# Chapter 16

IP Security

IP Security

- have considered some 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

IPSec

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

IPSec Uses
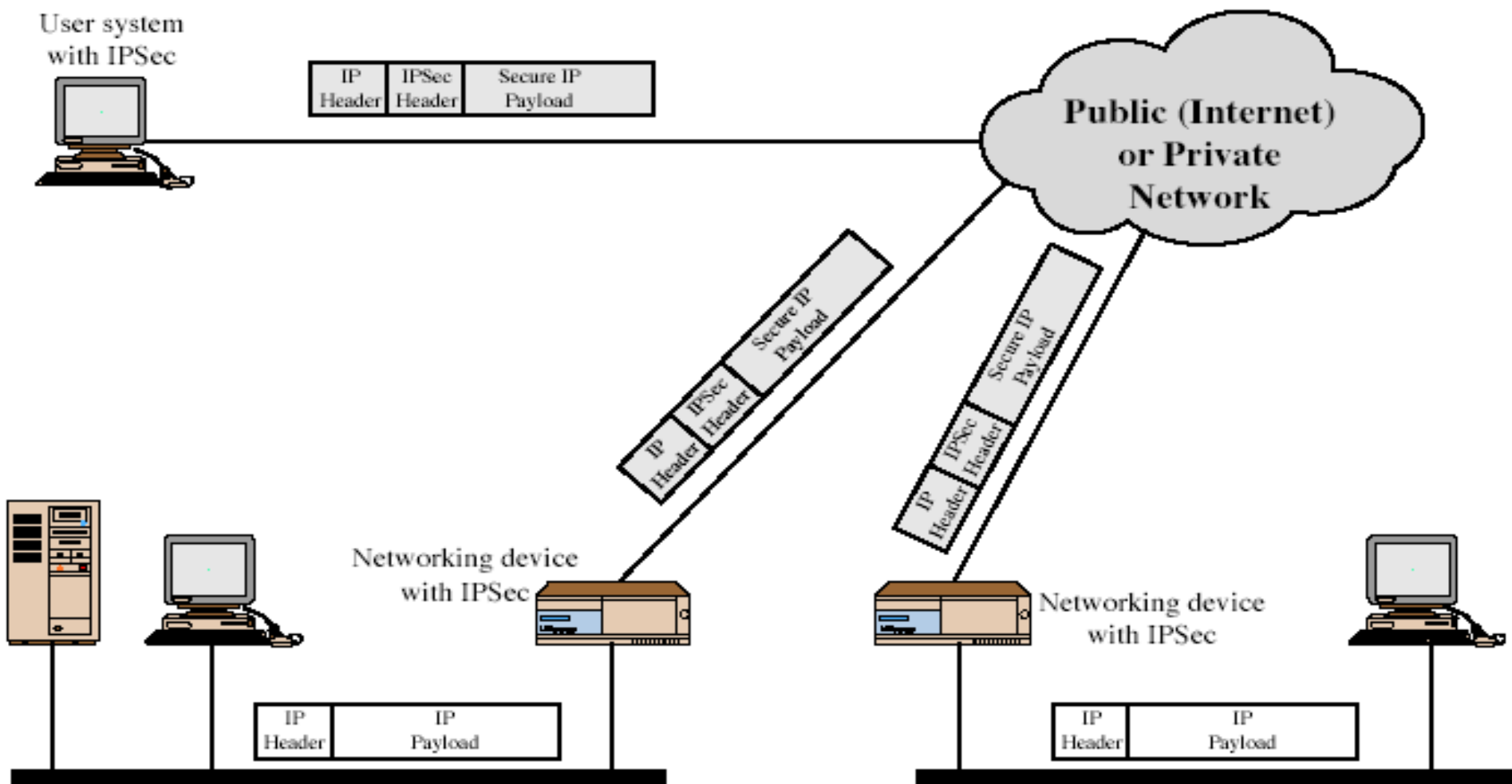
Benefits of IPSec

- in a firewall/router provides strong security to all traffic crossing the perimeter

