IP Security

IP Security Overview

- IPSec (Internet Protocol Security) is a suite of standards for providing a rich set of security services at the network layer.
- Transparent to applications (below transport layer – TCP, UDP)
- IPSec Main Features:
  - Source authentication
  - Message authentication and integrity check
  - Data confidentiality
  - Access control

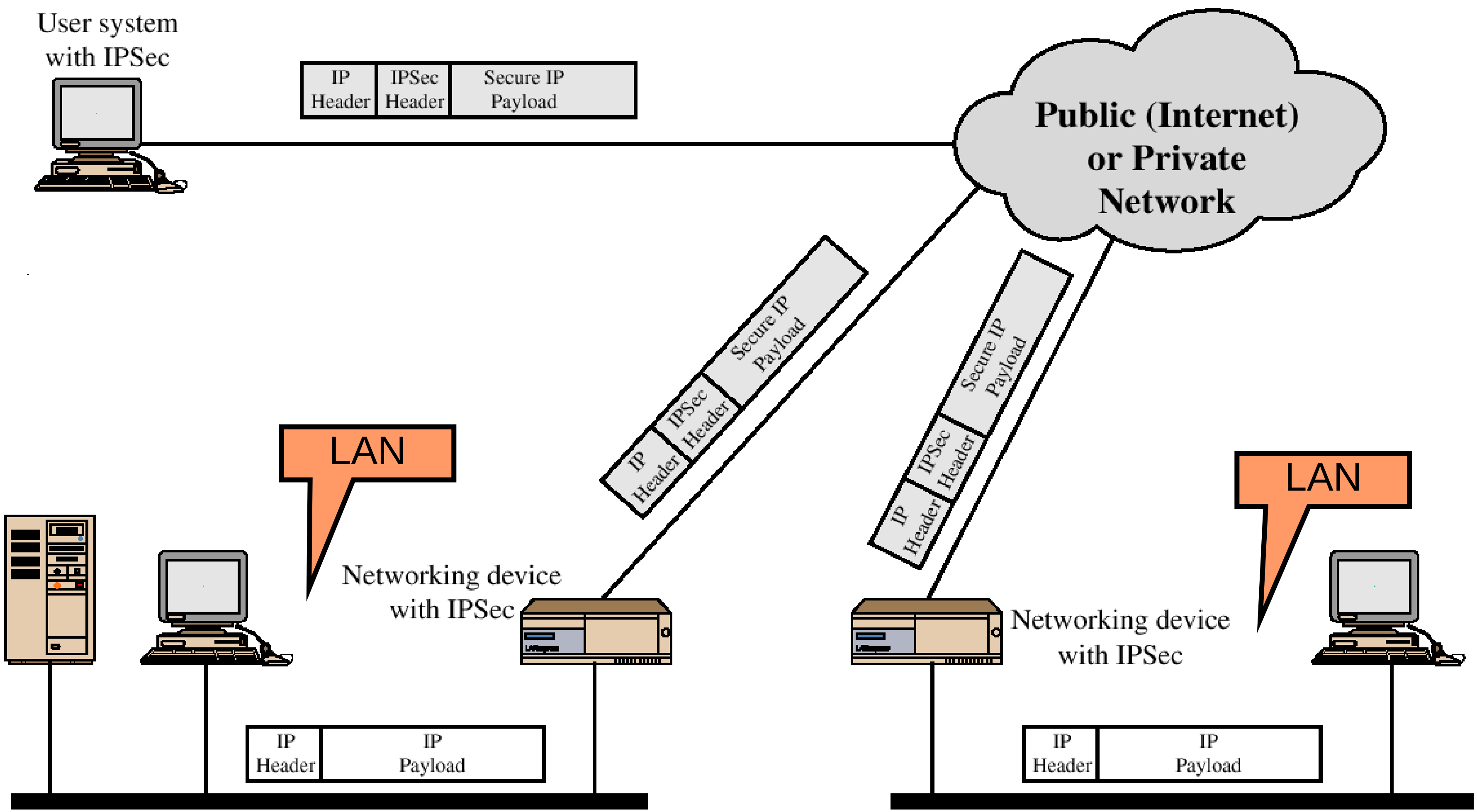
IP Security Overview

Applications of IPSec:

- **Secure branch office connectivity over the Internet**:
  A company can build a secure virtual private network over the internet to reduce cost.
- **Secure remote access over the Internet**:
  Using IPSec an remote user can make a local call to an ISP and gain secure access to a company network.

