BỘ GIÁO DỤC VÀ ĐÀO TẠO
ĐẠI HỌC ĐÀ NẴNG

NGUYỄN VĂN PHÚ

NGHIÊN CỨU VẤN ĐỀ AN NINH MẠNG MÁY TÍNH KHÔNG DÂY

Chuyên ngành: Khoa học máy tính
Mã số: 60.48.01

TÓM TẮT LUẬN VĂN THẠC SĨ KHOA HỌC

Đà Nẵng - Năm 2013

Công trình được hoàn thành tại
ĐẠI HỌC ĐÀ NẴNG

Người hướng dẫn khoa học: **PGS.TS. Lê Văn Sơn**

Phản biện 1: PGS. TSKH. Trần Quốc Chiến

Phản biện 2: PGS. TS. Lê Mạnh Thạnh

Luận văn đã được bảo vệ tại Hội đồng chấm Luận văn tốt nghiệp Thạc sĩ khoa học tại Đại học Đà Nẵng vào ngày 16 tháng 11 năm 2013

Có thể tìm hiểu luận văn tại:

- Trung tâm Thông tin-Học liệu, Đại học Đà Nẵng
- Trung tâm Học liệu, Đại học Đà Nẵng

MỞ ĐẦU

1. Tính cấp thiết của đề tài

Trong những năm gần đây, sự ra đời và phát triển mạnh mẽ của công nghệ không dây giúp cho người dùng linh động hơn trong việc liên lạc trao đổi thông tin. Mạng cục bộ không dây - WLAN, là hệ thống mạng máy tính cho phép người dùng kết nối với hệ thống mạng dây truyền thống thông qua một kết nối không dây.

Tuy nhiên, mạng không dây sử dụng kênh truyền sóng điện từ. Do đó, nó đặt ra nhiều thách thức trong việc xây dựng đặc tả và triển khai trong thực tế. Bên cạnh đó, các hệ thống mạng máy tính không dây thường được triển khai theo mô hình hệ thống mở không cài đặt cơ chế kiểm soát truy cập, cũng như bảo mật cho Access Point để giúp người dùng dễ dàng truy cập internet, mặc dù thiết bị đó có hỗ trợ các giao thức bảo vệ thông tin theo WEP, WPA hoặc cao hơn. Hiện tại có một số công ty cung cấp giải pháp triển khai an ninh nhưng hầu hết các giải pháp này tập trung chủ yếu vào việc kiểm soát truy cập internet, chưa quan tâm nhiều hoặc không quan tâm đến vấn đề bảo mật thông tin của người dùng.

Các vấn đề này đã và đang được rất nhiều viện nghiên cứu, các cơ quan, công ty về bảo mật cũng như những nhà sản xuất thiết bị không dây quan tâm. Đây là một hướng nghiên cứu mở cho những những người muốn nghiên cứu vấn đề an toàn trong hệ thống mạng không dây, đặc biệt là mạng máy tính không dây. Chính những lý đó nên tôi quyết định chọn đề tài: "*Nghiên cứu vấn đề an ninh mạng máy tính không dây*".

2. Mục tiêu nghiên cứu

Nghiên cứu tổng quan mạng máy tính không dây, các chuẩn của mạng không dây, các loại hình tấn công và các giải pháp an ninh

cho mạng không dây. Khảo sát thực nghiệm một số mô hình mạng máy tính không dây. Trên cơ sở đó đề xuất giải pháp, xây dựng ứng dụng đảm bảo an toàn an ninh mạng máy tính không dây ngành giáo dục.

3. Đối tượng nghiên cứu và phạm vi nghiên cứu

❖ ***Đối tượng nghiên cứu***

- Vấn đề an ninh mạng không dây.
- Các công nghệ, mô hình và các chuẩn của mạng không dây.
- Các kỹ thuật tấn công, giải pháp khắc phục.

❖ ***Phạm vi nghiên cứu***

- Thu thập các tài liệu liên quan, phân tích các thông tin liên quan đến đề tài.
- Tìm hiểu các mô hình mạng máy tính không dây trên địa bàn Thành phố Đà Nẵng.

4. Phương pháp nghiên cứu

Kết hợp phương pháp nghiên cứu tài liệu, phương pháp nghiên cứu điều tra và phương pháp nghiên cứu thực nghiệm.

5. Ý nghĩa khoa học và thực tiễn của đề tài

Đề tài góp phần hoàn thiện trong việc đảm bảo an toàn và toàn vẹn dữ liệu cho người sử dụng. Kết quả nghiên cứu của đề tài có giá trị thực tiễn đảm bảo an ninh về mạng máy tính không dây tại cơ quan và tham khảo trong công tác nghiên cứu các mạng không dây khác.

3. Cấu trúc luận văn

Cấu trúc luận văn gồm ba chương như sau:

Chương 1: Cơ sở lý thuyết

Chương 2: Khảo sát thực nghiệm

Chương 3: Xây dựng giải pháp

CHƯƠNG 1
CƠ SỞ LÝ THUYẾT

Chương này nghiên cứu tổng quan mạng máy tính không dây, các chuẩn của mạng không dây và một số mô hình mạng hiện nay đang sử dụng. Bên cạnh đó, chương này còn trình bày về vấn đề an ninh an toàn thông tin: các loại hình tấn công và giải pháp đảm bảo an ninh an toàn thông tin. Những nội dung trong chương này là cơ sở để thực hiện các chương tiếp theo.

1.1. TỔNG QUAN VỀ MẠNG MÁY TÍNH KHÔNG DÂY

1.1.1. Giới thiệu về mạng máy tính không dây

a. Mạng máy tính không dây là gì?

