# LỜI MỞ ĐẦU

Trong xã hội công nghệ hiện đại,hệ thống thông tin liên lạc có tầm quan trọng giống như hệ thống thần kinh xuyên suốt cơ thể con người.Sự gia tăng nhu cầu truyền số liệu tốc độ cao và đa dạng hoá các loại hình dịch vụ cung cấp như truy nhập Internet,thương mại điện tử đã thúc đẩy sự phát triển của các giải pháp mạng cục bộ vô tuyến (WLAN) với những ưu điểm vượt trội khắc phục nhược điểm của Lan hữu tuyến, cung cấp những giải pháp mạng hiệu quả hơn.

Công nghệ không dây là một phương pháp chuyển giao từ điểm này tới điểm khác xử dụng sóng vô tuyến làm phương tiện truyền dẫn như sóng radio,cell,hồng ngoại và vệ tinh giúp giảm thiểu dây dẫn trong quá trình truyền và nhận thông tin.

Ngày nay mạng không dây đã đạt được những bước phát triển đáng kể. Tại một số nước có nền kinh tế phát triển tại Châu Âu, Châu Mĩ mạng không dây đã rất phát triển trong đời sống.Chỉ với một laptop,PDA hoặc một phương tiện truy cập mạng không dây bất kì ta cũng có thể truy cập vào mạng tại bất cứ đâu,tại cơ quan,trường học, ngoài đường trong quán café hay những ngay trên các phương tiện giao thông công cộng khác,bất cứ đâu nằm trong phạm vi phủ sóng của mạng WLAN.

Nhưng chính sự hỗ trợ truy nhập công cộng với các phương tiện truy cập đơn giản cũng như phức tạp đã đem lại nhiều rắc rối cho các nhà quản trị trong việc bảo mật thông tin.Vấn đề tích hợp các biện pháp bảo mật vào các phương tiện truy nhập nhưng vẫn đảm bảo những tiện ích và việc hộ trợ truy cập công cộng là vấn đề rất đáng quan tâm.

Do đó em đã chọn vấn đề bảo mật trong mạng không dây WLAN là nội dung chính của Đồ Án này.Đồ Án gồm 8 chương với 3 nội dung chính :

- ❖Thứ nhất là đưa ra cái nhìn bao quát về mạng không dây từ cấu trúc, mô hình cho tới các giải pháp kĩ thuật.Nội dung nằm trong chương 1,chương 2 và chương 3.
- ❖Thứ hai là tìm hiểu về các khả năng tấn công từ ngoài vào hệ thống mạng không dây để từ đó đưa ra các khuyến cáo về bảo mật. Nôi dung bao quát trong 2 chương là chương 4 và chương 5.
- ❖Cuối cùng là việc tìm hiểu việc triển khai hệ thống mạng không dây tại Trường Đại học Dân Lập Hải Phòng.Nội dung nằm trong 3 chương còn lại là chương 6, chương 7 và chương 8.

Mong rằng Đồ Án sẽ giúp mọi người hiểu thêm 1 phần về mạng Wireless LAN và các vấn đề liên quan tới bảo mật mạng không dây.Do hạn chế về mặt kiến thức và tài liệu nên Đồ Án sẽ không tránh khỏi nhiều thiếu sót.Vì vậy em rất mong được sự chỉ bảo, phê bình và góp ý chân thành từ phía các thầy cô và các bạn.

# Chương 1

# GIỚI THIỆU VỀ WIRELESS LAN

## 1.1.KHÁI NIỆM WLAN

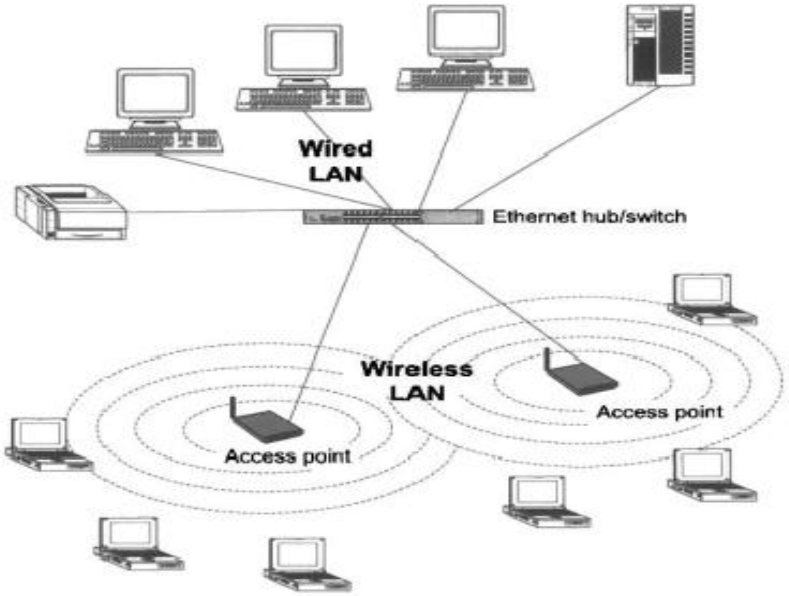
Mạng WLAN (Wireless Local Area Network) là một mạng truyền dữ liệu trên cơ sở một mạng cục bộ LAN. WLAN sử dụng sóng vô tuyến làm phương tiện truyền dẫn vì vậy giảm thiểu kết nối dây dẫn trong việc truyền và nhận thông tin.

WLAN là 1 công nghệ truy cập mạng băng thông 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 dộ 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 café, nhà ga, các trung tâm thương mại hay trung tâm báo chí.

## 1.2.CẤU TRÚC VÀ ĐẶC TÍNH CỦA MẠNG WLAN

### 1.2.1 Cấu trúc của mạng Wlan

WLAN tương tự như một hệ thống tế bào, mỗi điểm truy cập là một trạm cơ sở truyền dữ liệu giữa WLAN và cơ sở hạ tầng mạng có dây. Một điểm truy cập đơn lẻ có thể hỗ trợ một nhóm người dùng và cung cấp thông tin trong một bán kính cho phép. Các điểm truy cập được kết nối tới mạng có dây thông qua hub Ethernet hoặc switch. Và những người dùng truy cập WLAN thông qua các adapter WLAN (các adapter này cũng tồn tại trong các laptop) hoặc thông qua các PC card.




**Hình 1.1: Cấu trúc của WLAN**

### 1.2.2 Đặc tính của mạng Wlan

❖ **Khả năng di chuyển**:

Người dùng có thể di chuyển nhưng vẫn có thể truy nhập những hồ sơ, những tài nguyên mạng và internet mà không phải nối dây đến mạng có dây truyền thống. Những người sử dụng có thể di chuyển, tuy thế vẫn giữ nguyên sự truy nhập mạng LAN với tốc độ cao và thời gian thực.

❖ **Cài đặt nhanh**:

Thời gian yêu cầu cho việc cài đặt được rút ngắn bởi vì những kết nối mạng có thể làm mà không cần chuyển động, thêm dây hoặc kéo chúng xuyên qua tường và trần nhà như mạng có dây vẫn hay làm.

❖ **Linh hoạt**:

Nó linh hoạt vì dễ thiết lập và tháo gỡ ở mọi nơi. Vì thế những người dùng có thể nhanh chóng thiết lập một WLAN nhỏ cho những nhu cầu tạm thời như hội nghị thương mại hoặc trong các cuộc họp.

❖ **Tính chuyển đổi**:

Mạng cấu hình WLAN có thể dễ dàng được định hình để đáp ứng nhu cầu ứng dụng và cài đặt đặc biệt và có thể chuyển đổi từ những mạng nhỏ lên mạng lớn hơn.

❖ **Khả năng mở rộng**:

Hệ thống WLAN có thể cấu hình trong nhiều mô hình để đáp ứng các ứng dụng và cấu hình đặc thù dễ thay đổi và phạm vi từ mạng điểm - điểm xây dựng cho số nhỏ người dùng đến các mạng phối hợp với hàng ngàn người dùng cho phép chuyển vùng trên phạm vi rộng.

❖ **Hạ thấp chi phí triển khai**:

Mặc dù đầu tư ban đầu về phần cứng có thể cao hơn mạng có dây, tuy nhiên xét chi phí tổng thể và chi phí theo tuổi thọ có thể thấp hơn đáng kể. Về lâu dài, WLAN sẽ đem lại lợi ích rất lớn trong các môi trường động yêu cầu sự di chuyển và thay đổi nhiều.

## 1.3.ĐỐI TƯỢNG VÀ ỨNG DỤNG CỦA MẠNG WLAN

### 1.3.1 Đối tượng sử dụng

Mạng WLAN đang trở nên phổ biến trong các môi trường:

❖ **Hệ thống thông tin doanh nghiệp**:

Các nhà quản lý mạng có thể di chuyển nhân viên, lập ra các văn phòng tạm thời, hoặc cài đặt máy in và nhiều thiết bị khác mà không bị ảnh hưởng bởi chi phí và tính phức tạp của mạng có dây. Cấp lãnh đạo có thể truy cập vào hệ thống thông tin quan trọng của công ty từ phòng họp thông qua các thiết bị cầm tay được cài đặt card WLAN.

❖ **Du lịch**:

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

❖ **Giáo dục**:

Sinh viên và giảng viên có thể liên lạc với nhau từ bất cứ vị trí nào trong khuôn viên đại học để trao đổi hoặc tải về các bài giảng có sẵn trên mạng. Mạng WLAN còn giảm thiểu nhu cầu sử dụng phòng lab (phòng thực hành).

❖ **Thông tin sản phẩm**:

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

❖ **Y tế:**

Bác sĩ, y tá có thể trao đổi các thông tin về bệnh nhân hoặc liệu pháp chữa trị…

Tại việt nam thì các đối tượng được quan tâm là các khách hàng dùng Laptop, Pocket PC hay PC có card moderm như sinh viên ,doanh nhân, khách du lịch.

### 1.3.2 Khả năng ứng dụng

Khó khăn trong lắp đặt cáp là yếu tố thúc đẩy môi trường vô tuyến trở thành xu hướng ngày càng nhận được sự chấp nhận rộng rãi của con người. Môi trường vô tuyến đặc biệt hữu ích để thiết lập mạng cho:

❖ Những khu vực nhộn nhịp như tiền sảnh hay phòng tiếp tân.

❖ Những người liên tục di chuyển như y tá, bác sĩ trong bệnh viện.

❖ Khu vực và toà nhà biệt lập.

❖ Những phòng ban thường xuyên bị thay đổi kiểu bố trí vật lý.

WLAN được lắp đặt tại các khu tập trung đông người như : Các văn phòng, toà nhà,trường đại học,sân bay,nhà ga,sân vận động, khu triển lãm,khách sạn,siêu thị hay khu dân cư…

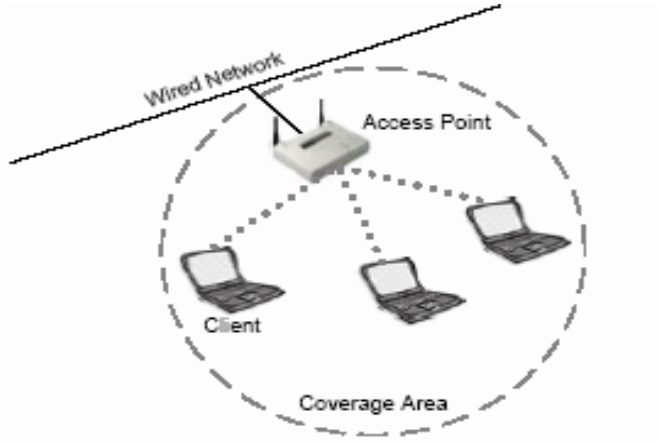
# Chương 2

# CÁC GIẢI PHÁP KĨ THUẬT

## 2.1.GIỚI THIỆU TỔNG QUAN

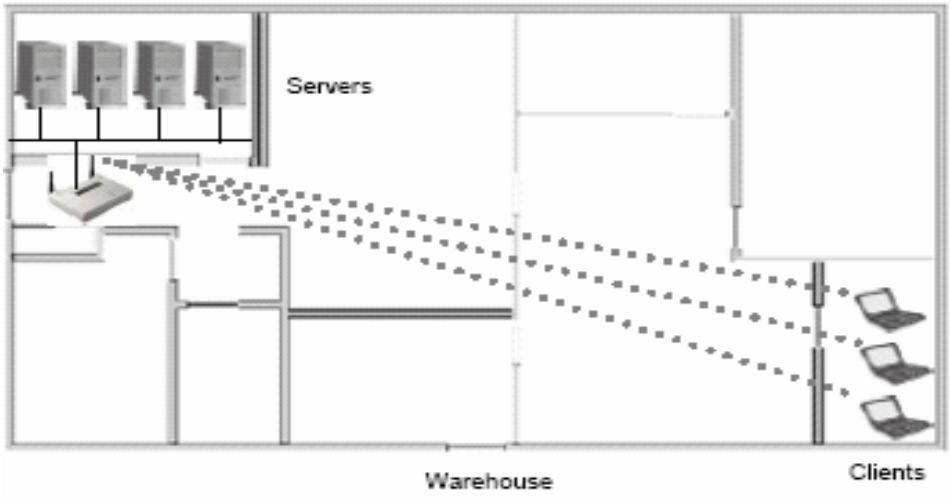
WLAN là một công nghệ truy cập mạng băng rộng không dây theo chuẩn của 802.11 của IEEE. Tiêu chuẩn IEEE 802.11 định nghĩa cả hai kiểu cơ sở hạ tầng, với số lượng tối thiểu các điểm truy nhập trung tâm tới một mạng hữu tuyến,và một chế độ là Peer-to-peer, trong đó một tập hợp những đài vô tuyến liên lạc 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 dùng có thể cố định hoặc di động hoặc thậm chí có thể đang ngồi trên 1 phương tiện chuyển động.

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



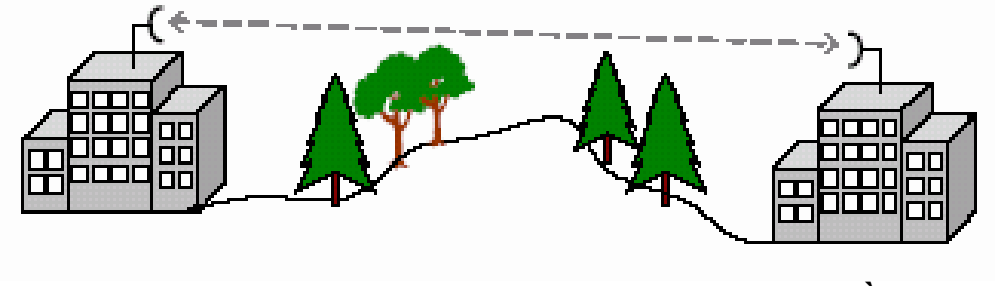

**Hình 2.1:khả năng mở rộng mạng**

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 đi dây.



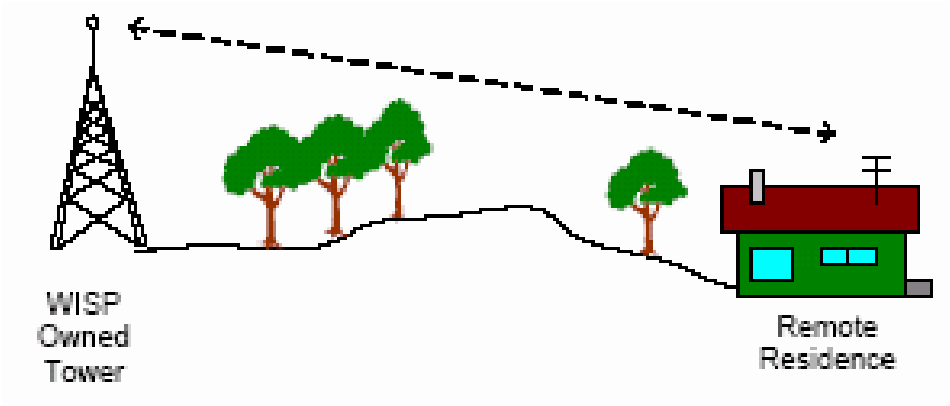

**Hình 2.2:khả năng truy cập mạng mà không phải đi dây**

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:



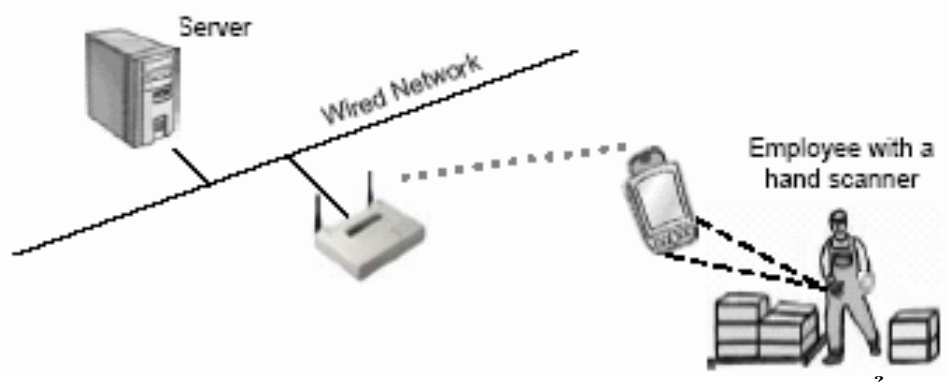
**Hình 2.3:tiện lợi trong việc xây dựng mạng trên miền núi**

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



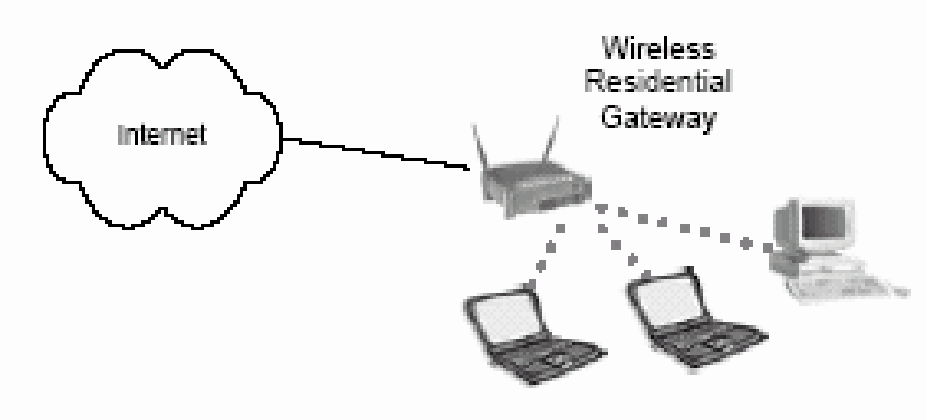

**Hình 2.4:Tại nơi có địa hình lòng chảo**

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




**Hình 2.5 : khả năng truy cập trong khi di chuyển**

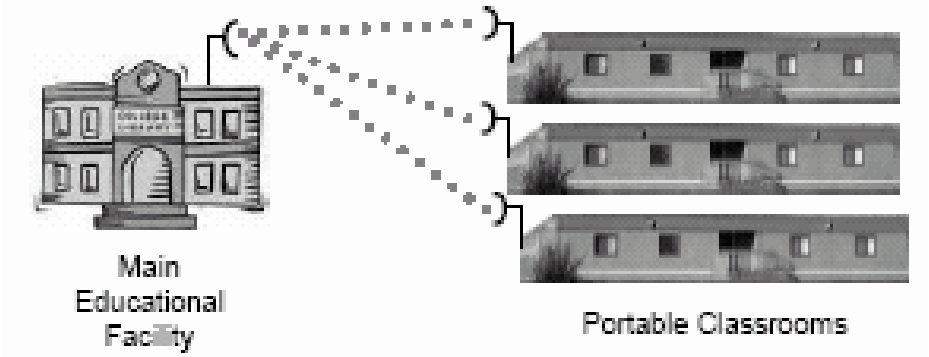
Từ các văn phòng, nhà riêng:




**Hình 2.6 : 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 2.7 :** truy cập từ các trường đại học

## 2.2.CÁC CHUẨN 802.11

**802.11 :** Năm 1997, IEEE (Institute of Electrical and Electronics Engineers) đã giới thiệu một chuẩn đầu tiên cho WLAN. Chuẩn này được gọi là **802.11** sau khi tên của nhóm được thiết lập nhằm giám sát sự phát triển của nó. Tuy nhiên, **802.11**chỉ hỗ trợ cho băng tần mạng cực đại lên đến 2Mbps – quá chậm đối với hầu hết các ứng dụng. Với lý do đó, các sản phẩm không dây thiết kế theo chuẩn **802.11** ban đầu dần không được sản xuất.

**802.11b**: IEEE đã mở rộng trên chuẩn 802.11 gốc vào tháng Bảy năm 1999, đó chính là chuẩn **802.11b.** Chuẩn này hỗ trợ băng thông lên đến 11Mbps, tương quan với Ethernet truyền thống.

**802.11b** sử dụng tần số vô tuyến (2.4 GHz) giống như chuẩn ban đầu 802.11. Các hãng thích sử dụng các tần số này để chi phí trong sản xuất của họ được giảm. Các thiết bị **802.11b** có thể bị xuyên nhiễu từ các thiết bị điện thoại không dây (kéo dài), lò vi sóng hoặc các thiết bị khác sử dụng cùng dải tần 2.4 GHz. Mặc dù vậy, bằng cách cài đặt các thiết bị 802.11b cách xa các thiết bị như vậy có thể giảm được hiện tượng xuyên nhiễu này.

- Ưu điểm của **802.11b** : giá thành thấp nhất; phạm vi tín hiệu tốt và không dễ bị cản trở.
- Nhược điểm của **802.11b** : tốc độ tối đa thấp nhất; các ứng dụng gia

đình có thể xuyên nhiễu.

**802.11a**: Trong khi 802.11b vẫn đang được phát triển, IEEE đã tạo một mở rộng thứ cấp cho chuẩn 802.11 có tên gọi **802.11a**. Vì 802.11b được sử dụng rộng rãi quá nhanh so với **802.11a**, nên một số người cho rằng **802.11a** được tạo sau 802.11b. Tuy nhiên trong thực tế, **802.11a** và 802.11b được tạo một cách đồng thời. Do giá thành cao hơn nên **802.11a** chỉ được sử dụng trong các mạng doanh nghiệp còn 802.11b thích hợp hơn với thị trường mạng gia đình.

**802.11a** hỗ trợ băng thông lên đến 54 Mbps và sử dụng tần số vô tuyến 5GHz. Tần số của **802**.11a cao hơn so với 802.11b chính vì vậy đã làm cho phạm vi của hệ thống này hẹp hơn so với các mạng 802.11b. Với tần số này, các tín hiệu 802.11a cũng khó xuyên qua các vách tường và các vật cản khác hơn.

