HỌC VIỆN KTQS
KHOA CÔNG NGHỆ THÔNG TIN

Bài 10. An ninh mạng không dây

Học phần: ĐẢM BẢO VÀ AN TOÀN THÔNG TIN

NỘI DUNG

Tổng quan về mạng không dây

1.Lịch sử mạng không dây

2.Mạng không dây là gì?

3.Phân loại

4.Chuẩn IEEE 802.11

5.Chế độ hoạt động

Bảo mật mạng không dây

1. Tổng quan về an ninh mạng không dây
2. Khả năng bảo mật của mạng không dây
3. Kết luận và một số khuyến cáo

PHẦN I: TỔNG QUAN

1. Lịch sử ra đời

- Do Guglielmo Marconi sáng lập ra.
- Năm 1894, Marconi bắt đầu các cuộc thử nghiệm và năm 1899 đã gửi thành công một bức điện báo băng qua kênh đào Anh mà không cần sử dụng bất kỳ loại dây nào.
- 3 năm sau, thiết bị vô tuyến của Marconi đã có thể chuyển và nhận điện báo qua Đại Tây Dương.
- Trong chiến tranh thế giới thứ nhất, lần đầu tiên nó được sử dụng ở cuộc chiến Boer năm 1899

1. Lịch sử ra đời

-Trước thập niên 1920, điện báo vô tuyến trở thành một phương tiện truyền thông hữu hiệu bởi nó cho phép gửi các tin nhắn cá nhân băng qua lục địa.

- Thập niên 1980, công nghệ vô tuyến là những tín hiệu analog.

- Thập niên 1990, chuyển sang tín hiệu số ngày càng có chất lượng tốt hơn, nhanh hơn và công nghệ ngày nay phát triển dột phá với tín hiệu 4G.

- Năm 1994, công ty viễn thông Ericsson đã bắt đầu sáng chế và phát triển công nghệ kết nối các thiết bị di động thay thế các dây cáp. Ho đặt tên thiết bị này là “Bluetooth”.

2. Mạng không dây là gì?

Khái niệm: Mạng không dây là một hệ thống các thiết bị được nối lại với nhau, có khả năng giao tiếp thông qua sóng vô tuyến thay vì các đường truyền dẫn bằng dây.

2. Mạng không dây là gì?

Ưu điểm

1. Giá thành giảm

2. Công nghệ không dây đã được tích hợp vào bộ vi xử lí của MTXT nên những người có MTXT đều có thể kết nối

3. Không bị giới hạn về kết nối vật lý

4. Tính linh động:tạo ra sự thoải mái trong việc truyền tải dữ liệu giữa các thiết bị có hỗ trợ mà không có sự ràng buộc về khoảng cách và không gian.

5. Mạng WLAN dùng sóng hồng ngoại và sóng radio để truyền, nhận dữ liệu.

2. Mạng không dây là gì?

Nhược điểm

1. Tốc độ mạng bị phụ thuộc vào băng thông, thấp hơn mạng cố định vì mạng không dây chuẩn phải xác nhận cẩn thận những frame đã nhận để tránh tình trạng mất dữ liệu.

2. Trong mạng cố định truyền thống thì tìn hiệu truyền trong dây dẫn nên có thể được bảo mật an toàn hơn. Còn mạng không dây sử dụng sóng radio thì có thể bị bắt và xử lí được bởi bất kì thiết bị nhận nào nằm trong phạm vi cho phép.

3. Mạng không dây có ranh giới không rõ ràng nên rất khó quản lý.

3.Phân loại

Mạng không dây	Mạng có dây
1.Tốc độ:11/54/106Mbps	10/100/1000Mbps
2.Bảo mật: Không đảm bảo bằng mạng có dây do phát sóng thông tin ra mọi phía	Đảm bảo chỉ bị lộ thông tin nếu can thiệp thẳng vào dây dẫn.
3.Thi công: Nhanh và dễ dàng	Thi công phức tạp do phải thiết kế đi dây cho toàn hệ thống
4.Khả năng mở rộng: Khả năng mở rộng khoảng cách tốt với chi phí hợp lý	Đòi hỏi chi phí cao khi muốn mở rộng hệ thống mạng đặc biệt là mở rộng bằng cáp quang
5.Tinh mềm dẻo: Các vị trí kết nối mạng có thể thay đổi mà không cần phải thiết kế lại	Các vị trí thiết kế không cơ động phải thiết kế lại nếu thay đổi vị trí kết nối mạng

Bảng so sánh hệ thống Mạng không dây và Mạng có dây

3.Phân loại

Dựa trên vùng phủ sóng

1.WPAN (Mạng vô tuyến cá nhân)

2.WLAN (Mạng vô tuyến cục bộ)

3.WMAN (Mạng vô tuyến đô thị)

4.WWAN(Mạng vô tuyến diện rộng)

5.WRAN (Mạng vô tuyến khu vực)

Dựa trên các công nghệ mạng

1.Kết nối sử dụng tia hồng ngoại

2.Sử dụng công nghệ Bluetooth

3.Kết nối bằng chuẩn Wifi

4. Chuẩn IEEE 802.11

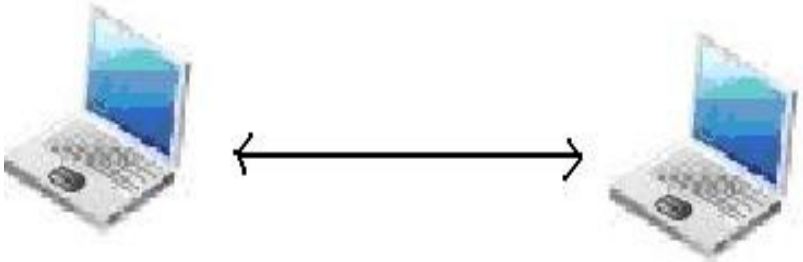
Wireless card đóng vai trò như một bộ thu phát tín hiệu giúp các thiết bị số trao đổi dữ liệu với nhau hoặc truy cập Internet tốc độ cao theo các chuẩn sau:

