

Outline

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

Simple Mail Transfer Protocol (SMTP, RFC 822)

- **SMTP Limitations - Can not transmit, or has a problem with:**
 - executable files, or other binary files (jpeg image)
 - "national language" characters (non-ASCII)
 - messages over a certain size
 - ASCII to EBCDIC translation problems
 - lines longer than a certain length (72 to 254 characters)

Header fields in MIME

- **MIME-Version:** Must be "1.0" -> RFC 2045, RFC 2046
- **Content-Type:** More types being added by developers (application/word)
- **Content-Transfer-Encoding:** How message has been encoded (radix-64)
- **Content-ID:** Unique identifying character string.
- **Content Description:** Needed when content is not readable text (e.g.,mpeg)

MIME Content Parts

Text	Plain	Unformatted text
	Enriched	HTML / RTF, etc
Multipart	Mixed	Independent Parts; present in order
	Parallel	Independent Parts; any order
	Alternative	Versions of same information
Message	rfc822	Encapsulated message
Image	jpeg	Image in jpeg format, jfif encoding
Video	mpeg	Video in MPEG format
Application	<various>	Postscript, Octet-stream, Word, etc.

S/MIME Functions

- **Enveloped Data:** Encrypted content and encrypted session keys for recipients.
- **Signed Data:** Message Digest encrypted with private key of "signer."
- **Clear-Signed Data:** Signed but not encrypted.
- **Signed and Enveloped Data:** Various orderings for encrypting and signing.

Algorithms Used

- **Message Digesting:** SHA-1 and MD5
- **Digital Signatures:** DSS (*should* RSA)
- **Secret-Key Encryption:** Triple-DES, RC2/40 (exportable)
- **Public-Private Key Encryption:** RSA with key sizes of 512 and 1024 bits, and Diffie-Hellman (for session keys).

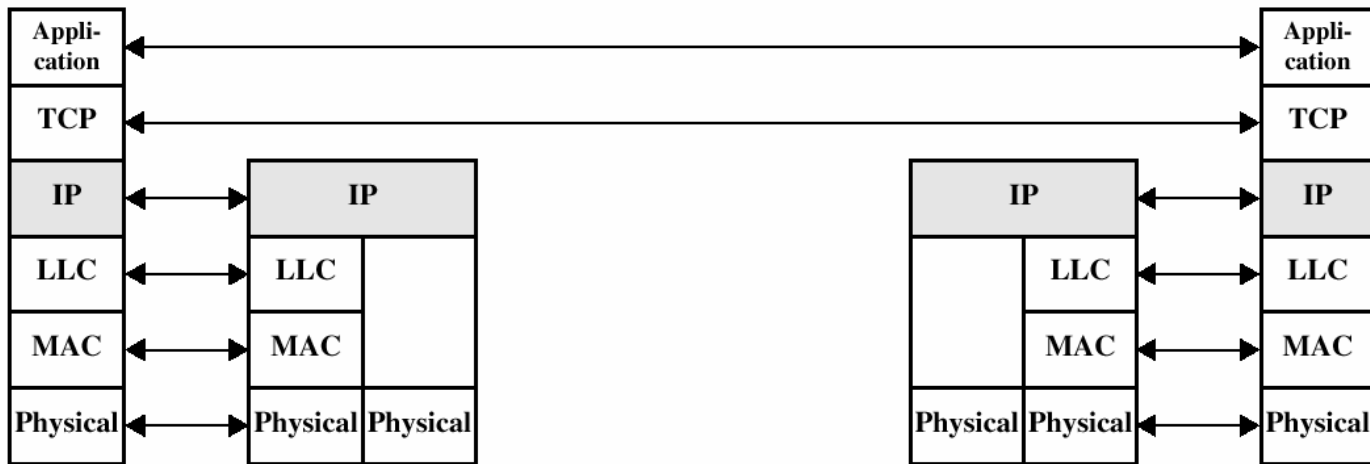
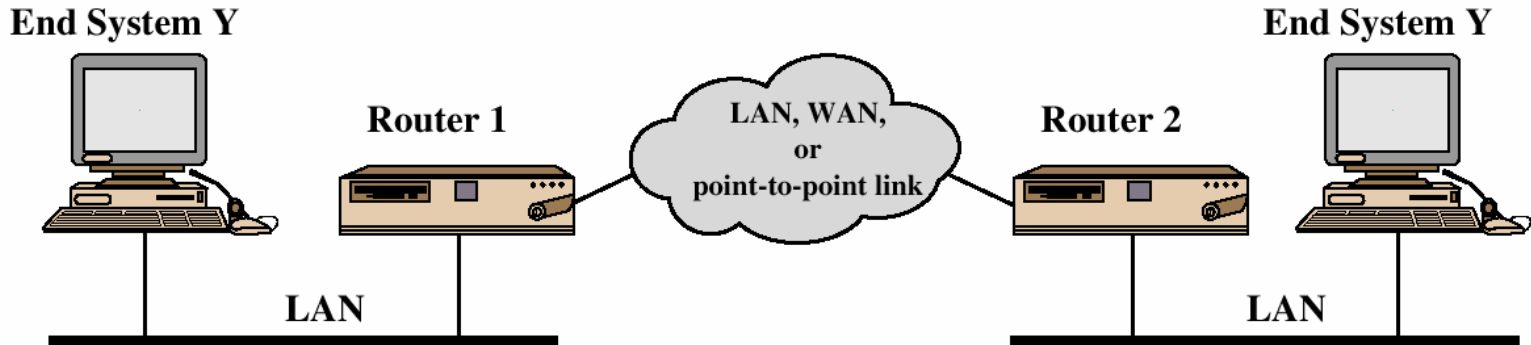
User Agent Role

- S/MIME uses Public-Key Certificates - X.509 version 3 signed by Certification Authority
- Functions:
 - **Key Generation** - Diffie-Hellman, DSS, and RSA key-pairs.
 - **Registration** - Public keys must be registered with X.509 CA.
 - **Certificate Storage** - Local (as in browser application) for different services.

