ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

Wireless and Mobile Security

Nhóm 4

20120262	Khúc Khánh Đăng
20120267	Nguyễn Tiến Đạt
20120380	Nguyễn Phúc Thuần
20120482	Nguyễn Tạ Huy Hoàng
20120615	Trần Nam Tuấn

GVHD: TS. Trương Toàn Thịnh
Môn học: Mã hóa ứng dụng

Thành phố Hồ Chí Minh - 2023

MỤC LỤC

Phần 1. Phân công công việc **5**
Phần 2. Nội dung **6**
A. Giới thiệu về Wireless LAN 6
I. Đặc trưng của mạng truyền thông không dây 6
Ưu điểm: 6
Nhược điểm 6
II. Tiêu chuẩn MAC không dây 6
III. Các vấn đề hiện hữu của mạng truyền thông không dây 7
IV. Tổng quan về công nghệ Wifi b-a-g 7
V. Kiến trúc 802.11 8
1. Kiến trúc hệ thống 8
2. Ngăn xếp giao thức 802.11 9
3. Lớp MAC 802.11 9
VI. DCF 10
1. Quyền truy cập cơ bản DCF 10
2. Thủ tục backoff 11
3. Thủ tục phục hồi 11
4. Thời gian đợi ngẫu nhiên và cửa sổ cạnh tranh (Conflict Window) 12
5. Sơ đồ DCF RTS/CTS 12
6. Phân mảnh DCF 13
VII. PCF 14
VIII. Cấu trúc gói tin MAC IEEE 802.11 15
1. Cấu trúc gói IEEE 802.11 MAC: 15
2. Loại gói: 15
3. Loại phụ: 15
4. Giải thích địa chỉ: 15
IX. Đồng bộ hóa MAC 15
X. Quản lý tiêu hao năng lượng 16
XI. Kết nối vào điểm truy cập 18
1. Nhận diện truy cập: 18
2. Xác thực - Authentication: 18
3. Kết hợp: 18
XII. Dynamic Host Configuration Protocol - DHCP 19
B. WEP 19

I. Giới thiệu chung 19
II. Ba mục đích của WEP trong thực tế: 20
III. Các thức hoạt động: 20
1. Authentication 20
2. Encryption 20
IV. Điểm yếu và lỗ hổng của WEP: 21
C. Kiểm soát truy cập với 802.1X, EAP và RADIUS Điểm yếu của WEP: 22
I. IEEE 802.11 : 22
1. 802.11X là gì ? 22
2. Các thành phần của IEEE 802.1X: 22
3. Kiến trúc của IEEE 802.1X : 23
4. Xác thực dùng Dial-In User. 24
5. Xác thực dùng người dùng mạng không dây. 24
II. EAPOL: 24
1. Ứng dụng của EAP: 25
2. EAP procedure 25
3. Lợi ích của EAP: 26
4. Bất lợi của EAP 26
5. Phân lớp chức năng của EAP 26
6. EAP Packet Format: 27
1. Bản tin Request và Response: 28
2. Bản tin Success và Failure: 28
7. Các Type của EAP: 28
8. Phương thức xác thực EAP. 29
III. RADIUS: 29
1. Thuật ngữ RADIUS 29
2. Cách thức hoạt động của xác thực RADIUS 30
3. Server RADIUS được sử dụng như thế nào? 31
D. Giao thức bảo toàn khóa tạm thời - Temporal Key Integrity Protocol (TKIP) 31
I. Giới thiệu về Temporal Key Integrity Protocol (TKIP) 31
II. Cơ chế hoạt động 31
III. Toàn vẹn thông điệp trong TKIP 32
IV. Phương pháp chọn Initial Vector (IV) 33
V. Kỹ thuật Per-Packet Key Mixing 34
E. Mã hoá trên WLAN và Mobile - AES và CCMP 36
I. Giới Thiệu 36
a. CCMP là gì? 36

b. Cung cấp chế độ bảo mật tốt hơn so với TKIP 36
c. Tại sao lại sử dụng thuật toán AES 36
d. Lý do áp dụng AES trong 802.11i được thực hiện sớm hơn việc điểm yếu của WEP bị phát hiện 37
e. WEP, TKIP and CCMP 37
II. AES Pairwise Key Hierarchy trong CCMP 37
III. AES Group Key Hierarchy trong CCMP 38
IV. Tổng quan về AES 39
V. Modes of Operator 39
- ECB Mode: 39
- Counter mode 39
- Counter mode + CBC MAC: CCM 40
- Offset Codebook Mode (OCB): 40
VI. CCMP được sử dụng trong RSN như thế nào? 40
VII. CCMP Processing 41
IX. CCMP Encryption 43
X. CCMP Decryption 45
III. Tham khảo 45

Phần 1. Phân công công việc

MSSV	Họ tên	Công việc
20120262	Khúc Khánh Đăng	Mã hoá trên WLAN và Mobile - AES và CCMP
20120267	Nguyễn Tiến Đạt	Giao thức bảo toàn khóa tạm thời - Temporal Key Integrity Protocol (TKIP)
20120380	Nguyễn Phúc Thuần	Giới thiệu về WEP, Kiểm soát truy cập với 802.1X, EAP và RADIUS
20120482	Nguyễn Tạ Huy Hoàng	Giới thiệu về Wireless LAN
20120615	Trần Nam Tuấn	Kiểm soát truy cập với 802.1X, EAP và RADIUS

Phần 2. Nội dung

A. Giới thiệu về Wireless LAN

WLAN ra đời năm 1980, WLAN viết tắt từ tiếng Anh "Wireless Local Area Network" hay "mạng không dây". WLAN là một mạng cho phép các thiết bị kết nối và giao tiếp không dây. Không giống như một mạng LAN có dây truyền thống, trong đó các thiết bị giao tiếp qua cáp Ethernet, các thiết bị trên mạng WLAN giao tiếp qua (sóng) WiFi .

I. Đặc trưng của mạng truyền thông không dây

Ưu điểm:

- Không giới hạn không gian vật lý.
- Độ linh hoạt cao.
- Tốc độ truyền tải cao.
- Tình đa dạng về ứng dụng.
- Dễ dàng sử dụng.
- Tiết kiệm chi phí.

Nhược điểm

- Nhiễu và nhiễu tín hiệu: Truyền thông không dây có thể bị nhiễu và nhiễu tín hiệu, gây ảnh hưởng đến hiệu suất truyền tải dữ liệu.
- Không thể giả định được tính đầy đủ kết nối: Trong truyền thông không dây, không thể giả định rằng các thiết bị có thể kết nối đầy đủ với tất cả các thiết bị khác.
- Sử dụng pin: Trong truyền thông không dây, các thiết bị thường sử dụng pin và do đó cần phải quản lý năng lượng tiêu thụ để giữ cho thiết bị hoạt động trong thời gian dài.
- Bảo mật: truyền thông không dây có thể bị tấn công bởi tin tặc hoặc hacker, do đó cần phải có các biện pháp bảo mật như mã hóa dữ liệu để đảm bảo tính an toàn và bảo mật cho hệ thống.

II. Tiêu chuẩn MAC không dây

Một mạng WLAN cần đảm bảo các yếu tố sau:

- Đảm bảo truy cập đồng thời và không xung đột của các thiết bị trong mạng.
- Đảm bảo tính công bằng trong việc truy cập truyền thông, không ưu tiên một thiết bị nào hơn thiết bị khác.
- Có khả năng xử lý và sửa chữa các lỗi xảy ra trong quá trình truyền thông, bằng cách sử dụng các giao thức phù hợp.
- Có khả năng quản lý và phân phối tài nguyên cho các thiết bị, như băng thông và thời gian truy cập truyền thông.
- Có khả năng hỗ trợ nhiều kỹ thuật truyền thông không dây khác nhau, cho phép tích hợp các thiết bị từ các nhà sản xuất khác nhau vào cùng một mạng.
- Đảm bảo tính ổn định và hiệu suất cao trong việc truyền thông dữ liệu, đặc biệt là khi mạng có số lượng lớn các thiết bị kết nối.
- Có khả năng đáp ứng các yêu cầu về bảo mật, bao gồm cả mã hóa và xác thực thiết bị, để đảm bảo tính an toàn và bảo mật cho mạng truyền thông không dây.

III. Các vấn đề hiện hữu của mạng truyền thông không dây

Có nhiều vấn đề về mạng không dây mà người dùng có thể gặp phải. Sau đây là một số vấn đề phổ biến:

- Thiết bị đầu cuối ẩn: Một thiết bị đầu cuối ẩn xảy ra khi hai nút đang giao tiếp với nút thứ ba, nhưng chúng không thể phát hiện tín hiệu của nhau. Điều này có thể dẫn đến mất gói, truyền lại và giảm thông lượng.
- Giảm thông lượng: Mạng không dây dễ bị nhiễu và mất tín hiệu, điều này có thể làm giảm thông lượng tổng thể của mạng. Điều này có thể dẫn đến tốc độ truyền dữ liệu chậm hơn, chất lượng giọng nói kém và bộ đệm video.
- Tăng độ trễ: Mạng không dây thường có độ trễ cao hơn mạng có dây, điều này có thể gây ra sự chậm trễ trong việc truyền dữ liệu. Điều này có thể dẫn đến thời gian phản hồi chậm hơn và hiệu suất kém cho các ứng dụng nhạy cảm với thời gian như hội nghị truyền hình hoặc chơi game trực tuyến.
- Thiết bị đầu cuối tiếp xúc: Một thiết bị đầu cuối bị lộ xảy ra khi một nút không truyền dữ liệu do tin rằng một nút khác hiện đang truyền, mặc dù nút khác không nằm trong phạm vi. Điều này có thể dẫn đến sự chậm trễ không cần thiết và giảm hiệu quả mạng.
- Giảm sử dụng kênh: Các mạng không dây chia sẻ cùng một phổ tần số, điều này có thể dẫn đến nhiễu và giảm mức sử dụng kênh. Điều này có thể dẫn đến giảm thông lượng và tốc độ truyền dữ liệu chậm hơn.
- Năng lượng hạn chế: Các thiết bị không dây dựa vào pin, có tuổi thọ hạn chế. Khi pin cạn kiệt, hiệu suất của thiết bị có thể suy giảm, dẫn đến giảm thông lượng, tăng độ trễ và giảm hiệu quả mạng.
- Phân vùng mạng: Mạng không dây có thể gặp phải tình trạng phân vùng mạng khi một nút không thể kết nối với các nút khác do các rào cản vật lý hoặc logic. Điều này có thể dẫn đến giảm vùng phủ sóng và giảm hiệu quả mạng.
- Tính di động: Các thiết bị không dây có thể di chuyển giữa các điểm truy cập, điều này có thể dẫn đến sự cố chuyển giao, mất tín hiệu và giảm hiệu quả mạng.
- Bảo mật: Mạng không dây dễ bị đe dọa bảo mật như nghe lén, truy cập trái phép và chặn dữ liệu. Điều này có thể dẫn đến vi phạm dữ liệu, mất thông tin nhạy cảm và giảm độ tin cậy của mạng.

IV. Tổng quan về công nghệ Wifi b-a-g

- **WiFi b (802.11b)**: Là chuẩn kết nối đầu tiên được phát triển, hoạt động trên băng tần 2.4GHz và có tốc độ truyền tải dữ liệu tối đa khoảng 11Mbps. Chuẩn này có tầm phủ sóng tốt, tuy nhiên tốc độ truyền tải không cao, được sử dụng phổ biến trong các mạng gia đình và văn phòng nhỏ.
- **WiFi a (802.11a)**: Chuẩn kết nối này hoạt động trên băng tần 5GHz và có tốc độ truyền tải dữ liệu tối đa lên đến 54Mbps. Với tốc độ truyền tải nhanh và chất lượng tín hiệu tốt hơn chuẩn b, chuẩn a thường được sử dụng trong các mạng doanh nghiệp hoặc các ứng dụng yêu cầu tốc độ cao.

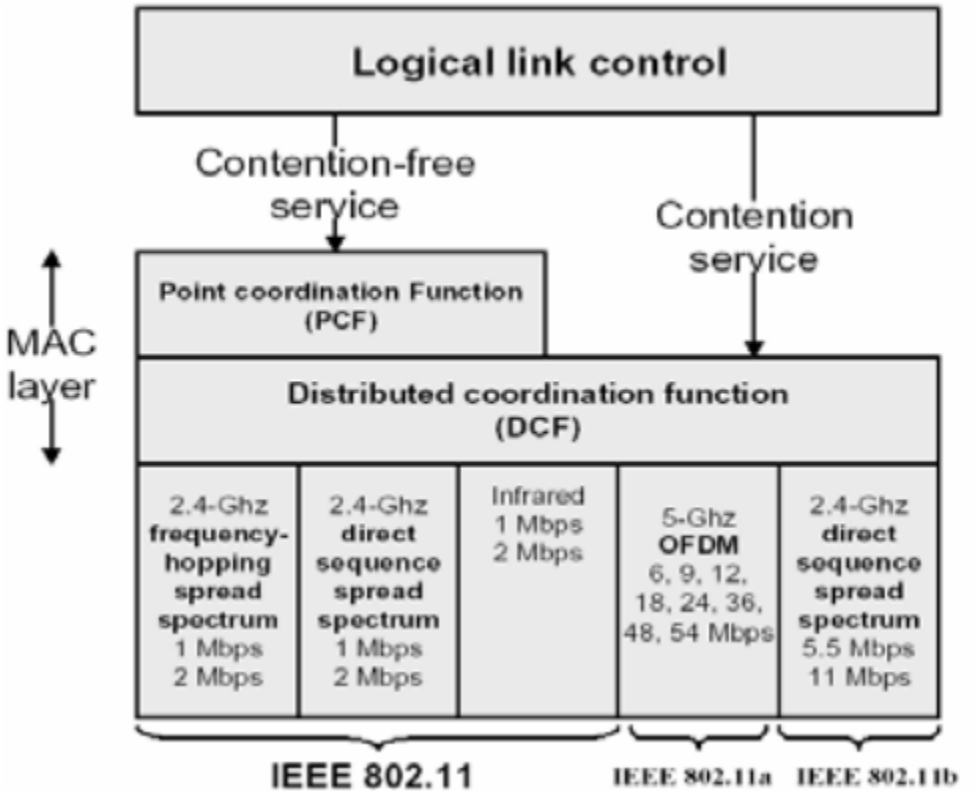
- **WiFi g (802.11g)**: Là chuẩn kết nối kế tiếp của chuẩn b, hoạt động trên băng tần 2.4GHz và có tốc độ truyền tải dữ liệu tối đa lên đến 54Mbps. Với tốc độ truyền tải cao và tương thích với chuẩn b, chuẩn g trở thành chuẩn kết nối phổ biến trong các mạng gia đình và văn phòng nhỏ.
- Ngoài ra còn có:
    + 802.11d - Phần mở rộng trong các miền quy định khác
    + 802.11e - MAC Cải tiến-Bảo mật/QoS
    + 802.11f - Giao thức liên điểm truy cập
    + 802.11h - Spectrum Managed 802.11a, tương thích với Châu Âu
    + 802.11i - Tăng cường bảo mật (TKIP và 802.1x) (sẽ đề cập ở mục C và mục D)

V. Kiến trúc 802.11

1. Kiến trúc hệ thống

- Tiêu chuẩn 802.11 xác định hai kiến trúc hệ thống cơ bản cho mạng LAN không dây:
- Đặc biệt: Trong một mạng đặc biệt, còn được gọi là mạng ngang hàng, các trạm không dây giao tiếp trực tiếp với nhau mà không cần điểm truy cập (AP). Mạng đặc biệt thường được sử dụng cho các kết nối không dây tạm thời giữa các thiết bị, chẳng hạn như giữa các máy tính xách tay trong phòng hội nghị.
- Dựa trên cơ sở hạ tầng: Trong mạng dựa trên cơ sở hạ tầng, các trạm không dây giao tiếp với nhau thông qua điểm truy cập (AP), đóng vai trò là điểm kiểm soát trung tâm cho mạng. AP quản lý thông tin liên lạc giữa các trạm không dây và có thể cung cấp các dịch vụ mạng bổ sung, chẳng hạn như xác thực, mã hóa và chất lượng dịch vụ (QoS).
- Điểm truy cập (Access Point) là một thiết bị mạng không dây (wireless) được sử dụng để kết nối các thiết bị không dây khác như máy tính, điện thoại di động, máy tính bảng, camera IP...với mạng dây (wired network) thông qua sóng radio.
- Chọn một AP và "liên kết" với nó: Điểm truy cập cung cấp các tín hiệu sóng Wifi cho các thiết bị không dây khác nhau, các thiết bị này có thể kết nối với điểm truy cập gần nhất. Khi một thiết bị không dây được kết nối với điểm truy cập, nó sẽ được cấp một địa chỉ IP để truy cập mạng dây.
- Hỗ trợ chuyển vùng: Khi một thiết bị không dây di chuyển qua nhiều vùng phủ sóng của các điểm truy cập khác nhau, điểm truy cập sẽ tự động chuyển thiết bị này sang điểm truy cập khác để giữ cho kết nối không bị gián đoạn. Chức năng này được gọi là chuyển vùng (roaming).
- Các chức năng khác:
- Đồng bộ hóa thời gian (đèn hiệu): Điểm truy cập có thể đồng bộ hóa thời gian giữa các thiết bị không dây để đảm bảo rằng chúng đang hoạt động theo cùng một giờ.
- Quản lý điện năng: Điểm truy cập có thể quản lý tiêu thụ điện năng để tiết kiệm năng lượng và kéo dài tuổi thọ của thiết bị.
- PCF (Point Coordination Function): Chức năng PCF giúp điểm truy cập điều khiển quyền truy cập vào kênh truyền, giúp giảm thiểu xung đột dữ liệu giữa các thiết bị không dây và cải thiện hiệu suất mạng.

