Mục lục

Contents

GIAO THỨC AN TOÀN MẠNG

CHƯƠNG 1: TỔNG QUAN VỀ AN TOÀN MẠNG

Các khái niệm chung:

- An toàn máy tính: khái niệm chung để chỉ những công cụ được thiết kế nhằm bảo vệ dữ liệu trên máy tính.
- An toàn mạng máy tính: Việc sử dụng rộng rãi các hệ thống phân tán, mạng máy tính và các thiết bị truyền thông để vận chuyển và bảo vệ dữ liệu giữa các máy tính.
- Hai trạng thái của dữ liệu:
    + Được lưu trữ
    + Đường truyền trên kênh
- Ba khía cạnh attt
    + Các tấn công
    + Các dịch vụ at
    + Các kỹ thuật at

1. Trình bày về tấn công bị động và tấn công chủ động, cho ví dụ.

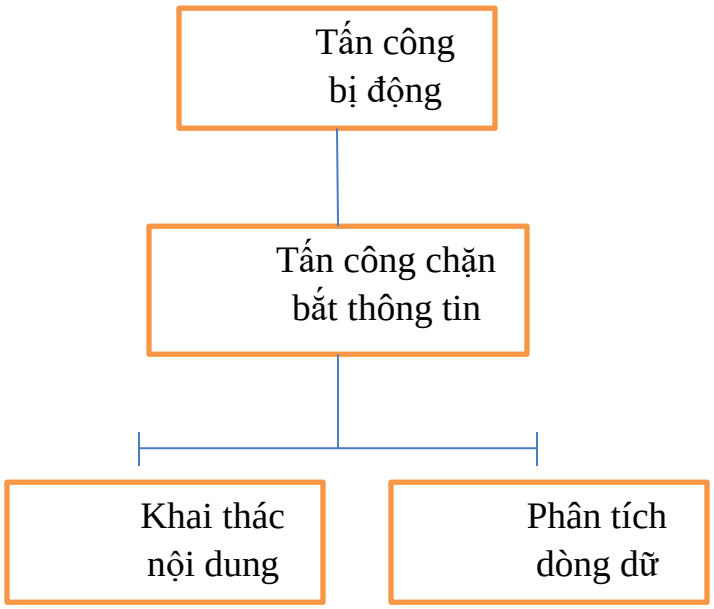
- Khái niệm các tấn công: là một hành động dẫn đến lộ thông tin của một tổ chức.
- Tấn công (attack) là hoạt động có chủ ý của kẻ phạm tội lợi dụng các thương tổn của hệ thống thông tin và tiến hành phá vỡ tính sẵn sàng, tính toàn vẹn và tính bí mật của hệ thống thông tin.

a) Tấn công bị động:

Là kiểu tấn công chặn bắt thông tin như nghe trộm và quan sát truyền tin.

- Mục đích của kẻ tấn công là biết được thông tin truyền trên mạng.

- Tấn công bị động rất khó bị phát hiện bởi vì chúng không thay đổi bất kỳ dữ liệu nào.

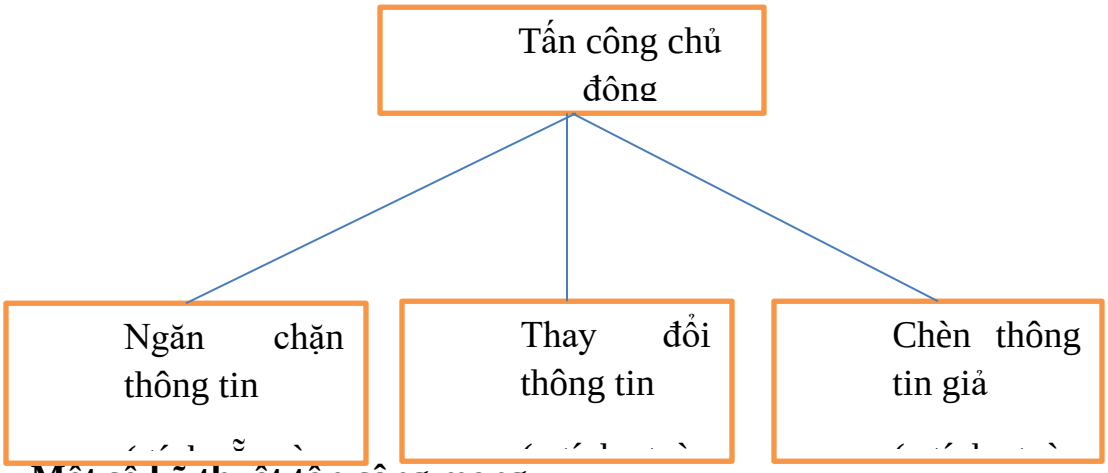


b) Tấn công chủ động:

Là các tấn công sửa đổi luồng dữ liệu hay tạo ra luồng dữ liệu giả, có thể được chia làm 4 loại nhỏ sau:

- Giả mạo (Masquerade): Một thực thể (người dùng, máy tính, chương trình, ...) giả mạo một thực thể khác.
- Phát lại (Replay): Thụ động bắt các thông báo và sau đó truyền lại nó nhằm đạt được mục đích bất hợp pháp.
- Sửa đổi thông báo (Modification of messages): Một bộ phận của thông báo hợp lệ được sửa đổi hoặc các thông báo bị làm trễ và thay đổi trật tự để đạt được mục đích bất hợp pháp.
- Từ chối dịch vụ: Ngăn hoặc cấm việc sử dụng bình thường hoặc quản lý các tiện ích truyền thông.

- Tấn công chủ động dễ phát hiện nhưng lại rất khó ngăn chặn tuyệt đối, đòi hỏi việc bảo vệ vật lý tất cả các phương tiện truyền thông ở mọi lúc, mọi nơi.



c) Một số kỹ thuật tấn công mạng

- Tấn công thăm dò
- Tấn công sử dụng mã độc
- Tấn công xâm nhập
- Tấn công từ chối dịch vụ
- Tấn công sử dụng kỹ nghệ xã hội.

2. Các dịch vụ an toàn và các kỹ thuật an toàn mạng, các khái niệm về giao thức an toàn.

a) Các dịch vụ an toàn mạng:

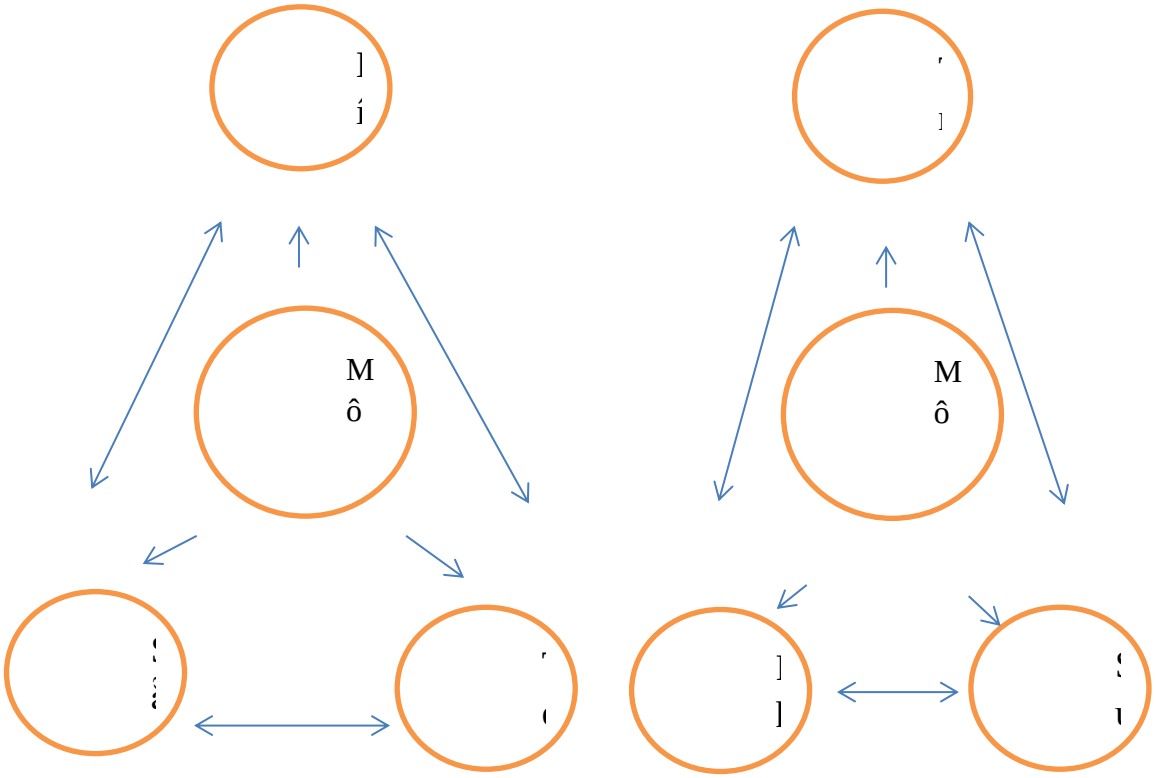
- **K/n:** Là dịch vụ nâng cao an toàn của các hệ thống xử lý dữ liệu và truyền tin của một tổ chức. Các dịch vụ này nhằm chống lại các tấn công của các tin tặc và sử dụng một hay nhiều cơ chế an toàn để cung cấp dịch vụ.

Có thể được phân loại như sau:

- **Dịch vụ bảo mật**: Nhằm chống lại các tấn công thụ động vào dữ liệu trên kênh truyền. Đối với loại đánh cắp nội dung thông tin, thì một vài mức bả vệ có thể được chỉ ra. Đây là loại dịch vụ nhằm bảo vệ dữ liệu trên kênh giữa hai người dùng trong một khoảng thời gian.
- **Dịch vụ xác thực:** Dịch vụ xác thực liên quan đến việc xác thực trong truyền thông. Trong trường hợp nhận một thông báo, dịch vụ xác thực đảm bảo người nhận xác thực được nguồn gốc thông báo. Trong trường hợp tương tác diễn ra trong một khoảng thời gian thì dịch vụ xác thực đảm bảo:
  - ✓ Tại thời điểm thiết lập kết nối, dịch vụ xác thực đảm bảo hai thực thể tham gia kết nối xác thực được lẫn nhau
  - ✓ Trong thời gian kết nối, dịch vụ đảm bảo không thể có một bên thứ ba đóng giả một trong hai thực thể truyền thông hợp pháp
- **Dịch vụ đảm bảo tính toàn vẹn:**
  - ✓ Đảm bảo tính toàn vẹn hướng kết nối đảm bảo dòng dữ liệu nhận được cũng như gửi không thể bị lặp lại, chèn thêm vào, thay đổi, thay đổi trật tự cũng như gửi lại. Dịch vụ này nhắm vào cả những thay đổi đối với dòng dữ liệu cũng như vấn đề từ chối dịch vu.

✓ Đảm bảo tính toàn vẹn không kết nối thì chỉ liên quan với từng thông báo riêng rẽ và nói chung chỉ nhằm chống lại việc thay đổi nội dung thông báo.

- **Dịch vụ chống chối bỏ:** nhằm ngăn chặn người gửi hoặc người nhận chối bỏ việc đã gửi thông báo hoặc đã nhận thông báo. Như vậy khi thông báo đã được gửi, người nhận có thể chúng minh được rằng ai là người đã gửi thông báo. Tương tự, khi thông báo đã được nhận, người gửi có thể chứng minh được ai là người đã nhận thông báo.
- **Dịch vụ kiểm soát truy cập:** nhằm hạn chế và kiểm soát truy cập tới các hệ thống máy chủ hoặc các ứng dụng qua các kênh truyền thông.
- **Dịch vụ đảm bảo tính sẵn sàng:** Đảm bảo ngăn ngừa hoặc phục hồi lại sự sẵn sang của tài nguyên trong hệ thống.



b) Các kỹ thuật an toàn mạng:

- **K/n:** là các kỹ thuật được thiết kế để phát hiện, ngăn ngừa hoặc loại bỏ tấn công.
- **Định danh:** là việc gắn định danh cho người dùng và kiểm tra sự tồn tại của định danh đó.

  Các kỹ thuật an toàn bao gồm:

- **Cấp quyền:** là việc xác định một chủ thể đã được xác thực được phép thực hiện những thao tác nào lên những đối tượng nào trong hệ thống
- **Xác thực:** là quá trình kiểm tra tính chân thực của danh tính được xác lập trong quá trình định danh
- **Mã hóa:** là phương pháp để biến thông tin từ định dạng bình thường sang dạng thông tin không thể hiểu được nếu không có phương tiện giải mã.
- **Ký:** Chữ ký điện tử là thông tin đi kèm theo dữ liệu nhằm mục đích xác định người chủ của dữ liệu đó
- **Công chứng:**

c) Các khái niệm về giao thức an toàn mạng:

- **Một giao thức an toàn** (giao thức mật mã) là một giao thức trừu tượng hay cụ thể mà thực hiện một chức năng liên quan đến an toàn và áp dụng các phương pháp mật mã. Nó thường được kết hợp với một trong các khía cạnh sau:
  - Trao đổi, thỏa thuận khóa
  - Xác thực thực thể
  - Mã hóa đối xứng và xác thực thông báo
  - An toàn truyền thông dữ liệu ở mức ứng dụng
  - Các phương pháp chống chối bỏ.

- Giao thức an toàn mạng là một kiểu của giao thức mật mã được sử dụng để bảo vệ dữ liệu trên máy tính và dữ liệu truyền thông.
- Một số tác vụ chính của các giao thức an toàn mạng thường là bảo mật việc truyền file, giao dịch Web và mạng riêng ảo:
    - Giao thức xác thực
    - Giao thức VPN
    - Giao thức an toàn email
    - Giao thức an toàn mạng không dây.

CHƯƠNG 2: CÁC GIAO THỨC XÁC THỰC

3. Khái niệm về xác thực, giao thức xác thực, các thuật ngữ được sử dụng trong giao thức xác thực.

- **Xác thực**: là hành vi xác nhận sự thật một thuộc tính của một dữ kiện hoặc tổ chức. Điều này có thể liên quan đến việc xác nhận danh tính của một người hoặc một chương trình phần mềm, dữ liệu máy tính, truy tìm nguồn gốc của một vật và đảm bảo các sản phẩm đã được công bố công khai là của mình.
- **Giao thức xác thực**: là một kiểu của giao thức mật mã với mục đích xác thực các thực thể có nhu cầu truyền thông an toàn, có nhiều kiểu giao thức xác thực(như AKA, CRAM-MD5, CAVE-based authentication….).
- **Một số thuật ngữ:**
    - Authenticator: là điểm cuối của liên kết yêu cầu xác thực. Authenticator cũng được coi như là Network Access Server (NAS) hoặc RADIUS client.

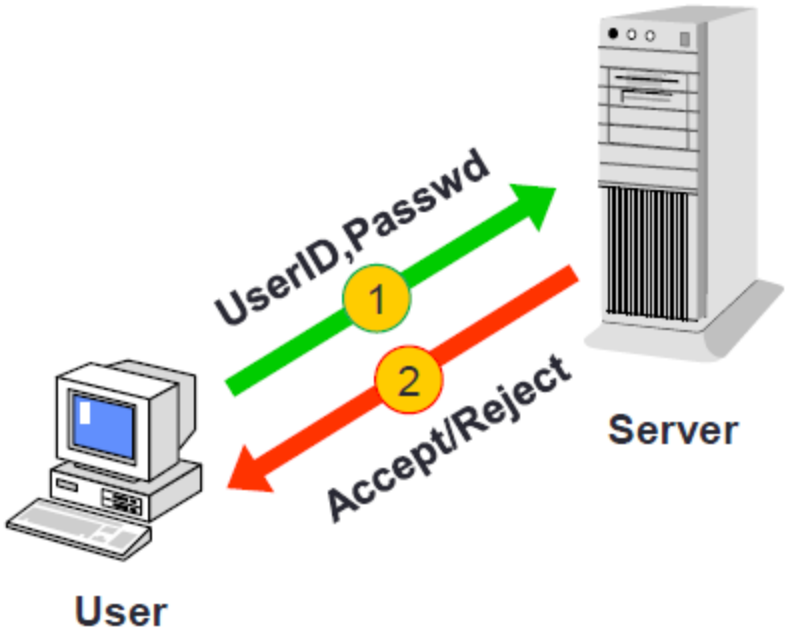
- Supplicant: là một thực thể sẽ được xác thực bởi Authenticator. Supplicant có thể được kết nối với Authenticator tại một điểm cuối của một phân đoạn LAN kiểu điểm- điểm hoặc của một liên kết không dây 802.11.
- Network Access Server (NAS): Server cung cấp dịch vụ truy cập vào mạng. NAS cũng được coi như là Authenticator hoặc RADIUS client.
- Authentication Server : một Server xác thực là một thực thể cung cấp dịch vụ xác thực tới Authenticator. Dịch vụ này kiểm tra yêu cầu định danh từ Supplicant.
- Peer: Điểm cuối khác của một két nối PPP, hoặc của một phân đoạn LAN kiểu điểm- điểm, hoặc của một liên kết không dây. Peer sẽ được xác thực bởi Authenticator.
- AAA (Authentication, Authorization, Accouting): cung cấp mô hình, hạ tầng cho cơ chế điều khiển truy nhập mạng. Các dịch vụ điều khiển truy nhập mạng được cung cấp bởi AAA là:
    - ✓ Authentication: dịch vụ kiểm tra định danh của người dùng hoặc thiết bị
    - ✓ Authorization: dịch vụ gán quyền cho một yêu cầu truy nhập mạng
    - ✓ Accouting: kiểm toán, phân tích hoặc tính cước,…

4. Các giao thức xác thực: PAP/CHAP, KERBEROS, EAP, RADIUS, Chuẩn 802.1x.

a) PAP (Password Authentication Protocol):

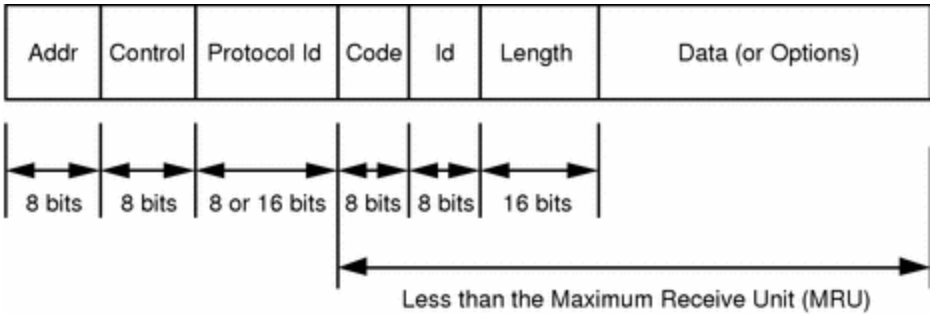
- Các đặc điểm cơ bản:
  - PAP (Password Authentication Protocol, RFC1334): là một giao thức bắt tay hai chiều có sử dụng mật khẩu.
  - Xác thực dựa trên mật khẩu là giao thức mà hai thực thể chia sẻ một mật khẩu trước và sử dụng mật khẩu như là cơ sở xác thực.
  - PAP được sử dụng bởi giao thức PPP để xác nhận người dùng trước khi cho phép họ truy cập vào tài nguyên hệ thống.
- Các thành phần
  - Client (Remote User)
  - Server (Authenticator)
- Cơ chế hoạt động

  PAP thực hiện hai bước xác thực cơ bản sau:



- **Client** (Remote User) gửi yêu cầu xác thực (Authentication-Request) cho Server (Authenticator): User_ID, Passwd
- **Server** gửi trả "Xác thực-OK" (Authentication-Ack) nếu thông tin về User_ID và Passwd là chính xác, còn không thì gửi trả "Không xác thực" (authentication-nak).

