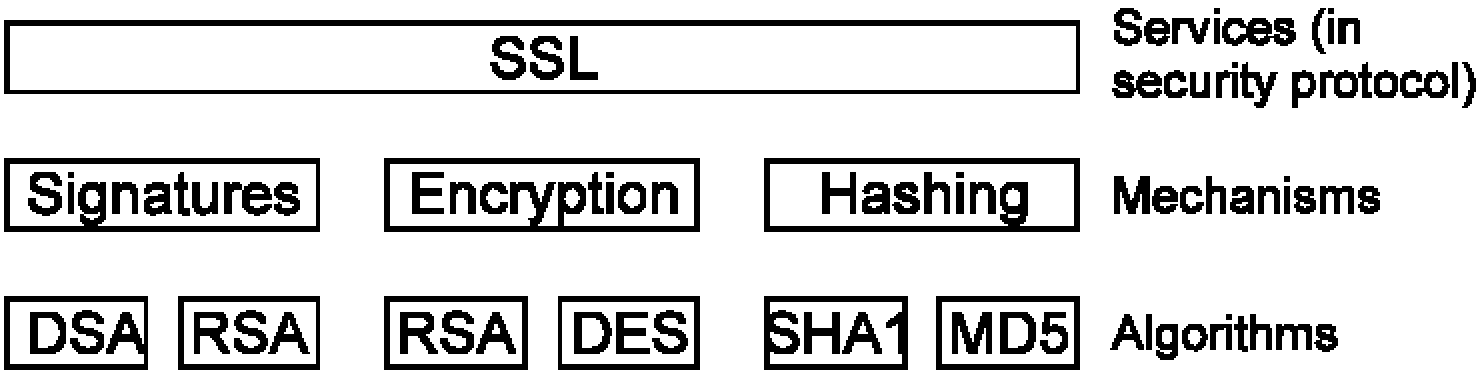
IPSec

IPSec provides the capability to secure communications across a LAN, across private and public wide area networks (WANs) and across the Internet

Services, Mechanisms, Algorithms

- A typical security protocol provides one or more services
- Services are built from mechanisms
- Mechanisms are implemented using algorithms



SSL

Services (in security protocol)

