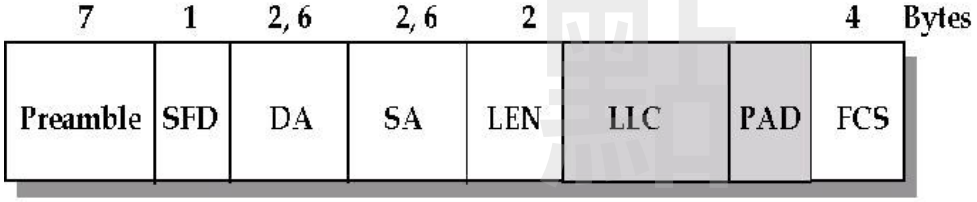
《電腦網路》

試題評析	本次試題的七個問題中大部份都是歷屆考題曾出過的類似題，所以只要細心的同學仔細作答，取得高分並不困難。尤其多個問題仍集中於802.3乙太網路與802.11無線網路的主題上。估計用功細心的考生可得85~90以上的高分。

一、就高速乙太網路（Fast Ethernet）而言，實體層的標頭（header）包含什麼資訊？功能為何？乙太網卡如何確保訊息傳遞正確？（10分）

試題評析	本題測驗對乙太網路的熟悉程度，上課時曾經提到五大通訊協定的通訊協定格式非常重要，其中包含乙太網路通訊協定，如果有注意提醒則本題就可輕鬆得分。
考點命中	《高點電腦網路講義第一回》，許振明編撰，頁109。

答：



(一)1.Preamble：同步訊號佔7個位元組，給實體層收到訊號時進行同步用途。

2.SFD（Start Frame Delimiter）：訊框起始邊界符號佔1個位元組，說明下一個位元組才是MAC訊框的開始。

3.DA（Destination Address）：目的乙太網路卡位址。

4.SA（Source Address）：來源乙太網路卡位址。

5.LEN/Type：記錄資料欄位長度或上層所使用的通訊協定。

(二)乙太網路透過標尾（Trail）的FCS（Frame Check Sequence）進行CRC檢測法執行資料的正確性判斷。

二、CHECKSUM錯誤偵測方法通常運用在網路層與傳輸層。假設送方會將傳送訊息切成一個個5-bit大小的區塊，再計算checksum區塊。試計算出0101011100001100011l的checksum區塊，並列出運算過程。（10分）

試題評析	這是在網路的檢查碼單元中的一個計算題，曾在100年交通人員試題中出現類似題，只要記住使用1’s補數加法的規則就可計算答案。
考點命中	《高點電腦網路講義第一回》，許振明編撰，頁76。

答：

執行1’s補數加法得 checksum: 01011

	01010 11100
1	00110
sum	00111 00110
sum	01101 00111
sum	10100
checksum	01011

三、就CSMA/CD而言，為何它不用像CSMA一般，於訊息傳遞後等待回應訊息（acknowledgement）後才能再傳送下一段訊息？一旦發生碰撞，它又會如何解決？請以繪圖方式描述整個處理流程，並註明必要的變數。（15分）

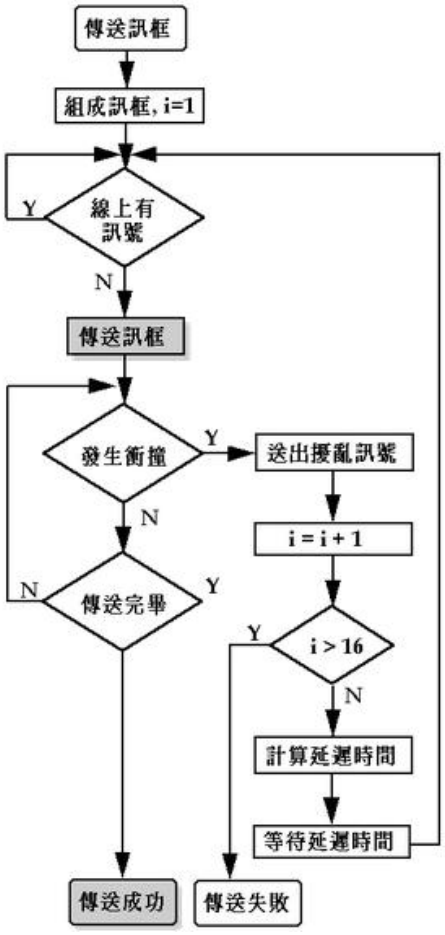
試題評析	本題測試乙太網路的規則外，也比較了與CSMA/CA的差異度，這個題型自古以來就是一個重要的主題，一般的考生就可以輕鬆取分。
考點命中	《高點電腦網路講義第一回》，許振明編撰，頁104。

