

《計算機網路》

試題評析	<p>今年司法人員檢察事務官的計算機網路試題十分平易，以較一般性的問題為主。第一題為基本網路架構問題，取分不難。第二題是資料連結層位元填塞法，為常考的問題。第三題是 Web server 特性的考題，若有一些實際經驗，應可以取分。第四題為網路安全上的特點。第五題是 NAT，也是基本的問題。第六題是無線通訊的問題與解決，屬於 WLAN 部份的考題。第七題則是 Link-State 路由方法的說明。</p> <p>大體而言，今年考題對應考人員並不會造成太多的困擾，命題廣泛但簡單，大致上分數應該都會不錯，預估要拿到七十分以上，甚至八、九十分以上，都不是難事。</p>
------	---

一、請列出使用 TCP/IP 通訊協定的網際網路，在層次架構上對應於國際標準組織（ISO）提議的 OSI（Open System Interconnection）架構可分為那幾層？並請簡述各層之主要功能。（15 分）

【擬答】

TCP/IP Reference Model	OSI Reference Model
Application Layer	Application Layer
	Presentation Layer
	Session Layer
Transport Layer	Transport Layer
Internet Layer	Network Layer
Host-to-Network	
Lan,Wan,...	Data Link Layer
	Physical Layer

- 一、Application：對應 OSI 的 layer 5,6,7，為各種應用所使用的協定，可以使用標準的協定，也可以由應用軟體設計者自行定義。應用層的協定如：FTP、Telnet、SMTP、HTTP、POP、DNS、SNMP等。
- 二、Transport Layer：對應 OSI 的 layer 4，負責將資料割成資料片段(segments)，將資料片段傳送到目的地，並可以保證資料的可靠性與順序的正確性。傳輸層的協定主要有 TCP(Transmission Control Protocol)與 UDP(User Datagram Protocol)，前者為 connection-oriented；後者為 connectionless 的協定。
- 三、Internet Layer：對應 OSI 的 layer 3，將資料片段包裝成封包，負責路徑的選擇，以轉送封包。主要為 IP(Internet Protocol)。
- 四、Host-to-Network：為資料鏈結及實體網路的訊框傳送。

二、位元為主的通訊協定（Bit Oriented Protocol）使用 01111110 訊息框（Frame）開始與結束的特定符號（Pattern），假設要傳送的資料內容如下：

0000 1111 1101 1111 0111 1111 1010 1001

為了避免與開始或結束符號混淆，請說明收送雙方處理的方法並列出傳送的資料說明之。（15 分）



【擬答】

使用開始旗標(Starting flag)與結尾旗標(ending flag)：來區別任意長度的位元序列，以使訊框中可以有任意長度個位元。起始與結尾旗標位元組為 01111110，而資料中若有連續五個 1 時，必須在其後加上一個 0，以免被接收端誤認為旗標位元組，此法即位元填塞(bit stuffing)。本題傳送的資料如下，有底線的是填塞位元：

01111110 0000 1111 10101 11110 0111 11011 1010 1001 01111110

三、使用 HTTP 通訊協定的瀏覽器 (Browser) 通常需要從 Web 伺服器網路請求下載文件或檔案後才再進一步處理顯示，不留狀態的伺服器 (Stateless Server) 具有那些特性？雙方需使用那種方法才能追蹤使用者以前的狀態？(15 分)

【擬答】

- 一、Stateless server 的特性是不記錄 client 先前所進行的工作，client 每一個要求，server 只會針對此一要求進行處理並回應，每個要求都是獨立的。此種方式的優點是：減少 server 與 client 所需記錄的時間與空間，但無法使具有關聯性的運作以方便的方式來進行。
- 二、若要追以前的狀態，可以在 server 與 client 上記錄 session information，例如：client login 後，便可以記錄下 user 的身份，以便進行權限的檢查。

四、請說明封包監測 (Packet Sniffing) 利用以太網路卡的那種方式運作，在網路安全上會有那些影響？(15 分)

【擬答】

- 一、packet sniffing 是利用 promiscuous mode，可以收取所有在網路上的訊框，而不是只接收目的 MAC 位址與自己相同的訊框。
- 二、可以竊聽並記錄網路上的封包，若正好有機密資料在傳送，私密性將會被破壞，因此在這種情形之下，加密技術變得很重要。

五、請舉例簡述 NAT (Network Address Translation) 的運作方式與功能。(15 分)

【擬答】

當企業所配置得到的 IP 位址不敷使用時，可以使用 private address space，但對外通訊時，必須使用所配發的 IP 位址，故必須將 private address space 轉換成對外的一組 IP 位址，封包才能與外界進行通訊，此種轉換即為 NAT。

六、請說明無線區域網路的終端機隱匿問題 (Hidden Terminal Problem)，可使用那種方法加以克服？(15 分)

【擬答】

隱藏節點問題(hidden station problem)：同時要發送的兩個互相競爭對手，因為互相的距離太遠，而無法互相偵測到對方，而同時發送以致碰撞發生而無法查覺。

採用 MACA(Multiple Access and Collision Avoidance)的做法，即資料傳送之前，傳送端與接收端先互相交換控制訊框，傳送端會送一個要求傳送的控制框(RTS, request to send)，說明傳送的資料框長度，接收端回應(CTS, clear to send)後才開始傳送。

七、簡述連線狀態繞徑法 (Link-State Routing) 的概略進行步驟，並說明其優缺點。(10 分)

【擬答】

- 一、找出相鄰的路由器(Learn about then Neighbors)：當一個 router 啟動之後，會送出一個 HELLO packet 到每條線上，而相鄰的 router 會將 name 回應回來，於是便可以知道有那些相鄰的 routers。
- 二、測量線路的成本(Measuring Line Cost)：每個 router 必須知道其與各相鄰 router 之間線路的 delay time(或合理的 delay time 的預測)。這個時間也可以用 ECHO packet 測量出來。
- 三、建立連結狀態封包(Building Link State Packets)：每個 router 蒐集到與其相鄰 routers 之間的路徑長度之後，必須建立一個 Link State Packet，以便能將路徑資訊告訴 AS 中其他的 routers。
- 四、發送與接收連結狀態封包(Distributing the Link State Packets)。
- 五、計算新的路徑(Computing the new routes)：當所需的資料蒐集完成，router 便在自行建立 subnet graph(每一條線路皆有雙向的兩個 arcs)。使用 Dijkstra's algorithm 來計算所有可能的目的地的最短路徑，並記錄到其 routing table 中。
- 六、有封包進入 router 時，便查詢 routing table，以選擇傳送的路徑。

