2. Protocoale de Securitate la Nivel Reţea

IPSec

- Completează IPv4 cu facilităţi de securitate
- Protocol de Nivel 3+
- Pune la dispoziţia protocoalelor de pe nivelul superior (TCP, UDP) servicii de comunicaţie securizate
- Pentru a suporta IPSec, stiva TCP/IP de pe clienţi sau gateway-uri trebuie modificată

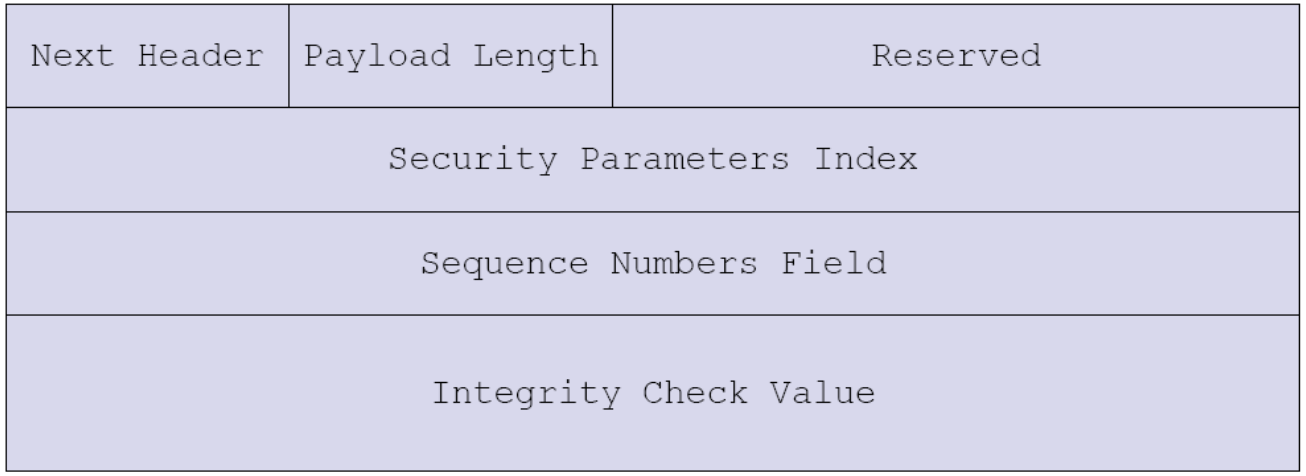
Arhitectura IPSec

- Descris în cadrul mai multor RFC
  - RFC 4301: An overview of the IPSec security architecture
  - RFC 4302: Specification of AH
  - RFC 4303: Specification of ESP
  - RFC 4305: Specification of algorithms for AH and ESP
  - RFC 4306: Specification of IKEv2
  - …
- Destul de complex, foarte multe opţiuni
- Probleme de interoperabilitate între diferite implementări

AH şi ESP

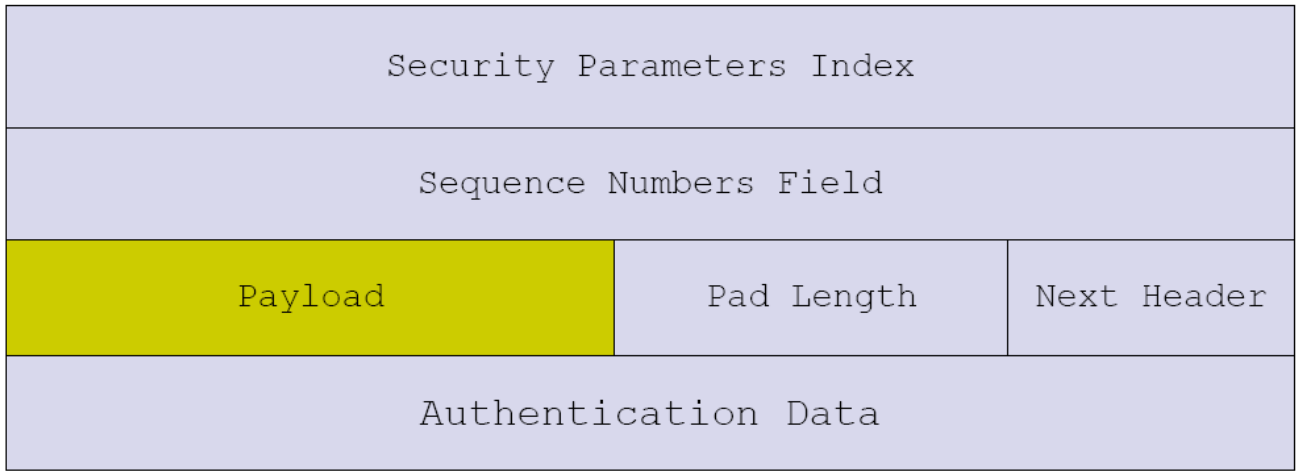
- Authentication Header Protocol (AH)
  - Integritatea pachetelor
  - Autentificarea originii datelor
- Encapsulating Security Payload Protocol (ESP)
  - Confidenţialitatea datelor
  - Autentificarea originii datelor
- Pot fi folosite independent sau combinat
- Moduri de operare
  - Transport
  - Tunel

