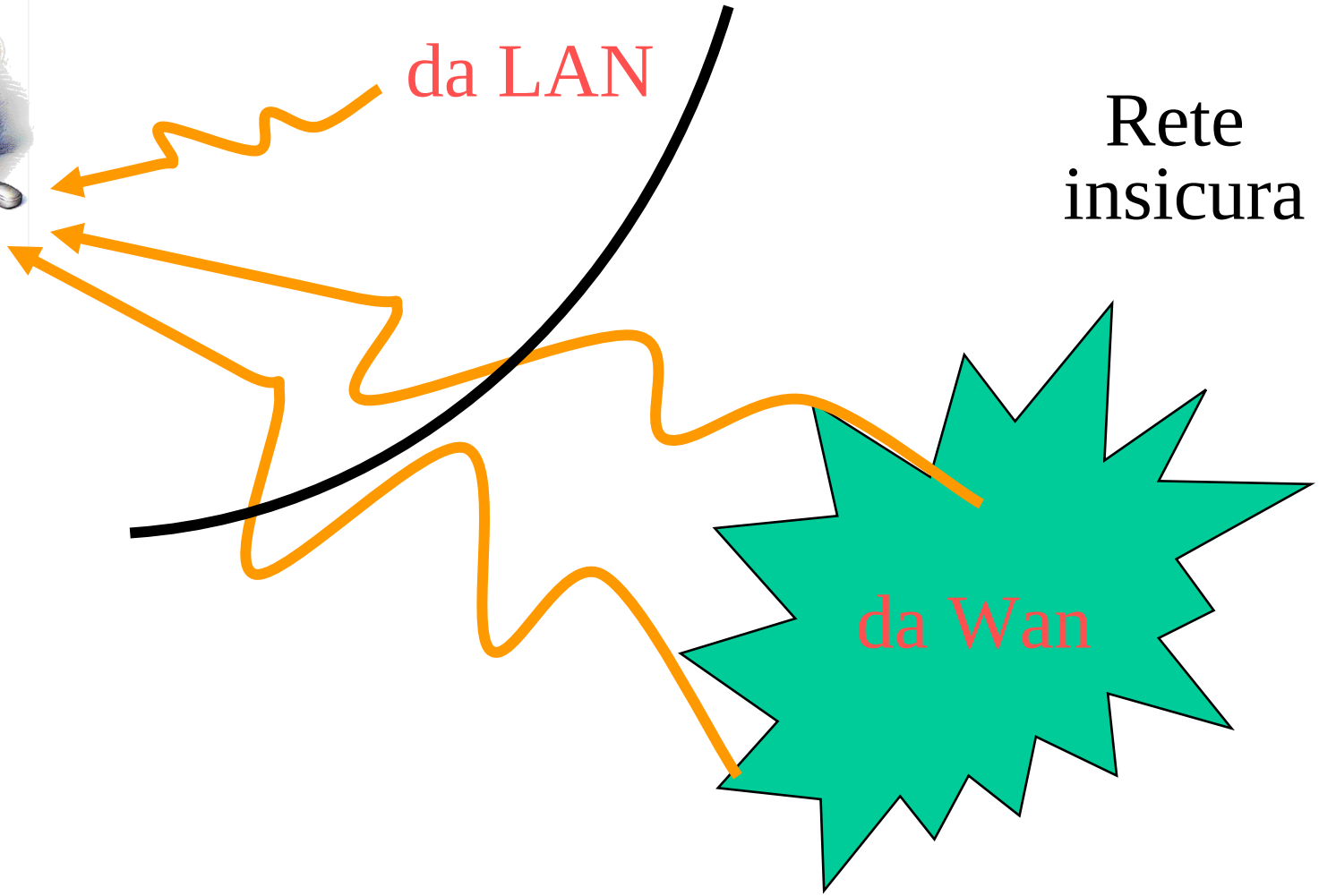
Connettere più LAN in modo sicuro con IPsec