Do **802.11a** và 802.11b sử dụng các tần số khác nhau, nên hai công nghệ này không thể tương thích với nhau. Chính vì vậy một số hãng đã cung cấp các thiết bị mạng hybrid cho 802.11a/b nhưng các sản phẩm này chỉ đơn thuần là bổ sung thêm hai chuẩn này.

- Ưu điểm của **802.11a** : tốc độ cao; tần số 5Ghz tránh được sự xuyên nhiễu từ các thiết bị khác.
- Nhược điểm của **802.11a** : giá thành đắt; phạm vi hẹp và dễ bị che khuất.

**802.11g**: Vào năm 2002 và 2003, các sản phẩm WLAN hỗ trợ một chuẩn mới hơn đó là **802.11g**, được đánh giá cao trên thị trường. 802.11g thực hiện sự kết hợp tốt nhất giữa 802.11a và 802.11b. Nó hỗ trợ băng thông lên đến 54Mbps và sử dụng tần số 2.4 Ghz để có phạm vi rộng. **802.11g** có khả năng tương thích với các chuẩn 802.11b, điều đó có nghĩa là các điểm truy cập **802.11g** sẽ làm việc với các adapter mạng không dây 802.11b và ngược lại.

- Ưu điểm của **802.11g** : tốc độ cao, phạm vi tín hiệu tốt và ít bị che khuất.
- Nhược điểm của **802.11g** : giá thành đắt hơn 802.11b; các thiết bị có

thể bị xuyên nhiễu từ nhiều thiết bị khác sử dụng cùng băng tần.

**802.11n** : Chuẩn mới nhất trong danh mục Wi-Fi chính là **802.11n**. Đây là chuẩn được thiết kế để cải thiện cho 802.11g trong tổng số băng thông được hỗ trợ bằng cách tận dụng nhiều tín hiệu không dây và các anten (công nghệ MIMO).

Khi chuẩn này được đưa ra, các kết nối **802.11n** sẽ hỗ trợ tốc độ dữ liệu lên đến 100 Mbps. **802.11n** cũng cung cấp phạm vi bao phủ tốt hơn so với các chuẩn Wi-Fi trước nó nhờ cường độ tín hiệu mạnh của nó. Thiết bị **802.11n** sẽ tương thích với các thiết bị 802.11g. Dù đến năm 2010, **802.11n** mới chính thức được phê duyệt, các sản phẩm dùng chuẩn này (thực chất là theo "dự thảo" chuẩn) sẽ không thay đổi nhiều. Hơn nữa, các router **802.11n** có khả năng tương thích ngược với thiết bị dùng chuẩn cũ, chỉ cần người dùng cài đặt vài bước.

- Ưu điểm của **802.11n** : tốc độ nhanh và phạm vi tín hiệu tốt nhất; khả năng chịu đựng tốt hơn từ việc xuyên nhiễu từ các nguồn bên ngoài.
- Nhược điểm của **802.11n** : giá thành đắt hơn 802.11g; sử dụng nhiều tín hiệu có thể gây nhiễu với các mạng 802.11b/g ở gần.

Lần đầu tiên xuất hiện tại một trường đại học ở ngoại ô thành phố New York (Mỹ), mạng cục bộ không dây theo chuẩn **802.11n** này có 720 điểm truy cập dùng thiết bị AP 320 thay cho các access point chuẩn 11a/b/g.

Chưa đủ thời gian để kiểm nghiệm hoạt động thực tế toàn hệ thống nhưng thày trò và nhân viên trường Morrisville State đều ghi nhận sự cải thiện lớn so với hạ tầng không dây theo các chuẩn 11 a/b/g cũ, cụ thể là những ứng dụng ngốn băng thông chạy nhanh hơn trên mạng này.

Các lớp học trong trường có thể phát bản tin dạng video và tổ chức họp trực tuyến mà không bị tình trạng ngưng trệ khi nạp dữ liệu (buffering delay).

Hiện tại, giờ cao điểm nhất ghi nhận hơn 1.200 máy khách truy cập không dây đồng thời, trong đó ngoài laptop còn có các thiết bị như máy nghe nhạc

iPod, điện thoại iPhone, một số thiết bị cầm tay hoặc máy chơi game console có tính năng kết nối wireless.

Trên đây là 4 chuẩn được nhắc tới nhiều nhất trong WLAN, ngoài ra chúng ta còn được biết tới một số chuẩn khác là các chuẩn mở rộng, mỗi chuẩn phục vụ cho 1 mục đích cụ thể như:

**802.11h**: chuẩn này là một biến thể của 802.11a ở Châu Âu có thêm các đặc tính tối ưu.

**802.11i**: chuẩn này vẫn đang được phát triển, nó là một lá chắn bảo vệ để các chuẩn WLAN tồn tại, nó sẽ nâng cao mức độ bảo mật bằng cách như là mật hoá tốt hơn và điều khiển truy cập.

**802.16**: một bản phác thảo của chuẩn WLAN cho mạng thành phố (MAN) dựa trên OFDM và sử dụng 802.11a làm cơ sở, được công bố vào tháng 4 năm 2002. 802.16 hỗ trợ kiến trúc "point-to-multipoint" trong dải tần từ 10 đến 66 GHz, tốc độ dữ liệu lên tới 120Mbps.

**802.11e**: cải thiện chất lượng dịch vụ, cho phép thiết lập mức độ ưu tiên.

**802.11x**: về bảo mật WLAN và các lớp khác của các dịch vụ cụ thể.

**802.11c**: cải thiện thao tác giữa hai thiết bị.

**802.11d**: chuẩn LAN/MAN, cải thiện "roaming".

(roaming là khả năng đưa một thiết bị không dây từ phạm vi của một điểm truy cập này tới phạm vi của một điểm truy cập khác mà không làm mất kết nối). Nói cách khác "roaming" tức là "chuyển vùng".

**802.11f**: để điều chỉnh liên điểm truy cập (regulate inter access point handoffs).

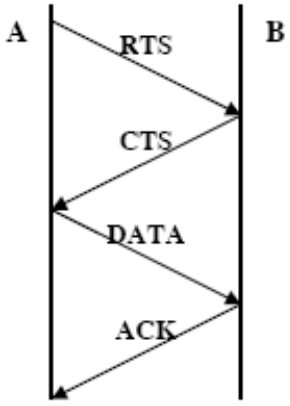
Cho dù chuẩn WLAN nào được sử dụng thì các khái niệm cơ bản về triển khai và bảo mật đều như nhau.

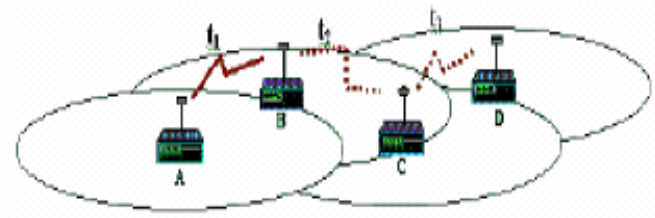
## 2.3.TRUY CẬP KÊNH TRUYỀN , CƠ CHẾ ĐA TRUY NHẬP CSMA/CA

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 dang 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



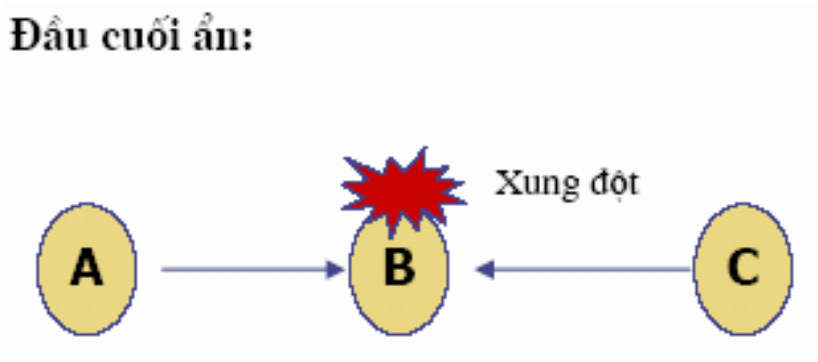




**Hình 2.8: Một quá trình truyền từ A đến B**

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).

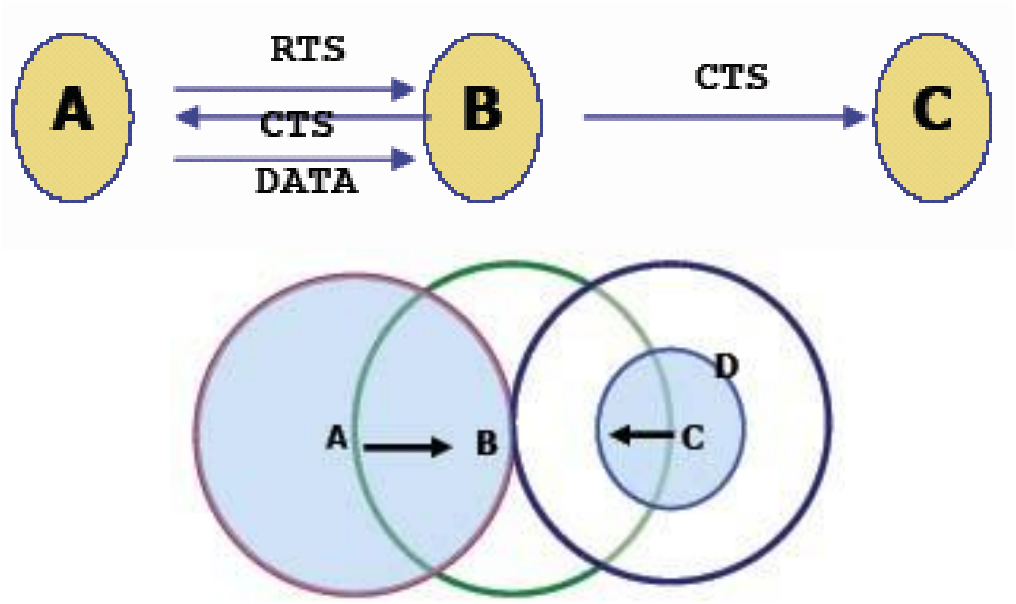
### 2.3.1 Vấn đề đầu cuối ẩn




**Hình 2.9: 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.

❖ **Giải quyết vấn đề đầu cuối ẩn**:

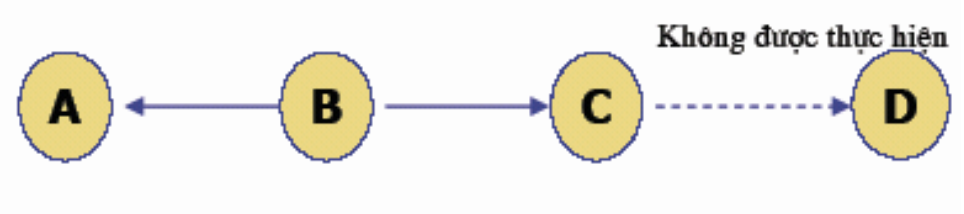



**Hình 2.10: Giải quyết vấn đề đầu cuối ẩn**

- 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.

### 2.3.2 Vấn đề đầu cuối hiện:




**Hình 2.11: Đầu cuối hiện**

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

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


**Hình 2.12: 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, những 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).

## 2.4.CÁC KĨ THUẬT ĐIỀU CHẾ

### 2.4.1 Kĩ 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.

Nguyên lý cơ bản của điều chế PSK là 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, khi số lượng các trạng thái pha tăng lên thì tốc độ bit cũng tăng nhưng tốc độ baud 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).

- **Binary PSK** (Binary Phase Shifp Keying -Khóa chuyển dịch pha nhị phân):

Đây là phương pháp thông dụng nhất, tín hiệu sóng mang được điều chế dựa vào chuỗi nhị phân, tín hiệu điều chế có biên độ không đổi và biến đổi giữa hai trạng thái 00 và 1800, mỗi trạng thái của tín hiệu điều chế được gọi là một symbol.

- **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 -900, 00, 900 và 1800.

- **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.

### 2.4.2 KĨ 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.

## 2.5.CÁC KĨ THUẬT TRUY CẬP

### 2.5.1 FDMA

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.

### 2.5.2 TDMA

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.

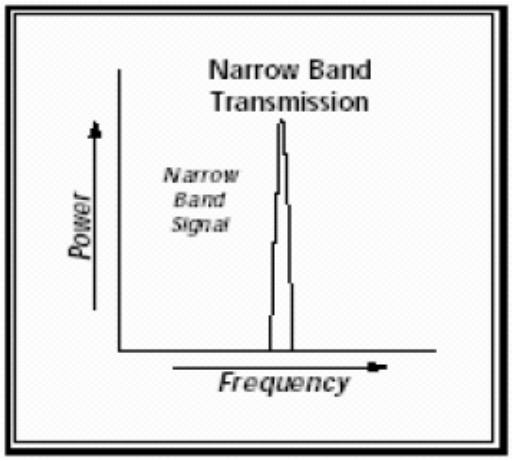
### 2.5.3 CDMA

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.

## 2.6.KỸ THUẬT VÔ TUYẾN

### 2.6.1 Kĩ thuật 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.

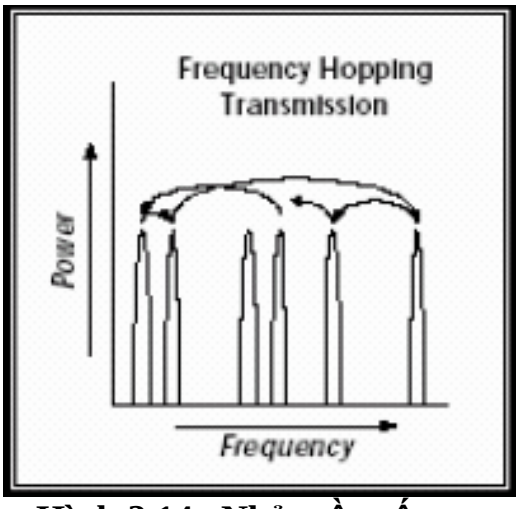



**Hình 2.13: Tín hiệu băng hẹp**

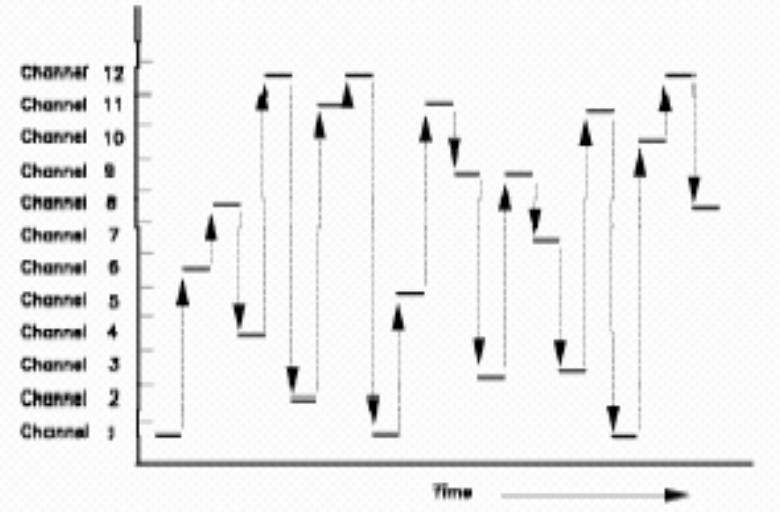
### 2.6.2 Kỹ thuật trải phổ :

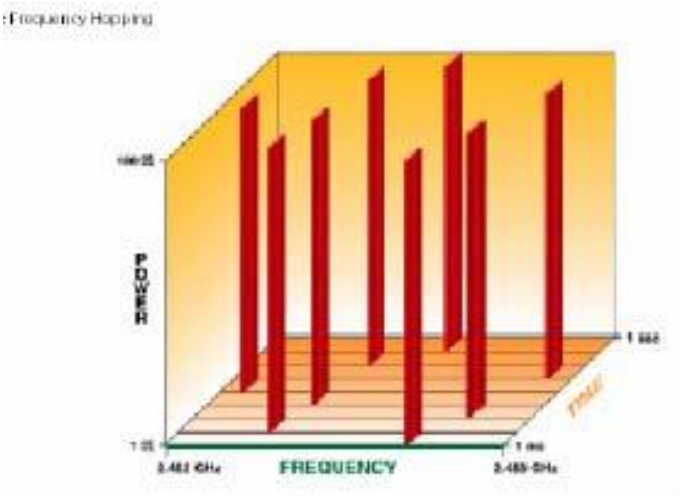
Khi tài nguyên vô tuyến ngày càng trở nên cạn kiệt, người ta bắt đầu phải áp dụng kỹ thuật trải phổ nhằm nâng cao hiệu năng sử dụng tần số. Có hai kỹ thuật trải phổ thông dụng nhất hiện nay là FHSS và DSSS. Băng thông cho mỗi CPE sẽ không còn là một dải hẹp mà sẽ là toàn bộ băng tần số, việc xác định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

### 2.6.3 FHSS (Frequency Hopping Spread Spectrum):




**Hình 2.14: Nhảy tần số**



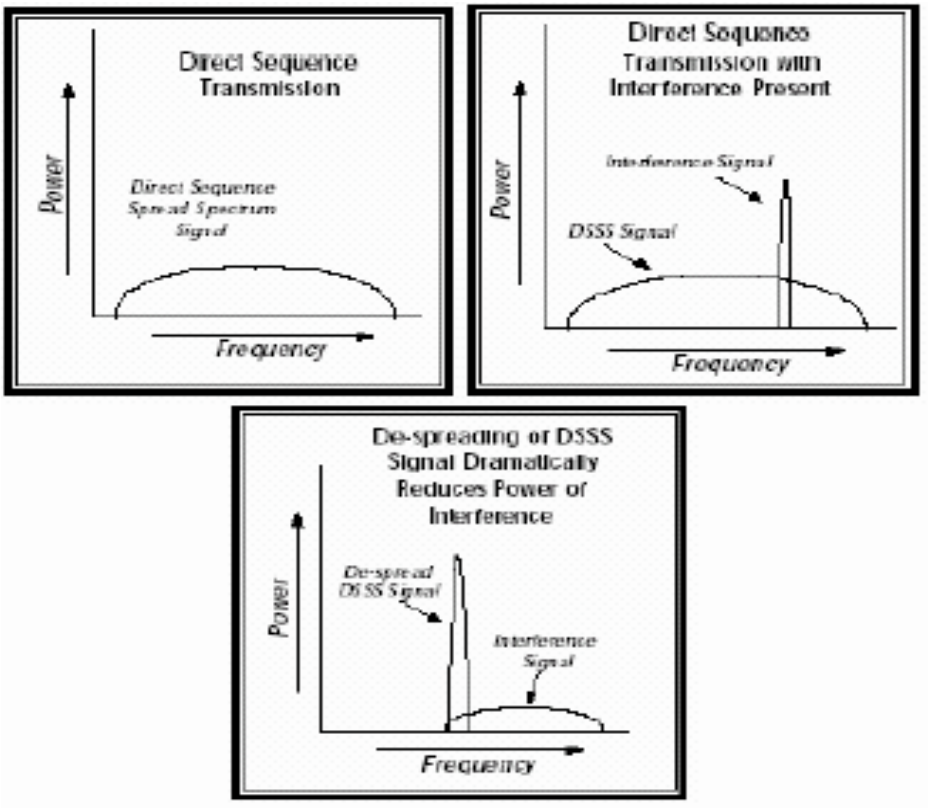

**Hình 2.15: Các kênh trong FHSS**

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.

### 2.6.4 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 2.16: 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).

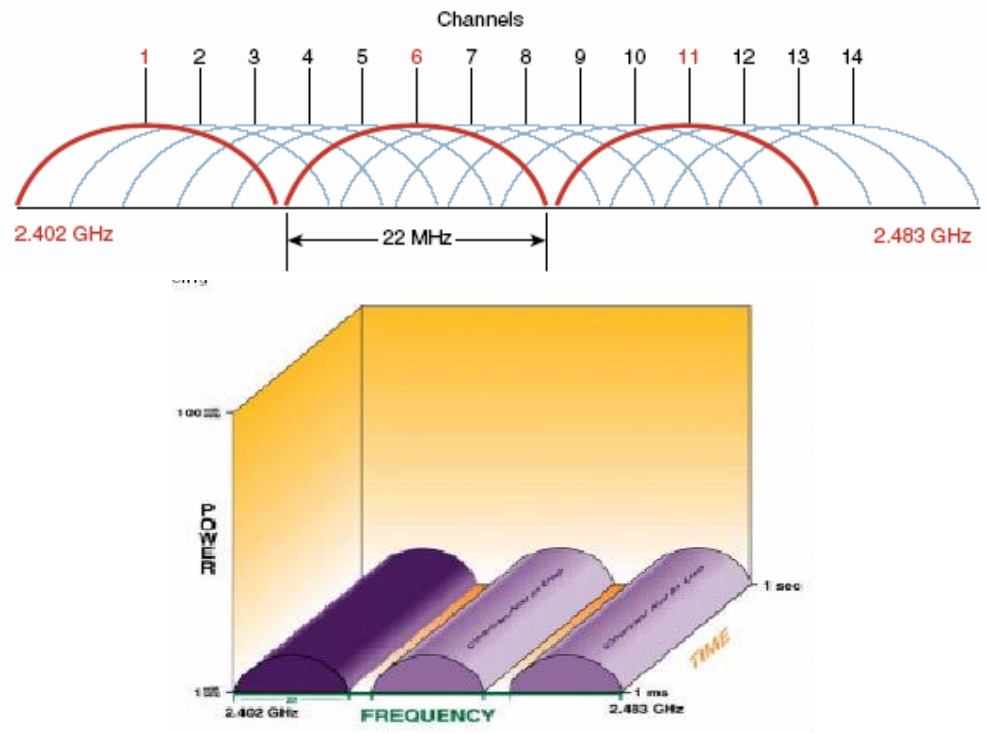
### 2.6.5 Tương quan giữa FHSS và DSSS

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.

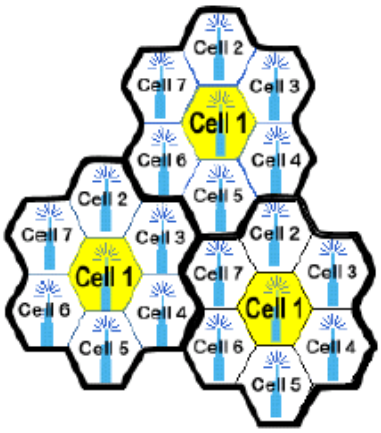
Như vậy chúng ta có thể thấy DSSS là kỹ thuật trải phổ có nhiều đặc điểm ưu việt hơn hẳn FHSS.

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 2.17: Bố trí số kênh phát trong một khu vực**




Sử dụng lại tần số trong mô hình có cấu trúc Cell

**Hình 2.18: Khả năng sử dụng lại tần số của phương pháp DSSS**

Như vậy trong 1 vùng đơn tốc độ bít vận chuyển đến có thể lên tới : 11Mbps x 3 = 33 Mbps, thay vì 11Mbps như khi chỉ có 1 kênh truyền được sử dụng trong 1 khu vực.