- is resistant to bypass

- is below transport layer, hence transparent to applications

- can be transparent to end users

- can provide security for individual users if desired

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

IPSec Services

- Access control

- Connectionless integrity

- Data origin authentication

- Rejection of replayed packets
  - a form of partial sequence integrity

- Confidentiality (encryption)

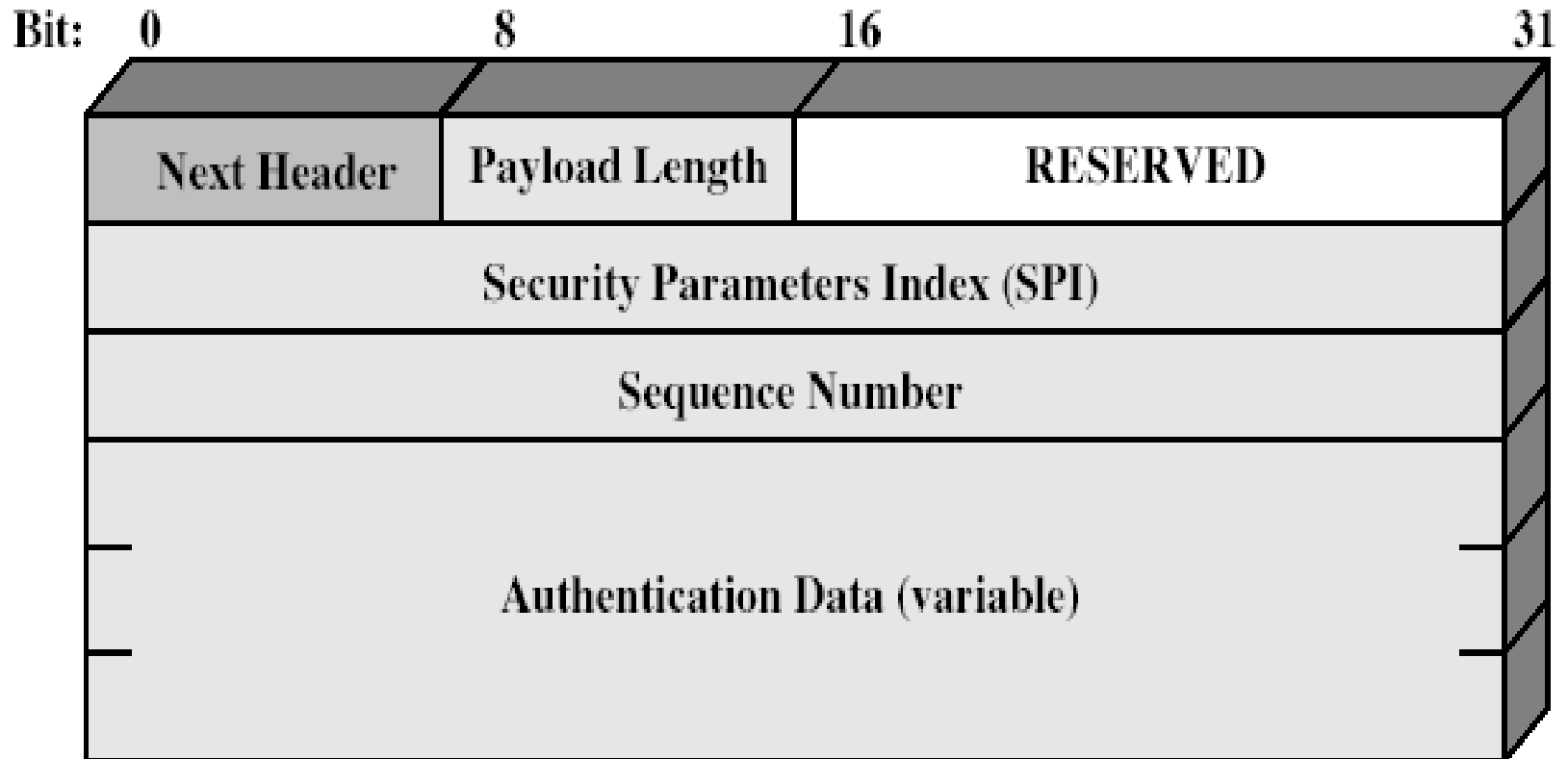- Limited traffic flow confidentiality

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
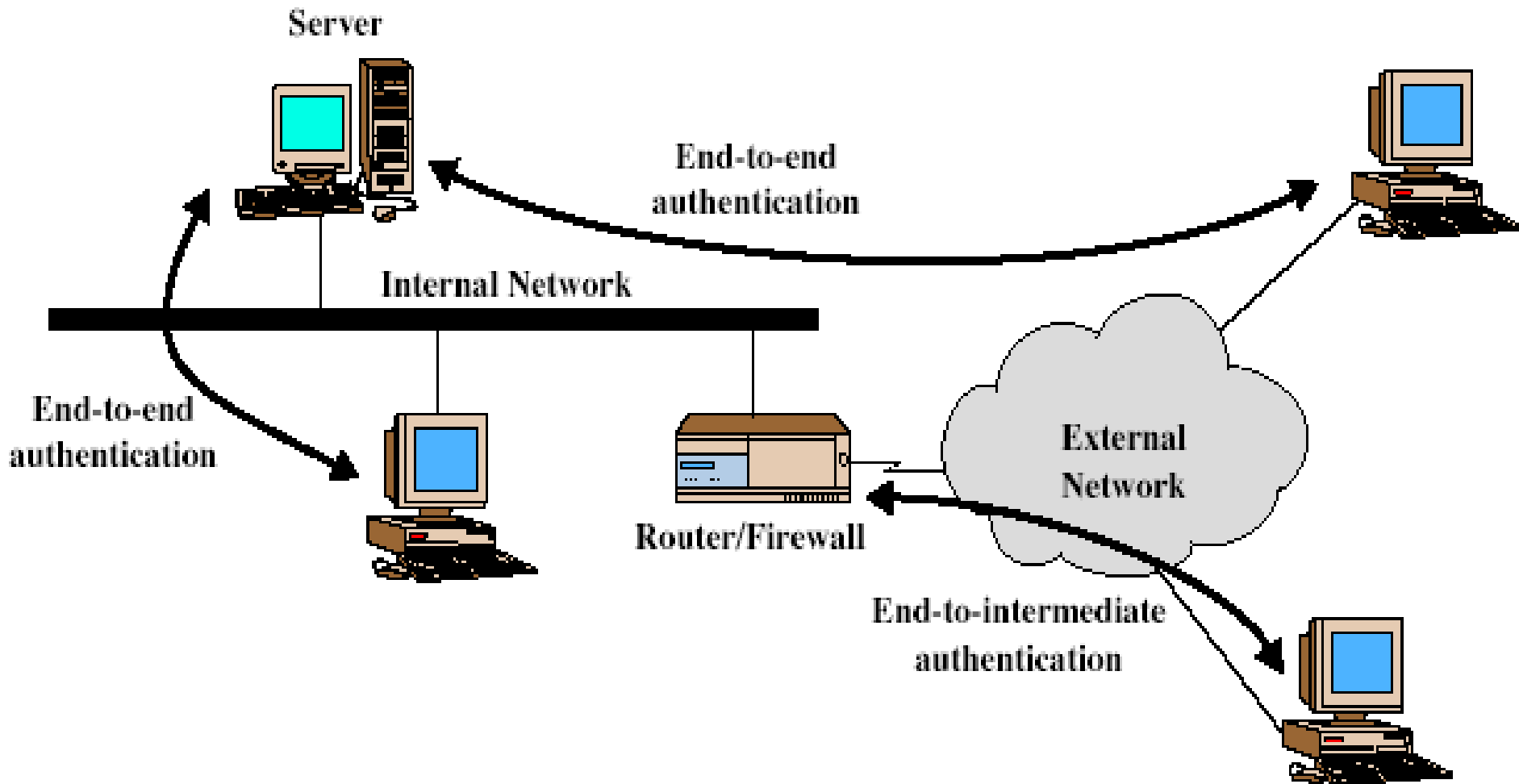- have a database of Security Associations

