《資通網路》

試題評析	本份試題第一、二題屬中層傳輸，涵蓋TCP壅塞控制、流量控制、IP協定；第四題為底層技術，主考VLAN；第三、五題則屬資訊安全範疇。 就網路部分，試題中規中矩，講義皆有涵括，高分重點在於考生是否能信、達、雅地將內容轉化呈現，將會是本科群雄逐鹿中原的關鍵所在。
考點命中	第一題：《高點‧高上資通網路講義》第三章，張又中編撰，頁3-25~27。 第二題：《高點‧高上資通網路講義》第三章，張又中編撰，頁3-12~13。 第三題：《高點‧高上資通網路講義》第三章，張又中編撰，頁3-17與上課補充。 第四題：《高點‧高上資通網路講義》第二章，張又中編撰，頁2-43。

一、回答下列有關於網際網路通訊協定套件（Internet Protocol Suite）或稱 TCP/IP 通訊協定疊（protocol stack）相關問題。

(一) 說明 TCP 協定的壅塞控制（congestion control）與流量控制（flow control）有何不同。（10 分)

(二) 說明 MSS 與 MTU 的功能與兩者之差異。（10 分）

答：

(一)TCP 壅塞控制為 TCP 假設封包遺失都是網路壅塞所引起，利用表示傳送端任何時間在網路上可以送出的位元組數之壅塞視窗(Congestion Window)進行處理。

(二)TCP 流量控制是用來溝通傳送端可傳送的資料區塊，當滑動視窗為 0 時傳送端暫停傳送，以避免接收端發生緩衝區溢位問題。

(三)最大分段大小(Maximum Segment Size, MSS)為 TCP 協定的參數，其以 Bytes 為單位，定義傳輸雙方所能接受的最大分段資料量。

(四)最大傳輸單元(Maximum Transmission Unit, MTU)指一通信協定於某一層所能通過的最大封包大小(以 Bytes 為單位)。例如：IP 協定可將封包切割，以符合傳輸路徑上路由器所能接受的 MTU，再重組回原始封包。

二、有一個新組織需要布建網路，他們擁有網段 192.168.4.0/24。希望分出三個子網路：一個子網路給辦公室員工使用、一個給後勤 IT 部門使用，第三個放在公共空間給民眾使用。

(一) 這三個子網路的 network ID 為何？（4 分）

(二) 這三個子網路的 Subnet mask 範圍為何？（4 分）

(三) 這三個子網路的 Host ID 範圍為何？（4 分）

(四) 這三個子網路各有多少個可使用的 Host ID？（4 分）

(五) 這三個子網路的 broadcast ID 為何？（4 分）

答：

(一) 192.168.4.0/26
192.168.4.64/26
192.168.4.128/26

(二) 255.255.255.192

(三) 192.168.4.1~192.168.4.62
192.168.4.65~192.168.4.126
192.168.4.129~192.168.4.190

(四) 2^6-2=62

(五) 192.168.4.63
192.168.4.127
192.168.4.191

三、ARP poisoning 或稱 ARP spoofing 是利用 ARP 通訊協定發動的攻擊。
(一) 說明 ARP poisoning 或稱 ARP spoofing 之攻擊原理。（10 分）
(二) 說明 ARP poisoning 或稱 ARP spoofing 攻擊之防範方法。（10 分）

答：

(一)攻擊者藉由發出標準的 ARP Request 或 ARP Response 來干擾或竄改某節點正常的 ARP 表，導致該節點發出的資料誤傳目的地，或使 OSI 第二層與第三層之服務無法連接，進而癱瘓網路。由於其隱密難以偵測，故常用來作為如中間人攻擊、連線劫奪之攻擊方法，以達到欺騙主機、反追蹤、避開安全機制、癱瘓網路等等目的。

(二)ARP Poisoning 攻擊之防範方法有：

1.使用靜態 ARP 表
網路每台主機的 ARP 表使用靜態方式來對應、更新，然不適用於大型網路。

2.DHCP Snooping
主要應用於交換器(Switch)，作用為屏蔽網路的非法 DHCP 伺服器。即開啟 DHCP Snooping 功能後，用戶端只能從管理員指定的 DHCP 伺服器獲取 IP 地址。

3.監聽網路異常的 ARP Response
若偵測到不正常的變動時可通知管理者。例如：UNIX 的 Arpwatch、Windows 的 XArp v2，或是網路裝置的 Dynamic ARP Inspection 功能。

四、網路是由許多區域網路（Local Area Network，簡稱 LAN）相連而成。
(一) 說明虛擬區域網路（Virtual Local Area Network，簡稱 VLAN）與 LAN 的差異性。（10 分）
(二) 說明 VLAN 優點。（10 分）

答：

(一)虛擬區域網路為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。
IEEE 802 委員會於 1995 年發表了 802.1Q VLAN 技術的實作標準與訊框結構，希望能透過設定邏輯位址(TPID、TCI)，對實體區域網路區隔成獨立虛擬網段，以規範封包廣播時的最大範圍。

(二)VLAN 優點：

1.安全性
例如：可限制網路病毒的擴散範圍於該 VLAN。

2.廣播控制
VLAN 相當於資料鏈結層的廣播網域(Broadcast Domain)，其能將廣播控制在內部，避免大範圍網路的廣播風暴(Broadcast Storm)。

3.頻寬利用
當 VLAN 切割後，其可提升交換器的處理效率，故可增加頻寬的利用率。

4.降低延遲
同上，故可降低延遲。

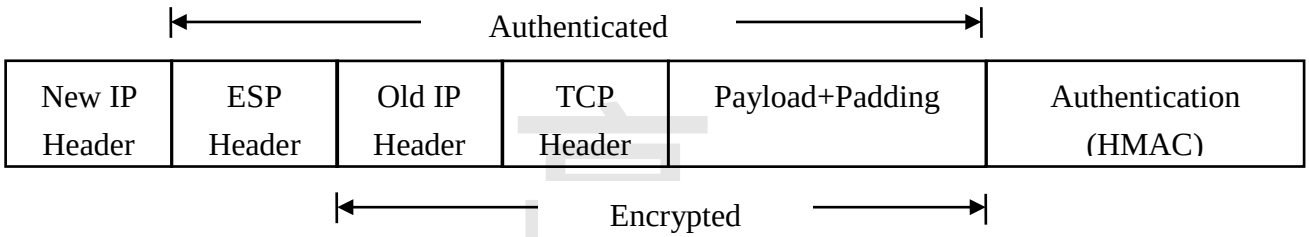
五、網際網路傳輸資料不安全，因此可以利用虛擬私有網路（Virtual Private Network，簡稱 VPN）方式達到安全服務。
(一) IPSec 可建立那一層的資料安全傳輸？說明如何使用 IPSec 通道模式（tunnel model）達到 VPN 功能。（10 分）
(二) 說明 IPSec tunneling 可以達到那些資料的安全服務。（10 分）

答：

(一)IPSec 作用於網路層(Network Layer)，為多服務、多演算法及多單元規模的架構。提供機密性、完整性，並避免重傳攻擊，描述於 RFC2401、2402、2406 及 2410。

IPSec 通道模式將整個 IP 封包重新封裝在一個全新標頭的 IP 封包中，故可支援 VPN。

(二)以 IPSec 封裝安全負載(Encapsulation Security Payload, ESP)的通道模式而言，其提供了以下的安全服務：



1.機密性(Confidentiality)
2.完整性(Integrity)
3.認證(Authentication)
4.存取控制(Access Control)