HỌC VIỆN KỸ THUẬT MẬT MÃ
KHOA AN TOÀN THÔNG TIN
********

# GIAO THỨC AN TOÀN MẠNG

## Bài 5. An toàn trong WLAN

1. Tổng quan về mạng không dây
2. Các cơ chế an toàn trong WLAN
3. Giao thức an toàn WEP
4. Giao thức an toàn WPA
5. Giao thức an toàn WPA2

# Mục tiêu bài học

## ❑Kiến thức

- Nắm được tổng quan về mạng không dây
- Nắm được tổng quan về các giao thức an toàn trong WLAN
- Nắm được cơ bản về các giao thức WEP, WPA, WPA2

## ❑Kỹ năng

- Phân tích hoạt động của các giao thức an toàn mạng không dây WLAN bằng phần mềm Wireshark.
- Thực hành được một số tấn công đơn giản lên các giao thức an toàn WLAN

# Tài liệu tham khảo


1. TS. Nguyễn Quốc Toàn, ThS. Hoàng Sỹ Tương, Giáo trình "Giao thức an toàn mạng máy tính", Học viện Kỹ thuật Mật mã, 2013.
   - Chương 5 "Các giao thức bảo mật mạng không dây" (Trang 106-148)
2. Eric Cole, Ronald L. Krutz, James W. Conley, Brian Reisman, Mitch Ruebush, and Dieter Gollmann, "*Network security fundamentals"*, Wiley 2007.
3. Jie Wang, Zachary A. Kissel, "*Introduction to network security theory and practice",* Wiley, 2015.
4. ThS. Lư Huệ Thu, ThS. Nguyễn Ngọc Đại, giáo trình *"Mạng không dây"* , Đại học Công nghệ, TP HCM, 2015.
   - Chương 5 "Bảo mật mạng WLAN" (Trang 104-108, 115-117)

1. Tổng quan về mạng không dây
2. Các cơ chế an toàn trong WLAN
3. Giao thức an toàn WEP
4. Giao thức an toàn WPA
5. Giao thức an toàn WPA2

# Tổng quan về mạng không dây

- 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.

# Tổng quan về mạng không dây

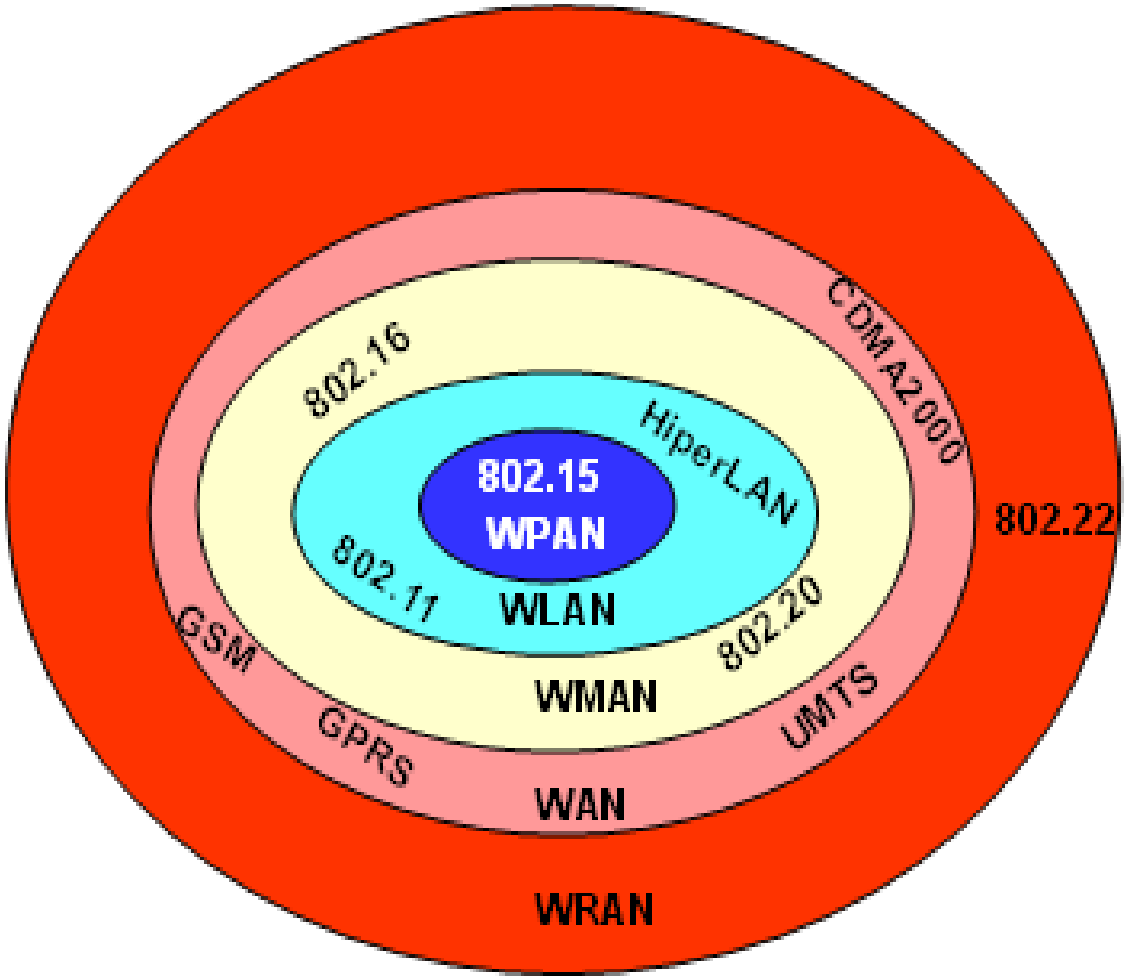
- **Định nghĩa**
  - Mạng không dây (Wireless Network): Là phương thức truyền dữ liệu từ điểm này đến điểm khác không sử dụng đường dây vật lý mà sử dụng sóng vô tuyến, sóng hồng ngoại và vệ tinh.
  - Các kết nối được thiết lập theo chuẩn định sẵn: 802.11, 802.15, 802.16…

# Tổng quan về mạng không dây

- Ưu điểm:
  - Tính di động
  - Tính đơn giản
  - Tính linh hoạt
  - Tiết kiệm chi phí
  - Khả năng mở rộng
- Nhược điểm:
  - Nhiễu
  - Độ an toàn
  - Phạm vi
  - Tốc độ

# Tổng quan về mạng không dây

- Phân loại: dựa trên vùng phủ sóng thì có 5 loại



# Tổng quan về mạng không dây

- Các mô hình mạng WLAN: Mạng 802.11 gồm ba mô hình mạng:
  - Mô hình mạng độc lập IBSS hay còn gọi là mạng Ad-hoc: (Independent Basic Service sets)
  - Mô hình mạng cơ sở: BSS (Basic Service sets)
  - Mô hình mạng mở rộng: ESS (Extended Service sets)

# Tổng quan về mạng không dây

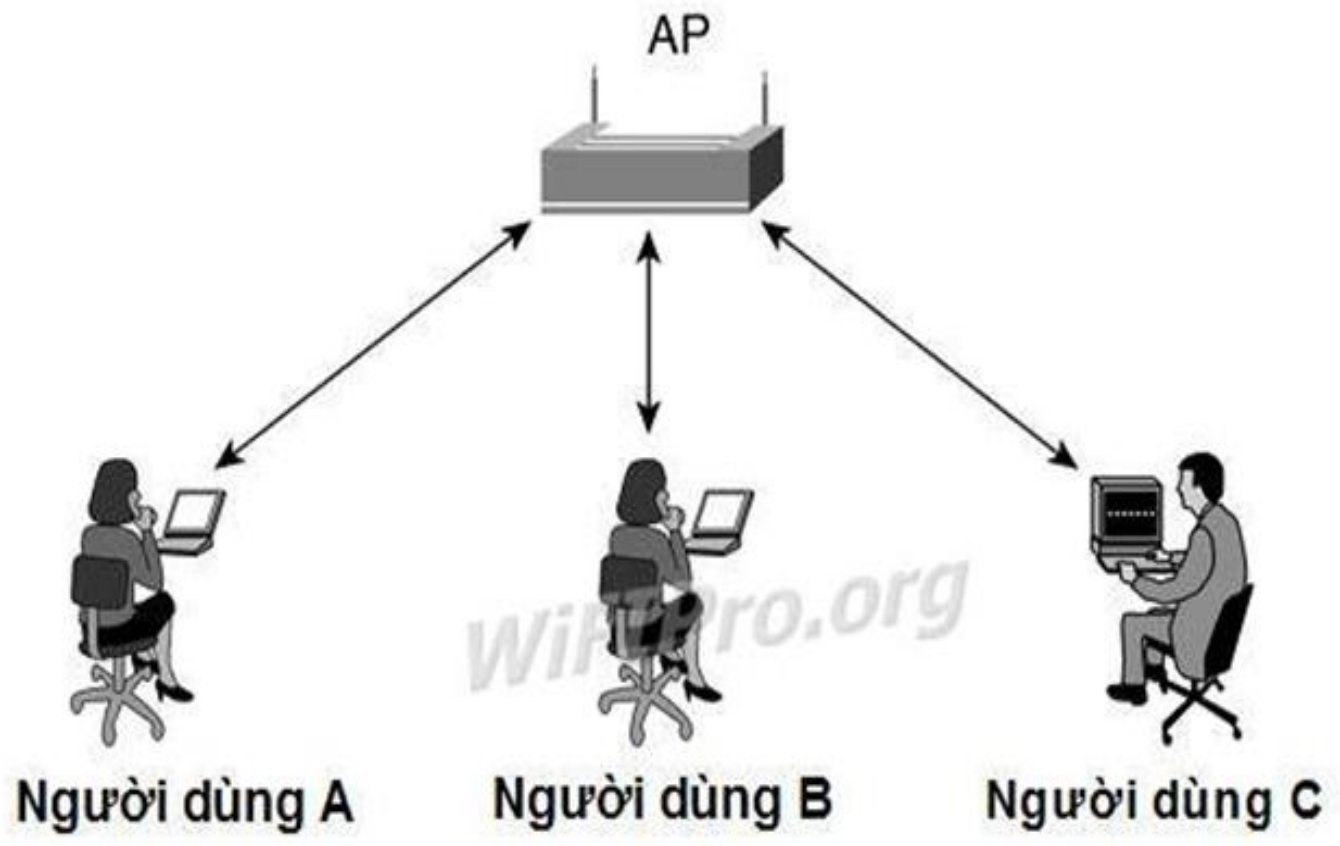
- Các mô hình mạng WLAN:
  - Mô hình mạng Ad-hoc:
    - Các máy trạm liên lạc trực tiếp với nhau mà không phải thông qua AP nhưng phải trong phạm vi cho phép.
    - Các máy trạm có vai trò ngang hàng với nhau. (Peer-to-peer)
    - Khoảng cách liên lạc trong phạm vi 100m.
    - Sử dụng thuật toán Spokesman Election Algorithm.
    - Máy trạm có trang bị card mạng không dây.

# Tổng quan về mạng không dây

- Các mô hình mạng WLAN:
  - Mô hình mạng cơ sở BSS:
    - Bao gồm các điểm truy nhập AP (Access Point) gắn với một đường mạng hữu tuyến và giao tiếp với các thiết bị di động trong vùng phủ sóng của một cell.
    - AP đóng vai trò điều khiển cell và điều khiển lưu lượng tới mạng.
    - Các thiết bị di động không giao tiếp trực tiếp với nhau mà giao tiếp với các AP.

