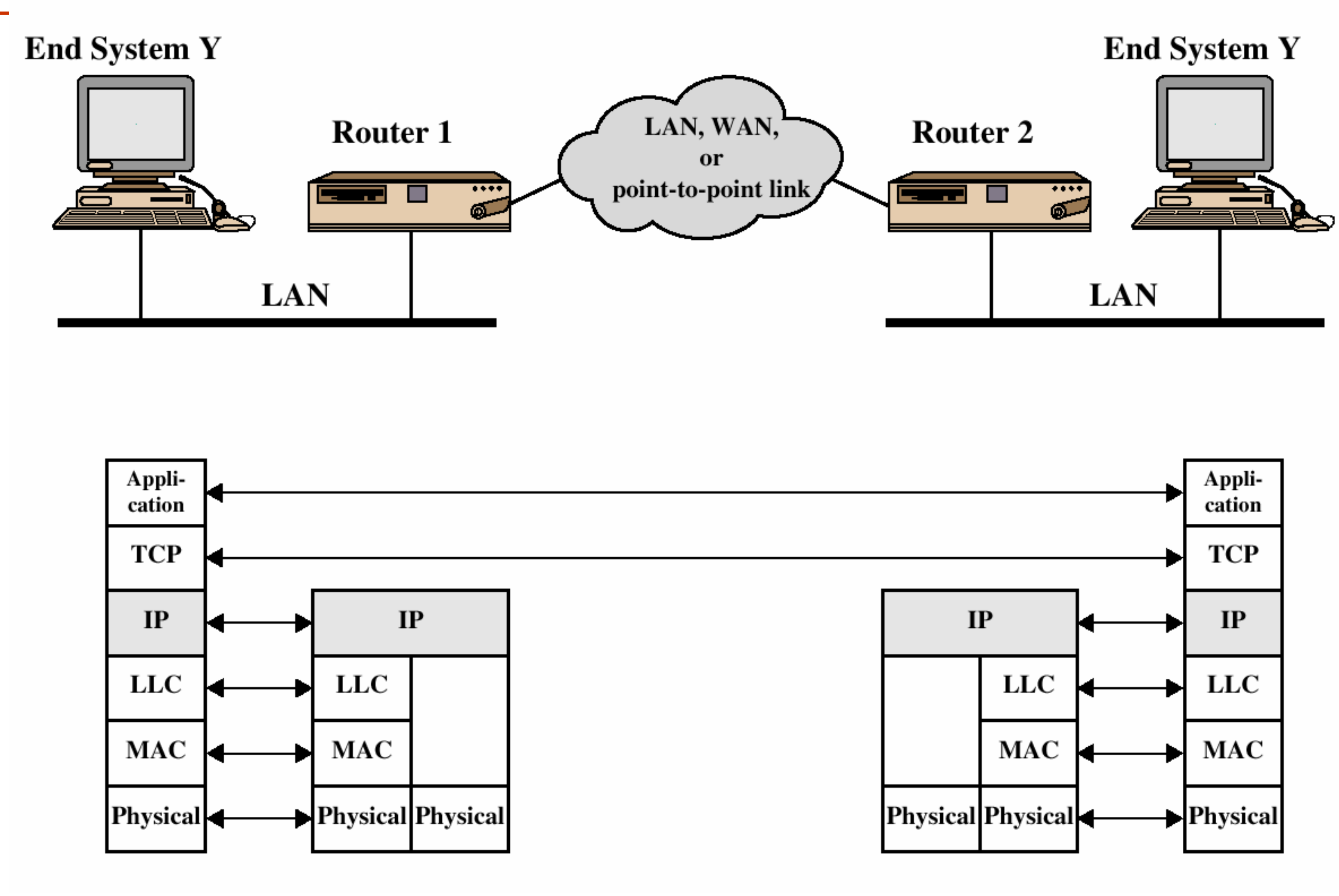
IP Security

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

TCP/IP Example



IP Security

- 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

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

IPSec

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

Benefits of IPSec

- in a firewall/router provides strong security to all traffic crossing the perimeter
- in a firewall/router is resistant to bypass
- is below transport layer, hence transparent to applications
- can be transparent to end users
- can provide security for individual users
- secures routing architecture

