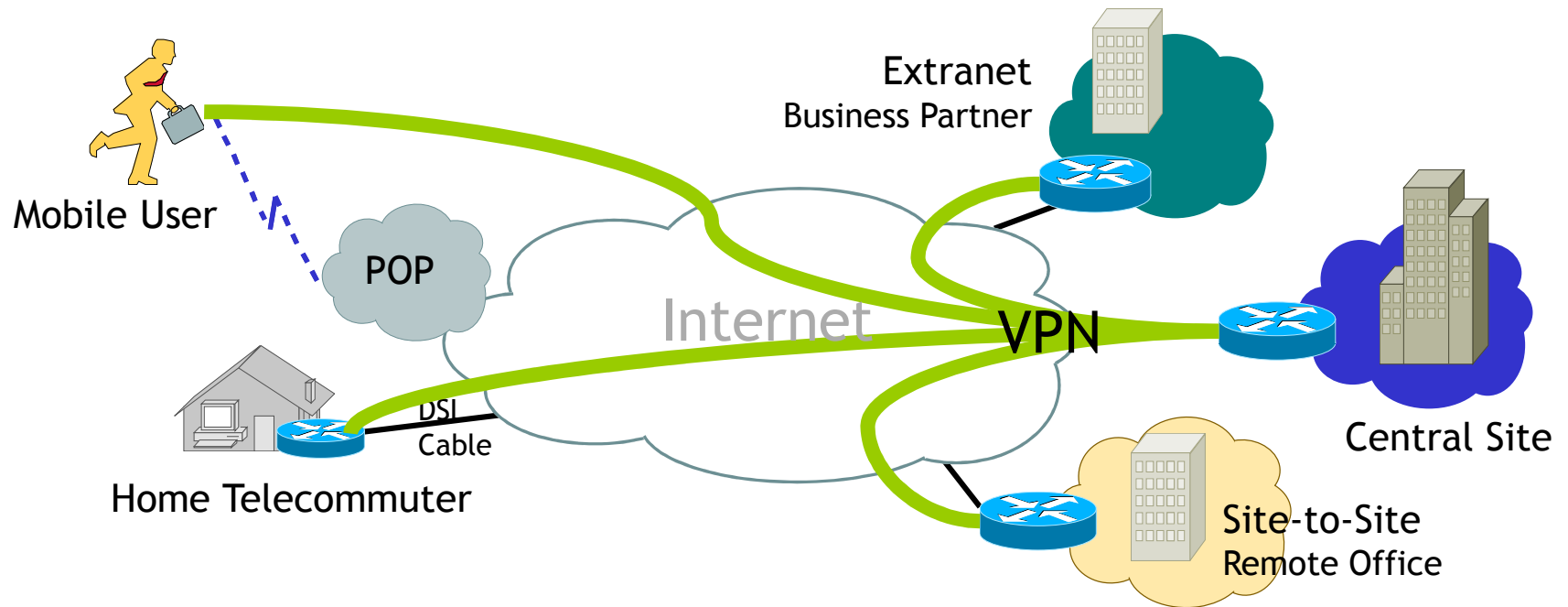




VPN

Virtual Private Networks
IPSec Lab

VPN



VPN

Variantes de protocolos:

- **PPTP**

Desarrollado por MS, no provee encriptación (capa 2)

- **L2TP**

Desarrollado por Cisco y MS, mejora al PPTP incluyendo encriptación a través de IPSec (ESP) (capa 2)

- **IPSec**

Considerado el estándar actual (capa3)

- **SSL**

No requiere cliente de software (capa 4)

IPsec

Suite de protocolos destinados a proveer seguridad a nivel de red

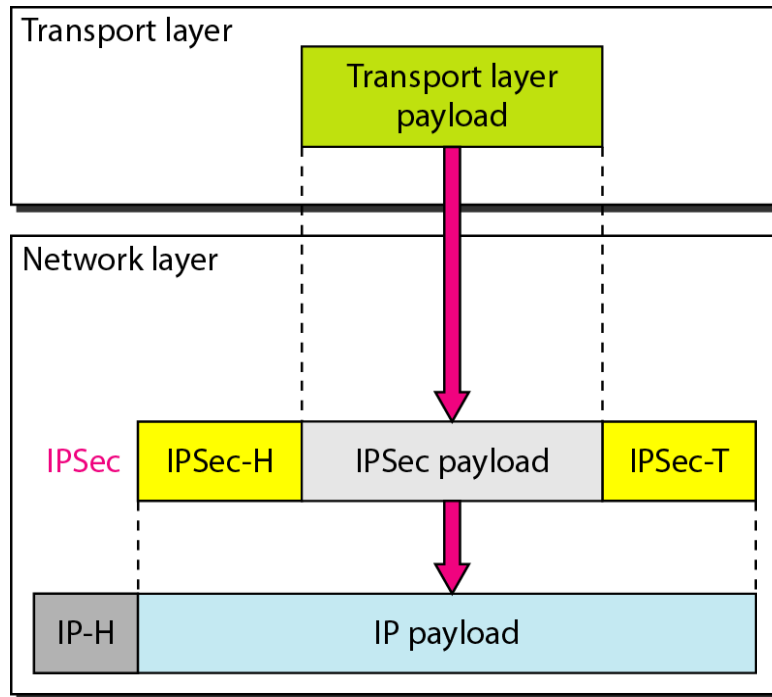
Dos modos de operación:

- Modo Transporte
- Modo Túnel

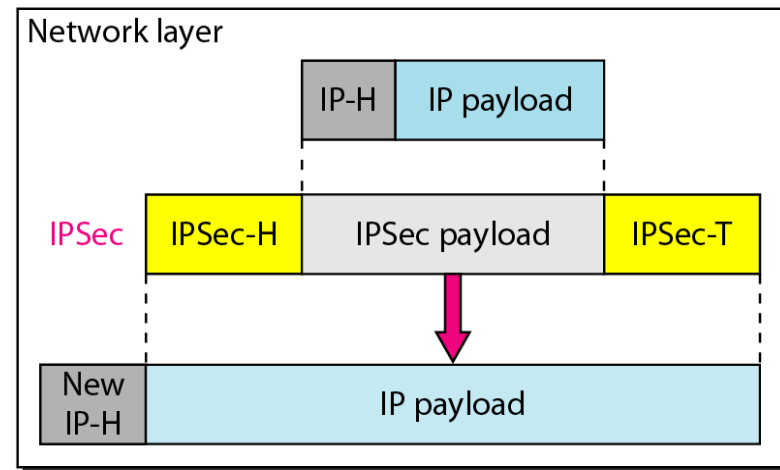
Dos protocolos:

- AH protocol
- ESP protocol

Modos de operación

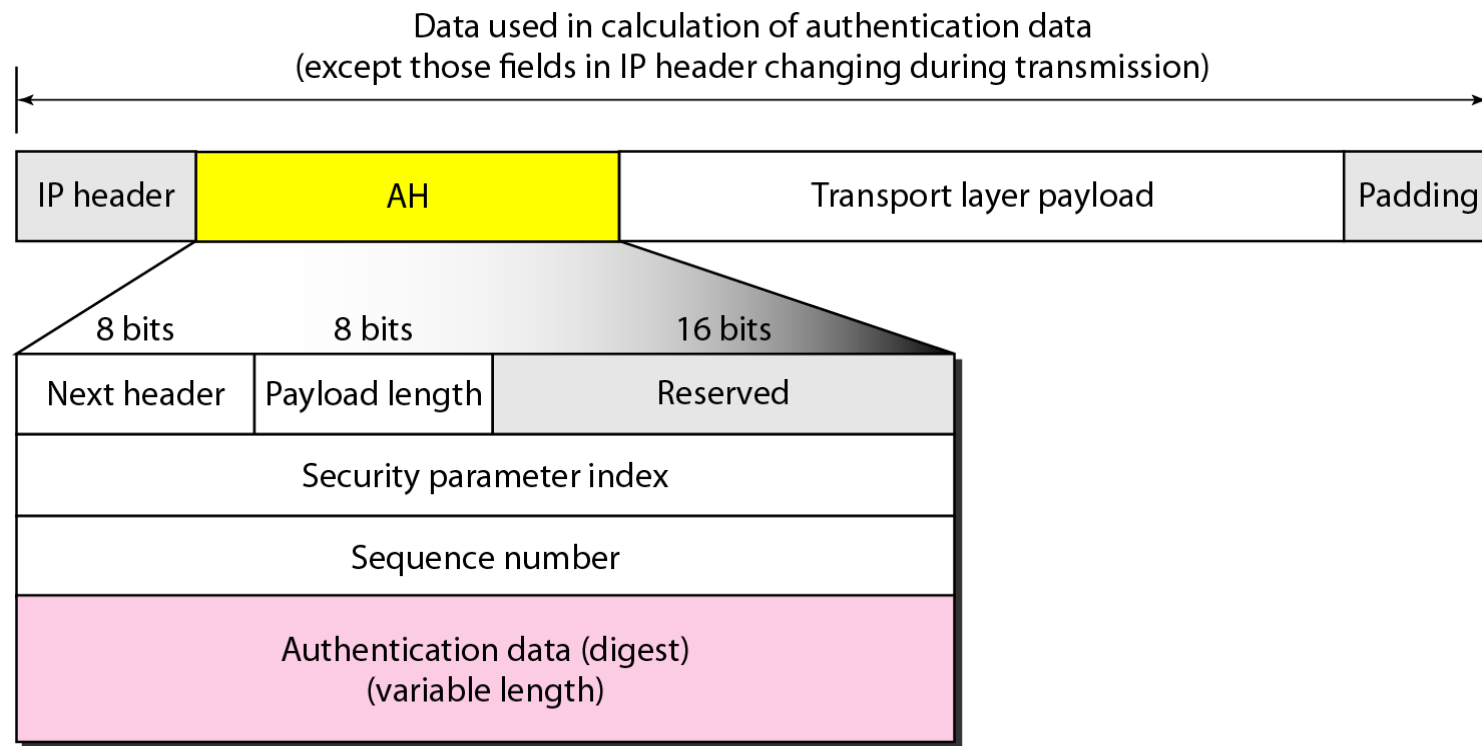


a. Transport mode



b. Tunnel mode

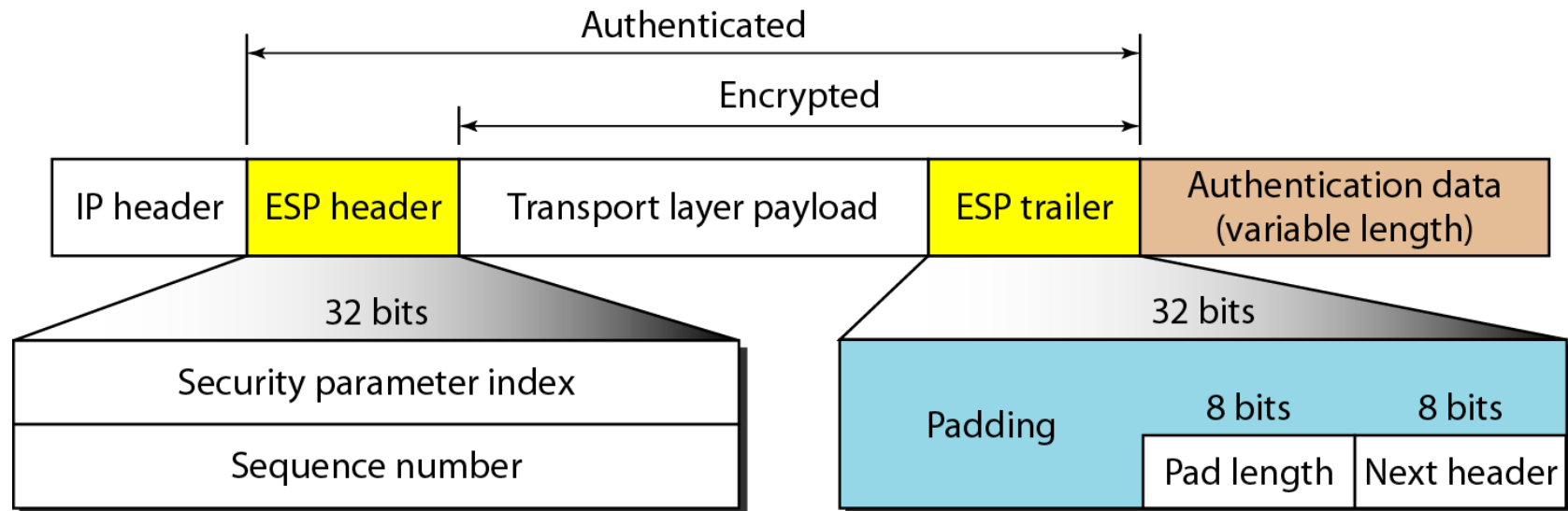
AH en modo transporte



AH provee:

Autenticidad del origen, Integridad de los datos pero
no privacidad

ESP en modo transporte



ESP provee:

Autenticidad del origen, Integridad de los datos y
privacidad

Implementación

- IKE Policy (Phase I)

crypto isakmp policy 1

authentication pre-share

hash sha

encryption 3des

crypto isakmp key *clave_privada* address 10.10.10.1

- IPsec Policy (Phase II)

crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac

access-list 102 permit ip X.X.X.X 0.0.0.255 Y.Y.Y.Y 0.0.0.255

crypto map IPSEC 20 ipsec-isakmp

set peer 10.10.10.1

match address 102

set transform-set ESP-3DES-SHA

interface serial 0

crypto map IPSEC