IP Security
- PartII

Professor Yeali S. Sun
Information Management Department
National Taiwan University

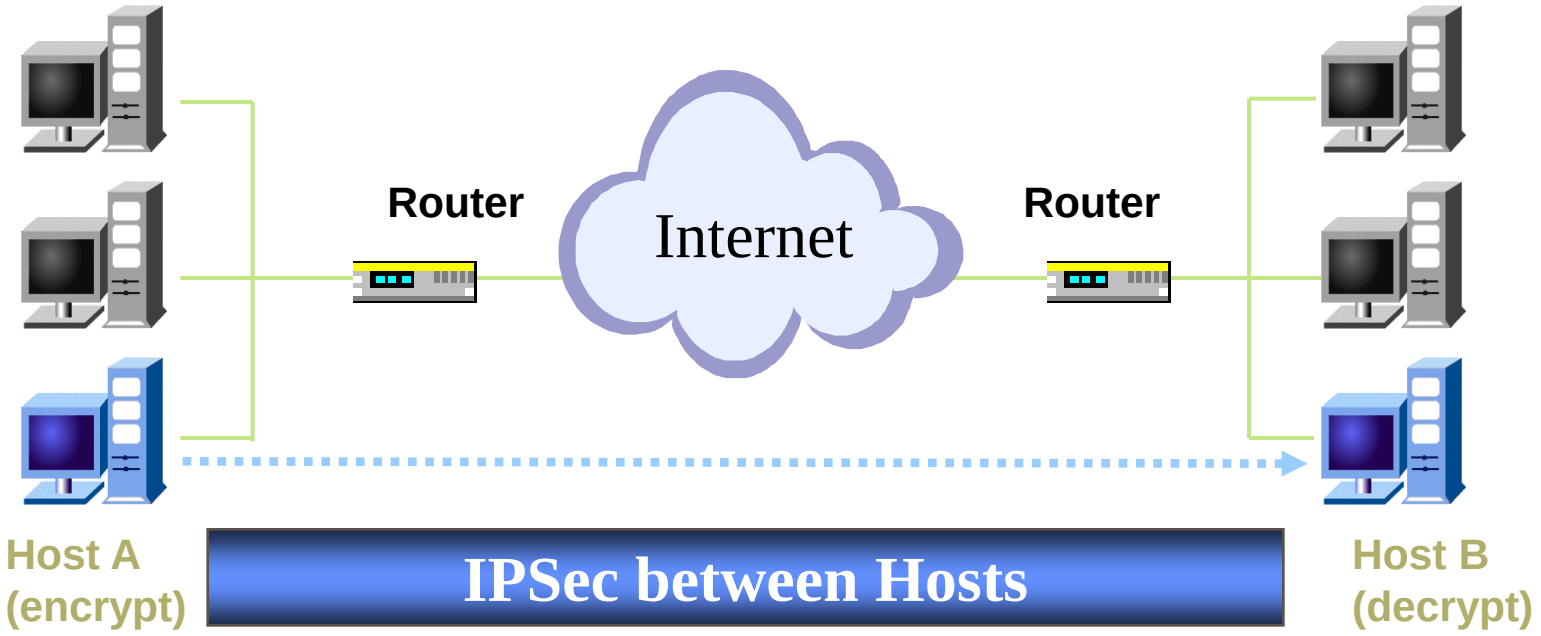
Security Protocols

- Operation Modes
- AH - Authentication Header
- ESP - Encapsulating Security Payload

Security Protocol – Operation Modes

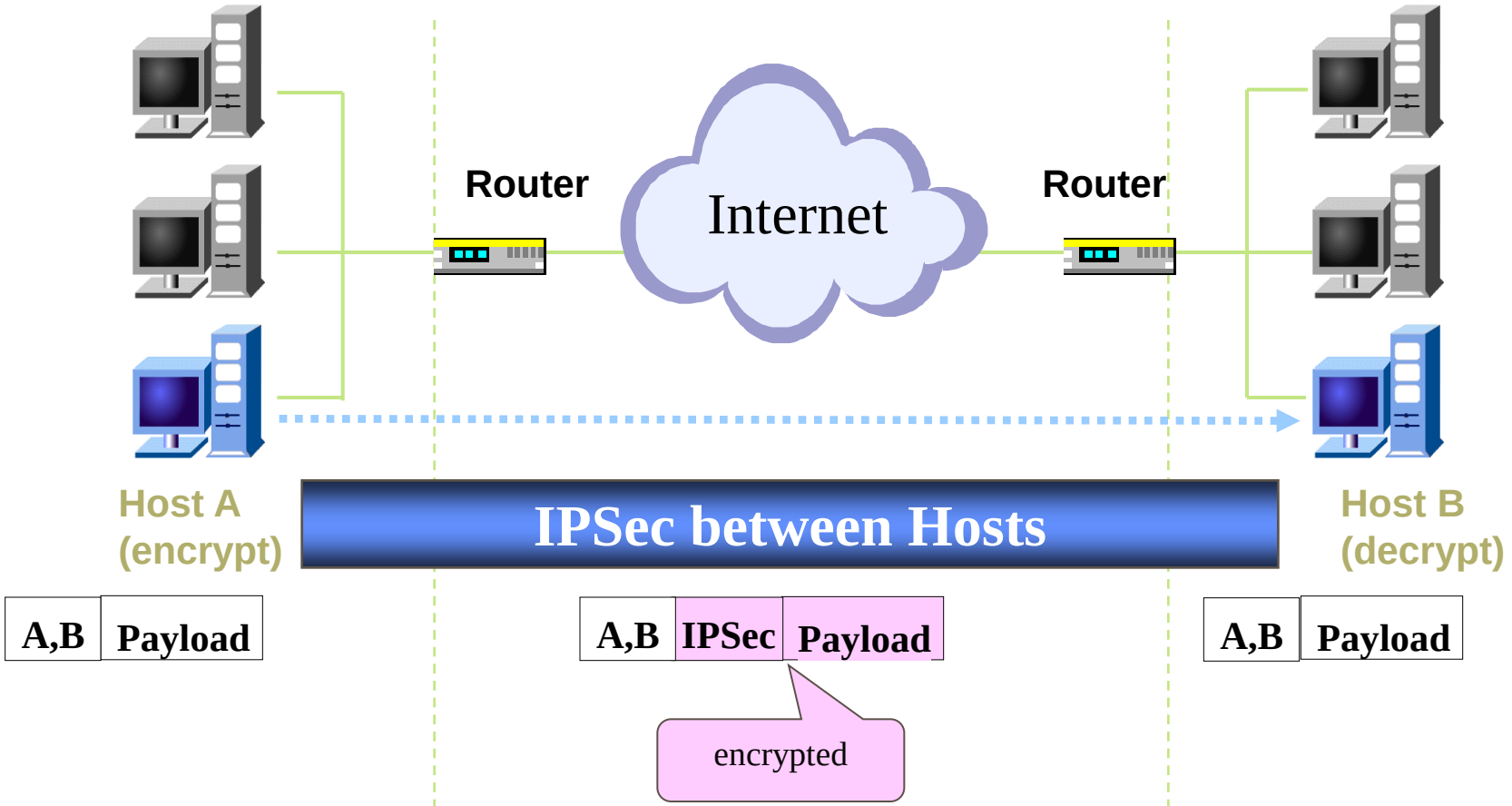
- Both AH and ESP support two modes
  - Transport
  - Tunnel

Transport Mode



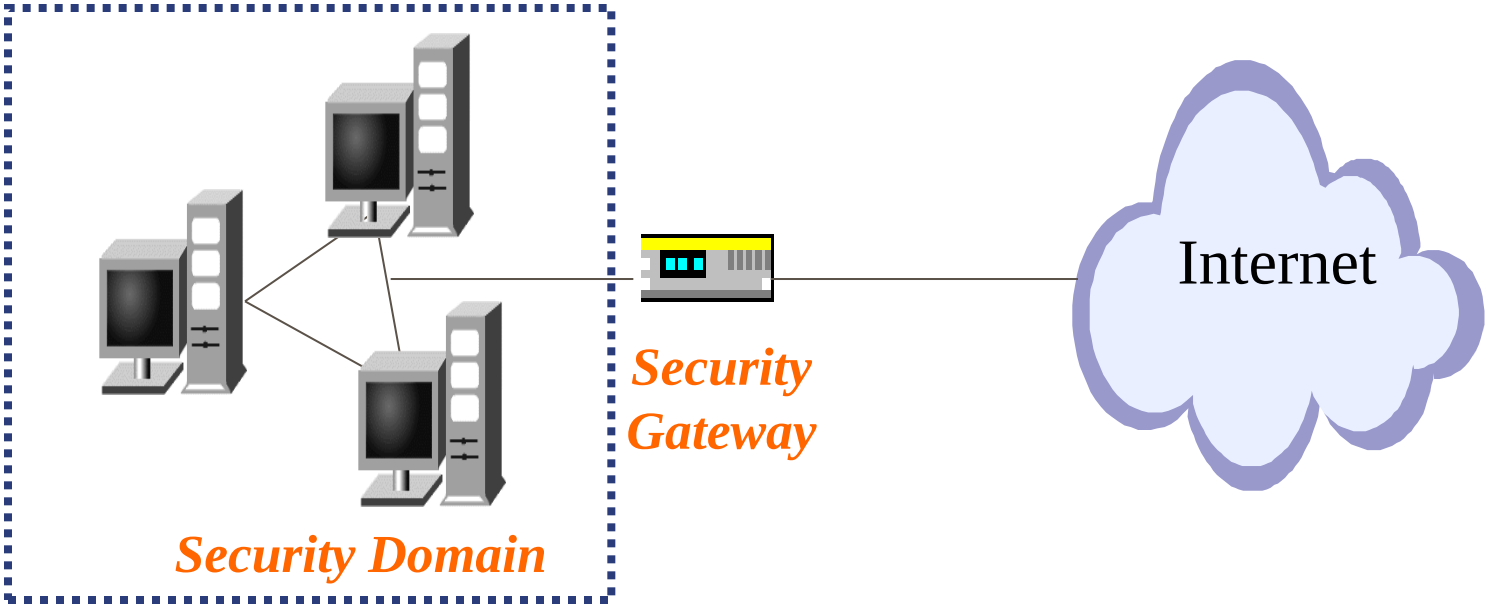
- Used for secure end-to-end communication between two ***hosts*** (host-to-host)
- Provides protection for *upper-layer protocols*, i.e., the payload of an IP packet

Transport Mode (cont'd)



