mang 2 bit. Như vậy trạng thái phase của tín hiệu điều chế sẽ chuyển đổi giữa các giá trị -90^0,0^0,90^0 và 180^0.



$$s(t) = \begin{cases} A\cos(2\pi f_c t + 0^\circ) & 00 \\ A\cos(2\pi f_c t + 90^\circ) & 01 \\ A\cos(2\pi f_c t + 180^\circ) & 10 \\ A\cos(2\pi f_c t + 270^\circ) & 11 \end{cases}$$

Dibit	Phase
00	0
01	90
10	180
11	270

Dibit (2 bits)

- **CCK(Complementary Code Keying): Khóa mã bổ xung**

CCK là một kỹ thuật điều chế phát triển từ điều chế QPSK, nhưng tốc độ bit đạt đến 11Mbps với cùng một băng thông(hay dạng sóng) như QPSK. Đây là một kỹ thuật điều chế rất phù hợp cho các ứng dụng băng rộng. Theo chuẩn IEEE802.11b, điều chế CCK dùng chuỗi số giả ngẫu nhiên có chiều dài mã là 8 và tốc độ chipping rate là 11Mchip/s. 8complex chips sẽ kết hợp tạo thành một symbol đơn (như trong QPSK – 4 symbol). Khi tốc độ symbol là 1,375MSymbol/s thì tốc độ dữ

liệu sẽ đạt được: 1,375x8=11Mbps với cùng băng thông xấp xỉ như điều chế QPSK tốc độ 2Mbps.

2.6.2. Kỹ thuật điều chế song công

Trong các hệ thống điểm-đa điểm, hiện nay tồn tại hai kỹ thuật song công (hoạt động ở cả chiều lên và chiều xuống, upstream và downstream) đó là:

Phân chia theo tần số (Frequency Division Duplexing, FDD): Kỹ thuật này cho phép phân chia tần số sử dụng ra làm hai kênh riêng biệt: một kênh cho chiều xuống và một kênh cho chiều lên.

Phân chia theo thời gian (Time Division Duplexing, TDD): Kỹ thuật này mới hơn, cho phép lưu lượng lưu thông theo cả 2 chiều trong cùng một kênh, nhưng tại các khe thời gian khác nhau.

Việc lựa chọn FDD hay TDD phụ thuộc chủ yếu vào mục đích sử dụng chính của hệ thống, các ứng dụng đối xứng (thoại) hay không đối xứng (dữ liệu).

Kỹ thuật FDD sử dụng băng thông tỏ ra không hiệu quả đối với các ứng dụng dữ liệu. Trong hệ thống sử dụng kỹ thuật FDD, băng thông cho mỗi chiều được phân chia một cách cố định. Do đó, nếu lưu lượng chỉ lưu thông theo chiều xuống, ví dụ như khi xem các trang Web, thì băng thông của chiều lên không được sử dụng. Điều này lại không xảy ra khi hệ thống được sử dụng cho các ứng dụng thoại: Hai chiều nói chuyện thường nói nhiều như nghe, do đó băng thông của hai chiều lên, xuống được sử dụng xấp xỉ như nhau. Đối với các ứng dụng truyền dữ liệu tốc độ cao hoặc ứng dụng hình ảnh thì chỉ có băng thông chiều xuống được sử dụng, còn chiều lên gần như không được sử dụng.

Đối với kỹ thuật TDD, số lượng khe thời gian cho mỗi chiều thay đổi một cách linh hoạt và thường xuyên. Khi lưu lượng chiều lên nhiều, số lượng khe thời gian dành cho chiều lên sẽ tăng lên, và ngược lại. Với sự giám sát số lượng khe thời gian cho một chiều, hệ thống sử dụng kỹ thuật TDD hỗ trợ cho sự bùng nổ thông lượng truyền dẫn đối với cả hai chiều. Nếu một trang Web lớn đang được tải xuống thì các khe thời gian của chiều lên sẽ được chuyển sang cấp phát cho chiều xuống.

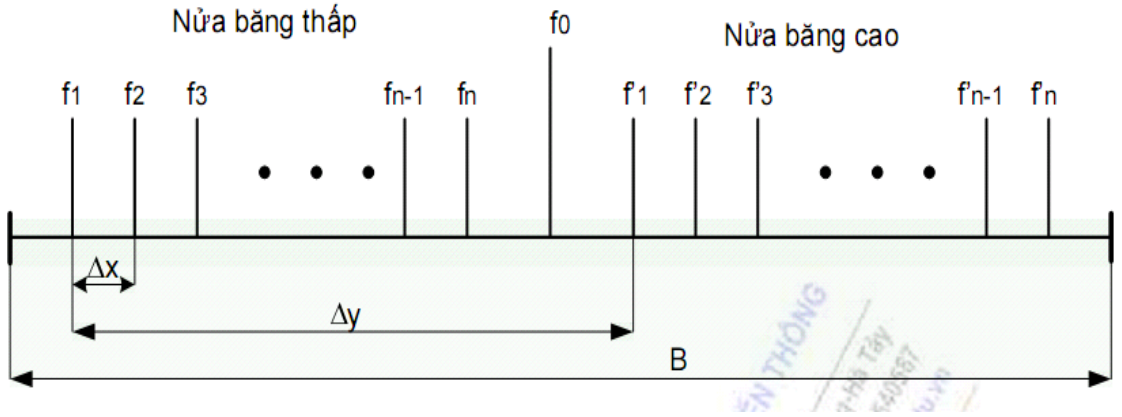
Nhược điểm chủ yếu của kỹ thuật TDD là việc thay đổi chiều của lưu lượng tốn nhiều thời gian, việc cấp phát khe thời gian là một vấn đề rất phức tạp cho các hệ thống phần mềm. Hơn nữa, kỹ thuật TDD yêu cầu sự chính xác cao về thời gian. Tất cả các máy trạm trong khu vực của một hệ thống sử dụng kỹ thuật TDD cần có một điểm thời gian tham chiếu để xác định chính xác các khe thời gian. Chính điều này làm giới hạn phạm vi địa lý bao phủ đối với các hệ thống điểm- đa điểm

2.7. Kỹ thuật truy nhập:

➢ **FDMA(Frequency Division Multiple Access) – đa truy nhập phân chia theo tần số**

Phổ tần dùng cho thông tin liên lạc được chia thành 2N dải tần số kế tiếp, cách nhau bởi một dải tần phòng vệ. Mỗi dải tần số được gán cho một kênh liên lạc, N dải dành cho liên lạc hướng lên, sau một dải tần phân cách là N dải tần dành cho liên lạc hướng xuống. Mỗi CPE được cấp phát một đôi kênh liên lạc trong suốt thời gian kết nối, nhiễu giao thoa xảy ra ở đây là rất đáng kể.

Trong mỗi nửa băng tần người ta bố trí các tần số cho các kênh. Trong các cặp tần số ở nửa băng thấp va nửa băng cao có cùng chỉ số được gọi là khoảng cách thu phát hay song công, một tần số sẽ được sử dụng cho máy thu của cùng một kênh, khoảng cách giữa 2 tần số này gọi là khoảng cách thu phát song công.



Hình 2.18: Mô hình FDMA

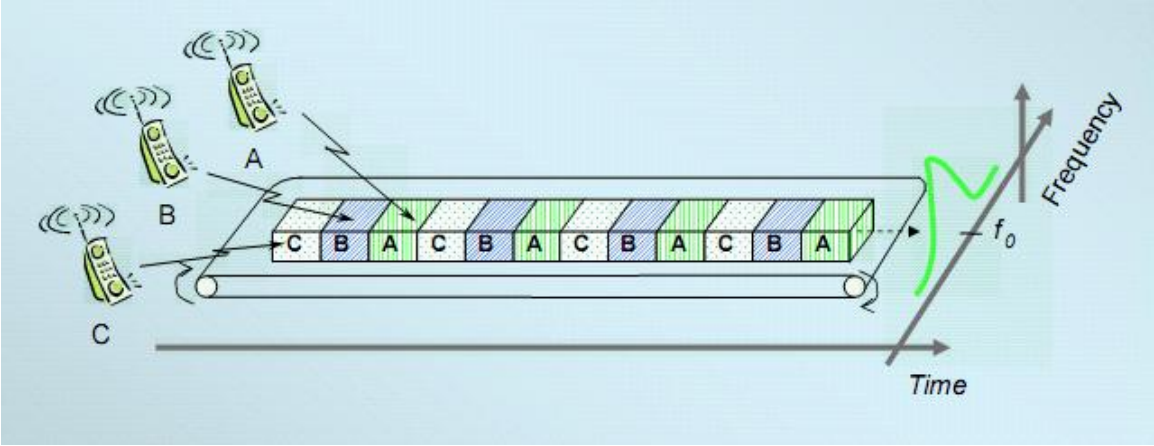
Trong đó:

- Δx: Khoảng cách tần số giữa 2 kênh lân cận

- Δy: Khoảng cách tần số thu phát
- B: Băng thông cấp phát cho hệ thống
- f0: Tần số trung tâm
- f'i: Tần số đường xuống
- fi: Tần số đường lên

➢ **TDMA(Time Division Multiple Access) – đa truy nhập phân chia theo thời gian.**

Phổ tần số được chia thành các dải tần liên lạc, mỗi dải tần này được dùng chung cho N kênh liên lạc. Mỗi kênh liên lạc là một khe thời gian trong chu kỳ một khung. Liên lạc được thực hiện song công theo mỗi hướng thuộc các dải tần liên lạc khác nhau, điều này sẽ làm giảm nhiễu giao thoa một cách đáng kể.



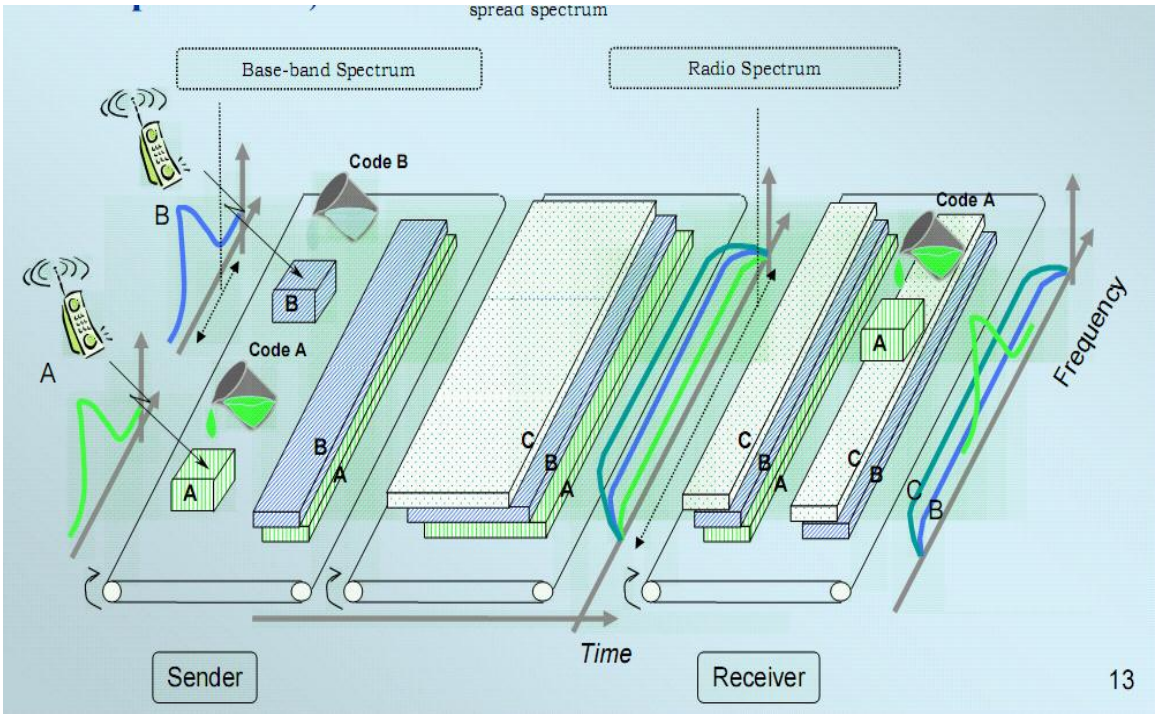
Hình 2.19: Mô hình TDMA

➢ **CDMA(Code Division Multiple Access)- đa truy nhập phân chia theo mã**

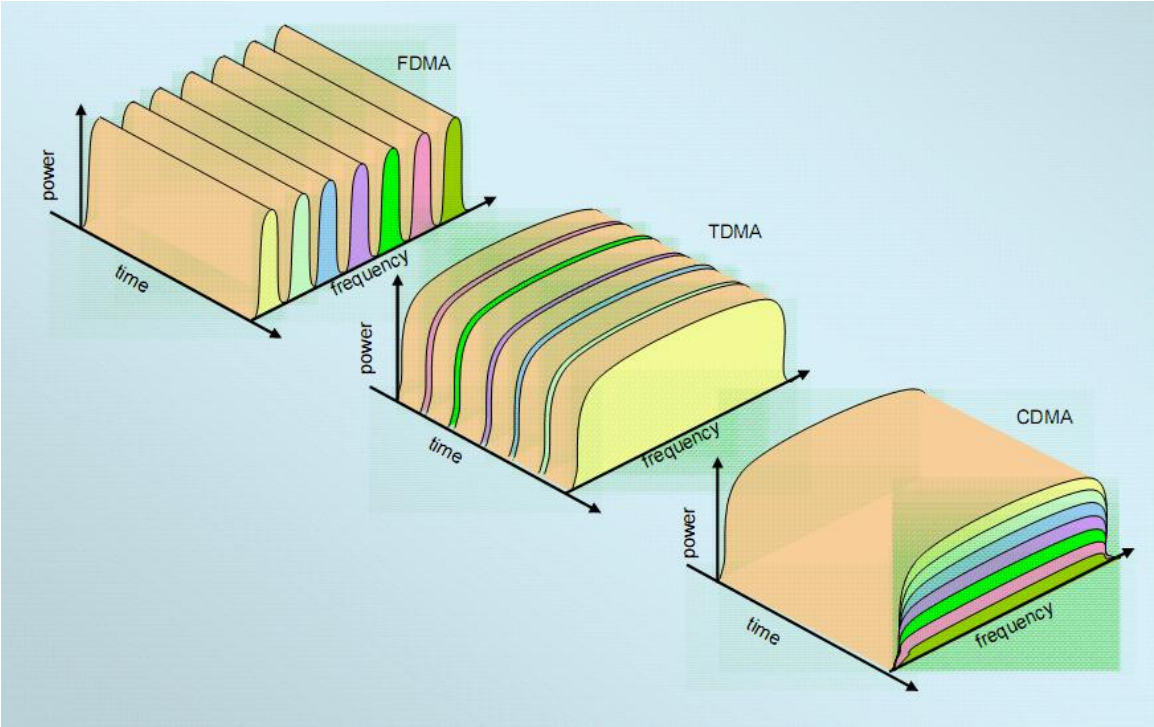
CDMA là phương pháp đa truy nhập mà ở đó mỗi kênh được cung cấp một cặp tần số và một mã duy nhất.

Mỗi CPE được gán một mã riêng biệt, với kỹ thuật trải phổ tín hiệu giúp cho các CPE không gây nhiễu lẫn nhau trong điều kiện đồng thời dùng chung một dải tần số. Dải tần số tín hiệu có thể rộng tới hàng chục Mhz. Sử dụng kỹ thuật trải phổ phức tạp cho phép tín hiệu vô tuyến sử dụng có cường độ trường rất nhỏ và chống

pha đinh hiệu quả hơn FDMA, TDMA. Bên cạnh đó việc các CPE trong cùng một trạm gốc sử dụng chung dải tần số sẽ giúp cho cấu trúc hệ thống truyền dẫn thu phát vô tuyến trở nên rất đơn giản.



Hình 2.20: Mô hình CDMA



Hình 2.21: Mô hinh tổng quát FDMA, TDMA, CDMA

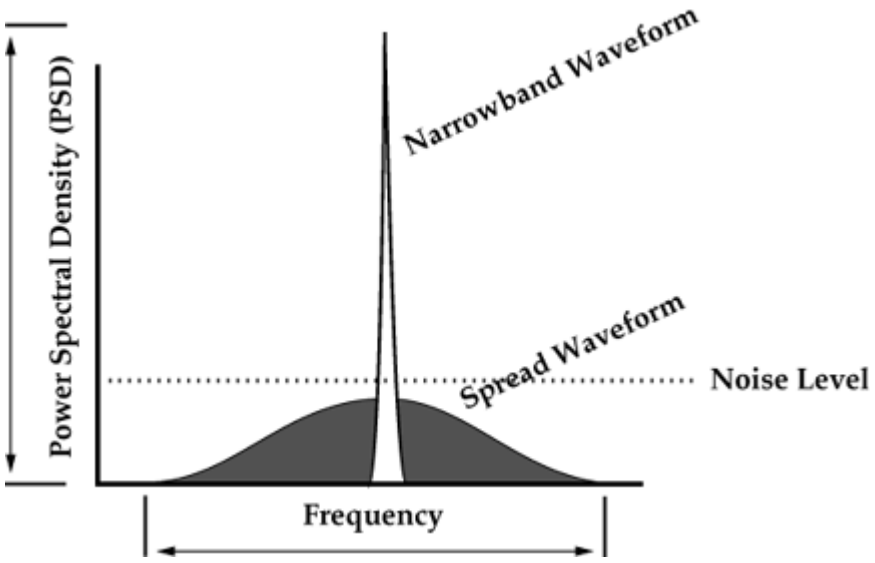
2.8. Kỹ thuật vô tuyến

➢ Viba truyền thống

Trong kỹ thuật viba truyền thống mỗi CPE sẽ được cụng cấp một hoặc một cặp tần số băng hẹp để hoạt động. Dải tần băng hẹp này được dành vĩnh viễn cho thuê bao đăng ký, mọi tín hiệu của các CPE khác lọt vào trong dải tần này được coi là nhiễu và làm ảnh hưởng đến hoạt động của kênh. Việc cấp phát tần số như trên làm hạn chế số người sủ dụng kênh vô tuyên vì tài nguyên vô tuyến là có hạn. Và vì là dải tần băng hẹp nên đương nhiên sẽ dẫn đến sự hạn chế về tốc độ của kênh truyền dẫn. Do đó viba truyên thống tỏ ra chỉ thích hợp cho các ứng dụng thoại và dữ liệu tốc độ thấp.