Authentication Header Protocol



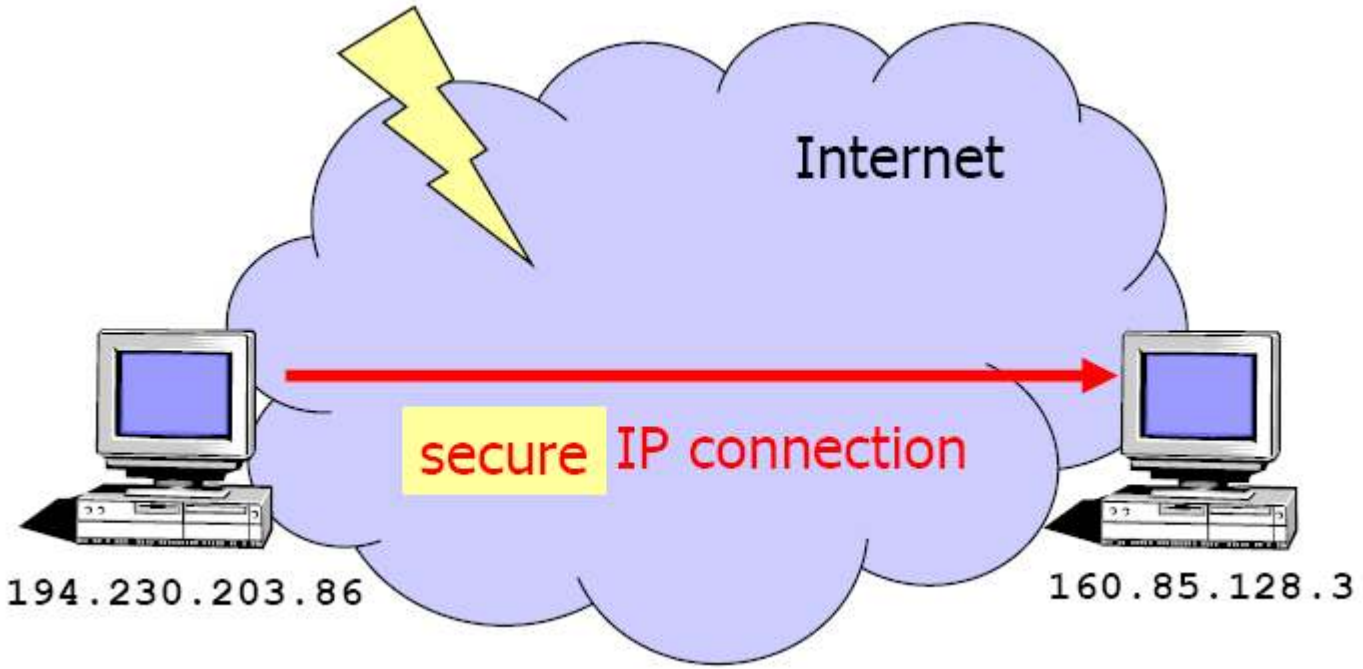
- **Numărul de protocol pentru AH este 51**
- **Numărul de secvenţă evită atacurile prin reluare**
- **Câmpul Integrity *Check Value* este calculat pentru toate câmpurile din pachetul IP cu excepţia celor ce pot suferi modificări (TOS, TTL, CRC, etc)**

