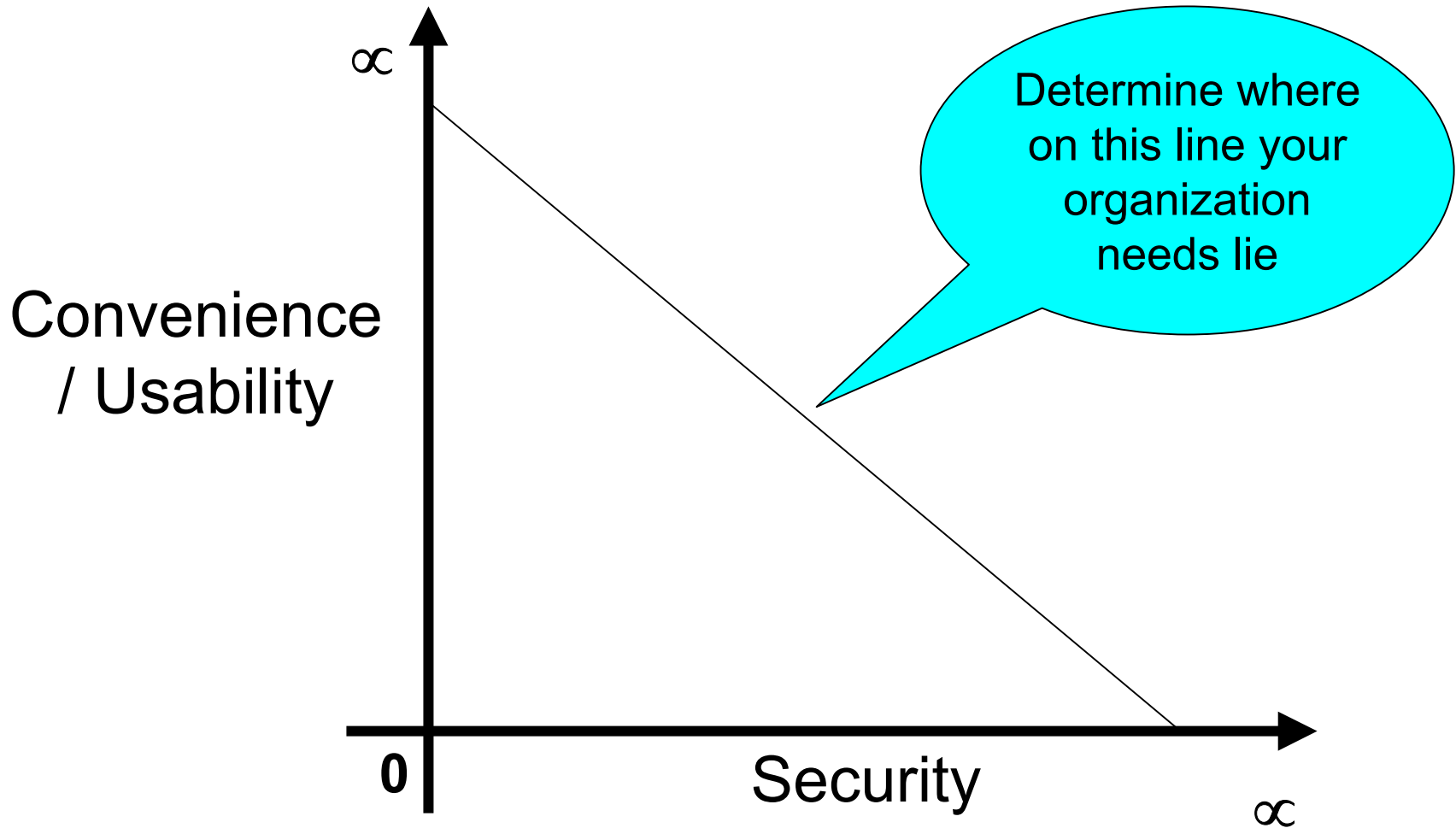


# IPSec

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

# Usability and Security

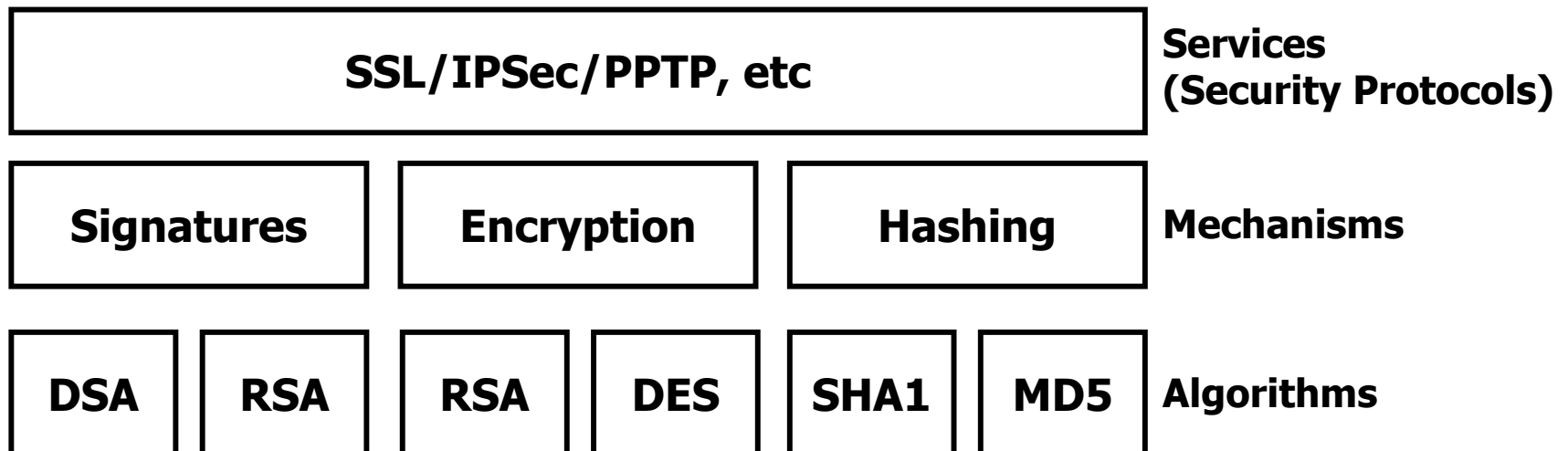
---



# Services, Mechanisms, Algorithms

---

- A typical security protocol provides one or more security services (authentication, secrecy, integrity, etc.)
- Services are built from mechanisms.
- Mechanisms are implemented using algorithms.