1. IEEE 802.11a: tốc độ truyền dẫn tối đa 54Mbps
2. IEEE 802.11b: tốc độ truyền dẫn tối đa 11Mbps
3. IEEE 802.11g: tốc độ truyền dẫn tối đa 54Mbps

5. Chế độ hoạt động

Chế độ Ad – hoc :

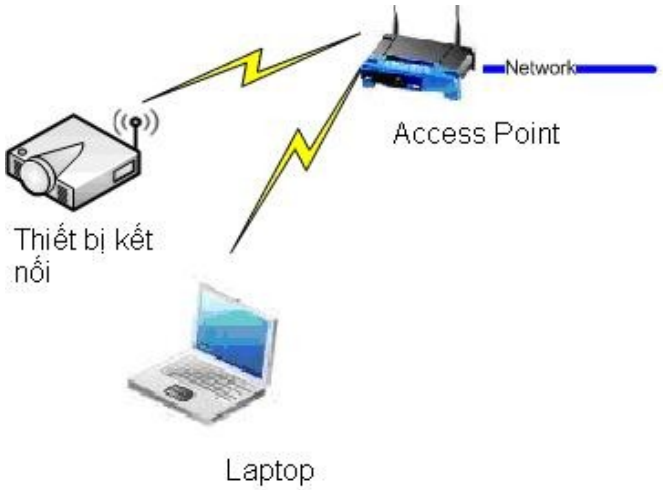
- Là mạng gồm 2 hay nhiều máy tính có trang bị card không dây (tương tự mô hình peer to peer trong mạng có dây)
- Các máy tính có vai trò như nhau
- Khoảng cách liên lạc 30-100m



5. Chế độ hoạt động

Chế độ hạ tầng: Là mạng gồm 1 hay nhiều AP để mở rộng phạm vi hoạt động của các máy trạm có thể kết nối với nhau với mộ phạm vi gấp đôi.

- AP đóng vai trò là điểm truy cập cho các máy trạm trao đổi dữ liệu với nhau và truy xuất tài nguyên của Server



PHẦN 2:
BẢO MẬT MẠNG KHÔNG DÂY

BẢO MẬT MẠNG KHÔNG DÂY

1. Tổng quan về an ninh mạng không dây
2. Khả năng bảo mật của mạng không dây
3. Kết luận và một số khuyến cáo

1. Tổng quan an ninh mạng không dây

Thực trạng vấn đề bảo mật mạng không dây:

1. Bảo mật mạng không dây là một bài toán khó

2. Mạng không dây phát triển mạng mẽ từ các doanh nghiệp tới người dùng đơn lẻ, tạo điều kiện cho hacker

3. Người dùng chưa quan tâm đúng mức tới an ninh mạng không dây

4. Mạng không dây vẫn tồn tại một số lỗ hổng nghiêm trọng giúp cho hacker có thể khai thác.

1. Tổng quan an ninh mạng không dây

Môt số mối đe dọa

1. War driver: Kẻ tấn công muốn truy cập Internet miễn phí nên cố gắng để tìm và tấn công các điểm truy cập WLAN không có an ninh hay an ninh yếu.
2. Tin tặc: Sử dụng mạng không dây như một cách để truy cập vào mạng doanh nghiệp mà không cần phải đi qua các kết nối Internet do có bức tường lửa.
3. Nhân viên: Nhân viên vô tình có thể giúp tin tặc truy cập vào mạng doanh nghiệp bằng nhiều cách.
4. Điểm truy cập giả mạo: kẻ tấn công thiết lập AP của riêng mình, với các thiết lập tương tự các AP hiện có. Khi người dùng sử dụng các AP giả mạo này sẽ bị lộ thông tin.

1. Tổng quan an ninh mạng không dây

Một số biện pháp sử dụng bảo mật hiện nay

1. Xác thực lẫn nhau

2. Mã hóa dữ liệu

3. Phát hiện hệ thống xâm nhập bất hợp pháp

2. Khả năng bảo mật của mạng không dây

Lịch sử phát triển của an ninh mang không dây

1997, chuẩn 802.11 chỉ cung cấp
SSID (Service Set Identifier)
Lọc trên địa chỉ MAC
WEP (Wired Equivalent Privacy)
2001
Fluhrer, Mantin và Shamir đã chỉ ra một số điểm yếu trong WEP
IEEE bắt đầu khởi động nhóm i (802.11i)

2. Khả năng bảo mật của mạng không dây

Lịch sử phát triển của an ninh mang không dây

2003
Wi-Fi Protected Access(WPA) được giới thiệu
Là một giải pháp tạm thời cho WEP
Một phần của IEEE 802.11i

2004
WPA2 được giới thiệu
Nó dựa trên chuẩn IEEE 802.11i
Được phê chuẩn vào 25/06/2004

Các tính năng an ninh cơ bản của 802.11

Kiểm soát truy cập dùng SSID

- Service Set Identifier.
- SSID là định danh của mạng cục bộ không dây.
- Người dùng được yêu cầu phải cung cấp SSID khi kết nối đến các Access Point.
- Khi thay đổi SSID cần phải thông báo đến mọi người.
- SSID được các máy trạm gửi dạng bản rõ nên dể dàng bị đánh cắp.