Prof. Francesco Bergadano

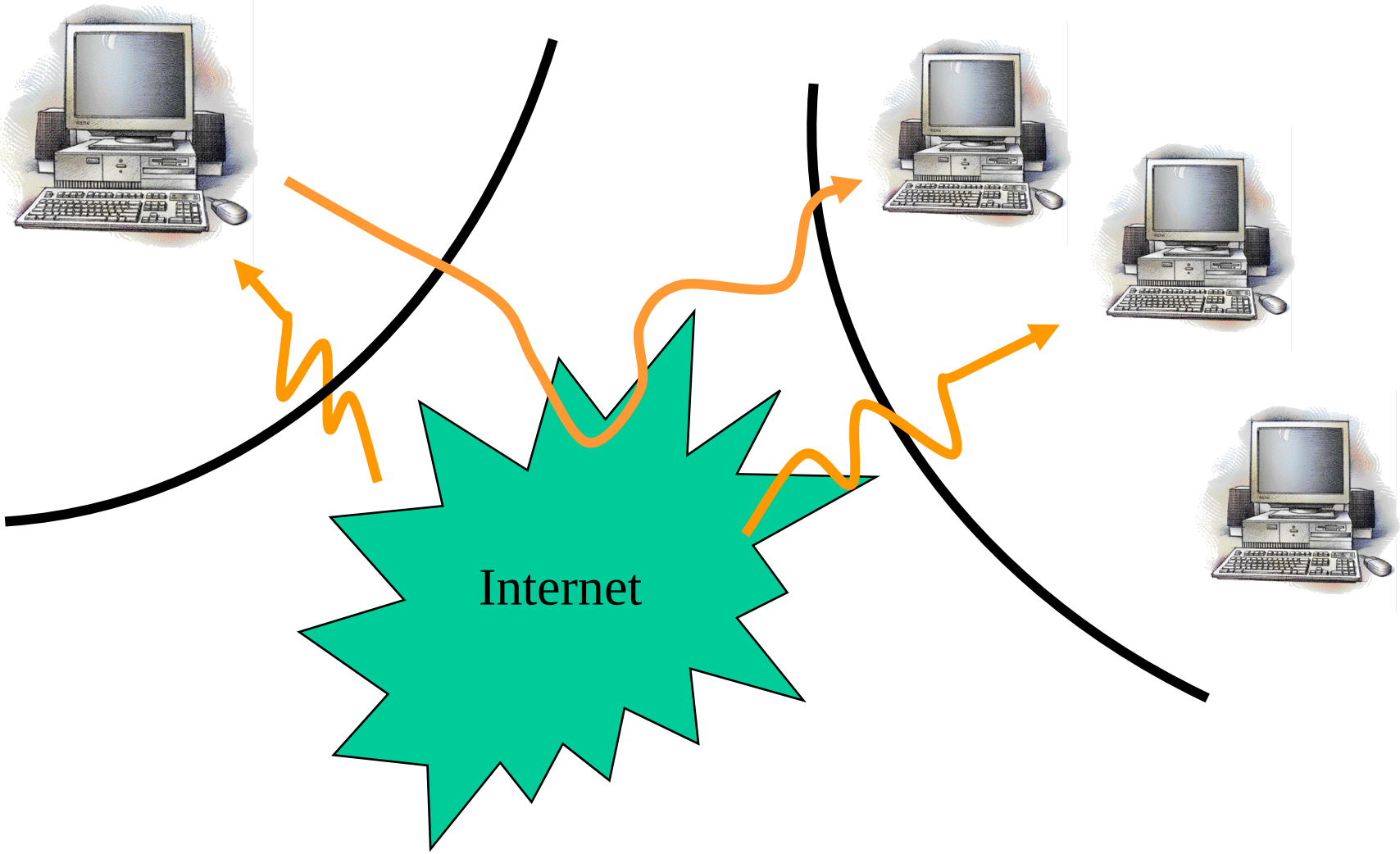
Dipartimento di Informatica

Università di Torino

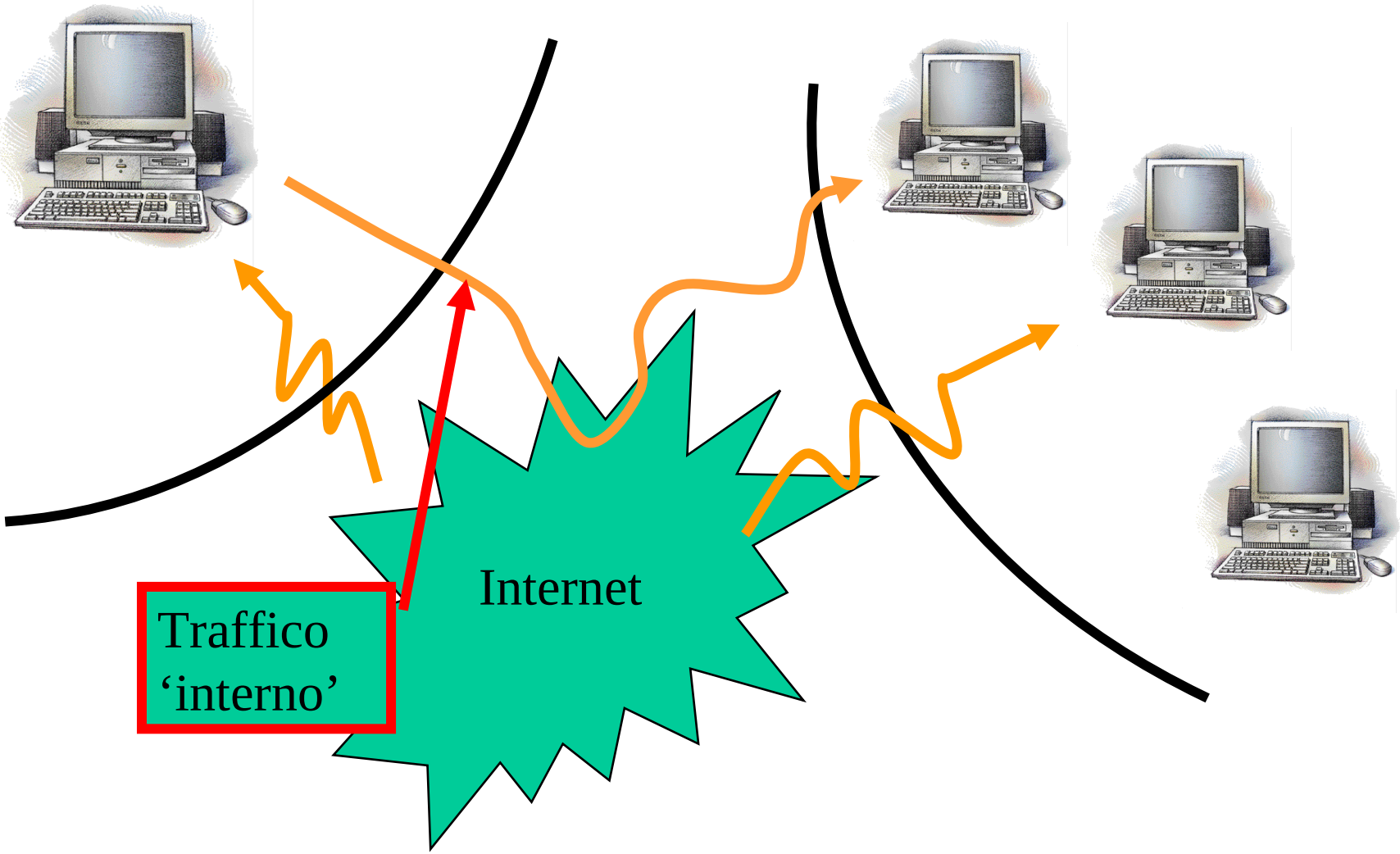
Sicurezza Rete Locale (LAN)



Sicurezza Reti Locali (LANs)



Sicurezza Reti Locali (LANs)



Obiettivi

- Avere la stessa sicurezza che avremmo con un un’unica rete locale
- Permettere anche traffico da e verso reti esterne, se necessario attraverso un Firewall
- Non introdurre ritardi significativi
- Non richiedere operazioni di riconfigurazione agli utenti (trasparenza)

Una buona soluzione:

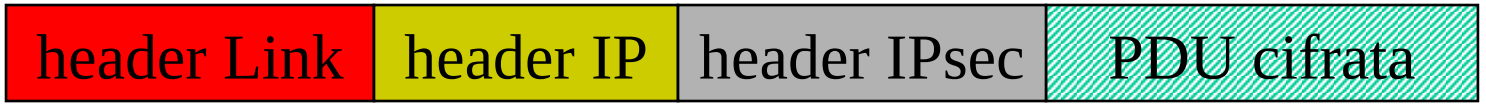
VPN (Virtual Private Network)

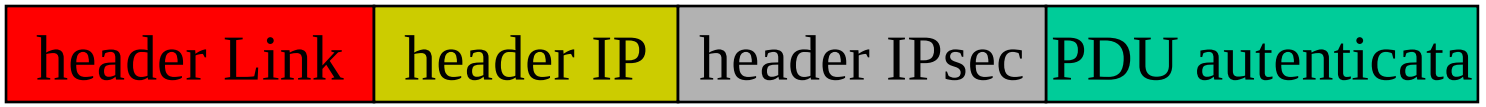
Esempio: IPsec (IP level security)

Schema generale descritto in RFC 1825 - “Security Architecture for the Internet Protocol”

IPsec - idea fondamentale

La PDU (Protocol Data Unit) trasportata dal pacchetto IP è cifrata e/o autenticata, e all'header IP vengono aggiunte informazioni che permettono al ricevente autorizzato di decifrare e/o di verificare l'autenticità e l'integrità del messaggio





Conseguenze

- I router vedono indirizzo mittente e destinatario così come appaiono nell’header IP
- I router non vedono la PDU se cifrata
- I router non possono modificare i messaggi senza che ciò sia visibile per il ricevente se la PDU è autenticata

Altre conseguenze

- Le reti aziendali sono protette da intercettazioni e modifiche su Internet
- Cifratura e autenticazione vengono gestite solo sulle LAN sorgente e destinazione
- IPsec non protegge da attacchi all'interno delle LAN private e dai rischi di sicurezza legati a servizi offerti verso l'esterno (per i quali non vi è cifratura/autenticazione a livello IP).