IPSec can provide security for varied applications since it encrypts and/or authenticates *all traffic* at the IP level.

IPSec Overview: A Typical Scenario



IPSec Overview: A Typical Scenario

- A company maintains LANs at dispersed locations, where nonsecure traffic is conducted in each LAN.
- IPSec protocols operate in networking devices (routers and firewalls) to secure offsite traffic.
- These devices encrypt & compress all outbound traffic, and decrypt & decompress all inbound traffic.
- These security operations are transparent to workstations and servers on each LAN.
- Security service is also possible for individual users who dial into the public network.

IPSec Security Protocols

- In IPSec, there are two major components:
  - security protocols
    - AH (Authentication Header) protocols
    - ESP (Encapsulating Security Payload) protocols
  - modes
    - transport mode
    - tunnel mode

IPSec Security Protocols

	AH	ESP (encr.)	ESP (encr.+auth.)
Access control	√	√	√
Connectionless integrity	√		√
Data origin auth.	√		√
Anti-replay	√	√	√
Confidentiality		√	√
Limited traffic flow conf.		√	√

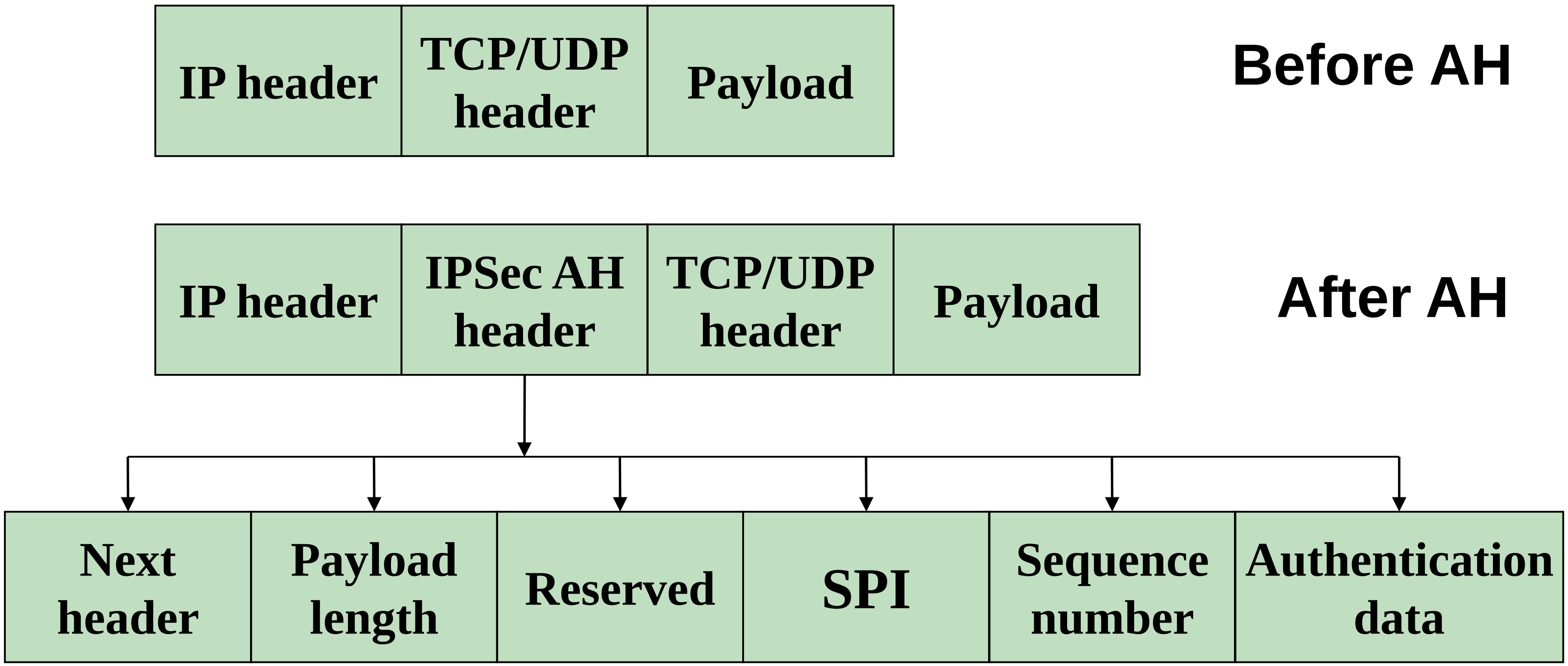
IPSec Protocols

- AH and ESP protocols are largely independent of the cryptographic algorithms used to secure the IP traffic.
- These protocols can use any underlying cryptographic algorithm to implement the authentication and confidentiality services, such as AES for encrypting the outbound traffic, HMAC-SHA256 to create hashed MAC.

IPSec Modes

- The AH & ESP protocols operate in one of two possible modes: *transport mode* or *tunnel mode*.
- In tunnel mode, an IP datagram contains *two* IP headers:
  - an outer IP header: specifies the IPSec processing destination
  - an inner IP header: contains the source and the ultimate destination of the packet.