"Mạng máy tính không dây" hay còn gọi là mạng WLAN (Wireless Local Area Network) mạng cục bộ không dây, gồm hai hay nhiều máy tính giao tiếp với nhau bằng những giao thức mạng chuẩn nhưng không cần dây cáp mạng.

b. Các thành phần cơ bản của mạng máy tính không dây

Kiến trúc WLAN cơ bản bao gồm:

- Access Point
- Card giao diện mạng NIC
- Anten
- Bridge và Workgroup Bridge
- Máy chủ AAA
- Switch và router "cảnh báo không dây"

c. Hoạt động của mạng máy tính không dây

Các mạng WLAN sử dụng các sóng điện từ không gian để truyền thông tin từ một điểm tới điểm khác. Các sóng vô tuyến thường được xem như các sóng mang vô tuyến do chúng chỉ thực hiện chức năng cung cấp năng lượng cho một máy thu ở xa. Dữ liệu

đang được phát được điều chế trên sóng mang vô tuyến sao cho có thể được khôi phục chính xác tại máy thu.

Trong một cấu hình mạng WLAN tiêu chuẩn, một điểm truy cập nối với mạng hữu tuyến từ một vị trí cố định sử dụng cáp tiêu chuẩn. Chức năng tối thiểu của điểm truy cập là thu, làm đệm, phát dữ liệu giữa mạng WLAN và cơ sở hạ tầng mạng hữu tuyến.

d. Ưu điểm và nhược điểm của mạng máy tính không dây

❖ *Ưu điểm*

Tính di động: Những người sử dụng mạng WLAN có thể truy nhập nguồn thông tin ở bất kỳ nơi nào trong phạm vi phủ sóng.

Tính đơn giản: Việc lắp đặt, thiết lập, kết nối một mạng WLAN rất dễ dàng, đơn giản và có thể tránh được việc kéo cáp qua các bức tường và trần nhà.

Tính linh hoạt: Có thể triển khai mạng WLAN ở những nơi mà mạng hữu tuyến không thể triển khai được hoặc khó triển khai.

Tiết kiệm chi phí lâu dài: WLAN rất dễ dàng mở rộng và có thể đáp ứng tức thì khi gia tăng số lượng người dùng mà không cần phải cung cấp thêm cáp kết nối như mạng LAN truyền thống.

Khả năng vô hướng: Các mạng WLAN có thể được cấu hình theo các topo khác nhau, dễ dàng thay đổi từ các mạng ngang hàng thích hợp cho một số lượng nhỏ người sử dụng đến các mạng có cơ sở hạ tầng đầy đủ dành cho hàng nghìn người sử dụng mà có khả năng di chuyển trên một vùng rộng.

❖ *Nhược điểm*

Về tính bảo mật: Do sử dụng sóng điện từ để thu/ phát dữ liệu nên tất cả mọi máy trạm nằm trong khu vực phủ sóng đều có thể thu được tín hiệu. Vì vậy, khả năng tấn công của người dùng là rất cao.

Về phạm vi: Một mạng chuẩn 802.11g với các thiết bị chuẩn chỉ có thể hoạt động tốt trong phạm vi vài chục mét như trong phạm vi gia đình hoặc văn phòng.

Về độ tin cậy: WLAN sử dụng sóng vô tuyến để truyền thông nên việc bị nhiễu, tín hiệu bị giảm do tác động của các thiết bị khác như lò vi sóng,… là điều không tránh khỏi.

Về tốc độ: Tốc độ của mạng không dây chậm hơn so với mạng sử dụng cáp.

1.1.2. Các chuẩn của mạng máy tính không dây

a. Chuẩn 802.11 WLAN

IEEE 802.11: Chuẩn không dây IEEE 802.11 cung cấp các giao tiếp không dây với tốc độ l Mbps hoặc 2 Mbps trong các dải ISM 2,4 GHz sử dụng FHSS hoặc DSSS.

IEEE 802.11b: Chuẩn IEEE 802.11b cung cấp việc truyền dữ liệu cho các mạng WLAN trong dải tần số 2,4 GHZ với tốc độ 1 Mbps; 2 Mbps; 5,5 Mbps và có thể đạt tốc độ cao nhất là 11 Mpbs.

IEEE 802.11a: Chuẩn IEEE 802.11a hoạt động trong dải tần số từ 5 Ghz đến 6 GHZ, sử dụng phương pháp điều biến OFDM và có thể nâng tốc độ truyền dữ liệu tối đa lên tới 54 Mbps.

IEEE 802.11g: Chuẩn IEEE 802.11g hỗ trợ việc truyền dữ liệu trong khoảng cách tương đối ngắn với tốc độ 20 Mbps đến 54 Mbps. 802.11g là sự kết hợp tốt nhất giữa 802.11a và 802.11b.

IEEE 802.11n: 802.11n là thế hệ hiện tại của mạng không dây tốc độ cao, khả năng hỗ trợ tốc độ, phạm vi phủ sóng lớn nhất hiện nay. Nó phù hợp với các ứng dụng cần băng thông lớn như các ứng dụng đa phương tiện. Wireless-N được xây dựng dựa trên cơ sở các chuẩn không dây trước đó kết hợp với công nghệ MIMO.

b. Chuẩn 802.16 Broadband wireless

Chuẩn IEEE 802.16 (WiMAX) là công nghệ không dây mang tính cách mạng trong ngành công nghiệp dịch vụ không dây băng rộng. Lớp MAC 802.16 hỗ trợ nền tảng point-to-multipoint trên băng tần 10-66 GHZ, tốc độ truyền tải dữ liệu từ 75 Mbps tới 120 Mbps. Nó sử dụng công nghệ OFDM, tương tự như 802.11a và 802.11g.

c. Chuẩn 802.15 Bluetooth

Bluetooth hoạt động ở dải tần 2,4 Ghz, sử dụng phương thức trải phổ FHSS. Trong mạng Bluetooth, các phần tử kết nối với nhau theo kiểu Adhoc ngang hàng hoặc theo kiểu tập trung, có 1 máy xử lý chính và có tối đa là 7 máy có thể kết nối vào.