2. Ngăn xếp giao thức 802.11



3. Lớp MAC 802.11

Ba cơ chế truy cập cơ bản trong tiêu chuẩn 802.11 là:

- CSMA / CA (Carrier Sense Multiple Access with Collision Avoidance): Cơ chế này được sử dụng trong Chức năng phối hợp phân tán (DCF) và là phương thức truy cập mặc định trong tiêu chuẩn 802.11. Nó liên quan đến việc thiết bị cảm nhận kênh trước khi truyền và hoãn truyền nếu kênh đang bận.
- DCF (CSMA/CA + RTS/CTS): Cơ chế này tăng cường phương thức CSMA/CA bằng cách sử dụng cơ chế Request to Send/Clear to Send (RTS/CTS) để giải quyết vấn đề về các thiết bị đầu cuối ẩn và bị lộ.
- PCF (Chức năng điều phối điểm): Cơ chế này cung cấp các dịch vụ giới hạn thời gian với sơ đồ dựa trên mức độ ưu tiên. Nó sử dụng Điều phối viên điểm (PC) để phân bổ kênh cho các thiết bị khác nhau theo cách vòng tròn.

Tiêu chuẩn 802.11 cũng xác định ba không gian liên khung hình được sử dụng để phân biệt giữa các loại khung hình khác nhau:

- DIFS (DCF Interframe Space): Không gian interframe này có mức độ ưu tiên thấp nhất và được sử dụng cho dữ liệu không đồng bộ.
- PIFS (Point Coordination Function Interframe Space): Không gian interframe này có mức độ ưu tiên trung bình và được sử dụng cho các dịch vụ giới hạn thời gian.

- SIFS (Không gian liên khung hình ngắn): Không gian liên khung hình này có mức độ ưu tiên cao nhất và được sử dụng cho các thông báo điều khiển ngắn, chẳng hạn như khung ACK.

Có hai cấp độ cảm giác sóng được sử dụng trong 802.11:

- Cảm giác sóng mang vật lý: Điều này được thực hiện bởi lớp vật lý của giao thức, lớp này lắng nghe bất kỳ tín hiệu vô tuyến nào trên kênh trước khi truyền dữ liệu. Nếu kênh bận, thiết bị sẽ đợi cho đến khi nó khả dụng.
- Cảm giác sóng mang ảo: Điều này được thực hiện bởi lớp MAC bằng cách sử dụng Vectơ phân bổ mạng (NAV). NAV là bộ hẹn giờ được đặt khi thiết bị tình cờ nghe thấy trao đổi RTS/CTS (Request-to-Send/Clear-to-Send) hoặc khung dữ liệu. Bộ hẹn giờ cho biết thời gian kênh sẽ bận và ngăn các thiết bị khác truyền cho đến khi bộ hẹn giờ hết hạn. Điều này giúp giải quyết vấn đề của các thiết bị đầu cuối ẩn và tiếp xúc.

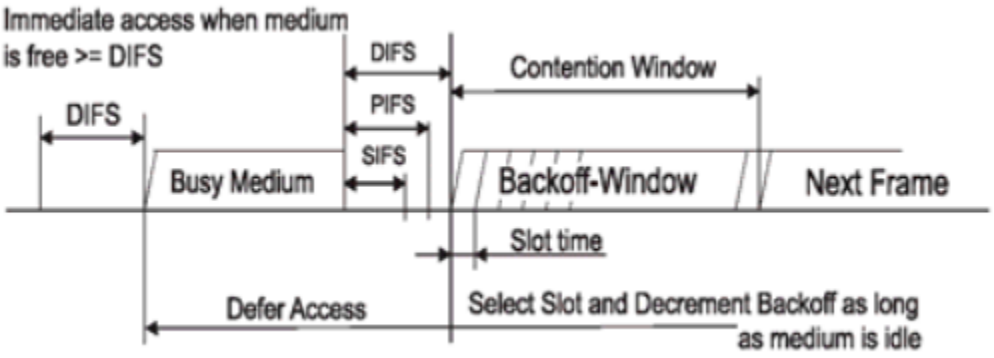
Các thiết bị đầu cuối ẩn xảy ra khi hai thiết bị không thể nghe thấy nhau, nhưng cả hai đều cố gắng truyền dữ liệu cùng một lúc, gây ra va chạm. Cơ chế cảm biến sóng mang ảo giúp ngăn ngừa va chạm bằng cách cho phép các thiết bị phát hiện khi kênh đang bận ngay cả khi chúng không thể nghe thấy các thiết bị khác.

Các thiết bị đầu cuối bị lộ xảy ra khi một thiết bị có thể nghe thấy một thiết bị khác đang truyền, nhưng không tự truyền vì nó giả định không chính xác rằng kênh đang bận. Cơ chế cảm biến sóng mang ảo cũng giúp ngăn chặn vấn đề này bằng cách cho phép các thiết bị phát hiện chính xác khi nào kênh có sẵn để truyền.

VI. DCF

1. Quyền truy cập cơ bản DCF

- DCF (Distributed Coordination Function) là một phương thức truy cập kênh của lớp MAC trong chuẩn mạng không dây 802.11. DCF sử dụng phương thức truy cập cơ bản để cho phép các STA (Station) truy cập kênh một cách công bằng.
- Phương thức truy cập cơ bản hoạt động theo cách sau:
- Khi một STA có dữ liệu để gửi, nó sẽ cảm nhận trạng thái của kênh trước khi truyền.
    + Nếu kênh trống và thời gian trống lớn hơn hoặc bằng DIFS (Distributed Interframe Space), STA có thể truyền một đơn vị dữ liệu MAC (MAC Protocol Data Unit - MPDU).
    + Nếu kênh đang bận, STA sẽ chờ một khoảng thời gian đợi ngẫu nhiên.
    + Sau khi STA truyền MPDU, nó sẽ chờ ACK (Acknowledgment) từ điểm truy cập (Access Point - AP) hoặc STA đích để xác nhận việc truyền thành công. Nếu STA không nhận được ACK sau một khoảng thời gian chờ nhất định, nó sẽ giả định rằng truyền bị lỗi và bắt đầu lại quá trình truyền.
- Về cơ bản, phương thức truy cập cơ bản trong DCF giúp đảm bảo rằng nhiều STA có thể chia sẻ kênh một cách công bằng và tránh xảy ra va chạm dữ liệu. Nó được sử dụng trong môi trường WLAN (Wireless Local Area Network) và được áp dụng rộng rãi trong các ứng dụng mạng không dây hiện đại.



2. Thủ tục backoff

- Thủ tục Backoff là quy trình được thực hiện bởi một STA khi nó muốn truyền một khung dữ liệu những kênh đang bận.

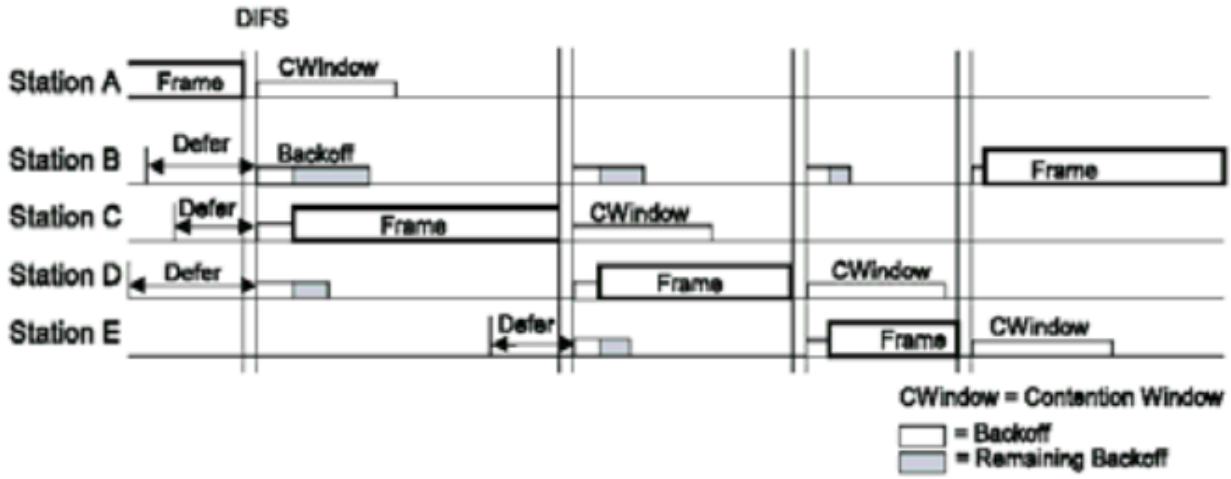
  + Trước tiên, STA sẽ đặt một thời gian đợi ngẫu nhiên, gọi là "Backoff Timer".

  + Sau đó, Backoff Timer bắt đầu giảm sau khi thời gian chờ DIFS kể từ lúc kênh bận.

  + Nếu trong quá trình chờ đợi, kênh đang bận, Backoff Timer sẽ bị tạm dừng và sẽ không tiếp tục giảm cho đến khi kênh trở thành trống trong khoảng thời gian DIFS.

  + Khi Backoff Timer đạt giá trị 0, STA có thể truyền khung dữ liệu mà không cần chờ đợi thêm.

- Tóm lại, thủ tục Backoff giúp giảm xác suất xảy ra va chạm giữa các STA truyền thông trên cùng một kênh trong mạng không dây. Khi một STA cảm nhận được kênh đang bận, nó sẽ đặt thời gian chờ ngẫu nhiên trước khi truyền lại để tránh xảy ra va chạm với các STA khác cũng đang chờ đợi truyền.



3. Thủ tục phục hồi

- Trong quá trình cạnh tranh truy cập kênh, có thể xảy ra va chạm giữa các STA khi chúng cùng thử truy cập kênh trong cùng một khoảng thời gian. Khi xảy ra va chạm, các STA cần phải thực hiện các thủ tục phục hồi sau đây để đảm bảo việc truyền thông được thực hiện thành công:

+ Khi xảy ra va chạm, các STA cần phải thực hiện việc truyền lại khung dữ liệu bằng cách chọn một thời gian đợi ngẫu nhiên mới và khởi động lại quá trình Backoff.

+ Đồng thời, cửa sổ cạnh tranh sẽ được kéo dài lên gấp đôi, cho phép các STA cạnh tranh truy cập kênh một cách công bằng.

+ Trong quá trình phục hồi, các STA không có đặc quyền đặc biệt để truyền lại dữ liệu, mà phải cạnh tranh truy cập kênh như các STA khác.

- Tổng hợp lại, quá trình phục hồi sau khi xảy ra va chạm giúp các STA có thể tiếp tục truyền dữ liệu một cách hiệu quả trên mạng không dây. Bằng cách tăng độ dài cửa sổ cạnh tranh và chọn thời gian đợi ngẫu nhiên mới, các STA có thể tránh được va chạm và đảm bảo việc truyền dữ liệu được thực hiện thành công.

4. Thời gian đợi ngẫu nhiên và cửa sổ cạnh tranh (Conflict Window)

- Thời gian đợi ngẫu nhiên (Random backoff time) được tính bằng cách chọn ngẫu nhiên một số nguyên trong khoảng từ 0 đến giá trị của cửa sổ cạnh tranh (CW), sau đó nhân với độ dài của Slot Time (aSlotTime), là một đặc tính của PHY (20µs cho DSSS).
- Cửa sổ cạnh tranh (CW) là một giá trị được sử dụng để tính thời gian đợi ngẫu nhiên trong quá trình cạnh tranh truy cập kênh. Sau mỗi lần thất bại trong việc truyền dữ liệu, giá trị của cửa sổ cạnh tranh sẽ tăng theo hàm số mũ, dẫn đến tăng trung bình thời gian đợi ngẫu nhiên. Việc tăng cửa sổ cạnh tranh nhằm đảm bảo rằng các STA sẽ cạnh tranh truy cập kênh một cách công bằng, giúp tránh tình trạng ưu tiên truy cập kênh của một số STA.
- Sau khi giá trị của cửa sổ cạnh tranh đạt đến giá trị tối đa, nó sẽ được giữ nguyên và không tăng thêm. Sau khi truyền dữ liệu thành công, giá trị của cửa sổ cạnh tranh sẽ được đặt lại về giá trị ban đầu để bắt đầu quá trình cạnh tranh truy cập kênh tiếp theo.

5. Sơ đồ DCF RTS/CTS

- Là phương thức truyền dữ liệu được sử dụng trong IEEE 802.11 để giảm thiểu hiện tượng mất dữ liệu do xung đột và giải quyết vấn đề về terminal bị che giấu (hidden terminal) và terminal bị tiết lộ (exposed terminal)
- Gồm bốn bước: RTS-CTS-DATA-ACK (tức là yêu cầu gửi, xác nhận gửi, gửi dữ liệu và xác nhận nhận)
- NAV (Network Allocation Vector)

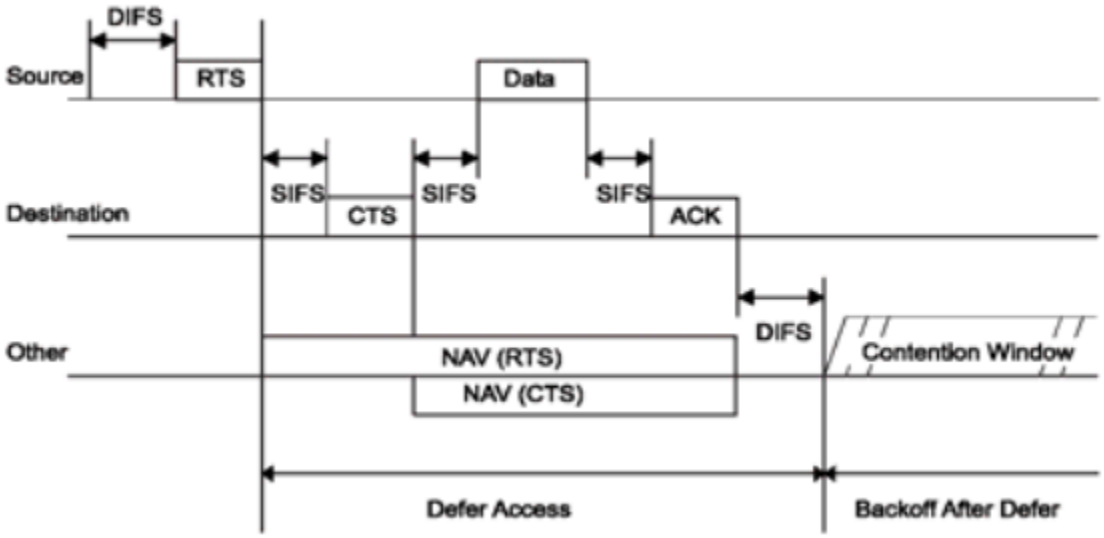
+ Khi một STA muốn truyền dữ liệu, nó sẽ gửi một gói tin RTS cho STA đích để yêu cầu quyền truyền và đặt thời gian truyền tối đa mà nó cần để truyền dữ liệu (Duration field)

+ Nếu STA đích đồng ý cho quyền truyền, nó sẽ gửi một gói tin CTS cho STA gốc để xác nhận quyền truyền và đặt lại thời gian truyền (Duration field) trên toàn bộ mạng

+ Trong thời gian này, NAV (Network Allocation Vector) sẽ được thiết lập tại các STA để biểu thị khoảng thời gian mà truyền dữ liệu không được bắt đầu

- Sau khi nhận được gói tin CTS, STA gốc sẽ bắt đầu truyền dữ liệu trong một khoảng thời gian được chỉ định trong trường Duration của gói tin RTS

- Khi một STA nhận được một khung truyền dữ liệu (DATA), nó sẽ cập nhật NAV của nó với giá trị trong trường Duration của khung truyền dữ liệu để tránh các STA khác truyền dữ liệu trong thời gian này
- Khi một STA nhận được khung ACK (xác nhận nhận), NAV của nó sẽ được đặt lại về giá trị 0 để cho phép truyền dữ liệu tiếp theo.



6. Phân mảnh DCF

Kiểm soát kênh

- Khi một STA muốn gửi một MSDU (MAC Service Data Unit) hoặc MMPDU (MAC Management Protocol Data Unit) lớn hơn kích thước tối đa của khung truyền, nó có thể sử dụng phương thức chia nhỏ khung truyền (fragmentation) để gửi các khung nhỏ hơn.
- Các bước chia nhỏ khung truyền:
    + STA chia nhỏ MSDU hoặc MMPDU thành các khối nhỏ hơn và đặt chúng vào các khung truyền riêng lẻ.
    + STA gửi các khung truyền này với thủ tục truyền cơ bản DCF (DCF Basic Access).
    + STA tiếp tục gửi các khung truyền cho đến khi:
        * Tất cả các khung của MSDU hoặc MMPDU đã được gửi.
        * Không nhận được ACK từ đích.
        * STA bị giới hạn không gửi thêm các khung truyền bởi lớp PHY.
- Khi STA nhận được ACK, nó sẽ tiếp tục gửi các khung truyền tiếp theo cho đến khi tất cả các khung của MSDU hoặc MMPDU đã được gửi hoàn tất.
- Chia nhỏ khung truyền được sử dụng để giảm thiểu hiện tượng mất dữ liệu và tăng cường độ tin cậy trong môi trường mạng không ổn định.

Trường thời gian

- Đối với RTS/CTS: Trường thời lượng trong khung RTS cho biết thời gian cho đến khi kết thúc khung ACK tương ứng, ACK0. Điều này rất quan trọng để đảm bảo rằng các trạm khác không cố gắng truyền trong thời gian này và gây ra va chạm.

