HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

ĐỖ VIẾT CÔNG

PHÂN TÍCH VÀ THIẾT KẾ TĂNG HIỆU NĂNG HỆ THỐNG MẠNG WIFI TẠI TRƯỜNG CAO ĐẲNG LÝ THÁI TỔ

LUẬN VĂN THẠC SĨ KỸ THUẬT

(Theo định hướng ứng dụng)

HÀ NỘI – 2020

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

ĐỖ VIẾT CÔNG

PHÂN TÍCH VÀ THIẾT KẾ TĂNG HIỆU NĂNG HỆ THỐNG MẠNG WIFI TẠI TRƯỜNG CAO ĐẲNG LÝ THÁI TỔ

Chuyên ngành: Kỹ thuật viễn thông

Mã số: 8.52.02.08

LUẬN VĂN THẠC SĨ KỸ THUẬT

(*Theo định hướng ứng dụng*)

NGƯỜI HƯỚNG DẪN KHOA HỌC:

TS. LÊ NGỌC THÚY

HÀ NỘI - 2020

LỜI CAM ĐOAN

Tôi cam đoan đây là công trình nghiên cứu của riêng tôi.

Các số liệu, kết quả nêu trong luận văn là trung thực và chưa từng được công bố trong bất kỳ công trình nào khác.

Hà Nội, tháng 05 năm 2020
Tác giả luận văn

Đỗ Viết Công

LỜI CẢM ƠN

Để hoàn thành luận văn này lời đầu tiên tôi xin tỏ lòng biết ơn sâu sắc đến TS. Lê Ngọc Thuý đã tận tình hướng dẫn và chỉ bảo trong suốt quá trình thực hiện.

Tôi chân thành cảm ơn các Thầy, Cô trong khoa Đào Tạo Sau Đại Học, Học viện Công nghệ Bưu chính Viễn thông Hà Nội đã tận tình giúp đỡ tôi trong quá trình hai năm tôi học tập và nghiên cứu.

Tôi cũng xin chân thành cảm ơn Hội đồng quản trị, Ban giám hiệu, Ban công nghệ thông tin, Khoa Tin học, các đồng nghiệp tại trường Cao đẳng Lý Thái Tổ đã tạo điều kiện thuận lợi nhất để những nghiên cứu trong luận văn này từ lý thuyết đến thực tế được áp dụng thành công.

Hà Nội, ngày 15 tháng 05 năm 2020

Đỗ Viết Công

MỤC LỤC

DANH MỤC CÁC KÝ HIỆU, CÁC CHỮ VIẾT TẮT

Từ viết tắt	Nghĩa tiếng Anh	Nghĩa tiếng Việt
AES	Advance Encryption Standar	Tiêu chuẩn mã hóa nâng cao
AP	Access Point	Điểm truy cập
AODV	Ad hoc on-demand distance vector routing	Định tuyến vectơ khoảng cách dựa trên yêu cầu trong mạng ad-hoc
BSS	Base Station Subsystem	Mô hình mạng cơ sở
CBR	Constant Bit Rate	Băng thông luôn được giữ cố định
DSR	Data Set Ready	Tập dữ liệu sẵn sàng
DSDV	Destination-Sequenced DistanceVector – Proactive	Giao thức định tuyến theo kiểu vector
DES	Data Encryption Standard	Chuẩn mã hóa dữ liệu
DS	Distribution System	Hệ thống phân phối
DSS	Direct Sequence Spectrum	Trải phổ chuỗi trực tiếp
ESS	Expanded network model	Mô hình mạng mở rộng
FHSS	Frequence Hopping Spread Spectrum	Phổ tần số nhảy tần
IBSS	Independent Basic Service Set	Chuyển đổi tích hợp dịch vụ băng thông rộng
IEEE	Institute of Electrical and Electronics Engineers	Hiệp hội nghề nghiệp và tổ chức toàn cầu
IPSec	Internet Protocol Security	Giao thức để bảo mật trên nền tảng Internet Protocol
NIC	Network Interface Card	card giao tiếp mạng
NIST	National Institute of Standards and Technology	Viện Tiêu chuẩn và Công nghệ Quốc gia Mỹ
SDM	Security Device Manager	Công cụ để quản lý thiết bị Router thông qua công nghệ JAVA
MAC	Media Access Control	kiểm soát truy cập phương tiện truyền thông
OFDM	Orthogonal Frequency Division Multiplex	Ghép kênh phân chia theo tần số
PDA	Personal Digital Associasion	Thiết bị kỹ thuật số hỗ trợ cá nhân
WIFI	Wireless Fidelity	Hệ thống mạng không dây chuẩn 802.11
WLAN	Wireless Local Area Network	mạng cục bộ không dây

DANH MỤC BẢNG BIỂU

DANH MỤC HÌNH VẼ

MỞ ĐẦU

Trong bối cảnh cách mạng công nghiệp 4.0 đang diễn ra mạnh mẽ cùng với sự phát triển của các phương tiện truyền tải thông tin liên lạc và nhu cầu cập nhật, trao đổi thông tin ở mọi lúc mọi nơi đang trở nên thiết yếu trong mọi lĩnh vực của đời sống xã hội đã góp phần thúc đẩy sự phát triển các hệ thống mạng viễn thông di động, và mạng không dây. Trong số này phải kể đến mạng không dây WLAN với hàng loạt chuẩn mạng mới được phát triển, tiêu biểu là IEEE 802.11. WLAN với nhiều lợi thế như dễ kết nối, tính cơ động cao, chi phí để sử dụng cộng nghệ mạng không quá đắt đỏ. Và khi công nghệ mạng không dây được cải thiện, thì chi phí phần cứng cũng thấp hơn giúp cho số lượng người cài đặt mạng không dây sẽ tăng cao hơn, khả năng ứng dụng rộng rãi hơn, nên việc nghiên cứu mạng WLAN thực sự là cần thiết. Tuy nhiên, việc nghiên cứu và triển khai ứng dụng công nghệ WLAN, cần phải quan tâm tới tính bảo mật an toàn thông tin. Do môi trường truyền dẫn là truyền dẫn vô tuyến nên WLAN rất dễ bị rò rỉ thông tin và đặc biệt là các nguy cơ bị xâm nhập trái phép. Do đó, cùng với sự phát triển của WLAN cần phải quan tâm phát triển các khả năng bảo mật WLAN, cung cấp thông tin hiệu quả, tin cậy cho người sử dụng. Đồng thời trên cơ sở nghiên cứu xem xét thực trạng vấn đề bảo vệ ngăn chặn xâm nhập trái phép của mạng WLAN, đưa ra giải pháp bảo mật mạng WLAN một cách hiệu quả và phù hợp nhất nhằm tăng hiệu năng mạng.

Do đó, cùng với sự phát triển của WLAN chúng ta phải quan tâm phát triển các khả năng bảo mật WLAN an toàn, cung cấp thông tin hiệu quả, tin cậy cho người sử dụng. Đồng thời trên cơ sở nghiên cứu xem xét thực trạng vấn đề bảo vệ ngăn chặn xâm nhập trái phép của mạng WLAN, đề xuất ứng dụng giải pháp bảo mật mạng WLAN một cách hiệu quả và phù hợp nhất nhằm tăng hiệu năng. Chính vì những lý do trên, học viên quyết định chọn đề tài: "***Phân tích và thiết kế tăng hiệu năng hệ thống mạng Wifi tại Trường Cao đẳng Lý Thái Tổ***" làm luận văn thạc sỹ. Trong suốt quá trình nghiên cứu và triển khai đề tài, học viên nhận thấy vấn đề hiệu năng của một hệ thống mạng là vô cùng quan trọng vì nó cho chúng ta biết

được khả năng đáp ứng cũng như hiệu quả cụ thể khi người sử dụng tham gia vào hệ thống mạng. Dựa trên thực tế hệ thống mạng của Cao đẳng Lý Thái Tổ trong nội dung chương 3 của luận văn học viên đã đi sâu và phân tích kỹ lưỡng các kỹ thuật để nhằm tăng hiệu năng cho mạng WLAN của trường một cách hiệu quả nhất.

Nội dung chính của luận văn gồm:

Chương I. Tổng quan chung về mạng không dây - WLAN

Chương II. Các vấn đề bảo mật trong mạng, yếu tố ảnh hưởng đến hiệu năng trong mạng WLAN

Chương III. Phân tích, mô phỏng tăng hiệu năng mạng cho hệ thống mạng WLAN Trường Cao đẳng Lý Thái Tổ

CHƯƠNG 1: TỔNG QUAN CHUNG VỀ MẠNG KHÔNG DÂY WLAN

1.1 Khái niệm và lịch sử hình thành mạng WLAN

WLAN là từ viết tắt của (Wireless Local Area Network) có nghĩa là Mạng cục bộ không dây, nó là phương thức kết nối không dây cho hai hoặc nhiều thiết bị sử dụng sóng radio tần số cao và thường bao gồm một điểm truy cập đến Internet.

Nhìn chung, mạng cục bộ không dây (WLAN) cung cấp liên lạc mạng không dây trong khoảng cách ngắn bằng cách sử dụng tín hiệu radio hoặc hồng ngoại thay vì cáp mạng truyền thống. Mạng WLAN là một loại mạng cục bộ (LAN). Mạng WLAN cho phép người dùng di chuyển xung quanh khu vực phủ sóng, thường là nhà hoặc văn phòng nhỏ, trong khi vẫn duy trì kết nối mạng.

Mạng không dây ngày nay bắt nguồn từ các giai đoạn phát triển của thông tin vô tuyến và những ứng dụng điện báo và radio. WLAN là công nghệ mạng do phía quân đội triển khai đầu tiên vào những năm 1990. Bởi vì họ cần một phương tiện đơn giản và dễ dàng, có thể bảo mật được sự trao đổi thông tin trong chiến tranh.

Thời điểm các nhà sản xuất giới thiệu sản phẩm hoạt động dưới băng tần 900MHz và tốc độ truyền dữ liệu khi đó là 1Mbps, thấp hơn rất nhiều so với tốc độ 10Mbps của hầu hết các mạng sử dụng cáp đương thời. Nhưng sự phát triển nổi bật của công nghệ WLAN đạt được vào kỷ nguyên của công nghệ điện tử và chịu ảnh hưởng lớn của nền kinh tế hiện đại, cũng như các khám phá khoa học trong lĩnh vực vật lý học.

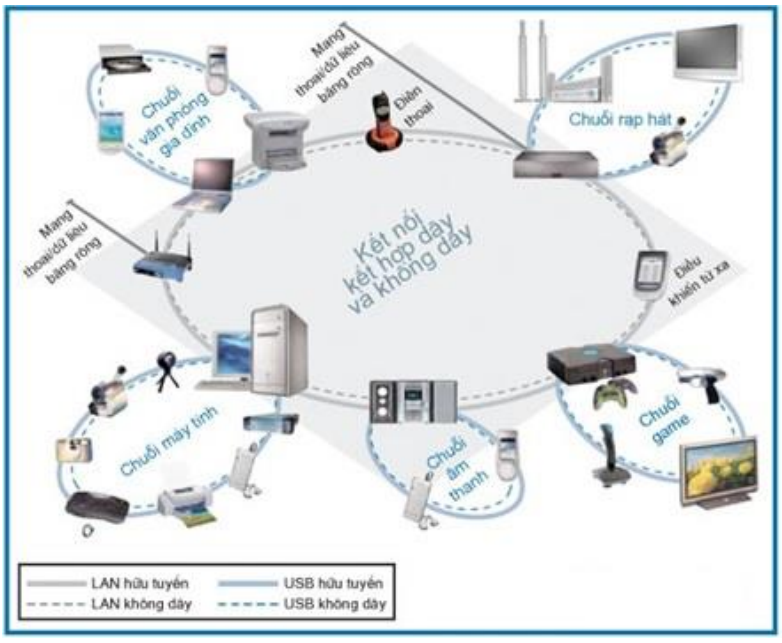
Năm 1992, các nhà sản xuất bắt đầu đưa ra những sản phẩm sử dụng băng tần 2,4 Ghz, có tốc độ truyền dữ liệu cao hơn. Tuy nhiên chúng là những giải pháp của riêng từng nhà sản xuất và chưa được công bố rộng rãi. Để thống nhất hoạt động giữa các thiết bị ở những dải tần khác nhau một số tổ chức quốc tế bắt đầu phát triển những chuẩn mạng không dây chung.

Năm 1997, IEEE đã phê chuẩn 802.11 và cũng được gọi với tên WIFI cho các mạng WLAN.

Năm 1999, IEEE bổ sung cho chuẩn 802.11 hai phương pháp truyền tín hiệu là các chuẩn 802.11a và 802.11b. Các thiết bị 802.11b truyền phát ở tần số 2,4GHz, cung cấp tốc độ truyền tín hiệu có thể lên tới 11Mbps, và 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.

Đầu năm 2003, IEEE công bố thêm một chuẩn nữa là 802.11g có thể truyền nhận thông tin ở cả hai dải tần 2,4GHz và 5GHz. Chuẩn 802.11g có thể nâng tốc độ truyền dữ liệu lên tới 54Mbps. Hơn thế nữa, những sản phẩm sử dụng chuẩn 802.11g cũng có thể tương thích với những thiết bị chuẩn 802.11b.

Cuối năm 2009, chuẩn 802.11n đã được IEEE phê duyệt đưa vào sử dụng chính thức và được Hiệp hội Wi-Fi (Wi-Fi Alliance) kiểm định và cấp chứng nhận cho các sản phẩm đạt chuẩn. Mục tiêu chính của công nghệ này là tăng tốc độ truyền và tầm phủ sóng cho các thiết bị bằng cách kết hợp các công nghệ vượt trội và tiên tiến nhất.



Hình 1.1: Sơ đồ mạng LAN phổ biến

1.2 Các tiêu chuẩn mạng thông dụng của WLAN

1.2.1 Tiêu chuẩn 802.11

Đây là chuẩn đầu tiên của hệ thống mạng không dây. Tốc độ truyền khoảng từ 1 đến 2 Mbps, hoạt động ở băng tần 2.4GHz. Chuẩn này chứa tất cả công nghệ truyền tải hiện hành bao gồm trải phổ chuỗi trực tiếp (DSS), trải phổ nhảy tần (FHSS) và hồng ngoại. Chuẩn 802.11 là một trong hai chuẩn miêu tả những thao tác của sóng truyền (FHSS) trong hệ thống mạng không dây. IEEE 802.11 bao gồm các chuẩn sau:

1.2.2 Tiêu chuẩn 802.11a

Chuẩn này được IEEE bổ sung và phê duyệt vào tháng 9 năm 1999, sử dụng cùng giao thức lớp liên kết dữ liệu (Data Link Layer) và định dạng frame như các chuẩn ban đầu 802.11-1997, nhưng dùng kỹ thuật OFDM (Orthogonal Division Multiplixing) cho truyền dẫn lớp vật lý. Dãi tần hoạt động của nó là băng tần 5GHz và có tốc độ truyền dẫn tối đa 54Mbps. Do dải tần 2.4GHz đã trở nên quá tải (nhiều thiết bị dân dụng cũng sử dụng chung dải tần này) nên việc sử dụng chuẩn 802.11a mang lại một lợi thế đáng kể. Tuy nhiên, phạm vi phủ sóng hiệu quả của 802.11a trong dãi tần 5GHz là thấp hơn so với các chuẩn giao thức 802.11b/g/n trong dãi tần 2,4GHz, do bởi tín hiệu hoạt động ở dãi tần cao hơn sẽ dễ dàng bị hấp thụ bởi các vật thể rắn hơn như tường, thép, cây cối… Tuy nhiên, chuẩn 802.11a và 802.11n lại ít chịu ảnh hưởng của nhiễu trong dãi tần 5GHz, do đó nhiều lúc chúng lại có phạm vi phủ sóng tương tự hoặc thậm chí lớn hơn 802.11b/g/n.

1.2.3 Tiêu chuẩn 802.11b

Là chuẩn mạng không dây 802.11 đầu tiên được áp dụng rộng rãi. chuẩn hoạt động ở băng tần 2.4 GHz, 11 Mbps, xác định môi trường truyền dẫn DSSS với các tốc độ dữ liệu 11 Mbit/s, 5,5 Mbit/s, 2Mbit/s và 1 Mbit/s, nó chịu ảnh hưởng rất nhiều từ nhiễu do hoạt động cùng tần số với những thiết bị dân dụng khác như các thiết bị Bluetooth, điện thoại không dây DECT và VoIP, lò vi sóng… Dải hoạt động

của hệ thống khoảng có phạm vi phát sóng trong nhà từ 100 đến 150 feet (1 feet = 0,308m) và tốc độ truyền lý thuyết tối đa là 11 Mbps nhưng trên thực tế chỉ đạt tối đa là 4 đến 6 Mbps. Ở Mỹ, thiết bị hoạt động ở dãy tần này không phải đăng ký.

1.2.4 Tiêu chuẩn 802.11g

802.11g là bước cải tiến kế tiếp từ 802.11b và các hệ thống tuân theo chuẩn này hoạt động ở băng tần 2,4 GHz và có thể đạt tới tốc độ 54 Mbit/s. Giống như IEEE 802.11a, IEEE 802.11g còn sử dụng kỹ thuật điều chế OFDM để có thể đạt tốc độc cao hơn.

Ngoài ra, các hệ thống tuân thủ theo IEEE 802.11g có khả năng tương thích ngược với các hệ thống theo chuẩn IEEE 802.11b vì chúng thực hiện tất cả các chức năng bắt buộc của IEEE 802.11b. Đây là chuẩn công nghiệp tiếp theo và một lần nữa được áp dụng rộng rãi cho các ứng dụng mạng WLAN do tốc độ truyền tải dữ liệu tăng lên.

Tương tự như 802.11b, các thiết bị 802.11g đều có thể bị ảnh hưởng xuyên nhiễu từ những thiết bị dân dụng khác hoạt động trên dãi tần 2.4GHz. Kỹ thuật OFDM được cho phép tại những tốc độ trên 20Mbps làm tăng đáng kể khả năng NLoS (Non-Line-of-Sight).

1.2.5 Tiêu chuẩn 802.11n

Chuẩn 802.11n đã được IEEE phê duyệt đưa vào sử dụng chính thức và cũng đã được Hiệp hội Wi-Fi (Wi-Fi Alliance) kiểm định và cấp chứng nhận cho các sản phẩm đạt chuẩn. Các yêu cầu cơ bản như: băng tần, tốc độ, các định dạng khung, khả năng tương thích ngược không thay đổi.

Về lý thuyết, chuẩn 802.11n cho phép kết nối với tốc độ 300 Mbps, tức là chuẩn này nhanh hơn khoảng 6 lần tốc độ đỉnh theo lý thuyết của các chuẩn trước đó như 802.11g/a (54 Mbps) và mở rộng vùng phủ sóng. 802.11n là mạng Wi-Fi đầu tiên có thể ứng dụng cạnh tranh với mạng có dây 100Mbps về mặt hiệu suất. Chuẩn 802.11n hoạt động ở cả hai tần số 2,4GHz và 5GHz, Nó có thể lên đến

600Mbps (trên lý thuyết) khi truyền đồng thời trên 4 luồng dữ liệu và độ rộng kênh 40MHz. Vì vậy 802.11n đang trở thành tiêu chuẩn phổ biến hiện nay.

1.2.6 Tiêu chuẩn 802.11ac

Là chuẩn Wifi mới nhất được IEEE giới thiệu, chuẩn ac có hoạt động ở băng tầng 5 GHz, với kỹ thuật OFDM và tốc độ tối đa lên đến 1730Mbps. Chuẩn được phát triển mở rộng từ chuẩn 802.11n cho các kênh với băng thông rộng RF (lên đến 160MHz, 80Mhz bắt buộc), hơn thế nữa luồng dữ liệu được truyền đi với công nghệ đa Anten lên đến 8 luồng dữ liệu (Spatial streams), nhiều người dùng MIMO (multi-user MIMO) và dùng cho nơi có mật độ người dùng cao (lên đến 256-QAM).

Chuẩn Wi-Fi 802.11ac còn có thể được áp dụng để truyền dữ liệu giữa các thiết bị trong một mạng nội bộ hoặc mạng gia đình với tốc độ cao hơn hiện nay. Một ứng dụng dễ thấy nhất là để stream video Full-HD. Trong một đợt trình diễn, hãng Netgear đã sử dụng router 802.11ac của họ để truyền 4 bộ phim Full-HD cùng lúc đến bốn chiếc HDTV khác nhau, điều không thể làm được với chuẩn Wi-Fi hiện nay. Nó giúp quá trình sao chép dữ liệu giữa máy tính, điện thoại thông minh, máy tính bảng với ổ cứng mạng cũng như giữa các thiết bị với nhau được nhanh hơn (về mặt lý thuyết là tốn 1/3 thời gian so với chuẩn 802.11n). Và thời gian chờ đợi ngắn hơn kéo theo thời lượng pin sẽ dài hơn bởi năng lượng tiêu thụ ít hơn.

1.2.7 Tiêu chuẩn 802.11ad

Chuẩn mạng vô tuyến 802.11ad mới cung cấp siêu thông lượng và năng lực mạng. Chuẩn 802.11ad cung cấp tốc độ thông lượng chưa từng có lên tới 7Gbps (Theo lý thuyết, đường truyền wifi theo chuẩn 802.11ad có thể đạt tới tốc độ 7Gbps hay thậm chí là 32Gbps cho 802.11ad chuẩn 2). Tuy nhiên, chuẩn wifi mới này có một khuyết điểm. Do cường độ cao nên tầm phủ sóng của nó khá hẹp, hẹp hơn nhiều so với những chuẩn wifi cũ. Để kết nối với modem sử dụng chuẩn wifi 802.11ad, người dùng phải ở gần thiết bị.

Chuẩn 802.11ad đầu tiên được phát triển bởi Liên minh vô tuyến Gigabit (Wireless Gigabit Alliance), nhưng sau đó tổ chức này sáp nhập với Liên minh WiFi (WiFi Alliance), chịu trách nhiệm trước mỗi chuẩn WiFi chính được đưa ra, bao gồm 802.11b,g,a,n, và ac. Hiện nay, Liên minh WiFi đã thiết đặt phát hành một bộ đặc tả kỹ thuật giao thức 802.11ad vào đầu năm 2014, khả năng sẽ trở thành xu hướng chính cho cả người dùng và doanh nghiệp.

CÁC CHUẨN WIFI 802.11					
Chuẩn IEEE	802.11a	802.11b	802.11g	802.11n	802.11ac
Năm phát hành	1999	1999	2003	2009	2013
Tần số	5 GHz	2.4 GHz	2.4 GHz	2.4/5 GHz	5 GHz
Tốc độ tối đa	54 Mbps	11 Mbps	54 Mbps	600 Mbps	1 Gbps
Phạm vi trong nhà	100 ft.	100 ft.	125 ft.	225 ft.	90 ft.
Phạm vi ngoài trời	400 ft.	450 ft.	450 ft.	825 ft.	1,000 ft.

Bảng 1.1: Bảng tổng hợp các chuẩn WiFi 802.11 thông dụng

1.2.8 Một số tiêu chuẩn khác

Ngoài các chuẩn phổ biến trên, IEEE còn lập các nhóm làm việc độc lập để bổ sung các quy định vào các chuẩn 802.11a, 802.11b, và 802.11g nhằm nâng cao tính hiệu quả, khả năng bảo mật và phù hợp với các chuẩn cũ như:

- IEEE 802.11c: Bổ sung việc truyền thông và trao đổi thông tin giữa LAN qua cầu nối lớp MAC với nhau.

- 802.11ah - tạo ra các mạng Wifi có phạm vi mở rộng vượt ra ngoài tầm của mạng 2.4-5GHz thông thường.

- 802.11aj - được phê chuẩn năm 2017, được sử dụng chủ yếu ở Trung Quốc.

- 802.11ax - đang chờ được phê chuẩn, dự là trong năm 2018, nếu được thông qua đây chính là chuẩn Wifi 6 đang được mọi người mong chờ.

- 802.11ay - đang chờ được phê chuẩn, dự là trong năm 2019.

- 802.11F - Inter-Access Point Protocol, được đề xuất cho giao tiếp giữa các điểm truy cập để hỗ trợ roaming client (2003).

- 802.11T - dự đoán Hiệu suất Không dây.

Các chuẩn IEEE 802.11F và 802.11T được viết hoa chữ cái cuối cùng để phân biệt đây là hai chuẩn dựa trên các tài liệu độc lập, thay vì là sự mở rộng / nâng cấp của 802.11, và do đó chúng có thể được ứng dụng vào các môi trường khác 802.11 (chẳng hạn WiMAX – 802.16).

Trong khi đó, 802.11x sẽ không được dùng như một tiêu chuẩn độc lập mà sẽ bỏ trống để trỏ đến các chuẩn kết nối IEEE 802.11 bất kì. Nói cách khác, 802.11 có ý nghĩa là "mạng cục bộ không dây", và 802.11x mang ý nghĩa "mạng cục bộ không dây theo hình thức kết nối nào đó (a/b/g/n/ac)".

1.3 Cấu trúc và mô hình mạng WLAN

Mạng sử dụng chuẩn 802.11 gồm có 4 thành phần chính:

- Hệ thống phân phối (Distribution System - DS).
- Điểm truy cập (Access Point).
- Môi trường truyền tải vô tuyến (Wireless Medium).
- Trạm (Stations).

Hình 1.2: Cấu trúc cơ bản của một mạng WLAN.

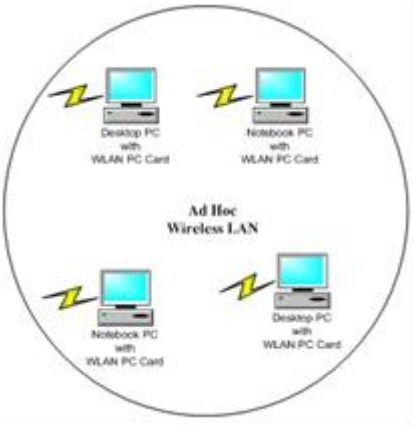
Mạng WLAN gồm 3 mô hình cơ bản như sau:

- Mô hình mạng độc lập (IBSS) hay còn gọi là mạng phi liên kết (Ad hoc).
- Mô hình mạng cơ sở (BSS).
- Mô hình mạng mở rộng (ESS).

1.3.1 Mô hình mạng độc lập IBSS hay còn gọi là mạng Ad-hoc

Các trạm (máy tính có hỗ trợ card mạng không dây) tập trung lại trong một không gian nhỏ để hình thành nên kết nối ngang cấp (peer-to-peer) giữa chúng. Các nút di động có card mạng wireless là chúng có thể trao đổi thông tin trực tiếp với nhau, không cần phải quản trị mạng.

- **Ưu điểm**: Kết nối Peer-to-Peer không cần dùng Access Point, yêu cầu cấu hình thấp và cài đặt đơn giản, chi phí thấp.
- **Khuyết điểm**: Khoảng cách kết nối giữa các máy trạm bị giới hạn, số lượng người dùng cũng bị giới hạn, không tích hợp được cùng hệ thống mạng có dây sẵn có.



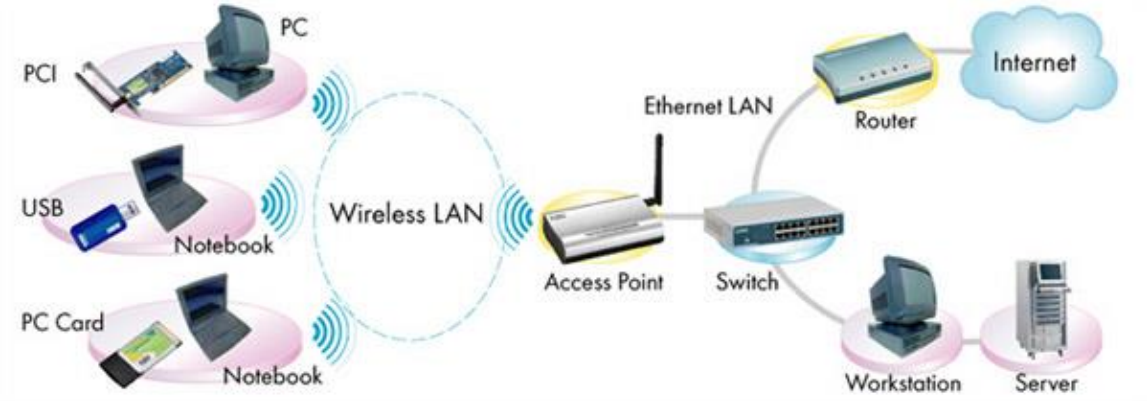
Hình 1.3: Mô hình mạng Ad-hoc

1.3.2 Mô hình mạng cơ sở BSS

Trong mô hình mạng cơ sở, các Client muốn liên lạc với nhau phải thông qua Access Point (AP). AP là điểm trung tâm quản lý giao tiếp trong mạng, khi đó các

Client (máy trạm) không thể liên lạc trực tiếp với như trong mạng độc lập. Để giao tiếp với nhau các Client phải gửi các khung dữ liệu đến AP, sau đó AP sẽ gửi đến máy nhận.

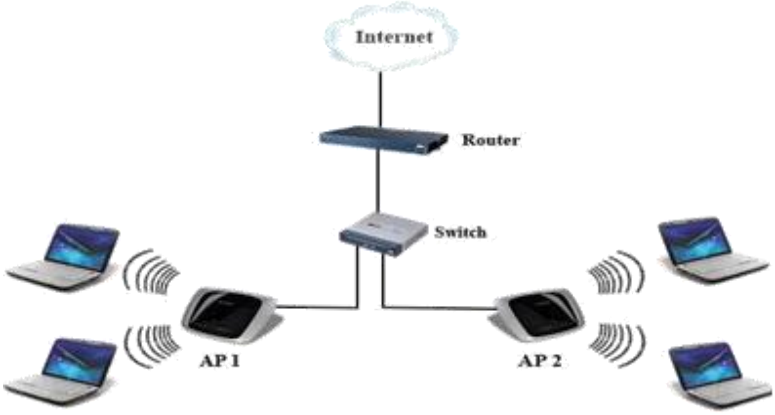
- **Ưu điểm:** Các Client (máy trạm) không kết nối trực tiếp được với nhau, các máy trạm trong mạng không dây có thể kết nối với hệ thống mạng có dây.
- **Khuyết điểm:** Giá thành cao, cài đặt và cấu hình phức tạp.



