TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI
KHOA ĐIỆN TỬ VIỄN THÔNG
----------o0o----------

BẢO MẬT MẠNG LAN KHÔNG DÂY

WIRELESS LAN SECURITY

Giáo viên hướng dẫn : **NGUYỄN TRUNG DŨNG**
Sinh viên thực hiện : **NGUYỄN HUY BẮC**
Lớp : **Chuyên đề 2B – K44**

HÀ NỘI - 2004

Danh mục hình vẽ

LỜI MỞ ĐẦU

Công nghệ không dây là một phương pháp chuyển giao từ điểm này đến điểm khác mà không sử dụng đường truyền vật lý, mà sử dụng radio, Cell, hồng ngoại và vệ tinh. Mạng không dây ngày nay bắt nguồn từ nhiều giai đoạn phát triển. của thông tin vô tuyến, và những ứng dụng điện báo và radio. Mặc dầu một vài phát minh xuất hiện từ những năm 1800, nhưng sự phát triển nổi bật đạt được vào kỷ nguyên của công nghệ điện tử, và chịu ảnh hưởng lớn của nền kinh tế học hiện đại, cũng như các khám phá trong lĩnh vực vật lý. Cho đến nay, mạng không dây đã đạt được những bước phát triển đáng kể. Tại một số nước có nền công nghệ thông tin phát triển, mạng không dây thực sự đi vào cuộc sống. Chỉ cần một laptop, PDA hoặc một phương tiện truy nhập mạng không dây bất kỳ, bạn có thể truy nhập vào mạng ở bất cứ nơi đâu, trên cơ quan, trong nhà, ngoài đường, trong quán cafe, trên máy bay v.v, bất cứ nơi đâu nằm trong phạm vi phủ sóng của WLAN. Tuy nhiên chính sự hỗ trợ truy nhập công cộng, các phương tiện truy nhập lại đa dạng, đơn giản, cũng như phức tạp, kích cỡ cũng có nhiều loại, đã đem lại sự đau đầu cho các nhà quản trị trong vấn đề bảo mật. Làm thế nào để tích hợp được các biện pháp bảo mật vào các phương tiện truy nhập, mà vẫn đảm bảo những tiện ích như nhỏ gọn, giá thành, hoặc vẫn đảm bảo hỗ trợ truy cập công cộng.v.v.

Trong tập tài liệu nhỏ bé này chúng ta sẽ có một cái nhìn tổng quan về WLAN, lịch sử phát triển, chuẩn thực hiện, một số đặc tính kỹ thuật, các phương pháp bảo mật vốn có và các giải pháp được đề nghị.

Để hoàn thành tập tài liệu này, em xin cám ơn:

Thầy **Nguyễn Trung Dũng**, giảng viên khoa Điện tử viễn thông, Trường Đại học Bách Khoa-Hà Nội

Anh **Nguyễn Đăng Hùng**, phó phòng Tích hợp và phát triển hệ thống, công ty VDC

Anh **Lê Minh Đức**, trưởng phòng kỹ thuật, trung tâm Saigonctt

đã chỉ bảo và giúp đỡ em hoàn thành tập tài liệu này.

Tôi cũng xin cảm ơn gia đình và bạn bè đã tạo điều kiện, giúp đỡ và động viên tôi trong quá trình viết tập tài liệu này.

Tập tài liệu này được chia làm hai phần

Phần I: Giới thiệu về WLAN

Phần II: Bảo mật mạng WLAN

Trong phần I trình bày một cái nhìn tổng quan về Wlan, công nghệ sử dụng, các chuẩn, các đặc tính kỹ thuật, khả năng ứng dụng trên thị trường Việt Nam. Phần này cũng đề cập đến vấn đề đa truy nhập, CSMA/CA, kỹ thuật điều chế, kỹ thuật đa truy nhập, FDMA, TDMA, và CDMA. Trong phần này cũng nói đến vấn để trải phổ, trải phổ trực tiếp và trải phổ nhảy tần, và giới thiệu sơ qua về các phương pháp bảo mật.

Phần II đi vào chi tiết từng phương pháp bảo mật, các phương pháp đã được công nhận chuẩn cũng như các phương pháp còn đang xem xét. Các nguy cơ mất an toàn đối với mạng và các biện pháp khắc phục. Cuối phần là một vài khuyến nghị được đưa ra đối với người thực hiện, nhằm khắc phục các nhược điểm cố hữu của các phương pháp bảo mật.

Trong quá trình làm, do điều kiện thời gian và trình độ có hạn, bên cạnh đó đây lại là một công nghệ còn khá mới ở Việt Nam, nên ít có điều kiện tiếp xúc với các thiết bị thực tế, do đó không tránh khỏi một số sai sót.

Vì vậy mong các bạn tham khảo và đóng góp ý kiến để dần hoàn thiện tập tài liệu này.

Mọi ý kiến đóng góp xin liên lạc theo địa chỉ: Nguyễn Huy Bắc, 0953.334337 hoặc qua hòm thư: bacnh@dts.com.vn.

Tôi xin chân thành cám ơn!

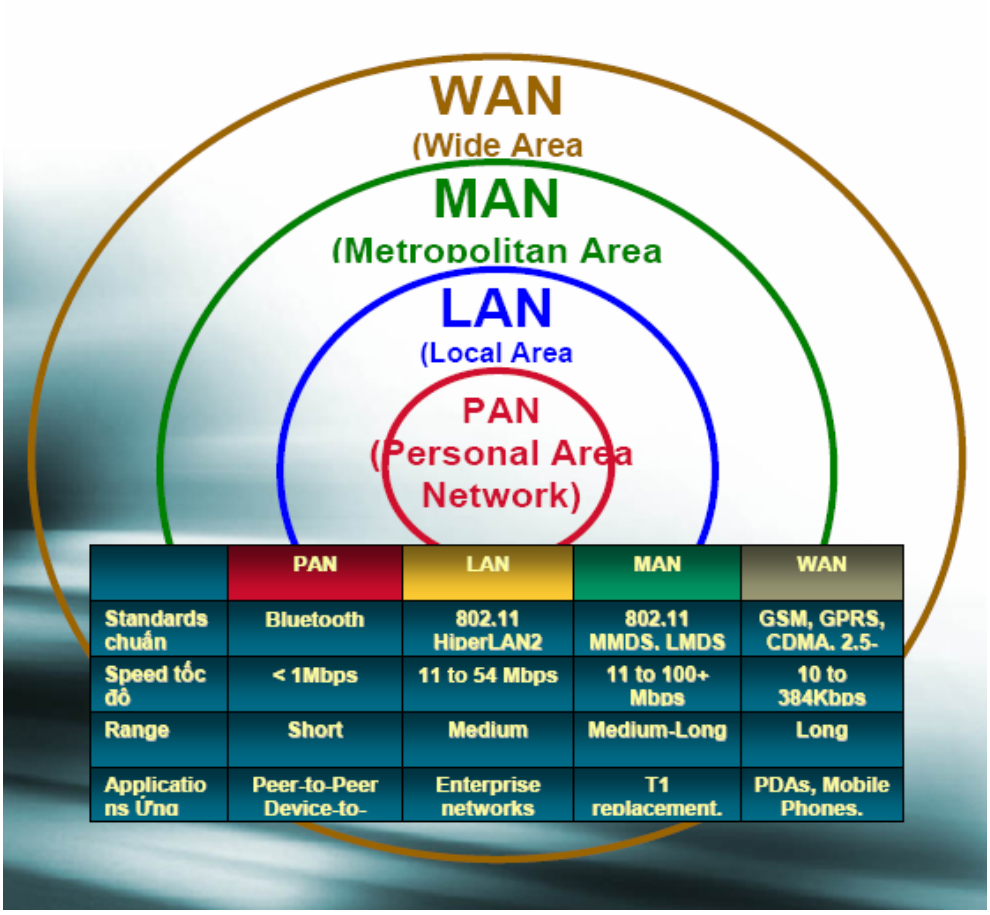
Huy Bắc, tháng 05 năm 2004

PHẦN I
GIỚI THIỆU VỀ WIRELESS LAN

I. TỔNG QUAN VỀ WLAN

1. Tổng quan:

Được phê chuẩn của IEEE 802.11 vào năm 1999, đến nay Wireless Local Area Network (**WLAN**) đã trở lên phát triển mạnh trên thế giới, tuy nhiên ở một số nước mà nền công nghệ thông tin mới 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...



	PAN	LAN	MAN	WAN
Standards chuẩn	Bluetooth	802.11 HiperLAN2	802.11 MMDS. LMDS	GSM, GPRS, CDMA. 2.5-
Speed tốc độ	< 1Mbps	11 to 54 Mbps	11 to 100+ Mbps	10 to 384Kbps
Range	Short	Medium	Medium-Long	Long
Applicatio ns Ứng	Peer-to-Peer Device-to-	Enterprise networks	T1 replacement.	PDAs, Mobile Phones.

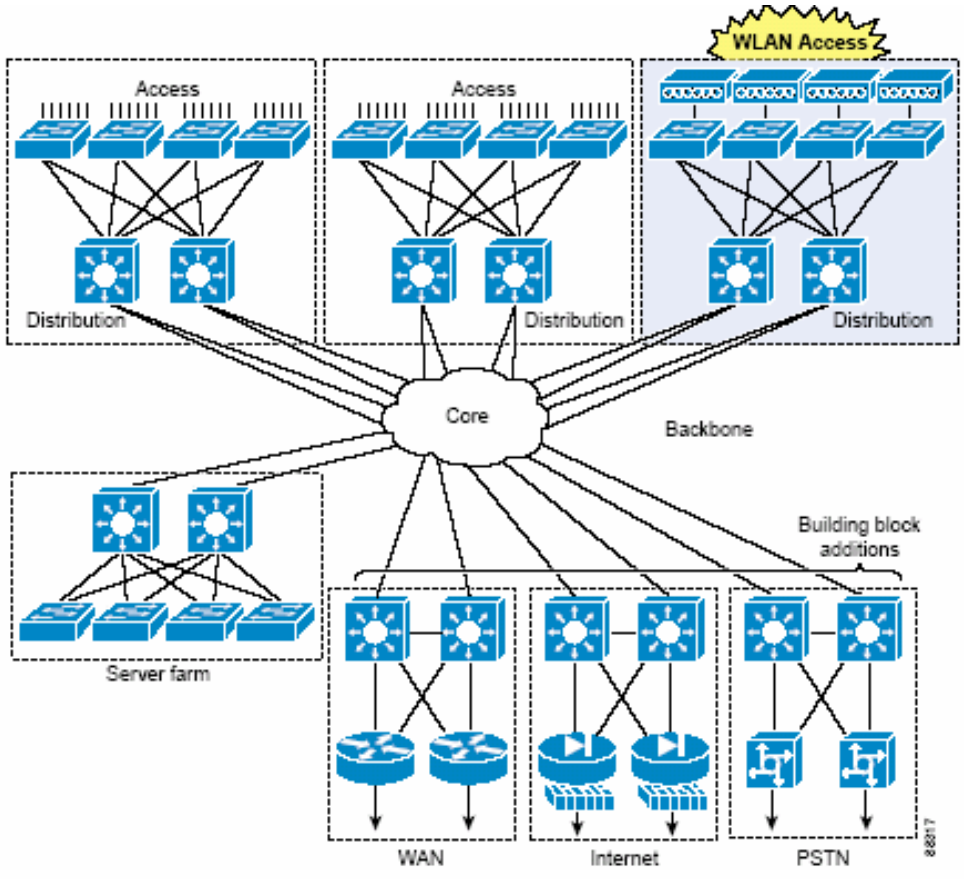
Hình 1: Vai trò và vị trí của Lan

2. Công nghệ sử dụng:

IEEE 802.11: "WLAN là một công nghệ internet không dây tốc độ cao theo chuẩn 802.11 IEEE"

- Kích thước phủ sóng mỗi HOTSPOT: < 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)



Hình 2: cấu trúc mạng

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 các đối tượng đáng quan tâm là các 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, . . .

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. . .

5. Khả năng ứng dụng tại Việt Nam:

- Việt nam là một nước công nghệ thông tin đang 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, năm 2003 vừa qua có các giải thể thao lớn như Seagames, Paragames .v.v. Các khách quốc tế, du lịch có Laptop cắm card để nối mạng WLAN, hoặc Laptop đời mới Cetrino là đối tượng người dùng. (theo boingo: năm 2005 90% Laptop có sãn 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 HOTSPOT 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 HOTSPOT, giảm giá cước, có chiến dịch xúc tiến, tiếp thị.

II/ PHƯƠNG ÁN KỸ THUẬT

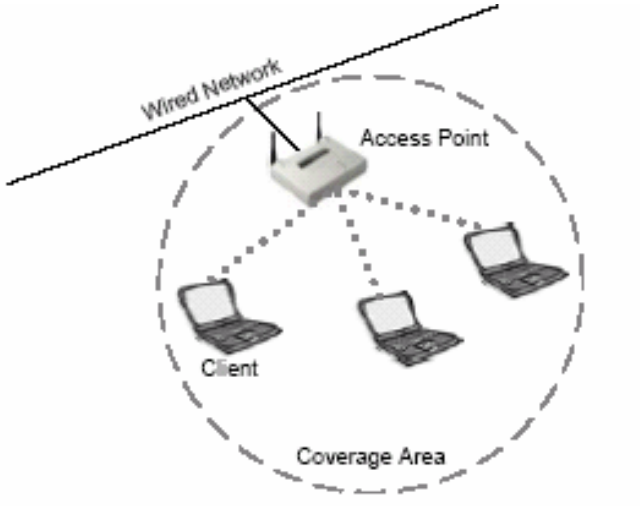
1. Tổng quan:

WLAN là một công nghệ truy cập mạng băng rộng không dây theo chuẩn của 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 để cung cấp đường truy cập internet băng thông rộng ngày càng nhiều ở các địa điểm công cộng như sân bay, cửa hàng cafe, nhà ga, các trung tâm thương mại hay trung tâm báo chí .

Tiêu chuẩn IEEE 802.11 định nghĩa cả hai kiểu cơ sở hạ tầng, với số lượng tối thiểu các điểm truy nhập trung tâm tới một mạng hữu 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 mở rộng truy cập tới các mạng cục bộ, như Intranet, cũng như hỗ trợ

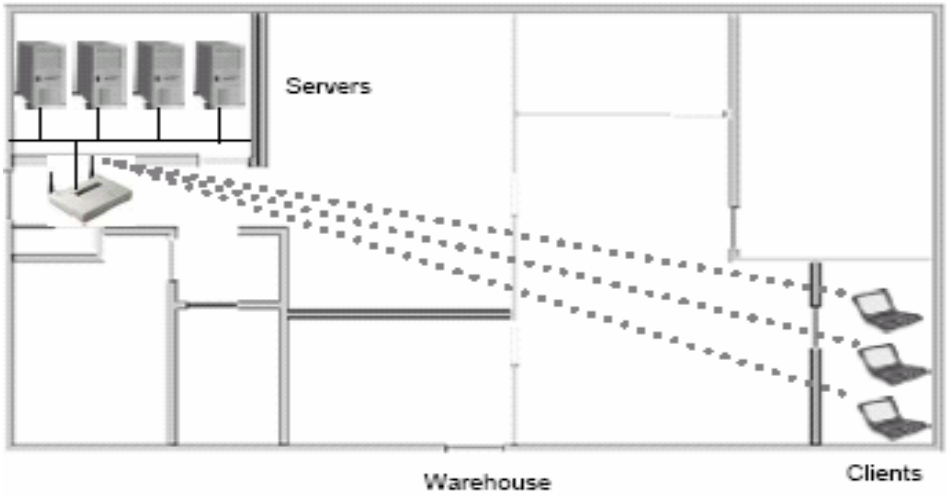
sự truy nhập băng rộng tới Internet tại các Hotspot. WLAN có thể cung cấp kết nối không dây nhanh chóng và dễ dàng tới các máy tính, các máy móc hay các hệ thống trong một khu vực, nơi mà các hệ thống cơ sở hạ tầng truyền thông cố định không tồn tại hoặc nơi mà sự truy nhập như vậy là không được phép. Người dung có thể 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 cho ban cái nhìn tổng quan về khả năng ứng dụng của WLAN:

Về khả năng sử dụng WLAN để mở rộng mạng hữu tuyến thông thường, với tốc độ cao và tiện lợi trong truy nhập mạng



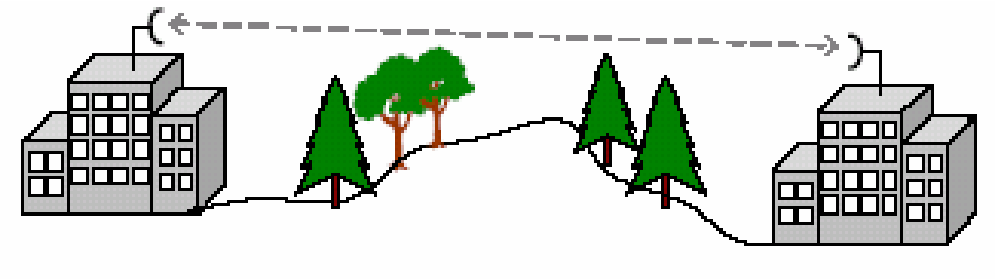
Hình 3: khả năng mở rộng mạng

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 di dây



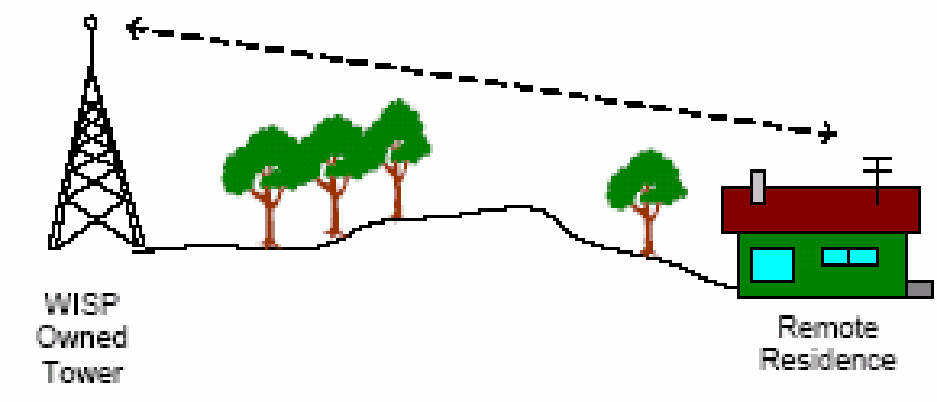
Hình 4: khả năng truy cập mạng mà không phải đi dây

Về khả năng đơn giản hóa việc kết nối mạng giữa hai tòa nhà mà giữa chúng là địa hình phức tạp khó thi công đối với mạng thông thường



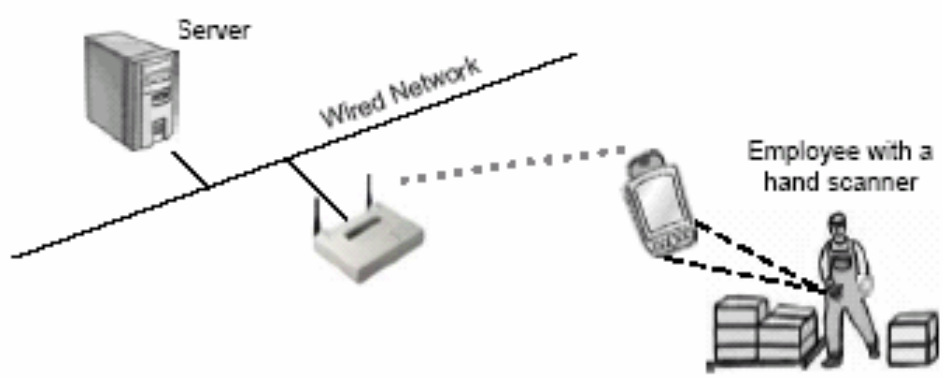
Hình 5: tiện lợi trong việc xây dựng mạng trên miền núi