1.1.3. Mô hình hoạt động của mạng máy tính không dây

a. Mô hình Ad-Hoc (IBSS – Independent Basic Service Set)

b. Mô hình Infrastructure (BSSs – Basic Service Set)

c. Mô hình mạng mở rộng ESS (Extended Service Set)

d. Các mô hình thực tế

1.2. AN NINH AN TOÀN TRONG MẠNG MÁY TÍNH KHÔNG DÂY

1.2.1. Khái niệm an ninh an toàn thông tin

An ninh an toàn thông tin nghĩa là thông tin được bảo vệ, các hệ thống và những dịch vụ có khả năng chống lại những hiểm họa, lỗi và sự tác động không mong đợi, các thay đổi tác động đến độ an toàn của hệ thống là nhỏ nhất.

1.2.2. Các loại hình tấn công mạng máy tính không dây

a. Tấn công bị động - Passive attacks

Tấn công bị động là một phương pháp tấn công WLAN đơn giản nhất nhưng vẫn rất hiệu quả. Passive attack không để lại một dấu vết nào chứng tỏ đã có sự hiện diện của hacker trong mạng vì

hacker không thật kết nối với AP để lắng nghe các gói tin truyền trên đoạn mạng không dây

b. Tấn công chủ động - Active attacks

Tấn công chủ động là tấn công trực tiếp vào một hoặc nhiều thiết bị trên mạng, ví dụ như vào AP, STA. Cuộc tấn công chủ động có thể được dùng để tìm cách truy nhập tới một Server để thăm dò, lấy những dữ liệu quan trọng, thậm chí thực hiện 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 nhiều, khi phát hiện ra chúng ta chưa kịp có phương pháp đối phó thì nó đã thực hiện xong quá trình phá hoại.

c. Tấn công kiểu chèn ép - Jamming attacks

Phương thức Jamming là sử dụng máy phát có tần số phát giống tần số mà mạng sử dụng để áp đảo làm mạng bị nhiễu, bị ngừng làm việc. Tấn công bằng Jamming không phải là sự đe dọa nghiêm trọng, nó khó có thể được thực hiện phổ biến do vấn đề giá cả của thiết bị, nó quá đắt trong khi kẻ tấn công chỉ tạm thời vô hiệu hóa được mạng.

d. Tấn công theo kiểu thu hút - Man in the middle attacks

Tấn công theo kiểu thu hút là dùng một khả năng mạnh hơn chen vào giữa hoạt động của các thiết bị và thu hút, giành lấy sự trao đổi thông tin của thiết bị về mình. Thiết bị chèn giữa đó phải có vị trí, khả năng thu phát trội hơn các thiết bị sẵn có của mạng.

e. Tấn công vào các yếu tố con người

Đây là một hình thức tấn công nguy hiểm nhất nó có thể dẫn tới những tổn thất hết sức khó lường. Kẻ tấn công có thể liên lạc với người quản trị hệ thống thay đổi một số thông tin nhằm tạo điều kiện cho các phương thức tấn công khác.

f. Một số kiểu tấn công khác

Ngoài các hình thức tấn công kể trên, kẻ tấn công còn sử dụng một số kiểu tấn công khác như tạo ra các virus đặt nằm tiềm ẩn trên các file khi người sử dụng do vô tình trao đổi thông tin qua mạng không dây mà người sử dụng đã tự cài đặt nó lên trên máy của mình..

1.2.3. Giải pháp đảm bảo an ninh an toàn mạng máy tính không dây

a. Bảo mật bằng WEP (Wired Equivalent Privacy)

WEP là một thuật toán bảo nhằm bảo vệ sự trao đổi thông tin chống lại sự nghe trộm, chống lại những kết nối mạng không được cho phép cũng như chống lại việc thay đổi hoặc làm nhiễu thông tin truyền. WEP sử dụng stream cipher RC4 cùng với một mã 40 bit và một số ngẫu nhiên 24 bit (initialization vector - IV) để mã hóa thông tin. Thông tin mã hóa được tạo ra bằng cách thực hiện phép toán XOR giữa keystream và plain text. Thông tin mã hóa và IV sẽ được gửi đến người nhận. Người nhận sẽ giải mã thông tin dựa vào IV và khóaWEP đã biết trước.

b. Bảo mật bằng WPA (Wifi Protected Access)

WPA là một giải pháp bảo mật được đề xuất bởi liên minh WiFi nhằm khắc phục những hạn chế của WEP. WPA được nâng cấp bằng việc cập nhật phần mềm SP2 của Microsoft.

WPA cải tiến 3 điểm yếu nổi bật của WEP

WPA cũng mã hóa thông tin bằng RC4 nhưng chiều dài của khóa là 128 bit và IV có chiều dài là 48 bit. Một cải tiến của WPA là WPA sử dụng giao thức TKIP nhằm thay đổi khóa dùng AP và user một cách tự động trong quá trình trao đổi thông tin.

WPA sử dụng 802.1x/EAP để đảm bảo tính nhận thực lẫn nhau chống lại kiểu tấn công xen vào giữa. Quá trình nhận thực dựa trên một server nhận thực (Radius/Diameter).

WPA sử dụng thuật toán kiểm tra tính toàn vẹn của bản tin MIC để tăng cường tính toàn vẹn của thông tin truyền. MIC là bản tin 64 bit được tính dựa trên thuật toán Michael. MIC được gửi trong gói TKIP, giúp người nhận kiểm tra xem thông tin nhận được có bị lỗi trên đường truyền hoặc bị thay đổi bởi kẻ phá hoại hay không.

Những điểm yếu của WPA

Điểm yếu đầu tiên của WPA là nó vẫn không giải quyết được kiểu tấn công từ chối dịch vụ. Kẻ phá hoại có thể làm nhiễu mạng WPA WiFi bằng cách gửi ít nhất hai gói thông tin với một khóa sai mỗi giây.