# Tổng quan về mạng không dây

- Các mô hình mạng WLAN:
  - Mô hình mạng cơ sở BSS:

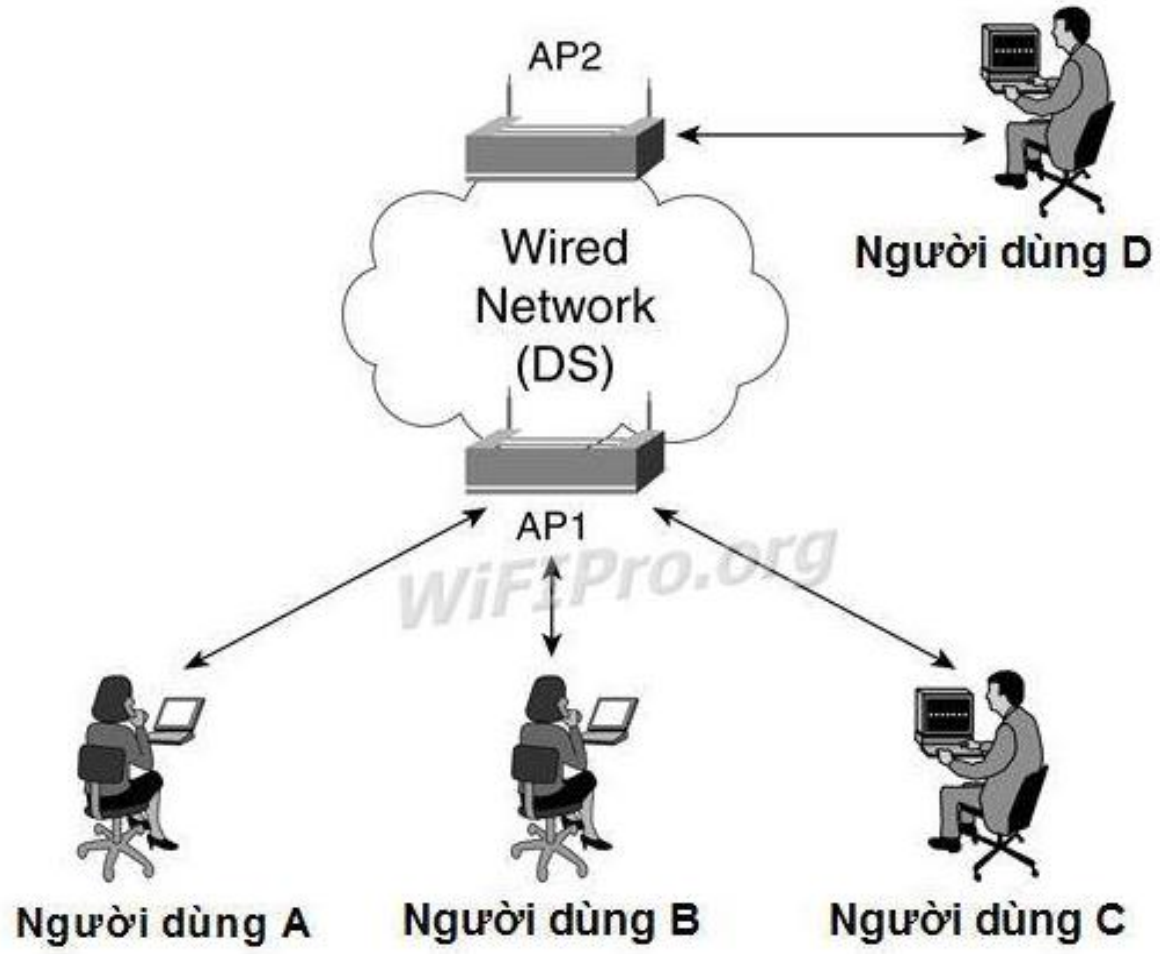


# Tổng quan về mạng không dây

- Các mô hình mạng WLAN:
  - Mô hình mạng mở rộng ESS:
    - Mạng ESS thiết lập hai hay nhiều AP với nhau nhằm mục đích mở rộng phạm vi phủ sóng.
    - Một ESS là một phân vùng mạng logic.
    - Tên mạng của một ESS được gọi là ESSID
    - Các Cell phải chồng lên nhau 10-15% để đạt được thành công trong quá trình chuyển vùng

# Tổng quan về mạng không dây

- Các mô hình mạng WLAN:
  - Mô hình mạng mở rộng ESS:



# Tổng quan về mạng không dây

- Các tấn công vào WLAN
  - Tấn công bị động
    - Kẻ tấn công chỉ lắng nghe trên mạng mà không làm ảnh hưởng tới bất kỳ tài nguyên nào trên mạng.
  - Tấn công chủ động
    - Kẻ tấn công sử dụng các kỹ thuật làm ảnh hưởng tới mạng.

# Tổng quan về mạng không dây

- Tấn công bị động
  - Không tác động trực tiếp vào thiết bị nào trên mạng
  - Không làm cho các thiết bị mạng biết được hoạt động của nó
    - **Phát hiện mạng:** Phát hiện Access Point, phát hiện máy trạm kết nối, phát hiện địa chỉ MAC của các thiết bị tham gia, kênh….
    - **Nghe trộm:** Chặn bắt lưu lượng, phân tích giao thức, nguồn và đích kết nối.

# Tổng quan về mạng không dây

- Tấn công chủ động
  - Là hình thức tấn công tác động trực tiếp lên thông tin, dữ liệu của mạng.
    - Dò tìm mật khẩu AP
    - Giả mạo AP
    - Tấn công người đứng giữa
    - Từ chối dịch vụ

1. Tổng quan về mạng không dây
2. Các cơ chế an toàn trong WLAN
3. Giao thức an toàn WEP
4. Giao thức an toàn WPA
5. Giao thức an toàn WPA2

# Lịch sử phát triển của an toàn WLAN

- Chuẩn IEEE 802.11 là chuẩn đầu tiên, hoạt động ở băng tần 2.4 GHz, tốc độ truyền dẫn 1- 2 Mb/s, cung cấp các phương pháp hỗ trợ cho bảo mật trong việc truyền dữ liệu trong mạng không dây như SSID, xác thực địa chỉ MAC, mã hóa WEP,…(còn có 802.11a, 802.11b, 802.11g, …).
- Chuẩn IEEE 802.11i là mở rộng của chuẩn 802.11 bằng cách cung cấp một mạng RSN (Robust Security Network) với hai giao thức: Bắt tay bốn bước và Trao đổi khóa nhóm.
- Chuẩn IEEE 802.1x được phát triển để nâng cao độ an toàn cho mạng không dây nhằm đảm bảo toàn vẹn dữ liệu và xác thực người dùng

# Lịch sử phát triển của an toàn WLAN

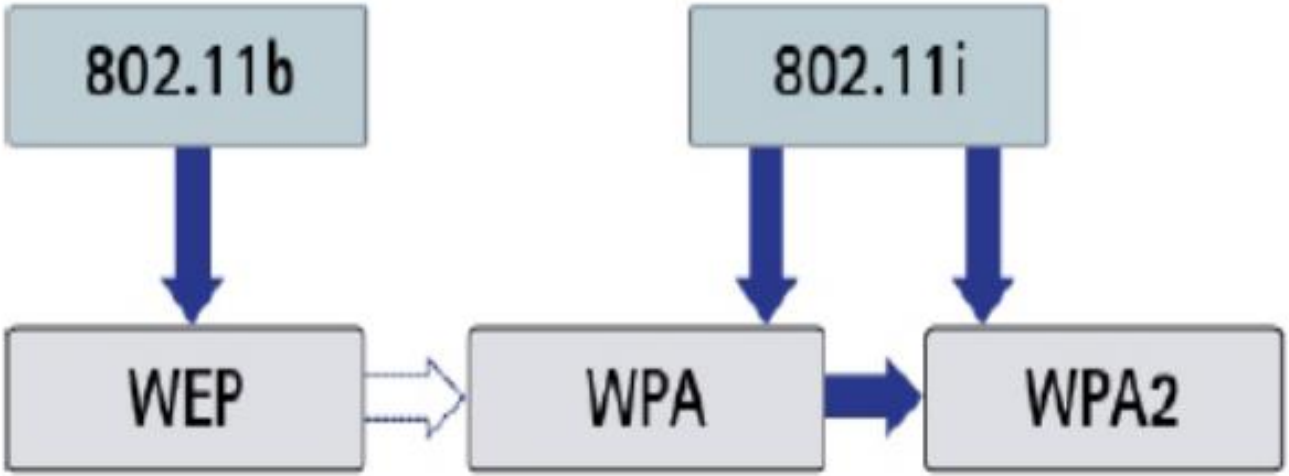
- 1997, chuẩn 802.11 chỉ cung cấp
  - SSID (Service Set Identifier)
  - Lọc trên địa chỉ MAC
  - WEP (Wired Equivalent Privacy)
- 2001
  - Fluhrer, Mantin và Shamir đã chỉ ra một số điểm yếu trong WEP
  - IEEE bắt đầu khởi động nhóm i (802.11i)

# Lịch sử phát triển của an toàn WLAN

- 2003
  - Wi-Fi Protected Access(WPA) được giới thiệu
  - Là một giải pháp tạm thời cho WEP
  - Một phần của IEEE 802.11i
- 2004
  - WPA2 được giới thiệu
  - Nó dựa trên chuẩn IEEE 802.11i
  - Được phê chuẩn vào 25/06/2004
- 2018:
  - Wi-Fi Alliance công bố chuẩn WPA3,

# Lịch sử phát triển của an toàn WLAN

- WPA thực hiện một tập hợp con của một bản dự thảo của 802.11i
- Wi-Fi Alliance đề cập đến việc triển khai đầy đủ các chuẩn 802.11i như **WPA2** , được gọi là **RSN**.



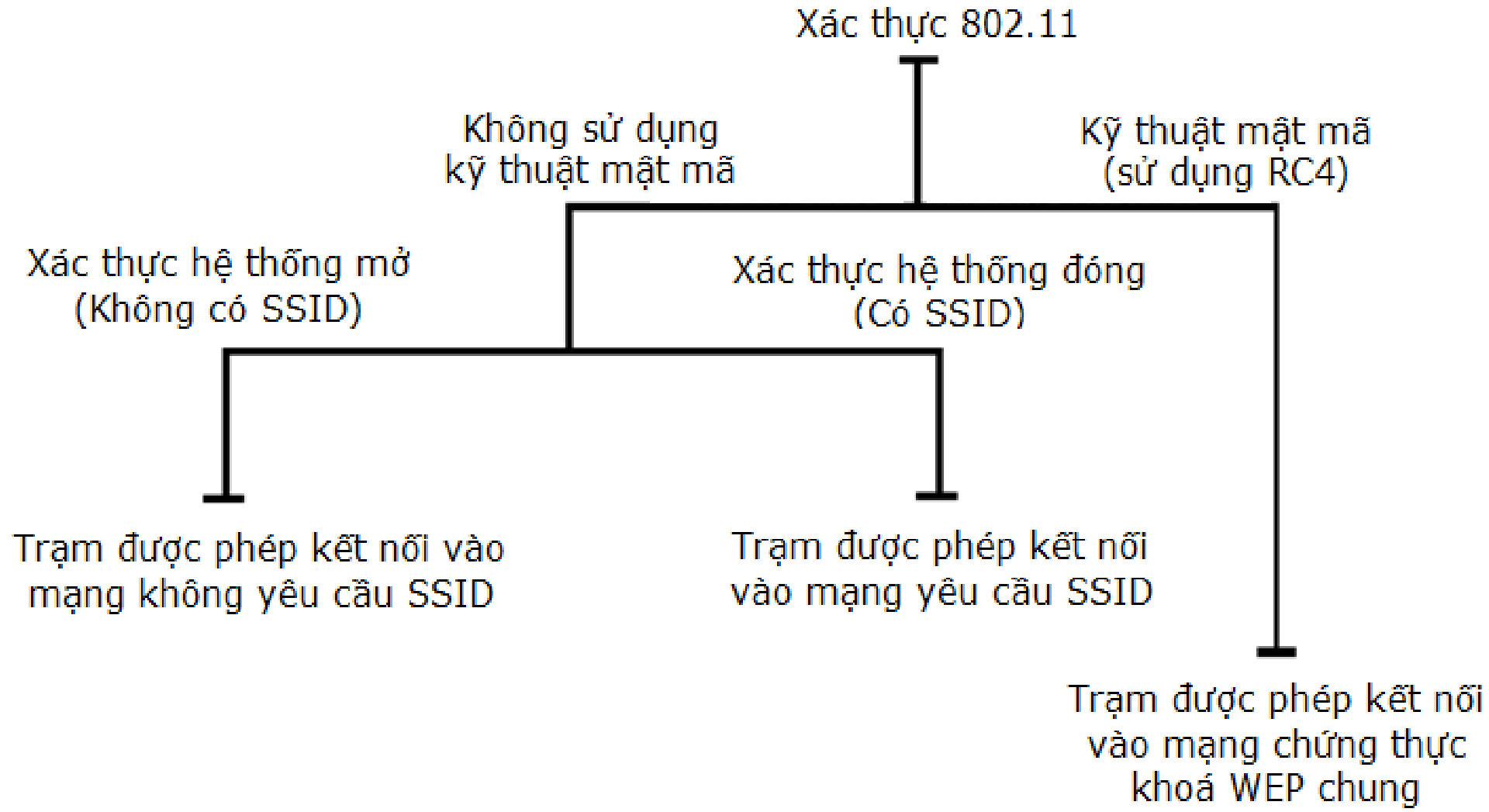
# Các cơ chế an toàn trong WLAN

- PHƯƠNG THỨC XÁC THỰC
  - Xác thực hệ thống mở
  - Xác thực khóa chung (Shared-key)
  - Xác thực địa chỉ MAC
  - Xác thực mở rộng EAP
- PHƯƠNG THỨC MÃ HOÁ
  - Mã hoá trong WEP
  - Mã hoá trong WPA/WPA2
- PHƯƠNG THỨC KIỂM SOÁT TRUY CẬP
  - Kiểm soát dựa vào SSID
  - Kiểm soát dựa vào địa chỉ MAC
  - Kiểm soát dựa vào giao thức

