Lời mở đầu

Ưu điểm của mạng máy tính đã được thể hiện khá rõ trong mọi lĩnh vực của cuộc sống. Đó chính là sự trao đổi, chia sẻ, lưu trữ và bảo vệ thông tin. Bên cạnh nền tảng mạng máy tính hữu tuyến, mạng máy tính không dây ngay từ khi ra đời đã thể hiện nhiều ưu điểm nổi bật về độ linh hoạt, tính giản đơn, khả năng tiện dụng. Trước đây, do chi phí còn cao nên mạng không dây còn chưa phổ biến, ngày nay khi mà giá thành thiết bị phần cứng ngày một hạ, khả năng xử lý ngày càng tăng thì mạng không dây đã được triển khai rộng rãi, ở một số nơi đã thay thế được mạng máy tính có dây khó triển khai.

Do đặc điểm trao đổi thông tin trong không gian truyền sóng nên khả năng thông tin bị rò rỉ ra ngoài là hoàn toàn dễ hiểu. Hơn nữa, ngày nay với sự phát triển cao của công nghệ thông tin, các hacker có thể dễ dàng xâm nhập vào mạng hơn bằng nhiều con đường khác nhau. Vì vậy có thể nói điểm yếu cơ bản nhất của mạng máy tính không dây đó là khả năng bảo mật, an toàn thông tin. Thông tin là một tài sản quý giá, đảm bảo được an toàn dữ liệu cho người sử dụng là một trong những yêu cầu được đặt ra hàng đầu. Chính vì vậy em đã quyết định chọn đề tài tìm hiểu về mạng không dây , về an ninh bảo mật mạng không dây , các biện pháp bảo mật .

Em xin chân thành cảm ơn thầy Vũ Trọng Chiến – Phó Giám đốc trung tâm thư viện trường đại học dân lập Hải Phòng đã giúp đỡ em nhiệt tình trong suốt quá trình làm đồ án cũng như xin được cảm ơn bạn bè đã góp ý, giúp đỡ em hoàn thành đồ án này.Do kiến thức còn hạn chế nên đồ án này chắc chắn sẽ không tránh được những sai sót, em rất mong nhận được những ý kiến đóng góp của thầy cô và các bạn.

cuu duong than cong . com

Hải Phòng 07/2009

TrầnĐứcViệt

CuuDuongThanCong.com

Mục lục

CuuDuongThanCong.com

CuuDuongThanCong.com

Chương 1: Giới thiệu một số công nghệ mạng không dây

1. Công nghệ sử dụng sóng hồng ngoại

Sử dụng ánh sáng hồng ngoại là một cách thay thế các sóng vô tuyến để kết nối các thiết bị không dây, bước sóng hồng ngoại từ khoảng 0.75-1000 micromet. Ánh sáng hồng ngoại không truyền qua được các vật chắn sáng, không trong suốt. Về hiệu suất ánh sáng hồng ngoại có độ rộng băng tần lớn, làm cho tín hiệu có thể truyền dữ liệu với tốc độ rất cao, tuy nhiên ánh sáng hồng ngoại không thích hợp như sóng vô tuyến cho các ứng dụng di động do vùng phủ sóng hạn chế. Phạm vi phủ sóng của nó khoảng 10m, một phạm vị quá nhỏ. Vì vậy mà nó thường ứng dụng cho các điện thoại di động, máy tính có cổng hồng ngoại trao đổi thông tin với nhau với điều kiện là đặt sát gần nhau.

2. Công nghệ Bluetooth

Bluetooth hoạt động ở dải tần 2.4Ghz, sử dụng phương thức trải phổ FHSS. Trong mạng Bluetooth, các phần tử có thể kết nối với nhau theo kiểu Adhoc ngang hàng hoặc theo kiểu tập trung, có 1 máy xử lý chính và có tối đa là 7 máy có thể kết nối vào. Khoảng cách chuẩn để kết nối giữa 2 đầu là 10 mét, nó có thể truyền qua tường, qua các đồ đạc vì công nghệ này không đòi hỏi đường truyền phải là tầm nhìn thẳng (LOS - Light of Sight). Tốc độ dữ liệu tối đa là 740Kbps (tốc độ của dòng bit lúc đó tương ứng khoảng 1Mbps. Nhìn chung thì công nghệ này còn có giá cả cao.

3. Công nghệ HomeRF

Công nghệ này cũng giống như công nghệ Bluetooth, hoạt động ở dải tần 2.4GHz, tổng băng thông tối đa là 1,6Mbps và 650Kbps cho mỗi người dùng. HomeRF cũng dùng phương thức điều chế FHSS

(*Frequency-hopping spread spectrum)* . Điểm khác so với Bluetooth là công nghệ HomeRF hướng tới thị trường nhiều hơn. Việc bổ xung chuẩn SWAP - Standard Wireless Access Protocol cho HomeRF cung cấp thêm khả năng quản lý các ứng dụng multimedia một cách hiệu quả hơn.

CuuDuongThanCong.com

4. Công nghệ HyperLAN

HyperLAN – High Performance Radio LAN theo chuẩn của Châu Âu là tương đương với công nghệ 802.11. HyperLAN loại 1 hỗ trợ băng thông 20Mpbs, làm việc ở dải tần 5GHz . HyperLAN 2 cũng làm việc trên dải tần này nhưng hỗ trợ băng thông lên tới 54Mpbs. Công nghệ này sử dụng kiểu kết nối hướng đối tượng (connection oriented) hỗ trợ nhiều thành phần đảm bảo chất lượng, đảm bảo cho các ứng dụng Multimedia

HiperLAN Type 1		**HiperLAN Type 2**	**HiperAccess**	**HiperLink**
Application	Wireless Ethernet (LAN)	Wireless ATM	Wireless Local Loop	Wireless Point-to-Point
Frequency	5 GHz	5 GHz	5 GHz	17 GHz
Data Rate	23.5 Mbps	~20 Mbps	~20 Mbps	~155 Mbps

cuu duong than cong . com

5. Công nghệ Wimax

Wimax là mạng WMAN bao phủ một vùng rộng lớn hơn nhiều mạng WLAN, kết nối nhiều toà nhà qua những khoảng cách địa lý rộng lớn. Công nghệ Wimax dựa trên chuẩn IEEE 802.16 và HiperMAN cho phép các thiết bị truyền thông trong một bán kính lên đến 50km và tốc độ truy nhập mạng lên đến 70 Mbps.

6. Công nghệ WiFi

WiFi là mạng WLAN bao phủ một vùng rộng hơn mạng WPAN, giới hạn đặc trưng trong các văn phòng, nhà hàng, gia đình,… Công nghệ WiFi dựa trên chuẩn IEEE 802.11 cho phép các thiết bị truyền thông trong phạm vi 100m với tốc độ 54 Mbps. Hiện nay công nghệ này khá phổ biến ở những thành phố lớn mà đặc biệt là trong các quán cafe.

cuu duong than cong . com

7. Công nghệ 3G

3G là mạng WWAN - mạng không dây bao phủ phạm phạm vi rộng nhất. Mạng 3G cho phép truyền thông dữ liệu tốc độ cao và dung lượng thoại lớn hơn cho

CuuDuongThanCong.com

những người dùng di động. Những dịch vụ tế bào thế hệ kế tiếp cũng dựa trên công nghệ 3G.

8. Công nghệ UWB

UWB (Ultra Wide Band) là một công nghệ mạng WPAN tương lai với khả năng hỗ trợ thông lượng cao lên đến 400 Mbps ở phạm vi ngắn tầm 10m. UWB sẽ có lợi ích giống như truy nhập USB không dây cho sự kết nối những thiết bị ngoại vi máy tính tới PC.

cuu duong than cong . com

cuu duong than cong . com

CuuDuongThanCong.com

Chương 2: Tổng quan về mạng máy tính không dây

I. Thế nào là mạng máy tính không dây ?

1. Giới thiệu

Thuật ngữ "mạng máy tính không dây" nói đến công nghệ cho phép hai hay nhiều máy tính giao tiếp với nhau dùng những giao thức mạng chuẩn nhưng không cần dây cáp mạng. Nó là một hệ thống mạng dữ liệu linh hoạt được thực hiện như một sự mở rộng hoặc một sự lựa chọn mới cho mạng máy tính hữu tuyến (hay còn gọi là mạng có dây). Các mạng máy tính không dây sử dụng các sóng điện từ không gian (sóng vô tuyến hoặc sóng ánh sáng) thu, phát dữ liệu qua không khí, giảm thiểu nhu cầu về kết nối bằng dây. Vì vậy, các mạng máy tính không dây kết hợp liên kết dữ liệu với tính di động của người sử dụng.

Công nghệ này bắt nguồn từ một số chuẩn công nghiệp như là IEEE 802.11 đã tạo ra một số các giải pháp không dây có tính khả thi trong kinh doanh, công nghệ chế tạo, các trường đại học… khi mà ở đó mạng hữu tuyến là không thể thực hiện được. Ngày nay, các mạng máy tính không dây càng trở nên quen thuộc hơn, được công nhận như một sự lựa chọn kết nối đa năng cho một phạm vi lớn các khách hàng kinh doanh.

2. Ưu điểm của mạng máy tính không dây

Mạng máy tính không dây đang nhanh chóng trở thành một mạng cốt lõi trong các mạng máy tính và đang phát triển vượt trội. Với công nghệ này, những người sử dụng có thể truy cập thông tin dùng chung mà không phải tìm kiếm chỗ để nối dây mạng, chúng ta có thể mở rộng phạm vi mạng mà không cần lắp đặt hoặc di chuyển dây. Các mạng máy tính không dây có ưu điểm về hiệu suất, sự thuận lợi, cụ thể như sau:

- ***Tính di động :*** những người sử dụng mạng máy tính không dây có thể truy nhập nguồn thông tin ở bất kỳ nơi nào. Tính di động này sẽ tăng năng suất và tính kịp thời thỏa mãn nhu cầu về thông tin mà các mạng hữu tuyến không thể có được.

CuuDuongThanCong.com

- ***Tính đơn giản :*** lắp đặt, thiết lập, kết nối một mạng máy tính không dây là rất dễ dàng, đơn giản và có thể tránh được việc kéo cáp qua các bức tường và trần nhà.

- ***Tính linh hoạt :*** có thể triển khai ở những nơi mà mạng hữu tuyến không thể triển khai được.

- ***Tiết kiệm chi phí lâu dài :*** Trong khi đầu tư cần thiết ban đầu đối với phần cứng của một mạng máy tính không dây có thể cao hơn chi phí phần cứng của một mạng hữu tuyến nhưng toàn bộ phí tổn lắp đặt và các chi phí về thời gian tồn tại có thể thấp hơn đáng kể. Chi phí dài hạn có lợi nhất trong các môi trường động cần phải di chuyển và thay đổi thường xuyên.

- ***Khả năng vô hướng :*** các mạng máy tính không dây có thể được cấu hình theo các topo khác nhau để đáp ứng các nhu cầu ứng dụng và lắp đặt cụ thể. Các cấu hình dễ dàng thay đổi từ các mạng ngang hàng thích hợp cho một số lượng nhỏ người sử dụng đến các mạng có cơ sở hạ tầng đầy đủ dành cho hàng nghìn người sử dụng mà có khả năng di chuyển trên một vùng rộng.

3. Hoạt động của mạng máy tính không dây

Các mạng máy tính không dây sử dụng các sóng điện từ không gian (vô tuyến hoặc ánh sáng) để truyền thông tin từ một điểm tới điểm khác. Các sóng vô tuyến thường được xem như các sóng mang vô tuyến do chúng chỉ thực hiện chức năng cung cấp năng lượng cho một máy thu ở xa. Dữ liệu đang được phát được điều chế trên sóng mang vô tuyến (thường được gọi là điều chế sóng mang nhờ thông tin đang được phát) sao cho có thể được khôi phục chính xác tại máy thu.

Nhiễu sóng mang vô tuyến có thể tồn tại trong cùng không gian, tại cùng thời điểm mà không can nhiễu lẫn nhau nếu các sóng vô tuyến được phát trên các tần số vô tuyến khác nhau. Để nhận lại dữ liệu, máy thu vô tuyến sẽ thu trên tần số vô tuyến của máy phát tương ứng.

Trong một cấu hình mạng máy tính không dây tiêu chuẩn, một thiết bị thu/phát (bộ thu/phát) được gọi là một điểm truy cập, nối với mạng hữu tuyến từ một vị trí cố định sử dụng cáp tiêu chuẩn. Chức năng tối thiểu của điểm truy cập là

CuuDuongThanCong.com

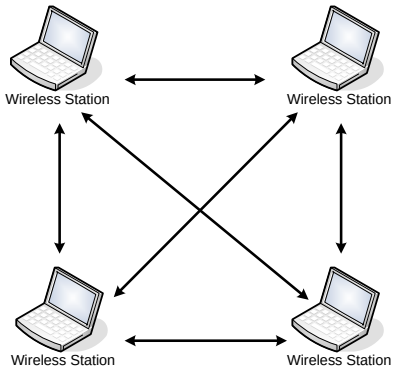
thu, làm đệm, và phát dữ liệu giữa mạng máy tính không dây và cơ sở hạ tầng mạng hữu tuyến. Một điểm truy cập đơn có thể hỗ trợ một nhóm nhỏ người sử dụng và có thể thực hiện chức năng trong một phạm vi từ một trăm đến vài trăm feet. Điểm truy cập (hoặc anten được gắn vào điểm truy cập) thường được đặt cao nhưng về cơ bản có thể được đặt ở bất kỳ chỗ nào miễn là đạt được vùng phủ sóng mong muốn.

Những người sử dụng truy cập vào mạng máy tính không dây thông qua các bộ thích ứng máy tính không dây như các Card mạng không dây trong các vi máy tính, các máy Palm, PDA. Các bộ thích ứng máy tính không dây cung cấp một giao diện giữa hệ thống điều hành mạng (NOS – Network Operation System) của máy khách và các sóng không gian qua một anten. Bản chất của kết nối không dây là trong suốt đối với hệ điều hành mạng.

4. Các mô hình của mạng máy tính không dây cơ bản

4.1. Kiểu Ad – hoc

Mỗi máy tính trong mạng giao tiếp trực tiếp với nhau thông qua các thiết bị card mạng không dây mà không dùng đến các thiết bị định tuyến hay thu phát không dây.



Mô hình mạng Ad – hoc (hay mạng ngang hàng)

4.2. Kiểu Infrastructure

Các máy tính trong hệ thống mạng sử dụng một hoặc nhiều các thiết bị định tuyến hay thiết bị thu phát để thực hiện các hoạt động trao đổi dữ liệu với nhau và các hoạt động khác.

CuuDuongThanCong.com

5. Cự ly truyền sóng, tốc độ truyền dữ liệu

Truyền sóng điện từ trong không gian sẽ gặp hiện tượng suy hao. Vì thế đối với kết nối không dây nói chung, khoảng cách càng xa thì khả năng thu tín hiệu càng kém, tỷ lệ lỗi sẽ tăng lên, dẫn đến tốc độ truyền dữ liệu sẽ phải giảm xuống.

Các tốc độ của chuẩn không dây như 11 Mbps hay 54 Mbps không liên quan đến tốc độ kết nối hay tốc độ download, vì những tốc độ này được quyết định bởi nhà cung cấp dịch vụ Internet.

Với một hệ thống mạng không dây, dữ liệu được giử qua sóng radio nên tốc độ có thể bị ảnh hưởng bởi các tác nhân gây nhiễu hoặc các vật thể lớn. Thiết bị định tuyến không dây sẽ tự động điều chỉnh xuống các mức tốc độ thấp hơn. (Ví dụ như là từ 11 Mbps sẽ giảm xuống còn 5,5 Mbps và 2 Mbps hoặc thậm chí là 1 Mbps).

II. Kỹ thuật điều chế trải phổ

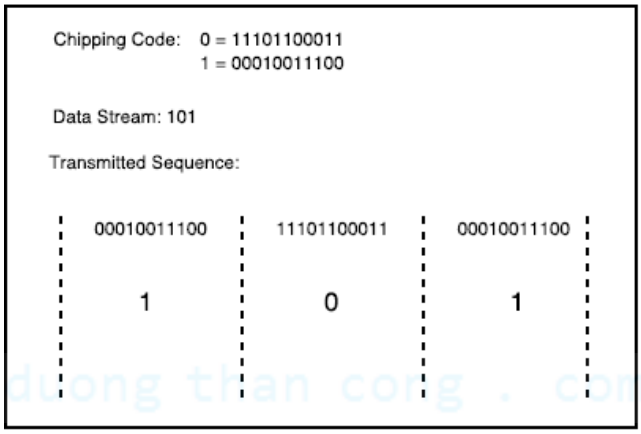
Hầu hết các mạng LAN không dây sử dụng công nghệ trải phổ. Điều chế trải phổ trải năng lượng của tín hiệu trên một độ rộng băng tần truyền dẫn lớn hơn nhiều so với độ rộng băng tần cần thiết tối thiểu. Điều này trái với mong muốn bảo toàn độ rộng băng tần nhưng quá trình trải phổ làm cho tín hiệu ít bị nhiễu điện từ hơn nhiều so với các kỹ thuật điều chế vô tuyến thông thường. Truyền dẫn khác và nhiễu điện từ thường là băng hẹp sẽ chỉ gây can nhiễu với một phần nhỏ của tín hiệu trải phổ, nó sẽ gây ra ít nhiễu và ít lỗi hơn nhiều khi các máy thu giải điều chế tín hiệu.

Điều chế trải phổ không hiệu quả về độ rộng băng tần khi được sử dụng bởi một người sử dụng. Tuy nhiên, do nhiều người sử dụng có thể dùng chung cùng độ rộng băng tần phổ mà không can nhiễu với nhau, các hệ thống trải phổ trở nên có hiệu quả về độ rộng băng tần trong môi trường nhiều người sử dụng. Điều chế trải phổ sử dụng hai phương pháp trải tín hiệu trên một băng tần rộng hơn: trải phổ chuỗi trực tiếp và trải phổ nhẩy tần.

CuuDuongThanCong.com

1. Trải phổ trực tiếp DSSS – Direct Sequence Spread Spectrum

Trải phổ chuỗi trực tiếp kết hợp một tín hiệu dữ liệu tại trạm gửi với một chuỗi bit tốc độ dữ liệu cao hơn nhiều, mà nhiều người xem như một chipping code (còn gọi là một gain xử lý). Một gain xử lý cao làm tăng khả năng chống nhiễu của tín hiệu. Gain xử lý tuyến tính tối thiểu mà FCC – Federal Communications Commission cho phép là 10, và hầu hết các sản phẩm khai thác dưới 20. Nhóm làm việc của Viện nghiên cứu điện-điện tử IEEE - Institute of Electrical and Electronics Engineers đặt gain xử lý tối thiểu cần thiết của 802.11 là 11.



