Security Engineering
Part III – Network Security

Security Protocols (II): IPsec

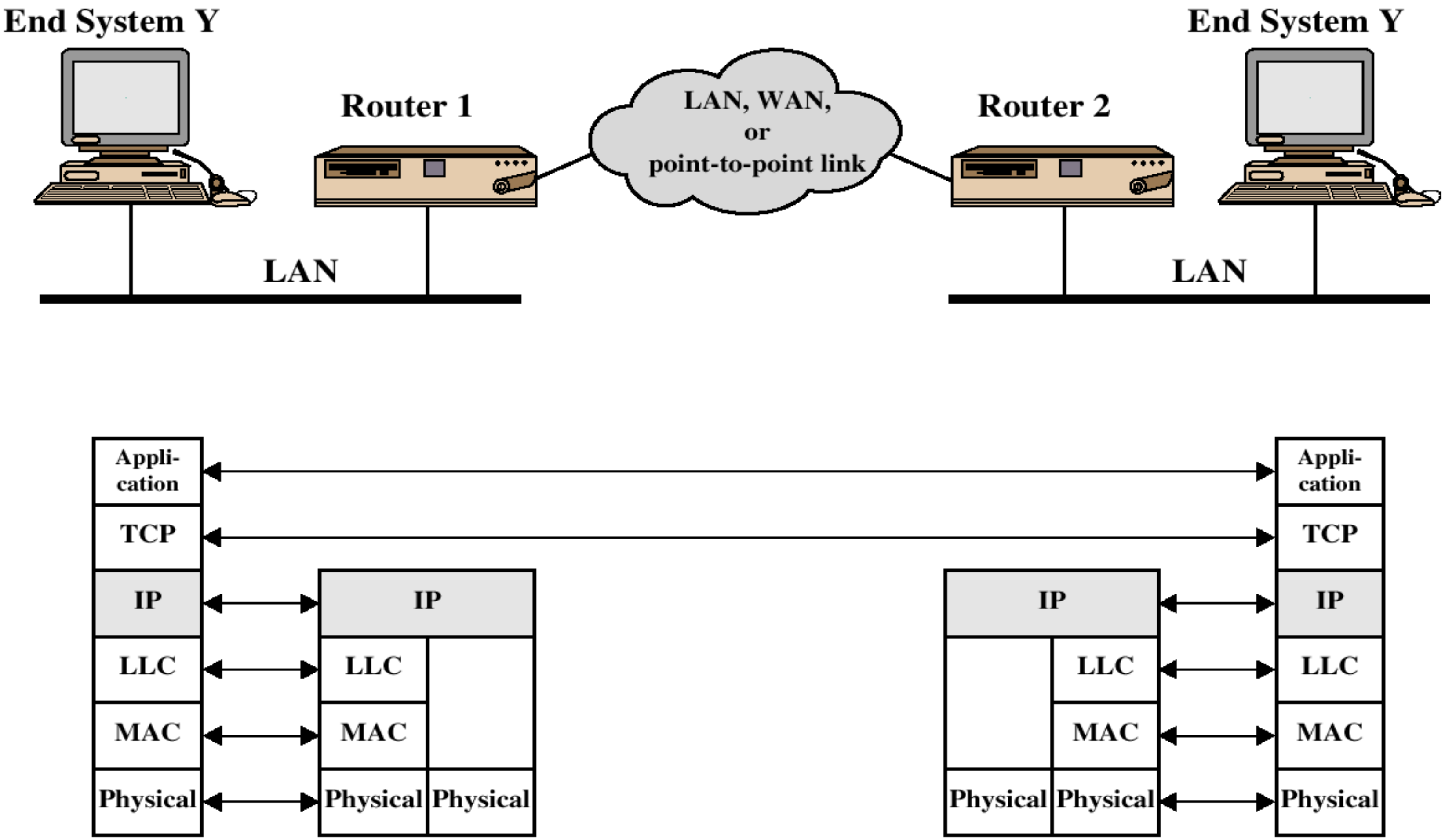
Juan E. Tapiador

jestevez@inf.uc3m.es

Department of Computer Science, UC3M

Security Engineering – 4th year BSc in Computer Science, Fall 2011

Preliminaries



End System Y

Router 1

LAN, WAN, or point-to-point link

Router 2

End System Y

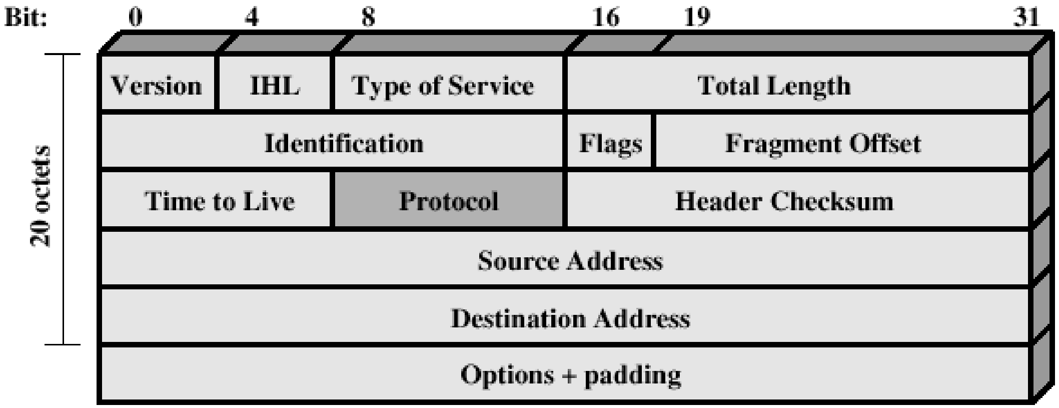
LAN

LAN

End System Y	Router 1		Router 2		End System Y
Appli-cation					Appli-cation
TCP					TCP
IP	IP		IP		IP
LLC	LLC			LLC	LLC
MAC	MAC			MAC	MAC
Physical	Physical	Physical	Physical	Physical	Physical

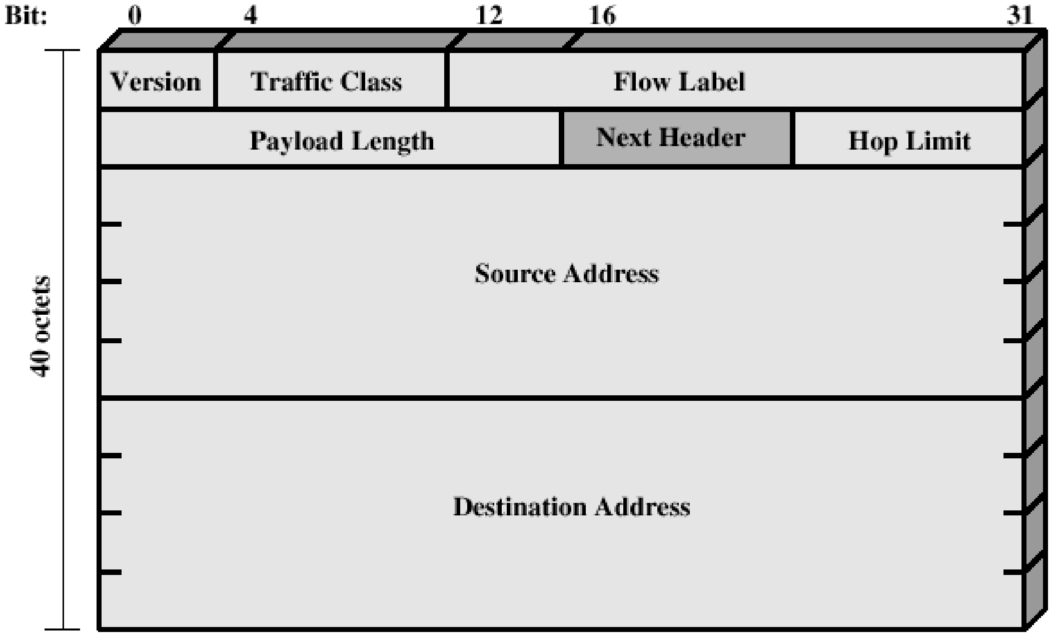
Preliminaries

