LỜI MỞ ĐẦU

Với tốc độ phát triển và không ngừng cải tiến của công nghệ mạng. Mọi người, từ công nhân cho đến những người chủ, từ sinh viên đến giáo viên, tổ chức doanh nghiệp cũng như chính phủ, tất cả đều có nhu cầu kết nối mọi lúc, mọi nơi. Vì vậy, mạng WLAN ra đời để đáp ứng nhu cầu trên.

Mạng WLAN ra đời thực sự là một bước tiến vượt bật của công nghệ mạng, đây là phương pháp chuyển giao từ điểm này sang điểm khác sử dụng sóng vô tuyến. Và hiện nay đã phổ biến trên toàn thế giới, mang lại rất nhiều lợi ích cho người sử dụng, nhất là khả năng di động của nó. Ở một số nước có nền thông tin công nghệ phát triển, mạng không dây thực sự đi vào cuộc sống. Chỉ cần có một Laptop, PDA hoặc một thiết bị truy cập không dây bất kỳ, chúng ta có thể truy cập vào mạng không đây ở bất kỳ nơi đâu, trên cơ quan, trong nhà, trên máy bay, ở quán Caffe… ở bất kỳ đâu trong phạm vi phủ sóng của WLAN.

Với rất nhiều lợi ích và sự truy cập công cộng như vậy, nhưng vấn đề bảo mật luôn làm đau đầu các nhà sản xuất, các tổ chức và cá nhân người sử dụng. Vì phương tiện truyền tin của WLAN là sóng vô tuyến và môi trường truyền tin là không khí, chỉ thiết bị thu chỉ cần nằm trong vùng phủ sóng là có có khả năng truy cập vào mạng. điều này dẫn đến vấn đề nghiêm trọng về bảo mật mạng WLAN. Chính vì vậy, trong học phần **Mạng không dây**, Nhóm 4 lớp MM02A trường CĐ CNTT Hữu Nghị Việt Hàn đã chọn đề tài "***Bảo mật mạng WLAN với chứng thực RADIUS***" để làm đồ án kết thúc học phần.

Tuy đã có nhiều cố gắng nhưng không thể tránh khỏi những sai sót trong đồ án, vì vậy Nhóm 4 mong nhận được sự đóng gói của bạn bè và thầy cô để đồ án được hoàn thiện hơn.

Đà nẵng ngày 5 tháng 11 năm 2010

Sinh viên thực hiện: Nhóm 4

MỤC LỤC

MỤC LỤC HÌNH ẢNH

CHƯƠNG 1. TỔNG QUAN VỀ WLAN

1.1. Tổng quan về WLAN

1.1.1. Mạng WLAN là gì?

Mạng LAN không dây viết tắt là WLAN (Wireless Local Area Network) hay WIFI (Wireless Fidelity), là một mạng dùng để kết nối hai hay nhiều máy tính với nhau mà không sử dụng dây dẫn. WLAN dùng công nghệ trải phổ, sử dụng sóng vô tuyến cho phép truyền thông giữa các thiết bị trong một vùng nào đó gọi là Basic Service Set.

Đây là một giải pháp có rất nhiều ưu điểm so với kết nối mạng có dây (wireline) truyền thống. Người dùng vẫn duy trì kết nối với mạng khi di chuyển trong vùng phủ sóng.

1.1.2. Lịch sử hình thành và phát triển.

Năm 1990, công nghệ WLAN lần đầu tiên xuất hiện, khi những nhà sản xuất giới thiệu những sản phẩm hoạt động ở băng tần 900 Mhz. Các giải pháp này (không có sự thống nhất của các nhà sản xuất) cung cấp tốc độ truyền dữ liệu 1Mbs, thấp hơn rất nhiều so với tốc độ 10 Mbs của hầu hết các mạng sử dụng cáp lúc đó.

Năm 1992, các nhà sản xuất bắt đầu bán những sản phẩm WLAN sử dụng băng tần 2.4GHz. Mặc dù những sản phẩm này có tốc độ truyền cao hơn nhưng chúng vẫn chỉ là những giải pháp riêng của mỗi nhà sản xuất và không được công bố rộng rãi. Sự cần thiết cho việc thống nhất hoạt động 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.

Năm 1997, IEEE (Institute of Electrical and Electronics Engineers) đã thông qua sự ra đời của chuẩn 802.11, và được biết đến với tên WIFI (Wireless Fidelity) cho các mạng WLAN.

Năm 1999, IEEE thông qua sự bổ sung cho chuẩn 802.11 là chuẩn 802.11a và 802.11b (định nghĩa ra những phương pháp truyền tín hiệu). Và các thiết bị WLAN dựa trên chuẩn 802.11b đã nhanh chóng trở thành công nghệ không dây nổi trội.

Năm 2003, IEEE công bố thêm sự cải tiến là chuẩn 802.11g, chuẩn này cố gắng tích hợp tốt nhất các chuẩn 802.11a, 802.11b và 802.11g. Sử dụng băng tần 2.4Ghz cho phạm vi phủ sóng lớn hơn.

Năm 2009, IEEE cuối cùng cũng thông qua chuẩn WIFI thế hệ mới 802.11n sau 6 năm thử nghiệm. Chuẩn 802.11n có khả năng truyền dữ liệu ở tốc độ 300Mbps hay thậm chí cao hơn.

1.1.3. Ưu điểm của WLAN

- ***Sự tiện lợi***: Mạng không dây cung cấp giải pháp cho phép người sử dụng truy cập tài nguyên trên mạng ở bất kì nơi đâu trong khu vực WLAN được triển khai (khách sạn, trường học, thư viện…). Với sự bùng nổ của máy tính xách tay và các thiết bị di động hỗ trợ wifi như hiện nay, điều đó thật sự rất tiện lợi.
- ***Khả năng di động:*** Với sự phát triển vô cùng mạnh mẽ của viễn thông di động, người sử dụng có thể truy cập internet ở bất cứ đâu. Như: Quán café, thư viện, trường học và thậm chí là ở các công viên hay vỉa hè. Người sử dụng đều có thể truy cập internet miễn phí.
- ***Hiệu quả:*** Người sử dụng có thể duy trì kết nối mạng khi họ đi từ nơi này đến nơi khác.
- ***Triển khai:*** Rất dễ dàng cho việc triển khai mạng không dây, chúng ta chỉ cần một đường truyền ADSL và một AP là được một mạng WLAN đơn giản. Với việc sử dụng cáp, sẽ rất tốn kém và khó khăn trong việc triển khai ở nhiều nơi trong tòa nhà.
- ***Khả năng mở rộng:*** Mở rộng dễ dàng và có thể đáp ứng tức thì khi có sự gia tăng lớn về số lượng người truy cập.

