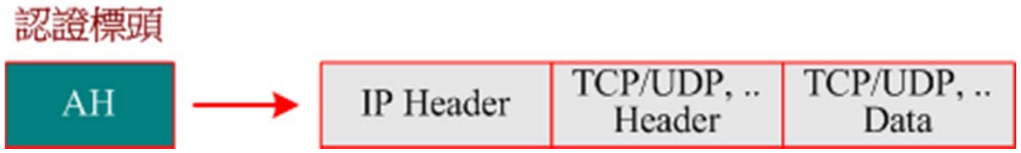
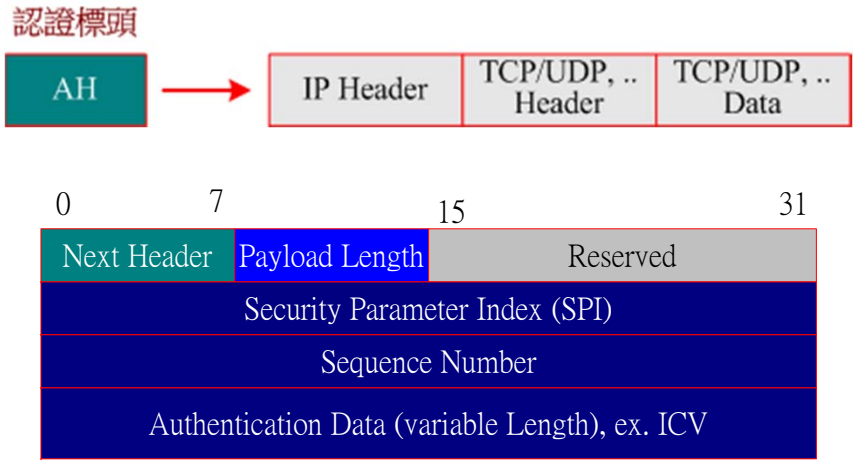
10-3-1 IPSec AH 協定簡介 (一)

- 『認證標頭』（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)



10-3-1 IPSec AH 協定簡介 (二)

- 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



10-3-1 IPSec AH 協定 (三)

IPsec AH 認證欄位 -認證欄位考慮因素

- 計算 MAC 值：
  - 產生『完整性檢查值』(Integrity Check Value, ICV)
  - 利用鑰匙加密
- 雙方必須協調：
  - ICV 加密的秘密鑰匙
  - 採用何種 MAC 演算法 (如 HMAC-SHA-1)
  - 選擇哪些欄位來計算 ICV 值