

TRƯỜNG CAO ĐẲNG NGHỀ CÔNG NGHIỆP HÀ NỘI

Tác giả: Nguyễn Thái Hà (chủ biên).

Lê Văn Úy.



GIÁO TRÌNH

Công nghệ mạng không dây

(Lưu hành nội bộ)

Hà Nội năm 2012

Tuyên bố bản quyền

Giáo trình này sử dụng làm tài liệu giảng dạy nội bộ trong trường cao đẳng nghề Công nghiệp Hà Nội

Trường Cao đẳng nghề Công nghiệp Hà Nội không sử dụng và không cho phép bất kỳ cá nhân hay tổ chức nào sử dụng giáo trình này với mục đích kinh doanh.

Mọi trích dẫn, sử dụng giáo trình này với mục đích khác hay ở nơi khác đều phải được sự đồng ý bằng văn bản của trường Cao đẳng nghề Công nghiệp Hà Nội

LỜI GIỚI THIỆU

Trong những năm qua, dạy nghề đã có những bước tiến vượt bậc cả về số lượng và chất lượng, nhằm thực hiện nhiệm vụ đào tạo nguồn nhân lực kỹ thuật trực tiếp đáp ứng nhu cầu xã hội. Cùng với sự phát triển của khoa học công nghệ trên thế giới, lĩnh vực Công nghệ thông tin nói chung và ngành Quản trị mạng ở Việt Nam nói riêng đã có những bước phát triển đáng kể.

Chương trình khung quốc gia nghề Quản trị mạng đã được xây dựng trên cơ sở phân tích nghề, phân kỹ thuật nghề được kết cấu theo các môđun. Để tạo điều kiện thuận lợi cho các cơ sở dạy nghề trong quá trình thực hiện, việc biên soạn giáo trình kỹ thuật nghề theo theo các môđun đào tạo nghề là cấp thiết hiện nay.

Mô đun 26: Công nghệ mạng không dây là mô đun đào tạo nghề được biên soạn theo hình thức tích hợp lý thuyết và thực hành. Trong quá trình thực hiện, nhóm biên soạn đã tham khảo nhiều tài liệu Quản trị mạng trong và ngoài nước, kết hợp với kinh nghiệm trong thực tế.

Mặc dầu có rất nhiều cố gắng, nhưng không tránh khỏi những khiếm khuyết, rất mong nhận được sự đóng góp ý kiến của độc giả để giáo trình được hoàn thiện hơn.

Xin chân thành cảm ơn!

Tháng 02 năm 2012

Nhóm biên soạn

MỤC LỤC

Đề mục	Trang
I. Lời giới thiệu	1
II. Mục lục	2
III. Nội dung mô đun	3
Bài 1 Tổng quan về mạng không dây	5
Bài 2 Các tầng mạng không dây	21
Bài 3 Kiến trúc mạng không dây	38
Bài 4 Bảo mật mạng không dây	45
IV. Tài liệu tham khảo	60

CHƯƠNG TRÌNH MÔ ĐUN ĐÀO TẠO CÔNG NGHỆ MẠNG KHÔNG DÂY

Mã số mô đun : MĐ39

Thời gian mô đun : 75 giờ;
(giờ)

(Lý thuyết 30 giờ, thực hành : 45

I. VỊ TRÍ, TÍNH CHẤT CỦA MÔ ĐUN

- Vị trí: Mô đun được bố trí sau khi sinh viên học xong các mô đun chuyên môn nghề ở trình độ cao đẳng
- Tính chất: Là mô đun đào tạo nghề bắt buộc.

II. MỤC TIÊU MÔ ĐUN:

- Biết được xu hướng sử dụng công nghệ mạng không dây trong thời đại mới;
- Thiết kế, xây dựng được các loại mô hình mạng không dây dạng ad-hoc và Infrastructure;
- Hiểu được các chuẩn của mạng không dây;
- Lắp đặt và cấu hình cho các thiết bị mạng không dây;
- Quản lý người dùng, nhóm người dùng và sử dụng được các tài nguyên chia sẻ trên mạng không dây;
- Biết được các giải pháp và kỹ thuật sử dụng để bảo mật cho mạng không dây
- Các kỹ thuật mở rộng hệ thống mạng không dây.
- Bố trí làm việc khoa học đảm bảo an toàn cho người và phương tiện học tập.

III. NỘI DUNG MÔ ĐUN :

1. Nội dung tổng quát và phân phối thời gian:

Số TT	Tên các bài trong mô đun	Thời gian			
		Tổng	Lý	Thực	Kiểm

		số	thuyết	hành	tra*
1	Tổng quan về mạng không dây	10	8	2	0
2	Các tầng mạng không dây	10	7	3	0
3	Kiến trúc mạng không dây	30	6	22	2
4	Bảo mật mạng không dây	25	9	15	1
	Cộng	75	30	42	3

YÊU CẦU VỀ ĐÁNH GIÁ HOÀN THÀNH MÔ ĐUN/MÔN HỌC

1. Phương pháp đánh giá:

Được đánh giá qua bài viết, kiểm tra vấn đáp hoặc trắc nghiệm, tự luận Phân biệt các chuẩn mạng không dây, kiến trúc mạng không dây, các hình thức bảo mật mạng không dây.

Dựa trên năng lực thực hành : trên cơ sở thực hành thiết lập mạng Adhoc, cấu hình AP; chia sẻ và quản trị được trên mạng không dây, đánh giá kỹ năng qua từng bài thực hành theo yêu cầu.

2. Nội dung đánh giá:

- Kiến thức:

Nắm được xu hướng sử dụng công nghệ mạng không dây trong thời đại mới

Thiết kế, xây dựng được các loại mô hình mạng không dây dạng ad hoc (là mạng không dây kết nối giữa các thiết bị đầu cuối mà không cần phải dùng các trạm thu phát gốc. Các thiết bị đầu cuối sẽ tự động bắt liên lạc với nhau để hình thành nên một mạng kết nối tạm thời dùng cho mục đích truyền tin giữa các nút mạng với nhau) và Infrastructure (Là một mạng có cấu trúc gồm các thiết bị không dây và thiết bị thu phát sóng)

Lắp đặt và cấu hình cho các thiết bị mạng không dây

Biết được các giải pháp và kỹ thuật sử dụng để bảo mật cho mạng không dây

Các kỹ thuật mở rộng hệ thống mạng không dây

- Kỹ năng:

Thiết kế, xây dựng và cấu hình được một hệ thống mạng không dây.

Cài đặt và cấu hình các chế độ bảo mật cho hệ thống mạng không dây

Chia sẻ dữ liệu trong mạng không dây

Chia sẻ kết nối Internet trong mạng Adhoc

- Thái độ:

Cẩn thận, thao tác nhanh chuẩn xác, tự giác trong học tập.

Có ý thức kỷ luật trong học tập, có tinh thần hợp tác, giúp đỡ lẫn nhau

Bài 1. TỔNG QUAN VỀ MẠNG KHÔNG DÂY

Mã bài : 39.1

Mục tiêu:

- Trình bày được khái niệm mạng không dây;
- Phân loại được các kiểu mạng không dây;
- Thiết lập được các ứng dụng mạng không dây;
- Mô tả được các chuẩn mạng không dây.
- Thực hiện các thao tác an toàn với máy tính.

Nội dung:

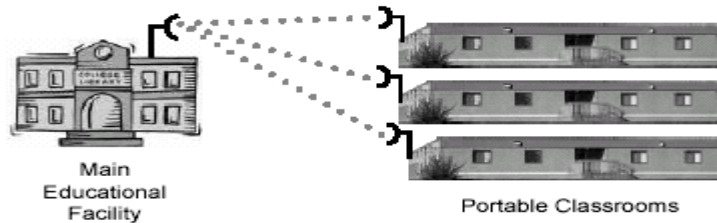
1. Lịch sử hình thành mạng không dây.

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

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

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

dụng mạng không dây, sẽ tránh được sự lan man và sẽ tiết kiệm thời gian và tiền bạc của công ty.



Hình 39.1 Mạng không dây trong trường học

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

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

Công nghệ WLAN lần đầu tiên xuất hiện vào cuối năm 1990, khi những nhà sản xuất giới thiệu những sản phẩm hoạt động trong băng tần 900Mhz. Những giải pháp này (không được thống nhất giữa các nhà sản xuất) cung cấp tốc độ truyền dữ liệu 1Mbps, thấp hơn nhiều so với tốc độ 10Mbps của hầu hết các mạng sử dụng cáp hiện thời.

- Năm 1992, những nhà sản xuất bắt đầu bán những sản phẩm WLAN sử dụng băng tần 2.4Ghz. Mặc dầu những sản phẩm này đã có tốc độ truyền dữ liệu cao hơn nhưng chúng vẫn là những giải pháp riêng của mỗi nhà sản xuất không được công bố rộng rãi. Sự cần thiết cho việc hoạt động thống nhất giữa các thiết bị ở những dãy tần số khác nhau dẫn đến một số tổ chức bắt đầu phát triển ra những chuẩn mạng không dây chung. Năm 1997, Institute of Electrical and Electronics Engineers(IEEE) đã phê chuẩn

sự ra đời của chuẩn 802.11, và cũng được biết với tên gọi WIFI (Wireless Fidelity) cho các mạng WLAN. Chuẩn 802.11 hỗ trợ ba phương pháp truyền tín hiệu, trong đó có bao gồm phương pháp truyền tín hiệu vô tuyến ở tần số 2.4Ghz.

- Năm 1999, IEEE thông qua hai sự bổ sung cho chuẩn 802.11 là các chuẩn 802.11a và 802.11b (định nghĩa ra những phương pháp truyền tín hiệu). Và những thiết bị WLAN dựa trên chuẩn 802.11b đã nhanh chóng trở thành công nghệ không dây vượt trội. Các thiết bị WLAN 802.11b truyền phát ở tần số 2.4Ghz, cung cấp tốc độ truyền dữ liệu có thể lên tới 11Mbps. IEEE 802.11b được tạo ra nhằm cung cấp những đặc điểm về tính hiệu dụng, thông lượng (throughput) và bảo mật để so sánh với mạng có dây.

- Năm 2003, IEEE công bố thêm một sự cải tiến là chuẩn 802.11g mà có thể truyền nhận thông tin ở cả hai dải tần 2.4Ghz và 5Ghz và có thể nâng tốc độ truyền dữ liệu lên đến 54Mbps. Thêm vào đó, những sản phẩm áp dụng 802.11g cũng có thể tương thích ngược với các thiết

2. Định nghĩa mạng không dây

WLAN là một loại mạng máy tính nhưng việc kết nối giữa các thành phần trong mạng không sử dụng các loại cáp như một mạng thông thường, môi trường truyền thông của các thành phần trong mạng là không khí. Các thành phần trong mạng sử dụng *sóng điện từ* để truyền thông với nhau

3. Các thành phần cấu hình mạng WLAN

4. Các chuẩn mạng WLAN

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

+ **802.11** : Đây là chuẩn đầu tiên của hệ thống mạng không dây. Chuẩn này chứa tất cả công nghệ truyền hiện hành bao gồm Direct Sequence Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS) và tia hồng ngoại. 802.11 là một trong hai chuẩn miêu tả những thao tác của sóng truyền (FHSS) trong hệ thống mạng không dây. Nếu người quản trị mạng không dây sử dụng hệ thống sóng truyền này, phải chọn đúng phần cứng thích hợp cho các chuẩn 802.11.

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

rộng DSL hoặc cáp và đủ cho âm thanh liên tục (streaming audio), 802.11b lại không đủ nhanh để truyền những hình ảnh có độ nét cao. Lợi thế chính của 802.11b là chí phí phần cứng thấp

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

+ **802.11g** : 802.11g là chuẩn nối mạng không dây được IEEE phê duyệt gần đây nhất (tháng 6 năm 2003). Các sản phẩm gắn liền với chuẩn này hoạt động trong cùng phổ 2,4GHz như những sản phẩm theo chuẩn 802.11b nhưng với tốc độ dữ liệu cao hơn nhiều - lên tới cùng tốc độ tối đa lý thuyết của các sản phẩm theo chuẩn 802.11a, 54 Mbit/s, với một thông lượng thực tế từ 15 đến 20 Mbit/s. Và giống như các sản phẩm theo chuẩn 802.11b, các thiết bị theo chuẩn 802.11g có một phạm vi phát huy hiệu lực trong nhà từ 100 đến 150 feet. Tốc độ cao hơn của chuẩn 802.11g cũng giúp cho việc truyền hình ảnh và âm thanh, lướt Web trở nên lý tưởng. 802.11g thiết kế để tương thích ngược với 802.11b và chúng chia sẻ cùng phổ 2,4GHz. Việc này làm cho các sản phẩm của 2 chuẩn 802.11b và 802.11g có thể hoạt động tương thích với nhau

- Chẳng hạn, một máy tính số tay với một PC card không dây 802.11b có thể kết nối với một điểm truy nhập 802.11g. Tuy nhiên, các sản phẩm 802.11g khi có sự hiện diện của các sản phẩm 802.11b sẽ bị giảm xuống tốc độ 802.11b. Trong khi các mạng 802.11a không tương thích với các mạng 802.11b hay 802.11g, các sản phẩm bao gồm một sự kết hợp của phổ vô tuyến 802.11a và 802.11g sẽ cung cấp những thứ tốt nhất. Đây là một tin tốt lành cho chuẩn 802.11a; trong môi trường gia đình, nơi mà tín hiệu vô tuyến cần phải xuyên qua nhiều bức tường và vật cản, chỉ một mình tính năng 802.11g có thể sẽ ít được lựa chọn bởi vì phạm vi hoạt động ngắn hơn của nó.

Bài tập và sản phẩm thực hành bài 39.1

Kiến thức:

Câu 1: Trình bày lịch sử hình thành mạng không dây

Câu 2: Trình bày các chuẩn mạng không dây

Câu 3: Phân loại mạng WLAN

Bài 2 CÁC TẦNG CỦA MẠNG KHÔNG DÂY

Mã bài; 39.2

Mục tiêu:

- Mô tả được cơ chế phân tầng của mạng không dây;
- Trình bày được chức năng của các tầng;
- Mô phỏng được quá trình giao tiếp giữa các tầng trong mạng không dây.
- Thực hiện các thao tác an toàn với máy tính

Nội dung

1. Các tầng mạng không dây

1.1 Tại sao cần phải chuẩn hóa mạng không dây

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

1.2. Những tổ chức tham gia xây dựng chuẩn

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

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

Sau đó, vào năm 1956, hai ủy ban riêng biệt của ITU, CCIF (Consultative Committee For International Telephony - Ủy Ban Cố Vấn Cho Điện Thoại Quốc Tế) và CCIT (Consultative Committee For International Telegraph Ủy Ban Cố Vấn Cho Thư Tín Quốc Tế) đã hợp nhất thành CCITT (Consultative

Committee For Internationaltelephony And Telegraph) để quản lý hữu hiệu hơn điện thoại và điện tín viễn thông.

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

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

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

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

+ American National Standards Institute – **ANSI** : Viện tiêu chuẩn quốc gia Hoa Kỳ. ANSI giữ vai trò của một tổ chức có nhiệm vụ định nghĩa các chuẩn mã và các chiến lược truyền tin hiệu tại Liên bang Hoa Kỳ; đồng thời nó đại diện cho Liên bang Hoa Kỳ tại ISO (International Organization for Standardization - Tổ chức Quốc tế về Tiêu chuẩn) và trong ITU (International Telecommunications Union - Liên đoàn Viễn thông Quốc tế). ANSI đã tham gia với tư cách một thành viên sáng lập của ISO và đóng một vai trò nổi bật trong việc quản trị của tổ chức này. Nó giữ một trong năm ghế thường trực tại Hội đồng Quản trị OSI. ANSI thúc đẩy việc sử dụng các tiêu chuẩn Liên bang ra toàn cầu, bảo vệ chính sách và các quan điểm kỹ thuật của Liên bang tại các tổ chức tiêu chuẩn vùng và quốc tế, và khuyến khích việc thừa nhận các tiêu chuẩn quốc tế như các tiêu chuẩn quốc gia khi những tiêu chuẩn này phù hợp các đòi hỏi của cộng đồng người dùng.

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

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

1.3 Mô hình OSI (Liên kết các hệ thống mở)

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

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

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

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

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

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

Cũng chú ý rằng trong khi mô hình OSI thường được sử dụng để tham khảo, các giao thức mà OSI tạo ra vẫn chưa trở thành phổ biến cho liên mạng, trước

nhất bởi vì tính phổ biến của bộ giao thức TCP/IP. Cho đến bây giờ, mô hình OSI vẫn được mô tả ở đây bởi vì nó định nghĩa được cách các giao thức truyền thông hoạt động như thế nào một cách tổng quát.

1.4. Chức năng của các tầng hữu tuyến

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

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

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

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

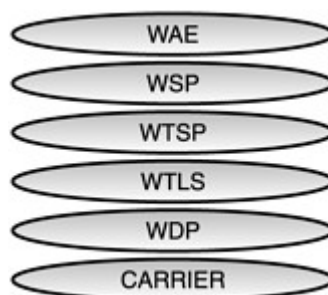
TẦNG CHUYỂN TẢI (Transport Layer) : Tầng này cung cấp quyền điều khiển cao cấp cho việc di chuyển thông tin giữa các hệ thống đầu cuối (end system) trong một phiên truyền thông. Các hệ đầu cuối có thể nằm trên cùng hệ thống mạng hay trên các mạng con trên hệ thống liên mạng. Giao thức tầng chuyển tải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

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

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

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

2. Các tầng mạng vô tuyến



Hình 39.2 Mô hình mạng vô tuyến

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

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

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

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

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

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

Bài tập và sản phẩm thực hành bài 39.2**Kiến thức:**

Câu 1: Nêu các tổ chức tham gia định chuẩn

Câu 2: Trình bày các lớp của mô hình OSI

Câu 3: Trình bày các tầng của mạng WLAN

BÀI 3 KIẾN TRÚC MẠNG KHÔNG DÂY

Mục tiêu:

- Mô tả được cấu trúc mạng không dây;
- Thiết kế được một mạng không dây cục bộ (WLAN);
- Phân biệt được ưu và nhược điểm của mạng không dây;
- Phân biệt được các chế độ của AP.
- Thực hiện các thao tác an toàn với máy tính.

Nội dung

1. Các thiết bị mạng không dây

1.1 Card mạng không dây

1.1.1. Card PCI Wireless

Là thành phần phổ biến nhất trong WLAN. Dùng để kết nối các máy khách vào hệ thống mạng không dây. Được cắm vào khe PCI trên máy tính. Loại này được sử dụng phổ biến cho các máy tính để bàn(desktop) kết nối vào mạng không dây



Hình 39.3. Card PCI Wireless

1.1.2. Card PCMCIA Wireless

Trước đây được sử dụng trong các máy tính xách tay(laptop) và các thiết bị hỗ trợ cá nhân số PDA(Personal Digital Association). Hiện nay nhờ sự phát triển của công nghệ nên PCMCIA wireless ít được sử dụng vì máy tính xách tay và PDA,... đều được tích hợp sẵn Card Wireless bên trong thiết bị



Hình 39.4 Card PCMCIA Wireless

1.1.3. Card USB Wireless

Loại rất được ưu chuộng hiện nay dành cho các thiết bị kết nối vào mạng không dây vì tính năng di động và nhỏ gọn . Có chức năng tương tự như Card PCI Wireless, nhưng hỗ trợ chuẩn cắm là USB (Universal ***** Bus). Có thể tháo lắp nhanh chóng (không cần phải cắm cố định như Card PCI Wireless) và hỗ trợ cắm khi máy tính đang hoạt động.



Hình 39.5 Card USB Wireless

1.2. ACCESS POINT(AP)

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

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

Tính năng lọc địa chỉ MAC. Một sóng vô tuyến của máy khách cố gắng truy cập phải có địa chỉ MAC trong bảng địa chỉ của AP trước khi AP cho phép kết hợp với AP.

Tính năng đóng mạng. Thông thường, một máy khách có thể chỉ định một ESSID của bất cứ sự kết hợp nào với bất cứ một mạng hiện hữu nào. Trong tính năng đóng mạng, máy khách phải chỉ định ESSID rõ ràng, hoặc nó không thể kết hợp với AP.

Tính năng Anten ngoài.

Tính năng kết nối liên miền.

Bản ghi mở rộng, thống kê, và thực hiện báo cáo.

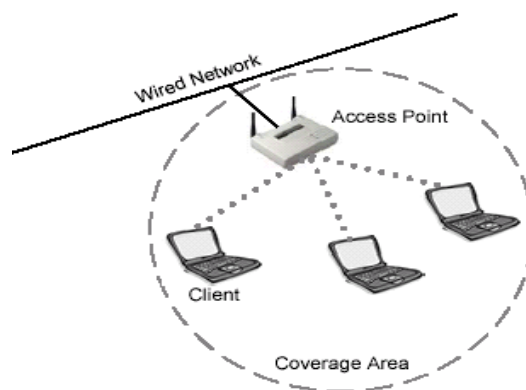


Hình 39.6 Mô hình AP

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

APs là sự lựa chọn lý tưởng cho những mạng cá nhân với nhiều máy khách đặt trong một khoảng không vật lý, đặc biệt là các đoạn mạng có cùng Subnet (giống như là doanh nghiệp hoặc khu trường sở). AP cung cấp mức

độ điều khiển cao để có thể truy cập bằng dây, nhưng giá của nó không rẻ (giá trung bình của một AP từ 800 đến 1000 USD)



Hình 39.6 Mô hình cài đặt Access Point

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

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

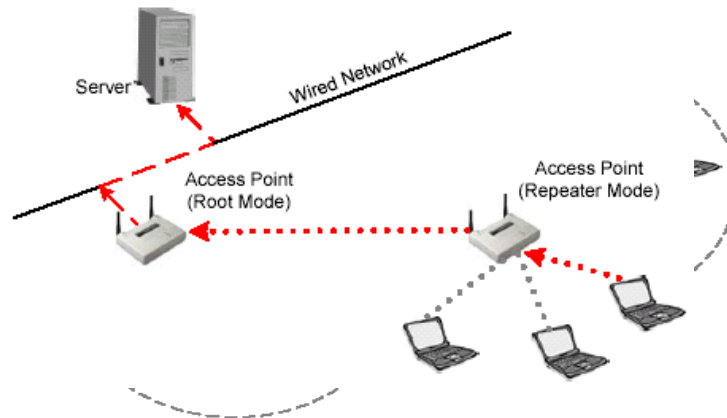
Cung cấp cho các máy khách(client) một điểm truy cập vào mạng "Nơi mà các máy tính dùng wireless có thể vào mạng nội bộ của công ty". AP là một thiết bị song công(Full duplex) có mức độ thông minh tương đương với một chuyển mạch Ethernet phức tạp(Switch).

2. Các chế độ của AP

2.1. Chế độ gốc (Root Mode)

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

các máy khách khác ở các ô khác nhau thông qua AP tương ứng để đi qua đoạn mạng hữu tuyến.



Hình 39.7 Access Point trong chế độ gốc

Chế độ gốc (Root mode): Root mode được sử dụng khi AP được kết nối với mạng backbone có dây thông qua giao diện có dây (thường là Ethernet) của nó. Hầu hết các AP sẽ hỗ trợ các mode khác ngoài root mode, tuy nhiên root mode là cấu hình mặc định. Khi một AP được kết nối với phân đoạn có dây thông qua cổng Ethernet của nó, nó sẽ được cấu hình để hoạt động trong root mode. Khi ở trong root mode, các AP được kết nối với cùng một hệ thống phân phối có dây có thể nói chuyện được với nhau thông qua phân đoạn có dây. Các client không dây có thể giao tiếp với các client không dây khác nằm trong những cell (ô tế bào, hay vùng phủ sóng của AP) khác nhau thông qua AP tương ứng mà chúng kết nối vào, sau đó các AP này sẽ giao tiếp với nhau thông qua phân đoạn có dây

2.2. Chế độ lặp (Repeater Mode)

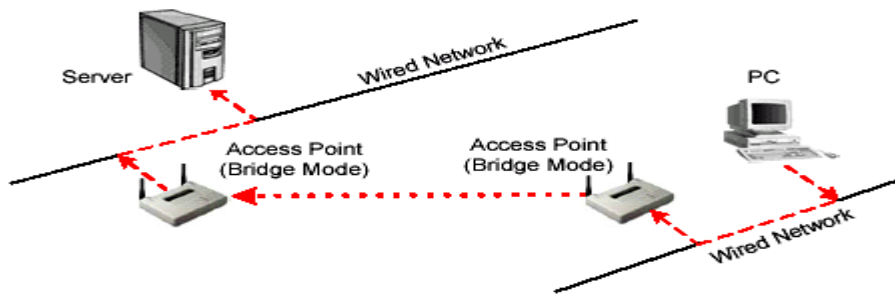
Trong chế độ lặp, APs có khả năng cung cấp những liên kết ngược trong mạng hữu tuyến khá hơn một liên kết hữu tuyến bình thường. Một AP được thỏa mãn như là một AP gốc và các AP khác giống như là các bộ lặp. AP ở chế độ lặp kết nối tới máy khách như là một AP và kết nối tới AP gốc ngược như là chính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

Chế độ lặp (repeater mode): AP có khả năng cung cấp một đường kết nối không dây upstream vào mạng có dây thay vì một kết nối có dây bình thường. Một AP hoạt động như là một root AP và AP còn lại hoạt động như là một

Repeater không dây. AP trong repeater mode kết nối với các client như là một AP và kết nối với upstream AP như là một client.

2.3.Chế độ cầu nối (Bridge Mode)

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

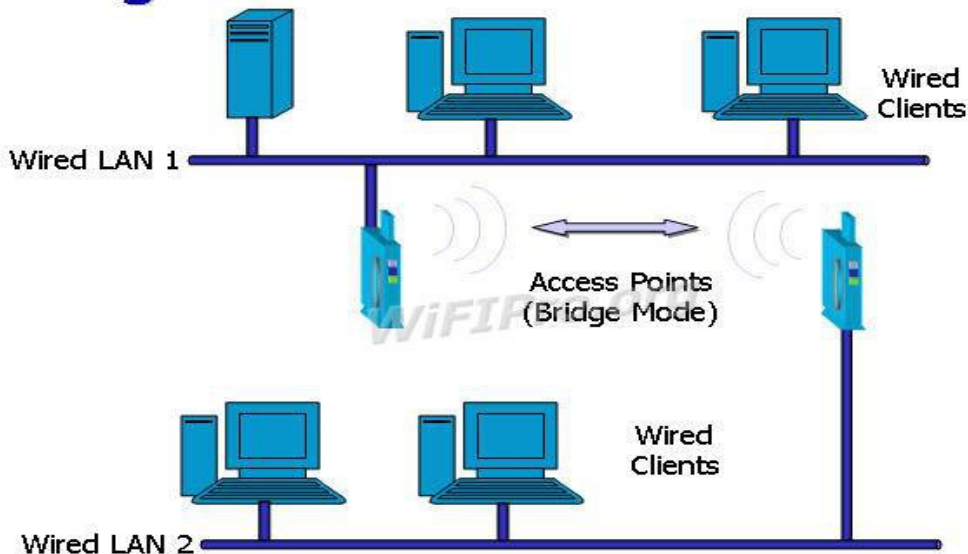


Hình 39.8 Access Point trong chế độ cầu nối

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

Chế độ cầu nối(bridge Mode): Trong Bridge mode, AP hoạt động hoàn toàn giống với một cầu nối không dây. AP sẽ trở thành một cầu nối không dây khi được cấu hình theo cách này. Chỉ một số ít các AP trên thị trường có hỗ trợ chức năng Bridge, điều này sẽ làm cho thiết bị có giá cao hơn đáng kể. Chúng ta sẽ giải thích một cách ngắn gọn cầu nối không dây hoạt động như thế nào

Bridge Mode



Hình 39.9 Mô hình Bridge Mode

Bài tập và sản phẩm thực hành bài 39.3

Kiến thức:

Câu 1: Trình bày ưu và nhược điểm của mạng WLAN

Câu 2: Trình bày các chế độ của AP

Câu 3: Trình bày các mô hình của mạng WLAN

Bài tập 1: Cài đặt cấu hình mạng và quản trị mạng ADHOC với mô hình như sau:



THIẾT LẬP MẠNG WIFI CHIA SẺ LAN KHÔNG CẦN ACSESS POINT

Ý tưởng của bài Lab này là tìm cách kết nối 2 máy laptop thông qua wifi mà không cần phải tốn tiền mua access point. Bài Lab được thực hiện trên 2 máy tính xách tay được cài Win XP SP2. Sẽ tạo ra một mạng Lan không dây giữa 2 máy tính xách tay để chia sẻ file với nhau mà không cần đến bất kỳ thiết bị Access Point nào.

Trước tiên ta phải chuẩn bị trước các thiết bị sau:

- Ta cần 02 máy tính xách tay có hỗ trợ WIFI, kiểm tra chuẩn của card WIFI trên các máy.
- Đặt 2 máy tính trong phạm vi sóng của chúng. Thông thường là 50 mét trong nhà. Tùy vào từng loại card và chuẩn mà cự ly có thể xa hơn hoặc gần hơn. Để sóng được truyền tốt nhất, bạn nên tránh đặt máy gần những vật chắn kim loại hoặc những nguồn gây nhiễu như lò vi sóng, những thiết bị Bluetooth đang hoạt động, điện thoại mẹ bồng con.
- Bạn phải chắc chắn rằng cả hai card WIFI phải hỗ trợ chế độ ad hoc và Windows XP Wireless Zero Configuration (WZC) service. Nếu WZC không được hỗ trợ thì bạn phải dung chương trình đi cùng với card của bạn để tạo mạng ad-hoc.

- Để cho phép chia sẻ file bạn phải đặt tên duy nhất cho mỗi máy và đặt chung cùng work group. Để làm điều này bạn click chuột phải vào My computer icon, chọn Properties rồi đi đến System Properties. Trên Computer name tab, click Change. Sau đó restart máy.