Hình 1.4: Mô hình mạng cơ sở

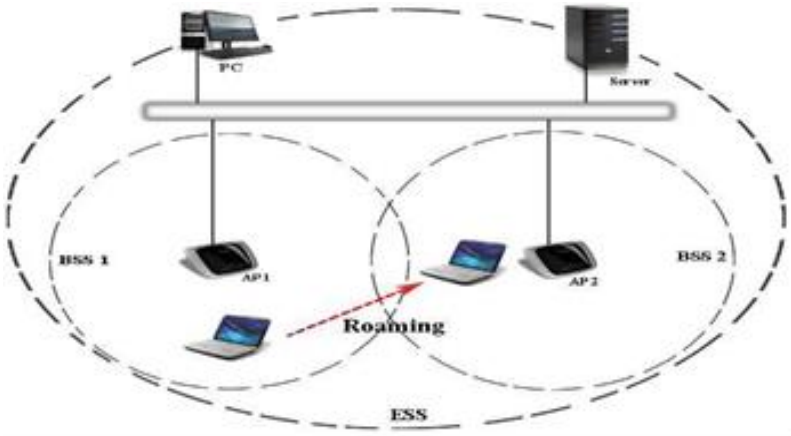
1.3.3 Mô hình mạng mở rộng ESS

Nhiều mô hình mạng cơ sở BSS kết hợp với nhau gọi là mô hình mạng ESS. Là mô hình sử dụng từ 2 AP trở lên để kết nối mạng. Khi đó các AP sẽ kết nối với nhau thành một mạng lớn hơn, có phạm vi phủ sóng rộng hơn, thuận lợi và đáp ứng tốt cho các Client di động.

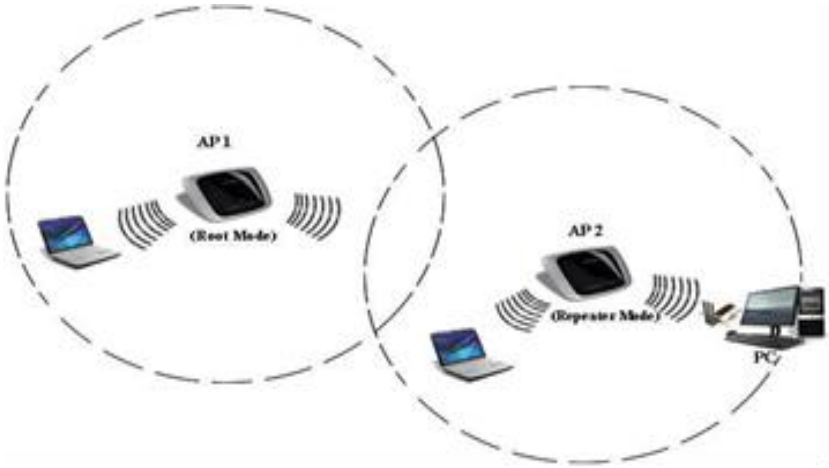


Hình 1.5: Mô hình mạng mở rộng

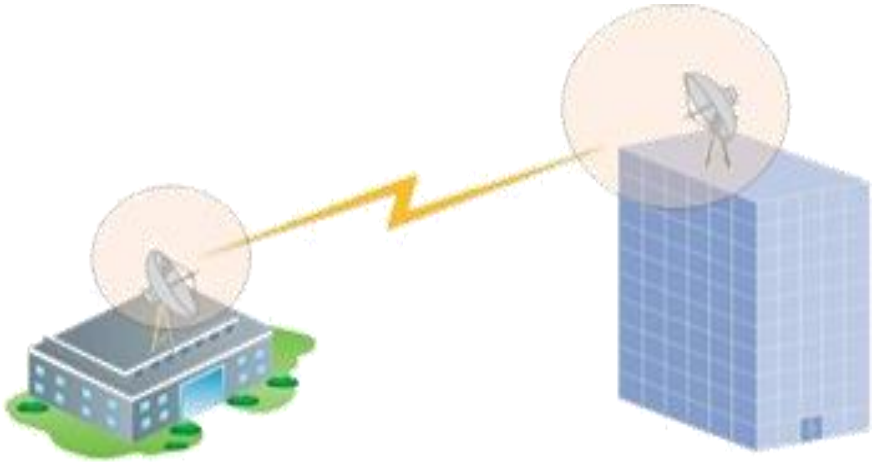
1.3.4 Một số mô hình mạng WLAN khác



Hình 1.6: Mô hình chuyển tiếp



Hình 1.7: Mô hình khuyếch đại tín hiệu



Hình 1.8: Mô hình điểm - điểm

Hình 1.9: Mô hình điểm - đa điểm

1.4 Đánh giá ưu, nhược điểm và thực trạng mạng WLAN hiện nay

1.4.1 Ưu điểm

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

- **Khả năng lưu động cải thiện hiệu suất và dịch vụ:** Các hệ thống mạng WLAN cung cấp cho sự truy cập thông tin thời gian thực tại bất cứ đâu cho người dùng mạng trong khu vực được thiết lập. Khả năng lưu động này hỗ trợ các yêu cầu về hiệu suất và dịch vụ mà mạng nối dây không thể triển khai thực hiện được.
- **Cài đặt đơn giản:** Cài đặt hệ thống mạng WLAN nhanh và dễ dàng.
- **Linh hoạt trong cài đặt:** Công nghệ không dây cho phép kết nối mạng đến các vị trí mà mạng nối dây không thể triển khai.
- **Giảm bớt giá thành sở hữu:** Giá thành đầu tư ban đầu hệ thống phần cứng cho mạng WLAN có giá thành cao hơn các hệ thống phần cứng mạng LAN hữu tuyến, nhưng chi phí cài đặt toàn bộ và giá thành trong quá trình sử dụng bảo dưỡng, sửa chữa thấp hơn đáng kể.

- **Tính linh hoạt:** Các hệ thống mạng WLAN được định hình cấu trúc theo các kiểu liên kết mạng khác nhau tùy thuộc các nhu cầu của các ứng dụng và các cài đặt cụ thể. Cấu hình mạng dễ dàng thay đổi từ các mạng độc lập phù hợp với số lượng nhỏ người dùng đến các mạng cơ sở hạ tầng với hàng nghìn người dùng trong một vùng rộng lớn.
- **Khả năng mở rộng:** Khả năng mở rộng của mạng không dây có thể đáp ứng tức thì khi gia tăng số lượng người sử dụng.

1.4.2 Nhược điểm

Công nghệ mạng LAN không dây, ngoài những tính năng và những ưu điểm được đề cập ở trên thì cũng có các nhược điểm như:

- **Bảo mật:** Môi trường truyền dẫn không dây là không gian tự do, nên khả năng bị tấn công vào hệ thống, người dùng là rất cao.
- **Phạm vi:** Với chuẩn mạng 802.11 mới nhất hiện nay, phạm vi ứng dụng của mạng WLAN đã có sự thay đổi lớn. Tuy nhiên nó vẫn chưa thể đáp ứng được hết nhu cầu của người dùng. Để mở rộng phạm vi vùng phục vụ cần phải trang bị thêm bộ lập hay điểm truy cập, dẫn đến chi phí gia tăng. Với những mô hình mạng lớn vẫn phải kết hợp với mạng hữu tuyến có dây.
- **Độ tin cậy:** Vì sử dụng sóng vô tuyến để truyền dẫn nên việc bị nhiễu, tín hiệu bị suy giảm do tác động của vật cản và các thiết bị khác (tường bê tông, lò vi sóng, tín hiệu radio…) là không tránh khỏi. Làm giảm đáng kể hiệu quả, phạm vi đáp ứng hoạt động của mạng.
- **Tốc độ:** Tốc độ của mạng không dây với các chuẩn mới đã có cải thiện tuy nhiên vẫn còn rất chậm so với mạng sử dụng cáp (100 Mbps đến hàng Gbps).

1.4.3 Thực trạng mạng WLAN hiện nay

Trong những năm vừa qua cùng với sự phát triển mạnh mẽ của Internet và các thiết bị mạng, sự phát triển của kinh tế thị trường, nhu cầu trao đổi thông tin và

dữ liệu của con người là rất lớn. Mạng WLAN hiện nay đã trở nên phổ biến và rất gần gũi trong cuộc sống. Chúng ta có thể dễ dàng kết nối sử dụng mạng không dây tại nhiều địa điểm như: cơ quan, trường học, văn phòng, quán Cafe, khu vui chơi giải trí… hoặc ngay tại nhà bằng nhiều thiết bị hiện đại như: Tivi, laptop, PDA, các thiết bị adroid. Tuy nhiên, vẫn còn một số tồn tại như:

- ✓ **Không thay đổi mật khẩu của nhà sản xuất:** Khi cầu hình các hầu hết đều không thay đổi mật khẩu truy cập của nhà sản xuất. Router rất dễ bị xâm nhập và thay đổi cấu hình.
- ✓ **Không kích hoạt các tính năng mã hóa:** khi tính năng không được kích hoạt, rất có thể dùng một số phần mềm dò mật khẩu để lấy những thông tin phục vụ cho những ý đồ xấu.
- ✓ **Kích hoạt phương pháp bảo mật cấp thấp hoặc không kích hoạt:** Hiện nay một số hệ thống mạng đang sử dụng không hề kích hoạt bất kỳ chế độ bảo mật nào. Hoặc nếu có kích hoạt thì cũng chỉ kích hoạt chế độ bảo mật ở cấp thấp như VD: WEP. Điều này hoàn toàn không nên. Người ngoài mạng có thể xâm nhập bẻ khóa và truy cập vào mạng [2] [3].

1.5 Kết luận Chương 1

Chương này giúp cho chúng ta có một cái nhìn tổng thể về sự phát triển của mạng không dây, các công nghệ ứng dụng trong mạng không dây. Chúng ta có thể hiểu một cách khái quát cơ chế hoạt động của mạng WLAN, ưu, nhược điểm cũng như các mô hình hoạt động của mạng WLAN.

Ngoài ra, chúng ta cũng tìm hiểu về chuẩn 802.11 và các thế hệ chuẩn mạng 802.11 thông dụng cho mạng WLAN, hiểu được những gì diễn ra trong quá trình thiết lập kết nối với một hệ thống WLAN đơn giản.

Trong chương tiếp theo chúng ta sẽ nghiên cứu thực trạng gây mất an ninh an toàn của mạng không dây, cách thức tấn công trong mạng không dây, các ứng dụng kỹ thuật mã hóa để bảo mật cho mạng không dây và một số giải pháp cho việc đảm bảo an ninh an toàn cho mạng không dây mà cụ thể là WLAN.

CHƯƠNG 2: CÁC VẤN ĐỀ BẢO MẬT, YẾU TỐ ẢNH HƯỞNG ĐẾN HIỆU NĂNG TRONG MẠNG WLAN

2.1 Khái quát bảo mật trong mạng cục bộ không dây WLAN

Trong mạng WLAN bảo mật là một trong những khuyết điểm lớn nhất. Do điều kiện môi trường truyền dẫn thông tin của loại mạng này, mà khả năng truy cập kết nối của các thiết bị ngoài trong phạm vi phát sóng là vô cùng lớn. Đồng thời, khả năng nhiễu sóng bởi các thiết bị điện tử cũng không thể tránh khỏi. Để an toàn trong sử dụng mạng WLAN, chúng ta cần phải bảo mật WLAN.

Kết nối mạng LAN hữu tuyến người ta sử dụng cần phải sử dụng dây cáp làm đường truyền, kết nối một điểm kết nối vào một cổng mạng. Với WLAN, người dùng chỉ cần sử dụng các thiết bị kết nối của họ trong vùng sóng phủ của mạng không dây. Việc quản lý các điểm kết nối trong mạng hữu tuyến là đơn giải. Vùng phủ sóng của mạng không dây (hay vô tuyến) sử dụng sóng vô tuyến có thể bao trùm ngoài phạm vi giới hạn không bên trong trụ sở hoặc toà nhà, người ngoài trong phạm vi phủ sóng có thể truy cập nhờ thiết bị thích hợp. Do đó mạng không dây có thể bị truy cập trái phép từ bên ngoài xâm nhập vào hệ thống để ăn cắp thông tin hoặc phá hoại. Giải pháp được đưa ra là phải làm sao để có thể bảo mật cho mạng này chống được việc truy cập theo kiểu này.

Hệ thống mạng sử dụng đường truyền dẫn hữu tuyến hoặc vô tuyến, đều có những lỗ hổng về mặt kỹ thuật điều này cho phép tin tặc xâm nhập vào hệ thống để lấy cắp thông tin hay phá hoại, do đó trên thực tế không có một hệ thống mạng nào được coi là bảo mật tuyệt đối. Vì vậy, người ta thường áp dụng nhiều kỹ thuật bảo mật đi kèm với các mạng để bảo đảm an toàn cho mạng. Đối với mạng không dây có thể sử dụng các phương pháp mã hóa để bảo đảm tính bí mật của thông tin, sử dụng các cơ chế chứng thực để kiểm tra tính hợp pháp của người dùng.

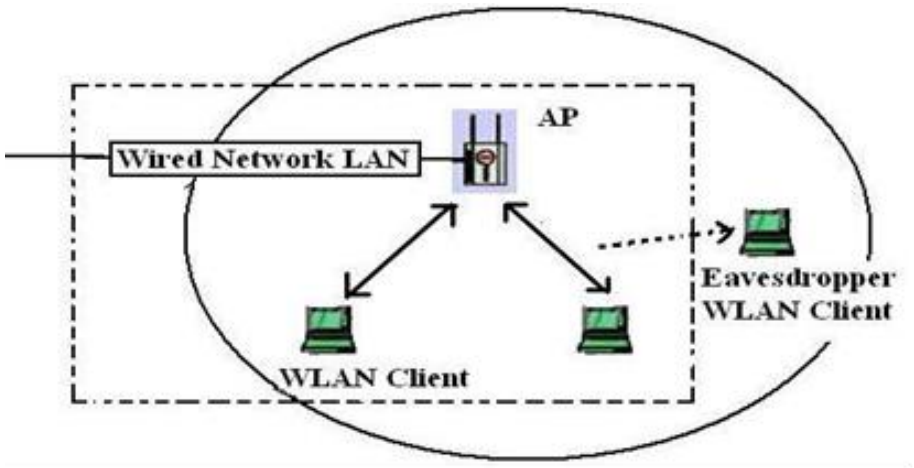
2.1.1 Những nguy cơ bảo mật trong mạng WLAN bao gồm:

- Mọi thiết bị đều có thể kết nối tới những điểm truy cập đang truyền tin SSID.
- Hacker sẽ cố gắng tìm kiếm các phương thức mã hoá đang được sử dụng trong quá trình truyền thông tin trên mạng, sau đó sử dụng phương thức giải mã riêng và lấy các thông tin nhạy cảm.
- Hacker có thể tấn công các kiến trúc mạng.

2.1.2 Vai trò của bảo mật mạng không dây WLAN

Bảo mật không dây vô cùng quan trọng. Đại đa số chúng ta đều kết nối một thiết bị di động, như điện thoại thông minh, máy tính bảng, máy tính xách tay, hoặc các thiết bị khác, với bộ định tuyến tại nhiều thời điểm trong ngày. Hơn nữa, các thiết bị Internet of Things cũng kết nối với Internet bằng WiFi.

Rõ ràng khi đã triển khai hệ thống mạng không dây thành công thì bảo mật là vấn đề kế tiếp cần được đặc biệt quan tâm, công nghệ và giải pháp bảo mật cho mạng WLAN hiện tại cũng đang gặp nhiều nan giải, rất nhiều giải pháp công nghệ đã được phát triển rồi đưa ra nhằm bảo vệ an toàn cho dữ liệu của hệ thống và người dùng. Nhưng bằng những công cụ phần mềm chuyên dùng thì các Hacker dễ dàng phá vỡ sự bảo mật này. Trong trường hợp bị tấn công gây mất an toàn về dữ liệu thì tổn thất về uy tín là rất lớn và có thể để lại hậu quả lâu dài.



Hình 2.1: Truy cập trái phép vào mạng không dây

Bởi vì mạng Wireless truyền và nhận dữ liệu dựa trên sóng radio và vì AP phát sóng lan truyền trong bán kính vùng phủ cho phép nên bất cứ thiết bị nào có hỗ trợ truy cập Wireless đều có thể bắt sóng này, sóng Wireless có thể truyền xuyên qua các vật liệu như bê tông, nhựa, sắt,. Cho nên rủi ro thông tin bị các Hacker "mũ đen" phá hoại hoặc nghe lén rất cao, vì hiện tại có rất nhiều công cụ hỗ trợ cho việc nhận biết và phân tích thông tin của sóng Wireless sau đó dùng thông tin này có thể dò khoá WEP (như AirCrack, AirSnort).

Vì dữ liệu được truyền qua sóng vô tuyến không phải qua các đường truyền dây mạng LAN hữu tuyến nên tính bảo mật của WLAN cần phải giải quyết được các vấn đề sau đây:

- Ngăn chặn thông tin người dùng bị tấn công khi thực hiện quá trình đàm phán xác thực thông tin truy cập vào mạng.
- Sau khi chứng thực hoàn tất thì phải bảo đảm sự an toàn riêng tư dữ liệu được truyền đi giữa máy khách và điểm truy cập.
- Kiểm tra chắc chắn rằng người dùng được phép truy cập vào mạng.

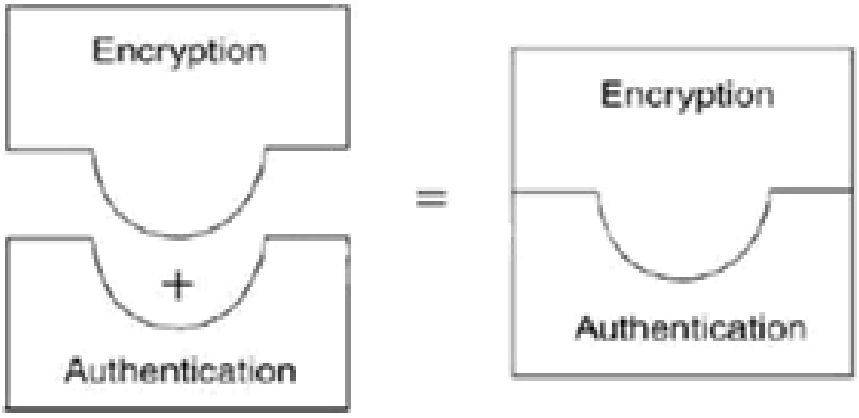
Rõ ràng khi truy cập vào mạng không dây luôn tiềm ẩn tồn tại những nguy hiểm về mặt xác thực và dữ liệu giao tiếp. Khi bắt đầu giao tiếp thì cần xác định quyền giao tiếp để tránh người dùng không được phép truy cập vào và sử dụng các hình thức tấn công hệ thống mạng. Khi đã xác thực thành công thì các nhà quản trị và hệ thống mạng cần là quản lý việc giao tiếp giữa các máy khách với nhau và với điểm truy cập sao cho tính riêng tư về dữ liệu được an toàn tuyệt đối và việc phá hoại từ các máy khách được kiểm soát. Đối với người sử dụng phải đảm bảo rằng mình đang truy cập vào một điểm truy cập đáng tin cậy, các dữ liệu trong thiết bị sử dụng vẫn được đảm bảo an toàn tuyệt đối để không có sự truy cập bất hợp pháp.

2.1.3 Mô hình chung của bảo mật mạng không dây WLAN

Như rất nhiều tài liệu nghiên cứu về bảo mật trong mạng Wireless thì để có thể bảo mật tối thiểu, người sử dụng và hệ thống WLAN cần có 2 thành phần sau:

- ***Authentication*** - chứng thực cho người dùng: quyết định cho ai có thể sử dụng mạng WLAN.
- ***Encryption*** - mã hóa dữ liệu: cung cấp tính bảo mật dữ liệu.

Authentication + Encryption = **Wireless Security**.



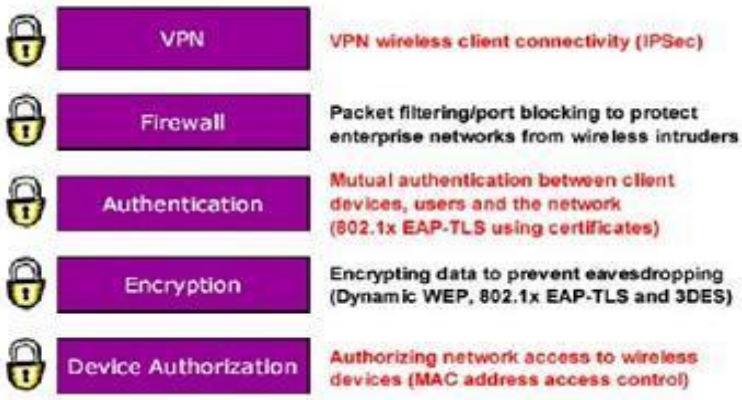
Hình 2.2: Bảo mật mạng không dây Wlan

Để bảo mật mạng WLAN, cần thực hiện qua các bước:

Authentication → Encryption → IDS & IPS.

- Chỉ có những người dùng được xác thực mới có khả năng truy cập vào mạng thông qua các Access Point.
- Các phương thức mã hoá được áp dụng trong quá trình truyền các thông tin quan trọng.
- Bảo mật các thông tin và cảnh báo nguy cơ bảo mật bằng hệ thống phát hiện xâm nhập (IDS) và hệ thống ngăn chặn xâm nhập (IPS). Xác thực và bảo mật dữ liệu bằng cách mã hoá thông tin truyền trên mạng [7].

Kiến trúc WLAN hỗ trợ mô hình bảo mật mở và toàn diện dựa trên chuẩn công nghiệp như thể hiện ở hình dưới. 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.



Hình 2.3: Mô hình bảo mật cho mạng không dây

Device Authorisation: Các Client (máy khách) không dây có thể bị ngăn chặn theo địa chỉ MAC của họ (địa chỉ phần cứng). EAS (một loại Access Server điều khiển việc truy cập- cung cấp sự điều khiển, quản lý các đặc tính bảo mật tiên tiến cho mạng không dây, duy trì một cơ sở dữ liệu của các Client không dây được cho phép và các AP riêng biệt khóa hay thông lưu lượng phù hợp).

Encryption: WLAN cũng hỗ trợ WEP, 3DES và chuẩn TLS sử dụng mã hóa để tránh người truy cập trộm.

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 các cấu hình lọc tùy chỉnh và tường lửa trên cổng dựa trên các chuỗi Linux IP. Việc cấu hình từ trước cho phép các loại lưu lượng chung được cho phép hay không cho phép.

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

2.2. Nguy cơ mất an ninh mạng

2.2.1 Những nguy hiểm cho an ninh mạng

Bảo mật là sự hạn chế khả năng lạm dụng tài nguyên và tài sản. Bảo mật trở nên đặc biệt phức tạp trong quản lý, vận hành những hệ thống thông tin có sử dụng các công cụ tin học, nơi có thể xảy ra và lan tràn nhanh chóng việc lạm dụng tài nguyên (các thông tin di chuyển vô hình trên mạng hoặc lưu trữ hữu hình trong các vật liệu) và lạm dụng tài sản (các máy tính, thiết bị mạng, thiết bị ngoại vi, các phần mềm của cơ quan hoặc người sở hữu hệ thống). Hạn chế ở đây có ý rằng không thể triệt phá hết ngay việc lạm dụng, cho nên cần sẵn sàng đề phòng mọi khả năng xấu với các phương cách thích hợp và chuẩn bị xử lý các sự cố nếu có việc lạm dụng xảy ra.

Kẻ tấn công trực tiếp có thể sử dụng công cụ để tấn công hoặc dùng kỹ thuật riêng để tấn công phá hoại, lấy cắp thông tin. Đây chính là bước hacker thu thập mã số tài khoản ngân hàng, tài khoản e-mail, tài khoản thẻ tín dụng, thông tin bí mật, hay mật khẩu hệ thống…của người hay tổ chức bị tấn công. Sau đó hacker sử dụng thông tin này để trục lợi hoặc có thể bán lại thông tin. Khi nắm được mật khẩu hệ thống trang tin, kẻ mạo danh có thể đăng nhập vào trang tin này và thay đổi nội dung trang tin.

Kẻ tấn công chiếm quyền sử dụng nhiều máy tính nối mạng, có thể bao gồm cả máy chủ. Các máy tính này có thể sử dụng để tấn công từ chối dịch vụ website nào đó cùng lúc. Khi có quá nhiều yêu cầu dịch vụ gửi đến cùng một lúc, băng thông tới website bị nghẽn, hệ thống máy chủ quá tải dẫn tới ngưng hoạt động.

2.2.2 Một số kiểu tấn công WLAN cơ bản

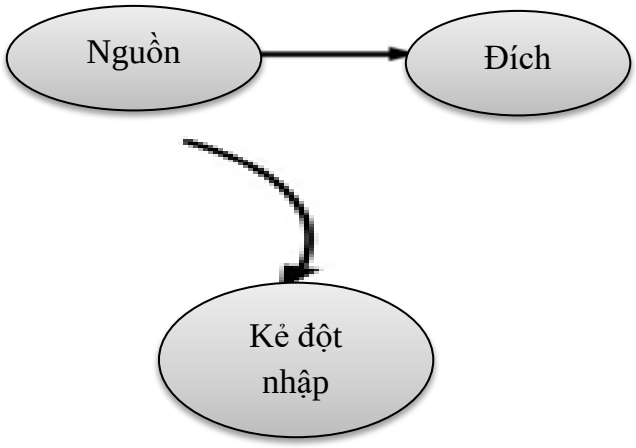
Kẻ tấn công có thể gây ra bốn loại tấn công cơ bản là: **tấn công bị động** (passive attack), **tấn công chủ động** (Active Attack), **tấn công chèn ép** (Jamming) và **tấn công thu hút** (Man-in-the-middle Attack).

2.2.2.1 Tấn công bị động

Tấn công bị động (Passive attack) hay nghe lén (eavesdropping) có lẽ là một phương pháp tấn công WLAN đơn giản nhất nhưng lại rất hiệu quả. Tấn công bị động là kiểu tấn công không tác động trực tiếp vào thiết bị nào trên mạng, các thiết bị trên mạng không biết được hoạt động của nó, vì thế kiểu tấn công này nguy hiểm ở chỗ nó rất khó phát hiện và không để lại một dấu vết nào. Hacker sử dụng WLAN sniffer hay các ứng dụng miễn phí có thể được sử dụng để thu thập thông tin về mạng không dây ở khoảng cách xa bằng cách sử dụng anten định hướng. Việc lấy trộm thông tin trong không vùng phủ sóng của các thiết bị đã khó phát hiện chứ chưa nói đến việc nó được đặt ở khoảng cách xa và sử dụng anten được định hướng tới nơi phát sóng. Phương pháp này cho phép hacker giữ khoảng cách với hệ thống mạng mà không để bị phát hiện.

- ***Sự đánh chặn.***

Sự đánh chặn là một tấn công thụ động vào độ tin cậy, ở đây một thực thể đột nhập là có khả năng đọc thông tin gửi từ một thực thể nguồn tới thực thể đích (hình 2.4). Sniffing (thăm dò) là một ví dụ của tấn công đánh chặn.



Hình 2.4: Sự đánh chặn trong một mạng

Kẻ đột nhập cố gắng nghiên cứu hoặc tạo cách sử dụng thông tin từ hệ thống, nhưng không ảnh hưởng tới các tài nguyên hệ thống. Sự nhận dạng thực thể nguồn có thể bị ngăn chặn và sau đó sử dụng trong một tấn công, hoặc kẻ đột nhập có thể quan tâm đến các nội dung message phát hành như là thông tin nhận thực, các mật

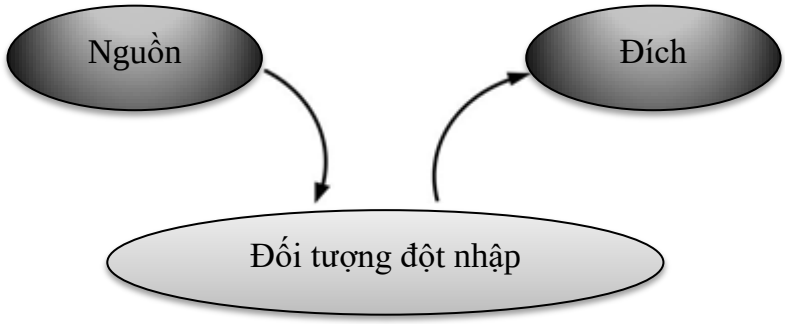
khẩu, các số thẻ tín dụng, sở hữu trí tuệ, hoặc các thông tin nhạy cảm khác. Kẻ đột nhập cũng có thể quan tâm đến thực hiện phân tích lưu lượng trên hệ thống để thu được hoặc suy luận ra thông tin từ các đặc trưng lưu lượng.

2.2.2.2 Tấn công chủ động

Tấn công chủ động (active) là tấn công trực tiếp vào một hoặc nhiều thiết bị trên mạng, ví dụ như vào AP, STA. Những kẻ tấn công có thể sử dụng phương pháp tấn công chủ động để thực hiện các chức năng trên mạng. Cuộc tấn công chủ động có thể được dùng để tìm cách truy nhập tới một server để thăm dò, để lấy những dữ liệu quan trọng hoặc thay đổi cấu hình cơ sở hạ tầng mạng. Kiểu tấn công này dễ phát hiện nhưng khả năng phá hoại của nó rất nhanh và nguy hiểm, khi phát hiện ra thì nó đã thực hiện xong quá trình phá hoại. Bằng cách kết nối với mạng không dây thông qua AP, hacker có thể xâm nhập sâu hơn vào mạng hoặc có thể thay đổi cấu hình của mạng. Ví dụ, một hacker có thể sửa đổi để thêm MAC địa chỉ của hacker vào danh sách cho phép của lọc MAC trên AP hay vô hiệu hóa tính năng lọc MAC giúp cho việc đột nhập sau này dễ dàng hơn. Admin thậm chí không biết được thay đổi nếu như không kiểm tra thường xuyên.

