# Cryptography and Network Security Chapter 16

Fourth Edition

by William Stallings

# Chapter 16 – IP Security

*If a secret piece of news is divulged by a spy before the time is ripe, he must be put to death, together with the man to whom the secret was told.*

**—*The Art of War*, Sun Tzu**

# IP Security

- have a range of application specific security mechanisms
  - eg. S/MIME, PGP, Kerberos, SSL/HTTPS
- however there are security concerns that cut across protocol layers
- would like security implemented by the network for all applications

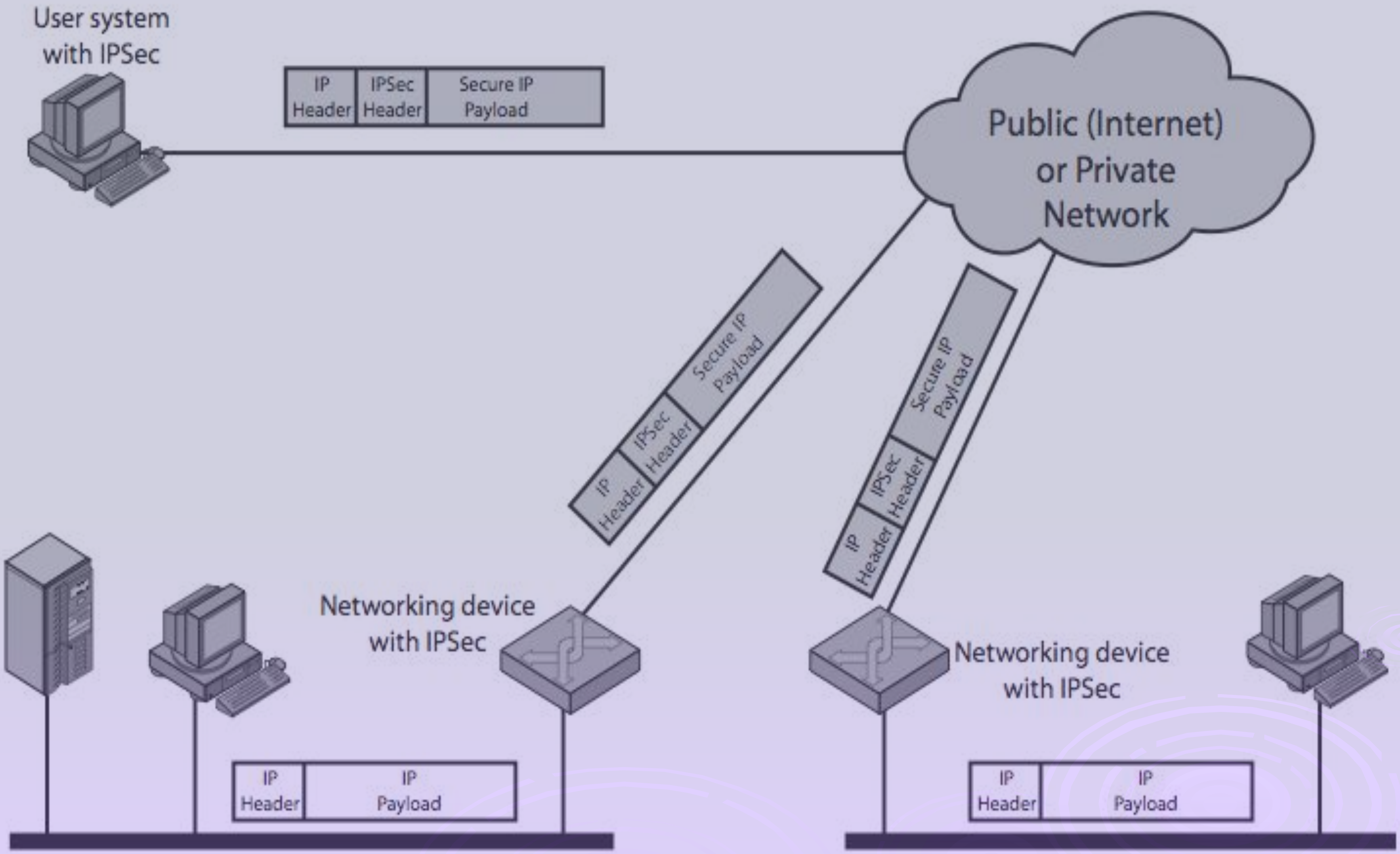
# Applications of IP Security

- Secure Branch office connectivity over the internet
- Secure remote access over the internet
- Establishing connectivity with parteners
- Enhances e-commerce security

# IPSec

- general IP Security mechanisms
- provides
  - authentication
  - confidentiality
  - key management
- applicable to use over LANs, across public & private WANs, & for the Internet

# IPSec Uses


User system with IPSec
IP Header
IPSec Header
Secure IP Payload
Public (Internet) or Private Network
IP Header
IPSec Header
Secure IP Payload
IP Header
IPSec Header
Secure IP Payload
Networking device with IPSec
Networking device with IPSec
IP Header
IP Payload
IP Header
IP Payload

# Benefits of IPSec

- in a firewall/router provides strong security to all traffic crossing the perimeter
- in a firewall/router is resistant to bypass
- is below transport layer, hence transparent to applications
- can be transparent to end users
- can provide security for individual users
- secures routing architecture

# IP Security Architecture

- specification is quite complex
- defined in numerous RFC’s
  - incl. RFC 2401/2402/2406/2408
  - many others, grouped by category
- mandatory in IPv6, optional in IPv4
- have two security header extensions:
  - Authentication Header (AH)
  - Encapsulating Security Payload (ESP)