1.1.4. Nhược điểm

Bên cạnh những thuận lợi mà mạng không dây mang lại cho chúng ta thì nó cũng mắc phải những nhược điểm. Đây là sự hạn chế của các công nghệ nói chung.

- ***Bảo mật:*** Đây có thể nói là nhược điểm lớn nhất của mạng WLAN, bởi vì phương tiện truyền tín hiệu là song và môi trường truyền tín hiệu là không khí nên khả năng một mạng không dây bị tấn công là rất lớn

❖ ***Phạm vi:*** Như ta đã biết chuẩn IEEE 802.11n mới nhất hiện nay cũng chỉ có thể hoạt động ở phạm vi tối đa là 150m, nên mạng không dây chỉ phù hợp cho một không gian hẹp.

❖ ***Độ tin cậy:*** Do phương tiện truyền tín hiệu là sóng vô tuyến nên việc bị nhiễu, suy giảm…là điều không thể tránh khỏi. Điều này gây ảnh hưởng đến hiệu quả hoạt động của mạng.

❖ ***Tốc độ:*** Tốc độ cao nhất hiện nay của WLAN có thể lên đến 600Mbps nhưng vẫn chậm hơn rất nhiều so với các mạng cáp thông thường (có thể lên đến hàng Gbps)

1.2. Cơ sở hạ tầng WLAN

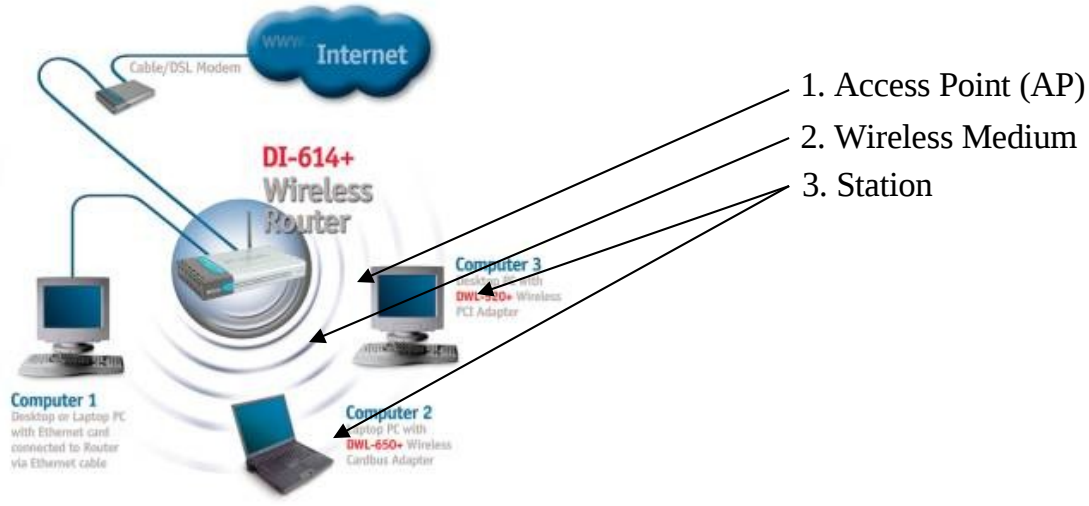
1.2.1. Cấu trúc cơ bản của WLAN

❖ ***Distribution System*** (Hệ thống phân phối): Đây là một thành phần logic sử dụng để điều phối thông tin đến các station đích.Chuẩn 802.11 không đặc tả chính xác kỹ thuật cho DS.

❖ ***Access Point:*** chức năng chính chủa AP là mở rộng mạng. Nó có khả năng chuyển đổi các frame dữ liệu trong 802.11 thành các frame thông dụng để có thể sử dụng trong mạng khác.

❖ ***Wireless Medium (tầng liên lạc vô tuyến)*:** Chuẩn 802.11 sử dụng tần liên lạc vô tuyến để chuyển đổi các frame dữ liệu giữa các máy trạm với nhau.

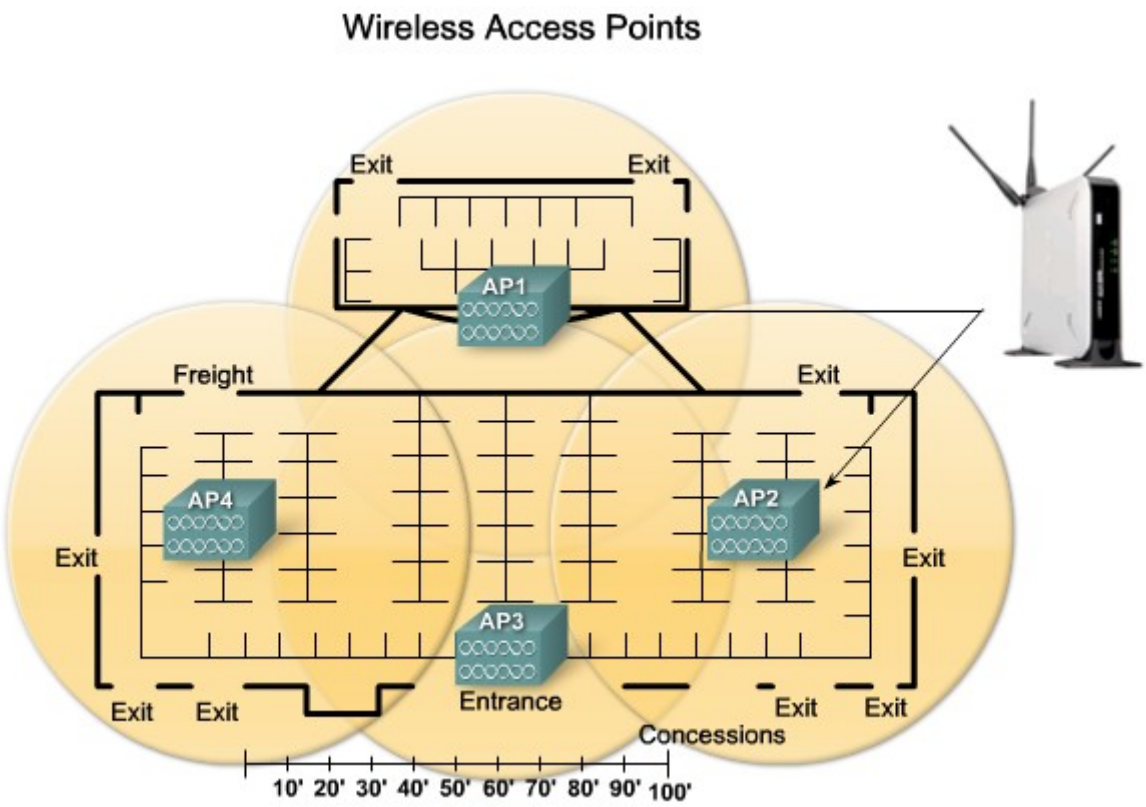
❖ ***Station (các máy trạm):*** Đây là các thiết bị ngoại vi có hỗ trợ kết nối vô tuyến như: laptop, PDA, Palm…



