# IP Security

Dr. KR Chowdhary,Professor
Dept. of Computer Sc. & Engg.
MBM Engineering College
(ref. William Stalling)

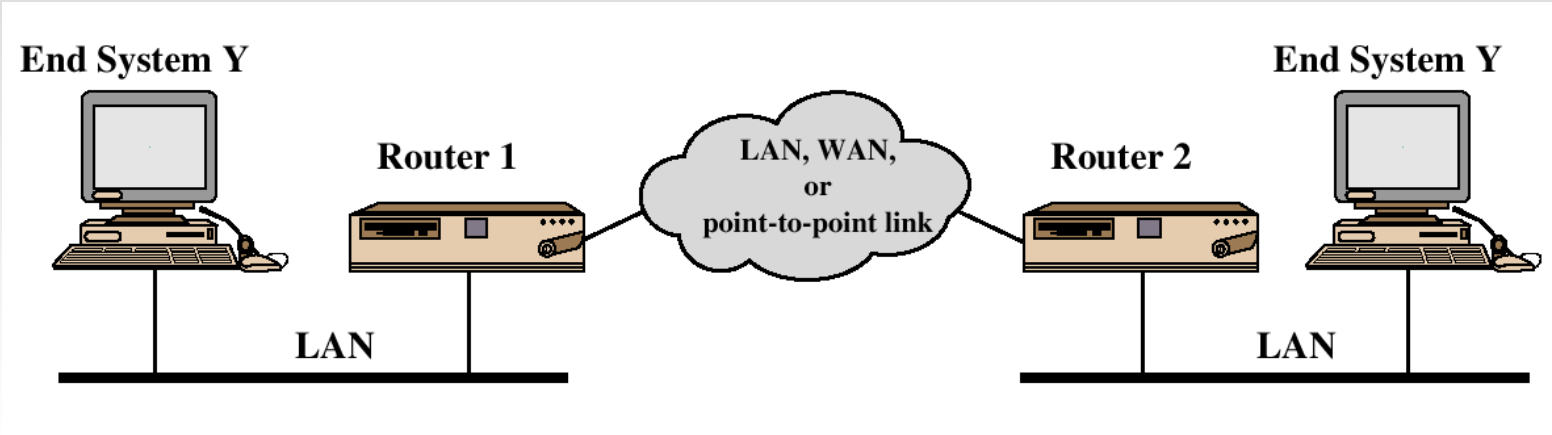
# Outline

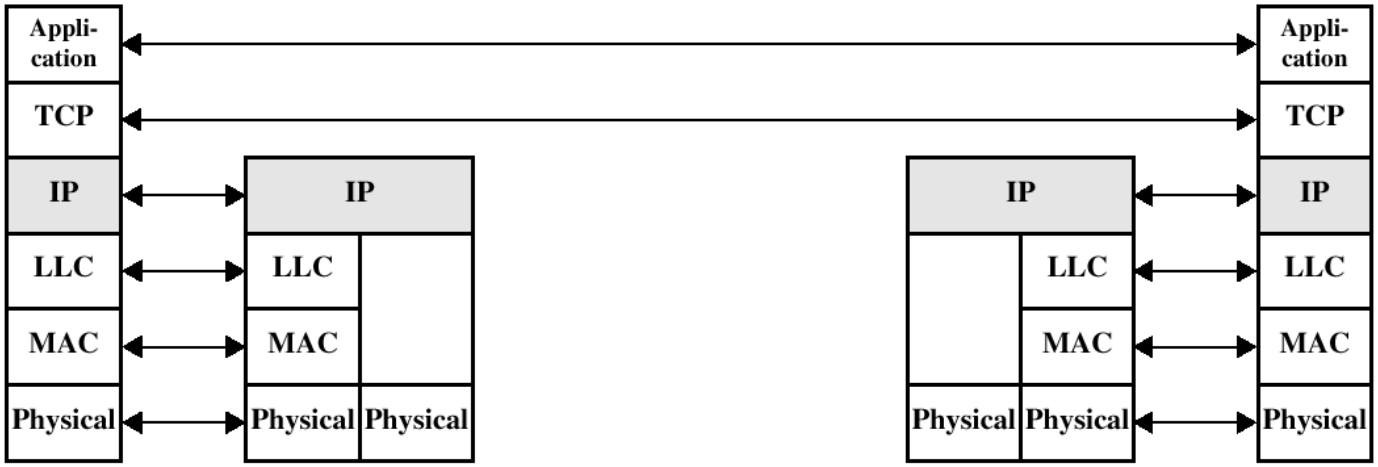
- Internetworking and Internet Protocols
- IP Security Overview
- IP Security Architecture
- Authentication Header
- Encapsulating Security Payload
- Combinations of Security Associations
- Key Management

# Key points

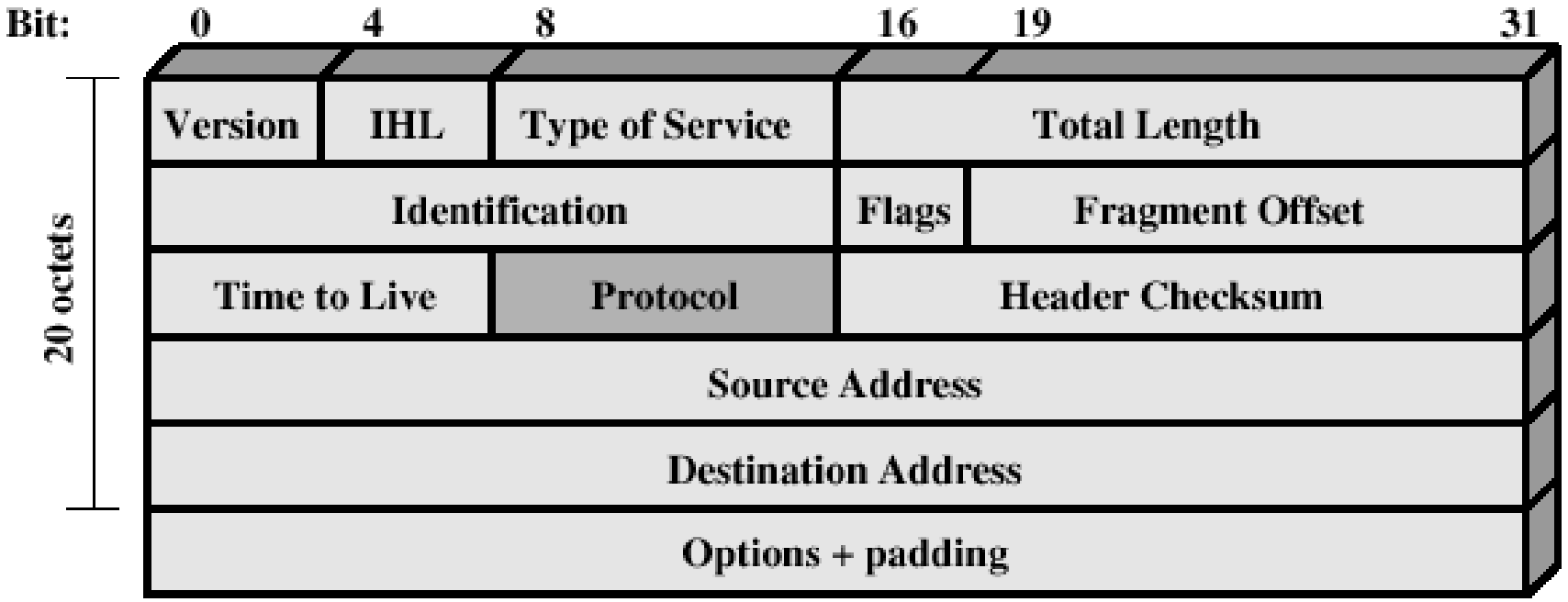
- can be added to ipv4, ipv6
- it is more powerful security
- authentication(pkt), confidentiality (encryption), key management
- Hence, all distributed apps. - remot login, c/s, email, ftp, web access are all protected.
- secure communication a LAN, WANs, Internet