Ngoài ra, WPA vẫn sử dụng thuật toán RC4 mà có thể dễ dàng bị bẻ vỡ 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. 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.

c. Bảo mật bằng WPA2

Đến năm 2006, WPA chính thức bị thay thế bởi WPA2. Một trong những cải tiến đáng chú ý nhất của WPA2 so với WPA là sự có mặt bắt buộc của AES và CCMP nhằm thay thế cho TKIP. AES sử dụng thuật toán mã hóa đối xứng theo khối Rijndael, sử dụng khối mã hóa 128 bit và 192 bit hoặc 256 bit. Chuẩn mã hóa này được sử dụng cho các cơ quan chính phủ Mỹ để bảo vệ các thông tin nhạy cảm.

d. Các công cụ bảo mật hệ thống

❖ *Chứng thực bằng địa chỉ MAC*

❖ *Chứng thực bằng SSID*

e. Bảo mật nhiều lớp

Dựa trên lý thuyết thì mô hình bảo mật an toàn nhất cho bất cứ mạng vô tuyến nào chính là sự kết hợp các phương pháp bảo mật nhỏ lại với nhau (WEP, WPA, WPA2, Firewall, VPN, Radius Server, lọc địa chỉ MAC).

Sự kết hợp giữa các phương pháp bảo mật này sẽ tạo ra cơ chế bảo mật nhiều lưới. Bởi vì mỗi giải pháp bảo mật chỉ nhằm phục vụ một mục đích khác nhất định nào đó nên kết hợp chúng lại thì sẽ giúp dữ liệu được an toàn dưới nhiều dạng tấn công hơn.

CHƯƠNG 2
KHẢO SÁT THỰC NGHIỆM

Trong chương này nghiên cứu thực trạng và yêu cầu đảm bảo an ninh an toàn thông tin đối với hệ thống mạng máy tính không dây ngành giáo dục. Nghiên cứu thực nghiệm một số mô hình, giải pháp mạng máy tính không dây tại một số trường đại học – cao đẳng. Đây là cơ sở để đề xuất giải pháp, xây dựng ứng dụng nhằm đảm bảo an ninh an toàn cho mạng máy tính không dây tại các trường học trong khu vực nói riêng và ngành giáo dục nói chung.

2.1. PHÂN TÍCH NHU CẦU ĐẢM BẢO AN NINH AN TOÀN THÔNG TIN ĐỐI VỚI HỆ THỐNG MẠNG MÁY TÍNH KHÔNG DÂY

2.1.1. Tiêu chí đánh giá hệ thống an ninh an toàn thông tin

a. Đánh giá trên phương diện vật lý

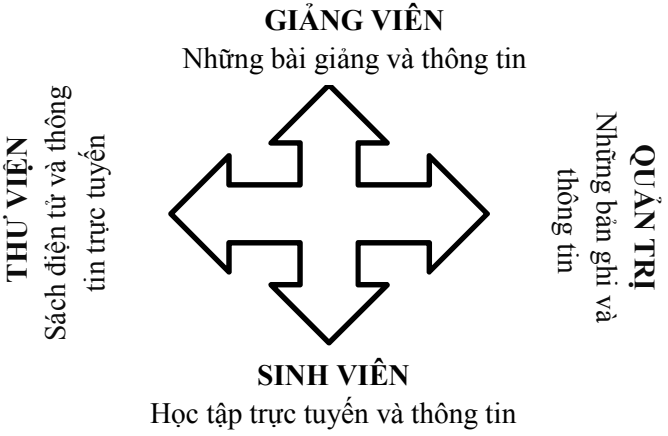
b. Đánh giá trên phương diện logic

2.1.2. Phân tích nhu cầu đảm bảo an ninh an toàn cho mạng máy tính không dây

2.2. PHÂN TÍCH NHU CẦU ĐẢM BẢO AN NINH AN TOÀN THÔNG TIN TRONG NGÀNH GIÁO DỤC

2.2.1. Vai trò của mạng máy tính không dây đối với giáo dục

Việc trang bị hệ thống mạng máy tính không dây ở các trường đại học sẽ làm tăng khả năng tương tác giữa giảng viên và sinh viên; giảng viên, sinh viên và người quản trị mạng hay giảng viên, sinh viên và hệ thống thư viện trực tuyến. Họ có thể truy cập thông tin và các ứng dụng mạng dễ dàng hơn ở bất cứ nơi nào trong khuôn viên của trường. Bên cạnh đó, nó còn khuyến khích sinh viên sử dụng máy tính xách tay có trang bị công nghệ không dây của chính họ nhằm giúp họ tăng khả năng học tập – nghiên cứu. Với hệ thống mạng máy tính này, hiệu quả học tập của sinh viên có thể được cải thiện vì họ không bị gò bó bởi không gian học tập.



Hình 2.1. Sự tương tác giữa các đối tượng sử dụng khi truy cập thông tin bằng mạng máy tính không dây

2.2.2. Yêu cầu đảm bảo an ninh an toàn thông tin đối với hệ thống mạng máy tính không dây ở các trường đại học – cao đẳng

a. Nhu cầu bảo vệ dữ liệu

Nhu cầu bảo vệ dữ liệu ở các trường đại học – cao đẳng là vấn đề đặc biệt quan trọng bởi vì toàn bộ cơ sở dữ liệu về quản lý đào tạo của nhà trường được lưu và thao tác tại các máy Server của trường. Nó bao gồm các dữ liệu về điểm học tập của sinh viên, kế hoạch giảng dạy – học tập của giảng viên và sinh viên, các thông tin về học phí,… Những dữ liệu này yêu cầu phải tuyệt đối đảm bảo an toàn không bị đánh cắp hoặc sửa chữa thông tin.

b. Nhu cầu bảo vệ các tài nguyên sử dụng trên mạng

Ở các trường đại học – cao đẳng thì nhu cầu sử dụng các tài nguyên trên mạng là rất lớn. Tuy nhiên những tài nguyên này luôn bị đe dọa bởi những kẻ tấn công. Đầu tiên chúng truy cập vào hệ thống, sau khi đã làm chủ được hệ thống bên trong thì chúng có thể sử dụng các máy này để phục vụ cho mục đích của mình như cài đặt các chương trình chạy ẩn để dò mật khẩu người sử dụng, ứng dụng các liên kết mạng sẵn có để lấy cắp các thông tin cần thiết hoặc tiếp tục tấn công các hệ thống khác, …

c. Nhu cầu bảo vệ danh tiếng trường học

Các con số thống kê về các cuộc tấn công thường không được thông báo một cách rộng rãi. Một trong những nguyên nhân là nỗi lo bị mất uy tín của trường học, đặc biệt là gây sự hoang mang không tin tưởng vào các thông tin mà nhà trường đã cung cấp. Đối với những 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.