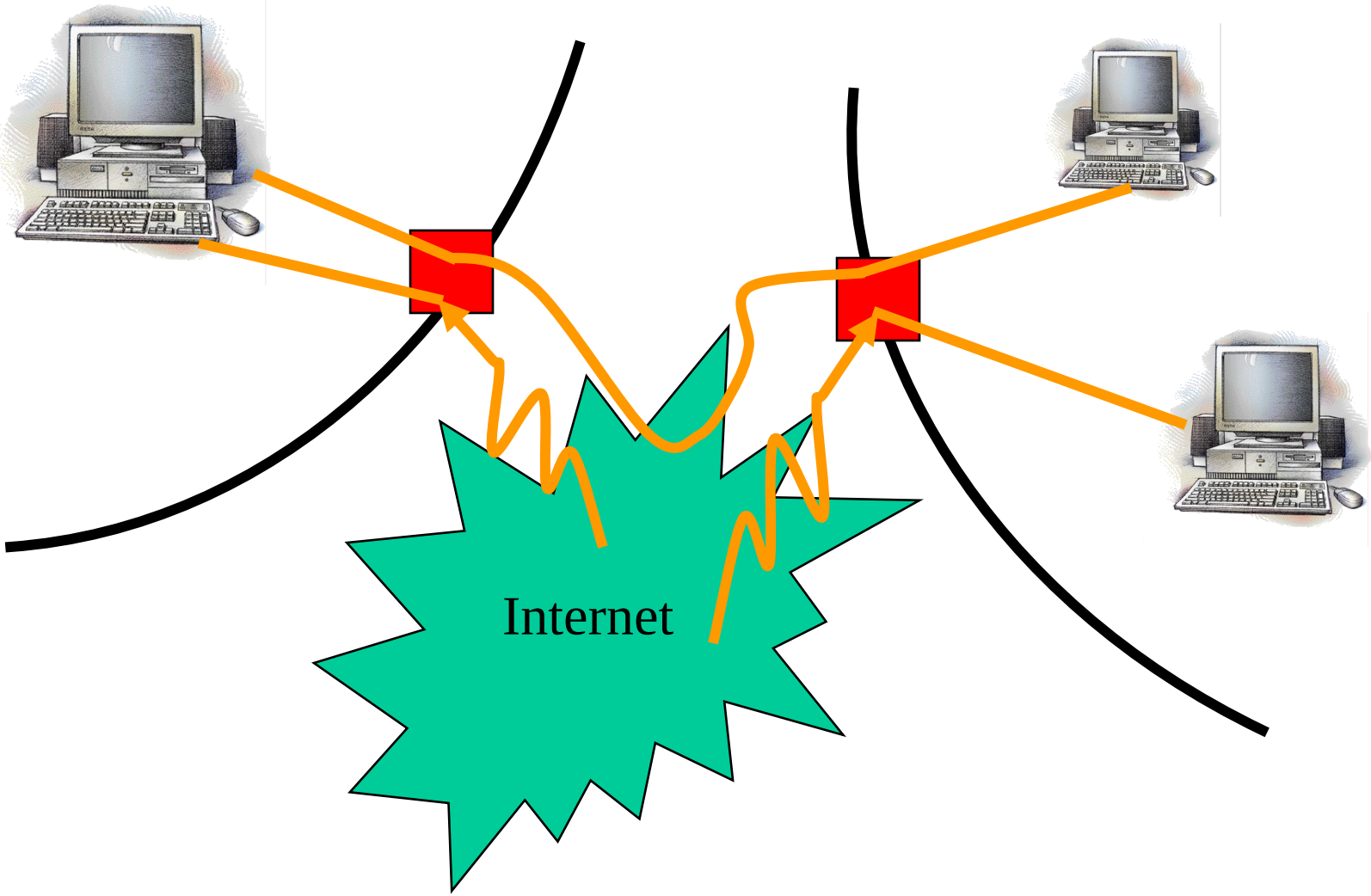
Problemi

- Come mascherare anche il traffico (nascondere indirizzi mittente e destinatario)?
- Come proteggersi da sniffing/spoofing all'interno delle LAN private?

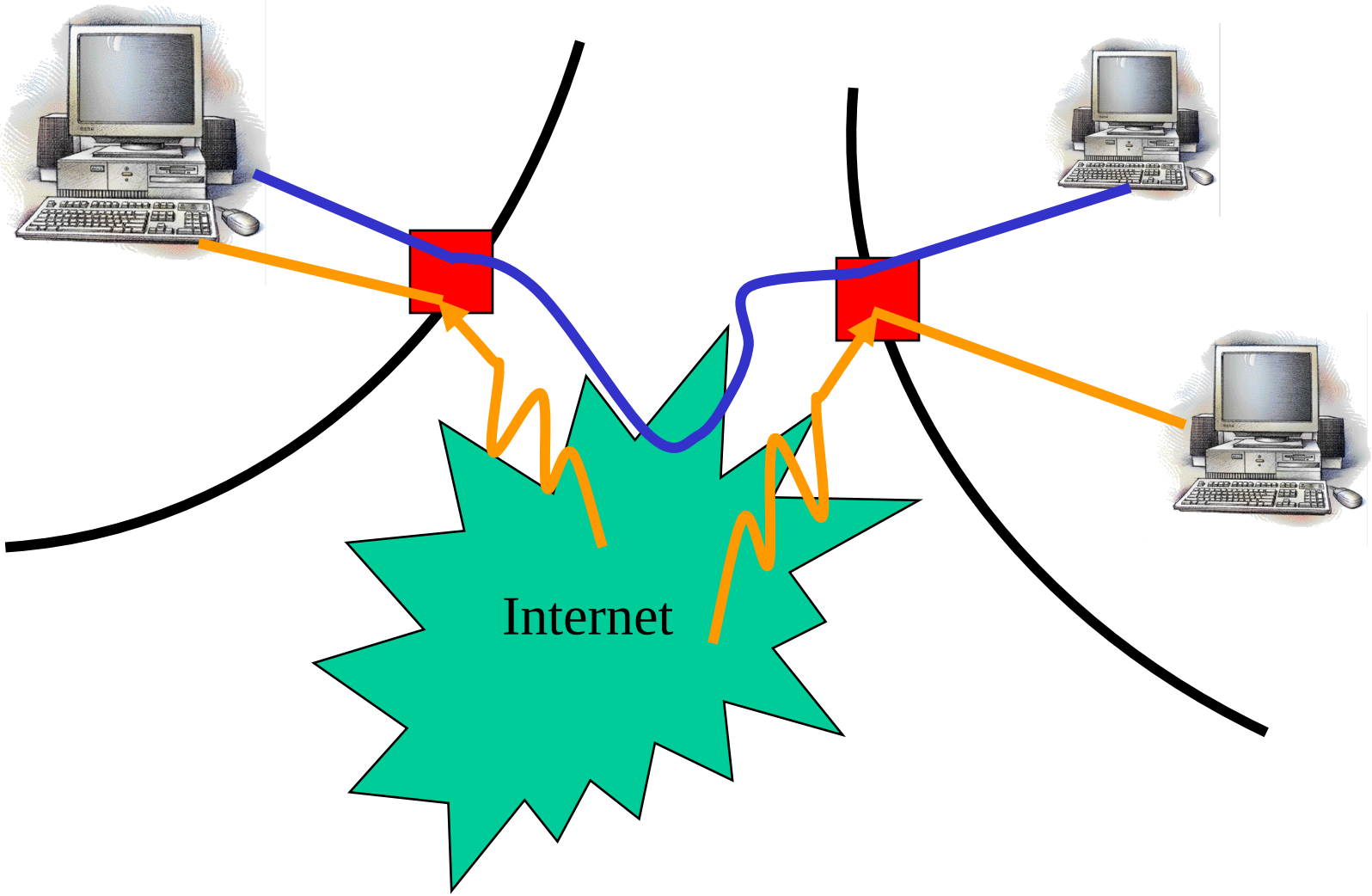
IPsec

- Trasport mode (cifratura e autenticazione su computer mittente e destinatario)
- Tunnel mode (cifratura e autenticazione su firewall o su router)