# TCP/IP Example

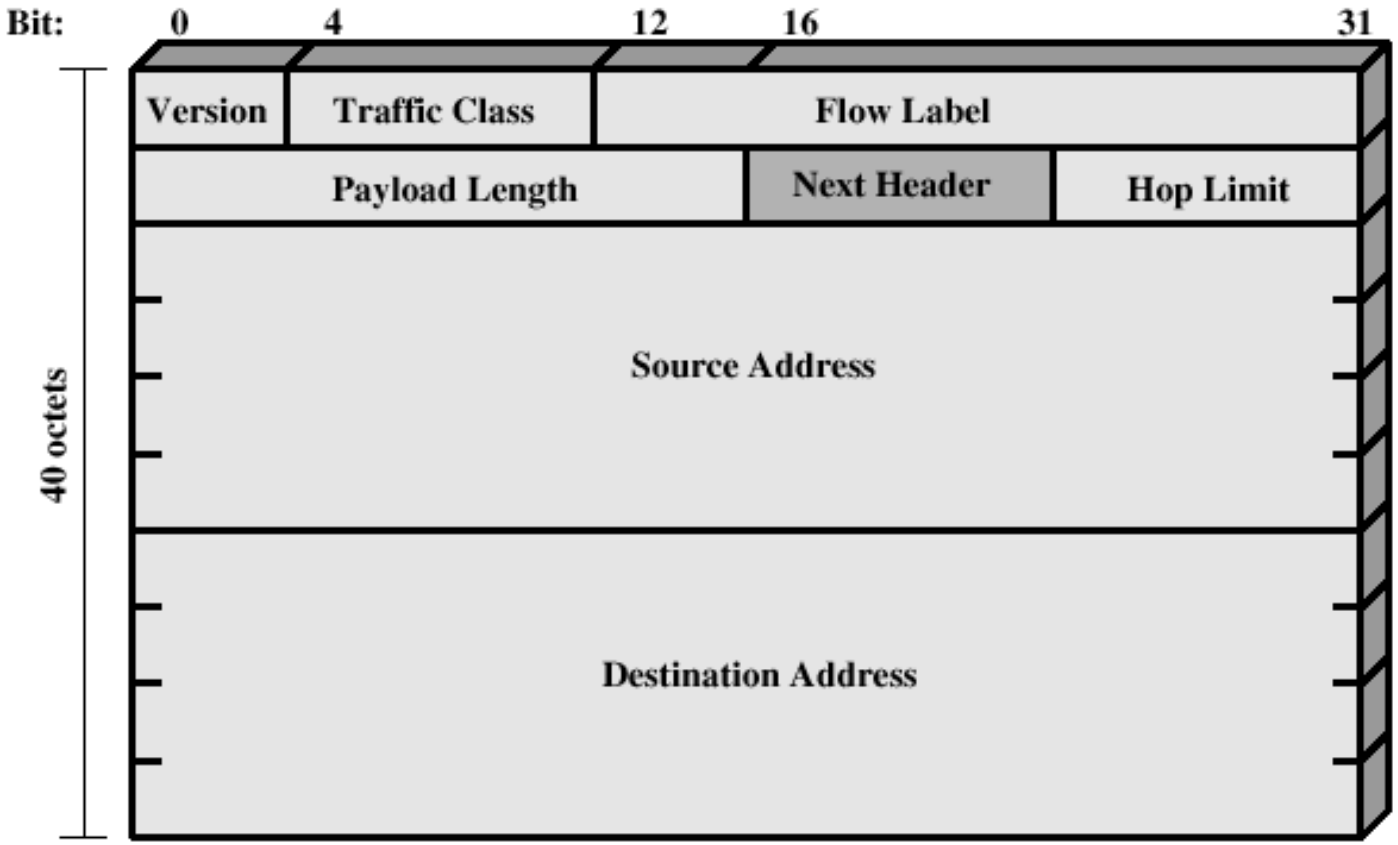


# IPv4 Header


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

# IPv6 Header


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

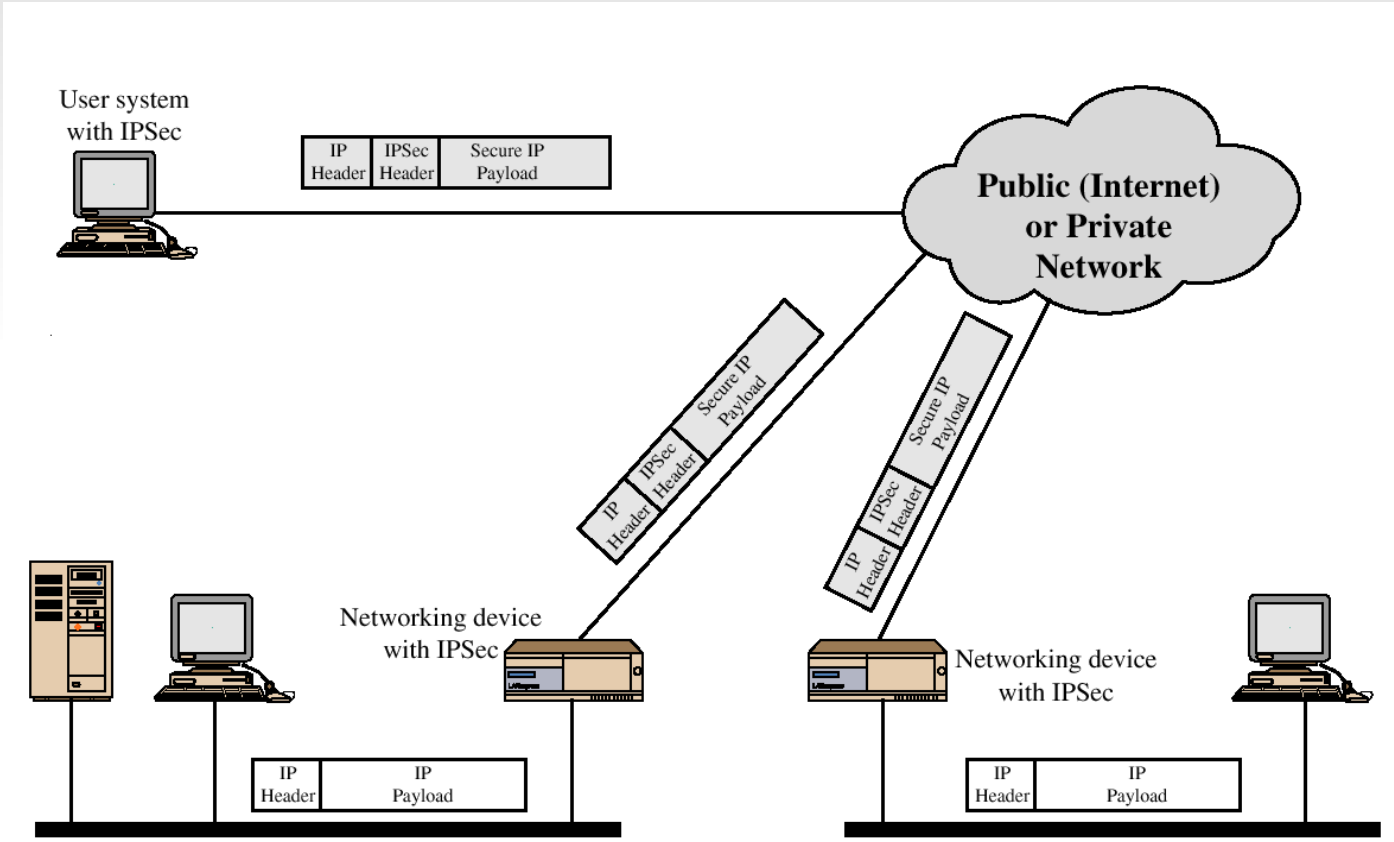
# IP Security Overview

- IPSec is not a single protocol.
- Instead, IPSec provides a set of security algorithms plus a general framework that allows a pair of communicating entities to use whichever algorithms provide security appropriate for the communication.