Các tính năng an ninh cơ bản của 802.11

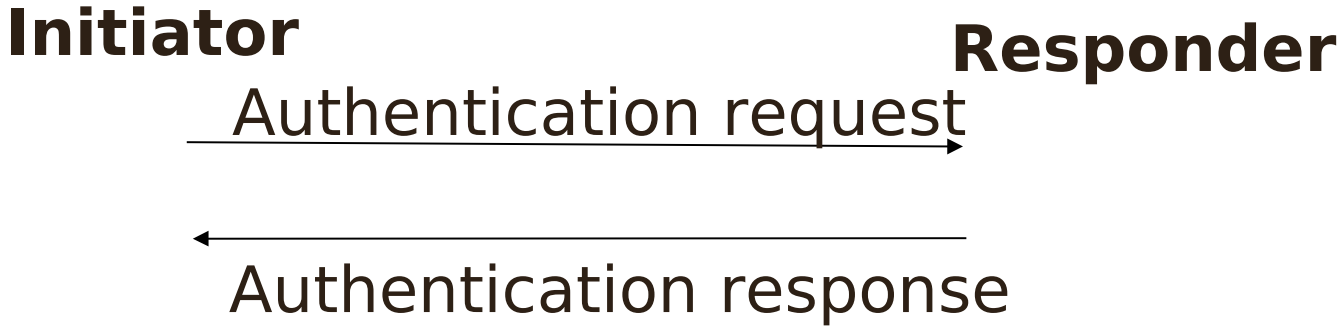
Lọc địa chỉ MAC

- Kiểm soát truy cập bằng cách chỉ cho phép các máy tính có các địa chỉ MAC khai báo trước được kết nối đến mạng.
- Địa chỉ MAC có thể bị giả mạo.
- Phải duy trì và phân phối một danh sách các địa chỉ MAC đến tất cả các Access Point.
- Không phải là giải pháp khả thi cho các ứng dụng công cộng.

Các tính năng an ninh cơ bản của 802.11

Xác thực người dùng

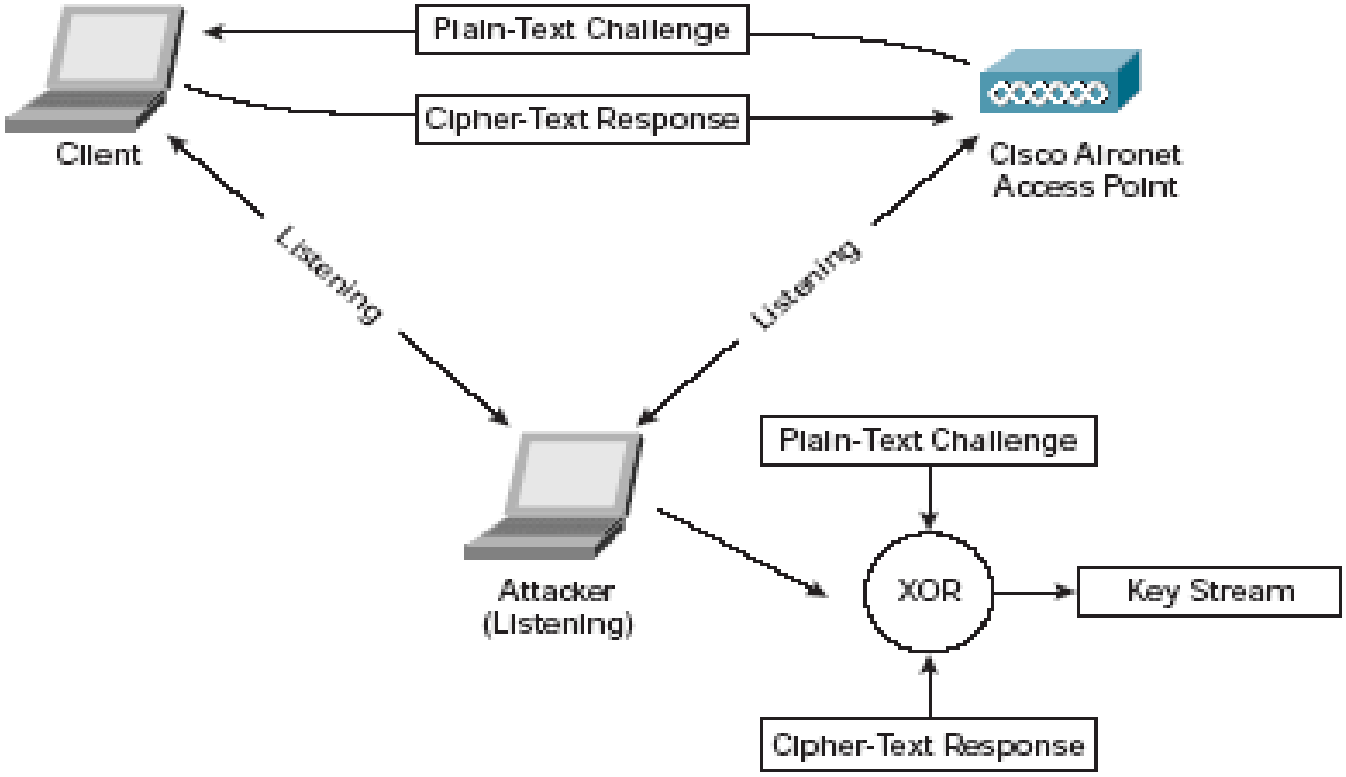
- Có hai loại xác thực người dùng
- Xác thực hệ thống mở
- Xác thực bất cứ ai yêu cầu xác thực
- Cung cấp dạng xác thực NULL



Các tính năng an ninh cơ bản của 802.11

Xác thực người dùng

- Xác thực dùng khóa chung
- Dễ dàng sniff khóa chung



Các tính năng an ninh cơ bản của 802.11

Ngoài vấn đề kiểm soát truy cập cũng cần phải đảm bảo bí mật và toàn vẹn thông tin giữa các máy trạm và Access Point.

- Chuẩn 802.11x định nghĩa WEP(Wired Equivalent Privacy) để kiểm soát truy cập và bảo vệ thông tin khi nó đi qua mạng cục bộ không dây.
- WEP cung cấp 3 dịch vụ cơ bản: xác thực, bí mật, toàn vẹn.

WEB

Dịch vụ xác thực

- Được dùng để xác thực các máy trạm khi kết nối đến các Access Point
- Trong hệ thống xác thực mở, máy trạm được xác thực nếu nó đáp ứng một địa chỉ MAC khi trao đổi ban đầu với Access Point -> không cung cấp danh tính của máy trạm.
- WEP cũng sử dụng một cơ chế xác thực dựa trên mật mã. Cơ chế này dựa trên một khóa bí mật dùng chung và thuật toán mã hóa RC4.
- Trao đổi xác thực dùng một hệ thống challenge – response.

