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

GIAO THỨC AN TOÀN MẠNG

Bài 4.1. Giới thiệu về VPN

TS. Trần Thị Lượng

1. Tổng quan về VPN
2. Giới thiệu IPsec
3. Tổ hợp an toàn SA
4. Giao thức AH

Mục tiêu bài học

❑Kiến thức

- Nắm được khái niệm "mạng riêng ảo" và các loại mạng riêng ảo
- Hiểu được lợi ích của mạng riêng ảo
- Nắm được các loại giao thức VPN
- Hiểu được cơ chế hoạt động của giao thức AH

❑Kỹ năng

- Phân tích hoạt động của giao thức AH ở các chế độ Transport hoặc Tunnel qua việc chặn thu lưu lượng mạng.

Tài liệu tham khảo

1. Giáo trình "Giao thức an toàn mạng máy tính"// Chương 3 "**Các giao thức bảo mật mạng riêng ảo**", năm 2013.
2. Giáo trình "An toàn mạng riêng ảo", năm 2007.
3. William Stalling, **Cryptography and Network Security Principles and Practice (5e)//Part 3, chapter 16 – pp. 483- 527**, Prentice Hall, 2011

1. Tổng quan về VPN
2. Giới thiệu IPsec
3. Tổ hợp an toàn SA
4. Giao thức AH

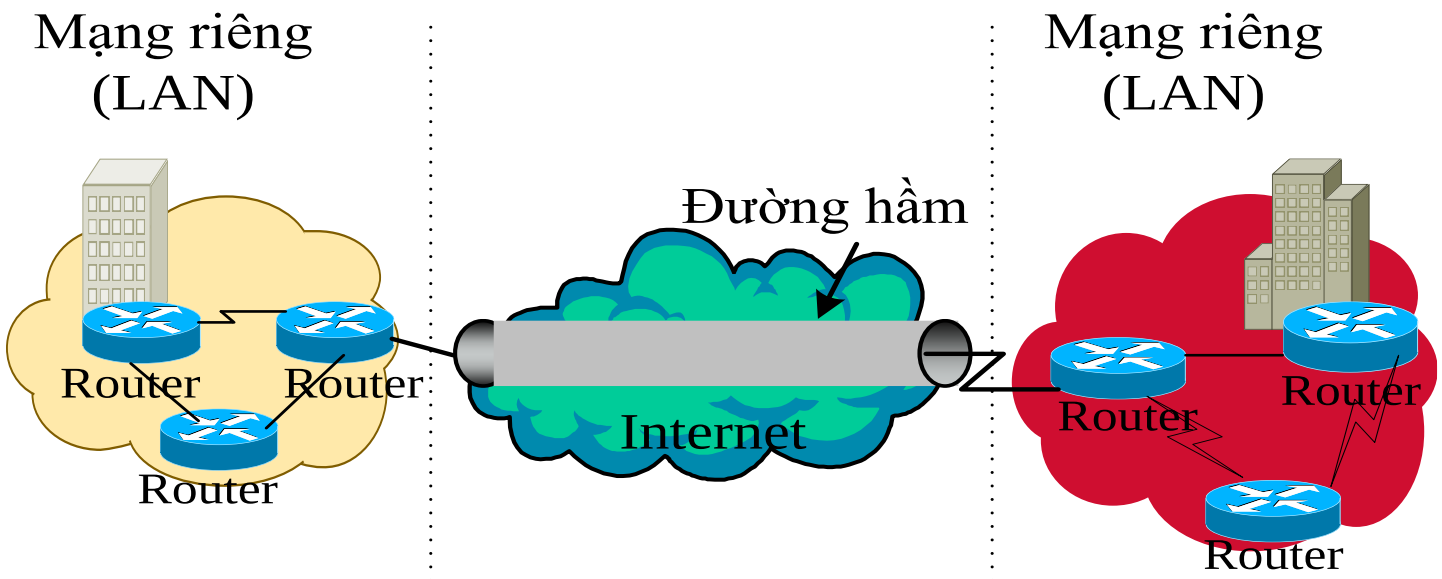
Mạng riêng

❑Mạng riêng (Private Network)

- Là mạng được xây dựng, vận hành bởi cá nhân, tổ chức cho mục đích riêng
- Là một tổ hợp trang thiết bị mạng tạo thành một vùng mạng riêng biệt nằm hoàn toàn dưới sự kiểm soát của chủ sở hữu
- Sử dụng cho: home LAN, office LAN và enterprise LAN
- Sử dụng dải IP dành riêng: 10.0.0.0/8, 172.16.0.0/12 và 192.168.0.0/16
- Lưu lượng của mạng riêng được cô lập không thể đi qua mạng chung (nếu không có sự chuyển đổi địa chỉ)

Mạng riêng ảo

- 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.



Mạng riêng ảo

- 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 riêng ảo

- Là mạng mà trong đó những phần tài nguyên dùng chung, nhưng có những đặc điểm của mạng riêng.
  - Toàn quyền quản trị
  - Cô lập lưu lượng
  - Sử dụng dải địa chỉ IP dành riêng
- VPN là một khái niệm, không phải là một giao thức. Nó có thể được hiện thực hóa bằng các giao thức khác nhau

Mạng riêng ảo

❑Ví dụ

- Mạng VLAN
- Mạng sử dụng đường leased line
- Mạng MPLS VPN
- Mạng IPsec VPN, SSL VPN...

- VPN là bất kỳ công nghệ nào mà cho phép **cô lập lưu lượng** của một chủ thể qua một cơ sở hạ tầng mạng dùng chung.
- VPN có thể sử dụng mật mã hoặc không.

Mạng riêng ảo: Phân loại

Phân loại theo chức năng

- Trusted VPN: MPLS VPN
- Secure VPN: IPsec
- Hybrid VPN: GRE with IPsec

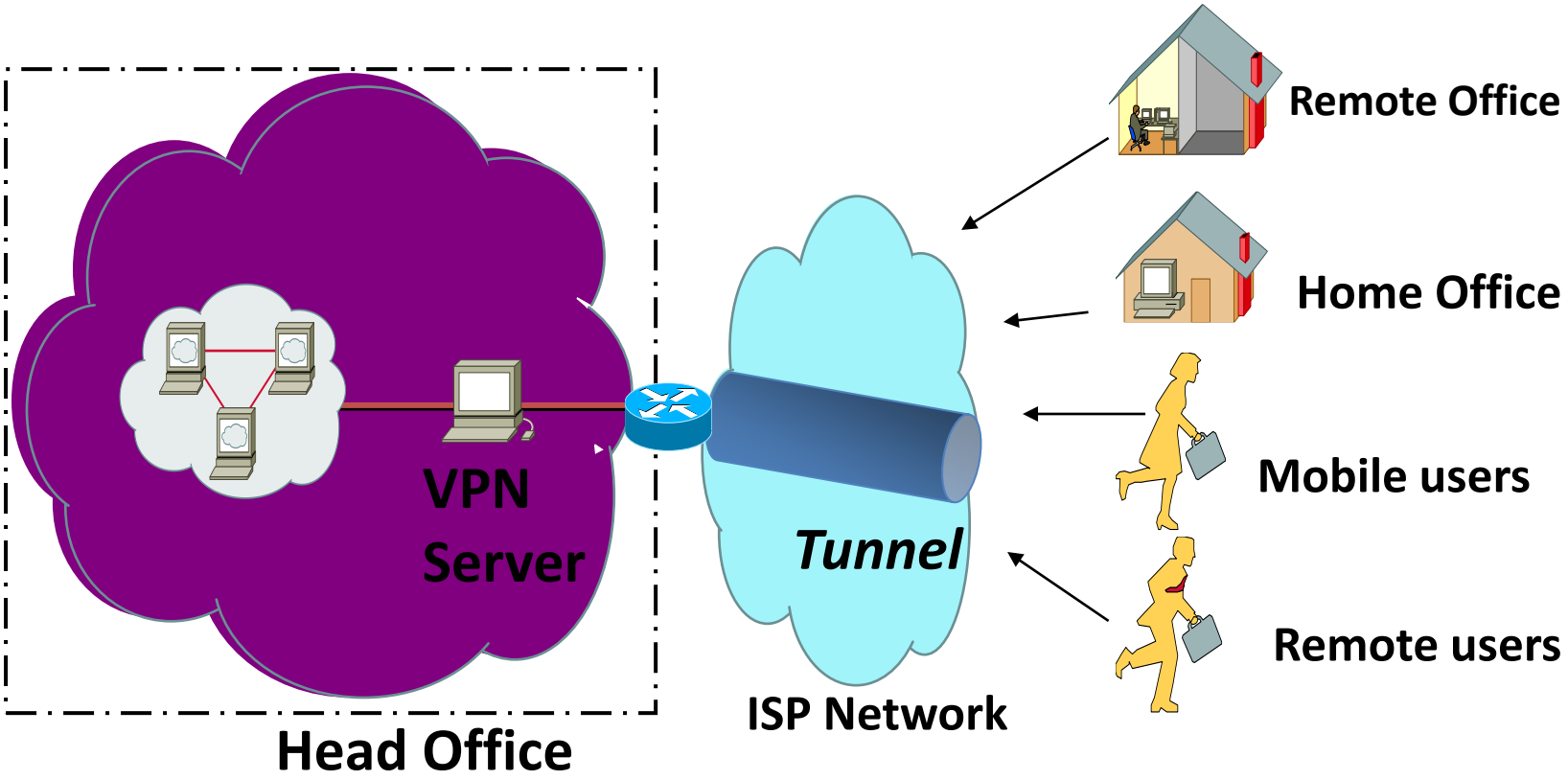
Phân loại theo mức hoạt động

- Layer 2: PPTP, L2TP, L2F, MPLS VPN L2
- Layer 3: IPSec, MPLS VPN L3
- Layer 4: SSL VPN

Phân loại theo kiến trúc

- Remote Access VPN
- Site-to-Site VPN (Intranet VPN & Extranet VPN)

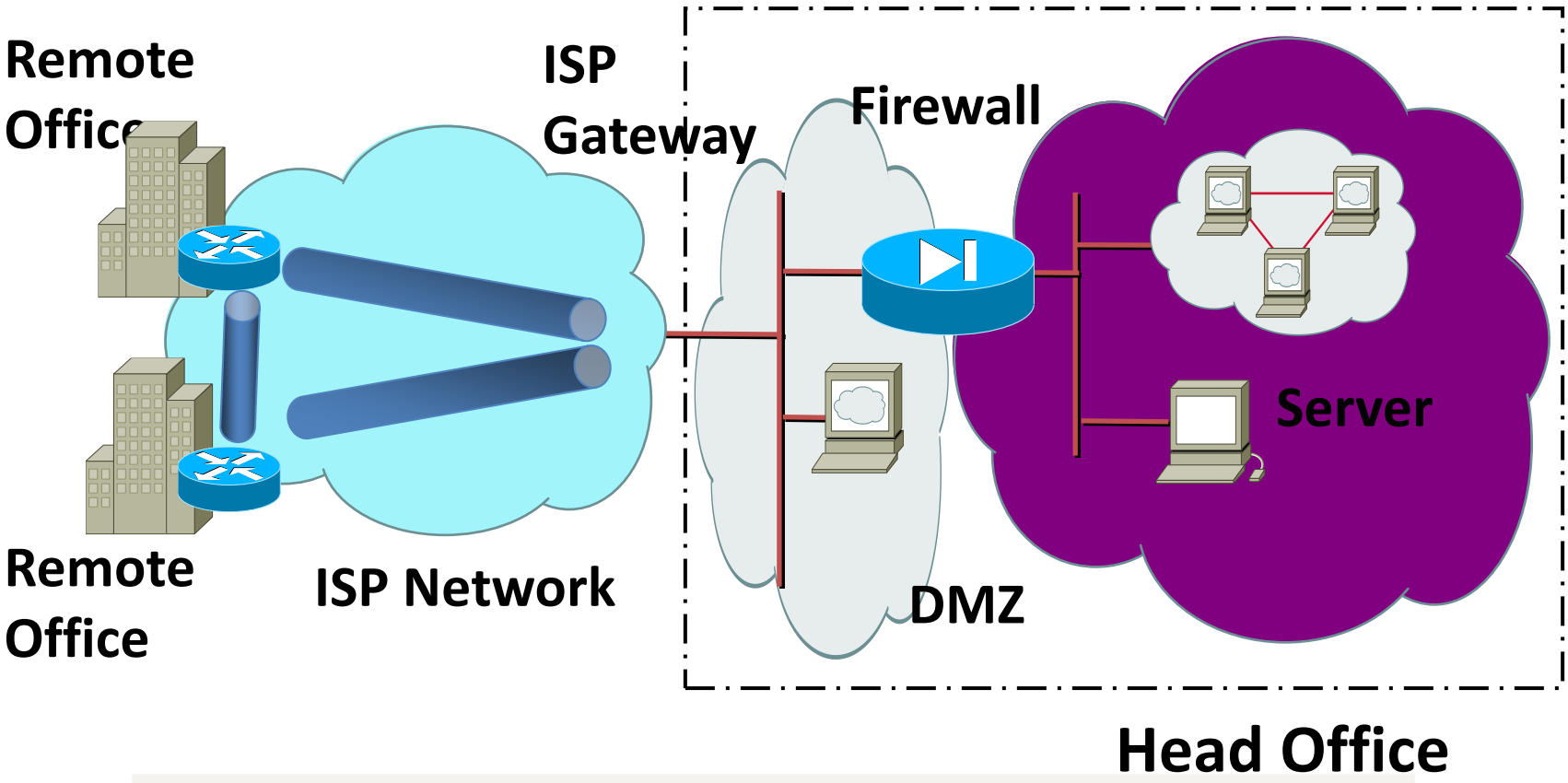
VPN truy cập từ xa (Remote Access VPN)



Cung cấp truy cập tin cậy cho các nhân viên di động,, nhân viên ở xa, nhân viên làm việc tại nhà.

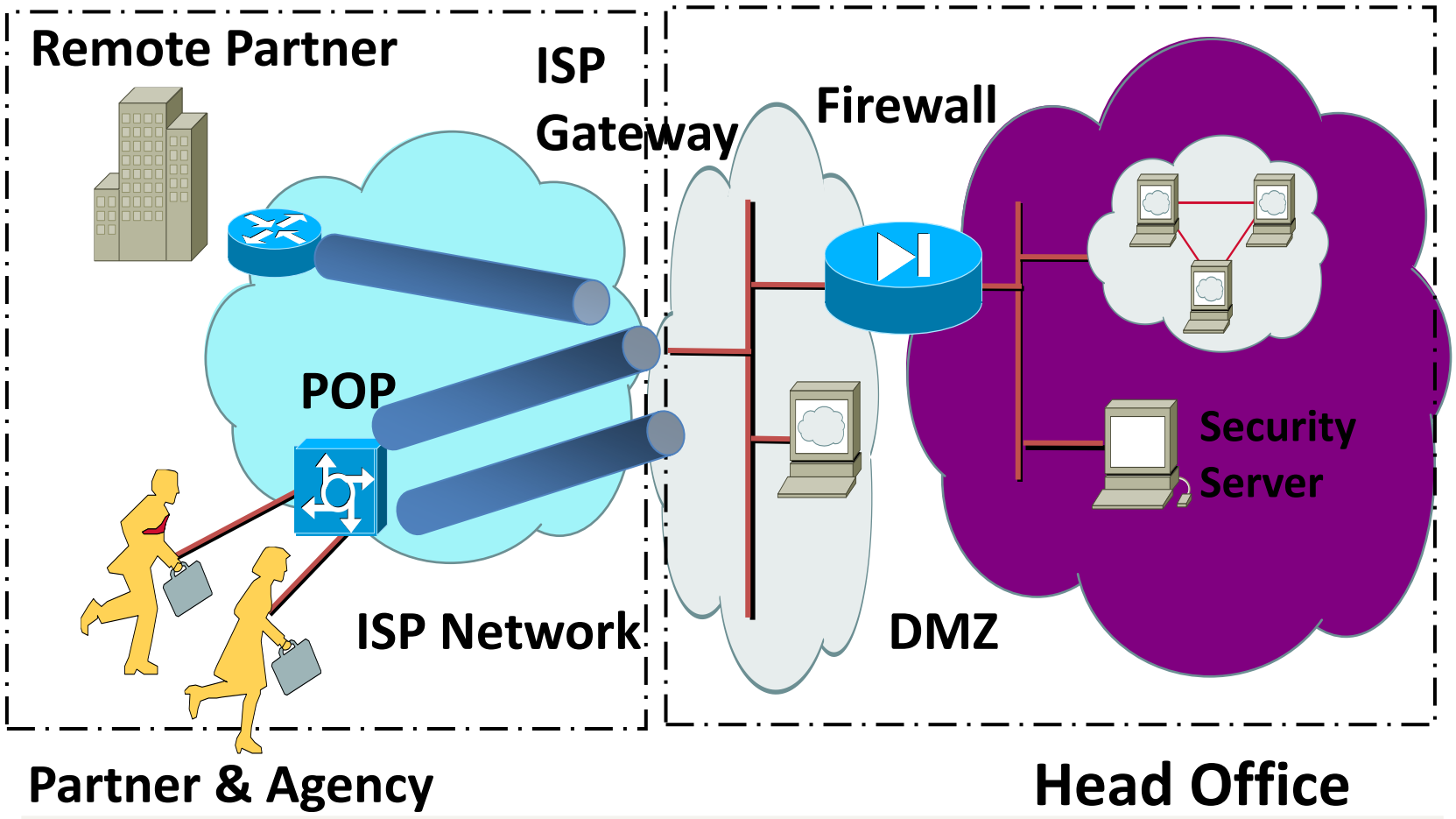
12

VPN cục bộ (Intranet VPN)



