《計算機網路》

試題評析	本次檢查事務官考試的計算機網路一科，大體而言應屬簡單，唯一值得注意的，是出現了兩題實務題，而且皆與資訊安全有關係。主要在測驗應考者對最近一段時間，所發生的電腦病毒與入侵問題，是否關心並且曾加以了解。 第一題是 CRC 碼的計算題，應考者可以輕易拿到分數。第二題則是乙太網路的最小封包長度計算，觀念清楚者應可計算出結果。第三題實際出自於 ARP 部份之觀念，對 ARP 觀念清楚者，取分很簡單。第四題是測驗應考者對 TCP 的錯誤偵察與復原方法的了解，亦屬於基本問題。第五題題意敘述有些微模糊，如果了解題意，計算上則很簡單。第六題與第七題則是測驗應試者對時事與實務上，網路安全的關心與了解程度，並非網路教科書中，正式的內容。 一般而言，此一科目的考試成績應在50~75之間，時事與實務的了解，對成績好壞的影響應該會很大。

一、有一傳輸系統使用CRC編碼來偵察傳輸錯誤。假設產生多項式(generator polynomial)為 X^5+X^2+1，當資料碼為10011101時，請問處理過的輸出碼為何？當接收端收到資料11100111011時，請問該系統是否會認為傳輸有錯誤？請出示計算過程。（10分）

【擬答】

(一)

M(x)=$x^7+x^4+x^3+x^2+1$

G(x)=x^5+x^2+1

```
          10001000
100101 ) 1001110100000
         100101
            100100
            100101
               01000
```

$$Q(x)=(M(x)\times x^5)\div G(x)=10001000$$

輸出為 $M(x)\times x^5-G(x)\times Q(x)=1001110101000$

(二)

```
          111111
100101 ) 11100111011
         100101
          111001
          100101
           111001
           100101
            111000
            100101
             111011
             100101
              111101
              100101
               11000
```

最後餘數並非全為0，故接收的資料有錯誤。

二、考慮一個一公里長，100Mpbs的以太網路(Ethernet)，其訊號傳遞速度為每微秒（10^{-6}秒）為200公尺。請問封包大小至少要為多少位元組(bytes)才能讓以太網路上工作站(station)偵測到所有的傳輸碰撞(collision)？（12分）

【擬答】

使用 RTT(Round-Trip Time)來計算

$$RTT=\frac{1000m\times 2}{200m/m\sec.}=10m\sec.$$

在RTT 期間必須持續傳送，故封包最小長度為

$$10m\sec.\times 100Mbps=1000bits=125bytes$$

三、假設我們有以太網路如下圖，其網路相關資料如以下表格，Network/Interface**欄位為網卡之位置，例如** Net 1/Host A**代表該網卡在**Host A**上連接到網路**Net 1. IP Address**與**MAC Address**欄位記載該網卡之**IP**與**MAC

地址。

Network/Interface	IP Address	MAC Address
Net 1/ Host A	10.0.0.2	80:12:AE:30:13:2A
Net 1/ Router A	10.0.0.1	80:12:AE:30:13:2B
Net 2/ Router A	10.0.1.1	80:12:AE:30:13:2C
Net 2/ Router B	10.0.1.2	80:12:AE:30:13:2D
Net 3/ Router B	10.0.2.1	80:12:AE:30:13:2E
Net 3/ Host B	10.0.2.3	80:12:AE:30:13:2F

假設路由器A與路由器B(Router A 與Router B)裡有正確與完整IP路由之資料。請回答以下問題。

(一)Host A傳送一個IP封包給10.0.2.3上的主機。請問這封包可否到達？如可，請問10.0.2.3上的主機所收到之封包上的來源IP地址(source IP address)為何？封包上的來源MAC地址(source MAC address)為何？（5分）

(二)Host B傳送一個以太網路封包給80:12:AE:30:13:2D上的主機。請問這封包可否到達？如可，請問80:12:AE:30:13:2D的主機所收到之封包上的來源IP地址為何？封包上的來源MAC地址為何？

(三)Host A傳送一個以太網路封包給80:12:AE:30:13:2B上的主機。請問這封包可否到達？如可，請問80:12:AE:30:13:2B的主機所收到之封包上的來源IP地址為何？封包上的來源MAC地址為何？（5分）