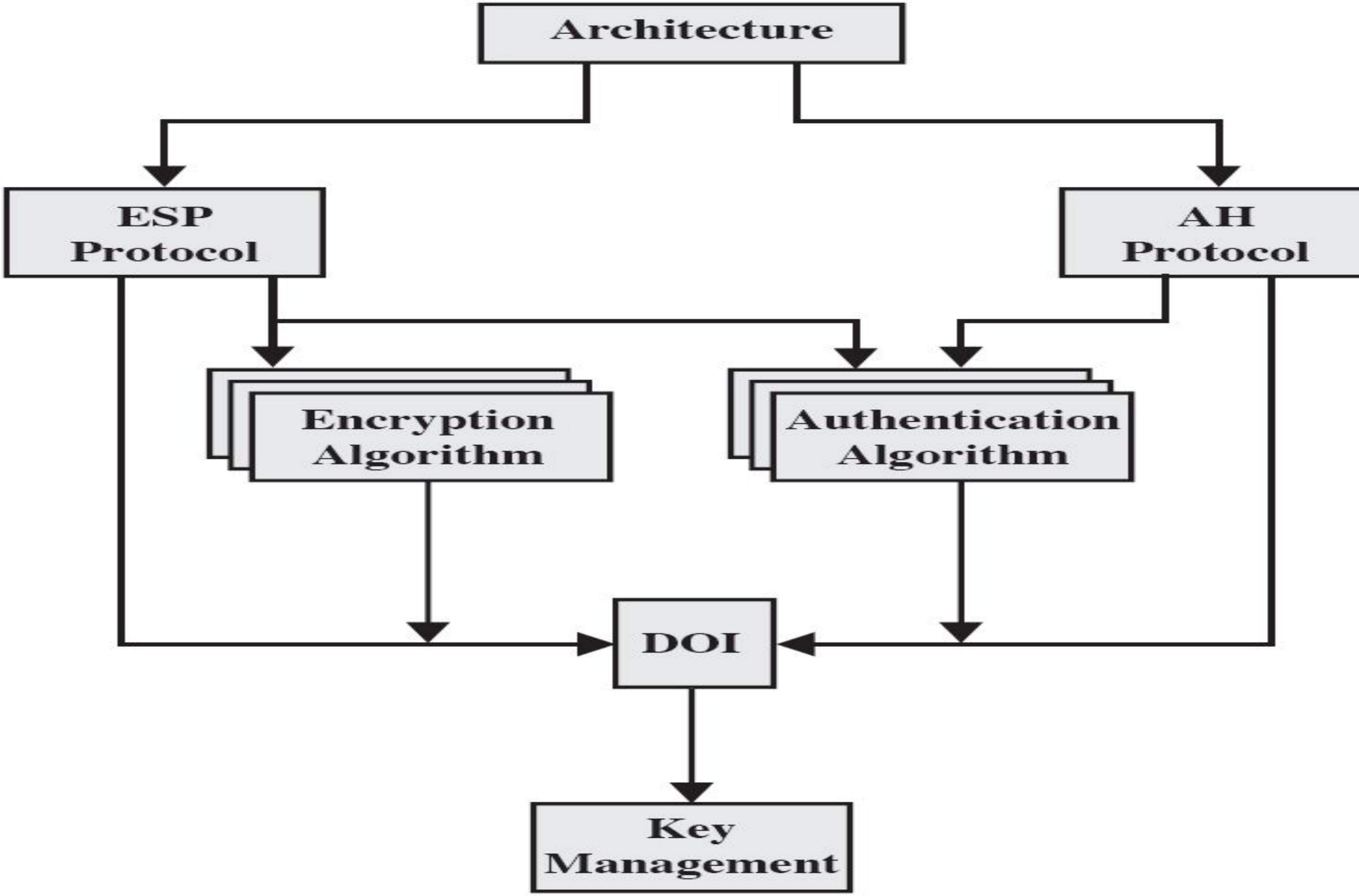


Figure 16.2 IPSec Document Overview

# IPSec Services

- Access control
- Connectionless integrity
- Data origin authentication
- Rejection of replayed packets
  - a form of partial sequence integrity
- Confidentiality (encryption)
- Limited traffic flow confidentiality

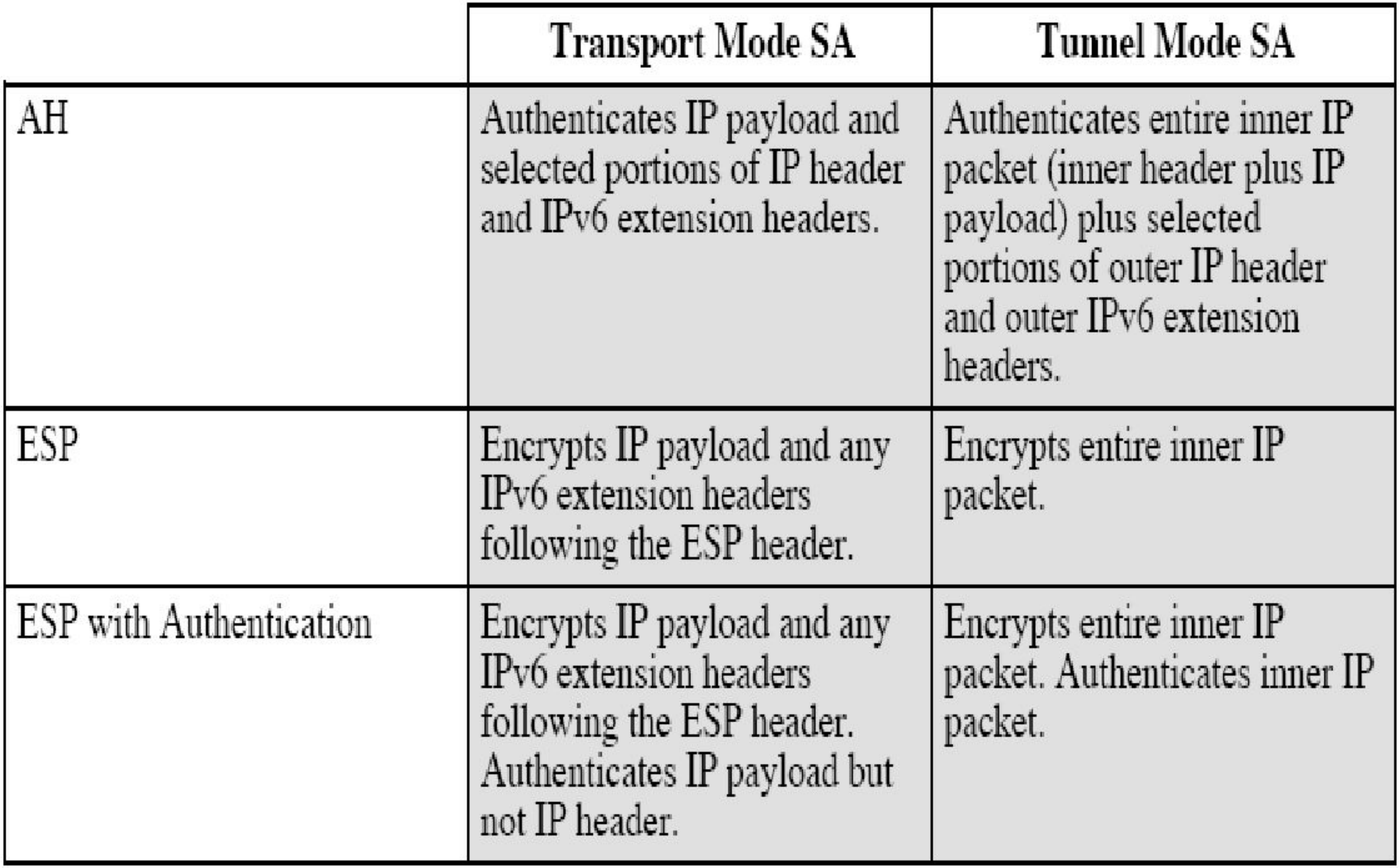
# Table 16.1 IPSec Services

| | AH | ESP (encryption only) | ESP (encryption plus authentication) |
|---|---|---|---|
| Access control | ✓ | ✓ | ✓ |
| Connectionless integrity | ✓ | | ✓ |
| Data origin authentication | ✓ | | ✓ |
| Rejection of replayed packets | ✓ | ✓ | ✓ |
| Confidentiality | | ✓ | ✓ |
| Limited traffic flow confidentiality | | ✓ | ✓ |

# Security Associations

- a one-way relationship between sender & receiver that affords security for traffic flow
- defined by 3 parameters:
  - Security Parameters Index (SPI)
  - IP Destination Address
  - Security Protocol Identifier
- has a number of other parameters
  - seq no, AH & EH info, lifetime etc
- have a database of Security Associations