Signatures

Encryption

Hashing

Mechanisms

DSA

RSA

RSA

DES

SHA1

MD5

Algorithms

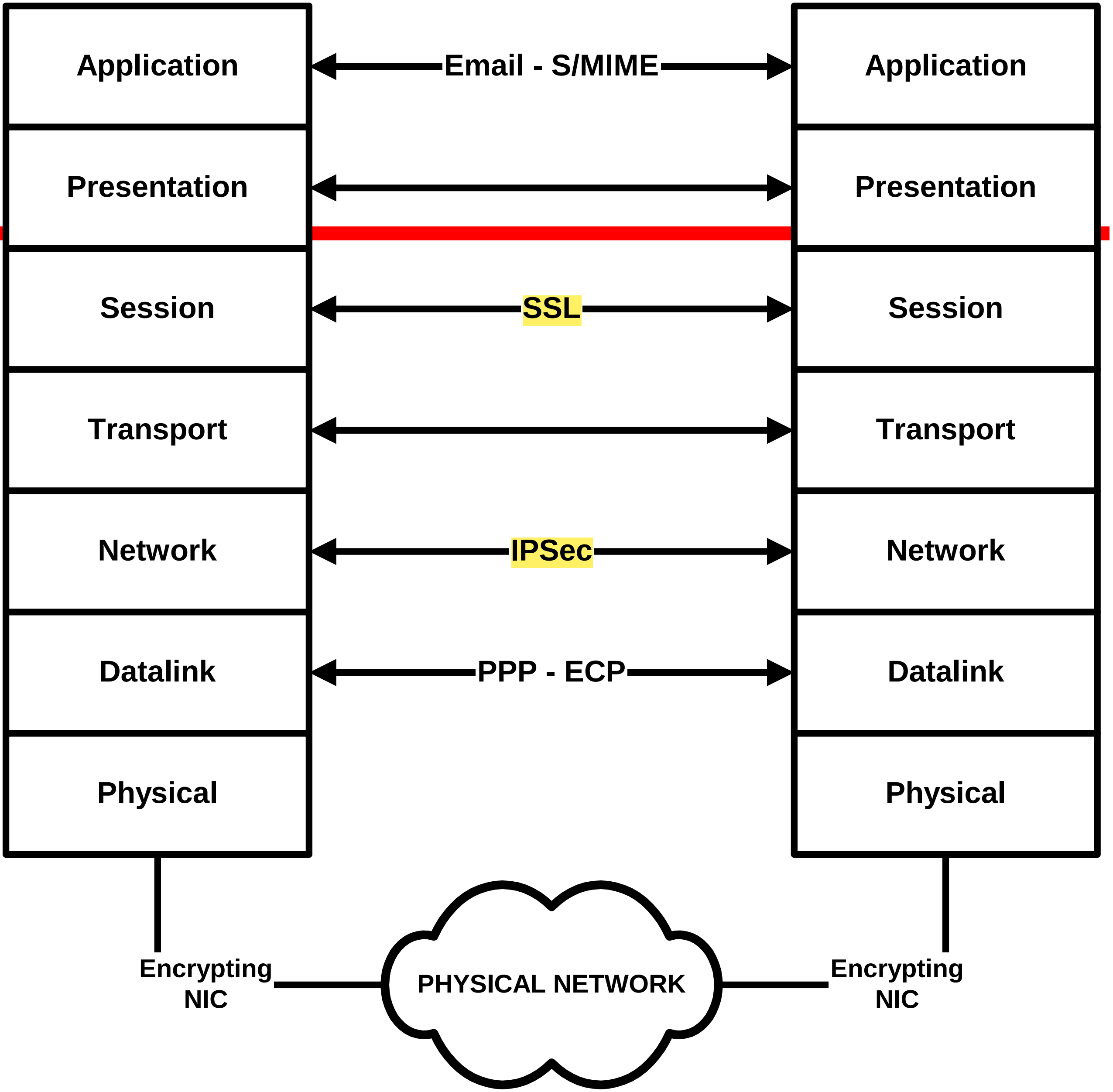
Security in the Internet Architecture

- Lack of security in the Internet Architecture
- Security was left up to the applications
- With the passage of time it was realized that universal security at the IP level will become a need and not a luxury

Security Protocol Layers

- The further down you go, the more transparent it is

- The further up you go, the easier it is to deploy



Some Pros of Security at the IP Level

- Can be end to end or at least multilink unlike link layer
- Could be hw/sw supported (hw support for encryption)
- Can shield unmodified host apps giving them crypto/security at the level of nets/hosts/and possibly users
- Can extend secure enclave across insecure areas

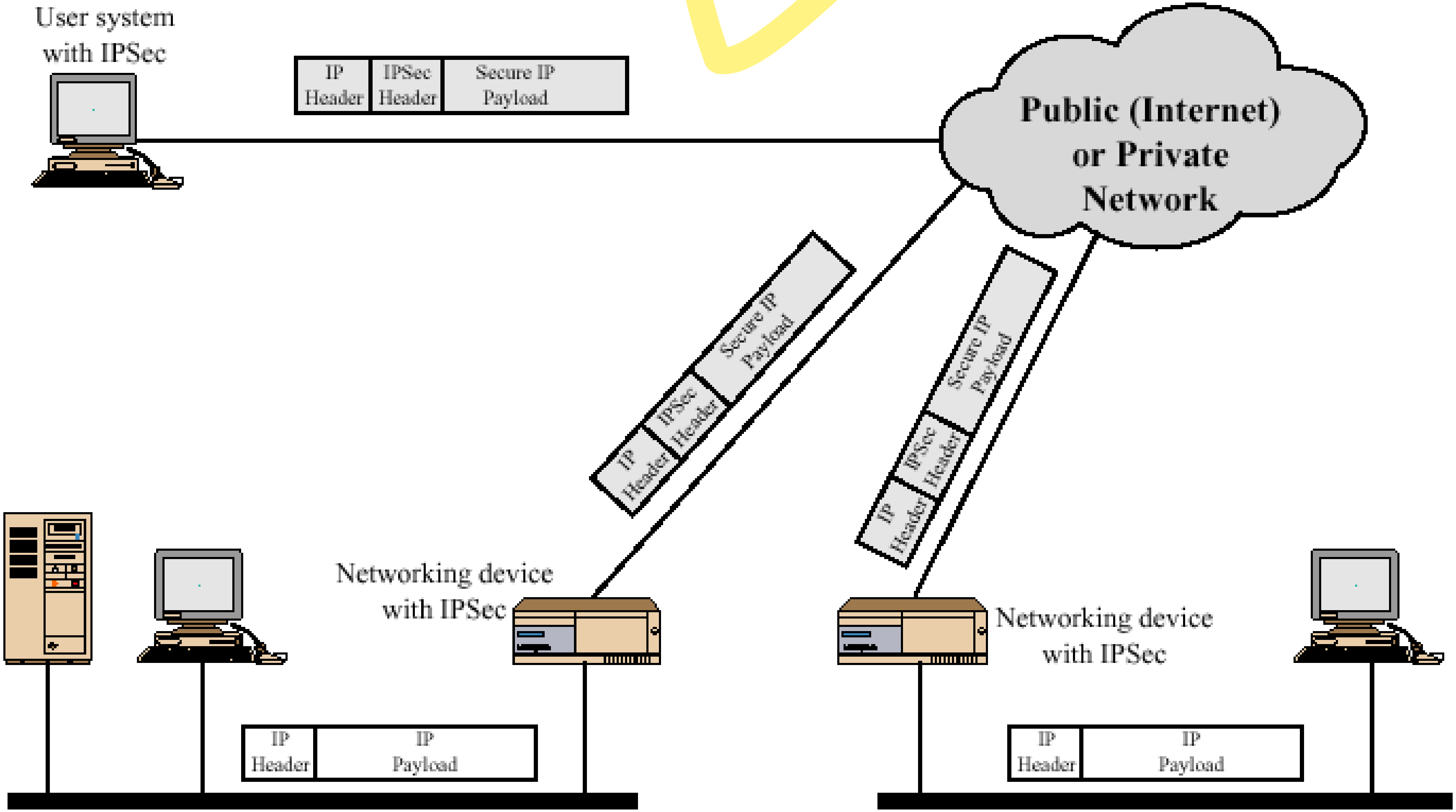
What is IPSec?