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
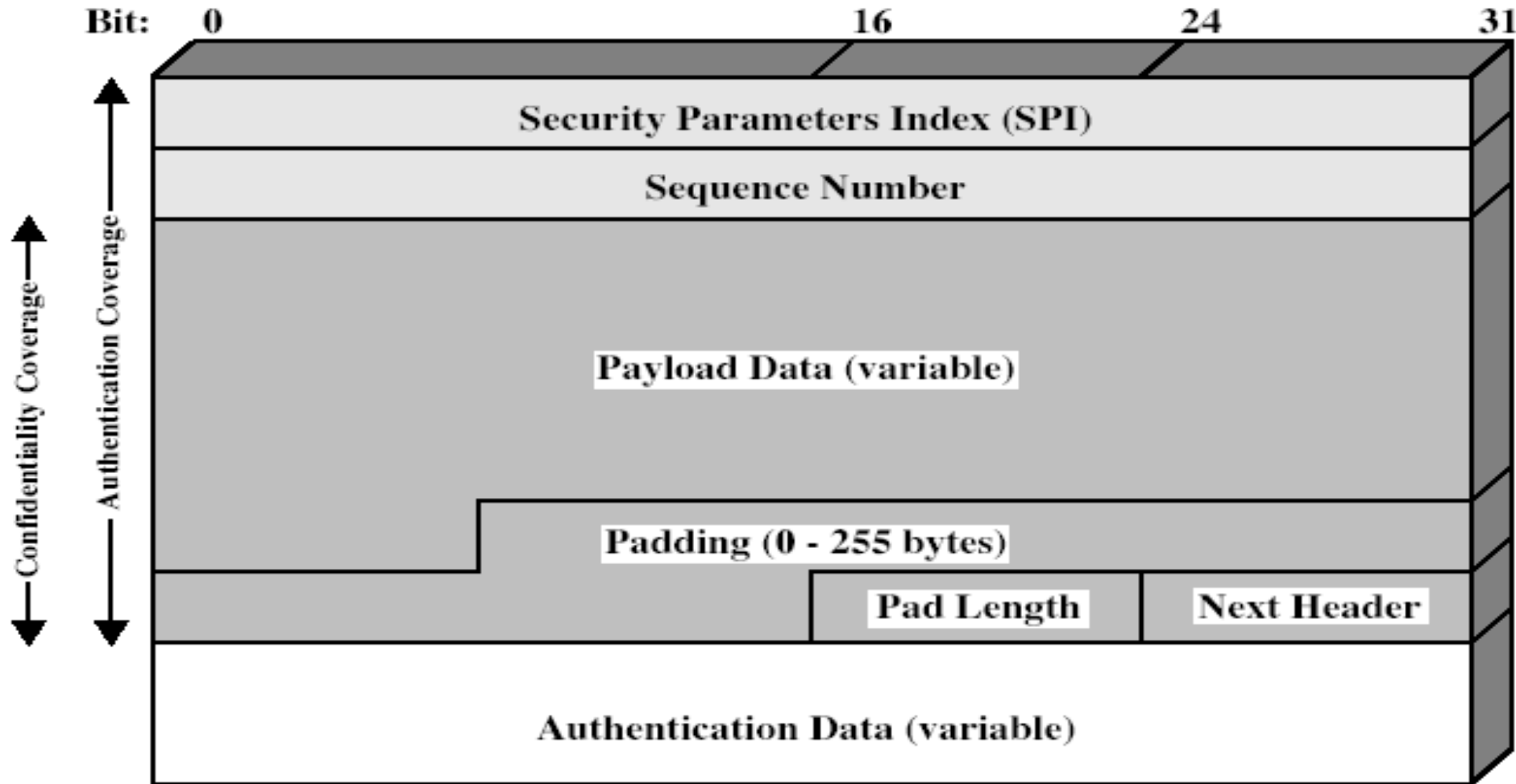
Authentication Header