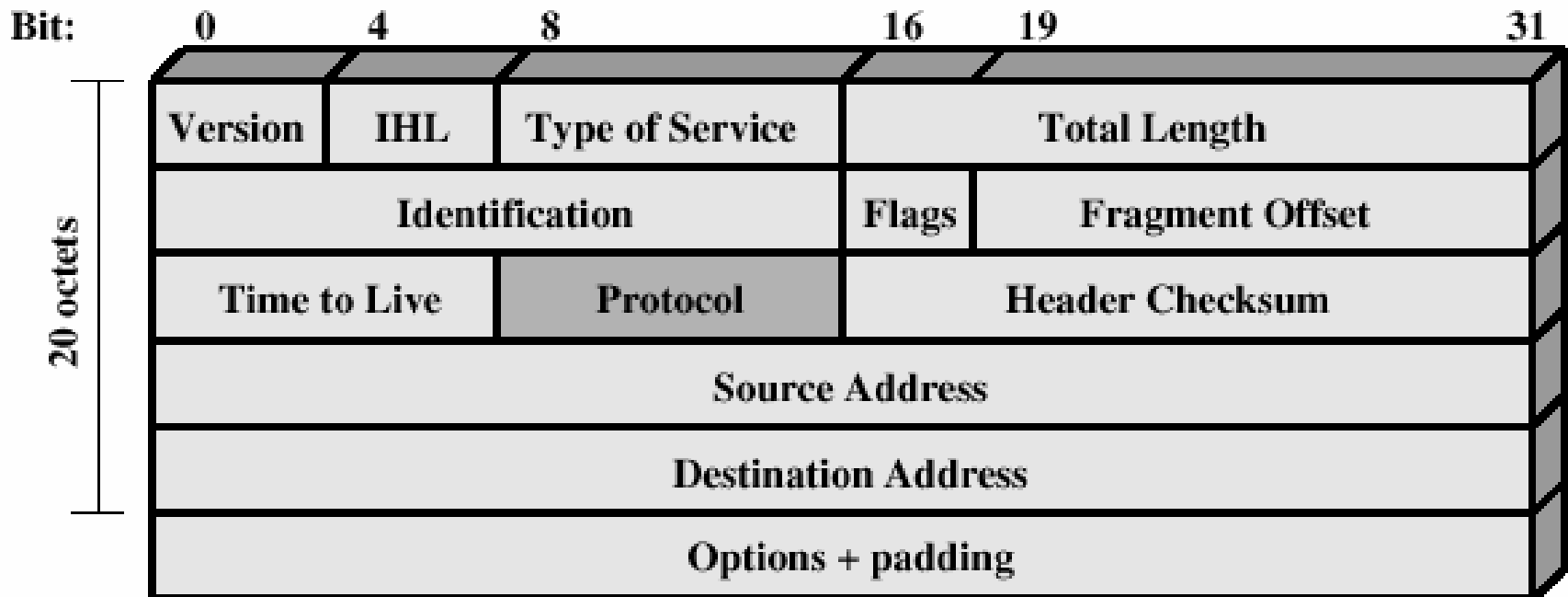
User Agent Role

- **Example: Verisign (www.verisign.com)**
 - **Class-1:** Buyer's email address confirmed by emailing vital info.
 - **Class-2:** Postal address is confirmed as well, and data checked against directories.
 - **Class-3:** Buyer must appear in person, or send notarized documents.