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



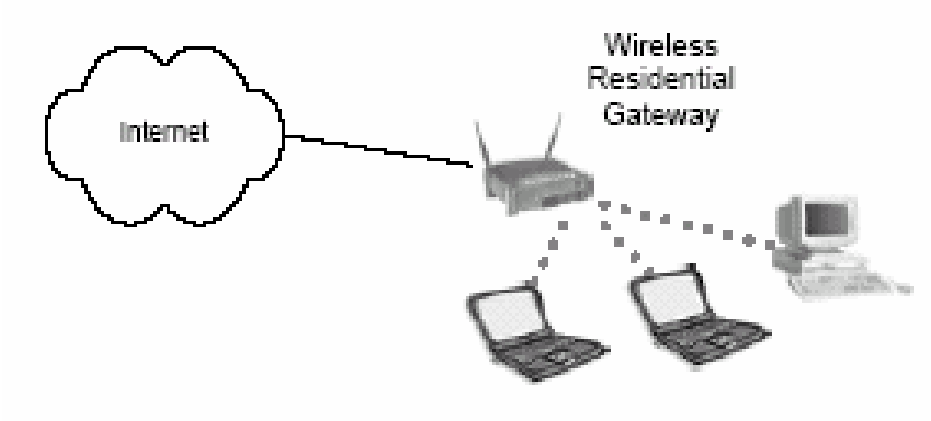
Hình 6: Tại nơi có địa hình lòng chảo

và sự tiện lợi trong việc truy cập mạng mà vẫn có thể di chuyển



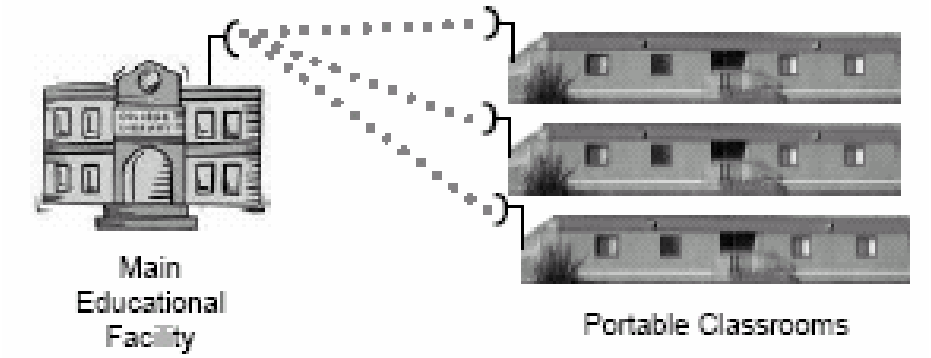
Hình 7: khả năng truy cập trong khi di chuyển

Từ các văn phòng, nhà riêng



Hình 8: truy cập từ nhà riêng

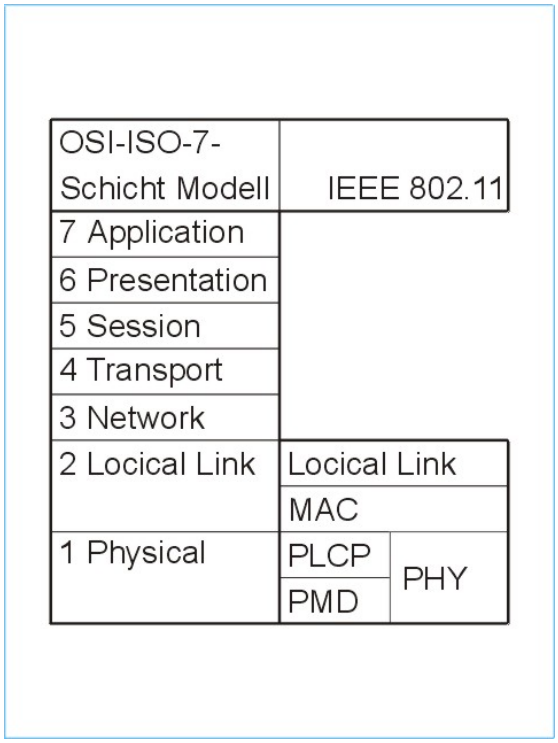
đến các khu lớn hơn nhiều như các trường đại học, các khu trung cư đều có thể truy cập mạng với tốc độ cao và quá trình thiết lập đơn giản



Hình 9: truy cập từ các trường đại học

2. Các tính năng của WLAN 802.11

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



Hình 10: Vị trí của WLAN trên mô hình 7 lớp

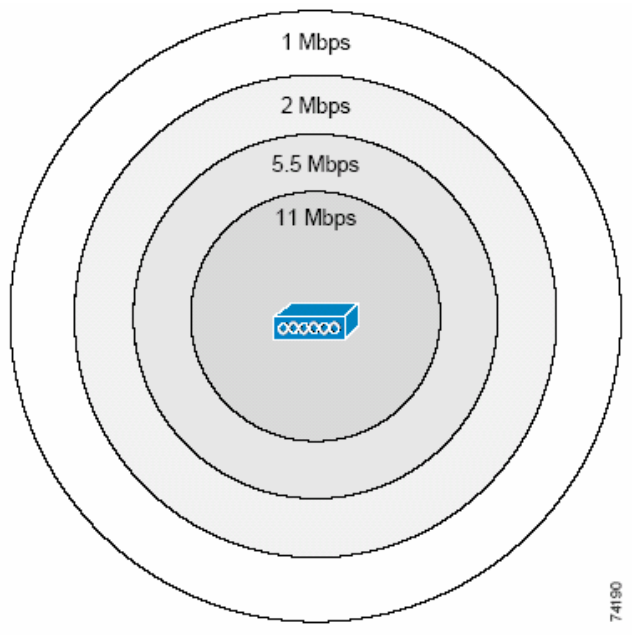
IEEE 802.11 gồm có các chuẩn:

- **802.11a:** 5÷6 GHz, 54Mbps, Sử dụng phương pháp điều chế OFDM (Orthogonal Frequency Division Multiplexing), hoạt động ở dải tần 5÷6 GHz, tốc độ truyền dữ liệu lên tới 54Mbps, hiện chuẩn này đang được một số hãng đầu tư để hy vọng chiếm lĩnh thị trường thay cho chuẩn 802.11b.
- **802.11b:** 2.4GHz, 11Mbps, DSSS đây là một chuẩn khá phổ biến, nó hoạt động ở dải tần 2.4GHz, là dải tần ISM (Industrial, Scientific và Medical). Ở Mỹ, thiết bị hoạt động ở dải tần này không phải đăng ký. 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 (frame) thông tin của 802.11.
- **802.11d:** cũng hỗ trợ các khung thông tin của 802.11 nhưng tuân theo những tiêu 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 2.4 GHz, nó là phiên bản nâng cấp của chuẩn 802.11b, được thông qua bởi IEEE, tốc độ truyền thể lên tới 54Mbps nhưng chỉ truyền được giữa những đối tượng nằm trong khoảng cách ngắn.

- **802.11h:** có thêm tính năng lựa chọn kênh tự động, Dynamic Channel Selection (DCS) và điều khiển công suất truyền dẫn (Transmit Power Control).
- **802.1x:** một chuẩn mới được cập nhật và thực hiện, nó cung cấp sự 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 WLANs để cung cấp một 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 có thể 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 sẽ vẫn tương thích với thuật toán RC4
- **802.11j:** là chuẩn thống nhất toàn cầu cho các tiêu chuẩn: IEEE, ETSI, HiperLAN2, ARIB, HiSWANa.

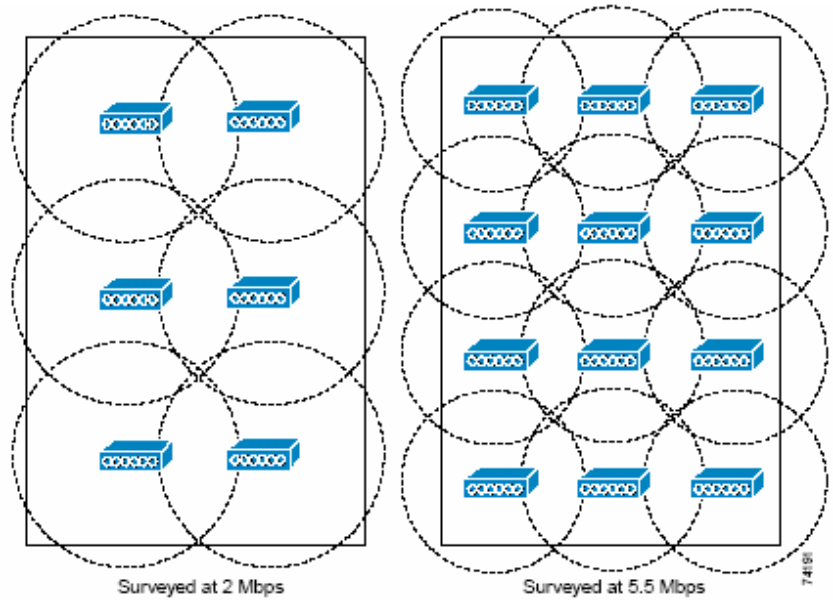
Với các chuẩn 802.11, thì chuẩn 802.11b và 802.11g hoạt động ở dải tần 2.4GHZ, tuy nhiên dải tần số ISM là dải tần số hoạt động mà không cần cấp phép, do đó có thể bị giao thoa đáng kể với các phương tiện như xe cấp cứu, ôtô cảnh sát, xe taxi, cũng như từ những người dùng khác và nhiều thiết bị gia đình và văn phòng hoạt động trong băng ISM. Vì lẽ đó mà chuẩn 802.11a được đưa ra. Nhưng tất cả các version 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 qua 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 11: 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 12: Tốc độ và số AP

Xét trong cùng một 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 5.5Mbps thì để phạm vi phủ sóng bao hết khu vực trên thì cần gấp đôi số AP, 12 AP (h.vẽ).

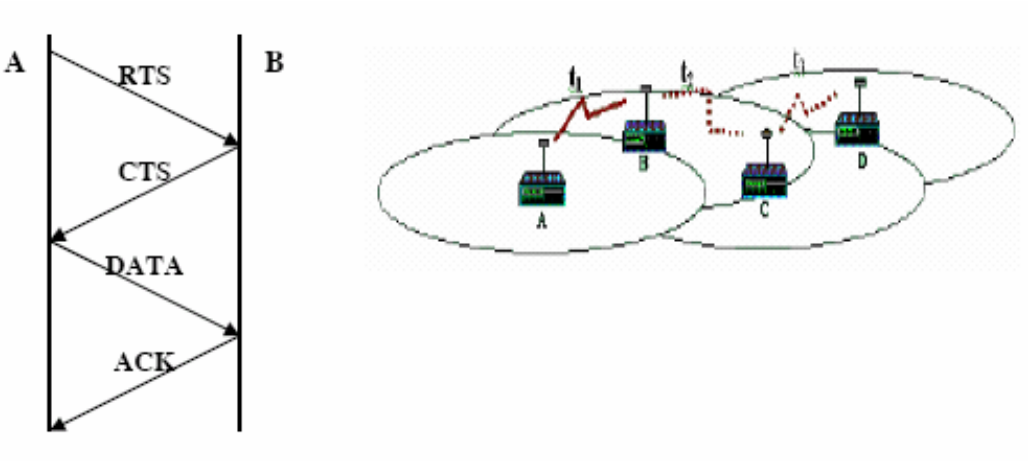
Khái niệm In-door và Out-door: In-door là khái niệm dùng vô tuyến trong phạm vi không gian nhỏ, như trong một tòa nhà. Out-door là khái niệm dùng vô tuyến trong phạm vi không gian lớn hơn, với WALN thì bán kính đến các CPE (Customer Premises Equipment) mà nó quản lý có thể từ 5÷40km. Với khoảng cách nhỏ hơn 1km thì thậm chí CPE không cần trong tầm nhìn thẳng (Light of Sight) 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 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.

3. Truy nhập kênh truyền, cơ chế đa truy nhập CSMA/CA:

Một trạm không dây muốn truyền khung, đầu tiên nó sẽ nghe trên môi trường không dây để xác định 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.

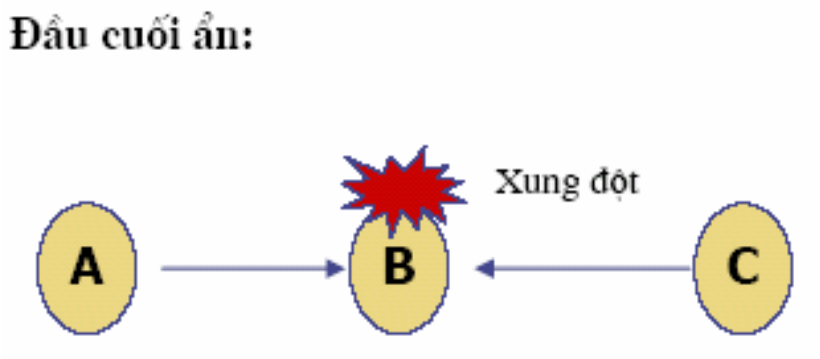
Important factors:

- Wait for silence
- Then talk
- Listen while talking.
- What do we do if there's 2 talkers? Backoff.
- Repeat



Hình 13: Một quá trình truyền từ A đến B:

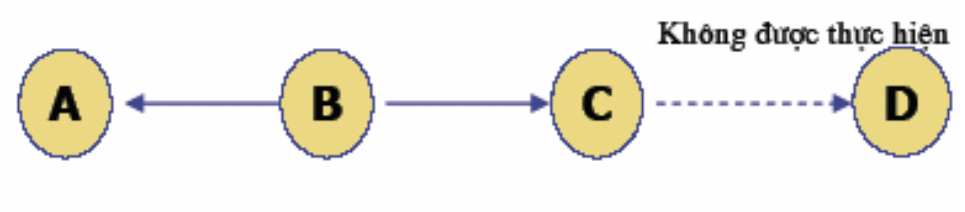
Trong cơ chế CSMA/CA ta cần quan tâm đến hai vấn đề là đầu cuối ẩn (Hidden Terminal) và đầu cuối hiện (Exposed Terminal).



Hình 14: Đầu cuối ẩn

- A nói chuyện với B
  - C cảm nhận kênh 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

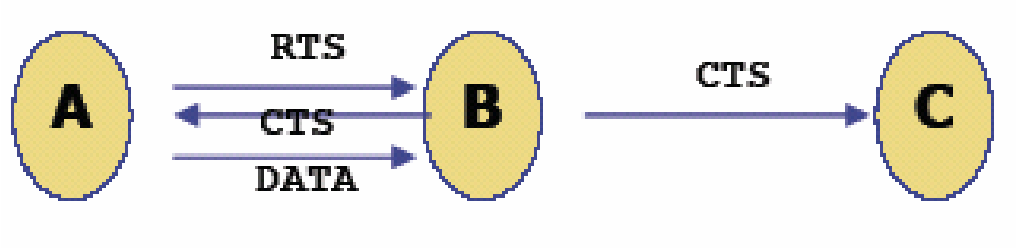
Đầu cuối hiện:

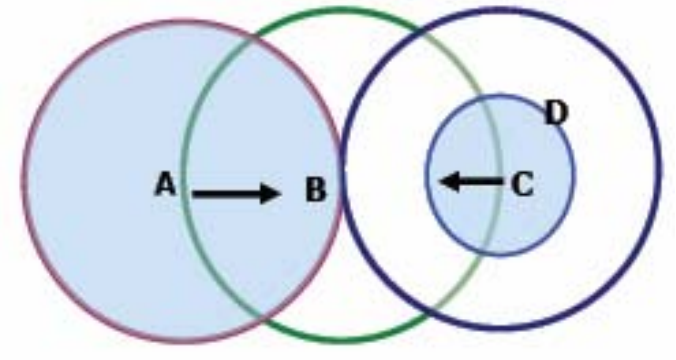


Hình 15: Đầu cuối hiện

- 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 16: Giải quyết vấn đề đầu cuối ẩn

- A gửi RTS cho B
  - B gửi lại CTS 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 dụng nó để đặt thời gian kìm hãm sự truyền.

Giải quyết vấn đề đầu cuối hiện:

Hình 17: Giải quyết vấn đề đầu cuối ẩn

- 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 bị 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 thi 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).

4. Kỹ thuật điều chế:

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 suất lỗi thấp nhất với mức tín hiệu thu cho trước khi đo một chu kỳ dấu hiệu.

a/ Nguyên lý cơ bản của điều chế PSK

Dạng xung nhị phân coi như là đầu vào của bộ điều chế 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

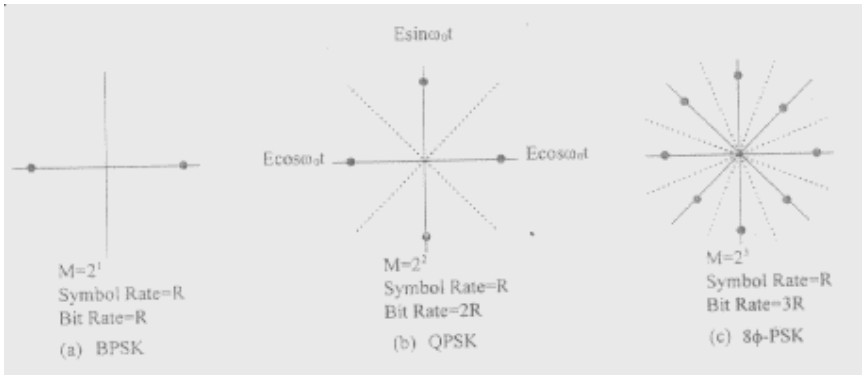
$$V_0(t) = E \sin\left[\omega_0 t + \frac{2\pi(i-1)}{M}\right]$$

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. Các trạng thái pha của chúng được minh hoạ trên hình .

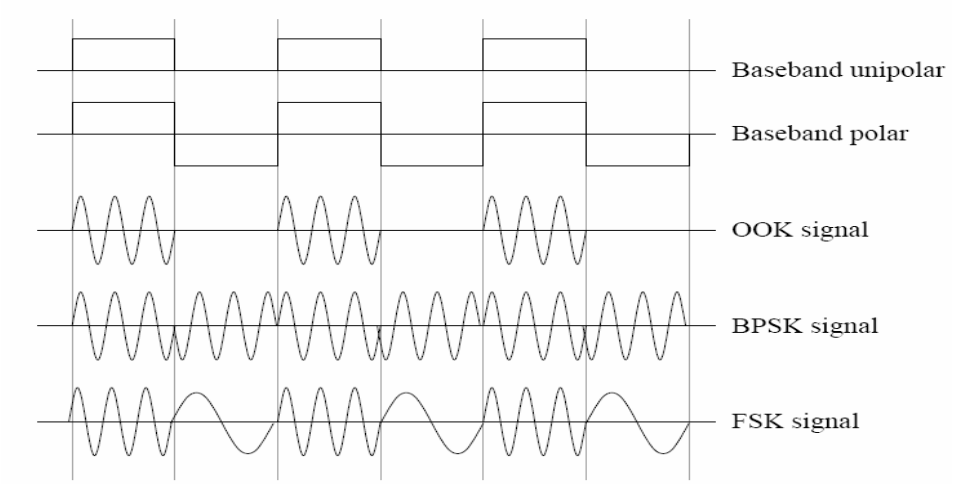


Hình 18: Các trạng thái pha của PSK

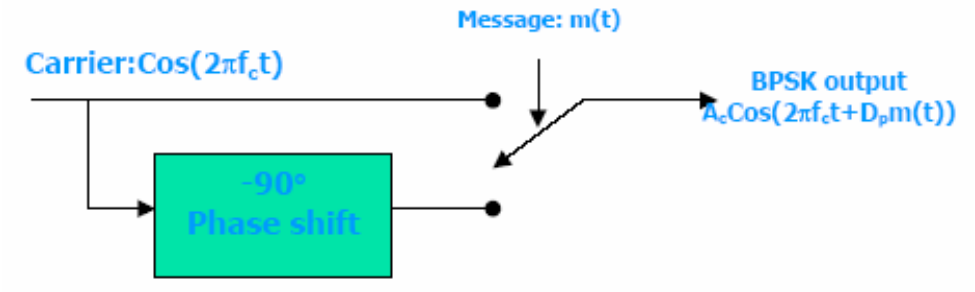
Ở đây cần ghi nhớ rằng khi số lượng các trạng thái pha tăng lên thì tốc độ bit cũng tăng nhưng tốc độ boud vẫn giữ nguyên. Tuy nhiên muốn tăng tốc độ số liệu thì phải trả giá. Nghĩa là, yêu cầu về SNR tăng lên để giữa nguyên được BER (tỷ lệ lỗi bit).

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

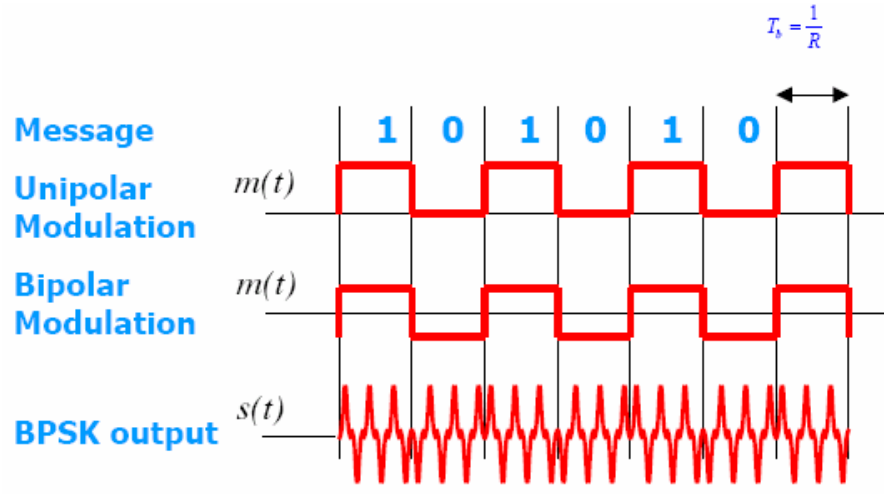
Đây là phương pháp thông dụng nhất, tín hiệu sóng mang được được điều chế dựa vào chuỗi nhị phân, tín hiệu điều chế có biên độ không đổi và biến đổi giữa hai trạng thái 0^0 và 180^0, mỗi trạng thái của tín hiệu điều chế được gọi là một symbol.