- Đối với các đoạn/ACK: Sau khi đoạn đầu tiên được truyền đi và nhận được ACK, trường thời lượng trong khung ACK trước đó cho biết thời gian cho đến khi kết thúc khung ACK tương ứng cho đoạn tiếp theo. Điều này đảm bảo rằng kênh được dành riêng cho toàn bộ quá trình truyền, bao gồm tất cả các đoạn và ACK tương ứng.
- Đối với đoạn cuối cùng/ACK: Sau khi đoạn cuối cùng của MSDU hoặc MMPDU được truyền đi, một ACK sẽ được người nhận gửi để xác nhận đã nhận được toàn bộ tin nhắn. Trường thời lượng trong khung ACK cho đoạn cuối cùng cho biết độ dài của chính khung ACK, vì đây là lần truyền cuối cùng trong chuỗi.
- Bằng cách thiết lập đúng các trường thời lượng trong khung điều khiển, sơ đồ phân mảnh trong DCF có thể giúp giảm va chạm và cải thiện độ tin cậy và hiệu quả của giao tiếp không dây.

VII. PCF

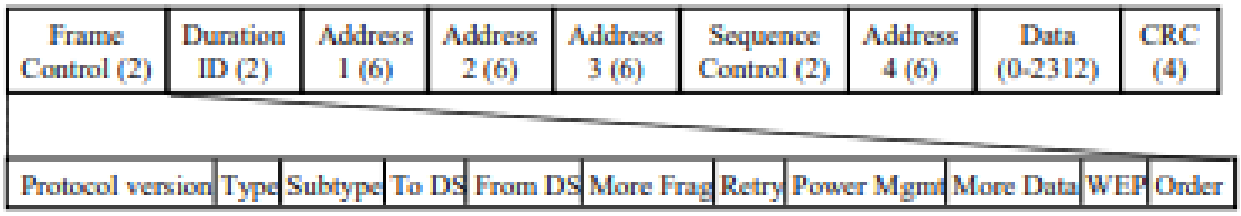
- PCF (Chức năng phối hợp điểm) chỉ khả dụng cho chế độ cơ sở hạ tầng trong mạng IEEE 802.11 vì nó yêu cầu sự hiện diện của điểm truy cập (AP) có thể đóng vai trò là điều phối viên điểm. Trong chế độ cơ sở hạ tầng, tất cả các giao tiếp giữa các trạm không dây được quản lý bởi AP, hoạt động như một điểm điều khiển trung tâm. Điều này trái ngược với chế độ đặc biệt, nơi các trạm không dây giao tiếp trực tiếp với nhau mà không cần AP.
- PCF được xây dựng dựa trên DCF (Chức năng phối hợp phân tán) trong IEEE 802.11 và cung cấp khoảng thời gian không có tranh chấp (CFP) sau đó là khoảng thời gian tranh chấp (CP) trong mỗi siêu khung hình. Trong CFP, PC (điều phối viên điểm) kiểm soát quyền truy cập vào phương tiện và thăm dò các STA (trạm) theo kiểu vòng tròn để truyền dữ liệu của họ. Điều này cung cấp một dịch vụ có giới hạn thời gian vì PC có thể phân bổ một lượng thời gian cố định cho mỗi STA trong CFP, điều này đảm bảo rằng mỗi STA có một khoảng thời gian đảm bảo để truy cập phương tiện. Điều này trái ngược với CP, nơi các STA tranh giành quyền truy cập vào phương tiện bằng cách sử dụng DCF.
- Nhìn chung, PCF cung cấp một cơ chế cung cấp dịch vụ giới hạn thời gian trong mạng IEEE 802.11 bằng cách cho phép PC kiểm soát quyền truy cập vào phương tiện trong CFP và phân bổ các khe thời gian cố định cho mỗi STA. Điều này có thể cải thiện hiệu suất và độ tin cậy của các ứng dụng thời gian thực, nhưng nó đòi hỏi sự hiện diện của AP để đóng vai trò là điều phối viên điểm.
- Trong PCF, khoảng thời gian không có tranh chấp (CFP) được dành riêng cho các dịch vụ có giới hạn thời gian. Điều phối viên điểm (PC) cấp khe thời gian cho các trạm để truyền dữ liệu trong giai đoạn này. PC kiểm soát quyền truy cập vào kênh và lên lịch truyền các trạm, cho phép đảm bảo thời gian truyền và cải thiện QoS (Chất lượng dịch vụ).
- Do đó, cơ chế PCF cung cấp các dịch vụ có giới hạn thời gian bằng cách dành một khoảng thời gian cụ thể để truyền và bằng cách lên lịch truyền các trạm, giúp giảm tranh chấp và đảm bảo cung cấp dữ liệu kịp thời.

VIII. Cấu trúc gói tin MAC IEEE 802.11

1. Cấu trúc gói IEEE 802.11 MAC:

Bao gồm các trường khác nhau được sử dụng để truyền dữ liệu qua mạng không dây. Các lĩnh vực khác nhau là:

- Trường điều khiển khung: Trường này dài 2 byte và chứa thông tin về loại khung và phiên bản giao thức.
- Trường Thời lượng: Trường này dài 2 byte và được sử dụng để chỉ định thời lượng truyền.
- Trường địa chỉ: Các trường này được sử dụng để chỉ định địa chỉ MAC của người gửi và người nhận. Có ba loại trường địa chỉ:
  + Địa chỉ người nhận (RA): dài 6 byte
  + Địa chỉ máy phát (TA): dài 6 byte
  + Địa chỉ nguồn (SA): dài 6 byte



- Trường điều khiển trình tự: Trường này dài 2 byte và được sử dụng để theo dõi số thứ tự của các khung hình.
- Payload: Trường này chứa dữ liệu thực tế cần truyền.
- Trình tự kiểm tra khung hình (FCS): Trường này dài 4 byte và được sử dụng để kiểm tra lỗi trong quá trình truyền dữ liệu.

2. Loại gói:

- Quản lý (00): Được sử dụng cho các khung quản lý mạng như khung xác thực và liên kết.
- Điều khiển (01): Được sử dụng cho các khung điều khiển như RTS, CTS, ACK, v.v.
- Dữ liệu (10): Được sử dụng cho các khung dữ liệu.

3. Loại phụ:

- Khung điều khiển có các kiểu con khác nhau như RTS, CTS, ACK,...
- Khung MAC có thể được truyền giữa các trạm di động, giữa các trạm di động và AP (Điểm truy cập) và giữa các AP qua DS (Hệ thống phân phối).

4. Giải thích địa chỉ:

- Địa chỉ bộ thu (RA): Địa chỉ MAC của người nhận khung hình dự kiến.
- Địa chỉ máy phát (TA): Địa chỉ MAC của người gửi khung.
- Source Address (SA): Địa chỉ MAC của người gửi ban đầu của frame.

IX. Đồng bộ hóa MAC

Đồng bộ hóa MAC trong IEEE 802.11 là quá trình đồng bộ hóa các trạng thái của các STA để có thể truyền và nhận các khung dữ liệu trên một kênh truyền chung. Điều này đảm bảo rằng các STA sẽ tránh giao tranh và xung đột trong quá trình truyền dữ liệu trên cùng một kênh.

Về hạ tầng mạng:

- AP chịu trách nhiệm tạo ra các cảnh báo có dấu thời gian hợp lệ
- Nếu kênh đang được sử dụng, hãy hoãn việc truyền đèn hiệu cho đến khi rảnh
    - Cần có ý nghĩa và tranh chấp sóng mạng nhưng không có ACK để phát sóng.
    - Không có cảm giác sóng mang ảo

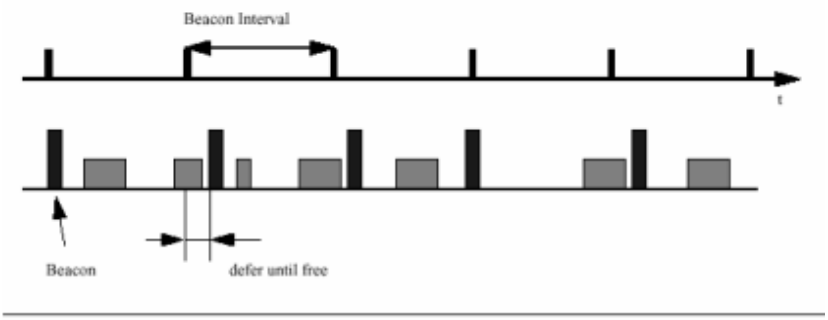


Figure 1: TSF for infrastructure networks in 802.11

- Mạng đặc biệt:
    - Mỗi trạm có trách nhiệm tạo ra đèn hiệu của nó
    - Tất cả các trạm cạnh tranh để truyền đèn hiệu bằng thuật toán lùi ngẫu nhiên tiêu chuẩn
    - Tất cả những người khác điều chỉnh thời gian của họ theo trạm chiến thắng

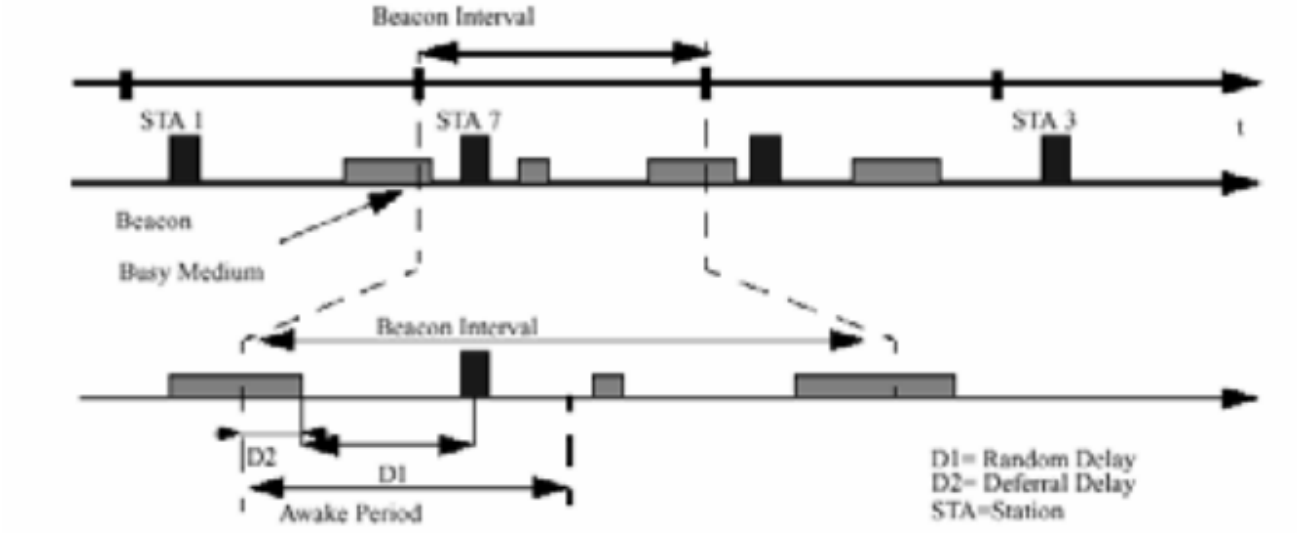


Figure 2: TSF for ad-hoc networks in 802.11

X. Quản lý tiêu hao năng lượng

- Là một cơ chế được sử dụng để tiết kiệm năng lượng của các thiết bị không dây bằng cách cho phép chúng chuyển sang trạng thái công suất thấp khi chúng không chủ động truyền hoặc nhận dữ liệu.
- Có hai trạng thái nguồn STA:

• Thức tỉnh - đầy đủ năng lượng

• Ngủ gật - công suất thấp, không thể truyền / nhận

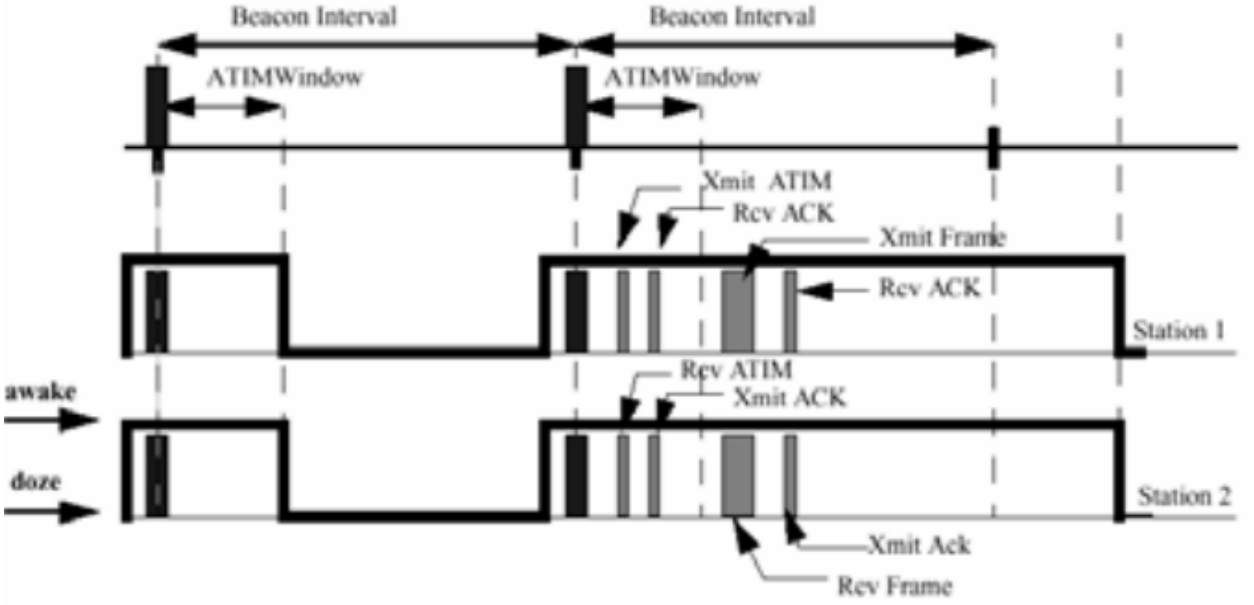
- Trong mạng cơ sở hạ tầng: Khi Trạm (STA) chuyển sang chế độ ngủ gật (chế độ nguồn điện thấp), nó sẽ thông báo cho Điểm truy cập (AP) và AP đệm bất kỳ khung hình nào dành cho STA đó. AP định kỳ gửi các đèn hiệu có chứa dấu thời gian và Bản đồ chỉ báo lưu lượng (TIM) để cho biết liệu có bất kỳ khung hình nào đang chờ xử lý cho STA ở chế độ ngủ gật hay không. Khi STA thức dậy để lắng nghe các đèn hiệu, nó sẽ kiểm tra TIM và nếu có bất kỳ lưu lượng truy cập nào đang chờ xử lý, nó sẽ tỉnh táo cho đến khi quá trình truyền hoàn tất. Điều này cho phép STA tiết kiệm điện khi không có lưu lượng đang chờ xử lý, nhưng vẫn nhận dữ liệu kịp thời khi cần thiết.

- Trong các mạng đặc biệt:

• PM hoạt động khác với trong các mạng cơ sở hạ tầng. Trong các mạng đặc biệt, một khoảng thời gian đặc biệt được gọi là cửa sổ ATIM (Thông báo chỉ báo giao thông đặc biệt) được giới thiệu để thông báo lưu lượng cho các trạm ở chế độ ngủ gật. Trong cửa sổ ATIM, tất cả các trạm, bao gồm cả những trạm ở chế độ ngủ gật, đều tỉnh táo và có thể nhận được thông báo giao thông.

• Khi một trạm ở chế độ ngủ gật thức dậy và phát hiện ATIM, nó sẽ gửi khung phản hồi ATIM đến người gửi lưu lượng truy cập, cho biết rằng nó đã thức và sẵn sàng nhận dữ liệu. Người gửi lưu lượng truy cập sau đó gửi khung dữ liệu đến trạm ở chế độ ngủ gật bằng cách sử dụng các cơ chế xác nhận và backoff tiêu chuẩn.

• Tất cả các trạm, bao gồm cả những trạm ở chế độ ngủ gật, sử dụng các thuật toán backoff tiêu chuẩn để tránh va chạm trong cửa sổ ATIM. Khi cửa sổ ATIM kết thúc, các trạm ở chế độ ngủ gật có thể quay trở lại chế độ ngủ cho đến khi đèn hiệu hoặc ATIM tiếp theo đánh thức chúng.



XI. Kết nối vào điểm truy cập

Điểm truy cập (Access Point - AP) là thiết bị cung cấp dịch vụ kết nối mạng không dây cho các thiết bị di động như điện thoại thông minh, máy tính bảng hoặc máy tính xách tay.

1. Nhận diện truy cập:

- Nhận diện điểm truy cập (AP) có thể được thực hiện thông qua hai phương pháp chính: Đèn hiệu và Thăm dò.
- Đèn hiệu là tín hiệu được AP gửi đi để quảng cáo sự hiện diện và tính khả dụng của nó. Một AP thường gửi đèn hiệu với tốc độ 10 lần mỗi giây. Khi thiết bị người dùng nhận được đèn hiệu, nó có thể trích xuất thông tin như SSID của AP, loại bảo mật và cường độ tín hiệu.
- Mặt khác, thăm dò liên quan đến việc thiết bị người dùng tích cực tìm kiếm các AP có sẵn. Thiết bị lần lượt quét tất cả các kênh để phát hiện bất kỳ đèn hiệu nào có sẵn. Ngoài ra, người dùng có thể gửi "tin nhắn yêu cầu thăm dò" để chủ động tìm kiếm các AP mới. Thăm dò thường nhanh hơn quét, vì nó tập trung vào việc tích cực tìm kiếm các AP có sẵn thay vì chờ đợi đèn hiệu.
- Khi thiết bị người dùng phát hiện nhiều AP có sẵn, nó có thể chọn một AP có cường độ tín hiệu mạnh nhất để kết nối, trừ khi nó đã được định cấu hình cụ thể để kết nối với một AP nhất định.

