《電腦網路》

試題評析

今年的的電腦網路考題考的題目較多，每個題目又區分爲數個子題，每個子題大約佔3至5分左右。因此是屬於簡答型的考題。相較於前幾年的考題來說，考的內容比較簡單，但範圍比較廣泛。大多數的考題集中在Ethernet網路、無線網路與TCP/IP的主題上，也包含了NAT與DNS等相關主題。考生只要熟讀電腦網路的概念就可以取得高分。用功的考生可得85分以上的高分

一、就OSI模式中的Data link層而言:

(一)送、收兩方交換那些“同一層”的重要訊息？（4分）

(二)如何傳遞這些訊息？（3分）

(三)如何與上方的Network層交換訊息？（3分）

答：

(一) 資料連結層的功能:

1. 提供網路層服務
2. 訊框化(Framing)
3. 錯誤控制(Error Control)
4. 壅塞控制(Congestion Control)

(二) 將要傳送的訊息放入header或tail內，由接收端解讀並執行。如Error check在Ethernet使用CRC的檢查碼放入tail中的FCS欄位。Congestion Control則由LLC header處理。

(三) 利用frame type欄位確定搭配的網路層協定，如Ethernet II的Type欄位。

【高分閱讀】

請參考許振明老師-電腦網路講義第一回第二章p. 68

二、送、收方如何設定滑動視窗（Sliding Window）的視窗大小以達到Go-Back-N ARQ的功能目標？（5分）

答：

發送端的window size最大值只能是最大的序號(MAX_Sequence)，因爲避免發生錯誤時無法辨識。接收端的window size只能是1，收到資料立刻回應ACK，若有發生錯誤，則糾收端將後續的資料立刻丟棄，也就是沒有準備buffer保存後續的資料。

【高分閱讀】

請參考許振明老師-電腦網路講義第一回第二章p. 74

三、試就CSMA/CD協定回答以下兩個問題：

(一)如何處理carrier sense？（4分）

(二)如何“偵測”訊息碰撞？（4分）

答：

(一) 每一個工作站在傳送之前必須先監聽同軸電纜上是否已經有訊號在傳送(Carrier Sense) ，如果沒有則可立刻將訊框傳送出去。如果有則表示其他工作站正在傳送，此時工作站繼續監聽同軸電纜上的訊號，直到訊號消失(該訊框傳送完畢)後立刻將其訊框傳送上電纜。

(二) 在傳送訊框同時也要繼續監聽同軸電纜上的訊號，看看是否由其他的訊號的干擾造成衝撞。如果發生衝撞則立即停止傳送訊框並且改傳送一個「擾亂訊號」(Jamming Signal)，強迫造成更嚴重的衝撞，使得每一個

參與衝撞的工作站能確實偵測出衝撞。否則表示該筆訊框成功的傳送出去。發生衝撞的工作站則在各自等待一段隨機延遲時間(random delay time) 之後再進行載波感應(Carrier Sense)。

【高分閱讀】
請參考許振明老師-電腦網路講義第一回第三章p. 95

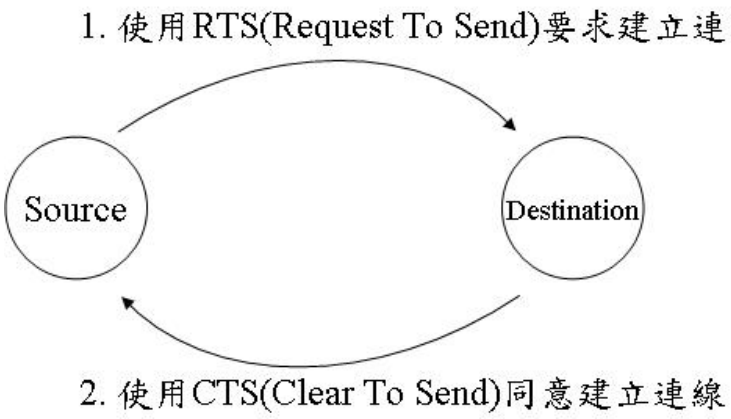
四、試就CDMA協定回答以下兩個問題：
(一)為何傳輸頻道需要展頻（Spreading Spectrum）？（4分）
(二)每一部連線的行動設備都必須擁有一個user code，請問這些user codes應該滿足什麼特性？（4分）