Hình 1-1 Cấu trúc cơ bản của WLAN

1.2.2. Thiết bị dành cho WLAN

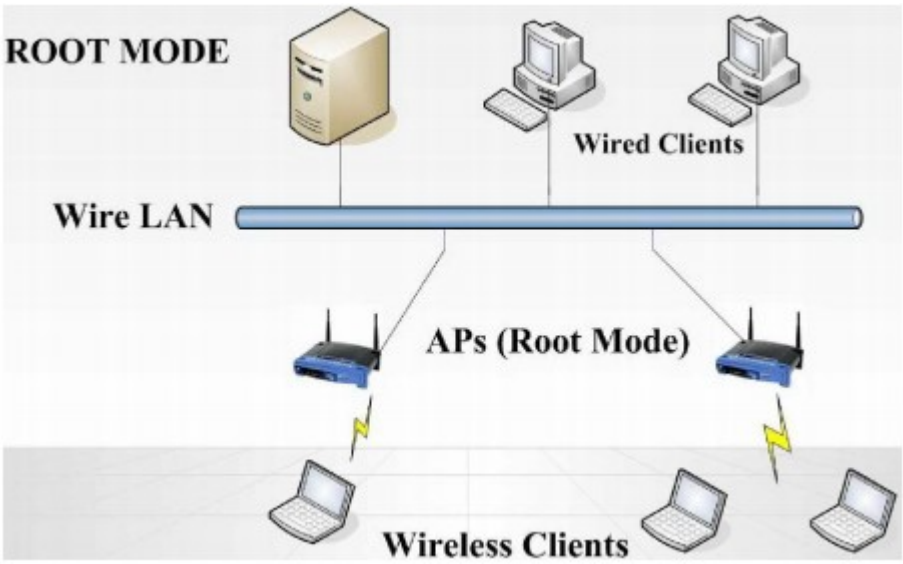
❖ **Wireless Accesspoint(AP):** Là thiết bị có nhiệm vụ cung cấp cho máy khách (client) một điểm truy cập vào mạng.



Hình 1-2 Thiết bị Wireless Accesspoint

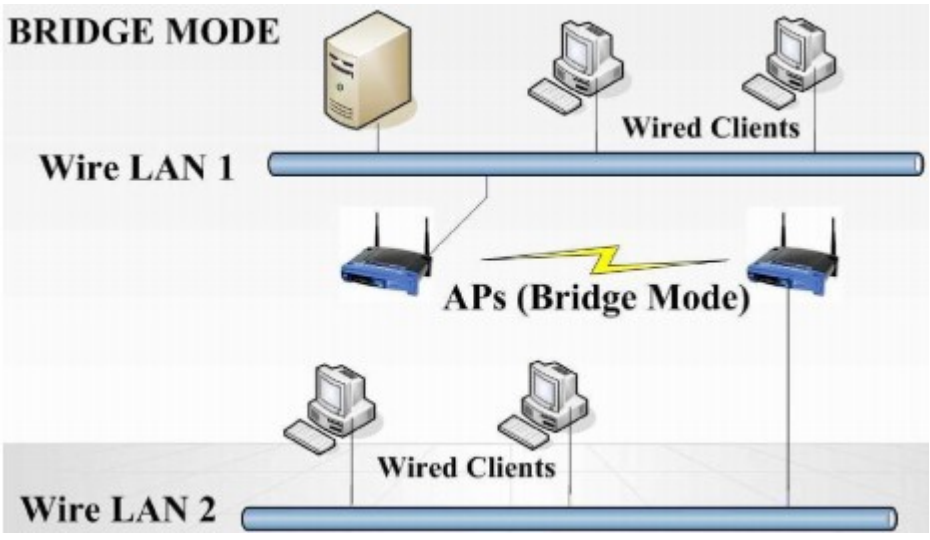
❖ **Các chế độ hoạt động của AP:** AP có ba chế độ hoạt động chính.

o **Chế độ gốc (root mode):** Root mode được sử dụng khi AP kết nối với mạng backbone có dây thông qua giao diện có dây (thường là Ethernet) của nó. Hầu hết các AP đều hoạt động ở chế độ mặc định là root mode.



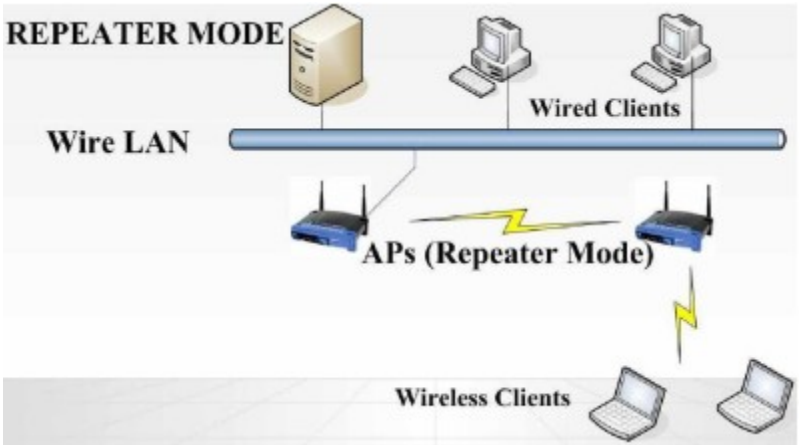
Hình 1-3: AP hoạt động ở root mode

o **Chế độ cầu nối(bridge mode):** Trong bridge mode, AP hoạt động hoàn toàn như cầu mối không dây. Với chế độ này, máy khách (client) sẽ không kết nối trực tiếp với AP, nhưng thay vào đó, AP dùng để nối hai hay nhiều đoạn mạng có dây lại với nhau. Hiện nay, hầu hết các thiết bị AP đều hỗ trợ chế độ bridge.



