Chương 1 :

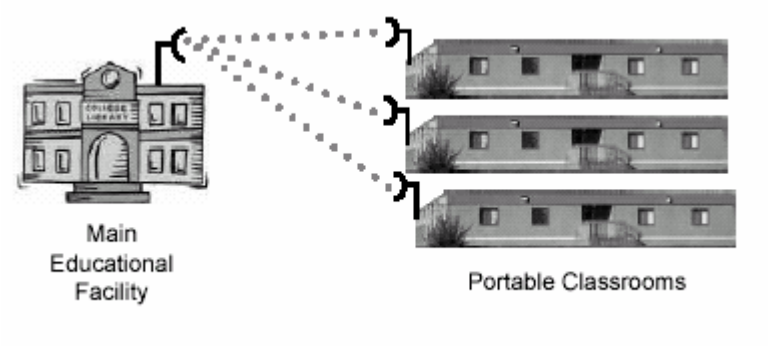
GIỚI THIỆU VỀ WIRELESS

1.1 LỊCH SỬ PHÁT TRIỂN

Trong khi việc nối mạng Ethernet hữu tuyến đã diễn ra từ 30 năm trở lại đây thì nối mạng không dây vẫn còn là tương đối mới đối với thị trường gia đình. Trên thực tế, chuẩn không dây được sử dụng rộng rãi đầu tiên, 802.11b, đã được Viện kỹ thuật điện và điện tử Mỹ (Institue of Electric and Electronic Engineers) IEEE phê chuẩn chỉ 4 năm trước đây (năm 1999). Vào thời điểm đó, phần cứng nối mạng không dây còn rất đắt và chỉ những công ty giàu có và có nhu cầu bức thiết mới có đủ khả năng để nối mạng không dây. Một điểm truy nhập (hay trạm cơ sở - Access Point), hoạt động như một cầu nối giữa mạng hữu tuyến và mạng không dây, có giá khoảng 1000 đô la Mỹ vào thời điểm năm 1999, trong khi các card không dây máy khách giành cho các máy tính sổ tay có giá khoảng 300 đô la. Vậy mà bây giờ bạn chỉ phải trả 55 đô la cho một điểm truy nhập cơ sở và 30 đô la cho một card máy khách 802.11b và đó là lý do tại sao mà việc nối mạng không dây lại đang được mọi người ưa chuộng đến vậy. Rất nhiều máy tính sổ tay-thậm chí cả những máy thuộc loại cấu hình thấp-bây giờ cũng có sẵn card mạng không dây được tích hợp, vì vậy bạn không cần phải mua một card máy khách nữa.

Mạng không dây là cả một quá trình phát triển dài, giống như nhiều công nghệ khác, công nghệ mạng không dây là do phía quân đội triển khai đầu tiên. Quân đội cần một phương tiện đơn giản và dễ dàng, và phương pháp bảo mật của sự trao đổi dữ liệu trong hoàn cảnh chiến tranh.

Khi giá của công nghệ không dây bị từ chối và chất lượng tăng, nó trở thành nguồn kinh doanh sinh lãi cho nhiều công ty trong việc phát triển các đoạn mạng không dây trong toàn hệ thống mạng. Công nghệ không dây mở ra một hướng đi tương đối rẻ trong việc kết nối giữa các trường đại học với nhau thông qua mạng không dây chứ không cần đi dây như trước đây. Ngày nay, giá của công nghệ không dây đã rẻ hơn rất nhiều, có đủ khả năng để thực thi đoạn mạng không dây trong toàn mạng, nếu chuyển hoàn toàn qua sử dụng mạng không dây, sẽ tránh được sự lan man và sẽ tiết kiệm thời gian và tiền bạc của công ty.



Mạng không dây trong trường học

Trong gia đình có thu nhập thấp, mạng không dây vẫn còn là một công nghệ mới mẻ. Bây giờ nhiều người đã tạo cho mình những mạng không dây mang lại thuận lợi trong công việc, trong văn phòng hoặc giải trí tại nhà.

Khi công nghệ mạng không dây được cải thiện, giá của sự sản xuất phần cứng cũng theo đó hạ thấp giá thành và số lượng cài đặt mạng không dây sẽ tiếp tục tăng. Những chuẩn riêng của mạng không dây sẽ tăng về khả năng thao tác giữa các phần và tương thích cũng sẽ cải thiện đáng kể. Khi có nhiều người sử dụng mạng không dây, sự không tương thích sẽ làm cho mạng không dây trở nên vô dụng, và sự thiếu thao tác giữa các phần sẽ gây cản trở trong việc nối kết giữa mạng công ty với các mạng khác.

1.2 TRUYỀN THÔNG VÔ TUYẾN

Truyền thông vô tuyến truyền các tín hiệu qua không trung và không gian sử dụng radio, microwave, và các tần số hồng ngoại trong khoảng megacycle/ giây và kilomegacycle/ giây. Các kỹ thuật truyền vô tuyến khác cũng có thể thực hiện, như các hệ thống laser point-to-point, nhưng các hệ thống này không phổ biến như các hệ thống radio, microwave. Ba loại truyền thông vô tuyến là:

- Truyền thông vô tuyến di động (Wireless mobile communications) Truyền thông sóng vô tuyến qua các tiện ích công cộng sử dụng packet-radio, các mạng cellular, và các trạm vệ tinh đối với các người sử dụng làm việc bên ngoài văn phòng hay làm việc ngay trên lộ trình của họ.

- Truyền thông LAN vô tuyến (Wireless LAN communication) Truyền thông sóng vô tuyến được thực hiện trong các khu vực của một công ty thông qua thiết bị

sở hữu cá nhân. Sự việc này thường liên quan đến các kết nối nhiều máy tính cá nhân trong một văn phòng hay một tầng của một tòa nhà.

- Bắc cầu nối vô tuyến và liên mạng (Wireless bridging and internetworking) Truyền thông sóng vô tuyến được sử dụng để kết nối các tòa nhà và các phương tiện trong các khuôn viên trường sở, các khu vực trung tâm, hay các văn phòng ở các vị trí khác trên hành tinh này (sử dụng vệ tinh).

1.3 TRUYỀN THÔNG DI ĐỘNG

Truyền thông di động - Wireless Mobile Communications - được sử dụng để giữ mối liên lạc giữa những người kinh doanh thường xuyên di chuyển, các trao đổi phân phối, các kỹ thuật viên dã chiến, và các đối tượng khác. Những người dùng máy tính di động sử dụng truyền thông vô tuyến để kết nối với các mạng liên đoàn, các cơ sở dữ liệu truy vấn liên đoàn, trao đổi thư điện tử, truyền tập tin, và thậm chí tham gia xử lý cộng tác. Tất cả đều được thực hiện bằng các máy tính xách tay, PDA (personal digital assistants), và các thiết bị truyền thông vô tuyến nhỏ khác nhau. Những người dùng cũng sẽ kết nối Internet thông qua các thiết bị này, và một ngôn ngữ đặc biệt được gọi là HDML (Hand-held Device Markup Language) được sáng tạo cho mục đích này.

Các nhà cung cấp hệ điều hành quan tâm đến những ai dùng di động bằng cách xây dựng các đặc tính mới để theo dõi vị trí của người sử dụng di động và duy trì môi trường từ session này sang session khác. Ví dụ, vì người dùng di động di chuyển từ nơi này sang nơi khác, người đó sẽ thường xuyên ngưng kết nối và sẽ kết nối lại với các hệ thống từ xa. Hệ điều hành có thể tự động phục hồi các kết nối vào desktop của session trước đó. Nếu một người nào đó truy xuất vào một cơ sở dữ liệu, thì các truy vấn trước đó tới cơ sở dữ liệu này sẽ chờ đợi họ trong lần kết nối tới. Những PDA thường sử dụng các giao diện xa lạ đối với hầu hết các hệ điều hành mạng và các ứng dụng. Tuy nhiên, các nhà đại lý sẽ tích hợp tất cả các hệ thống này khi số lượng những người dùng di động gia tăng.

Về bản chất,việc xử lý di động có liên quan đến những bộ tải điện thoại và các nhà cung cấp dịch vụ khác. Những người dùng chắc chắn sẽ quan tâm mức độ truy xuất (tầm vực và tính thông suốt của tín hiệu), tốc độ truyền dữ liệu tiềm năng, và các khả năng lưu trữ và chuyển đi cho phép người dùng lấy các thông điệp khi họ quay lại trong phạm vi tầm vực. Ví dụ, tốc độ thấp khi truyền dữ liệu đến và từ các

thiết bị di động sử dụng các hệ thống truyền thông được mô tả sau đây, chỉ từ 8 Kbit/ giây đến 19.2 Kbit/ giây. Các yêu cầu về sửa lỗi có thể tác động mạnh mẽ đến việc hạn chế tốc độ truyền.

Các đề mục sau đây mô tả các truyền thông vô tuyến cho các người dùng di động:

- AMPS (Advanced Mobile Phone service) Mô tả hệ thống điện thoại cellular chuyển mạch vòng tính hiệu tương tự (analog) đầu tiên

- CDPD (Cellular Digital Packet Data) Mô tả cách đóng gói và tải dữ liệu trên các hệ thống sóng vô tuyến cellular analog đang có, ví dụ AMPS

- Cellular Communication Systems Thảo luận sự khác nhau giữa các hệ thống analog và hệ thống số

- GMS (Global system for Mobile Communications) Mô tả hệ thống cellular sử dụng kỹ thuật số hoàn toàn được khai triển khắp thế giới

- Mobile Computing Mô tả các kỹ thuật xử lý di động

- Packet-Radio Communications Mô tả các dịch vụ do các trung tâm dịch vụ truyền thông quốc gia đưa ra như ARDIS (Advanced National Radio Data Service) và RAM Mobile Data

- PCS (Personal Communications Services) Mô tả cách các dịch vụ GSM được khai triển ở Mỹ

Các hệ thống kỹ thuật số sử dụng một cơ chế truyền tải riêng để chuyển thông tin giữa những người dùng di động và trạm làm việc cơ sở. Sau đây là hai cơ chế truyền tải chính :

- CDMA (Code Division Multiple Access) CDMA sử dụng các kỹ thuật quang phổ dải rộng, trong đó, các bit dữ liệu ở mỗi lần trao đổi được mã hóa và truyền đồng thời với các lần trao đổi khác. Đoạn mã giúp cho mỗi bộ tiếp nhận truy xuất các bit có nghĩa đối với chính mình. Dữ liệu đã mã hóa được truyền đi trong một tín hiệu băng tần rất rộng, mà những ai muốn nghe trộm khó có thể nghe được.

- TDMA (Time Division Multiple Access) Đây là một kỹ thuật khe thời gian trong đó mỗi thiết bị trên mạng được cho một khe thời gian cụ thể để truyền trong đó. Việc cấp phát thời gian đối với một thiết bị là cố định. Thậm chí nếu thiết bị nầy không có gì để truyền thì cũng giữ khe thời gian.

1.4 TRUYỀN THÔNG LAN VÔ TUYẾN

Như đã được đề cập, các LAN vô tuyến - Wireless Lan Communications - được đặt tiêu biểu trong một môi trường văn phòng. Ví dụ như các sản phẩm từ Radio LAN có thể truyền tới 120 feet trong các văn phòng nửa mở và trên 800 feet trong các văn phòng bên ngoài. Hầu hết các thiết kế LAN vô tuyến khai thác một máy thu phát vô tuyến cố định (Phát/ Thu) chiếm một vị trí trung tâm trong một văn phòng những người sử dụng các máy tính di động được cho phép di động trong một phạm vi nhất định nào đó, điển hình là trong khu vực máy thu phát tức thời. Các mạng LAN vô tuyến có thể hạn chế nhu cầu chạy cáp, đặc biệt nếu LAN được cài đặt tạm thời hay phục vụ như một nhóm làm việc có thể giải tán trong tương lai gần.

Việc cấu hình một mạng LAN vô tuyến bao gồm một bộ phận thu phát được kết nối với các máy chủ và thiết bị khác sử dụng cáp Ethernet chuẩn. Bộ phận thu phát nầy sẽ phát và nhật các tín hiệu từ các trạm làm việc ở quanh nó.

Dưới đây là một vài kỹ thuật truyền dữ liệu vô tuyến:

- Tia hồng ngoại (Infrared light) Phương pháp này đưa ra một băng tần (bandwidth) rộng, truyền các tín hiệu với tốc độ vô cùng cao. Việc truyền bằng tia hồng ngoại hoạt động bằng đường nhìn, vì thế bộ nguồn và bộ nhận phải nhắm tới hay tập trung vào lẫn nhau, tương tự như bộ điều khiển truyền hình từ xa. Những vật cản trong môi trường văn phòng phải được quan tâm, nhưng các gương (mirror) có thể được dùng để rẽ hướng các tia đồng ngoại nếu cần. Bởi vì việc truyền bằng tia hồng ngoại nhạy cảm với ánh xạ mạnh từ cửa sổ hay các nguồn khác, cho nên các hệ thống tạo ra các tia sáng mạnh hơn có lẽ rất cần thiết. Chú ý rằng ánh sáng hồng ngoại không bị chính phủ nghiêm cấm và lại không bị hạn chế về tốc độ truyền. Tốc độ truyền điển hình lên tới 10 Mbit/giây.

- Sóng vô tuyến phổ dải rộng (Spread spectrum radio) Kỹ thuật này phát các tín hiệu thành hai tần số: 900 MHz và 2.4 GHz. Cả hai băng tần đều không đòi hỏi giấy phép FCC. Sóng vô tuyến phổ rộng không có ảnh hưởng tới

sóng vô tuyến thông thường bởi vì mức năng lượng của nó rất yếu. Tốc độ truyền điển hình là 2 Mbit/giây, và khoảng cách chuyển tín hiệu là dưới 1,000 feet, nhưng các tốc độ và tầm vực này có thể được cải thiện.

§ Sóng vô tuyến băng tần hẹp (hay tần số đơn) (Narrowband (or single-frequency) radio) Kỹ thuật này tương tự như một phát tin từ một trạm phát sóng vô tuyến. Bạn dò tới một băng tần "chật" trên cả bộ thu và phát. Tín hiệu này có thể xuyên qua các bức tường và truyền qua các khu vực rộng, vì thế không cần tập trung vào một điểm. Tuy nhiên, việc truyền sóng vô tuyến băng tần hẹp gặp phải vấn đề về sự dội lại sóng vô tuyến và một vài tần số được quy định bởi FCC.

Một mạng LAN vô tuyến có một số lợi điểm. Mạng này không cần có cáp và thường bảo trì rẻ hơn. Tuy nhiên, thị trường LAN vô tuyến rất yếu bởi vì tốc độ dữ liệu dưới 2 Mbit/giây đối với hầu hết các sản phẩm. Nhưng đầu năm 1997, FCC đã mở rộng phổ tới 300 MHz đối với mạng cục bộ vô tuyến không đăng ký. Phổ từ 5.15 đến 5.35 GHz và 5.725 đến 5.825 GHz, là một tần số đủ cao để tốc độ truyền có thể đạt lên đến 20 Mbit/giây. Có thể sử dụng phổ miễn phí, như các phổ điện thoại không dây. Nhiều sản phẩm LAN vô tuyến tốc độ cao nổi bật đã sử dụng tần số mới này. Apple Computer chủ yếu đảm nhận việc thuyết phục FCC (Federal Communications Commission) không cấp phép cho phổ này. Vì hãng này dự định phát triển các sản phẩm để sử dụng trong trường học, nơi mà việc mắc lại dây điện thường không điều chỉnh chi phí. Phổ thông dụng được gọi là U-NII (Unlicensed National Information Infrastructure) và được thảo luận dưới đề mục "NII(National Information Infrastructure)."

