Chapter 6

IP Security

Henric Johnson

Blekinge Institute of Technology, Sweden

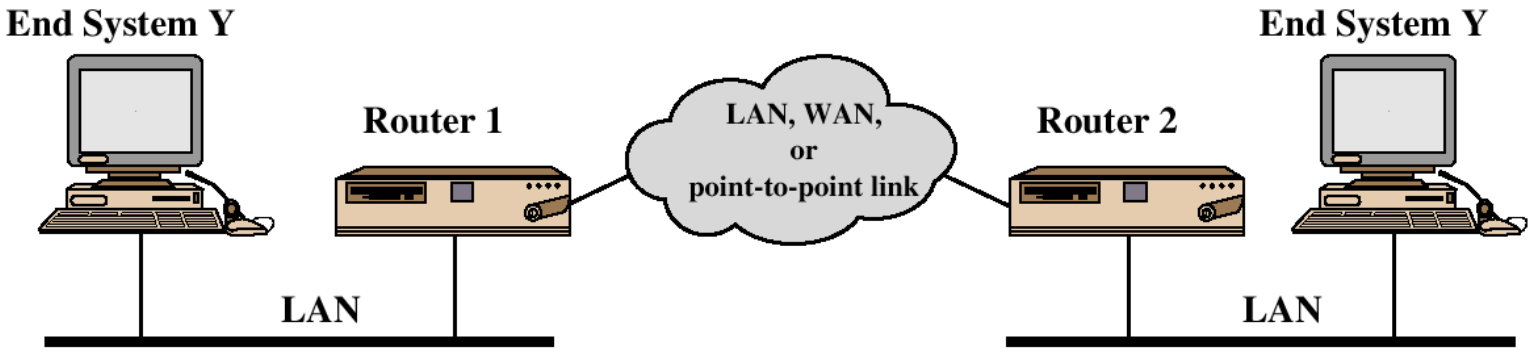
http://www.its.bth.se/staff/hjo/

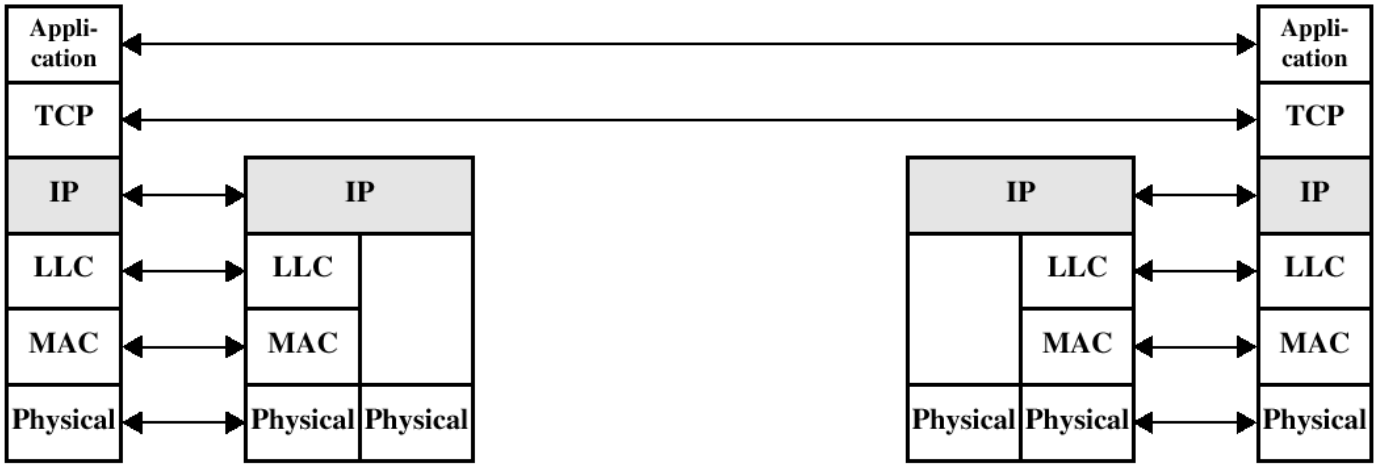
henric.johnson@bth.se

Outline

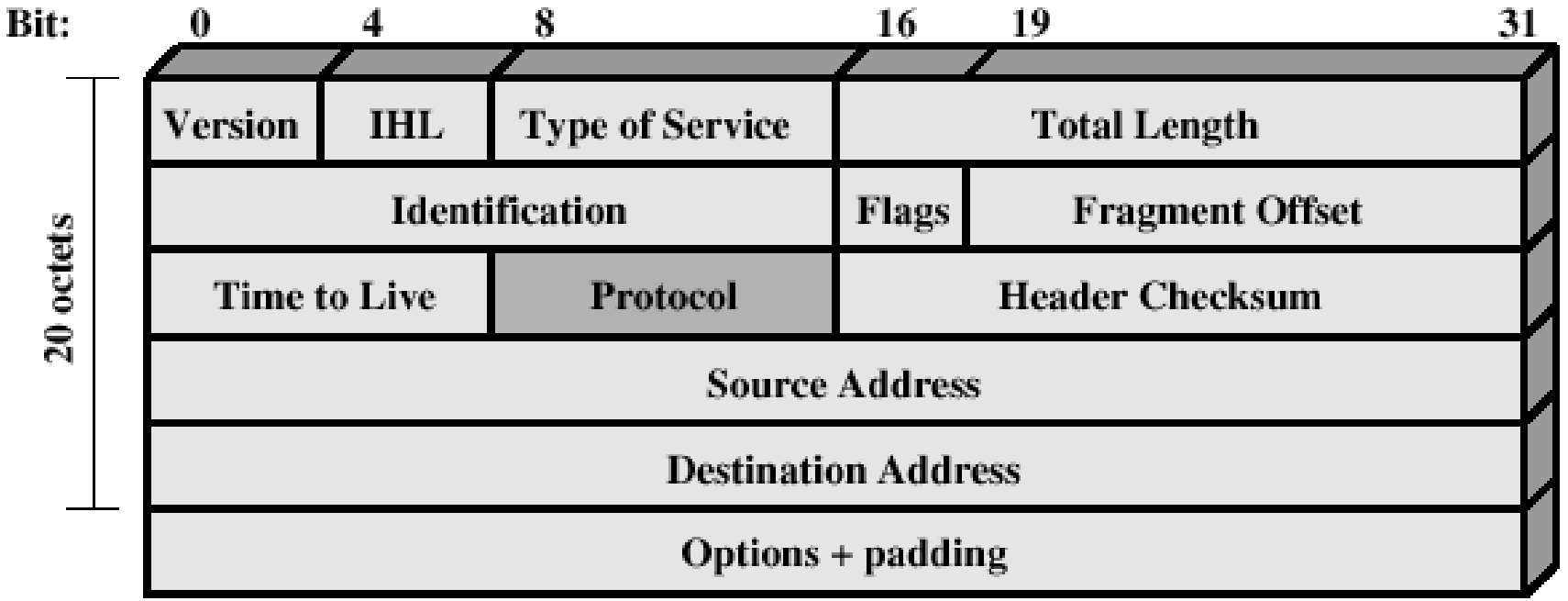
- Internetworking and Internet Protocols (Appendix 6A)
- IP Security Overview
- IP Security Architecture
- Authentication Header
- Encapsulating Security Payload
- Combinations of Security Associations
- Key Management