- In transport mode, IP datagram contains only *one* IP header, which specifies the apparent source address and the ultimate destination address of the packet.

AH in Transport Mode IPv4



Before AH

After AH

SPI: Security parameters index

Authentication is across all immutable fields

AH Header Fields

AH Header Field	*Description*
Next header	Identifies the type of the next payload after the Authentication Header
Payload length	Specifies the length of the Authentication Header in 32-bit words
Reserved	Reserved for future use
Security parameters index (SPI)	In conjunction with the destination IP address and the IPsec protocol (AH or ESP), uniquely identifies the security association (explained later) for a packet
Sequence number	Contains a monotonically increasing counter value for protection against replay attacks
Authentication data	Contains the integrity check value (ICV) for the packet for data origin authentication and connectionless integrity

AH in Tunnel mode IPv4

IP header	TCP/UDP header	Payload

Before AH

Transit IP header	IPSec AH header	Original IP header	TCP/UDP header	Payload

After AH

Next header	Payload length	Reserved	SPI	Sequence number	Authentication data

Authentication is across all immutable fields

Integrity Check Value (ICV)

- AH protocol excludes any unpredictable mutable fields when calculating ICV.
- AH protocol includes only the *immutable fields* and *mutable but predictable* fields when calculating an ICV for a packet.

Mutable vs Immutable Header Fields (IP V4)

Field	Immutable	Mutable
Version	✓	
Internet header length	✓	
Total length	✓	
Identification	✓	
Protocol	✓	
Source address	✓	
Destination address	✓	
Type of service (TOS)		✓
Flags		✓
Time to Live(TTL)		✓
Header checksum		✓