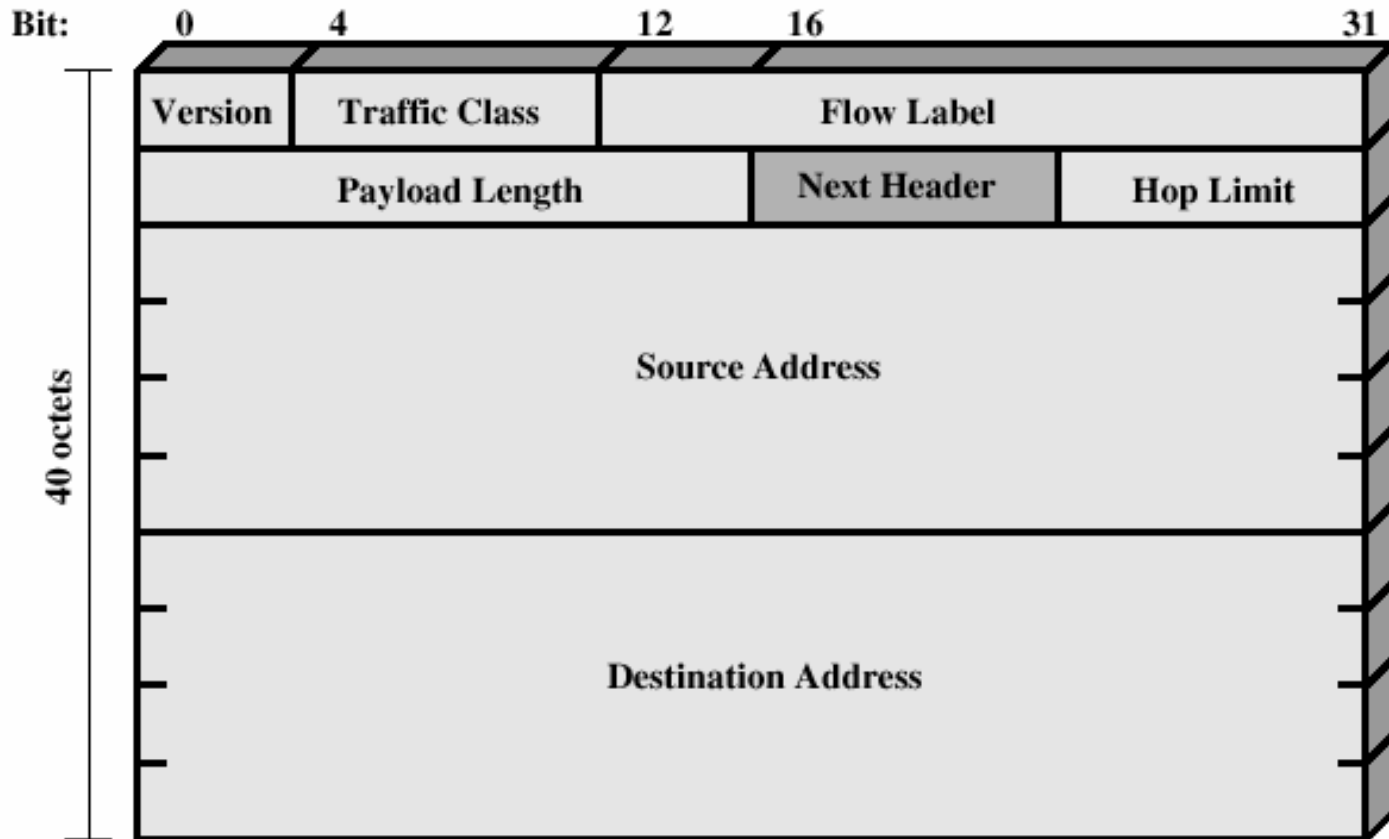
TCP/IP Example



IPv4 Header



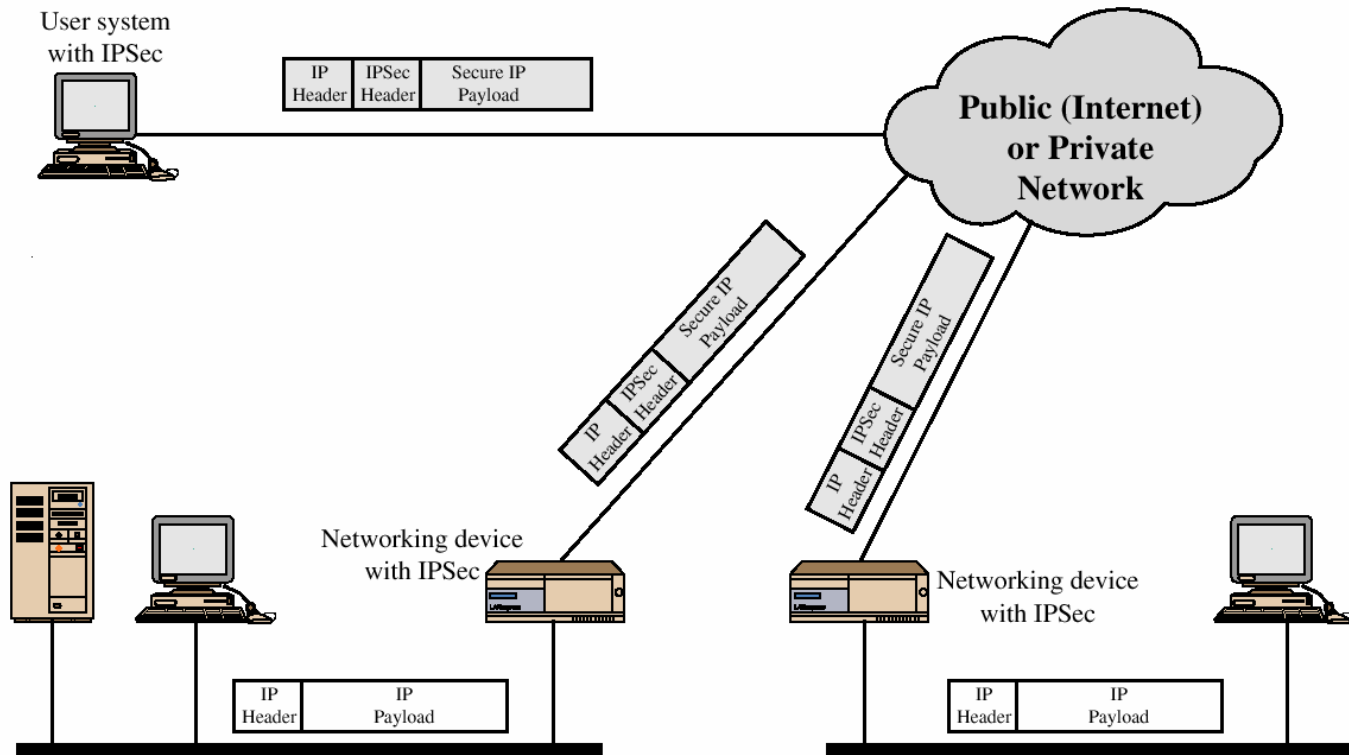
IPv6 Header



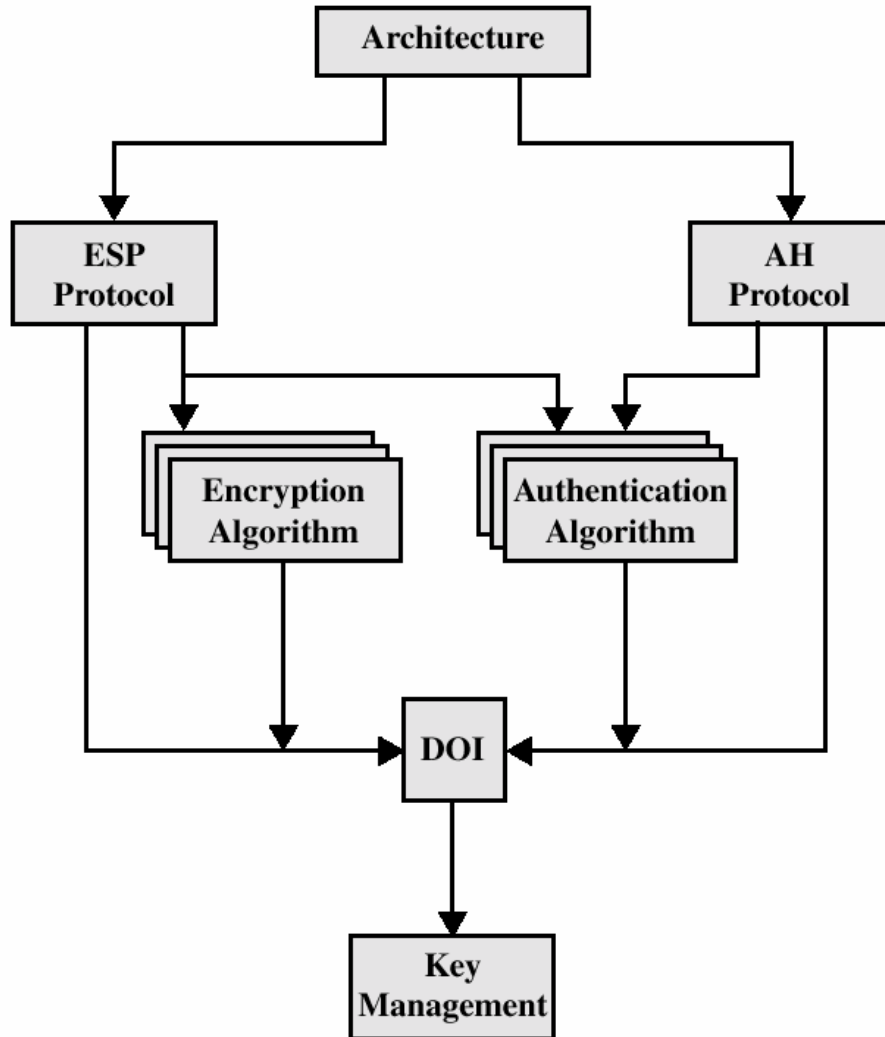
IP Security Overview

- 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



IPSec Document Overview



IPSec Services

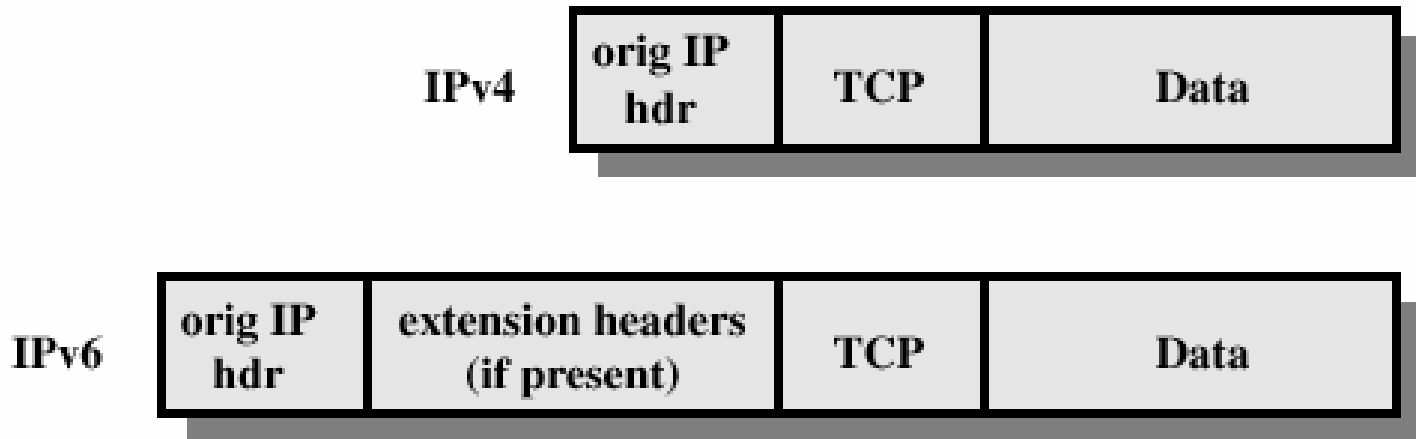
- Access Control
- Connectionless integrity
- Data origin authentication
- Rejection of replayed packets
- Confidentiality (encryption)
- Limited traffic flow confidentiality