CÁC BƯỚC THỰC HIỆN:

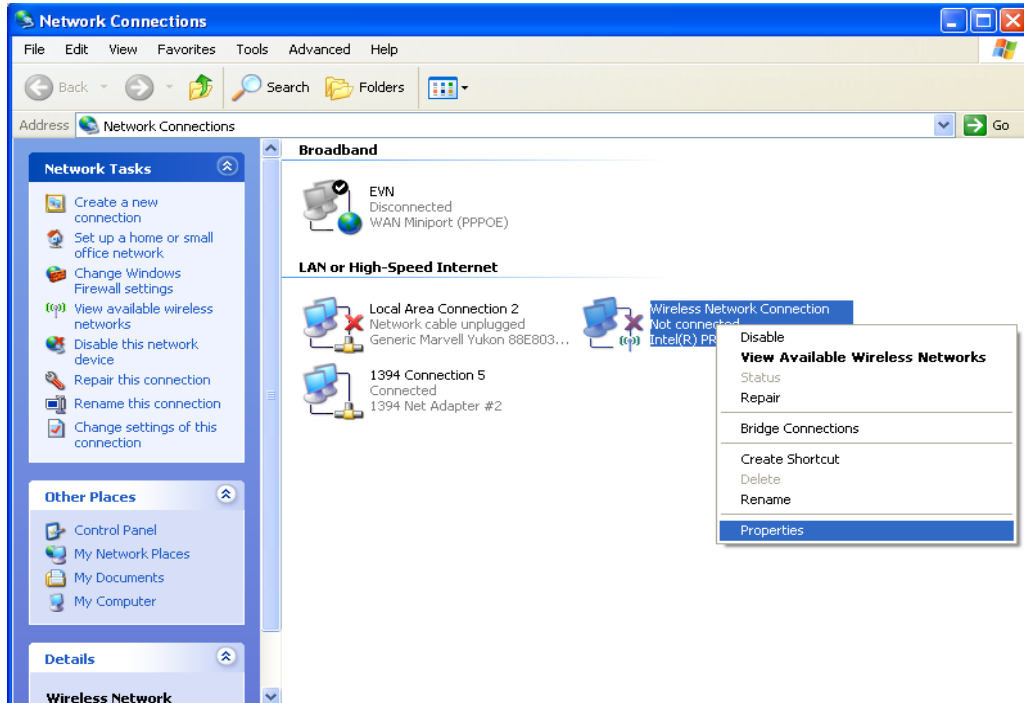
Mô hình của bài Lab như sau:



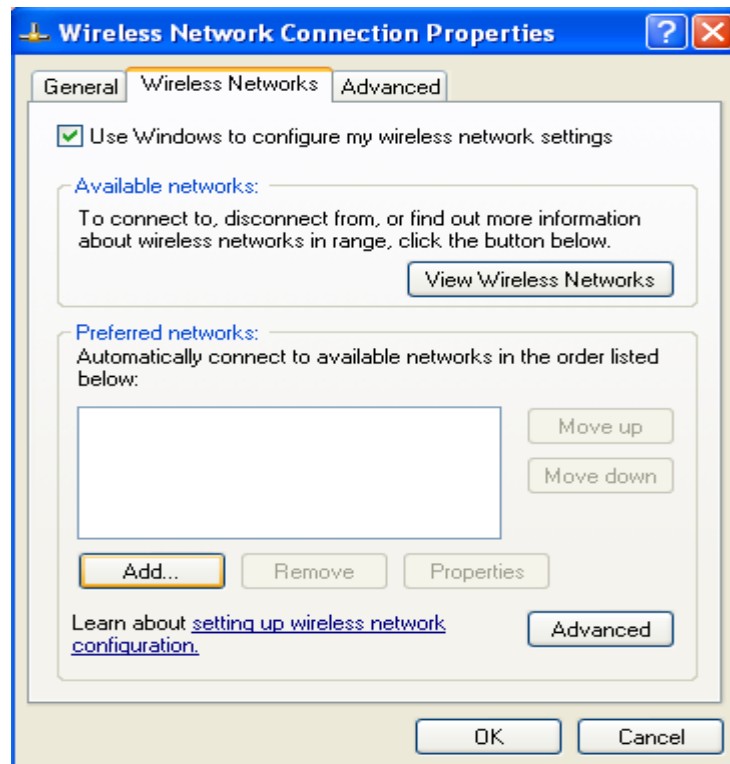
I. TRƯỜNG HỢP KHÔNG CÓ CẤU HÌNH BẢO MẬT WEP KEY

1. Cấu hình trên PC 1:

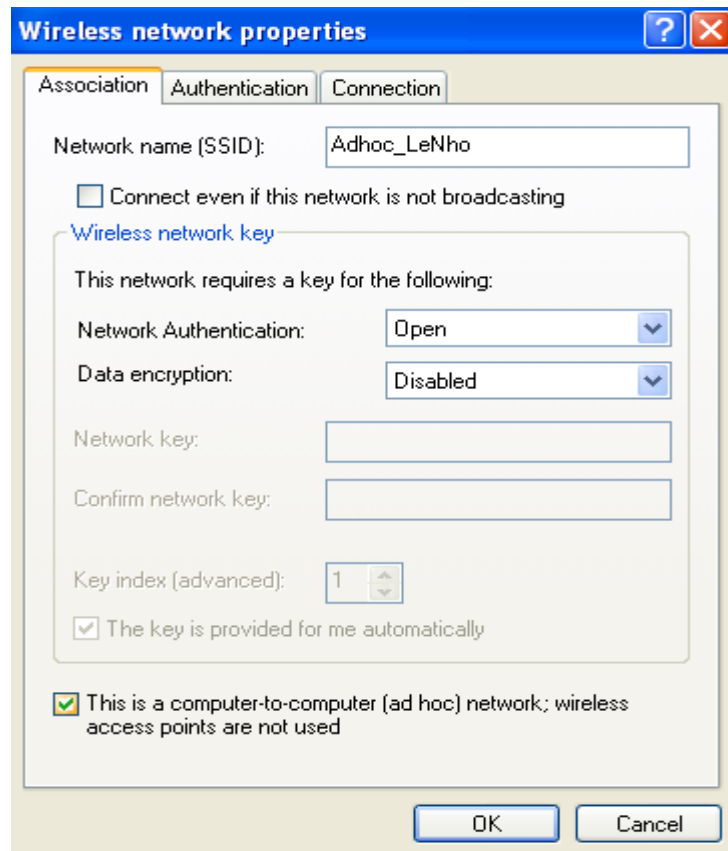
Bước 1: vào Network Connection/ kích phải chuột lên card Wireless/ chọn properties



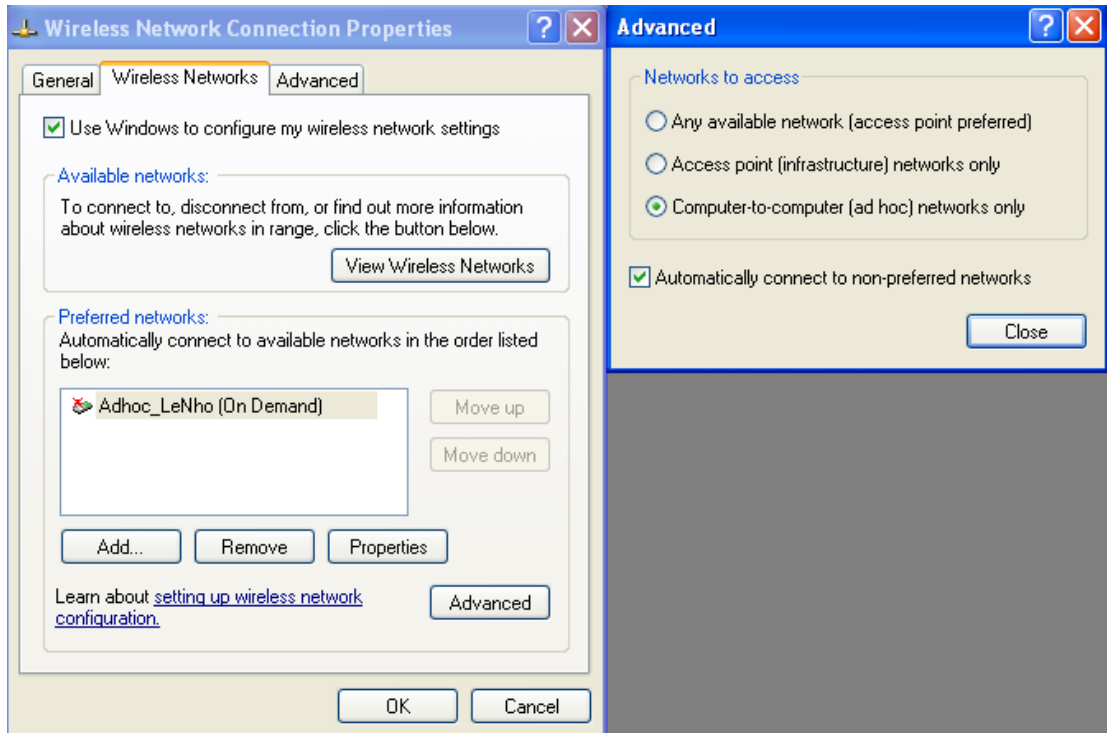
Bước 2: vào tab Wireless Networks/ kích chuột vào nút Add



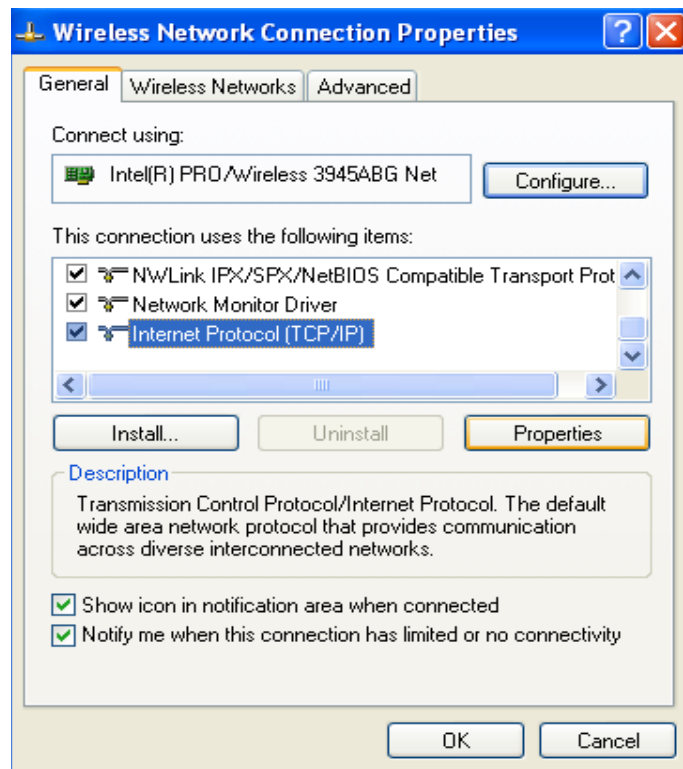
Bước 3: hộp thoại Wireless network properties xuất hiện. Nhập tên mạng (SSID) = Adhoc_LeNho và chọn các thông số như hình vẽ bên dưới. Sau đó nhấn OK.



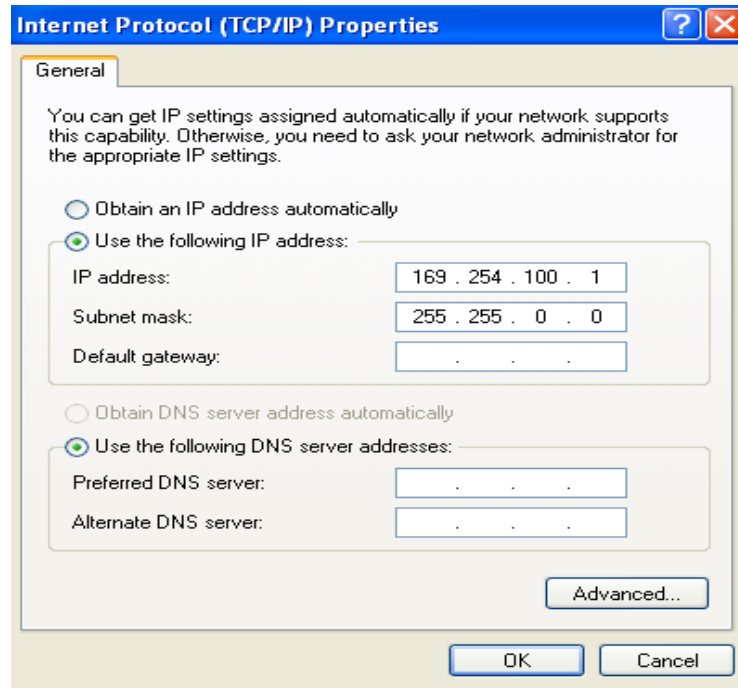
Bước 4: Trở lại tab Wireless Networks, kích chuột vào Adhoc_LeNho vừa tạo, sau đó kích chuột vào properties -> hộp thoại Advanced xuất hiện và ta chọn các tham số như hình vẽ bên dưới. Xong nhấn Close.



Bước 5: trở lại hộp thoại “Wireless Network Connection Properties”, kích chuột vào mục Internet Protocol (TCP/IP) và kích chuột vào Properties để đặt địa chỉ IP cho Card Wireless.

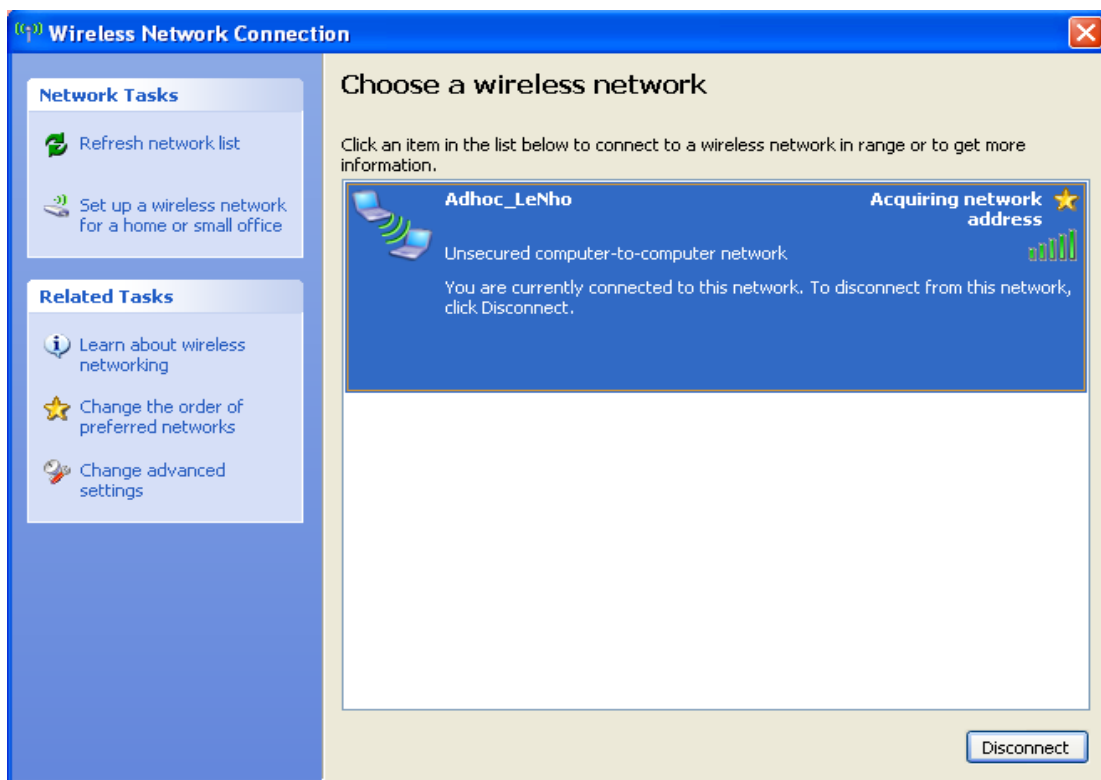


Hộp thoại Internet Protocol Properties xuất hiện, ta tiến hành đặt địa chỉ IP cho Card Wireless trên PC1. IP = 169.254.100.1 và Subnet mask = 255.255.0.0



2. Cấu hình trên PC 2:

Bước 1: trên PC2 ta kích phải chuột lên biểu tượng của card wireless ở góc dưới bên phải màn hình, chọn View Available Wireless Networks -> hộp thoại Wireless Network Connection xuất hiện, ta chọn tên mạng Adhoc_LeNho và nhấn nút Connection để thực hiện việc kết nối bằng Wireless đến PC1.



Bước 2: trên PC 2 ta màn hình Command Prompt và gõ lệnh ipconfig /all, để xem địa chỉ IP của PC2 xin địa chỉ IP của PC1 trên card Wireless.


```
C:\ Command Prompt
Primary Dns Suffix . . . . . :
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection 2:

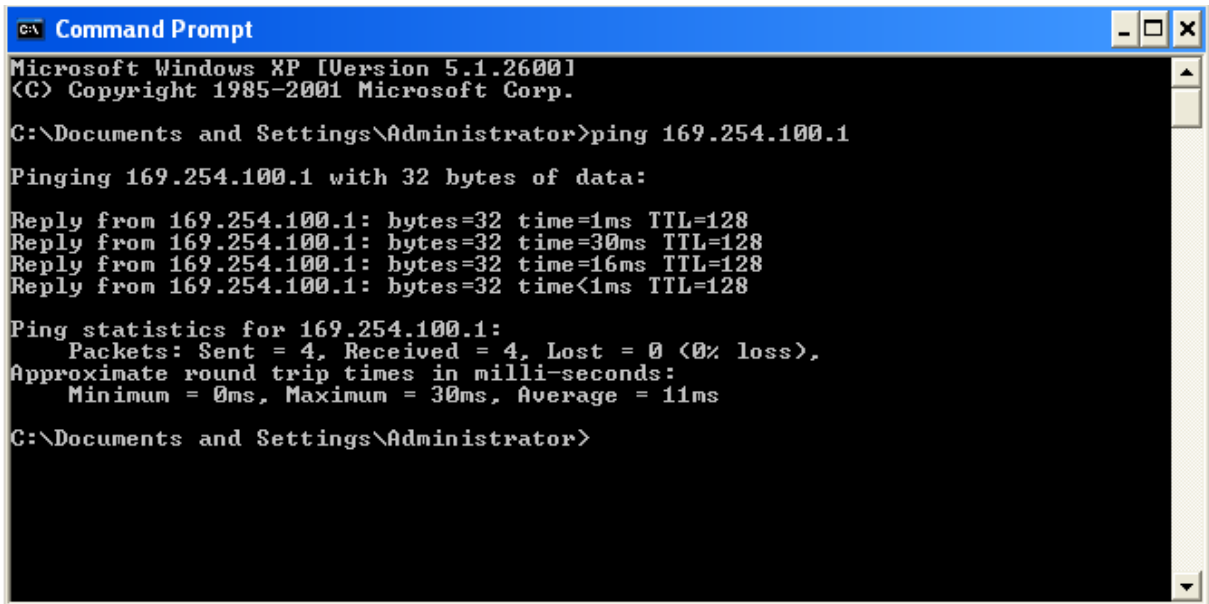
    Media State . . . . . : Media disconnected
    Description . . . . . : Generic Marvell Yukon 88E8039 PCI-E
Fast Ethernet Controller
    Physical Address. . . . . : 00-1D-72-46-9F-EF

Ethernet adapter Wireless Network Connection:

    Connection-specific DNS Suffix . . :
    Description . . . . . : Intel(R) PRO/Wireless 3945ABG Network
k Connection
    Physical Address. . . . . : 00-1C-BF-9A-83-D2
    Dhcp Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Autoconfiguration IP Address. . . : 169.254.154.97
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . :

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

Bước 3: thực hiện lệnh ping 169.254.100.1 để xem kết nối giữa PC2 và PC1 có thành công hay không. Nếu thành công thì sẽ xuất hiện màn hình bên dưới.



```

C:\ Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ping 169.254.100.1

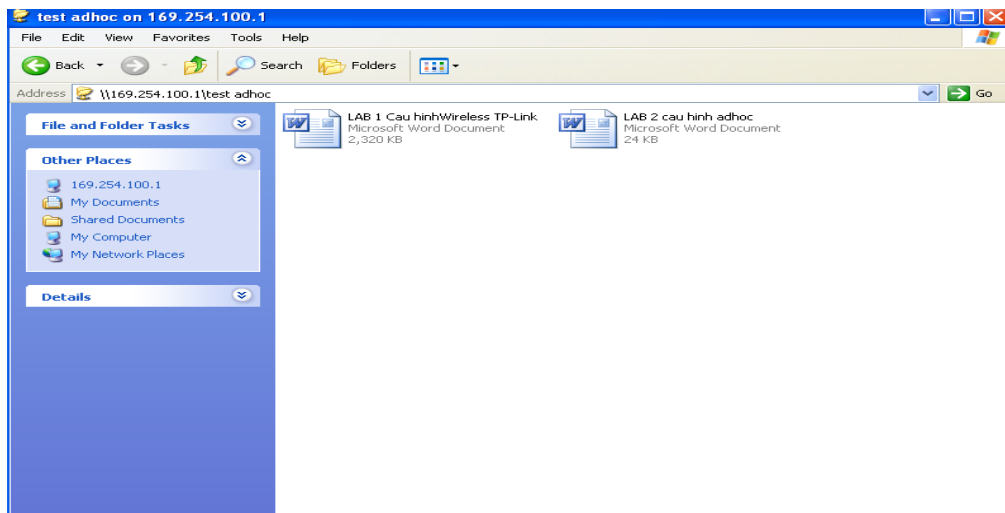
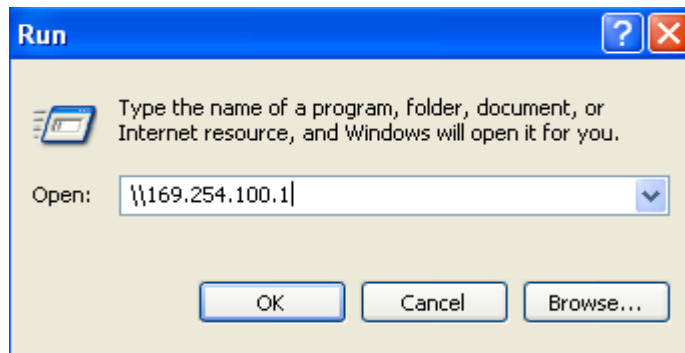
Pinging 169.254.100.1 with 32 bytes of data:

Reply from 169.254.100.1: bytes=32 time=1ms TTL=128
Reply from 169.254.100.1: bytes=32 time=30ms TTL=128
Reply from 169.254.100.1: bytes=32 time=16ms TTL=128
Reply from 169.254.100.1: bytes=32 time<1ms TTL=128

Ping statistics for 169.254.100.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 30ms, Average = 11ms

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

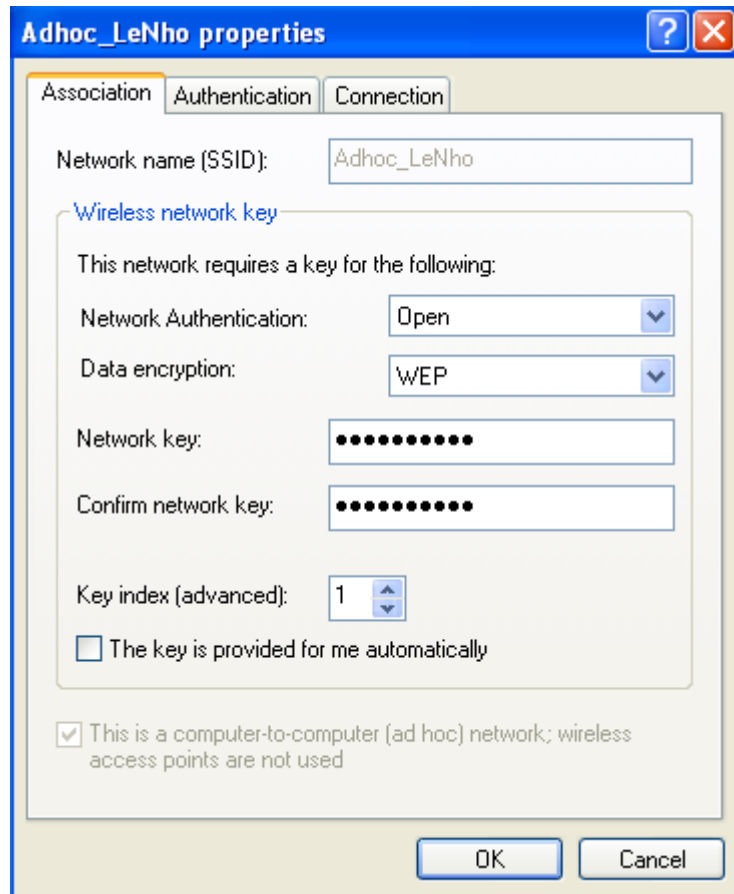
Bước 4: trên PC2 thực hiện việc truy cập đến dữ liệu được share trên PC1, thư mục share trên PC1 có tên là “test adhoc”.



II. TRƯỜNG HỢP CÓ CẤU HÌNH BẢO MẬT WEP KEY

1. Cấu hình trên PC 1:

Ta thực hiện tương tự từ bước 1 đến bước 5. Nhưng ở bước 3 hộp thoại Wireless network properties xuất hiện. Nhập tên mạng (SSID) = Adhoc_LeNho, Data encryption = WEP, nhập Wep key trong Network key và chọn các thông số như hình vẽ bên dưới. Sau đó nhấn OK.

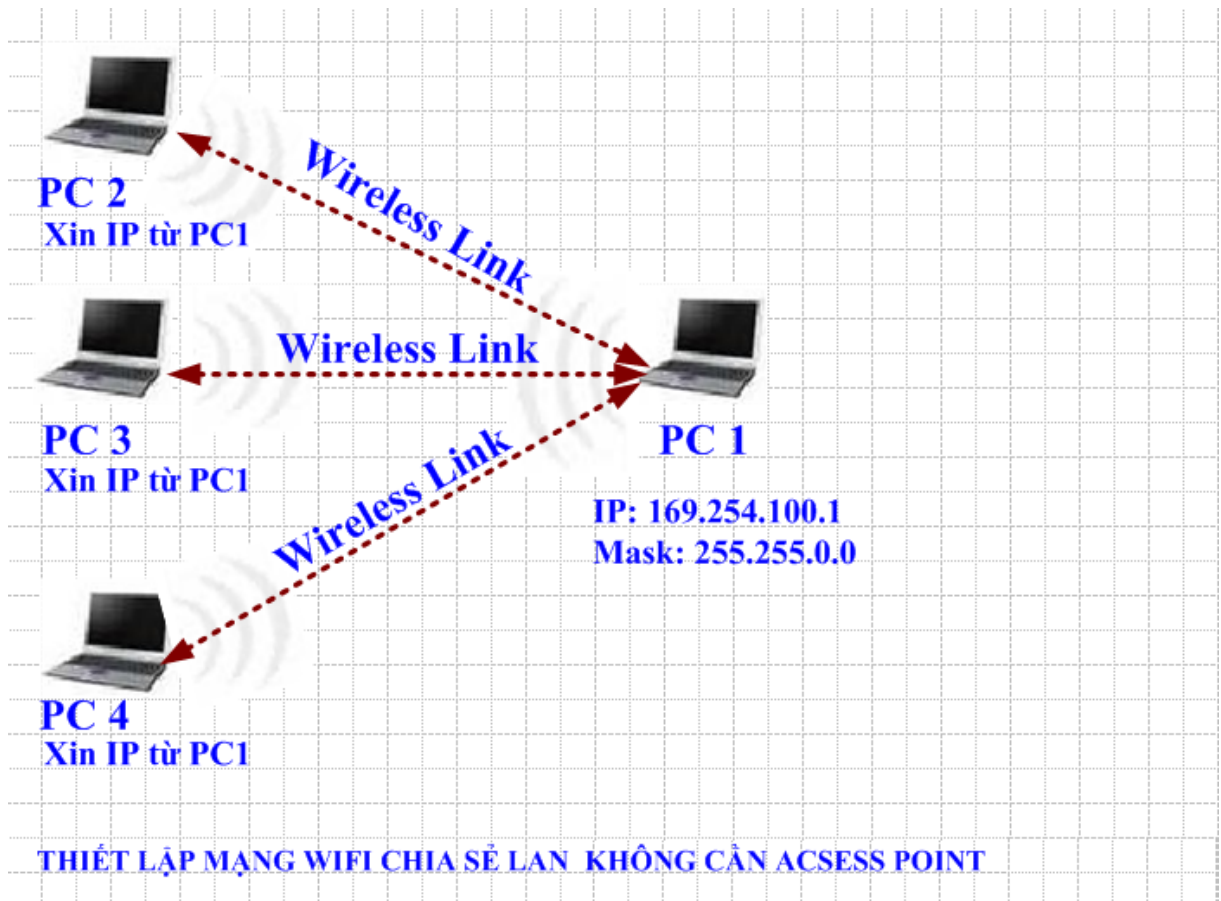


2. Cấu hình trên PC 2:

Ta thực hiện tương tự từ bước 1 đến bước 4. Nhưng ở bước 1 có hộp thoại yêu cầu nhập WEP KEY, ta nhập WEP KEY vào và thực hiện theo các bước ở trên.

III. KẾT LUẬN

Như vậy ta đã thực hiện được việc kết nối giữa PC1 và PC2 với nhau không cần dây cáp mạng mà bằng sóng Wireless. Trong bài Lab này thì PC1 đóng vai trò là 1 Acces Point phát sóng WiFi, còn PC2 là một máy tính bắt sóng WiFi đó và thiết lập kết nối giữa chúng. Ta có thể mở rộng mô hình này với nhiều máy tính cùng kết nối với nhau và có thể thiết lập thành mạng Lan không dây trong nội bộ văn phòng hay công ty theo hình vẽ minh họa dưới đây.



Bài thực hành số 2

THIẾT LẬP MẠNG WIFI CHIA SẼ LAN VÀ INTERNET KHÔNG CẦN ACCESS POINT

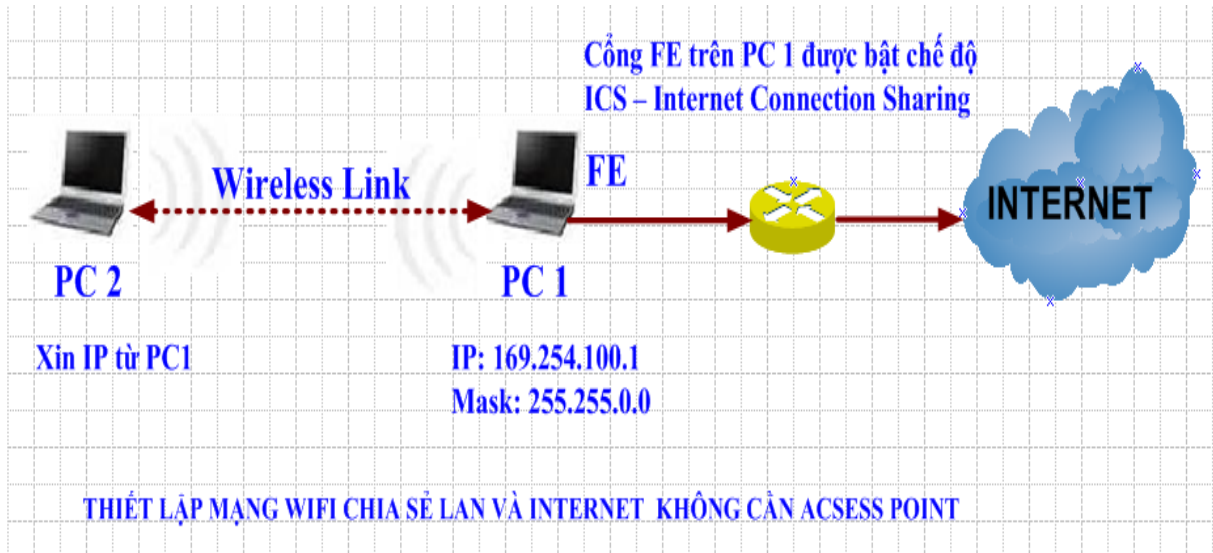
Ý tưởng của bài Lab này là tìm cách kết nối 2 máy laptop thông qua wifi mà không cần phải tốn tiền mua access point. Bài Lab được thực hiện trên 2 máy tính xách tay được cài Win XP SP2. Sẽ tạo ra một mạng Lan không dây giữa 2 máy tính xách tay để chia sẻ file và chia sẻ internet với nhau mà không cần đến bất kỳ thiết bị Access Point nào.