## 2.7.CHỨNG THỰC VÀ BẢO MẬT HỆ THỐNG WLAN

### 2.7.1 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.

### 2.7.2 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.

### 2.7.3 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.

### 2.7.4 Bảo mật dữ liệu thông qua EAP (Extensible Authentication Protocol) :

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

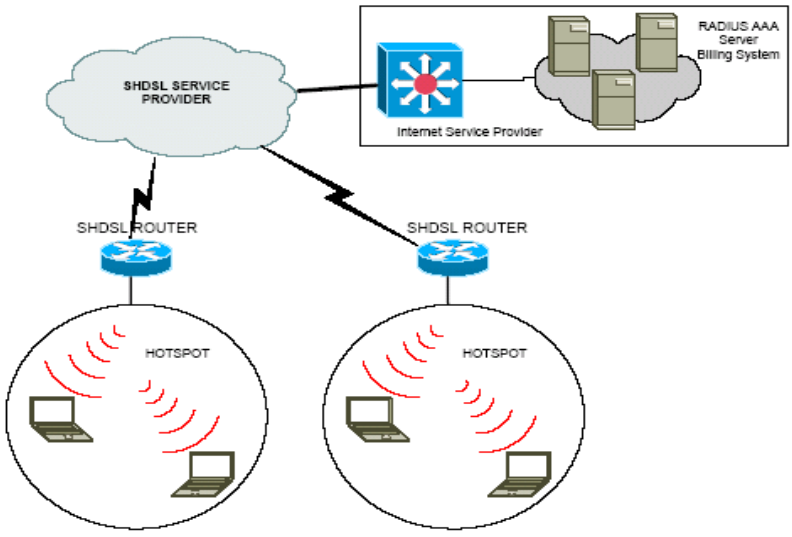
# Chương 3

# TRUYỀN DẪN TỚI ĐIỂM ĐẶT HOTSPOT VÀ CÁC MÔ HÌNH ĐẤU NỐI CHO HOTSPOT

## 3.1.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 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.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 3.1: Phương án truyền dẫn**

## 3.2.MÔ HÌNH ĐẤU NỐI CHO CÁC HOTSPORT

### 3.2.1 Các giải pháp kĩ 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.

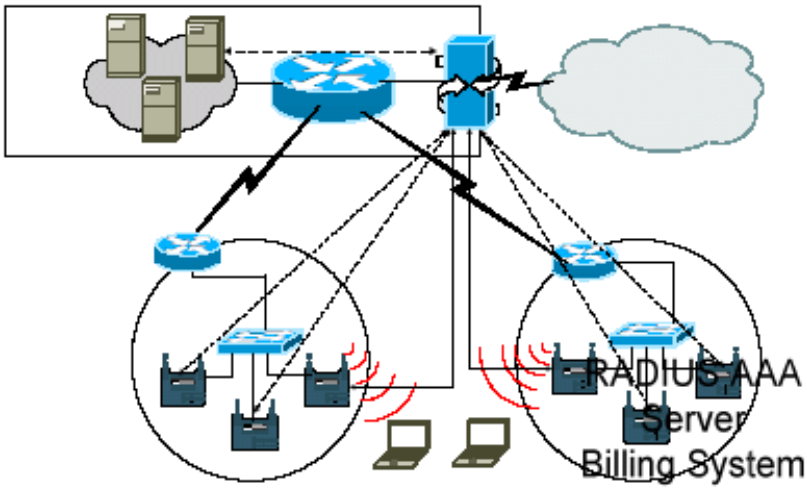
Người sử dụng sẽ được điều khiển tự động truy nhập vào một trang Web xác thực đã được xây dựng tích hợp trên các Subcriber Gateway. Tại đây, username/password sẽ được nhập vào. Subscriber Gateway liên lạc với AAA Server tập trung tại trung tâm quản lý điều hành mạng theo giao thức RADIUS để lấy thông 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.

### 3.2.2 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 3.2: Mô hình triển khai Gateway**

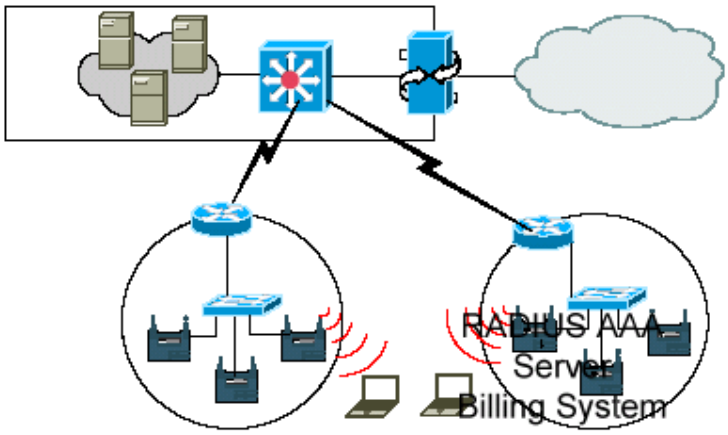
- **Ưu điểm**: Quản lý tập trung, trao đổi thông tin AAA giữa Subcriber Gateway và AAA Server chỉ là trao đổi thông tin trong mạng nội bộ.

- **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.

### 3.2.3 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 3.3: 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.

# Chương 4

# WEP VÀ LỌC(FILTERING)

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.

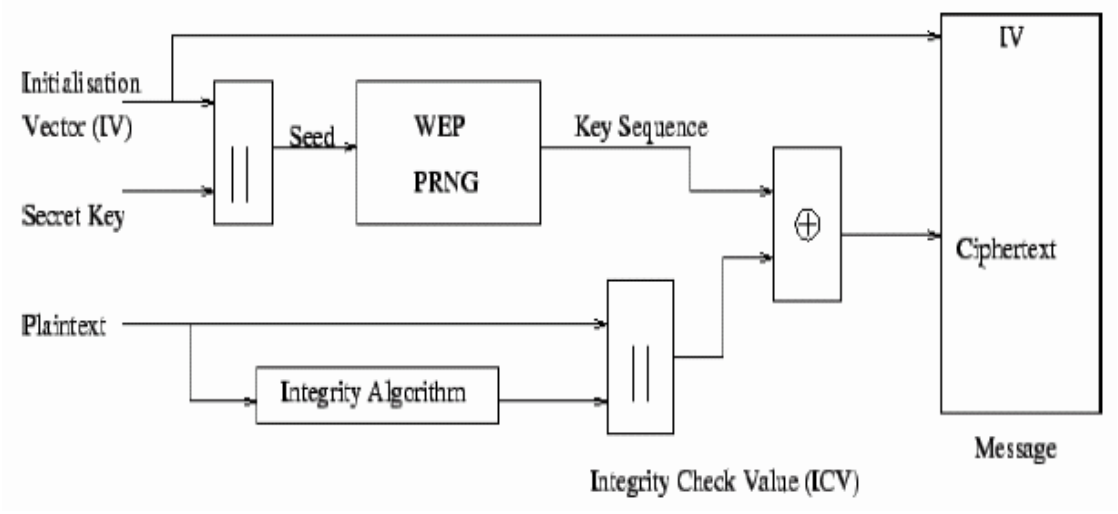
Trong phần này chúng ta cũng đề cập đến một vài biện pháp tấn công, từ đó mà người quản trị sẽ đưa được ra các biện pháp phòng ngừa. Sau đó chúng ta cũng bàn về các biện pháp bảo mật sẵn có, nhưng chưa được thừa nhận chính thức bởi bất cứ chuẩn 802. nào. Cuối cùng chúng ta cũng đưa ra vài khuyến nghị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

## 4.1.WEP ( WIRED EQUIVALENT PRIVACY )

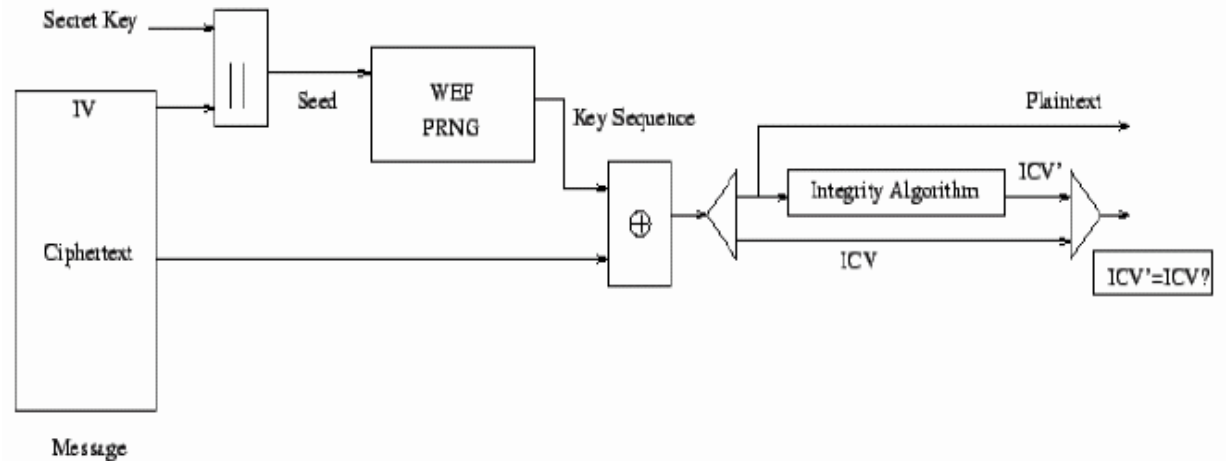
WEP (Wired Equivalent Privacy) là một thuật toán mã hóa sử dụng quá trình chứng thực khóa chia sẻ cho việc chứng thực người dùng và để mã hóa phần dữ liệu truyền trên những phân đoạn mạng Lan không dây. Chuẩn IEEE 802.11 đặc biệt sử dụng WEP.

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 4.1: Sơ đồ quá trình mã hóa sử dụng WEP**




**Hình 4.2: 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.

### 4.1.1 Tại sao WEP được 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.

### 4.1.2 Chìa khoá WEP

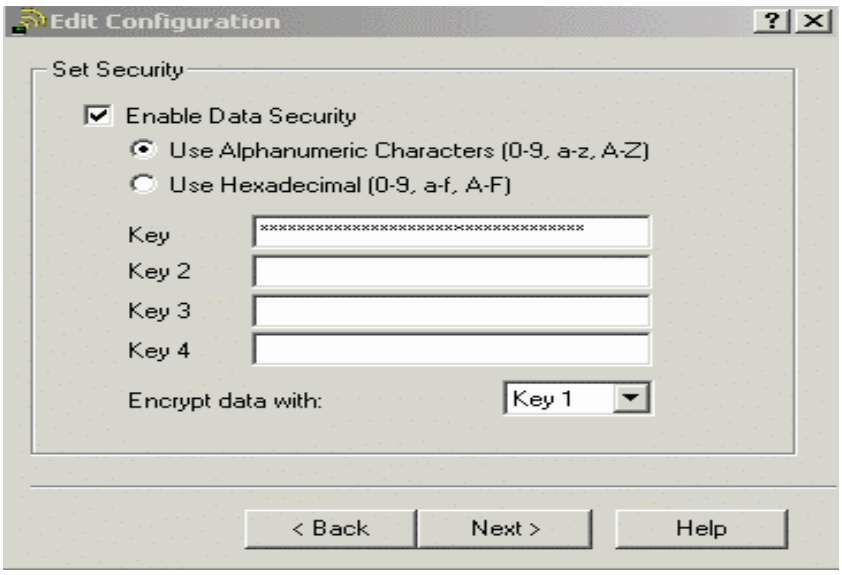
Vấn đề cốt lõi của WEP là chìa khóa WEP (WEP key). WEP key là một chuỗi ký tự chữ cái và số, được sử dụng cho hai mục đích cho WLAN

- 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 :



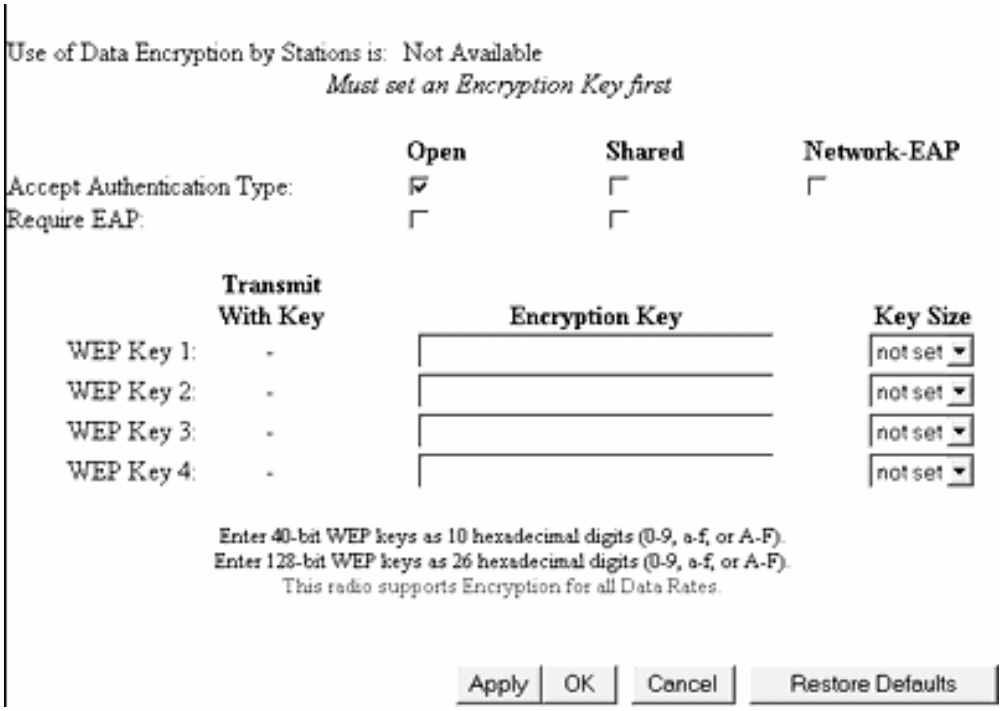

**Hình 4.3: Giao diện nhập chìa khóa Wep**

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.

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.




**Hình 4.4 : Sự hỗ trợ sử dụng nhiều chìa khóa WEP**

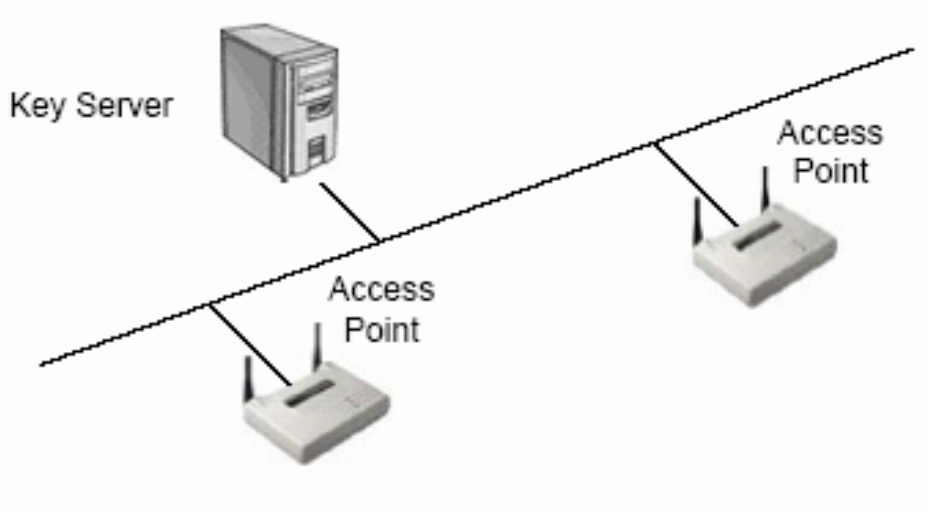
### 4.1.3 Sever quản lí chìa khoá mã hoá tập trung

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 4.5 : 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.

### 4.1.4 Cách sử dụng WEP

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

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

Khi các gói được gửi đi mà sử dụng mã hóa WEP, những gói này phải được giải mã. Quá trình giải mã này chiếm các chu kỳ của CPU, nó làm giảm đáng kể thông lượng trên WLAN. Một vài nhà sản xuất tích hợp các CPU trên các AP của họ cho mục đích mã hóa và giải mã WEP. Nhiều nhà sản xuất lại tích hợp cả mã hóa và giải mã trên một phần mềm và sử dụng cùng CPU mà được 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.

## 4.2.LỌC ( FILTERING)

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.

### 4.2.1 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.**

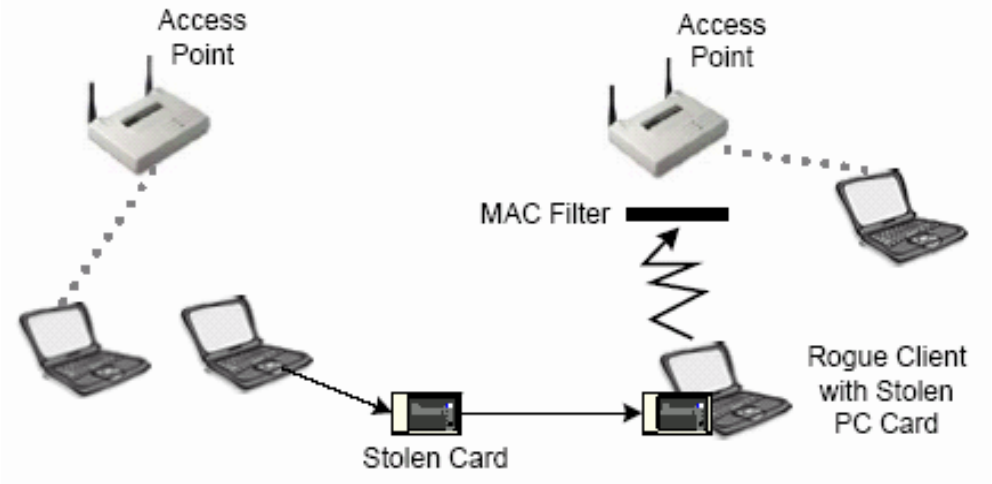
-***Làm cho SSID có gì đó liên quan đến công ty:*** Loại thiết lập này là một mạo hiểm về bảo mật vì nó làm đơn giản hóa quá trình một hacker tìm thấy vị trí vật lý của công ty. Khi tìm kiếm WLAN trong một vùng địa lý đặc biệt thì việc tìm thấy vị trí vật lý của công ty đã hoàn thành một nửa công việc. 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.

### 4.2.2 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 4.6: 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.

### 4.2.3 Circumventing Mac Filter

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

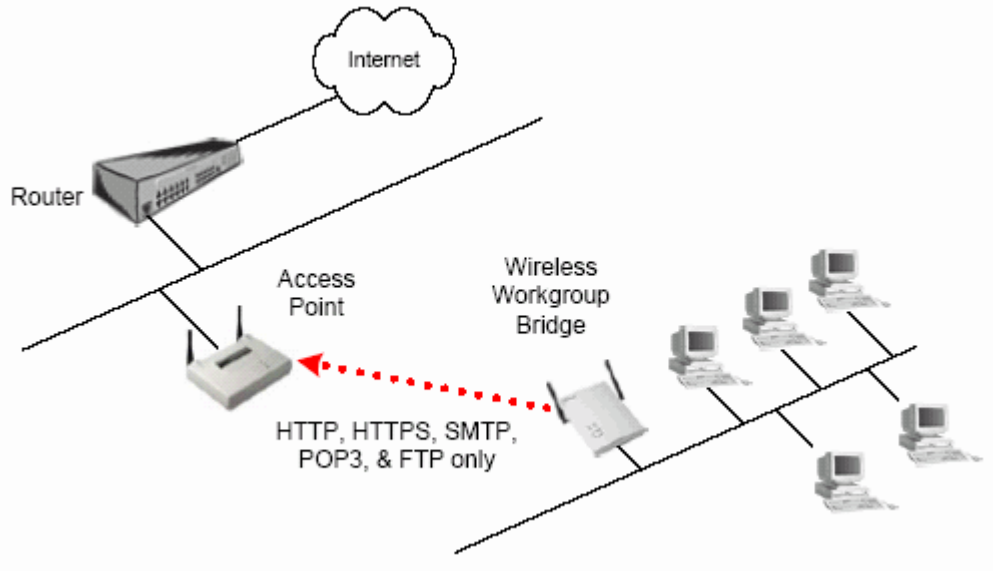
mạng là thời gian mà hacker có thể truy nhập vào mạng tốt nhất.

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

### 4.2.4 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 4.7: Lọc giao thức**

# Chương 5

# KHẢ NĂNG TẤN CÔNG TRÊN WLAN,CÁC GIẢI PHÁP,CHÍNH SÁCH VÀ KHUYẾN CÁO VỀ BẢO MẬT

## 5.1. CÁC KHẢ NĂNG TẤN CÔNG TRÊN WLAN

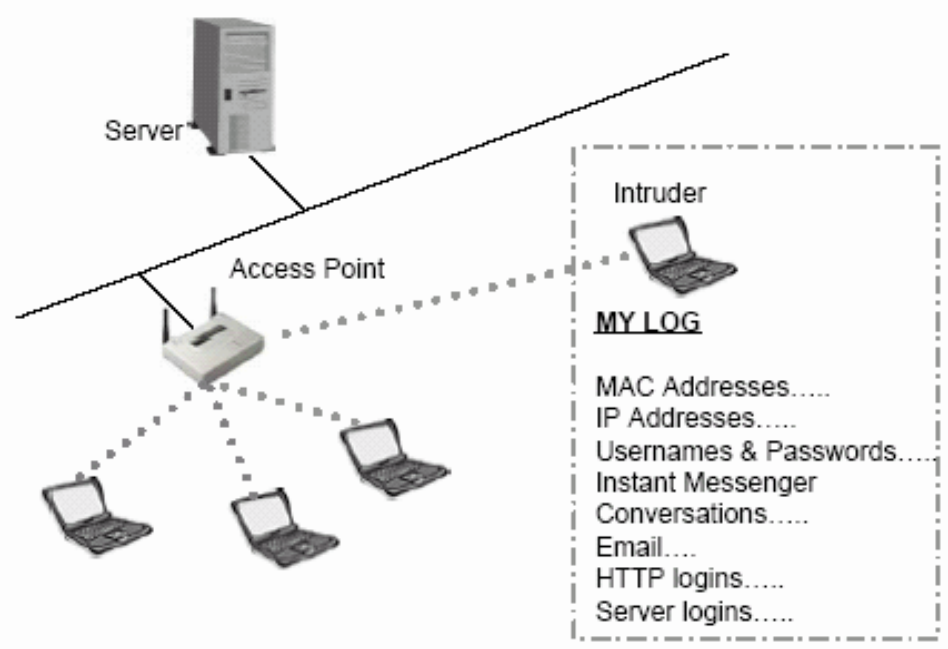
Một sự tấn công cố ý có thể gây vô hiệu hóa hoặc có thể tìm cách truy nhập WLAN trái phép theo một vài cách.

