

# LAN Technology

---

## Virtual LAN Protocol

*Arash Habibi Lashkari*  
*PHD of Computer Science - Information Security*  
*July 2010*

# *Virtual LAN Protocol*

---

## Outlines:

VLAN: Virtual Local Area Network and the IEEE 802.1Q

IEEE 802.1P: LAN Layer 2 QoS/CoS protocol for Traffic Prioritization

Create a VLAN in Network Lab

PPTP: Point to Point Tunneling Protocol

L2TP: Level 2 Tunneling Protocol

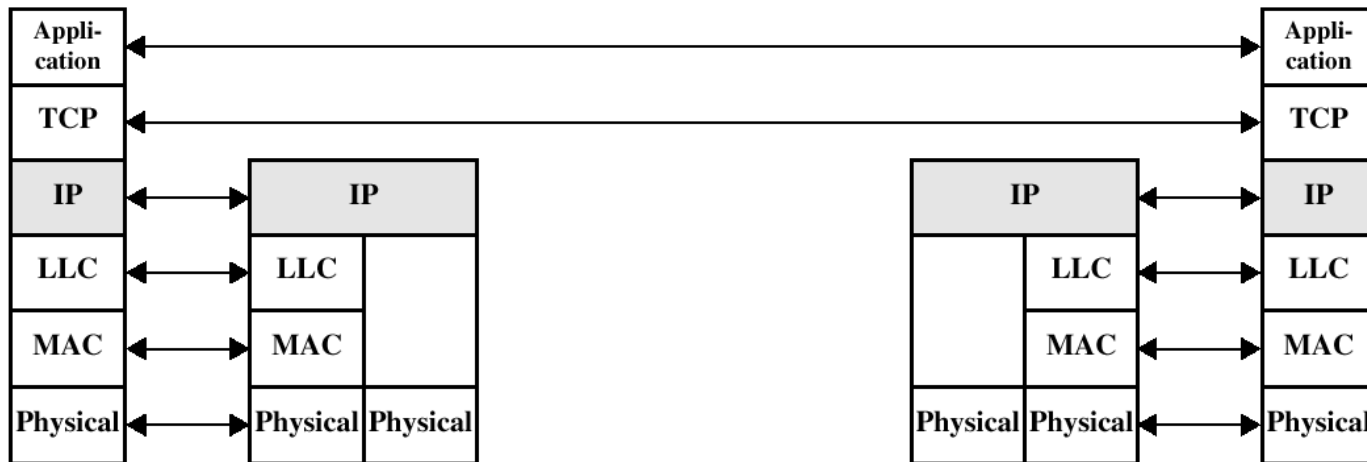
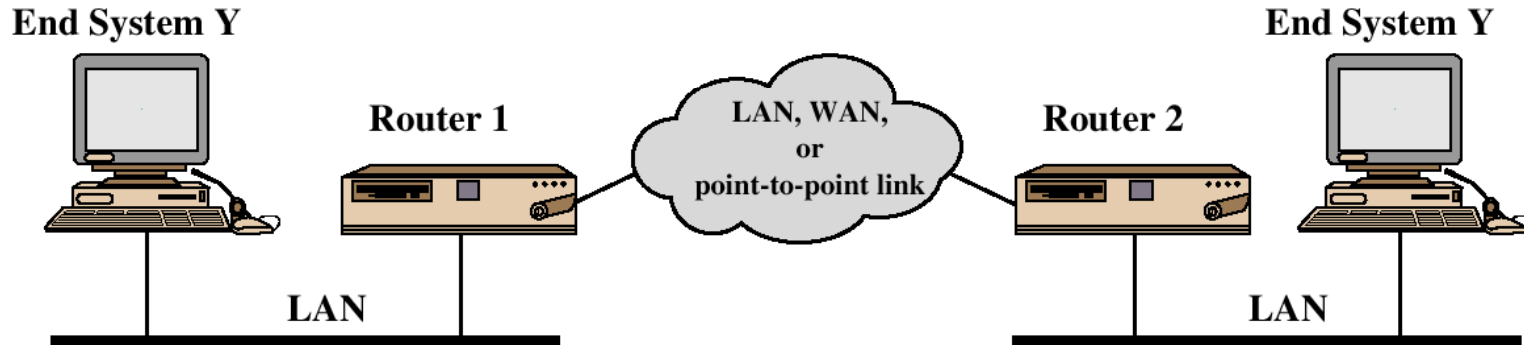
**IPSec: IP Security**

