國立交通大學

理學院科技與數位學習學程

碩士論文

結合身分認證之校園 IP 管理系統

Campus Ip Administration System based on POP3 Authentication

研 究 生：戴興能

指導教授：蔡文能　教授

中華民國　九十九　年六月

結合身分認證之校園 IP 管理系統

Campus Ip Administration System based on POP3 Authentication

研 究 生：戴興能　　Student：Hsin-Nung Dai

指導教授：蔡文能　　Advisor：Wen-Nung Tsai

國 立 交 通 大 學

理學院科技與數位學習學程

碩 士 論 文

A Thesis

Submitted to Degree Program of E-Learning

College of Science

National Chiao Tung University

in partial Fulfillment of the Requirements

for the Degree of

Master

in

Degree Program of E-Learning

June 2010

Hsinchu, Taiwan, Republic of China

中華民國九十九年六月

結合身分認證之校園 IP 管理系統

學生：戴興能　　指導教授：蔡文能

國立交通大學理學院碩士在職專班科技與數位學習學程

摘　要

網管人員管理校園 IP 位址，通常必須例行性以人工方式去盤查並記錄每部電腦的 IP 供日後使用，然而，使用者可能修改電腦的 IP 設定或帶筆記型電腦到校連接網路，造成網管人員手中的 IP 列表不是最新的；如果使用者濫用網路或中了會做網路攻擊的電腦病毒而造成網路問題時，IP 位址列表可以幫助網管人員在第一時間知道是哪部電腦有問題，以便在最快的時間內恢復網路的暢通，如果 IP 列表有誤或缺少，網管人員又得頭痛，必須將有可能出問題的電腦一部一部查起，費時又費力。

本研究將針對以上問題，提出一種以網頁為基礎，且能結合身分認證之校園 IP 管理系統，讓每部電腦要使用 Internet 時，都受到管控與申請，並在申請後記錄和綁定使用者帳號、電腦 IP 位址和與網路卡的 MAC 位址，日後如果遇到有問題的電腦時，可以快速的切斷該部電腦對外連線，讓網路保持暢通。

本實作是以學校現有的設備下，使用自由軟體與自行設計開發的程式，提供網管人員使用驗證本機制的可行性，實作的結果顯示本系統可以快速管控校園電腦 Internet 的使用權，確保網路的暢通。

關鍵字：網管人員、驗證、註冊、電腦病毒、網路攻擊、自由軟體

Campus Ip Administration System based on POP3 Authentication

Students：Hsin-Nung Dai　　Advisor：Wen-Nung Tsai

Degree Program of E-Learning
College of Science
National Chiao Tung University

ABSTRACT

The administrators of campus network usually have to manually check and record computer IP addresses for every computer for future use. However, the users might change the settings of the computer IP address and use their own laptop in the campus. This could result in the difference between the actual IP address in use and the existing IP address list hold by network administrators. The correct IP lists hold by the administrators are important when there is an abuse of the Internet by a user or when there is an infection of computer virus on a computer which might launch network attacks. An administrator can use the IP list to identify which computer causes the network problem and thus can fix it quickly.

In this study, we proposed a web-based solution for network IP management with user identity authentication. The system developed in this study records user ID, the IP address for that ID, as well as the MAC address after user registration. This can reduces the reaction time to cut off the connection for certain problematic computer when the above mentioned situation occurs on the network.

In addition to our self-developed programs, our implemention of the proposed system utilized the existing school facilities, and as well as the open source free software. The experimental results show that the system can effectively control the access of the network in the campus netwok environment and thus it can be used to help network administrators doing the management works.

Keywords：network administrator、Authentication、registration、computer virus、network attack、open source

誌　謝

這篇論文能夠順利完成首先要感謝蔡文能老師的諄諄教誨，在蔡老師細心的指導、啟發與幫助下，讓我在研究的過程中學到了嚴謹的研究方法和正確的學習態度，令我受益匪淺，在此由衷的感謝。

其次感謝同學與朋友們：瑛旗、建德、裕峰、佳倫、翎吟，因為在寫論文這一年，有你們提供我不少協助和幫忙，論文才能如期付梓。

最後，特別感謝我的另一半智善，謝謝妳對我的支持與包容，辛苦的照料寶寶讓我無後顧之憂地完成學業，也在我最無助的時候給予我鼓勵，讓我燃起希望勇往直前，感謝妳無怨無悔的陪我渡過求學生涯。

目　錄

表目錄

圖目錄

第一章 緒論

隨著網路資訊普及，電腦價格便宜，學校購置電腦數量愈多，網管人員在管理時就愈繁雜，大部分的校園電腦的 IP 取得多數是由 DHCP Server [1]分配或是由網管人員設定，如果網管人員不知哪個 IP 是由哪一部電腦所使用，一旦某部電腦濫用網路資源或中了會攻擊遠端電腦的病毒，而造成校園網路癱瘓，網管人員雖可以利用網路監聽軟體找出是哪個 IP 有問題，但卻不知是那個 IP 是哪一部電腦所用，只能一部一部的慢慢找，等找到那部電腦後，再進行問題的解決。

然而，網管人員如果花時間用人工作業將電腦 IP 與使用者做成對應列表，以防日後有問題時可以及時依該表找出有問題的電腦，但常常使用者會亂更改電腦的 IP 或自行帶筆記型電腦到校使用，造成網管人員的電腦 IP 與使用者的對應列表不正確不是最新的，而發生問題時，找不到有問題的電腦或是誰用的，網管人員也只好依有可能的電腦一部一部找起，費時又費力。

如果校園電腦要使用 Internet 時，必須填寫使用者、電腦 IP 和網路卡的 MAC 進行申請，等待申請核可，系統將電腦 IP 和網路卡的 MAC 進行綁定後，使用者才有 Internet 的使用權，這樣網管人員就有及時的電腦 IP 與使用者的對應列表供日後使用。本實作以學校現有的設備及自由軟體，並自行設計程式以網頁的方式進行 Internet 使用權申請，達成全面自動化的管理。

1.1 研究動機

隨著電腦普及化，電腦愈多，網管人員在管理電腦 IP 與網路的工作就愈重，現在各學校幾乎都是班班有電腦，中型學校的電腦總數約有 100 部，大型學校則約 200 部，在電腦數量眾多的環境想人工管理電腦 IP 將是一件很繁雜的工作，除了要求使用者別亂改網路設定之外，網管人員也要定期將電腦 IP 與使用者對應做成列表以供日後使用。

當使用者濫用網路造成校園網路癱瘓時，網管人員除了利用網路監聽軟體找出有問題的 IP 之外，還要利用 IP 列表找出是哪一部電腦，然後才可以及時去做適當的處理，如果該 IP 列表都是正確無誤的話，那網管人員一切的辛苦是值得的，而如果該 IP 列表不正確不是最新的，無法查出有問題的 IP 是哪一部電腦，那網管人員除了頭痛之外，又得再花時間去找有問題的 IP 可能是哪一部電腦，就無法及時恢復網路的通暢。

我們希望不更動現有的網路系統環境下，使用開放軟體讓使用者連上 Internet 之

前透過網頁申請註冊電腦 IP 與網路卡的 MAC 值，如此網管人員就可以即時線上得知正確最新的電腦 IP 與使用者對應列表，遇到問題需要查哪個 IP 是哪一部電腦所有時，也不會因為是舊的對應列表而找錯，亦可以線上及時將該部電腦中斷對外連線，使校園網路快速恢復通暢。然而，運行此架構並不會增加學校的經費預算，網管人員可以設定使用者申請註冊的時間（如半年一次），所以這期間使用者並不會更改上網使用經驗，而達到結合身分認證之 IP 管理系統的功能。

1.2 研究目的

本研究之目的為利用現有的硬體設備，在不改變使用者環境、不額外增加費用的考量下，提出一個適用於國中小結合身分認證之校園 IP 管理系統的架構。本系統架構預期可達到之功能如下：

1、自動導向網頁申請介面：

使用者在尚未註冊的電腦使用 Internet 時，網頁會自動導向申請介面讓使用者快速申請註冊網路使用權。

2、自動抓取電腦 IP 與網路卡的 MAC 值：

由於使用者的電腦程度不同，為了避免申請註冊時的難度，本系統會在申請註冊頁面，自動抓取使用者的電腦 IP 與網路卡的 MAC 值，使用者只需填寫此部電腦所在位置或使用單位即可，簡化申請的步驟。在申請註冊後，本系統會將電腦 IP 與網路卡的 MAC 進行綁定，如果使用者亂改電腦 IP 也無法正常連線成功。

3、已註冊的電腦，可正常使用 Internet 權：

如果使用者已為電腦申請註冊成功，約 3 秒後就可以正常使用 Internet，完全不用改變或重新教育上網習慣。

4、及時的電腦 IP 對應列表：

網管人員可以在網頁介面即時查看電腦 IP 對應列表，不必擔心列表資訊不正確擔誤處理時間。

5、可中斷有問題電腦的連線：

網管人員可以在網頁介面中斷有問題電腦的 Internet 使用權，先恢復網路的通暢，再行前往處理。

希望透過此系統所提供的功能，來簡化網管人員的負擔，加速解決問題的速度。最後，我們也將根據此一系統架構進行實作，來證明此一架構的可行性。

1.3 研究範圍

本研究設定在國中小校園網路，以網管人員管理電腦IP作業作為研究對象。另因為中小學經費普遍不足，為了不增加額外的費用，故本文實作之系統，採用開放原始碼（Open Source）的作業系統（FreeBSD）[2]、伺服器軟體（Apache）[3]、伺服器端網頁程式語言（PHP）[4]及資料庫伺服器（MySQL）[5]來設計結合身分認證之校園IP管理系統。由於人工記錄電腦IP與使用者列表費時費力，所以本研究使用FreeBSD內建防火牆(IPFW)[6]來管理使用者的Internet使用權，並用網頁的方式進行申請達到全自動的IP管理機制。

1.4 章節介紹

本論文共分六章節，第一章為研究動機與目的，第二章介紹相關背景知識，包括TCP/IP基本概念、動態主機設定協定(DHCP)、IPFIREWALL（IPFW)、地址解析協議(ARP)與網路連線使用權的管制等。第三章將對各學者所提IP管理的方法分析比較，分成 L2 Switch 管制網路使用權和防火牆管制網路使用權等方式。第四章為我們所提出的結合身分認證之校園IP管理系統架構。第五章則對本研究所提的方法設計、實作，並對系統做評估分析。最後，在第六章中依據先前章節所介紹之技術或系統，與本系統做比較分析，並對本研究做結論與未來的研究方向。

第二章 背景知識

本章節主要介紹及說明本論文主題相關的理論與技術，其內容包括 TCP/IP 基本概念；動態主機設定協定(DHCP, Dynamic Host Configuration Protocol)伺服器的介紹；使用 IPFIREWALL (IPFW) 防火牆管控校園網路內電腦對外連線等介紹；電腦 IP 與網路卡的 MAC 的 Address Resolution Protocol (ARP, 地址解析協議)介紹，最後，談及網路連線使用權的管制。

2.1 TCP/IP 基本概念

TCP/IP(Transmission Control Protocol/Internet Protocol)[7] [8] 是目前網際網路(Internet)應用最廣泛的協定，其模型共分為四層，由上而下分別為：應用層、傳輸層、網際網路層、連結層，是由文頓·格雷·瑟夫（Vinton Gray Cerf）與羅伯特·埃利奧特·卡恩（Robert Elliot Kahn）所開發出來的，取代了舊的網路控制協定（NCP, Network Control Protocol），也戰勝了由國際標準組織(International Organization for Standardization, ISO)所制定的 OSI模型(Open System Interconnection Reference Model)[9]，其模型共分為七層，由上而下分別為：應用層、展示層、會議層、傳輸層、網路層、資料連結層、實體層。

圖2-1為 OSI 七層及模型 TCP/IP 四層模型之大致對照，以下就TCP/IP四層之功能與任務簡介：

1、應用層：此層包含各種應用程式的資料通訊協定，常見的協定如 HTTP、FTP、SMTP、SSH、DNS等。

2、傳輸層：此層定義了資料傳遞的方法，解決了傳輸的可靠性和保證資料的順序性問題，可分為TCP和UDP協定，說明如下：

(1)TCP（Transmission Control Protocol：TCP是一種一問一答的可靠性傳輸協定，提供一種資料錯誤檢查功能保證資料的完整並無損且按順序的送達。

(2)UDP（User Datagram Protocol）：UDP是一種不問答的不可靠傳輸協定，其傳輸不檢查資料是否已到達目的地，允許資料遺失，也不保證這些資料是按順序到達的。如音頻和視頻的串流媒體(MMS)，在傳輸資料發生遺漏時，並不會有太大影響，又資料按時送達比起資料的可靠性更重要，所以才會使用UDP協定。

3、網際網路層：定義了Internet protocol（IP)、Internet Control Message Protocol（ICMP)、Internet Group Management Protocol（IGMP)等協定，也

定義了路由（Routing）協定，讓不同網域的資料可以交換。

4、連結層：此層知道底層網路的細節，定義了如何透過網路來傳送 IP 資料段，主要的功能是將資料從一個網路設備傳輸到另外一個網路設備。其底層網路包含了乙太網路（Ethernet）、光纖分散式數據介面（Fiber Distributed Data Interface, FDDI）、無線區域網路（Wireless LAN, WLAN）等。