- Khuôn dạng gói tin:



- Addr: trường địa chỉ là 1 byte, và là phần của khung hình HDLC giống như đối với PPP. Nó luôn luôn được đặt thành 0xff

- Control: trường điều khiển là 1 byte, và là một phần của khung hình HDLC giống như đối với PPP. Nó luôn luôn được được đặt thành 0x03
- Protocol Id: xác định loại thông tin chứa trong trường thông tin của khung và luôn luôn là 0xc023 cho các khung PAP
- Code: trường code là 1 byte và xác định loại khung PAP. Các mã PAP được chỉ định như sau:

0x01 Authenticate- Request

0x02 Authenticate- Ack

0x03 Authenticate- Nak

- Identifier: trường identifier là 1 byte và trợ giúp cho việc kết hợp các yêu cầu và trả lời.
- Length: trường length là 2 byte, và cho biết độ dài của khung PAP bao gồm trường code, identifier, length và data. Chiều dài không được vượt quá đơn vị nhận được tối đa (MRU)
- Data: trường data là 0 hoặc nhiều byte. Nó chứa thông tin liên quan đến đàm phán xác thực, theo định đạng được xác định bởi trường mã.

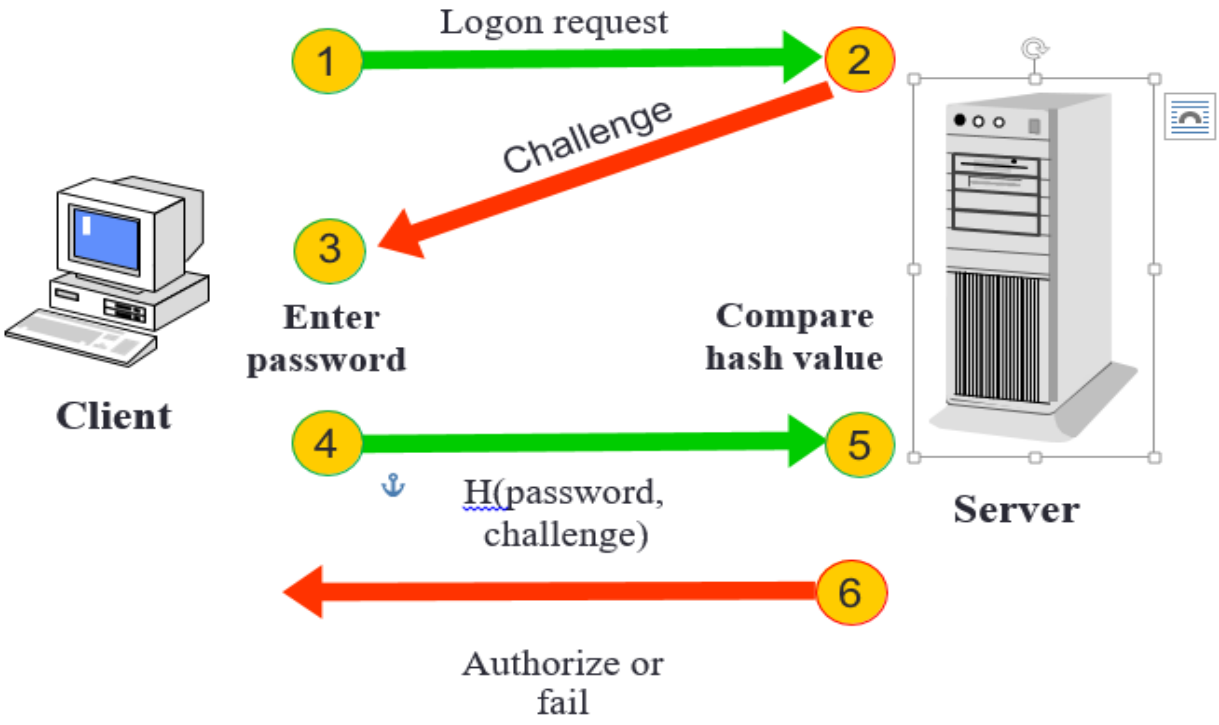
- Độ an toàn của giao thức xác thực :
  - Không đảm bảo độ an toàn do mật khẩu không được mã hóa trên đường truyền nên dễ bị đánh cắp mật khẩu.

b) CHAP

- Các đặc điểm cơ bản
  - CHAP (Challenge-Handshake Protocol, RFC 1994): Là mô hình xác thực dựa trên Username/Pasword.

- CHAP thực hiện xác thực dựa trên một bí mật được chia sẻ (vd mật khẩu người dùng).
- Thường được sử dụng khi Client logon vào các remote servers của công ty.

- Các thành phần
  - Client
  - Server
- Cơ chế hoạt động



Bước 1: client gửi yêu cầu kết nối tới Server

Bước 2: Server sẽ gửi lại Client một bản tin có các trường chính sau đây:

01 - Xác định loại bản tin là: challenge

ID - Xác định phiên đó - trường này có tác dụng chống hình thức tấn công gửi lại khi bên thứ 3 bắt được gói tin

random - số ngẫu nhiên sinh bởi Server

Server - Tên xác thực của nó - Tên của Server .tên này sẽ có trong cơ sở dữ liệu của Client và tương ứng sẽ là password kèm theo user này.

Bước 3: Client nhận được bản tin challenge (code=01) sẽ xử lý như sau:

Lấy ID, random ở bản tin challenge gửi sang, rồi căn cứ vào tên xác thực là Server để tìm ra password xác thực. Lúc này Client đã có các thông tin như : ID, số ngẫu nhiên và password tương ứng với username Server.3 thông số đó được lấy làm đầu vào hàm băm MD5 Hash. Đầu ra là một giá trị gọi là số hassh.

Sau khi xử lý xong, Client sẽ gửi lại Server một bản tin có code =02, gọi là bản tin response.

Trong bản tin này có 2 trường vẫn giữ nguyên giá trị như bản tin challenge là: ID và random. Ngoài ra còn có thêm kết quả của hàm hash, tên xác thực của Client cũng được gửi đi.

Bước 4: Server nhận được kết bản tin response từ Client.

Nó tìm kiếm password tương ứng với username mà nó nhận được.

Sau đó nó cũng tính toán giá trị MD5 Hash với 3 thông số đầu vào: ID, random và password vừa tim.

Cuối cùng nó so sánh giá trị 2 hàm Hash: giá trị nó tự tính toán và giá trị nó nhận được.

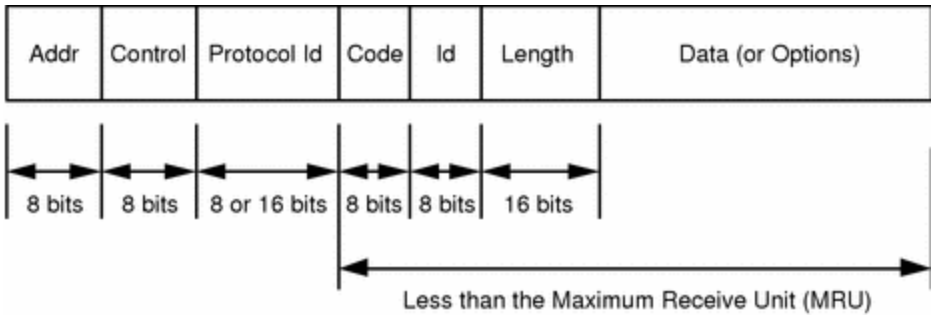
Bước 5:

Nếu giá trị nó tính và giá trị nó nhận được giống nhau thì gửi bản tin có code=03, success

Nếu không giống nhau thì gửi bản tin có code=04, faile.

Nếu Client nhận được bản tin code=03 thì quá trình xác thực kết thúc. Còn không thì xác thực ko thành công và kết nối bị Faile.

- Khuôn dạng gói tin:



  - Addr: trường địa chỉ là 1 byte, và là phần của khung hình HDLC giống như đối với PPP. Nó luôn luôn được đặt thành 0xff
  - Control: trường điều khiển là 1 byte, và là một phần của khung hình HDLC giống như đối với PPP. Nó luôn luôn được được đặt thành 0x03
  - Protocol Id: xác định loại thông tin chứa trong trường thông tin của khung và luôn luôn là 0xc223 cho các khung CHAP
  - Code: trường code là 1 byte và xác định loại gói CHAP. Các mã CHAP được chỉ định như sau:

    0x01 Challenge

    0x02 Respone

    0x03 Success

    0x04 Failure
  - Identifier: trường identifier là 1 byte và trợ giúp cho việc kết hợp các thách thức, phản hồi và trả lời.
  - Length: trường length là 2 byte, và cho biết độ dài cảu gói CHAP bao gồm trường code, identifier, length và data.

- Data: trường data là 0 hoặc nhiều byte. Nó chứa thông tin liên quan đến đàm phán xác thực, theo định dạng được xác định bởi trường mã.

- Độ an toàn của giao thức xác thực

An toàn hơn so với giao thức PAP vì mật khẩu đã được mã hóa trên đường truyền(sử dụng MD5 để băm mật khẩu, password được trao đổi qua chuỗi degit).

c) KERBEROS

- Các đặc điểm cơ bản
  - Là một giao thức mật mã dùng để xác thực trong các mạng máy tính hoạt động trên những đường truyền không an toàn.
  - Có khả năng chống lại việc nghe lén vào đảm bảo tính toàn vẹn của dữ liệu.
  - Mục tiêu khi thiết kế giao thức này là nhằm vào mô hình client – server và đảm bảo xác thực cho cả hai chiều.
  - Giao thức được xây dựng dựa trên mật mã khóa đối xứng và cần đến một bên thứ ba gọi là "Trung tâm phân phối khóa" (Key Distribution Center).
- Các thành phần
  - Client
  - Server
  - Máy chủ xác thực (*Authentication Server* – AS): sử dụng các thông tin có trong *database* để xác thực người dùng.

- Máy chủ cấp vé ((*Ticket Granting Server – TGS*): cung cấp vé dịch vụ cho phép người dùng truy nhập vào các máy chủ trên mạng.
- Cơ sở dữ liệu (*Database*): chứa dữ liệu của KDC và của người dùng (Client).
- Trung tâm phân phối khóa KDC (Key Distribution Center)

- Cơ chế hoạt động

- Sau đây là mô tả một phiên giao dịch (giản lược) của Kerberos. Trong đó: AS = Máy chủ chứng thực (authentication server), TGS = Máy chủ cấp vé (ticket granting server), SS = Máy chủ dịch vụ (service server).
- Một cách vắn tắt: người sử dụng chứng thực mình với máy chủ chứng thực AS, sau đó chứng minh với máy chủ cấp vé TGS rằng mình đã được chứng thực để nhận vé, cuối cùng chứng minh với máy chủ dịch vụ SS rằng mình đã được chấp thuận để sử dụng dịch vụ.

B1: Người sử dụng nhập tên và mật khẩu tại máy tính của mình (máy khách). Phần mềm máy khách thực hiện hàm băm một chiều trên mật khẩu nhận được. Kết quả sẽ được dùng làm khóa bí mật của người sử dụng.

B2: Phần mềm máy khách gửi một gói tin (không mật mã hóa) tới máy chủ dịch vụ AS để yêu cầu dịch vụ. Nội dung của gói tin đại ý: "người dùng XYZ muốn sử dụng dịch vụ". Cần chú ý là cả khóa bí mật lẫn mật khẩu đều không được gửi tới AS.

B3: AS kiểm tra nhân danh của người yêu cầu có nằm trong cơ sở dữ liệu của mình không. Nếu có thì AS gửi 2 gói tin sau tới người sử dụng:

- Gói tin A: "Khóa phiên TGS/máy khách" được mật mã hóa với khóa bí mật của người sử dụng.
- Gói tin B: "Vé chấp thuận" (bao gồm chỉ danh người sử dụng (ID), địa chỉ mạng của người sử dụng, thời hạn của vé và "Khóa phiên TGS/máy khách") được mật mã hóa với khóa bí mật của TGS.

B4: Khi nhận được 2 gói tin trên, phần mềm máy khách giải mã gói tin A để có khóa phiên với TGS. (Người sử dụng không thể giải mã được gói tin B vì nó được mã hóa với khóa bí mật của TGS). Tại thời điểm này, người dùng có thể nhận thực mình với TGS.

B5: Khi yêu cầu dịch vụ, người sử dụng gửi 2 gói tin sau tới TGS:

- Gói tin C: Bao gồm "Vé chấp thuận" từ gói tin B và chỉ danh (ID) của yêu cầu dịch vụ.
- Gói tin D: Phần nhận thực (bao gồm chỉ danh người sử dụng và thời điểm yêu cầu), mật mã hóa với "Khóa phiên TGS/máy khách".

B6: Khi nhận được 2 gói tin C và D, TGS giải mã D rồi gửi 2 gói tin sau tới người sử dụng:

- Gói tin E: "Vé" (bao gồm chỉ danh người sử dụng, địa chỉ mạng người sử dụng, thời hạn sử dụng và "Khóa phiên máy chủ/máy khách") mật mã hóa với khóa bí mật của máy chủ cung cấp dịch vụ.
- Gói tin F: "Khóa phiên máy chủ/máy khách" mật mã hóa với "Khóa phiên TGS/máy khách".
- Gói tin E thu được từ bước trước (trong đó có "Khóa phiên máy chủ/máy khách" mật mã hóa với khóa bí mật của SS).
- Gói tin G: phần nhận thực mới, bao gồm chỉ danh người sử dụng, thời điểm yêu cầu và được mật mã hóa với "Khóa phiên máy chủ/máy khách".

B7: Khi nhận được 2 gói tin E và F, người sử dụng đã có đủ thông tin để nhận thực với máy chủ cung cấp dịch vụ SS. Máy khách gửi tới SS 2 gói tin:

B8: SS giải mã "Vé" bằng khóa bí mật của mình và gửi gói tin sau tới người sử dụng để xác nhận định danh của mình và khẳng định sự đồng ý cung cấp dịch vụ:

- Gói tin H: Thời điểm trong gói tin yêu cầu dịch vụ cộng thêm 1, mật mã hóa với "Khóa phiên máy chủ/máy khách".

B9: Máy khách giải mã gói tin xác nhận và kiểm tra thời gian có được cập nhật chính xác. Nếu đúng thì người sử dụng có thể tin tưởng vào máy chủ SS và bắt đầu gửi yêu cầu sử dụng dịch vụ.

B10: Máy chủ cung cấp dịch vụ cho người sử dụng.

- Độ an toàn của giao thức xác thực : theo lý thuyết Kerberos là khá an toàn, tuy nhiên Kerberos chỉ cung cấp dịch vụ chứng thực, do đó nó không ngăn được dạng thỏa hiệp gây ra do lỗi phần mềm máy chỉ, quản trị viên cấp giấy phép cho người sử dụng trái phép, hoặc việc lựa chọn mật khẩu yếu.

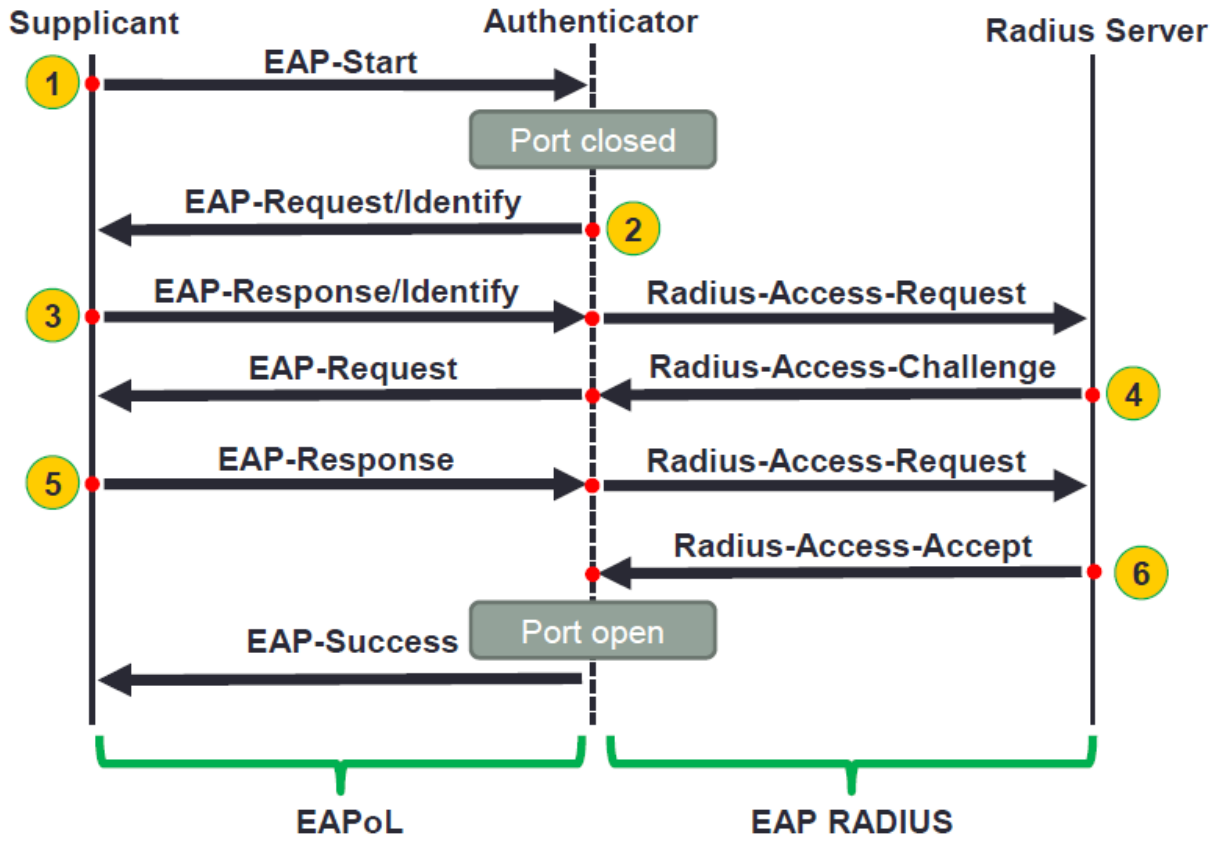
Nếu máy chủ trung tâm ngừng hoạt động thì mọi hoạt động sẽ ngừng lại. Điểm yếu này co thể được hạn chế bằng cách sử dụng nhiều máy chủ Kerberos.

d) EAP

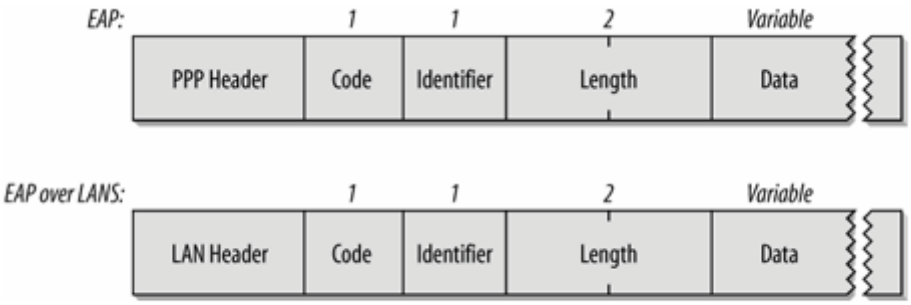
- Các đặc điểm cơ bản
  - EAP(Extensible Authentication Protocol, RFC 3748) hay còn gọi là giao thức xác thực mở rộng, là một framework xác thực thường được sử dụng trong các mạng không dây và trong các kết nối điểm-điểm (PPP).
  - Do hoạt động ở lớp 2 (Data link) nên EAP có thể truyền tin giữa các thiết bị mà không cần địa chỉ IP.
  - EAP là phương thức xác thực bao gồm yêu cầu định danh người dung (password,cetificate,…),giao thức được sử dụng (MD5,TLS_Transport Layer Security, OTP_ One Time Password,…) hỗ trợ tự động sinh khóa và xác thực lẫn nhau.
  - Bản thân EAP không phải là một phương thức xác thực. Khi sử dụng EAP ta cần chọn một phương thức xác thực cụ thể như CHAP, TLS, TTLS…
  - Ưu điểm của EAP là linh hoạt trong triển khai.
  - Có 4 loại EAP message:
    - EAP request
    - EAP response
    - EAP success
    - EAP failure
- Các thành phần của EAP
  - Peer (client): còn được gọi là supplicant (máy tính, điện thoại…).