GMRP: GARP Multicast Registration Protocol

GARP: Generic Attribute Registration Protocol

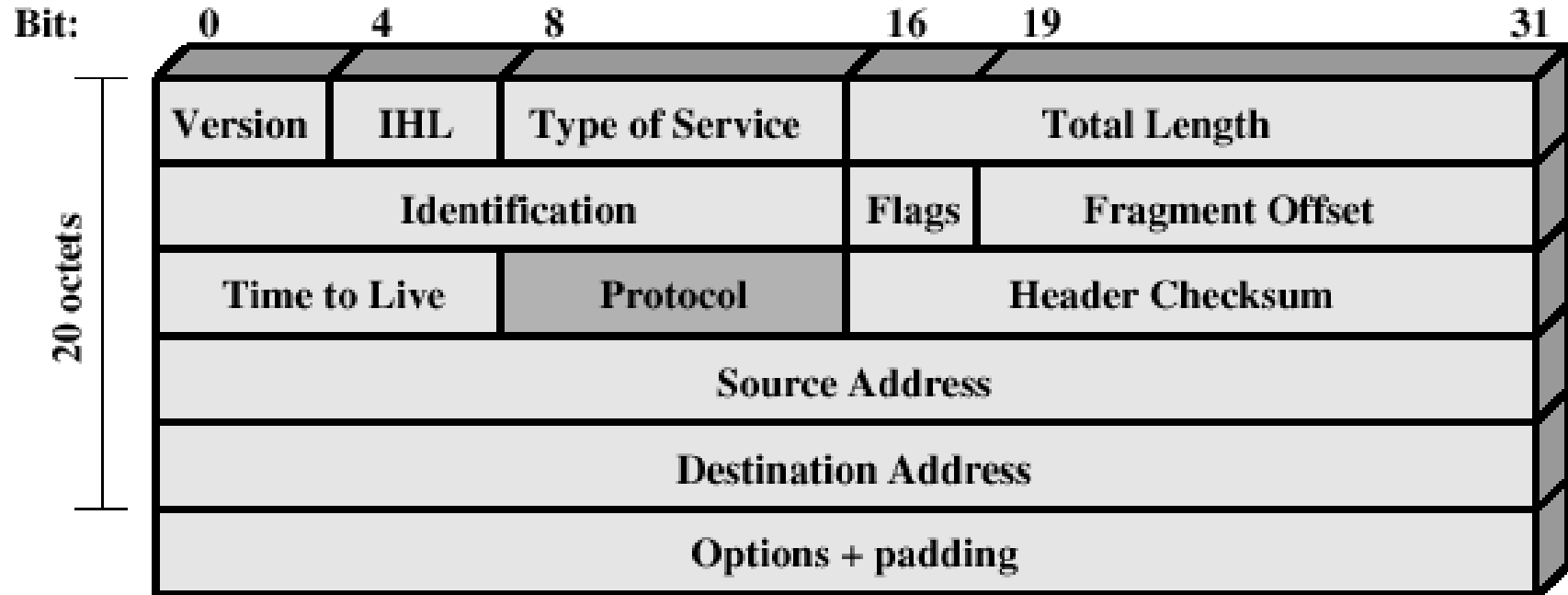
GVRP: CARP VLAN Registration Protocol

# TCP/IP Example



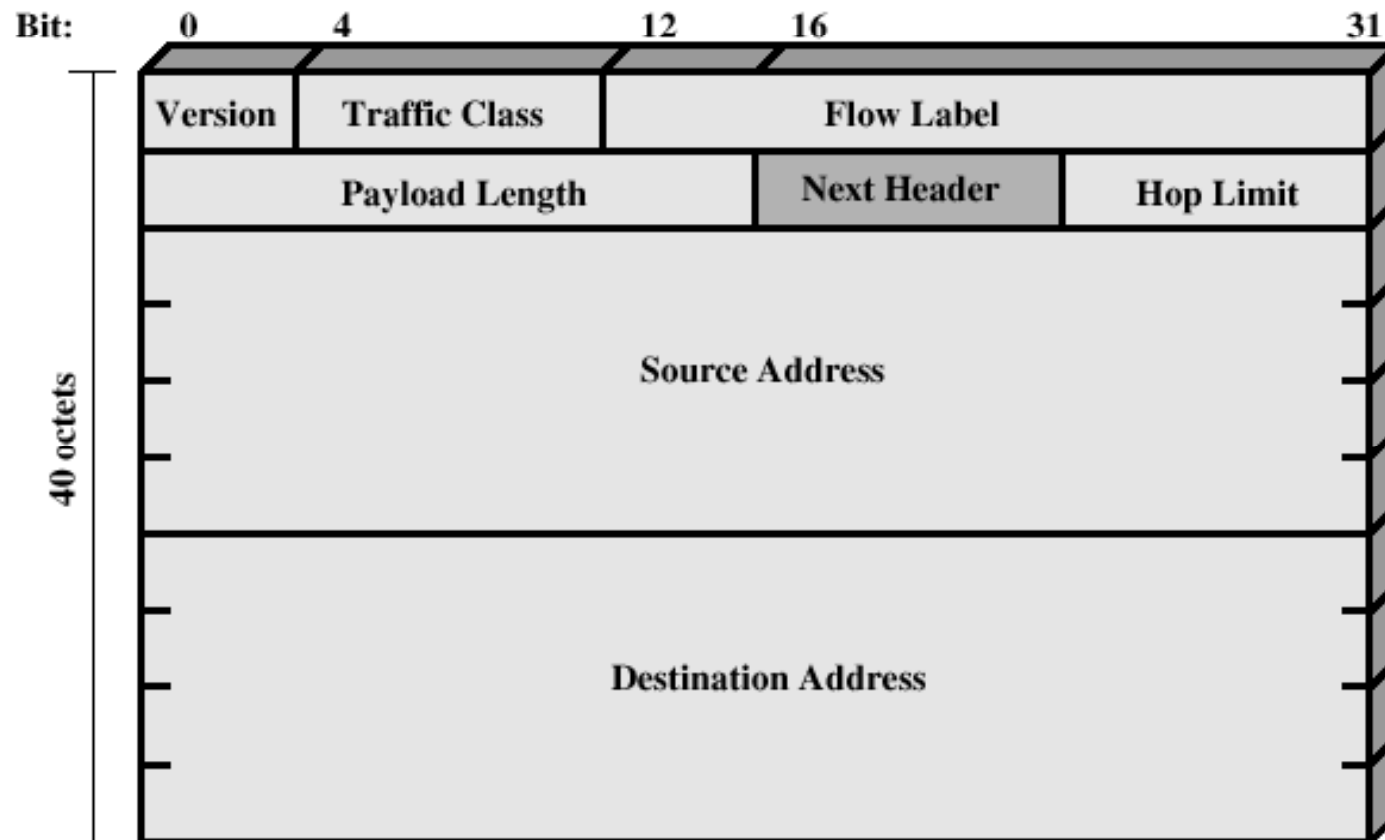
# IPv4 Header

---



# IPv6 Header

---



# *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

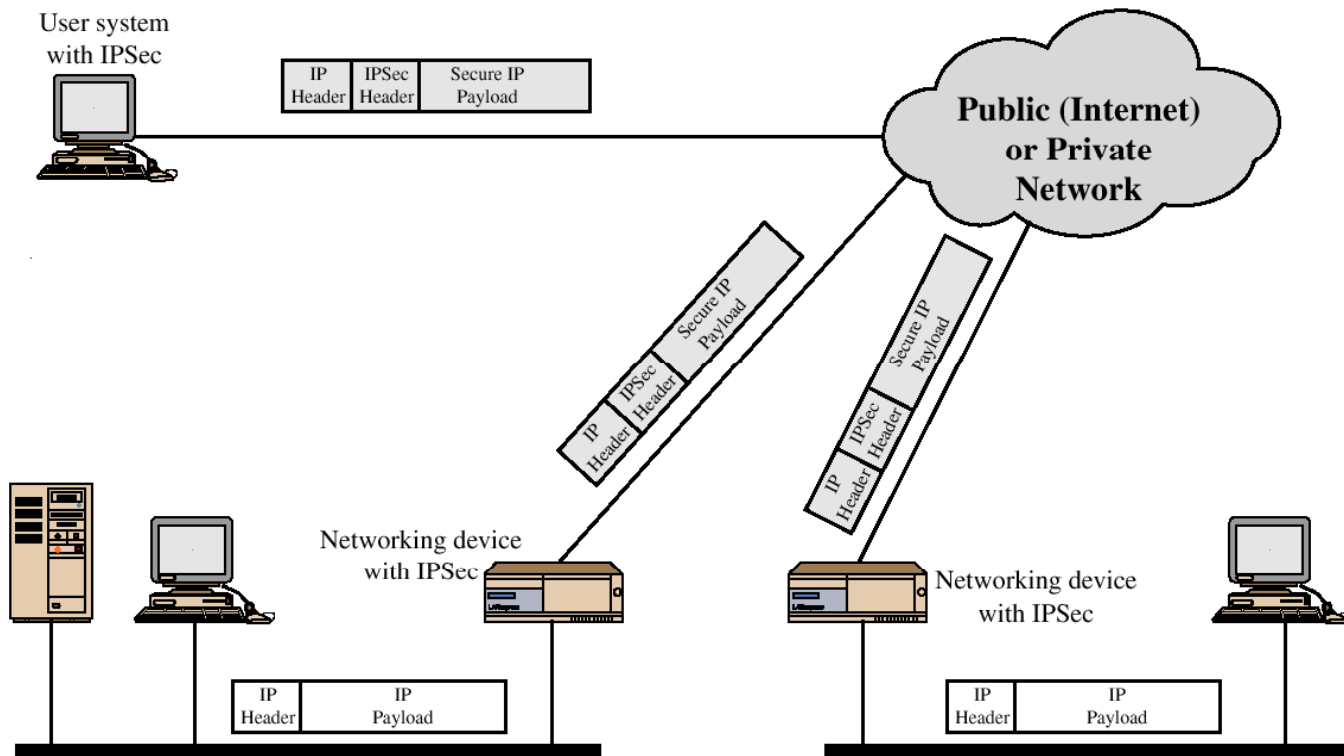
Secure branch office connectivity over the Internet

