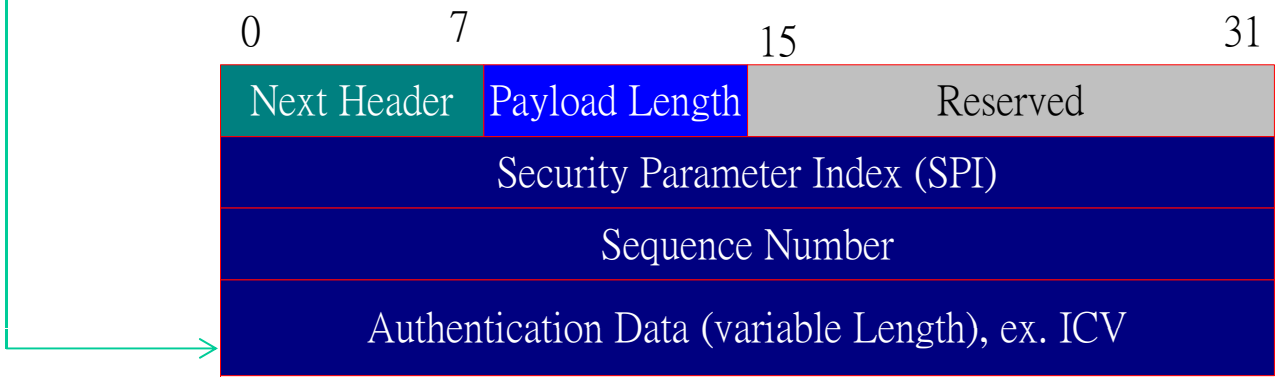
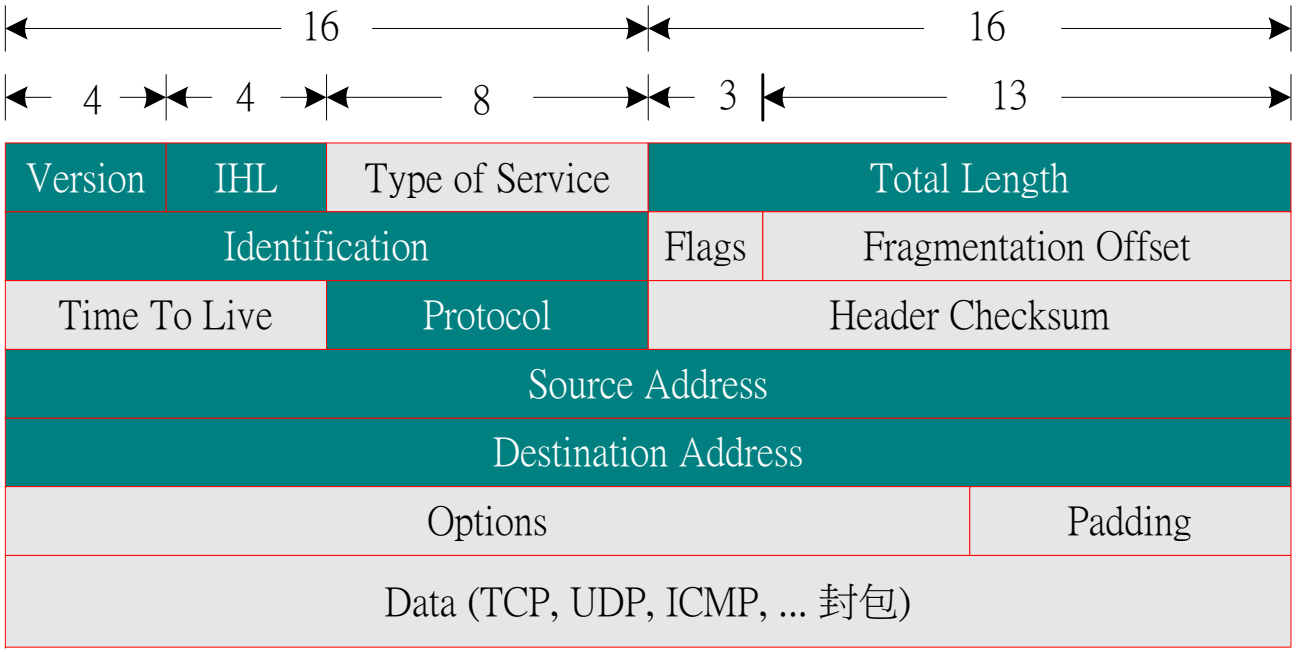
IPsec AH 認證欄位

- 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



IPsec AH 認證欄位

- IPv4 標頭可能參予計算 ICV 的欄位



IPsec AH 認證欄位

- IPv6 標頭可能參予計算 ICV 的欄位