Hoạt động của trải phổ chuỗi trực tiếp

Hình trên cho thấy một ví dụ về hoạt động của trải phổ chuỗi trực tiếp. Một chipping code được biểu thị bởi các bit dữ liệu logic 0 và 1. Khi luồng dữ liệu được phát, mã tương ứng được gửi. Ví dụ, truyền dẫn một bit dữ liệu bằng 0 sẽ dẫn đến chuỗi 00010011100 đang được gửi.

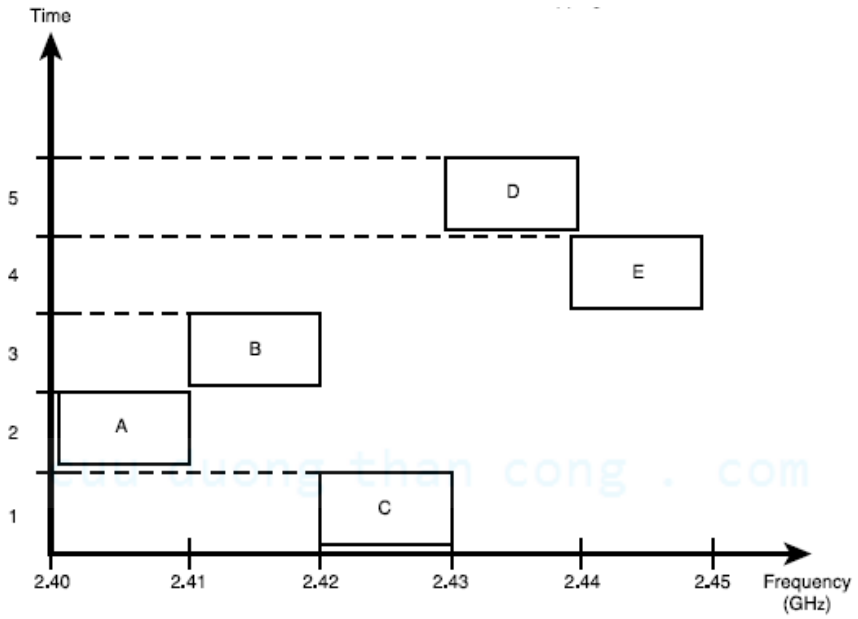
Nhiều sản phẩm trải phổ chuỗi trực tiếp trên thị trường sử dụng nhiều hơn một

kênh trên cùng một khu vực, tuy nhiên số kênh khả dụng bị hạn chế. Với chuỗi trực tiếp, nhều sản phẩm hoạt động trên các kênh riêng biệt bằng cách chia băng tần số thành các kênh tần số không gối nhau. Điều này cho phép một số mạng riêng biệt hoạt động mà không can nhiễu lẫn nhau. Tuy nhiên, độ rộng băng tần phải đủ để điều tiết các tốc độ dữ liệu cao, chỉ có thể có một số kênh.

CuuDuongThanCong.com

2. Trải phổ nhẩy tần FHSS – Frequency Hopping Spread Spectrum

Trong trải phổ nhẩy tần, tín hiệu dữ liệu của người sử dụng được điều chế với một tín hiệu sóng mang. Các tần số sóng mang của những người sủ dụng riêng biệt được làm cho khác nhau theo kiểu giả ngẫu nhiên trong một kênh băng rộng. Dữ liệu số được tách thành các cụm dữ liệu kích thước giống nhau được phát trên các tần số sóng mang khác nhau. Độ rộng băng tần tức thời của các cụm truyền dẫn nhỏ hơn nhiều so với toàn bộ độ rộng băng tần trải phổ. Mã giả ngẫu nhiên thay đổi các tần số sóng mang của người sử dụng, ngẫu nhiên hóa độ chiếm dụng của một kênh kênh cụ thể tại bất kỳ thời điểm nào. Trong máy thu nhẩy tần, một mã giả ngẫu nhiên được phát nội bộ được sử dụng để đồng bộ tần số tức thời của các máy thu với các máy phát. Tại bất kỳ thời điểm nào, một tín hiệu nhẩy tần chiếm một kênh đơn tương đối hẹp. Nếu tốc độ thay đổi của tần số sóng mang lớn hơn nhiều so với tốc độ ký tự thì hệ thống được coi như là một hệ thống nhẩy tần nhanh. Nếu kênh thay đổi tại một tốc độ nhỏ hơn hoặc bằng tốc độ ký tự thì hệ thống được gọi là nhẩy tần chậm.



Mô hình nhảy tần CABED

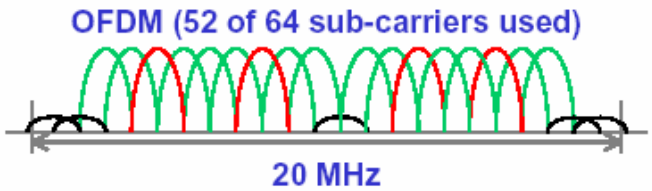
Một hệ thống nhẩy tần cung cấp một mức bảo mật, đặc biệt là khi sử dụng một số lượng lớn kênh, do một máy thu vô tình không biết chuỗi giả ngẫu nhiên của

CuuDuongThanCong.com

các khe tần số phải dò lại nhanh chóng để tìm tín hiệu mà họ muốn nghe trộm. Ngoài ra, tín hiệu nhảy tần hạn chế được fading, do có thể sử dụng sự mã hóa điều khiển lỗi và sự xen kẽ để bảo vệ tín hiệu nhảy tần khỏi sự suy giảm rõ rệt đôi khi có thể xảy ra trong quá trình nhảy tần. Việc mã hóa điều khiển lỗi và xen kẽ cũng có thể được kết hợp để tránh một kênh xóa bỏ khi hai hay nhiều người sử dụng phát trên cùng kênh tại cùng thời điểm.

3. Công nghệ ghép kênh phân chia theo tần số trực giao OFDM – Orthogonal Frequency Division Multiplexing

OFDM là một công nghệ đã ra đời từ nhiều năm trước đây, từ những năm 1960, 1970 khi người ta nghiên cứu về hiện tượng nhiễu xẩy ra giữa các kênh, nhưng nó chỉ thực sự trở nên phổ biến trong những năm gần đây nhờ sự phát triển của công nghệ xử lý tín hiệu số. OFDM được đưa vào áp dụng cho công nghệ truyền thông không dây băng thông rộng nhằm khắc phục một số nhược điểm và tăng khả năng về băng thông cho công nghệ mạng không dây, nó được áp dụng cho chuẩn IEEE 802.11a và chuẩn ETSI HiperLAN/2, nó cũng được áp dụng cho công nghệ phát thanh, truyền hình ở các nước Châu Âu.



Phương thức điều chế OFDM

OFDM là một phương thức điều chế đa sóng mang được chia thành nhiều luồng dữ liệu với nhiều sóng mang khác nhau (hay còn gọi là những kênh hẹp) truyền cùng nhau trên một kênh chính, mỗi luồng chỉ chiếm một tỷ lệ dữ liệu rất nhỏ. Sau khi bên thu nhận dữ liệu, nó sẽ tổng hợp các nhiều luồng đó để ghép lại bản tin ban đầu. Nguyên lý hoạt động của phương thức này cũng giống như của công nghệ CDMA .

CuuDuongThanCong.com

III. Các chuẩn của 802.11

IEEE (Institute of Electrical and Electronic Engineers) là tổ chức đi tiên phong trong lĩnh vực chuẩn hóa mạng LAN với đề án IEEE 802 nổi tiếng bắt đầu triển khai từ năm 1980 và kết quả là hàng loạt chuẩn thuộc họ IEEE 802.x ra đời, tạo nên một sự hội tụ quan trọng cho việc thiết kế và cài đặt các mạng LAN trong thời gian qua.

802.11 là một trong các chuẩn của họ IEEE 802.x bao gồm họ các giao thức truyền tin qua mạng không dây. Trước khi giới thiệu 802.11 chúng ta sẽ cùng điểm qua một số chuẩn 802 khác:

- 802.1: các Cầu nối (Bridging), Quản lý (Management) mạng LAN, WAN
- 802.2: điều khiển kết nối logic
- 802.3: các phương thức hoạt động của mạng Ethernet
- 802.4: mạng Token Bus
- 802.5: mạng Token Ring
- 802.6: mạng MAN
- 802.7: mạng LAN băng rộng
- 802.8: mạng quang
- 802.9: dịch vụ luồng dữ liệu
- 802.10: an ninh giữa các mạng LAN
- 802.11: mạng LAN không dây – Wireless LAN
- 802.12: phương phức ưu tiên truy cập theo yêu cầu
- 802.13: chưa có
- 802.14: truyền hình cáp
- 802.15: mạng PAN không dây
- 802.16: mạng không dây băng rộng

Chuẩn 802.11 chủ yếu cho việc phân phát các MSDU (đơn vị dữ liệu dịch vụ của MAC) giữa các kết nối LLC (điều khiển liên kết logic).

CuuDuongThanCong.com

Chuẩn 802.11 được chia làm hai nhóm: nhóm lớp vật lý PHY và nhóm lớp liên kết dữ liệu MAC.

1. Nhóm lớp vật lý PHY

1.1. Chuẩn 802.11b

802.11b là chuẩn đáp ứng đủ cho phần lớn các ứng dụng của mạng. Với một giải pháp rất hoàn thiên, 802.11b có nhiều đặc điểm thuận lợi so với các chuẩn không dây khác. Chuẩn 802.11b sử dụng kiểu trải phổ trực tiếp DSSS, hoạt động ở dải tần 2,4 GHz, tốc độ truyền dữ liệu tối đa là 11 Mbps trên một kênh, tốc độ thực tế là khoảng từ 4-5 Mbps. Khoảng cách có thể lên đến 500 mét trong môi trường mở rộng. Khi dùng chuẩn này tối đa có 32 người dùng / điểm truy cập.

Đây là chuẩn đã được chấp nhận rộng rãi trên thế giới và được triên khai rất mạnh hiện nay do công nghệ này sử dụng dải tần không phải đăng ký cấp phép phục vụ cho công nghiệp, dịch vụ, y tế.

Nhược điểm của 802.11b là hoạt động ở dải tần 2,4 GHz trùng với dải tần của nhiều thiết bị trong gia đình như lò vi sóng , điện thoại mẹ con ... nên có thể bị nhiễu.

cuu duong than cong . com

1.2. Chuẩn 802.11a

Chuẩn 802.11a là phiên bản nâng cấp của 802.11b, hoạt động ở dải tần 5 GHz , dùng công nghệ trải phổ OFDM. Tốc độ tối đa từ 25 Mbps đến 54 Mbps trên một kênh, tốc độ thực tế xấp xỉ 27 Mbps, dùng chuẩn này tối đa có 64 người dùng / điểm truy cập. Đây cũng là chuẩn đã được chấp nhận rộng rãi trên thế giới.

1.3. Chuẩn 802.11g

cuu duong than cong . com

Các thiết bị thuộc chuẩn này hoạt động ở cùng tần số với chuẩn 802.11b là 2,4 Ghz. Tuy nhiên chúng hỗ trợ tốc độ truyền dữ liệu nhanh gấp 5 lần so với chuẩn 802.11b với cùng một phạm vi phủ sóng, tức là tốc độ truyền dữ liệu tối đa lên đến 54 Mbps, còn tốc độ thực tế là khoảng 7-16 Mbps. Chuẩn 802.11g sử dụng phương pháp điều chế OFDM, CCK – Complementary Code Keying và PBCC – Packet Binary Convolutional Coding. Các thiết bị thuộc chuẩn 802.11b và 802.11g hoàn

CuuDuongThanCong.com

toàn tương thích với nhau. Tuy nhiên cần lưu ý rằng khi bạn trộn lẫn các thiết bị của hai chuẩn đó với nhau thì các thiết bị sẽ hoạt động theo chuẩn nào có tốc độ thấp hơn. Đây là một chuẩn hứa hẹn trong tương lai nhưng hiện nay vẫn chưa được chấp thuận rộng rãi trên thế giới.

2. Nhóm lớp liên kết dữ liệu MAC

2.1. Chuẩn 802.11d

Chuẩn 802.11d bổ xung một số tính năng đối với lớp MAC nhằm phổ biến WLAN trên toàn thế giới. Một số nước trên thế giới có quy định rất chặt chẽ về tần số và mức năng lượng phát sóng vì vậy 802.11d ra đời nhằm đáp ứng nhu cầu đó. Tuy nhiên, chuẩn 802.11d vẫn đang trong quá trình phát triển và chưa được chấp nhận rộng rãi như là chuẩn của thế giới.

2.2. Chuẩn 802.11e

Đây là chuẩn được áp dụng cho cả 802.11 a,b,g. Mục tiêu của chuẩn này nhằm cung cấp các chức năng về chất lượng dịch vụ - QoS cho WLAN. Về mặt kỹ thuật, 802.11e cũng bổ xung một số tính năng cho lớp con MAC. Nhờ tính năng này, WLAN 802.11 trong một tương lại không xa có thể cung cấp đầy đủ các dịch vụ như voice, video, các dịch vụ đòi hỏi QoS rất cao. Chuẩn 802.11e hiện nay vẫn đang trong qua trình phát triển và chưa chính thức áp dụng trên toàn thế giới.

2.3. Chuẩn 802.11f

Đây là một bộ tài liệu khuyến nghị của các nhà sản xuất để các Access Point của các nhà sản xuất khác nhau có thể làm việc với nhau. Điều này là rất quan trọng khi quy mô mạng lưới đạt đến mức đáng kể. Khi đó mới đáp ứng được việc kết nối mạng không dây liên cơ quan, liên xí nghiệp có nhiều khả năng không dùng cùng một chủng loại thiết bị.

2.4. Chuẩn 802.11h

Tiêu chuẩn này bổ xung một số tính năng cho lớp con MAC nhằm đáp ứng các quy định châu Âu ở dải tần 5GHz. Châu Âu quy định rằng các sản phẩm dùng

CuuDuongThanCong.com

dải tần 5 GHz phải có tính năng kiểm soát mức năng lượng truyền dẫn TPC - Transmission Power Control và khả năng tự động lựa chọn tần số DFS - Dynamic Frequency Selection. Lựa chọn tần số ở Access Point giúp làm giảm đến mức tối thiểu can nhiễu đến các hệ thống radar đặc biệt khác.

2.5. Chuẩn 802.11i

Đây là chuẩn bổ xung cho 802.11 a, b, g nhằm cải thiện về mặt an ninh cho mạng không dây. An ninh cho mạng không dây là một giao thức có tên là WEP, 802.11i cung cấp những phương thức mã hóa và những thủ tục xác nhận, chứng thực mới có tên là 802.1x. Chuẩn này vẫn đang trong giai đoạn phát triển.

IV. Các kiến trúc cơ bản của chuẩn 802.11

1. Trạm thu phát - STA

STA – Station, các trạm thu/phát sóng. Thực chất ra là các thiết bị không dây kết nối vào mạng như máy vi tính, máy Palm, máy PDA, điện thoại di động, vv... với vai trò như phần tử trong mô hình mạng ngang hàng Pear to Pear hoặc Client trong mô hình Client/Server. Trong phạm vi đồ án này chỉ đề cập đến thiết bị không dây là máy vi tính (thường là máy xách tay cũng có thể là máy để bàn có card mạng kết nối không dây). Có trường hợp trong đồ án này gọi thiết bị không dây là STA, có lúc là Client, cũng có lúc gọi trực tiếp là máy tính xách tay. Thực ra là như nhau nhưng cách gọi tên khác nhau cho phù hợp với tình huống đề cập.

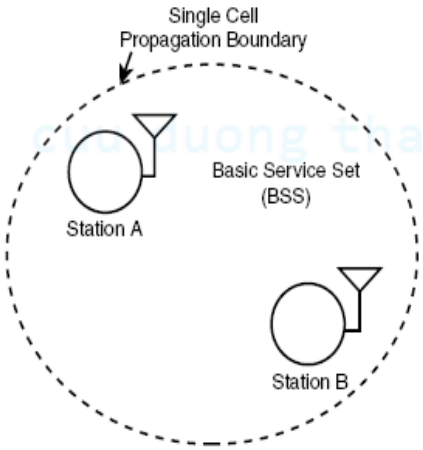
2. Điểm truy cập – AP

Điểm truy cập – Acces Point là thiết bị không dây, là điểm tập trung giao tiếp với các STA, đóng vai trò cả trong việc truyền và nhận dữ liệu mạng. AP còn có chức năng kết nối mạng không dây thông qua chuẩn cáp Ethernet, là cầu nối giữa mạng không dây với mạng có dây. AP có phạm vi từ 30m đến 300m phụ thuộc vào công nghệ và cấu hình.

CuuDuongThanCong.com

3. Trạm phục vụ cơ bản – BSS

Kiến trúc cơ bản nhất trong WLAN 802.11 là BSS – Base Service Set. Đây là đơn vị của một mạng con không dây cơ bản. Trong BSS có chứa các STA, nếu không có AP thì sẽ là mạng các phần tử STA ngang hàng (còn được gọi là mạng Adhoc), còn nếu có AP thì sẽ là mạng phân cấp (còn gọi là mạng Infrastructure). Các STA trong cùng một BSS thì có thể trao đổi thông tin với nhau. Người ta thường dùng hình Oval để biểu thị phạm vi của một BSS. Nếu một STA nào đó nằm ngoài một hình Oval thì coi như STA không giao tiếp được với các STA, AP nằm trong hình Oval đó. Việc kết hợp giữa STA và BSS có tính chất động vì STA có thể di chuyển từ BSS này sang BSS khác. Một BSS được xác định bởi mã định danh hệ thống (SSID – System Set Identifier), hoặc nó cũng có thể hiểu là tên của mạng không dây đó.



Mô hình một BSS

4. BSS độc lập – IBSS

Trong mô hình IBSS – Independent BSS, là các BSS độc lập, tức là không có kết nối với mạng có dây bên ngoài. Trong IBSS, các STA có vai trò ngang nhau. IBSS thường được áp dụng cho mô hình Adhoc bởi vì nó có thể được xây dựng nhanh chóng mà không phải cần nhiều kế hoạch.