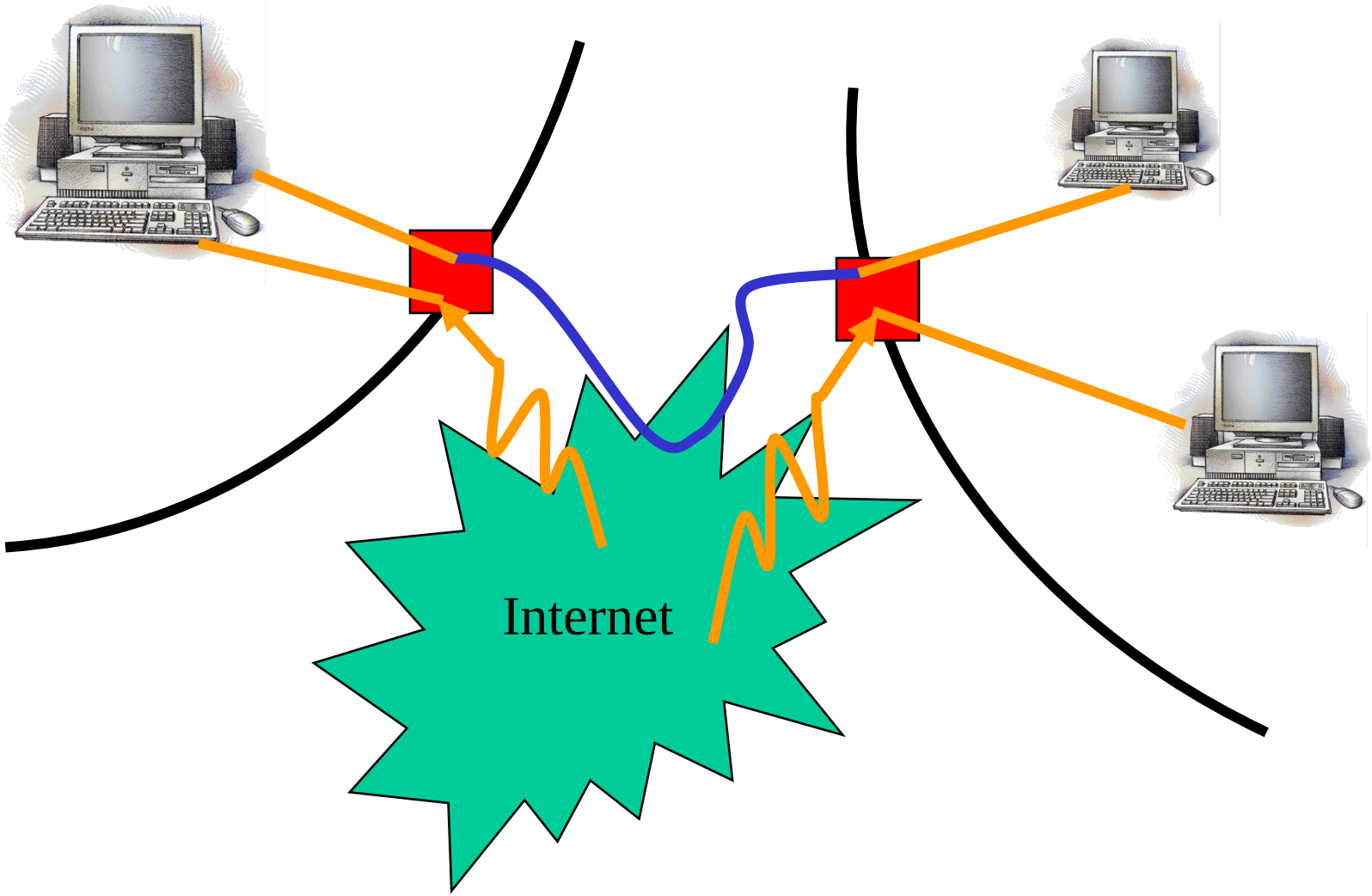
Transport/Tunnel mode



Transport mode



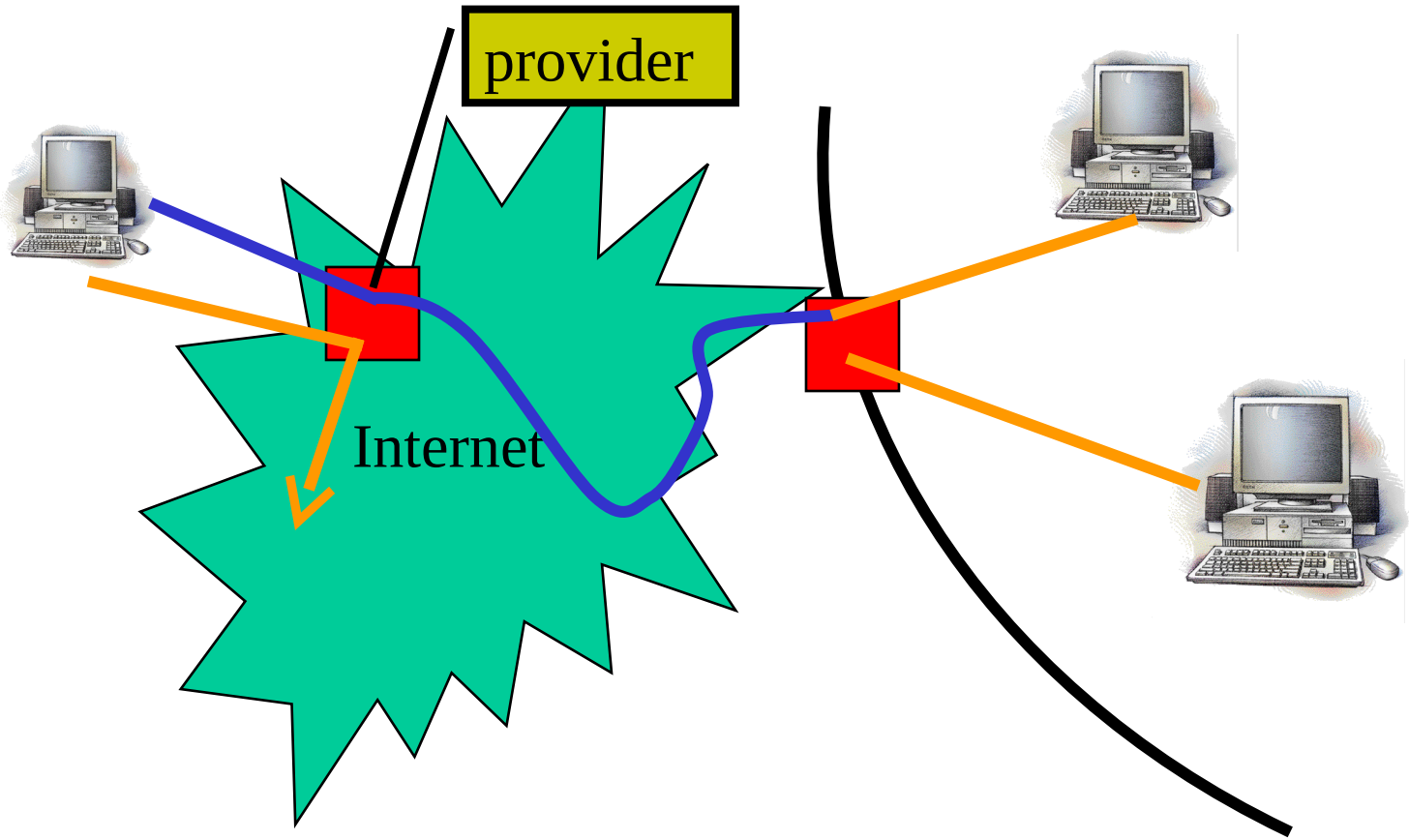
Tunnel mode



Transport mode

- Protegge da sniffing/spoofing su rete locale
- Rende visibile su Internet gli indirizzi mittente e destinatario
- Richiede una speciale configurazione del computer utente (non trasparente)
- Necessario per traffico da postazione mobile

Soluzione mista per postazione mobile



Tunnel mode

- Non protegge da sniffing/spoofing su rete locale
- Nasconde gli indirizzi dei singoli computer mittente e destinatario, non nasconde gli indirizzi della rete mittente e destinazione
- E’ trasparente all’utente singolo
- Veloce, prodotti affidabili per rouuter/firewall

Tunnel mode

- Non protegge da sniffing/spoofing su rete locale
- Nasconde gli indirizzi dei singoli computer mittente e destinatario, non nasconde gli indirizzi della rete mittente e destinazione
- E’ trasparente all’utente singolo
- Veloce, prodotti affidabili per rouuter/firewall

Servizi IPsec

- Autenticazione
  (AH -Authentication Header - RFC 1826)
- Cifratura (ESP - Encapsulating Security Payload - RFC 1827)

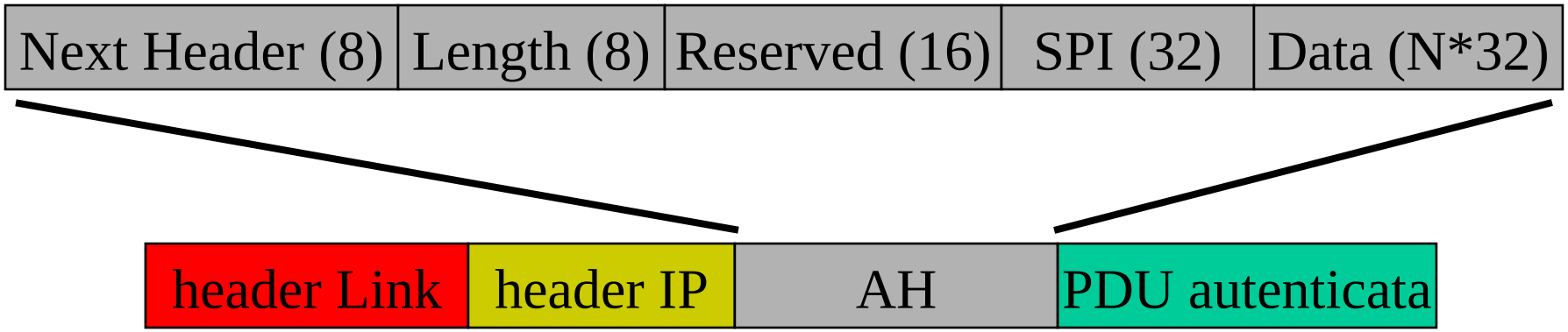
Cifratura e autenticazione sono simmetriche