Hình dưới minh họa sự khác nhau giữa truyền thông băng hẹp và truyền thông trải phổ. Chú ý là một trong những đặc điểm của băng hẹp là công suất đỉnh (peak power) cao. Khi sử dụng dãy tần số càng nhỏ để truyền thông tin thì công suất yêu cầu càng lớn. Để cho tín hiệu băng hẹp có thể nhận được chúng phải nằm ở trên mức nhiễu chung (còn gọi là nhiễu nền – noise floor) một lượng đáng kể.

Bởi vì băng tần của nó khá là hẹp, nên công suất đỉnh cao bảo đảm cho việc tiếp nhận tín hiệu băng hẹp không có lỗi.



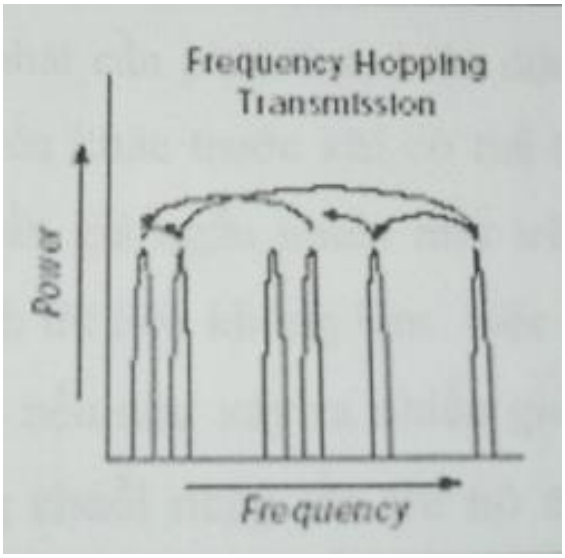
Hình 2.22: Truyền thông băng hẹp

Một chứng cứ thuyết phục chống lại truyền thông băng hẹp (ngoài việc yêu cầu sử dụng công suất đỉnh cao) là tín hiệu băng hẹp có thể bị jammed (tắt nghẽn) hay interference (nhiễu) rất dễ dàng. Jamming là một hành động cố ý sử dụng công suất rất lớn để truyền tín hiệu không mong muốn vào cùng dãy tần số với tín hiệu mong muốn. Bởi vì băng tần của nó là khá hẹp, nên các tín hiệu băng hẹp khác bao gồm cả nhiễu có thể hủy hoại hoàn toàn thông tin bằng cách truyền tín hiệu băng hẹp công suất rất cao

- **Kỹ thuật trải phổ**

Khi tài nguyên vô tuyến ngày càng trở nên cạn kiệt, người ta bắt đầu phải áp dụng kỹ thuật trải phổ nhằm nâng cao hiệu năng sử dụng tần số. Có hai kỹ thuật trải phổ thông dụng nhất hiện nay là FHSS và DSSS. Băng thông cho mỗi CPE sẽ không còn là một dải hẹp mà sẽ là toàn bộ băng tần số, việc xác định CPE thông qua một mã code của mỗi CPE – mã giả ngẫu nhiên (PN sequence)

FHSS(Frequency Hopping Spread Spectrum)



Hình 2.23: Nhảy tần số

Tín hiệu dữ liệu được truyền trên một dải tần rộng bằng kỹ thuật truyền tín hiệu trên những tần số sóng mang khác nhau tại những thời điểm khác nhau. Khoảng cách giữa các tần số sóng mang FHSS được qui định trước, băng thông cho mỗi kênh khoảng 1Mhz, trật tự nhảy tần được xác định bằng một hàm giả ngẫu nhiên. FCC yêu cầu băng thông phải được chia ít nhất thành 75 kênh (subchannel). FHSS radio được giới hạn chỉ gửi một lượng nhỏ dữ liệu trên mỗi kênh trong một chu kỳ thời gian xác định, trước khi nhảy sang kênh tần số kế tiếp trong chuỗi nhảy tần. Chu kỳ thời gian này gọi là dwell time, thường có giá trị khoảng 400 microseconds. Sau mỗi bước nhảy (hop) thiết bị thu phát cần phải thực hiện đồng bộ (resynchronize) với những tần số vô tuyến khác trước khi có thể truyền dữ liệu. Mục đích chủ yếu của việc nhảy tần giả ngẫu nhiên như trên là để tránh hiện tượng giao thoa tín hiệu không làm việc quá lâu trên một kênh tần số cụ thể nào đó. Giả sử nếu như xảy ra nhiễu giao thoa nghiêm trọng trên một tần số nào đó trong chuỗi nhảy tần thì nó cũng ảnh hưởng không nhiều đến hệ thống. Bởi quá trình truyền chỉ được thực hiện tại đây trong một khoảng thời gian nhỏ.

DSSS(Direct Sequence Spread Strectrum)

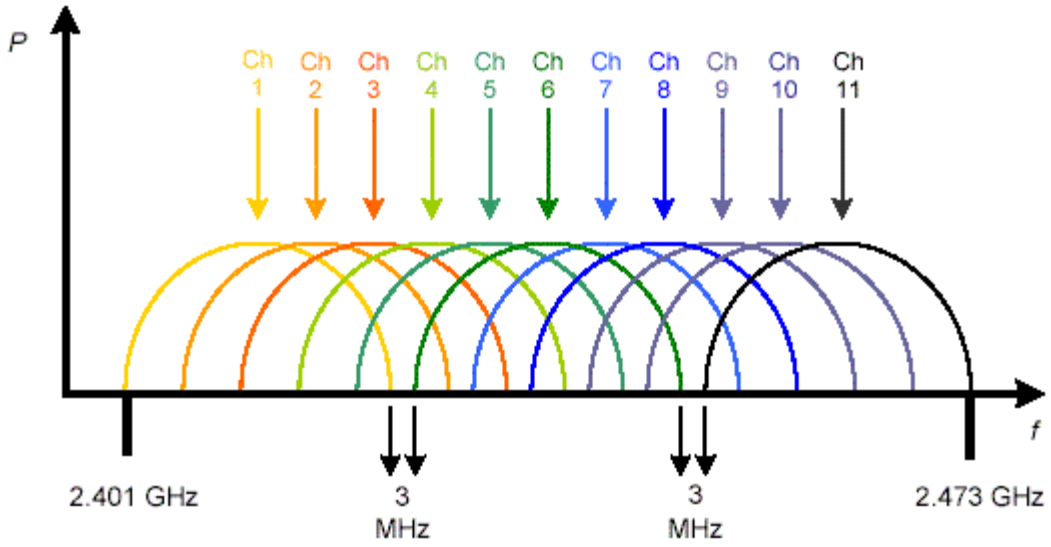
DSSS cũng thực hiện việc trải phổ tín hiệu như trên nhưng theo một kỹ thuật khác. Băng thông của tín hiệu thay vì được truyền trên một băng hẹp (narrow band)

như truyền thông viba, sẽ được truyền trên một khoảng tần số lớn hơn bằng kỹ thuật mã hoá giả ngẫu nhiên (Pseudo-noise sequence).

Tín hiệu băng hẹp và tín hiệu trải phổ cùng được phát với một công suất và một dạng thông tin nhưng mật độ phổ công suất của tín hiệu trải phổ lớn hơn nhiều so với tín hiệu băng hẹp. Tín hiệu dữ liệu kết hợp với chuỗi mã giả ngẫu nhiên trong quá trình mã hoá sẽ cho ra một tín hiệu với băng thông mở rộng hơn nhiều so với tín hiệu ban đầu nhưng với mức công suất lại thấp hơn. Một ưu điểm nổi bật của kỹ thuật DSSS là khả năng dự phòng dữ liệu. Bên trong tín hiệu DSSS sẽ gộp dự phòng ít nhất 10 dữ liệu nguồn trong cùng một thời gian. Phía thu chỉ cần đảm bảo thu tốt được 1 trong 10 tín hiệu dự phòng trên là đã thành công. Nếu có tín hiệu nhiễu trong băng tần hoạt động của tín hiệu DSSS, tín hiệu nhiễu này có công suất lớn hơn và sẽ được hiểu như một tín hiệu băng hẹp. Do đó, trong quá trình giải mã tại đầu thu, tín hiệu nhiễu này sẽ được trải phổ và dễ dàng loại bỏ bởi việc xử lý độ lợi (gain processing). Xử lý độ lợi là quá trình làm giảm mật độ phổ công suất khi tín hiệu được xử lý để truyền và tăng mật độ phổ công suất khi giải trải phổ, với mục đích chính là làm tăng tỉ số S/N.

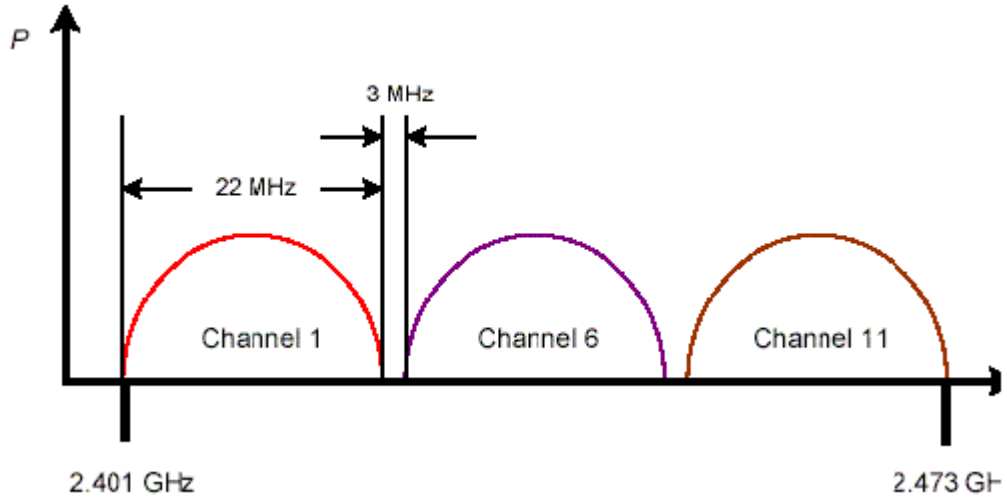
Theo chuẩn 802.11b, thì sử dụng 14 kênh DS(Direct Sequence) trong dải băng tần 2,4 GHz, mỗi kênh truyền rộng 22MHZ, nhưng các kênh chỉ cách nhau 5MHZ, vì vậy các kênh cạnh nhau sẽ giao thoa lẫn nhau.

Ví dụ, kênh 1 hoạt động từ 2.401 GHz đến 2.423 GHz (2.412 GHz +/- 11MHz); kênh 2 hoạt động từ 2.406 GHz đến 2.429 GHz (2.417 GHz +/- 11 MHz)… Hình dưới minh họa điều này



Hình 2.24: Các kênh trong DSSS

Do đó trong 1 khu vực người ta bố trí các kênh truyền sao cho miền tần số của chúng không chồng lên nhau, trong hệ thống 14 kênh DS thì có tối đa 3 kênh đảm bảo không chồng lấn trên lý thuyết, ví dụ trong hình sau thì các kênh 1,6,11 được sử dụng để phát trong một khu vực mà không gây nhiễu giao thoa cho nhau.



Hình 2.25: Kênh không trùng lặp trong DSSS

Như vậy trong 1 vùng đơn tốc độ bit vận chuyển đến có thể lên tới : 11Mbpsx3=33Mbps,thay vì 11Mbps như khi chỉ có một kênh truyền được sử dụng trong một khu vực.

So sánh FHSS và DSSS

FH không có quá trình xử lí độ lợi do tín hiệu không được trải phổ. Vì thế nó phải dùng nhiều công suất hơn để có thể truyền tín hiệu với cùng mức S/N so với tín hiệu DS. Tuy nhiên tại băng sóng ISM, theo quy định có mức giới hạn công suất phát, do đó FH không thể đạt được S/N giống như DS. Bên cạnh đó việc dùng FH rất khó khăn trong việc đồng bộ giữa máy phát và thu vì cả thời gian và tần số đều yêu cầu cần phải được đồng bộ. Trong khi DS chỉ cần đồng bộ về thời gian của các chip. Chính vì vậy FH sẽ phải mất nhiều thời gian để tìm tín hiệu hơn, làm tăng độ trễ trong việc truyền dữ liệu hơn so với DS.

Ngoài ra cả công nghệ FHSS và DSSS đều có điểm thuận lợi và bất lợi. Và nhiệm vụ của WLAN administrator là phải quyết định chọn lựa sử dụng công nghệ nào khi cài đặt mạng WLAN mới. Phần này sẽ mô tả một số yếu tố nên xem xét để xác định xem công nghệ nào là thích hợp với bạn nhất. Các yếu tố này bao gồm:

- Nhiễu băng hẹp
- Co-location
- Chi phí
- Tính tương thích và tính sẵn có của thiết bị
- Tốc độ và băng thông dữ liệu
- Bảo mật
- Hỗ trợ chuẩn.

Nhiễu băng hẹp

Điểm thuận lợi của FHSS là khả năng kháng nhiễu băng hẹp cao hơn so với DSSS. Hệ thống DSSS có thể bị ảnh hưởng bởi nhiễu băng hẹp nhiều hơn FHSS bởi vì chúng sử dụng băng tần rộng 22 MHz thay vì 79 MHz. Yếu tố này có thể được xem như là yếu tố quyết định khi bạn dự định triển khai mạng WLAN trong môi trường có nhiều nhiễu.

Chi phí

sKhi cài đặt mạng WLAN, những điểm thuận lợi của DSSS đôi khi hấp dẫn hơn FHSS đặc biệt là khi có ngân sách hạn chế. Chi phí của việc cài đặt một hệ thống DSSS thường thấp hơn rất nhiều so với FHSS. Thiết bị DSSS rất phổ biến trên thị trường và ngày càng giảm giá. Chỉ một vài năm gần đây, giá của thiết bị đã có thể chấp nhận được đối với khách hàng doanh nghiệp.

Co-location

Một điểm thuận lợi của FHSS so với DSSS là khả năng có nhiều hệ thống FHSS cùng hoạt động với nhau (co-located). Vì hệ thống nhảy tần sử dụng sự nhanh nhẹn của tần số và sử dụng 79 kênh riêng biệt nên số lượng co-located nhiều hơn so với DSSS (chỉ 3 co-locate system hay 3 AP)

Tuy nhiên, khi tính toán chi phí phần cứng của hệ thống FHSS để đạt được cùng băng thông như DSSS thì lợi thế này không còn nữa. Bởi vì DSSS có 3 co-located AP nên băng thông tối đa cho cấu hình này là:

3 AP * 11 Mbps = 33 Mbps

Với khoảng 50% băng thông dành cho chi phí do các giao thức được sử dụng nên băng thông còn lại khoảng :

33 Mbps / 2 = 16.5 Mbps

Trong khi đó, để đạt được cùng mức băng thông tương tự thì FHSS yêu cầu:

16 AP * 2 Mbps = 32 Mbps

Và cũng vơi 50% chi phí thì băng thông thật sự là

32 Mbps / 2 = 16 Mbps

Trong cấu hình này, hệ thống FHSS yêu cầu phải mua thêm 13 AP nữa để có được băng thông tương tự DSSS. Thêm vào đó là chi phí cho dịch vụ cài đặt, cable, đầu nối và anten.

Bạn có thể thấy rằng có nhiều thuận lợi khác nhau đối với mỗi loại công nghệ. Nếu như mục tiêu là chi phí thấp và băng thông cao thì hiển nhiên công nghệ DSSS sẽ thắng. Nếu như mục tiêu là phân chia người dùng sử dụng các AP khác nhau trong một môi trường co-located dày đặc thì FHSS sẽ thích hợp hơn.

Tính tương thích và tính sẵn có của thiết bị

WECA (Wireless Ethernet Compatibility Alliance) cung cấp kiểm tra tính tương thích DSSS của các thiết bị 802.11b để đảm bảo rằng những thiết bị như vậy sẽ hoạt động được với nhau và hoạt động được với các thiết bị 802.11b DSSS khác. Chuẩn tương thích mà WECA tạo ra được biết với tên gọi là Wi-Fi (Wireless Fidelity) và các thiết đã qua kiểm tra tương thích được gọi là các thiết bị tuân theo Wi-Fi (Wi-Fi compliant). Các thiết bị này được thêm vào logo Wi-Fi lúc xuất hiện trên thị trường. Logo này nói lên rằng thiết bị đó có thể giao tiếp được với các thiết bị khác có logo Wi-Fi.