Cho phép các văn phòng chi nhánh liên kết một cách bảo mật tới trụ sở chính của doanh nghiệp

VPN mở rộng (Extranet VPN)



Mở rộng cho phép cả khách hàng và đối tác có thể truy cập một cách bảo mật đến Intranet của doanh nghiệp

Mạng riêng ảo

❑Dịch vụ an toàn có thể cung cấp

- Đảm bảo tính bí mật
- Đảm bảo tính toàn vẹn
- Đảm bảo tính xác thực
- Chống tấn công phát lại

Mạng riêng ảo

❑ Lợi ích

- An toàn
- Chi phí thấp
  - Chi phí thực hiện
  - Chi phí quản trị
- Nâng cao khả năng kết nối
- Nâng cao khả năng mở rộng
- Sử dụng hiệu quả băng thông

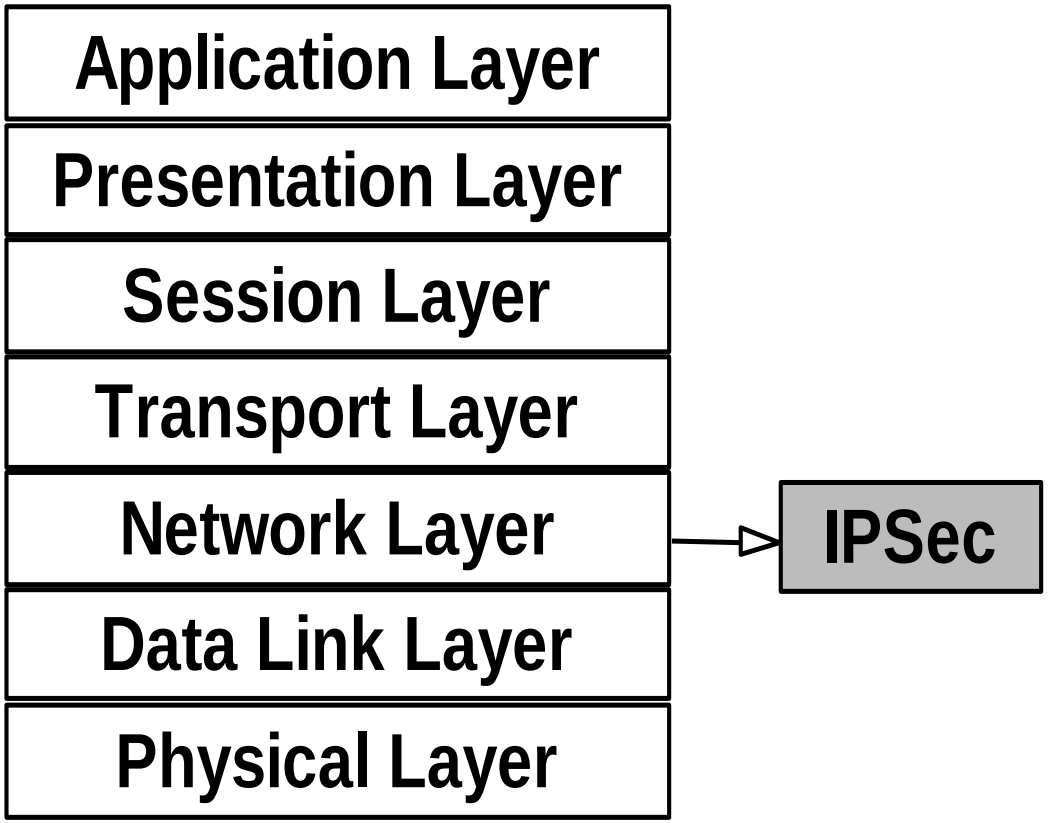
1. Tổng quan về VPN
2. Giới thiệu IPsec
3. Tổ hợp an toàn SA
4. Giao thức AH

Giới thiệu về IPSec

- **IPSec = Internet Protocol Security**
- 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

Giới thiệu về IPSec

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

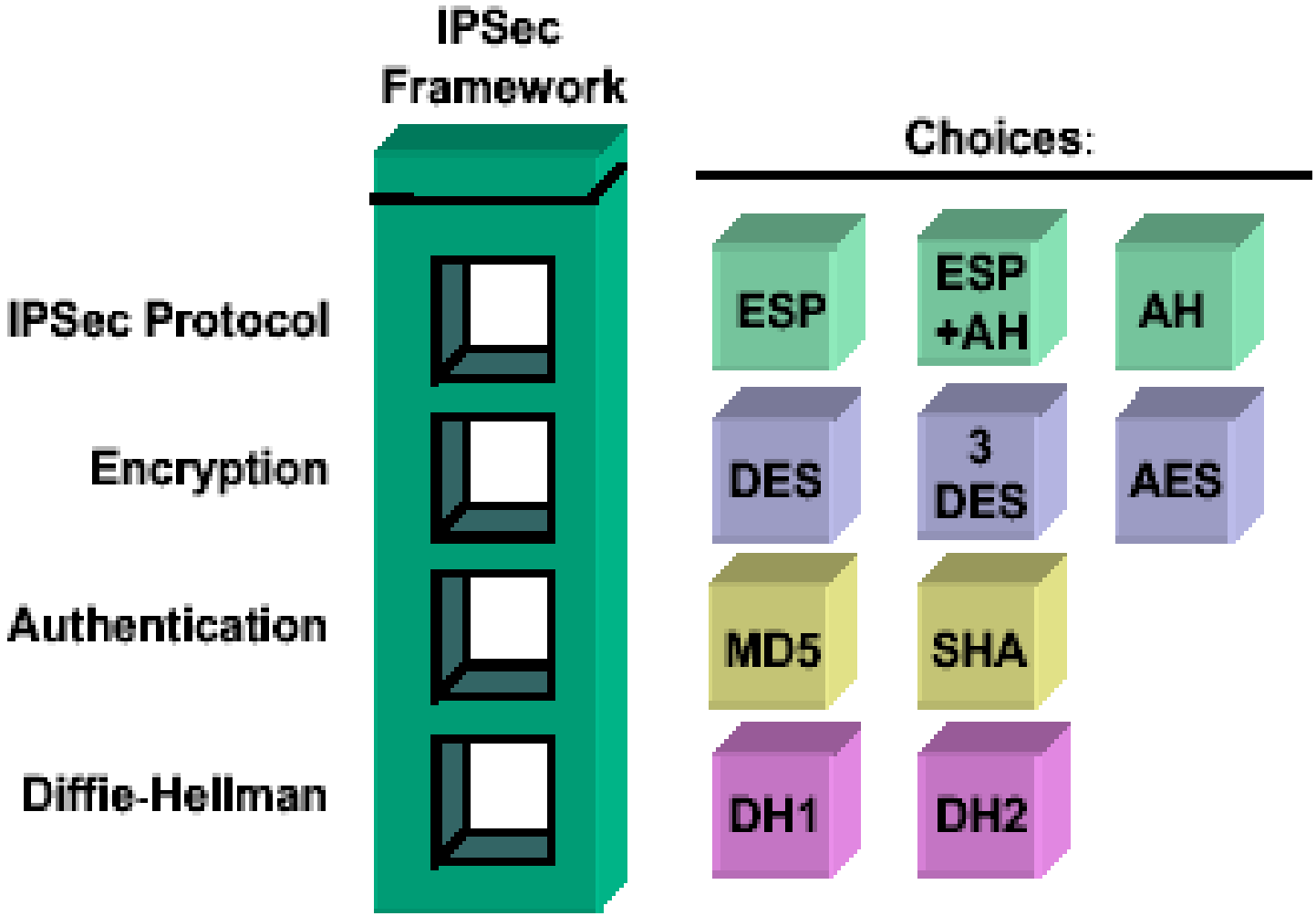


Giới thiệu về IPSec

- 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

Giới thiệu về IPSec

- Khung giao thức IPSec:

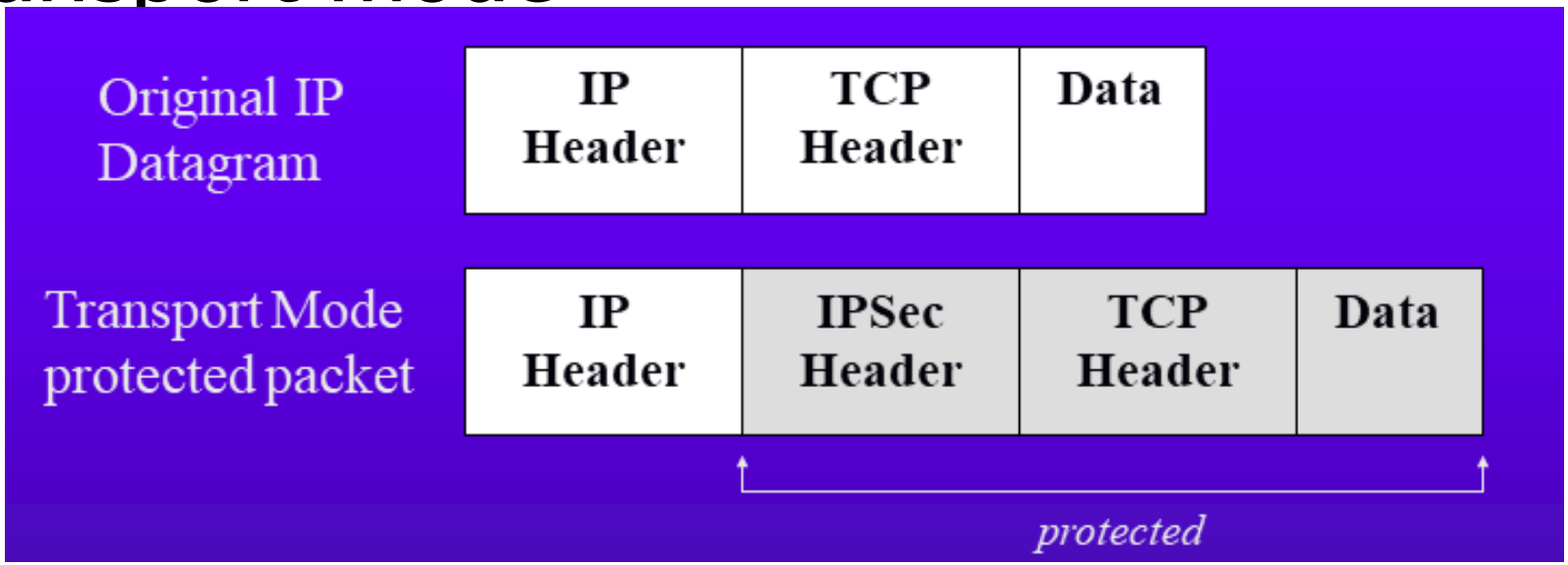


Giới thiệu về IPSec

- **IPSec cung cấp an toàn cho 3 tình huống:**
  - Host – to – host
  - Host – to – gateway
  - Gateway – to – gateway
- **IPSec hoạt động ở 2 chế độ:**
  - Chế độ Transport (end- to – end)
  - Chế độ Tunnel (cho VPN)

Các chế độ hoạt động của IPSec

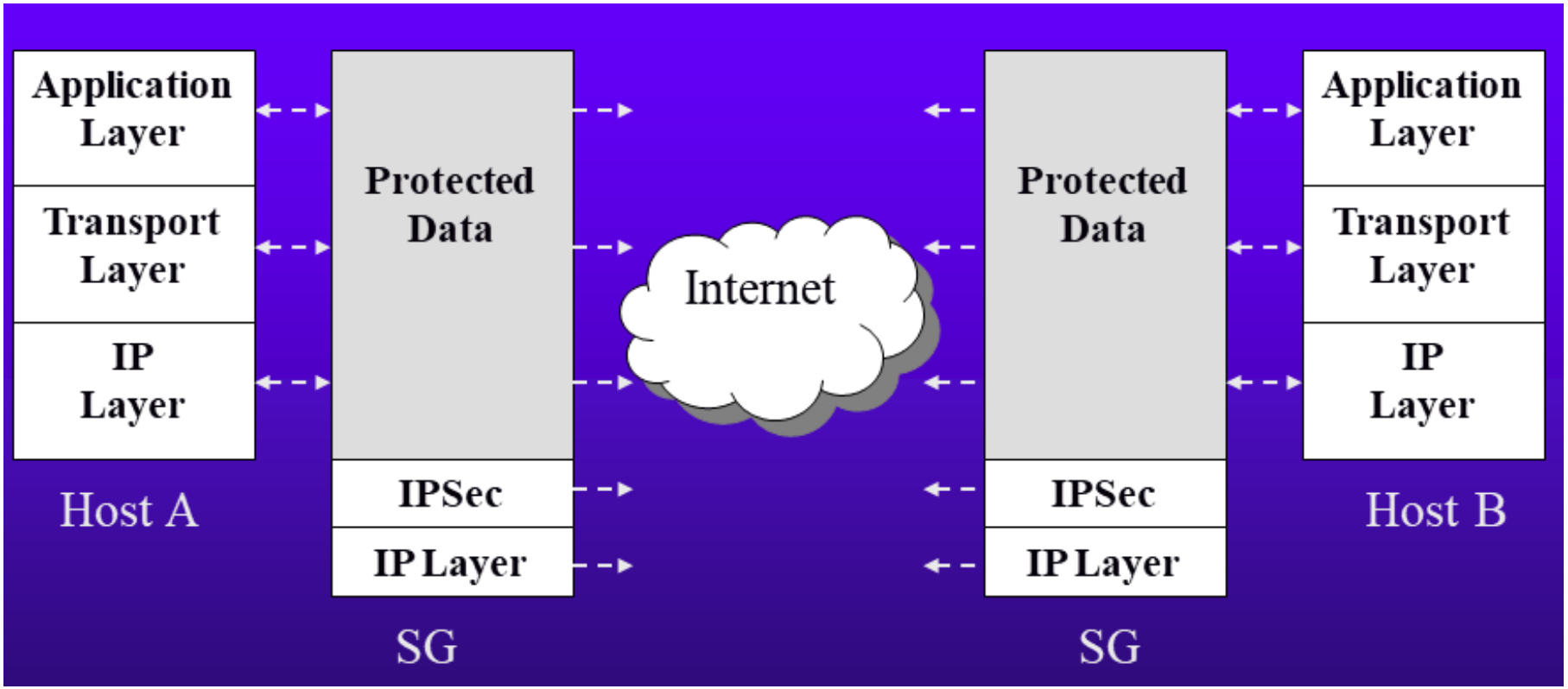
- Transport mode



- Tunnel mode

Tunnel mode

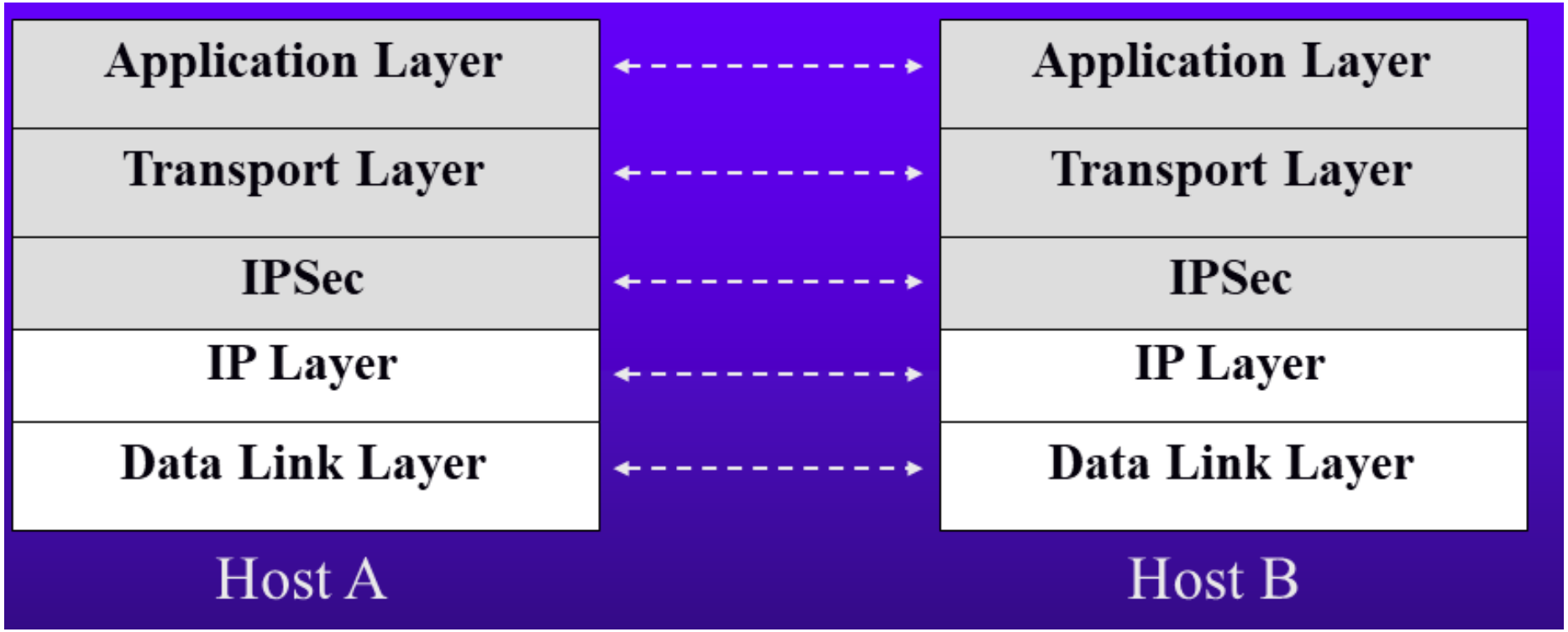
- Host-to-Gateway, Gateway-to-Gateway



SG = Security Gateway

Transport Mode

- Host-to-Host



Qúa trình hoạt động của IPSec

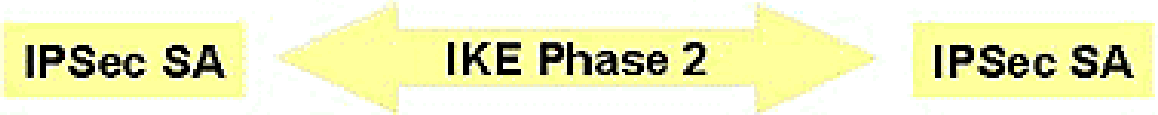
- Ban đầu: Xác định luồng lưu lượng cần bảo vệ.
- Bước 1: Pha IKE thứ 1 sẽ thoả thuận một SA (SA1).
- Bước 2: Thiết lập một kênh truyền thông an toàn và xác thực đối tác dựa trên SA1.
- Bước 3: Pha IKE thứ 2 thoả thuận IPSec SA (SA2) trên kênh an toàn vừa được thiết lập.
- Bước 4: Thực thi AH hoặc/và ESP với các thuật toán mã hoá, xác thực và khoá được chỉ ra bởi SA2.
  - Những thông số này được sử dụng để thống nhất việc trao đổi dữ liệu giữa hai bên.
  - Các khoá được lưu trữ trong csdl SAD.
- Kết thúc: đường hầm IPSec sẽ bị xoá.