- Authenticator: thường là các AP, NAS, đóng vai trò phân phối các thông báo EAP được gửi từ Client tới Server xác thực và ngược lại.
- Authentication Server: cung cấp các dịch vụ xác thực cho authenticator (Radius server…). AS tiếp nhận các thông báo EAP được chuyển từ authenticator đến và thực hiện xác thực client (peer).

- Cơ chế hoạt động: quá trình trao đổi EAP với Radius server



- Khuôn dạng gói tin:



- Code: trường code là 1 byte và xác định loại gói EAP. Các mã EAP được chỉ định như sau:
    1 Request
    2 Respone
    3 Success
    4 Failure
- Identifier: trường identifier là 1 byte và trợ giúp cho việc kết hợp các yêu cầu và phản hồi
- Length: trường length là 2 byte, và cho biết độ dài cảu gói EAP bao gồm trường code, identifier, length và data.
- Data: trường data là 0 hoặc nhiều byte. Định dạng của trường data được xác định bởi trường code.

EAP-TLS(TLS over EAP)

- Chỉ sử dụng giao thức bắt tay TLS
- Máy chủ xác thực và Client authentication, generation of master secret.
- Khóa chủ TLS(MK) trở thành khóa phiên
- Được dung trong giao thức WPA, là tùy chọn trong RSN

⇨ Kết quả sau khi thực hiện xong EAP-TLS:

- Suplicant và AS đã xác thực được với nhau
- Hai bên có thể thỏa thuận được một khóa bí mật chung.

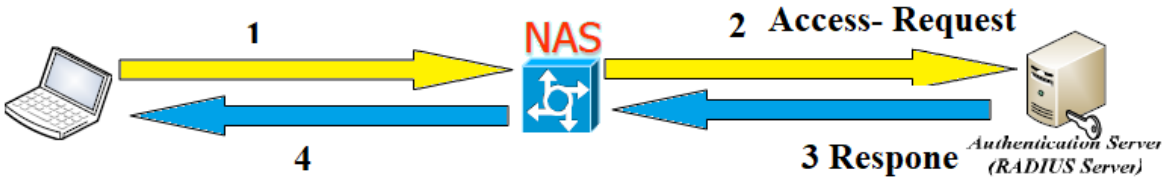
- **Độ an toàn:**

e) RADIUS

- Các đặc điểm cơ bản:

- RADIUS (Remote Authentication Dial-In User Service): giao thức hoạt động theo mô hình Client- Server, trong đó RADIUS client hay NAS (Network Access Server) tương tác với RADIUS server thông qua một hoặc nhiều RADIUS proxies.
- RADIUS được thiết kế dựa trên nền tảng kiến trúc AAA (Authentication-Authorization-Accouting) đó là Xác Thực - Ủy Quyền – Kế toán và hoạt động ở tầng 7 (Application Layer).
- RADIUS hỗ trợ nhiều phương thức xác thực khác nhau như PPP, PAP, CHAP…

- Các thành phần: Radius server, Radius client, Suplicant
- Cơ chế hoạt động



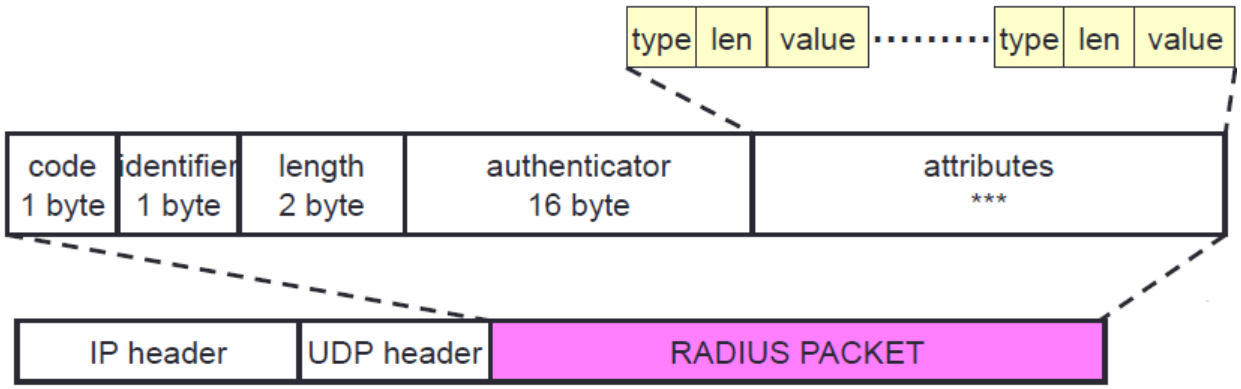
Hoạt động chung

1. User gửi thông tin dùng để xác thực tới NAS.
2. NAS sẽ đóng gói chúng vào AccesRequest và gửi tới RADIUS server.
3. 3. Server phản hồi: Yes/No/Challenge. 4
4. . NAS gửi phản hồi cho người dùng.

- Client sẽ tạo ra một “Access-Request” chứa các thuộc tính như trên: mật khẩu của user, ID của client và ID port mà user này sẽ truy cập vào. Mật khẩu khi nhập vào sẽ được ẩn (Mã hóa RSA hoặc MD5).

- “Access- Request” sẽ được gửi cho RADIUS server thông qua mạng. Nếu không trả lời trong một khoảng thời gian qui ước thì yêu cầu sẽ được gửi lại.
- RADIUS server xác nhận client gửi. Những yêu cầu từ các client nào không chia sẽ thông tin bảo mật với RADIUS sẽ không được xác nhận và trả lời. RADIUS server sẽ tìm kiếm trong cơ sở dữ liệu (CSDL) user có cùng tên trong yêu cầu. Chỉ mục của user trong CSDL sẽ chứa danh sách các đòi hỏi cần thiết cho phép user truy cập vào mạng.
- Nếu bất cứ điều kiện nào không thỏa mãn, RADIUS server sẽ gửi một trả lời “Access- Reject”
- Nếu tất cả các điều kiện đều thỏa mãn và RADIUS server muốn đưa ra một yêu cầu đòi hỏi user phải trả lời, thì RADIUS sẽ gửi một trả lời “Access-Challenge”
- Client sẽ gửi lại (re-submit) “Access-Request” với một số hiệu yêu cầu (request ID) mới, nhưng thuộc tính usename-password được lấy từ thông tin vừa mới nhập vào, và kèm luôn cả thuộc tính trạng thái từ Access-Challenge
- RADIUS server có thể trả lời một access-request bằng một Access-Accept, Access-Reject hoặc một Access-Challenge khác.
- Nếu tất cả các điều kiện đáp ứng, danh sách các giá trị cấu hình của user sẽ được RADIUS server đưa vào thông báo trả lời “Access- Accept”.

- Khuôn dạng gói tin”



- Code : Trường Code là một octet, và xác định kiểu gói của RADIUS. Khi một gói có mã không hợp lệ sẽ không được xác nhận.

  Các mã RADIUS (RADIUS Code) được gán như sau:

  1 Yêu cầu truy cập (Access-Request)

  2 Chấp nhận truy cập (Access- Accept)

  3 Từ chối truy cập (Access- Reject)

  4 Yêu cầu kiểm toán (Accouting- Request)

  5 Đáp ứng kiểm toán (Accouting- Response)

  11 Đòi hỏi truy cập (Access- Challenge)

  12 Trạng thái máy chủ (Status- Server)

  13 Trạng thái máy khách (Status- Client)

  255 Dự phòng (Reserved)

- Identifier: Trường Identifier là một octet, tương ứng giữa các Request-Respone.

- Length: Trường Length là hai octet, nó bao gồm chiều dài của các trường Code, Identifier, Length, Authenticator, Attribute. Những octet nằm ngoài khoảng quy định của trường Length bị xem như là octet dư thừa và sẽ bị bỏ qua khi nhận. Những gói ngắn hơn giá trị trường Length chỉ ra nó sẽ bị loại bỏ. Giá trị nhỏ nhất của trường Length là 20 và lớn nhất là 4096.
- Authenticator: Trường Authenticatior là 16 octet, chứa cá thông tin được dùng để xác thực giữa client và server, và được sử dụng trong thuật toán ẩn mật khẩu.
- Attributes: vùng chứa các thông tin xác thực, ủy quyền cũng như cấu hình chi tiết của gói tin RADIUS

- Độ an toàn của giao thức xác thực:

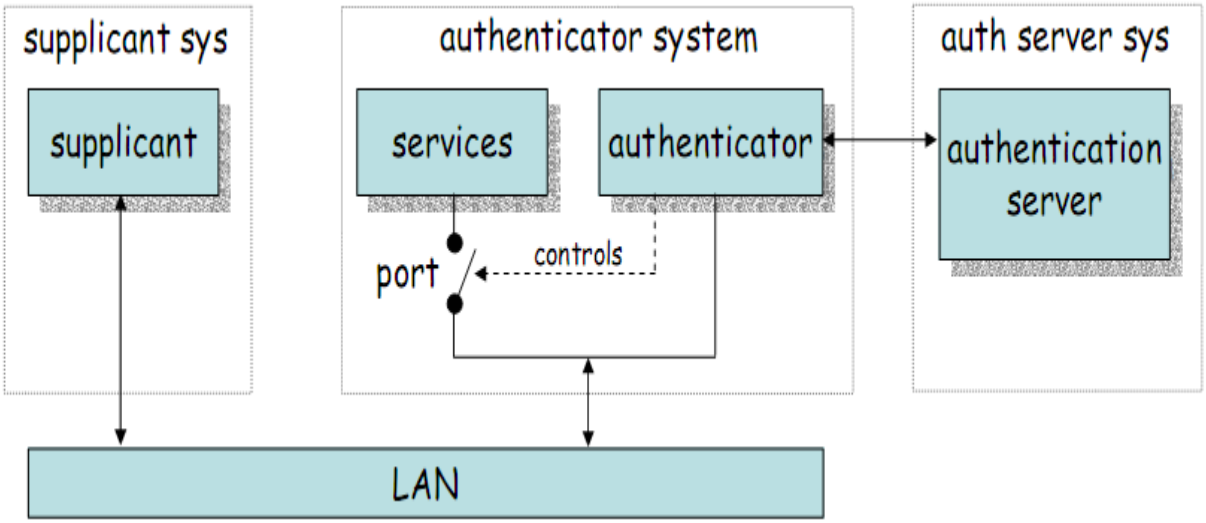
Authenticator giúp cho quá trình giao tiếp giữa NAS và máy chủ AAA được bảo mật nhưng nếu kẻ tấn công tóm được cả hai gói tin RADIUS Access-Request và Access-Response thì có thể thực hiện "tấn công từ điển" để phân tích việc đóng gói này. Trong điều kiện thực tế để việc giải mã khó khăn cần phải sử dụng những thông số dài hơn.

f) CHUẨN 802.1x

- Các đặc điểm cơ bản
    - Là chuẩn đặc tả cho việc truy cập dựa trên cổng (port-based) được định nghĩa bởi IEEE.
    - Hoạt động trên cả môi trường có dây truyền thống và không dây.
    - Khi một người dùng cố gắng kết nối vào hệ thống mạng, kết nối của người dùng sẽ được đặt ở trạng thái bị chặn (blocking) và chờ cho việc kiểm tra định danh người dùng hoàn tất.
- Các thành phần
    - Supplicant

- Authenticator
- Authenticator Server (AS)

- Cơ chế hoạt động



  - Supplicant yêu cầu truy nhập tới các dịch vụ (muốn kết nối vào mạng).
  - Authenticator kiểm soát truy cập vào các dịch vụ (kiểm soá của một cổng)
  - Authenticator Server (AS) cấp quyền truy cập tới các dịch vụ:
    - Supplicant xác thực nó với AS.
    - Nếu xác thực thành công, AS sẽ chỉ thị cho Authenticator mở công dịch vụ
    - AS thông báo cho Supplicant là truy cập được phép

- Các giao thức:
  - EAP (Extensible Authentication Protocol) [RFC 3748]
    - Là giao thức vận tải để mang các các thông điệp của các giao thức xác thực“thật sự” (VD: TLS)

- Rất đơn giản, gồm 4 thông điệp: EAP Request, EAP Response, EAP Success,EAP failure.
- Hoạt động ở tầng Datalink – OSI

- EAPOL (EAP over LAN) [802.1X]
  - Được dùng để đóng gói các thông điệp EAP vào trong các giao thức LAN(VD: Ethernet).
  - EAPOL được dùng để mang các thông điệp EAP giữa STA và AP
- RADIUS (Remote Access Dial-In User Service) [RFC 2865- 2869, RFC 2548]
  - Được dùng để mang các thông điệp EAP giữa AP và AS
  - Thuộc tính MS-MPPE-Recv-Key được dùng để truyền khóa phiên từ AS đến AP
  - RADIUS được dùng trong WPA và là tùy chọn cho RSN
  - Hoạt động ở tầng ứng dụng – OSI

5. So sánh các giao thức xác thực trên.

CHƯƠNG 3: CÁC GIAO THỨC AN TOÀN MẠNG RIÊNG ẢO

6. Định nghĩa về một mạng VPN, lợi ích của VPN, các mô hình VPN thông dụng.

❖ **Định nghĩa mạng riêng ảo** (Virtual Private Network - VPN): là mạng sử dụng mạng công cộng (như Internet, ATM/Frame Relay của các nhà cung cấp dịch vụ) làm cơ sở hạ tầng để truyền thông tin nhưng vẫn đảm bảo là một mạng riêng và kiểm soát được truy nhập.

VPN:

- Ảo (Virtual): Nghĩa là cơ sở hạ tầng vật lý của mạng hoàn toàn trong suốt với kết nối VPN.

- Riêng (Private):
  - Chỉ tính riêng biệt của lưu lượng dữ liệu khi qua VPN.
  - Dữ liệu truyền luôn luôn được giữ bí mật và chỉ có thể được truy cập bởi những người sử dụng được trao quyền.
- Mạng (Network):
  - Là thực thể hạ tầng mạng giữa những người sử dụng đầu cuối, những trạm hay những node để mang dữ liệu.
  - Dù không tồn tại vật lý, VPN vẫn được nhận biết và coi như một sự mở rộng hạ tầng mạng của một đơn vị/tổ chức.

Trong thực tế, người ta thường nói tới hai khái niệm VPN đó là: mạng riêng ảo kiểu tin cậy (Trusted VPN) và mạng riêng ảo an toàn (Secure VPN).

- Trusted VPN:
  - Được xem như một số mạch thuê của một ISP viễn thông.
  - Trusted VPN duy trì tính toàn vẹn và khả năng sử dụng tốt nhất cho mạng liên lạc của khách hàng.
  - Trusted VPN không đảm bảo an ninh an toàn và bảo mật cho khách hàng.
- Secure VPN :
  - Là các mạng riêng ảo có sử dụng mật mã để bảo mật (mã hóa và xác thực) dữ liệu.
  - Dữ liệu ở đầu ra của một mạng được mã hóa rồi chuyển vào mạng công cộng (ví dụ: mạng Internet) như các dữ liệu khác để truyền tới đích và sau đó được giải mã dữ liệu tại phía thu.

❖ **Lợi ích của việc sử dụng VPN bao gồm**:

- Tính bí mật
- Tính toàn vẹn
- Xác thực

- Chống tấn công phát lại

❖ **Các mô hình VPN thông dụng**:

- Mô hình VPN truy cập từ xa:
  - VPN truy cập từ xa cho phép người dùng từ xa của một Công ty có thể truy cập tới các tài nguyên mạng của đơn vị mình
  - Người dùng từ xa, người dùng đang di chuyển, người dùng làm việc tại nhà,…
  - Những người này không có kết nối cố định tới Intranet của công ty.
- Mô hình VPN nhánh mạng- tới- Nhánh mạng (site- to- site)
  - VPN cục bộ (Intranet VPN)
    - Mở rộng các dịch vụ của mạng nội bộ tới các trụ sở ở xa
    - Được dùng để kết nối các nhánh văn phòng ở xa của một Tổ chức với với Intranet tại văn phòng trung tâm của Tổ chức đó
    - Do đó, nó còn được gọi là Mạng riêng ảo chi nhánh
  - VPN mở rộng (Extranet VPN)
    - Mở rộng cho phép các khách hàng, nhà cung cấp, hay các đối tác thương mại có thể truy cập tới Intranet của Công ty

❖ Một số giao thức/ công nghệ VPN :

- Giao thức VPN tầng 2 : PPTP, L2TP, L2F, MPLS VPN tầng 2
- Giao thức VPN tầng 3 : IPsec, MPLS VPN tầng 3
- Giao thức VPN tầng 4 : SSL VPN

7. Lịch sử phát triển SSL, các đặc điểm cơ bản của giao thức SSL, những dịch vụ an toàn mà SSL cung cấp, các giao thức con của SSL. Quá trình bắt tay của client và server sử dụng SSL. So sánh SSL và TLS.