Hình 1-3 Chế độ cầu nối của AP

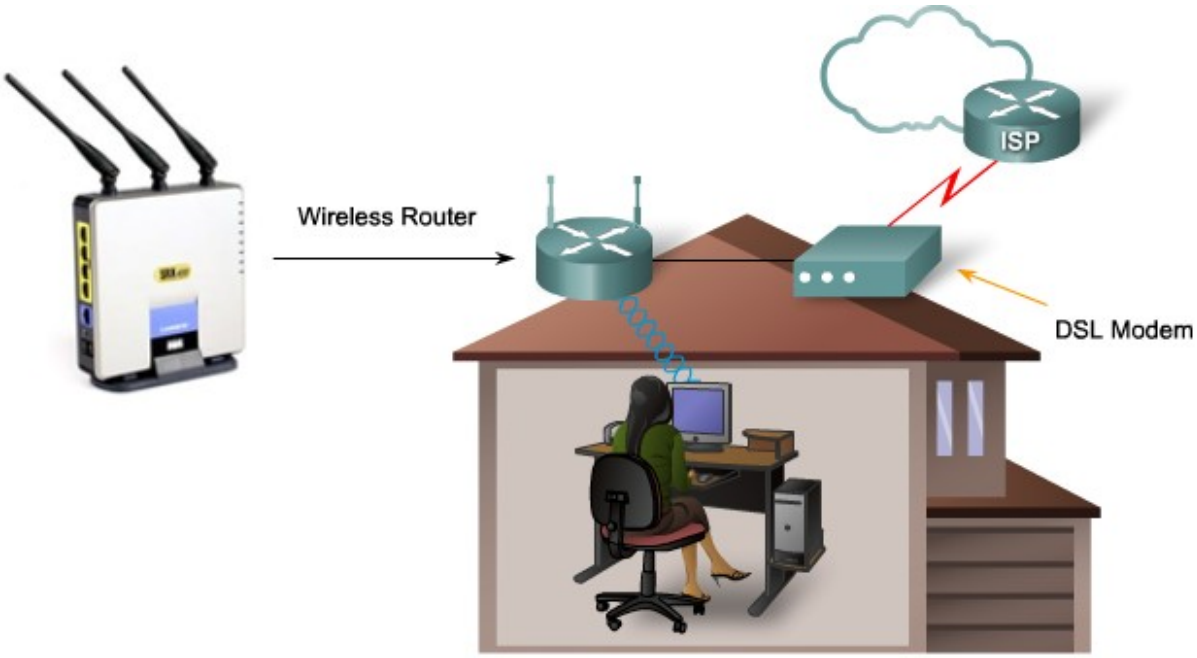
o **Chế độ lặp (Repeater mode):** Ở chế độ Repeater, sẽ có ít nhất hai thiết bị AP, một root AP và một AP hoạt động như một Repeater không dây. AP trong Repeater mode hoạt động như một máy khách khi kết nối với root AP và hoạt động như một AP khi kết nối với máy khách.



Hình 1-4 Chế độ Repeater của AP

❖ **Wireless Router**

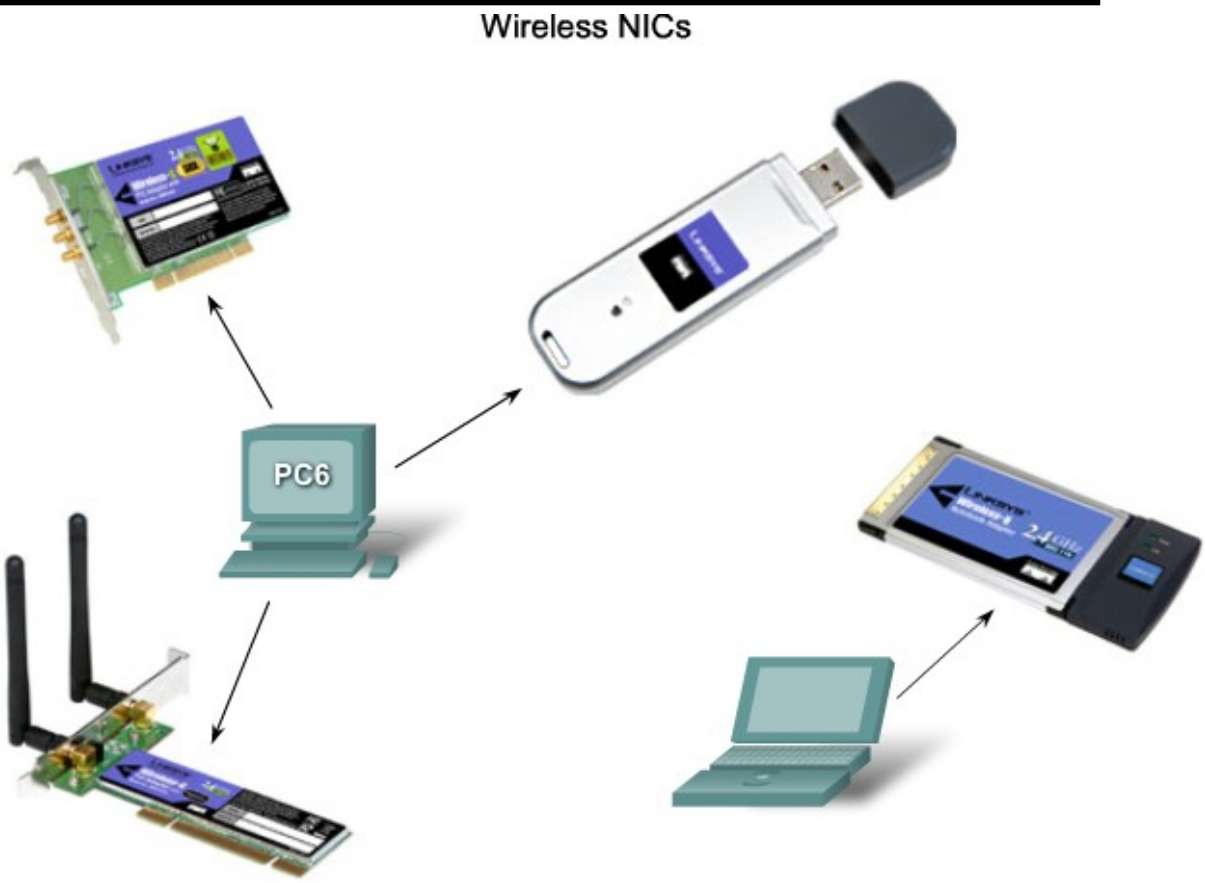
Ngày nay, với sự tiến bộ của công nghệ và kỹ thuật, sự ra đời của thiết bị đa năng Wireless Router với sự kết hợp chức năng cửa ba thiết bị là Wireless Accesspoint, Ethernet Switch và Router.



