



BÀI GIẢNG MÔN

An ninh mạng thông tin

TEL1401

Giảng viên:

TS. Phạm Anh Thư

Điện thoại/E-mail:

0912528188

thupa80@yahoo.com, thupaptit@gmail.com

Bộ môn:

Mạng viễn thông - Khoa Viễn thông 1

Học kỳ/Năm biên soạn: I/ 2022-2023



An toàn mạng Internet

- ❖ Mạng Internet hiện nay được sử dụng rộng rãi bởi mọi đối tượng
- ❖ Tuy nhiên, mạng Internet lại có rất nhiều nguy cơ thiếu an toàn
 - Tính bảo mật
 - Tính toàn vẹn
 - Tính xác thực
 - Tấn công DoS
- ❖ Rất cần các cơ chế an toàn

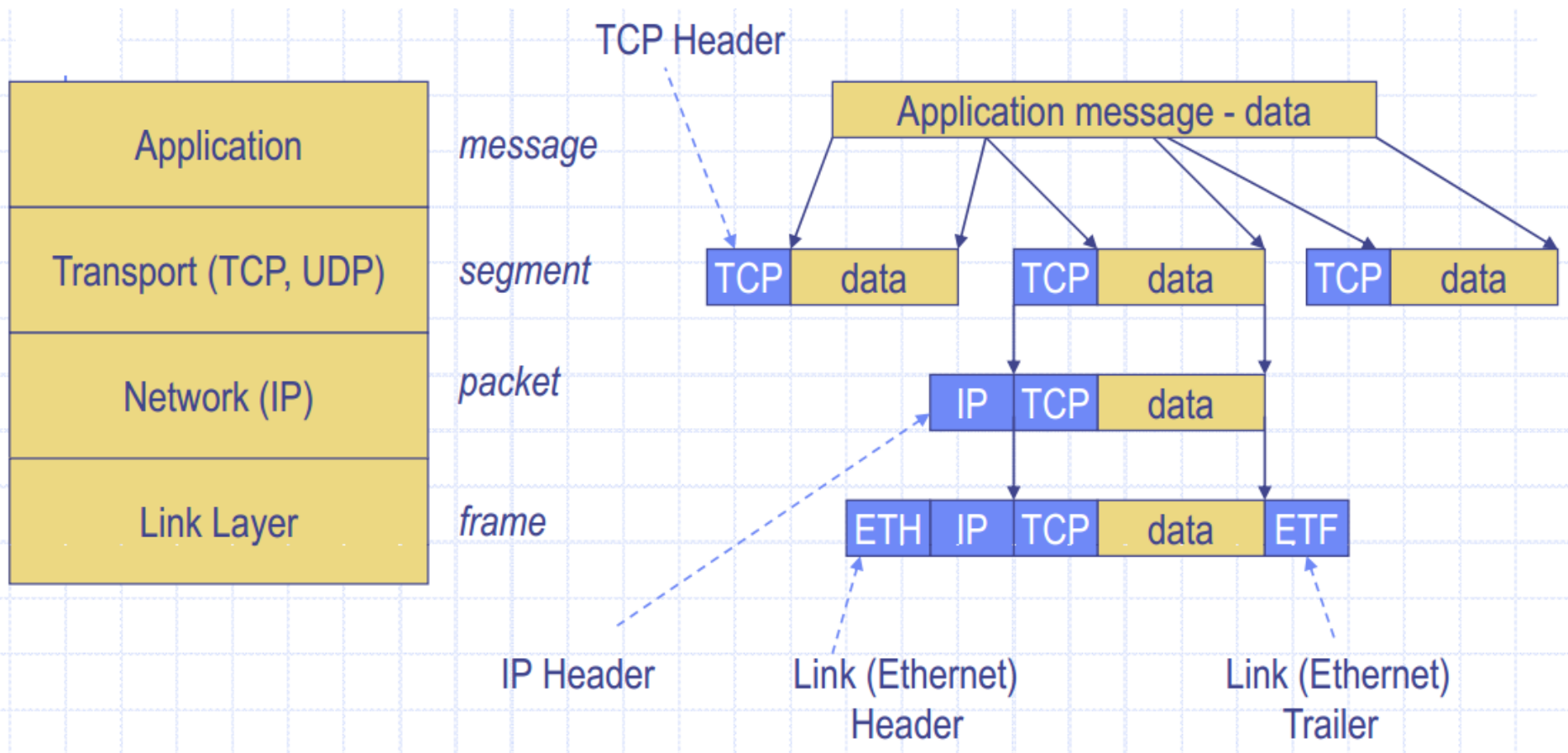


An toàn mạng Internet

- ❖ Mục tiêu của an toàn thông tin trên mạng Internet là làm sao bảo vệ được tính toàn vẹn và bảo mật thông tin từ bên gửi đến bên nhận khi được truyền qua mạng.
- ❖ Các khía cạnh cần đảm bảo an toàn:
 - **Xác thực:** xác thực người dùng và đảm bảo tính toàn vẹn của dữ liệu
 - **Bảo mật:** đảm bảo dữ liệu không bị tấn công trong quá trình truyền
 - **Lựa chọn các tham số an ninh tốt nhất và quản lý khóa tốt nhất:** lựa chọn các thuật toán mật mã phù hợp, cung cấp giải pháp phân loại các vấn đề nảy sinh khi người dùng sử dụng nhiều cặp khóa bí mật/công khai

An toàn mạng Internet

- Mô hình truyền dữ liệu trên mạng Internet





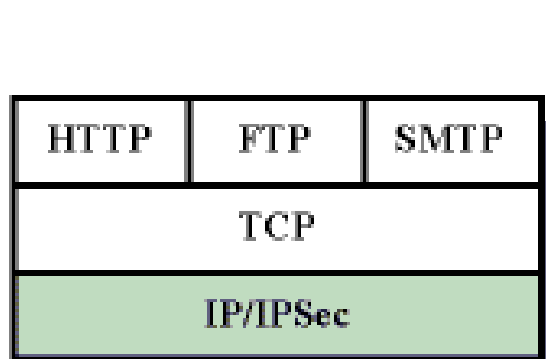
An toàn mạng Internet

- An toàn thông tin được cung cấp qua các lớp của mạng Internet

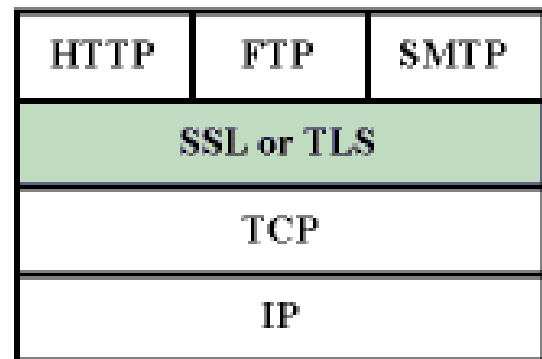
Communication layers	Security protocols
Application layer	ssh, S/MIME, PGP
Transport layer	SSL, TLS, WTLS
Network layer	IPsec MPLS
Data Link layer	PPTP, L2TP
Physical layer	Scrambling, Hopping, Quantum Communications

An toàn mạng Internet

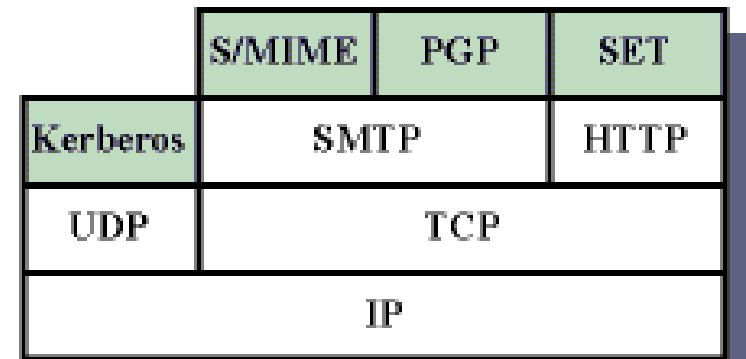
- Các giải pháp an toàn được thực hiện trên các lớp khác nhau:



(a) Network Level



(b) Transport Level



(c) Application Level

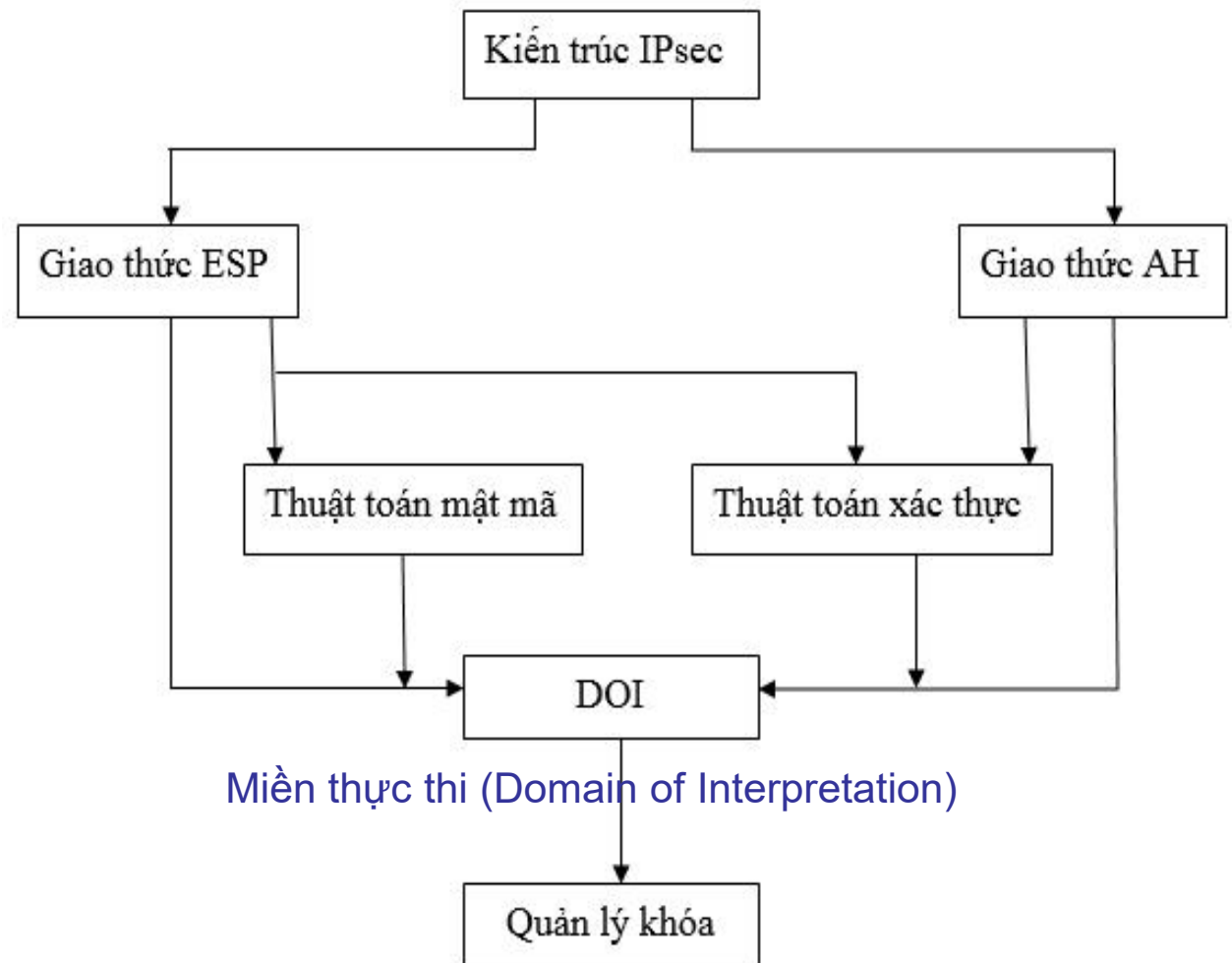


IPSec

- IPSec (Internet Protocol Security): gồm hệ thống các giao thức (AH, ESP và IKE) để bảo mật quá trình truyền thông tin trên nền tảng giao thức IP.
- IPSec có thể cung cấp cả tính bảo mật và xác thực cho mỗi gói IP trong quá trình trao đổi dữ liệu dựa trên hai giao thức:
 - AH (authentication header): cung cấp dịch vụ xác thực,
 - ESP (encapsulation security payload) : cung cấp dịch vụ bảo mật và dịch vụ xác thực

IPSec

- Kiến trúc của IPSec





IPSec

- ❖ AH (authentication header):
 - Cung cấp tính xác thực và toàn vẹn của gói tập tin chuyển đi
 - Xác thực được thực hiện nhờ MAC (mã xác thực bản tin)
- ❖ ESP (encapsulation security payload) :
 - Cung cấp dịch vụ bảo mật và xác thực dữ liệu;
 - Tính bảo mật dữ liệu được cung cấp thông qua mã hóa khóa đối xứng, dùng DES hoặc AES.



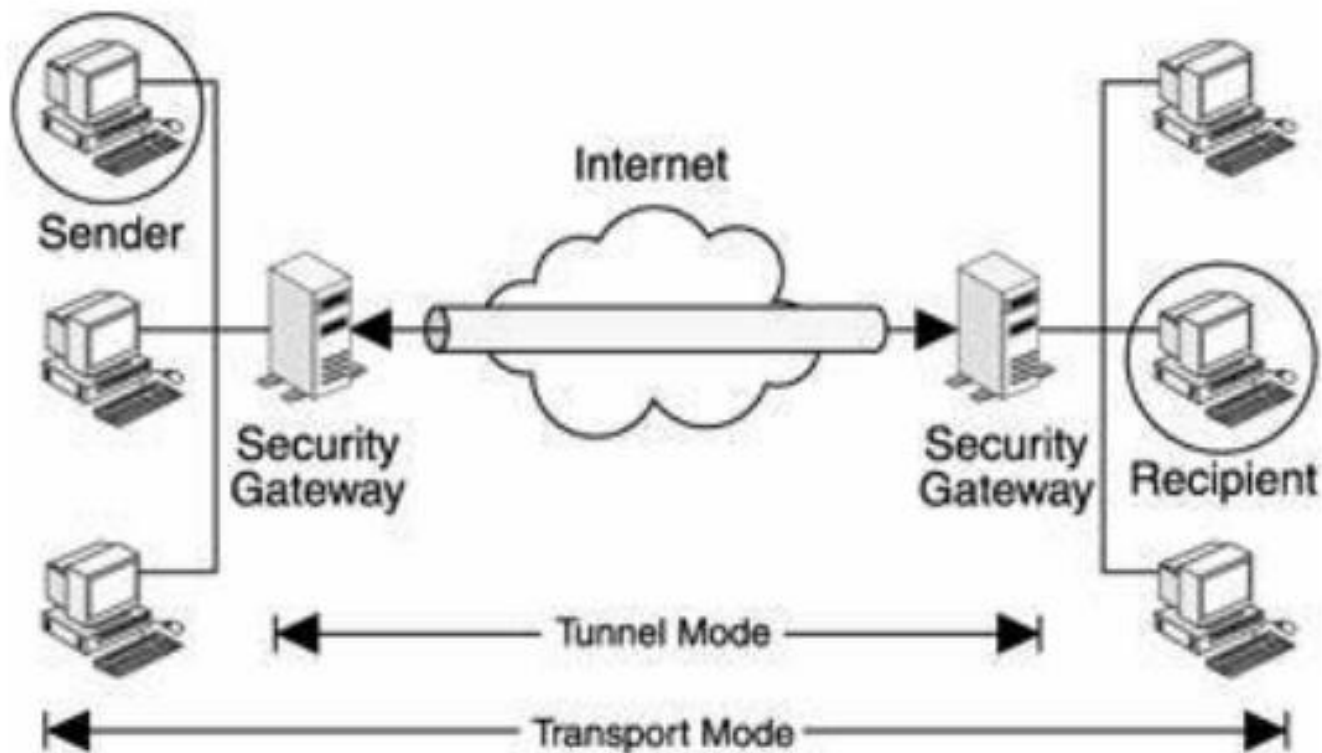
IPSec

- Có hai chế độ hoạt động:

- Chế độ vận chuyển (Transport): các máy chủ nguồn và đích phải trực tiếp thực hiện tất cả các thao tác mã hoá. Phương thức hoạt động này thiết lập tính an toàn từ đầu đến cuối đường truyền.
- Chế độ đường hầm (Tunnel): các gateway thực hiện quá trình xử lý mật mã chứ không phải các máy chủ nguồn và đích. Nhiều 'đường hầm' được tạo ra giữa các cổng kết nối gateway, thiết lập an ninh theo dạng gateway-to-gateway.

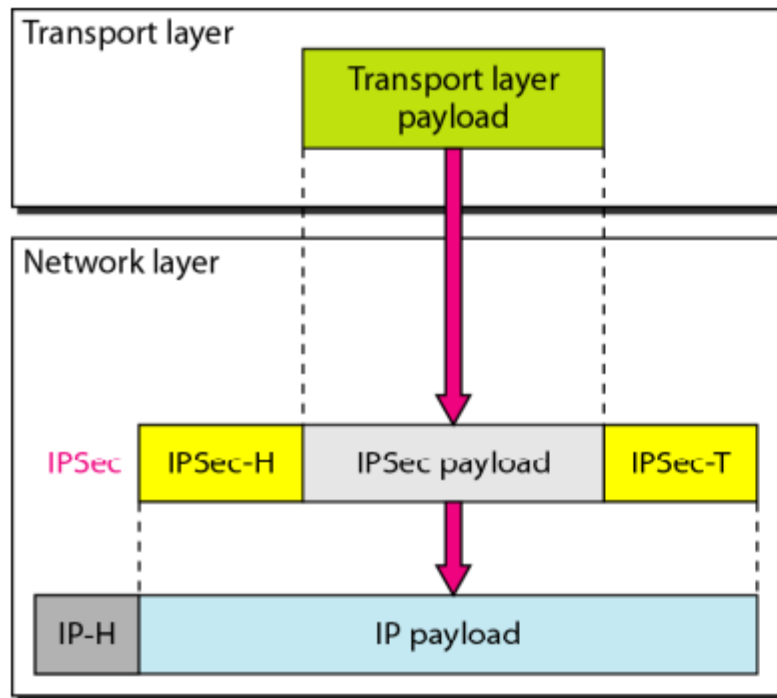
IPSec

- Hai chế độ hoạt động của IPSec:

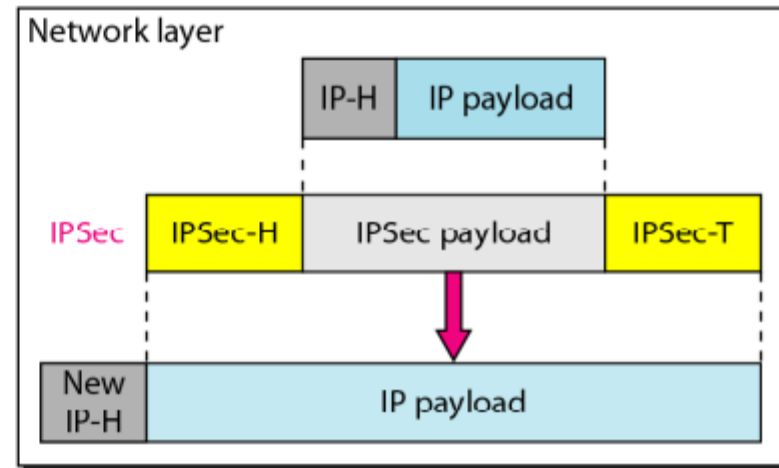


IPSec

- IPSec Tunnel mode and transport mode



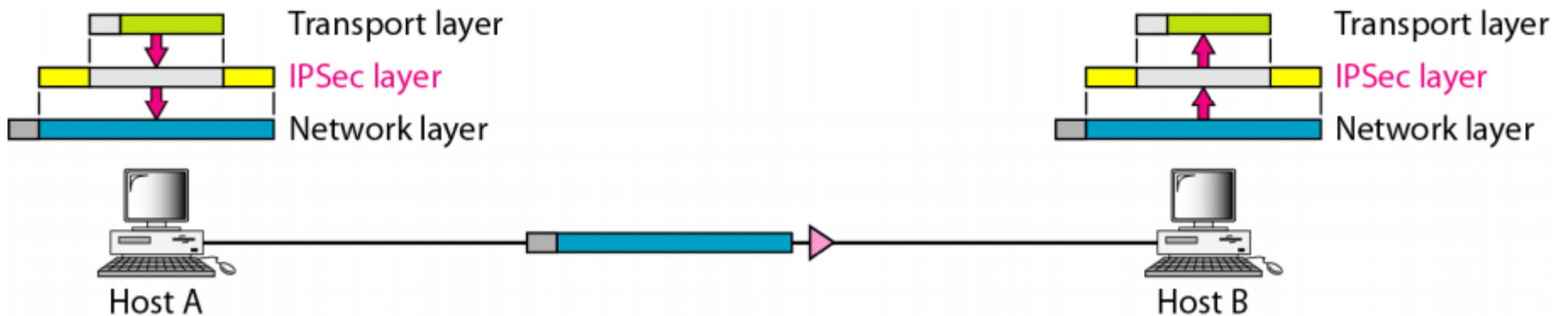
a. Transport mode



b. Tunnel mode

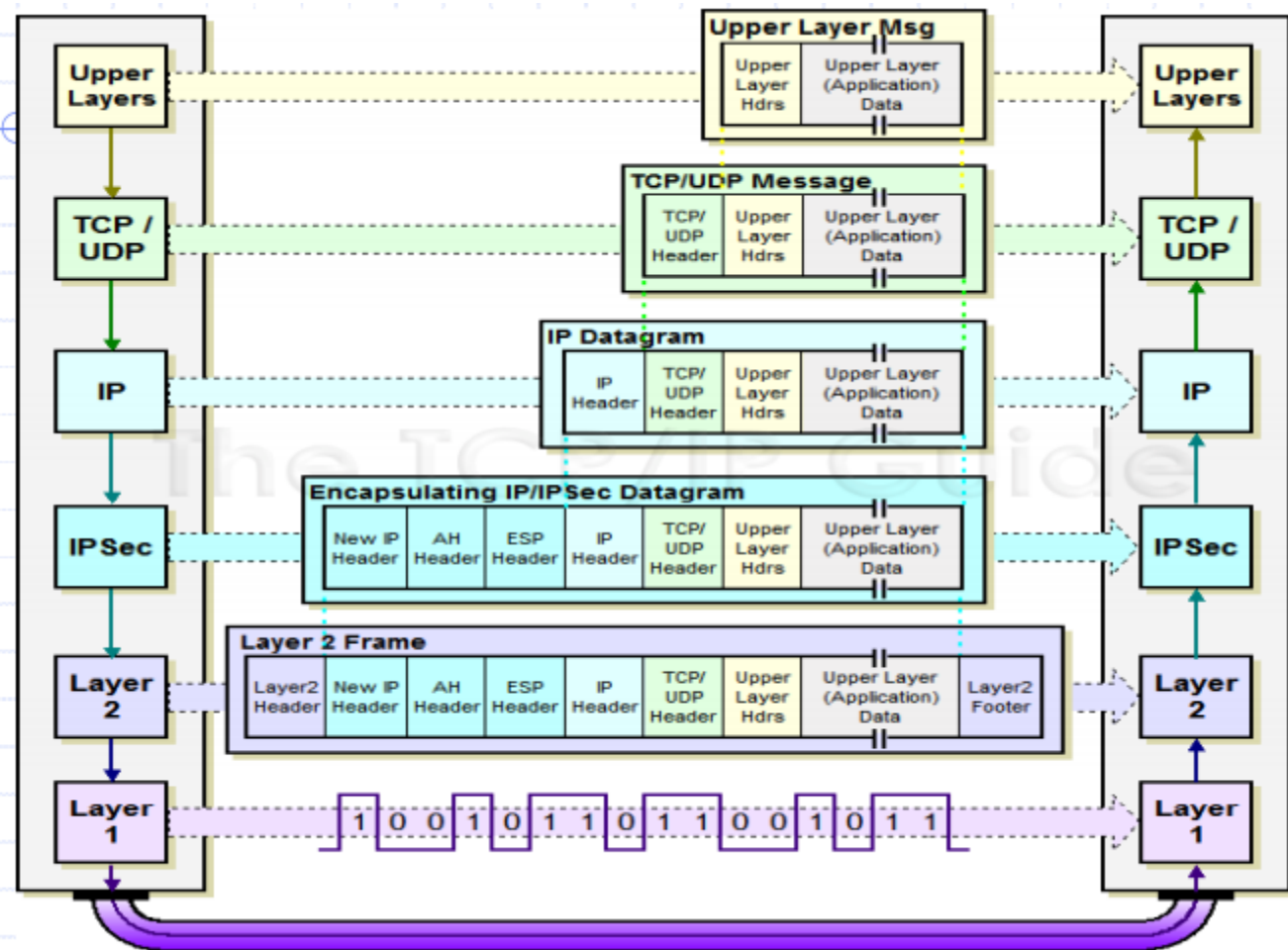
IPSec

- **IPSec Transport mode:** IPSec header được sử dụng thay thế cho IP header



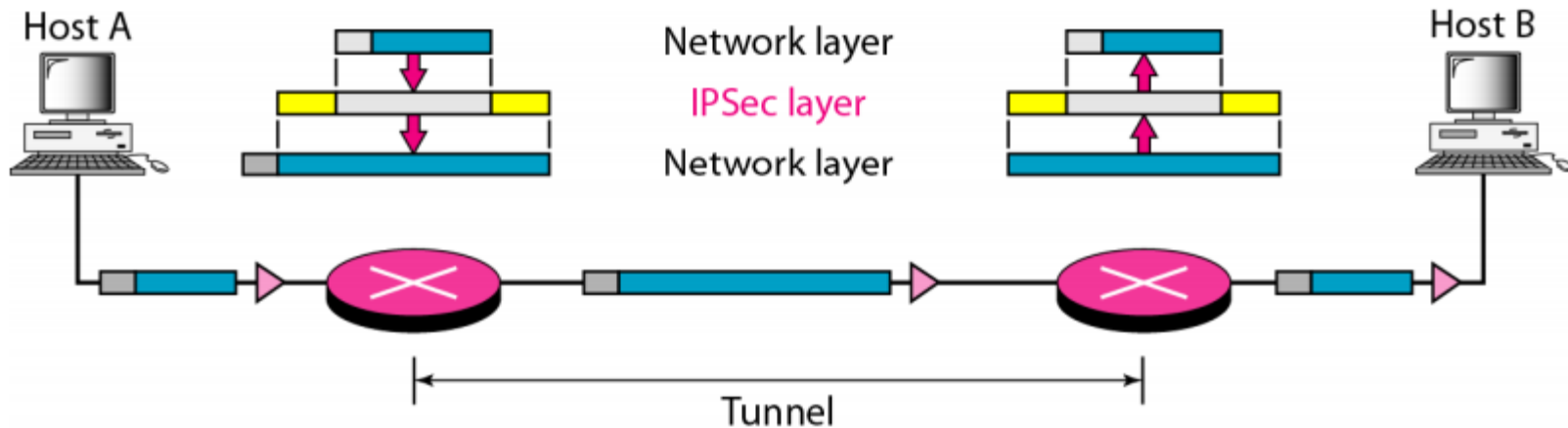
IPSec

- **IPSec Tunnel mode:**
- Tồn tại cả IP header và IPSec header



IPSec

- **IPSec Tunnel mode:** Tồn tại cả IP header và IPSec header





Giao thức AH

- Cung cấp xác thực nguồn, toàn vẹn dữ liệu, không bảo mật.
- AH header được chèn vào giữa mào đầu gói IP (IP header), và trường dữ liệu.
- Protocol field: 51
- Các router trung gian xử lý gói tin như thông thường.

