# 《資通網路》

| | |
|---|---|
| **試題評析** | 本份試題第五題屬資訊安全範疇，命題主要集中於講義前5章，試題整體而言中規中矩，學員如能熟讀講義內容，應可獲得不錯的成績。 |
| **考點命中** | 第一題：《高點・高上資通網路講義》第3章，張又中編撰，頁3-23~25。<br>第二題：《高點・高上資通網路講義》第4章，張又中編撰，頁4-36~37。<br>第三題：《高點・高上資通網路講義》第2章，張又中編撰，頁2-11~13；<br>《高點・高上資通網路講義》第5章，張又中編撰，頁5-29。<br>第四題：《高點・高上資通網路講義》第3章及上課補充，張又中編撰，頁3-10、3-37。<br>第五題：《高點・高上資訊安全實務講義》第3章，張又中編撰，頁3-13。 |

一、TCP 提供連接導向服務，請以主從架構模式說明 TCP 連線建立過程與 TCP Header 中的那些欄位用於 TCP 連線建立過程。（20分）

**答**：

TCP使用三方交握法(Three-way Handshaking)建立連線，步驟如下：

1.傳送端送出SYN

2.接收端收到後回傳SYN+ACK

3.傳送端收到後再傳送ACK，建立雙方傳輸連結

TCP連線建立過程會使用到的TCP Header欄位有序號(Sequence Number)、回應編號(Acknowledgement Number)，以及旗標(Flag)。

二、目前網路大多以 HTTP Streaming 傳輸影音串流，DASH 為 HTTP Streaming 之一。請說明 DASH 影音串流傳輸運作方式。（20分）

**答**：

為基於HTTP的動態適應串流(Dynamic Adaptive Streaming over HTTP)，使高品質串流媒體可以透過傳統的HTTP網路伺服器以Internet傳遞。類似Apple的HTTP Live Streaming(HLS)

DASH伺服器將影片內容分解成一系列基於HTTP的小型檔案片段，每個片段包含短長度的可播放內容，而總內容長度可能長達數小時(如電影或體育賽事直播)。內容將被製成多種資料速率的備選片段，以供不同資料速率的客戶端選擇使用。

三、無線網路傳輸不同於有線網路傳輸，請說明使用無線傳輸時，何種問題會造成無線傳輸通道損傷？（20分）

**答**：

以多重路徑衰減(Multipath Fading)為例，當傳送端發送訊號後，訊號在空中以發散的方式傳播，各發散電波經由折射、散射或延遲等不同路徑到達接收端，其訊號強度、相位及抵達時間也不盡相同，因此接收端收到的多筆訊號可能都為同一訊號所產生，因而發生干擾現象。

以藍牙(Bluetooth)為例，其1.2版定義一自適應跳頻(Adaptive Frequency Hopping, AFH)演算法，允許藍牙設備將頻道標記為好、壞及未知，再透過查找表使用好頻道、替換壞頻道。主設備可透過定期偵聽壞頻道來確定干擾是否消失，從設備亦可向主設備發送其對頻道品質的評價報告。美國聯邦通訊委員會(Federal Communication Committee, FCC)要求至少使用15個不同的頻道。



四、請說明whois 協定用途與可查詢那些資訊。（20 分）

**答**：

用來查詢Internet中網域IP及其所有者等資訊的傳輸協定，其使用TCP Port 43。每個網域、IP的資訊由對應的管理機構儲存，公眾可自由查詢而得。例如，於TWNIC查詢www.ntu.edu.tw可獲得下列資訊：

```
Ministry of Education Computer Center
   12th Fl, 106, Hoping E. Road, Sec 2.
   Taiwan Republic of China, R.O.C
   TW

   Domain Name: edu.tw

   Contact:
      TANet, Administrator  tanetadm@moe.edu.tw
      886-2-77129008
```

五、請說明 Zero-Day Attack 發生時機，會帶來何種資安危機與該如何因應。（20分）

**答**：

攻擊者利用尚未被公開、修補的弱點來攻擊被害者，弱點標的可能是各類型的作業系統、應用程式、信件軟體與網頁瀏覽器等。

因應零時差的攻擊的方法有：

1.建立防止零時差漏洞的安全過濾器。

2.定期接收新漏洞的更新規則並自動部署。

3.自動檢測是否有黑名單(Black List)之通訊。

4.支援通訊加密檢查，減少加密流量所帶來的資安盲點。

5.結合各類型的檢查技術，如深度封包檢查、進階惡意程式分析、威脅情資及網址信譽評等。