## Table 16.2 Tunnel Mode and Transport Mode Functionality

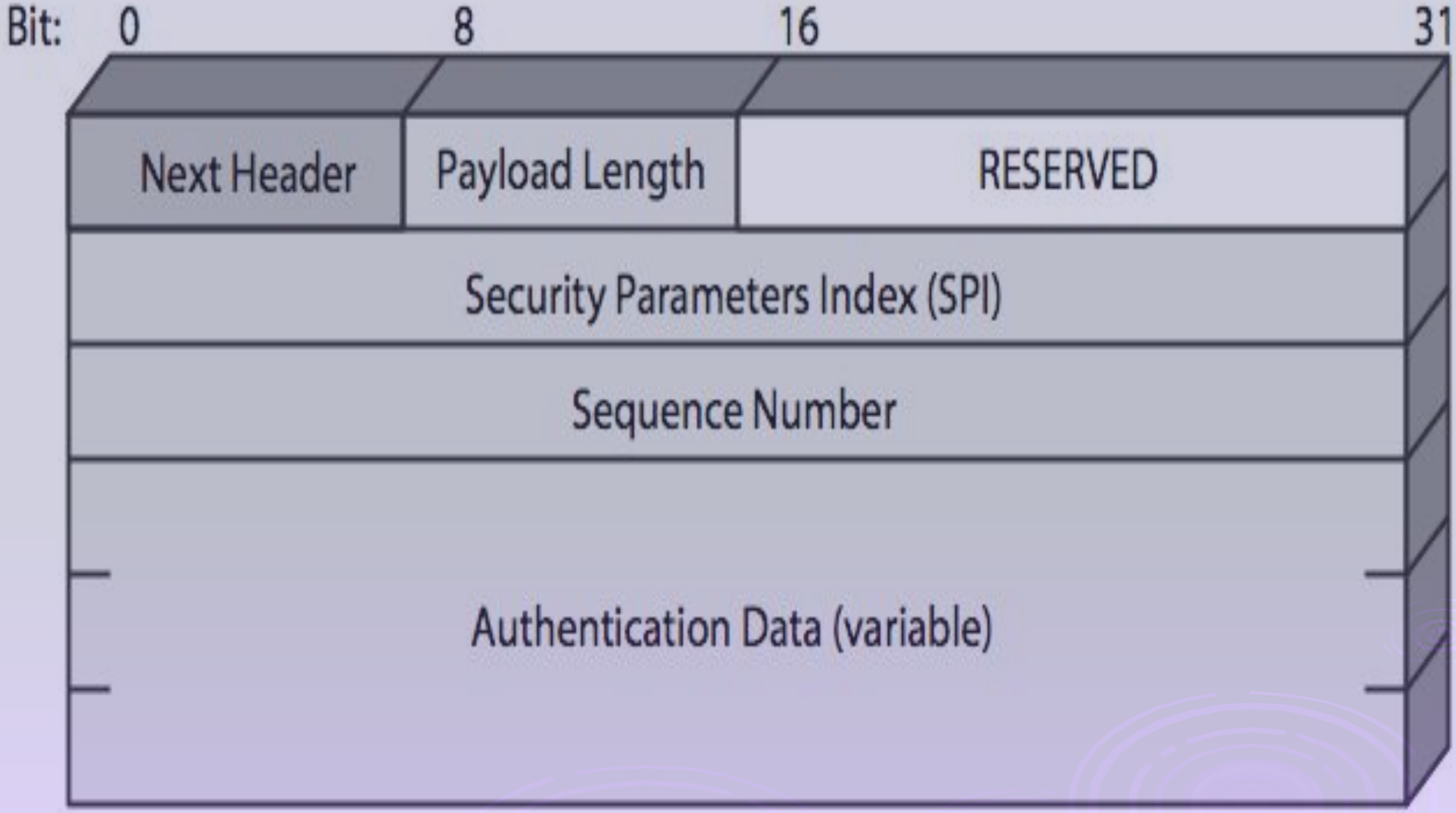


| | Transport Mode SA | Tunnel Mode SA |
|---|---|---|
| AH | Authenticates IP payload and selected portions of IP header and IPv6 extension headers. | Authenticates entire inner IP packet (inner header plus IP payload) plus selected portions of outer IP header and outer IPv6 extension headers. |
| ESP | Encrypts IP payload and any IPv6 extension headers following the ESP header. | Encrypts entire 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 entire inner IP packet. Authenticates inner IP packet. |

# Authentication Header (AH)

- provides support for data integrity & authentication of IP packets
  - end system/router can authenticate user/app
  - prevents address spoofing attacks by tracking sequence numbers
- based on use of a MAC
  - HMAC-MD5-96 or HMAC-SHA-1-96
- parties must share a secret key

# Authentication Header



Bit: 0 8 16 31

Next Header

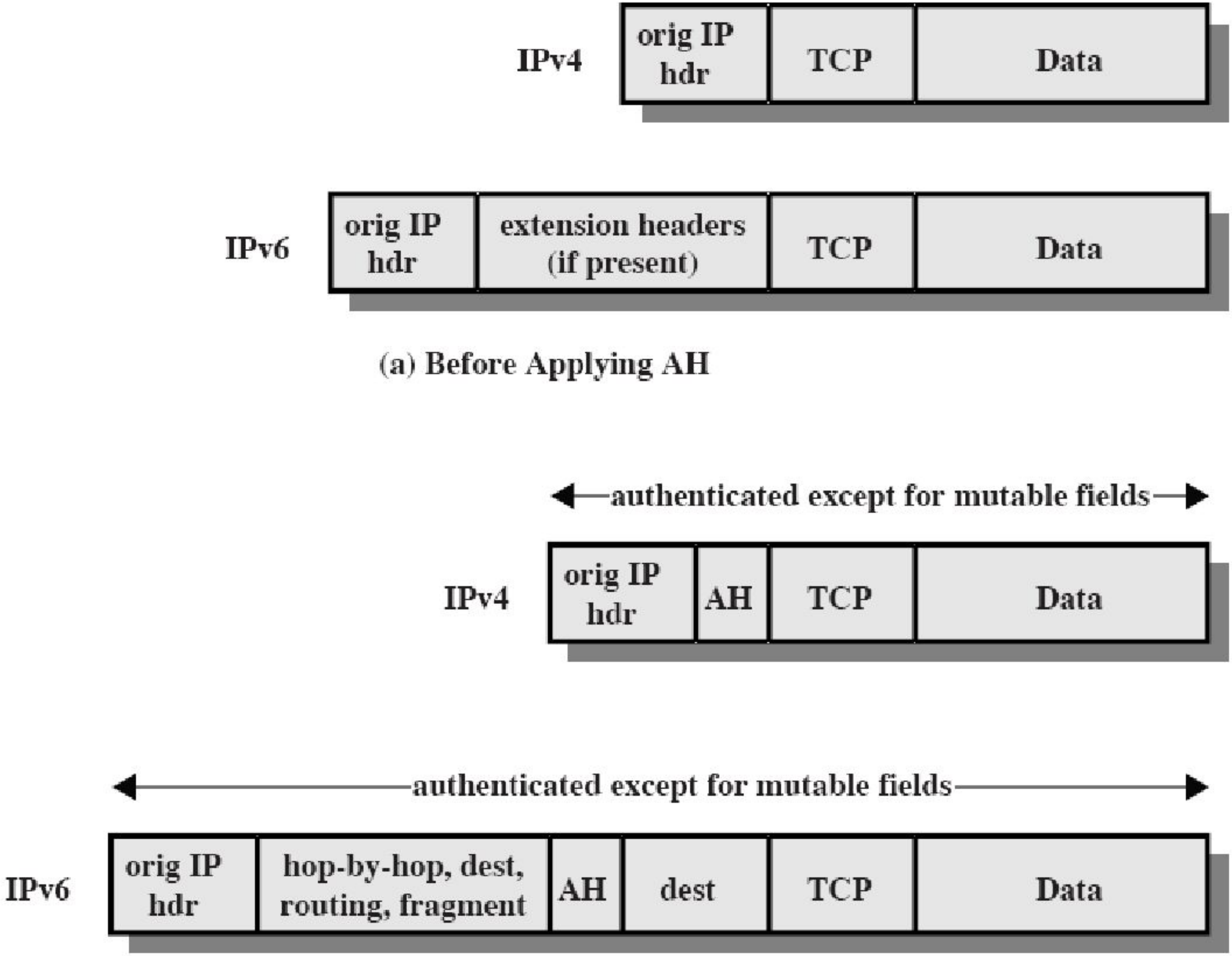
Payload Length

RESERVED

Security Parameters Index (SPI)

Sequence Number

Authentication Data (variable)