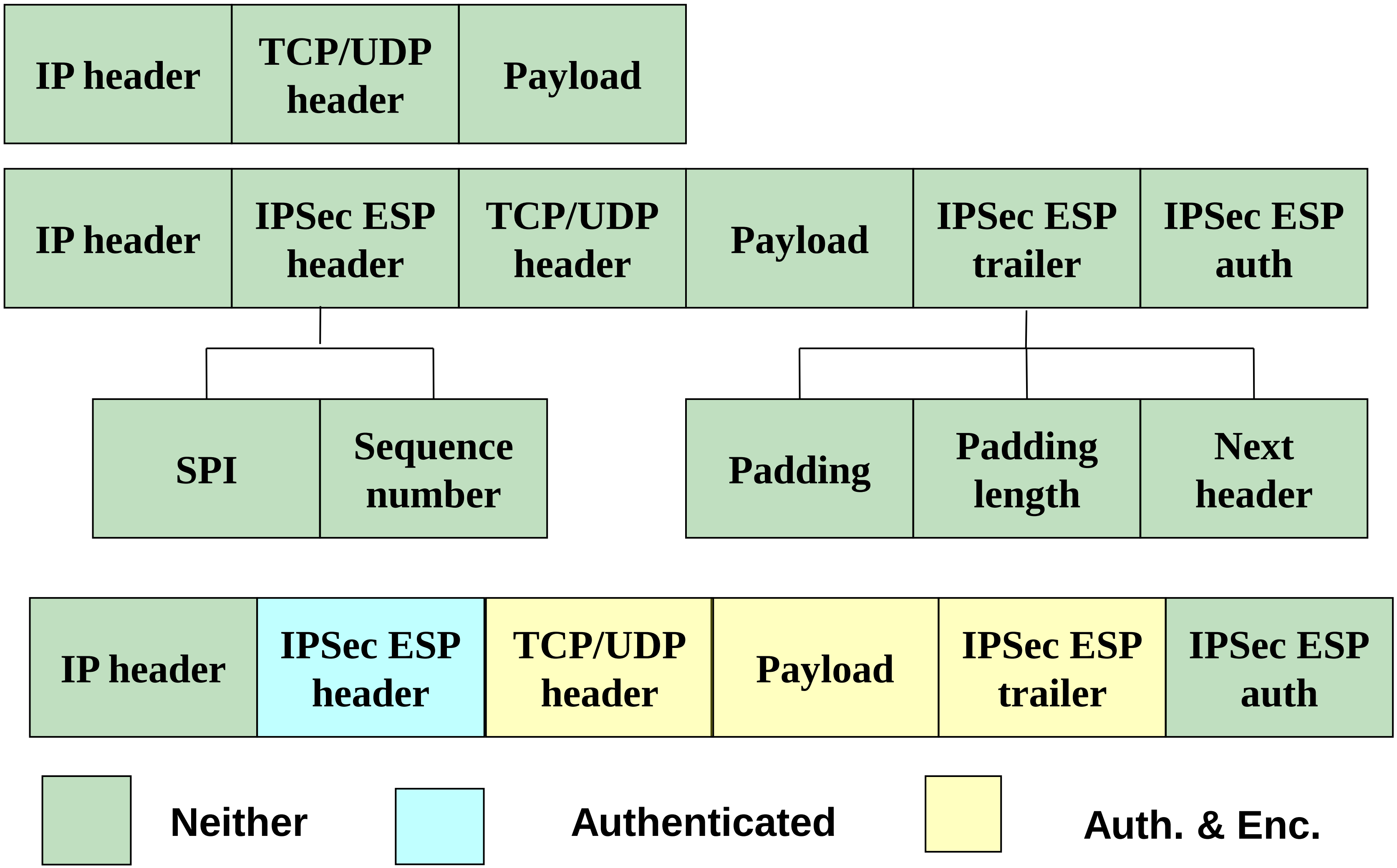
AH Protocol - ICV

- AH security protocol can use keyed message authentication codes (MACs) based on symmetric encryption algorithms or hashed MACs based on hash functions for calculations of ICV authentication data.
- Standards-compliant AH implementations must support HMAC.