IPv4 header



Bit:	0	4	8	16	19	31
20 octets	Version	IHL	Type of Service	Total Length		
	Identification			Flags	Fragment Offset	
	Time to Live		Protocol	Header Checksum		
	Source Address					
	Destination Address					
	Options + padding					

IPv6 header



Bit:	0	4	12	16	31
40 octets	Version	Traffic Class	Flow Label		
	Payload Length			Next Header	Hop Limit
	Source Address				
	Destination Address				

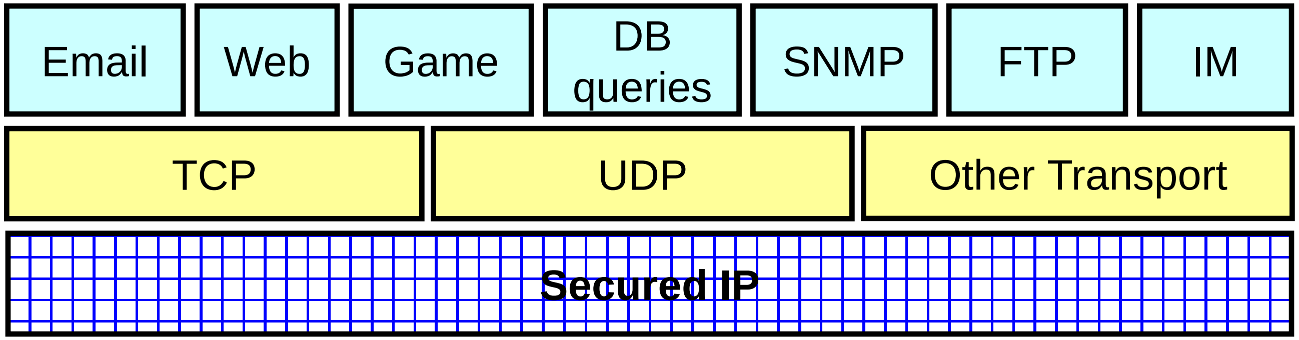
Preliminaries

We have application-specific security protocols

- S/MIME, PGP, SSL/TLS, …

But

- Some problems are common
- Some problems are inherent to the network layer and won't be solved by just securing the app layer