IPv4

orig IP hdr | TCP | Data

IPv6

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

(a) Before Applying AH

authenticated except for mutable fields

IPv4

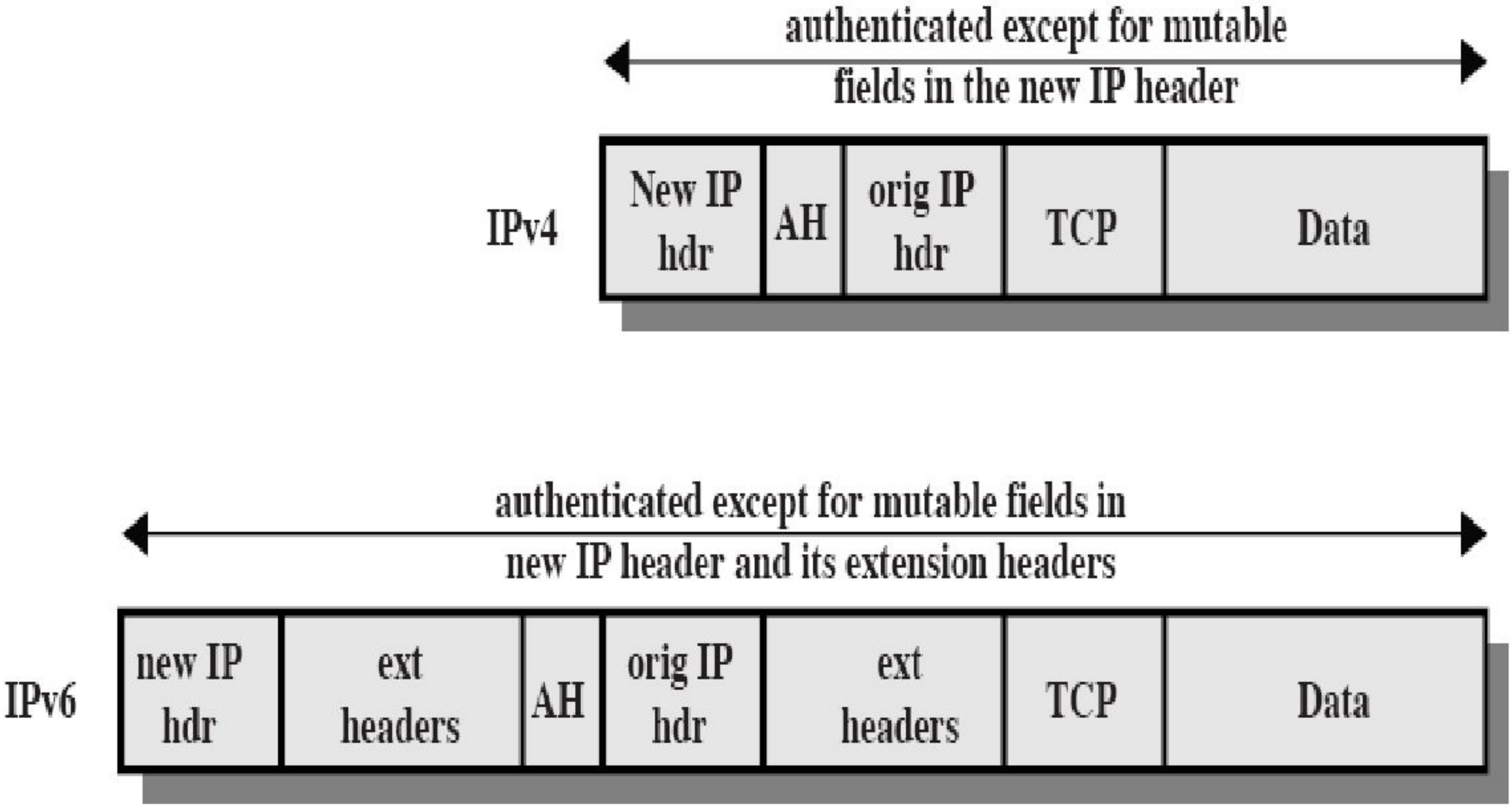
orig IP hdr | AH | TCP | Data

authenticated except for mutable fields

IPv6

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

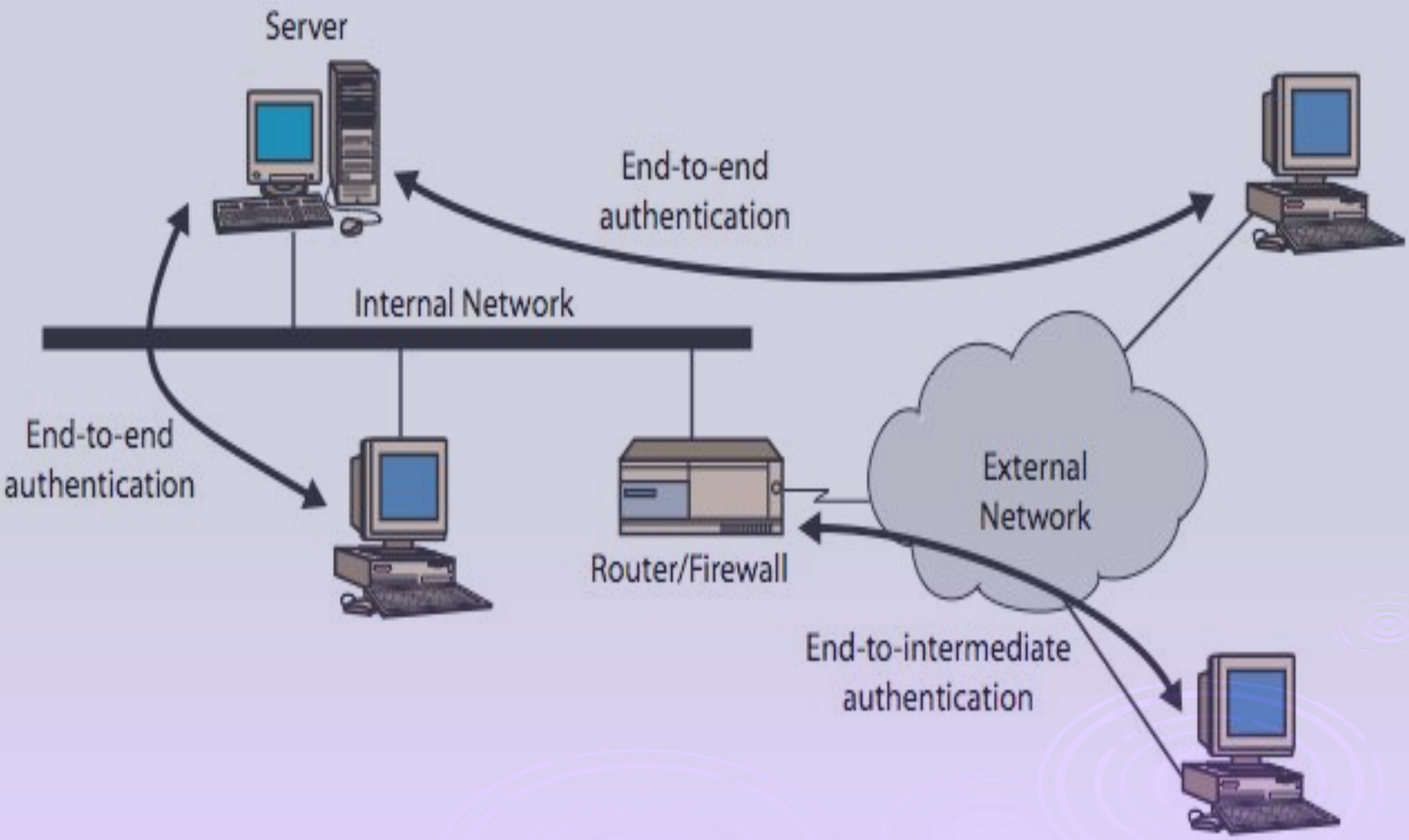
(b) Transport Mode


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

(c) Tunnel Mode

# Figure 16.6 Scope of AH Authentication

# Transport & Tunnel Modes


Server
End-to-end authentication
Internal Network
End-to-end authentication
Router/Firewall
External Network
End-to-intermediate authentication

# IPSec Components

- SPD - Security Policy Database
  - Defined by the sysadmin
  - Contains a set of rules

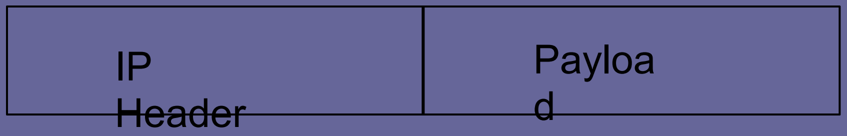
    Src IP | Dst IP | Ports | Action | IPSec Protocol | Mode | SA Index
- SAD – Security Association Database
  - Contains Security Associations
  - Each Security Association contains keys, sequence numbers
  - Must be stored in a secure place
- Key Management
  - Internet Key Exchange Protocol (IKE)
- Data Manipulation
  - For authentication, encryption and compression
  - Authentication Header (AH)
  - Encapsulation Security Payload (ESP)
  - IP Compression (IPCOMP)

