NHẬN XÉT CỦA GIẢNG VIÊN HƯỚNG DẪN

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

TP.HCM, Ngày tháng năm 2010

MỤC LỤC

LỜI MỞ ĐẦU

Wireless Lan là một trong những công nghệ truyền thông không dây được áp dụng cho mạng cục bộ. Sự ra đời của nó khắc phục những hạn chế mà mạng nối dây không thể giải quyết được, và là giải pháp cho xu thế phát triển của công nghệ truyền thông hiện đại. Nói như vậy để thấy được những lợi ích to lớn mà Wireless Lan mang lại, tuy nhiên nó không phải là giải pháp thay thế toàn bộ cho các mạng Lan nối dây truyền thống.

Dựa trên chuẩn IEEE 802.11 mạng WLan đã đi đến sự thống nhất và trở thành mạng công nghiệp, từ đó được áp dụng trong rất nhiều lĩnh vực, từ lĩnh vực chăm sóc sức khỏe, bán lẻ, sản xuất, lưu kho, đến các trường đại học. Ngày nay, mạng WLAN đang được đón nhận rộng rãi như một kết nối đa năng từ các doanh nghiệp. Lợi tức của thị trường mạng WLAN ngày càng tăng. Vì vậy, nhóm chúng em đã chọn đề tài tìm hiểu công nghệ Wirelesss LAN.

Chúng em xin chân thành cám ơn các thầy cô đã tạo điều kiện cho chúng em và đã nhiệt tình chỉ bảo cho chúng em, chúng em xin chân thành cảm ơn.

CHƯƠNG I

GIỚI THIỆU VỀ MẠNG WLAN

Mạng WLAN là một hệ thống thông tin liên lạc dữ liệu linh hoạt được thực hiện như phần mở rộng, hoặc thay thế cho mạng LAN hữu tuyến trong nhà hoặc trong các cơ quan. Sử dụng sóng điện từ, mạng WLAN truyền và nhận dữ liệu qua khoảng không, tối giản nhu cầu cho các kết nối hữu tuyến. Như vậy, mạng WLAN kết nối dữ liệu với người dùng lưu động, và thông qua cấu hình được đơn giản hóa, cho phép mạng LAN di động.

Các năm qua, mạng WLAN được phổ biến mạnh mẽ trong nhiều lĩnh vực, từ lĩnh vực chăm sóc sức khỏe, bán lẻ, sản xuất, lưu kho, đến các trường đại học. Ngành công nghiệp này đã kiếm lợi từ việc sử dụng các thiết bị đầu cuối và các máy tính notebook để truyền thông tin thời gian thực đến các trung tâm tập trung để xử lý. Ngày nay, mạng WLAN đang được đón nhận rộng rãi như một kết nối đa năng từ các doanh nghiệp. Lợi tức của thị trường mạng WLAN ngày càng tăng.

1.1 Các ứng dụng của Mạng WLAN:

Mạng WLAN là kỹ thuật thay thế cho mạng LAN hữu tuyến, nó cung cấp mạng cuối cùng với khoảng cách kết nối tối thiểu giữa một mạng xương sống và mạng trong nhà hoặc người dùng di động trong các cơ quan. Sau đây là các ứng dụng phổ biến của WLAN thông qua sức mạnh và tính linh hoạt của mạng WLAN:

- Trong các bệnh viện, các bác sỹ và các hộ lý trao đổi thông tin về bệnh nhân một cách tức thời, hiệu quả hơn nhờ các máy tính notebook sử dụng công nghệ mạng WLAN.
- Các đội kiểm toán tư vấn hoặc kế toán hoặc các nhóm làm việc nhỏ tăng năng suất với khả năng cài đặt mạng nhanh.
- Nhà quản lý mạng trong các môi trường năng động tối thiểu hóa tổng phí đi lại, bổ sung, và thay đổi với mạng WLAN, do đó giảm bớt giá thành sở hữu mạng LAN.
- Các cơ sở đào tạo của các công ty và các sinh viên ở các trường đại học sử dụng kết nối không dây để dễ dàng truy cập thông tin, trao đổi thông tin, và nghiên cứu.

- Các nhà quản lý mạng nhận thấy rằng mạng WLAN là giải pháp cơ sở hạ tầng mạng lợi nhất để lắp đặt các máy tính nối mạng trong các tòa nhà cũ.
- Nhà quản lý của các cửa hàng bán lẻ sử dụng mạng không dây để đơn giản hóa việc tái định cấu hình mạng thường xuyên.
- Các nhân viên văn phòng chi nhánh và triển lãm thương mại tối giản các yêu cầu cài đặt bằng cách thiết đặt mạng WLAN có định cấu hình trước không cần các nhà quản lý mạng địa phương hỗ trợ.
- Các công nhân tại kho hàng sử dụng mạng WLAN để trao đổi thông tin đến cơ sở dữ liệu trung tâm và tăng thêm năng suất của họ.
- Các nhà quản lý mạng thực hiện mạng WLAN để cung cấp dự phòng cho các ứng dụng trọng yếu đang hoạt động trên các mạng nối dây.
- Các đại lý dịch vụ cho thuê xe và các nhân viên nhà hàng cung cấp dịch vụ nhanh hơn tới khách hàng trong thời gian thực.
- Các cán bộ cấp cao trong các phòng hội nghị cho các quyết định nhanh hơn vì họ sử dụng thông tin thời gian thực ngay tại bàn hội nghị.

1.2 Các lợi ích của mạng WLAN:

Độ tin tưởng cao trong nối mạng của các doanh nghiệp và sự tăng trưởng mạnh mẽ của mạng Internet và các dịch vụ trực tuyến là bằng chứng mạnh mẽ đối với lợi ích của dữ liệu và tài nguyên dùng chung. Với mạng WLAN, người dùng truy cập thông tin dùng chung mà không tìm kiếm chỗ để cắm vào, và các nhà quản lý mạng thiết lập hoặc bổ sung mạng mà không lắp đặt hoặc di chuyển dây nối. Mạng WLAN cung cấp các hiệu suất sau: khả năng phục vụ, tiện nghi, và các lợi thế về chi phí hơn hẳn các mạng nối dây truyền thống.

- ***Khả năng lưu động cải thiện hiệu suất và dịch vụ***: Các hệ thống mạng WLAN cung cấp sự truy cập thông tin thời gian thực tại bất cứ đâu cho người dùng mạng trong tổ chức của họ. Khả năng lưu động này hỗ trợ các cơ hội về hiệu suất và dịch vụ mà mạng nối dây không thể thực hiện được.
- ***Đơn giản và tốc độ nhanh trong cài đặt***: Cài đặt hệ thống mạng WLAN nhanh và dễ dàng và loại trừ nhu cầu kéo dây qua các tường và các trần nhà.
- ***Linh hoạt trong cài đặt***: Công nghệ không dây cho phép mạng đi đến các nơi mà mạng nối dây không thể.
- ***Giảm bớt giá thành sở hữu***: Trong khi đầu tư ban đầu của phần cứng cần cho mạng WLAN có giá thành cao hơn các chi phí phần cứng mạng LAN hữu tuyến, nhưng chi phí cài đặt toàn bộ và giá thành tính theo tuổi thọ thấp hơn đáng kể. Các lợi ích về giá thành tính theo tuổi thọ là đáng kể trong môi trường năng động yêu cầu thường xuyên di chuyển, bổ sung, và thay đổi.

- ***Tính linh hoạt***: Các hệ thống mạng WLAN được định hình theo các kiểu topo khác nhau để đáp ứng các nhu cầu của các ứng dụng và các cài đặt cụ thể. Cấu hình mạng dễ thay đổi từ các mạng độc lập phù hợp với số nhỏ người dùng đến các mạng cơ sở hạ tầng với hàng nghìn người sử dụng trong một vùng rộng lớn.
- ***Khả năng vô hướng***: các mạng máy tính không dây có thể được cấu hình theo các topo khác nhau để đáp ứng các nhu cầu ứng dụng và lắp đặt cụ thể. Các cấu hình dễ dàng thay đổi từ các mạng ngang hàng thích hợp cho một số lượng nhỏ người sử dụng đến các mạng có cơ sở hạ tầng đầy đủ dành cho hàng nghìn người sử dụng mà có khả năng di chuyển trên một vùng rộng.

1.3 Bảng so sánh ưu và nhược điểm giữa mạng không dây và có dây:

1. Phạm vi ứng dụng

Mạng có dây	Mạng không dây
- Có thể ứng dụng trong tất cả các mô hình mạng nhỏ, trung bình, lớn, rất lớn - Gặp khó khăn ở những nơi xa xôi, địa hình phức tạp, những nơi không ổn định, khó kéo dây, đường truyền	- Chủ yếu là trong mô hình mạng nhỏ và trung bình, với những mô hình lớn phải kết hợp với mạng có dây - Có thể triển khai ở những nơi không thuận tiện về địa hình, không ổn định, không triển khai mạng có dây được

2. Độ phức tạp kỹ thuật

Mạng có dây	Mạng không dây
- Độ phức tạp kỹ thuật tùy thuộc từng loại mạng cụ thể	- Độ phức tạp kỹ thuật tùy thuộc từng loại mạng cụ thể - Xu hướng tạo khả năng thiết lập các thông số truyền sóng vô tuyến của thiết bị ngày càng đơn giản hơn

3. Độ tin cậy

Mạng có dây	Mạng không dây
- Khả năng chịu ảnh hưởng khách quan bên ngoài như thời tiết, khí hậu tốt - Chịu nhiều cuộc tấn công đa dạng,	- Bị ảnh hưởng bởi các yếu tố bên ngoài như môi trường truyền sóng, can nhiễu do thời tiết - Chịu nhiều cuộc tấn công đa dạng,

phức tạp, nguy hiểm của những kẻ phá hoại vô tình và cố tình - Ít nguy cơ ảnh hưởng sức khỏe	phức tạp, nguy hiểm của những kẻ phá hoại vô tình và cố tình, nguy cơ cao hơn mạng có dây - Còn đang tiếp tục phân tích về khả năng ảnh hưởng đến sức khỏe

4. Lắp đặt, triển khai

Mạng có dây	Mạng không dây
- Lắp đặt, triển khai tốn nhiều thời gian và chi phí	- Lắp đặt, triển khai dễ dàng, đơn giản, nhanh chóng

5. Tính linh hoạt, khả năng thay đổi, phát triển

Mạng có dây	Mạng không dây
- Vì là hệ thống kết nối cố định nên tính linh hoạt kém, khó thay đổi, nâng cấp, phát triển	- Vì là hệ thống kết nối di động nên rất linh hoạt, dễ dàng thay đổi, nâng cấp, phát triển

6. Giá cả

Mạng có dây	Mạng không dây
- Giá cả tùy thuộc vào từng mô hình mạng cụ thể	- Thường thì giá thành thiết bị cao hơn so với của mạng có dây. Nhưng xu hướng hiện nay là càng ngày càng giảm sự chênh lệch về giá

CHƯƠNG II

NGUYÊN TẮC HOẠT ĐỘNG CỦA WLAN

2.1 Cách làm việc của mạng WLAN:

Mạng WLAN sử dụng sóng điện từ (vô tuyến và tia hồng ngoại) để truyền thông tin từ điểm này sang điểm khác mà không dựa vào bất kỳ kết nối vật lý nào. Các sóng vô tuyến thường là các sóng mang vô tuyến bởi vì chúng thực hiện chức năng phân phát năng lượng đơn giản tới máy thu ở xa. Dữ liệu truyền được chồng lên trên sóng mang vô tuyến để nó được nhận lại đúng ở máy thu. Đó là sự điều biến sóng mang theo thông tin được truyền. Một khi dữ liệu được chồng (được điều chế) lên trên sóng mang vô tuyến, thì tín hiệu vô tuyến chiếm nhiều hơn một tần số đơn, vì tần số hoặc tốc độ truyền theo bit của thông tin biến điệu được thêm vào sóng mang.

Nhiều sóng mang vô tuyến tồn tại trong cùng không gian tại cùng một thời điểm mà không nhiễu với nhau nếu chúng được truyền trên các tần số vô tuyến khác nhau. Để nhận dữ liệu, máy thu vô tuyến bắt sóng (hoặc chọn) một tần số vô tuyến xác định trong khi loại bỏ tất cả các tín hiệu vô tuyến khác trên các tần số khác.

Trong một cấu hình mạng WLAN tiêu biểu, một thiết bị thu phát, được gọi một điểm truy cập *(AP - access point)*, nối tới mạng nối dây từ một vị trí cố định sử dụng cáp Ethernet chuẩn. Điểm truy cập *(access point)* nhận, lưu vào bộ nhớ đệm, và truyền dữ liệu giữa mạng WLAN và cơ sở hạ tầng mạng nối dây. Một điểm truy cập đơn hỗ trợ một nhóm nhỏ người sử dụng và vận hành bên trong một phạm vi vài mét tới vài chục mét. Điểm truy cập (hoặc anten được gắn tới nó) thông thường được gắn trên cao nhưng thực tế được gắn bất cứ nơi đâu miễn là khoảng vô tuyến cần thu được.

Các người dùng đầu cuối truy cập mạng WLAN thông qua các card giao tiếp mạng WLAN, mà được thực hiện như các card PC trong các máy tính notebook, hoặc sử dụng card giao tiếp ISA hoặc PCI trong các máy tính để bàn, hoặc các thiết bị tích hợp hoàn toàn bên trong các máy tính cầm tay. Các card giao tiếp mạng WLAN cung cấp một giao diện giữa hệ điều hành mạng (NOS) và sóng trời (qua một anten). Bản chất của kết nối không dây là trong suốt với NOS.

2.2 Các cấu hình mạng WLAN:

Mạng WLAN đơn giản hoặc phức tạp. Cơ bản nhất, hai PC được trang bị các card giao tiếp không dây thiết lập một mạng độc lập bất cứ khi nào mà chúng nằm

trong phạm vi của nhau. Nó được gọi là mạng ngang hàng. Các mạng này không yêu cầu sự quản trị hoặc sự định cấu hình trước. Trong trường hợp này mỗi khách hàng chỉ truy cập tới tài nguyên của khách hàng khác và không thông qua một nhà phục vụ trung tâm.

Hình 2.1. Một mạng ngang hàng không dây

Việc thiết lập một điểm truy cập mở rộng phạm vi của một mạng, phạm vi các thiết bị liên lạc được mở rộng gấp đôi. Khi điểm truy cập được nối tới mạng nối dây, mỗi khách hàng sẽ truy cập tới các tài nguyên phục vụ cũng như tới các khách hàng khác. Mỗi điểm truy cập điều tiết nhiều khách hàng, số khách hàng cụ thể phụ thuộc vào số lượng và đặc tính truyền. Nhiều ứng dụng thực tế với một điểm truy cập phục vụ từ 15 đến 50 thiết bị khách hàng.

Hình 2.2. Khách hàng và điểm truy nhập

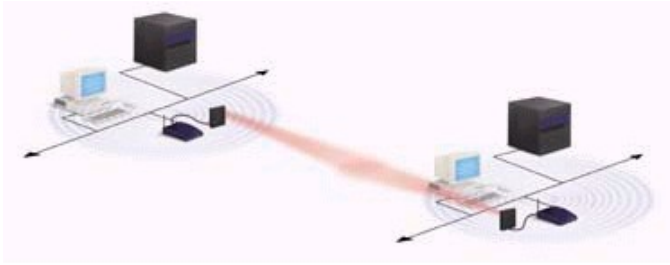
Các điểm truy cập có một phạm vi hữu hạn, 152,4m trong nhà và 304,8m ngoài trời. Trong phạm vi rất lớn hơn như kho hàng, hoặc khu vực cơ quan cần thiết phải lặp đặt nhiều điểm truy cập hơn. Việc xác định vị trí điểm truy dựa trên ph-ương pháp khảo sát vị trí. Mục đích sẽ phủ lên vùng phủ sóng bằng các cell phủ sóng chồng lấp nhau để các khách hàng di chuyển khắp vùng mà không mất liên lạc mạng. Khả năng các khách hàng di chuyển không ghép nối giữa một cụm của các điểm truy cập được gọi roaming. Các điểm truy cập chuyển khách hàng từ site này đến site khác một cách tự động mà khách hàng không hay biết, bảo đảm cho kết nối liên tục.

Hình 2.3. Nhiều điểm truy cập và Roaming

Để giải quyết các vấn đề đặc biệt về topology, nhà thiết kế mạng chọn cách sử dụng các điểm mở rộng (Extension Point - EP) để làm tăng các điểm truy cập của mạng. Cách nhìn và chức năng của các điểm mở rộng giống như các điểm truy cập, nhưng chúng không được nối dây tới mạng nối dây như là các AP. Chức năng của EP nhằm mở rộng phạm vi của mạng bằng cách làm trễ tín hiệu từ một khách hàng đến một AP hoặc EP khác. Các EP được nối tiếp nhau để truyền tin từ một AP đến các khách hàng rộng khắp, như một đoàn người chuyển nước từ người này đến người khác đến một đám cháy.

Hình 2.4. Cách sử dụng của một điểm mở rộng (EP)

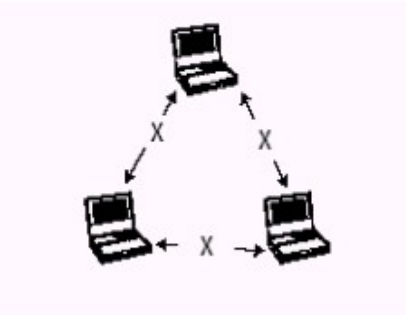
Thiết bị mạng WLAN cuối cùng cần xem xét là anten định hướng. Giả sử có một mạng WLAN trong tòa nhà A của bạn, và bạn muốn mở rộng nó tới một tòa nhà cho thuê B, cách đó 1,609 km. Một giải pháp là sẽ lắp đặt một anten định hướng trên mỗi tòa nhà, các anten hướng về nhau. Anten tại tòa nhà A được nối tới mạng nối dây qua một điểm truy cập. Tương tự, anten tại tòa nhà B được nối tới một điểm truy cập trong tòa nhà đó, mà cho phép kết nối mạng WLAN thuận tiện nhất.



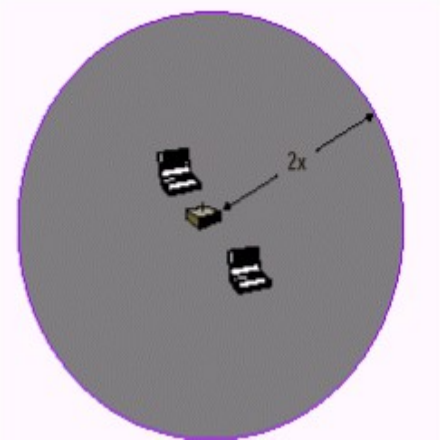
Hình 2.5. Cách sử dụng anten định hướng

2.2.1 Mạng WLAN độc lập (mạng ngang hàng):

Cấu hình mạng WLAN đơn giản nhất là mạng WLAN độc lập (hoặc ngang hàng) nối các PC với các card giao tiếp không dây. Bất kỳ lúc nào, khi hai hoặc hơn card giao tiếp không dây nằm trong phạm vi của nhau, chúng thiết lập một mạng độc lập (hình 2.6). Ở đây, các mạng này không yêu cầu sự quản trị hoặc sự định cấu hình trước.



Hình 2.6. Mạng WLAN độc lập

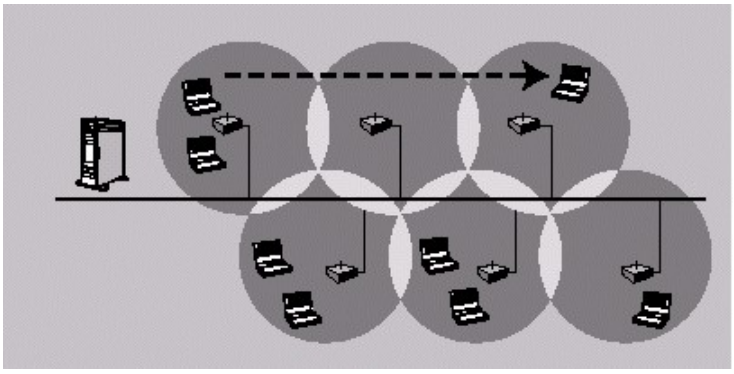


Hình 2.7. Mạng WLAN độc lập phạm vi được mở rộng sử dụng điểm truy cập như một bộ chuyển tiếp

Các điểm truy cập mở rộng phạm vi của mạng WLAN độc lập bằng cách đóng vai trò như là một bộ chuyển tiếp (hình 2.7), có hiệu quả gấp đôi khoảng cách giữa các PC không dây.

2.2.2. Mạng WLAN cơ sở hạ tầng (infrastructure):

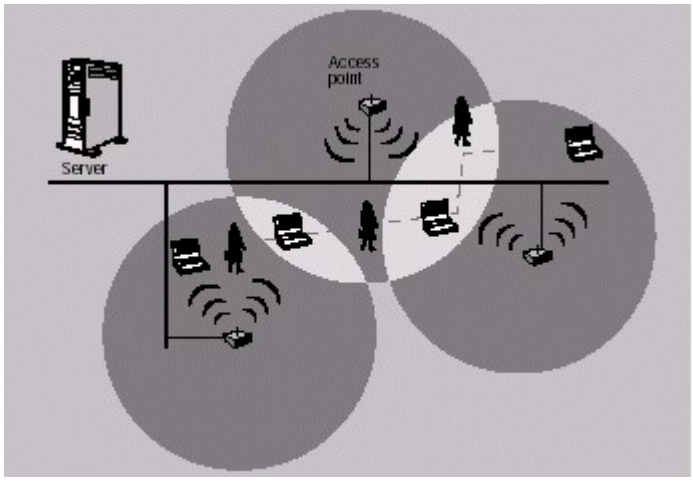
Trong mạng WLAN cơ sở hạ tầng, nhiều điểm truy cập liên kết mạng WLAN với mạng nối dây và cho phép các người dùng chia sẻ các tài nguyên mạng một cách hiệu quả. Các điểm truy cập không các cung cấp các truyền thông với mạng nối dây mà còn chuyển tiếp lưu thông mạng không dây trong khu lân cận một cách tức thời. Nhiều điểm truy cập cung cấp phạm vi không dây cho toàn bộ tòa nhà hoặc khu vực cơ quan.



Hình 2.8. Mạng WLAN Cơ sở hạ tầng

2.2.3 Microcells và roaming:

Thông tin vô tuyến bị giới hạn bởi tín hiệu sóng mang đi bao xa khi công suất ra đã cho trước. Mạng WLAN sử dụng các cell, gọi là các *microcell*, tương tự hệ thống điện thoại tế bào để mở rộng phạm vi của kết nối không dây. Tại bất kỳ điểm truy cập nào trong cùng lúc, một PC di động được trang bị với một card giao tiếp mạng WLAN được liên kết với một điểm truy cập đơn và microcell của nó, hoặc vùng phủ sóng. Các microcell riêng lẻ chồng lắp để cho phép truyền thông liên tục bên trong mạng nối dây. Chúng xử lý các tín hiệu công suất thấp và không cho người dùng truy cập khi họ đi qua một vùng địa lý cho trước.



Hình 2.9. Handing off giữa các điểm truy cập

2.3 Các tùy chọn công nghệ:

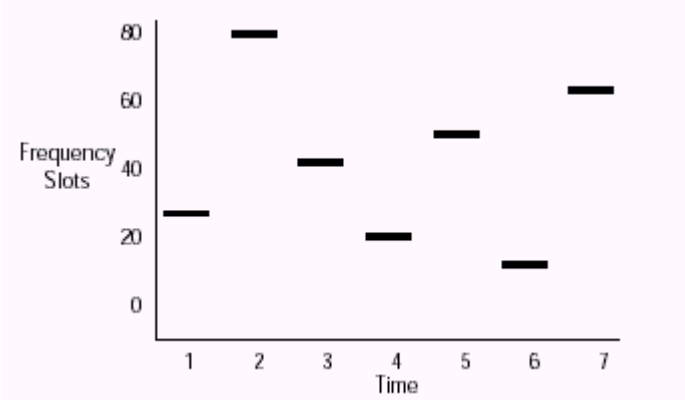
Các nhà sản xuất mạng WLAN chọn nhiều công nghệ mạng khác nhau khi thiết kế giải pháp mạng WLAN. Mỗi công nghệ có các thuận lợi và hạn chế riêng.

2.3.1 Trải phổ

Đa số các hệ thống mạng WLAN sử dụng công nghệ trải phổ, một kỹ thuật tần số vô tuyến băng rộng mà trước đây được phát triển bởi quân đội trong các hệ thống truyền thông tin cậy, an toàn, trọng yếu. Sự trải phổ được thiết kế hiệu quả với sự đánh đổi dải thông lấy độ tin cậy, khả năng tích hợp, và bảo mật. Nói cách khác, sử dụng nhiều băng thông hơn trường hợp truyền băng hẹp, nhưng đổi lại tạo ra tín hiệu mạnh hơn nên dễ được phát hiện hơn, miễn là máy thu biết các tham số của tín hiệu trải phổ của máy phát. Nếu một máy thu không chỉnh đúng tần số, thì tín hiệu trải phổ giống như nhiễu nền. Có hai kiểu trải phổ truyền đi bằng vô tuyến: nhảy tần và chuỗi trực tiếp.

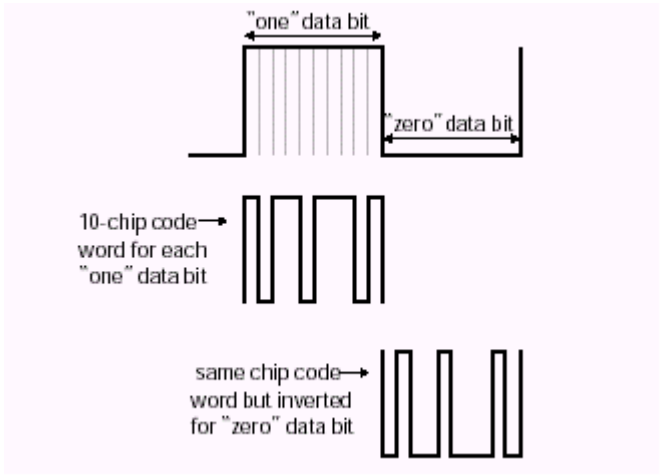
2.3.2 Công nghệ trải phổ nhảy tần (Frequency Hopping pread Spectrum)

Trải phổ nhảy tần (FHSS) sử dụng một sóng mang băng hẹp để thay đổi tần số trong một mẫu ở cả máy phát lẫn máy thu. Được đồng bộ chính xác, hiệu ứng mạng sẽ duy trì một kênh logic đơn. Đối với máy thu không mong muốn, FHSS làm xuất hiện các nhiễu xung chu kỳ ngắn.



Hình 2.10. Trải phổ nhảy tần

FHSS "nhảy" tần từ băng hẹp sang băng hẹp bên trong một băng rộng. Đặc biệt hơn, các sóng vô tuyến FHSS gửi một hoặc nhiều gói dữ liệu tại một tần số sóng mang, nhảy đến tần số khác, gửi nhiều gói dữ liệu, và tiếp tục chuỗi "nhảy - truyền" dữ liệu này. Mẫu nhảy hay chuỗi này xuất hiện ngẫu nhiên, nhưng thật ra là một chuỗi có tính chu kỳ được cả máy thu và máy phát theo dõi. Các hệ thống FHSS dễ bị ảnh hưởng của nhiễu trong khi nhảy tần, nhưng hoàn thành việc truyền dẫn trong các quá trình nhảy tần khác trong băng tần.



Hình 2.11. Trải phổ chuỗi trực tiếp

2.3.3 Công nghệ trải phổ chuỗi trực tiếp (Direct Sequence Spread Spectrum)

Trải phổ chuỗi trực tiếp (DSSS) tạo ra một mẫu bit dư cho mỗi bit được truyền. Mẫu bit này được gọi một *chip* (hoặc *chipping code*). Các chip càng dài, thì xác suất mà dữ liệu gốc bị loại bỏ càng lớn (và tất nhiên, yêu cầu nhiều dải thông). Thậm chí khi một hoặc nhiều bit trong một chip bị hư hại trong thời gian truyền, thì các kỹ thuật được nhúng trong vô tuyến khôi phục dữ liệu gốc mà không yêu cầu truyền lại. Đối với máy thu không mong muốn, DSSS làm xuất hiện nhiễu băng rộng công suất thấp và được loại bỏ bởi hầu hết các máy thu băng hẹp.

Bộ phát DSSS biến đổi luồng dữ liệu vào (luồng bit) thành luồng symbol, trong đó mỗi symbol biểu diễn một nhóm các bit. Bằng cách sử dụng kỹ thuật điều biến pha thay đổi như kỹ thuật QPSK (khóa dịch pha cầu phương), bộ phát DSSS

điều biến hay nhân mỗi symbol với một mã giống nhiễu gọi là chuỗi giả ngẫu nhiên (PN). Nó được gọi là chuỗi "chip". Phép nhân trong bộ phát DSSS làm tăng giả tạo dải băng được dùng phụ thuộc vào độ dài của chuỗi chip.

2.3.4 Công nghệ băng hẹp (narrowband)

Một hệ thống vô tuyến băng hẹp truyền và nhận thông tin người dùng trên một tần số vô tuyến xác định. Vô tuyến băng hẹp giữ cho dải tần tín hiệu vô tuyến càng hẹp càng tốt chỉ cho thông tin đi qua. Sự xuyên âm không mong muốn giữa các kênh truyền thông được tránh bằng cách kết hợp hợp lý các người dùng khác nhau trên các kênh có tần số khác nhau.

Một đường dây điện thoại riêng rất giống với một tần số vô tuyến. Khi mỗi nhà lân cận nhau đều có đường dây điện thoại riêng, người trong nhà này không thể nghe các cuộc gọi trong nhà khác. Trong một hệ thống vô tuyến, sử dụng các tần số vô tuyến riêng biệt để hợp nhất sự riêng tư và sự không can thiệp lẫn nhau. Các bộ lọc của máy thu vô tuyến lọc bỏ tất cả các tín hiệu vô tuyến trừ các tín hiệu có tần số được thiết kế.

2.3.5 Công nghệ hồng ngoại (Infrared)

Hệ thống tia hồng ngoại (IR) sử dụng các tần số rất cao, chỉ dưới tần số của ánh sáng khả kiến trong phổ điện từ, để mang dữ liệu. Giống như ánh sáng, tia hồng ngoại IR không thể thâm nhập các đối tượng chắn sáng; nó sử dụng công nghệ trực tiếp (tầm nhìn thẳng) hoặc công nghệ khuếch tán. Các hệ thống trực tiếp rẽ tiền cung cấp phạm vi rất hạn chế (0,914m) và tiêu biểu được sử dụng cho mạng PAN nhưng thỉnh thoảng được sử dụng trong các ứng dụng WLAN đặc biệt. Công nghệ hồng ngoại hướng khả năng thực hiện cao không thực tế cho các người dùng di động, và do đó nó được sử dụng để thực hiện các mạng con cố định. Các hệ thống IR WLAN khuếch tán không yêu cầu tầm nhìn thẳng, nhưng các cell bị hạn chế trong các phòng riêng lẻ.

2.4 Các chỉ tiêu kỹ thuật của mạng WLAN:

So với mạng LAN hữu tuyến, mạng WLAN linh hoạt hơn trong cài đặt, định cấu hình và tự do vốn có trong mạng lưu động. Các khách hàng mạng WLAN cũng như các nhân viên kỹ thuật cần xem xét các chỉ tiêu kỹ thuật sau.

2.4.1 Phạm vi/Vùng phủ sóng

Khoảng cách mà qua đó các sóng RF truyền thông là một nhiệm vụ của việc thiết kế sản phẩm (bao gồm thiết kế máy thu và công suất phát) và đường truyền dẫn mạng LAN, đặc biệt trong môi trường trong nhà. Các tương tác với các đối tượng xây dựng tiêu biểu, bao gồm tường nhà, kim loại, và thậm chí cả con người, ảnh hưởng đến cách truyền năng lượng, và như vậy tính được phạm vi và vùng phủ sóng của hệ thống. Đa số các hệ thống mạng WLAN sử dụng sóng RF vì các sóng vô tuyến thâm nhập qua tường và các bề mặt trong nhà. Phạm vi (hoặc bán kính phủ sóng) tiêu biểu của hệ thống mạng WLAN thay đổi từ dưới 30,48m tới hơn 152,4m.

Vùng phủ sóng được mở rộng, và sự tự do đích thực của khả năng lưu động thông qua roaming, được cung cấp qua các microcell.

2.4.2 Lưu lượng

Như các hệ thống mạng LAN hữu tuyến, lưu lượng thực tế trong mạng WLAN là sản phẩm và cơ cấu phụ thuộc. Các nhân tố ảnh hưởng tới lưu lượng bao gồm sự tắc nghẽn sóng (số lượng người dùng), các hệ số truyền, kiểu hệ thống mạng WLAN sử dụng, cũng như gốc trễ và các cổ chai trên các phần nối dây của mạng WLAN. Tốc độ dữ liệu tiêu biểu từ 1 đến 11 Mbps.

Mạng WLAN cung cấp lưu lượng đủ cho các ứng dụng văn phòng phổ biến trên nền mạng LAN, bao gồm sự trao đổi email, truy cập để chia sẻ thiết bị ngoại vi, và các truy cập tới cơ sở dữ liệu và các ứng dụng nhiều người dùng.

2.4.3 Sự toàn vẹn và độ tin cậy

Các công nghệ dữ liệu không dây đã được chứng minh qua hơn năm mươi năm sử dụng các ứng dụng không dây trong các hệ thống cả thương mại lẫn quân đội. Nhiễu vô tuyến gây ra sự giảm sút lưu lượng, nhưng chúng hiếm có tại nơi làm việc. Các thiết kế nổi bật của công nghệ mạng WLAN và giới hạn khoảng cách tín hiệu truyền dẫn tại các kết nối của mạng này mạnh hơn các kết nối điện thoại tế bào, và mạng cung cấp khả năng thực hiện toàn vẹn dữ liệu bằng hoặc hơn mạng nối dây.

2.4.4 Khả năng kết nối với cơ sở hạ tầng mạng nối dây

Đa số các hệ thống mạng WLAN cung cấp kết nối chuẩn công nghiệp với các hệ thống nối dây, bao gồm Ethernet (IEEE 802.3) và Token Ring (IEEE 802.5). Khả năng kết nối trên nền chuẩn làm các phần không dây của mạng trong suốt hoàn toàn với phần còn lại của mạng. Các nút mạng WLAN lược hỗ trợ bởi các hệ điều hành mạng theo cách giống như các nút mạng LAN khác qua trình điều khiển. Một khi được cài đặt, các hệ điều hành mạng xem các nút mạng như mọi thành phần khác của mạng.

2.4.5 Khả năng kết nối với cơ sở hạ tầng mạng không dây

Có thể có vài kiểu kết nối giữa các mạng WLAN. Điều này phụ thuộc cả cách lựa chọn công nghệ lẫn cách thực hiện của nhà cung cấp thiết bị cụ thể. Các sản phẩm từ các nhà cung cấp khác nhau sử dụng cùng công nghệ và cùng cách thực hiện cho phép trao đổi giữa các card giao tiếp và các điểm truy cập. Mục đích của các chuẩn công nghiệp, như các đặc tả kỹ thuật IEEE 802.11, sẽ cho phép các sản phẩm tương hợp vận hành với nhau mà không có sự hợp tác rõ ràng giữa các nhà cung cấp.

2.4.6 Nhiễu

Đối với các WLAN hoạt động ở băng tần vô tuyến 2,4 GHz các lò vi sóng là một nguồn nhiễu quan trọng. Các lò vi sóng công suất lên tới 750W với 150 xung trên giây và có bán kính bức xạ hoạt động khoảng 10 m. Như vậy đối với tốc độ dữ liệu 2 Mbit/s độ dài gói lớn nhất phải nhỏ hơn 20.000 bit hoặc 2.500 octet. Bức xạ

phát ra quét từ 2,4 GHz đến 2,45 GHz và giữ ổn định theo chu kỳ ngắn ở tần số 2,45 GHz. Cho dù các khối bị chắn thì phần lớn năng lượng vẫn gây nhiễu tới truyền dẫn WLAN. Các nguồn nhiễu khác trong băng tần 2,4 GHz gồm máy photocopy, các thiết bị chống trộm, các mô tơ thang máy và các thiết bị y tế.

2.4.7 Tính đơn giản và dễ dàng trong sử dụng

Người dùng cần rất ít thông tin mới để nhận được thuận lợi của mạng WLAN. Vì bản chất không dây của mạng WLAN là trong suốt đối với hệ điều hành mạng người dùng, nên các ứng dụng hoạt động giống như chúng hoạt động trên mạng LAN hữu tuyến. Các sản phẩm mạng WLAN hợp nhất sự đa dạng của các công cụ chẩn đoán để hướng vào các vấn đề liên quan đến các thành phần không dây của hệ thống; tuy nhiên, các sản phẩm được thiết kế để hầu hết các người dùng hiếm khi cần đến các công cụ này.

Mạng WLAN đơn giản hóa nhiều vấn đề cài đặt và định cấu hình mà rất phiền toái đối với các nhà quản lý mạng. Chỉ khi các điểm truy cập của mạng WLAN yêu cầu nối cáp, các nhà quản lý mạng được giải phóng khỏi việc kéo cáp cho các người đầu cuối mạng WLAN. Không có nối cáp cũng làm di chuyển, bổ sung, và thay đổi các hoạt động bình thường trên mạng WLAN. Cuối cùng, bản chất di động của mạng WLAN cho phép các nhà quản lý mạng định cấu hình trước và sửa lỗi toàn bộ mạng trước khi lắp đặt chúng tại các vị trí từ xa. Một kho được định cấu hình, mạng WLAN được di chuyển từ chỗ này đến chỗ khác mà ít hoặc không có sự cải biến nào.

2.4.8 Bảo mật

Vì công nghệ không dây bắt nguồn từ các ứng dụng trong quân đội, nên từ lâu độ bảo mật đã là một tiêu chuẩn thiết kế cho các thiết bị vô tuyến. Các điều khoản bảo mật điển hình được xây dựng bên trong mạng WLAN, làm cho chúng trở nên bảo mật hơn so với hầu hết các mạng LAN hữu tuyến. Các máy thu không mong muốn (các người nghe trộm) khó có khả năng bắt được tin đang lưu thông trong mạng WLAN. Kỹ thuật mã hóa phức tạp làm cho các giả mạo tốt nhất để truy cập không phép đến lưu thông mạng là không thể. Nói chung, các nút riêng lẻ phải cho phép bảo mật trước khi chúng được phép để tham gia vào lưu thông mạng.

2.4.9 Chi phí

Một mạng WLAN thực hiện đầy đủ bao gồm cả chi phí cơ sở hạ tầng, cho các điểm truy cập không dây, lẫn chi phí người dùng, cho các card giao tiếp mạng WLAN. Các chi phí cơ sở hạ tầng phụ thuộc chủ yếu vào số lượng điểm truy cập được triển khai; khoảng chi phí của các điểm truy cập từ 800$ tới 2000$. Số lượng điểm truy cập phụ thuộc tiêu biểu vào vùng phủ sóng được yêu cầu và/hoặc số và kiểu người dùng được dịch vụ. Vùng phủ sóng tỉ lệ bình phương với phạm vi sản phẩm. Các card giao tiếp mạng WLAN được yêu cầu trên nền máy tính chuẩn, và khoảng chi phí từ 200$ tới 700$. Chi phí lắp ráp và bảo trì một mạng WLAN nói chung thấp hơn giá lắp ráp và bảo trì của một mạng LAN hữu tuyến truyền thống, vì

hai lý do. Đầu tiên, một mạng WLAN loại trừ các chi phí trực tiếp của việc nối cáp và chi phí lao động liên quan đến lắp ráp và sửa chửa nó. Thứ hai, vì mạng WLAN đơn giản hóa việc di chuyển, bổ sung, và thay đổi, nên chúng giảm bớt các chi phí gián tiếp về thời gian nghỉ của người dùng và tổng phí hành chính.

2.4.10 Tính linh hoạt

Các mạng không dây được thiết kế để đơn giản vô cùng hoặc khá phức tạp. Các mạng không dây hỗ trợ số lượng nút mạng và/hoặc các vùng vật lý lớn lớn bằng cách thêm các điểm truy cập vào vùng phủ sóng được mở rộng hoặc tăng.

2.4.11 Tuổi thọ nguồn pin cho các sản phẩm di động

Các sản phẩm không dây của người dùng đầu cuối có khả năng được giải phóng hoàn toàn dây nhợ, và hoạt động quá nguồn pin trong máy tính notebook hoặc máy tính cầm tay chủ. Các nhà cung cấp mạng WLAN dùng các kỹ thuật thiết kế đặc biệt để làm tăng tuổi thọ pin và cách dùng nguồn năng lượng của máy tính chủ.

2.4.12 An toàn

Công suất ra của các hệ thống mạng WLAN rất thấp, ít hơn nhiều điện thoại tế bào cầm tay. Khi các sóng vô tuyến yếu dần nhanh chóng qua khoảng không thì có rất ít hướng để năng lượng RF cung cấp đến các vùng của hệ thống LAN không dây. Mạng WLAN phải thích hợp với sự quản lý nghiêm và các quy tắc công nghiệp để đảm bảo an toàn. Mạng WLAN không có hại cho sức khỏe cộng đồng.

