《電腦網路》

試題評析	本份試題命題集中於前三章(63分)，另22分為無線網路，15分則屬資訊安全範疇。主要為觀念之解析，例如：各種CSMA機制的差異比較，故可以表格的方式來呈現作答。
考點命中	第一題：《高點・高上電腦網路講義》第一回，張又中編撰，頁1-15。 第二題：《高點・高上電腦網路講義》第一回，張又中編撰，頁1-10～11；第三回，頁3-13、15～16。 第三題：《高點・高上電腦網路講義》第二回，張又中編撰，頁2-43；第五回，頁5-24～27。 第四題：《高點・高上電腦網路講義》第二回，張又中編撰，頁2-44；第五回，頁5-17～19。

一、(一)一個QPSK（Quadrature Phase Shift Keying）的星座圖（signal constellation），四點的座標分別在(1,1),(1,-1),(-1,1)和(-1,-1)。請問如果依據這樣的參數設計，在一個鮑率（baud）為1200的通信系統，所得到的資料速率（data rate）是多少bps？並說明理由。（5分）

(二)一個全雙工QAM-64（Quadrature Amplitude Modulation）的數據機（modem）總共使用了多少個頻率？並說明理由。（5分）

(三)請針對下面幾個面向，比較線路交換（circuit-switched）網路以及封包交換（packet switched）網路之不同。（10分）

1. 需要呼叫建立（call setup）與否
2. 是否有專屬實體路徑（dedicated physical path）
3. 每個封包是否走相同的路徑
4. 封包是否依所傳送的順序到達
5. 可能遭遇壅塞的時間點

答：

(一)1200×log24=2400(bps)

(二)2 個，一個用於上傳，一個用於下載。

(三)

交換方式	線路交換	封包交換
需要呼叫建立	是	否
是否有專屬實體路徑	是	否
每個封包是否走相同的路徑	是	不一定
封包是否依所傳送的順序到達	是	不一定
可能遭遇壅塞的時間點	呼叫建立時	每個封包都有可能發生壅塞

二、(一)比較資料鏈結層（data link layer）與傳輸層（transport）的功能特性，各舉出兩個相同點，以及兩個不同點。（10分）

(二)為什麼路由（routing）的計算，是網路層（network layer）的工作，而不是在傳輸層或資料鏈結層？（10分）

答：

【版權所有，重製必究！】

(一)

OSI	資料鏈結層	傳輸層
相同點	皆有流量控制(Flow Control)與錯誤控制(Error Control)。	
相異點	負責區域網路的訊框轉送 以 MAC 位址識別裝置	負責端對端的連線 以埠號識別所提供的服務

(二)路由計算牽涉封包的 IP 位址與網路遮罩/子網路遮罩，故為網路層的工作。

三、(一)假設在一個slotted ALOHA網路裡，只有三個工作站A，B，C。而每個工作站在一個時槽（time slot）裡會傳送訊框（frame）的機率，分別是$P_A=0.2$，$P_B=0.3$，$P_C=0.4$。則工作站A的吞吐量（throughput）約是多少？整個系統的吞吐量又是多少？（10分）

(二)請比較WiFi及藍牙（Bluetooth）的媒介存取協定（medium access control protocol）主要的不同點？至少舉出兩點。（10分）

答：

(一)工作站 A 的吞吐量=0.2*0.7*0.6=0.084

整個系統的吞吐量=0.084+0.144+0.224=0.452

(二)WiFi 的媒介存取協定為載波感測多重存取/碰撞避免(Carrier Sense Multiple Access with Collision Avoidance, CSMA/CA)。藍牙則是將每個微網中的時槽定義為 625 μsec，支援雙向 PCM 的語音通訊。此外，藍牙也提供非同步無連結(Asynchronous Connection-Less, ACL)與同步連結導向(Synchronous Connection Oriented, SCO)兩種傳輸方式。

四、(一)比較pure ALOHA、non-persistent CSMA、1-persistent CSMA、p-persistent CSMA之間的不同。（13分）

(二)CSMA/CA的CA（Collision Avoidance）碰撞避免的策略為何？舉兩個策略並說明之。（12分）

答：

(一)

MAC Protocol	pure ALOHA	non-persistent CSMA	1-persistent CSMA	p-persistent CSMA
媒體閒置	立即傳送	立即傳送	立即傳送	機率p傳送
媒體忙碌		等待一隨機時間後再傾聽	傾聽到其閒置為止再傳送	傾聽到其閒置為止，重複此演算法

(二)採用實體頻道偵測與虛擬頻道偵測兩種策略。實體頻道偵測為當某站台要傳輸資料時需先偵測頻道；虛擬頻道偵測則是利用 RTS、CTS、NAV 的機制，來避免發生隱藏站台問題(Hidden Terminal Problem)或是暴露站台問題(Exposed Terminal Problem)。

五、(一)假設Bob要傳送一份機密的文件給100個人，使用的是非對稱金鑰（asymmetric-key）方式確保機密性（confidentiality），請問需要使用到幾把金鑰？請說明理由。（3分）

(二)數位簽章（digital signature）可否提供：（並請說明理由）（6分）

1. 訊息認證（message authentication）
2. 機密性（confidentiality）
3. 不可否認性（nonrepudiation）

(三)下列那一個（或那幾個）是一種機密性（confidentiality）的攻擊？（並請說明理由）（6分）

1. 窺探（snooping）
2. 偽裝（masquerading）
3. 否認（repudiation）

【版權所有，重製必究！】

答：

(一)2x100=200(把)

(二)數位簽章可提供訊息認證與不可否認性，但無法提供機密性，需透過其他機制來達成。

(三)窺探是一種機密性攻擊，因其為對資料的非法存取或攔截。