# IPSec Modes

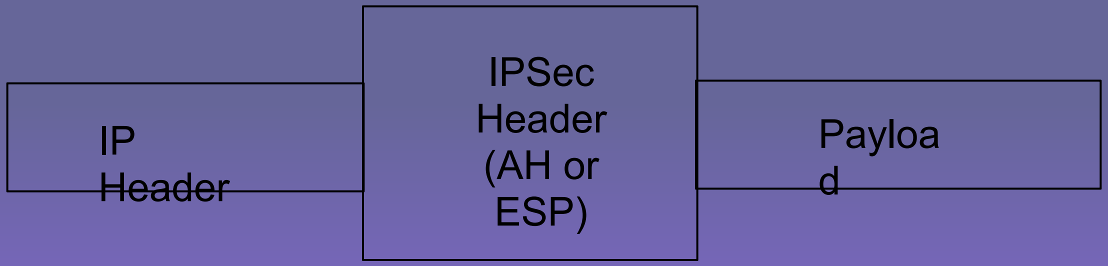
- Transport Mode
  - Used primarily to protect IP traffic between hosts
  - Adds requested protection to the datagram payload
- Tunnel Mode
  - The entire IP Datagram is treated as a block of data
  - Adds new header and protects the datagram
  - Used primarily between gateways

# IPSec Transport Mode

IP Datagram to be protected

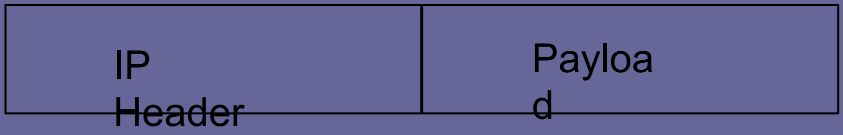


Protected Datagram



# IPSec Tunnel Mode

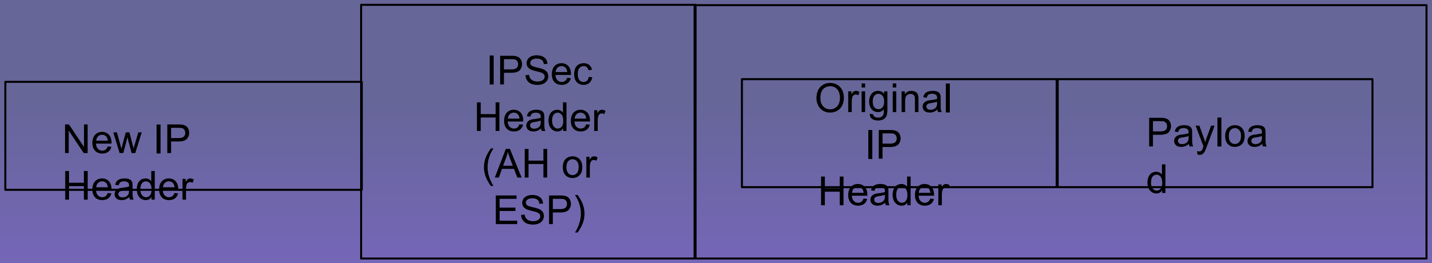
IP Datagram to be protected



IP Header

Payload

Protected Datagram (Tunnel Mode)



New IP Header

IPSec Header (AH or ESP)

Original IP Header

Payload

# IPSec Protocols (HEADERS)

- AH - Authentication Header
  - Connectionless integrity
  - Data origin authentication
  - Optional anti-replay service
- ESP – Encapsulating Security Payload
  - Confidentiality plus AH services

# Security Associations (SA)

- A Security Association is a simplex “connection” that provides security services to the traffic carried by it.
- SA's are different for tunnel mode and transport mode
- If either end of a security association is a security gateway the SA must be tunnel mode
- Every host must support both tunnel mode and transport mode

# Security Association Database (SAD)

- Separate SAD's are required for inbound traffic and outbound traffic
- The SAD contains parameters that are associated with each active security association
- A Selector is a set of IP and upper layer protocol field values that is used by the SPD to map traffic to a policy

# SAD Record Contents

| | | |
|---|---|---|
| SPI | 580 | 974 |
| Src IP | 192.168.2.1 | 192.168.1.1 |
| Dst IP | 192.168.1.1 | 192.168.2.1 |
| Src Port | Any | Any |
| Dst Port | Any | 80 |
| Parameters | stuff | stuff |
| Type | Inbound | Outbound |
| Pointer to SPD Entry | 4 | 7 |

# Additional SAD Record Fields

- Sequence Counter
- Sequence Counter Overflow
  - A flag when set causes an auditable event
- Anti-Replay Window
- AH Authentication Algorithm, keys, etc.
- ESP Encryption Algorithm, keys, IV Mode, IV, etc.
- ESP Authentication Algorithm, keys, etc.
- Lifetime of this SA
- IPSec protocol mode: tunnel, transport
- Path MTU

# Security Policy Database (SPD)

- Security association is a management construct to enforce a security policy
- A security policy specifies what services are to be offered to IP datagrams and in what fashion
- All processing of traffic both inbound and outbound must consult the SPD
- The SPD must specify what action will be taken on every packet

# SPD Record Contents

| Rule # | 1 | 2 |
|---|---|---|
| Src IP | 192.168.1.1 | 192.168.2.1 |
| Dst IP | 192.168.2.1 | 192.168.1.1 |
| Src Port | Any | Any |
| Dst Port | 23 | 443 |
| Action | IPSec | IPSec |
| Protocol | ESP | AH |
| Mode | Tunnel | Tunnel |
| Outbnd SA Index | 400 | 1 |

# Traffic processing

- Every inbound and outbound packet is processed by IPSec
- Three processing choices:
  - Discard
    - Not allowed to enter host
    - Auditable event
  - Bypass IPSec
  - Apply IPSec

# Outbound IP Traffic Processing

- The SPD must be consulted for every outbound packet
  - If no policy is found that matches the packet, the packet MUST be discarded and audited
  - If a policy is found that matches then the packet is mapped to an existing SA or a new SA is created.
- If IPSec is required the packet must be either mapped to an existing SA of a new SA is created
- Create a Header for Tunnel Mode

# Outbound IP Traffic Processing

- Some packet's selectors will match multiple SAs
- The SPD is ordered
- IPSec must
  1) Locate the first appropriate policy in the SPD
  2) Find first SA in the SAD that matches the packet's selectors
  3) If no SA is found create a new one and link to the appropriate policy in the SPD
  4) Do the required IPSec processing