- Extensions to the basis Internet Protocol to provide security functions at the IP level
- Applicable to both IP Version 4 and IP Version 6
- IPSec available in Windows 2000, Linux, Cisco Routers, etc.

How do you know IPSec is there?

- AH/ESP new IP layer protocols (50/51) with either
  - 1. an IP datagram encapsulated in them (tunnel mode)
  - 2. TCP/UDP and the rest above them (transport mode)
- Every packet may have AH/ESP applied to them:
  - AH for authentication;
  - ESP for encryption and authentication, this is bulk/perpacket encryption/authentication

IP Security Usage Scenario

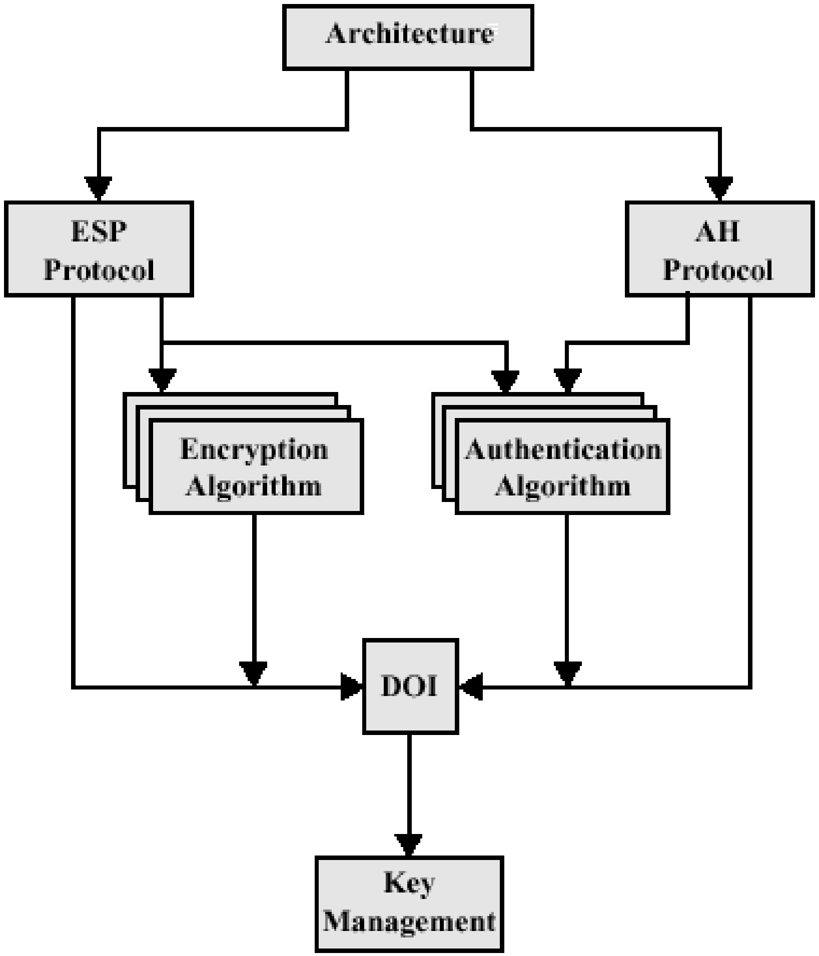


Applications of IPSec

- ⌘Secure Branch Office Connectivity Over the Internet
- ⌘Secure Remote Access Over the Internet
- ⌘Establishing Extranet and Intranet Connectivity with Business partners
- ⌘Enhancing Electronic Commerce Security