Hình 1-5 Thiết bị Wireless Router

❖ **Wireless NICs:**

Là các thiết bị được máy khách dùng để kết nối vào AP.



Hình 1-6 Wireless NICs

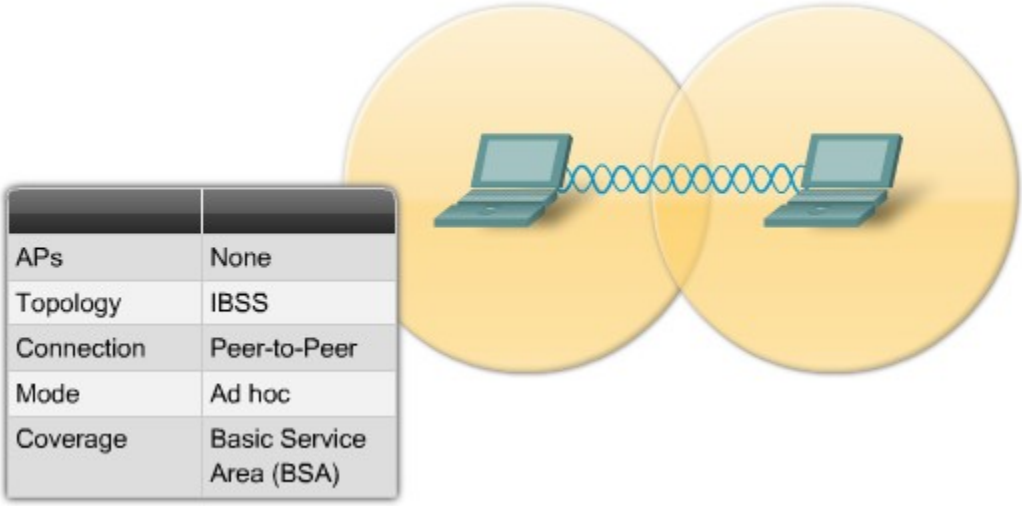
1.2.3. Các mô hình WLAN.

Mạng 802.11 rất linh hoạt về thiết kế, bao gồm 3 mô hình cơ bản sau

- Mô hình mạng độc lập (IBSSs) hay còn gọi là mạng Ad-hoc.
- Mô hình mạng cơ sở (BSSs).
- Mô hình mạng mở rộng (ESSs).

1.2.3.1. Mô hình mạng độc lập

Mạng IBSSs (Independent Basic Service Set) hay còn gọi là mạng ad-hoc, trong mô hình mạng ad-hoc các client liên lạc trực tiếp với nhau mà không cần thông qua AP nhưng phải ở trong phạm vi cho phép. Mô hình mạng nhỏ nhất trong chuẩn 802.11 là 2 máy client liên lạc trực tiếp với nhau. Thông thường mô hình này được thiết lập bao gồm một số client được cài đặt dùng chung mục đích cụ thể trong khoảng thời gian ngắn .Khi mà sự liên lạc kết thúc thì mô hình IBSS này cũng được giải phóng.

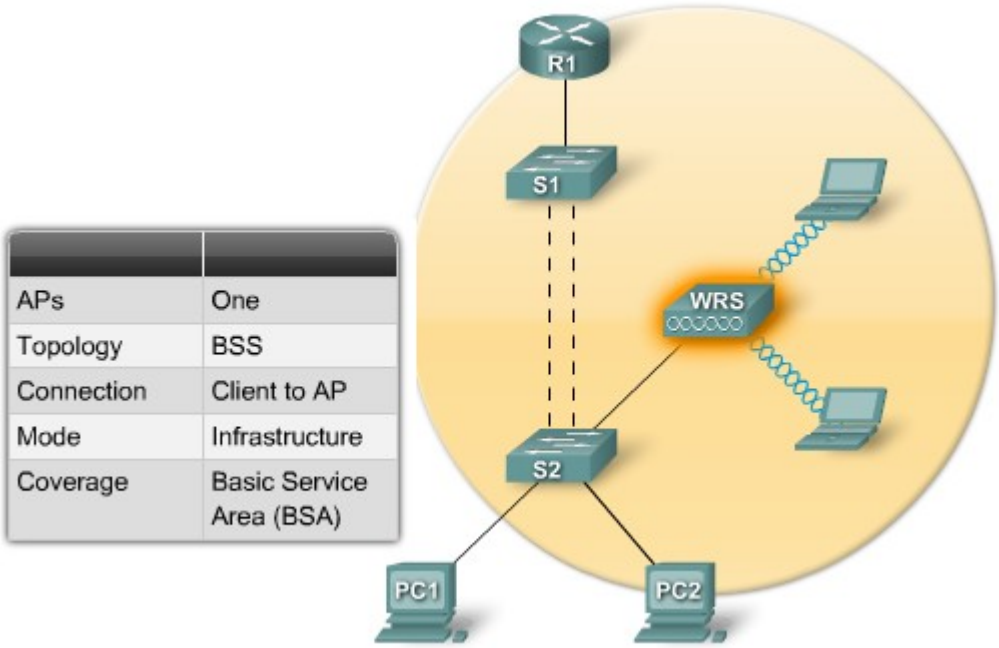


Hình 1-7 Mô hình mạng Ad-hoc.

1.2.3.2. Mô hình mạng cơ sở (BSSs)

The Basic Service Sets (BSS) là một topology nền tảng của mạng 802.11. Các thiết bị giao tiếp tạo nên một BSS với một AP duy nhất với một hoặc nhiều client. Các máy trạm kết nối với sóng wireless của AP và bắt đầu giao tiếp thông qua AP. Các máy trạm là thành viên của BSS được gọi là "có liên kết".