TCP/IP Example

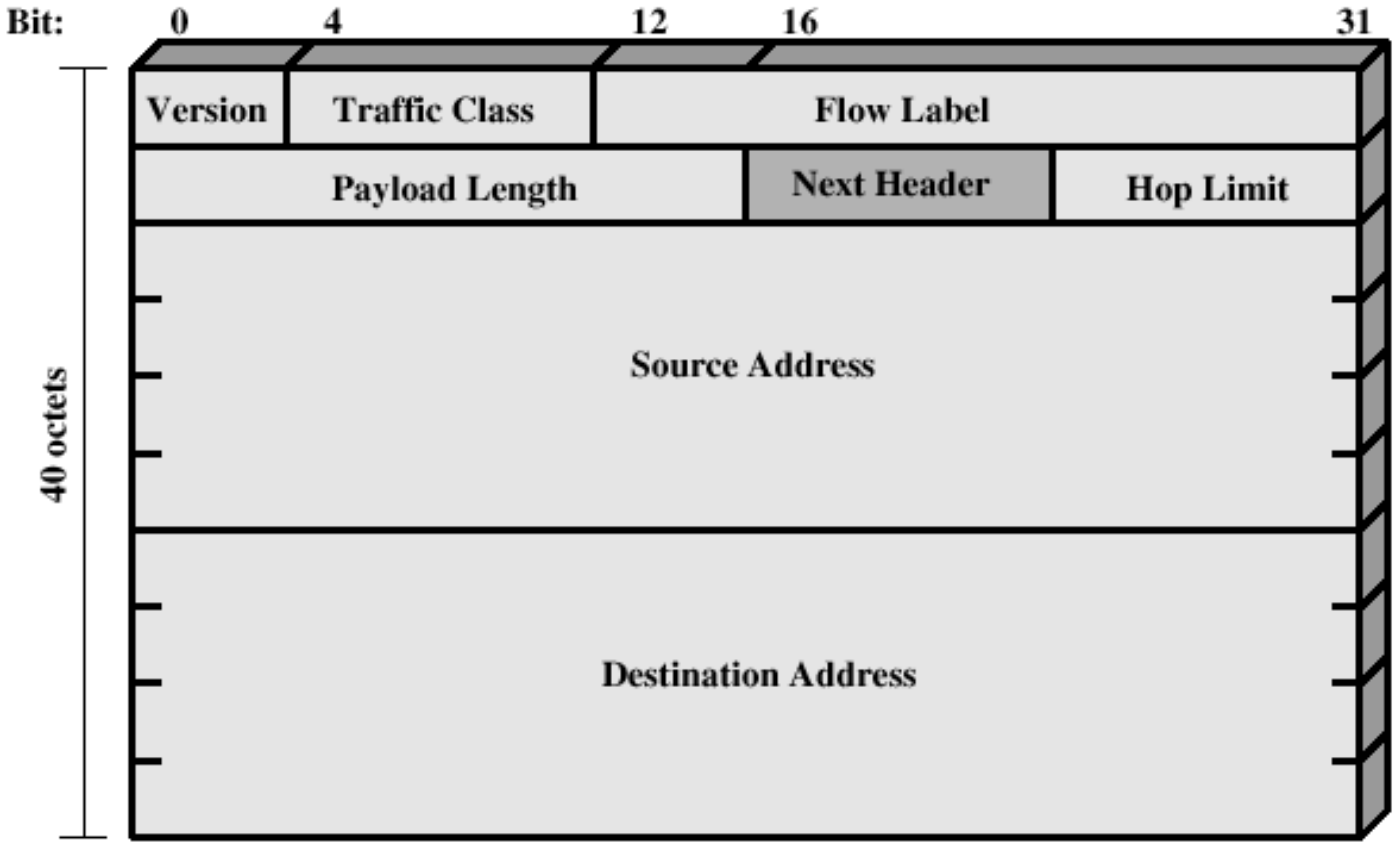




IPv4 Header


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
Version
Traffic Class
Flow Label
Payload Length
Next Header
Hop Limit
Source Address
Destination Address
40 octets