AH header bao gồm:

- Định danh kết nối
- Dữ liệu xác thực: tóm tắt bản tin nguồn được tính từ IP datagram nguồn.
- Trường mào đầu tiếp sau (next header field): xác định dạng của dữ liệu (e.g., TCP, UDP, ICMP)

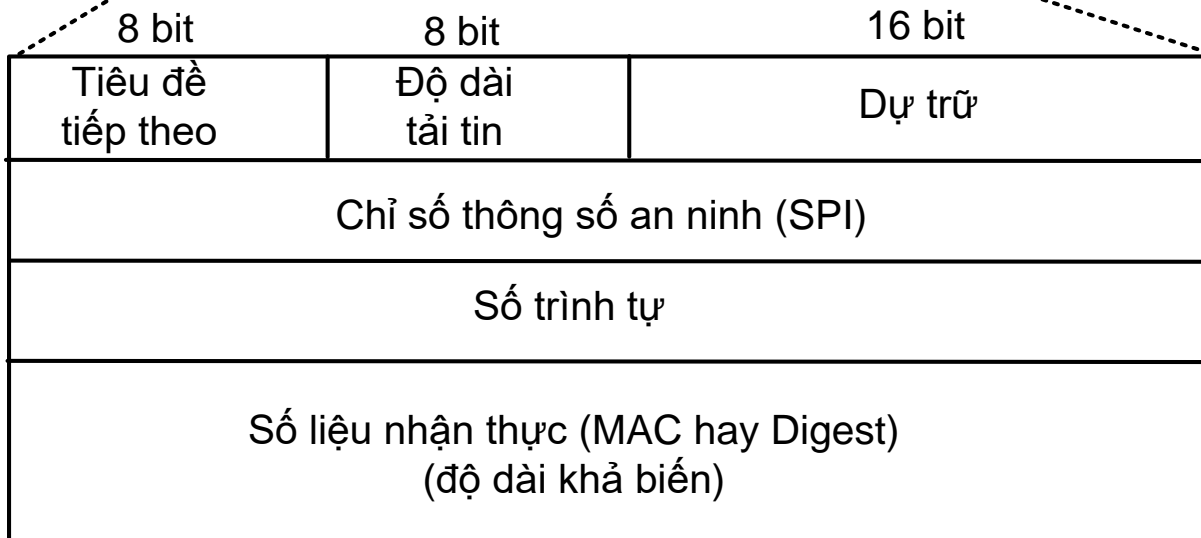
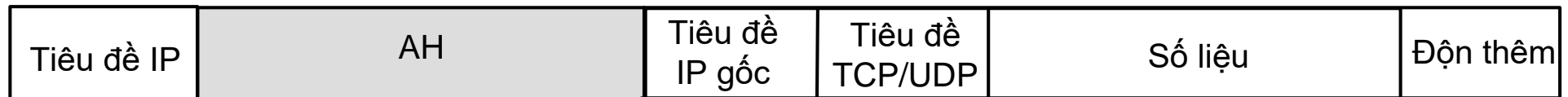
IP header

AH header

data (e.g., TCP, UDP segment)

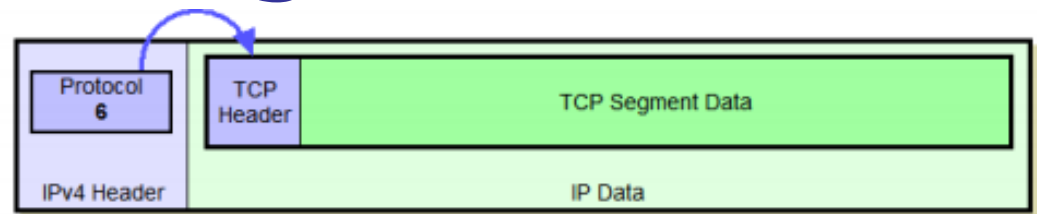
Giao thức AH trong IPSec

Số liệu được sử dụng để tính toán MAC cho nhận thực
(trừ các trường trong tiêu đề IP thay đổi trong truyền dẫn)

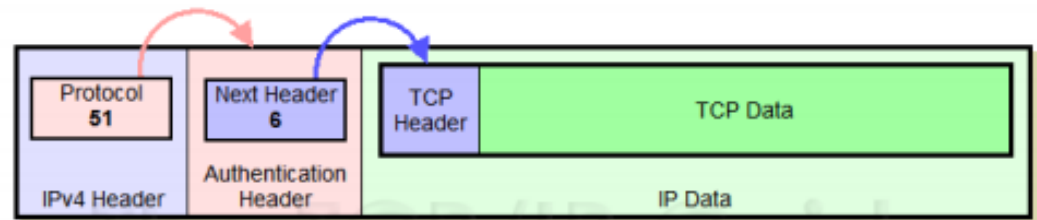


Giao thức AH trong IPSec

- Mối quan hệ giữa gói tin IPv4 ban đầu và gói tin sử dụng giao thức AH trong hai chế độ transport và tunnel

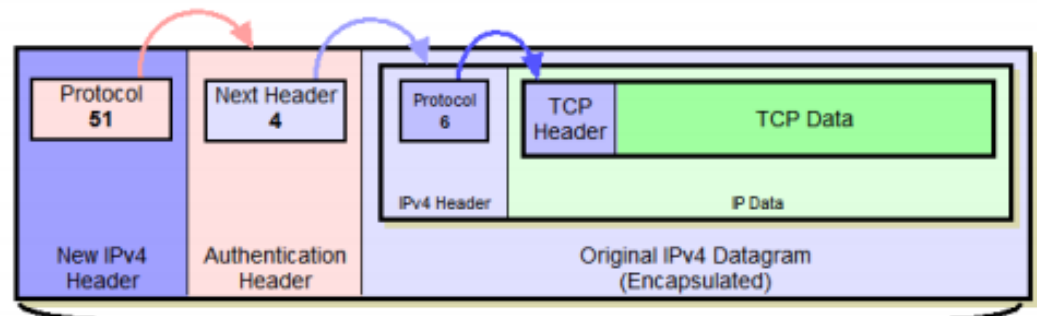


Original IPv4 Datagram Format



Authenticated Fields

IPv4 AH Datagram Format - IPSec Transport Mode



Authenticated Fields

IPv4 AH Datagram Format - IPSec Tunnel Mode

Giao thức AH trong IPSec

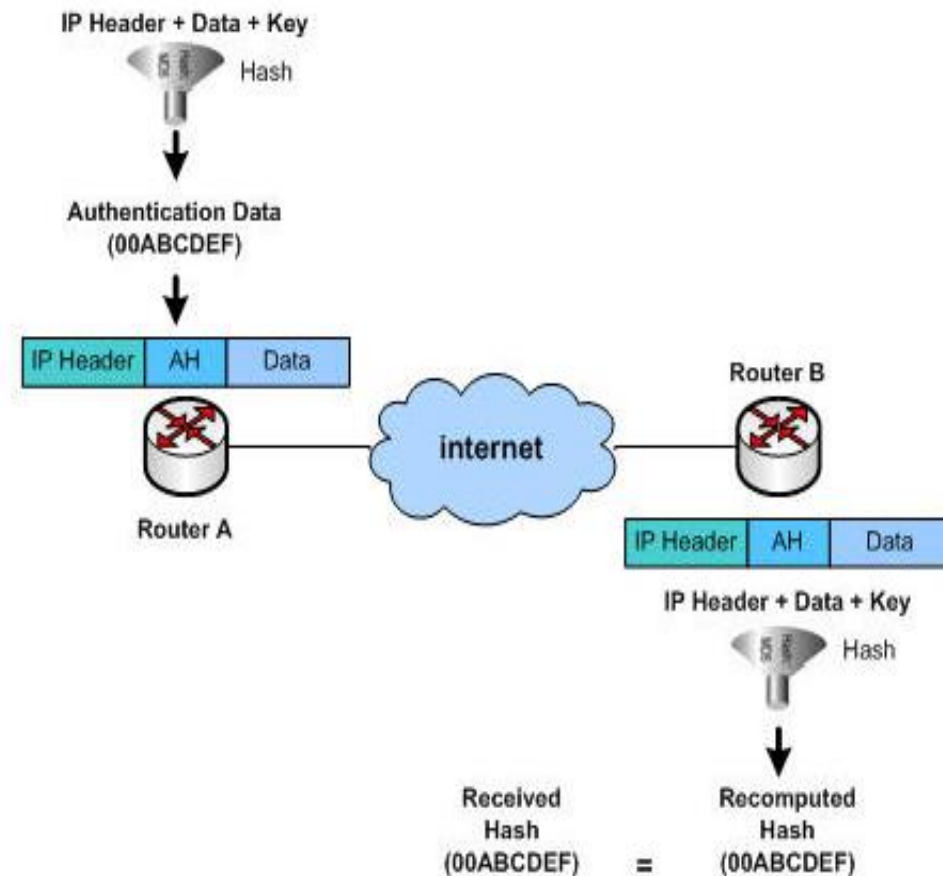
Hoạt động:

+ **B1:** AH sẽ đem gói dữ liệu (packet) bao gồm : Payload + IP Header + Key cho chạy qua giải thuật Hash 1 chiều và cho ra 1 chuỗi số, và chuỗi số này sẽ được gán vào AH Header.

+ **B2:** AH Header này sẽ được chèn vào giữa Payload và IP Header và chuyển sang phía bên kia.

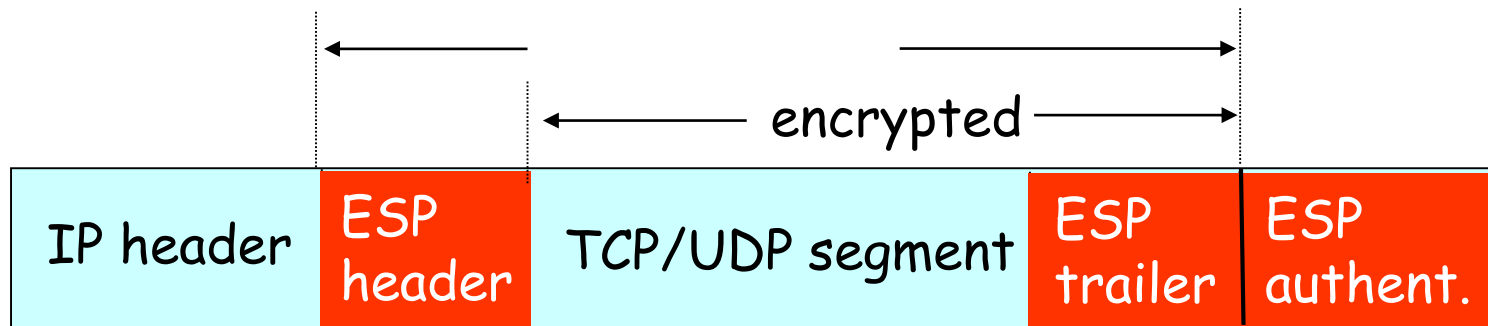
+ **B3:** Router đích sau khi nhận được gói tin này bao gồm : IP Header + AH Header + Payload sẽ được cho qua giải thuật Hash một lần nữa để cho ra một chuỗi số.

+ **B4:** so sánh chuỗi số nó vừa tạo ra và chuỗi số của nó nếu giống nhau thì nó chấp nhận gói tin



Giao thức ESP

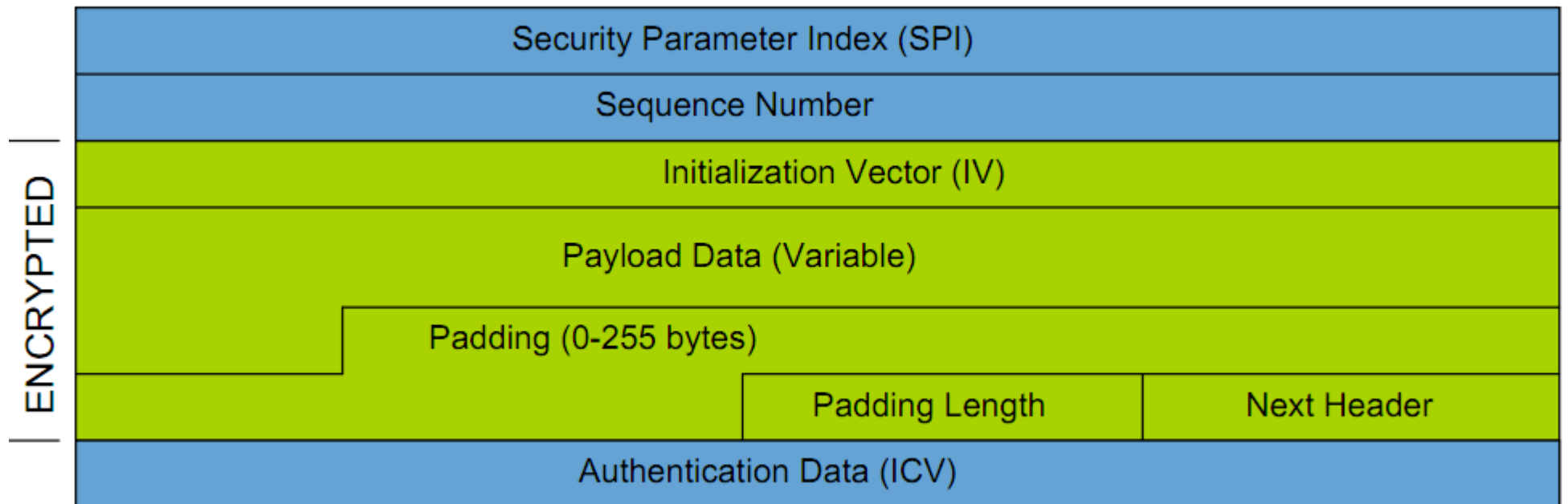
- Cung cấp tính bí mật, toàn vẹn và xác thực máy chủ.
- Dữ liệu, đuôi ESP được mã hóa.
- Trường xác thực ESP tương tự như trường xác thực của AH.



Giao thức ESP

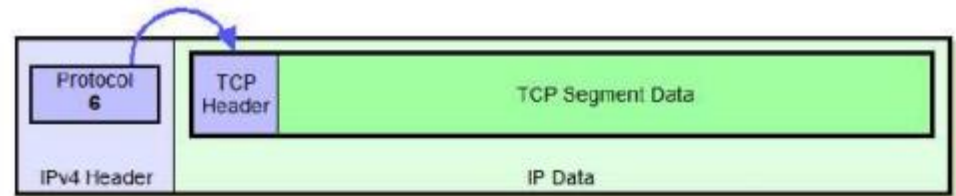
- Định dạng mào đầu ESP

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31

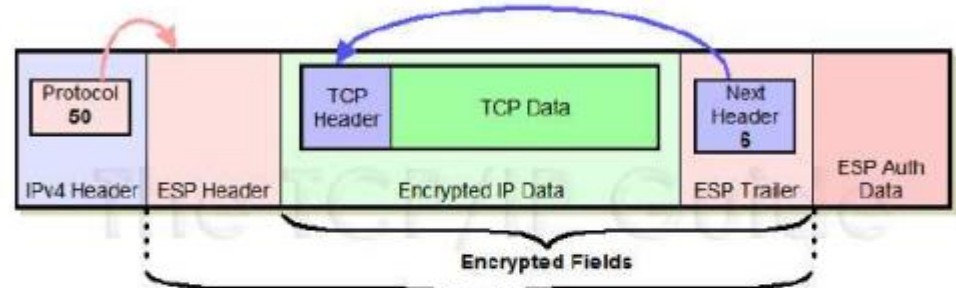


Giao thức ESP

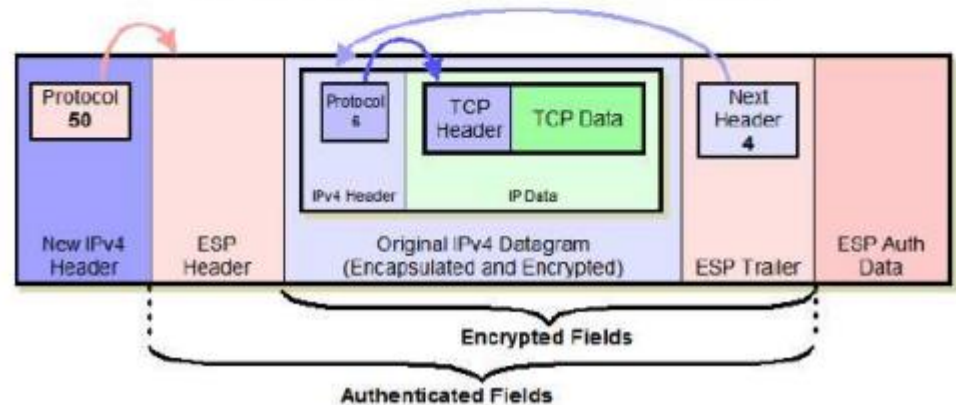
- Mối quan hệ giữa gói tin IPv4 ban đầu và gói tin sử dụng giao thức ESP trong hai chế độ transport và tunnel



Original IPv4 Datagram Format



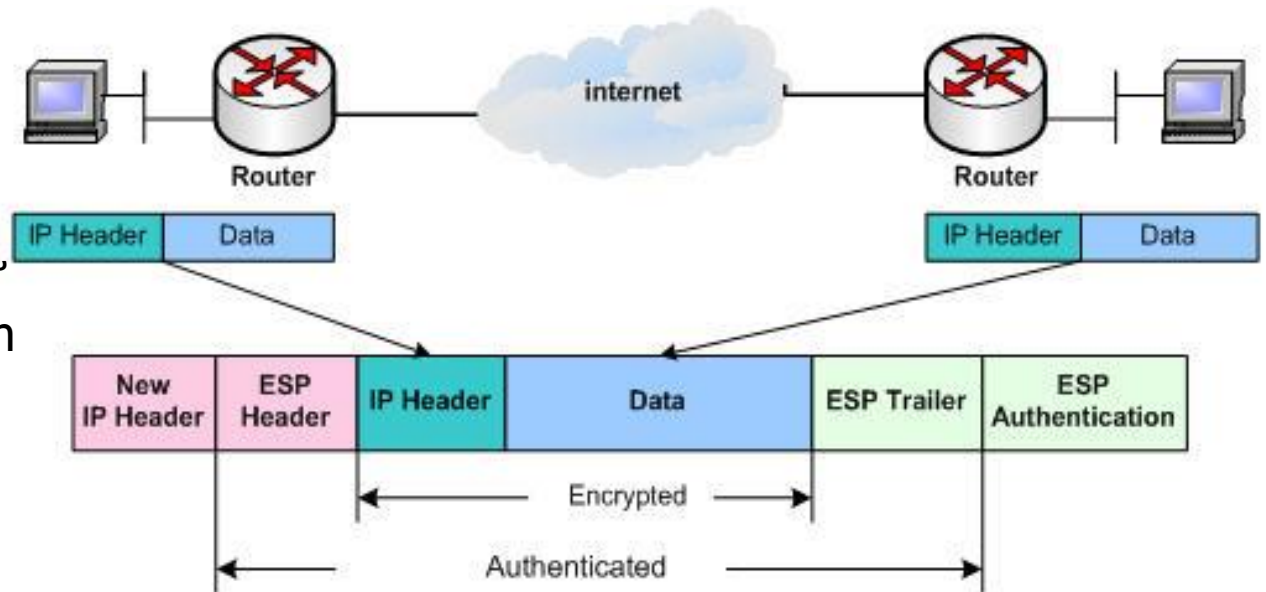
IPv4 ESP Datagram Format - IPsec Transport Mode



IPv4 ESP Datagram Format - IPsec Tunnel Mode

Giao thức ESP

- ESP sử dụng mật mã đối xứng để cung cấp sự mật hoá dữ liệu cho các gói tin IPSec.
- Khi một đầu cuối mã hoá dữ liệu, nó sẽ chia dữ liệu thành các khối (block) nhỏ, và sau đó thực hiện thao tác mã hoá nhiều lần sử dụng các block dữ liệu và khóa (key).
- Khi một đầu cuối khác nhận được dữ liệu mã hoá, nó thực hiện giải mã sử dụng key giống nhau và quá trình thực hiện tương tự, nhưng trong bước này ngược với thao tác mã hoá.

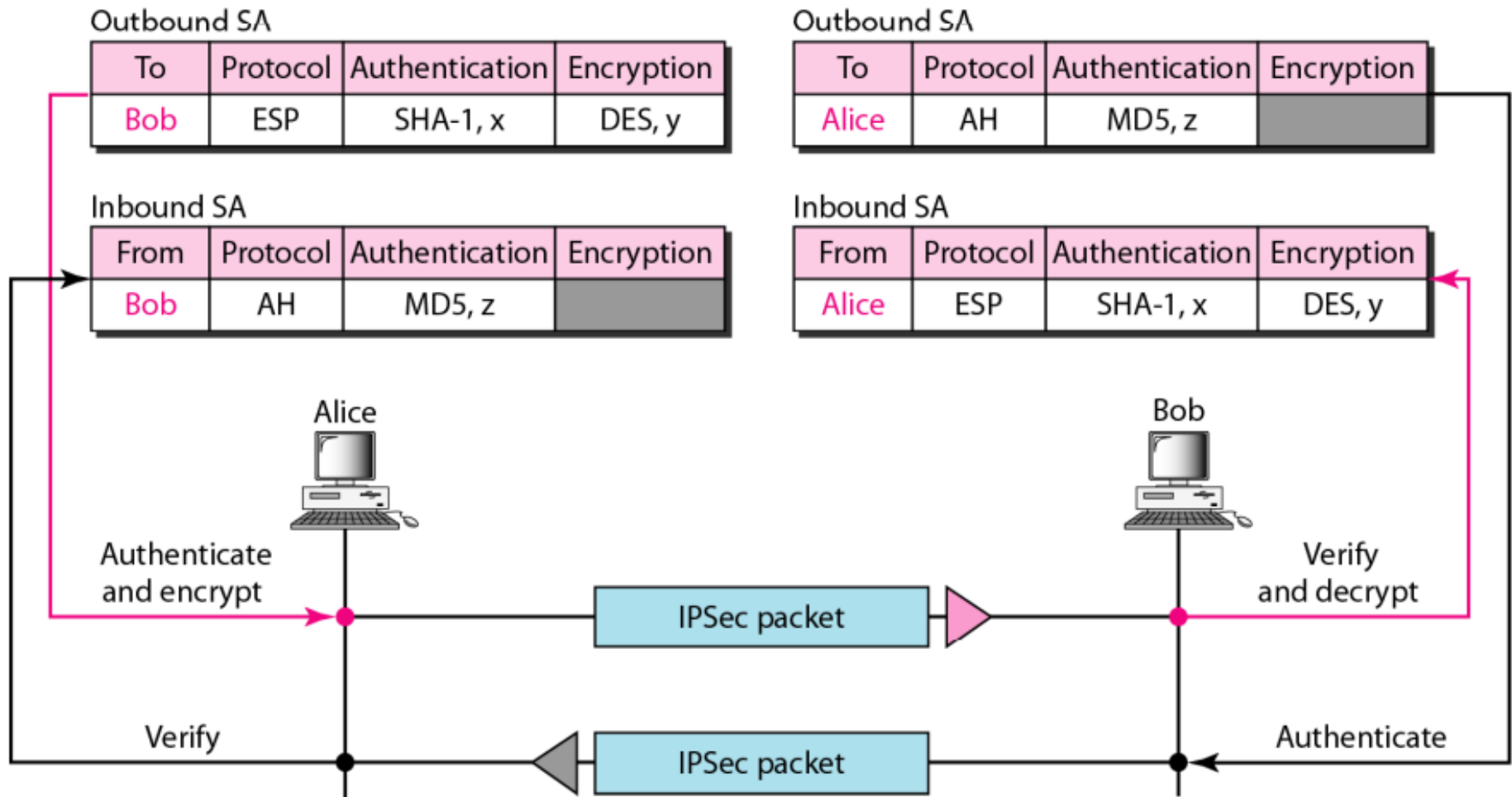




So sánh AH và ESP

<i>Services</i>	<i>AH</i>	<i>ESP</i>
Access control	Yes	Yes
Message authentication (message integrity)	Yes	Yes
Entity authentication (data source authentication)	Yes	Yes
Confidentiality	No	Yes
Replay attack protection	Yes	Yes

Simple inbound and outbound security associations





Trao đổi khóa IKE – Internet Key Exchange

- ❖ IKE thiết lập tự động các SA cho IPSec
- ❖ Mô tả trong RFC 4306
- ❖ Mỗi thực thể IPSec có chứng thư, bao gồm khóa công khai
- ❖ Gồm 2 pha:
 - Phase 1: thiết lập IKE SA
 - Phase 2: thiết lập IPSec SA



IKE – thiết lập IKE SA

- ❖ Trao đổi bản tin đầu tiên: Hai router sử dụng Diffie-Hellman mở IKE SA 2 chiều - tạo kênh mã hóa và xác thực giữa 2 router (khóa IKE SA) và master key cho IPSec SA;
- ❖ Trao đổi bản tin thứ hai: 2 router thông báo định danh bằng ký bản tin trên kênh IKE SA; 2 bên thỏa thuận thuật toán mã hóa và xác thực IPSec SA.



IKE – thiết lập IPSec SA

- ❖ Hai bên tạo SA trên mỗi phía: tạo khóa phiên mã hóa và khóa phiên xác thực cho SA tại mỗi bên;
- ❖ Sử dụng SA trao đổi bản tin an toàn.



SSL/TLS

(Secure Socket Layer/– Transport Layer Security)

- Cung cấp an toàn lớp giao vận cho tất cả các ứng dụng trên TCP.
 - Ví dụ giữa các trình duyệt Web (browsers) và các máy chủ thương mại điện tử (e-commerce), giữa email clients với các máy chủ mail.
- Các dịch vụ an toàn:
 - Xác thực máy chủ (server authentication), máy khách (client authentication).
 - Bảo mật dữ liệu: sử dụng mật mã
 - Tính toàn vẹn dữ liệu: sử dụng MAC
- TLS là SSL ver 3



SSL/TLS

- ❖ Vấn đề đảm bảo bảo mật:

- Mã hóa các thông điệp truyền đi
- Sử dụng các thuật toán DES, 3DES, RC2, RC4

- ❖ Vấn đề trao đổi khóa:

- Sử dụng hệ mật mã khóa công khai để trao đổi khóa bí mật
- Mật mã thường dùng là RSA hoặc Diffie-Hellman



SSL/TLS

- ❖ Vấn đề đảm bảo tính toàn vẹn

- Tính MAC
- Truyền MAC cùng với thông điệp
- Bên nhận tính lại MAC và so sánh với MAC nhận được
- Sử dụng hàm băm MD5 và SHA-1

- ❖ Vấn đề đảm bảo tính xác thực:

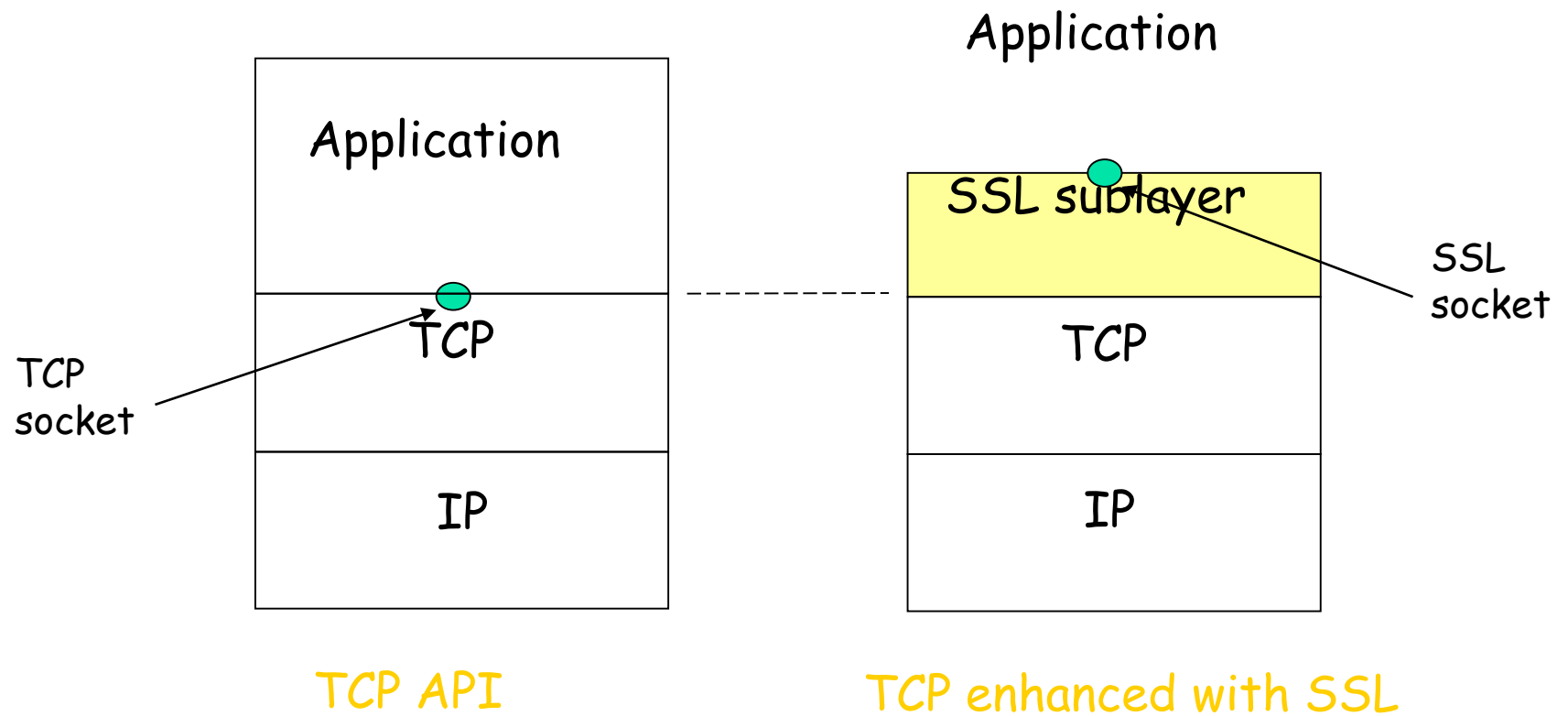
- Kiểm tra danh tính của thành phần tham gia truyền thông
- Chứng chỉ được sử dụng để đồng bộ định danh với khóa công khai và các thuộc tính khác



