Tema 4:
Seguridad en el nivel de Red.
Arquitectura de seguridad IPSEC

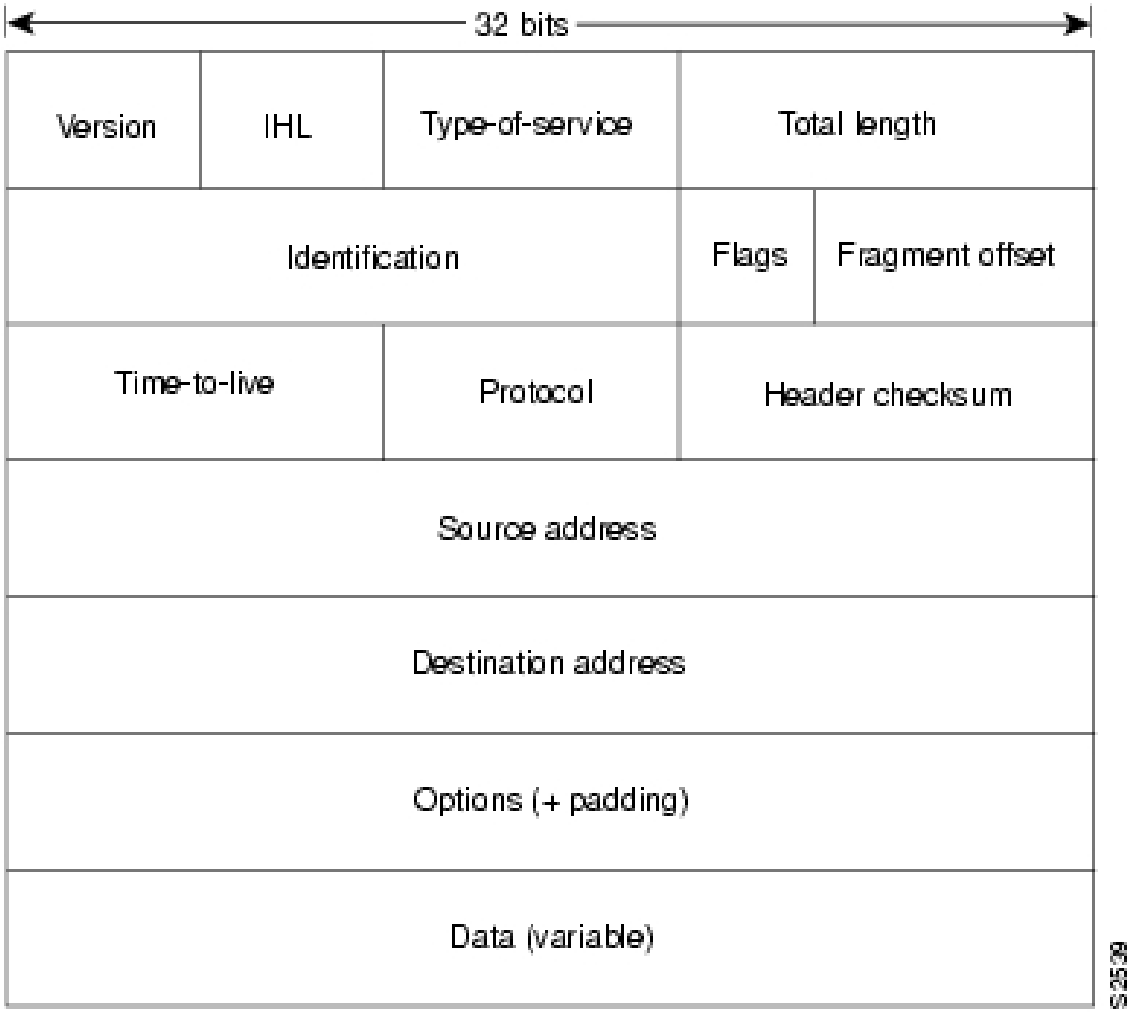
Introducción

- Seguridad en Internet
  - ¿es posible?
  - Continuas noticias, virus, ataques, engaños, ...
  - Aprovechar sus ventajas sin perder privacidad
- ¿qué diferencia a Ipsec?
  - Solución global
  - Aplicable a nodos finales e intermedios
  - Soluciones particulares sencillas que conforma un todo