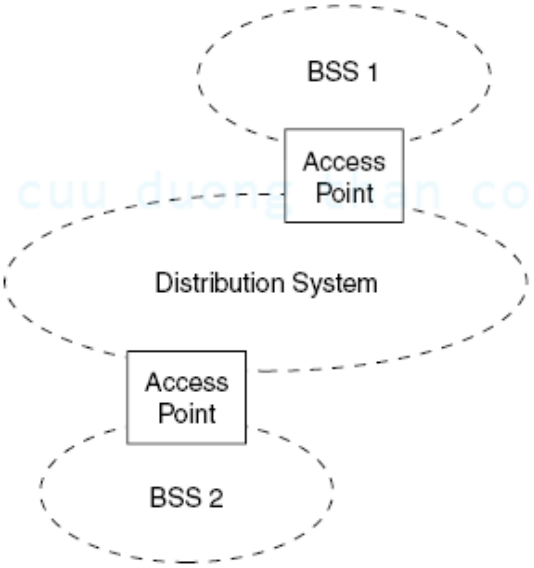
CuuDuongThanCong.com

5. Hệ thống phân tán – DS

Người ta gọi DS – Distribution System là một tập hợp của các BSS. Mà các BSS này có thể trao đổi thông tin với nhau. Một DS có nhiệm vụ kết hợp với các BSS một cách thông suốt và đảm bảo giải quyết vấn đề địa chỉ cho toàn mạng

6. Hệ thống phục vụ mở rộng - ESS

ESS – Extended Service Set là một khái niệm rộng hơn. Mô hình ESS là sự kết hợp giữa DS và BSS cho ta một mạng với kích cỡ tùy ý và có đầy đủ các tính năng phức tạp. Đặc trưng quan trọng nhất trong một ESS là các STA có thể giao tiếp với nhau và di chuyển từ một vùng phủ sóng của BSS này sang vùng phủ sóng của BSS mà vẫn trong suốt với nhau ở mức LLC – Logical Link Control.



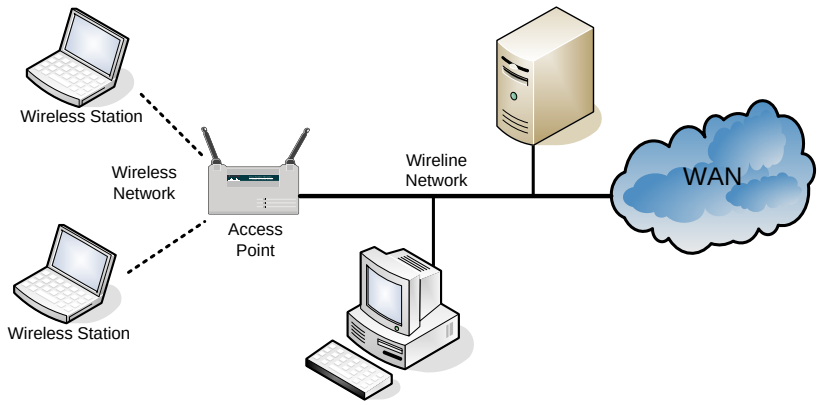
Mô hình ESS

7. Mô hình thực tế

Trên thực tế thì có rất nhiều mô hình mạng không dây từ một vài máy tính kết nối Adhoc đến mô hình WLAN, WWAN, mạng phức hợp. Sau đây là 2 loại mô hình kết nối mạng không dây phổ biến, từ 2 mô hình này có thể kết hợp để tạo ra nhiều mô hình phức tạp, đa dạng khác

CuuDuongThanCong.com

7.1. Mạng không dây kết nối với mạng có dây

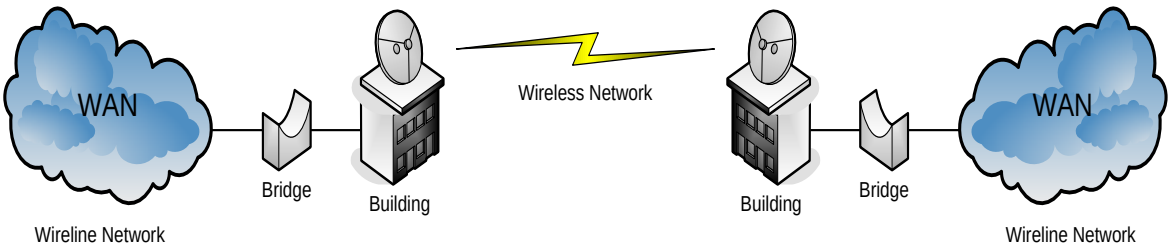


Mô hình mạng không dây kết nối với mạng có dây

AP sẽ làm nhiệm vụ tập trung các kết nối không dây, đồng thời nó kết nối vào mạng WAN (hoặc LAN) thông qua giao diện Ethernet RJ45, ở phạm vi hẹp có thể coi AP làm nhiệm vụ như một router định tuyến giữa 2 mạng này

7.2. Hai mạng có dây kết nối với nhau bằng kết nối không dây

cuu duong than cong . com



Mô hình 2 mạng có dây kết nối với nhau bằng kết nối không dây

Kết nối không dây giữa 2 đầu của mạng 2 mạng WAN sử dụng thiết bị Bridge làm cầu nối, có thể kết hợp sử dụng chảo thu phát nhỏ truyền sóng viba. Khi đó khoảng cách giữa 2 đầu kết nối có thể từ vài trăm mét đến vài chục km tùy vào loại thiết bị cầu nối không dây

CuuDuongThanCong.com

V. Một số cơ chế sử dụng khi trao đổi thông tin trong mạng không dây

1. Cơ chế CSMA-CA

Nguyên tắc cơ bản khi truy cập của chuẩn 802.11 là sử dụng cơ chế CSMA-CA viết tắt của Carrier Sense Multiple Access Collision Avoidance – Đa truy cập sử dụng sóng mang phòng tránh xung đột. Nguyên tắc này gần giống như nguyên tắc CSMA-CD (Carrier Sense Multiple Access Collision Detect) của chuẩn 802.3 (cho Ethernet). Điểm khác ở đây là CSMA-CA nó sẽ chỉ truyền dữ liệu khi bên kia sẵn sàng nhận và không truyền, nhận dữ liệu nào khác trong lúc đó, đây còn gọi là nguyên tắc LBT listening before talking – nghe trước khi nói.

Trước khi gói tin được truyền đi, thiết bị không dây đó sẽ kiểm tra xem có các thiết bị nào khác đang truyền tin không, nếu đang truyền, nó sẽ đợi đến khi nào các thiết bị kia truyền xong thì nó mới truyền. Để kiểm tra việc các thiết bị kia đã truyền xong chưa, trong khi "đợi" nó sẽ hỏi "thăm dò" đều đặn sau các khoảng thời gian nhất định.

2. Cơ chế RTS/CTS

Để giảm thiểu nguy xung đột do các thiết bị cùng truyền trong cùng thời điểm, người ta sử dụng cơ chế RTS/CTS – Request To Send/ Clear To Send. Ví dụ nếu AP muốn truyền dữ liệu đến STA, nó sẽ gửi 1 khung RTS đến STA, STA nhận được tin và gửi lại khung CTS, để thông báo sẵn sàng nhận dữ liệu từ AP, đồng thời không thực hiện truyền dữ liệu với các thiết bị khác cho đến khi AP truyền xong cho STA. Lúc đó các thiết bị khác nhận được thông báo cũng sẽ tạm ngừng việc truyền thông tin đến STA. Cơ chế RTS/CTS đảm bảo tính sẵn sàng giữa 2 điểm truyền dữ liệu và ngăn chặn nguy cơ xung đột khi truyền dữ liệu.

3. Cơ chế ACK

ACK – Acknowledging là cơ chế thông báo lại kết quả truyền dữ liệu. Khi bên nhận nhận được dữ liệu, nó sẽ gửi thông báo ACK đến bên gửi báo là đã nhận

CuuDuongThanCong.com

được bản tin rồi. Trong tình huống khi bên gửi không nhận được ACK nó sẽ coi là bên nhận chưa nhận được bản tin và nó sẽ gửi lại bản tin đó. Cơ chế này nhằm giảm bớt nguy cơ bị mất dữ liệu trong khi truyền giữa 2 điểm.

cuu duong than cong . com

cuu duong than cong . com

CuuDuongThanCong.com

Chương 3: Các vấn đề cần quan tâm của mạng máy tính không dây, vấn đề an ninh mạng

I. Các vấn đề của mạng không dây, tương quan đối với mạng có dây

Khi xây dựng một mạng máy tính, để đưa ra giải pháp kỹ thuật và thiết bị phù hợp, người ta phải dựa trên việc phân tích khả năng đáp ứng yêu cầu theo các tiêu chí đề ra. Để thấy được những vấn đề của mạng không dây cũng như tương quan những vấn đề đó so với mạng có dây, tôi xin đưa ra một số tiêu chí cơ bản và so sánh giải pháp của mạng có dây và mạng không dây.

1. Phạm vi ứng dụng

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

2. Độ phức tạp kỹ thuật

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

CuuDuongThanCong.com

3. Độ tin cậy

Mạng có dây	Mạng không dây
- Khả năng chịu ảnh hưởng khách quan bên ngoài như thời tiết, khí hậu tốt - Chịu nhiều cuộc tấn công đa dạng, phức tạp, nguy hiểm của những kẻ phá hoại vô tình và cố tình - Ít nguy cơ ảnh hưởng sức khỏe	- Bị ảnh hưởng bởi các yếu tố bên ngoài như môi trường truyền sóng, can nhiễu do thời tiết - Chịu nhiều cuộc tấn công đa dạng, phức tạp, nguy hiểm của những kẻ phá hoại vô tình và cố tình, nguy cơ cao hơn mạng có dây - Còn đang tiếp tục phân tích về khả năng ảnh hưởng đến sức khỏe

4. Lắp đặt, triển khai

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

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

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

6. Giá cả

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

CuuDuongThanCong.com

II. Tại sao an ninh mạng là vấn đề quan trọng của mạng máy tính không dây ?

Từ các phân tích của mục trên ta đã thấy được những ưu điểm và nhược điểm của mạng máy tính không dây. Trong các ưu, nhược điểm đó thì vấn đề an ninh mạng là quan trọng xét theo 2 khía cạnh sau:

1. Xem xét tương quan với các vấn đề khác

- Đối với mạng không dây các vấn đề như can nhiễu tín hiệu vô tuyến, kiểm soát năng lượng, ảnh hưởng sức khỏe có thể giảm thiểu ảnh hưởng tối đa đến mức cho phép nhờ sự phát triển của khoa học, kỹ thuật

- Giá cả thiết bị có thể giảm xuống do thị trường sử dụng ngày càng mở rộng

- An ninh mạng là điều ngày càng bức xúc, nguy cơ bị tấn công mạng ngày càng tăng. Bởi vì tấn công, phá hoại là do con người thực hiện, kỹ thuật càng phát triển, càng thêm khả năng đối phó, ngăn chặn thì kẻ tấn công cũng ngày càng tìm ra nhiều các kỹ thuật tấn công khác cũng như những lỗi kỹ thuật khác của hệ thống.

cuu duong than cong . com

2. Xem xét tương quan với mạng có dây

Sở dĩ nguy cơ bị tấn công của mạng không dây lớn hơn của mạng có dây là do những yếu tố sau:

- Kẻ tấn công thường thực hiện ngay trong vùng phủ sóng

- Thông tin trao đổi trong không gian, vì vậy không thể ngăn chặn được việc bị lấy trộm thông tin

- Công nghệ còn khá mới mẻ, nhất là đối với Việt Nam. Các công nghệ từ khi đưa ra đến khi áp dụng thực tế còn cách nhau một khoảng thời gian dài

cuu duong than cong . com

CuuDuongThanCong.com

III. Phạm vi nghiên cứu của đồ án này

Cũng như mạng mạng máy tính có dây, mạng máy tính không dây cũng có những cấu trúc từ đơn giản đến rất phức tạp. Đồ án này nghiên cứu dựa trên mạng máy tính không dây nhưng tập trung vào nghiên cứu các vấn đề an ninh mạng trên mạng máy tính nội bộ không dây cơ bản Wireless LAN hay gọi tắt là WLAN, vì đây là mạng không dây cơ bản, từ mô hình này có thể phát triển ra các mô hình mạng khác như mạng WAN không dây, mạng không dây kết hợp mạng có dây. Tiếp theo mới là các mô hình mạng máy tính không dây phức tạp khác.

cuu duong than cong . com

cuu duong than cong . com

CuuDuongThanCong.com

Chương 4: Bảo mật trong mạng WLAN

I. Cơ sở bảo mật mạng WLAN

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

1. Giới hạn lan truyền RF

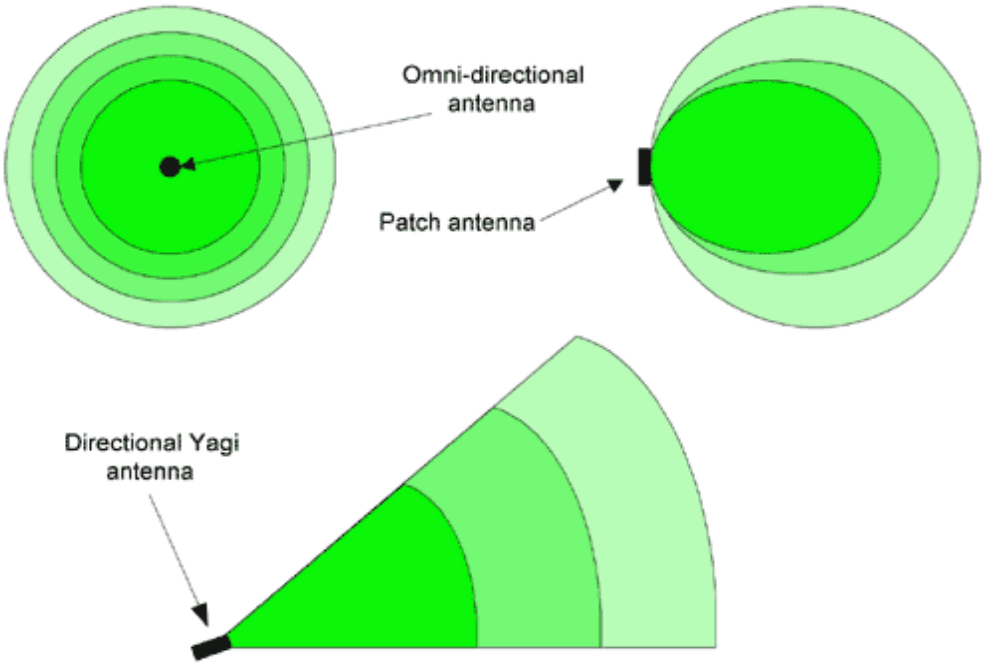
Trước khi thực hiện các biện pháp bảo mật, ta cần xét các vấn đề liên quan với lan truyền RF do các AP trong một mạng không dây. Khi chọn tốt, việc kết hợp máy phát và anten thích hợp là một công cụ bảo mật có hiệu quả để giới hạn truy cập tới mạng không dây trong vùng phủ sóng định trước. Khi chọn kém,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

cuu duong than cong . com

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

cuu duong than cong . com

CuuDuongThanCong.com



Các mẫu lan truyền RF của các anten phổ biến.

2. Định danh thiết lập Dịch vụ (SSID)

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

Trong kiểu hoạt động khác, SSID được sử dụng như một biện pháp bảo mật bằng cách định cấu hình AP để không lan truyền SSID của nó. Trong kiểu này, trạm vô tuyến muốn liên kết đến AP phải sẵn có SSID đã định cấu hình giống với SSID của AP. Nếu các SSID khác nhau, các khung quản lý từ trạm vô tuyến gửi đến AP sẽ bị loại bỏ vì chúng chứa SSID sai và liên kết sẽ không xảy ra.

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

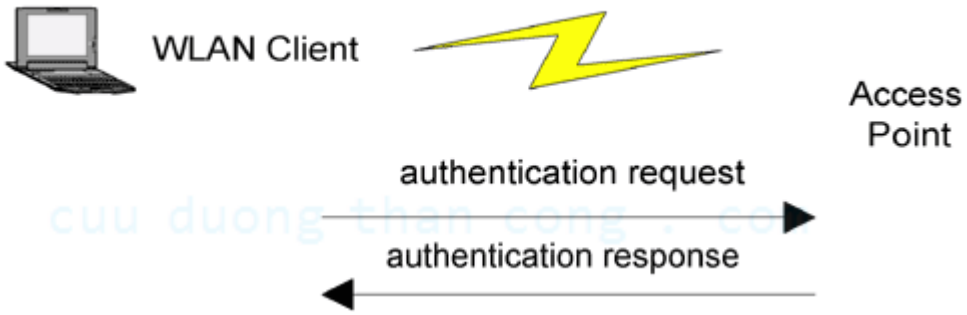
CuuDuongThanCong.com

3. Các kiểu Chứng thực

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

Chứng thực hệ thống mở

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



Chứng thực hệ thống mở.

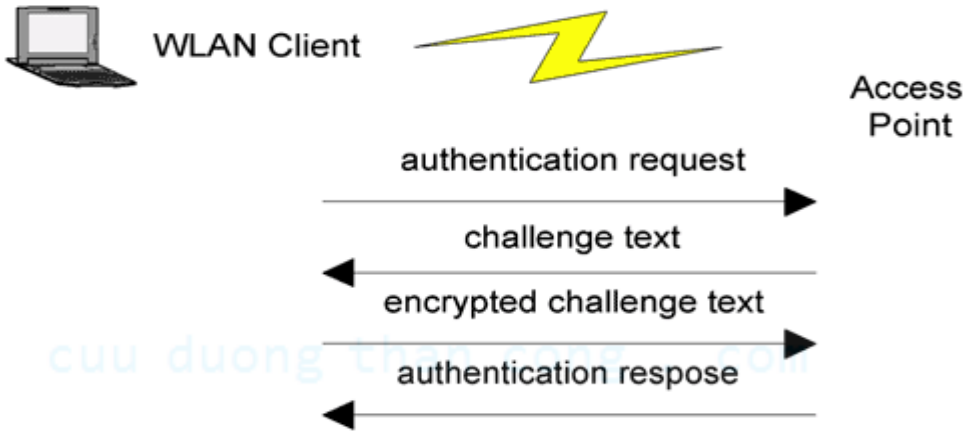
Chứng thực khóa chia sẻ

Chứng thực khóa chia sẻ (hình 4.4) được xác nhận trên cơ sở cả hai trạm tham gia trong quá trình chứng thực có cùng khóa "chia sẻ". Ta giả thiết rằng khóa này đã được truyền tới cả hai trạm suốt kênh bảo mật nào đó trong môi trường WM. Trong các thi hành tiêu biểu, chứng thực này được thiết lập thủ công trên trạm khách hàng và AP. Các khung thứ nhất và thứ tư của chứng thực khóa chia sẻ tương tự như các khung có trong chứng thực hệ thống mở. Còn các khung thứ hai và khung thứ ba khác nhau, trạm xác nhận nhận một gói văn bản yêu cầu (được tạo ra khi sử dụng bộ tạo số giả ngẫu nhiên giải thuật WEP (PRNG)) từ AP, mật mã hóa nó sử dụng khóa chia sẻ, và gửi nó trở lại cho AP. Sau khi giải mã, nếu văn bản yêu cầu phù hợp, thì chứng thực một chiều thành công. Để chứng thực hai phía, quá trình trên được lặp lại ở phía đối diện. Cơ sở này làm cho hầu hết các tấn công vào

CuuDuongThanCong.com

mạng WLAN chuẩn IEEE 802.11b chỉ cần dựa vào việc bắt dạng mật mã hóa của một đáp ứng biết trước, nên dạng chứng thực này là một lựa chọn kém hiệu quả. Nó cho phép các hacker lấy thông tin để đánh đổ mật mã hóa WEP và đó cũng là lý do tại sao chứng thực khóa chia sẻ không bao giờ khuyến nghị.