Trước tiên ta phải chuẩn bị trước các thiết bị sau:

- Ta cần 02 máy tính xách tay có hỗ trợ WIFI, kiểm tra chuẩn của card WIFI trên các máy.
- Đặt 2 máy tính trong phạm vi song của chúng. Thông thường là 50 mét trong nhà. Tùy vào từng loại card và chuẩn mà cự ly có thể xa hơn hoặc gần hơn. Để sóng được truyền tốt nhất, bạn nên tránh đặt máy gần những vật chắn kim loại hoặc những nguồn gây nhiễu như lò vi sóng, những thiết bị Bluetooth đang hoạt động, điện thoại mẹ bông con.
- Bạn phải chắc chắn rằng cả hai card WIFI phải hỗ trợ chế độ ad hoc và Windows XP Wireless Zero Configuration (WZC) service. Nếu WZC không được hỗ trợ thì bạn phải dung chương trình đi cùng với card của bạn để tạo mạng ad-hoc.
- Để cho phép chia sẻ file bạn phải đặt tên duy nhất cho mỗi máy và đặt chung cùng work group. Để làm điều này bạn click chuột phải vào My computer icon, chọn Properties rồi đi đến System Properties. Trên Computer name tab, click Change. Sau đó restart máy.
- Kiểm tra kết nối đi internet trên PC1

CÁC BƯỚC THỰC HIỆN:

Mô hình của bài Lab như sau:

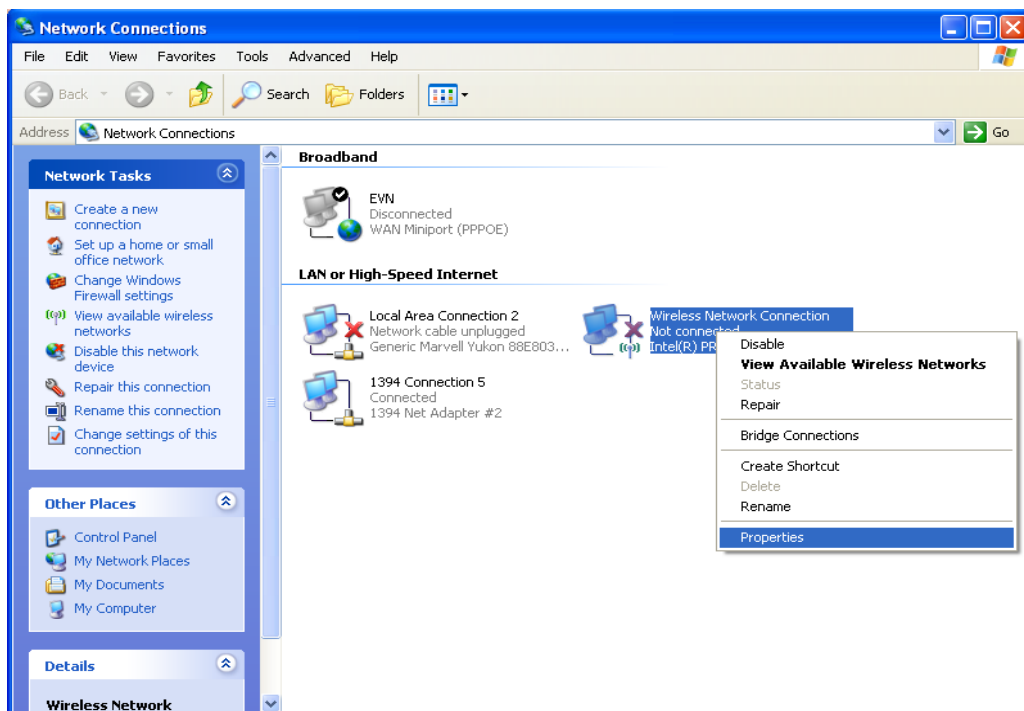


* Các bước thực hiện:

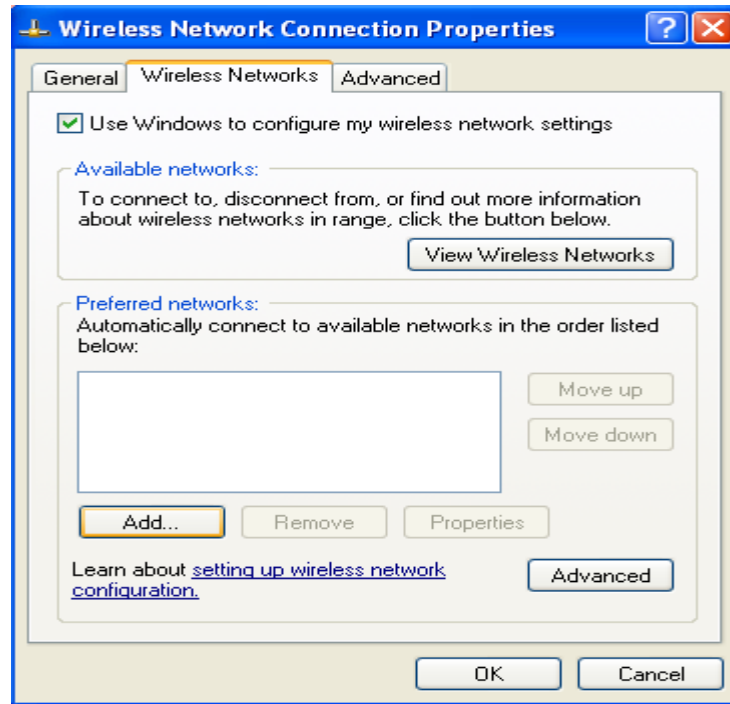
I. TRƯỜNG HỢP KHÔNG CÓ CẤU HÌNH BẢO MẬT WEP KEY

1. Cấu hình trên PC 1:

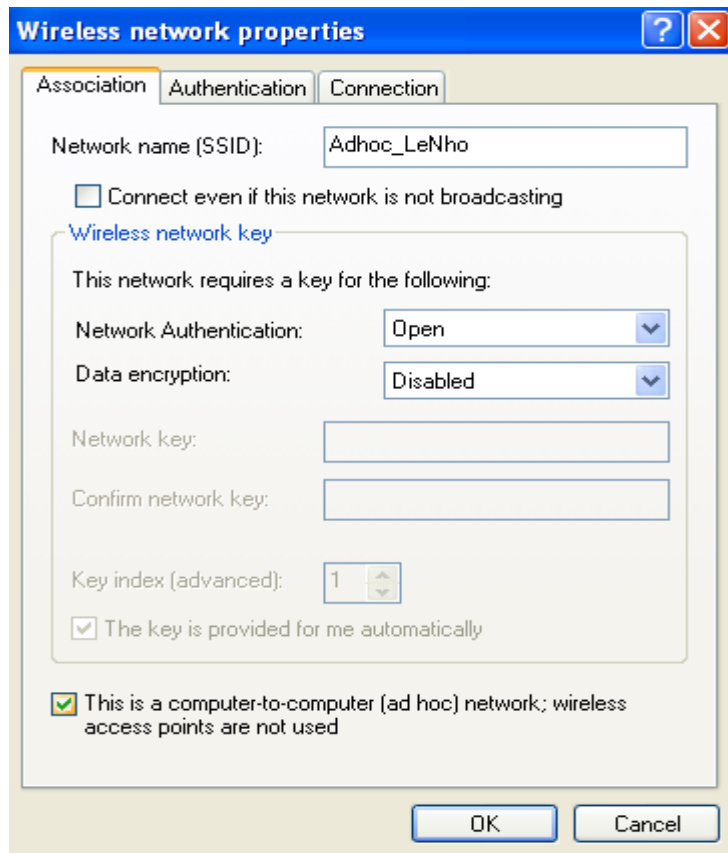
Bước 1: vào Network Connection/ kích phải chuột lên card Wireless/ chọn properties



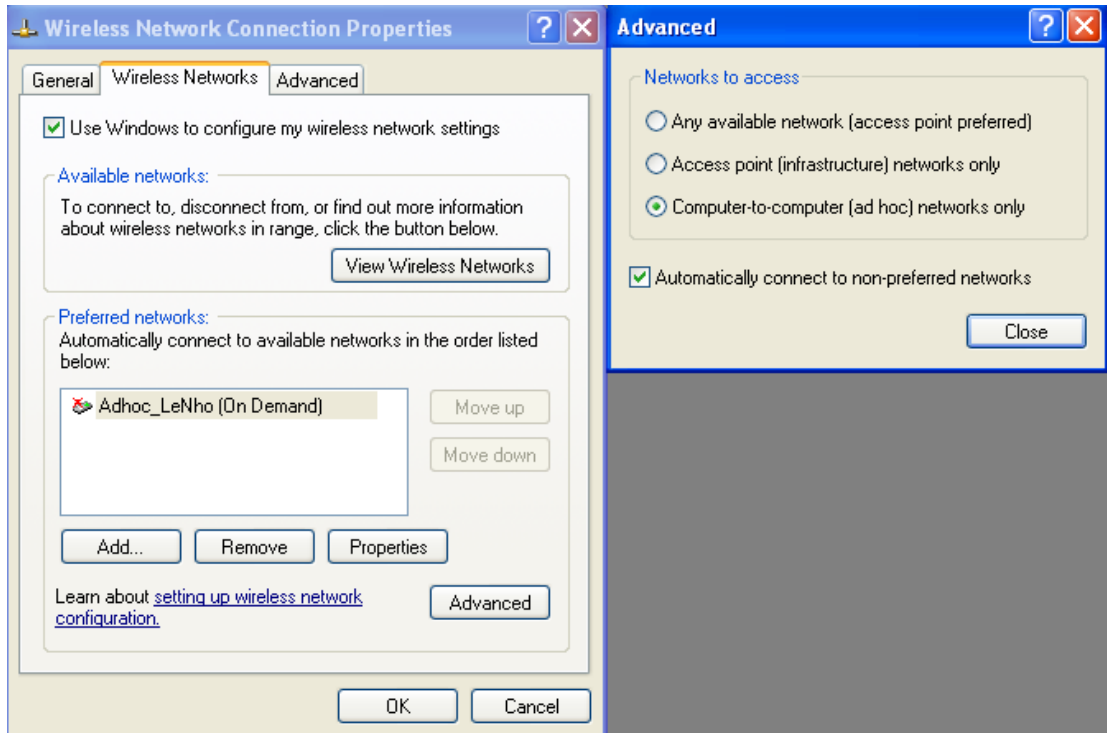
Bước 2: vào tab Wireless Networks/ kích chuột vào nút Add



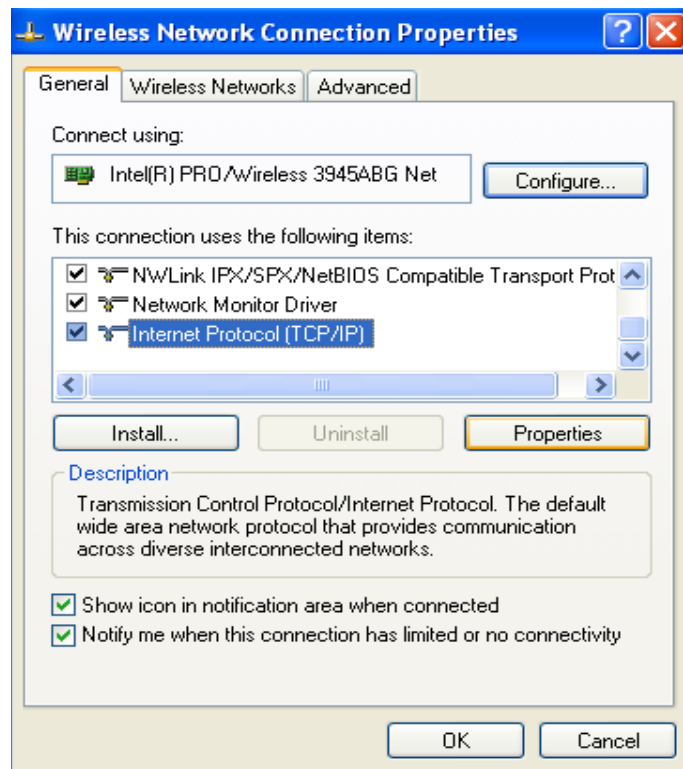
Bước 3: hộp thoại Wireless network properties xuất hiện. Nhập tên mạng (SSID) = Adhoc_LeNho và chọn các thông số như hình vẽ bên dưới. Sau đó nhấn OK.



Bước 4: Trở lại tab Wireless Networks, kích chuột vào Adhoc_LeNho vừa tạo, sau đó kích chuột vào properties -> hộp thoại Advanced xuất hiện và ta chọn các tham số như hình vẽ bên dưới. Xong nhấn Close.



Bước 5: trở lại hộp thoại “Wireless Network Connection Properties”, kích chuột vào mục Internet Protocol (TCP/IP) và kích chuột vào Properties để đặt địa chỉ IP cho Card Wireless.



Hộp thoại Internet Protocol Properties xuất hiện, ta tiến hành đặt địa chỉ IP cho Card Wireless trên PC1. IP = 169.254.100.1 và Subnet mask = 255.255.0.0

Internet Protocol (TCP/IP) Properties [?] [X]

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

Obtain an IP address automatically

Use the following IP address:

IP address:

Subnet mask:

Default gateway:

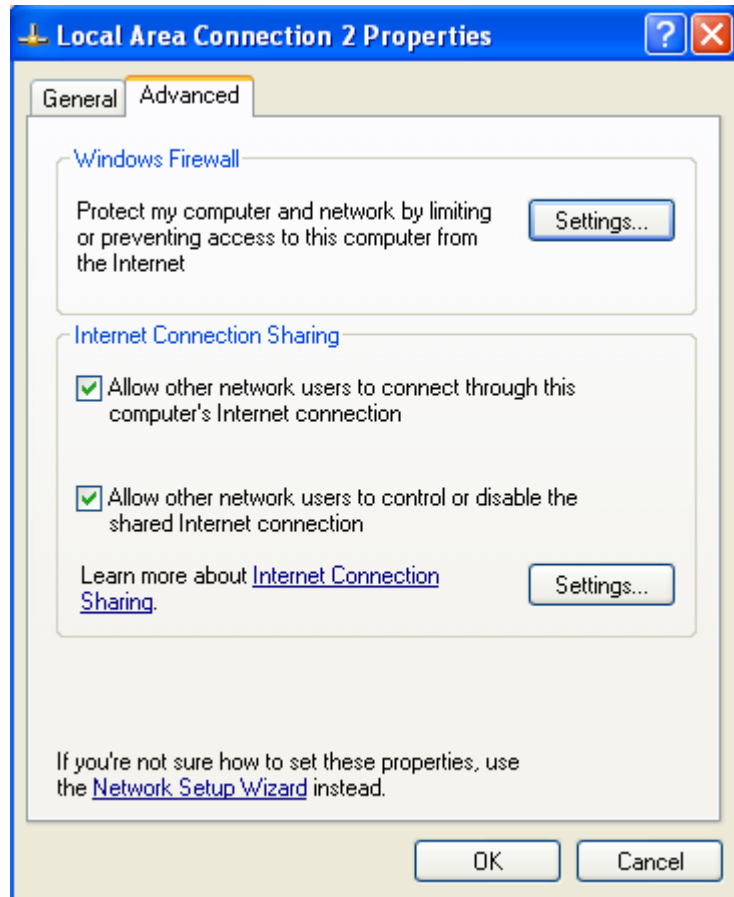
Obtain DNS server address automatically

Use the following DNS server addresses:

Preferred DNS server:

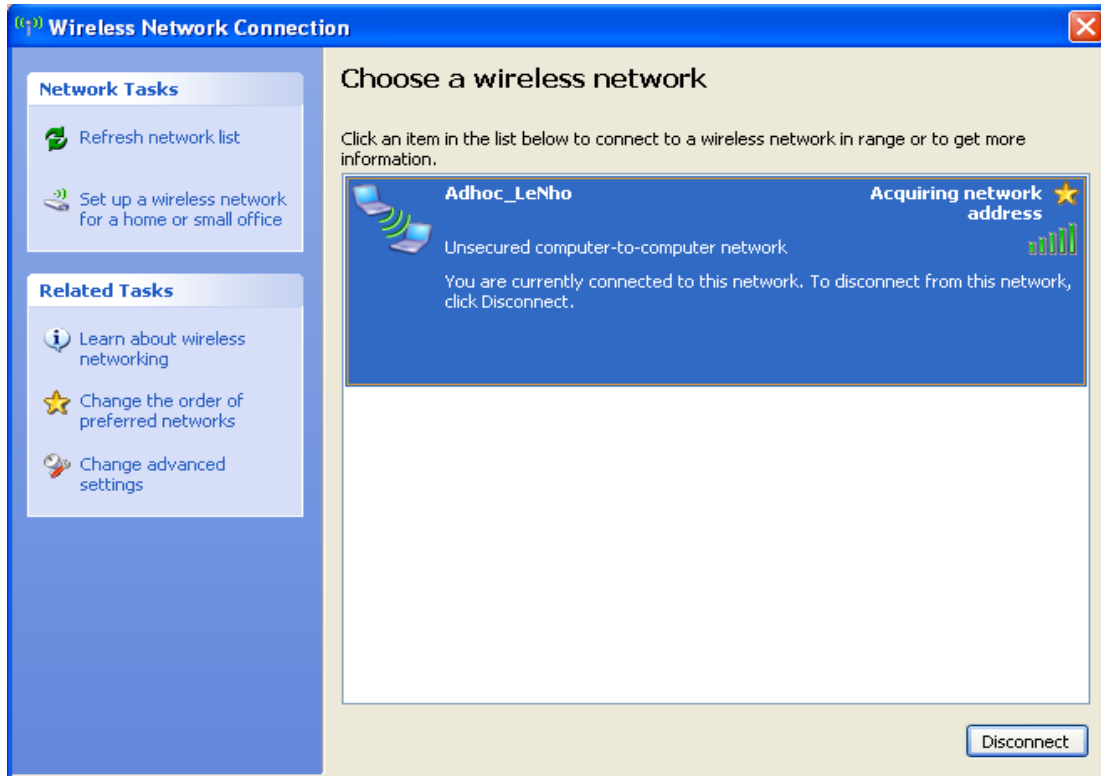
Alternate DNS server:

Bước 6: vào Network Connection/ kích phải chuột lên cổng FE của máy tính/ kích phải chuột chọn properties, chọn tab Advanced, kích chuột chọn cho phép share internet (Internet Connection Sharing) để cho phép cổng Fe trên PC1 có thể chia sẻ kết nối internet cho cổng Wireless và thiết lập các thông số như hình dưới đây.



2. Cấu hình trên PC 2:

Bước 1: trên PC2 ta kích phải chuột lên biểu tượng của card wireless ở góc dưới bên phải màn hình, chọn View Available Wireless Networks -> hộp thoại Wireless Network Connection xuất hiện, ta chọn tên mạng Adhoc_LeNho và nhấn nút Connection để thực hiện việc kết nối bằng Wireless đến PC1.



Bước 2: trên PC 2 ta mở màn hình Command Prompt và gõ lệnh ipconfig /all, để xem địa chỉ IP của PC2 xin địa chỉ IP của PC1 trên card Wireless.

```

C:\> Command Prompt

Primary Dns Suffix . . . . . :
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection 2:

Media State . . . . . : Media disconnected
Description . . . . . : Generic Marvell Yukon 88E8039 PCI-E
Fast Ethernet Controller
Physical Address. . . . . : 00-1D-72-46-9F-EF

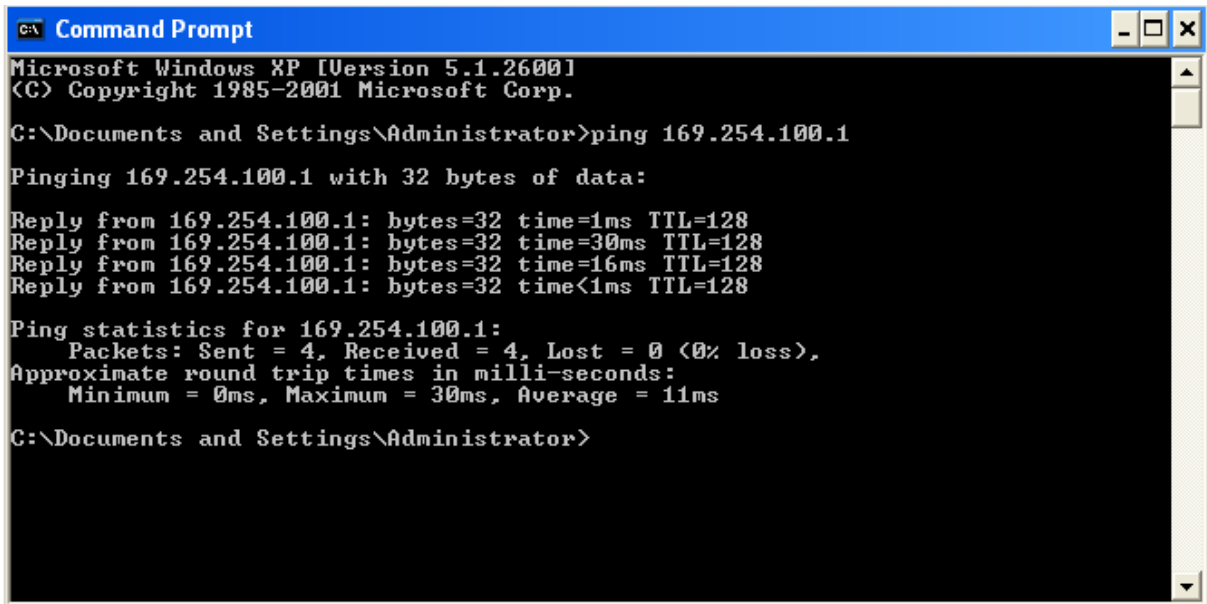
Ethernet adapter Wireless Network Connection:

Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) PRO/Wireless 3945ABG Network
Connection
Physical Address. . . . . : 00-1C-BF-9A-83-D2
Dhcp Enabled. . . . . : Yes
Autoconfiguration Enabled . . . : Yes
Autoconfiguration IP Address. . : 169.254.154.97
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . :

C:\Documents and Settings\Administrator>