Hình 19: Các dạng tín hiệu điều chế



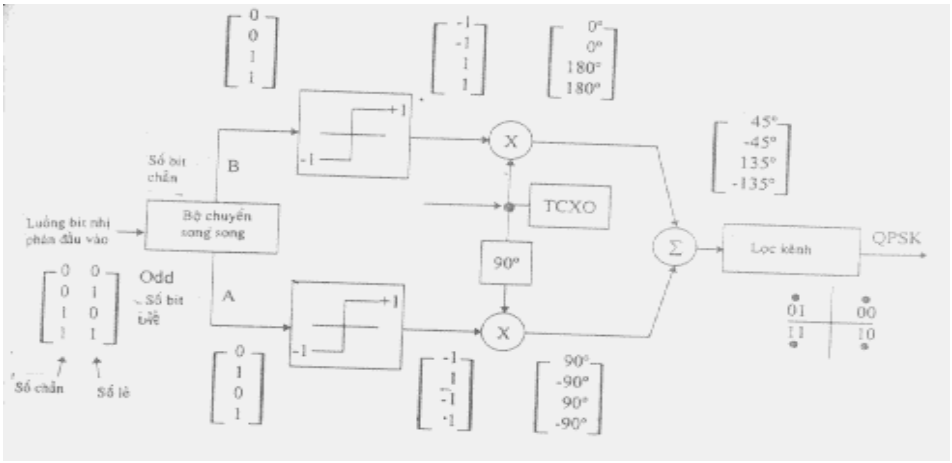
Hình 20: Sơ đồ điều chế BPSK



Hình 21: Tín hiệu điều chế BPSK

QPSK (Quardrature Phase Shift Keying):

Ở phương pháp BPSK, mỗi symbol biển diễn cho một bit nhị phân. Nếu mỗi symbol này biểu diễn nhiều hơn 1 bit, thì sẽ đạt được một tốc độ bit lớn hơn. Với QPSKsẽ gấp đôi số data throughput của PSK với cùng một băng thông bằng cách mỗi symbol mang 2 bits. 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.



Hình 22: Bộ điều chế QPSK

CCK (Complementary Code Keying):

CCK là một 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 complementary spreading code có chiều dài mã là 8 và tốc độ chipping rate là 11Mchip/s. 8 complex 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.

4.1 Kỹ thuật điều chế song công (DUPLEX SCHEME)

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 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 hai 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-voice) hay không đối xứng (dữ liệu-data). 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 (downstream), ví dụ như khi xem các trang Web, thì băng thông của chiều lên (upstream) không được sử dụng. Điều này lại không xảy ra khi hệ thống được sử dụng cho các ứng dụng thoại: Hai bên 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 được tăng lên, và ngược lại. Với sự giám sát số lượng khe thời gian cho mỗi 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 các máy trạm trong khu vực của một hệ thống sử dụng kỹ thuật TDD cần có một điểm thời gian tham chiếu để có thể xác được 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.

5. 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.

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.

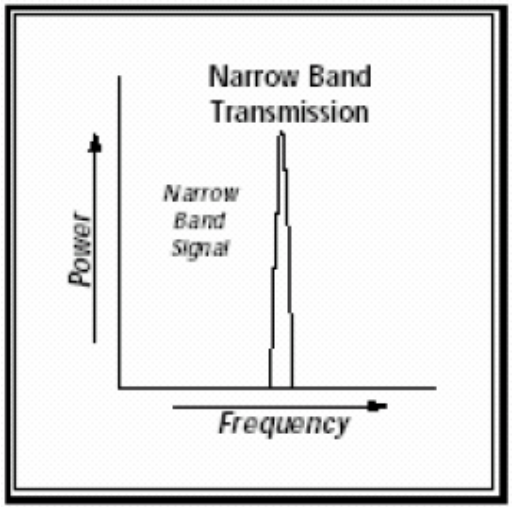
CDMA (Code Divison Multiple Access) - đa truy nhập phân chia theo mã

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.

6. Kỹ thuật vô tuyến

Viba truyền thống

Trong kỹ thuật vi ba truyền thống mỗi CPE sẽ được cung 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 sử dụng kênh vô tuyến 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 truyền thống tỏ ra chỉ thích hợp cho các ứng dụng thoại và dữ liệu tốc độ thấp.

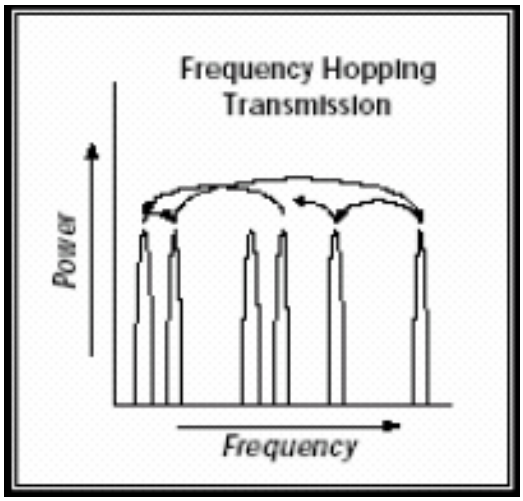


Hình 23: Tín hiệu băng hẹp

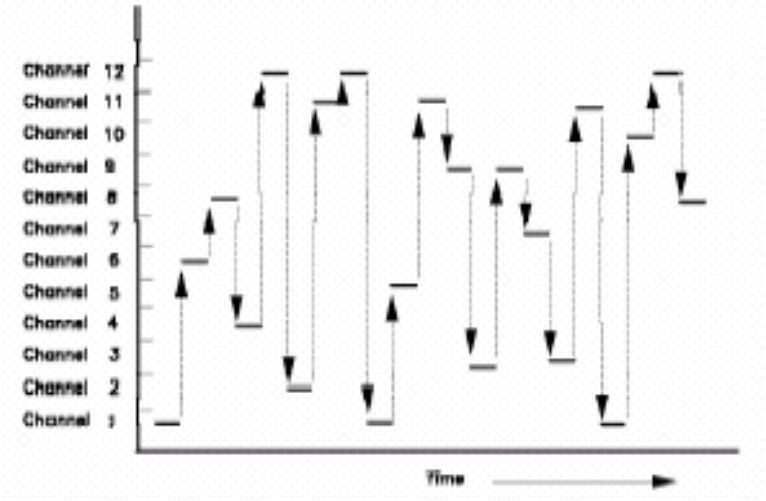
Kỹ thuật trải phổ

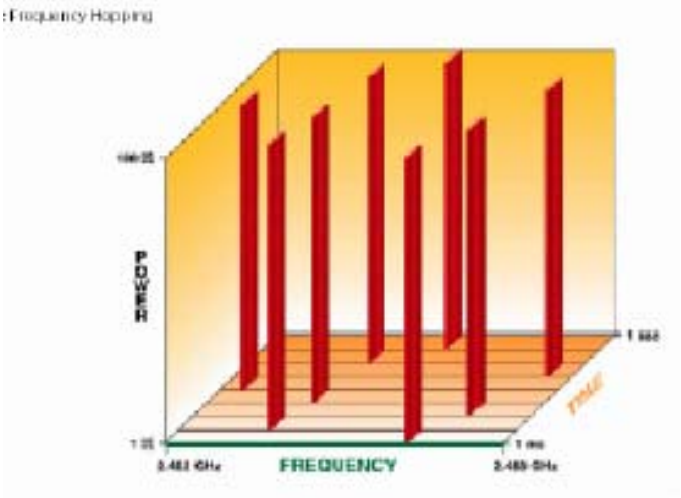
Khi tài nguyên vô tuyến ngày càng trở nên cạn kiệt, người ta bắt đầu phải áp dụng kỹ thuật trải phổ nhằm nâng cao hiệu năng sử dụng tần số. Có hai kỹ thuật trải phổ thông dụng nhất hiện nay là FHSS và DSSS. Băng thông cho mỗi CPE sẽ không còn là một dải hẹp mà sẽ là toàn bộ băng tần số, việc xác định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

FHSS (Frequency Hopping Spread Spectrum)



Hình 24: Nhảy tần số



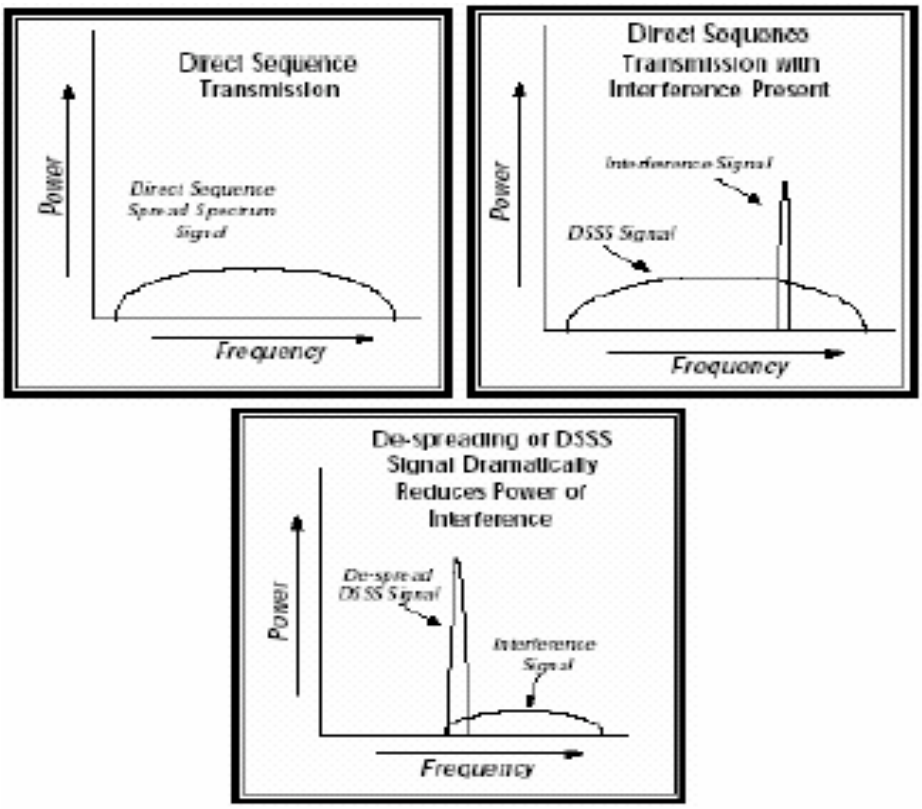


Hình 25: Các kênh trong FHSS

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 động bộ lại (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 do kênh dữ liệu 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 sẽ 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 hoàn toàn khác. Băng thông của tín hiệu thay vì được truyền trên một băng hẹp (narrow band) như truyền thông vi ba, sẽ được truyền trên một khoảng tần số lớn hơn bằng kỹ thuật mã hóa giả ngẫu nhiên (Pseudo-Noise sequence).



Hình 26: Quá trình trải và nén phổ trong DSSS

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 (power density) 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 nhiễn trong quá trình mã hóa 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 bất 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 là 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 sử lý độ lợi (gain processing). Xử lý độ lợi là quá trình làm giảm mật độ phổ công xuất khi tín hiệu được xử lý để truyền và tăng mật độ phổ công suất khi despread, với mục đích chính là làm tăng tỉ số S/N (Signal to Noise ratio).

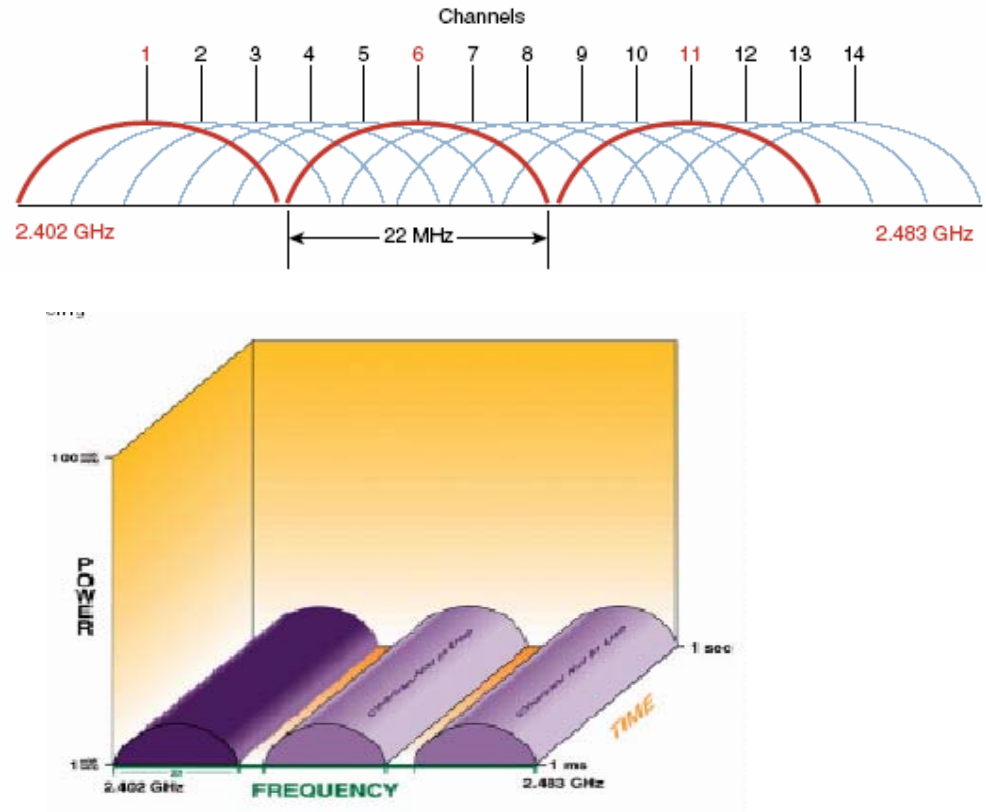
So sánh FHSS và DSSS

FH không có quá trình xử lý độ lợi do tín hiệu không được trải phổ. Vì thế nó sẽ phải dùng nhiều công xuất hơn để có thể truyền tín hiệu với cùng mức S/N

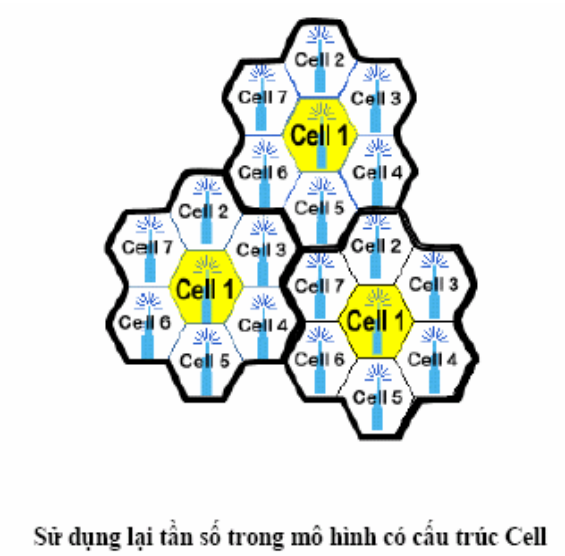
so với tín hiệu DS. Tuy nhiên tại ISM band theo quy định có mức giới hạn công xuất phát, do đó FH không thể được đạt S/N giống như DS. Bên cạnh đó việc dùng FH rất khó khăn trong việc đồng bộ giữa máy phát và thu vì cả thời gian và tần số đều yêu cầu cần phải được đồng bộ. Trong khi DS chỉ cần đồng bộ 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.

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

Theo chuẩn 802.11b, thì sử dụng 14 kênh DS (Direct Sequence) trong dải tần số 2,402GHz – 2,483GHz, mỗi kênh truyền rộng 22MHz, nhưng các kênh chỉ cách nhau 5MHz, vì vậy các kênh cạnh nhau sẽ gây giao thoa lẫn nhau, do đó trong một khu vực người ta bố chí các kênh truyền sao cho miền tần số của chúng không trồng lên nhau, trong hệ thống 14 kênh DS thì chỉ có 3 kênh đảm bảo không chồng lấn, ví dụ như 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 27: Bố trí số kênh phát trong một khu vực



Hình 28: Khả năng sử dụng lại tần số của phương pháp DSSS

Như vậy trong một vùng đơn tốc độ bit vận chuyển đến có thể lên tới: 11Mbps x 3 = 33Mbps, thay vì 11Mbps như khi chỉ có một kênh truyền được sử dụng trong một khu vực.

7. 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 2 hoặc nhiều hơn các điểm truy nhập không dây được kết nối đến 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 kỳ 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 xem một khách hàng không dây đang được chứng thực có biết về bí mật chung không. Điều này tương tự với khoá chứng thực đã được chia sẻ trước trong Bảo mật IP (IPSec). Chuẩn 802.11 hiện nay giả thiết rằng Khoá dùng chung được phân phối đến các tất cả các khách hàng đầu cuối thông qua một kênh bảo mật riêng, độc lập với tất cả các kênh khác của 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 đến 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 pham 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 được gửi giữa các node không dây. Mã hoá WEP dùng luồng mật mã đối xứng RC4 với từ khoá dài 40 bit hoặc104 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)

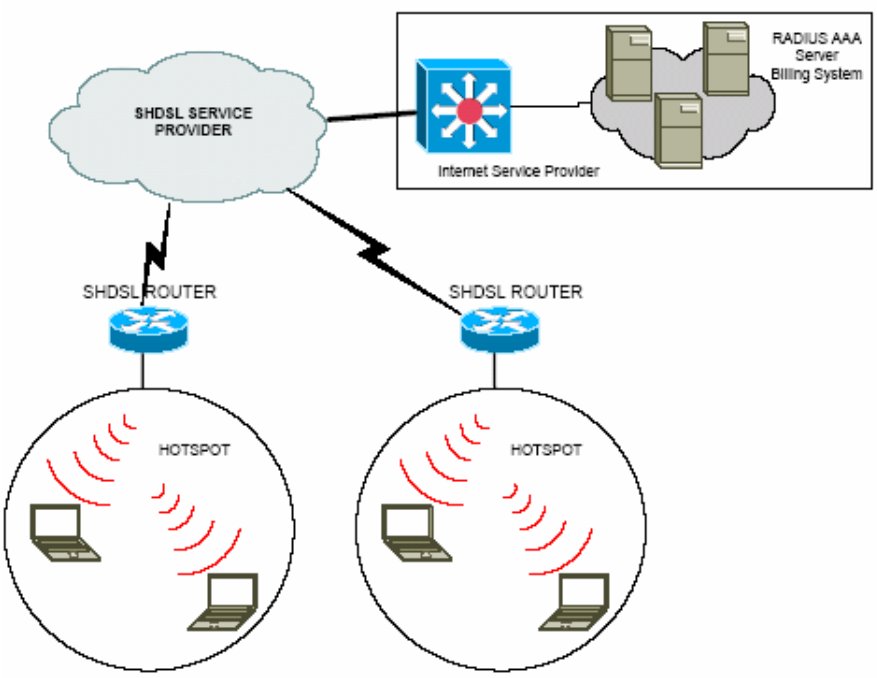
Đây là một trong những hình thức chứng thực động, khoá chứng thực được thay đổi giá trị một cách ngẫu nhiên ở mỗi lần chứng thực hoặc tại các khoảng có chu kỳ trong thời gian thực hiện một kết nối đã được chứng thực. Ngoài ra, EAP còn xác định chứng thực qua RADIUS có nghĩa là: khi một CPE muốn kết nối 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.

III/ PHƯƠNG ÁN TRUYỀN DẪN ĐẾN ĐIỂM ĐẶT HOTSPOT DÙNG XDSL-WAN

1. Phương án truyền dẫn:

Các điểm hotspot sẽ được kết nối tập trung về trung tâm quản lý mạng dưới sự điều khiển của Subsscriber Gateway chung để ra Internet. Phương thức truyền dẫn được lựa chọn đối với mô hình này sẽ là dich vụ xDSL WAN. Dựa trên chuẩn công nghiệp toàn cầu ITU, giải pháp SHDSL sử dụng truyền dữ liệu cân bằng với tốc độ có thể đạt từ 192 Kbps tới 2.3Mbps trên một đôi cáp đơn. Thêm vào đó, tín hiệu SHDSL có khả năng truyền dẫn xa hơn so với các kết nối sử dụng công nghệ ADSL và SDSL, cho phép các nhà cung cấp dịch vụ thoả mãn nhu cầu các khách hàng ở xa. Sử dụng công nghệ này, tại mỗi điểm truy cập hotspot phải có một SHDSL router. Cũng giống như ADSL Router, SHDSL

Router cũng được tích hợp DHCP và NAT server bên trong. Công nghệ này khiến cho chi phí đầu tư được giảm đi đáng kể do không phải đầu tư thêm hai server ngoài phục vụ DHCP và NAT.