Radio LAN giới thệu mạng LAN vô tuyến đầu tiên để hoạt động trong băng tầng sóng vô tuyến 5.8 GHz không đăng ký. Hệ thống này kết hợp băng hẹp, việc truyền tần số đơn với năng lượng thấp và đạt tốc độ 10 Mbit/giây. Băng tần này không bị cản trở bởi các thiết bị cạnh tranh (các đường điện thoại không dây, các lò vi ba, v.v.) Các sản phẩm này hoạt động ở năng lượng thấp, nên ít bị bức xạ điện từ hơn các kỹ thuật vô tuyến khác.

Vào tháng 6/1997, IEEE (Institute of Electrical and Electronic Engineers) đồng ý đặc tả kỹ thuật LAN vô tuyến 802.11, giải thích các chuẩn hoạt động với nhau cho các thiết bị LAN vô tuyến 1 Mbit/giây tới 2 Mbit/giây. Các chuẩn này cũng đẩy mạnh việc bắc cầu vô tuyến giữa các mạng. Tuy nhiên, nhiều người cảm thấy rằng

công nghệ nầy là "quá ít, quá trễ." Thật ra, IEEE đã nghiên cứu nâng cấp lên 10 Mbit/giây. Chuẩn hiện nay chỉ rõ tầm vực tần số 2.4 GHz sử dụng dải phổ rộng, tia hồng ngoại và các kỹ thuật khác. Aironet Wireless Digital Ocean và Lucent Technologies đã và đang phát triển một nghi thức truy xuất điểm thông dụng để bảo đảm tính liên hoạt động hiện thời.

1.5 WIRELESS BRIDGING AND INTERNETWORKING

Kết nối hai mạng riêng lẻ với nhau là một công việc thường xuyên dễ dàng. Bạn có thể cài đặt một cặp các cầu nối hay router và kết nối dây cáp giữa hai thiết bị, hay sử dụng một đường điện thoại quay số hay thuê bao. Nhưng những kết nối này không phải lúc nào cũng thiết thực hay hiệu quả về mặt chi phí. Trong các môi trường thuộc khuôn viên trường sở hay các khu vực trung tâm, sẽ thiết thực hơn nếu sử dụng các hệ thống vô tuyến để kết nối các mạng. Một lần nữa, tốc độ truyền dữ liệu là mối quan tâm đáng kể, nhưng chi phí về thiết bị và việc tiết kiệm cuối cùng các đường dây quay số hay các dây cáp riêng cũng là một mối quan tâm không nhỏ khác.

Vấn đề bắt cầu nối vô tuyến ít phức tạp hơn việc truyền thông LAN vô tuyến bởi vì các kết nối thường là điểm-tới-điểm và không cần phải quan tâm đến các vấn đề như các bức tường và các bức xạ. Cầu nối phải thực hiện việc lọc để giữ lưu lượng không cần thiết từ việc vượt qua một liên kết, hay một router có thể được sử dụng để điều khiển lưu lượng giữa các mạng. Việc bắc cầu nối vô tuyến cũng có thể được dùng để sao lưu (back up) các loại kết nối dữ liệu khác.

Hầu hết các cầu nối vô tuyến sử dụng các kỹ thuật sóng vô tuyến phổ dải rộng tần số nhảy, sẽ không dễ bị nhiễu và có một mức độ bảo mật cao. Hầu hết các sản phẩm đều có tầm vực 25 mile. Tốc độ truyền điển hình trong tầm vực 2 Mbit/giây, như các sản phẩm mới hơn hoạt động trong tầm vực 10 Mbit/giây.

Ratheon Wireless Solutions là một công ty bán các cầu nối vô tuyến. Sản phẩm Raylink Access Point của công ty này là một cầu nối vô tuyến LAN-to-Ethernet tuân theo chuẩn mạng LAN vô tuyến IEEE-802.11. Các công ty bán hàng khác như Digital Ocean, OTC Telecom, Aironet Wireless Communication, Breeze Wireless Communications, C-SPEC, Proxim, và Windata.

Các giải pháp vô tuyến khác bao gồm các hệ thống microwave trên mặt trái đất và các hệ thống truyền thông vệ tinh.

1.6 TIÊU CHUẨN MẠNG KHÔNG DÂY HIỆN NAY

Vì mạng không dây sử dụng tầng số sóng vô tuyến để truyền tín hiệu, nên mạng không dây chịu sự ảnh hưởng của các sóng từ khác, như là sóng AM/FM. Bang chuyển giao thông tin (FCC) đã nghiên cứu và tìm cách khắc phục lỗi này. Trong thị trường mạng không dây hiện nay có một số chuẩn riêng được sàn lọc và được xác nhận bởi Viện các kỹ sư điện và điện tử (IEEE), Hoa Kỳ.

Những chuẩn này được tạo bởi một nhóm người đại diện cho nhiều công ty khác nhau, bao gồm những viện sĩ, thương gia, sĩ quan,và chính phủ. Vì những chuẩn này thiết lập về phía IEEE có thể sẽ chạm phải sự phát triển của công nghệ, những chuẩn này có thể mất vài năm để tạo ra và được chấp nhận. Nhà sản xuất khuyến khích chúng ta phê bình hoặc đánh giá các chuẩn này trong thời gian nó đang được triển khai để cho ra một sản phẩm hoàn hảo.

Trên thực tế, chuẩn không dây được sử dụng rộng rãi đầu tiên, 802.11b, đã được IEEE phê chuẩn chỉ 4 năm trước đây (năm 1999). Vào thời điểm đó, phần cứng nối mạng không dây còn rất đắt và chỉ những công ty giàu có và có nhu cầu bức thiết mới có đủ khả năng để nối mạng không dây. Một điểm truy nhập (hay trạm cơ sở), hoạt động như một cầu nối giữa mạng hữu tuyến và mạng không dây, có giá khoảng 1000 đô la Mỹ vào thời điểm năm 1999, trong khi các card không dây máy khách giành cho các máy tính sổ tay có giá khoảng 300 đô la. Vậy mà bây giờ bạn chỉ phải trả 55 đô la cho một điểm truy nhập cơ sở và 30 đô la cho một card máy khách 802.11b và đó là lý do tại sao mà việc nối mạng không dây lại đang được mọi người ưa chuộng đến vậy. Rất nhiều máy tính sổ tay-thậm chí cả những máy thuộc loại cấu hình thấp-bây giờ cũng có sẵn card mạng không dây được tích hợp, vì vậy bạn không cần phải mua một card máy khách nữa.

1.6.1 CÁC CHUẨN CỦA MẠNG KHÔNG DÂY :

Các chuẩn của mạng không dây được tạo và cấp bởi IEEE.

- 802.11 : Đây là chuẩn đầu tiên của hệ thống mạng không dây. Chuẩn này chứa tất cả công nghệ truyền hiện hành bao gồm Direct Sequence Spectrum (DSSS), Frequence Hopping Spread Spectrum (FHSS) và tia hồng ngoại. 802.11 là một

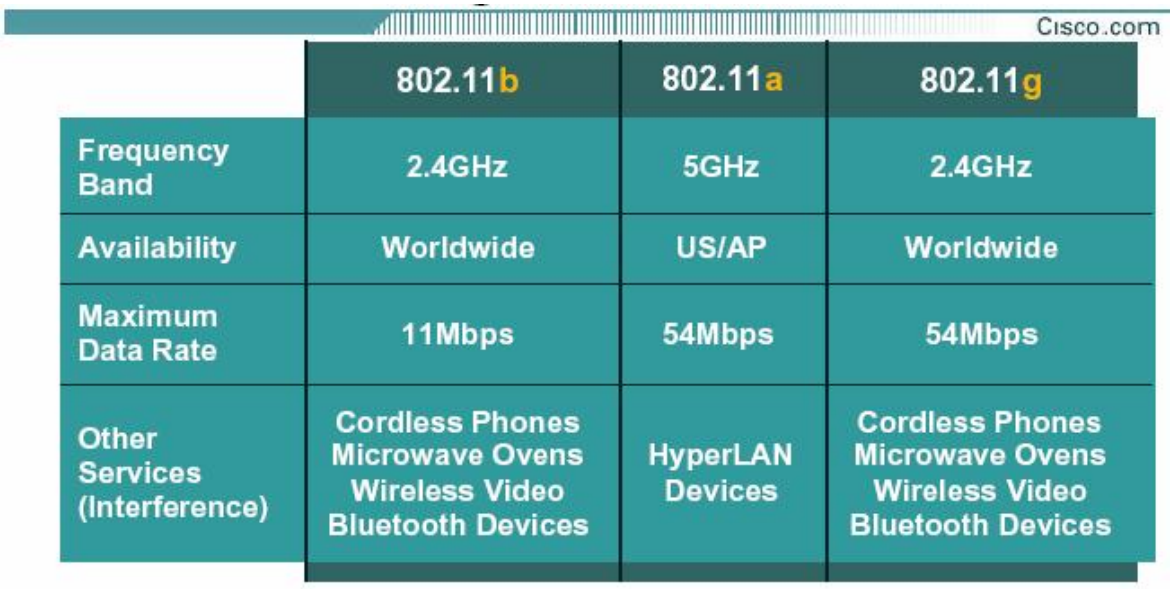
trong hai chuẩn miêu tả những thao tác của sóng truyền (FHSS) trong hệ thống mạng không dây. Nếu người quản trị mạng không dây sử dụng hệ thống sóng truyền này, phải chọn đúng phần cứng thích hợp cho các chuẩn 802.11.

- 802.11b : Hiện là lựa chọn phổ biến nhất cho việc nối mạng không dây; các sản phẩm bắt đầu được xuất xưởng vào cuối năm 1999 và khoảng 40 triệu thiết bị 802.11b đang được sử dụng trên toàn cầu. Các chuẩn 802.11b hoạt động ở phổ vô tuyến 2,4GHz. Phổ này bị chia sẻ bởi các thiết bị không được cấp phép, chẳng hạn như các điện thoại không dây và các lò vi sóng- là những nguồn gây nhiễu đến mạng không dây dùng chuẩn 802.11b. Các thiết bị 802.11b có một phạm vi hoạt động từ 100 đến 150 feet (1 feet = 0,3048m) và hoạt động ở tốc độ dữ liệu lý thuyết tối đa là 11 Mbit/s. Nhưng trên thực tế, chúng chỉ đạt một thông lượng tối đa từ 4 đến 6 Mbit/s. (Thông lượng còn lại thường bị chiếm bởi quá trình xử lý thông tin giao thức mạng và kiểm soát tín hiệu vô tuyến). Trong khi tốc độ này vẫn nhanh hơn một kết nối băng rộng DSL hoặc cáp và đủ cho âm thanh liên tục (streaming audio), 802.11b lại không đủ nhanh để truyền những hình ảnh có độ nét cao. Lợi thế chính của 802.11b là chí phí phần cứng thấp.

- 802.11a : Vào cuối năm 2001, các sản phẩm dựa trên một chuẩn thứ hai, 802.11a, bắt đầu được xuất xưởng. Không giống như 802.11b, 802.11a hoạt động ở phổ vô tuyến 5 GHz (trái với phổ 2,4GHz). Thông lượng lý thuyết tối đa của nó là 54 Mbit/s, với tốc độ tối đa thực tế từ 21 đến 22 Mbit/s. Mặc dù tốc độ tối đa này vẫn cao hơn đáng kể so với thông lượng của chuẩn 802.11b, phạm vi phát huy hiệu lực trong nhà từ 25 đến 75 feet của nó lại ngắn hơn phạm vi của các sản phẩm theo chuẩn 802.11b. Nhưng chuẩn 802.11a hoạt động tốt trong những khu vực đông đúc: Với một số lượng các kênh không gối lên nhau tăng lên trong dải 5 GHz, bạn có thể triển khai nhiều điểm truy nhập hơn để cung cấp thêm năng lực tổng cộng trong cùng diện bao phủ. Một lợi ích khác mà chuẩn 802.11a mang lại là băng thông cao hơn của nó giúp cho việc truyền nhiều luồng hình ảnh và truyền những tập tin lớn trở nên lý tưởng.

- 802.11g : 802.11g là chuẩn nối mạng không dây được IEEE phê duyệt gần đây nhất (tháng 6 năm 2003). Các sản phẩm gắn liền với chuẩn này hoạt động trong cùng phổ 2,4GHz như những sản phẩm theo chuẩn 802.11b nhưng với tốc độ dữ liệu cao hơn nhiều - lên tới cùng tốc độ tối đa lý thuyết của các sản phẩm theo chuẩn 802.11a, 54 Mbit/s, với một thông lượng thực tế từ 15 đến 20 Mbit/s. Và

giống như các sản phẩm theo chuẩn 802.11b, các thiết bị theo chuẩn 802.11g có một phạm vi phát huy hiệu lực trong nhà từ 100 đến 150 feet. Tốc độ cao hơn của chuẩn 802.11g cũng giúp cho việc truyền hình ảnh và âm thanh, lưới Web trở nên lý tưởng. 802.11g thiết kế để tương thích ngược với 802.11b và chúng chia sẻ cùng phổ 2,4GHz. Việc này làm cho các sản phẩm của 2 chuẩn 802.11b và 802.11g có thể hoạt động tương thích với nhau. Chẳng hạn, một máy tính sổ tay với một PC card không dây 802.11b có thể kết nối với một điểm truy nhập 802.11g. Tuy nhiên, các sản phẩm 802.11g khi có sự hiện diện của các sản phẩm 802.11b sẽ bị giảm xuống tốc độ 802.11b. Trong khi các mạng 802.11a không tương thích với các mạng 802.11b hay 802.11g, các sản phẩm bao gồm một sự kết hợp của phổ vô tuyến 802.11a và 802.11g sẽ cung cấp những thứ tốt nhất. Đây là một tin tốt lành cho chuẩn 802.11a; trong môi trường gia đình, nơi mà tín hiệu vô tuyến cần phải xuyên qua nhiều bức tường và vật cản, chỉ một mình tính năng 802.11g có thể sẽ ít được lựa chọn bởi vì phạm vi hoạt động ngắn hơn của nó.



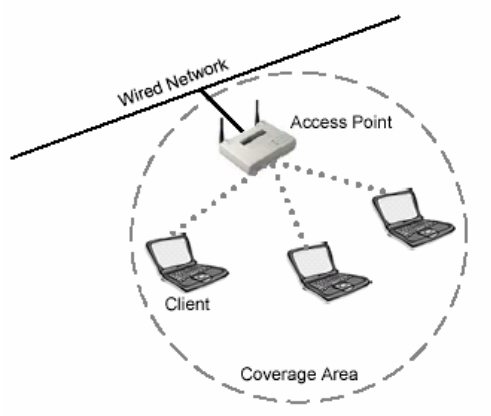
1.6.2 THỊ TRƯỜNG MẠNG KHÔNG DÂY

Khi những chiếc máy tính đầu tiên được tạo ra, chỉ có trường đại học hoặc các công ty lớn mới có khả năng sử dụng. Ngày nay bạn có thể kiếm 3 hoặc 4 máy vi tính trong nhà hàng xóm của bạn. Mạng không dây đã chiếm một phần không nhỏ, đầu tiên được sử dụng bởi những hãng lớn, và giờ đây ngay cả chúng ta cũng có thể mua được. Như là một công nghệ, mạng không dây đã được hưởng một chính sách

thuế chấp nhận được dẫn đến giá thành thấp, chấp nhận được. Trong đoạn này, chúng ta sẽ thảo luận một vài ứng dụng phổ biến và thích hợp nhất của mạng không dây.

1.7 VAI TRÒ TRUY CẬP

Mạng không dây là triển khai tốt nhất trong một vai trò truy cập lớp, nghĩa là chúng sử dụng như là một điểm đi vào mạng hữu tuyến. Trong quá khứ, việc truy cập thường là bằng quay số, ADSL, cáp, ethernet, mạng hình sao, bộ tiếp sóng khung (frame relay), ATM, v.v.. Mạng không dây là một phương pháp đơn giản khác để truy cập internet. Mạng không dây là dữ liệu trong tầng NetWork giống như tất cả các phương pháp trong danh sách. Tất cả những điều đó dẫn tới sự thiếu hụt tốc độ và sự phục hồi, mạng không dây không điều chỉnh những phương tiện trong sự phân bổ hoặc vai trò của lõi trong mạng. Tất nhiên, trong những mạng nhỏ, sẽ không có sự khác biệt giữa lõi, phân phối hoặc lớp truy xuất của mạng. Lớp lõi của mạng phải rất nhanh và vững chắc, có thể giữ một lượng lớn lưu lượng với một chút khó khăn và kinh nghiệm thời gian không giảm. Sự phân phối của lớp trong mạng nên nhanh, mềm dẻo và đáng tin cậy.



