An ninh mạng LAN không dây (IEEE 802.11)

Giáo viên: Nguyễn Hiếu Minh

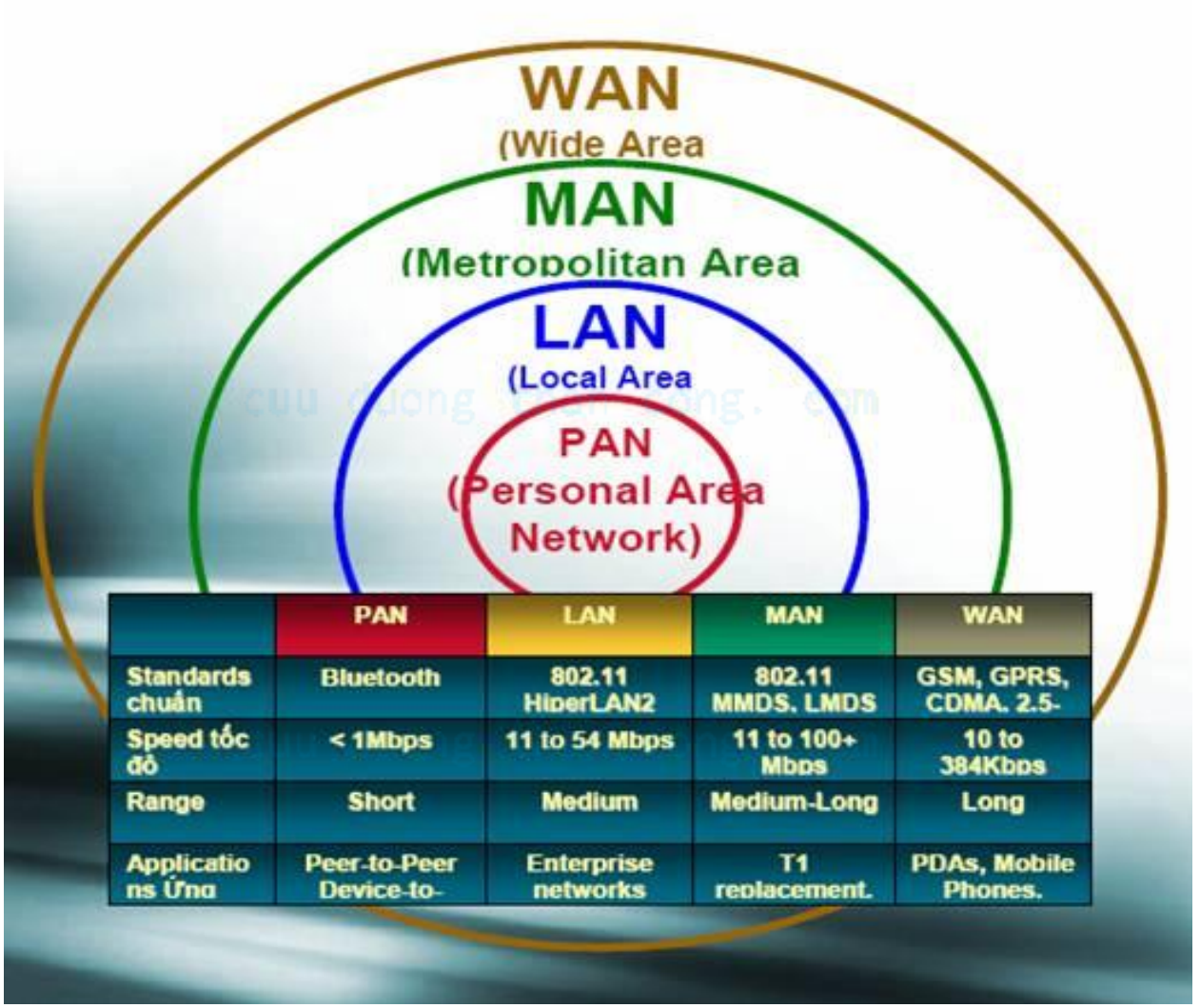
Các nội dung trình bày

1. Công nghệ WLAN
2. An ninh trong WLAN
3. Giao thức WEP
4. Giao thức WPA/WPA2

1. Công nghệ WLAN

- Năm 1985, Ủy ban liên lạc liên bang Mỹ FCC (*Federal Communications Commission*), quyết định "mở cửa" một số băng tần của giải sóng vô tuyến, cho phép sử dụng chúng mà không cần giấy phép của chính phủ.
- FCC đã đồng ý "thả" 3 giải sóng công nghiệp, khoa học và y tế cho giới kinh doanh viễn thông.
- Ba giải sóng này, gọi là các "băng tần rác" (*garbage bands* – 900 MHz, 2,4 GHz, 5,8 GHz), được phân bổ cho các thiết bị sử dụng vào các mục đích ngoài liên lạc.

Vai trò và vị trí của WLAN



	PAN	LAN	MAN	WAN
Standards chuẩn	Bluetooth	802.11 HiperLAN2	802.11 MMDS, LMDS	GSM, GPRS, CDMA, 2.5-
Speed tốc độ	< 1Mbps	11 to 54 Mbps	11 to 100+ Mbps	10 to 384Kbps
Range	Short	Medium	Medium-Long	Long
Applications Ứng	Peer-to-Peer Device-to-	Enterprise networks	T1 replacement.	PDAs, Mobile Phones.

Các chuẩn WLAN

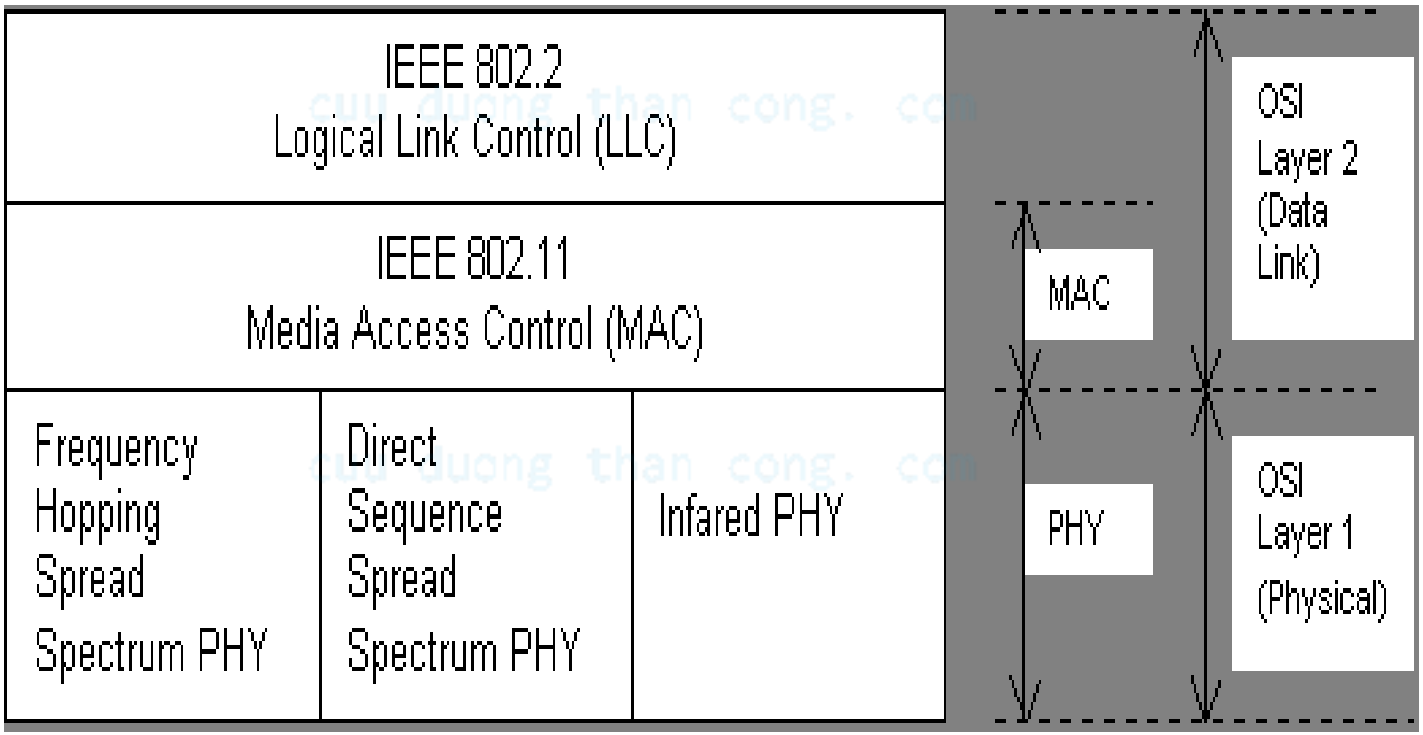
- Chuẩn IEEE 802.11 chính thức được ban hành năm 1997.
- IEEE 802.11 (chuẩn WiFi) biểu thị một tập hợp các chuẩn WLAN được phát triển bởi ủy ban chuẩn hóa IEEE LAN/MAN (IEEE 802.11).
- Thuật ngữ 802.11x có thể được sử dụng để biểu thị một tập hợp các chuẩn đối với tất cả các chuẩn thành phần của nó.
- IEEE 802.11 có thể được sử dụng để biểu thị chuẩn 802.11, đôi khi được gọi là 802.11 gốc (*802.11 legacy*).

- Sau đó 2 chuẩn, IEEE 802.11a (băng tần 5,8 GHz) và IEEE 802.11b (băng tần 2,4 GHz), lần lượt được phê duyệt tháng 12/1999 và tháng 1/2000.
- Sau khi có chuẩn 802.11b, các công ty bắt đầu phát triển những thiết bị tương thích với nó.

- Có 6 công ty bao gồm Intersil, 3Com, Nokia, Aironet, Symbol và Lucent liên kết với nhau để tạo ra Liên minh tương thích Ethernet không dây WECA (*The Wireless Ethernet Compatibility Alliance*).
- Mục tiêu hoạt động của tổ chức WECA là xác nhận sản phẩm của những nhà cung cấp phải tương thích thực sự với nhau.

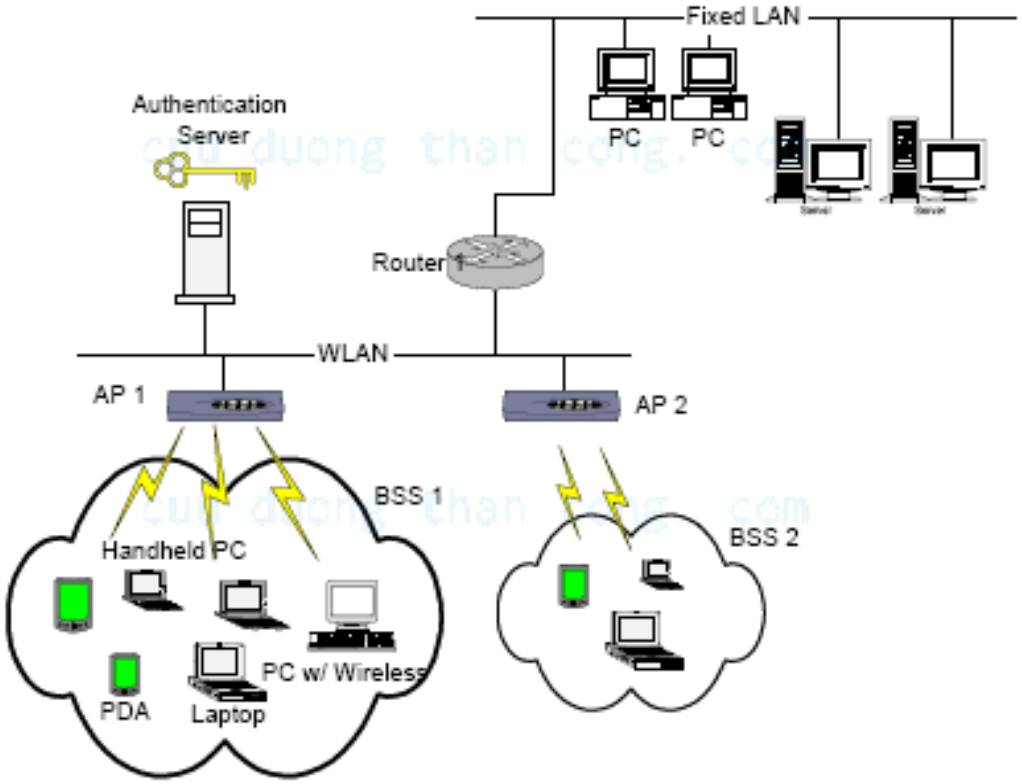
Quan hệ giữa IEEE 802.11 và OSI

- IEEE 802.11 là chuẩn đặc tả mạng cục bộ không dây, sử dụng phương pháp truy nhập CSMA/CA.



Cấu trúc WLAN

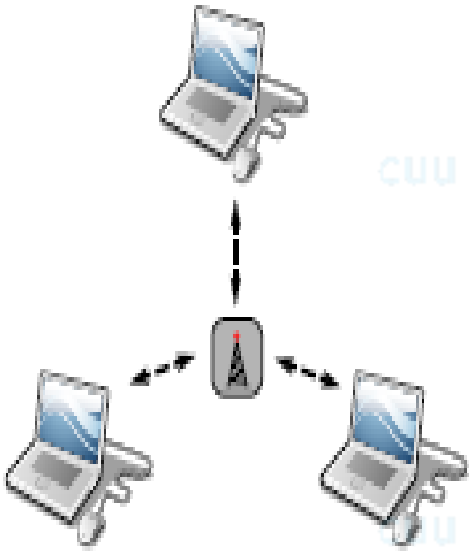
- Một WLAN thông thường gồm có 2 phần: các thiết bị truy nhập không dây (*Wireless Clients*), các điểm truy nhập (*Access Points – AP*).

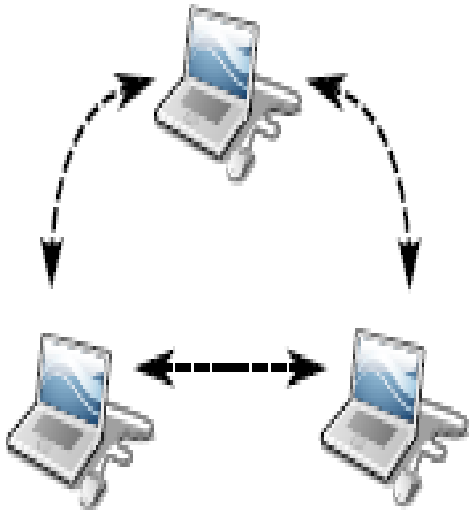


Chuẩn IEEE 802.11 và hạ tầng

- Có hai loại mạng không dây cơ bản:
- *Kiểu Ad-hoc*: Mỗi máy trong mạng giao tiếp trực tiếp với nhau thông qua các thiết bị không dây mà không dùng đến các thiết bị định tuyến (*Wireless Router)* hay thu phát không dây (*Wireless Access Point*).
- *Kiểu Infrastructure*: Các máy trong mạng sử dụng một hoặc nhiều thiết bị định tuyến hay thiết bị thu phát để thực hiện các hoạt động trao đổi dữ liệu với nhau.

Các chế độ hoạt động
(a, Infrastructure; b, Ad-hoc)





Các chuẩn an ninh hỗ trợ IEEE 802.11

- IEEE 802.11 (WEP)
- IEEE 802.1X
- Wi-Fi Protected Access (WPA)
- Wi-Fi Protected Access 2 (WPA2)

Chuẩn an ninh	Các phương pháp xác thực	Các phương pháp mã hóa	Kích thước khóa mã (bit)	Giải thích
IEEE 802.11	Hệ thống mở và khóa chia xẻ	WEP	40 và 104	Xác thực và mã hóa yếu
IEEE 802.1x	Các phương pháp xác thực EAP	N/A	N/A	EAP cung cấp khả năng xác thực mạnh
WPA–Enterprise	802.1X	TKIP/AES (Tùy chọn)	128	Xác thực mạnh, TKIP/AES.
WPA–Personal	PSK	TKIP/AES (Tùy chọn)	128	
WPA2–Enterprise	802.1X	TKIP và AES	128	
WPA2–Personal	PSK	TKIP và AES	128	

2. An ninh trong WLAN

- *Tại sao an toàn thông tin trong WLAN lại rất quan trọng?*

Điều này bắt nguồn từ tính cố hữu của môi trường không dây. Sóng vô tuyến có thể xuất hiện trên đường phố, từ các trạm phát của các mạng LAN này, và như vậy ai cũng có thể truy cập nhờ thiết bị thích hợp.

Các dịch vụ an ninh trong IEEE 802.11

- Ba dịch vụ an ninh cơ bản:

- **Sự xác thực**: Cung cấp khả năng điều khiển truy nhập tới mạng nhờ ngăn cấm truy nhập đối với các thiết bị được xác nhận không hợp lệ. Dịch vụ này hướng đến vấn đề – chỉ những người dùng hợp lệ mới được phép truy nhập tới mạng?
- **Tính bí mật (hoặc tính riêng tư)**: Mục tiêu của nó nhằm ngăn chặn việc đọc thông tin từ các đối tượng phi pháp. Dịch vụ này hướng đến vấn đề – chỉ những người dùng hợp lệ mới được phép đọc thông tin của mình?

- **Tính toàn vẹn**: Được phát triển nhằm mục đích đảm bảo cho các bản tin không bị sửa đổi khi truyền giữa các trạm và các điểm truy nhập. Dịch vụ này hướng đến vấn đề – thông tin trong mạng là đáng tin cậy hay nó đã bị giả mạo?
- Các dịch vụ trên chỉ ra rằng chuẩn IEEE 802.11 không đề cập đến các dịch vụ an ninh khác như kiểm toán, cấp quyền, và chống từ chối.