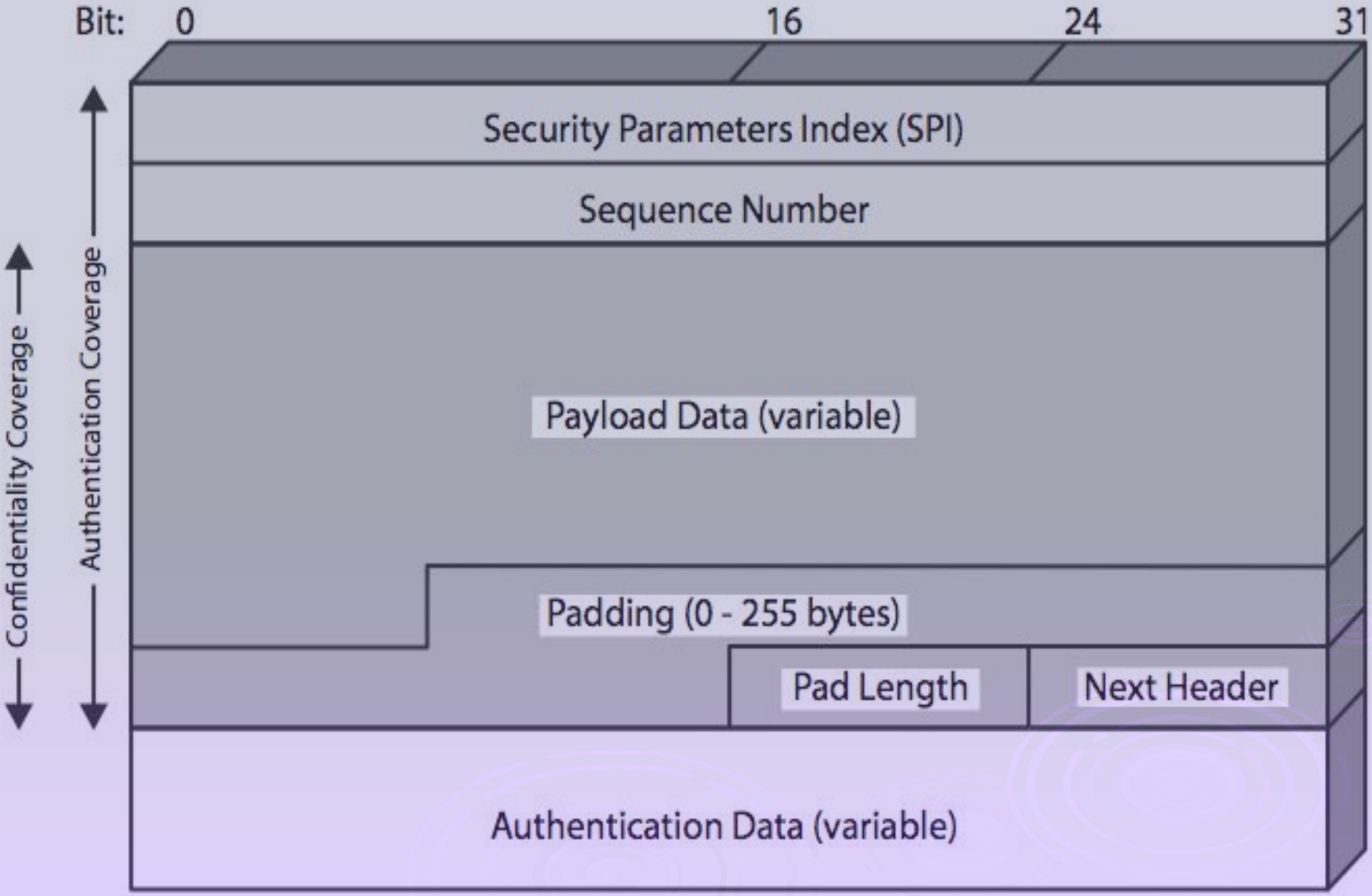
# Inbound IP Traffic Processing

- All fragments are reassembled
- Mapping the IP datagram to the appropriate SA depends on:
  - Outer IP header destination address
  - The IPSec protocol
  - The SPI
- If the mapping fails drop and log
- Otherwise use the SA to do the IPSec processing

# Encapsulating Security Payload (ESP)

- provides message content confidentiality & limited traffic flow confidentiality
- can optionally provide the same authentication services as AH
- supports range of ciphers, modes, padding
  - incl. DES, Triple-DES, RC5, IDEA, CAST etc
  - CBC & other modes
  - padding needed to fill blocksize, fields, for traffic flow

# Encapsulating Security Payload



Bit: 0 16 24 31

Security Parameters Index (SPI)

Sequence Number

Payload Data (variable)

Padding (0 - 255 bytes)

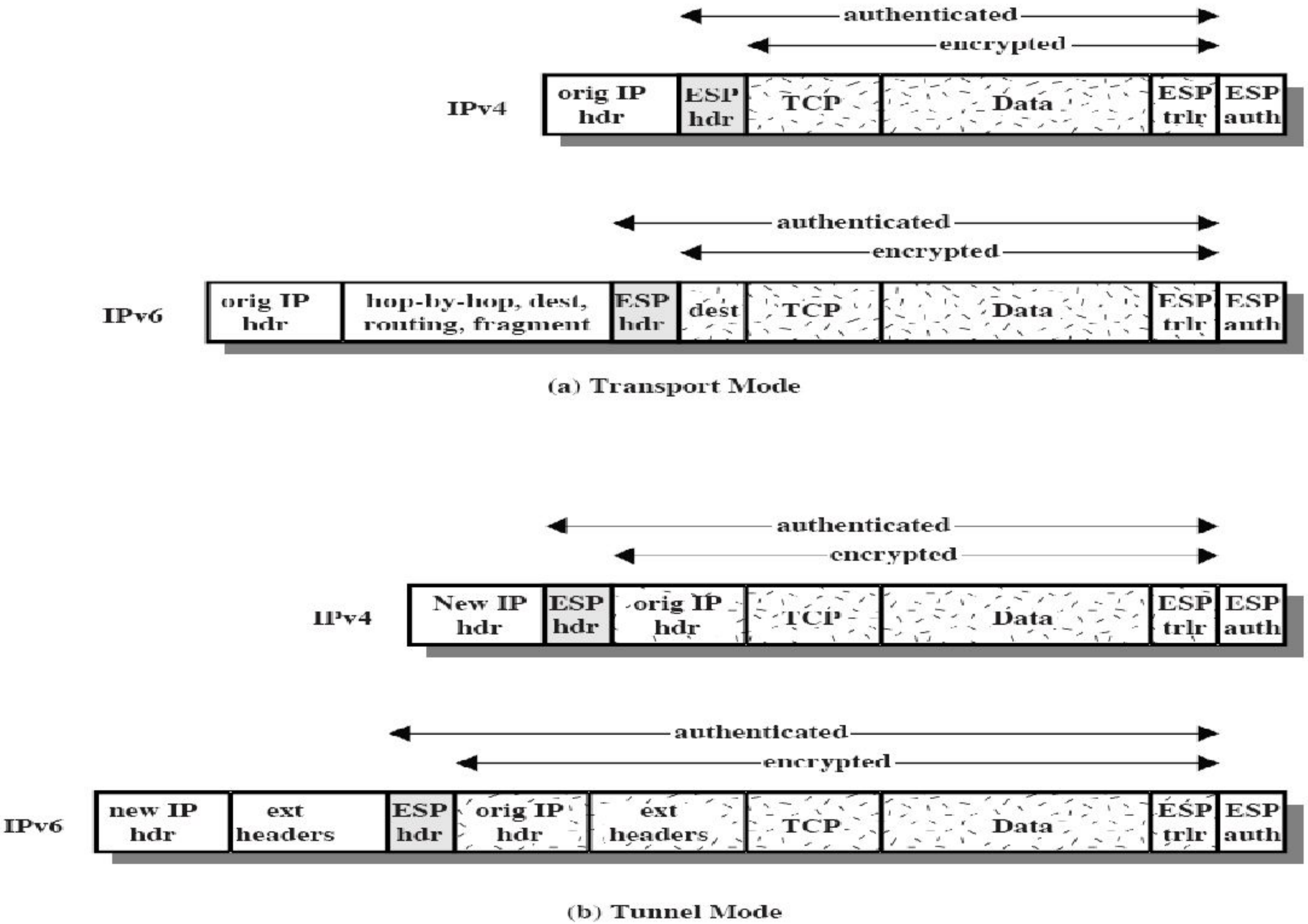
Pad Length

Next Header

Authentication Data (variable)

