《電腦網路》

一、如果訊框（frame）的大小為 8000 bits，而且傳送端與接收端之距離為 40 公里（km），假設訊號的傳遞速度為光速的 2/3（即為 200,000 km/sec），那滿足下列兩種協定之最小網路連線速度為多少 Mbps？其中 channel utilization(ρ)的定義為 $\rho = {T_t}/{(T_p + T_t)}$，其中 T_t 為 transmission time，亦即傳送 8000 bits 的 frame 所需的時間，而 T_p 為訊號的傳遞時間（propagation time）。（每小題 13 分，共 26 分）

(一)Stop-and-wait 協定，80% channel utilization。

(一)1 bit sliding window 協定，80% channel utilization。

試題評析	本題重點在於通道使用率計算，分成 stop-and-wait 與 sliding windows 兩個小題，必須了解傳輸特性上的差異，寫出正確算式才能解題。
考點命中	1.《高點資通網路講義》第二回，王致強編撰，頁 28～30。 2.《高點資通網路講義》第二回，王致強編撰，頁 36，範例 62。

【擬答】

先計算 $T_p = \dfrac{40km}{\dfrac{200{,}000km}{\sec}} = 0.2ms$

(一)stop-and-wait 的通道利用率 $\rho = \dfrac{T_t}{2T_p + T_t} = 80\%$，故 $T_t = 8T_p = 1.6ms$，

因此，連線速度 $= \dfrac{8000bits}{1.6ms} = 5Mbps$。

(二)1 bit sliding window 協定就代表 window size=2(sequence number=0 and 1)，

因此通道利用率 $\rho = \dfrac{2 \times T_t}{2T_p + T_t} = 80\%$，故 $T_t = \dfrac{4}{3}T_p = \dfrac{8}{30}ms$，

因此，連線速度 $= \dfrac{8000bits}{\dfrac{8}{30}ms} = 30Mbps$。

二、如果您是公司內部的網管人員，遇到公司內部使用者沒有辦法透過有線網路連線到 Internet/Intranet，您請使用者第一步先確認網路線有接上，但仍無法連線，請問可能的原因為何？（請試寫出五項）（25 分）

試題評析	本題為基本觀念實務題。

【擬答】

(一)實體線路故障，訊號無法傳遞。

(二)網卡的驅動程式未正確安裝，造成系統無法與網路正常連接。

(三)網卡通訊協定，網路位址，子網路遮罩，閘道器，或名稱伺服器未正確設定，造成訊息發送錯誤。

(四)名稱伺服器故障，無法查詢網址。

(五)網路連接設備故障或有設定上的問題。

三、試說明採購網路設備（如網路交換器）時，需考量那些因素。(請試寫出四項)(22 分)

試題評析	本題為基本觀念實務題。

【擬答】

採購網路設備時，需考慮的因素如下：

(一)網路使用的通訊協定種類，例如：乙太網路使用乙太交換器，ATM 網路使用 ATM 換器。

(二)port 數量是否足夠以連接所有主機，主機的數量與網路規模。

(三)是否具有安全機制，可以防範網路攻擊。

(四)設備的頻寬是否足夠應付傳輸的需求。

(五)擴增性(Scalability)：設備能否具有彈性，以應付未來主機數量的增減絀動。

(六)價格考量，經費預算是否足夠承擔網路設備與建置費用。

四、無線網路的認證方式有那些類型？請舉三種說明之。(12 分) 並請說明 802.11i 在使用者驗證、資料加密與資料完整性部分，各使用什麼機制。(15 分)

試題評析	本題重點在於無線網路相關安全協定，包括 802.11i 相關措施。
考點命中	《高點資通網路講義》第五回，王致強編撰，頁 7 以下。

【擬答】

(一)無線網路身份認證類型如下：

1.WEP(Wired Equivalent Privacy)：AP 設定有 WEP key，行動主機也必須設定相同的 key，兩者相同才能夠連線。由於 WEP 使用 RC4 加密法，由 26 個 16 進位數字構成，相當 26*4=104bits，再串接 24bits 的 IV(Initialization Vector)構成 128bits 的 WEP key，每一組 key 基本上只使用一次就立即更換 IV，以避免重覆，但 24bits 的 IV 只有 24bits，防護能力不夠。

2.WPA－PSK(Wi-Fi Protected Access－Pre－Shared Key)：WPA－PSK 做法與 WEP 相似，AP 與行動主機必須有相同的 Key 才能連接，不過使用了 TKIP(Temporal Key Integrity Protocol)，比較安全。

3.IEEE 802.1x 的 Port－Based Network Access Control，需架設 RADIUS 伺服器以存放使用者身份資料，當行動主機連線時輸入帳號密碼，必須向 RADIUS 伺服器進行驗證。

4.MAC ACL(Access Contorl List)：AP 上須建立允許連入的新機名單，只有 MAC 位址符合者可以連線。

(二)802.11i 的相關機制：

1.身份認證：802.11i 協議使用了 EAP(Extensible Authentication 通信協議)以及 802.1x，強迫使用者必須進行驗證以及交互驗證。主要包括三點：

(1)雙向認證機制，可有效地消除了中間人攻擊，防止像是假冒 AP 或遠端認證服務器。

(2)集中化認證管理和動態分配加密密鑰的機制，以解決管理上的困難。

(3)集中策略控制，當會話超時時，會觸發重新認證和生成新的密鑰。

2.資料完整性：使用了 MIC(Message Integrit Code)信息完整性編碼來檢測傳送的字節是否有被修改的情況。其基本做法是在送端在送出封包前，把明文的資料內容透過 Michael 演算法，計算出一個 64bits 的 MIC 值；而收端來說收到封包解密出明文後，也是透過 Michael 演算法計算 MIC 值，如果兩個值一致，就表示封包正確無誤；不一致，就表示封包在傳輸過程中發生錯誤。

3.資料加密：為了能提供更高級別的加密保護，使用 TKIP(Temporal Key Integrity Protocol)，將加密過程由靜態改成動態，讓攻擊者更難以破解。爲了能提供更高級別的加密保護，802.11i 採用新的 AES(Advanced Encryption Standard)標準。