《資通網路》

試題評析	第一題屬資訊安全範疇，第二題及第五題為中層傳輸，第三題屬無線網路，第四題則是高層應用。整體而言配分平均，然記憶題型較多，且各子小題的完整性亦需花費大量時間，為學員記憶力與論述能力的綜合考驗。
考點命中	第二題：《高點・高上資通網路講義》第三回，張又中編撰，頁3-25~26。 第三題：《高點・高上資通網路講義》第五回，張又中編撰，頁5-14~15。 第四題：《高點・高上資通網路講義》第四回，張又中編撰，頁4-19~20。 第五題：《高點・高上資通網路講義》第三回，張又中編撰，頁3-18~20。

一、加密機制可區分為對稱式或非對稱式加密機制，請說明這兩種機制的原理，優缺點，及功能上的差異。DES，RSA與公開金鑰系統分別屬於那種機制？（25分）

答：

對稱式加密法機制為傳送方對明文的加密與接收方對密文的解密都是使用同一把金鑰進行XOR運算，易於以硬體實做，適用於大量資料的加解密。

非對稱式加密法機制為傳送方對明文的加密與接收方對密文的解密使用兩把不同的金鑰，一把為公開金鑰(Public Key)，另一把為私密金鑰(Private Key)，適用於少量資料的加解密。

加密機制	對稱式加密	非對稱式加密
金鑰數目	單一鑰匙	成對鑰匙
金鑰種類	秘密的	一把公開的，一把秘密的
處理速度	快	慢
金鑰管理	簡單，不易有效管理	需要數位簽章或公正第三方(Third Party)
適用對象	大量資料	少量資料

DES為對稱式加密機制；RSA與公開金鑰系統則屬非對稱式加密機制。

二、要確認網路資料傳輸是否正確，有一種方法是檢查檢驗和（checksum），如TCP中的虛擬標頭所使用的方式。請問在IPv4的網路中，虛擬標頭的作用為何？包含那些欄位，長度又為何？請描述TCP封包傳送，發送端與接收端對虛擬標頭的檢驗和計算過程。（20分）

答：

由於TCP本身沒有關於位址的資訊，可能造成區段(Segment)錯誤路由(Misrouted)。因此，需提供足夠的資訊，讓Checksum可檢測錯誤路由，即為虛擬表頭(Pseudo Header)，其欄位如下：

(一)來源位址(Source Address)

32位元的傳送端IPv4位址。

(二)目的位置(Destination Address)

32位元的接收端IPv4位址。

(三)零(Zero)

8位元的00000000。

(四)協定(Protocol)

8位元的通訊協定號碼，例如TCP為6。

(五)TCP長度(TCP Length)

16位元的TCP Segment長度(標頭+資料)，然不包含虛擬標頭本身。

傳送端將欲計算Checksum的欄位以16位元為單位加總，包含虛擬表頭、TCP區段，以1的補數運算後而得Checksum。接收端收到後循相同步驟並加總Checksum，如最終結果1的補數皆為0即可知道資料無誤，如不為0則可偵知錯誤。

三、一個802.11訊框的組成包含那些單元？其中，在訊框標頭中有一個為Duration/ID的欄位，請問在不同的訊框型態上，此欄位的作用有何不同？此外，如何區與檢視傳送端與接收端的位址？（20分）

答：

802.11訊框的組成如下：

1.訊框控制(Frame Control)

2.持續期間(Duration)

表示訊框與回應將佔據頻道的時間長度。

3.位址(Address)

表示訊框的來源與目的位址；另兩個位址表示蜂巢細胞內傳輸的來源與目的基地台。

4.序號(Sequence)

用來切割片段標上號碼，其中 14 個位元表示訊框，4 個位元表示切割片段。

5.資料(Data)

包含資料負載，最長可達2312個位元組。

6.檢查和(Checksum)

採用CRC-32進行錯誤偵測。

Duration/ID有下列不同的訊框型態：

1.短訊框間隔(Short Interval Frame Space, SIFS)