Qúa trình hoạt động của IPSec

1. Host A sends interesting traffic to Host B.

2. Router A and B negotiate an IKE phase one session.

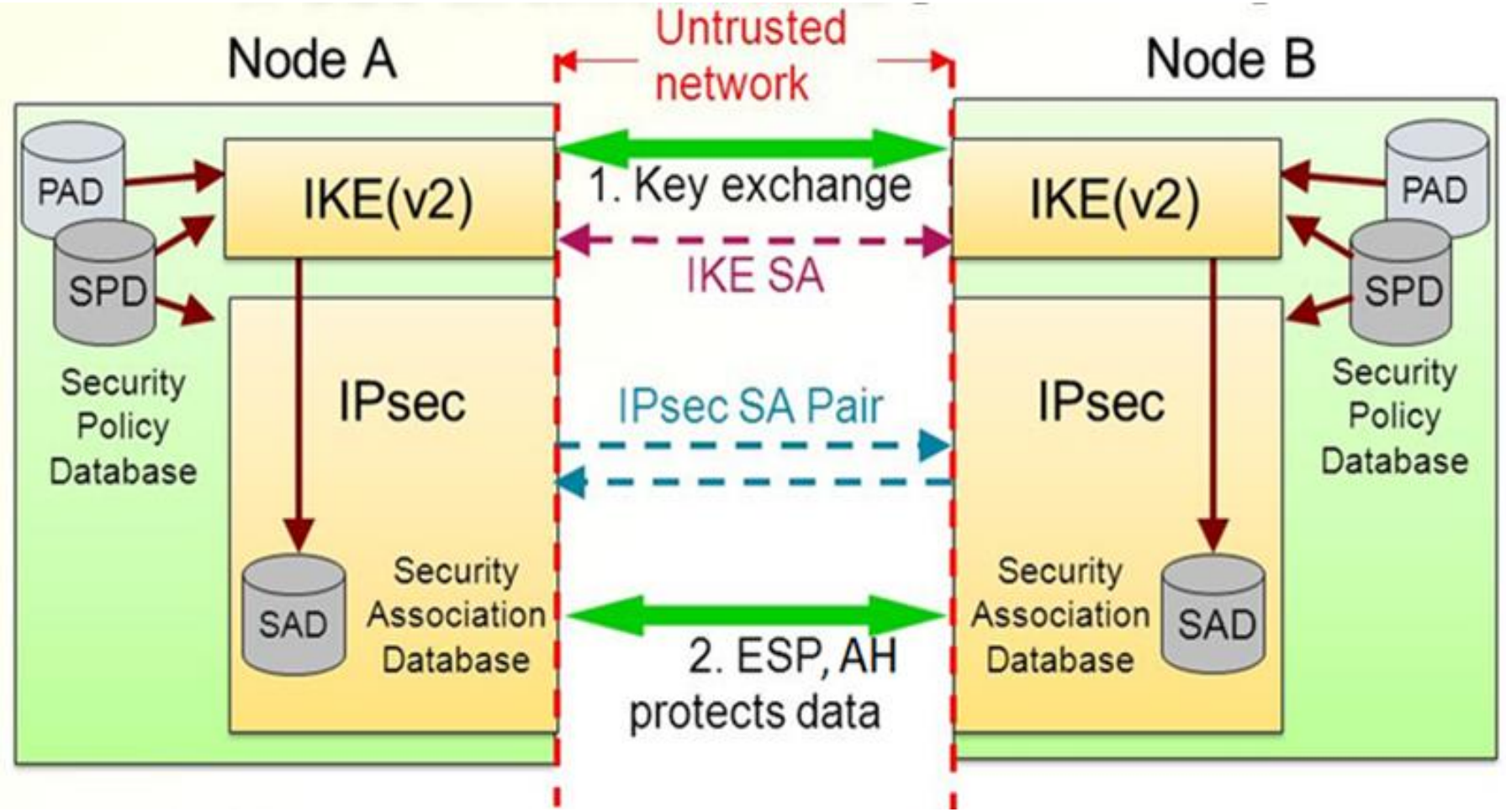
3. Router A and B negotiate an IKE phase two session.



4. Information is exchanged via IPSec tunnel.

5. IPSec tunnel is terminated.

Kiến trúc IPSec [RFC4301]



- IKE tạo ra các SA, các SA được IPSec ESP, AH sử dụng
- SPD hướng dẫn cách tạo và lựa chọn SA cho sử dụng

Pre-Shared Key (PSK) trong IPsec

- Khóa chia sẻ trước (PSK) là phương thức xác thực phổ biến nhất cho các đường hầm VPN IPsec site-to-site (không dùng cho remote access).
- PSK chỉ được sử dụng cho xác thực, không dùng cho mã hóa.
  - Các đường hầm IPsec dựa trên các giao thức ISAKMP/IKE để trao đổi các khóa để mã hóa, v.v. Nhưng trước khi IKE có thể hoạt động, cả hai bên cần xác thực lẫn nhau . Đây là phần duy nhất mà PSK được sử dụng (RFC 2409).

1. Tổng quan về VPN
2. Giới thiệu IPsec
3. Tổ hợp an toàn SA
4. Giao thức AH

Tổ hợp an toàn (SA)

- **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

Tổ hợp an toàn (SA)

- 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

Tổ hợp an toàn (SA)

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.

Tổ hợp an toàn (SA)

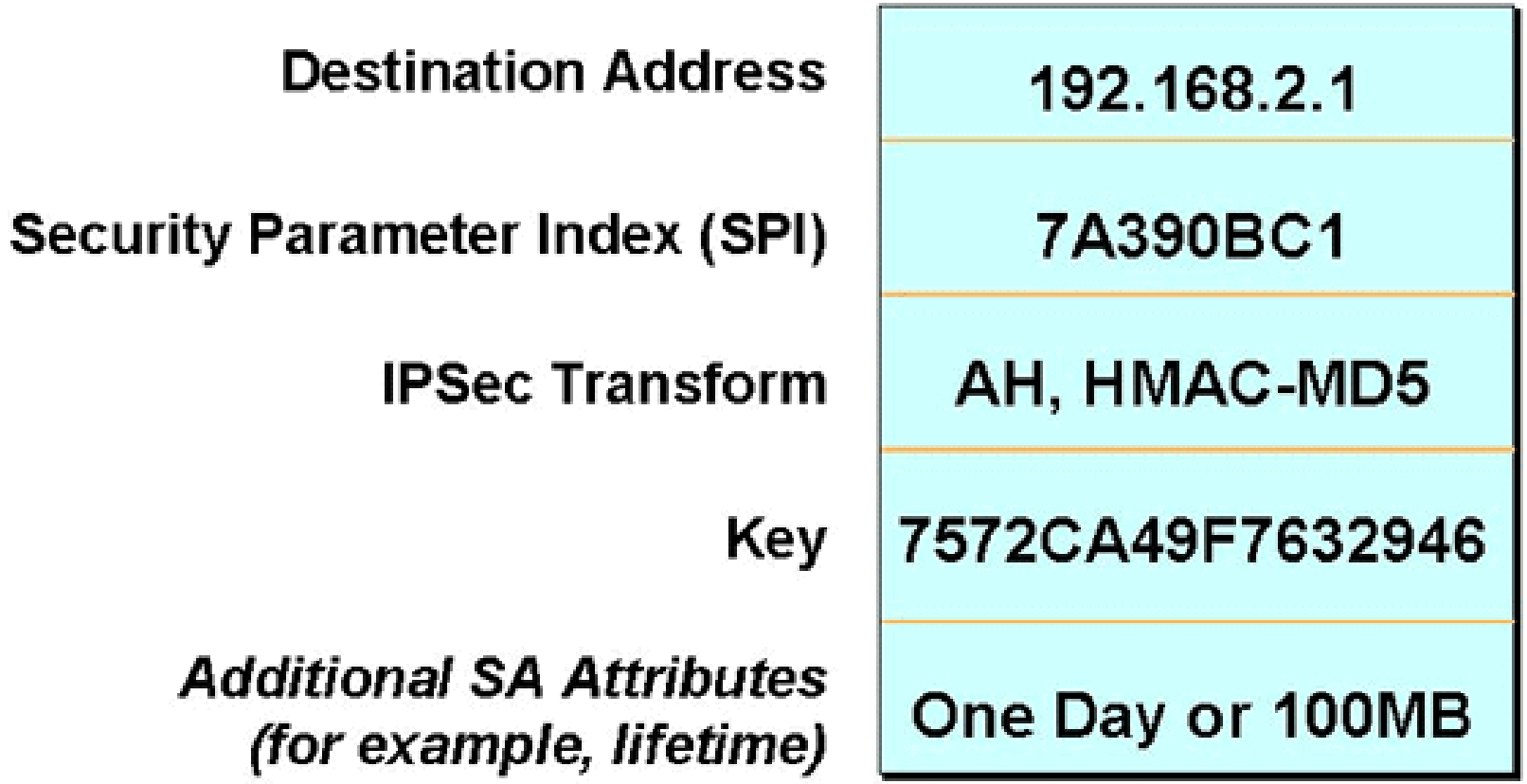
Là địa chỉ IP của Node đích

Mô tả giao thức an toàn IPSec được dùng, có thể là AH hoặc ESP

Nội dung của một SA

- Giao thức an toàn: AH, ESP
- Thuật toán, khóa mật mã: DES, 3DES
- Phương pháp, khóa xác thực cho AH | ESP: Hàm băm (HMAC, MD5, SHA1), chữ ký số (RSA), chứng thư số, Diffie-Hellman…
- Thông tin liên quan đến khoá: khoảng thời gian thay đổi, khoảng thời gian làm tươi.
- Thông tin liên quan đến chính SA: địa chỉ nguồn SA, khoảng thời gian làm tươi.

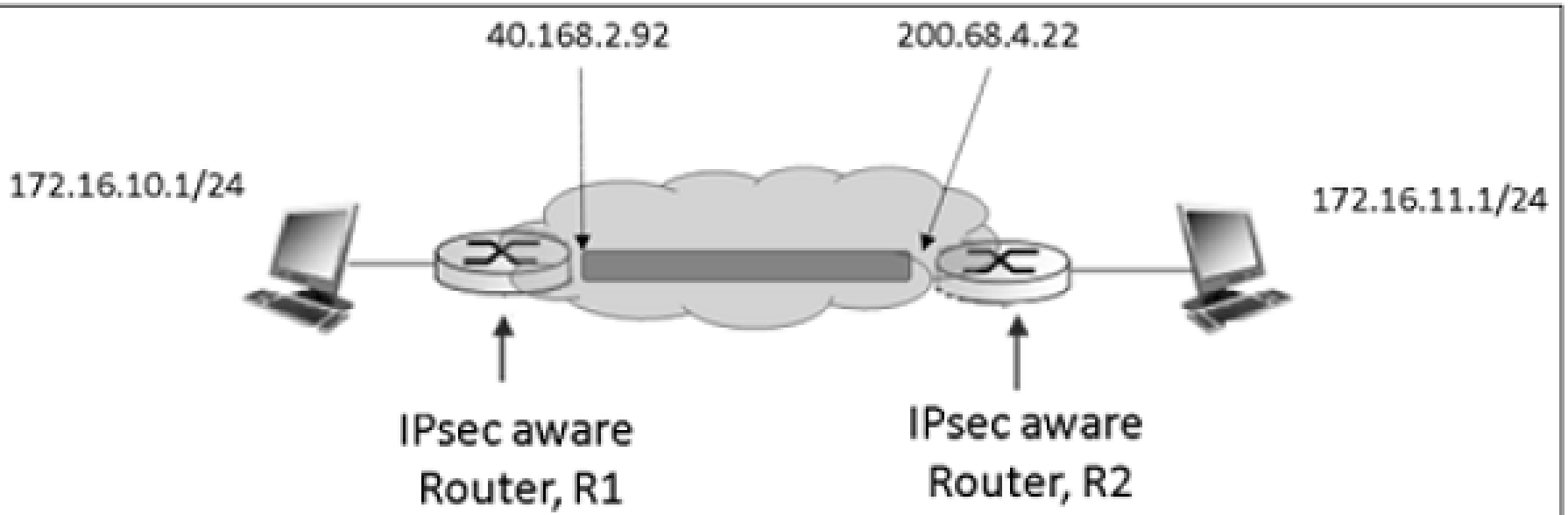
Ví dụ (1) về IPSec SA



Ví dụ (2) về IPSec SA

Địa chỉ đích	192.168.1.154
Giá trị SPI	7A390BC1
IPSec Transform	AH, HMAC-SHA1
Key	7572CA49F7632946
Thuộc tính	30 phút

Ví dụ (3) về IPSec SA



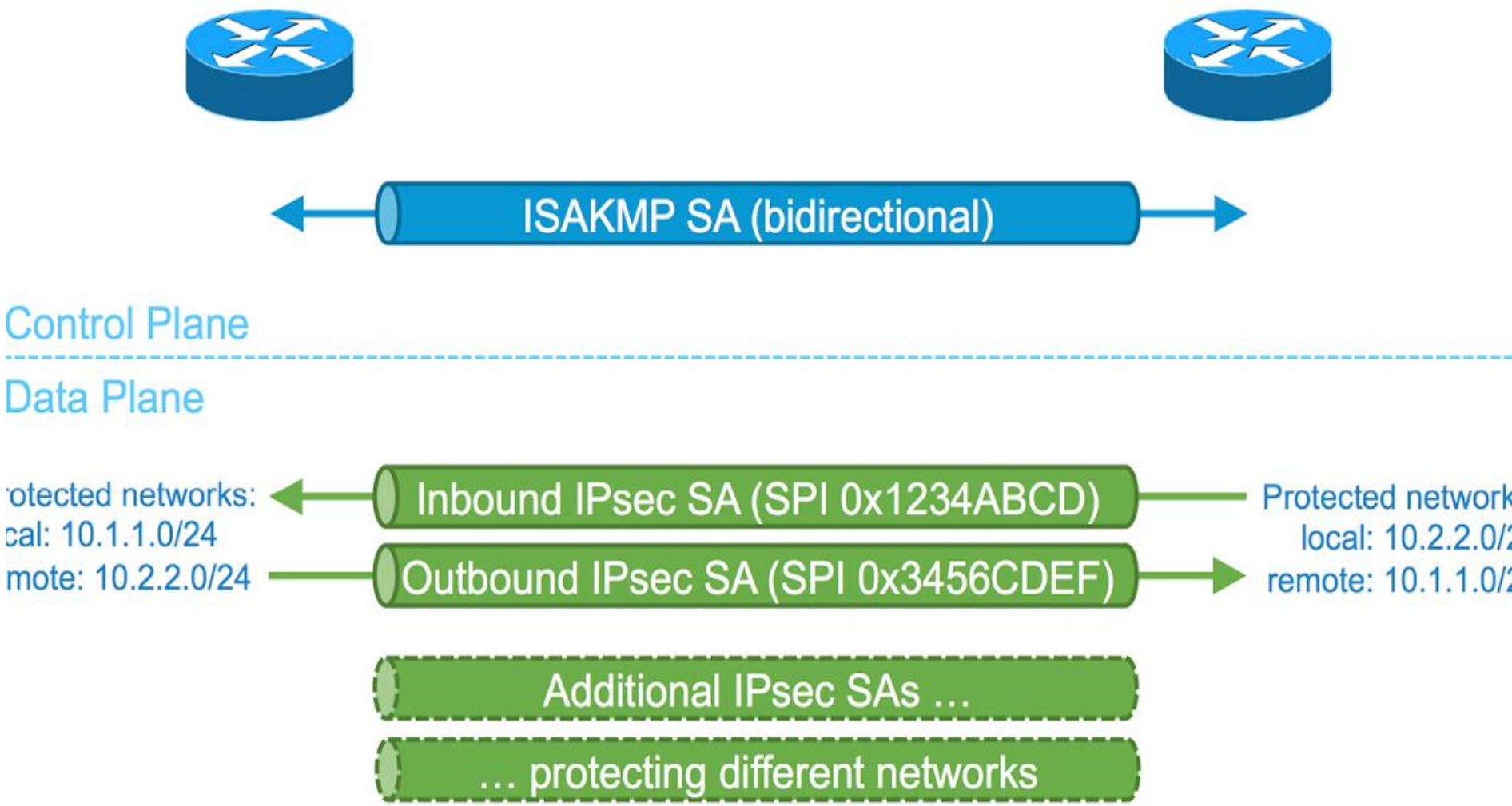
R1 stores for SA

- 32-bit identifier for SA: Security Parameter Index (SPI)
- Origin SA interface (40.168.2.92)
- Destination SA interface (200.68.4.22)
- Type of encryption used (say, 3DES with CBC)
- Encryption key
- Type of integrity check used (say, HMAC with MD5)
- Authentication key

Tính đơn hướng của SA

- 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.