AH - Authentication Header

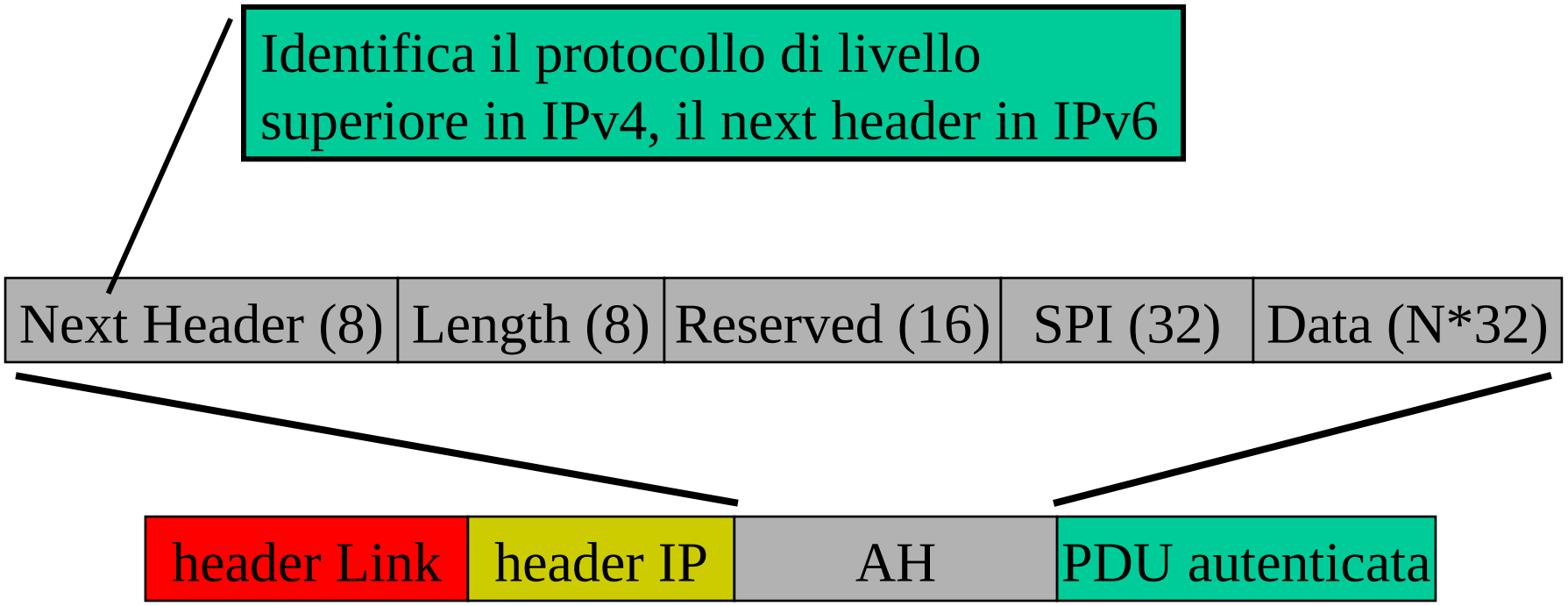
- Serve per autenticare il traffico IP, normalmente tra due LAN private, per evitare modifiche e falsificazioni

AH - Authentication Header

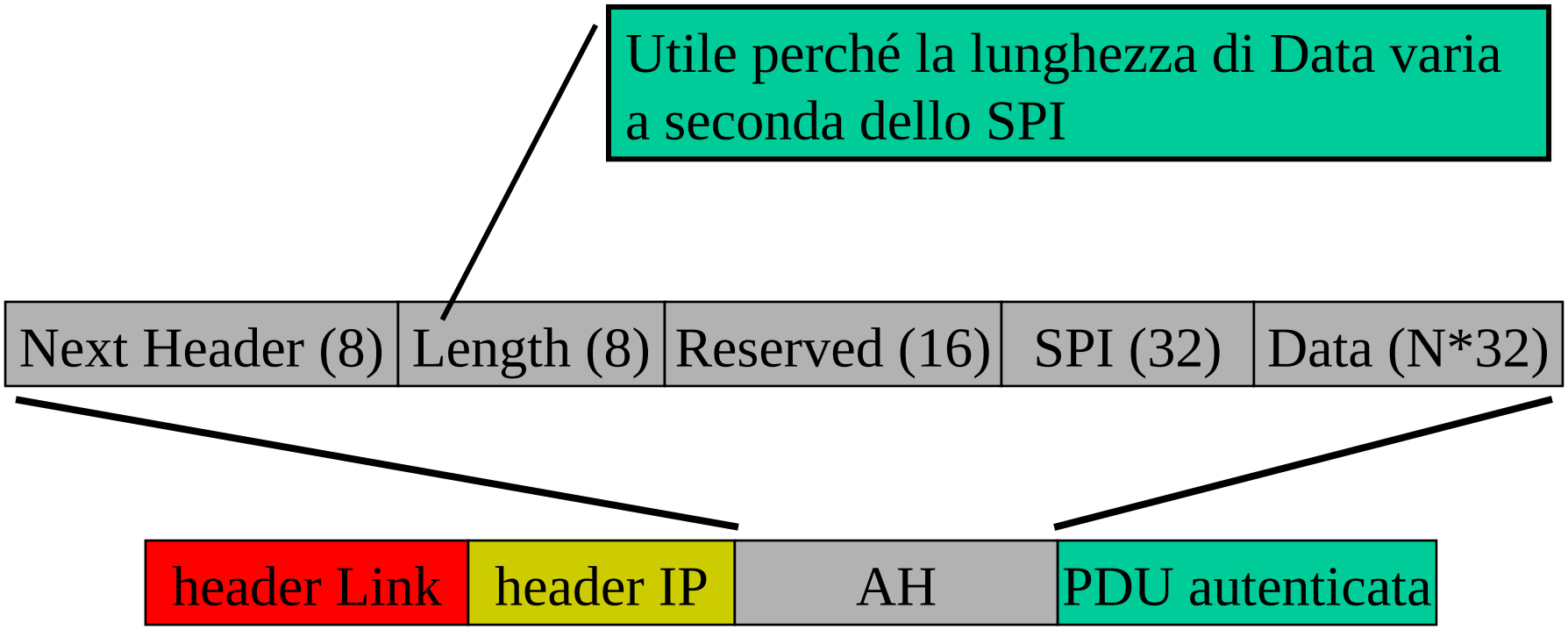
- Serve per autenticare il traffico IP, normalmente tra due LAN private, per evitare modifiche e falsificazioni