# PHƯƠNG THỨC XÁC THỰC

- Xác thực hệ thống mở (Open Authentication)
- Xác thực khóa chia sẻ trước (Pre-shared key Authentication)
- Xác thực địa chỉ MAC
- Xác thực mở rộng EAP

# PHƯƠNG THỨC XÁC THỰC

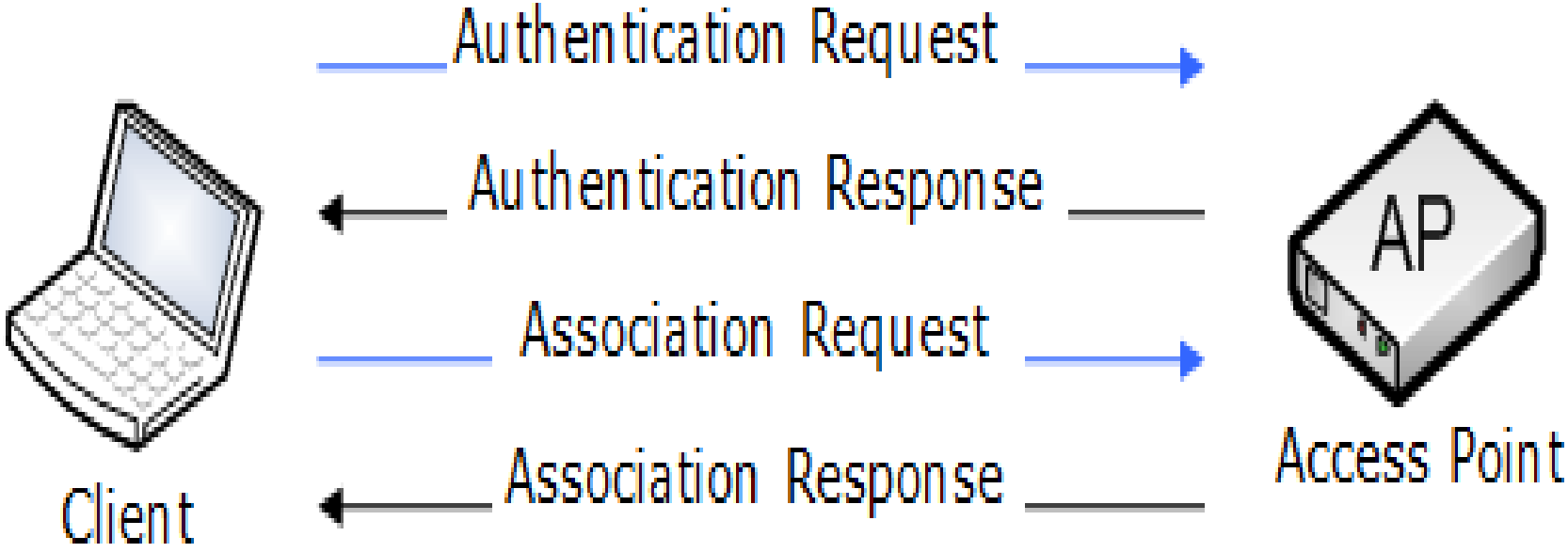


# PHƯƠNG THỨC XÁC THỰC

- *Xác thực hệ thống mở (Open Authentication):*
  - Các STA không cần cung cấp chứng thực của mình cho AP trong quá trình xác thực. Vì vậy bất kỳ một STA nào cũng có thể xác thực chính nó với AP và sau đó sẽ thực hiện phiên gắn kết với AP.
  - Xác thực bất cứ ai yêu cầu xác thực
  - Thường được dùng ở những nơi truy cập công cộng như Internet café, nhà ga, sân bay.
  - Được cài đặt mặc định trong các thiết bị WLAN.

# Các cơ chế an toàn trong WLAN

- *Xác thực hệ thống mở (Open Authentication):*




– Client sẽ gửi yêu cầu xác thực đến AP

– AP đáp trả bằng thông điệp đã xác thực

– Sau khi Client đã được xác thực thì sẽ gắn kết với AP

# PHƯƠNG THỨC XÁC THỰC

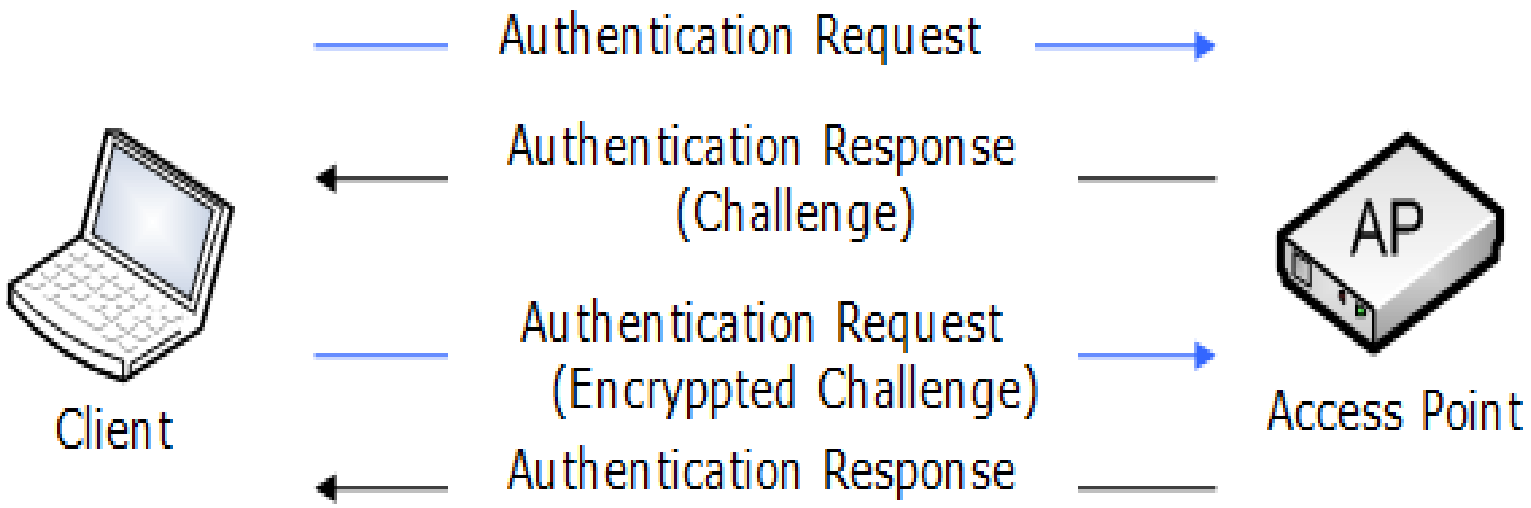
- Xác thực hệ thống mở (Open Authentication)
- Xác thực khóa chia sẻ trước (Pre-shared key Authentication)
- Xác thực địa chỉ MAC
- Xác thực mở rộng EAP

# PHƯƠNG THỨC XÁC THỰC

- *Xác thực khóa chia sẻ trước (Pre-shared key Authentication)*
  - Khóa chia sẻ sẽ được sử dụng để xác thực thông qua một giai đoạn bắt tay bốn bước như sau:
    - STA gửi một yêu cầu xác thực tới AP.
    - AP gửi trả một thông báo “challenge” ở dạng rõ.
    - STA phải mã hóa “challenge” sử dụng khóa WEP đã được chia sẻ và gửi bản mã cho AP.
    - AP sẽ giải mã và so sánh với “challenge” ban đầu, phụ thuộc vào kết quả so sánh này, AP sẽ chấp nhận xác thực STA hay không.

# PHƯƠNG THỨC XÁC THỰC

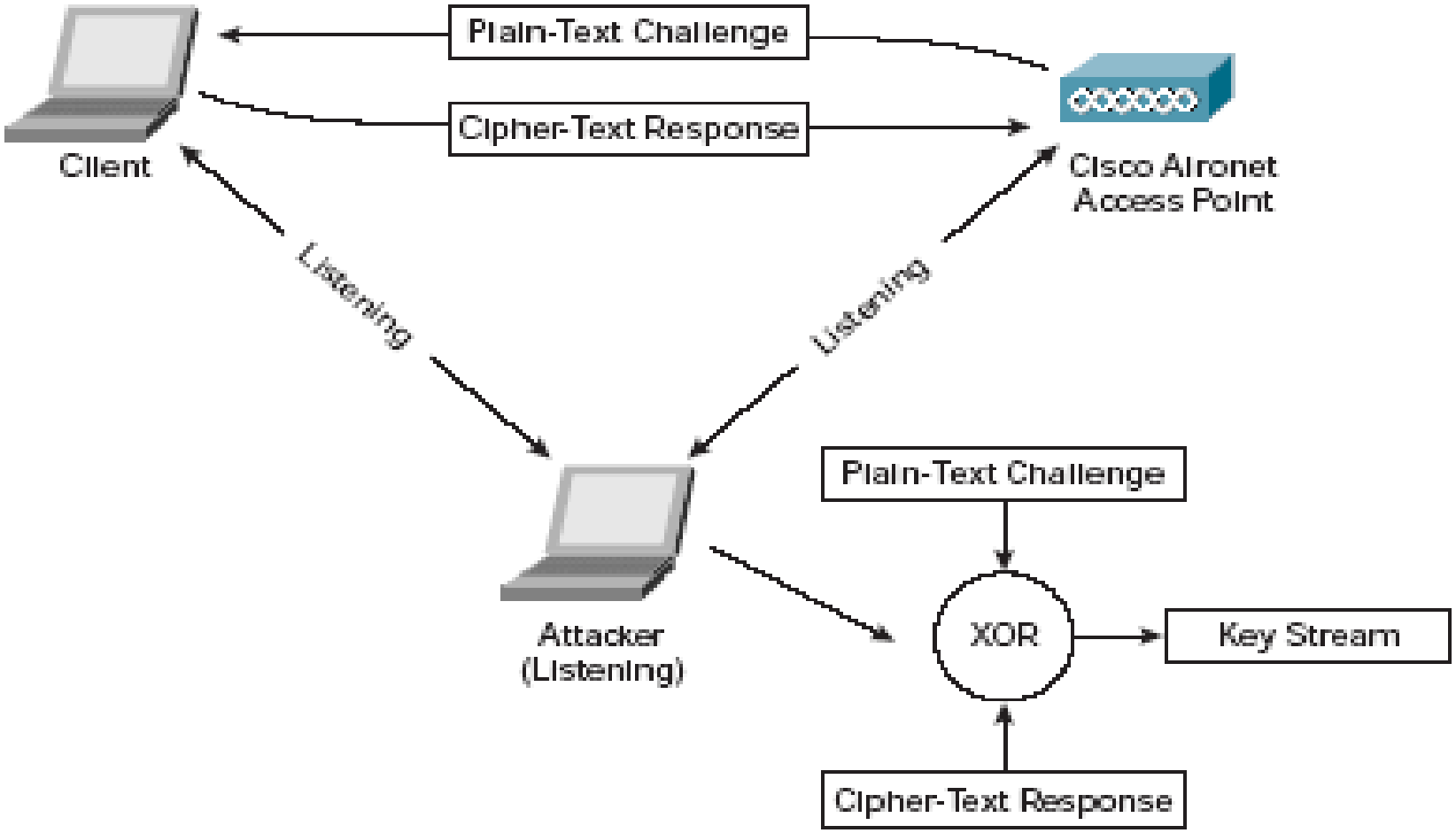
- *Xác thực khóa chia sẻ trước (Pre-shared key Authentication)*




Phương pháp này bắt buộc phải dùng WEP, khóa WEP được dùng để xác thực và mã hóa dữ liệu, đây chính là kẽ hở để hacker có cơ hội thâm nhập mạng. Hacker sẽ thu cả hai tín hiệu, văn bản chưa mã hóa do AP gửi và văn bản đã mã hóa do Client gửi để giải mã khóa WEP.