Security Associations (SA)

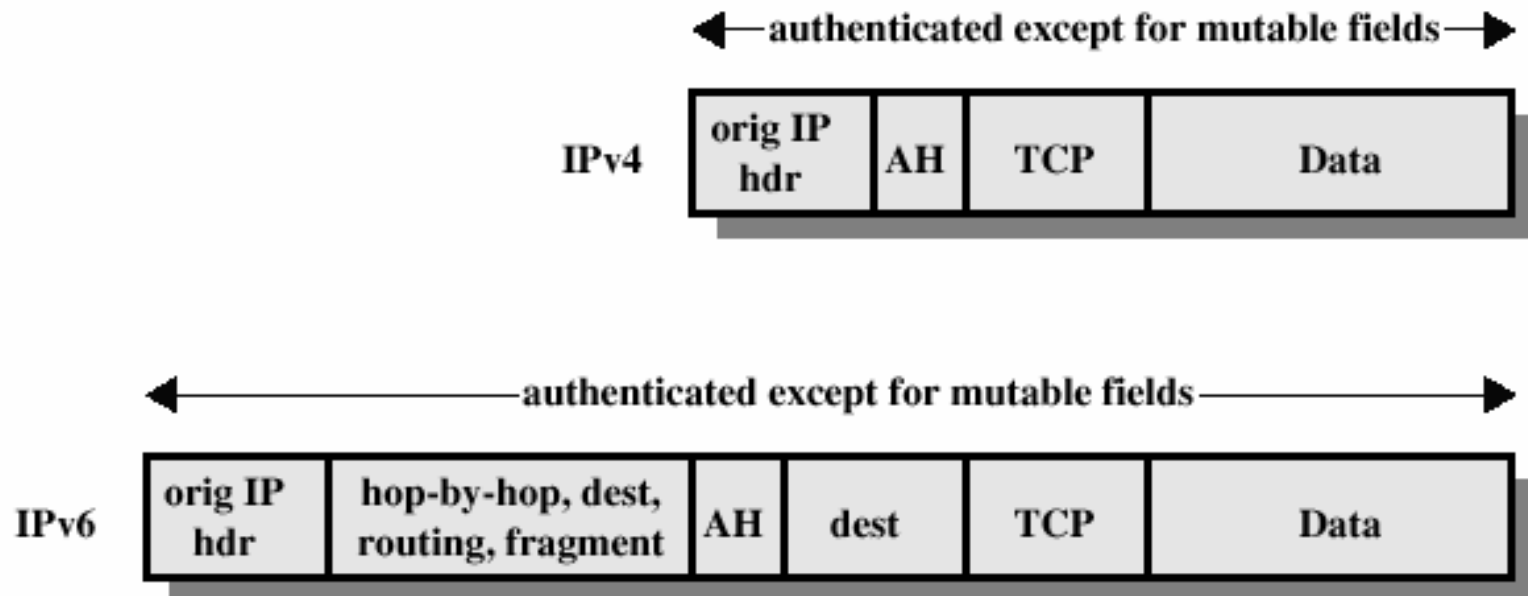
- A one way relationship between a sender and a receiver.
- Identified by three parameters:
 - Security Parameter Index (SPI)
 - IP Destination address
 - Security Protocol Identifier

	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.

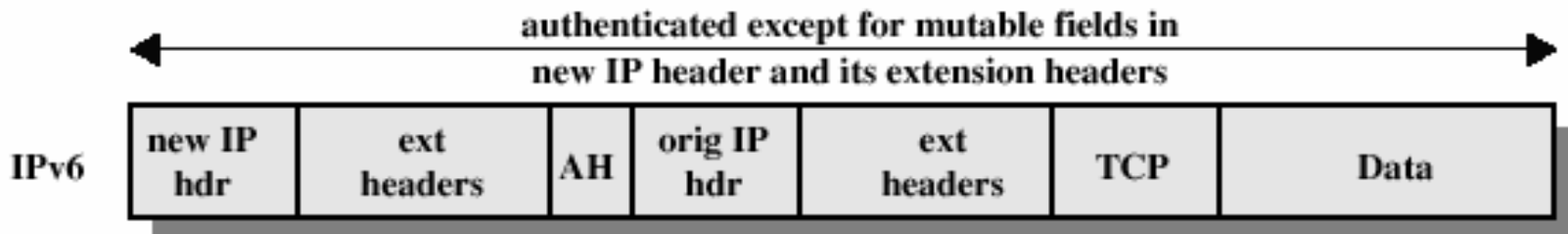
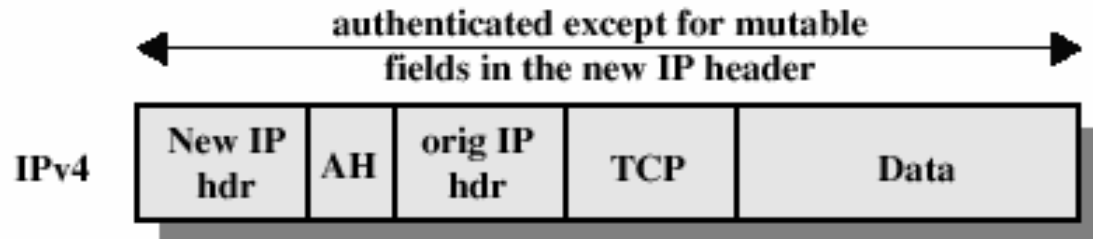
Before applying AH



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.

