HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

NGUYỄN THẾ NGUYÊN

NGHIÊN CỨU BẢO MẬT TRONG MẠNG KHÔNG DÂY VÀ GIẢI PHÁP AN NINH CHO MẠNG QUẢN LÝ CỦA BƯU ĐIỆN TỈNH HÒA BÌNH

CHUYÊN NGÀNH : TRUYỀN DỮ LIỆU VÀ MẠNG MÁY TÍNH

MÃ SỐ: 60.48.15

Người hướng dẫn khoa học: TS. Nguyễn Thành Phúc

TÓM TẮT LUẬN VĂN THẠC SĨ KỸ THUẬT

HÀ NỘI - 2011

MỞ ĐẦU

Khi thiết kế các yêu cầu kỹ thuật cho mạng không dây, chuẩn 802.11 của IEEE đã có tính đến vấn đề bảo mật dữ liệu đường truyền qua phương thức mã hóa. Trong đó, phương thức WEP đã được đa số các nhà sản xuất thiết bị không dây hỗ trợ như là một phương thức mặc định bảo mật không dây. Tuy nhiên, những phát hiện gần đây về điểm yếu của chuẩn 802.11 WEP cho thấy WEP không phải là một cơ chế bảo mật toàn diện cho mạng WLAN và các nhà nghiên cứu đã tìm ra một phương thức bảo mật mới WAP2 tương ứng là chuẩn 802.11i.

1. Cấu trúc của luận văn

Ngoài phần mở đầu và kết luận, nội dung của luận văn này được bố cục như sau:

Chương 1: **Trình bày tổng quan về mạng LAN không dây**.

Chương 2: **Trình bày về an ninh mạng LAN không dây, các kiểu tấn công và an ninh đối với mạng LAN không dây.**

An ninh mạng LAN không dây chuẩn 802.11i

Trình bày thuật toán mã hóa sử dụng trong chuẩn IEEE 802.11i.

Chương 3: **Giải pháp an ninh cho mạng quản lý của bưu điện tỉnh Hòa Bình**

Cuối cùng là tài liệu tham khảo.

Chương 1:

TỔNG QUAN VỀ MẠNG LAN KHÔNG DÂY CHUẨN IEEE 802.11

1.1 Các mô hình của mạng máy tính không dây cơ bản

- Independent Basic Service sets – IBSS
- Basic Service sets – BSS
- Extended Service sets – ESS

1.2 Các chuẩn của 802.11

Ngành công nghiệp không dây thiết lập tần số sóng vô tuyến và các chuẩn truyền dữ liệu đối với việc truyền tín hiệu của các máy tính trong mạng nội bộ không dây. Các

chuẩn đó được phát triển bởi viện kỹ thuật điện và điện tử - Institute of Electrical and Electronics Engineers (IEEE). Hiện tại có 4 chuẩn hỗ trợ cho mạng máy tính không dây: Wireless-A, Wireless-B, Wireless-G, và Wireless-N.

a) Không dây chuẩn-A (802.11a)

Hoạt động ở dải tần số 5GHz, ở dải tần này có nhiều sóng điện thoại và vi sóng hoạt động, đây có thể là nguyên nhân dẫn tới hiện tượng giao thoa. Mặc dù tốc độ đạt tới 54Mbs nhưng phạm vi phủ sóng chỉ đạt 75feet (khoảng 20m). Chuẩn A không dây không tương thích với cả chuẩn-B và chuẩn-G không dây vì nó hoạt động ở dải tần số khác.

b) Không dây chuẩn-B (802.11b)

Hoạt động ở dải tần số 2.4GHz và có thể truyền dữ liệu với tốc độ 11Mbps trong một phạm vi lên tới 100-150feet (khoảng 30-45m). Phạm vi phát sóng không dây có thể bị ảnh hưởng bởi các vật phản xạ hay các tín hiệu phát sóng khác như gương, bức tường, các thiết bị, vị trí, hoặc trong nhà hay ngoài trời.

c) Không dây chuẩn-G (802.11g)

Các đặc tính của không dây chuẩn-G tương tự với không dây chuẩn-B, nhưng tốc độ tăng gấp 5 lần, đạt 54Mbps. Hiện tại không dây chuẩn-G có giá trị và hiệu suất tốt nhất. Có thể cho các thiết bị không dây chuẩn-B hoạt động cùng với thiết bị không dây chuẩn-G nhưng không đạt được hiệu suất cao nhất của chuẩn-G về tốc độ.