Encapsulating Security Payload Protocol

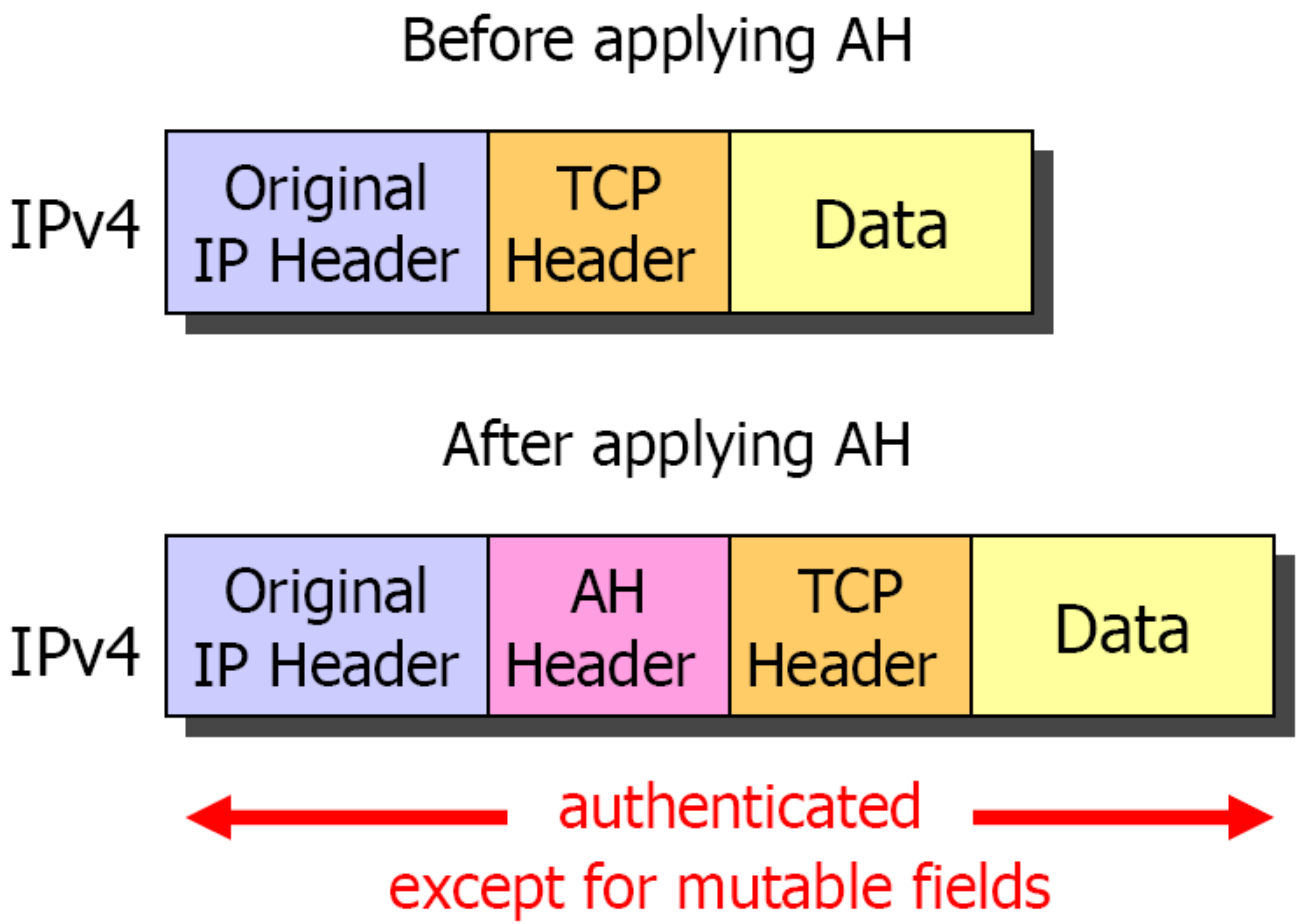


- **Numărul de protocol pentru ESP este 50**
- ***Authentication Data* este calculat numai pentru câmpurile din ESP**