SSL/TLS: các bước hoạt động

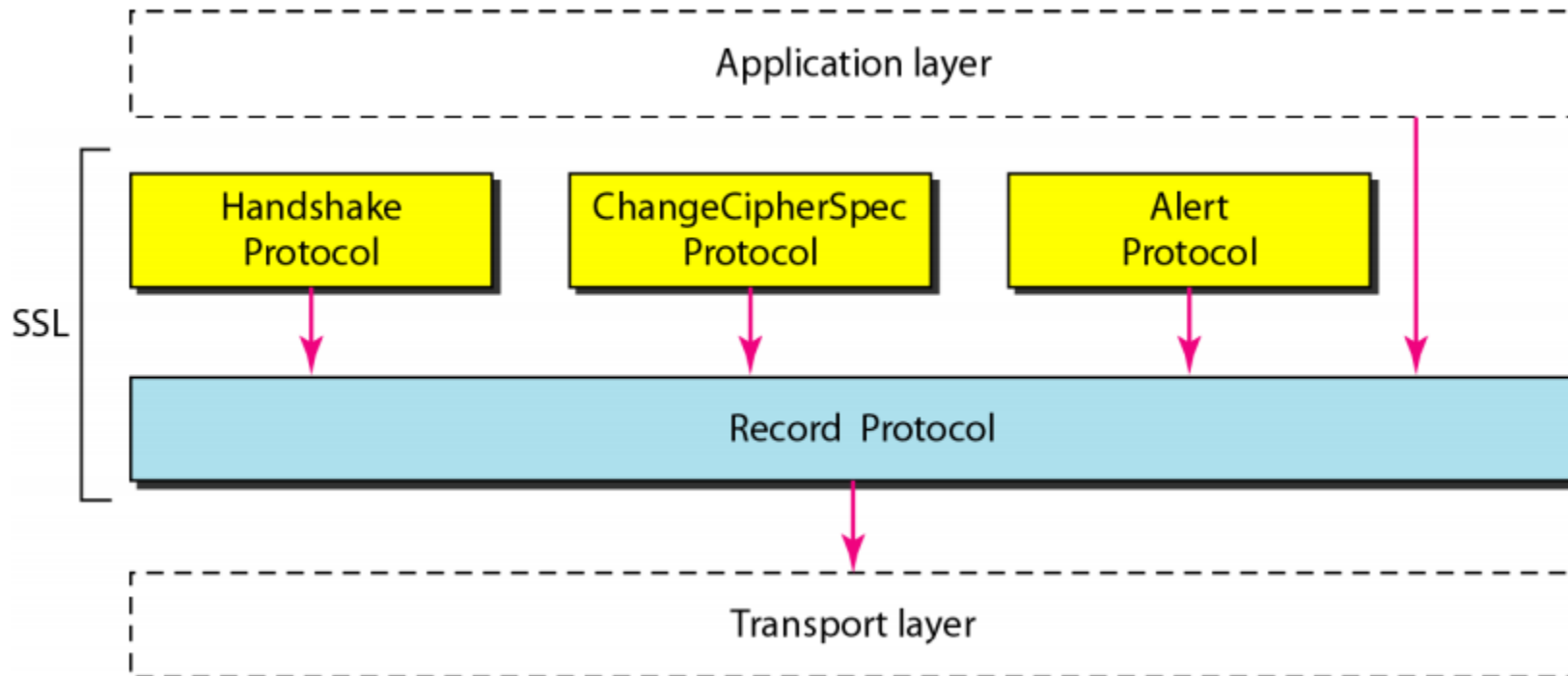
- ❖ Thiết lập 1 phiên làm việc:
 - Đồng bộ thuật toán mã hóa
 - Chia sẻ khóa bí mật
 - Thực hiện xác thực
- ❖ Truyền dữ liệu của ứng dụng:
 - Đảm bảo tính bí mật và toàn vẹn

SSL/TLS: kiến trúc

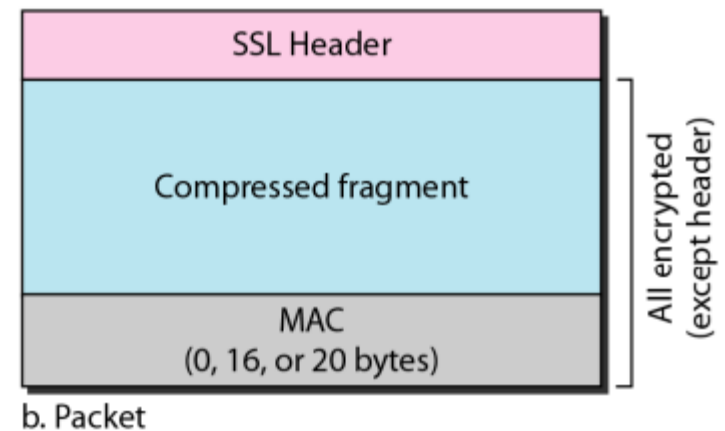
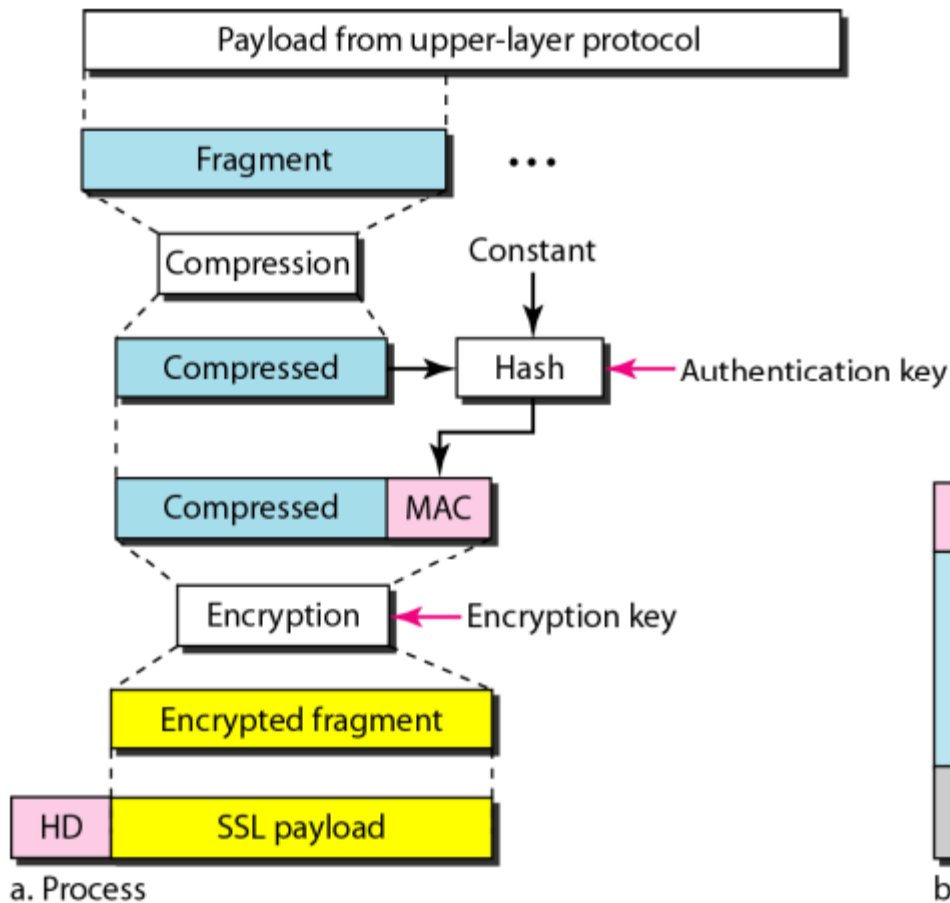


SSL/TLS: Kiến trúc

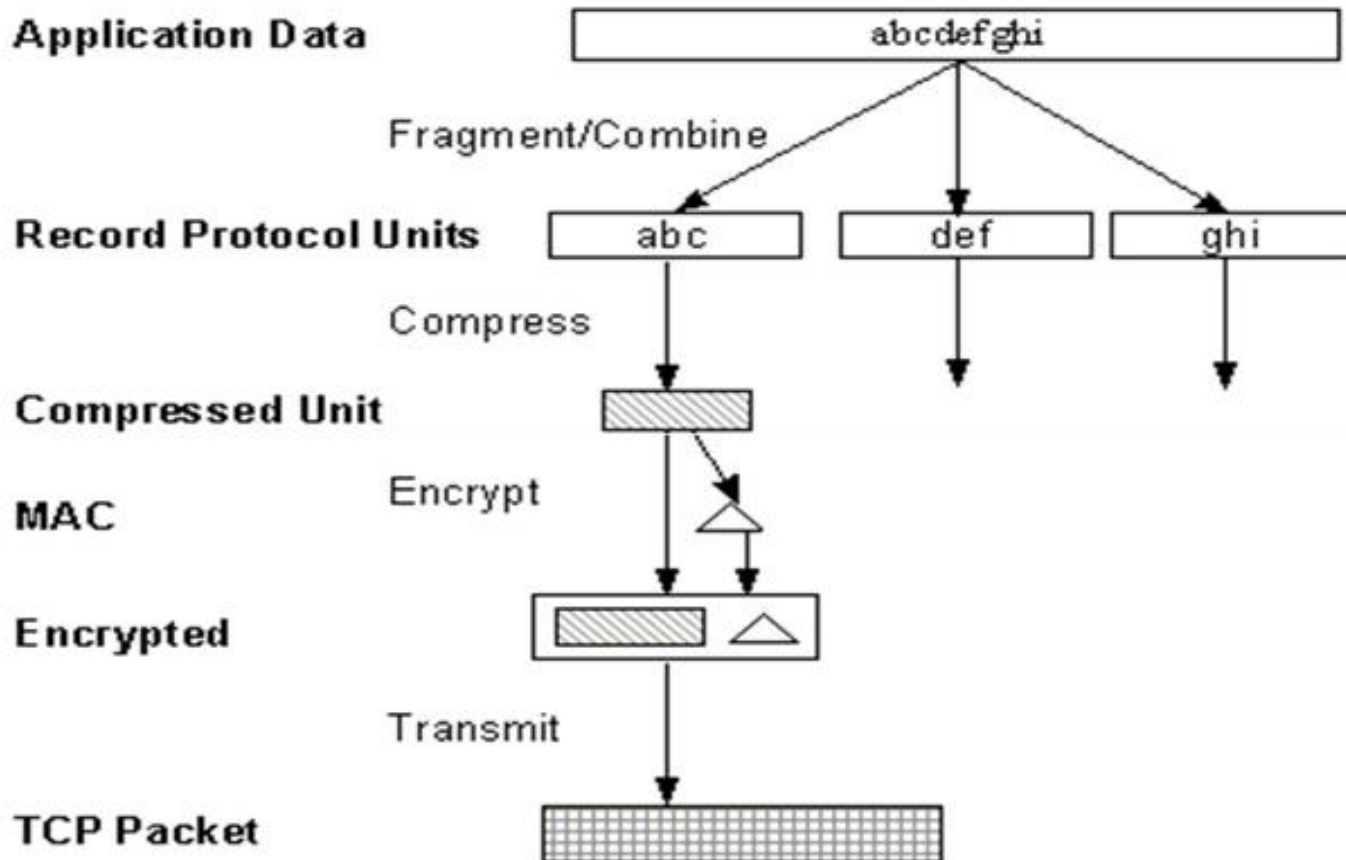
- ❖ Định nghĩa các bản tin để truyền thông tin của ứng dụng và của SSL/TLS
- ❖ Các phiên làm việc được thiết lập sử dụng giao thức bắt tay



SSL/TLS: record protocol



SSL/TLS: record protocol





SSL/TLS: Các giải thuật mật mã hóa

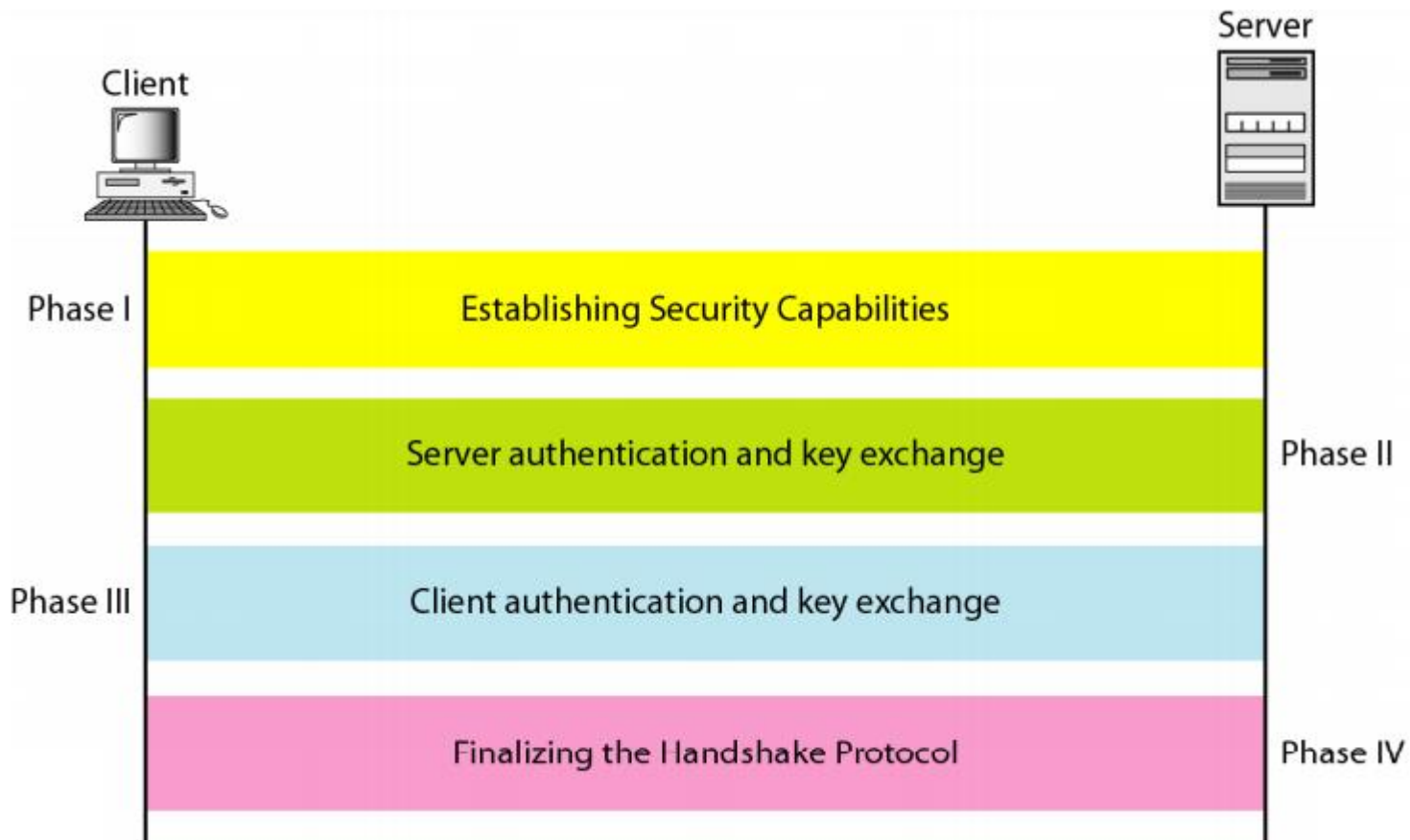
Block Cipher		Stream Cipher	
Algorithm	Key Size	Algorithm	Key Size
AES	128, 256	RC4-40	40
IDEA	128	RC4-128	128
RC2-40	40		
DES-40	40		
DES	56		
3DES	168		
Fortezza	80		



SSL/TLS: Các giao thức khác

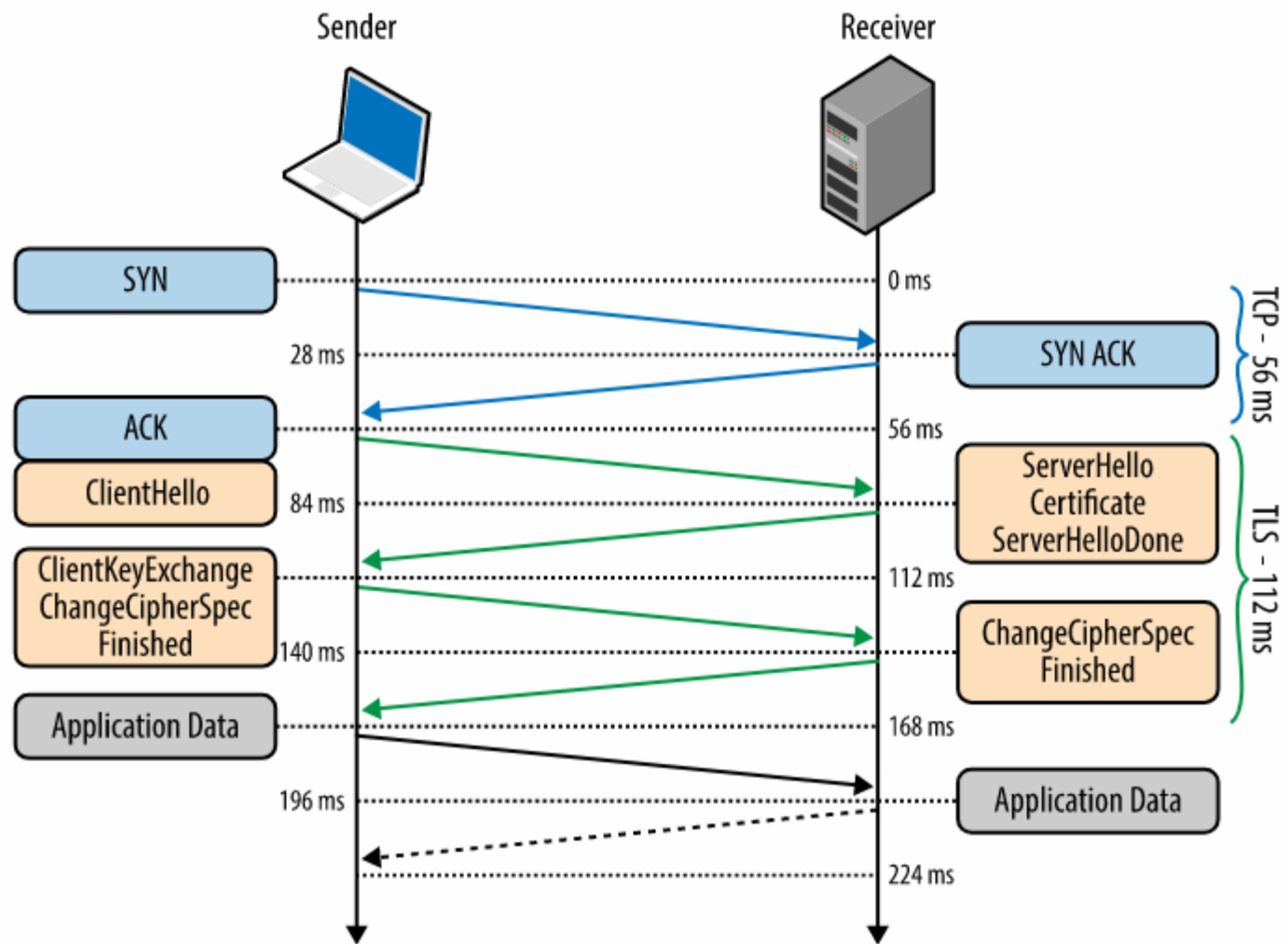
1. Change cipher spec protocol: update trạng thái mật mã của kết nối.
2. Alert protocol: truyền đạt cảnh báo cho đối tượng kết nối.
3. Handshake protocol: xác thực và thỏa thuận thuật toán, khóa

SSL/TLS: Giao thức bắt tay



SSL/TLS: Pha bắt tay

- ❖ Trước khi client và server có thể trao đổi dữ liệu ứng dụng với nhau qua TLS, một đường hầm bảo mật phải được đàm phán
- ❖ Hai bên phải thỏa thuận về phiên bản giao thức, bộ mã hóa phù hợp, kiểm tra chứng chỉ nếu cần thiết





HTTPS

- HTTP over Secure Socket Layer (SSL): kết hợp của HTTP và SSL;
- Sử dụng cổng 443 (thay cho 80 của HTTP);

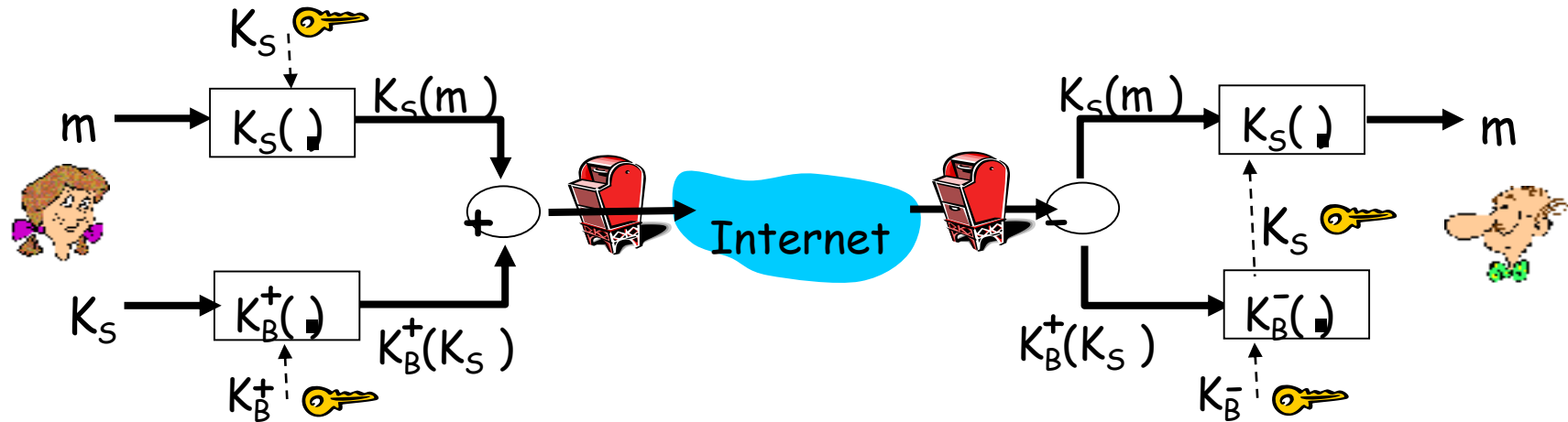


Các giao thức an toàn lớp ứng dụng

PGP	S/MIME	S-HTTP	HTTPS	SET	KERBEROS
Transport Layer					
Network Layer					

An toàn e-mail – Secured e-mail (1)

- Đảm bảo tính bí mật e-mail, m .

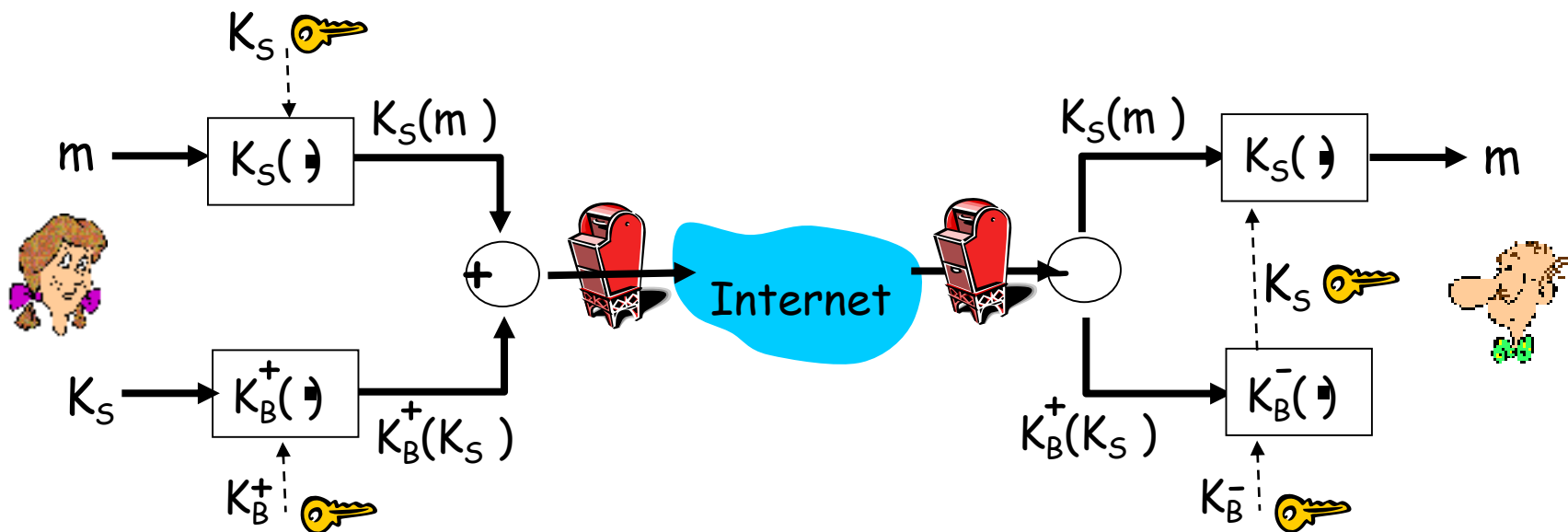


Người gửi:

- tạo khóa riêng (khóa đối xứng), K_S .
- mã hóa bản tin bằng K_S
- mã hóa khóa K_S bằng khóa công khai người nhận.
- gửi $K_S(m)$ và $K_B(K_S)$ cho người nhận.

An toàn e-mail – Secured e-mail (2)

- Đảm bảo tính bí mật e-mail, m .

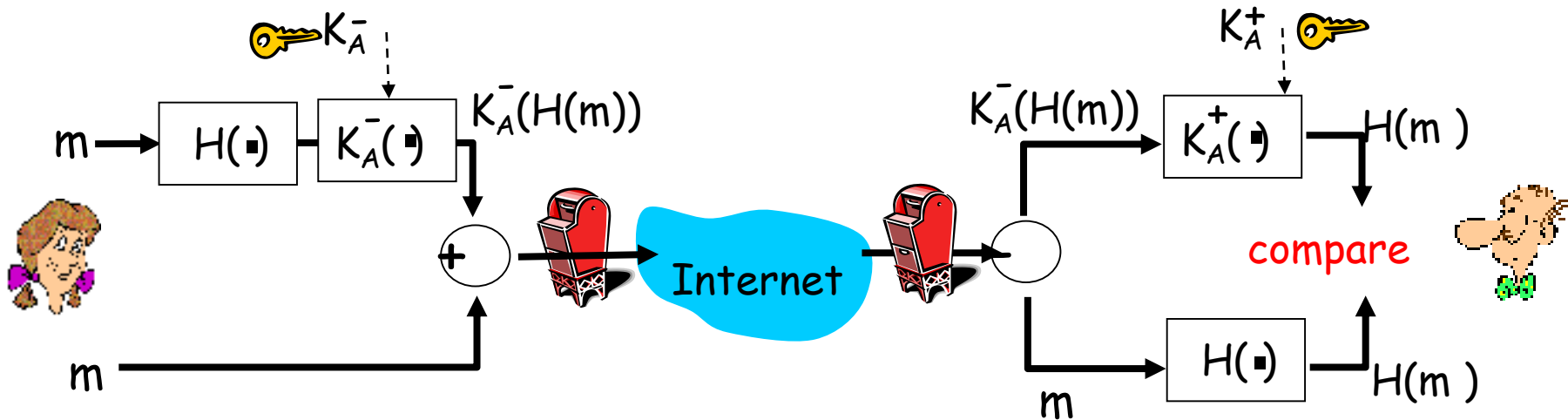


Người nhận:

- sử dụng khóa riêng giải mã và lấy K_S
- sử dụng khóa K_S giải mã $K_S(m)$ để nhận bản tin m

An toàn e-mail – Secured e-mail (3)

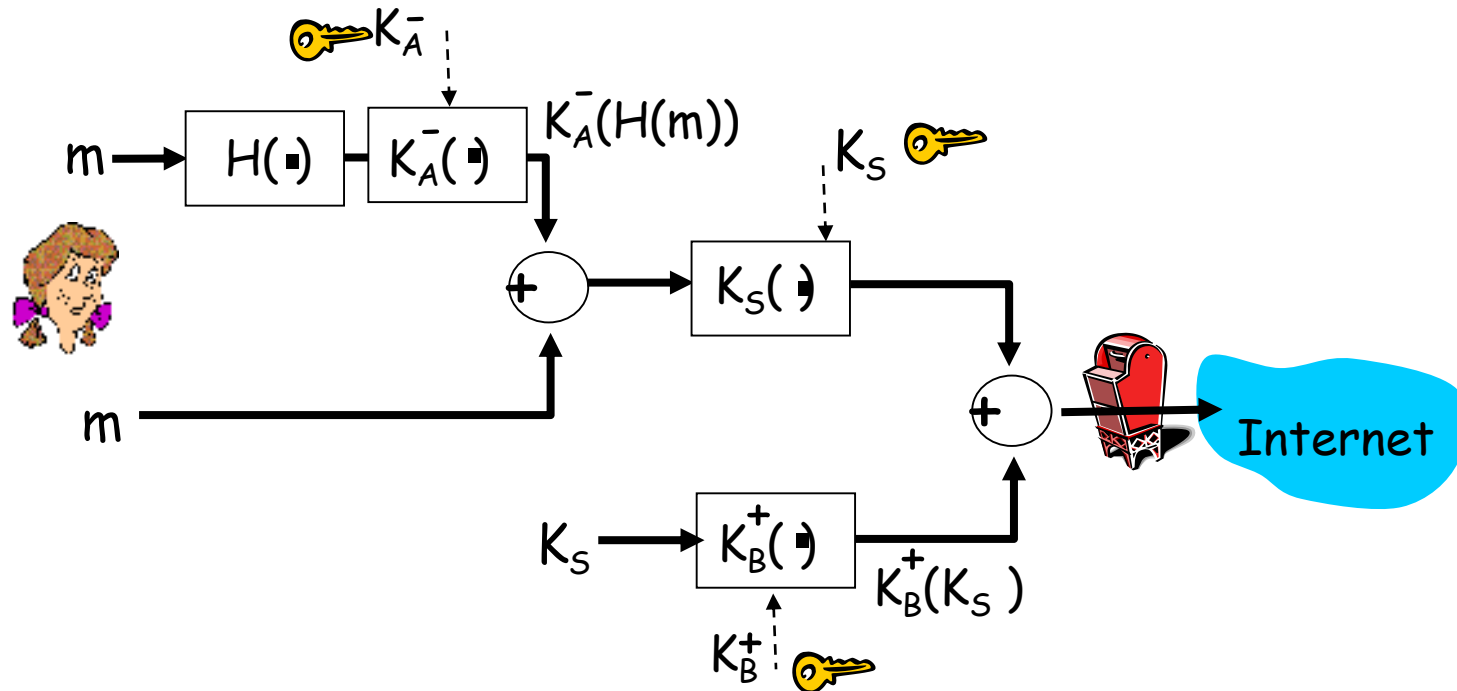
□ Đảm bảo tính xác thực, tính toàn vẹn.