Vai trò truy xuất của mạng không dây

Mạng không dây phải trả cho một giải pháp đặc biệt là vấn đề di động. Không còn nghi ngờ gì nữa, mạng không dây giải quyết vấn đề máy chủ để khi ở nhà cũng giống như khi đang ở công ty, và đó là vấn đề của tốc độ truyền và thông lượng truyền được. Giải pháp các ô hình mạng đã được ứng dụng trong một khoảng thời gian, người dùng phải trả cho sự lãng phí này trong khi kết nối vì tốc độ chậm và

giá thì rất cao. Trong khi mạng không dây trả cho một giải pháp tương tự nhưng mềm hơn không bất lợi. Mạng không dây nhanh, không đắt, và nó có thể có mặt ở mọi nơi.

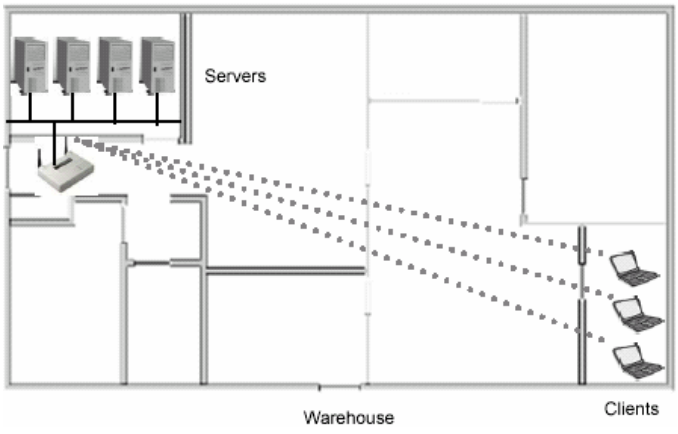
Khi bạn tính đến sẽ sử dụng mạng không dây, hãy cứ nghĩ rằng sử dụng chúng cho những ý định được mong đợi sẽ cho kết quả tốt nhất. Những người quản trị thực thi mạng không dây trong một lõi hoặc sự phân bổ vai trò nên hiểu chính xác rằng những gì thực hiện để mong đợi trước khi thực thi chúng trong kiểu cách để ngăn không xóa chúng sau này. Chỉ có sự phân bổ vai trò trong một mạng công ty là phải rõ ràng thích hợp cho mạng không dây như là triển khai theo kiểu cầu nối. Trong viễn cảnh này, mạng không dây có thể tính đến khi vai trò được phân bổ. Tuy nhiên, nó sẽ luôn luôn được quyết định trên các mảng cầu của mạng không dây khi sử dụng trong mạng.

Có vài dịch vụ cung cấp mạng không dây – Wireless Initernet Providers (WISPs) sử dụng mạng truyền bằng sóng từ trong vai trò phân bổ, nhưng hầu như không bao giờ sử dụng mạng chưa cấp phép.

1.8 MẠNG MỞ RỘNG

Mạng không dây có thể đáp ứng như là một mạng hữu tuyến. Có nhiều trường hợp cần tăng thêm cáp mà giá quá cao. Bạn có thể thấy rằng việc đi dây cáp và dây điện cho một văn phòng sẽ tốn khoảng 10.000 USD. Hoặc trường hợp của một cửa hàng lớn, khoảng cách có thể quá xa để sử dụng loại cáp 5 cho mạng cục bộ. Kết cấu có thể đã được cài đặt sẵn, yêu cầu có thể đầu tư nhiều thời gian và tiền của hơn. Cài đặt kết cấu có thể bao gồm nâng cấp Switch.

Mạng không dây có thể dễ dàng cung cấp những kết nối không liền mạch để điều khiển các khu vực trong khoảng thời gian triển khai, như hình dưới đây :



Vì một ít đoạn mạng cần cài đặt mạng không dây, giá của các máy chủ cài đặt và việc mua cáp cho mạng hữu tuyến có thể bị loại ra hoàn toàn.

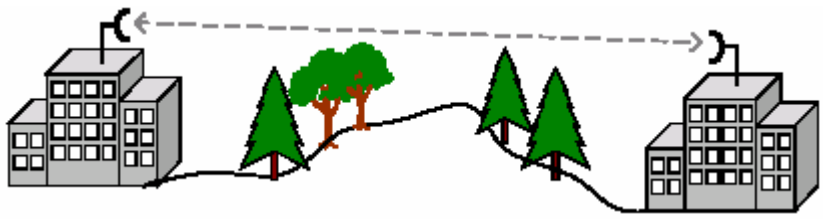
1.9 XÂY DỰNG KẾT NỐI

Trong điều kiện trường sở hoặc các tòa nhà, người sử dụng sẽ truy cập trong những tòa nhà khác nhau, ở bất cứ nơi đâu trong trường sở chỉ thông qua một trạm cơ sở. Trong quá khứ, kiểu kết nối này cũng đã được hoàn thành bằng cách chạy dây cáp dưới lòng đất từ tòa nhà này tới tòa nhà khác hoặc thuê một đường thuê bao khá đắt từ công ty cung cấp.

Sử dụng công nghệ không dây, sự trang bị bằng việc cài đặt dễ dàng và nhanh chóng cho phép hai hoặc nhiều tòa nhà trở thành một phần của một mạng giống nhau không cần tốn chi phí thuê đường thuê bao hoặc đào đường giữa các tòa nhà. Với một anten không dây thích hợp, bất cứ tòa nhà cũng có thể liên kết với nhau trên cùng một mạng. Tất nhiên cũng có những giới hạn trong việc sử dụng công nghệ không dây, như là bất cứ giải pháp kết nối dữ liệu nào, nhưng tính mềm dẻo, tốc độ và độ an toàn của nó là tuyệt đối cần thiết cho người quản trị mạng.

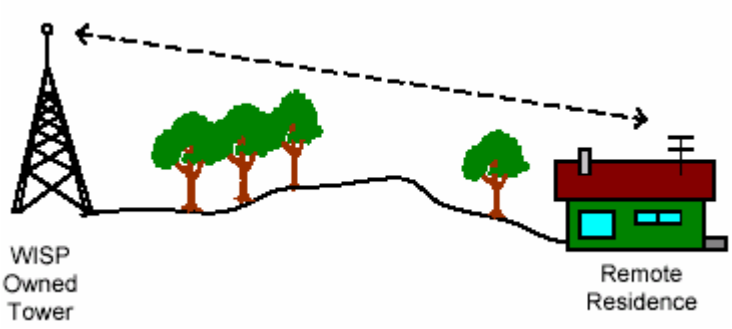
Có hai kiểu kết nối khác nhau giữa hai tòa nhà. Kiểu đầu tiên được gọi là điểm tới điểm (point-to-point – PTP), và kiểu thứ hai được gọi là điểm tới nhiều điểm (Point-to-Mutilpoint – PTMP).

PTP liên kết các kết nối không dây chỉ giữa hai tòa nhà, như là hình dưới đây :



PTMP liên kết các kết nối giữa ba hoặc nhiều tòa nhà, điển hình như là liên kết của niền xe và căm xe, sẽ có một tòa nhà là tiêu điểm của mạng. Tòa nhà trung tâm này có lõi mạng, kết nối internet, và một máy chủ cho thuê. PTMP liên kết giữa các tòa nhà điển hình sử dụng anten phát trong máy chủ truy cập trung tâm và anten thu trên các tòa nhà khác trong mạng.

Có nhiều cách thực thi hai kiểu kết nối cơ bản này, khi bạn sẽ không lưỡng lự cho công việc quản trị mạng hoặc tư vấn viên. Tuy nhiên, không có gì để thay đổi sự thi hành, tất cả chúng đều ở trong hai loại sau :



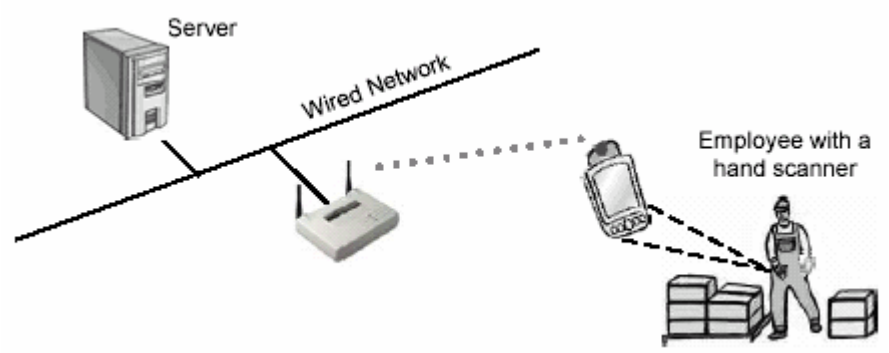
Tính đến trường hợp cả cáp và trạm thông tin của công ty đều chạm đến sự mở rộng khác nhau của nhiều đoạn mạng tính đến kết nối băng thông rộng tới nhiều hộ gia đình hoặc các công ty kinh doanh. Nếu bạn sống ở nông thôn, có thể bạn sẽ không truy cập tới băng thông rộng được (dùng modem hoặc DSL) và chắc chắn sẽ không nhanh. Phải có nhiều chi phí hiệu quả cho WISPs để tính đến khả năng truy cập mạng không dây từ xa bởi vì WISPs không chạm trán với những mức chi phí giống như thế khi sử dụng cáp hoặc trạm thông tin của công ty và sử dụng mạng không dây là sự trang bị cần thiết.

WISPs có một thách thức độc nhất đối với họ. Chỉ khi những nhà cung cấp xDSL gặp vấn đề đi xa hơn 18.000 feet (5,7km) từ văn phòng chính và nhà cung cấp cáp đưa ra loại cáp chia sẽ phương tiện tới người dùng. WISPs gặp vấn đế với các nóc nhà, những cái cây, núi, sét, những cái tháp và nhiều sự cản trở tới việc kết nối. Tất nhiên WISPs không có bằng chứng để kết tội, nhưng họ có khả năng tính đến việc sử dụng truy cập băng thông rộng, thêm những công nghệ được quy ước không thể vươn tới.

1.10 TÍNH DI ĐỘNG

Khi có một giải pháp truy cập lớp, mạng không đây không thể thay thế mạng hữu tuyến trong giới hạn truyền dữ liệu (100BaseTx đạt 100Mbps với IEEE 802.11a đạt 54Mbps). Kiểu kết nối của mạng không dây là không liên tục và có nhiều lỗi hơn khi sử dụng băng thông hẹp. Kết quả là, những ứng dụng và những giao thức được thiết kế cho mạng hữu tuyến đôi khi hoạt động không hiệu quả trong

môi trường mạng không dây. Những gì mà mạng không dây tính đến là sự tăng về tốc độ và chất lượng của các dịch vụ di động.



Trong kho lưu trữ, mạng không dây sử dụng các rãnh để lưu các vị trí và sự sắp đặt của sản phẩm. Dữ liệu này được đồng bộ hóa trong máy chủ cho những phần mua và vận chuyển. Mạng không dây đã trở nên bình thường trong các công ty với những nhân viên di chuyển trong giờ làm việc và kiểm tra mọi thứ.

Trong mỗi trường hợp, mạng không dây tạo ra khả năng truyền dữ liệu không cần phụ thuộc vào thời gian và nhân sự để đưa dữ liệu vào như cách thông thường. Kết nối mạng không dây hầu như loại ra tất cả các thiết bị kết nối sử dụng dây.

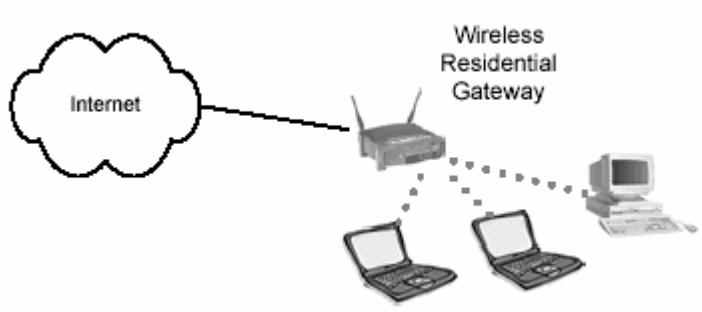
Một vài công nghệ không dây mới nhất cho phép người dùng đi lang thang, hoặc đi ra khỏi vùng phủ sóng của mạng không dây tới một khu vực khác không có kết nối, như là điện thoại di động, khách hàng có thể đi lang thang giữa các vùng của các khu vực được phủ sóng. Trong những công ty lớn hơn, khi vùng phủ sóng của mạng không dây nối những khu vực rộng lớn, khả năng lang thang là đáng kể, tăng khả năng sản xuất cho công ty, đơn giản là vì người dùng vẫn kết nối tới mạng khi họ ở xa trạm chính.

1.11 VĂN PHÒNG NHỎ - VĂN PHÒNG NHÀ

Khi là một IT chuyên nghiệp, bạn phải có nhiều hơn 1 chiếc máy tính trong nhà. Và nếu bạn làm việc, những cái máy tính phải được nối mạng với nhau để bạn có thể chia sẽ file, in, hoặc đường dây kết nối.

Kiểu cấu hình này hầu như được tận dụng bởi nhiều doanh nghiệp chỉ có vài nhan viên. Những doanh nghiệp này cần chia sẻ thông tin giữa những người dùng và một kết nối internet cho năng suất và khả năng sản xuất lớn hơn.

Cho các ứng dụng – văn phòng nhỏ - văn phòng nhà – SOHO – mạng không dây là một giải pháp đơn giản và hiệu quả.



Hình trên là là một kiểu của giải pháp SOHO. Thiết bị không dây SOHO đặc biệt có lợi khi nhân viên văn phòng muốn chia sẻ kết nối internet. Sự khác nhau của hướng đi là đi dây khắp nơi trong cả văn phòng nối liền tất cả các máy con. Nhiều văn phòng nhỏ không trang bị đầy đủ cho việc cài đặt lại các cổng mạng cục bộ, và chỉ có một vài nhà là có dây cho mạng cục bộ. Cố gắng trang bị thêm những bộ phận mới cho những nơi sử dụng cáp Cat5 thường cho kết quả là tạo ra những lỗ thủng xấu xí trên tường hoặc trần nhà. Với mạng không dây, người dùng có thể nối với nhau dễ dàng và gọn gàng.

1.12 VĂN PHÒNG DI ĐỘNG

Văn phòng di động hoặc phòng học cho phép người dùng tắt máy nhanh chóng và đem chúng đến một nơi khác. Vì những lớp đông kín người, bây giờ nhiều trường sử dụng những lớp di động để thay thế. Những lớp này thường lớn, sử dụng chuyển động, trong khi có cấu trúc xây dựng lâu bền hơn. Trong các loại mạng máy tính kết nối tới những tòa nhà tạm thời, cáp trên trời hoặc dưới lòng đất phải được cài đặt với phí tổn lớn. Mạng không dây kết nối từ tòa nhà chính của trường tới các lớp học di động cho phép các cấu hình mềm dẻo và giá chỉ bằng một phần nhỏ của việc kéo cáp.

Kết nối bằng mạng không dây rất có lợi cho không gian của văn phòng tạm. khi các công ty mọc lên, thường là các văn phòng có diện tích nhỏ hẹp, và cần chuyển vài nhân viên tới nơi gần đó, như là gần kế văn phòng hoặc trên tầng trên. Cài đặt Cat5 hoặc cáp quang cho những giai đoạn không hiệu quả, và thường những chủ nhân của tòa nhà không cho phép cắt bỏ những cáp đã cài đặt. Với mạng không dây,

thành phần của mạng có thể ngừng và chuyển đi tới một nơi khác nhanh chóng và dễ dàng.