Các phương pháp thực hiện các dịch vụ

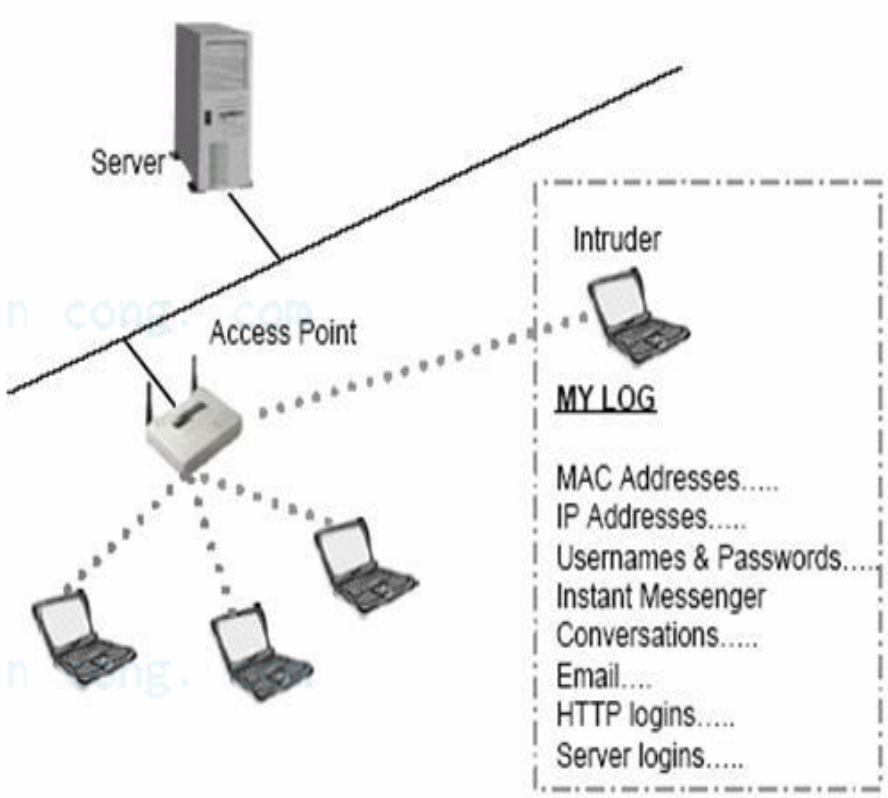
- **SSID** (*Services Set Identifier*): Là cách thức dùng để phân biệt các mạng khác nhau từ một thực thể. Khởi điểm các điểm truy nhập (*AP*) được xác lập các SSID mặc định bởi nhà sản xuất. Mặc định khi hoạt động các điểm truy cập sẽ quảng bá các SSID (sau mỗi vài giây) trong các '*Beacon Frames*'.
- **Xác thực**: Trước khi có thể thực hiện bất kỳ một phiên liên lạc nào giữa một trạm làm việc và điểm truy nhập, chúng phải thực hiện một hội thoại (*dialogue*). Quá trình này được thực hiện như một sự kết hợp giữa các thực thể.
- **WEP** (*Wired Equivalent Privacy*): Được thiết kế với mục đích bảo đảm cho những người sử dụng mức độ an toàn tương đương với mạng không dây.

Các kiểu tấn công trên WLAN

- Một số kiểu tấn công chủ yếu:
  - Tấn công bị động (nghe trộm – *Passive attacks*).
  - Tấn công chủ động (kết nối, dò và cấu hình mạng – *Active attacks*).
  - Tấn công kiểu chèn ép (*Jamming attacks*).
  - Tấn công theo kiểu thu hút (*Man–in-the-middle attacks*).
  - Tấn công lặp lại (*Replay attacks*).

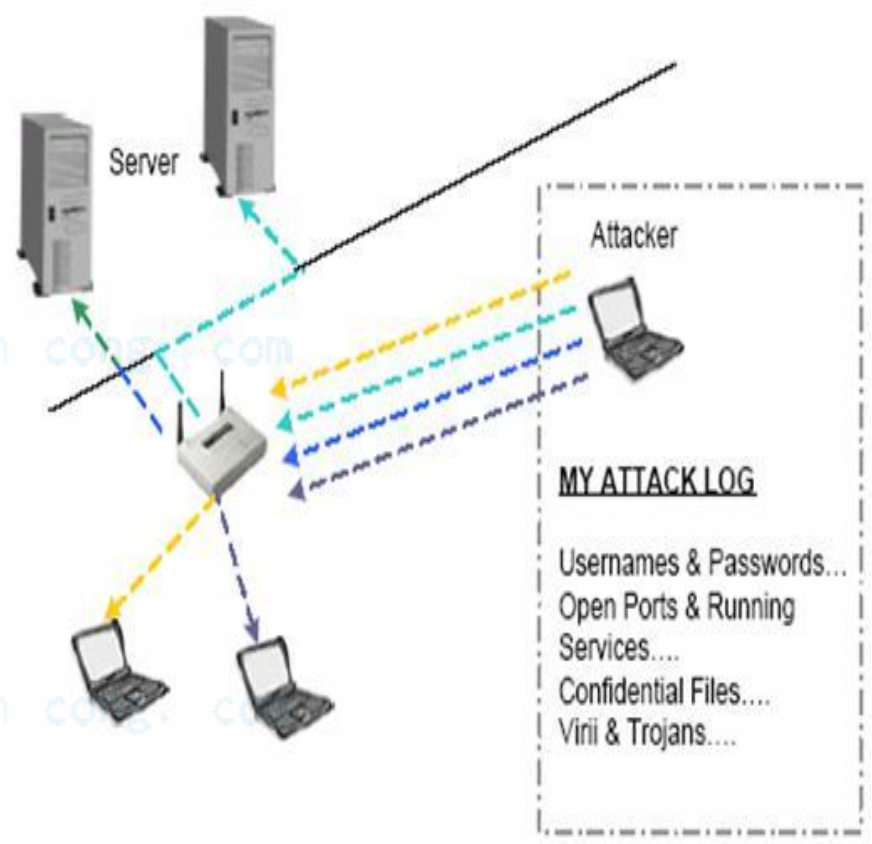
Tấn công bị động

- Tấn công bị động thực hiện như một cuộc nghe trộm.
- Những thiết bị phân tích mạng hoặc những ứng dụng khác được sử dụng để lấy thông tin của WLAN từ một khoảng cách với một anten hướng tính.

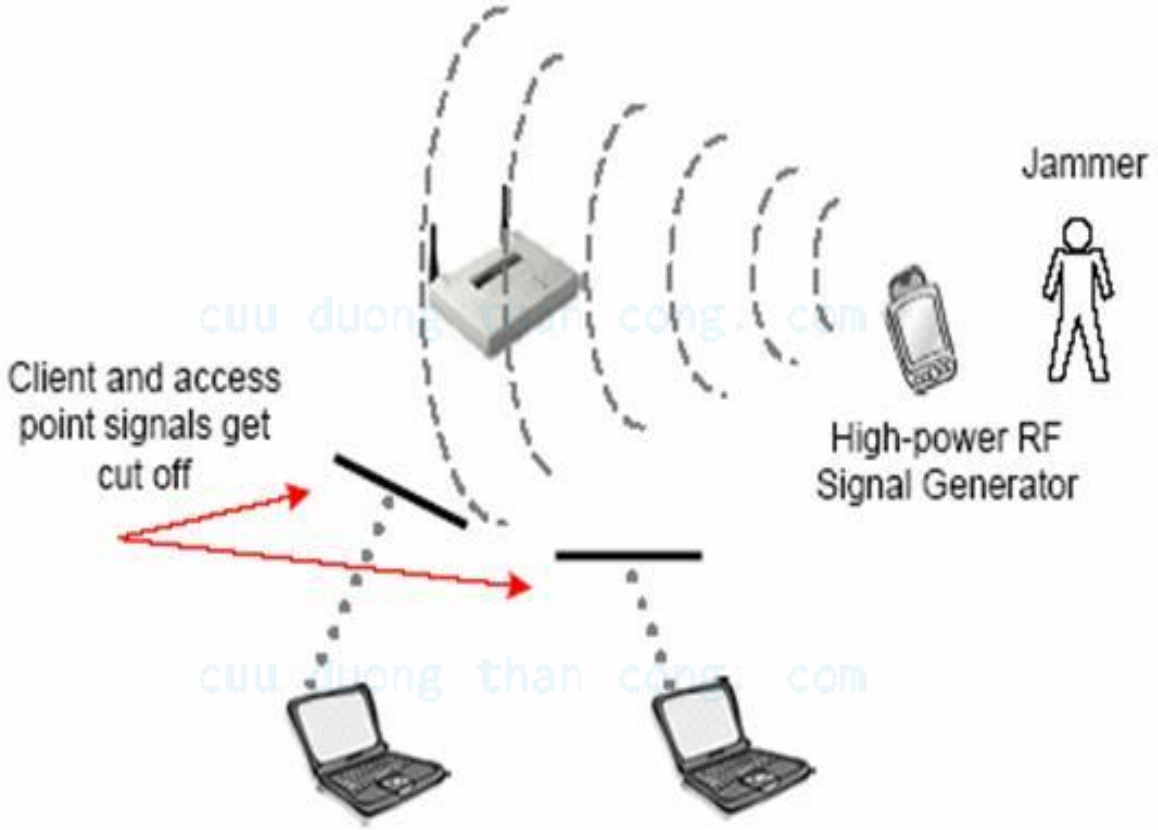


Tấn công chủ động

- Một tấn công chủ động có thể được dùng để tìm cách truy nhập tới một server để lấy những dữ liệu quan trọng, thậm chí thay đổi cấu hình cơ sở hạ tầng mạng.



Tấn công theo kiểu chèn ép



3. Giao thức WEP

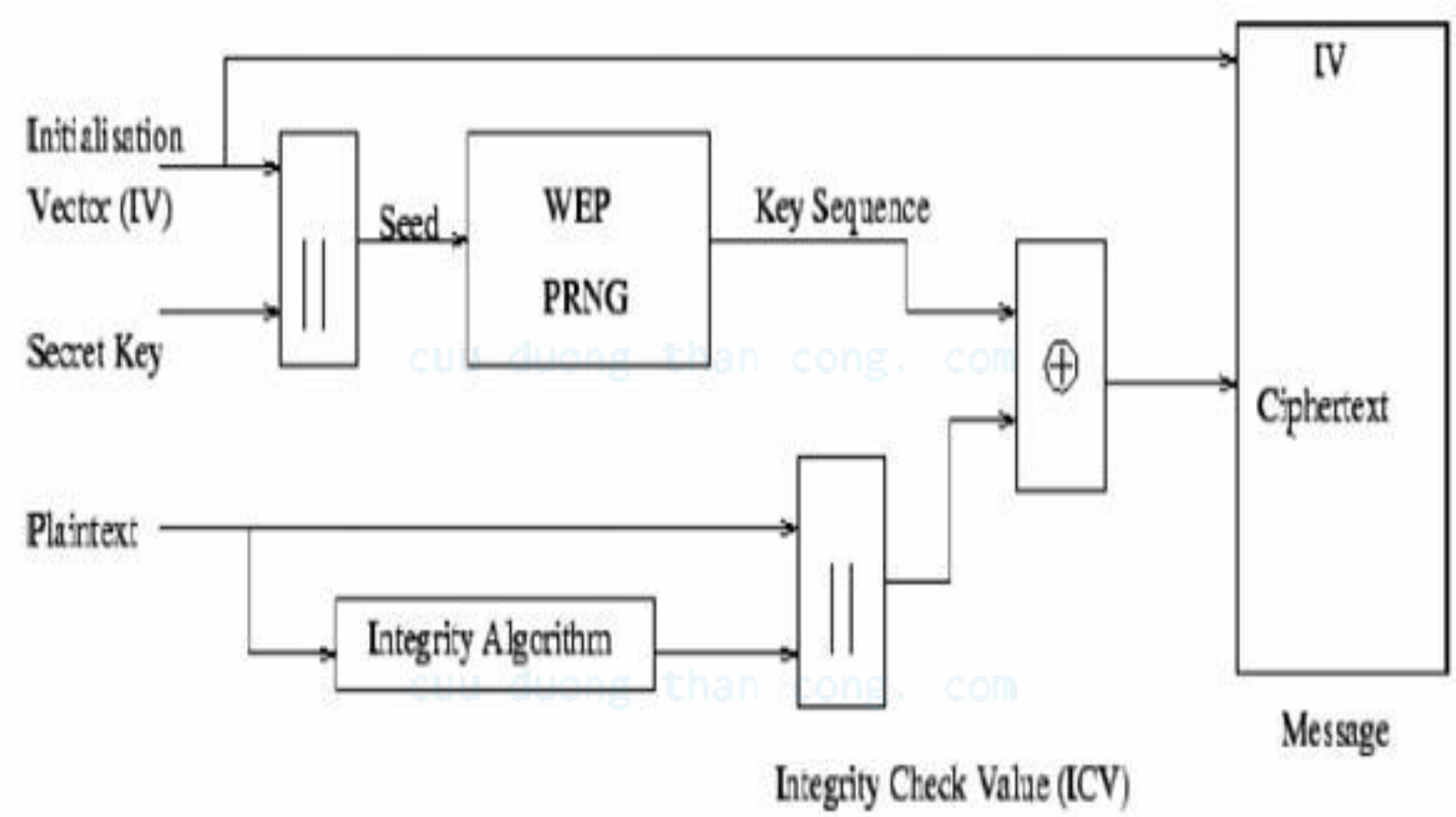
- Giao thức WEP được sử dụng trong các mạng IEEE 802.11 nhằm mục đích bảo vệ dữ liệu trong truyền dẫn không dây (mức liên kết).
- Theo định nghĩa, WEP được thiết kế để đảm bảo tính bảo mật cho mạng không dây đạt mức độ như mạng cáp truyền thống.

- Đối với mạng LAN (chuẩn IEEE 802.3), bảo mật dữ liệu trên đường truyền đối với các tấn công bên ngoài được đảm bảo qua biện pháp giới hạn vật lý, tức là hacker không thể truy xuất trực tiếp đến hệ thống đường truyền cáp. Do đó chuẩn 802.3 không đặt ra vấn đề mã hóa dữ liệu để chống lại các truy cập trái phép.
- Đối với chuẩn 802.11, vấn đề mã hóa dữ liệu được ưu tiên hàng đầu do đặc tính của mạng không dây là không thể giới hạn về mặt vật lý truy cập đến đường truyền, bất cứ ai trong vùng phủ sóng đều có thể truy cập dữ liệu nếu không được bảo vệ.

- WEP là một phương pháp mã hoá dữ liệu được thực hiện tại lớp điều khiển truy cập (*Media Access Control – MAC*).
- Phương pháp này sử dụng thuật toán mã hoá RC4 (*IV, k*) với một véc tơ *IV* có thể thay đổi được và một khoá *k* không thay đổi, được gán trước trong các máy trạm và các AP.
- Phương pháp này còn sử dụng một tổng kiểm tra CRC để xác thực bản tin.

- Trong vài năm đầu, thuật toán này được bảo mật và không sẵn có, tháng 9 năm 1994, một vài người đã đưa mã nguồn của nó lên mạng.
- Mặc dù bây giờ mã nguồn là sẵn có, nhưng RC4 vẫn được đăng ký bởi RSADSI.
- RC4 mã hóa và giải mã rất nhanh, nó rất dễ thực hiện, và đủ đơn giản để các nhà phát triển phần mềm có thể dùng nó để mã hóa các phần mềm của mình.

Sơ đồ quá trình mã hóa sử dụng WEP



Mô tả

- WEP dựa trên một khóa bí mật *k* được chia xẻ giữa các bên truyền thông để bảo vệ dữ liệu truyền.
- Mã hóa của 1 khung (*frame*) dữ liệu được thực hiện như sau:
- **Tính tổng kiểm tra**: Một tổng kiểm tra của bản tin cần mã hoá *M* (tổng kiểm tra được tính theo CRC) được tính và kí hiệu là *c*(*M*). Rồi kết hợp *c*(*M*) và *M* lại với nhau để tạo thành bản rõ (kí hiệu là *P* = (*M*, *c*(*M*)), *P* được dùng làm đầu vào cho giai đoạn thứ hai. Chú ý rằng, *c*(*M*) và *P* không phụ thuộc vào khoá *k*.