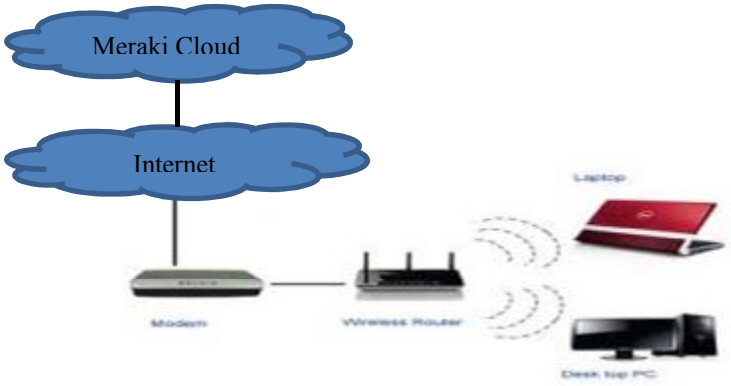
2.3. MÔ HÌNH MẠNG MÁY TÍNH KHÔNG DÂY Ở CÁC TRƯỜNG ĐẠI HỌC – CAO ĐẲNG TRÊN ĐỊA BÀN THÀNH PHỐ ĐÀ NẴNG

2.3.1. Mô hình mạng máy tính không dây tại trường Đại học Kinh Tế Đà Nẵng

a. Giới thiệu

b. Công nghệ và giải pháp Meraki Wireless

- *Công nghệ*
- *Giải pháp*



Hình 2.2. Mô hình mạng Wireless Meraki tại trường Đại Học Kinh Tế

c. Ưu điểm và nhược điểm mạng Wireless Meraki

- *Ưu điểm*

- Quản lý tập trung nhờ công nghệ điện toán đám mây làm Controller.

- Giảm chi phí mua Controller cực lớn, không tốn phí upgrade, hay sửa chữa controller, không bị tạm ngưng việc hoạt động của network khi controller cần upgrade.

- Công cụ bảo mật cao nhất với các tính năng được tích hợp sẵn như: IDS, RADIUS, TACACS+, LDAP, WPA2,...

- Nhiều SSID với nhiều mục đích phục vụ khác nhau: Mạng riêng biệt dành cho nội bộ hay sinh viên và mạng công cộng dành cho khách công cộng.

- Người quản trị hệ thống không cần phải có trình độ về chuyên ngành cao cũng có thể quản lý hệ thống thông qua hệ thống quản lý mạng trực tuyến.

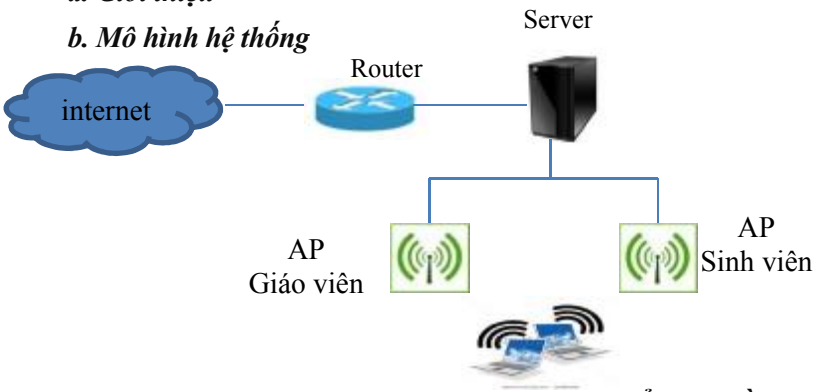
❖ *Nhược điểm*

- Giá thành đầu tư thiết bị đắt.

2.3.2. Mô hình mạng máy tính không dây tại trường Cao Đẳng Nghề Đà Nẵng

a. Giới thiệu

b. Mô hình hệ thống



Hình 2.3. Mô hình mạng không dây tại trường Cao Đẳng Nghề Đà Nẵng

d. Ưu điểm và nhược điểm của mạng không dây của trường

❖ *Ưu điểm*

- Hệ thống mạng máy tính không dây của trường được lắp đặt khá đơn giản.

- Chi phí cho hệ thống tương đối thấp.
- Không yêu cầu số người quản trị hệ thống nhiều.

❖ *Nhược điểm*

- Không quản lý tập trung.
- Không phân quyền cho người sử dụng.
- Không kiểm soát người dùng.
- Cơ chế bảo mật chỉ dựa trên WPA2 của thiết bị Wireless Access Point.
- Wireless Access Point Alcon 24005 với chuẩn IEEE 802.11g có băng thông thấp và số người dùng truy cập cùng lúc ít.

2.3.3. Đánh giá chung các mô hình mạng máy tính không dây tại khu vực khảo sát

Qua khảo sát thực nghiệm các mô hình mạng máy tính không dây trên địa bàn thành phố Đà Nẵng, tiêu biểu là hai mô hình mạng không dây của trường Đại học Kinh Tế và trường Cao Đẳng Nghề thì vẫn còn tồn tại nhiều hạn chế. Hầu hết các mô hình không dây chỉ dựa trên cơ chế bảo mật WPA, WPA2 trên các Access Point, người dùng sau khi đã nhập mật khẩu hay những kẻ tấn công bẻ khóa mật khẩu để truy nhập vào hệ thống mạng thì có thể sử dụng các công cụ như Net Tool, Net IP, … để lấy thông tin, dữ liệu từ các máy tính trong mạng.