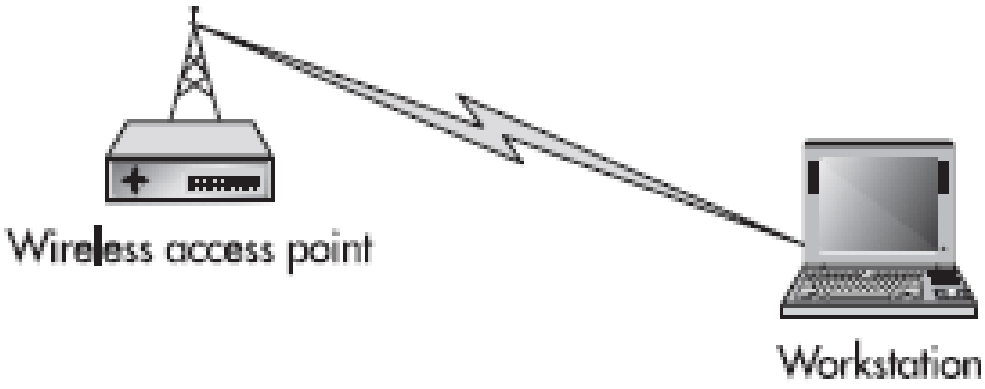
Dịch vụ xác thực

1. Workstation sends authentication request to the AP.

2. AP sends the random challenge to the workstation.

3. Workstation responds to the AP with the challenge encrypted using the shared secret.

4. If the challenge decrypts properly, the AP confirms success.



WEB

Dịch vụ xác thực

- Hệ thống challenge – response không xác thực Access Point.
- Vì vậy nó dể dàng bị tấn công như dùng Access Point giả mạo, “man in the midle”

Dịch vụ bí mật

- Cũng dựa trên RC4.
- Tạo ra dòng khóa giả ngẫu nhiên để mã hóa dữ liệu.
- Tuy nhiên WEP không chỉ định một cơ chế quản lý khóa.
- Điều này có nghĩa là WEP dựa trên các khóa tĩnh. Trong thực tế, các khóa tương tự được sử dụng cho tất cả các máy trạm trên mạng.