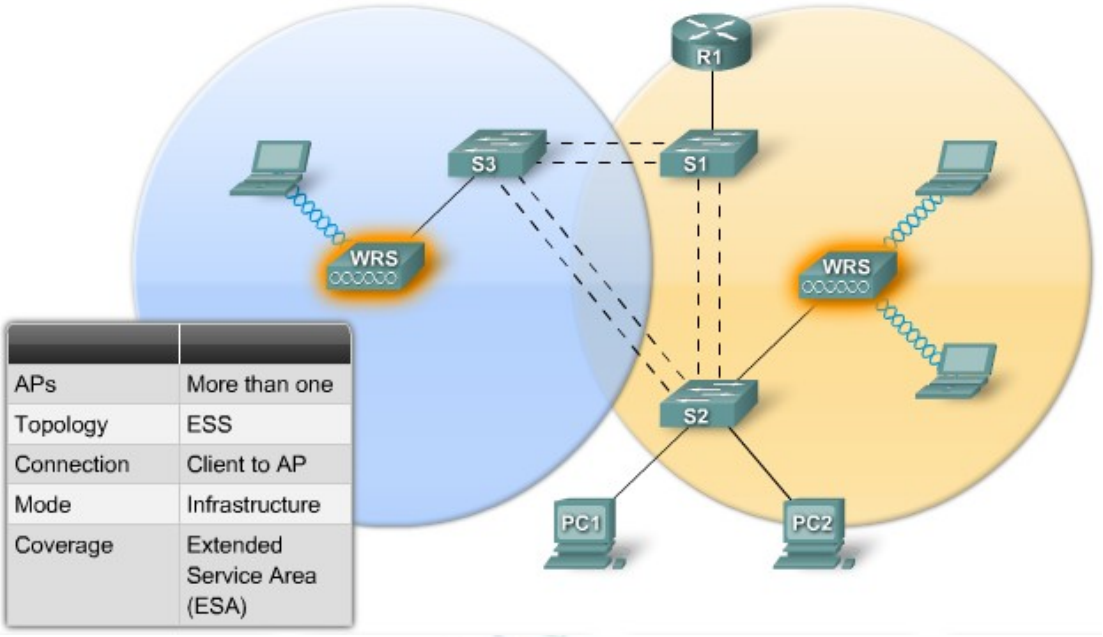
Thông thương các AP được kết nối với một hệ thống phân phối trung bình (DSM), nhưng đó không phải là một yêu cầu cần thiết của một BSS. Nếu một AP phục vụ như là cổng để vào dịch vụ phân phối, các máy trạm có thể giao tiếp, thông qua AP, với nguồn tài nguyên mạng ở tại hệ thống phân phối trung bình. Nó cũng cần lưu ý là nếu các máy client muốn giao tiếp với nhau, chúng phải chuyển tiếp dữ liệu thông qua các AP. Các client không thể truyền thông trực tiếp với nhau, trừ khi thông qua các AP. Hình sau mô tả mô hình một BSS chuẩn.



Hình 1-8 Mô hình mạng BSS chuẩn

1.2.3.3. Mô hình mạng mở rộng (ESSs)

Trong khi một BSS được coi là nền tảng của mạng 802.11, một mô hình mạng mở rộng ESS (extended service set) của mạng 802.11 sẽ tương tự như là một tòa nhà được xây dựng bằng đá. Một ESS là hai hoặc nhiều BSS kết nối với nhau thông qua hệ thống phân phối. Một ESS là một sự hội tụ nhiều điểm truy cập và sự liên kết các máy trạm của chúng. Tất cả chỉ bằng một DS. Một ví dụ phổ biến của một ESS có các AP với mức độ một phần các tế bào chồng chéo lên nhau. Mục đích đằng sau của việc này là để cung cấp sự chuyển vùng liên tục cho các client. Hầu hết các nhà cung cấp dịch vụ đề nghị các tế bào chồng lên nhau khoảng 10%-15% để đạt được thành công trong quá trình chuyển vùng.



Hình 1-9 Mô hình mạng ESS

CHƯƠNG 2. CÁC HÌNH THỨC TẤN CÔNG PHỔ BIẾN TRONG WLAN VÀ GIẢI PHÁP PHÒNG CHỐNG

2.1. Các hình thức tấn công phổ biến trong WLAN

Tấn công và phòng chống trong mạng WLAN là vấn đề được quan tâm đến rất nhiều hiện nay bởi các chuyên gia trong lĩnh vực bảo mật. Nhiều giải pháp tấn công và phòng chống đã được đưa ra nhưng cho đến bây giờ chưa có giải pháp nào được gọi là bảo mật an toàn, cho đến hiện nay mọi giải pháp phòng chống được đưa ra đều chỉ là tương đối (nghĩa là tính bảo mật trong mạng WLAN vẫn có thể bị phá vỡ bằng nhiều cách khác nhau). Vấn đề tấn công một mạng WLAN như thế nào? Và giải pháp phòng chống ra sao? Chúng ta sẽ cùng tìm hiểu rõ hơn trong phần dưới đây.

Theo rất nhiều tài liệu nghiên cứu, hiện tại để tấn công vào mạng WLAN thì các attacker có thể sử dụng một trong những cách sau:

- Rogue Access Point
- De-authentication Flood Attack
- Fake Access point
- Tấn công dựa trên cảm nhận lớp vật lý
- Disassociation Flood Attack

2.1.1. Rogue Access Point

2.1.1.1. Định nghĩa

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.

2.1.1.2. Phân loại

2.1.1.3.Access Point được cấu hình không hoàn chỉnh:

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

VD: 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 một 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 các người dùng được phép truy cập.

2.1.1.4.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.

VD: Windows XP tự động kết nối đến kết nối tốt nhất có thế xum 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 để lộ những dữ liệu nhạy cảm.

2.1.1.5.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 lấy trộm tất cả lưu lượng đi qua mạng. Rất khó khắn để tạo một cuộc tấn công "man in 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 phải tạo ra một AP thu hút nhiều sự lựa chọn hơn AP chính thống. AP giả này có thể thiết lập bằng cách sao chép tất cả các cấu hình của AP chính thống đó là: SSID, địa chỉ MAC…

Bước tiếp theo là làm cho nạn nhân thực hiện kết nối đến AP giả.

- Cách thứ nhất là đợi cho người dùng tự kết nối.
- Cách thứ 2 là gây ra một cuộc tấn công từ chối dịch vụ DOS trong AP chính thống do vậy người dùng sẽ phải kết nối lại với AP giả.