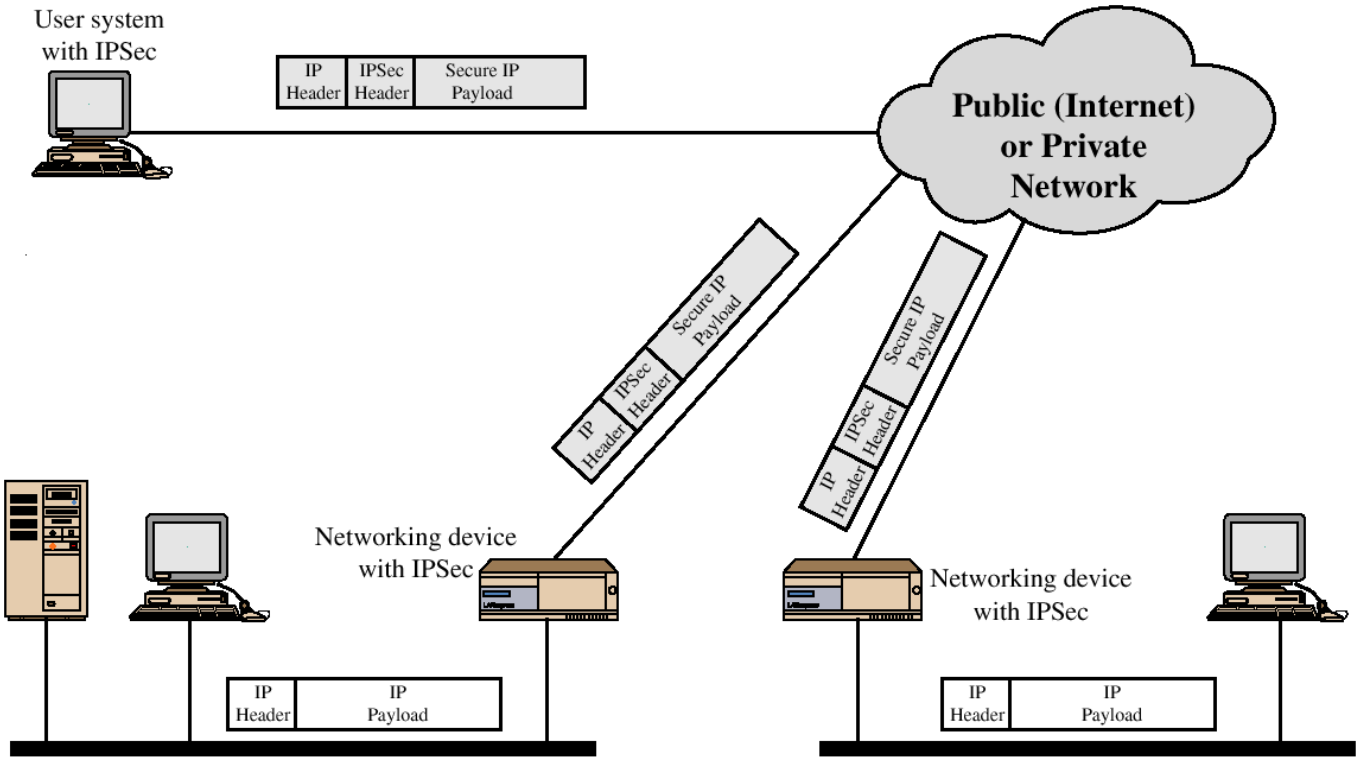
IP Security Overview

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



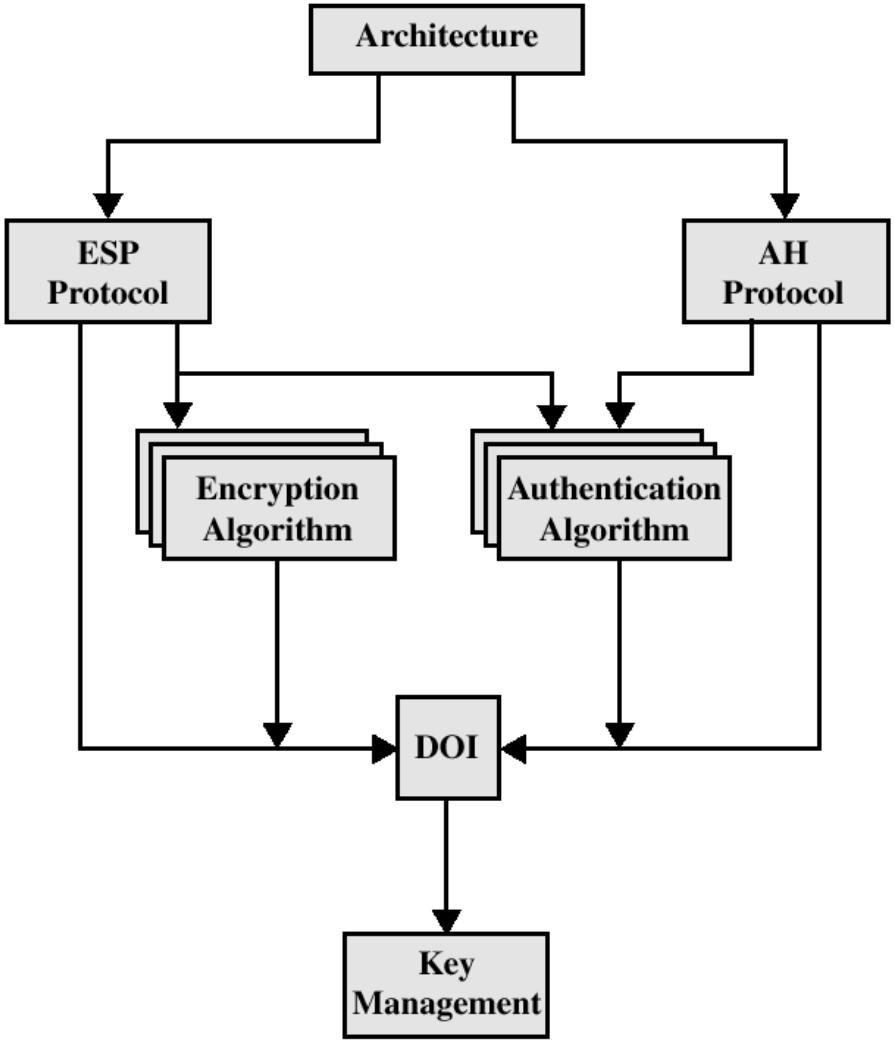
IP Security Overview

- Benefits of IPSec
  - 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 emcryption extension to IPv4 and IPv6
  - RFC 2408: Specification of key managament capabilities

IPSec Document Overview



IPSec Services

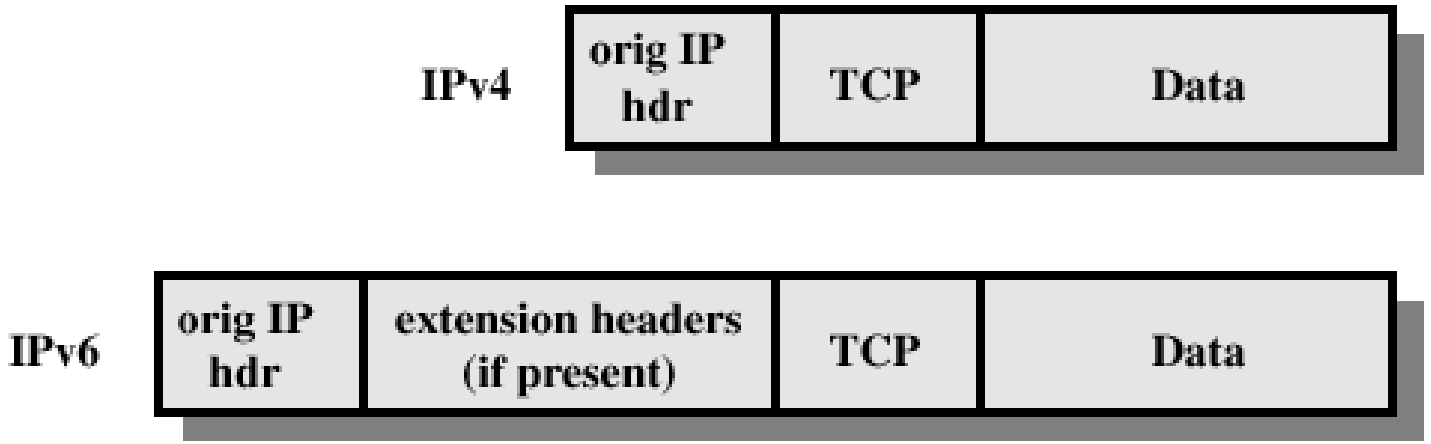
- Access Control
- Connectionless integrity
- Data origin authentication
- Rejection of replayed packets
- Confidentiality (encryption)
- Limited traffic flow confidentiallity

Security Associations (SA)