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

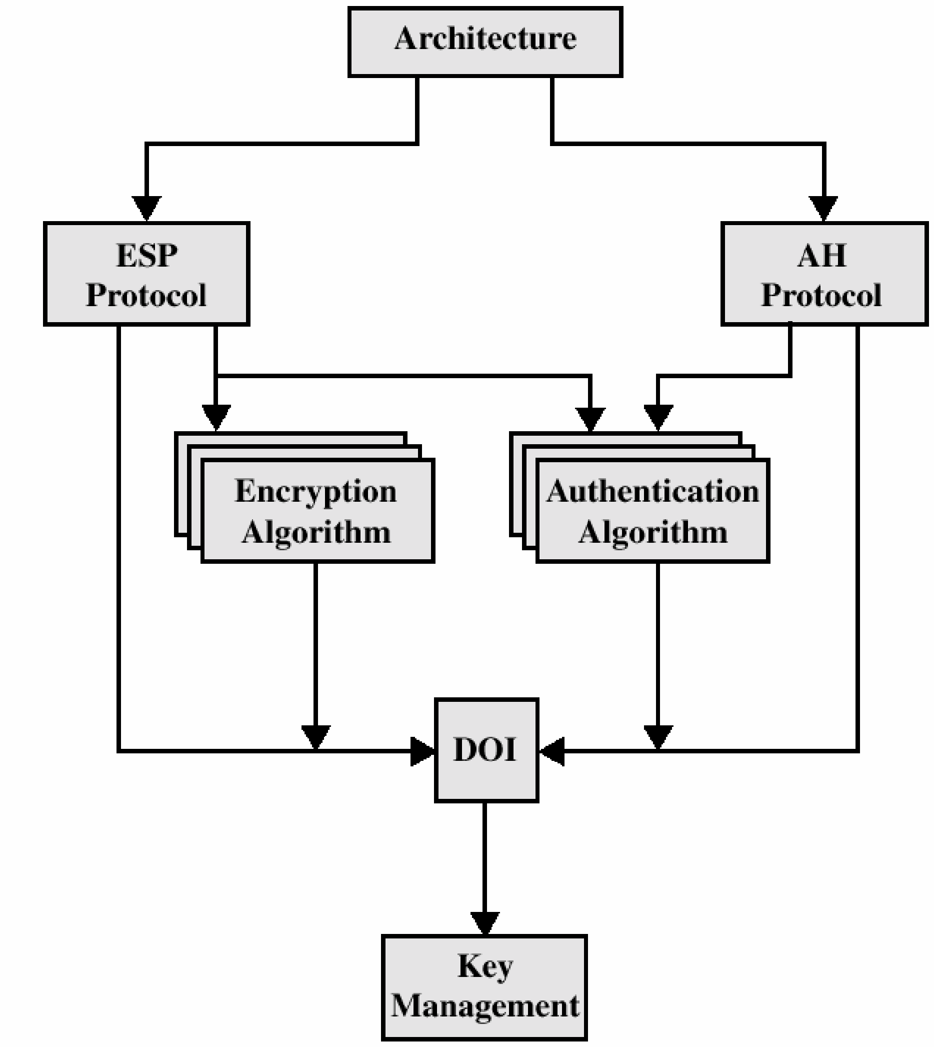
IPSec Services

- Access control
- Connectionless integrity
- Data origin authentication
- Rejection of replayed packets
  - a form of partial sequence integrity
- Confidentiality (encryption)
- Limited traffic flow confidentiality

