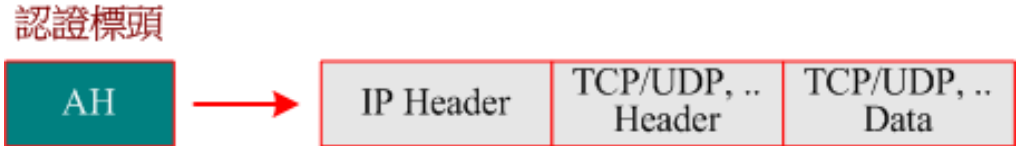
IPSec AH 協定

- **IPSec AH 協定 (Authentication Header, AH)**
  - **訊息確認碼 (Message Authentication Code, MAC)**
    - 偵測訊息傳遞當中，是否被竄改或偽造
    - 訊息摘要 (Message Digest, MD)
    - HMAC (Hash message Authentication Code)



AH 標頭格式

AH 標頭格式

- 下一個標頭 (Next Header, NH) ：TCP/UDP/ICMP/IP
- 承載長度 (Payload Length)
- 安全參數索引 (Security Parameter Index, SPI) ：安全關聯
- 序號 (Sequence Number) ：防止被重複攻擊
- 認證資料 (Authentication Data)：確認封包是否被竄改