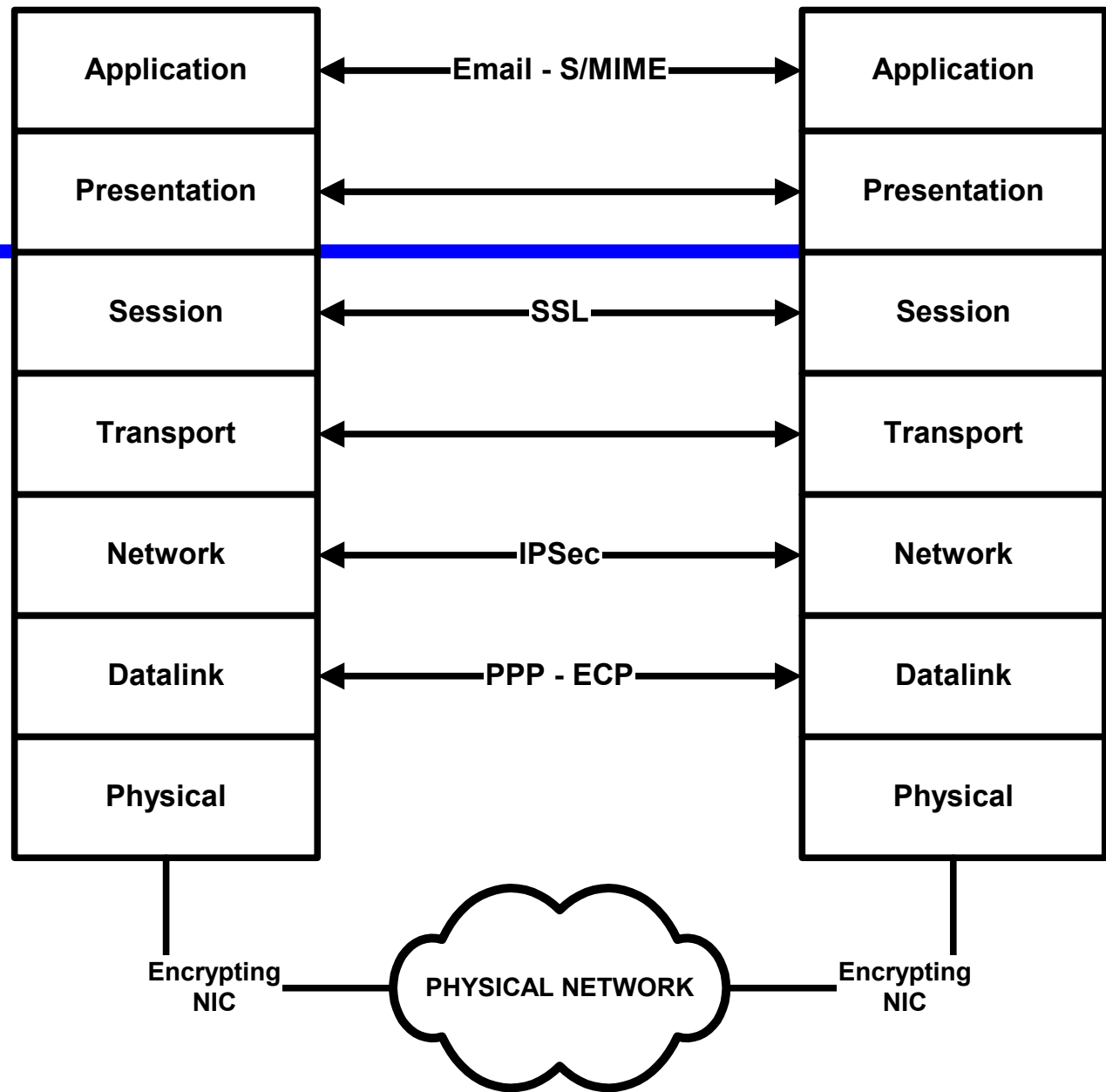
# Security in the Internet Architecture

---

- 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 multi-link 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?

---

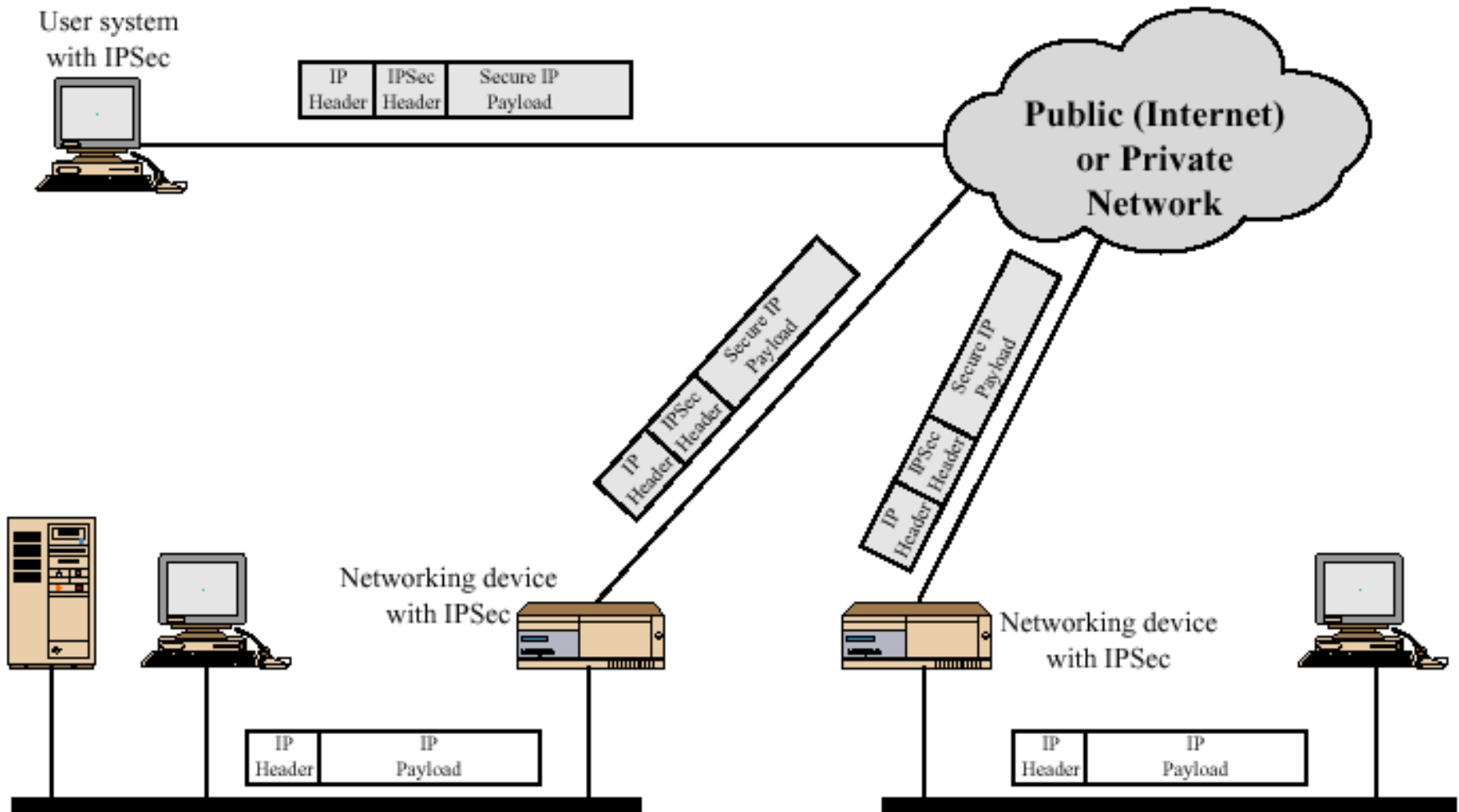
- Extensions to the basis Internet Protocol to provide security functions at the IP level
- Applicable to both IP Version 4 and IP Version 6
- IPSec available in Windows 2000, Linux, Cisco Routers, etc.

# 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/per-packet 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

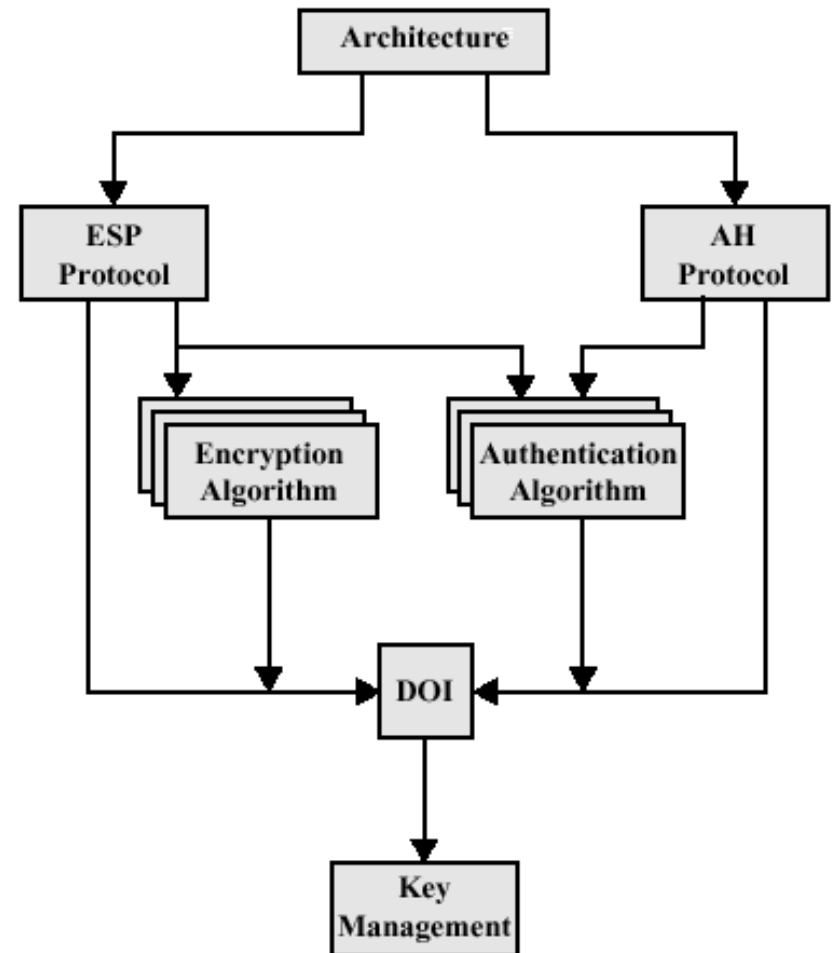
# IP Security Architecture

---

- Defined by IPSec Documents (RFCs)
- IP Security Protocol Working Group of IETF
- IP Security Evolving with the passage of time
- IPSec provides security services at the IP layer by enabling a system to select required security protocols, determine the algorithms to use for the services, and put in place any cryptographic keys required.