```

Bước 3: thực hiện lệnh ping 169.254.100.1 để xem kết nối giữa PC2 và PC1 có thành công hay không. Nếu thành công thì sẽ xuất hiện màn hình bên dưới.



```

C:\ Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ping 169.254.100.1

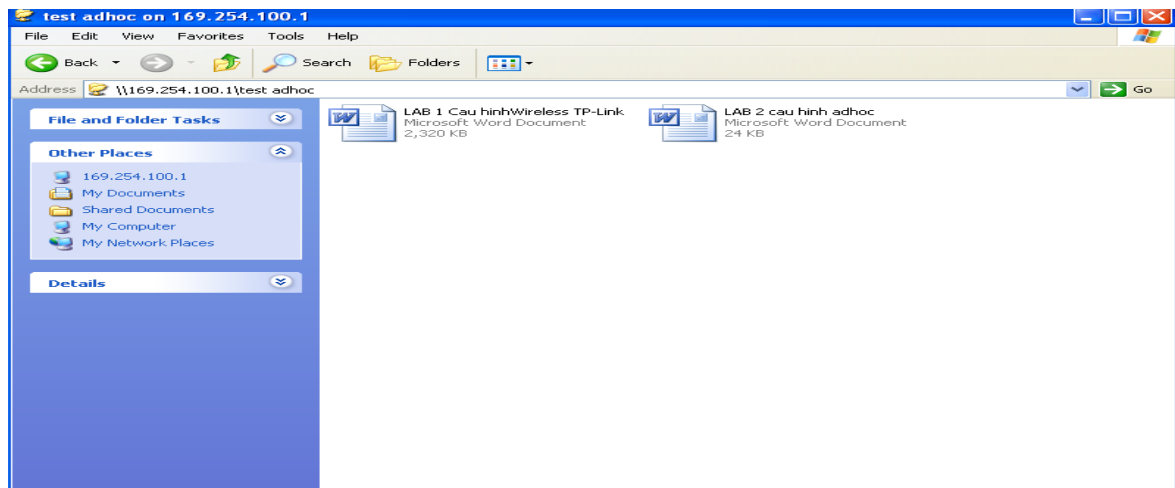
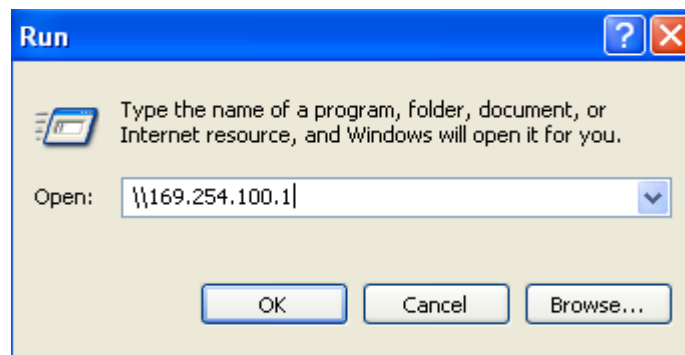
Pinging 169.254.100.1 with 32 bytes of data:

Reply from 169.254.100.1: bytes=32 time=1ms TTL=128
Reply from 169.254.100.1: bytes=32 time=30ms TTL=128
Reply from 169.254.100.1: bytes=32 time=16ms TTL=128
Reply from 169.254.100.1: bytes=32 time<1ms TTL=128

Ping statistics for 169.254.100.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 30ms, Average = 11ms

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

Bước 4: trên PC2 thực hiện việc truy cập đến dữ liệu được share trên PC1, thư mục share trên PC1 có tên là “test adhoc”.

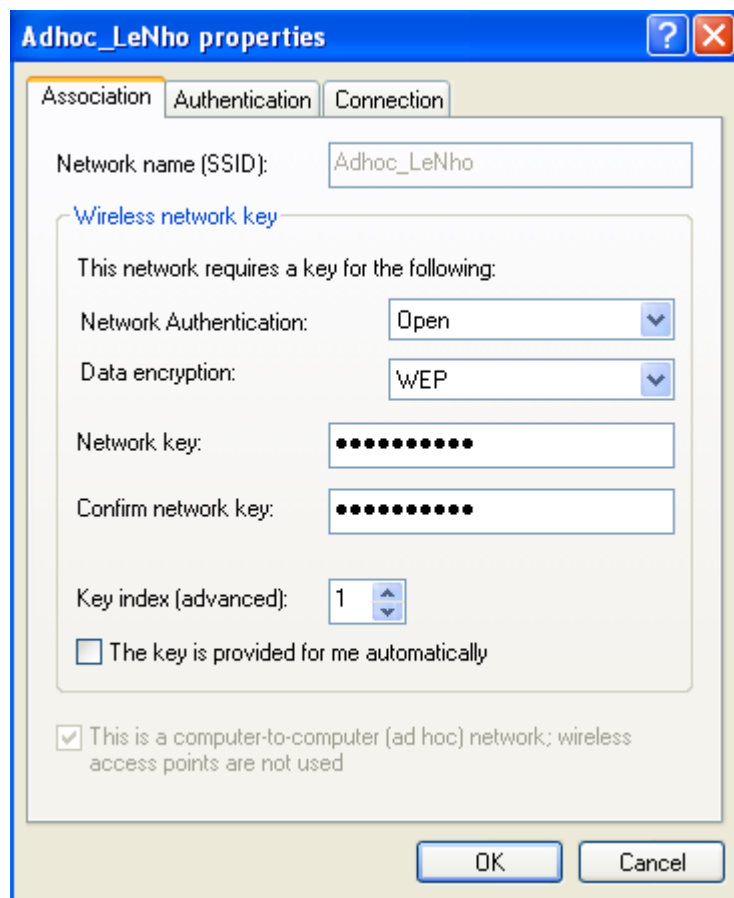


Bước 5: trên PC2 thực hiện lệnh ping google.com để kiểm tra kết nối đi internet của PC2 thông qua PC1 và vào internet explorer thử truy cập đến trang www.google.com

II. TRƯỜNG HỢP CÓ CẤU HÌNH BẢO MẬT WEP KEY

1. Cấu hình trên PC 1:

Ta thực hiện tương tự từ bước 1 đến bước 6. Nhưng ở bước 3 hộp thoại Wireless network properties xuất hiện. Nhập tên mạng (SSID) = Adhoc_LeNho, Data encryption = WEP, nhập Wep key trong Network key và chọn các thông số như hình vẽ bên dưới. Sau đó nhấn OK.



2. Cấu hình trên PC 2:

Ta thực hiện tương tự từ bước 1 đến bước 5. Nhưng ở bước 1 có hộp thoại yêu cầu nhập WEP KEY, ta nhập WEP KEY vào và thực hiện theo các bước ở trên.

III. KẾT LUẬN

Như vậy ta đã thực hiện được việc kết nối giữa PC1 và PC2 với nhau không cần dây cáp mạng mà bằng sóng Wireless. Trong bài Lab này thì PC1 đóng vai trò là 1 Acces Point phát sóng WiFi cho phép các PC chia sẻ file với nhau và thực hiện việc chia sẻ kết nối internet với các PC khác. Còn PC2 là một máy tính bắt sóng WiFi đó và thiết lập kết nối giữa chúng. Ta có thể mở rộng mô hình này với nhiều máy tính cùng kết nối với nhau và có thể thiết lập thành mạng Lan không dây trong nội bộ văn phòng hay công ty theo hình vẽ minh họa dưới đây.

THIẾT LẬP MẠNG WIFI CHIA SẺ LAN VÀ INTERNET KHÔNG CẦN ACSESS POINT

Bài tập 3

CẤU HÌNH ROUTER WIRELESS TP – LINK

Phần 1: Các bước cấu hình Router Wireless TP – Link TD W8910G

Bước 1: Login vào trang chủ

Vào trình duyệt web, gõ địa chỉ <http://192.168.1.1>

nhập username: admin

password: admin

nhấn OK để vào Router



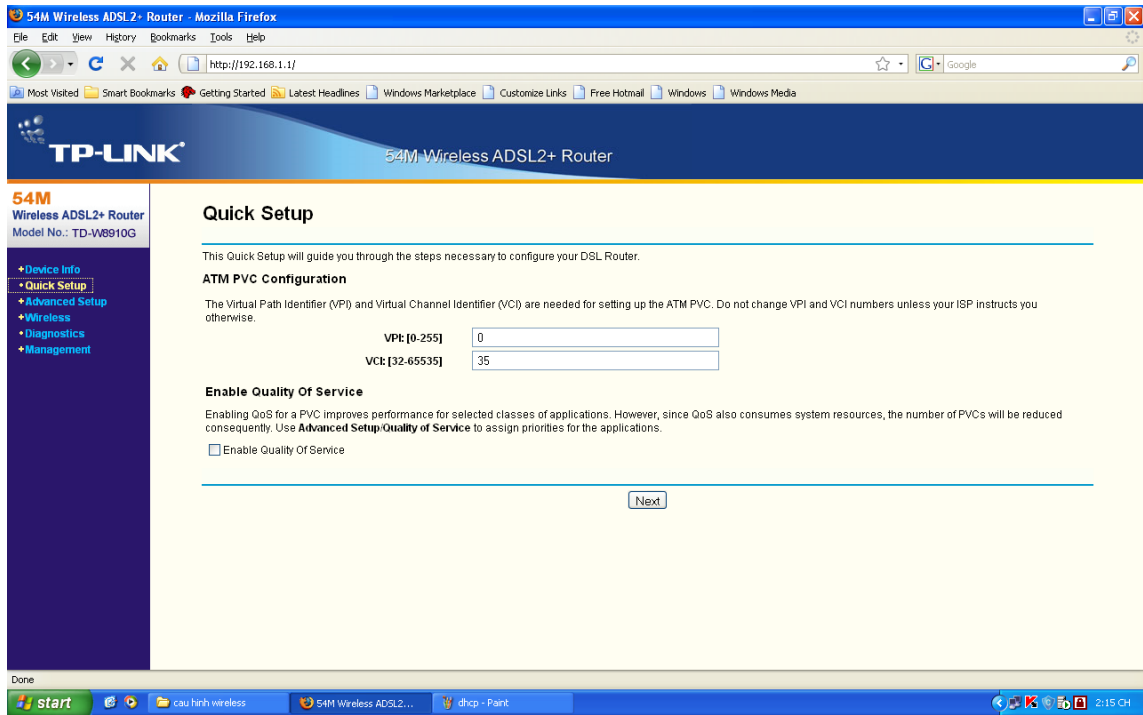
Bước 2: Vào mục Quick Setup (thiết lập nhanh)

Nhập giá trị VPI và VCI của nhà cung cấp dịch vụ.

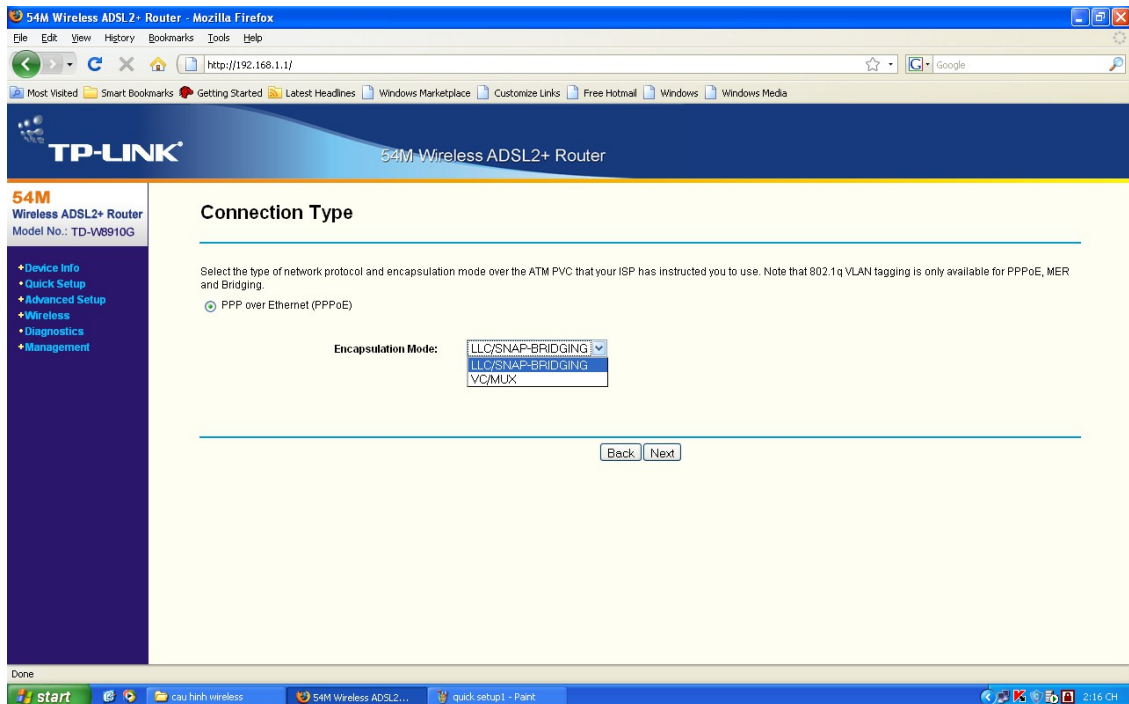
VPI - Virtual Path Identifier và VCI – Virtual Channel Identifier: cần cho việc thiết lập ATM PVC.

Ví dụ: của VNPT là (VPI = 0, VCI = 35), của EVNTelecom là (VPI = 8, VCI = 35)

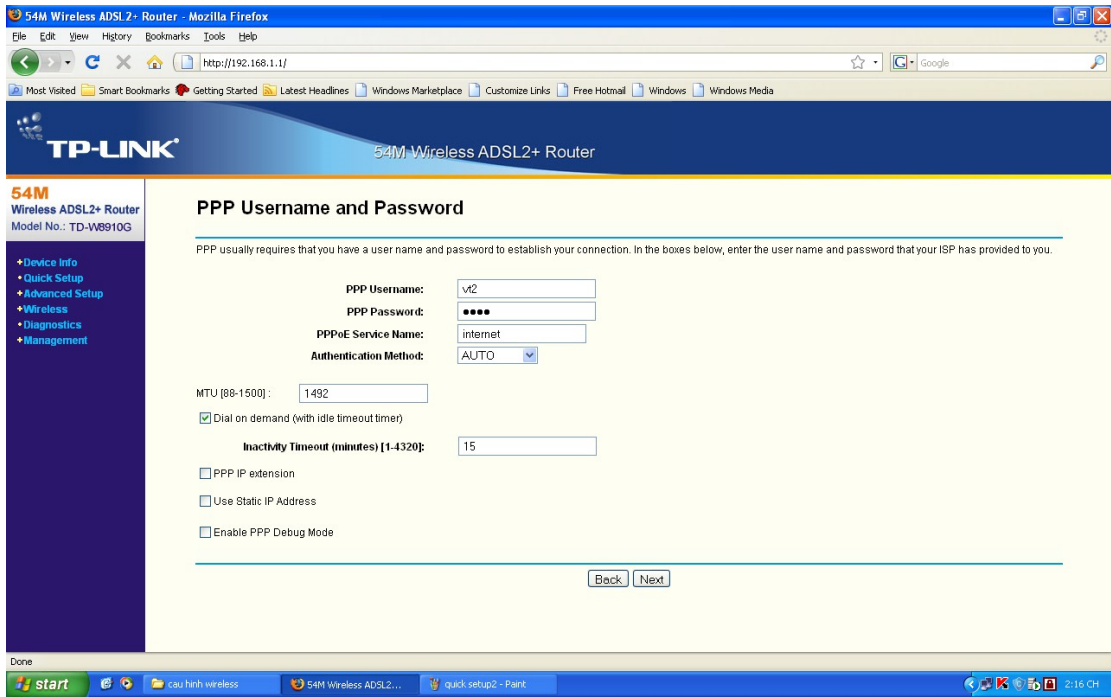
Nhấn Next để tiếp tục



Bước 3: Chọn kiểu kết nối (connection type): chúng ta chọn mode PPPoE và chọn mode Encapsulation = LLC/SNAP-BRIDGING.
Nhấn Next để tiếp tục



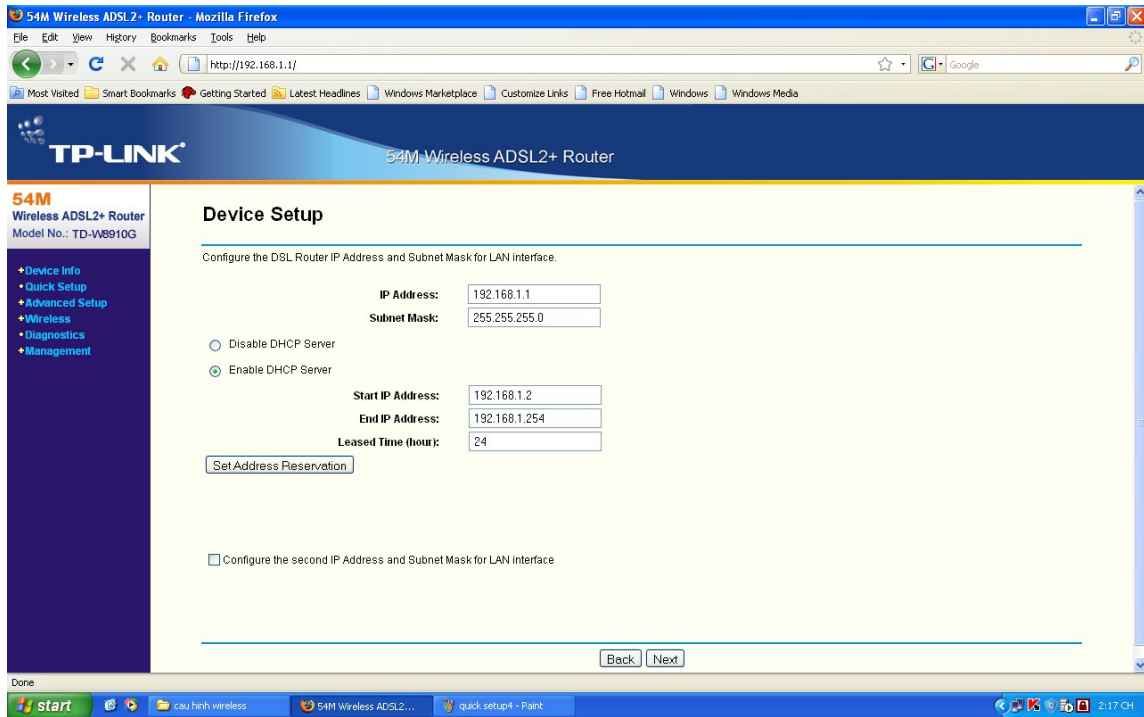
Bước 4: Nhập PPP Username và Password được cung cấp bởi nhà cung cấp dịch vụ
Nhấn Next để tiếp tục



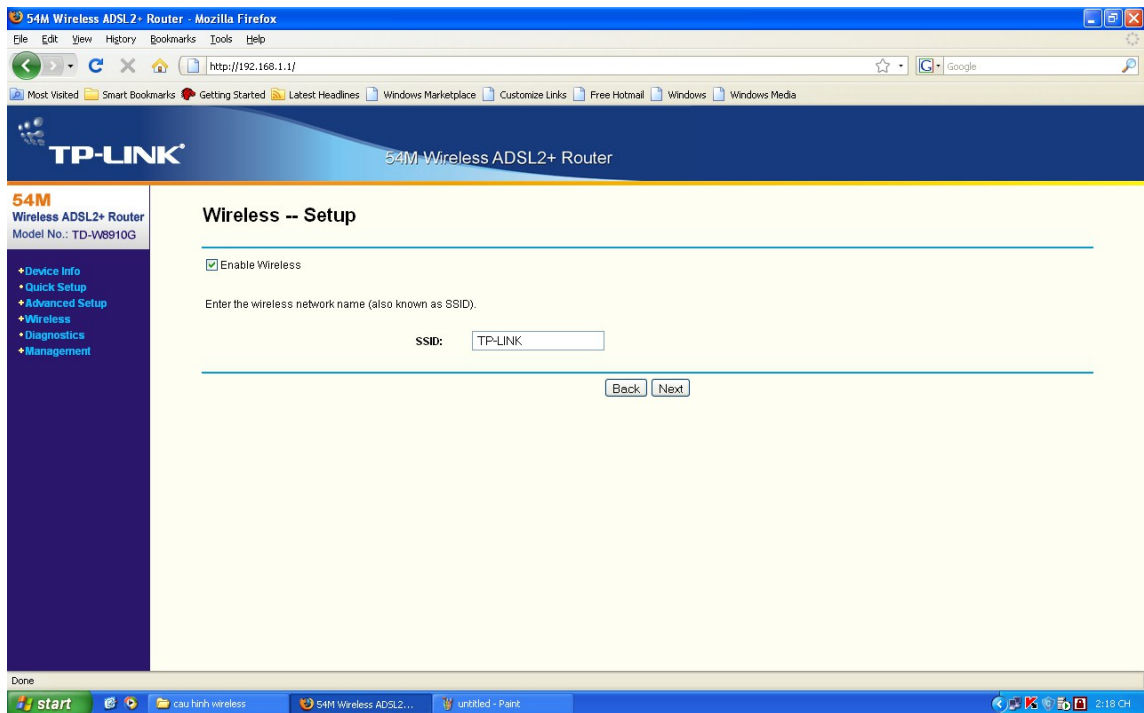
Bước 5: Thiết lập Enable cho IGMP Multicast và Wan Service Nhấn Next để tiếp tục



Bước 6: Thiết lập địa chỉ IP của thiết bị (nếu cần) và Enable DHCP Server Nhấn Next để tiếp tục



Bước 7: Thiết lập “Enable Wireless” và nhập SSID cho thiết bị (thông thường là tên của công ty hay tổ chức của mình).
Nhấn Next để tiếp tục



Bước 8: Sẽ xuất hiện màn hình Wan Setup – Summary.
kích chuột vào nút Save/Reboot để lưu các thiết lập và reboot Router.

54M Wireless ADSL2+ Router - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://192.168.1.1/

Most Visited Smart Bookmarks Getting Started Latest Headlines Windows Marketplace Customize Links Free Hotmail Windows Windows Media

TP-LINK 54M Wireless ADSL2+ Router

54M
Wireless ADSL2+ Router
Model No.: TD-W8910G

- Device Info
- Quick Setup
- Advanced Setup
- Wireless
- Diagnostics
- Management

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

VPI / VCI:	0 / 35
Connection Type:	PPPoE
Service Name:	pppoe_0_35_2
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Enabled
Quality Of Service:	Disabled

Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications.

NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.

[Back](#) [Save/Reboot](#)

Done

start cau hinh wireless 54M Wireless ADSL2... untitled - Paint 2:18 CH

* Các cấu hình nâng cao cho Modem Wifi

Bước 1: Cấu hình các thông số cơ bản của Wireless, như Enable Wireless, Enable SSID Broadcast, đặt SSID

54M Wireless ADSL2+ Router - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://192.168.1.1/

Most Visited Smart Bookmarks Getting Started Latest Headlines Windows Marketplace Customize Links Free Hotmail Windows Windows Media

TP-LINK 54M Wireless ADSL2+ Router

54M
Wireless ADSL2+ Router
Model No.: TD-W8910G

- Device Info
- Quick Setup
- Advanced Setup
- Wireless
 - Basic
 - Security
 - MAC Filter
 - Advanced
 - Statistics
 - Diagnostics
 - Management

Wireless -- Basic

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements. Click "Save/Apply" to configure the basic wireless options.

Enable Wireless

Enable SSID Broadcast

SSID:

BSSID:

Region:

Warning: Ensure you select a correct region to conform local law. Incorrect settings may cause interference.

[Save/Apply](#)

Done

start cau hinh wireless 54M Wireless ADSL2... quick setup7 - Paint 2:29 CH

Bước 2: Cấu hình security cho Wireless.

Bật chế độ chứng thực (Network Authentications = Open)

Enable mã hoá WEP (WEP Encryption = Enable)

Thiết lập số bit mã hóa (Encryption Stringth = 64-bit)

Thiết lập số Key hiện tại của mạng (Current Network Key = 1)

Thiết lập Key của mạng (Network Key 1 = 0905868586) (Nếu textbox này trống thì mạng Wifi sẽ không có tính bảo mật)

The screenshot shows the configuration interface for a TP-Link 54M Wireless ADSL2+ Router. The browser window is titled "54M Wireless ADSL2+ Router - Mozilla Firefox" and the address bar shows "http://192.168.1.1/". The page header includes the TP-LINK logo and the router model name. The main content area is titled "Wireless -- Security" and contains the following configuration options:

- Network Authentication:** Open
- WEP Encryption:** Enabled
- Encryption Strength:** 64-bit
- Current Network Key:** 1
- Network Key 1:** 0905868586
- Network Key 2:** (empty)
- Network Key 3:** (empty)
- Network Key 4:** (empty)

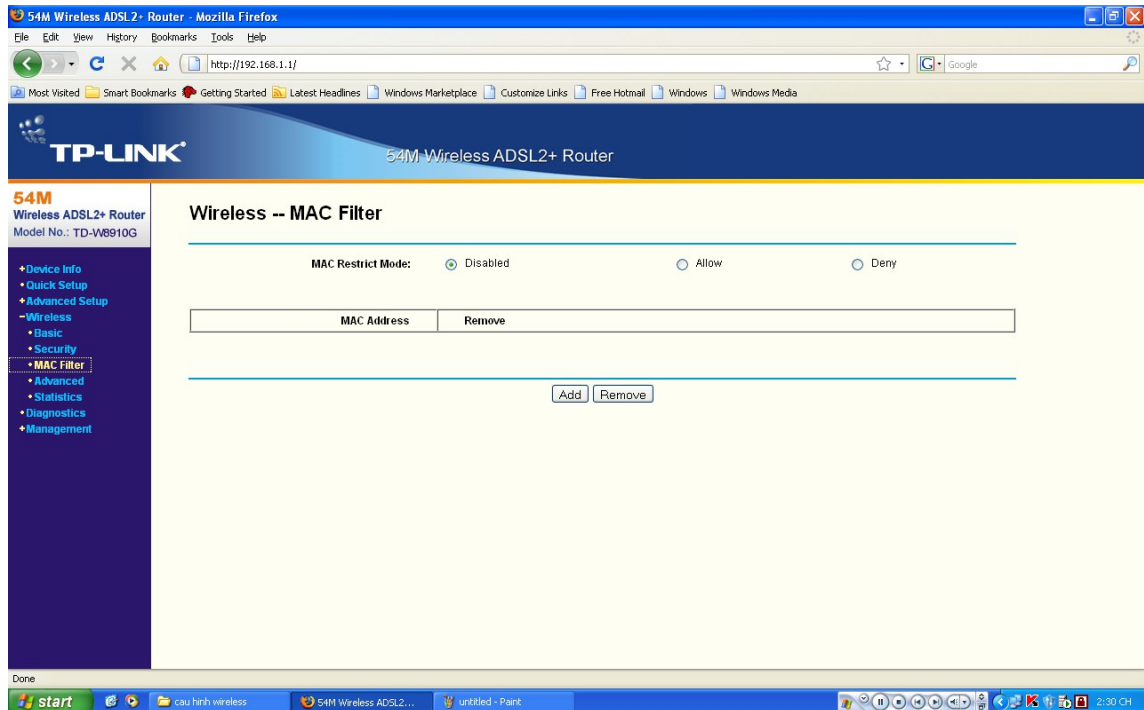
Below the keys, there are instructions: "Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys", "Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys", and "Enter 16 ASCII characters or 32 hexadecimal digits for 152-bit encryption keys". A "Save/Apply" button is located at the bottom of the configuration area.

Bước 3: Cấu hình lọc (Filter) MAC Address của các máy tính trong mạng.

Disabled: tắt chế độ lọc Mac address

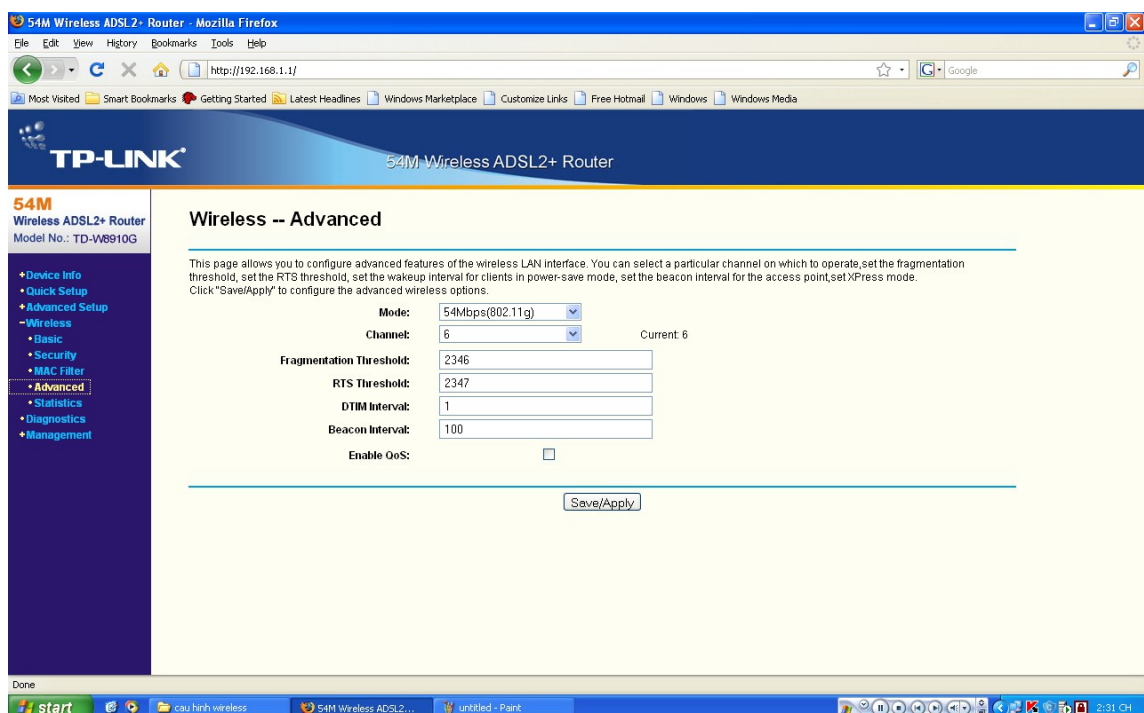
Allow: bật chế độ lọc Mac address, và cho phép các máy tính có Mac Address trong bảng được truy cập

Deny: bật chế độ lọc Mac address, và không cho phép các máy tính có Mac Address trong bảng được truy cập



Bước 4: cấu hình Wireless Advanced

Mode = 54Mbps(802.11g), còn các giá trị khác để mặc định



* Xem các thông tin về thiết bị (Device Info)

Bước 1: Device Info: xem các thông tin về:

Phiên bản phần mềm (Firmware Version)

Phiên bản phần cứng (Hardware Version)

Địa chỉ IP của mạng Lan (Lan IP Address)

DNS Server chính (Primary DNS Server)

DNS Server phụ (Secondary DNS Server)

54M Wireless ADSL2+ Router
Model No.: TD-W8910G

Device Info

Firmware Version:	1.3.4 Build 080731 Rel.35756n
Hardware Version:	TD-W8910G v2 0000235b

This information reflects the current status of your DSL connection.

Line Rate - Upstream (Kbps):	
Line Rate - Downstream (Kbps):	
LAN IP Address:	192.168.1.1
Default Gateway:	
Primary DNS Server:	192.168.1.1
Secondary DNS Server:	192.168.1.1

Bước 2: Wan Info: thông tin về các thiết lập cấu hình của mạng Wireless

54M Wireless ADSL2+ Router
Model No.: TD-W8910G

WAN Info

VPI/VCI	Category	Service	Interface	Protocol	IGMP	QoS	State	Status	IP Address	ppp Link Ctrl
0/35	UBR	pppoe_0_35_1	ppp_0_35_1	PPPoE	Enabled	Disabled	Enabled	ADSL Link Down		Connecting...

Bước 3: Statics – Lan: xem thông tin về các interface của Router

The screenshot shows the TP-Link 54M Wireless ADSL2+ Router web interface. The browser address bar shows the URL http://192.168.1.1/. The page title is "54M Wireless ADSL2+ Router". The left sidebar contains a navigation menu with the following items: Device Info, Summary, WAN, Statistics, LAN (selected), WAN, ATM, ADSL, Route, ARP, DHCP, Quick Setup, Advanced Setup, Wireless, Diagnostics, and Management. The main content area is titled "Statistics -- LAN" and displays a table with the following data:

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
Ethernet	119069	868	0	0	407310	938	0	0
Wireless	0	0	0	0	14123	160	0	0

Bước 4: Device Info – ARP

xem các địa chỉ Mac Address của các máy tính kết nối đến Wireless