# IP Security Overview

- Applications of IPSec
  - Secure branch office connectivity over the Internet
  - Secure remote access over the Internet
  - Establsihing extranet and intranet connectivity with partners
  - Enhancing electronic commerce security

# IP Security Scenario



# IP Security Overview

- Benefits of IPSec
  - can be provided in firewall/router
  - is below transport layer (below transport layer (TCP, UDP) and transparent to applications (applications are not effected by Ipsec. use)
  - Provide security for individual users, if required (for setting virtual subset)
- IPSec routing applications
  - A router or neighbor advertisement comes from an authorized router
  - A redirect message comes from the router to which the initial packet was sent
  - A routing update is not forged

(without this an opponent can disrupt communications/divert traffic).

# IPSec Services

Provides security services at IP layer by enabling syste to select reqired protocosl/services.

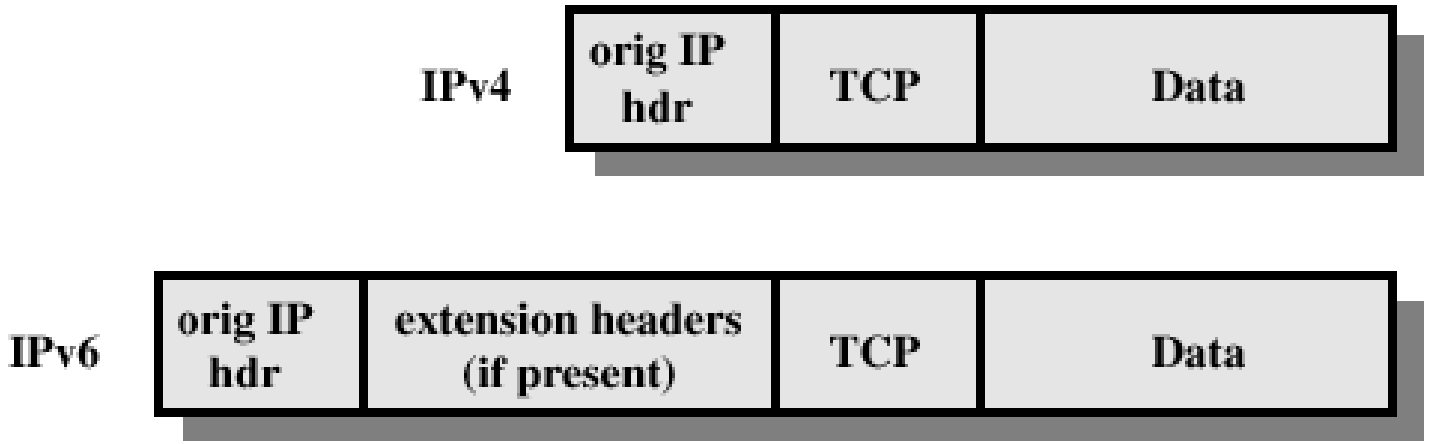
- Access Control
- Connectionless integrity
- Data origin authentication
- Rejection of replayed packets
- Confidentiality (encryption)
- Limited traffic flow confidentiallity

# Security Associations (SA)

- A one way relationsship between a sender and a receiver.
- Identified by three parameters:
  - Security Parameter Index (SPI)
  - IP Destination address
  - Security Protocol Identifier

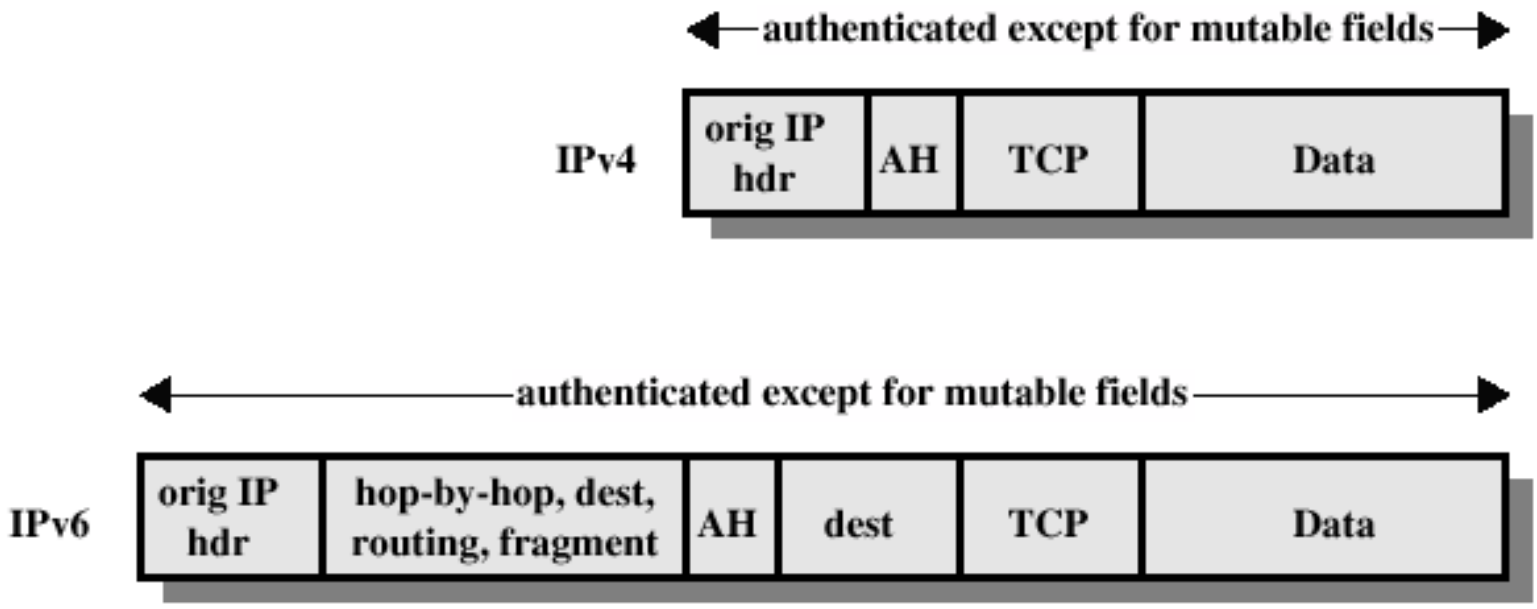
| | Transport Mode SA | Tunnel Mode SA |
|---|---|---|
| AH(authentication header) | Authenticates IP payload and selected portions of IP header and IPv6 extension headers | Authenticates entire inner IP packet plus selected portions of outer IP header |
| ESP(encapsulating security payload) | Encrypts IP payload and any IPv6 extesion header | Encrypts inner IP packet |
| ESP with authentication | Encrypts IP payload and any IPv6 extesion header. Authenticates IP payload but no IP header | Encrypts inner IP packet. Authenticates inner IP packet. |