- Người gửi ký số vào bản tin.
- Gửi cả bản tin nguyên thủy và chữ ký số.

An toàn e-mail – Secured e-mail (4)

- Đảm bảo tính bí mật, tính xác thực, tính toàn vẹn.



Người gửi sử dụng ba loại khóa: khóa riêng của người gửi, khóa công khai của người nhận, tạo khóa đối xứng (khóa bí mật) mới.



PGP: Pretty good privacy

- Cấu trúc mã hóa e-mail Internet, trở thành tiêu chuẩn.
- Sử dụng mã hóa khóa đối xứng, mã hóa khóa công khai, hàm băm, và chữ ký số.
- Cung cấp tính bí mật, xác thực người gửi, tính toàn vẹn.
- Người phát minh Phil Zimmerman.

Bản tin được ký số PGP:

```
---BEGIN PGP SIGNED MESSAGE---  
Hash: SHA1
```

```
Bob:My husband is out of town  
    tonight.Passionately yours,  
    Alice
```

```
---BEGIN PGP SIGNATURE---  
Version: PGP 5.0  
Charset: noconv  
yhHJRHhGJGhgg/12EpJ+lo8gE4vB3mqJhF  
    EvZP9t6n7G6m5Gw2  
---END PGP SIGNATURE---
```

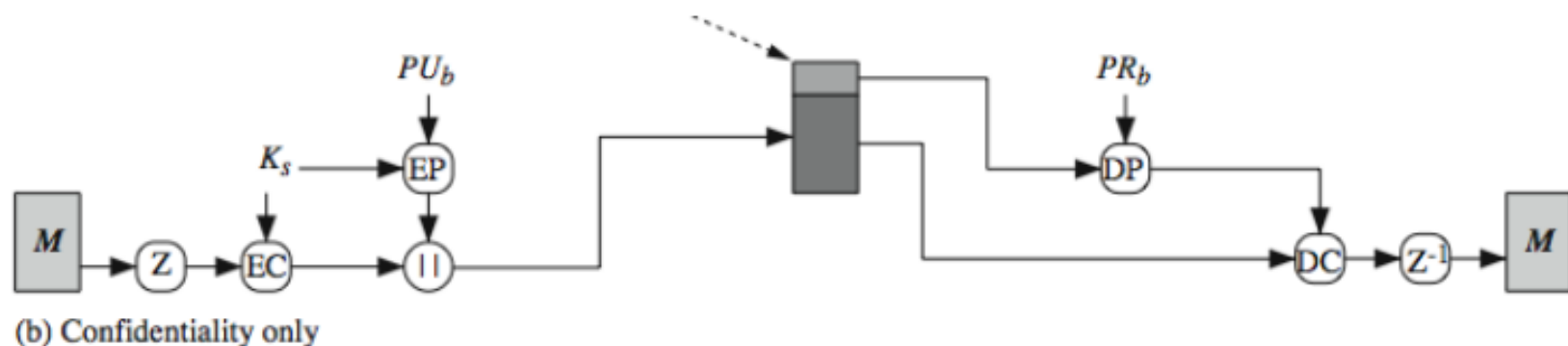
PGP Operation - Authentication

1. sender creates message
2. make SHA-1/60-bit hash of message
3. attached RSA signed hash to message
4. receiver decrypts & recovers hash code
5. receiver verifies received message hash



PGP Operation - Confidentiality

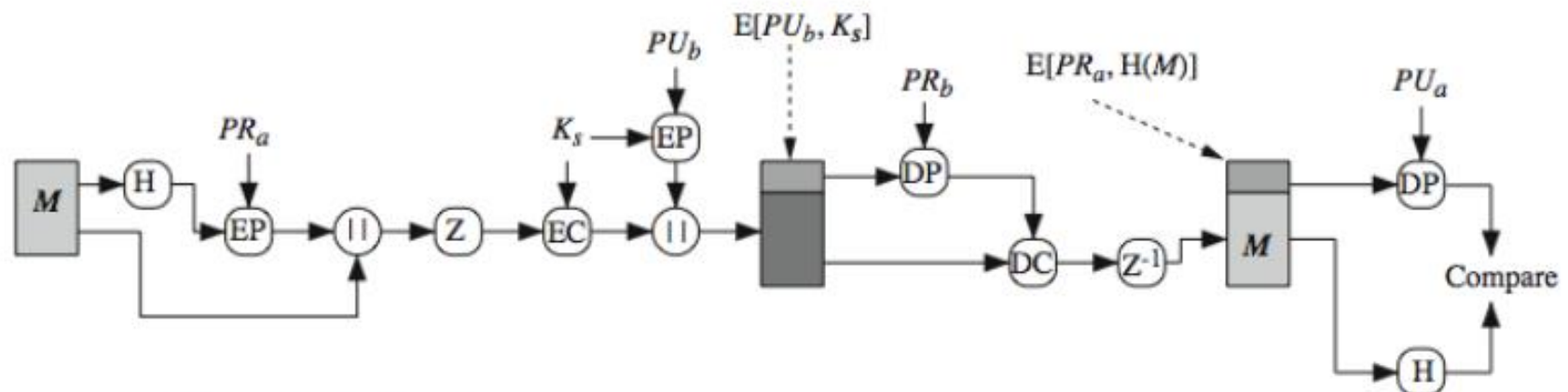
1. sender forms 128-bit random session key
2. encrypts message with session key
3. attaches session key encrypted with RSA
4. receiver decrypts & recovers session key
5. session key is used to decrypt message



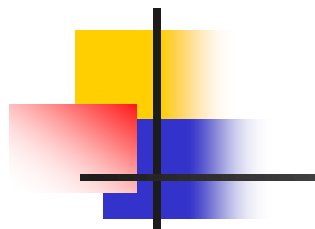
PGP – Authentication & Confidentiality

Can use both services on same message

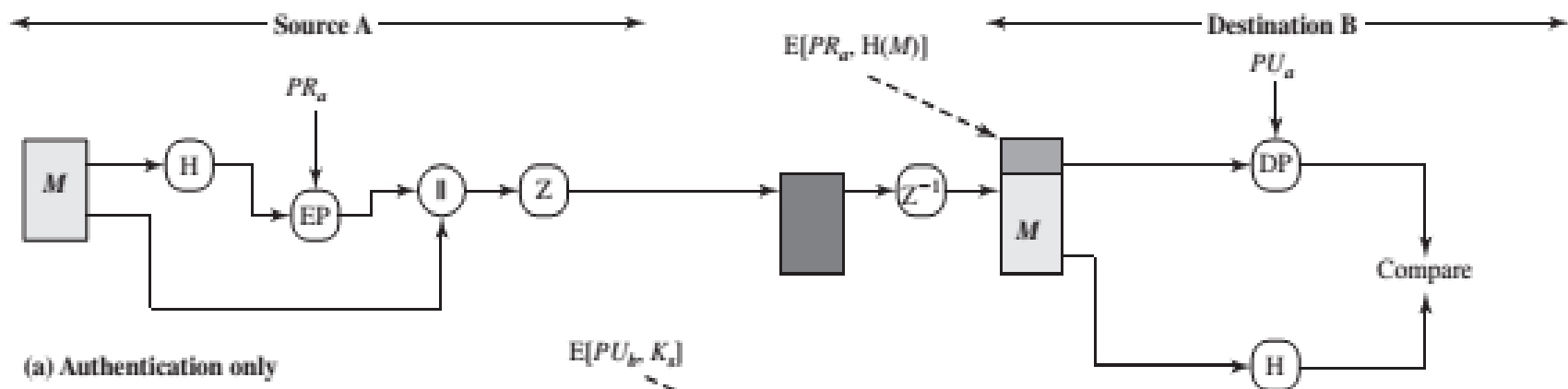
- create signature & attach to message
- encrypt both message & signature
- attach RSA/ElGamal encrypted session key



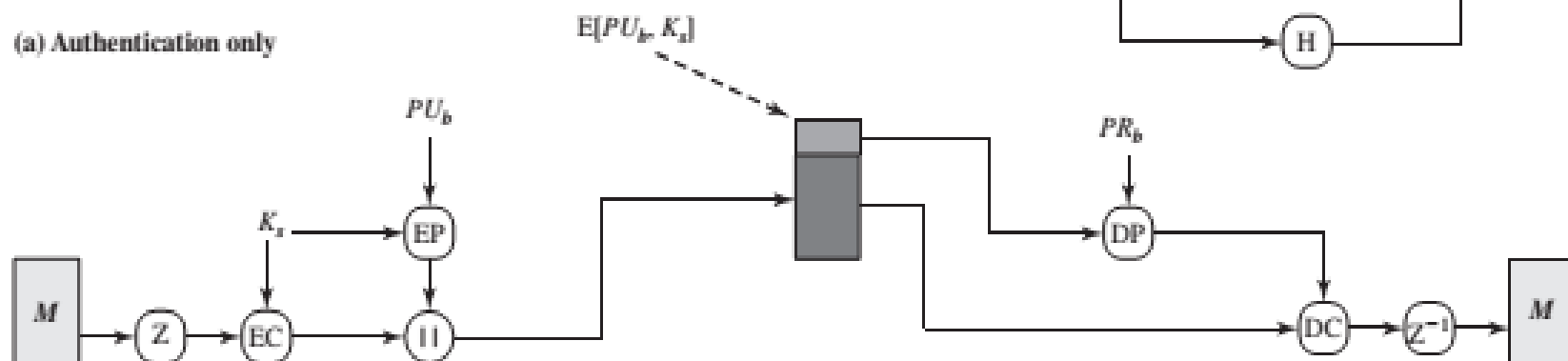
(c) Confidentiality and authentication



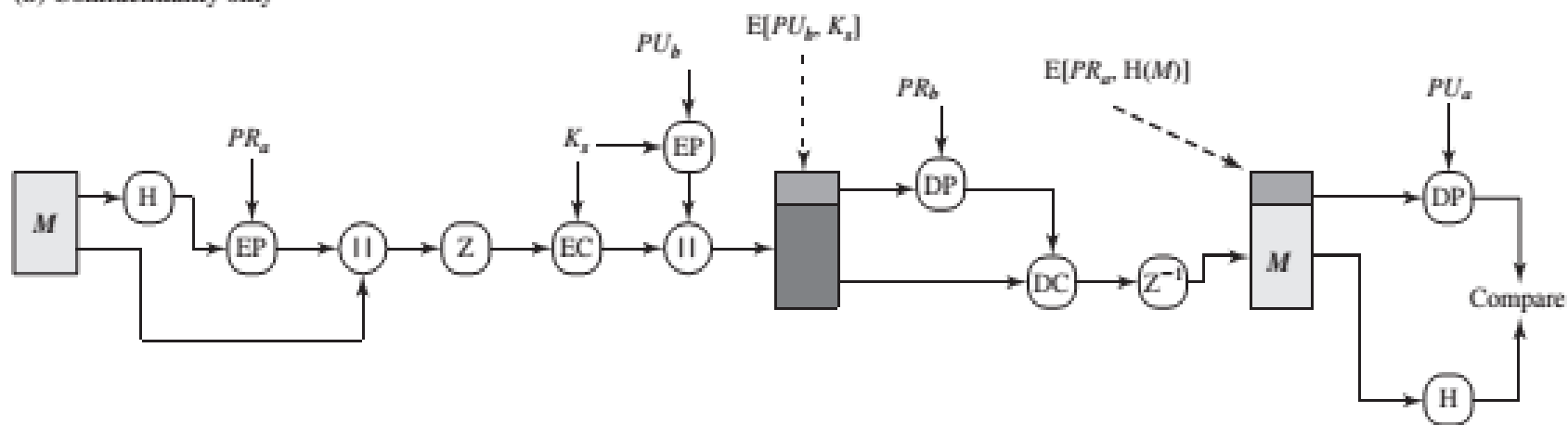
Chức năng mật mã PGP



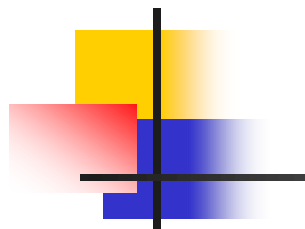
(a) Authentication only



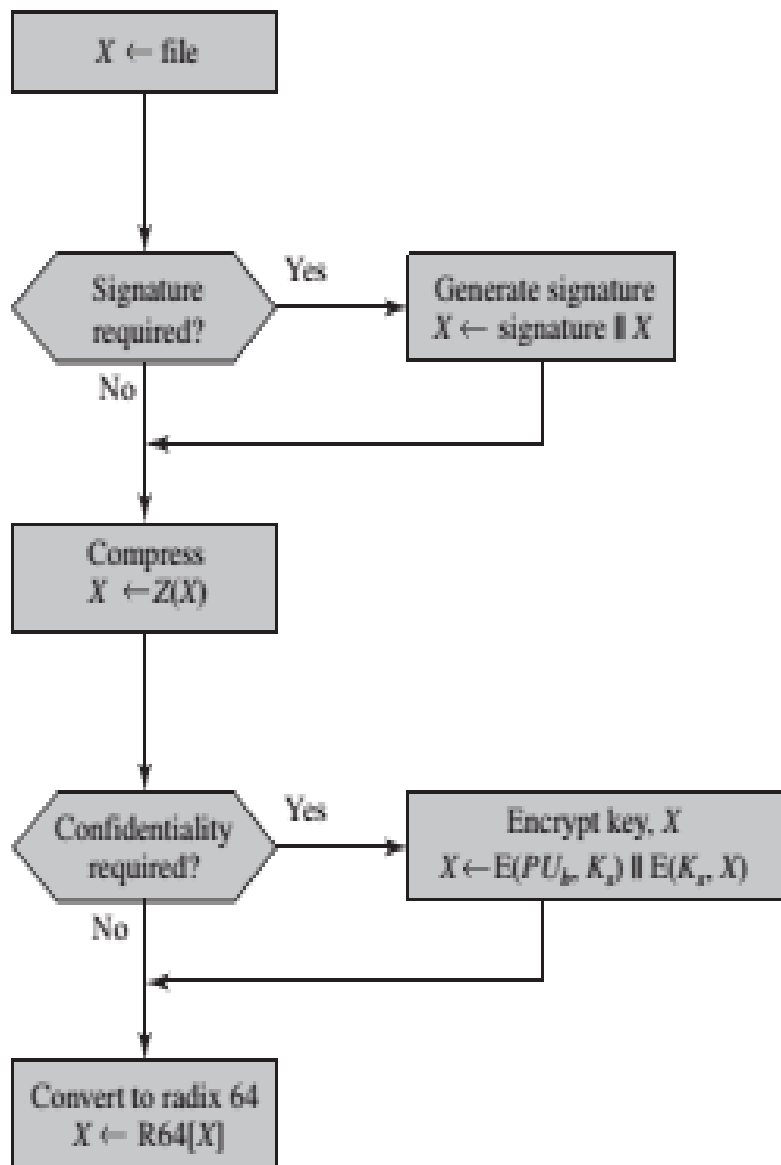
(b) Confidentiality only



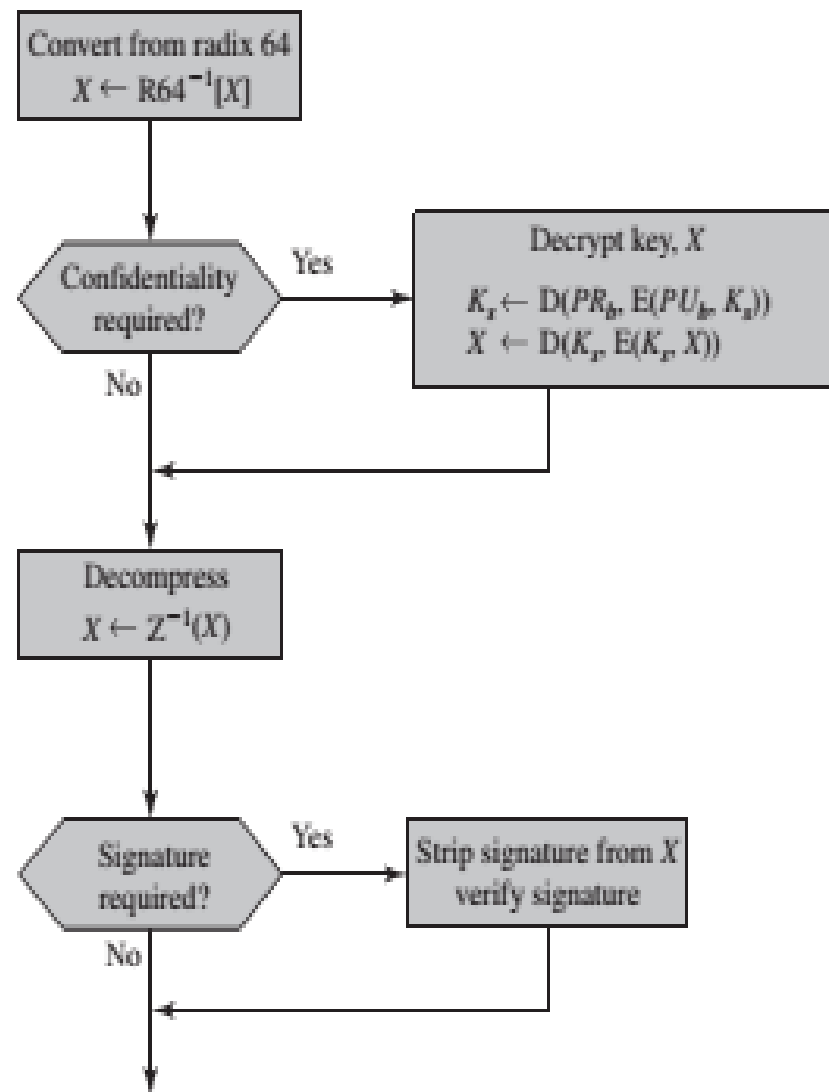
(c) Confidentiality and authentication



Quá trình gửi và nhận bản tin PGP



(a) Generic transmission diagram (from A)



(b) Generic reception diagram (to B)



S/MIME

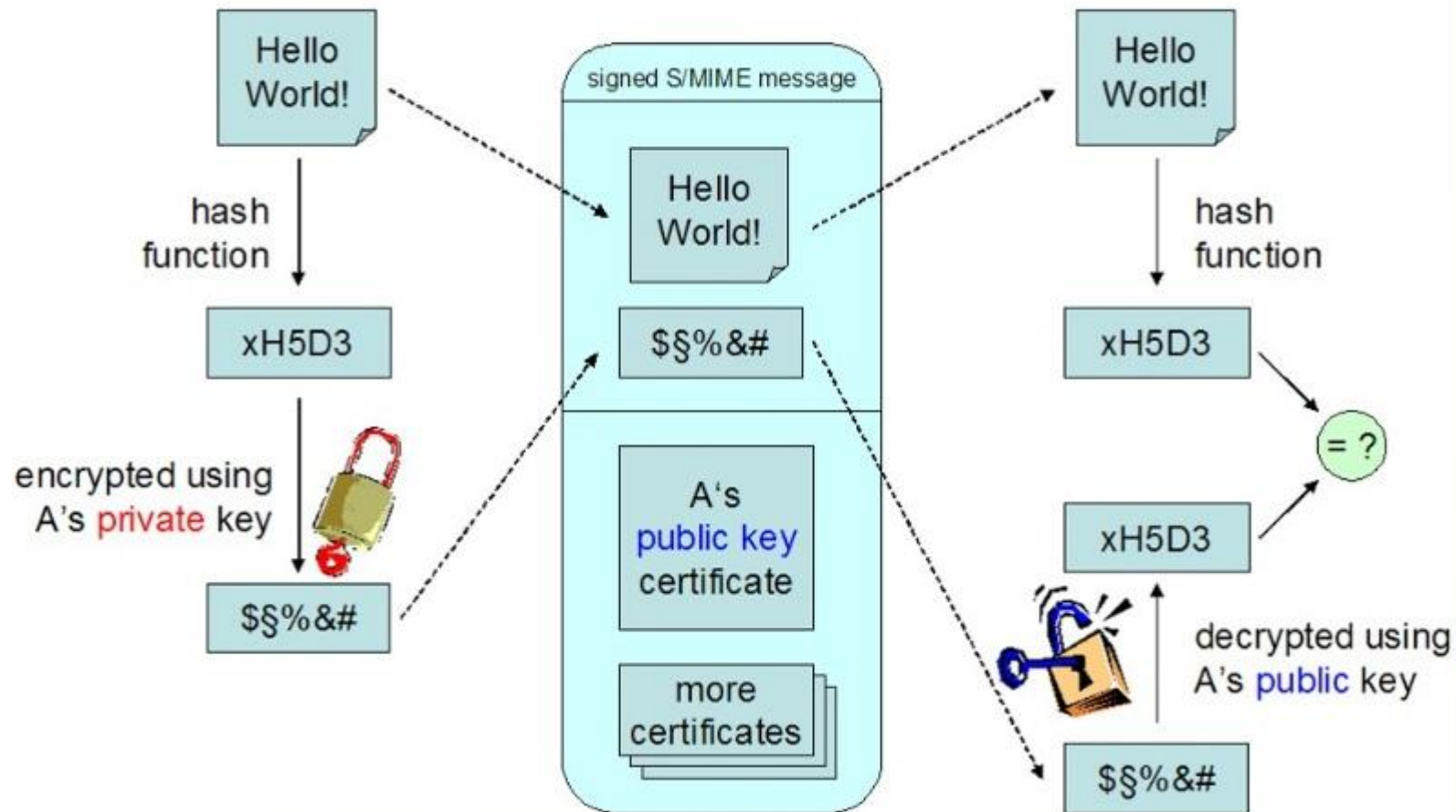
Secure/Multipurpose Internet Mail Extension

- ❖ MIME: giao thức mô tả truyền dữ liệu đa phương tiện; (RFC 1521). (MIME header – RFC 822, RFC 5322).
- ❖ S/MIME: bổ sung chữ ký số (băm bằng SHA, MD5; mã hóa chữ ký số bằng RSA, DSS) và mật mã hóa bản tin (3-DES, AES, RC2/40) vào MIME.
- ❖ Các tiêu chuẩn: RFC 3370, 3850, 3851, 3852.

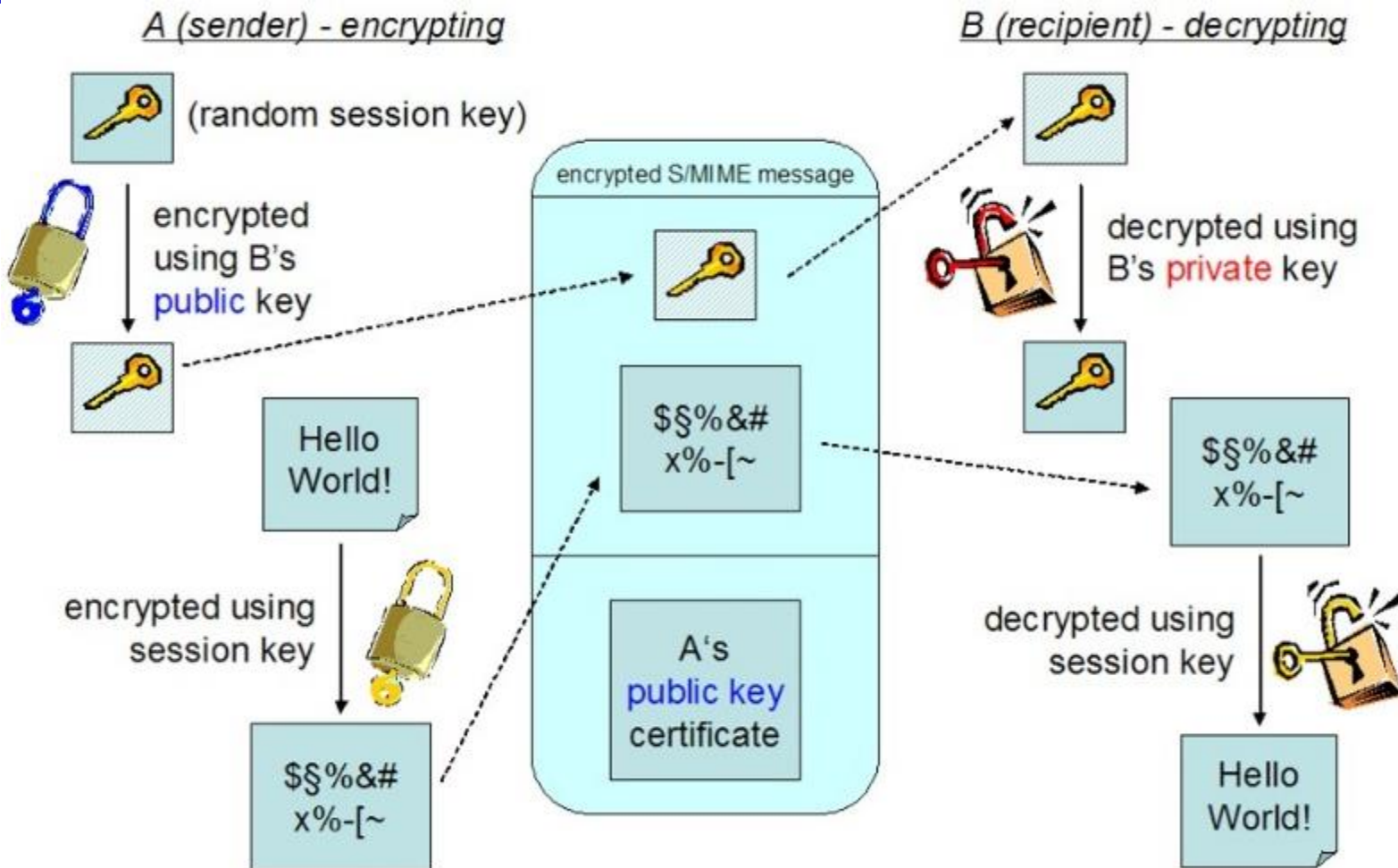
S/MIME: Signed Mail

A (sender) - signing

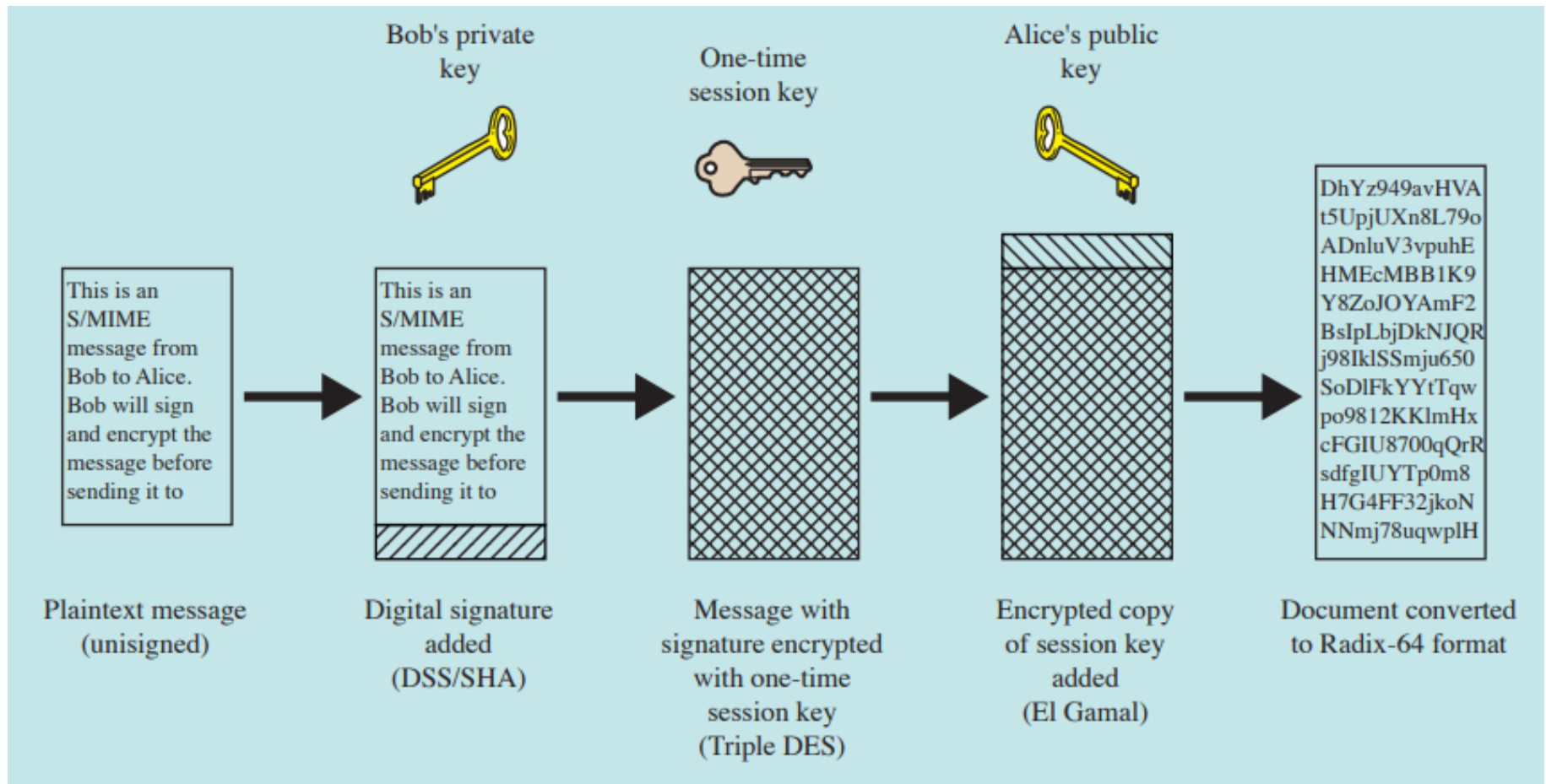
B (recipient) - verification



S/MIME: Encrypted Mail



S/MIME: xử lý tại bên gửi





Secure Electronic Transaction - SET

- ❖ Giao thức mã hóa do các công ty lập ra: Visa, MicroSoft, IBM, RSA, Netscape, Master Card, ...
- ❖ Sử dụng trong giao dịch điện tử: bí mật thông tin và giao dịch, toàn vẹn dữ liệu, xác thực người sử dụng thẻ, không phụ thuộc vào hạ tầng truyền dẫn, kết nối các nhà cung cấp phần mềm và mạng.