做為立即回應之訊框使用，計有要求傳送(Request To Send, RTS)、清除可傳(Clear To Send, CTS)、回應(Acknowledgement, ACK)，以及輪詢回應(Poll Response)…等。

2.PCF 訊框間隔(PIFS)

3.用於非競爭傳輸模式下，PCF 站台傳送訊框前所需等待的時間間隔。

4.DCF 訊框間隔(DIFS)

5.用於競爭傳輸模式下，DCF 站台傳送訊框前所需等待的時間間隔。

6.延伸訊框間隔(Extended IFS, EIFS)

7.站台重送訊框時所需等待的時間間隔。

8.間隔時間長短為：EIFS>DIFS>PIFS>SIFS，亦即訊框優先權為 RTS/CTS/ACK>PCF>DCF>重送訊框。

傳送端與接收端的位址需靠To DS與From DS欄位辨別，如下：

To DS	From DS	位址1	位址2	位址3	位址4
0	0	接收端	傳送端	BSS ID	N/A
0	1	接收端	傳送端AP	傳送端	N/A
1	0	接收端AP	傳送端	接收端	N/A
1	1	接收端AP	傳送端AP	接收端	傳送端

四、一個支援SNMP的網路環境，除了被管設備之外，管理系統需要包含那些部分？對於管理者與被被管元件間，一個SNMP系統是以何種模式運作？一個被管物件是如何被標示？（20分）

答：

(一)一個SNMP管理系統的組成如下：

1.SNMP 管理者(SNMP Manager)

為SNMP主要管理套件，安裝於網路管理系統上，負責向所管轄的設備索取管理訊息或設定網路組態，為SNMP管理環境的主要控制設備。

2.SNMP代理者(SNMP Agent)

一般安裝於被管理的網路設備上，如路由器、橋接器、主機等，其蒐集網路設備上的訊息，再以SNMP協定與SNMP管理者通訊，以達到管理目的。

3.被管理物件(Managed Object)

指被管理設備內的各種管理物件，如橋接器的網路介面卡、過濾資料庫等，皆以管理訊息結構(Structure of Management Information, SMI)的方式表達，且以樹狀識別碼(Tree Identifier)方式儲存於管理訊息資料庫

(Management Information Base, MIB)。

(二)SNMP運作模式

1.要求/回應(Request/Response)

SNMP 管理者利用 UDP Port 161 下達命令給 SNMP 代理者，代理者依據命令蒐集網路資訊後再回應 SNMP 管理者。

2.觸發(Trap)

由 SNMP 代理者利用 UDP Port 162 發送觸發(Trap)命令給 SNMP 管理者，管理者再回應給 SNMP 代理者。

(三)SNMP使用管理訊息結構(Structure of Management Information, SMI)來組織與管理設備，對每個設備配置物件識別碼(Object Identifier, OID)，並在樹狀架構中加以記錄與管理，可分為：

1.簡單資料型態

2.泛應用資料型態

五、(一)IPv4與IPv6兩種版本的協定在位址結構上，有何不同？（10分）

(二)一個IPv6主機的介面位址是如何組成的？（10分）

答：

(一)

IP	IPv4	IPv6
位址長度	32 Bits	128 Bits
標頭長度	20 Bytes(12欄)	40 Bytes(8欄)
標頭檢查和	Header Checksum	無
優先順序	Type of Service	Traffic Class
廣播位址	主機位址全為1	以多播、任播取代廣播
流量標籤	無	Flow Label
服務品質	些許	較佳
存活時間	0~255	Hop Limit
安全機制	Optional	IPsec
路由器偵測	Optional	路由器不用切割與檢查
自動網路組態	透過DHCP伺服器	依賴 Neighbor Discovery 通訊協定，從鄰近路由器的資訊取得

(二)

IPv6以8群4個16進位的數字表示，並以:分隔，表示如9000:0000:0000:0000:0123:4567:89AB:CDEF。由於位址中含有許多個0，可用::替代，上例可寫為9000::123:4567:89AB:CDEF。

IPv4位址可寫成::後的IPv6表示方式，如::FFFF:140.123.55.66，或是::FFFF:8C7B:3742。

(三)資料的非法存取或攔截。