# Before applying AH



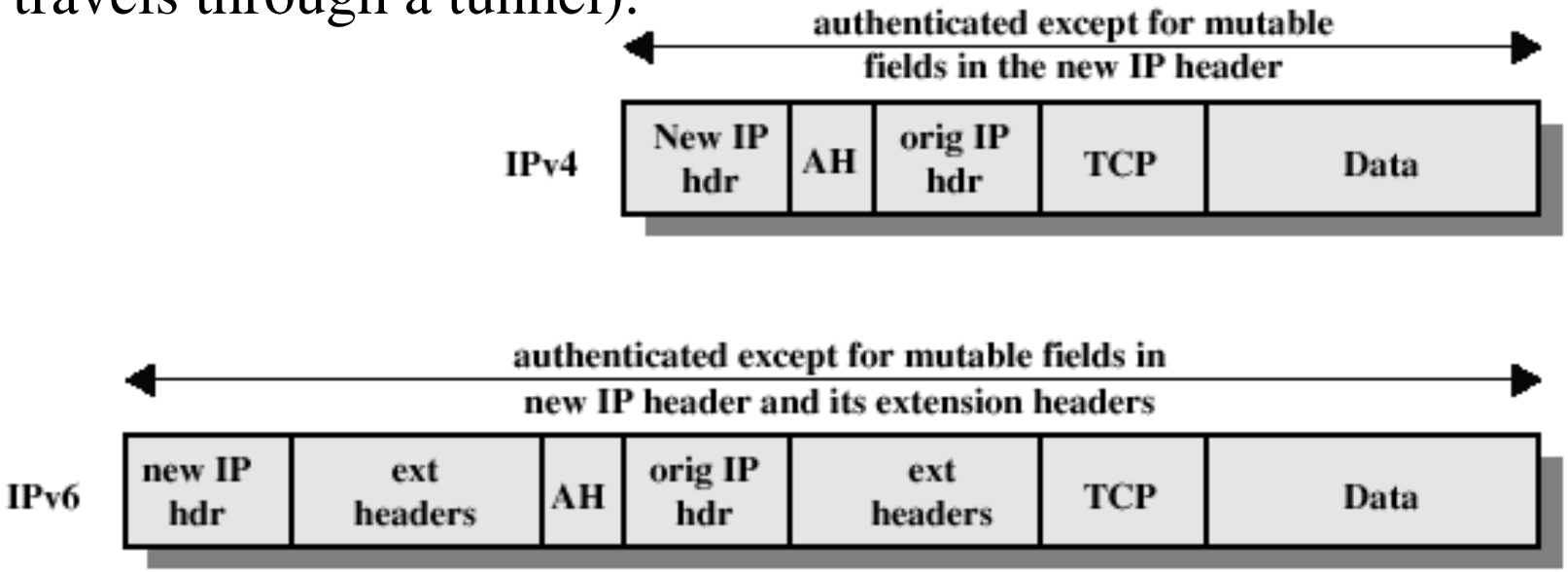
# Transport Mode (AH Authentication)

for upper layer of protocols (tcp/udp segments, for end-to-end comm



# Tunnel Mode (AH Authentication)

protection of entire ip packet(pkt+sec. fileds are payload), inner pakt travels through a tunnel).



# Authentication Header

- Provides support for data integrity and authentication (MAC code) of IP packets.
- Guards against replay attacks.

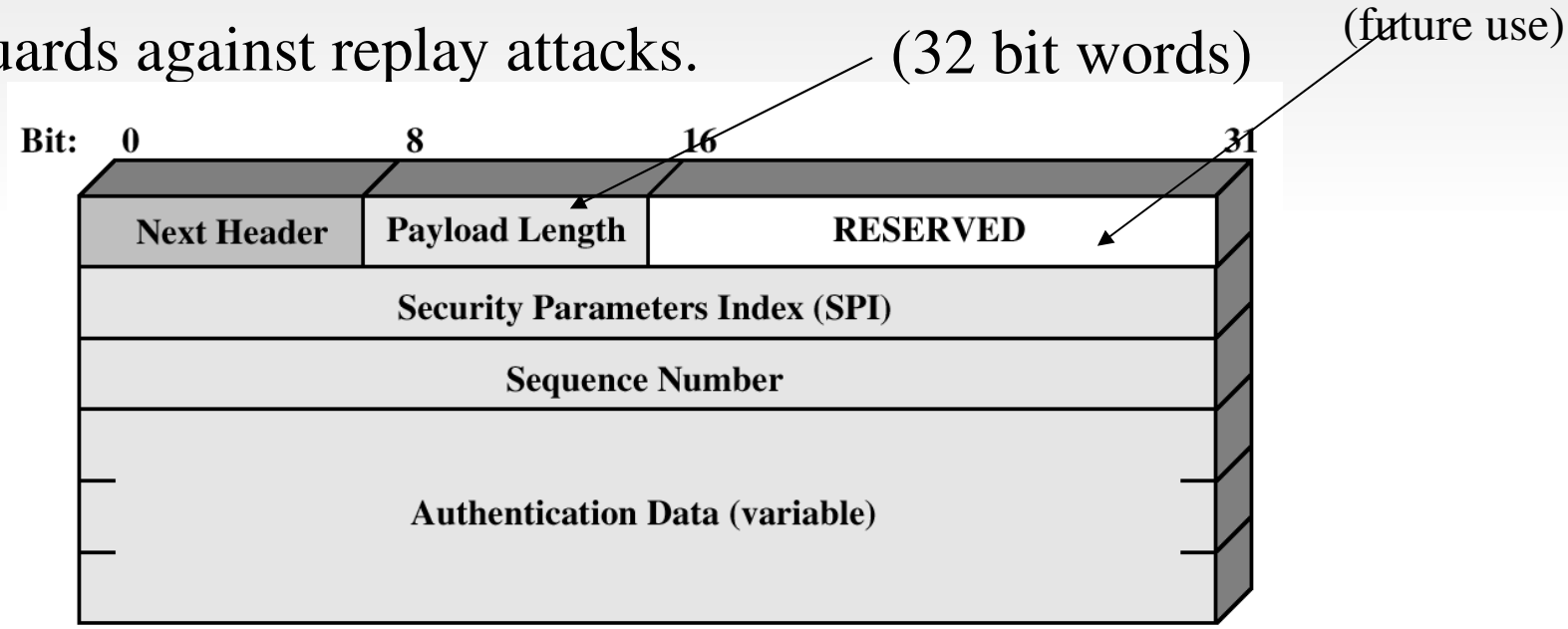
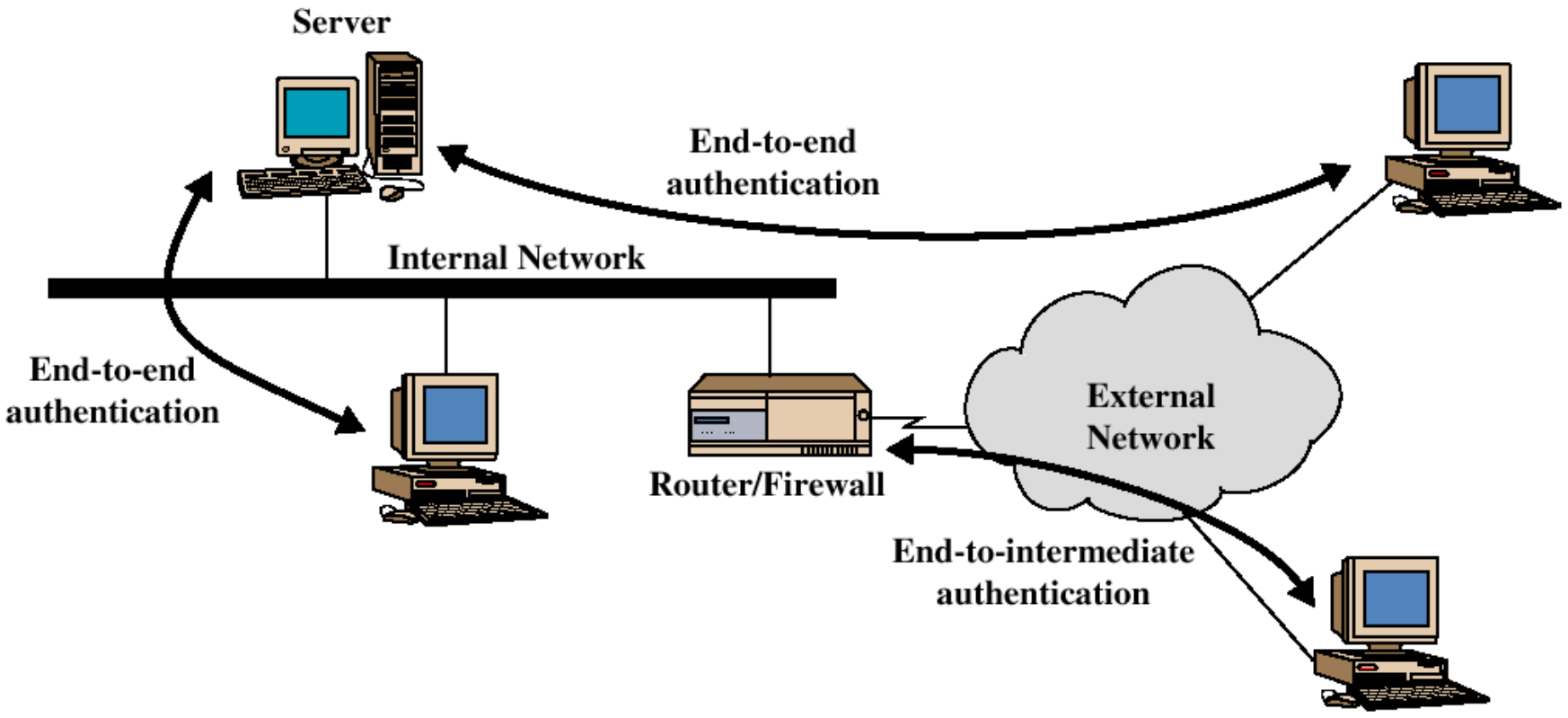