Secure remote access over the Internet

Establishing extranet and intranet connectivity with partners

Enhancing electronic commerce security

# IP Security Scenario





# *IP Security Overview*

---

## Benefits of IPSec

Transparent to applications (below transport layer (TCP, UDP))

Provide security for individual users

## IPSec can assure that:

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

# *IP Security Architecture*

---

## IPSec documents:

RFC 2401: An overview of security architecture

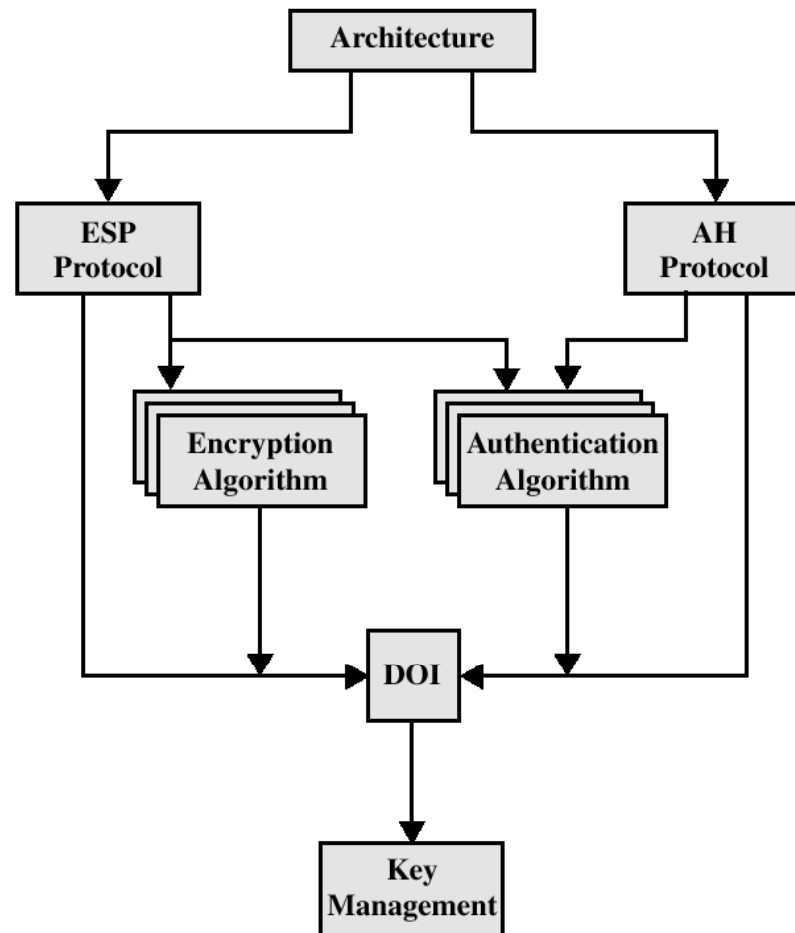
RFC 2402: Description of a packet encryption extension to IPv4 and IPv6

RFC 2406: Description of a packet encryption extension to IPv4 and IPv6

RFC 2408: Specification of key management capabilities

# *IPSec Document Overview*

---



# *IPSec Services*

---

Access Control

Connectionless integrity

Data origin authentication

Rejection of replayed packets

Confidentiality (encryption)

Limited traffic flow confidentiality

# *Security Associations (SA)*

---

A one way relationship between a sender and a receiver.

Identified by three parameters:

- Security Parameter Index (SPI)

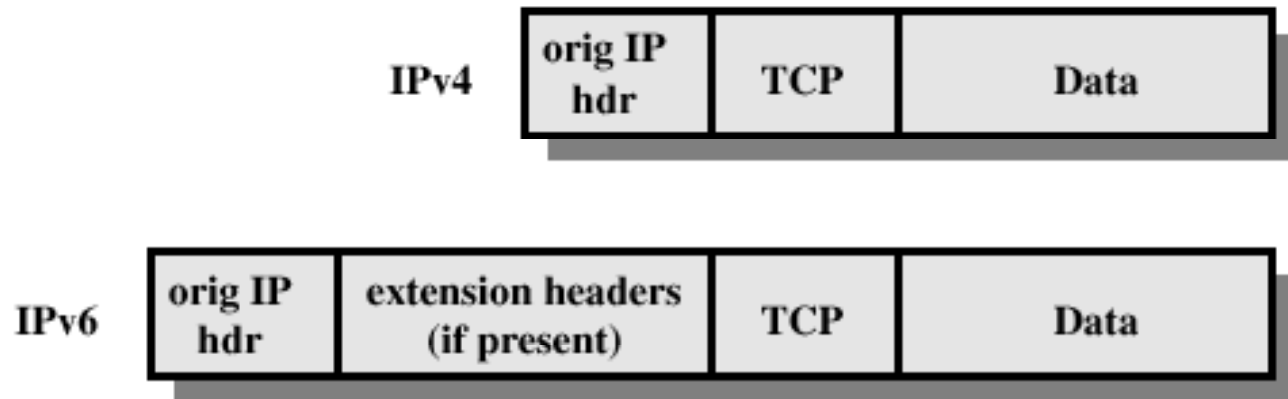
- IP Destination address

- Security Protocol Identifier

	Transport Mode SA	Tunnel Mode SA
AH	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	Encrypts IP payload and any IPv6 extension header	Encrypts inner IP packet
ESP with authentication	Encrypts IP payload and any IPv6 extension header. Authenticates IP payload but no IP header	Encrypts inner IP packet. Authenticates inner IP packet.