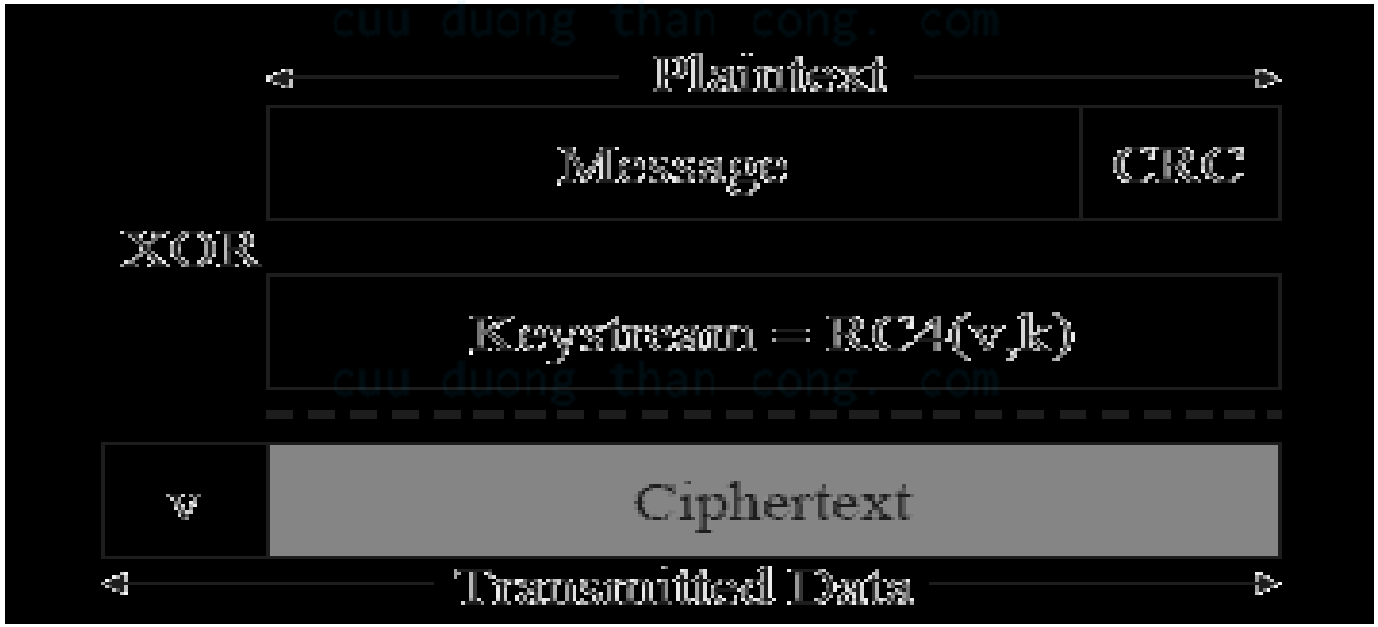
- **Mã hóa**: Tiếp theo bản rõ *P* được mã hoá sử dụng thuật toán mã hoá RC4.
- Một véc tơ khởi tạo (*IV*) *v* có thể thay đổi và một khoá *k* không đổi được chọn. Thuật toán RC4 sinh ra một khoá dòng (*keystream* – là một chuỗi dài các byte giả ngẫu nhiên, chúng là hàm của *v* và *k*). Dòng khoá được kí hiệu là RC4 (*v*, *k*) có độ dài bằng *P*.
- Sau đó bản rõ *P* và dòng khóa RC4 (*v*, *k*) được cộng mô đun hai (XOR hoặc $\oplus$) với nhau tạo nên bản mã (*ciphertext*), kí hiệu là *C* và

$$C = P \oplus \text{RC4}(v, k).$$

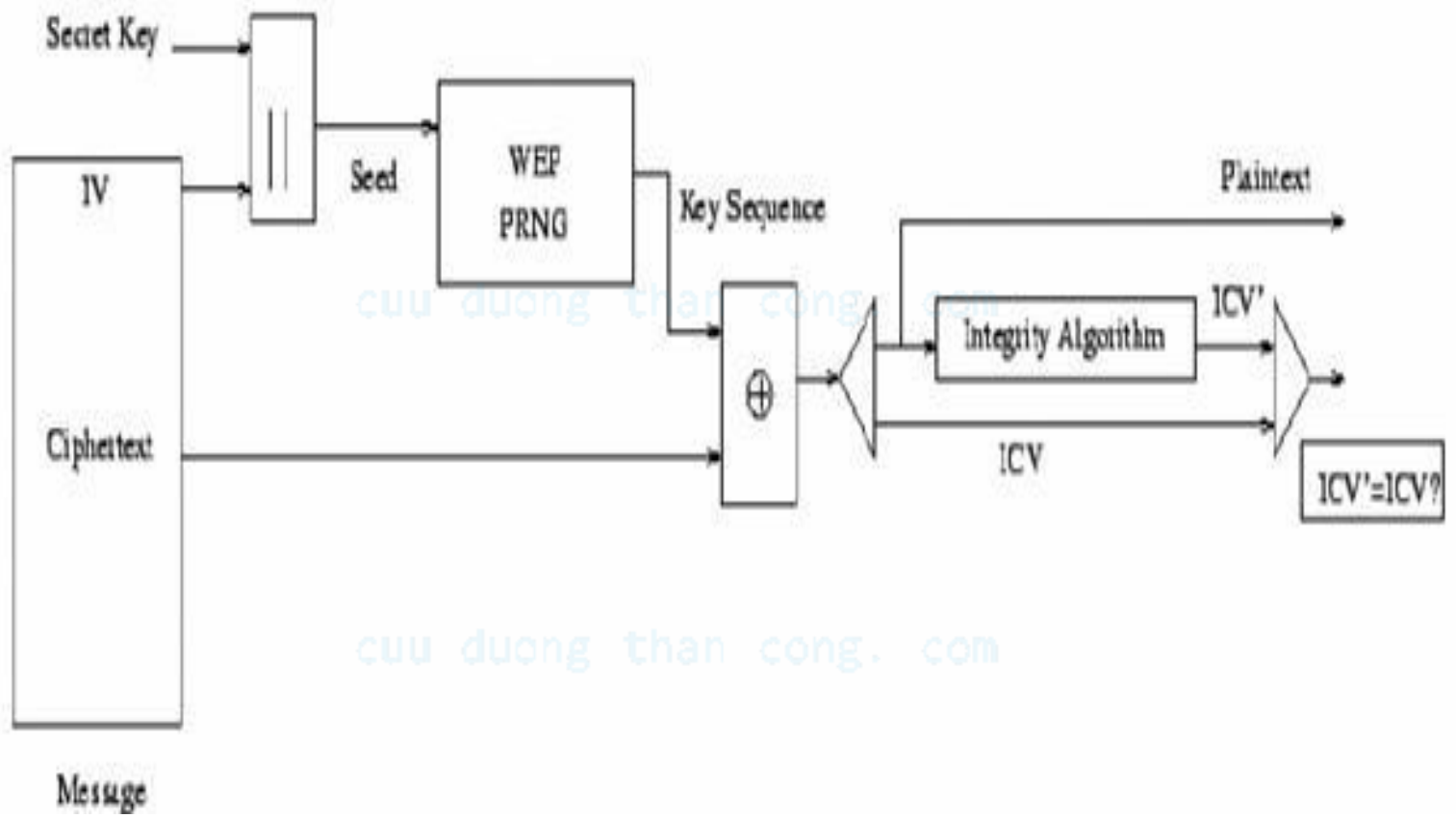
- **Truyền tin**: Cuối cùng, véc tơ khởi tạo *v* và bản mã *C* được truyền vào môi trường vô tuyến. Điều này có thể được biểu diễn như sau:

$$A \rightarrow B: v, (P \oplus RC4(v, k)).$$

Dạng của khung dữ liệu được mã hóa chỉ ra trên hình sau:



Sơ đồ quá trình giải mã sử dụng WEP



- Trước tiên, thực hiện việc XOR dòng khóa RC4 (*v*, *k*) và bản mã *C* để nhận được bản rõ P'.
- Tiếp theo bản rõ *P'* được kiểm tra xem có trùng với bản rõ P không, bằng cách chia *P'* thành dạng *P'* = (*M'*, *c'*(*M*)) và tính tổng kiểm tra của bản tin *M'*, và so sánh nó với tổng kiểm tra *c'*(*M*). Điều này sẽ đảm bảo rằng chỉ các khung dữ liệu với giá trị tổng kiểm tra hợp lệ mới được chấp nhận bởi người nhận.

Các rủi ro và các biện pháp đối phó trên giao thức WEP

- **Các nguy cơ rủi ro:**

  Sử dụng các khóa WEP tĩnh (*static WEP keys*) để chia xẻ khóa định danh trong một thời gian dài gây ra nguy cơ bị lộ khóa.

- ✓ Điều này bởi vì các giao thức WEP không cung cấp sự quản lý khóa dự phòng vì vậy trong trường hợp một máy tính bị hack (hoặc mất) sẽ gây tổn hại đến tất cả các máy tính khác có sử dụng khóa này.
- ✓ Thêm nữa, nếu mọi trạm trong mạng sử dụng cùng khóa thì số lượng các gói dữ liệu khóa sẽ tăng lên rất nhanh và đó chính là điều kiện thuận lợi cho phép các hacker thực hiện các tấn công trên khóa.

- Do WEP sử dụng RC4, một thuật toán sử dụng phương thức mã hóa dòng (*stream cipher*), nên cần một cơ chế đảm bảo hai dữ liệu giống nhau sẽ không cho kết quả giống nhau sau khi được mã hóa hai lần khác nhau. Đây là một yếu tố quan trọng trong vấn đề mã hóa dữ liệu nhằm hạn chế khả năng suy đoán khóa của hacker.
- Để đạt mục đích trên, một giá trị véctơ khởi tạo (*Initialization Vector – IV*) được sử dụng để cộng thêm với khóa nhằm tạo ra khóa khác nhau mỗi lần mã hóa.
- *IV* là một giá trị có chiều dài 24 bit và được chuẩn IEEE 802.11 đề nghị (không bắt buộc) phải thay đổi theo từng gói dữ liệu. Vì máy gửi tạo ra *IV* không theo định luật hay tiêu chuẩn, *IV* bắt buộc phải được gửi đến máy nhận ở dạng không mã hóa.
- Cách sử dụng giá trị *IV* là nguồn gốc của đa số các vấn đề với WEP.

✓Do giá trị *IV* được truyền đi ở dạng không mã hóa và đặt trong phần đầu (*header*) của gói dữ liệu 802.11 nên bất cứ ai "tóm được" dữ liệu trên mạng đều có thể thấy được. Với độ dài 24 bit, giá trị của *IV* dao động trong khoảng 16.777.216 trường hợp.

✓Những chuyên gia bảo mật tại đại học California-Berkeley đã phát hiện ra là khi cùng giá trị *IV* được sử dụng với cùng khóa trên một gói dữ liệu mã hóa (khái niệm này được gọi nôm na là va chạm *IV*), hacker có thể bắt gói dữ liệu và tìm ra được khóa WEP.

- *IV* là một phần của khóa mã RC4, nên trên thực tế khi một hacker biết được 24 bit của mỗi gói dữ liệu khóa và kết hợp với các điểm yếu trong thời gian biểu sử dụng khóa sẽ cho phép thực hiện các tấn công phân tích thành công chỉ sau khi thu và phân tích một số lượng nhỏ các gói dữ liệu thu được.
- Tấn công kiểu này đã được công bố mở trên thực tế và thực hiện dưới dạng mã nguồn mở.

- WEP không cung cấp khả năng bảo vệ tính toàn vẹn bằng mật mã.
- Tuy nhiên 802.11 MAC cung cấp một cơ chế (*Cyclic Redundancy Check – CRC*) để kiểm tra tính toàn vẹn của các gói dữ liệu và các gói được xác nhận với tổng kiểm tra đúng.
- Sự kết hợp giữa các kiểm tra không bằng các thuật toán mật mã kết hợp các khóa dòng là một giải pháp rất không an toàn.

Tại sao WEP được lựa chọn?

- Chuẩn 802.11 đưa ra các tiêu chuẩn cho một vấn đề để được gọi là bảo mật, đó là:

✓ Có thể xuất khẩu.

✓ Đủ mạnh.

✓ Khả năng tương thích.

✓ Khả năng ước tính được.

✓ Tùy chọn, không bắt buộc.

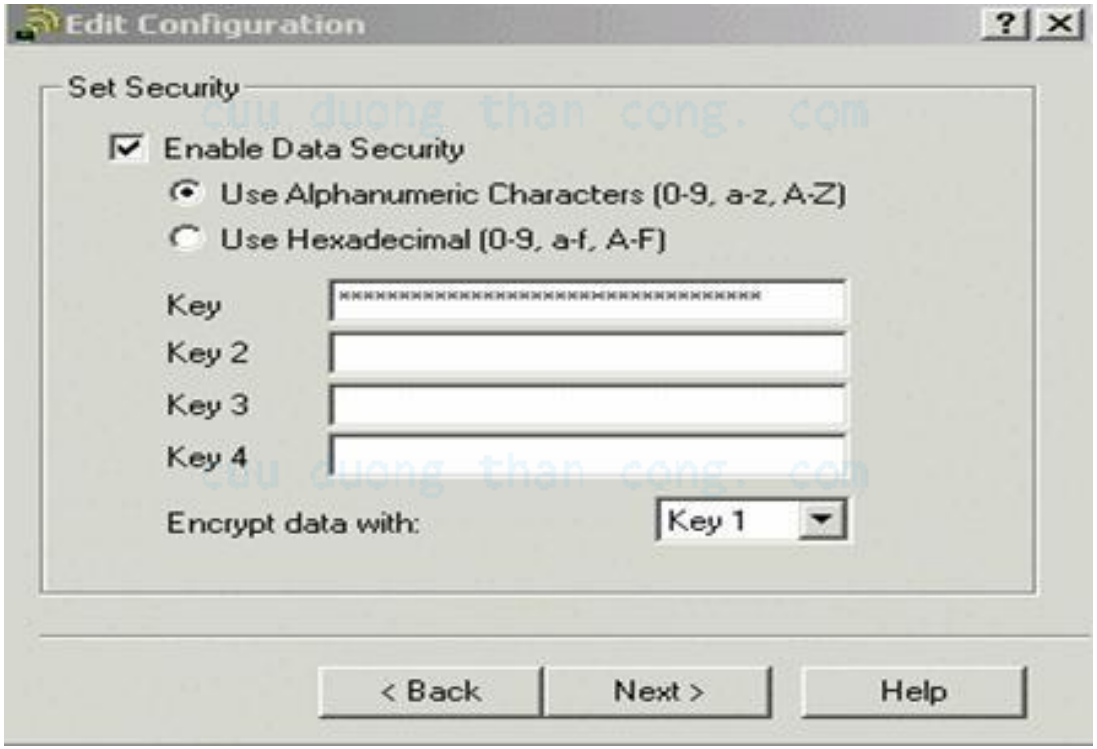
WEP hội tụ đủ các yếu tố này, khi được đưa vào để thực hiện, WEP hỗ trợ bảo mật cho mục đích tin cậy, điều khiển truy nhập, và toàn vẹn dữ liệu.

Các biện pháp đối phó

- Vấn đề cốt lõi của WEP là khóa WEP (*WEP key*). Khóa WEP là một chuỗi ký tự chữ cái và số, được sử dụng cho hai mục đích trong WLAN:
- Khóa WEP được sử dụng để xác định sự cho phép (xác thực) của một trạm làm việc;
- Khóa WEP dùng để mã hóa dữ liệu.

Giao diện nhập khóa WEP

- Có thể phân phối khóa WEP bằng tay hoặc sử dụng một phương pháp tiên tiến khác.
- Hệ thống phân bố khóa WEP có thể đơn giản như sự thực hiện khóa tĩnh, hoặc tiên tiến sử dụng Server quản lí khóa tập trung.



Quản lý khóa mã hóa tập trung

- Với những mạng WLAN quy mô lớn sử dụng WEP như một phương pháp bảo mật căn bản, server quản lý khóa mã hóa tập trung nên được sử dụng vì những lí do sau:

✓ Quản lí sinh khóa tập trung.

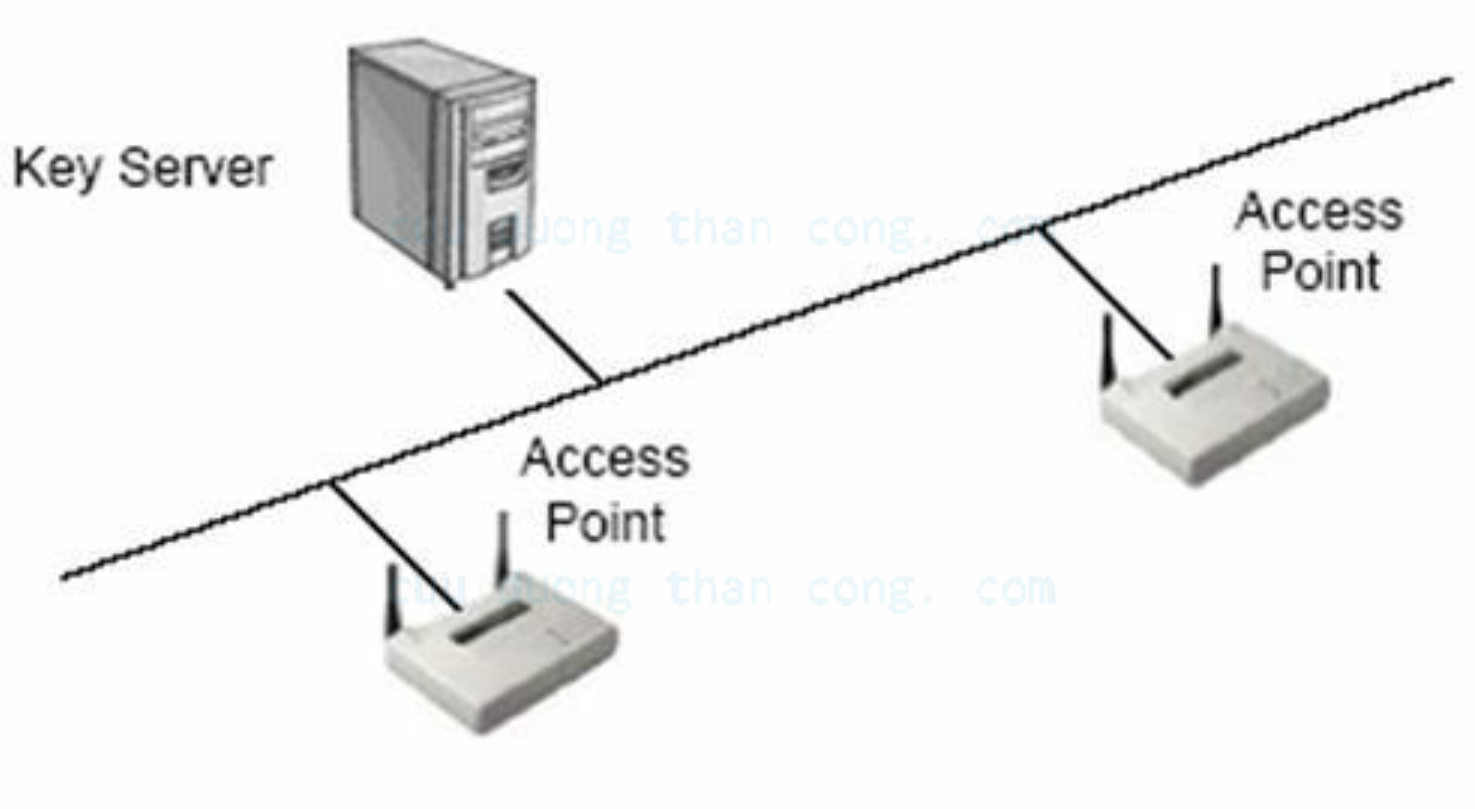
✓ Quản lí việc phân bố khóa một cách tập trung.

✓ Thay đổi khóa luân phiên.

✓ Giảm bớt công việc cho admin.