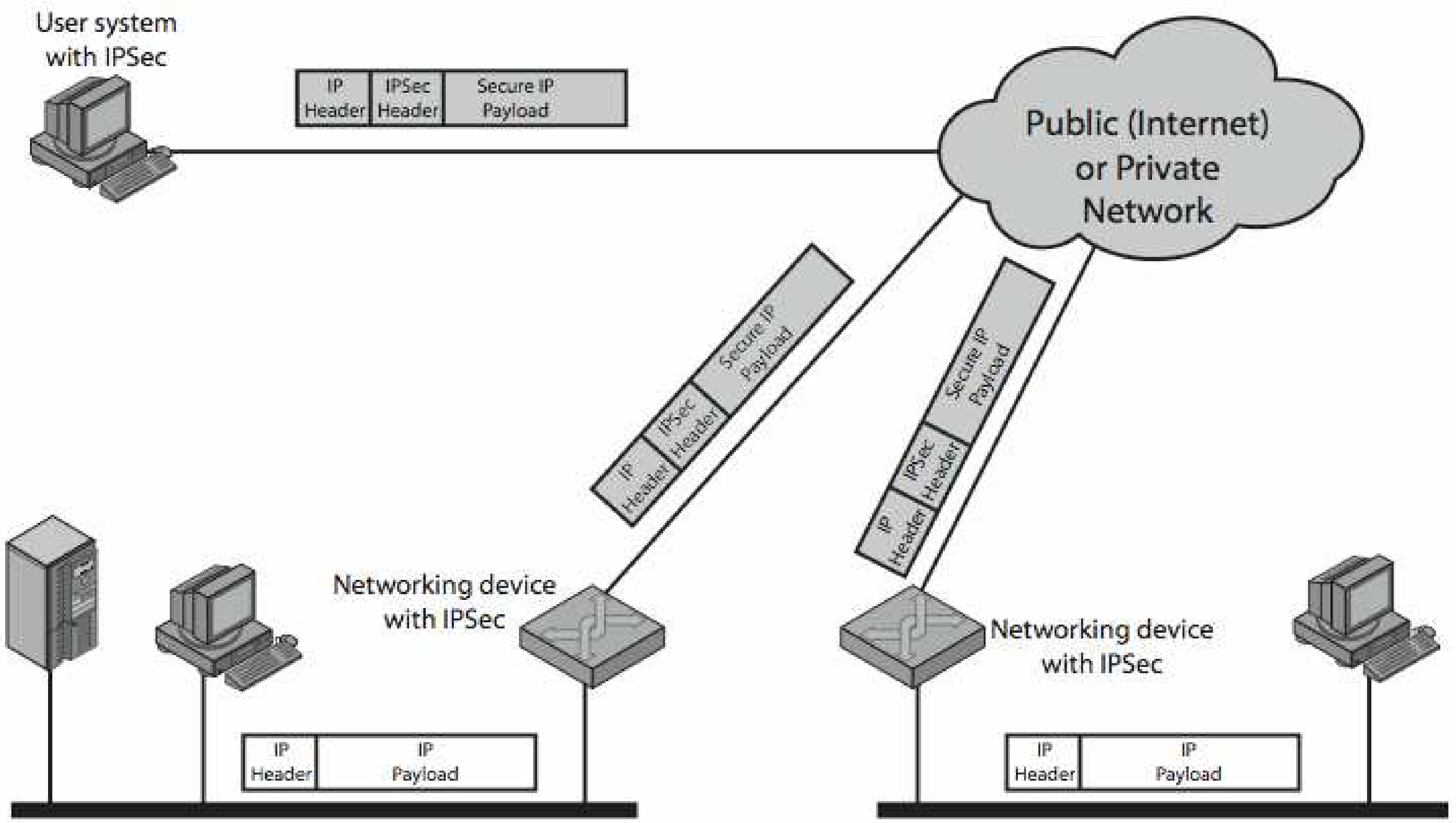
IP Security RFCs

- 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

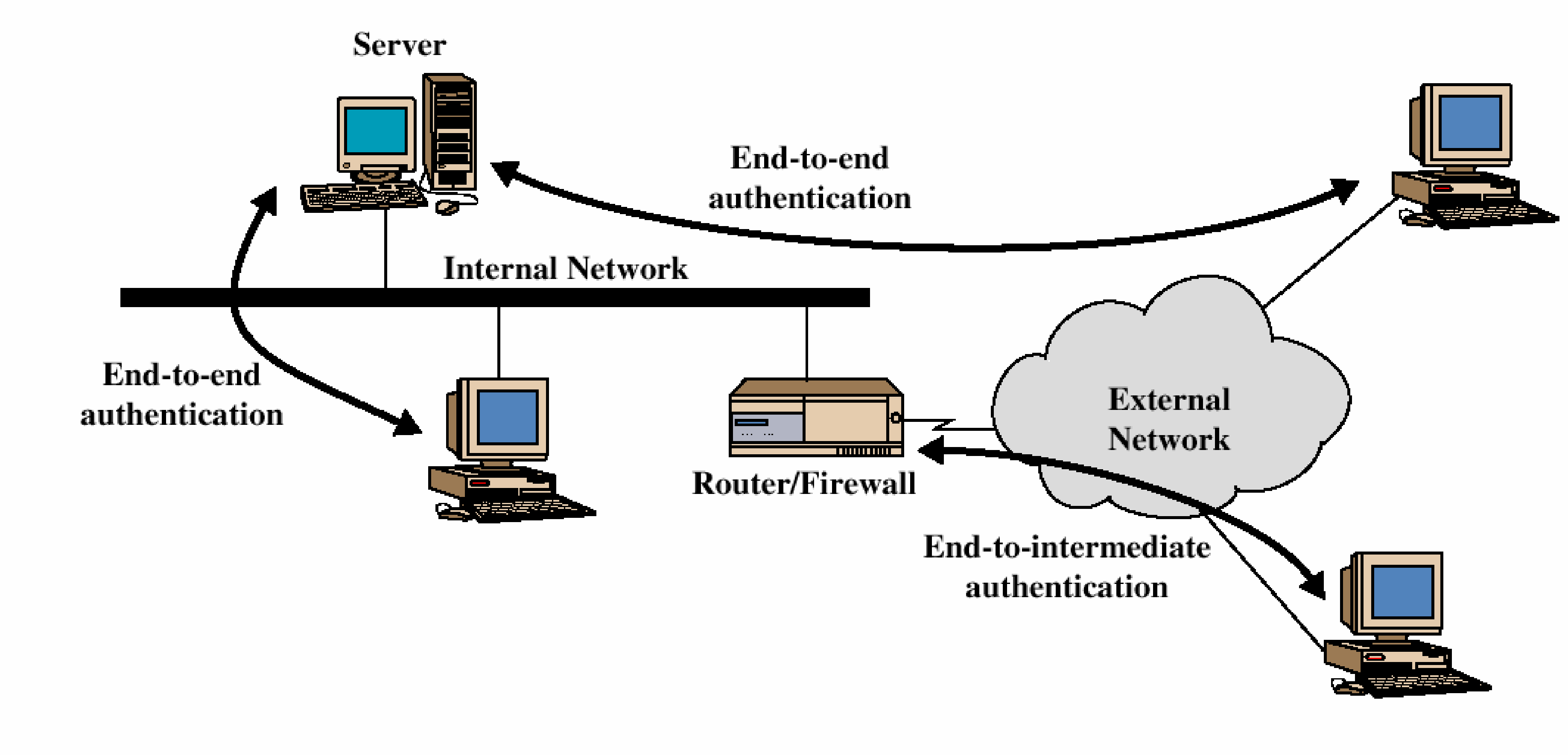
IPSec Document Overview



IPSec Uses


User system with IPSec
IP Header
IPSec Header
Secure IP Payload
Public (Internet) or Private Network
IP Header
IPSec Header
Secure IP Payload
IP Header
IPSec Header
Secure IP Payload
Networking device with IPSec
Networking device with IPSec
IP Header
IP Payload
IP Header
IP Payload

Transport & Tunnel Modes



IP Security Architecture

- specification is quite complex
- mandatory in IPv6, optional in IPv4
- have two security header extensions:
  - Authentication Header (AH)
  - Encapsulating Security Payload (ESP)