Không có một sự kiểm tra tương tự nào dành cho FHSS. Có các chuẩn sử dụng FHSS như 802.11 và OpenAir, nhưng không có tổ chức nào làm công việc kiểm tra tính tương thích FHSS tương tự như WECA cho DSSS.

Bởi vì tính phổ biến của các thiết bị 802.11b nên rất dễ dàng mua được chúng. Nhu cầu ngày càng phát triển cho các thiết bị tương thích Wi-Fi trong khi nhu cầu cho FHSS gần như đã bảo hòa và đi xuống.

Tốc độ và băng thông dữ liệu.

Như chúng ta đã biết là tốc độ của FHSS (2 Mbps) thấp hơn nhiều so với DSSS (11 Mbps). Mặc dù một số hệ thống FHSS có thể hoạt động ở tốc độ 3 Mbps hay lớn hơn nhưng các hệ thống này là không tương thích với chuẩn 802.11 và có thể không giao tiếp được với hệ thống FHSS khác. Hệ thống FHSS và DSSS có thông lượng (dữ liệu thật sự được truyền) chỉ khoảng một nửa tốc độ dữ liệu. Khi kiểm tra thông lượng lúc cài đặt một mạng WLAN mới thường chỉ đạt được 5 – 6 Mbps đối với DSSS và 1 Mbps đối với FHSS cho dù đã thiết lập tốc độ tối đa.

HomeRF sử dụng công nghệ nhảy tần băng rộng để đạt được tốc độ dữ liệu 10 Mbps (khoảng 5 Mbps thông lượng). HomeRF sử dụng công suất phát giới hạn là 125 mW.

Khi các frame wireless được truyền thì sẽ có khoảng thời gian tạm ngừng giữa các frame cho các tín hiệu điều khiển và các tác vụ khác. Với hệ thống nhảy tần thì khoảng chèn giữa các frame (interframe space) này là lớn hơn so với DSSS

gây ra giảm tốc độ truyền dữ liệu. Hơn nữa, hệ thống nhảy tần còn có thêm quá trình thay đổi tốc độ truyền, trong khoảng thời gian này thì không có dữ liệu nào được truyền. Một số hệ thống WLAN sử dụng các giao thức lớp vật lý riêng để làm tăng băng thông. Các phương pháp này làm tăng thông lượng lên đến 80% so với tốc độ dữ liệu nhưng có thể sẽ không tương thích được với thiết bị chuẩn.

Security

Theo các quảng cáo (thường là không đúng sự thật) thì hệ thống nhảy tần là an toàn hơn hệ thống DSSS. Chứng cứ đầu tiên bác bỏ điều này chính là FHSS radio chỉ được sản xuất bởi một số ít các nhà sản xuất nên chúng phải tuân theo chuẩn để có thể bán thiết bị được dễ dàng. Thứ 2 là các nhà sản xuất sử dụng một tập các chuỗi nhảy chuẩn thường là theo một danh sách xác định trước do các tổ chức như IEEE hay WLIF đưa ra. Hai điều này làm cho việc phát hiện được chuỗi nhảy khá là đơn giản.

Một lý do khác làm cho việc tìm được chuỗi nhảy của FHSS đơn giản chính là việc số kênh luôn được quảng bá (không mã hóa) trong mỗi Beacon phát ra. Địa chỉ MAC của AP truyền cũng bao gồm trong Beacon vì thế chúng ta có thể biết được nhà sản xuất thiết bị. Một số nhà sản xuất cho phép administrator định nghĩa linh động hop pattern tùy ý. Tuy nhiên, nó cũng chẳng tạo thêm được mức bảo mật nào cả vì một số thiết bị đơn giản như bộ phân tích phổ (Spectrum Analyzer), máy laptop có thể được sử dụng để theo dõi hopping pattern của FHSS radio trong vòng vài giây.

Hỗ trợ chuẩn

Như đã thảo luận ở phần trước, DSSS đã giành được sự chấp nhận rộng rãi do chi phí thấp, tốc độ cao, chuẩn tương thích Wi-Fi và nhiều yếu tố khác. Sự chấp nhận này làm thúc đẩy nghành công nghiệp chuyển sang công nghệ mới hơn và nhanh hơn DSSS như 802.11g hay 802.11a. Chuẩn tương thích mới của WECA là Wi-Fi5 dành cho hệ thống DSSS hoạt động ở 5 GHz UNII sẽ giúp đẩy nhanh ngành công nghiệp phát triển hơn nữa như Wi-Fi đã từng làm. Các chuẩn mới cho hệ thống FHSS như HomeRF 2.0 và 802.15 (hỗ trợ cho WPAN như Bluetooth) nhưng đều không nâng cấp hệ thống FHSS trong doanh nghiệp.

Như vậy chúng ta có thể thấy DSSS là kĩ thuật trải phổ có nhiều đặc điểm ưu việt hơn hẳn FHSS.

2.9.Vấn đề bảo mật

- **Chứng thực qua hệ thống mở (Open Authentication)**

Đây là hình thức chứng thực qua việc xác định chính xác SSIDs (Service Set Identifiers) một tập dịch vụ mở rộng (ESS- Extended Service Set) gồm hai hoặc nhiều hơn các điểm truy nhập không dây được kết nối tới cùng một mạng có dây, là một phân đoạn mạng logic đơn (còn được gọi là một mạng con) và được nhận dạng bởi SSID. Bất kì một CPE nào không có SSID hợp lệ sẽ không được truy nhập tới ESS.

- **Chứng thực qua khoá chia sẻ(Shared- Key authentication)**

Là kiểu chứng thực cho phép kiểm tra một khách hàng không dây đang được chứng thực có biết về bí mật chung không. Điều này tương tự với khoá chứng thực chia sử trước trong bảo mật IP(IP Sec). Chuẩn 802.11 hiện nay giả thiết rằng khoá dùng chung được phân phối đến tất cả các khách hàng đầu cuối thông qua một kênh bảo mật riêng phải độc lập với tất cả các kênh khác IEEE 802.11. Tuy nhiên, hình thức chứng thực qua khoá chia sẻ nói chung là không an toàn và không được khuyến nghị sử dụng .

- **Bảo mật dữ liệu thông qua WEP(Wired Equivalent Privacy)**

Với thuộc tính cố hữu của mạng không dây, truy nhập an toàn tại lớp vật lý tới mạng không dây là một vấn đề tương đối khó khăn. Bởi vì, không cần đến một cổng vật lý riêng bất cứ người nào trong phạm vi của một điểm truy nhập dịch vụ không dây cũng có thể gửi và nhận khung cũng như theo dõi các khung đang được gửi khác. Chính vì thế WEP(được định nghĩa bởi chuẩn IEEE 802.11) được xây dựng với mục đích cung cấp mức bảo mật dữ liệu tương đương với các mạng có dây. Nếu không có WEP, việc nghe trộm và phát hiện gói từ xa sẽ trở nên rất dễ dàng. WEP cung cấp các dịch vụ bảo mật dữ liệu bằng cách mã hoá dữ liệu để gửi giữa các node không dây. Mã hoá WEP dùng luồng mật mã đối xứng RC4 cách với từ khoá dài 40bit hoặc 104 bit. WEP cung cấp độ toàn vẹn của dữ liệu từ các lỗi

ngẫu nhiên bằng cách gộp một giá trị kiểm tra độ toàn vẹn (ICV- Integrity Check Value) vào phần được mã hoá của khung truyền không dây.

Việc xác định và phân phối các chìa khoá WEP không được định nghĩa và phải được phân phối thông qua một kênh an toàn và độc lập với 802.11.

- **Bảo mật dữ liệu thông qua EAP(Extensible Authentication Protocol)**

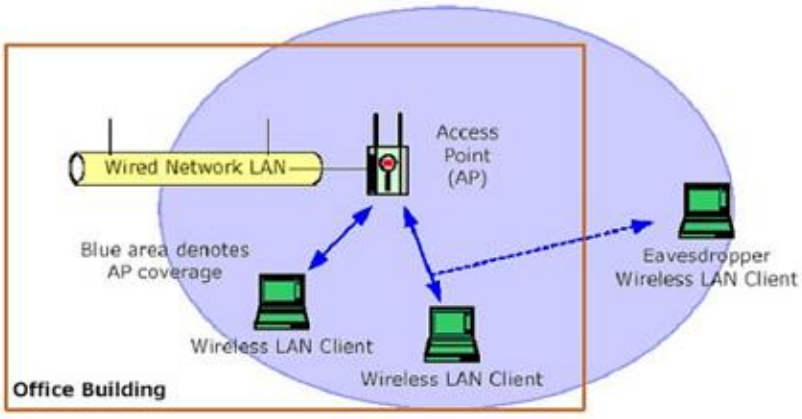
Đây là một trong những hình thức chứng thực động, khoá chứng thực được thay đổi giá trị một cách ngẫu nhiên ở mỗi lần chứng thực hoặc tại các khoảng có chu kỳ trong thời gian thực hiện một kết nối đã được chứng thực. Ngoài ra, EAP còn xác định chứng thực qua RADIUS có nghĩa là: Khi một CPE muốn kết nối vào mạng thì nó sẽ gửi yêu cầu tới AP. AP sẽ yêu cầu CPE gửi cho nó một tín hiệu Identify. Sau khi nhận được tín hiệu Identify của CPE, AP sẽ gửi tín hiệu Identify này tới server RADIUS để tiến hành chứng thực. Sau đó, RADIUS sẽ trả lời kết quả cho AP để AP quyết định có cho phép CPE đăng nhập hay không.

CHƯƠNG 3: BẢO MẬT MẠNG LAN KHÔNG DÂY

Bảo mật là vấn đề hết sức quan trọng đối với người dùng trong cả hệ thống (WLAN, LAN…). Để kết nối tới một mạng LAN hữu tuyến cần phải truy cập theo đường truyền dây cáp, phải kết nối một PC vào một cổng mạng. với mạng không dây chỉ cần có thiết bị trong vùng phủ sóng là có thể truy cập được nên vấn đề bảo mật mạng không dây là cực kỳ quan trọng và làm đau đầu người sử dụng mạng.

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

Hình sau thể hiện một người lạ có thể truy cập đến một LAN không dây từ bên ngoài như thế nào:



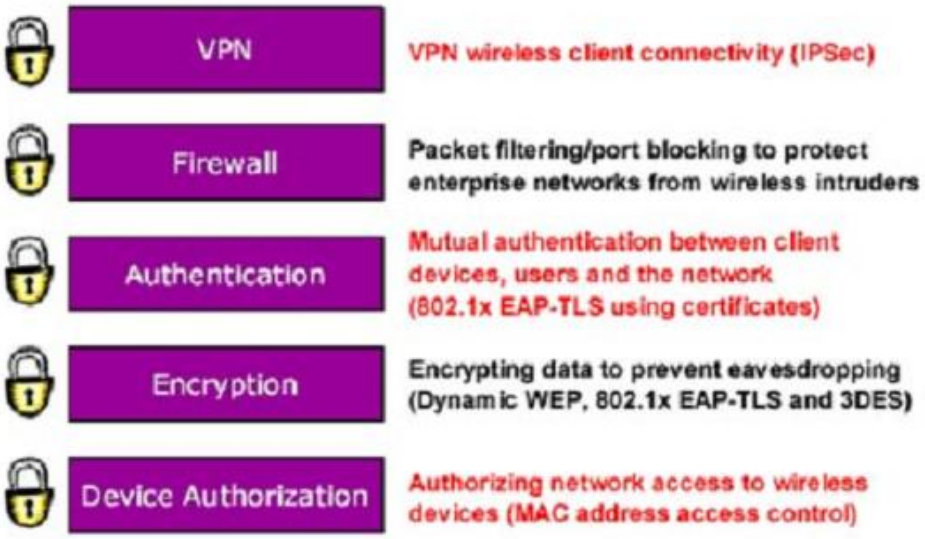
Hình 3.1: Một người lạ truy cập vào mạng

Chìa khóa để mở ra sự an toàn của WLAN và giữ cho 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 ra sự an toàn cho WLAN. Trong phần này chúng ta sẽ bàn đến biện pháp bảo mật theo chuẩn 802.11 đã biết, WEP. Tuy nhiên 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 mà chúng ta cần xem xét tại sao có sự hạn chế trong bảo mật WEP, phạm vi ứng dụng của WEP, và các biện pháp khắc phục..

Trong phần này chúng ta cũng đề cập đến một vài biện pháp tấn công, từ đó mà người quản trị đưa được ra các biện pháp phòng ngừa. Sau đó chúng ta cũng bàn về các biện pháp bảo mật sẵn có, nhưng chưa được thừa nhận chính thức bởi bất cứ chuẩn 802. nào. Cuối cùng chúng ta cũng đưa ra và khuyến nghị về các chính sách bảo mật cho WLAN.

3.1. Cách thiết lập bảo mật LAN không dây



Hình 3.2: Cách thiết lập bảo mật LAN không dây

1.*Device Authorization*: Các Client không dây *có thể bị ngăn chặn theo địa chỉ phần cứng của họ* (ví dụ như địa chỉ MAC). EAS duy trì một cơ sở dữ liệu của các Client không dây được cho phép và các AP riêng biệt khóa hay lưu thông lưu lượng phù hợp.

2.*Encryption*: WLAN cũng hỗ trợ *WEP, 3DES và chuẩn TLS(Transport Layer Sercurity)* sử dụng mã hóa để tránh người truy cập trộm. Các khóa WEP có thể tạo trên một **per-user, per session basic**.

3.Authentication: WLAN hỗ trợ sự ủy quyền lẫn nhau (bằng việc ***sử dụng 802.1x EAP-TLS***) để bảo đảm chỉ có các Client không dây được ủy quyền mới được truy cập vào mạng. EAS sử dụng một RADIUS server bên trong cho sự ủy quyền bằng việc sử dụng các chứng chỉ số. Các chứng chỉ số này có thể đạt được từ quyền chứng nhận bên trong (CA) hay được nhập từ một CA bên ngoài. *Điều này đã tăng tối đa sự bảo mật và giảm tối thiểu các thủ tục hành chính.*

4.*Firewall*: EAS hợp nhất *packet filtering* và *port blocking firewall* dựa trên các chuỗi IP. Việc cấu hình từ trước cho phép các loại lưu lượng chung được **enable hay disable.**

5.*VPN*: EAS bao gồm một *IPSec VPN server* cho phép các Client không dây thiết lập các session VPN vững chắc trên mạng.

3.2. Những tấn công trên mạng

Một sự tấn công cố ý có thể gây vô hiệu hoá hoặc có thể tìm cách truy nhập vào mạng.

Có thể tấn công vào WLAN trái phép theo một vài cách thức sau:

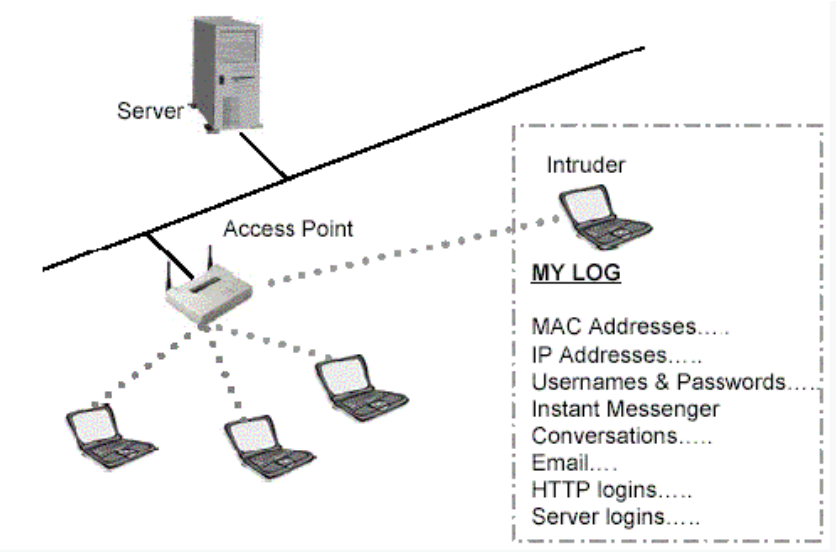
- **Tấn công bị động (**Nghe trộm**)** Passive attacks
- **Tấn công chủ động (**kết nối, dò và cấu hình mạng**)** Active attacks
- **Tấn công kiểu chèn ép,** Jamming attacks
- **Tấn công theo kiểu thu hút,** Man-in-the-middle attacks

Trên đây chỉ liệt kể một vài kiểu tấn công, trong đó một vài kiểu có thể thực hiện được theo nhiều cách khác nhau.

3.2.1. Tấn công bị động

Nghe trộm có lẽ là một 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. Những thiết bị phân tích mạng hoặc những ứng dụng khác được sử dụng để lấy thông tin của WLAN từ một khoảng cách với một anten định hướng.



Hình 3.3: 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.