Có nhiều tổ chức đã ứng dụng hiệu quả những mạng di chuyển, như là SuperBowl, the Olympics, rạp xiếc, các lễ hội, hội chợ, các công ty xây dựng,…

Chương 2 :
CÁC TẦNG CỦA MẠNG KHÔNG DÂY

2.1 CÁC TẦNG CỦA MẠNG HỮU TUYẾN

2.1.1 TẠI SAO PHẢI CẦN CÁC CHUẨN MẠNG ?

Ngày nay, công nghệ sản xuất ngày càng khác nhau. Các công ty phần mềm ngày càng cung cấp các dịch vụ và các ứng dụng khác nhau. Các chuẩn mạng giúp cho phần cứng và phần mềm có thể làm việc tương thích với nhau một cách hiệu quả, và giúp cho các hãng máy tính khác nhau có thể kết nối được với nhau và có thể chia sẻ tài nguyên và thông tin nếu muốn. Các chuẩn mạng còn giúp cho các máy tính bảo mật thông tin một cách hiệu quả.

2.1.2 NHỮNG TỔ CHỨC CHUẨN PHỔ BIẾN

- The **CCITT** (**I**nternational **C**onsulative **C**ommittee for **T**elegraphy and **T**elephony) : Ủy Ban tư vấn Quốc Tế về điện thoại và điện báo. CCITT là một bộ phận của ITU (Tổ chức Truyền thông Quốc tế), có lịch sử từ năm 1865. Trong những năm đó, có 20 nước tán thành về chuẩn hóa mạng điện tín. ITU được thành lập như là một phần của thỏa thuận này để triển khai việc chuẩn hóa. Trong những năm tiếp theo ITU tập trung vào xây dựng những qui định về điện thoại, liên lạc vô tuyến và phát thanh. Vào năm 1927, ITU tập trung vào việc cấp phát tần số cho các dịch vụ radio, gồm radio cố định, radio di động (hàng hải và hàng không), phát thanh và radio nghiệp dư. Trước đây gọi là ITU (International Telegraph Union - Hội Điện Báo Quốc Tế), vào năm 1934 hội này đổi tên thành International Telecommunication Union - Hiệp Hội Truyền Thông Quốc Tế) nhằm xác định chính xác hơn vai trò của nó trong tất cả các vấn đề truyền thông, kể cả hữu tuyến, vô tuyến, cáp quang, và các hệ điện từ.

Sau chiến tranh thế giới lần hai, ITU trở thành một cơ quan đặc biệt của Liên hiệp Quốc và chuyển tổng hành dinh sang Geneva. Cũng trong thời gian nầy, cơ quan nầy đã lập bảng cấp phát tần số (Table of Frequency Allocations), cấp phát các dải tần số cho từng dịch vụ radio. Bảng này nhằm tránh sự giao thoa giữa liên lạc trên không và dưới đất, các điện thoại trong xe, viễn thông đường biển, các trạm radio, và viễn thông vũ trụ.

Sau đó, vào năm 1956, hai ủy ban riêng biệt của ITU, CCIF (Consultative Committee For International Telephony - Ủy Ban Cố Vấn Cho Điện Thoại Quốc Tế) và CCIT (Consultative Committee For International Telegraph Ủy Ban Cố Vấn Cho Thư Tín Quốc Tế) đã hợp nhất thành CCITT (Consultative Committee For Internationaltelephony And Telegraph) để quản lý hữu hiệu hơn điện thoại và điện tín viễn thông.

Vào năm 1993, ITU được tổ chức lại và tên tiếng pháp được đổi thành ITU-T, nghĩa trong tiếng Anh là ITU's Telecommunications Standardization Sector. Hai bộ phận khác cũng hình thành trong thời gian này là ITU-R (Radiocommunications Sector) và ITU-T (Development Sector).

Mặc dù ngày nay ITU-T đang xây dựng các đề nghị và các chuẩn, các đề nghị của CCITT vẫn thường xuyên được đề cập hơn.

- **I**nstitue of **E**lectric and **E**lectronic **E**ngineers) **IEEE -** Viện kỹ thuật điện và điện tử. IEEE là một tổ chức của nước Mỹ chuyên phát triển nhiều loại tiêu chuẩn, trong đó có các tiêu chuẩn về truyền dữ liệu. Nó gồm một số ủy ban chịu trách nhiệm về việc phát triển những dự thảo về mạng LAN, chuyển sang cho ANSI (American National Standards Institute) để được thừa nhận và được tiêu chuẩn hoá trên toàn nước Mỹ. IEEE cũng chuyển các dự thảo cho ISO (International Organization for Standardization).

IEEE Computer Society là một nhóm các chuyên gia công nghiệp cùng theo đuổi mục tiêu thúc đẩy các công nghệ truyền thông. Tổ chức này tài trợ cho các nhà xuất bản sách, các hội nghị, các chương trình giáo dục, các hoạt động địa phương, các ủy ban kỹ thuật.

- **A**merican **N**ational **S**tandards **I**nstitute – **ANSI :** Viện tiêu chuẩn quốc gia Hoa Kỳ. ANSI giữ vai trò của một tổ chức có nhiệm vụ định nghĩa các chuẩn mã và các chiến lược truyền tín hiệu tại Liên bang Hoa Kỳ; đồng thời nó đại diện cho Liên bang Hoa Kỳ tại ISO (International Organization for Standardization - Tổ chức Quốc tế về Tiêu chuẩn) và trong ITU (International Telecommunications Union - Liên đoàn Viễn thông Quốc tế). ANSI đã tham gia với tư cách một thành viên sáng lập của ISO và đóng một vai trò nổi bật trong việc quản trị của tổ chức này. Nó giữ một trong năm ghế thường trực tại Hội đồng Quản trị OSI. ANSI thúc đẩy việc sử dụng các tiêu chuẩn Liên bang ra toàn cầu, bảo vệ chính sách và các quan điểm kỹ

thuật của Liên bang tại các tổ chức tiêu chuẩn vùng và quốc tế, và khuyến khích việc thừa nhận các tiêu chuẩn quốc tế như các tiêu chuẩn quốc gia khi những tiêu chuẩn này phù hợp các đòi hỏi của cộng đồng người dùng.

Theo ANSI, "nó không tự phát triển các Chuẩn Quốc gia Hoa kỳ; nó tạo điều kiện cho sự phát triển bằng cách thiết lập sự nhất trí giữa những nhóm được công nhận. Viện đảm bảo rằng những nguyên lý chủ đạo của nó - sự nhất trí, qui trình và sự cởi mở đúng đắn - được tuân thủ bởi hơn 175 tổ chức riêng biệt hiện được chỉ định bởi Liên bang...". Các tiêu chuẩn Liên bang được đưa ra tại các tổ chức tiêu chuẩn quốc tế bởi ANSI, ở đó chúng có thể được thừa nhận toàn bộ hay một phần như các tiêu chuẩn quốc tế. Những người tình nguyện từ nền công nghiệp và chính quyền thực hiện phần lớn công trình kỹ thuật, do đó công trình của ANSI sẽ thành công hay không phụ thuộc chủ yếu vào số lượng tham gia từ nền công nghiệp Liên bang và chính quyền Liên bang.

- **I**nternational **O**rganization for **S**tandardization - **ISO** : Tổ chức Quốc tế về Tiêu chuẩn. ISO là một liên đoàn quốc tế các tổ chức quốc gia về tiêu chuẩn, gồm các đại diên của trên 100 quốc gia. Nó là một tổ chức phi chính phủ được xây dựng vào năm 1947 với nhiệm vụ đẩy mạnh việc phát triển của các tiêu chuẩn quốc tế để thúc đẩy sự trao đổi thành quả và các dịch vụ giữa các quốc gia, và để phát triển việc hợp tác toàn cầu của các hoạt động tri thức, khoa học, công nghệ và kinh tế. Nó thúc đẩy môi trường mạng mở để các hệ thống máy tính khác nhau truyền thông với nhau bằng các giao thức được chấp nhận trên toàn thế giới bởi các thành viên ISO.

2.1.3 MÔ HÌNH ISO (Liên kết các hệ thống mở)

Tổ chức ISO là một liên đoàn toàn cầu chuyên môn đề ra các tiêu chuẩn quốc tế. Vào đầu thập niên 80, nó bắt đầu làm việc trên một tập hợp các giao thức phục vụ cho các môi trường mạng mở, cho phép các nhà kinh doanh hệ thống truyền thông bằng máy tính liên lạc với nhau thông qua các giao thức truyền thông đã được chấp nhận trên bình diện quốc tế. Cuối cùng tổ chức nầy phát triển ra mô hình tham khảo OSI.

Mô hình OSI định nghĩa kiến trúc nhiều lớp. Các giao thức được định nghĩa trong mỗi tầng có trách nhiệm về các vấn đề sau:

Truyền thông với các tầng giao thức ngang hàng đang hoạt động trên máy đối tác.

Cung cấp các dịch vụ cho các tầng trên nó (ngoại trừ mức cao nhất là tầng ứng dụng).

Peer-layer communication (truyền thông giữa các tầng ngang hàng) cung cấp phương pháp để mỗi tầng trao đổi các thông điệp hay dữ liệu khác. Ví dụ, transport protocol (giao thức chuyển tải) có thể gửi một thông báo "pause transmission" (ngưng truyền tải) đến giao thức ngang cấp với nó tại máy gởi (máy đang gửi tin đến). Rõ ràng là mỗi tầng không có một dây dẫn vật lý giữa nó và tầng cùng cấp trong hệ thống đối diện. Để gửi một thông điệp, transport protocol phải đặt thông điệp này trong một gói tin rồi chuyển nó qua tầng bên dưới. Như vậy, các tầng thấp phục vụ tầng cao hơn bằng cách nhận lấy các thông điệp của chúng và chuyển các thông điệp trong khối giao thức xuống tầng thấp nhất, ở đây các thông điệp được truyền tải qua các kết nối vật lý.

Chú ý rằng OSI chỉ là mô hình tham khảo, nghĩa là nó đưa ra các mô tả tổng quát của các dịch vụ phải được cung cấp tại mỗi tầng, nhưng nó không định nghĩa bất cứ tiêu chuẩn giao thức nào. Mặc dù ISO đã đưa ra một tập hợp các giao thức theo mô hình, tuy nhiên chúng vẫn chưa phải là định nghĩa. Thêm nữa, OSI là mẫu tham khảo nên nó thường được sử dụng để mô tả các loại giao thức khác như TCP/IP. Ví dụ, IP (Internet Protocol) được gọi là tầng giao thức mạng bởi vì nó hoàn thành các nhiệm vụ được định nghĩa trong tầng mạng của mô hình OSI.

Cũng chú ý rằng trong khi mô hình OSI thường được sử dụng để tham khảo, các giao thức mà OSI tạo ra vẫn chưa trở thành phổ biến cho liên mạng, trước nhất bởi vì tính phổ biến của bộ giao thức TCP/IP. Cho đến bây giờ, mô hình OSI vẫn được mô tả ở đây bởi vì nó định nghĩa được cách các giao thức truyền thông hoạt động như thế nào một cách tổng quát.

2.1.4 ***CÁC TẦNG*** :

Mỗi tầng của mô hình OSI được mô tả ở đây về những gì nó định nghĩa. Nhớ rằng ISO đã định nghĩa các giao thức của riêng nó, nhưng những thứ này không được sử dụng rộng rãi trong công nghệ máy tính. Những giao thức phổ biến hơn TCP/IP và IPX được đề cập với mối liên quan đến tầng mà chúng thuộc về. Dưới đây, để cho rõ ràng, tầng thấp nhất, tầng vật lý (physical layer) được đề cập trước.

TẦNG VẬT LÝ (Physical Layer) : Định nghĩa các đặc tính vật lý của giao diện, như các thiết bị kết nối, những vấn đề liên quan đến điện như điện áp đại diện là các số nhị phân, các khía cạnh chức năng như cài đặt, bảo trì và tháo dỡ các nối kết vật lý. Các giao diện của tầng vật lý gồm EIA RS-232 và RS-499, kế thừa của RS-232. RS-449 cho phép khoảng cách cáp nối dài hơn. Hệ thống LAN (Local Network Area: mạng cục bộ) phổ biến là Ethernet, Token Ring, và FDDI (Fiber Distributed Data Interface).

TẦNG LIÊN KẾT DỮ LIỆU (Data Link Layer) : Định nghĩa các nguyên tắc cho việc gửi và nhận thông tin băng qua các nối kết vật lý giữa 2 hệ thống. Mục đích chính của nó là phân chia dữ liệu gửi tới bởi các tầng mạng cao hơn thành từng frame (khung thông tin) và gửi các khung đó băng qua các nối kết vật lý. Dữ liệu được chia khung để truyền đi mỗi lần 1 khung. Tầng liên kết dữ liệu tại hệ thống nhận có thể báo cho biết đã nhận được một khung trước khi hệ thống gửi đến một khung khác. Chú ý rằng tầng liên kết dữ liệu là một liên kết từ điểm này đến điểm kia giữa hai thực thể. Tầng kế tiếp, tầng mạng - quản lý các liên kết điểm-điểm trong trường hợp các khung được truyền qua nhiều nối kết để đến đích. Trong phạm vi truyền thông mạng máy tính như của Ethernet, tầng thứ cấp MAC (medium access control: điều khiển truy cập môi trường) được bổ sung cho phép thiết bị chia sẻ và cùng sử dụng môi trường truyền thông.

TẦNG MẠNG (Network Layer) : Trong khi tầng liên kết dữ liệu được sử dụng để điều khiển các liên lạc giữa hai thiết bị đang trực tiếp nối với nhau, thì tầng mạng cung cấp các dịch vụ liên mạng. Những dịch vụ này bảo đảm gói tin sẽ đến đích của nó khi băng qua các liên kết điểm-điểm, ví dụ như có một tập hợp các liên mạng nối kết với nhau bằng các bộ định tuyến. Tầng mạng quản lý các nối kết đa dữ liệu một cách cơ bản. Trên một mạng LAN chung, các gói tin đã được đánh địa chỉ đến các thiết bị trên cùng mạng LAN được gửi đi bằng giao thức data link protocol (giao thức liên kết dữ liệu), nhưng nếu một gói tin ghi địa chỉ đến một thiết bị trên mạng LAN khác thì network protocol (giao thức mạng) được sử dụng. Trong bộ TCP/IP protocol, IP là network layer internetworking protocol (giao thức tầng network trên liên mạng). Còn trong bộ IPX/SPX, IPX là network layer protocol.

TẦNG CHUYỂN TẢI (Transport Layer) : Tầng nầy cung cấp quyền điều khiển cao cấp cho việc di chuyển thông tin giữa các hệ thống đầu cuối (end system) trong một phiên truyền thông. Các hệ đầu cuối có thể nằm trên cùng hệ thống mạng hay

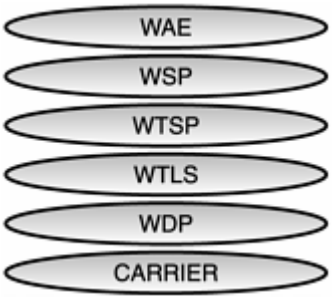
trên các mạng con trên hệ thống liên mạng. Giao thức tầng chuyển tải thiết lập một nối kết giữa nguồn và đích, rồi gửi dữ liệu thành dòng chảy các gói tin, nghĩa là mỗi gói tin được đánh số tứ tự tạo thành một dòng liên tục để có thể theo dõi, bảo đảm phân phối và nhận dạng chính xác trong dòng chảy. Dòng chảy này thường được gọi là "mạch ảo", và mạch này có thể được thiết lập trước xuyên qua các đường dẫn do bộ định tuyến chỉ định trên liên mạng. Giao thức này cũng điều hòa dòng gói tin để thích nghi với các thiết bị nhận chậm và bảo đảm quá trình truyền tải chưa trọn vẹn sẽ được hủy bỏ nếu có sự tranh chấp trong các liên kết xảy ra. (Nói cách khác, nó sẽ tiếp tục cố gắng gửi thông tin đi cho đến khi hết thời gian (time-out). TCP và SPX đều là các giao thức tầng chuyển tải.