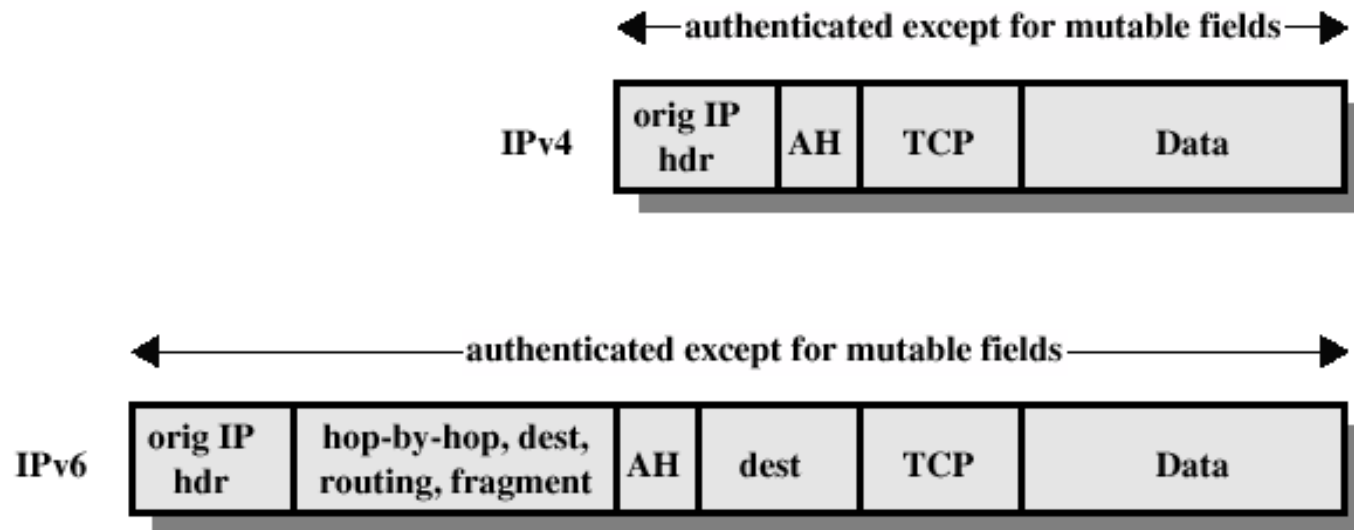
# *Before applying AH*

---



# Transport Mode (AH Authentication)

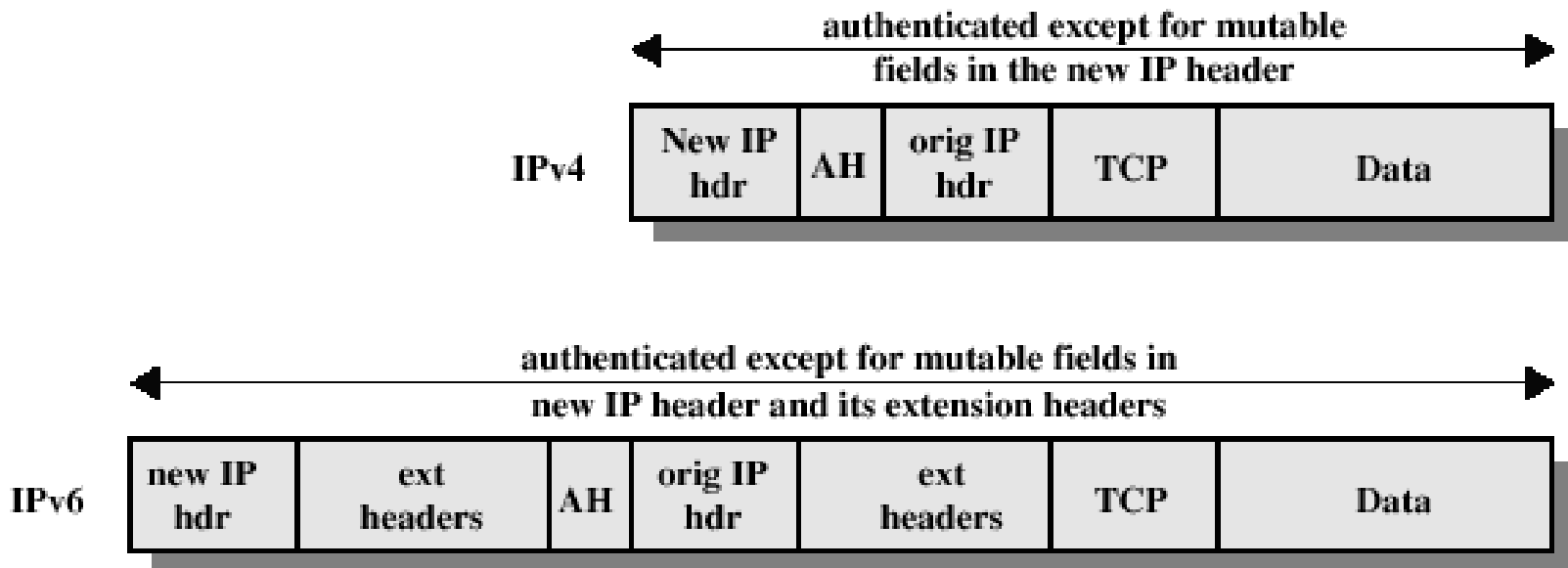
---





# *Tunnel Mode (AH Authentication)*

---