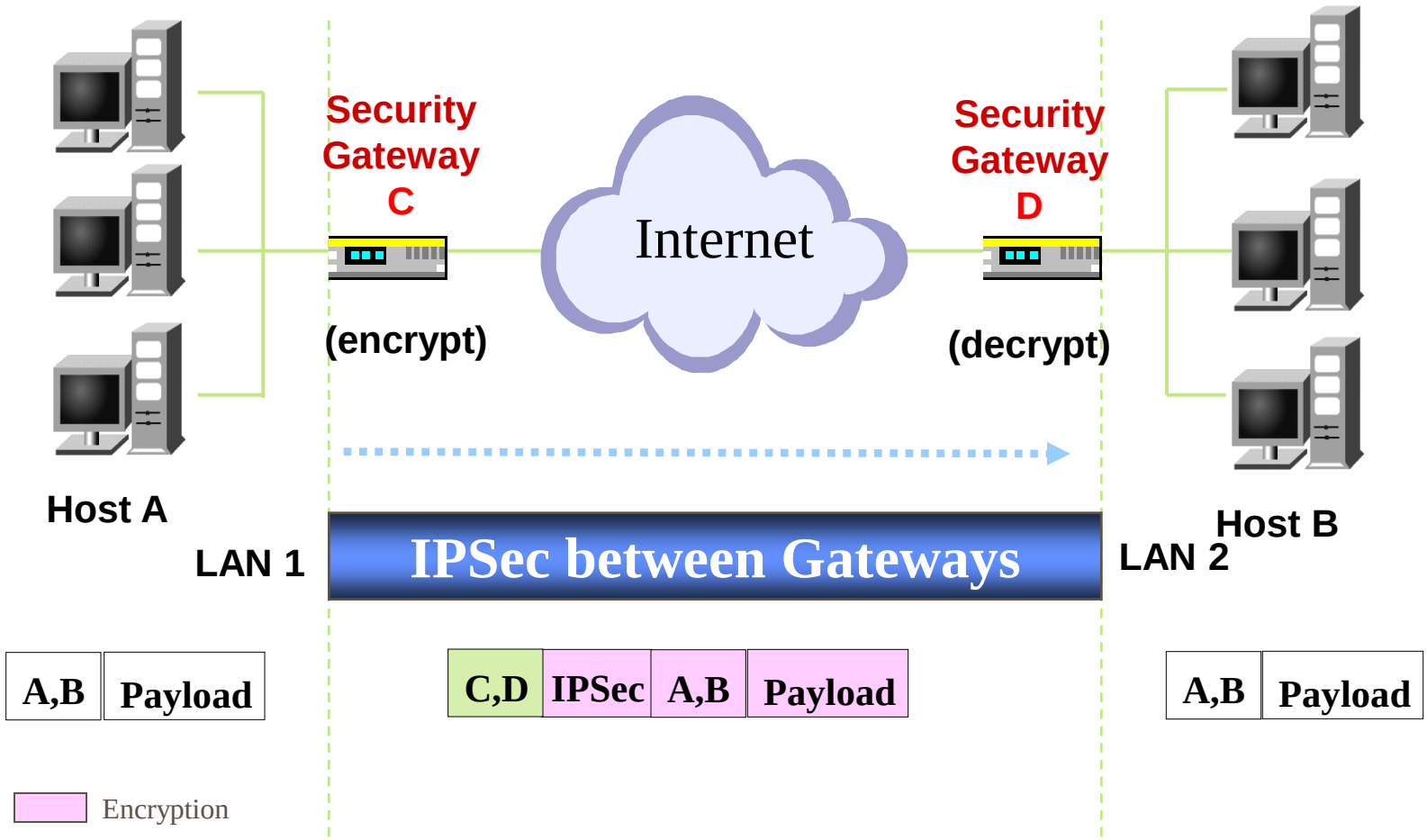
- In AH, IP payload and selected portions of the IP header are authenticated.
- In ESP, only IP payload is encrypted and optionally authenticated but NOT the IP header.

Tunnel Mode (1/3)



- Provides protection to the **entire** IP packet.
- The AH or ESP fields are added to the IP packet.

Tunnel Mode (2/3)



Tunnel Mode (3/3)

- The entire packet plus IPsec info is treated as the payload of the new IP packet with a new IP header.
- The new header may contain different source and destination addresses.
- Used when one or both ends of an SA is a security gateway (e.g., firewall or router with IPsec), i.e., Gateway-to-Gateway or Gateway-to-Host

Authentication Header (AH)

Authentication Header (AH) (1/2)

Functions

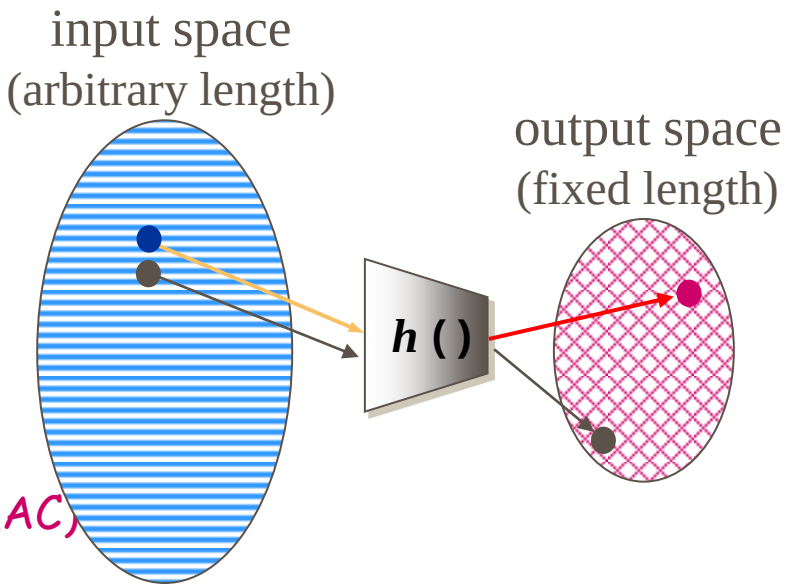
- Provides support for authentication of IP packets and data integrity
- Data Origin Authentication
- Connectionless Integrity

Goals

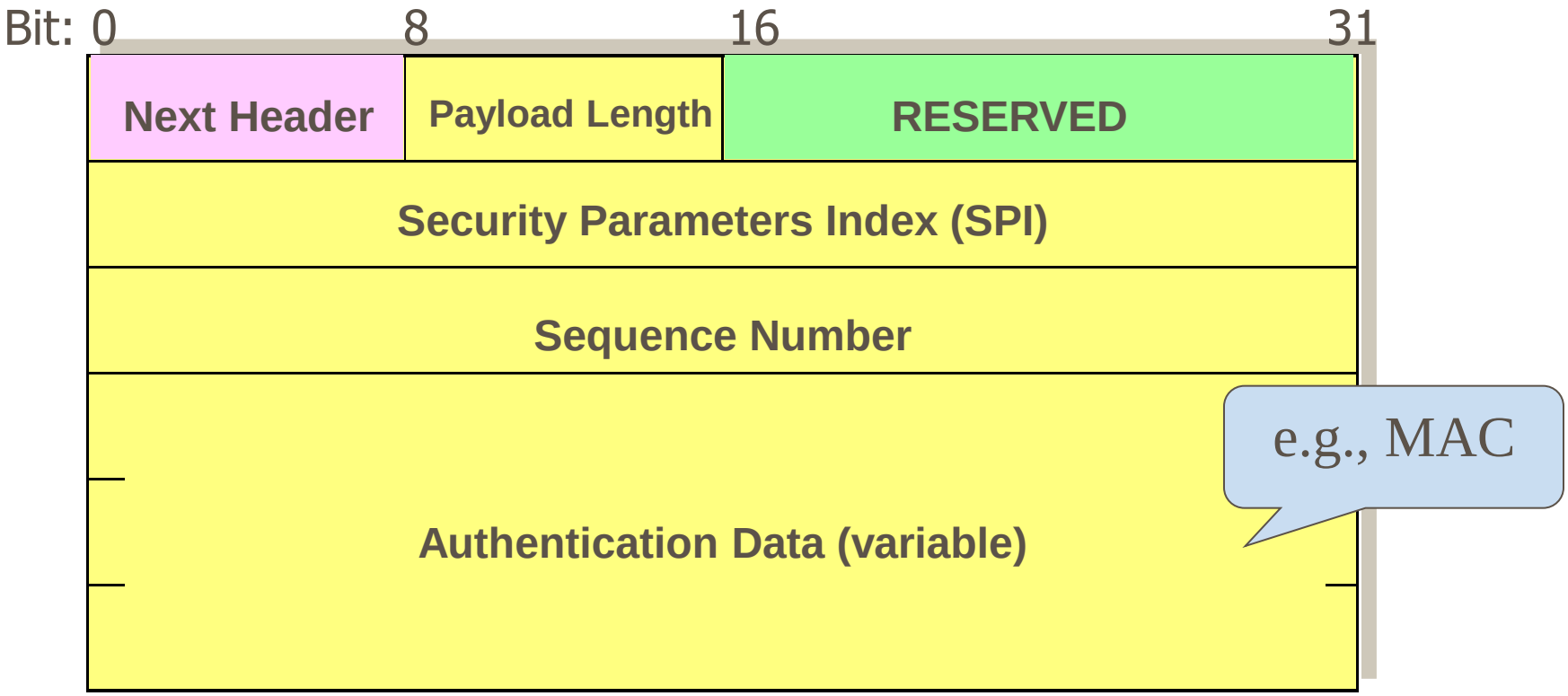
- Ensures NO undetected modification to a packet's content
- Prevents address spoofing attack
- Guards against the replay attack
- Use of Message Authentication Code (MAC)
  - Communicating two parties must share a secret key.

AH: Basic Idea (2/2)

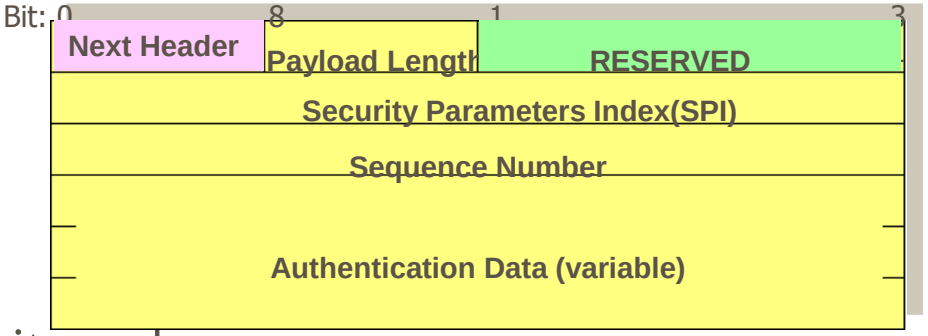
- Irreversable one-way hash function
  - output is unique
  - $h( )$ is easy, $h^{-1}( )$ is hard
- Two ways
  - without key
    - message digest
  - with key
    - message authentication code (MAC)
- Ex:
  - MD2，Md4，MD5 (128-bit)
  - SHA (160-bit)，SHA-1
  - RIPE-MD，HAVAL….