d) Không dây chuẩn-N (draft 802.11n)

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 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.

e) Không dây chuẩn-N hỗ trợ dải tần kép Dual-band (draft 802.11n)

Các thiết bị định tuyến Dual-band là tương thích với cả 2 dải tần số 2.4GHz và 5GHz. Loại thiết bị định tuyến không dây hiện tại không hỗ trợ dual-band chỉ cho phép làm việc với 1 dải tần số trong suốt quá trình thiết lập và cấu hình. Nhưng với loại hỗ trợ đặc tính dual-band cho phép hoạt động trên 2 dải cùng lúc, băng thông lúc nào cũng sẵn sàng và luồng dữ liệu truyền lớn hơn.

Chương 2:
AN NINH MẠNG LAN KHÔNG DÂY

2.1 Các kiểu tấn công đối với mạng không dây

Hacker có thể tấn công mạng WLAN bằng các cách sau:

- Passive Attack (eavesdropping)

- Active Attack (kết nối, thăm dò và cấu hình mạng)

- Jamming Attack

- Man-in-the-middle Attack

Các phương pháp tấn công trên có thể được phối hợp với nhau theo nhiều cách khác nhau

2.1.1 Passive Attack (eavesdropping)

Tấn công bị động (passive) hay nghe lén (eavesdropping) có lẽ 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

2.1.2 Active Attack

Hacker có thể tấn công chủ động (active) để thực hiện một số tác vụ trên mạng. Một cuộc tấn công chủ động có thể được sử dụng để truy cập vào server và lấy được những dữ liệu có giá trị hay sử dụng đường kết nối Internet của doanh nghiệp để thực hiện những mục đích phá hoại hay thậm chí là thay đổi cấu hình của hạ tầng mạng. 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. So với kiểu tấn công bị động thì tấn công chủ động có nhiều phương thức đa dạng hơn, ví dự như: Tấn công từ chối dịch vụ (DOS), Sửa đổi thông tin (Message Modification), Đóng giả, mạo danh, che dấu (Masquerade), Lặp lại thông tin (Replay), Bomb, spam mail, v v...

2.1.3 Jamming (tấn công bằng cách gây nghẽn)

Jamming là một kỹ thuật được sử dụng chỉ đơn giản để làm hỏng (shut down) mạng không dây. 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. Khi một hacker chủ động tấn công jamming, hacker có thể sử dụng một thiết bị WLAN đặc biệt, thiết bị này là bộ phát tín hiệu RF công suất cao hay sweep generator.

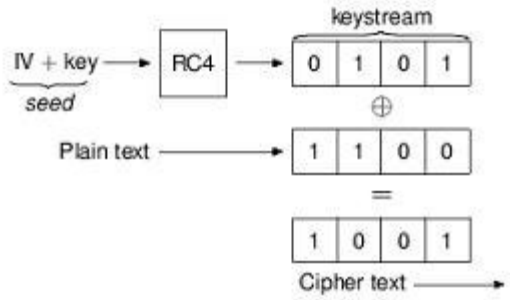
2.1.4 Man-in-the-middle Attack

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 gởi 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.

2.2 An ninh mạng máy tính không dây

2.2.1. 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. Sơ đồ mã hóa được miêu tả bởi hình 1.



Hình 1: Sơ đồ mã hóa bằng WEP

Những điểm yếu về bảo mật của WEP

+ WEP sử dụng khóa cố định được chia sẻ giữa một Access Point (AP) và nhiều người dùng (users) cùng với một IV ngẫu nhiên 24 bit. Do đó, cùng một IV sẽ được sử dụng lại nhiều lần. Bằng cách thu thập thông tin truyền đi, kẻ tấn công có thể có đủ thông tin cần thiết để có thể bẻ khóa WEP đang dùng.

+ Một khi khóa WEP đã được biết, kẻ tấn công có thể giải mã thông tin truyền đi và có thể thay đổi nội dung của thông tin truyền. Do vậy WEP không đảm bảo được sự cẩn mật (confidentiality) và toàn vẹn (integrity) của thông tin.