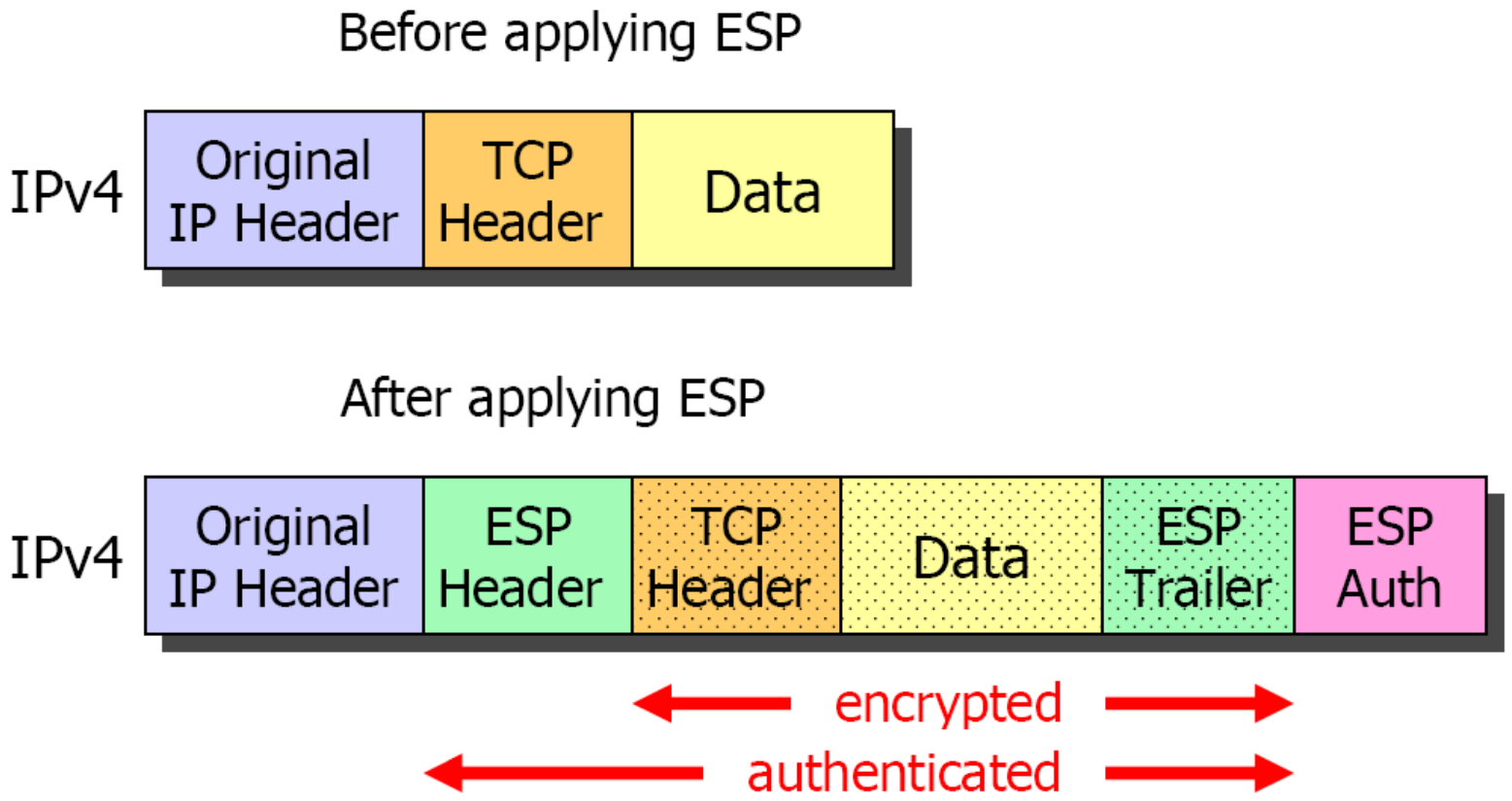
IPSec – Modul Transport



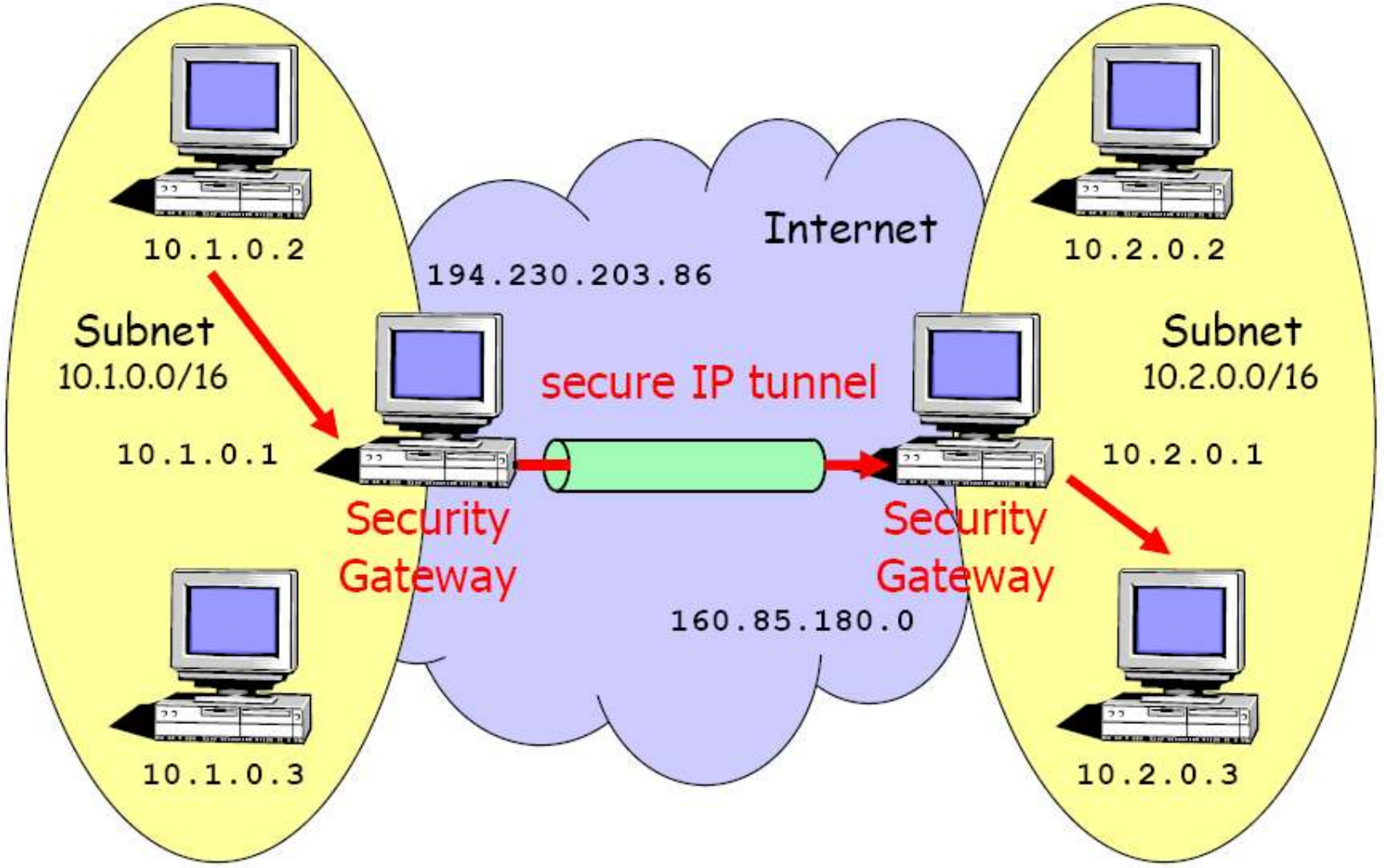
IPSec – Modul Transport (AH)