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

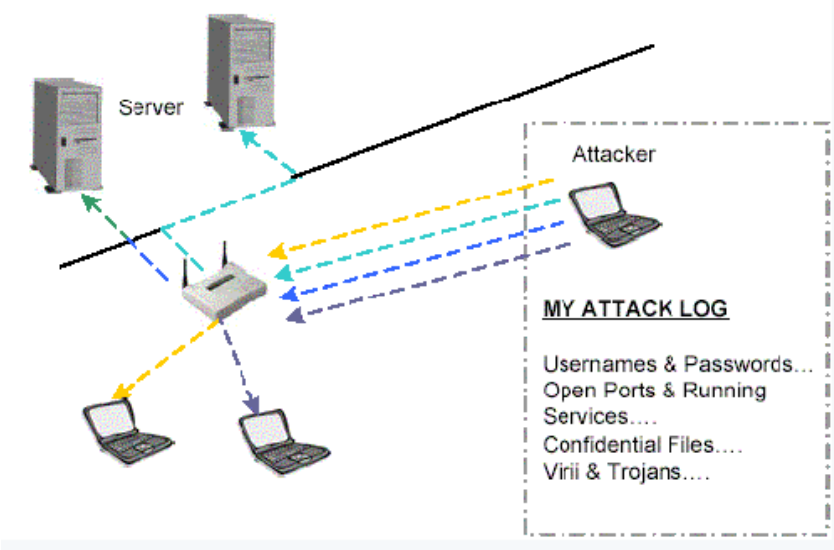
Hãy xem xét tác động nếu một hacker tìm được cách truy nhập tới một domain của người sử dụng, hacker đó sẽ đăng nhập vào domain của người sử dụng và gây hậu quả nghiêm trọng trên mạng. Tất nhiên việc đó là do hacker thực hiện, những người dùng là người phải trực tiếp chịu trách nhiệm, và gánh chịu mọi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

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

3.2.2. Tấn công chủ động

Những hacker có thể sử dụng phương pháp tấn công chủ động để thực hiện một vài chức năng trên mạng. Một sự tấn công chủ động có thể được dùng để truy nhập tới một server để lấy những dữ liệu quan trọng, sử dụng sự truy nhập tới mạng internet của tổ chức cho những mục có hại, thậm chí thay đổi cấu hình cơ sở hạ tầng mạng. Bằng cách kết nối tới một mạng WLAN thông qua một AP, một người sử dụng có thể bắt đầu thâm nhập sâu hơn và trong mạng và thậm chí làm thay đổi chính mạng không dây đó.

Chẳng hạn một hacker qua được bộ lọc MAC, sau đó hacker có thể tìm cách tới AP và gỡ bỏ tất cả các bộ lọc MAC, làm cho nó dễ dàng hơn trong lần truy nhập tiếp theo. Người quản trị có thể không đồng ý đến sự kiện này trong một thời gian. Hình dưới đây mô tả một kiểu tấn công chủ động trên WLAN.



Hình 3.4: Tấn công chủ động

Một vài ví dụ của tấn công chủ động có thể như việc gửi bomb mail, các spam do các spammer hoặc các doanh nghiệp đối thủ muốn truy nhập đến hồ sơ của bạn. Sau khi thu được một địa chỉ IP từ DHCP server của bạn, hacker có thể

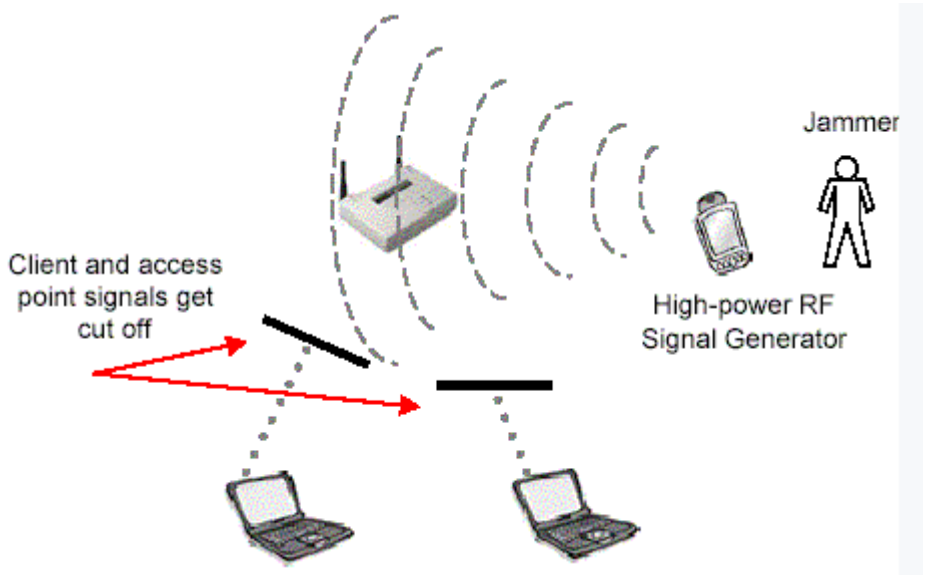
gửi hàng ngàn lá thư sử dụng kết nối Internet và ISP's email server của bạn mà bạn không biết. Kiểu tấn công này có thể là nguyên nhân mà ISP của bạn cắt kết nối cho email của bạn do sự lạm dụng email, mặc dù lỗi đó không phải do bạn gây ra. Một đối thủ có thể lấy bảng danh sách khách hàng, bảng lương của bạn mà không bị phát hiện.

Khi hacker đã kết nối không dây tới mạng của bạn thì anh ta cũng có thể truy nhập vào mạng hữu tuyến trong văn phòng, vì hai sự kiện không khác nhau nhiều. Nhưng kết nối không dây cho phép hacker về tốc độ, sự truy nhập tới server, kết nối tới mạng diện rộng, kết nối internet, tới desktop và laptop của những người sử dụng. Với một vài công cụ đơn giản, có thể lấy các thông tin quan trọng, chiếm quyền của người sử dụng, hoặc thậm chí phá huỷ mạng bằng cách cấu hình lại mạng.

Sử dụng các server tìm kiếm với việc quét các cổng, tạo những phiên rỗng để chia sẻ và có những server phục vụ việc cố định password, để hacker không thể thay đổi được pass, để nâng cao các tiện ích và ngăn chặn kiểu tấn công này.

3.2.3. Tấn công theo kiểu chèn ép

Trong khi một hacker sử dụng phương pháp tấn công bị động, chủ động để lấy thông tin từ việc truy cập tới mạng của bạn, tấn công theo kiểu chèn ép, Jamming, 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 được nhằm vào Web server, vì vậy một WLAN có thể ngừng làm việc bởi một tín hiệu RF áp đảo. Tín 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 chúng sẽ dùng một máy phát tín hiệu RF công suất cao hoặc máy tạo sóng quét.



Hình 3.5: 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. Có nhiều máy phân tích phổ trên thị trường, nhưng một máy phân tích phổ cầm tay và chạy bằng pin thì tiện lợi hơn cả.

Một vài nhà sản xuất chế tạo những bộ phân tích phổ cầm tay, trong khi một vài nhà sản xuất khác đã tạo ra các phần mềm phân tích phổ cho người dùng tích hợp ngay trong các thiết bị WLAN.

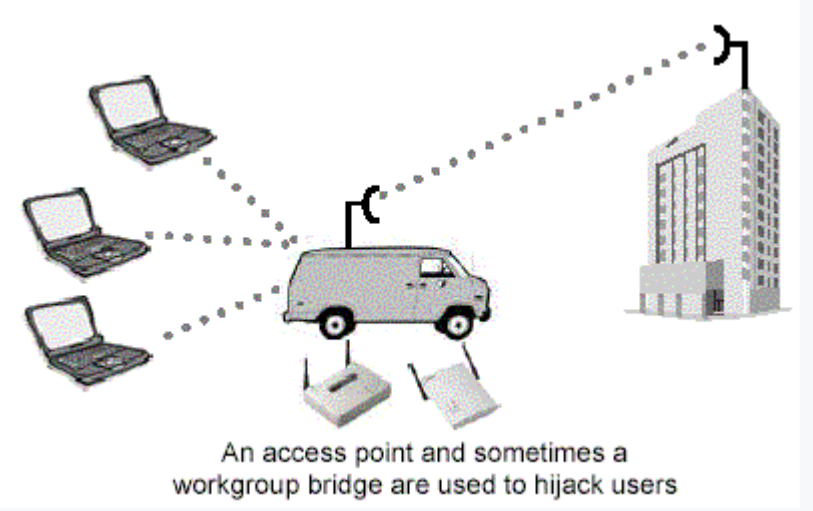
Khi jamming gây ra bởi một nguồn cố định, không chủ ý, như một tháp truyền thông hoặc các hệ thống hợp pháp khác, thì người quản trị WLAN có thể phải xem xét đến việc sử dụng bộ thiết đặt các tấn số khác nhau.

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 một nguồn giao thoa là một điện thoại, hoặc các thiết bị làm việc ở dải tần 2,4Ghz thì admin có thể sử dụng thiết bị ở dải tần UNII, 5Ghz, thay vì dải tần 802.11b, 2,4Ghz và chia sẻ dải tần ISM 2,4Ghz với các thiết bị khác.

Jamming không chủ ý gây ra với mọi thiết bị có dùng chung dải tần 2,4Ghz. 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 hoá được mạng.

3.2.4. Tấn công bằng cách thu hút

Kiểu tấn công này, Man-in-the-moddle Attacks, là một tình trạng mà trong đó một cá nhân sử dụng một AP để chiếm đoạt quyền 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 này, có thể là các thông tin nhạy cảm. Hình vẽ sau đưa ra một mô hình cho sự tấn công kiểu nay.



Hình 3.6: Man-in-the-middle attacks

Để các client liên kết với AP trái phép thì cồng suất của AP đó 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 qua trình vào mạng, và một vài client sẽ kết nối tới AP trái phép một cách ngẫu nhiên.

Người thực hiện man-in-the-middle attack trước tiên phải biết SSID mà client sử dụng, và phải biết WEP key đang sử dụng của mạng.

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 man-in-the-middle attack được sắp đặt sử dụng một laptop với hai PCMCIA card. Phần mềm AP chạy trên một laptop, 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 làm laptop thành một "man-in-the-middle attack" vận hành giữa client và AP hợp pháp. Một hacker theo kiểu man-in-the-middle attack có thể lấy được các thông tin có giá trị bằng cách chạy một chương trình phân tích mạnh trên laptop.

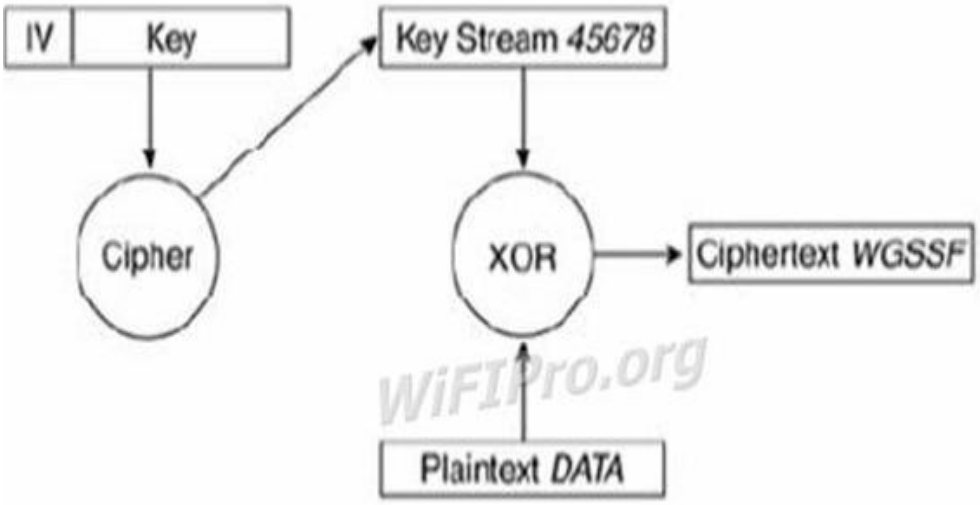
Một điều đặc biệt với kiểu tấn công này là người sử dụng không thể phát hiện ra được cuộc tấn công, và lượng thông tin thu nhặt được bằng kiểu tấn công này là giới hạn, nó bằng lượng thông tin thủ phạm lấy được trong khi còn trên mạng mà không bị phát hiện. Biện pháp tốt nhất để ngăn ngừa loại tấn công này là bảo mật lớp vật lý.

3.3. Các phương pháp bảo mật cho WLAN

3.3.1 WEP, WIRED EQUIVALENT PRIVACY

Mổ hình vector khởi tạo (IV)

Vector khởi tạo IV là một số được thêm vào khóa và làm thay đổi khóa . IV được nối vào khóa trước khi chuỗi khóa được sinh ra, khi IV thay đổi thì chuỗi khóa cũng sẽ thay đổi theo và kết quả là ta sẽ có ciphertext khác nhau. Ta nên thay đổi giá trị IV theo từng frame. Theo cách này nếu một frame được truyền 2 lần thì chúng ta sẽ có 2 ciphertext hoàn toàn khác nhau cho từng frame.

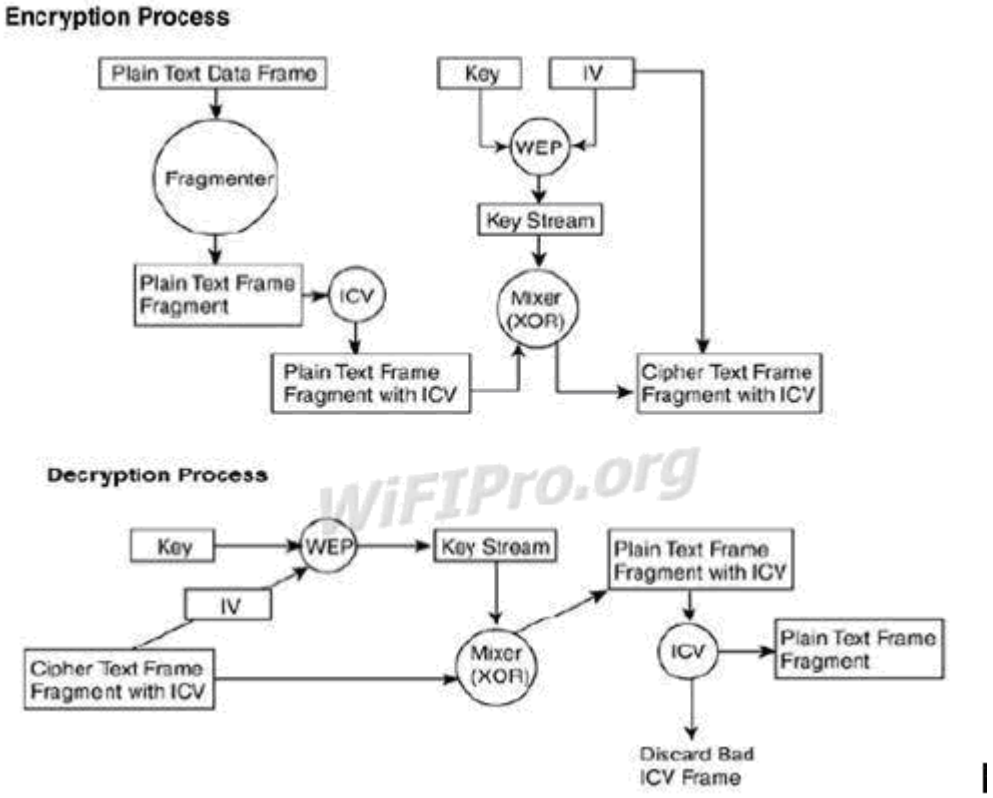


Hình 3.7 :Mô hình Vector khởi tạo IV

WEP (**Wired Equivalent Privacy)** là một thuật toán mã hóa sử dụng quá trình chứng thực khóa chia sẻ cho việc chứng thực người dùng và để mã hóa phần dữ liệu truyền trên những phân đoạn mạng LAN không dây. Chuẩn IEEE 802.11 đặc biệt sử dụng WEP.

WEP là một thuật toán đơn giản, sử dụng bộ phát một chuỗi giả ngẫu nhiên, Pseudo Random Number Generator (PRNG) và dòng mã RC4.

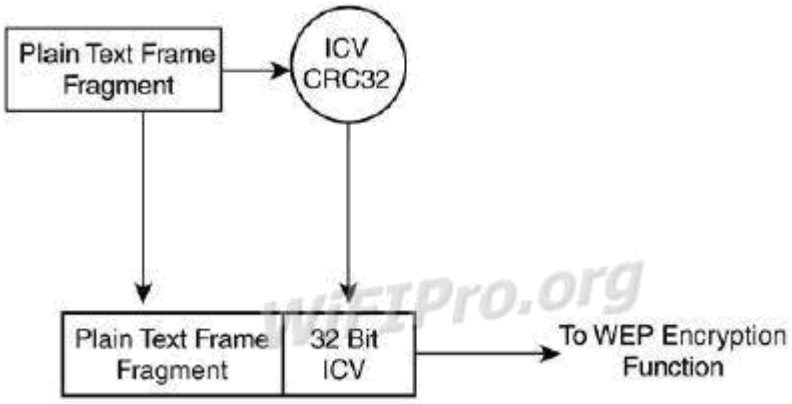
Trong vài năm, thuật toán này được bảo mật và không sẵn có, tháng 9 năm 1994, một vài người đã đưa mã nguồn của nó lên mạng. Mặc dù bây giờ mã nguồn sẵn có, nhưng RC4 vẫn được đăng ký bởi RSADSI. Chuỗi mã RC4 thì mã hóa và giải mã rất nhanh, nó rất dễ thực hiện, và đủ đơn giản để các nhà phát triển phần mềm có thể dùng nó để mã hóa các phần mềm của mình



Hình 3.8: Sơ đồ quá trình mã hóa và giải mã sử dụng WEP

ICV giá trị kiểm tra tính toàn vẹn

Ngoài việc mã hóa dữ liệu 802.11 cung cấp một giá trị 32 bit ICV có chức năng kiểm tra tính toàn vẹn của frame. Việc kiểm tra này cho trạm thu biết rằng frame đã được truyền mà không có lỗi nào xảy ra trong suốt quá trình truyền. ICV được tính dựa vào phương pháp **kiểm tra lỗi bits CRC-32(Cyclic Redundancy Check 32)**. Trạm phát sẽ tính toán giá trị và đặt kết quả vào trong trường ICV, ICV sẽ được mã hóa cùng với frame dữ liệu. Trạm thu sau khi nhận frame sẽ thực hiện giải mã frame, tính toán lại giá trị ICV và so sánh với giá trị ICV đã được trạm phát tính toán trong frame nhận được. Nếu 2 giá trị trùng nhau thì frame xem như chưa bị thay đổi hay giả mạo, nếu giá trị không khớp nhau thì frame đó sẽ bị hủy bỏ.