# PHƯƠNG THỨC XÁC THỰC

- *Xác thực khóa chia sẻ trước (Pre-shared key Authentication)*
  - Dễ dàng sniff khóa chung (stream key)



# PHƯƠNG THỨC XÁC THỰC

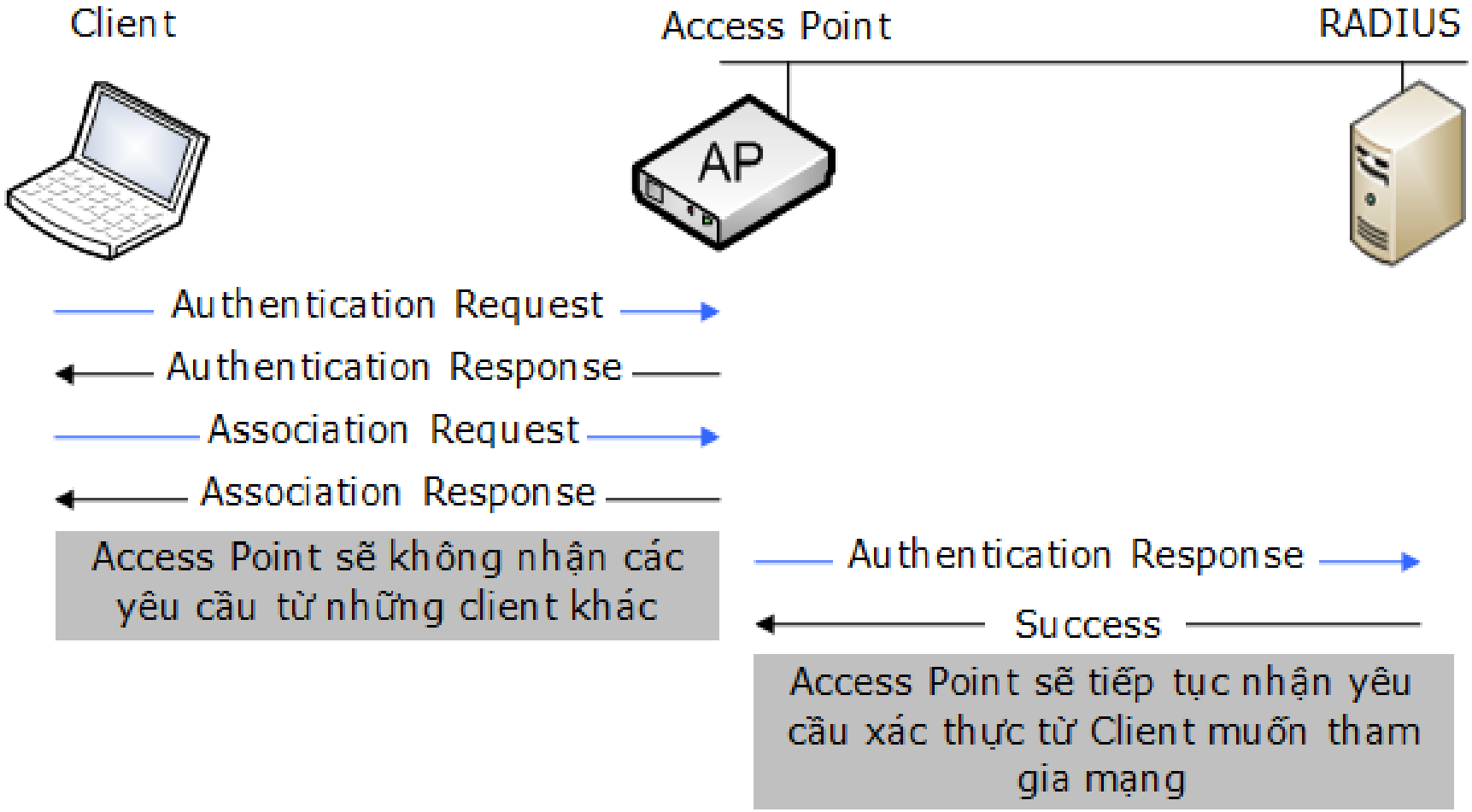
- Xác thực hệ thống mở (Open Authentication)
- Xác thực khóa chia sẻ trước (Pre-shared key Authentication)
- Xác thực địa chỉ MAC
- Xác thực mở rộng EAP

# PHƯƠNG THỨC XÁC THỰC

- *Xác thực địa chỉ MAC:*
  - AP sẽ gửi địa chỉ MAC của Client cho RADIUS Server, Server này sẽ kiểm tra địa chỉ MAC này với danh sách địa chỉ MAC được cho phép.
  - Nếu không có RADIUS Server, có thể tạo ra một danh sách địa chỉ MAC trên AP.
  - Vì các địa chỉ MAC được truyền dưới dạng văn bản, do đó có thể bằng cách dò sóng, những kẻ xâm nhập có thể tạo ra địa chỉ MAC hợp lệ truy cập vào mạng.

# PHƯƠNG THỨC XÁC THỰC

- *Xác thực địa chỉ MAC:*



# PHƯƠNG THỨC XÁC THỰC

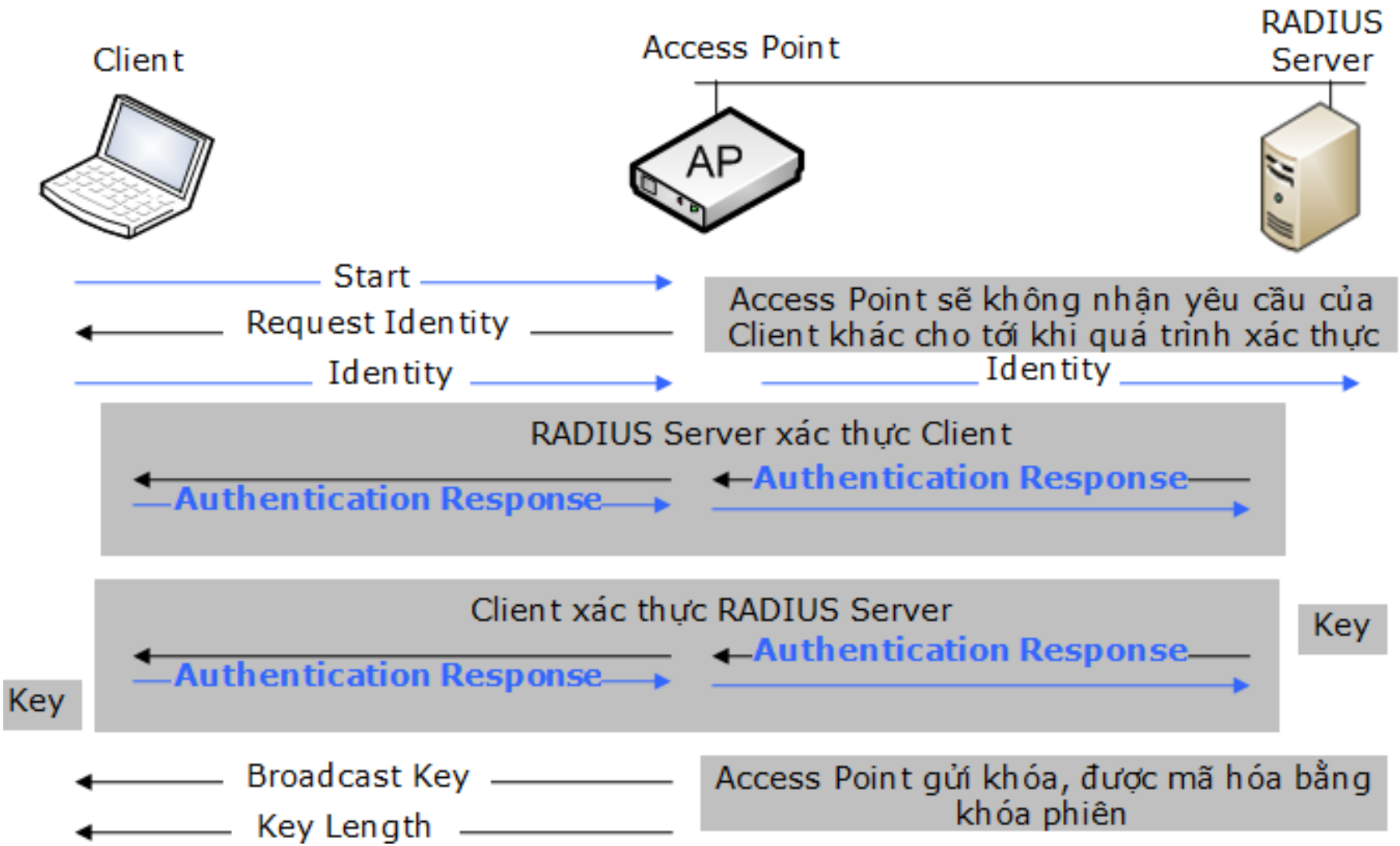
- Xác thực hệ thống mở (Open Authentication)
- Xác thực khóa chia sẻ trước (Pre-shared key Authentication)
- Xác thực địa chỉ MAC
- Xác thực mở rộng EAP

# Các cơ chế an toàn trong WLAN

- *Xác thực mở rộng EAP*
  - EAP (Extensible Authentication Protocol) được định nghĩa trong RFC 2284.
  - Cung cấp xác thực hai chiều, có nghĩa là mạng (RADIUS Server) sẽ xác thực người sử dụng và người sử dụng cũng xác thực mạng (RADIUS Server).
  - Sau khi quá trình xác thực hoàn tất, RADIUS Server và Client sẽ xác định (trao đổi) khóa WEP, Client sẽ sử dụng khóa này để bắt đầu phiên kết nối ($K_S$).
  - Trong khi đó, RADIUS Server sẽ mã hóa và gửi khóa WEP đó được gọi là khóa phiên ($K_S$) đến AP. AP sẽ sử dụng $K_S$ để mã hóa khóa quảng bá (broadcast key) và gửi đến Client. Client và AP sử dụng khóa này trong suốt một phiên làm việc.

# Các cơ chế an toàn trong WLAN

- *Xác thực mở rộng EAP*



# Các cơ chế an toàn trong WLAN

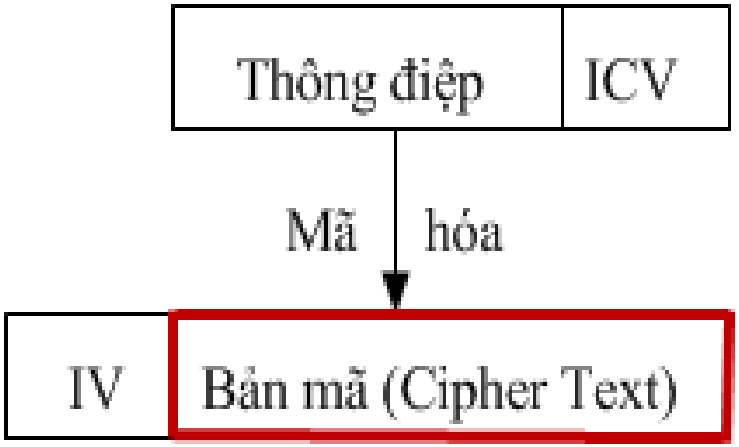
- PHƯƠNG THỨC XÁC THỰC
  - Xác thực hệ thống mở
  - Xác thực khóa chung (Shared-key)
  - Xác thực địa chỉ MAC
  - Xác thực mở rộng EAP
- PHƯƠNG THỨC MÃ HOÁ
  - Mã hoá trong WEP
  - Mã hoá trong WPA/WPA2
- PHƯƠNG THỨC KIỂM SOÁT TRUY CẬP
  - Kiểm soát dựa vào SSID
  - Kiểm soát dựa vào địa chỉ MAC
  - Kiểm soát dựa vào giao thức

# PHƯƠNG THỨC MÃ HOÁ

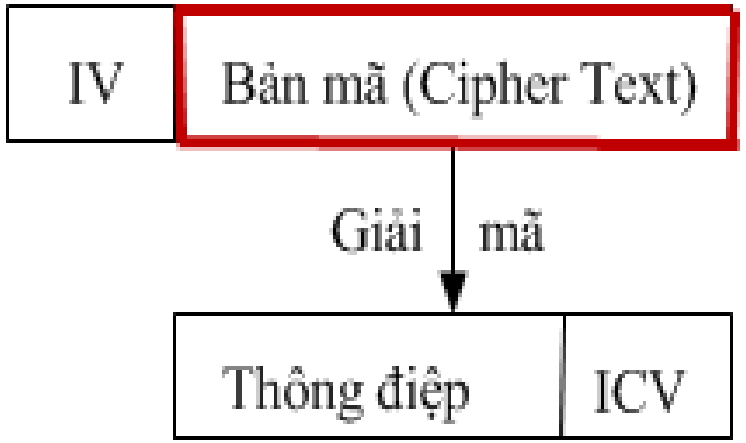
- B1: Trước khi gửi thông điệp lên mạng, hệ thống sẽ tính giá trị ICV (Integrity message digest) và chèn vào cuối thông điệp.
- B2: Tiếp đến dùng các thuật toán mã hóa để mã hoá thông điệp (gồm thông điệp gốc và ICV).
- B3: Cuối cùng là thêm phần Header vào thông điệp và truyền đến người nhận.