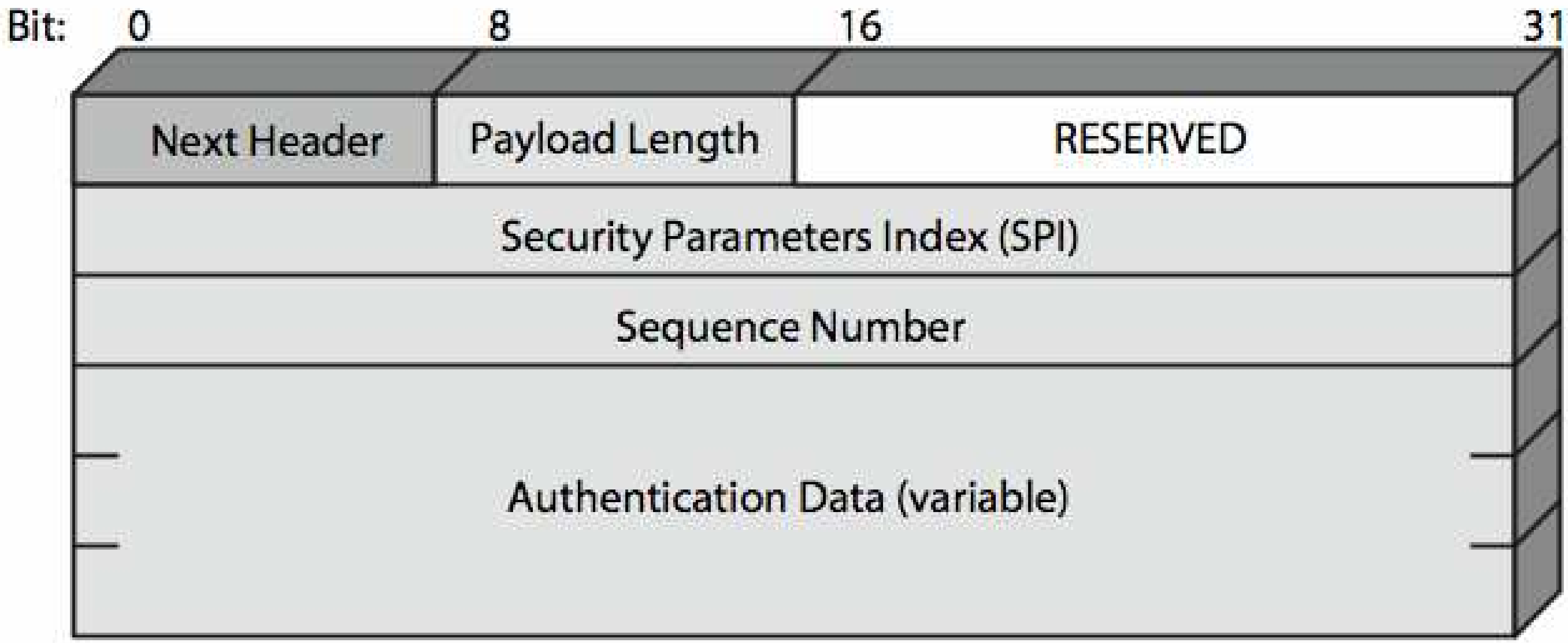
Security Associations

- a one-way relationship between sender & receiver that affords security for traffic flow
- identified by 3 parameters:
  - Security Parameters Index (SPI), like SA ID
  - IP Destination Address
  - Security Protocol Identifier, AH or ESP used
- 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

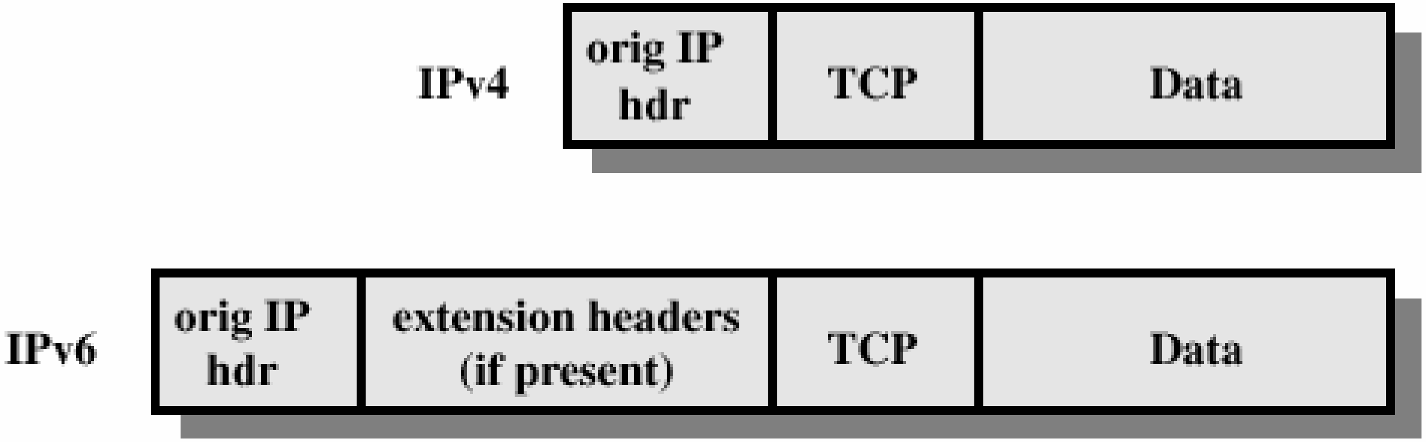
Next Header | Payload Length | RESERVED

Security Parameters Index (SPI)

Sequence Number

Authentication Data (variable)