2. Xác thực - Authentication:

- Để kết nối được với AP, người dùng cần phải xác thực với AP bằng cách cung cấp thông tin đăng nhập chính xác, chẳng hạn như mật khẩu hoặc giấy chứng nhận. Người dùng có thể gửi yêu cầu xác thực đến AP bằng cách kết nối đến mạng Wifi được cung cấp bởi AP và đăng nhập vào trang đăng nhập của AP.
- Sau khi nhận được yêu cầu xác thực, AP sẽ khởi tạo một giao thức phản hồi thách thức (challenge-response protocol) để xác thực thông tin đăng nhập của người dùng. Giao thức này thường sử dụng mật mã học để bảo vệ thông tin đăng nhập khỏi việc truy cập trái phép.
- Nếu thông tin đăng nhập được xác thực chính xác, AP sẽ cấp cho người dùng quyền truy cập vào mạng Wifi. Việc xác thực giúp đảm bảo rằng chỉ có những người dùng được phép truy cập vào mạng Wifi được kết nối với AP và tránh được các tấn công mạng từ những kẻ không có ý đồ tốt.

3. Kết hợp:

- Khi người dùng muốn kết nối với AP, họ sẽ gửi yêu cầu liên kết đến AP. Yêu cầu liên kết chứa thông tin về các khả năng và yêu cầu của người dùng, chẳng hạn như tốc độ dữ liệu được hỗ trợ và các giao thức bảo mật.
- AP phản hồi bằng phản hồi liên kết, bao gồm thông tin về trạng thái kết nối, tốc độ dữ liệu được hỗ trợ và các tài nguyên được phân bổ. Phản hồi liên kết cũng chứa một khoảng thời gian đèn hiệu chỉ định tần suất AP gửi các khung đèn hiệu, được sử dụng để giữ cho kết nối của người dùng hoạt động.
- Trong quá trình kết nối của người dùng với AP, người dùng có thể chuyển vùng giữa các AP. Để làm như vậy, trước tiên người dùng phải gửi một thông báo tách rời đến AP hiện tại, cho biết rằng nó không còn được liên kết với nó nữa. Sau đó, người dùng gửi một yêu cầu liên kết đến AP

mới mà nó muốn kết nối và quá trình xác thực và liên kết được lặp lại với AP mới. Quá trình chuyển vùng này cho phép người dùng duy trì kết nối liên tục khi họ di chuyển xung quanh mạng.

XII. Dynamic Host Configuration Protocol - DHCP

- Giao thức cấu hình máy chủ động (DHCP) thường được áp dụng trong mạng Wifi gia đình để tự động gán địa chỉ IP cho các thiết bị kết nối với mạng.
- Khi một thiết bị tham gia mạng, nó sẽ gửi yêu cầu DHCP đến máy chủ DHCP của mạng, thường là bộ định tuyến. Máy chủ DHCP sau đó chỉ định một địa chỉ IP có sẵn từ một nhóm địa chỉ và thông tin cấu hình mạng khác như mặt nạ mạng con, cổng mặc định và địa chỉ máy chủ DNS.
- Quy trình tự động này giúp loại bỏ nhu cầu người dùng gán địa chỉ IP theo cách thủ công cho từng thiết bị trên mạng. Nó cũng đảm bảo rằng không có xung đột địa chỉ IP, trong đó hai hoặc nhiều thiết bị có cùng địa chỉ IP trên mạng, điều này có thể gây ra sự cố giao tiếp mạng.

Tóm lại, DHCP được ứng dụng trong mạng Wifi gia đình để tự động hóa quá trình gán địa chỉ IP cho các thiết bị trên mạng, giúp người dùng kết nối và sử dụng mạng dễ dàng hơn.

B. WEP

I. Giới thiệu chung

Dần dà theo thời gian, số lượng người dùng Internet, đặc biệt là với Wifi ngày càng lớn, đặt ra yêu cầu về việc đảm bảo an toàn trong truyền thông dữ liệu không dây. Cả người dùng hợp lệ và hacker đều có quyền truy cập thông tin cũng như truyền tin trên mạng không dây, từ đó đòi hỏi một phương pháp để xác thực người dùng nhằm tránh các cuộc tấn công gây hại đến mạng và người dùng.

Lúc bấy giờ, chuẩn mạng không dây IEEE 802.11 đang là chuẩn có mặt trong đa số thiết bị cũng như sản phẩm công nghệ, do đó yêu cầu cụ thể là xây dựng các lớp cơ sở bảo mật cho IEEE 802.11. Từ yêu cầu thiết yếu đó, năm 1999, Hiệp hội Kỹ sư Điện - Điện tử (IEEE) đã công bố WEP (Wired Equivalent Protocol), và từ đó WEP đã được sử dụng rộng rãi trong lĩnh vực truyền thông thông tin đến tận năm 2005, trước khi bị "lấn át" bởi các giao thức khác bởi nhiều điểm yếu và lỗ hổng của nó.

Mặc dù vậy, WEP vẫn mang nhiều giá trị trong lĩnh vực nghiên cứu và giáo dục, cũng như là trong các hệ thống nhỏ, không đặt nặng yêu cầu bảo mật, sự eo hẹp về tài chính hoặc khó đề có thể thay thế các thiết bị cũ. [1]

Section 8.2.2 của tài liệu về WEP của IEEE công bố năm 1999 chỉ ra mục tiêu hướng đến khi xây dựng WEP là:

- Đủ mạnh để chống các cuộc tấn công từ hacker, đặc biệt là dò khóa thông qua brute-force.
- Khả năng tự đồng bộ.
- Tối ưu chi phí và bộ nhớ.
- Có thể đóng gói trong các sản phẩm lưu thông trên thị trường quốc tế.
- Không bắt buộc phải cài đặt trên chuẩn 802.11.

Từ đó có thể nhận định rằng WEP không được sinh ra cho mục đích bảo mật trong quân sự.

Có 2 lớp WEP: loại truyền thống sử dụng khóa 40 bit và loại mở rộng sử dụng khóa 128 bit.

II. Ba mục đích của WEP trong thực tế:

Trong thực tế, WEP có 03 mục đích chính:

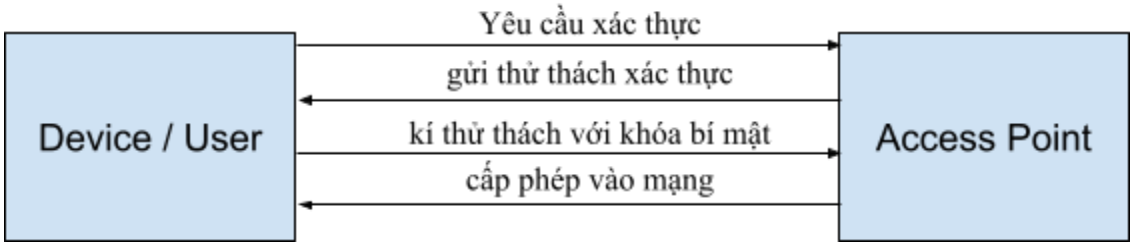
- Tính bảo mật (Confidentiality): bảo đảm thông tin trong mạng không bị nghe lén từ bên ngoài.
- Tính toàn vẹn (Integrity): bảo đảm thông tin truyền đi trong mạng không bị thay đổi.
- Kiểm soát truy cập: bảo đảm "kẻ ngoại lai" không sử dụng được hệ thống mạng.

III. Các thức hoạt động:

Bảo mật trên WEP gồm 2 phần chính: Authentication và Encryption

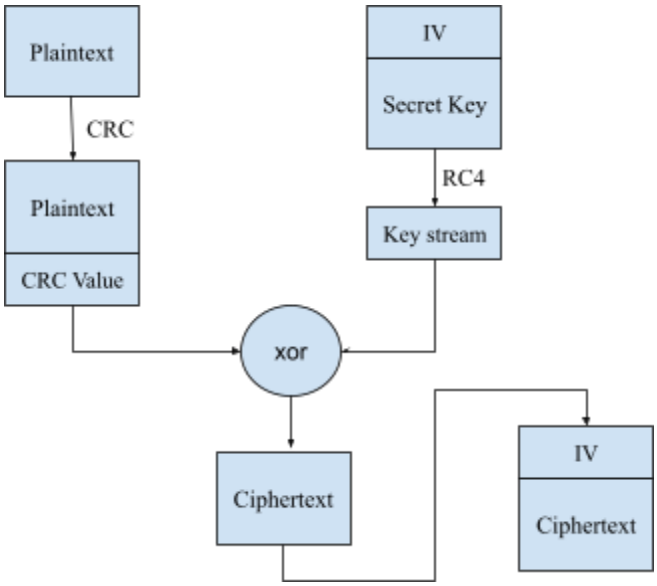
1. Authentication

Quá trình xác thực đảm bảo chỉ người dùng có khóa WEP mới được truy cập vào mạng. Quá trình xác thực được diễn ra như sơ đồ sau:



- Thử thách xác thực (challenge) là một văn bản có thể đọc dài 128 bit.
- Sau khi xác thực, WEP không hề tạo ra sự trao đổi khóa nào khác giữa 2 bên, và sử dụng luôn khóa bí mật ban đầu cho quá trình mã hóa. Do đó khi hacker có được khóa bí mật, WEP sẽ không có cách nào để nhận biết thông điệp được gửi đi là từ người dùng hay từ "kẻ ngoại lai".
- Hacker có thể sử dụng phương pháp Man-In-The-Middle để bắt lấy khóa bí mật trong quá trình xác thực.

2. Encryption



- Quá trình mã hóa có thể được mô tả như sơ đồ bên trên [2]

- WEP sử dụng CRC (Cyclic Redundancy Check) để tính toán tính toàn vẹn của thông điệp. Kết quả của quá trình CRC này được gắn với plaintext (1).
- Mặt khác, IV được gắn với khóa bí mật, thông qua RC4 tạo nên chuỗi khóa key stream (2).
- Giá trị (1) và (2) được XOR với nhau tạo nên ciphertext.
- Ciphertext kết hợp với IV được lưu trong frame header và gửi đi trong mạng.
- Đối với bên nhận, để đọc gói tin, đầu tiên lấy Ciphertext XOR với Keystream ở (2), sau đó đối chiếu giá trị CRC với ban đầu để đảm bảo thông điệp nhận được là đúng.
- IV có thể được tái sử dụng ở bất kì gói tin nào.

IV. Điểm yếu và lỗ hổng của WEP:

- Kích thước của IV nhỏ, dễ trùng lặp: với IV 24-bit chỉ có thể tạo ra 16,777,216 RC4 stream cipher khác nhau [3] và dễ dàng bị trùng lặp chỉ sau vài giờ hoạt động.
- Vấn đề khóa yếu trong trong mã hóa RC4: các IV có thể dễ dàng bị đoán ra, trở thành điểm yếu bị khai thác bởi passive attack..
- Dễ dàng tạo ra một tin nhắn xác thực giả mạo, chỉ thông qua quan sát quá trình xác thực mà hacker có thể tìm ra được keystream hoặc thậm chí khóa bí mật.
- Lỗ hổng trong checksum: CRC có thể kiểm tra lỗi trong plaintext nhưng lại không thực hiện việc kiểm tra trong ciphertext. Hacker thậm chí còn có thể tính toán một giá trị ICV dựa trên một plaintext bị lộ (known plaintext) để tạo nên một message giả và "cấy" nó vào trong mạng.

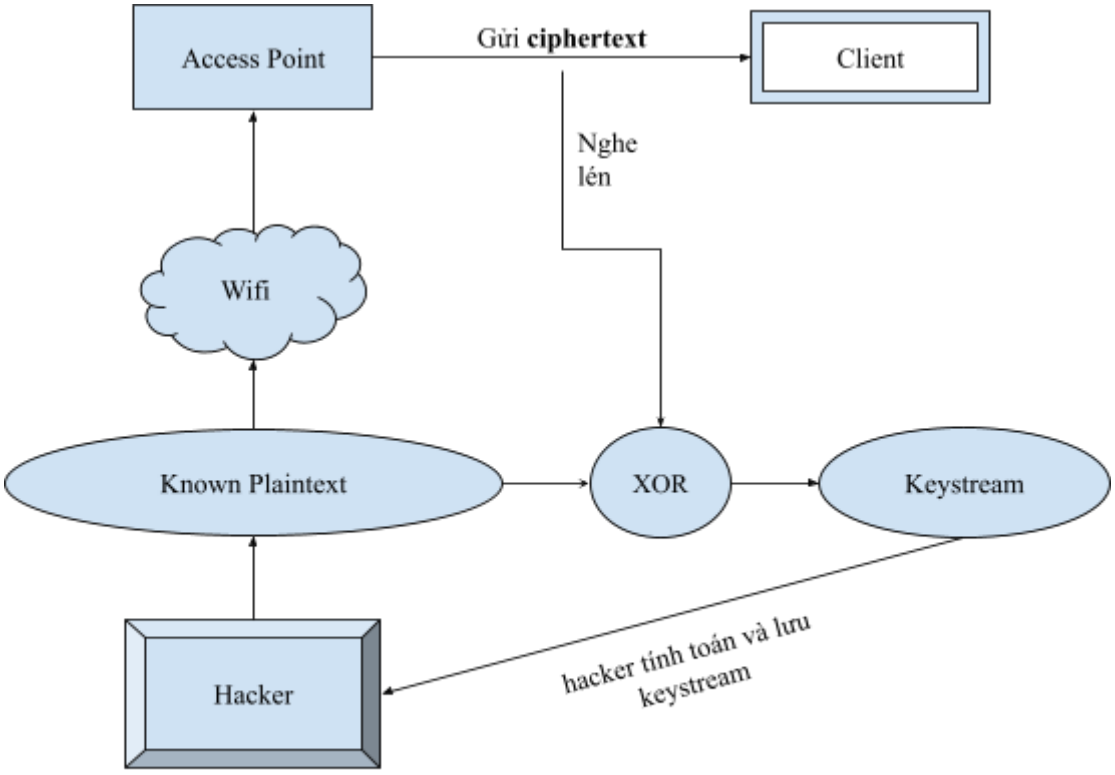


Figure: Known Plaintext Attack

C. Kiểm soát truy cập với 802.1X, EAP và RADIUS_Điểm yếu của WEP:

I. IEEE 802.11 :

1. 802.11X là gì ?

Giao thức IEEE 802.1X điều khiển truy cập dựa vào PORT hay Điều khiển truy cập mạng dựa trên cổng IEEE 802.1X được thiết kế để cung cấp quyền truy cập chức năng điều khiển cho mạng LAN. Bảng dưới định nghĩa ngắn gọn các thuật ngữ chính được sử dụng trong IEEE Chuẩn 802.11. Các định nghĩa trong phần này supplicant, network access point, authentication server tương ứng với các từ trong EAP peer, authenticator, authentication server.

2. Các thành phần của IEEE 802.1X:

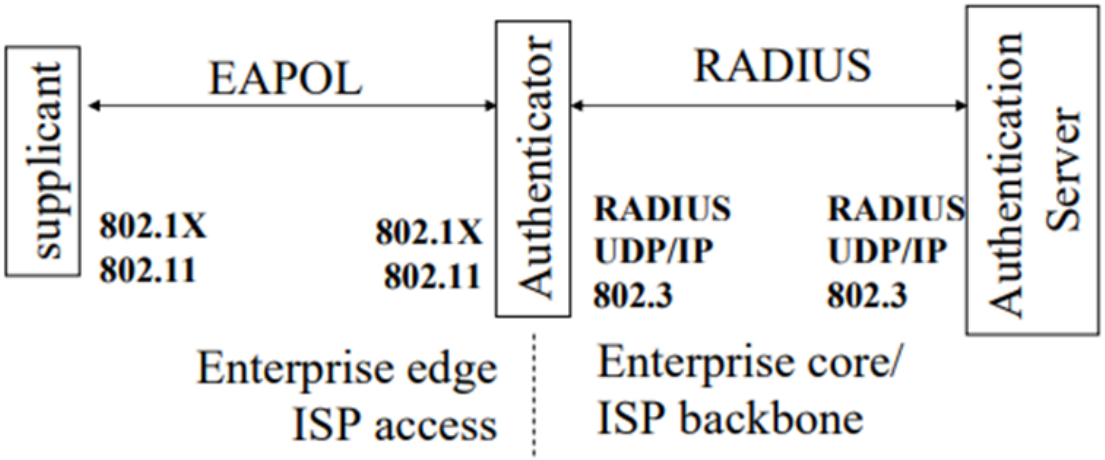
- Authenticator: Một thực thể ở một đầu của phân đoạn LAN Point-to-point có khả năng xác thực thực thể này với thực thể khác cuối liên kết**.**
- **Authentication Exchange:** Cuộc trò chuyện giữa hai bên giữa các hệ thống thực hiện quy trình xác thực
- **Authentication Process:** Các hoạt động mã hóa và khung dữ liệu hỗ trợ thực hiện xác thực.
- **Authentication Server(AS):** Một thực thể cung cấp dịch vụ xác thực cho một **Authenticator**. Dịch vụ này xác thực từ thông tin đăng nhập được cung cấp bởi **Supplicant**.
- **Authentication Transport:** Phiên làm việc tại tầng transport vận chuyển trao đổi xác thực giữa hai hệ thống.
- **Bridge port:** Một port của một bridge IEEE 802.1D hoặc 802.1Q.
- **Network access port**: Một port của một hệ thống với mạng LAN. Nó có thể là một cổng vật lý, chẳng hạn như một MAC LAN duy nhất được gắn vào một đoạn LAN vật lý hoặc một cổng logic, ví dụ, một liên kết IEEE 802.11 giữa một trạm thu phát và một điểm truy cập
- **Port access entity(PAE)**: Các thực thể giao thức liên kết với một cổng. Nó có thể hỗ trợ chức năng giao thức liên quan đến authenticator, supplicant, hoặc cả hai.
- Supplicant :

  Một thực thể ở một đầu của phân đoạn LAN point-to-point tìm cách được xác thực bởi authenticator gắn vào đầu kia của liên kết đó.