Elementos

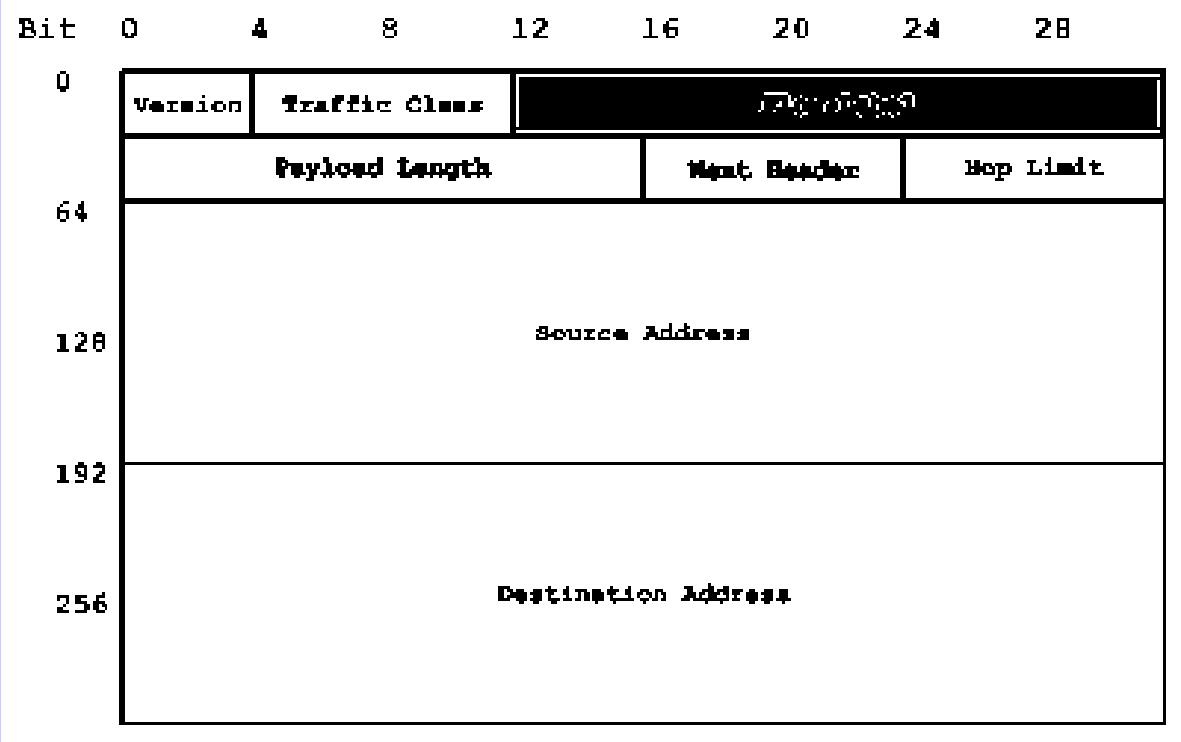
- Host
  - Sistema que puede iniciar/recibir mensajes, pero que no puede actuar como intermediario de comunicaciones
  - Solo puede suministrar servicios IPsec a sí mismo.
- Gateway (pasarela)
  - Sistema que puede iniciar/recibir mensajes, y puede actuar como intermediario de comunicaciones
  - Solo puede suministrar servicios IPsec a sí mismo.

o Paquete IPv4



TCP/IP

- Paquete IPv6



Arquitectura IPSEC

- Arquitectura de seguridad IPsec
  - Servicios de seguridad opcionales en el nivel de red (IETF)
  - Incluido en IPv6 Draft Standard (1998)
- IPsec incluye dos protocolos de seguridad
  - Cabecera de autenticación (AH)
    - Servicios de Integridad y autenticación
    - Mecanismos de firma digital o funciones resumen con clave