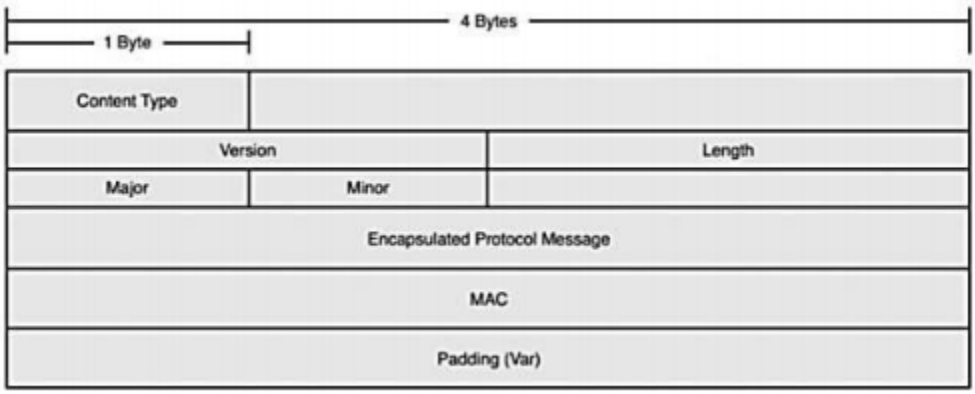
❖ **Lịch sử phát triển**

- SSL 1.0: Do Netscape thiết kế đầu năm 1994. Hiện không còn sử dụng
- SSL 2.0: Do Netscape công bố vào 11/1994. Không khuyên khích sử dụng trong môi trường thực tế
- SSL 3.0: Được thiết kế bởi Netscape và Paul Kocher vào 11/1996
- TLS 1.0(SSL 3.1): Transport Layer Security. Là chuẩn Internet dựa trên SSL 3.0, vào 1/1999, được quy định trong RFC 2246. Do IETF thiết kế. Không tương thích với SSL. Hiện nay đã có các phiên bản mới của TLS đó là TLS v1.1, TLS v1.3 và TLS v1.3(2016).
- SSL/TLS đem lai các yếu tố sau cho truyền thông trên internet: Bí mật(sử dụng mật mã). Toàn vẹn(sử dụng MAC). Xác thực(sử dụng chứng chỉ số X.509).
- SSL/TLS ngày nay được sử dụng ở các web server và các trình duyệt internet.

❖ **Đặc điểm cơ bản của giao thức SSL**

- SSL (Secure Sockets Layer) là một giao thức cung cấp dịch vụ truyền thông có bảo mật giữa client và server, cho phép client và server xác thực lẫn nhau sử dụng chữ ký số và bảo mật thông tin trao đổi qua lại bằng cách mã hóa các thông tin đó
- Được phát triển bởi hãng Netscape.
- SSL nằm giữa tầng application và tầng transport trong mô hình OSI, và sử dụng TCP làm giao thức vận chuyển nhằm truyền các gói tin một cách tin cậy.

- Bên trong mỗi gói tin SSL là phần Record header chịu trách nhiệm đóng gói các message sẽ truyền đi. Hình dưới đây là định dạng Record trong gói tin SSL



- Content type: 1byte, cho biết loại message được đóng gói bên trong record này. Có 4 loại message:
  - Handshake: 22
  - Change Cipher Spec:20
  - Application: 23
  - Alert: 21
- Length: 2 byte, chiều dài của recode này
- Encapsulated protocol message: Phần message hoặc application data được trao đổi giữa client và server trong phiên làm việc. Sau khi các tham số liên quan đến encryption và hash được thương lượng xong thì trường này sẽ được mã hóa
- MAC: giá trị MAC (message authentication code) được tính toán cho phần application data chứa trong encapsulated protocol message để đảm bảo tính toàn vẹn
- Padding: chèn thêm vào phàn encapsulated protocol message cho đủ kích thước của một block. Trường này không cần khi dùng kiểu mã hóa dòng (stream cipher)

❖ **Những dịch vụ an toàn mà SSL cung cấp**

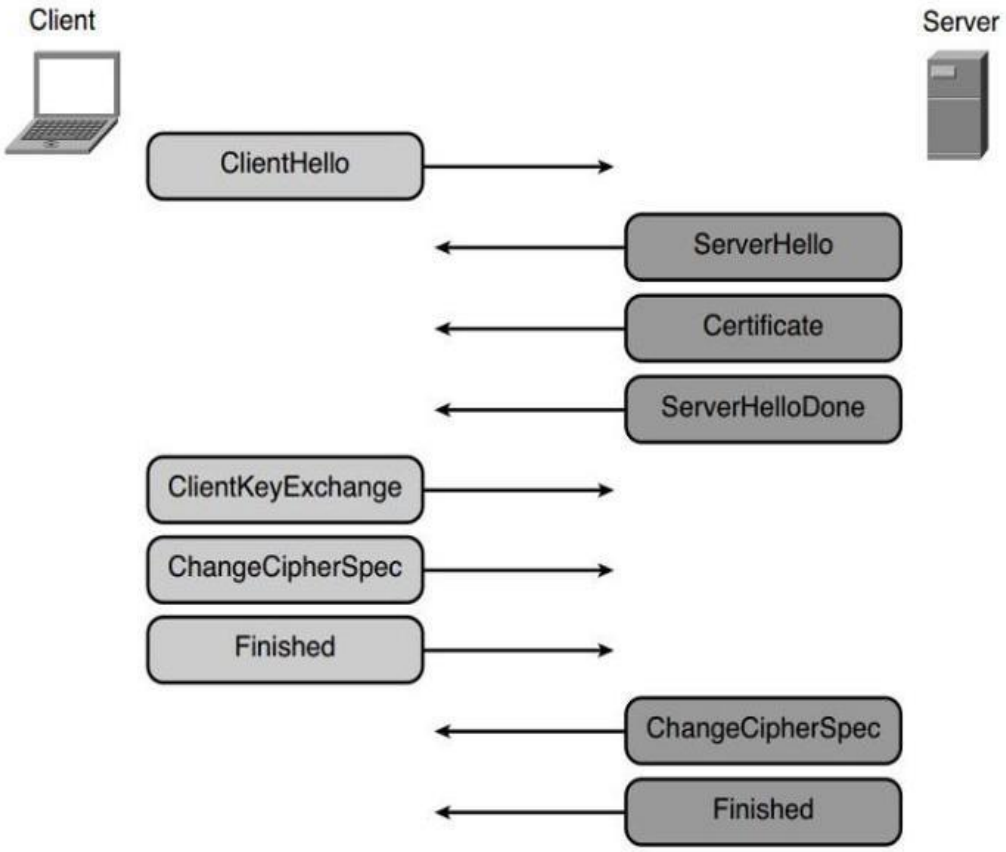
- Xác thực server: Cho phép người sử dụng xác thực được server muốn kết nối. Lúc này, phía browser sử dụng các kỹ thuật mã hoá công khai để chắc chắn rằng certificate và public ID của server là có giá trị và được cấp phát bởi một CA (certificate authority) trong danh sách các CA đáng tin cậy của client. Điều này rất quan trọng đối với người dùng. Ví dụ như khi gửi mã số credit card qua mạng thì người dùng thực sự muốn kiểm tra liệu server sẽ nhận thông tin này có đúng là server mà họ định gửi đến không.
- Xác thực Client: Cho phép phía server xác thực được người sử dụng muốn kết nối. Phía server cũng sử dụng các kỹ thuật mã hoá công khai để kiểm tra xem certificate và public ID của server có giá trị hay không và được cấp phát bởi một CA (certificate authority) trong danh sách các CA đáng tin cậy của server không. Điều này rất quan trọng đối với các nhà cung cấp. Ví dụ như khi một ngân hàng định gửi các thông tin tài chính mang tính bảo mật tới khách hàng thì họ rất muốn kiểm tra định danh của người nhận.
- Mã hoá kết nối: Tất cả các thông tin trao đổi giữa client và server được mã hoá trên đường truyền nhằm nâng cao khả năng bảo mật. Điều này rất quan trọng đối với cả hai bên khi có các giao dịch mang tính riêng tư. Ngoài ra, tất cả các dữ liệu được gửi đi trên một kết nối SSL đã được mã hoá còn được bảo vệ nhờ cơ chế tự động phát hiện các xáo trộn, thay đổi trong dữ liệu. (đó là các thuật toán băm – hash algorithm).

❖ **Các giao thức con của SSL**

- Giao thức SSL record: phân mảnh, nén, tính MAC, mã hóa dữ liệu

- Giao thức SSL handshake (gọi là giao thức bắt tay) : thực hiện chức năng thỏa thuận các thuật toán, tham số, trao đổi khóa, xác thực server và client (nếu có lựa chọn)
- Giao thức SSL Alert: thông báo lỗi
- Giao thức SSL Change cipher spec protocol: thông báo xác nhận kết thúc giai đoạn Hanshake protocol

❖ **Quá trình bắt tay của client và server sử dụng SSL**



- Giai đoạn 1: Thiết lập protocol version, ID phiên, thuật toán mã hóa, phương pháp nén, trao đổi giá trị random
  - B1: Client gửi một thông điệp ClientHello tới server. Các thành phần quan trọng của một thông điệp ClientHello:

- Version: phiên bản SSL cao nhất mà client hỗ trợ.
- Random: Một cấu trúc ngẫu nhiên được sinh ra, bao gồm một nhãn thời gian 32 bit và 28 byte được sinh bởi bộ sinh số ngẫu nhiên bảo mật.
- Session ID: định danh phiên
- CipherSuite: danh sách thuật toán mã hóa và băm mà client hỗ trợ (TLS_RSA_WITH_AES_128_CBC_SHA)
- Compression method: danh sách thuật toán nén dữ liệu mà client hỗ trợ.

- B2: Server gửi SeverHello tới client để trả lời cho gói ClientHello, nội dung tương tự như ClientHello, tuy nhiên có một số điểm khác biệt
  - Version : Server chọn ra phiên bản SSL cao nhất mà cả client và server cùng hỗ trợ.
  - Random : giá trị ngẫu nhiên được sinh ra bởi server, bốn byte đầu là nhãn thời gian (để tránh các giá trị ngẫu nhiên lặp lại), các byte còn lại sẽ được tạo bởi bộ sinh số ngẫu nhiên bảo mật lập mã.
  - CipherSuiter : lựa chọn ciphersuite tốt nhất trong danh sách các ciphersuite mà nó và client hỗ trợ.
  - CompressionMethod : lựa chọn một phương pháp nén trong các phương pháp nén mà nó nhận được từ client.

Sau hai bước này, client và server đã thương lượng xong các thuật toán mã, nén dữ liệu và thuật toán băm.

- Giai đoạn 2 : server gửi certificate, dữ liệu trao đổi khóa và ueeu cầu client gửi lại certificate nếu được thiết lập xác thực client.
  - Bước 3 : server gửi chứng thư (SSL certificate) của nó cho client, và trong certificate này có chứa public key của server.

Client nhận được certificate của server sẽ sử dụng public key cảu CA để kiểm tra chữ kỹ số đó. Nếu certificate của server hợp lệ thì client chấp nhận public key của server trong certificate đó.

- Bước 4 : server gửi ServerHelloDone tới client để cho biết server đã gửi hết tất cả các thông tin mà nó có cho client.

- Giai đoạn 3 : client gửi certificate nếu được yêu cầu, kết quả kiểm tra chứng chỉ server và dữ liệu trao đổi khóa)
  - Bước 5 : ClientKeyExchange do client gửi đến server và chứa thông tin để tạo ra masterkey
    - client sinh một Pre_master secret
    - mã hóa nó bằng public key lấy từ certificate của server
    - thuật toán mã hóa đã thương lượng (ví dụ RSA)

  Server :
    - giải mã private key của mình.
    - Bây giờ cả client và server sẽ sử dụng pre_master secret cùng với hai số ngẫu nhiên đã sinh trước đó để tạo ra master key
    - Từ master key sẽ tạo ra session key dùng để mã hóa dữ liệu
- Giai đoạn 4 : Change CipherSuit và kết thúc giai đoạn HandShake
  - Bước 6 : ChangCipherSpec : client gửi thông báo đến server để cho biết tất cả các gói tin trao đổi giữa client và server đều sẽ được mã hóa bằng các thuật toán và session key đã thương lượng trước đó.
  - Bước 7 : Finished : do client gửi đến server để cho biết client đã hoàn tất việc thiết lập tunnel
  - Bước 8 : ChangeCipheSpec : server gửi thông báo này đến client để cho biết tất cả các gói tin trao đổi giữa server và client đều sẽ được mã hóa bằng các thuật toán và sessio key đã thương lượng trước đó

- Bước 9 : Finished : do server gửi đến client để cho biết server đã hoàn tất việc thiết lập tunnel

❖ **So sánh SSL và TLS**

	SSL	**TLS**
Version	1.2, 2.0, 3.0	1.0 (SSL 3.1), 1.1, 1.2, 1.3
Nhà sản xuất	Netscape	IETF
Chuẩn	Chưa chuẩn hóa	được chuẩn hóa
Xác thực	MAC	HMAC (hàm băm+khóa)
Thông điệp cảnh báo	It thông điệp cảnh báo	Nhiều thông điệp cảnh báo và thêm nhiều giải thuật

8. Các tính năng cơ bản của SSL VPN, sự khác nhau giữa SSL VPN với IPSec.

Mục đích chính của SSL VPN là cung cấp truy cập từ xa an toàn tới các tài nguyên của tổ chức.

- **Tính năng cơ bản của SSL VPN**
  - Tính năng quản lý như báo cáo trạng thái, logging, và kiểm toán.
  - Tính sẵn sàng cao, trong suốt và khả năng mở rộng
  - Hỗ trợ đa dạng các loại thiết bị như các thiết bị mạng thông thường, các thiết bị cá nhân như PDA và điện thoại thông minh. SSL VPN không phụ thuộc vào loại đường truyền cũng như thiết bị mạng (chỉ với giao thức IP)
  - Khả năng vượt NAT

- SSL VPN cung cấp các thuật toán mật mã mạnh và độ dài khóa được coi là an toàn đối với thực tế hiện nay nên được sử dụng để mã hóa, đảm bảo tính xác thực và toàn vẹn dữ liệu.
- SSL VPN cung cấp khả năng kiểm soát truy cập cùng với tích hợp các thiết bị nghiệp vụ như USBToken thông qua hệ thống CA/Chứng thư số;

- **So sánh SSL VPN và IPSEC**
  - Giống nhau:
    - IPSec(qua IKE) và SSL cung cấp xác thực Client và Server
    - IPSec và SSL cung cấp tính năng đảm bảo an toàn và xác thực đối với dữ liệu, thậm chí trên các mức khác nhau của chồng giao thức.
    - IPSec và SSL có thể dùng các thuật toán mật mã mạnh cho việc mã hoá và các hàm băm, có thể sử dụng xác thực dựa trên chứng chỉ (IPSec qua IKE).
    - IPSec(qua IKE) và SSL cung cấp tính năng sinh khoá và làm tươi khoá mà không phải truyền bất kỳ khoá nào dưới dạng rõ hay ngoại tuyến.
  - Khác nhau:

	IPSec VPN	SSL VPN
Kiểu kết nối	Cố định	Tạm thời
Kiểu thiết bị	Quản lý được	Không quản lý
Kiểu truy cập	Site-to-site	Truy cập từ xa
Kiểm soát truy cập	Không chi tiết	Chi tiết
Phần mềm yêu cầu	IPSec client	Trình duyệt
Tương thích firewall, NAT	Không tương thích	Tương thích
Mã hoá	DES, Triple DES, AES	RC4, DES, TripleDES
Xác thực	RADIUS, ActiveDirectory RSA SecureID X.509	RADIUS,Active Directory RSA SecureID X.509
Ứng dụng	Tất cả các ứng dụng trên IP. Các ứng dụng trên nền Web,	Một số ứng dụng như email,Terminal services, CIFS.

Bảng 1: So sánh IPSec và SSL trong VPN

9. Trình bày về SA: khái niệm, các thành phần của SA, vai trò, định dạng của các thành phần này, các cơ sở dữ liệu dành cho SA, các ví dụ về SA. Phân biệt IKE SA và IPSec SA.

❖ **Khái niệm**

- SA (Security Associations) là một khái niệm cơ bản của bộ giao thức IPSec. SA là một kết nối logic theo một hướng duy nhất giữa hai thực thể sử dụng các dịch vụ IPSec.
- Có hai kiểu SA
  - ISAKMP SA (hay IKE SA)
  - IPSec SA

❖ **Các thành phần của SA, vai trò, định dạng của các thành phần này**

- Một IPSec SA bao gồm các thông tin sau:
  - Dùng giao thức an toàn nào: AH hay ESP
  - Thuật toán mã hóa/giải mã & khóa nào: DES | 3 DES
  - Phương pháp và khóa xác thực nào được dùng cho AH | ESP: Hàm băm (HMAC, MD5, SHA1), chữ ký số (RSA), chứng chỉ số, Diffie-Hellman để quản lý khóa…
  - Thông tin liên quan đến khoá như: khoảng thời gian thay đổi và khoảng thời gian làm tươi của khoá.
  - Thông tin liên quan đến chính SA, bao gồm: địa chỉ nguồn SA, khoảng thời gian làm tươi
- Một SA gồm 3 phần:

<Chỉ số tham số an toàn, Địa chỉ IP đích, Giao thức an toàn>

SPI	Destination IP Address	Sercurity Protocol

  - SPI:
    - Là một trường 32 bit, dùng để xác định một SA để gắn với một gói dữ liệu
    - Là một chỉ số duy nhất cho mỗi bản ghi của cơ sở dữ liệu SADB (giống khóa chính).
    - Được định nghĩa bởi người tạo SA, được lựa chọn bởi hệ thống đích khi thương lượng SA.
    - SPI nhận các giá trị trong khoảng từ 1…255
  - Địa chỉ IP đích: Là địa chỉ IP của Node đích

- Giao thức an toàn:
  - Mô tả giao thức an toàn IPSec được dùng, có thể là AH hoặc ESP
  - Với hai điểm liên lạc: cần một SA cho mỗi hướng.
  - SA có thể cung cấp các dịch vụ an toàn cho một phiên VPN (được bảo vệ bởi AH hay ESP).
    - Nếu một phiên VPN được bảo vệ kép bởi cả AH và ESP thì mỗi hướng kết nối cần định nghĩa 2 SA.