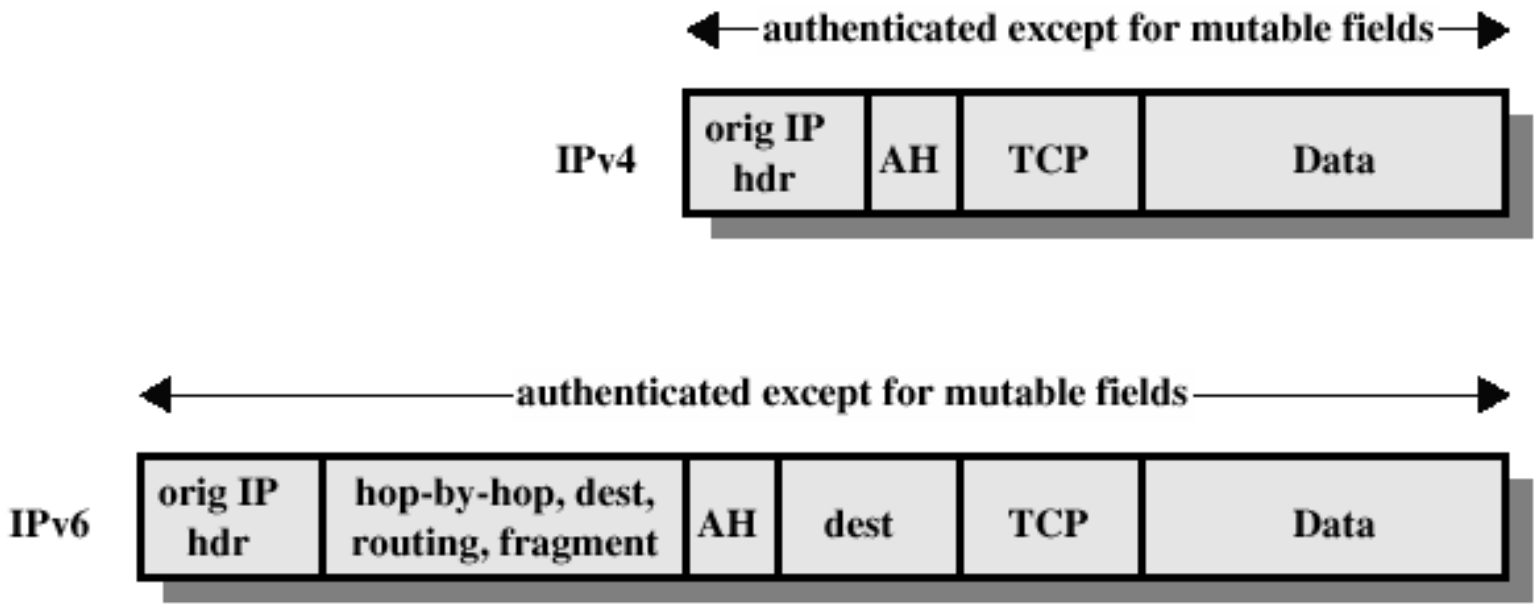
- A one way relationsship between a sender and a receiver.
- Identified by three parameters:
  - Security Parameter Index (SPI)
  - IP Destination address
  - Security Protocol Identifier

	Transport Mode SA	Tunnel Mode SA
AH	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 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.

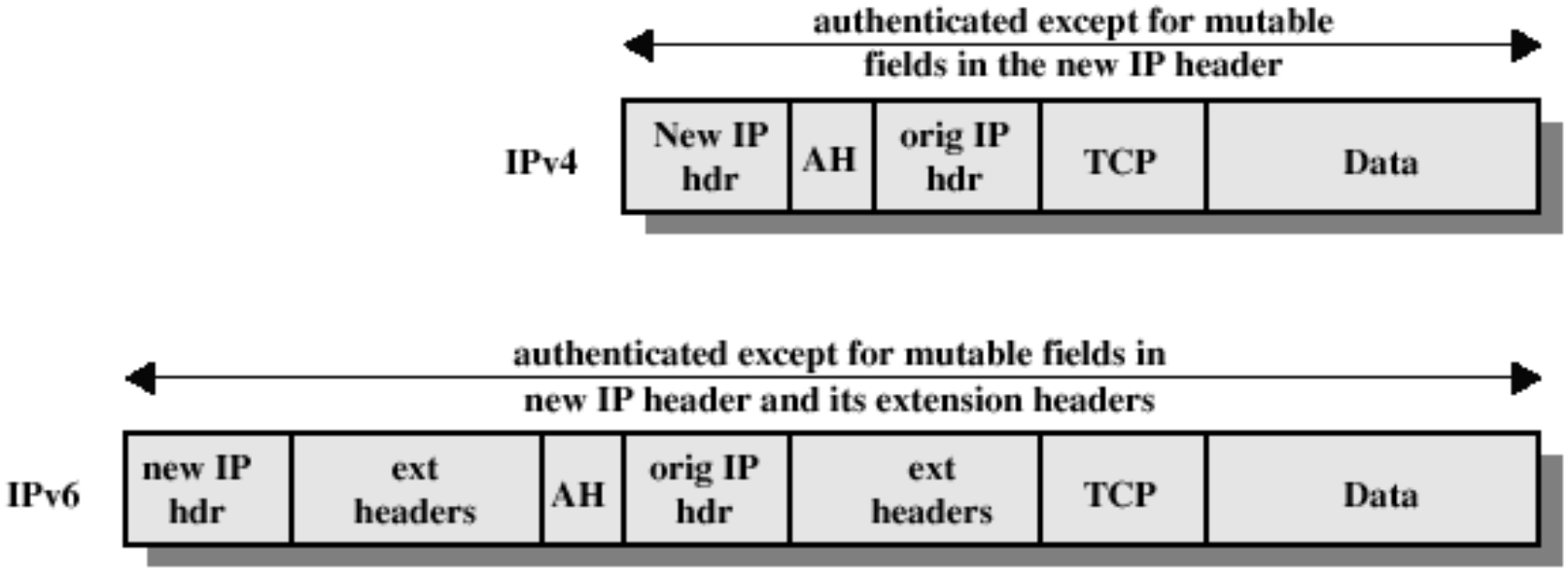
Before applying AH



Transport Mode (AH Authentication)



Tunnel Mode (AH Authentication)