# PHƯƠNG THỨC MÃ HOÁ

- Mã hóa thông điệp




Đóng gói và gởi thông điệp




Nhận và giải mã thông điệp

# PHƯƠNG THỨC MÃ HOÁ

- Một số phương thức mã hoá trong WLAN được dùng trong các giao thức: WEP, WPA, WPA2.

# PHƯƠNG THỨC MÃ HOÁ

| | WEP | WPA | WPA2 |
|---|---|---|---|
| Mã hoá | RC4 | RC4 | AES |
| Luân phiên khoá | Không | Khoá phiên động | Khoá phiên động |
| Phân phối khoá | Gán bằng tay trên mỗi thiết bị | Khả năng phân phối tự động | Khả năng phân phối tự động |
| Xác thực | Sử dụng khoá WEP để xác thực | Có thể dùng802.1x & EAP | Có thể dùng 802.1x & EAP |

# Các cơ chế an toàn trong WLAN

- PHƯƠNG THỨC XÁC THỰC
  - Xác thực hệ thống mở
  - Xác thực khóa chung (Shared-key)
  - Xác thực địa chỉ MAC
  - Xác thực mở rộng EAP
- PHƯƠNG THỨC MÃ HOÁ
  - Mã hoá trong WEP
  - Mã hoá trong WPA/WPA2
- PHƯƠNG THỨC KIỂM SOÁT TRUY CẬP
  - Kiểm soát dựa vào SSID
  - Kiểm soát dựa vào địa chỉ MAC
  - Kiểm soát dựa vào giao thức

# PHƯƠNG THỨC KIỂM SOÁT TRUY CẬP

- Kiểm soát dựa vào SSID
- Kiểm soát dựa vào địa chỉ MAC
- Kiểm soát dựa vào giao thức

1. Tổng quan về mạng không dây
2. Các cơ chế an toàn trong WLAN
3. Giao thức an toàn WEP
4. Giao thức an toàn WPA
5. Giao thức an toàn WPA2

# Các giao thức an toàn cho WLAN

- 802.11
  - WEP (Wired Equivalent Privacy):
    + CRC-32
    + RC4
- 802.11i
  - WPA (Wi-fi Protected Access):
    + TKIP (Temporal Key Integrity Protocol), Michael-64
    + RC4
    + 802.1x/EAP
  - WPA2 = RSN:
    + CCMP (Counter Mode CBC-MAC Protocol)
    + AES/TKIP (RC4, Michael)
    + 802.1X/EAP (TKIP, EAP-TLS)

# Giao thức an toàn WEP

- WEP-Wired Equivalent Privacy
  - Chuẩn 802.11 cung cấp tính riêng tư cho dữ liệu bằng giao thức WEP. WEP dựa trên mã dòng RC4 (Ron's code 4) được Ron Rivest thuộc hãng RSA Security Inc phát triển.
  - Một giá trị có tên Initialization Vector (IV) được sử dụng để cộng thêm với khóa nhằm tạo ra khóa khác nhau mỗi lần mã hóa.
  - Hiện nay, trên Internet đã sẵn có những công cụ có khả năng tìm khóa WEP như AirCrack, AirSnort, dWepCrack, WepAttack, WepCrack, WepLab.

# Giao thức an toàn WEP

- Xác thực:
  - Xác thực mở
  - Xác thực khóa chia sẻ
- Toàn vẹn dữ liệu
  - Sử dụng mã kiểm tra CRC-32
- Mã hóa
  - Sử dụng RC4, Khóa dài 40 bit, hoặc 104 bit
  - IV dài 24 bit
- Quản lý khóa:
  - Sử dụng khóa chia sẻ trước, không có trao đổi khóa tự động, không có cách quản lý cơ sở khóa an toàn, không làm mới khóa một cách an toàn.
- Vấn đề chống tấn công phát lại:
  - Không chống được

# Giao thức an toàn WEP

- Xác thực:
  - Gồm hai loại xác thực:
    - Xác thực mở
    - Xác thực khóa chia sẻ
  - Các STA cần xác thực với AP (nhưng AP không xác thực lại với STA)
  - Hai bên chia sẻ chung một khóa bí mật
  - Khóa này phải được thực hiện bằng tay
  - Khóa này là khóa tĩnh (rất hiếm khi được thay đổi)

# Giao thức an toàn WEP

- Xác thực:
  - Việc xác thực dựa trên giao thức thách thức-phản hồi đơn giản, gồm 4 bước:
    - B1: STA => AP: Yêu cầu xác thực
    - B2: AP => STA: Thách thức xác thực (r) // r là chuỗi 128 bits
    - B3: STA => AP: Phản hồi xác thực ($e_K(r)$).
    - B4: AP => STA: xác thực thành công/thất bại
  - K = RC4(IV + $K_{Shared}$), $K_{Shared}$ là khóa chia sẻ trước giữa AP và STA.

# Giao thức an toàn WEP

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

# Giao thức an toàn WEP

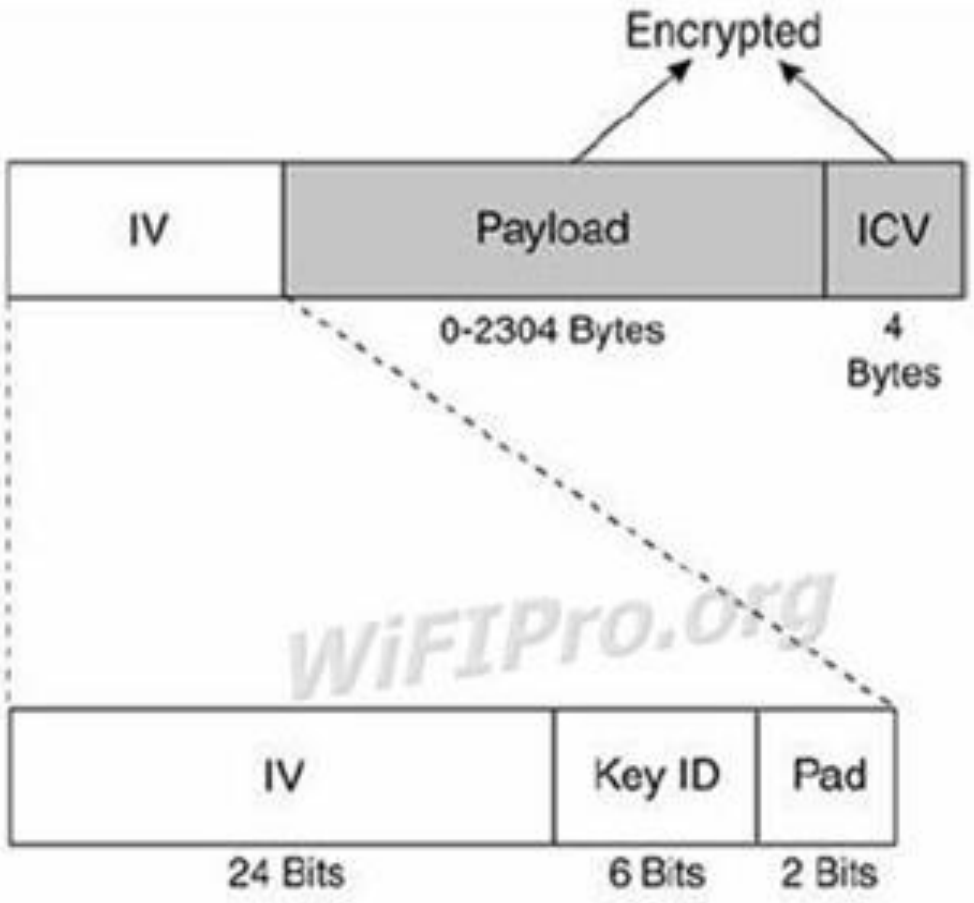
- Mã hóa: Dựa trên mã dòng RC4
  - Hoạt động: Đối với mỗi thông điệp được gửi đi:
    - RC4 được khởi tạo với khóa chia sẻ (giữa STA và AP)
    - RC4 tạo ra một chuỗi byte giả ngẫu nhiên (key stream). (Key stream = RC4 (IV + $K_{pre\text{-}shared}$))
    - Chuỗi key stream này được XOR với thông điệp
  - RC4 được khởi tạo với khóa chia sẻ và một giá trị IV (giá trị khởi đầu).
    - Khóa chia sẻ là giống nhau đối với mỗi thông điệp.
    - 24-bit IV thay đổi cho mỗi thông điệp

# Giao thức an toàn WEP

- Toàn vẹn:
  - Tính toàn vẹn trong WEP được bảo vệ bằng giá trị CRC (Cyclic Redundancy Check) được mã hóa.
  - Giá trị ICV (integrity check value) được tính toán và được gắn vào thông điệp.
  - Cả thông điệp và ICV được mã hóa cùng nhau.

# Giao thức an toàn WEP

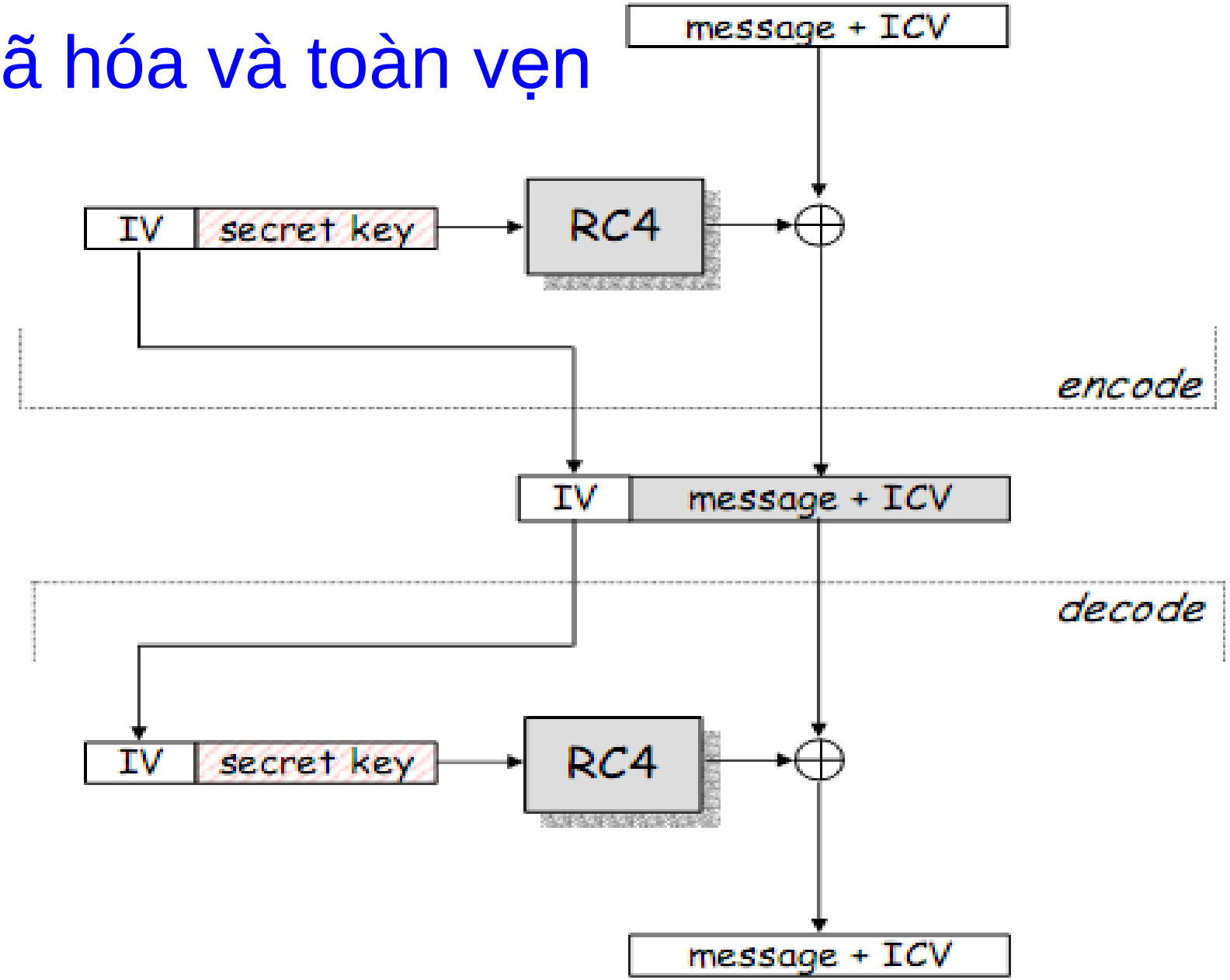
- + IV là một giá trị có chiều dài 24 bit và được chuẩn IEEE 802.11 đề nghị (không bắt buộc) phải thay đổi theo từng gói dữ liệu.
- + Vì máy gửi tạo ra IV không theo định luật hay tiêu chuẩn, IV bắt buộc phải được gửi đến máy nhận ở dạng không mã hóa.