Hình 29: Phương án truyền dẫn

IV/ MÔ HÌNH ĐẤU NỐI CHO CÁC HOTSPOT

1. Các kỹ thuật trong mô hình Wireless hotspot:

• **Đối với hệ thống Wi-Fi**: môi trường truyền dẫn là môi trường sóng, truyền tin theo các chuẩn 802.11a, 802.11b… Thực chất đây có thể coi là môi trường broadcast, tất cả các máy client đứng vào vùng phủ sóng đều có thể bắt được tín hiệu, các AP ít có khả năng điều khiển được truy nhập. Các Acces Point hiện nay bắt đầu được phát triển hỗ trợ chuẩn bảo mật thông tin trong môi trường Wireless là EAP (các hãng sản xuất thiết bị đưa ra các chuẩn EAP khác nhau như Cisco LEAP, Microsoft PEAP, Funk PEAP…). Với 802.1x các AP đã có khả năng xác thực client, và acconting nhưng hiện đang còn rất nhiều hạn chế như: các client phải có phần mềm điều khiển thích hợp, AP không có khả năng điều khiển truy nhập như Access Server trong môi trường Dial-up, AP có hỗ trợ RADIUS nhưng do có những thông số kỹ thuật mới nên chưa cho phép có khả

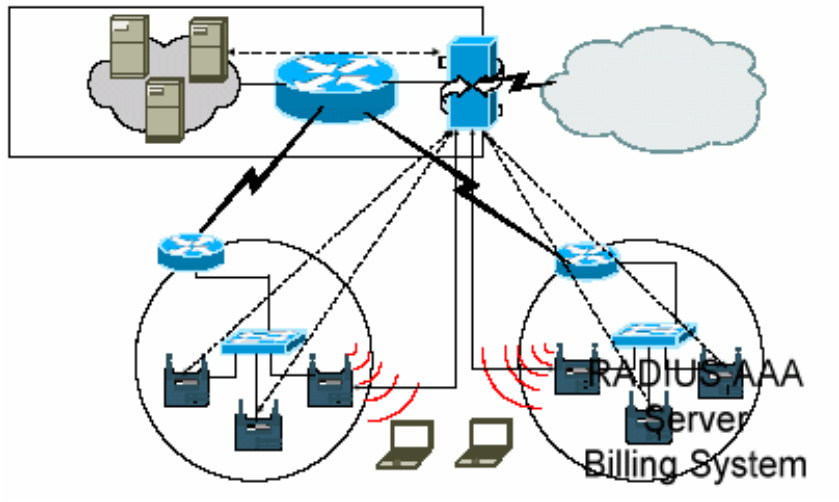
năng sử dụng các hệ thống database tập trung như ORACLE… do đó không có khả năng cung cấp dịch vụ trên AP như Access Server trong môi trường Dialup.

Giải pháp được đưa ra là sử dụng thiết bị Subscriber Gateway: Subscriber Gateway sẽ đứng chặn tại đường ra của các AP đi Internet, môi trường sóng sẽ luôn được các AP cung cấp cho bất cứ một máy trạm nào đứng trong môi trường truyền sóng. Nhưng khi người sử dụng truy nhập vào môi trường sóng của một Access point (AP) thì ngay lập tức Subscriber Gateway sẽ tiến hành việc xác thực thuê bao. Người sử dụng sẽ được điều khiển tự động truy nhập vào một trang Web xác thực đã được xây dựng tích hợp trên các Subcriber Gateway. Tại đây, username/password sẽ được nhập vào. Subscriber Gateway liên lạc với AAA Server tập trung tại trung tâm quản lý điều hành mạng theo giao thức RADIUS để lấy thông tin về khách hàng trong hệ thống cơ sở dữ liệu. Nếu xác thực thành công thì người sử dụng mới được phép thông qua Subscriber Gateway đi ra Internet, và thông tin tính cước sẽ được Subscriber Gateway gửi về AAA Server. Subscriber Gateway còn có khả năng điều khiển truy nhập theo thời gian thực, linh động, cho phép cung cấp các loại dịch vụ đa dạng.

2. Mô hình triển khai của Subscriber Gateway:

Yêu cầu của Subcriber Gateway là nó phải được đặt tại đường ra duy nhất của những hệ thống mà nó quản lý, nhờ đó nó mới có thể điều khiển được việc truy nhập thông tin của khách hàng. Phương án trong điều kiện hiện nay là dùng Subcriber Gateway tập trung tại trung tâm mạng.

- Đặc điểm: Trong mô hình này tất cả các điểm truy nhập (hotspot) phải kết nối tập trung về trung tâm mạng, sau đó đi qua hệ thống Subcriber Gateway để đi ra Internet. Hệ thống mạng giữa các điểm truy nhập với trung tâm mạng phải là mạng riêng không liên quan tới Internet, đường ra Internet duy nhất là qua hệ thống Subcriber Gateway.



Hình 30: Mô hình triển khai Gateway

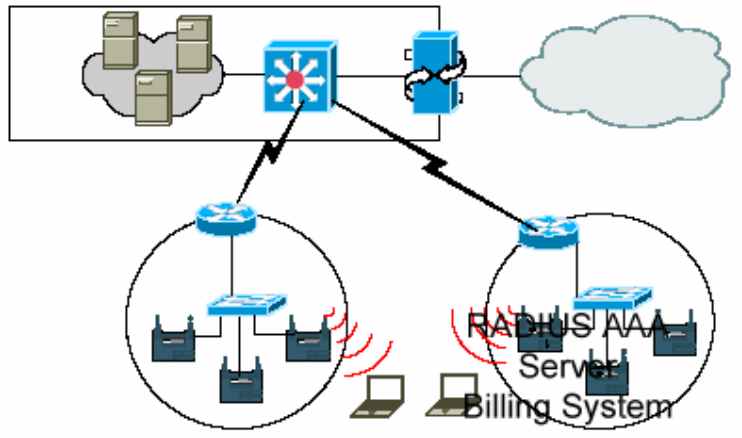
- Ưu điểm: **Quản lý tập trung**, trao đổi thông tin AAA giữa Subcriber Gateway và AAA Server chỉ là trao đổi thông tin trong mạng nội bộ

Đường kết nối Internet tập trung dễ quản lý.

- Nhược điểm: Tất cả lưu lượng đều phải đi qua WAN về Subcriber Gateway tại trung tâm mạng cho dù thuê bao là không hợp lệ, và không được phép đi Internet, các lưu lượng này sẽ làm giảm hiệu suất mạng.

3. Mô hình đấu nối của các hotspot:

Triển khai theo mô hình tập trung, kỹ thuật truyền dẫn sử dụng để đấu nối là SHDSL.



Hình 31: Mô hình đấu nối các Hotspot

Trong mô hình này các điểm hotspot bao gồm các AP được kết nối về trung tâm bằng một SHDSL Router. Các chức năng DHCP và NAT sẽ được thực hiện trên các Router.

PHẦN II
BẢO MẬT MẠNG LAN KHÔNG DÂY

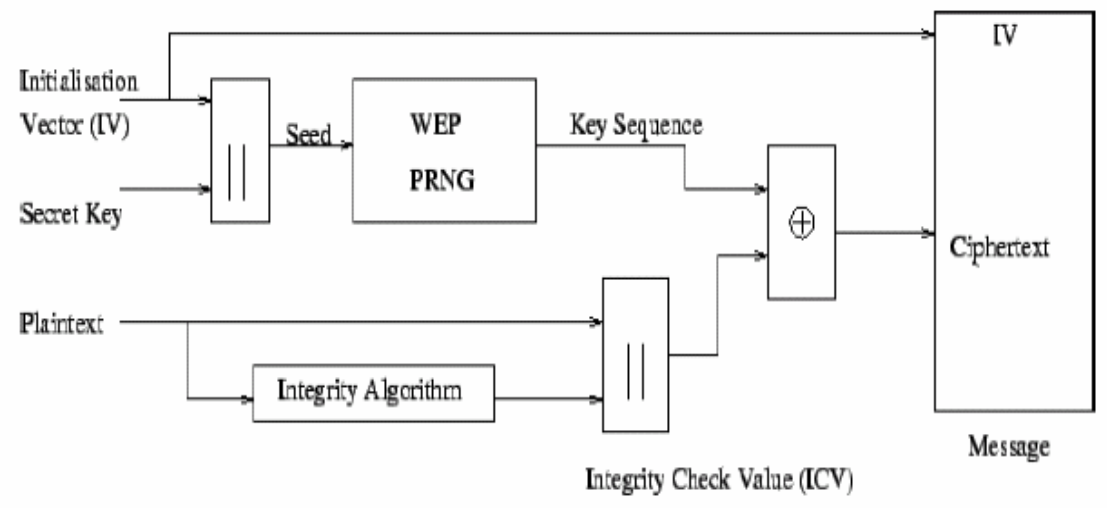
Wireless Lan vốn không phải là một mạng an toàn, tuy nhiên ngay cả với Wired Lan và Wan, nếu bạn không có biện pháp bảo mật thì nó cũng không an toàn. Chìa khóa để mở ra sự an toàn của WLAN và giữ cho nó được an toàn là sự thực hiện và quản lý nó. Đào tạo người quản trị một cách căn bản, trên những công nghệ tiên tiến là cách quan trọng để tạo 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 của 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 sẽ 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 vài khuyến nghị về các chính sách bảo mật cho WLAN.

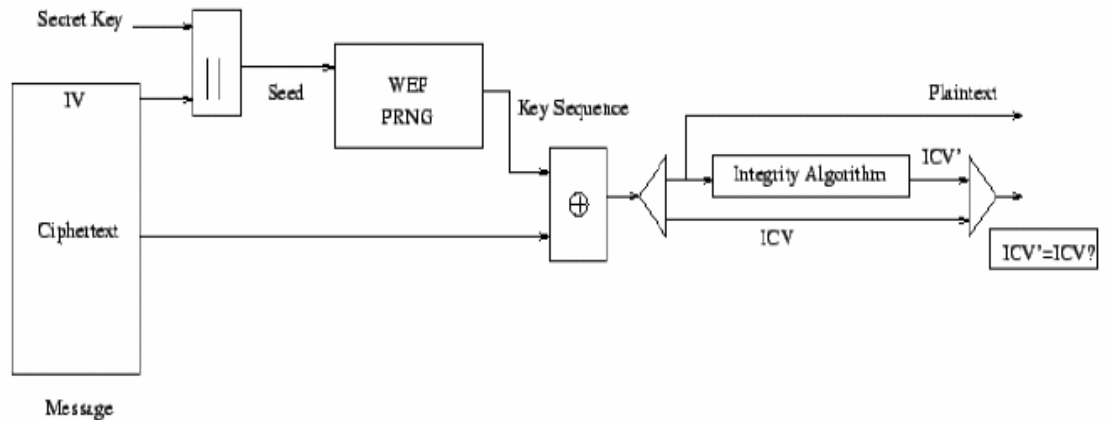
I/ WEP, WIRED EQUIVALENT PRIVACY

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 mã 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 bay giờ mã nguồn là 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 32: Sơ đồ quá trình mã hóa sử dụng WEP



Hình 33: Sơ đồ quá trình giải mã WEP

ICV giá trị kiểm tra tính toàn vẹn

Thuật toán RC4 không thực sự thích hợp cho WEP, nó không đủ để làm phương pháp bảo mật duy nhất cho mạng 802.11. Cả hai loại 64 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 dược 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 có thể 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 lừa điểm truy nhập.
- *Tấn công nhờ vào từ điển tấn công được xây dựng*: Sau khi thu thập đủ thông tin, chìa khóa WEP co thể bị crack bằng 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

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 để 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 802.1X với EAP hoặc VPN.

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 hai mục đích cho WLAN *(xem kỹ hơn trong phần phụ lục về vai trò của chìa khóa WEP, trong vấn đề chứng thực mở và chứng thực khóa chia sẻ):*

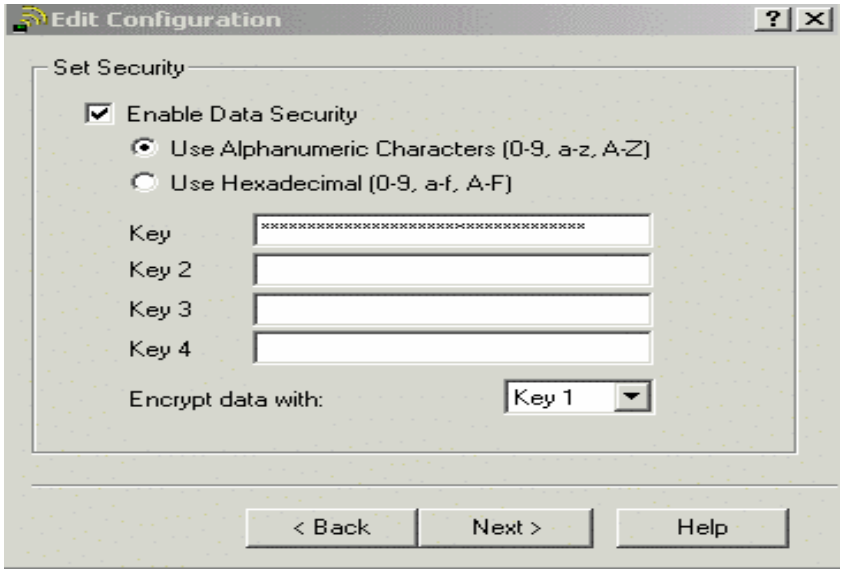
- Chìa khóa WEP được sử dụng để xác định sự cho phép của một Station

- 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 với 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 bố 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, hack.

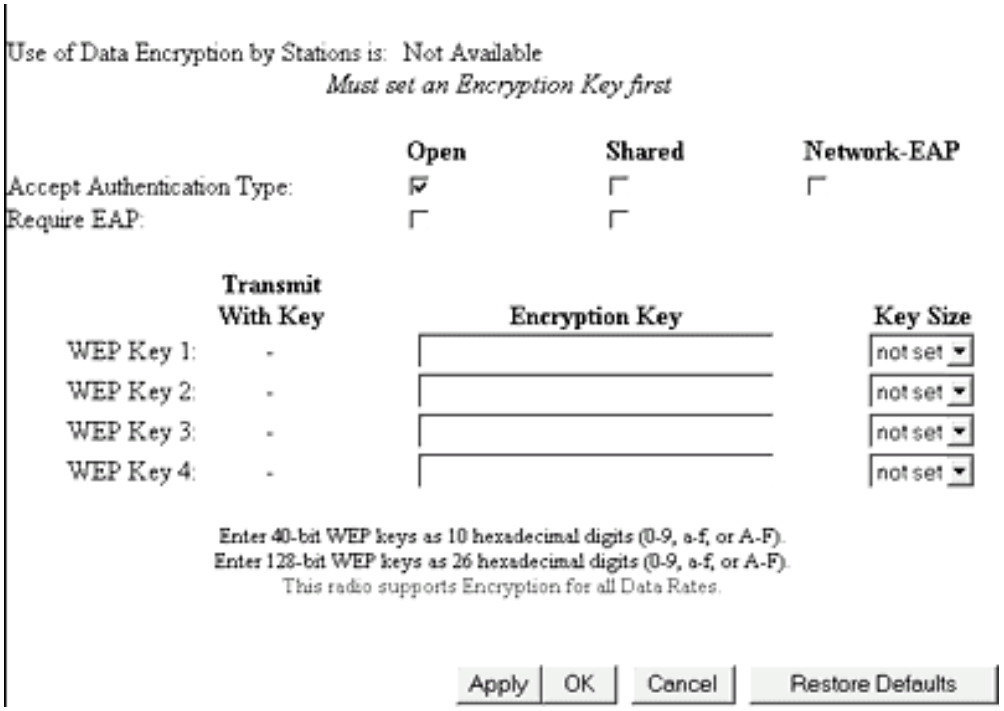
WEP key tồn tại hai loại, 64 bit và 128 bit, mà đôi khi bạn thấy viết là 40 bit và 104 bit. Lý do này là do cả hai loại WEP key đều sử dụng chung một vector khởi tạo, Initialization Vector (IV) 24 bit và một từ khóa bí mật 40 bit hoặc 104 bit. Việc nhập WEP key vào client hoặc các thiết bị phụ thuộc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



Hình 34: Giao diện nhập chìa khóa Wep

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, nếu một WEP key bị mất, thì chỉ phải thay đổi 25 Station và một đến hai AP thay vì toàn bộ mạng.

Một lí do nữa cho việc dùng nhiều WEP key, là nếu 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.



Hình 35: Sự hỗ trợ sử dụng nhiều chìa khóa WEP

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 hơn. 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.

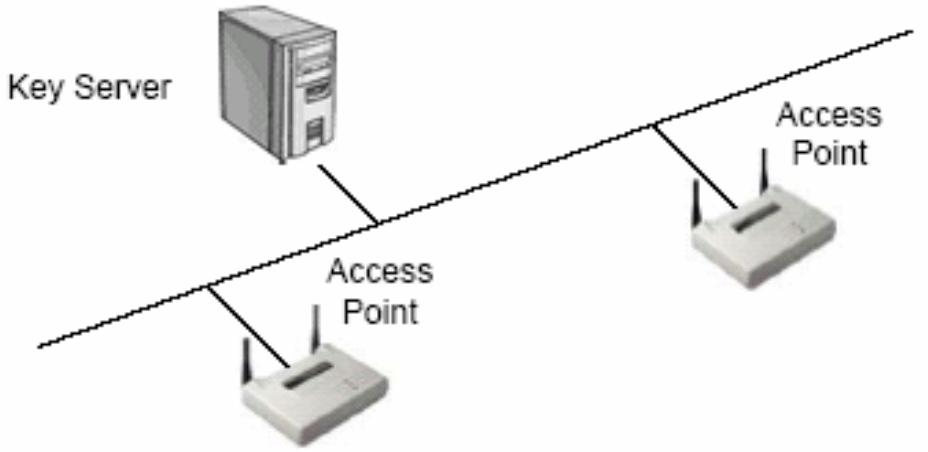
3. SERVER quản lý chìa khóa mã hóa tập trung

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 bố chìa khóa một cách tập trung

- Thay đổi chìa khóa luân 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 36: Cấu hình 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.

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 sử dụng 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 giải pháp này là giá thành của AP tăng lên hơn so với AP thông thường.

WEP có thể được thực hiện như một phương pháp bảo mật căn bản, nhưng các nhà quản trị mạng nên nắm bắt được những điểm yếu của WEP và cách khắc phục chúng. Các Admin cũng nên hiểu rằng, 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 Rijndale (RINE-dale) với những loại chìa khóa sau:

- 128 bit
- 192 bit
- 256 bit

AES được xét là một phương pháp không thể crack bởi hầu hết người viết mật mã, và NIST (National Institute of Standards and Technology) đã chọn AES cho FIPS (Federal Information Processing Standard). Như một phần cải tiến cho chuẩn 802.11, 802.11i được xem xét để sử dụng AES trong WEP 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 trình cơ sở trong AP và trong Client (Card vô tuyến PCMCIA) sẽ phải được nâng cấp để hỗ trợ AES. Phần mềm trạm khách (các driver và các tiện ích máy khách) sẽ hỗ trợ cấu hình AES cùng với chìa khóa bí mật.

II/ LỌC

Lọc (Filtering) là một cơ chế bảo mật căn bản mà 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 trên WLAN

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

Đoạn này sẽ miêu tả mỗi loại này là gì, nó có thể làm gì cho người quản trị và phải cấu hình nó như thế nào.

1. Lọc SSID

Lọc SSID (SSID Filtering) là một phương pháp lọc sơ đẳng, và nên 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, infracstructure 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 ra, 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 đặt cấu hình driver.