CHƯƠNG III

CHUẨN IEEE 802.11

3.1 Lời giới thiệu:

Mục đích chương này sẽ cung cấp tổng quan về chuẩn IEEE 802.11 mới với các khái niệm cơ bản, các nguyên lý hoạt động, và vài lý do đằng sau các đặc tính và các thành phần của chuẩn. Chương này hướng vào các khía cạnh MAC và các chức năng chính của nó.

3.2 Kiến trúc IEEE chuẩn IEEE 802.11:

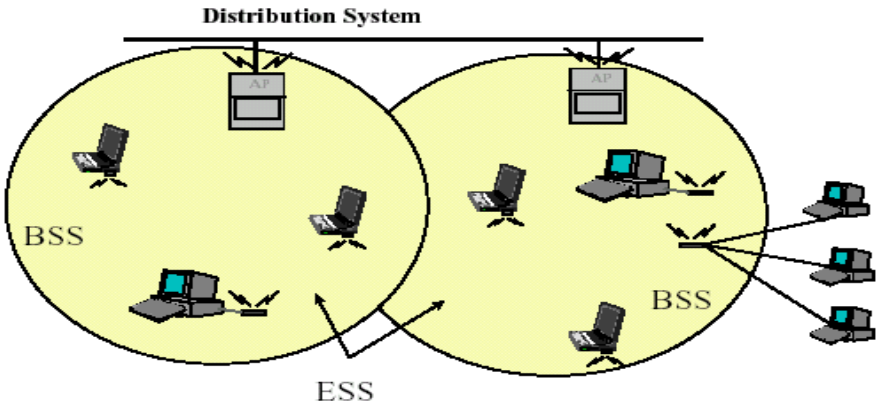
3.2.1 Các thành phần kiến trúc

Chuẩn mạng LAN IEEE 802.11 dựa vào kiến trúc tế bào, là kiến trúc trong đó hệ thống được chia nhỏ ra thành các cell, mỗi cell (được gọi là *Tập hợp dịch vụ cơ bản*, hoặc BSS) được kiểm soát bởi một trạm cơ sở (gọi là *điểm truy cập*, hoặc AP).

Mặc dù, một mạng LAN không dây có thể được hình thành từ một cell đơn, với một điểm truy cập đơn, nhưng hầu hết các thiết lập được hình thành bởi vài cell, tại đó các điểm truy cập được nối tới mạng xương sống (được gọi *hệ phân phối,* hoặc DS), tiêu biểu là Ethernet, và trong cả mạng không dây.

Toàn bộ liên kết lại mạng LAN không dây bao gồm các cell khác nhau, các điểm truy cập và hệ phân phối tương ứng, được xem xét thông qua mô hình OSI, như một mạng đơn chuẩn IEEE 802, và được gọi là *Tập hợp dịch vụ được mở rộng* (ESS).

Hình sau mô tả một chuẩn mạng LAN IEEE 802.11 tiêu biểu:



Hình 4.1. Mạng WLAN IEEE 802.11 tiêu biểu

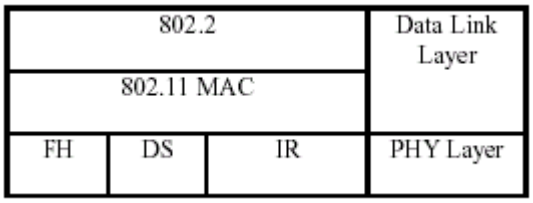
Chuẩn cũng định nghĩa khái niệm *Portal*, đó là một thiết bị liên kết giữa mạng LAN chuẩn IEEE 802.11 và mạng LAN chuẩn IEEE 802 khác. Khái niệm này mô tả về lý thuyết phần chức năng của "cầu chuyển dịch".

Mặc dù chuẩn không yêu cầu sự cài đặt tiêu biểu tất yếu phải có AP và *Portal* trên một thực thể vật lý đơn.

3.2.2 Mô tả các lớp chuẩn IEEE 802.11

Như bất kỳ giao thức chuẩn IEEE 802.x khác, giao thức chuẩn IEEE 802.11 bao gồm MAC và lớp vật lý, chuẩn hiện thời định nghĩa một MAC đơn tương tác với ba lớp vật lý (tất cả hoạt động ở tốc độ 1 và 2Mbit/s):

- FHSS hoạt động trong băng tần 2.4GHz
- DSSS hoạt động trong băng tần 2.4GHz, và
- Hồng ngoại



Hình 4.2. Lớp MAC

Ngoài các tính năng chuẩn được thực hiện bởi các lớp MAC, lớp MAC chuẩn IEEE 802.11 còn thực hiện chức năng khác liên quan đến các giao thức lớp trên, như Phân đoạn, Phát lại gói dữ liệu, và Các ghi nhận.

Lớp MAC: Lớp MAC định nghĩa hai phương pháp truy cập khác nhau, *Hàm phối hợp phân tán* và *Hàm phối hợp điểm*.

3.2.3. Phương pháp truy cập cơ bản: CSMA/CA

Đây là một cơ chế truy cập cơ bản, được gọi *Hàm phối hợp phân tán*, về cơ bản là đa truy cập cảm biến sóng mang với cơ chế tránh xung đột (CSMA/CA). Các giao thức CSMA được biết trong công nghiệp, mà phổ biến nhất là Ethernet, là giao thức CSMA/CD (CD nghĩa là phát hiện xung đột).

Giao thức CSMA làm việc như sau: Một trạm truyền đi các cảm biến môi trường, nếu môi trường bận (ví dụ, có một trạm khác đang phát), thì trạm sẽ trì hoãn truyền một lúc sau, nếu môi trường tự do thì trạm được cho phép để truyền.

Loại giao thức này rất có hiệu quả khi môi trường không tải nhiều, do đó nó cho phép các trạm truyền với ít trì hoãn, nhưng thường xảy ra trường hợp các trạm phát cùng lúc (có xung đột), gây ra do các trạm nhận thấy môi trường tự do và quyết định truyền ngay lập tức.

Các tình trạng xung đột này phải được xác định, vì vậy lớp MAC phải tự truyền lại gói mà không cần đến các lớp trên, điều này sẽ gây ra trễ đáng kể. Trong

trường hợp mạng Ethernet, sự xung đột này được đoán nhận bởi các trạm phát để đi tới quyết định phát lại dựa vào giải thuật *exponential random backoff*.

Các cơ chế dò tìm xung đột này phù hợp với mạng LAN nối dây, nhưng chúng không được sử dụng trong môi trường mạng LAN không dây, vì hai lý do chính:

1. Việc thực hiện cơ chế dò tìm xung đột yêu cầu sự thi hành toàn song công, khả năng phát và nhận đồng thời, nó sẽ làm tăng thêm chi phí một cách đáng kể.

2. Trên môi trường không dây chúng ta không thể giả thiết tất cả các trạm "nghe thấy" được nhau (đây là sự giả thiết cơ sở của sơ đồ dò tìm xung đột), và việc một trạm nhận thấy môi trường tự do và sẵn sàng để truyền không thật sự có nghĩa rằng môi trường là tự do quanh vùng máy thu.

Để vượt qua các khó khăn này, chuẩn IEEE 802.11 sử dụng một cơ chế tránh xung đột với một sơ đồ *Ghi nhận tính tích cực* (Positive Acknowledge) như sau:

Một trạm muốn truyền cảm biến môi trường, nếu môi trường bận thì nó trì hoãn. Nếu môi trường rãnh với thời gian được chỉ rõ (gọi là DIFS, Distributed Inter Frame Space, *Không gian khung Inter phân tán*), thì trạm được phép truyền, trạm thu sẽ kiểm tra mã CRC của gói nhận được và gửi một gói chứng thực (ACK). Chứng thực nhận được sẽ chỉ cho máy phát biết không có sự xung đột nào xuất hiện. Nếu máy phát không nhận chứng thực thì nó sẽ truyền lại đoạn cho đến khi nó được thừa nhận hoặc không được phép truyền sau một số lần phát lại cho trước.

Cảm biến sóng mang ảo (Virtual Carrier Sense)

Để giảm bớt xác suất khả năng hai trạm xung đột nhau vì chúng không thể "nghe thấy" nhau, chuẩn định nghĩa một cơ chế Cảm biến sóng mang ảo:

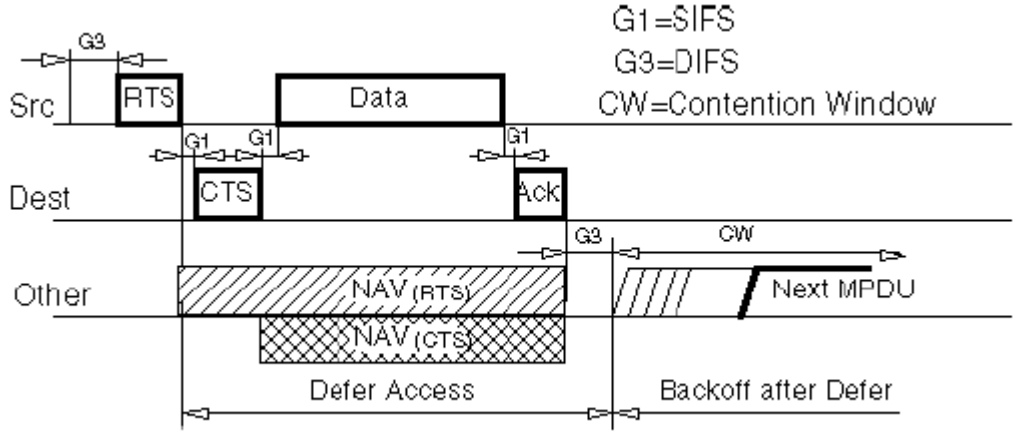
Một trạm muốn truyền một gói, trước hết nó sẽ truyền một gói điều khiển ngắn gọi là RTS (Request To Send) gồm nguồn, đích đến, và khoảng thời gian giao dịch sau đó (v.d. gói và ACK tương ứng), trạm đích sẽ đáp ứng (nếu môi trường tự do) bằng một gói điều khiển đáp lại gọi là CTS (Clear To Send) gồm cùng thông tin khoảng thời gian.

Tất cả các trạm nhận RTS và/hoặc CTS, sẽ thiết lập chỉ báo Virtual Carrier Sense của nó (gọi là NAV**,** Network Allocation Vector**,** *Vectơ định vị mạng*) cho khoảng thời gian cho trước, và sẽ sử dụng thông tin này cùng với Cảm biến sóng mang vật lý (Physical Carrier Sense) khi cảm biến môi trường.

Cơ chế này giảm bớt xác suất xung đột về vùng máy thu do một trạm "ẩn" từ máy phát, để làm ngắn khoảng thời gian truyền RTS, vì trạm sẽ nghe thấy CTS và "dự trữ" môi trường khi bận cho đến khi kết thúc giao dịch. Thông tin khoảng thời gian về RTS cũng bảo vệ vùng máy phát khỏi các xung đột trong thời gian ACK (bởi các trạm nằm ngoài phạm vi trạm nhận biết).

Cần chú ý thông tin khoảng thời ACK vì các khung RTS và CTS là các khung ngắn, Nó cũng làm giảm bớt mào đầu của các xung đột, vì chúng được nhận dạng nhanh hơn khi nó được nhận dạng nếu toàn bộ gói được truyền, (điều này đúng nếu gói lớn hơn RTS một cách đáng kể, như vậy là chuẩn cho phép kể cả các gói ngắn sẽ được truyền mà không có giao dịch RTS/CTS, và điều này được điều khiển bởi một tham số gọi là ngưỡng RTS).

Các sơ đồ sau cho thấy một giao dịch giữa hai trạm A và B, và sự thiết lập NAV của các trạm gần chúng:



Hình 4.3. Giao dịch giữa hai trạm A và B, và sự thiết lập NAV

Trạng thái NAV được kết hợp với cảm biến sóng mang vật lý để cho biết trạng thái bận của môi trường.

3.2.4 Các chứng thực mức MAC

Lớp MAC thực hiện dò tìm xung đột bằng cách chờ đợi sự tiếp nhận của một ghi nhận tới bất kỳ đoạn được truyền nào (Ngoại lệ các gói mà có hơn một nơi đến, như *Quảng bá*, chưa được thừa nhận).

3.2.5 Phân đoạn và Tái hợp

Các giao thức mạng LAN tiêu biểu sử dụng các gói với vài hàng trăm byte (ví dụ, gói Ethernet dài nhất dài trên 1518 byte) trên một môi trường mạng LAN không dây. Lý do các gói dài được ưa chuộng để sử dụng các gói nhỏ là:

- Vì tỉ lệ lỗi bit BER của thông tin vô tuyến cao hơn, xác suất một gói bị hư tăng thêm theo kích thước gói.
- Trong trường hợp bị hỏng (vì xung đột hoặc nhiễu), gói nhỏ nhất với ít mào đầu hơn gây ra sự phát lại gói.
- Trên một hệ thống FHSS, môi trường được ngắt định kỳ mỗi khi nhảy tần (trong trường hợp này là mỗi 20 mili - giây), như vậy nhỏ hơn gói, nhỏ hơn cơ hội truyền bị hoãn lại sau thời gian ngừng truyền.

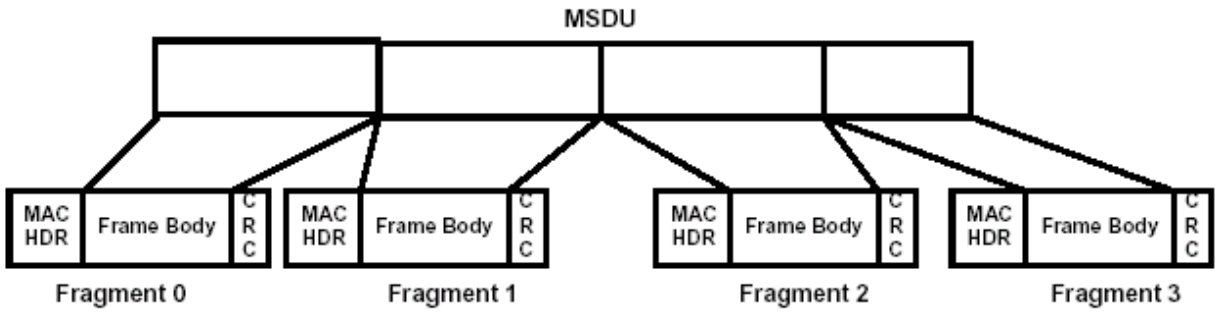
Mặc khác, nó không được giới thiệu như là một giao thức mạng LAN mới vì nó không thể giải quyết các gói 1518 byte được sử dụng trên mạng Ethernet, như vậy IEEE quyết định giải quyết vấn đề bằng cách thêm một cơ chế phân đoạn/tái hợp đơn giản tại lớp MAC.

Cơ chế là một giải thuật Send - and - Wait đơn, trong đó trạm phát không cho phép truyền một đoạn mới cho đến khi xảy ra một trong các tình huống sau đây:

1. Nhận một ACK cho đoạn, hoặc
2. Quyết định rằng đoạn cũng được truyền lại nhiều lần và thả vào toàn bộ khung

Cần phải nhớ rằng chuẩn cho phép trạm được truyền chỉ một địa chỉ khác giữa các phát lại của một đoạn đã cho, điều này đặc biệt hữu ích khi một AP có vài gói nổi bật với các đích đến khác nhau và một trong số chúng không trả lời.

Sơ đồ sau biểu diễn một khung (MSDU) được chia thành vài đoạn (MPDUs):



Hình 4.4. Khung MSDU

3.2.6 Các không gian khung Inter (Inter Frame Space)

Chuẩn định nghĩa 4 kiểu không gian khung Inter, được sử dụng để cung cấp các quyền ưu tiên khác nhau:

- SIFS - *Short Inter Frame Space*, được sử dụng để phân chia các truyền dẫn thuộc một hội thoại đơn (v.d. Ack - đoạn), và là Không gian khung Inter tối thiểu, và luôn có nhiều nhất một trạm đơn để truyền tại thời gian cho trước, do đó nó có quyền ưu tiên đối với tất cả các trạm khác. Đó là một giá trị cố định trên lớp vật lý và được tính toán theo cách mà trạm phát truyền ngược lại để nhận kiểu và khả năng giải mã gói vào, trong lớp vật lý chuẩn IEEE 802.11 FH giá trị này được thiết lập à 28 micrô - giây.
- PIFS - *Point Cooordination IFS*, được sử dụng bởi điểm truy cập (hoặc Point Coordinator, được gọi trong trường hợp này), để được truy cập tới môi trường trước mọi trạm khác. Giá trị này là SIFS cộng với một khe thời gian (sẽ được định nghĩa sau), ví dụ 78 micrô - giây.

- DIFS - *Distributed IFS*, Là không gian khung Inter được sử dụng bởi một trạm để sẵn sàng bắt đầu một truyền dẫn mới, mà là được tính toán là PIFS cộng thêm một khe thời gian, ví dụ 128 micrô - giây.
- EIFS - *Extended IFS*, Là một IFS dài hơn được sử dụng bởi một trạm đã nhận một gói không hiểu, nó cần để ngăn trạm (trạm mà không hiểu thông tin khoảng thời gian để Cảm biến sóng mang ảo) khỏi xung đột với một gói tương lai thuộc hội thoại hiện thời.

3.2.7 Giải thuật Exponential Backoff

Backoff là một phương pháp nổi tiếng để giải quyết các tranh dành giữa các trạm khác nhau muốn truy cập môi trường, phương pháp yêu cầu mỗi trạm chọn một số ngẫu nhiên (n) giữa 0 và một số cho trước, và đợi số khe thời gian này trước khi truy cập môi trường, nó luôn kiểm tra liệu có một trạm khác truy cập môi trường trước không.

Khe thời gian được định nghĩa theo cách mà một trạm sẽ luôn có khả năng xác định liệu trạm khác đã truy cập môi trường tại thời gian bắt đầu của khe trước đó không. Điều này làm giảm bớt xác suất xung đột đi một nửa.

Exponential Backoff có nghĩa rằng mỗi lần trạm chọn một khe thời gian và xảy ra xung đột, nó sẽ tăng giả trị theo lũy thừa một cách ngẫu nhiên.

Chuẩn IEEE 802.11 chuẩn định nghĩa giải thuật Exponential Backoff được thực hiện trong các trường hợp sau đây:

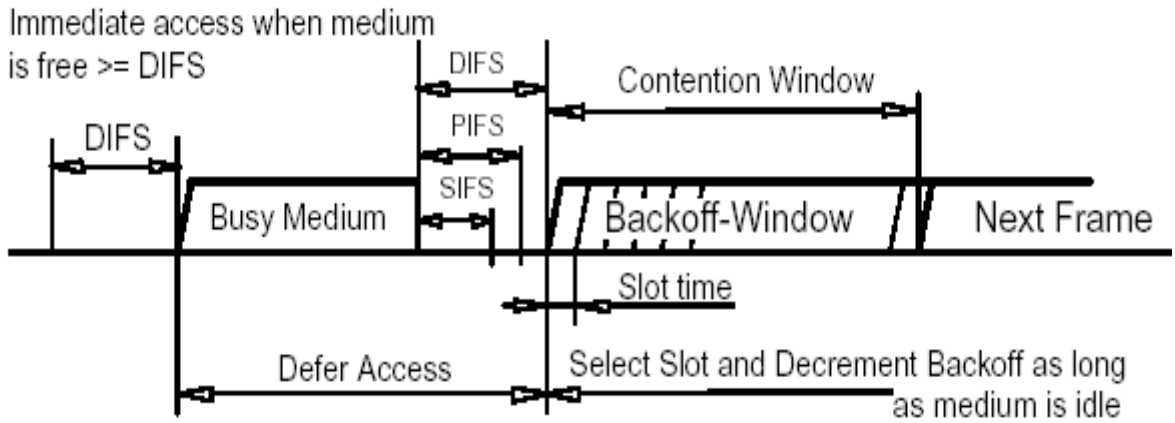
- Nếu khi trạm cảm biến môi trường trước truyền gói đầu tiên, và môi trường đang bận
- Sau mỗi lần truyền lại
- Sau một lần truyền thành công

Trường hợp duy nhất khi cơ chế này không được sử dụng là khi trạm quyết định truyền một gói mới và môi trường đã rãnh cho nhiều hơn DIFS.

Exponential backoff khiến các nút ***chịu khó*** chờ lâu hơn khi mức độ xung đột cao.

- bit time: thời gian truyền 1 bit.
- ***n*** là số lần xung đột khi truyền một frame nào đó.
- sau ***n*** lần xung đột, nút sẽ đợi 512 x ***K*** bit time rồi truyền lại; ***K*** được chọn ngẫu nhiên trong tập {0,1,2,…,2m – 1} với m:=min (n,10).

Hình sau biểu diễn sơ đồ cơ chế truy cập:



Hình 4.5. Sơ đồ cơ chế truy cập

3.3 Cách một trạm nối với một cell hiện hữu (BSS):

Khi một trạm muốn truy cập một BSS hiện hữu (hoặc sau chế độ bật nguồn, chế độ nghỉ, hoặc chỉ là đi vào vùng BSS), trạm cần có thông tin đồng bộ từ điểm truy cập (hoặc từ các trạm khác khi trong kiểu *Ad - hoc*).

Trạm nhận thông tin này theo một trong số hai cách sau:

1. Quét bị động: Trong trường hợp này trạm đợi để nhận một khung đèn hiệu (Beacon) từ AP, (khung đèn hiệu là một khung tuần hoàn chứa thông tin đồng bộ được gửi bởi AP), hoặc

2. Quét tích cực: Trong trường hợp này trạm cố gắng tìm một điểm truy cập bằng cách truyền các khung yêu cầu dò (Probe), và chờ đáp lại thông tin dò từ AP.

Hai phương pháp đều hợp lệ, và mỗi một phương pháp được chọn phải hài hoà giữa khả năng tiêu thụ điện và khả năng thực hiện.

3.3.1 Quá trình chứng thực

Mỗi khi trạm tìm thấy một điểm truy cập, nó sẽ quyết định nối các BSS, nó thực hiện thông qua quá trình chứng thực, đó là sự trao đổi thông tin lẫn nhau giữa AP và trạm, mà mỗi bên chứng minh sự nhận biết mật khẩu đã cho.

3.3.2 Quá trình liên kết

Khi trạm được xác nhận, sau đó nó sẽ khởi động quá trình liên kết, đây là sự trao đổi thông tin về các trạm và các BSS, và nó cho phép thực hiện DSS (tập hợp các AP để biết vị trí hiện thời của trạm). Chỉ sau khi quá trình liên kết được hoàn thành, thì một trạm mới có khả năng phát và nhận các khung dữ liệu.

3.4 Roaming:

Roaming là quá trình chuyển động từ cell này (hoặc BSS) đến cell khác với một kết nối chặt. Chức năng này tương tự như các điện thoại tế bào, nhưng có hai khác biệt chính:

- Trong một hệ thống mạng LAN dựa trên các gói, sự chuyển tiếp giữa các cell được thực hiện giữa các truyền dẫn gói, ngược với kỹ thuật điện thoại trong đó sự chuyển tiếp xuất hiện trong thời gian một cuộc nói chuyện điện thoại, điều này làm roaming mạng LAN dễ hơn một ít, nhưng
- Trong một hệ thống tiếng nói, một gián đoạn tạm thời không ảnh hưởng cuộc nói chuyện, trong khi trong một gói dựa vào môi trường, nó sẽ giảm đáng kể khả năng thực hiện vì sự chuyển tiếp được thực hiện bởi các giao thức lớp trên.

Chuẩn IEEE 802.11 không định nghĩa cách roaming được thực hiện, nhưng định nghĩa các công cụ cơ bản cho nó, điều này bao gồm sự quét tích cực/bị động, và một quá trình tái liên kết, trong đó một trạm roaming từ điểm truy cập này sang điểm truy cập khác sẽ được liên kết với một điểm truy cập mới.

3.5 Giữ đồng bộ:

Các trạm cần giữ đồng bộ, để giữ cho nhảy tần được đồng bộ, và các chức năng khác như tiết kiệm năng lượng. Trong một cơ sở hạ tầng BSS điều này được thực hiện bởi tất cả các trạm cập nhật các đồng hồ của chúng theo đồng hồ của AP, sử dụng cơ chế sau:

AP truyền các khung tuần hoàn gọi là các khung báo hiệu, các khung này chứa giá trị của đồng hồ AP tại thời điểm truyền (Chú ý rằng đây là thời điểm khi truyền dẫn thật sự xuất hiện, và không phải là thời điểm truyền khi nó được đặt vào hàng đợi để truyền, vì khung báo hiệu được truyền sử dụng các quy tắc CSMA, nên truyền dẫn trễ một cách đáng kể).

Các trạm thu kiểm tra giá trị đồng hồ của chúng ở thời điểm nhận, và sửa chữa nó để giữ đồng bộ với đồng hồ của AP, điều này ngăn ngừa sự trôi đồng hồ gây ra do mất đồng bộ sau vài giờ hoạt động.

3.6 Tiết kiệm năng lượng:

Mạng LAN không dây tiêu biểu liên quan đến các ứng dụng di động, và trong các kiểu ứng dụng này nguồn pin là một nguồn nhanh hết, đó là lý do tại sao chuẩn IEEE 802.11 trực tiếp hướng vào vấn đề tiết kiệm năng lượng và định nghĩa cả cơ chế để cho phép các trạm đi vào trong chế độ nghĩ ngơi cho các thời hạn dài mà không mất thông tin.

Ý tưởng chính đằng sau cơ chế tiết kiệm năng lượng là AP duy trì một bản ghi được cập nhật tại các trạm hiện thời đang làm việc trong chế độ tiết kiệm năng lượng, và nhớ đệm các gói được gửi tới các trạm này cho đến khi cả trạm yêu cầu

nhận các gói bằng cách gửi một yêu cầu kiểm tra tuần tự, hoặc cho đến khi chúng thay đổi thao tác của nó.

AP cũng truyền định kỳ (một phần của các khung báo hiệu) thông tin về trạm tiết kiệm năng lượng nào có các khung được nhớ đệm ở AP, như vậy các trạm này cần phải được đánh thức để nhận một trong số các khung báo hiệu đó, và nếu một chỉ báo cho biết có một khung được lưu trữ tại AP đợi để phân phát, thì trạm cần phải trong trạng thái hoạt động và gửi một thông báo kiểm tra tuần tự cho AP để có các khung này.

Quảng bá và Phát thanh được lưu trữ bởi AP, và được truyền ở một thời điểm được biết trước (mỗi DTIM), tại đó tất cả trạm tiết kiệm năng lượng muốn nhận kiểm khung này cần phải hoạt động.

3.7 Các kiểu khung:

Có ba kiểu khung chính:

- Khung dữ liệu: các khung được sử dụng để truyền dữ liệu
- Khung điều khiển: các khung được sử dụng điều khiển truy cập tới môi trường (ví dụ RTS, CTS, và ACK), và
- Khung quản lý: các khung được truyền giống như các khung dữ liệu để trao đổi thông tin quản lý, nhưng không hướng tới cho các lớp trên.

Mỗi kiểu được chia nhỏ ra thành các kiểu nhỏ hơn khác nhau, tùy theo chức năng của chúng.

3.8 Khuôn dạng khung:

Tất cả các khung chuẩn IEEE 802.11 đều có các thành phần sau đây:

Hình 4.6. Khuôn dạng khung chuẩn IEEE 802.11

3.8.1. Tiền tố (Preamble)

Nó phụ thuộc lớp vật lý, và bao gồm:

Synch: Một chuỗi 80 bit 0 và 1 xen kẽ, được sử dụng bởi bảo mật lớp vật lý để lựa chọn anten thích hợp (nếu tính sự phân tập được sử dụng), và ảnh hưởng tới việc sửa lỗi độ dịch tần số trạng thái vững đồng bộ với việc định thời gian gói nhận được.

SFD: Một bộ định ranh giới khung bắt đầu, nó gồm 16 bit nhị phân 0000 1100 1011 1101, được dùng để định nghĩa định thời khung.

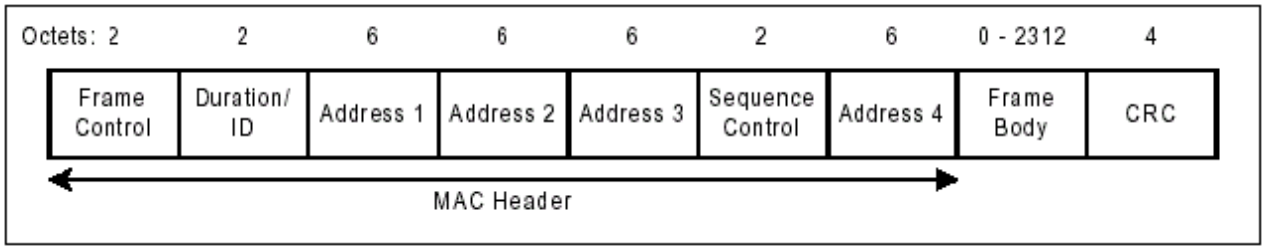
3.8.2 Đầu mục (Header) PLCP

Đầu mục PLCP luôn luôn được truyền ở tốc độ 1 Mbit/s và nó chứa thông tin Logic mà sẽ được sử dụng bởi lớp vật lý để giải mã khung, và gồm có:

- *Chiều dài từ PLCP_PDU*: biểu diễn số byte chứa trong gói, nó có ích cho lớp vật lý để phát hiện ra chính xác kết thúc gói,
- *Tường báo hiệu PLCP*: hiện thời, nó chỉ chứa đựng thông tin tốc độ, được mã hóa ở tốc độ 0.5 MBps, tăng dần từ 1Mbit/s tới 4.5 Mbit/s, và
- *Trường kiểm tra lỗi Đầu mục*: là trường phát hiện sai sót CRC 16 bit

3.8.3 Dữ liệu MAC

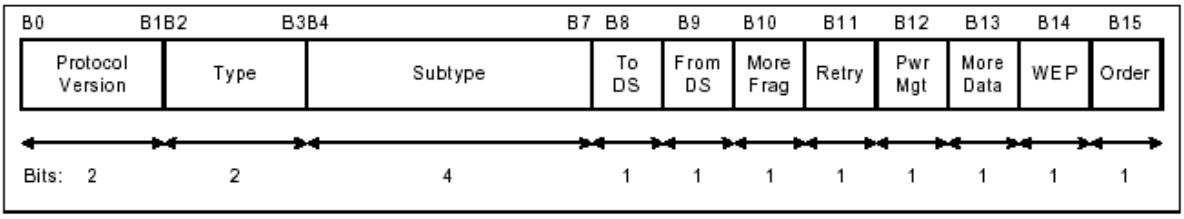
Hình sau cho thấy khuôn dạng khung MAC chung, các phần của trường trên các phần của các khung như mô tả sau đó.



Hình 4.7. Khuôn dạng khung MAC

3.8.3.1 Trường điều khiển khung (Frame Control)

Trường điều khiển khung chứa đựng thông tin sau:



a. Phiên bản giao thức (Protocol Verson)

Trường này gồm 2 bit có kích thước không đổi và xếp đặt theo các phiên bản sau của chuẩn IEEE 802.11, và sẽ được sử dụng để nhận biết các phiên bản tương lai có thể. Trong phiên bản hiện thời của chuẩn giá trị cố định là 0.

b. ToDS

Bit này là tập hợp các bit 1 khi khung được đánh địa chỉ tới AP để hướng nó tới hệ phân phối (gồm trường hợp mà trạm đích đặt lại khung giống với BSS, và AP). Bit là tập hợp các bit 0 trong tất cả các khung khác.

c. FromDS

Bit này là tập hợp các bit 1 khi khung đang đến từ hệ phân phối.

d. More Fragments

Bit này là tập hợp các bit 1 khi có nhiều đoạn hơn thuộc cùng khung theo sau đoạn hiện thời này.

e. Retry

Bit này cho biết đoạn này là một chuyển tiếp một đoạn trước đó được truyền, nó sẽ được sử dụng bởi trạm máy thu để đoán nhận bản sao được truyền của các khung mà xuất hiện khi một gói Chứng thực bị mất.

f. Power mangenment (Quản lý năng lượng)

Bit này cho biết kiểu quản lý năng lượng trong trạm sau khi truyền khung này. Nó được sử dụng bởi các trạm đang thay đổi trạng thái từ chế độ tiết kiệm năng lượng đến chế độ hoạt động hoặc ngược lại.

g. More Data (Nhiều Dữ liệu hơn)

Bit này cũng được sử dụng để quản lý năng lượng và nó được sử dụng bởi AP để cho biết rằng có nhiều khung được nhớ đệm hơn tới trạm này. Tạm quyết định sử dụng thông tin này để tiếp tục kiểm tra tuần tự hoặc kiểu đang thay đổi thậm chí để thay đổi sang chế độ hoạt động.

h. WEP

Bit này cho biết rằng thân khung được mã hóa theo giải thuật WEP

i. Order (Thứ tự)

Bit này cho biết rằng khung này đang được gửi sử dụng lớp dịch vụ Strictly - Order.

3.8.3.2 Khoảng thời gian/ID

Trường này có hai nghĩa phụ thuộc vào kiểu khung:

- Trong các bản tin Kiểm tra tuần tự tiết kiệm năng lượng, thì nó là ID trạm, và
- Trong tất cả các khung khác, nó là giá trị khoảng thời gian được dùng cho Tính toán NAV.

3.8.3.3 Các trường địa chỉ

Một khung chứa lên trên tới 4 địa chỉ phụ thuộc vào các bit ToDS và FromDS được định nghĩa trong trường điều khiển, như sau:

Địa chỉ - 1 luôn là địa chỉ nhận (ví dụ, trạm trên BSS mà nhận gói tức thời), nếu bit ToDS được lập thì đây là địa chỉ AP, nếu bit ToDS được xóa thì nó là địa chỉ trạm kết thúc.

Địa chỉ - 2 Luôn luôn là địa chỉ máy phát (ví dụ,. trạm đang truyền gói vật lý), nếu bit FromDS được lập thì đây là địa chỉ AP, nếu được xóa thì nó là địa chỉ trạm.

Địa chỉ - 3 Trong hầu hết các trường hợp còn lại, mất địa chỉ, trên một khung với bit FromDS được lập, sau đó Địa chỉ - 3 là địa chỉ nguồn gốc, nếu khung có bit ToDS lập, sau đó Địa chỉ - 3 là địa chỉ đích.

Địa chỉ - 4 được sử dụng trong trường hợp đặc biệt trong đó một hệ phân phối không dây được sử dụng, và khung đang được truyền từ điểm truy cập này sang điểm truy cập khác, trong trường hợp này cả các bit ToDS lẫn các bit FromDS được lập, vì vậy cả địa chỉ đích gốc và địa chỉ nguồn gốc đều bị mất.

Bảng sau tổng kết các cách dùng địa chỉ khác nhau theo cách thiết lập bit ToDS và bit FromDS:

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

3.8.3.4 Điều khiển nối tiếp

Trường điều khiển nối tiếp được dùng để biểu diễn thứ tự các đoạn khác nhau thuộc khung, và nhận biết các gói sao, nó gồm có hai trường con: trường Số đoạn, và trường Số nối tiếp, mà định nghĩa khung và số đoạn trong khung.

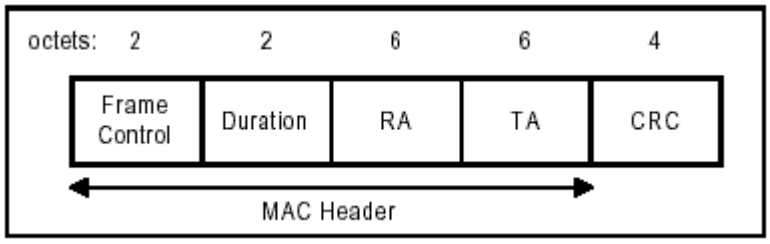
4.8.3.5 CRC

CRC là một trường 32 bit chứa một mã kiểm tra dư số chu kỳ 32 bit (CRC)

3.9 Các khung định dạng phổ biến nhất:

3.9.1 Khuôn dạng khung RTS

Khung RTS như sau:



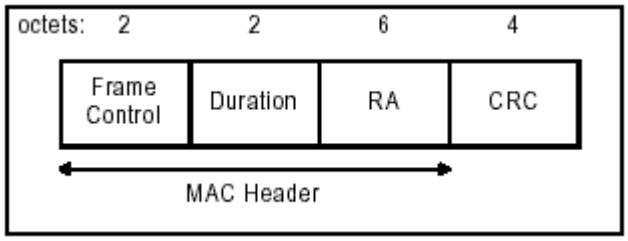
RA của khung RTS là địa chỉ STA, trong môi trường không dây, nó được dành để nhận dữ liệu tiếp theo hoặc khung quản lý một cách tức thời.

TA là địa chỉ của STA phát khung RTS.

Giá trị Khoảng thời gian là thời gian, tính theo micrô - giây, được yêu cầu để truyền dữ liệu liên tiếp hoặc khung quản lý, cộng với một khung CTS, cộng một khung ACK, cộng ba khoảng SIFS.

3.9.2 Khuôn dạng khung CTS

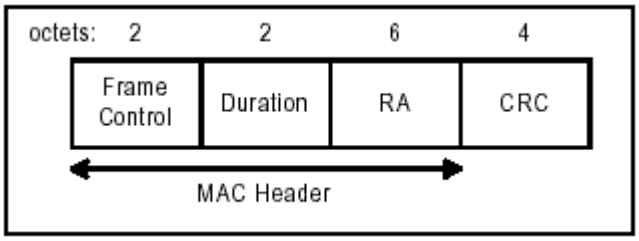
Khung CTS như sau:



Địa chỉ máy thu (RA) của khung CTS được copy từ trường địa chỉ máy phát (TA) của khung RTS ngay trước đó đến một đáp ứng CTS nào đó. Giá trị Khoảng thời gian là giá trị thu được từ trường Khoảng thời gian của khung RTS ngay trước đó, trừ thời gian (tính theo micrô - giây) được yêu cầu để phát khung CTS và khoảng SIFS.

3.9.3 Khuôn dạng khung ACK

Khung ACK như sau:



Địa chỉ Máy thu của khung ACK được sao chép từ trường Địa chỉ 2 của khung ngay trước đó. Nếu nhiều bit Đoạn hơn được xóa (0) trong trường điều khiển khung của khung trước đó, thì giá trị Khoảng thời gian là 0, nếu không thì giá trị Khoảng thời gian thu được từ trường Khoảng thời gian của khung trước đó, trừ đi thời gian (tính theo micrô - giây) được để phát khung ACK và khoảng SIFS của nó.

3.10 Hàm Phối hợp Điểm (PCF):

Bên cạnh Hàm Phối hợp Phân tán cơ bản, có một Hàm Phối hợp Điểm để chọn, mà sử dụng để thực hiện các dịch vụ biên - thời gian, như tiếng nói hoặc truyền video. Hàm Phối hợp Điểm làm cho điểm truy cập sử dụng quyền ưu tiên cao hơn bằng cách sử dụng một Không gian khung Inter (PIFS) nhỏ hơn.

Bằng cách sử dụng cao hơn này quyền ưu tiên truy cập, các vấn đề điểm truy cập kiểm tra tuần tự yêu cầu của các trạm để truyền dữ liệu, do đó điều khiển việc truy cập môi trường. Để cho phép cho các trạm bình thường khả năng vẫn còn truy

cập môi trường, có một chuẩn bị mà điểm truy cập phải để lại đủ thời gian cho Truy cập Phân tán trong giữa PCF

3.11 Các mạng Ad hoc:

Trong một số trường hợp các người dùng muốn lập một mạng LAN không dây mà không có một cơ sở hạ tầng (đặc biệt hơn không có một điểm truy cập), điều này bao gồm truyền file giữa hai người dùng máy notebook, cuộc họp giữa các cộng tác viên bên ngoài văn phòng, vân vân.

Chuẩn IEEE 802.11 giải quyết các nhu cầu này bằng cách định nghĩa một mô hình hoạt động "Ad hoc", trong trường hợp này không có điểm truy cập nào hoặc phần nào tính năng của nó được thực hiện bởi các trạm người dùng cuối (như tạo báo hiệu, đồng bộ, vân vân), và các chức năng khác không được hỗ trợ (như đặt lại giữa hai trạm không nằm trong phạm vi, hoặc tiết kiệm năng lượng).

3.12 Họ chuẩn IEEE 802.11:

3.12.1 Chuẩn IEEE 802.11a

Là một chỉ tiêu kỹ thuật IEEE cho mạng không dây hoạt động trong dải tần số 5 GHz (5.725 GHz tới 5.85 GHz) với tốc độ truyền dữ liệu cực đại 54 Mbps. Dải tần số 5 GHz không nhiều như tần số 2.4 GHz, vì chỉ tiêu kỹ thuật chuẩn IEEE 802.11 đề nghị nhiều kênh vô tuyến hơn so với chuẩn IEEE 802.11b. Sự bổ sung các kênh này giúp tránh giao thoa vô tuyến và vi ba.