Authentication Header



AH Format



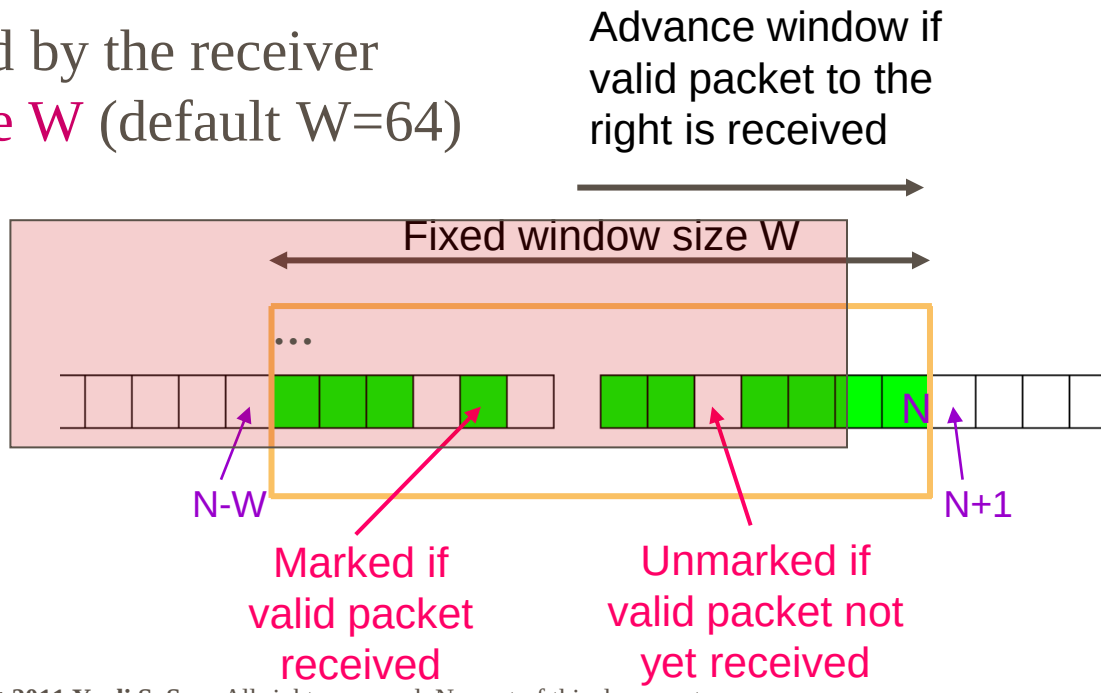
- Fixed AH header – three 32-bit words
- Next Header (8 bits)
  - Identifies the type of header immediately following this header
- Payload Length (8 bits)
  - Length of AH in 32-bit words, minus 2
  - Default AH data field is three 32-bit words
- Reserved (16 bits)
- Security Parameters Index (32 bits)
  - Identifies an SA
- Sequence Number (32 bits)
  - Initial value = 0
  - Incremented by one for each packet transmitted
- Authentication Data (variable)
  - Contains the Integrity Check Value (ICV) or MAC for this packet

Anti-Replay Service

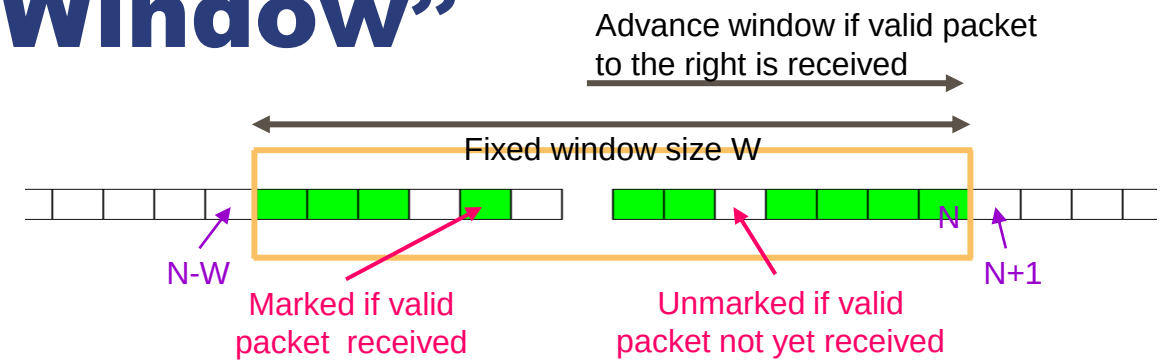
- A Replay Attack
  - An attacker obtains a copy of an authenticated packet and later transmits it to the intended destination.
  - The receipt of duplicate, authenticated IP packets may have some other undesired consequence.
- Sequence number
  - Initialized to 0; incremented by one for each packet transmitted; never cycle past 2^{32}-1 back to zero
- To prevent multiple valid packets with the same sequence number
- If the limit is reached, the sender should terminate current SA and negotiate a new SA with a new key.

Anti-Replay Mechanism

- Motivation
  - In the Internet, IP packets may be lost, arrive destination out of order or in duplicate.
- Anti-Replay Window
  - Implemented by the receiver
  - Window size W (default W=64)



Anti-Replay "Window" (cont'd)



- If a received packet falls within the window and is *new*, *the MAC is checked*.
  - If the packet is *authenticated*, the corresponding slot in the window is *marked*.
- If a received packet is to the *right* of the window and is *new*, *the MAC is checked*.
  - If the packet is *authenticated*, the window is *advanced* to this new sequence number and the corresponding slot in the window is *marked*
- If a received packet is to the left of the window, or if authentication fails, the packet is discarded.
  - This is an auditable event.

Integrity Check Value (ICV)

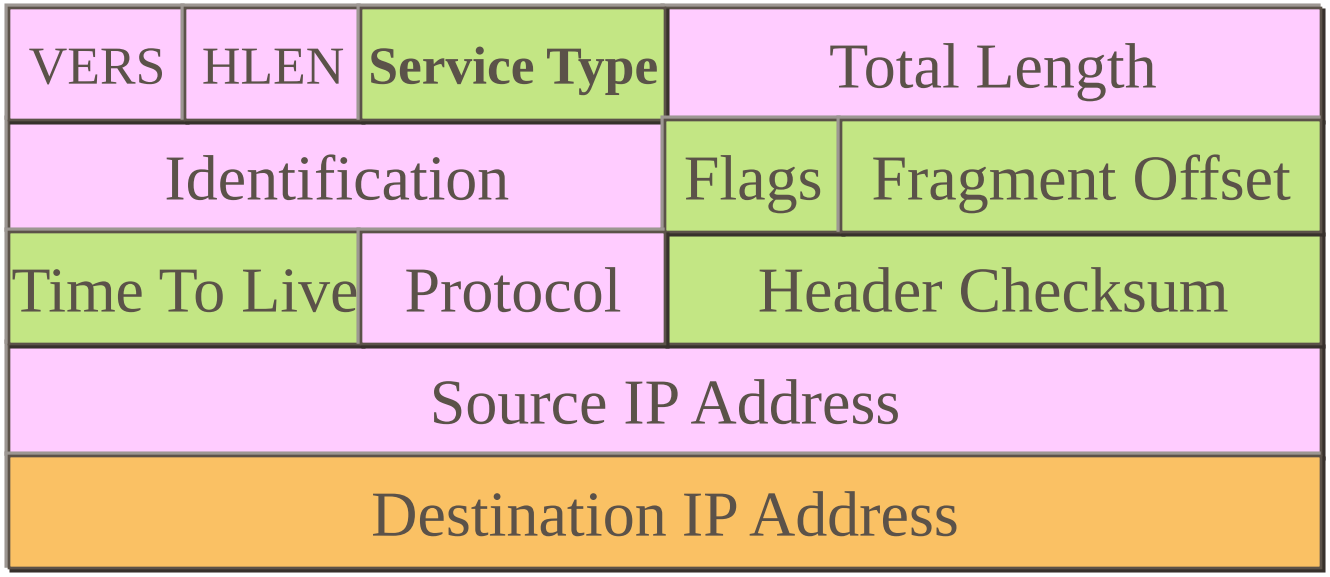
- In Authentication data field
- The ICV is a MAC (or truncated)
- The specification includes the support of
  - HMAC-MD5-96
  - HMAC-SHA-1-96

- HMAC-MD5-96 (*RFC-2403*)
  - Input data : variable length (segmented into 64-byte data blocks）
  - Output：128-bit
  - MAC：96-bit
  - key：fixed 128-bit

- HMAC-SHA-1-96 (*RFC-2404*)
  - Input data : variable length (segmented into 64-byte data blocks)
  - Output：160-bit
  - MAC：96-bit
  - key：fixed 160-bit