Bit:	0	8	16	31
	Next Header	Payload Length	RESERVED	
	Security Parameters Index (SPI)			
	Sequence Number			
	Authentication Data (variable)			

Transport & Tunnel Modes

Server

End-to-end authentication

Internal Network

End-to-end authentication

Router/Firewall

External Network

End-to-intermediate authentication

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 most common
  - pad to meet blocksize, for traffic flow

# Encapsulating Security Payload

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
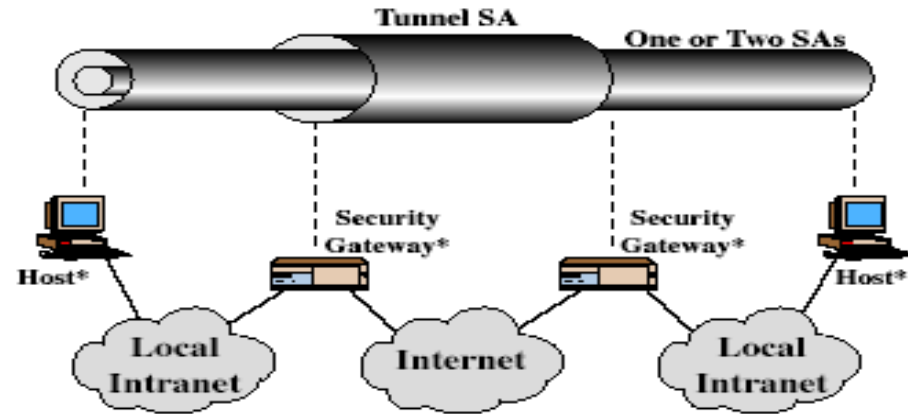 - good for VPNs, gateway to gateway security

Combining Security Associations

- SA's can implement either AH or ESP
- to implement both need to combine SA's
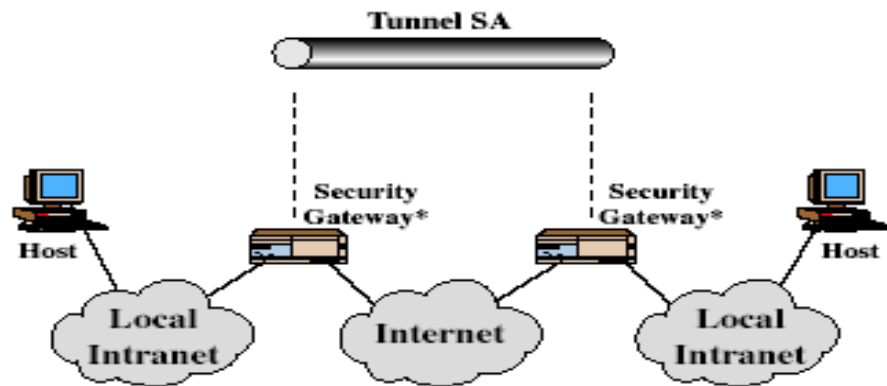 - form a security bundle
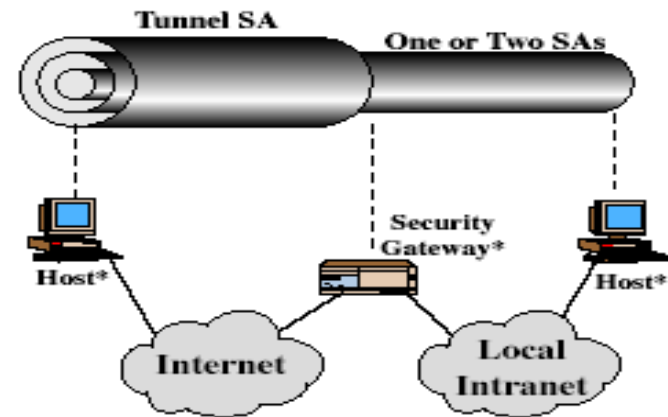- have 4 cases (see next)