Frame được mã hóa bởi WEP

# Giao thức an toàn WEP

- Mã hóa và toàn vẹn



# CÁC ĐIỂM YẾU CỦA WEP

- Xác thực chỉ là một chiều:
  - AP không được xác thực bởi STA
  - STA có thể gắn kết với một AP giả mạo
- Cùng một khóa chia sẻ giống nhau được dùng cho cả mã hóa và xác thực:
  - Điểm yếu này có thể được dùng để bẻ khóa
- Không có khóa phiên nào được thiết lập trong suốt quá trình xác thực
  - Kiểm soát truy cập không được tiếp tục
  - Khi một STA đã được xác thực và gắn kết với AP thì Attacker có thể gửi thông điệp sử dụng đ/c MAC của STA đó
  - Việc phát lại các thông điệp của STA vẫn có thể xảy ra

# CÁC ĐIỂM YẾU CỦA WEP

- STA có thể bị giả mạo
- Không có bảo vệ chống tấn công phát lại:
  - Giá trị IV không được tăng sau mỗi thông điệp
- Kẻ tấn công có thể thao tác trên các thông điệp mặc dù đã có cơ chế ICV và mã hóa.
- Sử dụng lại IV
  - Không gian IV quá nhỏ
  - Nhiều IV được khởi tạo bằng 0 ở giai đoạn khởi đầu
- Các khóa RC4 yếu

# Giao thức an toàn WEP

- 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.

1. Tổng quan về mạng không dây
2. Các cơ chế an toàn trong WLAN
3. Giao thức an toàn WEP
4. Giao thức an toàn WPA
5. Giao thức an toàn WPA2

# Giao thức an toàn WPA

- Wi-fi allience cùng với IEEE đã cùng nhau xây dựng một giải pháp bảo mật mạnh hơn WEP.
- Nó được tạo ra để thay thế WEP vì WEP đã trở nên lỗi thời vì dễ bị phá để tìm ra khóa.
- Vào 2003, WPA (*Wi-Fi Protected Access*) ra đời như một giải pháp bảo mật tăng cường cho WLAN.
- WPA thực thi một tập con của 802.11i, là bản thảo của 802.11i.
- WPA cung cấp bảo mật cho tất cả các phiên bản đã tồn tại của các thiết bị WLAN 802.11: a, b,

# Giao thức an toàn WPA

- Gồm hai chế độ hoạt động:
  - WPA doanh nghiệp: TKIP/MIC ; 802.1X/EAP
    - Yêu cầu một máy chủ xác thực
    - Sử dụng giao thức RADIUS để xác thực và phân phối khóa.
    - Tập trung vào việc quản lý thông tin người dùng.
  - WPA cá nhân: TKIP/MIC; PSK
    - Không yêu cầu máy chủ xác thực.
    - “Khóa chia sẻ” được dùng để xác thực với AP.

# Giao thức an toàn WPA

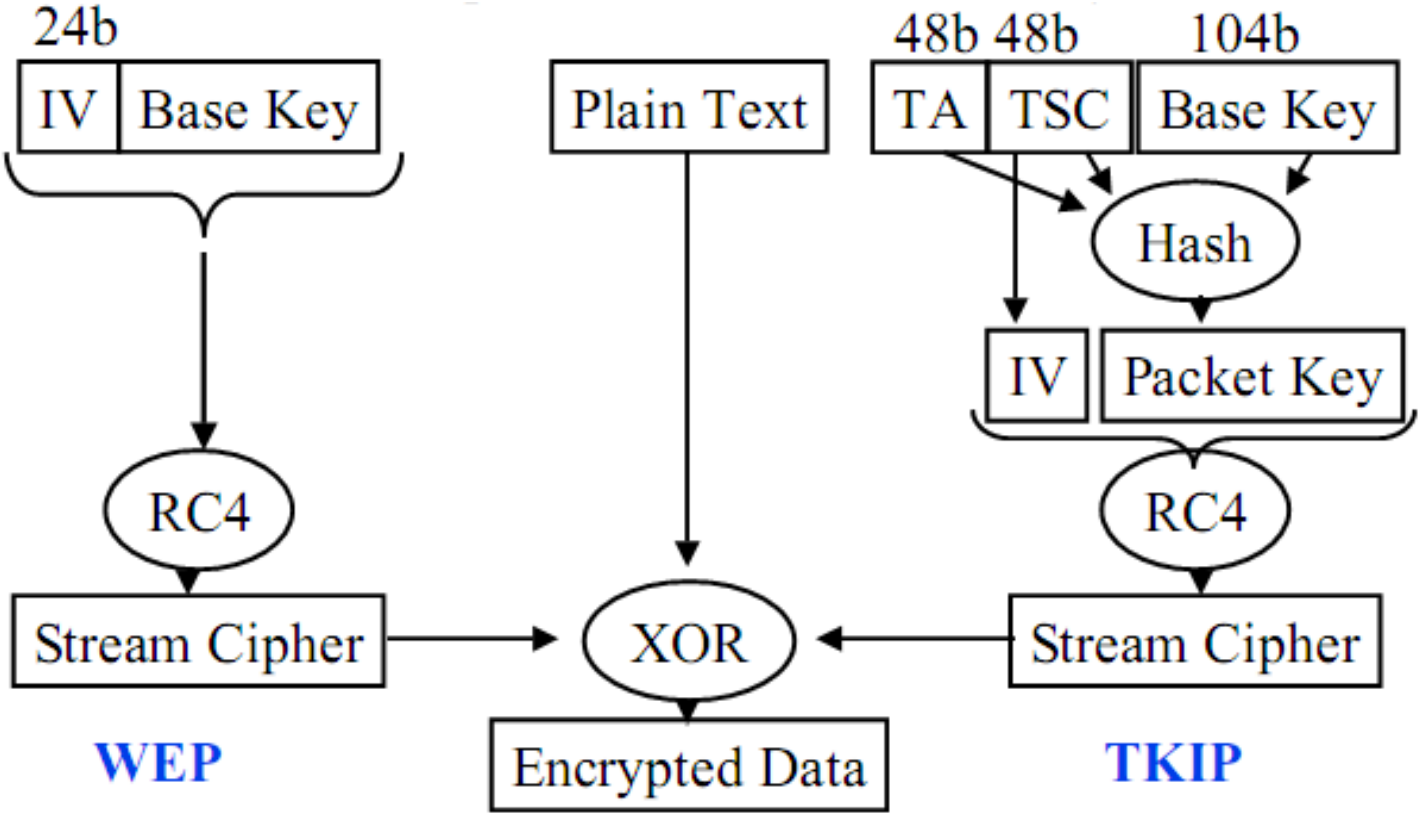
- Mã hóa:
  - Sử dụng TKIP (bắt buộc) để mã hóa:
    - Thuật toán mã: RC4 => Đã vá những lỗ hổng của WEP
    - IV dài hơn (48 bit) + Hàm trộn khóa (Lấy ra một khóa cho mỗi gói tin) + MIC (8 byte => Michael)
- Xác thực và quản lý khóa:
  - 802.1x kết hợp với EAP; PSK
- Toàn vẹn:
  - Thuật toán Michael (64 bit) => MIC
- Chống tấn công phát lại:
  - 48bit bộ đếm chuỗi TKIP (TSC) được dùng để sinh IV và tránh tấn công phát lại. IV được đặt lại bằng 0 khi thiết lập khóa mới.
- Các khóa khác nhau được dùng cho quá trình xác thực, mã hóa, toàn vẹn.
- Ngăn chặn việc tái sử dụng IV bằng cách thay đổi khóa WEP trong chu trình IV.

# Giao thức an toàn WPA

- Giao thức TKIP (Temporary Key Integrity Protocol):
  - Là giải pháp của IEEE được phát triển năm 2004.
  - Là một nâng cấp cho WEP nhằm vá những vấn đề bảo mật trong cài đặt mã dòng RC4 trong WEP.
  - TKIP dùng hàm băm (hashing) IV để chống lại việc giả mạo gói tin, nó cũng cung cấp phương thức để kiểm tra tính toàn vẹn của thông điệp MIC (message integrity check) để đảm bảo tính chính xác của gói tin.
  - TKIP sử dụng khóa động bằng cách đặt cho mỗi frame một chuỗi số riêng để chống lại dạng tấn công giả mạo.

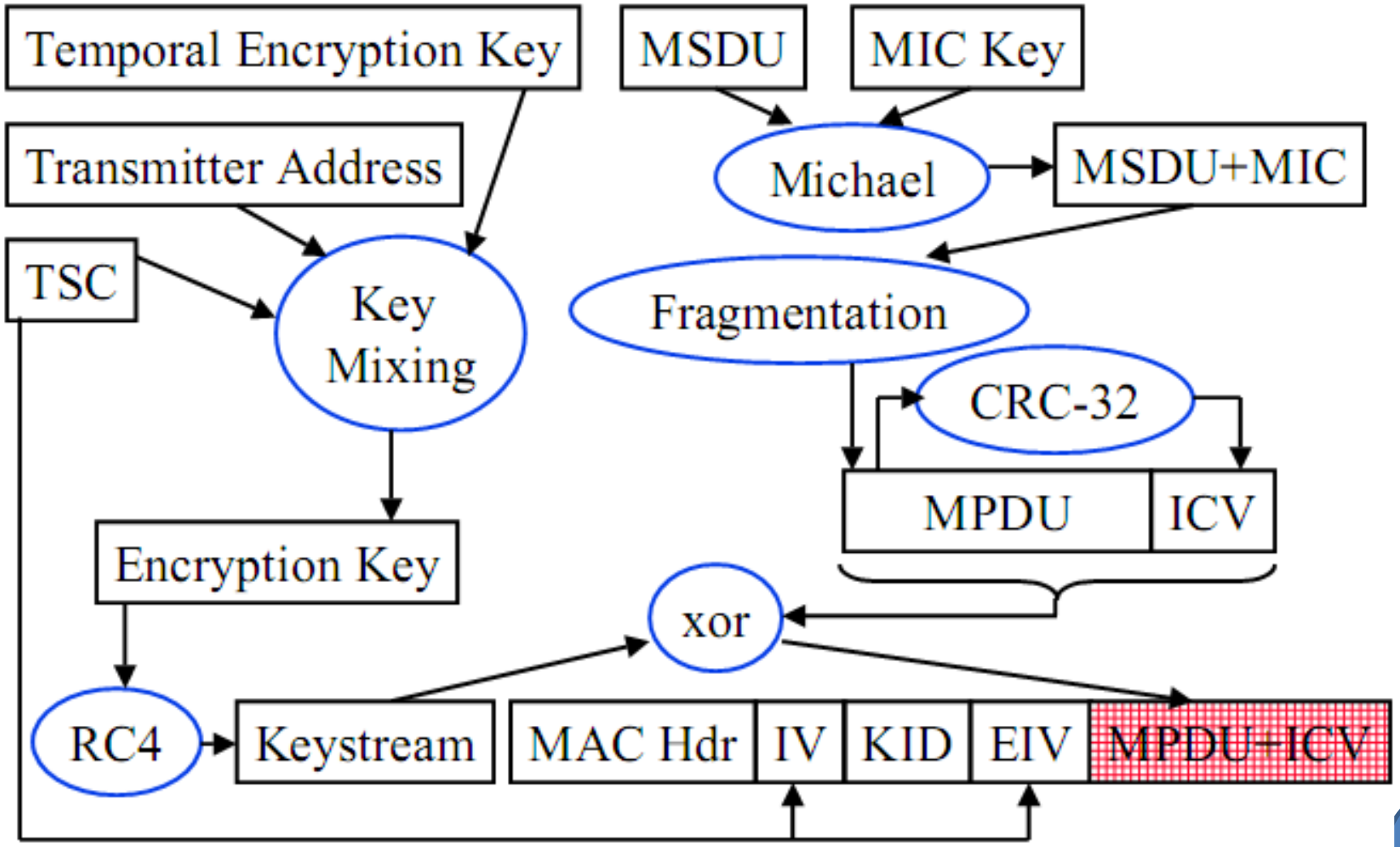
# Giao thức an toàn WPA

- Giao thức TKIP vs WEP:
  - WEP: Khóa cơ sở (base key) là giống nhau cho tất cả các gói tin
  - TKIP: Một khóa mới (packet key) sẽ được đưa ra cho mỗi một gói tin từ địa chỉ nguồn, 48 bit TKIP Seq counter (TSC), và 104 bit khóa cơ sở



# Giao thức an toàn WPA

- Truyền tin TKIP (tổng hợp)



# Giao thức an toàn WPA

- Giao thức TKIP
  - 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 thông điệp (MIC)*:
      - Thêm MIC ở cuối của mỗi thông điệp bản rõ nhằm đảm bảo thông điệp đó không bị giả mạo.
      - có thể thực hiện trên phần mềm chạy trên các CPU tốc độ thấp.
    - *Cơ chế đánh số thứ tự IV (IV sequencing discipline)*
    - *Hàm trộn khóa trên mỗi gói (Key-Mixing Function)*
      - Để làm mất sự tương quan giữa các IV với các khóa yếu
    - *Phân phối khóa (re-keying mechanism):* Để cung cấp các khóa mã hóa và khóa toàn vẹn tươi, chống lại các tấn công tái sử dụng khóa.

