《計算機網路》

試題評析	今年檢事官電子資訊組的計算機網路考題，有部份題目屬於較新的網路發展之內容，也有部份試題考到較細部的一些功能，一般電腦網路相關教科書也未必有足夠的說明，因此考生要取得高分恐怕不是很容易。第一、二題是較易取分的題目，但是第一題要注意：互斥或運算後，還必須再取補數，否則無法完全拿分。第二題取分應無困難。第三題考 VoIP 相關的做法，屬於較新的發展。第四題則是考 IPv6 自動組態模式的功能。第五題是 secret key 的身分認證法。第六題是考 IPv6 對各種相關協定影響。估計今年一般考生大致可取得 50 分左右的分數，欲取得更高的分數並不容易。

一、16 位元作 checksum 的 IP 傳輸機制中，若欲傳送如下（以 16 進位表示）之 32 位元資料：
A1　A2　01　02
實際傳送的資料應該為何（以 16 進位表示）？請詳述計算過程。（20 分）

【擬答】
以 16 位爲單位將資料進行位元式的互斥或運算

$$(A1A2)_{16} \oplus (0102)_{16} = (1010000110100010)_2 \oplus (0000000100000010)_2 = (1010000010100000)_2$$

再求其補數(complement)

$$\overline{(1010000010100000)_2} = (0101111101011111)_2$$

二、乙太網路使用何種通訊協定？有何特色？當兩部機器同時傳送資料時，若有碰撞的情形發生，該如何處理？請詳細描述。（20 分）

【擬答】
(一)乙太網路使用 CSMA/CD(Carrier Sense Multiple Access with Collision Detection)的 IEEE802.3 通訊協定，CSMA/CD 是一種自由競爭的協定，每個 station 要傳輸時先偵測線路是否有訊框在傳送，若有訊框在傳送，則持續監聽，若沒有訊框傳送則可以送出自己的訊框，在送出訊框之後，也會持續監聽通道，以確定是否發生碰撞。
(二)發生碰撞時，會取一亂數來決定等候的時槽數，若連續發生碰撞時，則繼續將取亂數的範圍加倍，直到沒有發生碰撞爲止，也就是二進位指數倒退演算法(Binary Exponential Back-off Algorithm)。

三、目前網路電話（Internet telephony）以採用 H．323 協定為主，架設 VoIP 需要什麼設備與步驟？新的標準 SIP 與目前以 H．323 的網路電話在架構上、傳輸訊息格式上與功能上有何異同？（15 分）

【擬答】
(一)H.323 的設備
1.Terminal：包含攝影機、螢幕、麥克風、喇叭等設備，也必需有 video 與 audio 的 code。
2.GateWay：連接 Internet 與電話網路(Telephone Network)。
3.Gatekeeper：The first is address translation services between LAN aliases for terminals and gateways and IP or IPX addresses. The second Gatekeeper function is bandwidth management.負責終端機在 LAN 的名稱與 IP 位址的轉換，以及頻寬管理等功能。
(二)當 PC(終端機)想要與遠處電話通話時，其步驟如下：
1.PC 先找到 LAN 中的 Gatekeeper，此一步驟是以 UDP port 1718 的 broadcast 來進行。
2.當 Gatekeeper 回應 PC 之後，PC 再向 Gatekeeper 註冊。
3.Gatekeeper 同意之後，PC 向 gatekeeper 要求頻寬，gatekeeper 同意之後，就可以進行 call setup。
4.PC 以 TCP 方式送出要求，經由 gatekeeper 轉送到 gateway，以便建立與遠端電話之連線。
5.當連線建立起來，PC 可以透過 gateway 與遠端電話通訊，不用再經過 gatekeeper。
(三)SIP 與 H.323 的異同

	SIP	H.323
架構	使用 User Agent 與一些 servers	使用 gatekeeper 與 gateway
訊息格式	使用 RTP 傳遞訊息、RTCP 做控制	使用 RTP 傳遞訊息、RTCP 做控制
功能	對 video conference 有限制	提供完整的 video conference 的功能

四、在 IPv4 網路中可藉由 DHCP 通訊協定來完成即插即用（Plug & Play）的要求，請問在 IPv6 網路中有什麼機制可以達到此即插即用的功能？如何完成？（15 分）

【擬答】

Ipv6 的主機可以設定成自動組態模式，也就是當主機連接到 Ipv6 網路時，以 multicast 方式發送一個 link-local 的要求，來詢問其所需要的組態設定資訊，路由器收到此一要求之後，會發送 router advertisement 的封包回去給主機，此種 advertisement 封包中，有相關的網路層設定所需的資訊，主機收到此一資訊即可據此設定其網路組態。除此之外，另外也有 DHCPv6 可以使用。

五、請詳細描述當兩個網路使用者以共用之秘密金鑰（shared secret key）進行認證的程序時，兩方需建立何種訊息交換，以確保對方的正確性？（15 分）

【擬答】

使用 shared secret key 進行認證時，雙方使用相同的 secret key，當甲方要求對乙方進行身分驗證時，可以：

(一)產生組隨機訊息，將此一訊息傳給乙方。

(二)乙方將此一訊息，以 secret key 加密後，傳回給甲方。

(三)甲方也將隨機訊息以同一組 secret key 加密。

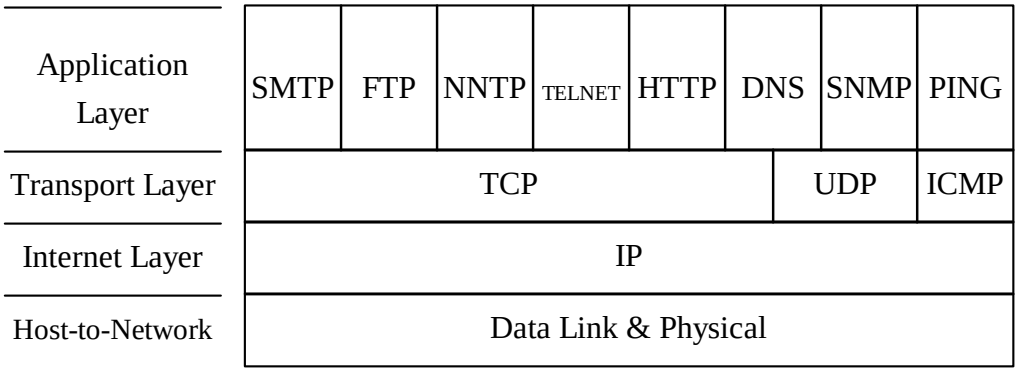
(四)比較乙方送來的密文，是否與甲方自己產生的密文相同。

(五)若相同則表示乙方通過身分認證；否則，就是未通過。

六、描述在 TCP/IP 網路環境進行資料傳輸時，各層通訊協定在資料包裝（如訊框或封包）中的關係？從 IPv4 改變為 IPv6 的過程中，TCP/IP 網路各層通訊協定受到的影響為何？

【擬答】

(一)各層資料包裝的關係如下圖



(二)Ipv4 轉換到 Ipv6 過程中的影響

1.TCP 與 UDP 未改變。

2.ICMP 修改成爲 ICMPv6，其功用與目的相同，只是修改得較適合 Ipv6。

3.ARP 與 IGMP 被合併到 ICMPv6 中；而 RARP 已很少使用，故被棄置。