<table>
<tr><th>Layer</th><th>OSI 七層模型</th><th colspan="2">協定</th><th>TCP/IP 四層模型</th></tr>
<tr><td>7</td><td>應用層
Application Layer</td><td rowspan="3">HTTP
FTP
SMTP
SSH</td><td rowspan="3">DNS
MMS</td><td rowspan="3">應用層
Application Layer</td></tr>
<tr><td>6</td><td>展示層
Presentation Layer</td></tr>
<tr><td>5</td><td>會議層
Session Layer</td></tr>
<tr><td>4</td><td>傳輸層
Transport Layer</td><td>TCP</td><td>UDP</td><td>傳輸層
Transport Layer</td></tr>
<tr><td rowspan="2">3</td><td rowspan="2">網路層
Network Layer</td><td colspan="2">IP, ICMP</td><td>網際網路層
Internet Layer</td></tr>
<tr><td colspan="2">ARP, RARP</td><td rowspan="2">連結層
Link Layer</td></tr>
<tr><td>2</td><td>資料連結層
Data Link Layer</td><td colspan="2" rowspan="2">Ethernet
FDDI
WLAN</td></tr>
<tr><td>1</td><td>實體層
Physical Layer</td></tr>
</table>

圖 2 - 1 OSI 與 TCP/IP 模型之大致對照

2.2 動態主機設定協定(DHCP)

一部電腦要能連上網路，在電腦中必須設定 IP 位址(IP Address)、子網路遮罩(Netmask)、通訊閘(Gateway)、DNS(Domain Name System, 領域名稱系統) 等，如果管網人員管理的電腦數量眾多，每一部電腦又得去手動設定，一方便容易設定錯誤，另一方面，如果日後要進行 IP 重新規劃就會增加管理的負擔。而 DHCP Server 可以讓網路中的電腦自動取得 IP 位址和相關設定，大幅減少網管人員的工作量，也讓使用者很方便就能上網。DHCP [10] [1](Dynamic Host Configuration Protocol)其前身是 BOOTP（Bootstrap Protocol）。因 BOOTP 不支援動態 IP 位址指派，當一個 IP 位址被指派出去後，就無法收回再提供給其他電腦使用，後來才有 DHCP 的產生，又 DHCP 廣為大家所用，所以 BOOTP 被 DHCP 所取代。

DHCP 系統運作是採用 client-server 模式，所以 Client 端電腦在未取得 IP 時，會發送 DHCPDISCOVER 廣播訊息，等待 DHCP Server 發出的 DHCPOFFER 回應，當 Client 端電腦收到 DHCP Server 回應後，即發出 DHCPREQUEST 廣播訊息給所有 DHCP Server 告知選擇了那個 DHCP Server，最後 DHCP Server 則傳送 DHCPACK 訊息給 Client 端的電腦，完成 IP 租約。

DHCP 之訊息傳遞方式如圖 2-2 所示：

1、請求 IP 租約：當 Client 端電腦的網路設定為自動取得 IP 時，會以廣播的方式發送 DHCPDISCOVER 訊息到網路上尋找可用的 DHCP Server。

2、提供 IP 租約：當 DHCP Server 收到一個來自 Client 端電腦的 IP 請求時，它會為 Client 端電腦保留一個 IP 位址，然後發送一個 DHCPOFFER 訊息給 Client 端電腦，此訊息包含了 DHCP Server 所提供的 IP 位址、提供 IP 的 DHCP Server 的 IP、Network Mask 和租期等相關資訊。

3、選擇 IP 租約：當 Client 端電腦會接受最先收到的 DHCPOFFER 訊息，然後會以廣播的方式發送一個 DHCPREQUEST 訊息給所有 DHCP Server，告知是選擇了哪個 DHCP Server 的租約，而未選中的其他 DHCP Server 將會回收之前保留的 IP 重新等待其他電腦來申請租約。

4、確認 IP 租約：當 DHCP Server 收到 Client 端電腦的 DHCPREQUEST 訊息後，則會送出 DHCPACK 訊息回應 Client 端電腦做確認，此訊息包含了與 DHCPOFFER 訊息所提供的資訊。

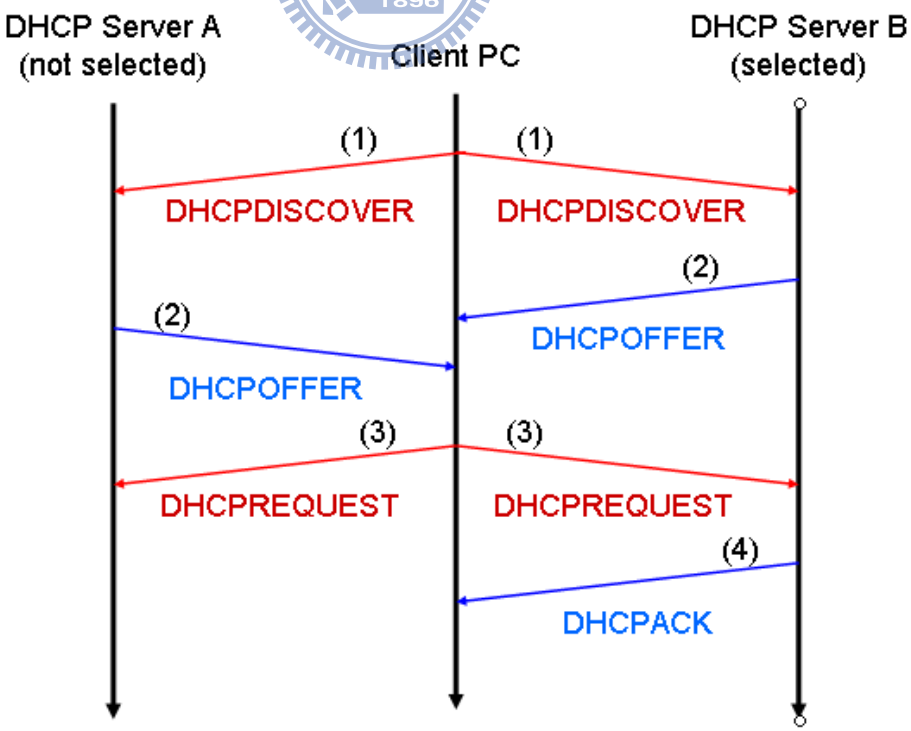

圖 2 - 2 DHCP 訊息傳遞方式

DHCP 有三種指派 IP 位址的方法：

1、自動分配(automatic allocation)：當 Client 端電腦向 DHCP Server 取得 IP 位址後，此 IP 位址就永久分配給該部電腦。

2、動態分配(dynamic allocation)：當 Client 端電腦向 DHCP Server 取得 IP 位址後，此 IP 位址並非永久分配給該部電腦，而是有租約期限，當期限過了，Client 端電腦必須釋放該 IP 位址給其他電腦使用，當然，Client 端電腦亦可延續租約或租用其他 IP 位址。

3、手動分配(manual allocation)：Client 端電腦的 IP 位址是由網管人員手動在設定檔中依 MAC 位址指定分配。

一般 DHCP Server 都是用動態分配(dynamic allocation)的方式指派 IP 位址，因為此方法很方便，不用一直在 Client 端電腦或 DHCP Server 去做設定。

DHCP Server 的設定檔[11] 通常為 dhcpd.conf，下表 2-1 為其設定項目簡介：

項目	說明
option domain-name	設定網域名稱。
option domain-name-servers	設定 DNS 伺服器 IP 位址。
option subnet-mask	設定給 client 電腦的預設子網路遮罩。
option broadcast-address	設定給 client 電腦的預設廣播位址。
option time-offset	設定本地時間和格林威治時間差幾秒。
default-lease-time	設定預設租期(秒)。租約到期後，伺服器會回收該 IP 位址。
max-lease-time	設定續租最長可以被使用多久(秒)。當租約到期後，Client 端電腦可以要求使用同一個 IP 位址續租。
ddns-update-style	設定是否支援 ddns 更新 IP 位址。
subnet	設定子網路與網路遮罩，如： subnet 192.168.1.0 netmask 255.255.255.0 { range dynamic-bootp 192.168.1.20 192.168.1.200; option routers 192.168.1.1; }
Host	設定電腦的網路卡 MAC 位址要使用固定 IP 位址，如：host pc001 { hardware ethernet 00:11:8B:1A:F2:D8; fixed-address 192.168.1.19; }

表 2 - 1 dhcpd.conf 設定簡介

2.3 IPFW 簡介

IPFW (IPFIREWALL)[6] 是 FreeBSD [2]內建的防火牆軟體，可以管理網路封包的進出，其工作就像學校門口的警衛管理人員之進出。而 FreeBSD 則是一套開放軟體的作業系統，通常用來當作網路伺服器使用。

IPFW 是由七個元件組成，其功能有：

1、防火牆過濾規則處理器(kernel firewall filter rule processor)和其整合的封包計數(its integrated packet accounting)功能。

2、紀錄(logging)功能。

3、與 NAT 結合的導向規則(divert rule which triggers the NAT)和進階的特殊目(advanced special purpose)功能。

4、流量控管(dummynet traffic shaper)功能。

5、fwd 規則轉向(fwd rule forward)功能。

6、橋接(bridge)功能。

7、隱藏防火牆(ipstealth)功能。

IPFW 的基本指令[11]如下：

ipfw -f flush：不提出詢問，清除所有規則。

ipfw list：列出目前使用的所有規則。

ipfw add [rule]：增加一條規則。

ipfw delete [number]：刪除編號為 number 的規則。

IPFW 的基本規則如下([ ] 包起來的表示可有可無)：

CMD [RULE_NUMBER] ACTION [LOGGING] SELECTION

CMD：使用 add 來增加一條規則。

RULE_NUMBER：IPFW 會依照數字從小到大的順序執行。如未設定，系統會依每一行的排列順序自動分配編號。

LOGGING：使用 log 來將符合此條規則封包記錄在 /var/log/security 中。

ACTION：如表 2-2 說明。

命令	說明
allow	符合此條規則就允許通過，並停止執行後面其他規則。相同於 accept, pass, permit。
check-state	檢查封包是否符合動態規則，如果符合，則執行所指定的動作並生成動態規則。 如果沒有 check-state 規則，則會在第一個 keep-state 或 limit 規則處，對動態規則表實施檢查。
Deny	符合此條規則就拒絕通過，並停止執行後面其他規則。相同於 drop。
divert port	將符合 divert sock 的封包轉向到指定的 port。
fwd ipaddr[,port]	將符合規則封包的轉向到 ipaddr 去，如果沒有設定 port，則會依原來的 port 進行轉向。
Pipe pipe_nr	傳遞封包給 pipe 用以限制頻寬，而 pipe_nr 是指 pipe 規則的編號。基本語法先將設定頻寬的規則加入： ipfw add pipe pipe_nr ... 再設定該規則的頻寬： ipfw pipe pipe_nr config bw B queue Q 其中，B 是指頻寬，可用 KBytes/s 或 MBytes/s 等表示。Q 是 queue size 的大小，單位為 Bytes。
skipto rule number	當符合規則條件時，就跳至 rule number 規則去。

表 2 - 2 IPFW ACTION 命令

SELECTION：protocol from src to dst [interface_spec] [option]

其中 protocol 是網路協定的名稱，如果使用 ip 或 all 表示所有協定，可使用的選項有 ip, all, udp, tcp, icmp 等。而 src 是封包來源，dst 是封包目的地，這兩個項目可使用的選項有 any, me, 或是以 address/mask [ports] 的方式明確指定位址及 port。

interface_spec 表示要指定的網路介面及流入或流出的網路封包，如下表 2-3。

關鍵字	說明
In	符合流入的封包。
Out	符合流出的封包。
via IF	表示封包一定要經過網路介面 IF 代號。

表 2 - 3 IPFW interface 關鍵字

options：如下表 2-4 說明。

選項名稱	說明
setup	當封包中有 SYN bits 而沒有 ACK bit 時就符合。只適用於 TCP 封包。
Keep-state	當符合規則時，ipfw 會建立一個動態規則，預設是讓符合規則的來源及目的，若使用相同的協定時就讓封包通過。
established	當封包中有 RST bits 或 ACK bits 時就符合。只適用於 TCP 封包。
limit {src-addr | src-port | dst-addr | dst-port} number	限定符合規則條件的最大連線數。 limit 和 keep-state 不能在同一規則中同時使用。

表 2 - 4 IPFW OPTION 關鍵字

以下為一些規則的範例：

```
# 不列出回應也不提出詢問的清除所有規則
 ipfw -q -f flush
# 只允許內部網路對 192.168.0.1 使用 telnet 服務
 ipfw add 1000 allow tcp from 192.168.0.0/24 to 192.168.0.1 23
# 拒絕連到 port 23，並記錄嘗試連線的 IP
 ipfw add 2000 deny log tcp from any to me 23
# 限制內部網域對外下載最大頻寬為 200KBytes/s，上傳最大頻寬為 50KBytes/s
 ipfw pipe 10 config bw 200KBytes/s
 ipfw add pipe 10 ip from any to 192.168.0.0/24 out
 ipfw pipe 20 config bw 50KBytes/s
 ipfw add pipe 20 ip from 192.168.0.0/24 to any in
# 拒絕任何 ICMP 封包
 ipfw add 400 deny icmp from any to any
# 拒絕所有連線
 ipfw add 65535 deny all from any to any
```

2.4 地址解析協議(ARP)

ARP(Address Resolution Protocol)[12][13] 中文叫地址解析協定，其基本功能為透過目標設備的 IP 位址，查詢目標設備的 MAC 地址，以確保通信的順利進行。

在同一區域網路中要讓不同類型的網路硬體進行溝通,就需要建立一些標準協定讓大家共同參考，而乙太網(Ethernet)就是目前最常用的協定，其在邏輯上的傳送是使用了 CSMA/CD (Carrier Sense Multiple Access/Collision Detect 即帶衝突檢測的載波監聽多路存取)技術，此技術會將封包在整個區域網路中進行廣播，就像廣播節目一樣，一個人說，大家都聽得到，所以每個節點都會收到封包，只有目的位址符合自己實體位址(Media Access Control, MAC) 的封包才會被接收下來。而在不同區域網路中，如 Internet，則是使用 TCP/IP(Transmission Control Protocol/Internet Protocol)進行封包傳送，此協定是透過硬體的 IP 位址進行溝通。

