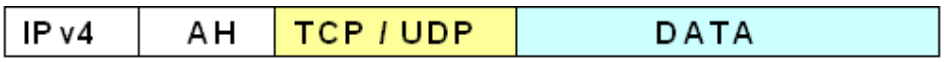
IPSEC

I servizi offerti da IPSEC sono disponibili alle entità IP con una modifica dei datagrammi IP.

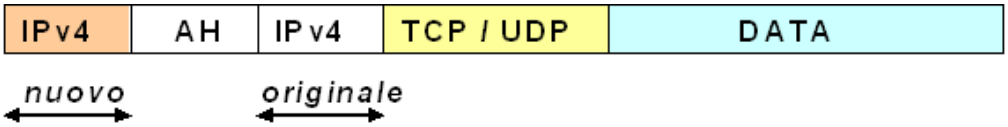
Per usufruire del servizio di autenticazione occorre inserire all'interno del datagramma IP l'intestazione **AH (valore campo protocol = 51).**

Le modalità di funzionamento possono essere:

- **modalità trasporto:**



- **modalità tunnel:**

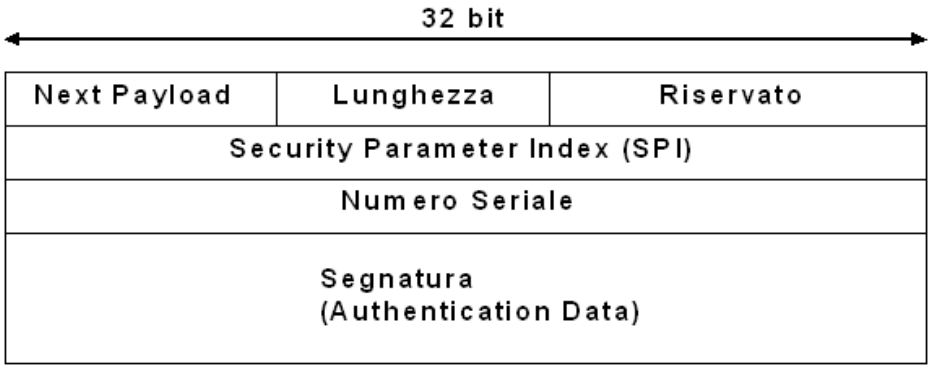


La modalità **trasporto** fornisce protezione per i protocolli di livello superiore rispetto ad IP; tale modalità viene utilizzata per implementare funzioni crittografiche fruibili direttamente dalle stazioni finali (end to end).

La modalità **tunnel** fornisce protezione all'intero datagramma IP; anche se questa modalità ha scopi end to end, viene usata molto anche per implementare funzioni crittografiche presso gli apparati di frontiera di una rete locale (router e firewall); la modalità tunnel è estremamente interessante per le realizzazioni VPN (Virtual Private Network)

Vantaggi di IPSEC:

- inibisce ogni forma di *address spoofing*, consentendo di autenticare la sorgente del datagramma IP
- elimina la possibilità di alterare i dati in transito su Internet, sostituendo il concetto di *checksum* del messaggio con un più complesso meccanismo di calcolo di un MAC permettendo di verificare l'integrità del messaggio trasmesso
- non permette ogni forma di *replay attack,* inserendo all'interno del datagramma dei numeri seriali che non si ripetono mai, prima di calcolare la segnatura
- perché il protocollo di autenticazione possa svolgere il proprio compito, ossia calcolare e verificare la segnatura del messaggio, è necessario che le stazioni coinvolte posseggano un segreto comune *(chiave segreta)* ed un sistema crittografico comune.



- **Next Payload (8 bit):** indica la natura dei dati incapsulati nel datagramma IP
- **Lunghezza (8bit):** indica la lunghezza del campo dati
- **Riservato:** utilizzato per scopi futuri
- **SPI:** indica a quale SA (associazione) appartiene il datagramma IP
- **Numero Seriale:** indica la posizione del datagramma all'interno del flusso di messaggi scambiati entro una data associazione (2^{32} – 1 datagrammi IP validi)
- **algoritmi digest:** MD5, SHA-1
- **Segnatura:** il protocollo di autenticazione per produrre la segnatura utilizza lo schema noto come HMAC (**Hash** Message Authentication Code). La segnatura viene calcolata sul risultato della concatenazione delle seguenti componenti:
    - intestazione IP standard (relativa ai campi che non subiscono alterazioni durante la trasmissione attraverso Internet)
    - intestazione di tipo AH (con il campo segnatura messo a zero)
    - campo dati contenuto nel datagramma IP