+ Việc sử dụng một khóa cố định được chọn bởi người sử dụng và ít khi được thay đổi (có nghĩa là khóa WEP không được tự động thay đổi) làm cho WEP rất dễ bị tấn công.

+ WEP cho phép người dùng (supplicant) xác minh (authenticate) AP trong khi AP không thể xác minh tính xác thực của người dùng. Nói một cách khác, WEP không cung ứng khả năng nhận thực lẫn nhau (mutual authentication).

2.2.2. Bảo mật bằng WPA (Wifi Protected Access)

WPA là một giải pháp bảo mật được đề xuất bởi liên minh WiFi (WiFi Alliance) 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 đối với WEP là WPA sử dụng giao thức TKIP (Temporal Key Integrity Protocol) nhằm thay đổi khóa dùng AP và user một cách tự động trong quá trình trao đổi thông tin. Cụ thể là TKIP dùng một khóa nhất thời 128 bit kết hợp với địa chỉ MAC của user host và IV để tạo ra mã khóa. Mã khóa này sẽ được thay đổi sau khi 10.000 gói thông tin được trao đổi.

+ WPA sử dụng 802.1x/EAP để đảm bảo tính nhận thực lẫn nhau nhằm chống lại kiểu tấn công xen vào giữa (man-in-middle attack). Quá trình nhận thực của WPA dựa trên một server nhận thực, còn được biết đến với tên gọi RADIUS/ DIAMETER. Server RADIUS cho phép xác thực user trong mạng cũng như định nghĩa những quyền kết nối của user. Tuy nhiên trong một mạngWiFi nhỏ (của công ty hoặc cơ quan,trường học), đôi khi không cần thiết phải cài đặt một server mà có thể dùng một phiên bản WPA- PSK (pre-shared

key). Ý tưởng của WPA-PSK là sẽ dùng một password giống như một chìa khóa vạn năng (Master Key) chung cho AP và các máy trạm (client devices). Thông tin nhận thực giữa user và server sẽ được trao đổi thông qua giao thức nhận thực mở rộng EAP (Extensible Authentication Protocol). Phiên EAP sẽ được tạo ra giữa user và server để chuyển đổi thông tin liên quan đến việc nhận dang của user cũng như của mạng. Trong quá trình này AP đóng vai trò là một EAP proxy, làm nhiệm vụ chuyển giao thông tin giữa server và user.

+ WPA sử dụng thuật toán kiểm tra tính toàn vẹn của bản tin MIC (Michael Message Integrity Check) để tăng cường tính toàn vẹn của thông tin truyền. MIC là một bản tin 64 bit được tính dựa trên thuật tóan Michael. MIC sẽ được gửi trong gói TKIP và 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.

Tóm lại, WPA được xây dựng nhằm cải thiện những hạn chế của WEP nên nó chứa đựng những đặc điểm vượt trội so với WEP. Đầu tiên, nó sử dụng một khóa động mà được thay đổi một cách tự động nhờ vào giao thức TKIP. Khóa sẽ thay đổi dựa trên người dùng, phiên trao đổi nhất thời và số lượng gói thông tin đã truyền. Đặc điểm thứ 2 là WPA cho phép kiểm tra xem thông tin có bị thay đổi trên đường truyền hay không nhờ vào bản tin MIC. Và đăc điểm nối bật thứ cuối là nó cho phép nhận thực lẫn nhau bằng cách sử dụng giao thức802.1x.

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 (denial-of-service (DoS) attack)[5]. Kẻ phá hoại có thể làm nhiễu mạng WPA WiFi bằng cách gửi ít nhất 2 gói thông tin với một khóa sai (wrong encryption key) mỗi giây. Trong trường hợp đó, AP sẽ cho rằng một kẻ phá hoại đang tấn công mạng và AP sẽ cắt tất cả các kết nối trong vòng một phút để trách hao tổn tài nguyên mạng. Do đó, sự tiếp diễn của thông tin không được phép sẽ làm xáo trộn hoạt động của mạng và ngăn cản sự kết nối của những người dùng được cho phép (authorized users).

Ngoài ra WPA vẫn sử dụng thuật tóan 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 (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.

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.