Authentication Header

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

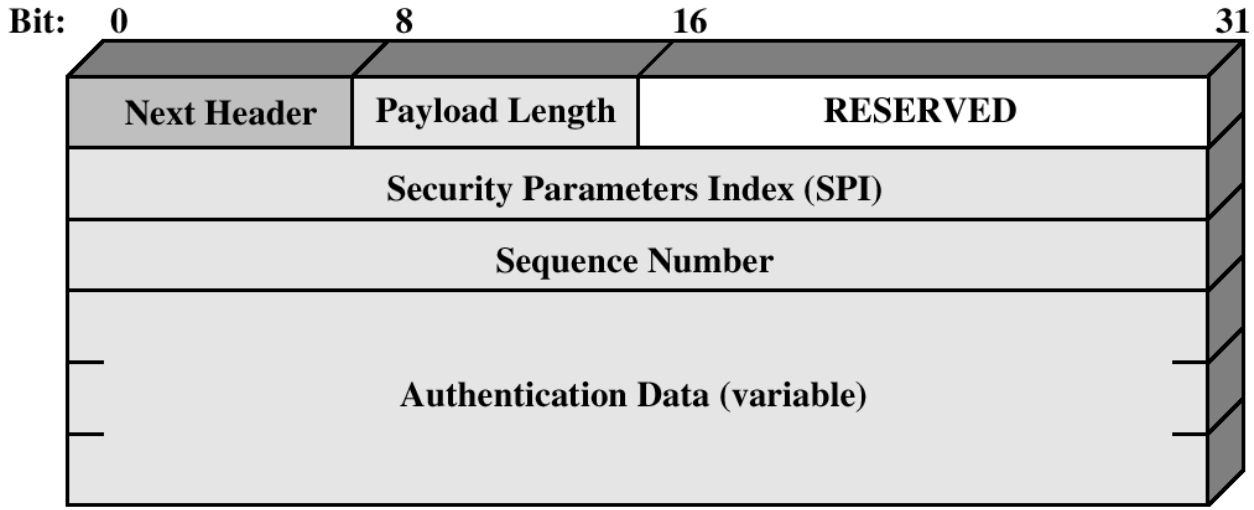
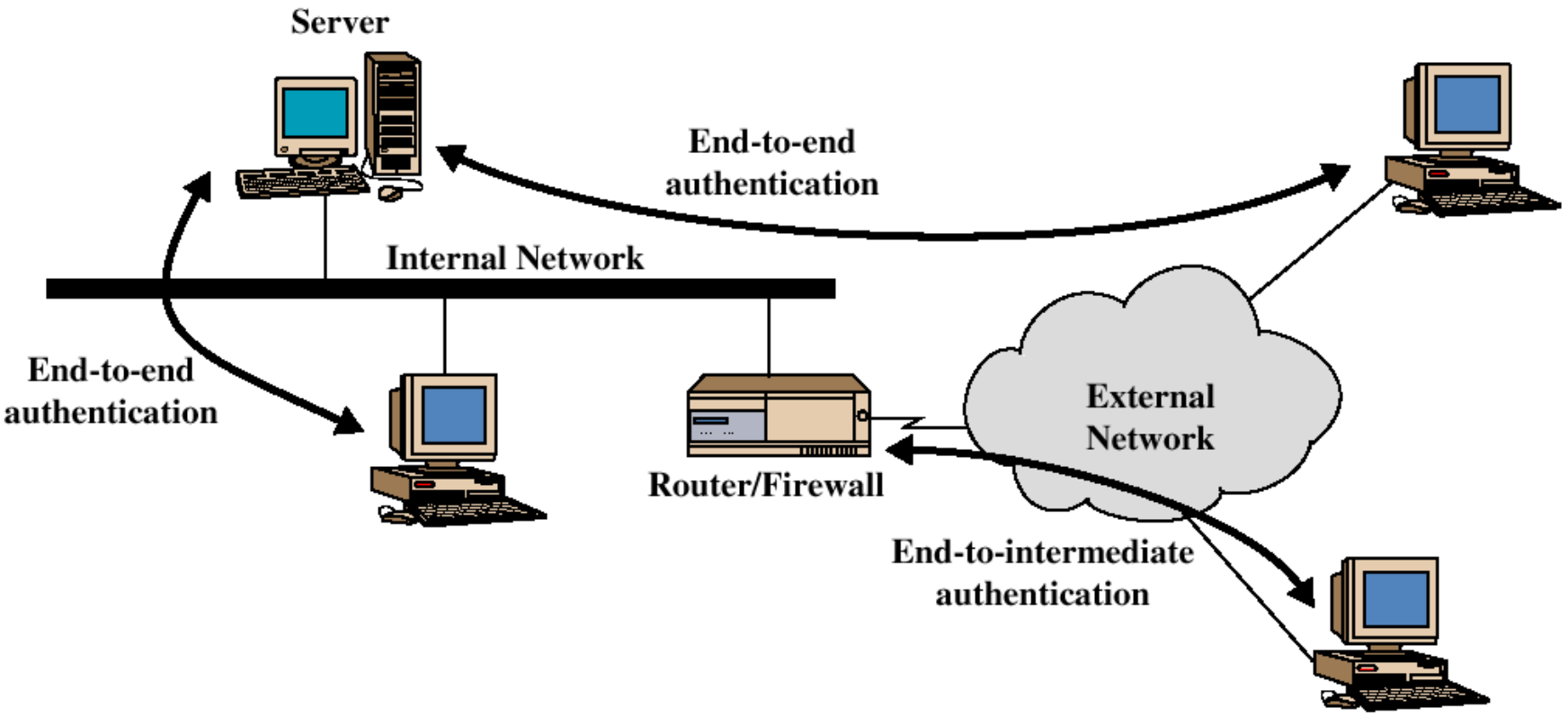


Figure 6.3 IPSec Authentication Header

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



Encapsulating Security Payload

- ESP provides confidentiality services

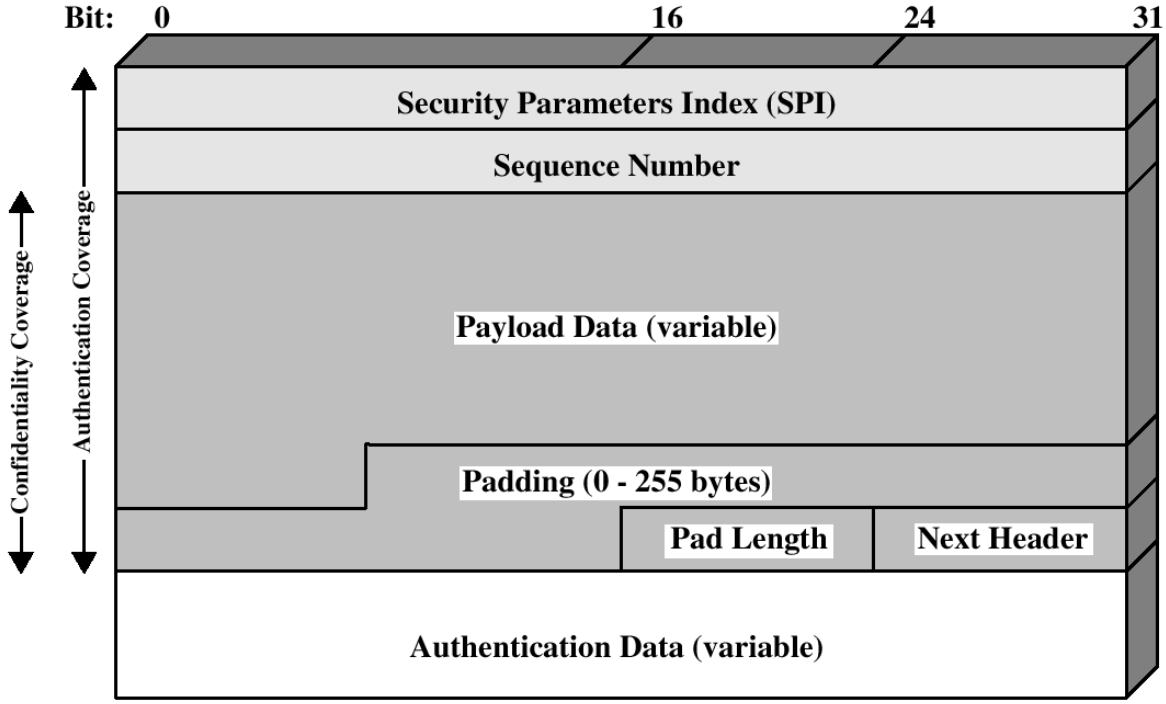
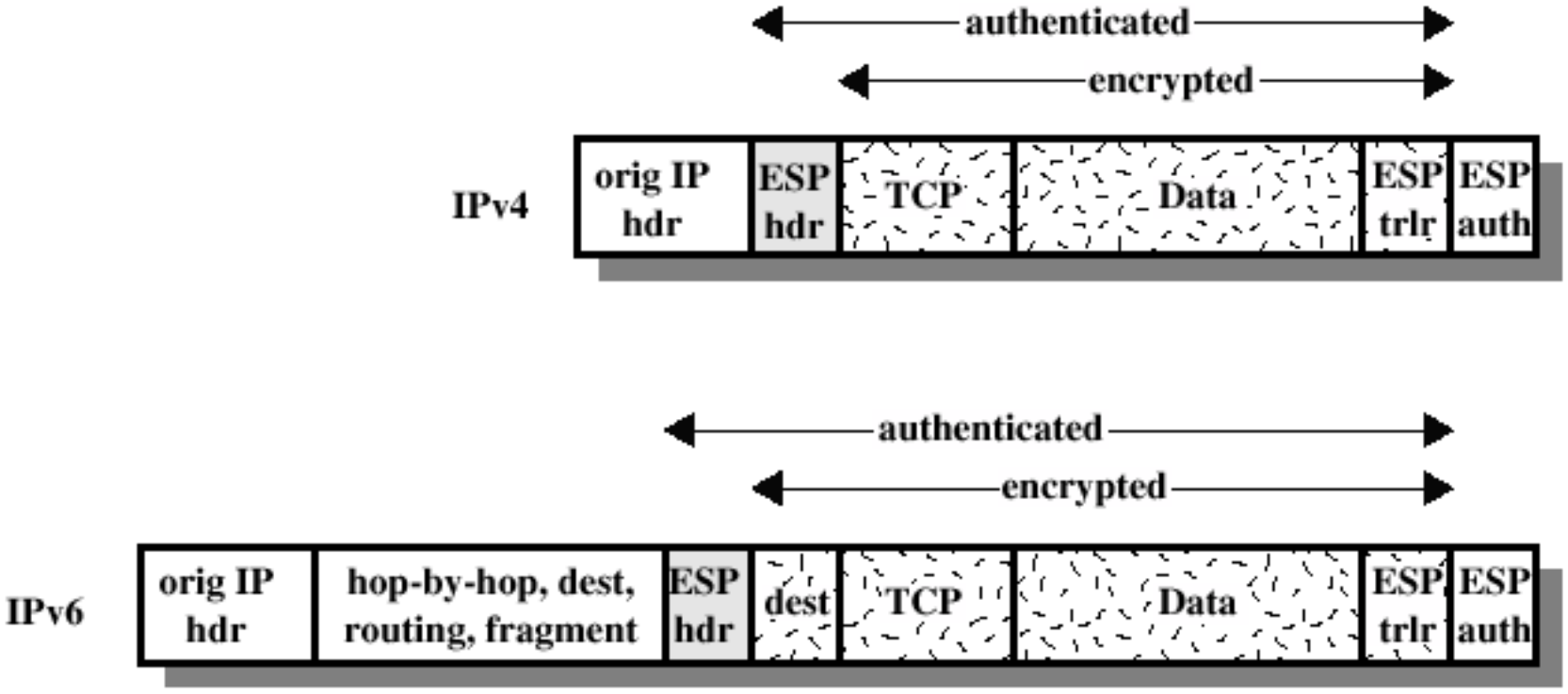