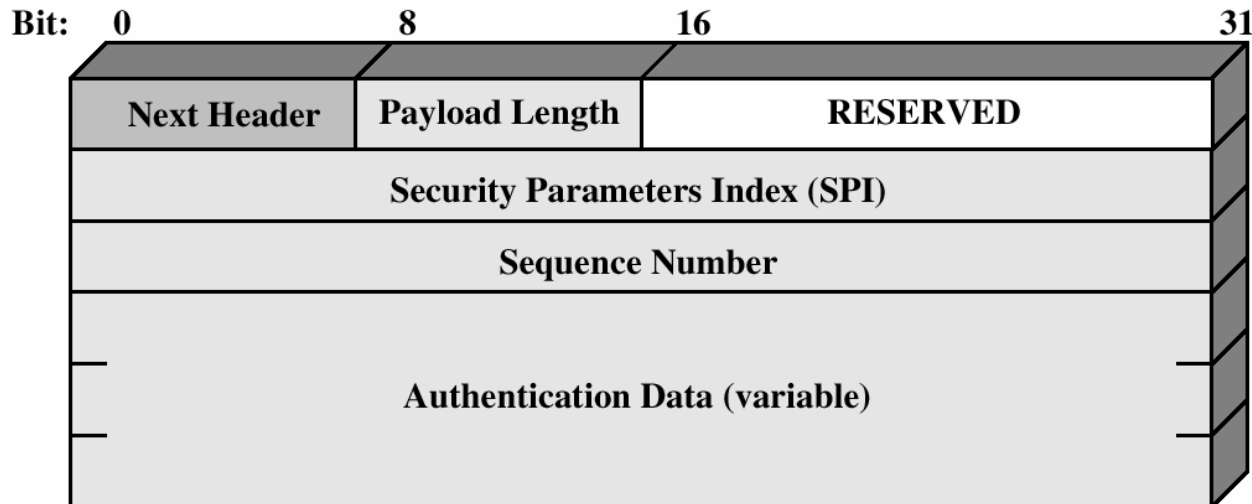
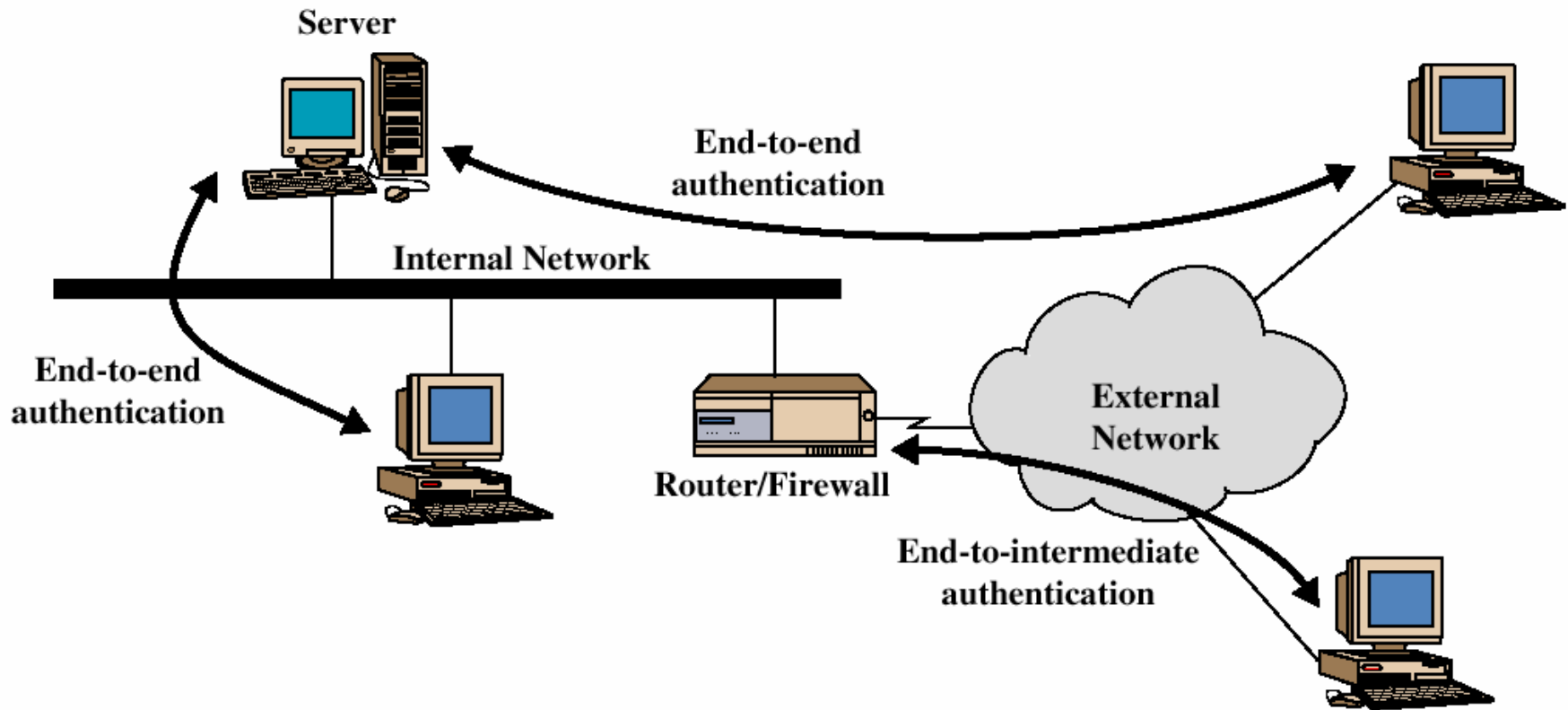