- **Tấn công bị động** (Nghe trộm) Passive attacks.
- **Tấn công chủ động** (kết nối, dò và cấu hình mạng) Active attacks.
- **Tấn công theo 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.

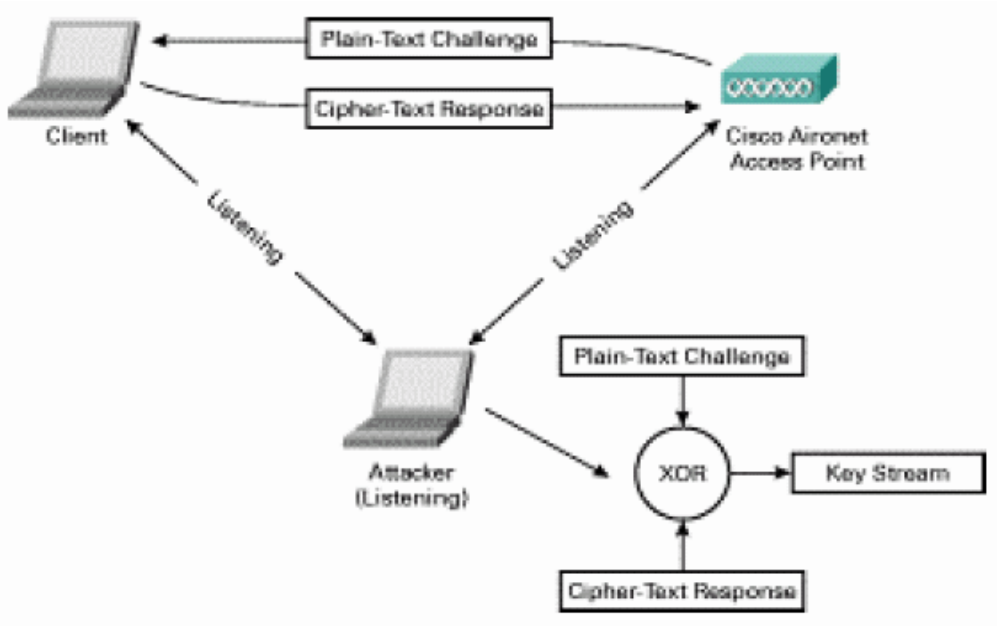
### 5.1.1 Tấn công bị động

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 5.1 : 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 5.2 : 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.

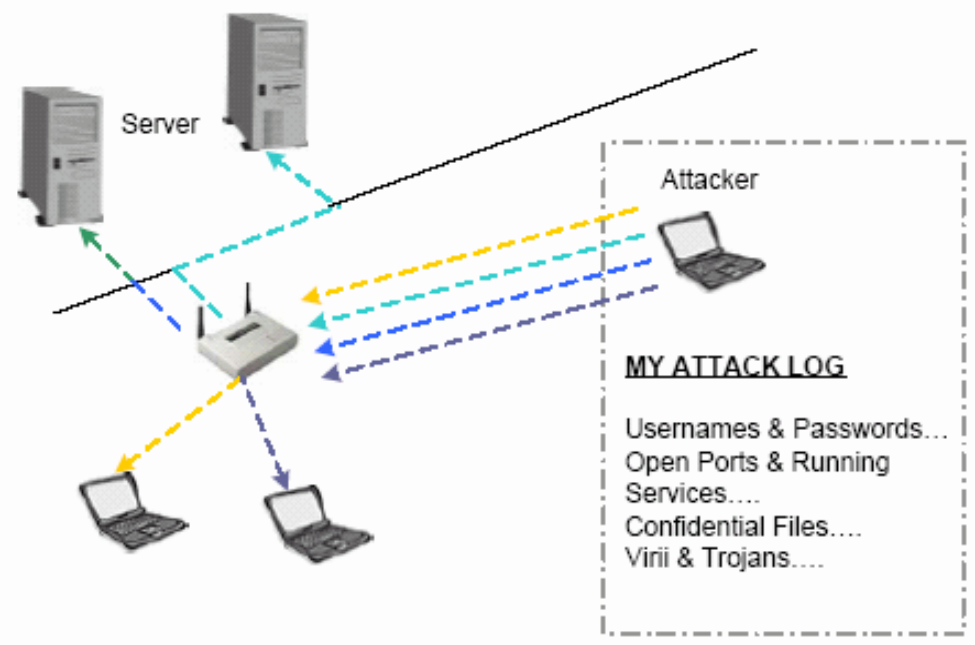
Hãy xem xét tác động nếu một hacker tìm được cách truy nhập tới một domain của người sử dụng, hacker đó sẽ đăng nhập vào domain của người sử dụng và gây hậu quả nghiêm trọng trên mạng. Tất nhiên việc đó là do hacker thực hiện, nhưng người dùng là người phải trực tiếp chịu trách nhiệm, và gánh chịu mọi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

### 5.1.2 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 5.3 : 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.

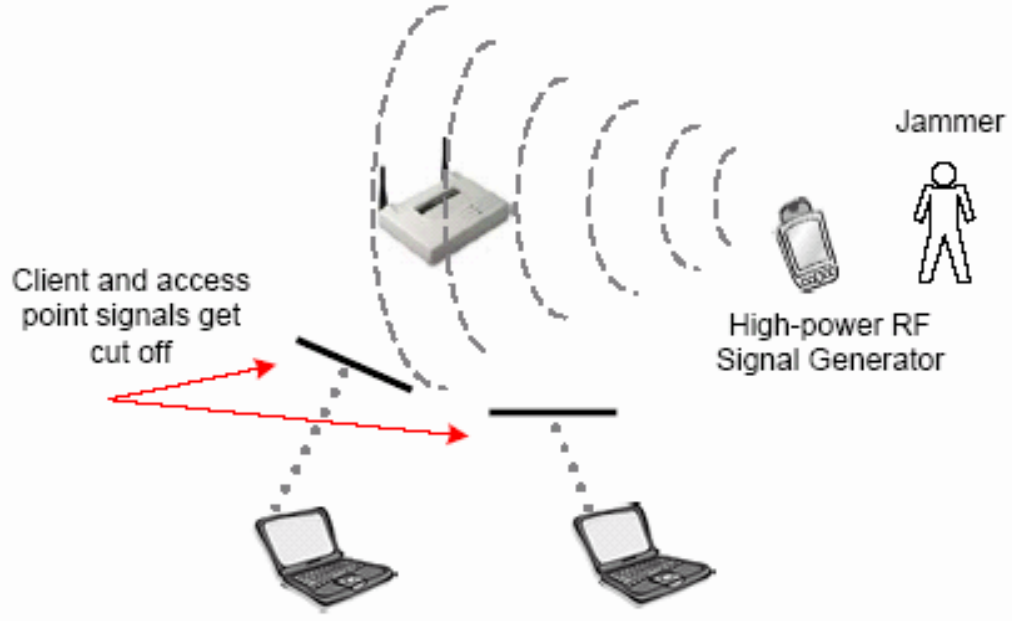
Khi hacker có kết nối không dây tới mạng của bạn thì anh ta cũng có thể truy cập vào mạng hữu tuyến trong văn phòng, vì hai sự kiện không khác nhau nhiều. Những kết nối không dây cho phép hacker về tốc độ, sự truy nhập tới server, kết nối tới mạng diện rộng, kết nối internet, tới desktop và laptop của 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.

### 5.1.3 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 5.4 : 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.

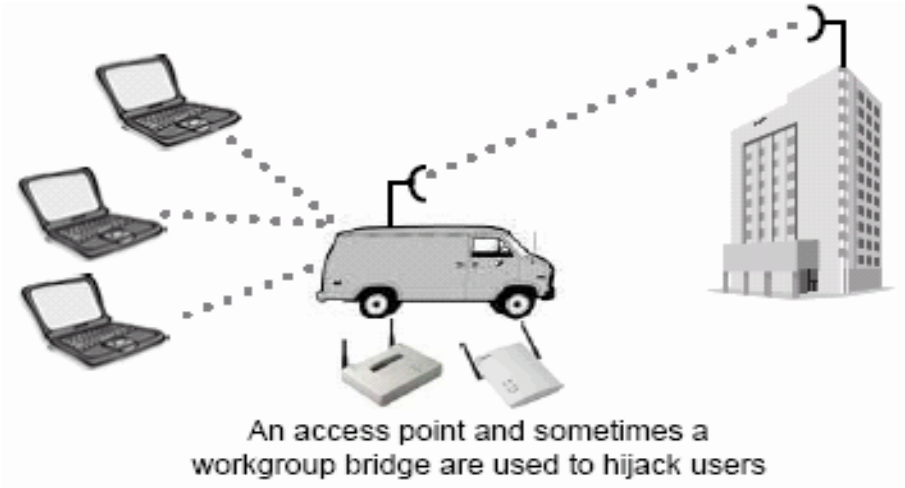
Khi Jamming gây ra bởi một nguồn cố định, không chủ ý, như một tháp truyền thông hoặc các hệ thống hợp pháp khác, thì người quản trị WLAN có thể phải xem xét đến việc sử dụng bộ thiết đặt các tần số khác nhau.

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.

### 5.1.4 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

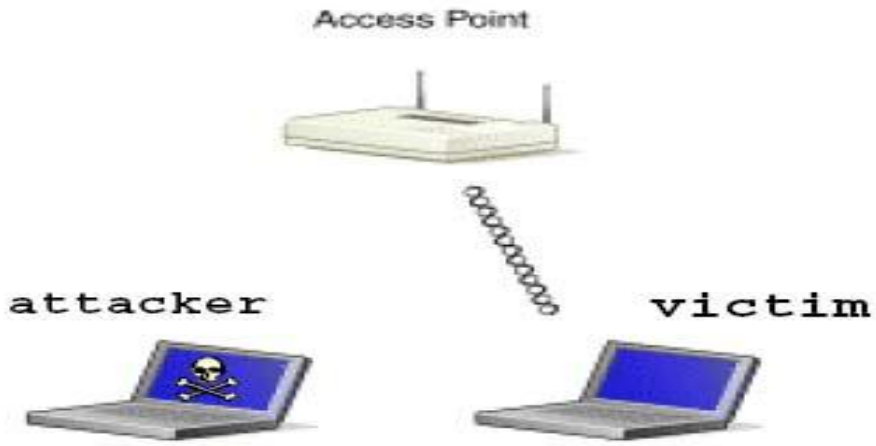



**Hình 5.5 : Man-in-the-middle attacks**

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 5.6 : Trước cuộc tấn công**


**Hình 5.7 : Và sau cuộc tấn công**

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

## 5.2.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 có thể đóng vai trò quan trọng trong mạng Lan không dây của bạn.

### 5.2.1 Quản lí chìa khoá 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.

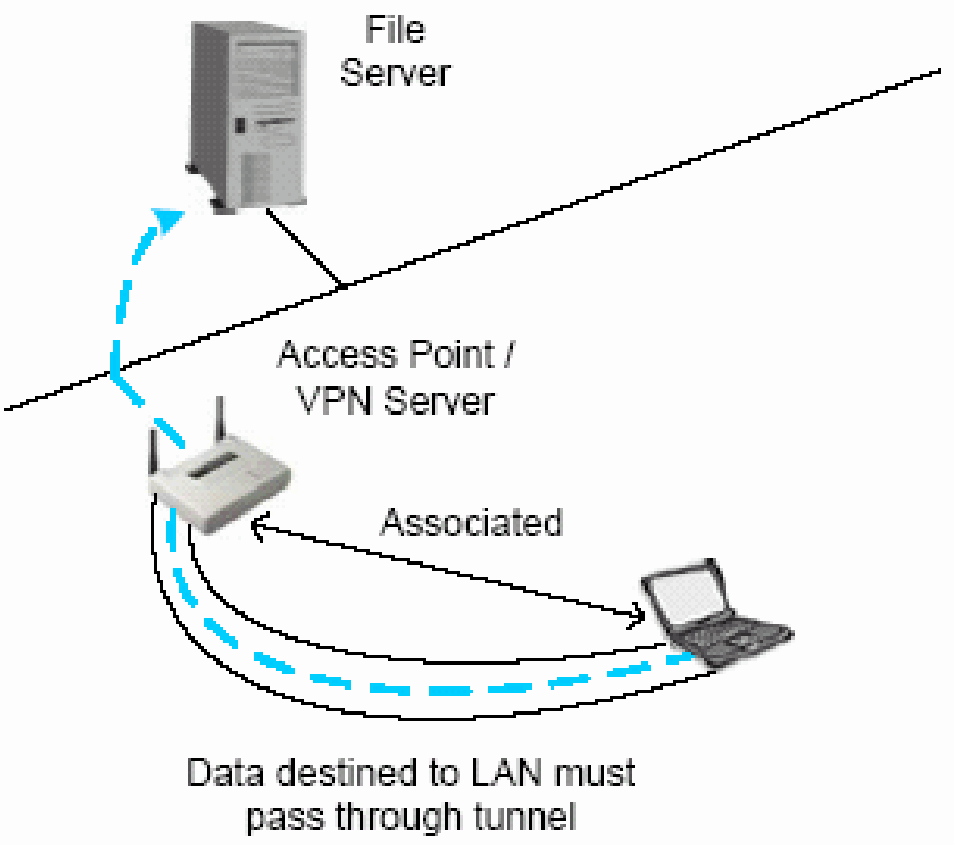
Để đặt một server quản lý chìa khóa mã hóa tập trung vào chỗ thích hợp, người quản trị WLAN phải tìm một ứng dụng mà thực hiện nhiệm vụ này, mua một server với một hệ điều hành thích hợp, và cấu hình ứng dụng theo nhu cầu. Quá trình này có thể tốn kém và cần nhiều thời giờ,

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.

### 5.2.2 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 5.8: 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 trên 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.

### 5.2.3 Kĩ thuật chì khoá 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.

### 5.2.4 Temporal Key Intergrity 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.

### 5.2.5 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.

### 5.2.6 Wireless Gateway

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

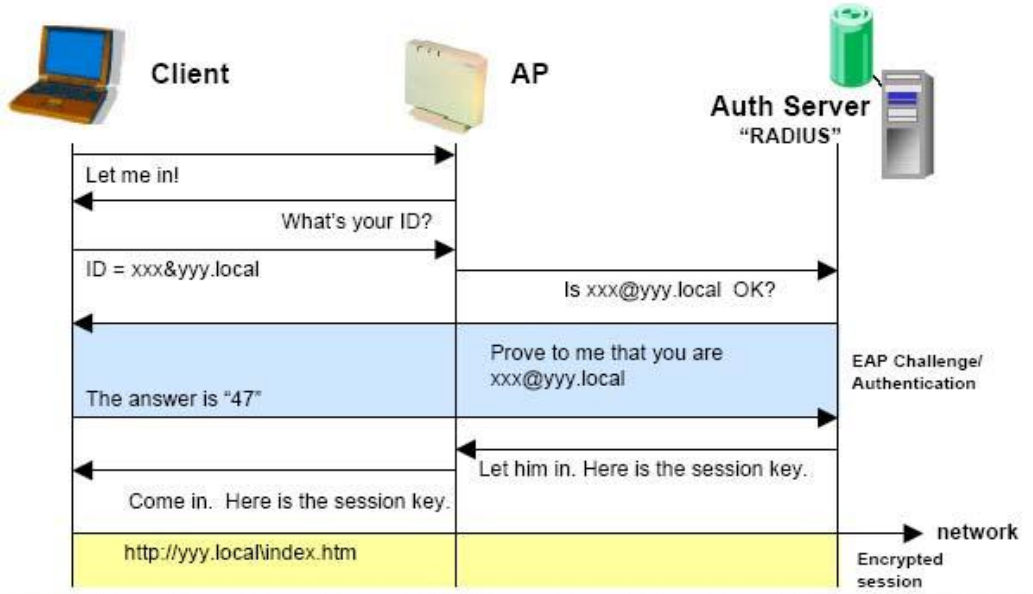
### 5.2.7 Về 802.1x và giao thức chứng thực mở

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 5.9: 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.

## 5.3.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.

### 5.3.1 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.

### 5.3.2 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 đề phòng thích hợp. Những biện pháp tối thiểu

phải làm là đặt lại bộ lọc MAC, thay đổi chìa khóa WEP,v.v.

Cho phép nhóm bảo vệ quét định kỳ xung quanh khu vực công ty để phát hiện những hoạt động đáng ngờ. Những nhân sự này được huấn luyện để nhận ra 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.

### 5.3.3 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.

### 5.3.4 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.

### 5.3.5 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.

### 5.3.6 Sự truy cập 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.

## 5.4.KHUYẾN CÁO VỀ BẢO MẬT

Vài khuyến cáo trong việc bảo mật mạng WLAN :

### 5.4.1 Khuyến cáo về 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.

### 5.4.2 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.

### 5.4.3 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.

### 5.4.4 Sự bảo mật cần thiết

Chọn một giải pháp bảo mật mà phù hợp với nhu cầu và ngân sách của tổ chức, cho cả bây giờ và mai sau. WLAN đang nhanh chóng phổ biến như vậy vì sự thực hiện dễ dàng. Một WLAN bắt đầu với 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.

### 5.4.5 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.

### 5.4.6 Theo dõi các phần cứng trái phép

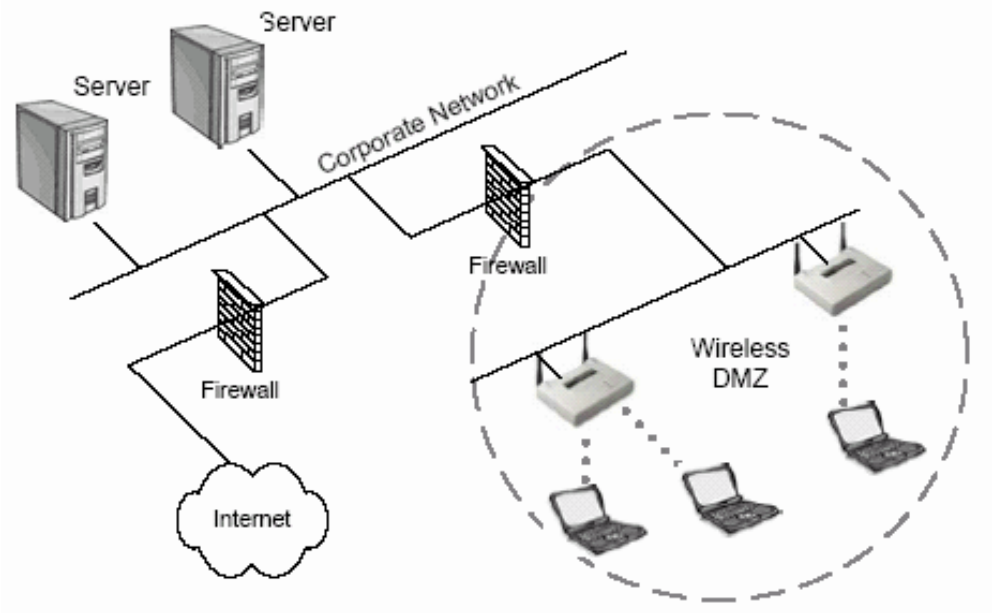
Để phát hiện ra các AP trái phép, các phiên dò các AP đó cần được hoạch định cụ thể nhưng không được công bố. Tích cực tìm và xóa bỏ các AP trái phép sẽ giữ ổn định cấu hình AP và làm tăng tính an toàn. Việc này có thể được thực hiện trong khi theo dõi mạng một cách bình thường và hợp lệ. Kiểu theo dõi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

### 5.4.7 Swiches 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.

### 5.4.8 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 5.10: Wireless DeMilitarized Zone**

### 5.4.9 Cập nhập 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.

# Chương 6

# TRIỂN KHAI MẠNG KHÔNG DÂY TẠI TRƯỜNG ĐẠI HỌC DÂN LẬP HẢI PHÒNG

Hiện nay mạng không dây ngày càng phổ biến, số giảng viên, cán bộ, sinh viên có máy tính xách tay ngày càng nhiều , nhu cầu làm việc,học tập thông qua mạng cũng tăng. Trước những đòi hỏi thực tế đó , việc xây dựng hệ thống mạng không dây cho nhà trường ngày càng cấp thiết.

## 6.1.Ý NGHĨA,MỤC ĐÍCH CỦA VIỆC TRIỂN KHAI MẠNG KHÔNG DÂY :

Phục vụ cho nhu vầu làm việc , học tập, nghiên cứu của giảng viên, cán bộ công nhân viên và sinh viên nhà trường.

- Phục vụ nhu cầu của học chế tín chỉ.
- Tận dụng tối đa nguồn tài nguyên mạng Lan và các đường truyền internet của nhà trường.
- Mở rộng khả năng làm việc của các ứng dụng nhà trường.
- Phục vụ sinh viên ngày càng tốt hơn.

Trung tâm Thông tin thư viện đã thành công nghiên cứu và thiết kế mạng không dây cho khu Giảng đường và khu Khách sạn sinh viên với mục tiêu :

- Cung cấp mạng không dây cho khách sạn sinh viên và khu giảng đường Trường Đại học Dân lập Hải Phòng.
- Kết nối mạng giữa khu Giảng đường và khu Khách sạn Sinh viên.
- Người dùng kết nối được ạng LAN, sử dụng các ứng dụng của

mạng nội bộ.

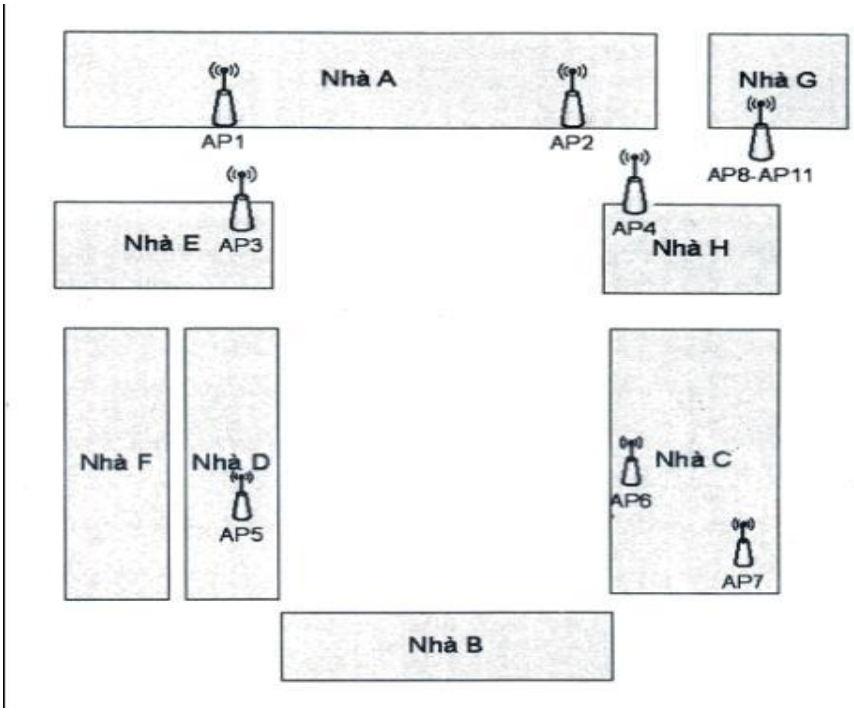
- Người dùng kết nối được vào mạng Internet tốc độ cao.
- Đáp ứng được cho 630 người dùng đồng thời.
- Đáp ứng được các nhu cầu bảo mật khác nhau.
- Linh hoạt khả năng tùy biến , thay đổi theo nhu cầu thực tế.