- **Xác thực: X.509 v3;**
- **Tính bí mật: DES;**
- **Toàn vẹn: SHA-1.**



Tổng quan an toàn mạng không dây

- ❖ Mạng không dây đang được sử dụng trong nhiều lĩnh vực vì các ưu điểm của nó:
 - Tính tiện lợi, di động, linh hoạt
 - Tiết kiệm, hiệu quả, dễ mở rộng
- ❖ Mạng không dây sử dụng kênh truyền là vô tuyến (truyền sóng điện từ) nên đặt ra nhiều thách thức về vấn đề an ninh cho các mạng này



Tổng quan an toàn mạng không dây

❖ Các nguy cơ tấn công:

- Nghe trộm
- Tấn công các kết nối
- DoS
- ...

❖ Các biện pháp an toàn:

- Xác thực
- Bảo mật
- Bảo vệ tính toàn vẹn
- Ngăn ngừa tấn công DoS



Tổng quan an toàn mạng không dây

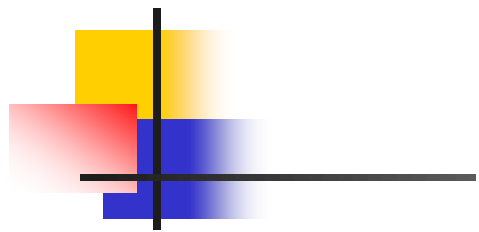
❖ Các giải pháp an ninh mạng không dây:

- MAC Authentication
- WEP (Wired Equivalent Privacy)
- 802.11i (WPA - Wifi Protected Access)
- EAP/LEAP (Extensible Authentication Protocol)
- WAP (Wireless Application Protocol)



Kiểm soát truy nhập mạng (Network Access Control - NAC)

- Access Requestor (AR): Người yêu cầu truy nhập;
- Policy Server (PS): Máy chủ chính sách xác định truy nhập nào được cho phép;
- Network access server (NAS): Máy chủ kiểm soát truy nhập mạng thực hiện chức năng là điểm kiểm soát kết nối vào mạng;



NAC

Supplicants



Network access servers

Authentication server



DHCP server



VLAN server



Policy server



Patch management



Antivirus



Antispyware

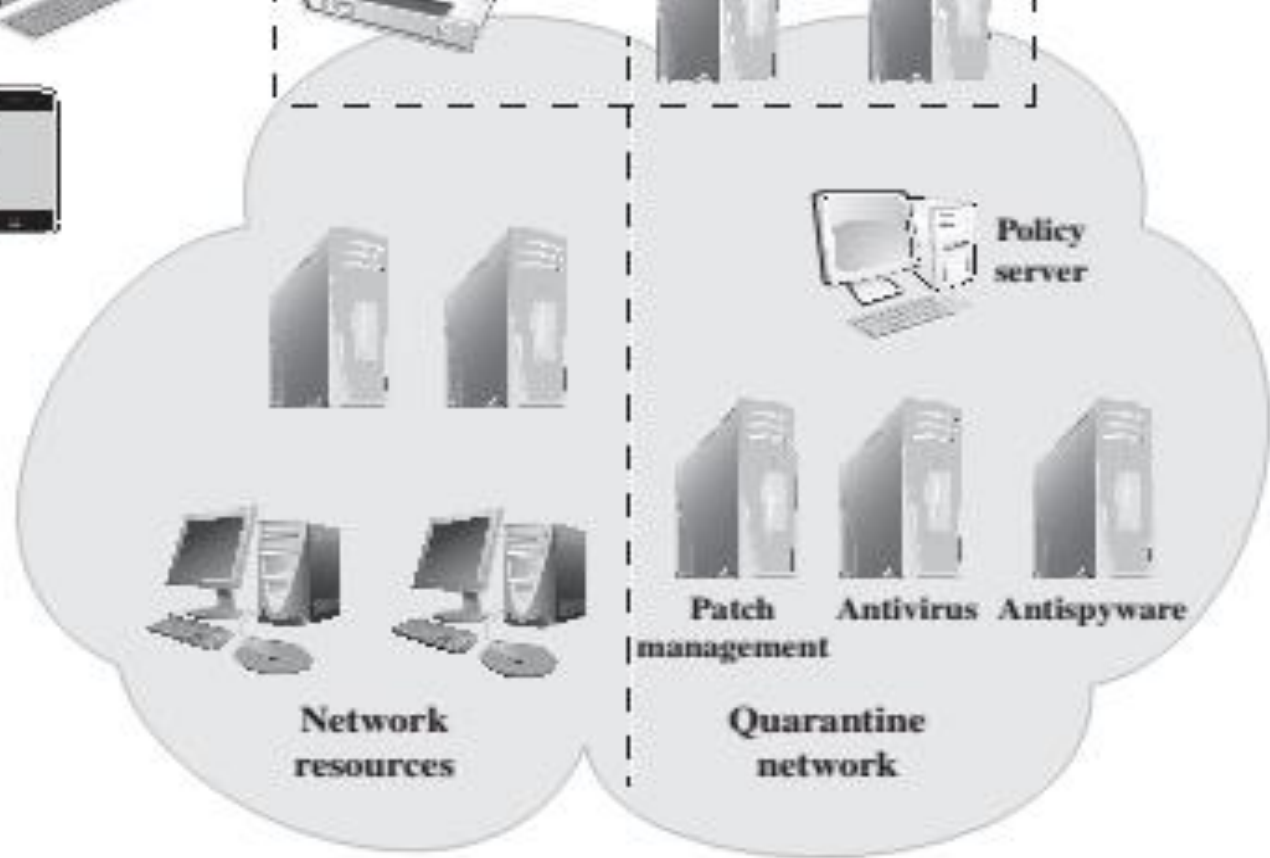


Network resources



Quarantine network

Enterprise network

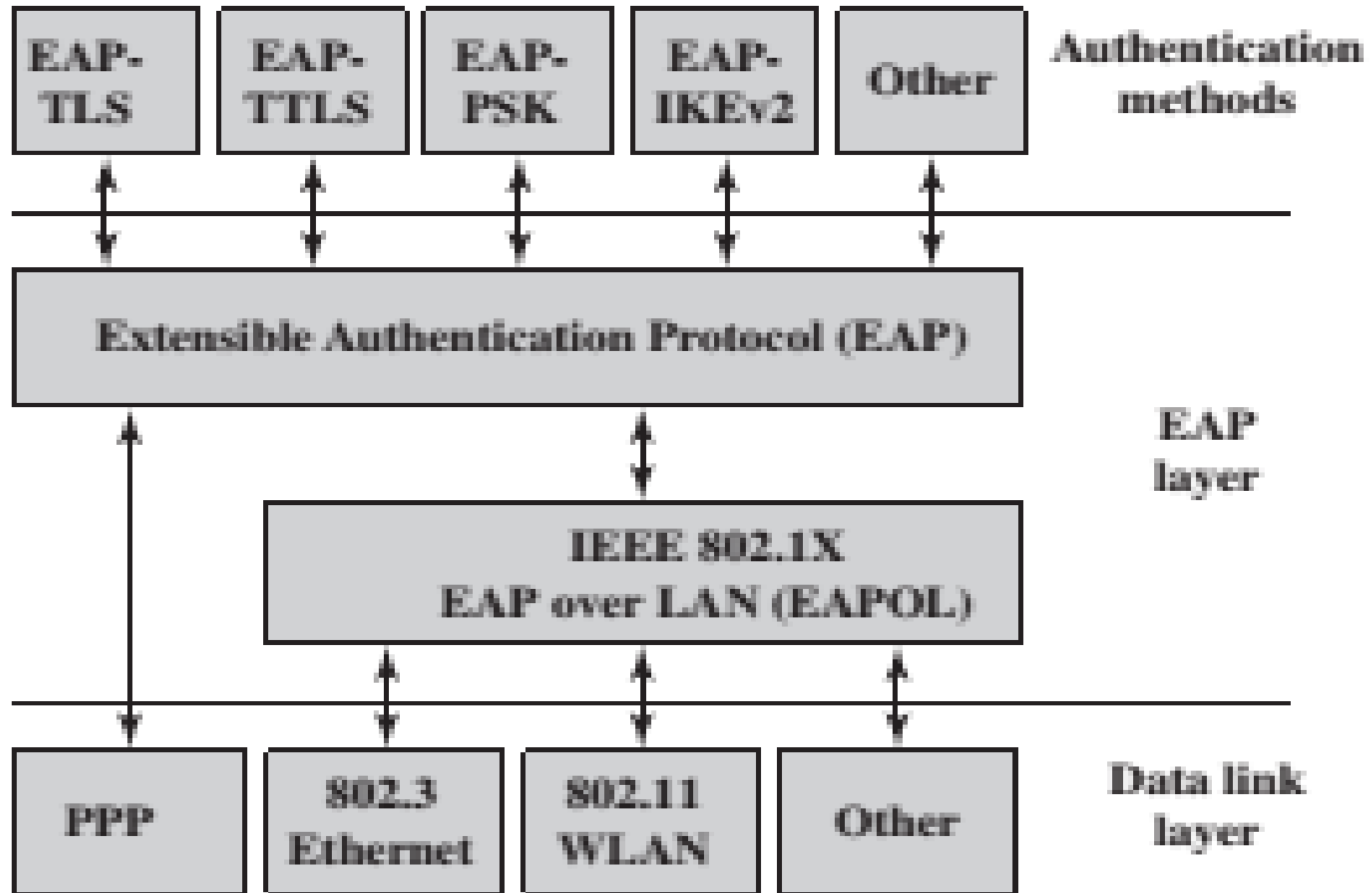


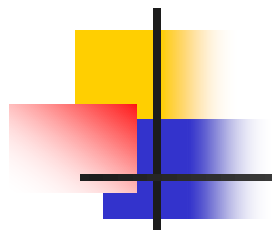


Các phương pháp kiểm soát truy nhập mạng

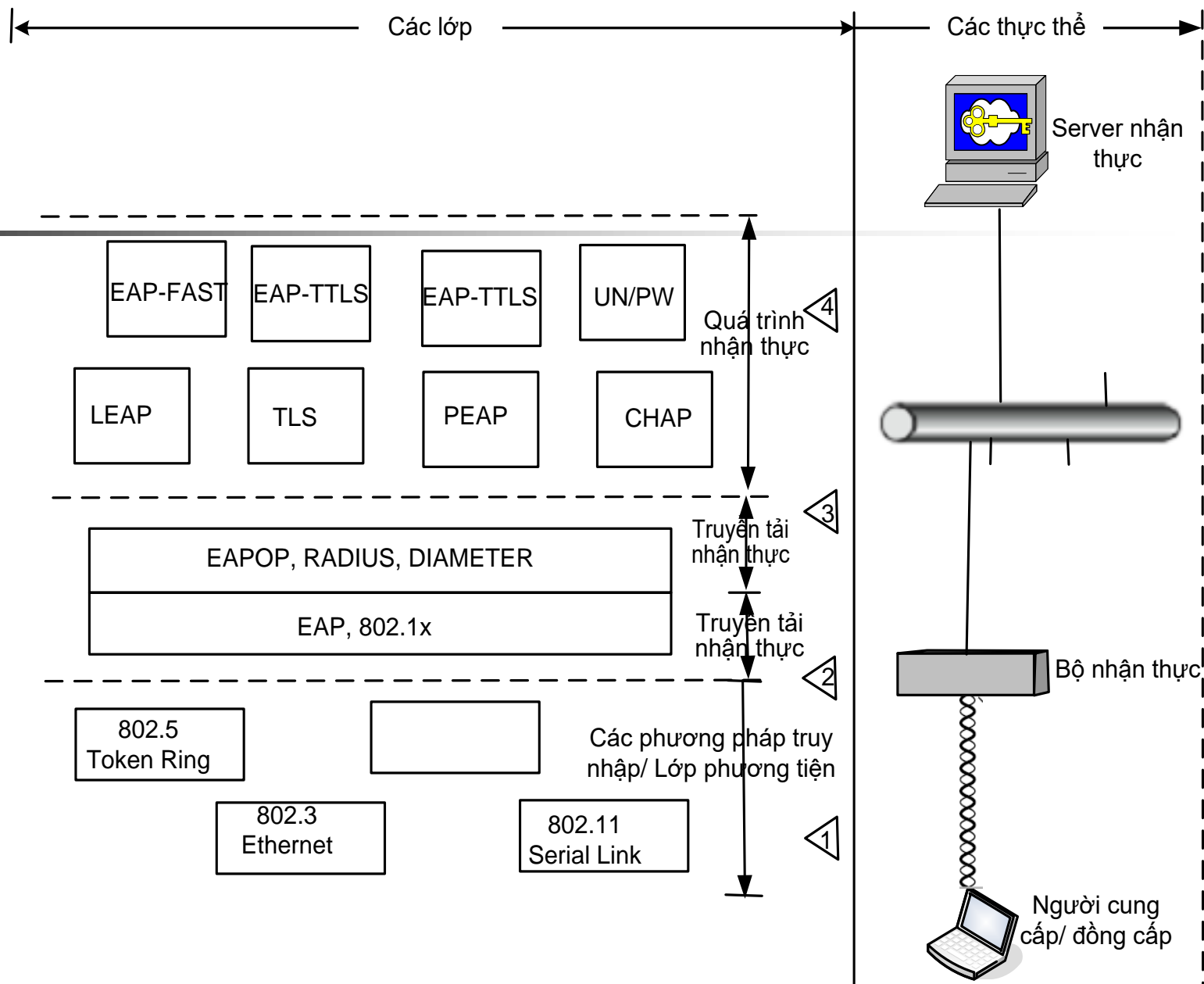
- IEEE 802.1x: Giao thức lớp liên kết, thực hiện xác thực trước khi gán cổng cho địa chỉ IP, sử dụng EAP (Extensible Authentication Protocol);
- VLAN: Chia LAN thành các VLAN được phân cấp truy nhập xác định bởi hệ thống NAC;
- Tường lửa (Firewall): kiểm soát lưu lượng đi qua;
- Quản lí DHCP: kiểm soát truy nhập được thực hiện thông qua cấp địa chỉ của DHCP;

Kiến trúc lớp EAP (RFC 3748)





Các phương pháp nhận thực

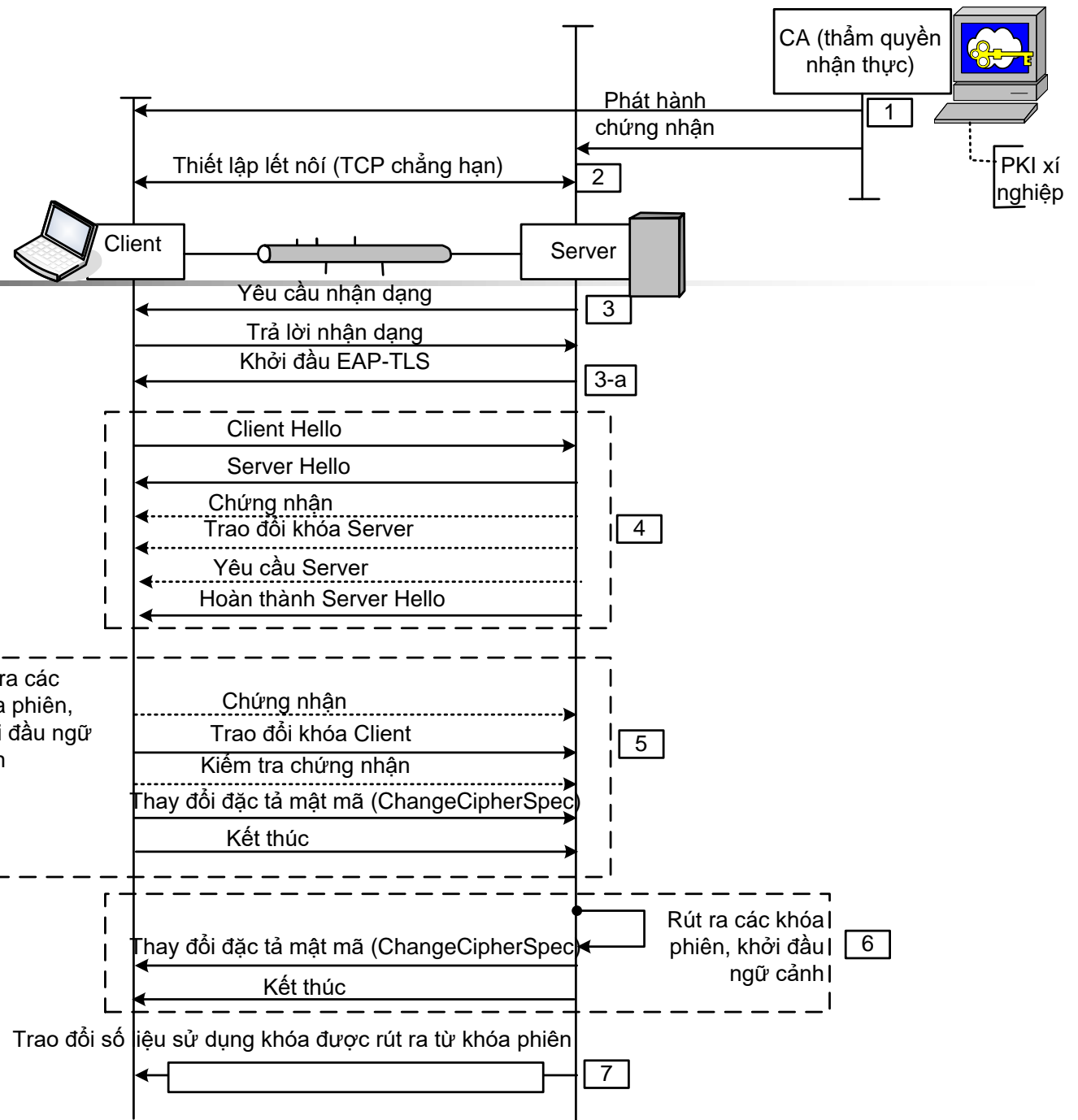




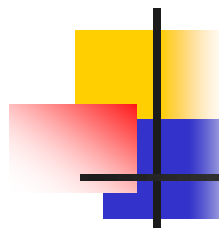
Các phương pháp xác thực

- EAP-TLS (RFC 5216): TLS được đóng gói trên EAP, chỉ sử dụng giai đoạn bắt tay của TLS;
- EAP-TTLS (EAP Tunneled TLS) (RFC 5281): như EAP-TLS, tuy nhiên server tự xác thực trước bằng chứng thư số, các kết nối an toàn được tiếp tục sử dụng để thực hiện quá trình xác thực;
- EAP-PSK (EAP Generalized Pre-shared Key) (RFC 5433): xác thực lẫn nhau và khóa phiên được tạo ra từ PSK.

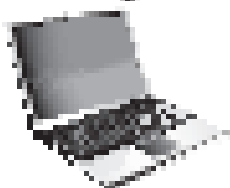
EAP-TLS



Trao đổi bản tin EAP



EAP peer

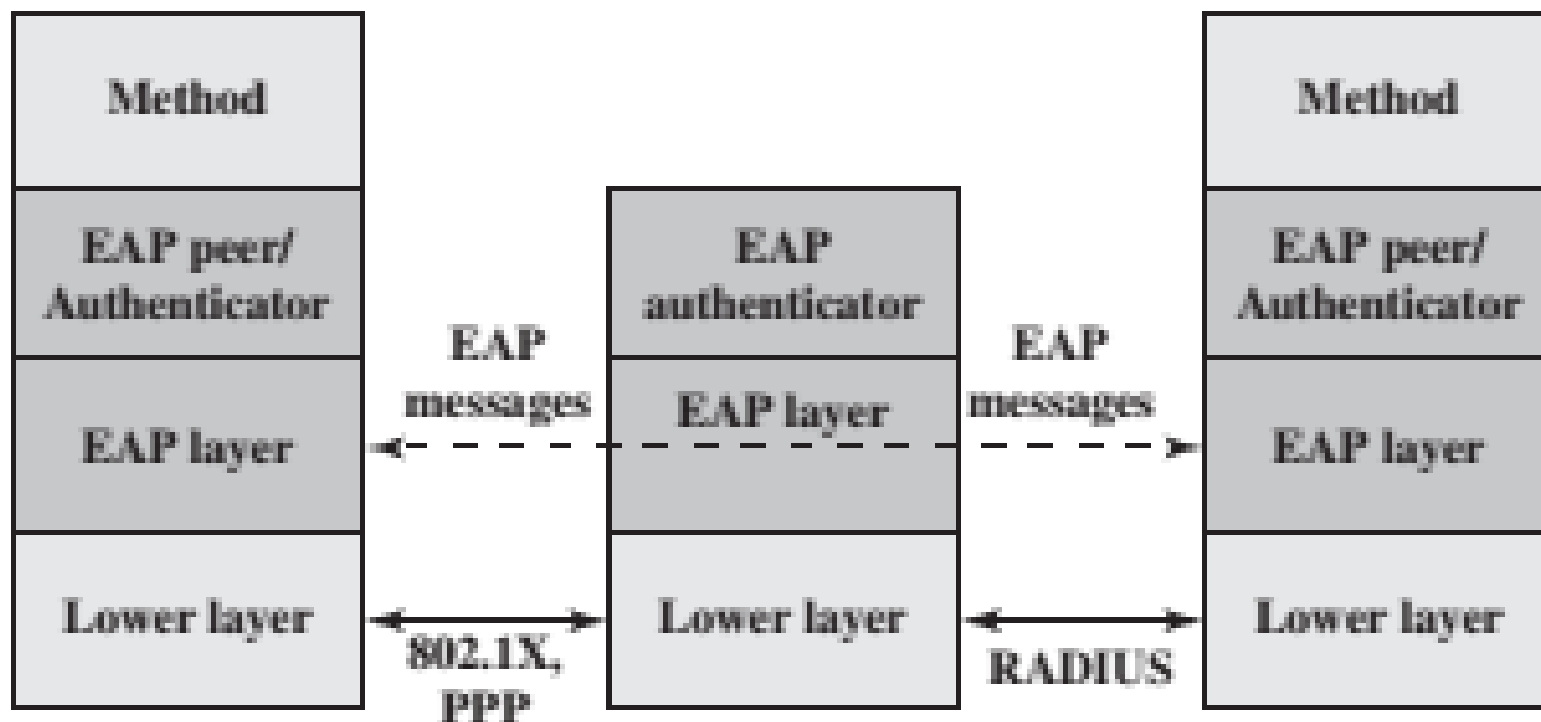


EAP authenticator



Authentication server

(RADIUS)

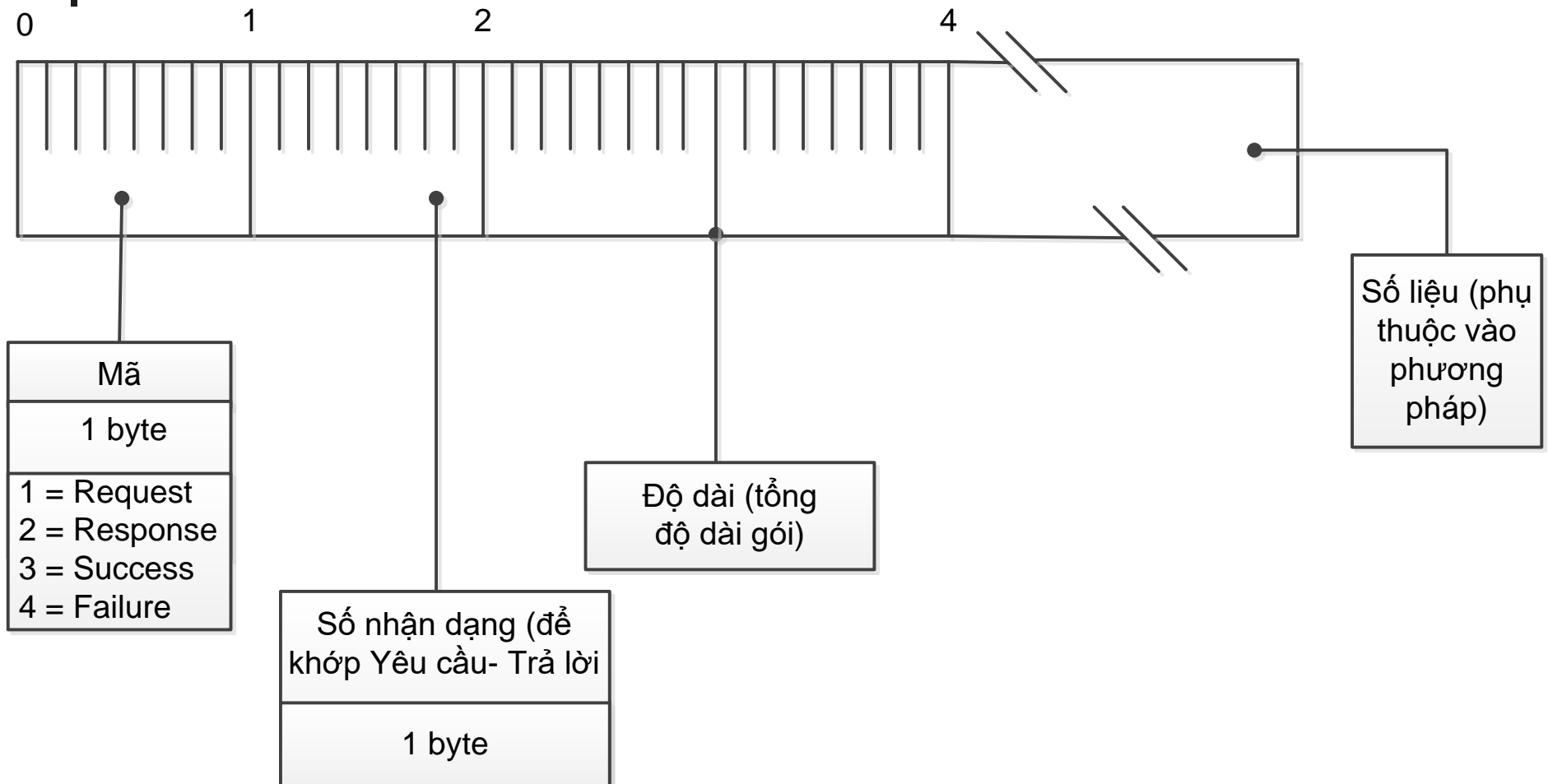


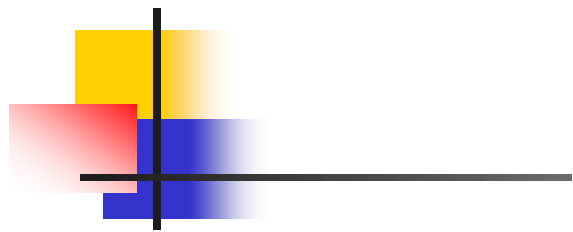
EAP – Extensible Authentication Protocol



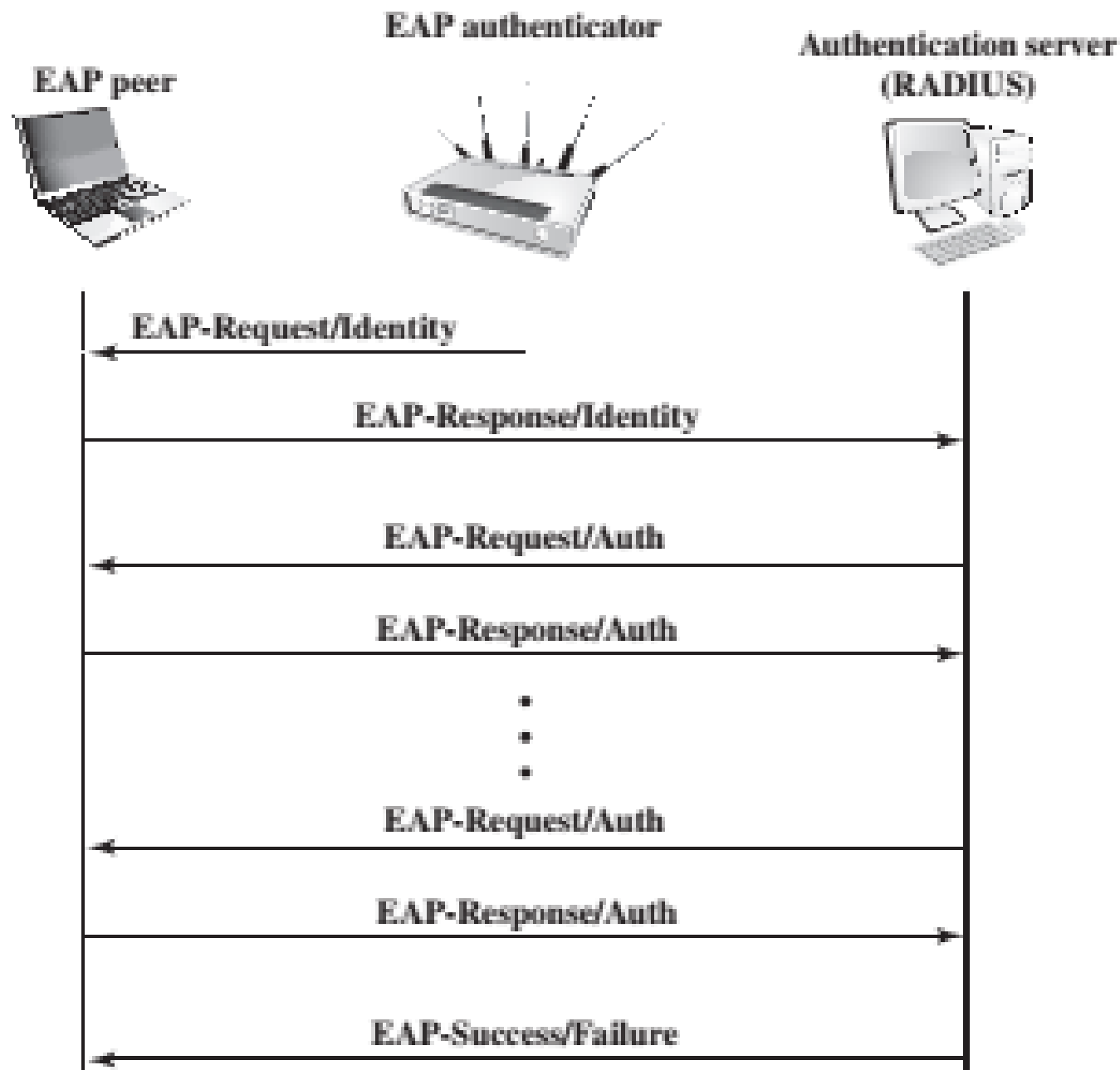
- Giao thức linh hoạt được sử dụng để mang thông tin nhận thực tùy ý;
- EAP có hai tính năng: Trước hết nó tách trao đổi bản tin ra khỏi quá trình nhận thực bằng cách cung cấp một lớp trao đổi độc lập. Nhờ vậy nó đạt được đặc tính thứ hai: tính khả mở rộng trực giao, nghĩa là các quá trình nhận thực có thể mở rộng hoạt động bằng cách tiếp nhận một cơ chế mới hơn và không cần thiết phải thay đổi lớp EAP.