TẦNG PHIÊN TRUYỀN THÔNG (Session Layer) : Tầng nầy phối hợp quá trình trao đổi thông tin giữa hai hệ thống bằng cách dùng kỹ thuật trò chuyện hay đối thoại. Các đối thoại có thể chỉ ra nơi bắt đầu truyền dữ liệu nếu nối kết tạm thời bị đứt đoạn, hay nơi kết thúc khối dữ liệu hoặc nơi bắt đầu khối mới. Tầng này là dấu vết lịch sử còn lại từ thiết bị truyền thông đầu cuối (terminal) và máy tính lớn.

TẦNG TRÌNH BÀY (Presentation Layer) : Các giao thức tại tầng này để trình bày dữ liệu. Thông tin được định dạng để trình bày hay in ấn từ tầng này. Các mã trong dữ liệu, như các thẻ hay dãy liên tục các hình ảnh đặc biệt, được thể hiện ra. Dữ liệu được mã hóa và sự thông dịch các bộ ký tự khác cũng được sắp đặt trong tầng này. Giống như tầng phiên truyền thông, tầng này là dấu vết còn lại từ thiết bị truyền thông đầu cuối và máy tính lớn.

TẦNG ỨNG DỤNG (Application Layer) : Các trình ứng dụng truy cập các dịch vụ mạng cơ sở thông qua các chương trình con được định nghĩa trong tầng này. Tầng ứng dụng được sử dụng để định nghĩa khu vực để các trình ứng dụng quản lý truyền tập tin, các phiên làm việc của trạm đầu cuối, và các trao đổi thông điệp (ví dụ như thư điện tử).

2.2 CÁC TẦNG CỦA MẠNG VÔ TUYẾN



Wireless Application Environment (WAE) : Tầng ứng dụng môi trường : Tầng này định nghĩa các chương trình và các tập lệnh sử dụng cho các ứng dụng không dây. Một trong những ngôn ngữ phổ biến nhất là WMLScript.

Wireless Session Protocol (WSP) : Tầng phiên giao thức : Tầng này chịu trách nhiệm về các kiểu thông tin đã thiết lập với các thiết bị. Nó định nghĩa rằng phiên kết nối đó thành công hay không.

Wireless Transaction Session Protocol (WTSP) : Tầng phiên xử lý giao tác : Tầng này dùng để phân loại dữ liệu chảy tràn như một con đường đánh tin cậy hoặc một con đường không đáng tin cậy.

Wireless Transport Layer Security (WTLS) : Tầng truyền tải : Tầng này là tầng bảo mật. Nó cung cấp mã hóa, chứng thực, kiểm tra tính nguyên vẹn của dữ liệu, và hơn thế nữa.

Wireless Dataqram Protocol (WDP) : Tầng giao thức gam dữ liệu : Tầng này là nơi chứa những dữ liệu bị hỏng hóc khi truyền. Vì có nhiều phương pháp truyền khác nhau, WDP không có những tiêu chuẩn hóa chắc chắn, nên bất cứ hãng truyền thông nào cũng có thể chuyển giao dữ liệu vô tuyến miễn là nó tương thích với WAP.

Network carriers : Tầng vận chuyển : Đây là phương pháp vận chuyển chịu trách nhiệm phân phát dữ liệu đến các thiết bị khác. Có rất nhiều phương pháp vận chuyển, bất cứ ai sẽ mang vác miễn là nó liên kết được với tầng WDP.

2.3 BẮT ĐẦU

Một mạng không dây được kết nối với Internet đòi hỏi các thành phần sau: Một kết nối Internet (tốt nhất là băng rộng), một modem, một bộ định tuyến, một tường lửa, một điểm truy nhập không dây và một bộ điều hợp mạng không dây cho máy tính xách tay của bạn (được xây dựng sẵn hoặc PC Card) hoặc cho máy tính để bàn (PCI). Một số hoặc tất cả các thành phần này thường được đóng gói cùng nhau trong một thiết bị.

Những gì bạn cần phải mua để nối mạng không dây tùy thuộc vào những gì bạn đã có. Đối với những người bắt đầu từ đầu, nếu bạn có một kết nối Internet băng

rộng thì bạn đã có modem mà bạn cần, thường là do nhà cung cấp dịch vụ Internet (ISP) của bạn cung cấp. Đây là trường hợp xảy ra đối với phần lớn những người thuê bao băng rộng, cho dù họ sử dụng cáp, DSL hay vệ tinh.

Nếu bạn xem xét việc tự mua modem cho mình, hãy lưu ý rằng nó phải được ISP của bạn phê duyệt vì lý do tương thích mạng. Và nếu bạn thuê một modem từ ISP của bạn, khi nó chết hoặc nếu nhà cung cấp chuyển đổi công nghệ và cần phải nâng cấp modem của bạn thì trách nhiệm thay thế thuộc về nhà cung cấp dịch vụ. Tuy nhiên, nếu bạn đang sử dụng modem của chính mình, bạn sẽ phải tự thay thế trong trường hợp modem đó không hoạt động.

Việc cấu hình một modem mới cũng có thể đòi hỏi phải có sự phối hợp với ISP của bạn. Các công ty cáp cho phép các modem cáp trên các mạng của họ dựa trên địa chỉ MAC (kiểm soát truy nhập đường truyền) của mỗi thiết bị. Khi nhà cung cấp dịch vụ truy nhập cáp mang đến một modem cho bạn, địa chỉ MAC của nó đã được đăng ký sẵn. Nhưng nếu bạn tự mua thiết bị cho mình thì bạn phải được nhà cung cấp dịch vụ cấp phép cho địa chỉ MAC của modem cáp đó trước khi bạn bắt đầu sử dụng nó. Thông thường thì việc này sẽ mất thời gian vì bạn sẽ phải chờ đợi để modem mà bạn tự mua được kích hoạt.

Không giống như cáp, là một môi trường dùng chung, DSL không gặp phải vấn đề xác thực modem. Các nhà cung cấp DSL phải đặt tín hiệu DSL trực tiếp vào đường dây điện thoại của người thuê bao, vì vậy nếu bạn có một tín hiệu, không cần phải thêm sự xác thực để kết nối modem vào mạng, cho dù bạn vẫn phải đăng nhập – không thường là qua PpoE.

2.4 CÁC CỔNG VÀO (GATEWAY)

Với những điều rắc rối phiền hà như vậy mà bạn có thể gặp phải để làm cho modem của bạn tương thích với ISP của bạn thì tại sao bạn phải bận lòng với việc tự mua thiết bị cho mình? Thứ nhất, bạn sẽ tránh được một khoản phí thuê modem hàng tháng. Thứ hai, các sản phẩm tích hợp tất cả các thiết bị và đơn giản hoá quá trình nối mạng tại nhà đang xuất hiện trên thị trường. Vì vậy, nếu bạn đã có modem và sử dụng nó hơn 1 năm và đã sẵn sàng nâng cấp nó hoặc nếu bạn chuẩn bị đăng ký sử dụng băng rộng lần đầu tiên, bạn có thể xem xét việc sử dụng một cổng vào. Một sản phẩm như vậy hoạt động như một modem, một bộ định tuyến, một tường lửa và một điểm truy nhập không dây, hoặc là một tổ hợp khác của những thiết bị

này, tất cả trong một chiếc hộp. Các nhà sản xuất thiết bị phần cứng nối mạng lớn, chẳng hạn như Netgear, Linksys và D-Link, cũng như một số ISP, đang bắt đầu cung cấp những cổng nối kiểu này.

2.5 BỘ ĐỊNH TUYẾN KHÔNG DÂY

Nếu bạn muốn nối mạng không dây nhưng lại không muốn gặp phải những điều rắc rối phức tạp của việc cấu hình một modem mới và máy tính của bạn được cắm trực tiếp vào modem cáp của bạn, bạn nên mua một bộ định tuyến không dây với một tường lửa được tích hợp sẵn. Một bộ định tuyến không dây thường bao gồm một bộ chuyển mạch Ethernet 4 cổng để bạn có thể kết nối các máy tính hữu tuyến của bạn vào điểm truy nhập không dây. Điểm truy nhập không dây này lại kết nối với các máy tính được nối mạng không dây của bạn.

Các bộ định tuyến cho phép bạn chia sẻ một địa chỉ IP đơn được cung cấp bởi ISP của bạn với nhiều máy tính trên mạng của bạn thông qua một cơ chế gọi là Bộ dịch địa chỉ mạng (NAT). NAT giúp đảm bảo an ninh cho bạn trên Internet bởi vì bộ định tuyến cho rằng địa chỉ IP chung được gán bởi ISP của bạn và mỗi máy tính của bạn được gán một địa chỉ IP riêng qua một máy phục vụ DHCP (giao thức cấu hình chủ động) được xây dựng trong bộ định tuyến. Trên Internet chúng ta không thể nhìn thấy những địa chỉ riêng này. Để đảm bảo an ninh, hãy chắc chắn rằng tường lửa của bộ định tuyến sử dụng công nghệ Kiểm tra gói Stateful (SPI) bên cạnh NAT. Một tường lửa SPI kiểm tra mỗi gói dữ liệu đi vào nhằm đảm bảo rằng nó tương ứng với một yêu cầu được gửi ra. Những yêu cầu không mong muốn được ngăn ngừa không cho xâm nhập vào mạng của bạn.

2.6 CÁC ĐIỂM TRUY CẬP

Nếu bạn đã có một mạng hữu tuyến đang hoạt động bình thường và bạn hài lòng với chiếc modem, bộ định tuyến và tường lửa mà bạn đang dùng thì tất cả những gì bạn cần để nối mạng không dây là một điểm truy nhập (AP). Một AP chỉ có một radio 802.11 được tích hợp và một vài thứ lặt vặt khác. Radio trong thiết bị này hoạt động như một cầu nối giữa mạng hữu tuyến và mạng không dây của bạn, nhận một tín hiệu hữu tuyến và truyền nó vô tuyến. Bạn chỉ việc cắm AP vào bộ định tuyến hữu tuyến hiện có trên mạng của bạn, cấu hình thiết bị để tăng cường an ninh, thế là xong.

2.7 THIẾT BỊ CHO MÁY TÍNH ĐỂ BÀN

Để kết nối máy tính để bàn của bạn với một mạng không dây, bạn có hai lựa chọn. Thứ nhất là một card PCI, nhưng để cài đặt bạn sẽ phải mở thùng máy tính. Đối với một số người sử dụng thì việc này thật đáng ngại. Cũng vậy, chiếc ăng ten thường được bố trí ở phía sau của card PCI, vì vậy nếu chiếc máy PC của bạn được đặt ở dưới bàn của bạn thì tín hiệu mà bạn nhận được có thể sẽ kém hơn so với khi hệ thống của bạn được đặt trên mặt bàn. Một số nhà sản xuất cung cấp một ăng ten ngoài được nối với một card PCI thông qua một cáp đồng trục. Và bạn có thể đặt ăng ten này trên bàn để tín hiệu thu được từ điểm truy nhập mạnh hơn.

Một phương án khác là một bộ điều hợp USB. Việc cài đặt nó chỉ đơn giản là cắm bộ điều hợp này vào một cổng USB trên máy tính của bạn và các tuyến bus trên bo mạch chính sẽ chịu trách nhiệm cấp điện cho bộ điều hợp này.

Một trong những điểm thuận lợi nhất của các bộ điều hợp USB so với các card PCI là quá trình cài đặt đơn giản. Bên cạnh đó, việc thay thế cũng dễ dàng hơn nhiều. Bạn có thể đặt bộ điều hợp không dây USB của bạn ở bất cứ đâu, tuỳ thuộc vào chiều dài dây cáp USB của bạn (tối đa là 15 feet do những hạn chế của USB). Việc này cho phép bạn di chuyển thiết bị này, đồng nghĩa với ăng ten của nó, để thu tín hiệu tốt nhất. Cùng một bộ điều hợp có thể hoạt động trên một máy tính để bàn và một máy tính xách tay.

Đa phần các bộ điều hợp USB trên thị trường sử dụng công nghệ USB 1.1 và hiệu suất bị hạn chế ở chuẩn 802.11b (12 Mbit/s) bởi vì thông lượng "cổ chai" của công nghệ USB 1.1 chậm hơn. Vào thời điểm này, chỉ có một nhà sản xuất đã xuất xưởng một sản phẩm 802.11b/USB 2.0: Buffalo AirStation 54 Mbit/s USB Adapter-G.

2.8 THIẾT BỊ CHO MÁY TÍNH XÁCH TAY

Nhiều máy tính sổ tay mới, thậm chí những mẫu tương đối rẻ, được trang bị một card nối mạng không dây PCI mini tích hợp sẵn. Nhưng trước khi bạn mua máy, bạn cần biết một số điều. Nếu bạn mua một máy tính sổ tay Centrino, bạn sẽ mua công nghệ 802.11b, chứ không phải công nghệ nhanh hơn và mới hơn, 802.11g.

Hiện tại, Intel chỉ cung cấp cho các nhà sản xuất một giải pháp "b", hỗ trợ chuẩn "g" cũng sắp sửa được cung cấp.

Centrino là kết quả của một giải pháp gồm 3 phần: một bộ xử lý Intel Pentium M, một chipset 855GM (bộ điều khiển bộ nhớ đồ hoạ) hoặc chipset 855PM (bộ điều khiển bộ nhớ) và giải pháp 802.11b của Intel là Intel PRO/Wireless 2100. Mặt khác, những máy tính sổ tay không thuộc dòng Centrino có thể tự do cung cấp bất cứ giải pháp không dây nào mà nhà sản xuất muốn và rất nhiều máy đã cung cấp giải pháp "g" mới để có thêm nhiều lợi ích với chi phí tăng thêm không đáng kể.

Nếu bạn định mua một máy tính sổ tay mới, tốt nhất là bạn nên mua loại có giải pháp "g" hoặc kết hợp "a/g". Nó sẽ tiết kiệm cho bạn một khe cắm giành cho PC Card và đảm bảo rằng bạn sẽ có thể nối mạng không dây ở bất cứ đâu có tồn tại một mạng 802.11. Nó bao gồm cả các mạng "b" vì "b" và "g" là có thể hoạt động tương thích với nhau.

Nếu bạn muốn nâng cấp máy tính sổ tay hiện có của bạn để bổ sung tính tương thích không dây, bạn có thể sử dụng một bộ điều hợp USB như đã đề cập ở trên nhưng những thứ đó có phần bất tiện khi bạn phải di chuyển. Có một giải pháp tốt hơn đó là một PC Card mà bạn sẽ cài đặt vào trong khe PCMCIA ở một bên của chiếc máy tính sổ tay. Các card thuộc cả hai loại "g/g" và "g" đều có trên thị trường với giá từ 80 đến 100 đô la Mỹ và mặc dù nó đắt hơn chí phí mà bạn phải bỏ ra cho một card “b” nhưng mạng gia đình của bạn sẽ cho thấy hiệu quả làm việc vượt trội của nó trong tương lai với chỉ một khoản tiền nhỏ phải trả thêm.

2.9 TÌM KIẾM NHÃN Wi-Fi

Cho dù bạn chọn loại thiết bị nào, bạn đều muốn chắc chắn rằng tất cả chúng có thể hoạt động cùng nhau, bất kể nhãn hiệu. Chẳng hạn, nếu bạn có một bộ định tuyến Linksys bạn muốn đảm bảo chắc chắn rằng nó có thể nói chuyện được với PC Card không dây của hãng Cisco mà bạn sử dụng. Đây là lý do để nhãn hiệu Wi-Fi xuất hiện.