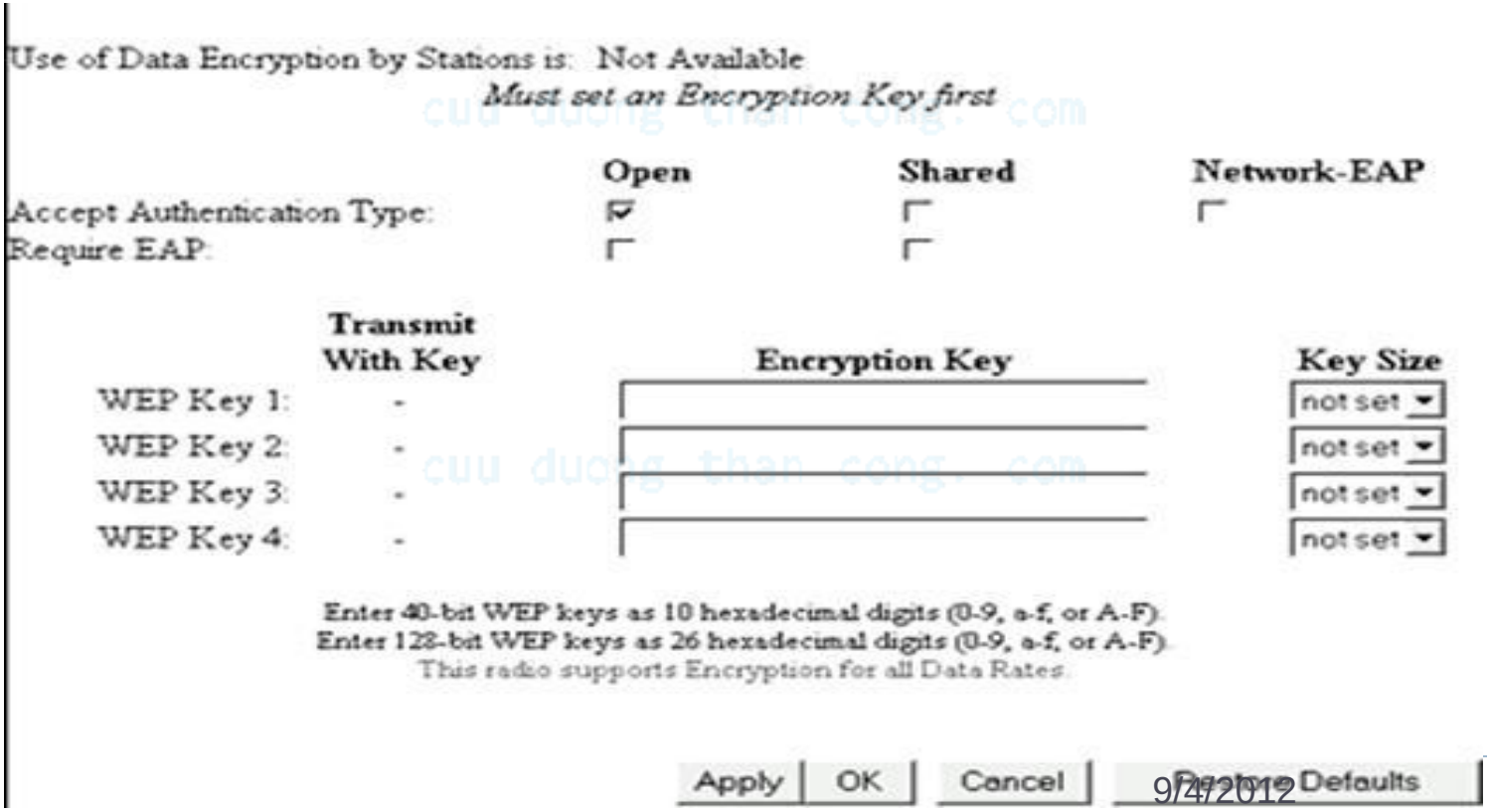
- Thay vì sử dụng khóa WEP tĩnh, mà có thể dễ dàng bị phát hiện bởi hacker. WLAN có thể được bảo mật hơn bởi việc thực hiện các khóa trên từng phiên, sử dụng một hệ thống phân phối khóa tập trung.

- Server quản lý khóa mã hóa tập trung cho phép sinh khóa trên mỗi gói, mỗi phiên, hoặc các phương pháp khác, phụ thuộc vào sự thực hiện của các nhà sản xuất.



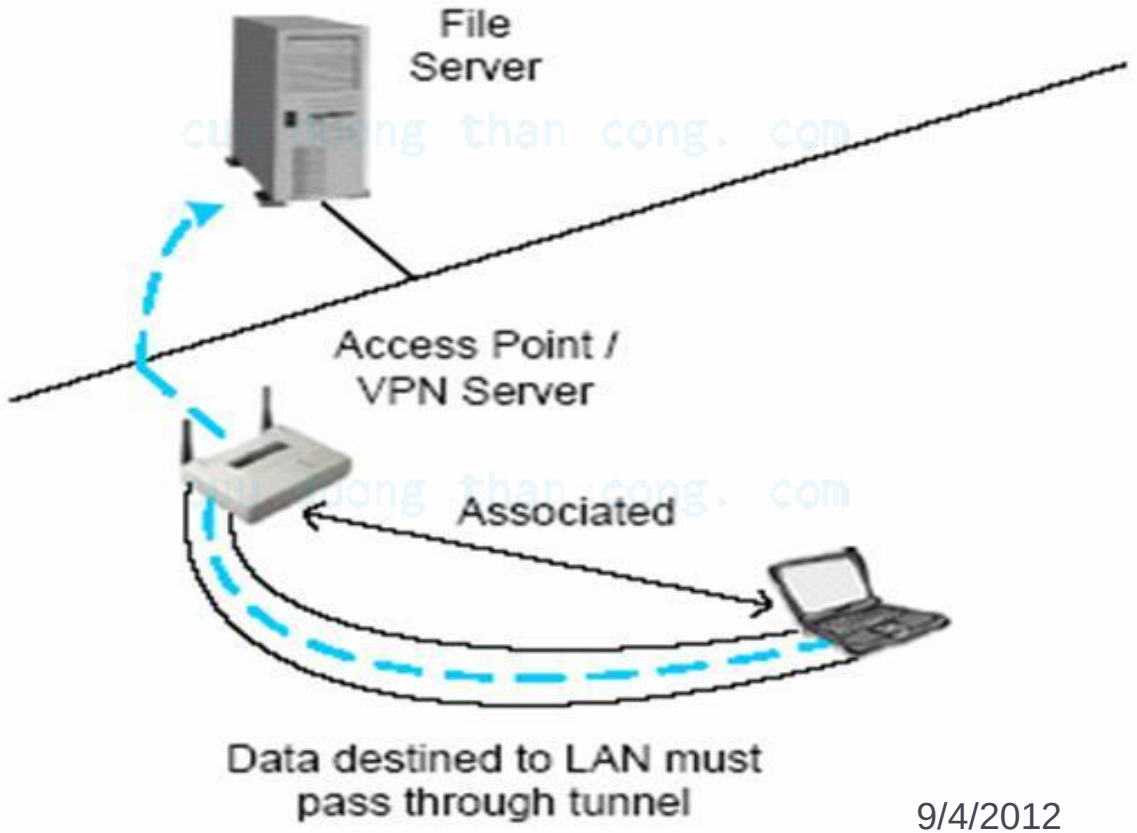
Sử dụng nhiều khóa WEP

- Hầu hết các máy trạm và AP có thể đưa ra đồng thời 4 khóa WEP, nhằm hỗ trợ cho việc phân đoạn mạng.



Giải pháp mạng riêng ảo (VPN)

- Khi VPN server được tích hợp vào AP, các máy trạm sử dụng phần mềm tạo VPN, sử dụng các giao thức như PPTP hoặc IPSec để hình thành một đường hầm kết nối trực tiếp tới AP.



Gia tăng mức độ bảo mật cho WEP

- Sử dụng khóa WEP có độ dài 104 bit.
- Thực thi chính sách thay đổi khóa WEP định kỳ.
- Sử dụng các công cụ theo dõi số liệu thống kê dữ liệu trên đường truyền không dây.
- Sử dụng các giải pháp kỹ thuật tăng cường.

Rủi ro và các biện pháp đối phó trên SSID

- **Các nguy cơ rủi ro:**

- Chuẩn IEEE 802.11 định rõ SSID như là một dạng mật khẩu đối với một người dùng khi kết nối với một mạng WLAN.
- 802.11 yêu cầu người dùng cần phải có cùng SSID như trên AP để có thể truy nhập và truyền thông đối với các thiết bị khác.
- Trên thực tế, SSID sẽ chỉ "an toàn" khi nó được sử dụng kết hợp với các dịch vụ an toàn khác.

Một vài lỗi

- Sử dụng SSID mặc định
- Làm cho SSID có gì đó liên quan đến công ty
- Sử dụng SSID như những phương tiện bảo mật mạng WLAN
- Không cần thiết quảng bá các SSID

Các biện pháp đối phó

- Xóa SSID khỏi các beacon frame (nếu thiết bị cho phép thực hiện điều đó).
- Thay đổi SSID so với giá trị mặc định (hầu hết các AP đều cho phép thực hiện điều này).
- Luôn luôn sử dụng SSID không liên quan đến Công ty.
- Luôn coi SSID chỉ như một cái tên mạng.

Rủi ro và các biện pháp đối phó trên MAC

- **Các nguy cơ rủi ro**
- WLAN có thể lọc dựa vào địa chỉ MAC của các máy trạm.
- Người quản trị mạng có thể biên tập, phân phối và bảo trì một danh sách những địa chỉ MAC được phép và ghichúng vào các AP.
- *Mặc dù Lọc MAC trông có vẻ là một phương pháp bảo mật tốt, chúng vẫn còn dễ bị ảnh hưởng bởi những thâm nhập sau*:
- Sự ăn trộm một Card PC trong có một bộ lọc MAC của AP.
- Việc thăm dò WLAN và sau đó giả mạo với một địa chỉ MAC để thâm nhập vào mạng.

Các biện pháp đối phó

- Sử dụng các RADIUS Server để quản lý các địa chỉ MAC.
- Sử dụng kết nối VPN giữa các máy trạm và AP.

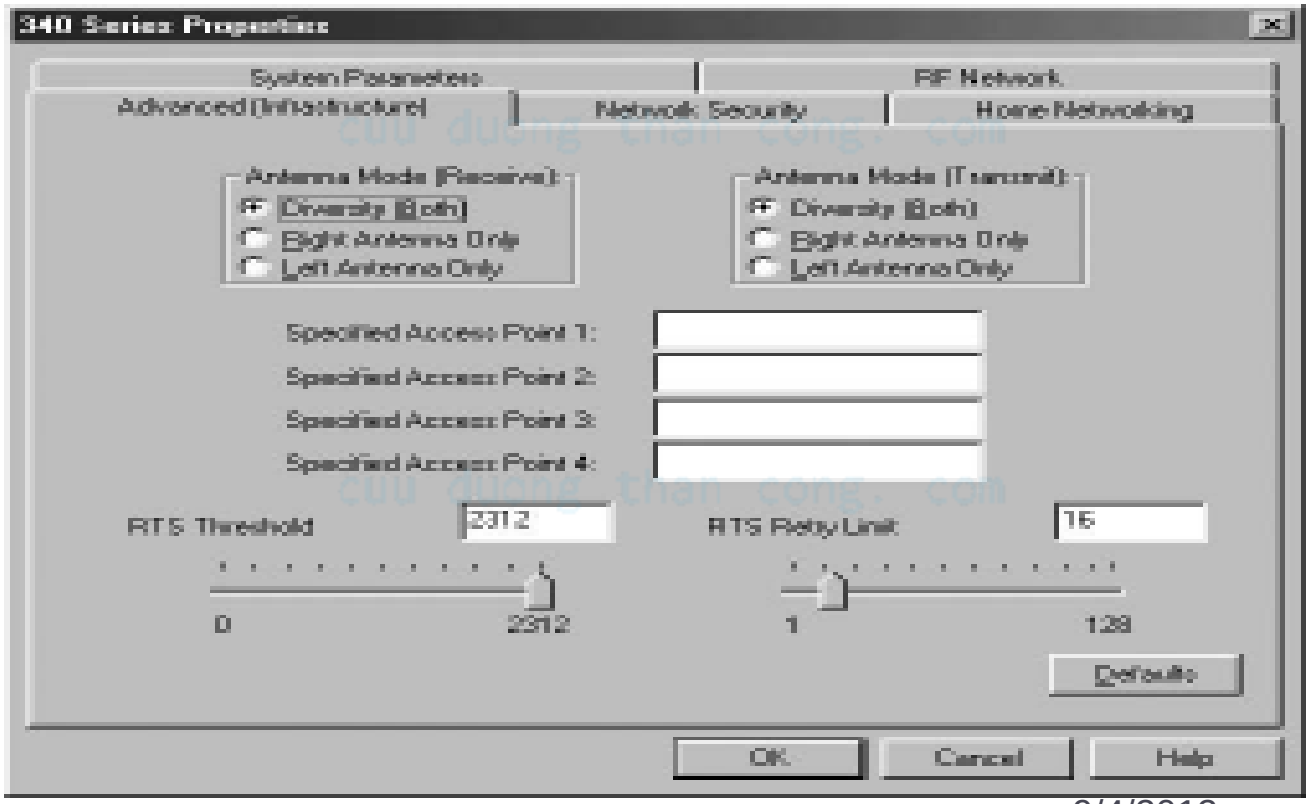
Rủi ro và các biện pháp đối phó với nghe trộm

Các nguy cơ rủi ro

- Khi sử dụng các anten có độ nhạy cao, cho phép có khả năng nhận được tín hiệu sóng vô tuyến từ các khoảng cách xa hơn. Trên thực tế, khi sử dụng các anten loại này cho phép nhận được (*capture*) các tín hiệu từ khoảng vài km tới các AP.
- Trên thực tế có rất nhiều các phần mềm (trên Internet – như AirSnort, Network Stumbler) cho phép bẻ khóa WEP khi thu nhận đủ số lượng các gói dữ liệu truyền.

Các biện pháp đối phó

- Chọn vị trí đặt an ten thích hợp (tại ví trí các trạm trong mạng đều có khả năng thu được thông tin, những tín hiệu không phát xạ đi quá xa) và có thể sử dụng các tấm che để giảm bớt việc bức xạ các tín hiệu RF đi quá xa.
- Điều chỉnh mức ngưỡng phát và thu thông qua các phần mềm điều khiển.



Rủi ro và các biện pháp đối phó với sự giả dạng

- **Các nguy cơ rủi ro:**

- Nếu một bên thứ ba có khả năng nghe trộm trên mạng WLAN thì nó có khả năng giả dạng để trở thành một thành viên chính thức của mạng.
- Đây là một nguy cơ mất an toàn rất nguy hiểm và khả năng thực hiện giả dạng phụ thuộc vào mức độ bảo mật của công ty.

Các biện pháp đối phó

- Có một số biện pháp cho phép làm giảm khả năng một người dùng không cấp phép truy nhập vào mạng như một người dùng hợp lệ.
- Các biện pháp này được thực hiện thông qua các chính sách xác thực, cấp quyền và kiểm toán (*AAA – authentication, authorization and accounting*).

- Với chuẩn IEEE 802.11, xác thực có thể thực hiện bằng cách mở hoặc chia xẻ khóa.
- Với phương thức xác thực đầu tiên (hệ thống mở) không cung cấp khả năng xác thực.
- Phương thức xác thực thông qua chia xẻ khóa cũng không an toàn.
- Có thể thực hiện một số biện pháp làm cho việc xác thực trở nên an toàn hơn.
- Hai trong số các biện pháp đó là sử dụng xác thực theo địa chỉ MAC và EAP.

- Trong chuẩn IEEE 802.11 không cung cấp dịch vụ cấp quyền. Để thay thế, cấp quyền thường được thực hiện theo cách gắn các định danh của người dùng (*User–ID*) và mật khẩu tới các tài nguyên mạng khác nhau.
- Nhờ cấu hình các tham số cấp quyền hợp lý có thể tối thiểu hóa khả năng một bên thứ ba truy nhập tới tài nguyên mạng.
- Dịch vụ cấp quyền rất quan trọng, nhưng nó có thể bị tổn thương nếu sử dụng khóa WEP tĩnh hoặc không sử dụng.

- Với dịch vụ kiểm toán, nhờ ghi lại các phiên truy nhập tới các tài nguyên mạng khác nhau, một cơ sở dữ liệu sẽ được tạo ra.
- Dựa trên cơ sở dữ liệu này có thể thực hiện các phân tích và đánh giá các kết quả nhận được

Rủi ro và các biện pháp đối phó với các điểm truy nhập giả (*rogue AP*)

- **Các nguy cơ rủi ro**

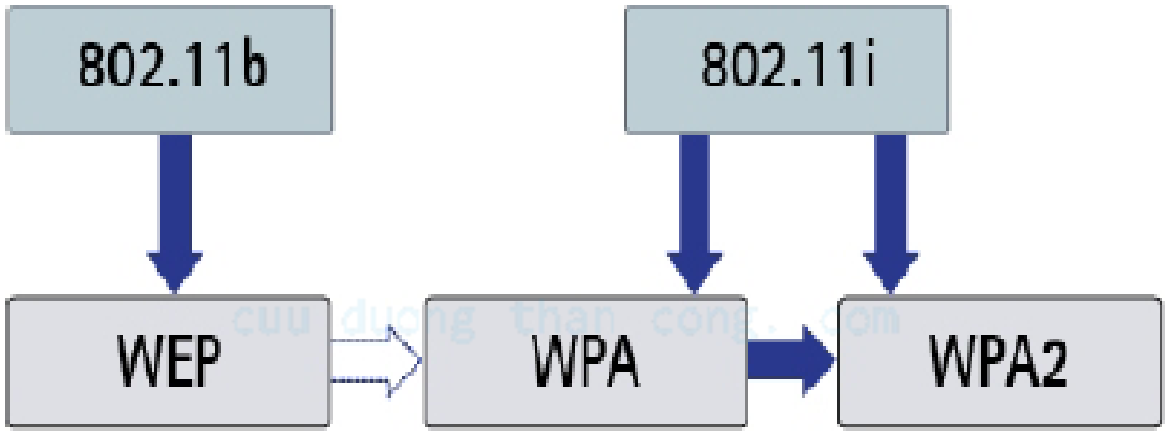
- Đây là kiểu nguy cơ mà hacker đứng ở giữa và trộm lưu lượng truyền giữa 2 nút.
- Nguy cơ này rất mạnh vì hacker có thể trộm tất cả lưu lượng đi qua mạng.
- Để thực hiện, hacker cần phải tạo ra một AP thu hút nhiều sự lựa chọn hơn AP chính thống. AP giả này có thể được thiết lập bằng cách sao chép tất cả các cấu hình của AP chính thống đó là: SSID, địa chỉ MAC, ...