IPSec Documents Overview

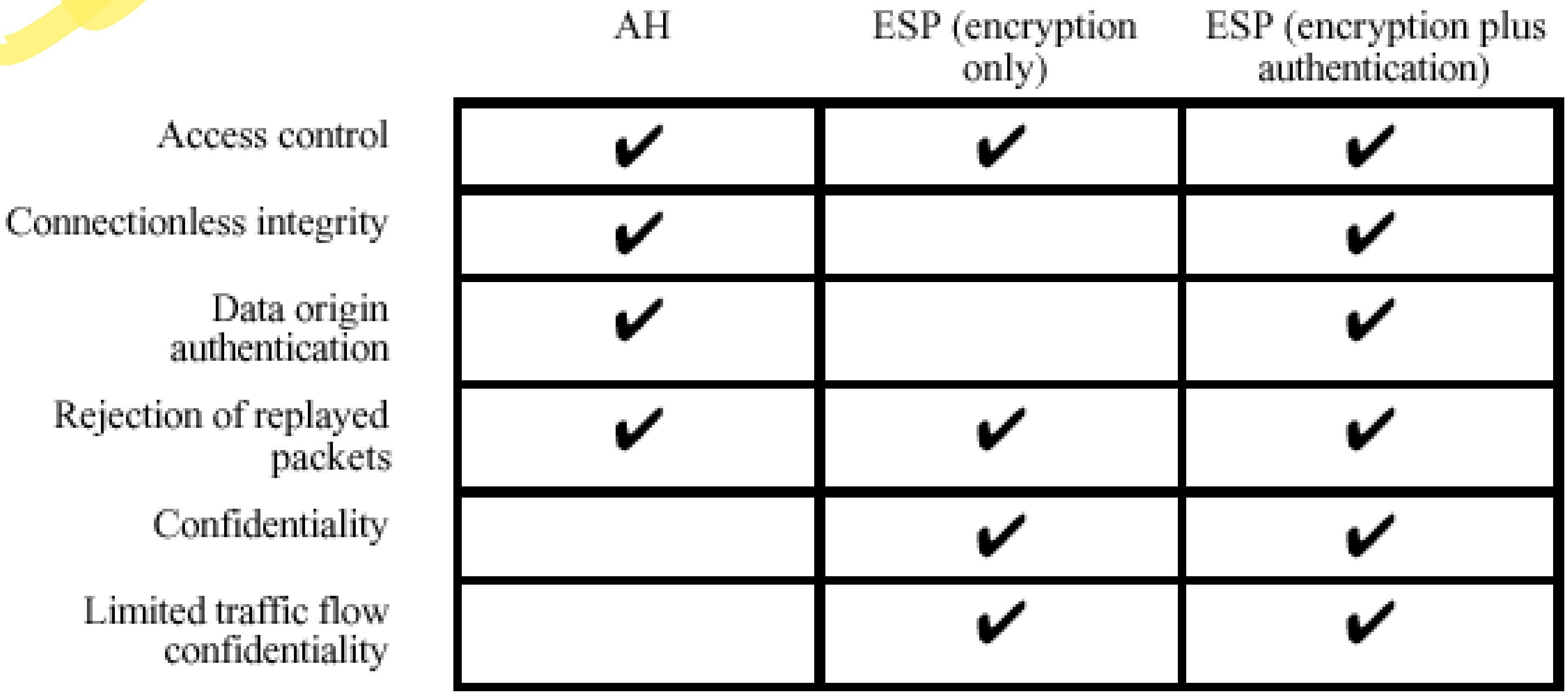
- **Relevant RFCs**
- RFC 1825: An overview of a security architecture
- RFC 1826: Description of a packet authentication extension to IP
- RFC 1828: A specific authentication mechanism
- RFC 1827: Description of a packet encryption extension to IP
- RFC 1829: A specific encryption mechanism



AH and ESP

- **AH**
  - The Authentication Header provides support for data integrity and authentication of IP packets
- **ESP**
  - The Encapsulating Security Payload provides confidentiality services, including confidentiality of message contents and limited traffic flow confidentiality. As an optional feature, ESP can also provide the same authentication service as AH.