Wi-Fi là viết tắt của Wireless Fidelity. Mặc dù thuật ngữ này thường được sử dụng để nói chung về nối mạng không dây, Wi-Fi thực sự là một nhãn hiệu được đăng ký của Liên minh Wi-Fi (http://www.wi-fi.org). Hiệp hội quốc tế phi lợi

nhuận này được thành lập năm 1999 để chứng nhận tính tương thích với nhau của các sản phẩm mạng nội bộ không dây (WLAN) dựa trên các tính năng kỹ thuật 802.11 của IEEE. Liên minh Wi-Fi có một bộ kiểm tra tính tương thích lẫn nhau mà các sản phẩm của các thành viên phải vượt qua để đủ tiêu chuẩn được chứng nhận và có những bài kiểm tra cho những sản phẩm được dựa trên mỗi chuẩn không dây IEEE (và các sản phẩm kết hợp nhiều hơn một chuẩn) cũng như Truy nhập được bảo vệ Wi-Fi (WPA). Bạn chỉ nên mua các sản phẩm có nhãn là đã được chứng nhận bởi Wi-Fi.

2.10 LÀM CHO MỌI THỨ HOẠT ĐỘNG

Khi đã có được tất cả những thiết bị mà bạn cần, bạn đã sẵn sàng để cài đặt mạng không dây của bạn. Dù bạn đã chọn một điểm truy nhập, một cổng nối hay một bộ định tuyến, tuỳ thuộc vào nhu cầu của bạn, bạn nên tìm một điểm tốt nhất cho thiết bị không dây của bạn để ăng ten được bố trí ở vị trí trung tâm so với khu vực phủ sóng mà bạn định sử dụng. Trên thực tế, hầu hết mọi người đều đặt thiết bị trong cùng một phòng có kết nối băng rộng của họ. Bạn hãy chắc chắn rằng thiết bị không bị che khuất đằng sau các vật thể khác. Ăng ten cần phải được đặt ở nơi thoáng đãng nhất để có được hiệu suất tối ưu.

Điều gì sẽ xảy ra nếu bạn không phủ sóng đủ những nơi bạn cần? Tùy thuộc vào kích cỡ của ngôi nhà cũng như những thứ khác như vật liệu xây dựng và số lượng tường, bạn cần phải cắm một điểm truy nhập thứ hai vào kết nối Ethernet hữu tuyến của bạn để phủ sóng tới những khu vực khó tiếp cận, chẳng hạn như sân sau, hay để cải thiện hiệu suất trong những khu vực mà tín hiệu của thiết bị thứ nhất quá yếu. Nhưng đa phần những người dùng không dây chỉ cần một thiết bị cho ngôi nhà của họ.

Nếu bạn dự định sử dụng mạng không dây của mình cho các mục đích truyền thống, chẳng hạn như chia sẻ một máy in và truy nhập băng rộng thì chỉ một thiết bị theo chuẩn "b" là đủ. Tuy nhiên, trong vài năm tới nhu cầu về mạng gia đình sẽ tăng lên để đáp ứng được các yêu cầu như âm thanh và hình ảnh liên tục (streaming). Nếu bạn dự định chắc chắn là bạn sẽ có nhu cầu như vậy với mạng của mình thì bạn cần đầu tư một thiết bị "a/g".

Chương 3 :

BẢO MẬT VÀ QUẢN LÝ MẠNG KHÔNG DÂY

3.1 ACCESS POINT

Access Points (APs) đầu tiên được thiết kế cho các khu trường sở rộng rãi. Nó cung cấp các điểm đơn mà người quản trị có thể cấu hình nó. Nó có những đặc thù cho phép một hoặc hai sóng vô tuyến cho mỗi AP. Về mặt lý thuyết, AP hỗ trợ hàng trăm người dùng cùng một lúc. AP được cấu hình bởi ESSID (Extended Service Set ID). Nó là một chuỗi các nhận dạng mạng không dây. Nhiều người sử dụng chương trình máy khách để cấu hình và có một mật khẩu đơn giản để bảo vệ các thiết lập của mạng.

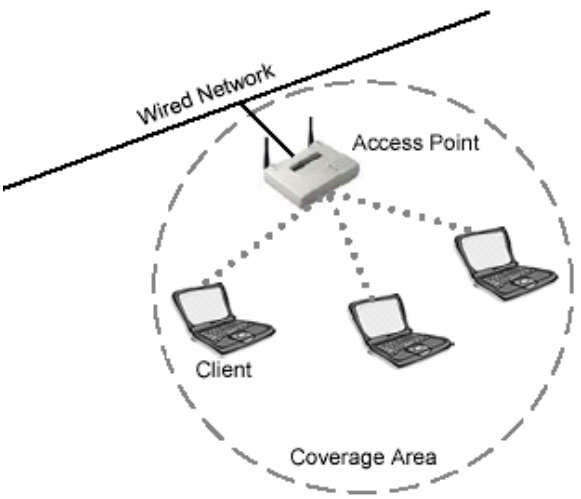
Hầu hết các AP đều tăng cường cung cấp các tính năng, như là :

- Tính năng lọc địa chỉ MAC. Một sóng vô tuyến của máy khách cố gắng truy cập phải có địa chỉ MAC trong bảng địa chỉ của AP trước khi AP cho phép kết hợp với AP.
- Tính năng đóng mạng. Thông thường, một máy khách có thể chỉ định một ESSID của bất cứ sự kết hợp nào với bất cứ một mạng hiện hữu nào. Trong tính năng đóng mạng, máy khách phải chỉ định ESSID rõ ràng, hoặc nó không thể kết hợp với AP.
- Tính năng Anten ngoài.
- Tính năng kết nối liên miền.
- Bản ghi mở rộng, thống kê, và thực hiện báo cáo.

Access point

Một tính năng tăng cường khác bao gồm quản lý khóa WEP động, khóa mã hóa trao đổi công cộng, kết ghép kênh, và các đồ chơi trẻ con khác. Nhưng đáng tiếc, những kiểu mở rộng hoàn toàn các hãng sản xuất (kiểu mẫu), và không có bảo hộ bởi bất cứ chuẩn nào, và không hoạt động với các sản phẩm khác. Điều đó có nghĩa là, một máy khách phải kết hợp nó với một AP, và nó sẽ không đi xa hơn các hạn chế của AP trên những dịch vụ mà máy khách có thể truy cập.

APs là sự lựa chọn lý tưởng cho những mạng cá nhân với nhiều máy khách đặt trong một khoảng không vật lý, đặc biệt là các đoạn mạng có cùng Subnet (giống như là doanh nghiệp hoặc khu trường sở). AP cung cấp mức độ điều khiển cao để có thể truy cập bằng dây, nhưng giá của nó không rẻ (giá trung bình của một AP từ 800 đến 1000 USD).



Mô hình cài đặt Access Point

Một lớp khác của AP thỉng thoảng được xem như là cổng nhà riêng. The Apple AirPort, Orinoco RG-1000 và Linksys WAP11 là các ví dụ cụ thể của các AP cấp thấp. Các sản phẩm này phải có giá thành thấp hơn các sản phẩm thương mại khác. Nhiều Modems được sản xuất, cho phép truy cập mạng không dây bằng cách quay số. Những dịch vụ cung cấp cân bằng nhất là Network Address Translation (NAT), DHCP, và dịch vụ cầu nối cho các máy khách. Trong khi các dịch vụ đó không thể hỗ trợ đồng thời nhiều máy khách như là AP cao cấp, thì chúng lại có thể cung cấp truy cập rẻ và đơn giản cho nhiều ứng dụng. Cấu hình một AP không đắt tiền cho kiểu bắt cầu mạng cục bộ, bạn có trình độ điều khiển cao hơn các máy khách riêng lẻ để có thể truy cập mạng không dây.

Không kể những AP giá cao, những AP là nơi để xây dựng hệ thống thông tin mạng không dây. Chúng là một dãy đặc biệt tốt để điều khiển sự lặp lại các vị trí, vì chúng dễ dàng cấu hình, tiêu thụ năng lượng thấp, và thiếu những bộ phận di chuyển.

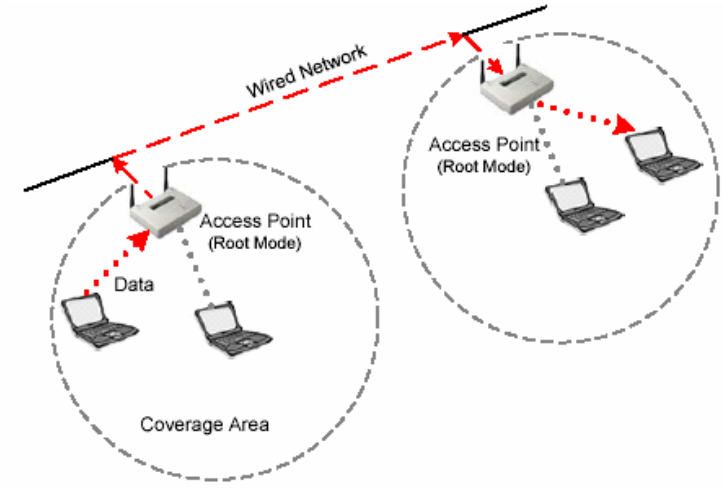
3.1.1 CÁC MODE CỦA AP

APs thông tin với những máy khách, với mạng hữu tuyến, và với một AP khác. Có ba chế độ trong AP mà chúng ta có thể cấu hình :

- Chế độ gốc
- Chế độ lặp
- Chế độ cầu nối

3.1.1.1 CHẾ ĐỘ GỐC (ROOT MODE)

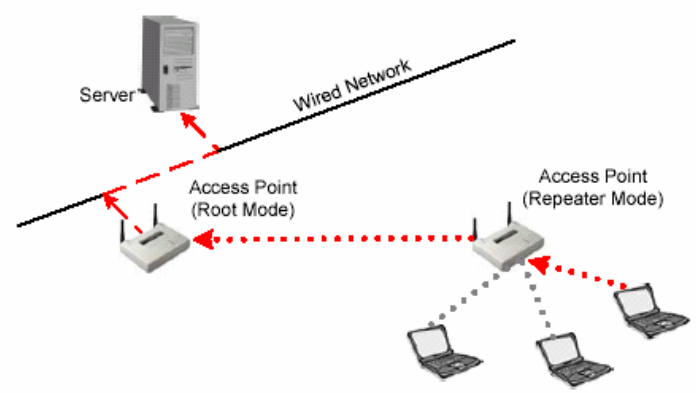
Chế độ gốc được dùng khi AP kết nối với mạng xương sống thông qua giao diện mạng cục bộ. Những AP mới nhất hỗ trợ những chế độ cao hơn chế độ gốc cũng cấu hình từ chế độ gốc mặc định. Khi AP kết nối tới đoạn mạng hữu tuyến thông qua cổng cục bộ, nó sẽ cấu hình mặc định ở chế độ gốc. Khi trong chế độ gốc, AP kết nối tới những đoạn mạng phân bổ giống nhau để có thể giao tiếp với các đoạn mạng khác. AP giao tiếp với mỗi chức năng lang thang có sắp xếp như là kết hợp lại. Các máy khách có thể thông tin với các máy khách khác ở các ô khác nhau thông qua AP tương ứng để đi qua đoạn mạng hữu tuyến.



Access Point trong chế độ gốc

3.1.1.2 CHẾ ĐỘ LẶP (REPEATER MODE)

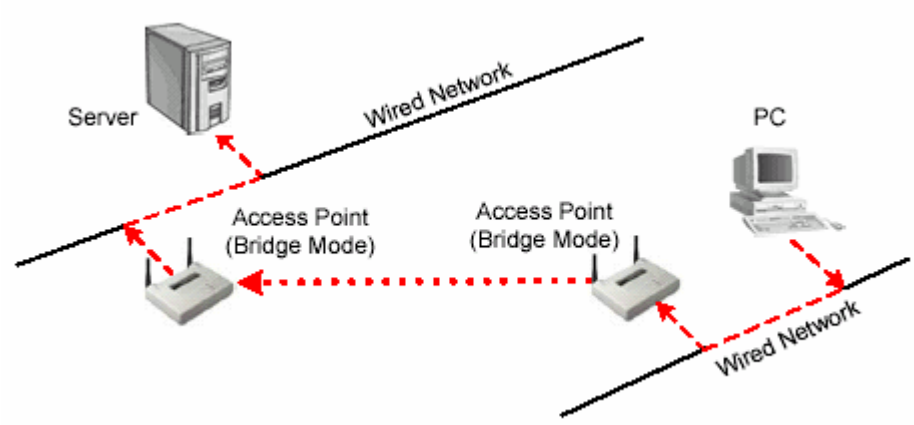
Trong chế độ lặp, APs có khả năng cung cấp những liên kết ngược trong mạng hữu tuyến khá hơn một liên kết hữu tuyến bình thường. Một AP được thỏa mãn như là một AP gốc và các AP khác giống như là các bộ lặp. AP ở chế độ lặp kết nối tới máy khách như là một AP và kết nối tới AP gốc ngược như là chính máy khách. Không đề nghị sử dụng AP ở chế độ lặp trừ khi cần sự tuyệt đối an toàn bởi vì các ô xung quanh mỗi AP trong viễn cảnh này phải được chồng lấp nhỏ nhất là 50%. Cấu hình này phải đủ mạnh để giảm bớt các kết nối của các máy khách tới AP ở chế độ lặp. Ngoài ra, AP ở chế độ lặp là sự truyền đạt với những máy khách chẳng khác gì AP ngược với liên kết không dây, giảm số lượng trên một đoạn mạng không dây. Người dùng gắn bó với AP ở chế độ lặp sẽ có kinh nghiệm hạn chế số lượng và những sự tiềm tàng cao trong viễn cảnh này. Đây là điển hình để vô hiệu hóa mạng cục bộ hữu tuyến trong chế độ lặp.



Access Point trong chế độ lặp

3.1.1.3 CHẾ ĐỘ CẦU NỐI (BRIGDE MODE)

Trong chế độ cầu nối, APs hành động chính xác như là những chiếc cầu không dây. Trên thực tế, nó trở thành những chiếc cầu không dây trong khi cấu hình trong kiểu đó. Chỉ có một số lượng nhỏ AP có chức năng cầu nối, sự trang bị có ý nghĩa so với giá phải trả. Các máy khách không kết hợp với nhữngcấu nối, nhưng đúng hơn, những cầu nối sử dụng liên kết hai hoặc nhiều hơn đoạn mạng hữu tuyến với mạng không dây.



Access Point trong chế độ cầu nối

AP được coi như là một cái cổng bởi vì nó cho phép máy khách kết nối từ mạng 802.11 đến những mạng 802.3 hoặc 802.5. AP có sẵn với nhiều chọn lựa phần cứng và phần mềm khác nhau.

3.2 BẢO MẬT

Trước đây, cài đặt thiết bị không dây thường là một việc vô cùng phức tạp nhưng trong vài năm trở lại đây, các nhà sản xuất đã cố gắng đơn giản hoá quá trình này một cách đáng kể. Thực tế, nhiều sản phẩm sẽ hoạt động tốt khi bạn lấy chúng ra khỏi hộp, đọc hướng dẫn, cắm đúng cáp vào đúng đầu nối và khởi động lại thiết bị của bạn theo đúng trình tự. Phần lớn các nhà sản xuất phần cứng nối mạng không dây cung cấp các trình thuật sĩ "dễ làm theo" để giúp bạn hoàn thành quá trình cài đặt và rất nhiều nhà sản xuất cung cấp hỗ trợ kỹ thuật 24 giờ/ngày, 7 ngày/tuần.

Để quá trình cài đặt dễ dàng nhất có thể, hầu hết các nhà sản xuất khi xuất xưởng các sản phẩm của họ đều đặt tất cả các lựa chọn an ninh ở chế độ tắt. Vì vậy, các mạng gia đình khi được lắp đặt xong là hoàn toàn không được bảo vệ. ở mức tối thiểu, bạn cũng cần phải thay đổi tên mạng mặc định (SSID) và mật khẩu của người quản trị-cả hai thứ này được giới hacker biết rất rõ-và đặt chế độ an ninh ở mức cao nhất mà các sản phẩm hỗ trợ. Bảo vệ tương đương hữu tuyến (WEP) hiện là tính năng an ninh được sử dụng rộng rãi nhất trong các thiết bị gia đình. Nhưng tất cả các sản phẩm mới sẽ sớm hỗ trợ WPA (truy nhập được bảo vệ không dây) thay thế.