Các biện pháp đối phó

- Sử dụng các công cụ kiểm soát đặc biệt để phát hiện các vị trí đặt AP giả.
- Sử dụng các giải pháp bảo mật mạnh để tránh việc phân tích thông tin và thu được tham số cần thiết.

4. Wi-Fi Protected Access –WPA/WPA2

- Wi-fi allience cùng với IEEE đã cùng nhau xây dựng một giải pháp bảo mật mạnh hơn.
- Vào tháng 10/2002, WPA ra đời như một giải pháp bảo mật tăng cường cho WLAN.



Relationship between WEP, WPA and WPA2

- WPA đã làm tăng rất nhiều mức độ bảo vệ dữ liệu và điều khiển truy nhập cho các mạng WLAN đang tồn tại, nó đã giải quyết tất cả các vấn đề về các nguy cơ tổn thương trong giải pháp WLAN trước đó. Và nó được dùng để thay thế hoàn toàn WEP trong đảm bảo an toàn WLAN.
- WPA cung cấp bảo mật cho tất cả các phiên bản đã tồn tại của các thiết bị WLAN 802.11: a, b, nó cũng được thiết kế để tối thiểu hóa sự ảnh hưởng đến hiệu năng hoạt động của mạng.

- Nó chạy như phần mềm nâng cấp trong các thiết bị bán trên thị trường (AP, NIC).
- Các công ty sẽ được yêu cầu sử dụng các server xác thực như RADIUS, nhưng WPA cho phép những văn phòng nhỏ/người sử dụng cá nhân hoạt động ở một chế độ đặc biệt không cần chúng (sử dụng cơ chế mật khẩu chia xẻ để thực hiện kích hoạt bảo vệ WPA).
- WPA cung cấp việc bảo mật dữ liệu ở mức độ cao và chỉ những người dùng có quyền mới có thể truy nhập mạng nhờ một thuật toán mã hóa mạnh và khả năng xác thực mạnh.

WPA hoạt động như thế nào

- Sử dụng TKIP để mã hóa (Temporary Key Integrity Protocol), sử dụng xác thực 802.1x với giao thức xác thực mở rộng EAP.
- TKIP sử dụng thuật toán RC4 đối với thiết kế chuẩn, một số nhà cung cấp có thể cung cấp AES như là một lựa chọn trong các sản phẩm WPA của họ.
- WPA sử dụng 48 bit IV thay cho 24 bit IV, nó làm tăng đáng kể mức an toàn.
- WPA có thể sử dụng khóa mới cho mỗi 802.11 frame, hoặc có thể dựa trên một thời khoảng được xác định trước trên AP.

- Sử dụng 8 byte MIC (Michael Message Integrity Check) để kiểm tra tính toàn vẹn bản tin.
- WPA sử dụng chuỗi IV để bảo vệ tấn công lặp lại.
- Giải pháp xác thực dựa trên 802.1X được tích hợp trong mỗi sản phẩm.
- WPA hỗ trợ sử dụng phương án EAP hoặc PSK để xác thực người dùng trong mạng.

So sánh các tính năng của WPA và WEP

	WEP	WPA
Encryption	Flawed, cracked by scientists and hackers	Fixes all WEP flaws
	40-bit keys	128-bit keys
	Static – same key used by everyone on the network	Dynamic session keys. Per user, per session, per packet keys
	Manual distribution of keys – hand typed into each device	Automatic distribution of keys
Authentication	Flawed, used WEP key itself for authentication	Strong user authentication, utilizing 802.1X and EAP

Các tính năng của WPA

Feature	WPA
Encryption	RC4
Authentication	PSK, EAP
Key Rotation	Per frame; configurable lifetimes
Standards-Based	Yes
Easy to Deploy?	NO
Requires OS patch or Supplicant Software	YES
Requires Wireless card software driver update?	YES
Supports PKI?	EAP-TLS and EAP-TTLS
Practical DoS Susceptibility	YES
Can provide end-to-end encryption beyond the Access Point	NO

IEEE 802.11i

- Tháng 1/2001, nhóm i được thành lập trong IEEE nhằm thực hiện nhiệm vụ nâng cao tính an toàn của vấn đề bảo mật và xác thực trong 802.11. IEEE 802.11i (WPA2), được phê chuẩn vào 24/6/2004, được thiết kế để tăng cường tính an ninh trong lớp MAC trong IEEE 802.11.
- Chuẩn 802.11i được giới thiệu như là một sự thay đổi nền tảng của các vấn đề xác thực, bảo mật và toàn vẹn, vì thế nó cung cấp một kiến trúc mới về an toàn mạng.
- Kiến trúc mới cho các mạng không dây được gọi là mạng an ninh mạnh (Robust Security Network - RSN) và sử dụng xác thực 802.1X, cơ chế phân phối khóa mạnh và các cơ chế kiểm tra toàn vẹn và bảo mật mới.

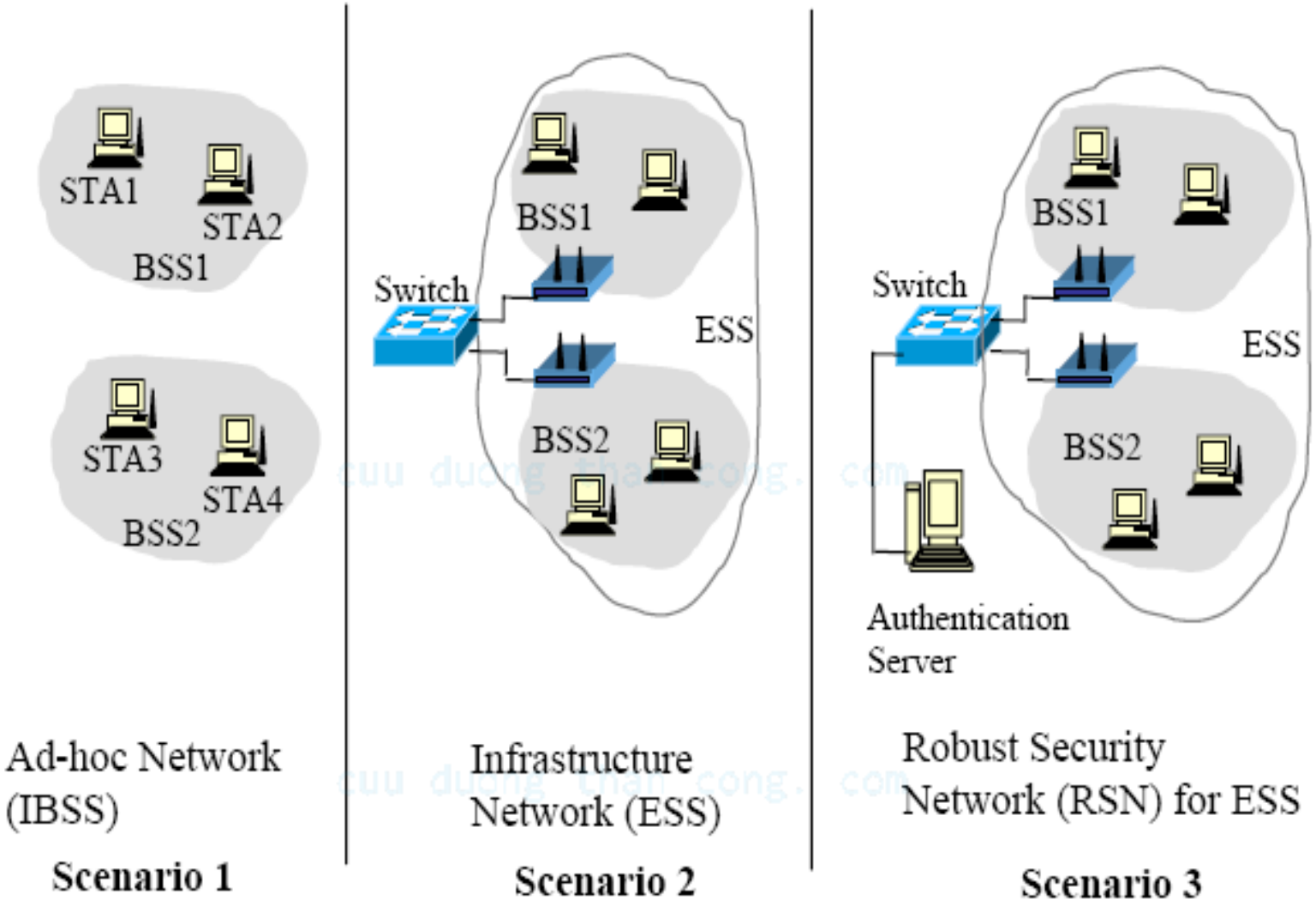


Figure 1 IEEE 802.11 Modes

Nguyên tắc hoạt động

- 802.11 quảng bá, xác thực và kết hợp: Khi một trạm (STA) bắt đầu hoạt động, nó sẽ dò tìm các AP trong khoảng cách cho phép sử dụng các frame yêu cầu tìm kiếm.
- Các frame yêu cầu tìm kiếm được gửi trên mỗi kênh STA hỗ trợ, trong một cố gắng tìm kiếm tất cả các AP có SSID phù hợp và có tốc độ dữ liệu đáp ứng yêu cầu.

- Tất cả các AP trong phạm vi tìm kiếm và phù hợp với các yêu cầu quét tìm kiếm của STA sẽ đáp lại với một frame đáp trả tìm kiếm bao gồm các thông tin đồng bộ, tải của AP và các thông số bảo mật.
- STA sẽ xác định kết nối vào AP nào thông qua việc xem xét các thông tin nhận được.
- Sau khi STA xác định được AP tối ưu để kết nối tới chúng, khi đó WPA được hỗ trợ.

Giao thức xác thực IEEE 802.1X

- IEEE 802.1X (điều khiển truy nhập mạng dựa trên cổng - Port-Based Network Access Control) được phát triển dành cho các mạng không dây, cung cấp các cơ chế xác thực, cấp quyền và phân phối khóa, và thực hiện điều khiển truy nhập đối với user truy nhập mạng.
- Cấu trúc IEEE 802.1X bao gồm 3 thành phần chính:
  - User truy nhập mạng.
  - Xác thực cung cấp điều khiển truy nhập mạng.
  - Server xác thực.

- Trong các mạng không dây, AP hoạt động như xác thực cung cấp điều khiển truy nhập mạng.
- Mỗi cổng vật lý (cổng ảo trong WLAN) được chia thành 2 cổng logic tạo nên thực thể truy nhập mạng - PAE (Port Access Entity).
- Authenticator PAE luôn luôn mở để cho phép các frame xác thực đi qua, trong khi các dịch vụ PAE chỉ được mở khi xác thực thành công. Quyết định cho phép truy nhập thường được thực hiện bởi thành phần thứ ba, được gọi là server xác thực (nó có thể là một server Radius dành riêng hoặc chỉ là một phần mềm chạy trên AP).

- Chuẩn 802.11i thực hiện một số thay đổi nhỏ đối với 802.1X để các mạng không dây kiểm toán khả năng ăn trộm ID.
- Bản tin xác thực được kết hợp chặt chẽ để đảm bảo rằng cả user và AP tính toán khóa bí mật và cho phép mã hóa trước khi truy nhập vào mạng.
- User và authenticator liên lạc với nhau sử dụng giao thức dựa trên EAP. Chú ý rằng vai trò của authenticator chủ yếu là thụ động – nó chỉ đơn giản chuyển tiếp tất cả các bản tin đến server xác thực.

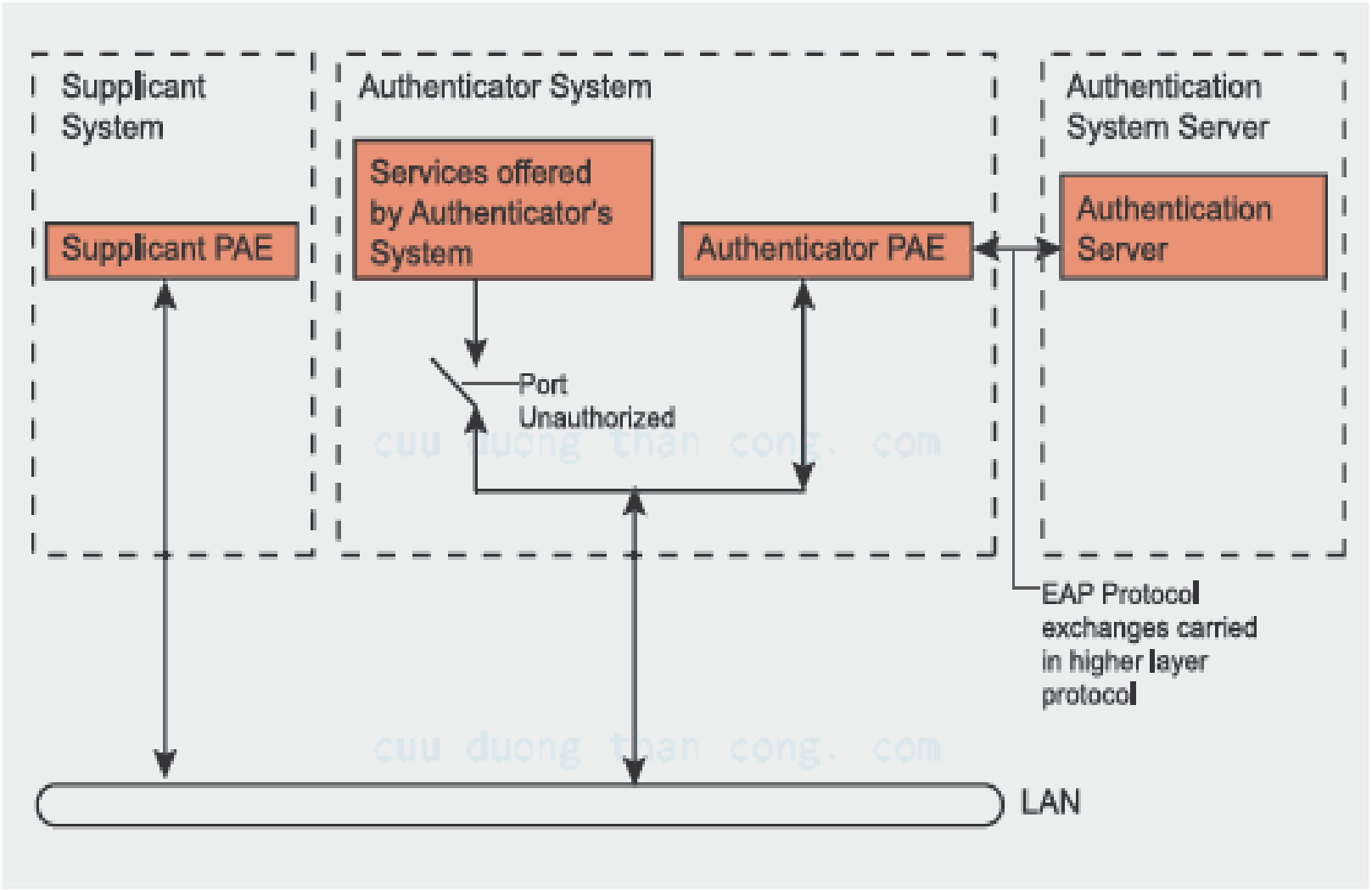


Figure 3. *IEEE 802.1X model from the IEEE 802.1X specification*

- EAP là một khung cho sử dụng các phương pháp xác thực khác nhau (cho phép chỉ một số giới hạn các loại message – Request, Respond, Succcess, Failure) và dựa trên việc lựa chọn các phương pháp xác thực: EAP-TLS, EAP-TTLS, PEAP, Kerberos v5, EAP-SIM, ... Khi quá trình này hoàn thành, cả hai thực thể có một khóa bí mật chủ (*Master key*).
- Truyền thông giữa authenticator và server xác thực sử dụng giao thức EAPOL (EAP Over LAN), được sử dụng trong các mạng không dây để chuyển tiếp các dữ liệu EAP sử dụng các giao thức lớp cao như Radius.

- Một RSN đặc thù sẽ chỉ chấp nhận các thiết bị có khả năng RSN, nhưng IEEE 802.1i cũng hỗ trợ một kiến trúc mạng an toàn chuyển tiếp (Transitional Security Network - TSN) để cả hai hệ thống RSN và WEP cùng tham gia, cho phép các user nâng cấp các thiết bị của họ theo thời gian.
- Các thủ tục xác thực và kết hợp sử dụng cơ chế bắt tay 4 bước, kết hợp được gọi là kết hợp mạng an toàn mạnh (Robust Security Network Association - RSNA).

- Thiết lập một phiên truyền thông bao gồm 4 giai đoạn:

- Tán thành các chính sách bảo mật.
- Xác thực 802.1X.
- Nhận được khóa nguồn và phân phối.
- Bảo mật và toàn vẹn dữ liệu RSNA.

