《資通網路》

試題評析	本份試題除了第六題屬資訊安全範疇外，主要集中於講義前4章，整體而言試題返璞歸真，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1章，張又中編撰，頁1-9~11。 第二題：《高點•高上資通網路講義》第3章，張又中編撰，頁3-33~34。 第三題：《高點•高上資通網路講義》第3章，張又中編撰，頁3-26。 第四題：《高點•高上資通網路講義》第4章，張又中編撰，頁4-22。 第五題：《高點•高上資通網路講義》第3章，張又中編撰，頁3-18~20。

一、國際標準化組織（ISO）提出了開放式系統互聯模型（Open System Interconnection Model），將電腦網路劃分為七個層。而網際網路協定堆疊（Internet protocol stack）則包含了五層。請問，開放式系統互聯模型的七層及網際網路協定堆疊的五層各為何？（20分）

答：

OSI七層：

(1) 實體層(Physical Layer)
(2) 資料鏈結層(Data Link Layer)
(3) 網路層(Network Layer)
(4) 傳輸層(Transport Layer)
(5) 會議層(Session Layer)
(6) 展現層(Presentation Layer)
(7) 應用層(Application Layer)

TCP/IP五層：

(1) 實體層(Physical Layer)
(2) 資料鏈結層(Data Link Layer)
(3) 網路層(Network Layer)
(4) 傳輸層(Transport Layer)
(5) 應用層(Application Layer)

二、IETF的RFC 1393裡介紹了traceroute，用於顯示封包在IP網路經過的路由器IP位址。試述其運作原理與所利用到的協定名稱。（15分）

答：

traceroute傳送ICMP回應封包給目的地，以確定到目的主機所經的路徑。其利用增加存活時間(TTL)來實現功能，發出的首3個封包TTL為1，之後3個封包TTL為2，依此類推，直到目的地回應或達到最大TTL為止。當封包經過一路由器時TTL－1，當TTL=0時便取消封包，並傳送ICMP Time Exceeded封包給原封包傳送者，可得一連串封包的傳輸路徑與來回時間。

三、TCP提供了擁塞控制的機制來調節傳輸速度。試述TCP Congestion Avoidance及TCP Slow Start的工作原理。（20分）

答：

以TCP Tahoe為例，演算法初始為慢速啟動(Slow Start)，每經過一個來回時間(Round-trip Time)，壅塞視窗呈指數成長，臨界值(Threshold)為視窗值的1/2，超過臨界值時進入壅塞避免(Congestion Avoidance)，壅塞視窗每次加1。

四、即時傳輸協定（Real-time Transport Protocol，RTP）定義了在網際網路上傳遞音訊和影片的標準封包格式，通常它是建立在UDP協定上的。RTP四個主要的RTP header欄位是payload type、sequence number、timestamp和synchronization source identifier。試述sequence number、timestamp和synchronization source identifier的意義。（15分）

答：

欄位	長度 (位元)	說明
資料類型 Payload Type	7	指定封包資料的編碼方式。
序號 Sequence Number	16	每傳送一個RTP封包序號值+1，接收端可用其來偵測封包遺失及恢復封包順序。
時間戳記 Timestamp	32	RTP資料封包第1個Bytes取樣時間。
同步來源識別 Synchronization Source Identifier	32	識別RTP串流的來源端。

五、IPv6是新一代的網際網路協定，用來解決IPv4所面臨的問題，請問是那些問題，IPv6針對這些問題做何改進。（15分）

答：

由於32位元的IPv4已逐漸不敷所需，因此網路學家想到利用長度更長、功能更完善的128位元IPv6來替代。

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

六、傳輸層安全性協定（Transport Layer Security）是IETF所定義的一種安全協定，目的是為網際網路通訊提供安全及資料完整性保障。試述其運作原理。又，其屬於網際網路協定堆疊裡那一層的協定？（15分）

答：

IETF將SSL標準化，以SSL 3.0為基礎，使用SSL 3.1，稱為TLS，定義於RFC2246，運作於傳輸層(Transport Layer)。TLS提供端對端身份認證與通訊保密，其基礎為PKI。協定設計在某種程度上能預防竊聽、干擾(Tampering)與訊息偽造。TLS包含三個階段：

(1) 協商支援的金鑰演算法：
　如協商雙方使用的雜湊函數：MD5、SHA1，及SHA256。
(2) 基於非對稱式金鑰的訊息加密和身份認證、基於 PKI 證書的身份認證：
　如RSA、Diffie-Hellman、DSA。
(3) 基於對稱式金鑰的資料加密：

如RC4、DES、3DES、AES、IDEA，及Camellia。

SSL/TLS最常見的應用為確保使用者瀏覽Web時的安全，使用者的Web瀏覽器為SSL/TLS用戶端，Web伺服器則為SSL/TLS伺服器端。當Web的HTTP在SSL/TLS上運作時，稱為HTTPS(HyperText Transfer Protocol Secure)。