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



Chứng thực khóa chia sẻ..

4. Mã hóa WEP

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

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

Giải thuật WEP thực chất là giải thuật giải mã hóa RC4 của Hiệp hội Bảo mật Dữ liệu RSA. Nó được xem như là một giải thuật đối xứng vì sử dụng cùng khóa cho mật mã hóa và giải mật mã UDP (Protocol Data Unit) văn bản gốc. Mỗi khi

CuuDuongThanCong.com

truyền, văn bản gốc XOR theo bit với một luồng khóa (*keystream*) giả ngẫu nhiên để tạo ra một văn bản được mật mã. Quá trình giải mật mã ngược lại.

Giải thuật hoạt động như sau:

- Ta giả thiết rằng khóa bí mật đã được phân phối tới cả trạm phát lẫn trạm thu theo nghĩa bảo mật nào đó.
- Tại trạm phát, khóa bí mật 40 bit được móc nối với một Vectơ Khởi tạo (IV) 24 bit để tạo ra một *seed* (hạt giống) cho đầu vào bộ PRNG WEP.
- Seed được qua bộ PRNG để tạo ra một luồng khóa (*keystream*) là các octet giả ngẫu nhiên.
- Sau đó PDU văn bản gốc được XOR với keystream giả ngẫu nhiên để tạo ra PDU văn bản mật mã hóa.
- PDU văn bản mật mã hóa này sau đó được móc nối với IV và được truyền trên môi trường WM.
- Trạm thu đọc IV và móc nối nó với khóa bí mật, tạo ra seed mà nó chuyển cho bộ PRNG.
- Bộ PRNG của máy thu cần phải tạo ra keystream đồng nhất được sử dụng bởi trạm phát, như vậy khi nào được XOR với văn bản mật mã hóa, PDU văn bản gốc được tạo ra.

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

CuuDuongThanCong.com

5. Trạng thái bảo mật mạng WLAN

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

- Các lớp liên kết đề xuất không được bảo mật.
- Sử dụng các cơ chế bảo mật cao hơn như IPsec và SSH, thay cho WEP.
- Xem tất cả các hệ thống được nối qua chuẩn IEEE 802.11 như là phần ngoài. Đặt tất cả các điểm truy cập bên ngoài bức tường lửa.

Giả thiết rằng bất cứ ai trong phạm vi vật lý đều có thể liên lạc trên mạng như một người dùng hợp lệ. Nhớ rằng một đối thủ cạnh tranh có thể dùng một anten tinh vi với nhiều vùng nhận sóng rộng hơn có thể được tìm thấy trên một card PC chuẩn IEEE 802.11 tiêu biểu

II. Các ví dụ kiến trúc bảo mật mạng WLAN

1. Chứng thực bằng địa chỉ MAC – MAC Address

Trước hết chúng ta cũng nhắc lại một chút về khái niệm địa chỉ MAC. Địa chỉ MAC – Media Access Control là địa chỉ vật lý của thiết bị được in nhập vào Card mạng khi chế tạo, mỗi Card mạng có một giá trị địa chỉ duy nhất. Địa chỉ này gồm 48 bit chia thành 6 byte, 3 byte đầu để xác định nhà sản xuất, ví dụ như:

00-40-96 : Cisco

00-00-86 : 3COM

00-02-2D : Agere Communications (ORiNOCO)

00-10-E7 : Breezecom

00-E0-03 : Nokia Wireless

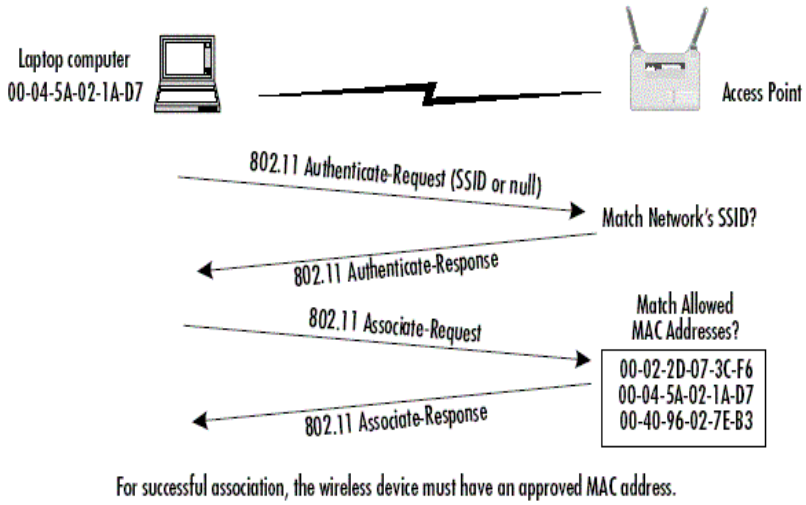
00-04-5A : Linksys

3 byte còn lại là số thứ tự, do hãng đặt cho thiết bị

Địa chỉ MAC nằm ở lớp 2 (lớp Datalink của mô hình OSI)

CuuDuongThanCong.com

Khi Client gửi yêu cầu chứng thực cho AP, AP sẽ lấy giá trị địa chỉ MAC của Client đó, so sánh với bảng các địa chỉ MAC được phép kết nối để quyết định xem có cho phép Client chứng thực hay không. Chi tiết quá trình này được biểu diễn ở hình dưới



Mô tả quá trình chứng thực bằng địa chỉ MAC

Nhược điểm

Về nguyên lý thì địa chỉ MAC là do hãng sản xuất quy định ra nhưng nhược điểm của phương pháp này kẻ tấn công lại có thể thay đổi địa chỉ MAC một cách dễ dàng, từ đó có thể chứng thực giả mạo.

- Giả sử người sử dụng bị mất máy tính, kẻ cắp có thể dễ dàng truy cập và tấn công mạng bởi vì chiếc máy tính đó mang địa chỉ MAC được AP cho phép, trong khi đó người mất máy tính mua một chiếc máy tính mới lúc đầu gặp khó khăn vì AP chưa kịp cập nhật địa chỉ MAC của chiếc máy tính đó.

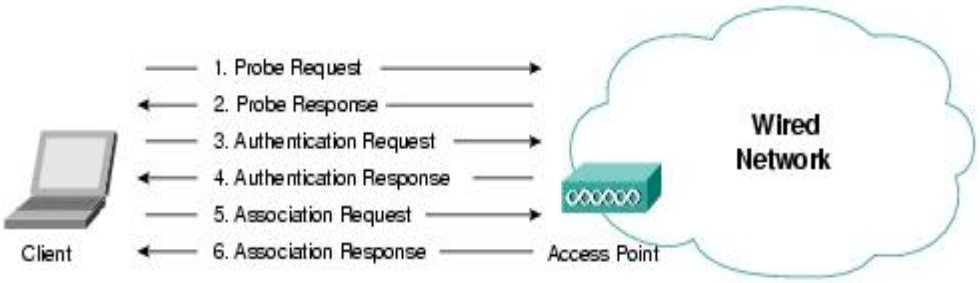
- Một số các Card mạng không dây loại PCMCIA dùng cho chuẩn 802.11 được hỗ trợ khả năng tự thay đổi địa chỉ MAC, như vậy kẻ tấn công chỉ việc thay đổi địa chỉ đó giống địa chỉ của một máy tính nào trong mạng đã được cấp phép là hắn có nhiều cơ hội chứng thực thành công

2. Chứng thực bằng SSID

Chứng thực bằng SSID - System Set Identifier, mã định danh hệ thống, là một phương thức chứng thực đơn giản, nó được áp dụng cho nhiều mô hình mạng nhỏ,

CuuDuongThanCong.com

yêu cầu mức độ bảo mật thấp. Có thể coi SSID như một mật mã hay một chìa khóa, khi máy tính mới được phép gia nhập mạng nó sẽ được cấp SSID, khi gia nhập, nó gửi giá trị SSID này lên AP, lúc này AP sẽ kiểm tra xem SSID mà máy tính đó gửi lên có đúng với mình quy định không, nếu đúng thì coi như đã chứng thực được và AP sẽ cho phép thực hiện các kết nối.



Mô tả quá trình chứng thực bằng SSID

Các bước kết nối khi sử dụng SSID:

1. Client phát yêu cầu Thăm dò trên tất cả các kênh

2. AP nào nhận được yêu cầu Thăm dò trên sẽ trả lời lại (có thể có nhiều AP cùng trả lời)

3. Client chọn AP nào phù hợp để gửi yêu cầu xin Chứng thực

4. AP gửi trả lời yêu cầu Chứng thực

5. Nếu thỏa mãn các yêu cầu chứng thực, Client sẽ gửi yêu cầu Liên kết đến AP

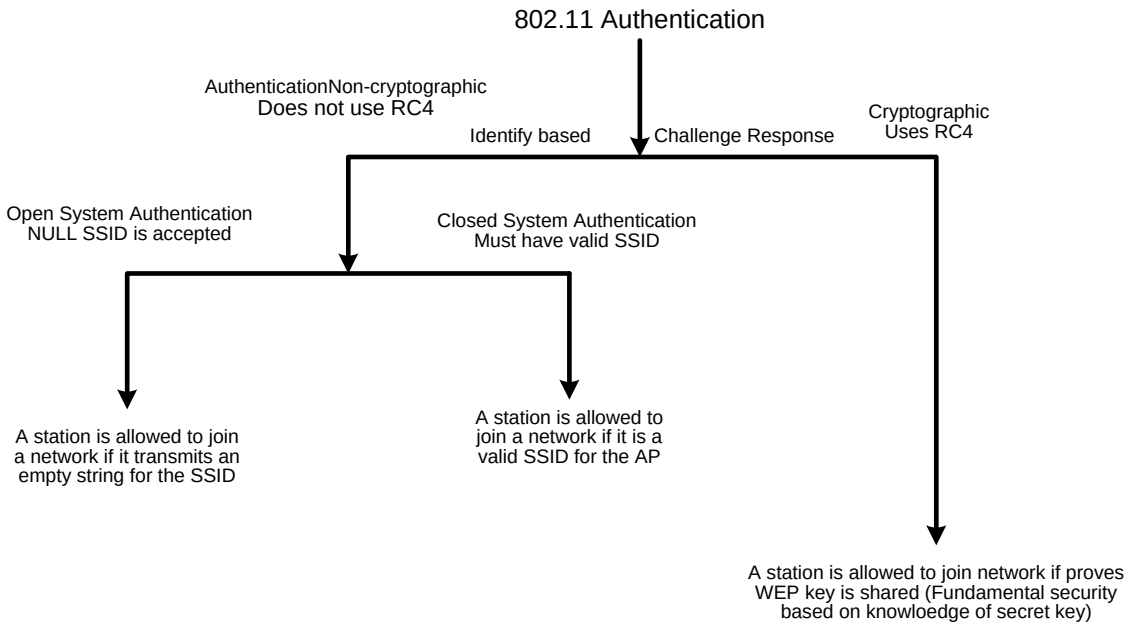
6. AP gửi trả lời yêu cầu Liên kết

7. Quá trình Chứng thực thành công, 2 bên bắt đầu trao đổi dữ liệu

SSID là một chuỗi dài 32 bit. Trong một số tình huống công khai (hay còn gọi là Chứng thực mở - Open System Authentication), khi AP không yêu cầu chứng thực chuỗi SSID này sẽ là một chuỗi trắng (null). Trong một số tình huống công khai khác, AP có giá trị SSID và nó phát BroadCast cho toàn mạng. Còn khi giữ bí mật (hay còn gọi là Chứng thực đóng - Close System Authentication), chỉ khi có SSID đúng thì máy tính mới tham gia vào mạng được. Giá trị SSID cũng có thể thay đổi thường xuyên hay bất thường, lúc đó phải thông báo đến tất cả các máy

CuuDuongThanCong.com

tính được cấp phép và đang sử dụng SSID cũ, nhưng trong quá trình trao đổi SSID giữa Client và AP thì mã này để ở nguyên dạng, không mã hóa (clear text).



Mô hình phương pháp chứng thực SSID của 802.11.

cuu duong than cong . com

Nhược điểm

Sử dụng SSID là khá đơn giản nhưng nó cũng có nhiều nhược điểm, cụ thể :

- Các hãng thường có mã SSID ngầm định sẵn (default SSID), nếu người sử dụng không thay đổi thì các thiết bị AP giữ nguyên giá trị SSID này, kẻ tấn công lợi dụng sự lơi lỏng đó, để dò ra SSID. Các SSID ngầm định của AP của một số hãng như sau:

Manufacturer	**Default SSID**
3Com	101, comcomcom
Addtron	WLAN
Cisco	Tsunami, WaveLAN Network
Compaq	Compaq
Dlink	WLAN
Intel	101, 195, xlan, intel
Linksys	Linksys, wireless
Lucent/Cabletron	RoamAbout

CuuDuongThanCong.com

NetGear	Wireless
SMC	WLAN
Symbol	101
Teletronics	any
Zcomax	any, mello, Test
Zyxel	Wireless
Others	Wireless

- Nhiều mạng sử dụng mã SSID rỗng (null), như vậy đương nhiên mọi máy tính có thể truy nhập vào mạng được, kể cả máy tính của kẻ tấn công

- AP bật chế độ Broadcast giá SSID, như vậy giá trị SSID này sẽ được gửi đi khắp nơi trong vùng phủ sóng, tạo điều kiện cho kẻ tấn công lấy được mã này

- Kiểu chứng thực dùng SSID là đơn giản, ít bước. Vì vậy nếu kẻ tấn công thực hiện việc bắt rất nhiều gói tin trên mạng để phân tích theo các thuật toán quét giá trị như kiểu Brute Force thì sẽ có nhiều khả năng dò ra được mã SSID mà AP đang sử dụng

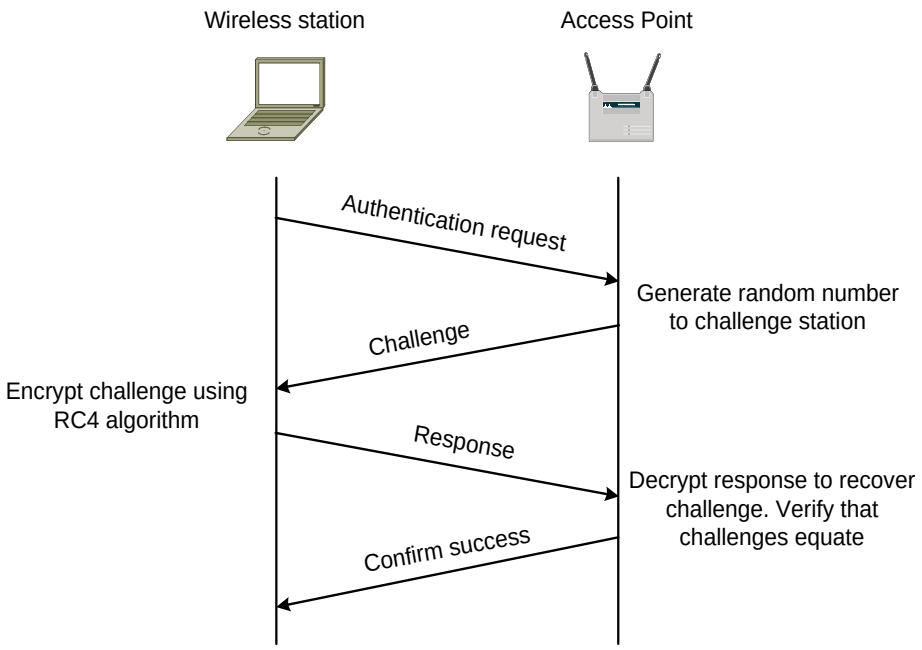
- Tất cả mạng WLAN dùng chung một SSID, chỉ cần một máy tính trong mạng để lộ thì sẽ ảnh hưởng an ninh toàn mạng. Khi AP muốn đổi giá trị SSID thì phải thông báo cho tất cả các máy tính trong mạng

3. Phương thức chứng thực và mã hóa WEP

Phương thức chứng thực của WEP cũng phải qua các bước trao đổi giữa Client và AP, nhưng nó có thêm mã hóa và phức tạp hơn

cuu duong than cong . com

CuuDuongThanCong.com



Mô tả quá trình chứng thực giữa Client và AP

Các bước cụ thể như sau:

Bước 1: Client gửi đến AP yêu cầu xin chứng thực

Bước 2: AP sẽ tạo ra một chuỗi mời kết nối (challenge text) ngẫu nhiên gửi đến Client

Bước 3: Client nhận được chuỗi này này sẽ mã hóa chuỗi bằng thuật toán RC4 theo mã khóa mà Client được cấp, sau đó Client gửi lại cho AP chuỗi đã mã hóa

Bước 4: AP sau khi nhận được chuỗi đã mã hóa của Client, nó sẽ giải mã lại bằng thuật toán RC4 theo mã khóa đã cấp cho Client, nếu kết quả giống với chuỗi ban đầu mà nó gửi cho Client thì có nghĩa là Client đã có mã khóa đúng và AP sẽ chấp nhận quá trình chứng thực của Client và cho phép thực hiện kết nối

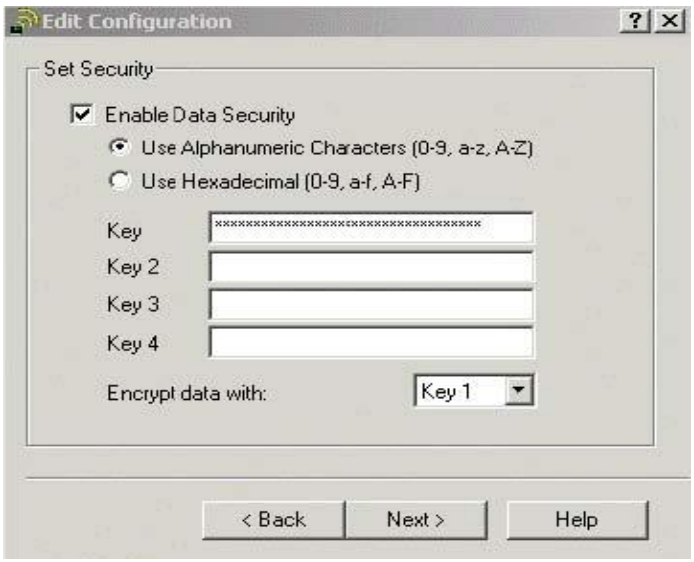
Phương thức mã hóa

WEP là một thuật toán mã hóa đối xứng có nghĩa là quá trình mã hóa và giải mã đều dùng một là Khóa dùng chung - Share key, khóa này AP sử dụng và Client được cấp. Chúng ta làm quen với một số khái niệm sau:

***Khóa dùng chung – Share key*:** Đây là mã khóa mà AP và Client cùng biết và sử dụng cho việc mã hóa và giải mã dữ liệu. Khóa này có 2 loại khác nhau về độ dài

CuuDuongThanCong.com

là 40 bit và 104 bit. Một AP có thể sử dụng tới 4 Khóa dùng chung khác nhau, tức là nó có làm việc với 4 nhóm các Client kết nối tới nó.