Hình 3.9: Mô hình hoạt động của ICV

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 bit và 128 bit đều có cùng vector khởi tạo, Initialization Vector (IV), là 24 bit. Vector 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 mà vector này cần được khởi động lại ít nhất mỗi lần một ngày, tức là các bit lại trở về 0. Khi WEP được sử dụng, vector khởi tạo (IV) được truyền mà không được mã hóa cùng với một gói được mã hóa. Việc phải khởi động lại và truyền không được mã hóa đó 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 chèn các gói tin vào mạng mà có thể hiểu được, mà không cần giải mã.

- *Tấn công chủ động để giải mã thông tin*: Dựa vào sự đánh lừu điểm truy nhập.

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

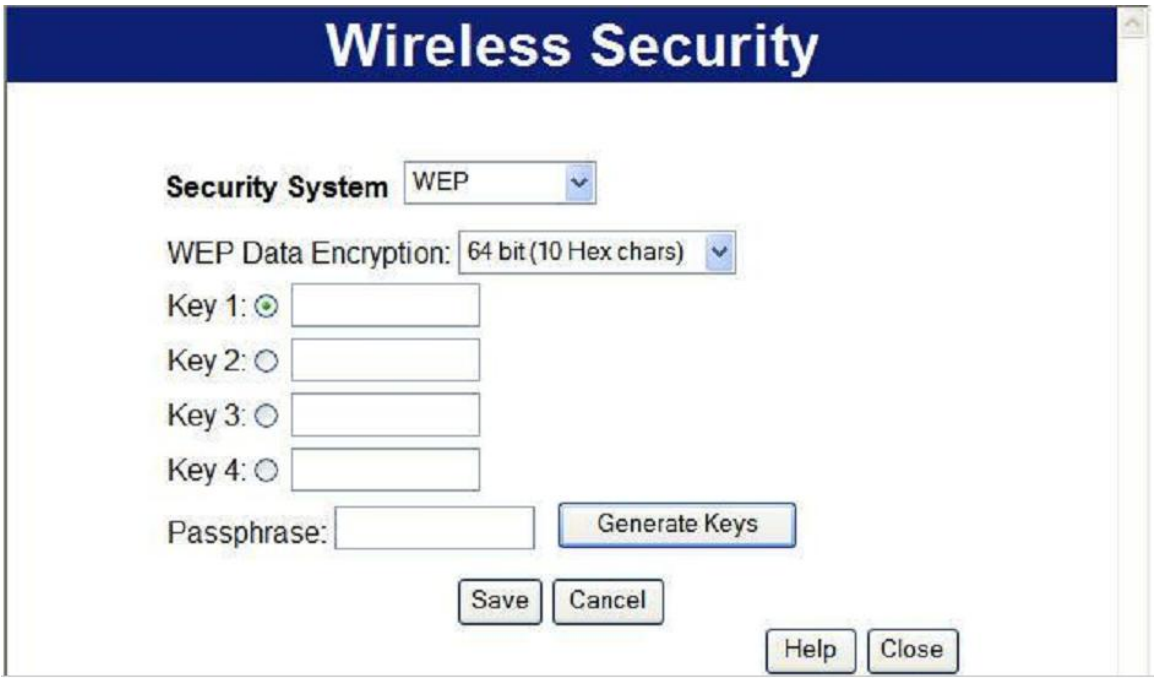
- *Tấn công bị động để giải mã thông tin*: Sử dụng các phân tích thống kê để giải mã dữ liệu của WEP.

3.3.1.1. Tại sao Wep được lựa chọn

WEP không được an toàn, vậy tại sao WEP lại được chọn và đưa vào chuẩn 802.11? Chuẩn 802.11 đưa ra các tiêu chuẩn cho một vấn đề được gọi là bảo mật, đó là:

- Có thể xuất khẩu
- Đủ mạnh
- Khả năng tương thích
- Khả năng ước tính được
- Tùy 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 cho mục đích 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 khóa WEP 40 bit, một vài hãng sản xuất lựa chọn cách tăng cường cho WEP, một vài hãng khác lại sử dụng một chuẩn mới như là 802.11X với EAP hoặc VPN



Hình 3.10: WEP Wireless Security

3.3.1.2. Chìa khóa WEP

Vấn đề cốt lõi của WEP là chìa khóa WEP (WEP key). WEP key là một chuỗi ký tự chữ cái và số, được sử dụng cho 2 mục đích của WLAN

- Chìa khóa WEP được sử dụng để xác định sự cho phép của một Station
- Chìa khóa WEP dùng để mã hóa dữ liệu.

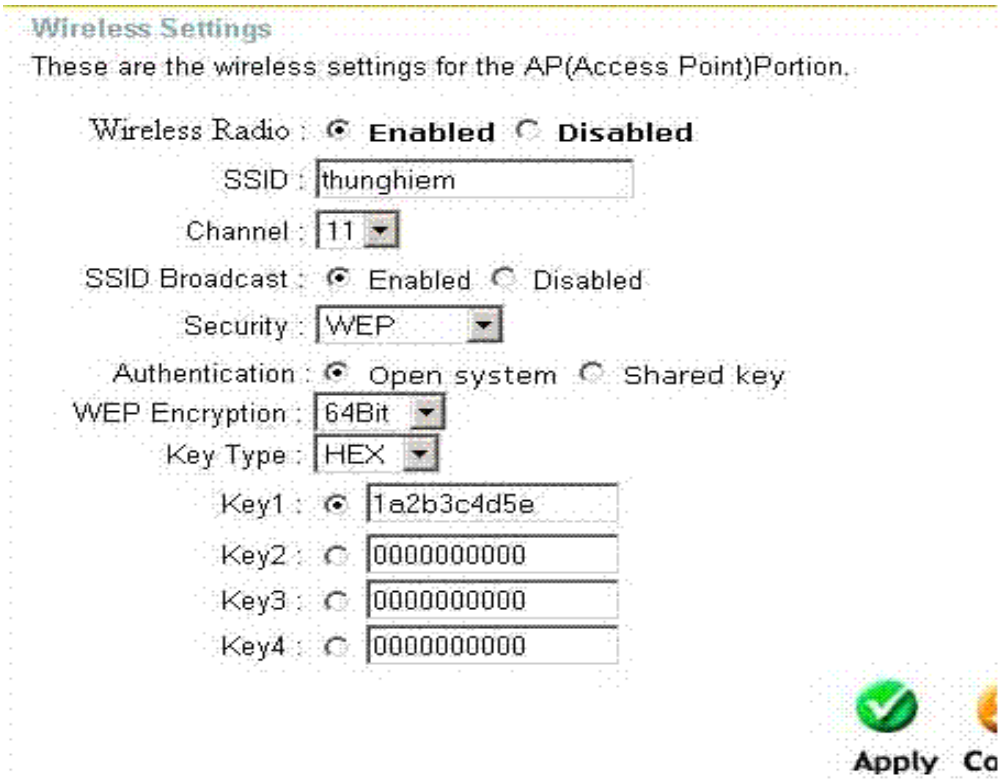
Khi một client mà sử dụng WEP cố gắng thực hiện một sự xác thực và liên kết tới một AP (Access Point). AP sẽ xác thực xem Client có chìa khóa có xác thực hay không, nếu có, có nghĩa là Client phải có một từ khóa là một phần của chìa khóa WEP, chìa khóa WEP này phải được so khớp trên cả kết nối cuối cùng của WLAN.

Một nhà quản trị mạng WLAN (Admin), có thể phân phối WEP key bằng tay hoặc một phương pháp tiên tiến khác. *Hệ thống phân phối WEP key có thể đơn giản như sự thực hiện khóa tĩnh, hoặc tiên tiến sử dụng Server quản lí chìa khóa*

mã hóa tập trung. Hệ thống WEP càng tiên tiến, càng ngăn chặn được khả năng bị phá hoại, hacker.

WEP key tồn tại hai loại, 64 bit và 128 bit, mà đôi khi bạn thấy viết là 40 bit và 104 bit. Lý do này là do cả hai loại WEP key đều sử dụng chung một vector khởi tạo, Initialization Vector (IV) 24 bit và một từ khóa bí mật 40 bit hoặc 104 bit. Việc nhập WEP key vào client hoặc các thiết bị phụ thuộc như là bridge hoặc AP thì rất đơn giản.

Hầu hết các Client và AP có thể đưa ra đồng thời 4 WEP key, nhằm hỗ trợ cho việc phân đoạn mạng. Ví dụ, nếu hỗ trợ cho một mạng có 100 trạm khách: đưa ra 4 WEP key thay vì một thì có thể phân số người dùng ra làm 4 nhóm riêng biệt, mỗi nhóm 25 người, nếu một WEP key bị mất, thì chỉ phải thay đổi 25 Station và một đến 2 AP thay vì toàn bộ mạng.



Hình 3.11: Giao diện setup của AP thử nghiệm

Một lí do nữa cho việc dùng nhiều WEP key, nếu là một Card tích hợp cả khóa 64 bit và khóa 128 bit, thì nó có thể dùng phương án tối ưu nhất, đồng thời nếu hỗ trợ 128 bit thì cũng có thể làm việc được với chìa khóa 64 bit.

Theo chuẩn 802.11, thì chìa khóa WEP được sử dụng là **chìa khóa Wep tĩnh.** Nếu chọn Wep key tĩnh bạn phải tự gán một Wep key tĩnh cho một AP hoặc Client liên kết với nó, Wep key 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. Nếu chỉ sử dụng WEP tĩnh thì rất dễ dẫn đến sự mất an toàn.

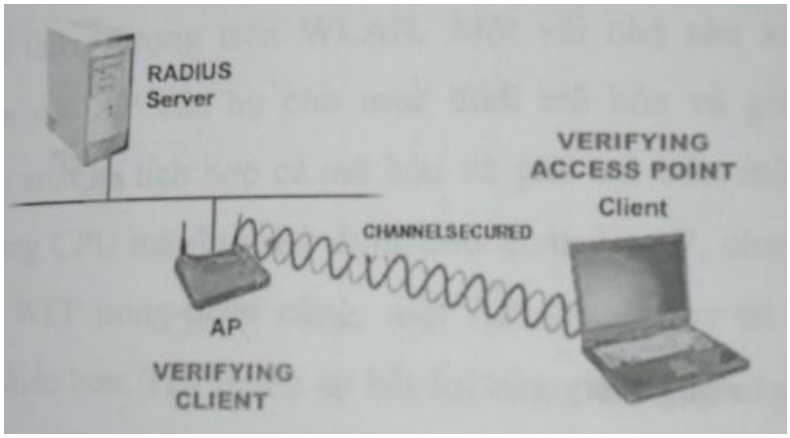
Xét trường hợp nếu một người nào đó "làm mất" Card mạng WLAN của họ, card mạng đó chứa chương trình cơ sở mà có thể truy nhập vào WLAN đó cho tới khi khóa tĩnh của WLAN được thay đổi.

3.3.1.3. SERVER quản lý chìa khóa mã hóa tập trung

Vỡi những mạng WLAN quy mô lớn sử dụng WEP như một phương pháp bảo mật căn bản, server quản lý chìa khóa mã hóa tập trung nên được sử dụng vì những lý do sau:

- Quản lí sinh chìa khóa tập trung
- Quản lý việc phân phối chìa khóa một cách tập trung
- Thay đổi chìa khóa luôn phiên
- Giảm bớt công việc cho nhà quản lý

Bất kỳ số lượng thiết bị khác nhau nào cũng có thể đóng vai trò một server quản lý chìa khóa mã hóa tập trung. Bình thường khi sử dụng WEP, những chìa khóa (được tạo bởi người quản trị) thường được nhập bằng tay vào trong các trạm và các AP. Khi sử dụng server quản lý chìa khóa mã hóa tập trung, một quá trình tự động giữa các trạm, AP và server quản lý sẽ thực hiện việc trao các chìa khóa WEP. Hình sau mô tả cách thiết lập một hệ thống như vậy.



Hình 3.12: Cấu hình chìa khóa mã hóa tập trung

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

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

3.2.1.4 Cách sử dụng WEP

Khi WEP được khởi tạo, dữ liệu phần tải của mỗi gói được gửi, sử dụng WEP, đã được mã hóa. Tuy nhiên, phần header của mỗi gói, bao gồm địa chỉ MAC, không được mã hóa, tất cả thông tin lớp 3 bao gồm địa chỉ nguồn và địa chỉ đích được mã hóa bởi WEP.

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

Khi các gói được gửi đi mà sử dụng mã hóa WEP, những gói này phải được giải mã. Quá trình giải mã này 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 hóa và giải mã WEP. Nhiều nhà sản xuất lại tích hợp cả mã hóa và giải mã trên một phần mềm và sử dụng cùng CPU mà được dử dụng cùng

cho quản lý AP, chuyển tiếp gói. Nhờ tích hợp WEP trong phần cứng, một AP có thể duy trì thông lượng 5Mbps hoặc nhiều hơn. Tuy nhiên sự bất lợi của giả pháp này là gía 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 nên nắm bắt được những điểm yếu của WEP và cách khắc phục chúng. Các admin cũng nên hiểu răng, mỗi nhà cung cấp sử dụng WEP có thể khác nhau, vì vậy gây ra trở ngại trong việc sử dụng phần cứng của nhiều nhà cung cấp.

Để khắc phục những khiếm khuyết của WEP, chuẩn mã hóa tiên tiến Advanced Encryption Standard (AES) đang được công nhận như một sự thay thế thích hợp cho thuật toán RC4. AES sử dụng thuật toán Rijndael (RINE- dael) với những loại chìa khóa sau:

- 128 bit
- 192 bit
- 256 bit

AES được xét là một phương pháp không thể bẻ khóa 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, 802.11x được xem xét để sử dụng AES trong WEP v.2.

AES nếu được đồng ý bởi 802.11i, sử dụng trong WEP v2, sẽ được thực hiện trong phần vi chương trình và các phần mềm bởi các nhà cung cấp. Chương trinh cơ sở trong AP và trong Client (Card vô tuyến PCMCIA) sẽ phải được năng 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 chìa khóa bí mật.

3.3.2. WPA (Wifi Protected Access)

Wi-Fi Alliance đã đưa ra giải pháp gọi là Wi-fi Protected Access (WPA). *Một trong những cải tiến quan trọng nhất của WPA là sử dụng hàm thay đổi khóa TKIP* (Temporal Key Integrity Protocol). WPA cũng sử dụng thuật toán RC4 như

WEP, nhưng mã hóa đầy đủ 128 bit. Và một đặc điểm khác là WPA thay đổi khóa cho mỗi gói tin. Các công cụ thu thập các gói tin để phá khóa mã hóa đều không thể thực hiện được với WPA. Bởi WPA thay đổi khóa liên tục nên hacker không bao giờ thu thập đủ dữ liệu mẫu để tìm ra mật khẩu. Không những thế, *WPA còn bao gồm kiểm tra tính toàn vẹn của thông tin* (Message Integrity Check). Vì vậy, dữ liệu không thể bị thay đổi trong khi đang ở trên đường truyền.

Một trong những điểm hấp dẫn nhất của WPA là không yêu cầu nâng cấp phần cứng. Các nâng cấp miễn phí về phần mềm cho hầu hết các card mạng và điểm truy cập sử dụng WPA rất dễ dàng và có sẵn. Tuy nhiên, WPA cũng không hỗ trợ các thiết bị cầm tay và máy quét mã vạch. Theo Wi-Fi Alliance, có khoảng 200 thiết bị đã được cấp chứng nhận tương thích WPA.

WPA có sẵn 2 lựa chọn: WPA Personal và WPA Enterprise. Cả 2 lựa chọn này đều sử dụng giao thức TKIP, và sự khác biệt chỉ là khóa khởi tạo mã hóa lúc đầu. WPA Personal thích hợp cho gia đình và mạng văn phòng nhỏ, khóa khởi tạo sẽ được sử dụng tại các *điểm truy cập và thiết bị máy trạm*. Trong khi đó, WPA cho doanh nghiệp cần một máy chủ xác thực và 802.1x để cung cấp các khóa khởi tạo cho mỗi phiên làm việc. Trong khi Wi-fi Alliance đã đưa ra WPA, và được coi là loại trừ mọi lỗ hổng dễ bị tấn công của WEP, nhưng người sử dụng vẫn không thực sự tin tưởng vào WPA.

Có một lỗ hổng trong WPA và lỗi này chỉ xảy ra với WPA Personal. Khi mà sử dụng hàm thay đổi khóa TKIP được sử dụng để tạo ra các khóa mã hóa bị phát hiện, nếu hacker có thể dự đoán được khóa khởi tạo hoặc một phần mật khẩu, họ có thể xác định được toàn bộ mật khẩu, do đó có thể giải mã được dữ liệu. Tuy nhiên, lỗ hổng này cũng sẽ bị loại bỏ bằng cách sử dụng những khóa khởi tạo không dễ đoán (đừng sử dụng những từ như "PASSWORD" để làm mật khẩu mà thay từ "password" bởi từ passphrase hoặc sử dụng kỹ thuật hàm băm (hash function) để bảo mật mật khẩu (passwork)).