**Figure 6.3 IPSec Authentication Header**

# End-to-end versus End-to-Intermediate Authentication



# Encapsulating Security Payload

- ESP provides confidentiality services

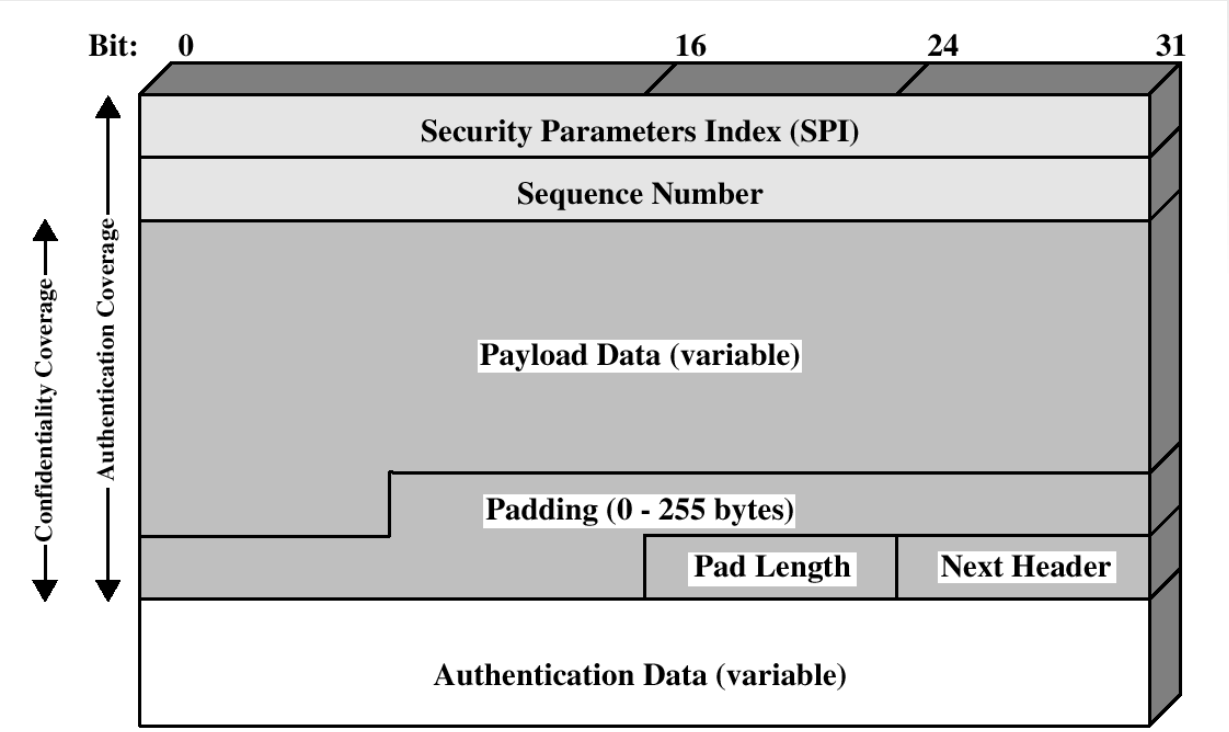
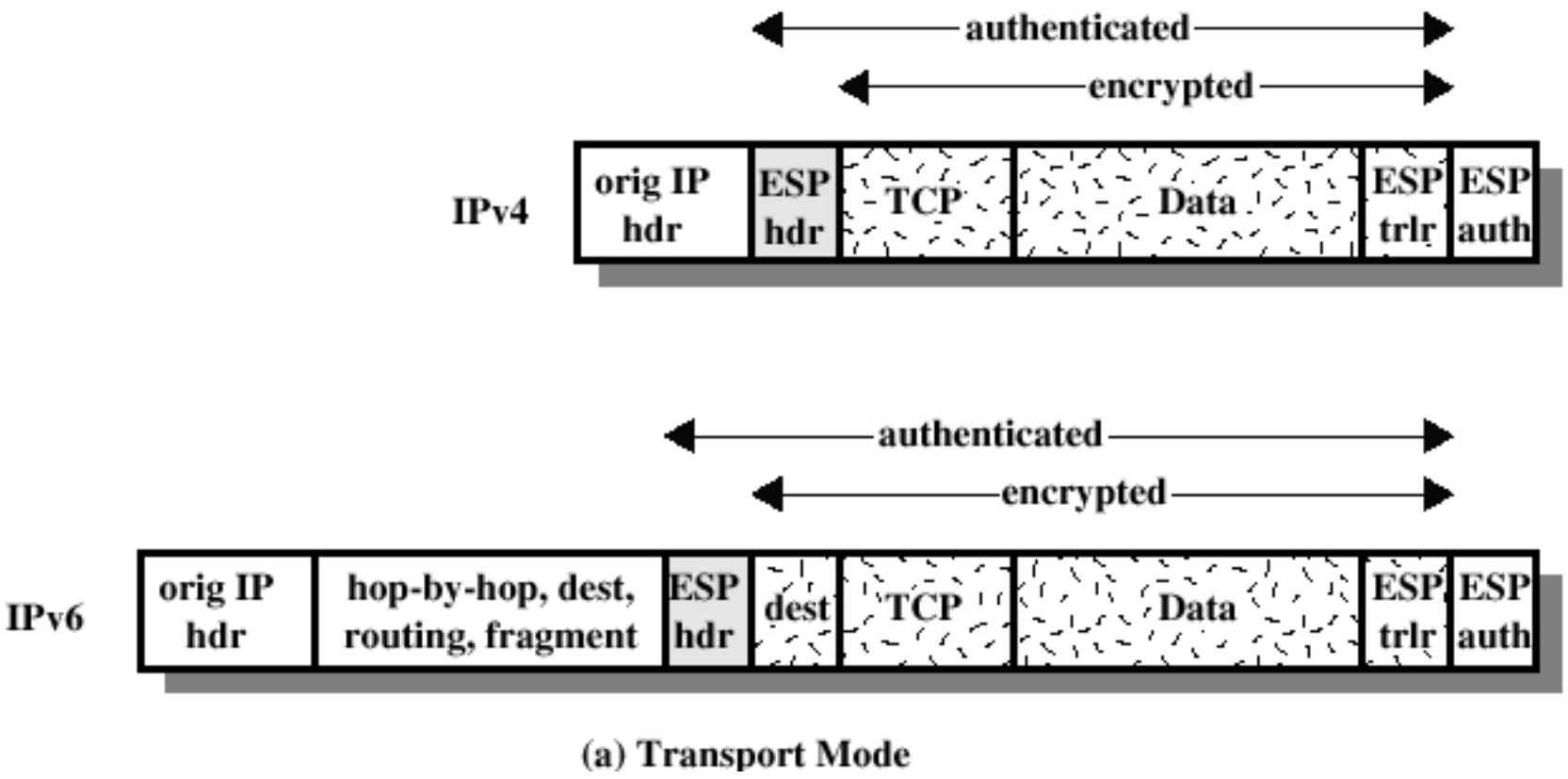