The screenshot shows the TP-Link 54M Wireless ADSL2+ Router web interface. The browser address bar shows the URL http://192.168.1.1/. The page title is "54M Wireless ADSL2+ Router". The left sidebar contains a navigation menu with the following items: Device Info, Summary, WAN, Statistics, Route, ARP (selected), DHCP, Quick Setup, Advanced Setup, Wireless, Diagnostics, and Management. The main content area is titled "Device Info -- ARP" and displays a table with the following data:

IP address	Flags	HW Address	Device
192.168.1.2	Complete	00:23:8B:28:84:A2	br0

Bước 5: Device Info – Route

xem thông tin về bảng định tuyến (Route) của Wireless

54M Wireless ADSL2+ Router - Mozilla Firefox

http://192.168.1.1/

TP-LINK 54M Wireless ADSL2+ Router

54M Wireless ADSL2+ Router
Model No.: TD-W8910G

Device Info

- Summary
- WAN
- Statistics
- Route
- ARP
- DHCP
- Quick Setup
- Advanced Setup
- Wireless
- Diagnostics
- Management

Device Info -- Route

Flags: U - up, I - reject, G - gateway, H - host, R - reinstate
D - dynamic (redirect), M - modified (redirect).

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
10.112.113.207	0.0.0.0	255.255.255.255	UH	0	pppoe_0_35_1	ppp_0_35_1
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0

Done

start | cau hinh wireless | 54M Wireless ADSL2+... | static_addr - Paint | 2:13 CH

Bước 6: Device Info – DHCP Leases

xem thông tin về các địa chỉ IP được cấp thông qua DHCP

54M Wireless ADSL2+ Router - Mozilla Firefox

http://192.168.1.1/

TP-LINK 54M Wireless ADSL2+ Router

54M Wireless ADSL2+ Router
Model No.: TD-W8910G

Device Info

- Summary
- WAN
- Statistics
- Route
- ARP
- DHCP
- Quick Setup
- Advanced Setup
- Wireless
- Diagnostics
- Management

Device Info -- DHCP Leases

Hostname	MAC Address	IP Address	Expires In
LETIENDUNG	00:23:8B:28:84:A2	192.168.1.2	23 hours, 54 minutes, 2 seconds

Done

start | cau hinh wireless | 54M Wireless ADSL2+... | arp - Paint | 2:14 CH

BÀI 4 BẢO MẬT VÀ QUẢN LÝ MẠNG KHÔNG DÂY

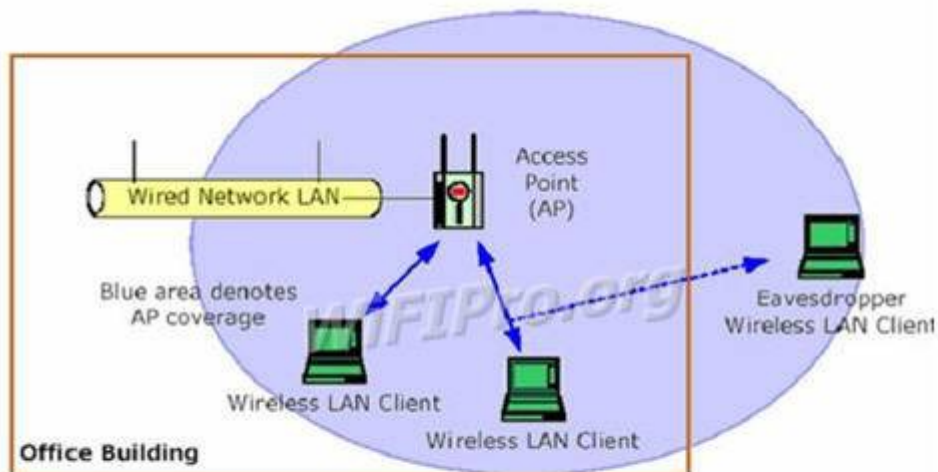
Mã bài: 39.4

Mục tiêu:

- Mô tả được cấu trúc mạng không dây;
- Thiết kế được một mạng không dây cục bộ (WLAN);
- Phân biệt được ưu và nhược điểm của mạng không dây;
- Phân biệt được các chế độ của AP.
- Thực hiện các thao tác an toàn với máy tính.

1. Tại sao phải bảo mật mạng không dây(WLAN)

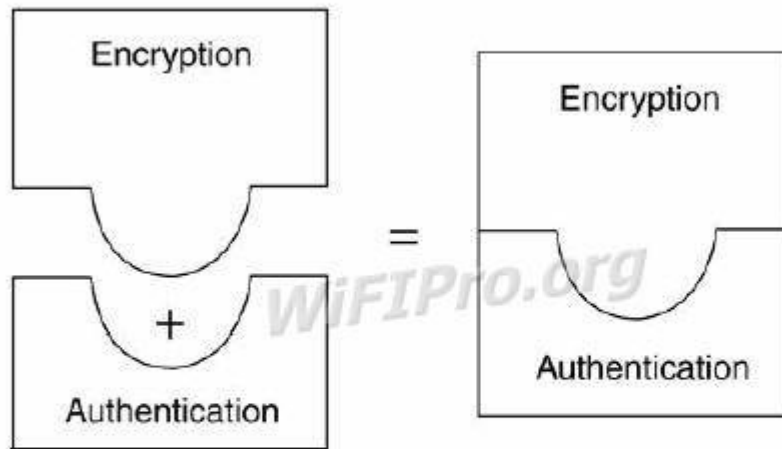
Để kết nối tới một mạng LAN hữu tuyến ta cần phải truy cập theo đường truyền bằng dây cáp, phải kết nối một PC vào một cổng mạng. Với mạng không dây ta chỉ cần có máy của ta trong vùng sóng bao phủ của mạng không dây. Điều khiển cho mạng có dây là đơn giản: đường truyền bằng cáp thông thường được đi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



Để cung cấp mức bảo mật tối thiểu cho mạng WLAN thì ta cần hai thành phần sau:

Cách thức để xác định ai có quyền sử dụng WLAN - yêu cầu này được thỏa mãn bằng cơ chế xác thực (authentication). Một phương thức để cung cấp tính riêng tư cho các dữ liệu không dây – yêu cầu này được thỏa mãn bằng một thuật toán mã hóa (encryption).

Encryption + Authentication = Wireless Security



2. Các kiểu tấn công mạng WLAN

2.1 .Rogue Access Point

Access Point giả mạo được dùng để mô tả những Access Point được tạo ra một cách vô tình hay cố ý làm ảnh hưởng đến hệ thống mạng hiện có. Nó được dùng để chỉ các thiết bị hoạt động không dây trái phép mà không quan tâm đến mục đích sử dụng của chúng.

Phân loại

+ Access Point được cấu hình không hoàn chỉnh

Một Access Point có thể bất ngờ trở thành 1 thiết bị giả mạo do sai sót trong việc cấu hình. Sự thay đổi trong Service Set Identifier (SSID), thiết lập xác thực, thiết lập mã hóa,... điều nghiêm trọng nhất là chúng sẽ không thể chứng thực các kết nối nếu bị cấu hình sai.

Ví dụ: trong trạng thái xác thực mở (open mode authentication) các người dùng không dây ở trạng thái 1 (chưa xác thực và chưa kết nối) có thể gửi các yêu cầu xác thực đến một Access Point và được xác thực thành công sẽ chuyển sang trạng thái 2 (được xác thực nhưng chưa kết nối). Nếu 1 Access Point không xác nhận sự hợp lệ của một máy khách do lỗi trong cấu hình, kẻ tấn công có thể gửi một số lượng lớn yêu cầu xác thực, làm tràn bảng yêu cầu kết nối của các máy khách ở Access Point, làm cho Access Point từ chối truy cập của các người dùng khác bao gồm cả người dùng được phép truy cập.

+ Access Point giả mạo từ các mạng WLAN lân cận

Các máy khách theo chuẩn 802.11 tự động chọn Access Point có sóng mạnh nhất mà nó phát hiện được để kết nối.

Ví dụ: Windows XP tự động kết nối đến kết nối tốt nhất có thể xung quanh nó. Vì vậy, những người dùng được xác thực của một tổ chức có thể kết nối đến các Access Point của các tổ chức khác lân cận. Mặc dù các Access Point

lân cận không cố ý thu hút kết nối từ các người dùng, những kết nối đó vô tình để lộ những dữ liệu nhạy cảm

+ Access Point giả mạo do kẻ tấn công tạo ra

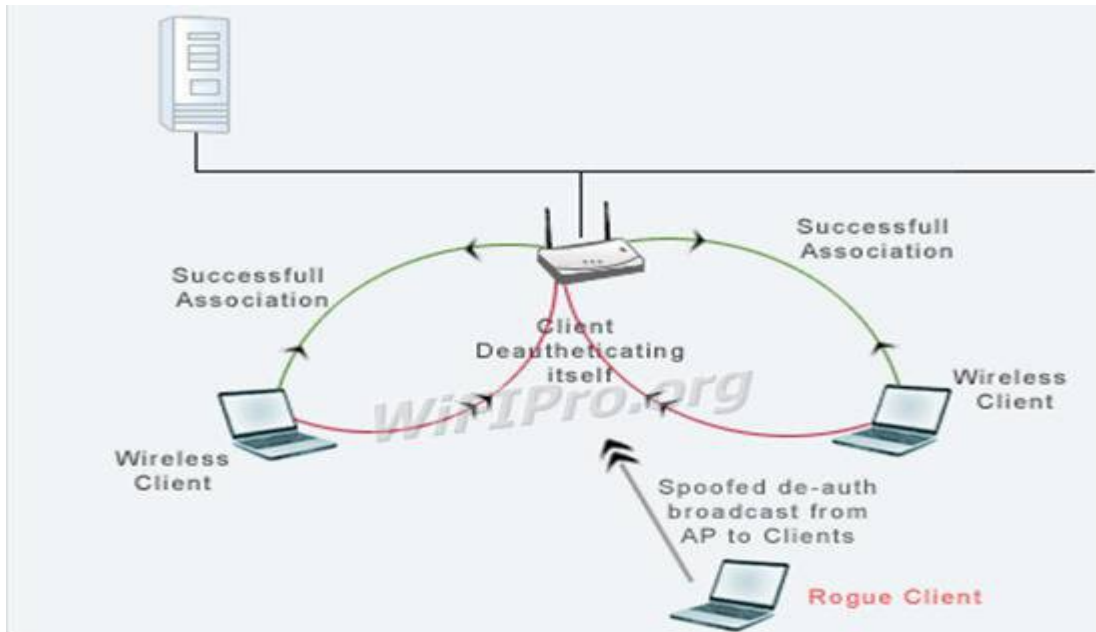
Giả mạo AP là kiểu tấn công “man in the middle” cổ điển. Đây là kiểu tấn công mà tin tặc đứng ở giữa và trộm lưu lượng truyền giữa 2 nút. Kiểu tấn công này rất mạnh vì tin tặc có thể trộm tất cả lưu lượng đi qua mạng. Rất khó khăn để tạo một cuộc tấn công “man in the middle” trong mạng có dây bởi vì kiểu tấn công này yêu cầu truy cập thực sự đến đường truyền. Trong mạng không dây thì lại rất dễ bị tấn công kiểu này. Tin tặc cần phải tạo ra một AP thu hút nhiều sự lựa chọn hơn AP chính thống. AP giả này có thể được thiết lập bằng cách sao chép tất cả các cấu hình của AP chính thống đó là: SSID, địa chỉ MAC v.v..Bước tiếp theo là làm cho nạn nhân thực hiện kết nối tới AP giả.

Trong mạng 802.11 sự lựa chọn AP được thực hiện bởi cường độ của tín hiệu nhận. Điều duy nhất tin tặc phải thực hiện là chắc chắn rằng AP của mình có cường độ tín hiệu mạnh hơn cả. Để có được điều đó tin tặc phải đặt AP của mình gần người bị lừa hơn là AP chính thống hoặc sử dụng kỹ thuật anten định hướng. Sau khi nạn nhân kết nối tới AP giả, nạn nhân vẫn hoạt động như bình thường do vậy nếu nạn nhân kết nối đến một AP chính thống khác thì dữ liệu của nạn nhân đều đi qua AP giả. Tin tặc sẽ sử dụng các tiện ích để ghi lại mật khẩu của nạn nhân khi trao đổi với Web Server. Như vậy tin tặc sẽ có được tất cả những gì anh ta muốn để đăng nhập vào mạng chính thống. Kiểu tấn công này tồn tại là do trong 802.11 không yêu cầu chứng thực 2 hướng giữa AP và nút. AP phát quảng bá ra toàn mạng. Điều này rất dễ bị tin tặc nghe trộm và do vậy tin tặc có thể lấy được tất cả các thông tin mà chúng cần. Các nút trong mạng sử dụng WEP để chứng thực chúng với AP nhưng WEP cũng có những lỗ hổng có thể khai thác. Một tin tặc có thể nghe trộm thông tin và sử dụng bộ phân tích mã hoá để trộm mật khẩu của người dùng

+ Access Point giả mạo được thiết lập bởi chính nhân viên của công ty

Vì sự tiện lợi của mạng không dây một số nhân viên của công ty đã tự trang bị Access Point và kết nối chúng vào mạng có dây của công ty. Do không hiểu rõ và nắm vững về bảo mật trong mạng không dây nên họ vô tình tạo ra một lỗ hổng lớn về bảo mật. Những người lạ vào công ty và hacker bên ngoài có thể kết nối đến Access Point không được xác thực để đánh cắp bằng thông, đánh cắp thông tin nhạy cảm của công ty, sử dụng hệ thống mạng của công ty tấn công người khác,...

2.2. De-authentication Flood Attack(tấn công yêu cầu xác thực lại)

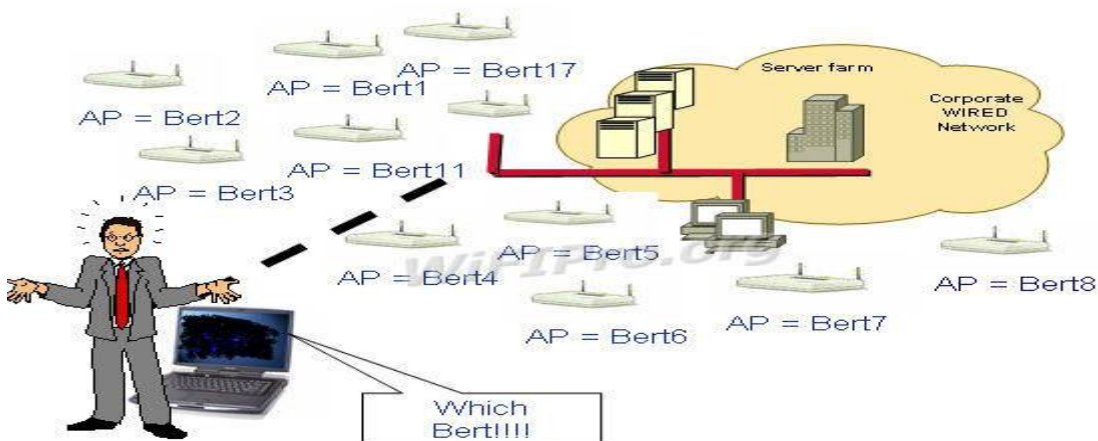


Kẻ tấn công xác định mục tiêu tấn công là các người dùng trong mạng wireless và các kết nối của họ (Access Point đến các kết nối của nó).

- Chèn các frame yêu cầu xác thực lại vào mạng WLAN bằng cách giả mạo địa chỉ MAC nguồn và đích lần lượt của Access Point và các người dùng.
- Người dùng wireless khi nhận được frame yêu cầu xác thực lại thì nghĩ rằng chúng do Access Point gửi đến.
- Sau khi ngắt được một người dùng ra khỏi dịch vụ không dây, kẻ tấn công tiếp tục thực hiện tương tự đối với các người dùng còn lại.
- Thông thường người dùng sẽ kết nối lại để phục hồi dịch vụ, nhưng kẻ tấn công đã nhanh chóng tiếp tục gửi các gói yêu cầu xác thực lại cho người dùng.

2.3. Fake Access Point

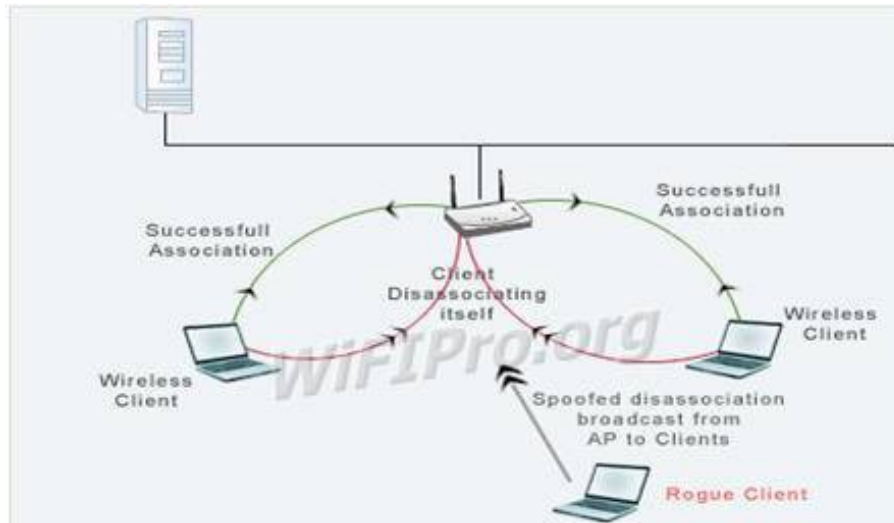
Kẻ tấn công sử dụng công cụ có khả năng gửi các gói beacon với địa chỉ vật lý (MAC) giả mạo và SSID giả để tạo ra vô số Access Point giả lập. Điều này làm xáo trộn tất cả các phần mềm điều khiển card mạng không dây của người dùng



2.4. Tấn công dựa trên sự cảm nhận sóng mang lớp vật lý