WEB

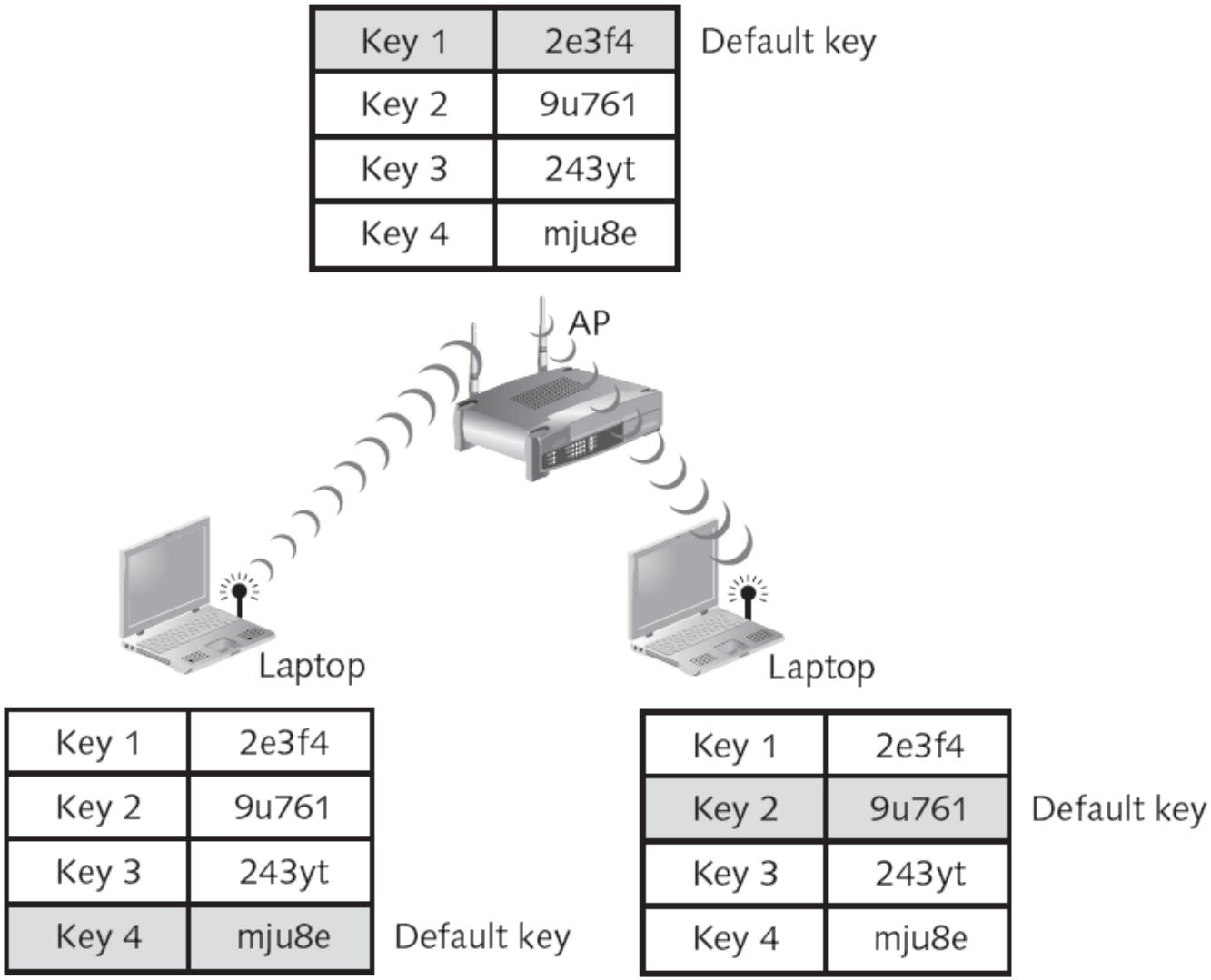


Figure 6-3 Default WEP key

WEB

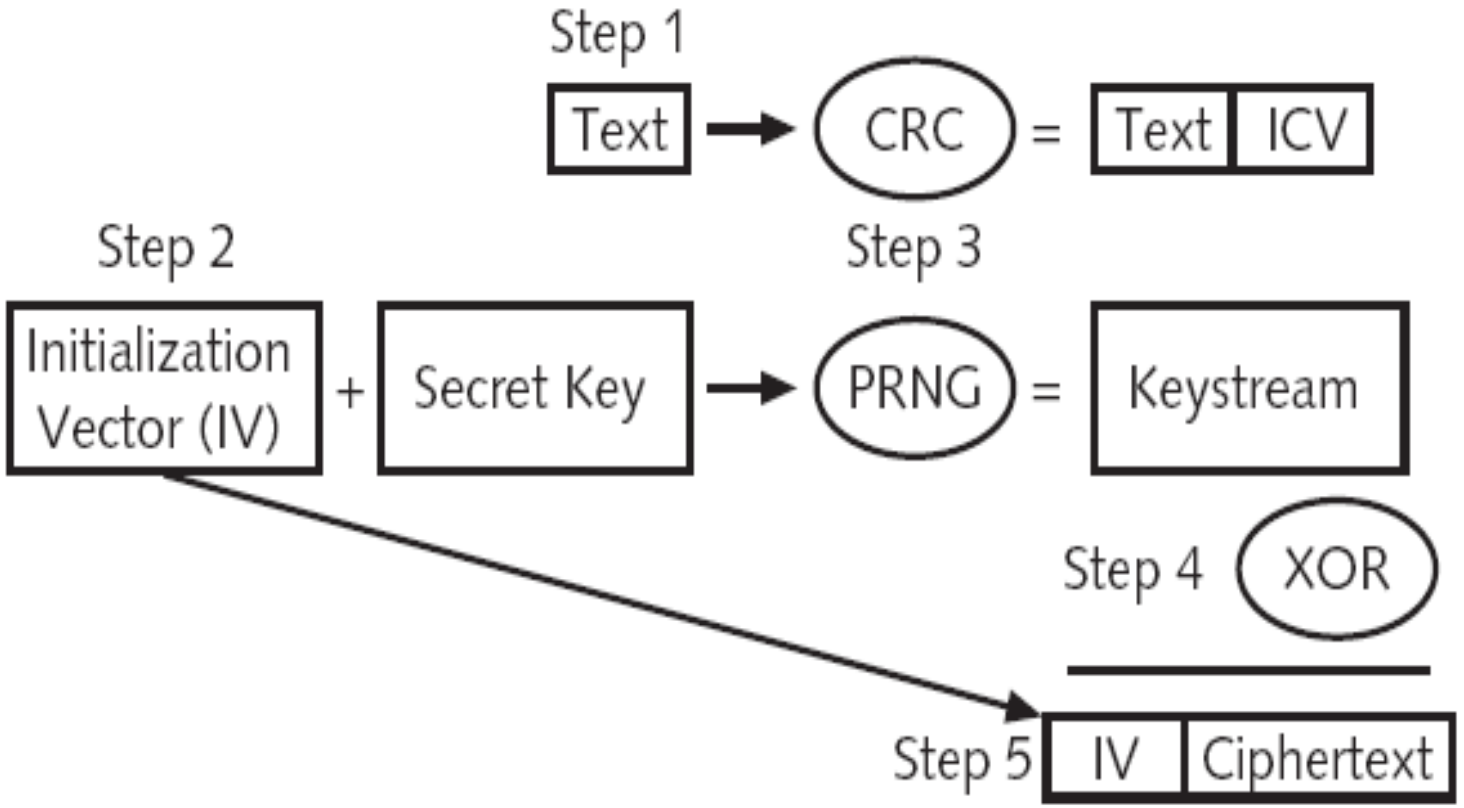


Figure 6-4 WEP encryption process

WEB

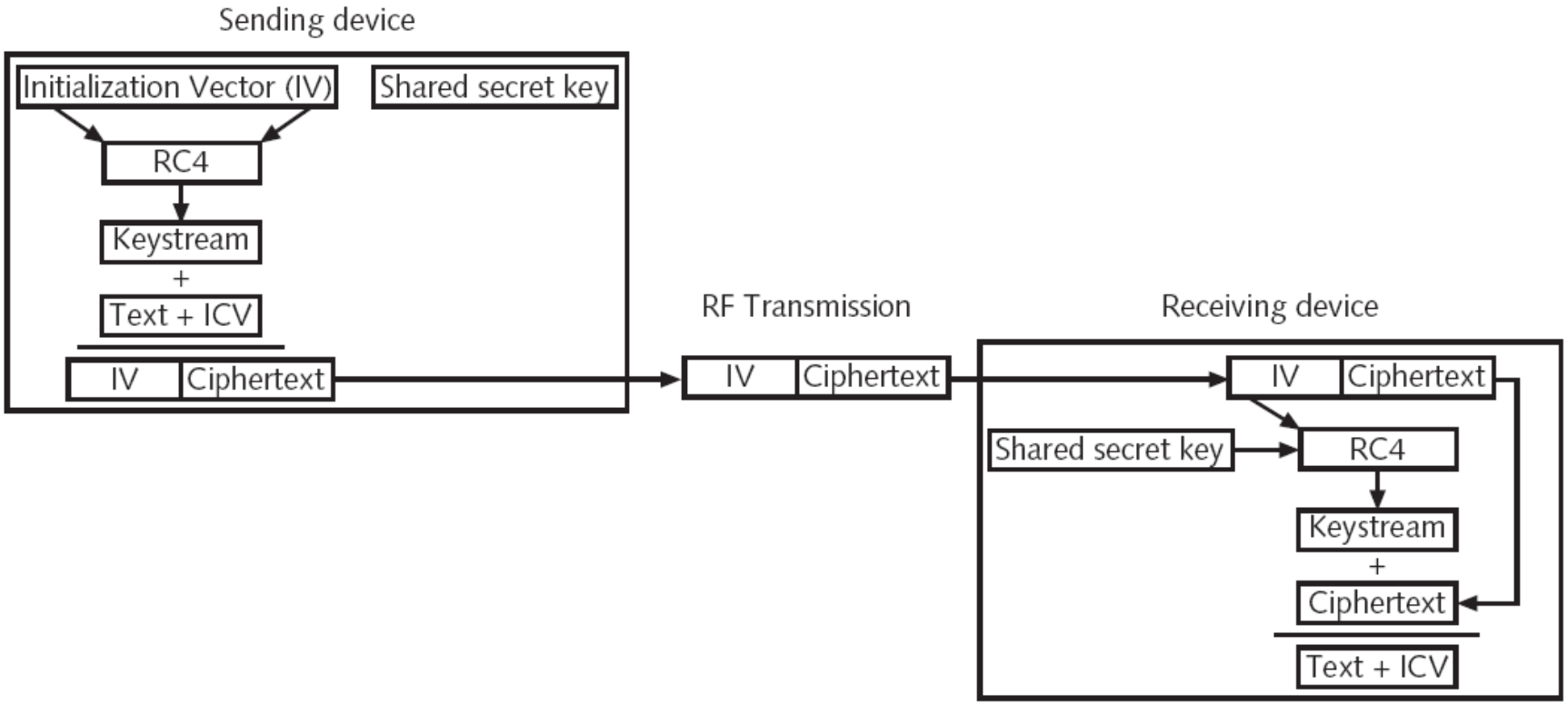


Figure 6-5 Transmitting with WEP

WEB

RC4 trong WEP

- Mã hóa dòng dùng khóa đối xứng
- Mã hóa và giải mã nhanh(10 lần nhan hơn so với DES)

Khóa bí mật k

- Gõ bằng tay
- 40bits/128bits

Vector khởi tạo IV

- Dùng PRG để tạo ra số ngẫu nhiên kích thước 24bits
- Gửi trong phần rõ trước bản mã: (IV+C)
- Khóa mã hóa RC4 độc lập với bản rõ

Dịch vụ bí mật

- Vector khởi tạo(IV) được gởi trong phần rõ của gói tin

- Vì vậy khi nắm bắt được vector khởi tạo và một số lượng gói tin, kẻ tấn công có thể xác định được khóa mã hóa

http://sourceforge.net/projects/wepcrack/

- Tóm lại RC4 không phải là thuật toán yếu nhưng việc hiện thực RC4 trong WEP là thiếu sót và mở dẫn đến bị thỏa hiệp.

Dịch vụ toàn vẹn

- Kiểm tra tính toàn vẹn trên mỗi gói tin.
- Dùng CRC(cyclic redundancy check) của 32 bits.
- CRC được tính toán trên mỗi gói tin trước khi gói tin được mã hóa.
- Dữ liệu và CRC được mã hóa và gởi đến đích.

CRC không phải mật mã an toàn tuy nhiên nó được bảo vệ bằng mã hóa.