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

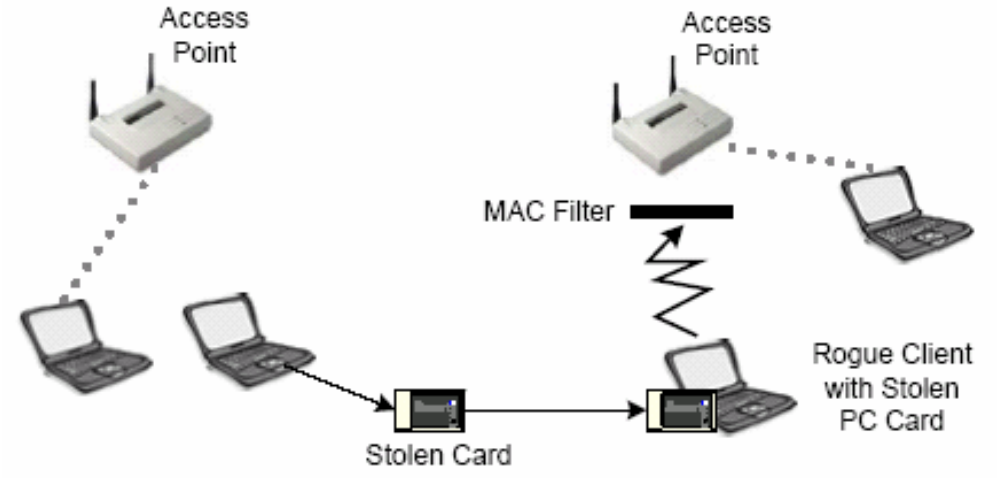
- ***Sử dụng SSID mặc định*:** Sự thiết lập này là một cách khác để đưa ra thông tin về WLAN của bạn. Nó đủ đơn giản để sử dụng một bộ phân tích mạng để lấy địa chỉ MAC khởi nguồn từ AP, và sau đó xem MAC trong

bảng OUI của IEEE, bảng này liệt kê các tiền tố địa chỉ MAC khác nhau mà 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 cty 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 nên được sử dụng như một phương tiện để phân đoạn mạng chứ không phải để bảo mật, vì thế hãy: ***luôn coi SSID chỉ như một cái tên mạng.***
- ***Không cần thiết quảng bá các SSID:*** Nếu AP của 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 bạn.

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 trong danh sách địa chỉ MAC của AP, nó sẽ không thể đến được điểm truy nhập đó. Hình vẽ:



Hình 37: Lọc địa chỉ MAC

Tất nhiên, lập trình các địa chỉ MAC của các Client trong mạng WLAN vào các AP trên một mạng rộng thì không thực tế. Bộ lọc MAC có thể được thực hiện trên vài 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, mà có thể phải được nhập bằng bất cứ cách nào, là một giải pháp tốt. RADIUS Server thường trỏ đến các nguồn chứng thực khác, vì vậy các nguồn chứng thực khác phải được hỗ trợ bộ lọc MAC.

Bộ lọc MAC có thể làm việc tốt trong chế độ ngược lại. Xét một ví dụ, một người làm thuê bỏ việc và mang theo cả Card Lan không dây của họ. Card Wlan này nắm giữ cả chìa khóa WEP và bộ lọc MAC vì thế không thể để họ còn được quyền sử dụng. Khi đó 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 còn dễ bị ảnh hưởng bởi những thâm nhập sau:

- Sự ăn trộm một Card PC trong có một bộ lọc MAC của AP
- 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 có một số lượng nhỏ các trạm khách, thì việc dùng bộ lọc MAC là một giải pháp bảo mật hiệu qủa. Vì không một hacker thông minh nào lại tốn hàng giờ để truy nhập vào một mạng có giá trị sử dụng thấp.

3. Circumventing MAC Filters

Địa chỉ MAC của Client WLAN thường được phát quảng bá bởi các AP và Bridge, ngay cả khi sử dụng WEP. Vì thế một hacker mà có thể nghe được lưu lượng trên mạng của bạn có thể nhanh chóng tìm thấy hầu hết các địa chỉ MAC mà được cho phép trên mạng không dây của bạn. Để một bộ phân tích mạng thấy được địa chỉ MAC của một trạm, trạm đó phải truyền một khung qua đoạn mạng không dây, đây chính là cơ sở 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 thông qua phần mềm hoặc thậm chí qua cách thay đổi cấu hình hệ thống. Một hacker có 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.

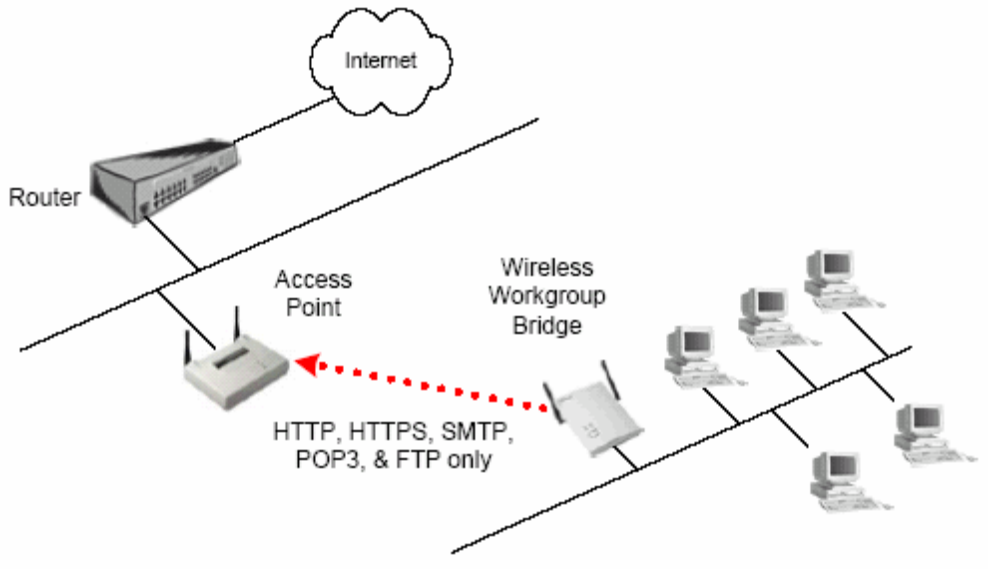
Do hai trạm với cùng địa chỉ MAC không thể đồng thời tồn tại trên một WLAN, hacker phải tìm một địa chỉ MAC của một trạm mà hiện thời không trên mạng. Chính trong thời gian trạm di động hoặc máy tính sách tay không có trên mạng là thời gian mà hacker có thể truy nhập vào mạng tốt nhất.

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

4. 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 mà kết nối lại tới AP của tòa nhà kỹ thuật trung tâm. Vì tất cả những người sử dụng trong remote building chia sẻ băng thông 5Mbs giữa những tòa nhà này, nên một số lượng đáng kể các điều khiển trên các sử dụng này phải được thực hiện. Nếu các kết nối này được cài đặt với mục đích đặc biệt của sự truy nhập internet của người sử dụng, thì bộ lọc giao thức sẽ loại trừ tất cả các giao thức, ngoại trừ SMTP, POP3, HTTP, HTTPS, FTP. . .



Hình 38: Lọc giao thức

III/ NHỮNG SỰ TẤN CÔNG TRÊN WLAN

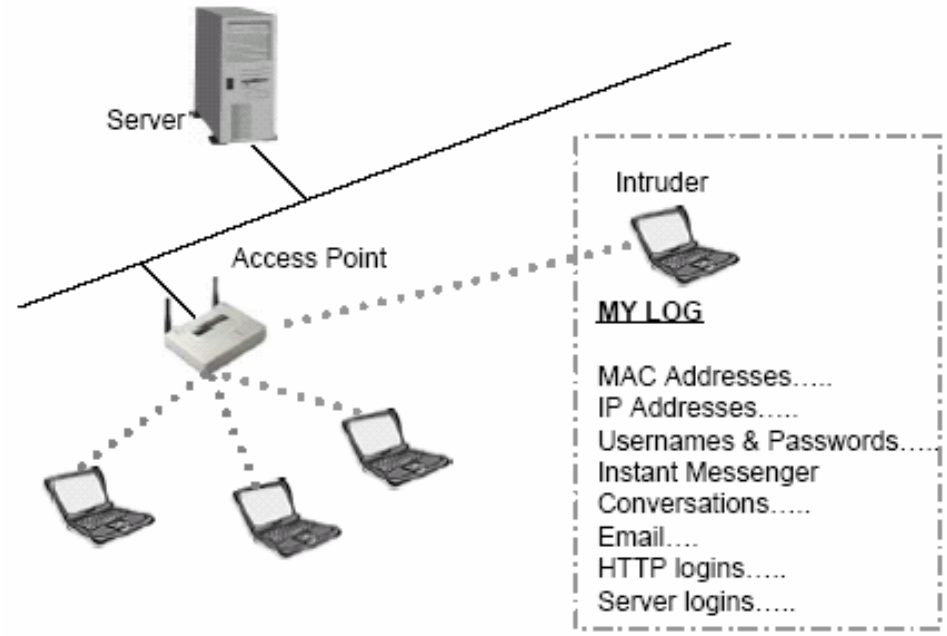
Một sự tấn công cố ý có thể gây vô hiệu hóa hoặc có thể tìm cách truy nhập WLAN trái phép theo một vài cách.

- **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 kê một vài kiểu tấn công, trong đó một vài kiểu có thể thực hiện được theo nhiều cách khác nhau.

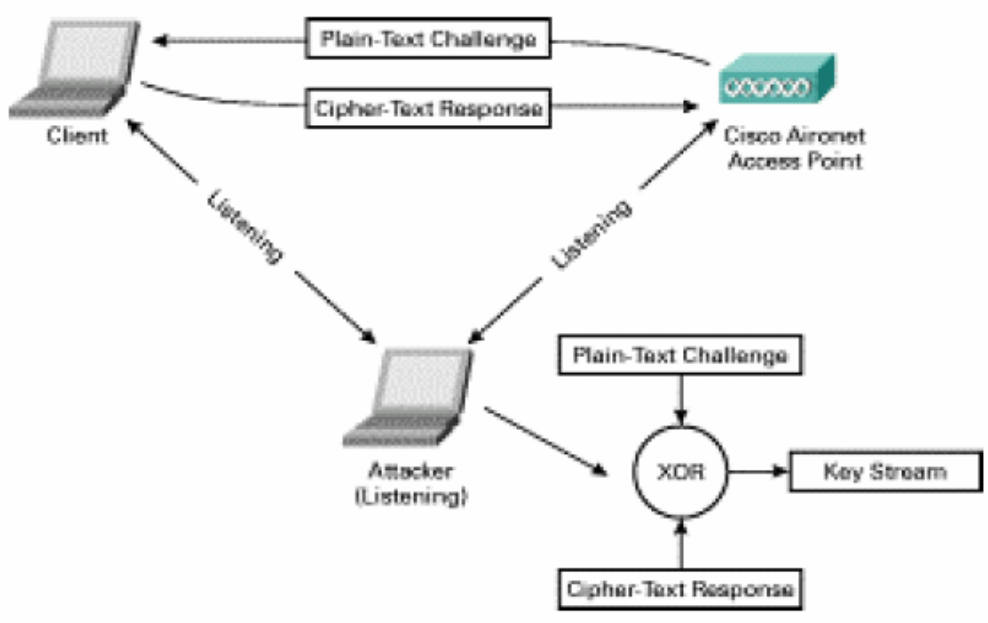
1. Tấn công bị động

Nghe trộm có lẽ là phương pháp đơn giản nhất, tuy nhiên nó vẫn có hiệu quả đối với WLAN. Tấn công bị động như một cuộc nghe trộm, mà không phát hiện được sự có mặt của người nghe trộm (hacker) trên hoặc gần mạng khi hacker không thực sự kết nối tới AP để lắng nghe các gói tin truyền qua phân đoạn mạng không dây. 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 hướng tính



Hình 39: 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.



Hình 40: Quá trình lấy chìa khóa WEP

Có những ứng dụng có khả năng lấy pass từ các Site HTTP, email, các instant messenger, các phiên FTP, các phiên telnet mà được gửi dưới dạng text không được mã hóa. Có những ứng dụng khác có thể lấy pass trên những phân đoạn mạng không dây giữa 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, nhưng người dùng là người phải trực tiếp chịu trách nhiệm, và gánh chịu mọi hậu quả, và có thể đi tới chỗ mất việc.

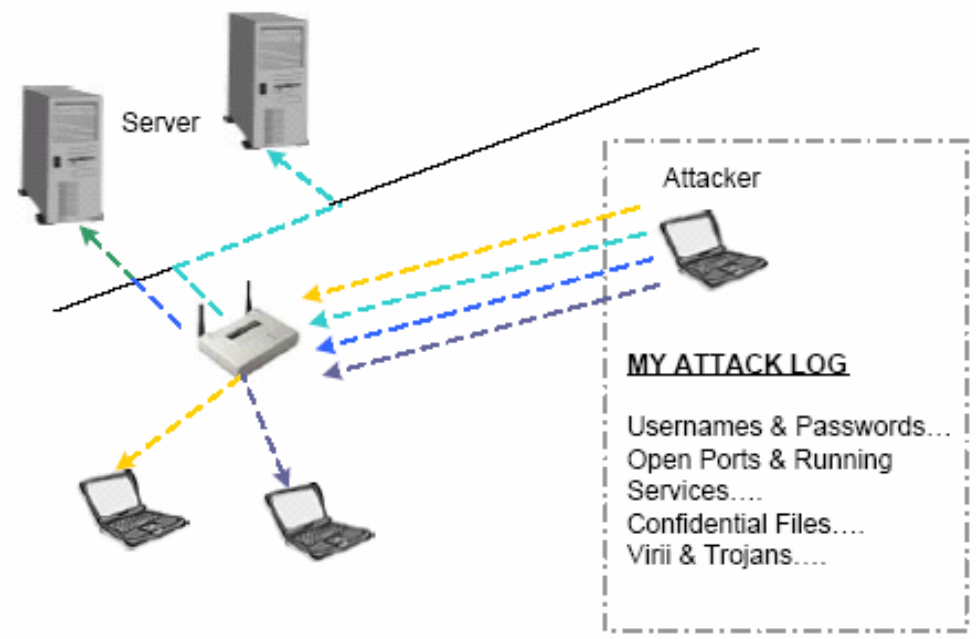
Xét một tình huống khác mà trong đó HTTP hoặc email password bị lấy trên những phân đoạn mạng không dây, và sau đó được hacker sử dụng với mục đích truy nhập tới WLAN đó.

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 tìm cách 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 đích 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 xâu hơn vào 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 để ý đến sự kiện này trong một thời gian. Hình dưới đây mô tả một kiểu tấn công chủ động trên WLAN



Hình 41: Tấn công chủ động

Một vài ví dụ của tấn công chủ động có thể như việc gửi bomb, 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.

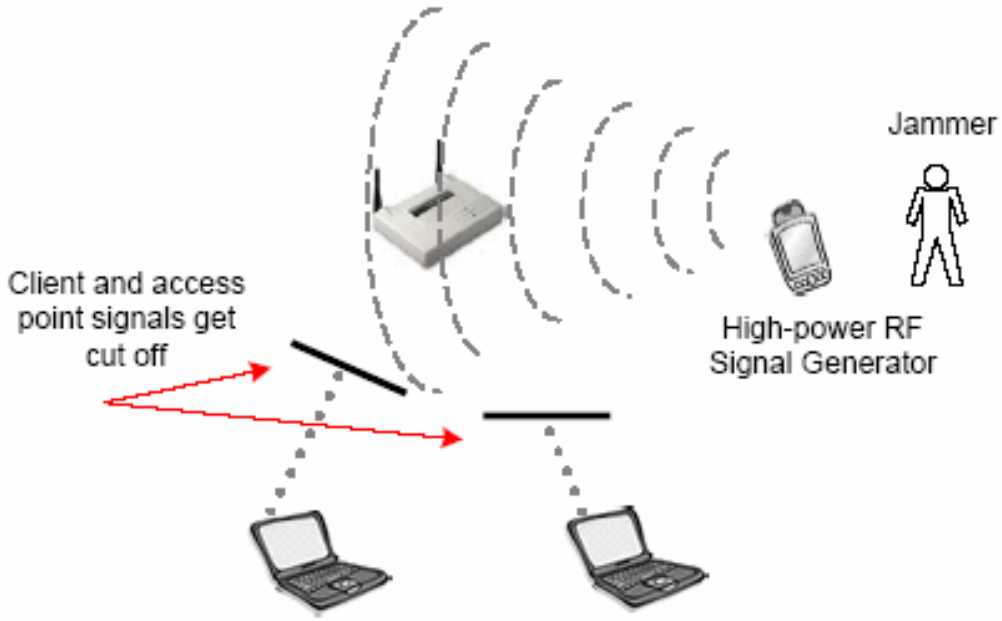
Khi hacker có kết nối không dây tới mạng của bạn thì anh ta cũng có thể truy cập vào mạng hữu tuyến trong văn phòng, vì hai sự kiện không khác nhau nhiều. Những kết nối không dây cho phép hacker về tốc độ, sự truy nhập tới server, kết nối tới mạng diện rộng, kết nối internet, tới desktop và laptop của 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 hủy 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. 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 hacker sẽ dùng một máy phát tín hiệu RF công suất cao hoặc máy tạo sóng quét.



Hình 42: Tấn công theo kiểu chèn ép

Để loại bỏ kiểu tấn công này, yêu cầu trước hết là tìm được nguồn phát tính 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 thi 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.

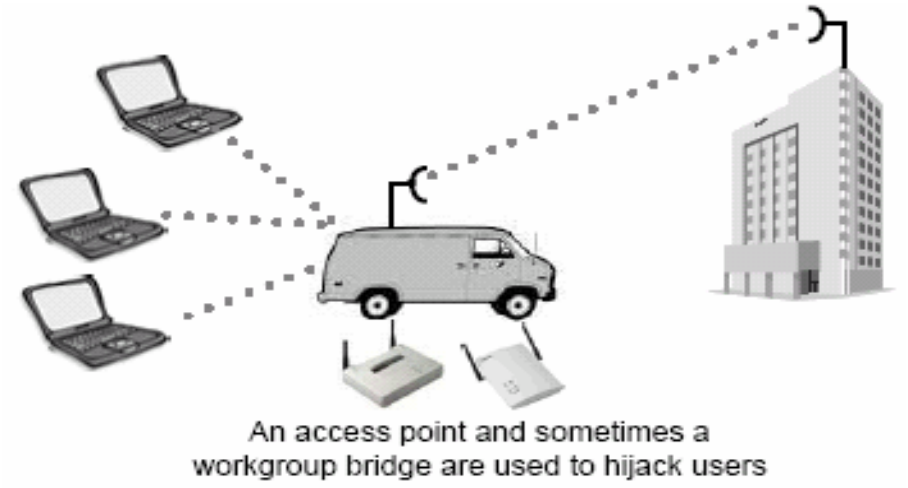
Khi Jamming gây ra bởi một nguồn cố định, không chủ ý, như một tháp truyền thông hoặc các hệ thống hợp pháp khác, thì người quản trị WLAN có thể phải xem xét đến việc sử dụng bộ thiết đặt các tần số khác nhau.

Ví dụ nếu một admin có trách nhiệm thiết kế và cài đặt một mạng RF trong một khu phòng rộng, phức tạp, thì người đó cần phải xem xét một cách kỹ càng theo thứ tự. Nếu nguồn giao thoa là một điện thoại, hoặc các thiết bị làm việc ở dải tần 2,4Ghz, 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.

Sự Jamming không chủ ý xảy ra với mọi thiết bị mà dùng chung dải tần 2,4Ghz. Jamming không phải là sự đe dọa nghiêm trọng vì jamming không thể được thực hiện phổ biến bởi hacker do vấn đề giá cả của thiết bị, nó quá đắt trong khi hacker chỉ tạm thời vô hiệu hóa được mạng..

4. Tấn công bằng cách thu hút

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

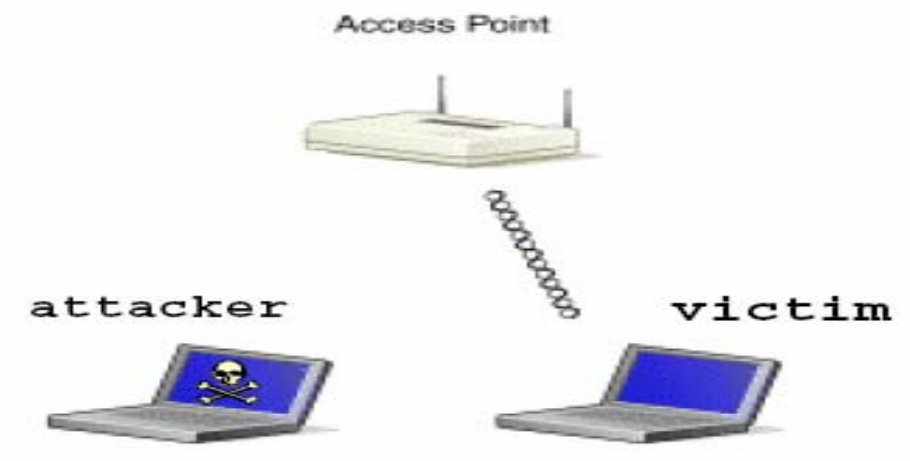


Hình 43: Man-in-the-middle attacks

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

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

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



Hình 44: Trước cuộc tấn công

Hình 45: Và sau cuộc tấn công

Một điều đặc biệt với kiểu tấn công này là người sử dụng không thể phát hiện ra được cuộc tấn công, và lượng thông tin mà 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.