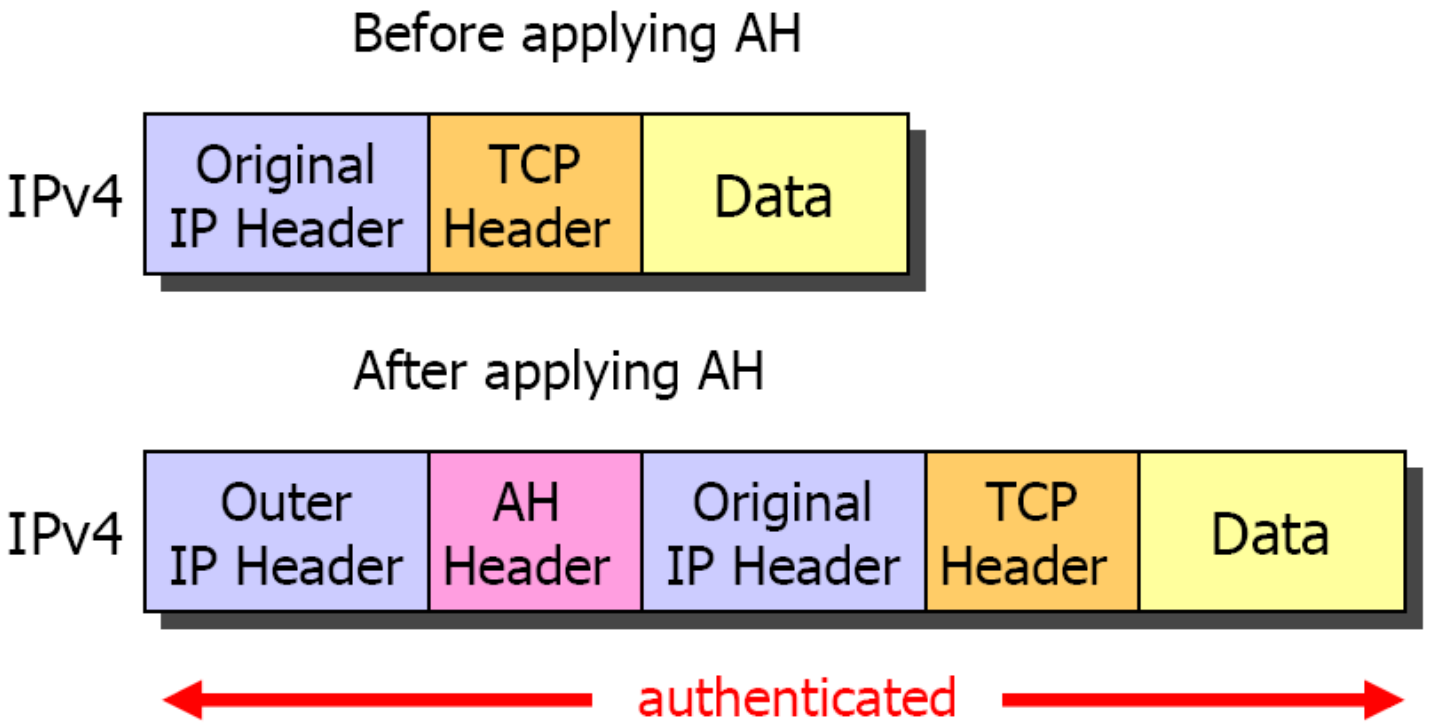
IPSec – Modul Transport (ESP)