- Do khi hiện thực mã hóa, WEP có một số thiếu sót dẫn đến sự toàn vẹn của các gói tin cũng dễ bị thỏa hiệp.

Chi tiết các điểm yếu

- 10/2000: Jesse Walker của Intel đã công bố ”Unsafe at any keysize; An analysis of the WEP encapsulation”

- 03/2001: Scott Fluhrer, Itsik Mantin, Adi Shamir công bố "Attacks on RC4 and WEP“, “Weaknesses in the Key Scheduling Algorithm of RC4“.

Dùng WPA để thay thế cho WEP

Wi-Fi Protected Access (WPA)

- Giải quyết hầu hết các điểm yếu của WEP

Là một tập con của 802.11i, tương thích 802.11i

- Mục tiêu là cải thiện vấn đề mã hóa và xác thực người dùng
- Gồm 2 chế độ hoạt động
  + WPA doanh nghiệp: TKIP/MIC ; 802.1X/EAP
  + WPA cá nhân: TKIP/MIC; PSK

Các chế độ hoạt động WPA

Doanh nghiệp

- Dùng 802.1x/EAP cho xác thực.

Nhà hay văn phòng nhỏ

- Dùng chế độ "Pre-Shared Keys (PSK)".
- Người dùng cung cấp khóa chủ trên mỗi máy tính.
- Khóa chủ kích hoạt TKIP và việc quay vòng khóa.

Chế độ hỗn hợp

- Hoạt động với WEP nếu máy trạm nào không hỗ trợ WPA.

Chế độ WPA doanh nghiệp

Xác thực(IEEE 802.1X/EAP)

- Xác thực lẫn nhau. Vì vậy bạn không bị tham gia các mạng giả mạo và cung cấp các thông tin bí mật của bạn.
- Hỗ trợ nhiều phương thức xác thực như dựa trên mật khẩu, chứng chỉ số.
- Quản lý thông tin người dùng tập trung.