Điều này cũng có nghĩa rằng kỹ thuật TKIP của WPA chỉ là giải pháp tạm thời, chưa cung cấp một phương thức bảo mật cao nhất. WPA chỉ thích hợp với những công ty mà không truyền dữ liệu "mật" về những thương mại, hay các thông

tin nhạy cảm… WPA cũng thích hợp với những hoạt động hàng ngày và mang tính thử nghiệm công nghệ.

3.3.3. 802.11i (WPA2)

Một giải pháp về lâu dài là sử dụng 802.11 tương đương với WPA2, được chứng nhận bởi Wi-Fi Alliance. Chuẩn này sử dụng thuật toán mã hóa mạnh mẽ và được gọi là Chuẩn mã hóa nâng cao AES (Advanced Encryption Standard). AES sử dụng thuật toán mã hóa đối xứng theo khối Rijndael, sử dụng khối mã hóa 128 bit, 192 bit và 256 bit.

Để đánh giá chuẩn mã hóa này, Viện nghiên cứu quốc gia về Chuẩn và Công nghệ Mỹ, NIST (National Institute of Standards and Technology), đã thông qua thuật toán đối xứng này. Và chuẩn mã hóa này được sử dụng cho các cơ quan chính phủ Mỹ để bảo vệ các thông tin nhạy cảm.

Trong khi AES được xem như là bảo mật tốt hơn rất nhiều so với WEP 128 bit hoặc 168 bit DES (Digital Encryption Standard). Để đảm bảo về mặt hiệu năng, quá trình mã hóa cần được thực hiện trong các thiết bị phần cứng như tích hợp vào chip. Tuy nhiên, rất ít người sử dụng mạng không dây quan tâm tới vấn đề này. Hơn nữa, hầu hết các thiết bị cầm tay Wi-Fi và máy quét mã vạch đều không tương thích với chuẩn 802.11i.

3.4. LỌC

Lọc (Filtering) là một cơ chế bảo mật căn bản có thể dùng bổ sung cho WEP và/ hoặc AES. Lọc theo nghĩa đen là chặn những gì không mong muốn và cho phép những gì được mong muốn. Filter làm việc giống như là 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 thì việc đó xác định xem các máy trạm là ai và phải cấu hình như thế nào. Có ba loại căn bản của Filtering có thể thực hiện trong WLAN

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

3.4.1. Lọc SSID

Lọc SSID (SSID Filtering) là một phương pháp lọc sơ đẳng, và chỉ được dùng cho hầu hết các điều khiển truy nhập. SSID (Service Set Identifier) chỉ 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 đặc biệt, Ad-hoc mode) để chứng thực và liên kết Client để thiết lập dịch vụ.

Vì lí do SSID được phát quảng bá trong những bản tin dẫn đường mà AP hoặc các Station gửi đi, nên dễ dàng tìm được 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 dẫn đường (beacon frame). Trong trường hợp này client phải so khớp 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 của 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 trong việc thiết lập cấu hình driver.

Một vài lỗi chung do người sử dụng WLAN tạo ra khi thực hiện SSID là: mạng để lấy địa chỉ MAC khởi nguồn từ AP, và sau đó xem MAC trong

- *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 để sử dụng một bộ phân tích bảng OUI của IEEE, bảng này liệt kê các tiền tố địa chỉ MAC khác nhau được gán cho các nhà sản xuất. Cách tốt nhất để khắc phục lỗi này là: *Luôn luôn thay đổi SSID mặc định.*

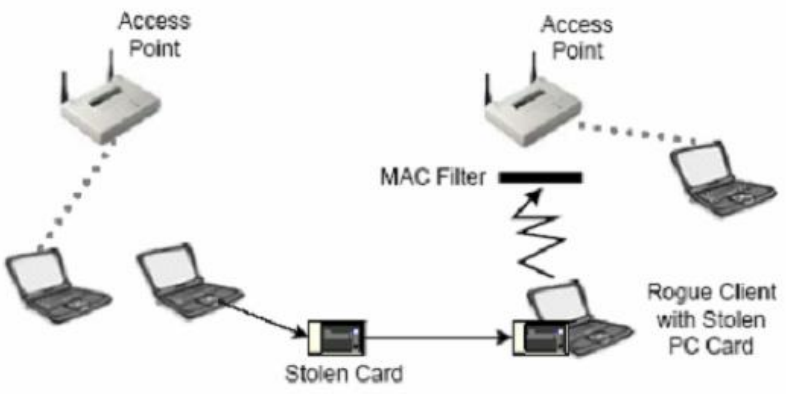
- *Làm cho SSID có gì đó liên quan đến công ty:* Loại thiết lập này là một mạo hiểm về bảo mật vì nó làm đơn giản hóa quá trình một hacker tìm thấy vị trí vật lý của công ty. Khi tìm kiếm WLAN trong một vùng địa lý đặc biệt thì việc tìm thấy vị trí vật lý của công ty đã hoàn thành một nửa công việc. Khi một người quản trị sử dụng SSID mà đặt tên liên quan đến tên công ty hoặc tổ chức, việc tìm thấy WLAN sẽ là rất dễ dàng. Do đó hãy nhớ rằng: *luôn 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 dùng thay đổi trong việc thiết lập cấu hình để vào mạng. Nó được sử dụng như một phương tiện để phân đoạn mạng chứ không phải để bảo mật, vì thế hãy: *luôn coi SSID chỉ như một cái tên mạng.*

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

3.4.2. Lọc địa chỉ MAC

WLAN có thể lọc dựa vào địa chỉ MAC của các trạm khách. Hầu hết tất cả các AP, thậm chí cả những cái rẻ tiền, đều có chức năng lọc MAC. 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 mà không ở trong danh sách địa chỉ MAC của AP, nó sẽ không thể đến được điểm truy nhập.



Hình 3.13: Lọc địa chỉ MAC

Tất nhiên, lập trình các địa chỉ MAC của Client trong mạng WLAN và các AP trên một mạng rộng thì không thực tế. Bộ lọc MAC có thể được thực hiện trên vài RADIUS Server thay vì trên mỗi điểm truy nhập. Cách 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 là đơn giản, và có thể phải được nhập bằng bất cứ cách nào, là một giải pháp

tôt. RADIUS Server thường trỏ đến các nguồn chứng thực khác, vì vậy các nguồn chứng thực khác phải được hôc trợ bộ lọc MAC.

Bộ lọc MAC có thể làm việc tốt trong chế độ ngược lại. Xét một ví dụ, một người làm thêu bỏ việc mà mang theo cả Card Lan không dây của họ. Card WLan này nằm giữ cả chìa khóa WEP và bộ lọc MAC vì thế không thể để họ còn được quyền sử dụng. Khi dó người quản trị có thể loại bỏ địa chỉ MAC của máy khách đó ra khỏi danh sách cho phép.

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

- Sự ăn trộm một Card PC trong có một bộ lọc MAC của PC
- Việc thăm dò WLAN và sau đó giả mạo với một địa chỉ MAC để thâm nhập vào mạng.

Với những mạng gia đình hoặc những mạng trong văn phòng nhỏ, nơi mà ở đó có một số lượng nhỏ các trạm khách, thì 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 mạng có giá trị sử dụng thấp.

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

Một vài card PC không dây cho phép thay đổi địa chỉ MAC của họ thồng qua phần mềm hoặc thậm chí qua cách thay đổi cấu hình hệ thống. Một hacker khi biết được danh sách các địa chỉ MAC cho phép, 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 tồn tại trên một WLAN, hacker phải tìm một địa chỉ MAC của một trạm mà hiện thời không ở trên

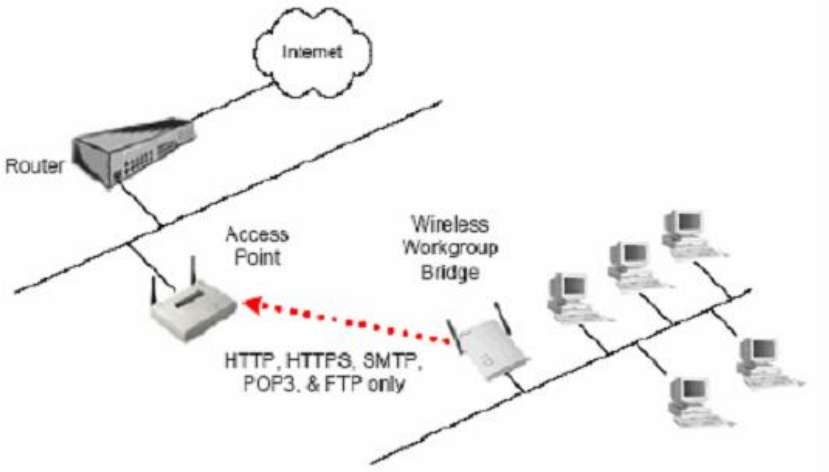
mạng. Chính trong thời gian trạm di động hoặc máy tính sách tay không có trên mạng là thời gian mà hacker có thể truy nhập vào mạng tốt nhất.

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

3.4.3. Lọc giao thức

Mạng Lan không dây 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 mạng hữu tuyến và vô tuyến của AP.

Tưởng tượng một hoàn cảnh, trong đó một nhóm cầu nối không dây được đặt trên một Remote building trong một mạng WLAN của một trường đại học có kết nối lại tới AP của toà nhà kỹ thuật trung tâm. Vì tất cả những người sử dụng trong remote building chia sẻ băng thông 5Mbs giao giữu 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 đặc biệt của sự truy nhập internet của người sử dụng, thi bộ lọc giao thức sẽ loại trừ tất cả các giao thức, ngoại trừ SMTP, POP3, HTTP, HTTPS, FTP…



Hình 3.14: Lọc giao thức

3.5. Các giải pháp bảo mật được khuyến nghị

Vì WLAN vốn không phải là đã an toàn, bên cạnh đó WEP cũng không phải là phương pháp bảo mật duy nhất và hoàn hảo cho WLAN, vì vậy cần đưa ra các phương pháp bảo mật bổ sung cho WLAN.

Những phương pháp bảo mật này được đưa ra, và tất nhiên còn chưa được công nhận bởi chuẩn 802.11, tuy nhiên có thể đóng vai trò quan trọng trong mạng LAN không dây của bạn. Như chuẩn 802.1x đã được chấp nhận bởi IEEE nhưng vẫn chưa được chính thức coi là một phần của họ 802.11. Chuẩn 802.11i thì vẫn còn nằm trên bản thảo.

3.5.1. Quản lý chìa khoá WEP

Thay vì sử dụng chìa khoá WEP tĩnh, mà vẫn dễ dàng bị các hacker phát hiện. WLAN có thể được bảo mật tốt hơn nhờ việc thực hiện các chìa khoá trên từng phiên hoặc từng gói, sử dụng một hệ thông chìa khoá phân phối tập trung.

Sự phân phối chìa khoá WEP cho mỗi phiên, mỗi gói sẽ gán một chìa khoá WEP mới cho cả Client và AP cho mỗi phiên hoặc mỗi gói được gửi giữa chúng. Mặc dù khoá động có thể làm tăng thêm tải cho hệ thống và giảm bớt lưu lượng, chúng làm cho hacker xâm nhập vào mạng thông qua những đoạn mạng không dây trở lên khó khăn hơn nhiều. Hacker có thể phải dự đoán chuỗi chìa khoá mà server phân phối chìa khoá đang dùng, điều này là rất khó.

Hãy nhớ là WEP chỉ bảo vệ thông tin lớp 3-7 và dữ liệu phần tải, nhưng không mã hoá địa chỉ MAC hoặc các thông tin dẫn đường. Một bộ phân tích mạng có thể bắt bất cứ thông tin nào được truyền quảng bá trong bản tin dẫn đường từ AP hoặc bất cứ thông tin địa chỉ MAC nào tròn những gói unicast từ client.

Để đặt một server quản lý chìa khoá mã hoá tập trung vào chỗ thích hợp, người quản trị WLAN phải tìm một ứng dụng để thực hiện nhiệm vụ này: mua một server với một hệ điều hành thích hợp, và cấu hình ứng dụng theo nhu cầu. Quá trình này có thể tốn kém và cần nhiều thời gian, phụ thuộc vào quy mô triển khai. Tuy nhiên chi phí sẽ nhanh chóng thu lại được nhờ việc ngăn ngừa những phí tổn thiệt hại do hacker gây ra.

3.5.2. Wireless VPN

Những nhà sản xuất WLAN ngày càng tăng các chương trình phục vụ mạng riêng ảo, VPN, trong các AP, Gateway, cho phép dùng kỹ thuật VPN để bảo mật cho kết nối WLAN. Khi VPN server được xây dựng vào AP, các client sử dụng phần mềm Off-the-shelf VPN, sử dụng các giao thức như PPTP hoặc IPsec để hình thành một đường hầm trực tiếp tới AP.

Trước tiên client liên kết tới điểm truy nhập, sau đó quay số kết nối VPN, được yêu cầu thực hiện để clientđi qua được AP. Tất cả lưu lượng được chuyển tải qua một đường hầm logic và có thể được mã hoá để thêm một lớp an toàn. Hình sau đây mô tả một cấu hình mạng như vậy:

Hình 3.15: Wireless VPN

Sự sử dụng PPTP với những bảo mật được chia sẻ rất đơn giản để thực hiện và cung cấp một mức an toàn hợp lí, đặc biệt khi được thêm mã hoá WEP. Sự sử dụng Idsec với những bí mật dùng chung hoặc được phép là giải pháp chung của sự lựa chọn giữa những kỹ năng bảo mật trong phạm vi hoạt động này. Khi một VPN server được cung cấp vào trong một gateway, quá trình xảy ra tương tự, chỉ có điều sau khi client liên kết với AP, đường hầm VPN được thiết lập với thiết bị gateway thay vì với bản thân AP.

Cũng có những nhà cung cấp đang đề nghị cải tiến những giải pháp VPN hiện thời của họ (phần cứng hoặc phần mềm) để hỗ trợ các client không dây và cạnh tranh trên thị trường WLAN. Những thiết bị hoặc những ứng dụng này phục vụ trong cùng khả năng như gateway, giữa những đoạn mạng vô tuyến và mạng lõi hữu tuyến. Những giải pháp VPN không dây khá đơn giản và kinh tế. Nếu một admin chưa có kinh nghiệm với các giải pháp VPN, thì nên tham dự một khoá đào tạo trước khi thực hiện nó. VPN mà hỗ trợ cho WLAN được thiết kế một cách khá đơn giản, có thể được triển khai bởi một người đang tập sự, chính điều đó lí giải tại sao các thiết bị này lại phổ biến như vậy đối với người dùng.

3.5.3. Kỹ thuật chìa khoá nhảy

Gần đây, kỹ thuật chìa khoá nhảy sử dụng mã hoá MD5 và những chìa khóa mã hoá thay đổi liên tục trở lên sẵn dùng trong môi trường WLAN. Mạng thay đổi liên tục,"hops", từ một chìa khoá này đến một chìa khoá khác thông thường 3 giây một lần. Giải pháp này yêu cầu phần cứng riêng cà chỉ là giải pháp tạm thời trong khi chờ sự chấp thuận chuẩn bảo mật tiên tiến 802.11i. Thuật toán chìa khoá này thực hiện như vậy để khắc phục những nhược điểm của WEP, như vấn đề về vector khởi tạo.

3.5.4. Temporal Key Integrity Protocol(TKIP)

TKIP thực chất là một sự cải tiến WEP mà vẫn giữ những vấn đề bảo mật đã biết trong WEP của chuỗi dòng số RC4. TKIP cung cấp cách làm rối vector khởi tạo để chống lại việc nghe lén các gói một cách thụ động. Nó cũng cung cấp việc kiểm tra tính toàn vẹn của thông báo để giúp xác định liệu có phải một người sử dụng không hợp pháp đã sửa đổi những gói tin bằng cách chèn vào lưu lượng để có thể crack chìa khoá. TKIP bao gồm việc sử dụng các chìa khoá động để chống lại sự ăn cắp các chìa khoá một cách bị động, một lỗ hổng lớn trong chuẩn WEP.

TKIP có thể thực hiện thông qua các vi chương trình được nâng cấp cho AP và bridge cũng như những chuẩn phầm mềm và vi chương trình nâng cấp cho thiết bị client không dây. TLIP chỉ rõ các quy tắc sử dụng vector khởi tạo, các thủ tục tạo lại chìa khoá dựa trên 802.1x, sự trộn chìa khoá trên mỗi gói và mã toàn vẹn

thông báo. Sẽ có sự giảm tính thực thi khi sử dụng TKIP, tuy nhiên bù lại là tính bảo mật được tăng cường đáng kể, nó tạo ra một sự cân bằng hợp lí.

3.5.5. Những giải pháp dựa trên AES

Những giải pháp dựa trên AES có thể thay thế WEP sử dụng RC4, nhưng chỉ tạm thời. Mặc dù không có sản phẩm nào sử dụng AES đang có trên thị trường, một vài nhà sản xuất đang thực hiện để đưa chúng ra thị trường. Bản dự thảo 802.11i chỉ rõ sự sử dụng của AES, và xem xét các người sử dụng trong việc sử dụng nó. AES có vẻ như là một bộ phận để hoàn thành chuẩn này.