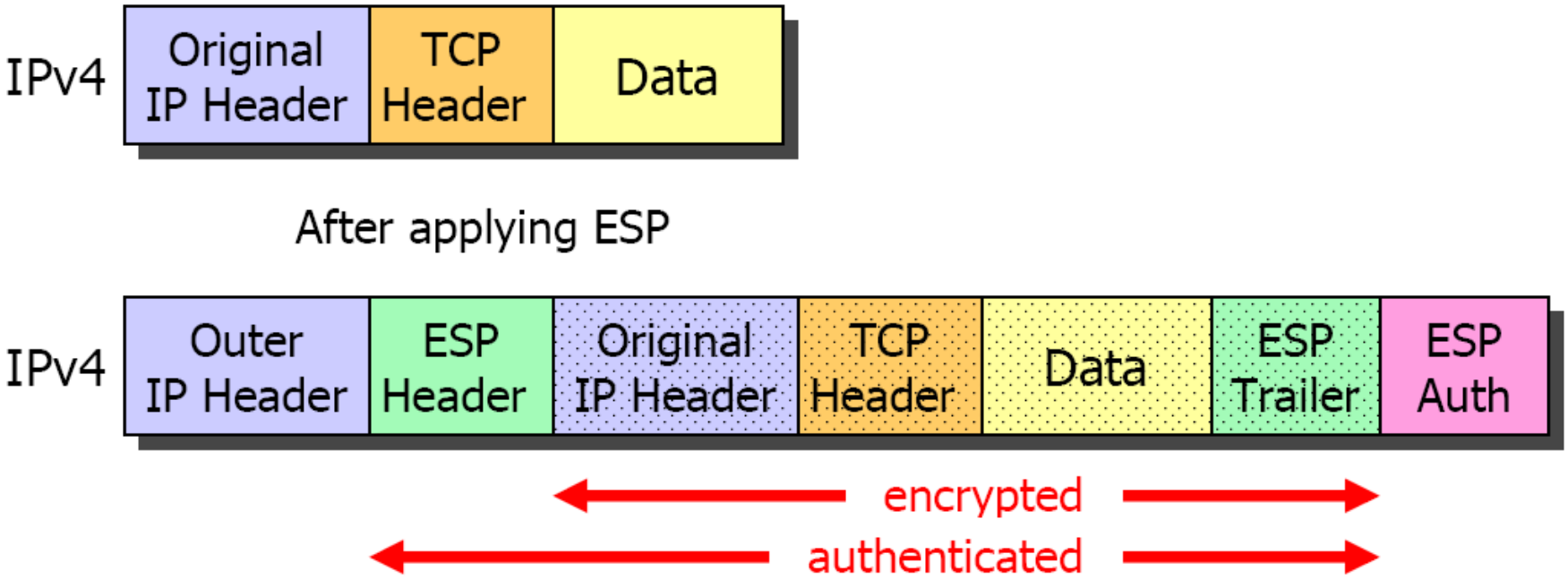
IPSec – Modul Tunel



IPSec – Modul Tunel (AH)



IPSec – Modul Tunel (ESP)



Security Association (SA)

- Un SA este un “contract” stabilit între cele două capete ale tunelului IPSec
  - parametrii criptografici (algoritmi, chei, etc)
  - timp de viaţă
- SA sunt stocate într-o bază de date. Fiecare SA are asociat un SPI (Security Parameters Index) pentru a putea fi regăsit în baza de date

Internet Key Exchange

- Managementul asocierilor de securitate (SA)
  - manual
  - automat
- ISAKMP (Internet Security Association and Key Management)
  - framework pentru managementul cheilor şi asocierilor de securitate
- IKE (Internet Key Exchange)
  - stabilirea parametrilor criptografici
    - algoritmul de criptare, funcţia hash, metoda de autentificare, etc
  - autentificarea mutuală între entităţi
    - pre-shared keys sau certificate digitale
  - stabilirea cheii de sesiune
    - Diffie-Hellman (DH)
  - foloseşte portul UDP 500 pentru comunicaţie
  - RFC 4306 (IKE v2)