Ví dụ (5) về IPSec SA



Cơ sở dữ liệu cho SA

- Một SA sử dụng hai cơ sở dữ liệu:
  - Cơ sở dữ liệu tổ hợp an toàn (SAD - Security Association Database)
  - Cơ sở dữ liệu chính sách an toàn (SPD- Security Policy Database)

SPD

- Nội dung
  - Xác định lưu lượng cần bảo vệ

    ☒IP traffic → ***selectors*** → IPSec policy. (SPD)

  - Các mục Policy xác định SA hoặc chuỗi các SA (SA Bundle) nào được sử dụng
  - Tham chiếu của Selector đến SPD gồm: Dest IP, Source IP, IPSec Protocol, Transport Protocol, Source & Dest Ports, …
- Mọi host hoặc gateway tham gia trong IPSec đều có SPD riêng của nó.

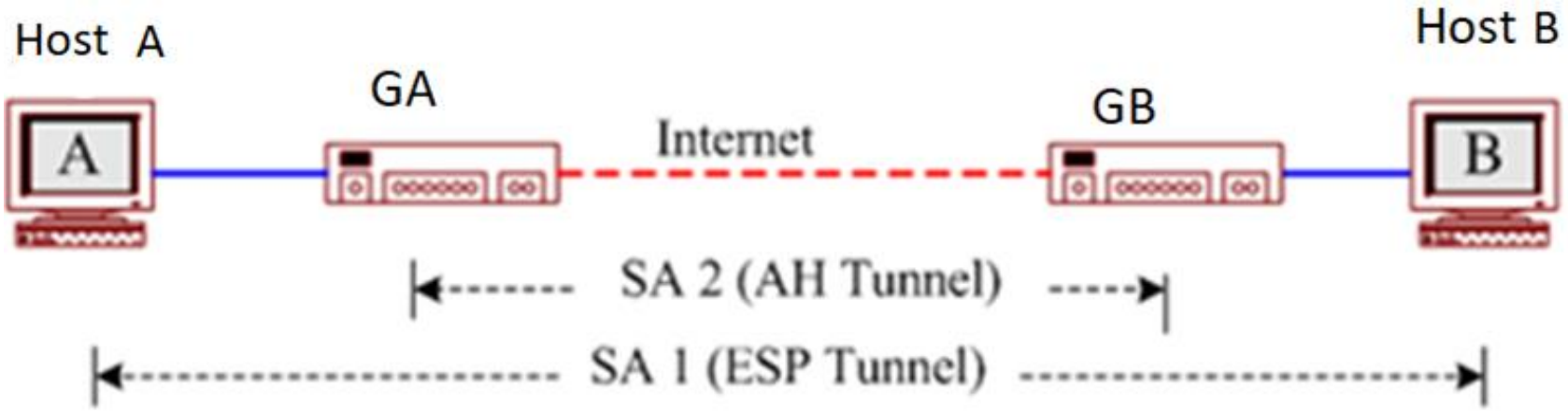
SPD

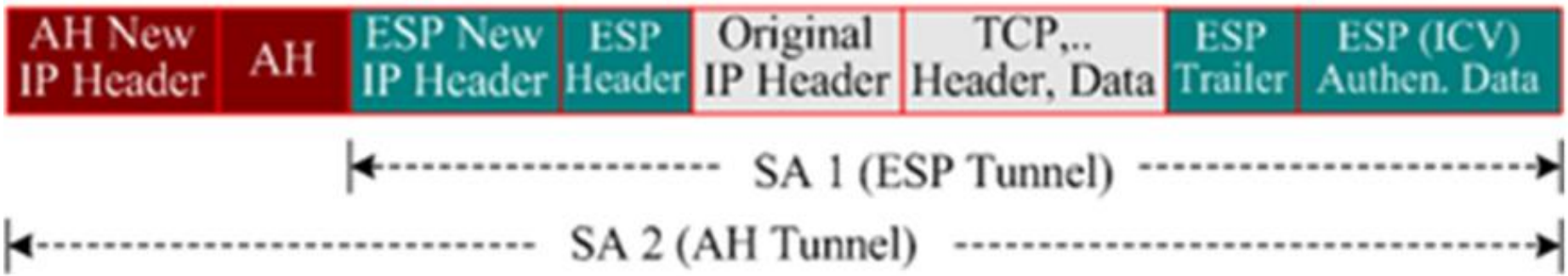
- Một trong ba hành động sau được thực hiện trên lưu lượng IP:
  - Discard: Không cho đi vào hoặc đi ra
  - Bypass:
    - Outbound: không áp dụng IPSec
    - Inbound: không mong muốn áp dụng IPSec
  - Protect:
    - Sử dụng một SA
    - Hoặc sử dụng SA bundle

SA Bundle

- Hơn một SA có thể áp dụng cho một gói tin
- Chẳng hạn, ESP không xác thực được phần New IP Header
  - Sử dụng SA thứ nhất để áp dụng xác thực của ESP cho gói tin ban đầu
  - Sử dụng SA thứ hai để áp dụng AH xác thực cho cả phần New IP Header

Ví dụ về SA Bundle





SAD

- Nội dung
  - Thời gian có hiệu lực của SA
  - Thông tin về AH và ESP (các khoá, các thuật toán, …)
  - Chế độ Transport hoặc Tunnel
- Mọi host hoặc gateway tham gia trong IPSec đều có SAD riêng của nó.

Ví dụ (1) về SPD, SAD

SPD (Security Policy Database)

From	To	Protocol	Port	Policy
1.1.1.1	2.2.2.2	TCP	1000	ESP with 3DES
1.1.1.1	2.2.2.2	*	*	ESP with DES

Inbound SAD (Security Association Database)

From	To	Protocol	SPI	SA RECORD
2.2.2.2	1.1.1.1	ESP	1	64 bit DES Key SA2
2.2.2.2	1.1.1.1	ESP	11	168 bit 3DES SA1Key

Ví dụ (2) về SPD, SAD

A's SPD

From	To	Protocol	Port	Policy
1.1.1.1	2.2.2.2	Any	Any	Transport AH with HMAC MD5

A's Outbound SADB

Src	Dst	Protocol	SPI	SA record
1.1.1.1	2.2.2.2	AH	10	MD5 key

$SA_{A\rightarrow B}$

RA's SPD

From	To	Protocol	Port	Policy	Tunnel dst
1.1.1/24	2.2.2/24	Any	Any	Tunnel ESP with 3DES	6.6.6.6

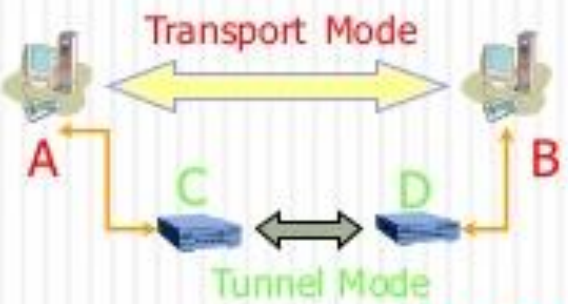
RA's Outbound SADB

Src	Dst	Protocol	SPI	SA record
5.5.5.5	6.6.6.6	ESP tunnel	11	168-bit 3DES key

$SA_{RA\rightarrow RB}$

Sử dụng 2 SA khác nhau:
+ SA cho AH - Transport
+ SA cho ESP – Tunnel (RA ⇔RB)

Ví dụ (3) về SPD, SAD



A's SPD

From	To	Protocol	Port	Policy
A	B	Any	Any	AH[HMAC-MD5]

A's SADB

From	To	Protocol	SPI	SA Record
A	B	AH	12	HMAC-MD5 key

From	To	Protocol	Port	Policy	Tunnel Dest
		Any	Any	ESP[3DES]	D

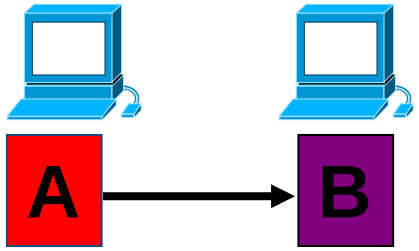
C's SPD

From	To	Protocol	SPI	SA Record
		ESP	14	3DES key

C's SADB

Xử lý Outbound

Outbound packet (Tại A)



IP Packet

SPD
(Policy)

SAD

Gói tin được bảo vệ bởi IPSec? Vậy thì lựa chọn policy nào?

...

...

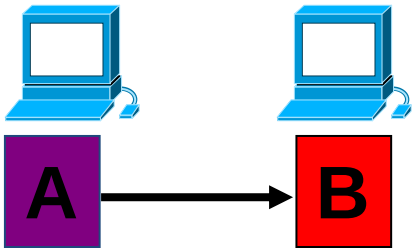
Xác định SA và SPI của nó

Xử lý IPSec

SPI & IPSec Packet

Gửi tới B

Xử lý Inbound



Inbound packet (tại B)

Từ A

SPI & Packet

Sử dụng SPI để tham chiếu tới SAD

SAD

...

"un-process"

SPD (Policy)

...

Gói tin có được đảm bảo an toàn?

Original IP Packet

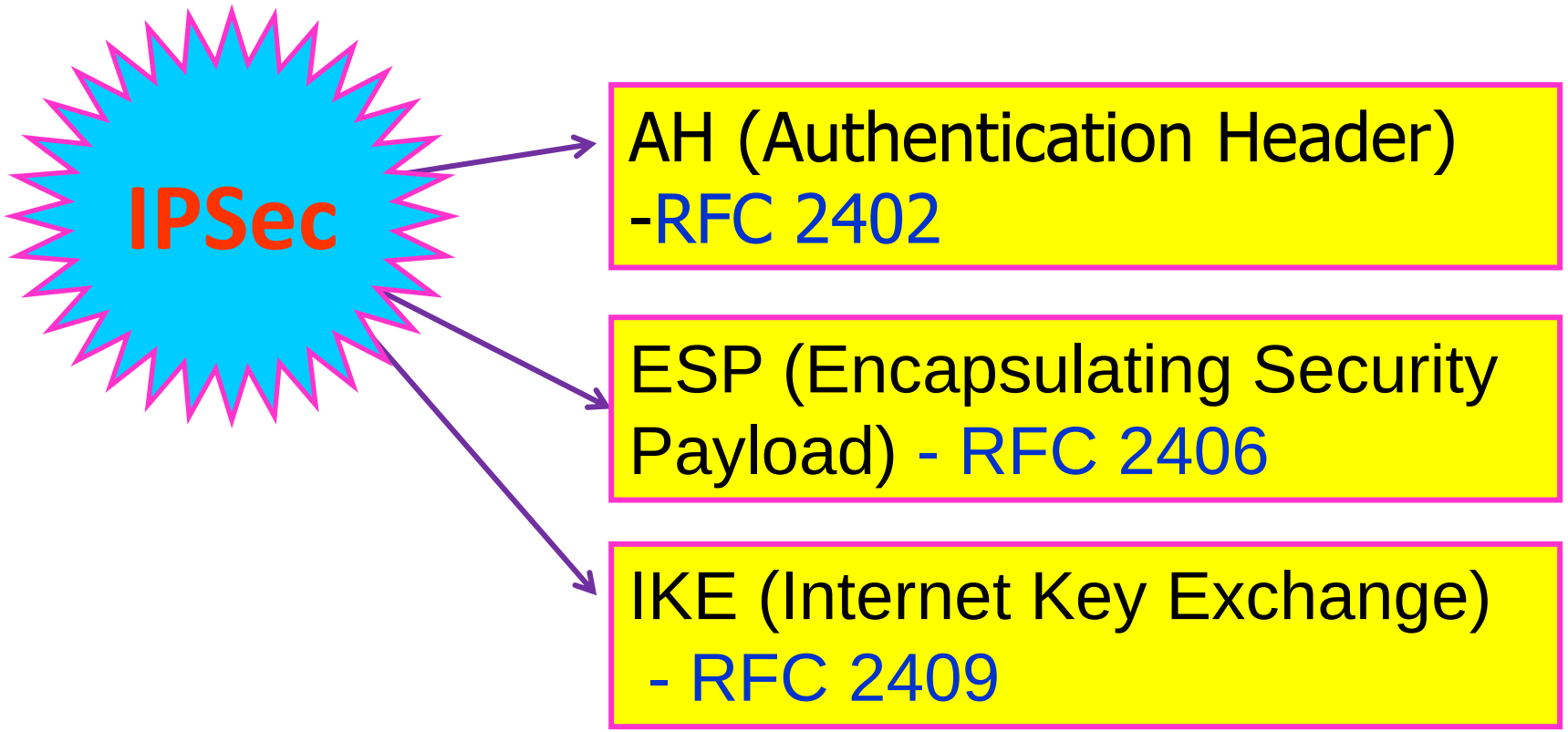
1 Tổng quan về VPN

2 Giới thiệu IPsec

3 Tổ hợp an toàn SA

4 Giao thức AH

Giao thức IPSec



Giao thức IPSec

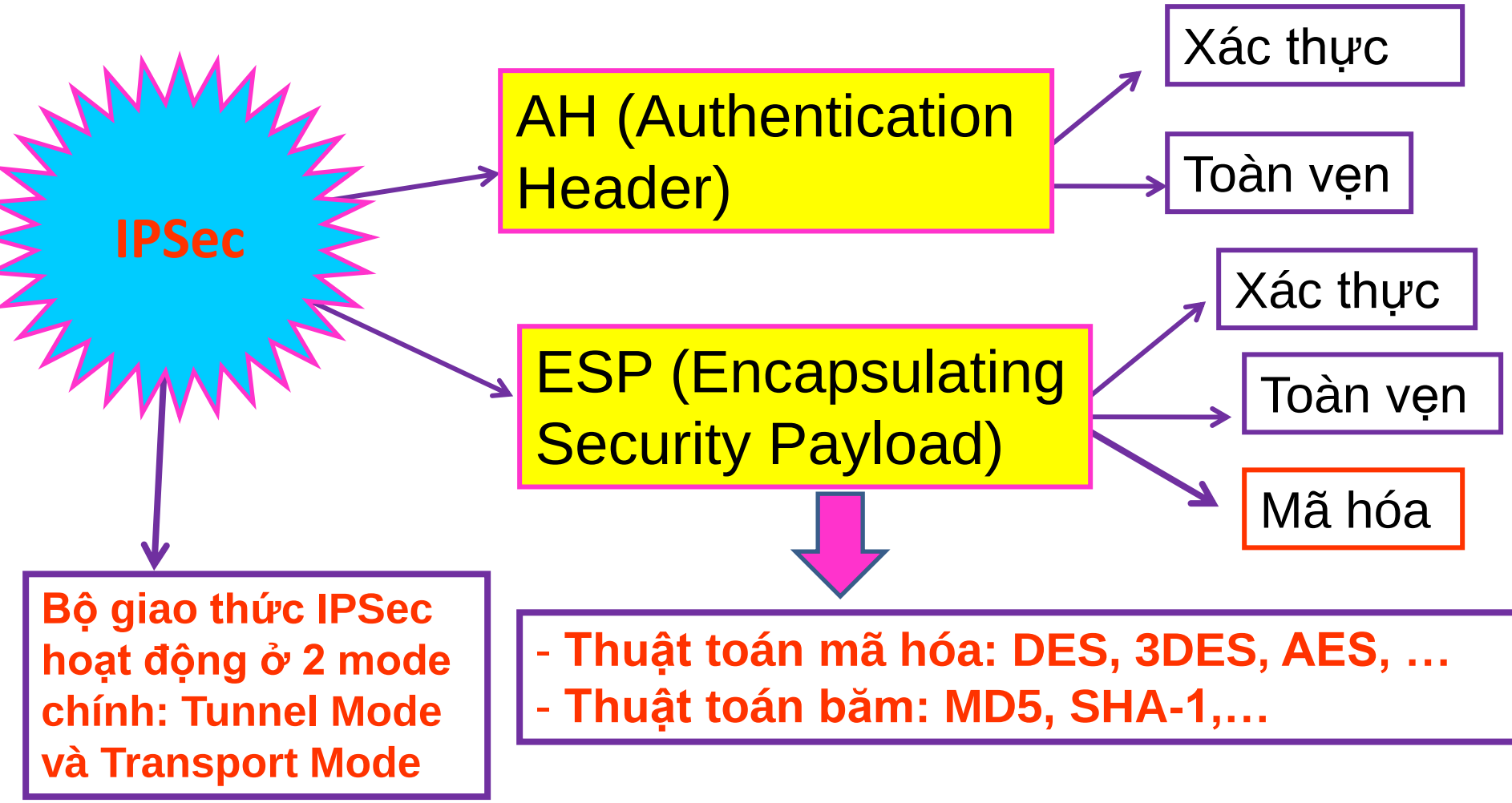
AH (Authentication Header)