2.4. KẾT LUẬN

Qua quá trình khảo sát thực tế các mô hình mạng máy tính không dây trên địa bàn, người nghiên cứu nhận thấy các mô hình trên vẫn còn nhiều hạn chế, không được hiệu quả. Cụ thể như sau:

Hoạt động: Sóng không ổn định vì không có sự hỗ trợ liên kết giữa các node (không mesh). Dễ dàng có điểm chết khi một node có vấn đề.

Quản lý mạng: Có Controller nên có thể quản lý mạng, nhưng việc quản lý bó buộc tại Controller, chức năng báo động sự cố chưa năng động lắm.

Khi có sự cố: Việc tự động cấu hình trở lại diễn ra chậm hơn.

Điểm yếu: Chi phí cho Controller rất cao, và controller vẫn bị hạn chế trong việc tải số lượng node. Hoạt động mạng phụ thuộc hoàn toàn vào Controller nên rủi ro cao.

CHƯƠNG 3
XÂY DỰNG GIẢI PHÁP

3.1. ĐỀ XUẤT GIẢI PHÁP ĐẢM BẢO AN NINH AN TOÀN MẠNG MÁY TÍNH KHÔNG DÂY NGÀNH GIÁO DỤC

3.1.1. Mô hình đề xuất

a. Nguyên tắc thiết kế

Hệ thống mạng không dây được xây dựng trong ngành giáo dục phải đáp ứng các nhu cầu sau:

- Đảm bảo truy cập không dây cho các thiết bị di động hỗ trợ.

- Đảm bảo cung cấp được khả năng truy cập tại các khu vực làm việc chính và một số khu vực khuôn viên bên ngoài các các tòa nhà trên.Cung cấp các thông tin, tài nguyên, giao tiếp giữa sinh viên và nhà trường.

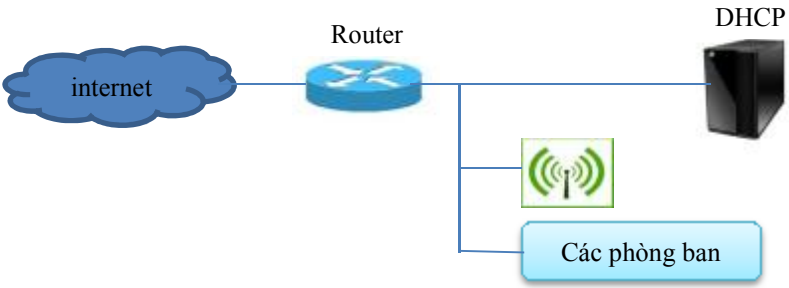
- Đảm bảo việc truy cập vào hệ thống Server của trường để đăng ký môn học của sinh viên trong toàn trường.

- Phải có khả năng cung cấp dịch vụ Roaming.

- Đảm bảo cung cấp các tính năng bảo mật phù hợp tin cậy để đảm bảo an toàn thông tin cho toàn bộ hệ thống cơ sở dữ liệu quan trọng của trường.

b. Thiết kế mô hình

Mô hình thiết kế vật lý chi tiết hệ thống mạng không dây đề xuất như sau:



Hình 3.1. Mô hình mạng không dây đề xuất

3.1.2. Giải pháp xây dựng ứng dụng của mô hình

b. Giải pháp kiểm soát người dùng thông qua địa chỉ MAC để cấp IP

DHCP Server tạo các lớp mạng IP khác nhau như lớp giáo viên, lớp sinh viên, khách, … Chỉ có lớp IP giáo viên được quyền truy cập vào hệ thống để lấy dữ liệu phục cho việc dạy học còn lớp IP khác như sinh viên, khách thì không có quyền.

Khi người dùng muốn kết nối vào mạng thông qua các điểm truy cập không dây thì người dùng đó phải chứng thực địa chỉ MAC máy của mình với người quản trị và người quản trị sẽ cấp một địa chỉ IP tương ứng với lớp người dùng dựa trên địa chỉ MAC thông qua DHCP Server.

c. Giải pháp quản lý tập trung như một Controller của router Draytek 5510

Sử dụng router Draytek như một Controller làm giải pháp quản lý tập trung toàn bộ hệ thống mạng. Thiết bị này có các tính năng bảo mật như chống virus, spam, chống xâm nhập, giới hạn băng thông và

các tính năng quản lý như quản lý địa chỉ IP hay nhóm địa chỉ IP, tạo ra các rule cho phép hay không cho phép người dùng truy cập internet, facebook, yahoo, skype, xem video streaming, khóa các truy cập trang web theo từ khóa hay khóa truy cập trang web theo nội dung và chuyên đề, ... Đặc biệt, nó có tính năng Smart Monitor giúp tìm ra và khóa những trang web không lành mạnh nhằm tạo một môi trường Internet an toàn.

d. Giải pháp điểm truy cập và mở rộng mạng không dây tốc độ cao

Với công nghệ chuẩn N tốc độ mạng không dây lên tới 300Mbps, TP-Link TL-WA901ND rất lý tưởng cho việc truy cập mạng không dây tốc độ cao và các ứng dụng tiêu tốn nhiều băng thông. Ngoài ra với công nghệ tiên tiến MIMO cung cấp băng tần không dây cao Tx/Rx có khả năng phát sóng ở phạm vi xa hơn lên tới 30 mét, đồng thời hoạt động thông qua ba ăn-ten ngoài Tx và Rx để vượt qua sự suy giảm tín hiệu hay vượt qua các rào cản vật lý, có khả năng xuyên tường và phát sóng tốt.

TP-Link TL-WA901ND cung cấp mã hóa WPA/WPA2 bảo mật mạng WLAN và hỗ trợ chế độ hoạt động Repeater giúp dễ dàng xây dựng mở rộng hệ thống mạng không dây tại những khu vực khó khăn hoặc loại bỏ vùng chết không dây.