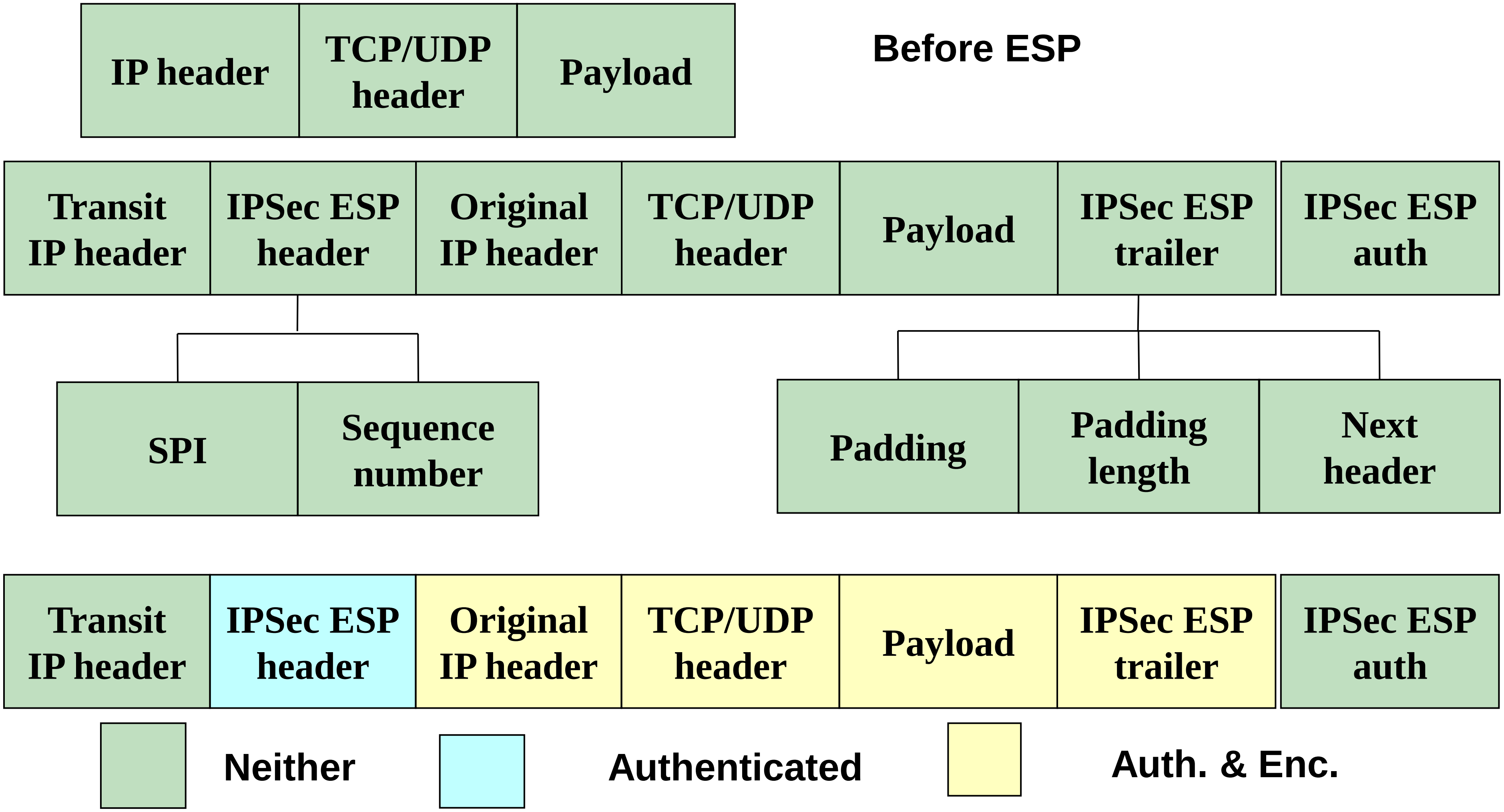
Encapsulating Security Payload (ESP) Protocol

- ESP security protocol selectively affords the confidentiality service or authentication service to IP traffic.
- In *transport mode*, ESP secures upper-layer protocols.
- In *tunnel mode*, ESP extends protection to the inner IP header.

ESP in Transport Mode IPv4



ESP in Tunnel Mode IPv4



Security Associations (SA)

- SA is a *simplex (unidirectional)*, logical connection that provides security services to a traffic stream between two IP nodes.
- An SA serves as a contract between two or more entities and completely specifies how they use security services to communicate securely.

Security Association

- An SA specifies a number of parameters, such as the AH authentication algorithm, the ESP encryption algorithm, the ESP authentication algorithm, keys, IVs, IPSec protocol transport or tunnel mode and *lifetime*.

SA Lifetime

- The lifetime of an SA is the interval after which the SA is no longer valid and must be terminated.
- If the key-management scheme uses PKI certificate for the identification of a peer node, the lifetime of the established SA must not exceed the validity period of the certificate.

IPSec Internet Key Exchange (IKE) Protocols

- The IKE protocol operates in two phases:
  - IKE establishes an SA to secure its own traffic.
  - It establishes another SA to provide security to application data.

IKE Phase 1

- There are two types of phase-1 exchanges, called *modes*:
  - Aggressive mode:
    - mutual authentication and session key establishment in three messages.
  - Main mode:
    - uses six messages and has additional functionality such as the ability to hide endpoint identifiers from eavesdroppers.