ESP (Encapsulating Security Payload)

AH được đóng gói bởi giao thức IP (trường protocol trong IP là 51)

ESP được đóng gói bởi giao thức IP (trường protocol trong IP là 50)

Giao thức IPSec



Giao thức AH

- Giao thức AH thêm một tiêu đề vào gói IP
  - Xác thực người gửi: Tiêu đề này dùng cho việc xác 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.
  - AH không mã hóa bất kỳ phần nào của gói tin

Giao thức AH

Các đặc trưng cơ bản:

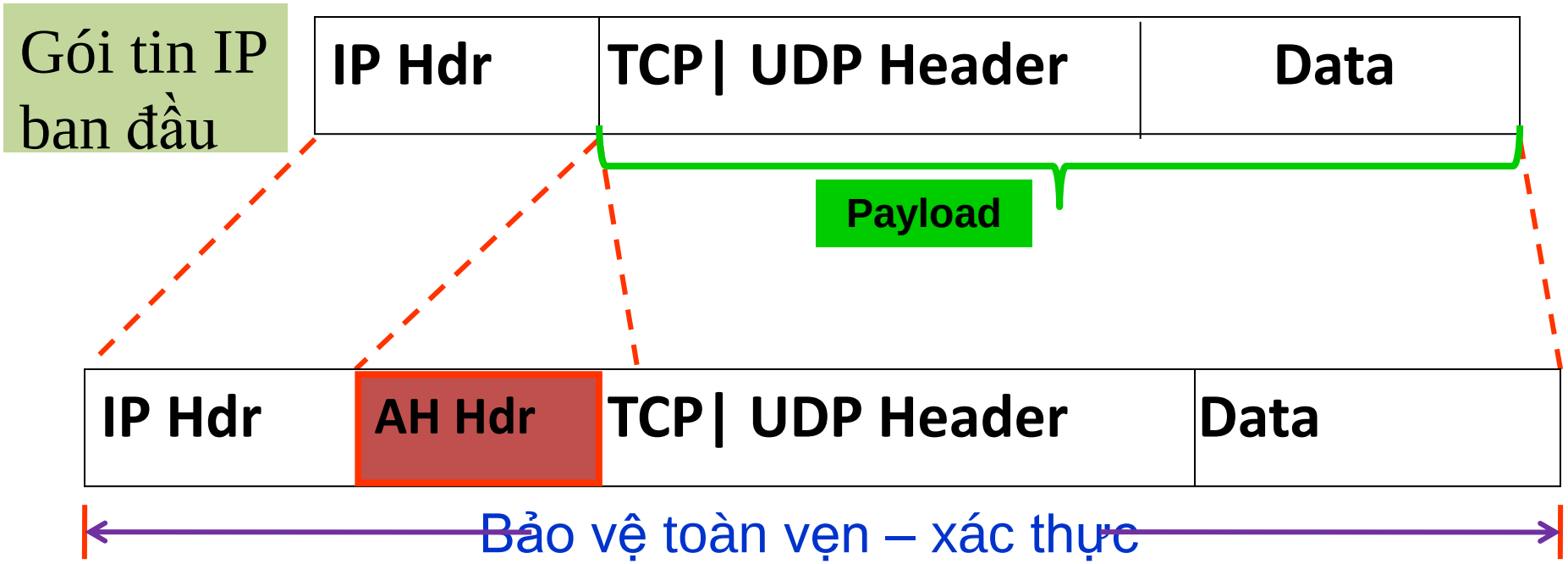
- Cung cấp tính toàn vẹn và xác thực
- Sử dụng mã xác thực thông điệp (HMAC)
- Nội dung các gói tin không được mã hoá.

Giao thức AH

- AH có thể sử dụng ở cả 2 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 trên như TCP hoặc UDP.
    - Không tạo một IP Header mới

Giao thức AH

- **Chế độ Transport:**



Gói tin AH trong chế độ transport

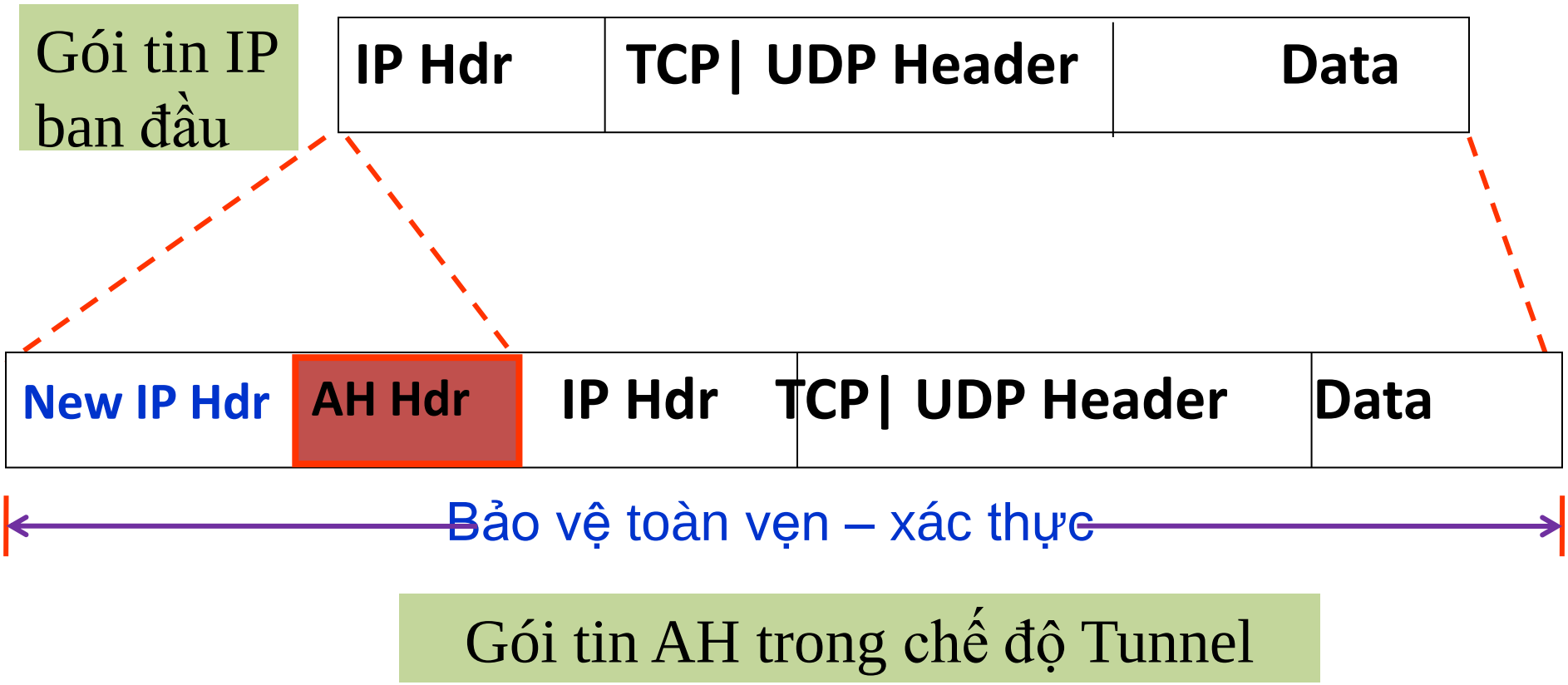
Giao thức AH

❑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 gateway)
- 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

Giao thức AH

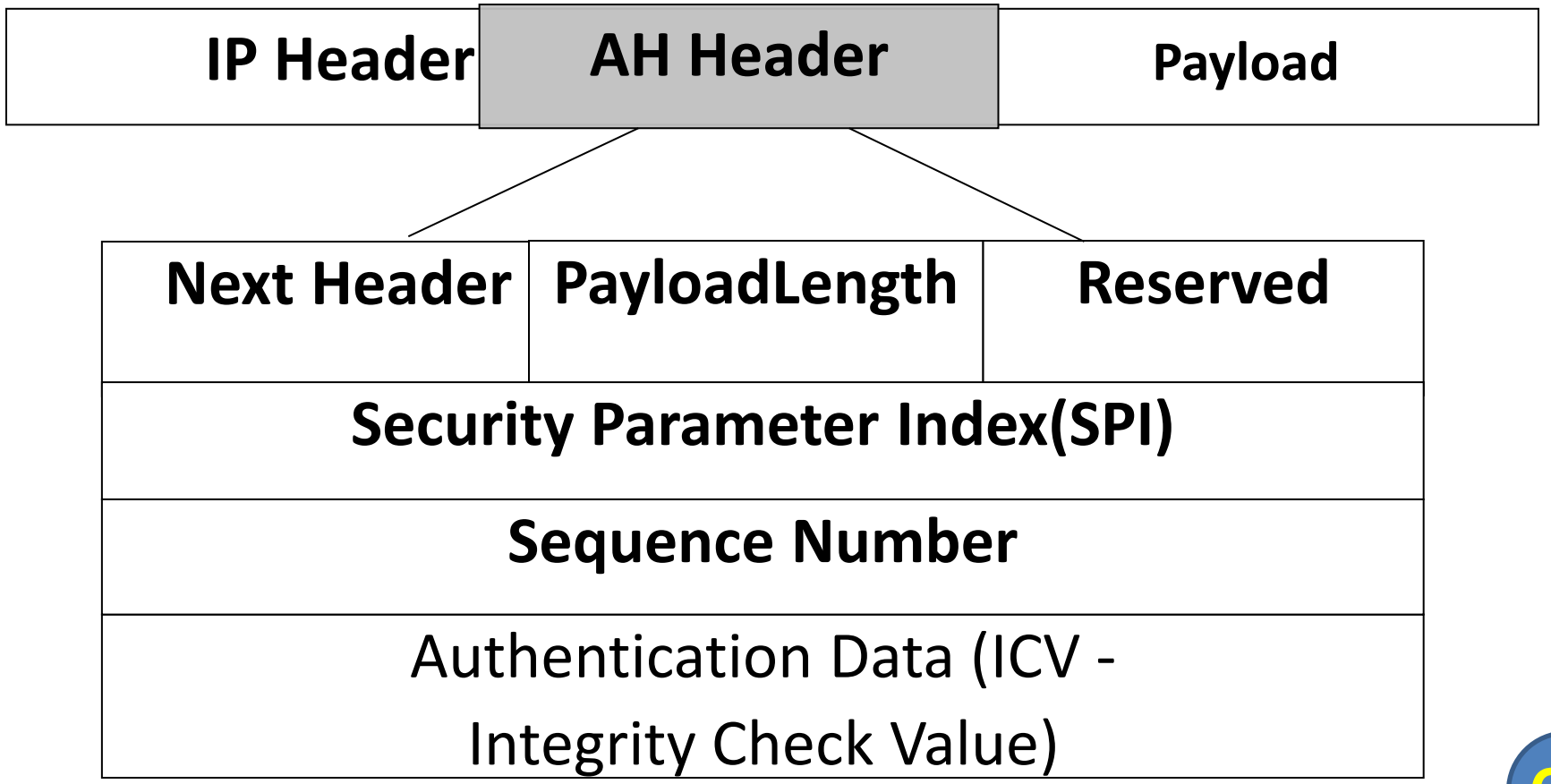
- **Chế độ Tunnel:**



Gói tin AH trong chế độ Tunnel

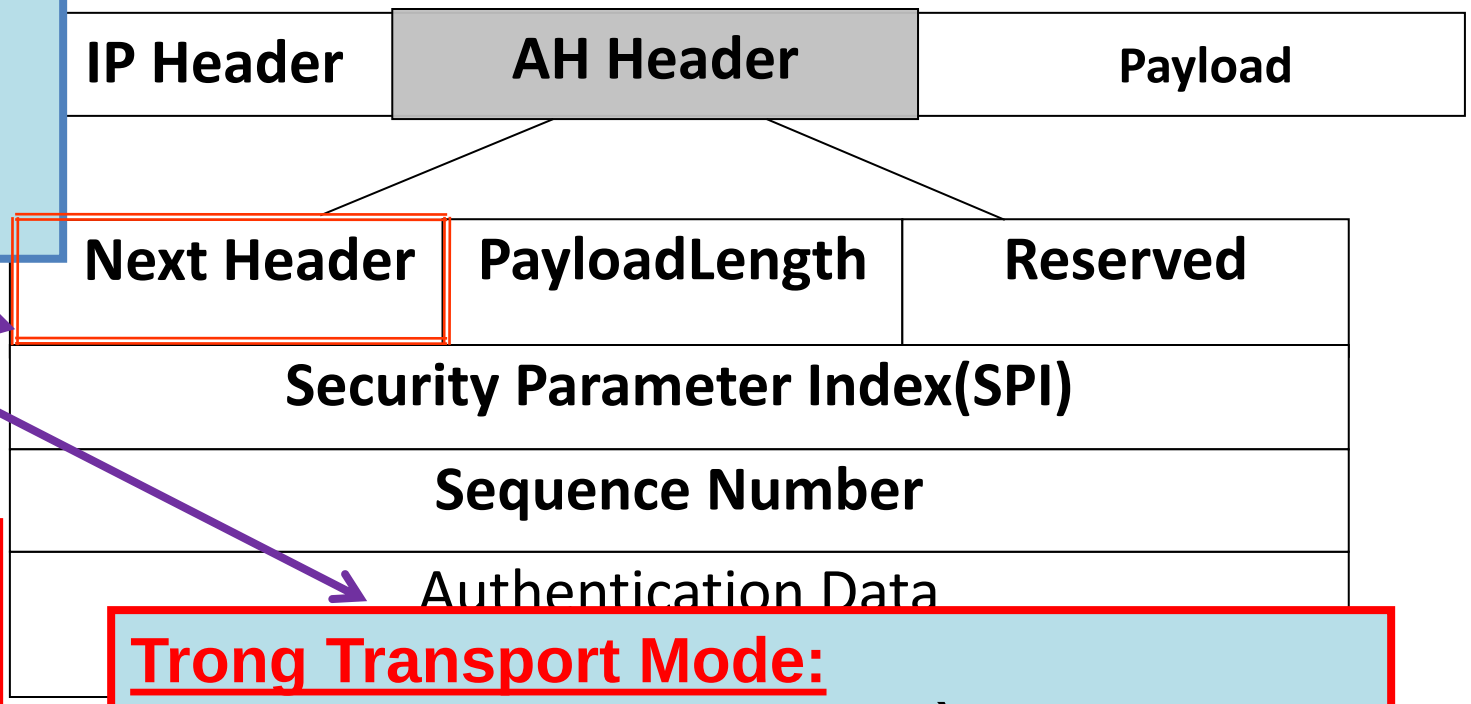
Giao thức AH

- **Khuôn dạng gói tin:**
  - Các trường trong AH Header đều là bắt buộc



Giao thức AH

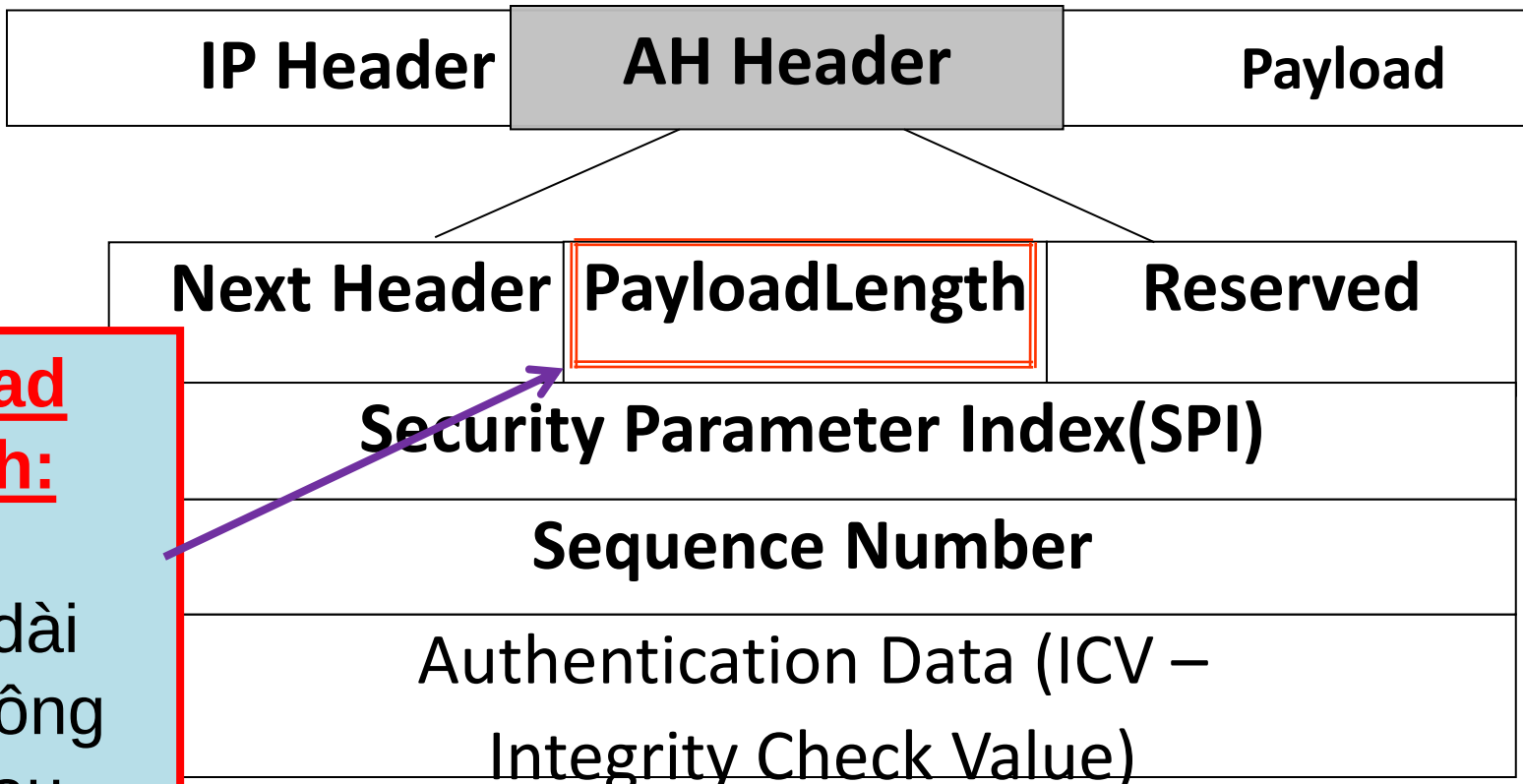
Next Header:
-Dài 8 bit
-Chứa chỉ số giao thức IP



