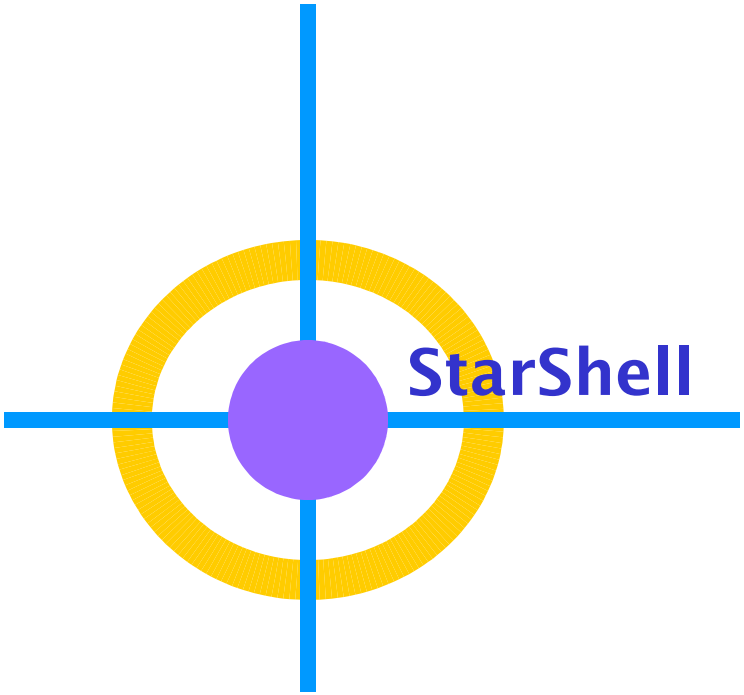


IPSec

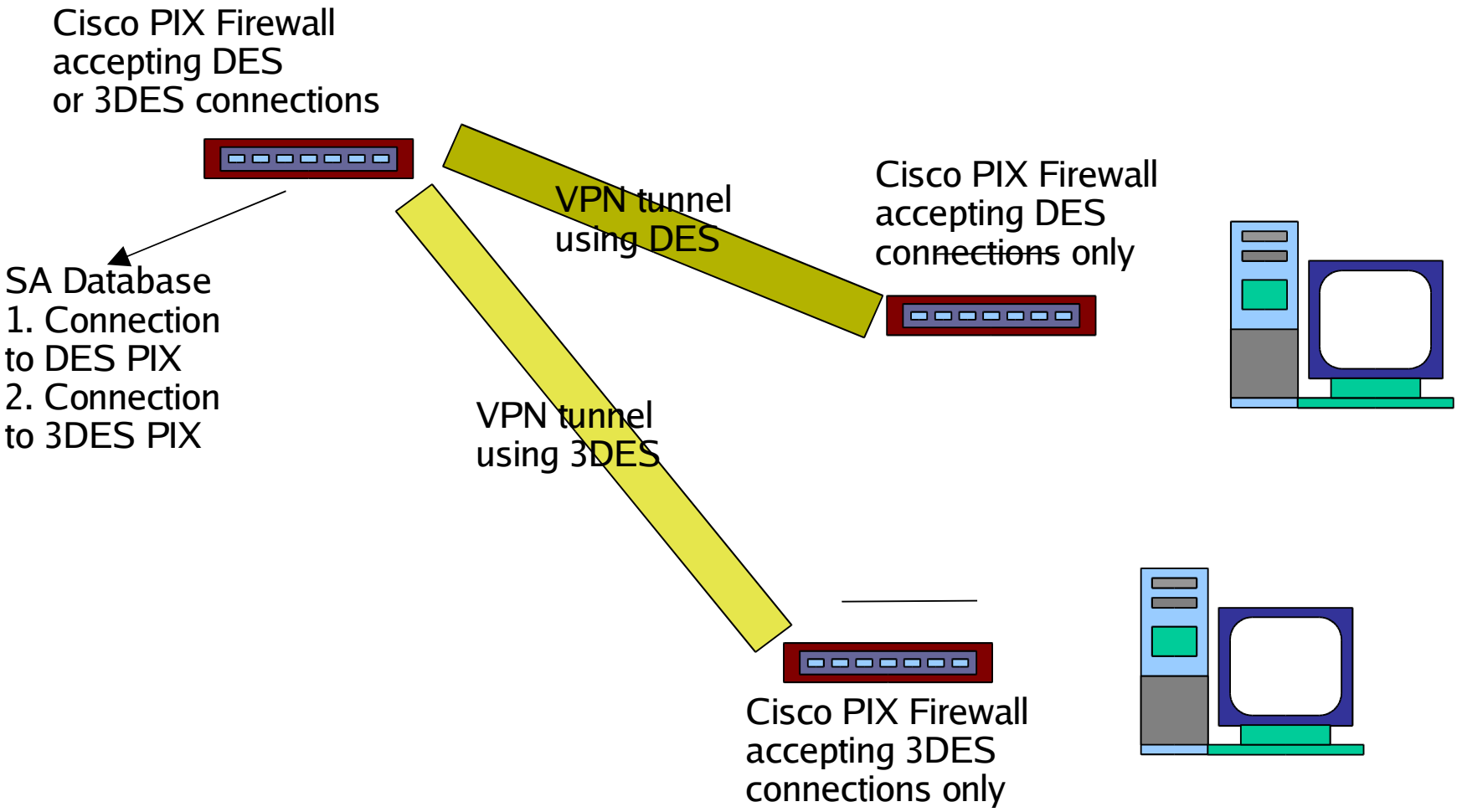
IPSec

  - Applicabile sia a Ipv4 che Ipv6
- Obiettivi:
  - Facilitare la confidenzialità, integrità ed autenticazione di informazioni trasferite tramite IP
  - Standard di interoperabilità tra più vendor
- Protocolli:
  - Internet Key Exchange (IKE)
  - Encapsulating Security Payload (ESP)
  - Authentication Header (AH)

Security Association (SA)

- Accordo tra due entità su come trasmettere le informazioni in modo sicuro - meccanismi
- Ogni sessione di comunicazione ha due SA
- Ogni partner negozia una nuova SA per ogni connessione IP
- I meccanismi supportati sono raccolti nella Security Policy Database (SPD)
- Le SA attive sono contenute nella Security Association Database (SAD)

Security Associations



Modi IPSec

- Transport Mode
  - Crittografa solo il payload dei pacchetti
  - Solo host-to-host
  - Ideale tra host sulla stessa rete
- Tunnel Mode
  - Crittografa l'intero pacchetto originale
  - Può essere host-to-host, host-to-gateway, gateway-to-gateway (l'ultimo caso più comune)