IV/ CÁC GIẢI PHÁP BẢO MẬT ĐƯỢC ĐỀ 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, nên đây là cơ hội quan trọng để 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.

1. Quản lý chìa khóa WEP

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

Sự phân phối chìa khóa WEP cho mỗi phiên, mỗi gói sẽ gán một chìa khóa WEP mới cho cả Client và AP cho mỗi phiên hoặc mỗi gói được gửi giữa chúng. Trong khi khóa động thêm nhiều overhead và giảm bớt lưu lượng, chúng làm cho việc hack vào mạng thông qua những đoạn mạng không dây trở lên khó khăn hơn nhiều. Hacker có thể phải dự đoán chuỗi chìa khóa mà server phân phối chìa khóa 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 hóa 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 trong những gói unicast từ client.

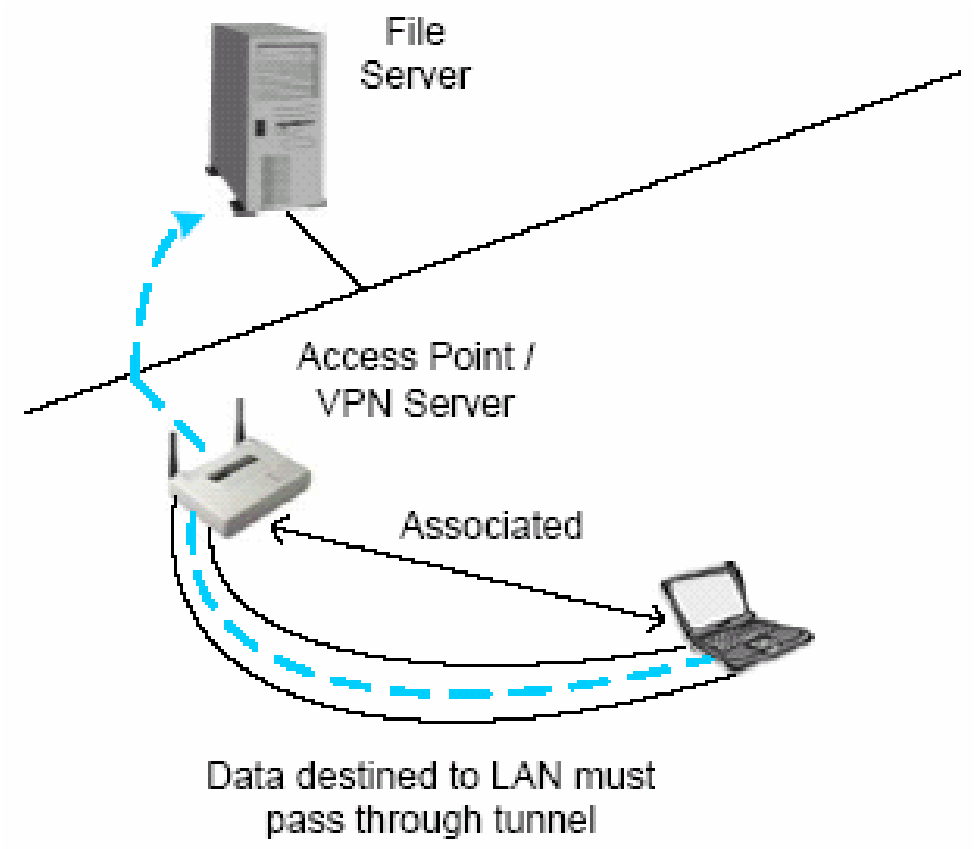
Để đặt một server quản lý chìa khóa mã hóa tập trung vào chỗ thích hợp, người quản trị WLAN phải tìm một ứng dụng mà thực hiện nhiệm vụ này, mua một server với một hệ điều hành thích hợp, và cấu hình ứng dụng theo nhu cầu. Quá trình này có thể tốn kém và cần nhiều thời giờ, phụ thuộc vào quy mô triển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

2. Wireless VPNs

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 client đi qua được AP. Tất cả lưu lượng được qua

thông qua đường hầm, và có thể được mã hóa để thêm một lớp an toàn. Hình sau đây mô tả một cấu hình mạng như vậy:



Hình 46: 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 hóa WEP. Sự sử dụng Ipsec với những bí mật dùng chung hoặc những sự cho phép là giải pháp chung của sự lựa chọn giữa những kỹ năng bảo mật trong phạm vi hoạt động này. Khi 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 đền ghị cải tiến cho những giải pháp VPN hiện thời của họ (phần cứng hoặc phần mềm) để hỗ trợ các client không dây và để cạnh tranh tên thị trường WLAN. Những thiết bị hoặc những ứng dụng này phục vụ trong cùng khả năng như gateway, giữa những đoạn 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

khóa 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. Kỹ thuật chìa khóa nhảy

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

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 sự kiểm tra tính toàn vẹn 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 khóa. TKIP bao gồm sự sử dụng các chìa khóa động để chống lại sự ăn cắp các chìa khóa 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 phần mềm và vi chương trình nâng cấp cho thiết bị client không dây. TKIP chỉ rõ các quy tắc sử dụng vector khởi tạo, các thủ tục tạo lại chìa khóa dựa trên 802.1x, sự trộn chìa khóa 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 lý.

5. Những giải pháp dựa trên AES

Những giải pháp dựa trên AES có thể thay thế WEP sử dụng RC4, nhưng chỉ là 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 hóa 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 khóa mã hóa

tập trung để tự động hóa quá trình trao đổi chìa khóa. Nếu một card vô tuyến của client bị mất, mà đã được nhúng chìa khóa mã hóa AES, nó không quan trọng với việc AES mạnh đến mức nào bởi vì thủ phạm vẫn có thể có được sự truy nhập tới mạng.

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 rất 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 phân bố hữu tuyến khỏi sự tấn công.

Một ví dụ một trường hợp tốt nhất để triển khai mô hình gateway như vậy có thể là hoàn cảnh sau: giả thiết một bệnh viện đã sử dụng 40 AP 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 bố (mà nối tới AP) và có thể đóng vai trò của server chứng thực, server VPN mà 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 tùy thuộc quy mô mạng) gateway có thể được cài đặt đàng 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.

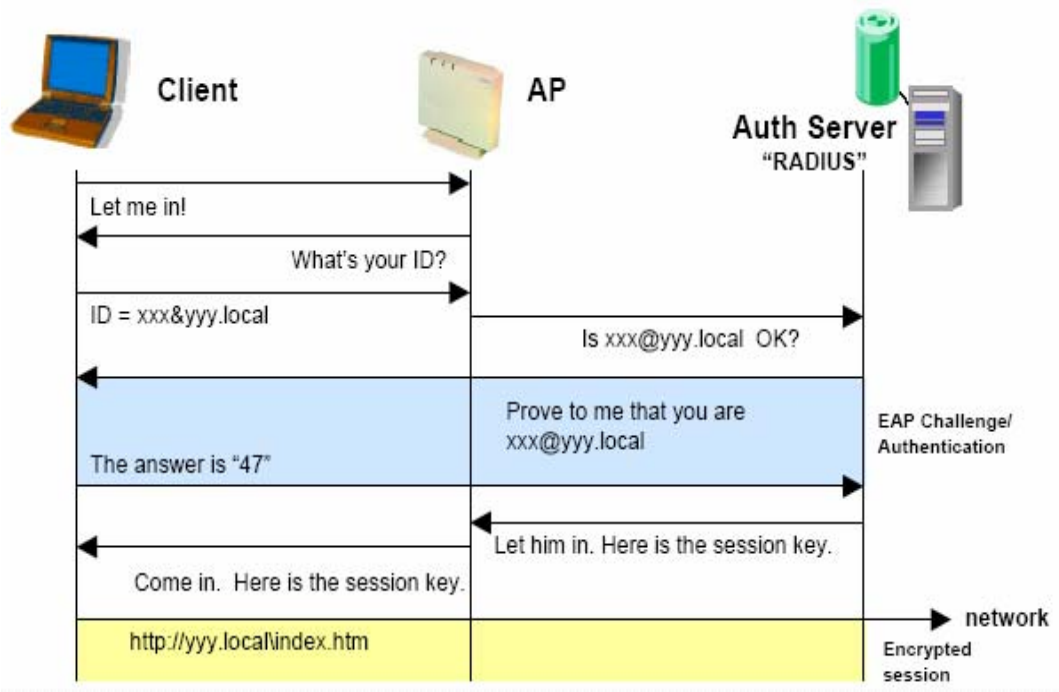
7. 802.1x và giao thức chứng thực mở

Chuẩn 802.1x cung cấp những chi tiết kỹ thuật cho sự điều khiển truy nhập thông qua những cổng cơ bản. Sự điều khiển truy nhập thông qua những cổng 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 khóa 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 khóa tự động và hỗ trợ sự chứng thực lẫn nhau. Có lẽ hiện thời có cả tá loại EAP trên thị trường, một khi cả những người sử dụng công nghệ và IEEE đều không đồng ý bất kỳ một loại riêng lẻ nào, hoặc một danh sách nhỏ các loại, để từ đó tạo ra một chuẩn.

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



Hình 47: Quá trình chứng thực 802.1x-EAP

1. Client yêu cầu liên kết tới AP
2. AP đáp lại yêu cầu liên kết với một yêu cầu nhận dạng EAP
3. Client gửi đáp lại yêu cầu nhận dạng EAP cho AP

4. Thông tin đáp lại yêu cầu nhận dạng EAP của client được chuyển tới Server chứng thực
5. Server chứng thực gửi một yêu cầu cho phép tới AP
6. AP chuyển yêu cầu cho phép tới client
7. Client gửi trả lời sự cấp phép EAP tới AP
8. AP chuyển sự trả lời đó tới Server chứng thực
9. Server chứng thực gửi một thông báo thành công EAP tới AP
10. AP chuyển thông báo thành công tới client và đặt cổng của client trong chế độ forward.

V/ CHÍNH SÁCH BẢO MẬT

Một công ty mà sử dụng WLAN nên có một chính 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 cty, 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 lý, sự sử dụng các giải 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 nhiêm 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.

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.

2. Sự an toàn vật lý

Mặc dù bảo mật vật lý khi sử dụng mạng hữu tuyến truyền thống 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 bấy 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 các 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 lý chặt 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 đền 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 phần cứng 802.11 và cảnh giác các nhân viên trong công ty luôn luôn quan sát những người không ở trong công ty đang 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. 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 trường 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 rất tốt để bảo mật mạng WLAN.

4. Sử dụng các giải 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 nhập đó xuất hiện.

Bởi chỉ có số ít được đào tạo về bảo mật WLAN, do đó những người này là rất 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 được lập tài liệu chi tiết.

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 virus trên laptop của họ. Đa số các mạng WLAN công cộng có 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.

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

VI/ 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.

1. Wep

Không được chỉ tin cậy vào WEP, không có một biện pháp nào hoàn 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 đến SSID hoặc tên của tổ chức làm cho 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 qủa 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.

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 tìm những nơi mà tốn ít thời gian và năng lượng nhất để tìm cách truy cập mạng. Vì lí do này, rất quan trọng khi 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 khôngphải là dễ bị ảnh hưởng bởi 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, nhưng 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 lựa 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. Sự chứng thực người dùng

Sự 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 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. Giả 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 qủa với người quản trị Radius đang tồn tại.

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 bay giờ và mai sau. WLAN đang nhanh chóng phổ biến như vậy vì sự thực hiện dễ dàng. Một WLAN bắt đầu với 1 AP và 5 client có thể nhanh chóng lên tới 15 AP và 300 client. Do đó cùng một cơ chế an toàn làm việc cho một AP là điều hoàn toàn không thể chấp nhận được cho 300 Ap, như thế sẽ làm tăng 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 giải pháp trên WLAN, thì các thiết bị này xét về lâu dài, là một nhân tố quan trọng để giảm chi phí.

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, và 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 hiên.

6. Theo dõi các phần cứng trái phép

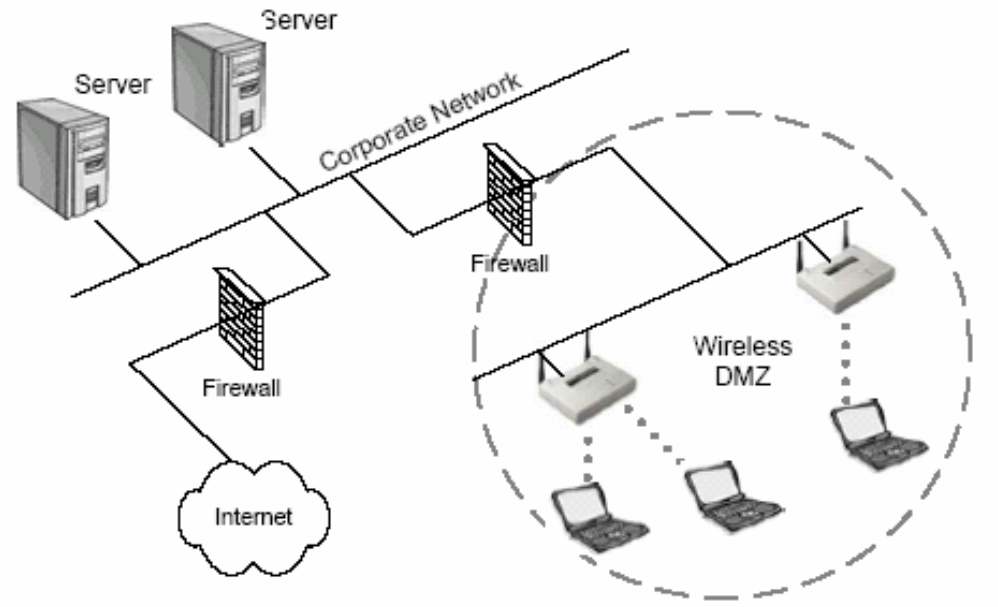
Để phát hiện ra các AP trái phép, các phiên dò các AP đó cần được hoạch định cụ thể nhưng không được công bố. Tích cực tìm và xóa bỏ các AP trái phép sẽ giữ ổn định cấu hình AP và làm tăng tính an toàn. Việc này có thể được thực hiện trong khi theo dõi mạng một cách bình thường và hợp lệ. Kiểu theo dõi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

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.

8. Wireless DMZ

Ý tưởng khác trong việc thực hiện bảo mật cho những segment không dây là thiết lập một vùng riêng cho mạng không dây, Wireless DeMilitarized Zone (WDMZ). Tạo vùng WDMZ sử dụng firewalls hoặc router thì có thể rất tốn kém, phụ thuộc vào quy mô, mức độ thực hiện. WDMZ nói chung được thực hiện với những môi trường WLAN rộng lớn. Bởi các AP về cơ bản là các thiết bị không bảo đảm và không an toàn, nên cần phải tách ra khỏi các đoạn mạng khác bằng thiết bị firewall.



Hình 48: Wireless DeMilitarized Zone

9. 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 card không dây của bạn. Thường thì các đặc tính an toàn, các vấn đề cơ bản sẽ được cố định, bổ sung thêm những đặc tính mới, sự khắc phục các lỗ hổng trong các cập nhật này.

PHỤ LỤC

CÁC THUẬT NGỮ ĐƯỢC SỬ DỤNG

AAA	**Authentication, Authorization, Accountting**
ACK	**Acknowlegment**
ADSL	**Asymmetric Digital Subscriber Line**
AES	**Advanced encryption standard**
AES	**Advanced Encryption Standard**
AP	**Access point**
ASK	**Amplitude shift keying**
CCK	**Complementary Code Keying**
CDMA	**Code Divison Multiple Access**
CPE	**Customer Premises Equipment**
CSMA/CA	**Carrier Sense Multiple Access /Collision Avoidance**
CTS	**Clear To Send**
DCS	**Dynamic Channel Selection**
DHCP	**Dynamic Host Configuration Protocol**
DSSS	**Direct Sequence Spread Strectrum**
EAP	**Extensible Authentication Protocol**
EAP	**Extensible Authentication Protocol**
ESS	**Extended Service Set**
FDD	**Frequency Division Duplexing**
FDMA	**Frequency Division Multiple Access**
FHSS	**Frequency Hopping Spread Spectrum**
FIPS	**Federal Information Processing Standard**
FSK	**Frequency Shift keying**
ICV	**Integrity Check Value**
IDS	**Intrusion Detection System**
IEEE	**Institute of Electrical and Electronics Engineers**
IMS	**Industrial, Scientific and Medical**
IV	**Initialization Vector**
MAC	**Media Access Control**

NIST	**National Institute of Standards and Technology**
OFDM	**Orthogonal Frequency Division Multiplexing**
PCMCIA	**Personal Computer Memory Card International Association**
PDA	**Personal digital assistant**
PRNG	**Pseudo Random Number Generator**
PSK	**Phase Shifp Keying**
QoS	**Quality of Service**
QPSK	**Quardrature Phase Shift Keying**
RADIUS	**Remote Authentication Dial _ In User Service**
RTS	**Request To Send**
SSIDs	**Service Set Identifiers**
TDD	**Time Division Duplexing**
TDMA	**Time Division Multiple Access**
TKIP	**Temporal Key Integrity Protocol**
VPN	**Virtual Private Network**
WDMZ	**Wireless DeMilitarized Zone**
WECA	**Wireless Ethernet Compatibility Alliance uh**
WEP	**Wired Equivalent Privacy**
WEP	**Wired Equivalent Privacy**
Wi-fi	**Wireless fidelity**

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

Beacons:

Viết đầy đủ là Beacon management frame, là các khung ngắn mà 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, thì chúng sẽ đồng bộ đồng hồ của mình với đồng hồ của 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, thì là các thông số về thời giản nhảy và ngừng. Còn với DSSS, bản tin dẫn đường chứa các thông tin về kênh truyền.

Thông tin về SSID:

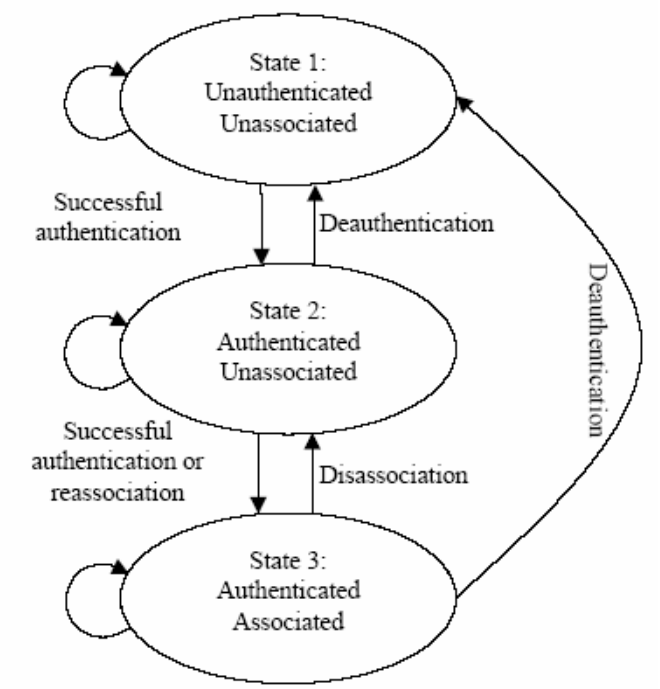
Các trạm tìm trong bản tin dẫn đường thông tin SSID của mạng mà chúng muốn truy cập. Khi các thông tin này được tìm thấy, các trạm xem địa chỉ MAC của nơi xuất phát bản tin dẫn đường và gửi yêu cầu chứng thực để liên kết với điểm truy nhập. Nếu một trạm được thiết lập để chấp nhận bất cứ SSID nào, trạm 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)

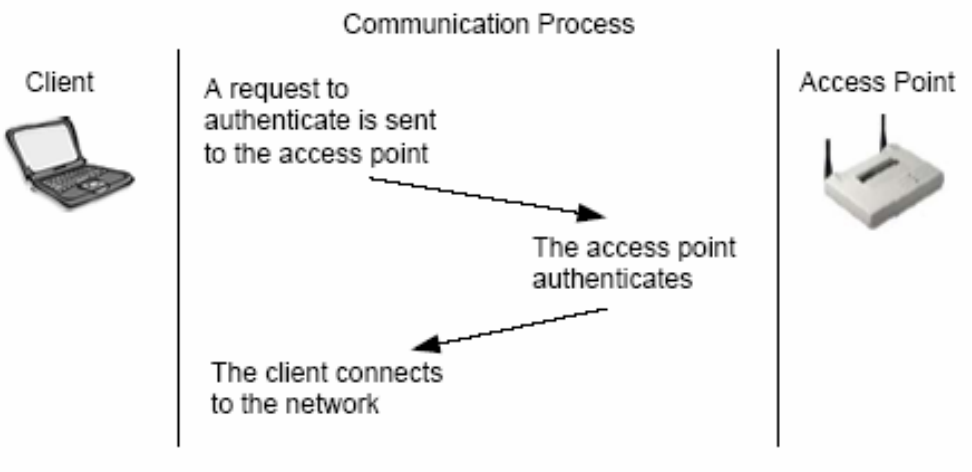
Xảy ra theo sơ đồ sau:



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



Phương pháp này thì 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

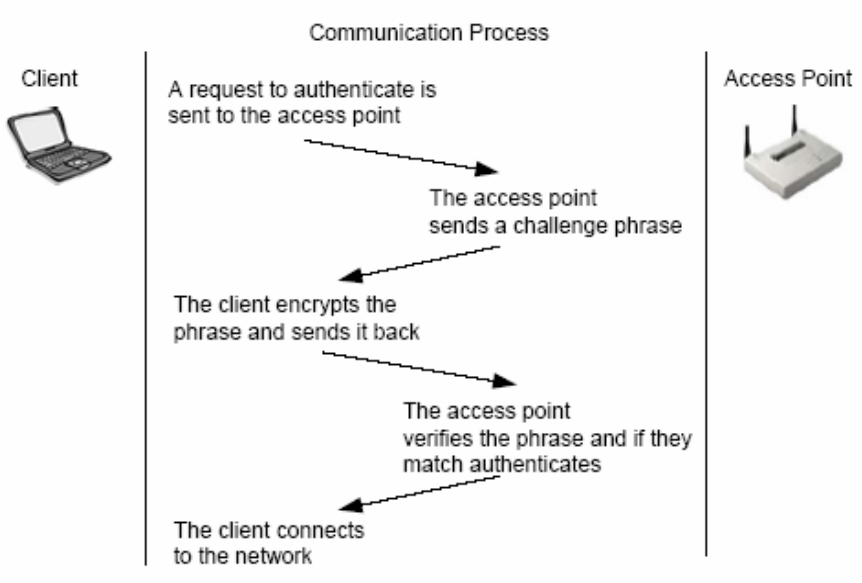
và môi trường không bảo mật. Trong phương pháp này thì WEP chỉ được sử dụng để mã hóa dữ liệu, nếu có.