    Encapsulación segura del campo de carga (ESP)
    - Servicios Confidencialidad, integridad y autenticación
    - Mecanismos de cifrado del campo de carga, firma digital o funciones resumen con clave

Protocolos de IPSec

- Protocolo para la gestión y negociación de parámetros de seguridad
  - Asociación de Seguridad (SA)
    - Una asociación de seguridad es una relación entre dos o más entidades y que describe cómo éstas utilizarán los servicios de seguridad para comunicarse de forma segura.
  - *Internet Security Association and Key Management Protocol*
  - Protocolo IKE e IKEv2
- Protocolo opcional
  - IPCOMP

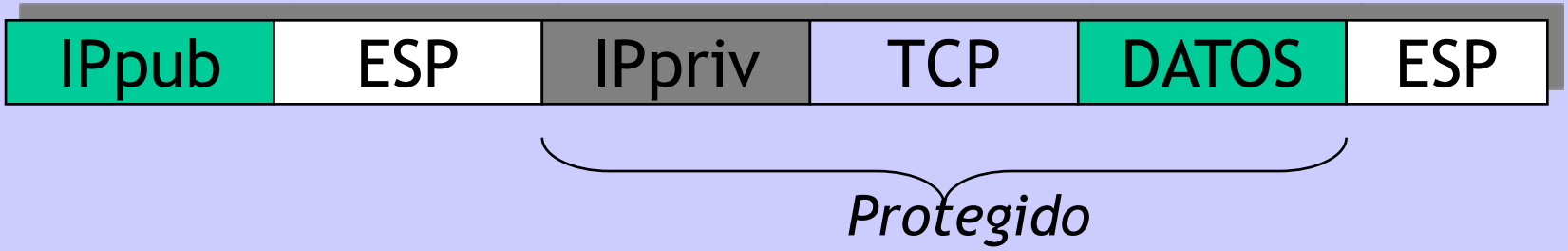
Modos de funcionamiento

- Transport mode
  - Protección primaria para las capas superiores , no modifica ni encapsula el protocolo IP.
- Tunnel mode
  - Se aplica una protección al todo el paquete IP, modificandolo.