Khuôn dạng EAP

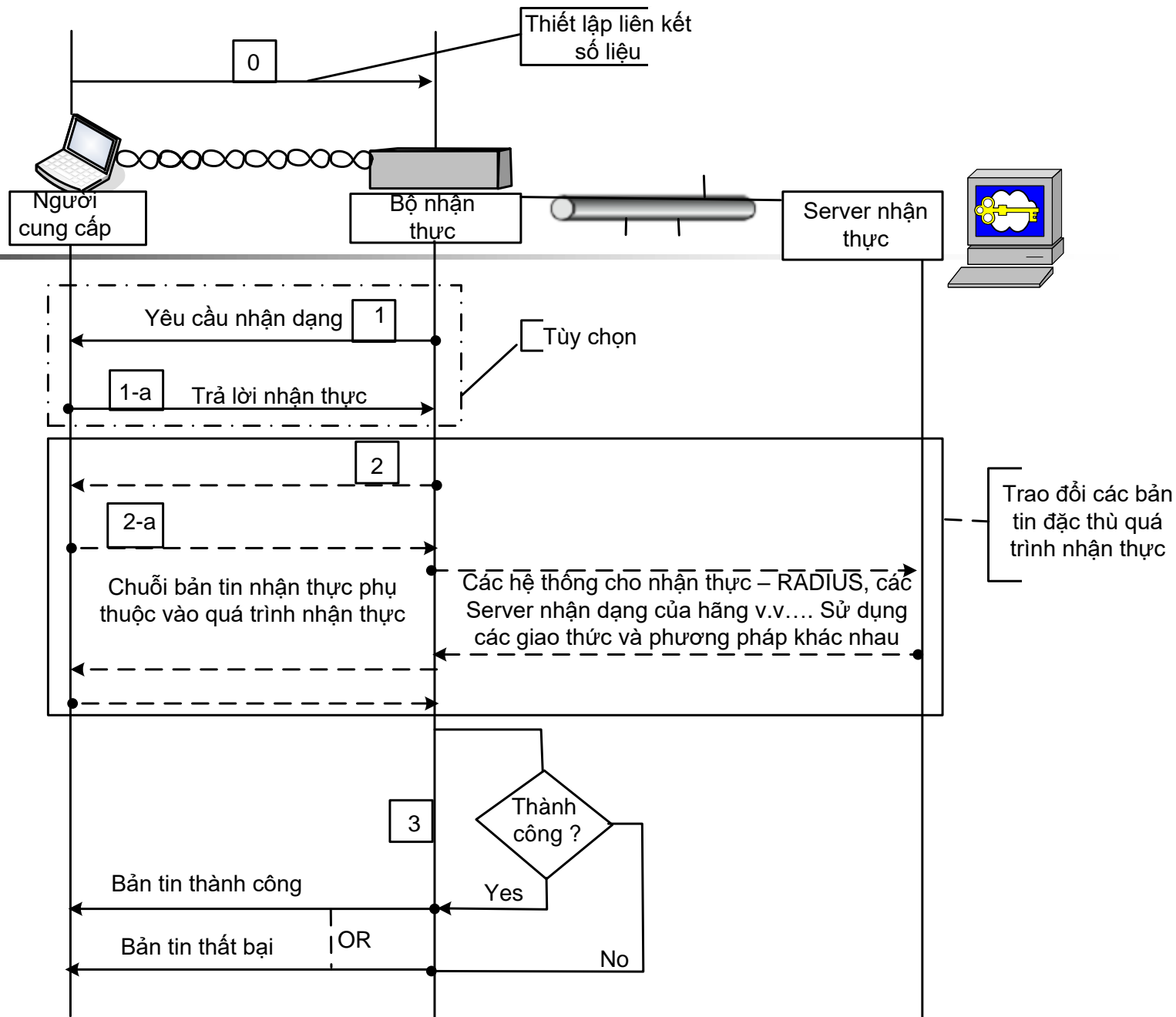




Chế độ Pass- through luồng bản tin EAP



Trao đổi bản tin EAP

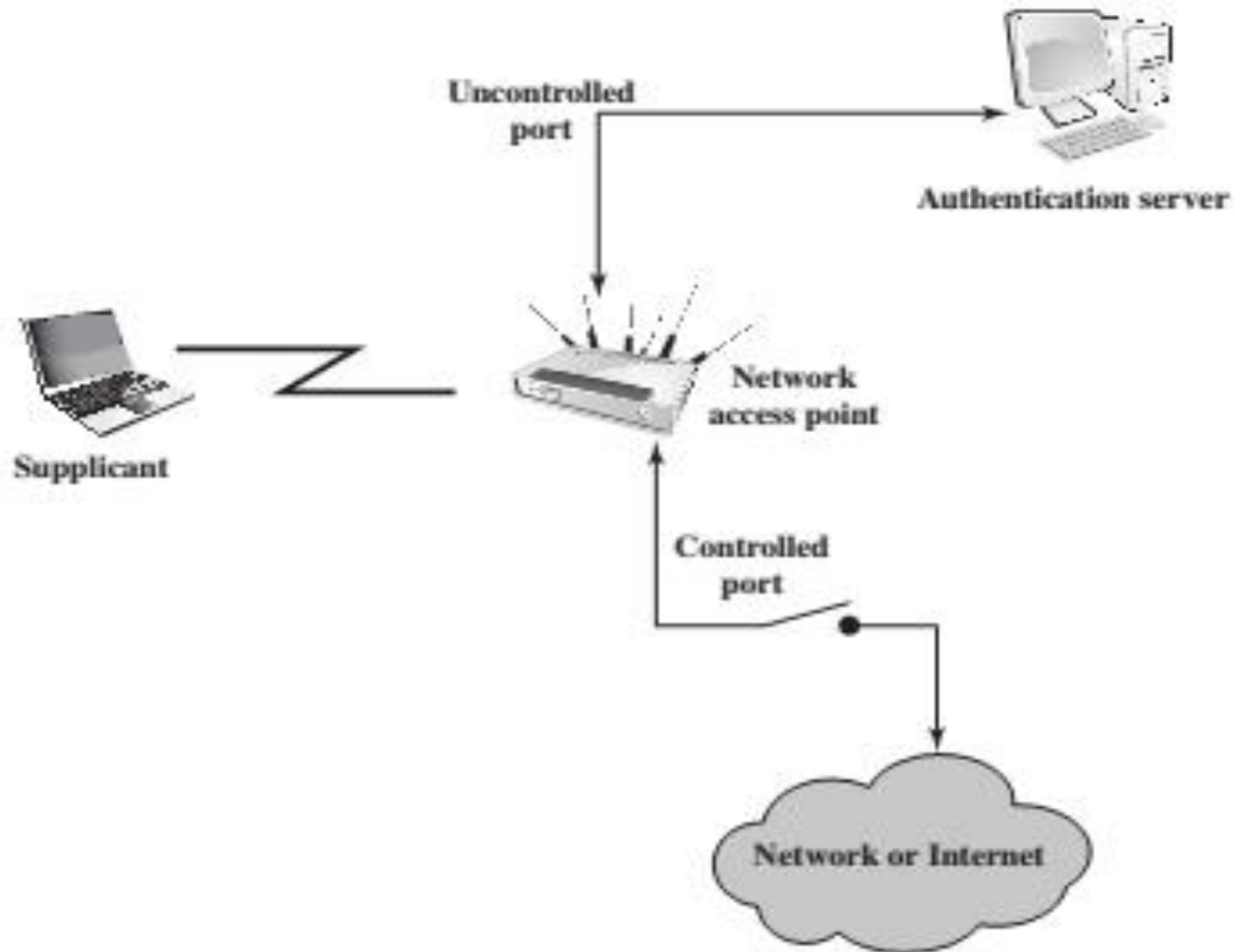




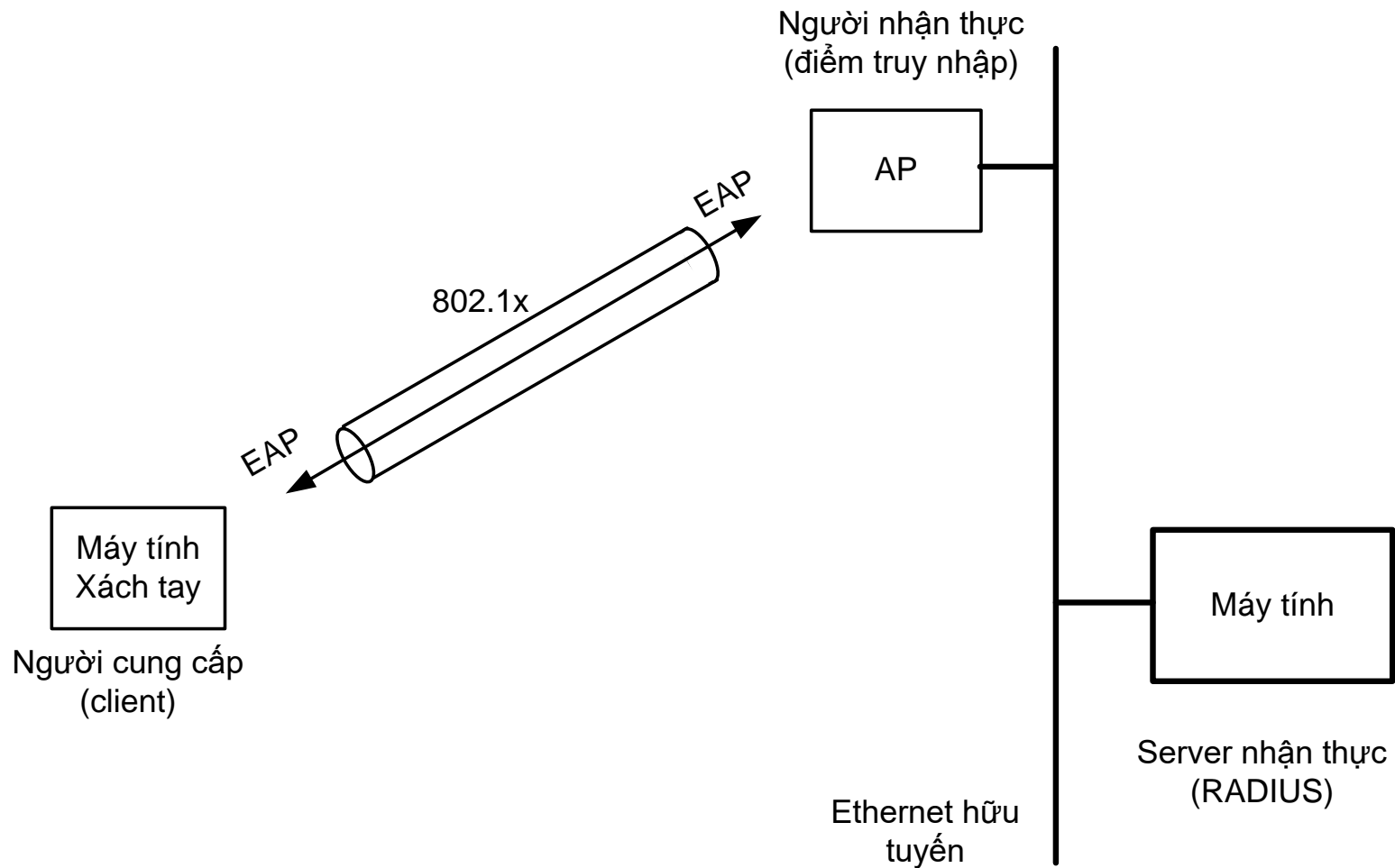
IEEE 802.1x

- ❖ 802.1x là một giao thức cho phép nhận dạng theo cửa (cửa vật lý).
- ❖ 802.1x cho phép đóng tất cửa đối với mọi lưu lượng chừng nào client không được nhận thực thông qua các chứng nhận được lưu trong server (thường là RADIUS server).
- ❖ 802.1x đơn giản là một giao thức trao đổi (EAP: Extensible Authentication Protocol) trên các mạng không dây và hữu tuyến.

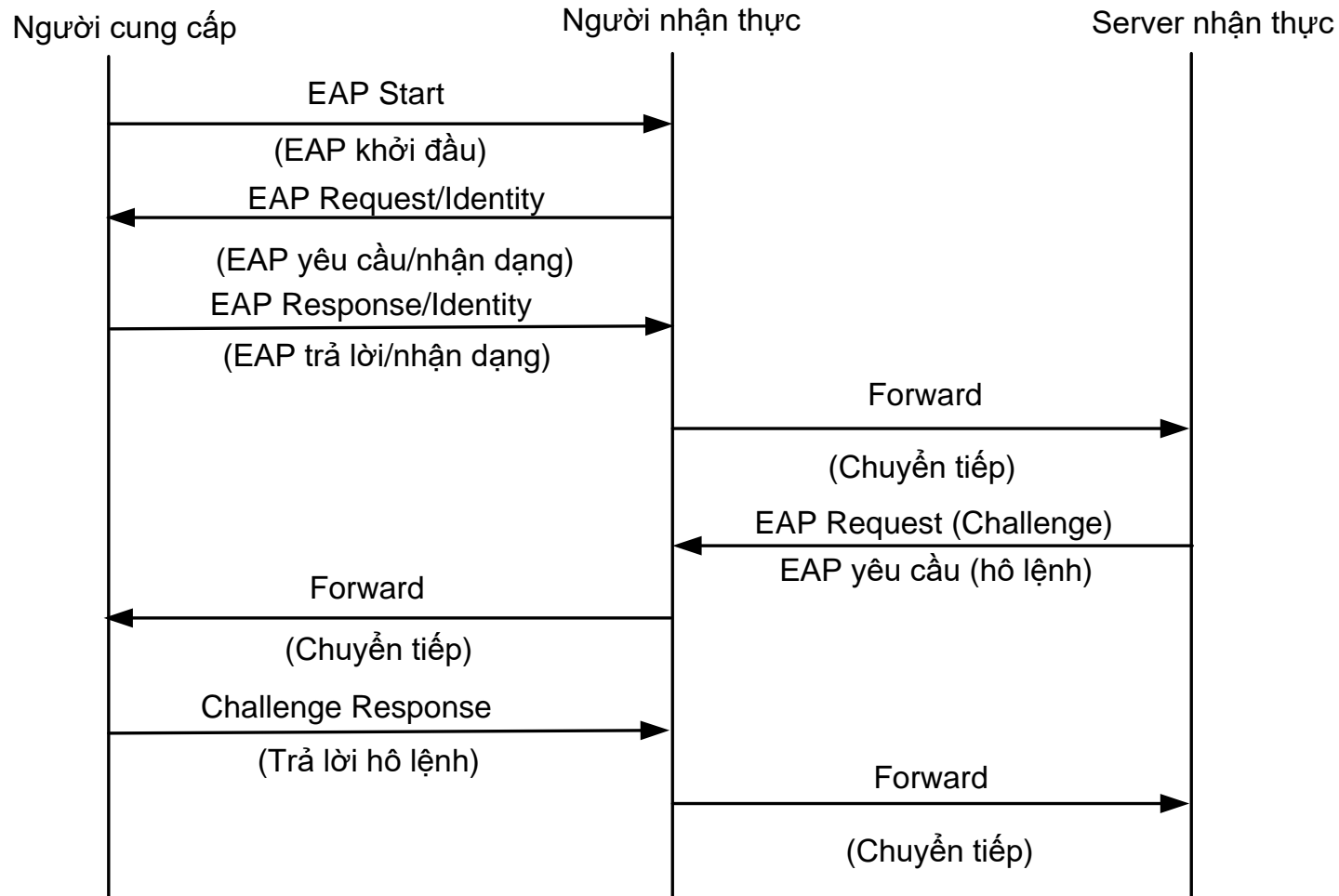
IEEE 802-1X Port-based NAC



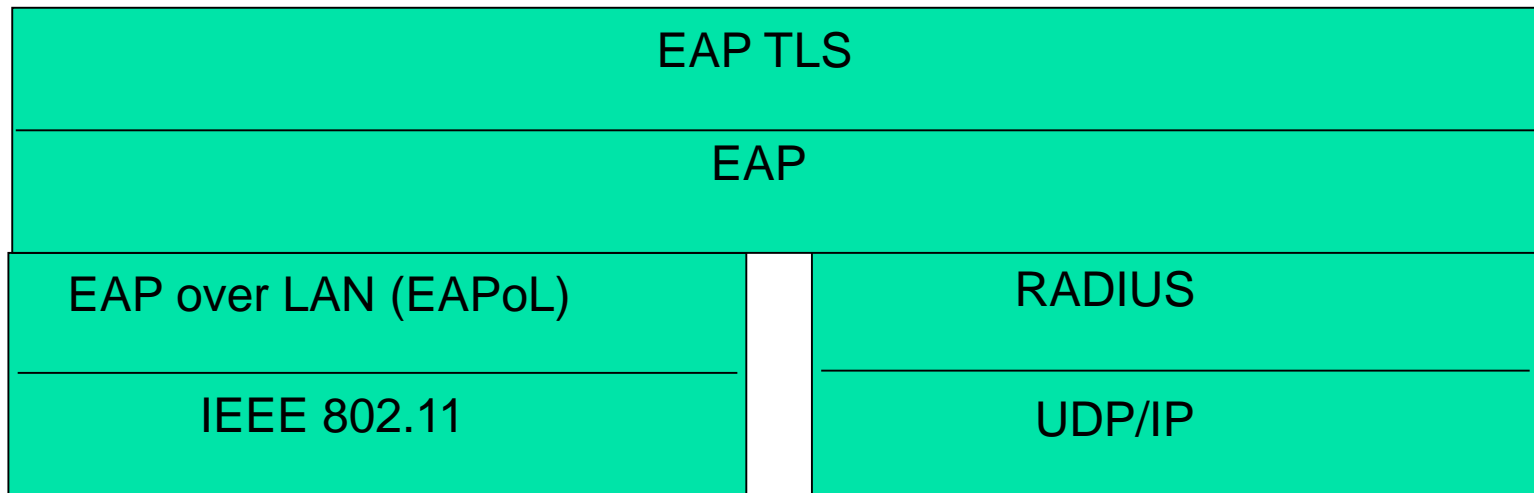
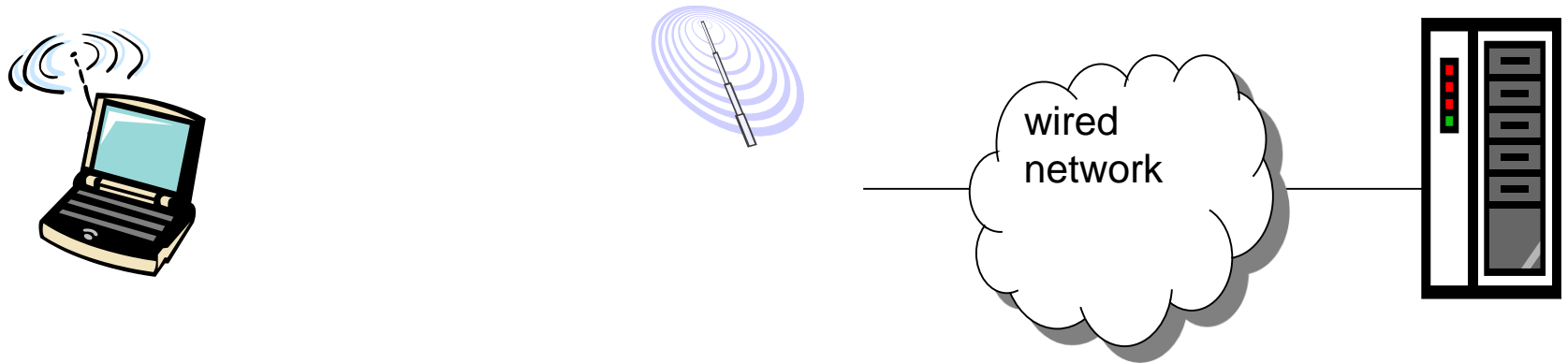
Mô hình 802.1x



Lược đồ nhận thực 802.1x



Giao thức EAPOL trong 802.1X

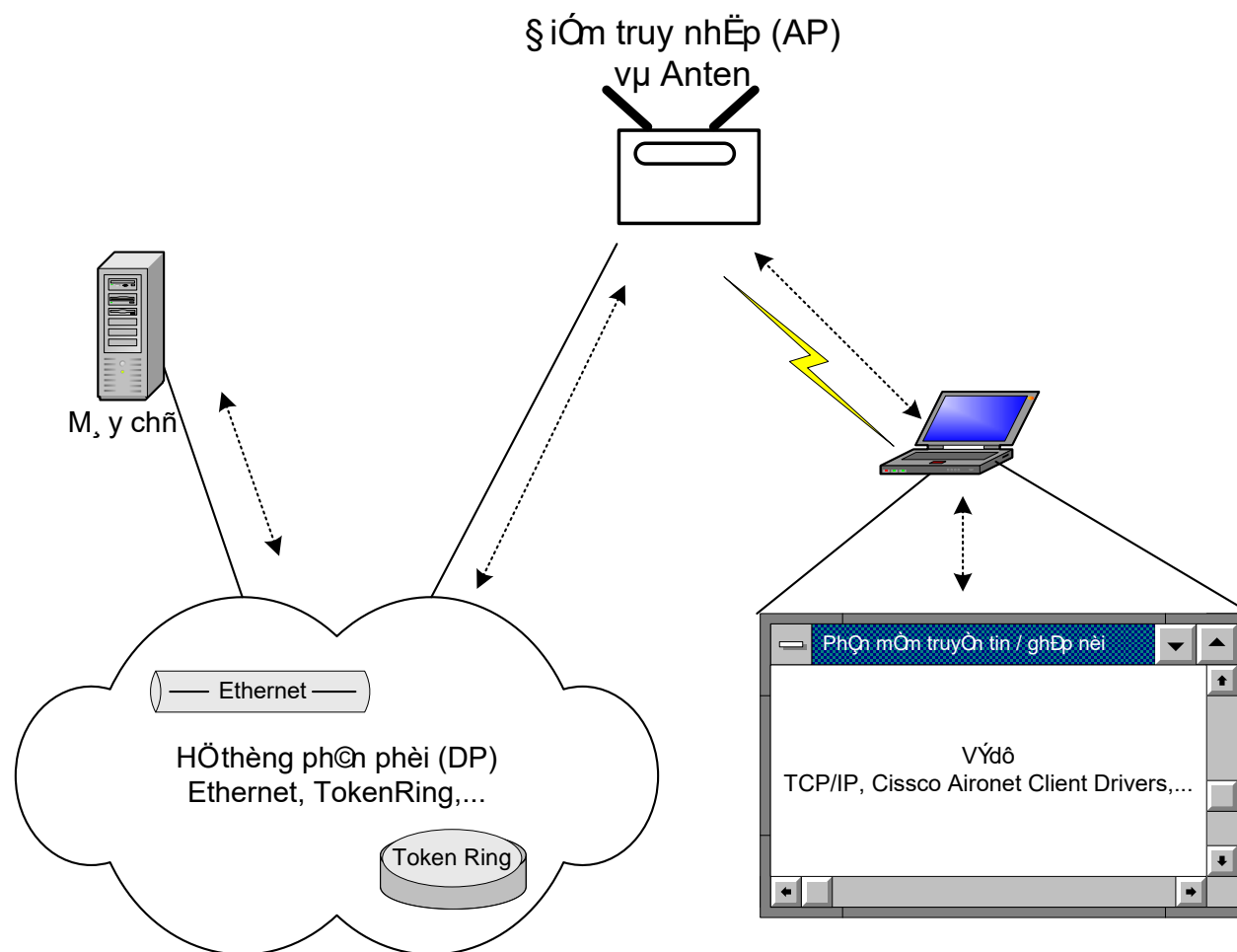




Một số tiêu chuẩn không dây

Công nghệ	Tần số (GHz)	Số liệu (Mbps)	Ứng dụng	Quốc gia
Bluetooth	2,4	0,8	Thoại di động	Toàn cầu
OpenAir	2,4	1,6	Gia đình	Toàn cầu
HomeRF	2,4	10	Gia đình	Toàn cầu
802.11b	2,4	11	Công sở	Bắc Mỹ
802.11a	5	54	Công sở	Bắc Mỹ
HiperLAN1	5	18	Công sở	Châu Âu
HiperLAN2	5	54	Công sở	Châu Âu

Hệ thống WLAN





Nguy cơ an toàn mạng không dây

- Liên kết ngẫu nhiên;
- Liên kết bất hợp pháp;
- Đánh cắp định danh;
- MIM;
- DoS;
- Xâm nhập bản tin vào mạng (network injection);



Giải pháp an toàn mạng không dây

➤ An toàn truyền thông không dây

Kỹ thuật giấu tín hiệu: tắt SSID (service set ID), mật mã SSID, giảm công suất phát vừa đủ, sử dụng an ten định hướng, ...