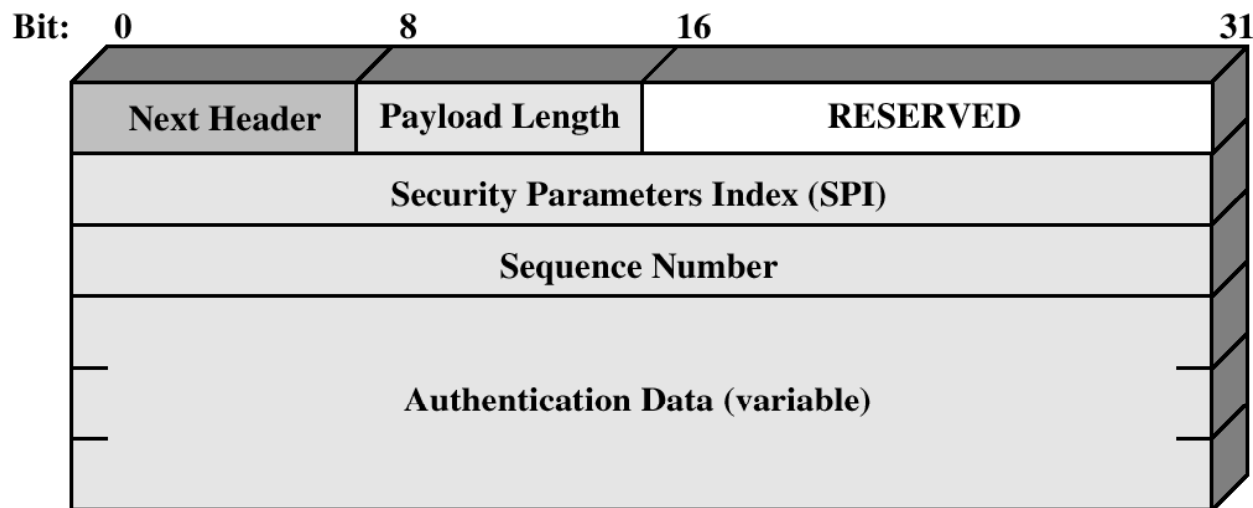


# *Authentication Header*

---

Provides support for data integrity and authentication (MAC code) of IP packets.

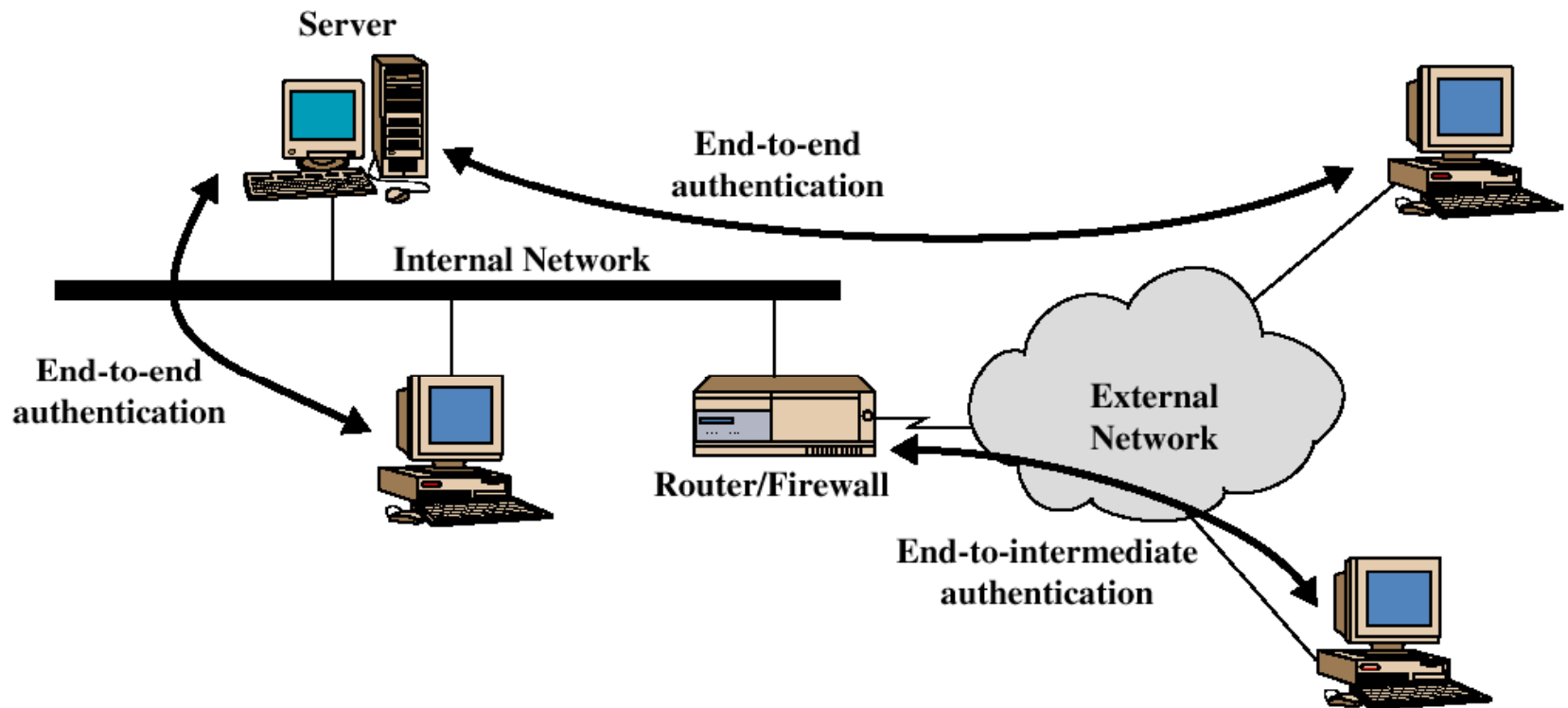
Guards against replay attacks.