2.2.3. Tăng cường bảo mật với chuẩn 802.11i

Chuẩn 802.11i được phê chuẩn vào ngày 24 tháng 6 năm 2004 nhằm tăng cường tính mật cho mạng WiFi. 802.11i mang đầy đủ các đặc điểm của WPA. Tập hợp những giao thức của 802.11i còn được biết đến với tên gọi WPA 2. Tuy nhiên, 802.11i sử dụng thuật toán mã hóa AES (Advanced Encryption Standard) thay vì RC4 như trong WPA. Mã khóa của AES có kích thước là 128, 192 hoặc 256 bit. Tuy nhiên thuật toán này đổi hỏi một khả năng tính toán cao (high computation power). Do đó, 802.11i không thể update đơn giản bằng software mà phải có một dedicated chip. Tuy nhiên điều này đã được ước tính trước bởi nhiều nhà sản xuất nên hầu như các chip cho card mạngWifi từ đầu năm 2004 đều thích ứng với tính năng của 802.11i.

Mô tả thuật toán

Quá trình mã hóa bao gồm 4 bước:

1. AddRoundKey - mỗi byte của khối được kết hợp với khóa con, các khóa con này được tạo ra từ quá trình tạo khóa con Rijndael.
2. SubBytes - đây là phép thế (phi tuyến) trong đó mỗi byte sẽ được thế bằng một byte khác theo bảng tra (Rijndael S-box).
3. ShiftRows - đổi chỗ, các hàng trong khối được dịch vòng.
4. MixColumns - quá trình trộn làm việc theo các cột trong khối theo một phép biến đổi tuyến tính.

Tại chu trình cuối thì bước MixColumns được thay thế bằng bước AddRoundKey

2.2.4 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 lới. 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. Ví dụ lọc địa chỉ MAC thì chỉ cho địa chỉ MAC nào đó các quyền truy nhập vào AP/network, tuy nhiên giải pháp này không thể áp dụng trong phạm vi nhỏ với vài máy tính/thiết bị đã biết rõ địa chỉ MAC. Vả lại việc bắt chước (cấu hình lại địa chỉ MAC) cũng khá dễ thực hiện. Chỉ cần nghe lén vào gói tin thì có thể biết chúng dùng địa chỉ MAC gì, rồi bắt chước lại là có thể truy cập vào ngon lành.

Ở các công ty họ thường dùng thêm VPN và firewall để bảo mật thông tin truyền đi. Đó chính là để đảm bảo nếu có bị crack WEP/WPA/WPA2 thì kẻ tấn công cũng chỉ có thể kết nối thông qua AP, nhưng không thâm nhập vào được mạng nội bộ, không biết được thông tin trao đổi là gì. Đồng thời họ cũng ứng dụng MAC hay HMAC để đảm bảo tính toàn vẹn của dữ liệu. Đó chính là sử dụng bảo mật nhiều lớp để tăng độ an toàn cho mạng. Một cách đơn giản việc kết hợp nhiều biện pháp bảo mật cũng giống như nhà sử dụng nhiều khóa để tăng độ an toàn.

2.2.5. Kết luận chương

Trên con đường đi từ WEP đến chuẩn 802.11i (WPA2), rất nhiều nội dung về bảo mật đã ra đời. Có 6 vấn đề cơ bản về bảo mật đó là : xác minh (Identification), nhận thực (Authentication), sự cấp phép (Authorization), sự cẩn mật (Confidentiality), và tính toàn vẹn (Integrity). WEP đã thất bại về mặt bảo mật vì nó đã được xây dựng mà không tính đến những vấn đề này. Khi mạng không dây phát triển bùng nổ yêu cầu về bảo mật cũng đòi hỏi cao hơn và chính là tiền đề cho chuẩn 802.11i ra đời để tăng cường bảo mật cho mạng không dây Wifi. Tuy nhiên 802.11i (WPA2) chỉ có thể nâng cấp phần mềm nếu phần cứng có thể đáp ứng tiêu chuẩn bảo mật tiên tiến AES . Nếu không thì phải cần nâng cấp phần cứng để có thể sử dụng 802.11i. Và một vấn đề nữa khi sử dụng WAP2 là những sản phẩm thích ứng với 802.11i lại không thể thích ứng với WEP.