MAC Calculation

IPv4 Packet Format

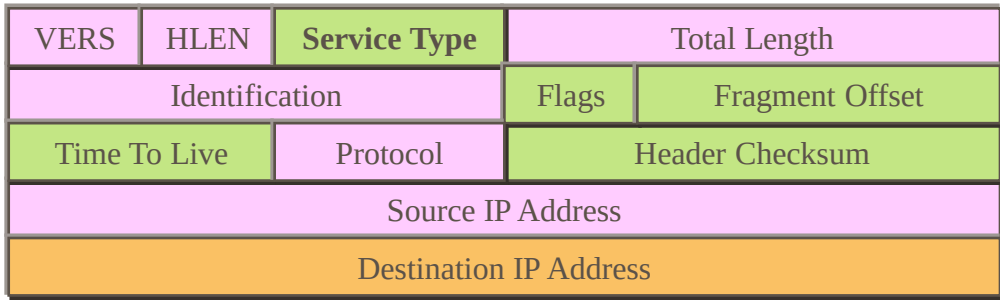


immutable

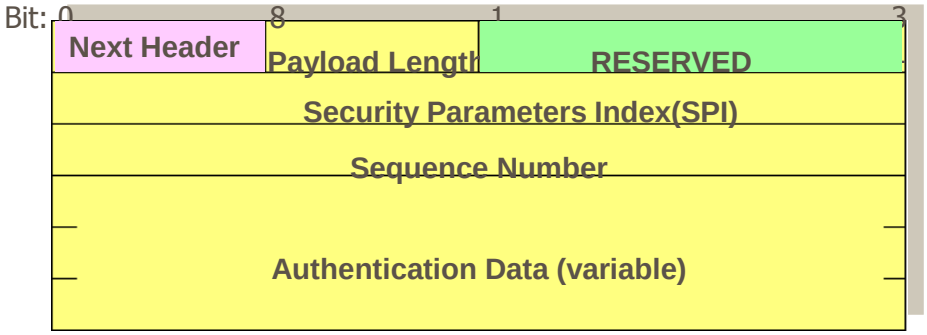
mutable

mutable but predictable

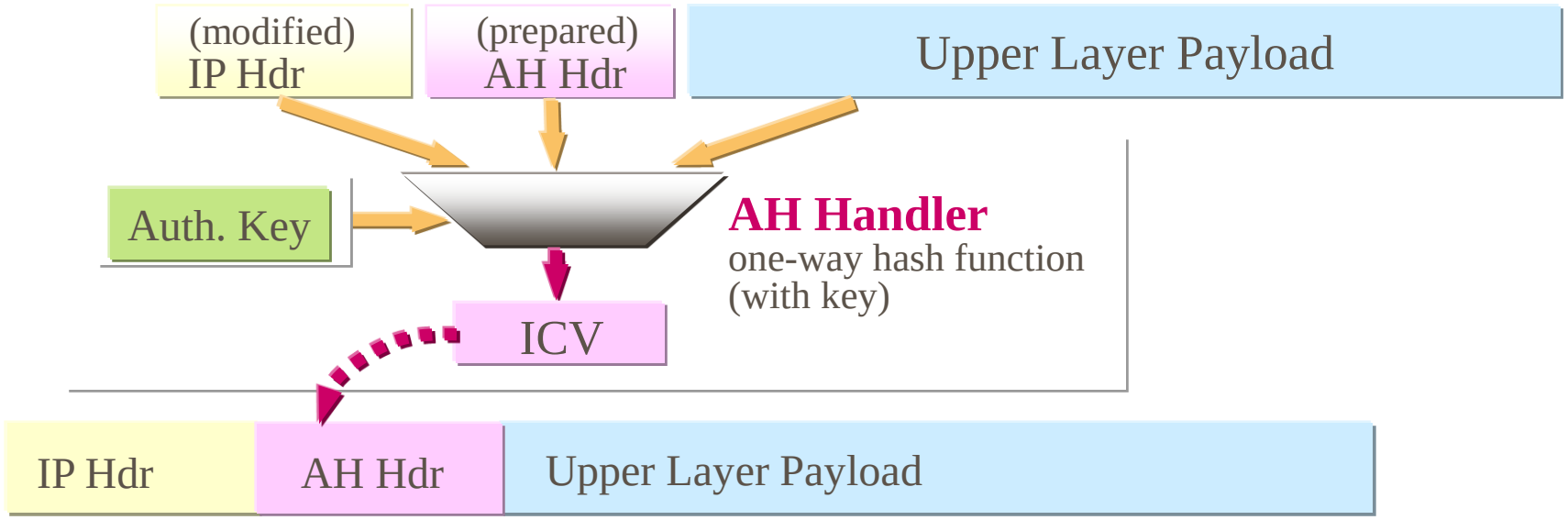
MAC Calculation Includes …



- IP header fields that do *not* change in transit (immutable) or are *predictable* in value upon arrival at the endpoint for the AH SA;
- Otherwise, the fields in the IP header are set to *zero* in calculation, e.g., TTL.
- The AH header other than the Authentication Data field which is set to zero in calculation.



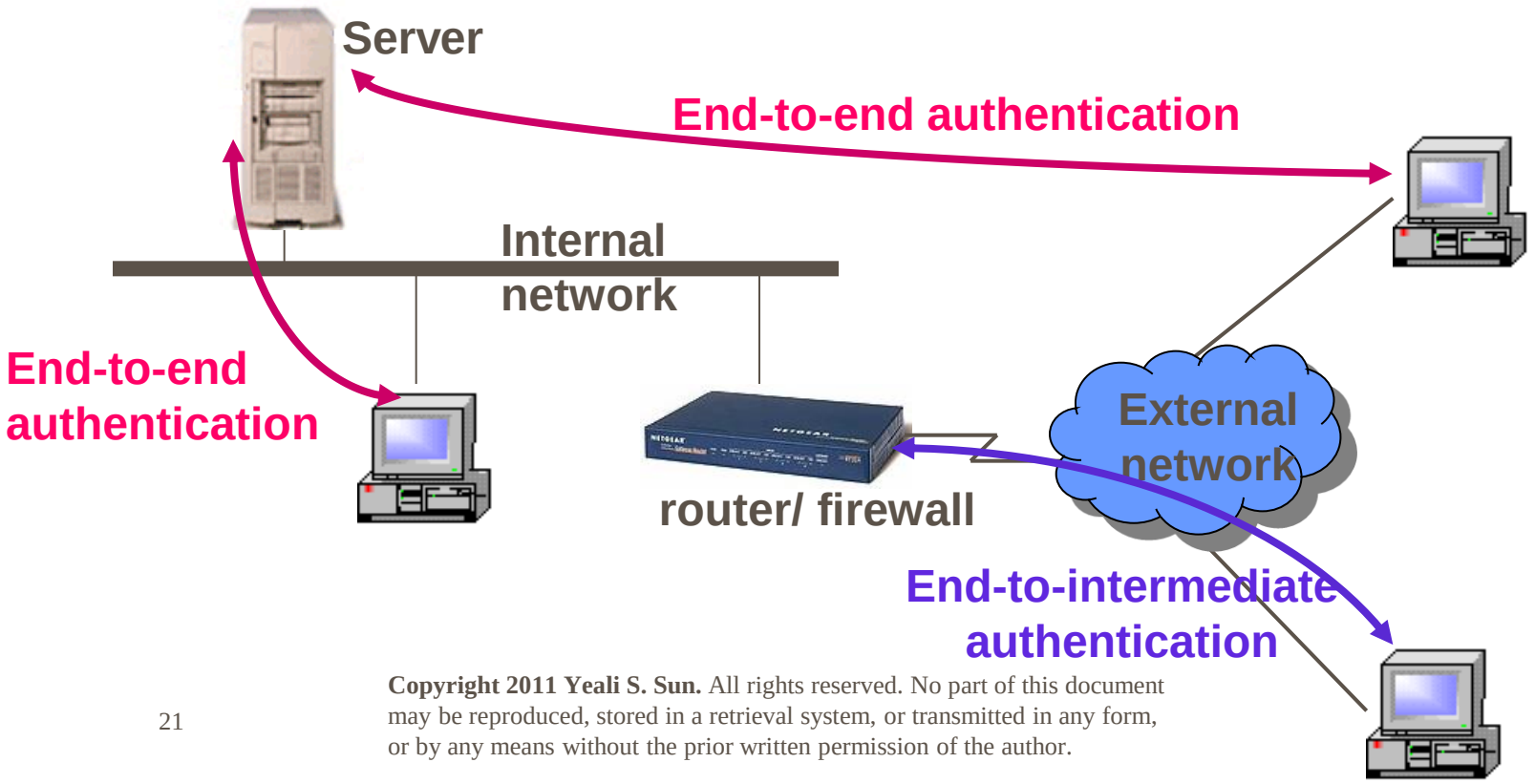
MAC Calculation in AH



The Scope of Authentication in AH

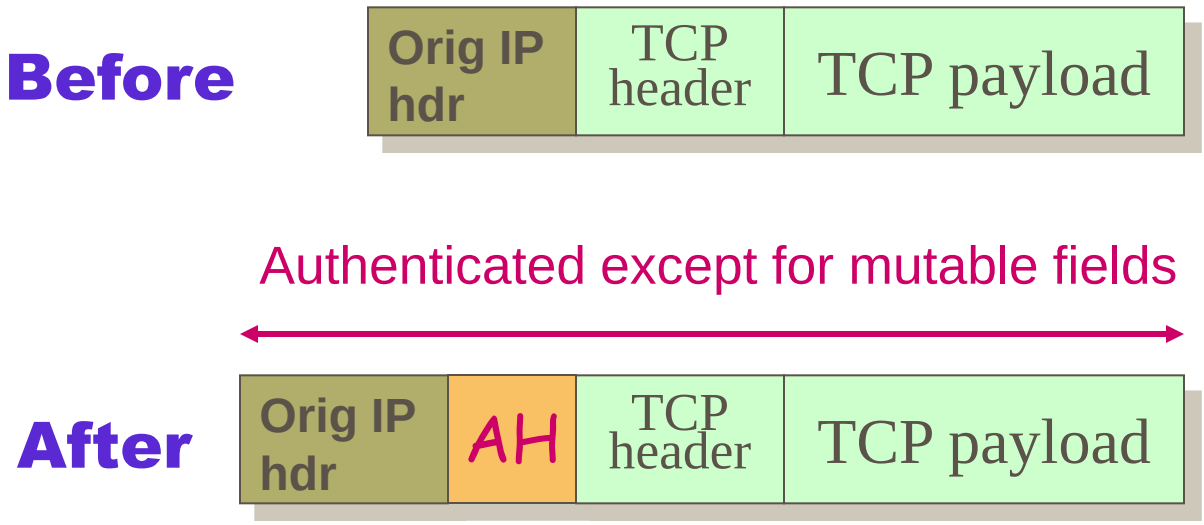
- Transport Mode – end-to-end authentication

vs. Tunnel Mode – end-to-intermediate authentication



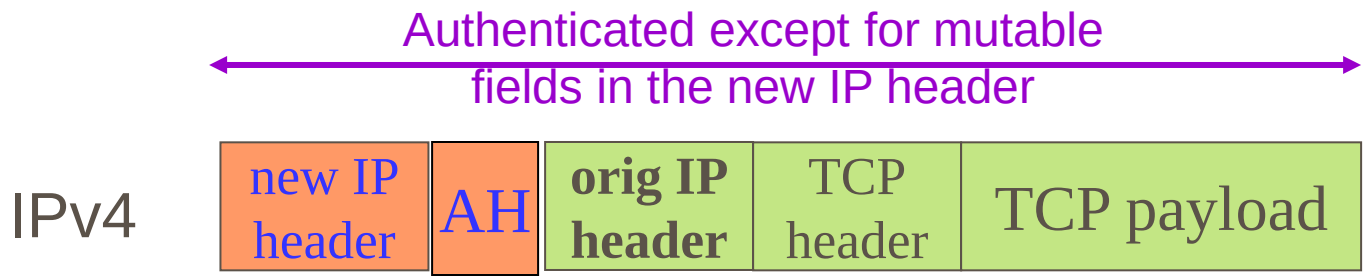
Transport Mode AH (1/2)

- In IPv4
  - The AH is inserted after the original IP header and before the IP payload
  - Authentication covers the entire packet



Tunnel Mode AH

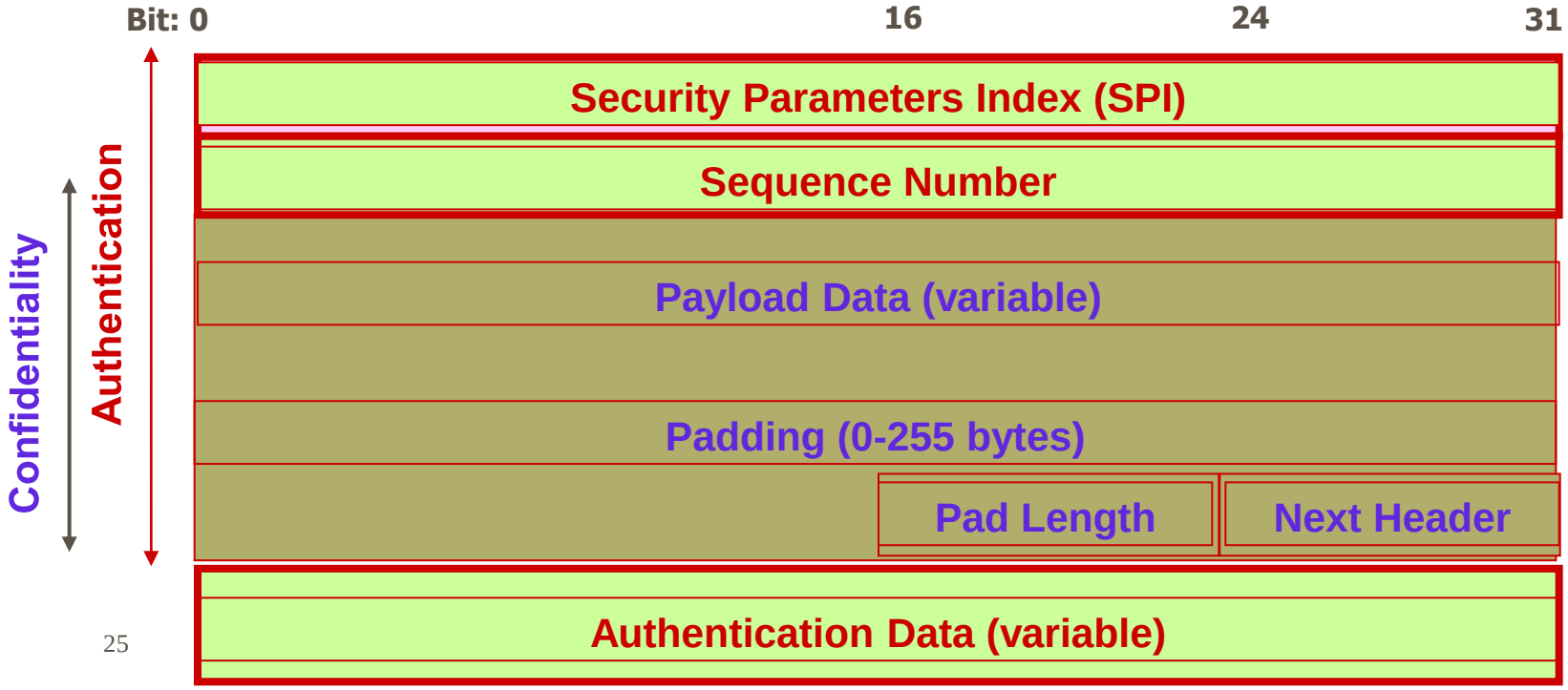
- A new IP header is generated.
- Authentication covers the *entire original packet* and the *new IP header*.
- AH is inserted