Thiết lập một phiên truyền thông

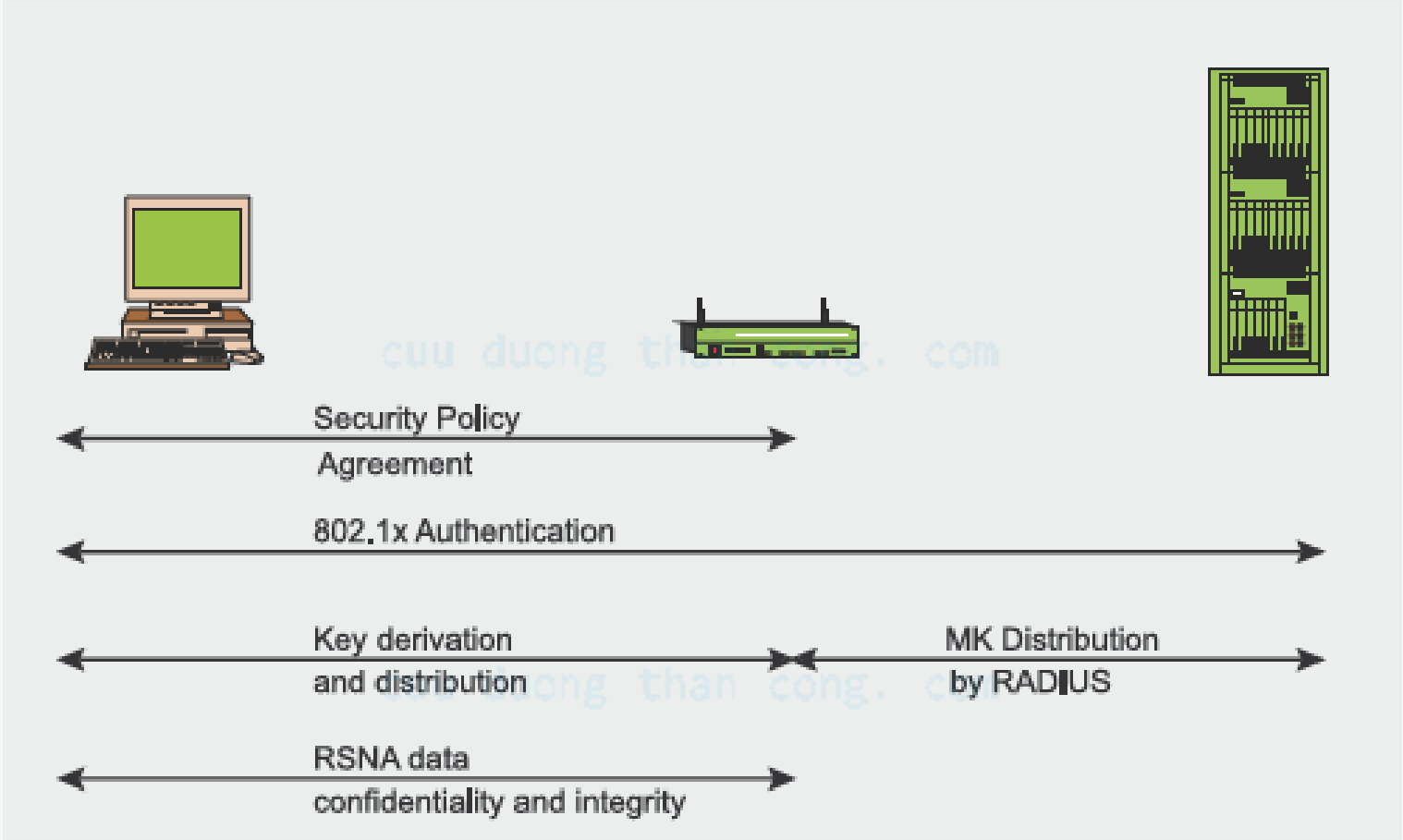


Figure 4. *802.11i operational phases*

- *Giai đoạn 1* - tán thành các chính sách bảo mật:

- Ở giai đoạn này yêu cầu các bên truyền thông thỏa thuận các chính sách bảo mật để sử dụng.
- Các chính sách bảo mật được hỗ trợ bởi AP được phát quảng bá trên các beacon hoặc trong các bản tin Probe Respond (tiếp sau một Probe Respond từ client).
- Tiếp theo là các xác thực mở (giống như trong các mạng TSN, ở đó xác thực là luôn luôn thành công).

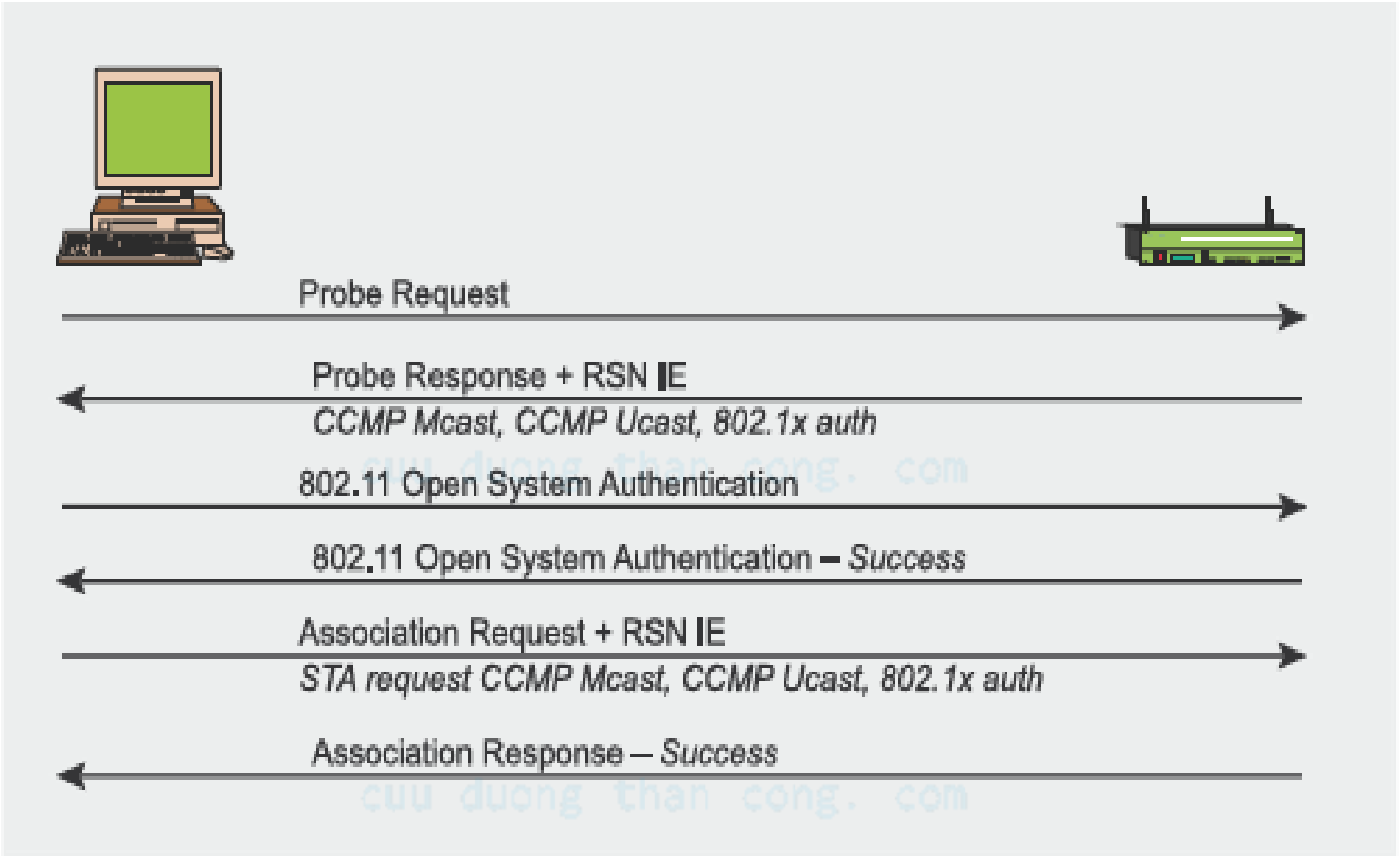


Figure 5. *Phase 1: Agreeing on the security policy*

- Client phản ứng đưa ra các yêu cầu trong Associaton Request và được phê chuẩn bởi Associaton Respond từ AP. Các thông tin chính sách an toàn được gửi trong trường RSN IE, bao gồm:
- Các phương pháp xác thực được hỗ trợ (802.1X, PSK).
- Các giao thức an toàn cho truyền thông unicast (CCMP, TKIP, ...) – cặp khóa mã hóa.
- Các giao thức an toàn cho truyền thông multicast (CCMP, TKIP, ...) - nhóm khóa mã hóa.
- Hỗ trợ tiền xác thực, cho phép các user tiền xác thực trước khi được chuyển tới truy nhập mạng.

Giai đoạn 2 – xác thực 802.1X

- Dựa trên EAP và các phương pháp xác thực được thỏa thuận ở giai đoạn 1 (EAP-TLS cho client và các chứng chỉ server (yêu cầu sử dụng PKI);, ...).
- 802.1X được bắt đầu khi AP yêu cầu định danh client, các thông tin đáp trả từ client bao gồm các thông tin về phương thức xác thực. Các bản tin hợp lệ sau đó được trao đổi giữa client và AS để sinh ra một khóa chủ (Master Key - MK).
- Tại điểm cuối của thủ tục một bản tin chấp nhận Radius được gửi từ AP tới client bao gồm MK và bản tin thành công EAP.

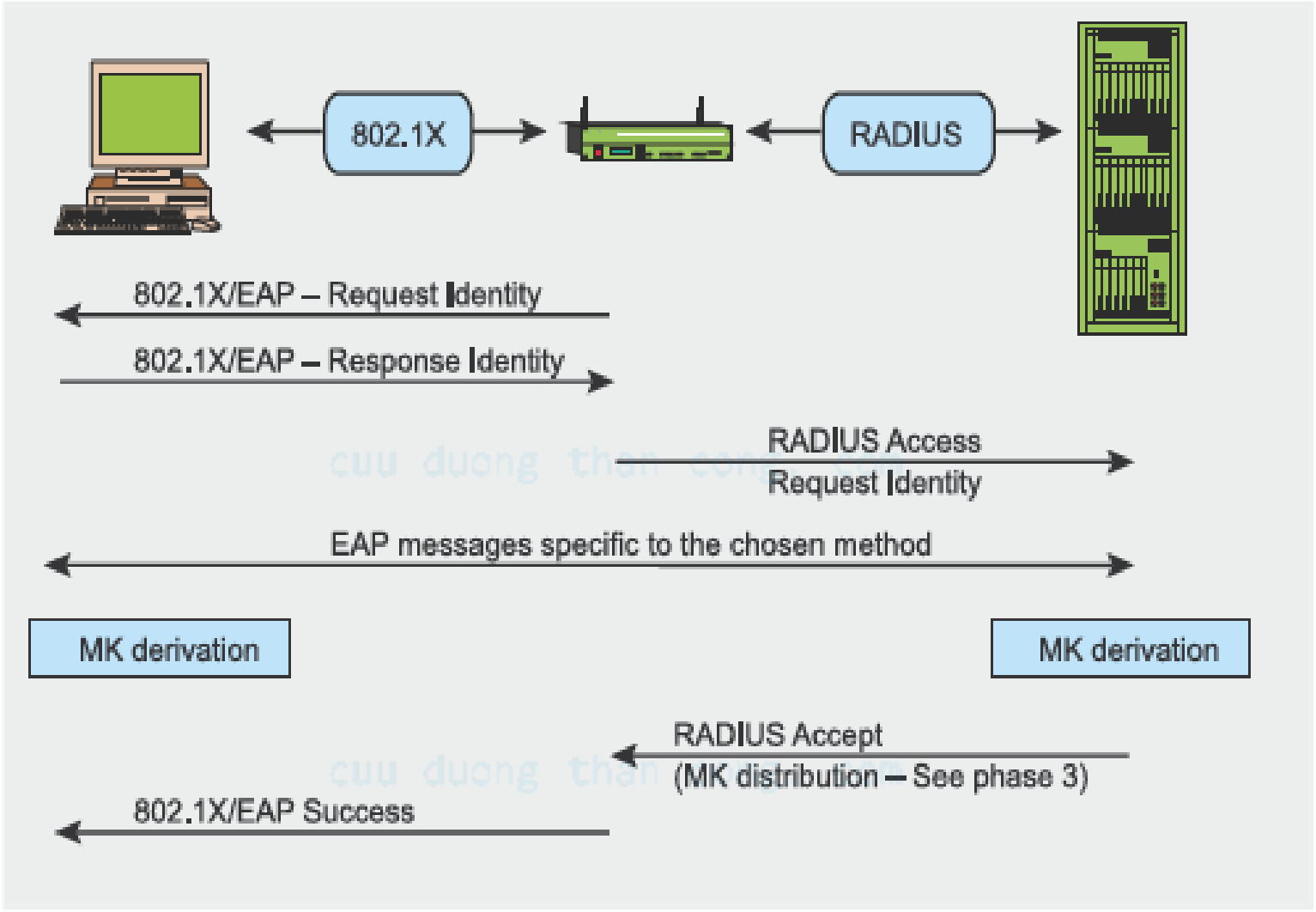


Figure 6. *Phase 2: 802.1X authentication*

Giai đoạn 3 – cây khóa và phân phối

- Kết nối an toàn dựa trên các khóa bí mật. Trong RSN, mỗi khóa có một thời gian sống giới hạn và bảo mật tổng thể được đảm bảo nhờ sử dụng một tập hợp các khóa khác nhau, được tổ chức thành cây. Khi một phiên bảo mật được thiết lập sau khi xác thực thành công, các khóa tạm thời (khóa phiên) được tạo và thường xuyên cập nhật cho đến khi phiên bảo mật kết thúc.
- Có 2 bước bắt tay trong khi sinh khóa.
  - 4-way Handshake sinh ra PTK (Pair-wire Transient Key) và GTK (Group Transient Key).
  - Group Handshake Key: tạo mới cho GTK.

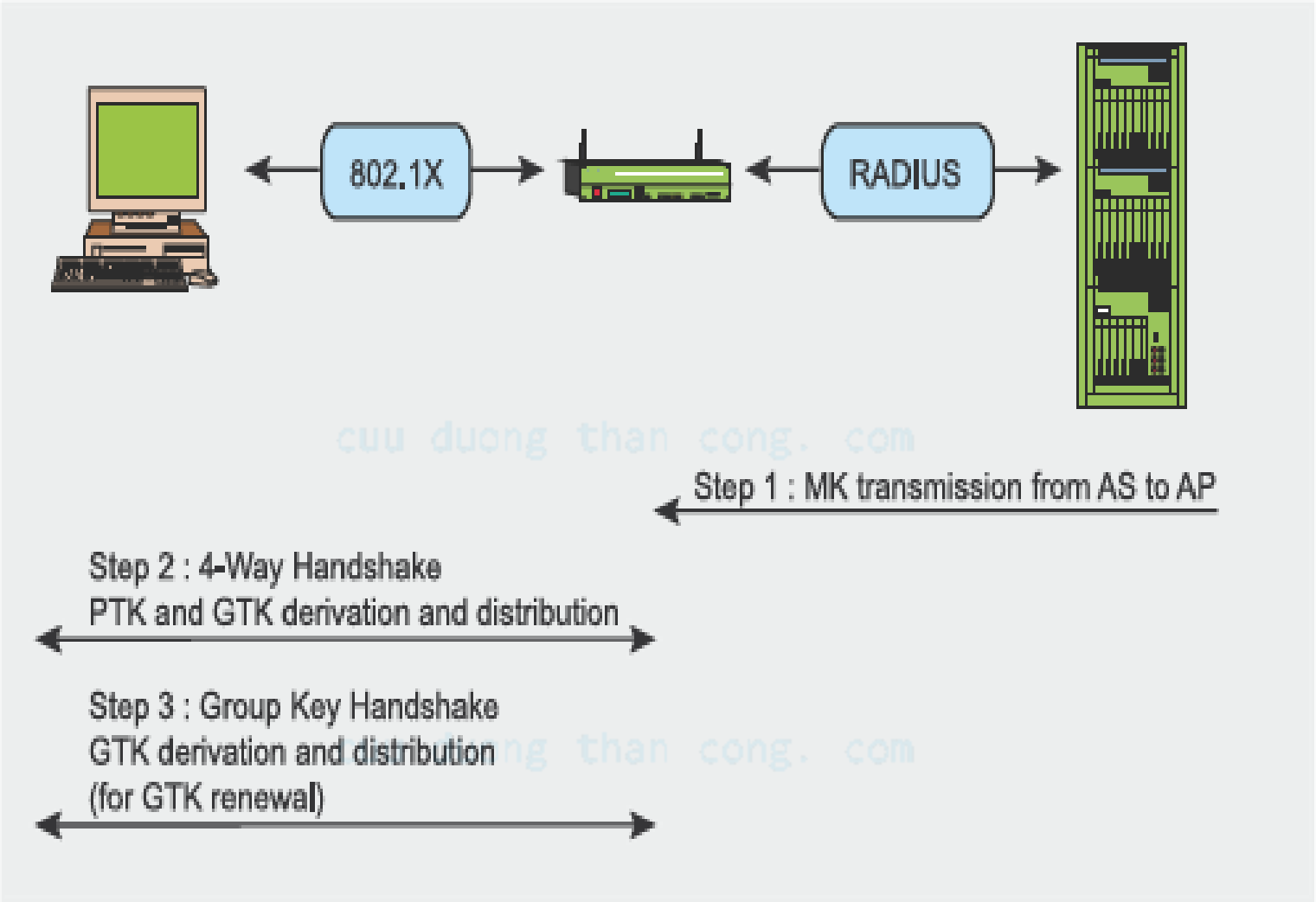


Figure 7. *Phase 3: Key derivation and distribution*

- PMK (Pairwire Master Key) nhận được dựa trên phương pháp xác thực được sử dụng:
- Nếu sử dụng PSK, PMK = PSK. PSK được sinh ra từ mật khẩu thông thường (từ 8-63 ký tự) hoặc là một chuỗi 256 bit, cung cấp các giải pháp bảo mật cho cá nhân hoặc văn phòng nhỏ (không cần server xác thực).
- Nếu một AS được sử dụng, PMK nhận được từ MK của xác thực 802.11 X.