3.12.2 Chuẩn IEEE 802.11b (Wifi)

Là chuẩn quốc tế cho mạng không dây hoạt động trong dải tần số 2.4 GHz (2.4 GHz tới 2.4835 GHz) và cung cấp một lưu lượng lên trên 11 Mbps. Đây là một tần số rất thường sử dụng. Các lò vi ba, các điện thoại không dây, thiết bị khoa học và y học, cũng như các thiết bị Bluetooth, tất cả làm việc bên trong dải tần số 2.4 GHz.

3.12.3 Chuẩn IEEE 802.11d

Chuẩn IEEE 802.11d là một chuẩn IEEE bổ sung lớp sự điều khiển truy cập (MAC) vào chuẩn IEEE 802.11 để đẩy mạnh khả năng sử dụng rộng mạng WLAN chuẩn IEEE 802.11. Nó sẽ cho phép các điểm truy cập truyền thông thông tin trên các kênh vô tuyến dùng được với các mức công suất chấp nhận được cho các thiết bị khách hàng. Các thiết bị sẽ tự động điều chỉnh dựa vào các yêu cầu địa lý.

Mục đích 11d là sẽ thêm các đặc tính và các hạn chế để cho phép mạng WLAN hoạt động theo các quy tắc của các nước này. Các nhà sản xuất Thiết bị không muốn để tạo ra một sự đa dạng rộng lớn của các sản phẩm và các người dùng chuyên biệt theo quốc gia mà người đi du lịch không muốn một túi đầy các card PC mạng WLAN chuyên biệt theo quốc gia. Hậu quả sẽ là các giải pháp phần sụn chuyên biệt theo quốc gia.

3.12.4 Chuẩn IEEE 802.11g

Tương tự tới chuẩn IEEE 802.11b, chuẩn lớp vật lý này cung cấp một lưu lượng lên tới 54 Mbps. Nó cũng hoạt động trong dải tần số 2.4 GHz nhưng sử dụng một công nghệ vô tuyến khác để tăng dải thông toàn bộ. Chuẩn này được phê chuẩn cuối năm 2003.

3.12.5 Chuẩn IEEE 802.11i

Đây là tên của nhóm làm việc IEEE dành cho chuẩn hóa bảo mật mạng WLAN. Bảo mật chuẩn IEEE 802.11i có một khung làm việc được dựa vào RSN (Cơ chế Bảo mật tăng cường). RSN gồm có hai phần:

1. Cơ chế riêng của dữ liệu và
2. Quản lý liên kết bảo mật.

Cơ chế riêng của dữ liệu hỗ trợ hai sơ đồ được đề xướng: TKIP và AES. TKIP (Sự toàn vẹn khóa thời gian) là một giải pháp ngắn hạn mà định nghĩa phần mềm vá cho WEP để cung cấp một mức riêng tư dữ liệu thích hợp tối thiểu. AES hoặc AES - OCB (Advanced Encryption Standard and Offset Codebook) là một sơ đồ riêng tư dữ liệu mạnh mẽ và là một giải pháp thời hạn lâu hơn.

Quản lý liên kết bảo mật được đánh địa chỉ bởi:

a) Các thủ tục đàm phán RSN,
b) Sự Chứng thực chuẩn IEEE 802.1x và
c) Quản lý khóa chuẩn IEEE 802.1x.

Các chuẩn đang được định nghĩa để cùng tồn tại một cách tự nhiên các mạng pre - RSN mà hiện thời được triển khai. Chuẩn này không kỳ vọng sẽ được thông qua cho đến khi kết thúc năm 2003.

3.12.6 Chuẩn IEEE 802.1x (Tbd)

Chuẩn IEEE 802.1x (Yêu cầu một nhà cung cấp dịch vụ RADIUS) cung cấp các doanh nghiệp & các nhà riêng một giải pháp chứng thực bảo mật, biến đổi được sử dụng kỹ thuật tái khóa (re - keying) động, sự chứng thực tên và mật khẩu người dùng và chứng thực lẫn nhau. Kỹ thuật tái khóa động, mà trong suốt với người dùng, loại trừ phân phối khóa không bảo mật và sự chi phốI thời gian và ngăn ngừa các tấn công liên quan đến các khóa WEP tĩnh. Sự chứng thực trên nền người dùng loại trừ các lỗ bảo mật xuất hiện từ thiết bị bị trộm hoặc mất khi sự chứng thực trên nền thiết bị được sử dụng, và sự chứng thực lẫn nhau giảm nhẹ tấn công dựa vào các điểm truy cập láu cá. Đồng thời, vì sự chứng thực chuẩn IEEE 802.1x thông qua một cơ sở dữ liệu RADIUS, nó cũng chia thang để dễ dàng điều khiển các số lượng người dùng mạng WLAN đang gia tăng.

CHƯƠNG IV

BẢO MẬT TRONG MẠNG WLAN

Chương này phác thảo các giao thức, các cơ chế bảo mật liên quan, và các kiến trúc của chuẩn IEEE 802.11 - mạng WLAN và thực hiện các khuyến nghị tới một thi hành được thực hiện dần của các mạng WLAN.

4.1 MỘT SỐ HÌNH THỨC TẤN CÔNG MẠNG:

Có thể tấn công mạng theo một trong các hình thức sau đây:

4.1.1 Dựa vào những lỗ hổng bảo mật trên mạng:

Những lỗ hổng này có thể các điểm yếu của dịch vụ mà hệ thống đó cung cấp, ví dụ những kẻ tấn công lợi dụng các điểm yếu trong các dịch vụ mail, ftp, web… để xâm nhập và phá hoại.

Các lỗ hổng này trên mạng là các yếu điểm quan trọng mà người dùng, hacker dựa đó để tấn công vào mạng. Các hiện tượng sinh ra trên mạng do các lỗ hổng này mang lại thường là : sự ngưng trệ của dịch vụ, cấp thêm quyền đối với các user hoặc cho phép truy nhập không hợp pháp vào hệ thống.

Hiện nay trên thế giới có nhiều cách phân loại khác nhau về lỗ hổng của hệ thống mạng. Dưới đây là cách phân loại sau đây được sử dụng phổ biến theo mức độ tác hại hệ thống, do Bộ quốc phòng Mỹ công bố năm 1994.

a. Các lỗ hổng loại C

Các lỗ hổng loại này cho phép thực hiện các phương thức tấn công theo DoS (Denial of Services - Từ chối dịch vụ). Mức độ nguy hiểm thấp, chỉ ảnh hưởng tới chất lượng dịch vụ, có thể làm ngưng trệ, gián đoạn hệ thống; không làm phá hỏng dữ liệu hoặc đạt được quyền truy nhập bất hợp pháp

DoS là hình thức tấn công sử dụng các giao thức ở tầng Internet trong bộ giao thức TCP/IP để làm hệ thống ngưng trệ dẫn đến tình trạng từ chối người sử dụng hợp pháp truy nhập hay sử dụng hệ thống. Một số lượng lớn các gói tin được gửi tới server trong khoảng thời gian liên tục làm cho hệ thống trở nên quá tải, kết quả là server đáp ứng chậm hoặc không thể đáp ứng các yêu cầu từ client gửi tới.

Một ví dụ điển hình của phương thức tấn công DoS là vào một số Web Site lớn làm ngưng trệ hoạt động của web site này: như www.google.com, www.ebay.com, www.yahoo.com v.v…

Tuy nhiên, mức độ nguy hiểm của các lỗ hổng loại này được xếp loại C; ít nguy hiểm vì chúng chỉ làm gián đoạn cung cấp dịch vụ của hệ thống trong một thời gian mà không làm nguy hại đến dữ liệu và những kẻ tấn công cũng không đạt được quyền truy nhập bất hợp pháp vào hệ thống.

b. Các lỗ hổng loại B

Các lỗ hổng cho phép người sử dụng có thêm các quyền trên hệ thống mà không cần thực hiện kiểm tra tính hợp lệ. Đối với dạng lỗ hổng này, mức độ nguy hiểm ở mức độ trung bình. Những lỗ hổng này thường có trong các ứng dụng trên hệ thống; có thể dẫn đến mất hoặc lộ thông tin yêu cầu bảo mật.

Các lỗ hổng loại B có mức độ nguy hiểm hơn lỗ hổng loại C, cho phép người sử dụng nội bộ có thể chiếm được quyền cao hơn hoặc truy nhập không hợp pháp.

Những lỗ hổng loại này thường xuất hiện trong các dịch vụ trên hệ thống. Người sử dụng cục bộ được hiểu là người đã có quyền truy nhập vào hệ thống với một số quyền hạn nhất định.

Một số lỗ hổng loại B thường xuất hiện trong các ứng dụng như lỗ hổng của trình SendMail trong hệ điều hành Unix, Linux... hay lỗi tràn bộ đệm trong các chương trình viết bằng C.

Những chương trình viết bằng C thường sử dụng một vùng đệm, là một vùng trong bộ nhớ sử dụng để lưu dữ liệu trước khi xử lý. Những người lập trình thường sử dụng vùng đệm trong bộ nhớ trước khi gán một khoảng không gian bộ nhớ cho từng khối dữ liệu. Ví dụ, người sử dụng viết chương trình nhập trường tên người sử dụng; qui định trường này dài 20 ký tự.

Do đó họ sẽ khai báo:

```
char first_name [20];
```

Với khai báo này, cho phép người sử dụng nhập vào tối đa 20 ký tự. Khi nhập dữ liệu, trước tiên dữ liệu được lưu ở vùng đệm; nếu người sử dụng nhập vào 35 ký tự; sẽ xảy ra hiện tượng tràn vùng đệm và kết quả 15 ký tự dư thừa sẽ nằm ở một vị trí không kiểm soát được trong bộ nhớ. Đối với những kẻ tấn công, có thể lợi dụng lỗ hổng này để nhập vào những ký tự đặc biệt, để thực thi một số lệnh đặc biệt trên hệ thống. Thông thường, lỗ hổng này thường được lợi dụng bởi những người sử dụng trên hệ thống để đạt được quyền root không hợp lệ.

Việc kiểm soát chặt chẽ cấu hình hệ thống và các chương trình sẽ hạn chế được các lỗ hổng loại B.

c. Các lỗ hổng loại A

Các lỗ hổng này cho phép người sử dụng ở ngoài có thể truy nhập vào hệ thống bất hợp pháp. Lỗ hổng này rất nguy hiểm, có thể làm phá hủy toàn bộ hệ thống.

Các lỗ hổng loại A có mức độ rất nguy hiểm; đe dọa tính toàn vẹn và bảo mật của hệ thống. Các lỗ hổng loại này thường xuất hiện ở những hệ thống quản trị yếu kém hoặc không kiểm soát được cấu hình mạng.

Những lỗ hổng loại này hết sức nguy hiểm vì nó đã tồn tại sẵn có trên phần mềm sử dụng; người quản trị nếu không hiểu sâu về dịch vụ và phần mềm sử dụng sẽ có thể bỏ qua những điểm yếu này.

Đối với những hệ thống cũ, thường xuyên phải kiểm tra các thông báo của các nhóm tin về bảo mật trên mạng để phát hiện những lỗ hổng loại này. Một loạt các chương trình phiên bản cũ thường sử dụng có những lỗ hổng loại A như: FTP, Gopher, Telnet, Sendmail, ARP, finger...

Ảnh hưởng của các lỗ hổng bảo mật trên mạng WLAN

Phần trên chúng ta đã phân tích một số trường hợp có những lỗ hổng bảo mật, những kẻ tấn công có thể lợi dụng những lỗ hổng này để tạo ra những lỗ hổng khác tạo thành một chuỗi mắt xích những lỗ hổng. Ví dụ, một kẻ phá hoại muốn xâm nhập vào hệ thống mà anh ta không có tài khoản truy nhập hợp lệ trên hệ thống đó. Trong trường hợp này, trước tiên kẻ phá hoại sẽ tìm ra các điểm yếu trên hệ thống, hoặc từ các chính sách bảo mật, hoặc sử dụng các công cụ dò xét thông tin (như SATAN, ISS) trên hệ thống đó để đạt được quyền truy nhập vào hệ thống. Sau khi mục tiêu thứ nhất đã đạt được; kẻ phá hoại có thể tiếp tục tìm hiểu các dịch vụ trên hệ thống, nắm bắt được các điểm yếu và thực hiện các hành động phá hoại tinh vi hơn.

Tuy nhiên, không phải bất kỳ lỗ hổng bảo mật nào cùng nguy hiểm đến hệ thống. Có rất nhiều thông báo liên quan đến lỗ hổng bảo mật trên mạng WLAN, hầu hết trong số đó là các lỗ hổng loại C, và không đặc biệt nguy hiểm đối với hệ thống. Ví dụ, khi những lỗ hổng về sendmail được thông báo trên mạng, không phải ngay lập tức ảnh hưởng trên toàn bộ hệ thống. Khi những thông báo về lỗ hổng được khẳng định chắc chắn, các nhóm tin sẽ đưa ra một số phương pháp để khắc phục hệ thống.

Dựa vào kẻ hở của các lỗ hổng này, kẻ xấu sẽ xây dựng các hình thức tấn công khác nhau nhằm không chế và nắm quyền kiểm soát trên mạng. Cho đến nay, các hacker đã nghĩ ra không biết bao nhiêu kiểu tấn công từ xa qua mạng khác nhau. Mỗi cuộc tấn công thường mở đầu bằng việc trực tiếp hoặc gián tiếp chui vào một hoặc nhiều máy tính đang nối mạng của người khác. Sau khi đã vào được hệ thống

mạng, hacker có thể đi đến các bước khác như xem trộm, lấy cắp, thay đổi và thậm chí phá huỷ dữ liệu hoặc làm treo các hoạt động của một hệ thống thông tin điện tử. Các hacker cũng có thể gài bẫy những người sử dụng thiếu cảnh giác hoặc đánh lừa những hệ thống thông tin kém phòng bị. Chẳng hạn, chúng sưu tầm các địa chỉ email và gửi thư kèm virus đến đó hoặc làm nghẽn tắc mạng bằng cách gửi thật nhiều các bức thư điện tử đến cùng một địa chỉ. Đôi khi các hacker xâm nhập vào một mạng máy tính nào mà nó phát hiện ra lỗi và để lại thông báo cho người quản trị mạng, tệ hơn nữa là chúng cài virus hoặc phần mềm nào đó để theo dõi và lấy đi những thông tin nội bộ. Dưới đây là một số kỹ thuật tấn công mạng chủ yếu đã được sử dụng nhiều trên thực tế.

4.1.2 Sử dụng các công cụ để phá hoại:

Ví dụ sử dụng các chương trình phá khóa mật khẩu để truy cập vào hệ thống bất hợp pháp;lan truyền virus trên hệ thống; cài đặt các đoạn mã bất hợp pháp vào một số chương trình.

Nhưng kẻ tấn công mạng cũng có thể kết hợp cả 2 hình thức trên với nhau để đạt được mục đích.

- Mức 1: Tấn công vào một số dịch vụ mạng : như Web, Email… dẫn đến các nguy cơ lộ các thông tin về cấu hình mạng. Các hình thức tấn công ở mức độ này có thể dùng Dó hoặc spam mail.

- Mức 2: Kẻ phá hoại dùng tài khản của người dùng hợp pháp để chiếm đoạt tài nguyên hệ thống (dựa vào các phương thức tấn công như bẻ khóa, đánh cắp mật khẩu…); kẻ phá hoại có thể thay đổi quyền truy cập hệ thống qua các lỗ hổng bảo mật hoặc đọc các thông tin trong tập tin liên quan đến truy nhập hệ thống như /etc/paswd

- Từ mức 3 đến mức 5: Kẻ phá hoại không sử dụng quyền của người dùng thông thường mà có thêm một số quyền cao hơn đối với hệ thống, như quyền kích hoạt một số dịch vụ, xem xét các thông tin khác trên hệ thống.

- Mức 6: Kẻ tấn công chiếm được quyền root trên hệ thống.

4.2 Cơ sở chuẩn IEEE 802.11:

Chuẩn IEEE 802.11 định nghĩa lớp vật lý (PHY) và lớp điều khiển truy cập môi trường (MAC) cho các mạng WLAN. Nó định nghĩa lớp vật lý hoạt động ở tốc độ dữ liệu 1Mbps và 2 Mbps trong băng tần RF 2.4 GHz và trong hồng ngoại (IR). Chuẩn IEEE 802.11 là một thành viên của họ chuẩn IEEE 802 được phát hành bởi IEEE mà gồm chuẩn IEEE 802.3 (Ethernet) và chuẩn IEEE 802.5 (Token Ring). Nó được mở rộng hai lần vào năm 1999 thành chuẩn IEEE 802.11a định nghĩa lớp vật

lý cho băng 5GHz ở tốc độ 54 Mbps, và chuẩn IEEE 802.11b định nghĩa lớp vật lý cho băng 2.4 GHz ở tốc độ 5.5 và 11 Mbps.

Mục đích của chuẩn IEEE 802.11 như IEEE định nghĩa là "để cung cấp kết nối không dây tới các thiết bị, hoặc các trạm tự động mà yêu cầu triển khai nhanh, và xách tay hoặc cầm tay, hoặc được gắn lên các phương tiện chuyển động bên trong một vùng".

4.2.1 Lớp vật lý

Chuẩn IEEE 802.11 quy định các lớp vật lý như bảng 2.1.

Bảng 3.1. So sánh các lớp vật lý của chuẩn IEEE 802.11.

Chuẩn	Tần số vô tuyến (RF)	Hồng ngoại (IR)	Cơ chế	Tốc độ dữ liệu cực đại (Mbps)
IEEE 802.11	2.4 GHz		DSSS	2
IEEE 802.11	2.4 GHz		FHSS	2
IEEE 802.11		850 - 950 nm	IR	2
IEEE 802.11a	5 GHz		OFDM	54
IEEE 802.11b	2.4 GHz		DSSS	11

Hệ thống trải phổ nhảy tần FHSS 2.4 GHz và hệ thống IR của chuẩn IEEE 802.11 ít khi được sử dụng. Lớp vật lý OFDM 5 GHz có phạm vi hạn chế (xấp xỉ 15m) nên nó ít được sử dụng. Đa số các sản phẩm hiện tại thực hiện công nghệ trải phổ chuỗi trực tiếp (DSSS) theo chuẩn IEEE 802.11b ở tốc độ dữ liệu lên trên tới 11 Mbps do lợi thế khả năng thực hiện và giá thành của nó.

Mục đích của công nghệ trải phổ là tăng thêm thông lượng và độ tin cậy của truyền dẫn bằng cách sử dụng nhiều dải tần. DSSS hoạt động bằng cách chuyển đổi mỗi bit truyền thành một chuỗi "chip" mà thực chất là một chuỗi số 1 và 0. Sau đó chip này được gửi song song qua một dải tần rộng. Vì sử dụng nhiều dải tần, nên nó tăng cường độ tin cậy truyền dẫn khi có giao thoa. Và mỗi bit được biểu diễn bởi một chuỗi chip, nên nếu phần nào đó của chuỗi chip bị mất vì giao thoa, thì gần như phần chip nhận được sẽ vẫn đủ để phân biệt bit gốc.

4.2.2 Điều khiển truy cập môi trường (MAC)

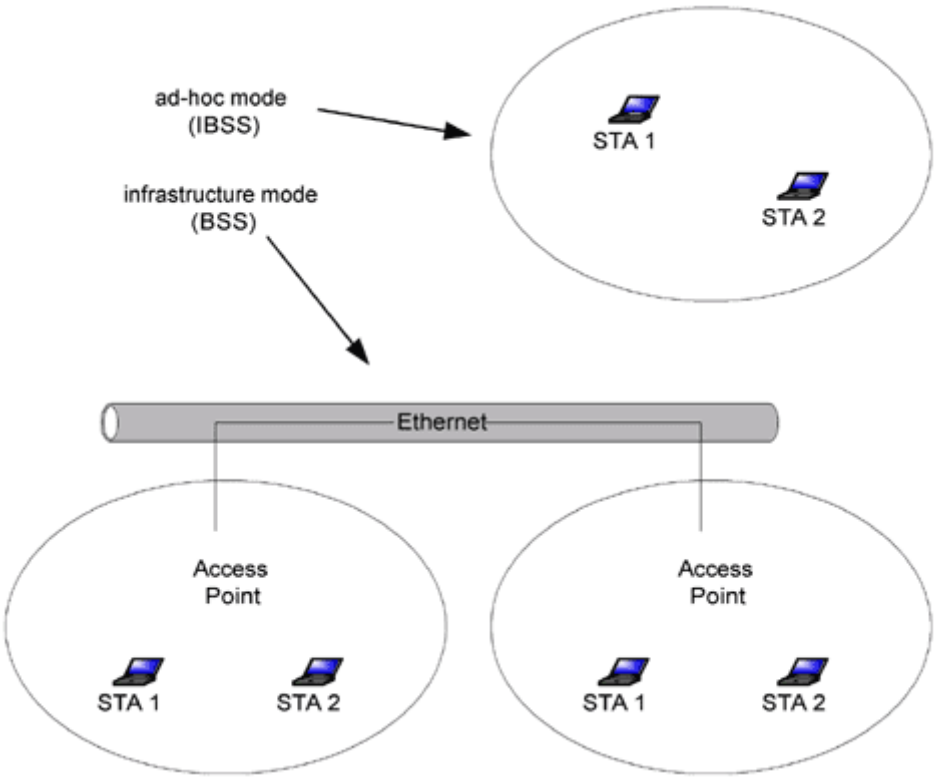
Trong khi lớp vật lý chuẩn IEEE 802.11 khác với chuẩn IEEE 802.3 Ethernet, thì chỉ tiêu kỹ thuật của MAC tương tự như chỉ tiêu kỹ thuật của MAC Ethernet chuẩn IEEE 802.3 cộng với Điều khiển liên kết Logic (LLC) chuẩn IEEE 802.2, nó làm cho không gian địa chỉ MAC chuẩn IEEE 802.11 thích hợp với không gian địa chỉ MAC của các giao thức IEEE 802. Trong khi MAC Ethernet chuẩn

IEEE 802.3 thực chất là CSMA/CD - đa truy cập nhạy sóng mang phát hiện xung đột, thì MAC chuẩn IEEE 802.11 là CSMA/CA - đa truy cập nhạy sóng mang tránh xung đột. Sự khác nhau này là do không có phương cách thiết thực để truyền và nhận cùng lúc trên môi trường không dây (môi trường WM). CSMA/CA cố gắng tránh các va chạm trên môi trường WM bằng cách đặt một khoảng thời gian thông tin trong mỗi khung MAC, để các trạm thu xác định thời gian còn lại của khung trên môi trường WM. Nếu khoảng thời gian của khung MAC trước đã hết và một kiểm tra nhanh trên môi trường WM chỉ ra rằng nó không bận, thì trạm truyền được phép truyền. Bằng cách này, nó cho phép nơi gửi truyền bất kỳ lúc nào mà môi trường không bận.

4.2.3 So sánh kiểu Cơ sở hạ tầng và kiểu Ad Hoc

Có hai phương pháp làm việc khác nhau cho thiết bị chuẩn IEEE 802.11: *Ad Hoc* (tập hợp các dịch vụ cơ bản độc lập, IBSS) và *Cơ sở hạ tầng* (tập hợp các dịch vụ được mở rộng, ESS). Một mạng *Ad Hoc* thông thường là một mạng tồn tại trong một thời gian hữu hạn giữa hai hoặc nhiều hơn hai thiết bị vô tuyến mà không được nối thông qua một điểm truy cập (AP) tới một mạng nối dây. Ví dụ, hai người dùng laptop muốn chia sẻ các file sẽ thiết lập một mạng *Ad Hoc* sử dụng các card NIC thích hợp chuẩn IEEE 802.11 và chia sẻ các file qua môi trường WM mà không cần phương tiện truyền thông ngoài nào (như đĩa mềm, các card flash).

Kiểu *Cơ sở hạ tầng* giả thiết có mặt một hoặc nhiều hơn các AP bắc cầu phương tiện truyền thông không dây với phương tiện nối dây truyền thông (hình 2.1). AP điều khiển việc chứng thực và liên kết trạm tới mạng không dây. Nhiều AP được nối bởi một hệ phân phối (DS) để mở rộng phạm vi của mạng không dây ra nhiều vùng lớn hơn. Trong các cài đặt tiêu biểu, DS đơn giản là cơ sở hạ tầng mạng IP hiện hữu. Với mục đích bảo mật, người ta thường sử dụng các mạng LAN ảo (VLAN) để tách riêng lưu thông mạng không dây với lưu thông mạng khác trên DS. Mặc dù chuẩn IEEE 802.11 cho phép các trạm vô tuyến liên kết chuyển mạch động từ điểm truy cập này đến điểm truy cập khác, nhưng nó không điều khiển cách trạm thực hiện. Kết quả là, các thi hành của nhà cung cấp khác nhau nói chung không tương tác với nhau trong ngữ cảnh này. Tại thời điểm hiện nay, khả năng thực hiện kiểu hoạt động này yêu cầu một giải pháp nhà cung cấp đơn.



Hình 4.1. So sánh kiểu Ad Hoc và kiểu cơ sở hạ tầng.

4.2.4 Liên kết và Chứng thực

Chuẩn IEEE 802.11 định nghĩa một trạm cuối là ánh xạ AP để các trạm khác trên mạng nối dây và mạng không dây có phương tiện để giao tiếp với trạm cuối. Ánh xạ này được gọi "liên kết". Trong khi các trạm cuối được phép liên kết động đến các AP khác, thì tại bất kỳ điểm cho trước một trạm cuối chỉ được liên kết đến một AP. Một trạm cuối "được liên kết" với một AP khá giống với một trạm cuối Ethernet được đặt vào trong cầu nối (bridge) của một switch. Không có cơ chế này, AP không có cách xác định để thúc đẩy các khung nhận được trên cổng Ethernet tới cổng không dây hay không.

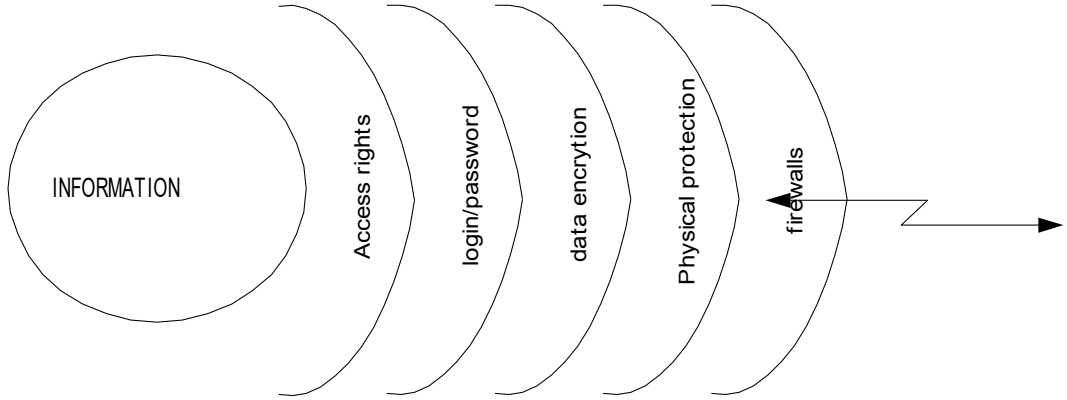
Liên kết là một quá trình ba trạng thái: (1) không được liên kết và không được xác thực; (2) không được liên kết nhưng được xác thực; (3) được liên kết và được xác thực.

Các bản tin đi qua trong thời gian thực hiện các bước này được gọi là các khung quản lý. Điều quan trọng trong quá trình này là liên kết sẽ không xảy ra cho đến khi chứng thực xảy ra. Sự chứng thực theo chuẩn IEEE 802.11 được nói kỹ trong phần 4.2.3.

4.3 CÁC MỨC BẢO VỆ AN TOÀN MẠNG:

Vì không có một giải pháp an toàn tuyệt đối nên người ta thường phải sử dụng nhiều mức bảo vệ khác nhau tạo thành nhiều lớp "rào chắn" đối với hoạt động xâm phạm. Việc bảo vệ thông tin trên mạng chủ yếu là bảo vệ thông tin cất giữ trong các

máy tính, đăc biệt là trong các server của mạng. Hình sau mô tả các lớp rào chắn thông dụng hiên nay để bảo vệ thông tin tại các trạm của mạng.



Hình 2 - Các mức độ bảo vệ mạng

Như hình minh họa trong hình trên, các lớp bảo vệ thông tin trên mạng gồm

- Lớp bảo vệ trong cùng là quyền truy nhập nhằm kiểm soát các tài nguyên (ở đây là thông tin) của mạng và quyền hạn (có thể thực hiện những thao tác gì) trên tài nguyên đó. Hiên nay việc kiểm soát ở mức này được áp dụng sâu nhất đối với tệp

- Lớp bảo vệ tiếp theo là hạn chế theo tài khoản truy nhập gồm đăng ký tên/ và mật khẩu tương ứng. Đây là phương pháp bảo vệ phổ biến nhất vì nó đơn giản, ít tốn kém và cũng rất có hiệu quả. Mỗi người sử dụng muốn truy nhập được vào mạng sử dụng các tài nguyên đều phải đăng ký tên và mật khẩu. Người quản trị hệ thống có trách nhiêm quản lý, kiểm soát mọi hoạt động của mạng và xác định quyền truy nhập của những người sử dụng khác tùy theo thời gian và không gian.

- Lớp thứ ba là sử dụng các phương pháp mã hóa (encrytion). Dữ liệu được biến đổi từ dạng " đọc được" sang dạng không " đọc được" theo một thuật toán nào đó. Chúng ta sẽ xem xét các phương thức và các thuật toán mã hóa được sủ dụng phổ biến ở phần dưới đây.
- Lớp thứ tư: là bảo vệ vật lý (physical protection) nhằm ngăn cản các truy nhập bất hợp pháp vào hệ thôngd. Thường dùng các biện pháp truyền thống như ngăn cấm người không có nhiệm vụ vào phòng đặt máy, dùng hệ thống khóa trên máy tính, cài đặt các hệ thống báo động khi có truy nhập vào hệ thống..
- Lớp thứ năm: Cài đặt các hệ thống tường lửa (firewall), nhằm ngăn chặn cá thâm nhập trái phép và cho phép lọc các gói tin mà ta không muốn gửi đi hoặc nhân vào vì một lý do nào đó.

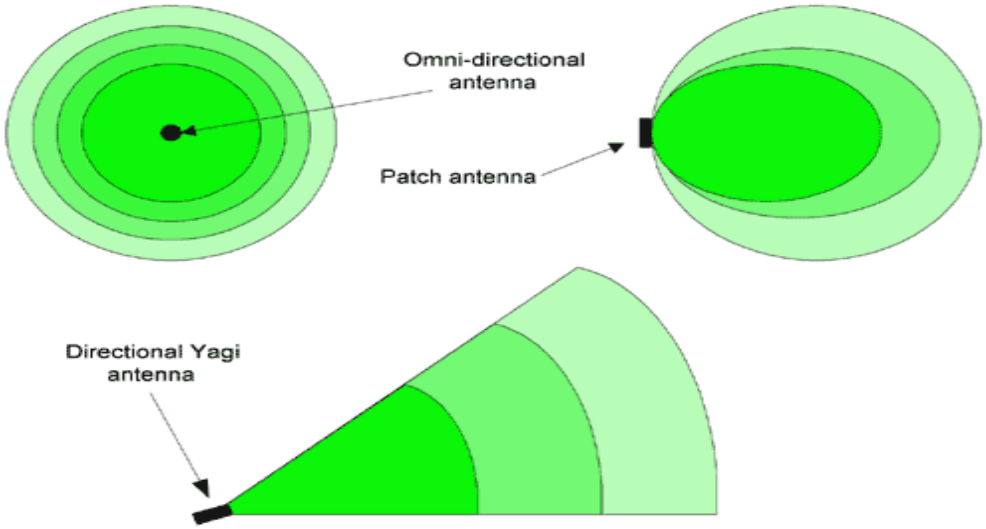
4.4 Cơ sở bảo mật mạng WLAN:

Chuẩn IEEE 802.11 có vài đặc tính bảo mật, như hệ thống mở và các kiểu chứng thực khóa dùng chung, định danh đặt dịch vụ (SSID), và giải thuật WEP. Mỗi đặc tính cung cấp các mức độ bảo mật khác nhau và chúng được giới thiệu trong phần này. Phần này cũng cung cấp thông tin về cách dùng anten RF để hạn chế lan lan truyền trong môi trường WM.

4.4.1 Giới hạn lan truyền RF

Trước khi thực hiện các biện pháp bảo mật, ta cần xét các vấn đề liên quan với lan truyền RF do các AP trong một mạng không dây. Khi chọn tốt, việc kết hợp máy phát và anten thích hợp là một công cụ bảo mật có hiệu quả để giới hạn truy cập tới mạng không dây trong vùng phủ sóng định trước. Khi chọn kém, sẽ mở rộng mạng ra ngoài vùng phỉ sóng định trước thành nhiều vùng phủ sóng hoặc hơn nữa.

Các anten có hai đặc tính chủ yếu: tính định hướng và độ khuếch đại. Các anten đa hướng có vùng phủ sóng 360 độ, trong khi các anten định hướng chỉ phủ sóng trong vùng hạn chế (hình 3.2). Độ khuếch đại anten được đo bằng dBi và được định nghĩa là sự tăng công suất mà một anten thêm vào tính hiệu RF.



Hình 4.2. Các mẫu lan truyền RF của các anten phổ biến.

4.4.2 Định danh thiết lập Dịch vụ (SSID)

Chuẩn IEEE 802.11b định nghĩa một cơ chế khác để giới hạn truy cập: SSID. SSID là tên mạng mà xác định vùng được phủ sóng bởi một hoặc nhiều AP. Trong kiểu sử dụng phổ biến, AP lan truyền định kỳ SSID của nó qua một đèn hiệu (beacon). Một trạm vô tuyến muốn liên kết đến AP phải nghe các lan truyền đó và chọn một AP để liên kết với SSID của nó.

Trong kiểu hoạt động khác, SSID được sử dụng như một biện pháp bảo mật bằng cách định cấu hình AP để không lan truyền SSID của nó. Trong kiểu này, trạm vô tuyến muốn liên kết đến AP phải sẵn có SSID đã định cấu hình giống với SSID

của AP. Nếu các SSID khác nhau, các khung quản lý từ trạm vô tuyến gửi đến AP sẽ bị loại bỏ vì chúng chứa SSID sai và liên kết sẽ không xảy ra.

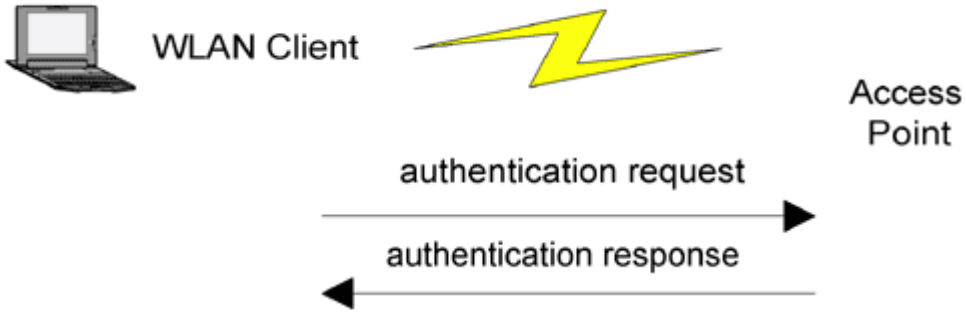
Vì các khung quản lý trên các mạng WLAN chuẩn IEEE 802.11 luôn luôn được gửi đến rõ ràng, nên kiểu hoạt động này không cung cấp mức bảo mật thích hợp. Một kẻ tấn công dễ dàng "nghe" các khung quản lý trên môi trường WM và khám phá SSID của AP.

4.4.3 Các kiểu Chứng thực

Trước khi một trạm cuối liên kết với một AP và truy cập tới mạng WLAN, nó phải thực hiện chứng thực. Hai kiểu chứng thực khách hàng được định nghĩa trong chuẩn IEEE 802.11: hệ thống mở và khóa chia sẻ.

4.4.3.1 Chứng thực hệ thống mở

Chứng thực hệ thống mở (hình 2.3) là một hình thức rất cơ bản của chứng thực, nó gồm một yêu cầu chứng thực đơn giản chứa ID trạm và một đáp lại chứng thực gồm thành công hoặc thất bại. Khi thành công, cả hai trạm được xem như được xác nhận với nhau.

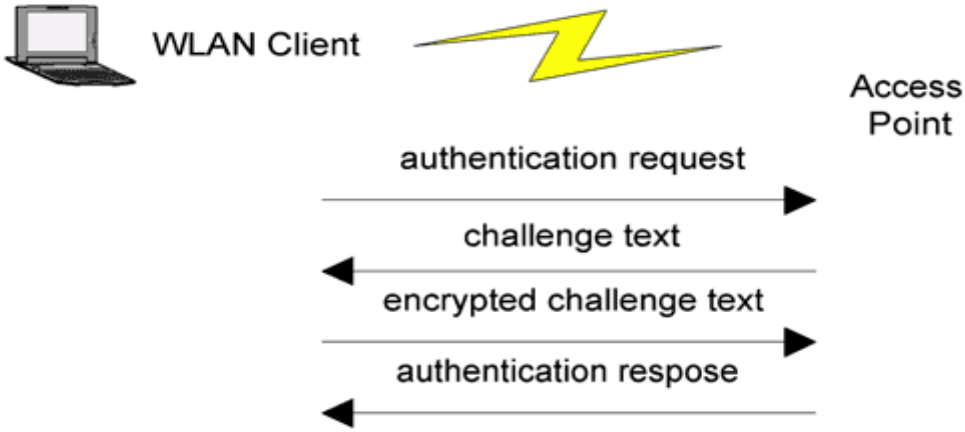


Hình 4.3. Chứng thực hệ thống mở.

4.4.3.2 Chứng thực khóa chia sẻ

Chứng thực khóa chia sẻ (hình 4.4) được xác nhận trên cơ sở cả hai trạm tham gia trong quá trình chứng thực có cùng khóa "chia sẻ". Ta giả thiết rằng khóa này đã được truyền tới cả hai trạm suốt kênh bảo mật nào đó trong môi trường WM. Trong các thi hành tiêu biểu, chứng thực này được thiết lập thủ công trên trạm khách hàng và AP. Các khung thứ nhất và thứ tư của chứng thực khóa chia sẻ tương tự như các khung có trong chứng thực hệ thống mở. Còn các khung thứ hai và khung thứ ba khác nhau, trạm xác nhận nhận một gói văn bản yêu cầu (được tạo ra khi sử dụng bộ tạo số giả ngẫu nhiên giải thuật WEP (PRNG)) từ AP, mật mã hóa nó sử dụng khóa chia sẻ, và gửi nó trở lại cho AP. Sau khi giải mã, nếu văn bản yêu cầu phù hợp, thì chứng thực một chiều thành công. Để chứng thực hai phía, quá trình trên được lặp lại ở phía đối diện. Cơ sở này làm cho hầu hết các tấn công vào mạng WLAN chuẩn IEEE 802.11b chỉ cần dựa vào việc bắt dạng mật mã hóa của một đáp ứng biết trước, nên dạng chứng thực này là một lựa chọn kém hiệu quả. Nó cho phép các hacker lấy thông tin để đánh đổ mật mã hóa WEP và đó cũng là lý do tại sao chứng thực khóa chia sẻ không bao giờ khuyến nghị.

Sử dụng chứng thực mở là một phương pháp bảo vệ dữ liệu tốt hơn, vì nó cho phép chứng thực mà không có khóa WEP đúng. Bảo mật giới hạn vẫn được duy trì vì trạm sẽ không thể phát hoặc nhận dữ liệu chính xác với một khóa WEP sai.



Hình 4.4. Chứng thực khóa chia sẻ.

4.4.4 WEP

WEP được thiết kế để bảo vệ người dùng mạng WLAN khỏi bị nghe trộm tình cờ và nó có các thuộc tính sau:

- **Mật mã hóa mạnh, đáng tin cậy**. Việc khôi phục khóa bí mật rất khó khăn. Khi độ dài khóa càng dài thì càng khó để khôi phục.
- **Tự đồng bộ hóa**. Không cần giải quyết mất các gói. Mỗi gói chứa đựng thông tin cần để giải mã nó.
- **Hiệu quả**. Nó được thực hiện đáng tin cậy trong phần mềm.

Giải thuật WEP thực chất là giải thuật giải mã hóa RC4 của Hiệp hội Bảo mật Dữ liệu RSA. Nó được xem như là một giải thuật đối xứng vì sử dụng cùng khóa cho mật mã hóa và giải mật mã UDP (Protocol Data Unit) văn bản gốc. Mỗi khi truyền, văn bản gốc XOR theo bit với một luồng khóa (*keystream*) giả ngẫu nhiên để tạo ra một văn bản được mật mã. Quá trình giãi mật mã ngược lại.