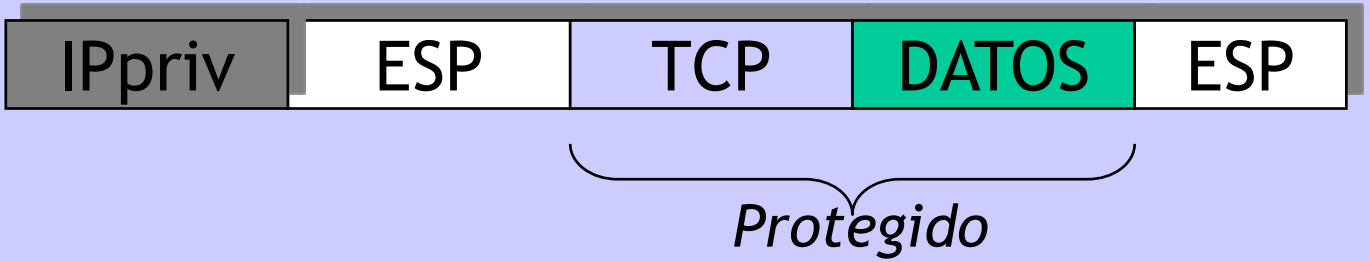
Encapsulado según modo

Original

Modo Túnel

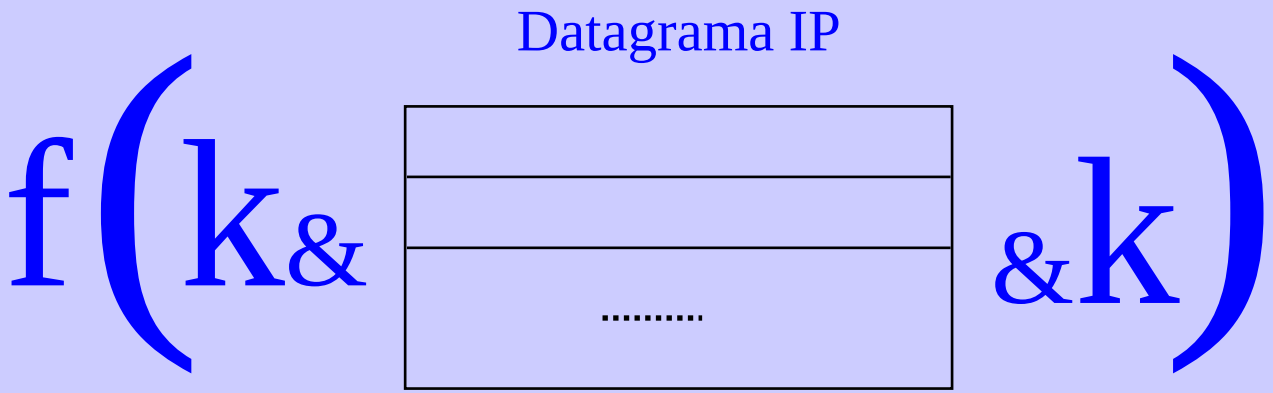


Modo Transporte



Cabecera de Autenticación (AH)

- Proporciona integridad y autenticación a los datagramas IP.
  - *Ésto se realiza computando una función resumen sobre el datagrama, empleando una clave secreta en dicho cálculo.*
- La información de auntenticación se calcula utilizando todos los campos del datagrama que no van a cambiar durante el tránsito



Cabecera de Autenticación

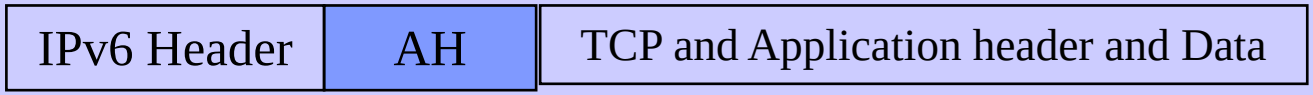
- Su uso aumentará los costes de procesamiento de protocolo IP y la latencia de las comunicaciones.
- Este mecanismo proporciona una seguridad más fuerte que la existente en la mayoría de la actual Internet, y no debe afectar a la interoperatividad, ni aumentar el coste de implementación.
- Las máquinas que soporten IPv6 tienen que implementar la Cabecera de Auntenticación con el algoritmo de MD5 y claves secretas de 128 bits.

AH

- Formato

Next Header	Payload Length	Reserved
Security Parameter Index		
Sequence Number Field		
Authentication Data		

