《計算機網路》

試題評析	本次的試題大部分都是歷屆考試曾經出過的類似題，主要測驗名詞解釋與操作原理，所以細心同學仔細作答，取得高分並不困難。試題的主題比較分散，從底層到應用層都有，估計用功細心的考生可得 80~90 以上的高分。 第一題：有關防火牆與入侵偵測系統是屬於資訊安全的主題，也是常見的試題，其中特別問到防火牆無法保護的事件，也就是問到防火牆的缺點並寫出改善的方法。 第二題：考 IPv4 位址不足的改善方法，包含 CIDR 與 NAT 的暫時解決性的方案。 第三題：問乙太交換機網路如何建立轉送表，其實原理與橋接器一樣，都是透過學習而來。 第四題：問進行網路連線時需要有哪些步驟？以網際網路瀏覽器連線 web 伺服器爲範例。 第五題：考出四個常見的名詞解釋，只要仔細回答即可。
考點命中	一、《高點電腦網路講義第四回》，許振明編撰，頁 2-6。 二、《高點電腦網路講義第二回》，許振明編撰，頁 33；《高點電腦網路講義第三回》，許振明編撰，頁 39。 三、《高點電腦網路講義第一回》，許振明編撰，頁 121；《高點電腦網路講義第三回》，許振明編撰，頁 3。 四、《高點電腦網路講義第一回》，許振明編撰，頁 19。 五、《高點電腦網路講義第二回》，許振明編撰，頁 27、頁 38、頁 63；《高點電腦網路講義第三回》，許振明編撰，頁 68。

一、請說明防火牆（Firewall）與入侵偵測系統（Intrusion Detection System）在保護網路功能之差異性。請敘述防火牆無法保護的事件，並提出對應的解決方法。（20 分）

【擬答】

(一)使用分封過濾器(Packet Filtering)保護組織，以防備來自網際網路端的非法傳輸。此功能可分成下列三種類型：

1.封包過濾器(Packet Filtering)：操作於路徑選擇器(Router)的程式。檢查主從式架構的 IP 分封，經由 IP 位址、port 及方向來控制資料的傳播，是網路層的防衛機制。

2.連線閘道器(Circuit Gateway)：是屬於連線層(Circuit-Level)的防衛機制，運作原理是本身先與所有內部對外服務的電腦建立連線，並開放這些服務對應的 TCP 連線埠號給外部的使用者。

3.應用閘道器(Application Gateway)：在應用層進行過濾，故能提供比封包過濾器更高的安全性。入侵偵測防系統(Intrusion Detection System)：分析網路或系統上傳輸之資料封包，以偵測是否有入侵或癱瘓服務之攻擊性封包。一般入侵偵測系統包含 3 個功能元件：

(1)資訊來源。

(2)提供一連串的事件記錄。

(3)分析引擎。

(二)防火牆無法保護的事件包含：

1.防火牆無法抵擋繞過防火牆的攻擊：檢查所有進出網路的通道，確認都必須經過防火牆，不能有另外的進出路徑。

2.防火牆對於來自內部的攻擊：增加對內部網路的資訊安全，杜絕非內部人員與非授權的使用者進行非授權的網路操作與使用。

3.防火牆無法防止已經中毒的檔案或程式的通過：進行所有檔案的掃毒與檢查，如有可疑的檔案經過，則進行提醒使用者與追蹤。

二、不分級網路（Classless Inter-Domain Routing，CIDR）和網路位址轉換（Network Address Translation，NAT）都是為了解決 IPv4 的 IP 位址短缺現象而產生，請說明 CIDR 和 NAT 的運作原理。（20 分）

【擬答】

CIDR(Classless Inter Domain Routing)：又稱爲超網路(Supernet)，將數個 Class C 的 IP 網路合併分給使用者使用的方法，以解決 IP 位址不足的問題。CIDR 工作原理如下：