Giải thuật hoạt động như sau:

- Ta giả thiết rằng khóa bí mật đã được phân phối tới cả trạm phát lẫn trạm thu theo nghĩa bảo mật nào đó.
- Tại trạm phát, khóa bí mật 40 bit được móc nối với một Vectơ Khởi tạo (IV) 24 bit để tạo ra một *seed* (hạt giống) cho đầu vào bộ PRNG WEP.
- Seed được qua bộ PRNG để tạo ra một luồng khóa (*keystream*) là các octet giả ngẫu nhiên.
- Sau đó PDU văn bản gốc được XOR với keystream giả ngẫu nhiên để tạo ra PDU văn bản mật mã hóa.

- PDU văn bản mật mã hóa này sau đó được móc nối với IV và được truyền trên môi trường WM.
- Trạm thu đọc IV và móc nối nó với khóa bí mật, tạo ra seed mà nó chuyển cho bộ PRNG.
- Bộ PRNG của máy thu cần phải tạo ra keystream đồng nhất được sử dụng bởi trạm phát, như vậy khi nào được XOR với văn bản mật mã hóa, PDU văn bản gốc được tạo ra.

PDU văn bản gốc được bảo vệ bằng một mã CRC để ngăn ngừa can thiệp ngẫu nhiên vào văn bản mật mã đang vận chuyển. Không may là không có bất kỳ các quy tắc nào đối với cách sử dụng của IV, ngoại trừ nói rằng IV được thay đổi "thường xuyên như mỗi MPDU". Tuy nhiên, chỉ tiêu kỹ thuật đã khuyến khích các thực thi để xem xét các nguy hiểm do quản lý IV không hiệu quả.

4.4.5 *WPA (Wi-Fi Protected Access)*

Nhận thấy được những khó khăn khi nâng cấp lên 802.11i, Wi-Fi Alliance đã đưa ra giải pháp khác gọi là Wi-Fi Protected Access (WPA). Một trong những cải tiến quan trọng nhất của WPA là sử dụng hàm thay đổi khoá TKIP (*Temporal Key Integrity Protocol*). WPA cũng sử dụng thuật toán RC4 như WEP nhưng mã hoá đầy đủ 128 bit. Và 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. Không những thế, WPA còn bao gồm kiểm tra tính toàn vẹn của thông tin (Message Integrity Check). Vì vậy, dữ liệu không thể bị thay đổi trong khi đang ở trên đường truyền. Một trong những điểm hấp dẫn nhất của WPA là không yêu cầu nâng cấp phần cứng. Các nâng cấp miễn phí về phần mềm cho hầu hết các Card mạng và điểm truy cập sử dụng WPA rất dễ dàng và có sẵn. Tuy nhiên, WPA cũng không hỗ trợ các thiết bị cầm tay và máy quét mã vạch.

WPA có sẵn 2 lựa chọn: WPA Personal và WPA Enterprise. Cả 2 lựa chọn này đều sử dụng giao thức TKIP và sự khác biệt chỉ là 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. Trong khi Wi-Fi Alliance đã đưa ra WPA, và được coi là loại trừ mọi lỗ hổng dễ bị tấn công của WEP nhưng người sử dụng vẫn không thực sự tin tưởng vào WPA. Có một lỗ hổng trong WPA và lỗi này chỉ xảy ra với WPA Personal. Khi mà sử dụng hàm thay đổi khoá TKIP được sử dụng để tạo ra các khoá mã hoá bị phát hiện, nếu hacker có thể đoán được khoá khởi tạo hoặc một phần của mật khẩu, họ có thể xác định được toàn bộ mật khẩu, do đó có thể giải mã được dữ liệu. Tuy nhiên, lỗ hổng này cũng sẽ bị loại bỏ bằng cách sử dụng những khoá khởi tạo không dễ đoán. Điều này cũng có nghĩa rằng 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... WPA cũng thích hợp với những hoạt động hàng ngày và mang tính thử nghiệm công nghệ.

4.5 Trạng thái bảo mật mạng WLAN:

Chuẩn IEEE 802.11b đã hình thành dưới sự khuyến khích từ nhiều hướng. Có nhiều tài liệu của các nhà nghiên cứu khác nhau đã chỉ ra các lỗ hổng bảo mật quan trọng trong chuẩn. Họ chỉ ra rằng giải thuật WEP không hoàn toàn đủ để cung cấp tính riêng tư trên một mạng không dây. Họ khuyến nghị:

- Các lớp liên kết đề xuất không được bảo mật.
- Sử dụng các cơ chế bảo mật cao hơn như IPsec và SSH, thay cho WEP.
- Xem tất cả các hệ thống được nối qua chuẩn IEEE 802.11 như là phần ngoài. Đặt tất cả các điểm truy cập bên ngoài bức tường lửa.
- Giả thiết rằng bất cứ ai trong phạm vi vật lý đều có thể liên lạc trên mạng như một người dùng hợp lệ. Nhớ rằng một đối thủ cạnh tranh có thể dùng một anten tinh vi với nhiều vùng nhận sóng rộng hơn có thể được tìm thấy trên một card PC chuẩn IEEE 802.11 tiêu biểu.

4.6 Các ví dụ kiến trúc bảo mật mạng WLAN:

Các kiến trúc mạng WLAN sau đây có nghĩa khi ta nghiên cứu toàn bộ các cách tiếp cận có thể. Nó không hướng vào các vấn đề mật mã hóa lớp cao của dữ liệu trên mỗi gói trong môi trường WM, như một mạng riêng ảo (VPN). Trong tất cả các trường hợp, ta giả thiết rằng một giải pháp VPN được ưu tiên hơn so với các kiến trúc khác để tăng mức bảo mật. Biện pháp bảo mật được thảo luận dưới đây nhằm bảo vệ sự lưu thông mạng được truyền giữa các AP và radio khách hàng. Do đó, ta giả thiết rằng mạng nối dây hiện tại đã thật sự được bảo vệ bởi một biện pháp nào đó chấp nhận được.

SSID cung cấp rất ít mức bảo mật vì bản chất "văn bản sạch" của nó và do đó ta không quan tâm đến SSID khi thảo luận về các kiến trúc bảo mật.

Sau đây là một danh sách kiến trúc mạng WLAN và các tán thành cũng như các phản đối đối với chúng. Bảng 2.2 so sánh các đặc tính của các kiến trúc bảo mật mạng WLAN.

Chứng thực mở không có giải thuật WEP (hình 4.3)

Các tán thành: không có mào đầu quản lý; bất kỳ khách hàng nào cũng có thể liên kết đến AP mà không có bất kỳ cấu hình bổ sung nào.

Các chống đối: không có bảo mật nào khác ngoài địa chỉ MAC dựa vào kỹ thuật lọc.

Chứng thực mở có giải thuật WEP (hình 4.3)

Các tán thành : tính bảo mật đủ tốt để ngăn cản bất kỳ kẻ xâm phạm tình cờ nào; có mào đầu quản lý khá.

Các chống đối: các khóa giải thuật WEP bị thỏa hiệp.

Chứng thực khóa chia sẻ với giải thuật WEP (hình 4.4)

Các tán thành: tính bảo mật đủ tốt để ngăn cản bất kỳ các kẻ xâm nhập nào; có mào đầu quản lý khá.

Các chống đối: sử dụng một cơ chế yêu cầu/đáp ứng không bảo mật; các khóa giải thuật WEP bị thỏa hiệp.

Chứng thực mở LAWN/MOWER

LAWN/MOWER là một kiến trúc sử dụng các giao thức chung và phần mềm nguồn mở để tách người dùng trên mạng WLAN ra khỏi mạng cho đến khi họ được xác nhận bởi một hệ thống tính toán. Một khi được xác nhận, các quy tắc được thêm vào router nó cho phép khách hàng giao tiếp trong mạng nối dây. Như một biện pháp bảo mật bổ sung, địa chỉ MAC và IP của khách hàng được mã hóa chết cứng trong cache nhớ MOWER ARP.

Các tán thành: độc lập (chỉ Bộ trình duyệt có khả năng SSL được yêu cầu); dựa vào phần mềm nguồn mở sẵn có tự do; chứng thực khá mạnh mẽ (SSL và Kerberos 128 bit).

Các chống đối: không có truy cập ngoài mạng WLAN mà không có chứng thực.

Cổng Gateway Firewall không dây Ames của NASA (WFG)

WFG tương tự với LAWN/MOWER chỉ có điều cơ sở dữ liệu trên nền RADIUS thay vì trên nền Kerberos. WFG được thiết kế quanh một nền đơn có khả năng định tuyến, lọc gói, chứng thực, và DHCP. Nó hoạt động bằng cách gán các địa chỉ IP suốt DHCP, xác nhận các người dùng qua một trang Web được mật mã hóa SSL, cho phép truyền thông cho IP chứng thực thông qua cổng gateway, và đăng nhập (logging). Khi DHCP được giải phóng, được sử dụng lại, bị hết hiệu lực hoặc được thiết lập lại, WFG gở bỏ các firewall theo địa chỉ đó. Điều này đánh địa chỉ từng phần liên quan thông qua hijacking (bắt cóc) một IP đã chứng thực sau khi người dùng hợp pháp rời mạng.

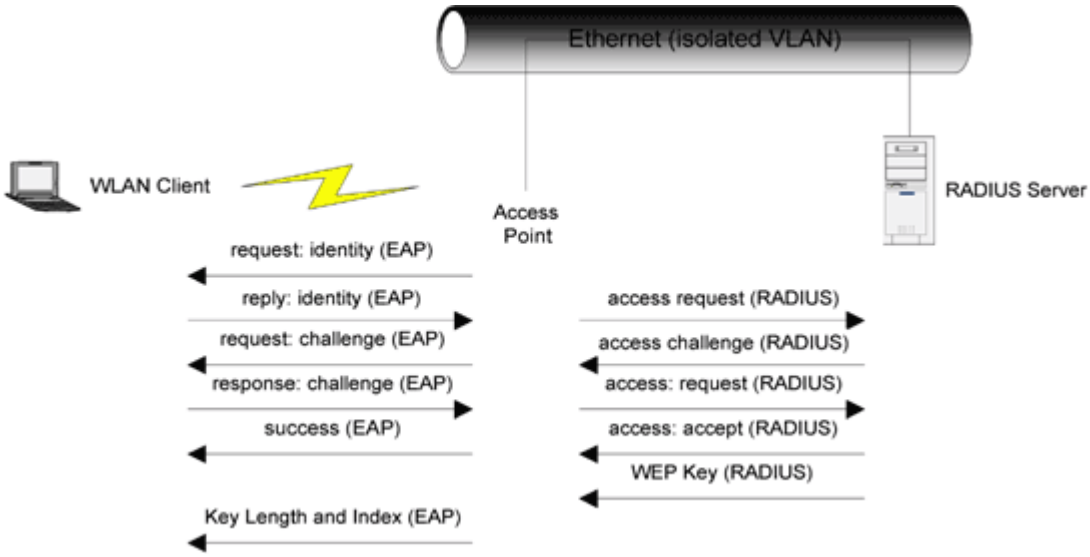
Các tán thành: độc lập nền; dựa vào phần mềm nguồn mở; quản trị username/password trung tâm.

Các chống đối: không truy cập bên ngoài mạng WLAN mà không có chứng thực.

Cisco LEAP/RADIUS (giải thuật WEP theo phiên + Chứng thực Mật khẩu) (hình 4.5)

Các tán thành: chứng thực username/password; quản trị username/password trung tâm; giải thuật WEP theo phiên có được từ bắt nguồn từ username/password.

Các chống đối: mặc dầu Cisco sở hữu nhưng nó dựa phần lớn vào các chuẩn AAA (ngoại trừ LEAP); phức tạp; khi sử dụng VPN với chi phí quản lý đáng kể; phần mềm khách hàng (các trình điều khiển, các phần sụn, các tiện ích) có còn lỗi.



Hình 4.5. Chứng thực LEAP/RADIUS Cisco.

Bảng 4.2. Các đặc tính của các kiến trúc bảo mật mạng WLAN.

Đặc tính	Chứng thực mở giải thuật w/WEP	LAWN/MOWER	WFG	LEAP/RADIUS
Mật mã hóa gói	X			X
Khóa WEP theo người dùng/theo phiên				X
Username/password		X	X	X
Logging (đăng nhập)	X	X	X	X
Độc lập nền	X	X	X	
Mào đầu quản lý thấp		X	X	
Nguồn mở	X			

4.7 Bảo mật:

Bảo mật là một trong các quan tâm hàng đầu của ai muốn triển khai một mạng LAN không dây, ủy ban chuẩn IEEE 802.11 đã hướng vào vấn đề này bằng cách cung cấp WEP (Wired Equivalent Privacy)

Quan tâm chính của người dùng là một kẻ quấy rày không có khả năng để:

- Truy cập các tài nguyên mạng bằng cách sử dụng thiết bị mạng LAN không dây tương tự, và
- Có thể chiếm được lưu thông mạng LAN không dây (nghe trộm)

4.7.1 Ngăn ngừa truy cập tới tài nguyên mạng

Nó được thực hiện bằng cách sử dụng một cơ chế chứng thực trong đó một trạm cần chứng minh sự nhận biết khóa hiện thời, nó tương tự như mạng LAN riêng nối dây, nó phát hiện kẻ xâm nhập (bằng cách sử dụng một khoá vật lý) để nối trạm làm việc của hắn tới mạng LAN nối dây.

4.7.2 Nghe trộm

Việc nghe trộm được ngăn ngừa bằng cách sử dụng giải thuật WEP, nó là một Bộ tạo số giả ngẫu nhiên (PRNG) được khởi tạo bởi một khoá bí mật dùng chung. PRNG này tạo ra một chuỗi khóa các bit giả ngẫu nhiên có chiều dài bằng với chiều dài của gói lớn nhất mà được kết hợp với gói đến/đi đang tạo ra gói được truyền trong không gian.

Giải thuật WEP là một giải thuật đơn giản được dựa vào giải thuật RC4 của RSA, nó có các thuộc tính sau:

- Độ tin cậy mạnh mẽ: các tấn công mạnh mẽ tới giải thuật này khó thực hiện bởi vì mỗi khung được gửi với một vector khởi tạo (IV) để bắt đầu lại PRNG cho mỗi khung.
- Tự đồng bộ: Giải thuật đồng bộ dựa vào mỗi bản tin, nó được cần để làm việc trong một môi trường không kết nối, tại đó các gói bị mất (như bất kỳ mạng LAN nào).

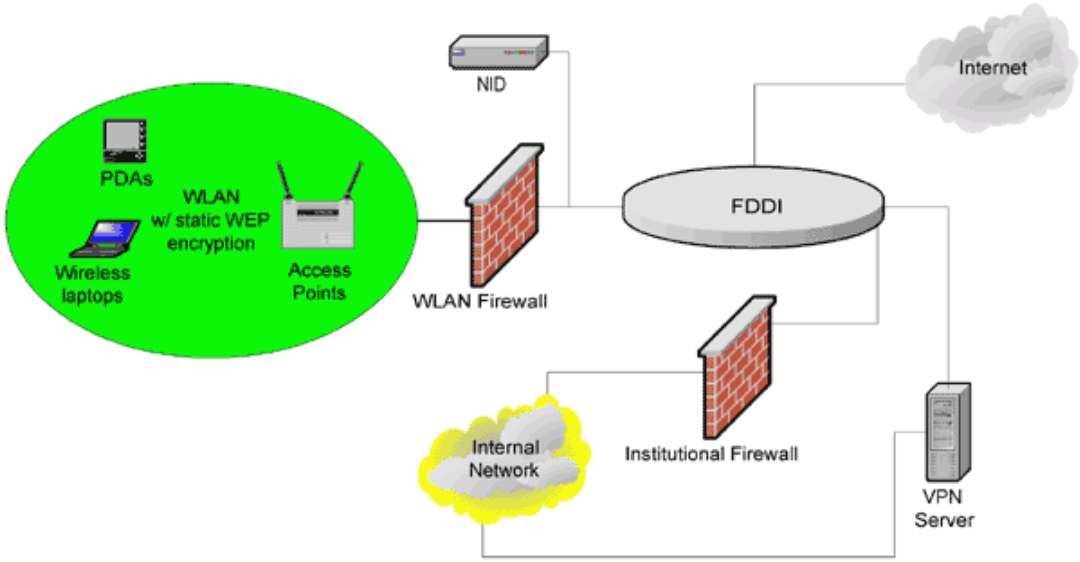
4.8 Kiến trúc khuyến nghị:

Phần này đề xướng một kiến trúc mạng WLAN dựa vào các nguyên lý sau đây:

- Mạng không dây được xem xét như một mạng không bảo mật cố hữu. Như vậy, nó cần phải có firewall bên ngoài.
- Sự mật mã hóa theo giải thuật WEP dễ bị bẻ gãy với các giải thuật thông thường, không tin cậy để bảo mật dữ liệu.
- WEP cung cấp ít nhất một số bảo vệ khỏi xâm nhập và nó nên được sử dụng nếu có chi phí quản lý thấp.
- Khi yêu cầu mật mã hóa dữ liệu mạnh, cần sử dụng giải pháp VPN/IPsec
- Vì truy cập tới mạng không dây khó điều khiển hơn so với các truy cập tới mạng nối dây, nên cần thực hiện bảo dưỡng khi cung cấp truy cập từ mạng

WLAN đến các mạng khác (thậm chí là mạng Internet) mà không có chứng thực trước.

Kiến trúc tổng quan



Hình 4.6. Kiến trúc mạng WLAN được đề xướng.

Kiến trúc được đề xướng (hình 4.6) có thể thay thế mạng không dây bên ngoài firewall. Ngoài ra, nó sử dụng các khóa WEP tĩnh trong mạng WLAN để có chi phí quản lý thấp và cung cấp một phương tiện Dò tìm Xâm nhập Mạng (NID) để theo dõi các cuộc tấn công bắt nguồn từ mạng WLAN đến mạng Internet và các mạng khác.

Người ta khuyến nghị rằng phạm vi địa chỉ IP và tên miền của mạng không dây đều liên kết với mạng nội bộ hiện hữu bất kỳ. Điều này sẽ cho phép tách các lưu thông không dây tốt hơn và giúp nhận diện và lọc lưu thông tới/ra khỏi mạng này.

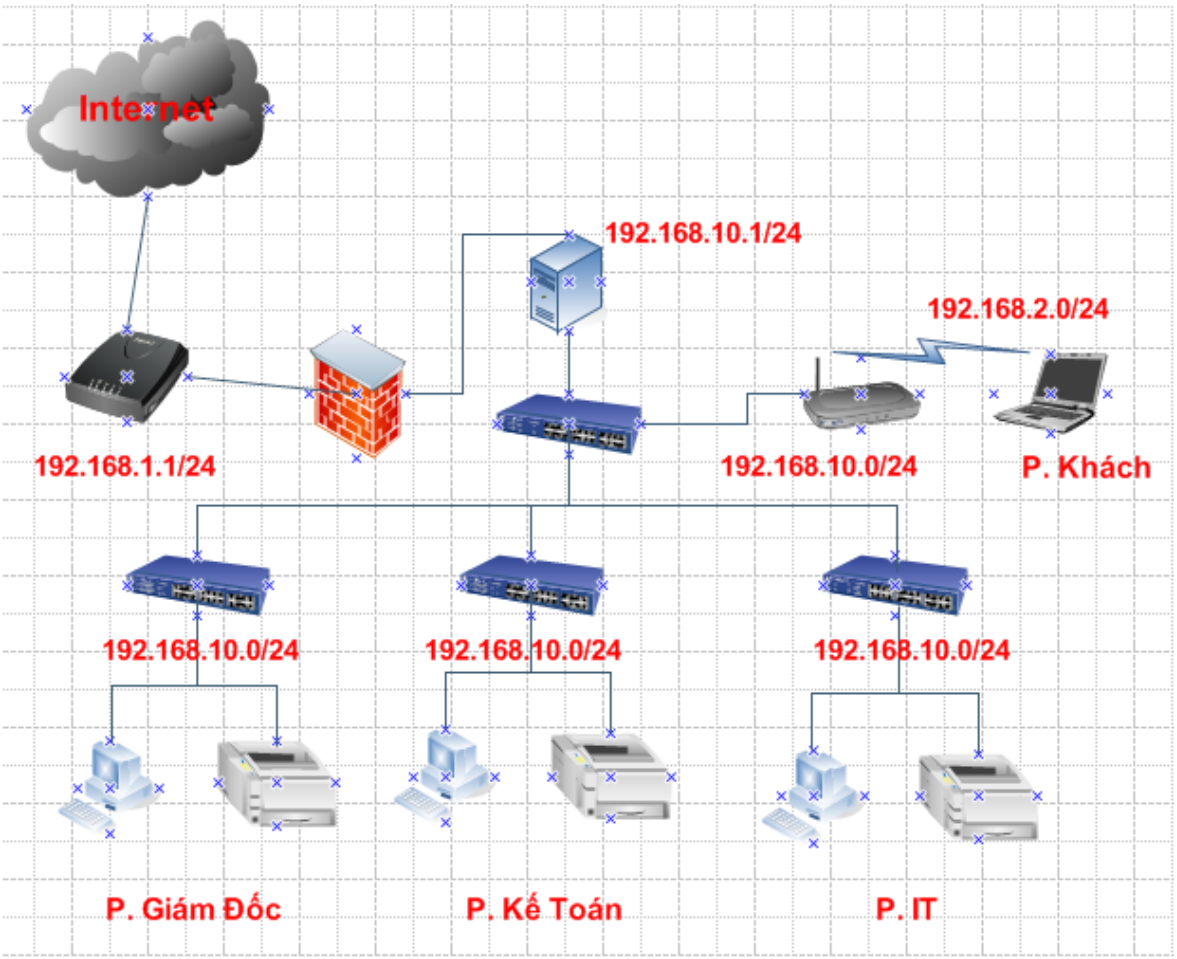
Kiến trúc được đề xướng hợp nhất hầu hết các nguyên lý thiết kế ban đầu trong khi cho phép một vài mức truy cập tới mạng Internet từ mạng không - VPN, từ người dùng không được xác thực. Giả sử lan truyền RF giới hạn trong vùng khảo sát và thiết lập công suất anten và máy phát thích hợp, mạng WLAN không biểu hiện bất kỳ dấu hiệu quan trọng nào đe dọa đến mạng nội bộ như mạng Internet.

Vì roaming giữa các AP vẫn nằm trong miền sở hữu, người ta khuyến cáo cao rằng tất cả AP phải được mua từ cùng nhà cung cấp. Điều này sẽ bảo đảm một trạm cuối được trang bị với bất kỳ card NIC tương thích chuẩn IEEE 802.11 sẽ roam giữa các AP. Ngoài ra, bất kỳ cải tiến bảo mật chuyên biệt mới nào được giới thiệu yêu cầu các AP đồng nhất.

CHƯƠNG V

THIẾT KẾ MÔ HÌNH MẠNG

5.1 MÔ HÌNH MẠNG:



Hình 5.1: Mô hình mạng Domain

Mô hình mạng của công ty gồm có:

- Một máy Domain để quản lý công ty gồm các dịch vụ: DHCP, DNS, ISA với địa chỉ IP là 192.168.10.1/24 .
- Các máy client dành cho nhân viên của công ty có địa chỉ IP random do dịch vụ DHCP cấp phát từ 192.168.10.10 => 192.168.10.100/24.

5.2. CẤU HÌNH PHẦN CỨNG:

5.2.1 Máy Server:

Máy Server dùng để quản lý và cung cấp các dịch vụ cho máy Client.

MAINBOARD : ASUS P5QL-E .

CPU: INTEL Core 2 Quad- Q6600(2.4 Ghz) 8M cache Bus 1066 .

RAM : 4GB DDR2 bus 800 KINGMAX.
HDD: 250GB SEAGATE Sata2.
CASE: CASE COOLER MASTER (không nguồn có 1 quạt 12 cm, nguyên liệu nhôm và thép cao cấp).
Power Supply: POWER COOLER MASTER 460W.
MONITOR: 16" AOC 1619SW.
CD ROM: DVD-18X ASUS (Sata).

5.2.2 Máy Client:

Máy Client được coi như là người sử dụng các dịch vụ trên mạng do một hoặc nhiều máy chủ (server) cung cấp.

MAINBOARD: ASUS P5N73-AM.

CPU: INTEL Duo Core-E5200(2.5Ghz) 2M cache Bus 800.

RAM : 1GB DDR2 bus 800 KINGMAX.

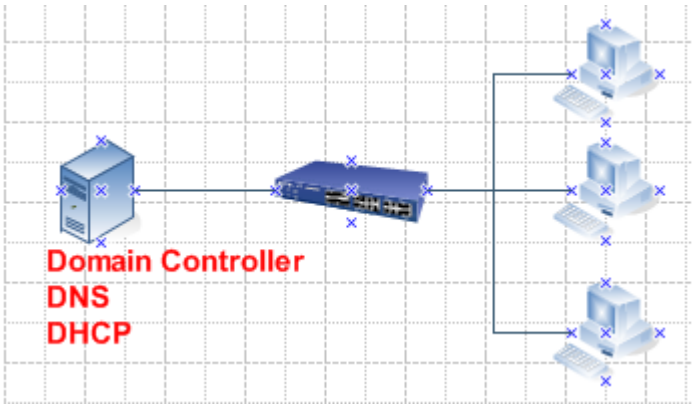
HDD: 250GB SEAGATE Sata2.

CASE : PATRIOT 450W (2 quạt 8cm).

Monitor : 17" Acer AL1716WAB.

CD ROM: DVD-18X ASUS (Sata).

5.3 CẤU HÌNH DOMAIN CONTROLLER:



Hình 5.2: Mô hình Domain-Client.

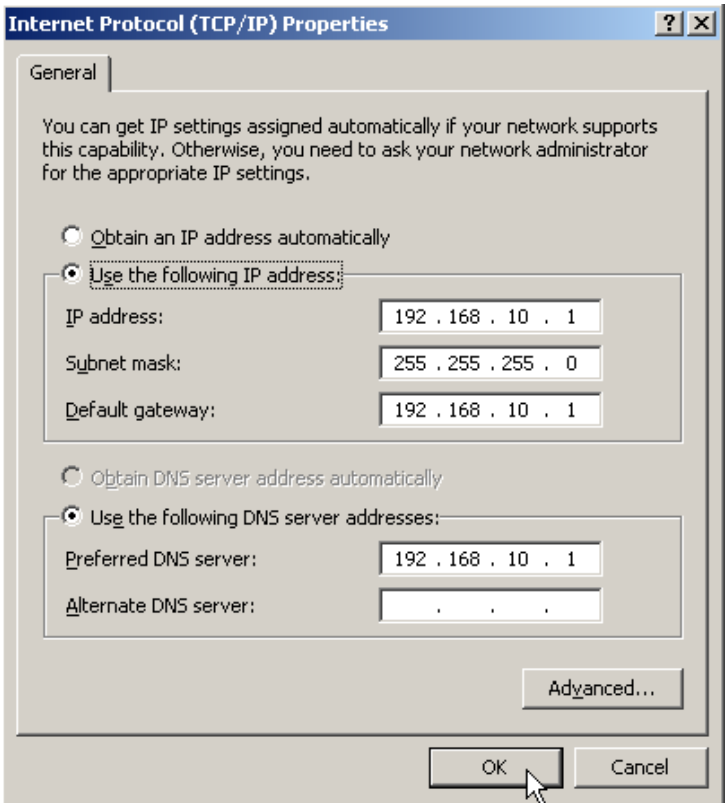
Trong mạng, bất kỳ máy trạm nào đang chạy hệ điều hành Windows XP cũng có một nhóm tài khoản người dùng tạo sẵn nào đó. Nếu máy trạm có chức năng như một hệ thống độc lập hoặc là một phần của mạng ngang hàng thì tài khoản người dùng mức máy trạm (được gọi là tài khoản người dùng cục bộ) không thể điều khiển truy cập tài nguyên mạng. Một lý do khác nữa là chẳng hạn, nếu máy tính của một người dùng bị phá hoại, người đó không thể đăng nhập vào máy tính khác để làm việc vì tài khoản họ tạo chỉ có tác dụng trên máy cũ. Nếu muốn làm được việc anh ta sẽ phải tạo tài khoản mới trên máy khác.

Domain có nhiệm vụ giải quyết các vấn đề vừa nêu và một số vấn đề khác nữa. Chúng sẽ tập trung hoá tài khoản người dùng (hay cấu hình khác, các đối tượng liên quan đến bảo mật...). Điều này giúp việc quản trị dễ dàng hơn và cho phép người dùng đăng nhập từ bất kỳ máy tính nào có trên mạng (trừ khi bạn giới hạn quyền truy cập người dùng).

5.3.1 CẤU HÌNH PHÍA SERVER (TẠO DOMAIN TÊN LÀ HungMy.com)

Trước khi cài đặt Domain Controller, ta phải tiến hành thiết lập địa chỉ IP cho DNS SERVER (vì khi Domain được cài đặt thì nó yêu cầu địa chỉ DNS để tham chiếu trong quá trình cấu hình).

- Vào **Control Panel** chọn **Network Connections**, nhấp phải chuột vào **Local Area Connection** => **Properties** =>**Internet Protocol(TCP/IP)** chọn **Properties.** Cửa sổ Internet Protocol (TCP/IP) Properties xuất hiện. Cửa sổ này có chức năng để người dùng thiết lập địa chỉ IP cho máy cũng như thiết lập địa chỉ IP cho DNS Server.



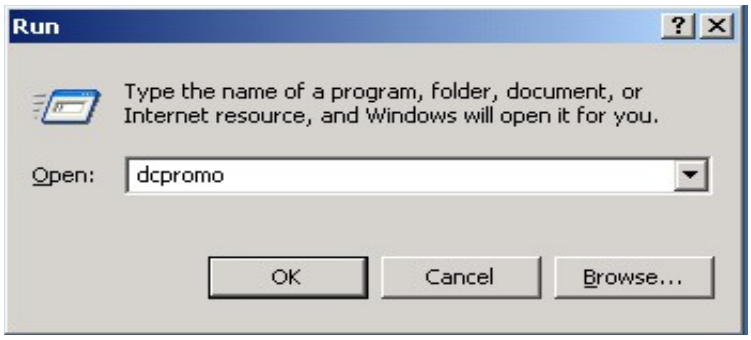
Hình 5.3: Internet Protocol (TCP/IP) Properties.

- Nhấp chọn vào mục **Use the Following IP Address**. Tiếp theo nhập địa chỉ IP trong mục **IP Addrress** là 192.168.10.1, **Subnet Mask** được đặt tự động. Sau đó nhấp chọn vào mục **Use the Following DNS Server Addresses** và nhập địa chỉ IP cho DNS Server trong mục **Preferred DNS Server**. Nhấp **OK** để kết thúc.

Chú ý : Địa chỉ IP của DNS Server phải trùng với địa chỉ IP của Server.

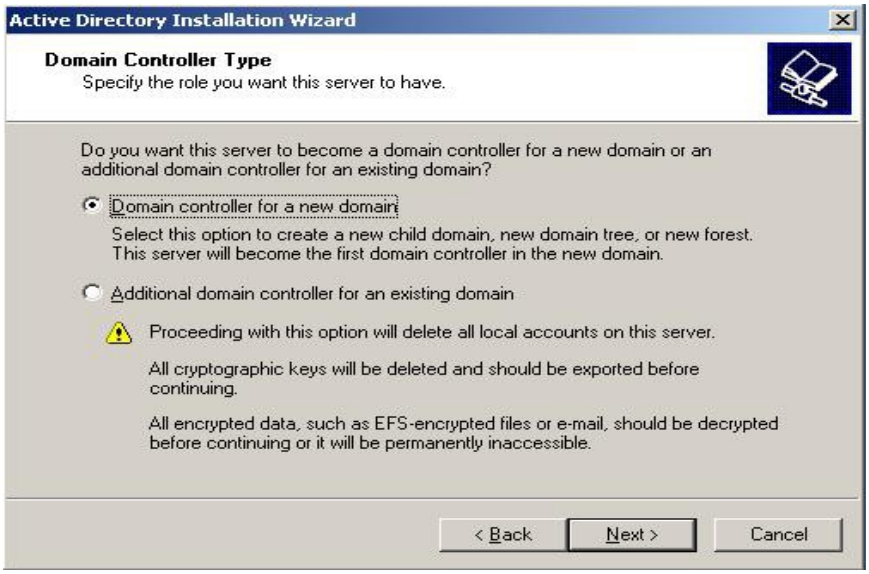
5.3.2 CẤU HÌNH DOMAIN CONTROLLER

- Vào **Start** -> **Run** -> gõ **dcpromo** -> **OK**.



Hình 5.4: Nhập lệnh dcpromo trong Run.

- Cửa sổ **Active Directory Install Wizard** xuất hiện. Nhấp **Next** hai lần để tiếp tục.

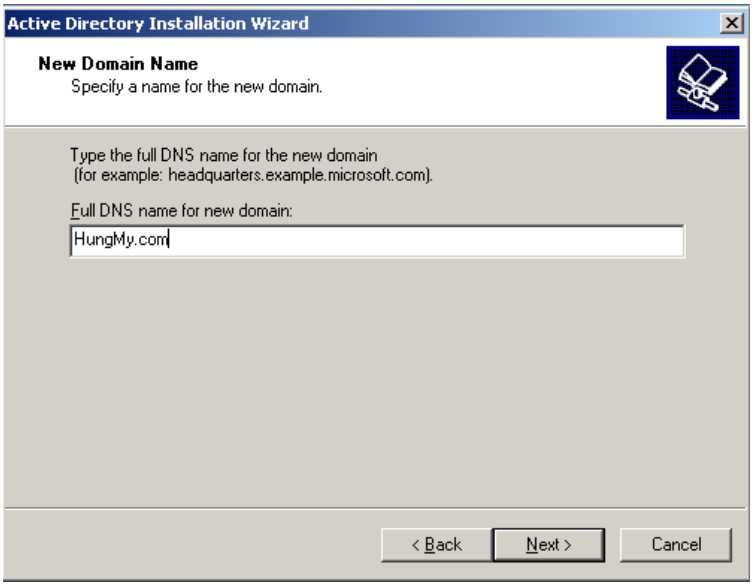


Hình 5.5: Domain Controller Type

- Với cửa sổ Active Directory Install Wizard, nhấp chọn vào **Domain Controller for a new domain** để tạo một Domain mới rồi nhấp **Next** để tiếp tục.

Hình 5.6: Create New Domain.

- Nhấp chọn vào mục **Domain in a new forest**, sau đó nhấp **Next** để tiếp tục.

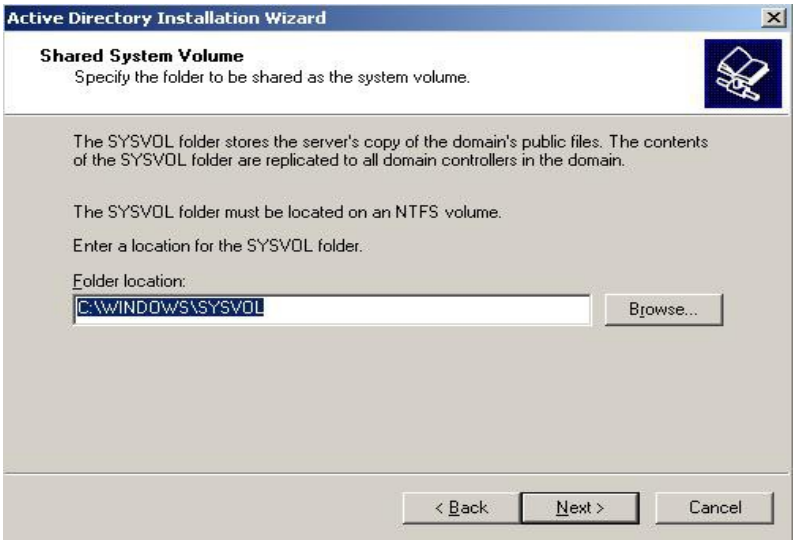


Hình 5.7: New Domain name.

- Nhập tên Domain là HungMy.com vào mục **Full DNS name for new domain**, sau đó Nhấp **Next** để tiếp tục.

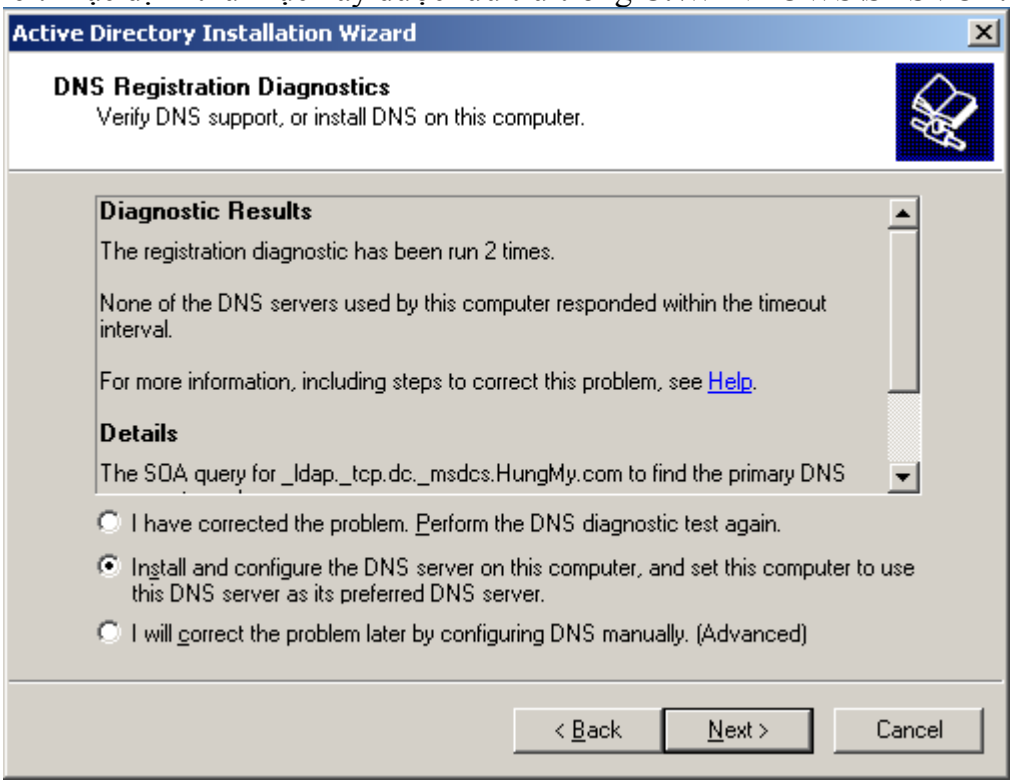
Hình 5.8: Database and Log Folder.

- Định nơi lưu trữ cơ sở dữ liệu của Active Directory và thư mục chứa File Log, sau đó nhấp **Next** để tiếp tục. Mặc định thì thư mục cơ sở dữ liệu và File Log được lưu trữ trong C:\WINDOWS\NTDS.



Hình 5.9: Share System Volume.

- Định nơi lưu trữ thư mục SYSVOL rồi nhấp **Next** để tiếp tục.Thư mục SYSVOL lưu trữ tất cả các tập tin mà Server muốn chia sẻ với các Clients trong Domain Controller. Mặc định thư mục này được lưu trữ trong C:\WINDOWS\SYSVOL.

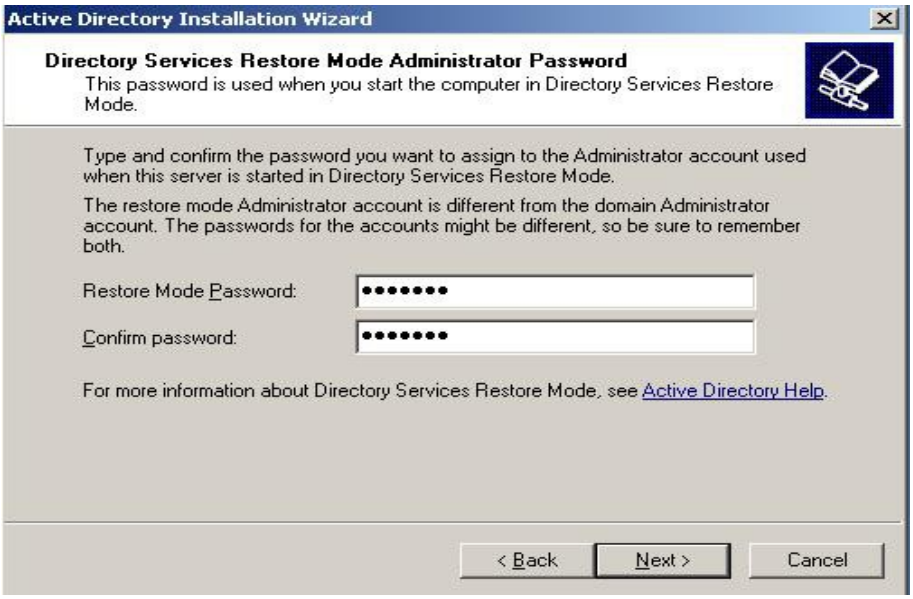


Hình 5.10: DNS Registration Diagnotics.

- Nhấp chọn vào **Install and configure the DNS server on this computer and set this computer to use this DNS server as its preferred DNS server**, sau đó nhấp **Next** để tiếp tục. Cửa sổ này cho phép bạn cài đặt, cấu hình và sử dụng DNS server.