Cài đặt mã khóa dùng chung cho WEP

Vector khởi tạo IV-Initialization Vector: Đây là một chuỗi dài 24 bit, được tạo ra một cách ngẫu nhiên và với gói tin mới truyền đi, chuỗi IV lại thay đổi một lần. Có nghĩa là các gói tin truyền đi liền nhau sẽ có các giá trị IV thay đổi khác nhau. Vì thế người ta còn gọi nó là bộ sinh mã giả ngẫu nhiên PRNG – Pseudo Random Number Generator. Mã này sẽ được truyền cho bên nhận tin (cùng với bản tin đã mã hóa), bên nhận sẽ dùng giá trị IV nhận được cho việc giải mã.

RC4: chữ RC4 xuất phát từ chữ Ron's Code lấy từ tên người đã nghĩ ra là Ron Rivest, thành viên của tổ chức bảo mật RSA. Đây là loại mã dạng chuỗi các ký tự được tạo ra liên tục (còn gọi là luồng dữ liệu). Độ dài của RC4 chính bằng tổng độ dài của Khóa dùng chung và mã IV. Mã RC4 có 2 loại khác nhau về độ dài từ mã là loại 64 bit (ứng với Khóa dùng chung 40 bit) và 128 bit (ứng với Khóa dùng chung dài 104 bit)

CuuDuongThanCong.com

Chương 5: Sử dụng Radius cho quá trình xác thực trong WLAN

Mạng WLAN bản thân nó là không bảo mật, tuy nhiên đối với mạng có dây nếu bạn không có 1 sự phòng ngừa hay cấu hình bảo vệ gì thì nó cũng chẳng bảo mật gì. Điểm mấu chốt để tạo ra 1 mạng WLAN bảo mật là phải triển khai các phương pháp bảo mật thiết yếu cho WLAN để giúp cho hệ thống mạng của mình được an toàn hơn.

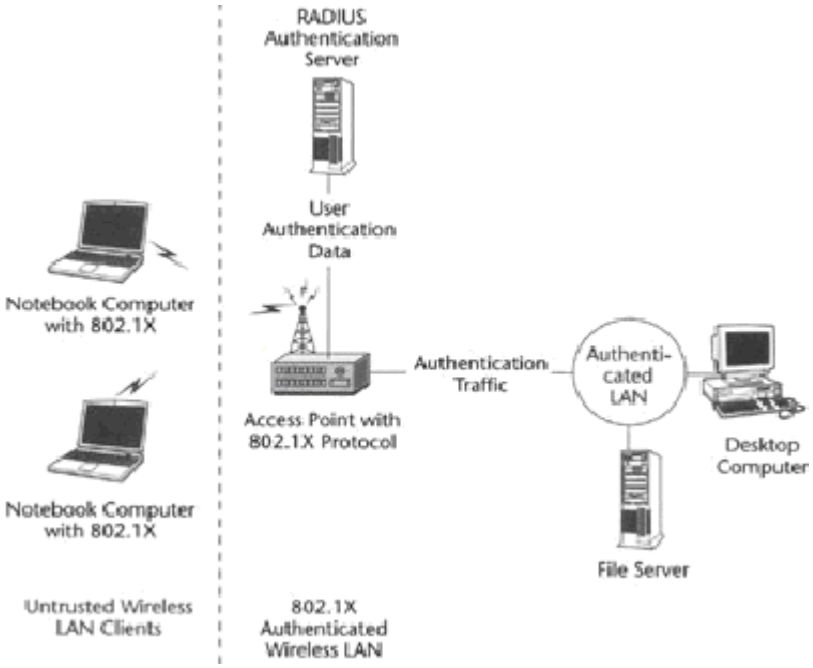
I. RADIUS SERVER

1. Định nghĩa

Việc chứng thực của 802.1x được thực hiện trên một server riêng, server này sẽ quản lý các thông tin để xác thực người sử dụng như tên đăng nhập (username), mật khẩu (password), mã số thẻ, dấu vân tay, vv.. Khi người dùng gửi yêu cầu chứng thực, server này sẽ tra cứu dữ liệu để xem người dùng này có hợp lệ không, được cấp quyền truy cập đến mức nào, vv.. Server này được gọi là RADIUS (Remote Authentication Dial−in User Service) Server – Máy chủ cung cấp dịch vụ chứng thực người dùng từ xa thông qua phương thức quay số. Phương thức quay số xuất hiện từ ban đầu với mục đích là thực hiện qua đường điện thoại, ngày nay không chỉ thực hiện qua quay số mà còn có thể thực hiện trên những đường truyền khác nhưng người ta vẫn giữ tên RADIUS như xưa.

cuu duong than cong . com

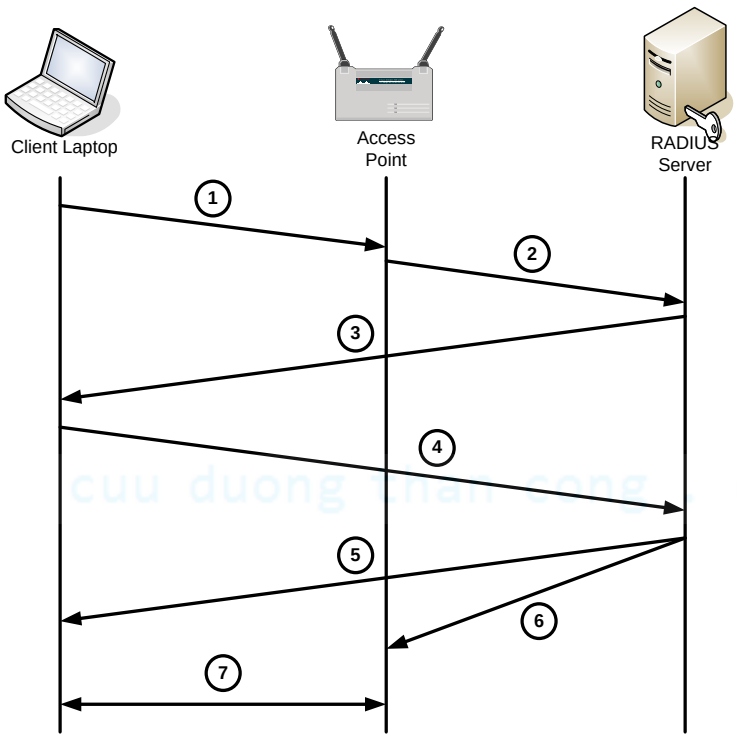
CuuDuongThanCong.com



Mô hình chứng thực sử dụng RADIUS Server

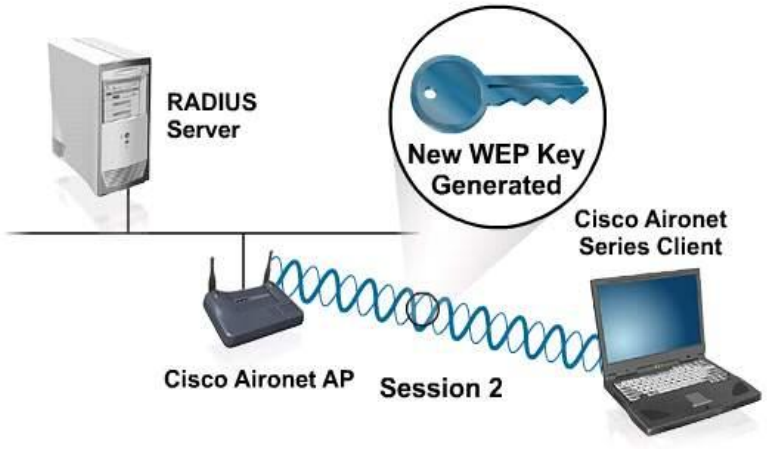
Các quá trình liên kết và xác thực được tiến hành như mô tả trong hình trên, và thực hiện theo các bước sau:

cuu duong than cong . com



cuu duong than cong . com

CuuDuongThanCong.com



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

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

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

4. Client gửi user/password đến RADIUS Server

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

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

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

Để nâng cao tính bảo mật, RADIUS Server sẽ tạo ra các khóa dùng chung khác nhau cho các máy khác nhau trong các phiên làm việc (session) khác nhau, thậm chí là còn có cơ chế thay đổi mã khóa đó thường xuyên theo định kỳ. Khái niệm khóa dùng chung lúc này không phải để chỉ việc dùng chung của các máy tính Client mà để chỉ việc dùng chung giữa Client và AP.

2. Các phương thức triển khai

Bảo mật trong Wireless là một vấn đề được rất nhiều người quan tâm hiện nay. Các phương pháp chứng thực gồm có (Wep Key, WPA. Radius). Tuy nhiên với một doanh nghiệp mà việc bảo đảm an toàn cho các kết nối mạng ko dây luôn được ưu tiên đặt lên hàng đầu, thì họ sẽ chọn phương thức chứng thực bằng Radius. Radius Server là một server chứng thực tập trung nó thông qua AD để bắt người

CuuDuongThanCong.com

dùng, khi kết nối vào mạng wireless thì phải xác nhận bằng user name và pass.Việc chứng thực bằng Radius sẽ đảm bảo mức độ bảo mật cao hơn so với Wepkey và WPA. Chúng ta cần quan tâm đến việc triển khai các tuỳ chọn cho các giải pháp sử dụng chuẩn 802.1X :

- Sử dụng Microsoft's RADIUS Server : một máy chủ chạy hệ điều hành Microsoft Windows Server 2000/2003 với việc sử dụng Microsoft's Internet Authentication Service (IAS) với Microsoft Active Directory . IAS cần thiết các nhà quản trị hay các user phải làm việc trên môi trường Windows. Và nó cũng là một trong những tính năng cao cấp của Microsoft Wireless Provisioning Service.

-Sử dụng giải pháp phần mềm mã nguồn mở như FreeRadius http://www.freeradius.org với khả năng hỗ trợ cho chuẩn 802.1X các máy chủ chạy hệ điều hành mã nguồn mở như Linux, Free or OpenBSD, OSF/Unix đều có thể sử dụng làm RADIUS Server

-Mua một Commercial RADIUS Server: Trong trường hợp phải sử dụng một giải pháp chuyên nghiệp cần hỗ trợ đầy đủ toàn bộ các tính năng cũng như khả năng an toàn, và độ ổn định bạn có thể mua các bản thương mại từ các nhà sản xuất khác, với tính năng hỗ trợ 802.1X và là một RADIUS Server chuyên nghiệp như :

+ Cisco Secure Access Control Server

+ Funk Odyssey Server

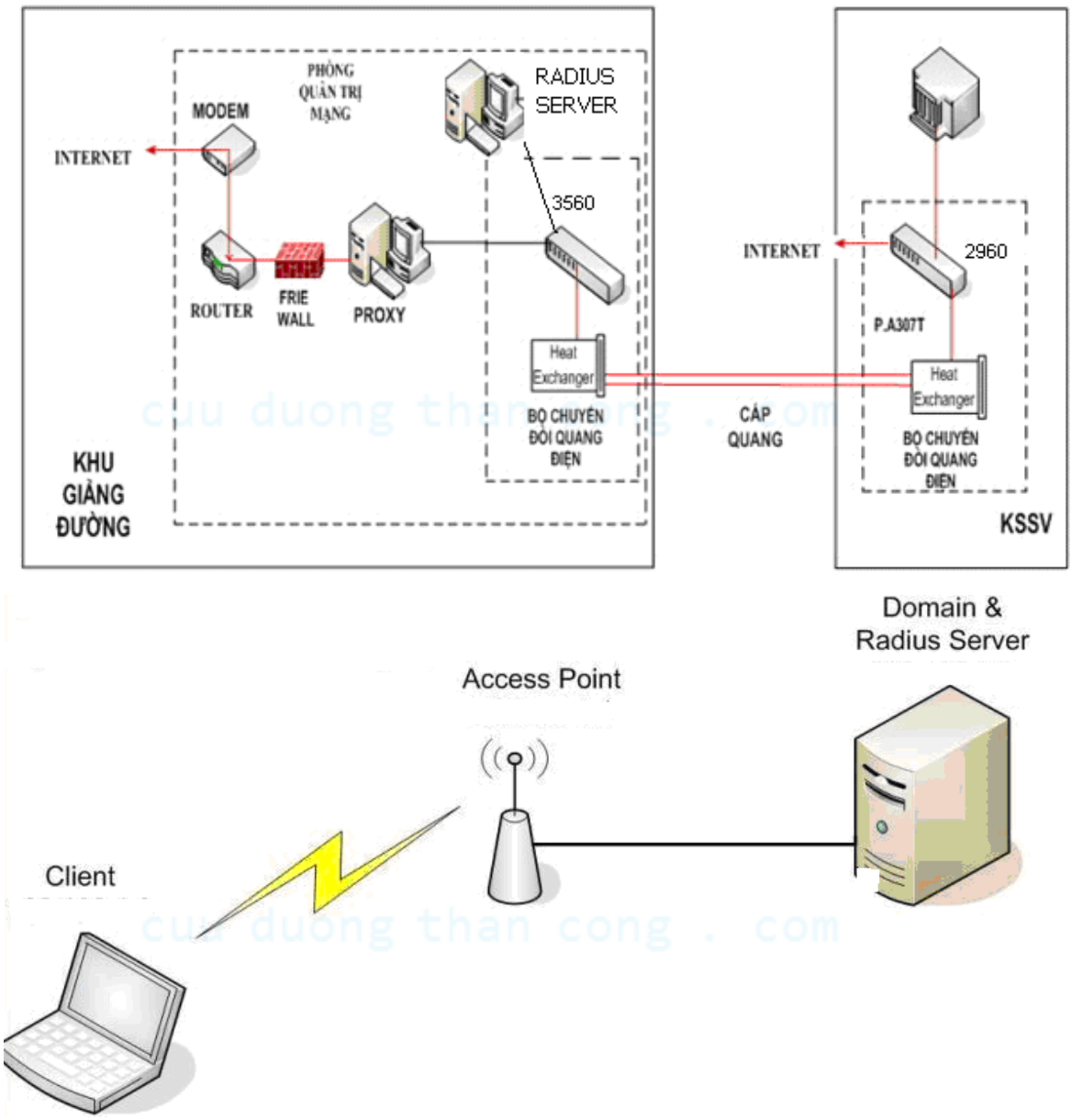
cuu duong than cong . com

CuuDuongThanCong.com

II. GIẢI PHÁP XÂY DỰNG RADIUS SERVER CHO MẠNG KHÔNG DÂY TRƯỜNG ĐHDL HP

Theo Phòng quản trị mạng trong tương lai trường có thể áp dụng mô hình quản lý trên Domain controller nên em chọn phương án sử dụng Microsoft Radius

1. Khảo sát và mô hình thiết kế mạng



CuuDuongThanCong.com

2. Công cụ và môi trường cài đặt

Sử dụng Microsoft's RADIUS Server : một máy chủ chạy hệ điều hành Microsoft Windows Server 2000/2003 với việc sử dụng Microsoft's Internet Authentication Service (IAS) với Microsoft Active Directory.

3. Thiết bị Thử nghiệm

-Server :

Intel ® Pentium™ Xeon 2,2Ghz Ram 2GB

Window Server 2003 SP1

-Access Point LinkSys WRT54G

-Client Latop Toshiba satellite with Wireless , Window XP SP2

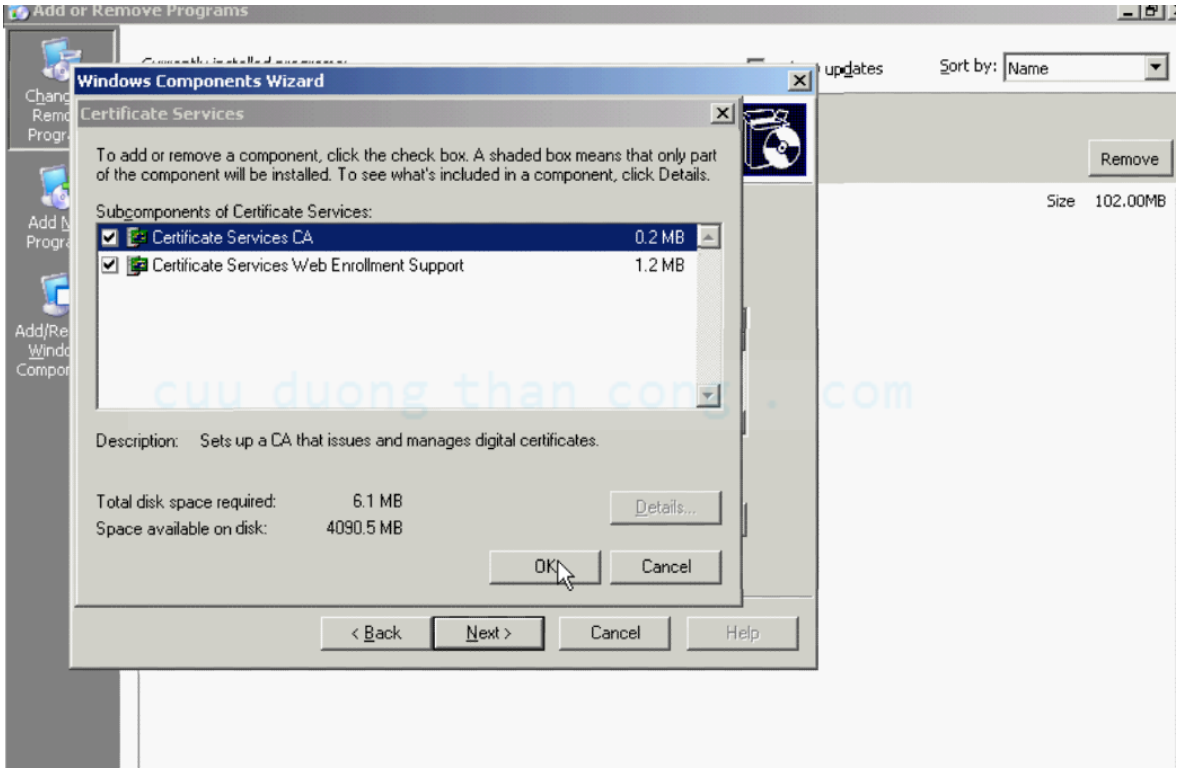
4. Tiến hành cài đặt

cuu duong than cong . com

4.1. Cài đặt trên máy Server

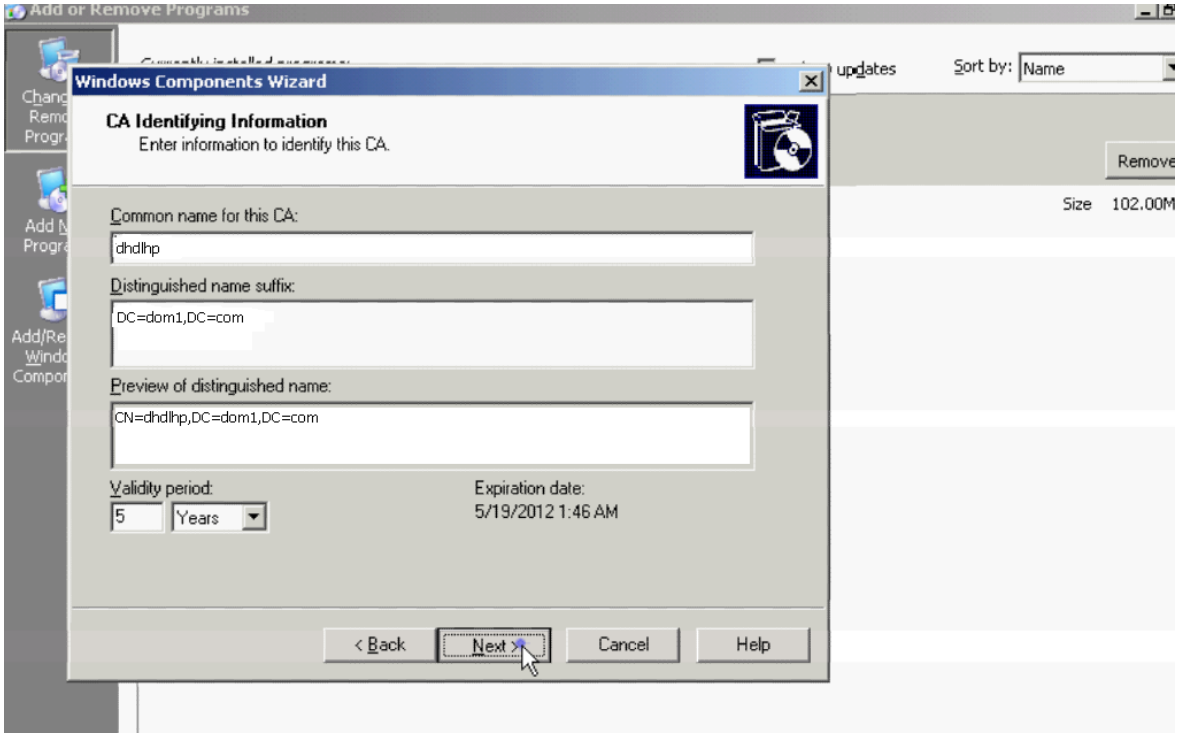
Máy chủ Radius đã lên Domain **Dom1.com** và cài IIS trước có Ip **172.16.3.1**