答：

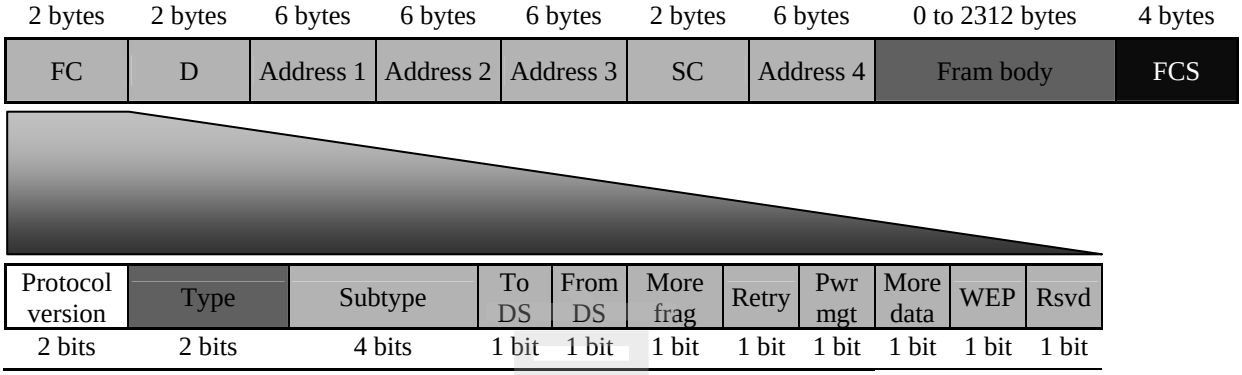
(一)乙太網路是一個不可靠的通訊協定，不像802.11 CSMA/CA的傳送錯誤率很高，乙太網路的傳輸錯誤率很低的情形下，所以不使用ACK的機制。

(二)如果發生碰撞(Collision)，乙太網路採用binary exponential back-off algorithm，產生一個亂數休息時間，休息過後，再次競爭下一次傳送權。

1. n : (n <= 16)：最多重送次數。
2. k : Min (n,10)：取n與10較小值。
3. r : (單位: slot time) between 0 <= r < 2k：隨機延遲時間。



四、下圖是IEEE 802.11的frame格式。假設同處在一個ad hoc網路下的兩部無線裝置A與B，A要傳送一段長1500 bytes的訊息給B，則data-link layer需要傳送多大的frame（單位byte）？frame裏面的address 1-4的內容分別為何？如果考量無線網路傳輸的不穩定性，將frame body以fragmentation方式分三次遞送，每次500 bytes，則總共需要傳送多少個bytes？（15分）



試題評析	試題已提供802.11的訊框格式，所以訊框切割的部分應可輕鬆回答。至於802.11的位址部分需熟悉802.11的工作原理才能拿到高分。
考點命中	1.《高點電腦網路講義第一回》，許振明編撰，頁19。 2.《高點電腦網路講義第二回》，許振明編撰，頁5。

答：

標頭長度：30 Bytes，標尾4 Bytes。

(一)因爲資料長度1500Bytes <= 2312 Bytes，所以資料不切割。

因此訊框長度爲 30Bytes + 1500Bytes + 4Bytes = 1534Bytes。

(二)

To/From DS	**意義**
To DS = 0, From DS = 0	訊框從一個工作站直接送給同一個BSS的工作站
To DS = 0, From DS = 1	訊框由分散式系統傳入到BSS
To DS = 1, From DS = 0	訊框由BSS送出到分散式系統
To DS = 1, From DS = 1	訊框從一個BSS送到另一個BSS

BSSID：BSS identifier

SA（Source Address）：起始工作站位址

DA（Destination Address）：目的地工作站位址

TA（Transmitter Address）：傳送工作站位址

RA（Receiver Address）：接收工作站位址

以下爲四個位址的意義

To DS	**From DS**	**Address 1**	**Address 2**	**Address 3**	**Address 4**
0	0	RA = DA	TA = SA	BSSID	N/A
0	1	RA = DA	TA = BSSID	SA	N/A
1	0	RA = BSSID	TA = SA	DA	N/A
1	1	RA	TA	DA	SA

(三)切割爲三次傳送，每次500Bytes，則每一個訊框長度爲

30Bytes + 500Bytes + 4Bytes = 534Bytes。

三個訊框總長度爲 534Bytes * 3 = 1602Bytes。

五、Mobile IP的功用為何？請闡釋其工作原理，並且說明在IPv4的環境下Mobile IP在封包轉送上有何效率問題？（20分）

試題評析	行動IP的問題是一個常考的問題，只要一般考生就可得到高分。
考點命中	《高點電腦網路講義第二回》，許振明編撰，頁58。

答：

(一)行動式IP(Mobile IP)：使IP電腦不僅能保有原先擁有的IP位址，而當其在不同網段的網路中移動時，仍能保持連線通訊持續不中斷。

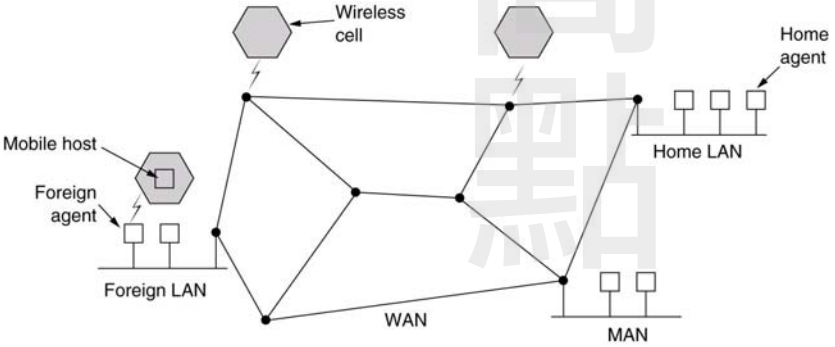
1.Mobile IP 主要組成包括：

(1)移動節點(Mobile Node：MN)