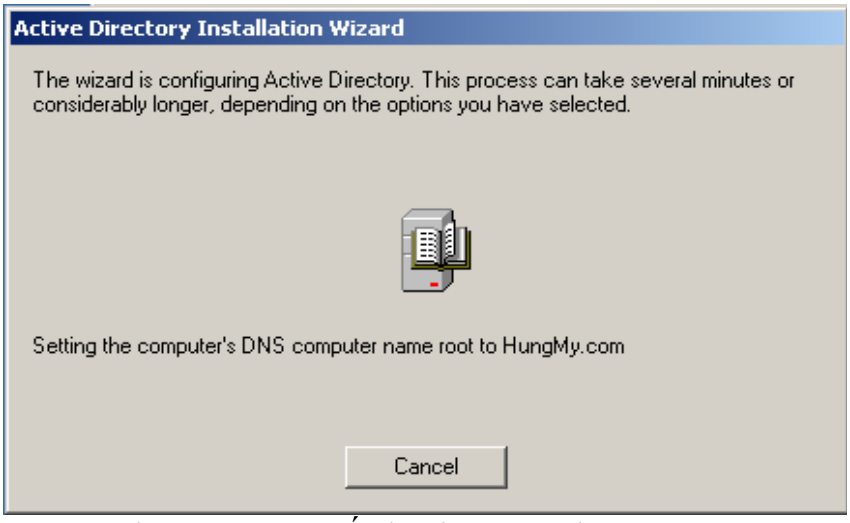
Hình 5.11: Permissions.

- Nhấp chọn vào **Permissions compatible only with Windows 2000 or Windows Server 2003 Operating Systems** rồi nhấp **Next** để tiếp tục. Lựa chọn này chỉ tương thích với Windows SERVER 2000 hoặc Windows SERVER 2003, nghĩa là nếu bạn chạy các chương trình Server trên hai hệ điều hành này (mà nó là thành viên của Active Directory Domain) thì người dùng được ủy quyền để đọc các thông tin trong Domain.



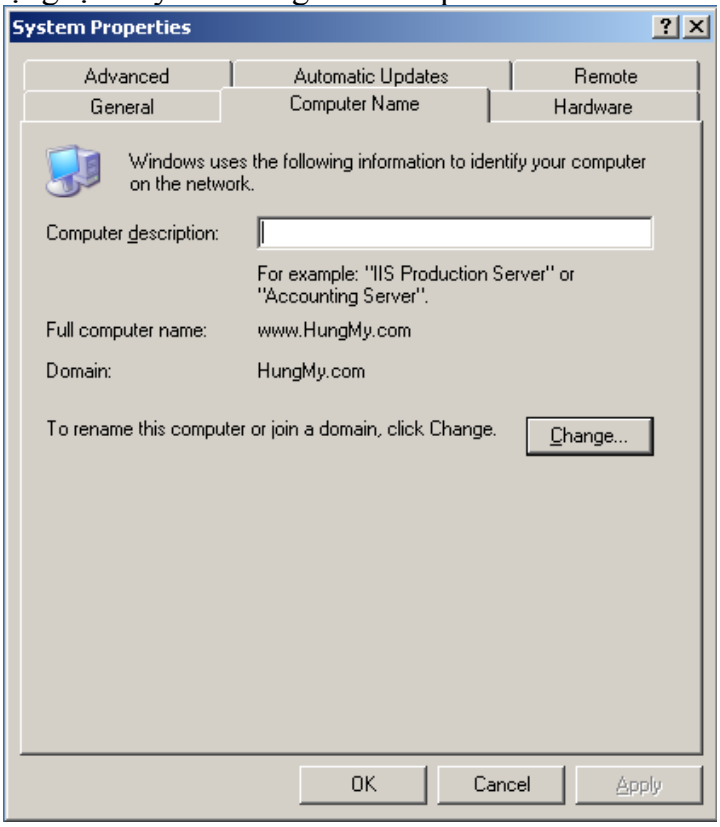
Hình 5.12: Nhập Password cho tài khoản Administrator.

- Nhập password trong mục **Restore password mode** và nhập lại password này trong mục **Confirm password** rồi nhấp **Next** để tiếp tục. Đây là password để bạn khởi động các dịch vụ thư mục .
- Bảng Summary xuất hiện, bạn nhấp **Next** để tiến hành cài đặt.



Hình 5.13: Đang tiến hành quá trình tạo Domain.

- Quá trình tạo Domain đang tiến hành. Sau khi tạo xong, bạn nhấp **Finish** để hoàn thành, sau đó khởi động lại máy tính bằng cách nhấp vào nút **Restar now.**



Hình 5.14: Tạo thành công Domain HungMy.com.

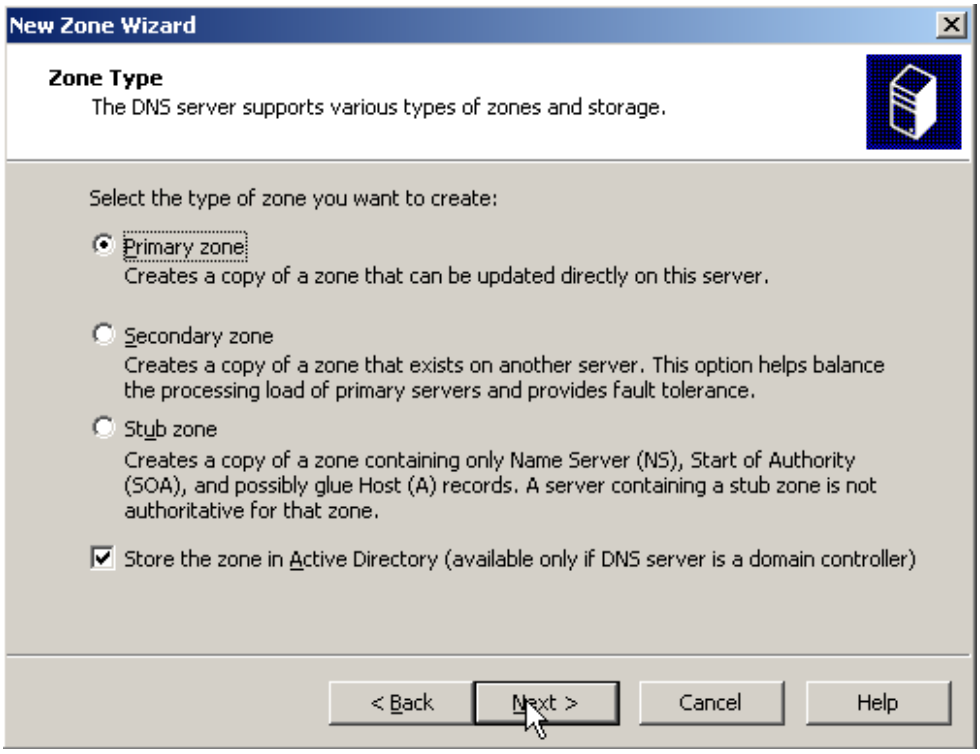
- Sau khi khởi động lại, chúng ta click chuột phải vào **My computer => Propertites,** chọn Tab **Computer Name** thấy tên Domain là **HungMy.com** có nghĩa là chúng ta đã tạo thành công domain **HungMy.com** rồi.

5.3.3 CẤU HÌNH DNS

DNS là dịch vụ chuyển đổi tên, nó chuyển đổi tên một cách đầy đủ (gồm tên máy và tên miền) thành địa chỉ IP để sử dụng trên mạng LAN , Internet....

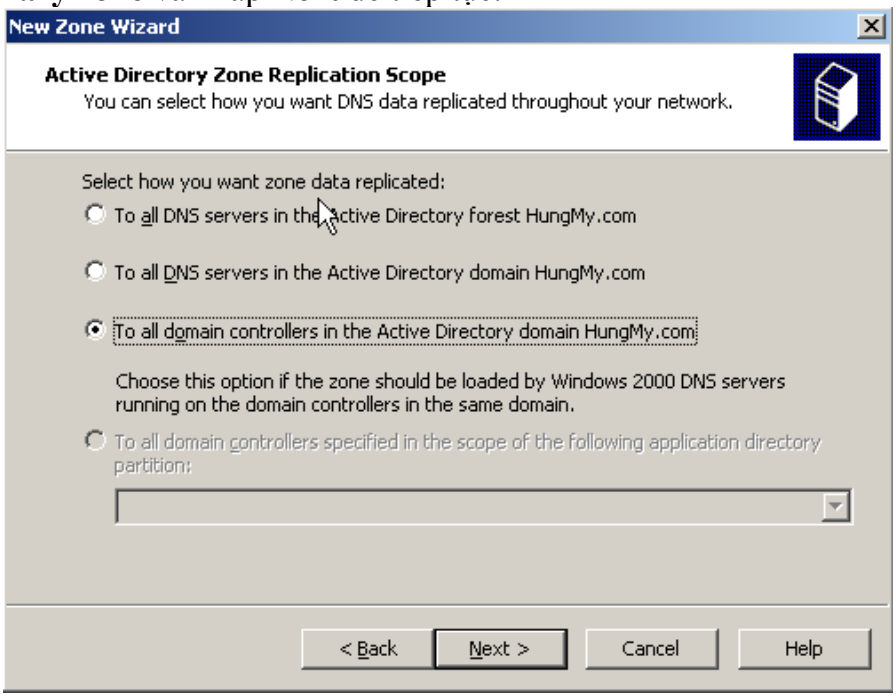
Vd: www.hungmy.com với www là tên máy và hungmy.com là tên miền.

- Vào **Start** => **Progam** => **Administrative tools** => Chọn **DNS**.
- Click chuột phải vào **Reverse Lookup Zones** chọn **New Zone**.
- Cửa sổ **Welcome to the New Zone Wizard** xuất hiện, ta chọn **Next** để tiếp tục cài đặt .



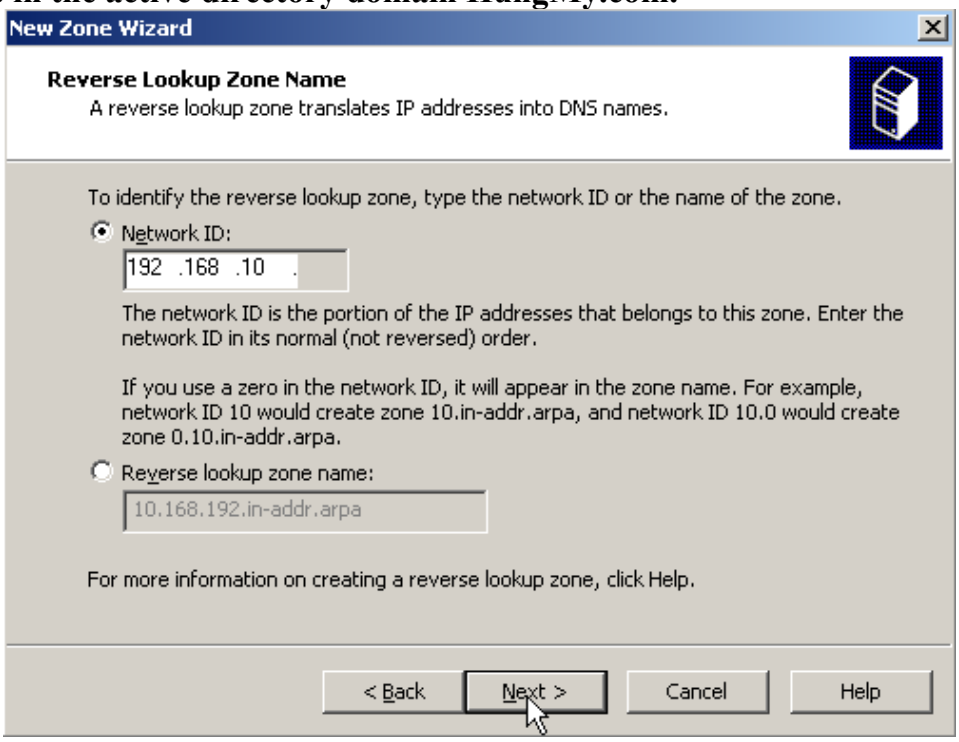
Hình 5.15: Zone Type.

- Chọn **Primary zone** và nhấp **Next** để tiếp tục.



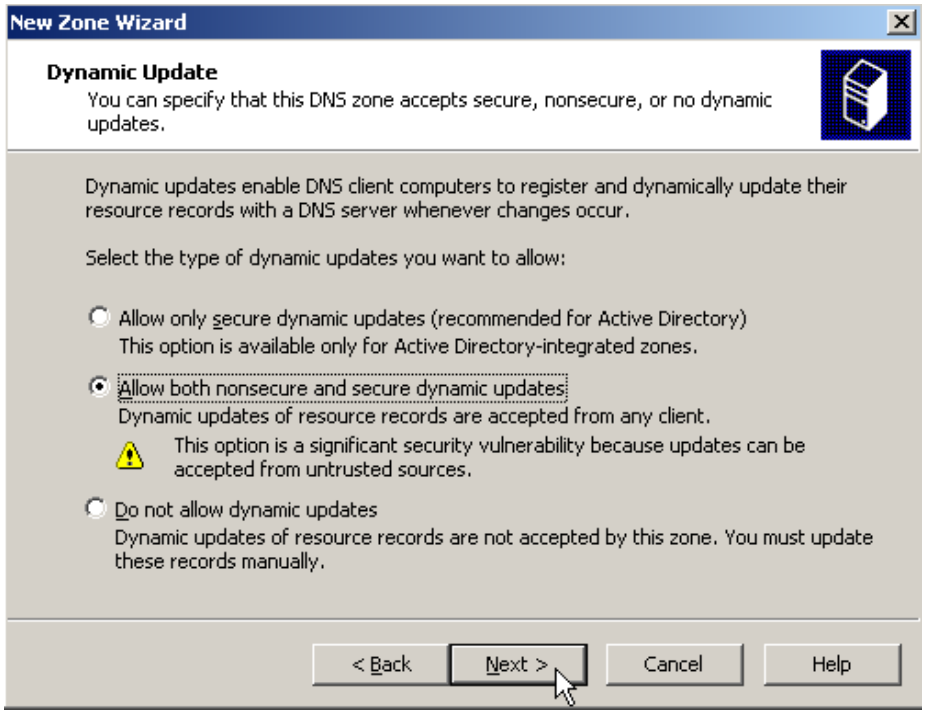
Hình 5.16 : Active Directory Zone Replication Scope.

- Tại cửa sổ **Active Directory Zone Replication Scope** ta chọn **To all domain controllers in the active directory domain HungMy.com.**



Hình 5.17: Reverse Lookup Zone Name.

- Trong cửa sổ Reverse Lookup Zone Name, mạng ta đang sử dụng là 192.168.10 nên chúng ta điền vào ô **Network ID** là 192.168.10.



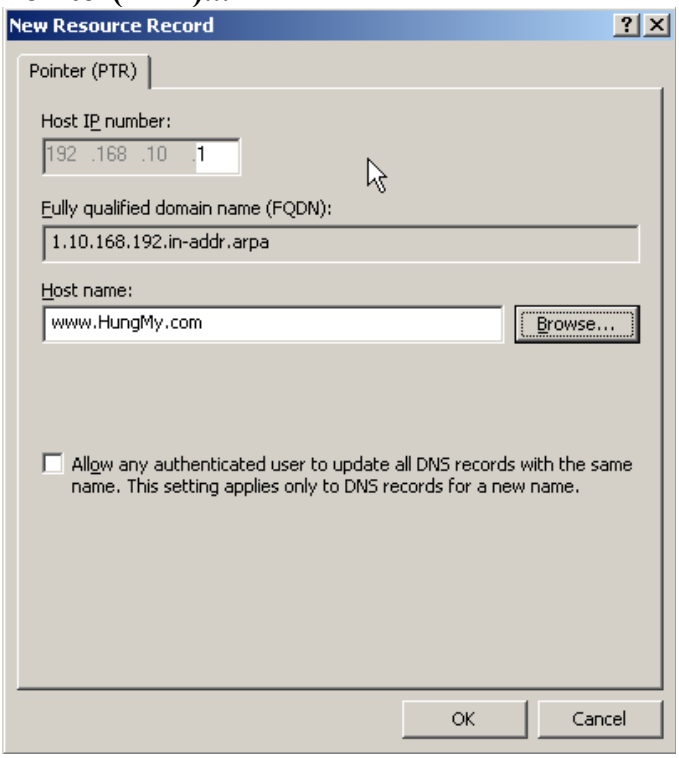
Hình 5.18: Dynamic Update.

- Trong cửa sổ Dynamic Update chọn **Allow both nonsecure and secure dynamic update** rồi chọn **Next**.

- Tiếp theo chọn **Finish** để kết thúc cài đặt Reverse Zone.

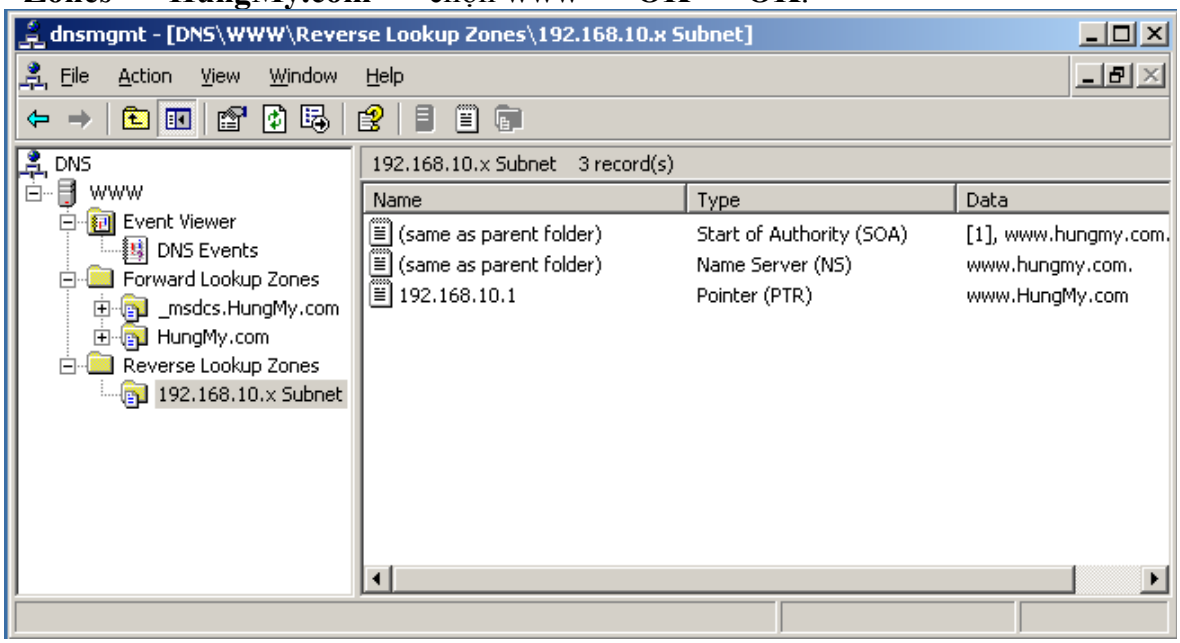
Name Server là www.HungMy.com nhưng còn thiếu **POINTER** chỉ định về www.HungMy.com cho Host Server nên ta phải tạo thêm POINTER cho Server.

- Click chuột phải vào "**192.168.10.x Subnet**" trong phần "**Reverse Lookup Zone**" => chọn **New Pointer(PTR)...**

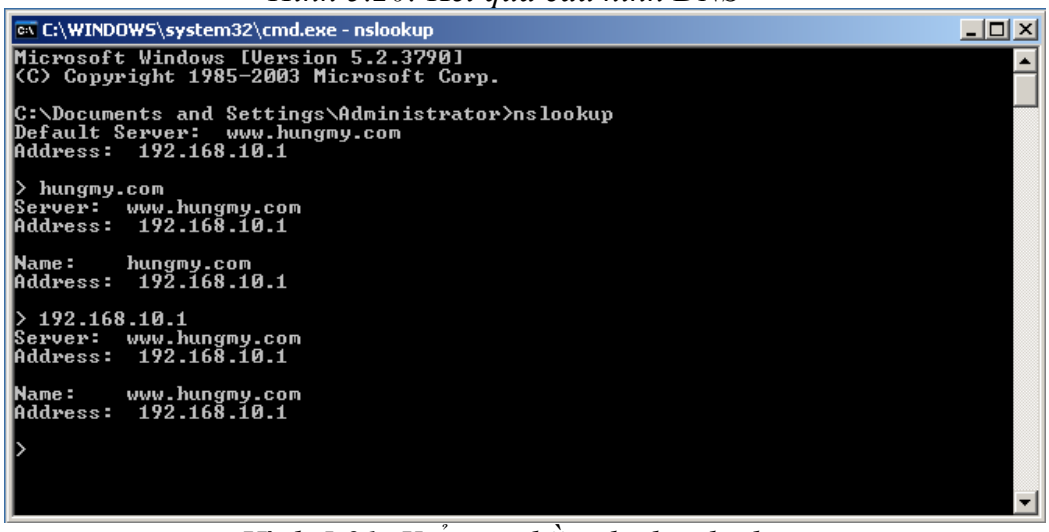


Hình 5.19: PTR.

- Điền địa chỉ của server là 192.168.10.1 vào "**Host IP number**", tại **Host name** ta nhấn nút Browse... chọn **WWW**(tên máy www) **Forward Lookup Zones** => **HungMy.com** => chọn **www** => **OK** => **OK**.



Hình 5.20: Kết quả cấu hình DNS



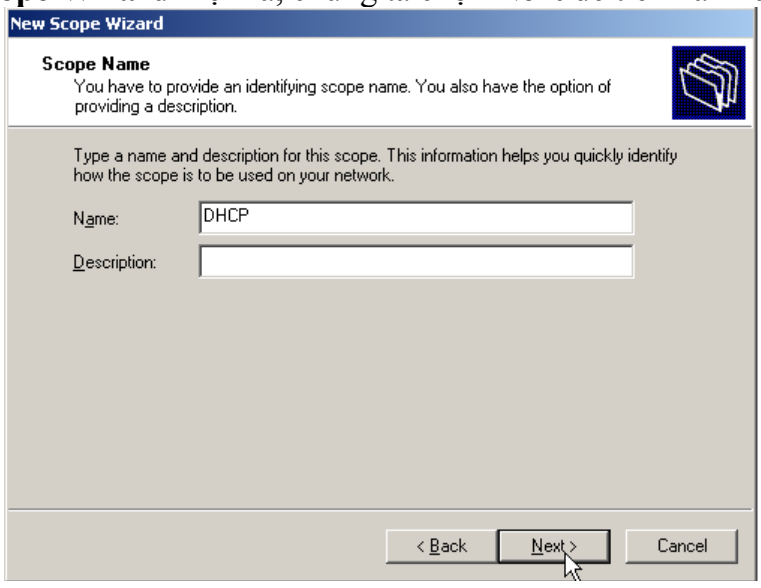
Hình 5.21: Kiểm tra bằng lênh nslookup.

- Để kiểm tra xem POINTER đã được tạo hay chưa ta vào DOS kiểm tra bằng lệnh "**nslookup**"

5.3.4 CẤU HÌNH DHCP:

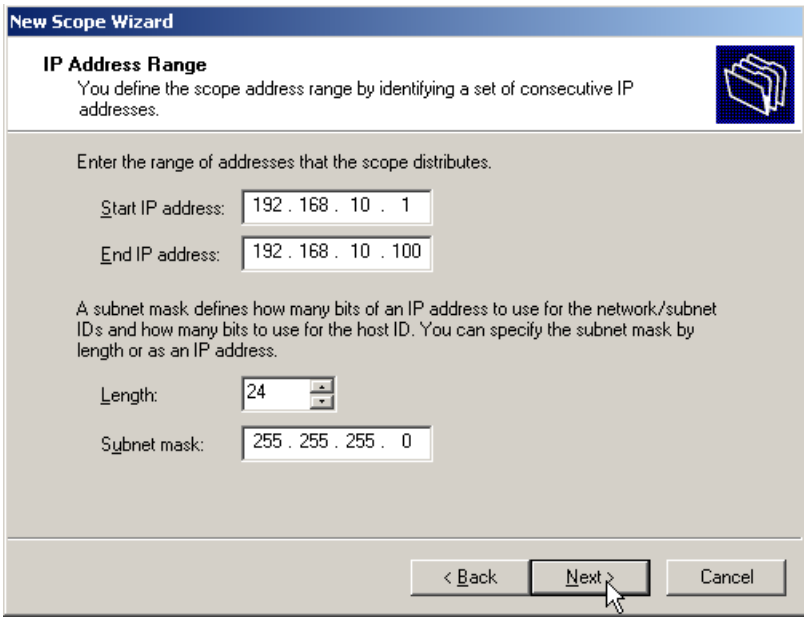
DHCP là một giao thức cấu hình động, được thiết kế để tập trung hóa cấu hình, quản lý thông tin cấu hình TCP/IP bằng cách gán tự động các địa chỉ IP cho các máy Client .

- Vào **Start** => **Progam** => **Aministrator tools** => **DHCP**.
- Click phải chuột vào Server chọn **New Scope**.
- Cửa sổ **New Scope Wizard** hiện ra, chúng ta chọn **Next** để tiến hành cấu hình.



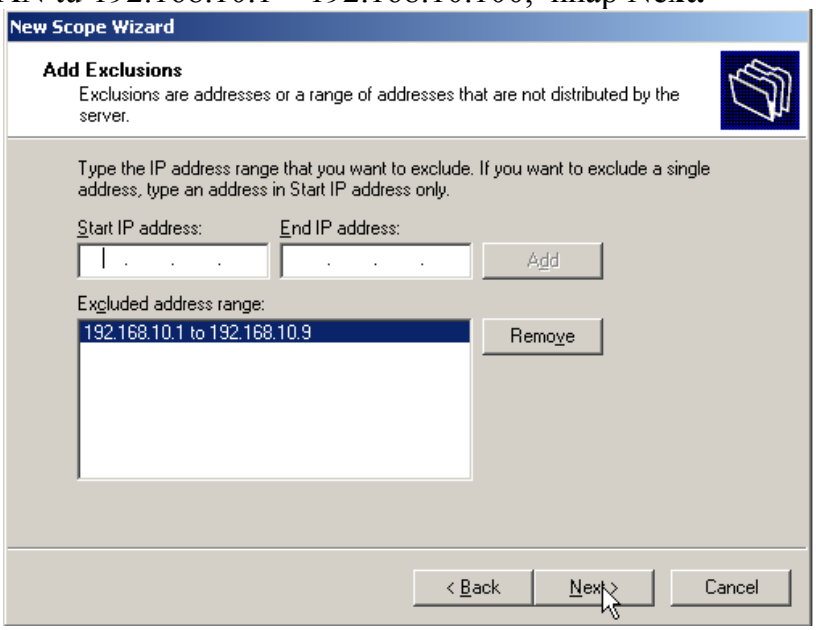
Hình 5.22: Scope name.

- Đặt tên cho Scope trong ô Name là DHCP.



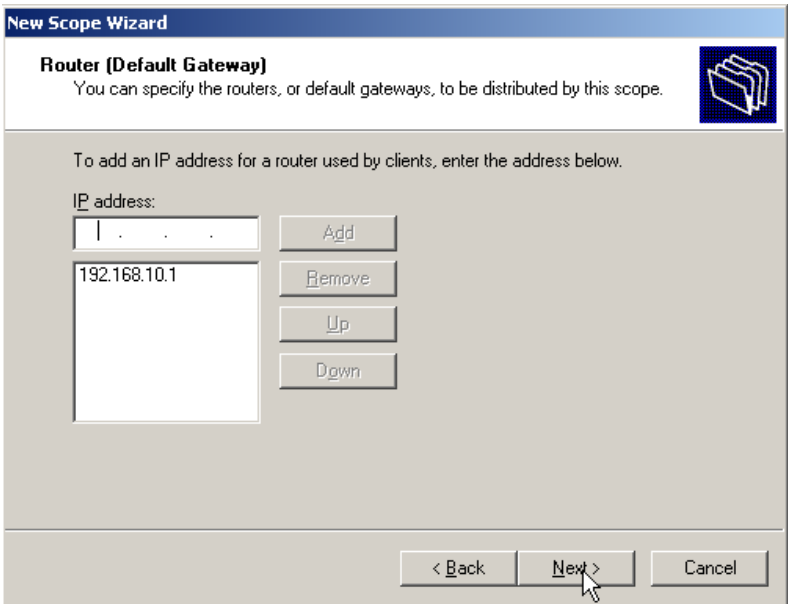
Hình 5.23 :IP Address Range.

- IP Address Range – khoảng IP chúng ta sẽ cấp cho mạng LAN, ở đây chúng ta cấp cho mạng LAN từ 192.168.10.1 – 192.168.10.100, nhấp **Next.**



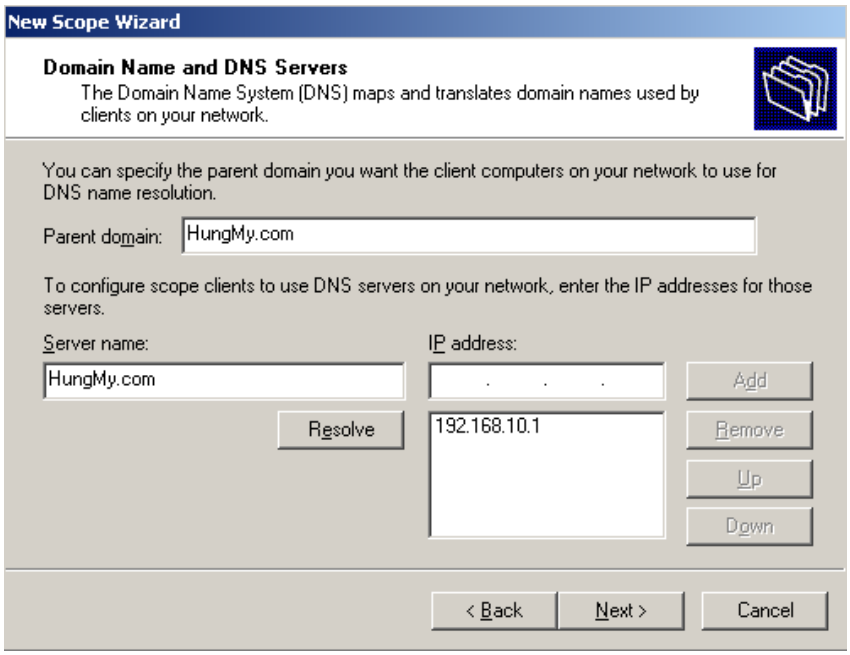
Hình 5.24: Add Exclusions.

- Trong cửa sổ ta điền khoảng loại trừ cấp phát IP từ 192.168.10.1 đến 192.168.10.9 vào **Start IP address** và **End IP address** => **Add**, nhấp **Next.**
- Trong cửa sổ **Lease Duration** ta nhấp **Next** để tiếp tục.
- Trong cửa sổ **Configure DHCP Option**, ta nhấp **Next**.



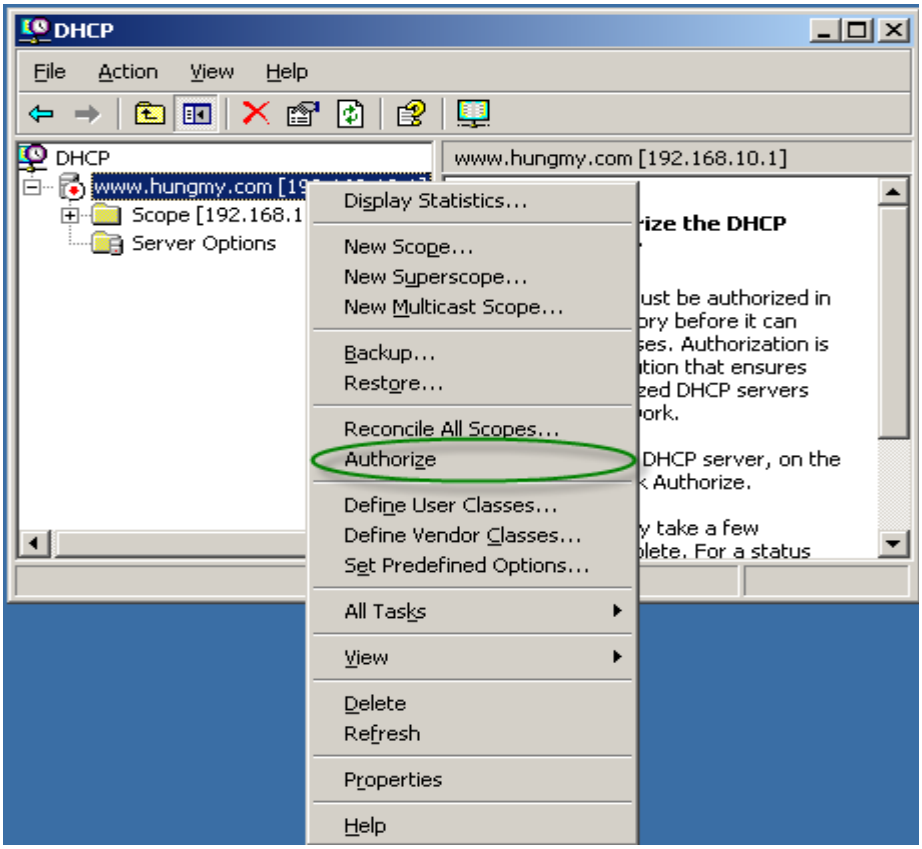
Hình 5.25 : Router(Default Gateway).

- Ta điền Default Gateway là 192.168.10.1 vào ô IP **Address**, nhấp **Next** .



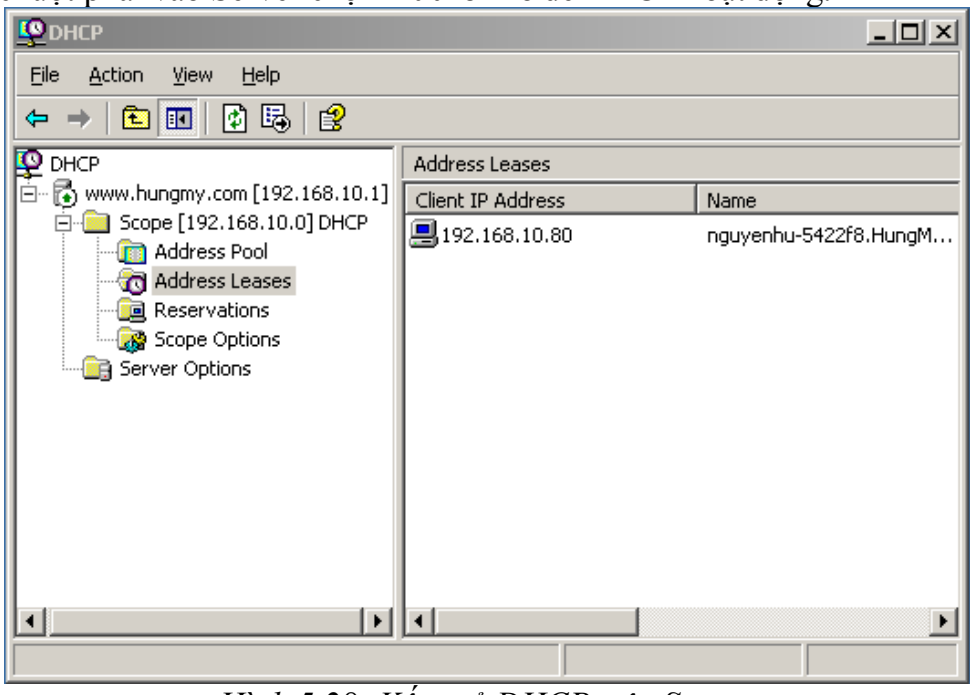
Hình 5.26: Domain name and DNS Server.

- Ta điền vào Parent Domain và Servername là tên của server "HungMy.com". Tiếp theo nhấp **Resolve** bên **IP address** sẽ hiện ra địa chỉ DNS là 192.168.10.1 => **Add**, rồi nhấp **Next.**
- Cửa sổ **WINS Severs** hiện ra ta nhấp **Next** để tiếp tục.
- Nhấp **Next** và **Finish** để kết thúc cài đặt.



Hình 5.27: Chứng thực Authorize

- Click chuột phải vào Server chọn **Authorize** để DHCP hoạt động.

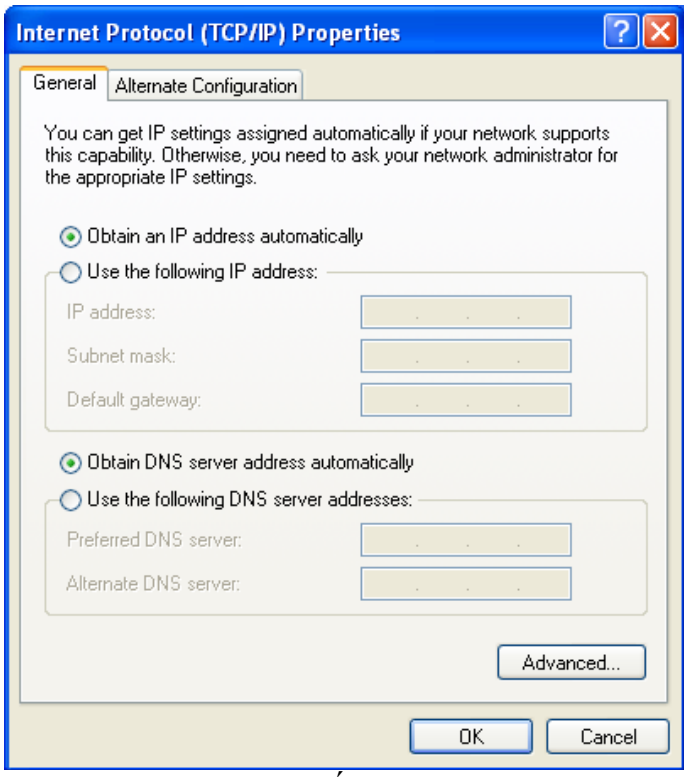


Hình 5.28: Kết quả DHCP trên Server

5.4 KẾT NỐI CLIENT ĐẾN SERVER:

Đầu tiên ta nhận địa chỉ IP từ dịch vụ DHCP của Server.

- Vào **Control Panel** chọn **Network Connections**, nhấp phải chuột vào **Local Area Connection** => **Properties** => **Internet Protocol(TCP/IP)** chọn **Properties.** Check vào **Obtain an IP address automatically** và **Obtain DNS address automatically**.



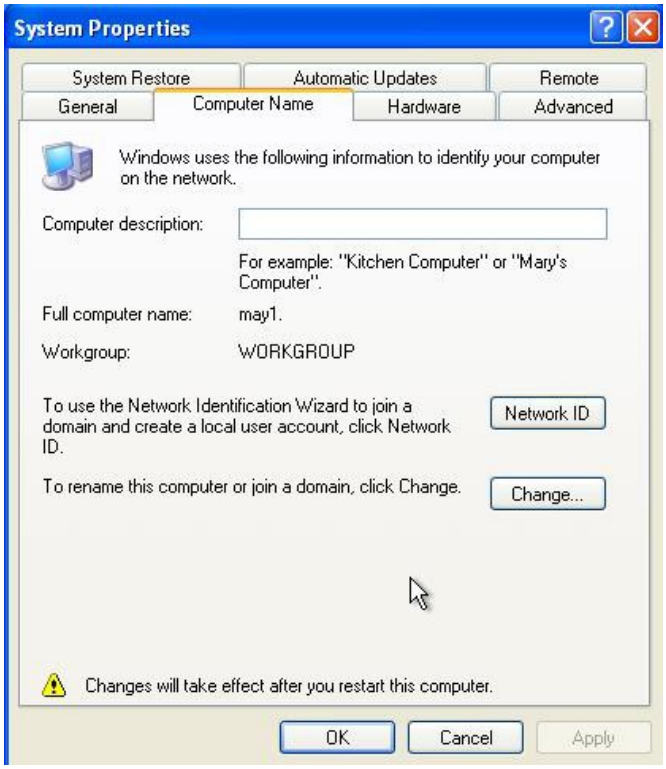
Hình 5.29: Cấu hình ip động

- Vào **Start** => **Run** gõ **cmd.**
- Gõ lệnh **ipconfig /release** để hủy địa chỉ IP hiện tại và gõ lệnh **ipconfig /renew** để nhận IP từ dịch vụ DHCP, sau đó ta gõ lênh **ipconfig** để kiểm tra lại.

```
C:\Documents and Settings\Administrator.HUNGMY>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : HungMy.com
        IP Address. . . . . . . . . . . . : 192.168.10.80
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.10.1

C:\Documents and Settings\Administrator.HUNGMY>
```

Hình 5.30: Client lấy ip động trên server cấp xuống

- Nhấp phải chuột vào biểu tượng **My Computer** trên Desktop, chọn **Properties**. Cửa sổ **System Properties** xuất hiện. Cửa sổ này chứa các thiết lập hệ thống, cũng như các chức năng quản lý toàn bộ hệ thống máy tính. Chọn thẻ **Computer Name**.