問題來了，在同一區域網路中，乙太網路協定是利用 MAC 位址進行溝通，而在不同區域網路中，TCP/IP 協定則是利用 IP 位址進行溝通，這兩者應如何轉換？這就是 ARP 要做的事，將目標 IP 位址轉換成目標 MAC 地址。在 Internet 進行資料傳送時，其封包只包含了目的主機的 IP 位址，一旦封包進入到區域網路內，就需透過 ARP 根據目的主機的 IP 位址，獲得其 MAC 位址，這樣才能將資料傳送至目的地。

在 FreeBSD 或 Linux 中，可使用 ifconfig 指令查看自己的 IP 位址與 MAC 位址，而在 WindowsXP 中，則可使用 ipconfig /all 指令取得，畫面如圖 2-3：

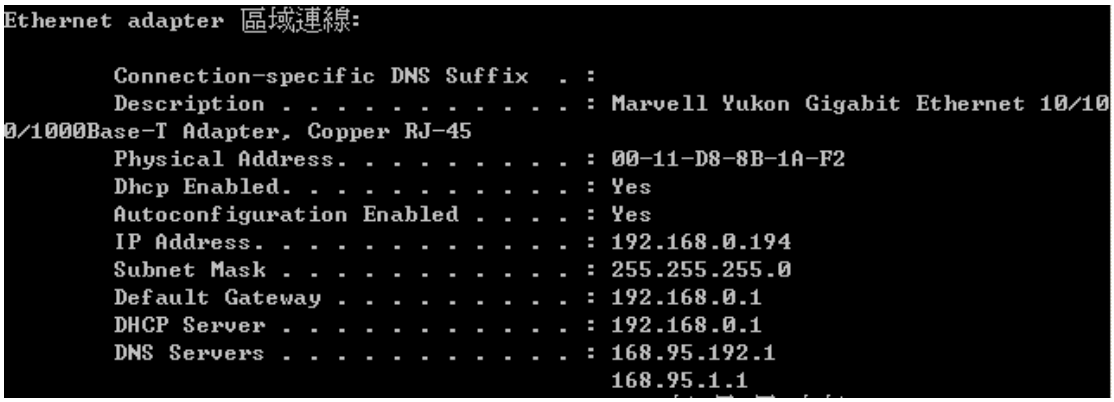

圖 2 - 3 ipconfig 查看 IP 位址畫面

ARP 是利用乙太網的廣播性質，設計出來的位址解析協定。它的主要特性和優點是它的位址對應關係是動態的，所以必須使用查詢的方式來獲得 IP 位址和實體位址的對應。在每部電腦或路由器裡都有一個 ARP Table 存在 ARP 快取緩衝區 (ARP Cache)中，此 ARP Table 裡的 IP 位址與 MAC 位址是對應的，如下表 2-5 所示。

主機名稱	IP 位址	MAC 位址
pc001	192.168.0.194	00-11-D8-8B-1A-F2
pc002	192.168.0.195	00-22-C7-7A-2B-A4
pc003	192.168.0.196	00-33-B6-6D-3C-C5
...	...	...

表 2 - 5 ARP Table 裡的 IP 位址與 MAC 位址表

以主機 pc001（192.168.0.194）向主機 pc002（192.168.0.195）傳送資料為例，說明其工作原理[14]：

1、首先，ARP 快取緩衝區是採用了老化機制，裡頭的每一筆資料在一段時間內沒有使用時，會根據自身的存活時間遞減而刪除，以確保資料的真實性和減少 ARP 快取緩衝區的長度，加快查詢速度。

2、當主機 pc001 傳送資料給主機 pc002 時，會獲得目的主機 pc002 的 IP 位址，此時主機 pc001 會在自己的 ARP 快取緩衝區中檢查是否有主機 pc002 的 MAC 位址，如果找到了，也就知道主機 pc002 的 MAC 位址為「00-22-C7-7A-2B-A4」，就直接使用此 MAC 位址來傳送資料。

3、如果主機 pc001 的 ARP 快取緩衝區中沒有主機 pc002 的 MAC 位址時，主機 pc001 就會發送一個目的 MAC 位址是「FF-FF-FF-FF-FF-FF」的 ARP Request 廣播封包，查詢目的主機 pc002 的 MAC 位址，這表示主機 pc001 向同一區域網路內的所有主機發出這樣的詢問：「192.168.0.195 的 MAC 位址是什麼？」如圖 2-4。

4、此時，同一區域網路內的所有主機都會收到這個 ARP 廣播詢問，都會檢查此封包查詢的 IP 位址是不是自己的，如果不是則忽略。如果是，也就是主機 pc002 接收到此 ARP 詢問封包時，會先將主機 pc001 的 MAC 位址和 IP 位址資料加到自己的 ARP 快取緩衝區中，如果已經有主機 pc001 的資料，就會用新的資料覆蓋原來的，然後才會向主機 pc001 送出回應(ARP Reply)：「192.168.0.195 的 MAC 位址是 00-22-C7-7A-2B-A4」如圖 2-5。

5、這樣，主機 pc001 就知道了主機 pc002 的 MAC 位址，就可以向主機 pc002 發送資料了。同時，主機 pc001 也更新了自己的 ARP 快取緩衝區，如果下次要再送資料給主機 pc002 時，就可以直接從自己的 ARP 快取緩衝區中找到主機 pc002 的 MAC 位址進行傳送了。

6、如果主機 pc001 沒有收到 ARP Reply，則宣告查詢失敗，無法傳送資料。

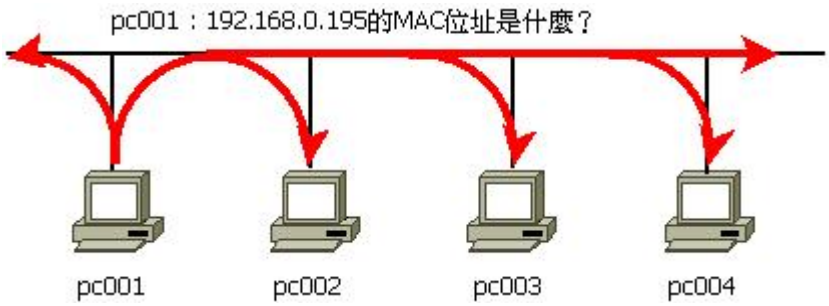

圖 2 - 4 ARP Request

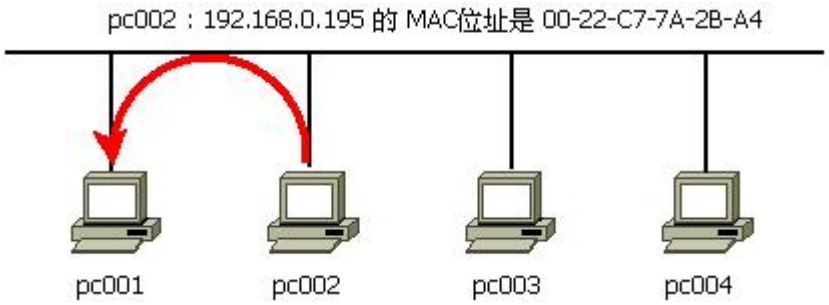

圖 2 - 5 ARP Reply

在 FreeBSD，Linux 或 WindowsXP 中，都可以使用 arp -a 指令查看自己的 ARP 快取緩衝區，如圖 2-6 為 FreeBSD 中所查看到的：

```
nat_server (192.168.0.1) at 00:0E:2E:33:55:81 on rl0 permanent [ethernet]
pc001 (192.168.0.194) at 00:11:D8:8B:1A:F2 on msk0 [ethernet]
pc002 (192.168.0.195) at 00:22:C7:7A:2B:A4 on vr0 [ethernet]
pc003 (192.168.0.196) at 00:33:B6:6D:3C:C5 on bge0 [ethernet]
for:dhcp (255.255.255.255) at ff:ff:ff:ff:ff:ff on rl0 permanent [ethernet]
```

圖 2 - 6 查看自己的 ARP 快取緩衝區

一般來說，MAC 位址是跟隨著硬體設備的不能更改，但 IP 位址可以任意更改。因為網路服務所使用的都是以 IP 位址為主，所以管理者一定要知道某個 IP 位址是被哪部電腦所使用，亦希望使用者不要私自更改 IP 位址，我們可以為每部電腦的 IP 位址與 MAC 位址做靜態的綁定。

2.4.1 使用 DHCP 伺服器綁定 IP 與 MAC

為了使 Client 電腦的 IP 位址能夠固定，可以使用 DHCP Server 進行 IP 位址和 MAC 位址綁定。一般 DHCP Server 可以設手動分配(manual allocation)固定 IP 位址給 Client 電腦使用，在設定檔中設定每部電腦的 MAC 位址及其固定的 IP 位址，這樣 Client 電腦在向 DHCP Server 取得 IP 位址時，就會依設定檔的設定來給固定的 IP 位址。然而，此種方法無法真正將 IP 位址和 MAC 位址進行綁定，因為 Client 電腦取得 IP 位址後，如果使用者私自將其 IP 位址更改時，此部電腦依然可以正常使用網路，不受此機制的管控。

2.4.2 使用 Switch 或無線基地台綁定 IP 與 MAC

為了使 Client 電腦的 IP 位址能夠固定，可以使用 Layer 3 Switch (交換器)[15]或 AP(Access Point)進行 IP 位址和 MAC 位址綁定(binding)。各家的 Switch 或 AP(無線基地台)設定不同，有的只支援使用指令的 SNMP 協定，有的則可以使用較親和力的瀏覽器介面進行設定，如將 Client 電腦的 IP 位址和 MAC 位址進行綁定後，IP 位址和 MAC 位址一定要符合才可能通行，如果使用者亂改 IP 位址，則無法進行連線，當然，改回原先的 IP 位址時，就恢復通行，因此可達成電腦固定 IP 位址的管控機制。此種方式亦是將 IP 位址和 MAC 位址寫入 ARP Table 中，讓此表資料成為靜態固定的。

2.5 網路連線使用權的管制

網路連線使用權的管制在此介紹鎖定網卡 MAC 位址的網路管制和使用 Captive Portal 機制的網路管制。

2.5.1 鎖定網卡 MAC 位址的網路管制

鎖定網卡 MAC 位址可以管制網路的使用權，其原理很簡單，在可管理 MAC 位址的設備中設有一份 MAC 位址的存取控制表列(Access Control List, ACL)[16]，這份存取控制表列中記載著可放行的網卡 MAC 位址，只要符合裡頭的 MAC 位址就可以存取使用網路資源，反之則拒絕使用。可管理 MAC 位址的設備需要有 OSI 參考模型的第二層資料

連結層的功能，通常我們使用 Layer 2 或 Layer 3 網管型網路交換器(Managed Switch)或無線網路基地台(Wireless Access Point, WAP 或 AP)等，這些設備都可以自行增加或刪除 MAC 位址的存取控制表列，以達到管制網路的使用權。其中 Layer 2 網管型網路交換器可管理 MAC 位址，如圖 2-8，而 Layer 3 網管型網路交換器則可管理 MAC 位址和 IP 位址。

通常這類的機制是需要使用者手動在瀏覽器輸入註冊申請的網址，待申請核可後，才有網路的使用權，像宿舍網路管理系統。此種機制的做法為將 Layer 3 網管型網路交換器的存取控制表列預設拒絕所有對外連線，只允許連往註冊申請的網址，當使用者打開瀏覽器手動進行註冊申請，待資料無誤核可後，Layer 3 網管型網路交換器的存取控制表列就會增加一筆 MAC 位址的放行資料，最後使用者就有完全的網路使用權。

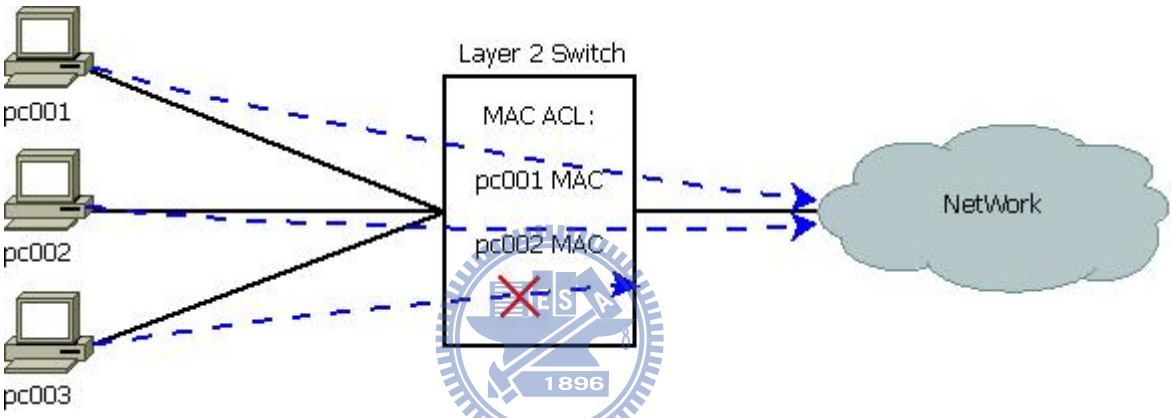

圖 2 - 7 Layer 2 Switch MAC ACL 管控圖

2.5.2 使用網頁認證機制的網路管制

使用 Captive Portal(網頁認證)機制[17]可以管制網路的使用權管制，其原理為將未認證許可的使用者，在使用網頁瀏覽器要連往 Internet 時，強制將使用者瀏覽器的頁面導向到認證伺服器所提供的認證畫面，經過認證許可後才能放行使用網路資源，反之則拒絕使用。使用 Captive Portal 機制的網路，在未認證許可時，所有連往 Internet 的服務都是不允許的，像是 FTP、SMTP、SSH 等都不被許可，除了使用者打開瀏覽器才會被強制的導向到認證伺服器提供的認證或付費的畫面，直到使用者認證成功或付費後才可使用網路資源，亦可使用其他網路服務。