- ***Sửa đổi.***

Sửa đổi là phương thức tấn công mà một thực thể đột nhập thay đổi thông tin đã được gửi từ một thực thể nguồn tới một thực thể đích (hình 2.5). Việc chèn một chương trình Trojan Horse hoặc virus là một ví dụ của tấn công sửa đổi.



Hình 2.5: Tấn công sửa đổi trong một mạng 802.11

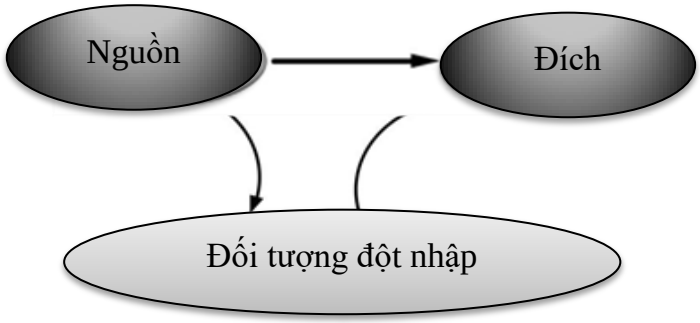
Phương thức bảo mật WEP là phương thức cực kém cho một tấn công sửa đổi (modification) mà không bị phát hiện bởi vì IV (initialization vector – IV) tăng một trị số và CRC là hàm tuyến tính mà nó chỉ sử dụng các phép cộng và phép nhân. Vì vậy biểu thức sau đây là đúng:

$$Crc(x + y) = crc(x) + crc(y).$$

Với việc kiểm tra tính toàn vẹn CRC-32, nó có khả năng thay đổi một hay nhiều bit trong bản tin gốc chưa mã hóa và dự đoán tổng các bit kiểm tra cần để thay đổi bản tin để duy trì tính hợp lệ của nó. Điều này nghĩa là nó có khả năng lấy bản tin từ một thực thể nguồn sau đó sửa đổi và chèn lại chúng trong một luồng dữ liệu không bị phát hiện.

- ***Phúc đáp***

Phúc đáp là phương thức tấn công chủ động vào tính toàn vẹn, ở đây một nhóm đột nhập gửi lại thông tin mà đã được gửi từ thực thể nguồn tới thực thể đích.

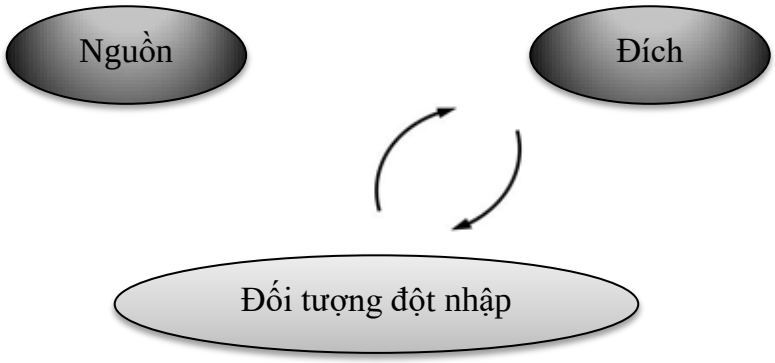


Hình 2.6: Tấn công phúc đáp trên một mạng

Phương thức bảo mật 802.11 cơ bản không có sự bảo vệ chống lại sự phúc đáp. Nó không bao gồm các mã số dãy hoặc các tem thời gian. Bởi vì các IV và các khóa có thể được dùng lại, do đó nó có thể phát lại các bản tin đã lưu trữ cùng với IV mà không bị phát hiện. Các gói tin riêng lẻ phải được nhận thực, không mật mã hóa. Các gói tin phải có các mã số dãy hoặc các tem thời gian.

- ***Sự phản ứng***

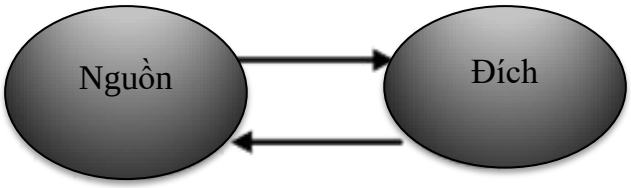
Sự phản ứng là một tấn công chủ động, ở đây các gói tin được gửi bởi một kẻ đột nhập tới đích (Hình 2.7). Kẻ đột nhập kiểm tra sự phản ứng, thông tin bổ sung có thể được tìm thấy ở kênh bên cạnh.



Hình 2.7: Ví dụ về tấn công phản ứng

- ***Sự phủ nhận.***

Sự phủ nhận là một tấn công chủ động đến thuộc tính không được phủ nhận được yêu cầu bởi nguồn hay đích, nghĩa là nguồn phủ nhận việc gửi một bản tin hoặc thực thể đích phủ nhận việc nhận bản tin (Hình 2.8).



Hình 2.8: Một ví dụ về phủ nhận

Bảo mật 802.11 cơ sở không có thuộc tính không được phủ nhận. Nếu không có thuộc tính không được phủ nhận, thì thực thể nguồn có thể liên tục phủ nhận việc gửi bản tin và thực thể đích có thể liên tục phủ nhận việc nhận bản tin.

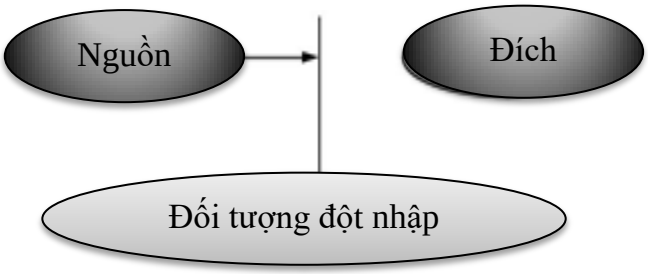
2.2.2.3 Tấn công bằng cách chèn ép (Jamming)

Jamming là một kỹ thuật được sử dụng đơn giản chỉ để làm hỏng (shut down) mạng không dây của người sử dụng. Tương tự như những kẻ phá hoại sử dụng tấn công DoS vào một web server làm nghẽn server đó thì mạng WLAN cũng

có thể bị shut down bằng cách gây nghẽn tín hiệu RF. Những tín hiệu gây nghẽn này có thể là cố ý hay vô ý và có thể loại bỏ được hay không loại bỏ được.

- ***Ngắt.***

Ngắt là một loại tấn công mà thực thể đột nhập chặn thông tin từ một thực thể gốc tới một thực thể đích (Hình 2.9).



Hình 2.9: Một ví dụ về ngắt

Kẻ đột nhập cố gắng làm cạn kiệt băng thông mạng bằng việc làm lụt ARP, phát quảng bá, làm lụt SYN giao thức điều khiển truyền dẫn (TCP), lụt hàng đợi và sử dụng các phương pháp làm ngập lụt khác…Kẻ đột nhập cũng có thể sử dụng một số cơ chế vật lý như nhiễu RF (Radio Frequency) để ngắt thành công một mạng.

Kẻ tấn công gửi disassociation frame bằng cách giả mạo thực thể nguồn Source và Destination MAC đến AP và các client tương ứng trong mạng. Client sẽ nhận các frame này và nghĩ rằng frame hủy kết nối đến từ AP. Đồng thời kẻ tấn công cũng gửi disassociation frame đến AP. Sau khi đã 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 động ngắt kết nối với AP. Khi các clients bị ngắt kết nối sẽ thực hiện kết nối lại với AP ngay lập tức. Kẻ tấn công tiếp tục gửi disassociation frame đến AP và client.

Các tấn công phủ nhận dịch vụ (DoS).

Tấn công phủ nhận dịch vụ là một hình thức tấn công nhằm ngăn chặn những người dùng hợp lệ được sử dụng một dịch vụ nào đó. Các cuộc tấn công có thể được thực hiện nhằm vào bất kì một thiết bị mạng nào bao gồm tấn công vào các thiết bị định tuyến, web, thư điện tử và hệ thống DNS.

Có 5 kiểu tấn công cơ bản sau đây:

- *Nhằm tiêu tốn tài nguyên tính toán như băng thông, dung lượng đĩa cứng hoặc thời gian xử lý.*
- *Phá vỡ các thông tin cấu hình như thông tin định tuyến.*
- *Phá vỡ các trạng thái thông tin như việc tự động reset lại các phiên TCP.*
- *Phá vỡ các thành phần vật lý của mạng máy tính.*
- *Làm tắc nghẽn thông tin liên lạc có chủ đích giữa các người dùng và nạn nhân dẫn đến việc liên lạc giữa hai bên không được thông suốt.*

Một cuộc tấn công từ chối dịch vụ có thể bao gồm cả việc thực thi malware (phần mềm độc hại) nhằm:

- *Làm quá tải năng lực xử lý, dẫn đến hệ thống không thể thực thi bất kì một công việc nào khác.*
- *Những lỗi gọi tức thì trong microcode của máy tính.*
- *Những lỗi gọi tức thì trong chuỗi chỉ thị, dẫn đến máy tính rơi vào trạng thái hoạt động không ổn định hoặc bị treo.*
- *Những lỗi có thể khai thác được ở hệ điều hành dẫn đến việc thiếu thốn tài nguyên hoặc bị thrashing.*
- *Gây tai nạn (crash) hệ thống.*
- *Tấn công từ chối dịch vụ IFrame: trong một trang HTML có thể gọi đến một trang web nào đó với rất nhiều yêu cầu và trong rất nhiều lần cho đến khi băng thông của trang web đó bị quá hạn.*
- *Các mạng giả mạo và tái định hướng trạm: một mạng 802.11 vô tuyến rất dễ bị ảnh hưởng bởi tấn công AP giả mạo. Một AP giả mạo được sở hữu một attacker xác nhận kết nối mạng và sau đó chặn lưu lượng và có thể thực hiện các tấn công man-in the middle trước khi lưu lượng được phép truyền trên mạng. Mục đích chính của mạng giả mạo là loại bỏ lưu lượng hợp lệ ra khỏi WLAN lên trên một mạng hữu tuyến để tấn công, sau đó chèn lại lưu lượng vào mạng hợp pháp.*

Như vậy các AP giả mạo có thể được triển khai dễ dàng trong các khu vực công cộng. Các tấn công DoS không cho phép một hacker giành quyền truy nhập mạng, đúng hơn về cơ bản chúng làm các hệ thống máy tính khó có thể truy nhập bằng cách làm quá tải các server hoặc mạng bằng việc sử dụng lưu lượng hợp lệ, vì vậy người sử dụng có thể không truy nhập được các tài nguyên. Mục đích là để ngăn chặn mạng tách khỏi việc cung cấp dịch vụ tới tất cả mọi người. Thông thường điều này hoàn thành bằng cách làm quá tải một tài nguyên. Sự quá tải tài nguyên làm Host trở nên không dùng được. Nhiều loại tấn công này tùy thuộc vào loại tài nguyên bị chặn (không gian ổ đĩa, băng thông, các bộ nhớ đệm).

Để loại bỏ kiểu tấn công này thì yêu cầu đầu tiên là phải xác định được nguồn tín hiệu RF. Việc này có thể làm bằng cách sử dụng một Spectrum Analyzer (máy phân tích phổ). Một cách khác là dùng các ứng dụng Spectrum Analyzer phần mềm kèm theo các sản phẩm WLAN cho client.

Jamming do vô ý xuất hiện thường xuyên do nhiều thiết bị khác nhau chia sẻ chung băng tần 2.4 ISM với mạng WLAN. Jamming một cách chủ động thường không phổ biến lắm, lý do là bởi vì để thực hiện được jamming thì rất tốn kém, giá của thiết bị rất mắc tiền, kết quả đạt được chỉ là tạm thời shut down mạng trong thời gian ngắn.

2.2.2.4 Tấn công thu hút (Man-in-the-middle Attack)

Các cuộc tấn công theo kiểu Man-in-the-Middle Attack giống như một người nào đó giả mạo danh tính để đọc các tin nhắn của bạn. Và người ở đầu kia tin rằng đó là bạn, bởi vì kẻ tấn công có thể trả lời một cách tích cực để trao đổi và thu thập thêm thông tin.

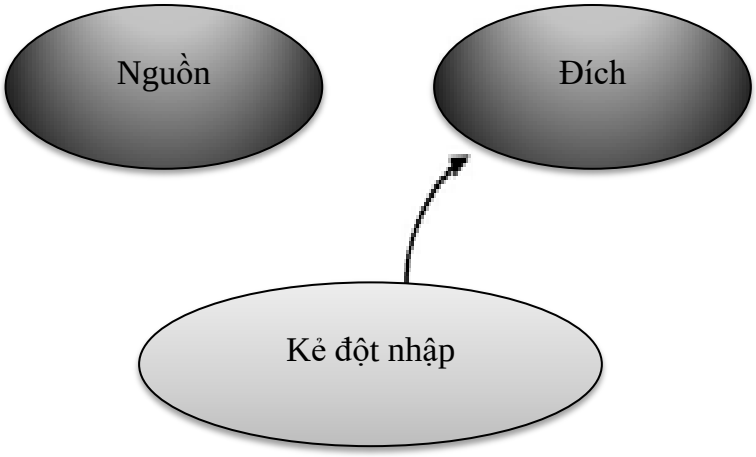
Tấn công theo kiểu Man-in-the-middle là trường hợp trong đó hacker sử dụng một AP để đánh cắp các node di động bằng cách gửi tín hiệu RF mạnh hơn AP hợp pháp đến các node đó. Các node di động nhận thấy có AP phát tín hiệu RF tốt hơn nên sẽ kết nối đến AP giả mạo này, truyền dữ liệu có thể là những dữ liệu nhạy cảm đến AP giả mạo và hacker có toàn quyền xử lý.

Để làm cho client kết nối lại đến AP giả mạo thì công suất phát của AP giả mạo phải cao hơn nhiều so với AP hợp pháp trong vùng phủ sóng của nó. Việc kết nối lại với AP giả mạo được xem như là một phần của roaming nên người dùng sẽ không hề biết được.

Hacker muốn tấn công theo kiểu Man-in-the-middle này trước tiên phải biết được giá trị SSID là các client đang sử dụng (giá trị này rất dễ dàng có được). Sau đó, hacker phải biết được giá trị WEP key nếu mạng có sử dụng WEP. Kết nối upstream (với mạng trục có dây) từ AP giả mạo được điều khiển thông qua một thiết bị client như PC card hay Workgroup Bridge. Nhiều khi, tấn công Man-in-the-middle được thực hiện chỉ với một laptop và 2 PCMCIA card. Phần mềm AP chạy trên máy laptop nơi PC card được sử dụng như là một AP và một PC card thứ 2 được sử dụng để kết nối laptop đến AP hợp pháp gần đó. Trong cấu hình này, laptop chính là man-in-the-middle (người ở giữa), hoạt động giữa client và AP hợp pháp. Từ đó hacker có thể lấy được những thông tin giá trị bằng cách sử dụng các sniffer trên máy laptop.

- ***Giả mạo AP (Access Point)***

Sự làm giả mạo là một tấn công mà kẻ đột nhập giả vờ là một thực thể nguồn (hình 2.10). Bắt chước các gói tin và làm giả các e-mail là các ví dụ của một tấn công làm giả mạo thông tin.



Hình 2.10: Sự làm giả mạo trong mạng

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 không dây hoạt động trái phép mà không cần quan tâm đến mục đích sử dụng.

Có bốn kiểu giả mạo:

- *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.

- *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.

- *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.

- Cách thứ nhất là đợi cho người dùng tự kết nối.
- Cách thứ hai 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.

- *Access Point giả mạo được thiết lập bởi chính nội bộ.*

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 nên họ vô tình tạo ra một lỗ hỏng 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 hệ thống mạng của công ty tấn công người khác.

- *Tấn công trung gian:*

Để thực hiện một tấn công trung gian, hai host phải tin chắc rằng máy tính ở giữa là một host khác. Phiên bản cũ của tấn công này xảy ra khi một người nào đó thu các gói tin từ mạng rồi sửa đổi chúng, sau đó đưa chúng trở lại mạng.

- *Tấn công gián điệp:*

Hoạt động định cấu hình một thiết bị để giành quyền truy nhập mạng hoặc chèn một thiết bị vào trong mạng cốt để mà giành quyền truy nhập mạng được gọi là tấn công gián điệp. Bằng cách cài đặt các Card mạng vô tuyến trong vùng phụ cận mạng đích, một thiết bị có thể được định cấu hình để giành quyền truy nhập. Các AP trái phép có thể được thử cài đặt để làm cho người sử dụng kết nối tới AP của các Hacker đúng hơn là phải kết nối tới AP mạng mong đợi. Nếu các AP này được cài đặt đằng sau tường lửa, nguy hiểm các tấn công lớn hơn rất nhiều.

- *Tấn công cưỡng bức:*

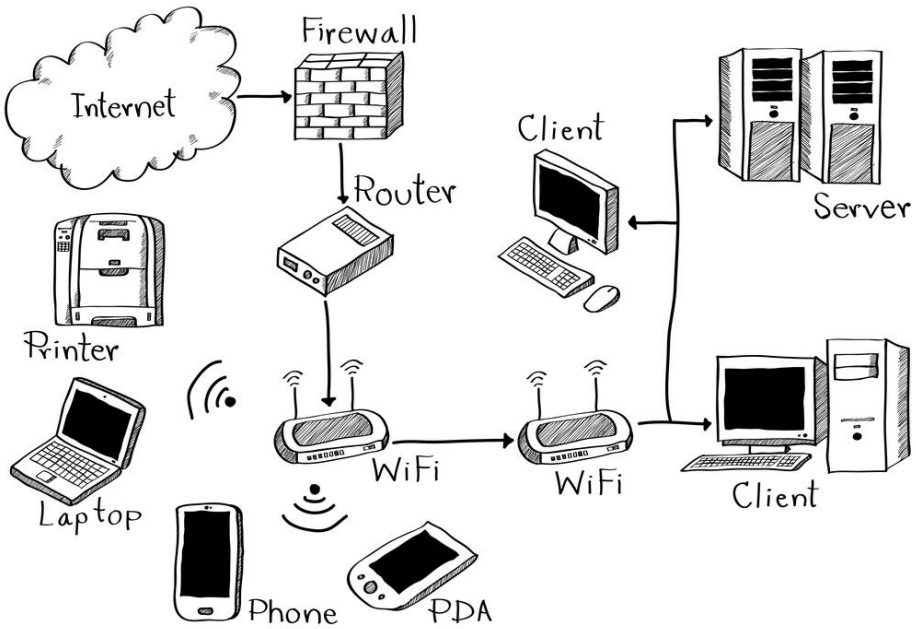
Còn được gọi là phá mật khẩu hay tấn công lần lượt, loại tấn công này sử dụng một từ điển và thực hiện thử lặp đi lặp lại để kiểm tra mật khẩu giành quyền truy nhập mạng. Loại tấn công này có thể thực hiện được thậm chí nếu mật khẩu nhận thực được thực hiện.

2.3 Kiến trúc mạng WLAN

2.3.1 Kiến trúc mạng WLAN điển hình

Mạng WLAN cần được bảo vệ từ những người sử dụng trên các AP vô tuyến. Hình 2.11 biểu diễn một nhóm kiến trúc hạ tầng mạng Internet kết nối tới

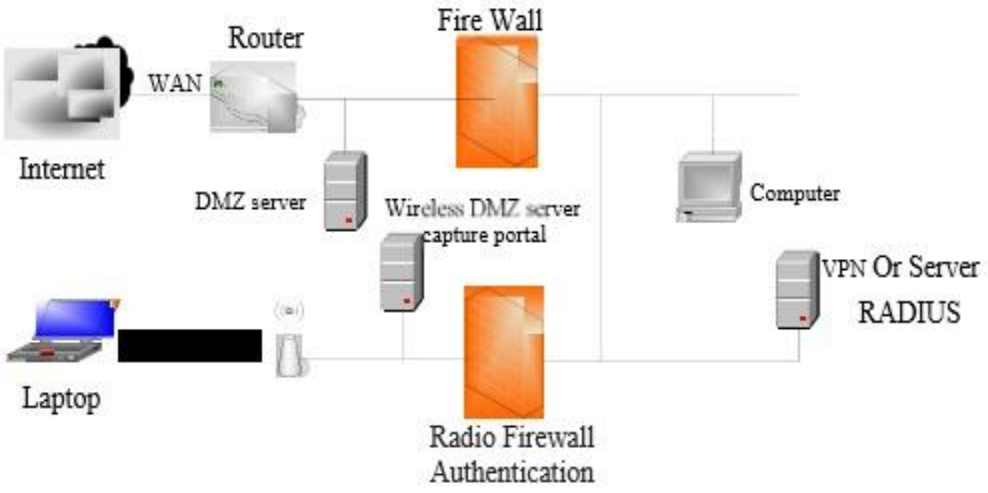
một router trên WAN biên. Trên LAN biên của router, người sử dụng có thể tuỳ chọn kết nối một server vùng không tranh chấp (DMZ) mà có thể truy nhập từ một tổ hợp mạng trên một LAN biên. Thông thường, chức năng tường lửa được bao gồm trong Router. Tuy nhiên, AP mới ngẫu nhiên tạo một đường để đi vào sau tường lửa thông qua liên kết không gian.



Hình 2.11: Kiến trúc WLAN điển hình

2.3.2 Kiến trúc mạng WLAN với giải pháp tường lửa vô tuyến

Kiến trúc mạng có thể bị thay đổi bằng cách bổ xung một tường lửa vô tuyến điều chỉnh truy nhập tới LAN bằng cách chỉ cho phép người sử dụng qua sau khi họ đã nhận thực, như biểu diễn trên hình 2.12. Một server DMZ tuỳ chọn hoặc một cổng chặn giữ có thể tồn tại trên WLAN biên của mạng. Tường lửa nhận thực vô tuyến tách rời WLAN khỏi LAN, vì thế sự bảo vệ các mạng tránh bị truy nhập qua thiết bị vô tuyến. Trong một giao thức nhận thực có thể mở rộng (EAP) 802.11x. AP sẽ bao gồm tường lửa và một sự bổ sung sever dịch vụ người sử dụng tham gia nhận thực từ xa (RADIUS) sẽ cần được định vị trên LAN. Trong một VPN, các host LAN tạo thành điểm đầu cuối của VPN tunnel. Cả hai loại tường lửa sẽ phải cần một lỗ hổng để mạng lưu lượng VPN từ WLAN biên và WAN tới LAN.



Hình 2.12: Tường lửa nhận thực vô tuyến bảo vệ LAN

2.4 Các phương thức bảo mật trong WLAN

2.4.1 WEP - Wired Equivalent Privacy

WEP là một hệ thống mã hoá dùng cho việc bảo mật dữ liệu cho mạng Wireless, WEP là một phần của chuẩn 802.11 gốc và dựa trên thuật toán mã hoá RC4, mã hoá dữ liệu 40bit để ngăn chặn sự truy cập trái phép từ bên ngoài. Thực tế WEP là một thuật toán được dùng để mã hoá và giải mã dữ liệu.

- Đặc tính kỹ thuật của WEP:

+ Điều khiển việc truy cập, ngăn chặn sự truy cập của những Client không có khóa phù hợp.

+ Sự bảo mật nhằm bảo vệ dữ liệu trên mạng bằng cách mã hoá chúng và chỉ cho những Client nào đó đúng khoá WEP giải mã.

2.4.2 WPA

WPA (Wi-Fi Protected Access) được thiết kế nhằm thay thế cho WEP vì có tính bảo mật cao hơn. Temporal Key Intergrity Protocol (**IP) còn được gọi là WPA key hashing là một sự cải tiến dựa trên WEP, là vì nó tự động thay đổi khoá,

điều này gây khó khăn rất nhiều cho các Attacker dò thấy khoá của mạng. WPA là một giao thức bảo mật của mô hình mạng không dây WLAN được liên minh WI-FI công bố vào tháng 11 năm 2002 nhằm mục đích thay thế giao thức bảo mật yếu kém WEP tồn tại trước đó.

Cụ thể, WPA cũng sử dụng thuật toán RC4 như WEP, nhưng mã hoá đầy đủ 128 bit và dành ra 64 bit cho chứng thực để tạo ra sự bảo mật tốt hơn, năm 2004 giải pháp TKIP (Temporal Key Integrity Protocol-Toàn vẹn khóa tạm thời) được IEEE đưa vào WPA nhằm vá những vấn đề bảo mật trong cài đặt mã dòng RC4. 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 MIC (Message Integrity Check- bản tin phi tuyến) để đảm bảo tính chính xác của gói tin. TKIP của WPA sử dụng khóa động bằng cách đặt cho mỗi frame một chuỗi số riêng để chống lại dạng tấn công giả mạo làm thay đổi khoá mật mã cho khoảng 10.000 gói tin. Nói cách khác, WPA thay đổi khoá cho mỗi gói tin. Các công cụ thu thập các gói tin để phá khoá mã hoá đều không thể thực hiện được với WPA. Bởi WPA thay đổi khoá liên tục nên hacker không bao giờ thu thập đủ dữ liệu mẫu để tìm ra mật khẩu.

WPA bao gồm nhiều phần của 802.11. Tuy nhiên, một số các phần tử khoá không được bao gồm như sự hỗ trợ cho một thuật toán mật mã mới gọi là tiêu chuẩn mật mã hoá cấp cao (AES), tiêu chuẩn này sẽ thay thế thuật toán mật mã RC4 cơ sở khi 802.11i trở nên phổ biến.

Ưu điểm của WPA

- Việc cải tiến hơn RC4 của WEP bằng việc sử dụng TKIP đã làm cho WPA có sức bảo mật tốt hơn, các khóa khi truyền tin được thay đổi liên tục làm cho việc suy đoán khóa của hacker trở nên khó khăn, điều này làm yếu tố bảo mật của WPA tốt hơn.
- Do hỗ trợ việc kiểm tra tính toàn vẹn nên dữ liệu được bảo vệ tốt hơn trên đường truyền.

- Việc tích hợp với các máy chủ xác thực RADIUS để cho phép quản lý, kiểm toán và khai thác mạng WLAN một cách an toàn cao.
- Dễ dàng nâng cấp các thiết bị phần cứng như card mạng và AP đơn giản bằng cách thay đổi phần mềm điều khiển giúp cho chi phí nâng cấp không đáng kể.

Nhược điểm của WPA.

- Với WPA Personal thì có thể việc sử dụng hàm thay đổi khoá TKIP, được sử dụng để tạo ra các khoá mã hoá nếu bị phát hiện hacker có thể đoán được khoá khởi tạo hoặc một phần của mật khẩu và họ có thể xác định được toàn bộ mật khẩu, do đó có thể giải mã được dữ liệu.
- Không tương thích với hệ điều hành cũ.
- Khi sử dụng WPA-PSK thì việc cài đặt trở nên phức tạp, không phù hợp cho người dùng gia đình điển hình.
- TKIP không loại trừ những điểm yếu cơ bản trong bảo mật WiFi. Nếu một attacker tấn công TKIP, hacker không chỉ bẻ gãy độ tin cậy, mà còn điều khiển truy nhập và nhận thực.
- WPA vẫn sử dụng thuật toán RC4 mà có thể dễ dàng bị bẻ khoá bởi tấn công FMS đã được đề xuất bởi những nhà nghiên cứu ở trường đại học Berkeley. Hệ thống mã hóa RC4 chứa đựng những khóa yếu (weak keys). Những khóa yếu này cho phép truy ra khóa mã. Để có thể tìm ra khóa yếu của RC4, chỉ cần thu thập một số lượng đủ thông tin truyền trên kênh truyền không dây.
- Bị tấn công từ chối dịch vụ (DoS) vẫn còn tồn tại.
- 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 người sử dụng mà không truyền dữ liệu "mật" về thương mại, hay các thông tin nhạy cảm. WPA-PSK là một biên bản yếu của WPA mà ở đó nó gặp vấn đề về quản lý password hoặc chia sẻ bí mật giữa nhiều người dùng. Khi một người trong nhóm (trong công ty) rời nhóm, một password/secret mới cần phải được thiết lập.

2.4.3 WPA2

WPA2 là một chuẩn ra đời sau đó và được kiểm định lần đầu tiên vào ngày 1/9/2004. WPA2 được NIST (Viện tiêu chuẩn và công nghệ quốc gia Hoa kỳ) khuyến cáo sử dụng. Trong kiến trúc WPA2, mỗi khách hàng sử dụng một tên người dùng và mật khẩu duy nhất để xác thực trên mạng không dây. WPA2 sử dụng thêm thuật toán mã hóa AES.

Tiêu chuẩn tiền nhiệm của AES là DES (Digital Encryption Standard), mã hóa ở 168 bit-DES là thuật toán mã hóa khối: nó xử lý từng khối thông tin của bản rõ có độ dài xác định và biến đổi theo những quá trình phức tạp để trở thành khối thông tin của bản mã có độ dài không thay đổi. Trong trường hợp của DES, độ dài mỗi khối là 64 bit. DES cũng sử dụng khóa để cá biệt hóa quá trình chuyển đổi. Nhờ vậy, chỉ khi biết khóa mới có thể giải mã được văn bản mã. Khóa dùng trong DES có độ dài toàn bộ là 64 bit. Tuy nhiên chỉ có 56 bit thực sự được sử dụng; 8 bit còn lại chỉ dùng cho việc kiểm tra. Vì thế, độ dài thực tế của khóa chỉ là 56 bit. Nhiều tấn công đã được chỉ ra cho dù DES có rất nhiều ưu điểm nổi trội. Thừa hưởng các đặc tính của tiêu chuẩn tiền nhiệm DES thì AES được kỳ vọng áp dụng trên phạm vi thế giới, đã được nghiên cứu rất kỹ lưỡng và là phương thức bảo mật mới nhất và bảo mật cao nhất trong mã hoá dữ liệu. WPA2 với 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.