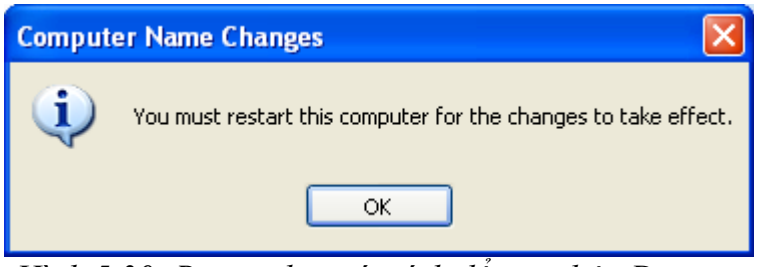


Hình 5.31: System properties.

- Nhấp nút **Change…** , Sau đó tại mục **Member of**, nhấp chọn **Domain**, tiếp theo nhập **HungMy.com**, cuối cùng nhấp **OK**.
- Cửa sổ **Computer Name Changes** xuất hiện. Tại mục **Username** nhập Administrator, nhập password của tài khoản Administrator đã đăng ký để tạo Domain), sau đó nhấp **OK** để đăng nhập.

Hình 5.32: Gia nhập Domain.

- Sau khi đăng nhập thành công, hệ thống sẽ thông báo với bạn là đã kết nối vào Domain thành công. Nhấp **OK** để tiếp tục, và nhấp **OK** lần nữa để khởi động lại máy tính.



Hình 5.30: Restart lại máy tính để gia nhập Domain

- Đăng nhập vào Domain, Nhập Username và Password, tiếp theo nhấp vào mục **Log On to** và chọn HUNGMY, sau đó nhấp **OK** để đăng nhập.

Hình 5.33: Gia nhập Domain thành công

5.5 GROUP POLICY (CHÍNH SÁCH NHÓM):

Các chính sách cần làm:

- Cho phép tài khoản người dùng trong phòng Kế Toán sử dụng các ứng dụng office như: Word, Exel, Internet Explore...
- Các người dùng thuộc phòng Kế Toán không được truy cập vào công cụ Control Panel, bỏ chức năng Run ở Start menu.
- Tắt chức năng Task Manager của những người dùng thuộc nhóm Kế Toán.

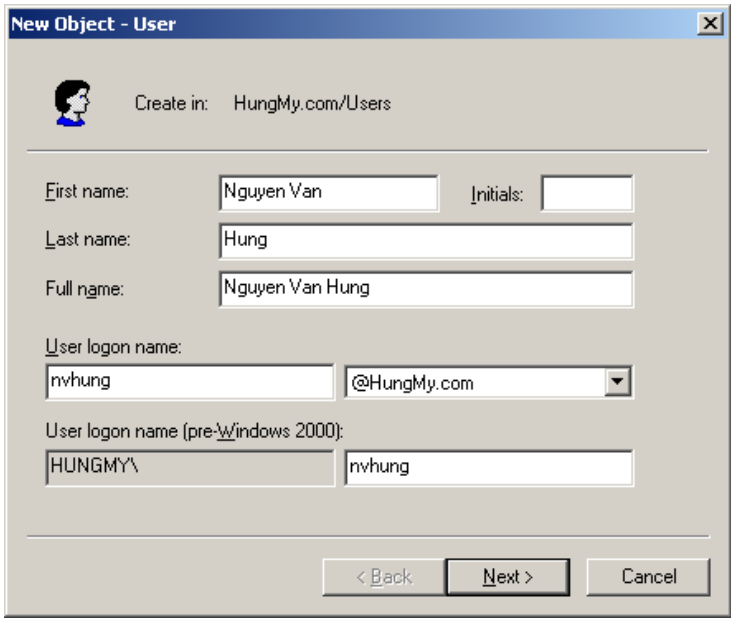
Vào **Start** => **Program** => **Administrator tools** => **Active Directory users and Computer**.

5.5.1 TẠO USER

Các nhân viên trong công ty sẽ được tạo 1 user để vào hệ thống máy tính trong công ty theo cách sau: lấy 2 kí tự đầu của Họ và Tên Lót + tên nhân viên.

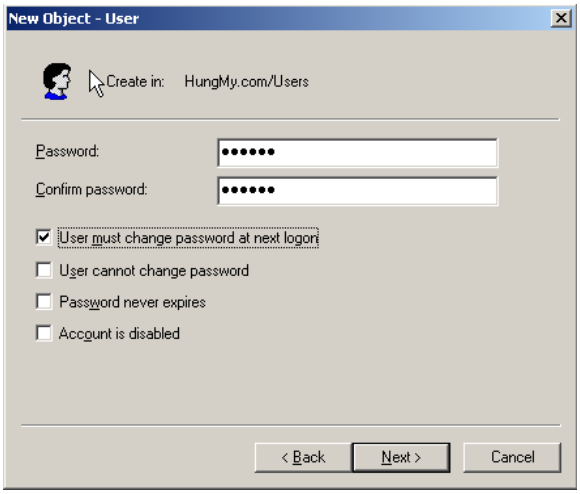
Vd : nhân viên Nguyễn Văn Hùng sẽ có user là nvhung.

- Click chuột phải vào Domain **HungMy.com** => **New** => **User**.



Hình 5.34: Tạo User.

- Cửa sổ **New Object-User** hiện ra, ta điền đầy đủ thông tin của nhân viên vào. Ở đây ta tạo user của nhân viên Nguyễn Văn Hùng của phòng Kế Toán nên ta điền họ tên của Nguyễn Văn Hùng vào **First name** và **Last name,** tạo user là **nvhung**. Chọn **Next**.



Hình 5.35 : Password User.

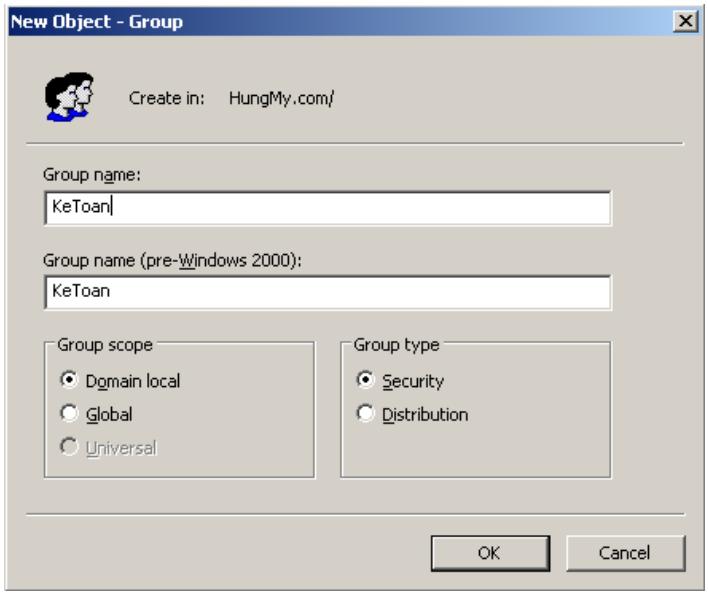
- Trong cửa sổ này, ta điền Password vào và chọn Option **User must change password at next logon** để user thay đổi password khi lần đầu tiên đăng nhập vào máy. Ta chọn **Next** => **Finish** để kết thúc quá trình tạo User.
- Giống như trên, ta tạo các user của các nhân viên trong công ty như: phòng Giám Đốc, phòng IT, và phòng Kế Toán.

5.5.2. TẠO GROUP

Trong công ty có 3 phòng ban nên ta tạo 3 Group để quản lý và chia sẻ tài nguyên .

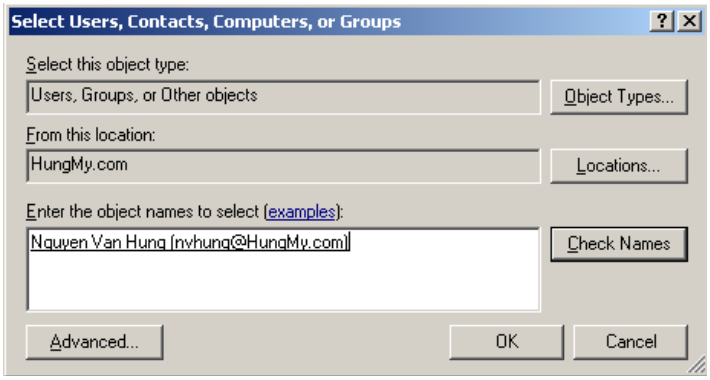
Các Group gồm : GiamDoc, KeToan, và IT.

- Click chuột phải vào tên Domain **HungMy.com** => **New** => **Group**.



Hình 5.36 : Group.

- Ta tạo một Group với tên là **KeToan** để quản lý và chia sẻ tài nguyên các nhân viên trong phòng Kế toán. Sau đó click chuột phải vào Group **KeToan** => **Properties** => qua Tab **Members** => **Add** để add các user thuộc nhân viên trong group **KeToan**



Hình 5.37: Add user vào Group.

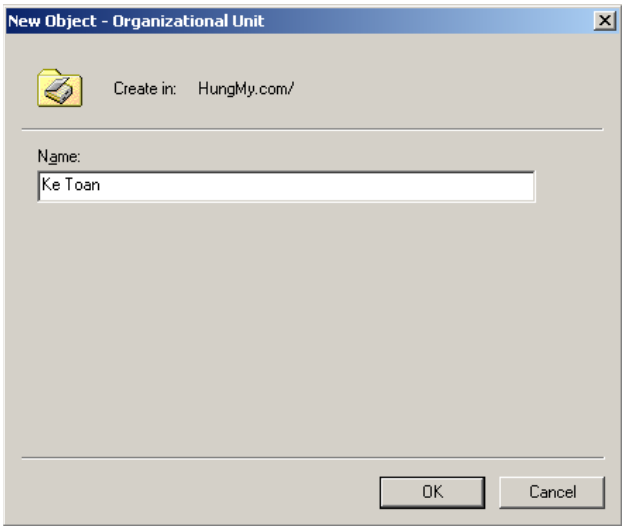
- Vào **Advanced** => **Find now** để tìm kiếm các user đã tạo. Ở đây ta Add user Nguyễn Văn Hùng(nvhung) vào Group **KeToan**.

- Giống như vậy ta tạo các Group của các phòng ban Giám đốc , và IT và add các nhân viên của phòng ban đó vào Group vừa tạo .

5.5.3. TẠO OU

Ở đây ta sử dụng **Group Policy Object**(GPO) để triển khai các chính sách cho các nhóm người dùng, mà GPO chỉ có thể apply lên các đơn vị quản lý nhỏ nhất là OU nên ta phải di chuyển các user vào OU để quản lý.

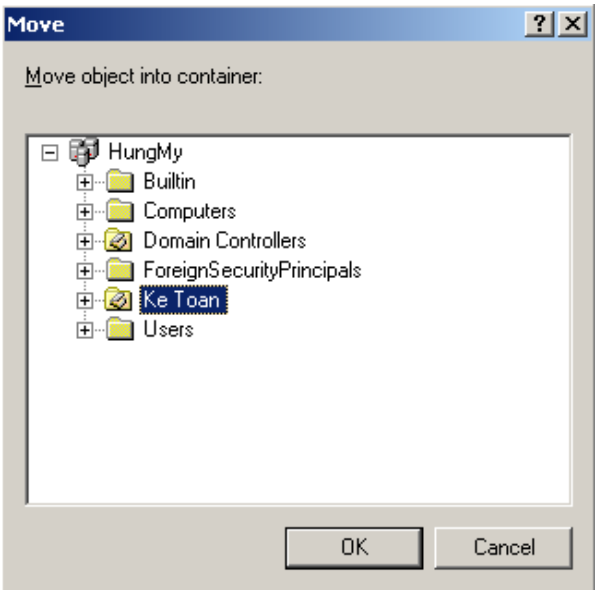
- Right Click vào tên Domain **HungMy.com** => **New** => **Organization Unit.**



Hình 5.38: Tạo OU.

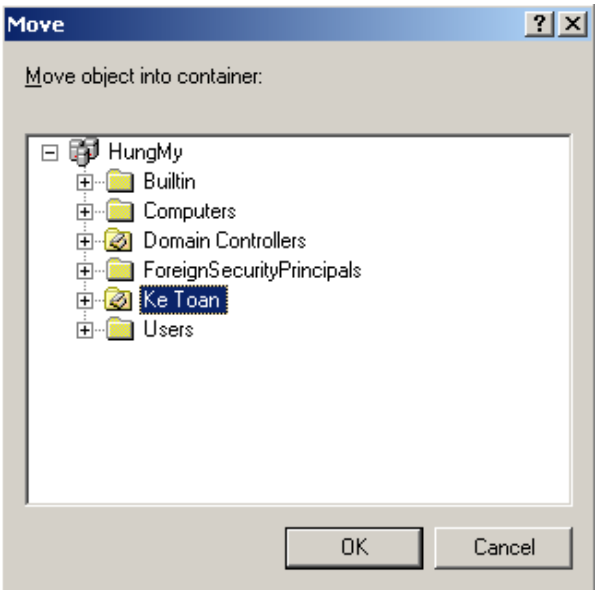
- Tạo một OU tên là **Ke Toan** để quản lý các user & group thuộc phòng Kế toán. Ta cũng tạo các OU của các phòng IT, Giám Đốc.

- Click chuột phải vào User **nvhung** => **Move.**



Hình 5.39: Di chuyển User vào OU.

- Chọn **Ke Toan** => **OK** để add user **nvhung** vào OU **Ke Toan**.
- Click chuột phải vào Group **KeToan** => **Move**



Hình 5.40: Di chuyển Group vào OU.

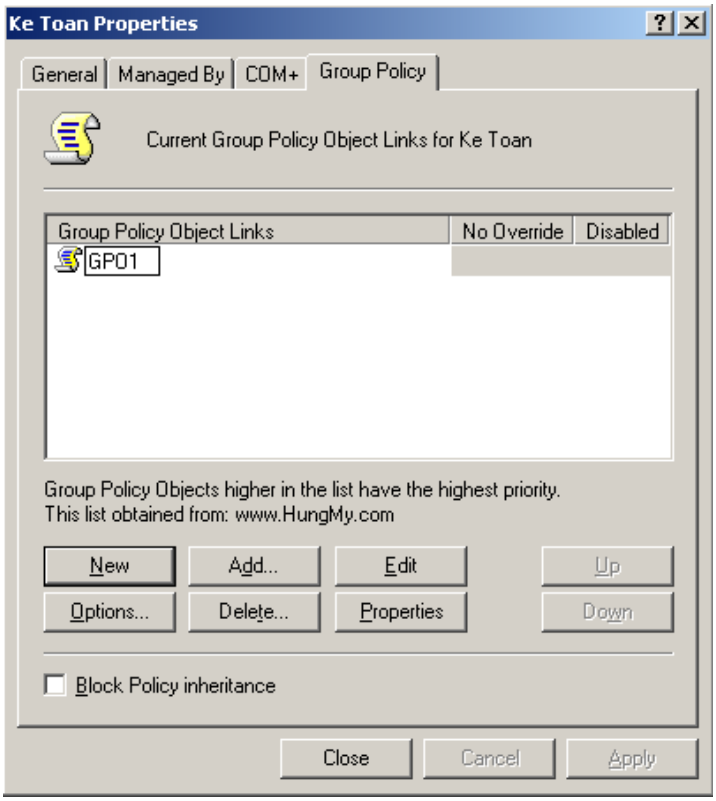
- Chọn **Ke Toan** => **OK** để add group **KeToan** vào OU **Ke Toan**.

Tương tự ta add các user & group của phòng Kế toán vào OU Ke Toan và add các user & group của nhân viên phòng nào vào OU phòng đó.

5.5.4. ÁP DỤNG CÁC CHÍNH SÁCH GROUP POLICY OBJECT (GPO)

- **Apply chính sách GP cho phép tài khoản người dùng trong phòng Kế Toán sử dụng các ứng dụng office như: Word, Exel, Internet Explore.....**

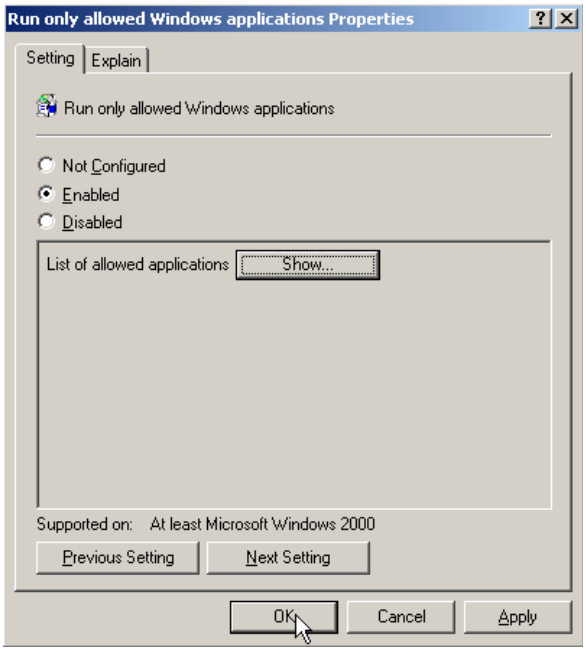
- Click chuột phải tại OU **Ke Toan** => **Properties.**



Hình 5.41: Tạo GPO1.

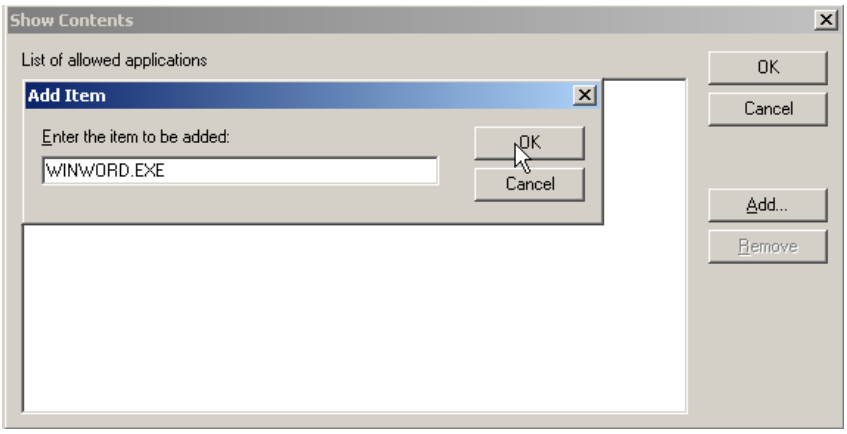
- Chọn Tab **Group Policy**, chọn new để tạo một **Group Policy Object**(GPO) với tên là **GPO1**. Tiếp theo chọn **Edit** để chỉnh sửa chính sách.

- Tại cửa sổ **Group Policy Object Editor** ta vào **User configuration** => **Administrative templates** => **System**. Chọn chính sách **Run only allow Windows application.**



Hình 5.42: Chính sách Run only allow Windows application.

- Ta chọn **Enable** và chọn **Show**.



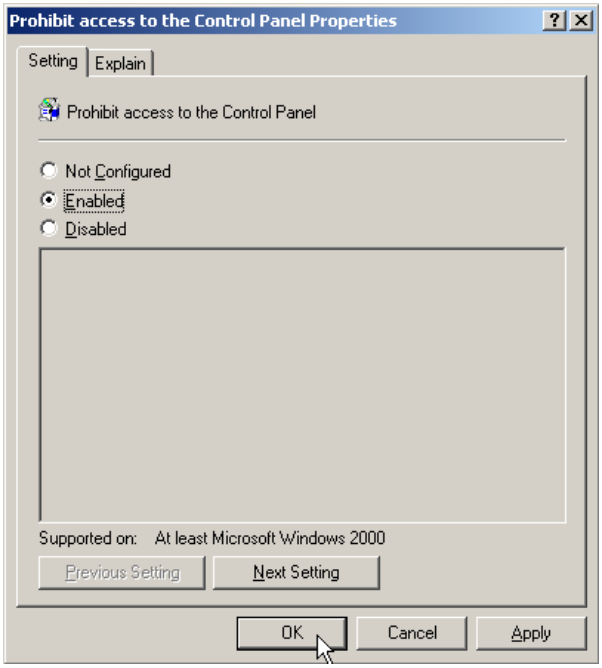
Hình 5.43: Add file chạy của các phần mềm cho phép.

- Tại cửa sổ **Show Contents**, ta chọn **Add...** nhập tên file chạy của chương trình ứng dụng. Ở đây ta nhập WINWORD.EXE(word), EXCEL.EXE(excel), IEDW.EXE(Internet Explorer Browser)....

Chọn xong ta nhấn **OK** => **OK** =>**OK**.

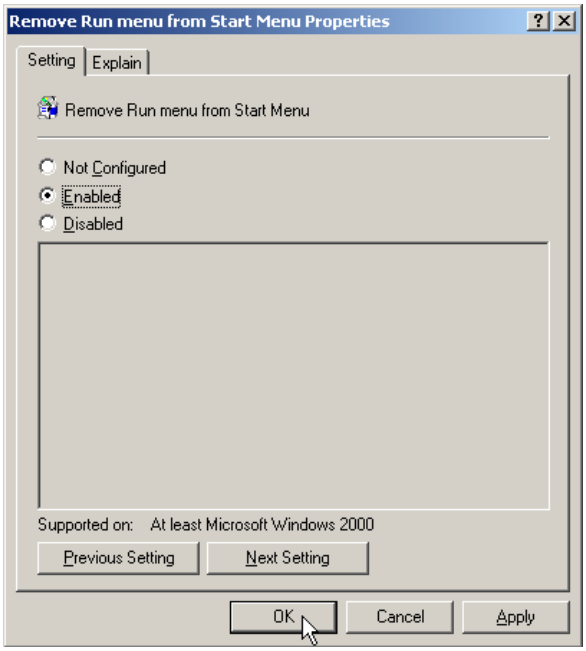
➢ **Cấm người dùng thuộc phong Kế Toán không được truy cập vào công cụ Control Panel, bỏ chức năng Run ở Start menu**

- Ta tạo một **GPO2** cho OU **Ke Toan**
- Ta vào đường dẫn **User Configuration** => **Administrative Templates** => **Control Panel**.
- Tại đây ta chọn chính sách tên là **Prohibit access to the Control Panel**.



Hình 5.44: Chính sách Prohibit access to the Control Panel.

- Check vào **Enable** => **OK**.
- Ta tạo một **GPO3** cho OU **Ke Toan**
- Vào **User Configuration** => **Administrative Templates** => **Start menu and Taskbar.**
- Chọn chính sách **Remove Run menu from Start Menu**.

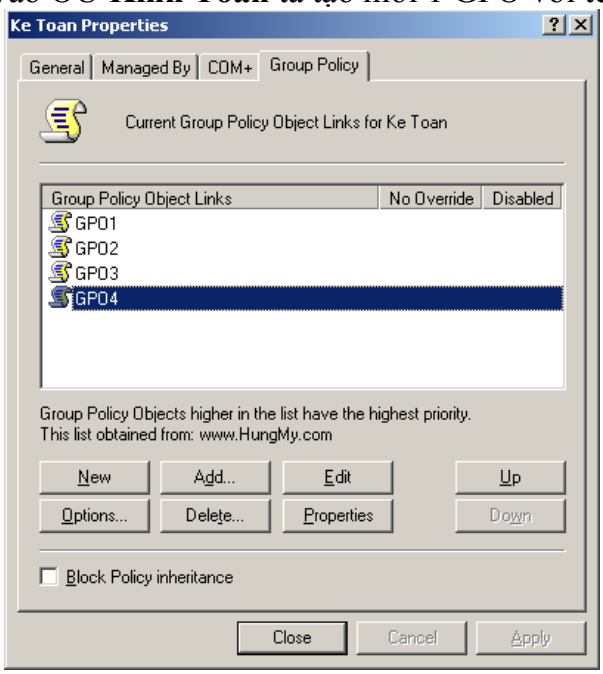


Hình 5.45: Chính sách Remove Run menu from Start Menu.

- Chọn **Enable** => **OK**.

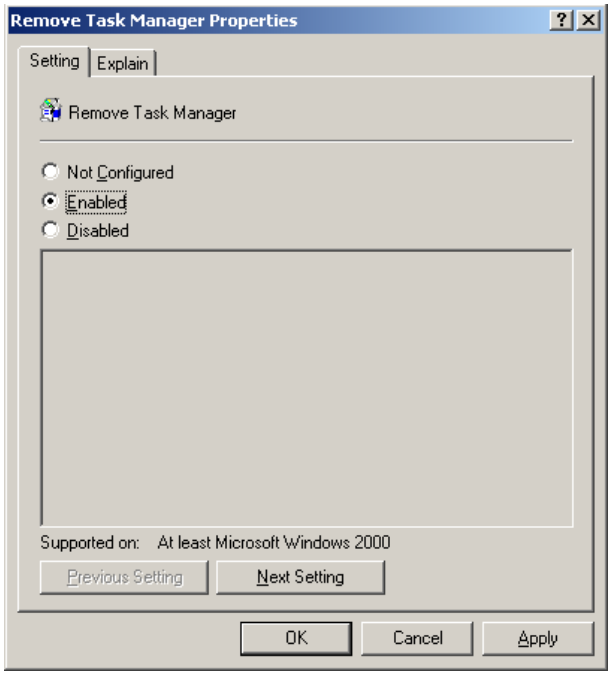
➢ **Tắt chức năng Task Manager của những người dùng thuộc nhóm KeToan**

- Click chuột phải vào OU **Kinh Toan** ta tạo mới 1 GPO với tên là **GPO4**.



Hình 5.46: Tạo GPO4

- Vào **User configuration** => **Administrative Tempaltes** => **System** => **Ctrl+Alt+Del Options** => chọn **Remove Task Manager**



Hình 5.47: Chính sách Remove Task Manager

- Chọn **Enable** => **OK**.

5.6. SHARE & NTFS PERMISSION:

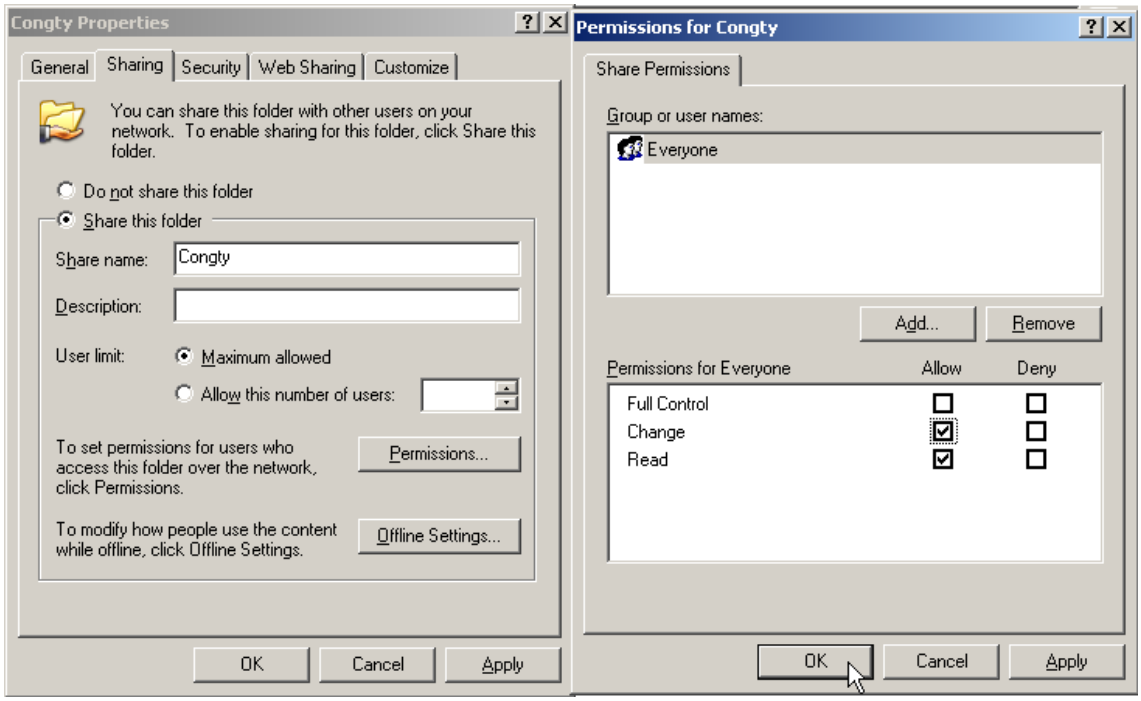
Quản lý việc chia sẻ các tài nguyên, cho phép User nào được sử dụng tài nguyên nào trong công ty

Yêu cầu :

- Chia sẻ thư mục cha là thư mục **Congty** cho toàn người dùng trên mạng có thể thấy và truy cập.
- Thư mục của phòng ban nào thì chỉ có những người dùng của phòng ban đó mới có quyền truy cập vào.
- Trong từng phòng ban thì có từng thư mục tương ứng cho từng phòng ban đó. Tương ứng với 1 thư mục thì chỉ có người dùng trong phong ban đó mới có thể truy cập vào và có toàn quyền trên thư mục của mình. Ngoài ra các phòng ban khác có thể truy cập vào nhưng chỉ có quyền đọc mà thôi.

5.6.1. SHARE PERMISSION

- Click chuột phải vào thư mục **Congty** cần Share chọn **Sharing and Security**.



Hình 5.48 : Share permission.

- Chọn **Permissions.**. => **Add** => thêm quyền **Change** cho **everyone** (mặc định quyền everyone có quyền read) để những user có quyền với thư mục làm việc con có thể ghi vào thư mục con .

5.6.2. NTFS PERMISSION

Sơ đồ phân quyền NTFS trên các thư mục :

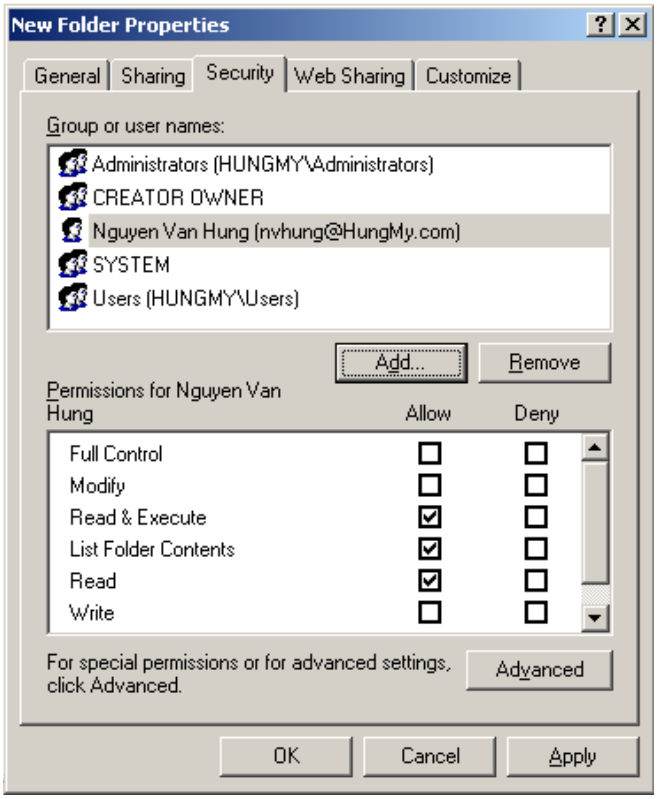
Thư mục / Người dùng	Congty
Everyone	R
IT	F

Thư mục / Người dùng	Ke toan	IT	Giam doc
Giam doc	R	R	F
IT	R	F	R
Ke toan	F	R	R

F : Full controll (đọc, viết, xóa,...).

R : Read (đọc).

- Click chuột phải vào thư mục cần phân quyền là **Ke toan =>** chọn **Properties** => chuyển qua Tab **Security**.



Hình 5.49: Security.

Add : thêm 1 người dùng hoặc một nhóm người dùng.

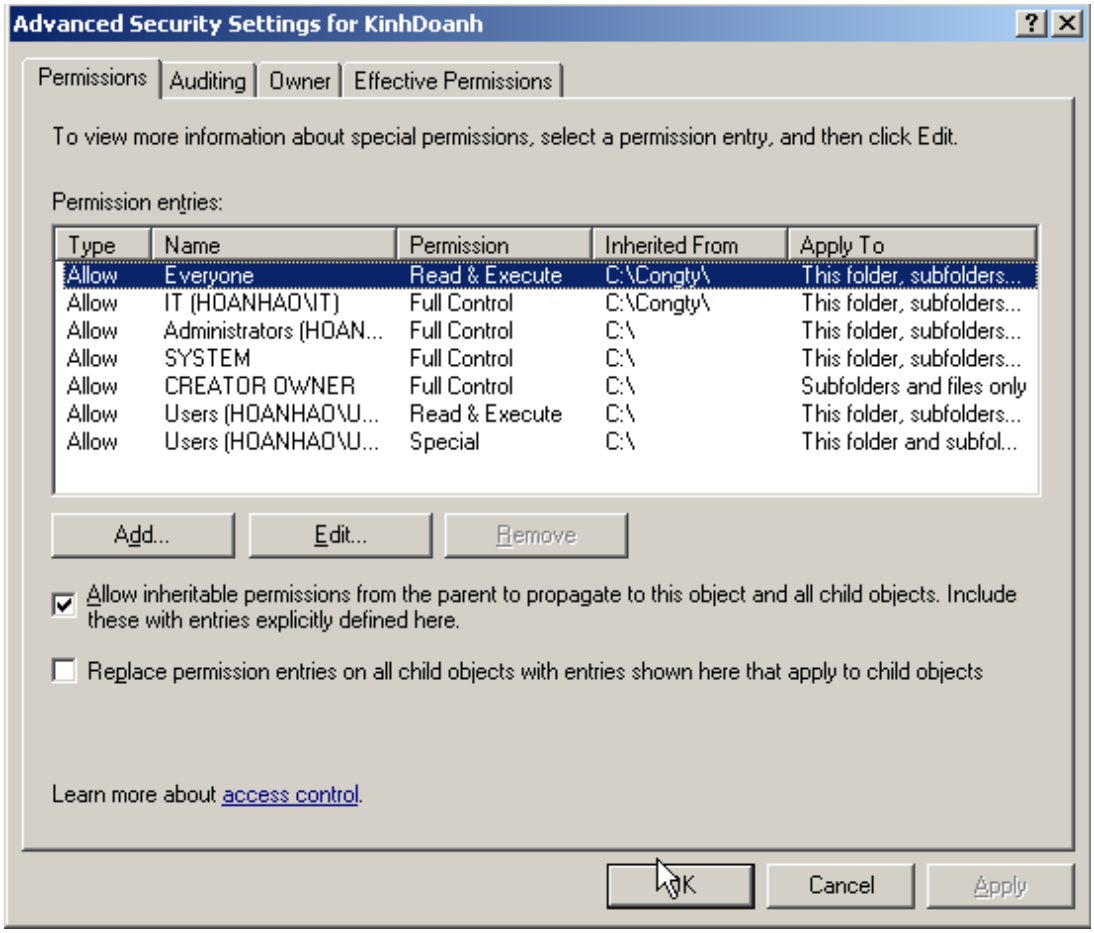
Remove : xóa người dùng hoặc nhóm người ra khỏi danh sách phân quyền .

Permission for : thay đổi quyền hạn người dùng và nhóm người dùng.

- Ở đây ta chọn **Full Control** cho nhóm **KeToan** còn nhóm **Giam Doc** và nhóm **IT** thì chọn **Read, Read & Execute, List Folder Contents.**

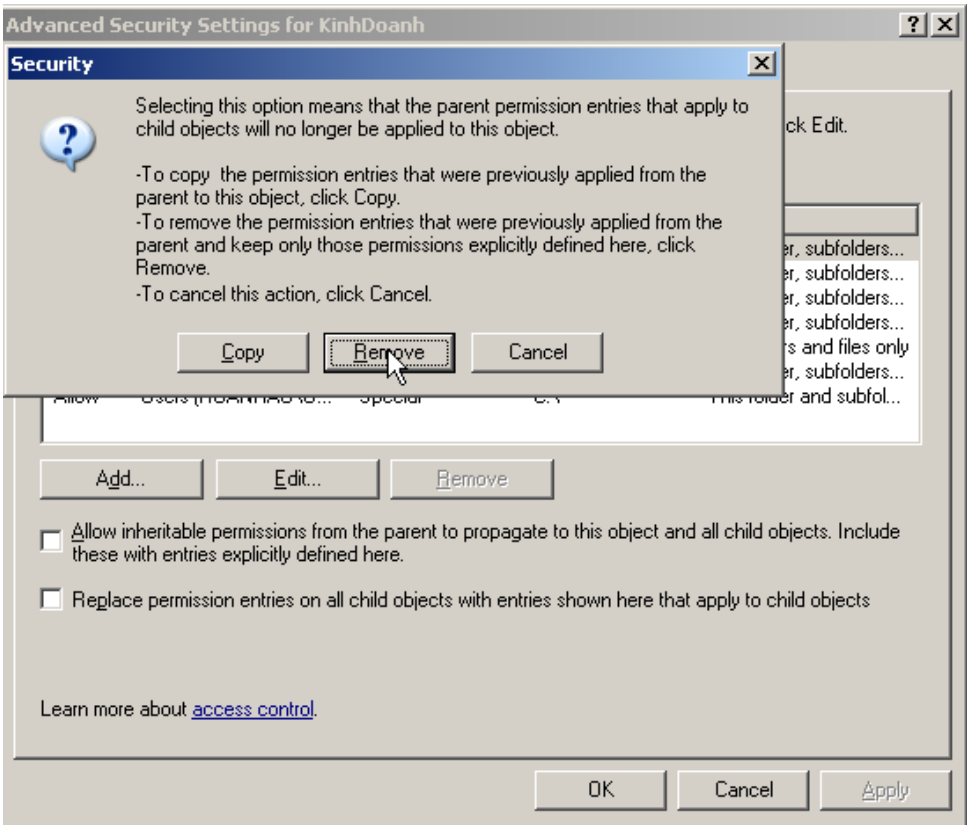
Khi thực hiên phân quyền cho một thư mục thì bị vấn đề thư mục con sẽ kế thừa quyền của thư mục cha. Cách để gỡ bỏ quyền kế thừa trên thư mục con như sau:

- Click chuột phải vào thư mục cần phân quyền là thư mục **Ke toan** => **Properties** => chuyển qua tab **Security** => **Advance**. Trong cửa sổ **Advance Security Settings** chọn tab **Permission**



Hình 5.50: Advance Security Settings.

- Ta bỏ chọn mục **Allow inheritable permission from the parent....**



Hình 5.51: Hộp thoại Security.

- Lúc này hiện ra hộp thoai Security với 3 tùy chọn :

  Copy : giữ nguyên những quyền đã được áp dụng trước đó trên thư mục cha.

  Remove : xóa toàn bộ quyền kế thừa từ thư mục cha.

  Cancel : Thoát.

- Ta chọn **Remove.**

- Sau đó ta chọn user **nvhung** có quyền **Full Controll** với thư mục **Ke toan,** nhóm Giam Doc và nhóm IT có quyền **Read**.

Giống như trên ta làm cho tất cả các thư mục được chia sẻ khác công ty.

5.7. SYSTEM POLICY:

System Policy hay còn gọi là chính sách hệ thống. System Policy xuất hiện trên môi trường WORKGROUP lẫn DOMAIN.

Trong môi trường WORKGROUP, chính sách hệ thống xuất hiện trong công cụ Local Security Policy(chỉ có tác dụng ngay trên chính máy User đang ngồi) .

Trong môi trường DOMAIN, chính sách hệ thống xuất hiện trên 2 công cụ Domain Security Policy và Domain Controller Security Policy: tác dụng trên các đối tượng trong Domain , group,.. và chỉ cần cấu hình trên máy Domain Controllers.

Các chính sách (cấu hình trên máy Domain) :

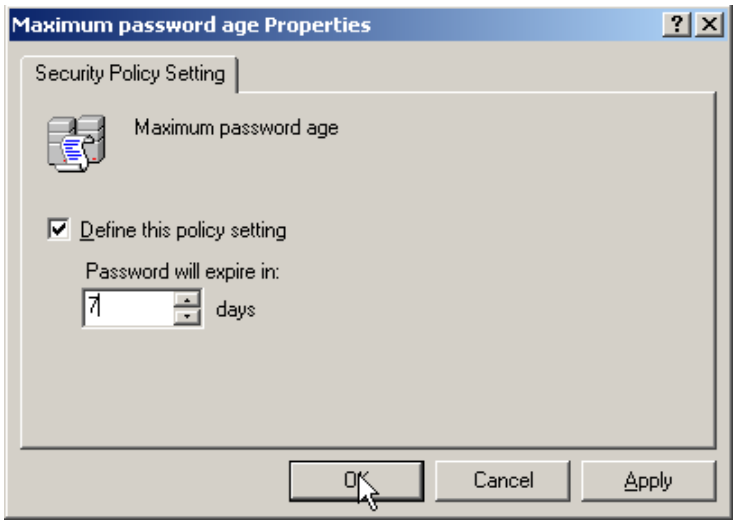
- Định thời gian thay đổi mật khẩu của một tài khoản người dùng là 7 ngày.
- Không yêu cầu password phức tạp.
- Nếu một tài khoản đăng nhập sai mật khẩu quá 3 lần thì bị khóa tài khoản 30 phút.
- Không yêu cầu bấm tổ hợp phím Ctrl+Alt+Del khi logon hệ thống.
- Không hiển thị tên người dùng logon trước đó.
- Cho phép người dùng được thay đổi giờ của hệ thống máy.
- Cho phép người dùng Shutdown hệ thống.