Encapsulating Security Payload (ESP)

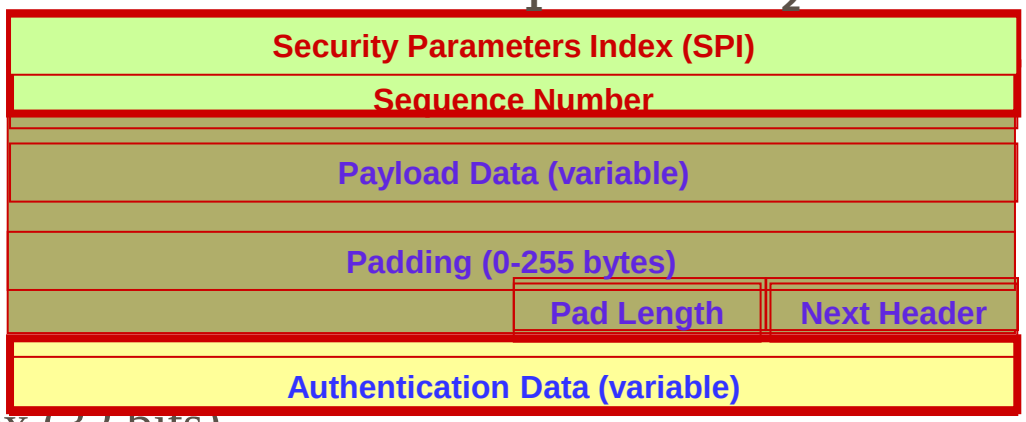
Encapsulating Security Payload (ESP)

- Provides *confidentiality* of message contents and limited traffic flow confidentiality.
  - Traffic flow confidentiality is to conceal source and destination addresses, message length, or frequency of communication by using ESP in tunnel mode, especially at a security gateway.
- ESP format



Transport mode

ESP Format



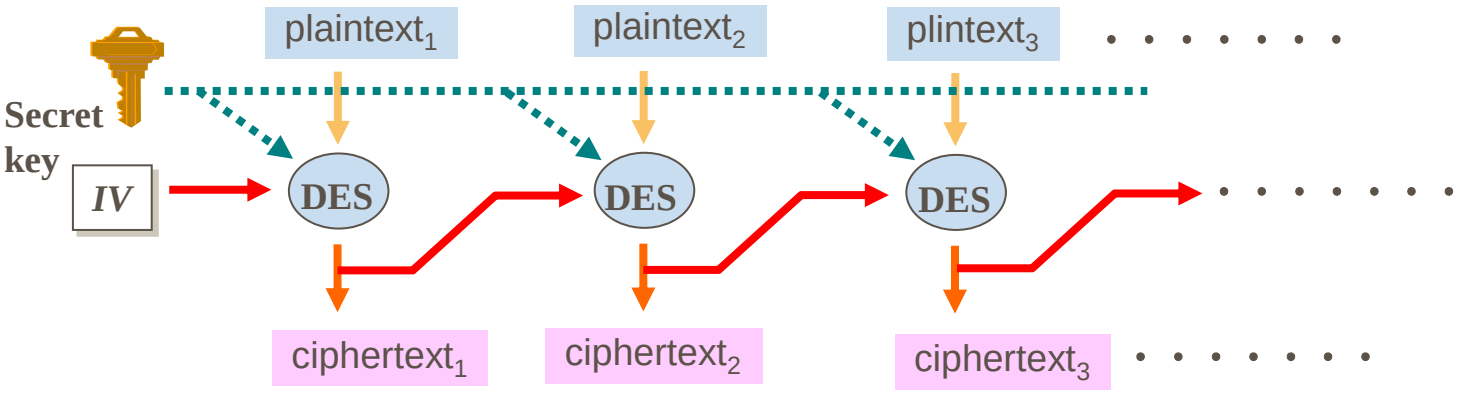
- Security Parameters Index (32 bits)
  - Identifies an SA
- Sequence Number (32 bits)
  - as in AH
- Payload Data (variable)
  - Contains transport-level segment (transport mode) or IP packet (tunnel mode) protected by encryption Padding (0-255 bytes)
- Pad Length (8 bits)
- Next Header (8 bits)
  - Identifies the type of data contained in the payload data field (e.g., an extension header in IPv6 or TCP in IPv4) (use protocol number 50 of IP header)
- Authentication Data (variable, optional)
  - Contains the Integrity Check Value (ICV) computed over the ESP packet minus the Authentication Data field

Encryption and Authentication Algorithms

- DES in Cyber Block Chaining (CBC) mode (RFC 2405)
  - key = 56 / 64-bit （（7-bit + 1-parity-bit）* 8）
  - data block = 64-bit
  - initialization vector (IV) = 64-bit
- ESP-NULL (RFC 2410)
  - No encryption (useful in tunnel mode)
  - Must do authentication
- 3DES
  - Triple-DES (RFC 2451)
  - key = 56*3 = 168-bit
  - security = （DES security）* 2^{56*2}
- Advanced Encryption Standard (AES)

ESP: DES-CBC

- Segment data stream into fixed-size data block
- Encryption Algorithm
  - The input: the XOR of the current plaintext block and the preceding ciphertext
- Randomly generated initialization vector (IV)
- To overcome the security deficiencies of ECB



AES is to replace Triple DES and DES.

- AES specifies three key sizes: 128, 192 and 256 bits.
- In decimal terms, this means that there are approximately:
  - 3.4×10^{38} possible 128-bit keys;
  - 6.2×10^{57} possible 192-bit keys; and
  - 1.1×10^{77} possible 256-bit keys.
- In comparison, DES keys are 56 bits long, which means there are approximately 7.2×10^{16} possible DES keys.
- Thus, there are on the order of 10^{21} times more AES 128-bit keys than DES 56-bit keys.
- NIST says it would take 149 trillion years to crack AES, while DES-3 could be broken in a mere 4.9 billion years.

Evaluation Criteria

Security

- the most important factor in the evaluation
- Encompassed features, e.g.,
  - resistance of the algorithm to crypt analysis
  - soundness of its mathematical basis
  - randomness of the algorithm output
  - relative security as compared to other candidates.

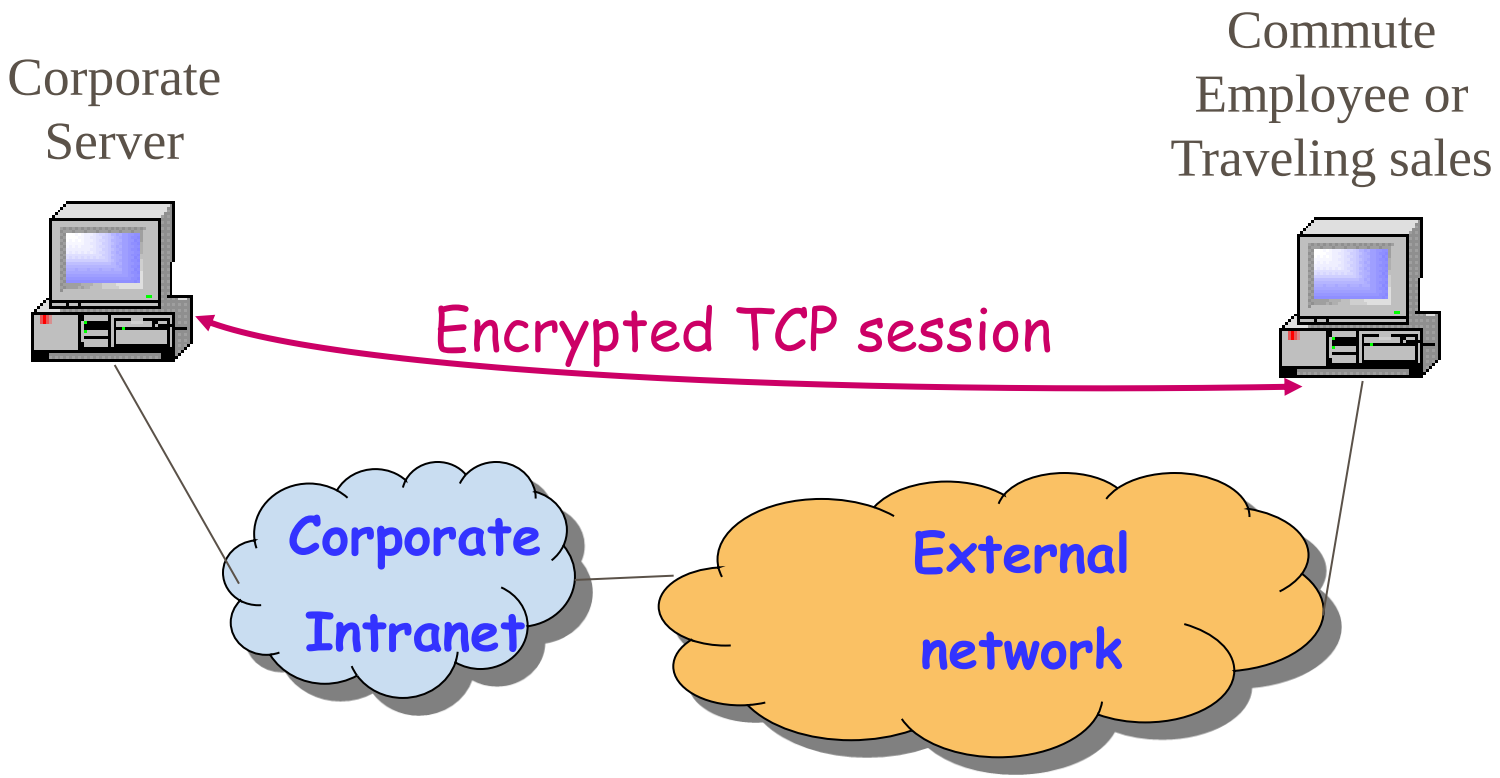
Cost

- Encompassed features
  - licensing requirements
  - computational efficiency (speed) on various platforms
  - memory requirements.