❖ **Các cơ sở dữ liệu dành cho SA**

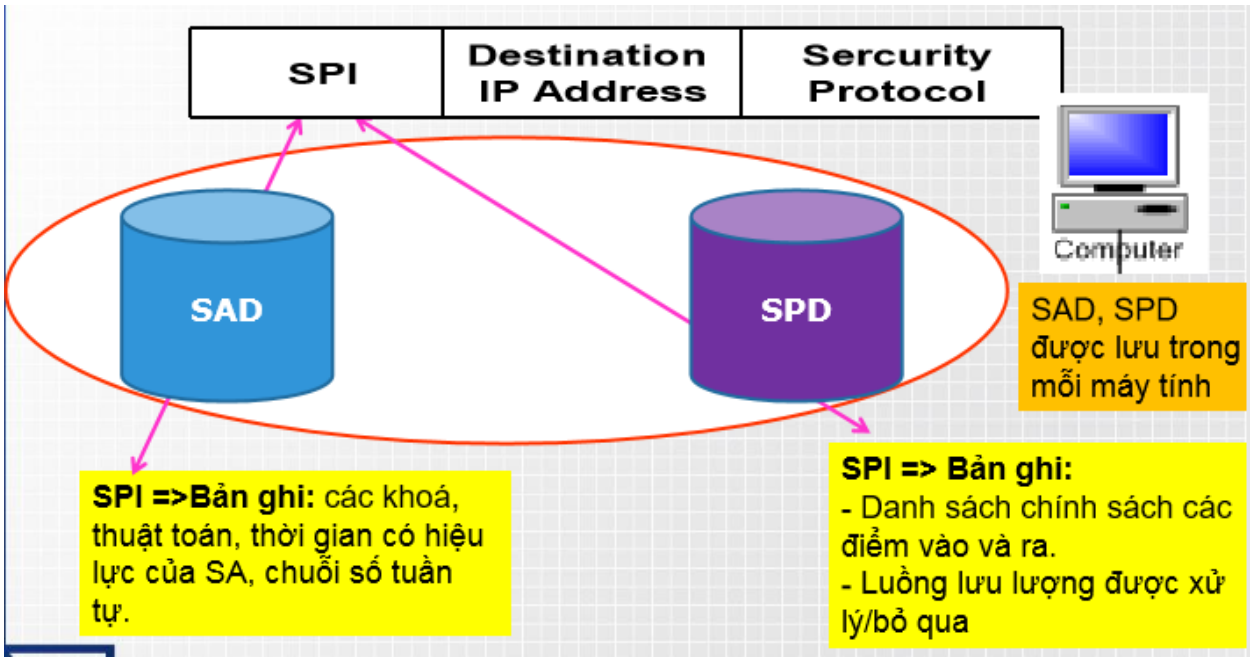
Một SA sử dụng 2 cơ sở dữ liệu

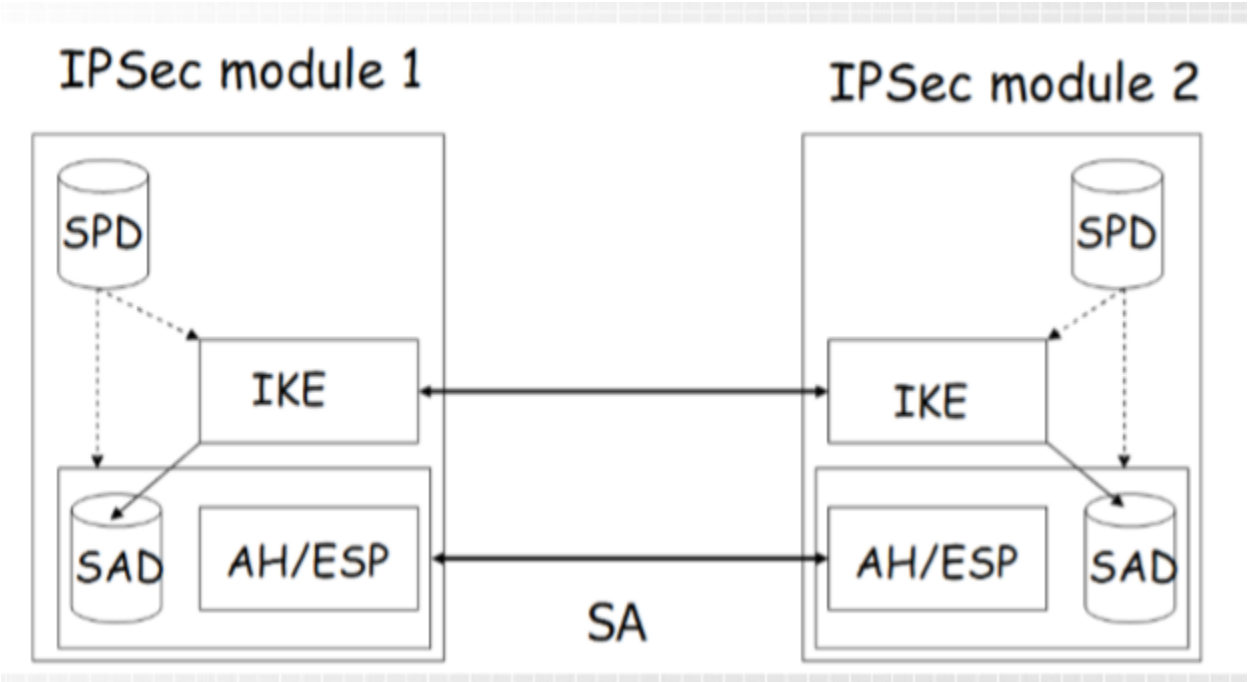
• Cơ sở dữ liệu tổ hợp an toàn (SAD - Security Association Database)

- Duy trì thông tin liên quan tới mỗi SA, bao gồm: các khoá, thuật toán, thời gian có hiệu lực của SA, chuỗi số tuần tự.

• Cơ sở dữ liệu chính sách an toàn (SPD - Security Policy Database)

- Lưu các chính sách để thiết lập các SA
- Duy trì thông tin về các dịch vụ an toàn kèm theo với một danh sách chính sách các điểm vào và ra.
- Định nghĩa luồng lưu lượng được xử lý/bỏ qua





❖ **Ví dụ về SA**:

- Ví dụ IPSec SA

DST address	192.168.105.2
Src address	192.168.105.1
SPI	AF11557D
protocol	ESP
Algorithm	ESP-ENCRYPT-DES ESP-AUTH-SHA1

- Ví dụ IKE SA

Địa chỉ đích	192.168.1.154
giá trị SPI	7A390BC1
IPSec Transform	AH, HMAC-SHA
key	7572CA49F7632946
Thuộc tính	30 phút

❖ **Phân biệt IKE SA và IPSec SA.**

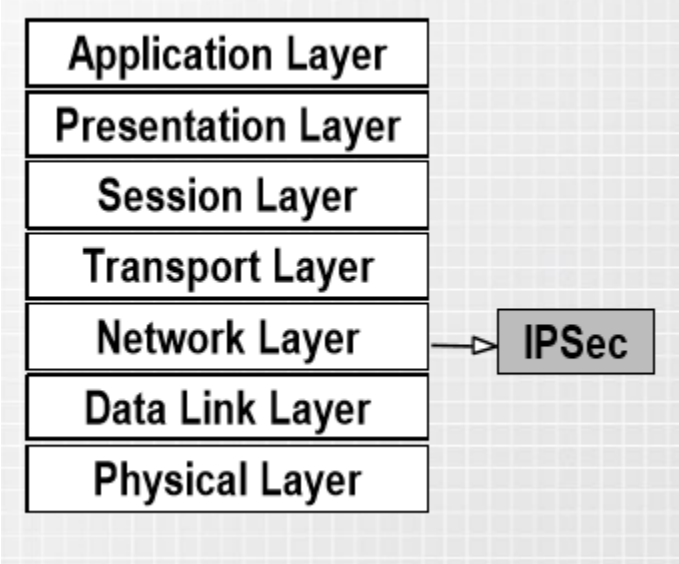
10. Các đặc điểm cơ bản về giao thức IPSec, các thành phần và giao thức con của IPSec, các dịch vụ an toàn mà IPSec đem lại. Ưu, nhược điểm của IPSec.

❖ **Các đặc điểm cơ bản về giao thức IPSec**

- IPSec = Internet protocol security là một bộ giao thức để đảm bảo an toàn thông tin liên lạc sử dụng bộ giao thức Internet bằng cách xác thực và mã hóa mỗi gói tin IP của một phiên.
- Được phát triển bởi IETF
- Thực hiện việc an toàn các gói IP
- Cung cấp các khả năng:
  - Xác thực nguồn gốc thông tin

- Kiểm tra tính toàn vẹn thông tin
- Đảm bảo bí mật nội dung thông tin
- Cung cấp khả năng tạo và tự động làm tươi khoá mật mã một cách an toàn

- IPSec cung cấp một khung an toàn tại tầng 3 của mô hình OSI



- Thực hiện đảm bảo an toàn tại tầng IP
- Các giao thức tầng trên và các ứng dụng có thể dùng IPSec để đảm bảo an toàn mà không cần phải thay đổi gì => Các gói IP sẽ được bảo vệ mà không phụ thuộc vào các ứng dụng đã tạo ra nó
- IPSec hoàn toàn trong suốt với người dùng
- IPSec hoạt động ở hai chế độ:
  - Chế độ Transport (end-to- end)
  - Chế độ Tunnel (cho VPN)

❖ **Các thành phần và giao thức con của IPSec, các dịch vụ an toàn mà IPSec đem lại.**

❖ IPSec bao gồm 2 giao thức:

- Tiêu đề xác thực (AH – Authentication Header)
  - Đảm bảo tính toàn vẹn,
  - Cung cấp khả năng bảo vệ chống lại sự giả mạo,
  - Cung cấp chế độ xác thực đối với máy chủ

  ICV = hash (IP header + payload + key)
- Đóng gói tải an toàn (ESP – Enscapsulating Security Payload)
  - Thực hiện các chức năng như AH, nhưng có thêm tính năng đảm bảo bí mật dữ liệu./.

    ICV = hash (New IP header + IP header + payload)

    Payload = encrypt (IP header + payload + IV)

❖ IPSec cung cấp an toàn cho 3 tình huống:

- Host – to – host
- Host – to – gateway
- Gateway – to – gateway

❖ **Ưu, nhược điểm của IPSec.**

❖ **Ưu điểm:**

- Khi IPSec được triển khai trên bức tường lửa hoặc bộ định tuyến của một mạng riêng thì tính năng an toàn của IPSec có thể áp dụng cho toàn bộ vào ra mạng riêng đó mà các thành phần khác không cần phải xử lý thêm các công việc liên quan tới bảo mật.
- IPSec được thực hiện bên dưới lớp TCP và UDP ,đồng thời nó hoạt động trong suốt đối với các lớp này.Do vậy không cần phải thay đổi phần mềm hay cấu hình lại các dịch vụ khi IPSec được triển khai.
- IPSec có thể được cấu hình để hoạt động một cách trong suốt đối với các ứng dụng đầu cuối,điều này giúp che dấu những chi tiết cấu hình phức tạp mà người dùng phải thực hiện khi kết nối đến mạng nội bộ từ xa thông qua Internet.

❖ **Nhược điểm:**

- Tất cả các gói được xử lý theo IPSec sẽ bị tăng kích thước do phải thêm vào các tiêu đề khác nhau, và điều này làm cho thông lượng hiệu dụng của mạng giảm xuống. Vấn đề này có thể được khắc phục bằng cách nén dữ liệu trước khi mã hóa, song các kĩ thuật như vậy vẫn còn đang nghiên cứu và chưa được chuẩn hóa.
- IPSec được thiết kế chỉ để hỗ trợ bảo mật cho lưu lượng IP, không hỗ trợ các dạng lưu lượng khác.
- Việc tính toán nhiều giải thuật phức tạp trong IPSec vẫn còn là một vấn đề khó đối với các trạm làm việc và máy PC năng lực yếu.
- Việc phân phối các phần cứng và phầm mềm mật mã vẫn còn bị hạn chế đối với chính phủ một số quốc gia

11. Các đặc điểm cơ bản của AH và ESP, định dạng gói tin, các khả năng AH và ESP đem lại. So sánh sự khác nhau AH và ESP. Nêu ưu và nhược điểm của AH và ESP.

a) Giao thức AH (Authentication Header)

❖ AH được thêm một tiêu đề vào gói tin IP

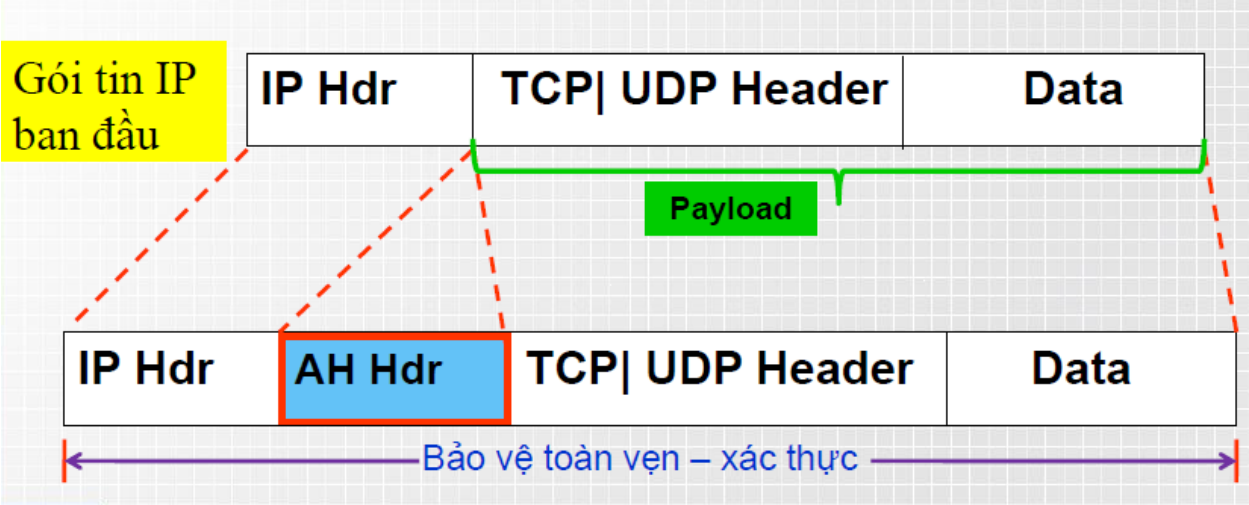
- Xác thực người gửi: tiêu đề này dùng cho việc thực gói dữ liệu IP gốc tại người nhận (Ai là người gửi gói tin)
- Toàn vẹn gói tin: tiêu đề này cũng giúp nhận biết bất kỳ sự thay đổi nào về nội dung của gói dữ liệu.
- Sử dụng mã xác thực thông điệp (HMAC)
- AH không mã hóa bất kỳ phần nào của gói tin.

❖ **Chế độ hoạt động**

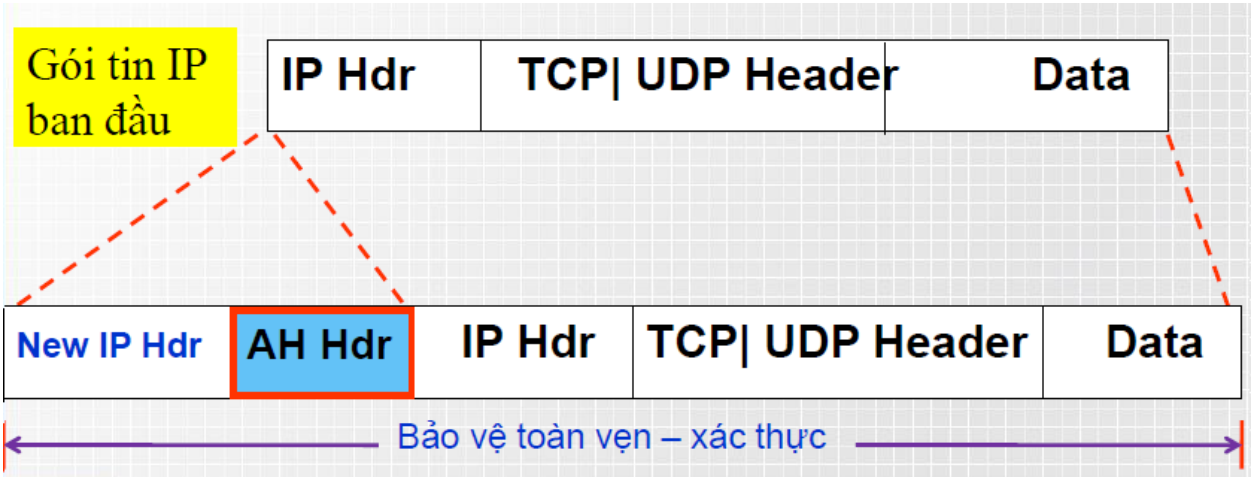
AH có thể sử dụng ở cả hai chế độ: truyền tải (Transport mode) và đường hầm (Tunnel mode)

- Chế độ Transport
  - Trong chế độ này tiêu đề AH được chèn vào sau tiêu đề IP và trước một giao thức lớp TCP hoặc UDP

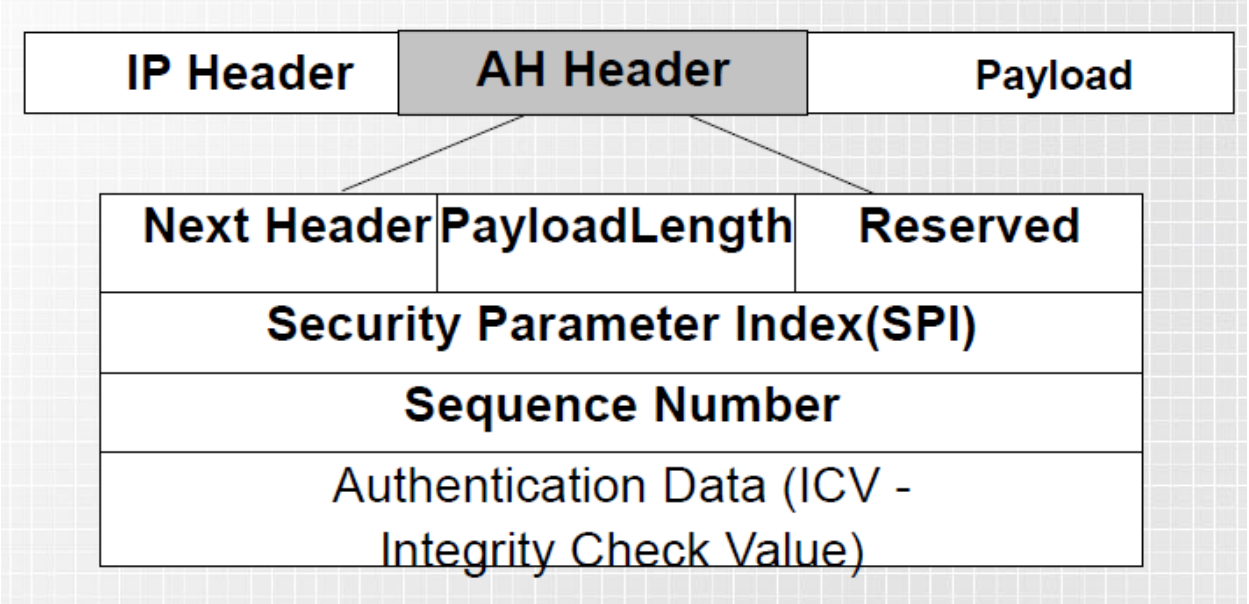
- Không tạo một IP Header mới



- Chế độ Tunnel
  - Một gói tin IP khác được thiết lập dựa trên gói tin IP cũ
  - Tạo một IP Header mới: liệt kê các đầu cuối của AH tunnel (như hai IPSec gate way)
  - Tiêu đề IP cũ (bên trong) chứa địa chỉ nguồn và đích, tiêu đề IP mới (bên ngoài) mang địa chỉ để định tuyến trên Internet



❖ **Khuôn dạng gói tin**: các trường AH Header đều là bắt buộc



- Next Header: dài 8bit, chứa chỉ số giao thức IP
  - Trong Tunnel mode: Payload là gói tin IP nên giá trị Next Header được cài đặt là 4
  - Trong Transport mode: Payload luôn là giao thức tầng Transport
    - UDP: Next Header là 17
    - TCP: Next Header là 6
- Payload length: chứa chiều dài của thông điệp AH
- Header Reserved: độ dài 16 bit, trường này không được sử dụng, các bit đều bằng 0
- SPI: 32 bit, chỉ ra SPI được sử dụng + SPD
  - Bên nhận dựa trên giá trị SPI cùng với IP đích và loai giao thức IPSec (ở đây là AH) => Xác định được chính sách SA dùng cho gói tin
  - SA: Loại giao thức IPSec nào được chọn (AH hay ESP) , Các thuật toàn nào được dùng để áp cho gói tin
- Sequence number: 32 bit, chỉ ra số thứ tự gói ti AH. Chỉ số này tăng lên 1 cho mỗi datagram khi một host gửi có liên quan đến chính sách SA tương ứng.
- Authentication Data (ICV): Có độ dài là bội của 32 bit. Phải được padding nếu chiều dài của ICV trong các byte chưa đầy. Được dùng để kiểm tra tính xác thực người gửi. Tính toàn vẹn của thông điệp