- Vào **Start** =>**Program** =>**Administrator tools** => **Domain Security policy** .

Tại cửa sổ **Default Domain Security Setting**, nhấp chuột vào dấu cộng tại **Account Policies** => **Password Policy**.

- **Để định thời gian thay đổi mật khẩu người dùng**

- Ta vào mục **Maximum password age**.

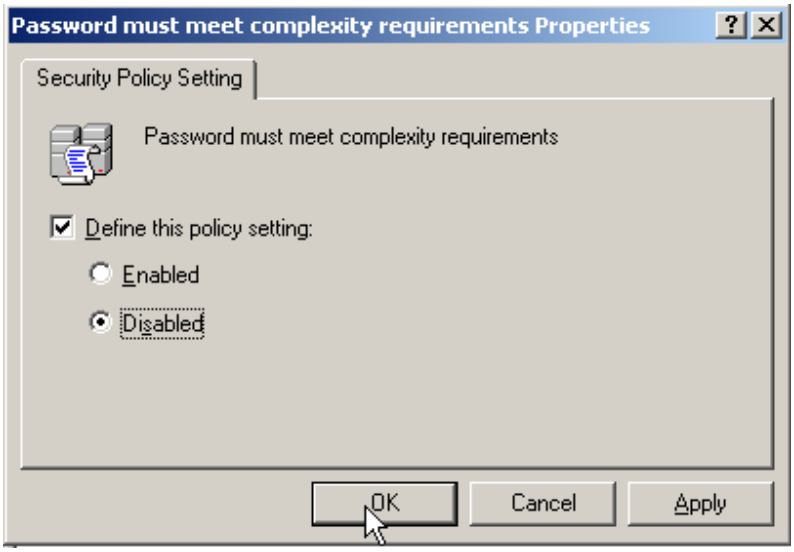


Hình 5.52: Chính sách Maximum password age.

- Tại ô **Password will expire in** , ta gõ số 7 nghĩa là 7 ngày đổi mật khẩu 1 lần.

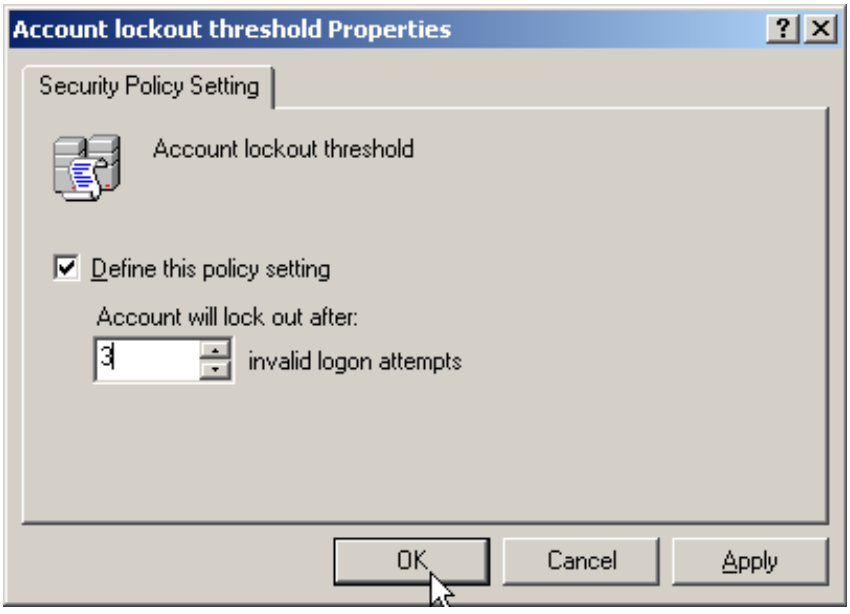
- **Chính sách không yêu cầu password có độ phức tạp.**

- Ta vào mục **Password must meet complexity requiments.**



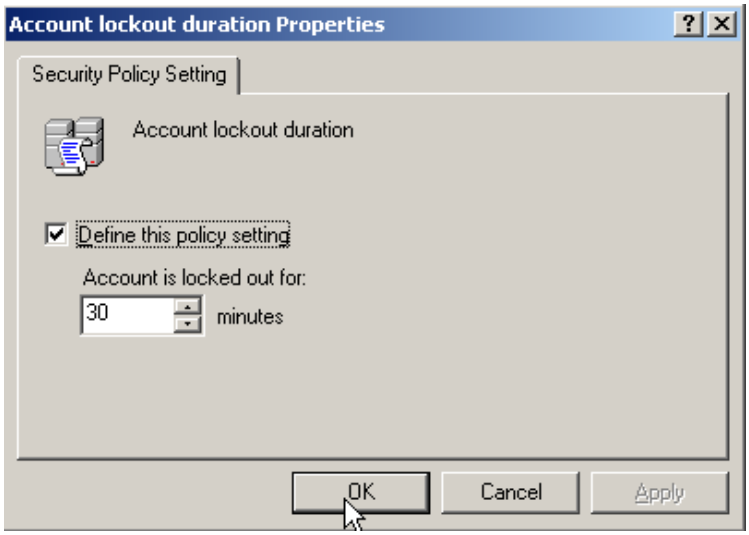
Hình 5.53: Chính sách Password must meet complexity requiments.

- Check vào mục **Disable** .
  - **Chính sách nếu tài khoản đăng nhập sai 3 lần thì khóa tài khoản 30 phút.**
- Vào **Account lockout policy** =>**Account clockout threshold.**



Hình 5.54: Chính sách Account clockout threshold.

- Nhập vào textbox giá trị là 3 để chỉ đinh nếu nhập sai password 3 lần thì account sẽ bị khóa.
- Tiếp theo, vào **Account lockout duration.**

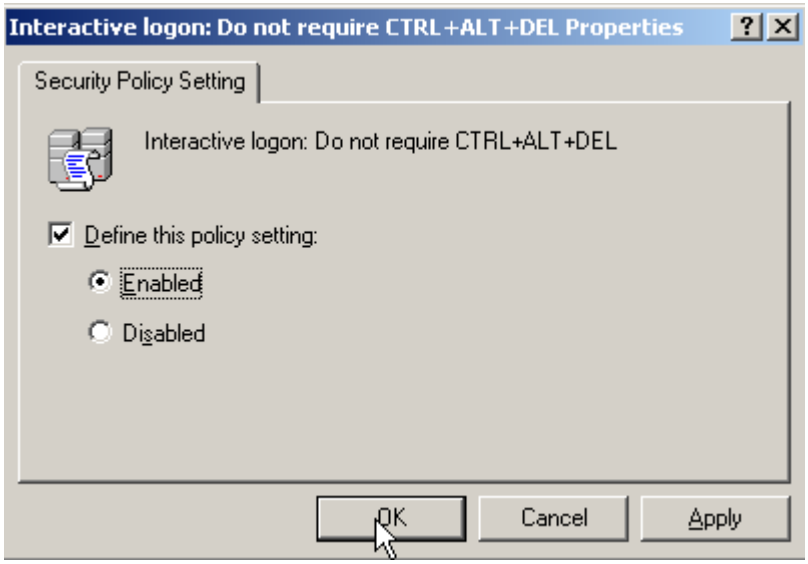


Hình 5.55: Account lockout duration.

- Nhập vào giá trị là 30, có nghĩa là account sẽ bị khóa 30 phút nếu bạn nhập sai 3 lần password => **OK**.

➢ **Không yêu cầu nhấn Ctrl+Alt+Del khi logon hệ thống.**

- Ta chọn **Local Policy** => **Security Options** chọn **Interactive logon: Do not require CTRL+ALT+DEL.**

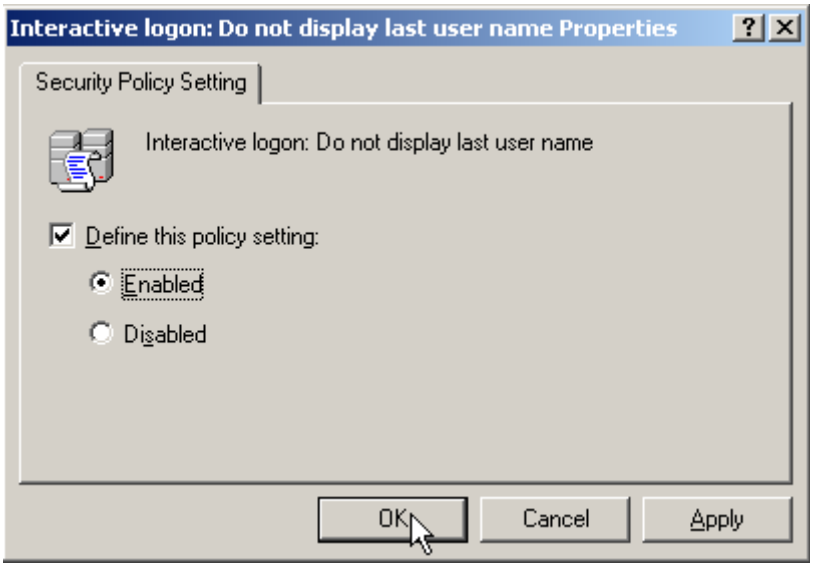


Hình 5.56: Chính sách Interactive logon: Do not require CTRL+ALT+DEL.

- Check **Enable => OK**.

➢ **Chỉnh không cho hiển thị tên người dùng logon trước đó:**

- Ta vào mục **Interactive logon: Do not display last user name.**



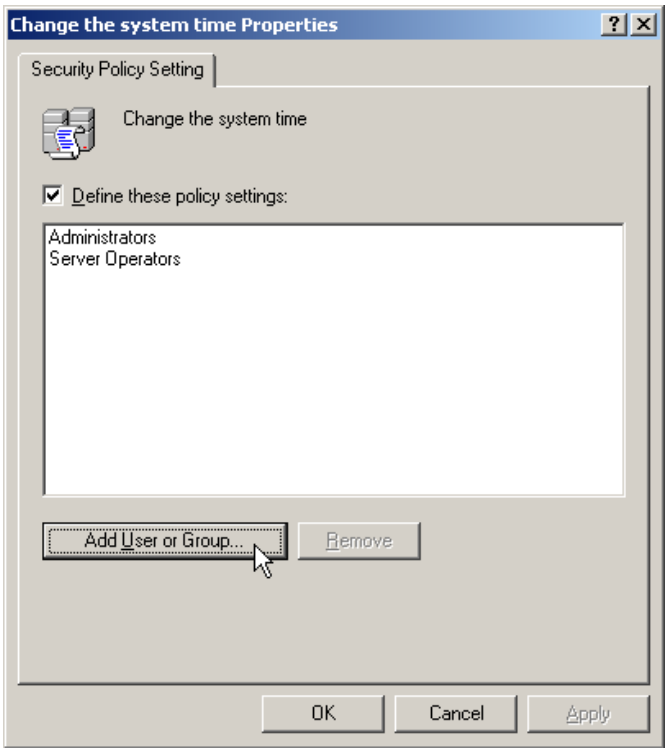
Hình 5.57: Chính sách Interactive logon: Do not display last user name.

- Chọn **Enable => OK**.

- Vào **Start** => **Program** => **Administrator tools** =>**Domain Controller Security Policy**. Tại cửa sổ **Default Domain Controller Security Settings**, nhấp chuột vào dấu cộng tại **Local policies** => **User Right Assignment**.

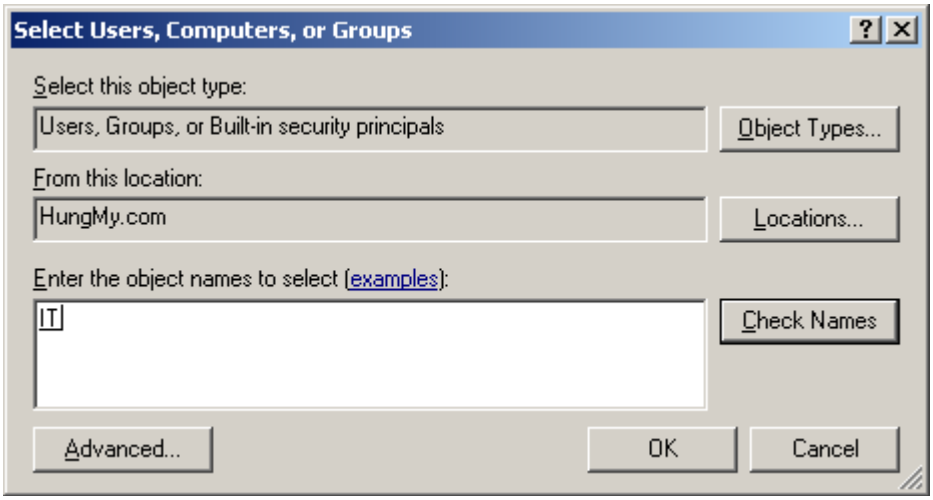
➢ **Cho phép người dùng được thay đổi giờ hệ thống của máy tính :**

- Ta tìm chính sách có tên là **Change the system time**.



Hình 5.58: Chính sách Change the system time.

- Vào **Add user or Group** => chọn **Browse...** để chọn user hay group add vào.

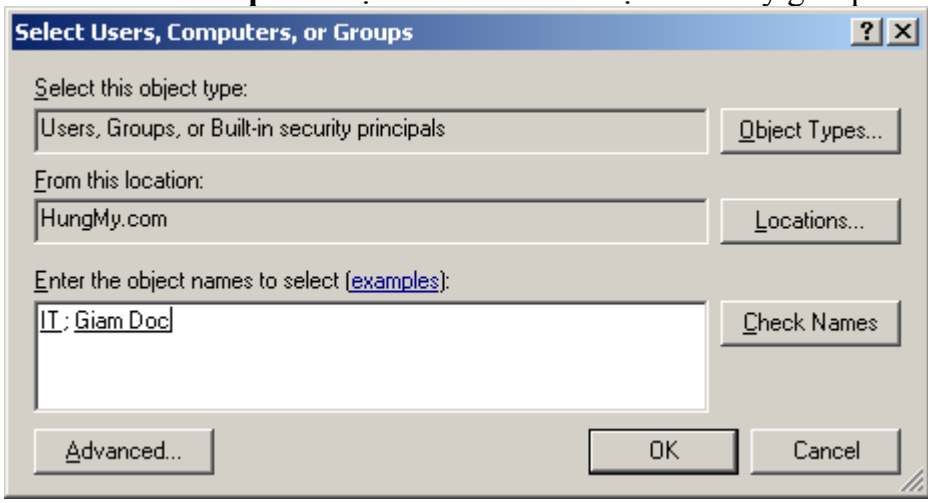


Hình 5.59: Add User, Group vào.

- Ta chọn nhóm IT có quyền thay đổi giờ hệ thống của máy Domain Controller.

➢ **Cho phép người dùng shutdown hệ thống** :

- Ta tìm chính sách có tên là **Shut down the system**.
- Vào **Add user or Group** => chọn **Browse...** để chọn user hay group add vào.



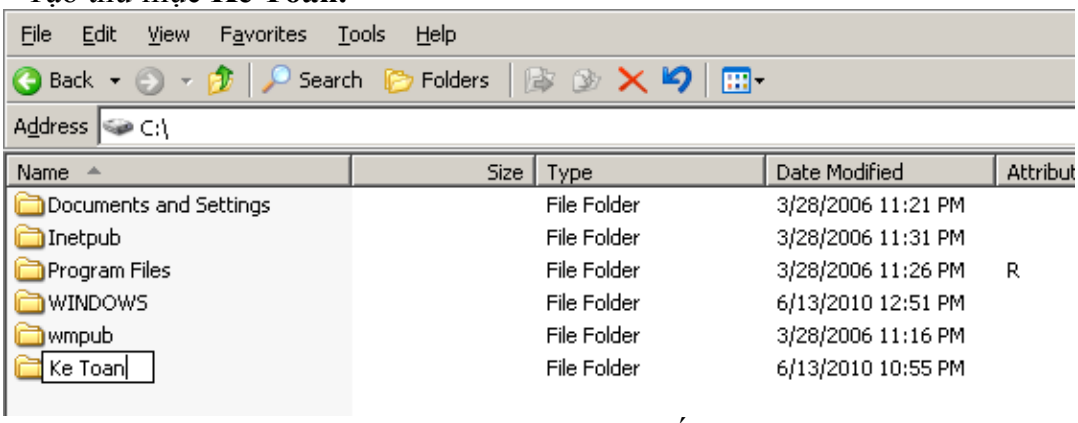
Hình 5.60: Add User, Group vào.

- Ta chọn nhóm IT và nhóm Giám đốc có thể tắt hệ thống Domain.

5.8. ÁNH XẠ Ổ ĐỈA:

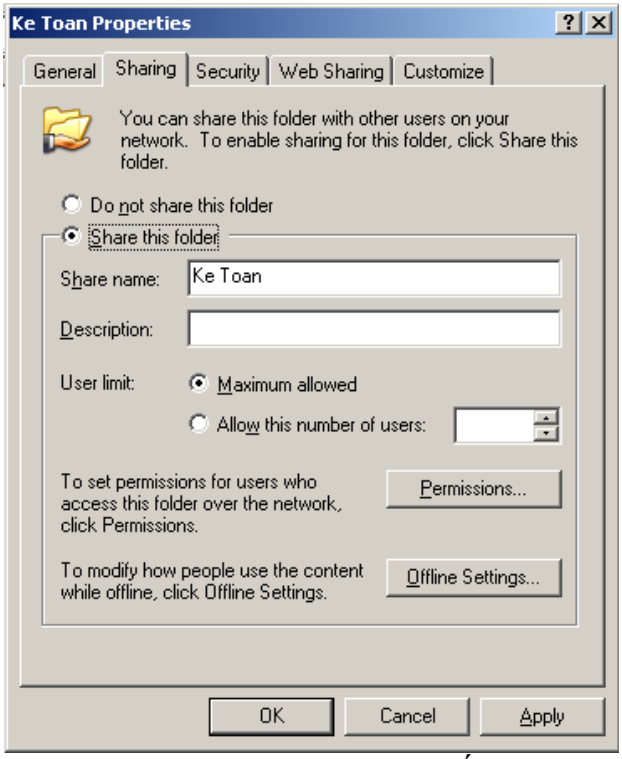
5.8.1. TRÊN SERVER:

- Tạo thư mục **Kế Toán.**



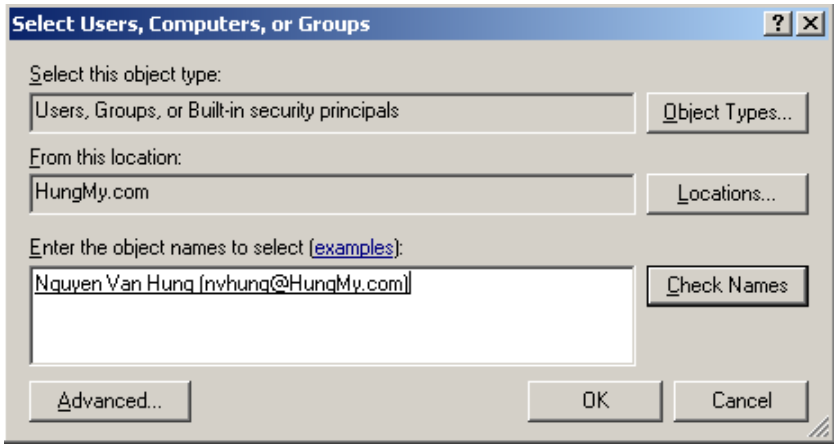
Hình 5.61: Tạo thư mục Kế Toán.

- Click chuột phải vào thư mục **Ke Toan** => **Properties =>** chuyển qua tab **Sharing** => chọn **share this folder**. Trong cửa sổ **Advance Security Settings** chọn tab **Permission.**



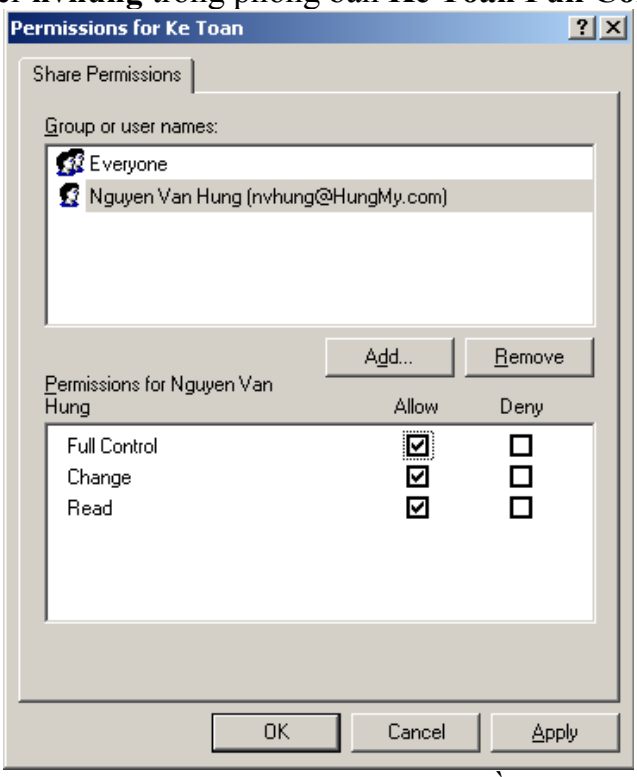
Hình 5.62: Share thư mục Kế Toán.

- Chọn **Permissions…** => Trong tab **Share Permissions** chọn **Add =>** nhập vào user hoặc group **Kế Toán.**



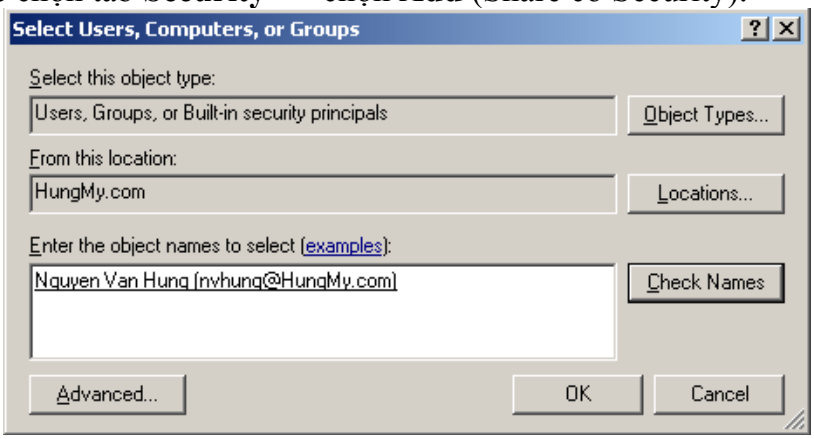
Hình 5.63: Add user nvhung

- Check cho user **nvhung** trong phòng ban **Kế Toán Full Control** quyền.



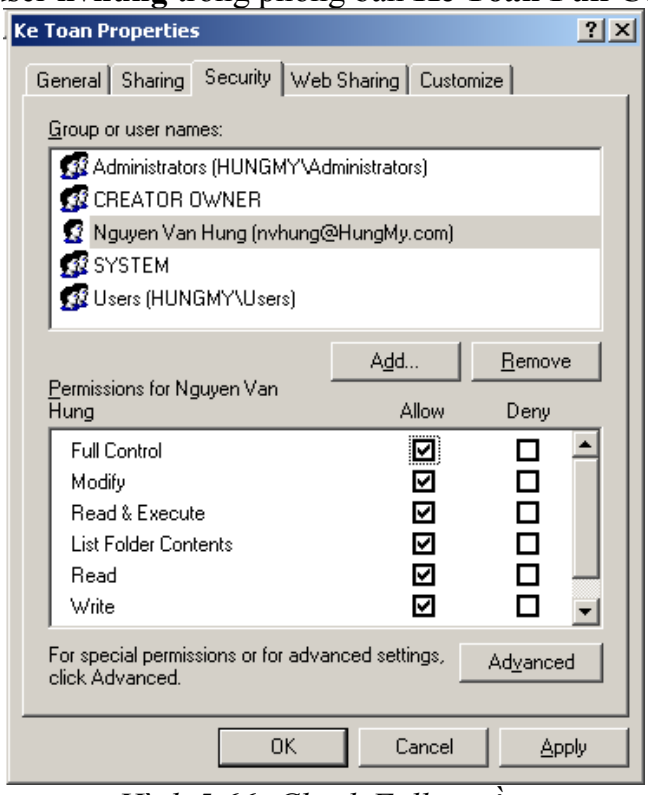
Hình 5.64: Check Full quyền.

- Tiếp tục chọn tab **Security** => chọn **Add** (Share có Security).



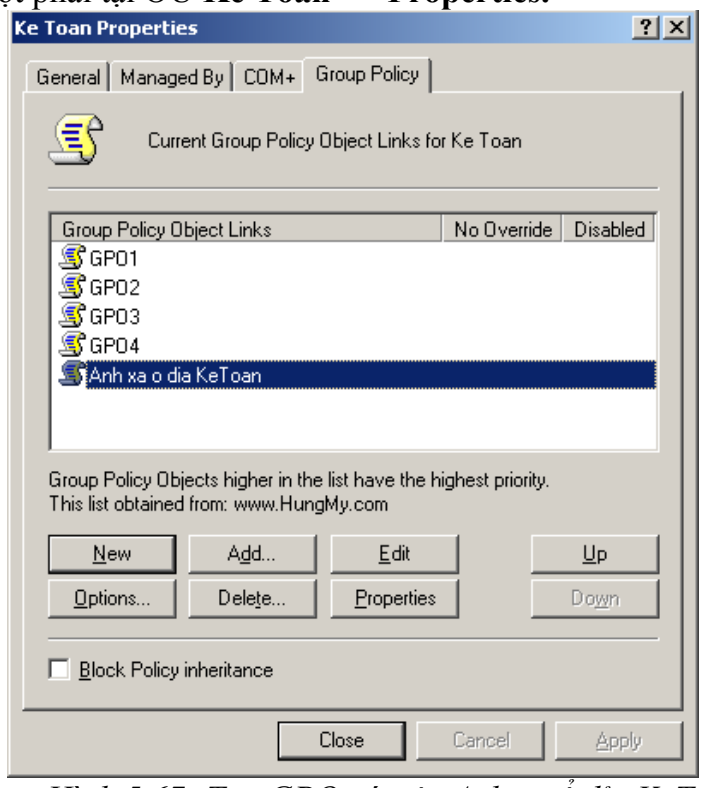
Hình 5.65: Add user nvhung vào

- Check cho user **nvhung** trong phòng ban **Kế Toán Full Control** quyền.



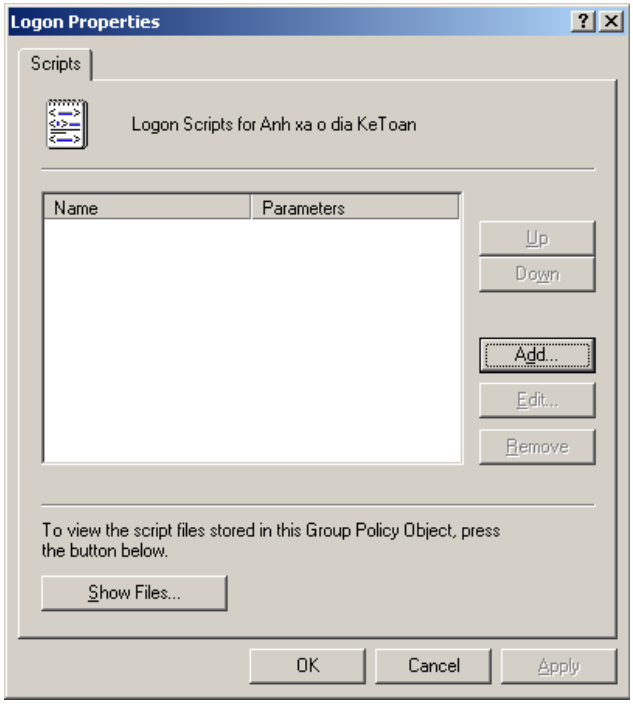
Hình 5.66: Check Full quyền.

- Vào **Start** => **Program** => **Administrator tools** => **Active Directory users and Computer**.
- Click chuột phải tại OU **Ke Toan** => **Properties.**



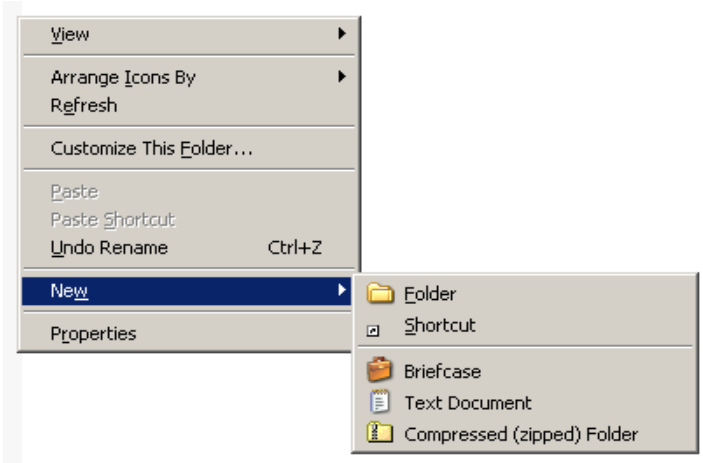
Hình 5.67: Tạo GPO với tên Anh xạ ổ đĩa KeToan.

- Chọn Tab **Group Policy**, chọn new để tạo một **Group Policy Object**(GPO) với tên là **Anh xạ ổ đĩa KeToan**. Tiếp theo chọn **Edit** để chỉnh sửa chính sách.
- Tại cửa sổ **Group Policy Object Editor** ta vào **User configuration** => **Windows Settings** => **Scripts(Logon/Logoff)**. Chọn chính sách **Logon.**

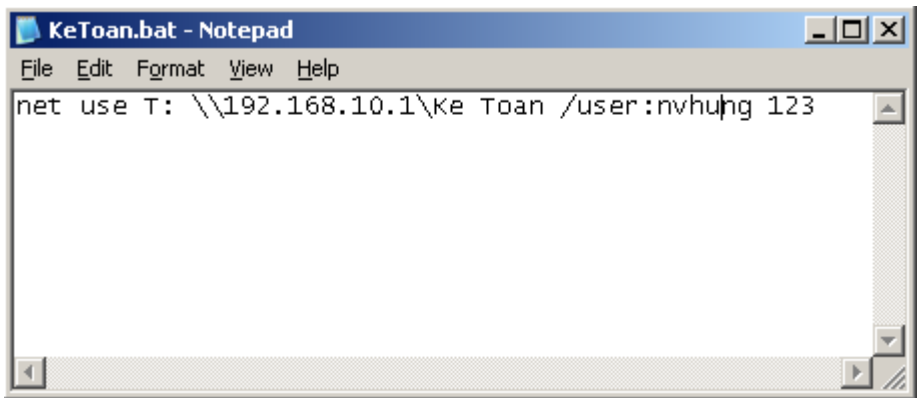


Hình 5.68: Logon

- Chọn Show Files…

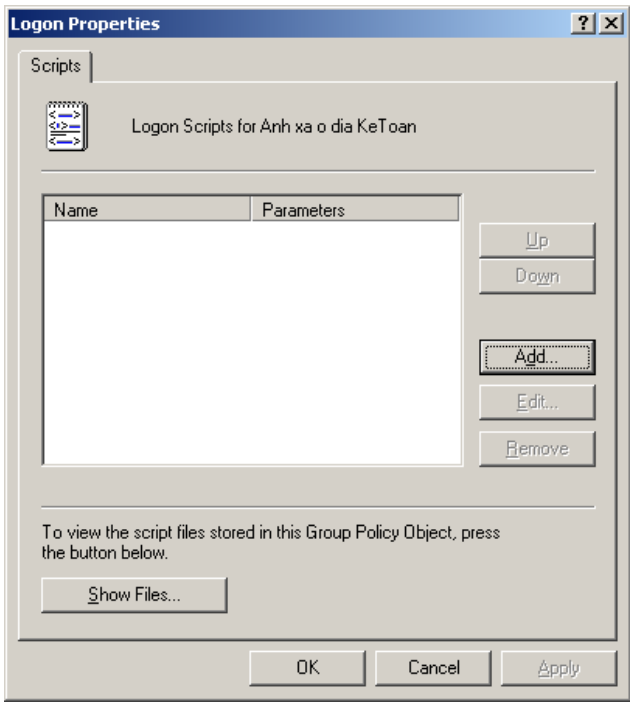


*Hình 5.69: Tạo file text với đuôi **.bat***

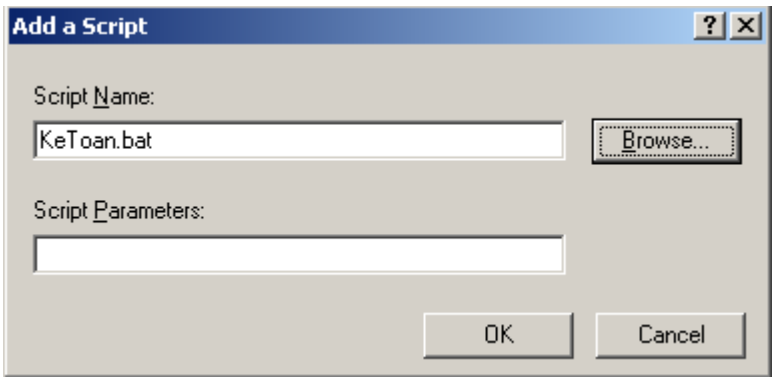


*Hình 5.70: Tạo file **KeToan.bat***

- Click vào **Add** để Add file **KeToan.bat** vừa tạo.

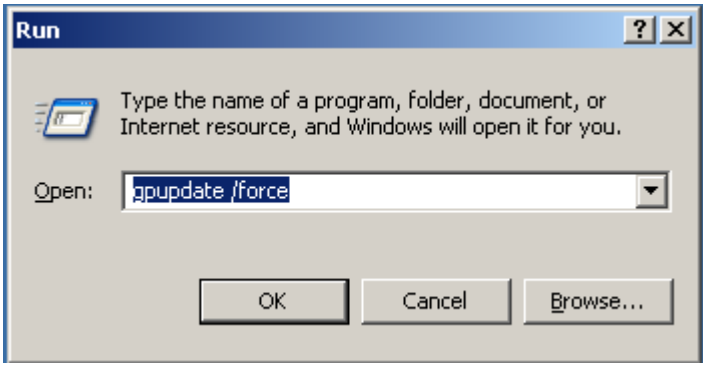


- Chọn **Browse** đến file **KeToan.bat** vừa tạo.



*Hình 5.71: Add file **KeToan.bat***

- Chọn **Ok** => **Ok** => **Close.**
- **Vào Start => Run.**

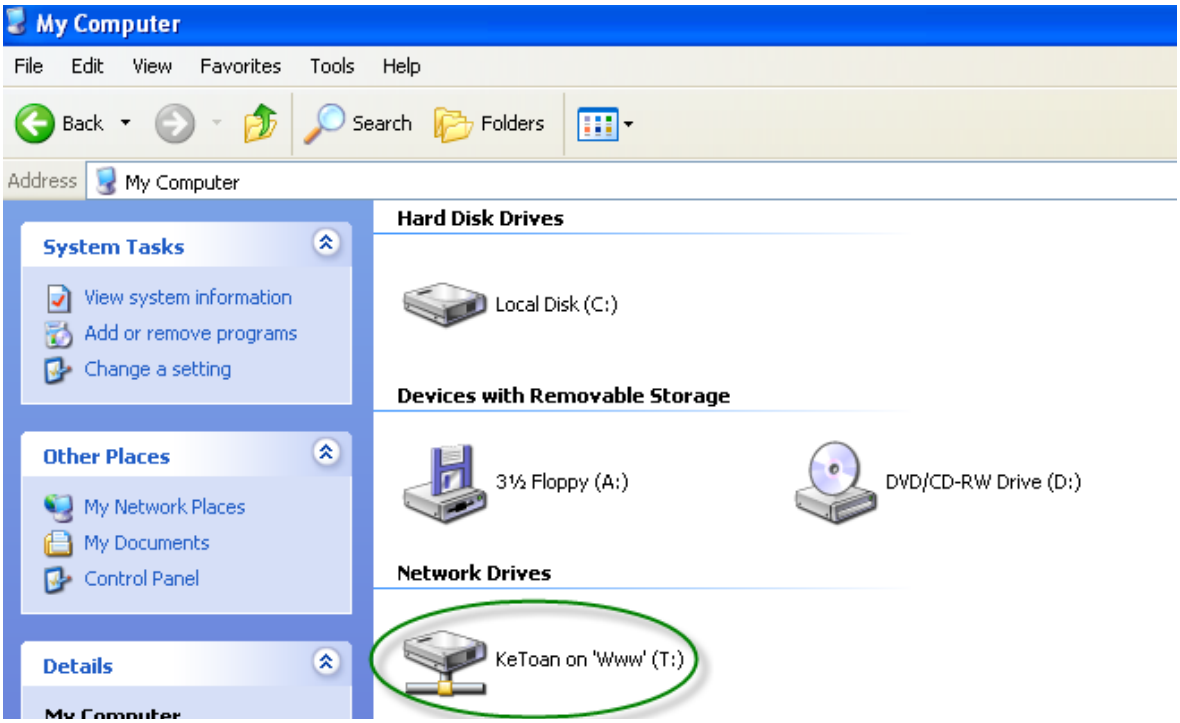


Hình 5.72: update policy

- Chọn **Ok** để hoàn tất.

5.8.2. TRÊN CLIENT:

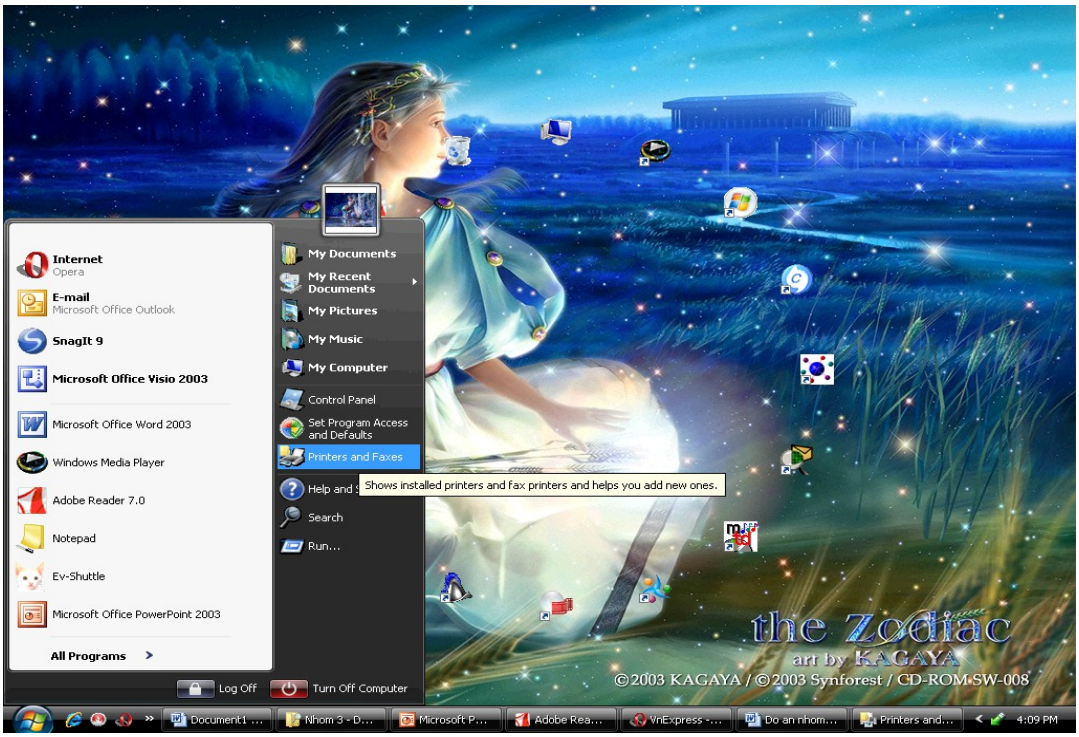
- Ta Logon user **nvhung** thuộc phòng ban **Kế Toán** thì sẻ thấy **ổ đĩa T** vừa tạo ánh xạ.



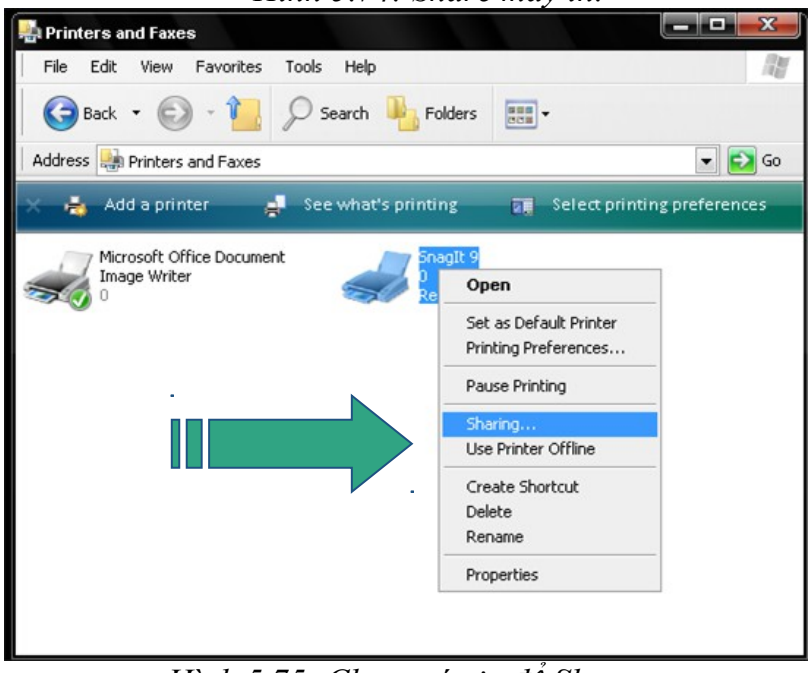
Hình 5.73: Ổ đĩa T vừa ánh xạ.