+ Cài CA (Certificate Service CA)

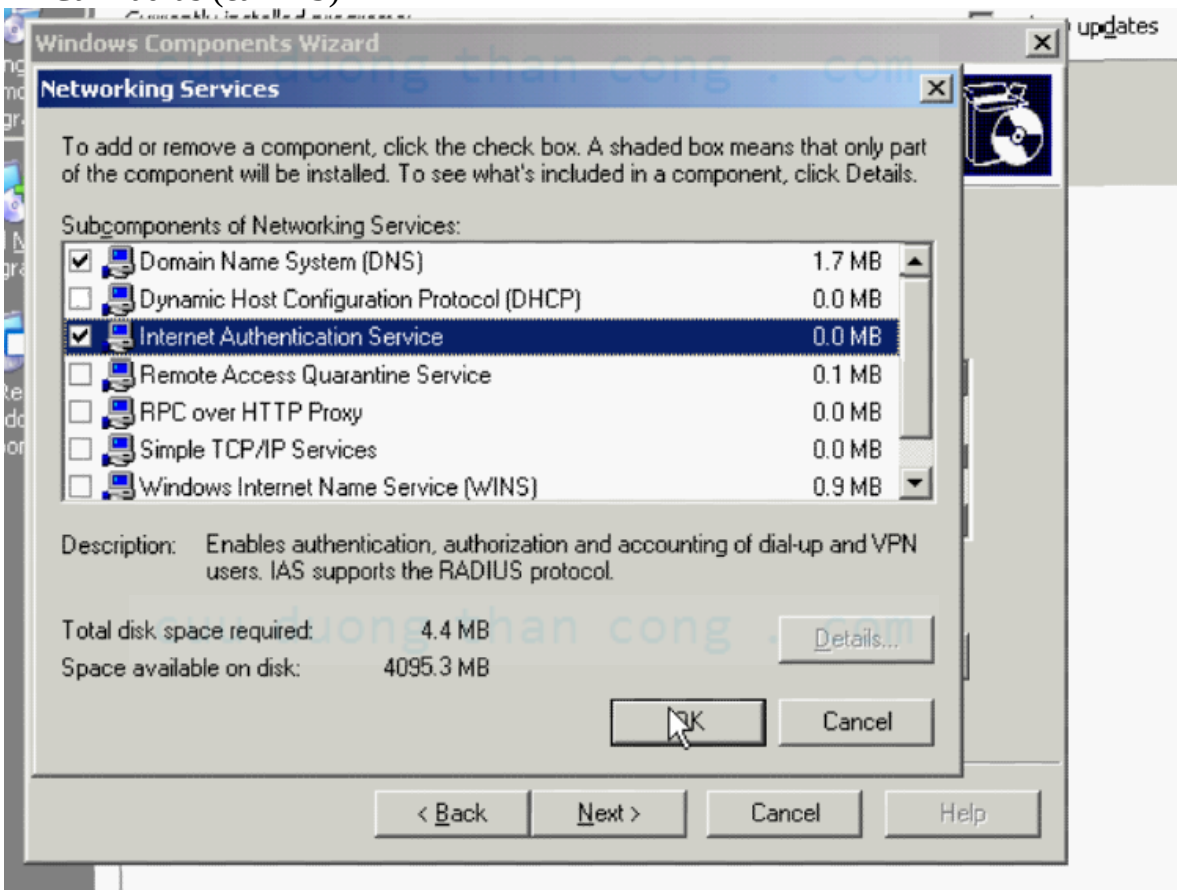


CuuDuongThanCong.com

.

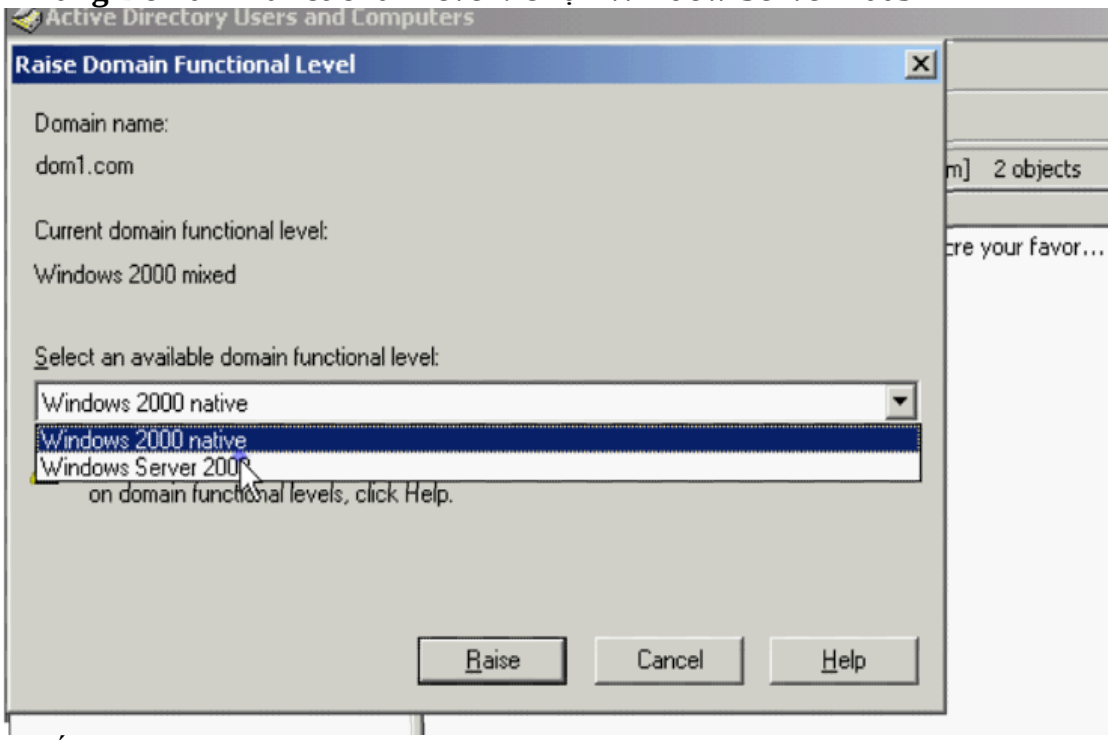


+ Cài Radius (cài IAS)

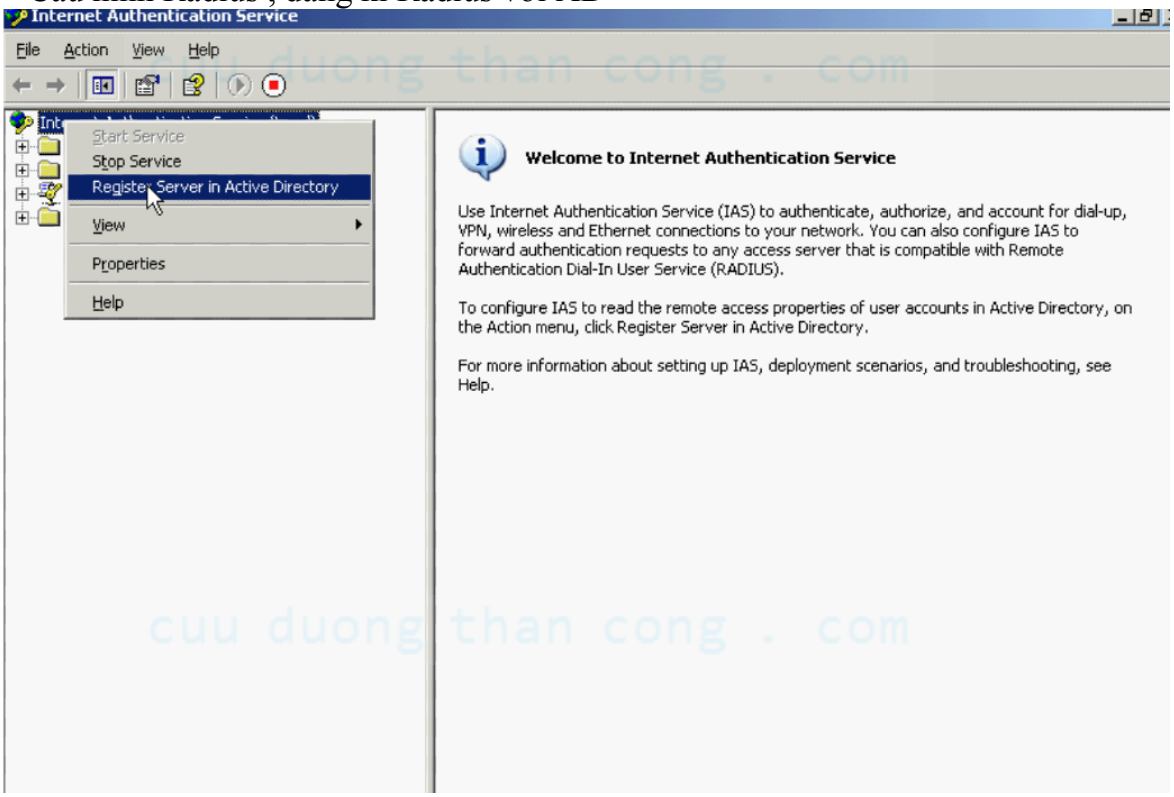


CuuDuongThanCong.com

+ **Nâng Domain Functional Level** : Chọn **Window Server 2003**

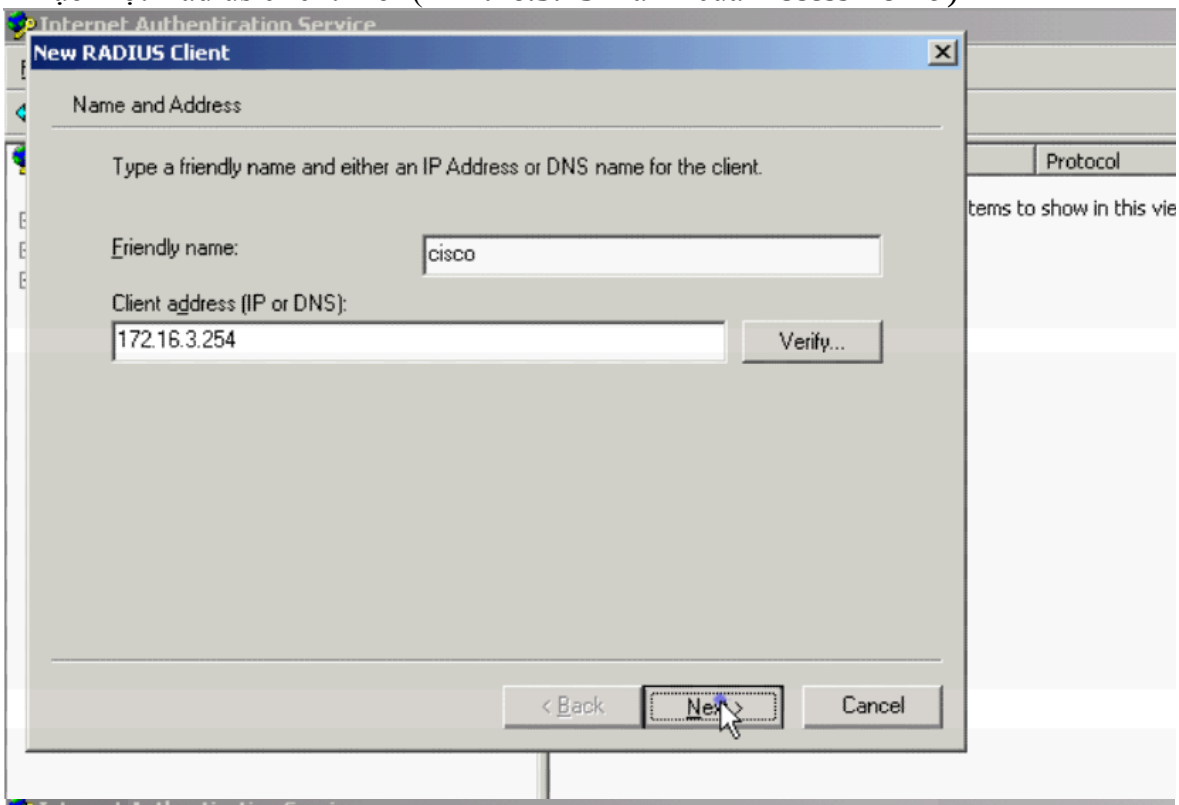


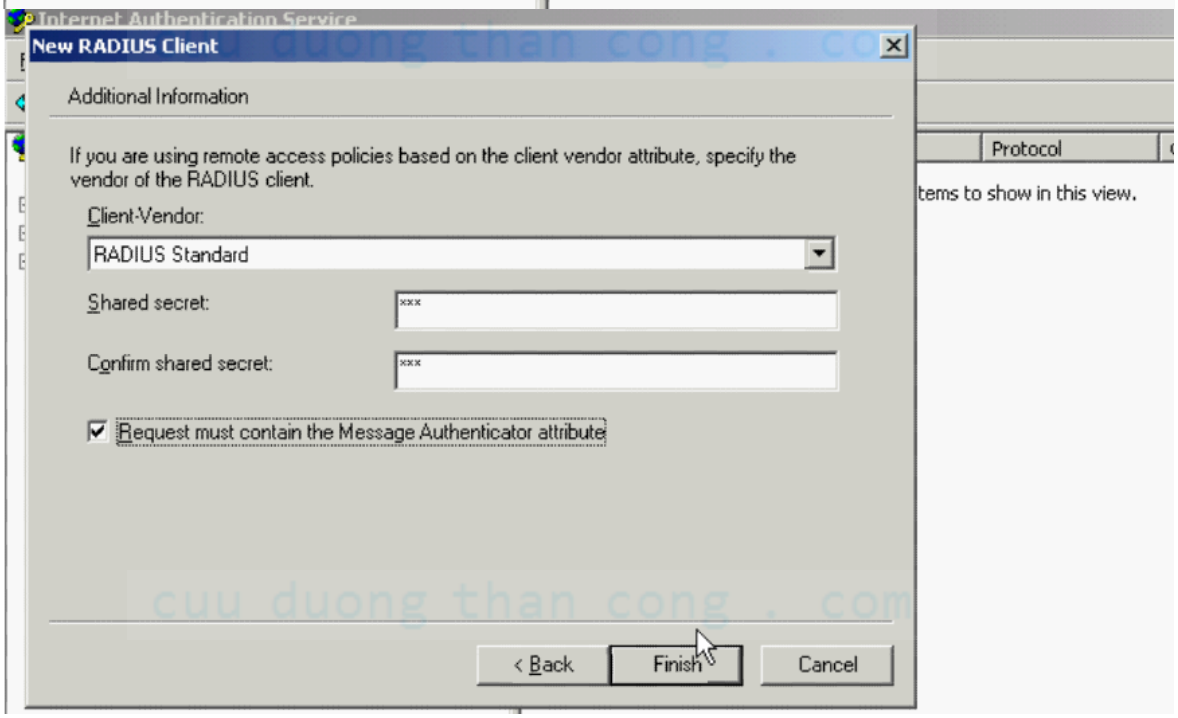
+ Cấu hình Radius , đăng kí Radius với AD



CuuDuongThanCong.com

+ Tạo một Radius client mới (**172.16.3.254** là IP của **Access Point**)