**Figure 6.3** IPsec Authentication Header

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

---



# *Encapsulating Security Payload*

---

ESP provides confidentiality services

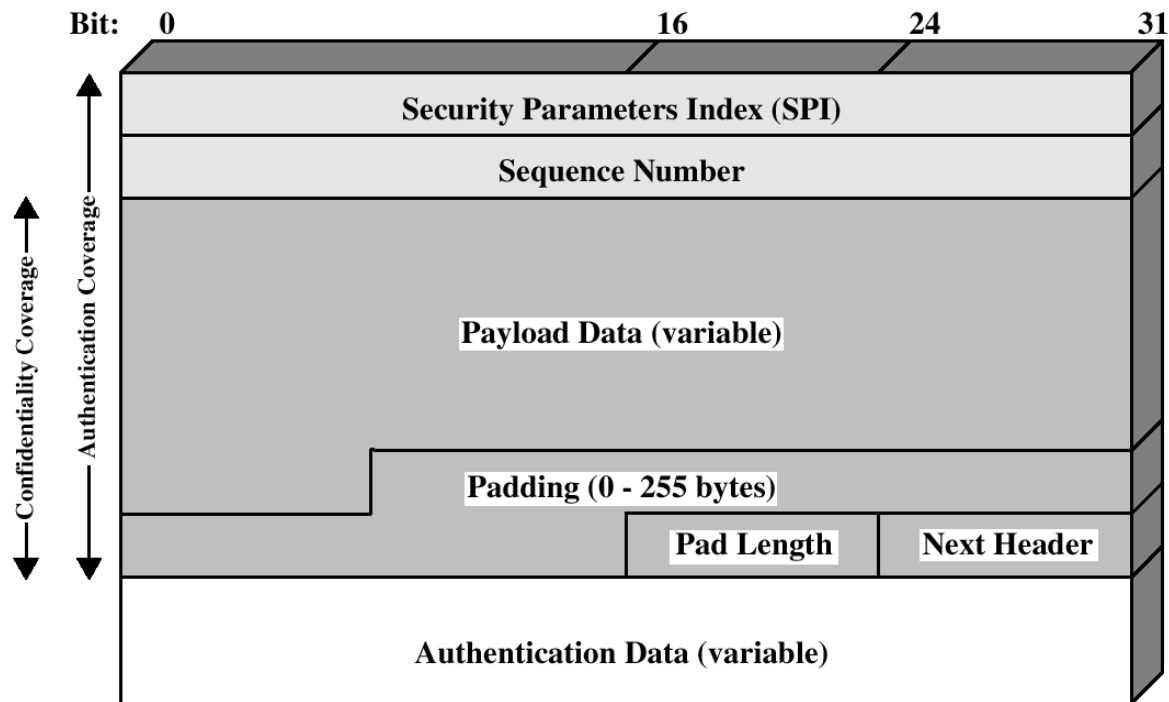


Figure 6.7 IPsec ESP Format

# *Encryption and Authentication Algorithms*

---

## Encryption:

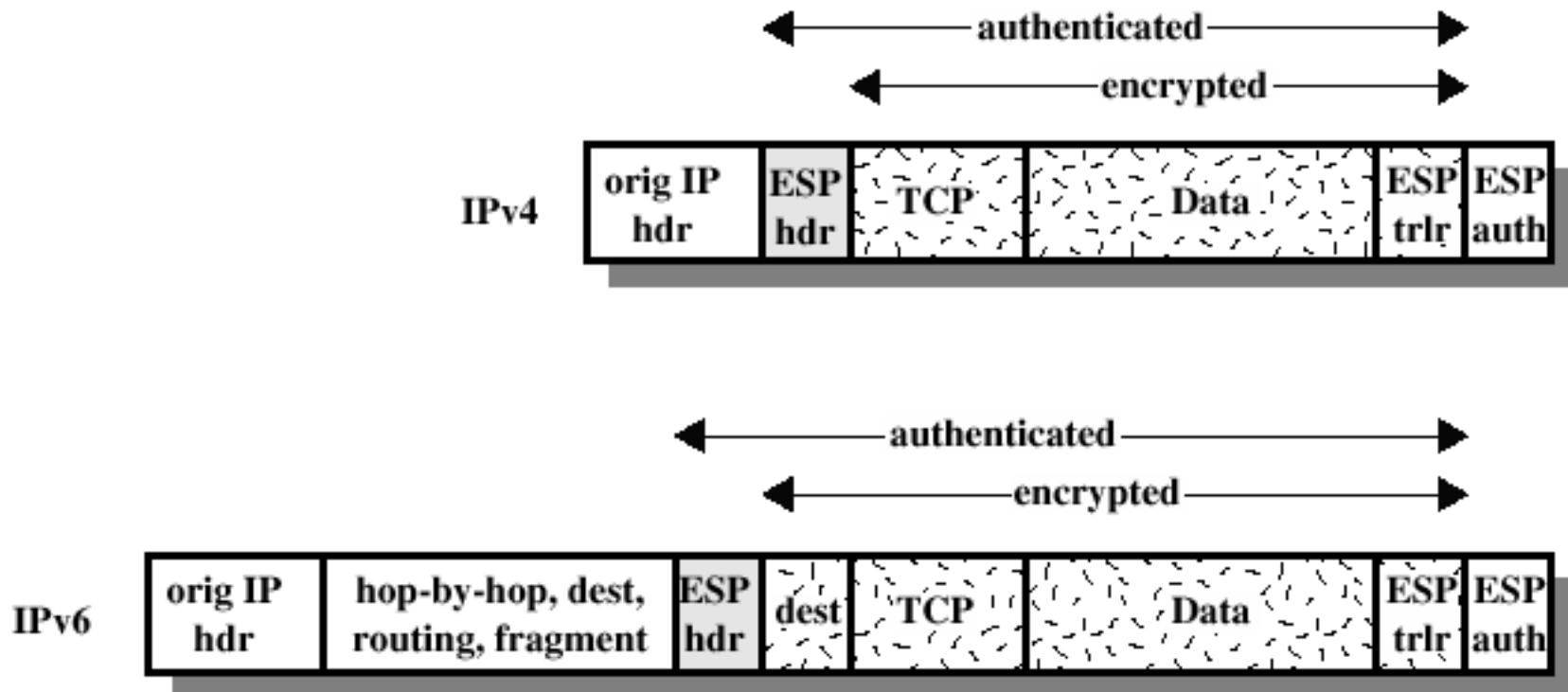
- Three-key triple DES
- RC5
- IDEA
- Three-key triple IDEA
- CAST
- Blowfish