Before applying AH



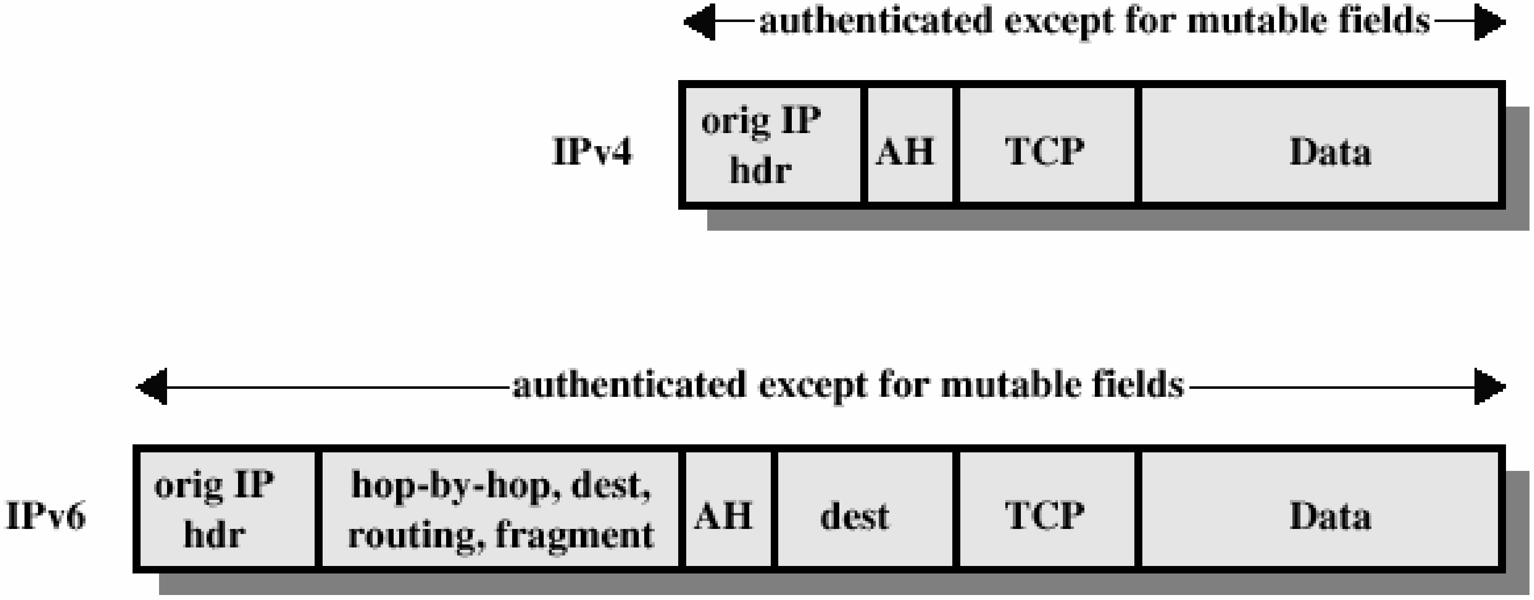
IPv4

orig IP hdr | TCP | Data

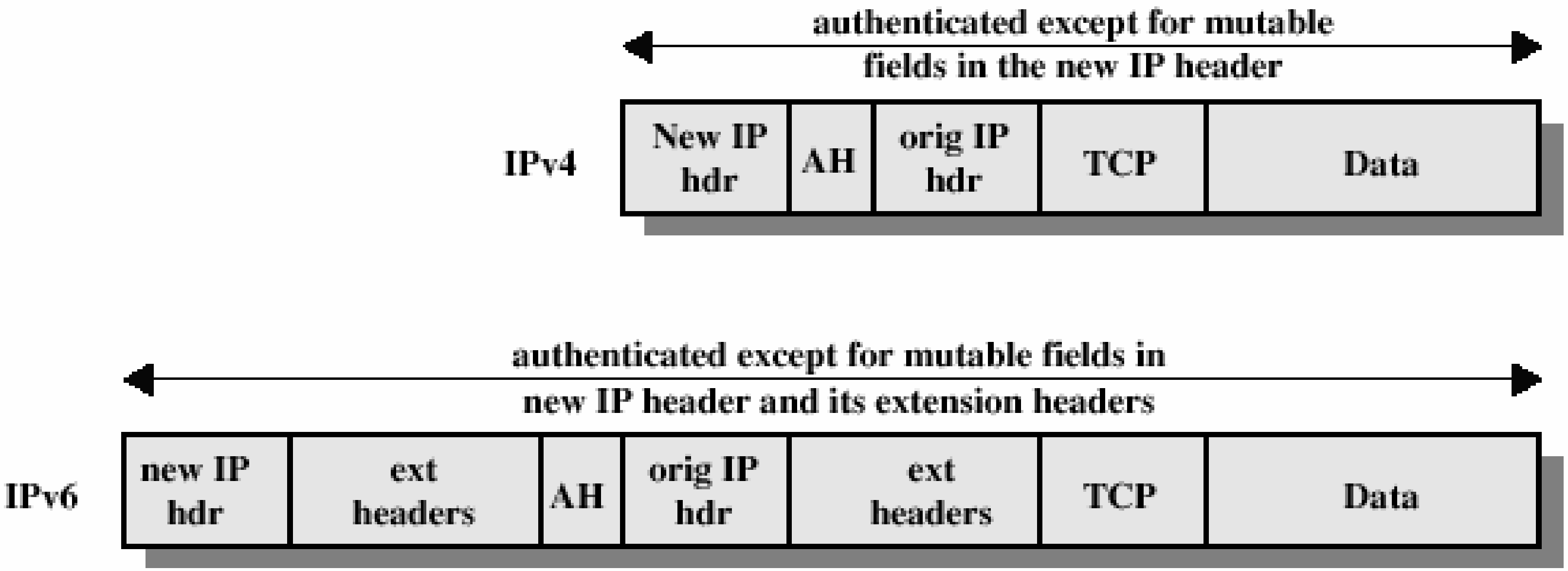
IPv6

orig IP hdr | extension headers (if present) | TCP | Data

Transport Mode (AH Authentication)


authenticated except for mutable fields
IPv4
orig IP hdr
AH
TCP
Data
authenticated except for mutable fields
IPv6
orig IP hdr
hop-by-hop, dest, routing, fragment
AH
dest
TCP
Data

Tunnel Mode (AH Authentication)



authenticated except for mutable fields in the new IP header

IPv4	New IP hdr	AH	orig IP hdr	TCP	Data

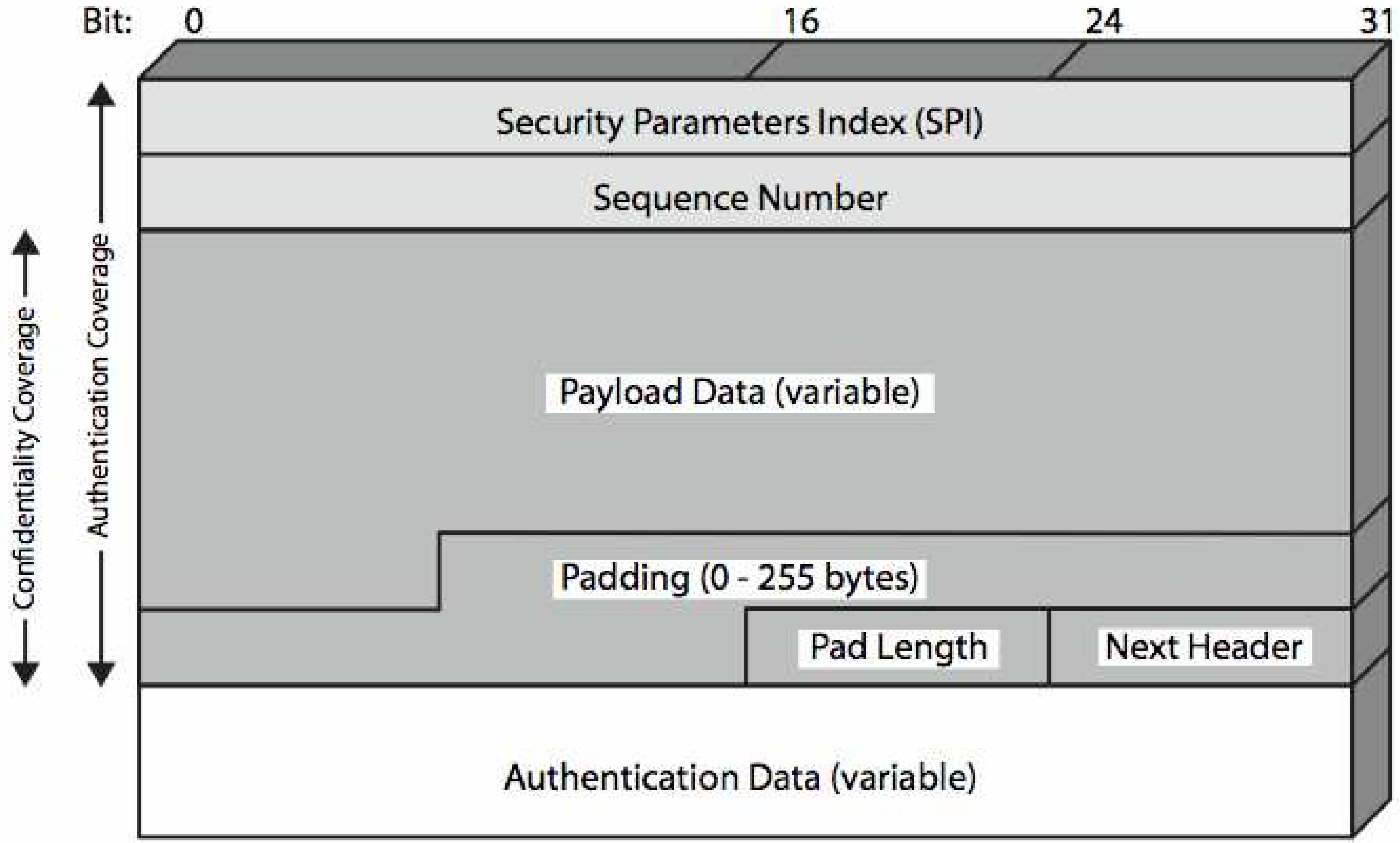
authenticated except for mutable fields in new IP header and its extension headers