# 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 encryptior 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 receiver 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.

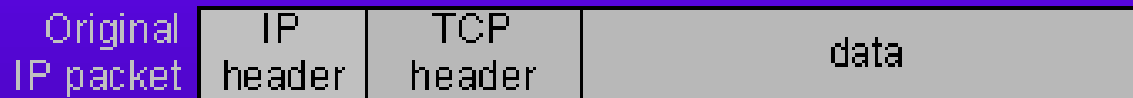
# Transport and Tunnel Modes

---

- 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

---



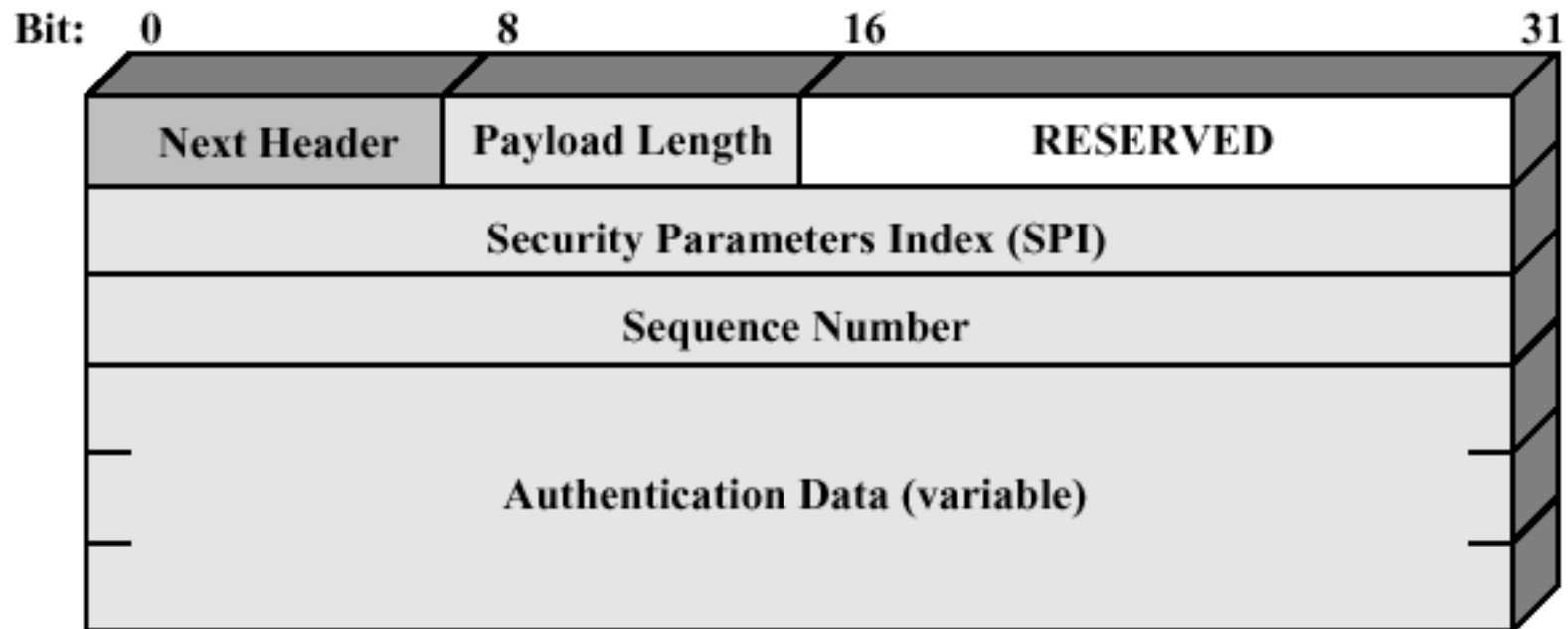
# Tunnel Mode and Transport Mode Functionality

---

	<b>Transport Mode SA</b>	<b>Tunnel Mode SA</b>
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