**Figure 6.7 IPSec ESP Format**

# Encryption and Authentication Algorithms

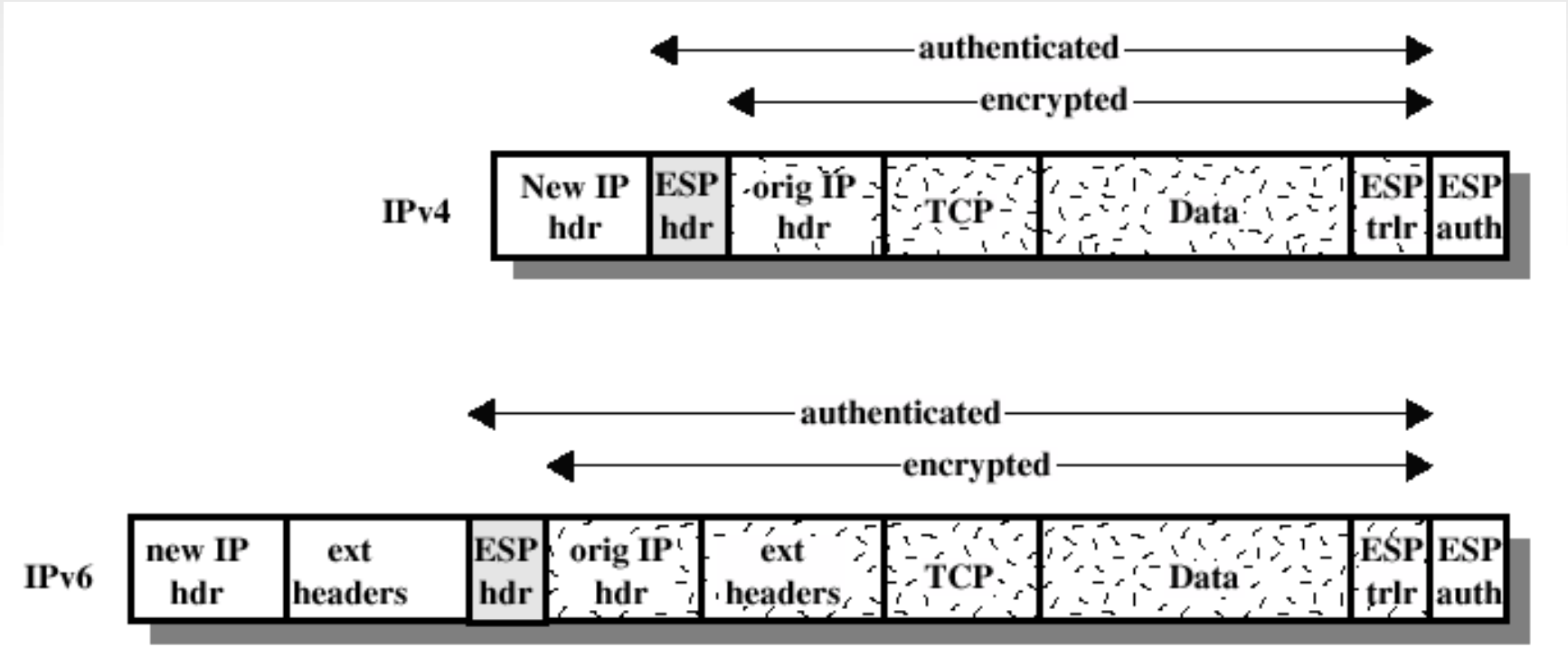
- Encryption:
  - Three-key triple DES
  - RC5
  - IDEA
  - Three-key triple IDEA
  - CAST
  - Blowfish
- Authentication:
  - HMAC-MD5-96
  - HMAC-SHA-1-96