5.9. SHARE MÁY IN DÙNG CHUNG:

- Vào **Start => Printers and Faxes** hoặc **Strat => Control Panel chọn Printer and Faxes.**

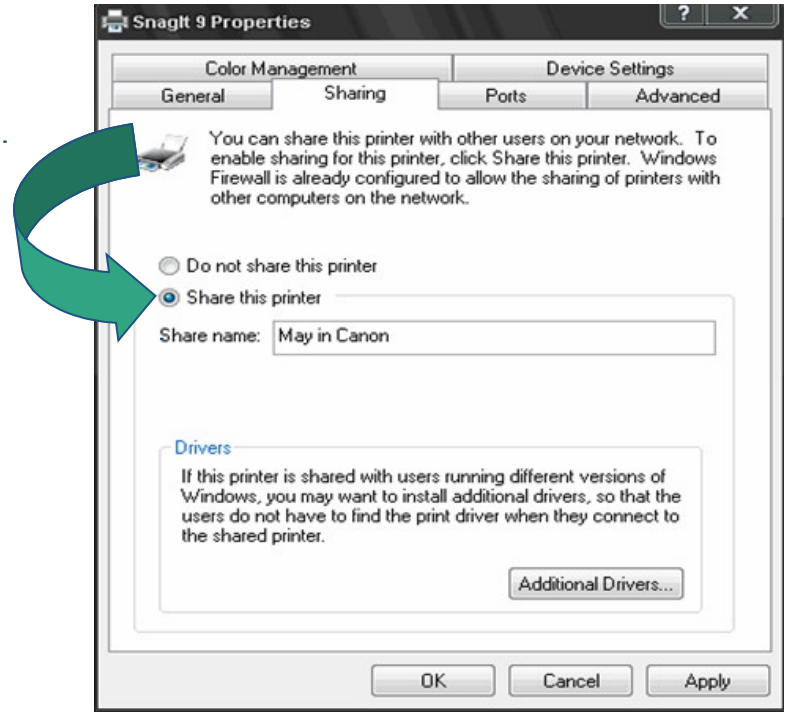


Hình 5.74: Share máy in.



Hình 5.75: Chọn máy in để Share.

- Click phải chuột vào máy in => chọn **Share** (Hình 5.75)

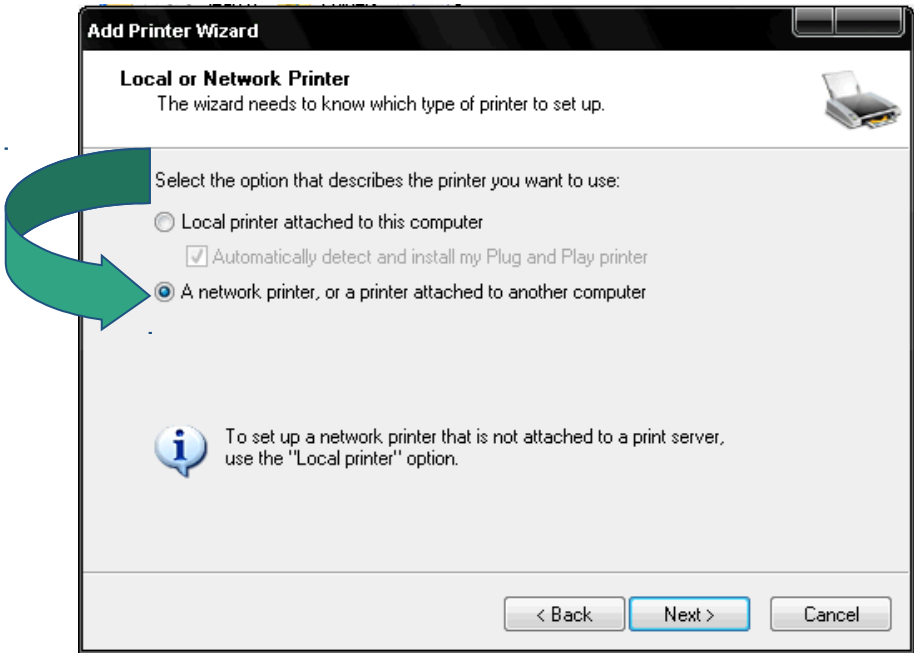


Hình 5.76: Đặt tên máy in.

- Trong menu **Properties** của máy in, vào thẻ **Sharing**, nhấn nút hình tròn bên cạnh dòng **Share this printer** và đặt tên cho máy là **Máy in Canon** để dễ nhận biết. Nhấn **OK** khi hoàn thành.
- Trên từng máy tính **Client**, bạn thêm máy in này bằng cách vào **Control Panel** => **Printers and Faxes** => nhấn đúp vào **Add a printer** => một cửa sổ xuất hiện => chọn **Next**.

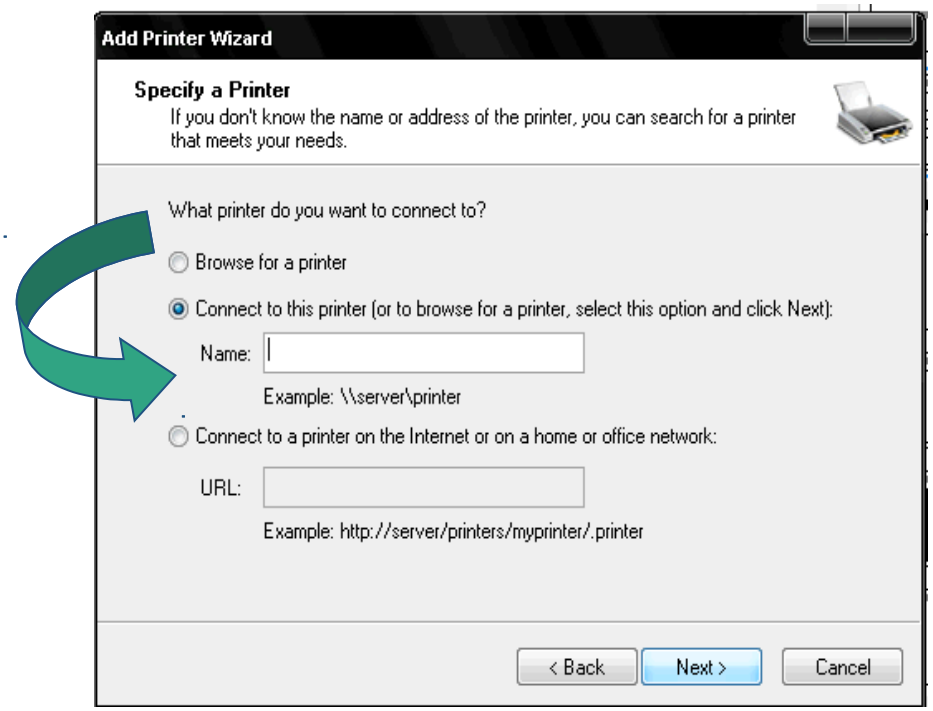
Hình 5.77: Add máy in cho các máy client trong mạng

- Đánh dấu vào **A network printer or a printer attached to another computer(Máy in qua mạng)** => Chọn **Next**.



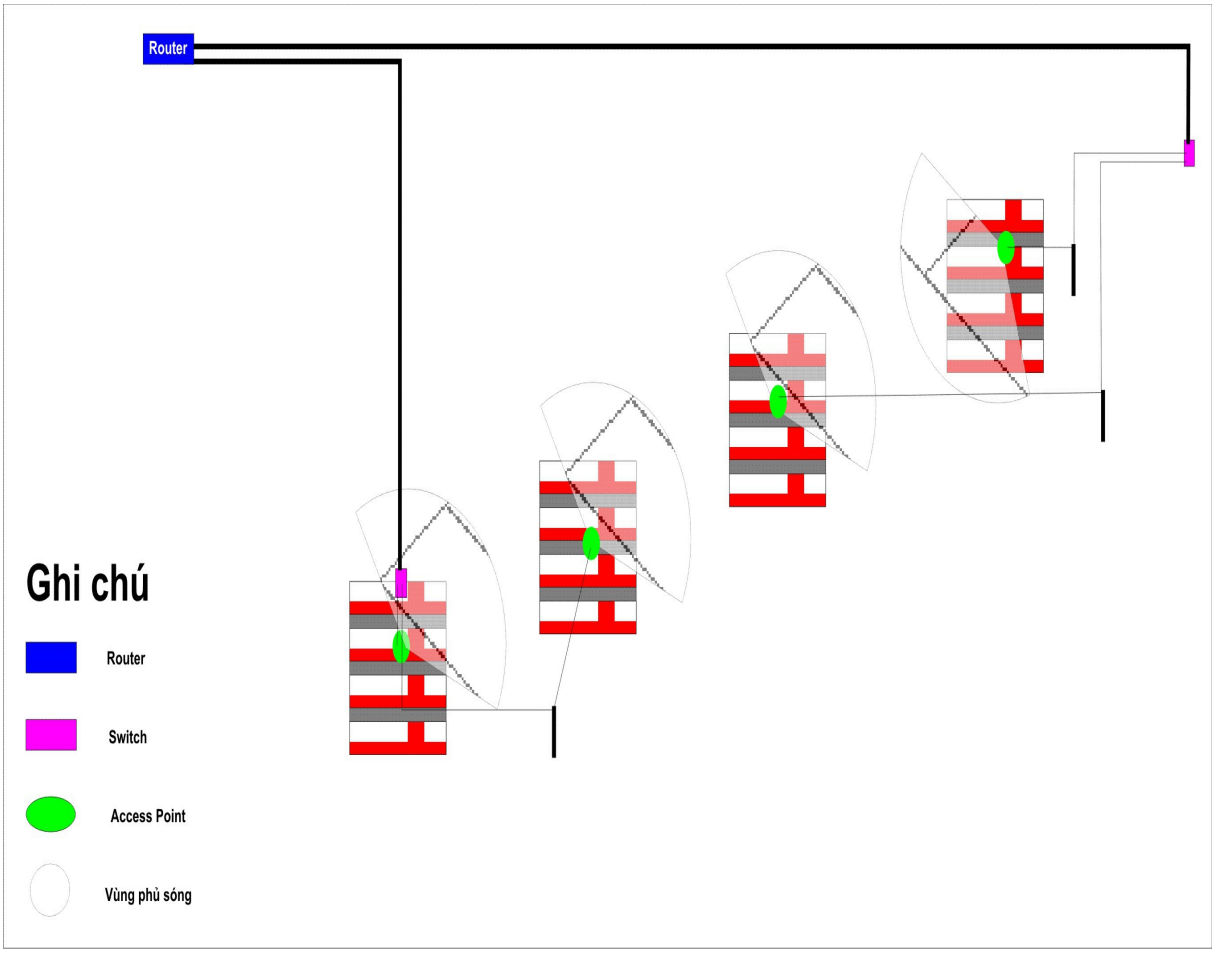
Hình 5.78: Chcek vào mục máy in qua mạng.

- Chọn **Connect to this printer** và gõ vào đường dẫn đến máy in theo cấu trúc nhấn **Next** để hoàn tất.



Hình 5.79: Nhập tên Share máy in vào

5.10. THIẾT KẾ MẠNG & GIẢI PHÁP BẢO MẬT CHO MẠNG WIRELESS:



Hình 5.80: Mô hình logic của mạng Wireless

Trong khi cấu hình các thiết bị không dây cần chú ý:

a/ Cấu hình router không dây

Hãy sử dụng một cáp mạng đi kèm với router không dây, bạn cần tạm kết nối máy tính của mình tới một trong những cổng còn trống của router không dây (bất cứ cổng nào mà không có nhãn Internet, WAN, hoặc WLAN). Bạn hãy bật máy của mình, PC của bạn sẽ tự động kết nối vào router.

Mở IE và gõ địa chỉ IP để cấu hình router, có thể sẽ phải gõ mật khẩu. Tên mật khẩu và địa chỉ sẽ rất khác nhau, phụ thuộc vào router mà bạn mua, bạn cần xem hướng dẫn trong tài liệu đi kèm. Bảng dưới đây là một cấu hình các địa chỉ, tên mật khẩu thường được sử dụng mặc định của hãng sản xuất.

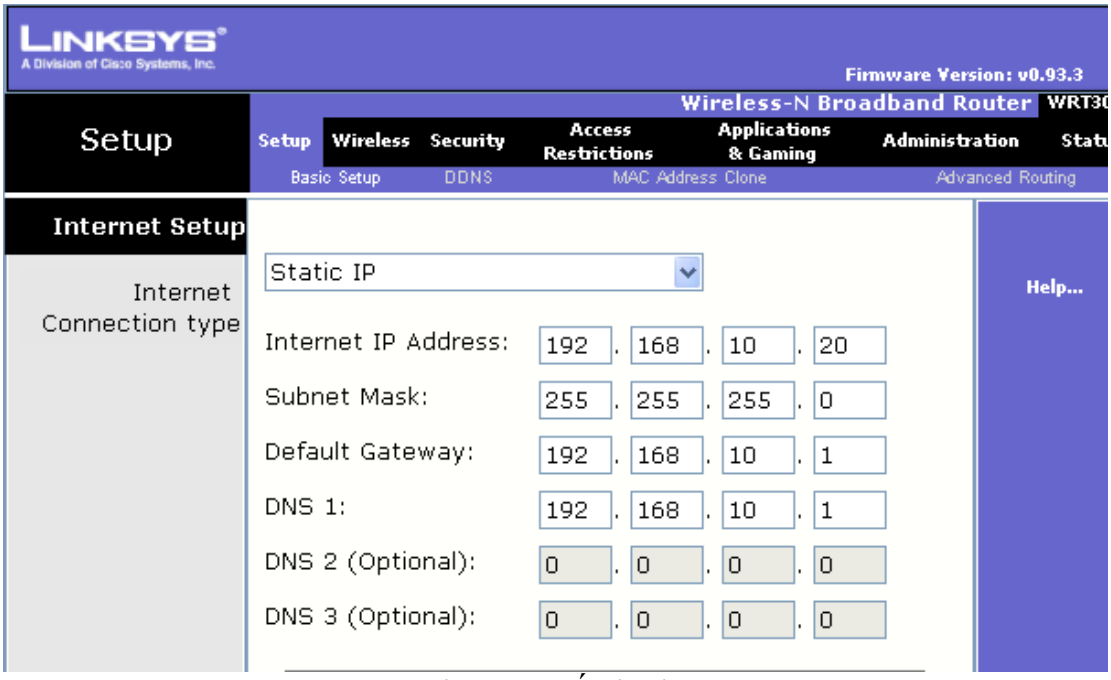
Router	Address	Username	Password
3Com	http://192.168.1.1	admin	admin
Linksys	http://192.168.1.1	admin	admin
Netgear	http://192.168.0.1	admin	password

IE sẽ hiển thị trang cấu hình router của bạn. Hầu hết các cấu hình mặc định đều tốt, tuy nhiên bạn cần chú ý:

- **Tên mạng không dây, thường gọi là SSID**: Cái tên này xác định mạng của bạn. Do đó, cần phải đặt tên khác và không giống như cái tên mà hàng xóm của bạn đang sử dụng.
- **Mã hóa không dây WEP, và bảo vệ truy cập không dây (WPA):** sẽ giúp mạng không dây của bạn bảo mật hơn. Hầu hết các router, bạn cần cung cấp vì kí tự để router của bạn tự sinh các khóa. Bạn hãy gõ các kí tự này duy nhất đừng lặp lại (bạn cũng không cần phải nhớ các kí tự này). Sau đó bạn hãy ghi lại các khóa mà router tự sinh.
- **Mật khẩu quản trị, chìa khóa cấu hình mạng không dây:** Cũng giống như các mật khẩu khác, mật khẩu cho router không thể là một từ nào đó trong từ điển, nó cần phải là sự kết hợp các kí tự, số, biểu tượng. nhưng cũng rất quan trọng là bạn phải nhớ chúng, bởi bạn sẽ phải gõ mật khẩu khi đăng nhập để cấu hình lại router.
- Các bước cấu hình có thể rất khác giữa các router, nhưng bao giờ trong mỗi lần thiết lập cấu hình cũng là có các mục như: **Save Settings**, **Apply**, và **OK** để lưu lại các thay đổi của bạn. Bây giờ, bạn có thể tắt kết nối mạng từ máy bạn đang dùng để cấu hình.

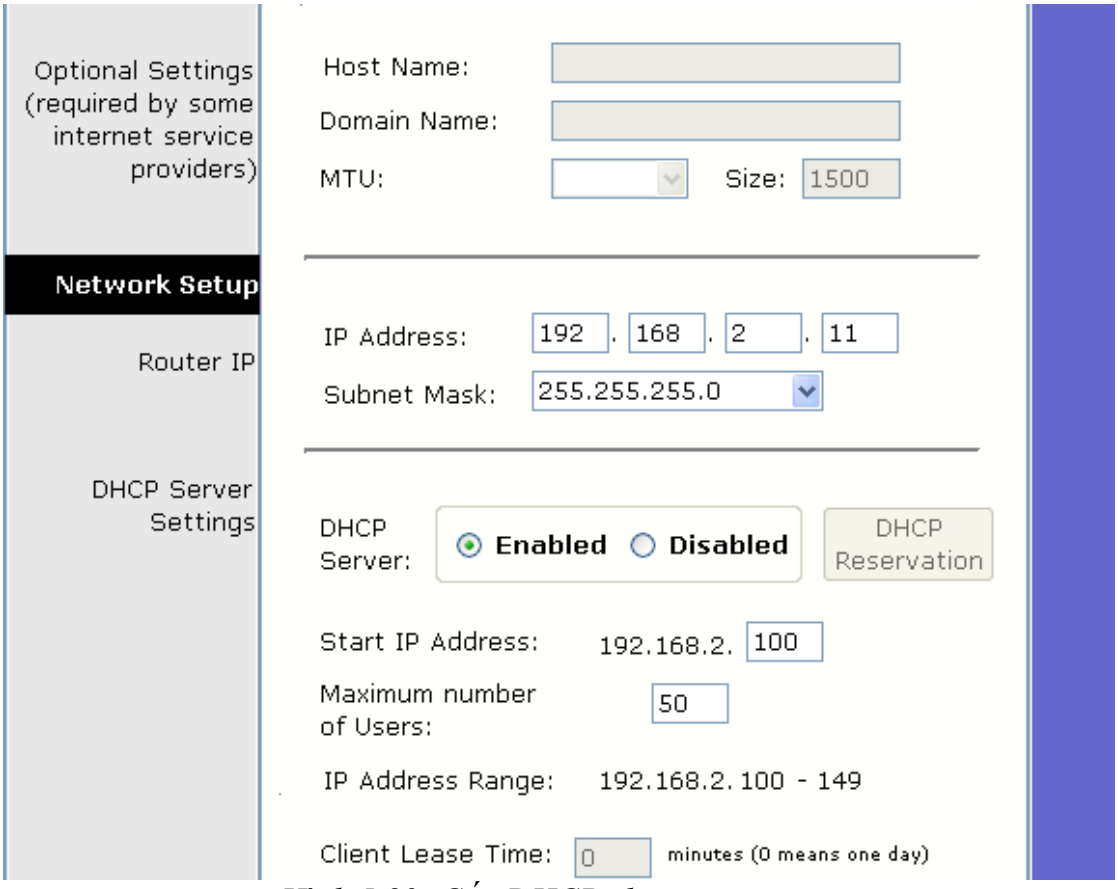
b/ Cấu hình AccessPoint & ISA server để cấp quyền truy cập internet và tài nguyên nội bộ cho nhân viên.

* Cấu hình DHCP của AP: Dùng máy 1 truy cập web cấu hình RouterWireless (http://192.168.1.1)



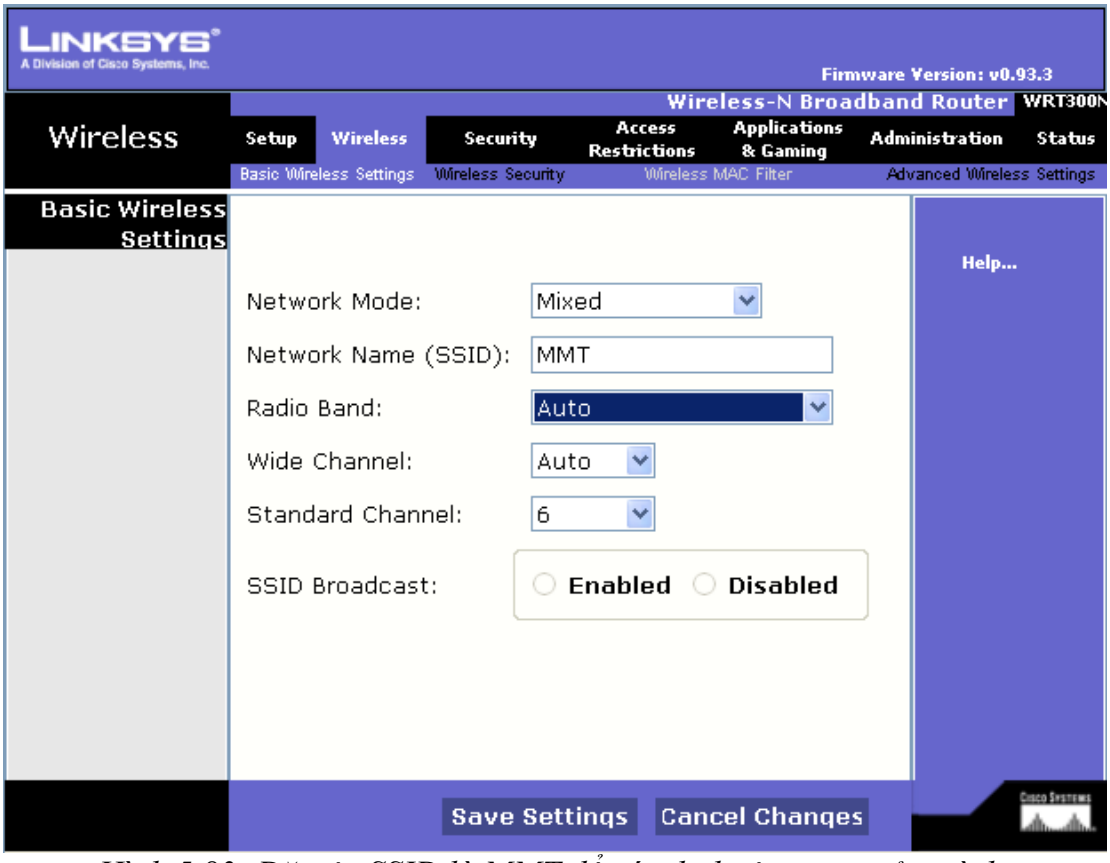
Hình 5.81: Cấu hình IP.

- Lan: IP address: 192.168.10.20, s.mask: 255.255.255.0, d.gateway: 192.168.10.1
- DHCP: start IP: 192.168.2.11 – end IP: 192.168.2.100

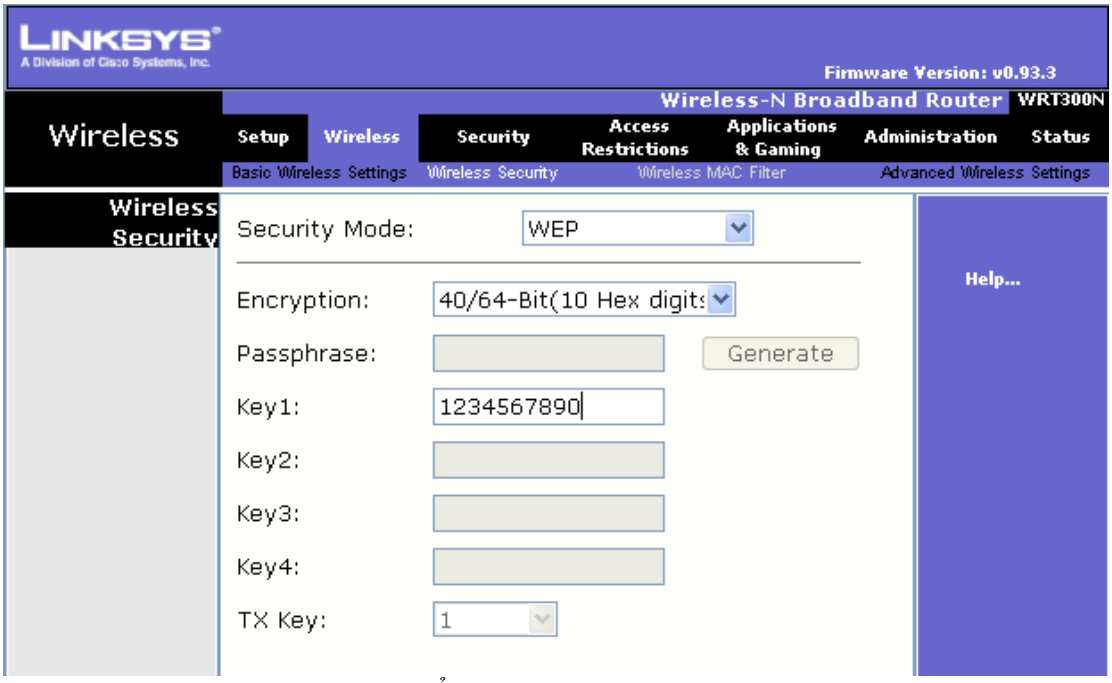


Hình 5.82: Cấp DHCP cho mạng trong.

- Cấu hình Wireless trên RouterWireless:

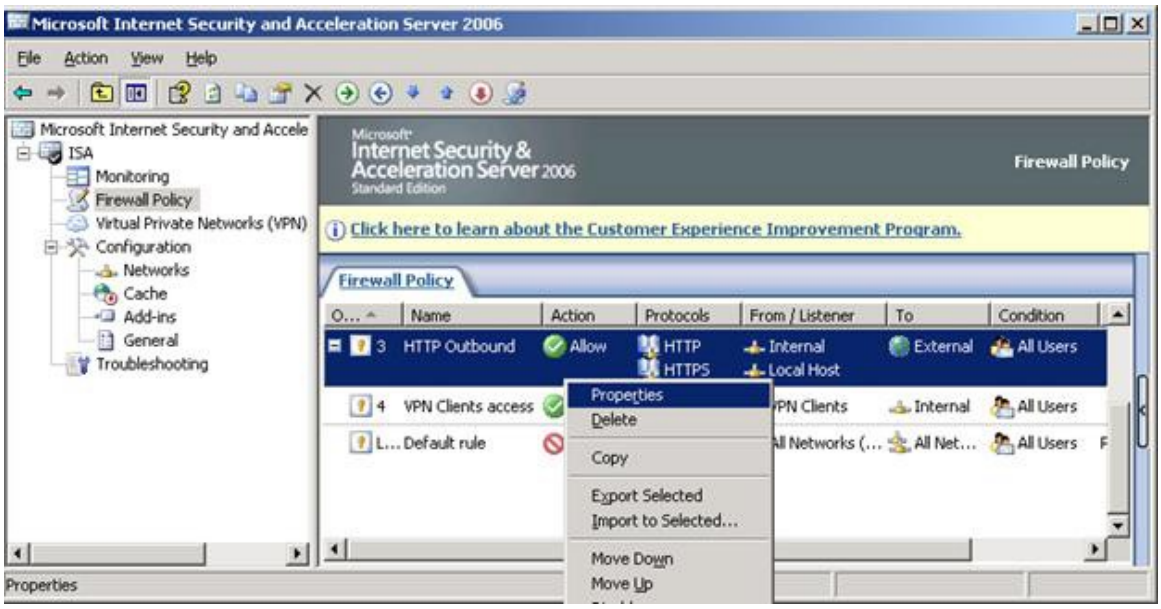


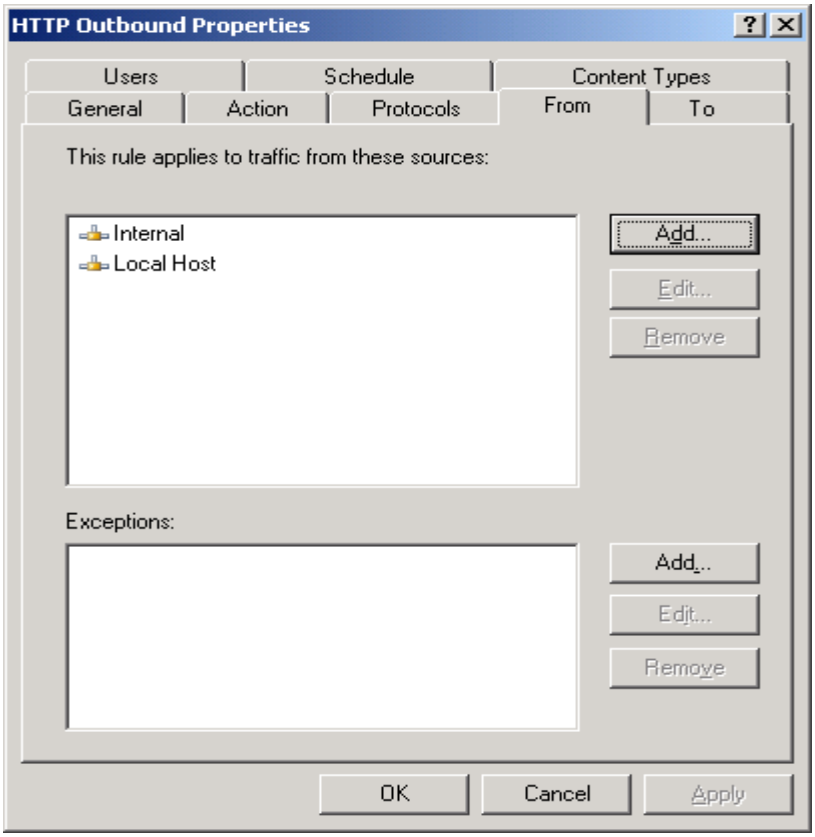
Hình 5.83: Đặt tên SSID là MMT để xác định tên mạng của mình.

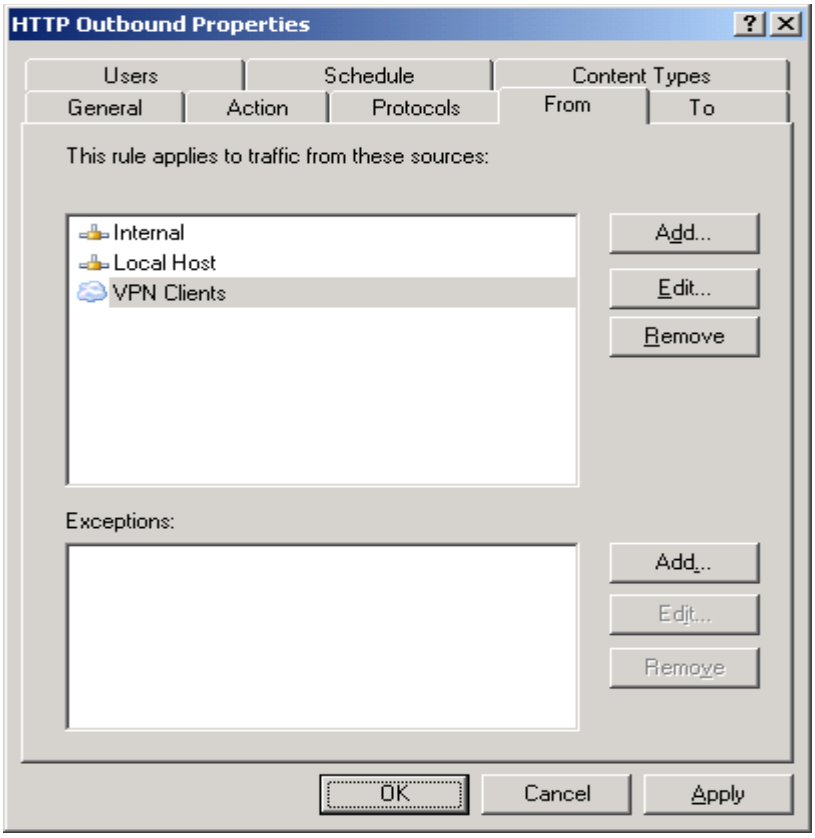


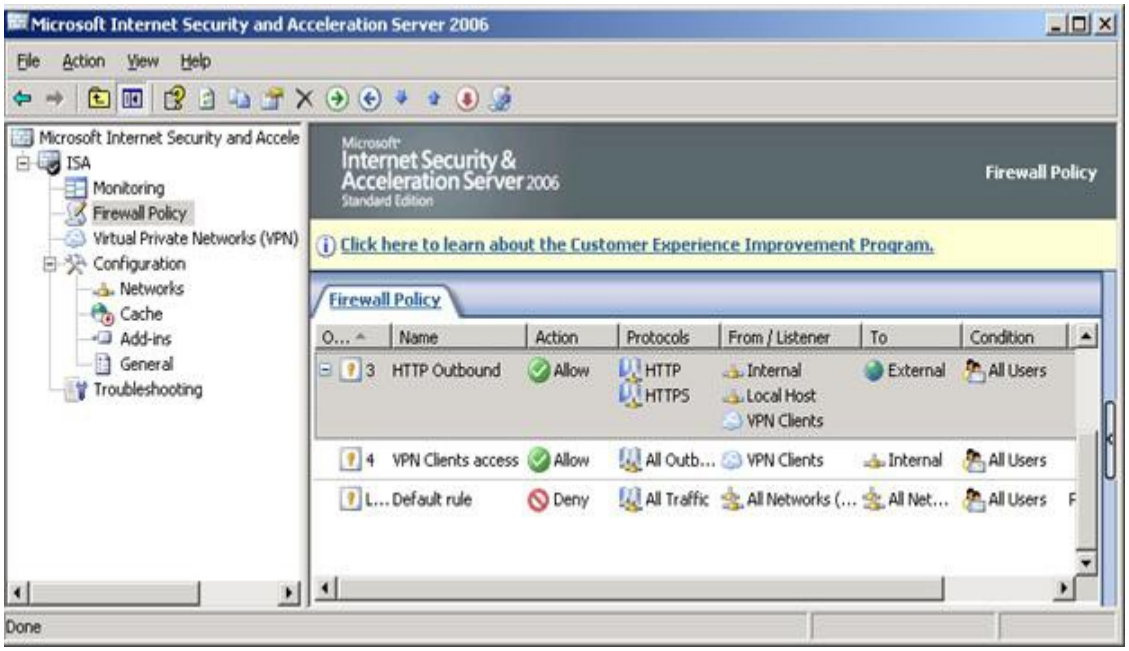
Hình 5.84: chọn kiểu chứng thực là Web nhập vào key1

* Thực hiện tại máy 2: **Log on Domain Administrator**. Điều chỉnh access rule "HTTP outbound", tab "From": thêm network "VPN Clients"









* Thực hiện tại máy 3: **Log on Administrator**.

Giả lập laptop nhân viên:

b1. Ngắt kết nối AP.

b2. Tạo conection VPN kết nối server 192.168.10.1 (ISA)

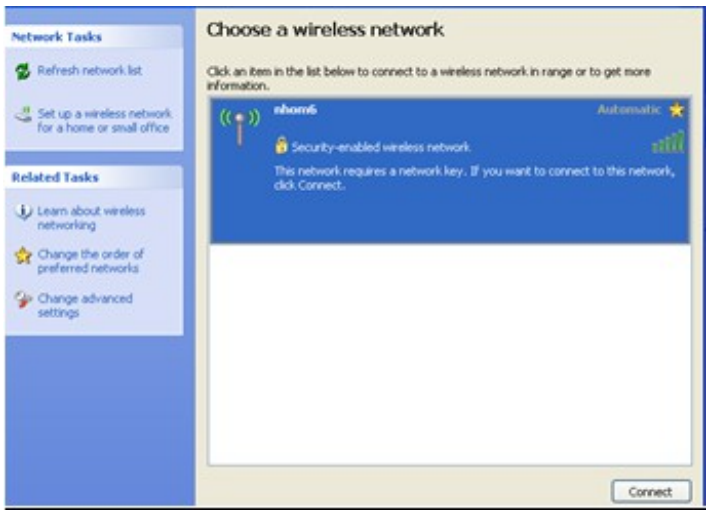
b3. Kết nối AP.

b4. Kết nối VPN. Username: **nvhung**, password: **123**

b5. Truy cập dữ liệu trên M1 (DC).

b6. Truy cập internet.

c/ Cấu hình máy Client kết nối vào mạng Wireless :

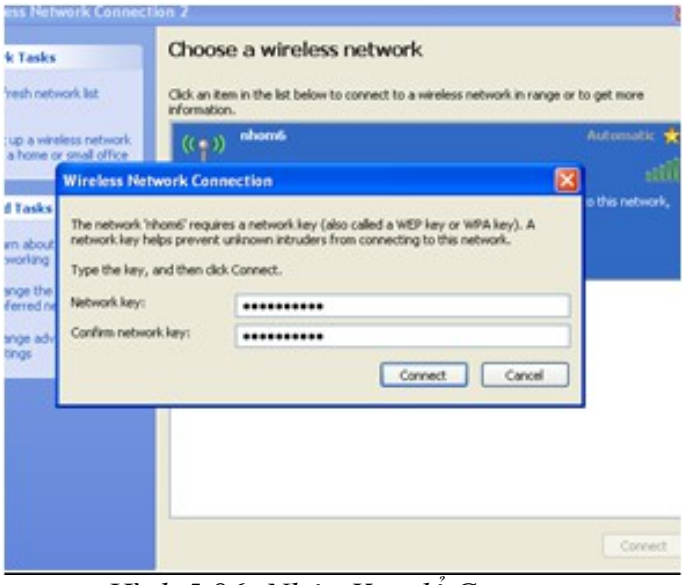


Hình 5.85: Connect máy Client vào mạng Wireless.

- Sau khi **Save Setting** trong phần cấu hình Wireless xong.
- Máy Client (có card mạng wireless như Laptop, card mạng USB…) chọn mục **Refesh network list** bên trái cửa sổ **Wireless Network Connection**
- Thấy tên **SSID** mà mình đặt để phân biệt hiện ra có thêm biểu tượng ổ khóa. Chọn vào nhóm số máy mình và nhấn **Connect**.

→ Khi đó xuất hiện hộp thoại yêu cầu nhập key vào

Ta nhập 2 lần số **key**: **1234567890**



Hình 5.86: Nhập Key để Connect.

- Sau đó nhấn nút **Connect**
- Quá trình kết nối thành công và ta truy cập internet được bằng **Security = WEP**

Giải pháp wireless cho công ty đáp ứng được:

- Không làm ảnh hưởng đến hạ tầng kiến trúc căn phòng
- Cung cấp kết nối tạm thời với mạng cáp có sẵn: người sử dụng mạng wireless có thể truy nhập thông tin thời gian thực tại bất kỳ nơi nào trong phòng mà không cần quan tâm đến chỗ cắm card mạng.
- Cài đặt rất nhanh chóng và dễ dàng hơn nhiều so với mạng cáp (wired).
- Giá hạ hơn so với mạng cáp mà vẫn đảm bảo tốc độ và chất lượng cuộc truyền
- Hỗ trợ khả năng mở rộng mạng một cách nhanh chóng và linh động

Số người trong phòng cùng truy nhập đồng thời vào mạng cáp để sử dụng các dịch vụ được cung cấp qua thiết bị Access Point lên tới 2048 người với mỗi người là đại diện cho một thiết bị đầu cuối. Điều này đặc biệt hữu ích trong trường hợp một cuộc hội thảo, cuộc họp hay buổi đào tạo được tổ chức tại đây. Mọi người đều có thể đồng thời truy nhập vào mạng qua thiết bị Access Point với các máy tính được cài Client Adapter phù hợp.

TÀI LIỆU THAM KHẢO

[1] Nguyễn Hồng Sơn, *Kỹ thuật truyền số liệu*, NXB Lao động Xã hội.

[2] Trần Văn Thành – Mang Thành Trung, *Quản Trị Windows Server 2003*, ĐH Quốc Gia Tp.Hồ Chí Minh - Trường ĐH Khoa Học Tự Nhiên.

[3] Phan Mai Linh, *Bài giảng An toàn mạng*, Khoa Công Nghệ Thông Tin CĐ Công Nghệ Thông Tin.

[4] Building A Cisco Wireless LAN *(Syngress Publishing 2002).*

[5] Các Website :

- http://www.wlana.com
- http://phutran.tk
- http://www.quantrimang.com
- http://www.cuocsongso.com.vn
- http://www.haiphongit.com.vn
- http://www.nhatnghe.com.vn
- http://www.adminviet.com.net (CCNA4_full)
- http://www.3c.com.vn