Figure 6.3 IPsec Authentication Header

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



Encapsulating Security Payload

- ESP provides confidentiality services

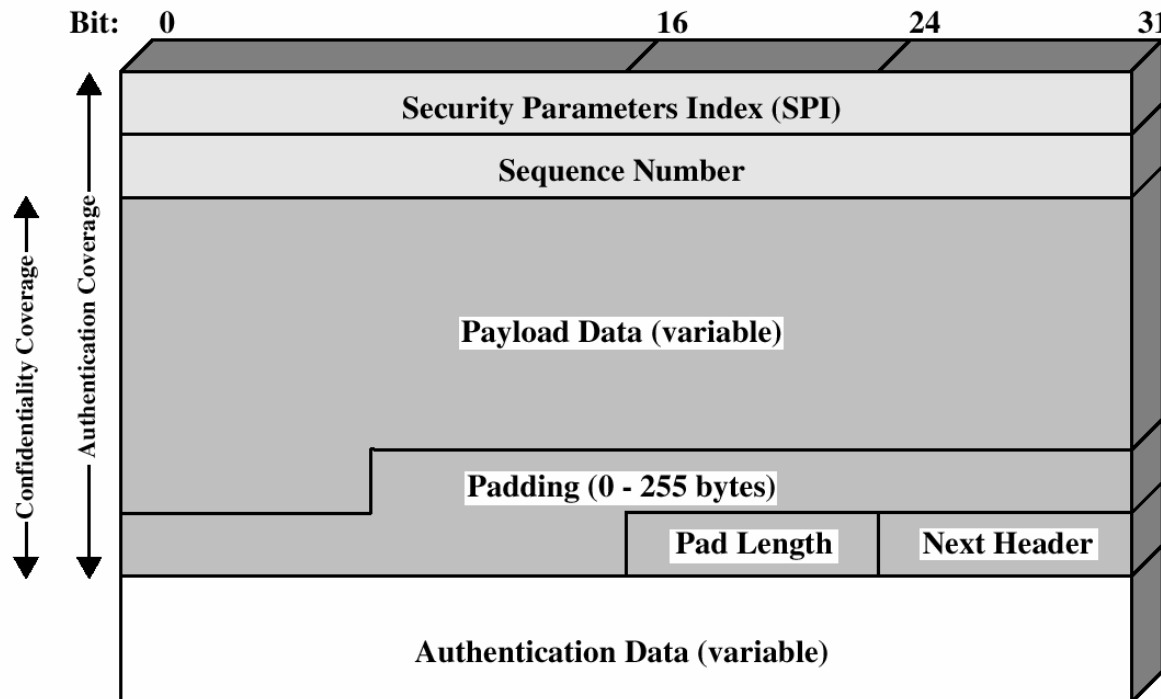
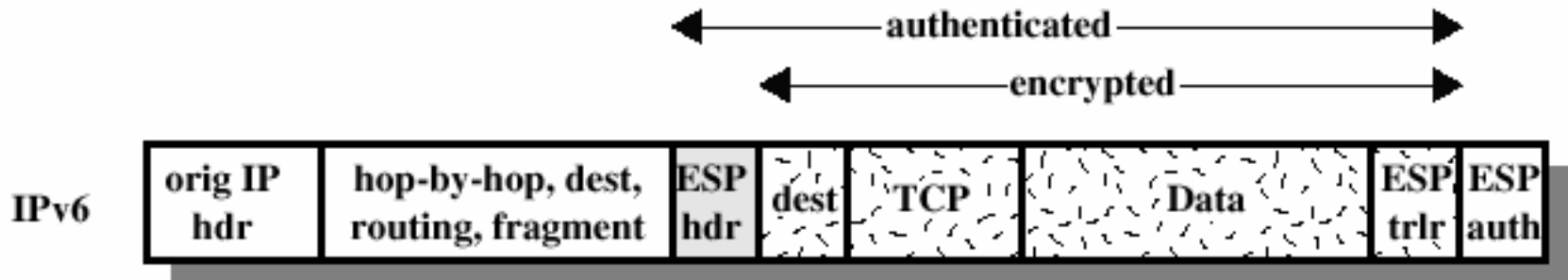
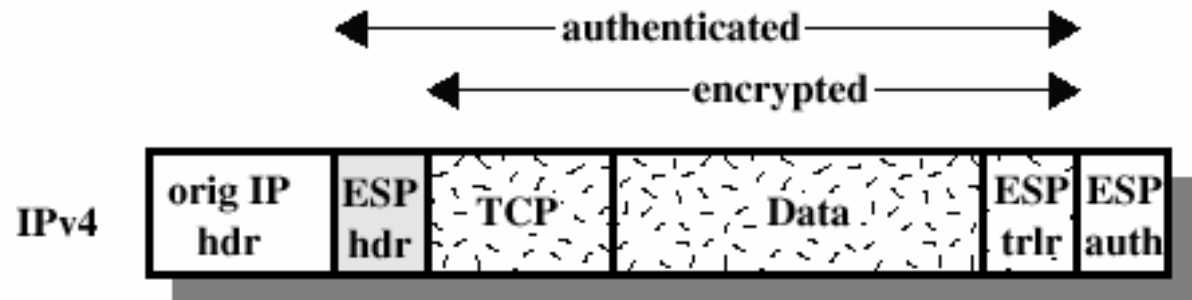


Figure 6.7 IPsec ESP Format

Encryption and Authentication Algorithms

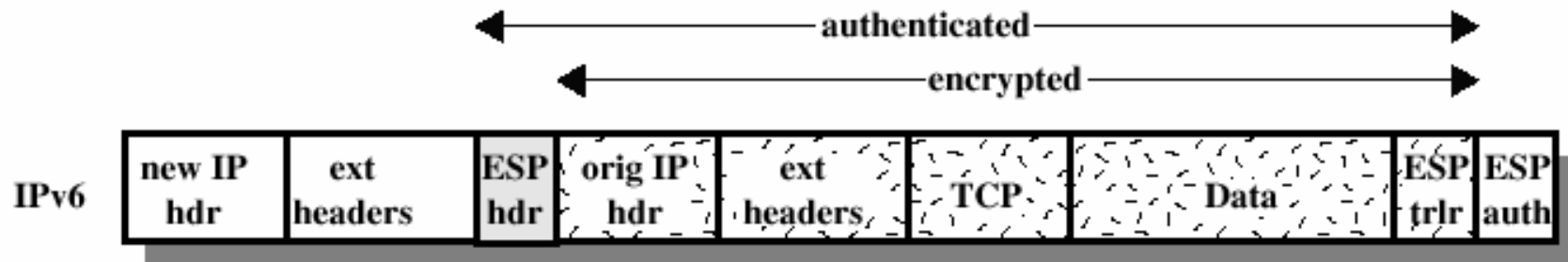
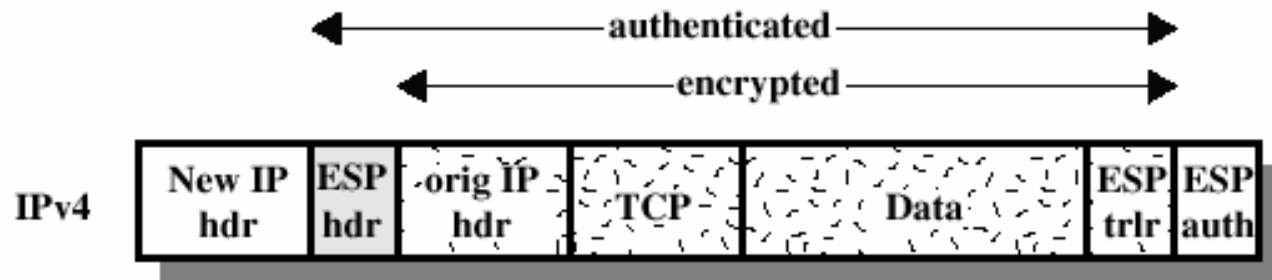
- Encryption:
 - Three-key triple DES
 - RC5
 - IDEA
 - Three-key triple IDEA
 - CAST
 - Blowfish
- Authentication:
 - HMAC-MD5-96
 - HMAC-SHA-1-96