Combining Security Associations
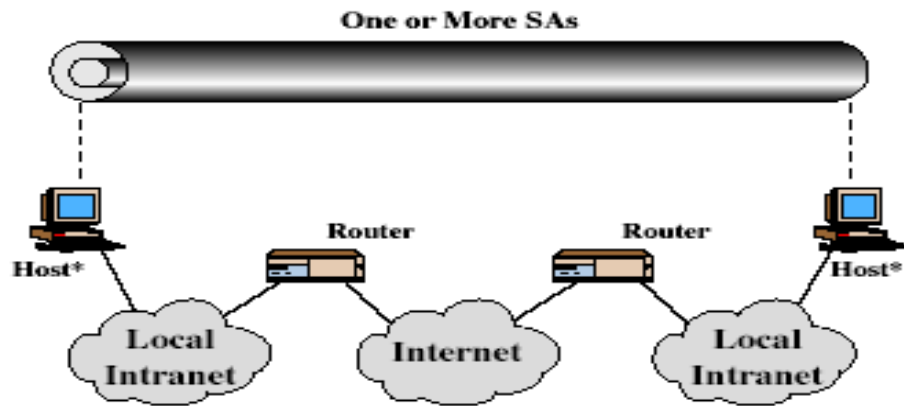
Key Management

- 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
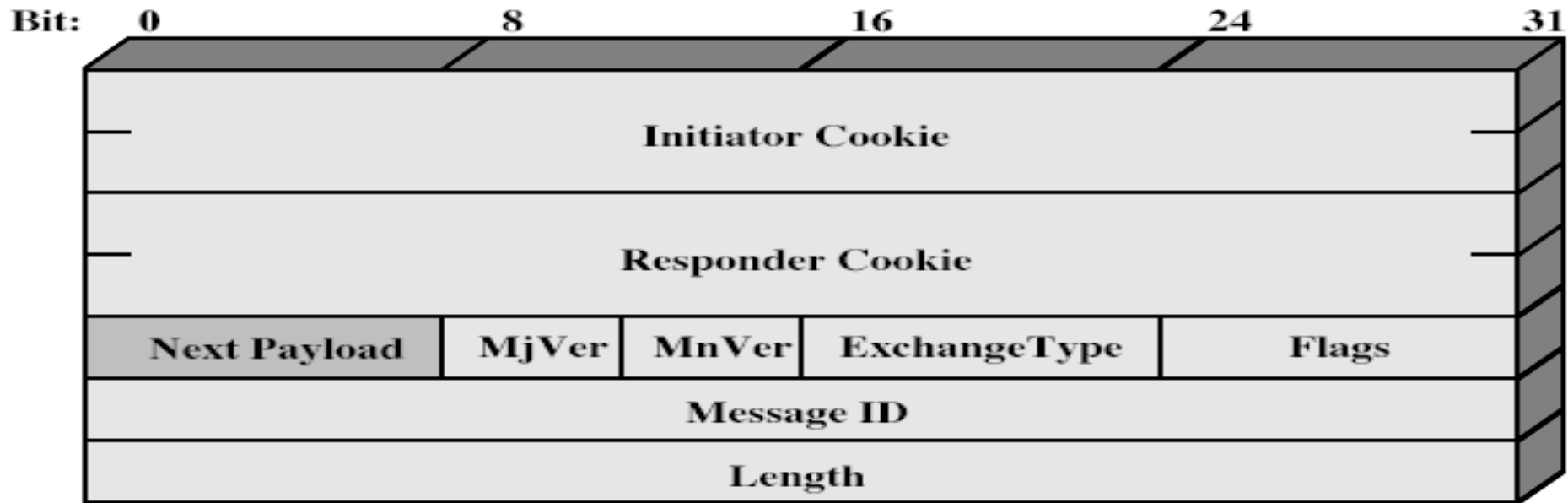
(a) ISAKMP Header

(b) Generic Payload Header

Summary

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