Rõ ràng WPA2 với AES cũng có cấp độ bảo mật rất cao tương tự như chuẩn WPA, nhằm bảo vệ cho người dùng và người quản trị đối với tài khoản và dữ liệu. Nhưng trên thực tế WPA2 cung cấp hệ thống mã hóa mạnh hơn so với WPA. Không như WPA, WPA2 lại không tương thích ngược; những Router cũ hơn có khả năng mã hoá WPA với TKIP không thể dùng được WPA2. WPA2 lại tương thích cả AES và TKIP và đây cũng là nhu cầu của các tập đoàn và doanh nghiệp có quy mô lớn. WPA2 sử dụng rất nhiều thuật toán để mã hóa dữ liệu như TKIP, RC4, AES và một vài thuật toán khác.

Ưu điểm của WPA2

- Giải pháp mã hóa tối cao với việc sử dụng đồng thời nhiều thuật toán mã hóa dữ liệu để mang lại hiệu quả mã hóa cao nhất, tăng độ tin cậy của hệ thống WLAN sử dụng nó.
- Do có cơ chế các thuật toán mã hóa tổng hợp nên WPA2 làm cho các Hacker không thể suy đoán các khóa cũng như bẻ gãy độ tin cậy và nắm quyền điều khiển truy nhập và nhận thực được.

Nhược điểm của WPA2

- Tồn tại một số tấn công nhằm vào AES như việc tấn công kênh bên. Tấn công kênh bên không tấn công trực tiếp vào thuật toán mã hóa mà thay vào đó, tấn công lên các hệ thống thực hiện thuật toán có sơ hở làm lộ dữ liệu. Ngoài ra hiện nay một lỗ hổng mới được phát hiện là lỗ hổng 196.
- Hầu hết các thiết bị cầm tay Wi-Fi, máy tính đời cũ và máy quét mã vạch đều không tương thích với chuẩn 802.11i.
- Việc nâng cấp lên chuẩn 802.11i với giao thức bảo mật WPA2 đòi hỏi phải có chi phí thay thế thiết bị phần cứng gồm cả AP và Card mạng không dây, điều này làm cho chi phí triển khai hệ thống tăng và giảm khả năng thích ứng của các thiết bị máy khách thông dụng.

2.4.4 Lọc (filtering)

Lọc là cơ chế bảo mật cơ bản có thể sử dụng cùng với WEP hoặc một số giao thức khác. Lọc hoạt động giống như Access list trên router, cấm những cái không mong muốn và cho phép những cái mong muốn. Có 3 kiểu lọc cơ bản có thể được sử dụng trong wireless lan:

- Lọc SSID
- Lọc địa chỉ MAC
- Lọc giao thức

2.4.4.1 Lọc SSID

Lọc SSID Filtering là một phương pháp lọc chỉ được dùng cho hầu hết các điều khiển truy nhập. SSID của một trạm WLAN phải khớp với SSID trên AP hoặc của các trạm khác để chứng thực và liên kết Client để thiết lập dịch vụ. Nhiều AP có khả năng lấy các SSID của các khung thông tin dẫn đường beacon frame.

SSID sẽ được tự động hiển thị khi người dùng tìm kiếm các mạng Wi-Fi xung quanh. Và nếu bạn thiết lập tắt SSID thì người dùng khác sẽ không thể dò tìm thấy mạng wifi của bạn hay nói một cách khác người dùng bên ngoài sẽ không thể truy cập vào mạng wifi của bạn một cách trái phép. Tuy nhiên các hacker và các người dùng khác vẫn có thể tìm thấy mạng wifi của bạn bằng cách chặn tín hiệu truyền từ router đến máy của bạn và từ máy của bạn đến router bằng các phần mềm và công cụ cần thiết.

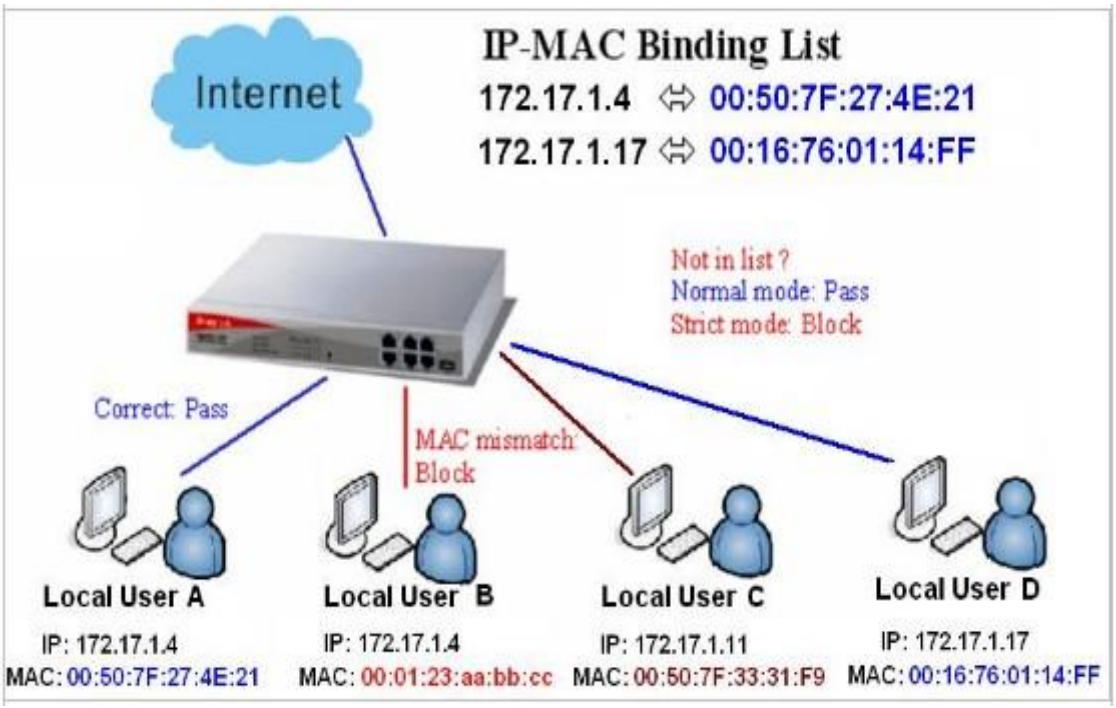
Hình 2.13: Sơ đồ hỗ trợ ẩn SSID ở các thiết bị định tuyến phổ biến

2.4.4.2 Lọc địa chỉ MAC

Trước khi nền công nghiệp Wi-Fi giải quyết được những vấn đề và thiếu sót của WEP (wireless encryption protocol) - công nghệ bảo mật bằng mã hóa, nhiều chuyên gia khuyến cáo sử dụng thêm cơ chế lọc địa chỉ MAC nhằm tăng cường bảo mật. Mỗi thiết bị Wi-Fi được gán duy nhất một địa chỉ MAC (Media Access Control) gồm 12 chữ số thập lục phân. Địa chỉ MAC là phần "ngầm" của thiết bị phần cứng và được gửi tự động tới điểm truy cập Wi-Fi mỗi khi thiết bị kết nối vào mạng.

Sử dụng trình quản lý cấu hình của điểm truy cập (Access Point - AP), bạn có thể lập được một danh sách thiết bị an toàn (được phép truy xuất vào mạng) hay danh sách thiết bị không được phép truy xuất vào mạng (black list – danh sách đen). Nếu bộ lọc địa chỉ MAC được kích hoạt, AP chỉ cho phép các thiết bị trong danh sách an toàn được kết nối vào mạng và cấm tất cả thiết bị trong danh sách đen truy xuất vào mạng, ngay cả khi bạn có khóa kết nối, bất kể bạn đang sử dụng giao thức kết nối nào.

Với sự xuất hiện của các giao thức mã hóa tin cậy, trong đó mạnh nhất là WPA2 (Wi-Fi Protected Access II), chúng ta ít nghe nói đến lọc địa chỉ MAC hơn. Tuy nhiên, tin tặc (hacker) cũng đã tìm ra cách để tấn công giao thức này, bằng cách giả mạo địa chỉ của thiết bị kết nối hay giả mạo là một trong số các thiết bị này.



Hình 2.14: Lọc địa chỉ MAC

Để thiết lập bộ lọc MAC, chúng ta cần lập danh sách địa chỉ MAC cho các thiết bị có nhu cầu kết nối vào mạng. Mỗi lần muốn thêm hay xóa một thiết bị, bạn phải đăng nhập vào trình quản lý cấu hình của AP. (AP cấp doanh nghiệp có thể cho phép thực hiện việc này bằng câu lệnh). Nếu client có địa chỉ MAC không nằm

trong danh sách lọc địa chỉ MAC của AP thì sẽ bị AP ngăn chặn không cho phép client đó kết nối vào mạng.

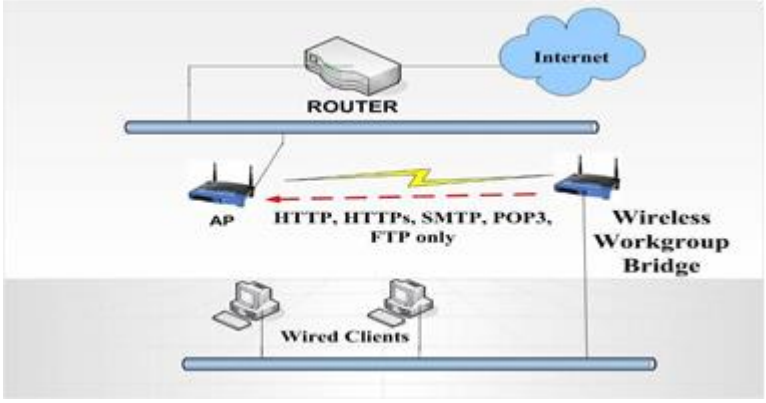
Đối với hệ thống mạng có nhiều client thì có thể xây dựng máy chủ RADIUS có chức năng lọc địa chỉ MAC thay vì dùng AP. Cấu hình lọc địa chỉ MAC là giải pháp bảo mật có tính mở rộng cao.

2.4.4.3 Lọc giao thức

Mạng Lan không dây có thể lọc các gói đi qua mạng dựa trên các giao thức từ lớp 2 đến lớp 7. Trong nhiều trường hợp người quản trị nên cài đặt lọc giao thức trong môi trường dùng chung, ví dụ trong trường hợp sau:

Có một nhóm cầu nối không dây được đặt trên một Remote building trong một mạng WLAN của một trường đại học mà kết nối lại tới AP của toà nhà kỹ thuật trung tâm.

Nếu các kết nối này được cài đặt với mục đích đặc biệt của sự truy nhập internet của người sử dụng, thì bộ lọc giao thức sẽ loại trừ tất cả các giao thức, ngoại trừ HTTP, SMTP, HTTPS, FTP…



Hình 2.15: Lọc giao thức

<u>Kết luận chung về các phương pháp lọc</u>

Khi nghiên cứu về cách bảo mật mạng WLAN bằng việc sử dụng các phương pháp lọc, chúng vẫn còn khá nhiều những khuyết điểm cần phải khắc phục nhưng các phương pháp này vẫn là các phương pháp được dùng khá phổ biến hiện

nay. Các phương pháp này vẫn nên được sử dụng đối với các hệ thống không triển khai được các giao thức bảo mật khác hoặc có thể áp dụng phương pháp này kèm các giao thức bảo mật khác để có hiệu quả bảo mật tốt hơn.

2.4.5 WLAN VPN

VPN là công nghệ được sử dụng phổ biến hiện nay nhằm cung cấp kết nối an toàn và hiệu quả để truy cập tài nguyên nội bộ công ty từ bên ngoài thông qua mạng Internet. Mặc dù sử dụng hạ tầng mạng chia sẻ nhưng chúng ta vẫn bảo đảm được tính riêng tư của dữ liệu giống như đang truyền thông trên một hệ thống mạng riêng. Giải pháp VPN "mềm" thích hợp cho số lượng người dùng nhỏ, để đáp ứng số lượng người dùng lớn hơn, có thể phải cần đến giải pháp VPN phần cứng.

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 thẻ 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.

Hiện nay VPN có hai loại phổ biến là VPN truy cập từ xa (Remote-Access) và VPN điểm-nối-điểm (site-to-site).

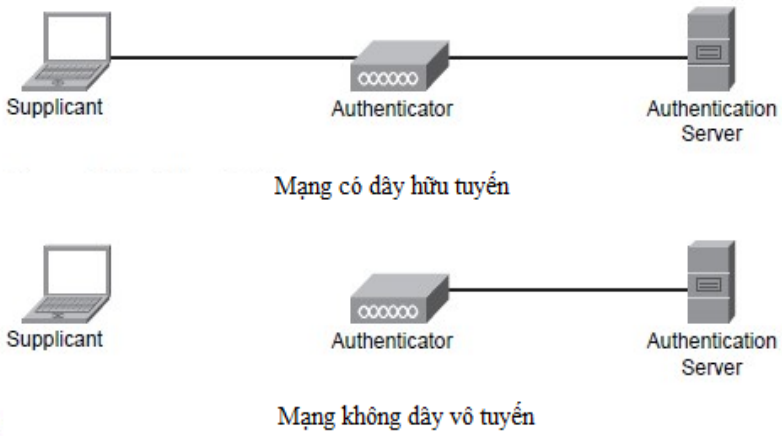
VPN truy cập từ xa còn được gọi là mạng Dial-up riêng ảo (VPDN), là một kết nối người dùng đến LAN, thường là nhu cầu của một tổ chức có nhiều nhân viên cần liên hệ với mạng riêng của mình từ rất nhiều địa điểm ở xa.

VPN điểm-nối-điểm là việc sử dụng mật mã dành cho nhiều người để kết nối nhiều điểm cố định với nhau thông qua một mạng công cộng như Internet. Loại này có thể dựa trên Intranet hoặc Extranet. Loại dựa trên Intranet: Nếu một công ty có nhiều trụ sở tham gia vào một mạng riêng duy nhất, họ có thể tạo ra một VPN intranet (VPN nội bộ) để nối LAN với LAN. Loại dựa trên Extranet: Khi một công

ty có mối quan hệ mật thiết với một công ty khác (ví dụ như đối tác cung cấp, khách hàng.), họ có thể xây dựng một VPN extranet (VPN mở rộng) kết nối LAN với LAN để nhiều tổ chức khác nhau có thể làm việc trên một môi trường chung.

2.4.6 Nhận thực và tiêu chuẩn xác thực 802.1x

802.1x là một chứng thực chuẩn IEEE, được sử dụng cho mạng có dây lẫn không dây. Là phương pháp đóng mở dựa trên điều kiện mà server AAA xác thực. Các thiết bị muốn đi vào mạng có dây được gọi là supplicant. Một supplicant có thể sử dụng phương thức EAP để dò ID của mình với authentication server. Giữa supplicant và authentication server là authenticator. Authenticator hoạt động như một switch ở trong mạng này. Switch này sử dụng giao thức EAP over LAN (EAPoL) giữa supplicant với nó và RADIUS giữa nó với anthentication server. Trên mạng không dây thì quá trình tương tự nhưng đổi lại là giao thức EAPoWLAN.



Hình 2.16: Nhận thực 802.1x

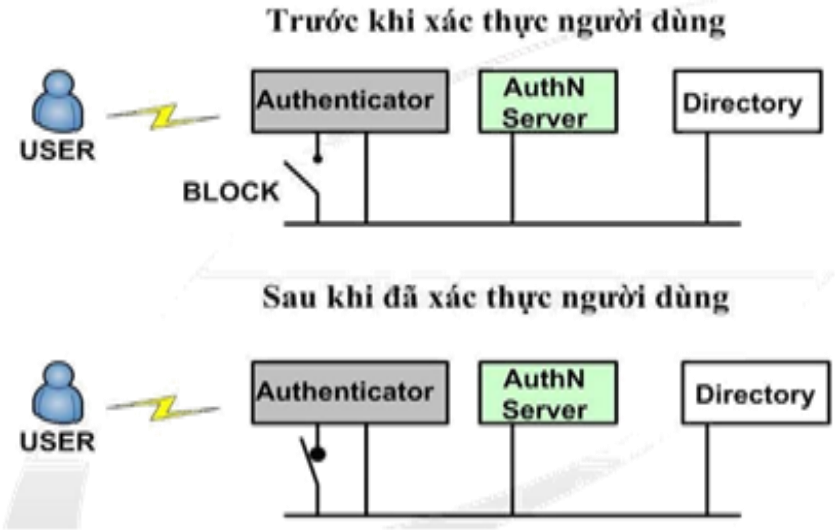
Quá trình chứng thực tương tự kiểu chứng thực mở Sau khi quá trình chứng thực mở ra, 2 bên có thể bắt đầu quá trình 802.1x. Trong suốt thời gian này, “port” vẫn bị chặn và xảy ra những điều sau đây:

- Supplicant gửi giấy chứng nhận đến authenticator.
- AP gửi thông tin chứng thực đến server thông qua gói tin RADIUS

- Luồng RADIUS được authentication server gửi đến client thông qua AP.
- Trong suốt quá trình thay đổi, client và AP sử dụng các key là duy nhất.
- RADIUS server gửi một thông điệp truy cập thành công đến client với một key seasion WEP.
- AP giữ key seasion WEP đó để sử dụng giữa AP và chính nó.
- AP gửi key seasion WEP cùng với một key broadcast/multicast WEP đến client.
- Client và AP có thể sử dụng key seasion WEP để mã hóa luồng lưu lượng

2.4.7 Bảo mật cấp cao (EAP)

EAP là chuẩn của IETF đưa ra vào tháng 3/1998 cho kết nối điểm-điểm. Đây là phương thức xác thực bao gồm yêu cầu định danh người dùng (password, cetificate…), 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 và được sử dụng thông qua các loại cơ chế xác thực khác nhau.



Hình 2.17: Mô hình hoạt động xác thực 802.1x

2.4.8 Phương pháp phát hiện xâm nhập trong mạng không dây (WIDS)

Mục tiêu của việc phát hiện xâm nhập là xác định các hoạt động trái phép, dùng sai, lạm dụng đối với hệ thống máy tính gây ra bởi cả người dùng trong hệ thống lẫn người xâm nhập ngoài hệ thống. Mục đích của IDS là phát hiện và ngăn ngừa các hành động phá hoại bảo mật hệ thống, hoặc những hành động trong tiến trình tấn công như dò tìm, quét các cổng. IDS cũng có thể phân biệt giữa những cuộc tấn công nội bộ (từ nhân viên trong tổ chức) và tấn công bên ngoài (từ hacker).

Wireless IDS bao gồm:

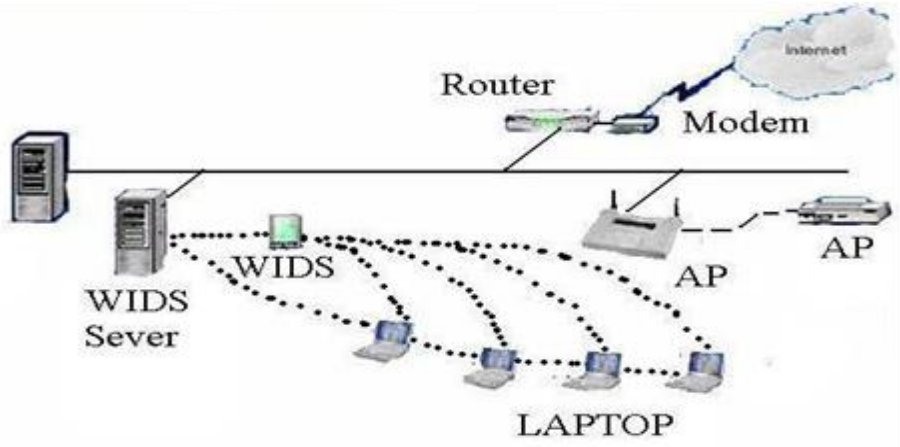
- Vị trí cần phải giám sát (rất chặt chẽ): bên trong và bên ngoài mạng.
- Thiết bị và chức năng gồm phần cứng và phần mềm chuyên dụng có nhiều tính năng như thu thập địa chỉ MAC, SSID. Với đặc tính thiết lập các trạm, tốc độ truyền, kênh, trạng thái mã hóa.

Nhiệm vụ

Giám sát và phân tích các hoạt động của người dùng và hệ thống. Nhận diện các loại tấn công đã biết.

Xác định các hoạt động bất thường của hệ thống mạng. Xác định các chính sách bảo mật cho WLAN.

Thu thập tất cả truyền thông trong mạng không dây và đưa ra các cảnh báo dựa trên những dấu hiệu đã biết hay sự bất thường trong truyền thông.



Hình 2.18: Hệ thống WIDS

Mô hình hoạt động:

WIDS tập trung có một bộ tập trung để thu thập tất cả các dữ liệu của các cảm biến mạng riêng lẻ và chuyển chúng tới thiết bị quản lý trung tâm IDS xử lý dữ liệu. Hầu hết các IDS tập trung đều có nhiều cảm biến để có thể phát hiện xâm nhập trong phạm vi toàn mạng. Các log file và các tín hiệu báo động đều được gửi về thiết bị quản lý trung tâm, thiết bị này có thể dùng quản lý cũng như cập nhật cho tất cả các cảm biến. WIDS tập trung phù hợp với mạng WLAN phạm vi rộng vì dễ quản lý và hiệu quả trong việc xử lý dữ liệu.

Phân tán: WIDS phân tán thực hiện cả chức năng cảm biến và quản lý. Mô hình này phù hợp với mạng WLAN nhỏ và có ít Access Point, Wireless IDS phân tán tiết kiệm chi phí hơn so với WIDS tập trung.

2.4.9 Giải pháp ngăn ngừa và phát hiện xâm nhập IDS/IPS

Hệ thống ngăn ngừa xâm nhập mạng (NIPS – Network-based Intrusion Prevention) hát hiện tấn công, có thể khởi tạo các hành động trên thiết bị khác để ngăn chặn tấn công. Nhận ra tấn công bằng cách phân tích bản sao của lưu lượng mạng. IPS thường được triển khai trước hoặc sau firewall. Khi triển khai IPS trước firewall là có thể bảo vệ được toàn bộ hệ thống bên trong kể cả firewall, vùng DMZ. Có thể giảm thiểu nguy cơ bị tấn công từ chối dịch vụ đối với firewall. Khi triển khai IPS sau firewall có thể phòng tránh được một số kiểu tấn công thông qua khai thác điểm yếu trên các thiết bị di động sử dụng VPN để kết nối vào bên trong.

Hệ thống ngăn ngừa xâm nhập host (HIPS – Host-based Intrusion Prevention) chặn đứng trước khi tấn công đến mạng bên trong. Cung cấp khả năng bảo vệ mạng dựa vào định danh, phận loại và ngăn chặn mối đe dọa được biết hoặc chưa biết như worm, virus, đe dọa đến ứng dụng, …thường được triển khai với mục đích phát hiện và ngăn chặn kịp thời các hoạt động thâm nhập trên các host. Để có thể ngăn chặn ngay các tấn công, HIPS sử dụng công nghệ tương tự như các giải pháp antivirus. Ngoài khả năng phát hiện ngăn ngừa các hoạt động thâm nhập, HIPS còn có khả năng phát hiện sự thay đổi các tập tin cấu hình.

Lý do cần triển khai IPS

Mỗi thành phần tham gia trong kiến trúc mạng đều có chức năng, điểm mạnh, điểm yếu khác nhau. Sử dụng, khai thác đúng mục đích sẽ đem lại hiệu quả cao. IPS là một trong những thành phần quan trọng trong các giải pháp bảo vệ hệ thống. Khi triển khai có thể giúp hệ thống:

- Theo dõi các hoạt động bất thường đối với hệ thống.
- Xác định ai đang tác động đến hệ thống và cách thức như thế nào, các hoạt động xâm nhập xảy ra tại vị trí nào trong cấu trúc mạng.
- Tương tác với hệ thống firewall để ngăn chặn kịp thời các hoạt động thâm nhập hệ thống.

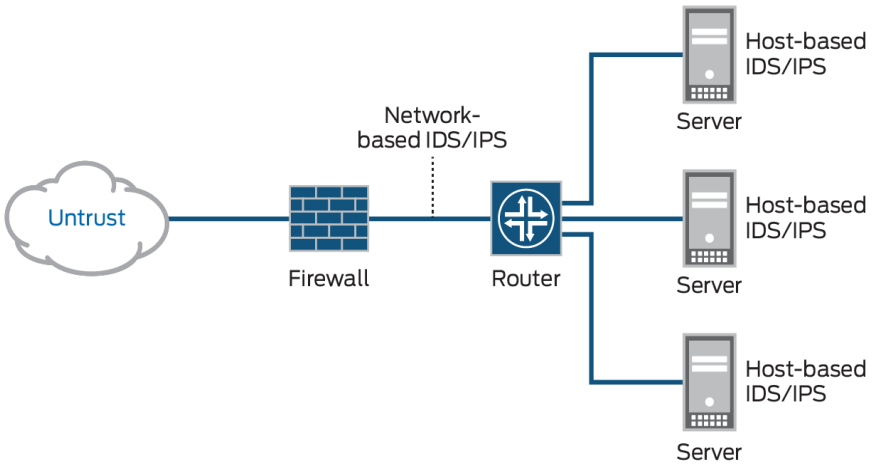
Ưu điểm, hạn chế của hệ thống ngăn ngừa xâm nhập

Ưu điểm:

- Cung cấp giải pháp bảo vệ tốt hơn đối với tài nguyên hệ thống.
- Ngăn chặn kịp thời các tấn công đã biết hoặc chưa được biết.

Hạn chế:

- Có thể gây ra tình trạng phát hiện nhầm (faulse positives), có thể không cho phép các truy cập hợp lệ tới hệ thống.



Hình 2.19: Giải pháp ngăn ngừa và phát hiện xâm nhập IDS/IPS

Một số tiêu chí triển khai

- Xác định công nghệ IDS/IPS đã, đang hoặc dự định triển khai.
- Xác định các thành phần của IDS/IPS.
- Thiết đặt và cấu hình an toàn cho IDS/IPS.
- Xác định vị trí hợp lý để đặt IDS/IPS.
- Có cơ chế xây dựng, tổ chức, quản lý hệ thống luật (rule).
- Hạn chế thấp nhất các tình huống cảnh báo nhầm (false positive) hoặc không cảnh báo khi có xâm nhập (false negative).

Có hai kiểu kiến trúc IPS chính là IPS ngoài luồng và IPS trong luồng.

✓ **IPS ngoài luồng (Promiscuous Mode IPS)**

Hệ thống IPS ngoài luồng không can thiệp trực tiếp vào luồng dữ liệu. Luồng dữ liệu vào hệ thống mạng sẽ cùng đi qua tường lửa và IPS. IPS có thể kiểm soát luồng dữ liệu vào, phân tích và phát hiện các dấu hiệu của sự xâm nhập, tấn công. Với vị trí này, IPS có thể quản lý bức tường lửa, chỉ dẫn nó chặn lại các hành động nghi ngờ mà không làm ảnh hưởng đến tốc độ lưu thông của mạng.

✓ **IPS trong luồng (In-line IPS)**

Vị trí IPS nằm trước bức tường lửa, luồng dữ liệu phải đi qua IPS trước khi tới bức tường lửa. Điểm khác chính so với IPS ngoài luồng là có thêm chức năng chặn lưu thông (traffic-blocking). Điều đó làm cho IPS có thể ngăn chặn luồng giao thông nguy hiểm nhanh hơn so với IPS ngoài luồng(Promiscuous Mode IPS). Tuy nhiên, vị trí này sẽ làm cho tốc độ luồng thông tin ra vào mạng chậm hơn.

Với mục tiêu ngăn chặn các cuộc tấn công, hệ thống IPS phải hoạt động theo thời gian thực. Tốc độ hoạt động của hệ thống là một yếu tố rất quan trọng. Quá trình phát hiện xâm nhập phải đủ nhanh để có thể ngăn chặn các cuộc tấn công ngay lập tức. Nếu không đáp ứng được điều này thì các cuộc tấn công đã được thực hiện xong và hệ thống IPS là vô nghĩa.[7]

2.5 Các yếu tố gây ảnh hưởng đến hiệu năng cho hệ thống mạng WLAN

2.5.1 Khái niệm hiệu năng mạng

Hiệu năng mạng là một vấn đề phức tạp do các yếu tố có thể tổng hợp đưa ra nhằm đánh giá vấn đề hiệu năng chưa thực sự rõ ràng. Tuy nhiên, trong thực tế rất cần có những khái niệm bản chất và sát thực tiễn với mục tiêu đánh giá được toàn bộ vấn đề hiệu năng bao gồm cả các yếu tố đo đạc, theo dõi, điều khiển đều được tính đến. Có thể sơ lược khái niệm hiệu năng mạng như sau: Hiệu năng mạng là hiệu quả và năng lực hoạt động của hệ thống mạng. Như vậy, việc đánh giá hiệu năng mạng chính là tính toán và xác định hiệu quả, năng lực thực sự của hệ thống mạng trong các điều kiện khác nhau.

Các điều kiện được sử dụng trong đánh giá hiệu năng là rất quan trọng, chúng ảnh hưởng trực tiếp tới các kết quả thu được. Trong các điều kiện ảnh hưởng tới quá trình đánh giá hiệu năng thì kịch bản mô tả là yếu tố then chốt quyết định giá trị hiệu năng tại điểm cần đo. Trong kịch bản cần xác định các tham số đầu vào rõ ràng như các nút tham gia hệ thống, thiết bị kết nối, tác nhân tham gia, giao thức hoạt động, ứng dụng triển khai, thời gian thực hiện và rất nhiều yếu tố khác kết hợp tạo ra một kịch bản hoàn thiện.

2.5.2 Các yếu tố gây ảnh hưởng đến hiệu năng cho hệ thống mạng WLAN

Các yếu tố gây ảnh hưởng đến hiệu năng của mạng không dây bao gồm: Thông lượng, Khả năng kết nối, Khả năng mở rộng, Các kỹ thuật vô tuyến không dây, Khả năng tương thích, Bảo mật, Cách sử dụng linh hoạt.

- ✓ **Thông lượng**

Thông lượng là được định nghĩa chính là số lượng của các gói dữ liệu được truyền bằng cách gửi và nhận bởi người nhận trong thời gian cho trước. Như vậy, đến một mức độ đủ lớn nào đó, hiệu năng của mạng phụ thuộc vào thông lượng cũng như ta cần mỗi gói dữ liệu được truyền thành công. Thông lượng có thể giảm sút nếu mạng thiết kế không thích hợp, định tuyến không rõ ràng, một lỗi liên kết hiện diện hoặc có sự chật chội trên đường truyền. Cách tốt nhất để có được thông

lượng mạng hiệu quả nhất là phải có một giao thức định tuyến tốt để các liên lạc diễn ra một cách hiệu quả.