答：
(一) 展頻就是將電波涵蓋的頻率範圍擴展開來，把功率降低，使波形由『尖高形』變成『寬扁形』，以增強抗干擾能力和隱密性，可以允許多個使用者在同一個頻帶上同時傳送資料，並減低了資料被竊取的機會。
(二) user code指的是展頻碼(Spreading Code)，CDMA之所以可以允許不同的串送端同時在一個頻帶上傳送，主要就是透過不同的展頻碼彼此正交的特性，如第1組的展頻碼爲(1 1 1 -1 1 -1 -1 -1)，第2組的展頻碼爲(1 -1 1 1 1 -1 1 1)，(1 1 1 -1 1 -1 -1 -1)* (1 -1 1 1 1 -1 1 1) = 0稱之。

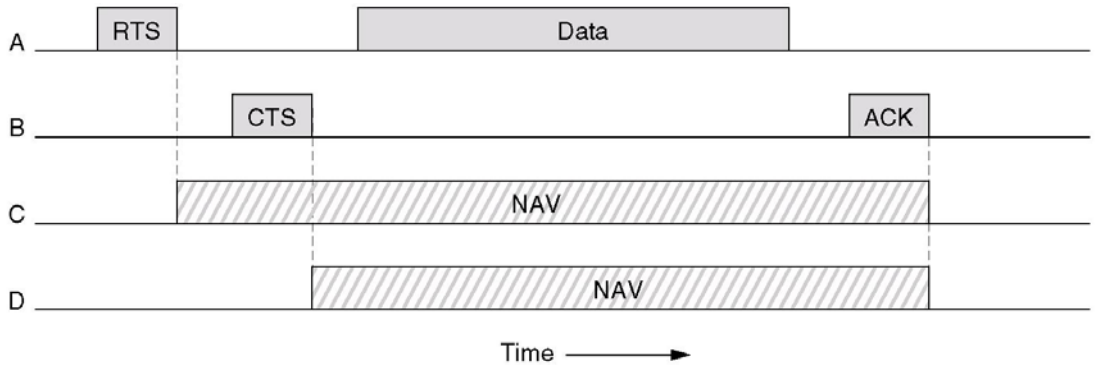
【高分閱讀】
請參考許振明老師-電腦網路總複習補充講義p. 4

五、試就IEEE 802.11協定回答以下問題：
(一)說明兩部電腦於連線過程中握手階段（Handshaking Period）的工作。（4分）
(二)在上述工作中，使用什麼機制來延緩或阻止其他電腦傳送資料，以免造成資料相沖。（4分）
(三)AP（Access Point）如何與轄區內的電腦互傳資料？（4分）

答：
(一)



(二)
使用預約使用網路時間的方式避免其他電腦傳送資料產生碰撞，其他電腦將被預約的剩餘時間記錄在NAV(Network Allocation Vector)裡面。



(三)
無線AP的架構是基礎建設式(Infrastructure Network)網路架構，所有電腦必須先與AP連線(使用RTS/CTS)後，透過AP將資料轉送給接收端電腦。

【高分閱讀】
請參考許振明老師-電腦網路講義第二回第五章p.5

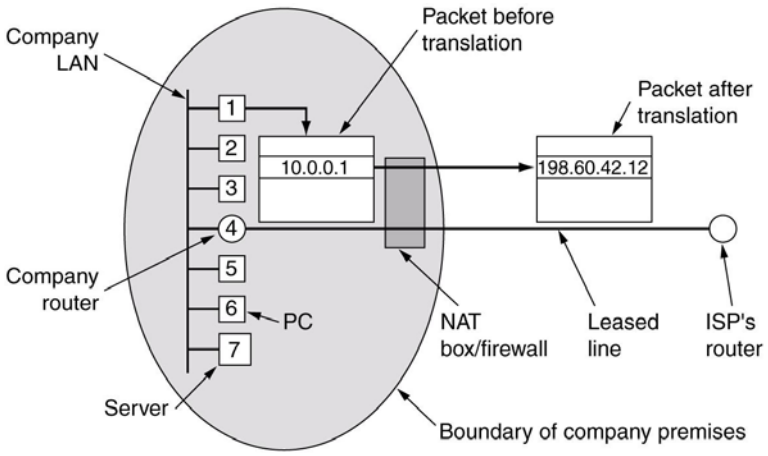
六、今有某單位之電腦獲分配IP位址為192.168.2.24/26，試問:
(一)該電腦所處網路之網路位址（network address）為何？（3分）
(二)該電腦所處網路可容納多少個IP位址？（3分）
(三)若你需要為該PC設定網路遮罩（network mask），則設定值為何？（3分）
(四)今查出某一台IP位址為192.168.2.128/26的電腦中毒，則此中毒電腦和上述電腦是否處在相同網路上？（此小題答案須敘明理由才予以計分）（4分）