【擬答】

(一)可以到達，source IP address 為 10.0.0.2，source MAC address 為 80:12:AE:30:13:2E。

(二)無法到達。因為 MAC address 80:12:AE:30:13:2D 不在 Net3 segment上，故 Router B 不會接收此一乙太網路封包。

(三)可以到達，source IP address 為 10.0.0.2，source MAC address 為 80:12:AE:30:13:2A。

四、請解釋TCP如何偵察傳輸錯誤(error detection)，以及錯誤復原(error recovery)之程序為何？（15分）

【擬答】

(一)資料傳送時，會進行 error-detection 及要求重送，以保證封包的完整性，因此傳輸資料是 error-free 的。接收端收到封包時，送出 acknowledgement回覆傳送端；資料有錯誤時，也可能會因為傳送端計時器逾時而重傳資料。

(二)每個封包都必須要有序號，以保證資料傳送之順序(sequence)是正確的。傳輸端將訊息切割成一個個封包，並加上序號；接收端會根據序號重新整理封包，然後組合(re-assemble)出正確的訊息。序號也同時被用在回覆訊息(ACK)上，以表明那一個封包已經被正確接收。

(三)錯誤檢查機制是使用 checksum。將 IP 虛擬標頭、TCP 標頭以及傳送之資料(payload)，以 16 bits 為單位，使用 1's complement 加法來加總，最後取 1's complement 以產生檢查和。注意在計算之前，檢查和先預設為 0，等計算後再放入計算所得的檢查和。接收端的檢查方式，則以 16 bits 為單位，使用 1's complement 加法來加總，若計算結果為 0，則表示正確；否則，表示有錯。

五、有一個路由器(Router)的傳送速度為R bps，假設封包長度為L bits。假設每L*N/R秒鐘有N個封包同時到達，請問封包平均等待時間為何？（13分）

【擬答】

同時到達的 N 個封包，第一個被router傳送出去的封包等候時間為 0；第二個被router傳送出去的封包等候時間為 L/R sec.；第三個被router傳送出去的封包等候時間為 2L/R sec.；餘此類推。故平均等候時間為

$$\frac{0+L/R+2L/R+...+(N-1)L/R}{N}=\frac{L(N-1)}{2R}\text{sec.}$$

六、最近微軟視窗系統遭受「疾風網蟲（Blaster worm）」攻擊，試述其成因與防治方法。（15分）

【擬答】

(一)Blaster worm 利用 Microsoft DCOM RPC 介面的缺口，侵入 Microsoft 的 Windows NT 4.0 , Windows 2000, Windows XP, Windows Server 2003 等系統。一旦進入系統後，首先由來源 copy 一份程式 msblast.exe 到該系統，並且執行之。然後，再由此一被感染的系統，繼續 網路上找尋其他可入侵的系統，繼續擴散病毒。

(二)Blaster主要是從缺口 TCP port 135 入侵，因此防治的主要方法有

1.儘早使用 Microsoft 的 patches 來修正作業系統。

2.將 DCOM 相關的 ports 功能關閉，包括 port 135,139,445 等。

3.使用網路設備來過濾封包，例如 router 的 ACL filtering 功能，過濾掉相關的有危險的封包。

4.若已經被入侵的現象，則可用掃毒軟體來清掃；並趕快使用 patches 來修正系統的缺口。

七、請解釋分散式阻斷服務（distributed denial-of-service, DDOS）攻擊的成因與防治方法。（20分）

【擬答】

(一)DDoS 主要是被入侵的機器，在網路上針對某個特定的對象(例如: server 或網路區域)，發送大量的封包，來癱瘓其通訊的管道。如果這種被入侵的系統持續增加，則被攻擊的對象的網路通道，將會完全被攻擊的封包塞滿而遭阻隔。

(二)必須由軟體、硬體及網路設備的廠商，共同針對其產品的缺失加以改進，並提供防範之道。主要困難點在於(1)只要軟體系統存在有入侵的缺口，就有可能有 DDoS 的攻擊發生。(2)網路設備要過濾這類的封包，但是如何能有效分辨封包是否具有攻擊性，抑或只是正常的封包。