1.將 Class B 網路切割成爲 256 個 Class C 子網路(Subnet)。

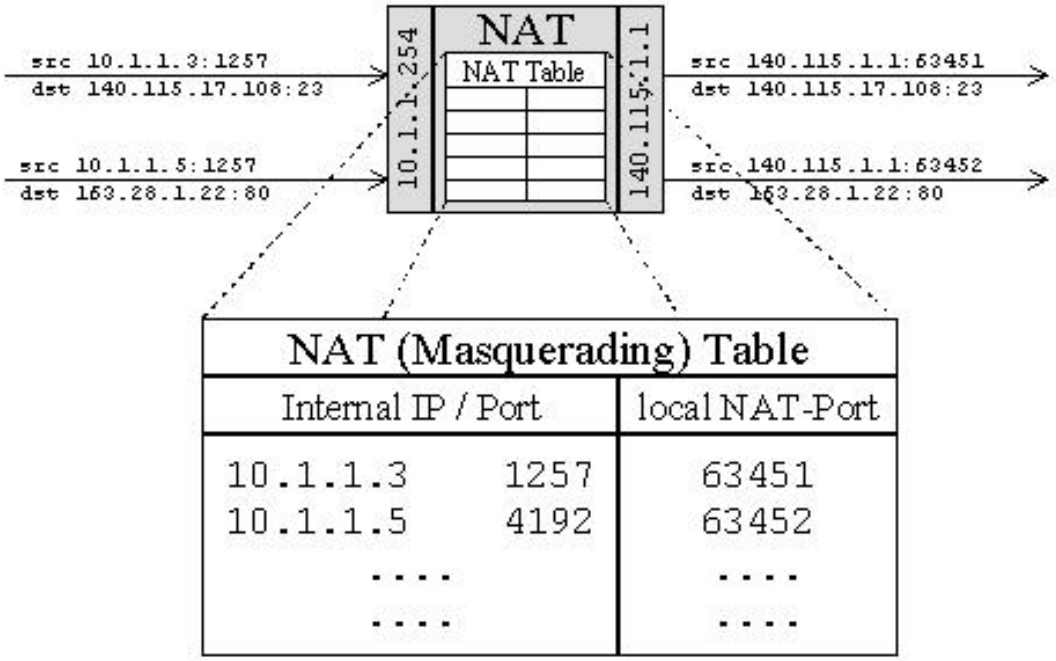
2.將利用 Class C 子網路以 2、4、8、16 等 2 冪次方個數的網路，合併成爲一個網路稱超網路(Supernet)。這樣就可以減少 IP 位址浪費。

NAT(Network Address Translation)：使用多台電腦使用虛擬 IP 共用一個實體 IP 的一種技術。目前業界使用此項技術建置公司內部網路。NAT 的工作原理如下：

步驟 1：來源(Source)電腦將 Virtual Source IP/Source Port 與 Destination IP/Destination Port 送到 NAT Server。

步驟 2：NAT 伺服器建立轉換表紀錄 Virtual Source IP/Source Port 與 Physical Source IP/Source Port。

步驟 3：NAT 伺服器使用 Physical Source IP/Source Port 與 Destination IP/Destination Port 送資料給目的地電腦。



三、乙太網路的連結設備交換器(Switch)的內部需維護一個 Forwarding Table，請先說明 Forwarding Table 的內容為何？交換器如何維護 Forwarding Table 的內容？交換器如何轉送（Forwarding）封包？（20 分）

【擬答】

(一)乙太網路的轉送表(Forwarding Table)內有 MAC 位址與埠號，紀錄由來源埠進入的訊框，根據目的 MAC 位址應傳送出去的目的埠號。例如：

目的 MAC 位址	目的埠號
01:AC:3F:87:AA:B1	3
BC:1C:BB:17:43:C2	4
32:55:72:87:A1:7A	5
00:CA:FF:74:53:11	6