- ✓ **Khả năng kết nối**

Một yếu tố quan trọng của hiệu năng mạng là khả năng kết nối. Khả năng kết nối nên được thực hiện theo cách mà có thể tự tổ chức trong trường hợp xảy ra vấn đề hoặc xuất hiện lỗi. Để đạt được điều này cần phải phát triển thuật toán điều khiển cấu hình và tự tổ chức.

- ✓ **Khả năng mở rộng**

Khả năng mở rộng là hoàn toàn cần thiết cho mỗi mạng. Định nghĩa cơ bản cho việc này là khi mạng phát triển và có thêm nhiều nút kèm theo hiệu năng của mạng không nên giảm. Một số vấn đề có thể xảy ra nếu mạng không có khả năng mở rộng là giao thức định tuyến có thể không có khả năng tìm thấy đường đi đáng tin cậy cho việc truyền dữ liệu. Thêm vào đó, giao thức vận có thể bị lỗi với kết quả là thông lượng quan trọng có thể bị giảm sút. Vì vậy, cần phải có các kỹ thuật cần thiết để mở rộng các giao thức từ tầng MAC đến tầng ứng dụng.

- ✓ **Các kỹ thuật vô tuyến không dây**

Các mạng không dây có một quy mô rất rộng lớn dựa trên các tín hiệu sóng vô tuyến được gửi đến hoặc từ các nút tham gia vào mạng. Vì vậy nó rất quan trọng và có tính quyết định khi mà các kỹ thuật sóng vô tuyến được sử dụng một cách hợp lý. Nếu kỹ thuật radio có hiệu quả thì việc mất dữ liệu được giảm xuống đến một mức độ lớn. Hầu hết các vấn đề xảy ra khi radio bị hỏng không bắt được tín hiệu hoặc tìm kiếm ở một số hướng khác. Điều này xảy ra với ăng ten đa hướng khi tín hiệu truyền xáy ra tình trạng tin tưởng vào các ăng ten cùng loại và chúng thay đổi tiêu cự liên tục. Hiệu ứng này gọi là " điếc " có nghĩa là người nhận đang tìm hướng bên phía ngoài vùng phát của người gửi. Vấn đề như thế này có thể được giải quyết nếu ta sử dụng ăng ten định hướng thông minh. Một giải pháp khác là lựa chọn các hệ thống Multi Input Multi Output hoặc ăng ten Multi-Radio.

- ✓ **Khả năng tương thích**

Các mạng không dây có khả năng tương thích với cả mesh client và client thông thường. Điều này có thể được thực hiện bởi các router với sự tích hợp của nhiều loại mạng không dây không đồng nhất. Ngoài ra các công cụ quản lý mạng này cần phải được thiết kế theo cách mà chúng thuận tiện cho các hoạt động, giám sát hiệu năng và các thông số thiết kế của mạng để làm cho hiệu suất cao hơn và đáng tin cậy hơn.

- ✓ **Bảo mật**

Topo của mạng không dây WLAN là dạng phân tán. Khi kiến trúc mạng trở nên phân tán hơn thì vấn đề bảo mật trên mạng càng gia tăng. Cho đến nay vẫn chưa có nhiều đề án liên quan đến an ninh trên mạng không dây. Lý do cho việc này là không cần phải đưa ra các khóa công khai cho các nút. Điều này mang lại nhiều hơn sự liên hệ khi quan sát đặc tính bảo mật của mạng không dây.

- ✓ **Cách sử dụng linh hoạt**

Các thiết kế của giao thức phải quan tâm nhiều hơn đến quyền tự chủ của các mạng như quản lý năng lượng, tự tổ chức, tự hàn gắn, và thủ tục chứng thực người sử dụng đăng ký mạng nhanh chóng. Ngoài ra các công cụ quản lý mạng yêu cầu phải được phát triển để duy trì có hiệu quả hoạt động, giám sát hiệu năng, cũng như cấu hình các thông số của mạng không dây. Cơ chế tự chủ trong các giao thức bên cạnh những công cụ này sẽ cho phép triển khai các mạng không dây một cách thành công.

2.5.3 Các tham số đánh giá hiệu năng

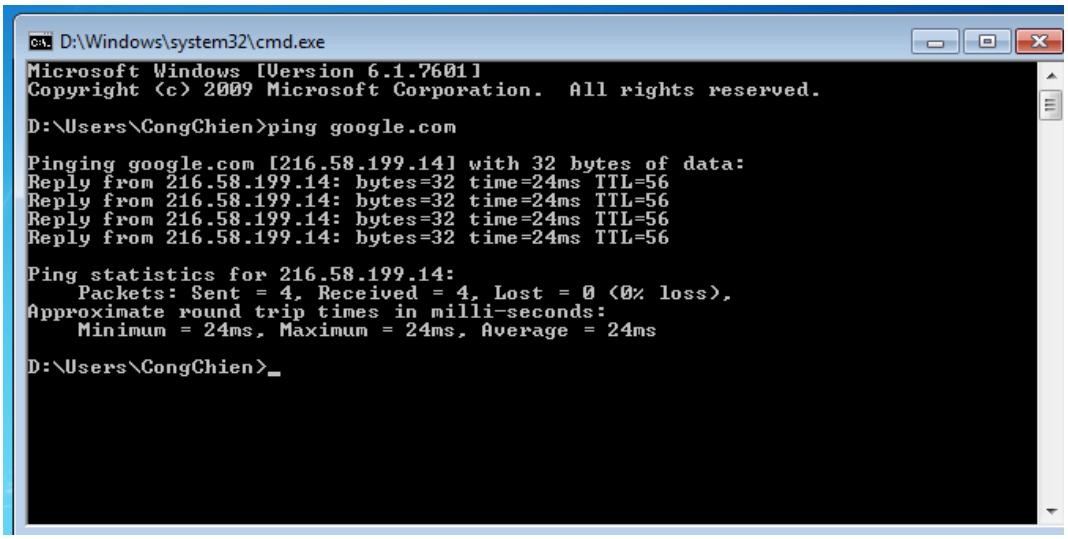
Để lượng hóa vấn đề hiệu năng mạng, cần thiết phải có bộ tham số tiêu biểu đặc trưng cho vấn đề này. Trong đó, các tham số sau đây được sử dụng như những khái niệm điển hình mà nhìn vào chúng có thể cho thấy kết quả của đánh giá hiệu năng mạng.

2.5.3.1 Tính sẵn sàng (Availability)

Tính sẵn sàng là thước đo đầu tiên khi xác định và đánh giá hiện trạng mạng có khả năng phục vụ, đáp ứng yêu cầu hay không. Tham số này cho

phép chỉ ra luồng thông tin có đang được chuyển tiếp qua hệ thống mạng hay bị tắc nghẽn cần phải xử lý, các dịch vụ mạng đang được cung cấp có sẵn sàng cho việc trả lời các yêu cầu đưa ra. Vấn đề liên thông giữa các hệ thống trong mạng cũng được đề cập trong tính sẵn sàng.

Một trong các công cụ, phương pháp đơn giản thường được sử dụng khi kiểm tra tính sẵn sàng của hệ thống mạng là sử dụng chương trình ping. Chương trình khi thực hiện sẽ gửi các gói tin dưới giao thức ICMP tới phía máy cần kiểm tra và đợi kết quả trả lời, nếu có kết quả trả lời chúng ta có thể xác định được tính sẵn sàng của hệ thống đích.



Hình 2.20: Kiểm tra tính sẵn sàng với chương trình ping

Ping là 1 phương thức kiểm tra kết nối của hai thiết bị trên đường truyền bằng cách đo tổng thời gian gửi và phản hồi khi gửi một gói tin chuẩn từ thiết bị nguồn đến thiết bị đích.

Đơn vị của ping thường được tính bằng ms.

Trong các phương thức trao đổi gói theo phương thức TCP thì người ta thường dùng Ping để ám chỉ chất lượng của đường truyền.

Ping phụ thuộc vào 3 yếu tố:

+ Kết nối: tốc độ mạng

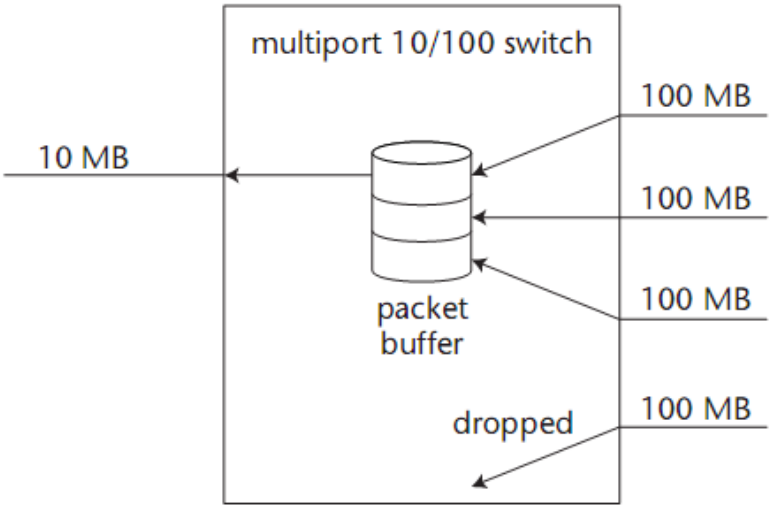
+ Điểm A: máy tính, điện thoại

+ Điểm B: server của nhà cung cấp dịch vụ

Trong ví dụ trên, yêu cầu gửi đi đã có kết quả đáp ứng, trong một số trường hợp và tình huống thực tế việc mất gói tin thường xuyên xảy ra, điều nay có thể do nhiều nguyên nhân khác nhau, trong đó có một số nguyên nhân điển hình sau:

- Xung đột xảy ra giữa các phân đoạn mạng: Các giao thức điều khiển truy cập đóng vai trò quan trọng trong quá trình kiểm soát xung đột, việc lựa chọn giao thức phù hợp ảnh hưởng lớn tới xử lý các gói tin khi hệ thống gặp vấn đề.

- Các gói tin bị hủy bởi các thiết bị mạng: Mỗi thiết bị đều có những bộ đệm nhằm lưu trữ những gói tin chưa kịp xử lý. Để kiểm soát bộ đệm, thông thường các thiết bị sẽ sử dụng một số giải thuật nhằm duy trì trật tự của bộ đệm như giải thuật DropTail, RED, DDR,... trong các giải thuật này luôn tồn tại phương án hủy gói tin khi thỏa mãn điều kiện hủy nhằm duy trì hoạt động tốt nhất cho thiết bị, tránh tắc nghẽn và quá thời gian xử lý.



Hình 2.21: Hiện tượng hủy gói tin trên bộ đệm của thiết bị

2.5.3.2 Thời gian đáp ứng (Response time)

Khi yêu cầu được gửi tới, sẽ có một khoảng thời gian dành cho việc xử lý trước khi trả về kết quả, khoảng thời gian này được gọi là thời gian đáp ứng, bao gồm thời gian đi, thời gian xử lý yêu cầu và thời gian về. Đây là tham số rất quan trọng ảnh hưởng tới quá trình đánh giá khả năng giải quyết vấn đề khi có yêu cầu và hạ tầng truyền thông. Thời gian đáp ứng chậm thường do khả năng giải quyết vấn đề của ứng dụng, hạn chế trong truyền và nhận thông tin trên giao thức và hạ tầng truyền thông tin. Có thể chỉ ra một số các yếu tố ảnh hưởng trực tiếp tới thời gian đáp ứng như sau:

- Quá tải trong các phân đoạn mạng
- Các lỗi xuất hiện trên mạng
- Khiếm khuyết khi mở rộng mạng
- Xử lý các thông tin quảng bá trên mạng chưa tốt
- Thiết bị mạng kém chất lượng
- Quá tải trên các nút mạng

Thời gian đáp ứng được đo bằng mili giây (ms). Thông thường với các kết nối mạng LAN thì thời gian đáp ứng nhỏ hơn 1 hoặc 2 mili giây, với các kết nối mạng WAN thời gian đáp ứng có thể lên tới 200 hoặc 300 mili giây là chấp nhận được, giá trị cụ thể tùy thuộc vào tốc độ đường truyền giữa các hệ thống.

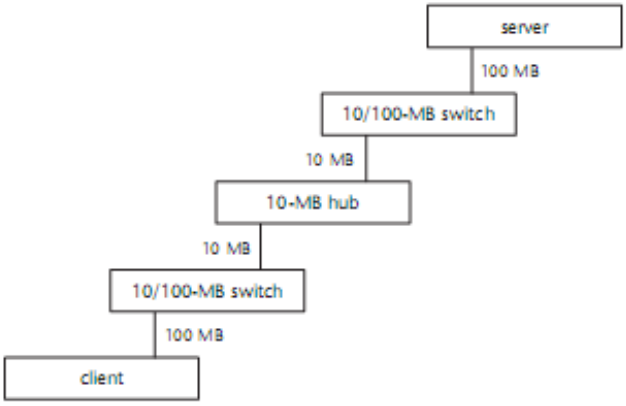
2.5.3.3 Khả năng sử dụng mạng (Network utilization)

Khi hệ thống mạng hoạt động, việc đánh giá khả năng sử dụng mạng là yếu tố quan trọng khi cần đánh giá hiệu năng mạng. Hệ thống mạng có thể hoạt động ở trạng thái bình thường trong đa số thời gian, tuy nhiên trong thực tế thì hệ thống có thể chưa hoạt động hết công suất và khả năng, như vậy phần dư thừa khi xây dựng mạng chưa tính đến cũng là yếu tố giảm đi hiệu năng của hệ thống. Để tính tham số khả năng sử dụng mạng, thông thường công

thức chính được sử dụng là phần trăm thời gian sử dụng mạng trong suốt thời gian hoạt động mạng. Trong rất nhiều tình huống, có những thời điểm hệ thống sử dụng 100% công suất nhưng có những thời điểm là về 0% cho trạng thái không có yêu cầu. Để tăng tính chính xác khi xác định khả năng sử dụng mạng, việc tính toán lưu lượng dữ liệu được truyền qua hệ thống trong tổng thời gian hoạt động đã được sử dụng. Giá trị cụ thể khi tính toán còn phụ thuộc nhiều vào phương thức truyền trên các kết nối được sử dụng tại các giao diện mạng. Thông lượng mạng (Network throughput) là tổng lượng dữ liệu chuyển tiếp qua các nút cần đo trong một thời điểm xác định.

Người quản trị hệ thống mạng có thể xác định thông lượng mạng bằng phương pháp tìm nút cổ chai giữa 2 điểm cần đo. Đồng thời, trong một số tình huống nhiều người sẽ khẳng định thông lượng của hai điểm sẽ được xác định bằng giá trị băng thông (Bandwidth) tại 2 điểm đó. Những điểm nêu trên là hoàn toàn không chính xác bởi 2 lý do chính sau đây:

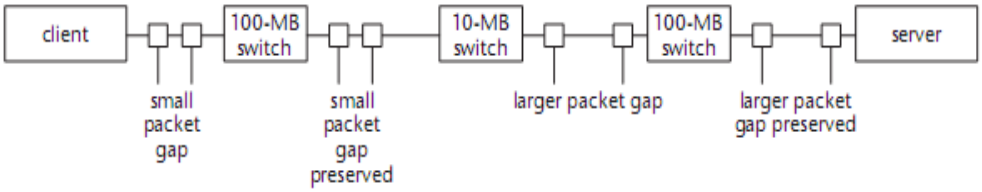
- Giá trị băng thông không phụ thuộc vào thời gian đo và đây là khái niệm khác hoàn toàn với thông lượng.
- Thông lượng thực tế phụ thuộc rất nhiều vào tổng thể kết nối, thiết bị sử dụng, ứng dụng hoạt động, dịch vụ cung cấp của hệ thống tại thời điểm cần đo.



Hình 2.22: Độ phức tạp khi xác định thông lượng giữa client và server

2.5.3.4 Khả năng của băng thông mạng (Network bandwidth capacity)

Khả năng của băng thông là một trong những yếu tố để xác định thông lượng mạng trong thời điểm cần đo. Tổng dung lượng băng thông có khả năng giữa hai nút mạng sẽ ảnh hưởng lớn tới hiệu năng của mạng điều này là khá hiển nhiên, khi ta kết nối mạng 100BaseTX thì đương nhiên luôn nhanh hơn với kết nối T1. Tuy nhiên việc xác định khả năng của băng thông giữa 2 điểm cần đo thường rất phức tạp do tổng thể kết nối của hệ thống tác động (mô tả tại hình 2.23), do vậy đòi hỏi phải có kỹ thuật cụ thể trong việc xác định giá trị lớn nhất trong khả năng của băng thông mạng khi hoạt động. Có 2 kỹ thuật chính được sử dụng để xác định khả năng băng thông đó là kỹ thuật packet pair/packet train và kỹ thuật thống kê gói tin.



Hình 2.23: Minh họa kỹ thuật packet pair/packet train

2.6 Kết luận Chương 2

Trong chương II này chúng ta đã nghiên cứu và đánh giá về các vấn đề bảo mật cho mạng WLAN, phân tích và đánh giá được vai trò của bảo mật trong mạng không dây. Tìm hiểu nguy cơ mất an ninh mạng không dây và giới thiệu một số dạng tấn công của mạng WLAN, cộng với sự đi sâu và tìm hiểu các kiến trúc cơ bản của mạng WLAN và các phương thức bảo mật và chống xâm nhập trái phép. Các yếu tố gây ảnh hưởng đến hiệu năng cho hệ thống mạng WLAN.

Trong chương III tiếp theo chúng ta sẽ phân tích hiện trạng hệ thống mạng WLAN của trường Cao đẳng Lý Thái Tổ, đưa ra giả pháp, đi sâu vào biện pháp cụ thể để tiến hành tăng hiệu năng cho mạng WLAN.

CHƯƠNG 3: PHÂN TÍCH, MÔ PHỎNG TĂNG HIỆU NĂNG CHO HỆ THỐNG MẠNG WLAN CAO ĐẲNG LÝ THÁI TỔ

3.1 Phân tích hiện trạng hệ thống mạng WLAN của Cao đẳng Lý Thái Tổ

3.1.1 Hiện trạng hệ thống mạng WLAN

Trường đứng chân trên địa bàn Phường Đình Bảng, Thị xã Từ Sơn, Tỉnh Bắc Ninh - một thành phố trẻ đang trong quá trình công nghiệp hoá mạnh mẽ, với vị trí đắc địa là cửa ngõ thủ đô Hà Nội. Bắc Ninh được biết đến là nơi tập trung của nhiều khu công nghiệp lớn như: VSIP, Tiên Sơn, Yên Phong. Đây là các khu công nghiệp hội tụ các doanh nghiệp hàng đầu về công nghệ cao cũng như các doanh nghiệp phụ trợ cho các tập đoàn lớn như Samsung, LG, Canon, Hồng Hải - các tập đoàn hàng năm có nhu cầu tuyển dụng nhân sự rất lớn để phục vụ nghiên cứu và phát triển sản xuất.

Hình 3.1: Sơ đồ phối cảnh quan trường Cao đẳng Lý Thái Tổ

Toàn thể trường là một khu liên hợp hiện đại bao gồm các hạng mục:

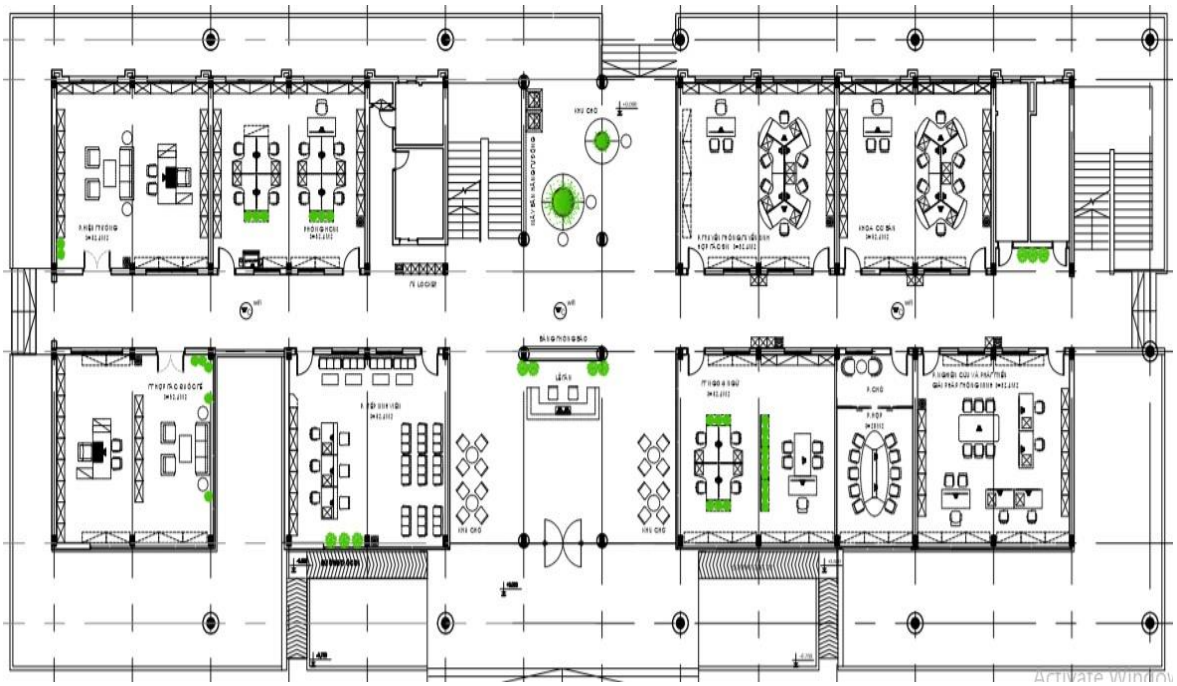
- Văn phòng nhà trường
- Nhà Hiệu bộ - Học chính
- Nhà Hội trường – Giảng đường
- Thư viện
- Khu nhà xưởng thực hành
- Ký túc xá
- Vườn sinh viên, hồ cá, Quảng trường…

Các hạng mục công trình được kết nối bằng hệ thống đường giao thông thuận lợi xen lẫn các khoảng sân vườn, tiểu cảnh cây xanh, vườn hoa. Toàn bộ các khối nhà trong trường được trang bị hệ thống điều hòa trung tâm sử dụng cho tất cả phòng học, phòng làm việc với hệ thống điều khiển thông minh vận hành tự động. Hệ thống loa thông báo, camera IP giám sát… Tất cả các hệ thống vận hành tự động và toàn bộ các hạng mục trên được nối mạng với nhau, phòng server được đặt trên tầng 3 nhà Hiệu Bộ là nơi chứa toàn bộ các Server, có thể nói phòng điều khiển này là đầu não của trường Cao đẳng Lý Thái Tổ.

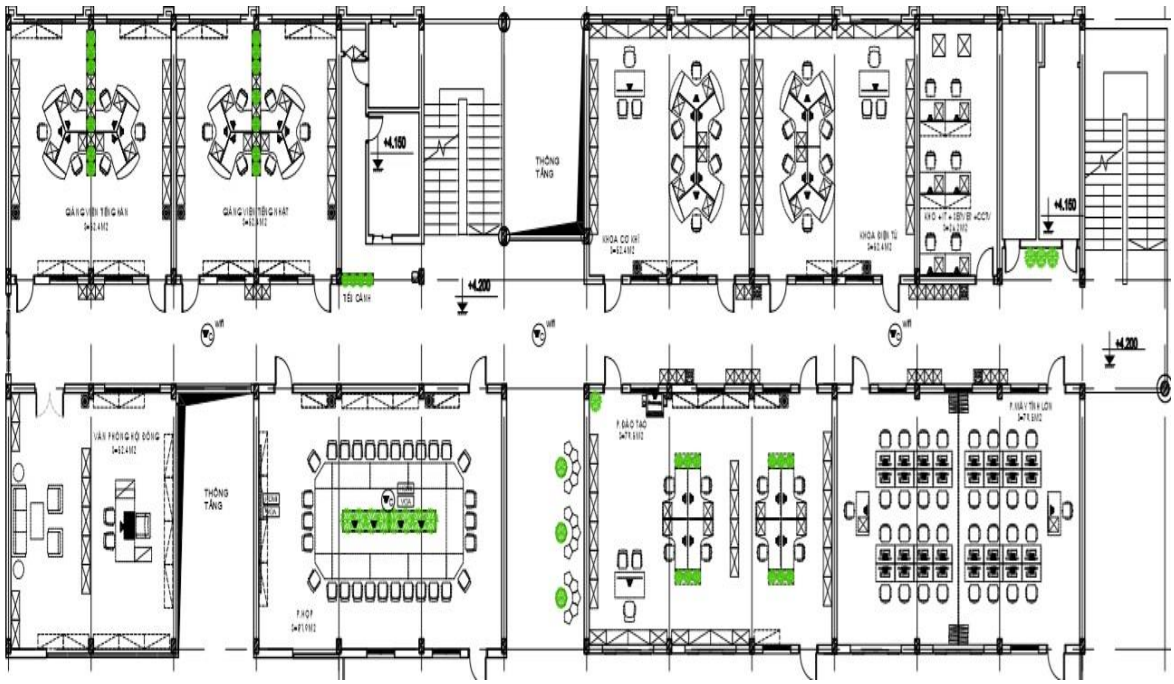
Toàn bộ trường được trang bị gần 840 máy tính cho phòng học, thư viện và phòng làm việc. Phòng làm việc bao gồm các phòng ban với gần 100 máy tính nằm tại nhà hiệu bộ được nối mạng với trung tâm dữ liệu, Thư viện với gần 100 máy tính được trang bị hệ thống Server riêng phục vụ cho sinh viên tra cứu sách, tài liệu và tự học trên mạng, trường còn có 10 phòng tự học nằm tại nhà hiệu bộ - học chính được trang bị Wifi Free phục vụ cho việc tự học và hệ thống phòng học khoa Tin học và các lớp tin học văn phòng với 8 phòng, mỗi phòng gồm 80 máy tính hiện đại cấu hình đủ đáp ứng tất cả các nhu cầu cho sinh viên khóa Tin học.

Nhà trường trang bị 02 đường cáp quang tốc độ cao phục vụ cho việc truy cập Internet của toàn trường, các thiết bị số như Camera IP, các Server và việc phủ sóng Wifi trong toàn bộ khuôn viên trường. 01 đường phục vụ riêng cho việc đăng ký học và trang chủ Website của trường, 01 đường phục vụ cho riêng thư viện, 01

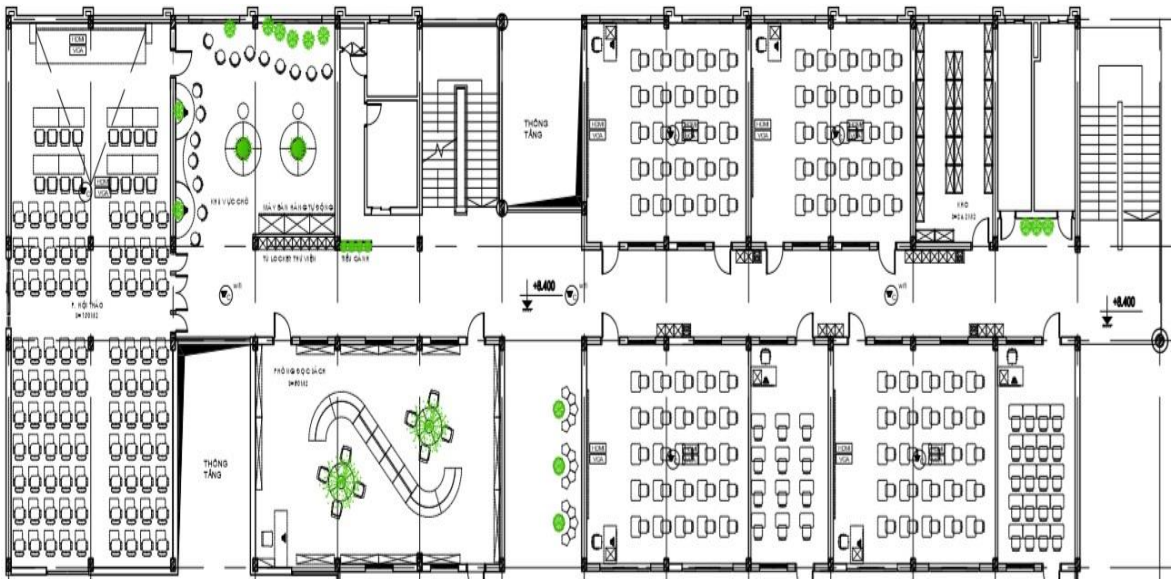
đường dành riêng cho phòng ban và bộ môn truy cập Internet và cuối cùng 01 đường chuyên dùng cho việc học Online, 01 đường phục vụ cho việc phủ sóng Wifi toàn trường phục vụ cho sinh viên.



Hình 3.2: Sơ đồ mặt bằng hệ thống mạng tầng 1 – nhà Hiệu bộ



Hình 3.3: Sơ đồ mặt bằng hệ thống mạng tầng 2 – nhà Hiệu bộ



Hình 3.4: Sơ đồ mặt bằng hệ thống mạng tầng 3 – nhà Hiệu bộ

Với mô hình như trên nên việc thiết kế mạng cho trường cũng đã được tính toán cẩn thận và chi tiết để có thể đáp ứng được nhu cầu hiện tại và khả năng dễ dàng nâng cấp khi có nhu cầu phát sinh trong tương lai.

3.1.2 Vấn đề bảo mật mạng WLAN tại Cao đẳng Lý Thái Tổ

Để làm nổi bật rõ các yêu cầu bảo vệ thông tin tại trường chúng ta cần phân tích nguyên nhân của sự mất an toàn thông tin.