Hơn một năm trước, những nhà phân tích và truyền thông đã có văn bản và xuất bản có tính chất có hại đến mạng không dây, như là tính mã hóa có thể bị bẻ gãy và những kẻ xâm nhập AP để kết nối tới mạng của bạn. Chú ý những điều nguy hiểm của WLAN dẫn tới khả năng vài hãng sẽ chính thức cấm WLAN hoàn toàn, nhưng bất cứ một tổ chức nào cũng sử dụng máy tính xách tay, điều đó là nguy hiểm ví nó dễ dàng trở thành những trạm không dây dẫn tới sự rủi ro cho việc bảo mật.

Tuy nhiên, sự bảo mật – các hãng đã nhận ra là phải củng cố mạng không dây của họ với những lớp gần như bảo mật. Điều đó có nghĩa là chấp nhận những bảo mật thực tiễn của mạng hữu tuyến. Tầng này gần như bảo mật những địa chỉ của những thành phần trong mạng bởi khóa ngay từ vành đai của WLAN, bảo mật thông tin qua WLAN, và kiểm tra lưu lượng mạng.

Trên thực tế, Gartner đã phát thảo ra ba đề nghị “phải” cho mạng không dây WLAN :

1) Cài đặt một tường lửa quản lý trung tâm trên tất cả các mát tính xách tay gắn card mạng không dây hoặc tích hợp. Điều này chống lại các kết nối ad

hoc (kết nối ngang hàng) và sự tấn công từ internet khi người dùng kết nối tới những nhà cung cấp internet.

2) Thực hiện dò tìm sự xâm phạm đến WLAN để khám phá sự xâm nhập AP, các thiết bị ngoại vi kết nối đến một nhóm các AP và ngẫu nhiên kết hợp với những AP gần chúng và những Ap này sẽ được sử dụng bởi các công ty khác.

3) Bật tính năng mã hóa và chứng thực hổ trợ cho việc sử dụng WLAN.

3.2.1 CÁC GIẢI PHÁP BẢO MẬT

3.2.1.1 WEP

WEP là một phương tiện như điểm đầu mút của giải pháp bảo mật mạng không dây. Môi trường bảo vệ không dây chỉ với WEP là môi trường không bảo mật. Khi sử dụng WEP, không sử dụng các khóa của WEP liên quan tới SSID hoặc tới tổ chức. Tạo các khóa WEP rất khó khăn để nhớ. Trong nhiều trường hợp, khóa WEP có thể dễ dàng đoán ra khi nhìn SSID hoặc tên của tổ chức.

WEP là một giải pháp hiệu quả cho việc giảm sự rình mò lén lút. Bởi vì một kẻ xấu cố gắng truy cập, nhưng chỉ có thể nhìn thấy được mạng của bạn, sẽ không thấy được khóa WEP, mà một cá nhân sẽ bị ngăn chặn nếu truy cập mạng mà không có khóa WEP.

3.2.1.2 KÍCH THƯỚC Ô

Trong lệnh giảm bớt cơ hội nghe trộm, người quản trị mạng nên chắc chắn rằng những kích thước ô của những AP là thích hợp. Phần lớn những hacker tìm kiếm các vị trí rất nhỏ và khả năng bị mất năng lực trong mạng để tấn công. Vì lí do đó, điều quan trọng là AP sẽ không phát ra những tín hiệu dư thừa để chuyển những gói tin cho tổ chức (hoặc những vị trí không bảo mật) trừ khi rất cần thiết. Vài mức AP của doanh nghiệp cho phép cấu hình nguồn điện xuất, với những điều khiển có hiệu quả với kích cỡ của ô RF (Radio Frequency) xung quanh AP. Nếu kẻ nghe trộm gói dữ liệu không thể tìm ra mạng của bạn, lúc đó mạng của bạn sẽ không dễ bị tấn công.

Điều này có thể thúc giục những nhà quản trị luôn luôn sử dụng nguốn điện xuất thiết lập trên tất cả các thiết bị WLAN trong việc cố gắng đặt một thông lượng cực

đại và mức độ bao phủ, nhưng những cấu hình không nhìn thấy sẽ dẫn đến sự phí tổn bảo mật. Một AP phải có một kích cỡ ô để có thể điều khiển bởi lượng nguồn điện mà AP phát ra và lợi ích của việc sử dụng ăng ten. Nếu ô đó không phù hợp với điểm mà khách qua đường tìm thấy, hoặc sẽ truy cập một cách trơn tru, thì chỗ yếu của mạng đó không cần thiết để bị tấn công. Kích thước ô thích hợp nên được ghi lại cùng với các cấu hình của AP hoặc cầu nối cho mỗi phần của khu vực. Điều này có thể cần thiết để cài đặt hai AP với khích thước ô nhỏ hơn nhằm ngăn ngừa để có thể bảo mật những chỗ yếu trong vài trường hợp.

Cố gắng định vị những AP của bạn về phía trung tâm nhà bạn hay trung tâm của văn phòng chính. Điều này sẽ giảm thiểu sự rò rỉ tín hiệu ra ngoài vùng kiểm soát. Nếu bạn đang sử dụng ăng ten ngoài, hãy chọn kiểu đúng của ăng ten có thể hữu ích cho việc giảm thiểu sự rò rỉ tín hiệu. Tắt AP khi không sử dụng. Điều này sẽ giảm thiểu sự phơi bày cho các hacker và giảm gánh nặng cho việc quản lý mạng.

3.2.1.3 CHỨNG THỰC NGƯỜI DÙNG

Từ khi sự chứng thực người dùng là liên kết kém cỏi nhất của WLAN, và chuẩn 802.11 không chỉ định các phương pháp chứng thực người dùng, thì đó là điều cấp bách mà người quản trị mạng thực thi chứng thực người dùng cơ bản ngay khi có thể thực hiện được trong lúc đang cài đặt cơ sở hạ tầng WLAN. Chứng thực người dùng cơ bản nên thực hiện trên các lược đồ thiết bị độc lập như là tên và mật khẩu người dùng, card thông minh, các hệ thống mã thông báo cơ bản (token-based) hoặc vài kiểu bảo mật khác như là nhận diện người dùng, không qua phần cứng. Giải pháp bạn thực thi nên hỗ trợ chứng thực hai chiều giữa chứng thực máy chủ (như là RADIUS) và chứng thực máy khách không dây.

RADIUS trên thực tế là một chuẩn trong hệ thống chứng thực người dùng tốt nhất trong thị trường công nghệ thông tin. Những AP gửi các yêu cầu chứng thực người dùng tới các máy chủ RADIUS, có thể xây dựng cơ sở dữ liệu người dùng hay cấp phép cho các yêu cầu chứng thực thông qua người điều khiển trung tâm (Domain Controller – DC), như là máy chủ NDS, máy chủ AD (Active Directory), hoặc ngay cả LDAP.

Người quản trị của máy chủ RADIUS có thể rất đơn giản hoặc rất phức tạp, quyết định bởi sự bổ sung. Bởi vì các giải pháp bảo mật không dây dễ bị ảnh hưởng, vì thế nên cẩn trọng khi chọn giải pháp máy chủ RADIUS để chắc rằng người quản

trị mạng có thể quản trị nó hoặc có thể làm việc hiệu quả với một máy chủ RADIUS có sẵn.

3.2.2 NHU CẦU BẢO MẬT

Chọn một giải pháp bảo mật mà thích hợp với nhu cầu và ngân sách của công ty, cả cho hiện tại và mai sau. WLAN phổ biến có ích đến mức là một phần chắc chắn vì chúng có thể bổ sung thoải mái. Điều đó có nghĩa là WLAN đã bắt đầu bằng một AP và 5 máy khách rồi phát triển tới 15 AP và 300 máy khách. Những kỹ thuật bảo mật giống nhau làm việc chỉ tốt cho môt AP sẽ không thể chấp nhận được, hoặc khi bảo mật, cho 300 người dùng. Một tổ chức có thể sẽ tốn nhiều tiền cho các giải pháp bảo mật khi mà chúng phát triển nhanh chóng như là WLAN. Trong nhiều trường hợp, những tổ chức đã thật sự có sự bảo mật như là kiểm tra sự xâm nhập hệ thống, tường lửa, và máy chủ RADIUS.

3.2.3 SỬ DỤNG THÊM CÁC CÔNG CỤ BẢO MẬT

Nắm được sự thuận lợi của các công nghệ, như là VPN, tường lửa, kiểm tra sự xâm nhập hệ thống – Intrustion Detection Systems (IDS), những chuẩn và giao thức như là 802.1x và EAP, và chứng thức máy khách với RADIUS có thể giúp tạo nên các giải pháp bảo vệ cao và xa hơn chuẩn 802.11 yêu cầu. Chi phí và thời gian là phương tiện cho các giải pháp tốt hơn từ các giải pháp SOHO đến các giải pháp cho các doanh nghiệp lớn.

3.2.4 THEO DÕI VIỆC LỪA ĐẢO PHẦN CỨNG

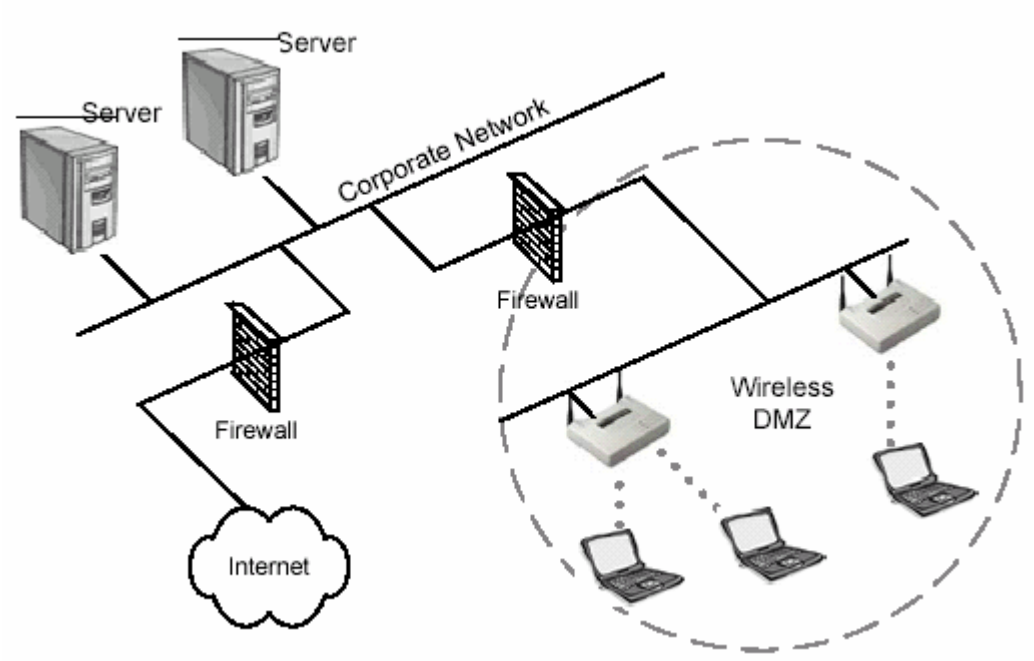
Phát hiện ra các AP lừa đảo, sự phát hiện ra các phiên của AP nên lập biểu nhưng không loan báo. Khám phá sự hoạt động và xóa các AP lừa đảo, sẽ giống như là loại bỏ hacker và cho phép người quản trị điều khiển duy trì mạng và bảo mật. Các kiểm định bảo mật nên được thực hiện cho các cấu hình không đúng của các AP mà các cấu hình này có thể gây nên sự nguy hiểm cho việc bảo mật. Tác vụ này có thể kết thúc trong khi theo dõi các AP lừa đảo như là một phần của một sự bảo mật bình thường. Các cấu hình hiện tại nên được so sánh đến các cấu hình trong quá khứ để có thể biết nếu người dùng hoặc hacker cấu hình lại AP. Việc ghi lại các truy cập nên là phương tiện và theo dõi cho mục đích của sự tìm ra bất cứ sự truy cập không chính đáng nào trên các đoạn mạng không dây. Kiểu theo dõi này có thể giúp tìm ra sự những thiết bị máy khách không dây đã mất hoặc bị lấy trộm.

3.2.5 SWITCH, KHÔNG PHẢI HUB

Một sự chỉ dẫn đơn giản khác là luôn luôn kết nối các AP với các Swicth thay vì các Hub. Các Hub là các thiết bị phát rộng, mỗi gói tin được nhận bởi một Hub sẽ được gửi cho tất cả các Hub khác. Nếu những AP đã kết nối đến Hub, thì mỗi gói tin đi qua đoạn mạng hữu tuyến sẽ bị phát tán. Chức năng này cho đem lại cho các hacker có được các thông tin như là mật mã và những địa chỉ IP.

3.2.6 DMZ KHÔNG DÂY

Một ý tưởng khác trong công cụ bảo mật cho các đoạn mạng WLAN là một tạo vùng phi quân sự không dây – Wireless Demilitarized zone (WDMZ). Tạo những WDMZ sử dụng tường lửa hoặc những bộ định tuyến (Router) có thể phụ thuộc vào chi phí của các công cụ. Những WDMZ là các công cụ thông thường trong sự triển khai sắp xếp trung bình – và lớn – của WLAN. Bởi vì các AP về cơ bản không có bảo mật và những thiết bị không đáng tin cậy, những AP này tách rời với các đoạn mạng khách bởi một thiết bị tường lửa.



DMZ không dây

3.2.7 PHẦN MỀM HỆ THỐNG VÀ NÂNG CẤP PHẦN MỀM

Nâng cấp phần mềm hệ thống và các bộ phận điều khiển (driver) trong các AP và các card không dây. Điều này luôn luôn đúng để sử dụng phần mềm hệ thống

mới nhất và các bộ phận điều khiển trong các AP và các card không dây. Những nhà sản xuất thường thường đưa ra những sữa chữa, bảo mật các lỗ hổng mạng, và bật những tính năng mới với những sự nâng cấp này.

3.2.8 CÁC THIẾT BỊ BẢO MẬT

Giống như gắn một cánh cửa vào một tòa nhà để tránh kẻ trộm, những doanh nghiệp phải điều khiển vành đai mạng của họ. Theo truyền thống của mạng hữu tuyến, tường lửa là lựa chọn hoàn hảo cho việc này. Tuy nhiên, WLAN giới thiệu một lựa chọn tốt hơn từ sự điều khiển tự nhiên của truyền sóng vô tuyến.

Với dữ liệu và những kết nối mạng phát rộng thông qua không khí và đi qua cửa sổ, tường, trần nhà và sàn nhà, vành đai của WLAN có thể gặp khó khăn để điều khiển cũng như xác định chúng. Tuy nhiên, nhiều doanh nghiệp có thể điều khiển vành đai của WLAN bởi những thiết bị bảo mật hoạt động như là điểm cuối của mạng.

Điều khiển vành đai của WLAN bắt đầu với việc triển khai các tường lửa cá nhân trên chiếc mỗi tính máy sách tay và cũng bao gồm triển khai những AP của các doanh nghiệp có sự bảo mật và khả năng quản lý cao. WLAN nên cách ly với mạng hữu tuyến để cho phép quản lý cụ thể và những chính sách bảo mật không ảnh hưởng đến mạng hữu tuyến.

Tất cả các AP phải hoàn toàn được khóa lại và cấu hình lại từ các thiết lập mặc đinh. SSIDs và những mật khẩu của AP phải thay đổi từ những tên mặc định ban đầu. Vài tổ chức được thành lập để thiết lập những kênh của thao tác cho mỗi AP để nhận dạng tất cả các kênh đã tắt khi có những hành động nghi ngờ.