Kỹ thuật mã hoá dữ liệu đang thay đổi tới một giải pháp đủ mạnh như AES sẽ tác động đáng kể trên bảo mật mạng WLAN, nhưng vẫn phải là giải pháp phổ biến sử dụng trên những mạng rộng như những server quản lý chìa khoá mã hoá tập trung để tự động hoá quá trình trao đổi chìa khoá. Nếu một card vô tuyến của client bị mất, mà đã được nhúng chìa khoá mã hoá AES, nó không quan trọng với việc AES mạnh đến mức nào bởi vì thủ phạm vẫn vó thể có được sự truy nhập tới mạng.

3.5.6. Wireless Gateways

Trên wireless gateway bây giờ sẵn sàng với công nghệ VPN, như là NT, DHCP, PPPoE, WEP, MAC filter và có lẽ thậm chí là một filewall xây dựng sẵn. Những thiết bị này đủ cho các văn phòng nhỏ với một vài trạm làm việc và dùng chúng kết nối tới Internet. Giá của những thiết bị này làm thay đổi phụ thuộc vào phạm vi những dịch vụ được đề nghị.

Những wireless gateway trên mạng quy mô lớn hơn là một sự thích nghi đặc biệt của VPN và server chứng thực cho WLAN. Gateway này nằm trên đoạn mạng hữu tuyến giữa AP và mạng hữu tuyến. Như tên của nó, gateway điều khiển sự truy nhập từ WLAN lên đoạn mạng hữu tuyến. Vì thế trong khi một hacker có thể lắng nghe hoặc truy cập được tới đoạn mạng không dây, gateway bảo vệ hệ thống khỏi sự tấn công.

Một ví dụ một trường hợp tốt nhất để triển khai mô hình gateway như vậy là như sau: giả thiết một bệnh viện đã sử dụng 40AP trên vài tầng của bệnh viện. Vốn đầu tư của họ vào đây là khá lớn. Vì thế nếu các AP không hỗ trợ các biện pháp an

toàn mà có thể nâng cấp, thì để tăng tính bảo mật, bệnh viện đó phải thay toàn bộ số AP. Trong khi đó nếu họ thuê một gateway thì công việc này sẽ đơn giản và đỡ tốn kém hơn nhiều. Gateway này có thể được kết nối giữa chuyển mạch lõi và chuyển mạch phân bổ (nối tới AP) và có thể đóng vai trò của server chứng thực, server VPN qua đó tất cả các client không dây có thể kết nối. Thay vì triển khai tất cả các AP mới, một (hoặc nhiều hơn tuỳ thuộc vào quy mô mạng) gateway có thể được cài đặt đằng sau các AP.

Sử dụng kiểu gateway này cung cấp một sự an toàn thay cho nhóm các AP. Đa số các gateway mạng không dây hỗ trợ một mảng các giao thức như PPTP, IPsec, L2TP, chứng thực và thậm chí cả QoS (Quality of Service– chất lượng dịch vụ).

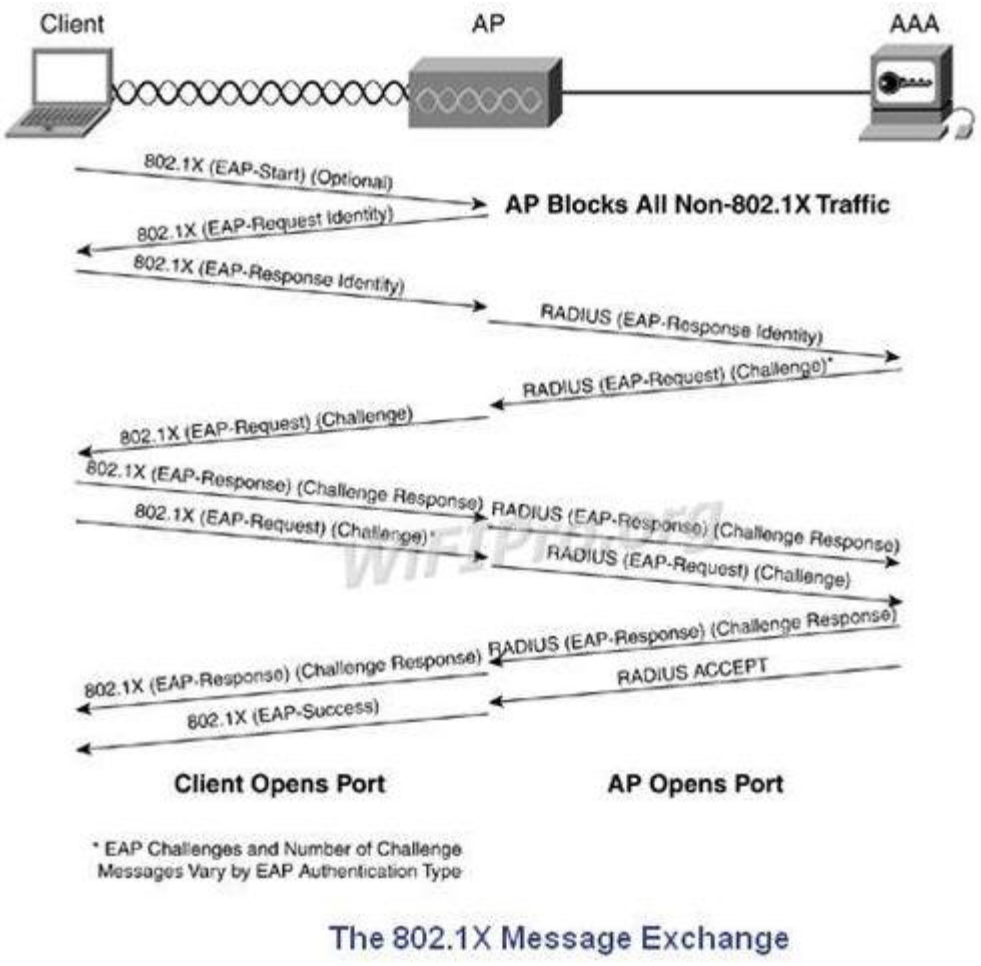
3.5.7. 802.1x giao thức chứng thực mở

Chuẩn 802.1x cung cấp những chi tiết kĩ thuật cho việc điều khiển truy nhập thông qua những cổng cơ bản. Việc điều khiển truy nhập thông qua những cổng truy nhập cơ bản được khởi đầu, và vẫn đang được sử dụng với chuyển mạch Ethernet. Khi người dùng thử nối tới cổng Ethernet, cổng đó sẽ đặt kết nối của người sử dụng ở chế độ khoá và chờ đợi sự xác nhận người sử dụng của hệ thống chứng thực.

Giao thức 802.1x đã được kết hợp vào trong hệ thống WLAN và gần như trở thành một chuẩn giữa những nhà cung cấp. Khi được kết hợp giao thức chứng thực mở (EAP), 802.1x có thể cung cấp một sơ đồ chứng thực trên một môi trường an toàn và linh hoạt.

EAP, được định nghĩa trước tiên cho giao thức point-to-point (PPP), là một giao thức để chuyển đổi một phương pháp chứng thực. EAP được định nghĩa trong RFC 2284 và định nghĩa những đặc trưng của phương pháp chứng thực, bao gồm những vấn đề người sử dụng được yêu cầu (password,certificate,v.v), giao thức được sử dụng (MD5, TLS, GMS, OTP, v.v), hỗ trợ sinh chìa khoá tự động và hỗ trợ sự chứng thực lẫn nhau.

Mô hình chứng thực 802.1x-EAP thành công thực hiện như sau:



Hình 3.16: Quá trình trao đổi thông tin xác thực 802.1x-EAP

1. Client yêu cầu liên kết với AP

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

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

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

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

6. AP chuyển yêu cầu cho phép tới client

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

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

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

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

Sinh chìa khoá động

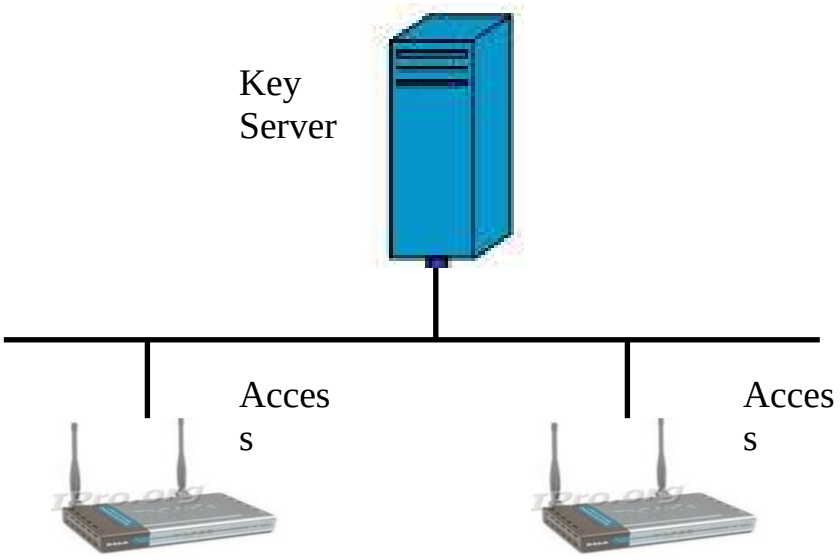
Để tránh việc giả mạo, mỗi một phiên kết nối với một client sẽ được RADIUS server cấp cho một key riêng, session key. Khi truyền key này cho Client, để tránh việc nghe trộm thông tin clear text, AP sẽ mã hoá session key này, và client sẽ dùng key của mình để giải mã, lấy session key cho mình. Tất cả các session key này đều được sinh bởi RADIUS server thông qua một thuật toán nào đó. Có khi mỗi phiên liên kết chỉ có một Key, nhưng bạn cũng có thể thiết lập trên RADIUS server để tạo các chu kỳ xác thực theo yêu cầu của bạn. Theo cơ chế này, RADIUS sẽ định kỳ, xác thực client, do đó tránh được truy cập mạng do vô tình.

Quản lí chìa khoá tập trung

Ngoài ra với những mạng WLAN quy mô lớn sử dụng WEP như một phương pháp bảo mật căn bản, server quản lý chìa khóa mã hóa tập trung nên được sử dụng vì những lí do sau:

- Quản lí sinh chìa khóa tập trung
- Quản lí việc phân bổ chìa khóa một cách tập trung
- Thay đổi chìa khóa luân phiên
- Giảm bớt công việc cho nhà quản lý

Bình thường, khi sử dụng WEP, những chìa khóa (được tạo bởi người quản trị) thường được nhập bằng tay vào trong các trạm và các AP. Khi sử dụng server quản lý chìa khóa mã hóa tập trung, một quá trình tự động giữa các trạm, AP và server quản lý sẽ thực hiện việc trao các chìa khóa WEP. Hình sau mô tả cách thiết lập một hệ thống như vậy:



Hình 3.17: Topo mạng quản lý chìa khóa mã hóa tập trung

Server quản lý chìa khóa mã hóa tập trung cho phép sinh chìa khóa trên mỗi gói, mỗi phiên, hoặc các phương pháp khác, phụ thuộc vào sự thực hiện của các nhà sản xuất. Phân phối chìa khóa WEP trên mỗi gói, mỗi chìa khóa mới sẽ được gán vào phần cuối của các kết nối cho mỗi gói được gửi, trong khi đó, phân phối chìa khóa WEP trên mỗi phiên sử dụng một chìa khóa mới cho mỗi một phiên mới giữa các node. Với những cải tiến của chuẩn 802.1x, các client được xác định thông qua username, thay vì địa chỉ MAC như các chuẩn cho trước đó. Nó không những tăng cường khả năng bảo mật mà còn làm cho quá trình AAA (Authentication, Authorization, and Accountting) hiệu quả hơn. Nếu không có sự xác thực lẫn nhau thì việc một client lầm tưởng một AP giả mạo là AP hợp pháp là điều hoàn toàn có thể xảy ra. Mô hình mạng sử dụng RADIUS server như trên đã khắc phục được điều đó thông qua việc xác thực ngược giữa Client và AP.

Thực tế quá trình xác thực xảy ra theo 3 pha, pha khởi đầu, pha chứng thực và pha kết thúc. Trong đó pha chứng thực với sự tham gia của RADIUS server cho phép hệ thống phân quyền người sử dụng thông qua các chính sách cài đặt trên server dựa trên tài khoản của người dùng. Nếu việc xác thực thông qua địa chỉ vật lý, MAC, chỉ là xác thực về mặt thiết bị, tức là không có sự phân quyền cho người dùng, thì xác thực dựa trên tên và mật khẩu cho phép chúng ta phân quyền người

dùng. Vấn đề cấp quyền, Authorization, tùy thuộc chính sách của người quản trị, có thể phân quyền theo giao thức, thông qua cổng, theo phạm vi dữ liệu, hoặc theo sự phân cấp về người dùng, admin, mod, member,v.v.

Thông qua việc quản lý và cấp quyền nói trên, người quản trị hoàn toàn có thể ghi lại được vết của người sử dụng, theo dõi các trang, thư mục cũng như ghi lại được tất cả quá trình truy cập của người dùng.

3.6. Chính sách bảo mật

Một công ty mà sử dụng WLAN nên có một chinh sách bảo mật thích hợp. Ví dụ, nếu không có chính sách đúng đắn mà để cho kích thước cell không thích hợp, thì sẽ tạo điều kiện cho hacker có cơ hội tốt để truy cập vào mạng tại những điểm ngoài vùng kiểm soát của công ty, nhưng vẫn nằm trong vùng phủ sóng của AP. Các vấn đề cần đưa ra trong chính sách bảo mật của công ty đó là các vấn đề về password, chìa khóa WEP, bảo mật vật lí, sự sử dụng các biện pháp bảo mật tiên tiến, và đánh giá phần cứng WLAN. Danh sách này tất nhiên không đầy đủ, bởi các giải pháp an toàn sẽ thay đổi với mỗi một tổ chức. Độ phức tạp của chính sách bảo mật phụ thuộc vào những yêu cầu an toàn của tổ chức cũng như là phạm vi của mạng WLAN trong mạng.

Những lợi ích của việc thực hiện, bảo trì một chính sách bảo mật đem lại là việc ngăn ngừa sự ăn cắp dữ liệu, sự phá hoại của các tập đoàn cạnh tranh, và có thể phát hiện và bắt giữ các kẻ xâm nhập trái phép.

Sự bắt đầu tốt nhất cho các chính sách bảo mật là việc quản lý. Các chính sách bảo mật cần được xem xét và dự đoán, và cần đưa vào cùng với các tài liệu xây dựng tập đoàn. Việc bảo mật cho WLAN cần được phân bổ thích hợp, và những người được giao trách nhiệm thực hiện phải được đào tạo một cách quy mô. Đội ngũ này lại phải thành lập chương mục tài liệu một cách chi tiết để có thể làm tài liệu tham khảo cho các đội ngũ kế cận.

3.6.1. Bảo mật các thông tin nhạy cảm

Một vài thông tin nên chỉ được biết bởi người quản trị mạng là:

- Username và password của AP và Bridge
- Những chuỗi SNMP
- Chìa khóa WEP
- Danh sách địa chỉ MAC

Những thông tin này phải được cất giữ bởi một người tin cậy, có kinh nghiệm, như người quản trị mạng, là rất quan trọng bởi nó là những thông tin nhạy cảm mà nếu lộ ra thì có thể là nguyên nhân của sự truy nhập trái phép, hoặc thậm chí là sự phá hủy cả một mạng. Những thông tin này có thể được cất giữ trong nhiều kiểu khác nhau.

3.6.2. Sự an toàn vật lý

Mặc dù bảo mật vật lý khi sử dụng mạng hữu tuyến truyền thông là quan trọng, thậm chí quan trọng hơn cho một công ty sử dụng công nghệ WLAN. Như đã đề cập từ trước, một người mà có card PC wireless (và có thể là một anten) không phải trong cùng khu vực mạng có thể truy cập tới mạng đó. Thậm chí phần mềm dò tìm sự xâm nhập không đủ ngăn cản những hacker ăn cắp thông tin nhạy cảm. Sự nghe lén không để lại dấu vết trên mạng bởi vì không có kết nối nào được thực hiện. Có những ứng dụng trên thị trường bây giờ có thể phát hiện các card mạng ở trong chế độ pha tạp (dùng chung), truy nhập dữ liệu mà không tạo kết nối.

Khi WEP là giải pháp bảo mật WLAN thích hợp, những điều khiển chặt chẽ nên đặt trên những người dùng mà có sở hữu các thiết bị client không dây của công ty, để không cho phép họ mang các thiết bị client đó ra khỏi công ty. Vì chìa khóa WEP được giữ trong chương trình cơ sở trên thiết bị client, bất kỳ nơi nào có card, vì thế làm cho mối liên kết an toàn của mạng yếu nhất. Người quản trị WLAN cần phải biết ai, ở đâu, khi nào mỗi card PC được mang đi.

Thường những yêu cầu như vậy là quá giới hạn của một người quản trị, người quản trị cần nhận ra rằng, bản thân WEP không phải là một giải pháp an toàn thích hợp cho WLAN. Kể cả với sự quản lí chặt chẽ như vậy, nếu một card bị mất hoặc bị ăn trộm, người có trách nhiệm với card đó (người sử dụng) phải được yêu cầu báo cáo ngay với người quản trị, để có những biện pháp đề phòng thích hợp.