ESP Encryption and Authentication



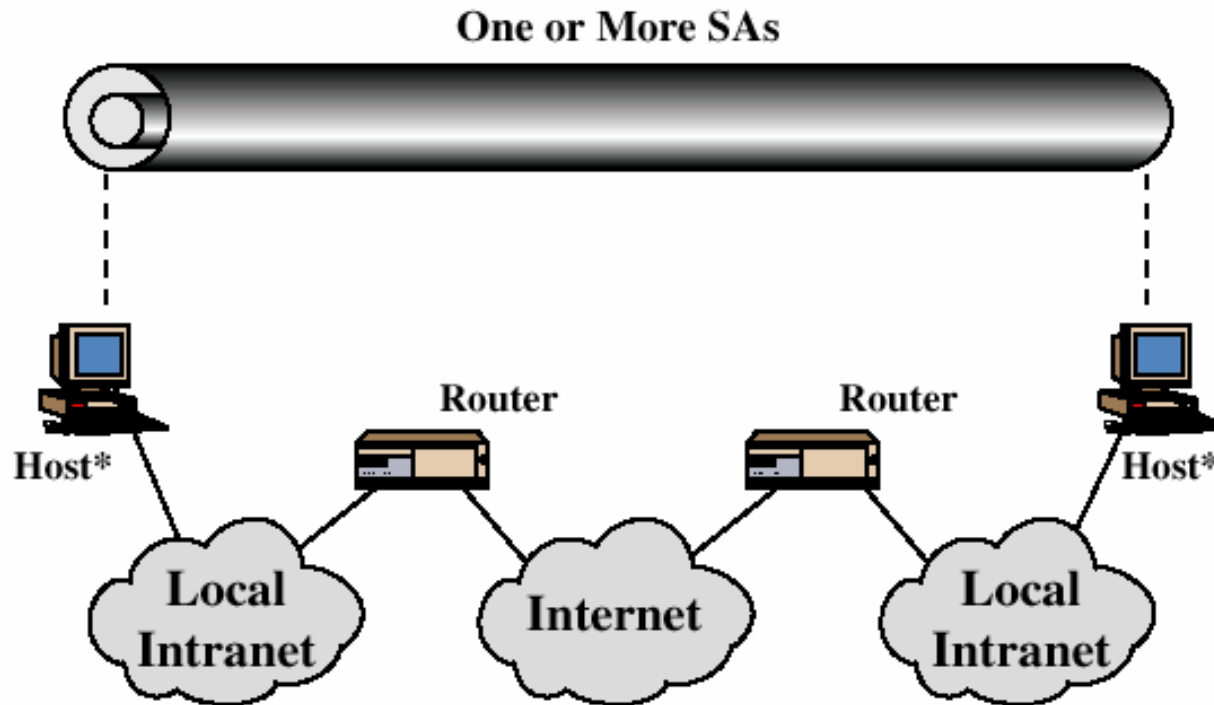
(a) Transport Mode

ESP Encryption and Authentication



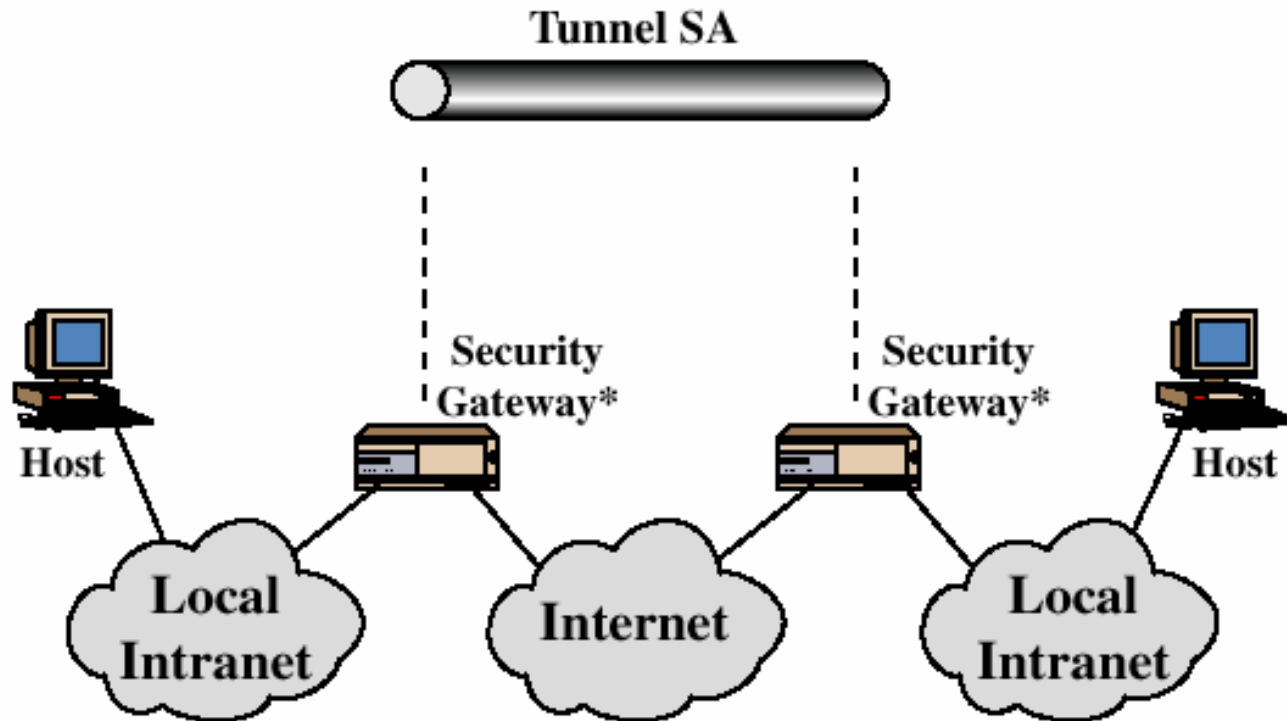
(b) Tunnel Mode

Combinations of Security Associations



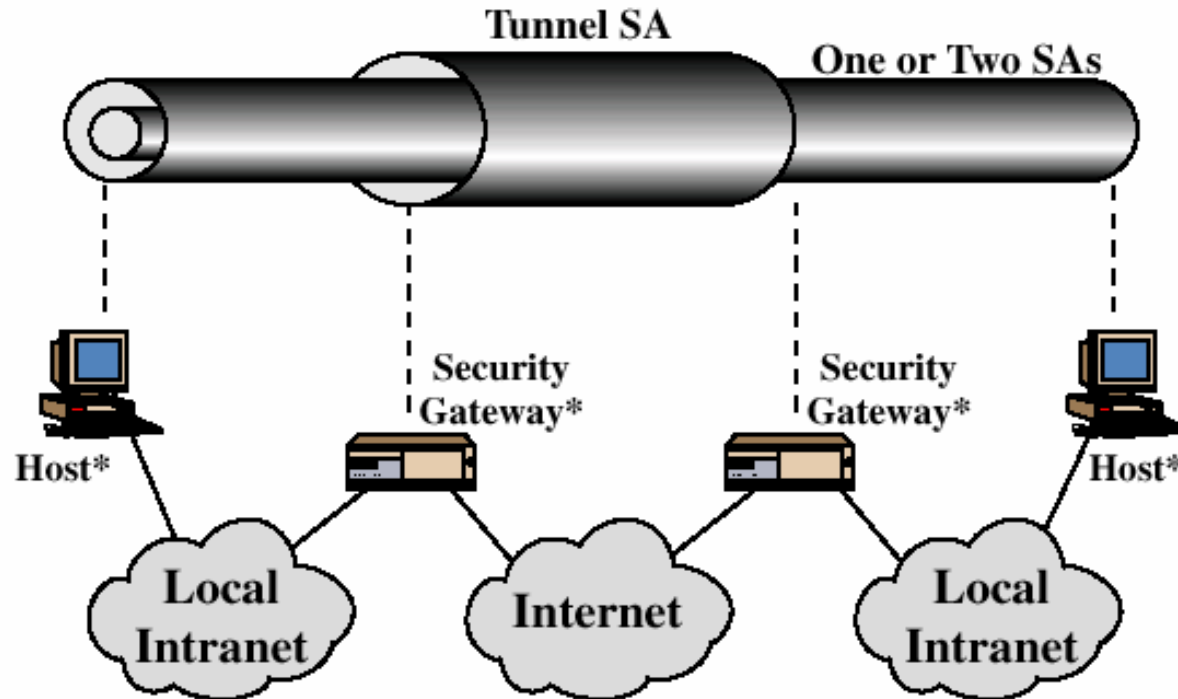
(a) Case 1

Combinations of Security Associations



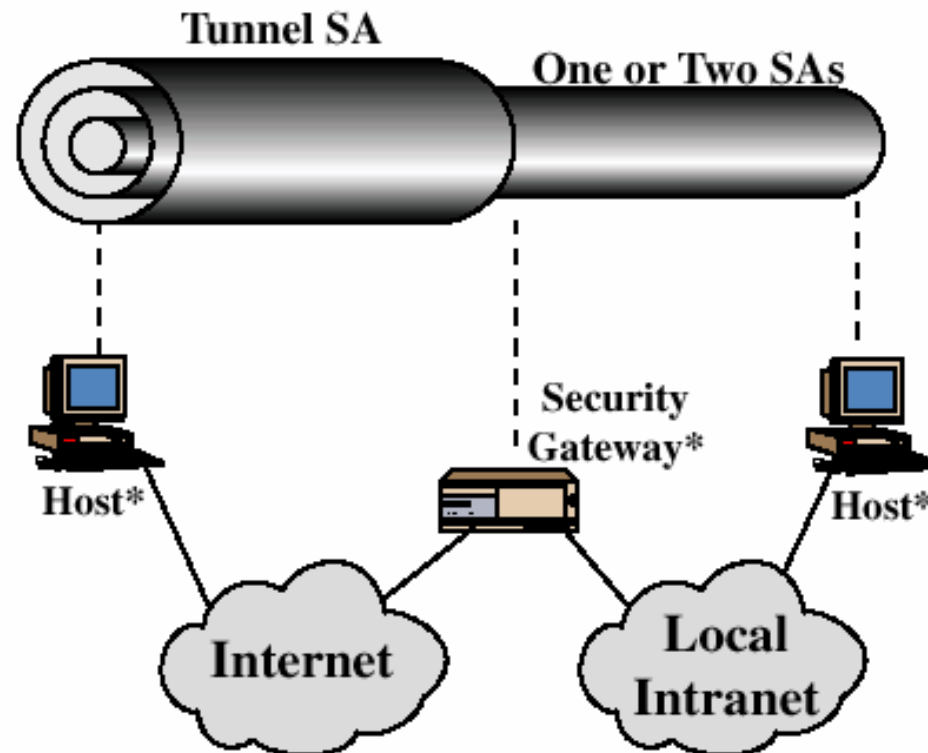
(b) Case 2

Combinations of Security Associations



(c) Case 3