(2)本地代理人(Home Agent：HA)

(3)外地代理人(Foreign Agent：FA)

(4)通信者(Correspondent Node：CN)：指在Internet 上任一與MN 通信裝置。



2.行動式IP運作可分三個階段：

(1)代理人探索(Agent Discovery)：移動主機尋找本地及外地代理人階段。

(2)註冊(Registration)：移動主機向本地代理人(HA：Home Agent) 及外地代理人(FA：Foreign Agent) 登記現有位置階段。

(3)建立隧道(Tunneling)：本地代理人(HA)建立與外地之移動主機間通道階段。

在代理人探索階段後，移動主機得到一個暫時IP位址，我們稱之爲轉送位址（Care-of Address；CoA），此位址可以從FA廣播取得（稱爲FA CoA）或由DHCP或手動設定得到（稱爲Collocated CoA）。在註冊階段時，移動主機直接或透過FA向HA註冊其CoA，此時HA在記憶體中建立一個稱爲移動連結表（mobility binding table），其中記錄移動主機原始的IP與現在的CoA對應；若在註冊時透過FA，則FA同時會在記憶體中建立一個來訪者表（visitor list）。因此，當在網際網路上有通信者欲與移動主機通信時，資料傳送至移動主機原先所在之網路時立刻會被HA所攔截；若原先移動主機直接向HA註冊，則HA會建立起一IP隧道將之轉送至移動連結表所註冊之移動主機CoA處，FA從該IP隧道解開封裝後再將資料傳給移動主機；若原先移動主機透過FA向HA註冊，則FA就無需執行IP隧道解封裝的動作，只需如路由器般執行轉送動作即可。但若移動主機欲與通信者通信，則移動主機可將資料直接送給FA再由FA將其直接繞至通信者即可。

(二)Mobile IPv4每次來源端傳送資料都須透過HA轉送給FA後資料才會到達目的端電腦，因此透過層層轉送自然效率比較差。

六、網管人員常會用到traceroute（或是tracert）這個程式。請說明這個程式在網路管理上的用途以及其背後的工作原理。（15分）

試題評析	Traceroute指令用法也是常見的考題，一般考生就可得到高分。
考點命中	《高點電腦網路講義第三回》，許振明編撰，頁13。

答：

(一)traceroute命令：可找出通往目的地的所有經過的路由位址，並以數字將路由順序標識出來。如在網路不通

時可用來追蹤是哪個路由器故障。

(二)工作原理

1.首先，traceroute命令會向目標位址送出UDP偵測封包，但將第一個送出的封包之TTL設爲1。這樣，第一個路由節點在處理這個封包的時候，減掉1，並發現TTL爲0，於是就不處理這個封包，並同時送回一個ICMP 封包。這樣，發送端就知道第一個路由節點在哪裡了。

2.當接到第一個ICMP返回的時候，程式會檢查返回主機是否就是目標主機，如果不是，則再送出第二個封包，但TTL比上次增加1。

3.這樣，第一路由節點接到的封包之TTL就不是0，那麼處理完畢後送給下一個節點，同時將TTL扣除1。這樣，當下一個站收到這個封包，再扣掉TTL爲0，也會送回ICMP封包，這樣，程式就知道第二個路由節點在哪裡了。

4.然後重覆上一個動作，直到找到目標主機爲止，或是封包的最大TTL（通常爲30）都用光爲止。

七、請簡介ARP（Address Resolution Protocol）spoofing和IP spoofing背後的技術原理，並說明其造成的資安威脅為何？（15分）

試題評析	Spoofing問題也是歷屆考題常見的問題，仔細回答就可得到高分。
考點命中	《高點電腦網路講義第三回》，許振明編撰，頁11。

答：

(一)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。

(二)IP Spoofing（IP位址欺僞）：這是一種攻擊者得知主機位址之後，利用外部封包攻擊主機的方法，由於封包（Packet）的來源位址和內部封包一樣，因此主機（Host）會認爲這是來自內部的封包，因而允許進行鏈結（Link），這種攻擊方法也會被內部破壞者使用。

(三)無論是ARP spoofing或IP spoofing技術都是透過欺騙（spoofing）的方式達到目的，這兩種方式都會造成接收端誤認資料的正確性造成入侵。