  AS(Authentication server) xác thực một supplicant (sử dụng giao thức xác thực), authenticator chuyển các thông điệp điều khiển và xác thực giữa các supplicant và AS; kênh điều khiển 802.1X không bị chặn, nhưng kênh dữ liệu 802.11 bị chặn. Khi một supplicant được xác thực và các khóa được cung cấp, authenticator có thể chuyển tiếp dữ liệu từ supplicant, tùy thuộc vào quyền truy cập được xác định trước kiểm soát các hạn chế cho supplicant vào mạng. Trong những trường hợp này, kênh dữ liệu được bỏ chặn.

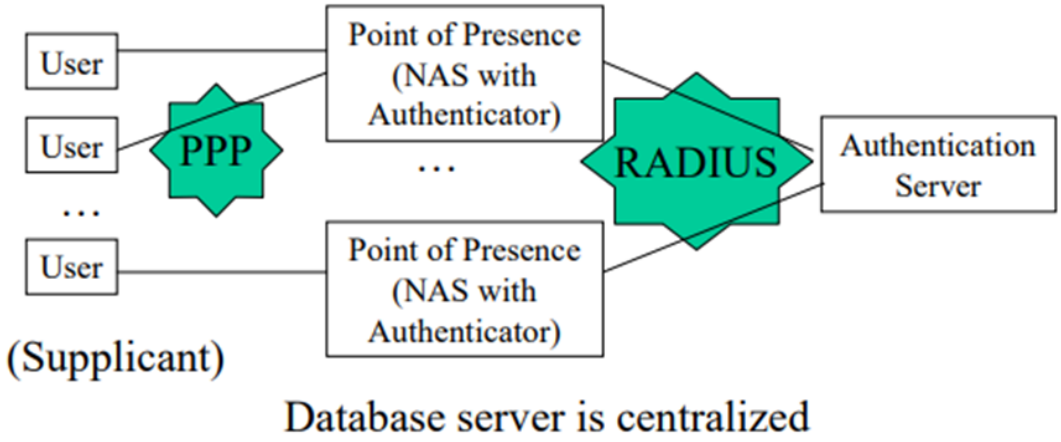
Như được chỉ ra trong hình bên dưới 802.1X sử dụng các khái niệm về kiểm soát và không kiểm soát cổng(port). Các port là các thực thể logic được xác định trong authenticator và kết nối cổng vật lý. Mỗi cổng logic được ánh xạ tới một trong hai loại này của các cổng vật lý. Một cổng không được kiểm soát cho phép trao đổi các đơn vị dữ liệu giao thức (PDU) giữa supplicant và AS, bất kể trạng thái xác thực của supplicant. Một cổng được kiểm soát cho phép trao đổi PDU giữa một supplicant và các hệ thống khác trên mạng chỉ khi trạng thái hiện tại của supplicant được phép trao đổi.

3. **Kiến trúc của IEEE 802.1X :**



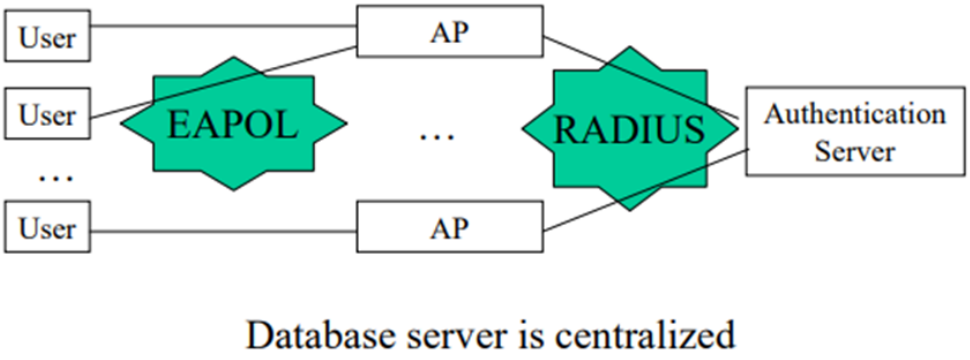
- Authenticator hoạt động như một cầu nối
- 802.1X là một framework, không phải là một đặc điểm kỹ thuật hoàn chỉnh. Cơ chế xác thực thực tế được thực hiện bởi Authentication Server.

4. **Xác thực dùng Dial-In User.**



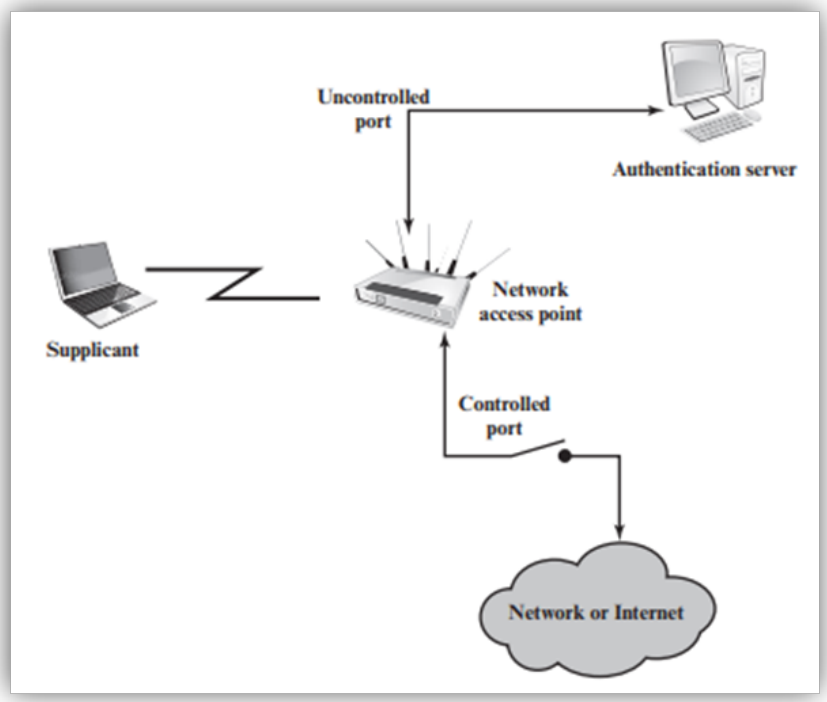
- PPP: Giao thức xác định hai phương thức xác thực yếu: PAP và CHAP : Người dùng cung cấp USERNAME và PASS.
- PAP (Giao thức xác thực mật khẩu): USERNAME và PASS được truyền dưới dạng văn bản rõ.
- CHAP(Giao thức xác thực bắt tay):Mã hóa các bí mật trao đổi giữa client và server.

5. **Xác thực dùng người dùng mạng không dây.**



II. EAPOL:

Thành phần thiết yếu được sử dụng trong 802.1X là một giao thức được gọi là EAPOL (EAP qua mạng LAN). EAPOL hoạt động ở các lớp mạng và sử dụng chuẩn IEEE 802 LAN, chẳng hạn như Ethernet hoặc Wifi, ở tầng liên kết. EAPOL cho phép supplicant giao tiếp với một authenticator và hỗ trợ trao đổi các gói EAP cho authentication server.



Authenticator: Một đầu của link EAP, chịu trách nhiệm khởi tạo việc xác thực. Trong môi trường truy nhập, thường authenticator là các Access Switch.
Supplicant/Peer: Một đầu của link EAP, chịu trách nhiệm trả lời authenticator. Supplicant có thể là máy tính người dùng, hoặc bất kỳ thiết bị điện tử nào muốn truy cập vào hệ thống mạng (điện thoại, máy in, máy chấm công, camera, IPPhone…)
Backend authentication server: Một phần tử mạng, cung cấp dịch vụ xác thực cho authenticator. Đây có thể là một phần của authenticator, hoặc tách thành một phần tử độc lập với authenticator (gọi là EAP server).

1. **Ứng dụng của EAP:**

   Sử dụng cho mục đích xác thực quyền truy nhập hệ thống ở lớp Access. Có thể hiểu, **EAP là một framework**, cung cấp cơ chế trao đổi các gói tin giữa authenticator và supplicant để phục vụ xác thực. Còn việc trao đổi thông tin gì, xác thực các thông tin đó ra làm sao là nhiệm vụ của các giao thức xác thực (ex. TLS, PEAP, FAST…).
2. **EAP procedure**

   - Authenticator gửi ra bản tin Request để xác thực peer (supplicant). Nội dung bản tin Request chứa các trường thông tin mô tả đối tượng được request. Thông thường, Authenticator cần gửi bản tin Identity Request để thu thập thông tin mô tả

supplicant => Có thể bypass nếu authenticator có thể lấy được các thông tin cần thiết từ bằng các phương pháp khác nhau, tùy thuộc vào phương thức xác thực đang dùng (ex. Supplicant đang cắm cổng nào, địa chỉ MAC của supplicant…).

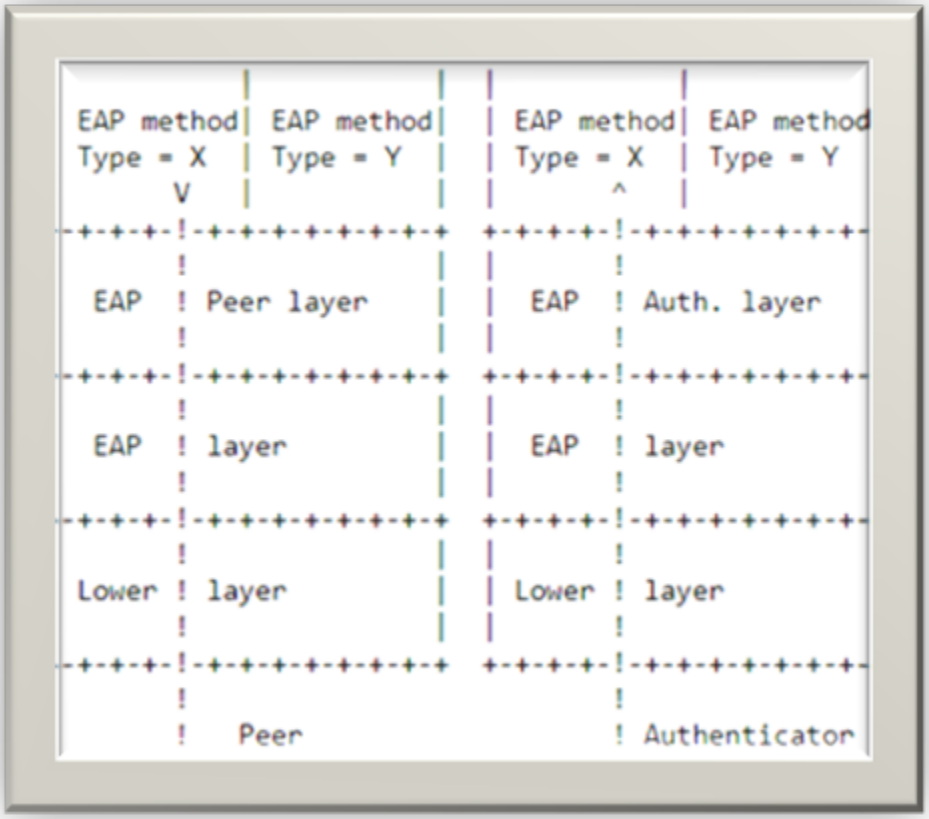
- Peer trả lời bản tin Response, chứa các nội dung trả lời cho Request (Type field giống với trong bản tin Request).

- Sau khi nhận được bản tin Response, nếu chưa thu thập đủ thông tin, Authenticator tiếp tục gửi bản tin Request. Authenticator chỉ gửi ra bản tin Request khi nhận được bản tin Response từ peer. Trong trường hợp không nhận được Response, authenticator có thể retransmit bản tin Request.

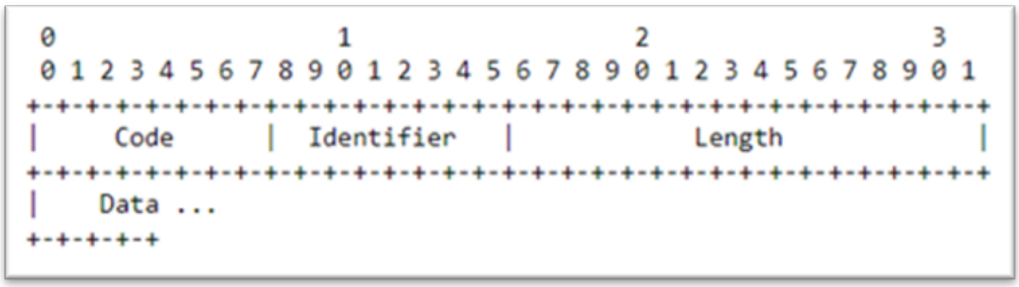
- Quá trình Request thông tin được lặp lại cho đến khi authenticator có thể xác thực peer. Nếu xác thực không thành công (có một Response không hợp lệ từ peer) => Authenticator gửi ra EAP Failure (Code 4). Ngược lại, nếu xác thực thành công => Authenticator gửi ra EAP Success (Code 3)

3. **Lợi ích của EAP:**
   - EAP hỗ trợ nhiều phương thức xác thực khác nhau mà không cần pre-negotiate
   - Network Access Server (NAS) (ex. Access Switch) không cần phải biết các giao thức xác thực, và có thể hoạt động ở chế độ pass-through.
   - Việc phân tách authenticator khỏi backend authentication server giúp cho việc quản trị và thực hiện chính sách đơn giản hơn.
4. **Bất lợi của EAP**
   - Access Switch, AP cần hỗ trợ 802.1x để có thể sử dụng EAP.
   - Phân tách authenticator khỏi backend authentication server khiến việc phân tích bảo mật trở nên phức tạp hơn
5. **Phân lớp chức năng của EAP**
   - **Lower layer**: Chứa các chức năng gửi và nhận EAP frame giữa peer và authenticator. EAP có thể chạy trên các môi trường PPP, wired 802 LAN (802.1x), wireless LAN (802.11), UDP, IKEv2, TCP.
   - **EAP layer**: Làm việc với lower layer để gửi và nhận EAP packet, phát hiện duplicate, retransmission.
   - **EAP peer và authenticator layer:** Một thiết bị có thể vừa là peer, vừa là authenticator. Vì vậy, lớp này giúp thiết bị phân tách các gói tin EAP vào đúng luồng xử lý của peer hoặc authenticator. Thiết bị sẽ căn cứ vào trường Code trong gói tin EAP để xác định sẽ đẩy EAP packet vào EAP peer layer hay EAP authenticator layer.

- **EAP method layer:** Là các thuật toán/phương pháp thực hiện xác thực. Do bản thân EAP không hỗ trợ fragmentation, nên EAP method layer cũng chứa chức năng phân mảnh dữ liệu vào các



6. EAP Packet Format:



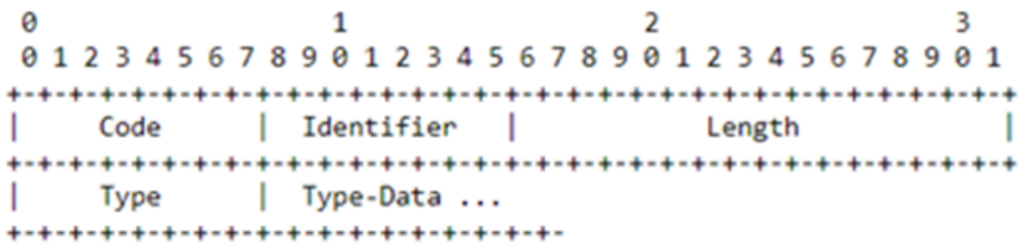
Code: Mô tả loại EAP packet

- Request
- Response
- Success

- Failure

Identifier: Thông tin so khớp giữa bản tin Response và Request.
Length: Độ dài của EAP packet, đơn vị octet.

1. **Bản tin Request và Response:**



Mỗi bản tin Request gửi ra được đánh một giá trị Identifier khác với những giá trị đã gửi ra trước đó. Nếu là bản tin re-transmiss, thiết bị sẽ giữ nguyên giá trị Identifier của bản tin Request đang được gửi lại. Bản tin Response phải có trường Identifier giống với bản tin Request, nếu không sẽ bị drop**.**

2. **Bản tin Success và Failure:**

Success packet được gửi ra bởi authenticator sau khi nó hoàn thành quá trình thực hiện xác thực EAP, thông báo cho peer biết nó đã được xác thực thành công. Ngược lại, nếu không thể xác thực thành công, authenticator sẽ gửi cho peer bản tin Failure với Code = 4.
Do chỉ có mục đích thông báo trạng thái Success hoặc Failure nên bản tin này không có trường Data.

7. **Các Type của EAP:**

(1) Identity
(2) Notification
(3) Nak (chỉ dùng cho bản tin Response)
(4) MD5-Challenge
(5) One Time Password – OTP
(6) Generic Token Card – GTC
Ngoài các giá trị cơ bản ở trên, một số Type value phổ biến bao gồm:
(25) PEAP
(26) EAP/MS-CHAPv2
(43) EAP-FAST
…
Identity Type

Identity Type được sử dụng để lấy thông tin mô tả của peer (ex. Username…), thường được gửi ra khi bắt đầu một Request – Response conversation.
Notification Type
Những thông tin trong Notification Request sẽ được hiển thị đến người dùng.
Nak Type
Được peer dùng trong bản tin Reponse để báo cho authenticator rằng authentication method không được hỗ trợ. Nếu nhận được Nak từ peer, authenticator có thể lựa chọn một authentication method khác => Đây có thể coi là phương án để negotiate giữa peer và authenticator. Trong trường hợp peer không hỗ trợ bất kỳ authentication method nào, nó sẽ trả lời bản tin Nak Response với giá trị = 0, khi đó authenticator sẽ không gửi thêm Request nữa.