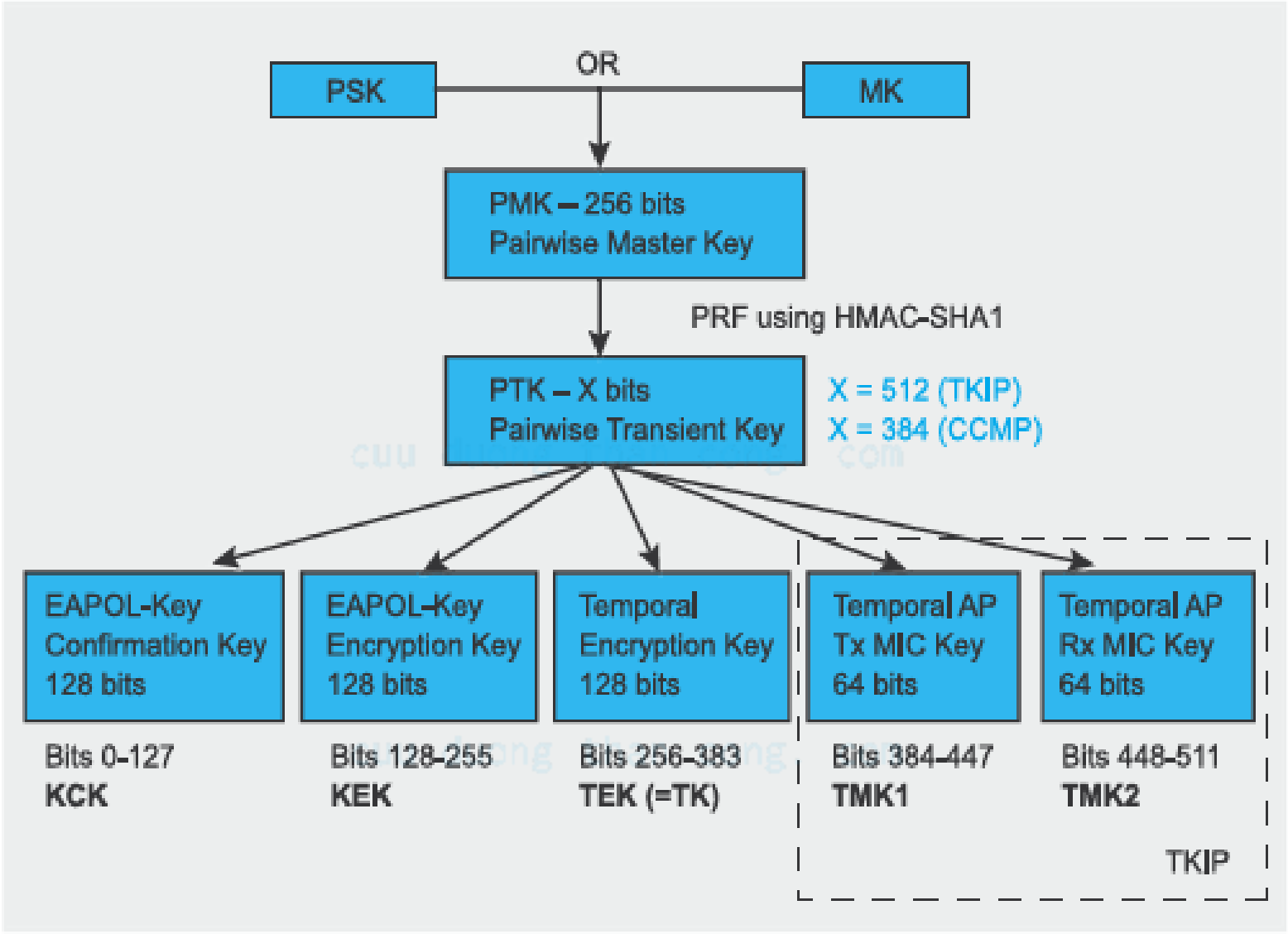


Figure 8. *Phase 3: Pairwise Key Hierarchy*

- PMK bản thân không bao giờ được sử dụng cho mã hóa và kiểm tra toàn vẹn. nó được sử dụng để sinh ra một khóa mã hóa tạm thời PTK. Độ dài của PTK phụ thuộc vào giao thức mã hóa: 512 bit cho TKIP và 384 cho CCMP.
- PTK bao gồm các phần sau:

- KCK – 128 bit: khóa dành cho xác thực các bản tin (MIC) trong quá trình 4-way handshake và group handshake key.
- KEK - 128 bit: khóa để đảm bảo bảo mật dữ liệu trong quá trình 4-way handshake và group handshake key.
- TK – 128 bit: khóa cho mã hóa dữ liệu (được sử dụng bởi TKIP hoặc CCMP).
- TMK – 2x64 bit: khóa dành cho xac thực dữ liệu (được sử dụng chỉ với MIC). Một khóa dành riêng cho mỗi kênh liên lạc.

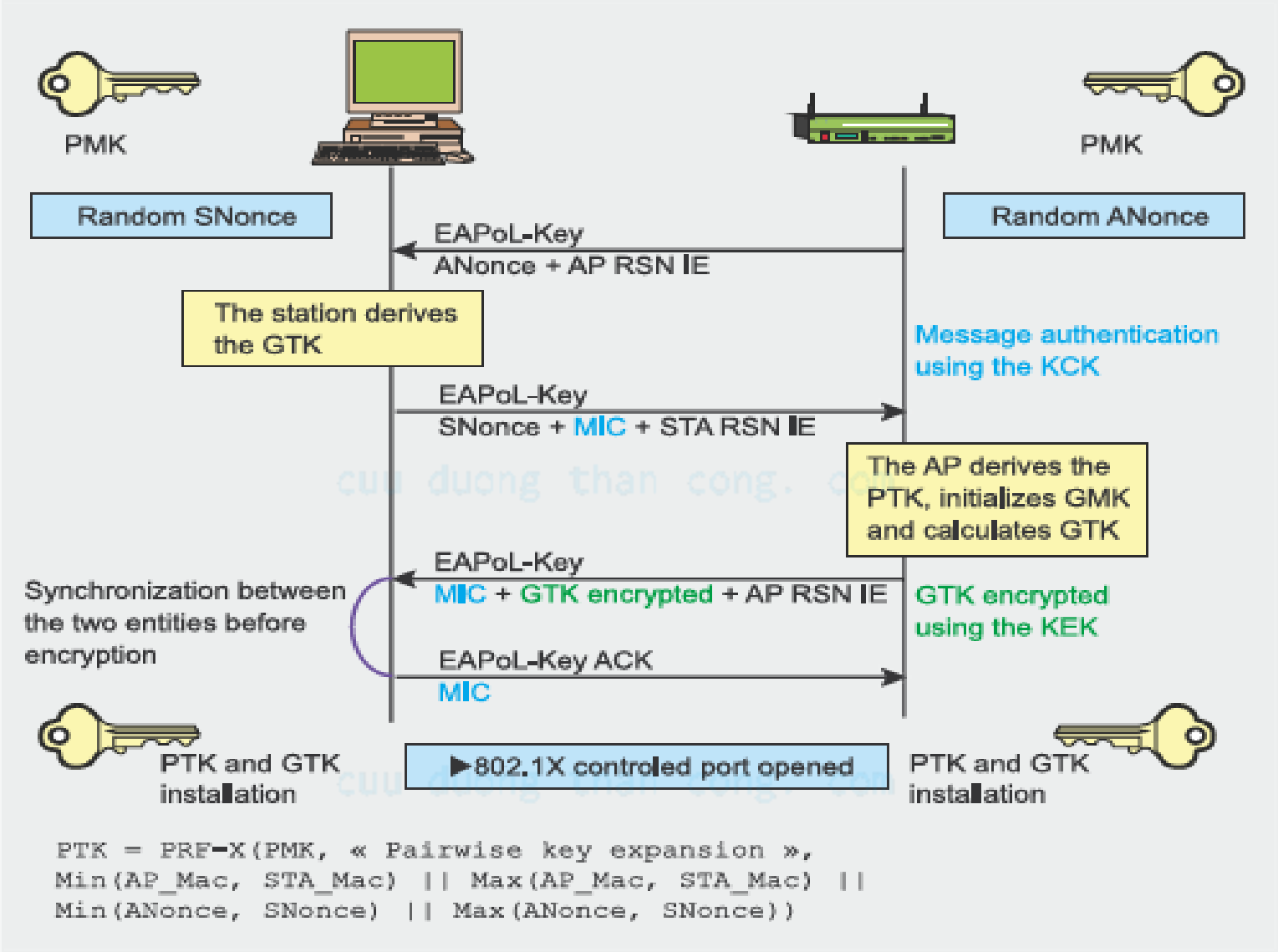


Figure 9. *Phase 3: 4-Way Handshake*

4-way handshake: được khởi nguồn từ AP, tạo cho nó có các khả năng:

- Xác nhận sự nhận biết của client với PTK.
- Sinh ra PTK mới.
- Cài đặt các khóa mã hóa và toàn vẹn.
- Xác nhận bộ mã hóa được chọn.

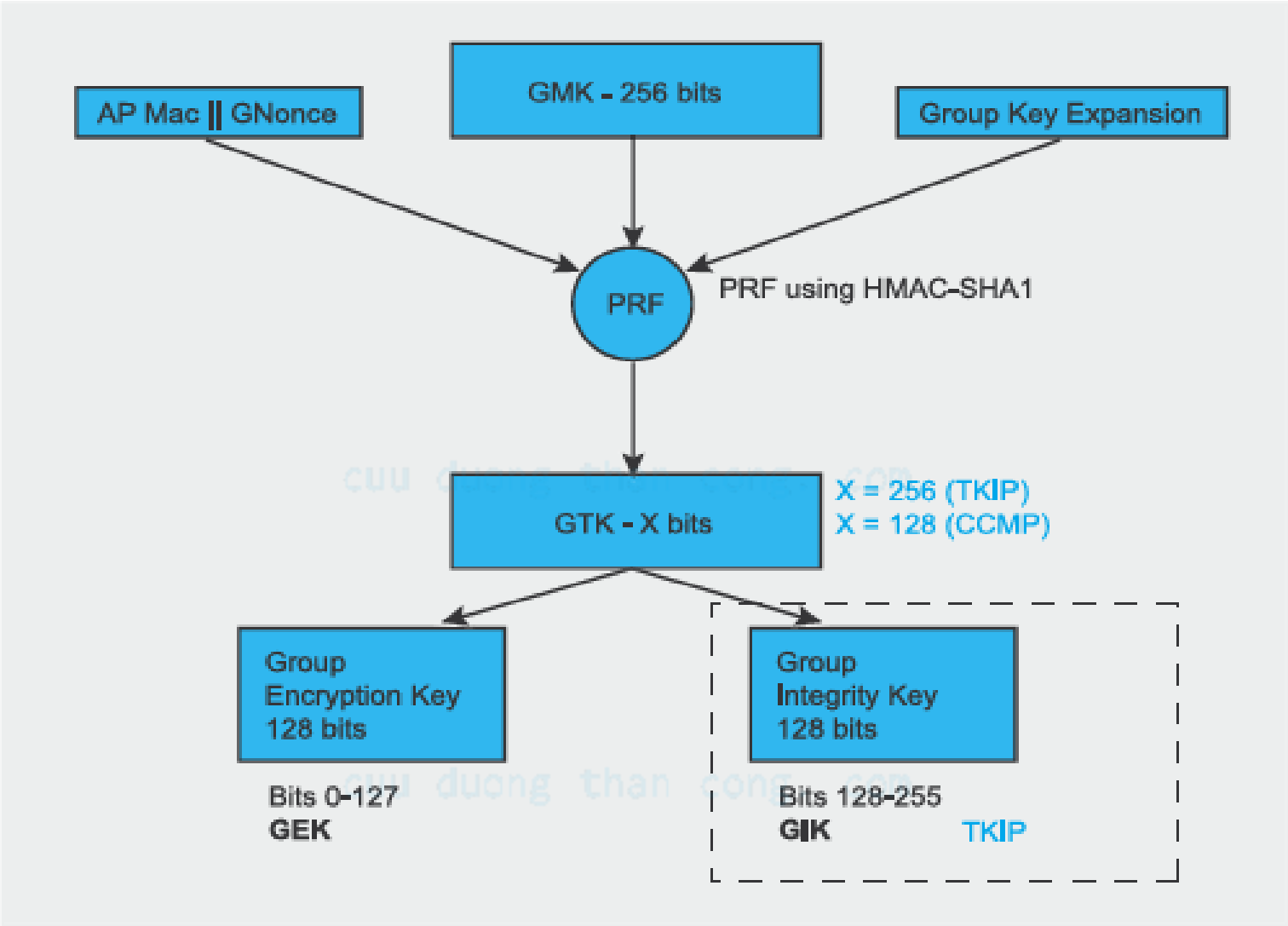


Figure 10. *Phase 3: Group Key Hierarchy*

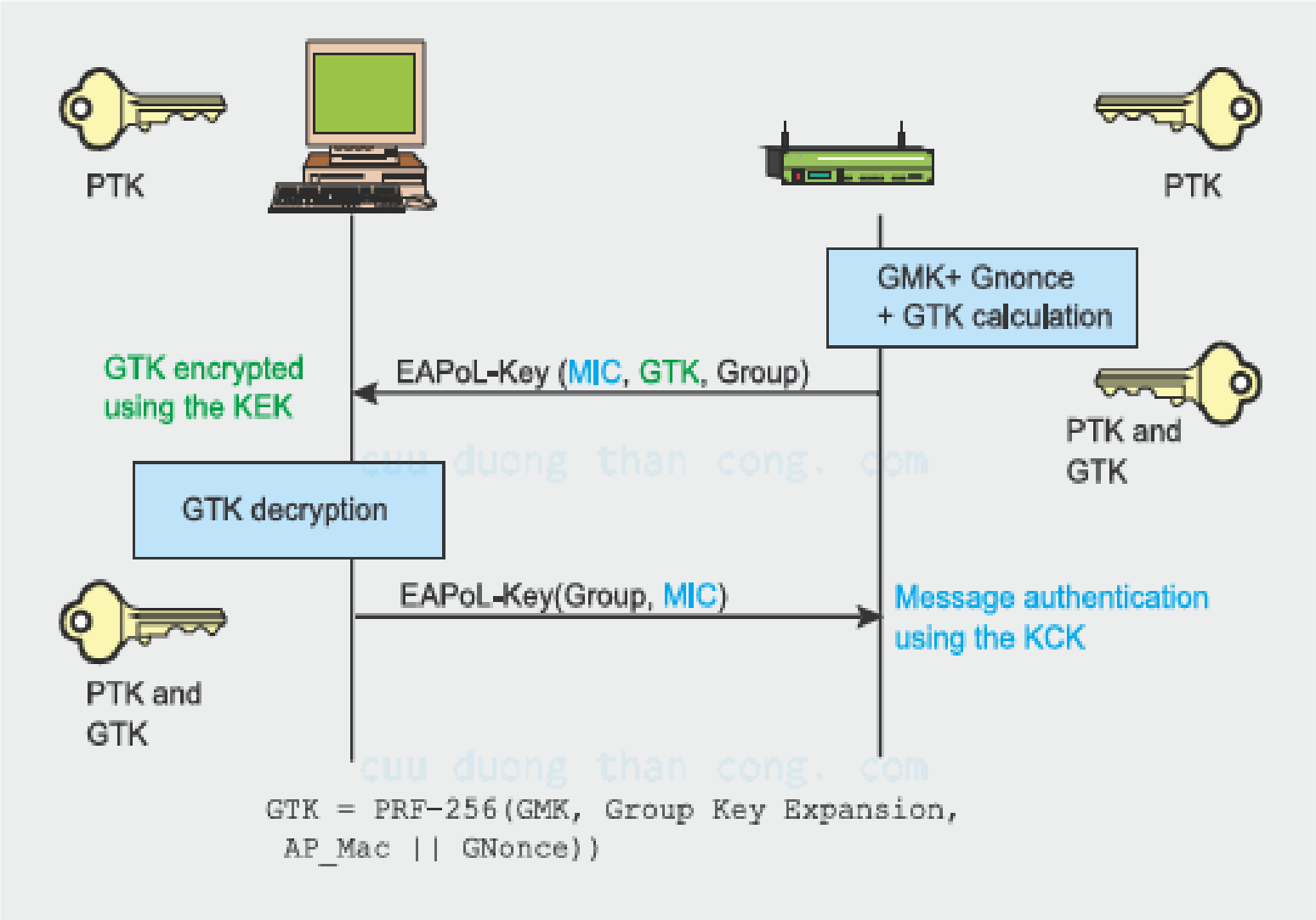


Figure 11. *Phase 3: Group Key Handshake*

Giai đoạn 4 – RSNA bảo mật và toàn vẹn dữ liệu

- Tất cả các khóa sinh ra ở các giai đoạn trên được sử dụng trong các giao thức hỗ trợ RSNA bảo mật và toàn vẹn.
- TKIP (Temporal Key Hash).
- CCMP (Counter-Mode/ Cipher Bock Chaining Message Authentication Code Protocol).
- WRAP (Wireless Robust Authenticated Protocol).

TKIP

- WPA được xây dựng tương thích hoàn toàn với các thiết bị WLAN đang tồn tại. TKIP tăng nâng cao khả năng bảo mật và phải tuân theo các yêu cầu tương thích, vì vậy nó cũng sử dụng thuật toán mật mã dòng RC4. Vì vậy để sử dụng TKIP chỉ cần nâng cấp phần mềm.
- Trong thực tế hầu hết các chuyên gia tin rằng TKIP là một giải pháp mã hóa mạnh hơn WEP. Tuy nhiên họ cũng đồng ý rằng TKIP chỉ là một giải pháp tạm thời vì nó sử dụng RC4.

- Ưu điểm chính của TKIP so với WEP là sự luân phiên khóa.
- TKIP sử dụng thay đổi thường xuyên các khóa mã cho RC4 (khoảng 10000 packet), và véc tơ khởi tại IV được tạo khác.
- TKIP được bao gồm trong 802.11i như là một lựa chọn.

- Trên thực tế, TKIP bao gồm 4 thuật toán để thực hiện tốt nhất các khả năng an toàn:
- Mã kiểm tra tính toàn vẹn bản tin (MIC): có thể thực hiện trên phần mềm chạy trên các CPU tốc độ thấp.
- Nguyên tắc chuỗi IV mới.
- Chức năng trộn khóa trên mỗi gói.
- Phân phối khóa: một phương pháp mới để phân phối khóa.