Đứng trước nhu cầu nghiên cứu học tập ngày càng lớn cán bộ, sinh viên, với xu hướng ngày càng hiện đại hóa cơ sở vật chất nhằm đưa trường Đại học Dân Lập Hải Phòng trở thành 1 ngôi trường hiện đại hệ thống mạng không dây đã được chấp thuận triển khai tại khu Giảng đường và khu Khách sạn sinh viên với trang thiết bị hạ tầng cở sở hiện đại.

## 6.2.SƠ ĐỒ TRIỂN KHAI :

### 6.2.1 Khu Giảng Đường

❖ **Sơ đồ thiết kế :**



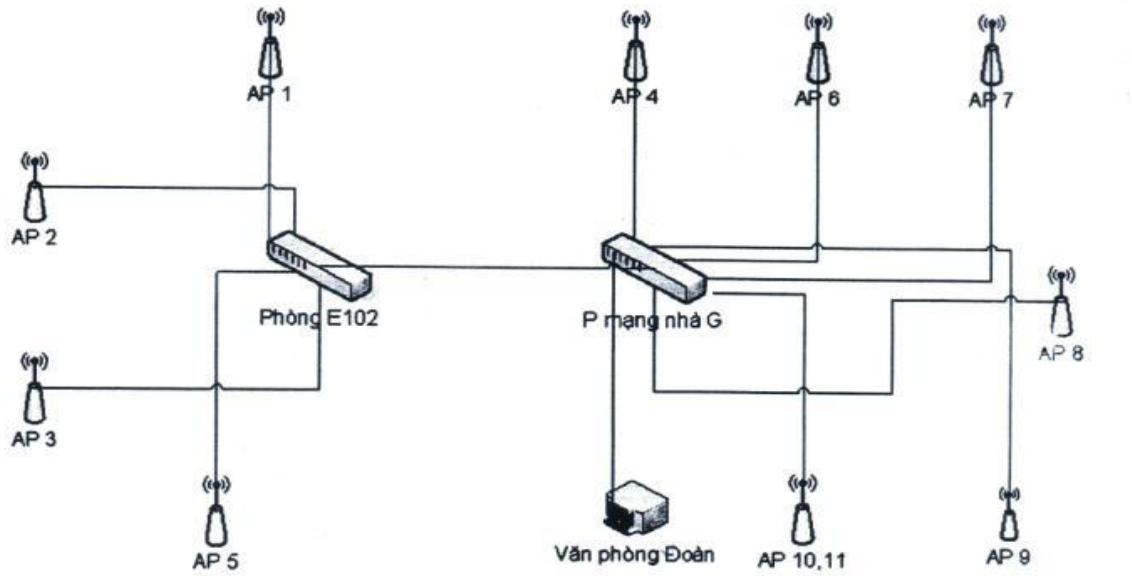

**Hình 6.1 : Vị trí lắp đặt các AP tại khu Giảng đường**

Hệ thống các AccessPoint bao gồm 11 Wireless Router được bố trí lắp đặt tại các vị trí lần lượt 2 Wireless Router tại phía trước khu nhà A, 1 Wireless Router tại phía trước nhà C , 1 Wireless Router tại nhà D, 1 thiết bị tại nhà H, 1 thiết bị tại nhà E , 1 thiết bị tại nhà phòng quản trị mạng, 1 thiết bị tại cawngtin sinh viên và 4 Wireless Router lắp đặt tại các tầng khu nhàG.

| AP | Loại thiết bị | Vị trí | Kênh | Ghi chú |
|---|---|---|---|---|
| AP1 | WRT110N hoặc WRT610N | A202 | 1 | |
| AP2 | WRT110N hoặc WRT610N | A204 | 5 | |
| AP3 | WRT110N hoặc WRT610N | E301 | 9 | |
| AP4 | WRT110N hoặc WRT610N | Ban dự án | 11 | |
| AP5 | WRT110N hoặc WRT610N | C203 | 3 | |
| AP6 | WRT110N hoặc WRT610N | D202 | 7 | |
| AP7 | WRT110N hoặc WRT610N | Phía sau C104 | 10 | Dùng cho căngtin SV |
| AP8 | WRT110N hoặc WRT610N | Tầng 2 nhà G | 2 | |
| AP9 | WRT110N hoặc WRT610N | Tầng 3 nhà G | 6 | |
| AP10 | WRT110N hoặc WRT610N | Tầng 4 nhà G | 8 | |
| AP11 | WRT110N hoặc WRT610N | Tầng 5 nhà G | 4 | |

❖ **Sơ đồ kết nối vật lý :**

**2. Sơ đồ kết nối vật lý các AP**




**Hình 6.2 : sơ đồ kết nối vật lý các AP tại khu Giảng đường**

Các AP 1,2,3,5 được nối về phòng Quản trị mạng E102, các AP 4,6,7,8,9,10 được nối về Phòng mạng nhà G, ngoài ra tăng cường cho Văn phòng Đoàn 1 đường mạng nối về nhà G. Các AP truy cập mạng internet thông qua Proxy của trường.

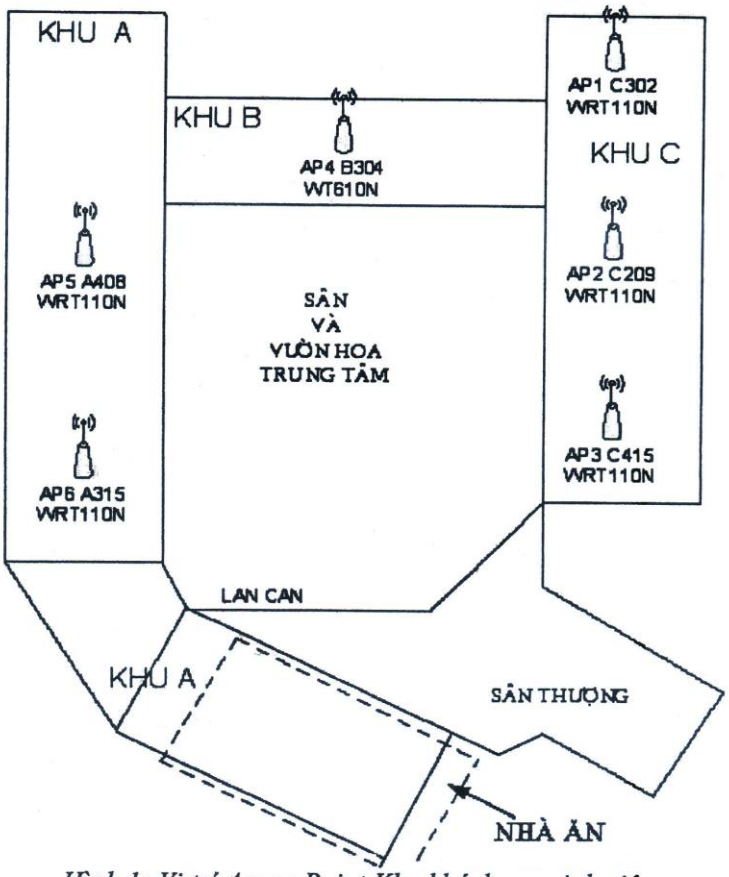
Cấu hình thiết bị :

| Thiết bị | IP | Gateway | SSID | DHCP | Ghi chú |
|---|---|---|---|---|---|
| **AP1** | **10.8.1.1/16** | **10.8.0.1** | **HPU** | **10.8.1.10:40** | |
| **AP2** | **10.8.2.1/16** | **10.8.0.1** | **HPU** | **10.8.1.10:40** | |
| **AP3** | **10.8.3.1/16** | **10.8.0.1** | **HPU** | **10.8.1.10:40** | |
| **AP4** | **10.8.4.1/16** | **10.8.0.1** | **HPU** | **10.8.1.10:40** | |
| **AP5** | **10.8.5.1/16** | **10.8.0.1** | **HPU** | **10.8.1.10:40** | |
| **AP6** | **10.8.6.1/16** | **10.8.0.1** | **HPU** | **10.8.1.10:40** | |

| | | | | | |
|---|---|---|---|---|---|
| **AP7** | **10.8.1.1/16** | **10.9.0.1** | **HPU** | **10.9.1.10:40** | |
| **AP8** | **10.8.2.1/16** | **10.9.0.1** | **HPU** | **10.9.1.10:40** | |
| **AP9** | **10.8.3.1/16** | **10.9.0.1** | **HPU** | **10.9.1.10:40** | |
| **AP10** | **10.8.4.1/16** | **10.9.0.1** | **HPU** | **10.9.1.10:40** | |

### 6.2.2 Khu Khách Sạn Sinh Viên

❖ **Sơ đồ thiết kế :**



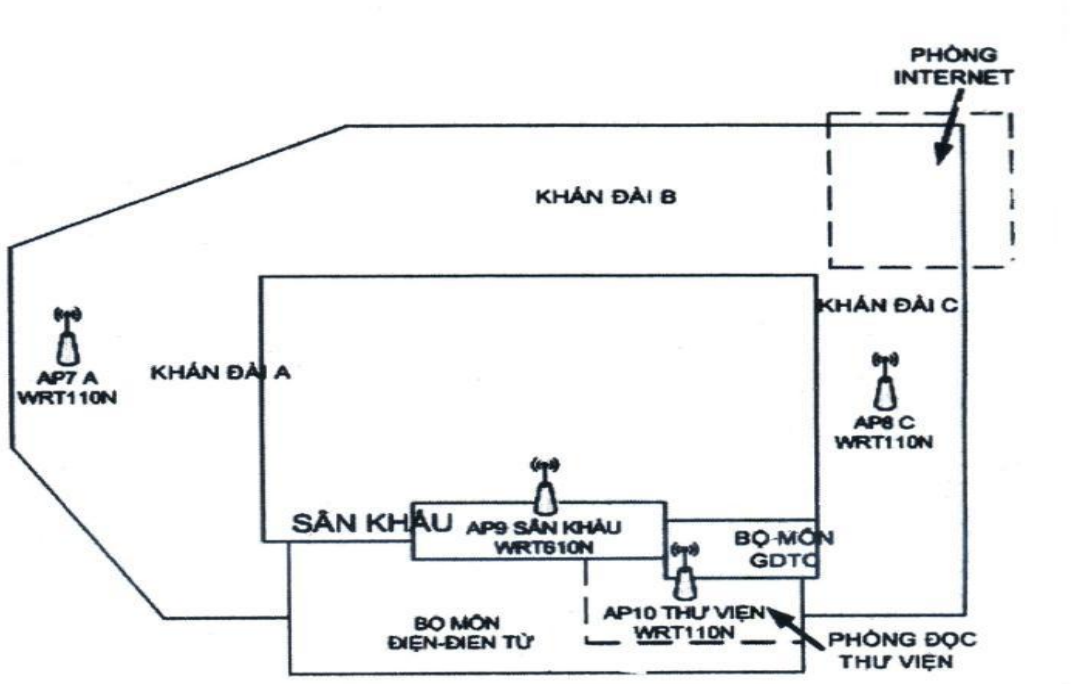

*Hình 1: Vị trí AccessPoint Khu khách sạn sinh viên*

**Hình 6.3 : vị trí các AccessPoint lắp đặt tại Khu khách sạn sinh viên**

Hệ thống các AccessPoint bao gồm 6 Wireless Router được bố trí lắp đặt tại các vị trí thích hợp bao quát toàn bộ khu vực Khách sạn sinh viên nhằm đảm bảo các bạn sinh viên nội trú trong khách sạn đều có thể truy cập vào mạng không dây của trường.

| AP | Loại thiết bị | Vị trí | Kênh | Ghi chú |
|---|---|---|---|---|
| AP1 | WRT110N hoặc WRT610N | C302 | 1 | |
| AP2 | WRT110N hoặc WRT610N | C209 | 3 | |
| AP3 | WRT110N hoặc WRT610N | C415 | 5 | |
| AP4 | WRT110N hoặc WRT610N | B304 | 7 | |
| AP5 | WRT110N hoặc WRT610N | A408 | 9 | |
| AP6 | WRT110N hoặc WRT610N | A315 | 11 | |

### 6.2.3 Khu Nhà Tập Đa Năng

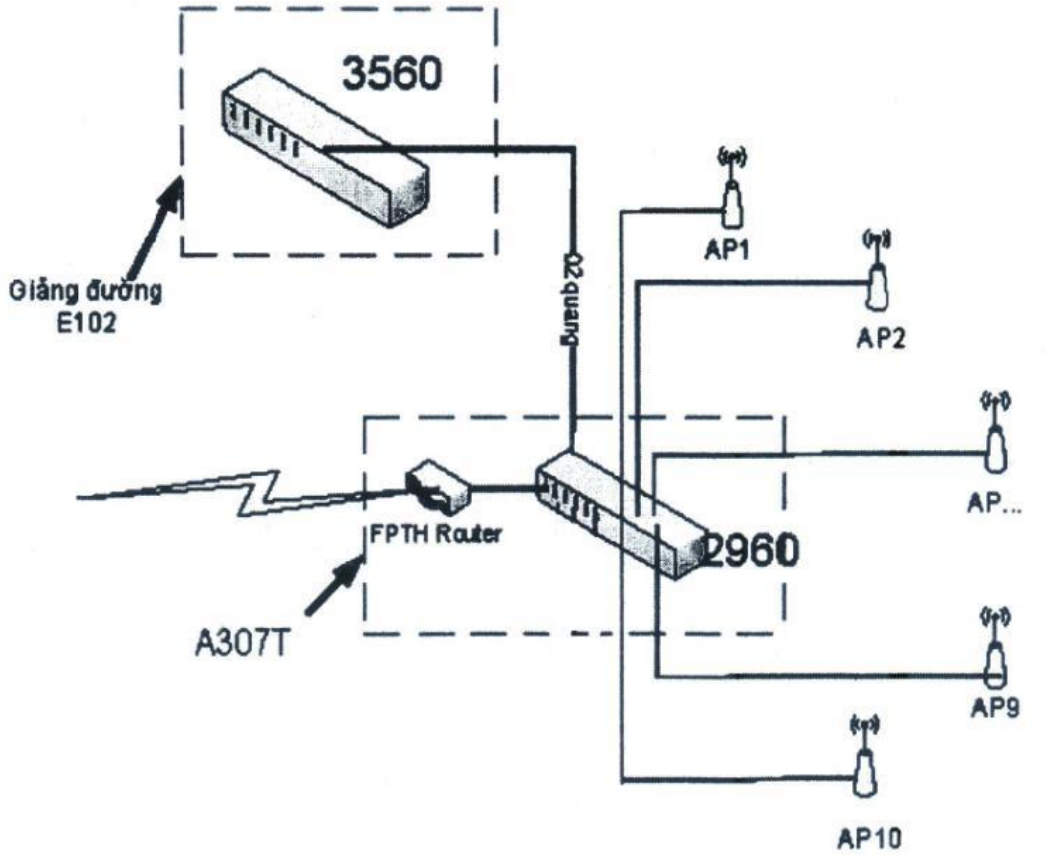



**Hình 6.4 : Vị trí các AccessPoint Khu nhà tập đa năng**

Hệ thống các Wireless Router được bố trí 4 thiết bị đặt tại 4 vị trí khác nhau bao gồm từ AP 7 tới AP 10.

| AP | Loại thiết bị | Vị trí | Kênh | Ghi chú |
|---|---|---|---|---|
| AP7 | WRT110N hoặc WRT610N | Khán đài A | 2 | |
| AP8 | WRT110N hoặc WRT610N | Khán đài C | 4 | |
| AP9 | WRT110N hoặc WRT610N | Đỉnh sân khấu | 6 | |
| AO10 | WRT110N hoặc WRT610N | Phòng đọc thư viện | 8 | |

❖ **Sơ đồ kết nối vật lý các AP tại khu Khách sạn sinh viên** :




**Hình 6.5 : mô hình kết nối vật lý AP khu Khách sạn sinh viên**

Tất cả các AP đều được nối về Swich 2960 tại phòng A307T, để phục vụ cho công việc của ban công tác Sinh viên, Phòng đọc, Phòng máy KSSV-Trung tâm thông tin thư viện.

Các AP truy cập internet thông qua đường FPTH tại phòng A307T, Khi các AP làm việc với các ứng dụng trong trường sẽ thông qua đường cáp quang , riêng Phòng đọc KSSV và Phòng quản sinh thì được điều chỉnh truy cập vào internet theo đường nào tùy theo nhu cầu thực tế.

Cấu hình các thiết bị :

| Thiết bị | IP | Gateway | SSID | DHCP | Route add | Ghi chú |
|---|---|---|---|---|---|---|
| **FPTH** | **10.11.0.2/16** | | | | | **No AP** |
| **AP1** | **10.11.1.1/16** | **10.11.0.2** | **KSSV** | **10.11.1.10:40** | **10.11.0.0/16 > 10.1.0.1** | |
| **AP2** | **10.11.2.1/16** | **10.11.0.2** | **KSSV** | **10.11.2.10:40** | **10.11.0.0/16 > 10.1.0.1** | |
| **AP3** | **10.11.3.1/16** | **10.11.0.2** | **KSSV** | **10.11.3.10:40** | **10.11.0.0/16 > 10.1.0.1** | |
| **AP4** | **10.11.4.1/16** | **10.11.0.2** | **KSSV** | **10.11.4.10:130** | **10.11.0.0/16 > 10.1.0.1** | |
| **AP5** | **10.11.5.1/16** | **10.11.0.2** | **KSSV** | **10.11.5.10:40** | **10.11.0.0/16 > 10.1.0.1** | |
| **AP6** | **10.11.6.2/16** | **10.11.0.2** | **KSSV** | **10.11.6.10:40** | **10.11.0.0/16 > 10.1.0.1** | |
| **AP7** | **10.11.7.1/16** | **10.11.0.2** | **KSSV** | **10.11.7.10:40** | **10.11.0.0/16 > 10.1.0.1** | |
| **AP8** | **10.11.8.1/16** | **10.11.0.2** | **KSSV** | **10.11.8.10:40** | **10.11.0.0/16 > 10.1.0.1** | |
| **AP9** | **10.11.9.1/16** | **10.11.0.2** | **KSSV** | **10.11.9.10:130** | **10.11.0.0/16 > 10.1.0.1** | |
| **AP10** | **10.11.10.1/16** | **10.11.0.2** | **KSSV** | **10.11.10.10:40** | **10.11.0.0/16 > 10.1.0.1** | |

Hệ thống mạng của khu Khách sạn sinh viên và khu Giảng đường được kết nối với nhau bởi 2 đường cáp quang tốc độ 1 Gbx2 nối giữa 1 thiết bị Swich 3560 tại phòng E102 ( khu Giảng đường) và Swich 2960 tại phòng A307T ( khu Khách sạn sinh viên).

# Chương 7

# CẤU HÌNH THIẾT BỊ MẠNG KHÔNG DÂY

## 7.1.CẤU HÌNH THIẾT BỊ WIRELESS ROUTER

Hệ thống mạng không dây Wireless Lan bao gồm 2 phần là Lan và Wireless trong đó Wireless là phần không dây bao gồm hệ thống các Wireless Router lắp đặt cố định tại các điểm đã thiết kế.Khác với các Access Point (chỉ có cổng cắm LAN) không cấp phát địa chỉ IP, cắm vào là dùng được luôn, bên cạnh đó là bảo mật kém và chỉ nên dùng khi đặt trong một mạng an toàn có sẵn tường lửa, router...thì Wireless Router (thêm cổng cắm ghi rõ chữ WAN) có khả năng bảo mật tốt hơn, được cấu hình là DHCP Server để cấp phát địa chỉ IP động, vừa làm nhiệm vụ kết nối không dây, vừa kết nối các máy không có adapter wireless với Internet như máy tính để bàn thông thường . Các Wireless Router được sử dụng trong hệ thống gồm 2 loại là WRT110N và WRT610N, 2 loại Wireless Router này có tính năng tương thích với nhau , có thể thay thế lẫn nhau.

### 7.1.1 Linksys Wireless Router WRT110N

- **Mặt trước, mặt sau**


**Hình 7.1** : **Linksys Wireless Router**

❖ **Các tính năng nổi trội** :

- Chia sẻ kết nối Internet và 4 cổng chuyển mạch, được tích hợp sẵn tính năng nâng cao tốc độ và vùng phủ sóng.

- Công nghệ anten thông minh MIMO hỗ trợ mở rộng khoảng cách và làm giảm các điểm chết.

- làm việc với các thiết bị chuẩn N sẽ nhanh hơn tốc độ chuẩn G nhiều lần, nó có thể làm việc được với các thiết bị không dây chuẩn G và B.

- Các tín hiệu không dây được bảo vệ nhờ kỹ thuật mã hoá bảo mật không dây và bảo vệ mạng tránh được các tấn công từ ngoài Internet dựa vào tính năng tường lửa SPI .WRT110 tích hợp 3 thiết bị trong một hộp. Thứ nhất, điểm truy nhập không dây hỗ trợ truy cập mạng mà không cần đến dây dẫn. Thứ hai, tích hợp 4 cổng chuyển mạch 10/100 để kết nối tới mạng có dây. Cuối cùng, chức năng định tuyến có khả năng định tuyến toàn bộ mạng LAN của bạn ra ngoài Internet qua một kết nối DSL hay cáp.

- WRT110 sử dụng công nghệ mạng không dây mới nhất hiện nay là Wireless-N (draft 802.11n). Dựa vào khả năng bao phủ rộng nhiều tín hiệu

sóng vô tuyến, nên công nghệ MIMO của Wireless-N đem lại hiệu suất truyền dữ liệu rất lớn. Không như các công nghệ mạng không dây trước đó luôn bị hạn chế bởi sự phản xạ tín hiệu thì công nghệ MIMO thường sử dụng các tín hiệu phản xạ đó để làm tăng phạm vi và làm giảm "điểm chết" trong vùng phủ sóng mạng không dây.