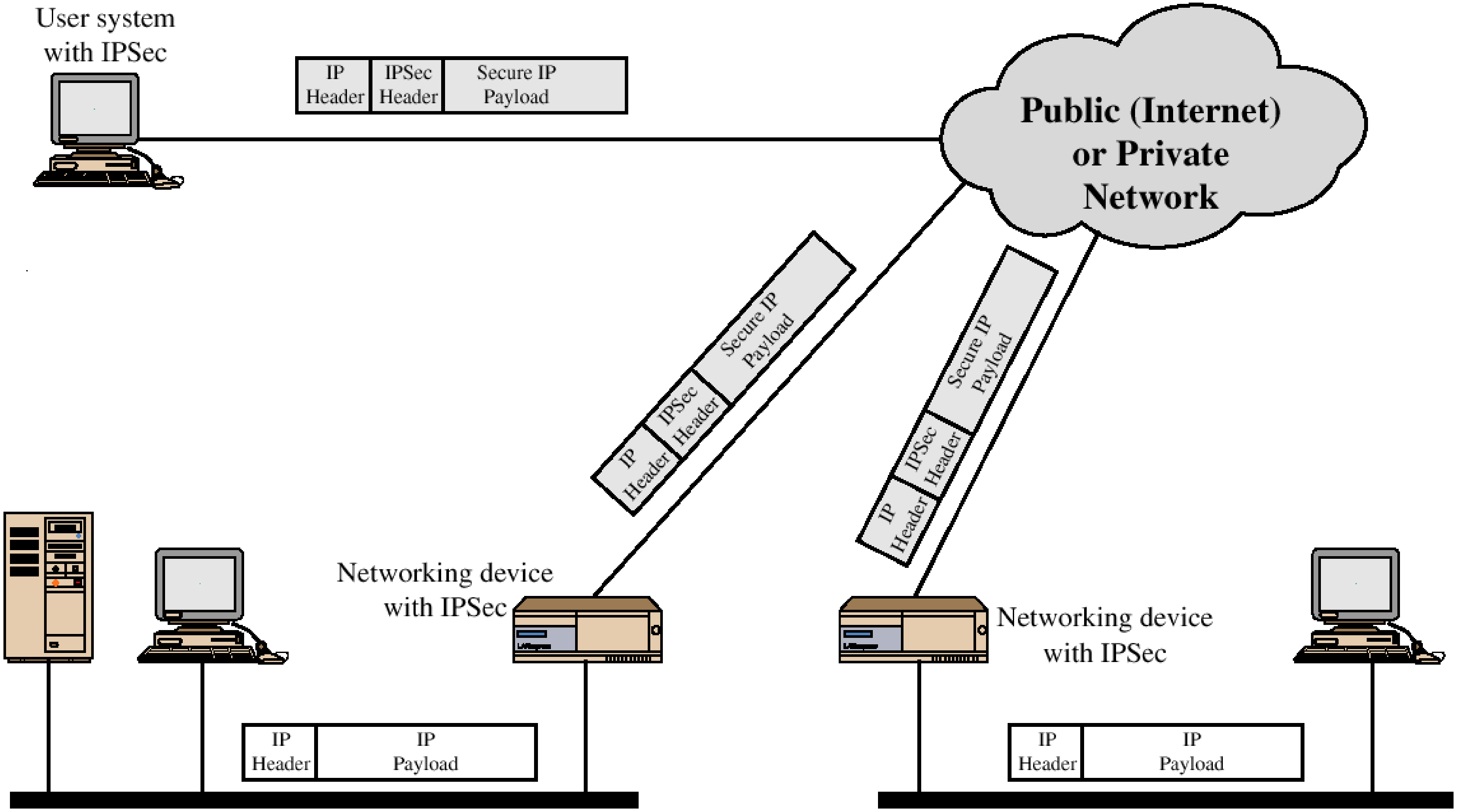


IPsec – A typical usage scenario

- Protocol architecture and algorithms to provide
  - Access control
  - Data authentication
  - Data integrity
  - Confidentiality
  - Detection of replayed packets
  - Key management

- Some applications
  - Remote access using untrusted networks (e.g. Internet)
  - Connectivity to various networks using untrusted networks (VPN, *Virtual Private Networks*)
  - Some security features to routing (e.g., route announcements come from authorised router, no fake messages, etc.)
  - Security enhancements to some applications
    - e-commerce
    - …

IPsec – A typical usage scenario



IPsec essentials

IPsec is optional in IPv4 and mandatory in IPv6

Two main protocols:

- **Authentication Header (AH)**
  - Data authentication + integrity, but no confidentiality
  - MAC-based using a shared secret key

- **Encapsulating Security Payload (ESP)**
  - Encrypts packets. Authentication is optional.
  - Based on various ciphers and encryption modes.