IPSec Services



	AH	ESP (encryption only)	ESP (encryption plus authentication)
Access control	✓	✓	✓
Connectionless integrity	✓		✓
Data origin authentication	✓		✓
Rejection of replayed packets	✓	✓	✓
Confidentiality		✓	✓
Limited traffic flow confidentiality		✓	✓

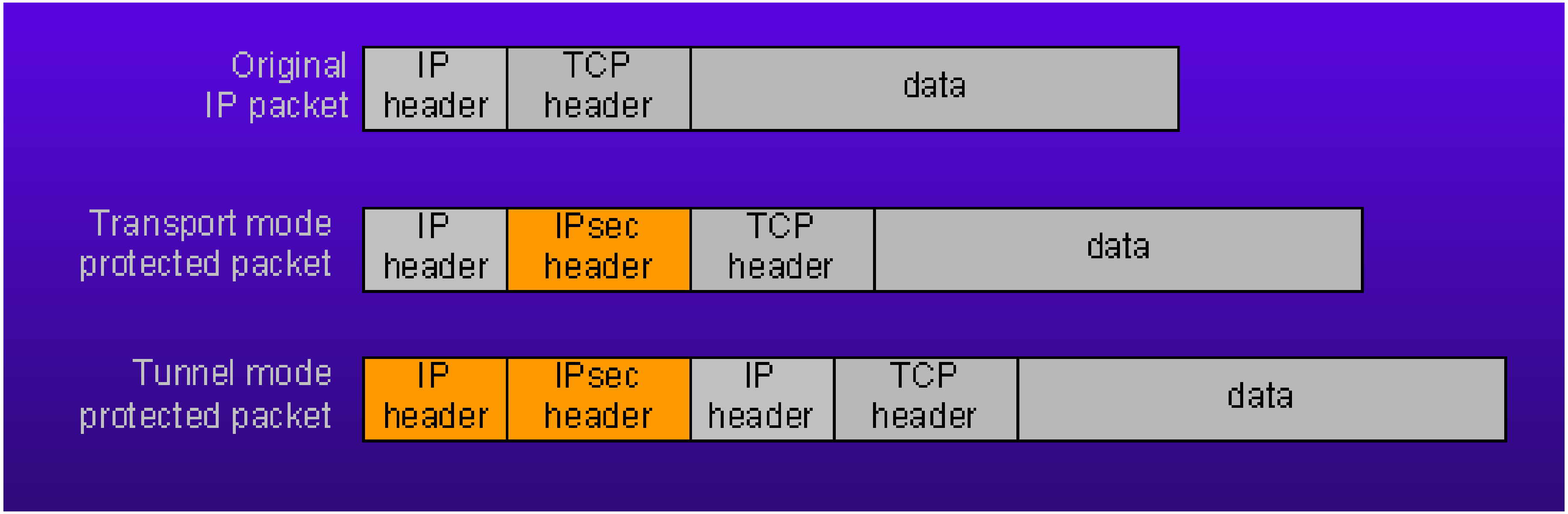
Security Associations

- What is a SA?
  - An SA is a one way relationship between a sender and a received that affords security services to the traffic carried on it.
- SA Parameters
  - Security Association Database stores parameters associated with each of the SAs
- SA Selectors
  - Each SPD entry is defined by a set of IP and upper layer protocol field values called selectors.

Transport and Tunnel Modes

- ⌘Tunnel Mode means that one outgoing IP packet is encapsulated in another packet with typically a different IP destination
- ⌘Tunnels can be (1) Router to Router (2) Router to host or host to router (3) host to host