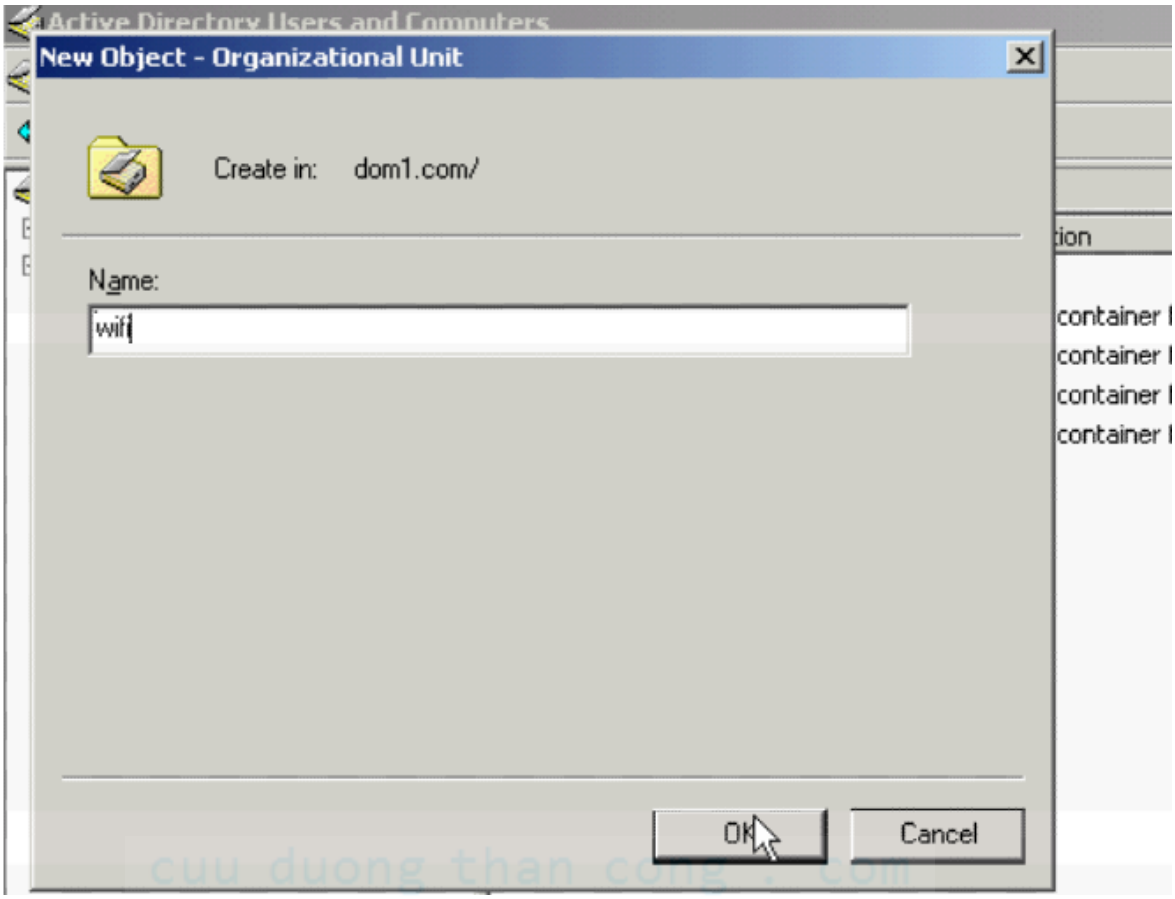


Share secret key ta nhập ở đây là 123

+Tạo user và cấp quyền remote access cho user và computer

Trong cửa sổ AD tạo tạo 1 **new Organizational Unit** là " **Wifi** "trong **dom1.com**

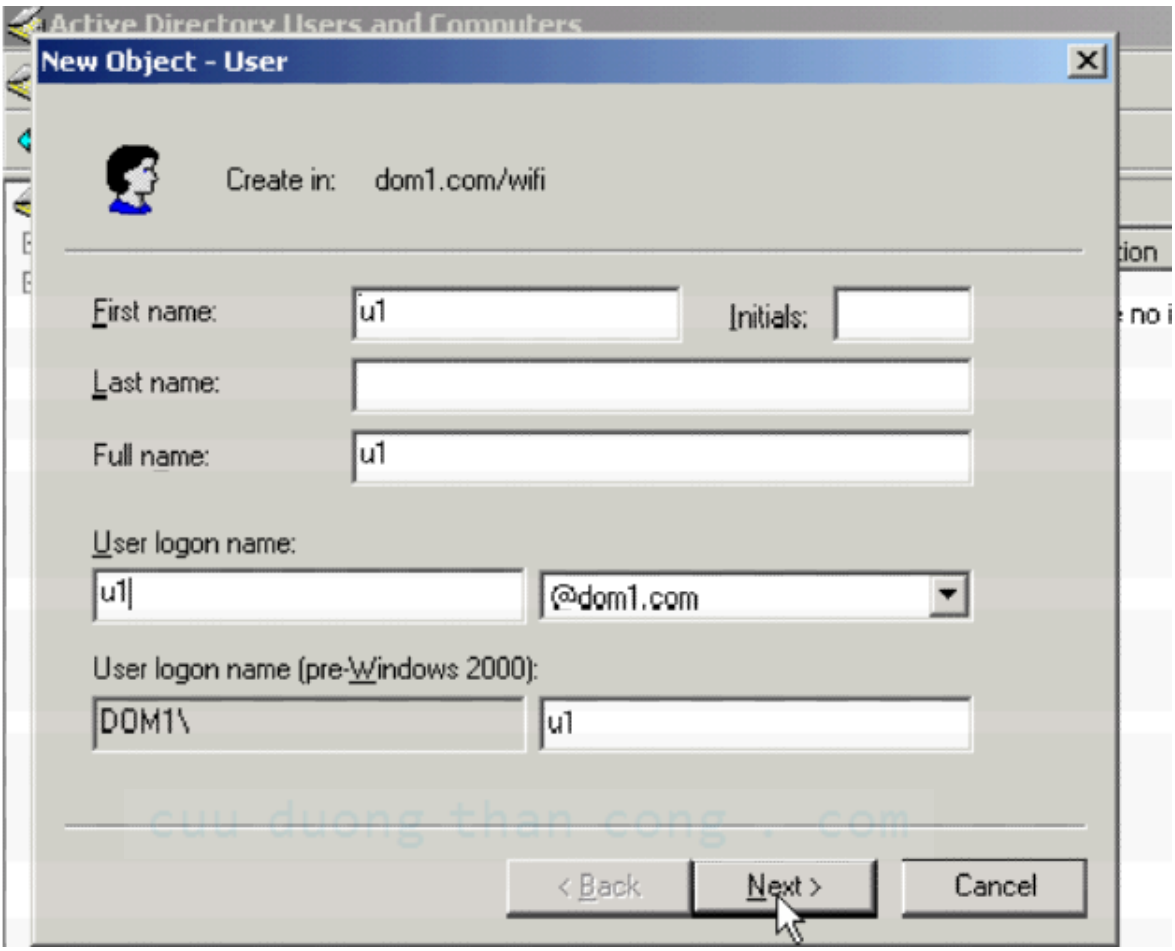
CuuDuongThanCong.com



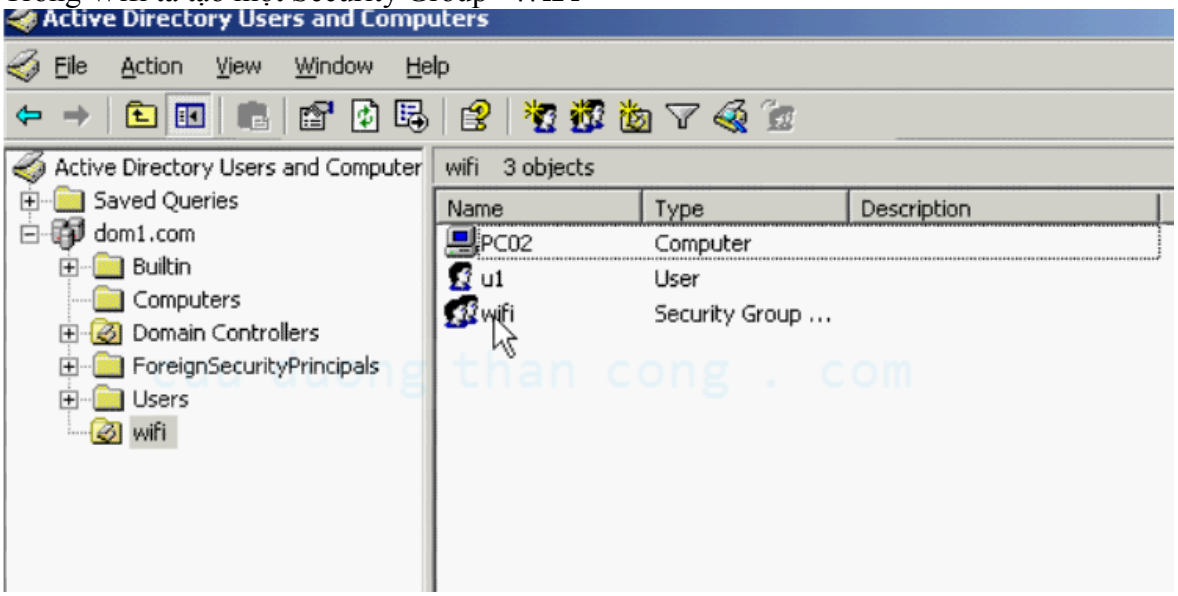
cuu duong than cong . com

CuuDuongThanCong.com

Tạo user trong Wifi vừa tạo

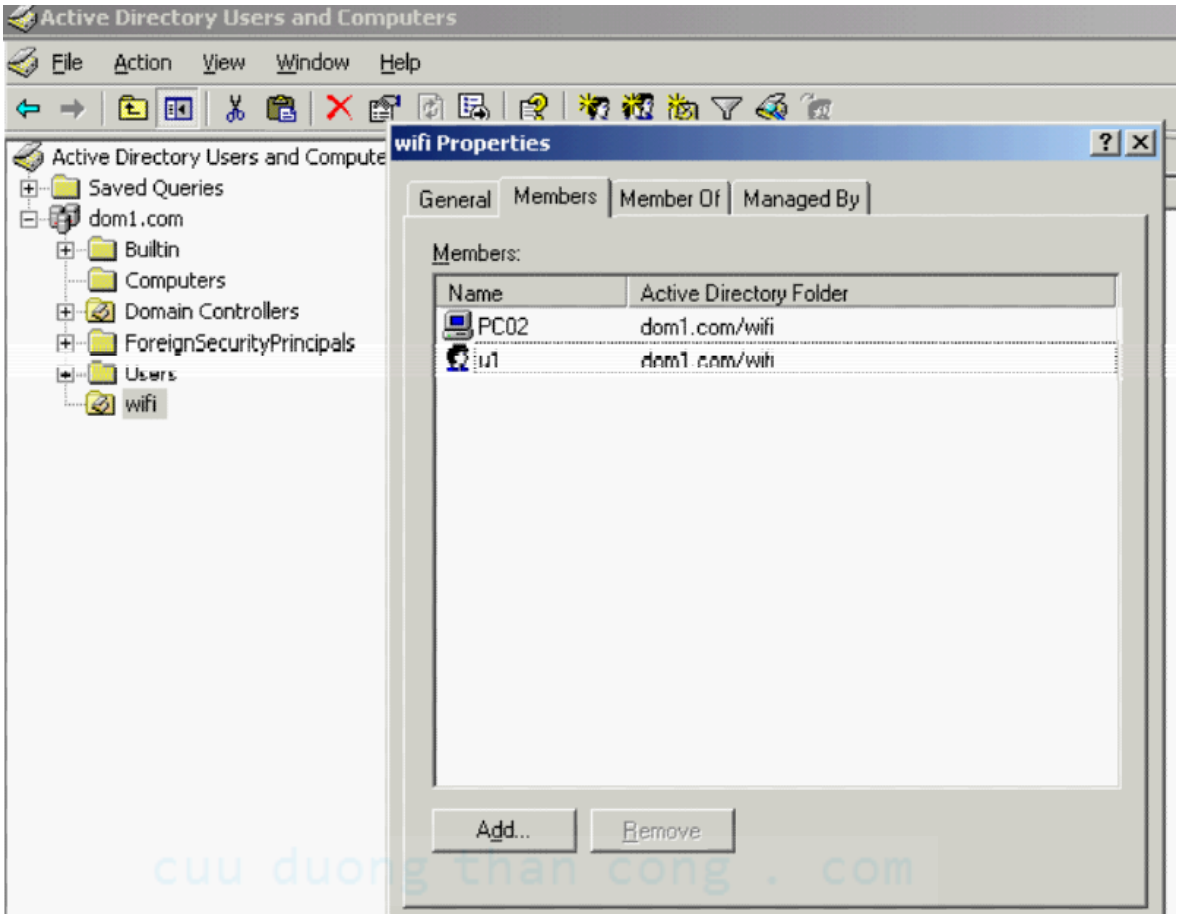


Trong Wifi ta tạo một Security Group "**WiFi**"

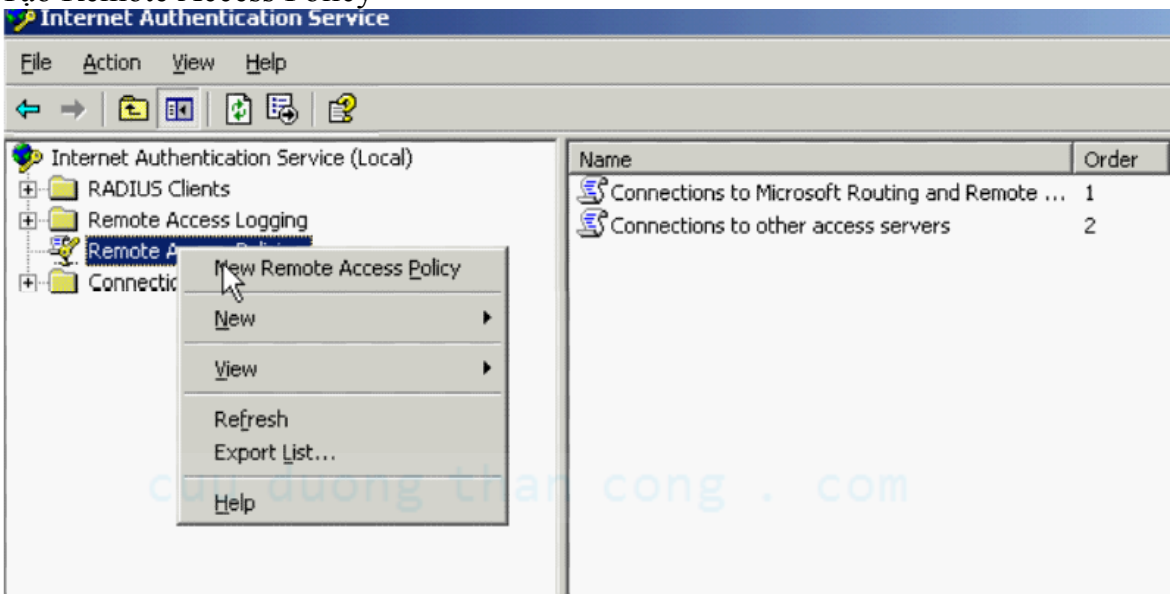


Đưa user vừa tạo và tài khoản Computer vào Group Wifi

CuuDuongThanCong.com

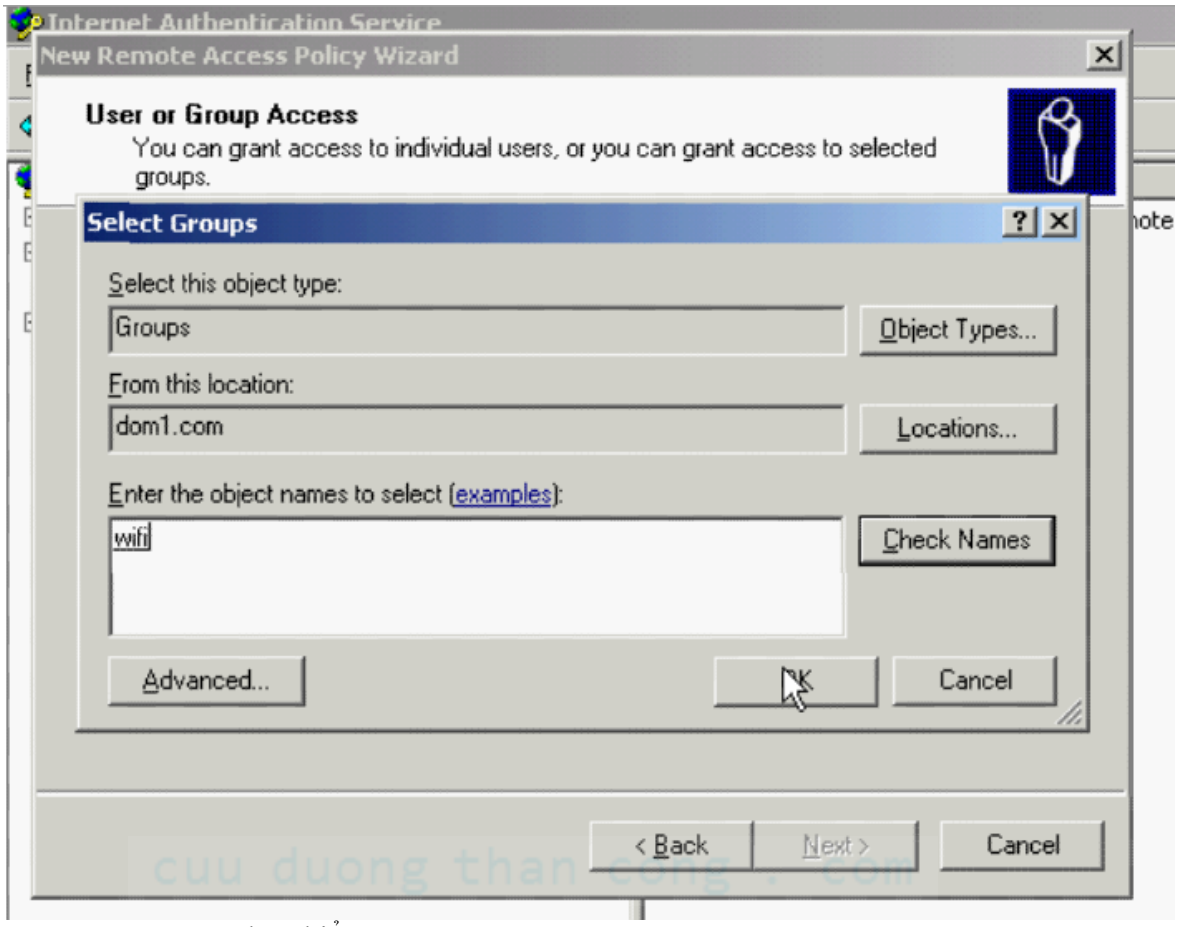


Tạo Remote Access Policy



Ta tạo 1 Policy " **Wifi** " Access method là **Wireless ,** mục Group ra gõ như hình dưới