Mật mã hóa;

➤ Bảo vệ điểm truy nhập không dây

802.1X port-based NAC;

➤ Bảo vệ mạng không dây

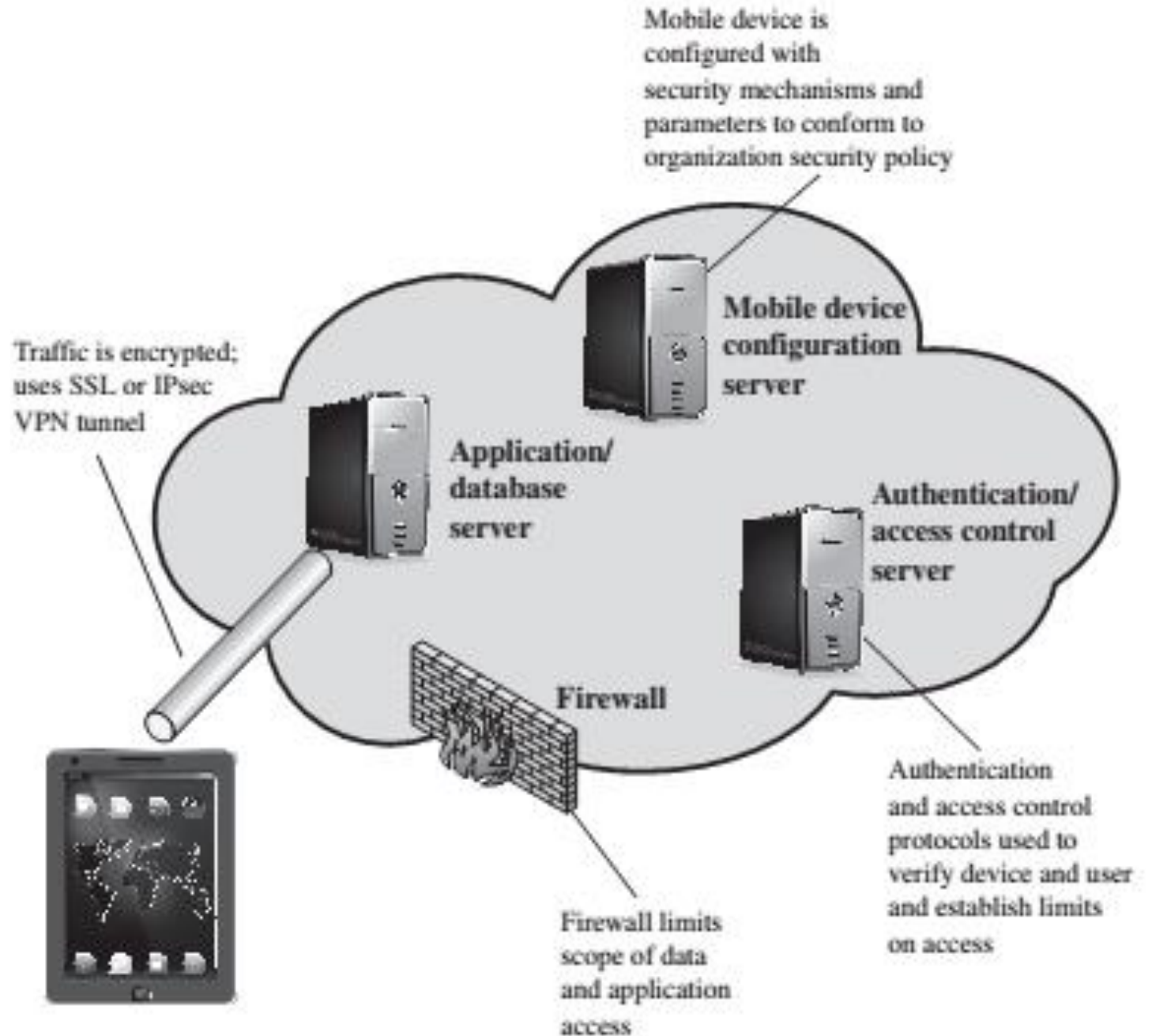
Mật mã hóa lưu lượng;

Tường lửa, phần mềm chống virus và spyware;

Không broadcast ID, thay đổi ID thiết bị;

Quản lý Password

Bảo vệ thiết bị di động

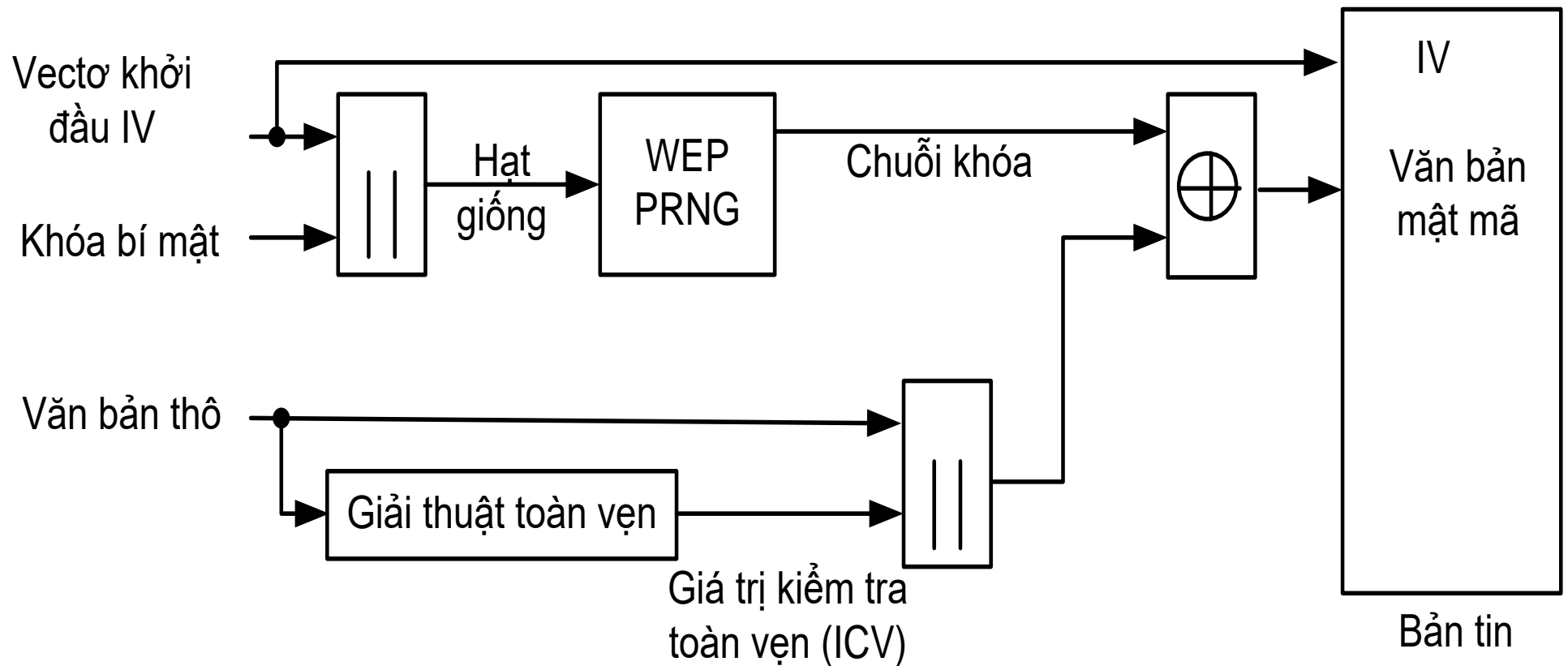




An ninh trong 802.11

- Giao thức bảo mật tương đương hữu tuyến (WEP: Wired Equivalent Privacy) để bảo vệ tín hiệu trên đường truyền vô tuyến: bảo mật, nhận thực, toàn vẹn.
- WPA: Wi-Fi Protected Access dựa trên 802.11i;
- Robust Security Network: RSN tiêu chuẩn cuối của 802.11i;

Mật mã WEP



Mật mã hóa WEP – RC4

Kiểm tra tính toàn vẹn - CRC

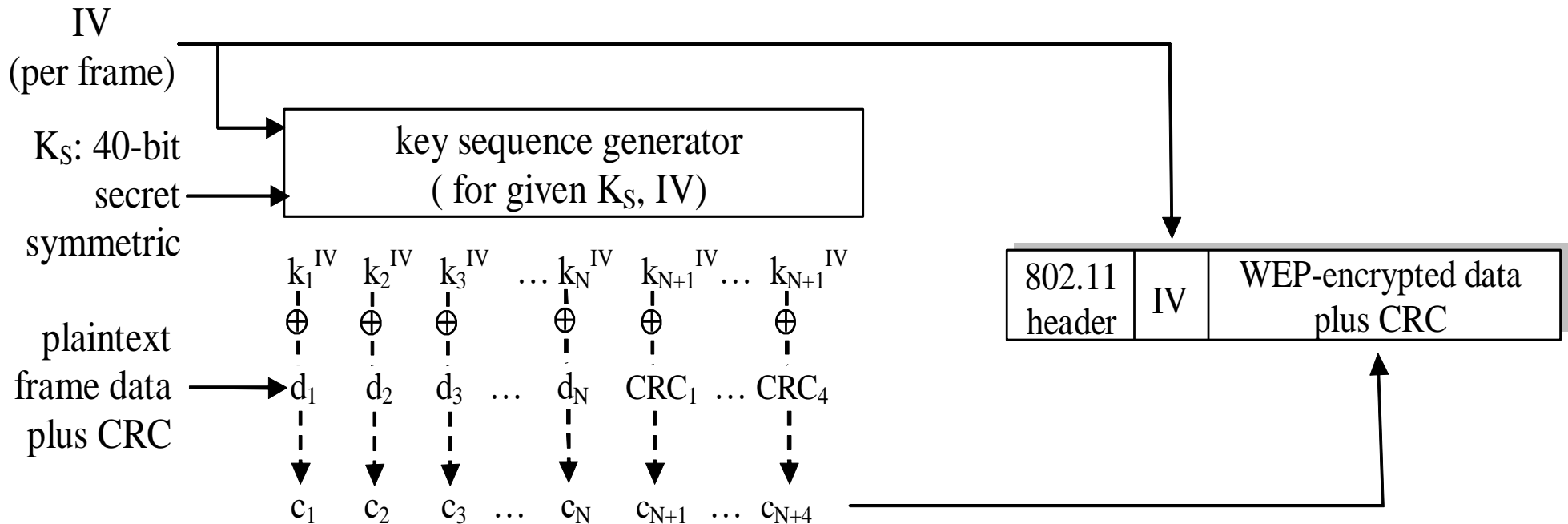
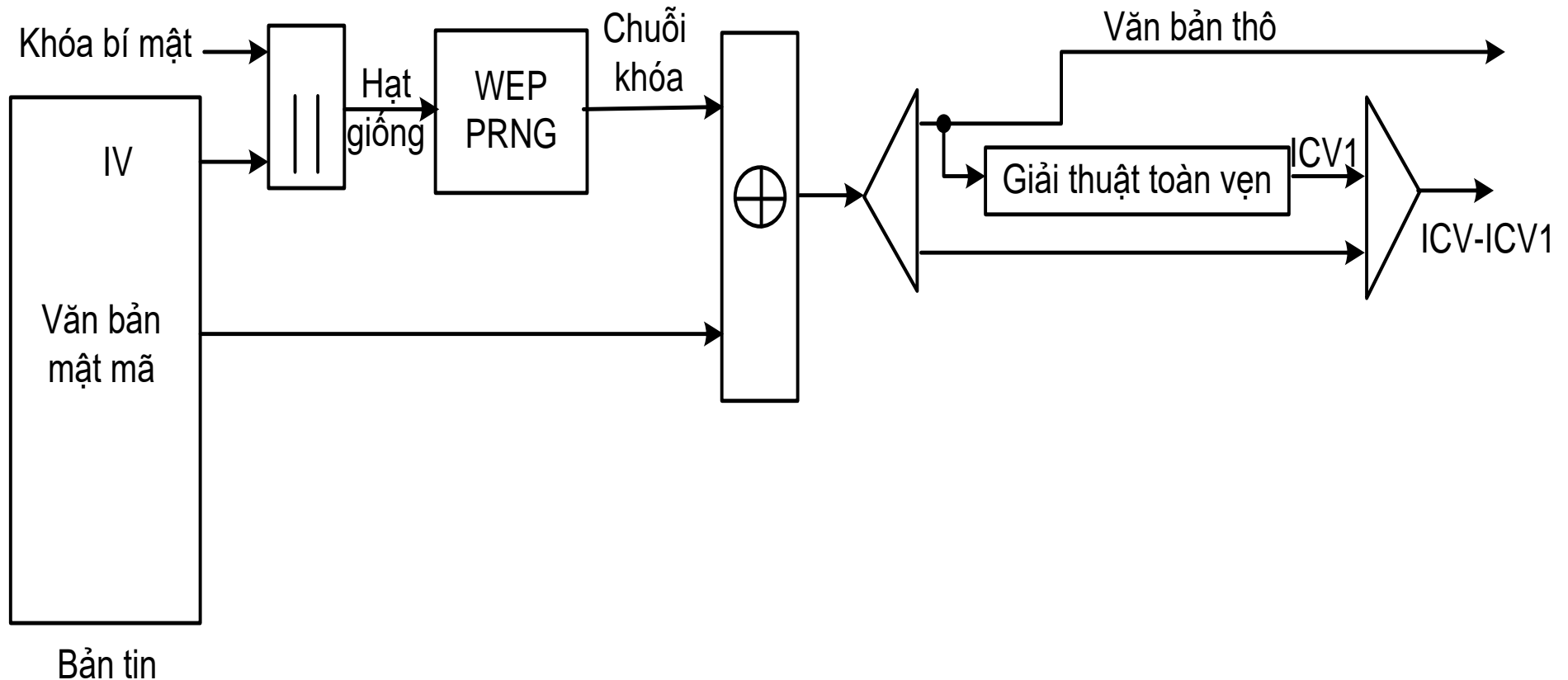
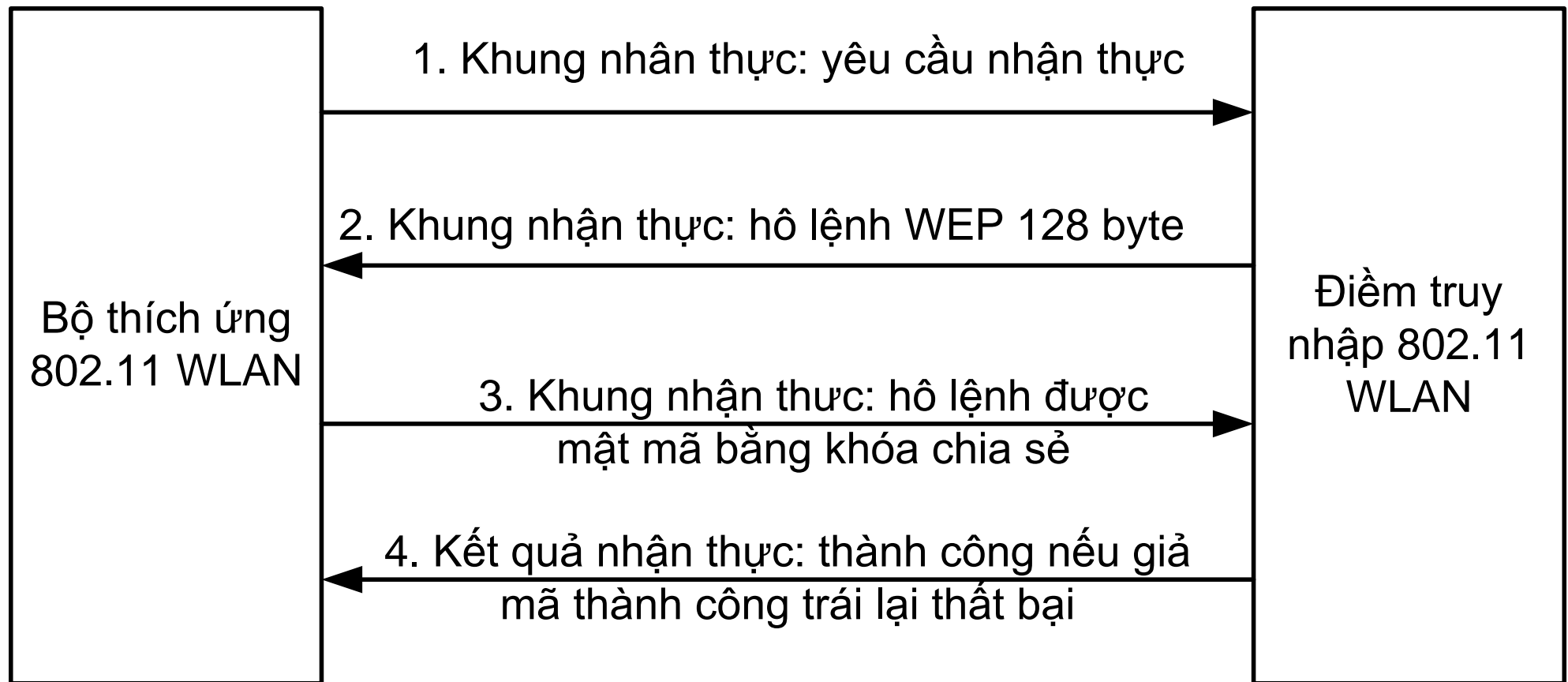


Figure 7.8-new1: 802.11 WEP protocol

Giải mật mã WEP



Nhận thực WEP





Quản lý khóa WEP

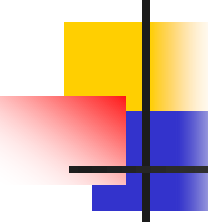
Khóa chia sẻ được đặt trong cơ sở dữ liệu về thông tin quản lý của từng trạm di động. Tiêu chuẩn 802.11 không định nghĩa cách phân phối khóa cho từng trạm mà chỉ cung cấp hai sơ đồ quản lý các khóa WEP trong một WLAN:

- ❖ Một tập bốn khóa chia sẻ chung cho tất cả các trạm bao gồm cả các client không dây và các điểm truy nhập của chúng
- ❖ Một client thiết lập một quan hệ chuyển đổi với một trạm khác.



Các điểm yếu WEP

- Quản lý khóa;
- Xung đột;
- Đóng giả nhận thực;
- Tấn công giải mã: chặn bắt một gói mật mã và sau đó áp dụng một khối lượng rất lớn tính toán;
- Tấn công FMS (**Fluhrer, Mantin and Shamir**): Tấn công FMS dựa trên việc chặn bắt khối lượng lớn lưu lượng mật mã sau đó sử dụng một máy tính công suất tính toán nhỏ cho một giải thuật phá khóa.



Điểm yếu WEP - Quản lý khóa

- ✓ Vậy là cách nào để phân phối khóa giữa các người sử dụng? và điều gì sẽ xảy ra khi số người sử dụng quá lớn.
- ✓ Mỗi người sử dụng phải biết khóa và giữ nó bí mật. Điều gì sẽ xảy ra khi một người để quên máy tính tại công sở hoặc bị đánh cắp: người này phải được cấp khóa mới và phải nhập nó và cấu hình của client.
- ✓ Ngoài ra kẻ tấn công có thể lấy cắp khóa này từ một phiên và sử dụng nó để giải mã các phiên khác vì mọi người đều sử dụng cùng một khóa.



Điểm yếu WEP – vấn đề xung đột

- ❑ Nếu ta chọn IV một cách ngẫu nhiên (số IV $2^{24}-1$) thì sau vài giờ IV sẽ lặp. Khi một IV được sử dụng lại, ta gọi đây là một xung đột.
- ❑ Khi xảy ra một xung đột, tổ hợp giữa khóa bí mật và IV được sử dụng lặp sẽ tạo ra một luồng khoá đã được sử dụng trước đây. Vì IV được phát đi ở dạng văn bản thô một kẻ tấn công có thể theo dõi tất cả lưu lượng và xác định thời điểm xảy ra xung đột để thực hiện tấn công luồng khoá.
- ❑ Tấn công luồng khoá là một phương pháp rút ra luồng khoá bằng cách phân tích hai gói được rút ra từ cùng một IV. Tấn công này dựa trên nguyên tắc sau: tổng modul 2 của hai văn bản đã mật mã bằng tổng modul 2 của hai văn bản thô. Vì thế nếu kẻ tấn công biết được hai văn bản mật mã (từ theo dõi lưu lượng) và một văn bản thô thì hẳn có thể biết được văn bản thô thứ hai.



Điểm yếu WEP – tấn công phá khóa

- Người tấn công yêu cầu người sử dụng mã hóa bản plaintext đã biết $d_1 d_2 d_3 d_4 \dots$
- Người tấn công thu được: $c_i = d_i \text{ XOR } k_i^{\text{IV}}$
- Người tấn công biết $c_i d_i$, có thể tính k_i^{IV}
- Người tấn công biết khóa mã $k_1^{\text{IV}} k_2^{\text{IV}} k_3^{\text{IV}} \dots$
- Nếu lần sau sử dụng lại IV, người tấn công có thể giải mã!



Điểm yếu WEP – giả mạo nhận thực

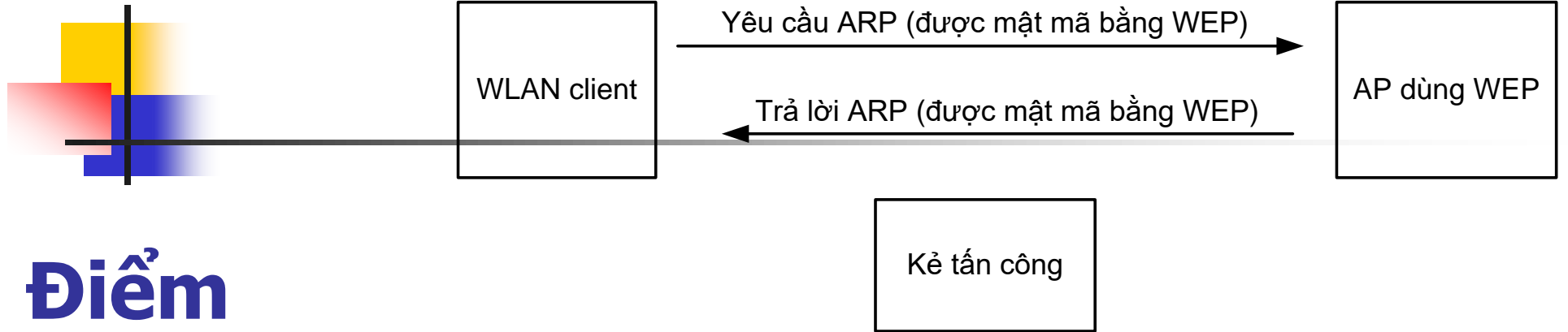
- Kẻ tấn công quan sát quá trình đàm phán nhận thực, nó sẽ biết được văn bản thô và văn bản mật mã liên quan (trả lời hô lệnh).
- Sử dụng phương pháp làm giả bản tin, kẻ tấn công có thể rút ra được khoá luồng và yêu cầu nhận thực từ AP sau đó sử dụng khóa luồng này cùng với văn bản hô lệnh để tạo ra trả lời hợp lệ.
- Khi này kẻ tấn công sẽ được AP nhận thực ngay cả khi kẻ này không biết được khóa WEP.



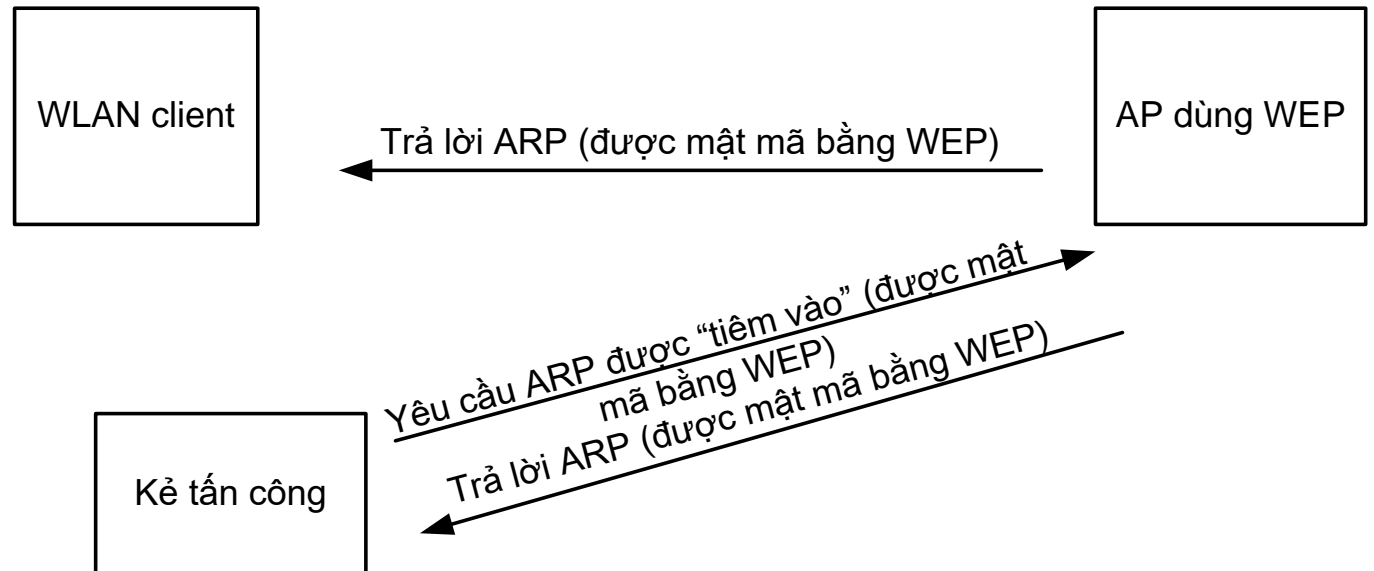
Điểm yếu WEP – tấn công giải mã

- Khóa bí mật 40 bit -> phá khóa trong vòng 1 phút.
- Giải pháp: Tăng độ dài khóa lên 104 bit.

a) Kẻ tấn công chặn bắt yêu cầu ARP dựa trên kích thước gói 28 byte biết trước



b) kẻ tấn công phát lại yêu cầu ARP nhiều lần để nhận được đủ lưu lượng cho tấn công FMS



**Điểm
yếu
WEP –
tấn
công
FMS**

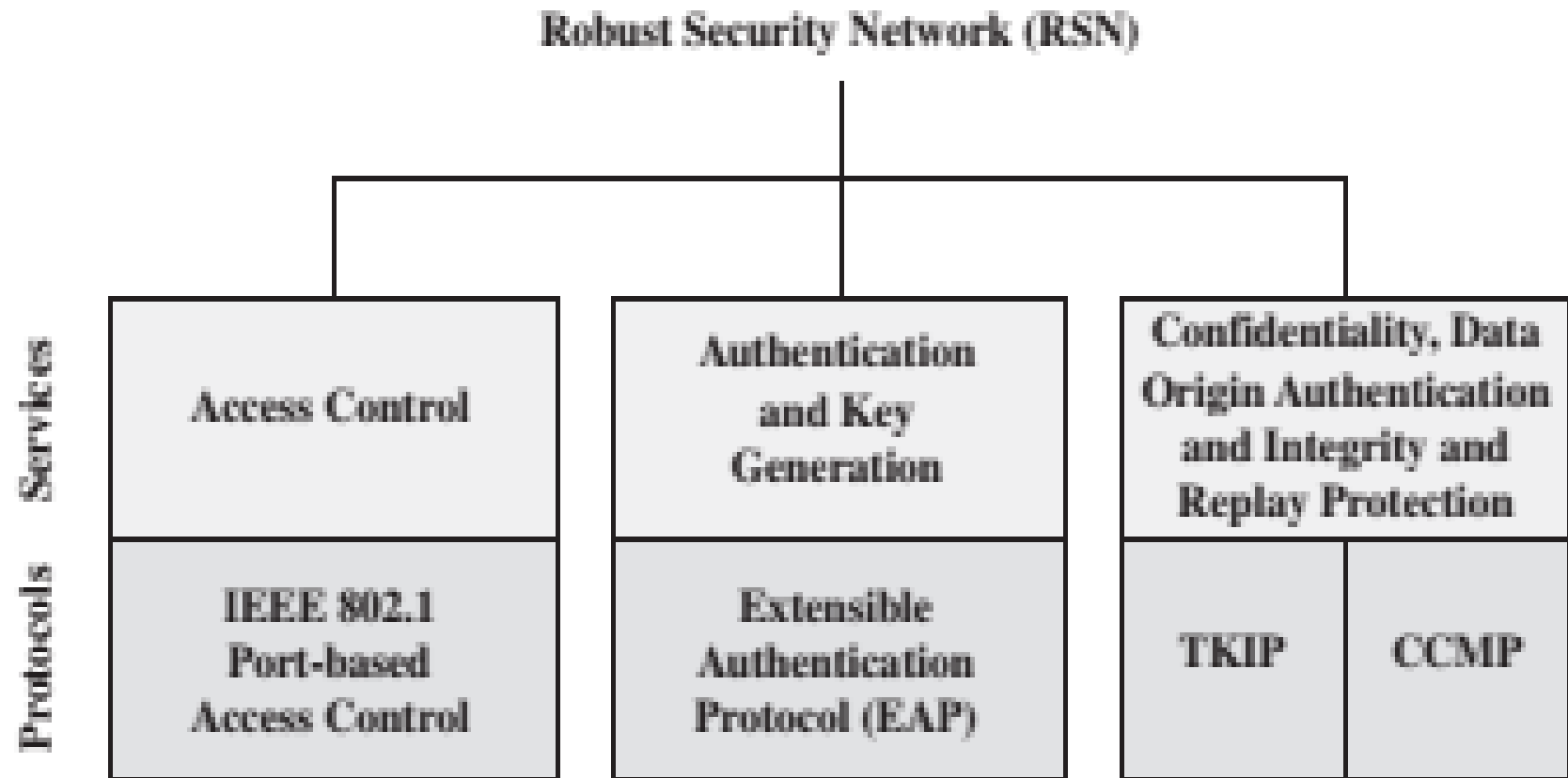


Giải pháp an ninh 802-11i

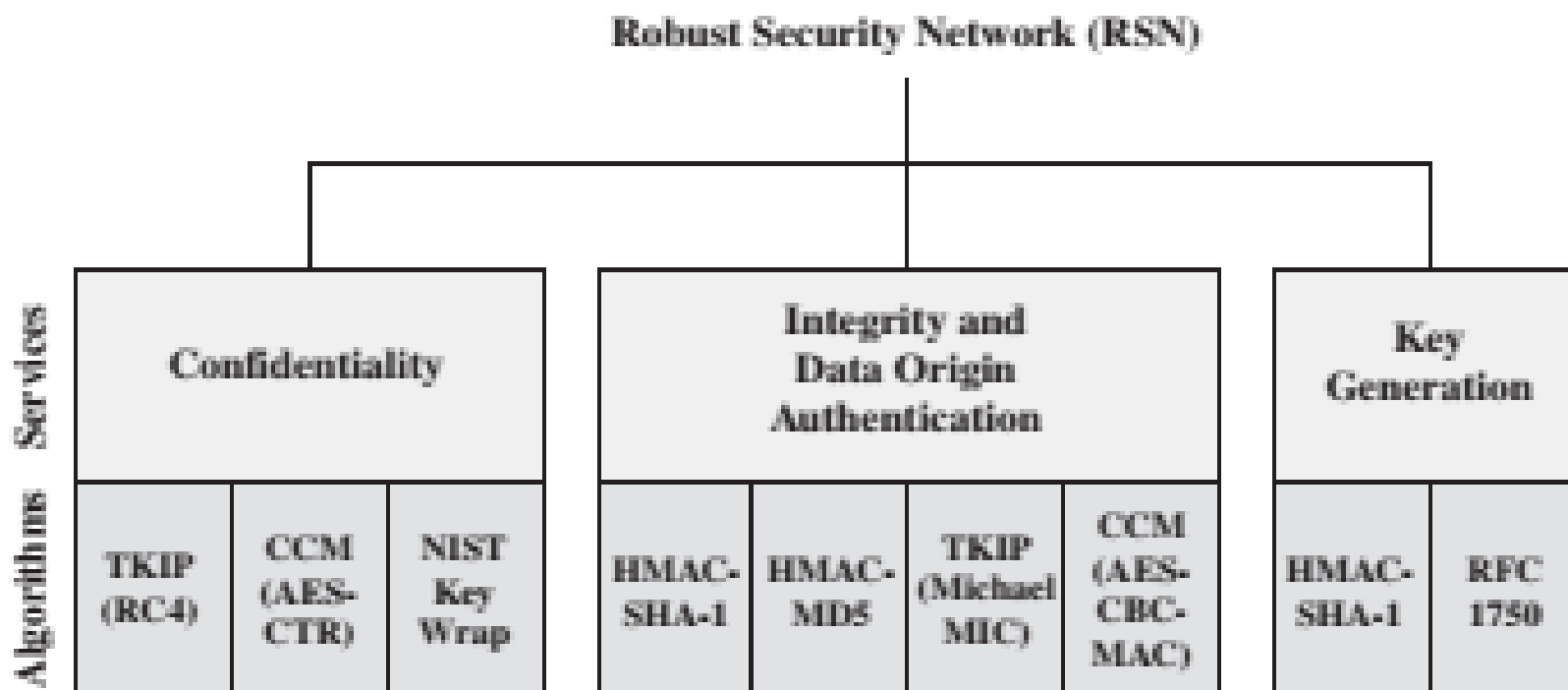
- Mã hóa bằng các kỹ thuật mạnh hơn (TKIP, CCMP, AES).
- Phân phối khóa
- Sử dụng nhận thực bằng máy chủ nhận thực tách biệt với AP (nhận thực bằng mô hình 802.1x)