- Với công nghệ chuẩn Wireless-N bạn có thể ở khoảng cách xa hơn mà vẫn có thể truy nhập được vào mạng không dây hay có thể truyền dữ liệu với tốc độ nhanh hơn. WRT110 có khả năng làm việc với các thiết bị không dây chuẩn -G và –B, nhưng chỉ đạt hiệu suất cao nhất khi ở cả hai đầu đều là các thiết bị chuẩn Wireless-N. Khi làm việc với các thiết bị chuẩn -G và –B hiệu suất sẽ không đạt tối đa, tuy vậy hệ thống vẫn hoạt động bình thường.

- Để bảo vệ tính riêng tư của dữ liệu, WRT110 hỗ trợ các công nghệ mã hoá bảo mật như WEP và WPA, có khả năng mã hoá tất cả các đường truyền không dây nhờ sức mạnh của kỹ thuật mã hoá 256-bits. Công nghệ lọc địa chỉ MAC, cũng giúp bạn có thể cho phép các đối tượng nào có thể truy nhập vào mạng không dây của mình hay không. WRT110 hỗ trợ tiện ích cấu hình dựa trên trình duyệt web thân thiện. Được tích hợp tính năng DHCP Server nên nó có thể cấp địa chỉ IP động cho các máy tính trong mạng của bạn.

- Với tốc độ vô cùng lớn mà WRT110 hỗ trợ, thì nó là một giải pháp lý tưởng cho bạn khi muốn chạy các ứng dụng như VoIP, chơi game hay xem video. Khi đặt thiết bị này tại trung tâm trong mạng văn phòng hay gia đình, bạn có thể chia sẻ các kết nối Internet tốc độ cao, ứng dụng chạy các ứng dụng đa phương tiện, chơi game trực tuyến, chia sẻ máy in hay truyền các file dữ liệu với tốc độ cao.

### 7.1.2 Linksys WRT610N-Dual-Band Wireless-N Gigabit Router

❖ **Các tính năng :**

- Bộ định tuyến chia sẻ Internet với 4 cổng chuyển mạch Gigabit, được xây dựng trên kiến trúc dual-band, nhằm cải thiện về khả năng phủ sóng và tốc độ cho điểm truy cập không dây.

- Sử dụng hai dải tần số radio riêng biệt nhằm tăng băng thông cho mạng.Công nghệ không dây chuẩn N sử dụng nhiều tần số radio với mục đích tăng công suất phát tín hiệu, mở rộng vùng phủ sóng, cải thiện tốc độ, và giảm thiểu điểm chết.

- Kết nổi tới ổ đĩa cứng hoặc thiết bị lưu trữ Flash cho phép truy cập tới các file ca nhạc, video, hoặc file dữ liệu từ mạng nội bộ hoặc mạng Internet.

- Tính năng bảo mật nâng cao và tường lửa SPI cho phép bảo vệ những tấn công từ bên ngoài Internet vào trong mạng.

- Kiểu dáng đẹp, được thiết kế đồng thời với dải tần kép, thiết bị router không dây làm việc đồng thời với hai băng tần radio trong cùng một thời điểm. Hoạt động với băng thông tăng gấp hai lần một cách trôi chảy cho những ứng dụng giải trí như video, gaming, và ca nhạc một cách liên tục, trong khi truy cập Internet, chia sẻ files, gửi nhận email, in ấn và một số tác vụ khác. Công nghệ không dây chuẩn N mang đến cho bạn khả năng phủ sóng và tốc độ cho cả hai dải tần số.

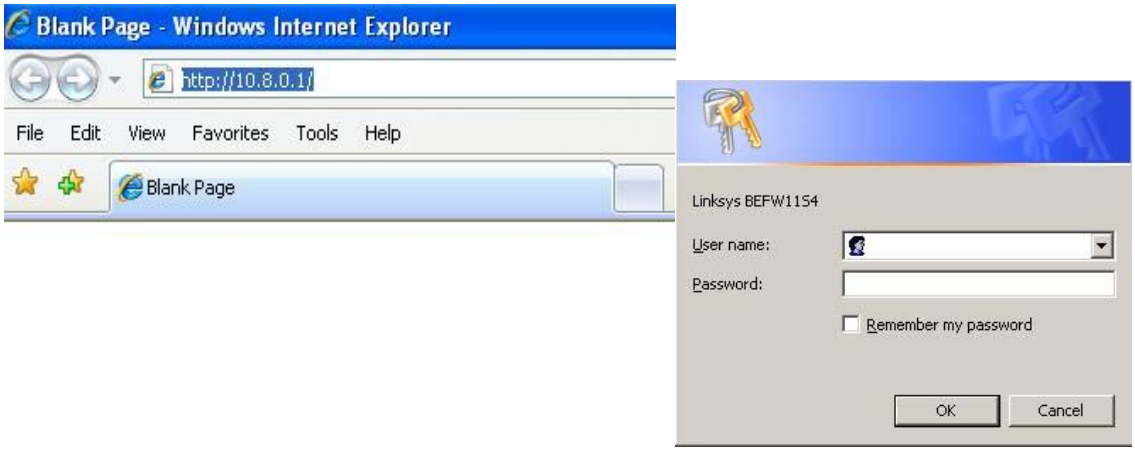
- Với thuộc tính liên kết thiết bị lưu trữ cho phép bạn kết nối tới ỗ đĩa cứng hoặc thiết bị lưu trữ USB trực tiếp tới mạng của bạn một cách dễ dàng với tốc độ gigabytes của thiết bị lưu trữ. Truy cập tới các file ca nhạc, file video, hoặc các file dữ liệu từ máy tính cá nhân với hệ thống mạng của bạn. Xây dựng trên kiến trúc cổng Gigabit cung cấp cho một kết nối ở xa nhanh hơn tới các thiết bị trong mạng có dây qua cổng Ethernet.

- Cài đặt dễ dàng và nhanh chóng với máy tính cá nhân hoặc máy Mac, tích hợp cài đặt cho người sử dụng lần đầu tiên, và tạo ra kết nối không dây có tính bảo mật cao bằng cách nhấn nút Wi-fi Protected SetupTM, thiết bị bao gồm chương trình Linksys EasyLink Advisor như một công nghệ dành cho chuyên gia giúp cho bạn quản lý và điều chỉnh mạng của bạn khi mạng của bạn phát triển.

- Với thiết bị Linksys Simultaneous Dual-N Band Wireless Router đặt tại trung tâm trong gia đình hoặc văn phòng, bạn có thể dễ dàng sử dụng tính năng lưu trữ, chia sẻ kết nối Internet tốc độ cao. Chia sẻ file, in ấn và chạy những ứng dụng game…

### 7.1.3 Thiết lập cấu hình

Truy cập trực tiếp vào địa chỉ 10.8.0.1, đăng nhập với User name và password của Admin để conect tới thiết Wireless Router và thiết lập các thông số theo yêu cầu :




**Hình 7.2 : kết nối tới Wireless Router**

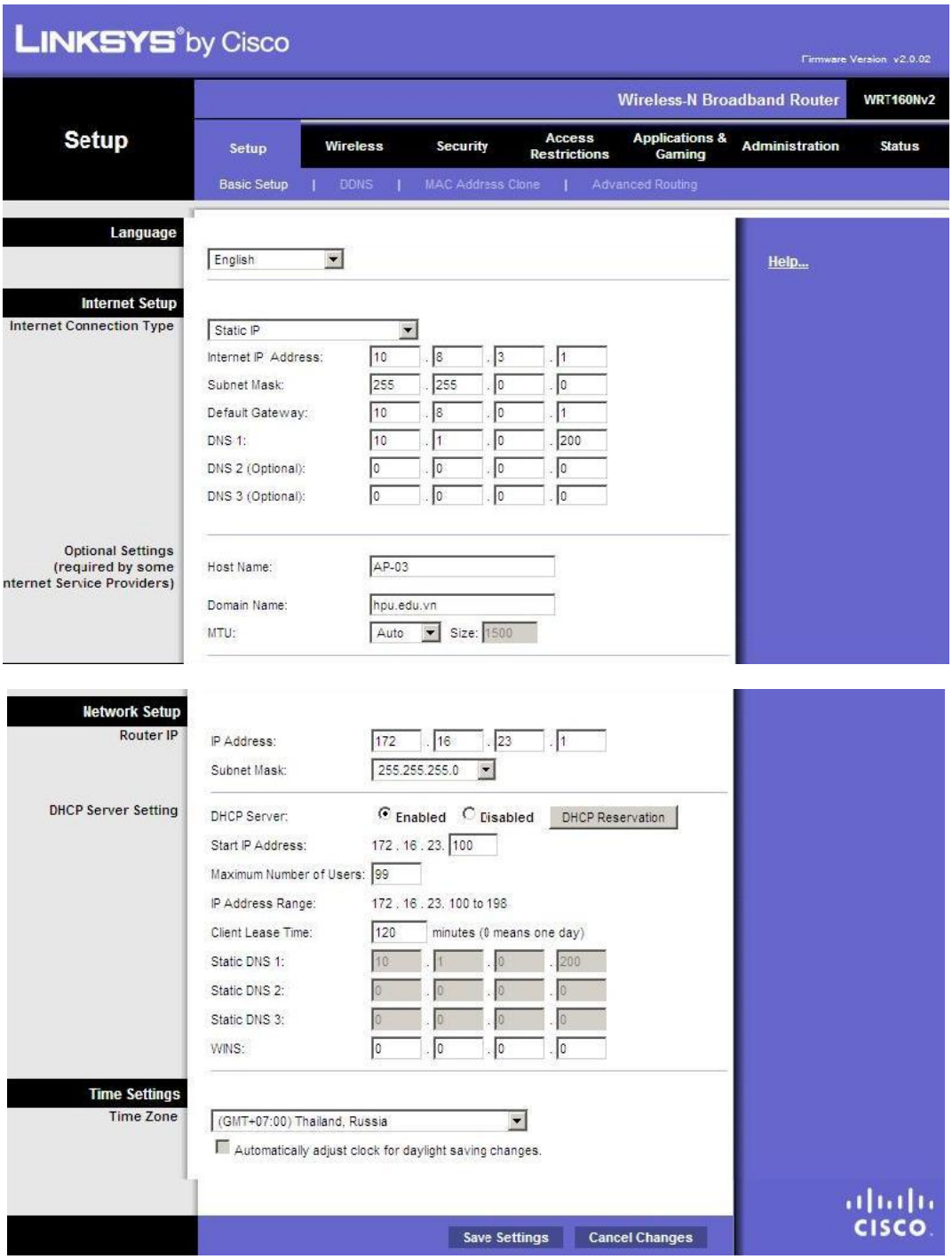
Thiết lập các thông số kĩ thuật:

#### 7.1.3.1. Phần Setup

❖ **Basic setup** :

Gồm các thiết lập Internet setup(Ở đây router hỗ trợ 6 kiểu kết nối

Internet phổ biến là Automatic Configuration - DHCP, Static IP, PPPoE, PPTP, Telstra Cable và L2TP, tùy thuộc nhà cung cấp dịch vụ Internet hoặc sơ đồ đấu nối mà chọn và cung cấp các thông tin cho phù hợp; Network setup( kich hoạt cấu hình DHCP và cung cấp địa chỉ IP động).

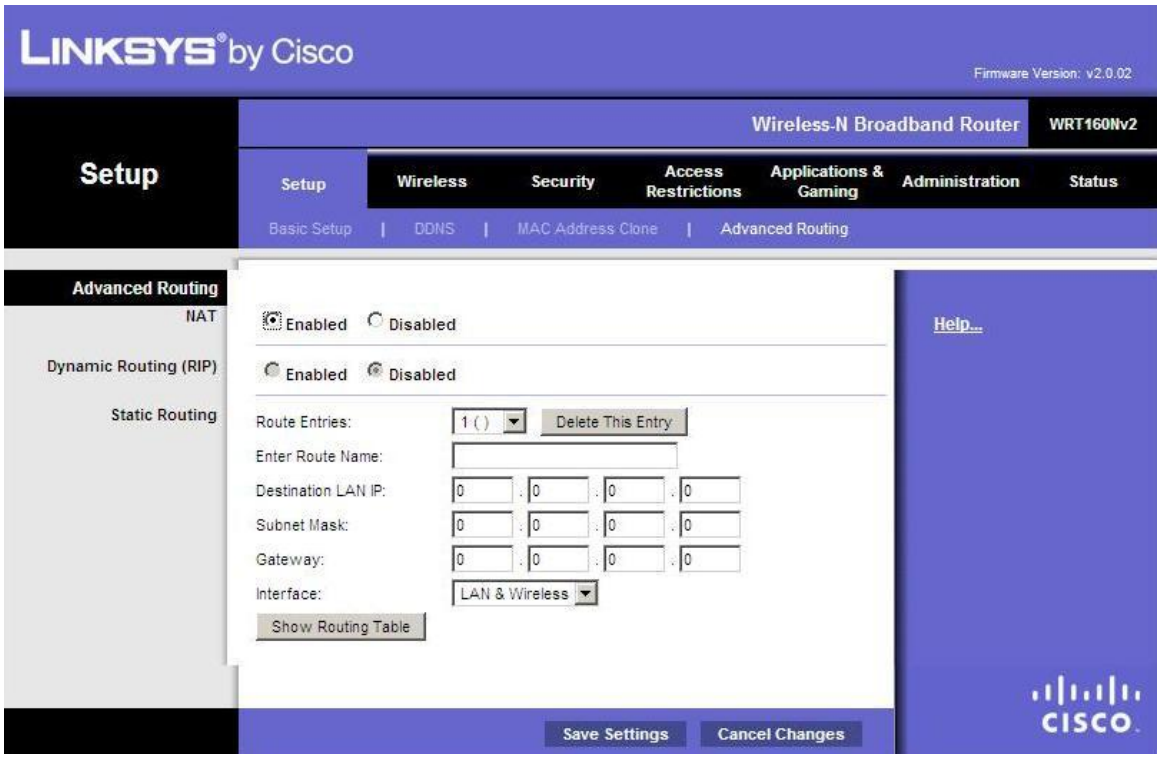



**Hình 7.3 : Thiết lập Baisic setup**

❖ **Mac Address clone**


**Hình 7.4 : Thiết lập Mac Adress clone**

❖ **Advanced Routing**




**Hình 7.5 : Thiết lập Advance Routing**

### 7.1.3.2. Phần Wireless

- **Basic Wireless setting** : Thiết lập SSID ứng với hệ thống mạng không dây bên khu Giảng đường là HPU còn khu Khác sạn sinh viên là KSSV ở chế độ quảng bá.


**Hình 7.6 Thiết lập Basic Wireless Settings**

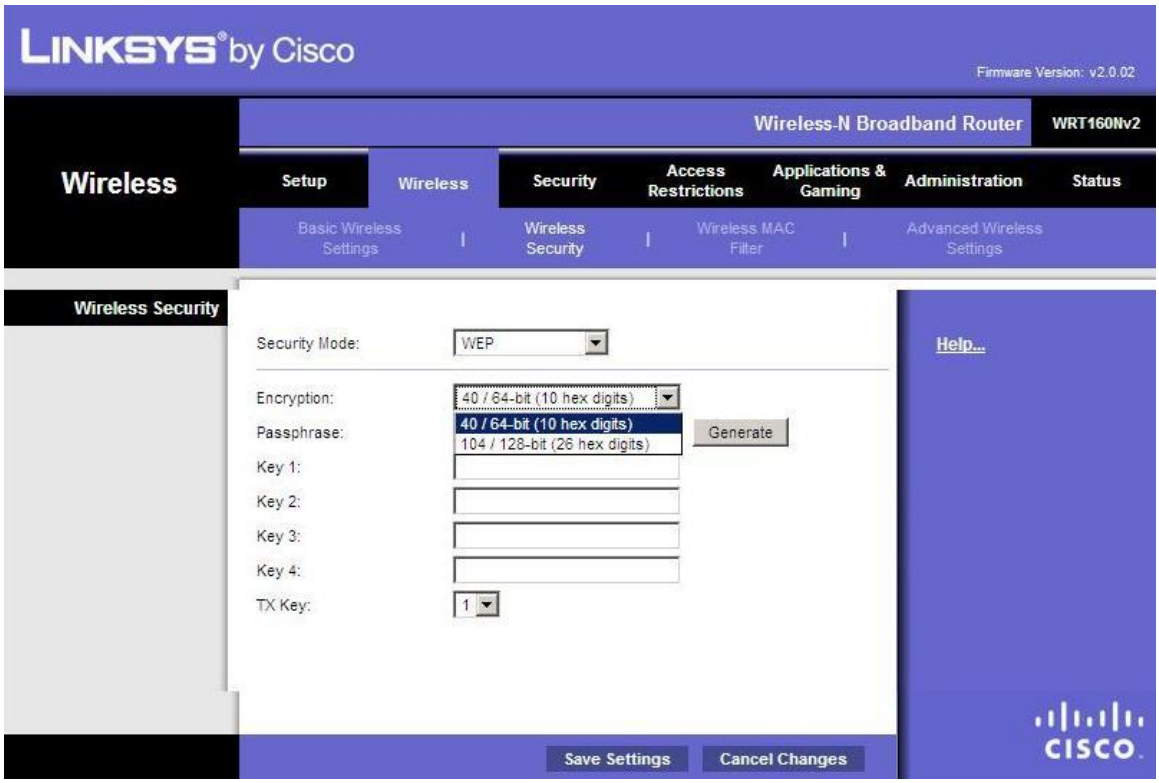
- **Wireless Security**


**Hình 7.7 : Thiết lập Wireless security**

Tại thiết lập Wireless Security ta có thiết lập với nhiều tùy chọn bảo mật hệ thống như WEP;WPA Personal; WPA2 Personal; WPA Enterprise; WPA2 Enterprise và RADIUS.

❖ **WEP(Wired Equivalent Privacy) :**

WEP sử dụng một khoá mã hoá không thay đổi có độ dài 64 bit hoặc 128 bit, (nhưng trừ đi 24 bit sử dụng cho vector khởi tạo khoá mã hoá, nên độ dài khoá chỉ còn 40 bit hoặc 104 bit) được sử dụng để xác thực các thiết bị được phép truy cập vào trong mạng, và cũng được sử dụng để mã hoá truyền dữ liệu.Với những mạng WLAN quy mô lớn có thể sử dụng WEP như một phương pháp bảo mật căn bản nhưng nhưng các nhà quản trị mạng nên nắm bắt được những điểm yếu của WEP và cách khắc phục chúng nhưng các nhà quản trị mạng nên nắm bắt được những điểm yếu của WEP và cách khắc phục chúng.

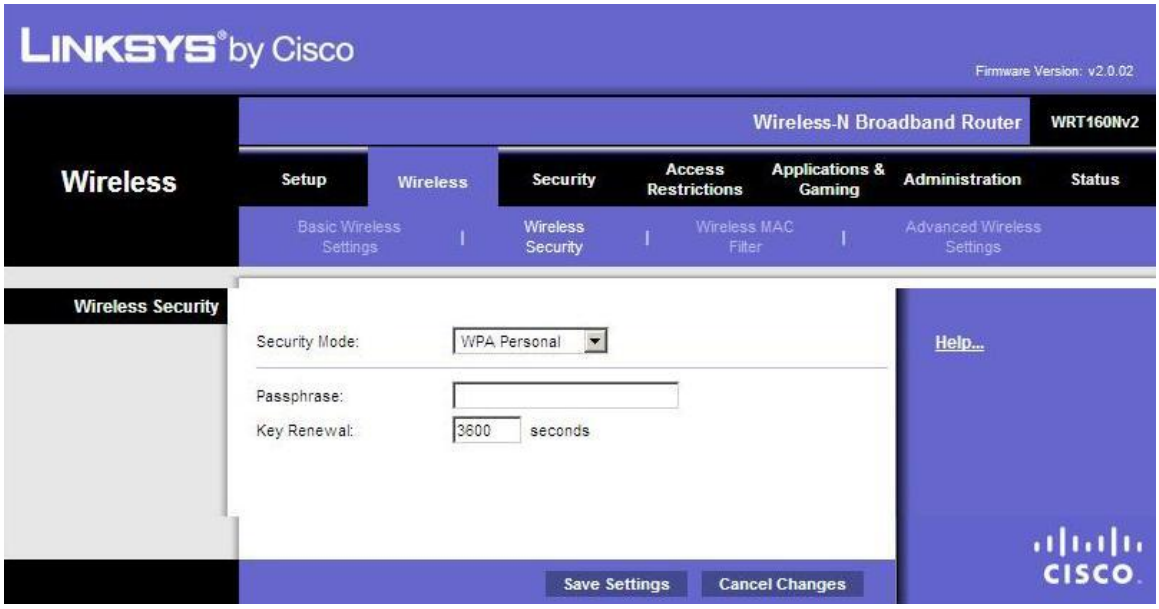



**Hình 7.8 : Thiết lập WEP Security**

❖ **WPA (Wi-Fi Protected Access)**

WPA cũng sử dụng thuật toán RC4 như WEP, nhưng mã hoá đầy đủ 128 bit, một đặc điểm khác là WPA thay đổi khoá cho mỗi gói tin. Các công cụ thu thập các gói tin để phá khoá mã hoá đều không thể thực hiện được với WPA, bởi WPA thay đổi khoá liên tục nên hacker không bao giờ thu thập đủ dữ liệu mẫu để tìm ra mật khẩu. WPA sử dụng hàm thay đổi khoá TKIP (Temporal Key Integrity Protocol) và không yêu cầu nâng cấp phần cứng.WPA có sẵn 2 lựa chọn: WPA Personal và WPA Enterprise.