AH - Authentication Header

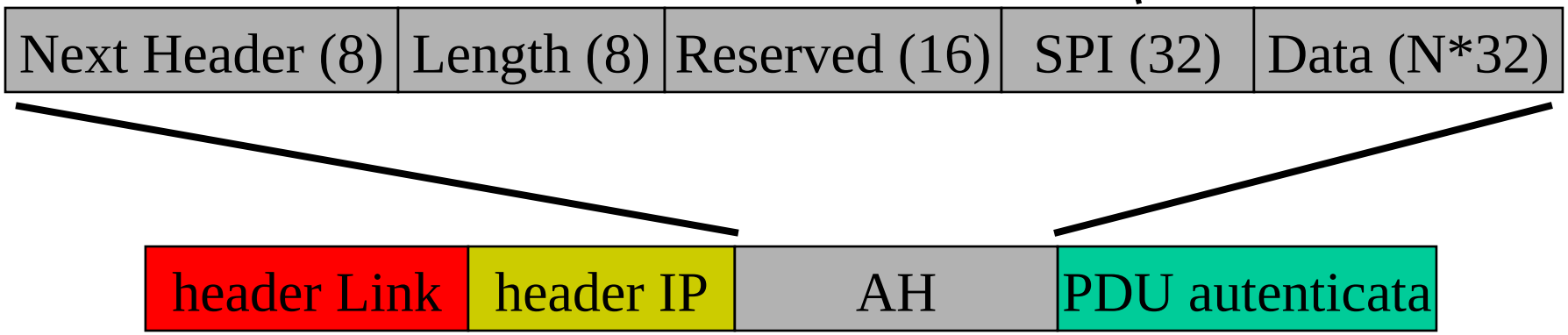


AH - Authentication Header



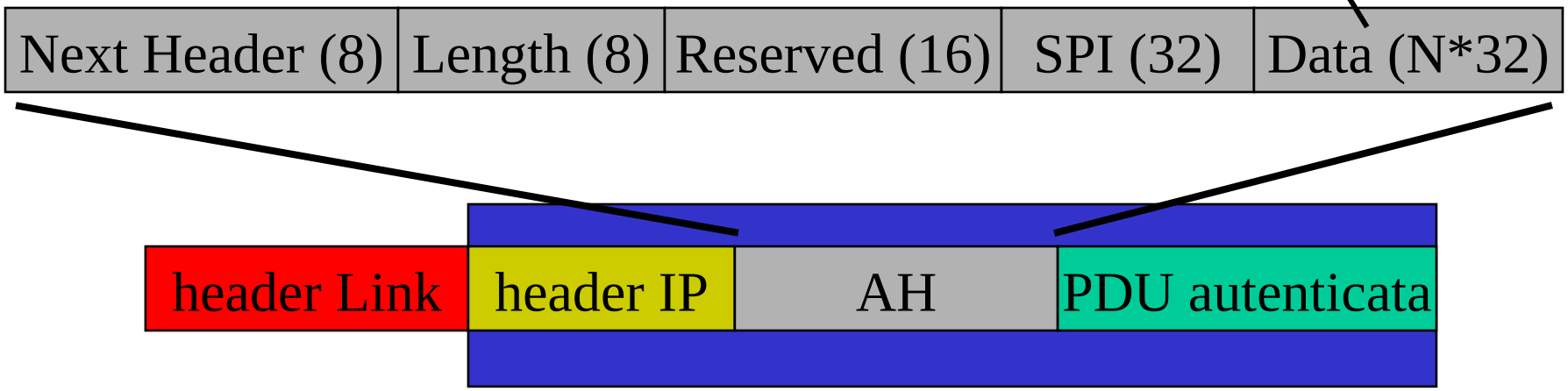
AH - Authentication Header

Security parameters index: identifica un indice dell'algoritmo e delle chiavi crittografiche



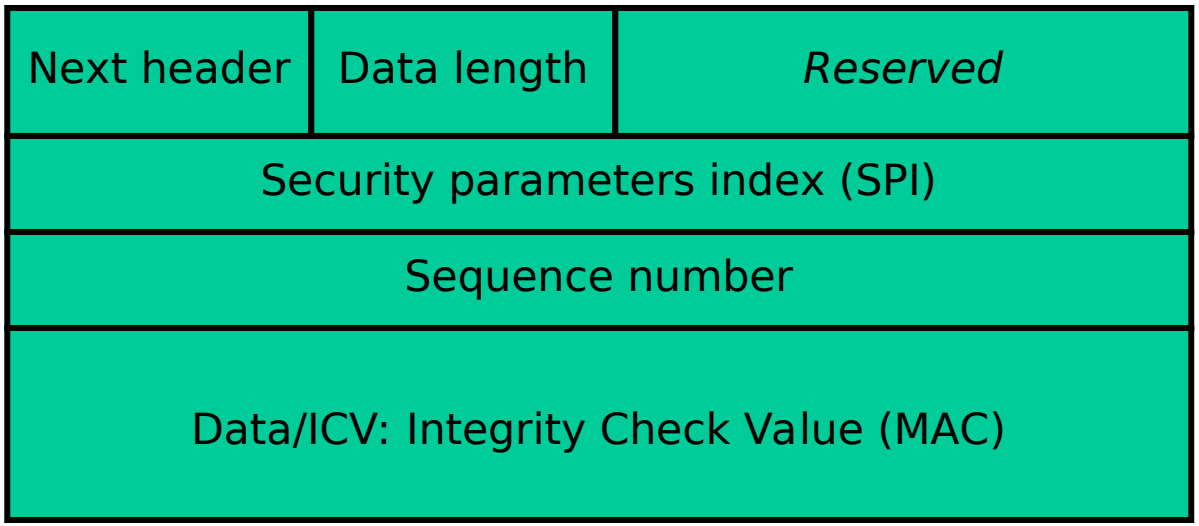
AH - Authentication Header

Codici di autenticazione (MAC) riferiti a tutto il pacchetto, ma dove i campi variabili (TTL, checksum) sono uguali a 0



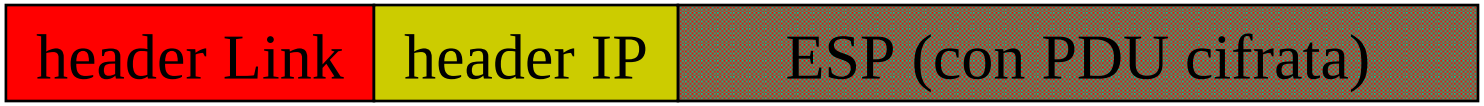
AH - Authentication Header

- L’authentication header non serve per evitare intercettazioni e non permette di nascondere gli specifici indirizzi IP di mittente e destinatario.



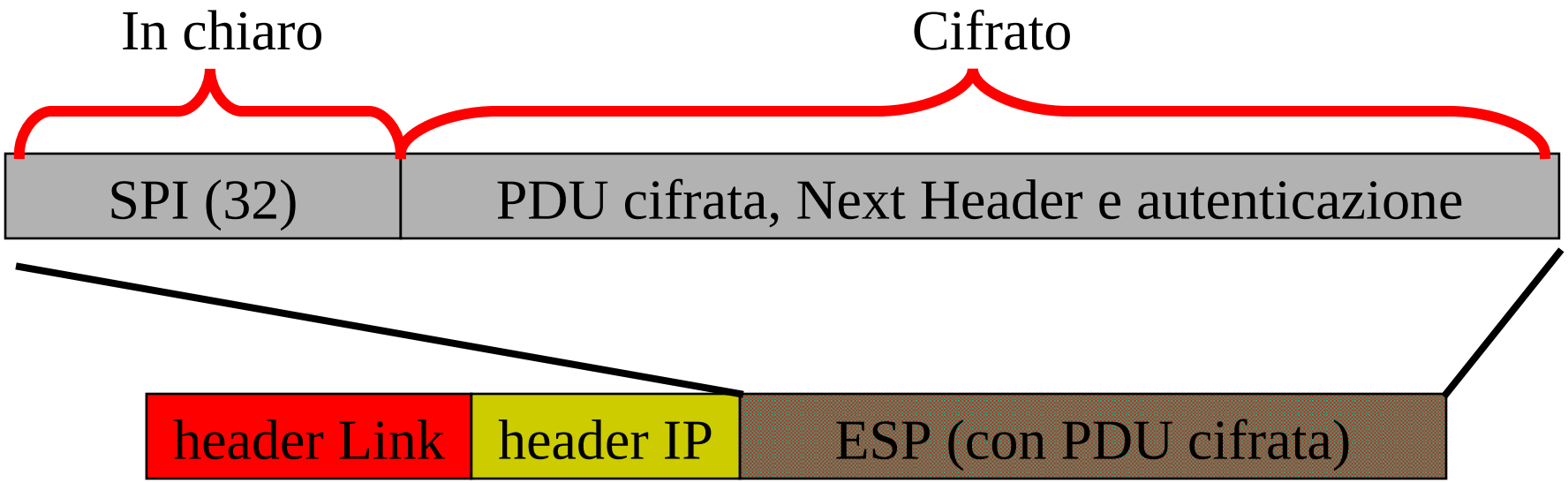
ESP - Encapsulating Security Payload

- Serve per cifrare il traffico IP, normalmente tra due LAN private, per evitare intercettazioni