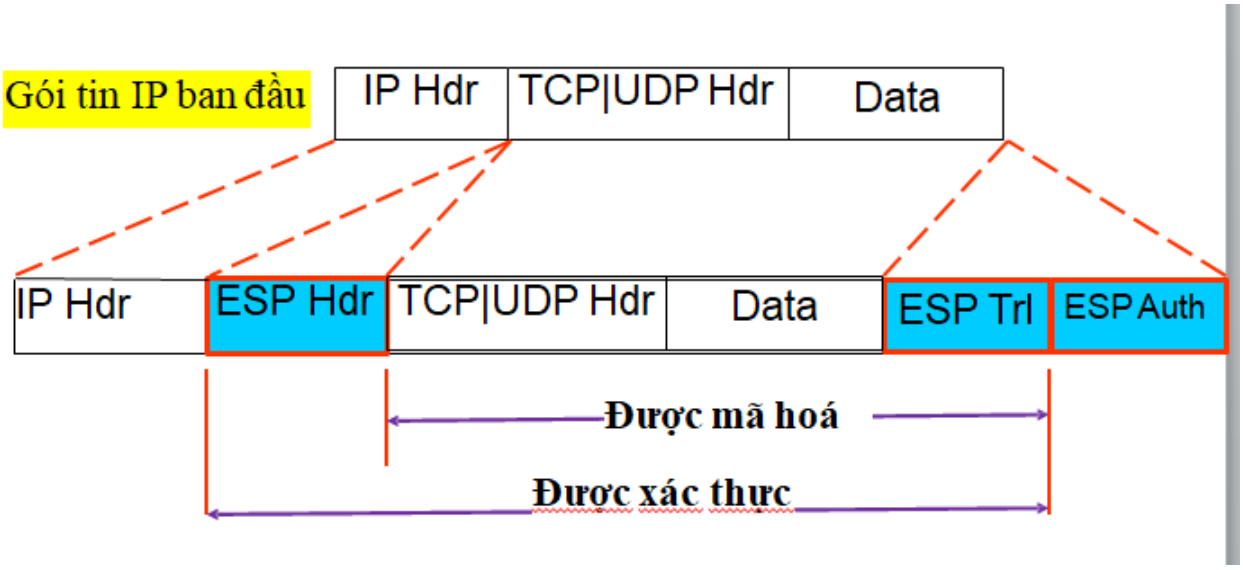
Authentication Data (ICV): 96 bit ICV = Hash (IP Header + Payload + Key)

b) Giao thức ESP (Encapsulating Security Payload):

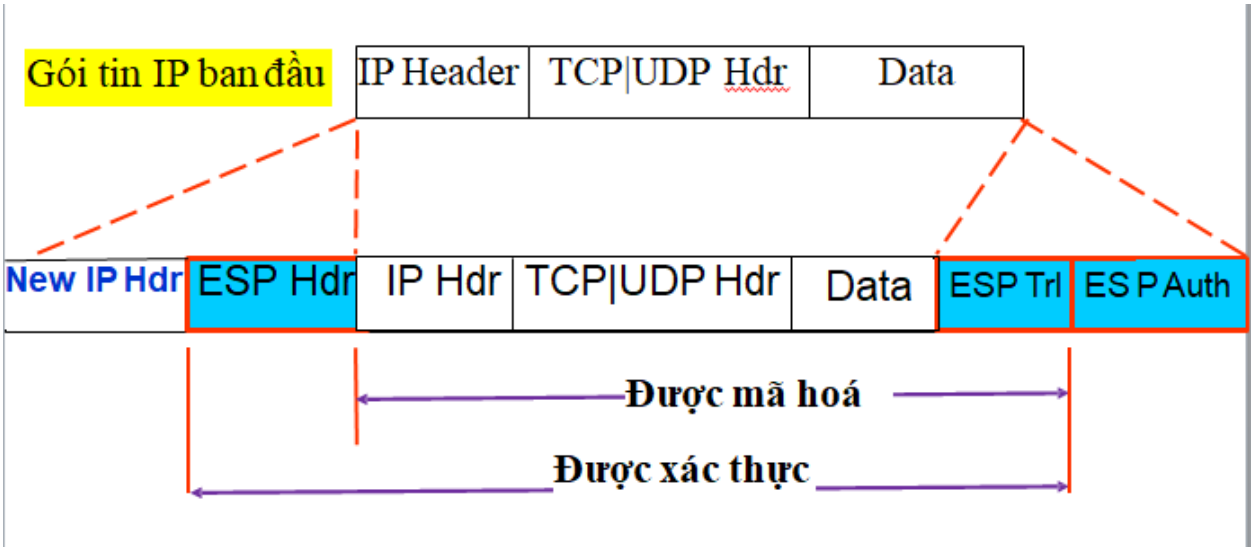
Là giao thức đóng gói tải an toàn của IPSec. Đảm bảo tính toàn vẹn, tính bí mật, xác thực, chống replay gói tin cũ.

❖ Chế độ hoạt động:
ESP có thể sử dụng ở cả hai chế độ: truyền tải (Transport mode) và đường hầm (Tunnel mode)

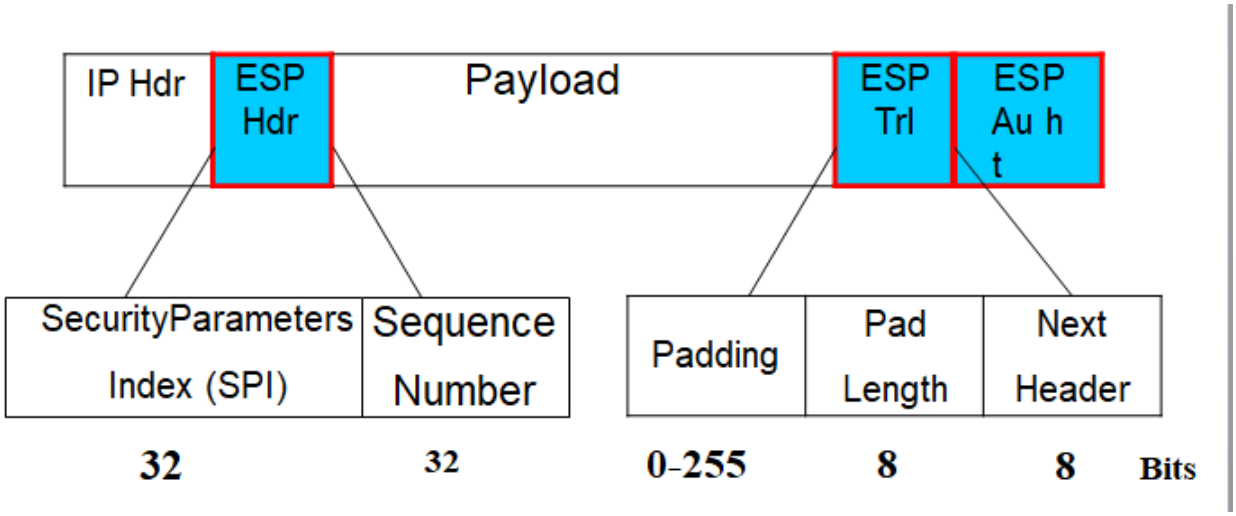
- Chế độ transport
  - Dùng IP Header gốc
  - Chỉ mã hóa và/ hoặc đảm bảo toàn vẹn cho nội dung gói tin và một số thành phần ESP, nhưng không có IP Header



- Chế độ tunnel
  - Tạo một IP Header mới: liệt kê các đầu cuối của ESP Runnel (như 2 IPSec Gateway)
  - Mã hóa và/ hoặc đảm bảo toàn vẹn cho nội dung gói tin, có cả IP Header và một số thành phần ESP



❖ Khuông dạng gói tin



- SPI: mỗi bên liên lạc tùy chọn giá trị SPI, bên nhận dựa vào SPI, địa chỉ IP đích, giao thức IPSec (ESP) để xác định một SA duy nhất để áp cho gói tin nhận được.
- Sequence Number: khởi tạo bằng 0, tăng 1 nếu mỗi gói tin được gửi, để chống trùng lặp gói tin
- Payload: là phần payload data được mã hóa
- Padding (0-255 byte): là phần dữ liệu được thêm vào gói tin (trước khi mã hóa) để đoạn dữ liệu được mã hoa là một số nguyên lần của một khối các byte. Nó cũng được dùng để che dấu độ dài thực của Payload
- Pad Length: trường này xác định số byte padding đã thêm vào

- Next Header:
  - Trong Tunnel mode: Payload là gói tin IP, thì Next Header = 4 (IP- in IP)
  - Trong Transport mode: Payload là giao thức tầng 4 Transport
    - TCP: next header = 6
    - UDP: next header = 17
- Authentication Data: chứa giá trị ICV (phải là bội của 32 bit)
  ICV = HMAC(ESP Hdr + Payload + ESPTrl +Key)

c) So sánh sự khác nhau AH và ESP

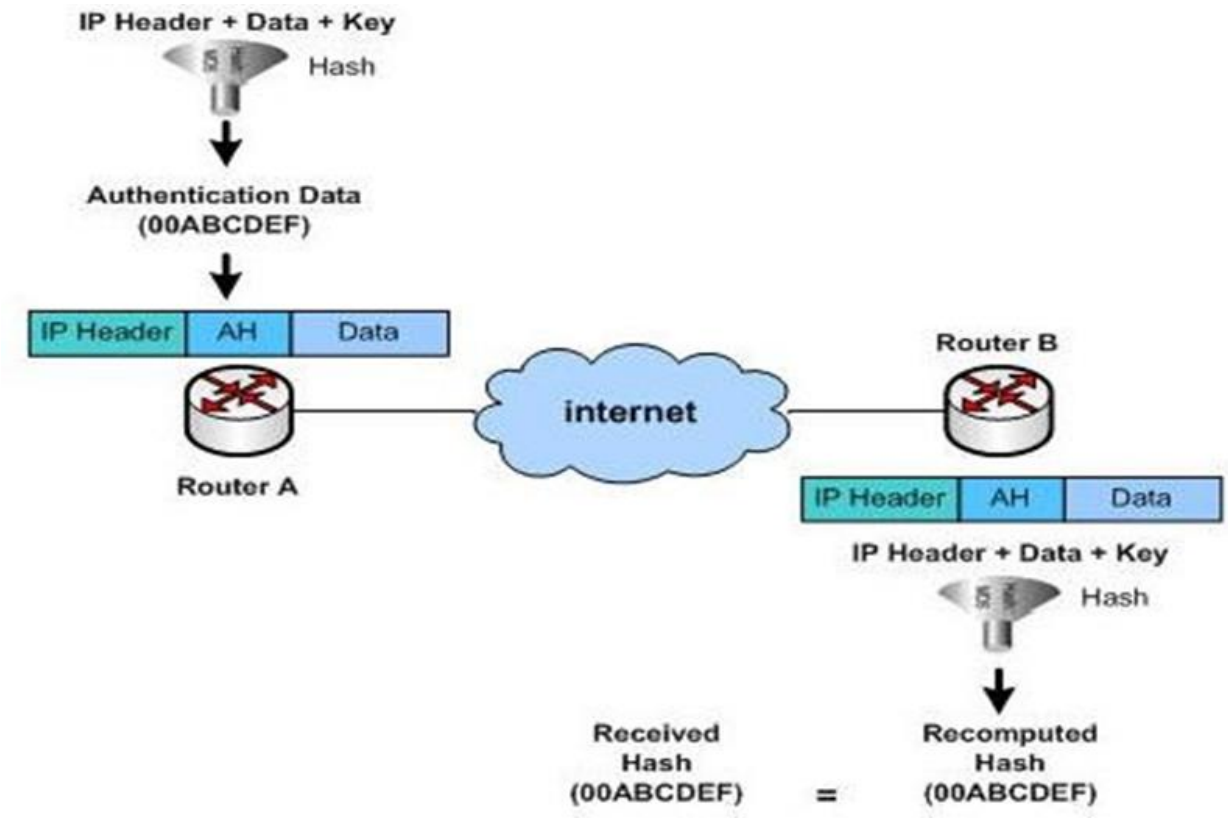
AH xác thực cả IP Header, ESP thì không

Bảng so sánh giữa giao thức AH và ESP

Security	AH	ESP
Layer-3 IP protocol number	51	50
Provides for data integrity	yes	Yes
Provides for data authentication	Yes	yes
Provides for data encryption	No	Yes
Protects against data replay attacks	yes	yes
Works with NAT	No	yes
Works with PAT	No	No
Protects the IP packet	yes	No
Protects only the data	No	yes

d) Ưu, nhược điểm của AH và ESP

12. Giải thích khả năng đảm bảo toàn vẹn và xác thực dữ liệu cho gói tin IP nhờ giao thức AH



Bước 1: toàn bộ gói IP (bao gồm IP Header và Data) được chạy qua một giải thuật băm một chiều cùng với 1 key (hai bên đã thỏa thuận trước)

Bước 2: giá trị băm thu được dùng xây dựng một AH Header, đưa header này chèn vào dữa IP Header và Data của gói tin ban đầu.

Bước 3: Gói dữ liệu sau khi thêm AH header được truyền tới đối tác.

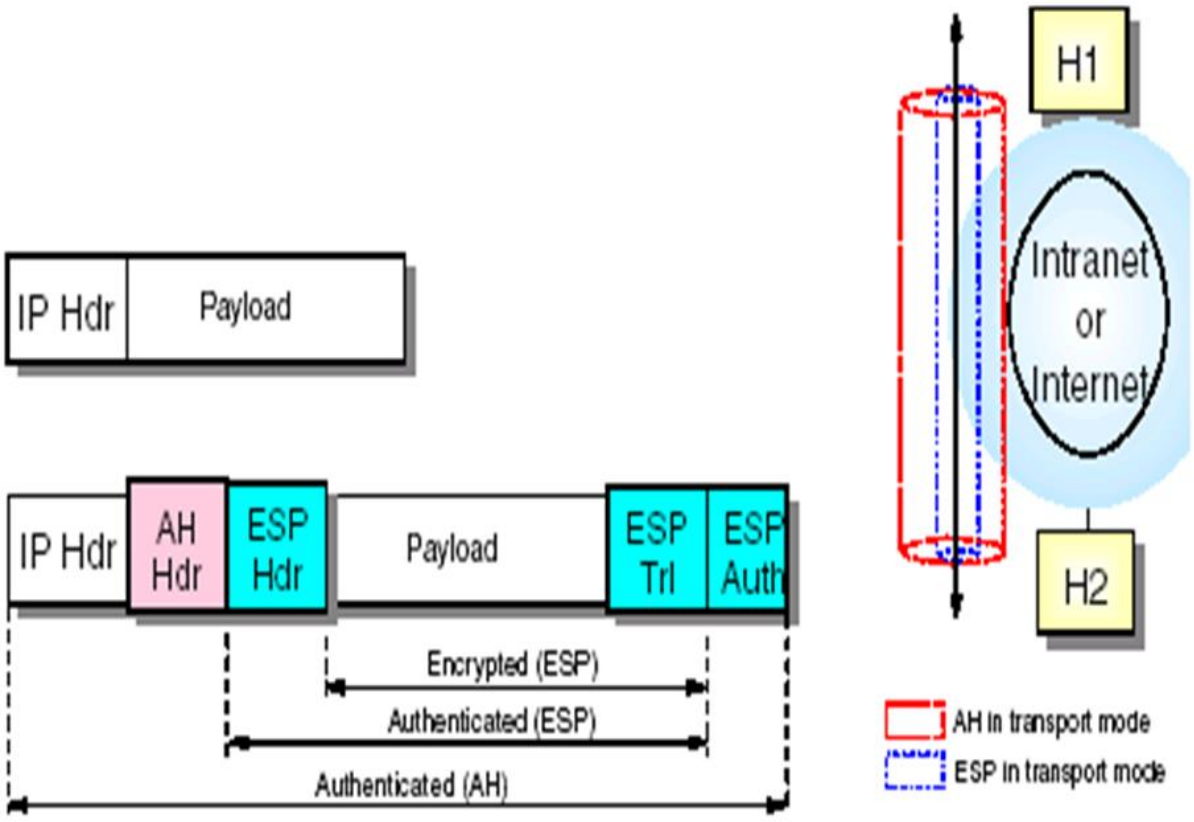
Bước 4: Bên thu thực hiền hàm băm với IP Header và data với key mà hai bên đã thỏa thuận trước, kết quả thu được một giá trị băm

Bước 5: bên thu tách giá trị băm trong AH Header và so sánh với giá trị băm mà nó vừa tính. Nếu hai mã này giống nhau thì gói tin này đã được đảm bảo toàn vẹn và xác thực, nếu khác nhau thì bên thu sẽ phát hiện ra ngay gói tin này không còn toàn vẹn (dựa vào tính chất kháng va chạm của hàm băm)

13. Vẽ và phân tích định dạng gói tin khi được bảo vệ kép với AH và ESP

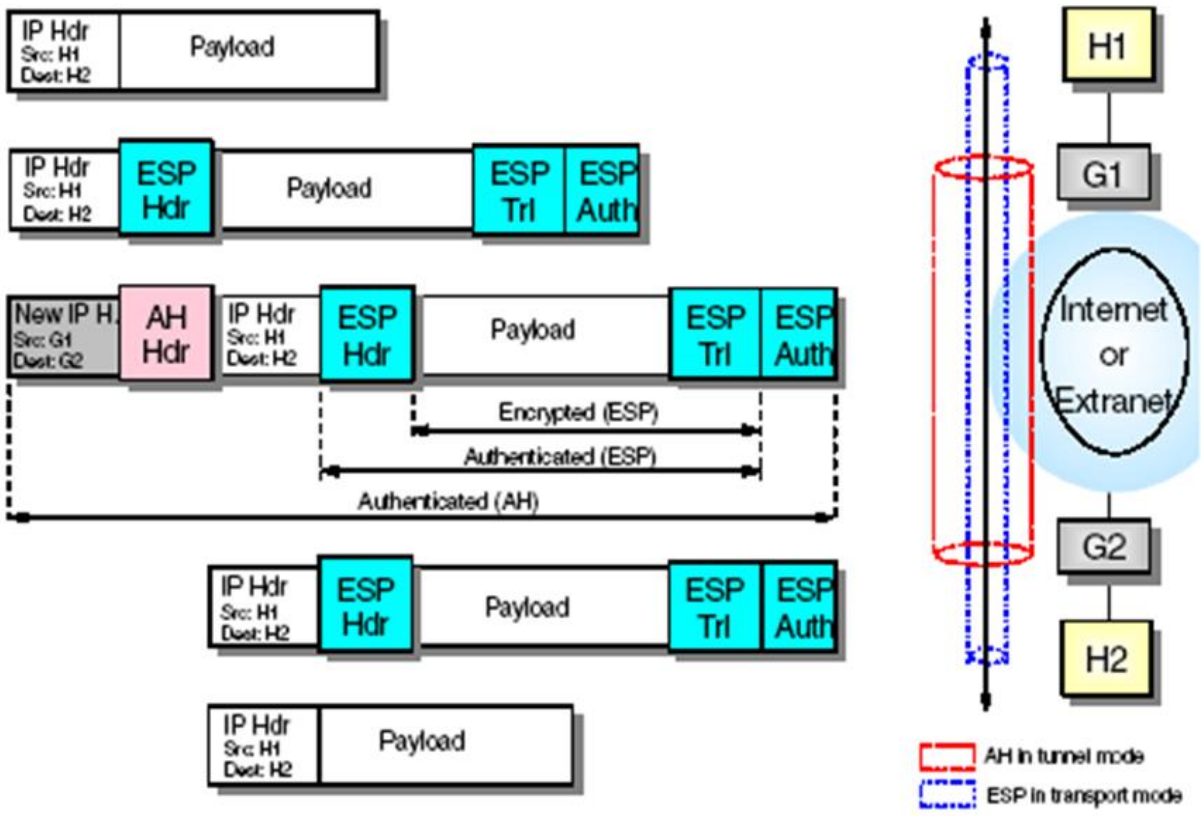
- ❖ Kết hợp AH và ESP chế độ transport

Gói IP ban đầu được tách Header ra, tiếp theo phần Payload được xử lý ESP sau đó được xử lý bằng AH. Cuối cùng, IP Header được thêm vào. Như vậy gói tin sẽ được đảm bảo an toàn 2 lớp: lớp bên ngoài là AH, lớp bên trong là ESP.