Figure 6.7 IPSec ESP Format

Encryption and Authentication Algorithms

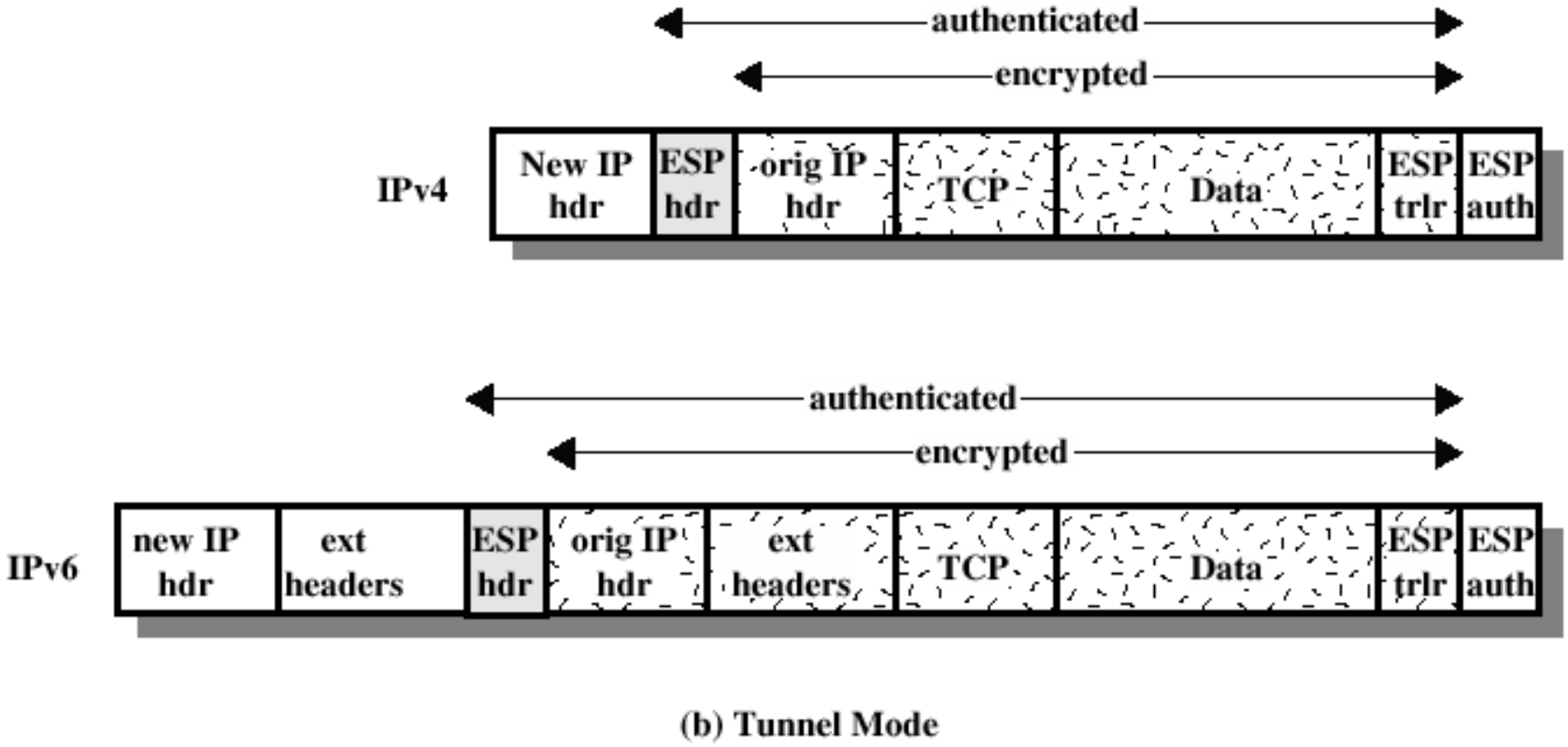
- Encryption:
  - Three-key triple DES
  - RC5
  - IDEA
  - Three-key triple IDEA
  - CAST
  - Blowfish
- Authentication:
  - HMAC-MD5-96
  - HMAC-SHA-1-96