IPv6	new IP hdr	ext headers	AH	orig IP hdr	ext headers	TCP	Data

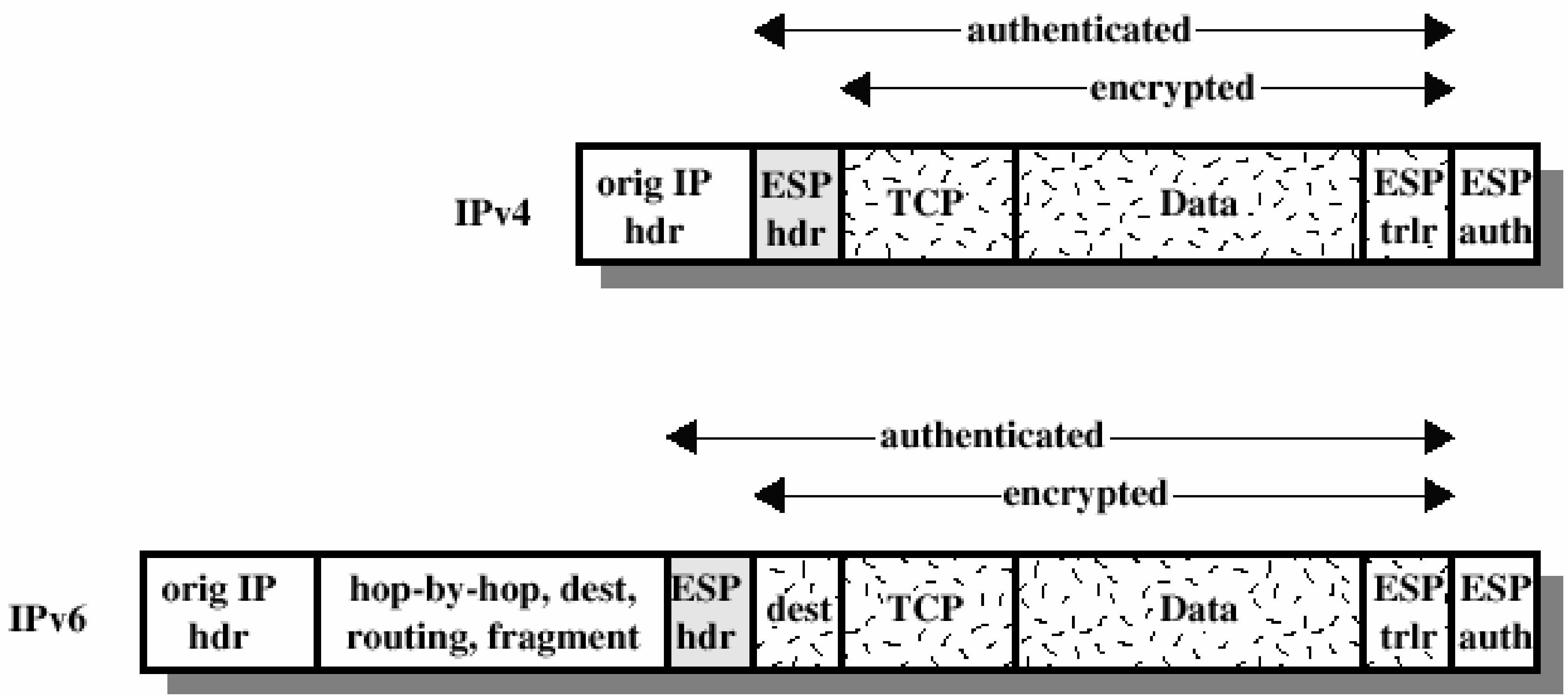
Encapsulating Security Payload (ESP)

- 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 & other modes
  - padding needed to fill blocksize, fields, for traffic flow