Authentication Coverage

Confidentiality Coverage



(a) Transport Mode

(b) Tunnel Mode

Figure 16.9 Scope of ESP Encryption and Authentication

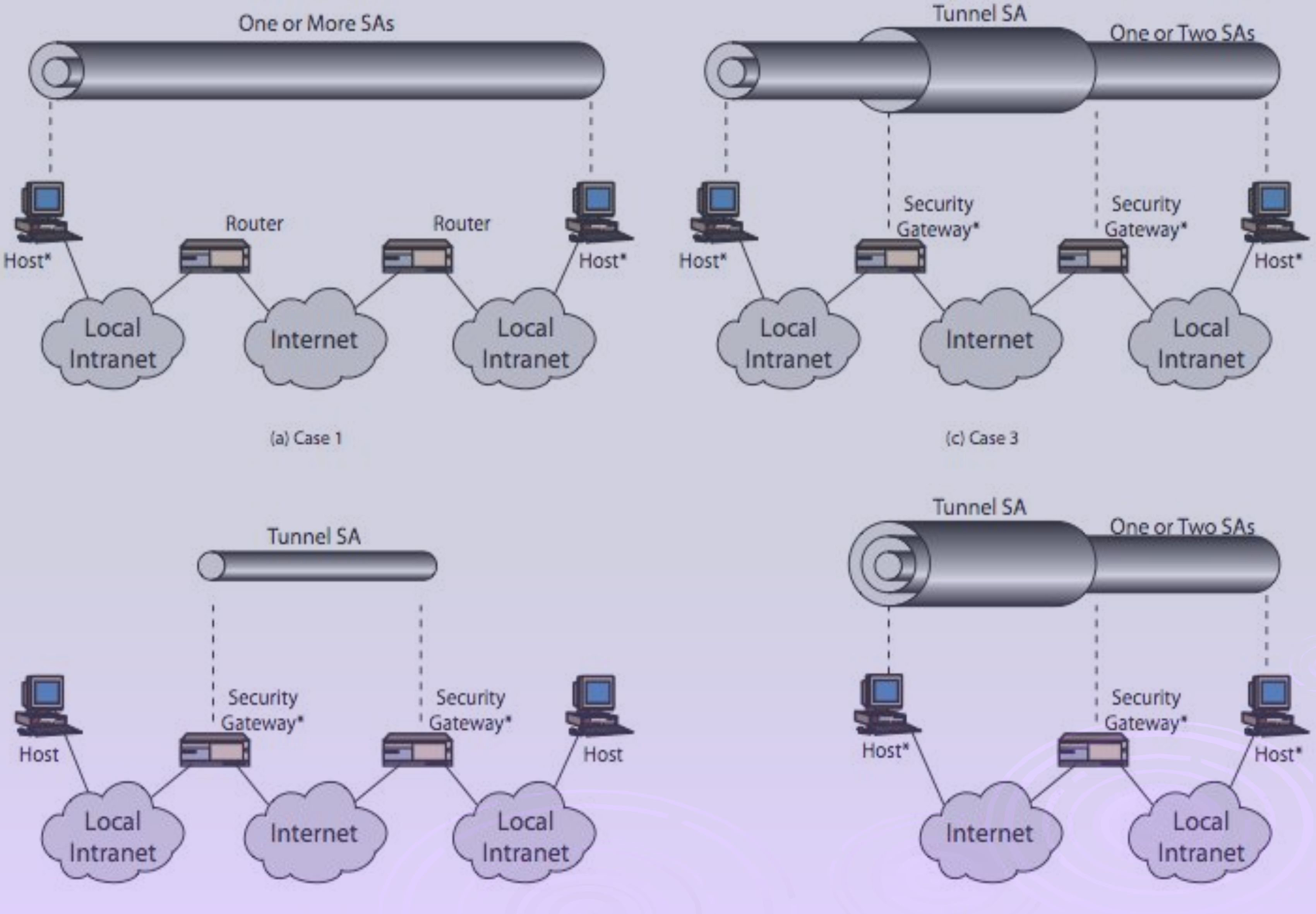
# Transport vs Tunnel Mode ESP

- transport mode is used to encrypt & optionally authenticate IP data
  - data protected but header left in clear
  - can do traffic analysis but is efficient
  - good for ESP host to host traffic
- tunnel mode encrypts entire IP packet
  - add new header for next hop
  - good for VPNs, gateway to gateway security

# Combining Security Associations

- SA's can implement either AH or ESP
- to implement both need to combine SA's
  - form a security association bundle
  - may terminate at different or same endpoints
  - combined by
    - transport adjacency
    - iterated tunneling
- issue of authentication & encryption order

# Combining Security Associations



(a) Case 1

(c) Case 3

(b) Case 2

(d) Case 4

# Key Management

- handles key generation & distribution
- typically need 2 pairs of keys
  - 2 per direction for AH & ESP
- manual key management
  - sysadmin manually configures every system
- automated key management
  - automated system for on demand creation of keys for SA’s in large systems
  - has Oakley & ISAKMP elements

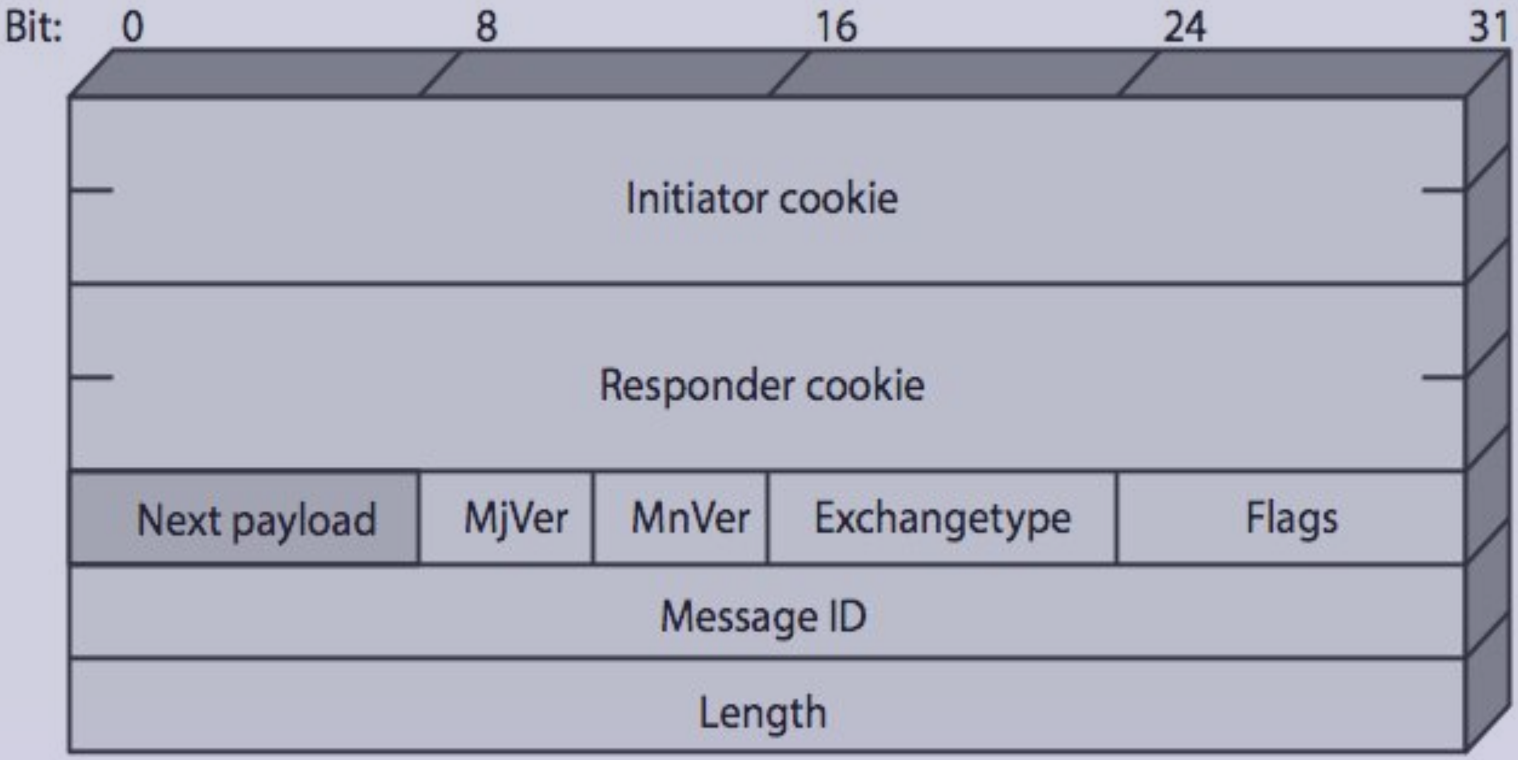
# Oakley

- a key exchange protocol
- based on Diffie-Hellman key exchange
- adds features to address weaknesses
  - cookies, groups (global params), nonces, DH key exchange with authentication
- can use arithmetic in prime fields or elliptic curve fields

# ISAKMP

- Internet Security Association and Key Management Protocol
- provides framework for key management
- defines procedures and packet formats to establish, negotiate, modify, & delete SAs
- independent of key exchange protocol, encryption alg, & authentication method