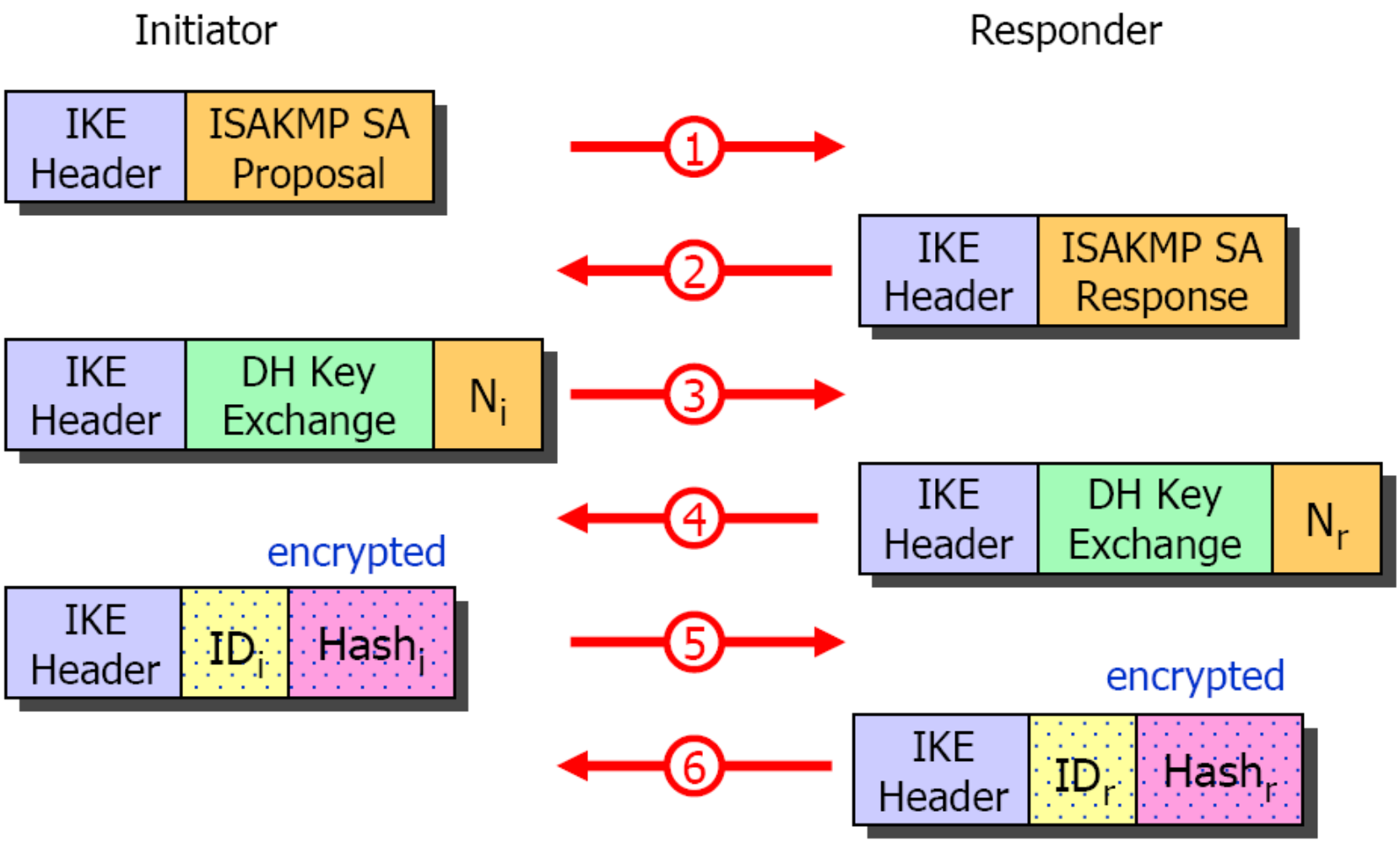
Moduri de lucru

- **Faza 1**
  - negocierea unui SA iniţial (ISAKMP SA)
  - Modul principal
    - 6 mesaje
  - Modul agresiv
    - 3 mesaje
    - nu asigură protecţia identităţii
- **Faza 2**
  - negocierea unui SA general (IPSec SA)
  - reîmprospătarea cheilor de sesiune
  - Modul rapid

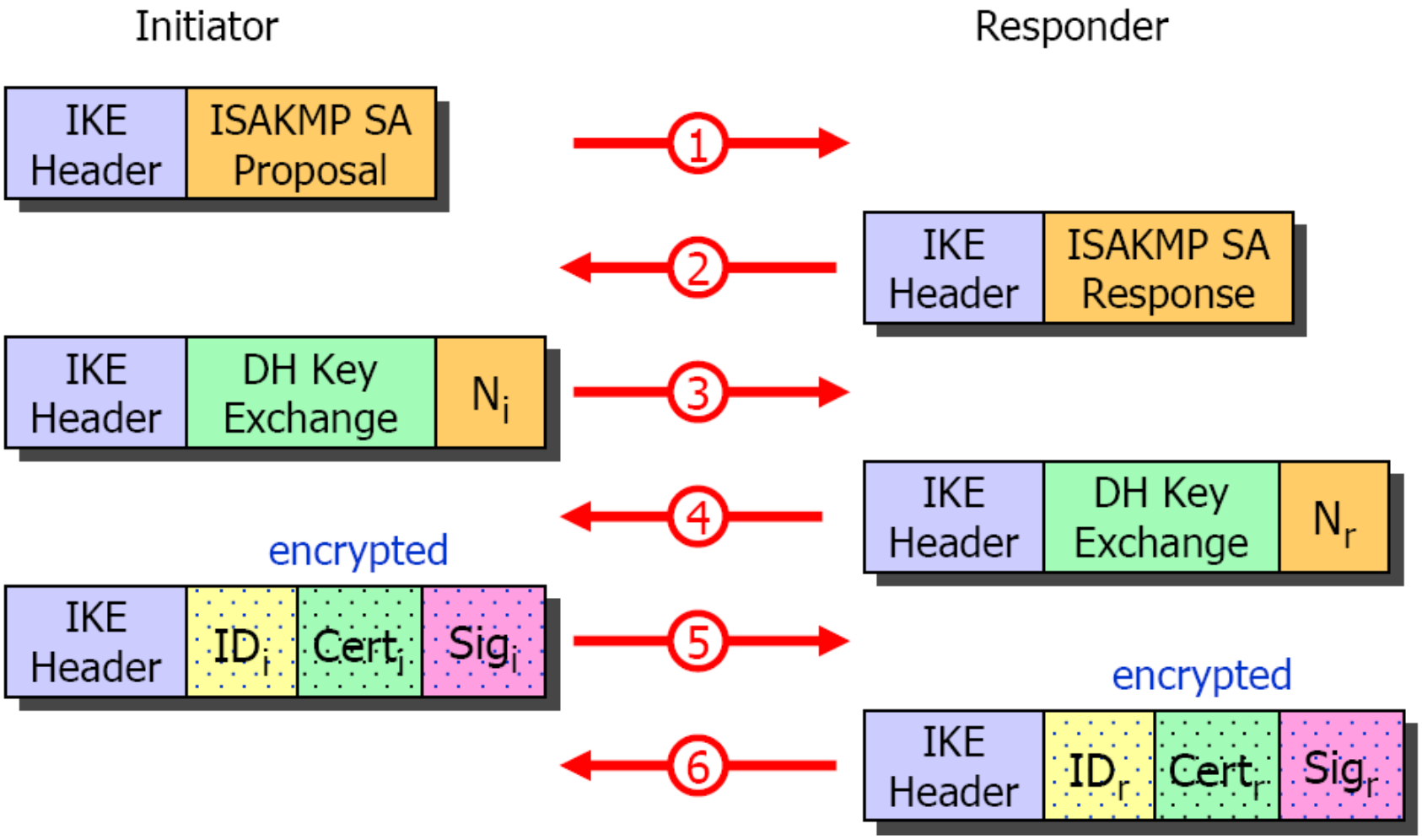
Moduri de lucru (cont.)