8. **Phương thức xác thực EAP.**
   - **EAP-MD-5 (Message Digest)** là loại xác thực EAP cung cấp hỗ trợ EAP cấp cơ sở. EAP-MD-5 thường không được khuyến nghị sử dụng cho việc triển khai Wi-Fi LAN vì nó có thể cho phép nguồn gốc mật khẩu của người dùng. Nó chỉ cung cấp xác thực một chiều - không có xác thực chung của máy khách Wi-Fi và mạng. Và rất quan trọng là nó không cung cấp một phương tiện để dẫn xuất các khóa quyền riêng tư tương đương (WEP) động mỗi phiên có dây.
   - **EAP-TLS (Bảo mật lớp truyền tải)** cung cấp xác thực chung và dựa trên chứng chỉ của máy khách và mạng. Nó dựa trên chứng chỉ phía máy khách và phía máy chủ để thực hiện xác thực và có thể được sử dụng để tự động tạo ra các khóa WEP dựa trên phiên và người dùng để đảm bảo liên lạc tiếp theo giữa máy khách WLAN và điểm truy cập. Một hạn chế của EAP-TLS là chứng chỉ phải được quản lý ở cả phía máy khách và máy chủ. Đối với một cài đặt WLAN lớn, đây có thể là một tác vụ rất rườ i.
   - **EAP-TTLS (Tunneled Transport Layer Security)** do Funk Software* và Certicom* phát triển, như một phần mở rộng của EAP-TLS. Phương pháp bảo mật này cung cấp xác thực chung, dựa trên chứng chỉ của máy khách và mạng thông qua một kênh được mã hóa (hoặc đường hầm), cũng như một phương tiện để dẫn ra các khóa WEP động, mỗi người dùng, mỗi phiên. Không giống như EAP-TLS, EAP-TTLS chỉ yêu cầu chứng chỉ phía máy chủ.

III. RADIUS:

1. Thuật ngữ RADIUS

Được viết tắt từ cụm từ Remote Authentication Dial-In User Service và nó hoạt động dựa trên mô hình client (máy khách) – server (máy chủ). RADIUS cho phép các server liên hệ, kết nối với server trung tâm nhằm mục đích xác thực tính hợp pháp của người dùng khi truy cập mạng.

2. Cách thức hoạt động của xác thực RADIUS

Với RADIUS người dùng mạng từ xa sẽ thông qua thiết bị NAS (máy chủ lưu trữ kết nối mạng) để kết nối với mạng của họ. Client RADIUS không phải là một cá nhân mà đó chính là hệ thống NAS còn server xác thực chính là server RADIUS.

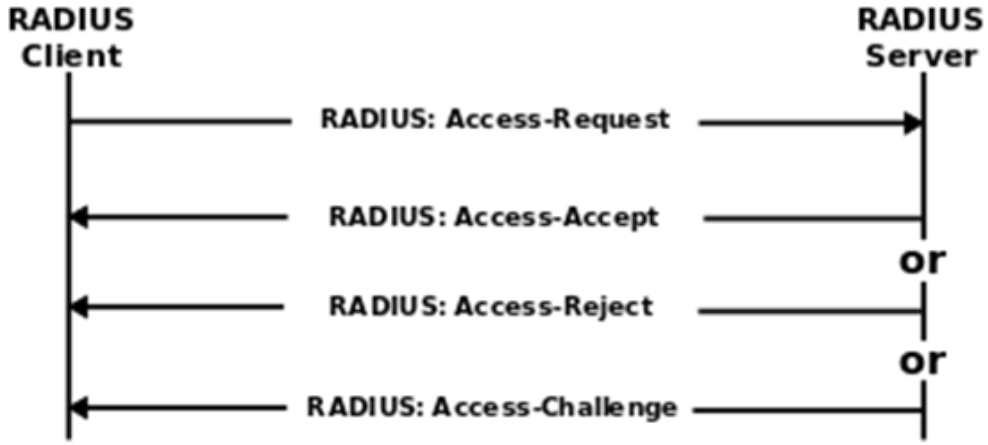
Người dùng muốn truy cập từ xa vào mạng được bảo vệ bởi RADIUS thì họ phải cung cấp ID, mật khẩu, địa chỉ IP. Và những thông tin này sẽ được NAS chuyển tới server RADIUS để tiến hành xác thực. Các loại server RADIUS gồm:

- **Dial-in servers:** đóng vai trò trung gian để người dùng truy cập vào mạng công ty hoặc ISP bằng modem.

- **Virtual private network servers**: xác thực để người dùng từ xa kết nối thành công, an toàn với mạng riêng ảo.

- **Wireless access points**: chấp nhận yêu cầu từ wireless clients (thiết bị kết nối với bộ phát wifi) để kết nối với mạng.

- **Managed network access switches**: giao thức xác thực 802.1x được loại server RADIUS này triển khai để cho phép người dùng từ xa kết nối mạng thành công.



Từ chối truy cập - Access Reject

Người dùng bị từ chối truy cập vào tất cả các tài nguyên mạng. Lý do có thể bao gồm việc không cung cấp chứng nhận hoặc tài khoản người dùng không xác định hoặc không hoạt động, bị khóa, v.v...

Yêu cầu gửi thêm thông tin truy cập - Access Challenge

Yêu cầu thông tin bổ sung từ người dùng như mật khẩu phụ, mã PIN, mã thông báo hoặc thẻ. Access Challenge cũng được sử dụng trong các hộp thoại xác thực

phức tạp hơn, khi đường hầm (tunnel) bảo mật được thiết lập giữa máy người dùng và máy chủ RADIUS để giấu thông tin đăng nhập khỏi NAS.

Chấp nhận truy cập - Access Accept

Người dùng được cấp quyền truy cập. Khi người dùng được xác thực, máy chủ RADIUS sẽ thường kiểm tra xem người dùng có được phép sử dụng dịch vụ mạng được yêu cầu hay không. Chẳng hạn một người dùng nào đó có thể được phép sử dụng mạng không dây, nhưng không được sử dụng VPN của công ty. Thông tin này có thể được lưu trữ cục bộ trên máy chủ RADIUS hoặc có thể được truy vấn tại một nguồn bên ngoài như LDAP hoặc Active Directory.

3. **Server RADIUS được sử dụng như thế nào?**

Sau khi nhận được yêu cầu từ thiết bị NAS, server RADIUS xác thực bằng hai cách:

- **Giao thức xác thực mật khẩu (PAP):** những thông tin về người dùng từ xa như ID, mật khẩu sẽ được client RADIUS chuyển tới server xác thực RADIUS. Nếu hồ sơ của người dùng đúng, chính xác thì họ sẽ được kết nối với mạng.
- **Giao thức xác thực bắt tay (CHAP):** hình thức này còn được gọi là bắt tay ba bước, CHAP mã hó các bí mật được trao đổi giữa client và server. So với PAP thì xác thực CHAP bảo mật cao hơn.

Một RADIUS proxy client được thiết kế phù hợp để chuyển tiếp những thông tin cần xác thực tới các server RADIUS khác. Trong khi đó các proxy RADIUS lại tạo điều kiện xác thực tập trung ở những mạng quy mô lớn hoặc phân tán về yếu tố địa lý.

D. Giao thức bảo toàn khóa tạm thời - Temporal Key Integrity Protocol (TKIP)

I. Giới thiệu về Temporal Key Integrity Protocol (TKIP)

- Giao thức Temporal Key Integrity Protocol (TKIP) là một phần của chuẩn Wifi IEEE 802.11i, được sử dụng để đảm bảo an toàn thông tin truyền qua mạng Wifi.
- TKIP được thiết kế để cải tiến mức độ an toàn so với giao thức WEP (Wired Equivalent Privacy), bằng cách tăng cường tính bảo mật và khắc phục những lỗ hổng của WEP.
- TKIP sử dụng nhiều kỹ thuật mã hóa khác nhau để giữ cho mật khẩu và dữ liệu được truyền đi an toàn, bao gồm việc sử dụng mã hóa RC4 với độ dài khóa lớn hơn.
- Tuy nhiên, TKIP được xem là không còn an toàn và hiệu quả sau khi bị phân tích và phát hiện nhiều lỗ hổng bảo mật. Hiện nay, giao thức bảo mật chính được sử dụng trong Wifi là giao thức AES-CCMP (Advanced Encryption Standard - Counter with CBC-MAC Protocol) (sẽ đề cập trong mục E).

II. Cơ chế hoạt động

Cơ chế của TKIP bao gồm các thành phần chính sau:

- Sử dụng khóa tạm thời: TKIP sử dụng khóa tạm thời để mã hóa dữ liệu trên đường truyền. Khóa này được tạo ra bằng cách kết hợp một mật khẩu với một số thông tin khác (như địa chỉ MAC của thiết bị).
- Tự động thay đổi khóa: Khi sử dụng TKIP, khóa tạm thời sẽ được thay đổi định kỳ (thường xuyên) trong khi truyền dữ liệu. Điều này làm giảm khả năng tấn công từ điểm truy cập nguy hiểm.
- Mã hóa RC4: TKIP sử dụng RC4 (Rivest Cipher 4) là một thuật toán mã hóa số học để mã hóa dữ liệu trên đường truyền.
- Kiểm tra tính tổng thể: TKIP kiểm tra tính toàn vẹn của gói dữ liệu trên đường truyền để đảm bảo rằng không có ai đã sửa đổi nó giữa lúc truyền.

Tóm lại, TKIP là một giao thức bảo mật bằng cách sử dụng khóa tạm thời, thay đổi khóa định kì, mã hóa RC4 và kiểm tra tính tổng thể của gói dữ liệu.

III. Toàn vẹn thông điệp trong TKIP

Trong TKIP, tính chất toàn vẹn Message Integrity là một phần quan trọng của quá trình bảo vệ dữ liệu. bằng cách xác thực và giám sát tính toàn vẹn của gói tin khi chúng được truyền qua mạng WiFi.

Để đảm bảo tính toàn vẹn của thông điệp, TKIP sử dụng một thuật toán băm hash mang tên *Michael*. Trong quá trình truyền dữ liệu, TKIP sẽ băm dữ liệu và gửi kèm theo mã băm trong gói tin. Máy nhận sẽ lấy lại mã băm từ gói tin, tính toán lại mã băm từ dữ liệu còn lại và so sánh hai mã băm này. Nếu hai giá trị băm khớp nhau, thông điệp được xác thực là có tính toàn vẹn và không bị thay đổi trong quá trình truyền tải.

TKIP sử dụng một kỹ thuật đã được gọi là Message Integrity Check (MIC) để đảm bảo tính toàn vẹn của các gói dữ liệu. MIC là một giá trị được tính toán từ dữ liệu gốc và được thêm vào gói tin dữ liệu đang truyền đi. Khi các thiết bị nhận được gói tin dữ liệu này, nó sẽ tính toán lại giá trị MIC và so sánh với giá trị ban đầu để kiểm tra tính toàn vẹn của gói dữ liệu.

MIC là viết tắt của "Message Integrity Code" - Mã kiểm tra tính toàn vẹn thông điệp, là một giá trị bảo mật được sử dụng để xác thực tính toàn vẹn của thông điệp. MIC sử dụng một thuật toán băm (hashing) đặc biệt để tạo ra một mã số ngắn (thường là 64 bit hoặc 128 bit) từ các phần của thông điệp gốc. Sau khi mã số này được tạo ra, nó được gửi cùng với thông điệp và sau đó được giải mã và xác thực khi đến đích.

Ta có thể nhận định TKIP bao gồm cả việc sinh khóa động (hay tạm thời) kèm theo thông số ngẫu nhiên và kiểm tra toàn vẹn thông điệp.

Thông thường, khi một người dùng muốn gửi một tin nhắn cho người nhận, họ sẽ sử dụng thuật toán băm để tạo ra một giá trị băm dựa trên nội dung của tin nhắn. Phía nhận sẽ thực hiện lại quá trình này và so sánh giá trị băm. Nếu giá trị băm khớp, điều đó có nghĩa là tin nhắn không bị thay đổi trong quá trình truyền. Nếu giá trị băm không khớp, thì tin nhắn có thể đã bị thay đổi hoặc bị tấn công.

IV. Phương pháp chọn Initial Vector (IV)

IV Selection là quá trình khởi tạo và chọn IV (Initialization Vector - vector khởi tạo) để sử dụng trong quá trình mã hóa dữ liệu của giao thức WEP và TKIP trong mạng Wifi.

Trong mạng Wifi, việc chọn số IV là rất quan trọng để đảm bảo tính an toàn và tránh các cuộc tấn công. Khi sử dụng *giao thức WEP*, số IV được chọn theo cách đơn giản là những số nguyên tăng dần từ 0 đến $2^{24} - 1$. Đây là một lỗ hổng mà kẻ tấn công có thể dễ dàng khai thác bằng cách dự đoán và thử tất cả các giá trị của IV.

Với TKIP, quá trình chọn số IV được thực hiện một cách phức tạp hơn. Các số IV được lựa chọn một cách ngẫu nhiên và "biến thiên", điều này góp phần ngăn chặn các cuộc tấn công giả mạo và giúp có thể phục hồi khóa tạm thời của TKIP. Trong quá trình chia sẻ và sử dụng khóa tạm thời, TKIP sử dụng một cơ chế tạo ra số IV mới mỗi khi dữ liệu được truyền đi, do đó làm cho việc tấn công dựa trên IV trở nên khó khăn hơn.

Các số IV được lựa chọn theo cách thức được mô tả trong chuẩn IEEE 802.11b và được gửi kèm với gói tin mã hóa. Điều này đảm bảo rằng mỗi lần gửi gói tin, một IV khác nhau sẽ được sử dụng, do đó làm tăng *"đề kháng"* với các cuộc tấn công.

TKIP sử dụng IV có 48-bit, gấp đôi con số 24 bit của WEP. Tuy nhiên, thay vì sử dụng IV giống nhau cho mỗi gói như WEP, TKIP sử dụng IV ngẫu nhiên sẽ được tạo mới sau mỗi gói dữ liệu. Điều này giúp TKIP tránh được nhiều cuộc tấn công nghiêm trọng mà WEP bị đối mặt.

IV size increase trong TKIP (tạm dịch là tăng kích thước của IV trong TKIP) được thực hiện để giảm thiểu khả năng xảy ra các cuộc tấn công phát hiện đồng bộ ngẫu nhiên trên các gói tin mã hóa TKIP. Trước đây, WEP sử dụng IV 24-bit và đã trở nên dễ dàng bị tấn công do chỉ cần chạy khoảng 5000 gói tin, thuộc tính đồng bộ hóa ngẫu nhiên lại lặp lại và giải mã WEP không an toàn. Vì vậy, hệ thống đã được nâng cấp lên TKIP với IV selection tự động, sau đó sử dụng một IV 48-bit cùng với PPKM (Per-packet Key Mixing) để kiểm soát khả năng tái sử dụng IV mã hóa và gia tăng tính bảo mật của mạng.

IV value rollover là một cơ chế được sử dụng trong TKIP để gia tăng kích thước của IV từ 24 bit lên 48 bit. Cơ chế này cho phép sử dụng IV ở một thời điểm trên nhiều gói tin chỉ bằng cách kiểm tra xem giá trị IV mới có khác với giá trị IV cũ hay không. Nếu có sự khác biệt, một giá trị offset được sử dụng để tính toán giá trị IV cho gói tin mới tiếp theo. Việc sử dụng cơ chế này giúp tăng độ an toàn cho hệ thống bảo mật Wi-Fi khi sử dụng giao thức TKIP.

Cơ chế 48-bit IV (Initial Value) được sử dụng trong TKIP như một biện pháp bảo mật thay thế cho việc sử dụng plaintext 24-bit IV của WEP, giúp tăng khả năng chống lại các cuộc tấn công thông qua việc tăng độ dài của IV và thêm tính ngẫu nhiên cho chuỗi khởi đầu. Với cơ chế 48-bit IV, ma trận IV được chia thành hai phần: một phần có độ dài 32 bit được gọi là Extended IV (EIV), và phần còn lại có độ dài 16 bit được gọi là Base IV. Khi một khung mới được mã hóa, giá trị EIV được tăng lên một, trong khi Base IV khác được tạo ra ngẫu nhiên từ các giá trị không trùng lặp. Việc liên kết EIV và Base IV với khóa phiên và địa chỉ MAC nguồn để tạo khóa trộn đã được giải thích trong PPKM, trong đó giá trị Base IV được sử dụng như là một tham số đầu vào cho hàm băm.

Tuy nhiên, việc sử dụng base IV tạo ra một lỗ hổng bảo mật trong TKIP, được gọi là "IV collision attacks". Nếu hai khung được truyền với Base IV giống nhau và cùng EIV, thì kẻ tấn công có thể quét nhanh tất cả các khóa tiềm năng để tìm ra Key Streaming để giải mã các khung được mã hóa đi đôi với EIV đó. Để tránh IV collision attacks, TKIP sử dụng giá trị Base IV như một bộ đếm duy nhất có độ dài 16 bit, như vậy mỗi IV sẽ được sử dụng một lần duy nhất trong một phiên. Tổng thể, cơ chế 48-bit IV của TKIP mang lại tính bảo mật cao hơn so với WEP, tuy vậy, nó vẫn tồn tại một số lỗ hổng bảo mật và sắp được thay thế bằng Wi-Fi Protected Access II (WPA2).

V. Kỹ thuật Per-Packet Key Mixing

Per-Packet Key Mixing (PPKM) là một kỹ thuật được sử dụng trong giao thức bảo mật khóa tạm thời TKIP để đảm bảo tính an toàn của các gói tin dữ liệu truyền qua mạng không dây. Trong PPKM, key-mixing key (KMK) và *một số thông tin khác* được kết hợp với IV và số thứ tự gói tin (Packet Number) để tạo ra một khóa duy nhất có thể sử dụng cho việc mã hóa và giải mã dữ liệu.