Combinations of Security Associations



(d) Case 4

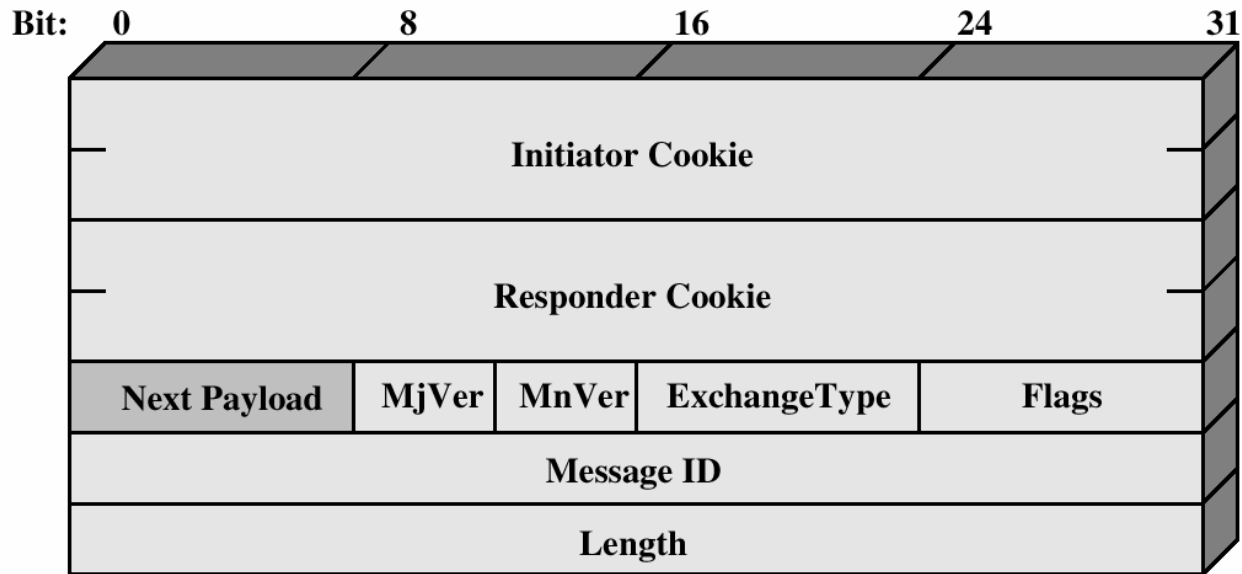
Key Management

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

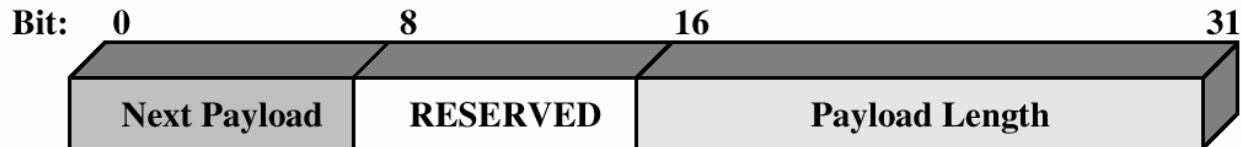
Oakley

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

ISAKMP



(a) ISAKMP Header



(b) Generic Payload Header

Figure 6.12 ISAKMP Formats
Security, Fall 2003

Recommended Reading

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