在 Captive Portal 機制通常會有白名單(whitelist)[18] 管控哪些使用者可以使用網路資源。一般經過認證許可後，會有一段使用期限，超過這個使用期限就得再次認證許可，所以 Captive Portal 機制的認證伺服器系統會有一個白名單，記載著哪些使用者可以通行和其使用期限，其白名單可以設定來源 IP 位址、來源 MAC 位址、目的 IP

位址或目的 port 等進行管控，如圖 2-9。常見的 Captive Portal 機制有三種，分別為使用 HTTP 302 重導向、IP 重導向和 DNS 查詢重導向。

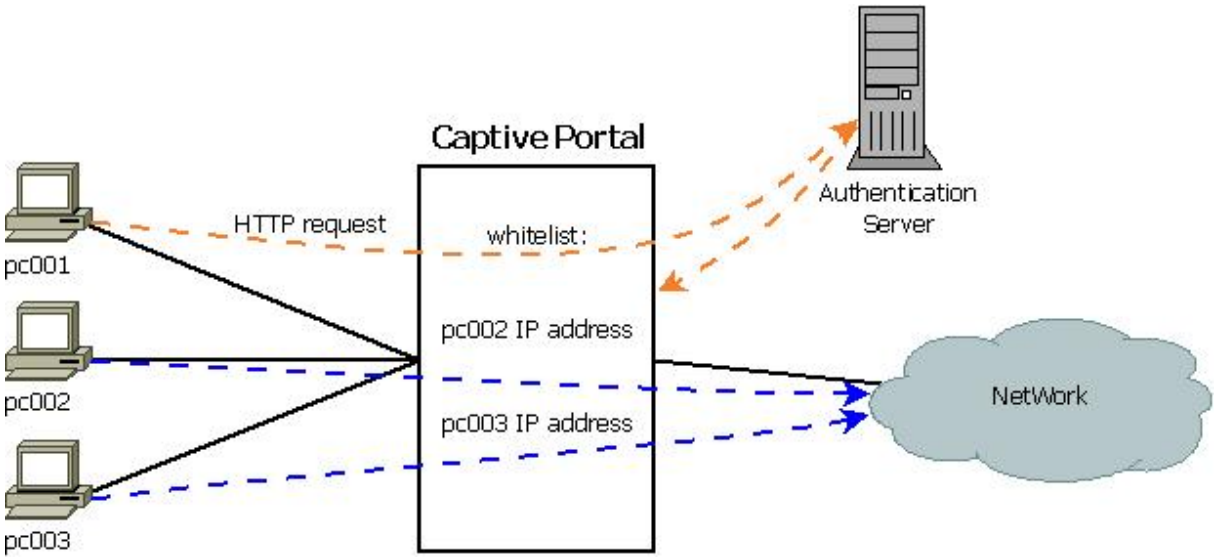

圖 2 - 8 Captive Portal 機制管控圖

2.5.2.1 使用 HTTP 302 重導向

如果未認證許可的 Client 電腦想要連往 Internet 的某個網站，首先 Client 電腦會送出 DNS 查詢，詢問該網站的 IP 位址，查詢後就進行連線，但此連線會被防火牆強制中斷並導向轉址伺服器去，此時轉址伺服器會送出 HTTP 狀態 302 封包[19]給 Client 電腦的瀏覽器將網頁導向認證網頁，因為 HTTP 狀態 302 封包中含有認證伺服器的認證網頁網址，而 HTTP 狀態 302 是說明目的網址已移動，並告知移動後的網址，所以才會進行強制網頁導向，如圖 2-10，但有些安全性較高的瀏覽器會將 HTTP 狀態 302 封包視為非法連線，而造成無法正常將網頁導向認證網頁。

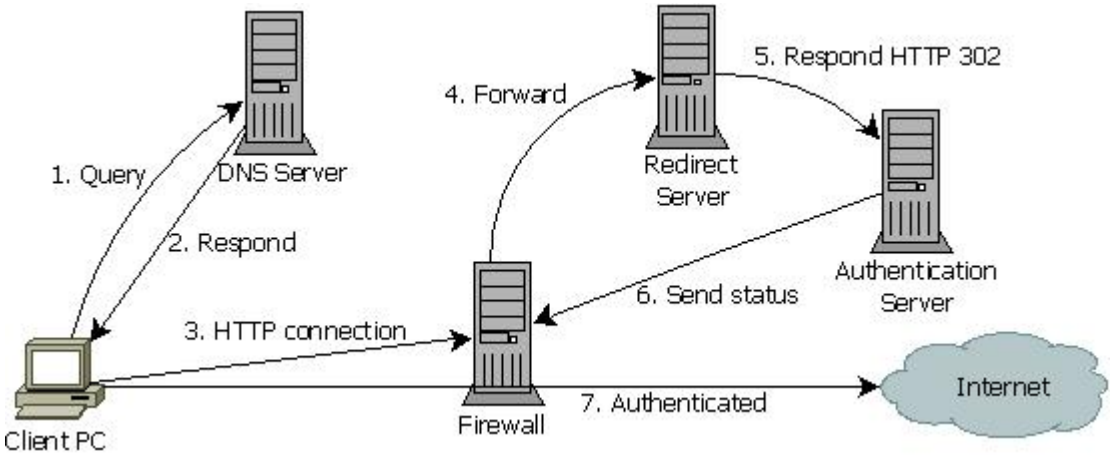

圖 2 - 9 HTTP 302 重導向流程

2.5.2.2 IP 重導向

將未認證許可的 HTTP 連線,使用防火牆等設備強制使目的 IP 直接重導向至認證伺服器的 IP，不須透過瀏覽器判斷該往何處進行認證，如圖 2-11。但因為一般的防火牆只能進行 IP 的重導向，無法進行 HTTP 指令的重導向，所以如果 Client 電腦的 HTTP 連線有其他指令內容的話，將無法正確的執行認證伺服器的認證網頁。

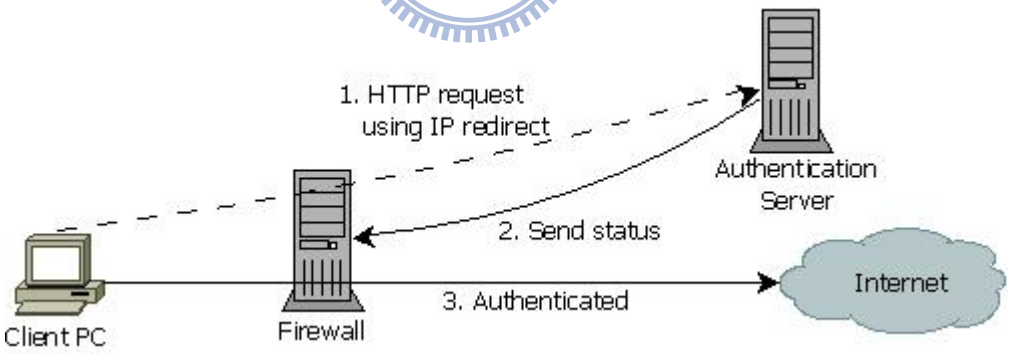

圖 2 - 10 IP 重導向流程

2.5.2.3 DNS 查詢重導向

當未認證許可的 Client 電腦使用瀏覽器要連往 Internet 某個網站時，會送出 DNS 查詢，詢問該網站的 IP 位址，此時 Captive Portal 機制系統的 DNS 會送出認證伺服器的 IP 位址給 Client 電腦，而使瀏覽器連往認證伺服器的認證網頁。DNS 查詢重導向運作原理是 Client 電腦在透過 DHCP 伺服器取得 IP 位址和 DNS 伺服器位址相關設定時，

故意將 DNS 伺服器位址設為 Captive Portal 機制系統專屬的 DNS 伺服器位址，所以不管 Client 電腦送出要查哪個網站的 IP 址位，此 DNS 伺服器都會回答認證伺服器的 IP 位址，這樣就能使瀏覽器重導向至認證伺服器的認證網頁，等認證許可後，才會將正常的 DNS 伺服器位址給 Client 電腦進行一般的 DNS 查詢，如此就可以正常的使用網路資源了，如圖 2-12。

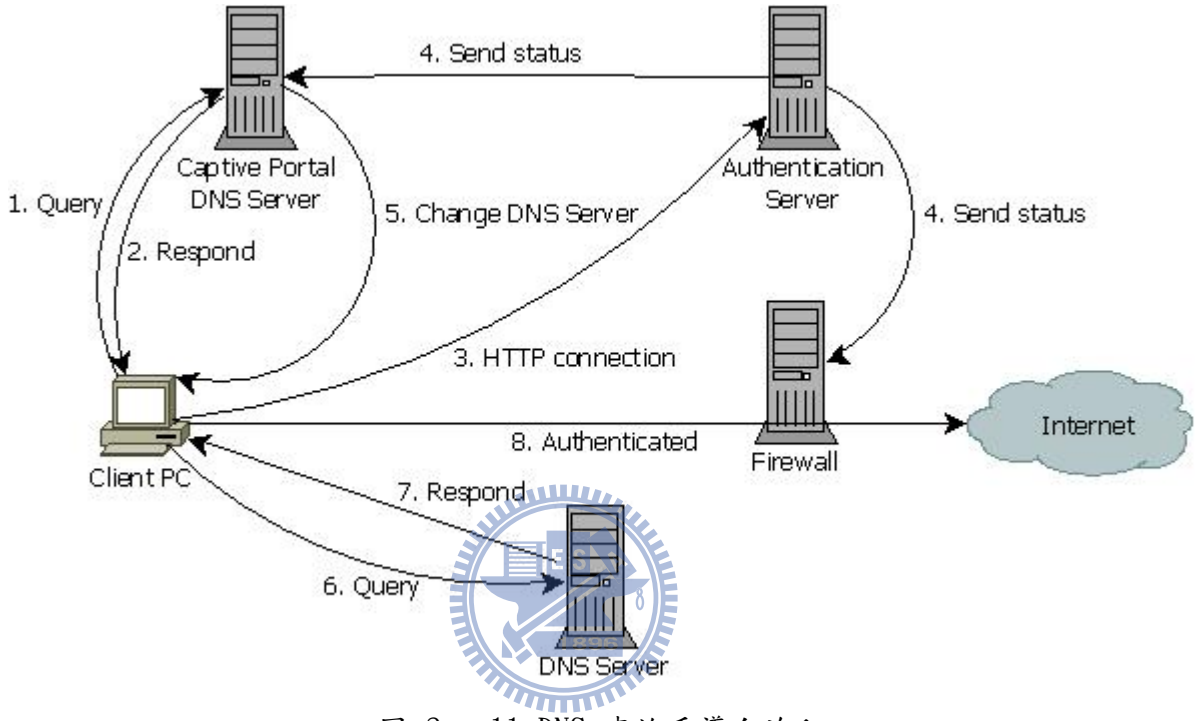

圖 2 - 11 DNS 查詢重導向流程

如果一開始 Client 電腦使用瀏覽器輸入 IP 位址進行 Internet 連線時，此機制將不會啟動，因為並沒有用到 DNS 伺服器查詢 IP 位此功能，另外，如果使用者更改自己電腦的網路設定，將 DNS 伺服器 IP 位址設定成功能正常的伺服器時，此機制也將不會啟動，因為系統並沒有將認證伺服器的認證網頁告知使用者來進行認證。為了解決以上的問題，還需搭配防火牆一起使用，未經過認證許可的電腦只能使用 Captive Portal 機制系統專屬的 DNS 伺服器，而其他的 DNS 伺服器通通拒絕連線，待認證成功後才各別開放使用正常的 DNS 伺服器。

第三章 相關研究

為了掌握內部 IP 位址的使用狀況，避免網路資源被有心人士濫用，各學者對 IP 位址管理或網路使用權的管制都有其一套方法，本章以諸多管制網路使用權技術文章，擷取與本研究相關的文章討論。其內容包括了 IP 位址分配與管理、L2 Switch 管制網路使用權和防火牆管制網路使用權。

3.1 IP 位址分配與管理

區域網路中的 IP 位址管理是一門學問，除了使用者與 IP 位址對應要正確之外，減少網管人員的工作時間和方便管理也是很重要，在 2001 年時，林碧華[20]設計了一個可調適之 IP 位址分配與管理系統，為了提高 IP 位址的使用效能，其系統架構如圖 3-1。一般來說，網管人員在管理 IP 位址都人工逐筆記錄下來，並隨時更新資料，雖然這樣的管理方式很簡單而容易，但是如果 IP 位址數目過多或者 IP 位址常常異動時，要保持這份資料的正確性和即時性，將是網管人員的一大問題。所以，為了解決這樣的問題，並且讓 IP 位址的使用效能提高，此系統藉由瀏覽器存取的方式，提供管理者線上維護管理的功能，由各單位分層負責，確保資料的正確性，增加 IP 位址使用效能，另外，也讓一些不常使用的固定 IP 位址或是租約未到期而沒使用的的 IP 位址，在 IP 位址快要分配用完時，能夠釋放出來讓需要的 Client 電腦借用，讓 IP 位址的使用效能提高。