Kẻ tấn công lợi dụng giao thức chống ñụng ñộ CSMA/CA, tức là nó sẽ làm cho tất cả người dùng nghĩ rằng lúc nào trong mạng cũng có 1 máy tính đang truyền thông. Điều này làm cho các máy tính khác luôn luôn ở trạng thái chờ ñợi kẻ tấn công ấy truyền dữ liệu xong dẫn đến tình trạng ñổn trong mạng. Tần số là một nhược ñiểm bảo mật trong mạng không dây. Mức ñộ nguy hiểm thay ñổi phụ thuộc vào giao diện của lớp vật lý. Có một vài tham số quyết ñịnh sự chịu ñựng của mạng là: năng lượng máy phát, ñộ nhạy của máy thu, tần số RF, băng thông và sự ñịnh hướng của anten. Trong 802.11 sử dụng thuật toán đa truy cập cảm nhận sóng mang (CSMA) để tránh va chạm. CSMA là một thành phần của lớp MAC. CSMA được sử dụng để chắc chắn rằng sẽ không có va chạm dữ liệu trên ñường truyền. Kiểu tấn công này không sử dụng tạp âm để tạo ra lỗi cho mạng nhưng nó sẽ lợi dụng chính chuẩn ñó. Có nhiều cách để khai thác giao thức cảm nhận sóng mang vật lý. Cách ñơn giản là làm cho các nút trong mạng ñều tin tưởng rằng có một nút đang truyền tin tại thời ñiểm hiện tại. Cách ñể nhất ñạt được điều này là tạo ra một nút giả mạo để truyền tin một cách liên tục. Một cách khác là sử dụng bộ tạo tín hiệu RF. Một cách tấn công tinh vi hơn là làm cho card mạng chuyển vào chế ñộ kiểm tra mà ở ñó nó truyền đi liên tiếp một mẫu kiểm tra. Tất cả các nút trong phạm vi của một nút giả là rất nhạy với sóng mang và trong khi có một nút đang truyền thì sẽ không có nút nào được truyền.

2.5. Tấn công ngắt kết nối (Disassociation flood attack)



Kẻ tấn công xác ñịnh mục tiêu (wireless clients) và mối liên kết giữa AP với các clients. Kẻ tấn công gửi disassociation frame bằng cách giả mạo Source và Destination MAC đến AP và các client tương ứng. Client sẽ nhận các frame này và nghĩ rằng frame hủy kết nối đến từ AP. Ñồng thời kẻ tấn công cũng gửi disassociation frame đến AP.

Sau khi ñã ngắt kết nối của một client, kẻ tấn công tiếp tục thực hiện tương tự với các client còn lại làm cho các client tự ñộng ngắt kết nối với AP. Khi

các clients bị ngắt kết nối sẽ thực hiện kết nối lại với AP ngay lập tức. Kế tiếp công tiếp tục gửi disassociation frame đến AP và client

Có thể ta sẽ rất dễ nhầm lẫn giữa 2 kiểu tấn công : Disassociation flood attack và De-authentication Flood Attack. Giống nhau : về hình thức tấn công , có thể cho rằng chúng giống nhau vì nó giống như một đại bác 2 nòng , vừa tấn công **Access Point** vừa tấn công Client. Và quan trọng hơn hết , chúng "nả pháo" liên tục.

Khác nhau :

+ De-authentication Flood Attack : yêu cầu cả AP và client gửi lại frame xác thực dẫn đến xác thực failed

+ Disassociation flood attack : gửi disassociation frame làm cho AP và client tin tưởng rằng kết nối giữa chúng đã bị ngắt.

*** Tổng kết:**

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

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

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

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

rằng một thế giới không có dây thì ít rối rắm phức tạp hơn và việc sử dụng mạng không dây trong gia đình của bạn sẽ được cải thiện đáng kể.

3. Bảo mật mạng không dây(WLAN)

Một WLAN gồm có 3 phần: Wireless Client, Access Points và Access Server.

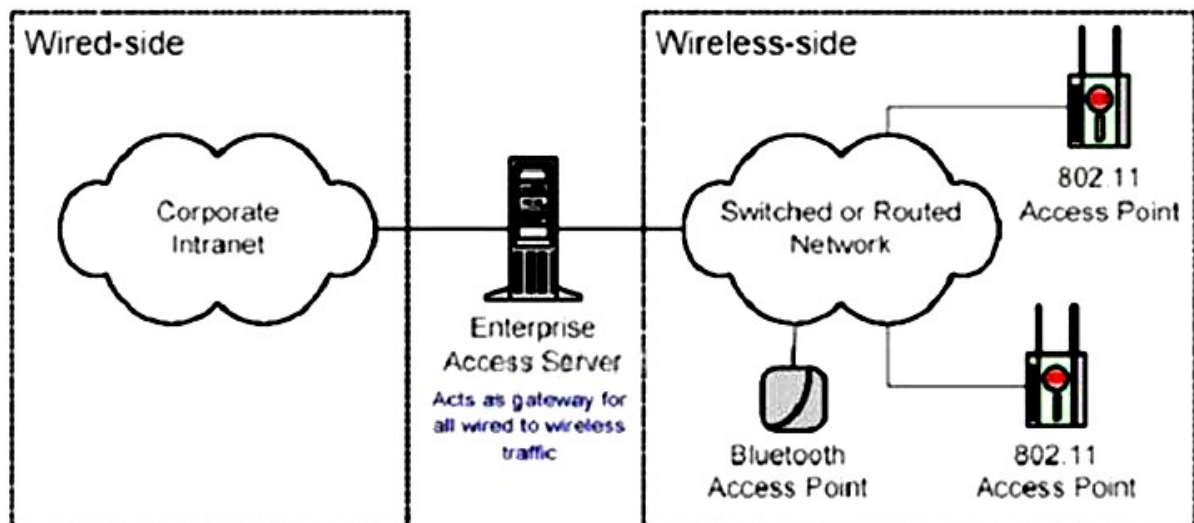
+ Wireless Client điển hình là một chiếc laptop với NIC (Network Interface Card) không dây được cài đặt để cho phép truy cập vào mạng không dây.

+ Access Points (AP) cung cấp sự bao phủ của sóng vô tuyến trong một vùng nào đó (được biết đến như là các cell (tế bào)) và kết nối đến mạng không dây.

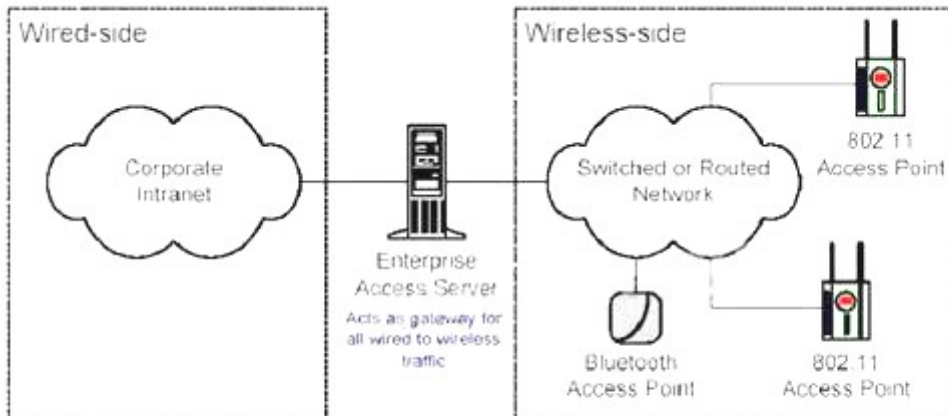
+ Còn Access Server điều khiển việc truy cập. Một Access Server (như là Enterprise Access Server (EAS)) cung cấp sự điều khiển, quản lý, các đặc tính bảo mật tiên tiến cho mạng không dây Enterprise

Một bộ phận không dây có thể được kết nối đến các mạng không dây tồn tại theo một số cách. Kiến trúc tổng thể sử dụng EAS trong “Gateway Mode” hay “Controller Mode”.

Trong Gateway Mode (hình 3-4) EAS được đặt ở giữa mạng AP và phần còn lại của mạng Enterprise. Vì vậy EAS điều khiển tất cả các luồng lưu lượng giữa các mạng không dây và có dây và thực hiện như một tường lửa



Trong **Controll Mode** (hình 3-3), EAS quản lý các AP và điều khiển việc truy cập đến mạng không dây, nhưng nó không liên quan đến việc truyền tải dữ liệu người dùng. Trong chế độ này, mạng không dây có thể bị phân chia thành mạng dây với firewall thông thường hay tích hợp hoàn toàn trong mạng dây Enterprise. Kiến trúc WLAN hỗ trợ một mô hình bảo mật được thể hiện trên hình 4. Mỗi một phần tử bên trong mô hình đều có thể cấu hình theo người quản lý mạng để thỏa mãn và phù hợp với những gì họ cần



VPN

VPN wireless client connectivity (IPSec)



Firewall

Packet filtering/port blocking to protect enterprise networks from wireless intruders



Authentication

Mutual authentication between client devices, users and the network (802.1x EAP-TLS using certificates)



Encryption

Encrypting data to prevent eavesdropping (Dynamic WEP, 802.1x EAP-TLS and 3DES)



Device Authorization

Authorizing network access to wireless devices (MAC address access control)

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

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

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

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

enable hay disable.

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

3.1. WEP

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

Chức năng chính của WEP là dựa trên khóa, là yếu tố cơ bản cho thuật toán mã hóa. Khóa WEP là một chuỗi kí tự và số được sử dụng theo 2 cách: Khóa WEP được sử dụng để định danh xác thực client. Khóa WEP được dùng để mã hóa dữ liệu. Khi client sử dụng WEP muốn kết nối với AP thì AP sẽ xác định xem client có giá trị khóa chính xác hay không? Chính xác ở đây có nghĩa là client đã có khóa là một phần của hệ thống phân phát khóa WEP được cài đặt trong WLAN. Khóa WEP phải khớp ở cả hai đầu xác thực client và AP. Hầu hết các AP và client có khả năng lưu trữ 4 khóa WEP đồng thời. Một lý do hứa ích của việc sử dụng nhiều khóa WEP chính là phân đoạn mạng. Giả sử mạng có 80 client thì ta sử dụng 4 khóa WEP cho 4 nhóm khác nhau thay vì sử dụng 1 khóa. Nếu khóa WEP bị ***** thì ta chỉ cần thay đổi khóa WEP cho 20 client thay vì phải thay đổi cho toàn bộ mạng. Một lí do khác để có nhiều khóa WEP là trong môi trường hỗn hợp có card hỗ trợ 128 bit và có card chỉ hỗ trợ 64 bit. Trong trường hợp này chúng ta có thể phân ra hai nhóm người dùng.

❖ Giải pháp WEP tối ưu:

Với những điểm yếu nghiêm trọng của WEP và sự phát tán rộng rãi của các công cụ dò tìm khóa WEP trên Internet, giao thức này không còn là giải pháp bảo mật được chọn cho các mạng có mức độ nhạy cảm thông tin cao. Tuy nhiên, trong rất nhiều các thiết bị mạng không dây hiện nay, giải pháp bảo mật dữ liệu được hỗ trợ phổ biến vẫn là WEP. Dù sao đi nữa, các lỗ hổng của WEP vẫn có thể được giảm thiểu nếu được cấu hình đúng, đồng thời sử dụng các biện pháp an ninh khác mang tính chất hỗ trợ. Để gia tăng mức độ bảo mật cho WEP và gây khó khăn cho hacker, các biện pháp sau được đề nghị:

Sử dụng khóa WEP có độ dài 128 bit: Thường các thiết bị WEP cho phép cấu hình khóa ở ba độ dài: 40 bit, 64 bit, 128 bit. Sử dụng khóa với độ dài 128 bit gia tăng số lượng gói dữ liệu hacker cần phải có để phân tích IV, gây khó khăn và kéo dài thời gian giải mã khóa WEP

- Thực thi chính sách thay đổi khóa WEP định kỳ: Do WEP không hỗ trợ phương thức thay đổi khóa tự động nên sự thay đổi khóa định kỳ sẽ gây khó khăn cho người sử dụng. Tuy nhiên, nếu không đổi khóa WEP thường xuyên

thì cũng nên thực hiện ít nhất một lần trong tháng hoặc khi nghi ngờ có khả năng bị lộ khóa.

- Sử dụng các công cụ theo dõi số liệu thống kê dữ liệu trên đường truyền không dây: Do các công cụ dò khóa WEP cần bắt được số lượng lớn gói dữ liệu và hacker có thể phải sử dụng các công cụ phát sinh dữ liệu nên sự đột biến về lưu lượng dữ liệu có thể là dấu hiệu của một cuộc tấn công WEP, đánh động người quản trị mạng phát hiện và áp dụng các biện pháp phòng chống kịp thời.

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

3.2. Kích thước ô

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

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

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

3.3. Chứng thực người dùng

Từ khi sự chứng thực người dùng là liên kết kém cỏi nhất của WLAN, và chuẩn 802.11 không chỉ định các phương pháp chứng thực người dùng, thì đó

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

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

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

3.4. Theo dõi WLAN

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

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

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

3.4.1. Yêu cầu cho WLAN

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

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

có thêm những giải pháp để có thể hỗ trợ, phân bổ một cách tự nhiên trong mạng.

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

3.4.2. Quản lý cấu hình

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

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

Theo dõi tốc độ xử lý của máy và cấu hình phần dây phụ để chắc rằng những AP và những trạm còn lại vẫn trong trạng thái cấu hình xác định. Sự tràn năng lượng hoặc ngưng hoạt động có thể làm cho AP tự động xác lập lại các thiết lập mặc định. Các nhân viên có thể thay đổi những thiết lập cho thiết bị để có thể truy cập mạng trở lại. Phân tích lưu lượng của mạng không dây để nhận dạng các mạng cấu hình sai.

3.4.3. Chẩn đoán lỗi

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

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

3.4.4. Theo dõi sự thực thi