# Giao thức an toàn WPA

- Các nâng cấp của TKIP đối với các điểm yếu của WEP

| Điểm yếu | Nâng cấp |
|---|---|
| Sự tương quan của các IV với các khóa yếu | Hàm trộn khóa cho mỗi gói tin |
| Tấn công phát lại | Đánh số thứ tự IV |
| Dễ bị giả mạo | MIC (Message Integrity Code) |

# CÁC HẠN CHẾ CỦA WPA

- *Vấn đề về chia sẻ khóa trước*
  - WPA vẫn sử dụng chế độ chia sẻ khóa trước, đây chính là điểm yếu dễ bị tấn công của WPA.
- *Vấn đề về toàn vẹn dữ liệu*
  - Sử dụng thuật toán Michael - 64 bít xác thực. Thuật toán này yếu và chỉ tốt hơn mã kiểm tra CRC32.
- *Vấn đề về mã hóa*
  - Sử dụng mã hóa yếu RC4.

# So sánh giữa WEP và WPA

| WEP | WPA |
|---|---|
| **Chia sẻ khóa bí mật (manual key sharing)** | Sử dụng 802.1x và EAP cho xác thực và thỏa thuận khóa tự động. Nhưng vẫn hỗ trợ manual key sharing giống như WEP. |
| **Mã pháp RC4** | Mã pháp RC4 |
| **Sinh khóa trên mỗi gói tin bằng cách ghép nối IV trực tiếp với khóa chia sẻ trước** | Giải quyết vấn đề của WEP bằng cách (a) giới thiệu khái niệm PTK trong kiến trúc khóa và (b) sử dụng hàm dẫn xuất khóa thay vì ghép nối trực tiếp để tạo ra khóa mã cho mỗi gói tin. |
| **Hạn chế về không gian khóa (khóa tĩnh, IV ngắn, phương pháp sinh và sử dụng khóa trực tiếp), việc thay đổi IV là tùy chọn.** | Tăng kích cỡ IV lên 48 bít, sử dụng PTK để làm tươi khóa cho mỗi phiên liên lạc, làm tăng không gian khóa. IV được đặt về 0 mỗi khi thiết lập một PTK mới. |
| **Thuật toán toàn vẹn dữ liệu là CRC32, không xác thực header.** | Thuật toán toàn vẹn dữ liệu là Michael, xác thực địa chỉ nguồn và đích. |
| **Không có giải pháp chống tấn công replay.** | Sử dụng IV như là một số thứ tự để chống tấn công replay. |
| **Không hỗ trợ STA xác thực mạng WLAN.** | Sử dụng 802.1x và EAP cho phép xác thực hai chiều. |

1. Tổng quan về mạng không dây
2. Các cơ chế an toàn trong WLAN
3. Giao thức an toàn WEP
4. Giao thức an toàn WPA
5. Giao thức an toàn WPA2

# Giao thức an toàn WPA2

- 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. Chuẩn IEEE 802.11i, được phê chuẩn vào 24/6/2004, được thiết kế để tăng cường tính an ninh trong lớp MAC trong IEEE 802.11.
- Kiến trúc mới cho các mạng không dây được gọi là mạng an toàn 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.

# Giao thức an toàn WPA2

- WPA2 = RSN:
- Mã hóa:
  - Sử dụng thuật toán AES
    - Chế độ CCMP (Counter mode (CRT) và CBC-MAC) (bắt buộc)
    - Cần phần cứng mới hỗ trợ AES
  - Giao thức TKIP (RC4 => chạy trên phần cứng cũ, Michael, đã vá các lỗ hổng của WEP) (tùy chọn)
- Xác thực:
  - 802.1X/EAP (TKIP, EAP-TLS), PSK
- Toàn vẹn:
  - CCMP (Counter Mode CBC-MAC Protocol) = CRT + CBC-MAC
- Chống tấn công phát lại:
  - Dùng số thứ tự gói tin (48 bit) – PN để ngăn chặn tấn công phát lại
- An toàn chống tấn công ngắt kết nối và hủy xác thực
- An toàn cho truyền thông ngang hàng (chế độ Ad-hoc)

# Giao thức an toàn WPA2

- AES/CCMP:
  - CCMP nghĩa là CTR mode and CBC-MAC
    - Bảo vệ tính toàn vẹn dựa vào CBC-MAC (sử dụng AES)
    - Mã hóa dựa vào CRT mode (sử dụng AES)
  - CBC-MAC
    - CBC-MAC được tính trên MAC header, CCMP header, và MPDU (dữ liệu được phân mảnh)
    - Các trường hay thay đổi được đặt bằng 0
    - Đầu vào được đệm các số 0 nếu độ dài không là bội của 128 bit.
    - Khối khởi đầu của CBC-MAC gồm:
      - flag (8)
      - priority (8)
      - source address (48)
      - packet number (48)
      - data length (16)
    - Khối cuối cùng128-bit của mã CBC bị cắt 64 bit cao lấy giá trị CBC-MAC.

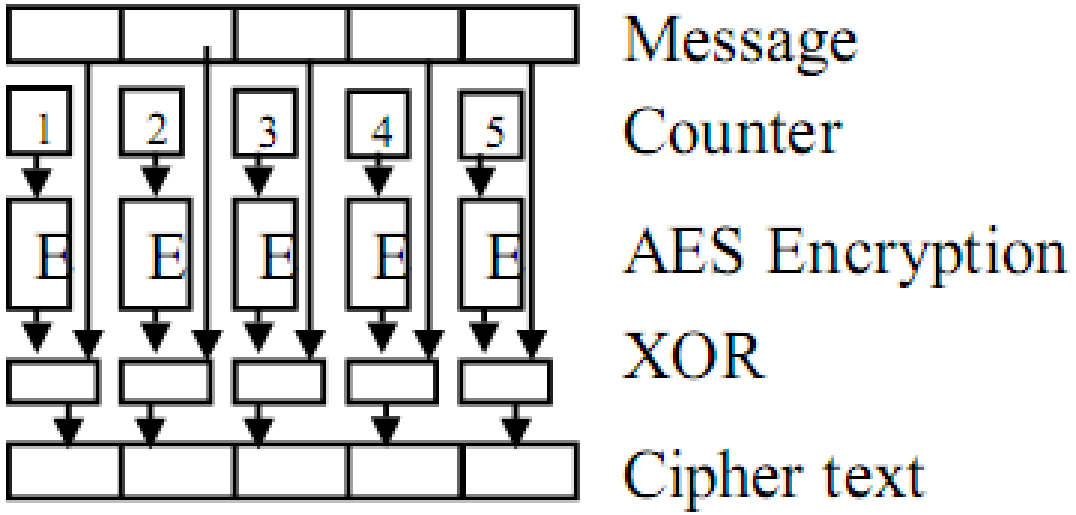
# Giao thức an toàn WPA2

- AES/CCMP:
  - Chế độ mã hóa CTR
    - MPDU và giá trị CBC-MAC được mã hóa, MAC Header và CCMP Header thì không
    - Định dạng của biến đếm - counter thì tương tự với khối CBC-MAC ban đầu
      - "data length" được thay thế bởi "counter"
      - counter được khởi tạo bằng 1 và được tăng lên sau mỗi khối được mã hóa.

# Giao thức an toàn WPA2

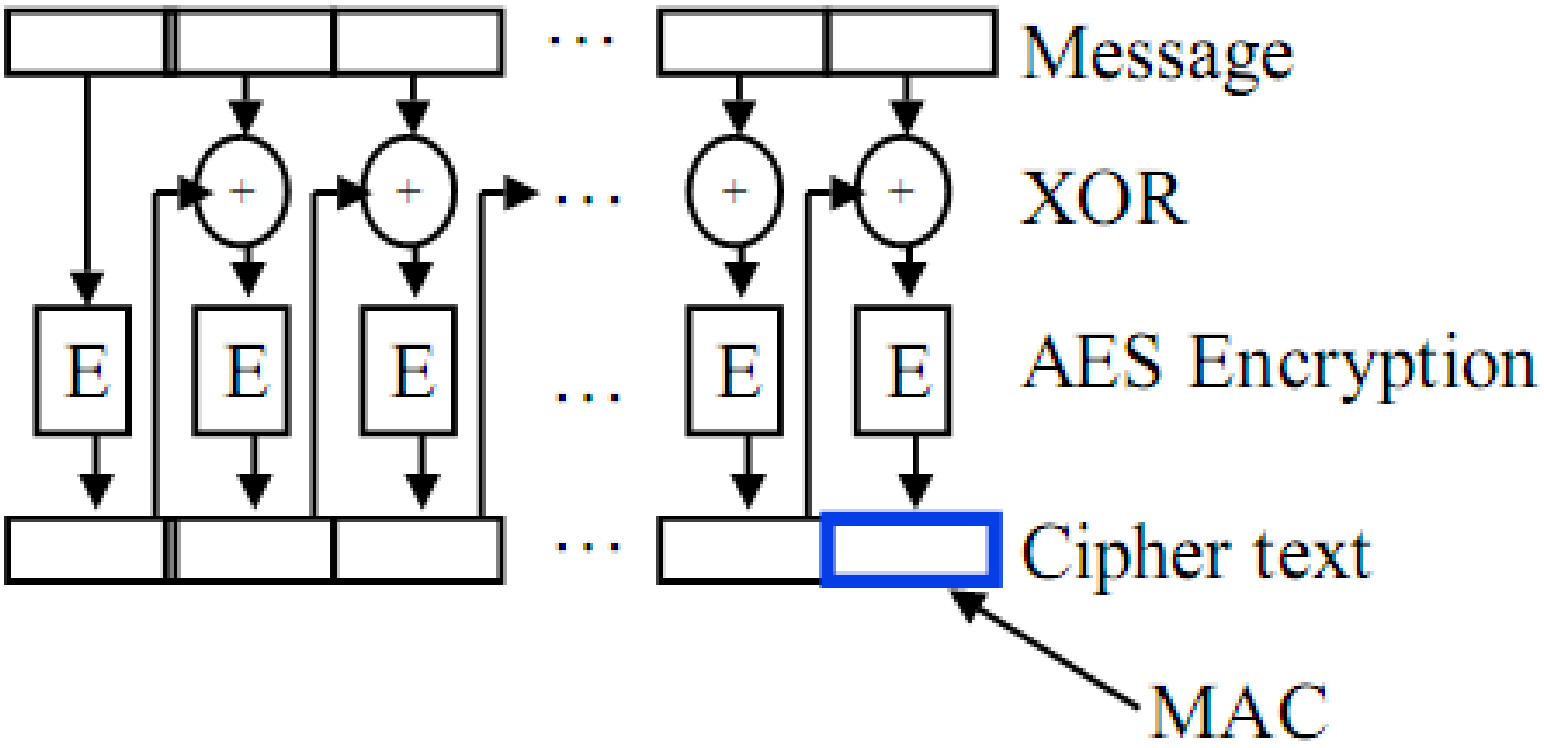
- AES-CTR
  - Advanced Encryption Standard (AES) làm việc ở chế độ Counter
  - AES là một mã khối có nhiều chế độ
  - 802.11i sử dụng chế độ Counter-Mode để mã hóa dữ liệu
  - Biến đếm - Counter tăng lên đối với mỗi khối dữ liệu liên tiếp.
  - Counter được mã hóa sau đó được XOR với dữ liệu.