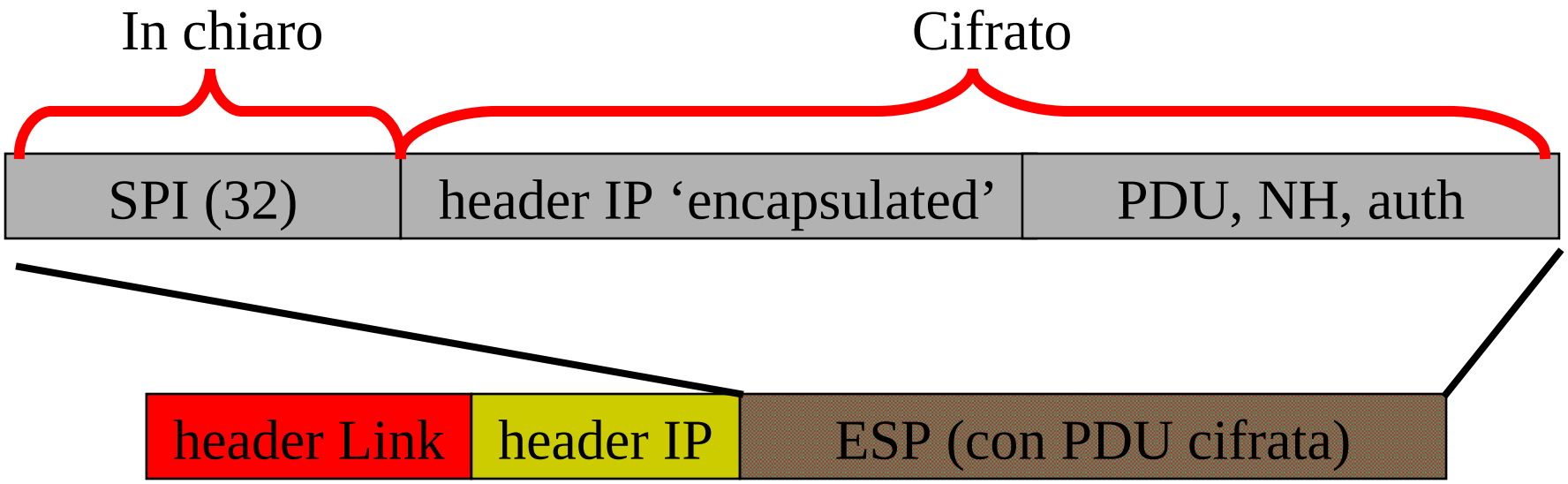
ESP - Encapsulating Security Payload

Transport mode

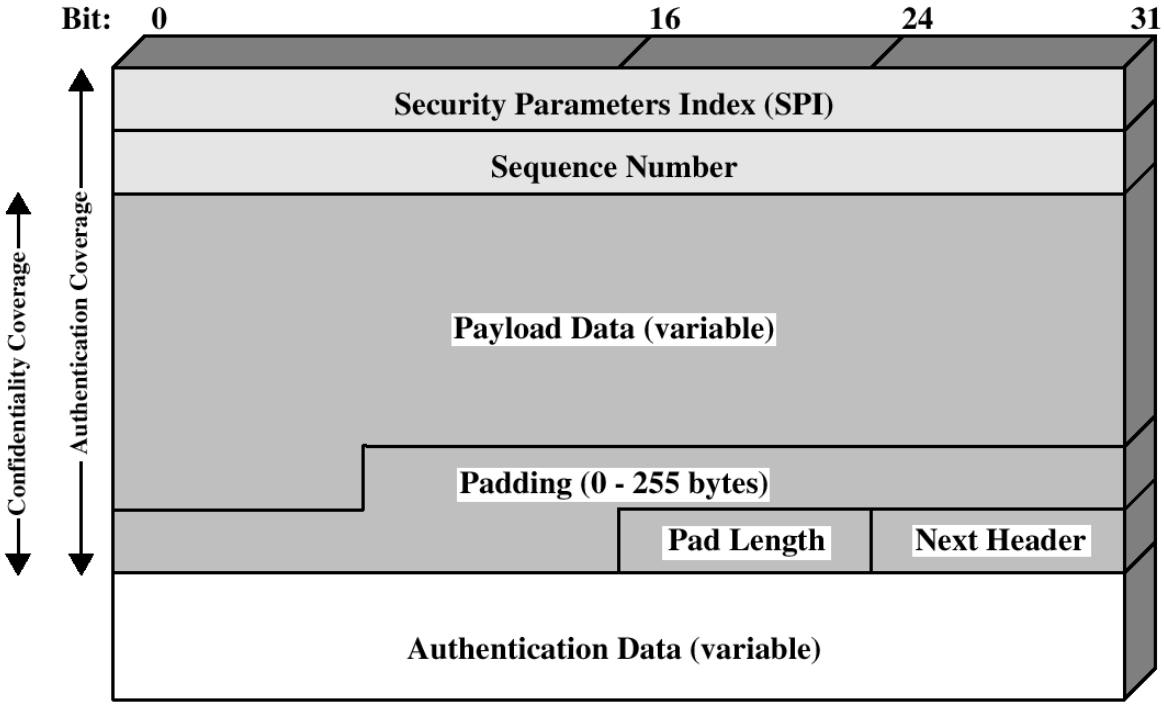


ESP - Encapsulating Security Payload

Tunnel mode

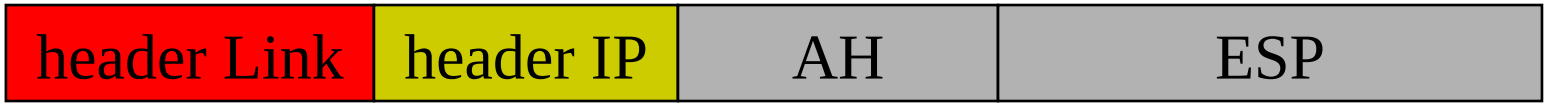


ESP - Encapsulating Security Payload

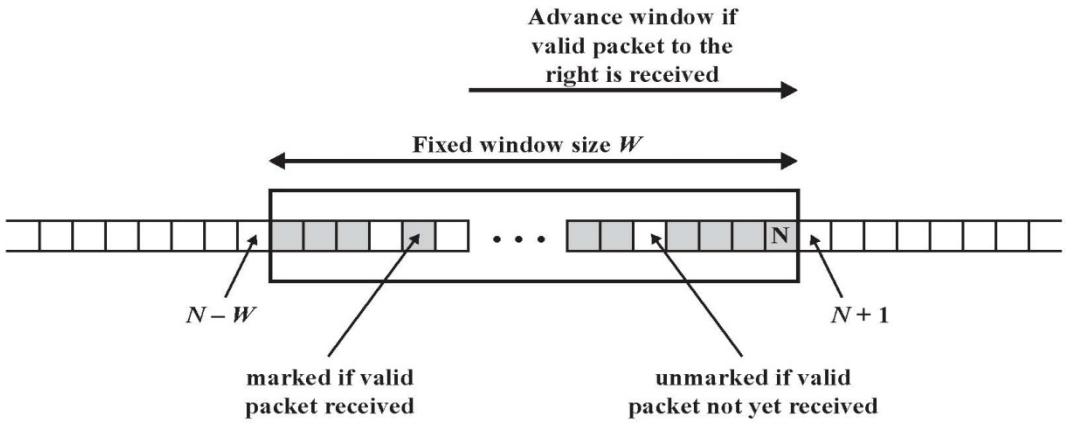


AH + ESP

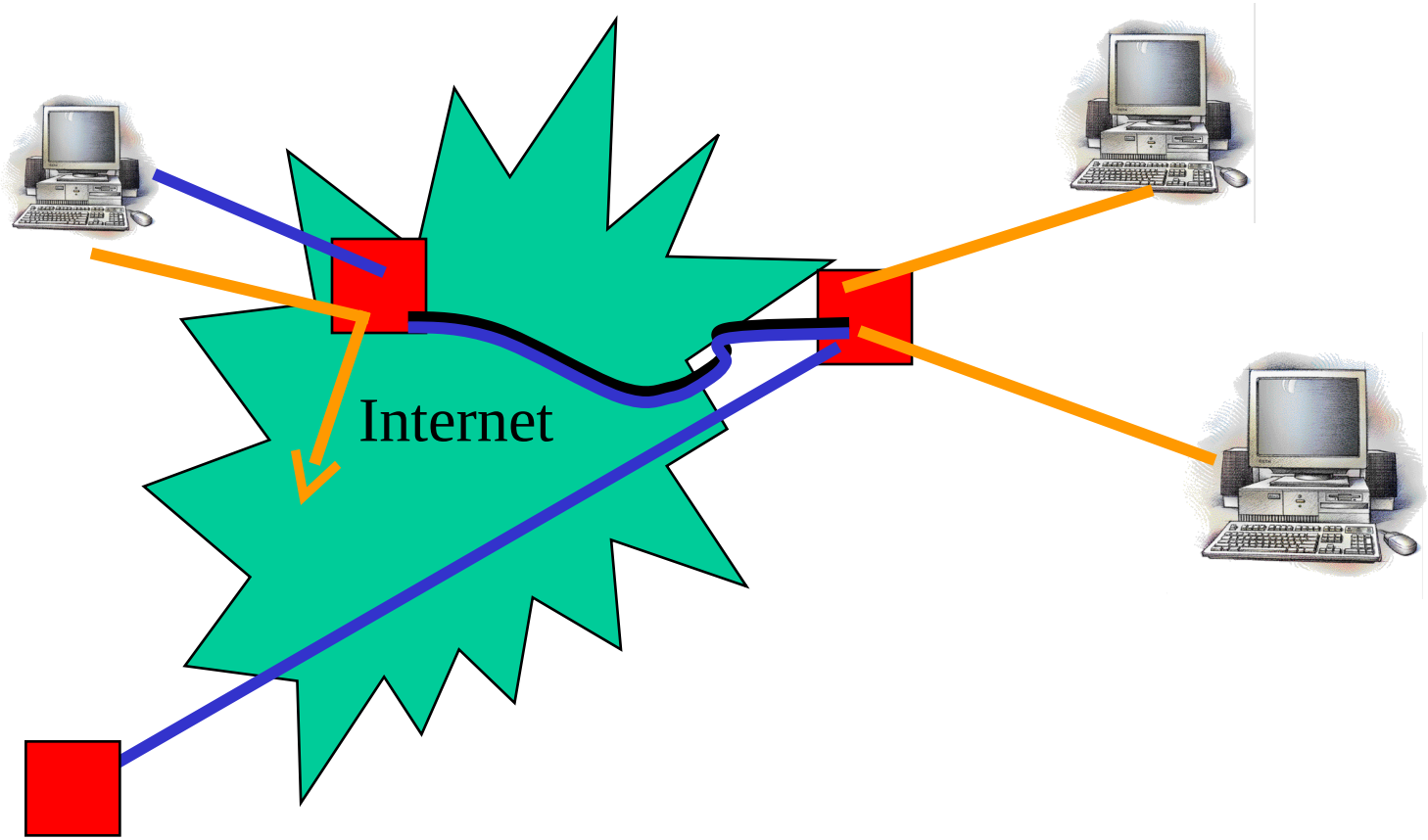
E’ possibile cifrare e autenticare



IPsec anti-replay



IPsec “annidate”



IPsec

Domanda: Come si determinano chiavi e algoritmo crittografico?

Risposta: Usando le SPI, l'indirizzo IP mittente e destinatario, e una tabella di associazione presente sulle macchine di mittente e ricevente

IPsec

Domanda: Come si installa la tabella di associazione e come si inizializzano le chiavi?