Encapsulating Security Payload

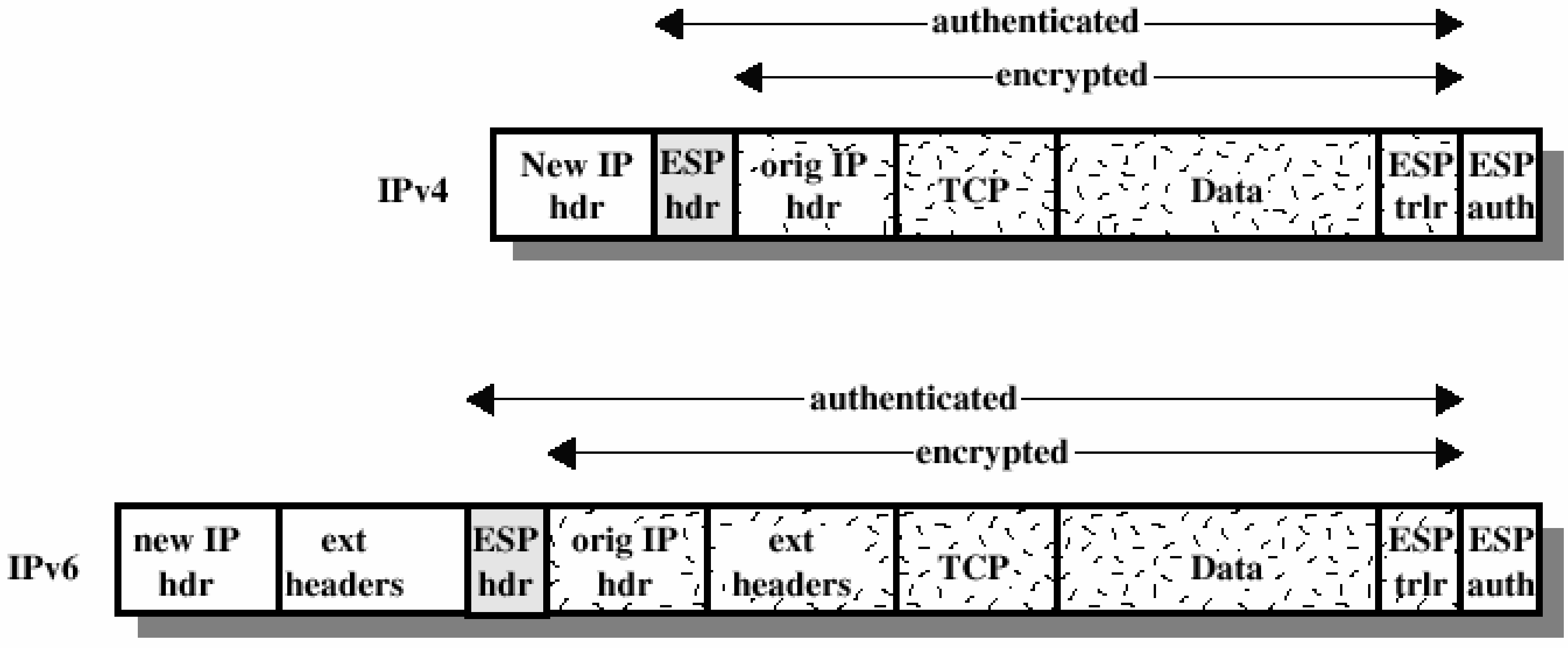


ESP Encryption and Authentication



(a) Transport Mode

ESP Encryption and Authentication



(b) Tunnel Mode

Encryption and Authentication Algorithms in EPS

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

Transport vs Tunnel Mode ESP

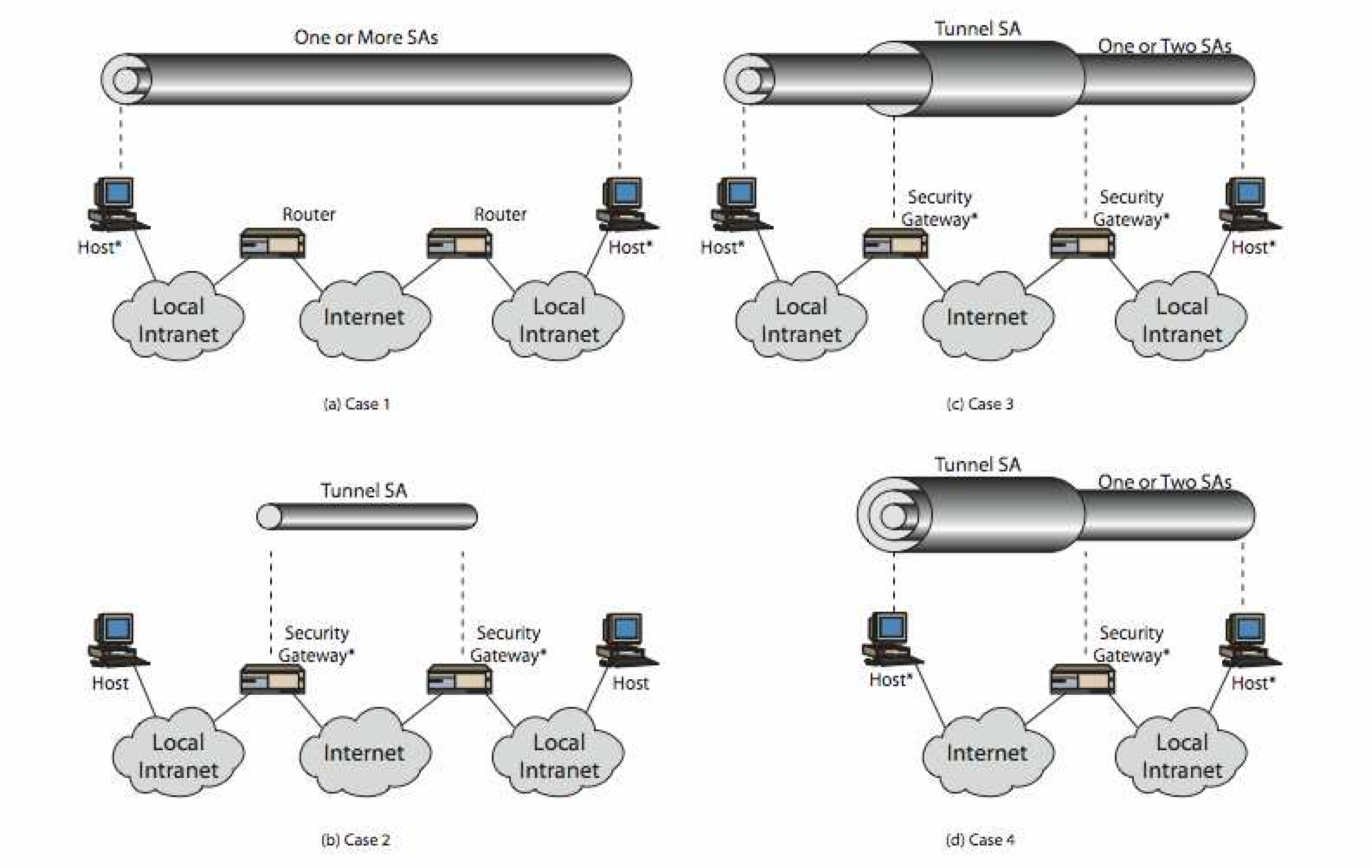
- transport mode is used to encrypt & optionally authenticate IP data
  - data protected but header left in clear
  - can do traffic analysis but is efficient
  - good for ESP host to host traffic
- tunnel mode encrypts entire IP packet
  - add new header for next hop
  - good for VPNs, gateway to gateway security