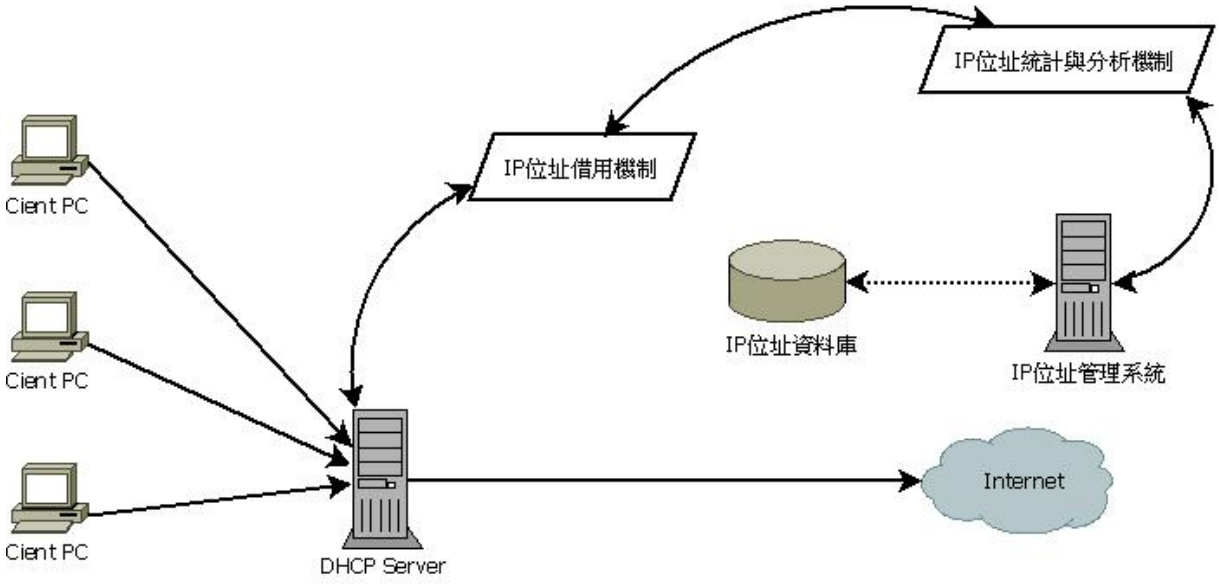

圖 3 - 1 可調適之 IP 位址分配與管理系統架構圖

此系統分為兩大部分，第一部分為 IP 位址管理系統，各單位管理者將管轄內每一個 IP 位址的使用資訊上網登錄，確保資料的正確性，隨時掌握最新的異動狀況，並透過 IP 位址統計與分析機制將目前 IP 位址使用情況記錄在資料庫中，做為 IP 位址管理的依據。第二部分為可調適之 IP 位址分配與管理系統，為了能夠借用已分配給固定使用者之 IP 位址，因此必須定期取得可借用固定 IP 位址的資訊進資料庫中，透過 IP 位址借用機制配合 DHCP Server 的 IP 位址集中管理，提供動態適時調整 IP 位址配置的功能，改善 IP 位址使用情形，其 IP 位址偵測架構如圖 3-2。

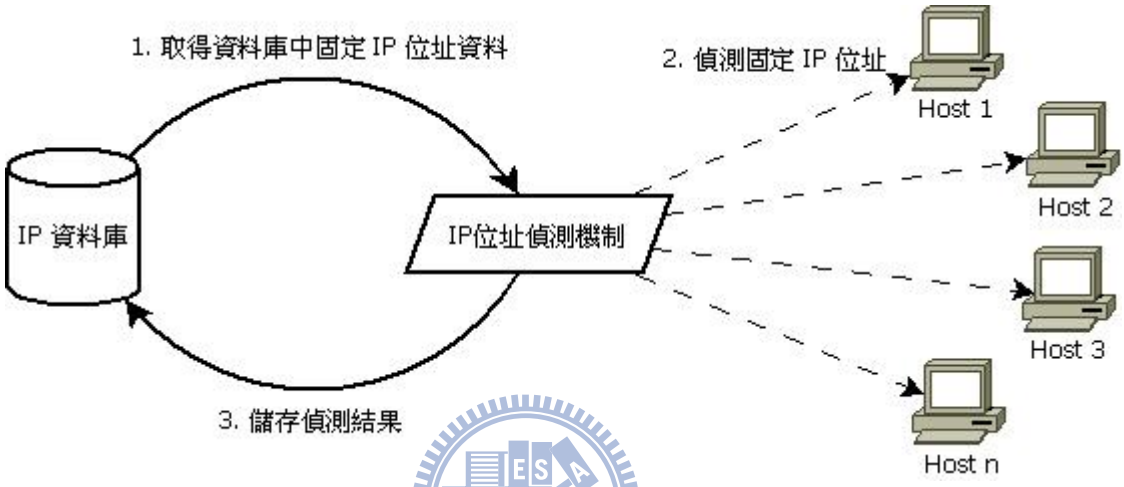

圖 3 - 2 IP 位址偵測架構圖

在 IP 位址分配與管理系統中，依使用者的需求分成三個不同的模組並設定不同的權限，其三個模組分別為網路管理者模組、單位管理者模組和一般使用者模組，其功能分別詳述如下：

1、網路管理者模組：提供網管人員線上即時維護管理的功能，除了有伺服器和網路設備等基本資料查詢外，還提供 IP 位址的子網路段的分配、網路設備、IP 位址及管理者等相關資料之新增、刪除、修改和查詢等功能。

2、單位管理者模組：在一個龐大的組織單位中，每一個單位 IP 位址的使用情形只有該單位最清楚了，所以各單位的 IP 位址資訊管理就直接授權給各單位自行維護，如此分層負責將 IP 位址的管理工作減化，除了可分擔網管人員的負擔，也可確保 IP 位址資料的正確性。

3、一般使用者模組：開放一般使用者查詢所提供的網路服務之伺服器資訊和目前所有 IP 位址的分配及使用情形。

此系統雖達到以電腦化和分層負責的作業方式來管理 IP 位址之使用，取代原本人工用紙張登記的方式，確實節省了網管人員在管理 IP 位址的時間，也讓 IP 位址的使用資訊更正確，在查詢時較以前方便許多，但在網路管理部分，缺少了阻斷濫用網路資源的機制。

在 2007 年時，曾憲民[21]提出非法連網自動偵測與資源效能監控機制系統，為了解決使用者私下連接網路設備或非法更改現有設備的 IP 位址等相關問題。雖然網管人員對於 IP 位址的運用都有自己一套的管理政策，但是在內部網路中，仍有許多問題需要去解決，像是有多少 IP 位址被使用、使用者不遵守網管人員分配的 IP 位址導致 IP 相衝或是發生中毒能否迅速找到該部電腦等問題，所以此系統整合了用戶者基本資料、固定 IP 位址管理與使用統計及非法 IP 位址偵測管理等功能來解決上述問題，來減低網管人員的維護成本，也能加速異常網路問題處理時效性。此系統其目的為：

1、有效建置使用者基本資料與 IP 位址的配置。

2、快速監控非法連接網路與執行組絕其連線。

3、管理網路資源使用情況，以利掌握網路使用現況。

為了達成以上目的，網管人員需要將所有的網路設備資料輸入至資料庫中，如廠牌、MAC、IP、埠數和位置等，如果即可在線上方便的查詢所有網路設備資料。而使用者要儘速獲得合法 IP 位址的申請，則需要透過網頁的方式，將自己的單位、姓名、聯絡電話和 MAC 等輸入至申請表單中，因為此系統分配的 IP 位址是採固定式的，所以使用者在填寫 IP 申請表之後，由網管人員線上做申請資料審查的動作並給予一個 IP 位址，如果址 IP 位址未被使用，即將 MAC 及 IP 寫入 DHCP 設定檔裡並自動重新啟動 DHCP 伺服器讓設定值生效，並同時新增至資料庫的 IP 基本資料中做以後查詢使用，其使用者資料及 DHCP 建置流程如圖 3-3，此 DHCP 網址分配資料流程大大節省人力維護時效。

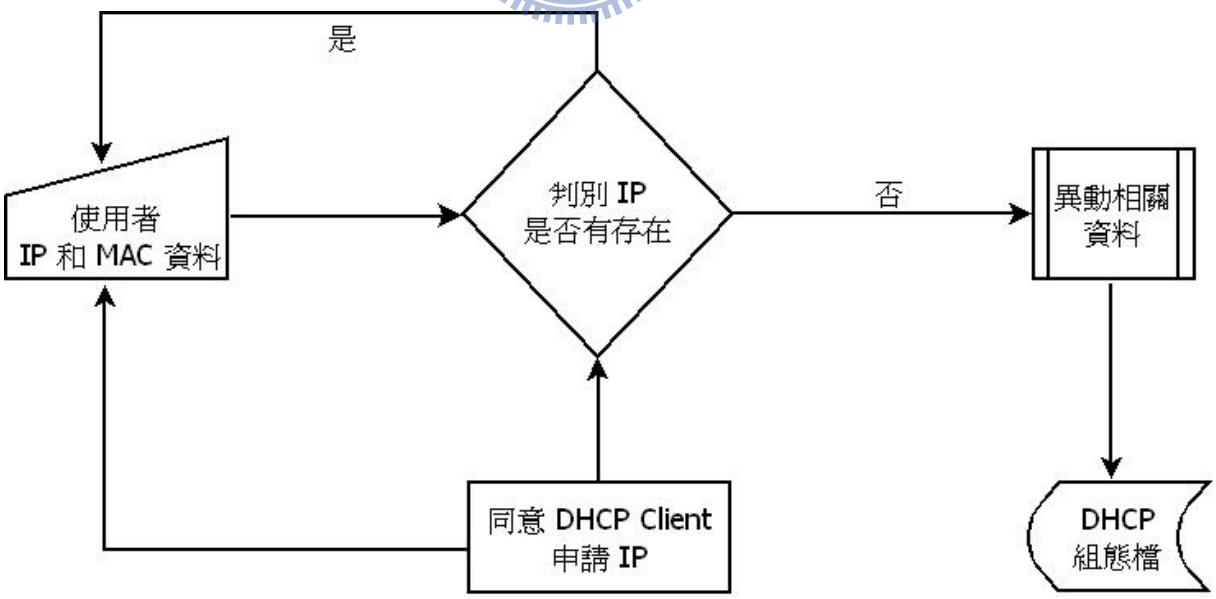

圖 3 - 3 使用者資料及 DHCP 建置流程圖

網管人員如果想知道網路設備上 port 的 IP 使用情況，就需要採購含有 snmp 功能的網路設備，為了不增加網路的管理成本，此系統使用 nmap 工具主動定期偵測區域網路內所有的 IP 使用情形，和利用 arp 取得 arp table 資料，這些資料與資料庫中的使用者資料表 IP 進行比對並統計 IP 使用次數，並寫至資料庫中以利後續查詢，而在比對時，如果 IP 或 MAC 有誤時，就判定為非法連接的 IP 位址或 MAC 位址，並將這些資訊寫入資料庫中做後續的追蹤與管制，其系統與資料庫運作流程如圖 3-4。

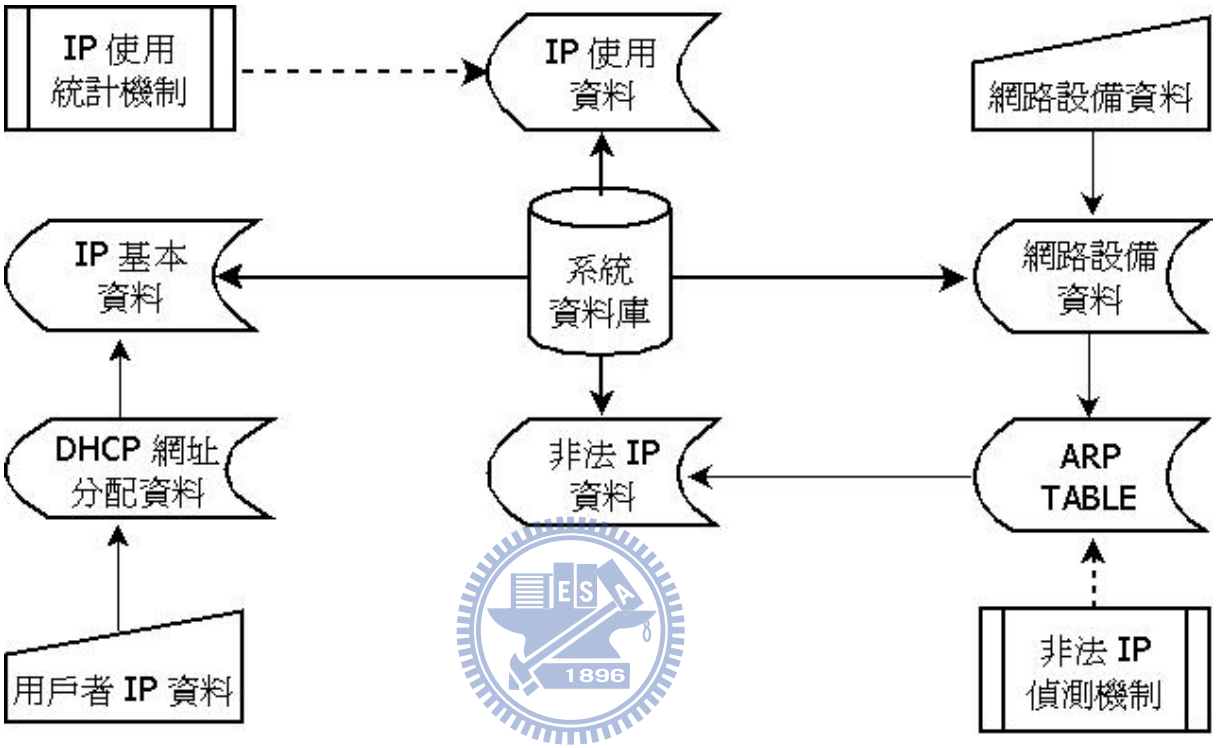

圖 3 - 4 系統與資料庫運作流程圖

曾憲民提出非法連網自動偵測與資源效能監控機制系統，比林碧華設計的可調適之 IP 位址分配與管理系統加強了偵測非法 IP 位址和可阻斷濫用網路資源的機制，這對管網人員來說是很重要的功能，但對網路使用權的管制並沒有認證機制，這對資訊安全會有不少衝擊。