Ngày nay cùng với sự phát triển của các công nghệ mạng, thì mạng LAN không dây (WLAN) đã được sử dụng rộng rãi trong nhiều cơ quan tổ chức. Lợi thế của mạng không dây chính là việc sử dụng đường truyền vô tuyến, tuy nhiên cùng với lợi thế đó là vấn đề bảo mật cho nó trở nên khó hơn. Sóng vô tuyến truyền trong không gian nên có thể bị truy cập dễ dàng nếu sử dụng các thiết bị thích hợp.

Cùng với sự phát triển không ngừng của Internet và các dịch vụ trên Internet, số lượng các vụ tấn công trên Internet cũng tăng theo cấp số nhân. Trong khi các phương tiện thông tin đại chúng ngày càng nhắc nhiều đến Internet với những khả năng truy nhập thông tin dường như đến vô tận của nó, thì các tài liệu chuyên môn bắt đầu đề cập nhiều đến vấn đề bảo đảm an ninh và an toàn dữ liệu cho các máy tính được kết nối vào mạng Internet.

Không chỉ số lượng các cuộc tấn công tăng lên nhanh chóng, mà các phương pháp tấn công cũng liên tục được hoàn thiện. Nhu cầu bảo vệ thông tin của trường Cao đẳng Lý Thái Tổ được chia thành ba loại gồm: Bảo vệ dữ liệu; Bảo vệ các tài nguyên sử dụng trên mạng và Bảo vệ danh tiếng của cơ quan:

Hiện nay hệ thống mạng tại Cao đẳng Lý Thái Tổ đã được trang bị Firewall ASA5510, 250 máy tính và máy chủ đã trang bị phần mềm diệt virút bản quyền.

Bảng 3.1: Bảng hiện trạng hệ thống mạng trường Cao đẳng Lý Thái Tổ

TT	Giải pháp bảo mật của hệ thống	Khả năng đáp ứng	
		Mức đáp ứng	có/không
1	Giải pháp tường lửa (Firewall)	Layer 3 - 4	có
		Layer 4 - 7	không
2	Giải pháp dùng phần mền diệt Virut	Máy chủ	30%
		máy trạm	có
3	Giải pháp lưu trữ / phục hồi dữ liệu (Backup/restore)	Backup/restore độc lập	có
		Backup/restore tập chung, đặt lịch, lưu trữ	không
4	Giải pháp dùng các thiết bị phục vụ hỗ trợ phòng chống tấn công, xâm nhập (IDS/IPS)	Toàn mạng	không
5	Giải pháp giám sát an ninh: Phát hiện máy tính mới cắm váo mạng, các dịch vụ không được sử dụng…	Vùng Server quan trọng	không
6	Giải pháp thiết bị phục vụ hỗ trợ xác thực	Xác thực tập trung	không
7	Giải pháp thiết bị phục vụ hỗ trợ kiểm tra đánh giá định kỳ	Toàn mạng	không

Qua bảng tổng hợp trên và để từng bước tăng hiệu năng mạng cũng như khả năng bảo mật cho hệ thống mạng WLAN của Cao đẳng Lý Thái Tổ thì chúng ta cần phải đưa ra được giải pháp có khả năng phát hiện các truy cập bất hợp pháp, những cuộc tấn công vào máy chủ, dịch vụ mạng nhằm đảm bảo cho hệ thống hoạt động có tính bảo mật cao. Vì vậy giải pháp sử dụng công nghệ IDS/IPS có thể đảm đương nhiệm vụ này.

3.2 Đề xuất các phương pháp tăng hiệu năng cho hệ thống mạng WLAN tại Cao đẳng Lý Thái Tổ

Từ thực trạng hệ thống mạng WLAN đang sử dụng tại trường Cao Đẳng lý Thái Tổ đề xuất các giải pháp tăng hiệu năng cho hệ thống như:

- Đối với hệ thống phần cứng mạng sử dụng phần mềm VNPT-CAB để tối ưu.
- Đối với hệ thống phần mềm dùng các phương pháp Kiểm soát hiệu năng của mạng không dây như: Định tuyến; Chất lượng dịch vụ; Vấn đề về an ninh trong mạng không dây.

3.2.1 Sử dụng phần mềm VNPT-CAB tối ưu hệ thống mạng WLAN

3.2.1.1 Vùng phủ

Khi triển khai một mạng vô tuyến "indoor", việc xác định vùng phủ sóng là một vấn đề cơ bản. Vùng phủ sóng được xác định qua khoảng cách mà một mạng vô tuyến có thể phát và thu ở một tốc độ cho trước theo các nguyên tắc hoạt động trong băng tần của nó.

Có sự nhầm lẫn khi cho rằng băng tần hoạt động của hệ thống càng cao thì vùng phủ sóng càng nhỏ. Thực sự điều này chỉ đúng đối với môi trường "outdoor" hay các môi trường không gian tự do. Môi trường "indoor" thường có nhiều vật cản hay các vật hấp thụ sóng vô tuyến, do vậy không thể sử dụng mô hình không gian tự do để việc xác định vùng phủ sóng của mạng vô tuyến "indoor".

Vùng phủ sóng của mạng sẽ quyết định và có ảnh hưởng trực tiếp đến việc xác định chi phí và dung lượng của hệ thống tức là ảnh hưởng đến tốc độ truy nhập. Việc phân tích, xác định vùng phủ sóng của một mạng vô tuyến "indoor" dựa trên các biến và tham số của hệ thống và mô hình suy hao đường truyền tín hiệu cho các mạng vô tuyến.

Các tham số hệ thống: vùng phủ sóng được tính toán dựa trên giá trị công suất phát xạ cực đại cho phép (giá trị EIRP) và độ nhạy thu danh định.

Mô hình suy hao đường truyền tín hiệu: vùng phủ sóng của một mạng vô tuyến trong môi trường "indoor" có khác biệt đáng kể so với môi trường "outdoor". Việc xác định vùng phủ sóng này được dựa trên mô hình suy hao công suất phát (suy hao này là do bị hấp thụ bởi các vật cản trong môi trường). Biên độ suy hao được đo nhiều lần và được sử dụng để điều chỉnh trong các mô hình suy hao đường truyền của môi trường không gian tự do nhằm tăng độ chính xác trong việc xác định suy hao đường truyền tín hiệu đối với môi trường "indoor", qua đó sẽ xác định chính xác hơn vùng phủ sóng của mạng. Mô hình suy hao đường truyền tuyến tính được chọn để mô tả suy hao đường truyền trong trường hợp máy phát và máy thu trong cùng một tầng. Theo mô hình này, suy hao đường truyền của môi trường "indoor" (tính theo dB) được xác định bằng suy hao đường truyền của không gian tự do cộng với một hệ số biến đổi theo cự ly. Hệ số này được xác định thông qua các thử nghiệm thực tế. Kết quả là suy hao đường truyền tín hiệu trung bình được tính theo công thức sau:

$$PL(d, f)[dB] = PL_{FS}(d, f) + a.d$$

với d là khoảng cách tính theo đơn vị mét, f là tần số, PL_{FS} là suy hao đường truyền của không gian tự do và a là hệ số suy giảm. Thông thường, a có giá trị bằng 0,47 [dB/m] Vùng phủ sóng của mạng: sẽ được xác định thông qua giá trị d trong công thức trên với suy hao đường truyền được xác định theo công thức sau với giá trị của các biến và tham số tương ứng với các băng tần khác nhau.

$$\Pr[dB] = Pt[dB] + Gt[dB] - PL(d, f)[dB] + Gr[dB]$$

với $\Pr[dB]$ là công suất thu tối thiểu đáp ứng yêu cầu PER/FER

$Pt[dB]$ là công suất phát cực đại cho phép

$Gt[dB]$ là tăng ích anten phát

$Gr[dB]$ là tăng ích anten thu

$PL(d, f)[dB]$ là suy hao đường truyền của môi trường "indoor".

Một vấn đề khác nữa là mỗi một điểm truy nhập trong mạng chia sẻ một băng tần cố định cho tất cả các đối tượng sử dụng kết nối đến nó. Do vậy vấn đề quan trọng là cần phải đảm bảo cài đặt số điểm truy nhập hiệu quả cho một lượng đối tượng sử dụng và lưu lượng mong muốn. Tức là cần phải cân bằng giữa vùng phủ sóng với tốc độ truy nhập của hệ thống. Để có thể giải quyết vấn đề này cần phải nghiên cứu về mật độ người sử dụng trong khu vực lắp đặt, và phải dự báo về khả năng mở rộng phát triển của hệ thống cũng như dự báo nhu cầu của người sử dụng trong khu vực này trong tương lai [3].

3.2.1.2 Sử dụng phần mềm VNPT-CAB tối ưu hệ thống phần cứng

Hiệu năng của WLAN được thiết lập cho dù hệ thống đó có an toàn hay không. Hiệu quả của một hệ thống cũng dựa vào hiệu năng của nó. Vì vậy điều quan trọng là một hệ thống không bao giờ xảy ra sự cố trong một thời gian dài và các gói dữ liệu không bị mất giữa các nút khác nhau. Đối với các TOPO mạng chung, hiệu năng của mạng nói chung tỷ lệ nghịch với khoảng cách giữa nguồn và đích. Tuy nhiên, đây không phải là trường hợp của WLAN như khả năng mở rộng có thể tăng hiệu năng bởi vì các nút của mạng lưới cung cấp nhiều đường dẫn giữa nguồn và đích. Các trường hợp khác khi hiệu năng của mạng giảm chính là khi tín hiệu yếu dần, nghẽn mạch trên đường dẫn hoặc sử dụng giao thức không thích hợp.

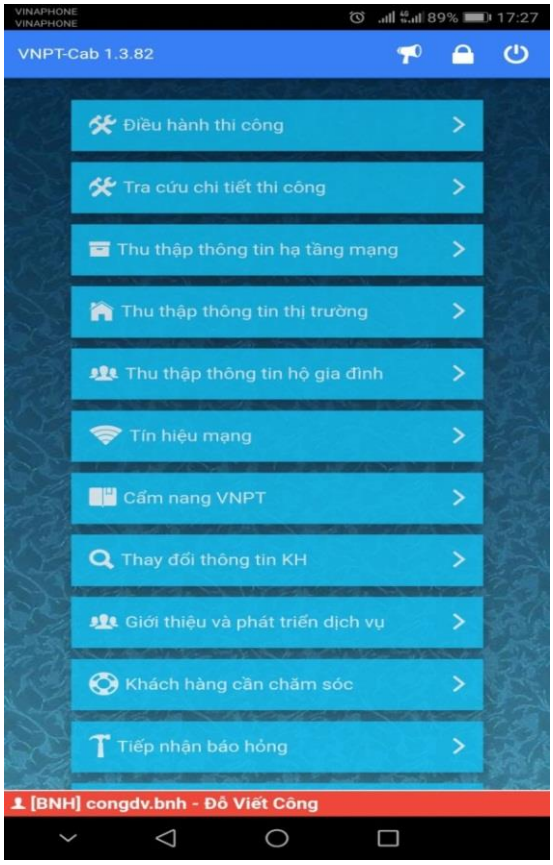
Sử dụng phần mềm VNPT-CAB để tối ưu hệ thống mạng wifi, đảm bảo cường độ tín hiệu tại các điểm trong tòa nhà tốt nhất có thể với hệ thống phần cứng hiện có trong trường.

Phần mềm VNPT-CAB là phần mềm được VNPT phát triển, sử dụng trên điện thoại di động. Mục đích dùng cho nhân viên kinh doanh và kỹ thuật sử dụng trong công trong công tác sản xuất kinh doanh. Đăng nhập bằng USER tập trung do tập đoàn VNPT cấp. Ngoài ra phần mềm còn trang bị tính năng đo kiểm sóng di động, Wifi.

Các modul tính năng của phần mềm

- Điều hành thi công
- Tra cứu chi tiết thi công
- Thu thập thông tin hạ tầng mạng
- Thu thập thông tin thị trường
- Thu thập thông tin hộ gia đình
- Xử lý phản hồi của khách hàng
- Tín hiệu mạng
- Cẩm nang VNPT
- Các báo cáo thống kê…

Trong các modul tính năng của phàn mềm thì tính năng Tín hiệu mạng được sử dụng để đo cường độ tín hiệu từ AP đến.



Hình 3.5: Chức năng đo kiểm sóng của phần mềm VNPT-CAB

Sử dụng phần mềm:

Phần mềm được viết ra mục đích sử dụng phục vụ cho công tác sản xuất dinh doanh của các đơn vị trực thuộc tập đoàn, quản lý tập trung các hoạt động sản xuất kinh doanh của các đơn vị như: Sửa chữa báo hỏng, lập hợp đồng cung cấp dịch vụ, tra cứu thông tin hạ tầng mạng, nhu cầu dịch vụ, hạ tầng đối thủ, đo kiểm chất lượng sóng di động, Wifi…

Áp dụng sử dụng phần mềm trong việc tối ưu phần cứng hệ thống mạng Wifi:

- Đăng nhập bằng User do Tập đoàn cấp.
- Kết nối điện thoại sử dụng phần mềm đến từng AP.
- Đo kiểm với khoảng cách đo thử test sóng từ Client đến AP với bán kính là 20m.
- Dựa vào kết quả đo dịch chuyển vị trí AP đến vị trí tối ưu nhất.

Hình 3.6: Chức năng đo kiểm sóng của phần mềm VNPT-CAB

Yêu cầu sau khi tối ưu hệ thống phần cứng mạng WLAN. Hệ thống WLAN phủ sóng khắp toà nhà, có chất lượng tín hiệu sóng đảm bảo cho các kết nối từ AP đến Client. Khoảng cách đo thử test sóng từ Client đến AP là 20m.

Bảng 3.2: Kết quả đo kiểm sóng bằng phần mềm VNPT-CAB tại trường Cao đẳng Lý Thái Tổ

STT	SSID	Tốc độ	Cường độ	Đánh giá
1	Hieubo 11	70 Mbps	-47 dBm	đạt
2	Hieubo 12	67 Mbps	-56 dBm	đạt
3	Hieubo 13	71 Mbps	-46 dBm	đạt
4	Hieubo 21	65 Mbps	-57 dBm	đạt
5	Hieubo 22	72 Mbps	-46 dBm	đạt
6	Hieubo 23	71 Mbps	-45 dBm	đạt
7	Hieubo 31	69 Mbps	-52 dBm	đạt
8	Hieubo 32	70 Mbps	-47 dBm	đạt
9	Hieubo 33	68 Mbps	-55 dBm	đạt
10	Thuvien	72 Mbps	-46 dBm	đạt
11	Quangtruong	73 Mbps	-45 dBm	đạt

3.2.2 Kiểm soát hiệu năng của mạng không dây

Thông lượng, độ trễ và tỷ lệ mất gói tin là một trong những vấn đề quan trọng quyết định mạng hoặc truyền thông có tin cậy hay không. Nó khá rõ ràng ngoài khả năng mở rộng và các vấn đề về an ninh, vì vậy trong phần này của luận văn chúng ta sẽ tập trung chủ yếu vào các yếu tố có thể trợ giúp để có được thông lượng tốt hơn và do đó sẽ cải thiện được hiệu năng của mạng. Thông lượng tốt sẽ làm cho chúng ta có thể bảo mật dữ liệu thành công từ một điểm này tới một điểm

khác. Và một cách làm hiệu quả để tăng hiệu năng của mạng chính là thông qua hiệu quả của việc định tuyến. Một yếu tố khác có thể giúp tăng cường thông lượng mạng là cân bằng tải. Mất cân băng tải có thể xảy ra tại một thời điểm, một thời gian nhất định và nó sẽ làm dòng lưu lượng đi trệch hướng. Vì thế điều này sẽ dẫn đến hiện tượng tắc nghẽn mạng và giảm thông lượng mạng.

3.2.2.1 Tăng hiệu năng của mạng không dây:

Thông lượng của một mạng không dây có thể được tăng lên bằng chính 3 phương pháp sau:

- Sử dụng có hiệu quả các số liệu và các giao thức định tuyến.
- Sử dụng sự cân bằng lưu lượng để cải thiện chất lượng dịch vụ (QoS).
- Tăng cường bảo mật và phòng chống xâm mạng trái phép để không gây ảnh hưởng tới thông lượng của hệ thống mạng.

3.2.2.2 Định tuyến:

Định tuyến là một quá trình để giải quyết từ đầu đến cuối con đường đi giữa nguồn và nút đích. Các đặc điểm chính của định tuyến là cho phép chúng ta truyền thông tin cậy và đảm bảo chất lượng dịch vụ (QoS). Các nhiệm vụ quan trọng liên quan đến việc định tuyến là để có thể lựa chọn con đường đi tốt nhất mà điều đó đảm bảo rằng dữ liệu sẽ đạt được là đáng tin cậy nhất và chính xác nhất từ người gửi đến người nhận. Điều này được thực hiện bằng cách chọn giao thức thích hợp mà tránh ùn tắc và do đó ngăn ngừa mất dữ liệu.

Điều cần quan tâm chính của chủ đề này là việc kiểm tra các yêu cầu cho việc thiết kế và đo đạc trong các mạng nhằm hỗ trợ hiệu năng mạng cao, chẳng hạn như thông lượng cao và độ trễ của gói tin là thấp nhất. Việc sản xuất ra một phép phân tích sâu sắc về các điều kiện tiên quyết cho việc thiết kế số liệu định tuyến trong mạng phải dựa vào sự am hiểu của 2 yếu tố: Các giao thức định tuyến được sử dụng trong mạng WLAN và các đặc điểm của mạng WLAN. Đầu tiên, các giao thức định tuyến khác nhau có thể đưa ra các chi phí khác nhau theo quan điểm

thông điệp và quản lý mức độ phức tạp, cần thiết phải biết được giao thức định tuyến nào là thích hợp cho mạng không dây. Chính bằng cách này, việc thiết kế số liệu định tuyến phải tương thích với hiệu quả của giao thức định tuyến. Tiếp theo là đặc điểm của mạng WLAN, chẳng hạn như tính chất ổn định của các nút mạng và tính chất chia sẻ của thiết bị không dây trung gian, điều này cũng đặt ra những thách thức cho việc thiết kế của số liệu định tuyến.

Các giao thức định tuyến khác nhau yêu cầu việc thiết kế số liệu định tuyến khác nhau. Do đó, điều kiện cần thiết đầu tiên là cần nắm bắt được ý tưởng giao thức định tuyến nào là phù hợp cho mạng WLAN. Hơn thế nữa, chúng ta cần hiểu rằng những thuộc tính cần thiết của thiết kế số liệu định tuyến nhằm hỗ trợ việc nâng cao hiện quả giao thức trong mạng WLAN. Khả năng của giao thức định tuyến cho mạng WLAN có thể được chia thành 2 loại: Định tuyến nguồn và định tuyến cho từng chặng (hop by hop). Tất cả các giao thức định tuyến này có các chi phí khác nhau và độ phức tạp quản lý khác nhau.

Trên lý thuyết, có nhiều giao thức định tuyến được đề xuất trong mạng không dây ad hoc. Vì WLAN là mạng multi-hop nên các giao thức thiết kế cho mạng ad hoc cũng làm việc tốt trên mạng WLAN. Mục tiêu chính của các giao thức này là nhanh chóng thích ứng với sự thay đổi của đường đi chỉ đường khi đường đi bị gián đoạn bởi sự di chuyển của các nút. Các triển khai hiện tại cho mạng WLAN cũng sử dụng các giao thức đang sử dụng cho mạng ad hoc như AODV (Ad hoc On-Demand Distance Vector), DSR (Dynamic Source Routing) và TBRPF (Topology Boardcast based on Reverse Path Fowarding)… Tuy nhiên, trong mạng không dây, các router rất ít di chuyển và không có sự ràng buộc về năng lượng, trong khi đó các client thì là cơ động và giới hạn về năng lượng. Sự khác biệt này cần được xem xét để phát triển các giao thức hiệu quả áp dụng cho mạng không dây. Khi các liên kết trong mạng không dây tồn tại lâu, thì việc tìm ra một con đường tin cậy và có thông lượng cao là vấn đề được quan tâm chính hơn là việc thích ứng nhanh chóng với lỗi đường truyền ở các mạng ad hoc.

3.2.2.3 Chất lượng dịch vụ (QoS)

QoS là viết tắt của Quality of Service (chất lượng dịch vụ). Đây là một cách thức điều khiển mức độ ưu tiên băng thông của hệ thống mạng. Hiểu một cách đơn giản là QoS có nhiệm vụ truyền tín hiệu với thời gian trễ tối thiểu và cung cấp lưu lượng băng thông cho những ứng dụng truyền thông đa phương tiện.

Hơn hết QoS hoạt động trên tất cả các tầng mạng khác nhau của hệ thống mạng. QoS chỉ hoạt động khi hiện tượng nghẽn cổ chai xảy ra tại bất kỳ vị trí nào đó trong hệ thống. Quan trọng hơn hết là những vị trí xảy ra tình trạng này được thiết lập các thông số có liên quan đến băng thông.

Nghĩa là nếu các thiết lập của QoS mà khi thiết lập vượt quá mức băng thông mà nhà cung cấp cho phép, nhưng lưu lượng băng thông trên router lại không được ưu tiên vì hệ thống ứng dụng nghĩ rằng lưu lượng băng thông này hoàn toàn là hợp lý. Tuy nhiên, việc tiếp tục thực hiện hay không lại không phải do chúng ta quyết định mà là do nhà cung cấp ứng dụng quyết định.

Tuy nhiên, nếu tự thiết lập mức băng thông của QoS thấp hơn so với tiêu chuẩn của ISP thì có nghĩa là chúng ta đang tự tạo ra nút cổ chai (Bottleneck) nhân tạo. Nghĩa là các dịch vụ sẽ bị gián đoạn lưu lượng băng thông thấp. Khi lưu lượng băng thông thấp do nút cổ chai tạo nên thì QoS sẽ làm tăng hiệu suất bằng cách giảm độ trễ và giải phóng băng thông.

Như vậy, sẽ giúp làm tăng hiệu suất sử dụng mạng nói chung. Tuy nhiên, cần lưu ý rằng mỗi lưu lượng truy cập khác trong hệ thống mạng sẽ có một cơ chế hoạt động khác nhau. Cơ chế hoạt động này còn phụ thuộc vào lưu lượng đó có nhạy cảm với độ trễ hay nhạy cảm với băng thông. Trên thực tế thì khi hệ thống mạng yêu cầu lưu lượng băng thông tăng lên thì sẽ xảy ra hiện tượng nghẽn mạng. Vì vậy để giải quyết được vấn đề này thì lưu lượng băng thông phải được tăng lên hoặc thay thế những thiết bị phần cứng khác.

Khi gặp phải tình huống này QoS sẽ ưu tiên một số traffic quan trọng hoặc những traffic này sẽ đòi hỏi việc xử lý nhanh về thời gian. Khi đó QoS sẽ mô tả cách chuyển mạch của gói tin được diễn ra như thế nào.

Hình 3.7: Băng thông internet khi không có QoS và cài đặ QoS

Như chúng ta đã biết, hiện nay băng thông được sử dụng khá phổ biến. Chính vì vậy mà khi đề cập đến modem dường như là một điều khá lạ lẫm. Tuy nhiên đối với doanh nghiệp nhỏ hoặc hộ gia đình thì họ vẫn đang sử dụng modem để kết nối internet.

Bên cạnh đó, khi sử dụng modem thì số lượng băng thông sẽ hạn chế nhưng người dùng lại yêu cầu lượng băng thông lớn. Như vậy sẽ khiến việc thực hiện truyền thông tin một cách trực tiếp bị gián đoạn. Từ đó sẽ khiến tốc độ kết nối của máy chủ gặp vấn đề. Đặc biệt, có nhiều sự khác nhau trong tốc độ liên kết có thể làm cho dữ liệu dồn ứ trong hàng đợi đã kết nối với liên kết chậm.

Khi đó, QoS sẽ bắt đầu thực hiện vai trò của nó và điều chỉnh lưu lượng băng thông. Nếu bạn cài QoS trên host có chia sẻ kết nối internet thì host này sẽ ghi đè lên kích thước cửa sổ nhận. Như vậy sẽ làm giảm bớt các vấn đề bị gây ra bởi tốc độ mạng không hợp kiểu.

3.2.2.3 Vấn đề về an ninh trong mạng không dây

Trong bối cảnh toàn cầu hoá, sự bùng nổ nhu cầu truyền số liệu tốc độ cao và nhu cầu đa dạng hoá các loại hình dịch vụ cung cấp như truy nhập Internet, thư điện

tử, thương mại điện tử, truyền file,. đã thúc đẩy sự phát triển của các giải pháp mạng cục bộ vô tuyến (WLAN). Mục đích của WLAN nhằm cung cấp thêm một phương án lựa chọn cho khách hàng bên cạch các giải pháp như xDSL, Ethernet, GPRS, 3G,. WLAN là một phần của giải pháp văn phòng di động, cho phép người sử dụng kết nối mạng LAN từ các khu vực công cộng như khách sạn, sân bay và thậm chí có thể ngay cả trên các phương tiện vận tải. Tuy nhiên, để kết nối được thì các khách hàng di động phải nằm trong vùng phủ sóng của các AP. Để đảm bảo các vùng được phủ sóng hoàn toàn, các ISP sẽ cần phải cài đặt thêm các điểm cung cấp dịch vụ internet không dây (hotspot) tại các địa điểm chiến lược để mở rộng tầm phủ sóng hiện có. Ngoài ra, triển khai các điểm cung cấp dịch vụ internet không dây cũng làm tăng thêm các chi phí lắp đặt và quan trọng hơn là chi phí vận hành. Một số router được trang bị giao diện có dây và phục vụ với mục đích của một cổng vào (gateway) để cung cấp kết nối đến Internet. Các nút người dùng có thể hoạt động như các nút trung gian cho các nút lân cận của chúng để mở rộng thêm khả năng kết nối. Các tấn công với mạng không dây có thể từ bên ngoài cũng như từ bên trong. Những cuộc tấn công từ các nút bên ngoài có thể được ngăn chặn bằng cách dùng đến các kỹ thuật mật mã như mã hóa và xác thực. Mặt khác, các cuộc tấn công bên trong được thực hiện bởi các nút là thành phần của mạng không dây. Mục đích của các kiểu tấn công là nhằm làm suy yếu hiệu năng của mạng và gây thất thoát thông tin, do đó chúng ta cần phải có cơ chế hợp tác cho phép các nút khác trong mạng phát hiện và có thể cô lập các nút lỗi. Vậy chúng ta có thể kết luận rằng tiềm năng thực sự của mạng không dây có thể không được khai thác mà không cần xem xét kỹ càng và quan tâm đúng mức trong các vấn đề an ninh nội bộ cũng như bên ngoài.

Chính vì những lý do trên và để tăng hiệu năng sử dụng mạng nội bộ nói chung và mạng WLAN ứng dụng nói riêng trong khuôn viên của trường Cao đẳng Lý Thái Tổ thì giải pháp quan trọng để bảo vệ hệ thống mạng sử dụng tính năng IDS/IPS, phát hiện và ngăn chặn các truy cập bất hợp pháp và các phương pháp định tuyến của hệ thống để không ảnh hưởng tới thông lượng cũng như hiệu năng của mạng.

Bảng 3.3: Các mục tiêu khác khi hệ thống mạng thay đổi

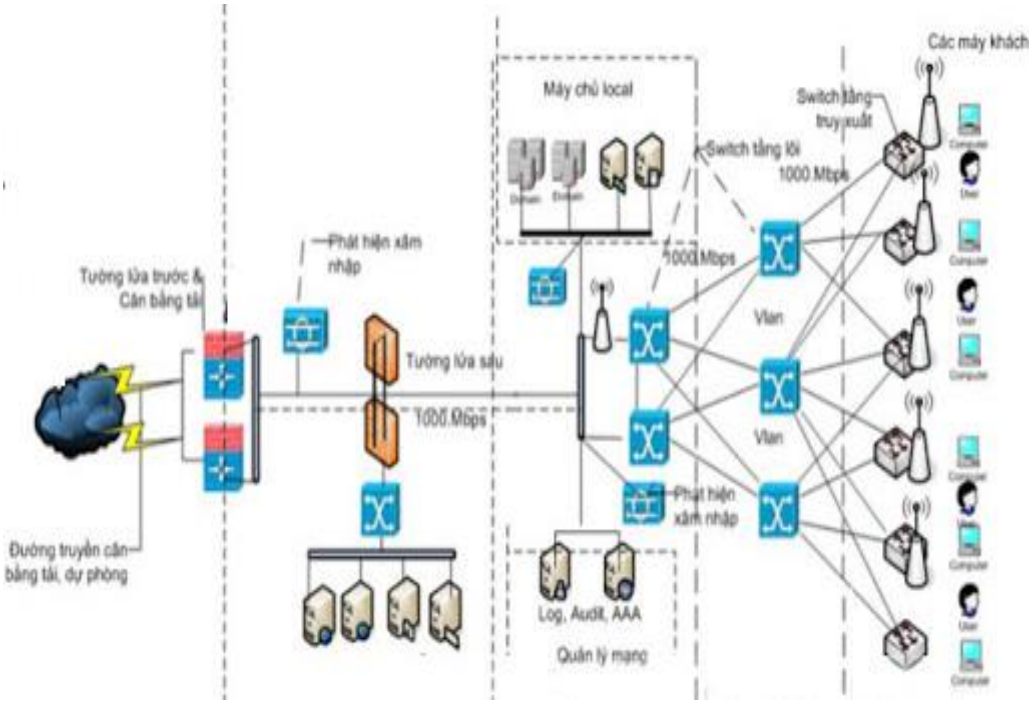
STT	Tính năng	Mô Tả
1	Sẵn sàng	- Thiết bị có chức năng inline fail-open mode, khi có sự cố về thiết bị hay hỏng nguồn điện, thiết bị tự động bypass traffic, không làm gián đoạn traffic
		- Triển khai thiết bị ở chế độ IDS thì sử dụng cổng SPAN trên các thiết bị switch, router để đổ luồng traffic cần giám sát, không ảnh hưởng tới hoạt động mạng
2	Hiệu suất	- Độ trễ khi xử lý, phân tích gói tin <1ms.
		- Throughput của thiết bị tối thiểu 1Gbps.
		- Hệ thống có khả năng lưu trữ tối thiểu 30 triệu events
3	Khả năng phát hiện, ngăn chặn	- IDS/IPS phải có khả năng phát hiện và ngăn chặn các cuộc tấn công, và các truy cập bất hợp pháp tới hệ thống mạng.
		- Thiết bị phải được cấu hình update các lỗ hổng bảo mật, tinh chỉnh các rule tự động, phát hiện và ngăn ngừa các cuộc tấn công mới.
4	Quản lý	- Giải pháp IDS/IPS phải có khả năng quản lý tập trung và phân cấp quyền quản trị nhằm đáp ứng mềm dẻo trong quản trị.
5	Mở rộng	- Giải pháp quản lý tập trung IDS/IPS phải cho phép quản lý phân cấp, có khả năng quản lý nhiều thiết bị IDS/IPS.
		- Mỗi thiết bị IDS/IPS có tối thiểu 8 port 10/100/1000 Mbps. Với việc cấu hình dùng SPAN port, có thể lựa chọn VLAN, dải VLAN cần giám sát tùy từng thời điểm
6	Tính năng IPS bảo vệ các vùng mạng	- Phát hiện các cuộc tấn công từ bên ngoài như Worms, Trojans, Buffer overflows, DoS attacks, Backdoor attacks, Spyware, Port, scans, VoIP attacks, IPv6 attacks, Statistical anomalies, Protocol, anomalies, P2P attacks, Blended threats, Zero-day attacks… vào các server dịch vụ
		- có thể xác lập các qui tắc ngăn chặn các cuộc tấn công hoặc xác lập chế độ tự động tinh chỉnh tùy theo các dịch vụ
		- Đưa ra các báo cáo về các cuộc tấn công, các lỗ hổng bảo mật
7	Tính năng IDS phát hiện các cuộc tấn công cho các VLAN thiết lập giám sát	- phát hiện và đưa ra các báo cáo về các cuộc tấn công, các nguy cơ bảo mật, lỗ hổng an ninh… của các server, dịch vụ của các VLAN giám sát.
		- phát hiện các cuộc tấn công, các nguy cơ bảo mật… từ người dùng
		- Trong trường hợp xảy ra tấn công từ ngoài vào các host trong vùng giám sát thì có thể thiết lập tính năng IPS trên thiết bị để bảo vệ các host ngăn chặn tấn công từ bên ngoài vào các vùng đó
8	Tính năng giám sát cảnh báo tức thời (Real time Network Awarreness - RNA)	- RNA giúp phát hiện các nguy cơ an ninh mạng: Network profile (OS, Services, Open Ports, Vulnerability, Host static). RNA kết hợp với IPS, IDS để tự động active/disable các rules cần thiết để bảo vệ hệ thống mạng.
		- Tính năng Passive Scan cho phép RNA phát hiện nguy cơ an ninh hệ thống mạng mà không ảnh hưởng tới năng lực hệ thống mạng
9	Tính năng giám sát hệ thống (IT Policy complicance)	- Đưa ra những cảnh báo những vi phạm về chính sách bảo mật. Những vi phạm này có thể là: một cuộc tấn công nguy hiểm xảy ra, một sự cố liên quan tới một máy chủ hay một dịch vụ.
		- Cảnh báo có thể thực hiện qua Email, SNMP hay SYSLOG.

