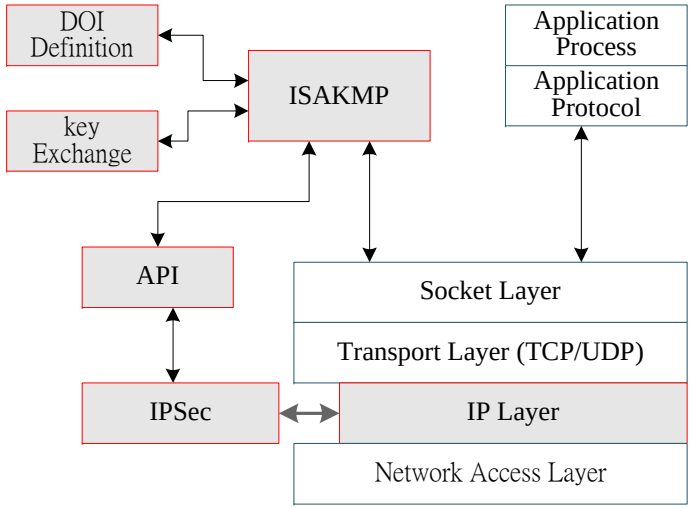
10-5-2 ISAKMP 協定功能

- **ISAKMP 協定特性**
  - **協議事項**
    - 安全協定（AH 或 ESP）、操作模式（傳輸或通道）、SA 壽命、認證金鑰、加密金鑰、以及各種編碼演算法
  - **建立與管理 SA**
    - SA Database
    - 『安全參數索引』（Security Parameter Index, SPI）
  - **認證機制**
    - 憑證授權（Certificate Authorities, CA）
    - 金鑰分配中心（Key Distribution Center, KDC）
  - **隱密性機制**
    - 利用公鑰系統來交換鑰匙材料，並建立通訊所需的會議金鑰（Session Key）

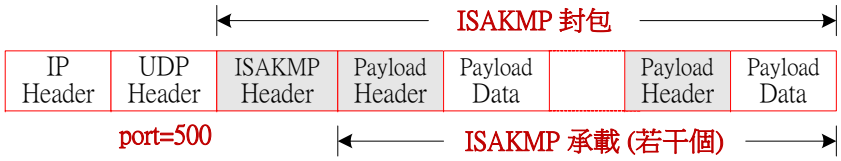
10-5-3 ISAKMP 協定堆疊(一)

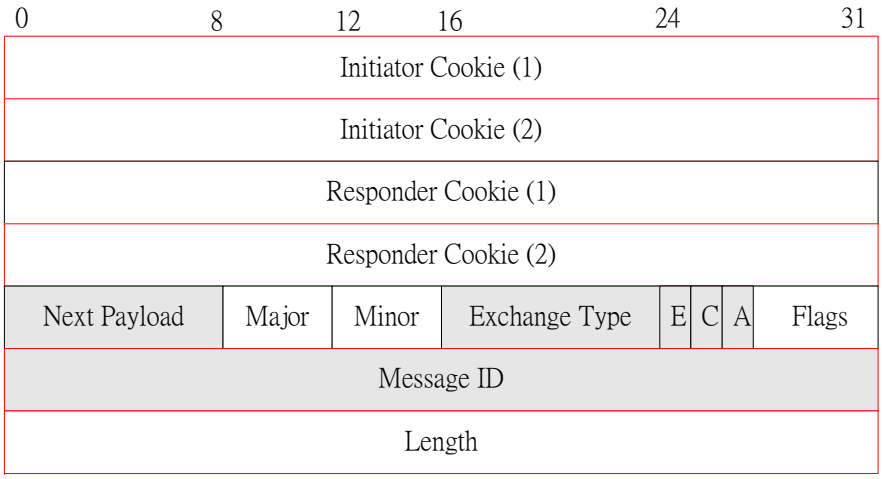
ISAKMP 協定堆疊

- 500 /udp



ISAKMP 包裝與標頭





10-5-3 ISAKMP 協定堆疊(二)

交換種類（Exchange Type）

交換型態	表示值
未使用（None）	0
基本交換（Base Exchange）	1
身份保護交換（Identity Protection Exchange）	2
僅認證交換（Authentication Only Exchange）	3
積極交換（Aggressive Exchange）	4
訊息交換（Information Exchange）	5
ISAKMP 未來使用	6-31
DOI 描述使用	32-239
私人使用	240-255