(二)當有訊框出現時，就可以知道此訊框的來源 MAC 位址，因此就可以登錄此 MAC 位址到這個埠號上。這個紀錄法則稱爲學習(Learning)法則。如來源埠號 2 發現一個訊框，來源 MAC 位址是 01:35:7C:BB:AC:DA，

則加入此資料到轉送表：

目的 MAC 位址	目的埠號
01:AC:3F:87:AA:B1	3
BC:1C:BB:17:43:C2	4
32:55:72:87:A1:7A	5
00:CA:FF:74:53:11	6
01:35:7C:BB:AC:DA	2

(三)當有一個訊框到達乙太網路交換機時，則根據目的 MAC 位址查詢轉送表的” 目的 MAC 位址”欄位，由欄位”目的埠號”找出對應輸出的埠號就可進行傳送動作。

四、當使用者利用網頁瀏覽器（Browser）向網頁伺服器（Web Server）讀取 http://www.yahoo.com 網頁時，該使用者的主機將會執行那些步驟才能看到網頁內容？（20 分）

【擬答】

開啓網頁須執行下列步驟：

步驟一：啓動 DNS(Domain Name System) 功能，先將網址 http://www.yahoo.com 傳換成 IP 位址。

步驟二：由瀏覽器啓動 HTTP 協定，接下來開始進行網路通訊的標頭封裝，包含：

1.若有加密的網頁則進行 SSL 的標頭封裝。

2.傳輸層 TCP 標頭封裝。

3.網路層 IP 標頭封裝。

4.資料連結層 CSMA/CD 標頭封裝(假設使用乙太網路)。

步驟三：接下來將封包送出，封包經過 Internet 繞路後到達 web 伺服器。

步驟四：web 伺服器收到封包後開始解封裝。

步驟五：web 伺服器將網頁的 HTML 檔傳回瀏覽器。

步驟六：瀏覽器顯示結果。

五、請說明下列各詞：(每小題 5 分，共 20 分)

(一)交遞（Handover 或 Handoff）

(二)無線射頻辯識系統（RFID）

(三)小型文字檔案（Cookie）

(四)存活時間（Time To Live, TTL）

【擬答】

(一)交遞(Handover 或 Handoff)：當一個移動主機(mobile host)由一個基地台(base station)移動到另一個基地台的傳輸範圍中，必須將在原來基地台上跟手機相關的資訊傳送給新的基地台，以便繼續通訊稱之。

(二)無線射頻身分識別系統(Radio Frequency IDentification System：RFID)：又稱電子標籤，爲一種通信技術，其原理主要利用無線頻率(如：電磁感應、微波等)識別目標並且進行資料的傳輸和讀取相關資訊，無需透過機械或光學接觸。RFID 是一種先進的無線辨識技術，透過商品上的微晶片「標籤」，可將資訊連至電腦網路裡，用以辨別、追蹤與確認商品的狀態。

(三)小型文字檔(Cookie)：Cookie 名稱源自一個 UNIX 的程式「幸運餅」(Fortune Cookie)，它是用於網際網路上確認使用者身分的一小段程式或資料。在網際網路上，一個網頁可由伺服器傳遞給用戶的一段資料，並儲存在用戶的電腦中，當使用者下次再度光臨該網頁時，伺服器就可以比對 Cookie 資料以辨識使用者的身分，而伺服器傳送的 Cookie 每次都不同，就好像隨機所產生的亂數一樣，故以具有相同運氣成份的 Fortune Cookie 命名之。

(四)存活時間(Time To Live，TTL)：封包在 IP 網路上的存活時間。在許多網路協定中都會碰到。當一個封包被賦予 TTL 值(以秒或跳站數目(hop)爲單位)，之後就會進行倒數計時。在 IP 協定中，TTL 是以 hop 爲單位，每經過一個 router 就減一)，如果封包 TTL 值被降爲 0 的時候，就會被丟棄。這樣，當封包在傳遞過程中由於某些原因而未能抵達目的地的時候，就可以避免其一直充斥在網路上面。