3.3 Mô phỏng tăng hiệu năng mạng WLAN tại Cao đẳng Lý Thái Tổ

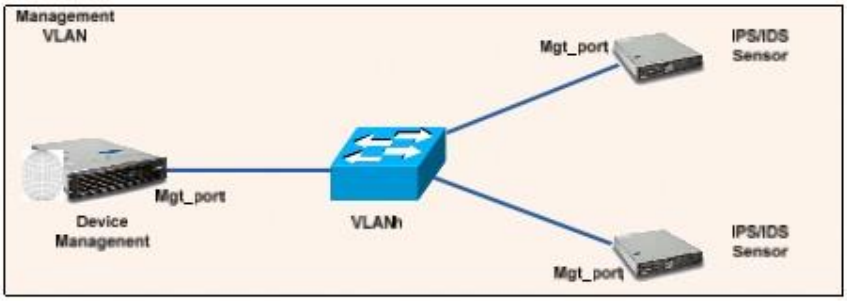
Mô phỏng được thực hiện thông qua công cụ mô phỏng Cisco SDM (Security Device Manager) là công cụ để quản lý thiết bị Router thông qua công nghệ JAVA. SDM sử dụng để cấu hình Router thông qua các interface HTTP hoặc HTTPs giúp chúng ta cấu hình LAN, WAN và các tính năng bảo mật khác của Router (ACLs, VPN,…). SDM được thiết kế cho người quản trị mạng hay reseller SMB mà không yêu cầu người sử dụng có kinh nghiệm nhiều trong việc cấu hình Router. Việc cấu hình Router thông qua SDM giúp cho việc định tuyến và cân bằng tải trong hệ thống mạng nhằm tránh tắc nghẽn đường truyền mạng và duy trì sự ổn định của hệ thống.

3.3.1 Các công cụ cần thiết để thực hiện việc mô phỏng

- Hệ điều hành window 7
- Phần mềm giả lập GNS3
- Tool SDM của cisco
- Máy PC phải cài gói java để hỗ trợ cho SDM

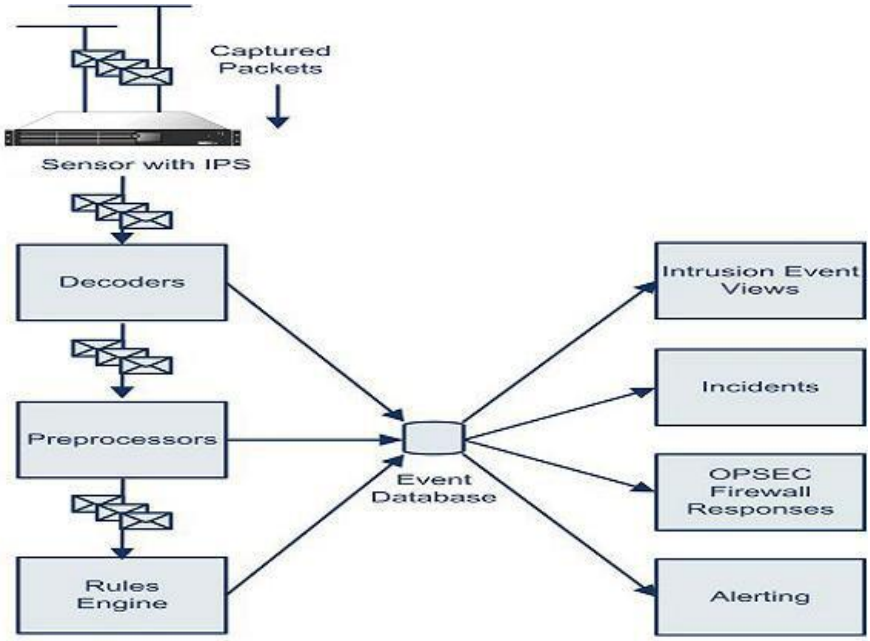


Hình 3.8: Mô hình tổng thể hệ thống mạng của Cao đẳng Lý Thái Tổ



Hình 3.9: Mô hình quản lý tập trung

Thiết lập mạng quản lý cho các thiết bị IDS/IPS: Kết nối các cổng mangement trên các thiết bị IDS/IPS với thiết bị quản lý. Từ đây, thiết bị Quản lý có thể quản lý tất cả các thiết bị IDS/IPS.



Hình 3.10: Mô hình nguyên lý hoạt động

Khi gói tin được nhận được bởi thiết bị, gói tin đó sẽ được:

- Giải mã gói tin bởi thành phần bộ giải mã của thiết bị.
- Sau đó gói tin sẽ được chuyển vào quá trình tiền xử lý.
- Gói tin sẽ được so sánh với tập Rules được sử dụng.
- Quá trình đó sẽ đưa ra được một cơ sở dữ liệu về các sự kiện.
- Các sự kiện đó có thể được lọc ra thành các dạng sự kiện khác nhau.

Mô tả các kết quả đem lại.

- Tính năng IPS: Bảo vệ mạng trước các cuộc tấn công mạng.
- Tính năng IDS/IPS kết hợp với RNA: Phát hiện và phân tích các báo cáo tình trạng bảo mật mạng sử dụng IDS hay IPS.
- Tính năng RNA phát hiện hệ thống mạng: Host active, Open Port, Protocols, Vulnerabilities.

Bảng 3.4: Các kết quả đem lại qua một đợt tấn công

STT	Tình huống bị tấn công	kết quả đem lại
1	**Trước**	Tính năng RNA của thiết bị giúp phát hiện các nguy cơ an ninh mạng: Network profile (OS, Services, Open Ports, Vulnerability, Host static)
		RNA kết hợp với IPS, IDS để tự động active/disable các rules cần thiết để bảo vệ hệ thống mạng
		Tính năng Passive Scan cho phép RNA phát hiện nguy cơ an ninh hệ thống mạng mà không ảnh hưởng tới năng lực hệ thống mạng
2	**Trong**	Phát hiện và ngăn chặn các cuộc tấn công từ bên ngoài như Worms, Trojans, Buffer overflows, DoS attacks, Backdoor attacks, Spyware, Port scans, VoIP attacks, IPv6 attacks, Statistical anomalies, Protocol anomalies, P2P attacks, Blended threats, Zero-day attacks… vào các server dịch vụ.
		Có thể xác lập các qui tắc ngăn chặn các cuộc tấn công hoặc xác lập chế độ tự động tinh chỉnh tùy theo các dịch vụ.
		Đưa ra các báo cáo về các cuộc tấn công, các lỗ hổng bảo mật.
3	**Sau**	Sourcefire với hệ thống báo cáo đầy đủ, thông minh giúp người quản trị phân tích được những ảnh hưởng đối với hệ thống sau khi bị tấn công.
		RNA kết hợp với tính năng Report thiết lập độ ưu tiên cho các Events, tính năng này cho phép giảm thiểu đáng kể thời gian phân tích các Events sau khi hệ thống bị tấn công.
		RNA phân tích lỗ hổng bảo mật đưa ra các khuyến cáo về vá lỗ hổng bảo mật cho hệ thống.
		Tính năng IT Policy Compliance: Đưa ra những cảnh báo những vi phạm về chính sách bảo mật. Những vi phạm này có thể là: một cuộc tấn công nguy hiểm xảy ra, một sự cố liên quan tới một máy chủ hay một dịch vụ. Cảnh báo có thể thực hiện qua Email, SNMP hay SYSLOG.

Những sự cố không mong muốn của giải pháp

Khi triển khai IPS vào một hệ thống mạng đôi khi xảy ra những sự cố không mong muốn như: Dịch vụ mạng bị IPS phát hiện nhầm dẫn đến không thể hoạt động được. Đôi khi cảnh báo sai.

Cách giải quyết xem xét cụ thể rules nào của IPS tác động tới dịch vụ này, phân tích và cấu hình lại.

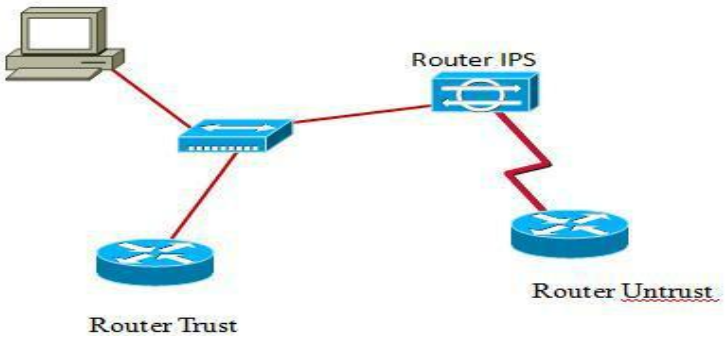
Có điểm yếu tương tự như các bộ quét virus (virus scanner), Thiết bị chỉ có thể chống lại các cuộc tấn công một cách hiệu quả nếu như nó biết được dấu hiệu (signature) của các cuộc tấn công đó. Dựa vào điểm này, các hacker "cao thủ" có thể điều chỉnh các cuộc tấn công để thay đổi signature của cuộc tấn công đó. Từ đó các cuộc tấn công này có thể "qua mặt" được sự giám sát của thiết bị.

Cách giải quyết là liên tục cập nhật bản mới. Nếu không cập nhật liên tục bản mới, IDS/IPS biến thành một doorstop. Điều này có nghĩa là đánh giá sự cam kết dài hạn cho thị trường IDS/IPS của các nhà cung cấp là một phần quan trọng của quyết định lựa chọn nhà cung cấp. Đây cũng là một việc không mong muốn nếu đánh giá nhầm.

3.3.2 Mục tiêu của mô phỏng

Mô phỏng giúp thấy được tính năng, hoạt động cũng như các bước cấu hình IDS/IPS trên router. Thực hiện tính năng gây ra cảnh báo nếu có vi phạm.

3.3.3 Mô hình mô phỏng



Hình 3.11: Mô hình mô phỏng

3.3.4 Các bước mô phỏng

Tại router ips cấu hình địa chỉ ip và quảng bá mạng dùng giao thức rip như sau:

Router ips(config)#int f0/0

Router ips(config -if)#ip add 192.168.12.2 255.255.255.0

Router ips(config -if)#no shut

Router ips(config -if)#exit

Router ips(config)#int s1/0

Router ips(config -if)#ip add 192.168.23.2 255.255.255.0 Router ips(config -if)#no shut

Router ips(config -if)#clock rate 64000

Router ips(config -if)#exit

Router ips(config)#router rip

Router ips(config -router)#net 172.16.12.0

Router ips(config -router)#net 172.16.23.0

Tại router trusted và untrusted có cấu hình ip và default route như sau:

Trusted router(config)#int f0/0

Trusted router(config-if)#ip add 192.168.12.1 255.255.255.0

Trusted router(config-if)#no shut

Trusted router(configif)#exit

Trusted router(config)#ip router 0.0.0.0 0.0.0.0 192.168.12.2 Untrusted router(config)#int s0/0

Untrusted router(config-if)#ip add 192.168.23.1 255.255.255.0

Untrusted router(config-if)#no shut

Untrusted router(config-if)#clock rate 64000

Untrusted router(configif)#exit

Untrusted router(config)#ip route 0.0.0.0 0.0.0.0 192.168.23.2 Cho phép chạy SDM trên router ips

Router ips(config)#ip http server

Router ips(config)#ip http secure-server

Router ips(config)#ip http authentication local

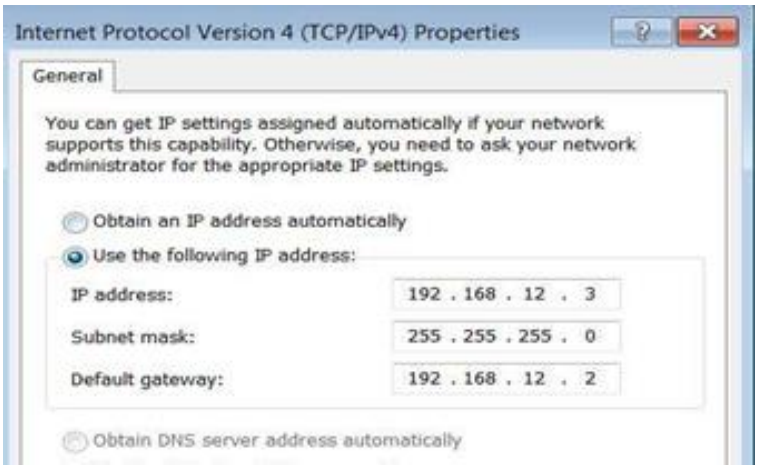
Router ips(config)#username cisco privilege 15 password 0 cisco Router ips(config)#line vty 0 4

Router ips(config-line)#privilege level 15

Router ips(config -line)#login local

Router ips(config -line)#transport input telnet Router ips(config -line)#transport input telnet ssh

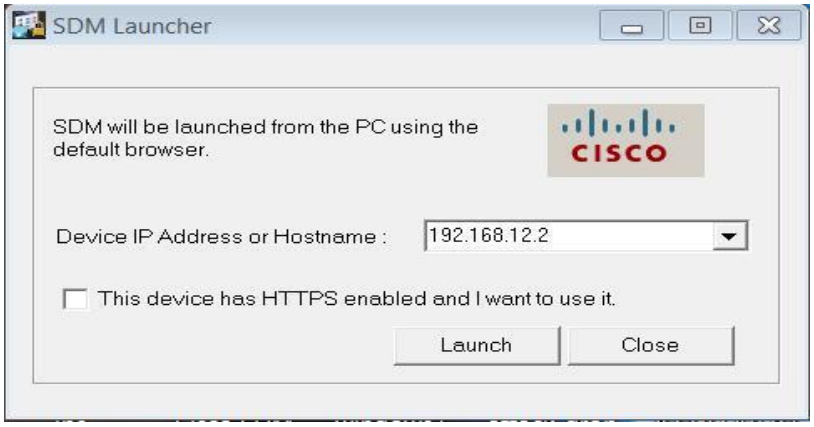
Tại pc chỉnh ip và default gateway về router ips(hình 3.12)



Hình 3.12: Cài đặt IP và default gateway

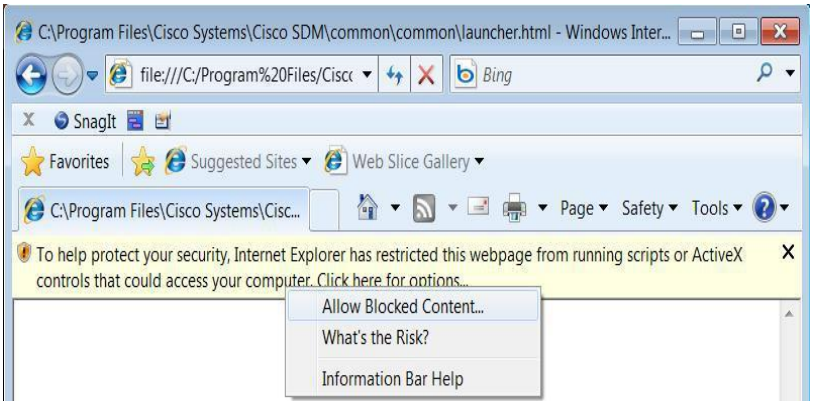
Trên pc cài đặt gói java và tool SDM cho computer và chạy ciscoSDM

Tại màn hình SDM Launcher chọn ip của router ips: 192.168.12.2



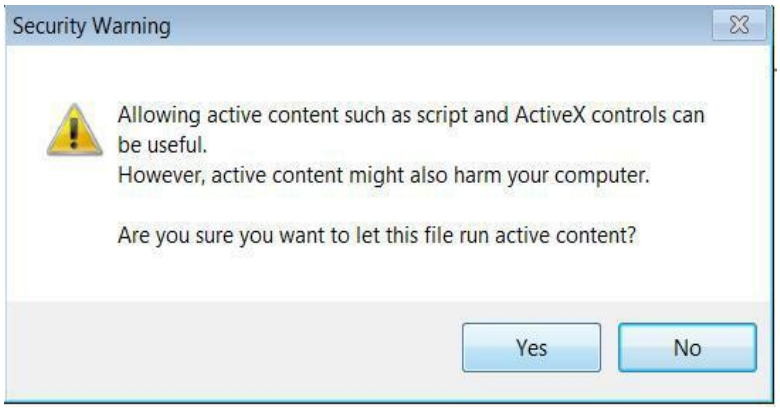
Hình 3.13: IP của router chạy SDM

Màn hình internet explorer xuất hiện sau khi bấm Launch ở bước trên, kích phải chuột chọn allow blocked content



Hình 3.14: Cho phép chạy pop up

Xuất hiện cảnh báo chọn yes

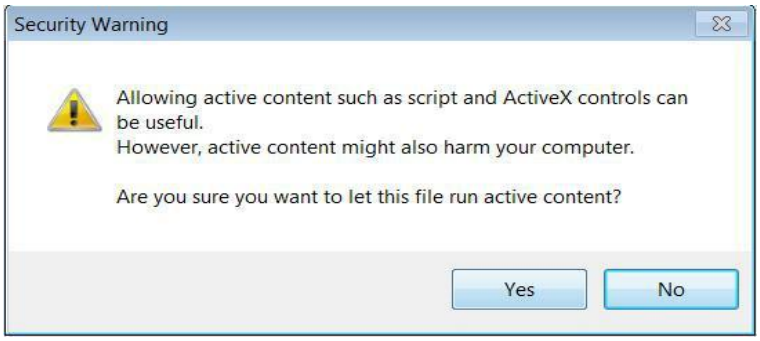


Hình 3.15: Cảnh báo

Màn hình đăng nhập chứng thực xuất hiện, đăng nhập với tài khoản và mật khẩu có level 15

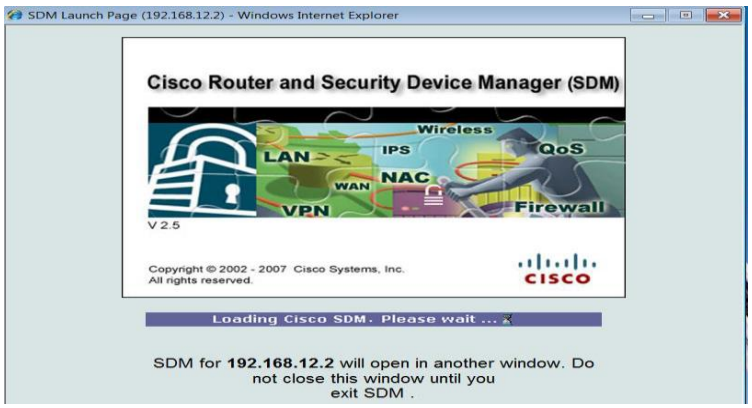
Hình 3.16: Chứng thực tài khoản và mật khẩu

Xuất hiện cửa sổ internet explorer, chọn allow blocked content



Hình 3.17: Cảnh báo

Sau khi nhấn yes xuất hiện trang load SDM từ router tới máy tính

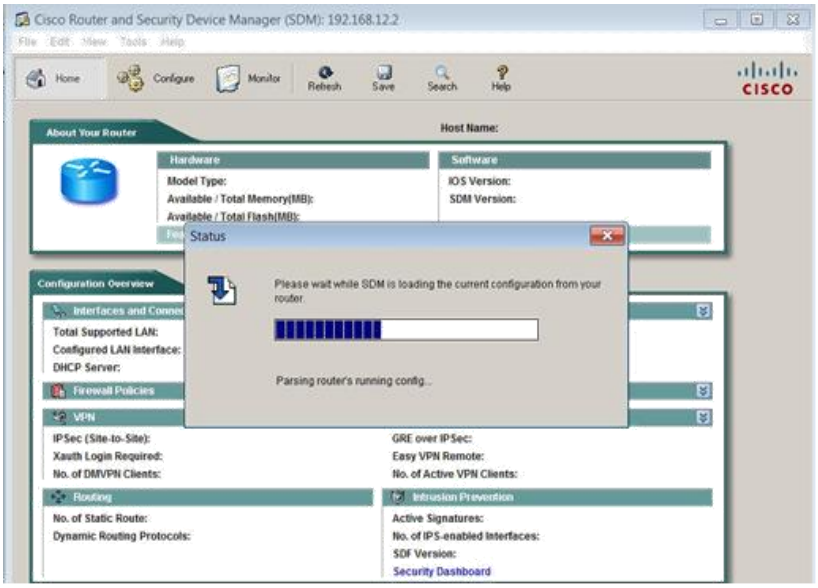


Hình 3.18: Quá trình nạp SDM

Xuất hiện màn hình đăng nhập, tiếp tục đăng nhập với tài khoản và mật khẩu level 15

Hình 3.19: Yêu cầu chứng thực tài khoản và mật khẩu

Màn hình load SDM tới máy tính bắt đầu và yêu cầu đổi username và password cho lần đầu tiên sau đó đăng nhập lại với user mới

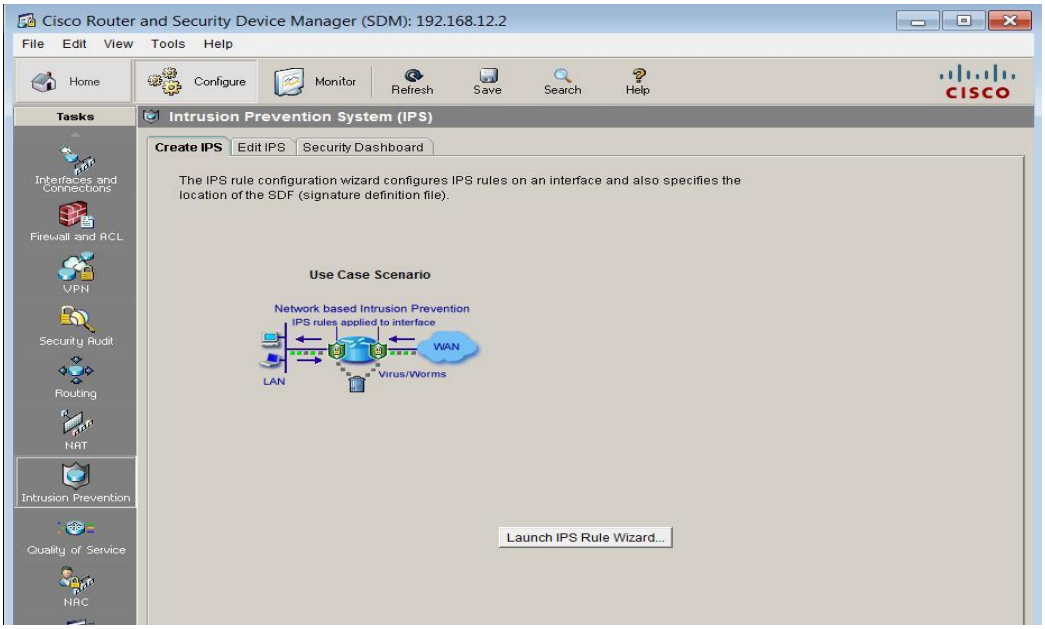


Hình 3.20: Quá trình nạp cấu hình từ router lên sdm

Giao diện đầu tiên khi vào chế độ cấu hình cho router thông qua giao diện, chọn configure để cấu hình cho router ips.

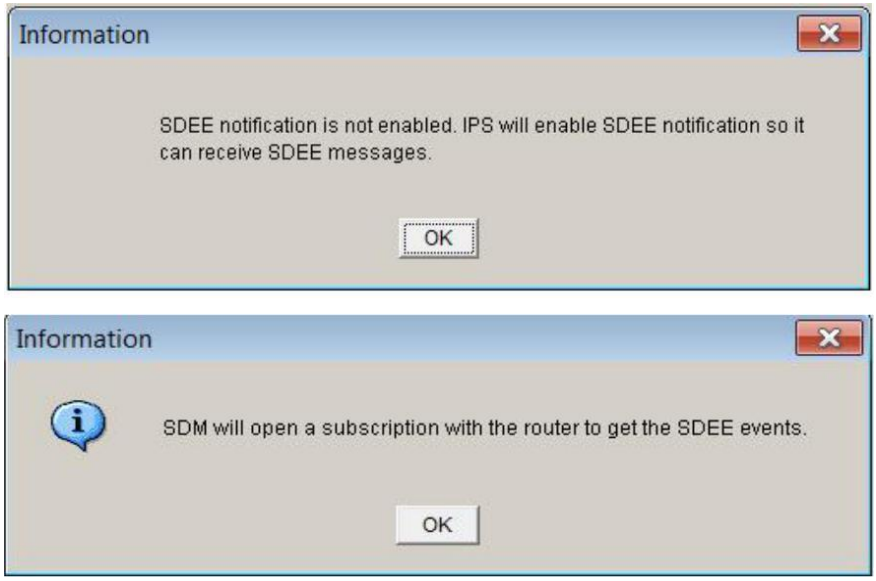
Hình 3.21: Hiển thị các tính năng có trên router

Kích chọn tính năng instruction prevention để cấu hình cho IPS, kích chọn "launch ips rule winzard" để bắt đầu tạo một luật ips mới.



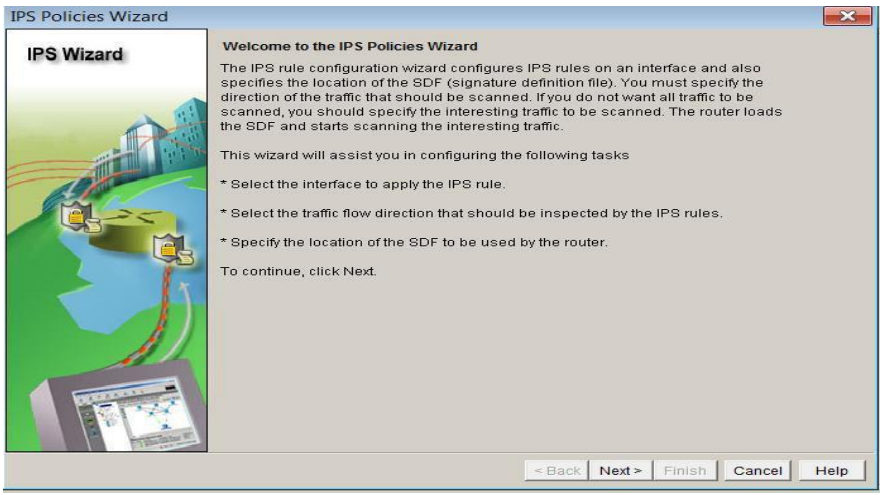
Hình 3.22: Tính năng IPS trên router

Cisco SDM yêu cầu thông báo sự kiện IPS qua SDEE để cấu hình tính năng Cisco IOS IPS, theo mặc định, thông báo SDEE không được kích hoạt. Cisco SDM sẽ nhắc nhở người dùng để cho phép thông báo sự kiện IPS qua SDEE chọn ok.