Như vậy thì mặc dù với sự ra đời của nhiều biện pháp mới như chuẩn 802.11i hay các thiết bị phần cứng và phần mềm được tích hợp nhiều phương án bảo mật để có thể bảo mật

nhiều lớp song rõ ràng vấn đề bảo mật trong mạng WiFi vẫn còn là một vấn đề cần tiếp tục được quan tâm nghiên cứu nhiều hơn nữa.

Chương 3:

GIẢI PHÁP AN NINH CHO MẠNG LAN KHÔNG DÂY CỦA MẠNG QUẢN LÝ BƯU ĐIỆN TỈNH HÒA BÌNH

3.1 Mô tả bài toán

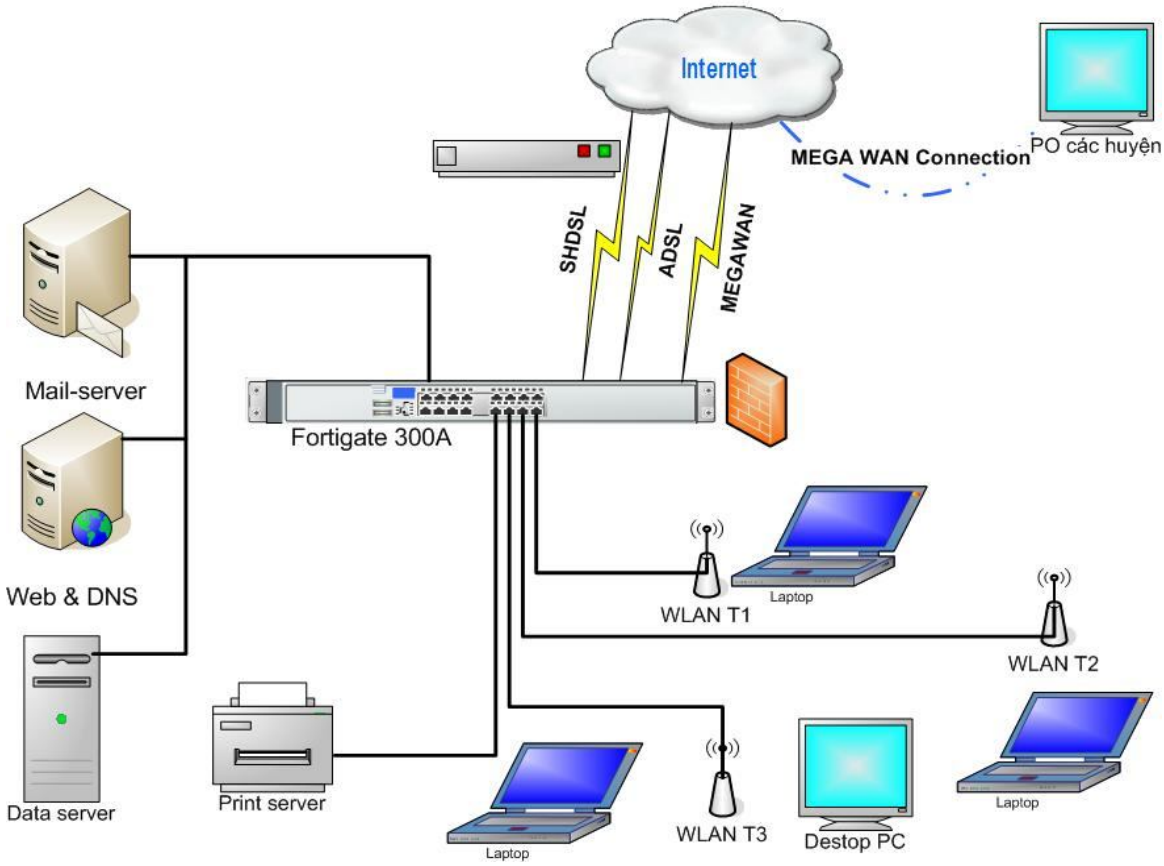
3.1.1Nguyên tắc thiết kế

Hệ thống mạng không dây được xây dựng tại trường bưu điện tỉnh Hòa Bình để 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 phòng ban làm việc.
- Phải có khả năng cung cấp dịch vụ Roaming (Người dùng mạng không dây có thể di truyển qua nhiều vùng phủ sóng của các Access Point khác nhau mà không bị ngắt quãng truy cập).
- Đảm báo 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 cơ quan. Đối với mỗi người dùng đảm bảo quyền truy cập và sử dụng các Data và tài nguyên mạng ở các cấp độ khác nhau.