Chế độ WPA doanh nghiệp

Chứng thực từ server

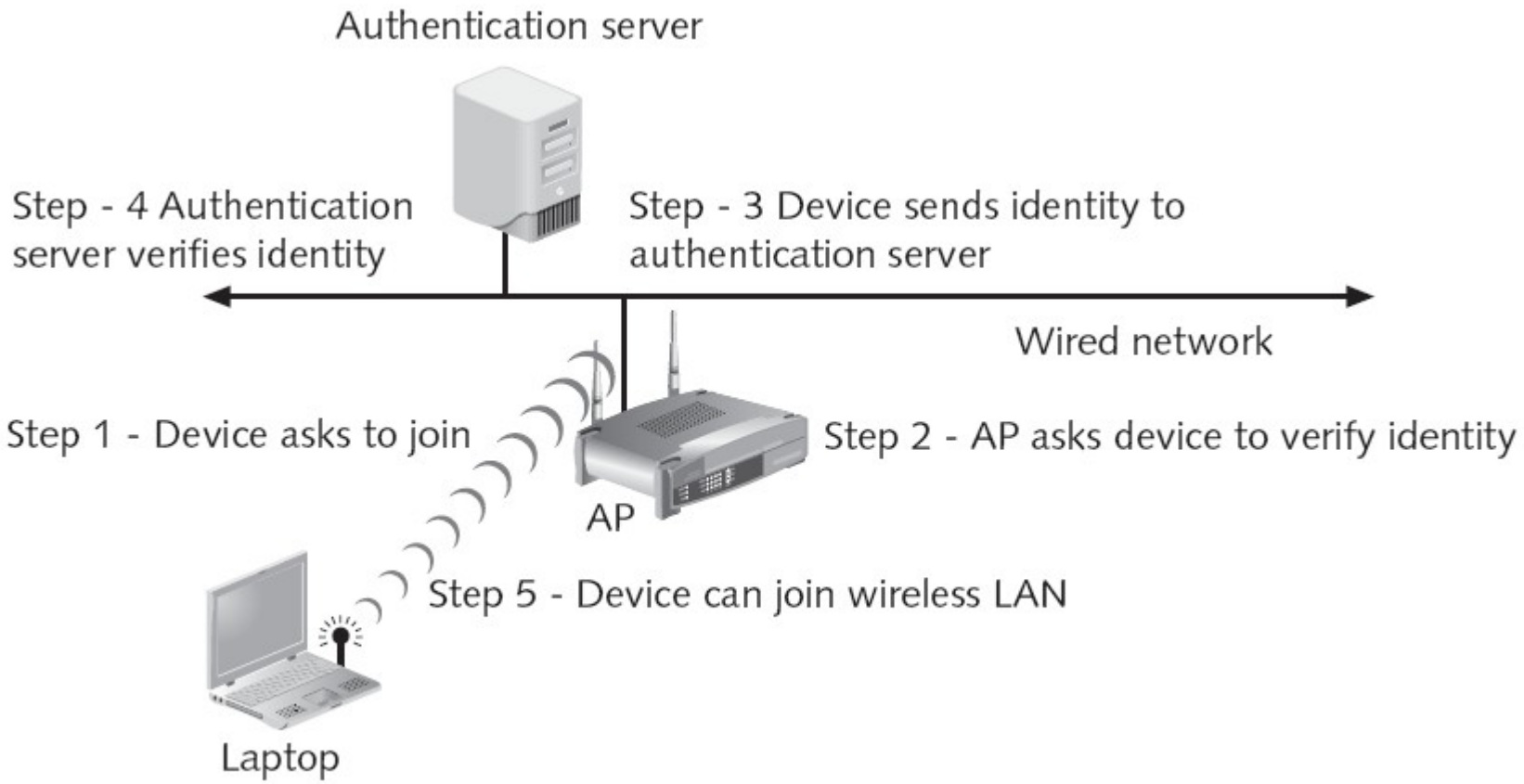
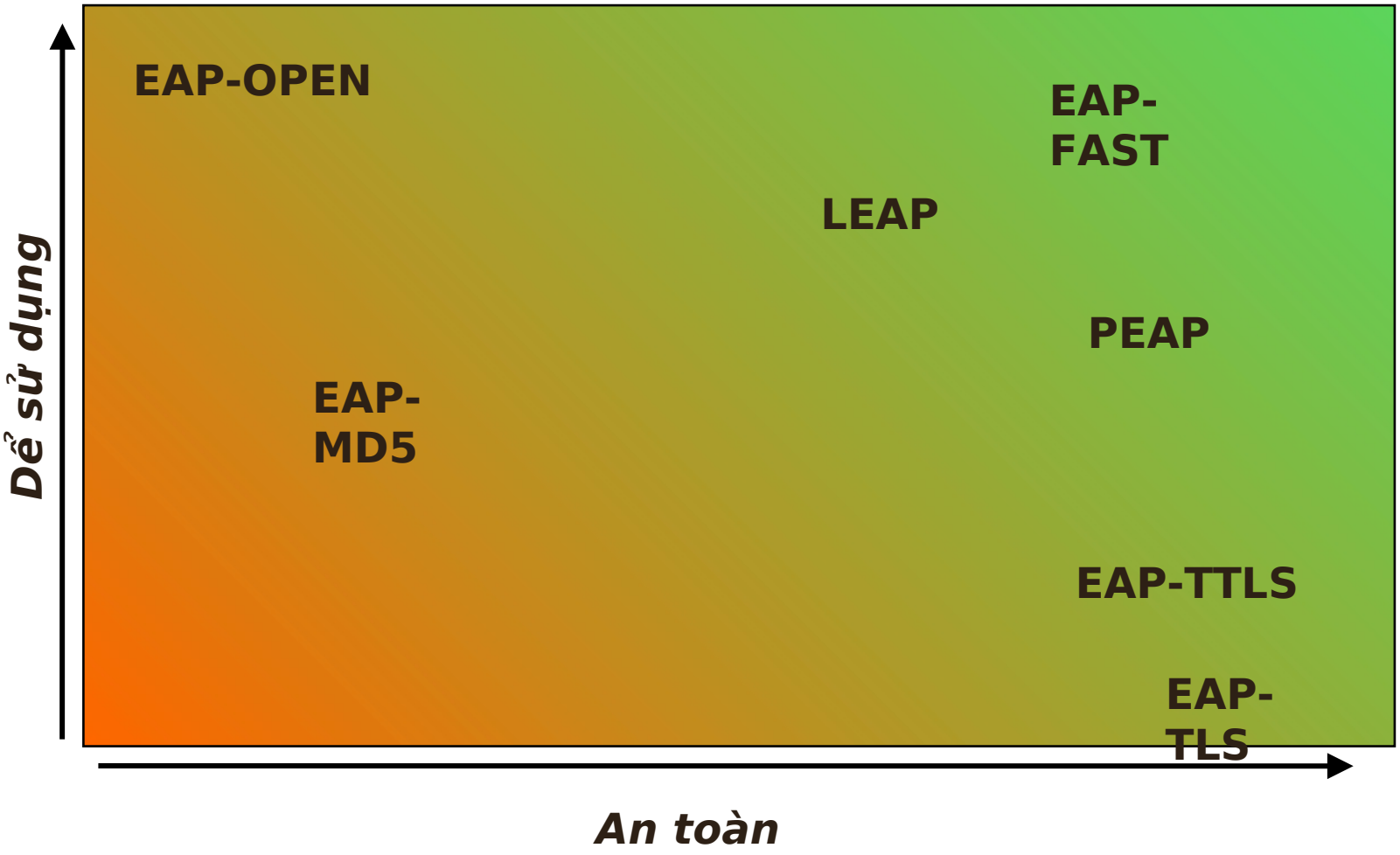