- Colocación



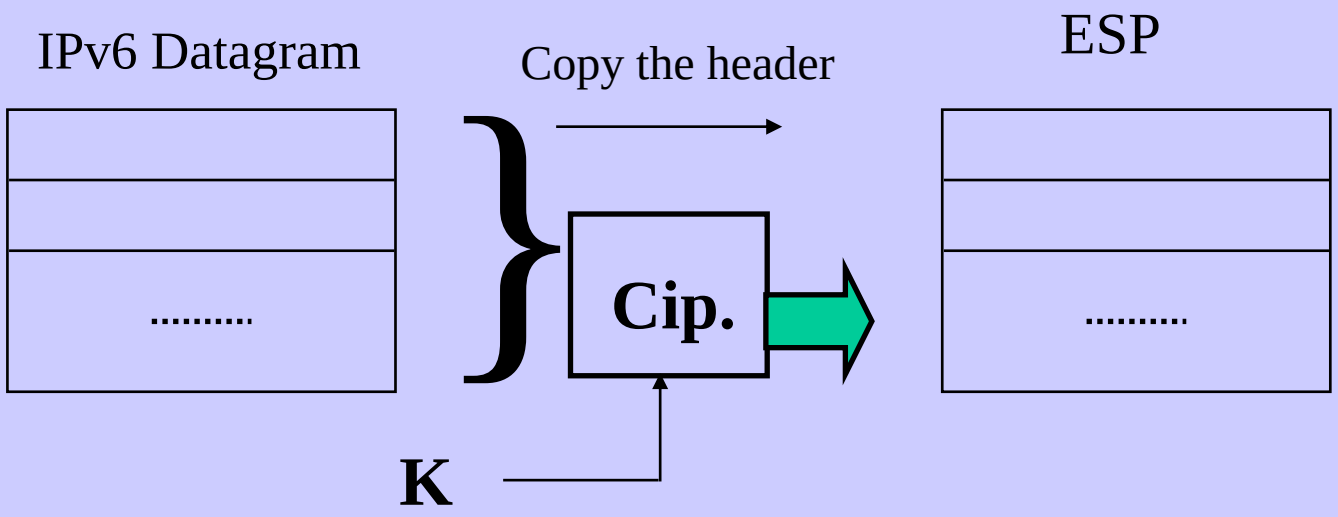
Encapsulación Segura del Campo de Carga

- Integridad, autenticación y confidencialidad
  - Encapsulación cifrada del datagrama IP (ESP)
- Cabecera no cifrada
  - se utiliza para conducir los datos protegidos a través de la red. El receptor retira y descarta la cabecera y sus opciones no cifradas
- La utilización de ESP puede provocar un decremento importante del rendimiento y la latencia de las comunicaciones de los sistemas de información.

ESP

- Encapsulating Security Payload

  Se cifra el datagrama y este se incluye en un paquete ESP.



ESP

- Formato

Security Parameter Index
Sequence Number Field
Encrypted Data and Parameters
Authentication Data

- Colocación

IPv6 Header	ESP Header	ESP Payload	ESP Trailer	Auth. Data

IKE en general

- Internet Key Exchange (IKE) permite que dos extremos se autentiquen mutuamente y establezcan un canal seguro.
- A continuación, IKE permitirá negociar las asociaciones de seguridad (SA) del protocolo IPsec.

Internet Key Exchange

- Alternativa al intercambio manual de claves
- Su objetivo es la negociación de una Asociación de Seguridad (AS) IPsec
- Se trata de un protocolo en dos fases
  - Fase I
    - Protección del canal de comunicación
      - AS ISAKMP
    - Modos de funcionamiento
      - Main (principal), Aggresive (acelerado) y Base
  - Fase II
    - Negociación de un par de AS
      - AS IPSEC
    - Quick Mode (rápido)

IKE

- Fase I
  - Autenticación
    - Secreto compartido (PSK)
    - Firma digital
    - Cifrado de clave pública
    - Kerberos
  - Intercambio (Main Mode)

```
Initiator                          Responder
----------                               -----------

HDR, SA                  -->

                         <--     HDR, SA

HDR, KE, Ni              -->

                         <--     HDR, KE, Nr

HDR*, IDii, HASH_I       -->

                         <--     HDR*, IDir, HASH_R
```

IKE

- Fase II
  - Negociación de AS IPSEC (una o varias)
- Quick Mode

```
Initiator                              Responder

    -----------                            -----------

     HDR*, HASH(1), SA, Ni

       [, KE ] [, IDci, IDcr ] -->

                                    <--    HDR*, HASH(2), SA, Nr

                                                  [, KE ] [, IDci, IDcr
]

     HDR*, HASH(3)                  -->
```

IKE

- Esquema general para la negociación de parámetros de seguridad
- Definición de Dominios de Interpretación (DoI)
- Gestión común de la negociación
  - Nuevos protocolos de cualquier capa de la pila de red
  - Protocolos actuales de seguridad

L2TP/IPSec

- Encapsulado L2TP de la trama PPP.
- Encapsulado IPSec del mensaje L2TP.
- Cifrado IPSEc del contenido de los paquetes L2TP.
- De los protocolos de IPSec (AH y ESP) se utiliza ESP (Encapsulating Security Payload).