答:
192.168.2.24/26代表網路欄位佔26位元，主機欄位佔6位元
(一) 取出192.168.2.24的前26位元即爲網路位址 => 192.168.2.0
(二) 主機欄位佔6位元，因此共有26個IP位址，也就是有64個IP位址。
(三) netmask爲 192.168.2.192
(四) 192.168.2.128/26的網路位址爲192.168.2.128，與192.168.2.24的網路位址192.168.2.0不同，因此隸屬不同區域網路。

【高分閱讀】
請參考許振明老師-電腦網路講義第二回第六章p.29

七、試就NAT（Network Address Translation）回答下列問題：
(一)為何需要使用NAT？（4分）
(二)某單位使用NAT後，若欲在單位內部設置WWW網路以供外界存取，可行否？（此小題答案須敘明理由才予以計分）（3分）

答:
(一) NAT(Netowrk Address Translation): 使用多台電腦使用虛擬 IP 共用一個實體 IP 的一種技術。目前業界使用此項技術建置公司內部網路。



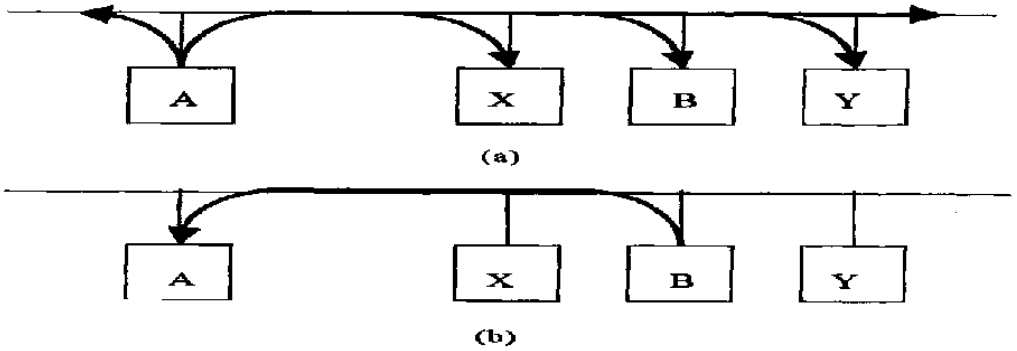
(二) 在NAT伺服器的內網中建立WWW伺服器，所以WWW伺服器所使用的虛擬IP位址，而無實體的IP位址。因此，外部電腦無法知道WWW的實體位址，因此符法與WWW伺服器連線。

【高分閱讀】
請參考許振明老師-電腦網路講義第三回第九章p.37

八、試就ARP（Address Resolution Protocol）協定回答下列問題：
(一)協定的工作原理為何？（6分）
(二)何謂ARP spoofing？（4分）
(三)ARP spoofing會造成何種資安危害？（4分）

答：

(一) ARP 運作原理
1. 查詢者A發出ARP訊框查詢
2. 在LAN上有兩種電腦會回答，第一個是ARP伺服器，或者是被查詢的電腦



(二) ARP Spoofing(ARP欺騙)攻擊的根本原理是因爲電腦中維護著一個 ARP 快取記憶體，並且這個ARP 快取記憶體是隨著電腦不斷的發出ARP請求和收到ARP回應而不斷的更新的， ARP快取記憶體的目的是把機器的IP位址和MAC位址相互映射，使得IP資料包在乙太網內得順利而正確找到目的MAC位址，然後正確無誤的傳送。如果你可以藉由發出標準的ARP請求或ARP回應來擾亂或竄改某電腦或路由器內正常的ARP表，而導致該電腦發出的資料包誤傳目的地，或使OSI的第二層乙太網和第三層無法連接，進而癱瘓網路，我們就稱你使用了ARP欺騙攻擊。

(三) ARP Spoofing如中間人攻擊(Man-in-the-Middle attack)與連線劫奪(Session Hijacking)就是採取ARP spoofing等攻擊手法達到欺騙主機、反追蹤或是避開交換器訪問安全存取的安全機制的防護。連線劫奪(Session Hijacking)