❖ Kết hợp AH và ESP chế độ tunnel

Ban đầu, gói tin IP được xử lý ESP ở chế độ Transport, tiếp theo đó toàn bộ gói tin ESP được xử lý AH trong chế độ Tunnel.



14. Trình bày cơ bản về giao thức IKE, vai trò IKE trong IPsec, vai trò của từng pha trong giao thức IKE, Cho ví dụ.

❖ **Giao thức trao đổi khóa IKE (Internet key exchange)**

- Là giao thức để quản lý, trao đổi khóa trong IPSec
- Cho phép thương lượng và tạo tự động các IPSec SA giữa các bên liên lạc IPSec.
- IKE cũng chịu trách nhiệm xoá các khoá, SA sau khi một phiên truyền tin kết thúc
- IKE không nhanh nhưng hiệu quả vì một số lượng lớn SA được thương lượng chỉ với một số thông điệp vừa phải.
- IKE được xây dựng dựa trên nền tảng của hai giao thức
    - Giao thức phân phối khóa Oakley

- Giao thức quản lý khóa ISAKMP
- IKE Có thể được sử dụng bên ngoài IPSec
- IKE hiện đã được phát triển với 2 phiên bản, phiên bản IKEv1 và IKEv2.

❖ **Vai trò IKE trong bộ giao thức IPsec**

- IPSec cần các SA để bảo vệ lưu lượng
- Nếu chưa có các SA, IPSec sẽ yêu cầu IKE cung cấp các IPSec SA.
- IKE mở một phiên quản lý với các bên tham gia, và thương lượng tất cả các SA và các khóa cho IPSec.
- IPSec bắt đầu thực hiện bảo vệ lưu lượng.

❖ **Vai trò của từng pha trong giao thức IKE**

IKE gồm 2 pha: 2 pha trao đổi khoá sẽ tạo ra IKE SA và một đường hầm an toàn giữa 2 hệ thống

• Một bên sẽ đưa ra một trong các thuật toán, phía kia sẽ chấp nhận hoặc loại bỏ kết nối.

• Khi 2 bên đã thống nhất được thuật toán sử dụng thì sẽ tạo khoá cho IPSec

• Khoá này có được nhờ sử dụng thuật toán DiffieHellman.

- Pha 1:

+ Mục tiêu: Xác thực các bên tham gia và cung cấp bảo vệ cho việc thương lượng ở pha 2.

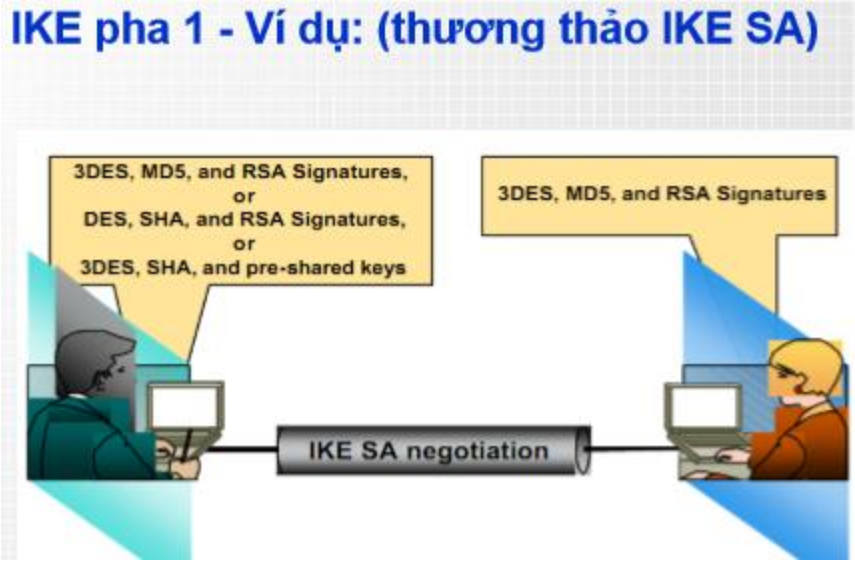
+ Sử dụng Diffie-Hellman để sinh một khóa bí mật chia sẻ cho việc mã hóa sau này.

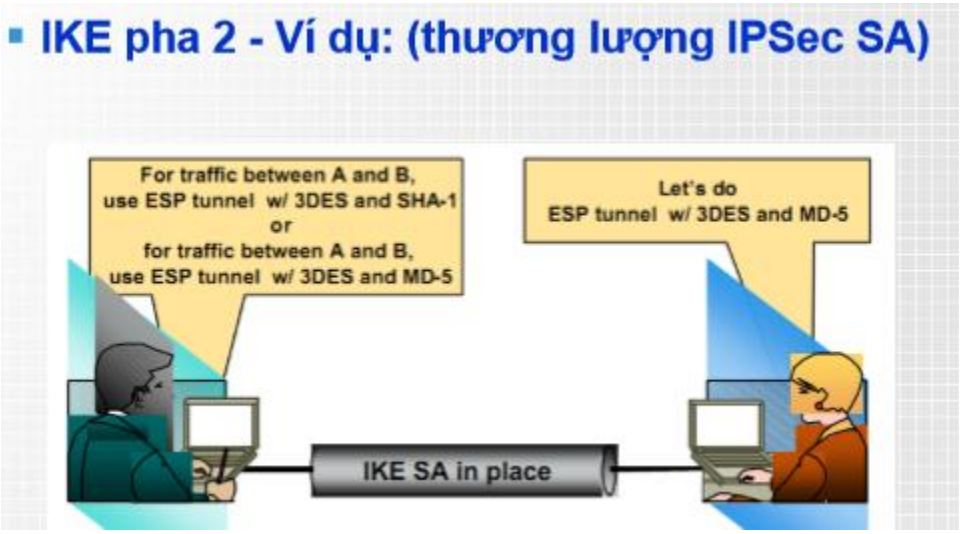
+ Kết quả là một IKE SA (2 hướng)

- Pha 2:

+ Mục đích chính là thỏa thuận được các khóa mật mã sử dụng để bảo vệ đường truyền cho các thực thể, và các SA cho trao đổi dữ liệu

Cho ví dụ

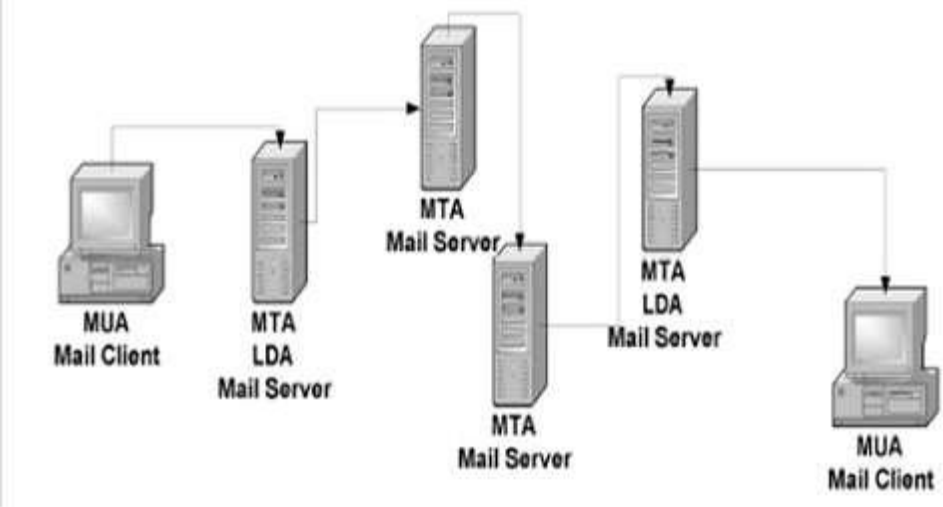




CHƯƠNG 4: CÁC GIAO THỨC BẢO MẬT DỊCH VỤ

15.Trình bày về mô hình truyền/nhận thư điện tử. Các thành phần chính trong hệ thống, mối quan hệ giữa các thành phần đó ?

❖ Mô hình truyền/nhận thư điện tử:



- WebMail(Phần mềm thư điện tử qua Web): loại phần mềm thư điện tử không cần phải cài đặt mà nó được cung ứng bởi các máy chủ (web server)

Ví dụ: mail.Yahoo.com, hay hotmail.com, gmail.com

- MUA (Mail User Agent) –Email Client: Là loại phần mềm thư điện tử được cài đặt trên từng máy tính của người dùng.

Ví dụ: Microsoft Outlook, Microsoft Outlook Express, Netscape Comunicator, hay Eudora.

- MTA (Mail Transfer Agent): là máy chủ thư điện tử, nhằm cung ứng các dịch vụ thư điện tử

❖ Cách thức truyền tin:

- Soạn thảo: nhập các trường chính như: chủ đề, nội dung, đối tượng nhận gửi, thông tin phần định dạng,…
- Thư sẽ được chuyển đổi sang một định dạng chuẩn xác định bởi RFC 822 (Standard for the Format of ARP Internet Text Messages)
- Thư sau khi chuyển đổi sẽ gồm hai phần: phần tiêu đề (header) và phần thân (body)

❖ Quá trình gửi thư

- MUA kết nối tới MTA trên Mail Server
- MUA cung cấp thông tin cho MTA: định danh đối tượng gửi, nhân thư, DNS,…

- Máy chủ thư sẽ thực hiện các thao tác: Định danh đối tượng nhận, thiết lập kết nối truyền thư

16. Trình bày một số giao thức truyền/nhận thư cơ bản: SMTP, MINE, IMAP, POP3; tìm hiểu và cho ví dụ về mã hóa base64.

a) SMTP:

- SMTP là giao thức tầng ứng dụng, SMTP được đánh giá là một giao thức truyền thông điệp thư đáng tin cậy và có hiệu quả cao
- SMTP chạy trên tầng TCP/IP, sử dụng port 25.

❖ **Định dạng bản tin**

SMTP: giao thức để trao đổi các bản tin thư điện tử

RFC 822: chuẩn định dạng bản tin dạng văn bản

- Header lines, ví dụ
  – To:
  – From:
  – Subject:

  khác *Lệnh SMTP*

- body
  – bản tin, ký tự ASCII

❖ **Thủ tục làm việc SMTP:**

Mỗi phiên làm việc SMTP gồm các phần sau:

– Khởi tạo phiên (Session Initiation)

– Khởi tạo Client (Client Initiation)

– Truyền thư (Mail Transactions)

– Kết thúc phiên và kết nối (Terminating Session and Connections)

❖ **Các trạng thái của SMTP:**

– Khi Client gửi 1 lệnh SMTP tới Server, client nhận trả về 1 mã trạng thái cho máy gửi biết điều gì đã xảy ra.

– Với thông điệp đáp trả có gắn 3 con số ở đầu dòng để thể hiện từng trạng thái riêng.

❖ **Hạn chế của SMTP:**

– Chỉ sử dụng với dữ liệu dạng ASCII 7 bit.

– Không có cơ chế xác thực

– Thông điệp gửi đi không được mã hóa

– Dễ bị tổn thương (bởi spam, mất định danh người gửi)

❖ **Giải pháp:**

– SMTP mở rộng

– MIME (Mở rộng thư tín Internet đa mục tiêu)

b) Giao thức MINE

MIME (Multipurpose Internet Mail Extension): RFC 2045, 2046.

- Là một chuẩn Internet về định dạng cho thư điện tử. Hầu như mọi thư điện tử Internet được truyền qua giao thức SMTP theo định dạng MIME. Vì gắn liền với chuẩn SMTP và MIME nên đôi khi thư điện tử Internet còn được gọi là thư điện tử **SMTP/MIME**.
- MIME cho phép gửi các thông điệp trên internet mà không chỉ thuần là văn bản, có thể gửi mail kèm ảnh, link, ….
- MIME không chỉ dùng cho mail mà có thể dùng cho các message nói chung, ví dụ như trong http
- Thêm các dòng trong Header của bản tin khái báo kiểu nội dung MIME : MIME version, method sử dụng để mã hóa dữ lieeuk, kiểu dữ liệu đa phương tiện, kiểu con, khai báo tham số, dữ liệu đã mã hóa
- Biến đổi dữ liệu non-ASCII sang dạng ASCII

c) Phương pháp mã hóa base64

❖ Gồm các bước chính sau:

- Chia file nhị phân thành nhiều nhóm nhỏ dài 3byte
- Mã hóa từng nhóm 3byte thành 4 ký tự ASCII 7bit in ấn như sau:
    - Gộp 3 byte thành 24bit liên tiếp, chia thành 4 nhóm 6bit có giá trị từ 0-63.
    - Mỗi nhóm 6bit tương ứng với 1 ký tự in ấn như sau:

      0-25 -> A-Z
      26-51-> a-z
      52-61-> 0-9
      62-> +
      63-> /

❖ Ví dụ:

Thông báo M	77	97	110
Bit pattern	0 1 0 0 1 1 0 1	0 1 1 0 0 0 0 1	0 1 1 0 1 1 1 0
Index	19	22	5	46
Base64-encoded	T	W	F	u

d) Giao thức POP3

❖ **Tổng quan giao thức:**

- POP3 (Post Office Protocol ver 3) là giao thức tầng ứng dụng, dùng để truy nhập và lấy thư điện tử từ mailbox trên máy chủ thư tín thông qua kết nối TCP/IP, port 110.
- Trước POP3 có 2 phiên bản ra đời trước là: Năm 1984 sử dụng POP, 1988 sử dụng POP2. Đến nay, POP3 được sử dụng thông dụng nhất và được xác định trong RFC 1939.

❖ **Hoạt động của POP3**

- POP3 client xác thực thành công với server, server có khóa và mở được maildrop thích hợp. Client có thể truy nhập tới mailbox của mình trên server để kiểm tra, nhận thư…
- Nếu Maildrop không mở (-ERR), server đóng kết nối or client gửi lệnh xác nhận và bắt đầu lại từ đầu
- Thiết lập kết nối TCP ở công 110
- Client gửi lệnh QUIT tới server thì trạng thái Trasaction chuyển sang Update.
- Server gửi goodbye tới client và đóng kết nối TCP, kết thúc phiên làm việc.

e) Giao thức IMAP

❖ **Tổng quan giao thức:**

- IMAP (Internet Messages Access Protocol) được phát minh bởi Mark Crispin năm 1986 tại trường ĐH Stanford.
- IMAP là giao thức hoạt động ở tầng ứng dụng, cho phép Client truy nhập email trên một Server từ xa.
- IMAPv2 được phát minh năm 1987, IMAPv4 được phát minh năm 1994, được miêu tả trong RFC 2060 sử dụng port 143/tcp.
- IMAPv4 email được lưu trữ trên mail server và có thể truy cập từ bất kì máy email client IMAP4 nào trên mạng.

- IMAP4 có thể thực hiện các thao tác như: tạo, xóa, sửa đổi tên mailbox, kiểm tra mail mới, update mail cũ (trong RFC 2822), thiết lập và xóa cờ trạng thái

❖ **Mục đích sử dụng IMAP:**

- Tương thích đầy đủ với các chuẩn thông điệp Internet (MIME)
- Cho phép truy nhập & quản lý thông điệp từ nhiều máy tính khác nhau
- Hỗ trợ truy nhập đồng thời tới các mailbox dùng chung
- Phần mềm bên Client không cần biết kiểu lưu trữ file của Server

17. Tìm hiểu cơ bản về S/MINE và PGP

a) Giao thức S/MINE

- S/MIME (Security/Multipurpose Internet Mail Extensions (MIME): Là một phiên bản cho giao thức MIME hỗ trợ mã hóa.
- SMIME đưa vào hai phương pháp an toàn cho email dựa trên mã hóa bất đối xứng và PKI.

  - Mã hóa email: Động tác mã hóa = mã hóa message bằng public key của người nhận. Giải mã bằng private key của người nhận.

  - Xác thực email: Động tác ký = mã hóa message bằng private key của người gửi. Xác thực = dùng public key của người gửi giải mã bản tin.

- Các phiên bản S/MIME
  - Phiên bản S/MIME v1: năm 1995, nhưng không được công bố chính thức.
  - Phiên bản S/MIME v2 được IETF chính thức công bố vào tháng 3/1998 là một tiêu chuẩn Internet tại RFC 2311 và RFC 2312 . S/MIME đã trở thành một trong những tiêu chuẩn hàng đầu về bảo mật thông điệp.
  - Phiên bản S/MIME v3 được IETF đề xuất vào tháng 6/1999 nhằm tăng cường khả năng của S/MIME, bao gồm RFC 2632 ,

RFC 2633 và RFC 2634, được cập nhật mới đây nhất tại RFC 5751 tháng 1/2010.

- Trong Thông tư số 01/2011/TT-BTTTT ngày 04/01/2011 của Bộ Thông tin và Truyền thông Công bố Danh mục tiêu chuẩn kỹ thuật về ứng dụng công nghệ thông tin trong cơ quan nhà nước quy định Bắt buộc áp dụng tiêu chuẩn S/MIME v3.2 và được xếp vào nhóm Tiêu chuẩn về an toàn thông tin.

a) Giao thức PGP

- PGP (Pretty Good Privacy):

  - Là một chương trình cung cấp tính năng mã hóa và xác thực cho dữ liệu. PGP thường được sử dụng để ký, mã hóa, và giải mã văn bản, e-mail, các tập tin, thư mục và phân vùng đĩa toàn bộ để tăng tính bảo mật của thông tin liên lạc e-mail.

  - Được tạo ra bởi Phil Zimmermann vào năm 1991.

  - PGP còn được sử dụng khá phổ biến cho nhiều đối tượng cũng như các ứng dụng khác ngoài e-mail.

- PGP sử dụng các thuật toán:

  • Mã hóa đối xứng: DES, 3DES, AES, v.v.

  • Mã khóa KCK: RSA, ElGamal.

  • Hàm băm: SHA-1, MD-5, v.v.