3.2.9 BẢO MẬT THÔNG TIN – CHỨNG THỰC VÀ MÃ HÓA

Trong sự triển khai bảo mật WLAN, điều khó nhất cho người quản lý mạng và bảo mật là lựa chọn làm sao để bảo mật thông tin WLAN với nhiều loại chứng thực và mã hóa.

Giống như việc cài đặt khóa và những chìa khóa để điều khiển cho ai có thể mở nó, tầng tiếp theo của bảo mật WLAN là điều khiển người dùng có thể truy cập WLAN. Để cung cấp những chứng thực cơ bản, AP hỗ trợ địa chỉ lọc MAC, duy trì một danh sách những địa chỉ MAC hợp lệ. Trong khi điều này không mấy rõ ràng,

lọc địa chỉ MAC cung cấp những điều khiển cơ bản vượt lên những trạm có thể kết nối tới mạng của bạn.

Những tổ chức tin vào cách lọc địa chỉ mạng ở trên cho việc điều khiển cho phép chính họ tấn công đến kẻ đột nhập. Những doanh nghiệp lớn hơn với WLAN phức tạp có hàng trăm trạm và hàng tá AP yêu cầu việc điều khiển truy cập tinh xảo hơn thông qua dịch vụ hợp nhất chứng thực quay số từ xa – Remote authentication dial-in service (RADIUS). Cisco Systems, Microsoft, và Funk Software là những tập đoàn dẫn đầu trong lĩnh vực này.

Quan tâm đến những công nghệ tiêu chuẩn, IEEE giới thiệu chuẩn 802.1x cung cấp các điểm điều khiển truy cập đơn giản, xác nhập với việc máy chủ chứng thực. tuy nhiên, vài phiên bản của 802.1x đã có vài lỗ hổng. Cisco giới thiệu Giao thức chứng thực có thể mở rộng - LightWeight Extensible Authentication Protocol (LEAP) như là giải pháp chứng thực riêng dựa trên chuẩn 802.1x nhưng thêm vào những phần tử riêng của bảo mật. LEAP là một phần thêm của việc bảo mật, và Cisco chuyển từ LEAP sang Giao thức Chứng thực bảo vệ mở rộng – Protected Extensible Authentication Protocol (PEAP).

Sự mã hóa cung cấp lõi của bảo mật cho WLAN bằng cách bảo vệ dữ liệu mà giao với sóng không khí. Tuy nhiên, những lỗi của các chuẩn mã hóa và chứng thực vẫn chưa được bổ sung. Giao thức toàn bộ khóa biểu thị thời gian – Temporal Key Integrity Protocol (TKIP) được giới thiệu đến những địa chỉ thiếu sót của WEP với mỗi gói dữ liệu có khóa trộn lẫn, một thông báo kiểm tra toàn bộ và một bộ máy gán lại khóa.

Những công nghệ chuẩn mới và những giải pháp độc quyền giờ đây đã được giới thiệu cả hai kênh điều khiển mã hóa và chứng thực. Cisco, RSA Security, và Microsoft phát triển PEAP như là một trong những giải pháp độc quyền. Tuy nhiên, Microsoft và Cisco đã tách rời PEAP của họ để nổ lực phát triển và giới thiệu những phiên bản của giao thức này. Phiên bản PEAP của Microsoft không làm việc với các phiên bản PEAP của Cisco. Trong khi phiên bản PEAP của Microsoft gói gọn trong máy tính sách tay, thì phiên bản PEAP của Cisco đề nghị phải cài phần mềm cho máy khách và quản lý trên mỗi trạm người dùng trong WLAN.

Trong tháng 6 năm 2003, khối liên minh Wi-Fi Bảo Vệ truy cập Wi-Fi – Wi-Fi Protected Access (WPA) như là một chuẩn cấp thấp của chuẩn bảo mật tương lai

802.11i trong TKIP. Những đại lý tốt nhất loan báo rằng những AP đang hoạt động có thể được nâng cấp phần sụn từ sự hỗ trợ của WPA. Tuy nhiên, những AP mới sẽ cần một chuẩn 802.11i phiên bản cuối.

Mạng riêng ảo – Virtual Private Network (VPN) của những cổng vào WLAN cung cấp một chuẩn riêng khác về mã hóa và chứng thực. Tường lửa và các đại lý cổng vào VPN, như là Check Point và NetScreen Technologies, VPN về cơ bản là một đường hầm internet dùng để vận chuyển giao thức ngoại lai ngang qua mạng. Những giải pháp của VPN là dùng giao thức IPSec (IP Security) và không làm việc tốt với WLAN khi người dùng đi lang thang giữa AP hoặc tín hiệu có thể bị biến đổi và hạ thấp, và sẽ có nhiều người dùng chứng thực lại và bắt đầu một tác vụ mới.

Những đại lý, như là Bluesocket, ReefEdge, và Vernier Networks, cung cấp cổng vào WLAN bao gồm những tính năng thêm vào cho việc lang thang trên mạng và quản lý băng thông làm cho nó thích ứng với WLAN. Một phần khác của các đại lý VPN không dây, là bao gồm Fortress Technologies và Crantie Systems, cung cấp thêm những giải pháp bảo mật với Layer 2 được mã hóa.

Trong khi VPN cung cấp sự mã hóa và chứng thực mạnh mẽ, thì vấn đề hóc búa của quản lý máy khách là các phần mềm cài trên nó.

3.3 QUẢN LÝ

3.3.1 THEO DÕI WLAN

Như là một chiếc máy quay phim, theo dõi tất cả các hoạt động trong ngày, theo dõi nhận dạng những kẻ xâm nhập WLAN, dò tìm những kẻ xâm phạm và những mối đe dọa sắp đến, và gán các chính sách bảo mật cho WLAN (enforce policies).

Một ví dụ cho việc cần thiết phải theo dõi : AP được nâng cấp bởi WPA, AP phải được theo dõi để chắc rằng AP đó vẫn có cấu hình đúng.

Theo dõi WLAN của các doanh nghiệp cần phải rõ ràng rành mạch. Vài giải pháp đã được thực hiện cho các tổ chức nhỏ nhưng không đủ qui mô cho các doanh nghiệp lớn hơn với hàng tá hoặc hàng trăm công ty trên khắp thế giới. Những doanh nghiệp lớn yêu cầu những giải pháp có hiệu quả, có sự quản lý trung tâm và không đòi hỏi nhiều tài nguyên con người.

3.3.2 YÊU CẦU CHO QUẢN TRỊ WLAN

Bảo mật WLAN cũng giống như sự bảo mật của mạng hữu tuyến, dẫn đến sự quản lý đúng đắn cho việc quản lý WLAN. Những nhà quản lý mạng nên thật sự biết rõ những yêu cầu cơ bản của việc quản lý WLAN nhưng phải có những giải pháp chủ chốt trong việc chẩn đoán lỗi, cấu hình quản lý, tạo trương mục sử dụng mạng, thực hiện việc theo dõi, và gán các chính sách (policy).

Quản lý một mạng không dây nhỏ có khoảng 5 hoặc 10 AP có thể dễ dàng hoàn thành với việc xây dựng chức năng trong những AP. Tuy nhiên, quản lý một mạng không dây lớn hơn khoảng từ 12 đến hàng trăm AP trong phạm vi trường sở hoặc trong phạm vi nhiều khu vực của cả nước yêu cầu cần phải có thêm những giải pháp để có thể hỗ trợ, phân bổ một cách tự nhiên trong mạng.

Quản lý những mạng không dây sẽ cảm thấy hài lòng với sự kết hợp của các giải pháp cung cấp cơ sở hạ tầng cho mạng không dây, như là Cisco System và Symbol Technologies, nhiều công ty đã bắt đầu, như là Aruba Networks và Trapeze Networks. Tuy nhiên, hệ thống quản lý mạng không dây tốt nhất là tính đến sự giới hạn bởi những khả năng để chỉ quản lý AP sản xuất bởi đại lý cung cấp của hệ thống WLAN.

3.3.3 QUẢN LÝ CẤU HÌNH

Quản lý các cấu hình của mạng không dây thông qua tất cả các AP và các trạm thường đưa ra những thách thức lớn cho việc quản lý mạng. Trong mức độ khó nhất, mỗi thiết bị phải có quan hệ chắc chắn đến các thiết lập thích hợp cho việc bảo mật, sự thực thi và những chính sách đúng đắn. Có nhiều sự đề nghị để quản lý mạng WLAN, như là Cisco’s Wireless LAN Solution Engine (WLSE) hoặc Symbol’s Wireless Switch System, có thể quản lý từ xa các cấu hình AP và áp dụng nhiều các cấu hình tạm thời đến các đoạn mạng khác nhau của một mạng không dây.

Quản lý các cấu hình người dùng gặp phải những thách thức lớn hơn bởi vì những người quản lý mạng có thể không hướng dẫn truy cập người dùng tới tất cả các trạm, và một số ít trạm có thể là những dự án tốn nhiều thời gian.

Theo dõi tốc độ xử lý của máy và cấu hình phần dây phụ để chắc rằng những AP và những trạm còn lại vẫn trong trạng thái cấu hình xác định. Sự tràn năng lượng

hoặc ngưng hoạt động có thể làm cho AP tự động xác lập lại các thiết lập mặc định. Các nhân viên có thể thay đổi những thiết lập cho thiết bị để có thể truy cập mạng trở lại. Phân tích lưu lượng của mạng không dây để nhận dạng các mạng cấu hình sai.

3.3.4 CHẨN ĐOÁN LỖI

Các nhân viên và những người dùng có thể có lợi ích từ mạng không dây chỉ khi nó hoạt động. Đáp ứng các cuộc gọi hỗ trợ có thể là một thao tác làm át hẳn phạm vi hoạt động của IT (Information Technology) để đáp ứng sự hỗ trợ mạng không dây trong các vị trí điều khiển.

Những thiết bị quản lý mạng không dây, được cung cấp bởi Cisco và Symbol, có thể thăm dò những thiết bị mạng từ mạng hữu tuyến để quan sát những nét đặc trưng và thuộc tính của các thiết bị đó, rồi báo cho các nhân viên các kết quả thu được. Trong một mức cao hơn của việc chuẩn đoán lỗi : việc theo dõi tốc độ xử lý của máy, khảo sát những thiết bị WLAN, phân tích những kiểu dáng lưu lượng và báo cáo những thiết bị lỗi và những tạp nhiễu quá mức trong không khí dẫn đến làm tê liệt mạng không dây.

3.3.5 THEO DÕI SỰ THỰC THI

Sau lần đầu tiên chắc rằng mạng đã hoạt động, những người quản lý mạng phải theo dõi và phân tích việc hoạt động của một WLAN bảo đảm mạng này hoạt động tốt nhất. Những công cụ quản lý WLAN, như là Cisco WLSE, có thể cung cấp vài thông tin thực thi từ mạng hữu tuyến. Thêm vào đó, theo dõi tốc độ xử lý máy tính sẽ xác định được những thực thi phát sinh mà có thể chỉ thấy được từ không khí, như là tín hiệu bị hạ thấp từ sự chồng lấp kênh, sự can thiệp tầng số từ những thiết bị có chuẩn 802.1x, và lượng quá tải của một AP.

3.3.6 TRƯƠNG MỤC – CÁCH SỬ DỤNG MẠNG

Nhiều như những việc chẩn đoán lỗi và kiểm tra thực thi, trương mục cho việc sử dụng mạng là thực hiện việc nối gần các nền tảng quản lý và theo dõi 24x7. Những nền tảng quản lý mạng từ những nền tảng giống của Cisco và Symbol kết nối các trạm của WLAN tới những ứng dụng khác nhau trên mạng cho mục đích tiến hành tạo trương mục.

Kiểm tra lưu lượng mạng WLAN thông qua sóng không khí cho phép những người quản lý mạng kiểm tra việc sử dụng mạng cơ bản trên công suất cao nhất của mỗi AP và băng thông cao nhất – những trạm chi phối và những AP. Điều này cho phép những người quản lý mạng có sơ đồ cho việc tăng công suất khi cần thiết và đối phó với những người dùng riêng lẻ lạm dụng WLAN để tải xuống những tập tin không liên quan đến công việc của công ty, như là MP3,…

3.3.7 GÁN CHÍNH SÁCH (POLICY)

Sự bằng lòng cho các chính sách đi qua WLAN ảnh hưởng đến hầu hết mỗi khía cạnh của việc quản lý và bảo mật mạng. Các chính sách khống chế các cấu hình, việc sử dụng, các thiết lập bảo mật, và những giới hạn thực thi của WLAN. Tuy nhiên, các chính sách bảo mật và quản lý sẽ vô ích khi mạng đã đặt sự theo dõi cho các chính sách được ưng thuận và tổ chức có những bước hoạt động để gán các chính sách.

Theo dõi tốc độ xử lý máy tính, theo dõi 24x7 của lưu lượng không dây phát sinh các vi phạm chính sách sau :

- Những kẻ lừa đảo WLAN – bao gồm cả phần mềm cho các AP.
- Không có chứng thực hoặc mã hóa.
- Những trạm không được phép.
- Các mạng ngang hàng.
- Các SSID mặc định hoặc không thích hợp.
- Những AP và những trạm trung tâm trên các kênh không được phép.
- Lưu lượng trong thời gian không phải cao điểm.
- Các đại lý phần cứng không được cấp phép.
- Tỷ lệ dữ liệu không cho phép.
- Những giới hạn thực thi biểu thị sức ổn định của WLAN.

3.4 TỔNG KẾT

Với sự bùng nổ của công nghệ không dây, vai trò của những nhà sản xuất phần cứng và các tổ chức như là FCC, IEEE, WECA, WLANA sẽ tăng thêm phần quan trọng để giải quyết các giải pháp của mạng không dây. Những quy định được đặt vào các tổ chức điều tiết như là FCC với những chuẩn, và những tổ chức như là IEEE, WLANA và WECA sẽ là tiêu điểm của kỹ nghệ sản xuất mạng không dây.

WLAN sẽ cải tiến tốt hơn trong giới hạn của tốc độ, sự tiện lợi, và bảo mật. Sự chứng thực và các kỹ thuật PKI chỉ là sự bắt đầu cho việc hạ giá WLAN để bạn có thể điều khiển truy cập tới bất cứ tài nguyên nào trong mạng.

Một phần quan trọng nhất, là phải ngăn ngừa sự nguy hiểm tới mạng của bạn trước khi nó xảy ra. Tránh xa các cặp mắt nghi ngờ và phải chắc chắn rằng thông báo cho những người dùng trong mạng biết rằng hãy cảnh giác với những người truy cập mạng và những điều luật thông qua các chính sách để chỉ những người dùng được phép mới có thể truy cập tới các tài nguyên trong mạng. Nếu bạn kiểm tra và thấy rằng tất cả đã kết nối, bạn phải chắc chắn rằng bạn có thể cung cấp đủ sự bảo mật một cách tận tâm cho mạng của bạn.

Công nghệ không dây ra đời đã làm thay đổi diện mạo của nền công nghệ thông tin trên toàn thế giới. Nó mang đến cho thế giới một cách nhìn mới về các công nghệ tiên tiến. Công nghệ không dây đã trãi qua một quá trình dài từ khi nó là ý tưởng của quân đội. Sự ưa chuộng và mức độ của công nghệ sử dụng mạng không dây vẫn tiếp tục mọc lên với tỷ lệ cao đến không ngờ. Sản xuất và tạo ra vô số giải pháp cho những mạng không dây là cần thiết. Sự thuận tiện, phổ biến, có lợi và giá cả của các phần cứng của mạng không dây cung cấp cho chúng ta nhiều lựa chọn khác nhau. bạn đã sẵn sàng gia nhập vào đội ngũ những người chuyển sang nối mạng không dây. Bạn sẽ thấy rằng một thế giới không có dây thì ít rối rắm phức tạp hơn và việc sử dụng mạng không dây trong gia đình của bạn sẽ được cải thiện đáng kể.