IKE Phase 1 – Main Mode

1. Alice → Bob: crypto suites I support
2. Bob → Alice: crypto suite I choose
3. Alice → Bob: g^a mod p
4. Bob → Alice: g^b mod p
5. Alice → Bob: g^{ab} mod p{Alice, signature on previous messages}
6. Bob → Alice: g^{ab} mod p{Bob, signature on previous messages}

IKE Main Mode using Digital Signature

Initiator (Alice) | **Responder (Bob)**

negotiation:
- **CKY-A, <list>** →
- ← **CKY-A, CKY-B, <algo>**

key exchange:
- **CKY-A, CKY-B, g^x, N_A** →
- ← **CKY-A, CKY-B, g^y, N_B**

authentication:
- **CKY-A, CKY-B, $\{A, Sig_A(M_{AB})\}_{Ke}$** →
- ← **CKY-A, CKY-B, $\{B, Sig_B(M_{BA})\}_{Ke}$**

- CKY: cookie
- KM: derived from (N_A | N_B, g^{xy})
- Ke: derived from KM
- M_{AB}: $MAC_{KM}(g^x \mid g^y \mid \text{CKY-A} \mid \text{CKY-B} \mid \text{<list>} \mid A)$
- M_{BA}: $MAC_{KM}(g^y \mid g^x \mid \text{CKY-B} \mid \text{CKY-A} \mid \text{<list>} \mid B)$

Features of IKE key establishment

- Cookies are used to avoid denial of service attacks which exploit the computational expense of calculating keys.
  - The idea is to force legitimate parties to carry out a cookie exchange before significant computations are carried out.
- Parameters for the Diffie-Hellman key exchange can be negotiated.
  - Including the group, with the option of some Elliptic curve based DH exchanges possible.
  - Public keys for DH can be exchanged, with authenticity to avoid man-in-the-middle attacks.
- Nonces are used to protect against replay attacks.

IKE Phase 1 – Aggressive Mode

1. Alice → Bob: Alice, g^a mod p, crypto proposal
2. Bob → Alice: g^b mod p, crypto choice, proof I'm Bob
3. Alice → Bob: proof I'm Alice

IKE Aggressive Mode using Digital Signature

Initiator (Alice) **Responder (Bob)**

CKY-A, <list>, g^x, N_A, A →

← **CKY-A, CKY-B, <algo>, g^y, N_B, B, $Sig_B(M_{BA})$**

CKY-A, CKY-B, $Sig_A(M_{AB})$ →

- Only three message flows
- No identity protection

IKE Phase 2

- Once an IKE SA is setup between Alice and Bob, either Alice or Bob can initiate an IPSec SA through the phase 2 “quick mode” exchange.
- The quick mode exchange negotiates IPSec ESP/AH SAs, and optionally does a Diffie-Hellman exchange.
  - All the information exchanged are protected by the IKE SA
  - Optional DH exchange – to provide forward secrecy

IKE V2

- Simplification, increased efficiency & security
- Initial Exchange
  - 4 messages
  - Establish IKE SA
  - Similar as IKEv1 Phase1
    - IKEv1 has various options for key exchange mechanism
    - IKEv2 has only 1 option
- Phase 2: CREATE_CHILD_SA Exchange
  - 2 messages
  - Establish IPSec SA

A		B
	Stage 1: IKE_INIT	
$N_A \in_R [0,L], r_A \in_R \mathbb{Z}_q$		
$t_A = g^{r_A}$	$\xrightarrow{\texttt{list}, t_A, N_A}$	$N_B \in_R [0,L], r_B \in_R \mathbb{Z}_q$
$\mathbf{Z} = t_B^{r_A}$	$\xleftarrow{\texttt{algo}, t_B, N_B}$	$t_B = g^{r_B}$
		$\mathbf{Z} = t_A^{r_B}$
	Stage 2: IKE_AUTH	
	Derive keys K_M, K_E from $\mathbf{Z}, N_A, N_B$	
	$\xrightarrow{\{ID_A, \mathsf{Sig}_A(\texttt{list}, t_A, N_A, N_B, \mathsf{MAC}_{K_M}(ID_A))\}_{K_E}}$	
		Decrypt then verify MAC and signature
Decrypt then verify MAC and signature	$\xleftarrow{\{ID_B, \mathsf{Sig}_B(\texttt{algo}, t_B, N_B, \mathsf{MAC}_{K_M}(ID_B))\}_{K_E}}$	

Protocol 5.33: IKEv2 protocol, initial exchanges

Boyd et al., *Protocols for Authentication and Key Establishment.* pp. 223

IKE V2 Initial Exchange

- Cookies are allowed, but not used in the basic protocol
  - added only on demand when a denial-of-service attack is suspected
- Diffie-Hellman starts from the first two messages
  - A must make an assumption that her preferred Diffie-Hellman group will be accepted by B
  - If not, need to restart the protocol