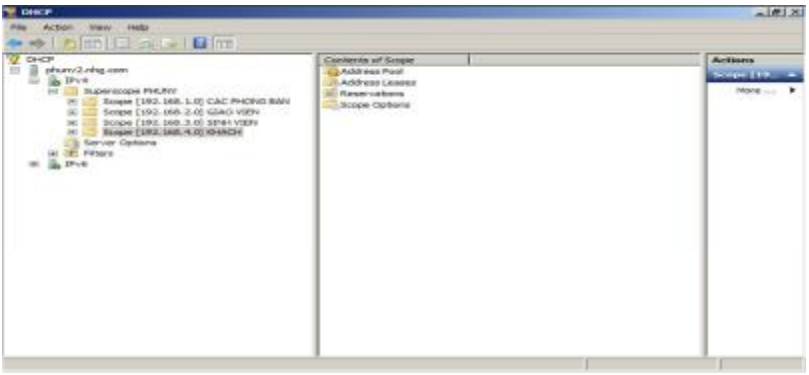
3.2. KẾT QUẢ MÔ PHỎNG MÔ HÌNH ĐỀ XUẤT

3.2.1. DHCP Server

DHCP Server dùng để tạo 4 lớp địa chỉ IP, cấp IP cho 4 nhóm người dùng khác nhau:

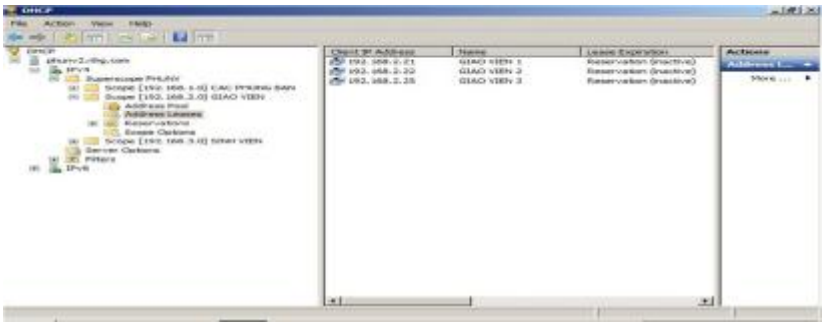
- Lớp 192.168.1.x : là lớp IP cấp cho các phòng ban.
- Lớp 192.168.2.x : là lớp IP cấp cho giáo viên.
- Lớp 192.168.3.x : là lớp IP cấp cho sinh viên.

- Lớp 192.68.4.x: là lớp IP cấp cho lớp khách.



Hình 3.5. Lớp IP cấp cho nhóm người dùng

Người dùng phải gởi địa chỉ MAC của máy mình tới người quản trị và ứng với mỗi địa chỉ MAC người quản trị sẽ cấp một địa chỉ IP tương ứng với lớp người dùng đó. Ví dụ người dùng là giáo viên thì sẽ được cấp IP trong lớp giáo viên là 192.168.2.x, người dùng là sinh viên thì sẽ được cấp IP trong lớp sinh viên là 192.168.3.x.



Hình 3.6. Cấp IP cho lớp người dùng dựa trên địa chỉ MAC của người dùng

3.2.2. Router Draytek VigorPro 5510

a. Cấu hình Objects Setting

❖ *IP Object/IP Group:* tạo những nhóm địa chỉ IP (địa chỉ của

tất cả các host trong một bộ phận) thành tên.

❖ *Service Type Object:* tạo các đối tượng dịch vụ như Web http, Mail …

b. Cấu hình Content Security Management (CSM)

❖ *CSM >>APP Enforcement Profile:* tạo bộ lọc dùng để cho phép hoặc không cho phép các ứng dụng, chương trình chat IM, P2P, các Video Streaming.

❖ *URL Content Filter Profile:* tạo các bộ lọc ngăn chặn các chức năng trên web và đồng thời cũng có thể chặn luôn các trang web cấm mà không cần quan tâm đến IP của trang web đó.

❖ *Web Content Filter:* tạo bộ lọc khóa truy cập các trang web theo nội dung và chuyên đề. Vào CSM>>Web Content Filter Profile.

c. Cấu hình Firewall

❖ *General Setup:* lọc các ứng dụng, đối tượng, URL, … với các rule đã tạo.

❖ *Filter Setup:* dùng để lọc các đối tượng IP, đối tượng dịch vụ, … với các rule đã tạo.

❖ *DoS Defense:* nhằm giúp hệ thống giảm bớt nguy cơ bị quá tải vì bị tấn công DoS.

d. Cấu hình Defense Configuration

Defense Configuration là tính năng được tích hợp sẵn trên router với các công cụ bảo mật cao nhất như: Anti-Virus, Anti-Spam, Anti-Intrusion để ngăn chặn các sự tấn công ngay từ đầu vào.

e. Cấu hình Bandwidth Management

❖ *Session Limit:* giới hạn phiên truyền thông người dùng để ngăn chặn nghẽn mạng do các session.

❖ *Bandwidth Limit:* Là tính năng giới hạn băng thông người dùng nhằm giới hạn tốc độ download và upload của các máy tính trong mạng.

f. Cấu hình công cụ Smart Monitor

❖ ***Mô hình ứng dụng***

Trực tiếp: Máy tính cài Smart Monitor nối dây mạng trực tiếp đến port Lan Mirror trên DrayTek Vigor.

Gián tiếp: Máy tính cài Smart Monitor nối dây mạng đến một port Mirror trên Swicth; từ Swicth nối dây mạng đến bất kỳ port Lan nào trên DrayTek Vigor.

3.2.3. Wireless Access Point TP-Link TL-WA901ND

a. Kết nối

b. Truy cập

c.Thiết lập cấu hình

3.3. ĐÁNH GIÁ KẾT QUẢ

➢ **Khả năng kết nối**

Mô hình này đảm bảo cho người dùng truy cập mạng an toàn, thuận tiện có nghĩa là sinh viên hoặc giảng viên có thể sử dụng thông tin quan trọng khi họ cần, giúp họ trở nên có năng suất cao hơn ngay cả khi họ không ngồi trước bàn làm việc.