Dịch vụ và giao thức RSN



Dịch vụ và giải thuật RSN



(b) Cryptographic algorithms

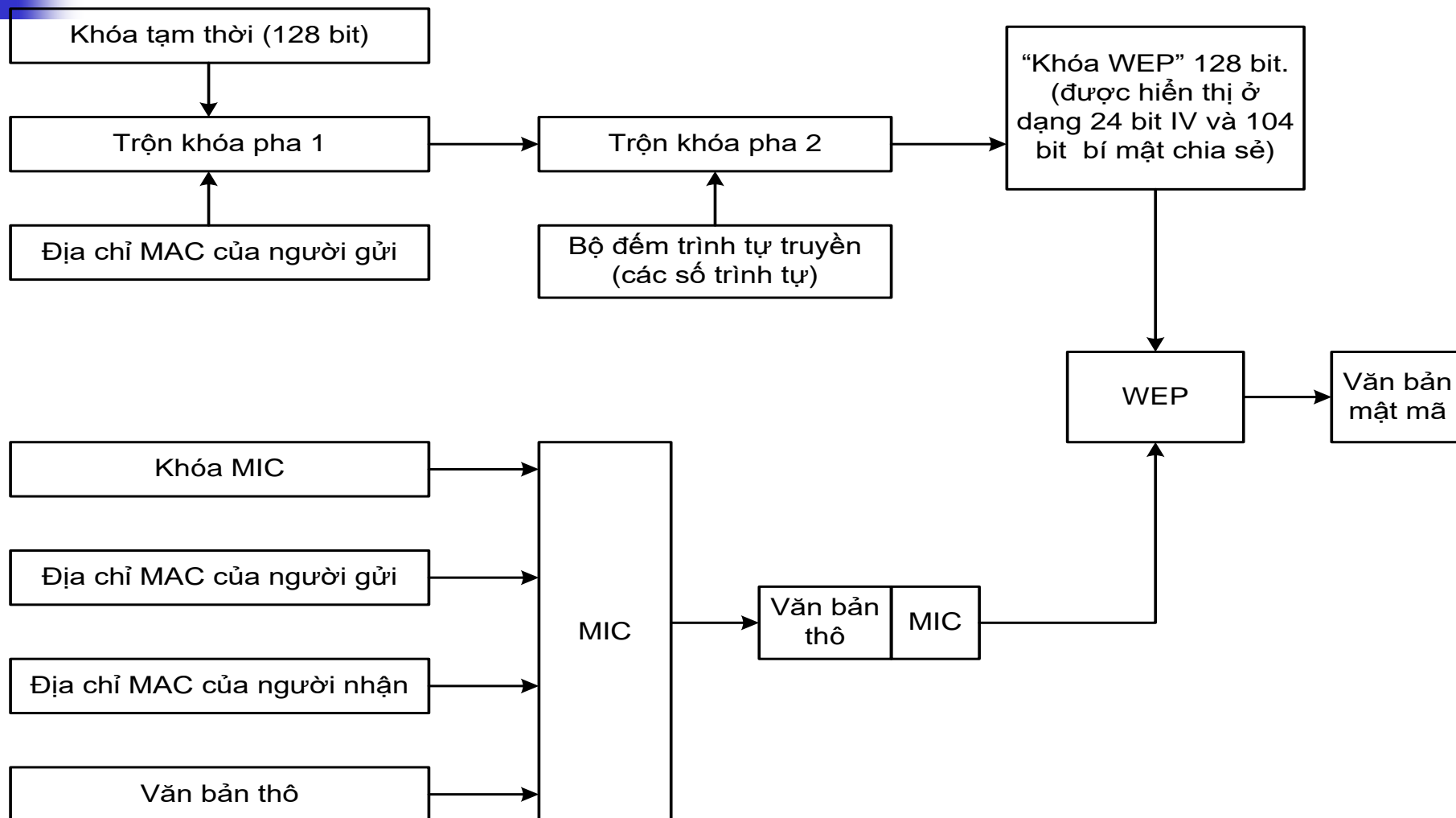
- CBC-MAC ■ Cipher Block Chaining Message Authentication Code (MAC)
- CCM ■ Counter Mode with Cipher Block Chaining Message Authentication Code
- CCMP ■ Counter Mode with Cipher Block Chaining MAC Protocol
- TKIP ■ Temporal Key Integrity Protocol



Temporal Key Identity Protocol - TKIP

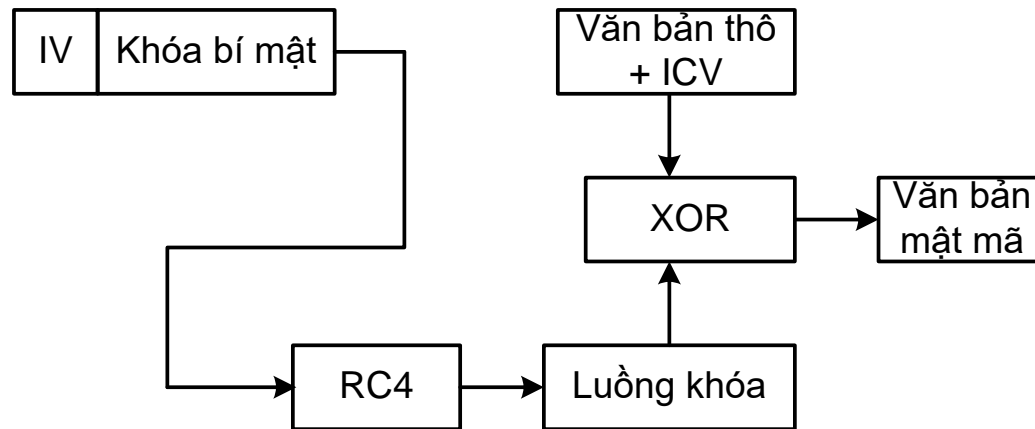
- Tấn công phát lại: có thể sử dụng các IV không theo thứ tự.
- Các tấn công giả mạo: ICV (integrity check value) sử dụng 32 bit CRC là tuyến tính và có thể điều khiển.
- Các tấn công xung đột khóa: các xung đột IV
- Các tấn công khóa yếu: bộ mật mã luồng RC4 bị xâm phạm do các tấn công FMS (AirSnort, WEPCrack...)

Mật mã hóa TKIP

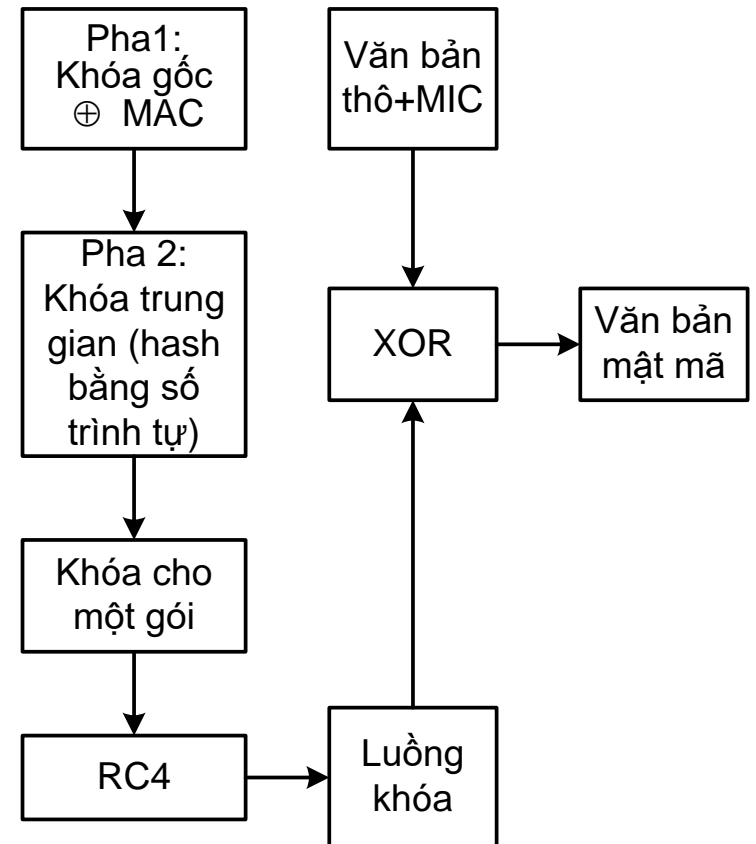


Hàm trộn khóa TKIP

WEP



TKIP





Cải tiến WEP - TKIP

- Khóa mật mã: 128 bit.
- Mã toàn vẹn bản tin MIC (message integrity code): Khóa toàn vẹn số liệu 64 bit, sử dụng hàm hash.
- Loại bỏ xung đột: IV tăng từ 24 bit lên 48 bit; Bộ đếm trình tự truyền.



Các bước vận hành của 802.11i

- 1) Phát hiện: AP thông báo chính sách an toàn, STA xác định AP liên kết, lựa chọn dạng xác thực và mật mã hóa;
- 2) Xác thực: AP và STA xác thực lẫn nhau;
- 3) Quản lí và phân phối khóa: quá trình tạo khóa tại AP và STA;
- 4) Truyền tải dữ liệu được bảo vệ;
- 5) Kết thúc kết nối.



Phát hiện

Nhận biết, thỏa thuận kĩ thuật an toàn, mở liên kết cho truyền thông dữ liệu.

➤ Kĩ thuật an toàn: Giao thức bảo mật và toàn vẹn MPDU (WEP, TKIP, CCMP,...), phương pháp xác thực, giải pháp quản lí khóa AKM (802.11X, Pre-shared Key PSK).

➤ Trao đổi MPDU: phát hiện mạng và khả năng an toàn, mở hệ thống xác thực (trao đổi ID), liên kết (thỏa thuận kĩ thuật an toàn).



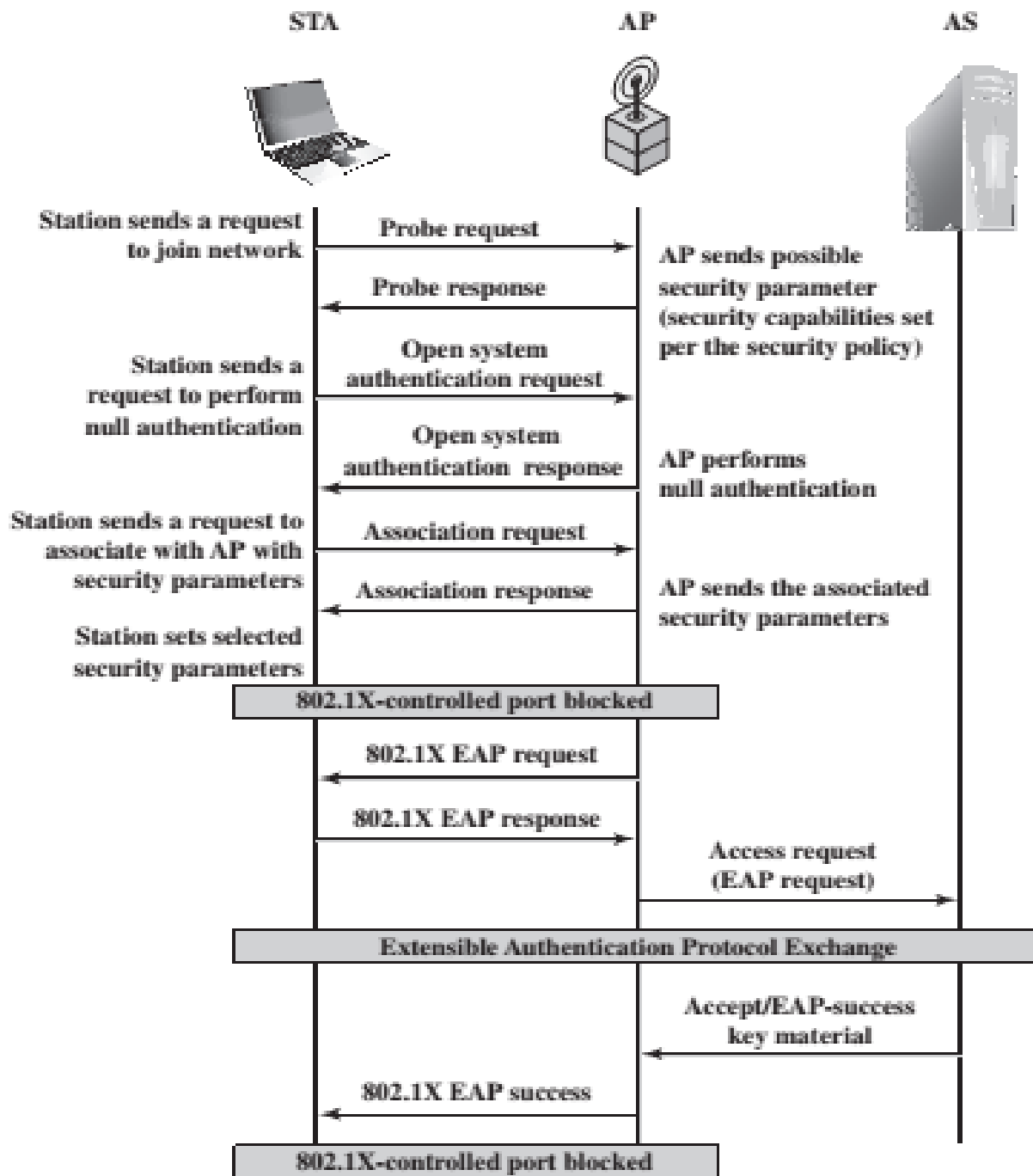
Xác thực

Giải pháp 802.1X port-based NAC.

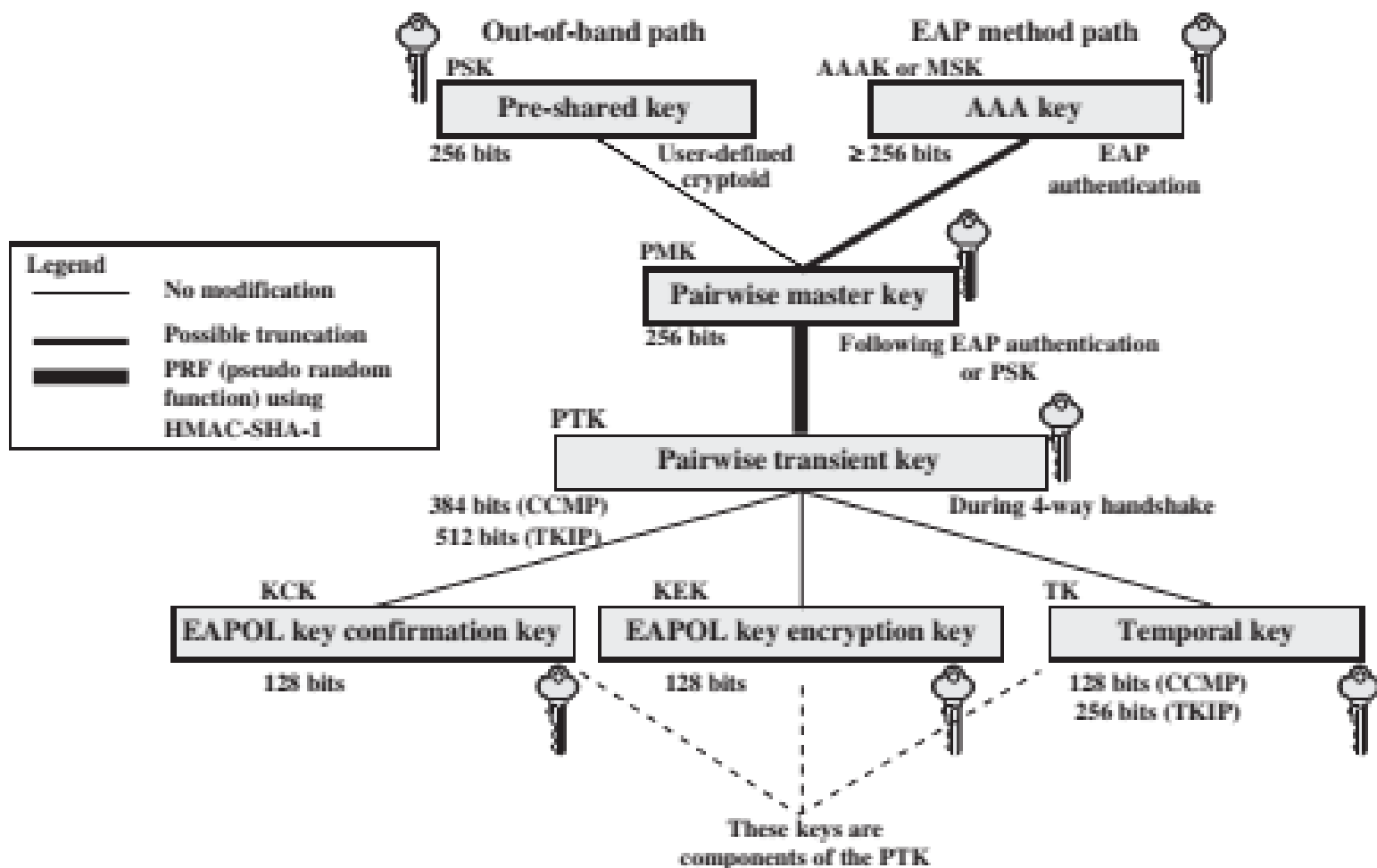
➤ Trao đổi MPDU: kết nối với AS (gửi yêu cầu đến AS), trao đổi EAP (xác thực giữa STA và AS), phân phối khóa an toàn (AS tạo khóa chủ MSK/khóa AAK gửi cho STA).

➤ Trao đổi EAP:
STA-AP: EAPOL;
AP-AS: RADIUS.

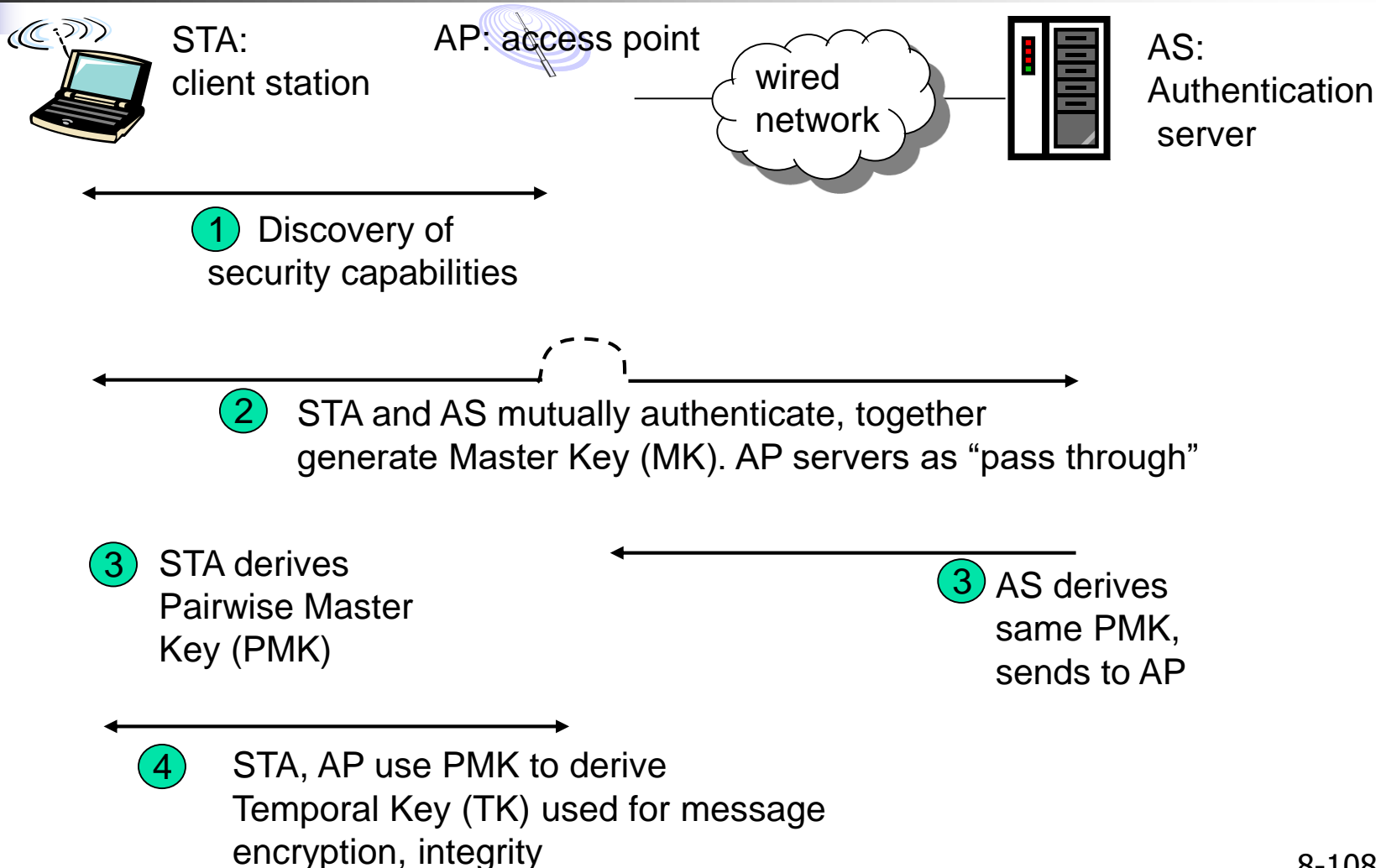
Phát hiện Xác thực và Liên kết



Quản lí khóa



Ví dụ hoạt động đơn giản của 802.11i





Truyền tải dữ liệu

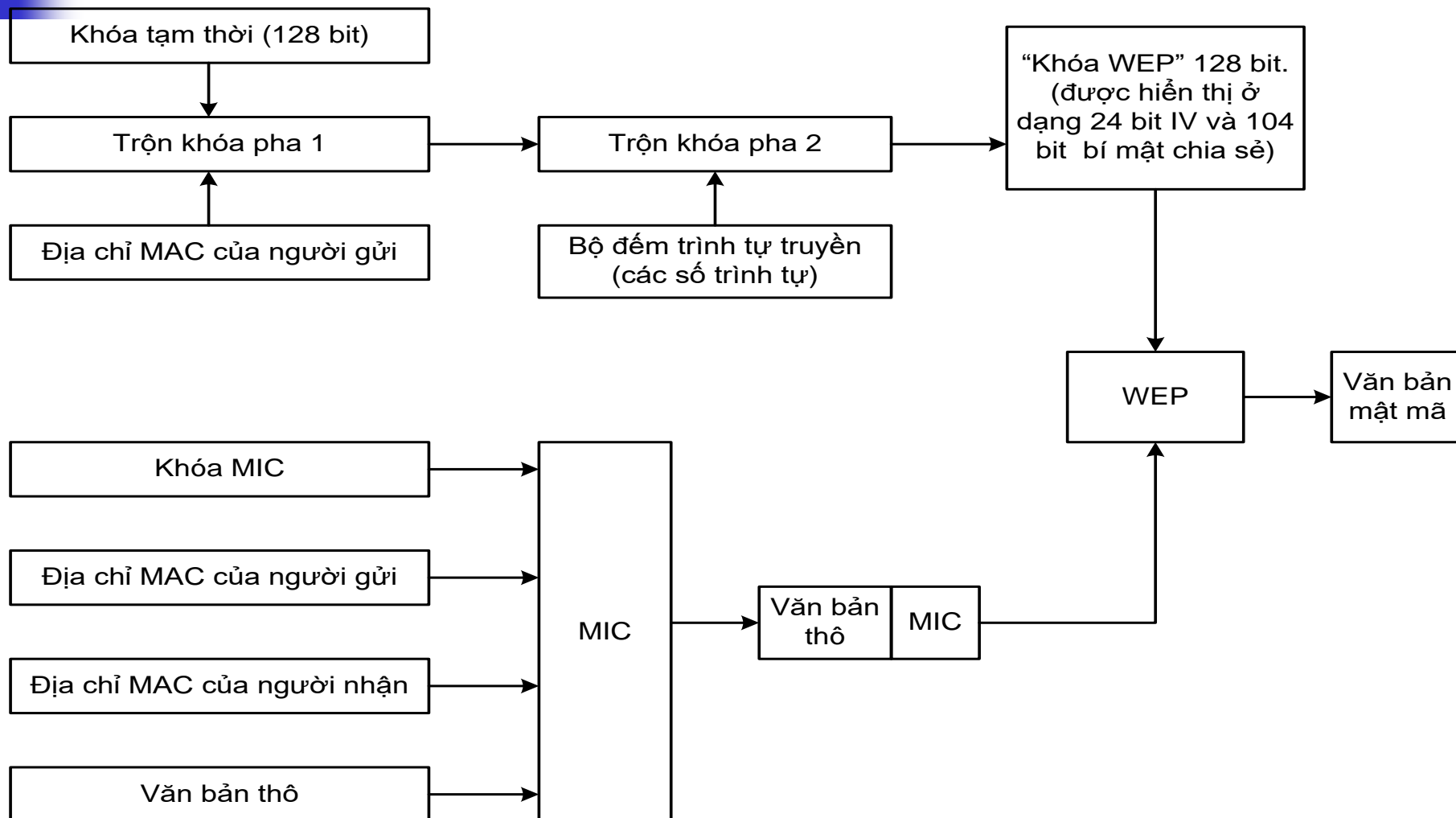
- Giao thức định danh khóa tạm thời: Temporal Key Identity Protocol (TKIP).
- Giao thức Counter Mode CBC-MAC.



Cải tiến WEP - TKIP

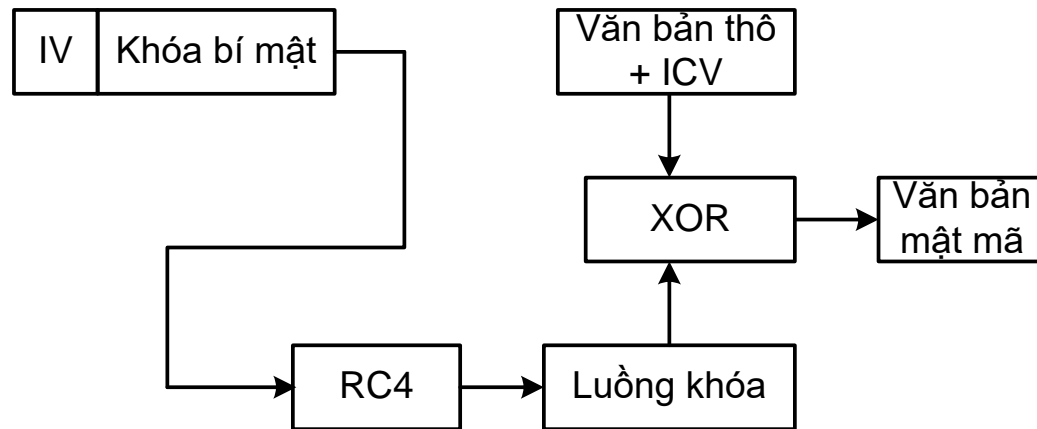
- Khóa mật mã: 128 bit.
- Mã toàn vẹn bản tin MIC (message integrity code): Khóa toàn vẹn số liệu 64 bit, sử dụng hàm hash.
- Loại bỏ xung đột: IV tăng từ 24 bit lên 48 bit; Bộ đếm trình tự truyền.

Mật mã hóa TKIP



Hàm trộn khóa TKIP

WEP



TKIP