3.2 Layer 2 Switch 管制網路使用權

網路使用權的管制如有認證機制，可額外加強資訊安全的防護，如在 2005 年時，劉則明、程毓明、刁建成的自動化宿舍網路註冊管理系統[22]中，為了能夠在最短時間內完成定位與鎖定流量異常的電腦，利用開放軟體 Linux 作業系統當註冊認證平台與管理系統，Layer 3 Switch 則當網路通行管制系統，使用 Static ARP Table 與 MAC Address

對應的特性來鎖定使用者，完成宿舍網路註冊系統，此系統讓宿舍網路 IP 管理更方便，能在短時間內找出有問題的電腦並加以中斷連線，亦節省繁瑣費時的書面申請，管理者大幅減少花費管理的時間。

此系統管理主要包括 IP 位址的申請開通、更換與管制，也能夠輔助流量分析統計軟體，在最短的時間內阻斷異常流量的電腦，為了要達到友善的操作介面及跨平台性，使用 web 的介面來操作，而在控制網路設備的部分，則是使用 snmp protocol 和 telnet command 來完成。其申請運作流程如圖 3-6，方式為：

1、為了避免未註冊的使用者可以連上 Internet，所以在 Layer 3 Switch 的 Access Control List 預先設定未註冊者只能連至註冊認證伺服器，其他地方則拒絕通行，如圖 3-5：

```
Extended IP access list RegUsers
      permit ip any 192.168.0.1              <- 註冊認證伺服器
      permit ip host 192.168.0.11 any        <- 有註冊的 IP 位址
      permit ip host 192.168.0.12 any        <- 有註冊的 IP 位址
```

圖 3 - 5 Access Control List

2、學生使用自己的電腦透過宿舍網路向 DHCP Server 取得到一組未經過認證的 IP 位址，然後打開瀏覽器連至註冊認證伺服器進行申請，登入系統進入申請介面後，只需輸入個人基本資料即可，其 IP 位址為系統提供。輸入完成時，認證程式會核對此申請者是否為住宿生，亦判斷 Clinet 電腦的 IP 位址是否來自於宿網，一切無誤才允許註冊。

3、為必免使用者將 MAC 位址輸入錯誤，系統會送出 SNMP 命令向 Layer 3 Switch 和下一層的 Layer 2 Switch 詢問確認此 IP 位址的 MAC 位址為何，如果 MAC 址位是符合的才允許註冊。

4、註冊完成後，系統會將該使用者所分配到的 IP 位址經由 Web 畫面告知申請者，並將該 IP 位址和 MAC 位址分別寫入 Access Control List 和 Layer 3 Switch 的 Static ARP Table 中，亦將申請者的基本資料、IP 位址、MAC 位址等寫入資料庫中，即完成網路開通動作。

此系統的系統架構如圖 3-7。為了使此系統管理自動化和操作方便，在資料庫的規劃方面，使用了三個資料表：住宿生的基本資料、記錄註冊者基本資料的表格和紀錄網路設備對資訊節點編號及 IP 位址的對照表，而在系統管理方面，此系統提供了 Web 介面管理，其宿網管理方面，可執行新增、修改、停權及刪除使用者或其資料，亦可將資料庫中的記錄存入 Layer 3 Switch 中，另外，在用戶管理方面，則有新增管理者或更改管理者權限。

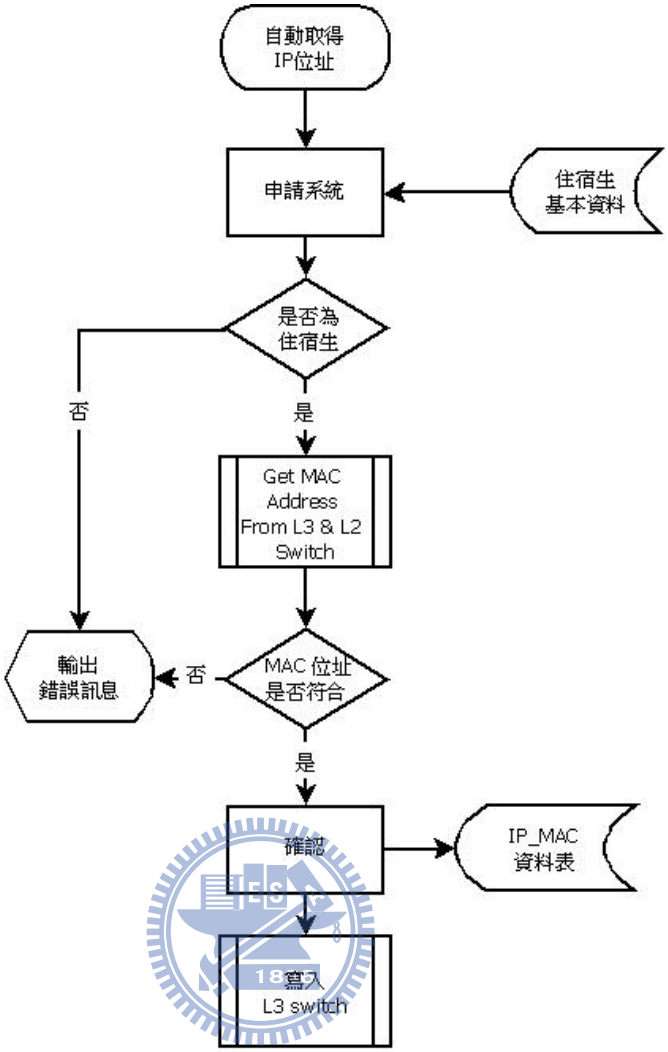

圖 3 - 6 註冊申請流程

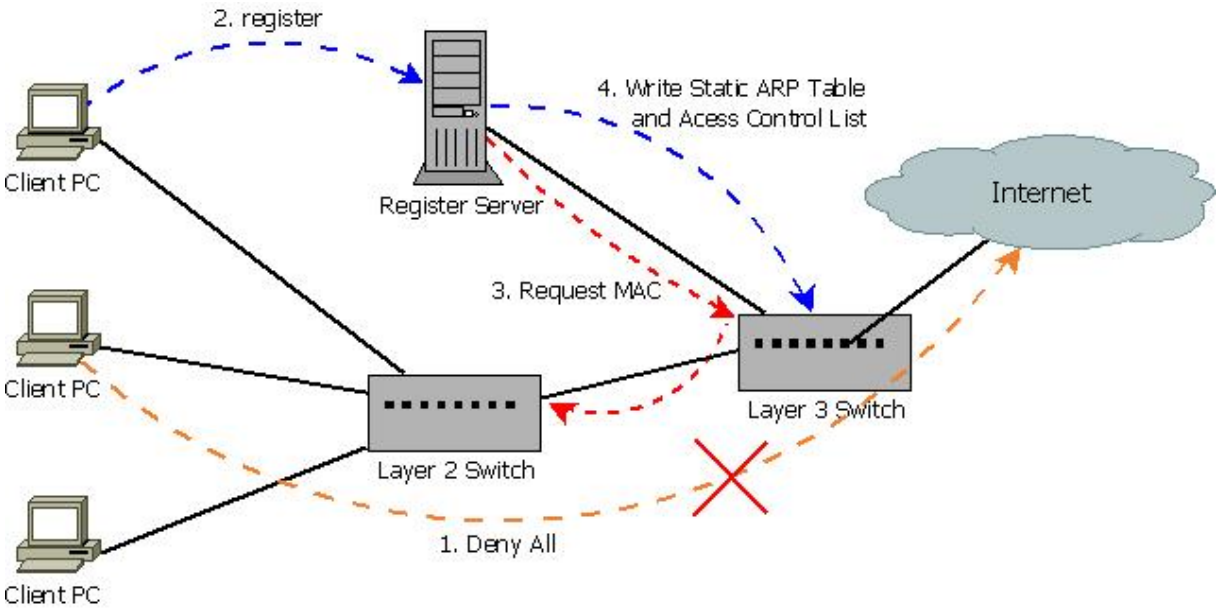

圖 3 - 7 宿舍網路註冊系統架構圖

3.3 防火牆管制網路使用權

網路使用權的管制除了使用 L2 Switch 之外，亦可以用防火牆來管制，各有優缺點，防火牆比 L2 Switch 花費少、建置容易、管理方便，但不如 L2 Switch 管制來得安全可靠，所以使用防火牆來管制網路的使用權也有其重要地位。如 Robert Beck [23] 在 1999 年時，設計了一套利用 telnet 登入認證後，即開通防火牆規則讓 Client 電腦可以連往 Internet。該實驗室想管制內部網路電腦對外的網路使用權，想以：

1、簡單而且廉價的方式進行部署。

2、使用者必須在原本且方便的的環境中使用，除了不需額外安裝軟體外，也不需太多的前置教育。

3、能夠使用原本存在 UNIX 的五萬個帳號為基礎做為認證，而不須另外建置其他帳號做為認證來源。

4、未認證的使用者拒絕連線至 Internet。

5、在已認證期間中，使用者可以不受限制的使用 Internet。

雖然業界有解決方案，但費用太高，所以該實驗室利用開放軟體的 OpenBSD 作業系統做為身分認證閘道器(Authenticating Gateway)，預設是拒絕所有的對外連線，如圖 3-8，當使者使用 telnet 登入到此身分認證閘道器經過認證後，該身分認證閘道器就產生一條防火牆規則讓此 Client 電腦可連往 Internet，如圖 3-9，而等使用者將 telnet 登出後，該身分認證閘道器就會把之前產生的防火牆規則給刪除，恢復無法對外連線的狀態，下次使用者要再連往 Internet 時，得再次 telnet 登入進行認證，如圖 3-10。

```
# 允許內部網路的電腦連線至認證伺服器 IP (129.128.38.65)
pass in quick on fxp0 from any to 129.128.38.65/32
# 網路卡 fxp0 中，拒絕所有的連線
block in on fxp0 from any to any
```

圖 3 - 8 防火牆禁止連線預設規則

```
# 電腦 IP 為 129.128.38.100 的認證後，防火牆產生放行規則
pass in quick from 129.128.38.100/32 to any
```

圖 3 - 9 認證後增加的防火牆規則

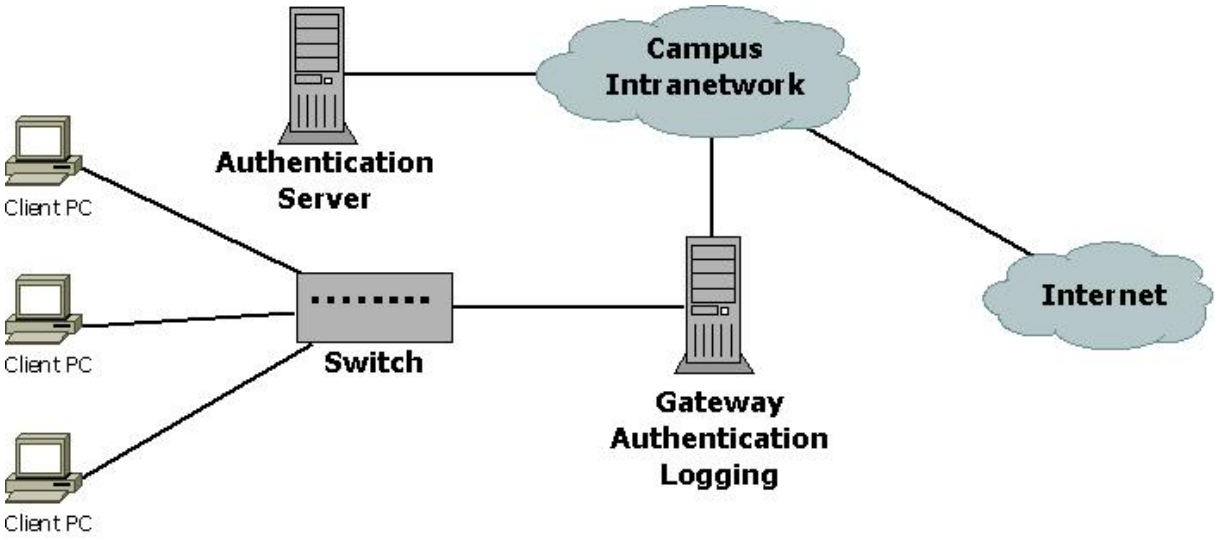

圖 3 - 10 Authenticating gateway 圖

此系統雖然方便，但使用者要額外使用 telnet 軟體進行登入認證才有完整的網路使用權，如果能結合原本的網路操作環境或使用者常用的軟體，如瀏覽器，這樣就更方便更容易了。

楊有信[24] 在 2008 年時，結合了原本的網路操作環境，設計了一套經微軟(Microsoft)開發的 Active Directory(AD) 伺服器認證後，即開通防火牆規則讓 Client 電腦可以連往 Internet。為了解決傳統手工 IP 位址與使用者的對應表，和正確找出惡意使用者假造 IP 位址濫用網路資源，其作法為使用開放軟體的 Linux 作業系統當防火牆，管控使用者的網路使用權，預設是拒絕所有的對外連線，當使用者登入 AD Server 證認伺服器後，會產生使用者的帳號和 IP 位址等資料，再利用微軟開發的 MSDN API 可以達到存取相關認證資料，即可送往 Linux 的防火牆產生放行規則，讓使用者可連往 Internet，如圖 3-11。