## Authentication:

- HMAC-MD5-96
- HMAC-SHA-1-96

# ESP Encryption and Authentication

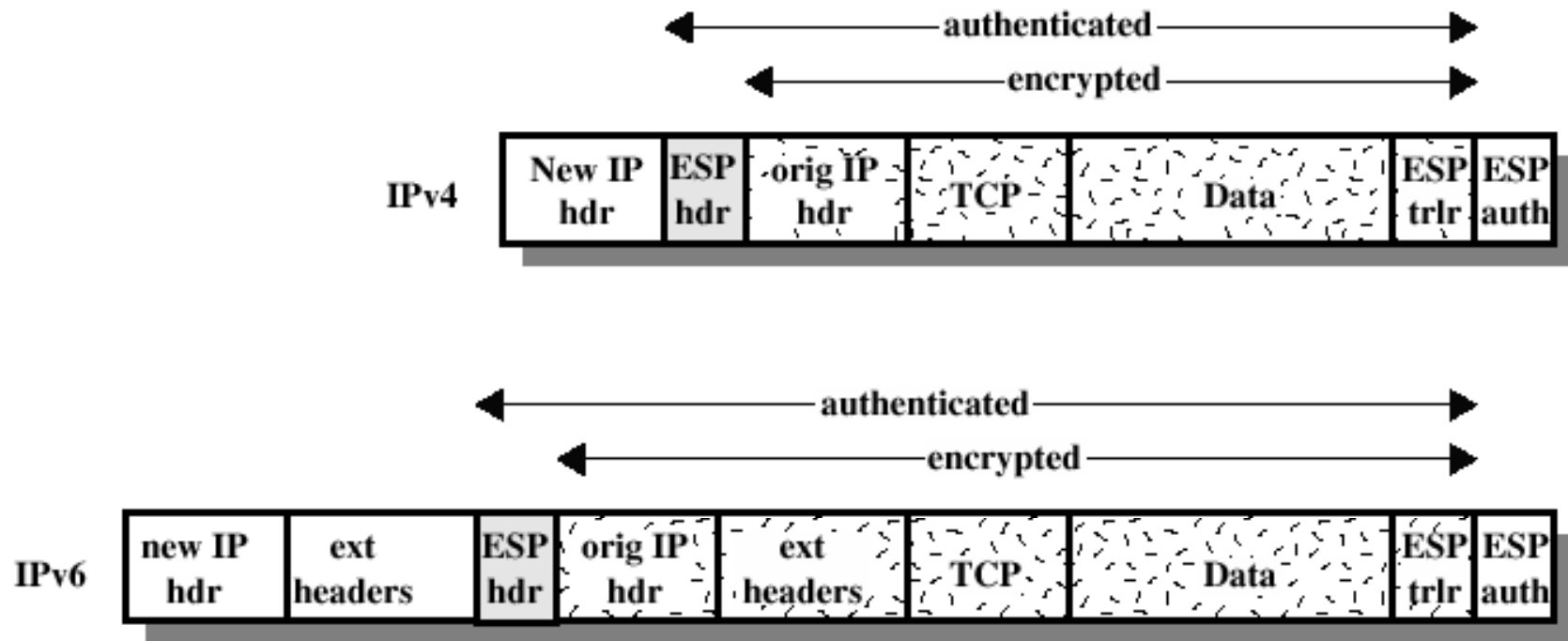
---



(a) Transport Mode

# ESP Encryption and Authentication

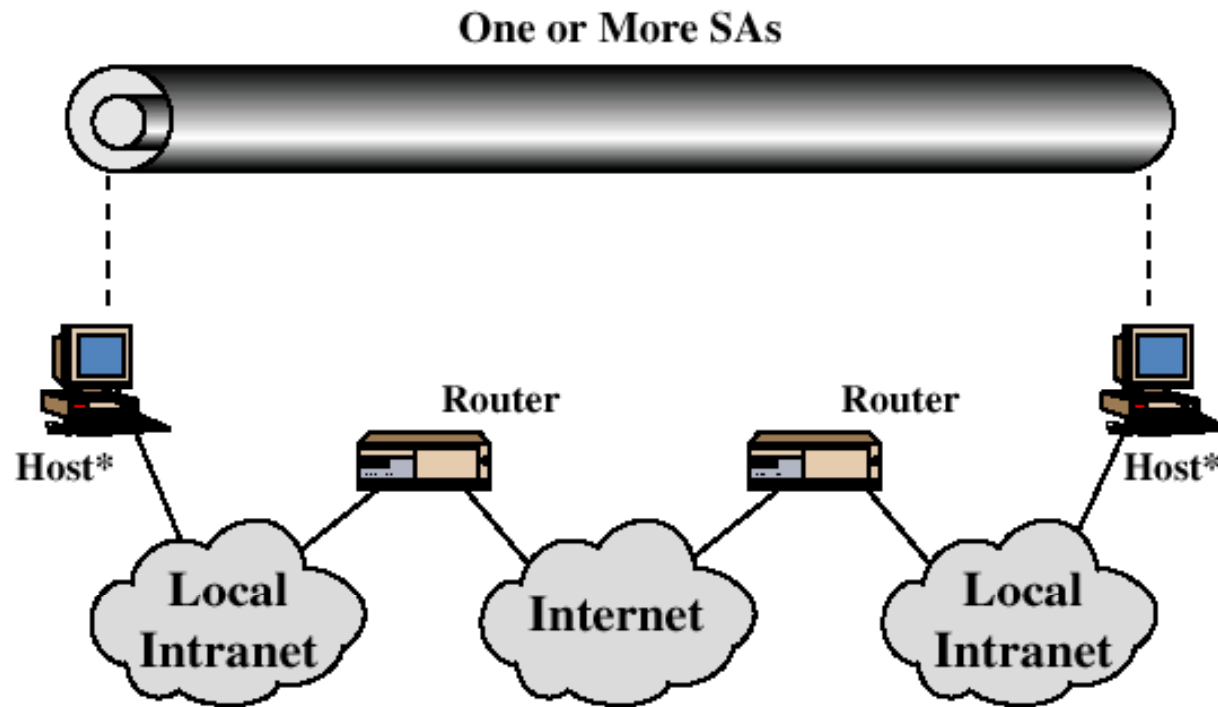
---



(b) Tunnel Mode

# Combinations of Security Associations

---