ESP Encryption and Authentication



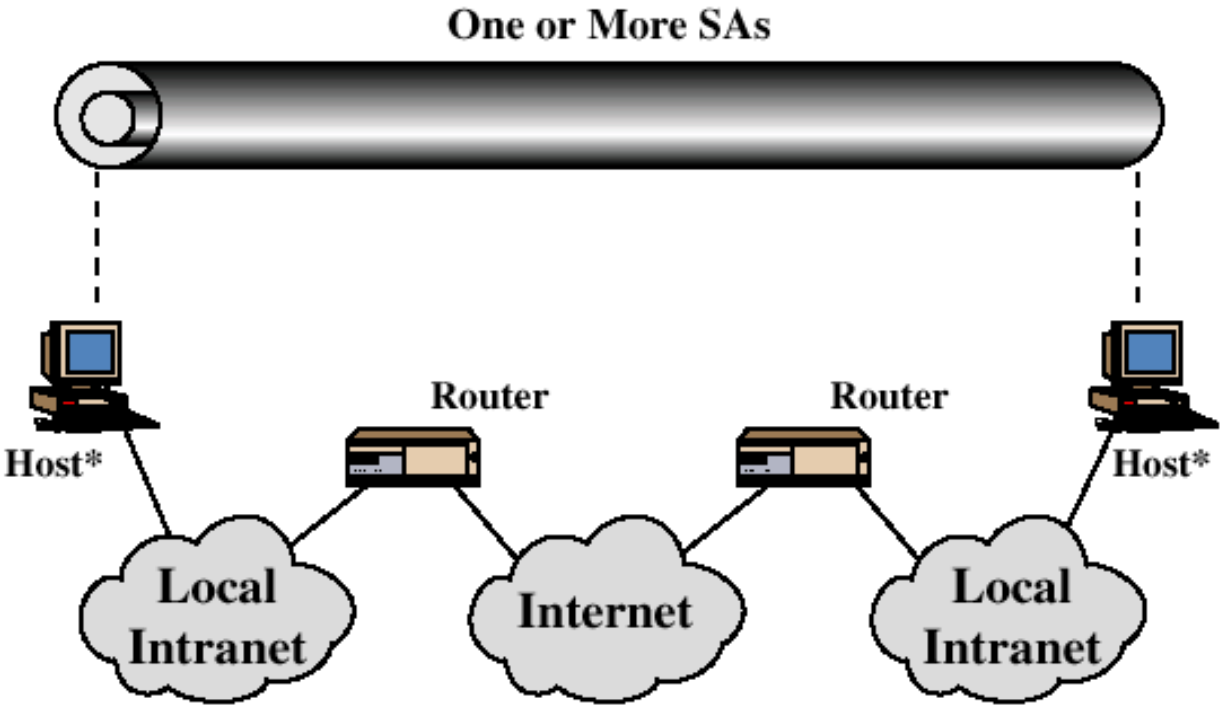
(a) Transport Mode

ESP Encryption and Authentication



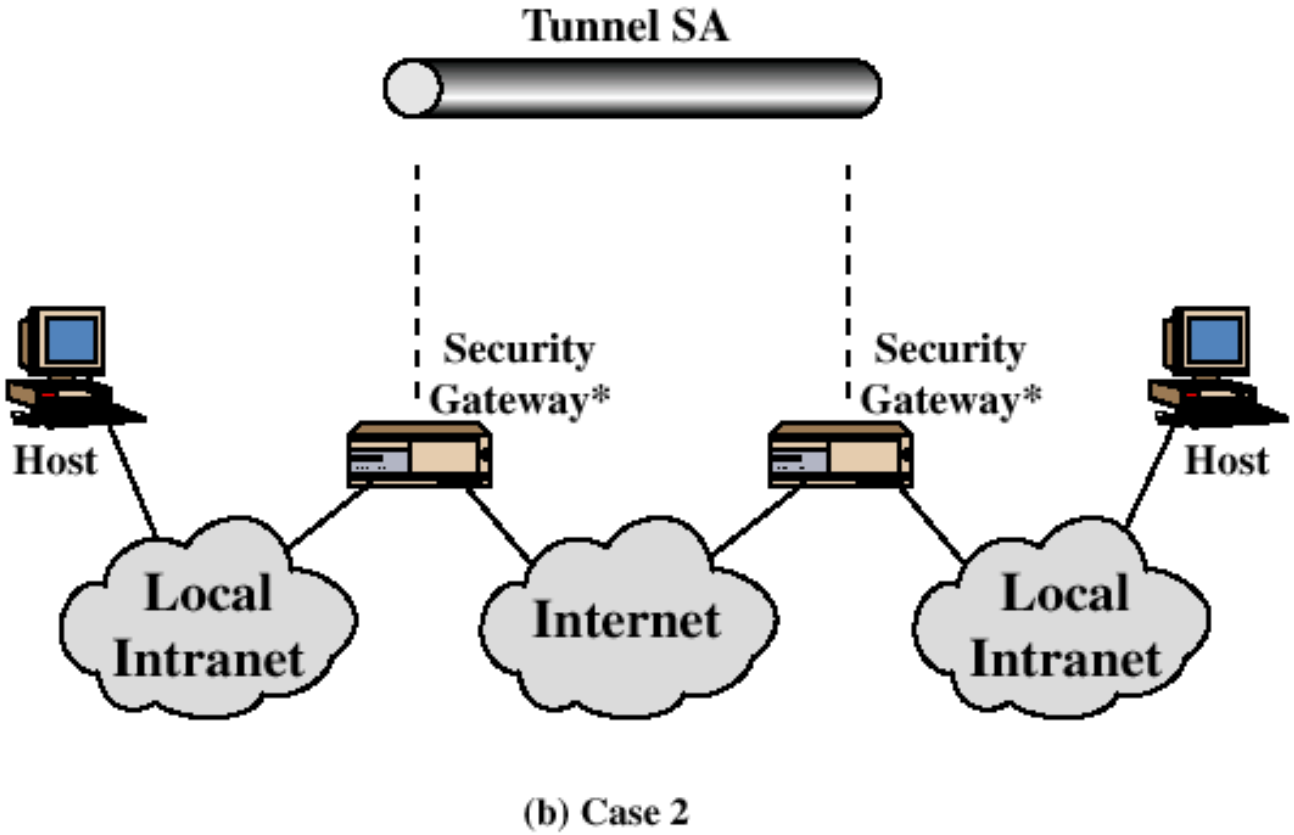
(b) Tunnel Mode

Combinations of Security Associations



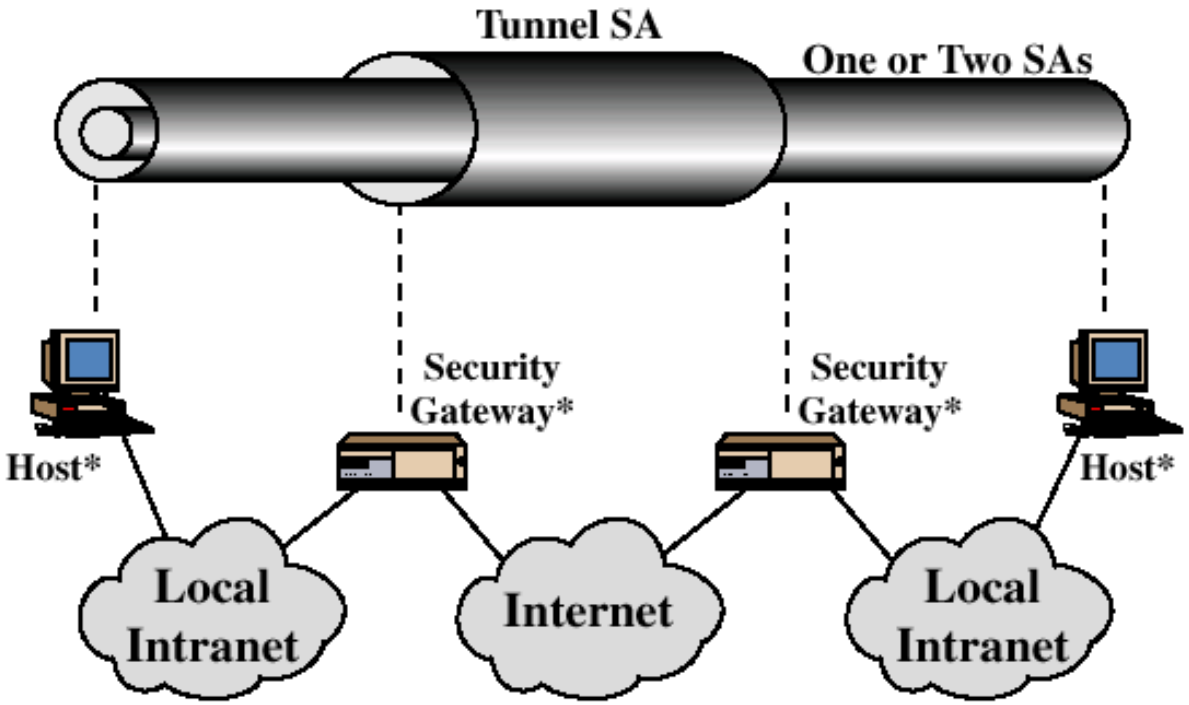
(a) Case 1

Combinations of Security Associations



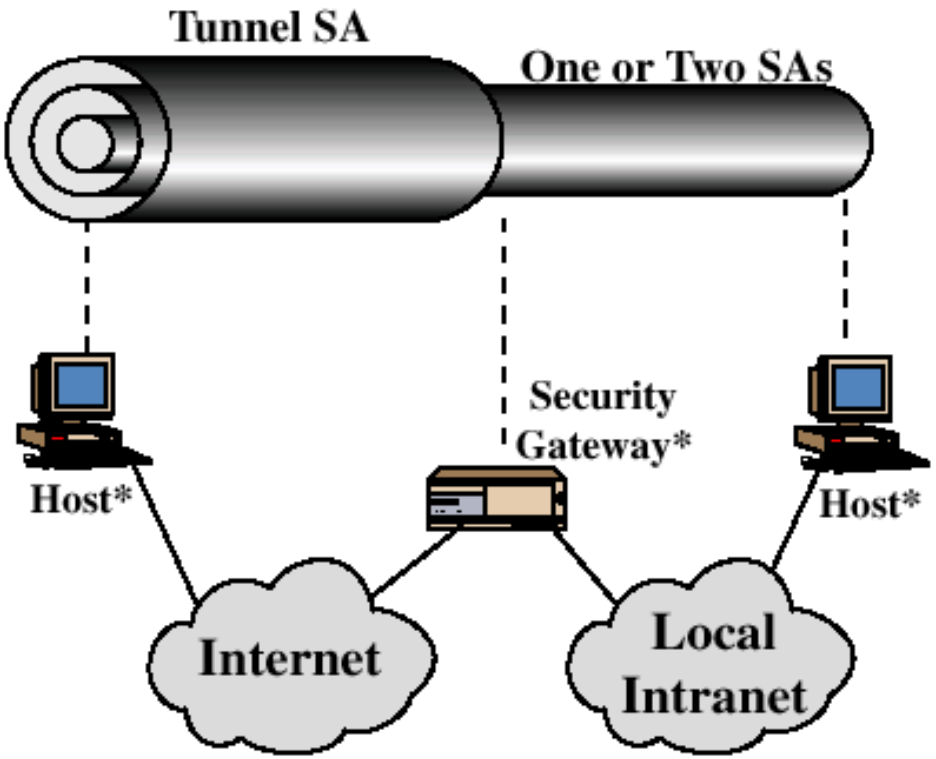
(b) Case 2

Combinations of Security Associations



(c) Case 3

Combinations of Security Associations