Sau lần đầu tiên chắc rằng mạng đã hoạt động, những người quản lý mạng phải theo dõi và phân tích việc hoạt động của một WLAN bảo đảm

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

3.5. Gán chính sách(POLICY)

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

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

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

3.6. WLAN VPN

Mạng riêng ảo VPN bảo vệ mạng WLAN bằng cách tạo ra một kênh che chắn dữ liệu khỏi các truy cập trái phép. VPN tạo ra một tin cậy cao thông qua việc sử dụng một cơ chế bảo mật như IPSec (Internet Protocol Security). IPSec dùng các thuật toán mạnh như Data Encryption Standard (DES) và Triple DES (3DES) để mã hóa dữ liệu, và dùng các thuật toán khác để xác thực gói dữ liệu. IPSec cũng sử dụng thể xác nhận số để xác nhận khóa mã (public key). Khi được sử dụng trên mạng WLAN, cổng kết nối của VPN đảm nhận việc xác thực, đóng gói và mã hóa.



2. TKIP (Temporal Key Integrity Protocol)

Là giải pháp của IEEE được phát triển năm 2004. Là một nâng cấp cho WEP nhằm vá những vấn đề bảo mật trong cài đặt mã dòng RC4 trong WEP. TKIP dùng hàm băm (hashing) IV để chống lại việc giả mạo gói tin, nó cũng cung cấp phương thức để kiểm tra tính toàn vẹn của thông điệp MIC (message integrity check) để đảm bảo tính chính xác của gói tin. TKIP sử dụng khóa động bằng cách đặt cho mỗi frame một chuỗi số riêng để chống lại dạng tấn công giả mạo

3. AES (Advanced Encryption Standard)

Là một chức năng mã hóa được phê chuẩn bởi NIST (Nation Institute of Standard and Technology). IEEE đã thiết kế một chế độ cho AES để đáp ứng nhu cầu của mạng WLAN. Chế độ này được gọi là CBC-CTR (Cipher Block Chaining Counter Mode) với CBC-MAC (Cipher Block Chaining Message Authenticity Check). Tổ hợp của chúng được gọi là AES-CCM. Chế độ CCM là sự kết hợp của mã hóa CBC-CTR và thuật toán xác thực thông điệp CBC-MAC. Sự kết hợp này cung cấp cả việc mã hóa cũng như kiểm tra tính toàn vẹn của dữ liệu gửi

Mã hóa CBC-CTR sử dụng một biến đếm để bổ sung cho chuỗi khóa. Biến đếm sẽ tăng lên 1 sao khi mã hóa cho mỗi khối (block). Tiến trình này đảm bảo chỉ có duy nhất một khóa cho mỗi khối. Chuỗi ký tự chưa được mã hóa sẽ được phân mảnh ra thành các khối 16 byte.

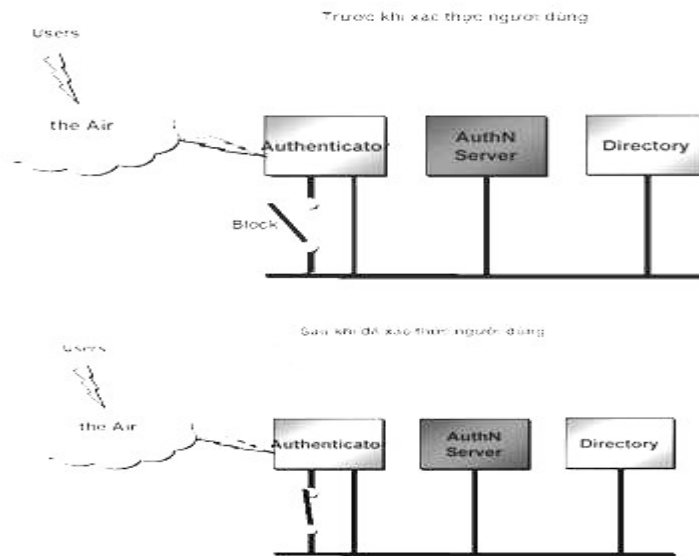
CBC-MAC hoạt động bằng cách sử dụng kết quả của mã hóa CBC cùng với chiều dài frame, địa chỉ nguồn, địa chỉ đích và dữ liệu. Kết quả sẽ cho ra giá trị 128 bit và được cắt thành 64 bit để sử dụng lúc truyền thông.

AES-CCM yêu cầu chi phí khá lớn cho cả quá trình mã hóa và kiểm tra tính toàn vẹn của dữ liệu gửi nên tiêu tốn rất nhiều năng lực xử lý của CPU khá lớn.

4. 802.1x và EAP

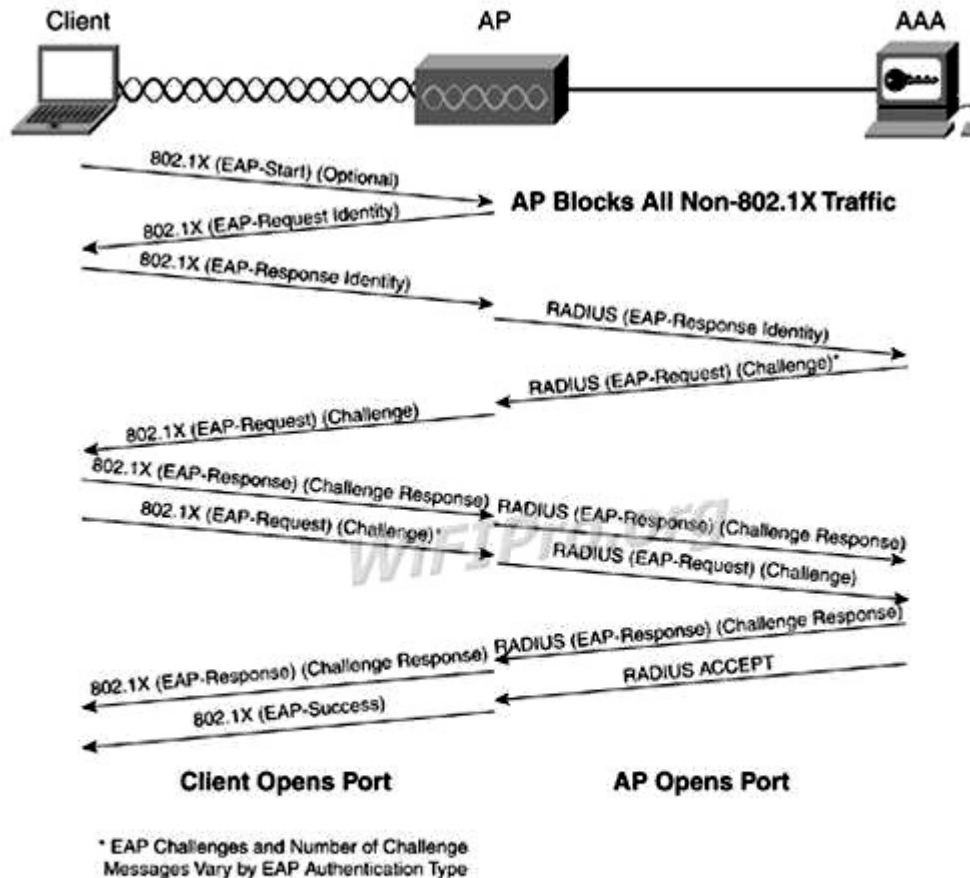
802.1x là chuẩn đặc tả cho việc truy cập dựa trên cổng (port-based) được định nghĩa bởi IEEE. Hoạt động trên cả môi trường có dây truyền thống và không dây. Việc điều khiển truy cập được thực hiện bằng cách:

Khi một người dùng cố gắng kết nối vào hệ thống mạng, kết nối của người dùng sẽ được đặt ở trạng thái bị chặn(blocking) và chờ cho việc kiểm tra định danh người dùng hoàn tất.



EAP là phương thức xác thực bao gồm yêu cầu định danh người dùng(password, certificate,...), giao thức được sử dụng(MD5, TLS_Transport Layer Security, OTP_ One Time Password,...) hỗ trợ tự động sinh khóa và xác thực lẫn nhau.

Mô hình xác thực 802.1X-EAP cho Client diễn ra như sau:



3.7. WPA (Wi-Fi Protected Access)

WEP được xây dựng để bảo vệ một mạng không dây tránh bị nghe trộm. Nhưng nhanh chóng sau đó người ta phát hiện ra nhiều lỗ hổng ở công nghệ này. Do đó, công nghệ mới có tên gọi WPA (Wi-Fi Protected Access) ra đời, khắc phục được nhiều nhược điểm của WEP.

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. WPA có sẵn 2 lựa chọn: WPA Personal và WPA Enterprise. Cả 2 lựa chọn 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

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 (đừng sử dụng những từ như "PASSWORD" để làm mật khẩu).

Điều này cũng có nghĩa rằng kỹ thuật TKIP của WPA chỉ là giải pháp tạm thời, chưa cung cấp một phương thức bảo mật cao nhất. WPA chỉ thích hợp với những công ty mà không truyền dữ liệu "mật" về những thương mại, hay các thông tin nhạy cảm... WPA cũng thích hợp với những hoạt động hàng ngày và mang tính thử nghiệm công nghệ.

3.8. WPA 2

Một giải pháp về lâu dài là sử dụng 802.11i tương đương với WPA2, được chứng nhận bởi Wi-Fi Alliance. Chuẩn này sử dụng thuật toán mã hoá mạnh mẽ và được gọi là Chuẩn mã hoá nâng cao AES (Advanced Encryption Standard). AES sử dụng thuật toán mã hoá đối xứng theo khối Rijndael, sử dụng khối mã hoá 128 bit, và 192 bit hoặc 256 bit. Để đánh giá chuẩn mã hoá này, Viện nghiên cứu quốc gia về Chuẩn và Công nghệ của Mỹ, NIST

(National Institute of Standards and Technology), đã thông qua thuật toán mã đối xứng này.

Quote:

Và chuẩn mã hoá này được sử dụng cho các cơ quan chính phủ Mỹ để bảo vệ các thông tin nhạy cảm.

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

Bài tập và sản phẩm thực hành bài 39.4

Kiến thức:

Câu 1: Nêu các hình thức tấn công trên mạng WLAN

Câu 2: Trình bày các hình thức bảo mật mạng WLAN

Kỹ năng bài tập 4:

Cài đặt và cấu hình Router ADSL Wireless Cisco

CẤU HÌNH ROUTER CISCO



1. Cấu hình kết nối ADSL

Lưu ý: Trước khi truy cập vào trang web cấu hình thiết bị, phải chắc chắn điện nguồn đã được bật và máy tính nối với một trong những cổng Ethernet phía sau thiết bị. Cổng DSL phía sau thiết bị được nối với splitter.



Bước 1:

Mở trình duyệt web **Internet Explorer**. Trên thanh Address gõ địa chỉ IP mặc định **192.168.1.1** sau đó nhấn Enter.



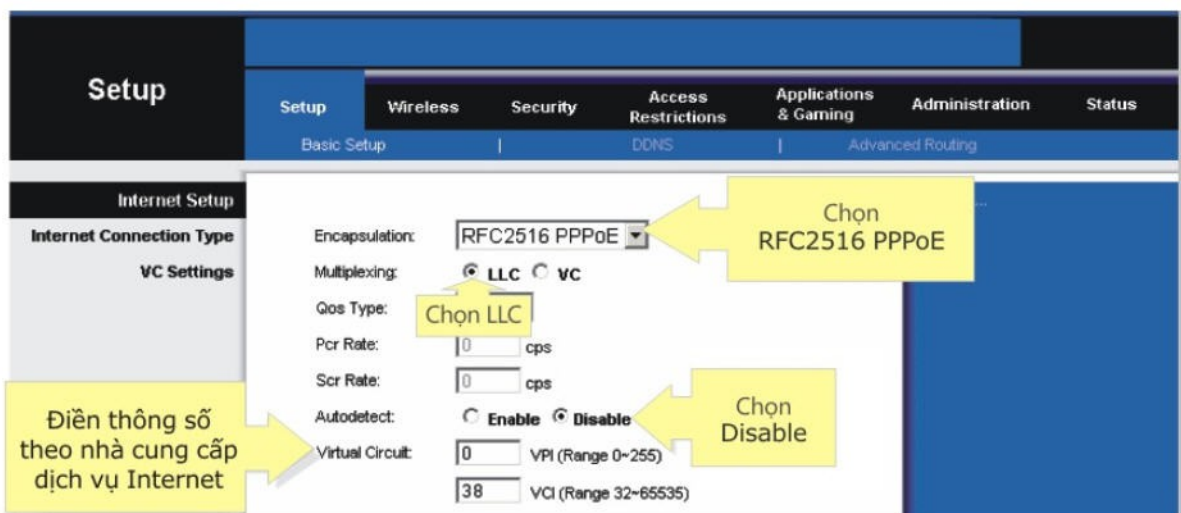
Bước 2:

Điền Username = admin và Password = admin vào cửa sổ đăng nhập, sau đó click OK.



Bước 3:

Khi trang web cấu hình thiết bị Router ADSL xuất hiện, tìm mục Encapsulation và chọn RFC2516 PPPoE ở menu thả xuống. Tìm mục VC Settings và chọn thông số Multiplexing phù hợp.



Encapsulation:	RFC2516 PPPoE	Encapsulation:	RFC2516 PPPoE
Multiplexing:	<input checked="" type="radio"/> LLC <input type="radio"/> VC	Multiplexing:	<input checked="" type="radio"/> LLC <input type="radio"/> VC
Qos Type:	UBR	Qos Type:	UBR
Pcr Rate:	0 cps	Pcr Rate:	0 cps
Scr Rate:	0 cps	Scr Rate:	0 cps
Autodetect:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Autodetect:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Virtual Circuit:	8 VPI (Range 0~255) 35 VCI (Range 32~65535)	Virtual Circuit:	0 VPI (Range 0~255) 33 VCI (Range 32~65535)

VNN & Viettel FPT

PPPoE Settings	User Name:	<input type="text"/>	Nhập Username và Password đăng ký với nhà cung cấp dịch vụ Internet
	Password:	<input type="text"/>	
	<input type="radio"/> Connect on Demand: Max Idle Time	5 Min.	
	<input checked="" type="radio"/> Keep Alive: Redial Period	30 Sec.	

Bước 4:

Click chuột chọn **Save Settings** để lưu thông tin cấu hình

Bước 5:

Chọn tab Status để kiểm tra hiện trạng kết nối

Status | Setup | Wireless | Security | Access Restrictions | Applications & Gaming | Administration | Status

Gateway Information

Firmware Version: **V1.00.09**
 MAC Address: **00:1D:7E:B7:34:86**
 Current Time: **28-11-2008 05:35:47**

Internet Connection

Login Type: **RFC 2516 PPPoE**
 Interface: **Up**
 IP Address: **222.254.154.45**
 Subnet Mask: **255.255.255.255**
 Default Gateway: **222.254.175.1**
 DNS 1: **203.162.4.190**
 DNS 2: **203.162.4.191**

Kết nối thành công

Chọn status

Nếu IP được cấp xuống như hình bên cạnh: Cấu hình thành công

Internet Connection

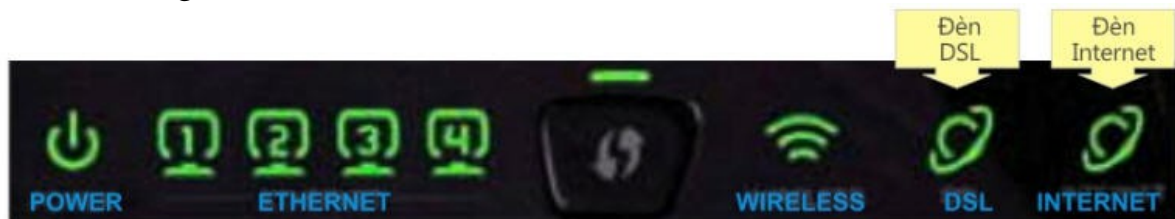
Login Type: **RFC 2516 PPPoE**
 Interface: **Down**
 IP Address: ---
 Subnet Mask: ---
 Default Gateway: ---
 DNS 1: ---
 DNS 2: ---
 DNS 3: ---
 WINS: ---

Chưa kết nối thành công

Disconnect Connect

Nếu IP chưa được cấp xuống như hình bên cạnh: Nhấn Connect

Nếu vẫn không nhận được IP, kiểm tra lại đèn LED trên thiết bị. Có 2 đèn hiển thị trạng thái kết nối như hình dưới.

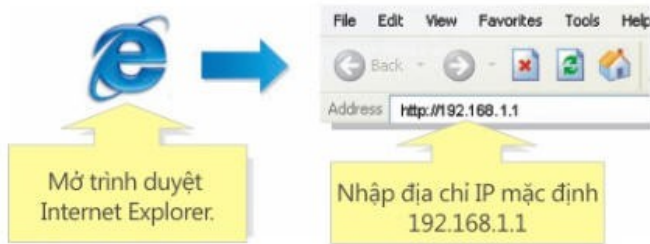


Đèn DSL phải đứng không chớp tắt. Nếu đèn này nhấp nháy liên tục không dừng. Hãy gọi đến nhà cung cấp dịch vụ Internet để yêu cầu kiểm tra lại tín hiệu. Đèn Internet phải sáng xanh. Nếu hiển thị màu đỏ hãy kiểm tra lại Username và Password đã nhập.

2.Cấu hình mạng không dây (Wireless).

Bước 1:

Truy nhập vào trang web cấu hình thiết bị bằng địa chỉ IP **192.168.1.1** khi trang web cấu hình thiết bị router xuất hiện, click vào **Wireless**.

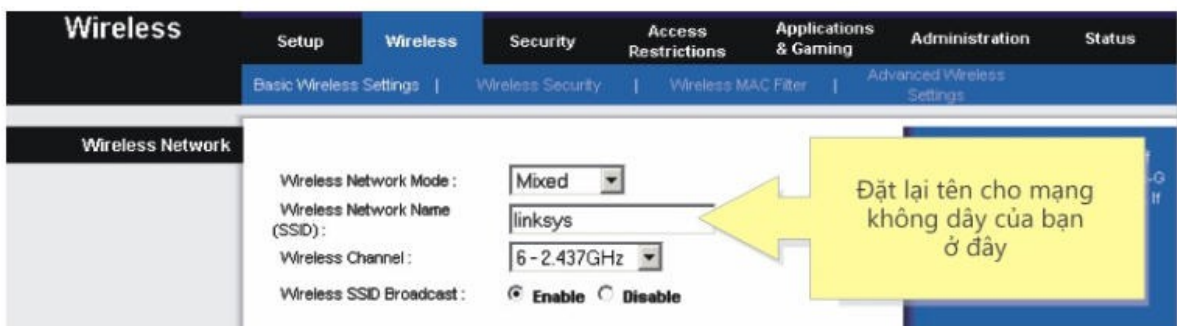


Tại mục **Wireless > Basic Wireless Settings**, chọn nút **Manual** để cấu hình wireless.



Bước 2:

Tìm mục **Wireless Network Name (SSID)** và đổi nó thành tên bạn muốn dùng cho mạng không dây của mình.



Bước 3:

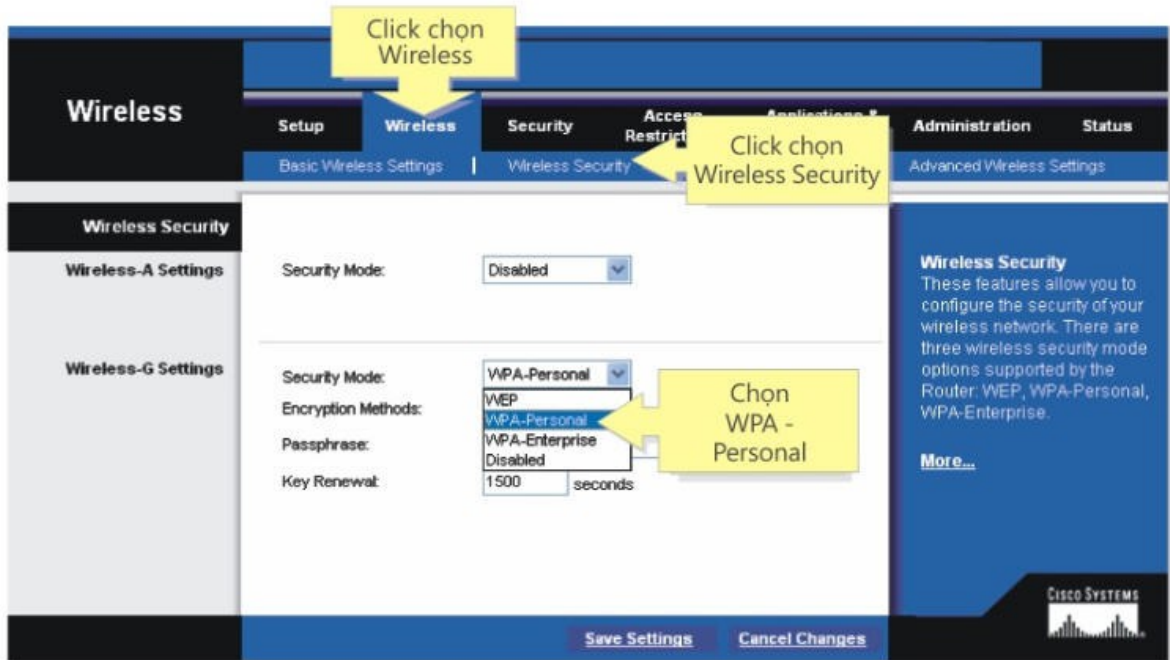
Click chuột vào nút **Save Settings** để cấu hình đã thiết lập.

Bước 4:

Khi trang web cấu hình thiết bị router xuất hiện, click chuột vào **Wireless** sau đó click chuột vào **Wireless Security**

Bước 5:

Tìm mục **Security Mode** và chọn **WPA-Personal** ở menu thả xuống.



Bước 6:

Tìm mục **Encryption Methods** và chọn **TKIP**

Bước 7:

Tìm mục **Passharase** và gõ password bạn muốn (ít nhất 8 ký tự). Password này sẽ được dùng khi nào bạn kết nối vào mạng không dây của mình.