Trong Tunnel Mode:
Payload là gói tin IP nên giá trị Next Header được cài đặt là **4**

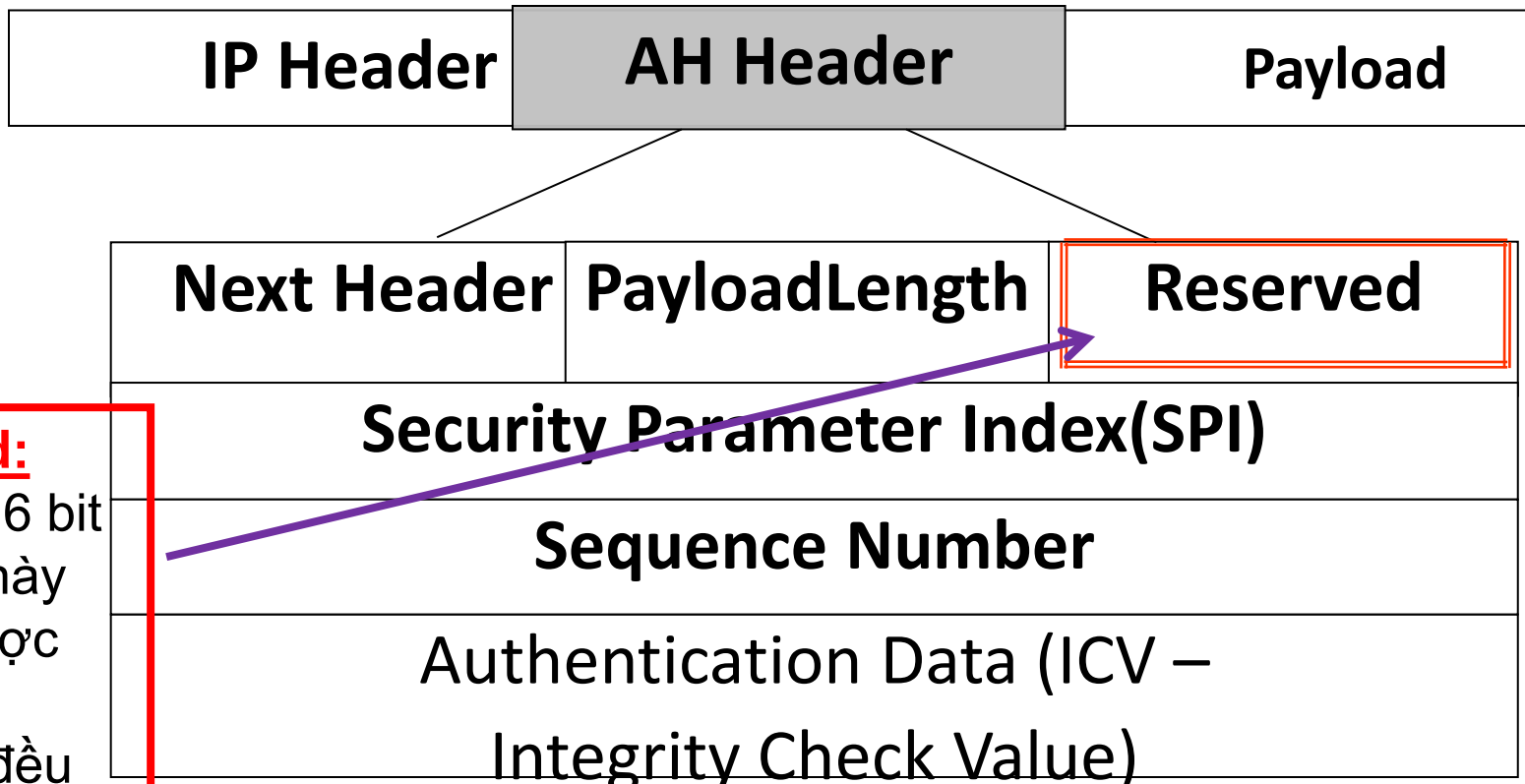
Trong Transport Mode:
- Payload luôn là giao thức tầng Transport.
+ Nếu giao thức tầng Transport là TCP, thì Next Header =**6**
+ Nếu là UDP thì Next Header = **17**

Giao thức AH



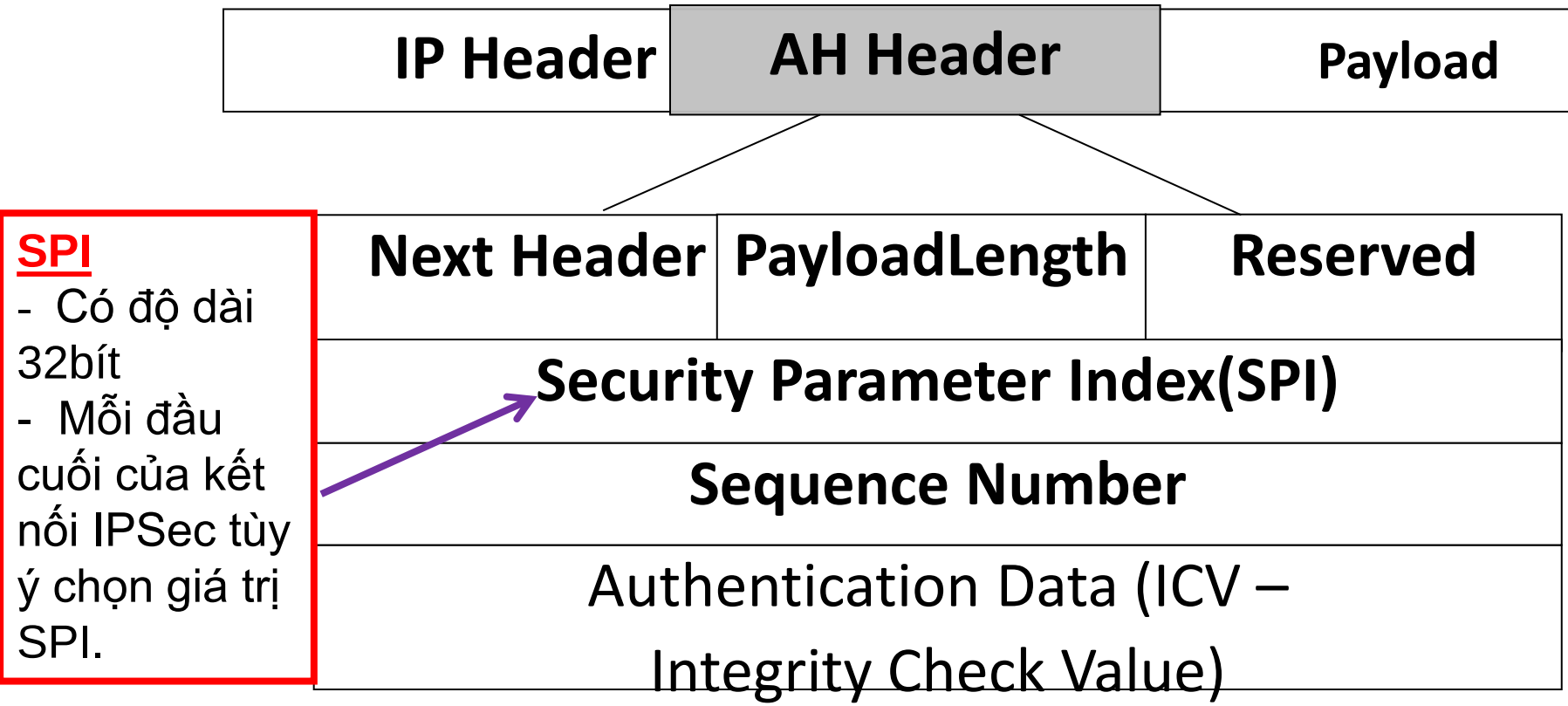
Payload Length:
-Chứa chiều dài của thông điệp sau AH Header.

Giao thức AH

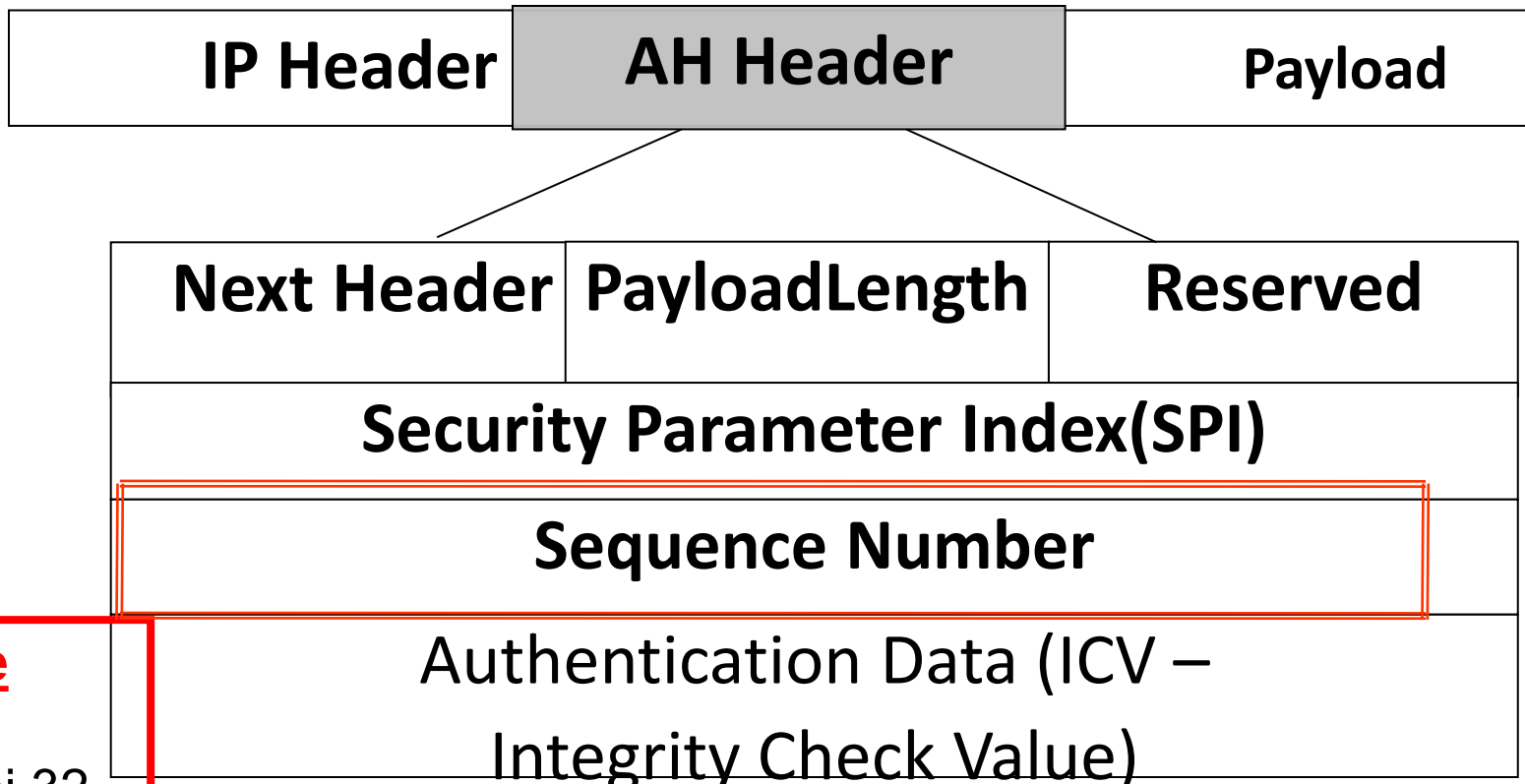


Reserved:
- Độ dài 16 bit
- trường này không được sử dụng
- Các bit đều bằng 0.

Giao thức AH


IP Header
AH Header
Payload
Next Header
PayloadLength
Reserved
Security Parameter Index(SPI)
Sequence Number
Authentication Data (ICV – Integrity Check Value)
SPI
- Có độ dài 32bít
- Mỗi đầu cuối của kết nối IPSec tùy ý chọn giá trị SPI.

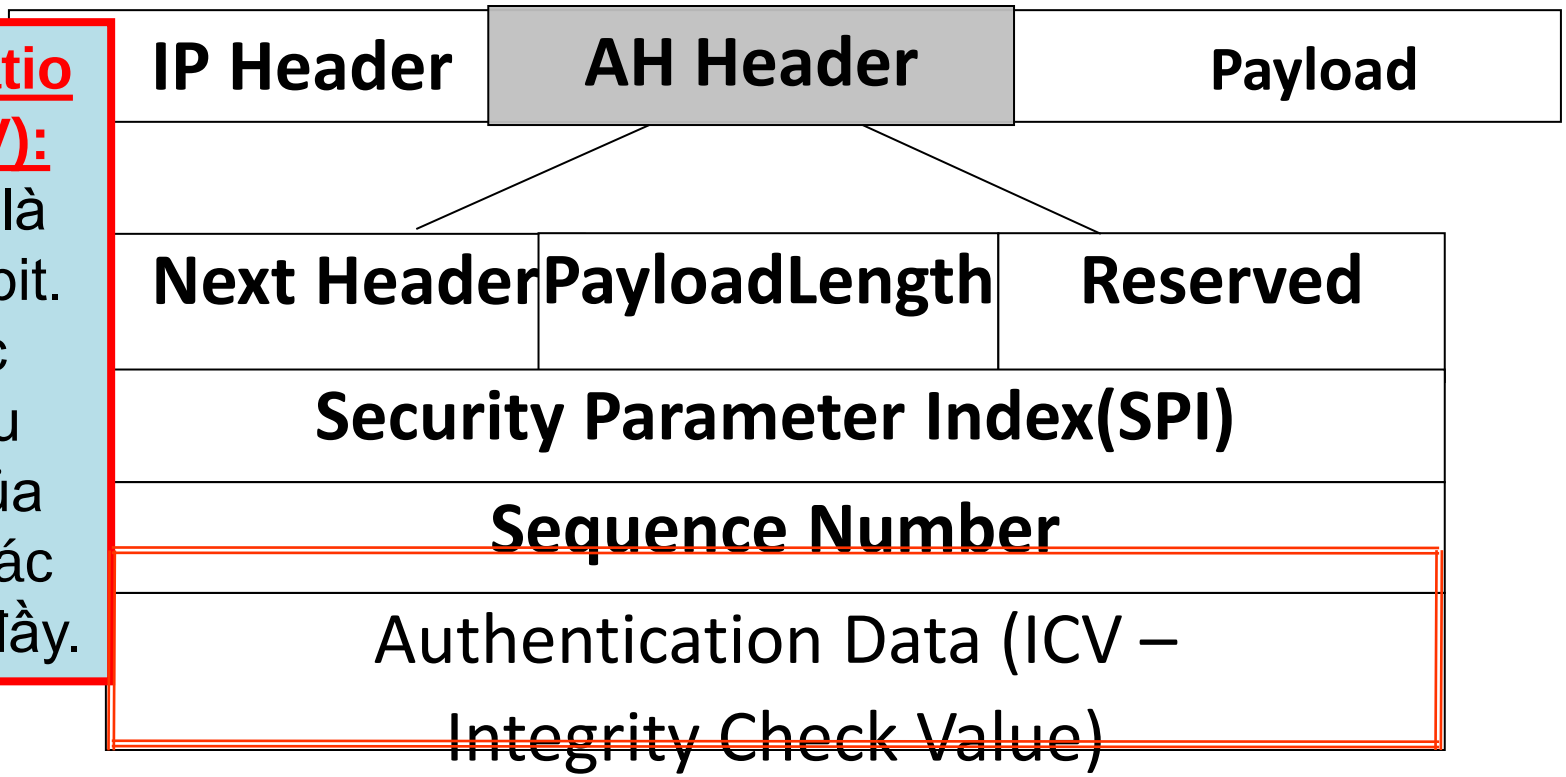
Giao thức AH



Sequence Number:
- Có độ dài 32 bit.
- Số tuần tự của gói tin AH

Giao thức AH

Authentication Data (ICV):
- Có độ dài là bội của 32 bit.
- Phải được padding nếu chiều dài của ICV trong các byte chưa đầy.