(d) Case 4

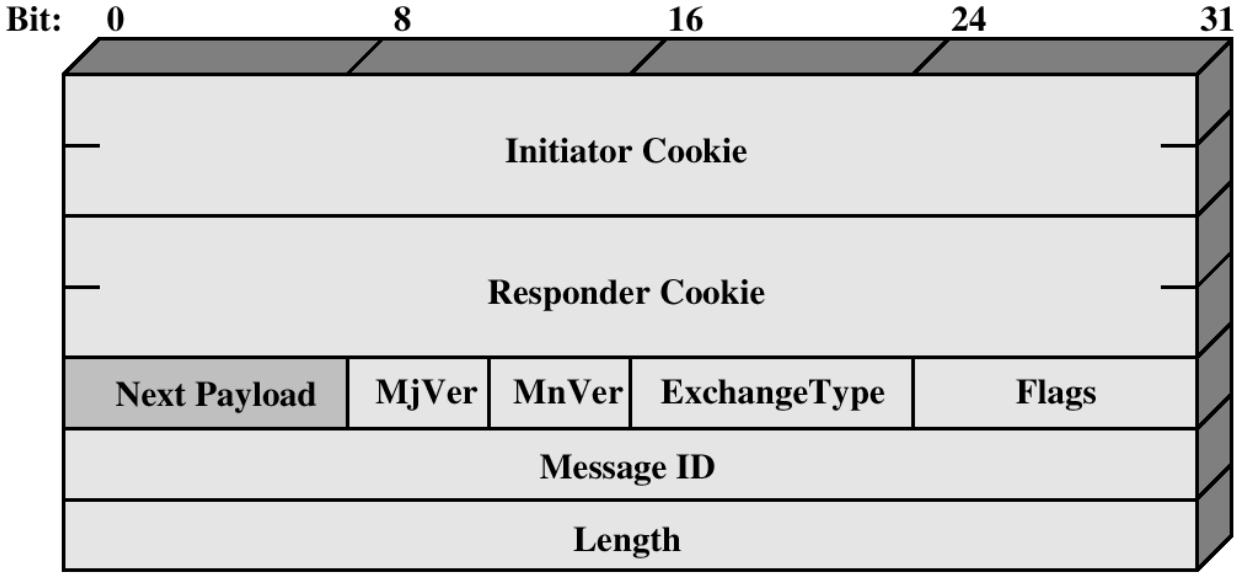
Key Management

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

Oakley

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

ISAKMP



(a) ISAKMP Header

(b) Generic Payload Header

Figure 6.12 ISAKMP Formats

Recommended Reading

- Comer, D. *Internetworking with TCP/IP, Volume I: Principles, Protocols and Architecture*. Prentic Hall, 1995
- Stevens, W. *TCP/IP Illustrated, Volume 1: The Protocols*. Addison-Wesley, 1994