Security associations (SA)

- Bundle of algorithms and paramenters associated with one flow in one direction. Defines provided security services

- In a bidirectional communication, each host must establish an SA with the other party.

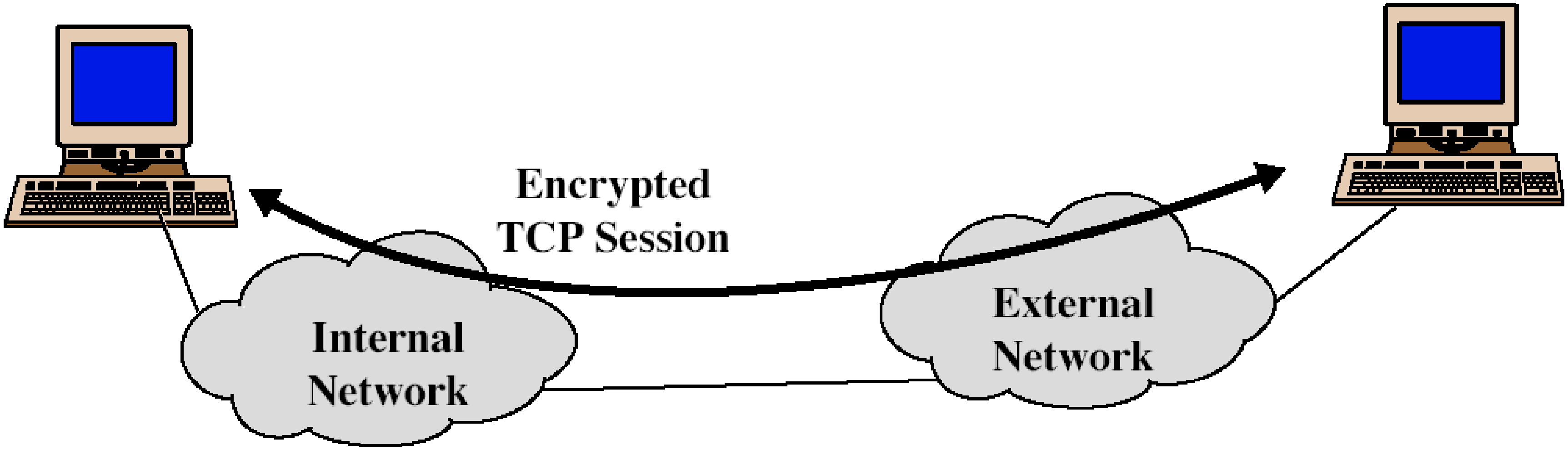
- Indexed in the local SADB by:
  - Security Parameter Index (SPI)
  - IP destination address

- So when a packet arrives, the host knows which SA manages it

- When establishing an SA, one must choose between AH or ESP, but not both simultaneously