WPA Personal thích hợp cho gia đình và mạng văn phòng nhỏ,khoá khởi tạo sẽ được sử dụng tại các điểm truy cập và thiết bị máy trạm:



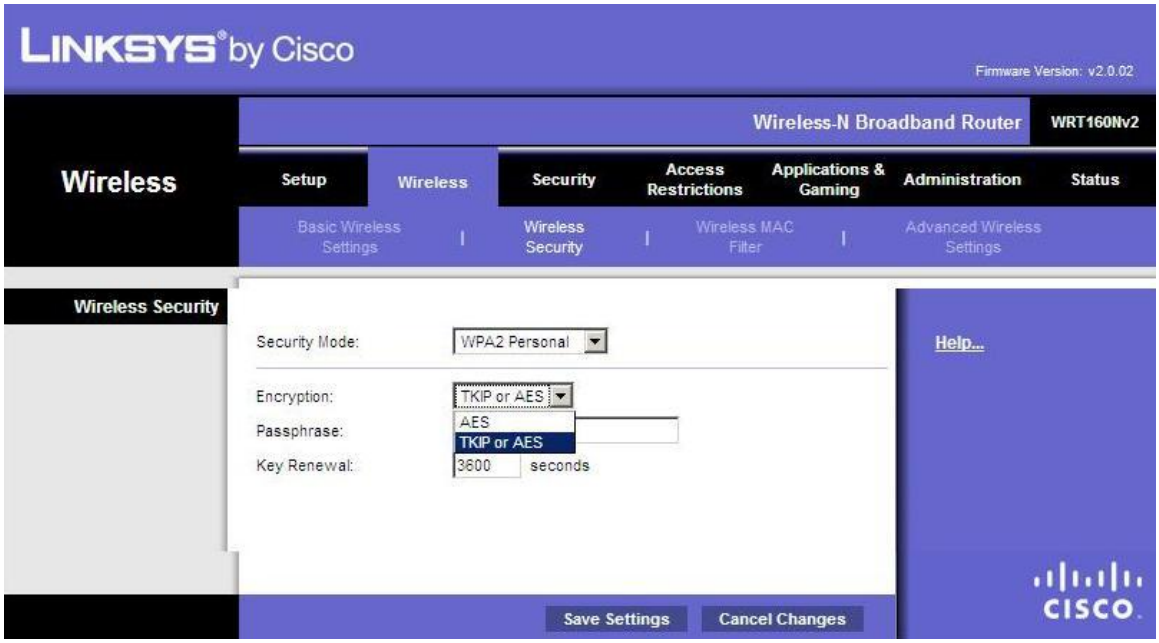

**Hình 7.9 : Thiết lập WPA Personal Security**

WPA Enterprise là thiết lập cho doanh nghiệp cần một máy chủ xác thực và 802.1x để cung cấp các khoá khởi tạo cho mỗi phiên làm việc. Kĩ thuật TKIP của WPA chỉ là giải pháp tạm thời , chưa cung cấp một phương thức bảo mật cao nhất. WPA chỉ thích hợp với những công ty mà không không truyền dữ liệu "mật" về những thương mại, hay các thông tin nhạy cảm…


**Hình 7.10 : Thiết lập WPA Enterprise Security**

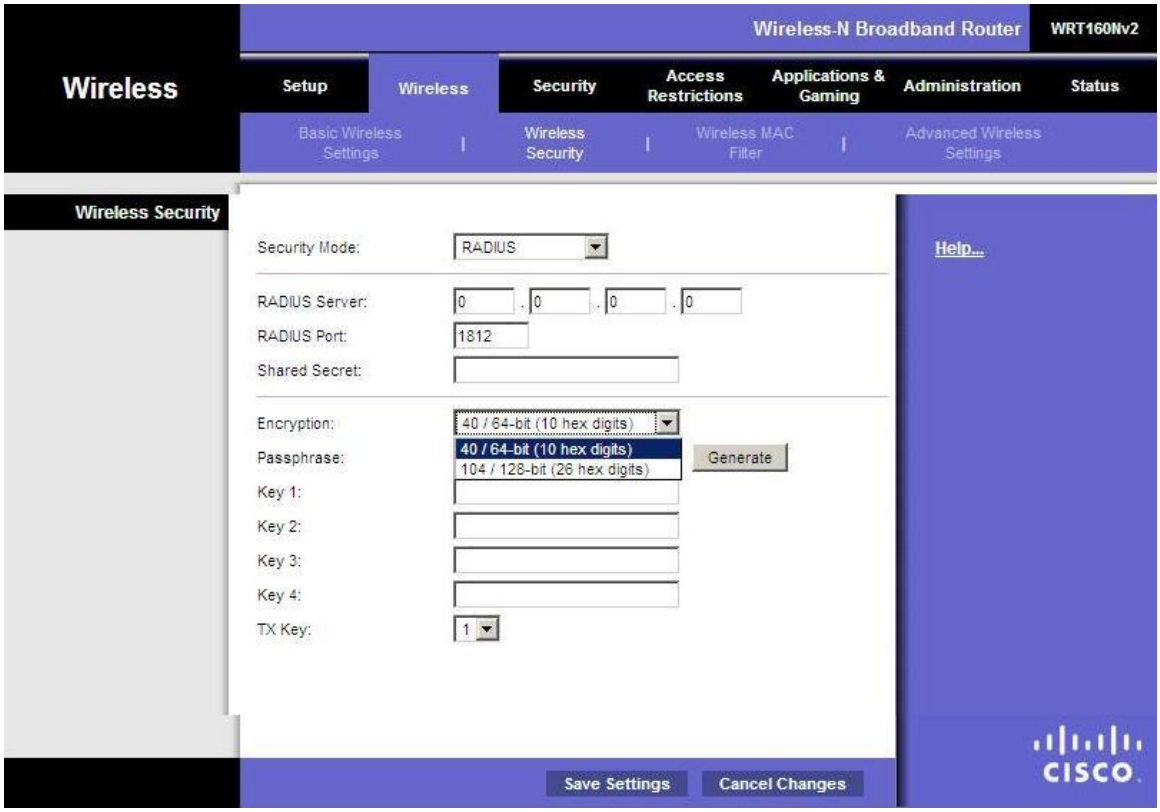
❖ **WPA2** :

Một giải pháp về lâu dài là sử dụng 802.11i, được chứng nhận bởi Wi-Fi Alliance. Chuẩn này sử dụng thuật toán mã hoá mạnh mẽ và được gọi là Chuẩn mã hoá nâng cao AES (Advanced Encryption Standard). AES sử dụng thuật toán mã hoá đối xứng theo khối Rijndael, sử dụng khối mã hoá 128 bit, và 192 bit hoặc 256 bit. AES được xem như là bảo mật tốt hơn rất nhiều so với WEP 128 bit hoặc 168 bit DES (Digital Encryption Standard). Để đảm bảo về mặt hiệu năng, quá trình mã hoá cần được thực hiện trong các thiết bị phần cứng như tích hợp vào chip do đó gặp nhiều vấn đề về không tương thích của thiết bị.Tương ứng với WPA thì WPA2 cũng có 2 lựa chọn là WPA2 Personal và WPA2 Enterprise cho người dùng và doanh nghiệp.




**Hình 7.11 : Thiết lập WPA2 Security**

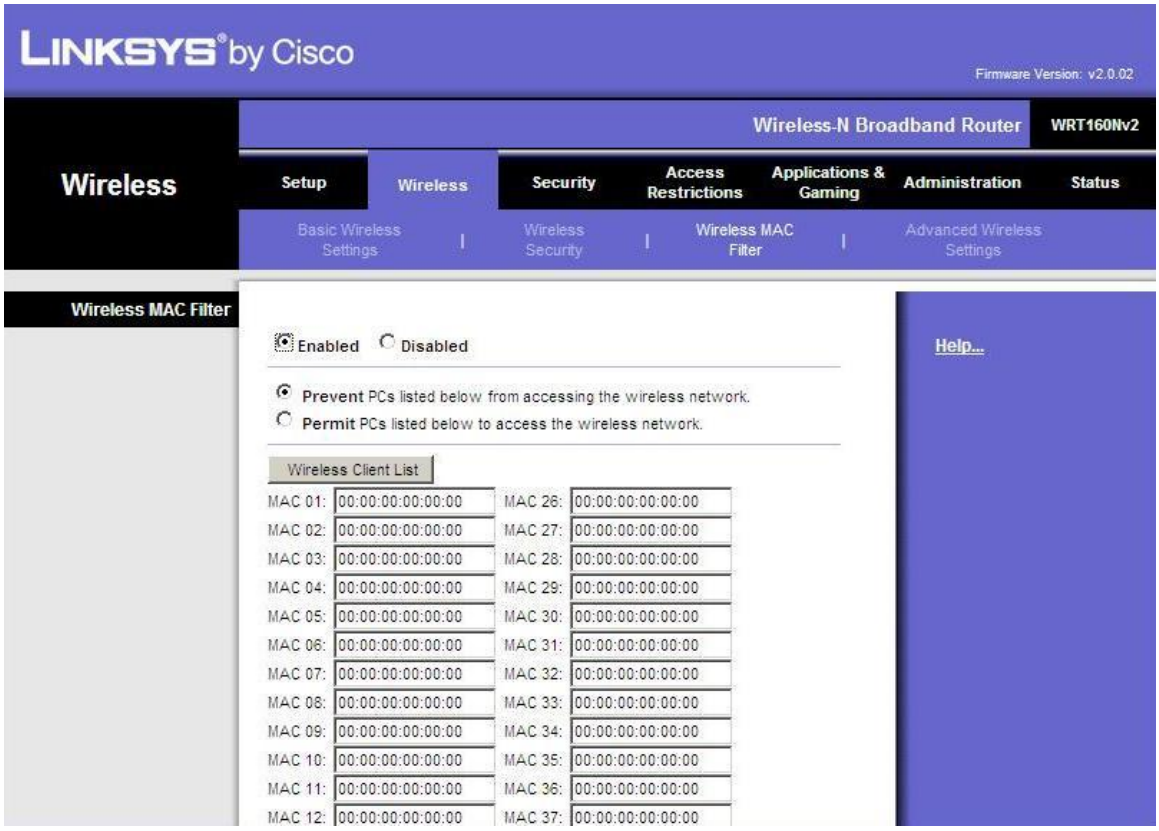
- **RADIUS**




**Hình 7.12 : Thiết lập Radius Security**

RADIUS là chuẩn không chính thức trong hệ thống chứng thực người sử dụng. 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.

❖ **Wireless MAC filter (Lọc MAC)**




**Hình 7.13 : Thiết lập Wireless MAC Filter**

Thiết bị hỗ trợ thiết lập tối đa là 50 địa chỉ MAC với 2 tùy chọn là "Prevent PCs listed below from accessing the Wireless network" và " Permit PCs listed below to access the Wireless network".

Với tùy chọn "Prevent PCs listed below from accessing the Wireless network" thì hệ thống sẽ tiến hành kiểm tra địa chỉ MAC của những thiết bị bất hợp pháp và đua chúng vào danh sách (Wireless Cilent Lít) với tối đa 50 địa chỉ MAC khác nhau. Những thiết bị có địa chỉ MAC nằm ngoài danh sách này có thể truy cập vào mạng 1 cách bình thường, điều này sẽ cũng có nghĩa là không giới hạn những người dùng hợp pháp. Trong khi đó, với tùy

chọn "Permit PCs listed below to access the Wireless network" thì hệ thống sẽ chỉ cho phép tối đa 50 thiết bị hợp pháp truy cập vào mạng còn ngoài ra những thiết bị khác sẽ bị coi là bất hợp pháp. Việc này giúp giới hạn người dùng,thiết bị thì hỗ trợ tối đa là 50 thiết bị hợp pháp tuy nhiên hệ thống sẽ hoạt động tốt nhất với nhỏ hơn hoặc bằng 30 thiết bị.

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 còn việc lập trình các địa chỉ MAC của các Client trong mạng WLAN vào các AP trên một mạng rộng thì không thực tế.

### 7.1.3.3. Thiết lập Security Firewall của thiết bị


**Hình 7.14 : Thiết lập Firewall**

Với thiết lập SPI Firewall Protection ở chế độ Enabled và tick vào các tùy chọn( Filter Anonymous Internet Requests; Filter Muticast; Filter Internet NAT Redirection; Filter IDEN (Port13)) ở phần Internet Filter thì sẽ giúp bảo mật các thông tin của những người dùng tránh không cho người

dùng không mong muốn có thể nhìn thấy các dữ liệu mà người dùng khác đã hoặc đang chia sẻ. Tuy nhiên với thiết lập này sẽ khiến cho hiệu năng của thiết bị cũng như hiệu suất của vùng hệ thống mạng tại thiết bị đó giảm đi khoảng 30 % và  gây khó khăn cho quản trị viên trong việc thực hiện công việc theo dõi giám sát hoạt động của thiết bị từ phòng mạng máy tính(nơi đặt hệ thống máy chủ).

# Chương 8

# VẤN ĐỀ BẢO MẬT HỆ THỐNG MẠNG KHÔNG DÂY TẠI TRƯỜNG ĐẠI HỌC DÂN LẬP HẢI PHÒNG

Khi đã thiết lập hệ thống mạng thì điều quan tâm thứ nhì sau việc cài đặt hoạt động chính là vấn đề đau đầu làm sao để để bảo mật được hệ thống trước những nguy cơ bị tấn công dẫn tới việc truy cập trái phép, mất thông tin quan trọng, hệ thống bị thay đổi, mất quyền điều khiển gây ra nhiều thiệt hại.

Hiện tại hệ thống mạng không dây tại trường Đại Học Dân Lập Hải Phòng chưa thiết lập và triển khai hoạt động bảo mật, các phương án bảo mật vẫn đang được nghiên cứu nhằm đưa ra biện pháp bảo mật an toàn, hiệu quả và phù hợp nhất.

Việc bảo mật hệ thống là rất cần thiết, khi đã xác định được vấn đề bảo mật thì phải tiến hành nghiên cứu tìm hiểu để đưa ra một giải pháp bảo mật phù hợp nhất. Trong phạm vi đề tài này em xin đề cập đến hai giải pháp bảo mật cho hệ thống mạng không dây, mỗi phương án đều có những ưu nhược điểm riêng.

Một điều cần ghi nhớ là chúng ta cần phải đối diện với 2 vấn đề: xác thực và bảo mật thông tin. Xác thực nhằm đảm bảo chắc chắn người sử dụng hợp pháp có thể truy cập vào mạng. Bảo mật giữ cho truyền dữ liệu an toàn và không bị lấy trộm trên đường truyền.

## 8.1.VỀ MẶT THIẾT BỊ HỖ TRỢ

Hệ thống mạng không dây tại trường Đại học Dân Lập Hải Phòng được xây dựng sử dụng hầu hết là các thiết bị Wireless Router Linksys của cisco do đó đều hỗ trợ hầu hết các giải pháp bảo mật từ cơ sở tới nâng cao.

Các tín hiệu không dây được bảo vệ nhờ kỹ thuật mã hoá bảo mật không dây và bảo vệ mạng tránh được các tấn công từ ngoài Internet dựa vào tính năng tường lửa SPI tốt hơn hẳn so với NAT .Wi-fi Protected Setup là chuẩn an ninh dành cho laptop của một router Wi-Fi,Để kết nối qua hệ thống WPS, người dùng phải có mật khẩu. Để bảo vệ tính riêng tư của dữ liệu, WRT110 hỗ trợ các công nghệ mã hoá bảo mật như WEP và WPA,WPA2 có khả năng mã hoá tất cả các đường truyền không dây nhờ sức mạnh của kỹ thuật mã hoá 256-bits. Công nghệ lọc các kết nối Wi-Fi bằng địa chỉ MAC, cũng giúp bạn có thể cho phép các đối tượng nào có thể truy nhập vào mạng không dây của mình hay không.Bên cạnh đó thiết bị cũng giúp nâng cao tính bảo mật với phương pháp chứng thực 802.1x bằng máy chủ RADIUS.

## 8.2.CÁC GIẢI PHÁP CÓ THỂ TRIỂN KHAI

Hệ thống mạng không dây tại trường Đại học Dân Lập Hải Phòng là 1 hệ thống qui mô lớn do đó các giải pháp bảo mật cơ sở được hỗ trợ bởi các thiết bị là không đủ đáp ứng các yêu cầu về bảo mật.

Trong khi WEP là giải pháp bảo mật quá tồi khi đưa cả xác thực người dùng và đảm bảo an toàn dữ liệu vào cùng một phương thức không an toàn, khoá mã hoáWEP có thể dễ dàng bị bẻ gãy thì VPN Fix chỉ là giải pháp tình thế chứ không phải là sự kết hợp với WLAN,giải pháp này cần lưu lượng VPN lớn hơn cho tường lửa và cần phải tạo các thủ tục khởi tạo cho từng người sử dụng. Các phương pháp kiểm soát truy cập như ẩn SSID, không cung cấp DHCP đều có thể vượt qua được dễ dàng, MAC filtering thì

không hiệu quả vì MAC có thể dễ dàng bị thay đổi, số lượng MAC có thể thiết lập nhỏ đối với thiết bị.

Với 1 hệ thống mạng không dây có qui mô lớn như hệ thống mạng không dây tại trường Đại học Dân Lập Hải Phòng về cơ bản là có 2 giải pháp bảo mật là phương pháp bảo mật bằng mã hoá WPA và phương pháp xác thực bằng RADIUS Sever.

### 8.2.1 Phương pháp bảo mật bằng mã hoá WPA

WPA **(**Wi-Fi Protected Access**)** và nâng cao hơn là WPA2 đều có sẵn 2 lựa chọn: WPA Personal và WPA Enterprise. Cả 2 lựa chọn này đều sử dụng giao thức TKIP, và sự khác biệt chỉ là khoá khởi tạo mã hoá lúc đầu. WPA Personal thích hợp cho gia đình và mạng văn phòng nhỏ, khoá khởi tạo sẽ được sử dụng tại các điểm truy cập và thiết bị máy trạm. Trong khi đó, WPA cho doanh nghiệp cần một máy chủ xác thực và 802.1x để cung cấp các khoá khởi tạo cho mỗi phiên làm việc.

❖ **Ưu điểm :**

- WPA mã khóa dài hơn,đầy đủ 128 bits so với 64 bit của WEP còn WPA2 sử dụng phương pháp mã hóa mạnh hơn AES(Advanced Encryption Standard) với độ dài khóa 256 bits.

- Sử dụng hàm thay đổi khoá TKIP (Temporal Key Integrity Protocol) giúp thay đổi khoá cho mỗi gói tin giúp chống lại việc dò tìm khoá do đó nâng cao độ bảo mật.

- WPA không yêu cầu nâng cấp phần cứng.

❖ **Nhược điểm :**

- Khoá WPA cũng có thể bẻ được

- Quản lí khoá khó khăn do yếu tố con người, khó khăn trong việc giữ bí mật khoá này do những người sử dụng có thể nói cho nhau hoặc bị lộ do vô tình ghi khóa ra đâu đó.

- quá trình mã hoá AES cần được thực hiện trong các thiết bị phần cứng như tích hợp vào chip do đó gây khó khăn về mặt tương thích thiết bị.

- Không có khả năng cung cấp cho mỗi người sử dụng một mật khẩu riêng.

WPA là 1 giải pháp tốt tuy nhiên nếu triển khai cho hệ thống mạng không dây tại trường Đại học Dân Lập Hải Phòng sẽ phải lựa chọn giải pháp phân chia cho 1 nhóm người 1 user dùng chung thay vì mỗi người 1 user do số lượng user quá lớn, bộc lộ những khó khăn do yếu tốt con người.

Hệ thống mạng không dây tại Trường Đại học Dân Lập Hải Phòng được xây dựng với mục đích hướng tới đối tượng người dùng là sinh viên là chủ yếu do lượng sinh viên chiếm số đông còn lượng cán bộ nhân viên chỉ chiếm 1 phần nhỏ.Người dùng sinh viên là đối tượng người dùng không cố định trong mạng không dây,có thể bất ngờ tiến hành kết nối xác thực với số lượng rất lớn vào 1 thời điểm bất kì. Đối với người dùng cố định số lượng người dùng kết nối xác thực tới hệ thống luôn không thay đổi thì WPA tỏ ra là 1 phương pháp bảo mật tốt, có thể triển khai với nhiều ưu điểm.Tuy nhiên với hệ thống mạng không dây tại trường Đại học Dân Lập Hải Phòng thì WPA trở thành không khả thi.

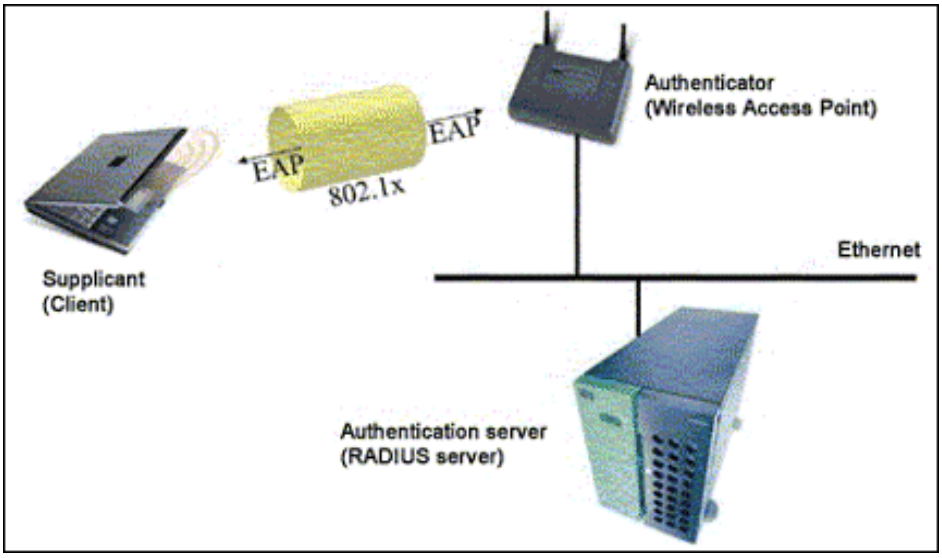
### 8.2.2 Phương pháp bảo mật sử dụng RADIUS Sever cho quá trình xác thực

Với khả năng hỗ trợ xác thực cho cả chuẩn không dây 802.1X, RADIUS(Remote Authentication Dial−in User Service) hay là AAA sever bao gồm việc xác thực(Authentication), cấp quyền (Authorization) và tính cước (Accounting) là giải pháp không thể thiếu cho các hệ thống mạng lớn muốn quản lý tập trung và tăng cường tính bảo mật cho hệ thống.

Với cơ sở tập trung - Giải pháp sử dụng RADIUS cho mạng WLAN là rất quan trọng bởi nếu một hệ thống mạng có rất nhiều Access Point việc cấu hình để bảo mật hệ thống này là rất khó nếu quản lý riêng biệt, người

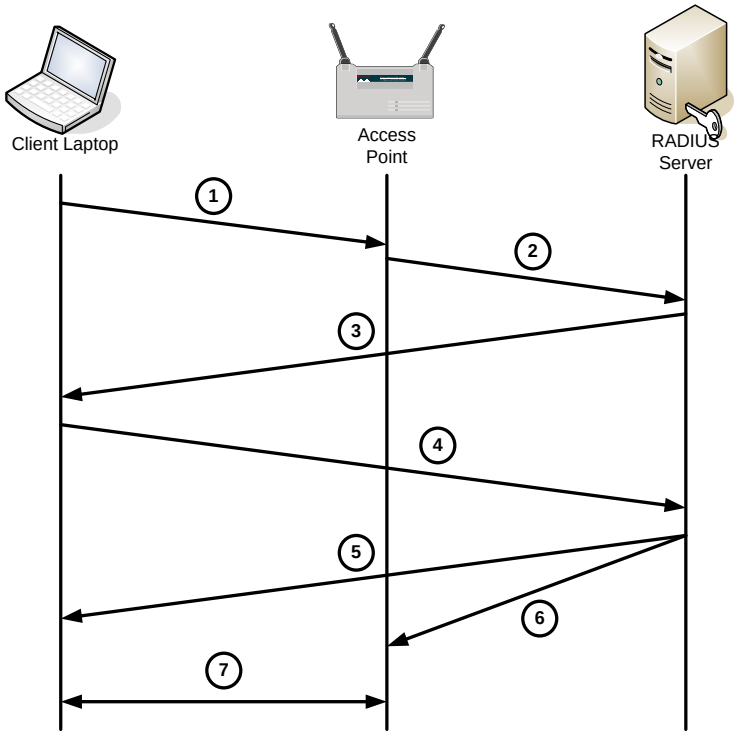
dùng có thể xác thực từ nhiều Access Point khác nhau và điều đó là không bảo mật.Khi sử dụng RADIUS cho WLAN mang lại khả năng tiện lợi rất cao, xác thực cho toàn bộ hệ thống nhiều Access Point,cung cấp các giải pháp thông minh hơn.