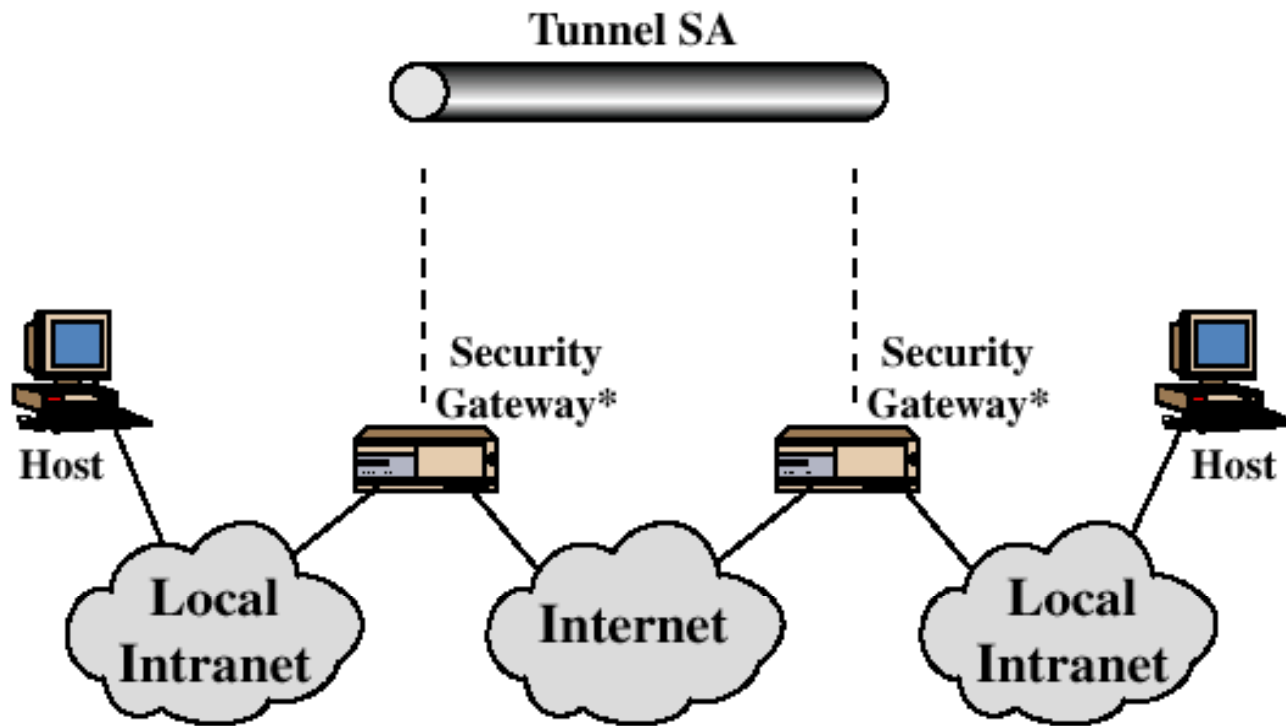


(a) Case 1



# Combinations of Security Associations

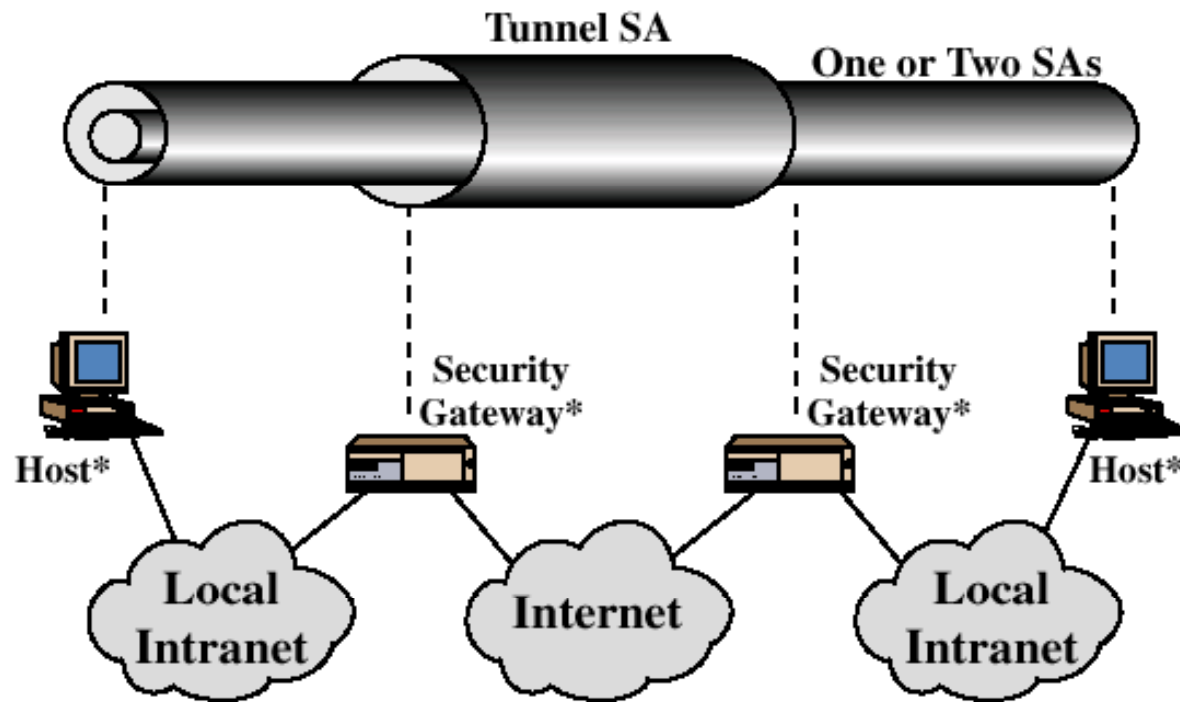
---



(b) Case 2

# Combinations of Security Associations

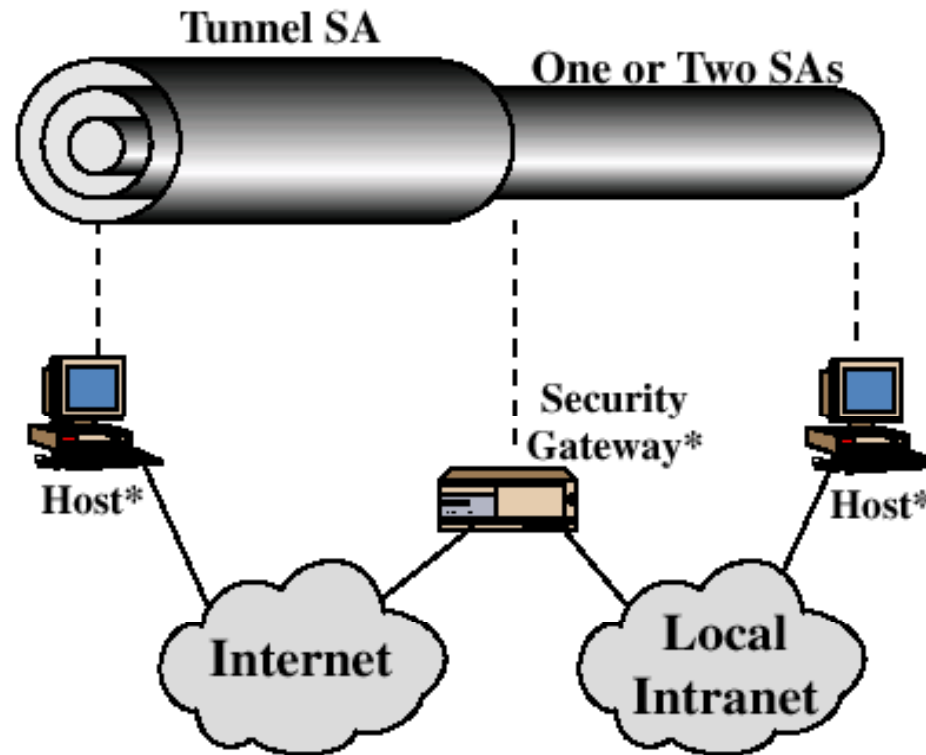
---



(c) Case 3

# Combinations of Security Associations

---



(d) Case 4

# *Questions*

---