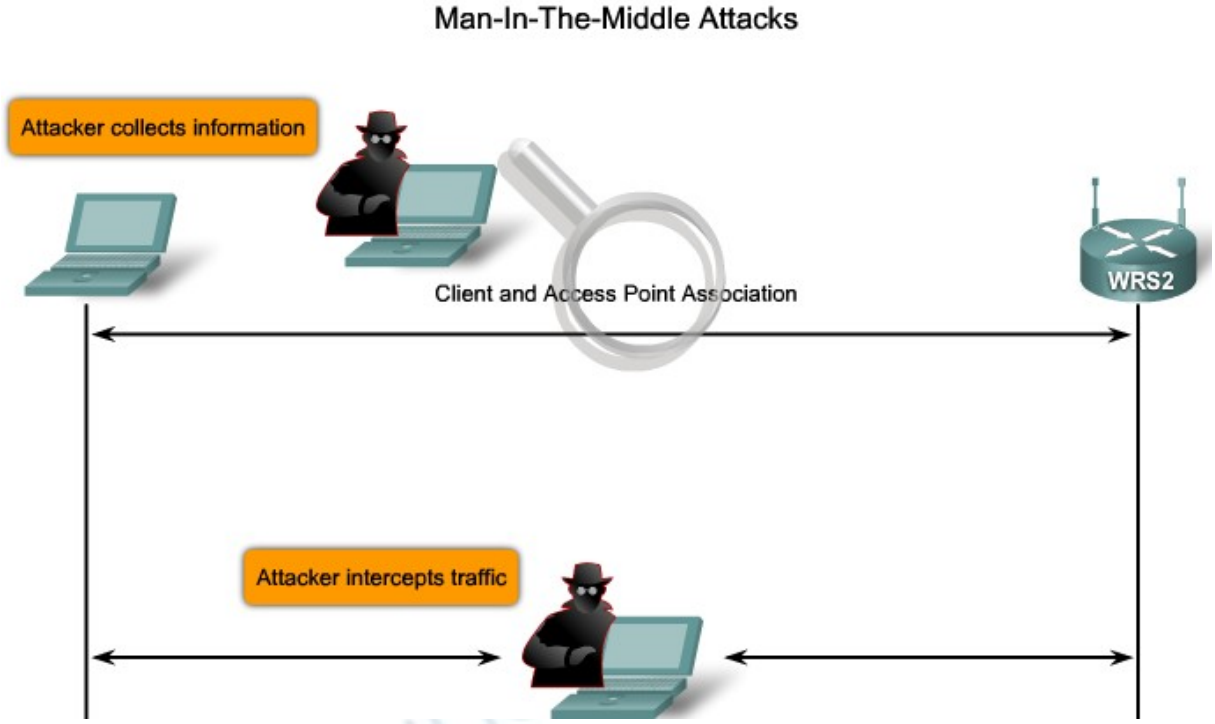
Trong mạng 802.11 sự lựu chọn được thực hiện bởi cường độ tính hiệu nhận. Điều duy nhất mà tin tặc phải thực hiện là chắc chắn rằng AP

của mình phải có cường độ tín hiệu của mình 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 kĩ thuật anten định hướng. Sau khi nạn nhận 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 trao đổi với Web Server. Như vậy tin tặc sẽ có được 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 xác 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 xác 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 hóa để trộm mật khẩu của người dùng.

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

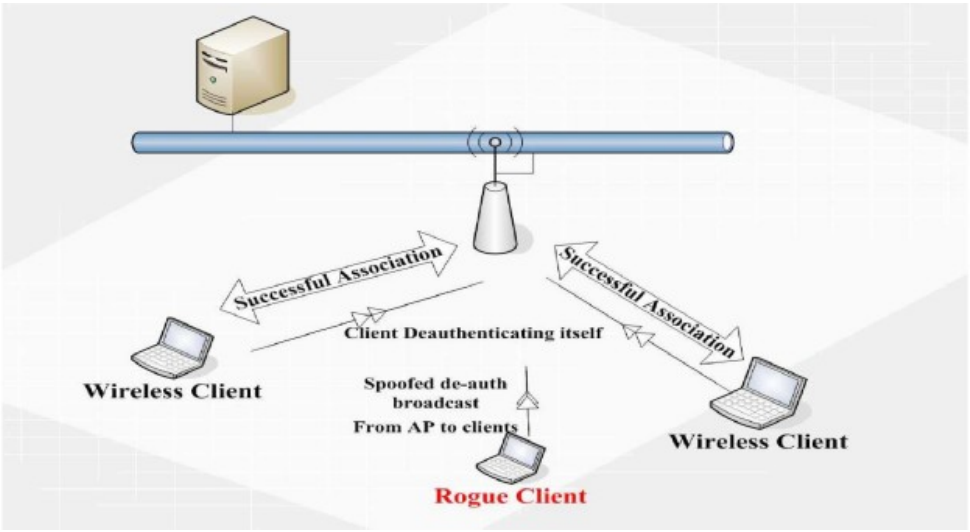
Vì sự tiện lợi của mạng không dây một số nhân viên của công ty đã tự trang bị Access Point và kết nối chúng vào mạng có dây của công ty. Do không hiểu rõ và nắm vững về bảo mật trong mạng không dây nên họ vô tình tạo ra một lỗ hổng lớn về bảo mật.

Những người lạ vào công ty và hacker bên ngoài có thể kết nối đến Access Point không được xác thực để đánh cắp băng thông, đánh cắp thông tin nhạy cảm của công ty, sử dụng mạng của công ty tấn công người khác……



Hình 2-10 Tấn công Man-In-The-Middle

2.1.2. Tấn công yêu cầu xác thực lại



Hình 2-11 Mô hình 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).