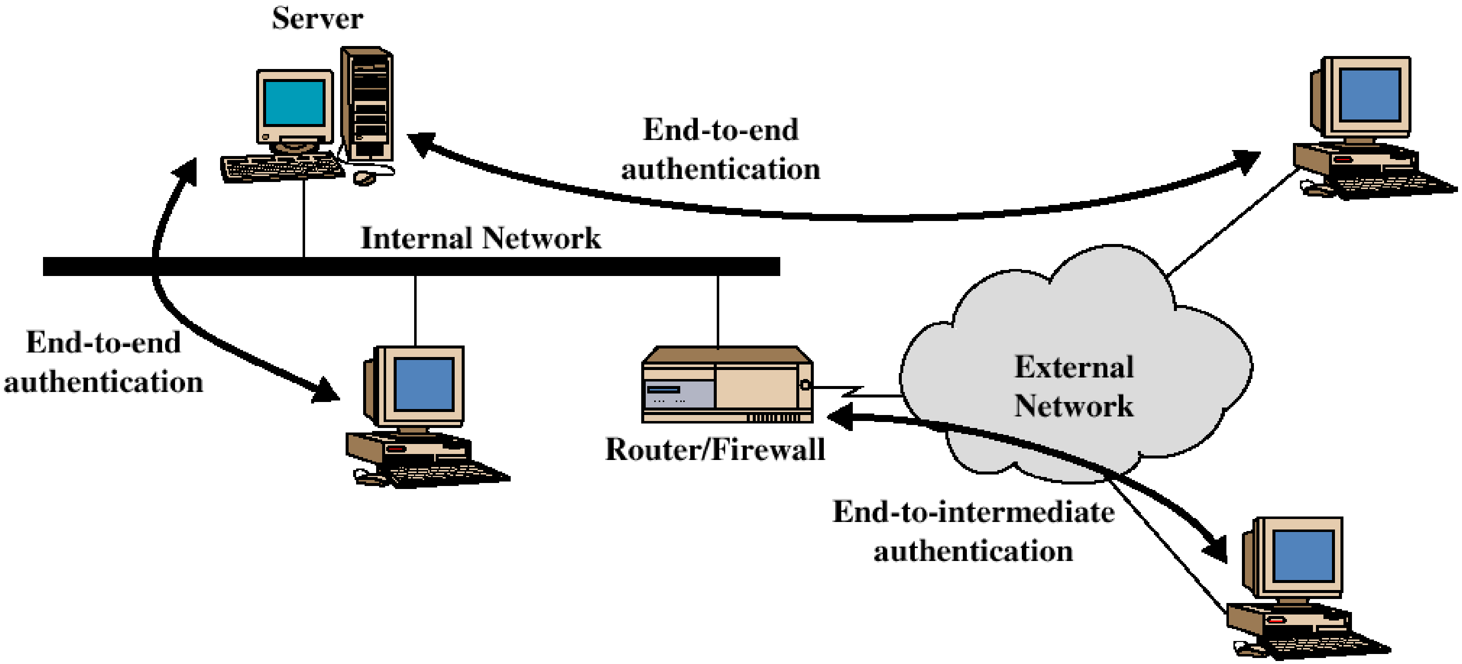
IPsec modes of operation

- **Transport mode**
  - Only payload is protected
  - Used for securing end-to-end communications



IPsec modes of operation

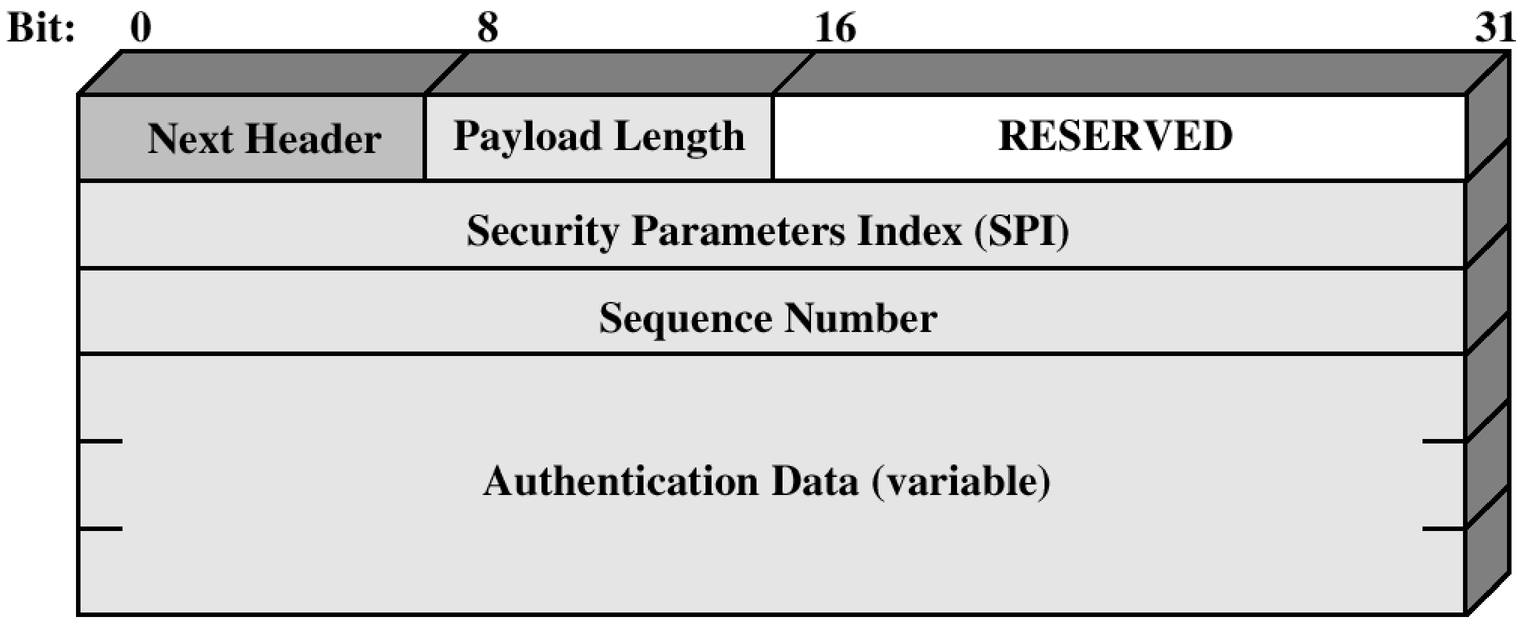
- **Tunnel mode**
  - Protects the entire IP packet, including the IP header
  - Used to connect security gateways
  - Hosts not required to implement IPsec