# ESP Encryption and Authentication



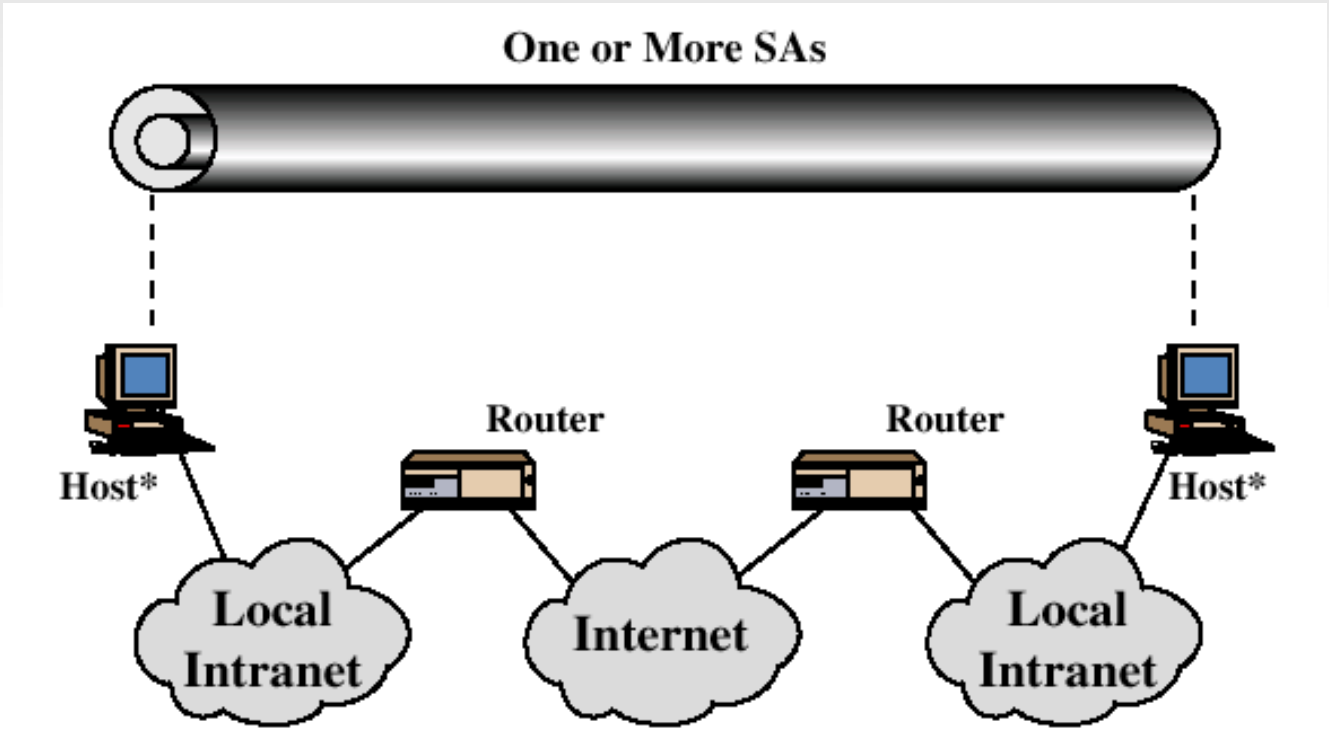

(a) Transport Mode

# ESP Encryption and Authentication



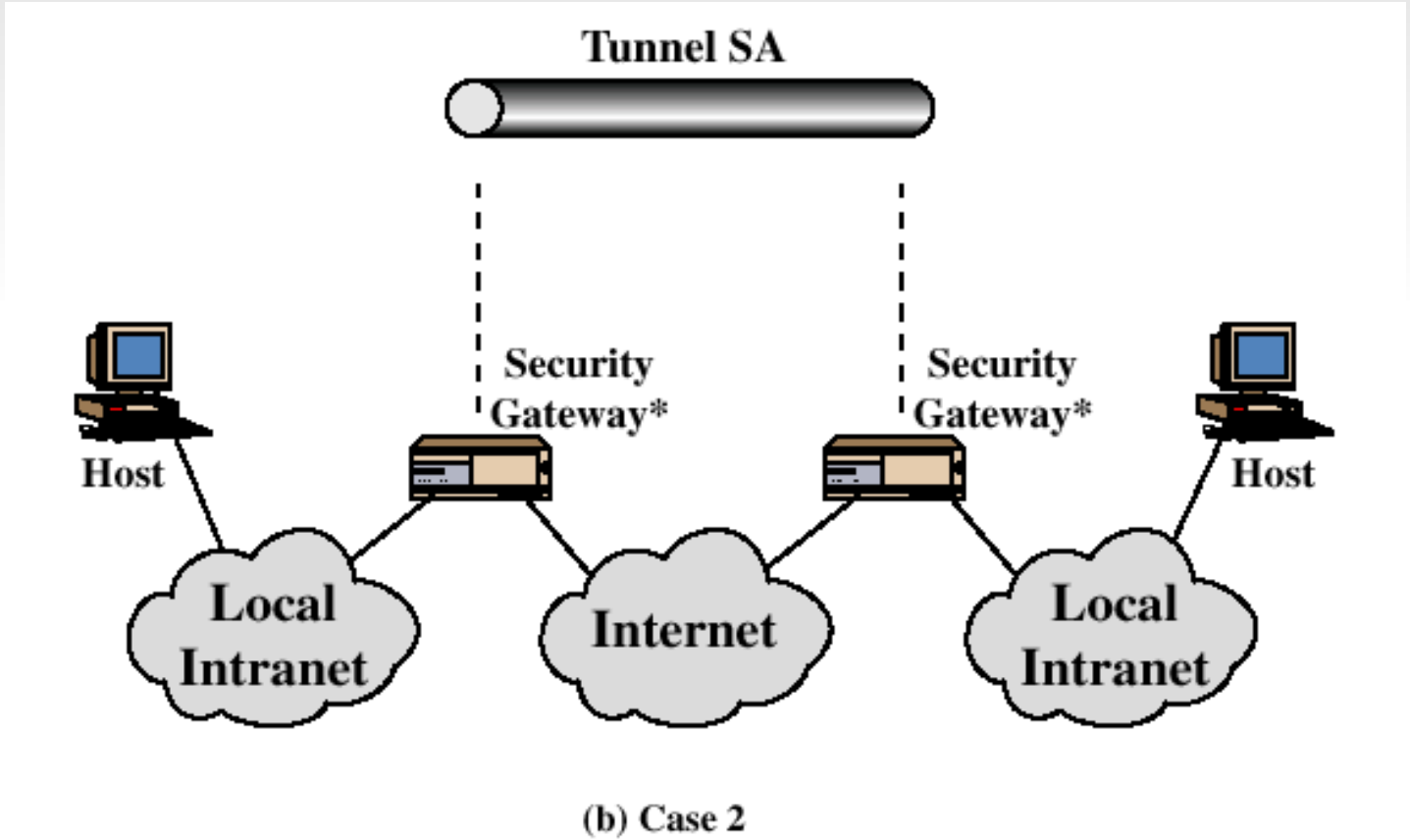

(b) Tunnel Mode

# Combinations of Security Associations



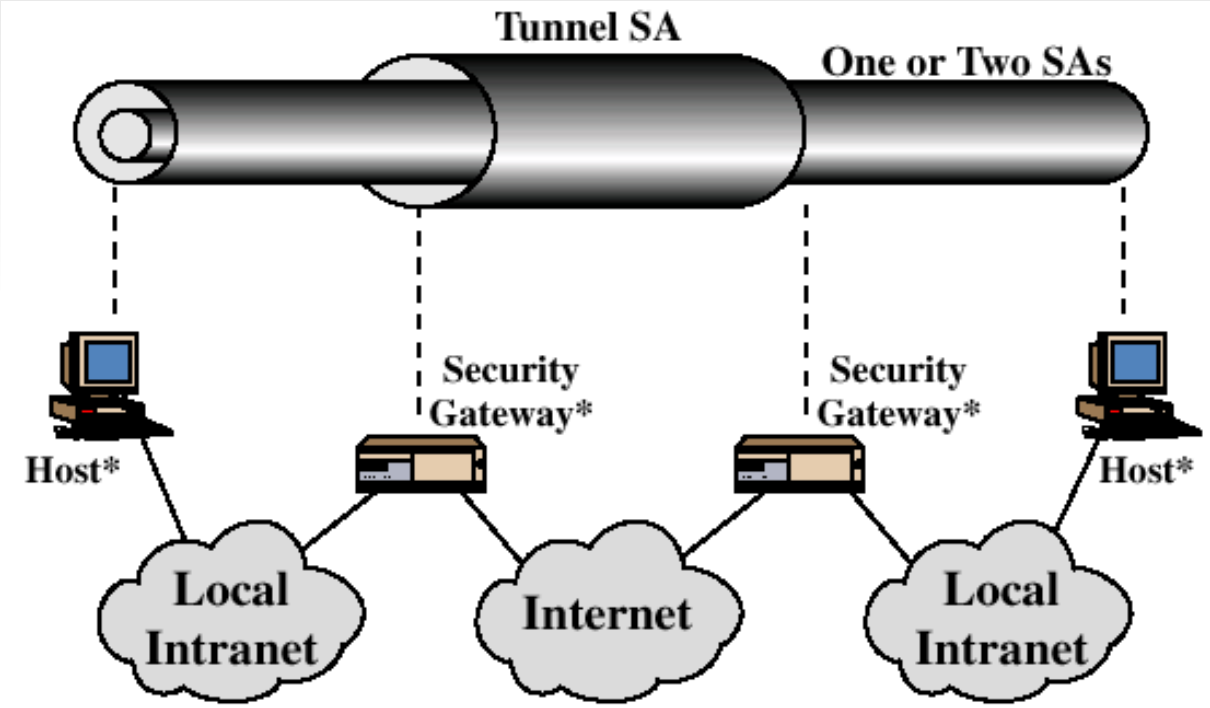

(a) Case 1

# Combinations of Security Associations



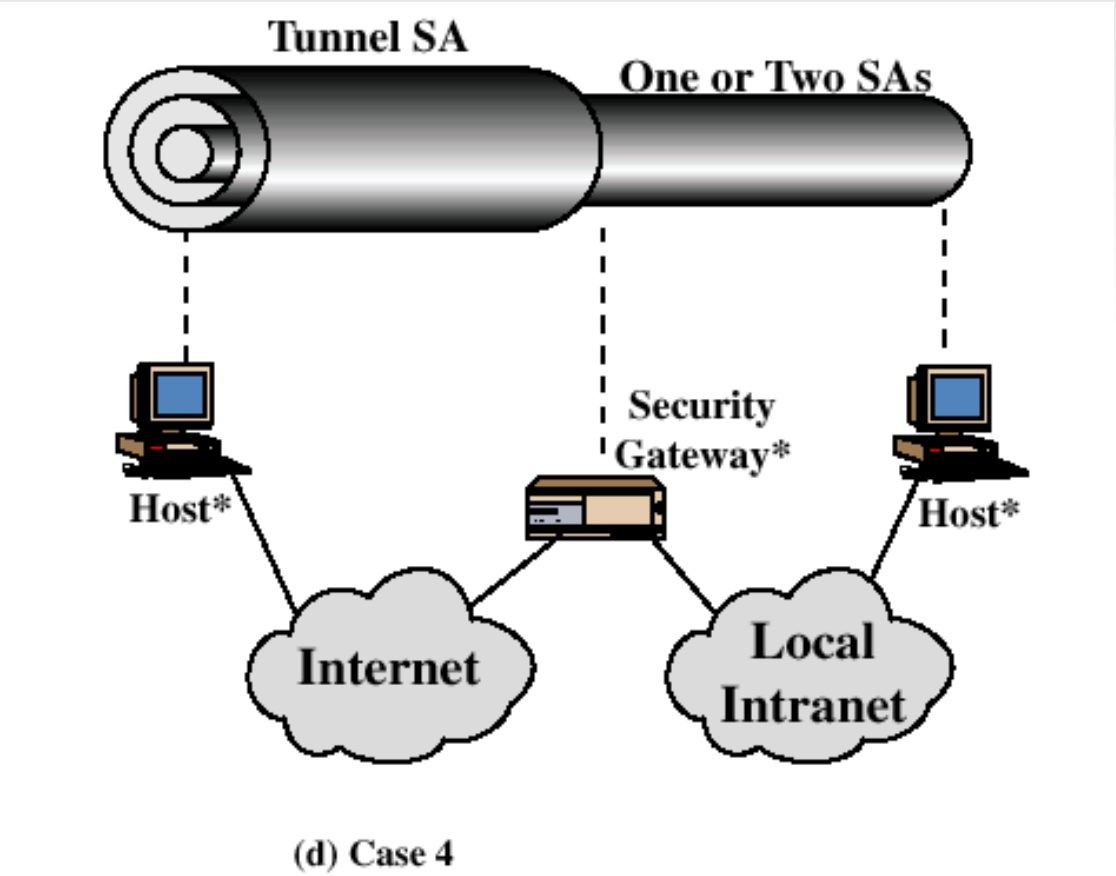

(b) Case 2

# Combinations of Security Associations




(c) Case 3

# Combinations of Security Associations




(d) Case 4

# Key Management

- Two types:
  - Manual
  - Automated