Algorithm and Implementation

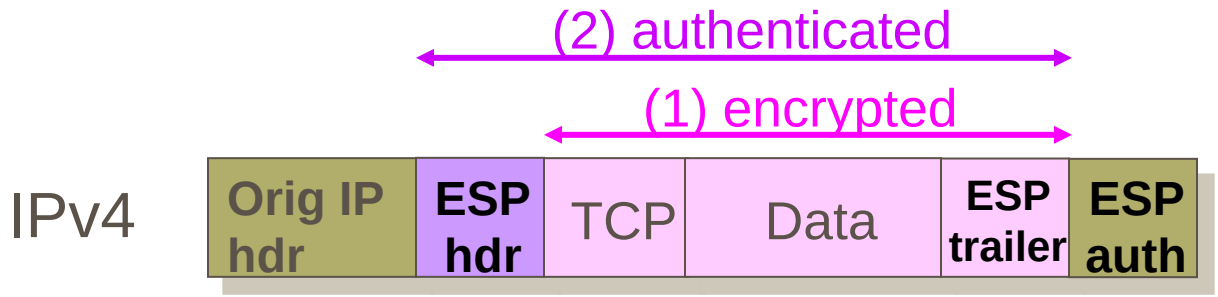
- AES algorithm is available worldwide on a royalty-free basis.
- Hardware implementations

Transport Mode ESP



Transport Mode ESP: IPv4

- Encryption – Transport Layer segment, ESP trailer
  - The *ESP Trailer* is appended to the data, then both are encrypted. but the *ESP Header* is not.
  - *ESP Header* contains two fields, the SPI and Sequence Number.
- Authentication (option) – all of the ciphertext plus the ESP header

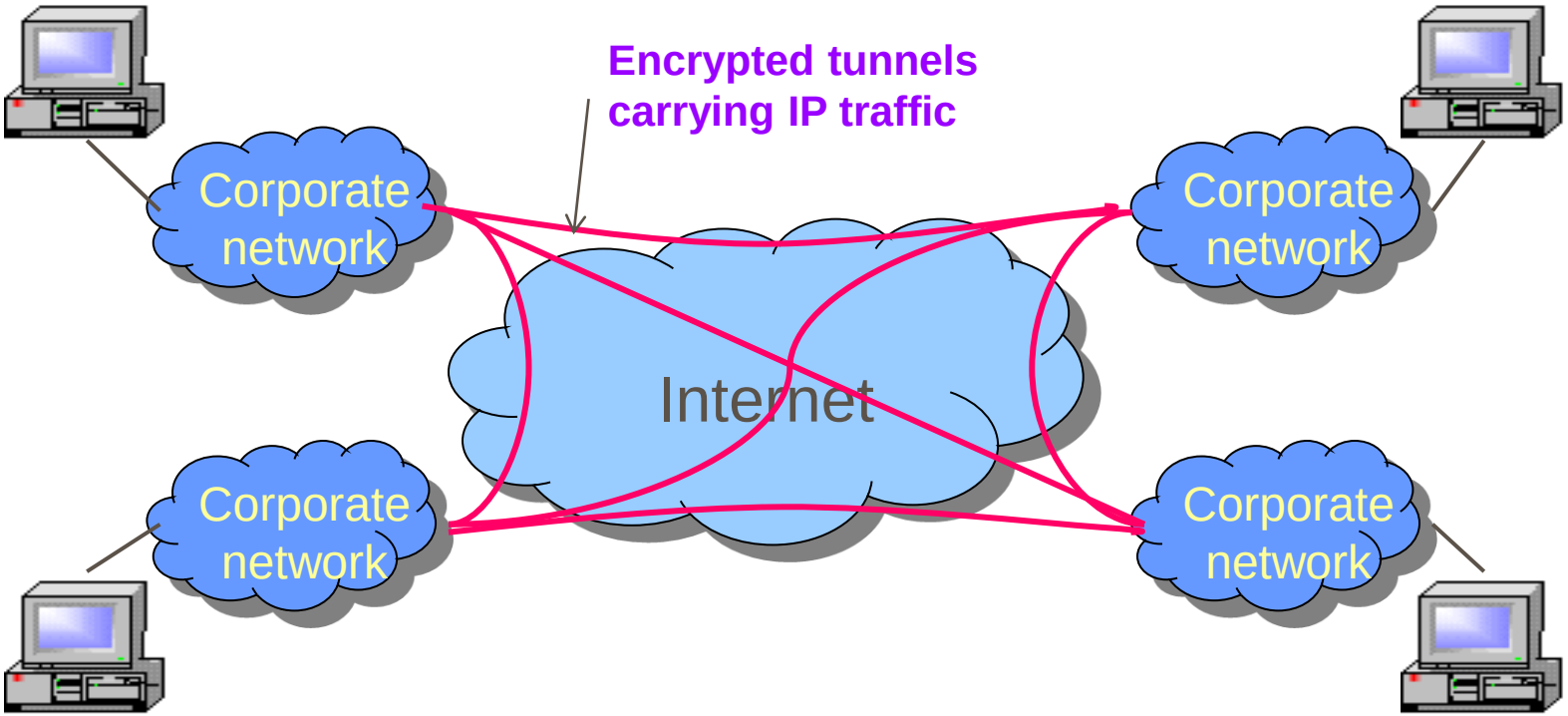


ESP format

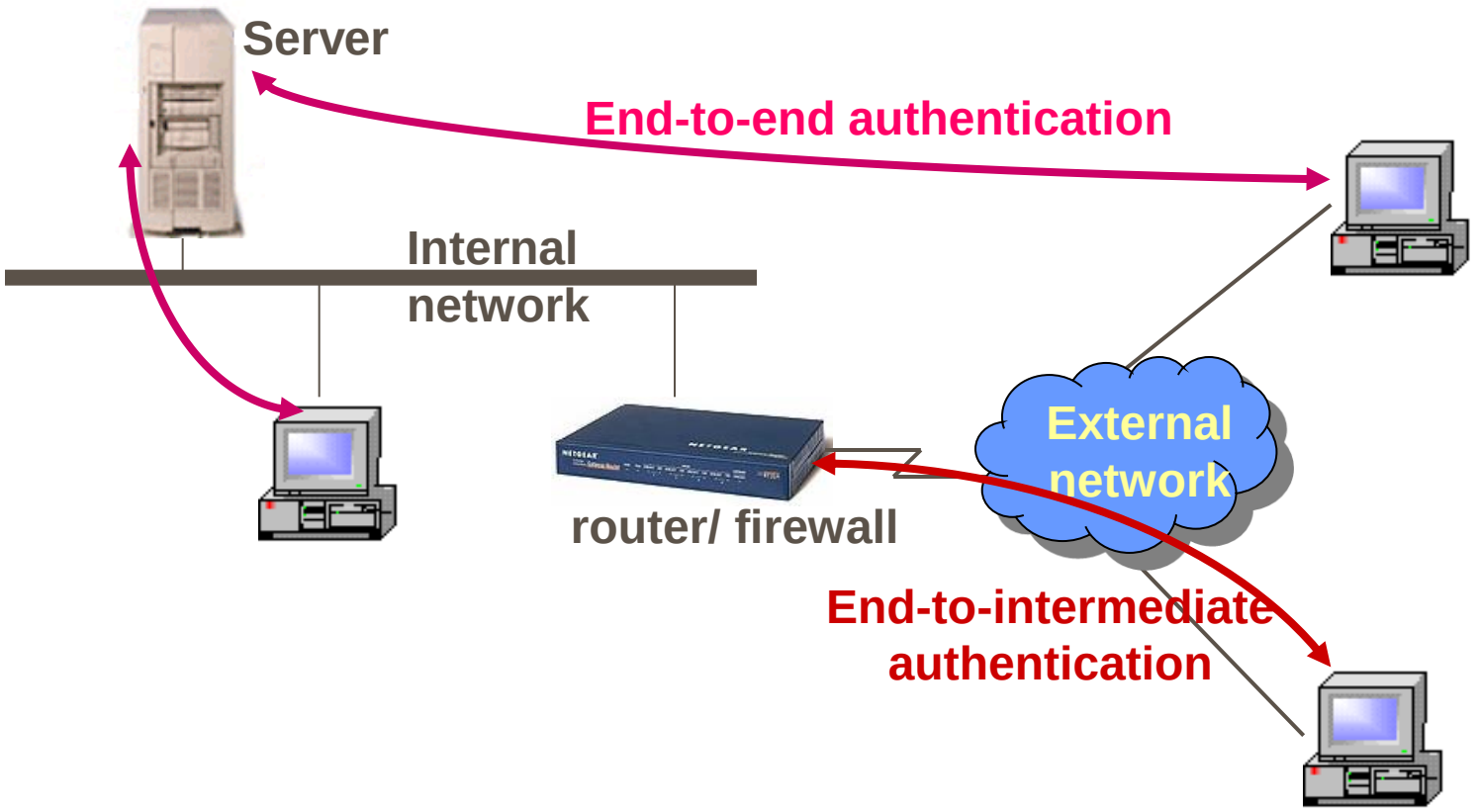
Transport Mode ESP

- Outbound traffic: do encryption then authentication
- Inbound traffic: do authentication check then decryption
  - To cope with denial of service!
  - Parallel processing of decryption and authentication

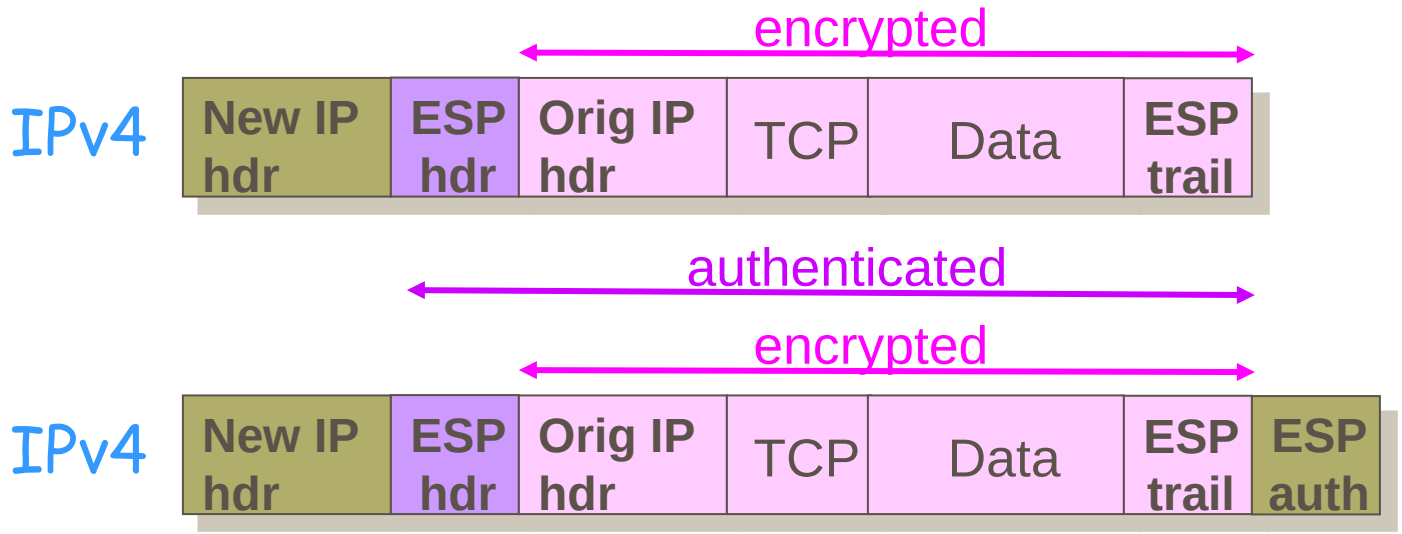
Tunnel Mode ESP – Virtual Private Network (VPN) Application