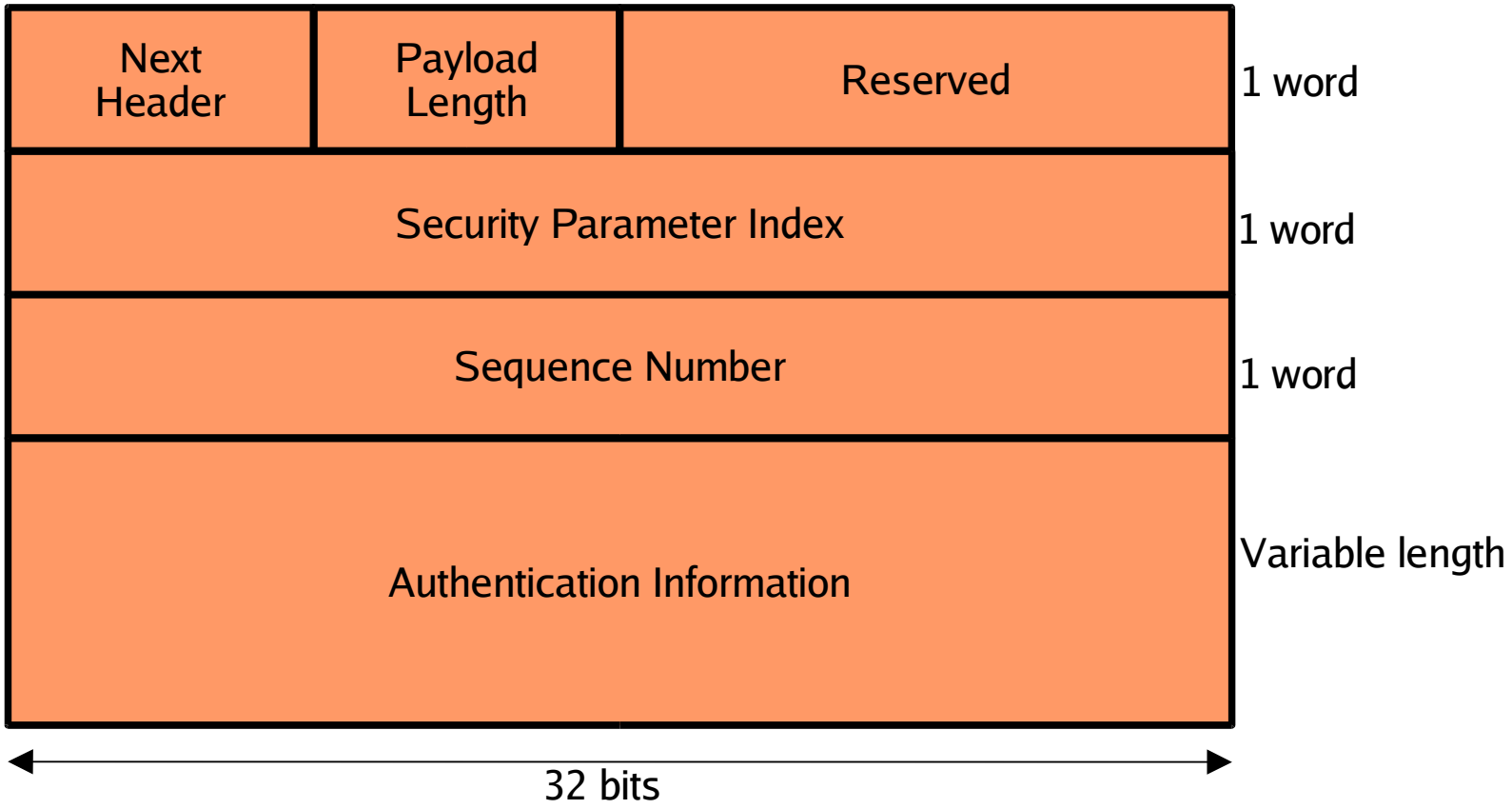
IKE Protocol

- IKE è l'autenticatore e negoziatore di IPSec
- Combinazione di due protocolli
  - **Internet Security Association and Key Management Protocol (ISAKMP)**
  - **Oakley (Diffie-Hellman)**
- Due Fasi:
  - **Fase 1: autenticazione dell'utente remoyo e interscambio di chiavi pubbliche per la Fase 2**
  - **Fase 2: negoziazione dei parametri per le SA di IPSec**

Authentication Header Protocol

- IP protocolo numero 51
- Autenticazione e protezione dell'integrità del pacchetto IP
- Integrity Check Value: valore hash per garantire l'integrità del pacchetto
- L'informazione IP non è nascosta
- Problemi in presenza di NAT
- Niente confidenzialità dei dati
  - **payload è in chiaro**
- Bassi requisiti di calcolo