CuuDuongThanCong.com



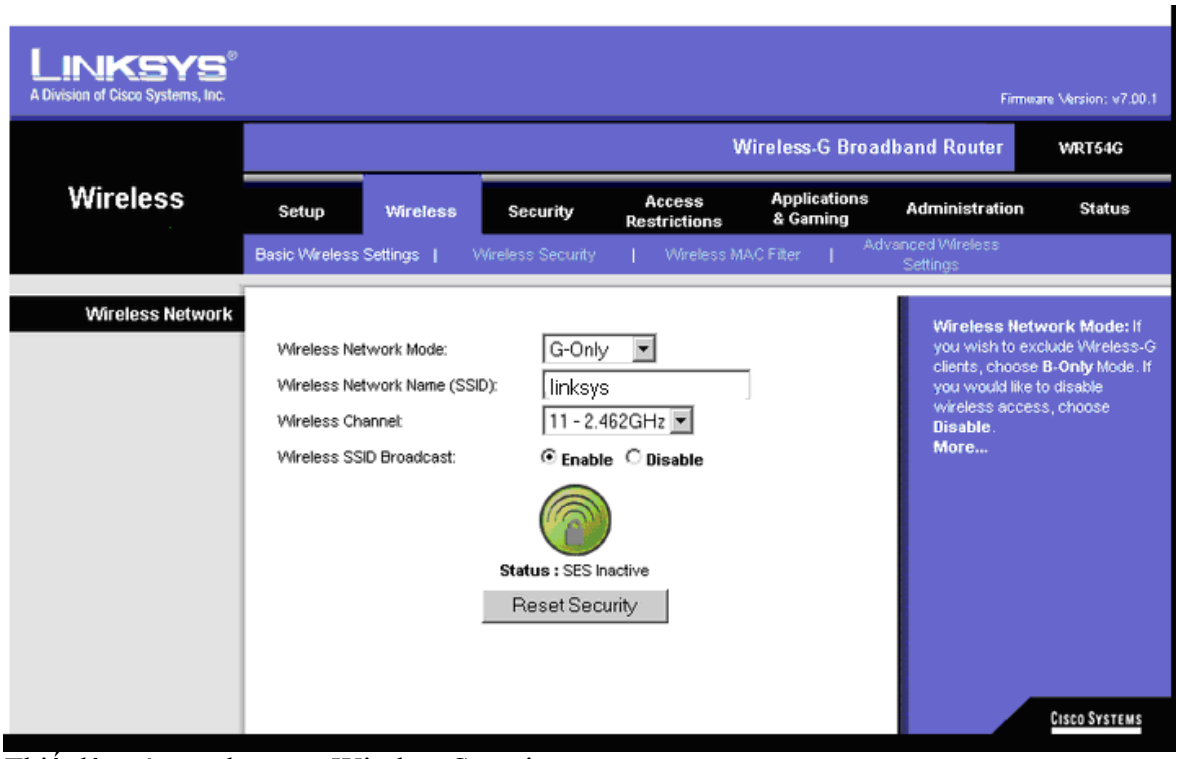
Mục EAP type ta chọn kiểu **Protected EAP (PEAP)**

4.2. Cấu hình trên Accesspoint

Thiết lập SSID

CuuDuongThanCong.com

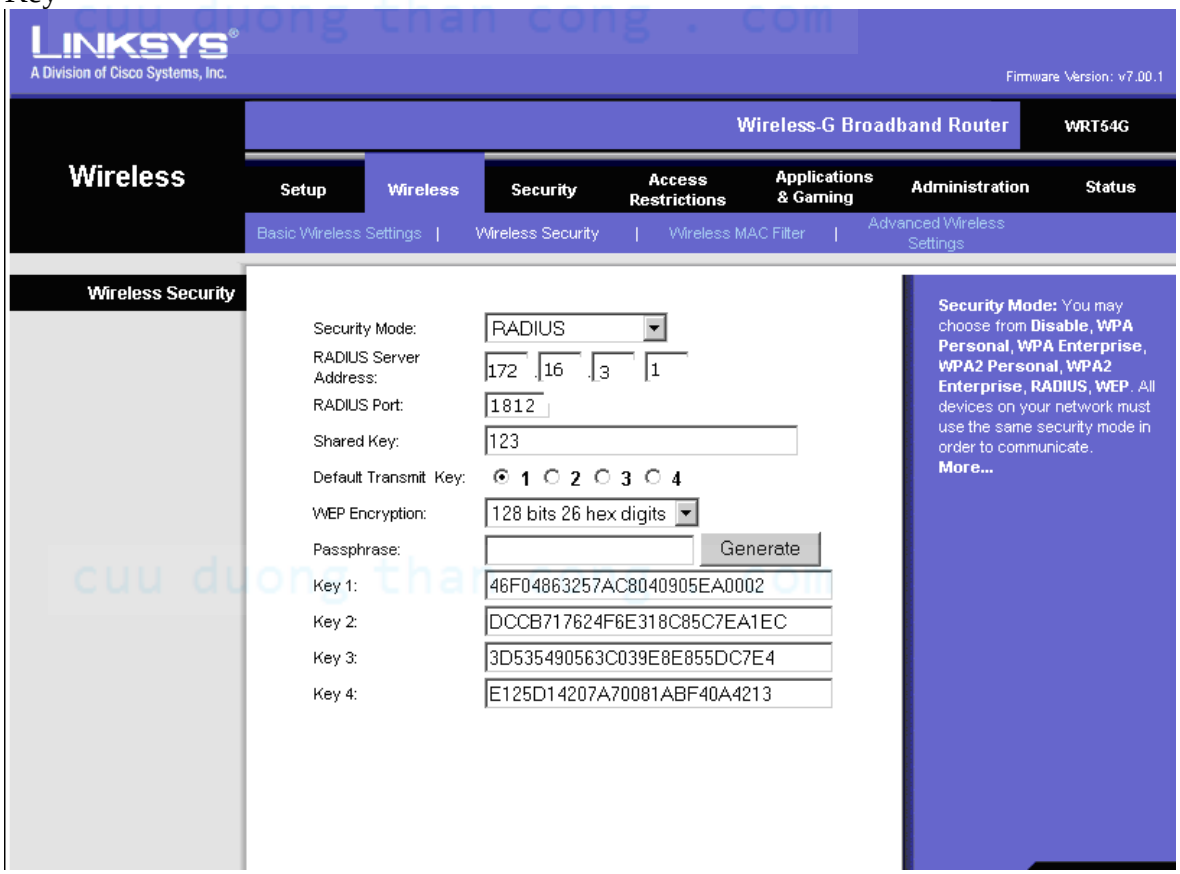
.



Thiết lập các mode trong Wireless Security

Địa chỉ máy RADIUS

Share Key

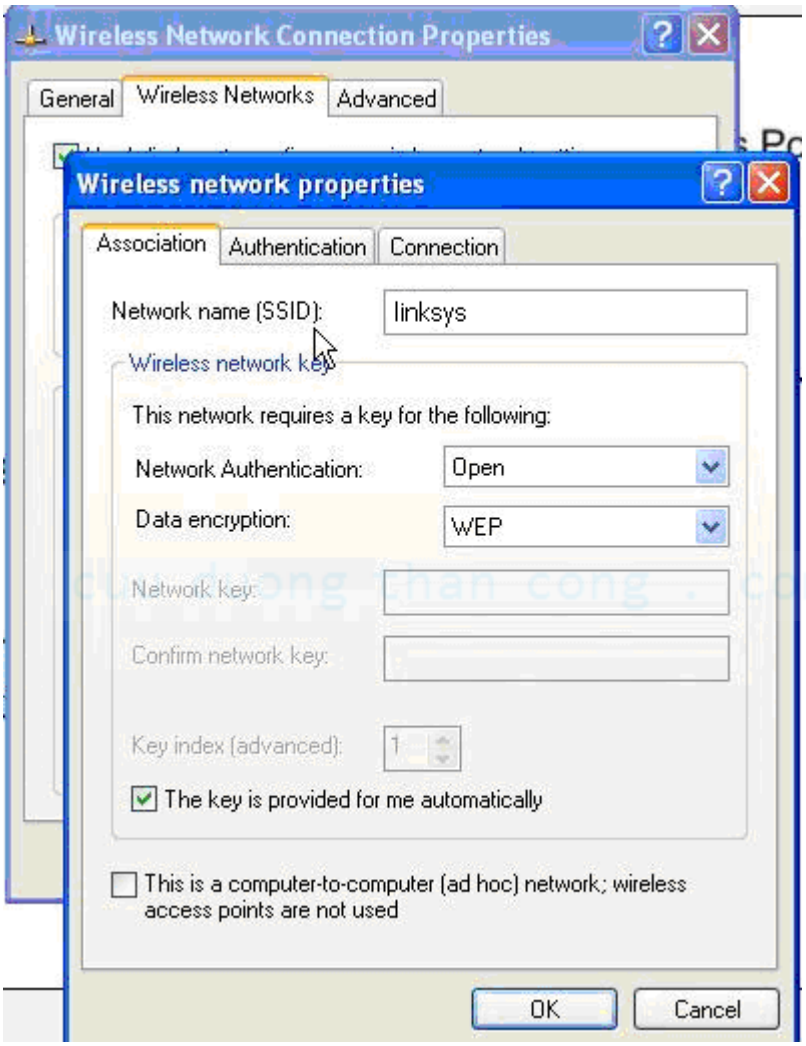


.

CuuDuongThanCong.com

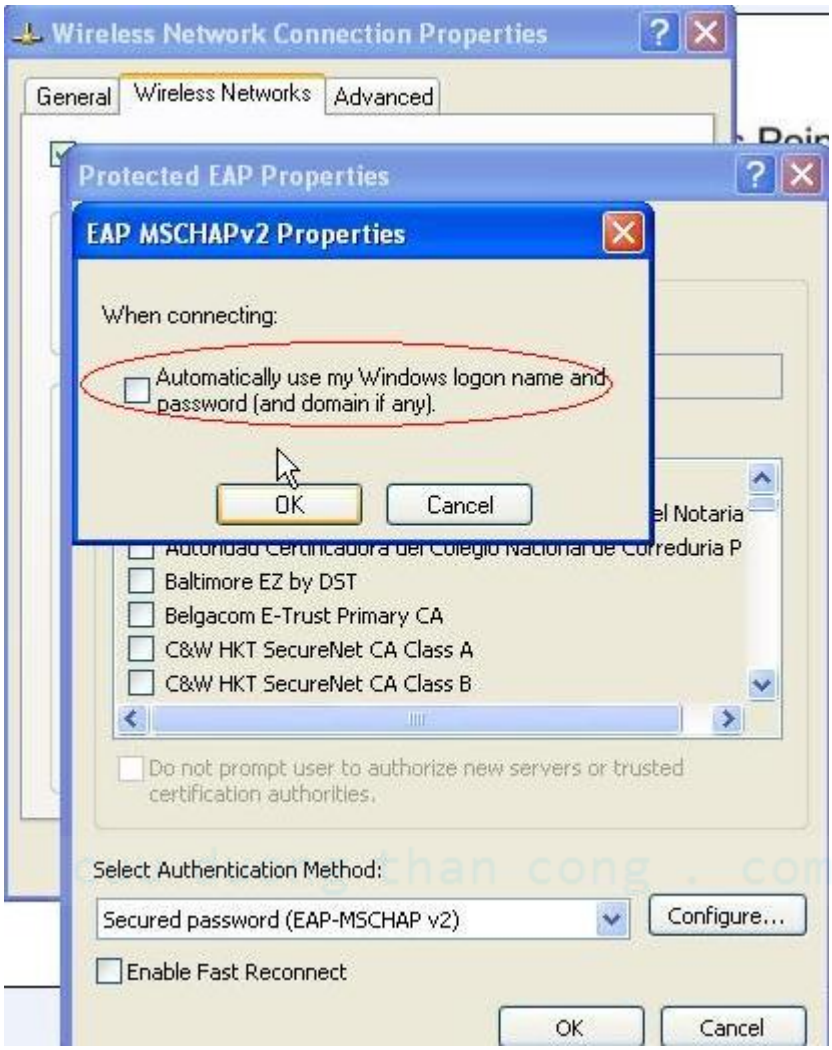
4.3. Cấu hình trên client và kết nối đến Server

Trong cửa Wireless Network Properties tab Accosiation nhập tên Network Name (SSID), tab Authentication chọn Protected EAP click vào Properties bỏ dấu tại check box Validate Server Certificate. Trong mục Configure bỏ check box Automatically use my Windows



cuu duong than cong . com

CuuDuongThanCong.com

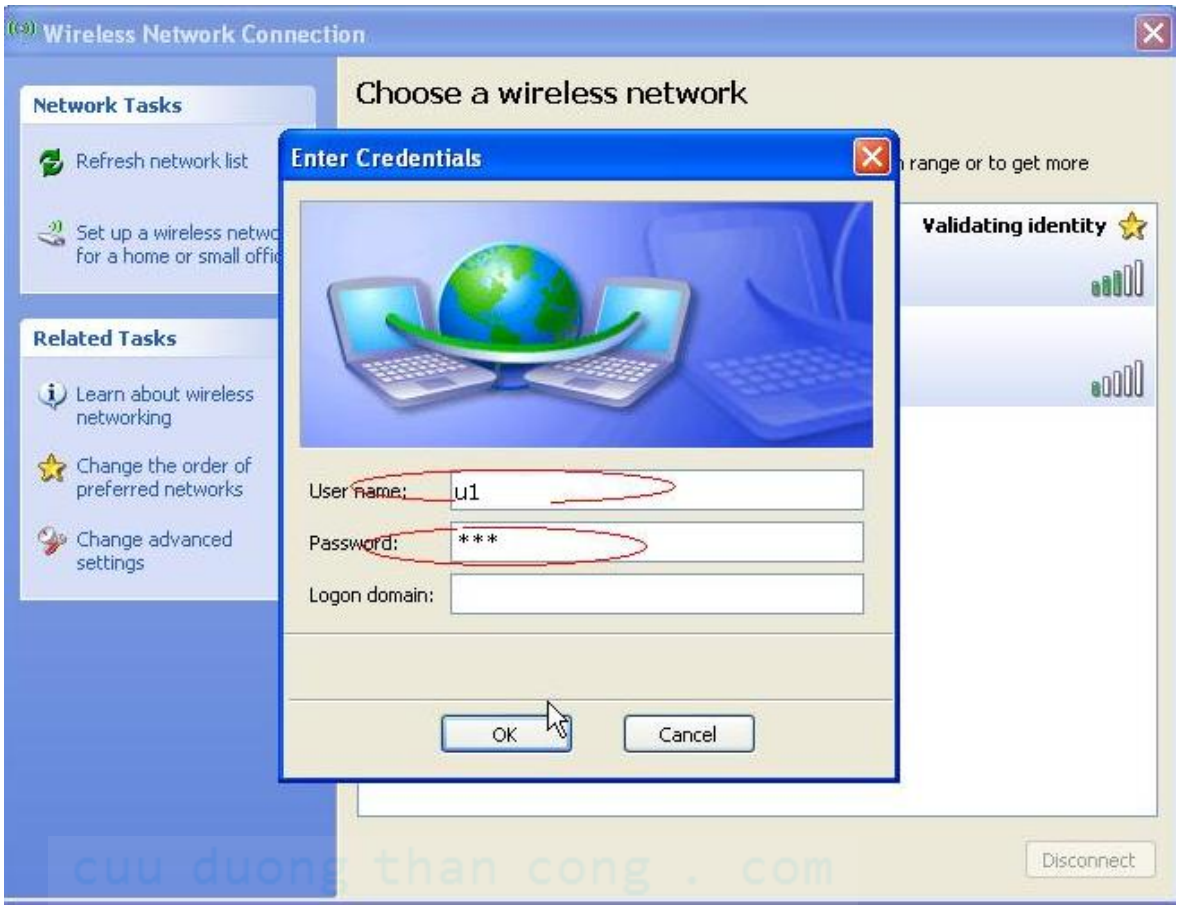


Client kết nối đến Server

Click vào biểu tượng kết nối chọn **Wireless Network Connection** chọn **Accespoint** cần kết nối **-> Connect->** Nhập **User Name** và **pass -> OK.** Kiểm tra lại kết nối tới **Access Point** bằng lệnh **Ping**.

cuu duong than cong . com

CuuDuongThanCong.com



cuu duong than cong . com

CuuDuongThanCong.com

5. Kết quả thực nghiệm , nhận xét đánh giá

-Người dùng di dộng khi muốn kết nối sử dụng mạng Wifi đã được chứng thực bằng User và Password

-Người dùng cần phải nhập chính xác User và password được cấp mới có thể kết nối vào mạng

- Quản lý theo cấu trúc danh bạ: tất cả các đối tượng (group, user, computer account…) và tài nguyên đều được quản lý tập trong bằng dịch vụ Active Directory (AD)

- Là một mô hình quản lý tập trung, ví dụ 1 policy khi triển khai cùng lúc có thể ảnh hưởng trên nhiều máy hoặc nhiều user account.

- Hỗ trợ Single Sign On, mỗi người sử dụng trong hệ thống chỉ cần một user account cho tất cả các nhu cầu: logon, truy cập tài nguyên, sử dụng e-mail…

-Quản lý và thiết lập được thời gian logon , quyền truy cập của user

-Có thể tạo một lúc nhiều User hoặc import user từ 1 danh sách cho trước (txt , Excel ..) bằng cách sử dụng các lệnh DSADD, CSVDE, LDIFDE hoặc dùng SCRIPT

cuu duong than cong . com

CuuDuongThanCong.com

Kết Luận

Mạng không dây hiện nay phát triển rất nhanh đó là nhờ vào sự thuận tiện của nó. Hiện nay công nghệ không dây, nhất là Wi-Fi hiện đang được ứng dụng ngày càng mạnh mẽ trong đời sống. Nhưng đa số mọi người đều chỉ sử dụng Wi-Fi ở các lĩnh vực liên quan đến máy tính mà không biết rằng bằng sóng Wi-Fi, người dùng dùng máy tính để điều khiển hệ thống đèn, quạt, máy lạnh, lò sưởi, máy tưới, hệ thống nước… Nhưng vấn đề quan trọng nhất của mạng không dây hiện nay là sự bảo mật của nó chưa có một giải pháp nào ổn định.

Trong đề tài này em đã trình bày một số những cơ chế bảo mật và những kiến thức cơ bản về Công nghệ mạng không dây. Với khả năng nghiên cứu, thời gian còn hạn chế cũng như vấn đề về thiết bị phần cứng, phần mềm cho mạng không dây nên vẫn còn có những thiếu sót trong đề tài này. Tuy nhiên với những gì đã nghiên cứu và tìm hiểu thì: Mạng không dây theo em nghĩ là một giải pháp hay và thời đại, nó giúp cho chúng ta tiết kiệm được thời gian cũng như công sức trong việc lắp đặt cũng như sử dụng.

cuu duong than cong . com

CuuDuongThanCong.com

Tài liệu tham khảo

Tài liệu tiếng việt :

[1]. *Mạng máy tính và các hệ thống mở*

Nguyễn Thúc Hải

[2]. *Bài giảng mạng máy tính*

Phạm Thế Quế

Tài liệu tiếng anh :

[3]. *Wireless Local Area Netwozzrks*

Pierfranco Issa 1999

[4]. *Designing A Wireless Network*

Syngress Publishing 2001

Website :

[5]. www.wifipro.org

[6]. www.wimaxpro.org

cuu duong than cong . com

cuu duong than cong . com

CuuDuongThanCong.com