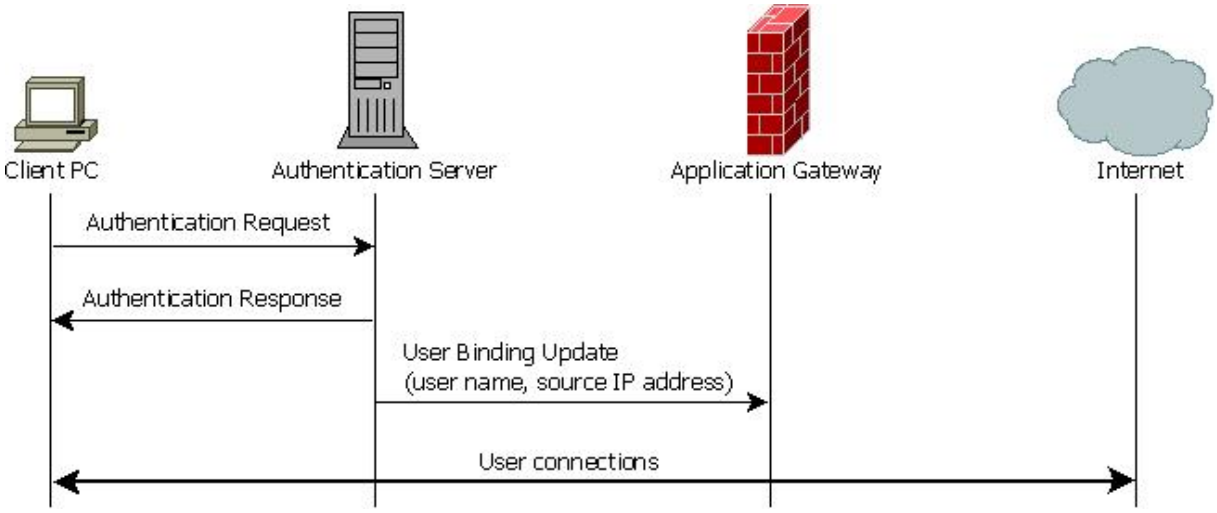

圖 3 - 11 Binding updates 圖

在 Linux 的防火牆中，IP 位址和使用者的對應部分，是藉由身分認證伺服器的協助下，動態地紀錄在 Linux 核心中。當使用者連往 Ineternet 有新的連線產生時，系統則會利用此連線的 IP 位址去查詢在 Linux 核心中的對應關係，找出是誰在使用這個 IP 位址並記錄在此連線中，而等到此連線結束時，則會將此 IP 位址和使用者的對應關係記錄到系統上供以後使用。

在圖 3-12 中，呈現了系統元件在辨識與過濾檢查過程之間的相互作用：

1、使用者要使用任何 Ineternet 資源之前，必須通過身分的認證。

2、身分認證驗證後，身分認證伺服器會送該使用者的相關訊息給 Information Loader，當 Information Loader 收到訊息後，會設定 IP 位址和使用者的對應表並送往 Connection Identifier 使用，而在 Linux 核心中則會更新 IP 位址和使用者對應關係。

3、當使用者連線產生的第一個封包則會送往 Connection Identifier 來識別此 IP 連線的使用者是誰，然後將此封包連線相關訊息送往 Filtering Component 進行過濾和比對的動作。

4、該連線之後的封包則會直接送往 Filtering Component 做過濾的動作。

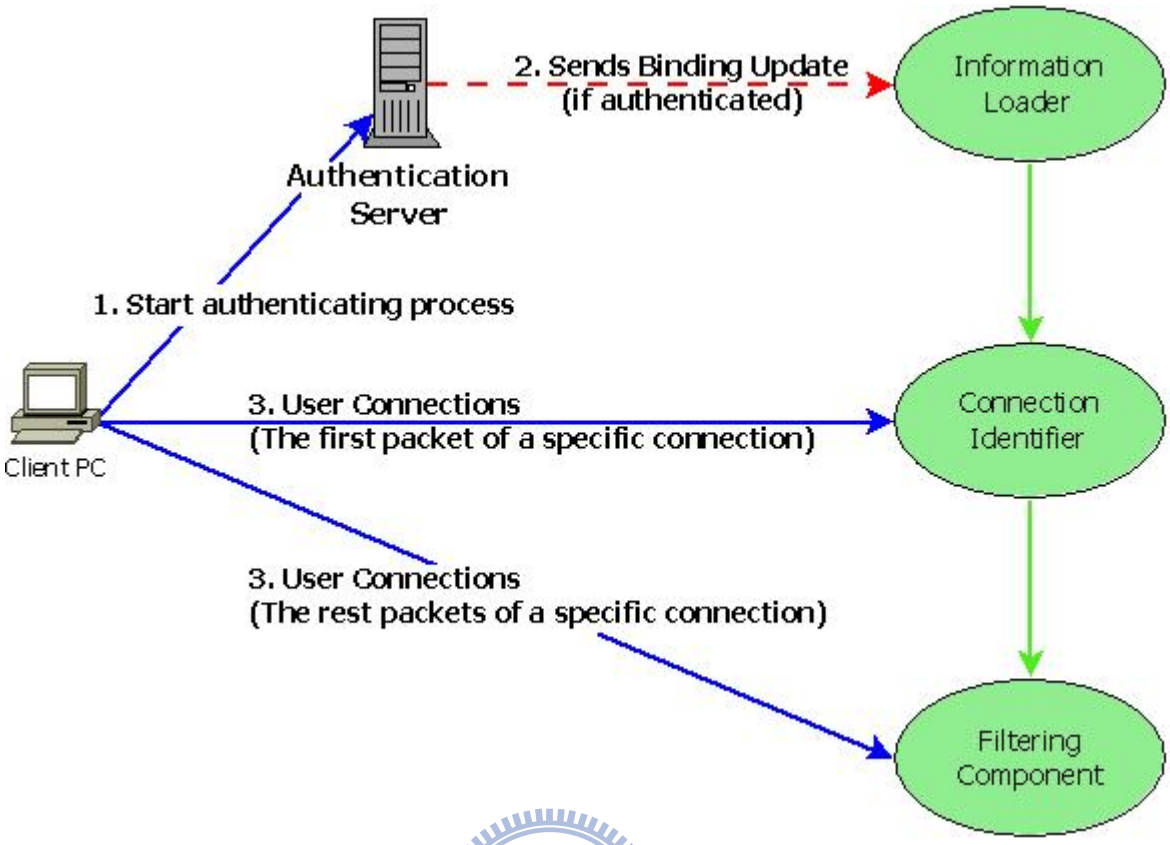

圖 3 - 12 Co-operations between system components 圖

因為此系統在原本的網路操作環境中結合網路使用權的認證,確實讓使用者不用額外再學習如何操作使用，只要依原本操作登入 AD Server 即可完整的使用網路資源，大大減少管理 IP 位址的維護成本。

第四章 結合身分認證之校園 IP 管理系統(CIASPA)

在過去網路尚未普及之前，電腦設定 IP 位址都採人工登記或是自由取得的方式，因為電腦數量不多和使用者使用網路的行為較單純，所以網管人員還能以人工作業的方式進行簡單之管理，而使用者濫用網路資源時，也因為電腦數量不多，所以能及時找到是哪部電腦出了問題；但隨著科技網路蓬勃發展，電腦價格下滑，使得校園電腦數量大增，使用者能用的網路資源也多樣化，在這樣複雜的網路環境中，網管人員如果還是使用過去的方式來管理 IP 位址，那將是非常繁雜且辛苦的工作，因此，如果能將管理 IP 位址的工作電腦化，透過使用者認證機制後才能使用網路權，這樣就能節省網管人員管理 IP 位址的時間，也能迅速找出濫用網路資源的使用者並加以阻斷，讓校園網路時時保持暢通，所以如何有效的管理 IP 位址和透過認證管制網路使用權，成了一個需要解決的問題。

4.1 CIASPA 概說

本系統最重要的環節是如何在不變更現有的網路環境、不增加使用者操作負擔和不增加軟硬體經費下，讓使用者能定期認證一次，即可取得網路使用權，並設計一套校園 IP 管理機制來保持校園網路的暢通，讓網管人員較容易的管理 IP 位址，能及時查詢有問題的 IP 位址之電腦在何處。

基於以上問題，我們建置了一套能配合認證機制而有效管制網路使用權的校園 IP 管理系統(CIASPA)，如圖 4-1，所有使用者在使用網路權之前，都必須透過認證申請 IP 位址，我們使用了防火牆來管制網路權的使用可否，將未申請者的瀏覽器自動導向認證網頁進行申請，希望藉由使用原本電子信箱的帳號和密碼做為認證依據，定期讓使用者在上網前登入電子信箱的帳號和密碼進行 IP 位址申請，便可使 IP 址位使用列表保持最新最正確，減少網管人員人工管制 IP 位址的麻煩，達到網路使用權的管制。另外，本系統可以線上即時阻斷有問題 IP 位址的網路使用權，以確保校園網路的暢通，當然，透過系統以資料庫儲存 IP 位址的使用紀錄，可做為發生資安問題時追查來源依據，確保其他使用者的權益。

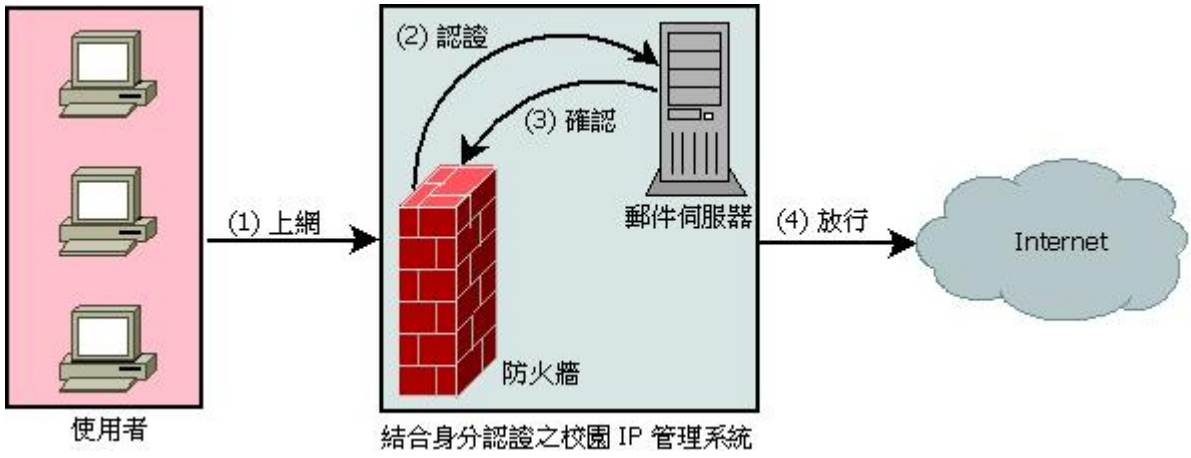

圖 4 - 1 系統示意圖

4.2 CIASPA 架構

我們為了讓使用者容易使用且不用多做額外的教育訓練，也讓管網者能對 IP 位址的管理更能即使掌控，所以將系統分割成兩個子系統：IP 位址申請子系統與網路安全管理子系統。而其主要的核心功能由下列六個模組所組成：網頁認證模組、IP 位址註冊模組、來賓帳號管理模組、IP 位址使用列表模組、IP 位址控管模組與 IP 位址歷史紀錄模組，其系統架構如圖 4-2。

