

考試別：司法人員
等 別：三等考試
類科組：檢察事務官電子資訊組
科 目：計算機網路
考試時間：2小時

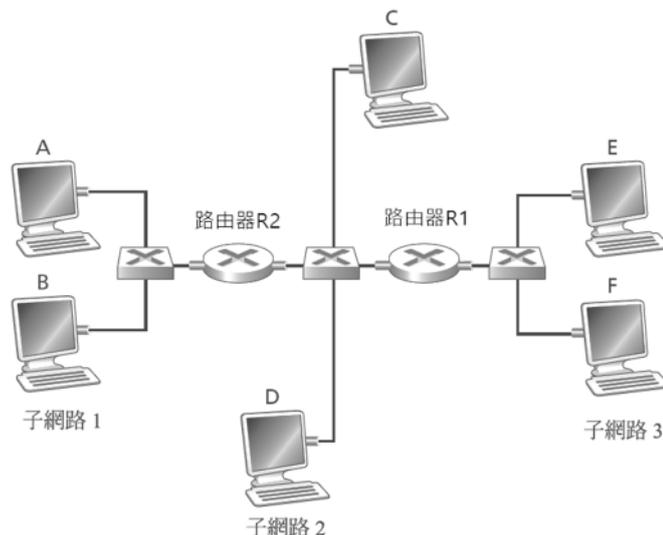
座號：_____

※注意：(一)禁止使用電子計算器。

(二)不必抄題，作答時請將試題題號及答案依照順序寫在試卷上，於本試題上作答者，不予計分。

(三)本科目除專門名詞或數理公式外，應使用本國文字作答。

- 一、在網路資料傳輸中，TLS（安全的 TCP 連線，Transport Layer Security）為補強 TCP 以納入安全性服務（如機密性、完整性等）的常用協定，試說明 TLS 的各階段（如連線握手、產生金鑰、資料傳輸等階段）運作過程。（25 分）
- 二、TCP 為網路傳輸層中相當重要的客戶端與伺服器之間的連線協定。在 TCP 連線的過程中，客戶端與伺服器會分別處於相互搭配的一連串不同狀態，以順利完成由連線建立至連線結束的生命週期。請說明 TCP 連線生命週期中，客戶端與伺服器經歷的一連串相互搭配狀態序列。（25 分）
- 三、考量以下網路架構，並假設子網路之間使用的是可提供實體至網路層服務的路由器 R1 與 R2 進行資料交換。
 - (一)若從主機 E 傳送 IP 封包給主機 F，主機 E 是否會要求路由器 R1 協助轉送該封包，請說明其原因。（10 分）
 - (二)假設主機 E 想要傳送 IP 封包給主機 B，若 E 的 ARP 表格中沒有 B 的 MAC 位址，則 E 是否執行 ARP 查詢以尋找 B 的 MAC 位址，請說明其原因。（15 分）



四、在計算機網路中，錯誤偵測技術一般運用循環冗餘檢查（cyclic redundancy check, CRC）編碼技術。

(一) 假設有待傳送資料 $D: 101110$ 、位元產生器 $G: 1001$ 以及位元數 $r: 3$ ，請說明 CRC 編碼的計算過程，並計算此待傳送資料 D 的 CRC 編碼。
(15 分)

(二) 請說明 CRC 編碼可以檢測出那些資料錯誤。(10 分)