Chức năng trộn khóa trên mỗi gói

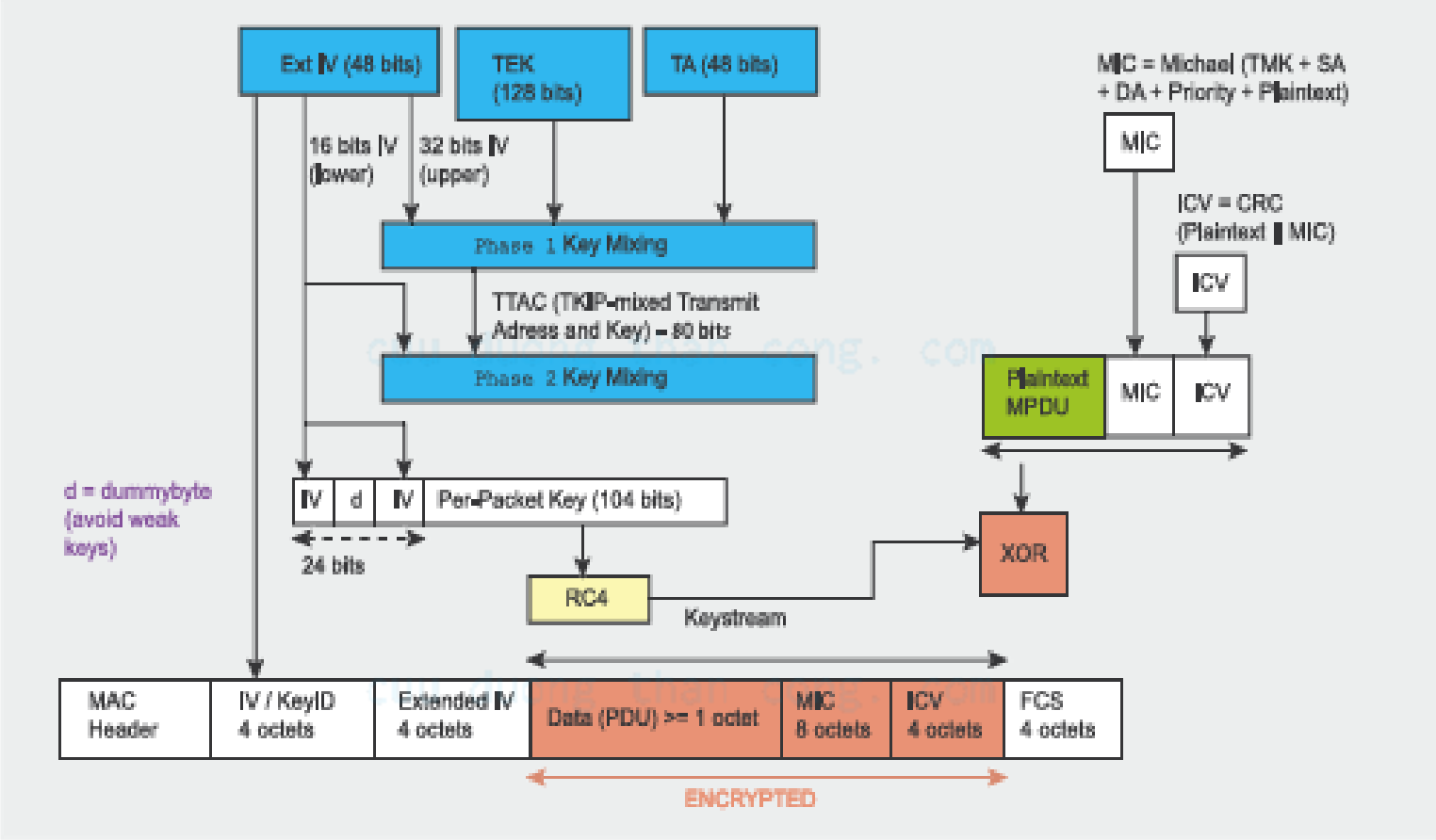


Figure 12. *TKIP Key-Mixing Scheme and encryption*

Giá trị MIC được tính

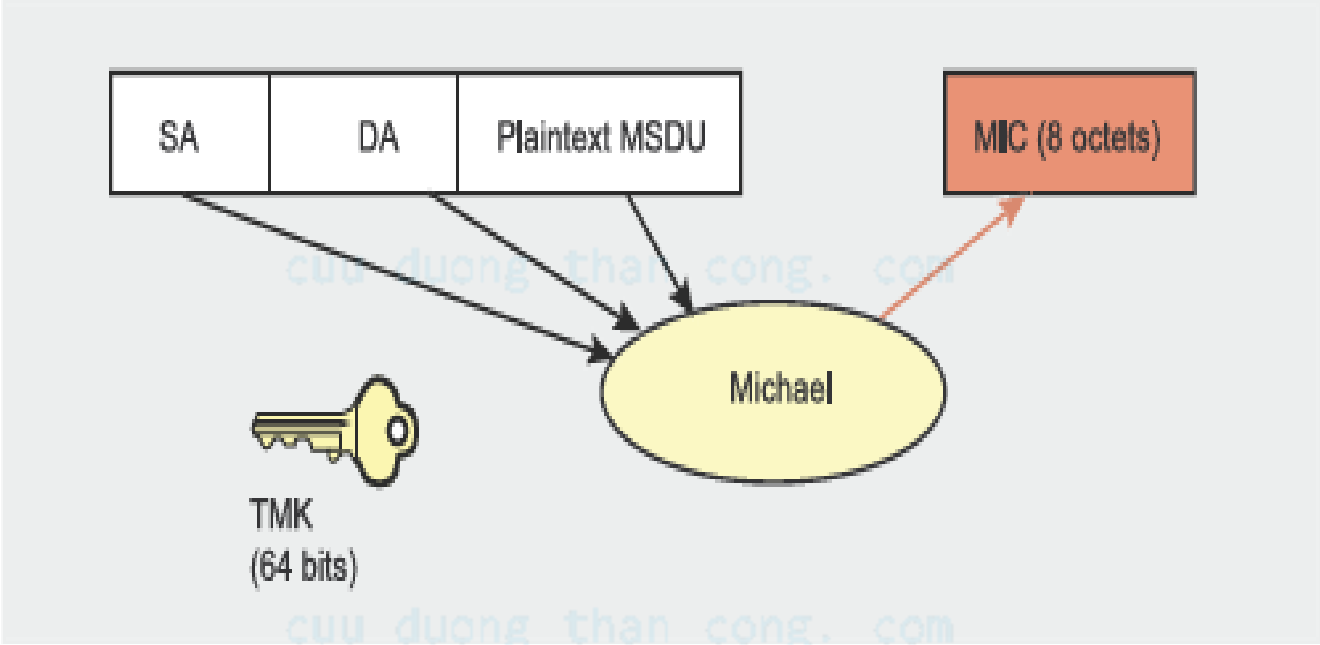


Figure 13. *MIC computation using the Michael algorithm*

CCMP

- Không giống như TKIP bắt buộc phải được xây dựng để tương thích với các phần cứng WEP đã có. CCMP là một giao thức được thiết kế mới.
- CCMP sử dụng chế độ đếm (Counter mode) kết hợp với một phương thức xác thực bản tin được gọi là CBC-MAC để tạo MIC.
- Một số tính năng mới cũng được phát triển thêm như sử dụng một khóa đơn cho mã hóa và xác thực (với các IV khác nhau) hoặc bao phủ phần dữ liệu không được mã hóa bởi xác thực.

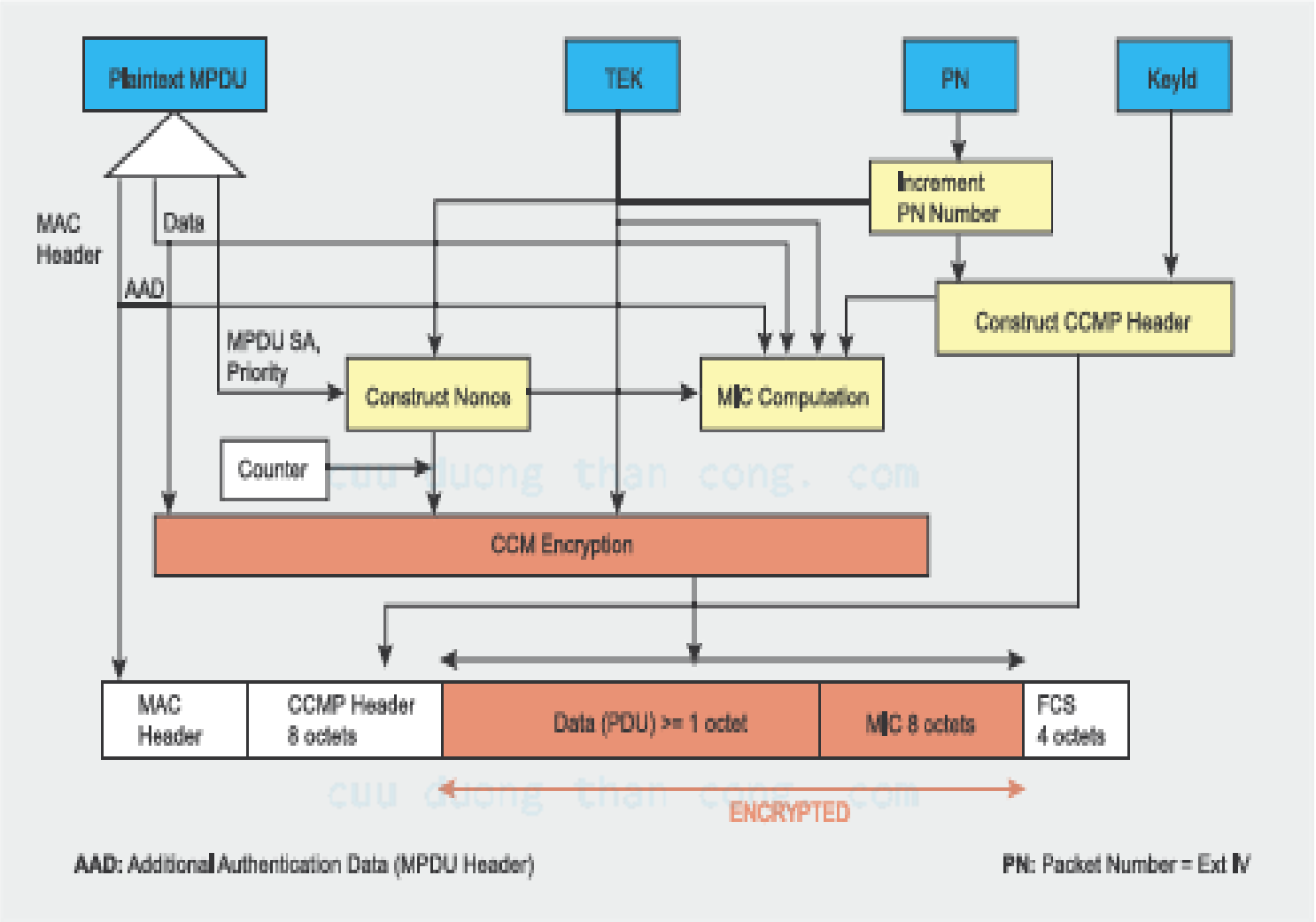


Figure 14. *CCMP encryption*

Các điểm yếu trong WPA/WPA2

- Chỉ một ít các điểm yếu nhỏ được phát hiện trên WPA/WPA2 từ khi chúng được phê chuẩn, không có điểm yếu là là quá nguy hiểm.
- Hầu hết các điểm yếu thực tế là tấn công chống lại khóa PSK của WPA/WPA2.
- Như đã biết PSK là phương án thay thế của 802.1x PMK sinh ra bởi AS. Nó là một chuỗi 256 bit hoặc một mật khẩu từ 8-63 ký tự, được sử dụng để sinh ra sử dụng thuật toán: PSK = PMK = PBKDF2 (pass, SSID, SSID length, 4096, 256), ở đây PBKDF2 là một phương pháp được sử dụng trọng PKCS #5, 4096 là số lượng của các hàm hash và 256 là giá trị lối ra. PTK được sinh ra từ PMK sử dụng 4-way handshake và tất cả thông tin được sử dụng để tính toán giá trị của nó được truyền ở dạng plaintext.

- Sức mạnh của PTK vì thế dựa trên các giá trị của PMK, để PSK hiệu quả bằng cách sử dụng các mật khẩu mạnh. Như đã được chỉ ra bởi Robert Moskiwitz, bản tin thứ hai của 4-way handshake phải chịu được các tấn công sử dụng từ điển và brute force.
- Có một số tiện ích được tạo ra để lợi dụng điểm yếu này, aicrack được sử dụng để tấn công PSK trong WPA.

- Giao thức thiết kế (4096 hàm hash cho mỗi pass) nghĩa là một tấn công brute force sẽ rất chậm.
- Một biện pháp chống lại tấn công mật khẩu là sử dụng ít nhất mật khẩu 20 ký tự.
- Để thực hiện tấn công này attacker phải bắt được các bản tin trong quá trình 4-way handshake nhờ chế độ giám sát thụ động mạng không dây hoặc sử dụng tấn công không xác thực.

Các bước tấn công

- Bước 1: kích hoạt chế độ quan sát.
- # airmon.sh start ath0
- Bước tiếp theo sẽ tìm kiếm các mạng và các client kết nối tới nó.
- Bước cuối là thực hiện một tấn công sử dụng từ điển

Listing 7. *Discovering nearby networks*

```
# airodump ath0 wpa-crk 0

 BSSID              PWR  Beacons    # Data  CH  MB  ENC   ESSID
 00:13:10:1F:9A:72   56      112        16   1  48  WPA   hakin9demo


 BSSID              STATION            PWR  Packets  ESSID

 00:13:10:1F:9A:72  00:0C:F1:19:77:5C   34        1  hakin9demo
```


Listing 8. *Launching a dictionary attack*

```
$ aircrack -a 2 -w some_dictionnary_file -0 wpa-psk.cap
Opening wpa-psk.cap
Read 541 packets.
 BSSID              ESSID       Encryption
 00:13:10:1F:9A:72  hakin9demo  WPA (1 handshake)
```

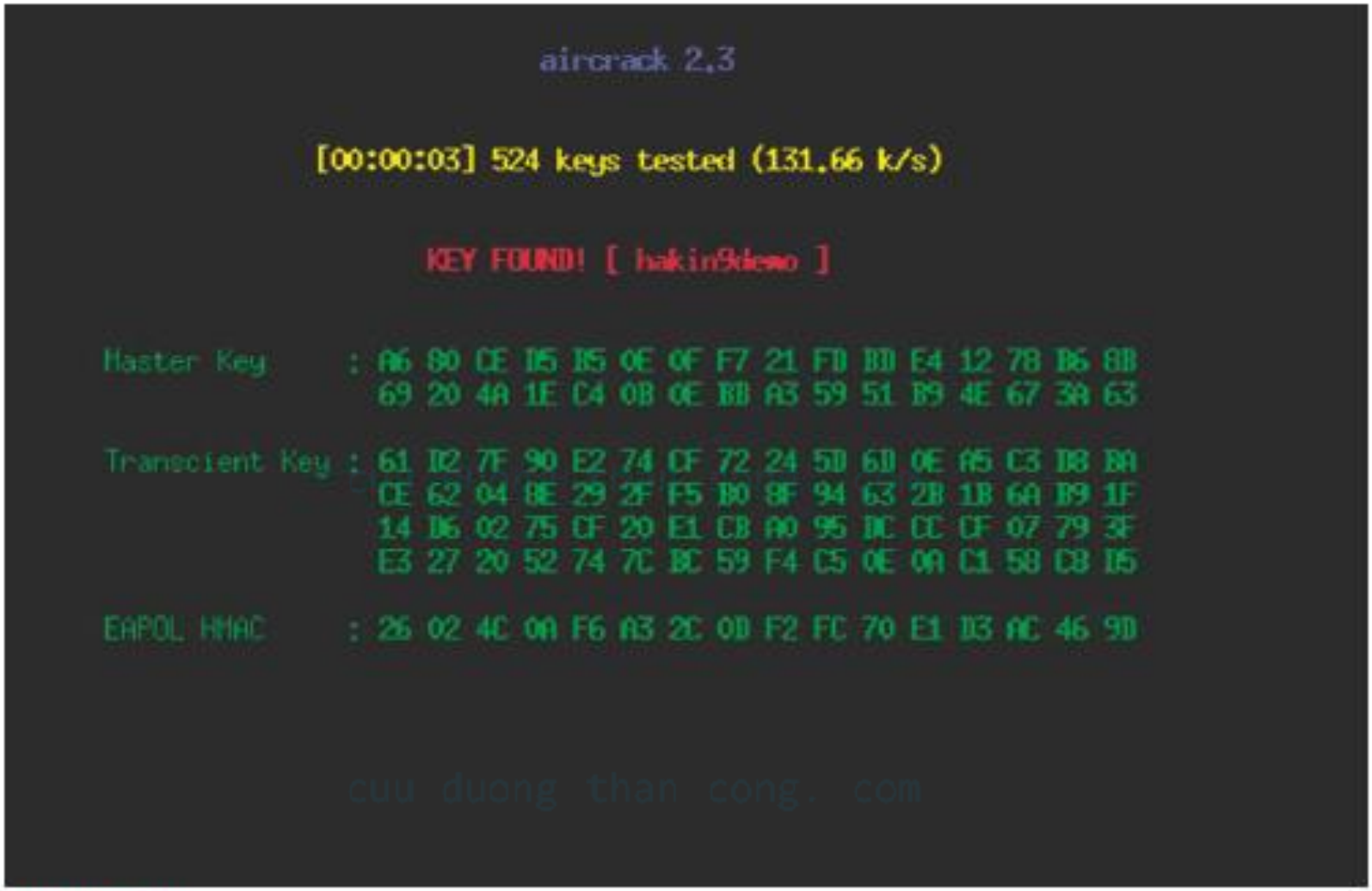


Figure 15. *Weak WPA PSK found with Aircrack*