---



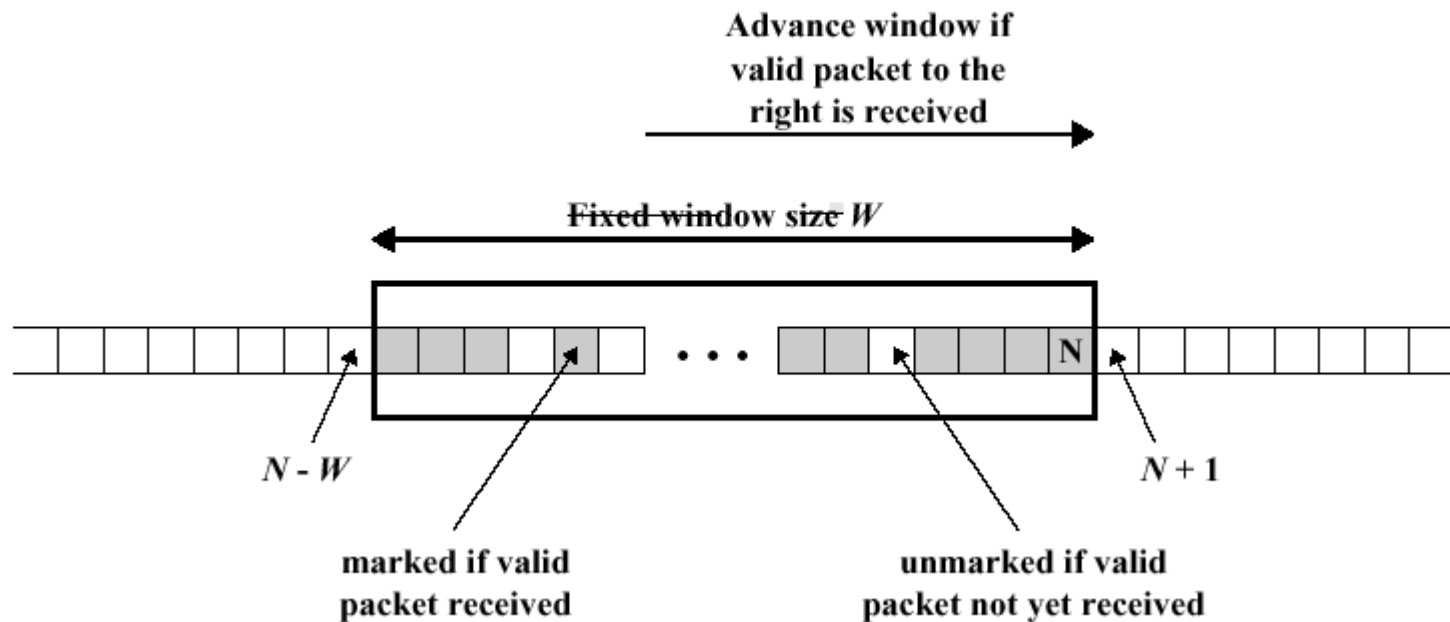
# Services Provided by AH

---

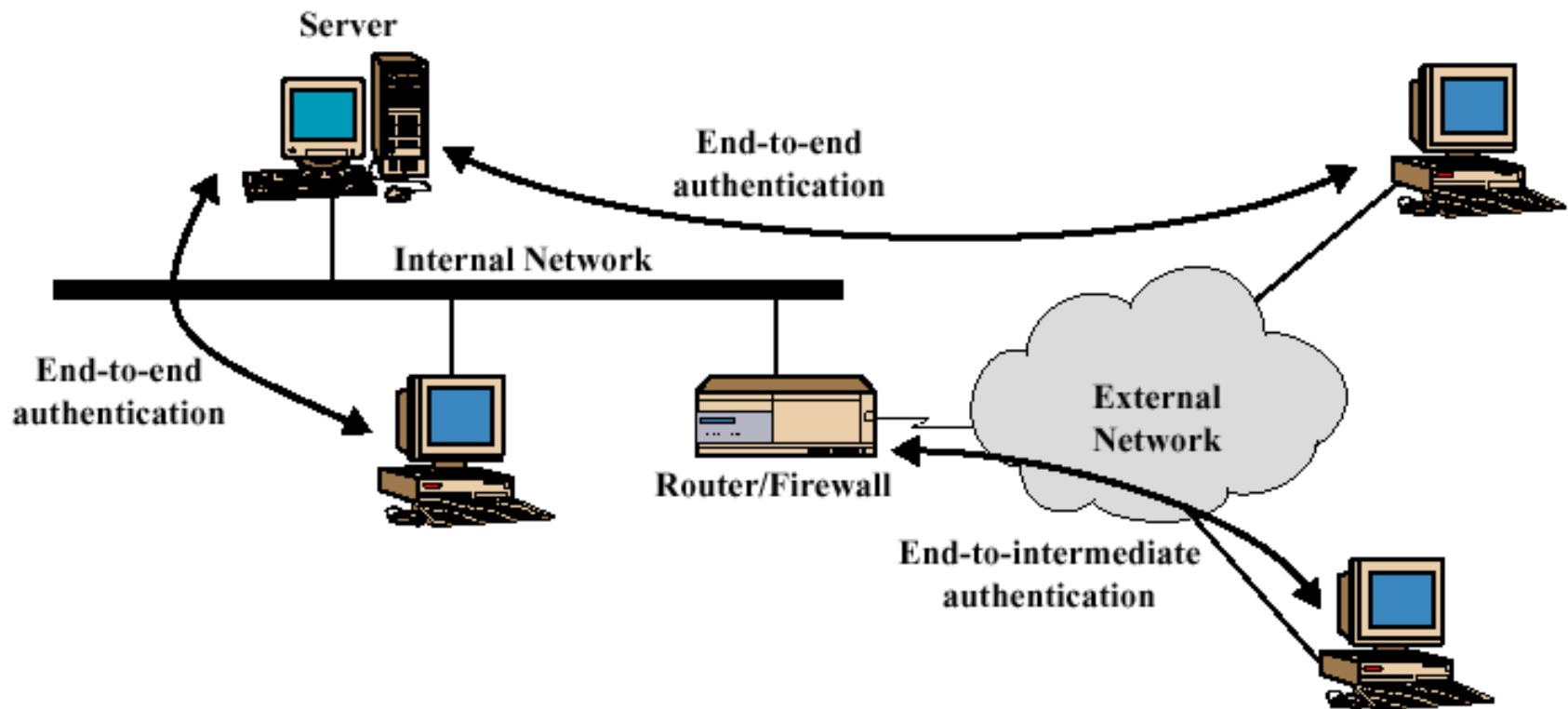
- Anti-Replay Service
- Integrity Check Value

# Anti-Replay Service

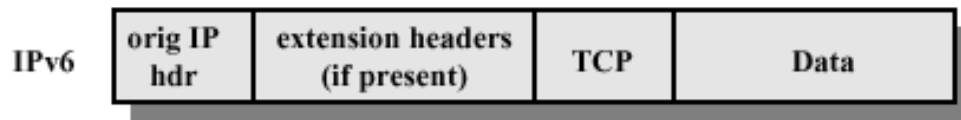
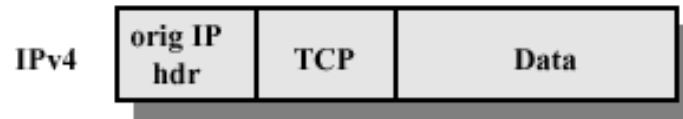
---



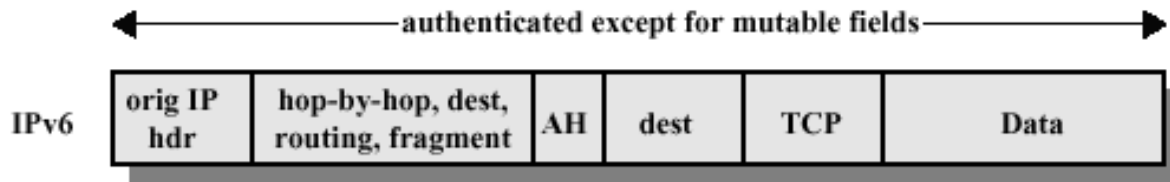
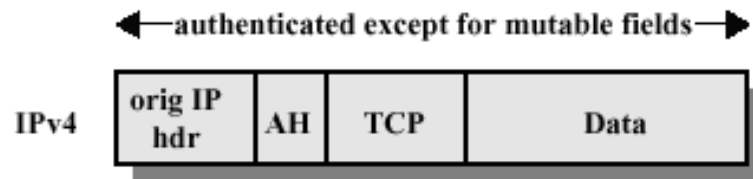
# Transport and Tunnel Modes



# Scope of Authentication Header



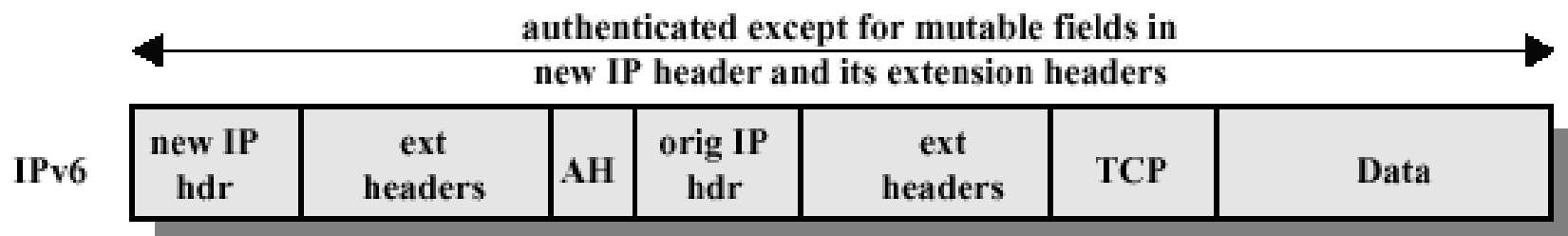
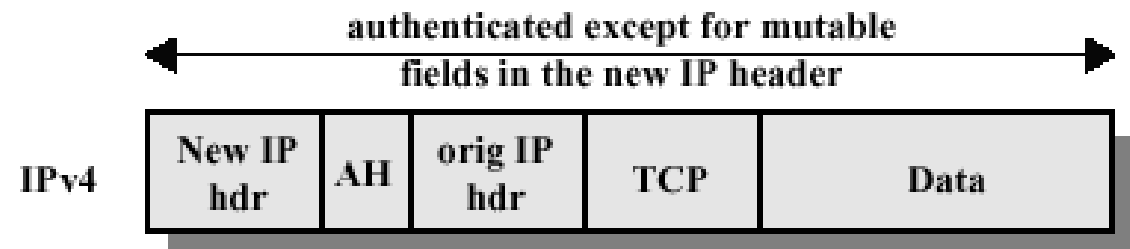
(a) Before Applying AH