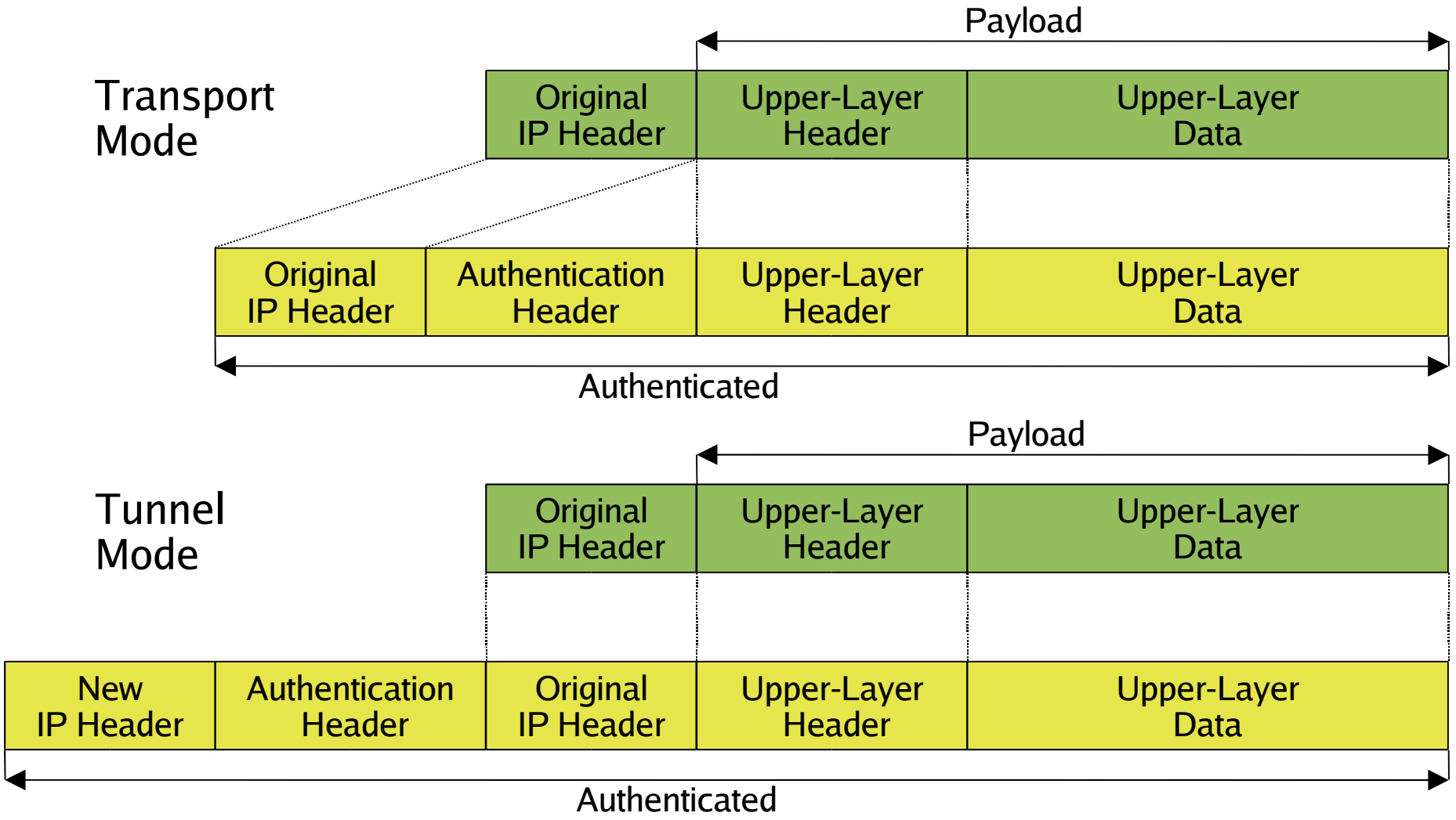
AH Packet Header



AH Packet Header

- Next Header
  - **Tipo di testata di protocollo che segue la testata AH**
- Payload Length
  - **Lunghezza della testata AH header, in parole da 4 byte meno 2**
- Reserved
  - **Settato a zero**
- Authentication Data
  - **ICV secondo l'algoritmo scelto dalla SA**
    - **Default HMAC-MD5-SHA1: 96 bit ICV**
  - **Non include i campi mutevoli della testata IP:**
    - **TOS, Offset di Frammento, Flag di Frammentazione, Time-to-live, IP Header Checksum**
  - **Include tutti gli altri campi della testata IP**