	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.

Combining Security Associations

- SA’s can implement either AH or ESP
- to implement both need to combine SA’s
  - form a security association bundle
  - may terminate at different or same endpoints
  - combined by
    - transport adjacency
    - iterated tunneling
- issue of authentication & encryption order

Combining Security Associations



(a) Case 1

(c) Case 3

(b) Case 2

(d) Case 4

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

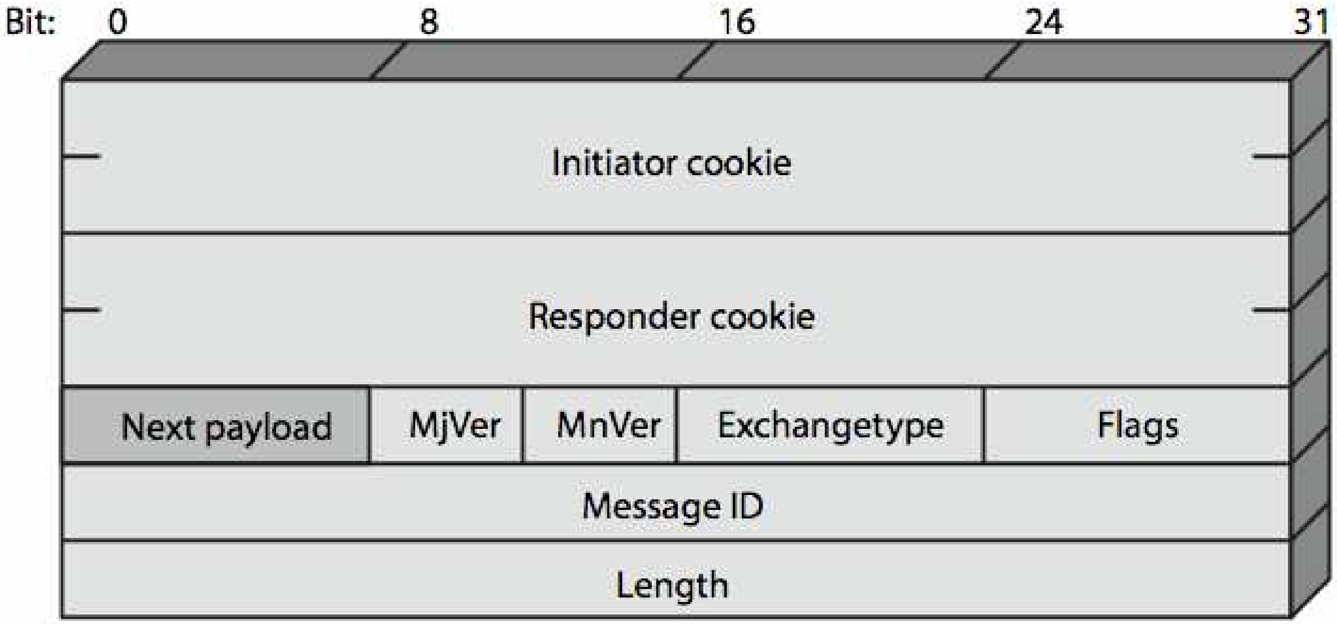
- a key exchange protocol
- based on Diffie-Hellman key exchange
- adds features to address weaknesses
  - cookies, groups (global params), nonces, DH key exchange with authentication
- can use arithmetic in prime fields or elliptic curve fields

ISAKMP

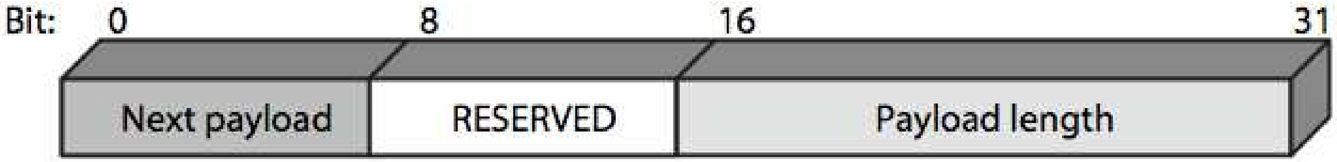
- Internet Security Association and Key Management Protocol
- provides framework for key management
- defines procedures and packet formats to establish, negotiate, modify, & delete SAs
- independent of key exchange protocol, encryption alg, & authentication method

ISAKMP

-



(a) ISAKMP Header



(b) Generic Payload Header

ISAKMP Payloads & Exchanges

- have a number of ISAKMP payload types:
  - Security, Proposal, Transform, Key, Identification, Certificate, Certificate, Hash, Signature, Nonce, Notification, Delete
- ISAKMP has framework for 5 types of message exchanges:
  - base, identity protection, authentication only, aggressive, informational