Lưu ý: không nên đưa password cho bất kỳ ai. Password này sẽ giúp bảo mật mạng không dây của bạn.



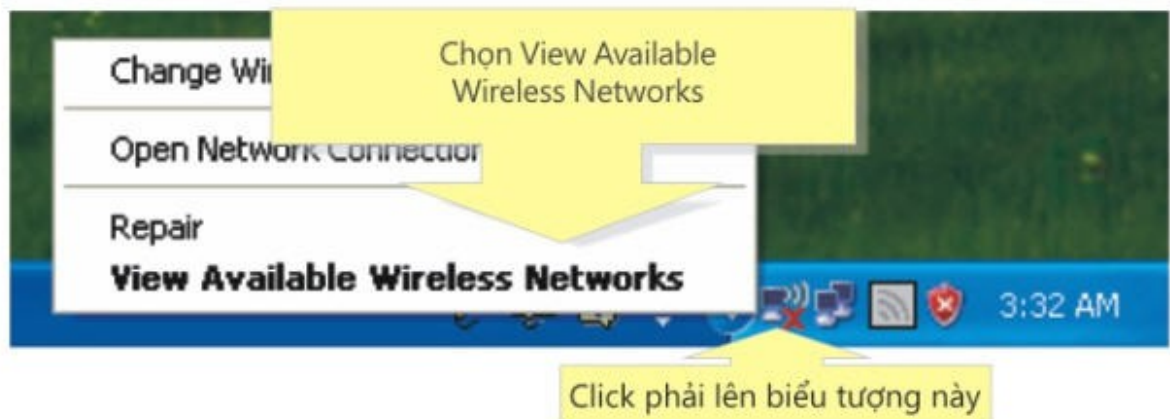
Bước 8:

Click chuột vào nút **Save Settings** để lưu thay đổi cấu hình

3. Kết nối Laptop vào mạng không dây

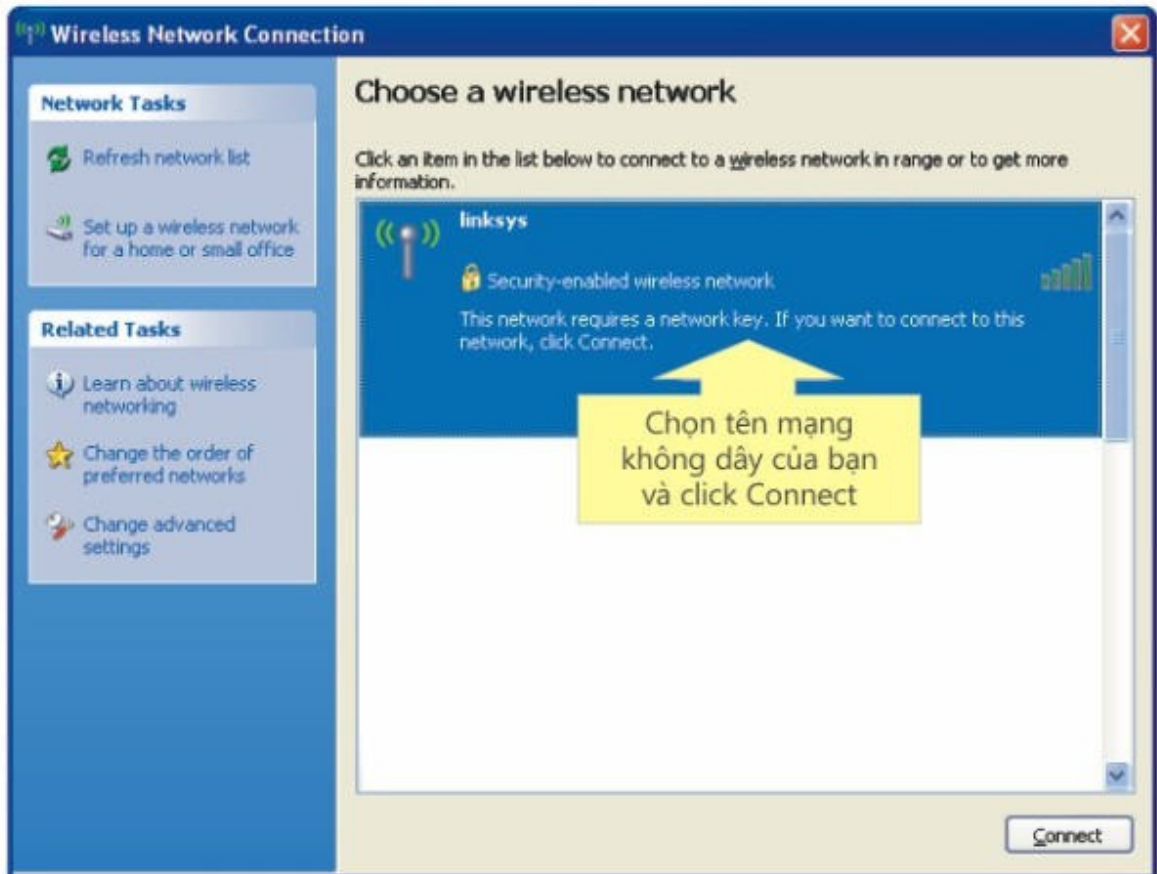
Bước 1:

Click phải chuột lên biểu tượng **Wireless Network Connection** ở góc phải – bên dưới màn hình và chọn **View Available Wireless Networks**.

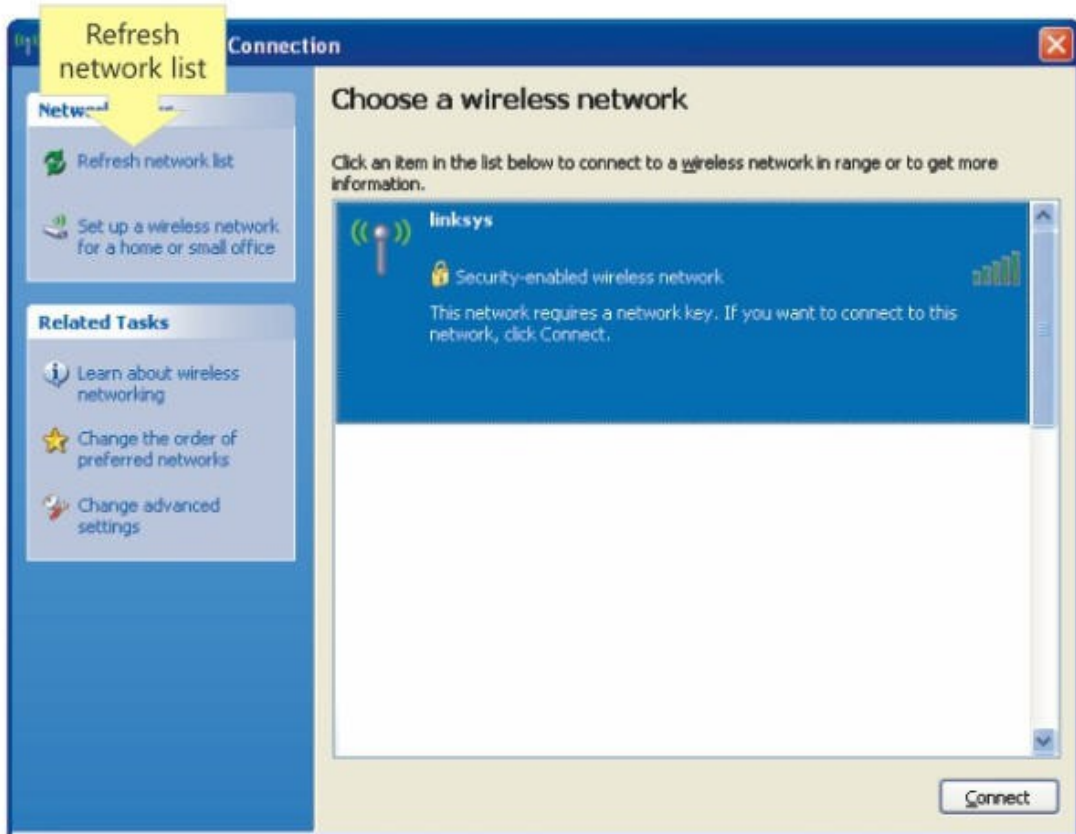


Bước 2:

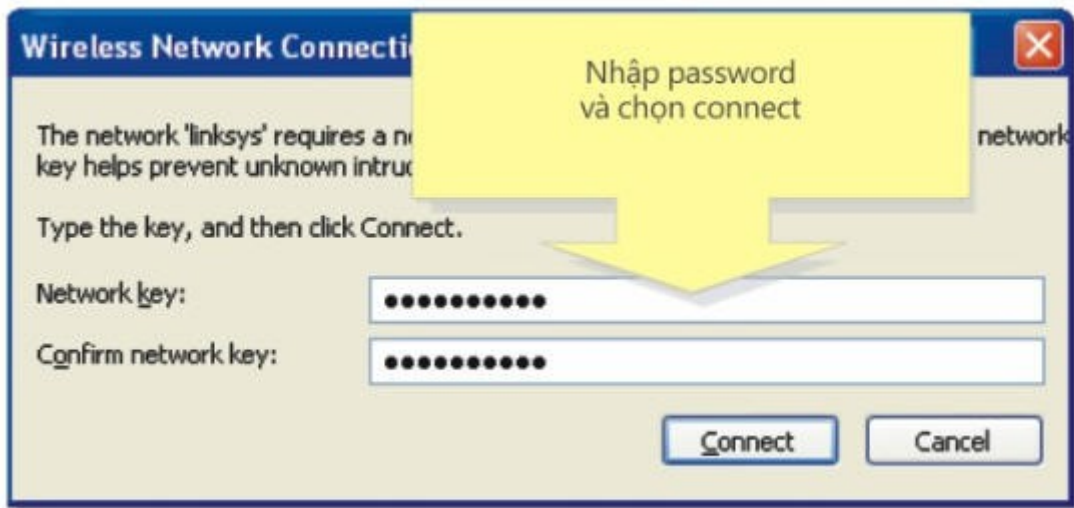
Chọn tên mạng không dây của bạn và click **Connect**



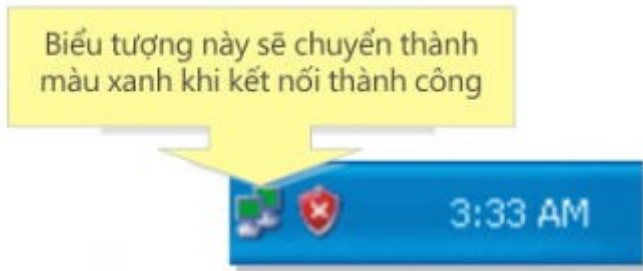
Nếu máy tính không phát hiện được bất kỳ mạng không dây nào, click **Refresh network list**



Nếu chế độ bảo mật WPA được bật trên thiết bị Wireless router, một cửa sổ sẽ hiện ra yêu cầu nhập password để vào mạng.



Lưu ý: Biểu tượng **Wireless Network Connection** tại góc phải – bên dưới màn hình sẽ chuyển sang màu xanh nếu máy tính kết nối được với mạng không dây.



Bài tập 5

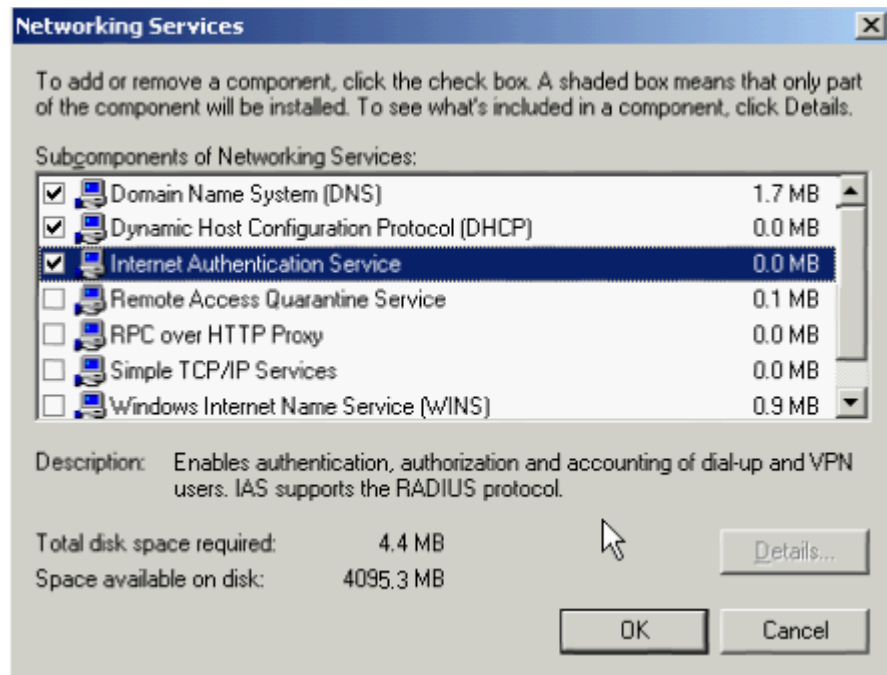
CHỨNG THỰC NGƯỜI DÙNG THÔNG QUA RADIUS SERVER

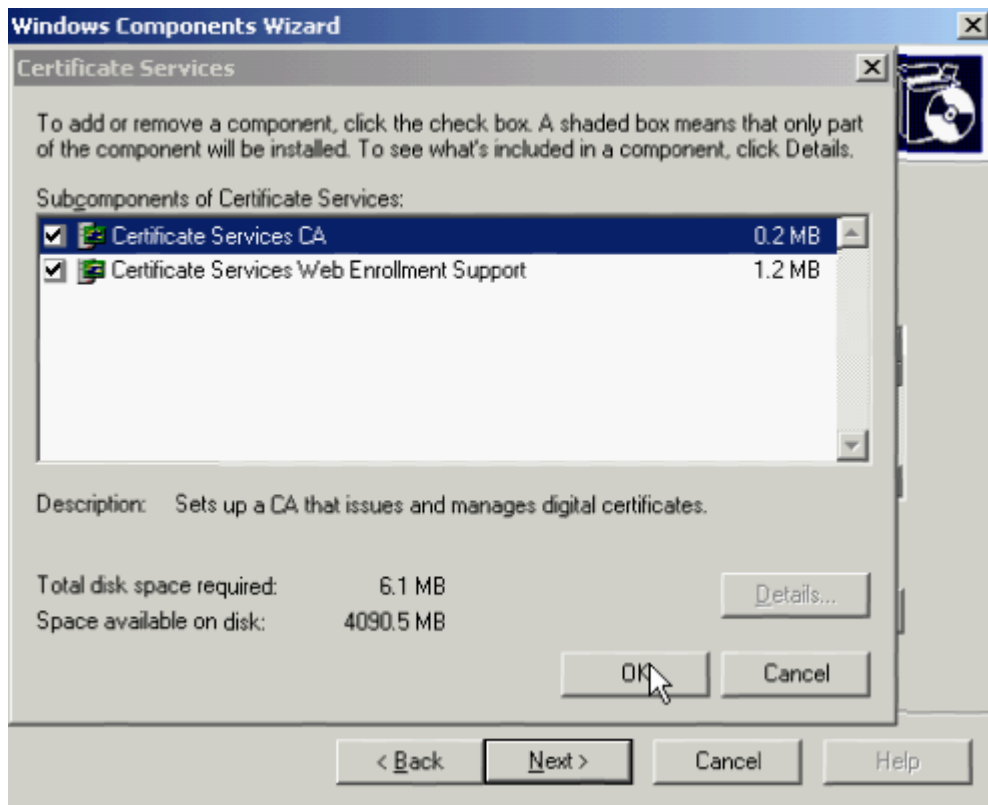
Qui trình cài đặt:

1. Cài đặt DHCP, Enterprise CA và Radius:

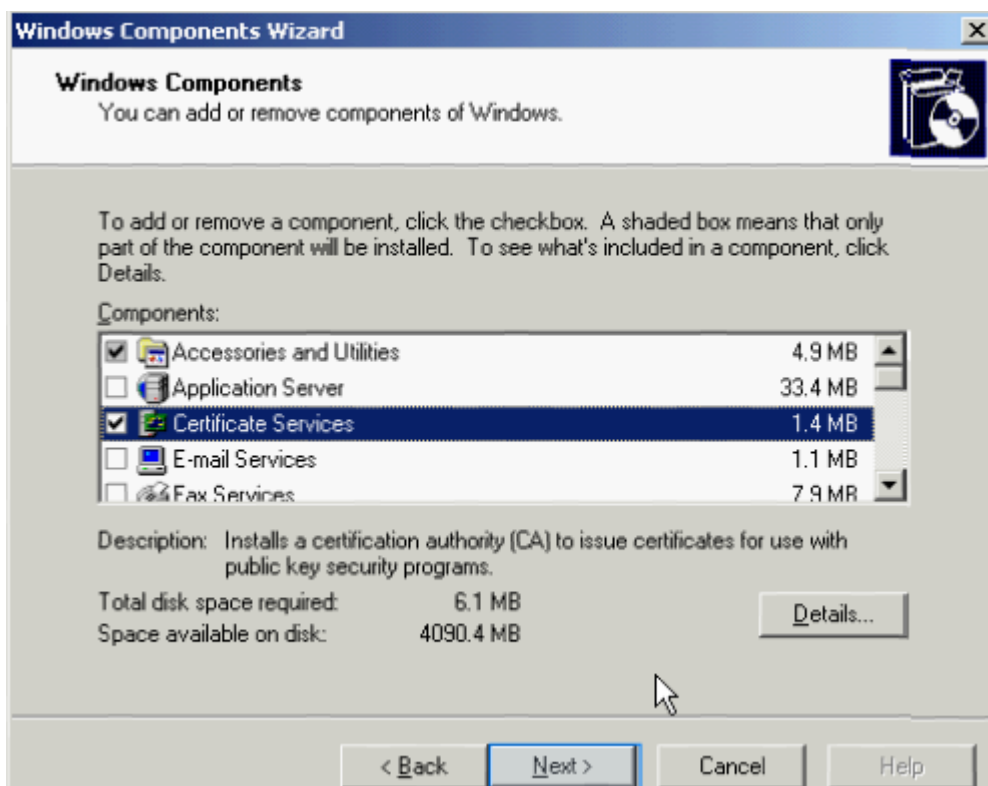
Vào Start → Control Panel → Add or Remove Program → Chọn Add/Remove Windows Components.

Cửa sổ các dịch vụ hiện ra ta tiến hành tích chọn các dịch vụ DNS, DHCP, Internet Authentication Service như hình bên dưới

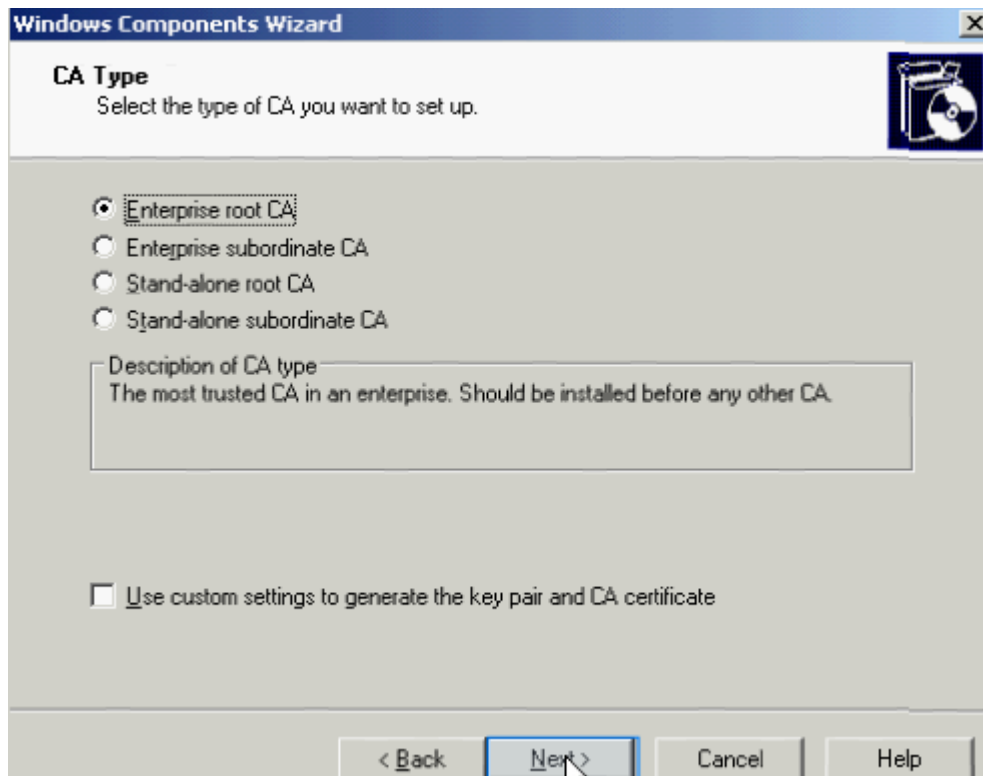




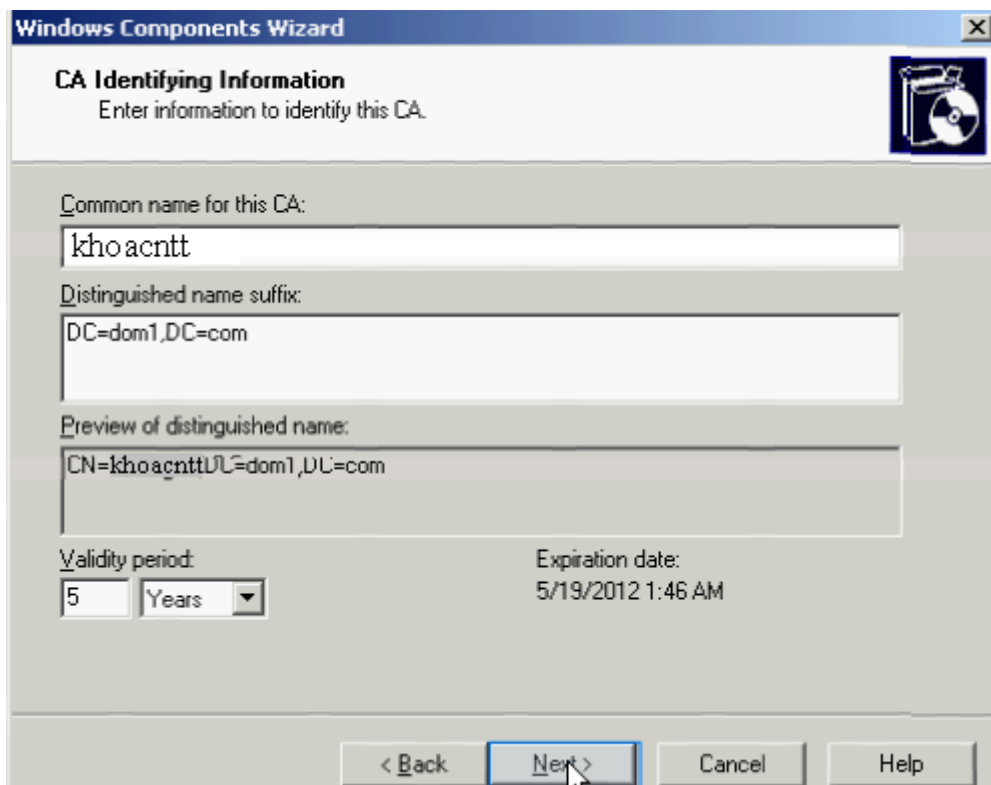
Kích chuột vào nút Next để tiếp tục cài CA

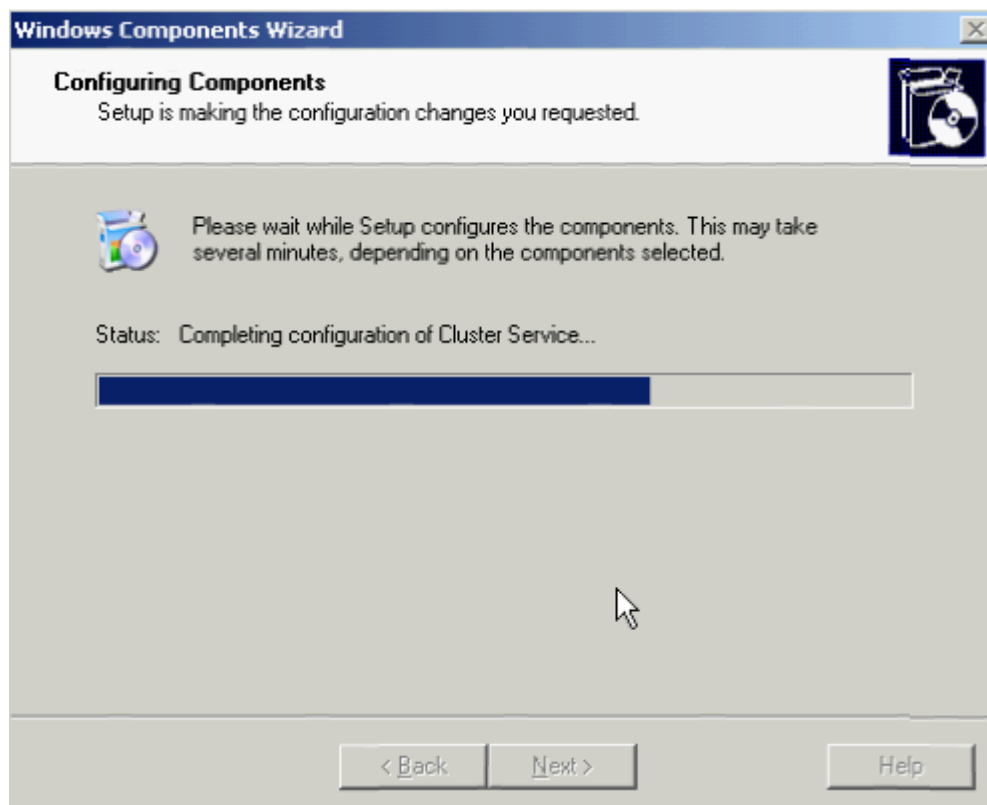
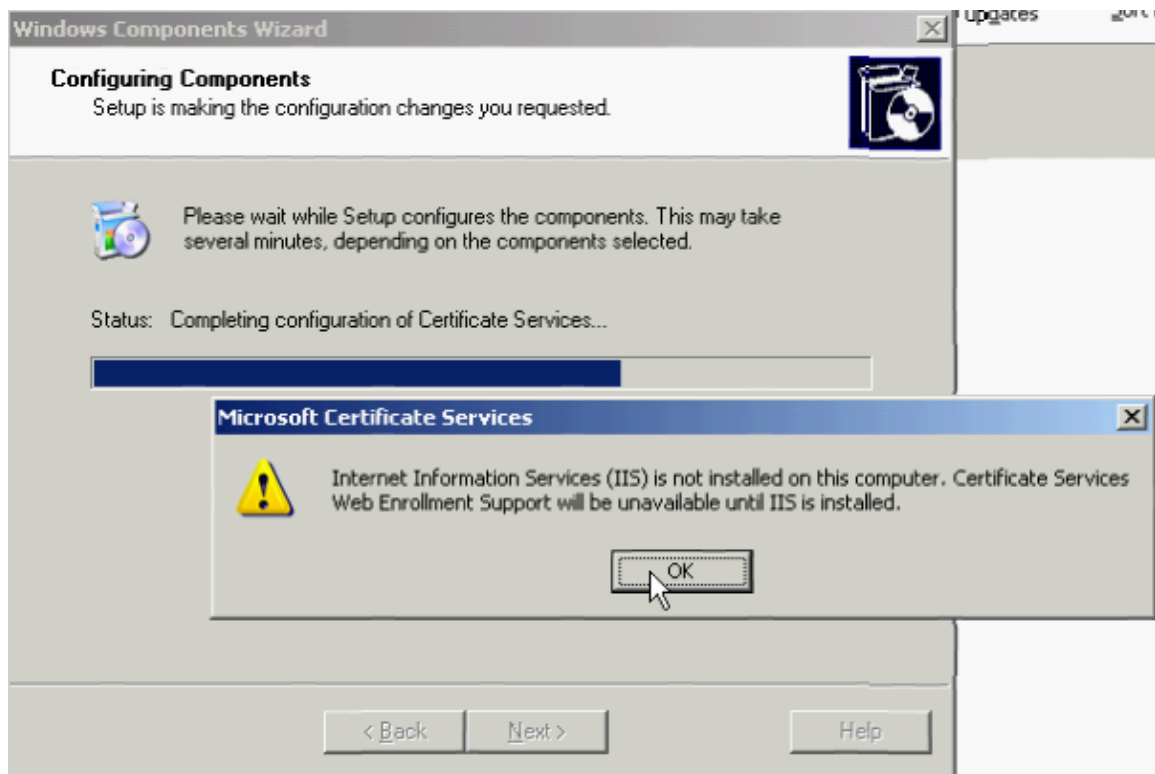


Tiếp tục kích chuột vào nút Next



Điền tên CA = khoa cntt, và kích chuột vào nút Next để hoàn tất quá trình cài đặt



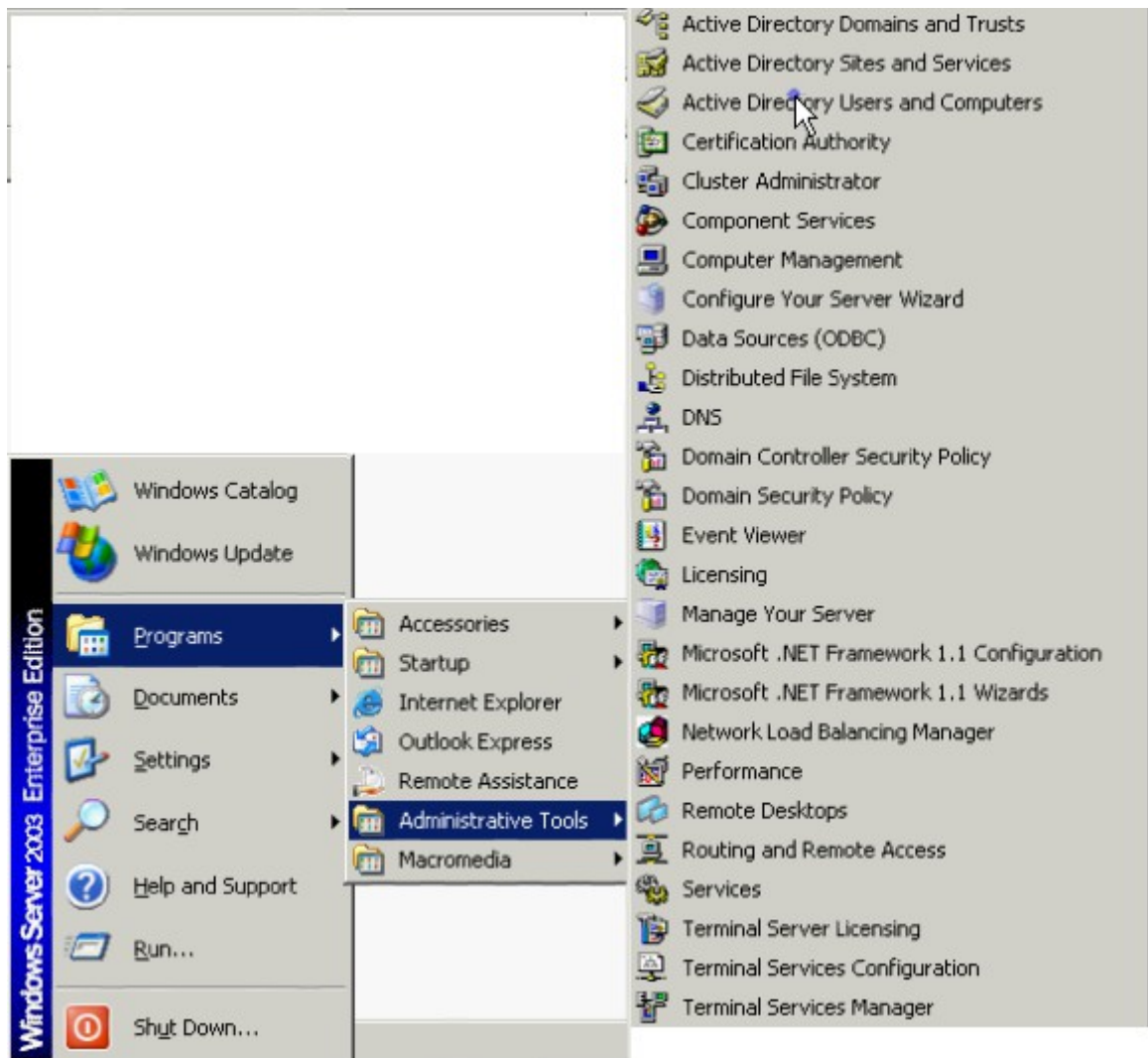


Kích chuột vào nút Finish để kết thúc

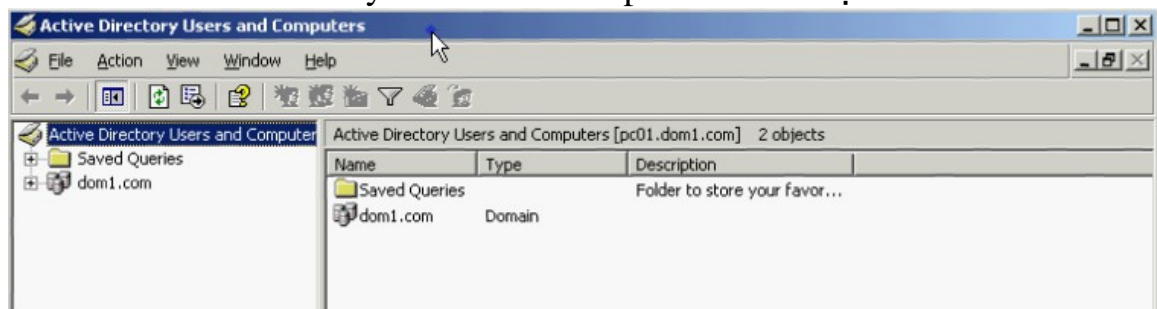


2. Chuyển Server sang Native Mode

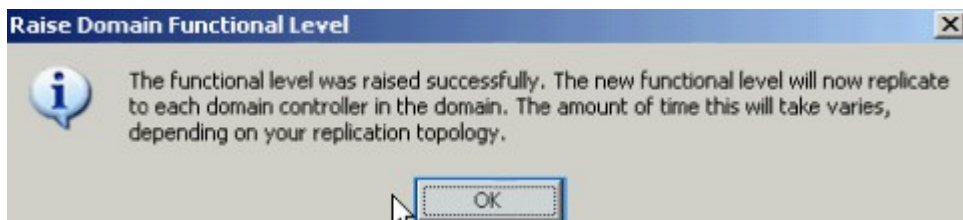
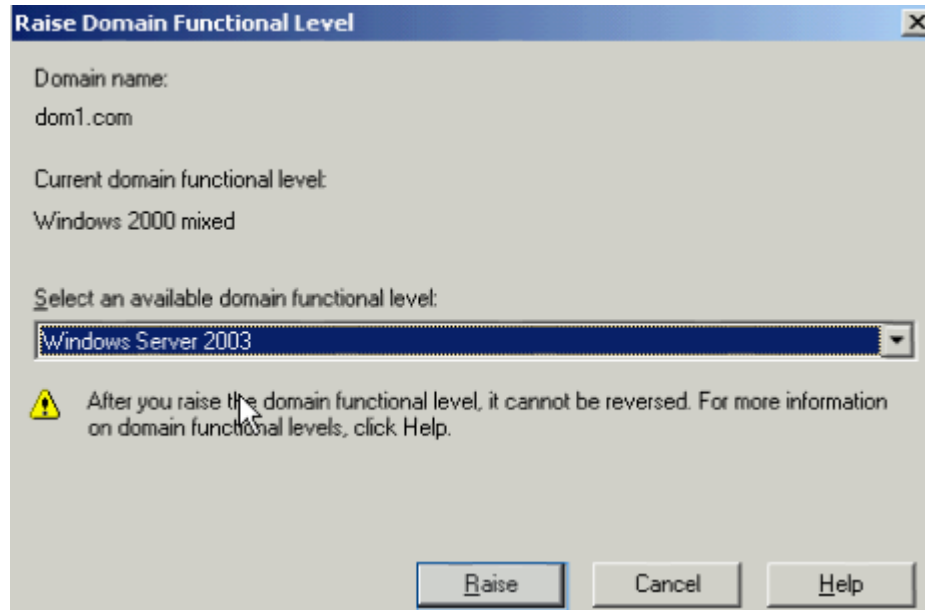
Kích chuột vào nút Start → Program → Administrative Tools → Active Directory Users and Computers



Màn hình Active Directory Users and Computers xuất hiện

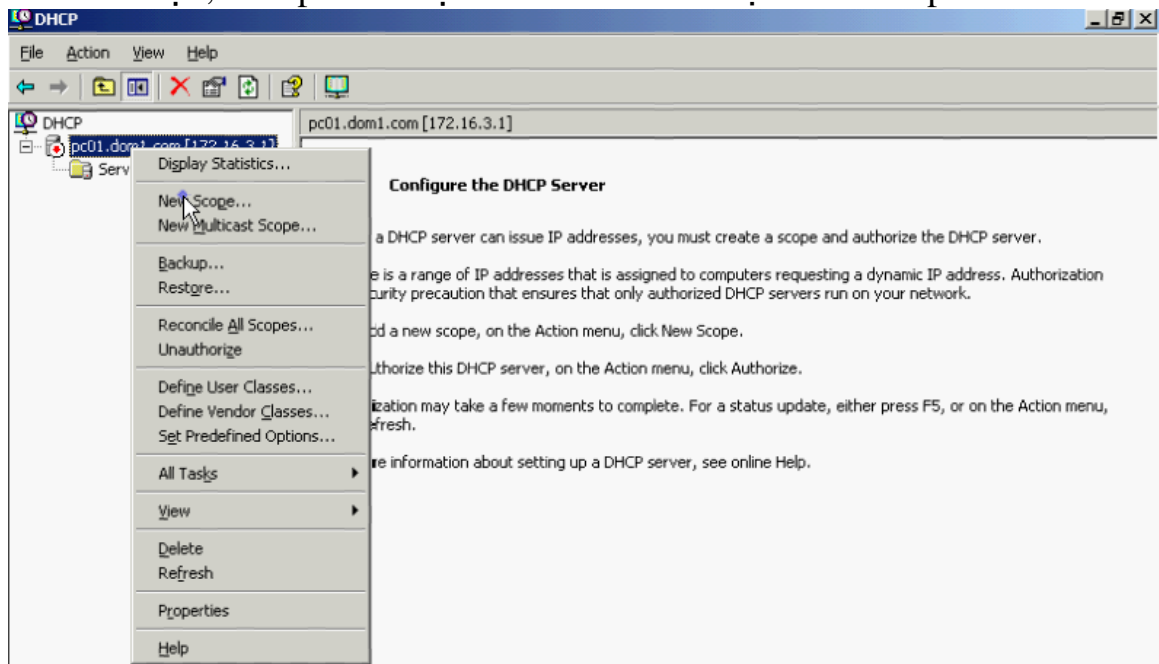


Kích phải chuột lên domain dom1.com → chọn Raise Domain Funtional Level → hộp thoại xuất hiện tít chọn Windows Server 2003 → kích nút Raise để thực hiện



3. Cấu hình DHCP

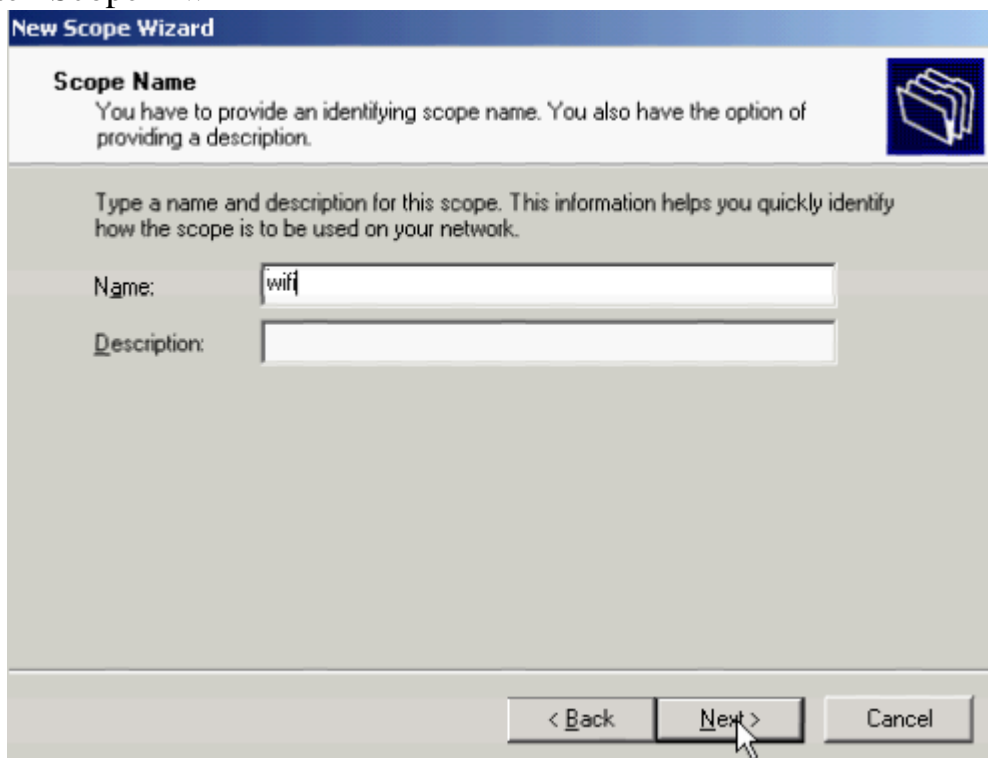
Kích chuột vào nút Start → Program → Administrative Tools → DHCP màn hình xuất hiện, kích phải chuột vào domain → chọn New Scope



Hộp thoại xuất hiện → chọn Next để tiếp tục



Nhập tên Scope = wifi



Nhập dãy IP để cung cấp DHCP vào, kích chuột vào nút Next để tiếp tục

New Scope Wizard

IP Address Range
You define the scope address range by identifying a set of consecutive IP addresses.

Enter the range of addresses that the scope distributes.

Start IP address: 172 . 16 . 3 . 10

End IP address: 172 . 16 . 3 . 100

A subnet mask defines how many bits of an IP address to use for the network/subnet IDs and how many bits to use for the host ID. You can specify the subnet mask by length or as an IP address.

Length: 16

Subnet mask: 255 . 255 . 255 . 0

< Back Next > Cancel

Add Default Gateway = 172.16.3.1 vào

New Scope Wizard

Router (Default Gateway)
You can specify the routers, or default gateways, to be distributed by this scope.

To add an IP address for a router used by clients, enter the address below.

IP address: 172 . 16 . 3 . 1

Add

Click the Add button

Down

< Back Next > Cancel

Nhập các thông số Parent domain = dom1.com, IP address = 172.16.3.1 và kích chuột vào nút Add → Kích chuột vào nút Next.

New Scope Wizard

Domain Name and DNS Servers
The Domain Name System (DNS) maps and translates domain names used by clients on your network.

You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

Parent domain:

To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.

Server name:	IP address:	
<input type="text"/>	<input type="text" value="172 . 16 . 3 . 1"/>	<input type="button" value="Add"/>
<input type="button" value="Resolve"/>	<input type="text"/>	<input type="button" value="Remove"/>
		<input type="button" value="Up"/>
		<input type="button" value="Down"/>

Hộp thoại xuất hiện, kích chuột vào nút Next và Finish để kết thúc

New Scope Wizard

Activate Scope
Clients can obtain address leases only if a scope is activated.

Do you want to activate this scope now?

Yes, I want to activate this scope now

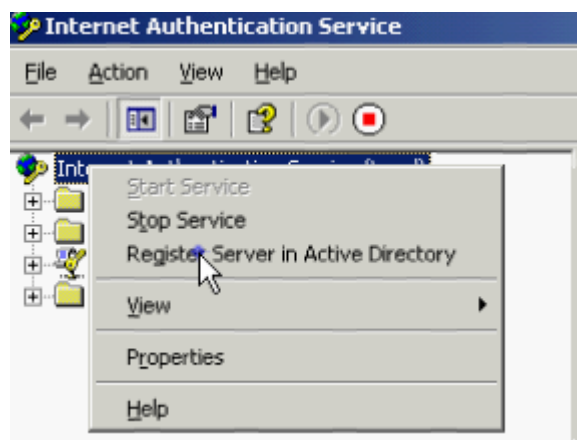
No, I will activate this scope later

4.Cấu hình Radius:

Kích chuột vào nút Start → Program → Administrative Tools → Internet Authentication Service



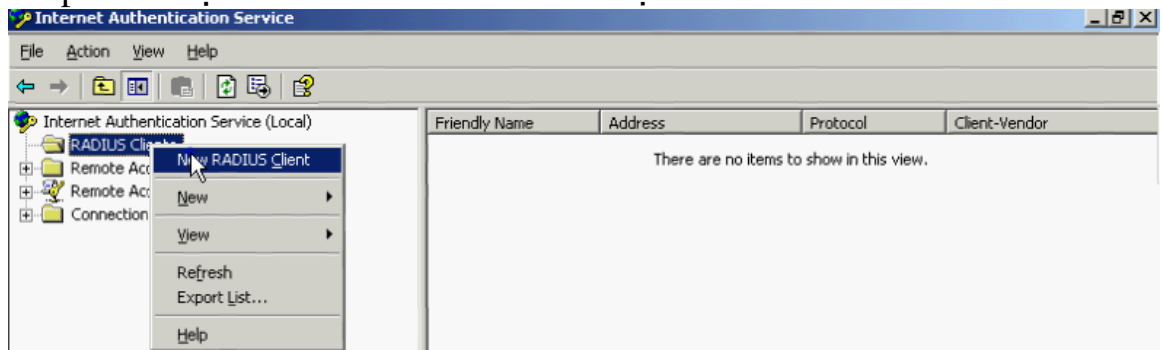
Kích phải chuột lên Internet Authentication Service → chọn Register Server In Active Directory



Hộp thoại xuất hiện → kích vào nút OK



Kích phải chuột vào RADIUS Client → chọn New RADIUS Client



Hộp thoại xuất hiện: điền các thông số như hình → kích chuột vào nút Next để tiếp tục

New RADIUS Client

Name and Address

Type a friendly name and either an IP Address or DNS name for the client.

Friendly name:

Client address (IP or DNS):

< Back **Next >** Cancel

Hộp thoại xuất hiện → nhập mật khẩu xác thực Radius → tích chọn Request must contain the Message Authenticator attribute → kích vào nút Finish để kết thúc

New RADIUS Client

Additional Information

If you are using remote access policies based on the client vendor attribute, specify the vendor of the RADIUS client.

Client-Vendor:

Shared secret:

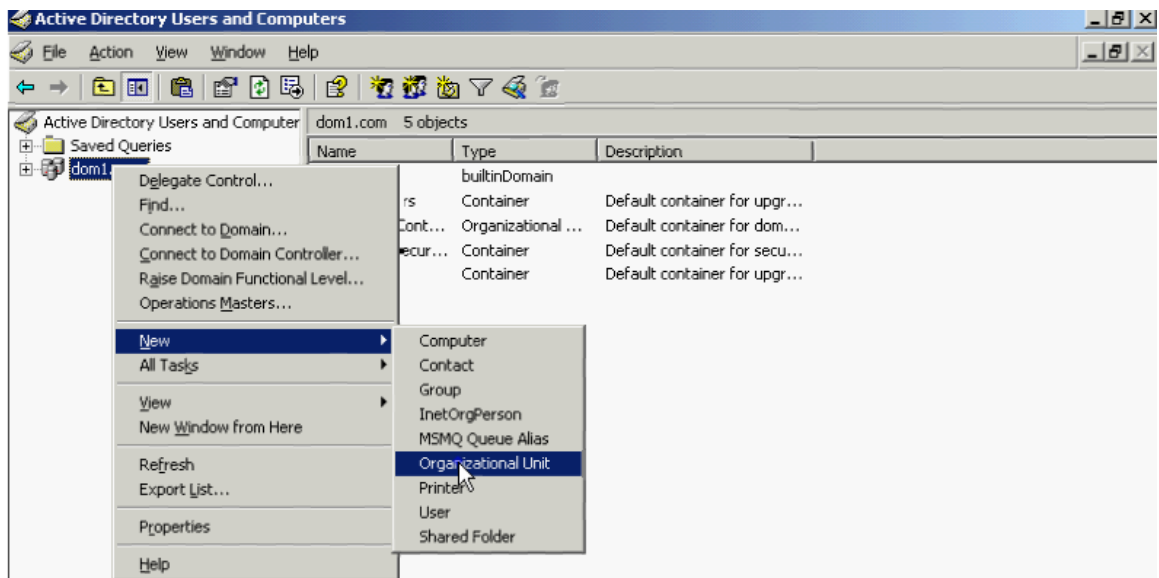
Confirm shared secret:

Request must contain the Message Authenticator attribute

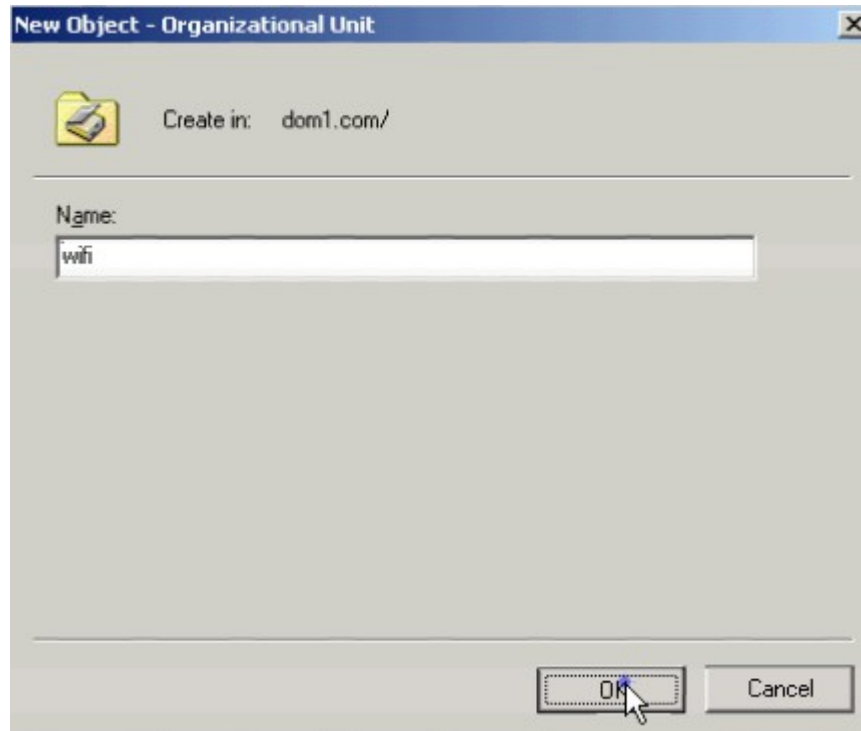
< Back **Finish** Cancel

5. Tạo User, cấp quyền Remote Access cho user và cho computer

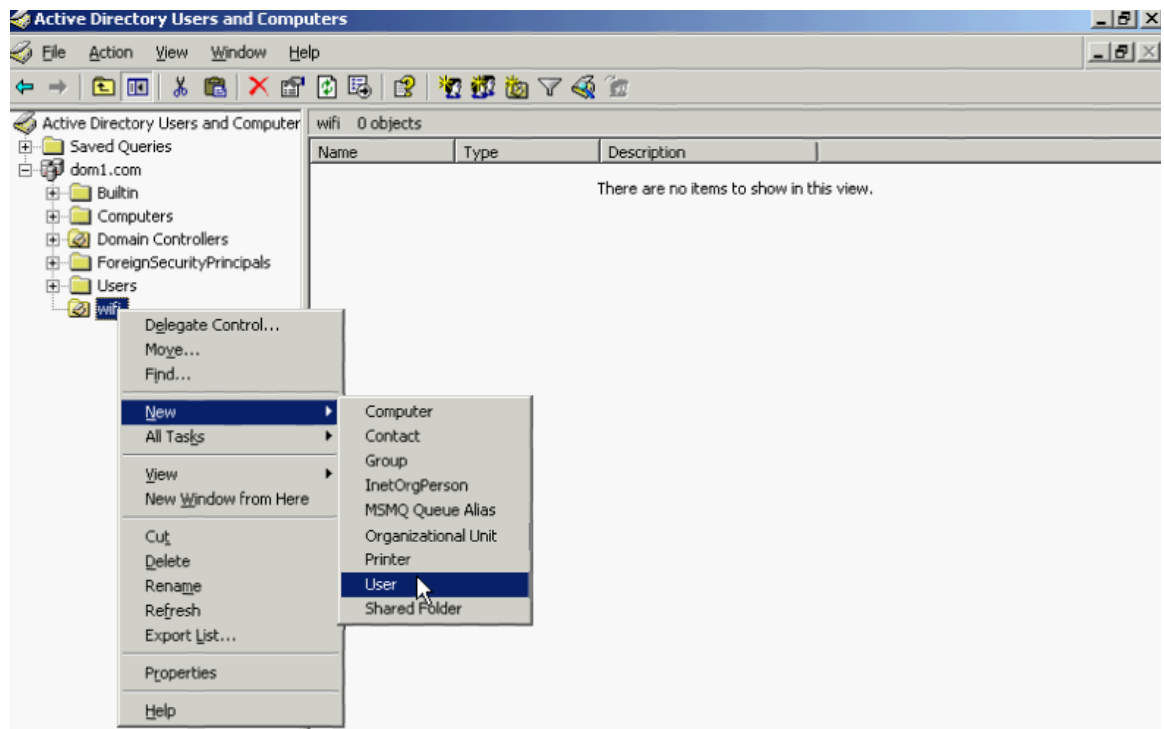
Kích chuột vào nút Start → Program → Administrative Tools → Active Directory Users and Computers → kích phải chuột chọn New → Organizational Unit



Tạo 1 OU mới: Name = wifi



Kích phải chuột vào OU wifi mới tạo → chọn New → User



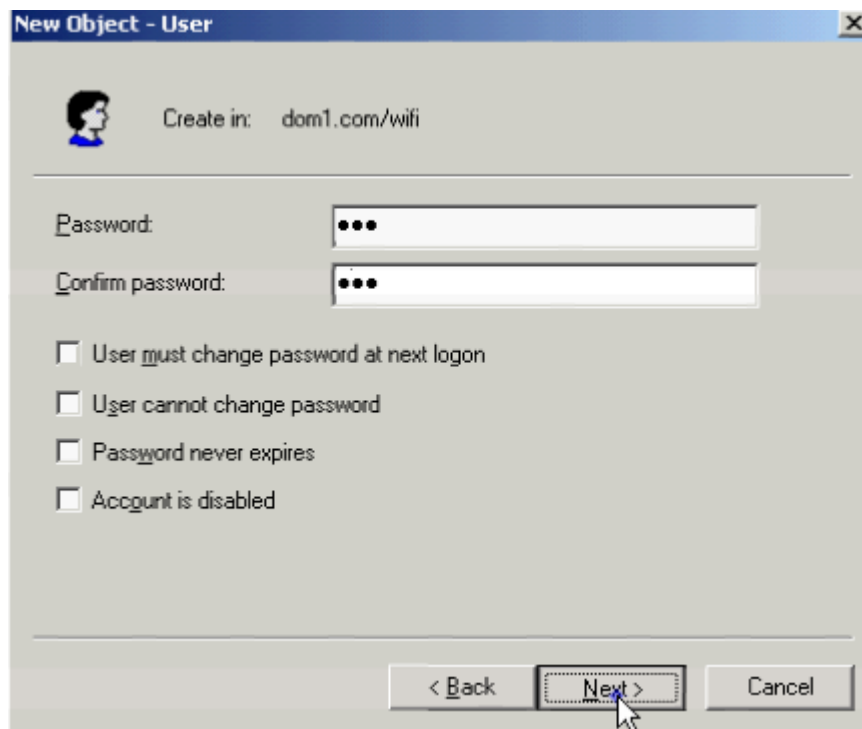
Nhập tên user mới như hình và nhấn nút Next

The 'New Object - User' dialog box is shown with the following fields:

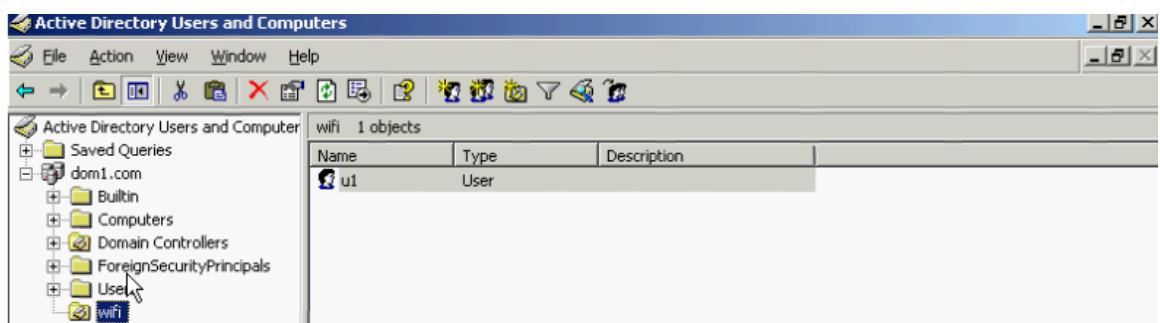
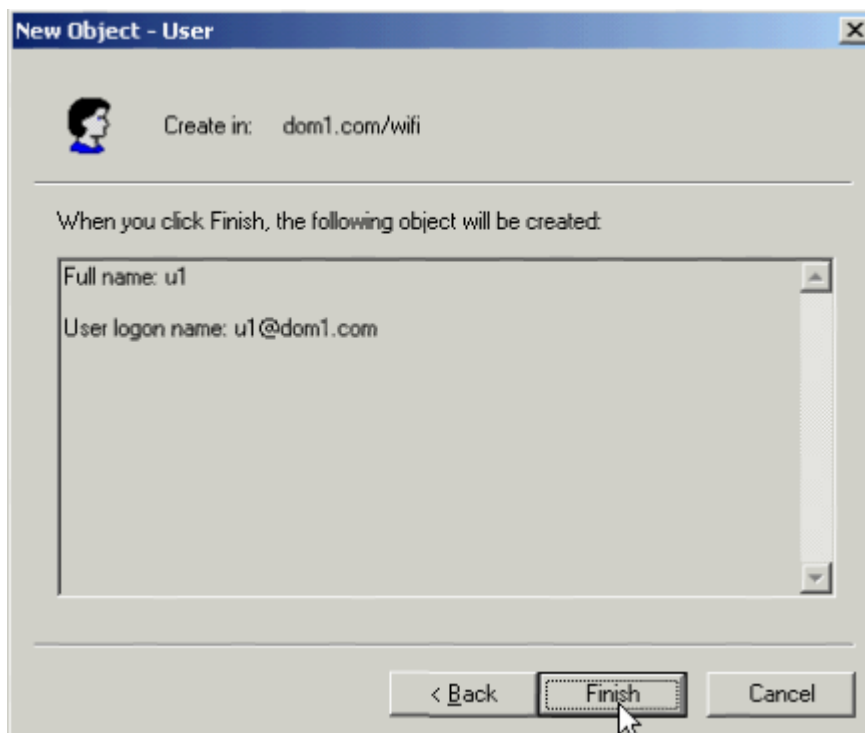
- Create in: dom1.com/wifi
- First name: u1
- Initials: (empty)
- Last name: (empty)
- Full name: u1
- User logon name: u1 @dom1.com
- User logon name (pre-Windows 2000): DOM1\ u1

Buttons at the bottom: < Back, Next >, Cancel

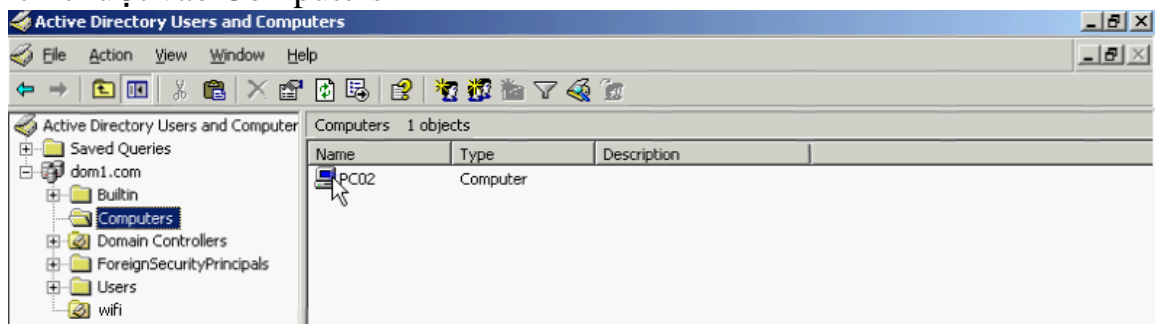
Thiết lập password cho user mới



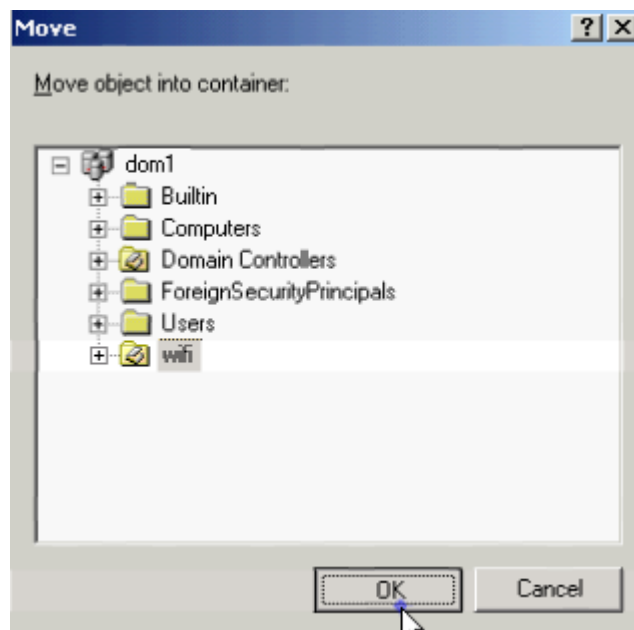
Nhấn nút Finish để kết thúc



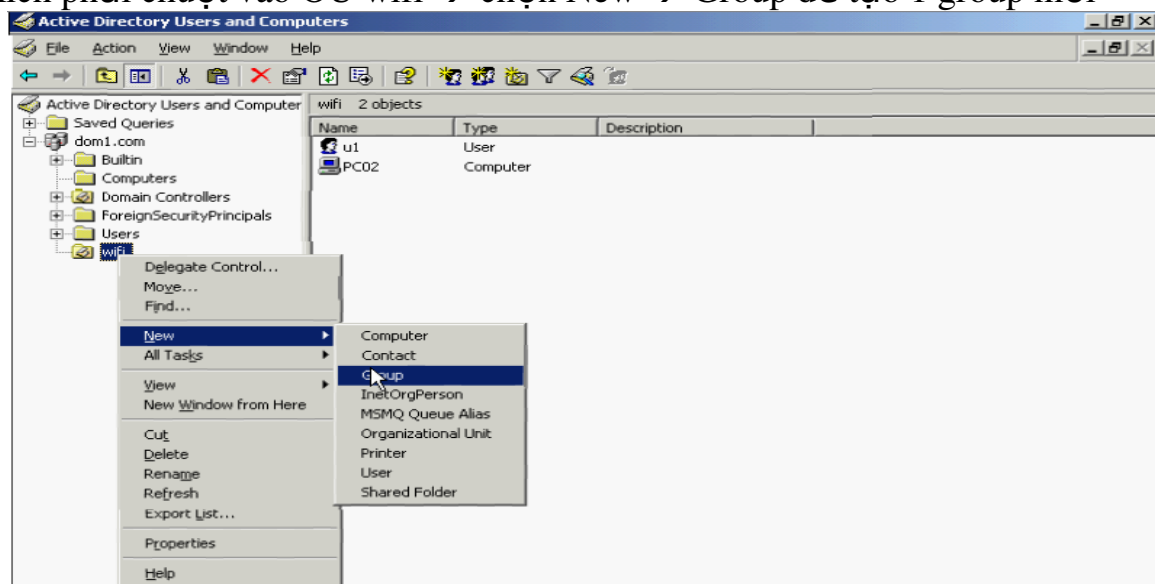
Kích chuột vào Computers



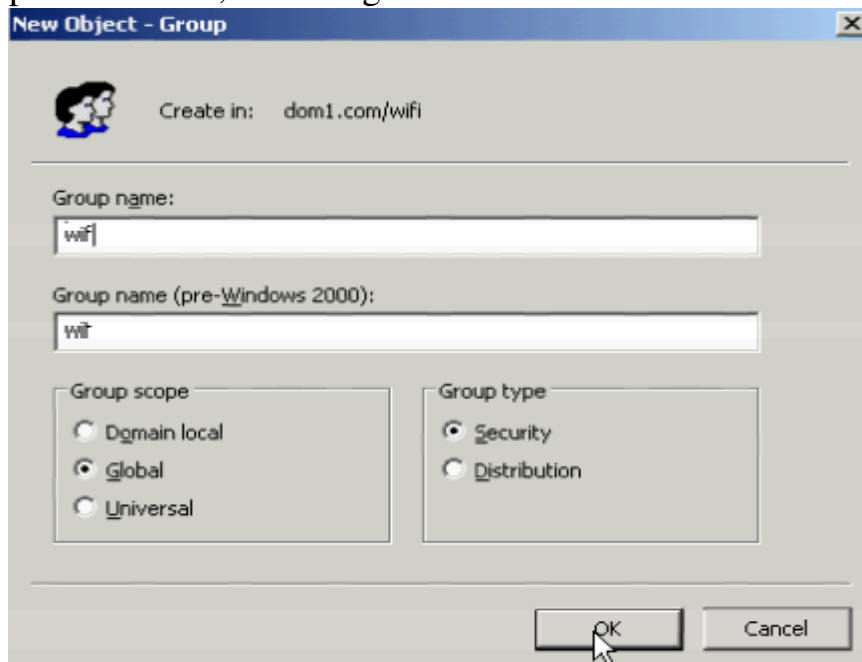
Kích phải chuột vào PC02 → chọn More → hộp thoại xuất hiện → kích chọn vào wifi → nhấn nút OK để kết thúc



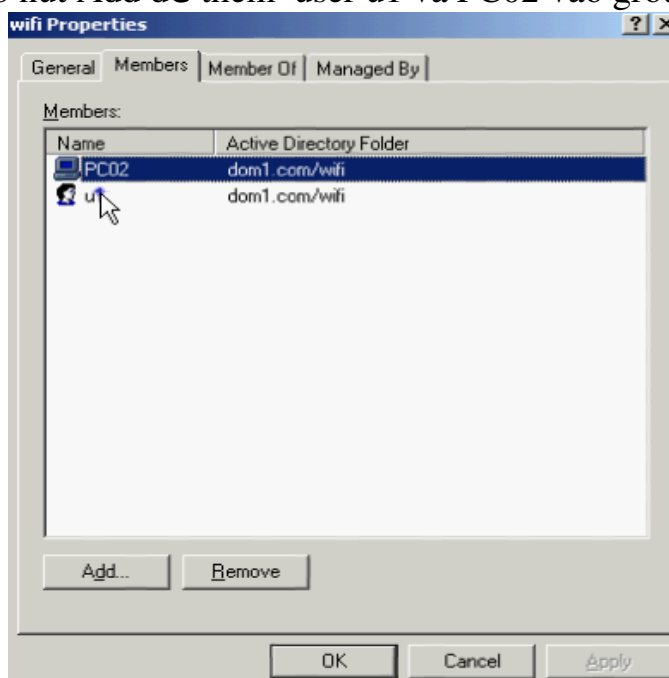
Kích phải chuột vào OU wifi → chọn New → Group để tạo 1 group mới



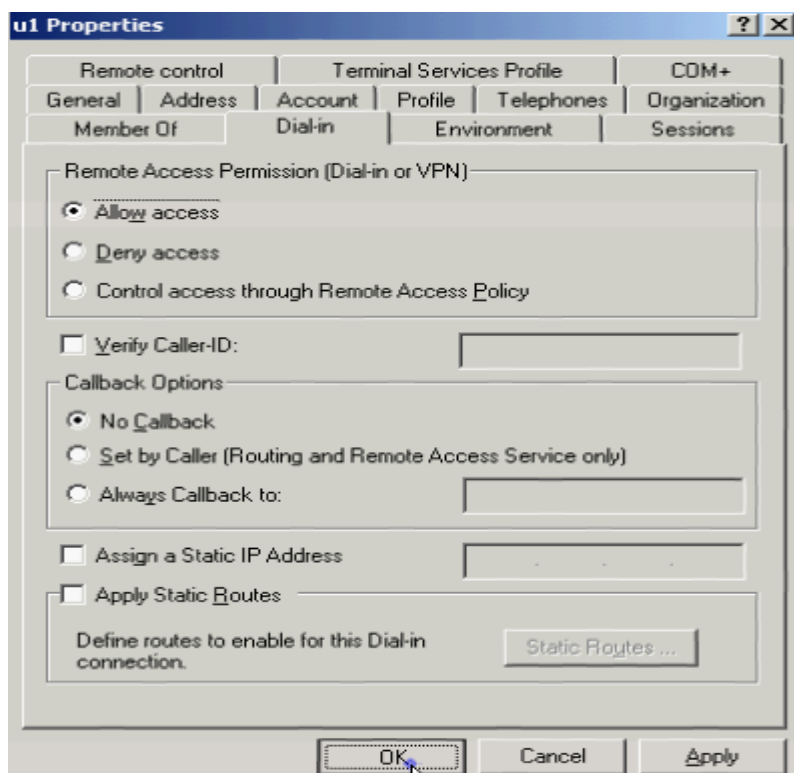
Nhập Group name = wifi, các thông số như hình



Kích phải chuột lên Group wifi → hộp thoại xuất hiện → chọn tab Members → kích chuột vào nút Add để thêm user u1 và PC02 vào group này

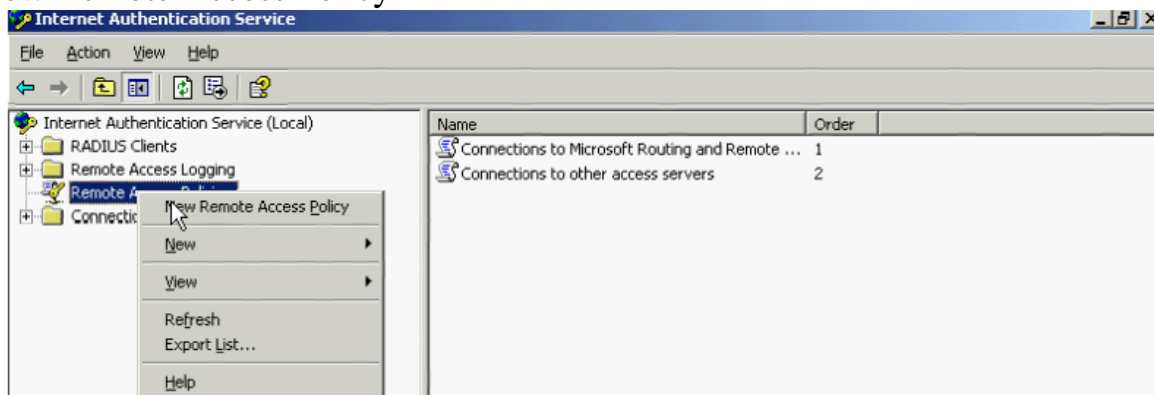


Kích phải chuột vào user = u1 và chọn Properties → chọn tab Dial-in → tích chọn Allow Access để cho phép user u1 có thể Remote Access vào domain. Và làm tương tự như vậy đối với PC02

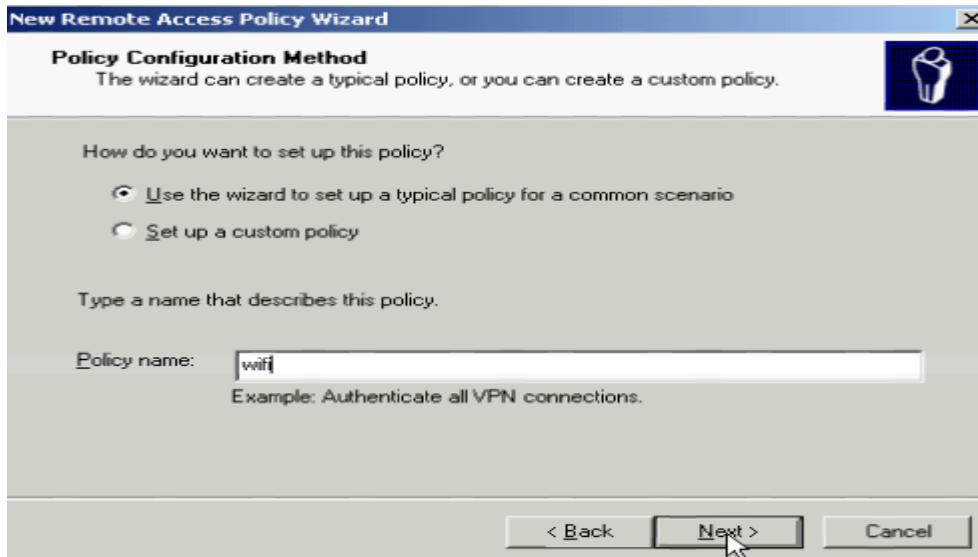


6. Tạo Remote Access Policy

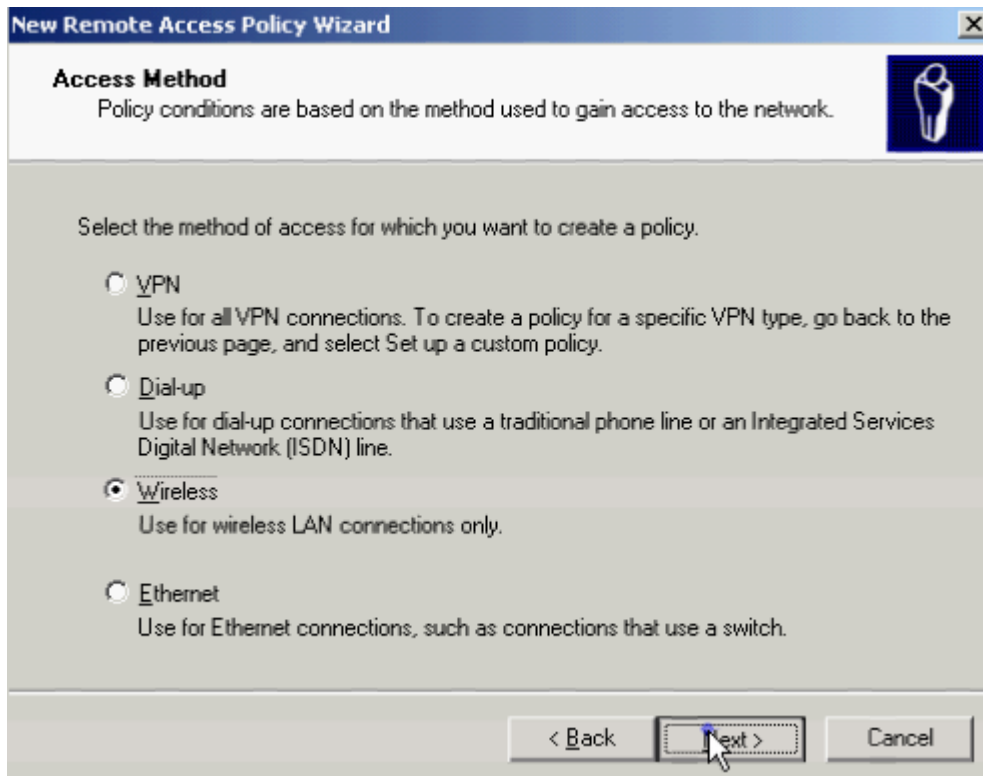
Kích chuột vào nút Start → Program → Administrative Tools → Internet Authentication Service → kích phải chuột vào Remote Access Policy → chọn New Remote Access Policy



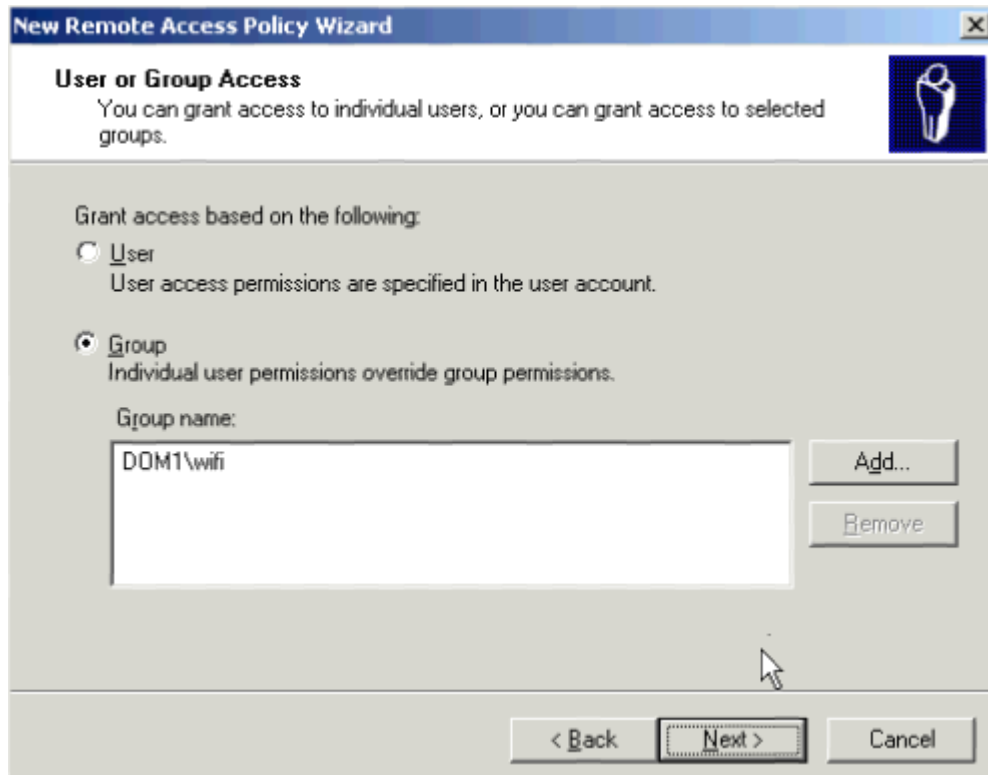
Hộp thoại xuất hiện → nhập tên policy = wifi → kích nút Next



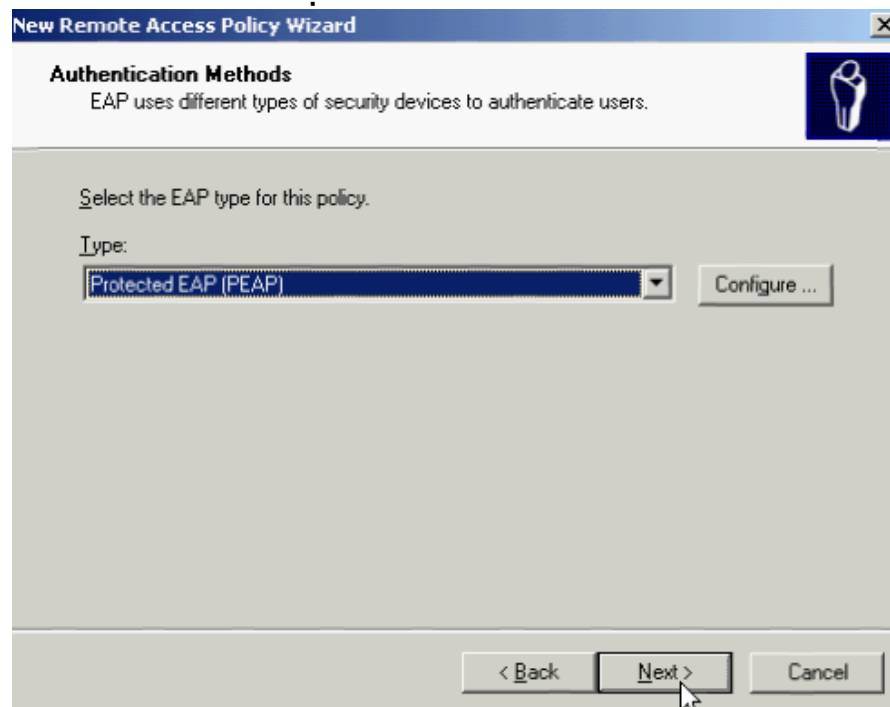
Chọn Wireless → nhấn nút OK



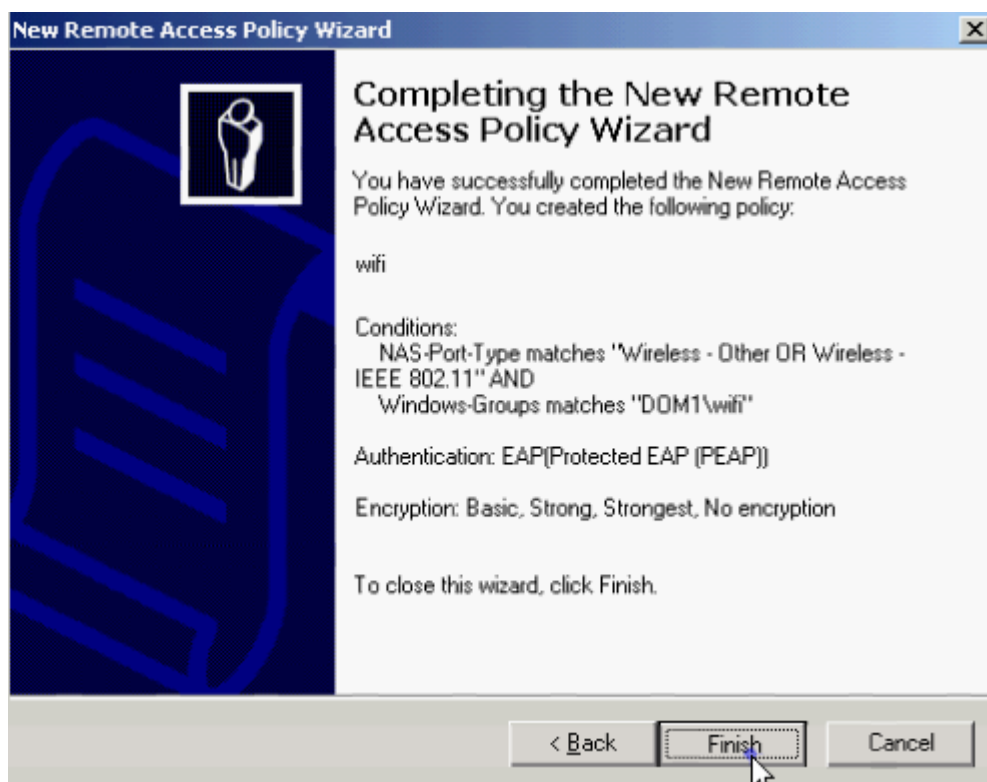
Hộp thoại xuất hiện → chọn Group → kích chuột vào nút Add để thêm user wifi vào → nhấn nút Next để tiếp tục



Chọn kiểu PEAP → kích chuột vào nút Next

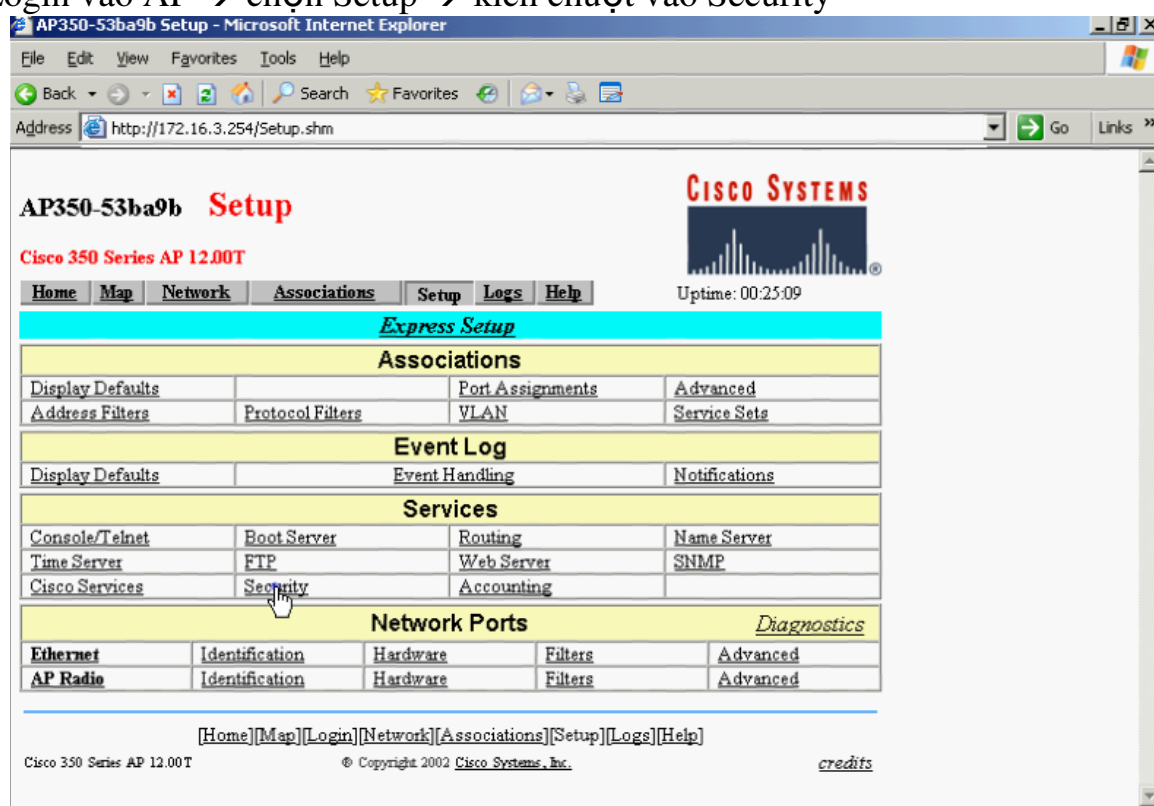


Nhấn nút Finish để kết thúc



7. Cấu hình AP-wifi, khai báo địa chỉ Radius Server = 172.16.3.1 để xác thực bằng Radius Server

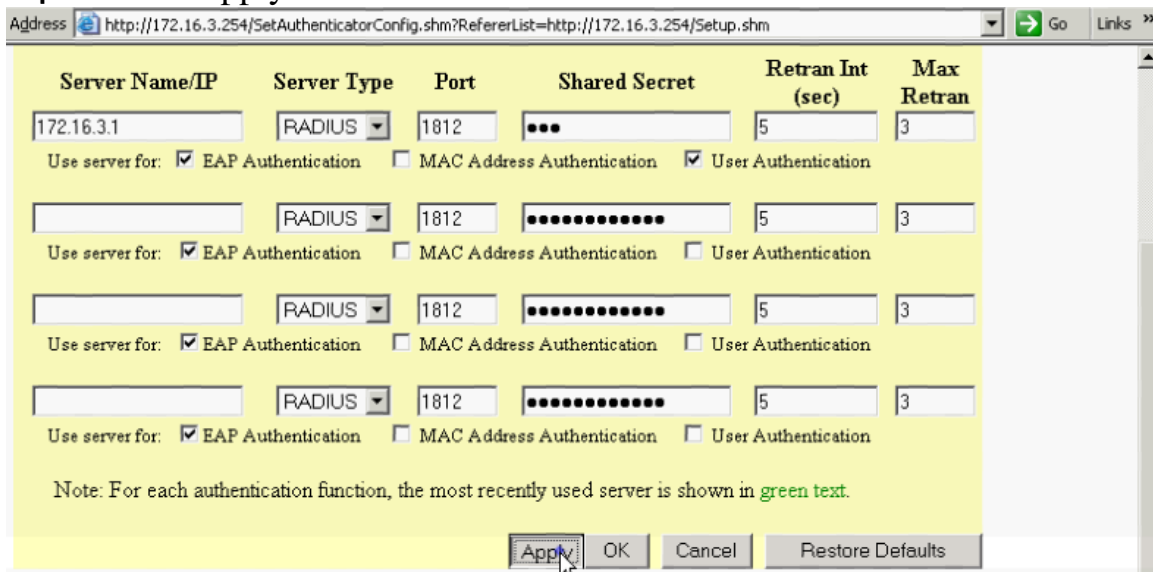
Login vào AP → chọn Setup → kích chuột vào Security



Kích chuột vào Authentication Server

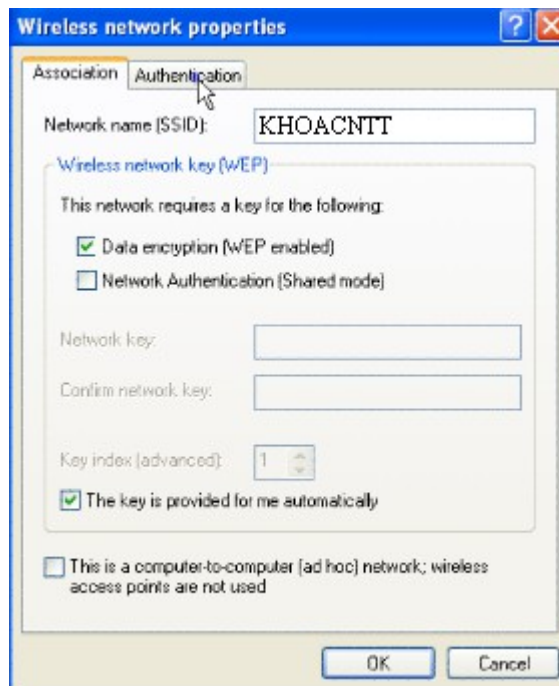


Khai báo địa chỉ Radius Server = 172.16.3.1, Shared Secret = 123 → nhấn chuột vào nút Apply để hoàn tất

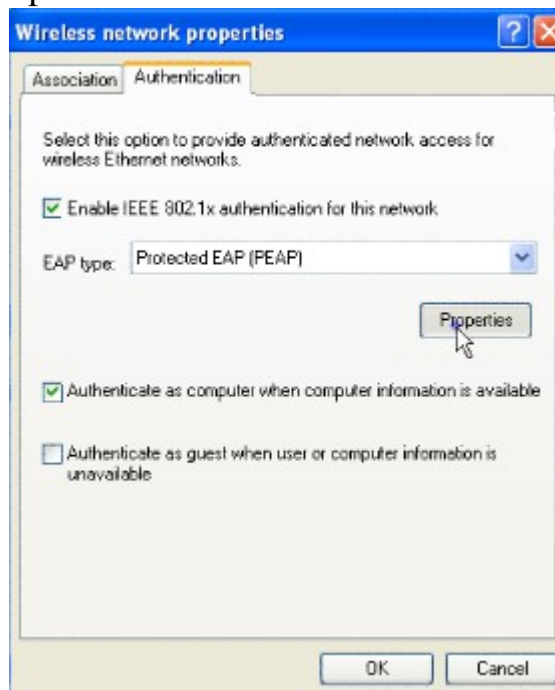


8. Kết nối PC-Client vào AP bằng cách xác thực qua Radius

Vào Network Connections → kích phải chuột lên Wireless Network Connection 2 → chọn Properties → kích chuột vào tab Wireless Networks → chọn AP – khoacntt → kích chuột vào nút Configuration → hộp thoại xuất hiện



Kích chuột vào tab Authentication → tí chọn các thông số như hình → sau đó kích chuột vào nút Properties



Hộp thoại xuất hiện