AH e Modi


Payload
Transport Mode
Original IP Header
Upper-Layer Header
Upper-Layer Data
Original IP Header
Authentication Header
Upper-Layer Header
Upper-Layer Data
Authenticated
Payload
Tunnel Mode
Original IP Header
Upper-Layer Header
Upper-Layer Data
New IP Header
Authentication Header
Original IP Header
Upper-Layer Header
Upper-Layer Data
Authenticated

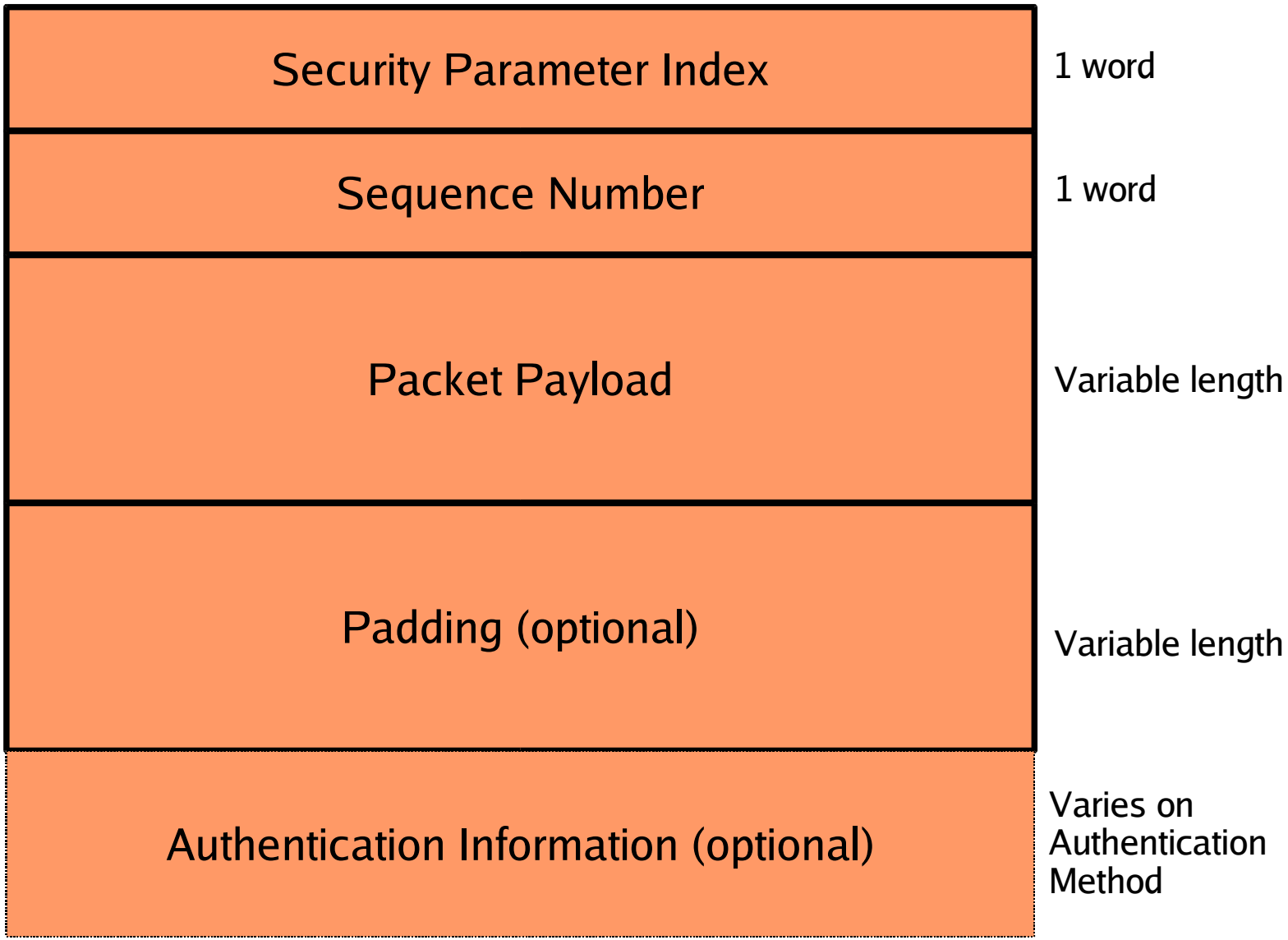
Encapsulating Security Payload Protocol

- IP protocollo numero 50
- Transport mode:
  - **Aggiunge la sua testata dopo la testata IP**
  - **Crittografa le informazioni dal livello 4 in su**
  - **Se è specificato il servizio di autenticazione, aggiunge un trailer con le informazioni ICV**
    - **Lo ICV di ESP non usa le informazioni della testata IP**
- Tunnel mode:
  - **Incapsula e crittografa pienamente l'intero pacchetto**
  - **Crea una nuova testata IP seguita dalla testata ESP**
  - **Può aggiungere un trailer con ICV se è richiesta autenticazione**