VPN (Virtual Private Network)



ESP – Tunnel Mode



ESP - Discussion

- In ESP, at least one - authentication or encryption must be performed, e.g.,
  - Encryption only
  - Encryption and authentication
  - Authentication with NULL Encryption

- Compare the authentication in ESP with AH
  - AH : authenticate entire IP packet
  - ESP : only authenticate data payload

Tunnel Mode and Transport Mode Functionality

	Transport Mode SA	Tunnel Mode SA
AH	Authenticates IP payload and selected portions of IP header and IPv6 extension headers.	Authenticates entire inner IP packet (inner header plus IP payload) plus selected portions of outer IP header and outer IPv6 extension headers.
ESP	Encrypts IP payload and any IPv6 extension headers following the ESP header.	Encrypts inner IP packet.
ESP with Authentication	Encrypts IP payload and any IPv6 extension headers following the ESP header. Authenticates IP payload but not IP header	Encrypts inner IP packet. Authenticates inner IP packet.

Combining Security Associations

Motivation

- How about a traffic flow needs IPsec services between hosts and another separate services between security gateways?

-> multiple levels of security

Security Association Bundle

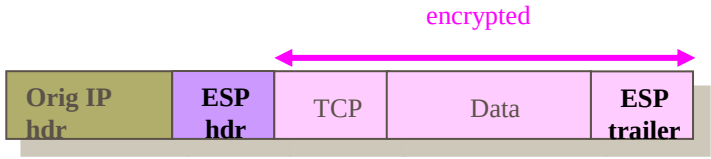
- A sequence of SAs through which traffic must be processed so to provide the desired set of IPsec services .
- The SA bundle may terminate at different endpoints or at the same endpoints.
- SA can be combined in two ways:
  - Transport adjacency
  - Iterated tunneling

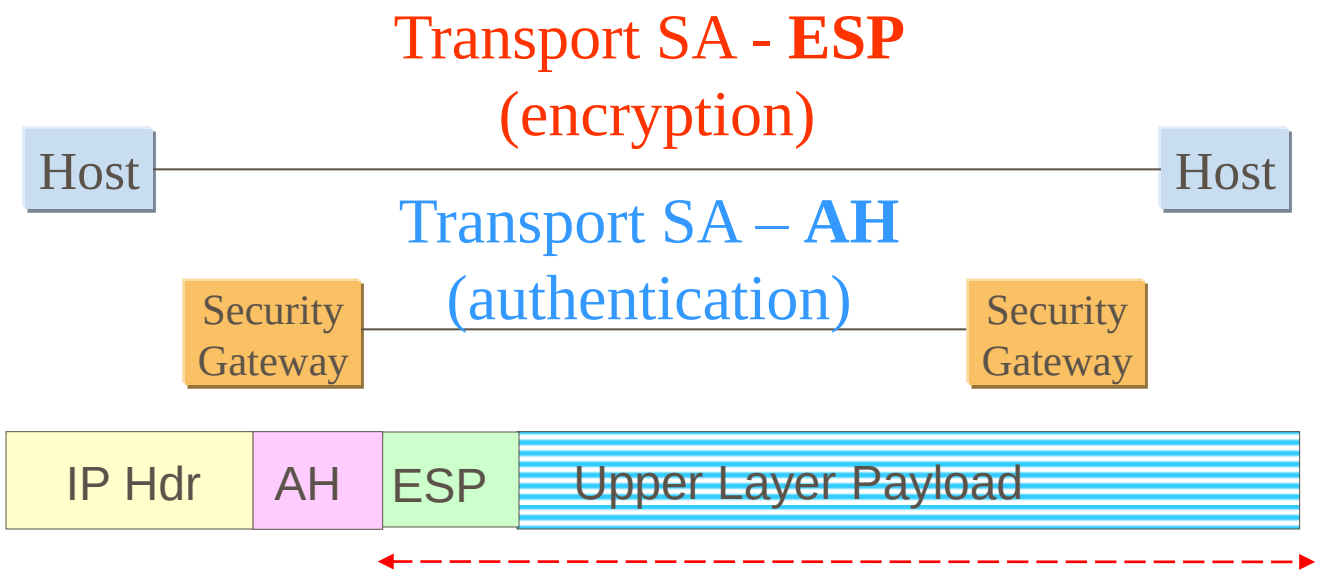
Case #1: Simply ESP with Authentication Option

- Transport Mode ESP
  - Authentication and encryption apply to the **IP payload** to a host
  - IP header is not protected

- Tunnel Model ESP
  - Authentication applied to the **entire IP packet** destined to the outer IP destination address (e.g., a firewall)
  - Authentication check is performed at destination
  - The entire inner IP packet is protected by encryption to the inner destination

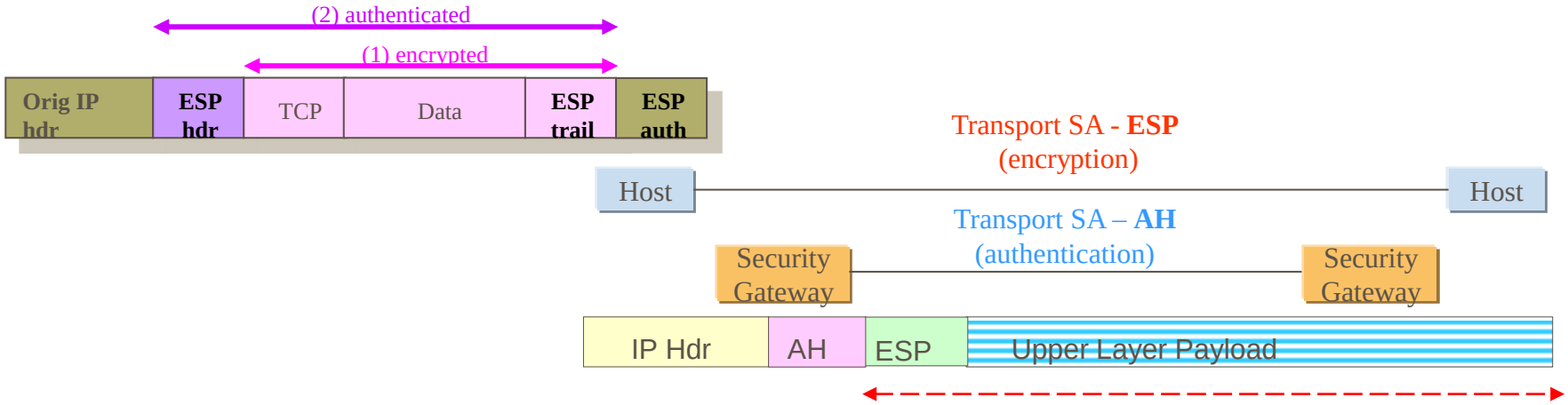
Case #2 : Transport Adjacency (1/2)





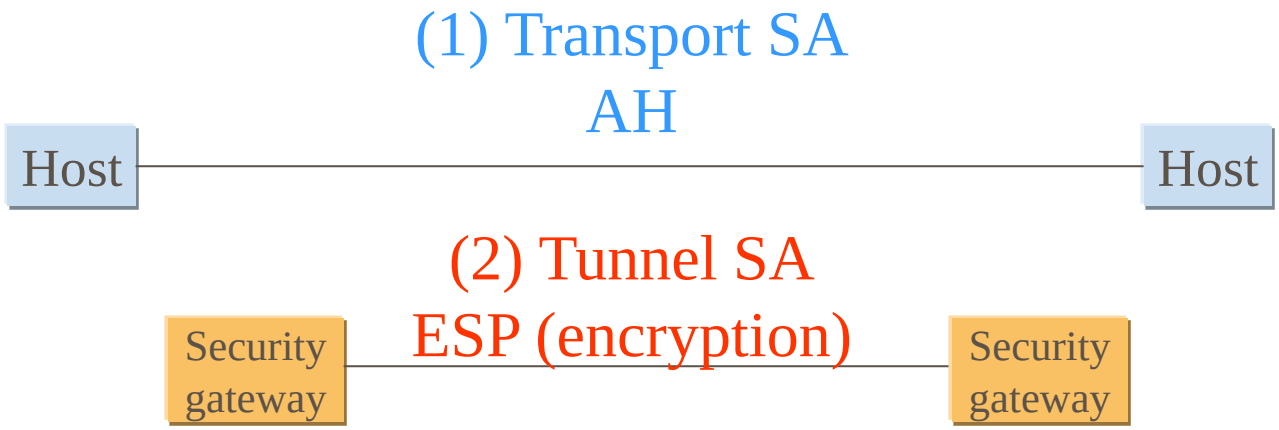
- An inner ESP SA - encryption on IP payload without authentication option
- An outer AH SA- authenticate ESP and the original IP header except for mutable fields
- A transport ESP SA between hosts traveling through a transport AH SA between security gateways

Case #2 : Transport Adjacency (2/2)



- Compare with using one single ESP SA with authentication option - authentication covers more fields, including the source and destination IP addresses.
- The disadvantage – overhead of two SAs

Case #3: Transport - Tunnel Bundle (1/2)



Authentication then Encryption

- Authenticate the entire original IP packet except for mutable fields
- The authenticated inner packet is then encrypted and a new outer IP header (and extension) is added.
- Authentication data is protected by encryption.