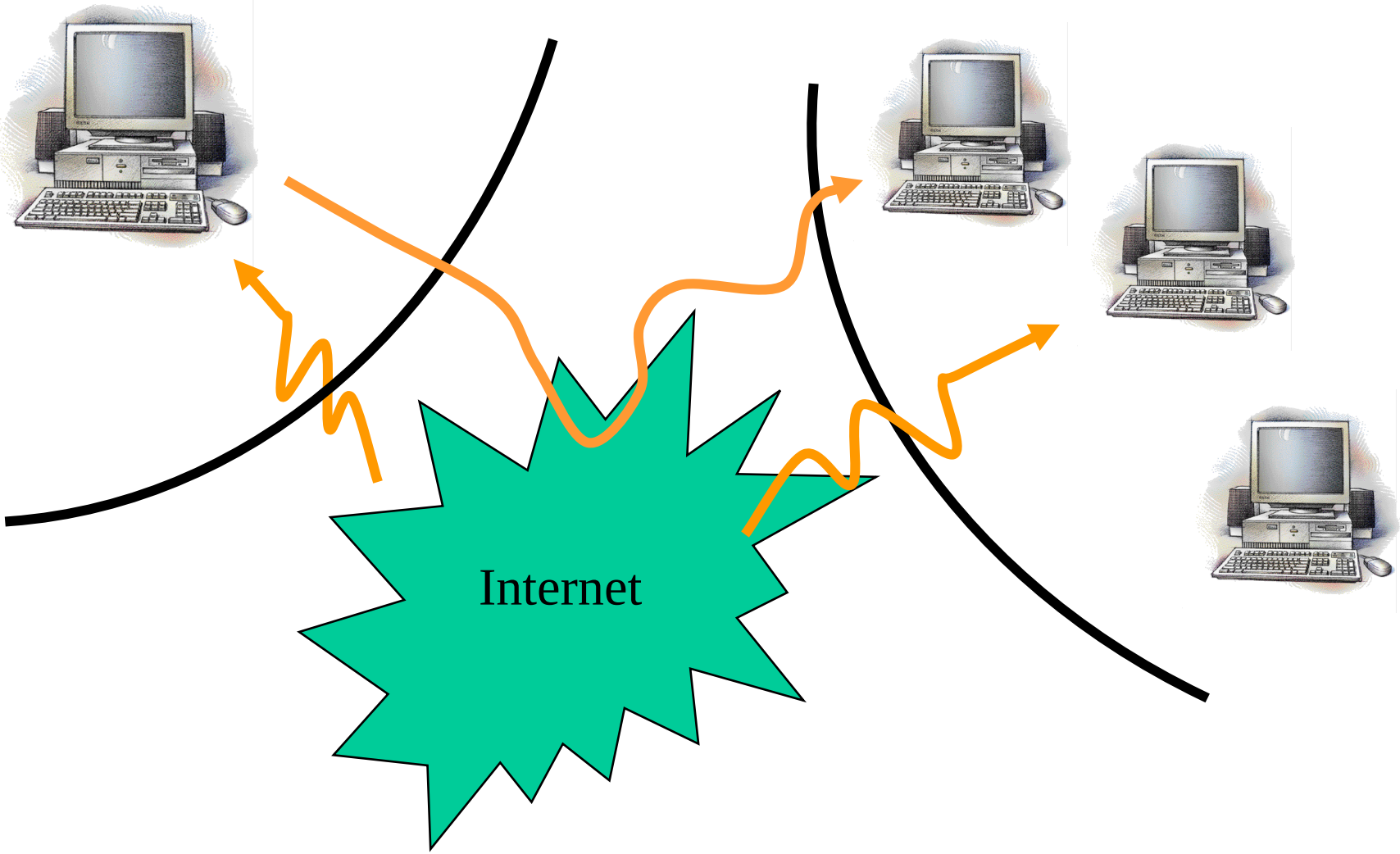
Risposta: A mano, durante l'installazione del prodotto Ipsec selezionato. Alcuni prodotti prevedono scambio di chiavi con tecniche asimmetriche, raramente usato.

IPsec

Domanda: Che algoritmi di cifratura e autenticazione vengono usati?

Risposta: Algoritmi convenzionali (simmetrici) perché il procedimento deve essere efficiente

IPsec: una buona soluzione



Conclusione - IPsec permette di:

- Avere la stessa sicurezza che avremmo con un un'unica rete locale
- Permettere anche traffico da e verso reti esterne, se necessario attraverso un Firewall
- Non introdurre ritardi significativi
- Non richiedere operazioni di riconfigurazione agli utenti (trasparenza) se intallato in tunnel mode