    - Oakley Key Determination Protocol
    - Internet Security Association and Key Management Protocol (ISAKMP)

# Oakley

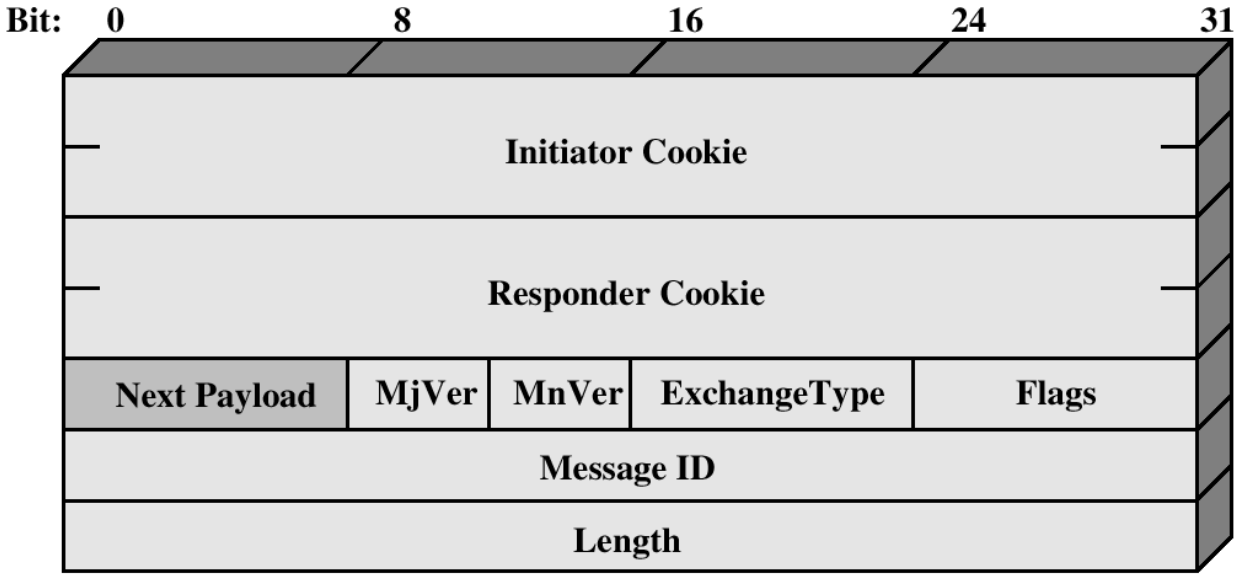
It is refinement of diffie-hellman key exhange protocol.

- Three authentication methods:
  - Digital signatures
  - Public-key encryption
  - Symmetric-key encryption

# ISAKMP

- defines procedures and packet format to establish, negotiate, modify, and delete security associates
- defines payload formats for key generation and exchange

# ISAKMP




(a) ISAKMP Header


(b) Generic Payload Header

Figure 6.12 ISAKMP Formats