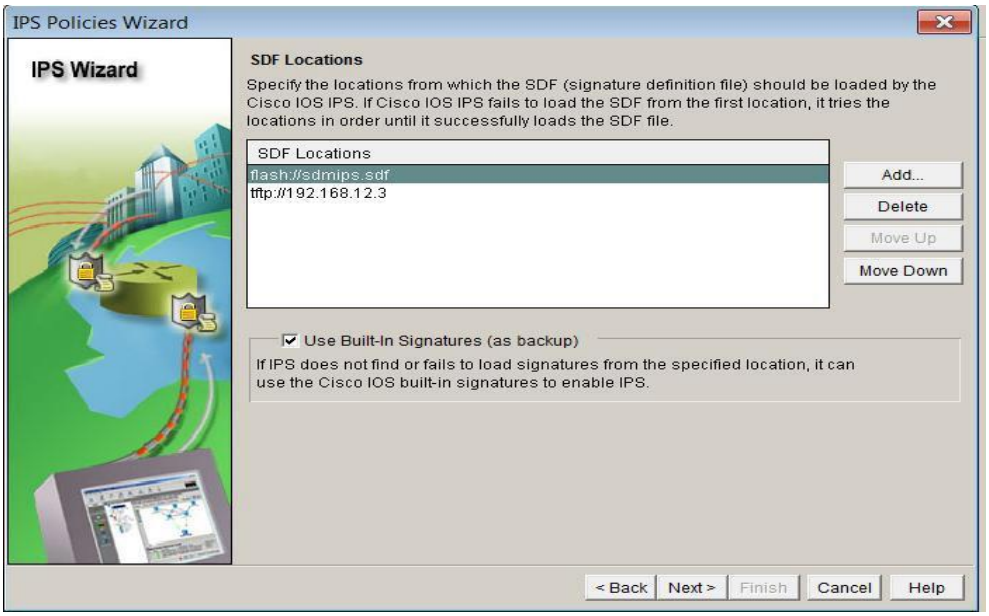
Hình 3.23: Thông báo khi chạy ips

Nhấp vào "Next" trên dưới cùng của giao diện dẫn đến trang tiếp theo trong Wizard IPS. Chọn giao diện trong danh sách và đánh dấu vào ô trống cho cả hai hướng trong hay ngoài đối với các giao diện mà muốn kích hoạt tính năng IPS. Cisco đề nghị cho phép hướng cả trong và ngoài khi kích hoạt IPS trên giao diện. Click "Next" khi đã kết thúc việc chọn lựa.



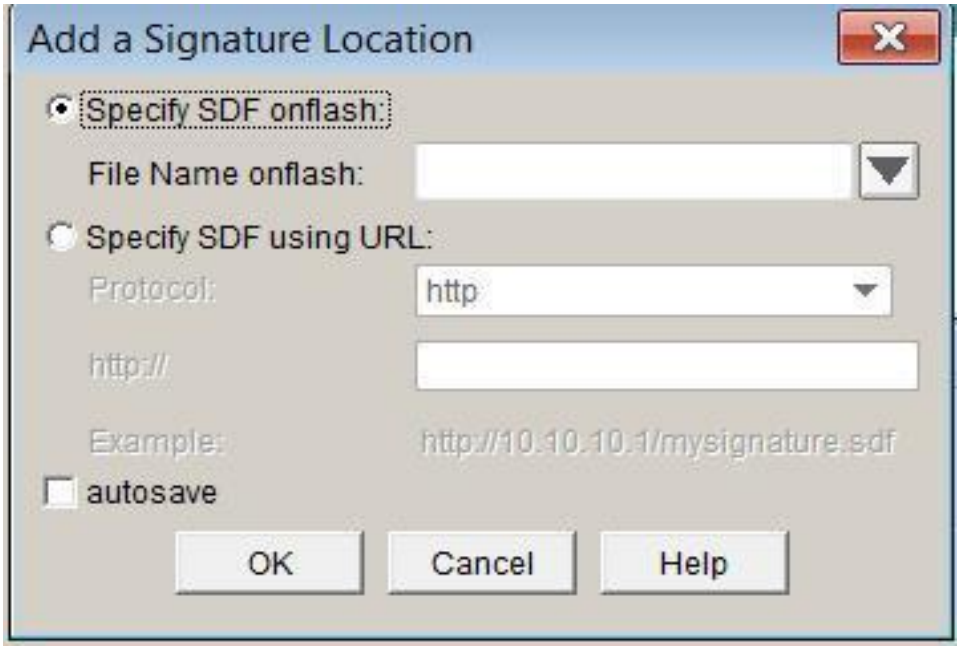
Hình 3.24: Hướng dẫn các bước cấu hình

Màn hình tiếp theo cho thấy vị trí SDF của Wizard IPS. Để cấu hình địa điểm SDF, hãy nhấp vào "Add." nút bên phải của danh sách.



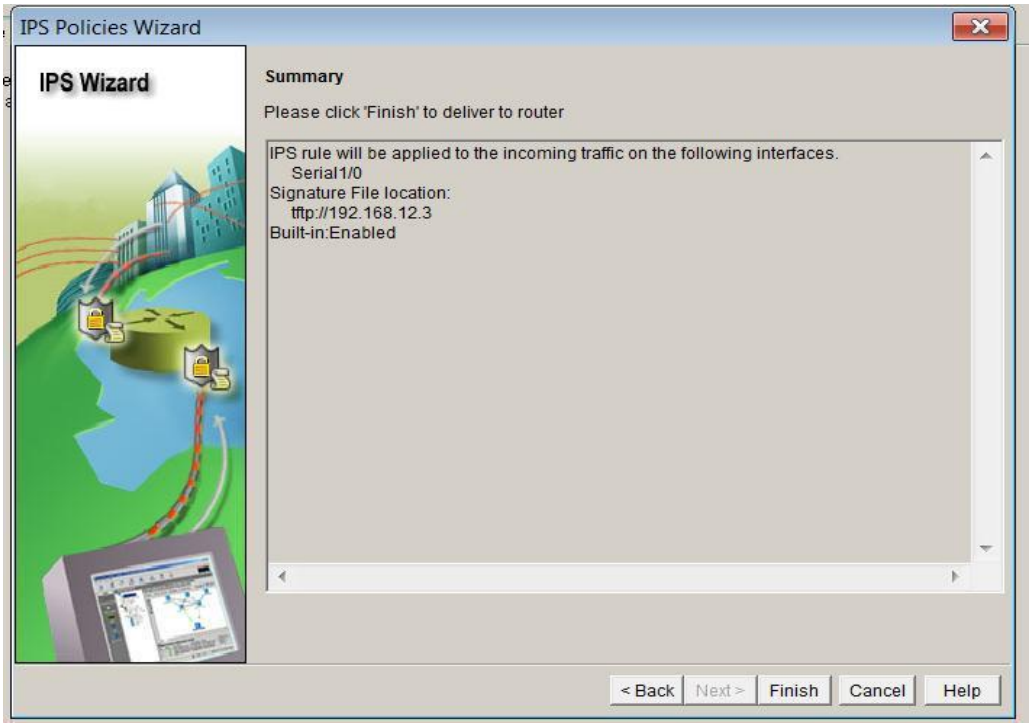
Hình 3.25: Mô tả cách nạp signature

Cửa sổ “Add a signature location” xuất hiện chọn secify sdf using url và chọn tftp (để thực hiện được quá trình copy File.sdf này ở pc chạy tftp),hoặc có thể qua bước này để chọn add file.SDF từ pc.



Hình 3.26: Chọn vị trí signature

Kế đến màn hình tổng kết các quá trình cấu hình rule và nạp signature, chọn finish để kết thúc các bước trên.



Hình 3.27: Kết thúc các quá trình cấu hình

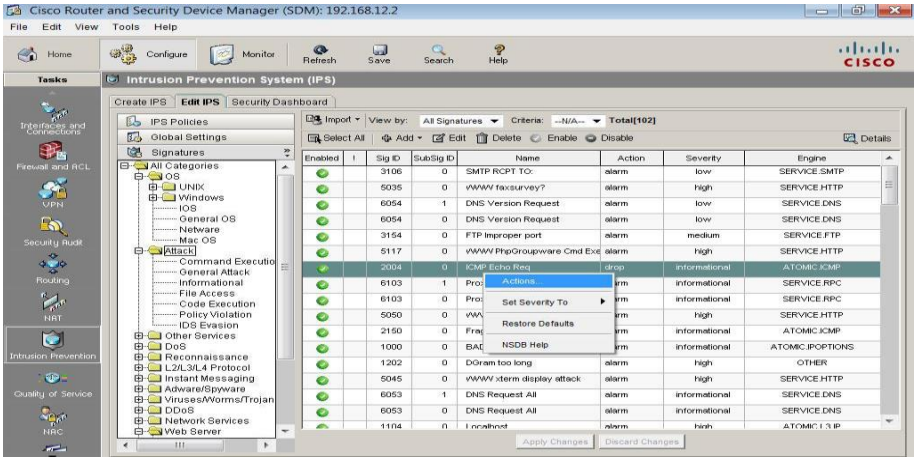
Để kiểm tra cấu hình các signature được nạp trên router vào giao diện như hình SDM UI Path: Configure-> Intrusion Prevention -> Edit IPS -> Signatures

Từ giao diện này có thể định nghĩa thêm signature sau khi kích hoạt default SDF. Có thể định nghĩa thêm các signature bằng cách chức năng import. Để nhập chữ ký mới, chọn default SDFs, hoặc các IOS-Sxxx.zip cập nhật tập tin để nhập chữ ký bổ sung

SDM UI Path: Configure->Intrusion Prevention -> Edit IPS -> Signatures ->Import

Chọn nút nhấn “import” trong thanh công cụ trên cùng của bảng danh sách chữ ký. Kế tiếp chọn “from pc” để chỉ đường dẫn tới file chưa ký.

Tại màn hình này cũng có thể chỉnh lại hoạt động của chữ ký bằng cách kích chọn vào chữ ký-> action và chọn lựa hành động muốn ở đây chọn alarm.



Hình 3.28: Hiển thị các signature được nạp và cấu hình signature

Lưu ý: trong quá trình nạp signature thêm vào CPU sẽ hoạt động cao và trong lúc nạp không nên làm các hành động khác sẽ làm cho quá trình nạp signature chậm lại. Sau khi chữ ký được nạp có một vài trường hợp không được enable nếu muốn có thể enable cho phù hợp với nhu cầu cần thiết của hệ thống.

3.3.5 Mô phỏng các giao thức định tuyến DSR nâng cao hiệu năng mạng WLAN

Để đánh giá các thông số kịch bản mô phỏng hiện trạng và định tuyến DRS với các tính toán từ dữ liệu đầu vào của mô phỏng, hoặc có thể là biến đầu vào. Nó không phụ thuộc vào giao thức định tuyến hoặc quá trình mô phỏng.

3.3.5.1 Thông số di chuyển

Đánh giá sự chuyển động trong mạng bằng cách tính toán di chuyển của nút mạng liên quan giữa các cặp nút mạng trên mạng. Thông số này tương ứng với số thay đổi liên kết trong mô hình khi mà nút mạng di chuyển theo mô hình định trước.

Chuyển động bao gồm cả vận tốc và hướng di chuyển, nó được tính với cùng tốc độ mẫu.

3.3.5.2 Thời gian tạm dừng

Mỗi node bắt đầu di chuyển từ một vị trí ngẫu nhiên tới một vị trí đích ngẫu nhiên với tốc độ được lựa chọn ngẫu nhiên trong khoảng 0 đến 20m/s. Khi đến được

đích thì một đích ngẫu nhiên khác sẽ là mục tiêu tiếp theo sau một khoảng thời gian. Thời gian tạm dừng của tất cả các nút trong mô phỏng được sử dụng để đánh giá, đo kiểm tương tự như thông số chuyển động. Khi giá trị trung bình càng lớn thì nút mạng càng ít di chuyển trong mạng. Trong luận văn này sử dụng 4 giá trị pause time khác nhau là: 0, 30, 60, 120s.

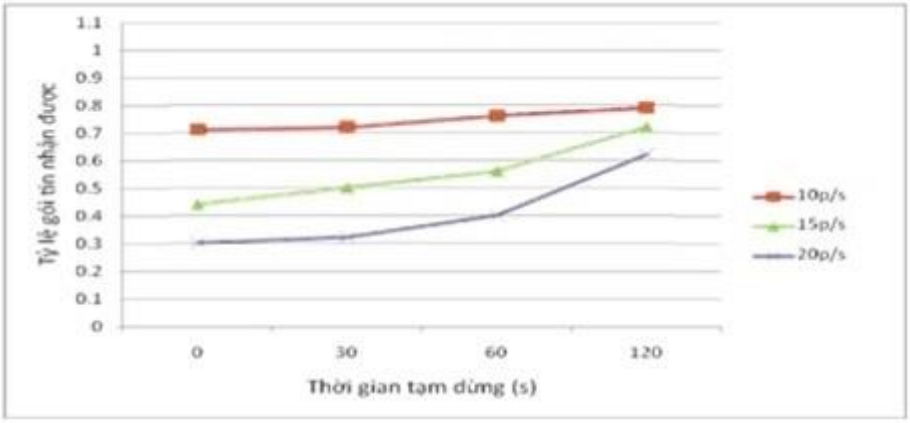
3.3.6 Kết quả thu được từ quá trình mô phỏng

Khi đánh giá ảnh hưởng của tải trong mạng, ta có thể thay đổi kích thước gói hoặc số luồng CBR, tuy nhiên thay đổi tốc độ phản ánh chính xác hơn, ta sử dụng 3 tình huống sau: 10 gói tin/giây; 15 gói tin/giây và 20 gói tin/giây

Với các thông số khác được thiết lập như bảng dưới đây:

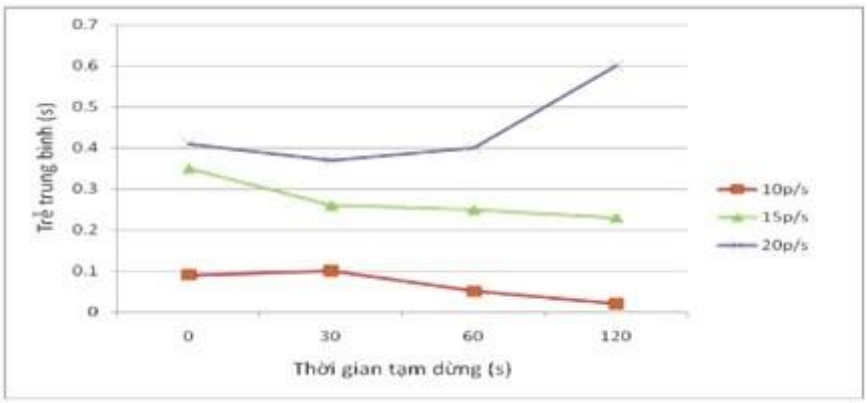
Thông số	Giá trị
Phạm vi truyền dẫn	250m
Băng thông	2Mbps
Thời gian mô phỏng	120s
Kích cỡ môi trường mô phỏng	670×670m
Loại lưu lượng	CBR
Kích thước gói tin	512 bytes
Số kết nối	20
4 giá trị của thời gian tạm dừng	0, 30, 60, 120s

3.3.6.1 Kết quả mô phỏng hiện trạng hiệu năng với hệ thống mạng Wifi trường Cao đẳng Lý Thái Tổ



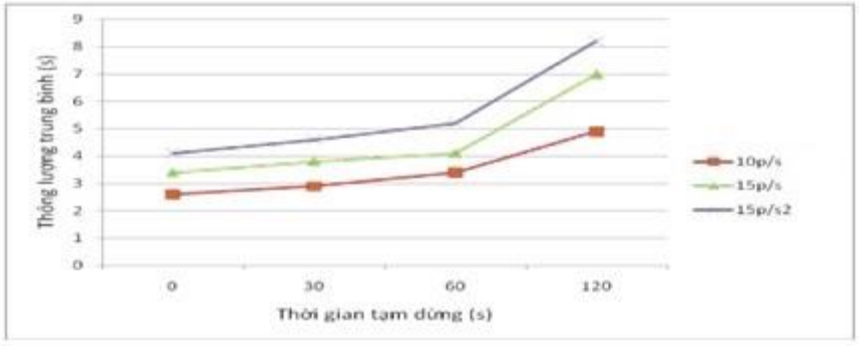
Hình 3.29: Mô phỏng hiện trạng tỷ lệ gói tin nhận được

Khi không sử dụng giao thức định tuyến với tốc độ gửi gói tin là 10 gói tin/s thì tỷ lệ gói tin nhận được giảm nhanh hơn khi thông số di chuyển cao. Tại tốc độ 15 gói tin/s, 20 gói tin/s thì gói tin hủy bỏ nhiều hơn, khi thời gian tạm dừng là 0 thì chỉ có khoảng 30-40% gói tin được nhận.



Hình 3.30: Mô phỏng hiện trạng trễ trung bình đầu cuối

Giá trị trễ bị ảnh hưởng khi tốc độ gói CBR cao. Bộ đệm bị đầy nhanh chóng nên gói tin ở trong bộ đệm lâu hơn, ta có thể quan sát khi tốc độ 20 gói tin/giây. điểm khác biệt dễ thấy khi tốc độ là 10 gói tin/giây. Giá trị trễ cao khi thông số di chuyển cao hay thời gian tạm dừng bằng 0 và tốc độ gói tin là 20 gói tin/giây, do bộ đệm bị đầy nhanh chóng và thậm chí đường định tuyến tồn tại dài hơn.

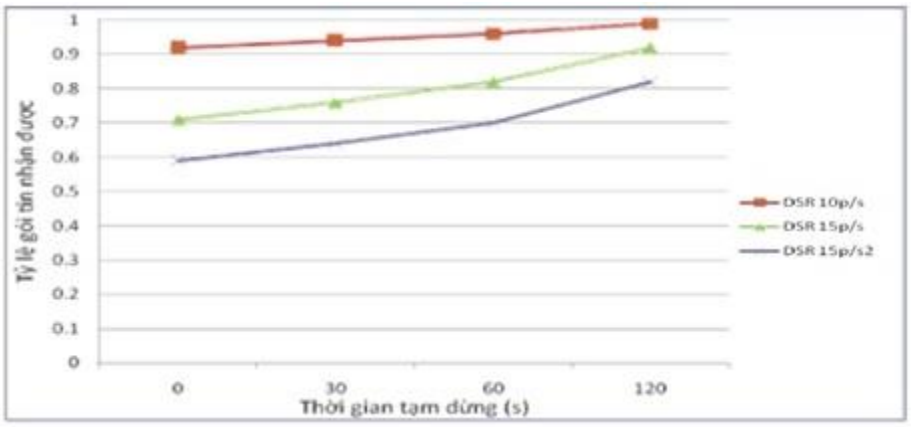


Hình 3.31: Mô phỏng hiện trạng thông lượng từ đầu cuối

Ở tốc độ CBR thấp, thông lượng bị ảnh hưởng nhiều bởi thông số di chuyển, giá trị vào khoảng 1.5 kbps. Với tốc độ CBR cao hơn, thông lượng giảm khi thông số di chuyển tăng, thể hiện khi tốc độ CBR=10 gói tin/giây. Đây cũng là kết quả của

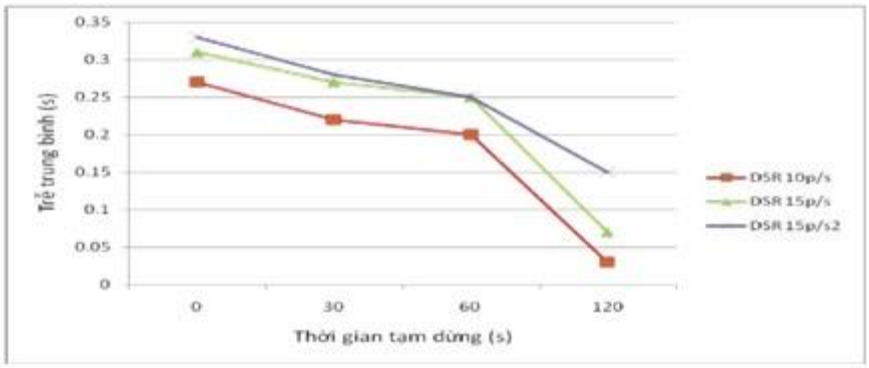
số lượng gói tin bị rơi nhiều, thậm chí với CBR=15, 20 gói tin/giây, thì bên nhận gần như không nhận được gói tin.

3.3.6.2 Kết quả mô phỏng sử dụng phương pháp định tuyến DSR nâng cao hiệu năng



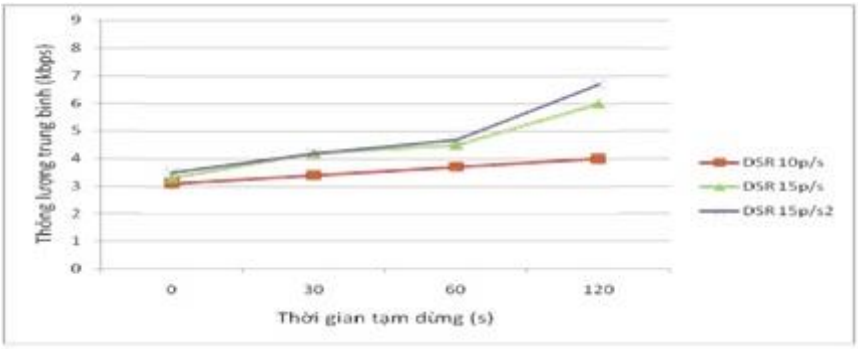
Hình 3.32: Mô phỏng định tuyến DSR tỷ lệ gói tin nhận được

Khi tốc độ gửi gói tin là 10 gói tin/s thì tỷ lệ gói tin nhận được khá cao, với thời gian tạm dừng bằng 120s tỷ lệ nhận gói tin nhận được xấp xỉ 100%. Tại tốc độ 15 gói tin/s, 20 gói tin/s thì hủy bỏ nhiều gói tin hơn, khi thời gian tạm dừng là 0 thì chỉ có khoảng 60-70% gói tin được nhận.



Hình 3.33: Mô phỏng định tuyến DSR trễ trung bình đầu cuối

Giá trị trễ cao khi thông số di chuyển cao hay thời gian tạm dừng bằng 0 và tốc độ gói tin là 20 gói tin/giây, do bộ đệm dần đầy lên và đường định tuyến tồn tại dài hơn. Với thời gian tạm dừng truyền càng cao thì độ trễ càng giảm.



Hình 3.34: Mô phỏng định tuyến DSR thông lượng từ đầu cuối

Ở tốc độ CBR thấp, thông lượng của DSR không bị ảnh hưởng nhiều bởi thông số di chuyển, giá trị vào khoảng 2,5 kbps. Với tốc độ CBR cao hơn, thông lượng giảm khi thông số di chuyển tăng, thể hiện khi tốc độ CBR=10 gói tin/giây, tuy nhiên nó giảm nhẹ, chỉ khi tốc độ đạt 15 gói tin/giây và 20 gói tin/giây. Đây cũng là kết quả của số lượng gói tin bị rơi nhiều.

3.3.6.3 So sánh đánh giá

Bảng 3.5: Bảng tổng hợp đánh giá các kết quả mô phỏng

Kết quả mổ phỏng	Tốc Độ (gói tin/giây)	Thời gian tạm dừng							
		0s		30s		60s		120s	
		Hiện trạng	Định tuyến DSR	Hiện trạng	Định tuyến DSR	Hiện trạng	Định tuyến DSR	Hiện trạng	Định tuyến DSR
Tỷ lệ gói tin nhận được	10	70%	90%	70%	93%	78%	97%	80%	100%
	15	43%	70%	50%	75%	55%	81%	70%	90%
	20	30%	60%	32%	65%	40%	70%	60%	80%
Trễ trung bình đầu cuối	10	0.1s	0.27s	0.1s	0.22s	0.05s	0.2s	0s	0.03s
	15	0.35s	0.3s	0.25s	0.27s	0.25s	0.25s	0.22s	0.07s
	20	0.4s	0.32s	0.37s	0.27s	0.7s	0.25s	0.6s	0.2s
Thông lượng từ đầu cuối	10	0.27s	0.3s	0.3s	0.32s	0.32s	0.37s	0.5s	0.4s
	15	0.35s	0.32s	0.37s	0.4s	0.4s	0.45s	0.7s	0.6s
	20	0.4s	0.32s	0.45s	0.4s	0.5s	0.47s	0.82s	0.65s

Từ kết quả của quá trình mô phỏng nhận thấy:

Tỷ lệ gói tin nhận được: Khi sử dụng giao thức định tuyến DSR cao hơn rất nhiều so với hiện trạng hiệu năng hệ thống mạng Wifi trường Cao đẳng Lý Thái Tổ. Khi thời gian tạm dừng bằng 0 thì giao thức định tuyến DSR thì tỷ lệ nhận được gói

tin nhận được vào khoảng 60-70% so với 30-40%. Thời gian tạm dừng bằng 120s thì DSR nhận được gần như toàn bộ các gói tin gửi đến.

Trễ trung bình đầu cuối: Với DSR khi truyền các gói tin với các tốc độ 10 gói tin/giây, 15 gói tin/giây và 20 gói tin/giây độ trễ không trênh lệch nhiều, thời gian tạm dừng càng lớn độ trễ càng giảm. Còn với hiện trạng độ trễ chỉ tốt nhất với tốc độ 10 gói tin/giây, tốc độ 15 gói tin/giây và 20 gói tin/giây độ trễ càng lớn.

Thông lượng từ đầu cuối: Giao thức định tuyến DSR ở tốc độ 15 gói tin/giây, 20 gói tin/giây tỷ lệ gói tin bị rớt nhiều. Nhưng so với hiện trạng không sử dụng giao thức định tuyến ở cùng tốc độ thì bên nhận gần như không nhận được gói tin.

Như vậy, với giao thức định tuyến DSR đã giải quyết được bài toán tăng hiệu năng cho hệ thống mạng WIFI cho trường Cao đẳng Lý Thái Tổ. Hiệu năng hệ thống mạng được cải thiện tốt hơn so với hiện trạng ban đầu.

3.4 Kết luận Chương 3

Chương 3 đã trình bày tóm lược mô phỏng công cụ phân tích kết quả Tracegraph. Từ đó tác giả thực hiện chương trình mô phỏng đánh giá hiệu năng hiện trạng hệ thống mạng và khi sử dụng giao thức định tuyến DSR. Mô phỏng đều thực hiện trên một đồ hình mạng giống nhau với các kịch bản được xây dựng. Giao thức DSR thực hiện chuyển tiếp các gói dữ liệu tương đối tốt khi tỷ lệ chuyển động và tốc độ di của node là thấp. Tuy nhiên khi chuyển động của các node tăng lên thì tỷ lệ gói rớt bắt đầu tăng. Hiệu suất của giao thức DSR rất tốt khi toàn bộ node dịch chuyển, mặc dù giao thức này yêu cầu số byte mào đầu định tuyến tăng. Cuối cùng hiệu suất của giao thức DSR khi tốc độ các node di chuyển và nó giảm được số byte mào đầu định tuyến. Tuy nhiên nó vẫn yêu cầu truyền dẫn nhiều gói mào đầu định tuyến và ở tốc độ di chuyển của các node cao nó thực sự tốn hơn so với giao thức DSR.

Hệ thống phát hiện và ngăn chặn xâm nhập rất hiệu quả trong lĩnh vực bảo mật cũng như tăng hiệu năng sử dụng cho hệ thống mạng của các doanh nghiệp, tổ chức, công ty có nhu cầu bảo mật cao. Thông qua việc mô phỏng có thể thấy được cách cài đặt và sử dụng tính năng IPS trên router hệ thống sẽ gây ra cảnh báo hay ngắt kết nối nếu vi phạm chữ ký được định nghĩa chữ ký trên ips router.

KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN CỦA ĐỀ TÀI

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 WLAN hiện đang được ứng dụng ngày càng mạnh mẽ trong đời sống. Nhưng đa số mọi người đều chỉ sử dụng WLAN ở các lĩnh vực liên quan đến máy tính mà không biết rằng bằng sóng WLAN, người dùng máy tính để điều khiển hệ thống đèn, quạt, máy lạnh, lò sưởi, máy tưới, hệ thống nước (internet of thing)… 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 cố gắng tổng hợp tất cả những cơ chế bảo mật và tất cả 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 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.

Trong điều kiện cho phép, công việc nghiên cứu sẽ được tiếp tục như sau:

- Tìm hiểu sâu hơn kỹ thuật bảo mật hiện nay đang được sử dụng phổ biến.
- Nghiên cứu các lỗ hổng và các cách tấn công mạng WLAN để tìm ra phương pháp bảo mật hiệu quả cho mỗi ngành giúp cho việc quản trị và trao đổi tài nguyên giữa các trạm làm việc trong mạng WLAN.
- Áp dụng giải pháp IPS/IDS vào mạng, từ đó đưa ra những mặt mạnh và những mặt còn hạn chế.

Em xin chân thành cám ơn TS Lê Ngọc Thúy đã tận tình hướng dẫn, giúp đỡ em trong thời gian thực hiện đề tài này và trong quá trình thực hiện thì luận văn vẫn còn có nhiều thiếu sót, mong thầy cô góp ý để em có thể hoàn thiện tốt hơn.

TÀI LIỆU THAM KHẢO

[1]. Hãng HP, Tài liệu giảng dạy nội bộ "Xây dựng hệ thống mạng không dây".

[2]. Nguyễn Khánh Trình "Tìm hiểu về mạng không dây và phát triển dịch vụ trên mạng không dây" – Luận văn thạc sỹ đại học Bách Khoa Hà Nội.

[3]. Phan Thành Vinh "Nguyên cứu giải pháp bảo mật mạng không dây" – Luận văn thạc sỹ Học viện Kỹ thuật Quân Sự.

[4]. Dr. Eric Cole, Dr. Ronald Krutz, and James W. Conley, Network Security Bible, Copyright © 2005 by Wiley Publishing, Inc., Indianapolis, Indiana.

[5]. MIR MOHAMMAD SEYED DANESH, A Surveyon Wireless Security protocols - Faculty of Management – Multimedia University of Malaya.

[6]. Nicolas Sklavos and Xinmiao Zhang 3/2007, Wireless Securiry and Cryptography – Specifications and Implementations.

[7]. Sybex CWNA Certified Wireless Network Administrator Study Guide Exam PW0-100 Sep 2006.

Danh mục các Website tham khảo:

[8]. https: //antoanthongtin.vn

[9]. https: //www.ddth.com

[10]. https: //quantrimang.com/

[11]. https: //vnpro.vn/