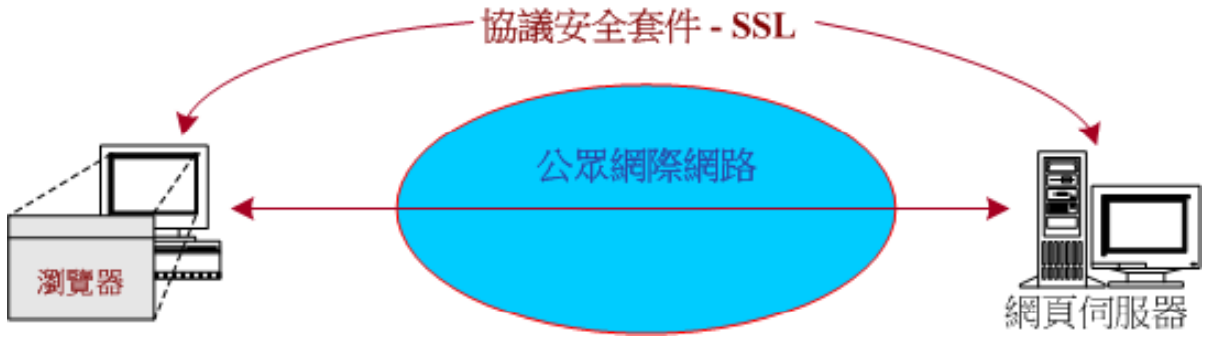
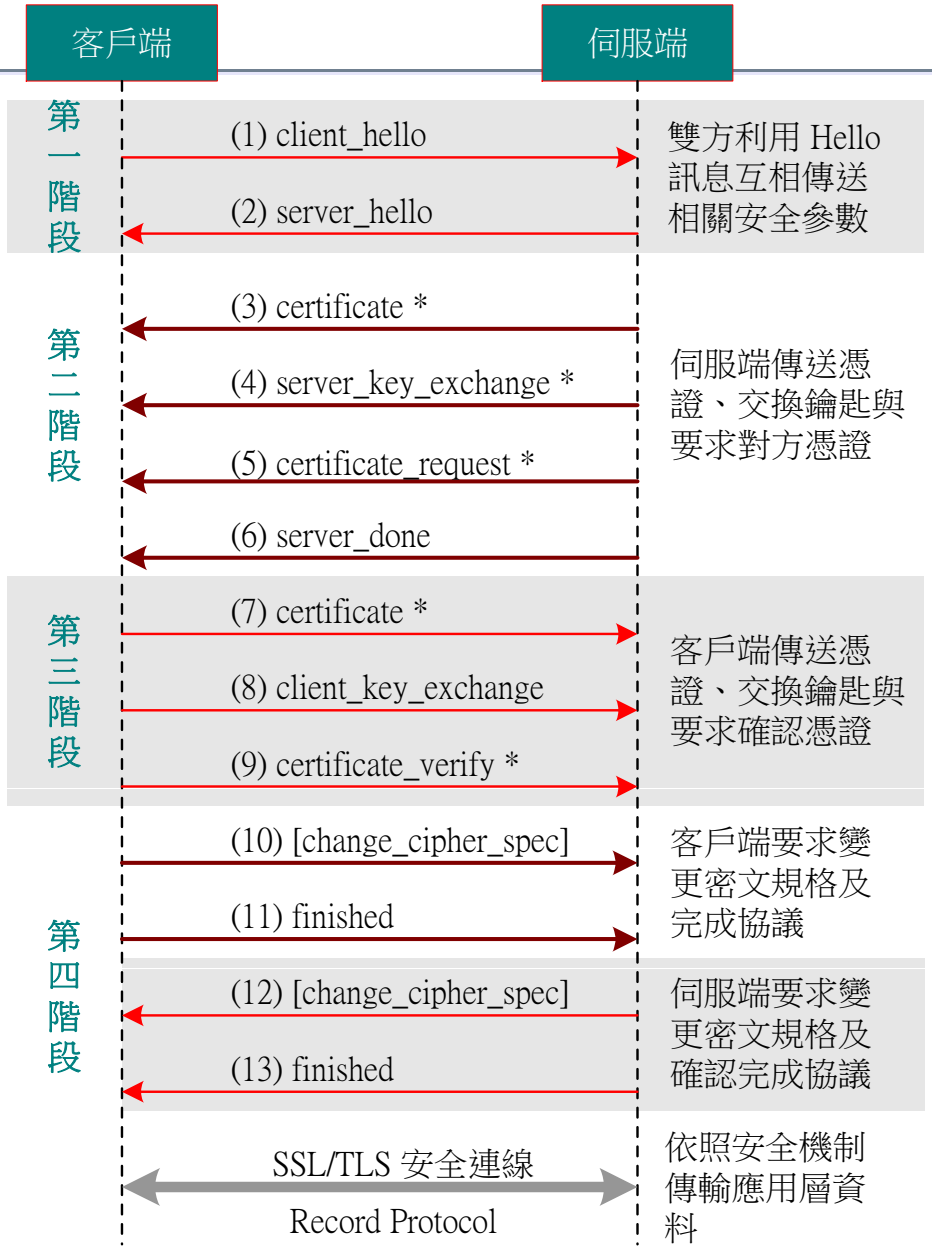
SSL 握手協定的運作

- 協商步驟

1. 交換 Hello 訊息，協議演算法，並檢視是否有 Session ID 可重複使用。
2. 交換鑰匙材料，及製作『前置主秘鑰』(Pre-master Secret)
3. 交換『身份憑證』。
4. 利用 Pre-master Secret 製作 Master Secret。
5. 將安全參數登錄於 Session Connection。
6. 保證協議當中未受到駭客攻擊。



SSL 握手協定運作



備註：有星號 (*) 表示選項訊息