Figure 6-11 IEEE 802.1x

EAP(Extensible Authentication Protocol)

- **Cisco LEAP**
  - Dùng Username/password
  - Dễ bị tổn thương bởi tấn công mật khẩu/ dựa trên bảng băm.
- **EAP-TLS**
  - Xác thực lẫn nhau dùng chứng chỉ X.509
  - Mặc định của 802.11i
- **EAP-TTLS/PEAP**
  - TLS qua đường hầm
  - Không yêu cầu chứng chỉ của client.
- **EAP-GTC**
  - Xác thực dùng mật khẩu một lần
- **EAP-FAST**
  - Client & server có cùng khóa, thiết lập đường hầm an toàn
  - Xác thực xảy ra trên đường hầm an toàn
  - Giống như xác thực VPN

Đánh giá các loại EAP



Chế độ WPA doanh nghiệp

Mã hóa(TKIP/MIC)

TKIP

- Temporal Key Integrity Protocol.
- Sửa lỗi phục hồi khóa trong WEP. Bảo vệ IV bằng cách loại bỏ khả năng dự đoán.
- Sử dụng thuật toán mã hóa RC4 như WEP.
- Thêm MIC ở cuối của mỗi thông điệp bản rõ nhằm đảm bảo thông điệp đó không bị giả mạo.

MIC

- Message Integrity Code.
- Chống lại tấn công bit-flip.
- Phải được hiện thực trên client & AP.

Chế độ WPA doanh nghiệp

Mã hóa (TKIP/MIC)

- Dùng khóa 64 bits
- Chia gói tin thành các khối 32 bits
- Dùng shifts, XORs, + đến mỗi khối 32 bits để lấy ra thẻ xác thực 64 bits
- Khóa MIC được tính toán trên dữ liệu địa chỉ nguồn và địa chỉ đích
- MIC = MIC_key(SA, DA, PlainMSDU)
- Tránh bắt gói, thay đổi và gởi lại các gói tin

Chế độ WPA doanh nghiệp

Mã hóa (TKIP/MIC)

- Mỗi khóa mã hóa trên mỗi gói.
- IV có chiều dài 48bits dẫn đến giảm việc tái sử dụng IV.
- IV mã hóa trước khi gởi.
- MIC thay thế CRC.
- Có thể nâng cấp dể dàng cho phần cứng hỗ trợ WEP.

Chế độ WPA doanh nghiệp

Mã hóa (TKIP)

Authentication (PSK - Pre-shared key)

- Chế độ đặc biệt (không có hạ tầng 802.1x)
- Passphrase được cung cấp trên tất cả máy trạm và các Access Point
- Dựa trên bắt tay khóa bốn lần
  + Hai lần đầu: máy trạm và access point trao đổi các giá trị ngẫu nhiên để xác thực lẫn nhau.
  + Hai lân kế tiếp : access point hướng dẫn máy trạm để cài đặt khóa được tính toán trước. Máy trạm xác nhận.

Các tính năng an ninh cải tiến

WPA2/802.11i

- WPA là một giải pháp tình thế
- WPA2 là chuẩn IEEE 802.11i
- 802.11i dùng khái niệm an ninh mạng mạnh mẽ(RSN -Robust Security Network)
- Khác biệt lớn nhất: AES được dùng cho mã hóa
- Mã hóa AES được thực hiện trong phần cứng

Đòi hỏi bộ xử lý mạnh hơn

Chế độ WPA doanh nghiệp

Doanh nghiệp

- Xác thực dùng 802.1X/EAP
- Mã hóa dùng AES-CCMP

Nhà hay văn phòng nhỏ

- Xác thực dùng PSK
- Mã hóa dùng AES-CCMP

AES-CCMP

- AES là mã hóa khóa đối xứng
- Chiều dài khối và khóa là 128 bits
- CCMP: Counter-Mode/CBC-Mac Protocol
- Mã hóa dùng chế độ Counter
- Toàn vẹn dữ liệu dùng CMC-MAC

So sánh các chuẩn an ninh WLAN

	WEP	WPA	WPA2
Mã hóa	RC4	RC4 với TKIP/ MIC	AES
Quay vòng khóa	Không	Các khóa phiên động	Các khóa phiên động
Phân phối khóa	Gõ bằng tay vào mỗi thiết bị	Phân phối tự động	Phân phối tự động
Xác thực	Dùng khóa WEP	Có thể dùng 802.1x & EAP	Có thể dùng 802.1x & EAP

Kết luận và các khuyến cáo

- An ninh mạng nói chung không phải là một trạng thái mà là một tiến trình.

- Các khuyến cáo cho an ninh WLAN

+ Dùng thiết bị tương thích và có chứng nhận Wi-Fi

+ Thay đổi SSID và không quảng bá SSID

+ Cấu hình lọc địa chỉ MAC nếu bạn quản lý được người dùng và các Access Point

+ Cấu hình WEP với khóa có chiều 128 bits và thay đổi khóa WEP thường xuyên nếu không thể nâng cấp firmware hỗ trợ WPA/WPA2

+ Nâng cấp firmware để cấu hình WPA/WPA2 và dùng 802.1x/EAP để xác thực người dùngS