(b) Transport Mode

# Scope of Authentication Header

---

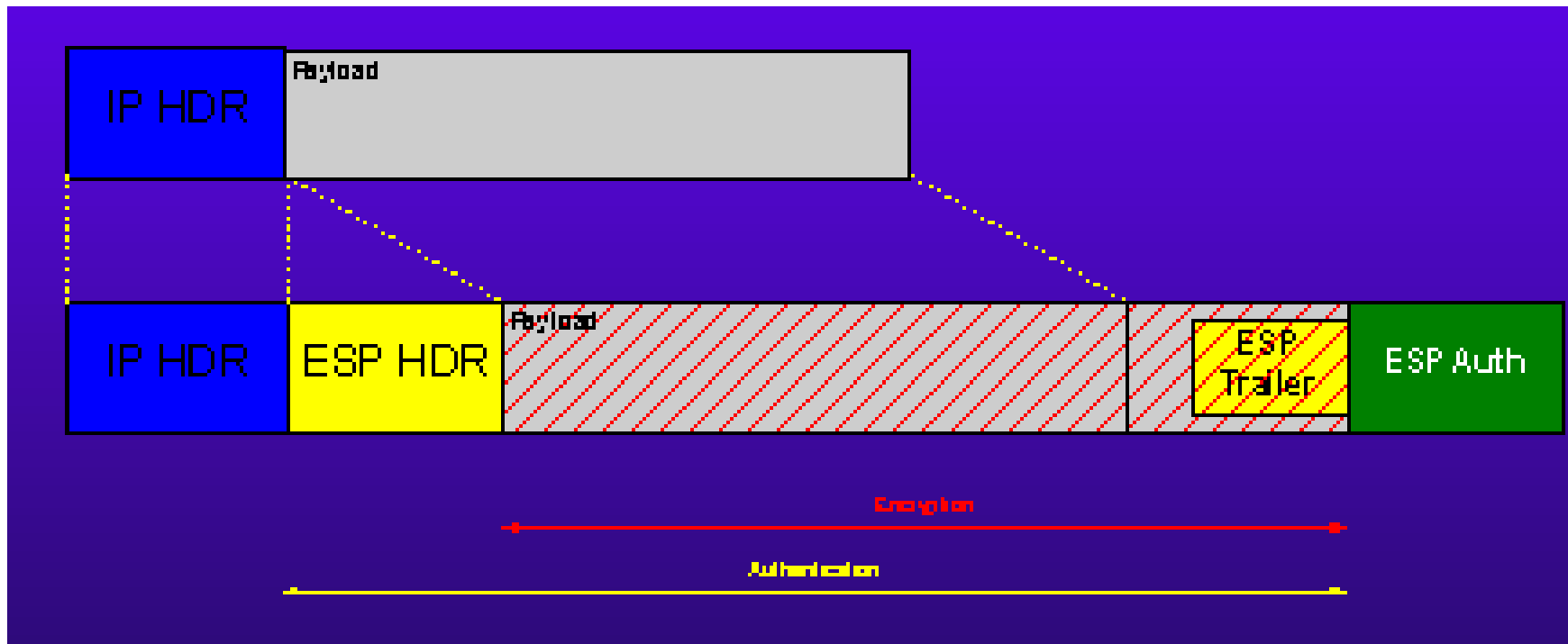


# Encapsulating Security Payload - ESP

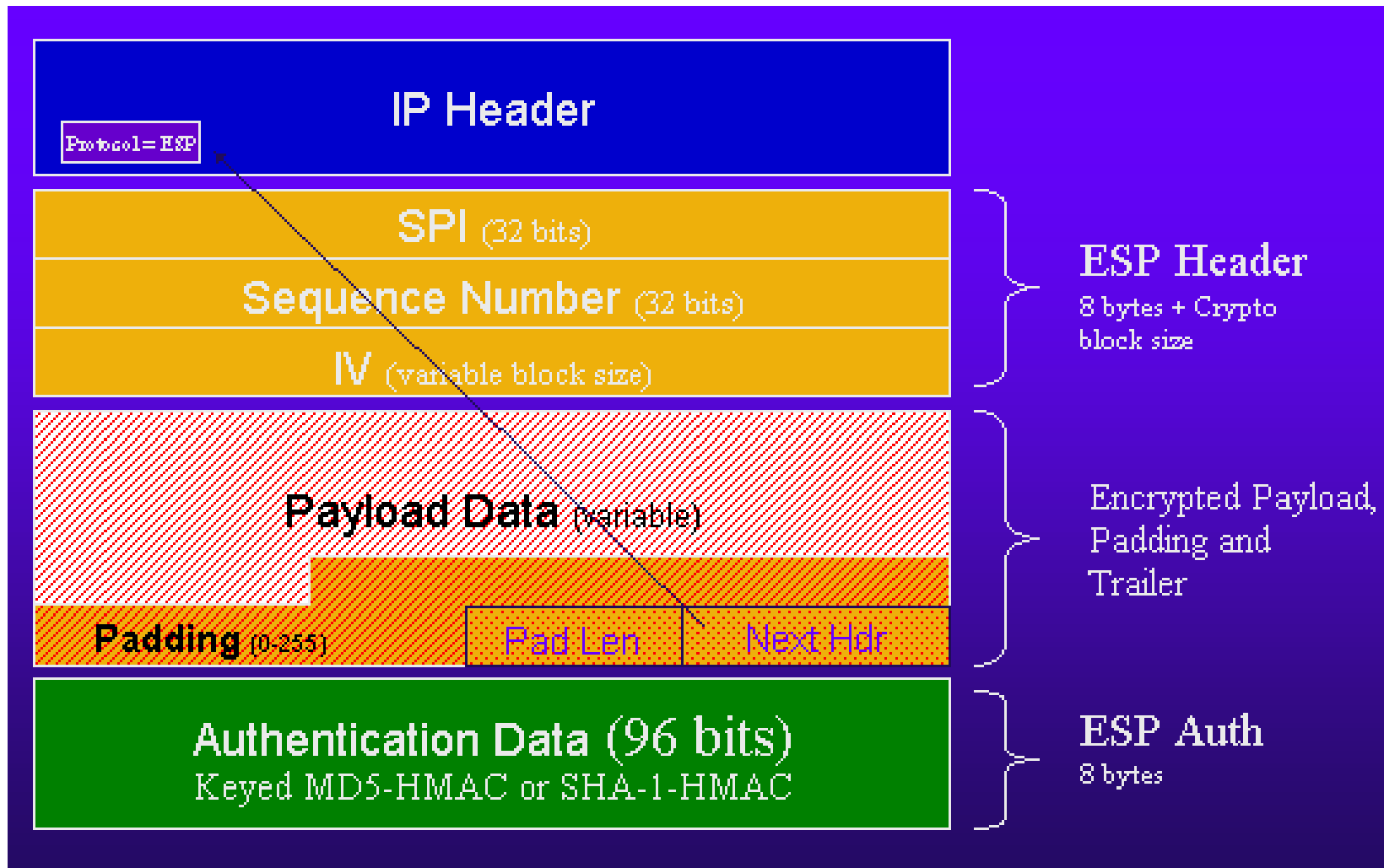
---

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

# ESP

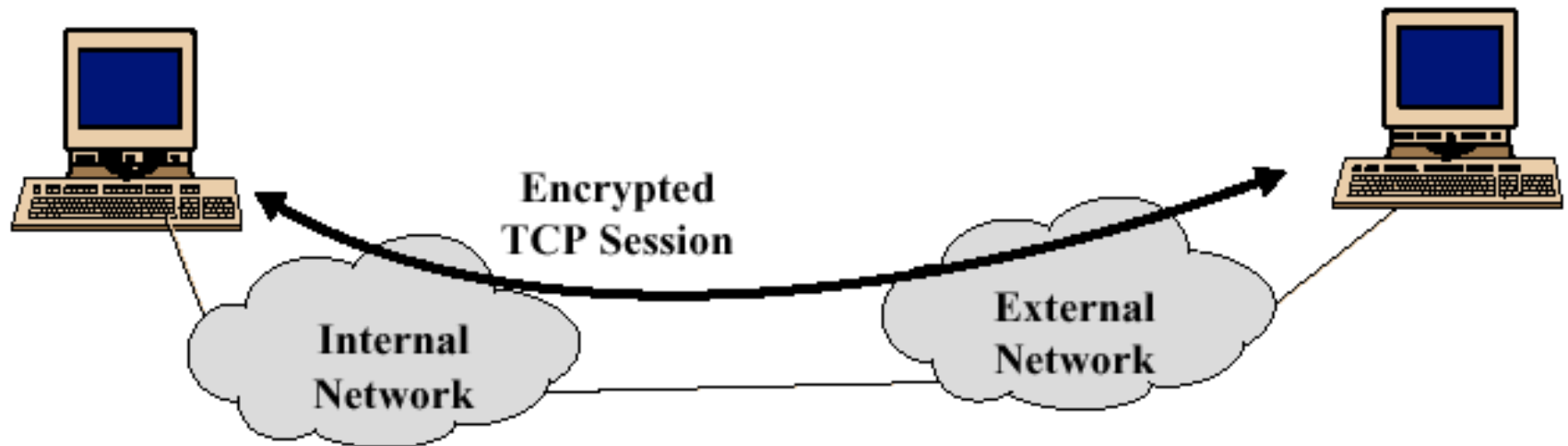


# ESP Format



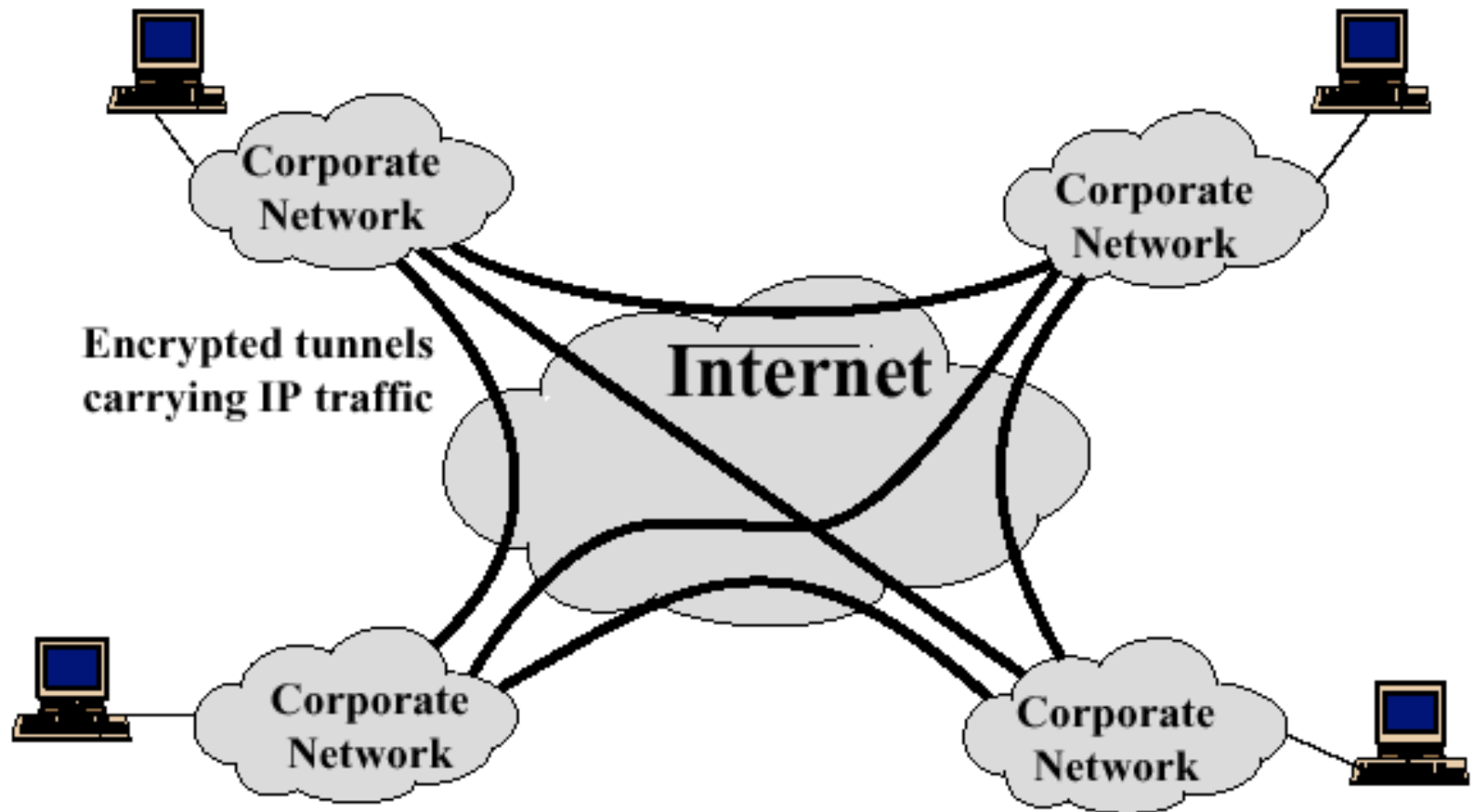
# Transport-level security

---



# A virtual private network via Tunnel Mode

---

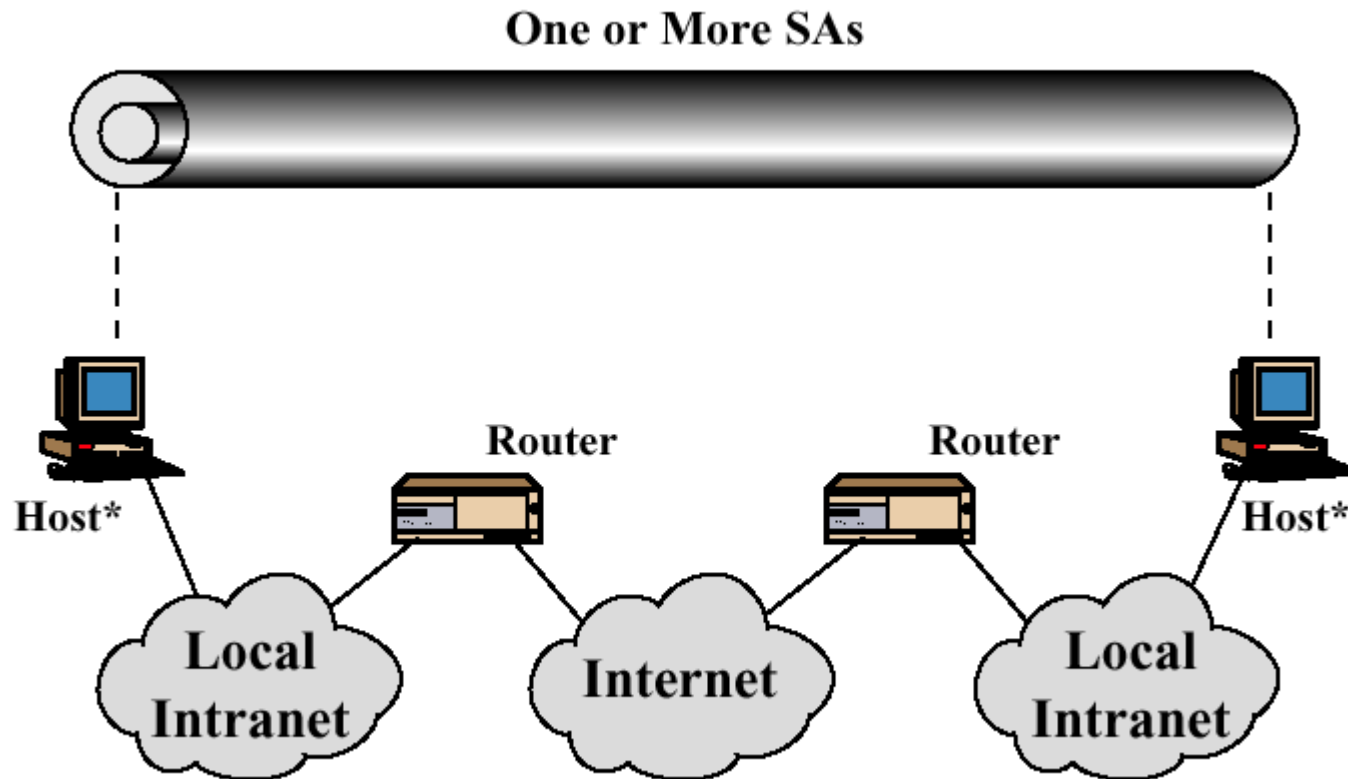


# Scope of ESP Encryption and Authentication

---

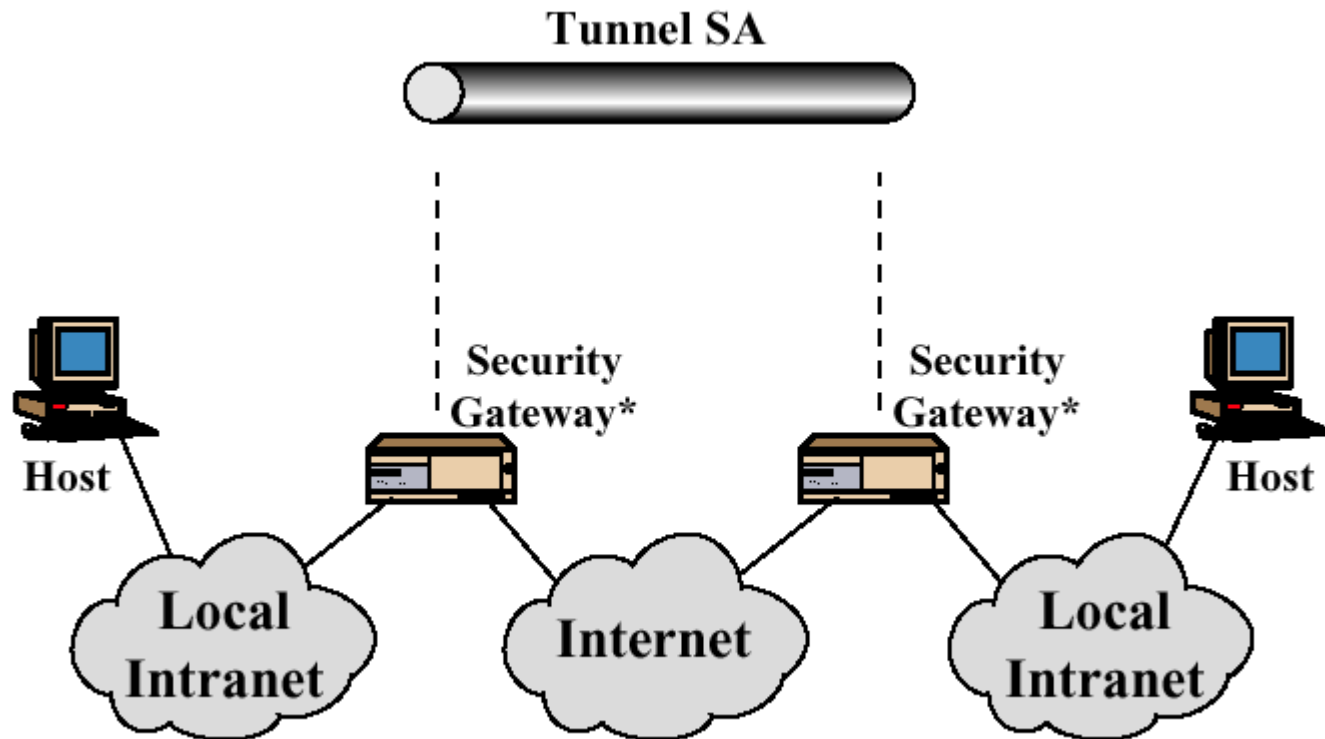
# Combining Security Associations

---

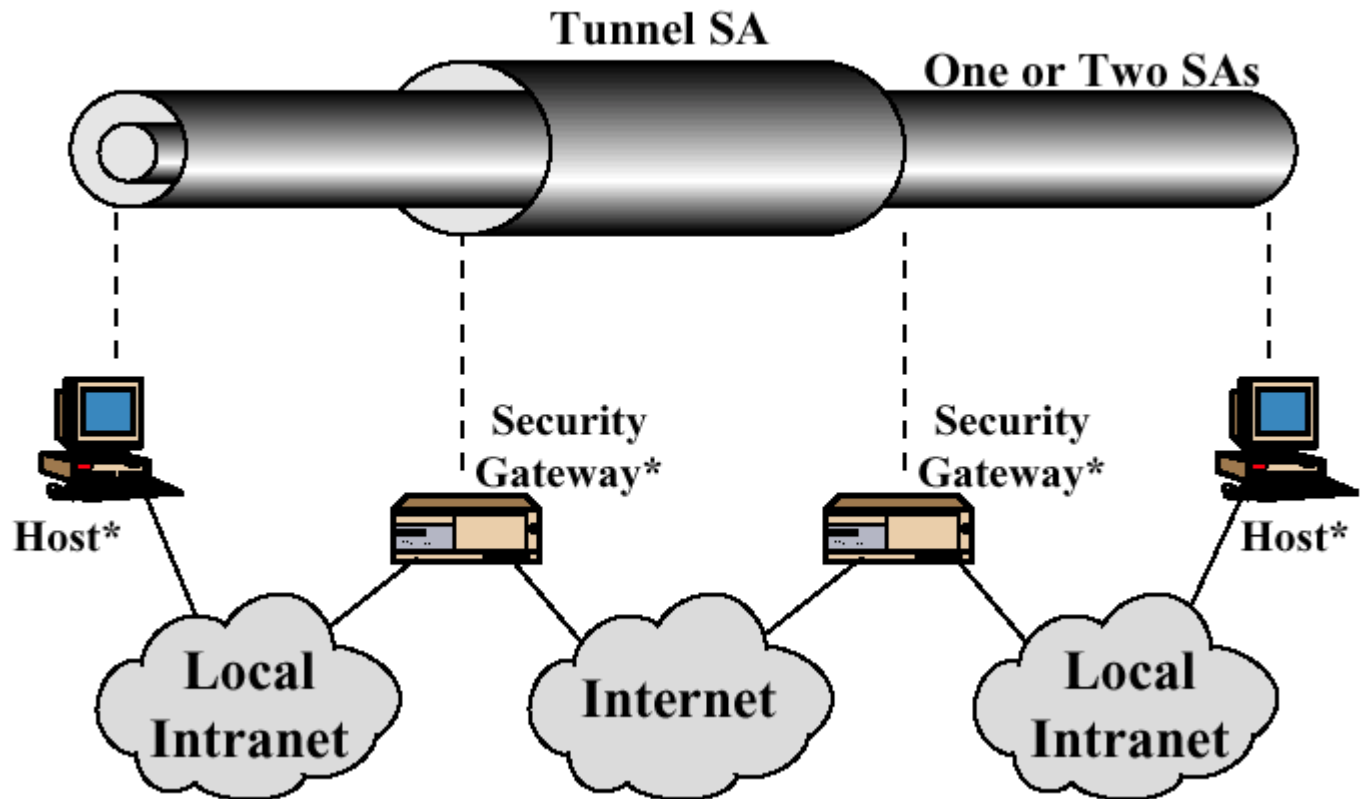


# Combining Security Associations

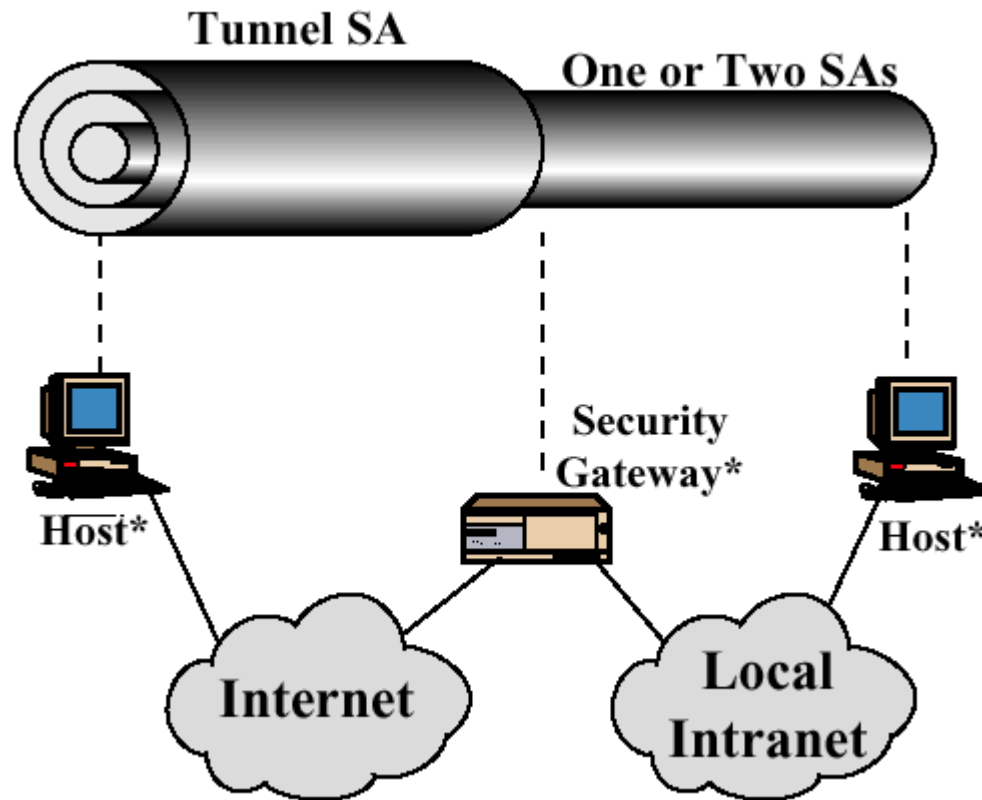
---



# Combining Security Associations



# Combining Security Associations



# Key Management

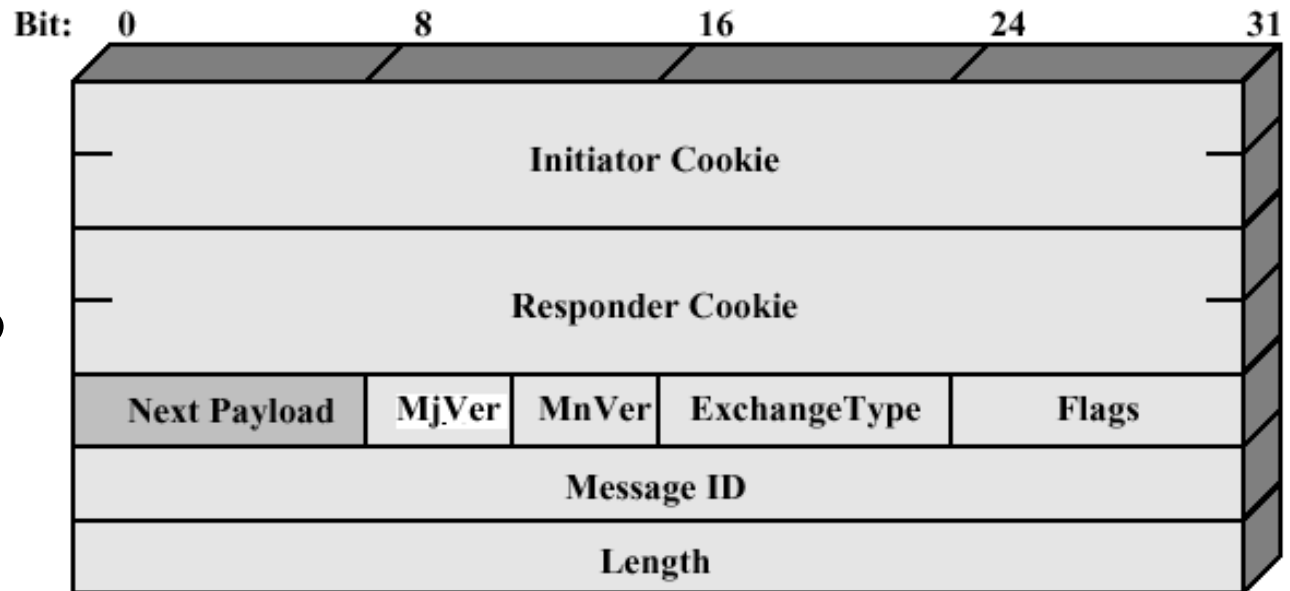
---

- Involves the determination and distribution of secret keys
- Typically four keys are used between two applications
- Two types of key management
  - ⊗ Manual
  - ⊗ Automated