# ISAKMP



Bit: 0 8 16 24 31

Initiator cookie

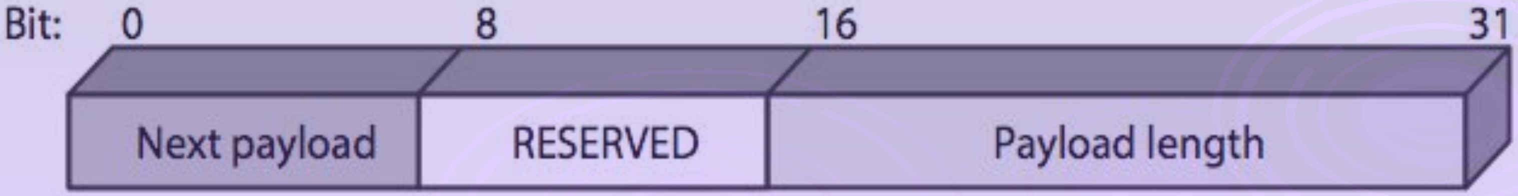
Responder cookie

Next payload | MjVer | MnVer | Exchangetype | Flags

Message ID

Length

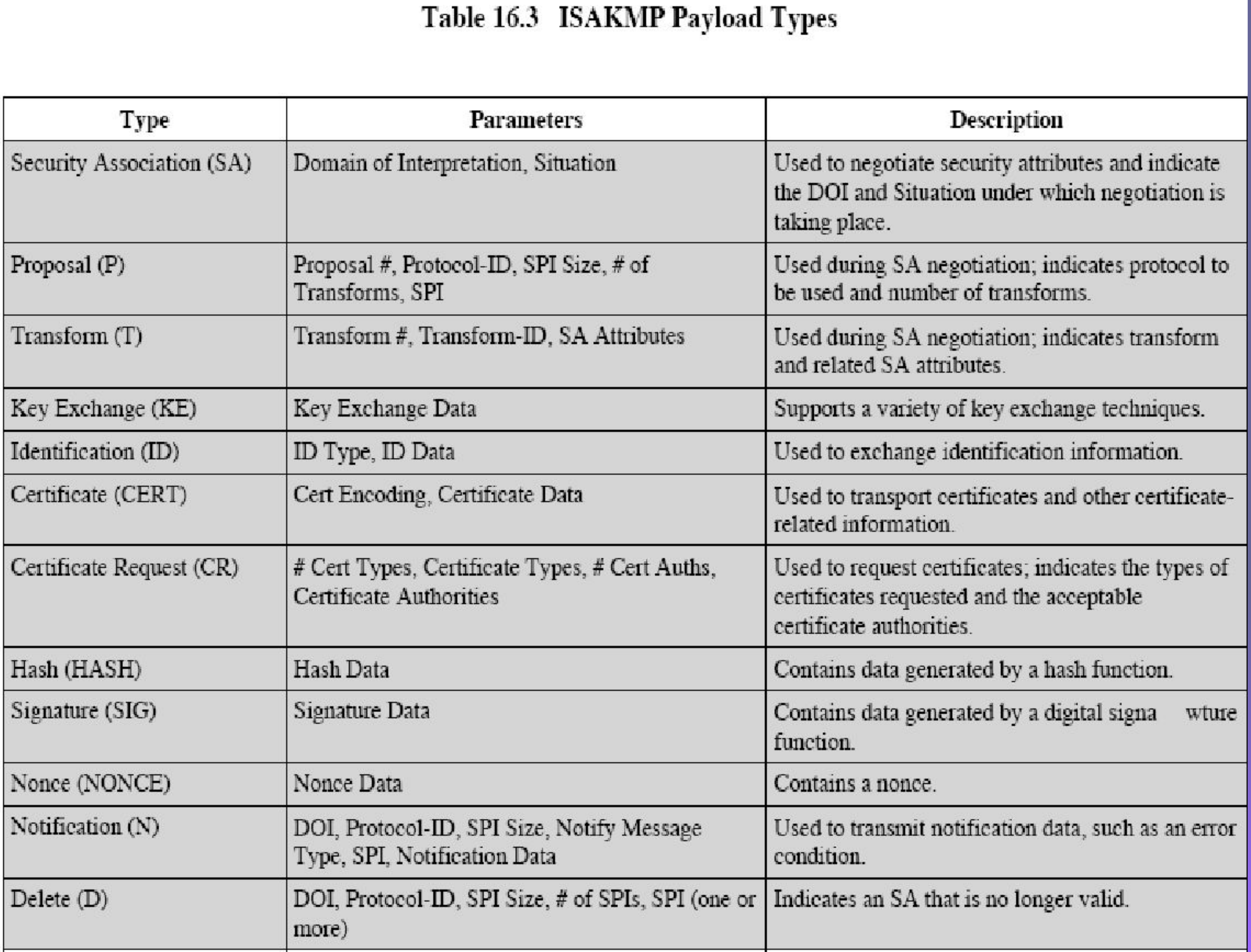
(a) ISAKMP Header



Bit: 0 8 16 31

Next payload | RESERVED | Payload length

(b) Generic Payload Header



## Table 16.3 ISAKMP Payload Types

| Type | Parameters | Description |
|---|---|---|
| Security Association (SA) | Domain of Interpretation, Situation | Used to negotiate security attributes and indicate the DOI and Situation under which negotiation is taking place. |
| Proposal (P) | Proposal #, Protocol-ID, SPI Size, # of Transforms, SPI | Used during SA negotiation; indicates protocol to be used and number of transforms. |
| Transform (T) | Transform #, Transform-ID, SA Attributes | Used during SA negotiation; indicates transform and related SA attributes. |
| Key Exchange (KE) | Key Exchange Data | Supports a variety of key exchange techniques. |
| Identification (ID) | ID Type, ID Data | Used to exchange identification information. |
| Certificate (CERT) | Cert Encoding, Certificate Data | Used to transport certificates and other certificate-related information. |
| Certificate Request (CR) | # Cert Types, Certificate Types, # Cert Auths, Certificate Authorities | Used to request certificates; indicates the types of certificates requested and the acceptable certificate authorities. |
| Hash (HASH) | Hash Data | Contains data generated by a hash function. |
| Signature (SIG) | Signature Data | Contains data generated by a digital signa wture function. |
| Nonce (NONCE) | Nonce Data | Contains a nonce. |
| Notification (N) | DOI, Protocol-ID, SPI Size, Notify Message Type, SPI, Notification Data | Used to transmit notification data, such as an error condition. |
| Delete (D) | DOI, Protocol-ID, SPI Size, # of SPIs, SPI (one or more) | Indicates an SA that is no longer valid. |

## Table 16.4 ISAKMP Exchange Types

| Exchange | Note |
|---|---|
| **(a) Base Exchange** | |
| (1) **I → R:** SA; NONCE | Begin ISAKMP-SA negotiation |
| (2) **R → I:** SA; NONCE | Basic SA agreed upon |
| (3) **I → R:** KE; $ID_I$; AUTH | Key generated; Initiator identity verified by responder |
| (4) **R → I:** KE; $ID_R$; AUTH | Responder identity verified by initiator; Key generated; SA established |
| **(b) Identity Protection Exchange** | |
| (1) **I → R:** SA | Begin ISAKMP-SA negotiation |
| (2) **R → I:** SA | Basic SA agreed upon |
| (3) **I → R:** KE; NONCE | Key generated |
| (4) **R → I:** KE; NONCE | Key generated |
| (5)* **I → R:** $ID_I$; AUTH | Initiator identity verified by responder |
| (6)* **R → I:** $ID_R$; AUTH | Responder identity verified by initiator; SA established |
| **(c) Authentication Only Exchange** | |
| (1) **I → R:** SA; NONCE | Begin ISAKMP-SA negotiation |
| (2) **R → I:** SA; NONCE; $ID_R$; AUTH | Basic SA agreed upon; Responder identity verified by initiator |
| (3) **I → R:** $ID_I$; AUTH | Initiator identity verified by responder; SA established |
| **(d) Aggressive Exchange** | |
| (1) **I → R:** SA; KE; NONCE; $ID_I$ | Begin ISAKMP-SA negotiation and key exchange |
| (2) **R → I:** SA; KE; NONCE; $ID_R$; AUTH | Initiator identity verified by responder; Key generated; Basic SA agreed upon |
| (3)* **I → R:** AUTH | Responder identity verified by initiator; SA established |
| **(e) Informational Exchange** | |
| (1)* **I → R:** N/D | Error or status notification, or deletion |

# ISAKMP Payloads & Exchanges

- have a number of ISAKMP payload types:
  - Security, Proposal, Transform, Key, Identification, Certificate, Certificate, Hash, Signature, Nonce, Notification, Delete
- ISAKMP has framework for 5 types of message exchanges:
  - base, identity protection, authentication only, aggressive, informational

# Summary

- have considered:
  - IPSec security framework
  - AH
  - ESP
  - key management & Oakley/ISAKMP