3.2 Sơ đồ mạng mô phỏng:

Sơ đồ mạng quản lý bưu điện tỉnh Hòa Bình



3.3 Cấu hình bảo mật

3.3.1. Cấu hình trên thiết bị Access Point

(Ở đây minh họa với thiết bị Access Point Linksys WAP200)

Mong muốn người dùng

Mong muốn sử dụng hệ thống mạng không dây để chia sẻ kết nối và tài nguyên trong mạng LAN cho máy tính xách tay hoặc máy tính PC có card mạng Wireless sử dụng một cách an toàn.

Giải pháp

Sử dụng thiết bị WAP200 Linksys có khả năng phát sóng không dây làm điểm truy cập cho máy tích xách tay và máy tính PC với card wireless và các thiết bị không dây với mạng LAN.

Tính năng Multi SSID cho phép cấu hình nhiều tên mạng WiFi khác nhau, đáp ứng nhu cầu bảo mật với hệ thống mạng.

Tiến hành cấu hình WAP2:

Cấu hình tính năng bảo mật WPA2-AES

Trong phần cấu hình **Wireless** bạn chọn tab **Wireless security**, màn hình giao diện như hình dưới:

Hình 3.7: Cấu hình WAP2 trên Access Point

Bạn có thể chọn kiểu mã hóa để đảm bảo tính bảo mật cho hệ thống mạng không dây của bạn.

(Ví dụ hình dưới tôi chọn mã hóa WPA2-AES, sử dụng key thứ 1 với password là 1234567890)

Hình 3.8: Cấu hình WAP2

Ấn **Save Settings** để lưu lại cấu hình bạn vừa chỉnh sửa. Với những bước cấu hình như trên ta đã có hệ thống Wireless sử dụng phương thức bảo mật WAP2

KẾT LUẬN

An toàn dữ liệu máy tính luôn là vấn đề rất được quan tâm, đặc biệt là vấn đề an toàn dữ liệu mạng khi mà mạng máy tính trong giai đoạn phát triển mạnh mẽ. Mạng LAN không dây 802.11 sử dụng môi trường truyền dẫn không dây điện từ với những đặc điểm riêng của nó cần có những giải pháp an ninh riêng bên cạnh các giải pháp an ninh truyền thống cho mạng hữu tuyến. Việc tập trung nghiên cứu, đánh giá mức độ an ninh của mạng này không chỉ có ý nghĩa đối với riêng lĩnh vực quân sự, kỹ thuật mà còn đối với tất cả các lĩnh vực đang áp dụng nó.

Do vậy luận văn trước hết thực hiện việc tìm hiểu, phân tích các giải pháp an ninh cũng như các rủi ro từ mạng 802.11 dựa trên các tiêu chí đảm bảo: tính an toàn, tính xác thực, tính toàn vẹn. Qua đó có thể thấy chuẩn an ninh 802.11i với mục tiêu cung cấp một giải pháp an ninh mới cho mạng 802.11 đủ khả năng để mang lại mã hóa an toàn cho dữ liệu.

Theo hướng tìm hiểu được cho thấy phương pháp Rijndael thích hợp cho việc triển khai trên nhiều hệ thống khác nhau, Ngoài ra, tất cả các bước xử lý của việc mã hóa và giải mã đều được thiết kế thích hợp với cơ chế xử lý song song nên phương pháp Rijndael càng chứng tỏ thế mạnh của mình trên các hệ thống thiết bị mới.

Mặc dù vậy, do hạn chế về mặt thời gian, điều kiện thiết bị, cộng với trình độ có hạn, luận văn chưa tiến hành được về mặt thực nghiệm mô hình lý thuyết đã đề xuất. Do đó chỉ có được những đánh giá bước đầu về lĩnh vực tìm hiểu.

Phương pháp Rijndael với mức độ an toàn rất cao cùng các ưu điểm đáng chú ý khác chắc chắn sẽ nhanh chóng được áp dụng rộng rãi trong nhiều ứng dụng trên các hệ thống khác nhau. Do đó, trong tương lai, việc tiếp tục nghiên cứu phương pháp mã hóa này cũng là vấn đề cần quan tâm cả về mặt lý thuyết lẫn áp dụng trong hệ thống thực tiễn.