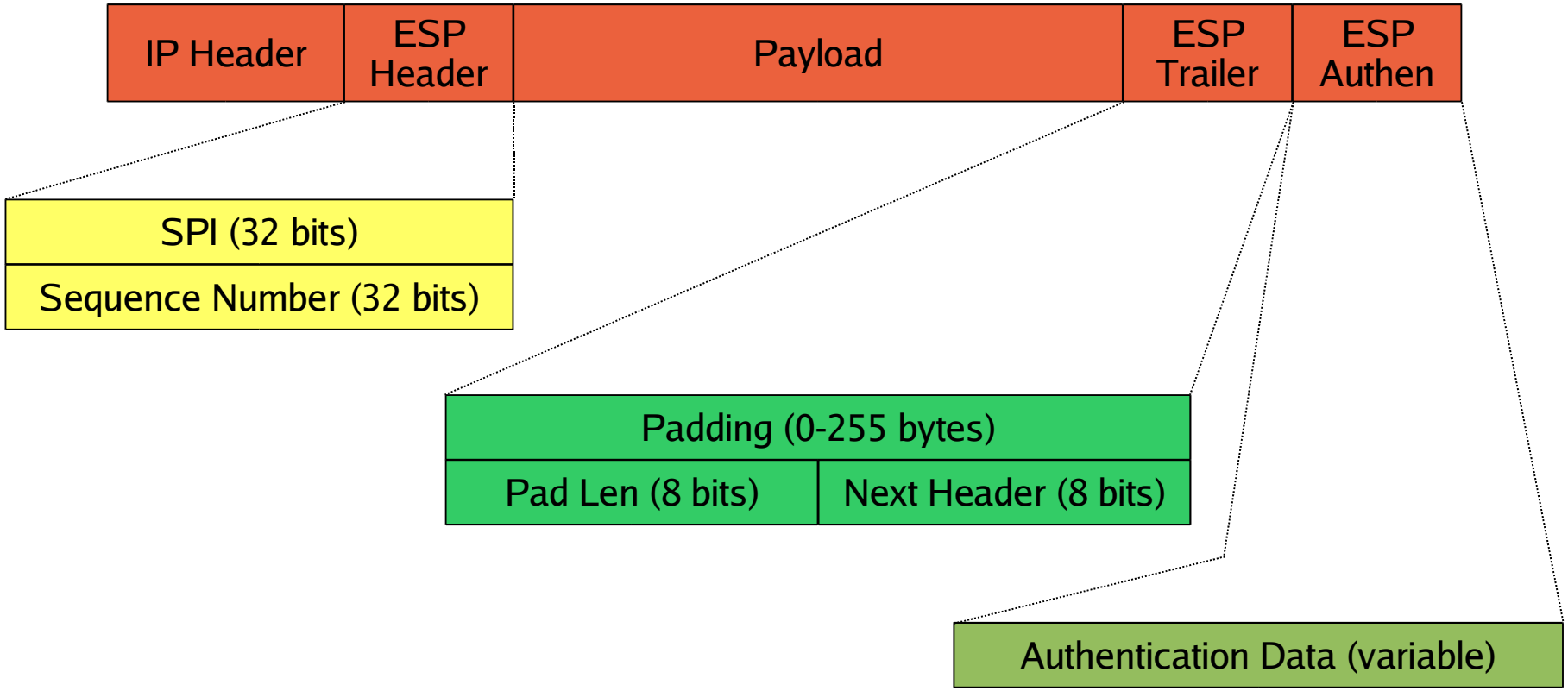
ESP e il NAT

- Tunnel mode:
  - **Transita dal NAT con successo**
    - **L'intero pacchetto originale è incapsulato, incluse sia le informazioni IP che di Livello 4**
  - **Ci possono essere problemi con i NAT uno-a-molti (PAT)**
- Transport mode:
  - **Il checksum TCP usa anche Indirizzi Sorgente e Destinazione dalla testata IP**
  - **Problema simile con UDP**
  - **Una soluzione può essere di disabilitare i checksum**

