

《資通網路》

試題評析	本份試題除了第四題屬資訊安全範疇外，主要集中於底層技術、高層應用與無線網路三章。整體而言試題難易度適中，若熟讀講義內容，應可獲得不錯的成績。
考點命中	第一題：《高點・高上資通網路講義》第二回，張又中編撰，頁2-44。 第二題：《高點・高上資通網路講義》第二回，張又中編撰，頁2-10~11； 《高點・高上資通網路講義》第五回，張又中編撰，頁5-5、50。 第三題：《高點・高上資通網路講義》第四回，張又中編撰，頁4-37~38。 第五題：《高點・高上資通網路講義》第四回，張又中編撰，頁4-4~6。

一、在交換式的區域網路（Switched Local Area Network）上，VLAN是常見的網路架構，請說明：（每小題5分，共20分）

- （一）什麼是VLAN？
- （二）建置VLAN之目的？
- （三）同一VLAN如何跨兩個或多個交換器？
- （四）不同VLAN上之使用者如何互送資料？

答：

- （一）VLAN是建構於區域網路交換器的網路管理技術，網管人員可透過設定組態表(Configuration Table)，控制交換器分派出入區域網路的封包到正確的Port，對不同實體區域網路中的設備進行邏輯分群，可於一或多個交換器上實現。
- （二）VLAN目的如下：
 - 1.提升安全性。
 - 2.控制廣播。
 - 3.增加頻寬利用率。
 - 4.降低延遲。
- （三）可利用802.1Q建立Trunk，使其可以跨兩或多個Switch。
- （四）可利用路由器(Router)來讓不同VLAN的使用者相互送資料。

二、以下為無線網路與通訊中常見之術語，請列出它們之英文全名，並試述其用意。（每小題4分，共20分）

- （一）QPSK
- （二）3GPP
- （三）MANET
- （四）FHSS
- （五）MIMO

答：

- （一）四象限相位位移調變(Quadrature Phase Shift Keying, QPSK)，固定振幅，以4種可能的相位位移來表示，每個訊號包含2個位元。
- （二）第三代合作夥伴計劃(3rd Generation Partnership Project, 3GPP)，是一個於1998年12月成立的標準化機構，其目標為國際電信聯盟制訂與實現全球性的行動電話系統規範。
- （三）行動隨意網路(Mobile Ad Hoc Network, MANET)，亦稱行動網狀網路(Mobile Mesh Network)，是一種以行動裝置透過無線連結自我組態所形成的網路，屬於無線隨意網路的一種。
- （四）跳頻展頻(Frequency Hopping Spread Spectrum, FHSS)，將可用的頻段畫分為若干小頻道，傳送端於小頻道間變換傳送，接收端也在相同的小頻道跳躍順序下接收訊號，以達成雙方通訊。
- （五）多重輸入多重輸出(Multiple Input Multiple Output, MIMO)，利用多天線技術，來提高資料速率或是強化傳輸訊號。

三、(一)何謂HTTP串流(Streaming)?(5分)

(二)HTTP串流有那些優點?(5分)

(三)試說明HTTP串流之運作方式。(10分)

答：

(一)HTTP串流為基於HTTP(Hypertext Transfer Protocol)的串流媒體網路傳輸協定。

(二)HTTP串流優點有：

- 1.易於發佈。
- 2.易於穿透防火牆(Firewall)或代理伺服器(Proxy Server)。
- 3.可依據客戶端網路的資料速率，提供不同品質的媒體串流。

(三)以HTTP Live Streaming(HLS)為例，其為蘋果公司提出基於HTTP的串流媒體網路傳輸協定，2017年8月，RFC 8216發佈，描述了HLS協定第7版的定義。

HLS工作原理是將整個串流切割成一個個基於HTTP的小文件來下載，每次只下載一些。當媒體串流在播放時，用戶端可選擇從許多不同的來源以不同的速率下載，允許串流媒體適應不同的資料速率。

四、區塊加密(Block Cipher)是一類常用的對稱加密方式，但它在處理長串之訊息時有些缺點，因此加密區塊連結(Cipher Block Chaining)技術被用來改善區塊加密。

(一)請說明區塊加密之缺點。(8分)

(二)加密區塊連結技術如何運作以改善區塊加密之缺點?(12分)

答：

(一)區塊加密是一種對稱式金鑰加密演算法，其將明文分成多個等長的區塊，使用演算法和對稱式金鑰對每組區塊分別加密/解密，典型的應用如DES、AES。區塊加密的缺點在於相同的明文加密後會出現相同的密文，因此攻擊者可比對區塊明文與密文間的關係。

(二)加密區塊則是加入初始向量(Initialization Vector, IV)，在第一回合時，明文先與初始作XOR運算，再將運算結果導入演算法加密，而得第一個密文區塊；第二回合時，再將第一個密文區塊與本次的明文區塊進行XOR運算，再將其結果導入演算法加密，而得第二個密文區塊，依此類推。如此一來，攻擊者將難以比對區塊明文與密文間的關係。

五、網頁瀏覽已經是現代生活之一部分，而瀏覽器大多必須透過網域名稱系統(Domain Name System; DNS)來運作，請問：

(一)DNS的任務是什麼?(5分)

(二)針對一個使用者請求，DNS如何運作?(6分)

(三)DNS伺服器分成三大類，試說明之。(9分)

答：

(一)DNS使用TCP、UDP Port 53的一種索引查詢服務，將人們可閱讀的ASCII字串形式主機名稱，對應轉換成數字形式的IP位址，亦支援郵件目的位址和IP位址間的對應。

(二)當應用程式需要將網域名稱對應到IP位址時，先將名稱做為參數呼叫函式庫中的解析程式(Resolver)，解析程式送出UDP封包至DNS伺服器，DNS伺服器找出網域名稱對應的IP位址並回傳給解析程式，其再傳回給呼叫的應用程式。

(三)DNS伺服器類型有：

- 1.主要名稱伺服器(Primary Name Server)
儲存區域內各主機資料的正本，若此區域資料有所變更時，直接入此伺服器的資料庫，通稱為區域檔案(Zone File)。
- 2.次要名稱伺服器(Secondary Name Server)
定期向另一部名稱伺服器拷貝區域檔案，稱為區域傳送(Zone Transfer)。
- 3.快取伺服器(Cache Only Server)
快取伺服器會向指定的DNS伺服器查詢，並將查詢回應存放於自己的快取並回覆給用戶端。