Chứng thực khóa chia sẻ:

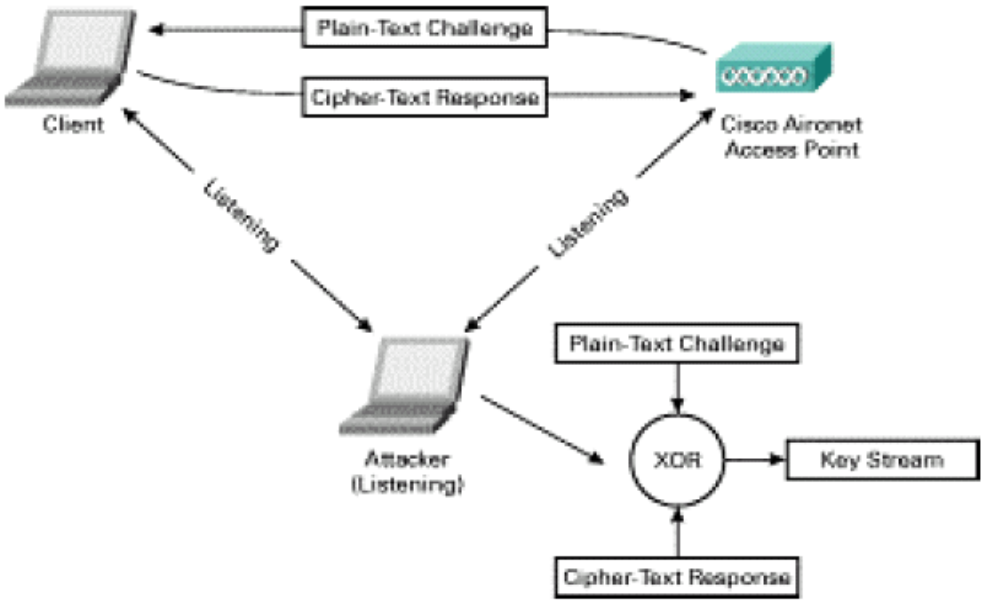
Phương pháp này bắt buộc phải dùng WEP.

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

1. Một clien 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. Clien 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.



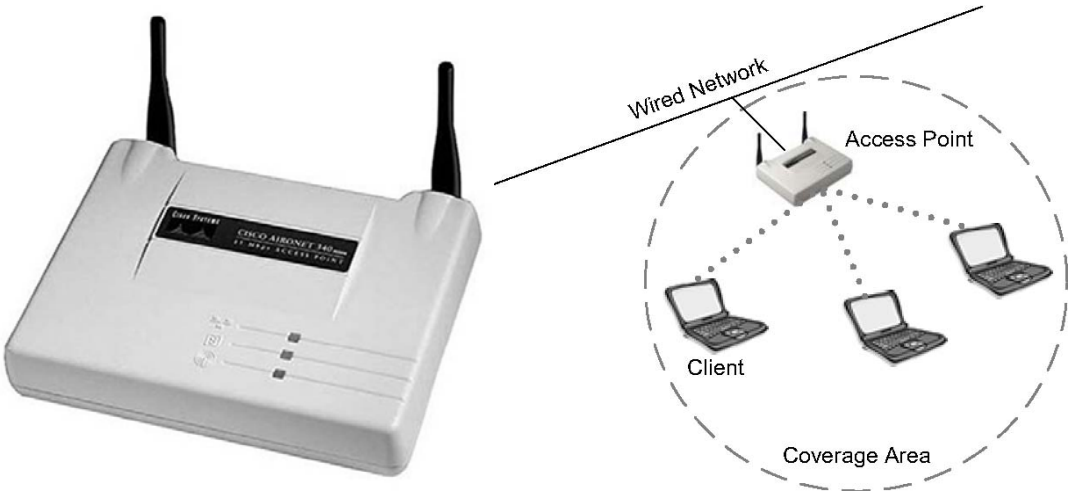
Nhìn qua thì phương pháp này có vẻ an toàn hơn phương pháp chứng thực hệ thống mở, nhưng nếu xem xét kỹ thì trong phương pháp này, chìa khóa Wep được dùng cho hai mục đích, để chứng thực và để mã hóa dữ liệu, đây chính là kẽ hở để hacker có cơ hội thâm nhập mạng. Hacker sẽ thu cả hai tín hiệu, văn bản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



Các thiết bị cơ bản của WLAN

Access Point

Thiết bị này là một trong những thiết bị phổ biến nhất trong cơ sở mạng WLAN. Nó có vai trò là một điểm truy nhập, cung cấp cho khách hàng một điểm truy nhập vào trong mạng. AP là một thiết bị bán song công. Hình sau mô tả một AP với hai anten và vị trí của một AP trong mạng



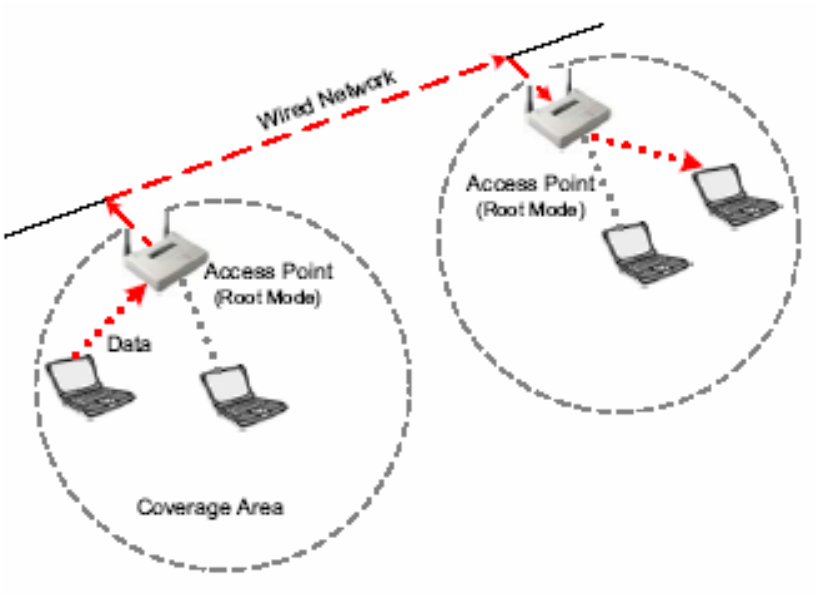
Các chế độ làm việc của AP:

AP liên lạc với các máy Client, với mạng hữu tuyến, với các AP khác, theo ba chế độ mà nó có thể được cấu hình:

Chế độ gốc, chế độ repeater, chế độ bridge

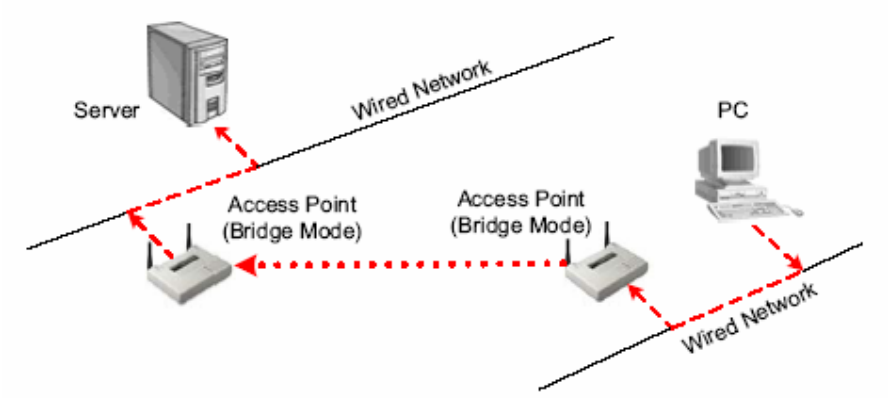
Chế độ gốc:

Chế độ này được cấu hình mặc định trong mạng WLAN, nó được dùng khi AP được nối tới một mạng backbone, thông qua mạng hữu tuyến, thường là mạng Ethernet.



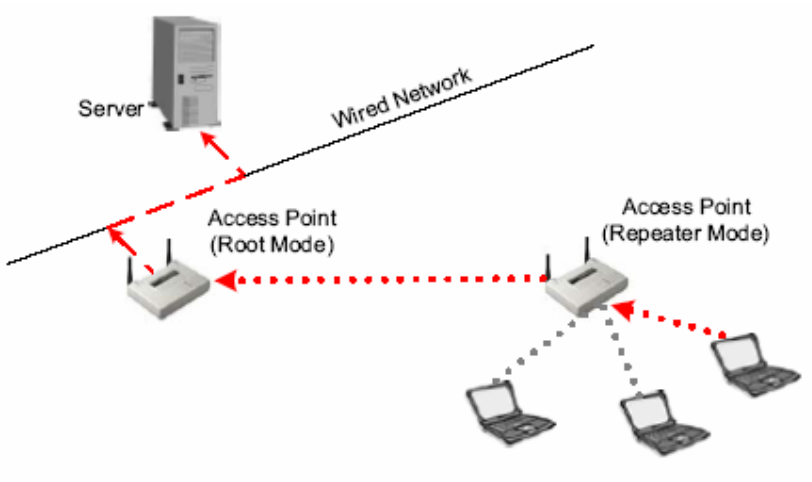
Chế độ cầu nối

Trong chế độ này, AP đóng vai trò như một cầu nối không dây, wireless bridge, thực tế chúng đóng vai trò cầu nối trong khi cấu hình chúng theo cách này. Chỉ một số lượng nhỏ các AP có chức năng cầu nối, nó là do vấn đề giá cả thiết bị. Với vai trò là một cầu nối, thì AP được sử dụng để kết nối hai hay nhiều đoạn mạng với nhau mà không cần dây.



Chế độ lặp:

Trong chế độ bộ lặp, AP sử dụng để cung cấp đường link không dây đến mạng thông thường tốt hơn là các kết nối thông thường



Anten cố định và anten có thể tháo rời

Tùy thuộc vào nhu cầu của người sử dụng mà bạn có thể chọn thiết bị anten cố định hoặc anten có thể tháo rời. Một anten mà có thể tháo rời được sẽ cho bạn khả năng kết nối tới một anten khác mà không cần quan tâm lắm tới độ dài cable bạn đang có

Card vô tuyến có thể tháo rời được

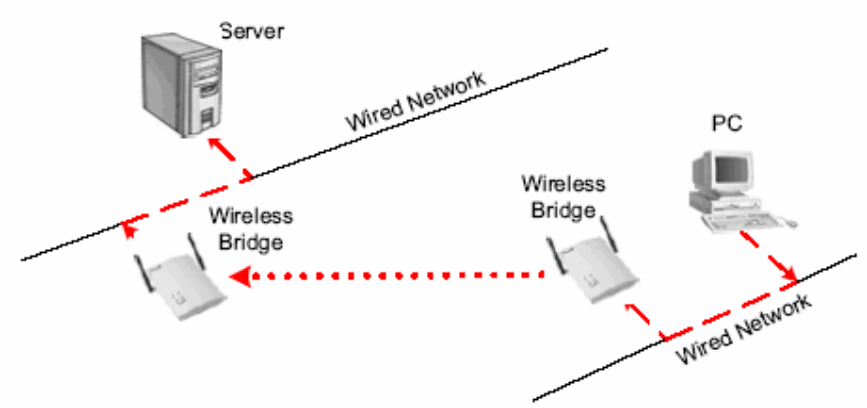
Một vài nhà sản xuất cho phép bạn có thể thêm hoặc bỏ card vô tuyến trong khe cắm PCMCIA trên AP. Một vài AP có thể có hai khe PCMCIA cho những chức năng đặc biệt. Có hai khe trong một AP cho phép một card vô tuyến đóng vai trò một điểm truy nhập, AP, trong khi card kia đóng vai trò một cầu nối. Một tiện ích khác là có thể sử dụng hai card như các AP độc lập. Mỗi card đóng vai trò một AP độc lập cho phép một người quản trị cung cấp được cho gấp đôi số người sử dụng trong cùng một phạm vi vật lí mà không phải dùng hai AP. Tuy nhiên khi cấu hình theo cách này thì để đảm bảo vấn đề chống nhiễu giao thoa, mỗi card vô tuyến nên được cấu hình trên những kênh không chồng lấn lên nhau, ví dụ như kênh 1 và kênh 11.

Bộ biến đổi công suất đầu ra:

Công suất đầu ra biến đổi cho phép người quản trị điều khiển công suất mà AP sử dụng để phát tín hiệu. Điều khiển công suất đầu ra rất có ích trong việc cấu hình vật lí một mạng. Nó có thể tăng công suất đầu ra để mở rộng phạm vi kết nối của các khách hàng, nhưng đồng thời cũng có thể điều chỉnh phạm vi phủ sóng hợp lí, để tránh sự "rò rỉ" thông tin ra ngoài.

Cầu nối không dây

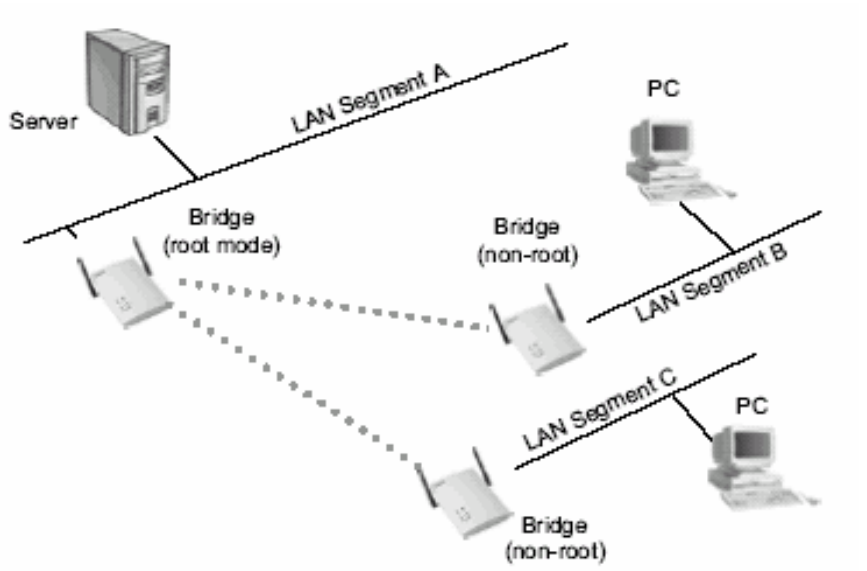
Một cầu nối không dây cung cấp kết nối giữa hai phân đoạn mạng LAN hữu tuyến, nó được dùng trong cấu hình point-to-point hoặc cấu hình point-to-multipoint. Một cầu nối không dây là một thiết bị bán song công, chỉ hoạt động trên kết nối không dây của lớp hai. Hình sau đưa ra một hình ảnh của cầu nối không dây, và vị trí của cầu nối không dây trên mạng LAN không dây.



Cũng như AP, cầu nối không dây cũng hoạt động trong nhiều chế độ khác nhau:

Chế độ gốc:

Trong chế độ này mỗi cầu nối trong nhóm cầu nối phải được thiết lập như một cầu nối gốc. Một cầu nối gốc chỉ có thể liên lạc với những cầu nối không phải là gốc và các thiết bị Client khác mà không thể liên kết với cầu nối gốc khác.



Chế độ non - root

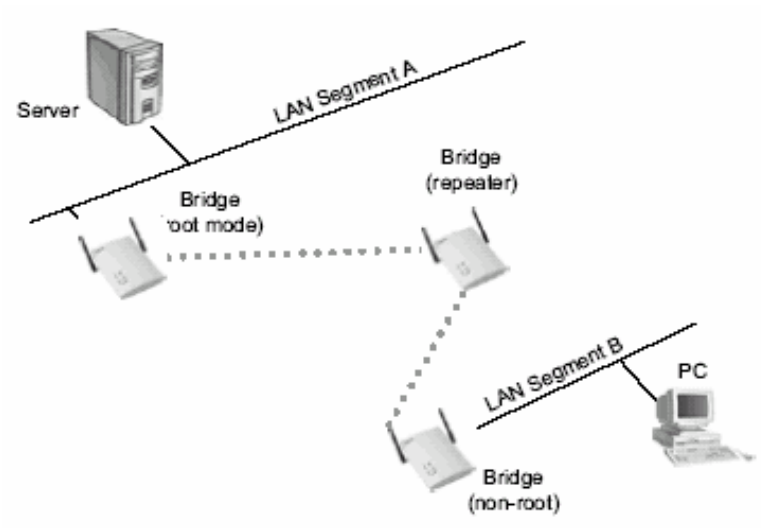
Kết nối với cầu nối ở chế độ gốc, theo cấu hình trên

Chế độ AP

Một vài nhà sản xuất cho phép những người quản trị có thể kết nối các Client tới cầu nối, lúc này cầu nối đóng vai trò như một AP.

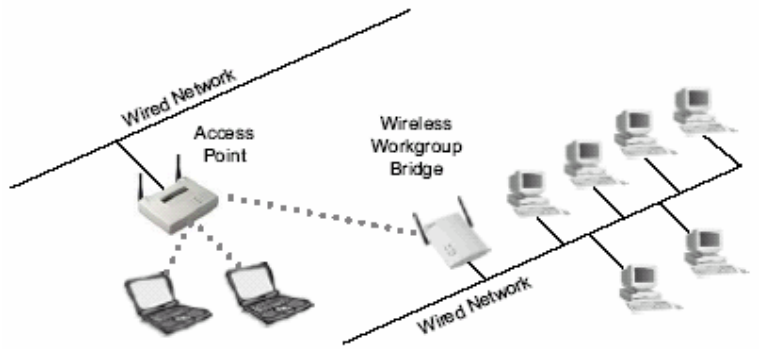
Chế độ lặp

Cầu nối cũng có thể cấu hình như một bộ lặp, đóng vai trò kết nối hai mạng với nhau, cầu nối lúc này phải là cầu nối ở chế độ không phải là chế độ gốc.



Nhóm cầu nối không dây

Tương tự và đôi khi nhầm lẫn với cầu nối không dây là nhóm cầu nối không dây. Sự khác nhau cơ bản của cầu nối không dây và nhóm cầu nối không dây là nhóm cầu nối không dây là một thiết bị máy khách. Nhóm cầu nối không dây có vai trò kết nối cho một nhóm các máy khách của đoạn mạng hữu tuyến với đoạn mạng vô tuyến. Hình vẽ:



Các thiết bị máy khách của WLAN

- PCMCIA và Card flash
- Wireless Ethernet & serial converter
- Bộ tương hợp USB, USB Adapter
- PCI và ISA adapter

PCMCIA & Compact Flash Cards

Đây là thành phần chung cho mọi mạng không dây, thường được gọi là "PC card", thiết bị này được dùng trong laptop và PDA. PC card là thành phần cung cấp kết nối giữa thiết bị client và mạng. Server PC card như một modul vô tuyến trong AP, Bridge, Workgroup bridges, USB adapters, PCI & ISA adapters, và thậm chí cả Server phục vụ in ấn. Hình dưới đây là PCMCIA card

Wireless Ethernet & serial converter

Bộ tiếp hợp USB

USB adapter trở nên thông dụng do khả năng kết nối đơn giản của chúng. Thiết bị máy khách USB hỗ trợ plug-and-play. Một vài USB client có card có thể dễ dàng rút ra được, trong khi một vài cái khác thì không thể rút card ra được.