Transport and Tunnel Modes

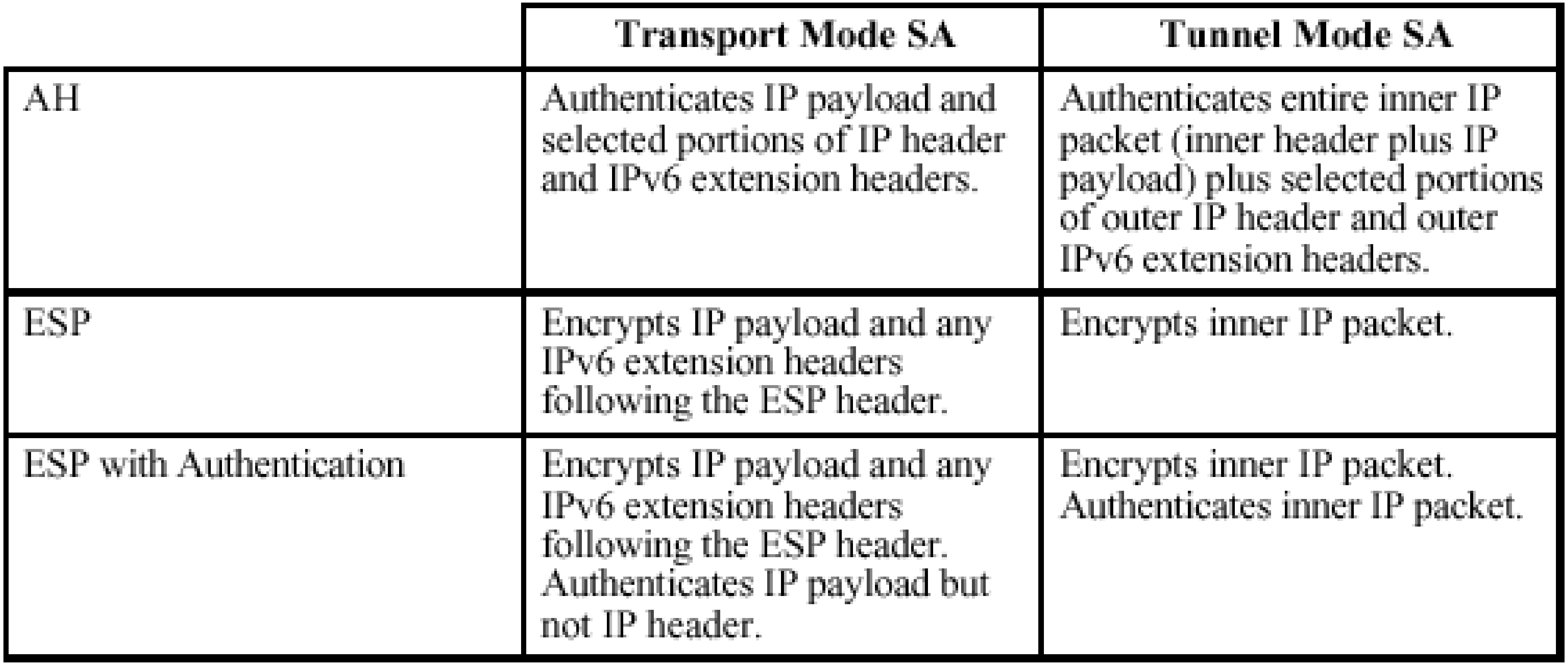


Original IP packet: IP header | TCP header | data

Transport mode protected packet: IP header | IPsec header | TCP header | data

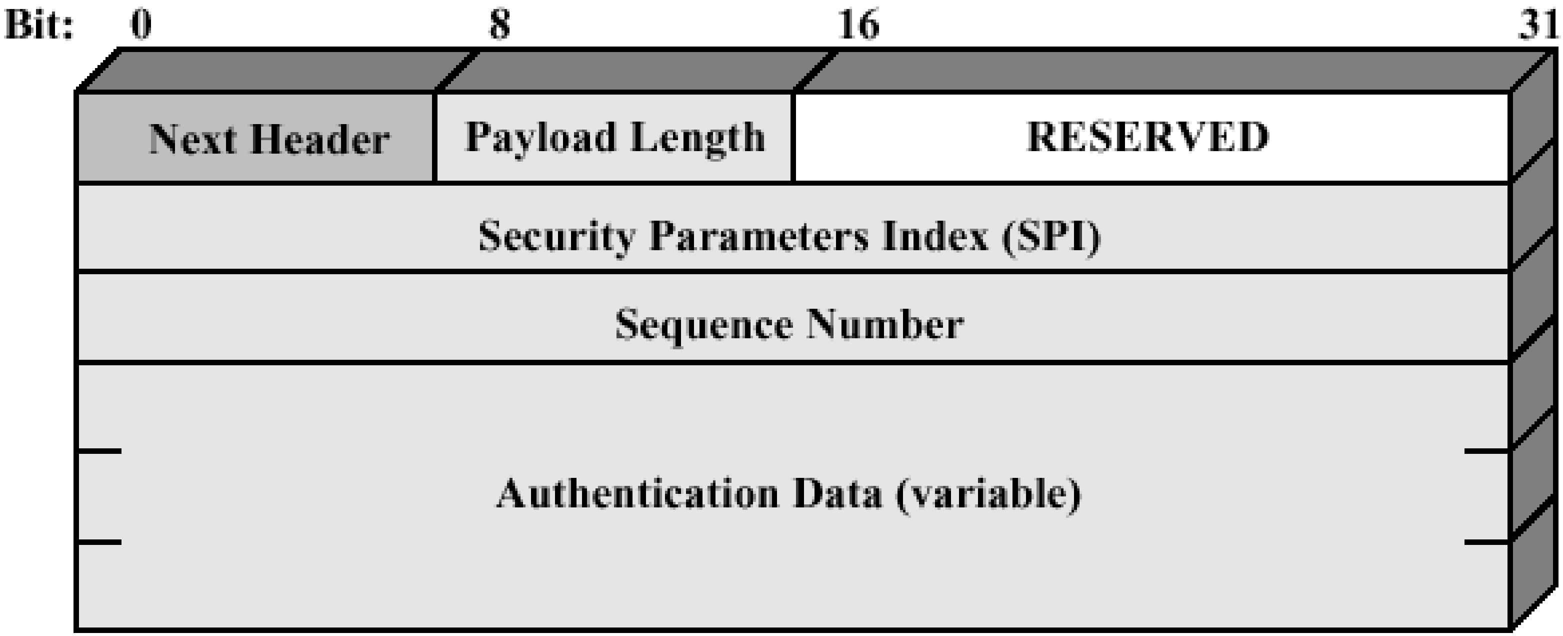
Tunnel mode protected packet: IP header | IPsec header | IP header | TCP header | data