利用ARP欺騙將使用者正常的連線搶過來；中間人攻擊則利用ARP同時欺騙使用者(Client)與服務器(Server)兩邊使所有兩邊的交談都要透過入侵人的轉述，達到欺騙、側錄、竄改資料的目的。

【高分閱讀】
請參考許振明老師-電腦網路講義第三回第八章p.9

九、試就TCP協定回答下列問題：

（一）TCP Client發起three-way handshaking動作時，其TCP表頭中的sequence欄位值如何設定？為什麼？（4分）

（二）何謂SYN flooding攻擊？（4分）

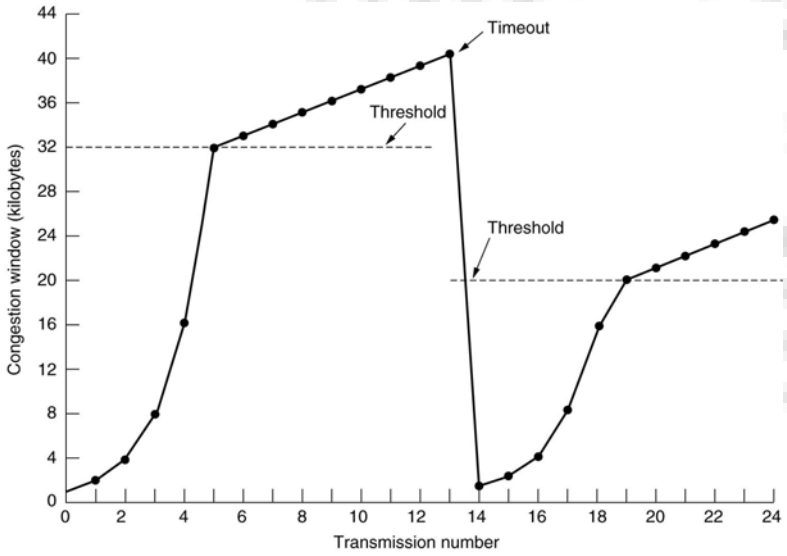
（三）TCP如何做到Congestion control？（4分）

答：

(一)當資料要從一台主機傳送去另一台主機的時候，發送端會爲封包建立起一個起始序號，然後按照所傳送的資料長度(位元組數值)，依次的遞增上去。根據此一原理，我們可使用遞增之後的值來作爲下一個封包的序號。這樣的設計除了能規範封包順序以進行資料重組之外，還有另一個非常有用的功能，TCP 的確認會指出接收端下一個期望接收到的位元組序號。

(二) SYN floods:是一種駭客通過向服務端發送虛假的包以欺騙伺服器的做法。具體說，就是將包中的原IP地址設置爲不存在或不合法的值。伺服器一旦接受到該包便會返回接受請求包，但實際上這個包永遠返回不到來源處的電腦。這種做法使伺服器必需開啓自己的監聽埠不斷等待，也就浪費了系統各方面的資源。

(三) 使用 slow start 的方式設定 Sliding Window size，達到 window size 一半前倍數成長，一半後則加 1 成長。



【高分閱讀】
請參考許振明老師-電腦網路講義第二回第七章p.96

十、試就DNS（Domain Name Server）回答下列問題：

（一）為何需要DNS？（4分）

（二）Root DNS server的功用為何？（4分）

（三）所謂Authoritative response意指為何？（3分）

答：

(一) 網域名稱系統(Domain Name System，簡稱DNS)，就是提供網域名稱與IP位址的對應服務，例如:www.ncku.edu.tw <--> 140.116.2.125。由網域名稱查詢IP位址，一般稱爲DNS正解(forward domain)；由IP位

址反查網域名稱，一般稱爲DNS反解(reverse domain)。

(二) 根名稱伺服器(Root name server): 記錄了各 top domain 分別是由哪些 DNS server 負責，全世界共有十三個根名稱伺服器。DNS系統基本是採樹狀階層式(hierarchy)的架構。網際網路上有十來個最上層的頂層root DNS servers，在這些系統中，記錄著所有最頂層(Top Level Domain，以下簡稱TLD)，TLD DNS servers的資料，經由這些最頂層負責的DNS servers，我們可以從root DNS servers一層一層，一路往下。找到各domain zone實際負責的(authoritative)DNS servers。

(三) 認證名稱伺服器(Authoritative name server): Host都會來此主機註冊。當root server亦無法解析名稱時，就會詢問Authoritative name server。

【高分閱讀】
請參考許振明老師-電腦網路講義第三回第九章p. 41