HMAC-SHA1-96, HMAC-MD5-96

Authentication Data (ICV): 96 bit

ICV = Hash (IP Header + Payload + Key)

Giao thức AH

Xử lý gói AH đầu vào & đầu ra

(SV tìm hiểu thêm trong Giáo trình "Các giao thức bảo mật mạng riêng ảo", HVKTMM, năm 2013)

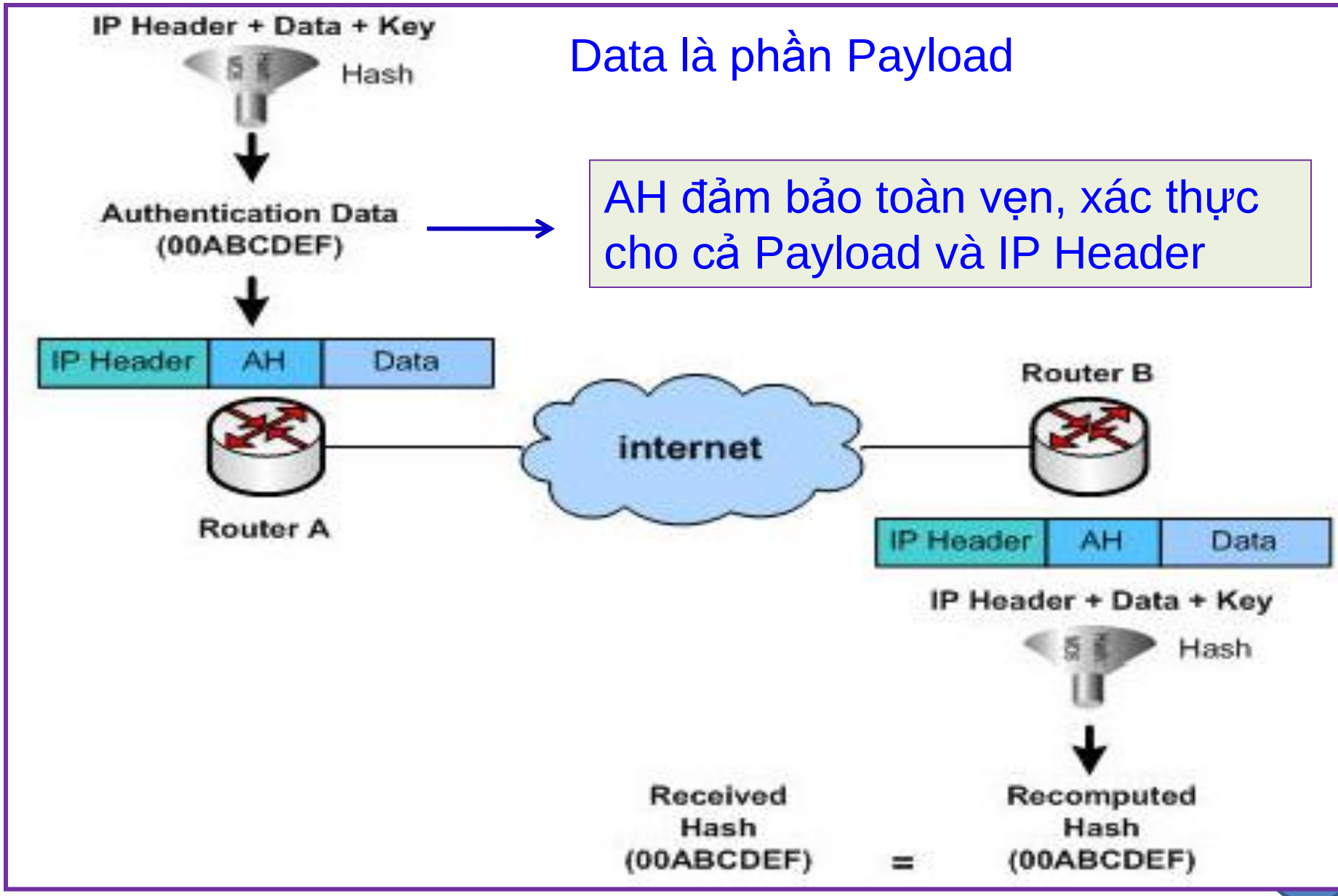
Giao thức AH

- Xử lý gói đầu vào:
  - Ghép mảnh:
  - Tìm kiếm SA
  - Kiểm tra SN (Sequence Number):
- Xử lý gói đầu ra:
  - Tìm SA
  - Tạo SN (Sequence Number):
  - Tính ICV
  - Padding
  - Phân mảnh

Giao thức AH

AH: Xác thực & toàn vẹn dữ liệu

Giao thức AH

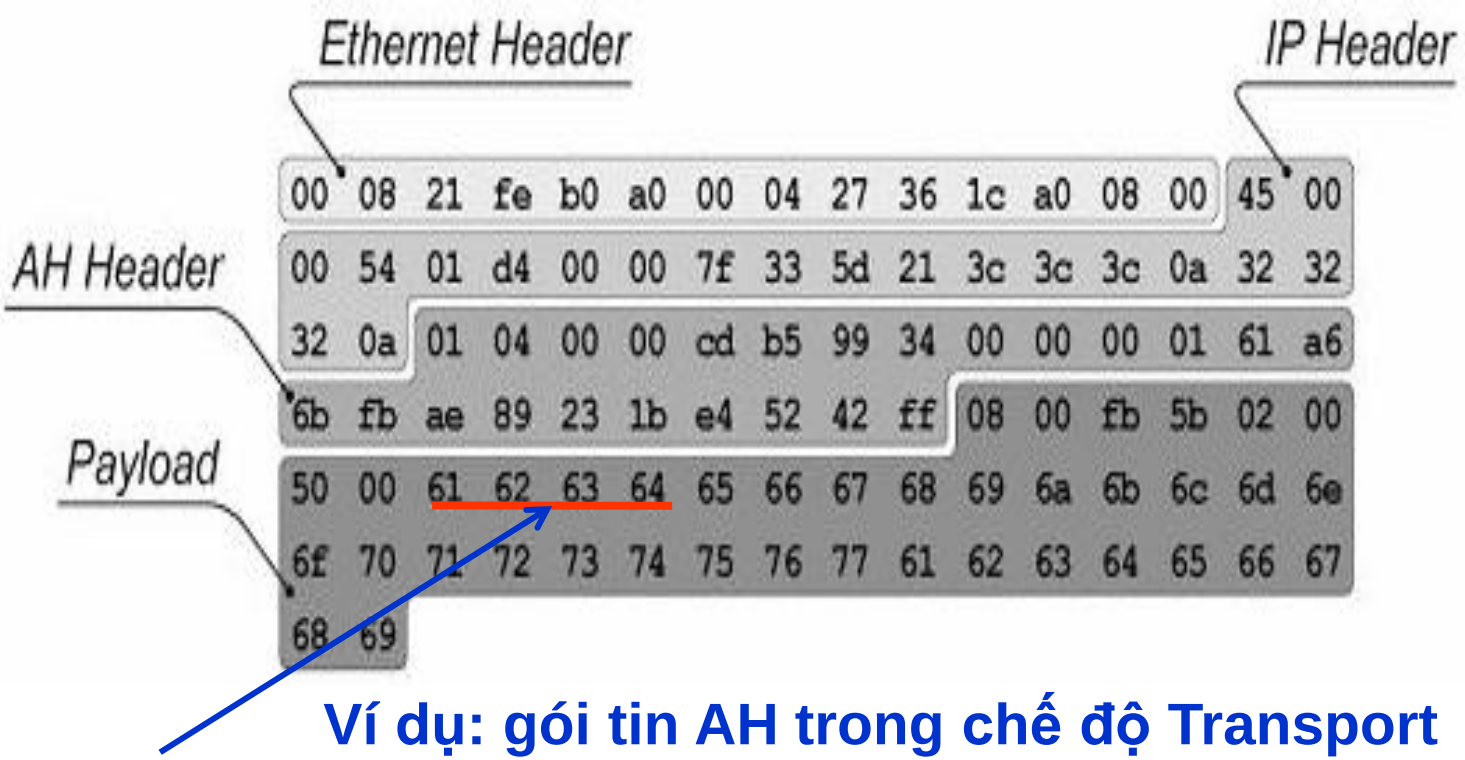

IP Header + Data + Key
Hash
Authentication Data
(00ABCDEF)
Data là phần Payload
AH đảm bảo toàn vẹn, xác thực cho cả Payload và IP Header
IP Header
AH
Data
Router A
internet
Router B
IP Header
AH
Data
IP Header + Data + Key
Hash
Received Hash (00ABCDEF)
=
Recomputed Hash (00ABCDEF)

Giao thức AH

Phân tích gói tin AH

Giao thức AH

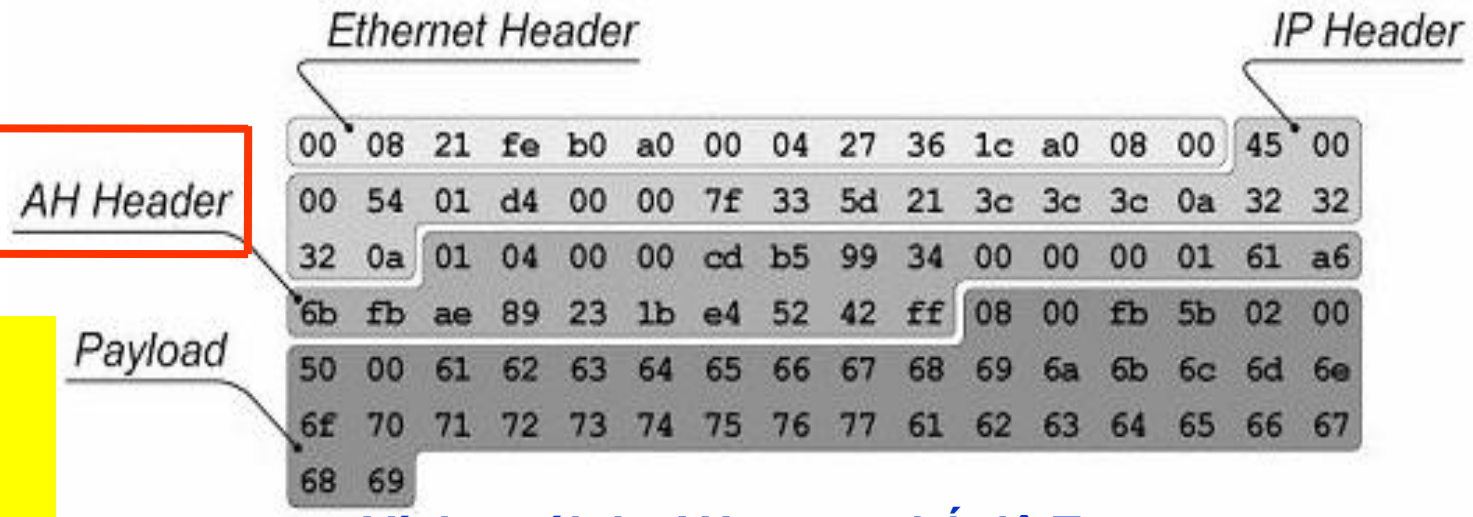
1. Đây là một gói AH ở chế độ Transport (chỉ có một IP Header)



Ví dụ: gói tin AH trong chế độ Transport

2. Phần Payload chứa ICMP echo Request (Ping). Ping gốc chứa chuỗi mẫu tự tăng dần bởi giá trị Hex

Giao thức AH



Ví dụ: gói tin AH trong chế độ Transport

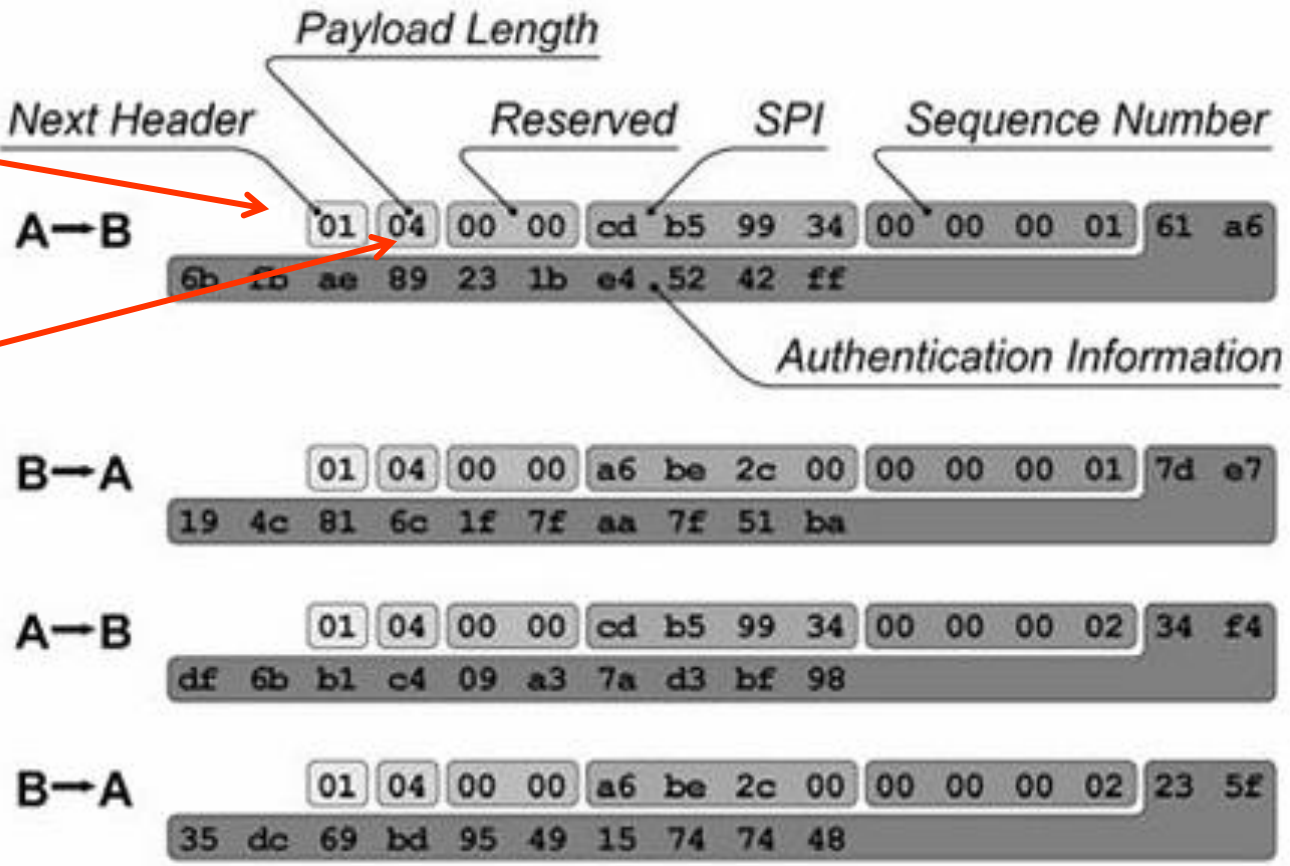
4. Phân tích các trường trong AH Header

3. Sau khi áp dụng AH, phần ICMP Payload không thay đổi (không được mã hóa)
Vì AH chỉ cung cấp toàn vẹn, xác thực.

Giao thức AH

Next Header (1B) =1 => ICMP

Payload Length (1B) =4, phần Payload có 4 Byte

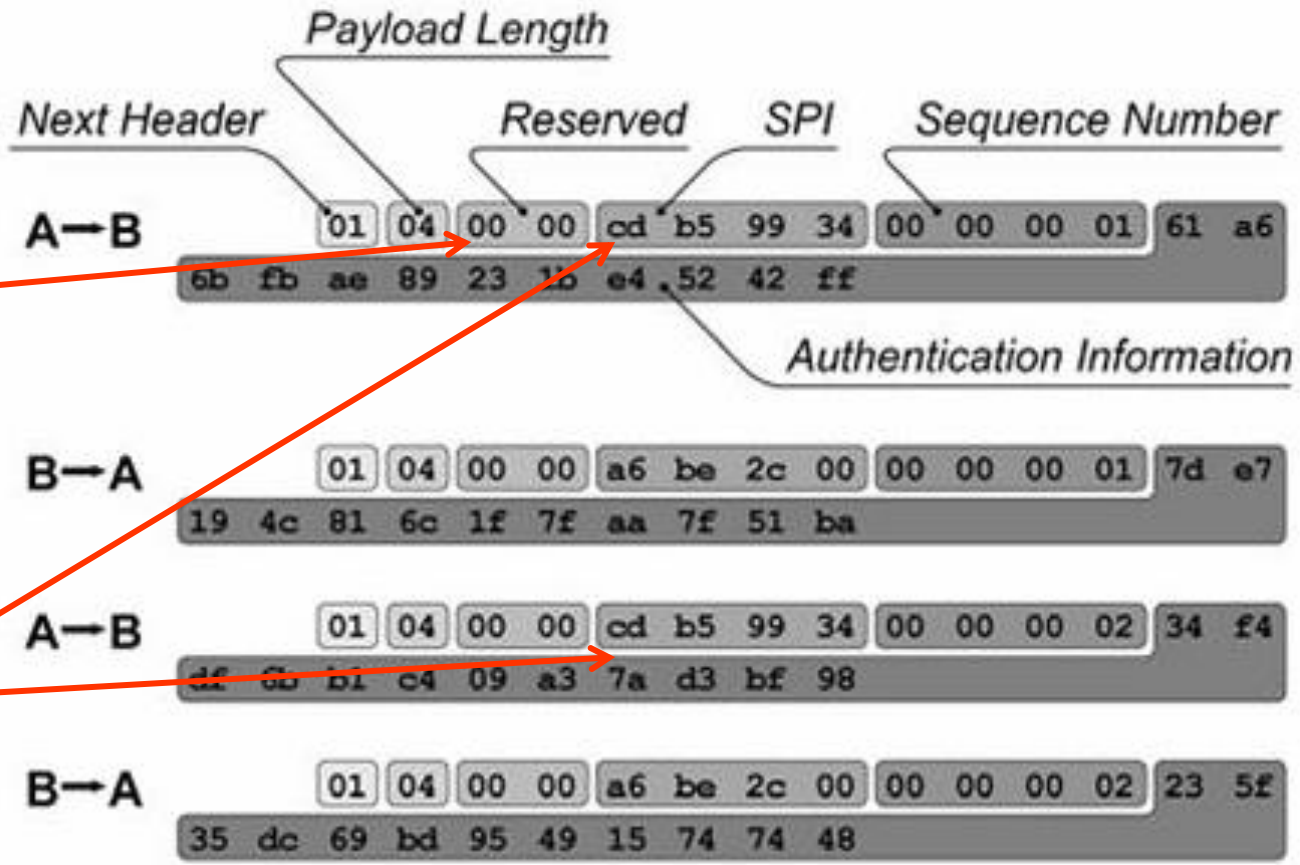


4 gói tin đầu tiên trong phiên AH giữa host A và host B

Giao thức AH

Reserved (2B) =0000, không sử dụng.