Tunnel Mode and Transport Mode Functionality



	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 (inner header plus IP payload) plus selected portions of outer IP header and outer IPv6 extension headers.
ESP	Encrypts IP payload and any IPv6 extension headers following the ESP header.	Encrypts inner IP packet.
ESP with Authentication	Encrypts IP payload and any IPv6 extension headers following the ESP header. Authenticates IP payload but not IP header.	Encrypts inner IP packet. Authenticates inner IP packet.

Authentication Header

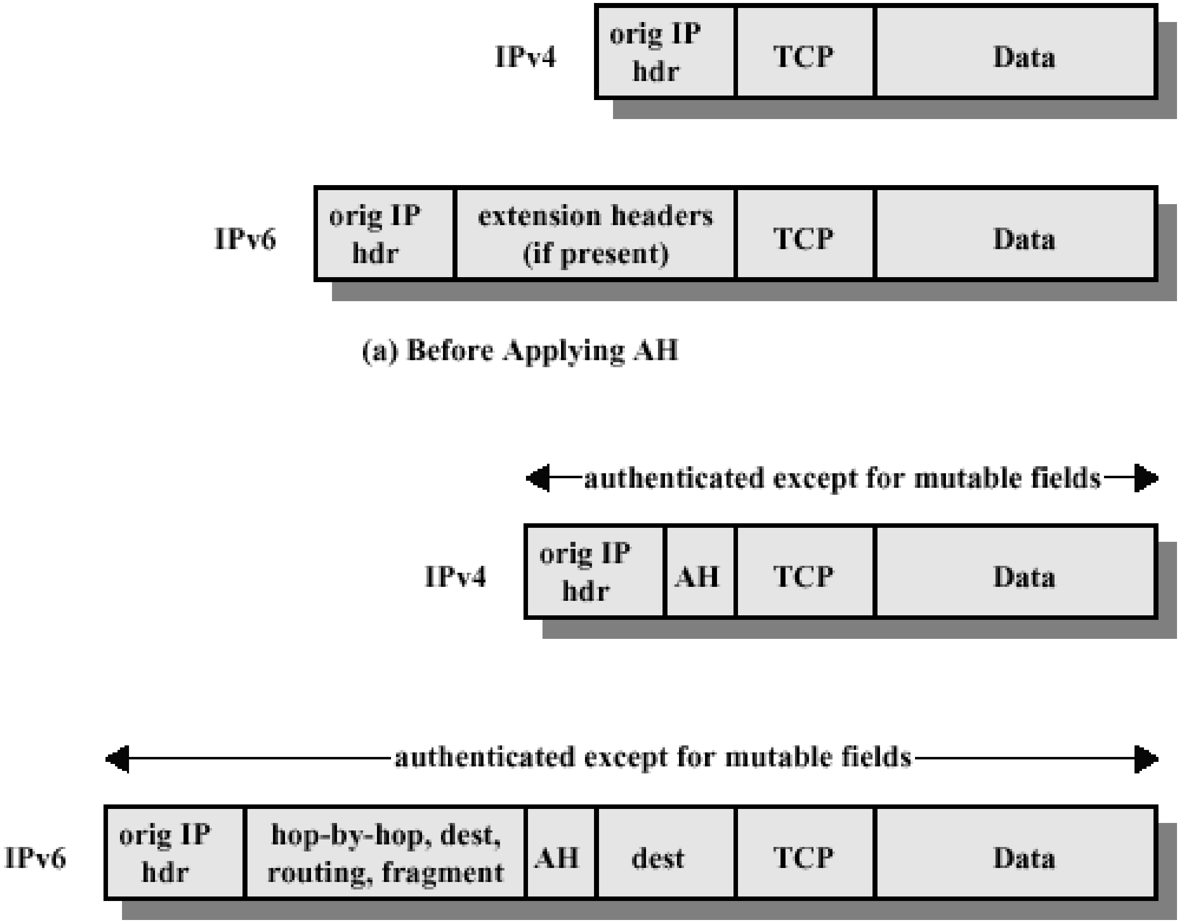


Bit:	0	8	16	31
	Next Header	Payload Length	RESERVED	
	Security Parameters Index (SPI)			
	Sequence Number			
	Authentication Data (variable)			