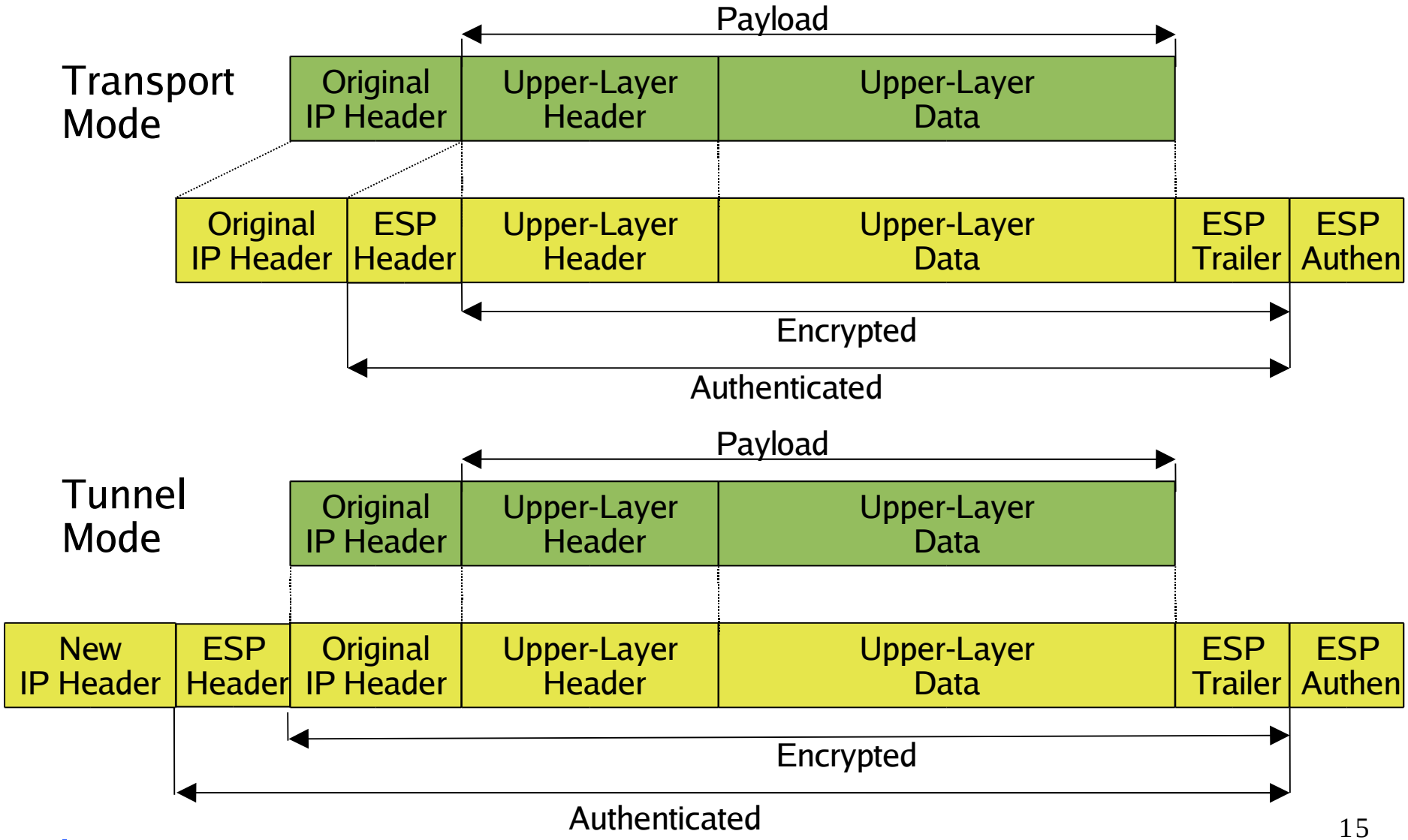
ESP Packet Header



Formati Segmento ESP



Modi ESP



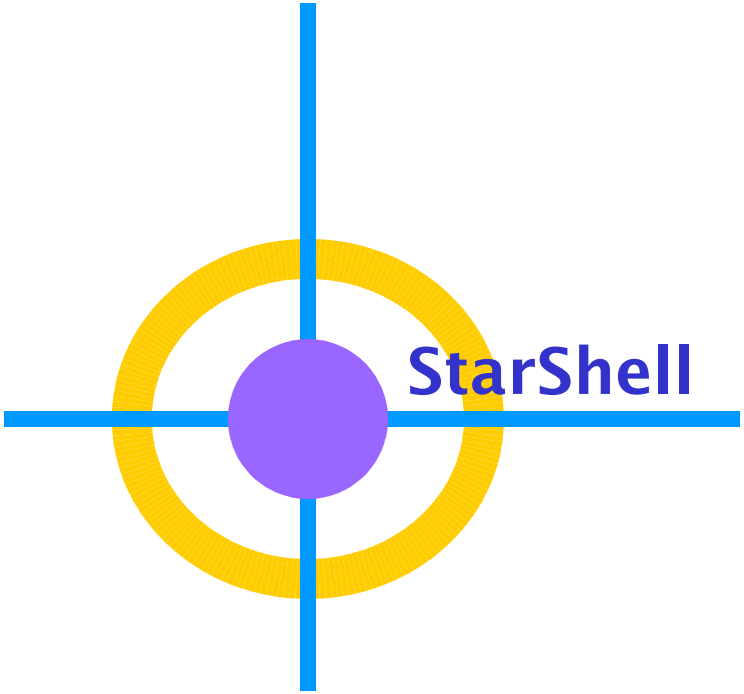
StarShell

Considerazioni IPSec

- Architetture
  - Host-to-Host
    - **Gli utenti esterni devono accedere a un singolo host interno**
    - **Occorre configurare i client e lo host**
  - Host-to-Gateway
    - **Gli utenti esterni devono acceder a molti host interni**
    - **Occorre configurare i client e il gateway**
    - **Nessun cambiamento sugli host**
  - Gateway-to-Gateway
    - **Tra due reti esterne separate**
    - **Occorre configurare i due gateway**
    - **Nessun cambiamento ai client e agli host**

Considerazioni IPSec

- Deployment
  - **Concentratori VPN**
    - **Soluzione costosa e ingombrante**
    - **Si possono combinare con Firewall e NAT**
  - **Firewall**
    - **Lavoro extra di crittografazione riduce l'efficienza**
  - **Router**
    - **Soluzione più economica per i VPN Gateway-to-Gateway**
- Riconfigurazione delle Difese Perimetrali
  - **VPN Passthrough**
    - **Evita NAT e PAT**
    - **Usare solo ESP se il NAT non si può evitare**
    - **Non usare VPN se il PAT non si può evitare**


StarShell