+ Biến Counter có thể bắt đầu ở một giá trị tùy ý
+ Các khối giống nhau thì cho ra bản mã khác nhau



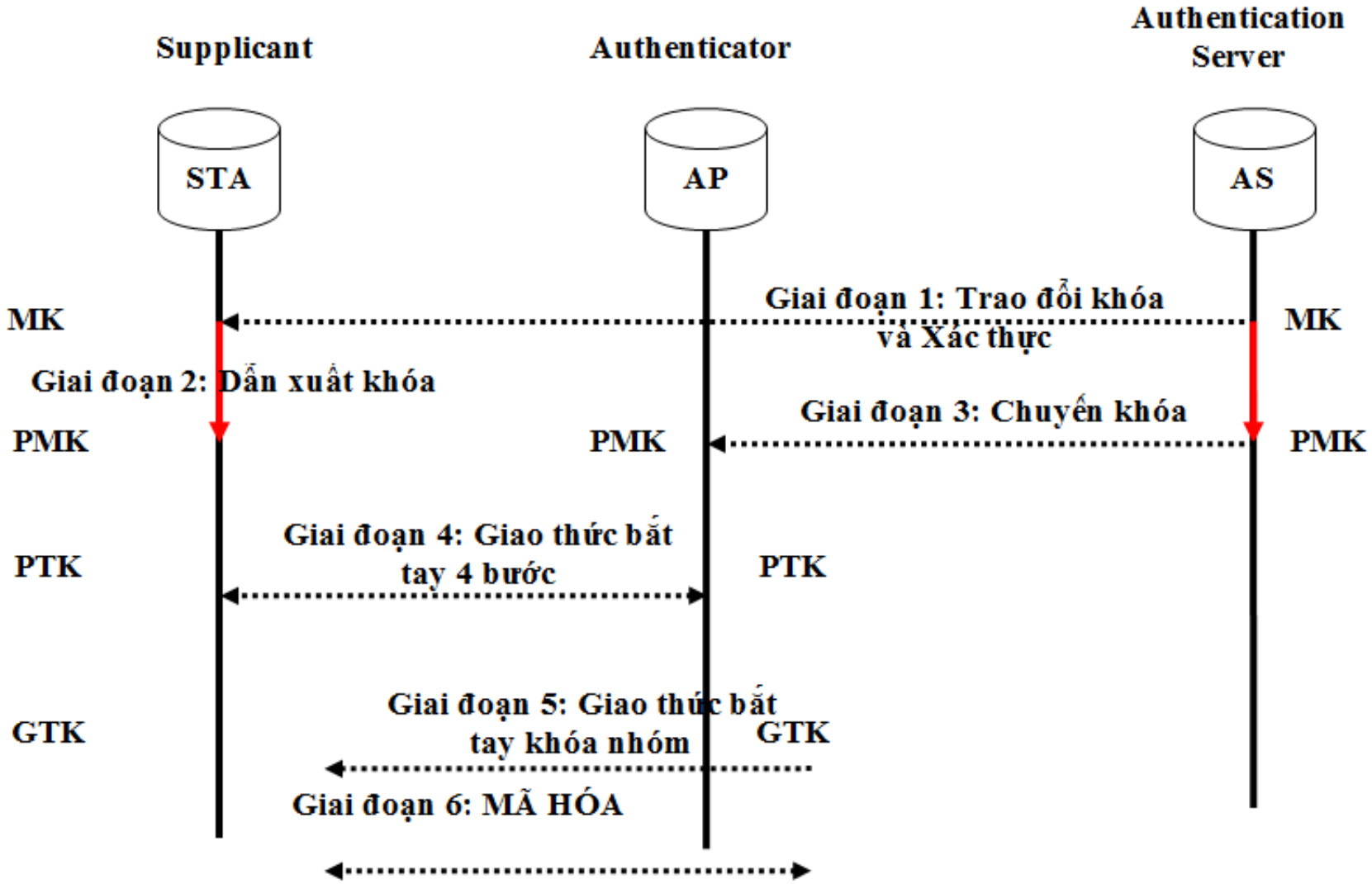
# Giao thức an toàn WPA2

- AES/CBC-MAC:
  - Chế độ xích mã khối (CBC - CipherBlock Chaining) được dùng để tạo ra một mã xác thực thông điệp (MAC – message authentication code)



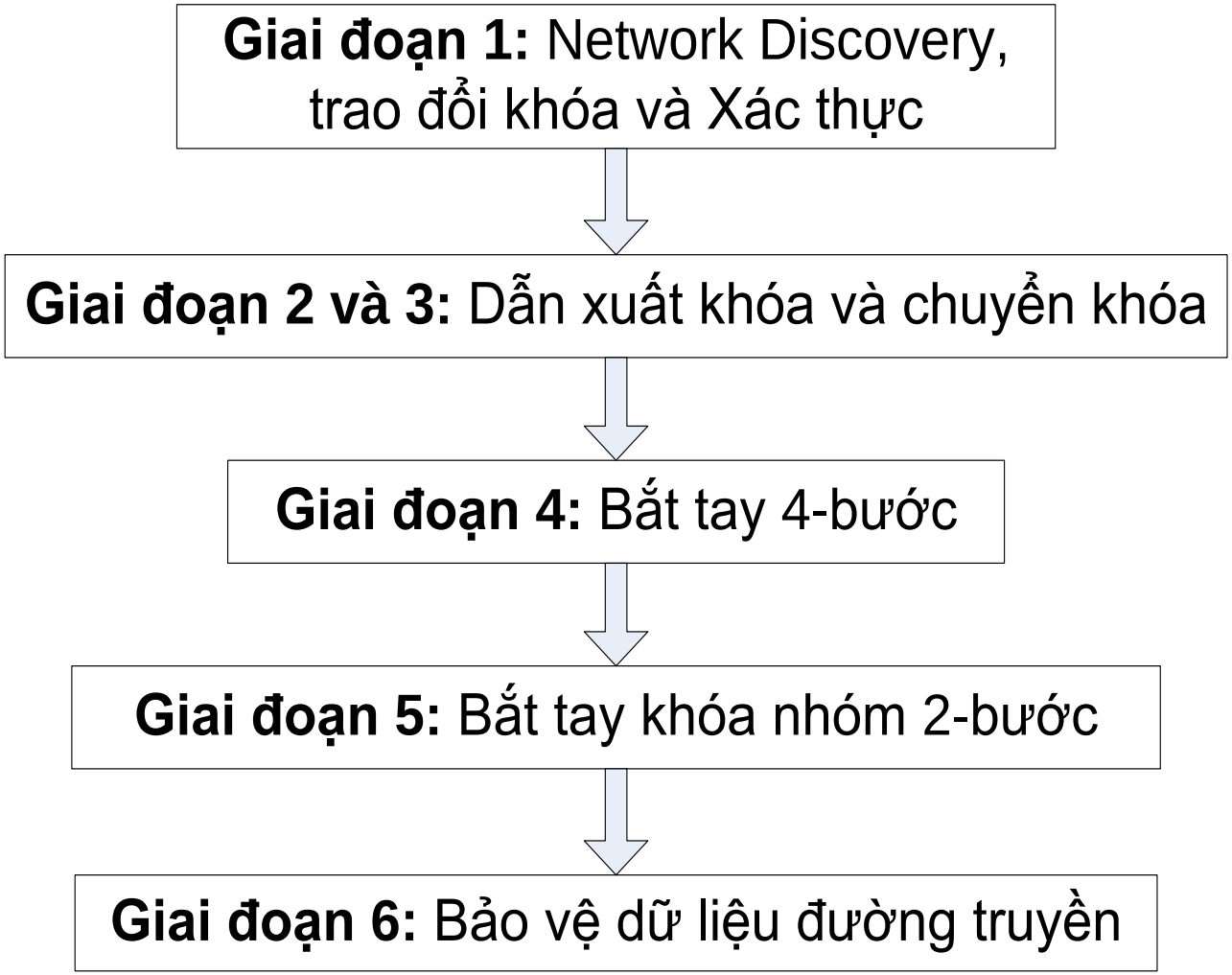
# Giao thức an toàn WPA2

- Toàn bộ quá trình quản lý, trao đổi, sinh khóa và mã hóa của WPA2 như sau:



# Giao thức an toàn WPA2

- Tổng kết các thành phần của WPA2:



# Giao thức an toàn WPA2

- Xác thực và trao đổi khóa: 802.1x – EAP, Preshared Key.
- Giai đoạn 4 - Giao thức bắt tay 4 bước (4-way Handshake): Tồn tại tấn công DoS đối với thông báo 1.
- Giai đoạn 5 - Trao đổi khóa nhóm: Tồn tại một tấn công ở bên trong, Security Hole 196 (năm 2010).
- Giai đoạn 6 - Mã hóa và toàn vẹn (CCMP): AES-CCM, giao thức này được coi là an toàn. Chưa có công bố tấn công nào đối với giao thức này ở thời điểm hiện tại.

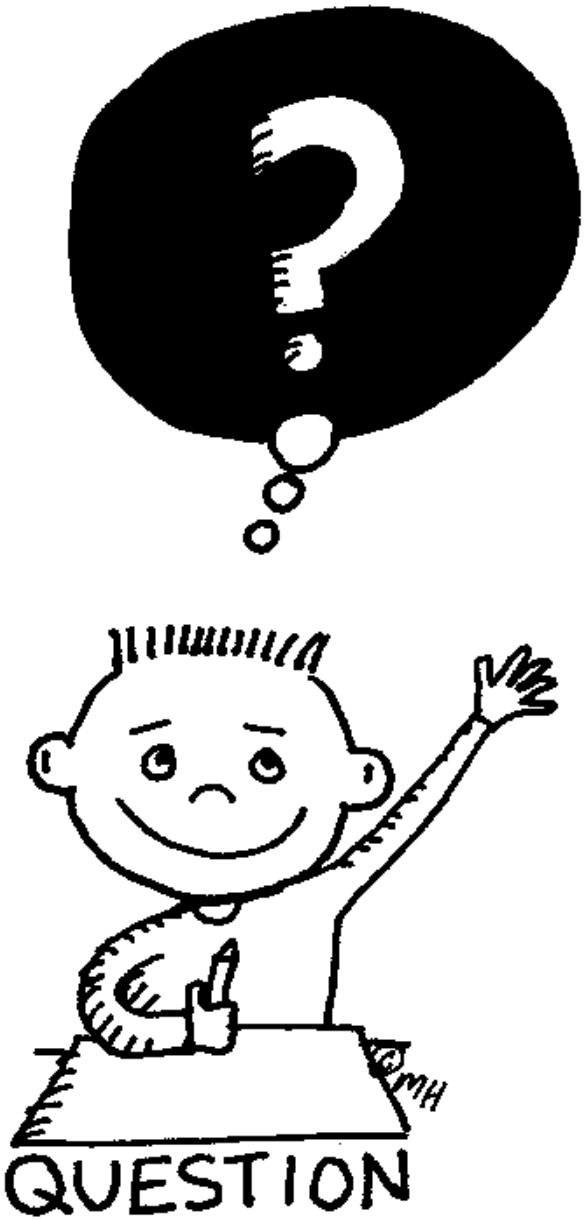
# So sánh các giao thức an toàn trong WLAN

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

| | WEP | WPA | 802.11i |
|---|---|---|---|
| **Trao đổi và phân phối khóa** | Trao đổi và thay đổi khóa thủ công | Trao đổi khóa tự động, mặc định 600s trao đổi lại PTK và GTK, 1 ngày trao đổi lại PMK, GMK | Trao đổi khóa tự động, mặc định 600s trao đổi lại PTK và GTK, 1 ngày trao đổi lại PMK, GMK |
| **Thuật toán mã hóa** | RC4 | RC4 | AES - ở chế độ CCM |
| **Độ dài khóa** | 40 bít, 104 bít mã hóa, 32 bít xác thực CRC | 128 bit mã hóa, 64 bit xác thực Michael | 128 |
| **Độ dài IV** | 24 bít | 48 bít | 128 bít IV cho AES CBC-MAC nhưng chỉ thay đổi 48 bít, 128 bít Counter cho AES-CTR nhưng chỉ thay đổi 16 bít (đủ lớn hơn max=(64*7395*8/128)=29580 khối 128 bít) |
| **Khóa mã hóa/gói tin** | Mỗi gói tin sử dụng 1 giá trị IV | Sử dụng hàm trộn của TKIP | Không cần thiết |
| **Toàn vẹn cho phần header** | CRC-32 | Địa chỉ nguồn/đích được bảo vệ bởi thuật toán Michale | Toàn vẹn theo CBC-MAC |
| **Toàn vẹn dữ liệu** | CRC-32 | Mã MIC – sử dụng thuật toán Michale | Toàn vẹn theo CBC-MAC |
| **Replay** | Không | Có | Có |

# Tổng kết các giao thức an toàn cho WLAN

| | WEP | WPA | 802.11i |
|---|---|---|---|
| Cipher Algorithm | RC4 | RC4 (TKIP) | AES-CCMP |
| Encryption Key | 40-bit | 128-bit | 128-bit |
| Initialization Vector | 24-bit | 48-bit | 48-bit |
| Authentication Key | None | 64-bit | 128-bit |
| Integrity Check | CRC-32 | Michael | CCM |
| Key Distribution | Manual | 802.1X (EAP) | 802.1X (EAP) |
| Key Unique To: | Network | Packet, Session, User | Packet, Session, User |
| Key Hierarchy | No | Derived from 802.1X | Derived from 802.1X |
| Ad-hoc Security (P2P) | No | No | Yes (IBSS) |
| Pre-authentication | No | No | Yes (EAPOL) |


QUESTION