Services Provided by AH

- ⌘Anti-Replay Service
- ⌘Integrity Check Value

Scope of Authentication Header



IPv4

orig IP hdr | TCP | Data

IPv6

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

(a) Before Applying AH

authenticated except for mutable fields

IPv4

orig IP hdr | AH | TCP | Data

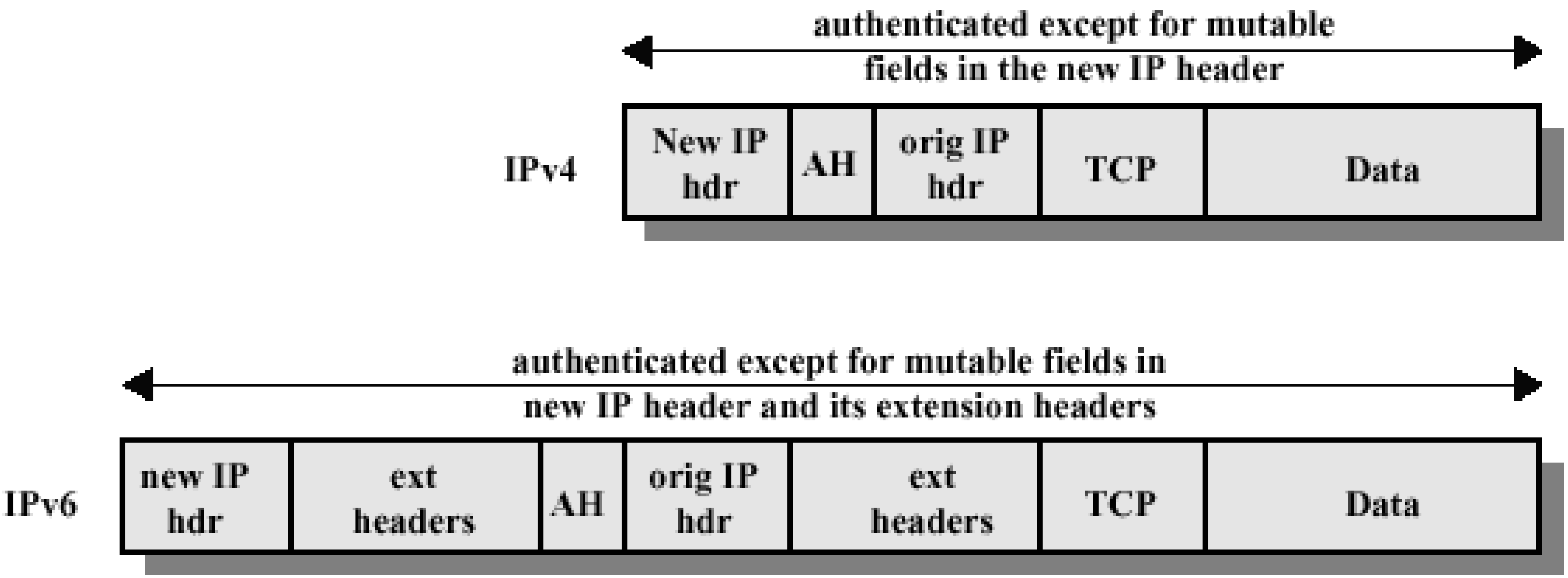
authenticated except for mutable fields

IPv6

orig IP hdr | hop-by-hop, dest, routing, fragment | AH | dest | TCP | Data

(b) Transport Mode

Scope of Authentication Header



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

- ESP Services
  - Confidentiality
  - Authentication Services
- ESP Format
  - SPI
  - SN
  - PD
  - Padding
  - Pad Length
  - Next Header
  - Authentication Data

Conclusion

- IPSec provides Universal IP level security for all applications
- Two choices are available AH and ESP
- IPSec can be used in a transport mode for end to end authentication and encryption or in tunnel mode for router to router authentication and encryption
- IPSec can be implemented IPV4 as options and is a required part of the implementation of IPV6