Case #3: Transport - Tunnel Bundle (2/2)

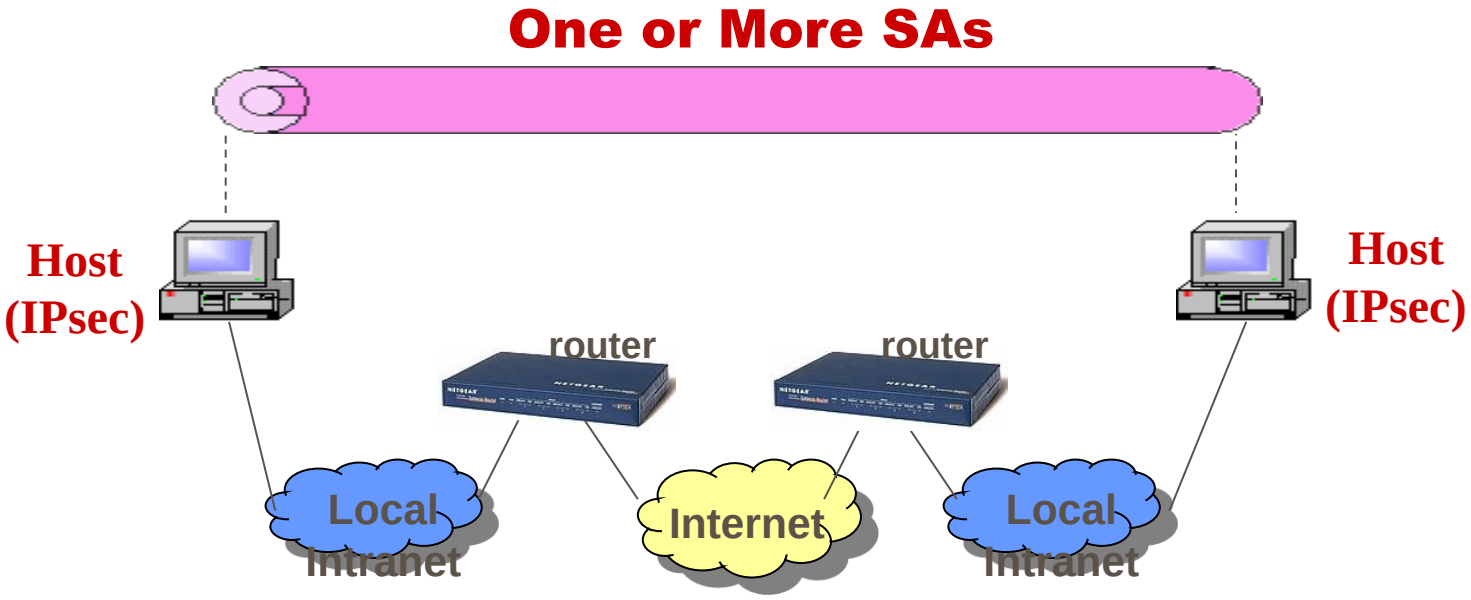
- Advantages
  - Authentication data are protected by encryption
  - Impossible for interception and alteration of the authentication data without detection
  - It may be desirable to store the authentication information with the message at the destination for later reference.

Authentication plus Confidentiality

- Encryption and authentication are combined to provide both confidentiality and authentication between hosts.

- Example Scenarios

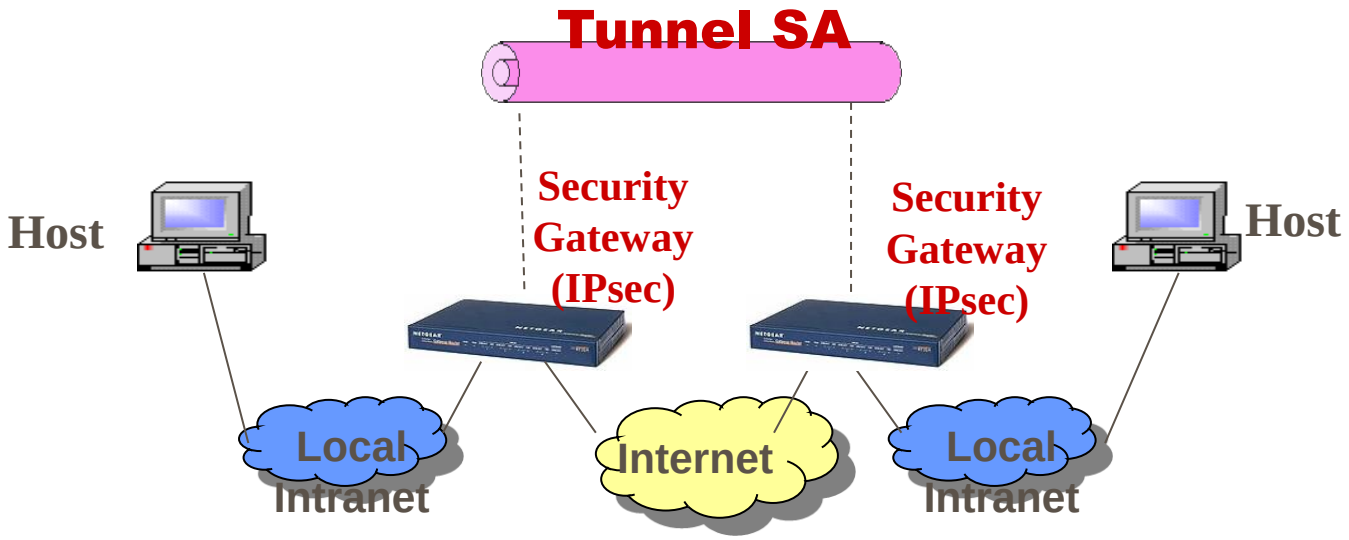
Scenario#1: host-to-host



Possible combinations

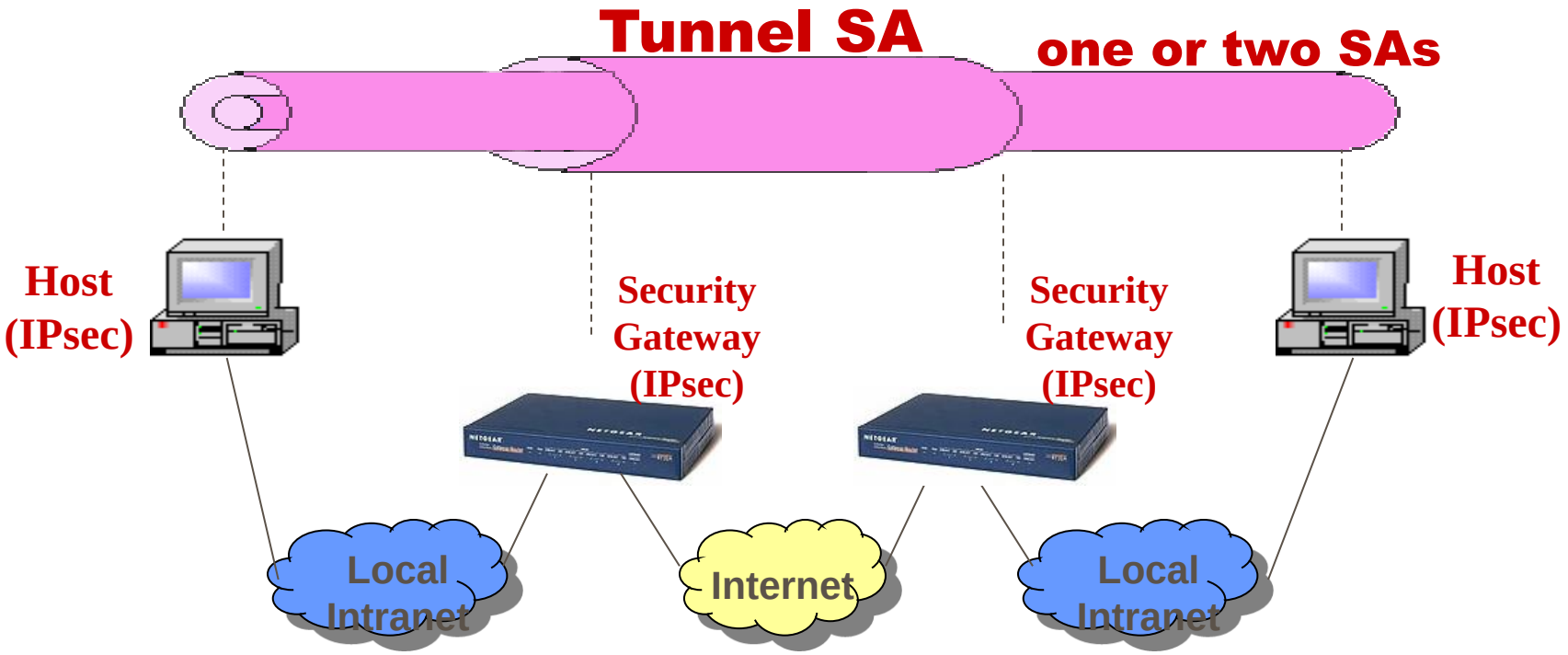
- AH in transport mode
- ESP in transport mode
- An AH SA inside an ESP SA in transport mode
- Any of above inside an AH or ESP in tunnel mode

Scenario #2: gateway-to-gateway

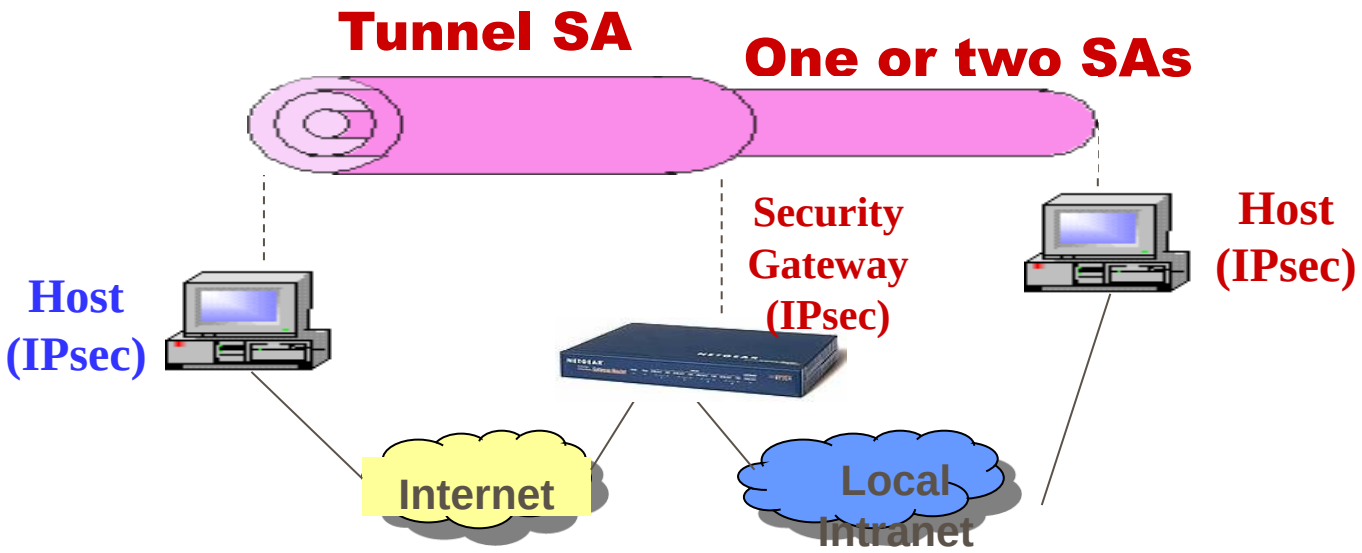


- Security is provided between gateways only.
- AH, ESP or ESP with authentication
- No nested tunnels are necessary because the IPsec services apply to the entire inner packet.

Scenario #3: gateway-to-gateway plus end-to-end security



Scenario #4: Remote Access



- Support for *a remote host* that uses the Internet to reach an organization's *firewall* and then gain access to some *server behind the firewall*.
- Tunnel mode is required between the remote host and the firewall.
- One or two SAs may be used between two hosts.

The end. ☺