AH protocol

- Provides
  - Data integrity
  - Data origin authentication
  - Protection against replay attacks (see Seq. No. in AH header)

  of the IP packet



Bit: 0 8 16 31

Next Header | Payload Length | RESERVED

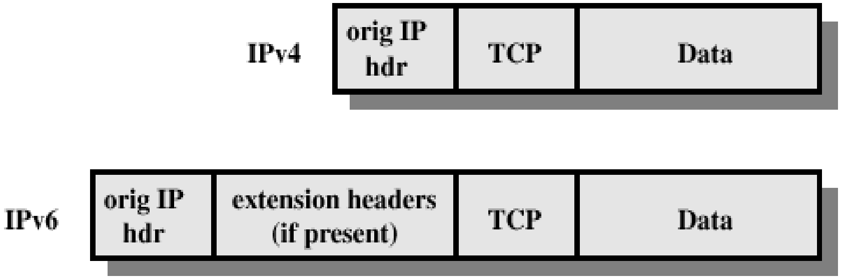
Security Parameters Index (SPI)

Sequence Number

Authentication Data (variable)

AH protocol

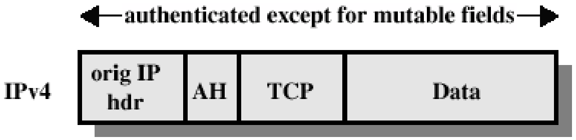
Original IP packet



IPv4: orig IP hdr | TCP | Data

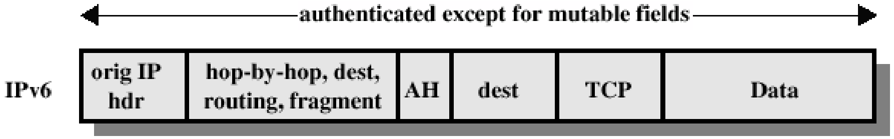
IPv6: orig IP hdr | extension headers (if present) | TCP | Data

AH (transport mode)



authenticated except for mutable fields

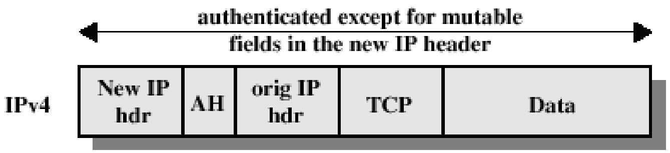
IPv4: orig IP hdr | AH | TCP | Data



authenticated except for mutable fields

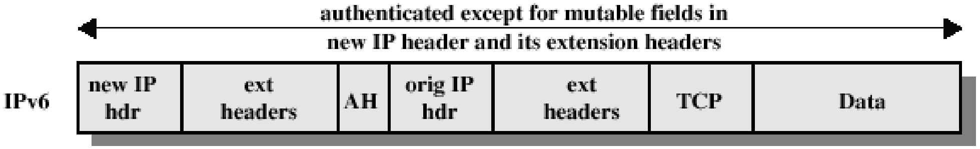
IPv6: orig IP hdr | hop-by-hop, dest, routing, fragment | AH | dest | TCP | Data

AH (tunnel mode)



authenticated except for mutable fields in the new IP header

IPv4: New IP hdr | AH | orig IP hdr | TCP | Data



authenticated except for mutable fields in new IP header and its extension headers

IPv6: new IP hdr | ext headers | AH | orig IP hdr | ext headers | TCP | Data

AH protocol

- Data Auth+Integrity based on an ICV (*Integrity Check Value*)
- In practice, implemented as a MAC:
    - AuthData = HMAC_k(Payload)
- Both hosts must share key *k*
- Why do we want a protocol providing *only* data auth+int.?
    - Useful in environments were encryption is restricted
    - Fast implementation
    - Receiver chooses whether he wishes to check it or not