PCI & ISA Adapters

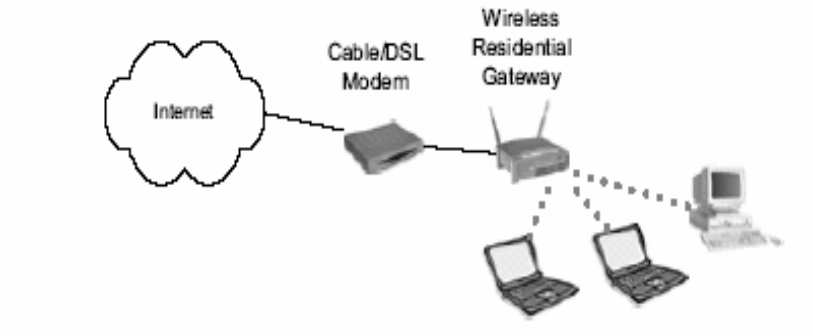
A sample PCI Adapter

Wireless Residential Gateways

Wireless gateway là một thiết bị được thiết kế để kết nối một số lượng nhỏ các node không dây tới một thiết bị đơn lẻ của lớp 2 (mạng vô tuyến hoặc hữu tuyến) và lớp 3 của internet hoặc tới một mạng khác. Nhiều nhà sản xuất tích hợp cả AP và Gateway trên một thiết bị. được kết nối.

A sample wireless residential gateway

A wireless residential gateway installed on a network

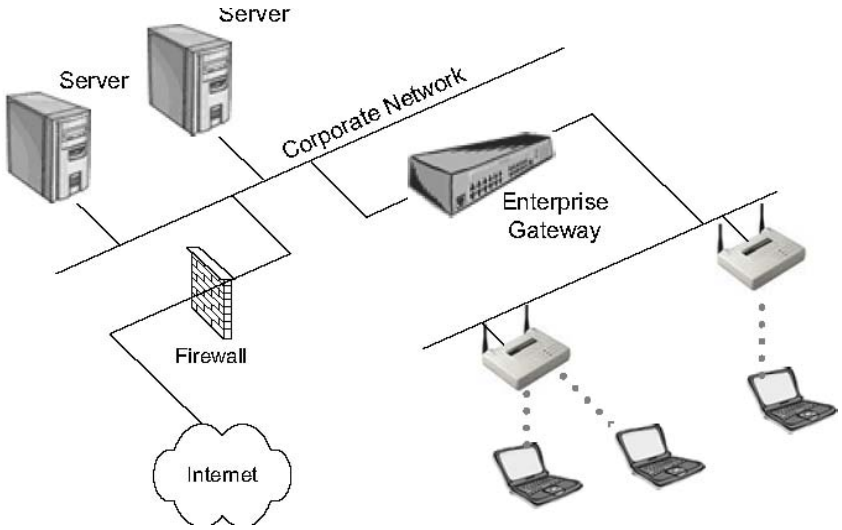


Enterprise Wireless Gateway

Đây là thiết bị mà có thể cung cấp khả năng chứng thực và kết nối đặc biệt cho những client không dây. Nó thích hợp với một mạng WLAN quy mô lớn, cung cấp rất nhiều các dịch vụ có thể quản lý cho WLAN, như giới hạn tốc độ, chất lượng dịch vụ (QoS) .v.v.

Thiết bị gateway này vẫn có một CPU công suất lớn, và một giao diện Ethernet nhanh, để nó có thể hỗ trợ nhiều AP, gửi và nhận thông tin qua nó. Gateway loại này thường hỗ trợ nhiều loại WLAN hay WPAN như các thiết bị chuẩn 802.11, Bluetooth, HomeRF, và nhiều loại nữa.

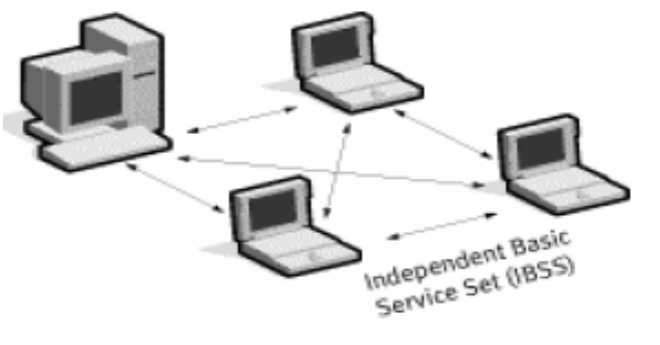
Ví dụ của một Gateway nói trên và vị trí của nó trong mạng



Các Topo mạng căn bản trong WLAN

Tập dịch vụ cơ bản độc lập: Independent Basic Service Set (IBSS)

Topo này tham chiếu tới cầu hình mạng độc lập, hay Ad-hoc, của WLAN. Một cấu hình IBSS tương tự một mạng peer-to-peer mà trong đó không có một node đơn nào có chức năng như một server. IBSS WLAN bao gồm một số node hoặc trạm không dây liên lạc trực tiếp với nhau trên cấu hình cơ sở Ad-hoc, peer-to-peer. Như vậy nó gồm tập hợp các trạm không dây liên lạc trực tiếp với nhau mà không sử dụng bất cứ AP cũng như bất cứ kết nối nào đến mạng hữu tuyến. Cấu trúc này hữu ích cho việc thiết lập nhanh chóng và dễ dàng một mạng WLAN ở tại những nơi mà cơ sở hạ tầng mạng không dây không tồn tại hoặc không được yêu cầu, như phòng trong khách sạn, trung tâm hội nghị, sân bay v.v. Topo mạng loại này che phủ một diện tích giới hạn và không kết nối tới bất kỳ mạng rộng hơn nào.

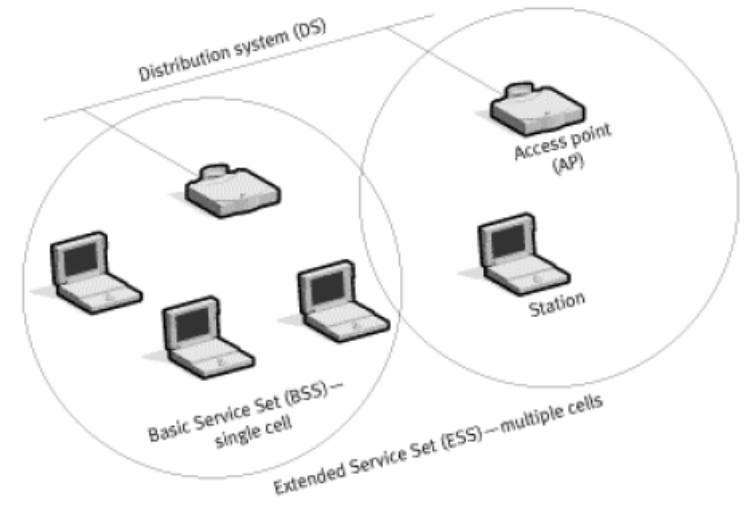


Tập dịch vụ cơ bản: Basic Service Set (BSS)

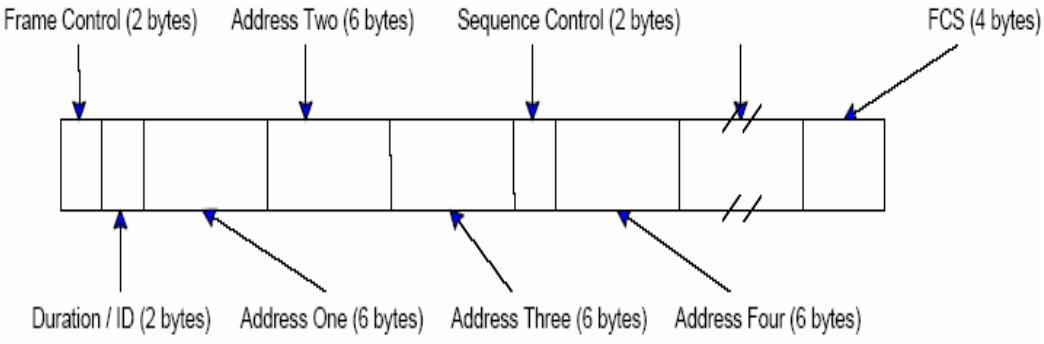
BSS bao gồm ít nhất một AP được kết nối tới cơ sở hạ tầng của mạng hữu tuyến và một tập các trạm không dây cuối ***(Infrastructure mode)***. Trong cấu hình này AP đóng vai trò như một server cho một ô mạng hoặc kênh WLAN đơn. Truyền thông giữa node A và node B sẽ thực hiện từ node A tới AP và sau đó từ AP đến node B.

Tập dịch vụ mở rộng: Extended Service Set (ESS)

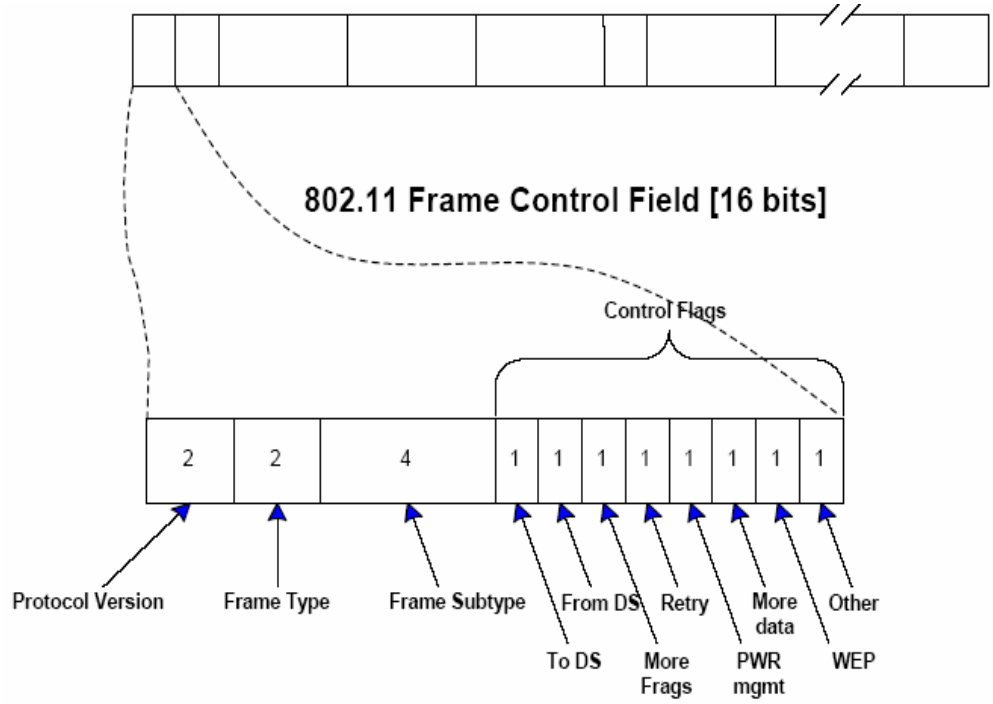
ESS bao gồm một nhóm các BSS gối lên nhau (mỗi cái chứa đựng AP) kết nối với nhau theo hệ thống phân bố. Distributed System (DS). Mặc dù hệ thống phân bố có thể là bất cứ kiểu mạng nào nhưng thường là mạng Ethernet LAN. Những node di động có thể "roam" giữa các AP. Cấu hình này phù hợp với những mạng WLAN mà yêu cầu truy nhập tới các mạng Lan hữu tuyến cho các dịch vụ như (files servers, Printer, Internet links)



802.11 Frame Format [34 - 2344 bytes]



802.11 Frame Control Field [16 bits]



Danh mục sách tham khảo

1. Wireless LAN Protokolle und Anwendungen
2. Introduction to Wireless Technology
3. Designing a Wireless Network
4. Building a Cisco Network Wireless LAN
5. Security problems and solutions in WLAN access zones
6. 802.11 Wireless Network
7. Building Wireless Community Networks
8. Hack broofing your Wireless Network
9. Cisco AVVID Wireless Design
10. IEEE Std 802.11-1999

PHẦN III: QUÁ TRÌNH CẤU HÌNH THIẾT BỊ WIRELESS

Tên thiết bị: Wireless-B, Broadband Router, 2.4GHz 802.11b

Các bước cấu hình

Các thông số cụ thể và chức năng của các cổng, nút, đèn led có trong tài liệu đi kèm thiết bị

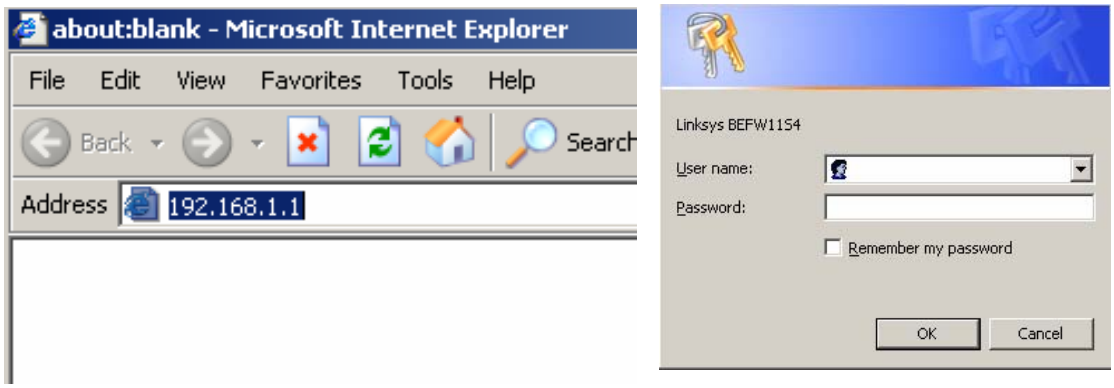
Figure 3-1: The Broadband Router's Back Panel

Figure 3-2: The Broadband Router's Front Panel

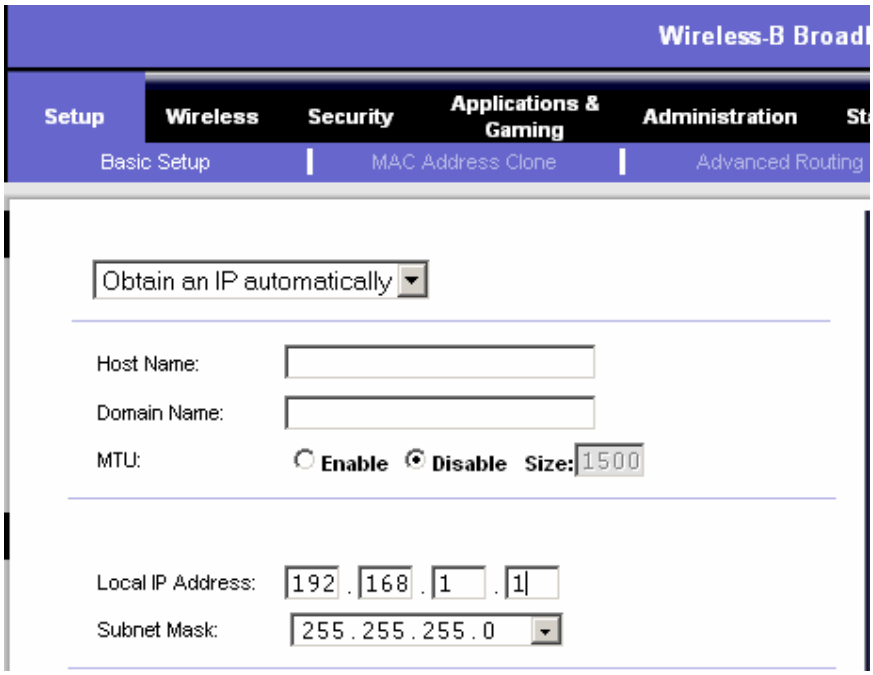
Đặt thiết bị tại trung tâm khu vực phủ sóng, tránh các vật cản (như đã đề cập trong phần khuyến nghị).

Kết nối cable mạng vào cổng internet (hình vẽ trên) và nối thiết bị mạng của bạn vào trong 4 cổng còn lại: 1,2,3,4

Cấp nguồn cho Router và cấu hình cho thiết bị theo các bước sau:
- Thiết bị này mặc định địa chỉ là 192.168.1.1, địa chỉ này nên thay đổi ngay khi cấu hình.

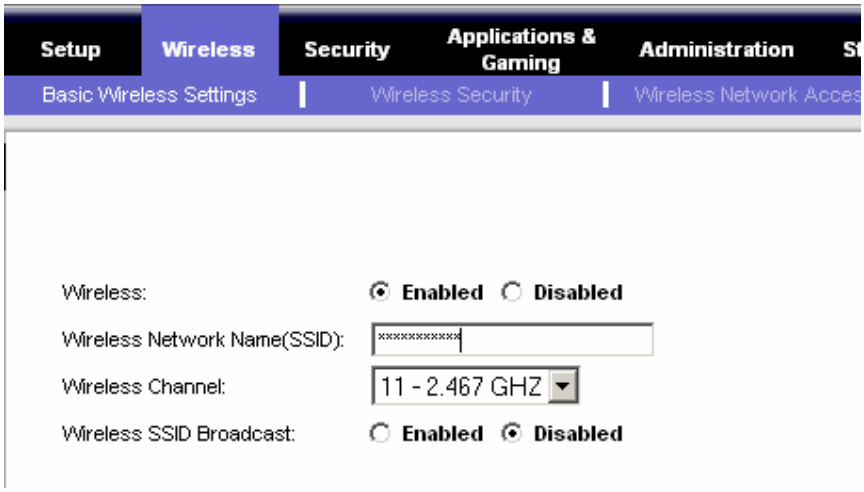


Nhập user name và password do nhà sản xuất cung cấp

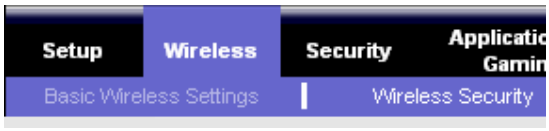


Thiết lập các thông số theo yêu cầu của bạn
Đặt SSID ở chế độ không quảng bá:

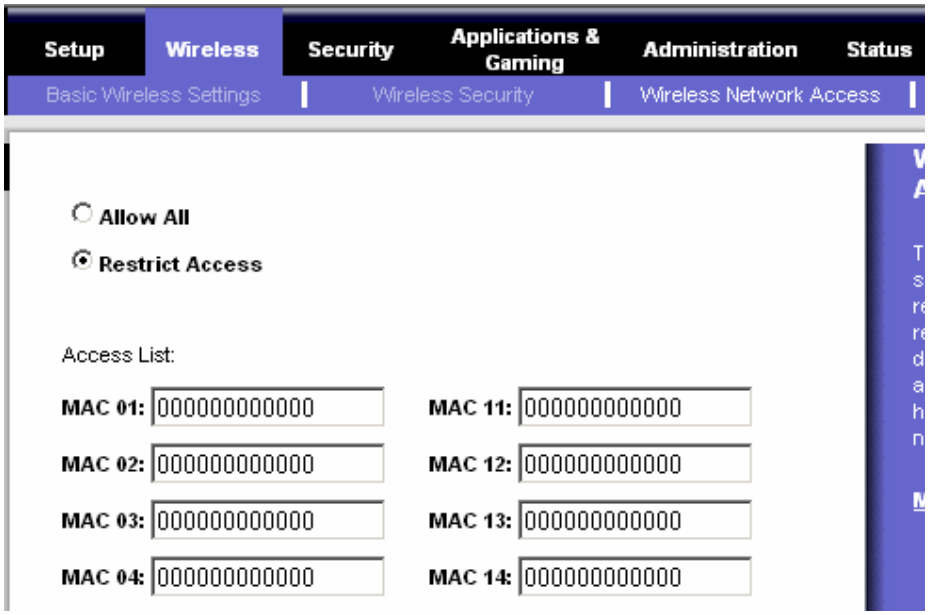
Wireless SSID Broadcast: **Enabled** **Disabled**



Vào Wireless Security để đặt chìa khóa Wep:



Vào Wireless Network Access để đặt bảng địa chỉ Mac, và xem các thiết bị mạng hiện đang truy cập mạng thông qua router



Ngoài ra bạn cũng có thể đặt các biện pháp bảo mật như: đặt bảng lọc địa chỉ MAC, thay đổi SSID, giới hạn số máy tham gia mạng trong một thời gian, bằng cách cấp một số giới hạn các địa chỉ IP, v.v.

Thường xuyên theo dõi các máy truy cập mạng thông qua Router wireless, thay đổi password admin thường xuyên