SPI của A (4B) =cdb59934

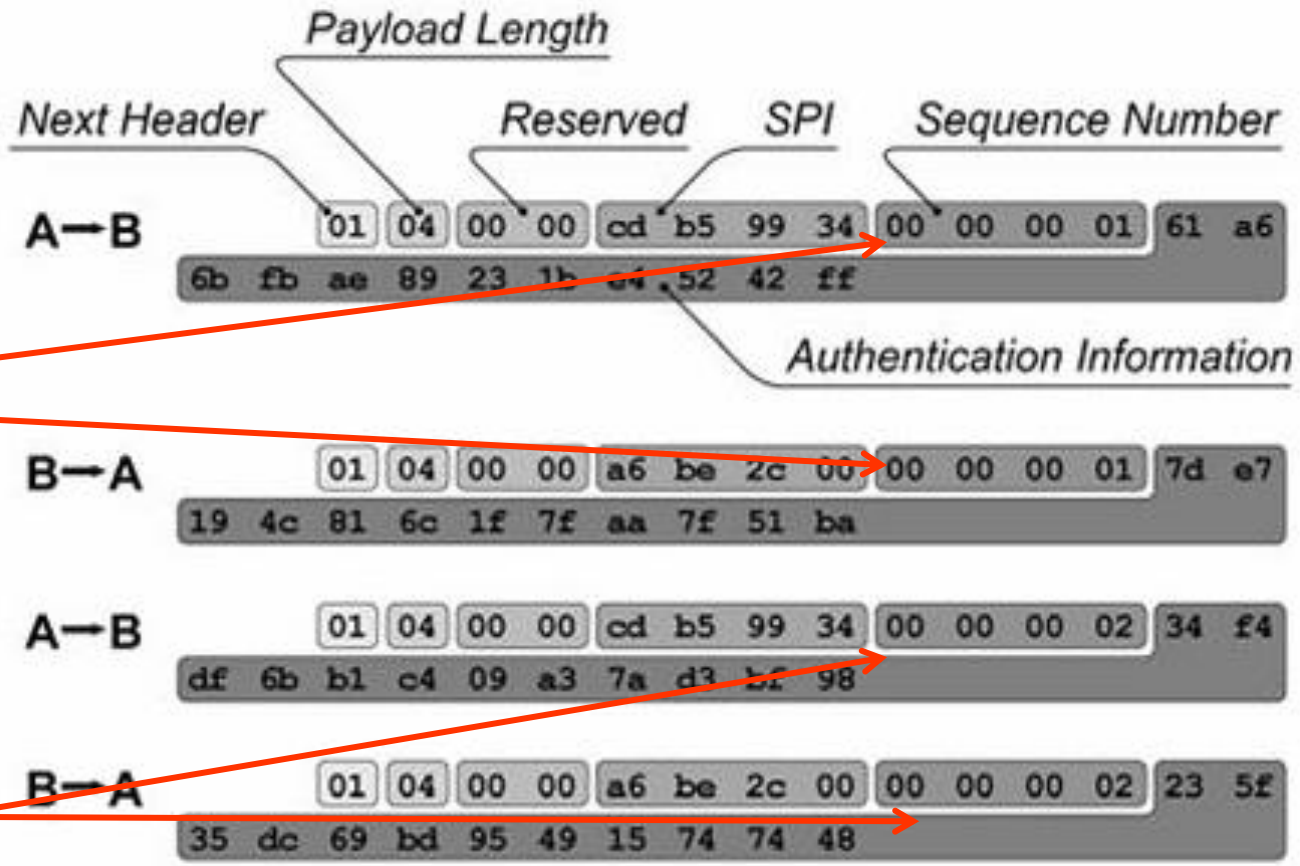


4 gói tin đầu tiên trong phiên AH giữa host A và host B

Giao thức AH

Sequence Number (4B), cả 2 host đều được thiết lập =1

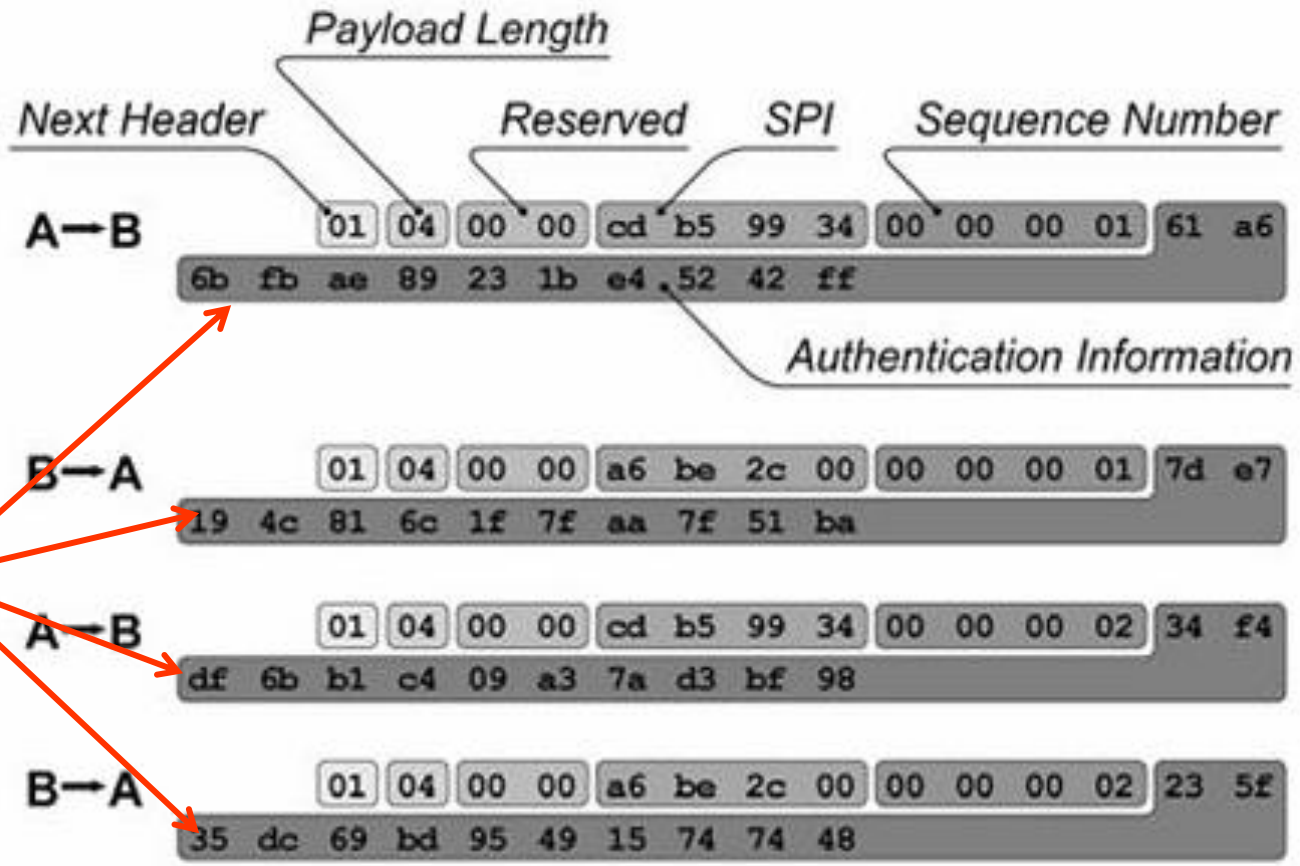
Sequence Number (4B), cả 2 host đều tăng lên 2 với gói tin thứ 2.



4 gói tin đầu tiên trong phiên AH giữa host A và host B

Giao thức AH

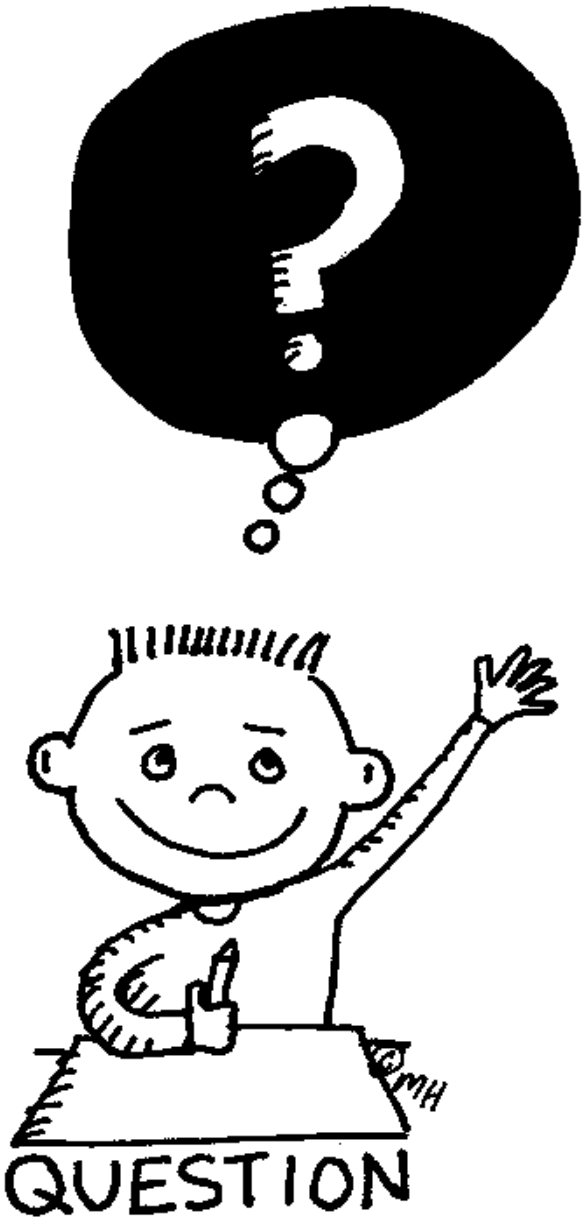
Authentication Information: phần ICV được băm để đảm bảo tính toàn vẹn, xác thực của mỗi gói tin = 96 bit (12 byte)



4 gói tin đầu tiên trong phiên AH giữa host A và host B

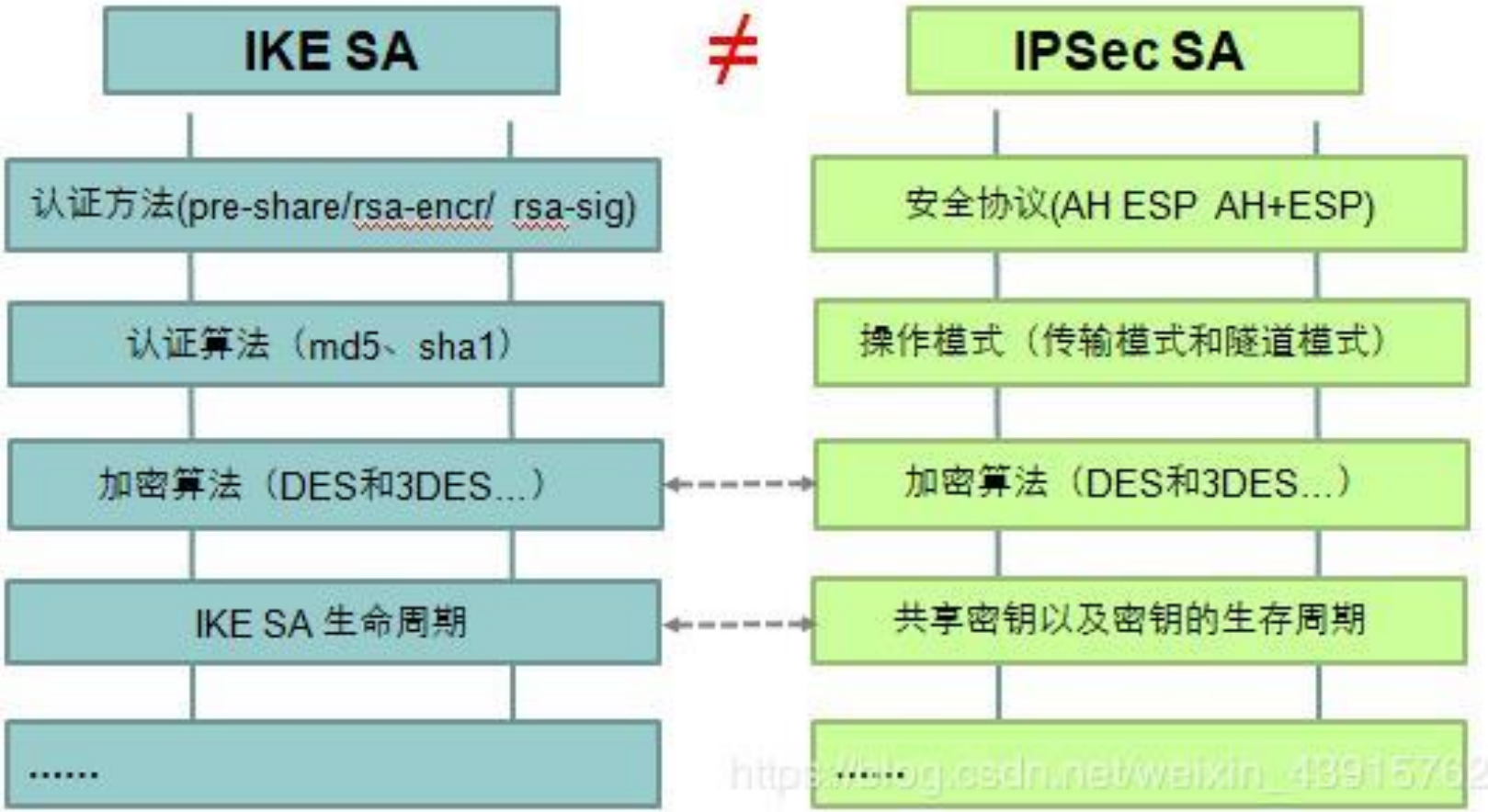
Tóm lược về giao thức AH

- AH cung cấp dịch vụ đảm bảo tính toàn vẹn, xác thực (cả dữ liệu và header) và chống replay gói tin cũ.
- AH hoạt động ở hai chế độ: Tunnel Mode, Transport Mode
- Trong IPSec version 1, giao thức ESP chỉ cung cấp mã hóa, không xác thực và toàn vẹn => người ta thường kết hợp AH và ESP
- AH version 3 hỗ trợ: HMAC-SHA1-96, HMAC-MD5-96, AES-XCBC-MAC-96


QUESTION

Ví dụ (4) về IPSec SA

IKE SA与IPSec SA



Host SPD example

- SPD for host 1.2.3.101 in intranet 1.2.3.0/24, connecting to server 1.2.4.10 in network 1.2.4.0/24 (DMZ) and to the Internet

Protocol	Local IP	Port	Remote IP	Port	Action	Comment
UDP	1.2.3.101	500	*	500	BYPASS	IKE
ICMP	1.2.3.101	*	*	*	BYPASS	Error messages
*	1.2.3.101	*	1.2.3.0/24	*	PROTECT: ESP in transport-mode	Encrypt intranet traffic
TCP	1.2.3.101	*	1.2.4.10	80	PROTECT: ESP in transport-mode	Encrypt to server
TCP	1.2.3.101	≥1024	1.2.4.10	443	BYPASS	Allow TLS, no double encryption
*	1.2.3.101	*	1.2.4.0/24	*	DISCARD	Others in DMZ
*	1.2.3.101	*	*	*	BYPASS	Internet

- What is the danger in bypassing TLS traffic (line 5)?
- What is the danger in bypassing outbound ICMP (line 2)?
- Note that the other endpoint (other intranet hosts and 1.2.4.10) must have an IPsec policy that specifies the same protection for the same packets