- Se foloseşte modul principal / agresiv pentru a stabili un SA iniţial (ISAKMP SA)
- Se foloseşte modul rapid pentru a negocia un SA general (IPSec SA)
- Se foloseşte IPSec SA pentru transmiterea datelor până când acesta expiră şi trebuie negociat un nou IPSec SA
- Se foloseşte modul rapid pentru reînnoirea IPSec SA

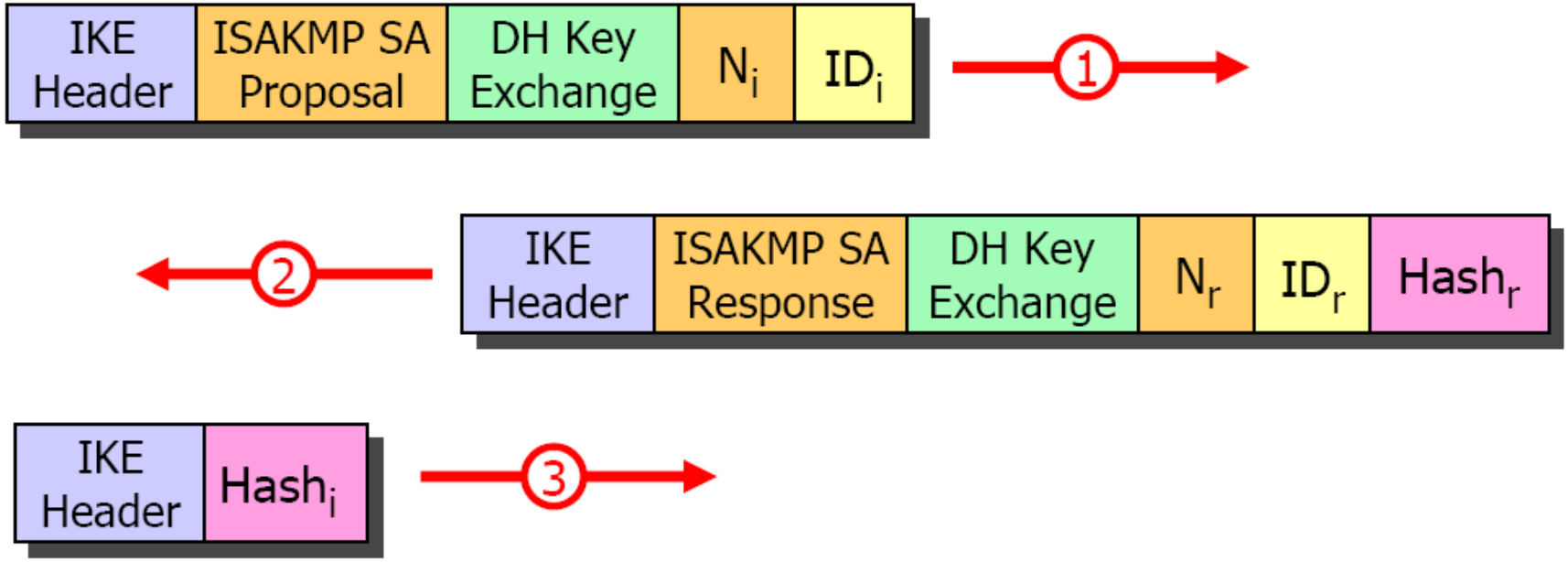
IKE - Modul Principal



IKE - Modul Principal (cont.)



IKE – Modul Agresiv



IKE – Modul Rapid

- Schimb de mesaje criptate folosind cheia de sesiune stabilită în faza anterioară
- Negocierea parametrilor pentru IPSec SA
- 3 mesaje
- IPSec SA este bidirecţional (unul pentru conexiunea de intrare şi unul pentru conexiunea de ieşire)
- Schimbarea periodică a cheilor de sesiune
  - Perfect Forward Secrecy

Consideraţii privind implementarea IPSec VPN

- Algoritmi criptografici recomandaţi
  - Criptarea datelor: 3DES, AES
  - Integritatea datelor: SHA-1
- Fragmentarea pachetelor
  - antetele AH şi ESP cresc dimensiunea pachetelor
  - scăderea performanţei reţelei
- Translaţia de adresă (NAT)
  - translaţia de adresă modifică pachetele IP! (distruge integritatea datelor)
  - folosire NAT înainte de IPSec
  - IPSec NAT Traversal (NAT-T)
    - încapsularea pachetelor IPSec în datagrame UDP
- Configurare firewall
  - AH (IP Protocol Number 51), ESP (IP Protocol Number 50)
  - IKE (UDP Port 500)
  - IPSec NAT-T (UDP Port 4500)
- Suport pentru mecanisme extinse de autentificare
  - Extended Authentication (XAUTH)
    - RADIUS, TACACS+, RSA SecurID