➢ **Khả năng tương tác**

Mô hình trên giúp mở rộng đáng kể phạm vi địa lý của giáo dục và tạo điều kiện thuận lợi cho việc tương tác cũng như cộng tác thông qua khả năng truy cập nhanh hơn đối với kho nghiên cứu, thư

viện trực tuyến, cổng đào tạo, hệ thống quản lý khóa học và nhiều hơn nữa.

- **An ninh mạng**

Thông qua chuẩn mã hóa không dây DES và AES, các hệ thống băng thông rộng của các thiết bị trong mô hình giúp những trường học, khu vực trường, trường cao đẳng và đại học riêng lẻ tạo và duy trì các mức an ninh cao để hỗ trợ và bảo vệ yêu cầu giáo dục kép bao gồm sáng tạo mở và chia sẻ thông tin.

- **An toàn cho khuôn viên và trường học**

Mô hình cho phép người quản trị có thể quản lý tập trung người dùng dựa trên địa chỉ MAC để nâng cao an ninh cho cơ sở và khuôn viên trường cũng như tăng cường an toàn cá nhân cho sinh viên, giảng viên và nhân viên.

- **Giảm chi phí**

Mô hình trên với những thiết bị đơn giản và cách lắp đặt hệ thống cũng không phức tạp nhưng đảm bảo tính an toàn cho cả hệ thống. Đặc biệt, chi phí đầu tư cho hệ thống mạng máy tính không dây như mô hình đề xuất ở trên không lớn. Do vậy, nếu nó được ứng dụng sẽ giúp tiết kiệm khoản chi phí đầu tư.

KẾT LUẬN

An ninh mạng máy tính không dây là vấn đề luôn được đặt ra cho các nhà triển khai dịch vụ và thu hút rất nhiều nghiên cứu cả về lý thuyết cũng như ứng dụng. Tuy nhiên, hiện tại chưa có một giải pháp nào được xem là hoàn hảo cho mọi tình huống. Chính vì vậy, khi thiết kế hệ thống mạng máy tính không dây, chúng ta phải dựa trên cơ sở, yêu cầu thực tế của hệ thống, cân nhắc giữa các lợi hại của các phương pháp để đưa ra các chính sách an ninh, bảo mật hợp

lý nhất. Trong thực tế xây dựng hệ thống mạng Internet không dây cho nhà trường đều có sự tham gia của các thành phần khác nhau và có những yêu cầu bảo mật khác nhau. Phân tích kỹ lưỡng các điều này giúp ta quyết định biện pháp nào là phù hợp nhất với hệ thống.

1. Kết quả đạt được

Nghiên cứu được thực hiện trong một thời gian không dài, song nó vẫn đạt được một số kết quả như sau:

- Trình bày tổng quan về mạng máy tính không dây cung cấp cho người đọc một cách khái quát cơ chế hoạt động của mạng WLAN, ưu điểm cũng như các mô hình hoạt động của mạng WLAN.
- Trình bày thực trạng mất an ninh an toàn của mạng không dây, các kiểu tấn công trong mạng không dây và một số giải pháp cho việc đảm bảo an ninh an toàn cho mạng không dây.
- Tìm hiểu, đánh giá về các mô hình mạng máy tính không dây ở một vài địa điểm thực tế. Từ đó, tác giả đưa ra đề xuất giải pháp đảm bảo an ninh an toàn cho mạng WLAN ngành giáo dục góp phần bảo mật thông tin khi trao đổi qua mạng WLAN của ngành đáp ứng yêu cầu đặt ra.

2. Hạn chế của đề tài

Trong khuôn khổ của luận văn này, việc nghiên cứu mới chỉ dừng lại ở mức phân tích và đưa ra một số các nhận xét về các biện pháp và công cụ an ninh, bảo mật đã có cũng như các phương thức bảo mật đang được phát triển và sử dụng với hệ thống mạng máy tính không dây nhằm cung cấp thêm cho người quản trị mạng có cái nhìn tổng quan hơn về các công nghệ hiện hành và khả năng bảo mật thật sự của hệ thống mạng máy tính không dây, từ đó ra quyết định lựa chọn phương án an ninh, bảo mật cho hệ thống của mình.

Do phạm vi bảo mật mạng WLAN là rất rộng, đòi hỏi tính chuyên môn cao. Bên cạnh đó, điều kiện, môi trường để ứng dụng hệ thống mạng máy tính không dây còn gặp nhiều khó khăn nên tôi chưa thể tiến hành mô phỏng thực nghiệm các ứng dụng bảo mật trên hệ thống. Toàn bộ nội dung luận văn mới chỉ dừng lại ở mức độ cấu hình trên các thiết bị hiện có.

Thời gian thực hiện nghiên cứu có giới hạn cũng như kiến thức và trình độ bản thân còn hạn chế nên luận văn không thể tránh những thiếu sót. Tôi mong rằng sẽ nhận được những ý kiến đóng góp của các thầy cô và các anh/chị để luận văn hoàn thiện hơn, có ích hơn trong thực tế và trong công việc hàng ngày của tôi.

3. Hướng nghiên cứu trong tương lai

- Đi sâu vào nghiên cứu các thuật toán, các giao thức, kỹ thuật bảo mật.
- Nghiên cứu về các công cụ phần mềm cũng như phần cứng được sử

  dụng để tấn công mạng WLAN trong nhiều môi trường điều hành khác nhau để phân tích, so sánh điểm mạnh, điểm yếu của từng công cụ nhằm mục đích sử dụng nó tìm ra lỗ hổng, điểm yếu tồn tại trong WLAN để đưa ra các giải pháp để hạn chế và khắc phục các điểm yếu và lỗ hỏng đó
- Nghiên cứu các biện pháp tích hợp hệ thống chứng thực điện tử cho việc đảm bảo an toàn thông tin.