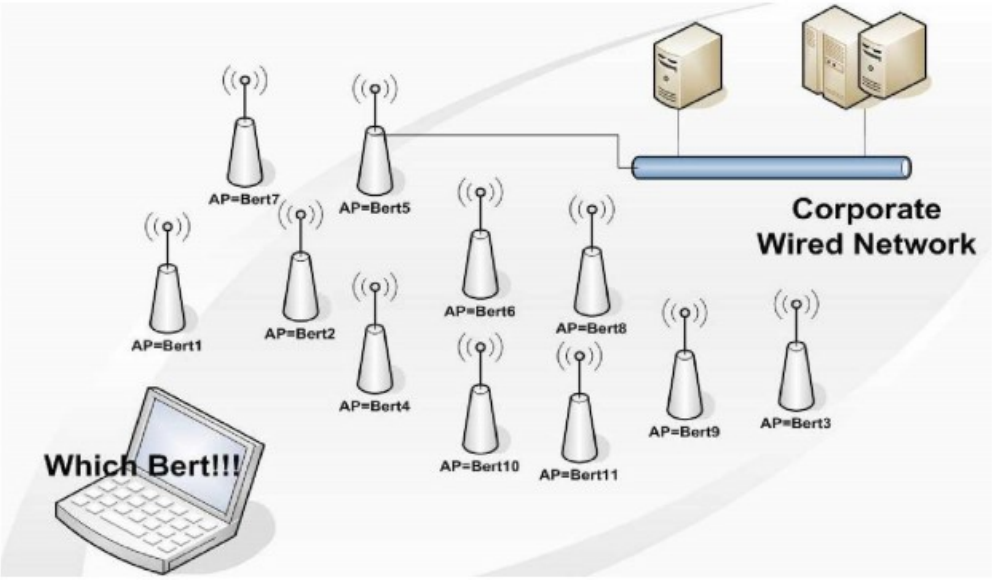
❖ Chèn các frame yêu cầu xác thực lại vào mạng WLAN bằng cách giả mạo địa chỉ MAC nguồn và đích lần lượt của Access Point và các người dùng.

❖ 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 thì người dùng sẽ kết nối lại để phục hồi dịch vụ, nhưng kẻ tấn công đã nhanh chóng gửi các gói yêu cầu xác thực lại cho người dùng.

2.1.3. Face 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 các Access Point giả lập. Điều này làm xáo trộn tất cả các phần mềm điều khiển card mạng không dây của người dùng.



Hình 2-12 Mô hình tấn công Fake Access Point

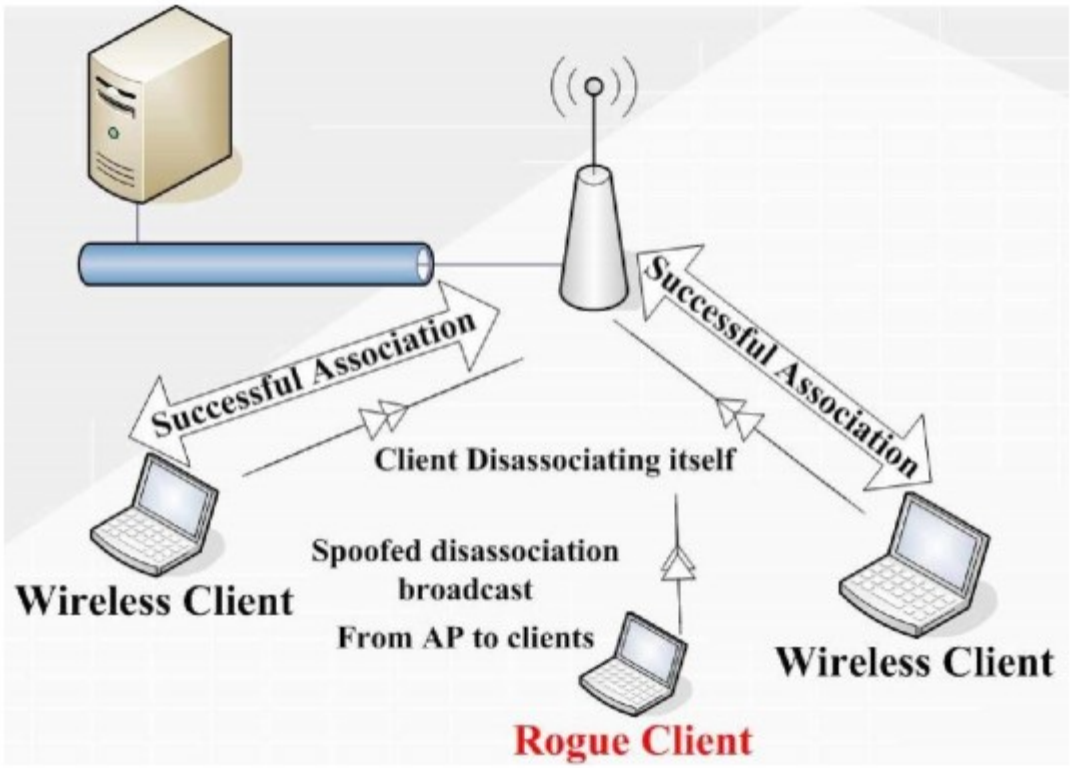
2.1.4. Tấn công dựa trên sự cảm nhận sóng mang lớp vật lý

Kẻ tấn công lợi dụng giao thức chống đụng độ CSMA/CA, tức là nó sẽ làm cho tất cả người dùng nghĩ rằng lúc nào trong mạng cũng có một máy đang truyền thông. Điều này làm cho các máy tính khác luôn luôn ở trạng thái chờ đợi kể tấn công ấy truyền dữ liệu xong, dẫn đến tình trạng nghẽn trong mạng.

Tần số là một nhược điểm bảo mật trong mạng không dây. Mức độ nguy hiểm thay đổi phụ thuộc vào giao diện của lớp vật lý. Có một vài tham số quyết định sự chịu đựng của mạng là: năng lượng máy phát, độ nhạy của máy thu, tần số RF (Radio Frequency), băng thông và sự định 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 phần của lớp MAC. CSMA được sử dụng để chắc chắn sẽ không có va chạm dữ

liệu trên đường truyền. Kiểu tấn công này không sử dụng tạp âm để tạo ra lỗi cho mạng nhưng nó sẽ lợi dụng chính chuẩn đó. Có nhiều cách để khai thác giao thức cảm nhận sóng mang vật lý. Cách đơn giản là làm cho các nút trong mạng đều tin tưởng rằng có một nút đang truyền tin tại thời điểm hiện tại. Cách dễ nhất để đạt 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 tin vi hơn là làm cho card mạng chuyển vào chế độ kiểm tra mà ở đó nó truyền đi liên tiếp một mẩu 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.

2.1.5. Tấn công ngắt kết nối



Hình 2-13 Mô hình tấn công ngắt kết nối

- ❖ Kẻ tấn công xác định mục tiêu (wireless cliens) và mối liên kết giữa AP với các client.
- ❖ Kẻ tấn công gửi disassociation frame bằng cách giả mạo source và Destination MAC đến AP và các clien tương ứng.
- ❖ Client sẽ nhận các frame này và nghĩ rằng frame hủy kết nối đến từ AP. Đồng thời kẻ tấn công cũng gửi gói disassociation frame đến AP.