# ISAKMP

•The default automated key management protocol from IPsec is referred to as ISAKMP/Oakley

•Oakley is a refinement of Diffie Hellman Key Exchange Protocol



(a) ISAKMP Header



(b) Generic Payload Header

# ISAKMP Exchange Types

Exchange	Note
<b>(a) Base Exchange</b>	
(1) I → R: SA; NONCE	Begin ISAKMP-SA negotiation
(2) R → I: SA; NONCE	Basic SA agreed upon
(3) I → R: KE; ID <sub>I</sub> ; AUTH	Key generated; Initiator identity verified by responder
(4) R → I: KE; ID <sub>R</sub> ; AUTH	Responder identity verified by initiator; Key generated; SA established
<b>(b) Identity Protection Exchange</b>	
(1) I → R: SA	Begin ISAKMP-SA negotiation
(2) R → I: SA	Basic SA agreed upon
(3) I → R: KE; NONCE	Key generated
(4) R → I: KE; NONCE	Key generated
(5)* I → R: ID <sub>I</sub> ; AUTH	Initiator identity verified by responder
(6)* R → I: ID <sub>R</sub> ; AUTH	Responder identity verified by initiator; SA established
Notation: I = initiator R = responder * = signifies payload encryption after the ISAKMP header	
<b>(c) Authentication Only Exchange</b>	
(1) I → R: SA; NONCE	Begin ISAKMP-SA negotiation