Việc chứng thực của 802.1x được thực hiện trên một server riêng, server này sẽ quản lý các thông tin để xác thực người sử dụng như tên đăng nhập (username), mật khẩu (password), mã số thẻ, dấu vân tay, v.v… Khi người dùng gửi yêu cầu chứng thực, server này sẽ tra cứu dữ liệu để xem người dùng này có hợp lệ không, được cấp quyền truy cập đến mức nào.




**Hình 8.1: Cơ chế xác thực của Radius sever**

Quá trình các bước xác thực của Radius sever :




**Hình 8.2 : quá trình liên kết xác thực người dùng bởi radius sever**

1. Máy tính Client gửi yêu cầu kết nối đến AP.

2. AP thu thập các yêu cầu của Client và gửi đến RADIUS server.

3. RADIUS server gửi đến Client yêu cầu nhập user/password.

4. Client gửi user/password đến RADIUS Server.

5. RADIUS server kiểm tra user/password có đúng không, nếu đúng thì RADIUS server sẽ gửi cho Client mã khóa chung.

6. Đồng thời RADIUS server cũng gửi cho AP mã khóa này và đồng thời thông báo với AP về quyền và phạm vi được phép truy cập của Client này.

7. Client và AP thực hiện trao đổi thông tin với nhau theo mã khóa được cấp.

Để nâng cao tính bảo mật, RADIUS Server sẽ tạo ra các khóa dùng chung khác nhau cho các máy khác nhau trong các phiên làm việc (session) khác nhau, thậm chí là còn có cơ chế thay đổi mã khóa đó thường xuyên

theo định kỳ. Khái niệm khóa dùng chung lúc này không phải để chỉ việc dùng chung của các máy tính Client mà để chỉ việc dùng chung giữa Client và AP.

Với một hệ thống mạng không dây qui mô lớn sử dụng sử dụng chuẩn 802.1X thì lựa chọn việc triển khai RADIUS là hợp lý.

### 8.2.3 Phương thức triển khai RADIUS sever

Có 2 phương thức chính để triển khai hệ thống RADIUS sever cho hệ thống mạng không dây :

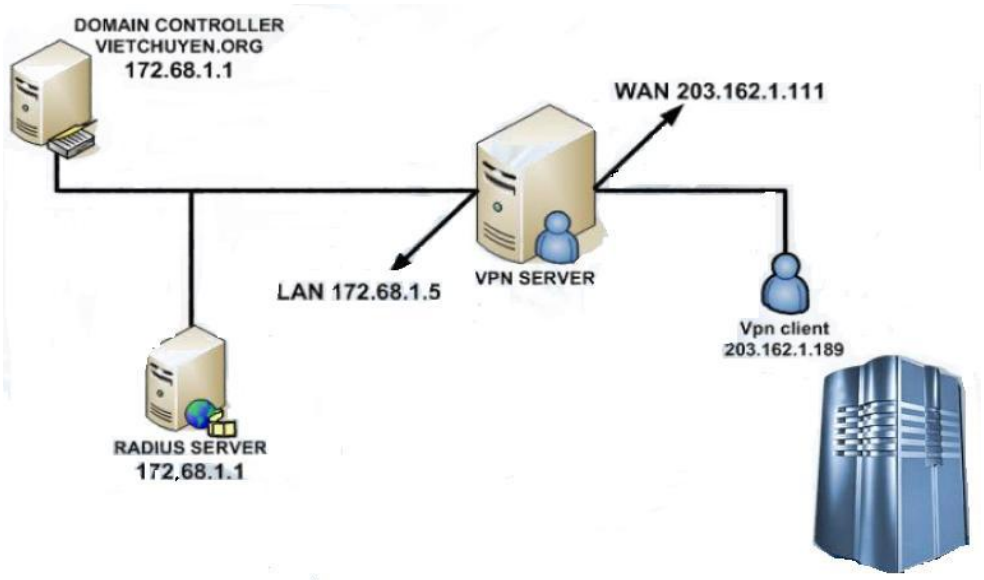
#### 8.2.3.1. Thiết lập RADIUS Sever trên máy chủ chạy hệ điều hành sử dụng phần mềm bản quyền Windows Sever 2000/20003 của Microsoft

Phương thức thứ nhất được đề cập tới là sử dụng Microsoft's RADIUS sever(use Microfoft's RADIUS Sever): thiết lập trên 1 máy chủ chạy hệ điều hành Microsoft Windows Server 2000/2003 với việc sử dụng Microsoft's Internet Authentication Service (IAS). Có rất nhiều tài liệu nói về việc triển khai IAS ví dụ như tài liệu về "802.1X Port Authentication with Microsoft Active Directory" có thể tham khảo tại :

http://www.foundrynet.com/pdf/wp-8021x-authentication-active-directory.pdf.

IAS cần thiết các nhà quản trị hay các user phải làm việc trên môi trường Windows. Và nó cũng là một trong những tính năng cao cấp của Microsoft Wireless Provisioning Service.

Mô hình xây dựng :




**Hình 8.3 : Mô hình RADIUS Sever**

Để thiết lập hệ thống RADIUS Sever cần tối thiểu là 1 sever cho RADIUS và cần 1 Sever cho AD hay có thể gọi là DC(Domain Controller).

Khi 1 máy trạm kết nối vào Wireless Router để truyền thông được với những máy tính khác thì khi đó hệ thống sẽ yêu cầu RADIUS Sever chứng thực thông tin về người dùng đăng nhập.Nếu người dùng đăng nhập hợp lệ thì hệ thống sẽ cho phép kết nối vào.

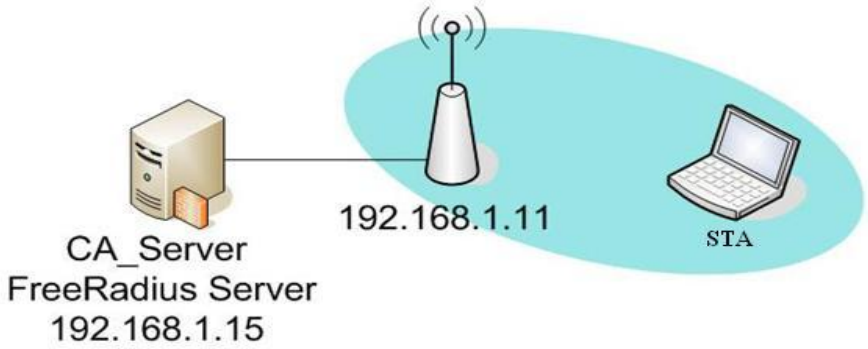
Các bước cần thực hiện :

- Bước 1 : Cài đặt Windows Sever 2003 và nâng cấp lên thành AD(là một hệ thống quản lý phân quyền các user theo domain một cách tập trung và thống nhất)
- Bước 2 : Cài đặt CA(Certification Authority)
- Bước 3 : Cài đặt cấu hình IAS Sever
- Bước 4 : Tạo các tài khoản người dùng.
- Bước 5 : Cấu hình AccessPoint sử dụng RADIUS Sever.
- Bước 6 : Cấu hình tại máy trạm.
- Bước 7 : Tiến hành kiểm tra.

### 8.2.3.2. Thiết lập RADIUS Sever trên máy chủ chạy hệ điều hành sử dụng phần mềm mã nguồn mở

Một phương thức khác để thiết lập RADIUS Sever cho hệ thống mạng không dây của ta là sử dụng sử dụng giải pháp phần mềm mã nguồn mở nếu không có một phiên bản Windows(Install an Open Source RADIUS Server**).**Có thể tham khảo tại: http://www.freeradius.org với khả năng hỗ trợ cho chuẩn 802.1X các máy chủ chạy hệ điều hành mã nguồn mở như Linux, Free or OpenBSD, OSF/Unix, hoặc Solaris đều có thể sử dụng làm RADIUS Server**.**

Mô hình xây dựng :




**Hình 8.4 : Mô hình xây dựng FreeRadius**

Để thiết lập hệ thống RADIUS Sever chỉ cần 1 sever FreeRadius Sever duy nhất. Để thiết lập hệ thống RADIUS Sever cũng cần tiến hành các bước như sau :

- Bước 1 : Cài đặt các phần mềm (Software installation).
- Bước 2 : Khởi tạo 1 CA Sever(Create CA).
- Bước 3 : Tiến hành chạy RADIUS Sever (Running Radius Server).
- Bước 4 : Cấu hình AccessPoint sử dụng RADIUS Sever(Access point setup).
- Bước 5 : Cấu hình tại máy trạm (CA sever).
- Bước 6 : Chứng thực truy nhập cho người dùng(khách)(import Certificate to client).
- Bước 7 :Cấu hình CBs(CBs configuration).

- Bước 8 : Kiểm tra kết quả (Result).

#### 8.2.3.3. Tương quan so sánh giữa 2 phương thức thiết lập RADIUS Sever

Với việc sử dụng phương thức thiết lập RADIUS Sever bằng Use Microsoft's RADIUS Server sẽ giúp cho việc cài đặt, thiết lập hệ thống dễ dàng hơn với nền giao thức đồ hoạ và nguồn tài liệu phong phú trong khi đó phương thức thiết lập sử dụng giải pháp phần mềm mã nguồn mở sẽ dẫn tới nhiều khó khăn cho nhà quản trị mạng khi ngồn tài liệu ít ỏi và phải thực hiện chủ yếu trên nền giao thức câu lệnh.

Tuy nhiên việc sử dụng phương thức Use Microsoft's RADIUS Server sẽ phải tiêu tốn 1 khoản kinh phí để mua bản quền các phần mềm của Microsoft còn phương thức sử dụng mã nguồn mở thì lại hoàn toàn miễn phí. Nhưng với việc sử dụng các phần mềm bản quyền sẽ đem lại sự yên tâm hơn, dễ dàng nắm bắt, phòng tránh và khắc phục được các rủi ro bởi những lỗi hệ thống phát sinh.

Với khuyến cáo trong việc triển khai thiết lập RADIUS sever bằng phương thức sử dụng Windows Sever của Microsoft sẽ đáp ứng được từ 400 tới 500 người dùng thì nên thiết lập 1 RADIUS Sever do đó với số lượng 8000 sinh viên và cán bộ nhân viên trong trường ước tính cần lắp đặt khoảng 10 RADIUS Sever. Còn với việc sử dụng mã nguồn mở thì không có khuyến cáo về số lượng người dùng trên 1 Sever RADIUS, trong khi thực nghiệm có thể cho tới 1000 người tiến hành xá thực trên 1 RADIUS Sever thì với việc thiết lập theo mã nguồn mở,số lượng sẽ chỉ là 5 RADIUS Sever.

#### 8.2.3.4. Giải pháp khác và phương án đề xuất

Ngoài 2 phương thức thiết lập RADIUS Sever kể trên trong trường hợp phải sử dụng một giải pháp chuyên nghiệp cần hỗ trợ đầy đủ toàn bộ các tính năng cũng như khả năng an toàn, và độ ổn định ta có thể mua một

Commercial RADIUS Server các nhà sản xuất khác, với tính năng hỗ trợ 802.1X và là một RADIUS Server chuyên nghiệp như :

Aradial WiFi : http://www.aradial.com

Bridgewater Wi-Fi AAA : http://www.bridgewatersystems.com

Cisco Secure Access Control Server : http://www.cisco.com

Funk Odyssey : http://www.funk.com/

Hoặc 1 số nhà cung cấp khác, Commercial RADIUS Servers có giá cả tuỳ vào khả năng của sản phẩm. RADIUS server cũng có thể bao gồm cả giá của phần cứng/phần mềm phụ thuộc nhiều vào nhà cung cấp phần mềm hay các đại lý của các hãng khác nhau.

Phương thức thiết lập RADIUS sever sử dụng phần mềm mã nguồn mở sẽ tiêu tốn chi phí ít hơn so với phương thức thiết lập sử dụng phần mềm bản quyền của Microsoft do phần mềm sử dụng là miễn phí không phải tốn chi phí đê mua.Thêm vào đó chi phí cũng giảm do phần mềm mã nguồn mở không có khuyến cáo về số lượng người dùng xác thực trên 1 Radius sever nên tiêu tốn ít máy chủ RADIUS sever hơn.Phương thức sử dụng phần mềm mã nguồn mở  là phương án thích hợp trong điều kiện kinh phí eo hẹp hoặc muốn tiết kiệm chi phí.tuy nhiên sử dụng phần mềm mã nguồn mở thì sẽ gặp khó khăn trong quá trình thiết lập và việc xử lí lỗi hệ thống.

Bởi vậy với hệ thống trang thiết bị sẵn có đáp ứng được các yêu cầu về mặt kĩ thuật em xin đề xuất xử dụng phương án xây dựng hệ thống RADIUS Sever bằng phần mềm bản quyền của Microsoft. Như vậy sẽ giúp cho việc thiết bảo mật cho hệ thống mạng không dây tại trường Đại Học Dân Lập Hải Phòng trở nên nhanh chóng và dễ dàng hơn.Điều đó sẽ mang lại 1 giải pháp bảo mật thật sự, đảm bảo lợi ích tối đa của người dùng qua đó sẽ góp phần phát triển hệ thống mạng không dây hoàn thiện hơn tạo ra 1 môi trường học tập thân thiện với sinh viên cũng như môi trường làm việc tốt đối với các cán bộ nhân viên trong trường.

# DANH MỤC CÁC THUẬT NGỮ VIẾT TẮT

| | | |
|---|---|---|
| AAA | Authentication, Authorization, Accountting | Xác thực, cấp quyền,tính cước |
| ACK | Acknowlegment | Bản tin báo nhận |
| ADSL | Asymmetric Digital Subscriber Line | Đường dây thuê bao số bất đối xứng |
| ASK | Amplitude shift keying | Khoá dịch biên độ |
| AP | Access Point | Điểm truy cập |
| BPSK, | Binary phase-shift keying | Khoá dịch pha |
| CTS | Clear To Send | Tín hiệu(báo) sẵn sàng để truyền |
| CCK | Complementary Code Keying | Khoá mã bổ sung. |
| CPE | Customer Premises Equipment | Thiết bị khách |
| CDMA | Code Divison Multiple Access | Đa truy nhập phân chia mã |
| DHCP | Dynamic Host Configuration Protocol | Giao thức cấu hình host động. |
| DSSS | Direct Sequence Spread Spectrum | Trải phổ chuỗi trực tiếp. |
| DES | Data Encryption Standard | Chuẩn mã hoá dữ liệu |
| EAP | Extensible Authentication Protocol | Giao thức chứng thực mở rộng |

| | | |
|---|---|---|
| FSK | Frequency Shift keying | Đánh tín hiệu dịch tần số |
| FDD | Frequency Division Duplexing | Dồn kênh bằng chia tần số |
| FDMA | Frequency-division multiple access | Đa truy cập phân chia tần số |
| FHSS | Frequency Hopping Spread Spectrum | Trải phổ nhảy tần |
| FTP | File Transfer Protocol | Giao thức truyền tập tin |
| FIPS | Federal Information Processing Standards | Chuẩn xử lí dữ liệu liên bang (Mỹ) |
| FCC | Federal Communications Commission | Hộ đồng truyền thông liên bang |
| IP | Internet protocol | Một giao thức được sử dụng để gửi dữ liệu qua một mạng |
| ISP | Internet Service Provider | Nhà cung cấp dịch vụ Internet |
| ICV | initial chaining value | Giá trị liên kết ban đầu |
| IV | Initialization Vector | Vector khởi đầu |
| ISM | Industrial ScientificMedical | Dãy tần số công nghiệp, khoa học và y tế. |
| IEEE | Institute of Electrical and Electronics Engineer | Viện kỹ thuật và điện tử. |
| LAN | Local area network | Mạng cục bộ |
| MAN | Metropolitant Area | Mạng khu vực đô thị |

| | | |
|---|---|---|
| | Network: | |
| MAC | Medium Access Control: | Điều khiển truy cập truyền thông |
| NIST | National Institute of Standards and Technology | viện tiêu chuẩn và công nghệ quốc gia (Hoa kỳ) |
| QoS | quality of service | Chất lượng dịch vụ |
| PCMCIA | Personal Computer Memory Card International Association | Hiệp hội PCMCIA |
| POP3 | Post Office Protocol 3 | Giao thức làm việc 3 |
| QPSK | quaternary phase shift keying | Đánh tín hiệu dịch pha một phần tư |
| PSK | phase shift keying | Kỹ thuật khóa chuyển pha |
| PC | Personal Computer | Máy tính cá nhân |
| PDA | Personal Digital Assistant | Máy trợ giúp cá nhân dùng kỹ thuật số. |
| OFDM | Orthogonal frequency division multiplexing | Hợp kênh phân chia tần số |
| TKIP | Temporal Key Integrity | |
| SMTP | Simple Mail Transfer Protocol | Giao Thức Chuyển Thư Điện Tử Đơn Giản |
| SDSL | Simultaneous digital subscriber line | Đường dây thuê bao số đồng thời |
| RADIUS | Remote Authentication Dial In User Service | Dịch vụ người dùng quay số chứng thực từ xa. |

| | | |
|---|---|---|
| SSID | Subsystem identification | Sự nhận biết hệ thống con |
| TDD | Time Division | Sự phân chia thời gian |
| TDMA | Time Division Multiple Access | Đa truy cập phân chia thời gian |
| VPN | Virtual Private Network | Mạng riêng ảo |
| WDMZ | Wireless DeMilitarized Zone | Dồn kênh phân bước sóng trong mạng cục bộ (LAN) |
| WPA | Wi-Fi Protected Access | Sự bảo vệ mạng không dây |
| WEP | WIRED EQUIVALENT PRIVACY | |
| Wi-Fi | Wireless fidelity | Một cái tên được gọi thay thế cho mạng không dây. |
| WLAN | Wireless local area network | Mạng không dây cục bộ |

# KẾT LUẬN

Ngày nay mạng không dây đã trở nên không còn xa lạ gì trong cuộc sống,tại những thành phố lớn của nước ta có thể dễ dàng nhận biết được các hệ thống mạng không dây tại gia đình, văn phòng,công sở hay tại các địa điểm công cộng như quán café, bệnh viện, trường đại học, các thiết bị cầm tay thì ngày càng hỗ trợ nhiều hơn tính năng truy cập mạng không dây, cập nhập những công nghệ mới nhất.Song song với việc  nghiên cứu phát triển hạ tầng thiết bị mạng không dây thì vấn đề bảo mật cho hệ thống cũng đặc biệt được ưu tiên. Việc nghiên cứu vẫn luôn được quan tâm nhằm tìm kiếm những giải pháp bảo mật tốt hơn, hoàn thiện nữa.

Sau 1 thời gian tìm tòi và nghiên cứu tài kiệu cộng với sự hướng dẫn chỉ bảo tận tình của thầy giáo **ThS Trần Hữu Trung** em đã hoàn thành đồ án.Qua việc thực hiện Đồ Án đã giúp em hiểu thêm được về hệ thống mạng không dây về mạng không dây,từ cái nhìn bao quát những ưu điểm của nó,ứng dụng trong cuộc sống cho tới việc xây dựng 1 hệ thống hoàn chỉnh và tầm quan trọng và cần thiết của vấn đề bảo mật.

Do những hạn chế về mặt kiến thức, tài liệu và khả năng của bản thân nên đồ án không tránh khỏi nhiều thiếu sót,em rất mong được sự đóng góp của các thầy cô và các bạn để hoàn thiện hơn đồ án này.

Em xin chân thành cảm ơn Thầy giáo **ThS Trần Hữu Trung** đã tận tình chỉ bảo giúp em hoàn thành khoá luận này.

# DANH MỤC SÁCH THAM KHẢO

## ❖ Sách tham khảo

[1] **802.11 Wireless Networks**,The Definitive Guide by Matthew Gast,April 2002

[2] **Các bài thực hành trong 5 phút-Nối mạng không dây**,Trần Việt An,NXB Giao Thông Vận Tải,2006

[3] **Căn bản mạng không dây(Wireless),**Ks Trương Hoàng Vĩ-Đức Hùng,NXB Hải Phòng,2007

[4] **Hacking Wireless Kỹ Thuật Thâm Nhập Mạng Không Dây**,Lê Tấn Liên-Minh Quân,NXB Hồng Đức,2009

[5] **Mạng máy tính**, Hồ Đắc Phương,NXB Đại Học Quốc Gia HN,2006

[6**] Mạng căn bản-Networking Essentials**,biên dịch VN-GUIDE, Hiệu đính TH.S Lê Phụng Long,MSCA Nguyễn Tam Trung,2003

[7] **Wireless Lan written by Meetali Goel**,Thien An Nguyen,Edited by Prof Melody Moh,2002

## ❖ Website

[8] Http://www.quantrimang.com

[9] Http://www.wireless.com

[10] Http://www.cisco.com

# LỜI CẢM ƠN

Trước hết em xin chân thành gửi lời cảm ơn và lòng biết ơn sâu sắc tới Thầy giáo **Th.S Trần Hữu Trung** đã trực tiếp hướng dẫn, chỉ bảo tận tình trong suốt quá trình em làm đồ án.

Em xin chân thành cảm ơn các thầy giáo trong Phòng Quản trị mạng Trường Đại Học Dân Lập Hải Phòng đã giúp đỡ, tạo điều kiện cho em được tìm hiểu thiết bị trong thời gian làm đồ án và chỉ bảo tận tình giúp em nắm bắt được hoạt động của chúng.

Em cũng xin chân thành cảm ơn các thầy cô giáo trong Trường Đại Học Dân Lập Hải Phòng đã hết lòng dạy bảo chúng em trong những năm học Đại Học, giúp chúng em có những kiến thức và kinh nghiệm quý báu trong chuyên môn và cuộc sống, giúp chúng em bước những bước đi đầu tiên trong hành trang vào đời.

Cuối cùng, em xin cảm ơn những người thân trong gia đình và bạn bè đã luôn giúp đỡ, động viên để em có thể hoàn thành đồ án này!

Hải Phòng, tháng 7 năm 2009

Sinh viên

Vũ Đức Thắng