Các giai đoạn trong PPKM gồm hai giai đoạn như sau:

- Giai đoạn precomputation: Ở đây những giá trị cần thiết được tính toán trước với Session key như RC4key, hash(Key + extIV + MAC), MIC-key, và initial sequence counter (TSC). Việc tính toán này giúp tăng hiệu suất, tránh các xung đột về giá trị IV cũng như tạo khóa mới cho từng packet.

- Giai đoạn Per-packet: Khi có một packet cần được mã hóa, người ta sẽ sử dụng các giá trị đã được tính toán ở phase 1 cùng với IV để tạo ra khóa mã hóa mới cho từng packet riêng biệt. Sau đó, khóa được sử dụng để mã hóa packet và tính toán MIC. Việc sử dụng khóa mới cho từng packet giúp ngăn chặn kẻ tấn công khai thác lỗi từ khóa yếu như trong WEP.

Quá trình key-mixing (hay trộn khóa) được thực hiện trước khi mã hóa và sau khi giải mã mỗi gói tin riêng biệt, khác với WEP chỉ thực hiện quá trình key-mixing trước khi mã hóa. Điều này làm giảm nguy cơ bị tấn công và tăng tính an toàn cho hệ thống mạng không dây.

TKIP sequence counter: TKIP sequence counter là một giá trị đếm được sử dụng trong TKIP để đảm bảo tính toàn vẹn của gói tin. Khi một trạm truyền một gói tin, nó sẽ tăng giá trị của TKIP sequence counter lên một đơn vị và đưa giá trị này vào khối phụ bổ sung trong gói tin. Khi trạm nhận một gói tin, nó sẽ kiểm tra giá trị của TKIP sequence counter có đúng với giá trị mong đợi hay không. Nếu giá trị này không đúng, gói tin sẽ bị coi là không hợp lệ và bị xử lý theo cơ chế khôi phục lỗi. Việc sử dụng TKIP sequence counter giúp đảm bảo rằng các gói tin được truyền đi và nhận được trên mạng Wi-Fi là đầy đủ và không bị thay đổi hoặc bị thêm vào các gói tin giả mạo.

VI. Chống các cuộc tấn công vào khóa yếu

Có nhiều phương pháp để chống lại việc tấn công vào khóa yếu, bao gồm:

- Sử dụng các thuật toán mã hóa và giải mã được xem là bảo mật hơn, như AES (Advanced Encryption Standard).

- Sử dụng chữ ký số để đảm bảo tính toàn vẹn của dữ liệu truyền.
- Tăng độ dài khóa: việc sử dụng khóa dài hơn có thể làm cho việc tấn công khóa yếu trở nên khó khăn hơn.
- Sử dụng các cơ chế tự động tái sinh khóa như Perfect Forward Secrecy (PFS) trong các kết nối SSL/TLS để ngăn chặn một khóa đã bị tấn công được sử dụng cho các phiên tiếp theo.
- Cập nhật các hệ thống hỗ trợ mã hóa để đảm bảo rằng chúng luôn sử dụng các phiên bản mới nhất và an toàn nhất.
- Chỉ sử dụng các giao thức bảo mật được chứng nhận và phổ biến nhất.
- Tạo ra các khóa duy nhất và sử dụng ngẫu nhiên, không được lặp lại.
- Giám sát lưu lượng mạng để phát hiện các hoạt động độc hại và các nỗ lực tấn công được hướng đến khóa.
- Sử dụng mã hóa điểm đến (endpoint encryption) để bảo vệ dữ liệu khi di chuyển từ kho lưu trữ đến máy tính hoặc thiết bị di động.
- Thực hiện kiểm tra bảo mật thường xuyên và bảo vệ khóa bằng hình thức vật lý để đảm bảo rằng chỉ những người có quyền truy cập mới có thể truy cập vào khóa.

RC4 (Rivest Cipher 4) là một thuật toán mã hóa dữ liệu với khóa đối xứng, được phát triển bởi Ron Rivest của Viện Công nghệ Massachusetts (MIT) vào những năm 1987. RC4 có khả năng hoạt động nhanh và phù hợp cho các phương pháp mã hóa dữ liệu real-time, qua đó trở thành một trong những thuật toán mã hóa phổ biến nhất và được sử dụng rộng rãi trên Internet. Tuy nhiên, RC4 đã bị phát hiện có những lỗ hổng bảo mật quan trọng, do đó hiện tại không còn được xem là một thuật toán an toàn để sử dụng.

Điểm yếu của RC4 nằm ở khóa yếu (weak keys) như đã đề cập ở trên, điều này có thể dẫn đến việc tấn công tương tự như với mã hóa WEP. Ngoài ra, có nhiều tấn công khác cũng được phát triển để tấn công RC4, cho phép tin tặc khôi phục được khóa bí mật.

Để khắc phục điểm yếu này, một số giải pháp đã được đưa ra:

- Sử dụng thuật toán mã hóa đối xứng mạnh hơn như AES thay vì RC4.
- Tránh sử dụng khóa yếu: các khóa được tạo bằng một số thuật toán RNG (Random Number Generator) không an toàn có thể dẫn đến việc tạo ra khóa yếu. Vì vậy, sử dụng các khóa được tạo ra bằng cách sử dụng các thuật toán RNG mạnh và an toàn.
- Áp dụng phương pháp đổi chỗ khóa mới (key scheduling) để đảm bảo rằng khóa được tạo theo cách ngẫu nhiên, loại bỏ các khóa yếu và các chuỗi khóa liên quan.
- Thêm lớp bảo vệ bổ sung như đầu vào bổ sung (nonce) cho các hàm khóa.

Mặc dù một số cải tiến đã được thực hiện, nhưng RC4 vẫn được coi là một thuật toán mã hóa cũ và có độ bảo mật thấp hơn so với các thuật toán hiện đại.

E. Mã hoá trên WLAN và Mobile - AES và CCMP

I. Giới Thiệu

a. CCMP là gì?

CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) hay Counter Mode – CBC MAC Protocol là một giao thức bảo mật được sử dụng trong mạng không dây Wifi để bảo vệ dữ liệu truyền qua mạng.

CCMP là một phần của tiêu chuẩn bảo mật Wifi Protected Access II (WPA2) và được sử dụng để mã hóa dữ liệu truyền qua mạng không dây và xác thực tính hợp lệ của các thiết bị truy cập. CCMP sử dụng một thuật toán mã hóa mạnh là Advanced Encryption Standard (AES) với khóa 128-bit để đảm bảo tính bảo mật cao.

CCMP thường được coi là một trong những giao thức bảo mật mạng không dây an toàn nhất và hiện nay được sử dụng rộng rãi trong các mạng Wifi công cộng và doanh nghiệp.

Là chế độ mặc định của chuẩn an ninh 802.11i.

b. Cung cấp chế độ bảo mật tốt hơn so với TKIP

Một số lý do mà CCMP bảo mật hơn TKIP:

- Sử dụng thuật toán AES: CCMP sử dụng thuật toán mã hóa Advanced Encryption Standard (AES) để mã hóa dữ liệu. AES được coi là một trong những thuật toán mã hóa bảo mật nhất hiện nay. Trong khi đó, TKIP sử dụng thuật toán mã hóa RC4, một thuật toán đã bị phát hiện có lỗ hổng bảo mật.
- Tách khóa mã hóa và khóa xác thực: Trong CCMP, khóa mã hóa và khóa xác thực được tách ra thành hai khóa riêng biệt, giúp tăng tính bảo mật của hệ thống. Trong khi đó, TKIP sử dụng cùng một khóa để thực hiện cả hai chức năng này, làm giảm tính bảo mật.
- Tách khóa mã hóa và khóa xác thực: Trong CCMP, khóa mã hóa và khóa xác thực được tách ra thành hai khóa riêng biệt, giúp tăng tính bảo mật của hệ thống. Trong khi đó, TKIP sử dụng cùng một khóa để thực hiện cả hai chức năng này, làm giảm tính bảo mật.
- Tách khóa mã hóa và khóa xác thực: Trong CCMP, khóa mã hóa và khóa xác thực được tách ra thành hai khóa riêng biệt, giúp tăng tính bảo mật của hệ thống. Trong khi đó, TKIP sử dụng cùng một khóa để thực hiện cả hai chức năng này, làm giảm tính bảo mật.
- CCMP được thiết kế từ scratch, vì thế sẵn sàng thích ứng với các kĩ thuật phổ biến.

c. Tại sao lại sử dụng thuật toán AES

- Vì AES được xem là một trong những thuật toán mã hoá đối xứng bảo mật nhất hiện nay.
- AES được thiết kế mà khi khoá có độ dài càng lớn thì độ bảo mật càng cao. AES còn được xây dựng trên cơ sở nguyên lý thiết kế mã hoá đối xứng của Feistel Network, là kiểu thiết kế phổ biến và được sử dụng rộng rãi trong lĩnh vực bảo mật.
- AES đã được sử dụng trong nhiều ứng dụng bảo mật, bao gồm cả trong các chuẩn bảo mật Wifi, SSL (Secure Socket Layer), TLS (Transport Layer Security), và cả trong các chương trình mã hóa dữ liệu và đĩa cứng.
- Đối với CCMP, việc sử dụng AES giúp tăng tính bảo mật của hệ thống mã hóa, giảm khả năng bị tấn công và đảm bảo tính riêng tư và an toàn cho các thông tin được truyền qua

mạng Wifi. Ngoài ra, sử dụng AES cũng cho phép CCMP tương thích với các thiết bị và phần mềm hỗ trợ mã hóa AES, giúp đơn giản hóa quá trình triển khai và tăng tính linh hoạt của hệ thống mã hóa.

d. Lý do áp dụng AES trong 802.11i được thực hiện sớm hơn việc điểm yếu của WEP bị phát hiện

- Vì dự kiến sẽ không nâng cấp của WEP cho tiêu chuẩn mới do triển khai phần cứng của mật mã.
- TKIP được sử dụng nhằm lấp chỗ trống do lỗ hổng của WEP đã bị phát hiện và yêu cầu một giải pháp lập tức cho các hệ thống trong khi CCMP cần thời gian để để được phê chuẩn.

e. WEP, TKIP and CCMP

- WPA/TKIP và RSN/CCMP có nhiều điểm chung. VD: Quản lý khoá.
- CCMP sử dụng 1 khóa để mã hoá và bảo vệ
- Sự khác biệt rõ ràng nhất là về thuật toán mã hoá – cái cách mà dữ liệu được mã hoá và giải mã.

II. AES Pairwise Key Hierarchy trong CCMP

- AES Pairwise Key Hierarchy là một phần của giao thức CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) được sử dụng để bảo mật mạng Wifi. CCMP là một phần của tiêu chuẩn Wifi Protected Access II (WPA2) được sử dụng rộng rãi để bảo vệ mạng Wifi.
- Trong CCMP, mỗi thiết bị mạng Wifi có một bộ khóa định danh duy nhất được gọi là PMK (Pairwise Master Key). PMK này được tạo ra bằng cách sử dụng một phương thức chia sẻ khóa bảo mật như 802.1X hoặc Pre-Shared Key (PSK).
- Khi hai thiết bị mạng Wifi muốn trao đổi dữ liệu, chúng sử dụng PMK để tạo ra các khóa đối xứng tạm thời gọi là PTK (Pairwise Transient Key). PTK bao gồm ba khóa đối xứng tạm thời: khóa mã hóa (Encryption Key), khóa xác thực thông điệp (Message Integrity Code Key) và khóa vector khởi tạo (Initialization Vector Key).
- Sau khi PTK được tạo ra, khóa mã hóa được sử dụng để mã hóa dữ liệu trên mạng Wifi, khóa xác thực thông điệp được sử dụng để xác thực tính toàn vẹn của dữ liệu và khóa vector khởi tạo được sử dụng để tạo ra các vector khởi tạo duy nhất cho mỗi gói dữ liệu.
- Một cách để tăng cường bảo mật của CCMP là sử dụng AES Pairwise Key Hierarchy, trong đó mỗi PTK được tạo ra sẽ được sử dụng để tạo ra các khóa PTK mới cho các phiên trao đổi dữ liệu tiếp theo. Việc tạo ra các khóa PTK mới này được thực hiện bằng cách sử dụng một phép toán khóa và một chuỗi số ngẫu nhiên để tạo ra các khóa con (subkeys) mới.
- Trong thực tế, AES Pairwise Key Hierarchy sử dụng một cây khóa đối xứng, với mỗi node trung gian trên cây tạo ra các khóa con mới bằng cách sử dụng các khóa con ở các node cha. Mỗi node lá trên cây tương ứng với một PTK được sử dụng để bảo vệ các phiên trao đổi dữ liệu cụ thể.

- Các khóa tạm thời được tạo ra từ PTK trước đó và không được tái sử dụng trong các phiên trao đổi dữ liệu sau này. Điều này giúp ngăn chặn các cuộc tấn công giải mã bằng cách sử dụng các khóa tạm thời đã bị lộ ra từ các phiên trao đổi dữ liệu trước đó.
- Ngoài ra, AES Pairwise Key Hierarchy cũng giúp tăng tính linh hoạt và hiệu quả của CCMP bằng cách cho phép các khóa tạm thời được tạo ra một cách động, tránh việc sử dụng các khóa tĩnh và giảm thiểu khả năng bị tấn công.

=> AES Pairwise Key Hierarchy là một phương pháp tăng cường bảo mật của CCMP bằng cách sử dụng một cây khóa đối xứng để tạo ra các khóa tạm thời duy nhất và không tái sử dụng cho các phiên trao đổi dữ liệu trên mạng Wifi. Điều này giúp ngăn chặn các cuộc tấn công giải mã và tăng tính linh hoạt và hiệu quả của giao thức bảo mật.

III. AES Group Key Hierarchy trong CCMP

- AES Group Key Hierarchy (GKH) trong CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) là một quá trình tạo ra khóa mã hóa cho việc trao đổi dữ liệu nhóm (multicast/broadcast) trong mạng không dây.
- GKH bao gồm các bước sau:
    - Xác định khóa nhóm (Group Master Key, GMK): GMK là một khóa chung được sử dụng để tạo ra các khóa nhóm (Group Transient Key, GTK) cho việc trao đổi dữ liệu nhóm.
    - Tạo ra giá trị ngẫu nhiên (Group Key Nonce): Group Key Nonce là một giá trị ngẫu nhiên được tạo ra để đảm bảo tính ngẫu nhiên và duy nhất của khóa nhóm.
    - Tạo ra GTK: Dựa vào GMK và Group Key Nonce, một GTK mới sẽ được tạo ra.
    - Phân phối GTK: GTK sẽ được gửi đến các thành viên của nhóm cần trao đổi dữ liệu.
    - Sử dụng GTK: GTK sẽ được sử dụng để mã hóa và giải mã dữ liệu trao đổi giữa các thành viên của nhóm.
- Tổng kết, AES Group Key Hierarchy là một quá trình tạo ra khóa mã hóa cho việc trao đổi dữ liệu nhóm trong mạng không dây bằng cách sử dụng:
    - Sử dụng khóa nhóm (Group Master Key, GMK) và giá trị ngẫu nhiên (Group Key Nonce) để tạo ra khóa nhóm (Group Transient Key, GTK).
    - Phân phối GTK cho các thành viên của nhóm cần trao đổi dữ liệu.
    - Sử dụng GTK để mã hóa và giải mã dữ liệu trao đổi giữa các thành viên của nhóm.
- Với cách sử dụng này, AES Group Key Hierarchy giúp tạo ra khóa mã hóa an toàn và hiệu quả cho việc trao đổi dữ liệu nhóm (multicast/broadcast) trong mạng không dây sử dụng CCMP.

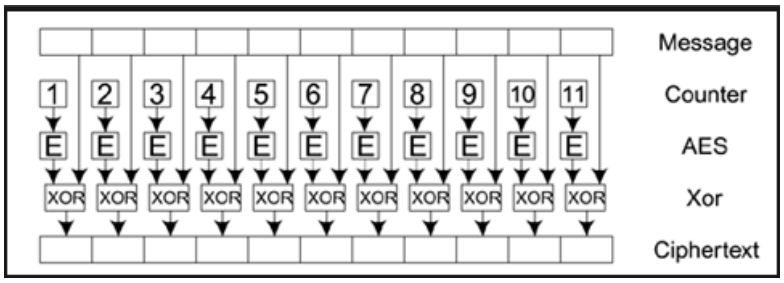
IV. Tổng quan về AES

- AES (Advanced Encryption Standard, hay Tiêu chuẩn mã hoá nâng cao) là một thuật toán mã hoá khối được chính phủ Hoa Kỳ áp dụng làm tiêu chuẩn mã hoá.
- Thuật toán được xây dựng dựa trên Rijndael Cipher phát triển bởi 2 nhà mật mã học người Bỉ: Joan Daemen và Vincent Rijmen.
- AES làm việc với các khối dữ liệu 128bit, 192bit hoặc 256bit. Các khoá mở rộng sử dụng trong chu trình tạo ra bởi thủ tục sinh khóa Rijndael.
- Hầu hết các phép toán trong AES đều thực hiện trong trường hữu hạn các byte. Mỗi khối dữ liệu đầu vào 128bit được chia thành 16 byte, có thể xếp thành 4 cột, mỗi cột 4 phần tử hay một ma trận 4x4 của các byte, nó gọi là ma trận trạng thái.
- Tùy thuộc vào độ dài khóa khi sử dụng 128 bit, 192 bit hay 256 bit mà thuật toán được thực hiện lặp lại với số lần khác nhau.
- Khá khó trong khả năng có bất kỳ điểm yếu cơ bản nào sẽ bị phát hiện trong thời gian gần.
- CCMP hạn chế kích thước khóa và kích thước khối của khi sử dụng AES là 128bit.