Những biện pháp tối thiểu phải làm là đặt lại bộ lọc MAC, thay đổi chìa khóa WEP,v.v.

Cho phép nhóm bảo vệ quét định kỳ xung quanh khu vực công ty để phát hiện những hoạt động đáng ngờ. Những nhân sự này được huấn luyện để nhận ra phàn cứng 802.11 và cảnh giác các nhân viên trong công ty luôn luôn quan sát những người không ở trong công ty đàng trốn quanh tòa nhà với các phần cứng cơ bản của 802.11 thì cũng rất hiệu quả trong việc thu hẹp nguy cơ tấn công.

3.6.3. Kiểm kê thiết bị WLAN và kiểm định sự an toàn

Như một sự bổ sung tới chính sách an toàn vật lý, tất cả các thiết bị WLAN cần được kiểm kê đều đặn để lập chương mục cho phép và không cho phép các người sử dụng thiết bị WLAN truy nhập tới mạng của tổ chức. Nếu mạng quá lớn và bao gồm một số lượng đáng kể các thiết bị không dây thì việc kiểm kê định kỳ có thể không khả thi. Trong những trương hợp như vậy thì cần thiết thực hiện những giải pháp bảo mật WLAN mà không dựa trên phần cứng, nhưng dĩ nhiên là vẫn dựa trên username và password hoặc một vài loại khác trong các giải pháp bảo mật không dựa trên phần cứng. Với những mạng không dây trung bình và nhỏ, sự kiểm kê hàng tháng hoặc hàng quý giúp phát hiện những sự mất mát các phần cứng. Quét định kỳ với các bộ phân tích mạng để phát hiện các thiết bị xâm nhập, là cách tốt nhât để bảo mạng mạng WLAN

3.6.4. Sử dụng các giaỉ pháp bảo mật tiên tiến

Những tổ chức WLAN cần tận dụng một vài cơ chế bảo mật tiên tiến có sẵn trên thị trường. Điều đó cũng cần được đề cập trong chính sách bảo mật của công ty. Vì những công nghệ này khá mới, còn độc quyền và thường được sử dụng phối hợp với các giao thức, các công nghệ khác. Chúng cần được lập thành tài liệu hướng dẫn, để nếu có một sự xâm phạm xuất hiện, thì người quản trị có thể xác định nơi và cách mà sự xâm phạm đó xuất hiên.

Bởi chí số ít được đào tạo về bảo mật WLAN, do đó những người này rất là quan trọng, vì thế chính sách tiền lương cũng được đề cập đến trong các chính sách

bảo mật của công ty, tập đoàn. Nó cũng là một trong các mục cần lập tài liệu chi tiết.

3.6.5. Mạng không dây công cộng

Điều tất yếu sẽ xảy ra là những người sử dụng của công ty với những thông tin nhạy cảm của họ sẽ kết nối từ laptop của họ tới WLAN công cộng. Điều này cũng nằm trong chính sách bảo mật của công ty. Những người dùng đó phải chạy những phần mềm firewall cá nhân và các phần mềm chống vi rút trên laptop của họ. Đa số các mạng WLAN công cộng ít hoặc không có sự bảo mật nào, nhằm làm cho kết nối của người dùng đơn giản và để giảm bớt số lượng các hỗ trợ kỹ thuật được yêu cầu .

3.6.6. Sự truy nhập có kiểm tra và giới hạn

Hầu hết các mạng LAN lớn đều có một vài phương pháp để giới hạn và kiểm tra sự truy nhập của người sử dụng. Tiêu biểu là một hệ thống hỗ trợ chứng thực, sự cấp phép, và các dịch vụ Accounting, (Authentication, Authorization, Accountting (AAA)) được triển khai.

Những dịch vụ AAA cho phép tổ chức gắn quyền sử dụng vào những lớp đặc biệt của người dùng. Ví dụ một người dùng tạm thời có thể chỉ được truy cập vào internet trong một phạm vi nào đó.

Việc quản lý người sử dụng còn cho phép xem xét người đó đã làm gì trên mạng, thời gian và chương mục họ đã vào.

3.7. Những khuyến cáo về bảo mật

Như một sự tóm lược của phần II, phần dưới đây đưa ra vài khuyến cáo trong việc bảo mật mạng WLAN.

3.7.1. Wep

Không được chỉ tin cậy vào Wep, không có một biện pháp nào an toàn tốt để mà bạn có thể chỉ dùng nó để bảo mật. Một môi trường không dây mà chỉ được bảo vệ bởi Wep thì không phải là một môi trường an toàn. Khi sử dụng WEP không

được sử dụng chìa khóa WEP mà liên quan tới SSID hoặc tên của tổ chức làm chìa khóa WEP khó nhớ và khó luận ra. Có nhiều trường hợp trong thực tế mà chìa khóa WEP có thể dễ dàng đoán được nhờ việc xem SSID hoặc tên của tổ chức.

WEP là một giải pháp có hiệu quả để giảm bớt việc mất thông tin khi tình cờ bị nghe thấy, bởi người đó không có chìa khóa WEP thích hợp, do đó tránh được sự truy nhập của đối tượng này.

3.7.2. Định cỡ cell

Để giảm bớt cơ hội nghe trộm, người quản trị nên chắc chắn rằng kích cỡ cell của AP phải thích hợp. Phần lớn hacker tìn thấy những nơi mà tốn ít thời gian và năng lượng nhất để tìm cách truy cập mạng. Vì lí do này, rất quan trọng không cho phép những AP phát ra những tín hiệu ra ngoài khu vực an toàn của tổ chức, trừ khi tuyệt đối cần thiết. Vài AP cho phép cấu hình mức công suất đầu ra, do đó có thể điều khiển kích thước cell RF xung quanh AP. Nếu một người nghe trộm nằm trong khu vực không được bảo vệ của tổ chức và không phát hiện được mạng của bạn, thì mạng của bạn không phải là dễ bị ảnh hưởng của loại tấn công này.

Có thể người quản trị mạng sử dụng các thiết bị với công suất lớn nhất để đạt thông lượng lớn và vùng bao phủ rộng, những điều này sẽ phải trả giá bằng việc chi phí về các biện pháp bảo mật. Vì vậy với mỗi điểm truy nhập cần biết các thông số như công suất, vùng phủ sóng, khả năng điều khiển kích thước cell. Và việc điều khiển bán kính cell cần phải được nghiên cứu cho kỹ và lập thành tài liệu hướng dẫn cùng với cấu hình của AP hoặc của bridge cho mỗi vùng. Trong vài trường hợp có thể cần thiết đặt hai AP có kích cỡ cell nhỏ hơn thay vì một AP để tránh những tổn hại không nên có.

Cố gắng đặt AP của bạn về phía trung tâm của tòa nhà, nó sẽ giảm thiểu việc rò tín hiệu ra ngoài phạm vi mong đợi. Nếu bạn đang sử dụng những anten ngoài, phải lựu chọn đúng loại anten để có ích cho việc tối giản phạm vi tín hiệu. Tắt các AP khi không sử dụng. Những điều này sẽ giảm thiểu nguy cơ bị tấn công và giảm nhẹ gánh nặng quản lý mạng.

3.7.3. Sự chứng thực người dùng

Sụ chứng thực người dùng là một mối liên kết yếu nhất của WLAN, và chuẩn 802.11 không chỉ rõ bất kỳ một phương pháp chứng thực nào, đó là yêu cầu bắt buộc mà người sử quản trị phải làm với người sử dụng ngay khi thiết lập cơ sở hạ tầng cho WLAN. Sự chứng thực người dùng dựa vào Username và Password, thẻ thông minh, mã thông báo hoặc một vài loại bảo mật nào đó dùng để xác định người dùng, không phải là phần cứng. Giải pháp thực hiện cần hỗ trợ sự chứng thực song hướng giữa server chứng thực và các client không dây, ví dụ như RADIUS server.

RADIUS là chuẩn không chính thức trong hệ thống chứng thực người sử dụng. Các AP gửi những yêu cầu chứng thực người sử dụng đến một RADIUS server, mà có thể hoặc có một cơ sở dữ liệu được gắn sẵn hoặc có thể qua yêu cầu chứng thực để tới một bộ điều khiển vùng, như NDS server, active directory server, hoặc thậm chí là một hệ thống cơ sở dữ liệu tương hợp LDAP.

Một vài RADIUS vendor có những sản phẩm RADIUS hữu hiệu hơn, hỗ trợ các bản mới nhất cho các giao thức chứng thực như là nhiều loại EAP.

Việc quản trị một RADIUS server có thể rất đơn giản nhưng cũng có thể rất phức tạp, phụ thuộc vào yêu cầu cần thực hiện. Bởi các giải pháp bảo mật không dây rất nhạy cảm do đó cần cẩn thận khi chọn một giải pháp RADIUS server để chắc chắn rằng người quản trị có thể quản trị nó hoặc nó có thể làm việc hiệu quả với người quản trị RADIUS đang tồn tai.

3.7.4. Sự bảo mật cần thiết

Chọn một giải pháp bảo mật mà phù hợp với nhu cầu và ngân sách của tổ chức, cho cả bây giờ và mai sau. WLAN đang nhanh chóng phổ biến như vậy vì sự thực hiện dễ dàng một WLAN bắt đầu với một AP và 5client có thể nhanh chóng nên tới 15 AP và 300 client. Do đó cùng một cơ chế an toàn làm việc cho một AP là điều mà hoàn toàn không thể chấp nhận cho 300 AP, như thế sẽ làm tăng thêm chi phí bảo mật một cách đáng kể. Trong trường hợp này tổ chức cần có các phương pháp bảo mật cho cả hệ thống như: hệ thống phát hiện xâm nhập, firewalls,

radius server. Khi quyết định các biện pháp trên WLAN, thì các thiết bị này xét về lâu dài là một nhân tố quan trọng để giảm chi phí.

3.7.5.Sử dụng thêm các công cụ bảo mật

Tận dụng các công nghệ sẵn có như VPNs, firewall, hệ thống phát hiện xâm nhập, Intrusion Detection System (IDS), các giao thức và các chuẩn như 802.1x và EAP, chứng thực client với RADIUS có thể giúp đỡ các giải pháp an toàn nằm ngoài phạm vi mà chuẩn 802.11 yêu cầu và thừa nhận. Giá và thời gian thực hiện các giải pháp này thay đổi tùy theo quy mô thực hiện.

3.7.6. Theo dõi các phần cứng trái phép

Để phát hiện ra các IP trái phép các phiên dò các AP đó cần được hoạch định cụ thể nhưng không được công bố. Tích cực tìm và xóa bỏ các AP trái phep và sẽ giữ ổn định cấu hình AP và làm tăng tính an toàn. Việc này có thể được thực hiện trong khi theo dõi mạng một cách bình thường và hợp lệ. Kiểu theo dõi này có thể tìm thấy các thiết bị bị mất.

3.7.7. Switches hay Hubs

Một nguyên tắc đơn giản khác là luôn kết nối các AP tới Switch thay vì Hub, Hub là thiết bị quảng bá, do đó dễ bị mất pass và IP address

3.7.8. Cập nhật các vi chương trình và các phần mềm.

Cập nhật vi chương trình và driver trên AP và card không dây của bạn luôn luôn sử dụng những chương trình cơ sở và driver mới nhất trên AP và các không dây của bạn. Thường thì các đặc tính an toàn, các vấn đề cơ bản sẽ được cố định, bổ sung thêm các đặc tính mới, sự khắc phục các lố hổng trong các cập nhật này.

3.7.9. Các chế độ Ad hoc ở trên các mạng Wifi

Chế độ Ad-hoc là chế độ mà ở đó một máy tính sau khi kết nối được với AP có thể làm thay nhiệm vụ của AP, cho phép các máy tính khác cũng đang bật chế độ Ad-hoc có thể kết nối vào mạng thông qua nó. Chế độ này có thể tiết kiệm được chi phí mua AP nhưng lại rất không an toàn. Khi một máy có thể kết nối vào mạng

thông qua một máy tính khác thi nó có thể nhìn thấy tất cả các thông tin trên máy tính kia và có thể xâm nhập vào mạng may tính chính. Do đó để an toàn hãy khuyến cáo tất cả các máy tính trong mạng có các wifi nên tắt chế độ Ad-hoc của card mạng đi.

KẾT LUẬN

Sau thời gian thực hiện đề tài, với sự giúp đỡ nhiệt tình của thầy Hồ Văn Canh, đề tài luận văn tốt nghiệp: " Tổng quan về Wireless LAN và vấn đề bảo mật Wireless LAN " đã được hoàn thành đúng thời hạn.

Trong đồ án tốt nghiệp của mình, em đã tập trung tìm hiểu sâu kỹ thuật mạng WLAN và nghiên cứu độ an toàn cùng với các cơ chế bảo mật cho WLAN. Do điều kiện tiếp cận với mạng không dây trong thực tế khó được thực hiện. Em biết một vài cơ quan hoặc công ty đã ứng dụng mạng WLAN (Bộ Công An, Bộ Bưu Chính Viễn Thông,…) nhưng em không được phép tiếp cận do tính bảo mật riêng tư của đơn vị.

Vì vậy, chắc chắn là còn nhiều thiếu sót trong đề tài luận văn có thể xảy ra, em mong được sự góp ý, chỉ dẫn của các thầy cô để em có điều kiện hoàn thành tốt hơn luận văn của mình và có cơ sở để đưa lý thuyết áp dụng vào thực tiễn.

Em xin chân thành cảm ơn!

Hải phòng, 07/2009

Sinh viên thực hiện

Vũ Thị Dung

CÁC THUẬT NGỮ ĐƯỢC SỬ DỤNG

AAA	Authentication, Authorization, Accountting	Chứng thực, cấp phép, kế toán
ACK	Acknowlegment	Xác nhận
ADSL	Asymmetric Digital Subscriber Line	Mạng thuê bao không đồng bộ
AES	Advanced Encryption Standard	Chuẩn mã hóa nâng cao
AP	Access point	Điểm truy nhập
ASK	Amplitude shift keying	Điều biên
BPSK	Binary phase shift keying	Điều chế khóa dịch pha nhị phân
CCK	Complementary Code Keying	Khóa mã bổ xung
CDMA	Code Divison Multiple Access	Đa truy nhập phân chia theo mã
CPE	Customer Premises Equipment	Thiết bị tại nhà của khách hàng
CSMA/CA	Carrier Sense Multiple Access/ Collision Avoidance	Đa truy xuất cảm biến mang tránh xung đột
CTS	Clear To Send	Xóa nhận dạng gửi
DCS	Dynamic Channel Selection	
DHCP	Dynamic Host Configuration Protocol	Cơ chế đánh địa chỉ động
DSSS	Direct Sequence Spread Strectrum	Trải phổ trực tiếp
EAP	Extensible Authentication Protocol	Giao thức chứng thực mở rộng
ESS	Extended Service Set	Bộ dịch vụ mở rộng
FDD	Frequency Division Duplexing	
FDMA	Frequency Division Multiple	Đa truy nhập phân chia theo

	Access	tần số
FHSS	Frequency Hopping Spread Spectrum	Trải phổ nhảy tần
FIPS	Federal Information Processing Standard	
FSK	Frequency Shift Keying	Điều tần
ICV	Integrity Check Value	Giá trị kiểm tra toàn bộ
IDS	Intrusion Detection System	
IEEE	Institute of Electrical and Electronic Engineers	Viện kĩ thuật điện và điện tử
IMS	Industrial, Scientific and Medical	Băng tần dành cho Công nghiệp, khoa học và y tế
IV	Initialization Vector	Vector khởi tạo
MAC	Media Access Control	Điều khiển truy cập môi trường
NIST	National Institute of Standards and Technology	Viện tiêu chuẩn và kỹ thuật quốc gia
OFDM	Orthogonal Frequency Division Multiplexing	Phân chia tần số trực giao đa bộ phận
PCMCIA	Personal Computer Memory Card International Association	
PDA	Personal Digital Assistant	Máy trợ lý cá nhân dùng kỹ thuật số
PRNG	Pseudo Random Number Generator	Thiết bị tạo số giả ngẫu nhiên
PSK	Phase Shifp Keying	Điều pha
QoS	Quality of Service	Chất lượng dịch vụ
QPSK	Quardrature Phase Shift Keying	Điều chế khóa dịch pha cầu phương
RADIUS	Remote Authentication	Dịch vụ truy nhập bằng điện

	Dial_In User Service	thoại xác nhận từ xa
RTS	Request To Send	Yêu cầu gửi
SSID	Service Set Identifiers	Bộ nhận dạng dịch vụ
TDD	Time Division Duplexing	Phân chia theo thời gian
TDMA	Time Division Multiple Access	Đa truy nhập phân chia theo thời gian
TKIP	Temporal Key Integrity Protocol	Hàm thay đổi khóa
VPN	Virtual Private Network	Mạng riêng ảo
WDMZ	Wireless DeMilitarized Zone	Vùng phi quân sự không dây
WECA	Wireless Ethernet Compatibility Alliance	
WEP	Wired Equivalent Privacy	
Wi-fi	Wireless Fidelity	

DANH MỤC TÀI LIỆU THAM KHẢO

1. Kỹ thuật thâm nhập mạng không dây- Lê Tiến Liên.Minh Quân
2. Quản trị mạng.com.vn
3. 802.11 Wireless Network
4. Building a Cisco Network Wireless LAN, Cisco systems
5. IEEE Std 802.11-1999
6. Inttrodution to Wireless Technology, IBM
7. Security problems and solutions in WLAN access zones