  • Chữ ký: RSA, DSS, ECDSA, v.v

CHƯƠNG 5: CÁC GIAO THỨC BẢO MẬT MẠNG KHÔNG DÂY

18. Phân loại mạng không dây, các mô hình WLAN thông dụng.

a.Phân loại mạng không dây:

- WPAN (Wireless Personal Area Network):
    - Mạng không dây cá nhân: Bao gồm các công nghệ vô tuyến có vùng phủ sóng trong phạm vi vài chục mét.
    - Mục đích phục vụ các thiết bị ngoại vi: máy in, bàn phím, chuột, đồng hồ, ĐTDĐ.
    - Các công nghệ sử dụng: Bluetooth, Wibree, ZigBee, Wireless USB,
    - Chuẩn của công nghệ: IEEE 802.15
    - Sóng Bluetooth:
        - Là công nghệ không dây tầm gần giữa các thiết bị điện tử.
        - Hỗ trợ truyền dữ liệu ở khoảng cách ngắn giữa các thiết bị di động và cố định.
        - Tốc độ tối đa: 1Mbps
        - Sóng vô hướng và dải băng tần 2,4 GHz
- WLAN (Wireless Local Area Network):
    - Mạng không dây cục bộ (Wifi): Bao gồm các công nghệ vô tuyến có vùng phủ sóng trong phạm vi vài trăm mét.
    - Nổi bật là công nghệ Wifi với nhiều chuẩn mở rộng khác nhau thuộc họ 802.11 a/b/g/h/i/n...
    - Mục đích phục vụ các thiết bị: Laptop, thiết bị cầm tay, máy in…
    - Các công nghệ sử dụng: Wifi, HiperLAN và HiperLAN2
    - Chuẩn của công nghệ: IEEE 802.11
- WMAN (Wireless Metropolitan Area Network):

- Mạng không dây đô thị (WiMax): Phạm vi phủ sóng trong vòng vài Km, thường bao phủ cả một quận, huyện, khu dân cư, hay thành phố.
- Công nghệ sử dụng: WiMax
- Tốc độ truyền dữ liệu: 128 Mbps – 300 Mbps
- Mục đích phục vụ: Cung cấp mạng không dây trong đô thị.
- Chuẩn của công nghệ: IEEE 802.16

- WWAN (Wireless Wide Area Network):
  - Mạng không dây diện rộng: Công nghệ UMTS/GSM/CDMA2000.
  - Phạm vi phủ sóng là một khu vực rộng, một quốc gia, thậm chí toàn cầu.
  - Mạng 2,5G. 3G
- WRAN (Wireless Regional Area Network):
  - Mạng vô tuyến khu vực: Công nghệ IEEE 802.22
  - Phạm vi phủ sóng 40-100 Km.
  - Tốc độ 22 Mbps
  - Sử dụng các khoảng trắng trong phổ tần số TV, băng tần UHF, VHF 6/7/8Mhz
  - Mục đích truyền thông tới các vùng xa xôi hẻo lánh.

b. Các mô hình WLAN thông dụng:

❖ **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.
- Cách thiết lập:
    - Thiết bị: Card không dây
    - Trình điều khiển (Driver)
    - Tiện ích.
- Cấu hình:
    - Các Station phải cùng SSID: Service set identifier

❖ **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.
- Thiết bị AP có thể sẽ yêu cầu một trong những điều kiện sau, trước khi cho phép một máy trạm tham gia vào:
    - SSID phải giống nhau.
    - Một tốc độ truyền dữ liệu tương thích.
    - Hoàn tất vấn đề xác thực.

❖ **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

19. Các cơ chế an toàn cơ bản như: xác thực, kiểm soát truy cập, mã hóa trong mạng WLAN.

❖ Cơ chế xác thực

- Xác thực hệ thống mở:
    - 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.
- Xác thực khóa chung (Shared-key):
    - 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 sẻ 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.
- 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.

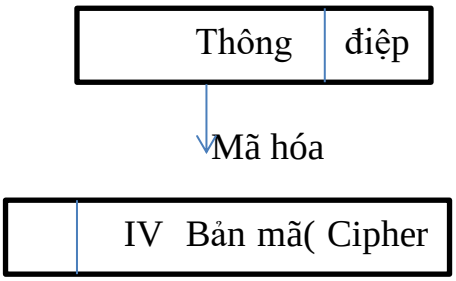
- Nếu không có RADIUS Server, có thể tạo ra một danh sách địa chỉ MAC trên AP.
- Vì các địa chỉ MAC được truyền dưới dạng văn bản, do đó có thể bằng cách dò sóng, những kẻ xâm nhập có thể tạo ra địa chỉ MAC hợp lệ truy cập vào mạng.

- 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 khóa WEP, Client sẽ sử dụng khóa này để bắt đầu phiên kết nối (KS).
  - Trong khi đó, RADIUS Server sẽ mã hóa và gửi khóa WEP đó được gọi là khóa phiên (KS) đến AP. AP sẽ sử dụng KS 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.
  - EAP là một cơ sở tốt cho xác thực và có thể được sử dụng cho một vài giao thức xác thực khác.
  - EAP-TLS – Extensible Authentication Protocol Transport Layer Security.
  - EAP-FAST – EAP Flexible Authentication via Secured Secured
  - EAP-SIM – EAP Subcriber Identity Module
  - Cisco LEAP – Lightweight Extensible Authentication Protocol
  - EAP-PEAP– EAP Protected Extensible Authentication Protocol
  - EAP-MD5 – EAP Message Digest Algorithm 5

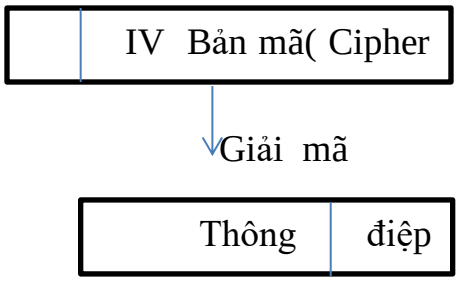
- EAP-OTP – EAP On Time Password
- EAP-TTLS – EAP Tunneled Transport Layer Security

❖ **Cơ chế 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.



Đóng gói và gửi thông điệp



Nhận và giải mã thông điệp

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

	WEP	WPA	WPA2
Mã hóa	RC4	RC4	AES
Luân phiên khóa	không	Khóa phiên động	Khóa phiên động
Phân phối khóa	Gán bằng tay trên mỗi thiết bị	Khả năng phân phối tự động	Khả năng phân phối tự động
Xác thực	Sử dụng khóa WEP để xác thực	Có thể dùng 802.1x & EAP	Có thể dùng 802.1x & EAP

❖ **Cơ chế kiểm soát truy cập**

- Kiểm soát dựa vào SSID:
    - SSID là thuật ngữ tên mạng, vì SSID được quảng bá mà không được mã hóa trong các Beacon nên rất dễ phát hiện.
    - Trong hệ thống xác thực đóng, người dùng phải khai báo đúng giá trị SSID để có thể xác thực và kết nối với mạng.
    - Sử dụng chế độ tắt quảng bá SSID để kiểm soát giá trị SSID.
- Kiểm soát dựa vào địa chỉ MAC:
    - Danh sách các địa chỉ MAC truy nhập ứng với thiết bị cho phép được thiết lập trên AP.
    - Khi thiết bị có địa chỉ MAC không nằm trong danh sách kết nối vào mạng sẽ bị ngăn chặn kết nối mạng.
- Kiểm soát dựa vào giao thức:
    - WLAN có thể lọc các gói tin truyền trên mạng dựa trên các giao thức lớp 2 đến lớp 7.
    - Các giao thức ứng với dịch vụ mạng sẽ bị cấm hoặc cho phép tùy thuộc vào địa chỉ MAC hoặc địa chỉ IP được cấp phát đến thiết bị người dùng

20. Giao thức xác thực bắt tay 4 bước trong WLAN. Phân tích ưu và nhược điểm của giao thức này.

a.Giao thức xác thực bắt tay 4 bước trong WLAN(giai đoạn 4)

- Bước 1: Authenticator(AP) tạo 1 giá trị ngẫu nhiên ANonce, sau đó gửi thông báo 1 có chứa ANonce sang cho Supplicant.
- Bước 2: Supplicant nhận thông báo 1 từ Authentication và xử lý thông điệp này, lấy ra ANonce và thwucj hiện hàm dẫn xuất để tạo ra khóa PTK theo công thức

PTK=SHA256-PRF(PMK, “Pairwise key expansion”,

Min(AA, SA)||Max(AA, SA)|| Min(ANonce, SNonce)|| Max(ANonce, SNonce))

"Pairwise key expansion" là nhãn sử dụng trong dẫn xuất

- AA(Authentication Address): Địa chỉ của AP, có độ dài 48bit
- SA(Supplicant Address): Địa chỉ của Supplicant, 48bit
- ANonce: Giá trị Nonce của Authenicator, 356bit

+ Tạo giá trị MIC cho thông báo 2, sử dụng khóa KCK

+ Gửi thông báo 2 có chứa ANonce và MIC

- Bước 3: Authenticator nhận thông báo 2 từ Supplicant và xử lý thông báo này, lấy ra SNonce và giá trị MIC. Tính giá trị PTK theo công thức

Min(AA, SA) || Max(AA, SA) || Min(ANonce, SNonce) || Max(ANonce, SNonce)

+ Sử dụng KCK, tính lại giá trị MIC cho thông điệp 2 để đảm bảo 2 bên có cùng PTK.

+ Sinh khóa nhóm GTK, kiến thiết thông điệp 3 và tạo MIC cho thông điệp này/ Mã hóa khóa GTK, sử dụng khóa KEK. Gửi thông điệp 3 có chứa khóa GTK đã mã hóa và MIC.

- Bước 4: Supplicant nhận thông báo 3 từ Authenticator và xử lý thông điệp này:
  - Kiểm tra tính toàn vẹn(MIC) của thông báo 3, sử dụng khóa KCK.
  - Sử dụng khóa KEK để giải mã thu được khóa GTK
  - Cài đặt các khóa PTK, GTK để mã hóa dữ liệu
  - Kiến thiết thông báo 4 chứa giá trị(ACK) +MIC và gửi thông báo 4 sang cho Authenticator.

+ Authenticator nhận thông báo 4, kiểm tra giá trị MIC. Nếu thành công, cài đặt PTK, GTK.

➔ Kết quả sau giai đoạn 4:

PTK SA :

- ✓ chung PTK gồm (KCK, KEK, TK)
- ✓ Thuật toán mã hóa
- ✓ Địa chỉ MAC của STA
- ✓ Địa chỉ MAC của AP

b)Ưu nhược điểm của giao thức xác thực bắt tay 4 bước

21. Trình bày các đặc điểm cơ bản (mã hóa, xác thực, toàn vẹn, khả năng chống tấn công phát lại) của giao thức WEP.

❖ Xác thực:

- Gồm hai loại xác thực: Xác thực mở và 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)
- 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.

❖ Toàn vẹn dữ liệu

- Sử dụng mã kiểm tra CRC-32
- Tính toàn vẹn trong WEP được bảo vệ bằng giá trị CRC (Cyclic Redundancy Check) được mã hóa
- Giá trị ICV được tính toán và được gắn vào thông điệp
- Cả thông điệp và ICV được mã hóa cùng nhau
  - ICV 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 dũ liệu
  - Vì máy gửi tạo ra ICV không theo định luật hay tiêu chuẩn, IV bắt buộc phải được gửi đến máy nhận ở dạng không mã hóa

❖ Mã hóa

- Sử dụng RC4, Khóa dài 40 bit, hoặc 104 bit
- Sử dụng IV dài 24 bit

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).
- 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

❖ 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

22. Trình bày các đặc điểm cơ bản (mã hóa, xác thực, toàn vẹn, khả năng chống tấn công phát lại) của giao thức 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

❖ 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.

23. Trình bày các đặc điểm cơ bản (mã hóa, xác thực, toàn vẹn, khả năng chống tấn công phát lại) của giao thức WPA2.

❖ 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)

❖ 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

24. Các tấn công phổ biến vào mạng 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.

– 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.

❖ Tấn công chủ động : Kẻ tấn công sử dụng các kỹ thuật làm ảnh hưởng tới mạng.

– Là hình thức tấn công tác động trực tiếp lên thông tin, dữ liệu của mạng.

- Dò tìm mật khẩu AP :

  + Vét cạn (WPS - Wifi Protected Setup)

  + Tấn công từ điển

- Giả mạo AP:kẻ tấn công có thể sao chép tất cả các thông tin về AP hợp pháp như địa chỉ MAC, SSID,… để giả mạo AP hợp pháp. Gửi các gói beacon với địa chỉ vật lý (MAC) giả mạo và SSID giả để tạo ra vo số AP giả mạo.
- Tấn công người đứng giữa
- Từ chối dịch vụ
  + Làm ngắt kết nối: kẻ tấn công gửi liên tục các frame hủy kết nối bằng cách giả mạo địa chỉ MAC nguồn và đích của AP đến Client. Client nhận được frame này sẽ ngắt kết nói
  + Chèn ép tín hiệu: sử dụng bộ phát tín hiệu RF (radio frequency) công suất cao làm nghẽn hoặc nhiễu tín hiệu RF của các AP hợp pháp

25. Độ an toàn, ưu, nhược điểm của các giao thức WEP, WPA, WPA2.

❖ **WEP**

a) Độ an toàn

- Giao thức mã hóa yếu

- WEP có thể được coi như một cơ chế bảo mật ở mức độ thấp nhất, vì vậy WEP không cung cấp độ bảo mật cần thiết cho đa số các ứng dụng không dây cần độ an toàn cao. WEP có thể bị bẻ khóa dễ dàng bằng các công cụ sẵn có.

b) Ưu điểm

- Sinh khóa trên mỗi gói tin bằng cách ghép nối IV trực tiếp với khóa chia sẻ trước

c) Nhược điểm (Yếu điểm)

- Về vấn đề xác thực:

- Xác thực chỉ là một chiều

+ AP không được xác thực bởi STA

+ STA có thể gắn kết với một AP giả mạo: cùng 1 khóa chia sẻ giống nhau được dung cho cả mã hóa và xác thực

➔ Điểm yếu này có thể được dung 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 địa chỉ MAC của STA đó

+ Việc phát lại các thông điệp của STA vẫn có thể xảy ra.

- **Về vấn để toàn vẹn dữ liệu:** Sử dụng mã kiểm tra CRC-32
- **Về vấn đề mã hóa:** Sử dụng mã hóa yếu RC4, độ dài khóa 40bit hoặc 104 bít

Sử dụng IV có độ dài 24 bít(cỡ 17tr giá trị có thể của IV, nếu một STA có thể tr trung bình 500 frame(có độ dài tối đa trong một giây thì số lượng IV này sẽ sư dụng được trong khoảng 7h, IV sẽ bị lặp lại sau mỗi 7h).

- **Vấn đề về khóa:** Sử dụng khóa chia sẻ trước, không có trao đổi khó 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:** WEP không được thiết kế để chống tấn công phát lại

❖ **WPA**

Độ an toàn

- Phân phối khóa hiệu quả
- Giới thiệu giao thức TKIP cải tiến so với WEP

+ Xác thực mạnh với 802.1x và EAP

+ Tăng độ dài IV và độ dài khóa mã là 104 bít

+ Sử dụng thuật toán toàn vẹn Michael

Ưu điểm

- Giải quyết được các vấn đề của WEP bằng cách giới thiệu khái niệm PTK trong kiến trúc khóa và sử dụng hàm dẫn xuất khóa thay vì ghép nối khóa trực tiếp để tạo khóa cho mỗi gói tin.

Nhược điểm

- Chia sẻ khóa trước: WPA vẫn sử dụng chế độ chia sẻ khóa trước, dễ bị tấn công.
- Toàn vẹn dữ liệu: Sử dụng thuật toán Michael- 64 bit để xác thực, chỉ tốt hơn mã kiểm tra CRC32
- Mã hóa: Sử dụng mã hóa yếu RC4

❖ **WPA2**

Độ an toàn

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)

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)WPA2 (802.11i)

Ưu điểm

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)WPA2 (802.11i)

Nhược điểm

26.So sánh sự khác nhau giữa ba giao thức WEP- WPA- WPA2/ WEP-WPA.

So sánh WEP- WPA- WPA2

	WEP	WPA	WPA2
Mã hóa	RC4	RC4 với TKIP	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 khá WEP	Có thể dung 802.1x & EAP	Có thể dung 802.1x & EAP

So sánh WEP- WPA- 802.11i

	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	Trao đổi khóa tự động, mặc định 600s trao đổi lại PTK và GTK, 1 ngày trao đổi lại PMK và GMK

		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 bít mã hóa, 64 bít 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
Toanf vẹn cho phần Header	CRC-32	Địa chỉ nguồn-đích được bảo vệ bởi thuật toán Michael	Toàn vẹn theo CBC-MAC
Toàn	CRC-	Mã	Toàn vẹn theo CBC-MAC

vẹn dữ liệu	32	MIC- sử dụng thuật toán Michael	
Replay	Không	Có	Có

So sánh WEP- WPA- WPA2

WEP	WPA	WPA2
Là thành phần tùy chọn trong tiêu chuẩn IEEE 802.11	Tiêu chuẩn an ninh của wifi alliance đặt ra	Tương tự WPA
Khóa WEP đc cấu hình thủ công trên AP và các STA	Khuyến nghị nên sd xác thực 802.1X/EAP để nhận khóa tự động, có hỗ trợ cài đặt thủ công như WEP	Tương tự WPA
Sử dụng mã hóa dòng	Tương tự WEP	Sử dụng mã hóa khối, có hỗ trợ mã hóa dòng
Mã hóa trên từng gói tin dựa vào sự thay đổi giá trị IV, giá trị đc kết hợp trực tiếp với PMK để hình	Sd phương pháp mã hóa liên tiếp và phức tạp hơn, qt tạo khóa có thông qua khóa trung gian PTK	Tương tự WPA

thành khóa		
Độ dài khóa nhỏ, 64 bít hoặc 128 bit	Độ dài khóa lớn, kết hợp nhiều thành phần thông tin để sinh khóa	Tương tự WPA
Sd thuật toán CRC để ktra tính toàn vẹn dl, độ tin cậy thấp	Sd thuật toán Michael để tính toán ra mã MIC. Độ tin cậy cao hơn CRC	Sd CCMP/AES để tính mã MIC, độ tin cậy cao nhất
K có khả năng xác thực 2 chiều	Hỗ trợ khả năng xác thực 2 chiều, sd IEEE 802.1X/EAP	Tương tự WPA
Phương pháp đơn giản, k yc cao về năng lực phần cứng	Phức tạp hơn WEP nhưng cũng k yc cao về phần cứng	Phức tạp, yc cao về năng lực xử lý của phần cứng
Thích hợp vs mạng quy mô nhỏ	Phù hợp mạng quy mô nhỏ và trung bình	Thiwchs hợp với mạng quy mô lớn và các doanh nghiệp

So sánh 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 la,f tươi khóa cho mỗi phiên liwwn lạc, làm tăng không gian khóa. IV đươuọc đặt về 0 mỗi khi thiết lập một PTK mới.
Thuật toán khóa vẹn dữ liệu là CRC32, không xác thực header	Thuật toán toàn vẹn dữ liệu 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 mạng STA xác thực mạng WLAN	Sử dụng 802.1x và EAP cho phép xác thực hai chiều.

27. Bổ sung

Các nâng cấp của TKIP để khắc phục điểm yếu của WEP

Điểm yếu	Nâng cấp
Sự tương quan của các IV với các khóa yếu	Hàm trộn khóa cho môi gói tin
Tấn công phát lại	Đánh số thứ tự IV
Dễ bị giả mạo	MIC