V. Modes of Operator

- AES có tới 16 cơ chế hoạt động khác nhau (được công khai trên website của NIST), và vẫn đang tìm kiếm những cơ chế hoạt động mới.
- **ECB Mode:**
    a. Mã hóa từng block một cách độc lập; Cần sử dụng Padding; Có thể hoàn thành song hoá từng block.
    b. Cùng một block sẽ tạo ra cùng một mật mã.
- **Counter mode**
    a. Mã hoá counter, cái sẽ được tăng 1 với mỗi block, và thực hiện XOR kết quả với data để tạo ra được ciphertext.
    b. Giải mã thì thực hiện tương tự theo cách mã hoá, padding là không cần thiết
    c. Có thể thực hiện song hoá
    d. Không có message authentication, chỉ có thực hiện mã hoá.
    e. Giá trị ban đầu (a nonce) của counter và step size cần được gửi đến cho bên nhận thông tin.
    f. Là khả dĩ cho 2 block giống hệt nhau nhưng khác plaintext có thể tạo ra cùng một ciphertext nếu như counter được thực hiện từ 1.

- **Counter mode + CBC MAC: CCM**



i. Được tạo ra dành riêng cho IEEE 802.11i RSN

ii. Được tạo bởi D.Whiting, R. Houseley, và N. Ferguson trong nhóm 802.11i tiêu chuẩn.

iii. Được xây dựng dựa trên Counter mode; sử dụng counter mode kết hợp với phương pháp message authentication được gọi là Cipher Block Chaining (CBC).

- CBC được sử dụng để tạo ra Message Integrity Code (MIC).

iv. Quá trình thực hiện: Mã hoá AES cho block đầu, sau đó XOR với block thứ hai và lấy kết quả đi mã hoá AES. Cứ tiếp tục như thế cho tới khi nào không còn block nào còn lại. Kết quả chính là block đơn ở MIC.

v. Cần sử dụng padding

vi.Liên kết xác thực và mã hoá

vii.CCM mode cho phép mã hoá được thực hiện trên một phần con của message được xác thực bởi CBC-MAC.

1. Header CCM nên được truyền dưới dạng plaintext nhưng không được sửa đổi

viii. IVs (nonce) cho counter mode và cho các phần CBC – MAC là khác nhau, dẫn tới sẽ có những key khác nhau.

ix.Quá trình đơn giản nhưng không thể song hoá .

- **Offset Codebook Mode (OCB):**
  a. Đạt được cả việc encryption và authentication.
  b. OCB có thể song hoá nên có thể thực hiện một cách nhanh chóng hơn bằng cách sử dụng đa hardware blocks.
  c. OCB rất là hiệu quả, chỉ mất hơn một chút so với hoạt động mã hoá tối hiểu lý thuyết có thể.
  d. OCB khá là bảo mật, có thể xem là bảo mật như AES.
  e. OCB không được áp dụng vào 802.11i vì là độc quyền.

VI. CCMP được sử dụng trong RSN như thế nào?

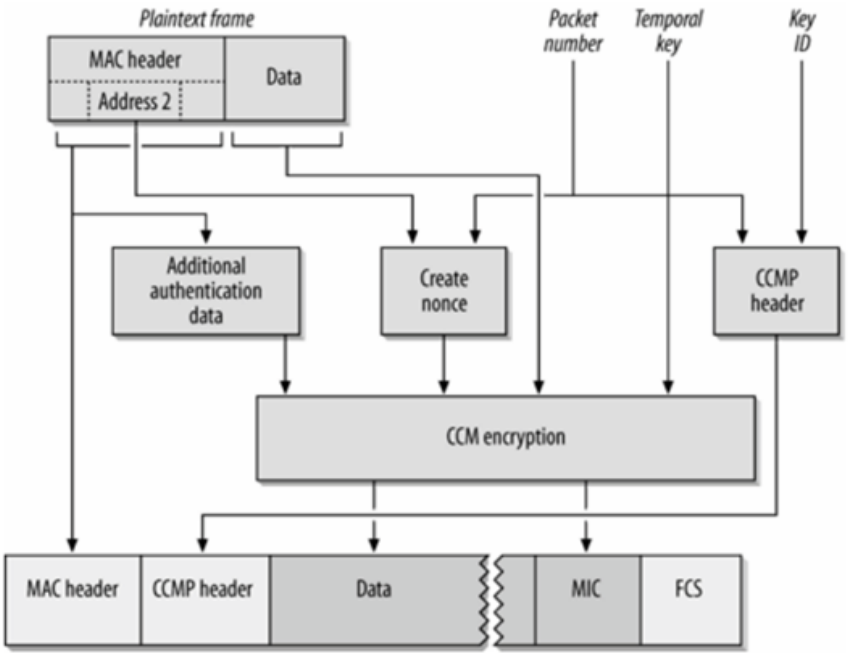
- CCMP sử dụng AES để mã hóa dữ liệu và CBC-MAC để xác thực tính toàn vẹn dữ liệu.
- Khi một khối dữ liệu được truyền đi, nó được mã hóa bằng AES và mã xác thực CBC-MAC được tạo ra từ khối dữ liệu này.

- Mã xác thực CBC-MAC được gắn vào cuối khối dữ liệu đã được mã hóa và truyền đi cùng với dữ liệu đã được mã hóa.
- Khi điểm truy cập nhận được dữ liệu đã được mã hóa và mã xác thực CBC-MAC, nó sẽ sử dụng khóa kết nối để giải mã dữ liệu và kiểm tra tính toàn vẹn của mã xác thực.
- Nếu mã xác thực không hợp lệ, điểm truy cập sẽ từ chối dữ liệu đã được truyền đi và gửi lại yêu cầu để truyền lại dữ liệu mới.

VII. CCMP Processing

Tại phía gửi, khi thông điệp cần gửi đi được chuyển xuống CCMP, quá trình diễn ra như sau:

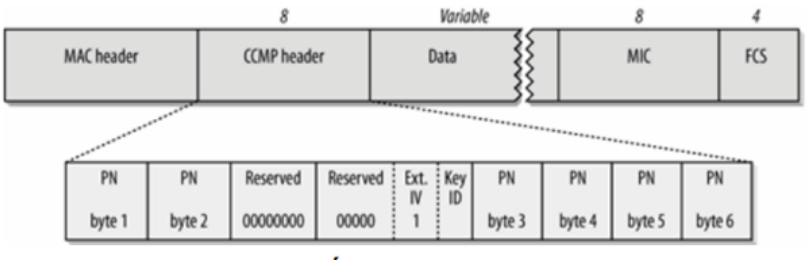
- Mỗi thông điệp được gán một số thứ tự gói (PN) có độ lớn 48bit. Số thứ tự gói cũng giống như TKIP IV, là duy nhất và không được sử dụng lại cho từng khóa phiên.
- Trường Dữ liệu xác thực bổ sung được tạo ra chứa giá trị những thông tin trong khung tin 802.11 cần được kiểm tra tính toàn vẹn nhưng không được mã hóa (AAD) bao gồm phiên bản giao thức, loại khung tin, các bit hệ thống, số hiệu mảnh, các bit thứ tự, địa chỉ MAC …
- Tiếp đó, giá trị CCMP nonce được tạo ra. Giá trị này được hình thành từ số thứ tự gói cùng với địa chỉ nguồn để đảm bảo việc mã hóa chỉ thực hiện trên dữ liệu duy nhất. Đây chính là số đếm sử dụng trong chế độ đếm để mã hóa dữ liệu
- Các giá trị này cùng với phần dữ liệu của thông điệp được chuyển vào bộ CCM, trong đó phần thân thông điệp được mã hóa AES sử dụng khóa phiên và CCMP nonce, còn trường AAD và dữ liệu được tạo mã kiểm tra toàn vẹn 8 byte MIC nhờ CBC-MAC sử dụng khóa phiên.



Tại phía nhận, khi nhận được khung tin, quá trình giải mã và kiểm tra diễn ra như sau:

- Khung tin nhận được bởi tầng MAC sẽ được kiểm tra giá trị FCS trước khi chuyển xuống cho CCMP xử lý.
- Trường AAD được tạo ra từ khung tin nhận được.
- Giá trị CCMP nonce được tính toán.
- Phía nhận giải mã dữ liệu sử dụng khóa phiên và CCMP nonce.
- Giá trị MIC được tính toán trên trường AAD và dữ liệu đã giải mã rồi so sánh với giá trị MIC trong khung tin nhận được. Nếu 2 giá trị này khác nhau, quá trình xử lý dừng.
- Giá trị số thứ tự gói được kiểm tra để chống lại hình thức tấn công replay.
- Khung tin nguyên thuỷ được hình thành.

VIII. CCMP Header

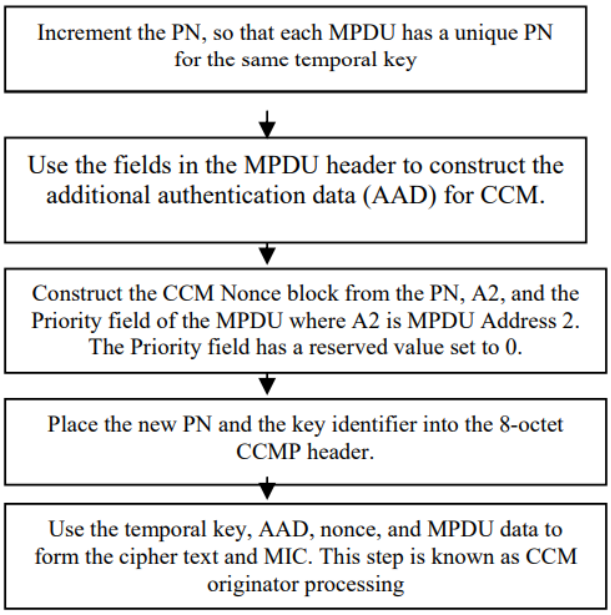


- Cấu trúc của CCMP header bao gồm các trường sau:

1. Quản lý truy cập (PN): Đây là trường dùng để quản lý số thứ tự gói tin truyền đi trong quá trình mã hóa và giải mã. PN được mã hóa để bảo mật thông tin truyền trên mạng.
2. Địa chỉ MAC (DA, SA): Đây là trường chứa địa chỉ MAC của trạm nhận (DA) và trạm gửi (SA).
3. Control: Trường này chứa các thông tin điều khiển cho quá trình mã hóa và giải mã, bao gồm các thông tin về kích thước khối mã hóa, số thứ tự gói tin, và cờ bảo mật.
4. Điều khiển bảo mật (MIC): Đây là trường chứa mã xác thực tin cậy (MIC), được sử dụng để đảm bảo tính toàn vẹn của thông tin truyền trên mạng.

- CCMP header cần được phải thêm trước data được mã hoá và truyền dưới dạng plaintext.
- CCMP header chứa 48bit packet number (PN) mà cung cấp replay protection và cho phép người nhận lấy được the nonce cho mã hoá.
- CCMP header cũng chứa trường KeyID để chỉ định group key nào đã được sử dụng.

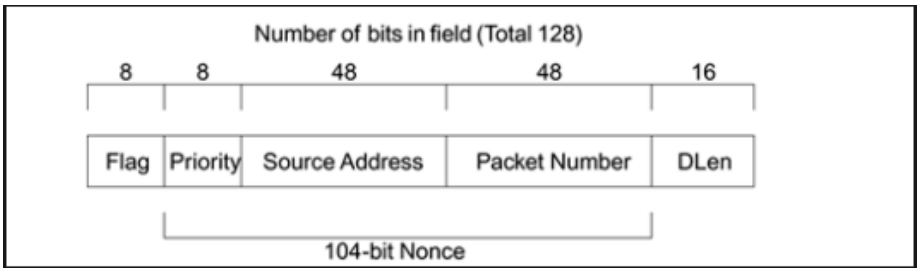
IX. CCMP Encryption



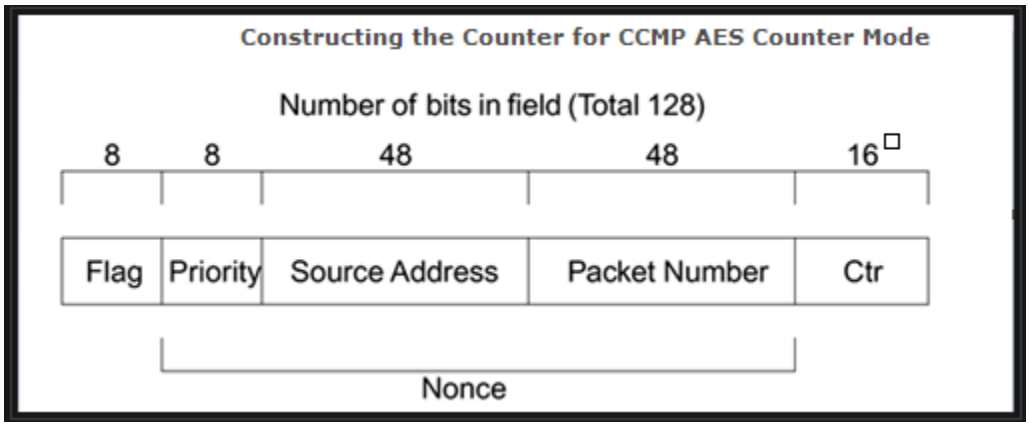
- Các bước thực hiện mã hóa theo CCMP bao gồm:
  - Tạo Vector khởi động (IV): Đây là giá trị bắt đầu của chuỗi số ngẫu nhiên được sử dụng trong quá trình mã hóa. IV được tạo ra bằng cách kết hợp địa chỉ MAC của trạm gửi và số thứ tự gói tin.
  - Tạo khối mã hóa (block): Dữ liệu cần được mã hóa sẽ được chia thành các khối có kích thước 128-bit, được mã hóa bằng AES.

- Tạo khối MIC: Sau khi dữ liệu được mã hóa, một khối MIC (Message Integrity Code) được tạo ra để đảm bảo tính toàn vẹn của dữ liệu truyền trên mạng.
- Tạo Vector đếm (CTR): Vector đếm là giá trị được sử dụng để tạo các khối mã hóa tiếp theo. Vector đếm được tạo ra bằng cách kết hợp IV, số thứ tự gói tin, và một giá trị đếm.
- Kết hợp các khối mã hóa và khối MIC: Các khối mã hóa và khối MIC được kết hợp để tạo thành gói tin mã hóa hoàn chỉnh.
- Gửi gói tin mã hóa: Gói tin được gửi qua kênh truyền không dây bằng cách sử dụng phương thức truyền dữ liệu Wifi.

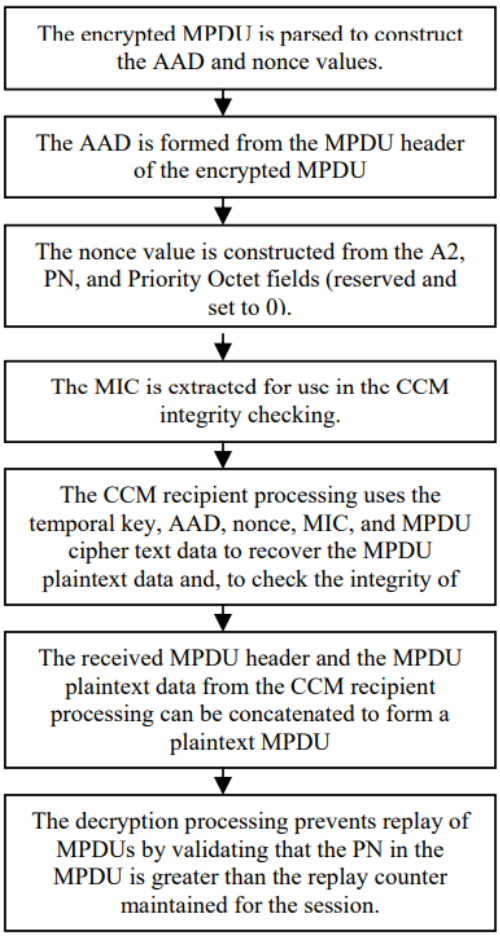
- Block đầu nhằm MIC computation
  a. Flag được để là 01011001, nhằm thể hiện rằng MIC field là độ dài 64bit
  b. Priority, SA và PN tạo thành nonce duy nhất.
  c. DLen chỉ độ dài của plaintext



- Padding cho 2 phần, counter mode mã hoá chỉ hoạt động trên plaintext và MIC.
- Cấu trúc counter cho AEC Counter Mode (128 bit)
  a. Counter chạy từ 1 cho 1 frame



X. CCMP Decryption



\

- Khi gói tin đến đích, gói tin được giải mã bằng cách thực hiện các bước trên ngược lại.
  - Kiểm tra PN
  - Description
  - Kiểm tra MIC
- Vì Counter Mode AES mã hoá counter thông qua AES và vì thế Encryption/Decryption là giống nhau.

III. Tham khảo

- CWSP – CCMP Encryption Method
- Dr.G.Padmavathi, Dr.P.Subashini, and Ms.D.Devi Aruna:"*CCMP-AES Model with DSR routing protocol to secure Link layer and Network layer in Mobile Adhoc Networks*"
- Xiuzhen Chen: "*Csci388 Wireless and Mobile Security Wireless and Mobile Security – AES-CCMP*"
- NGHIÊN CỨU MỘT SỐ GIẢI PHÁP AN_NINH TRONG MANG WLAN 802.11

- Wireless Security: WEP, WPA và WPA2
- Tổng quan và loại EAP 802.1x
- [Network Access Control] Hiểu thế nào về EAP?
- Muhamad Juwaini, Raed Al Saqour, Maha Abdelhaq, Ola Al Sukour: *"A REVIEW ON WEP WIRELESS SECURITY PROTOCOL"*, Journal of Theoretical and Applied Information Technology 2012.
- Shivaputrappa Vibhuti: *"IEEE 802.11 WEP (Wired Equivalent Privacy): Concepts and Vulnerability"*, San Jose State University, CA, USA at *CS265 Spring 2005*.