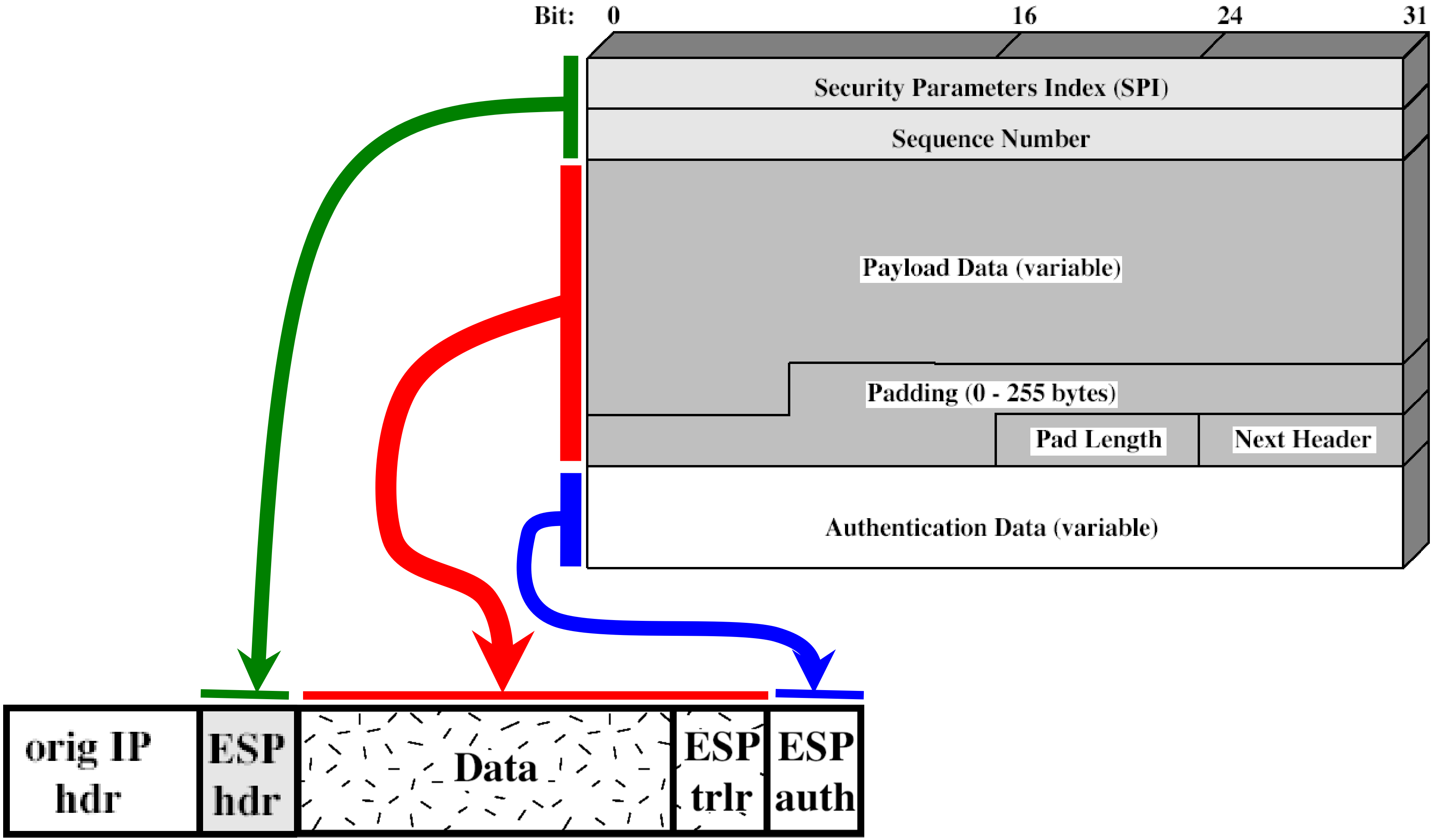
ESP protocol

- Provides confidentiality by encrypting the IP packet
  - Various standard block ciphers supported: DES, 3DES, RC5, IDEA, CAST, …
  - Most common mode: CBC (caution!)
  - Padding to avoid traffic analysis attack and also to fit block size required by the cipher

- It provides AH-like services too:
  - Data origin authentication
  - Data integrity
  - Detection of replay attacks

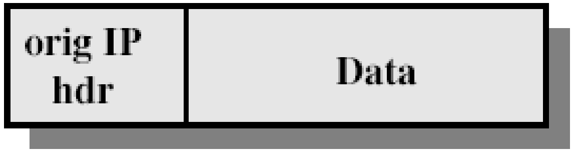
- So ESP admits three configurations:
  - **Authentication-only (WHY?)**
  - **Encryption-only (DON'T!)**
  - **Encryption+Authentication**

ESP protocol



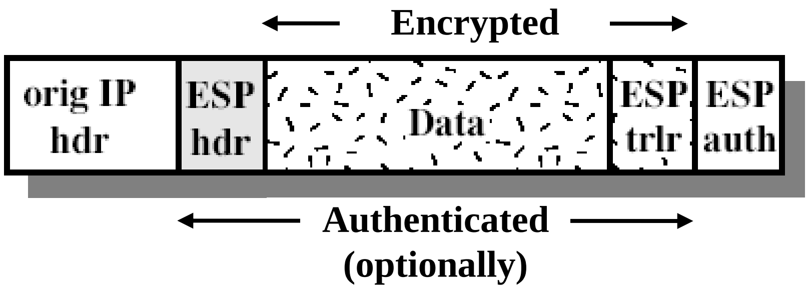
ESP protocol

Original IP packet



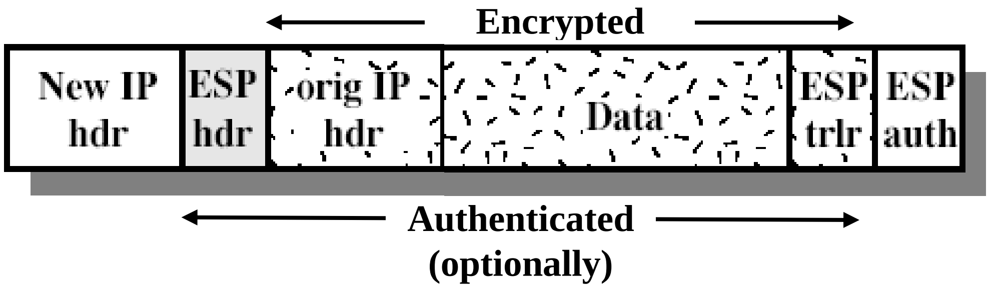
Transport mode:

Only the payload is encrypted and authenticated



Tunnel mode:

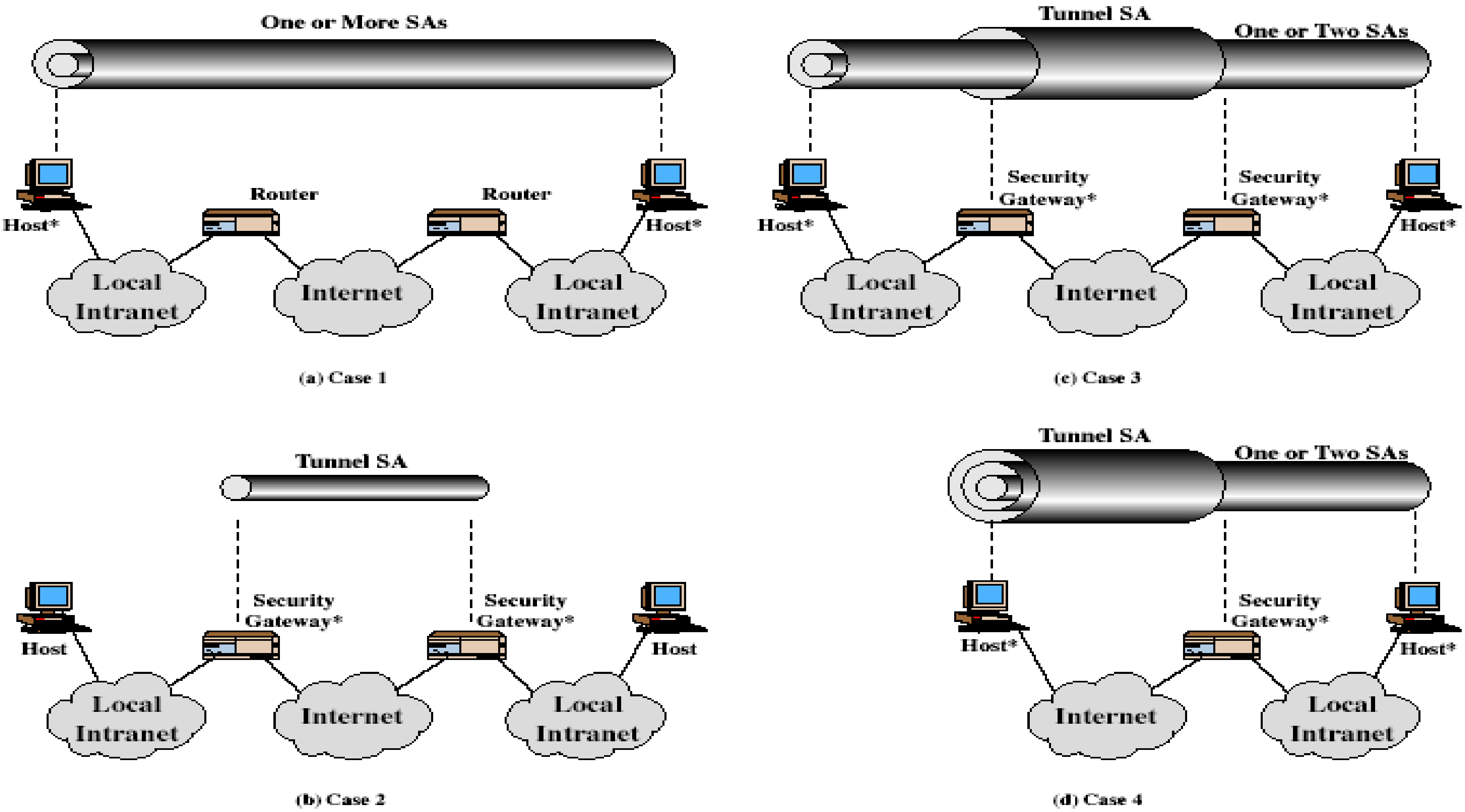
- **The entire packet is encrypted and authenticated**



IPsec protocols and modes

	SA transport mode	SA tunnel mode
AH	**Authenticates**: payload + parts of IP header + IPv6 extensions	**Authenticates**: internal IP packet + parts of external IP header
ESP (Enc. Only)	**Encrypts**: payload + any IPv6 extension	**Encrypts**: internal IP packet
ESP with Auth	**Encrypts**: payload + any IPv6 extension. **Authenticates**: payload only	**Encrypts**: internal IP packet **Authenticates**: internal IP packet

SA combinations



(a) Case 1

(c) Case 3

(b) Case 2

(d) Case 4

IPsec: key management

- AH and ESP require shared keys (typically 2 pairs per comm.)
- **ISAKMP** (*Internet Security Association and Key Management Protocol*)
  - Framework for authentication (entity) and key exchange
  - Authenticated keying material provided:
    - Manually with pre-shared keys
    - Internet Key Exchange (IKE, IKEv2)
    - Kerberized Internet Negotiation of Keys (KINK)
    - IPSECKEY DNS records