(2) R → I: SA; NONCE; ID <sub>R</sub> ; AUTH	Basic SA agreed upon; Responder identity verified by initiator
(3) I → R: ID <sub>I</sub> ; AUTH	Initiator identity verified by responder; SA established
<b>(d) Aggressive Exchange</b>	
(1) I → R: SA; KE; NONCE; ID <sub>I</sub>	Begin ISAKMP-SA negotiation and key exchange
(2) R → I: SA; KE; NONCE; ID <sub>R</sub> ; AUTH	Initiator identity verified by responder; Key generated; Basic SA agreed upon
(3)* I → R: AUTH	Responder identity verified by initiator; SA established
<b>(e) Informational Exchange</b>	
(1)* I → R: N/D	Error or status notification, or deletion

# ISAKMP Payload Types

Type	Parameters	Description
Security Association (SA)	Domain of Interpretation, Situation	Used to negotiate security attributes and indicate the DOI and Situation under which negotiation is taking place.
Proposal (P)	Proposal #, Protocol-ID, SPI Size, # of Transforms, SPI	Used during SA negotiation; indicates protocol to be used and number of transforms.
Transform (T)	Transform #, Transform-ID, SA Attributes	Used during SA negotiation; indicates transform and related SA attributes.
Key Exchange (KE)	Key Exchange Data	Supports a variety of key exchange techniques.
Identification (ID)	ID Type, ID Data	Used to exchange identification information.
Certificate (CERT)	Cert Encoding, Certificate Data	Used to transport certificates and other certificate-related information.
Certificate Request (CR)	# Cert Types, Certificate Types, # Cert Auths, Certificate Authorities	Used to request certificates; indicates the types of certificates requested and the acceptable certificate authorities.
Hash (HASH)	Hash Data	Contains data generated by a hash function.
Signature (SIG)	Signature Data	Contains data generated by a digital signature function.
Nonce (NONCE)	Nonce Data	Contains a nonce.
Notification (N)	DOI, Protocol-ID, SPI Size, Notify Message Type, SPI, Notification Data	Used to transmit notification data, such as an error condition.
Delete (D)	DOI, Protocol-ID, SPI Size, # of SPIs, SPI (one or more)	Indicates an SA that is no longer valid.

# 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