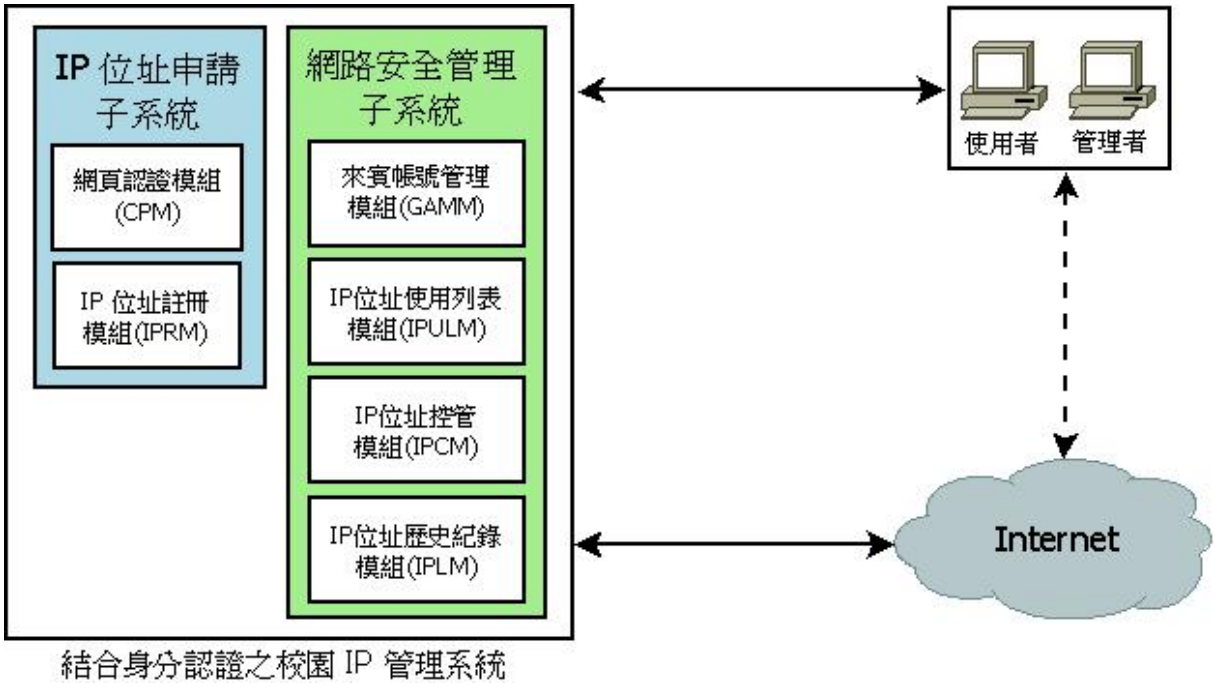

圖 4 - 2 CIASPA 系統架構圖

接著我們將對此六個模組的工作內容與設計理念做深入的說明。

1、網頁認證模組(Captive Portal Module, CPM)：

工作內容：

(1)阻斷未申請者的網路使用權。

(2)強制導向到認證的網頁。

(3)提供跨校 Email 認證機制。

(4)IP 位址與 MAC 位址綁定。

(5)檢查申請有效時間。

設計理念：

使用者在未申請之前，都無法使用網路權，為了不增加使用者申請的負擔，本系統採用網頁認證，使用者只要打開網頁，就會自動導向認證的網頁中，減少操作上的不便，其流程如圖 4-3。在認證方面，則是透過學校原有的 Email 帳號密碼來認證，不必額外記住其他帳號密碼，亦可以設定同時使用跨校 Email 認證服務和來賓帳號認證機制，方便校外人員到校研習使用，如圖 4-4。在 IP 位址與 MAC 位址管理方面，為了避免使用者私下更動自己的 IP 位址，本系統在 IP 位址申請後，立即將使用者的 IP 位址與 MAC 位址透過靜態 arp 進行綁定作業。最後，系統會定期檢查每個 IP 位址的申請有效時間，期限到了，則關閉網路使用權，並解除 IP 位址與 MAC 位址綁定，讓此 IP 位址可以被重新申請。

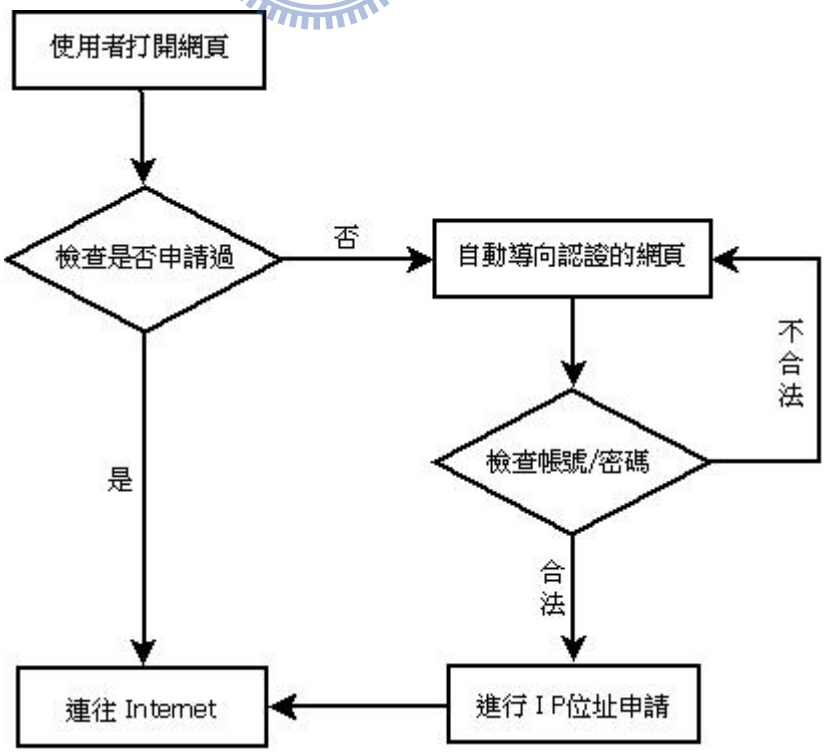

圖 4 - 3 網頁認證流程圖

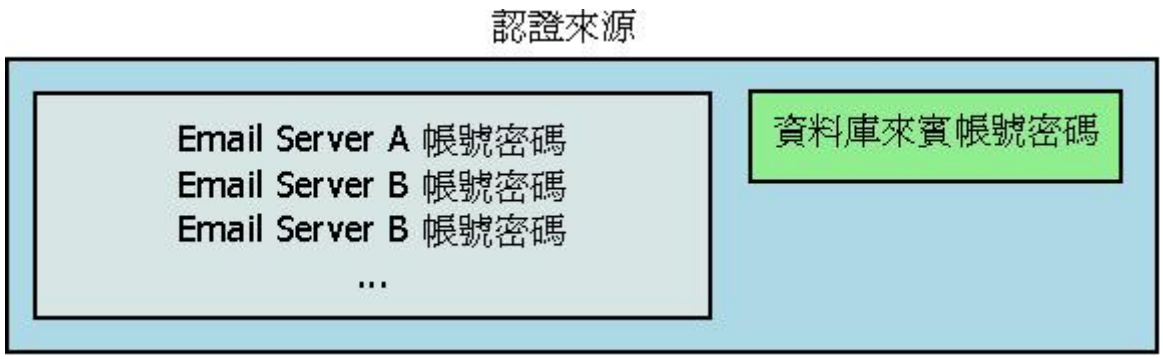

圖 4 - 4 CPM 之認證來源

2、IP 位址註冊模組(IP Register Module, IPRM)：

工作內容：

(1)自動抓取使用者 IP 位址和 MAC 位址。

(2)判斷 IP 位址和 MAC 位址是否重複。

(3)設定申請時效。

(4)紀錄使用者的單位。

(5)註冊後開通自動化，不需人工開通。

(6)註冊完，網頁自動導向原本網址。

設計理念：

為了方便使用者申請作業，本系統在網頁認證後，會自動透過伺服器網頁資訊抓取使用者 IP 位址和透過 arp 指令取得 MAC 位址，避免使用者輸入錯誤以減少申請難度，所以在註冊 IP 位址時，使用者只需選擇申請的時效和輸入使用單位即可，之後系統會馬上進行程序的處理，防火牆會自動開通網路使用權並將申請資訊記錄起來，IP 位址資訊資料表結構如表 4-1。最後在網頁呈現註冊成功和下次申請時間等訊息，也會在設定的時間內自動導向使用者原本想去的網址，如圖 4-5。

欄位名稱	欄位型態	欄位說明
ip	char	IP 位址
mac	char	MAC 位址
user_id	varchar	使用者帳號
where_use	varchar	使用單位
use_net	char	是否有網路使用權
no_use_time	datetime	重新認證時間

表 4 - 1 IP 位址資訊資料表結構

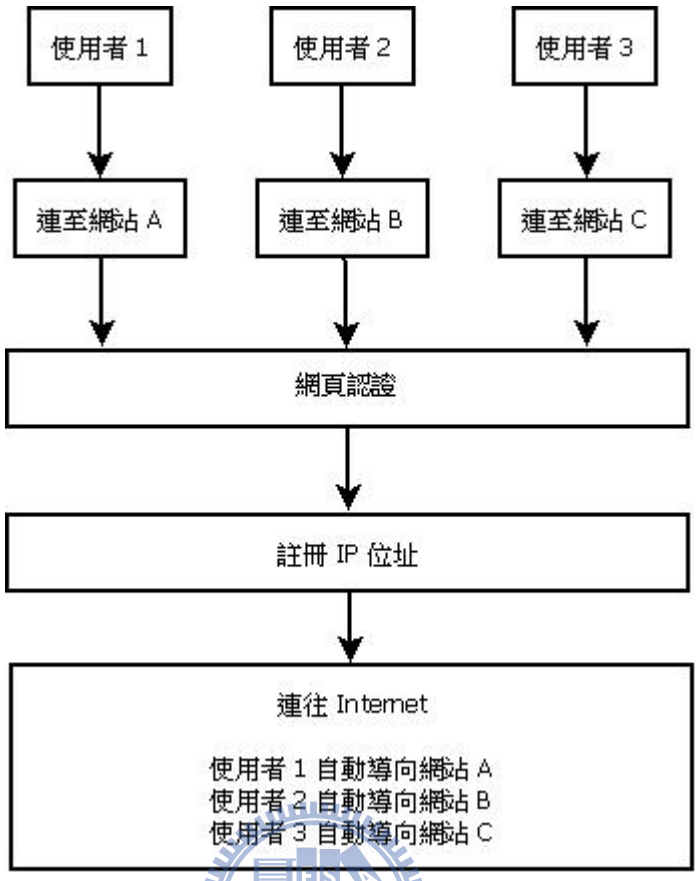

圖 4 - 5 註冊後網頁自動導向示意圖

3、來賓帳號管理模組(Guest Account Management Module, GAMM)：

工作內容：

(1)設定來賓帳號有效期限與開通後的使用時間。

(2)建立、查詢與列印來賓帳號。

設計理念：

校園網路使用權受到管制之後，將會面臨到他校的老師到校參加研習時而無法使用網路的問題，除了跨校 Email 帳號認證之外，如果參加研習的老師是來自較多不同的學校情況下，此模組可以產生來賓帳號供予短時間的使用。管理者可以設定來賓帳號的命名，然後以此命名加流水號的方式進行發放，也可以設定來賓帳號的有效期限和開通後的使用時間，避免被重複使用產生資安問題，如圖 4-6，建立完成的來賓帳號會受到有效期限和是否開通而被系統自動刪除，增加帳號管理的方便性。來賓帳號資料表結構如表 4-2。

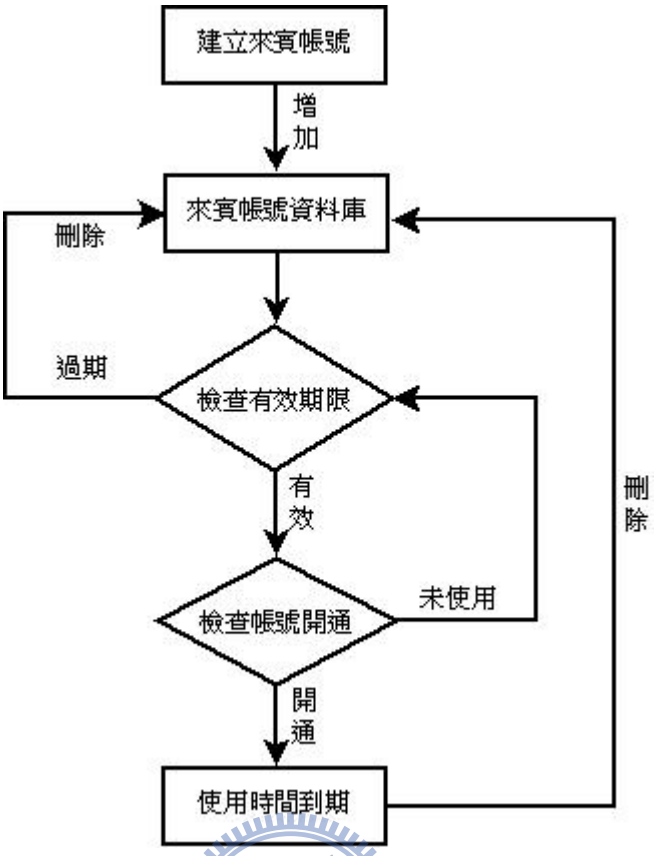

圖 4 - 6 來賓帳號管理流程

欄位名稱	欄位型態	欄位說明
user_name	varchar	來賓帳號
user_passwd	varchar	密碼
where_use	varchar	使用單位(用途)
have_use	char	是否開通
use_time	datetime	開通後可用多久
no_use_time	datetime	開通後失效時間
del_time	datetime	此帳號有效時間

表 4 - 2 來賓帳號資料表結構

4、IP 位址使用列表模組(IP Using List Module, IPULM)：

工作內容：

(1)列出目前正在使用的 IP 位址資訊列表。

(2)列出目前防火牆對 IP 位址管制的規則。

設計理念：

IP 位址使用列表模組可以線上列出目前正在使用的 IP 位址資訊列表，此列表是最新最正確的，讓網管人員更容易管理 IP 位址和明瞭 IP 位址使用現況。在此模組亦能顯示目前防火牆對 IP 位址管制的規則，可做初步檢核系統是否有正常運作。防火牆資料表結構如表 4-3。

欄位名稱	欄位型態	欄位說明
number	char	IPFW 序號
ip	char	IP 位址
use_it	char	是否啟用
rule	varchar	IPFW 規則

表 4 - 3 防火牆資料表結構

5、IP 位址控管模組(IP Control Module, IPCM)：

工作內容：

(1)設定下次申請時間。

(2)限速設定。

(3)阻斷有問題電腦的網路使用權。

(4)開通已註冊者的網路使用權。

設計理念：

資訊科技發展日新月異，使用者濫用網路資源也因此變多，嚴重時會造成校園網路的癱瘓，為了能讓校園網路保持暢通，此模組能進行阻斷有問題電腦的網路使用權動作，讓濫用網路資源的使用者暫時無法使用網路權，進行問題的解決。如圖 4-7，使用者在註冊 IP 位址之後，IP 位址控管模組即會開放網路使用權，使用者可以不受限制的連往 Internet，如果使用者濫用網路資源造成校園網路的癱瘓時，IP 位址控管模組可以將其連線阻斷，而網管人員可以依 IP 位址資訊找到該使用者電腦，進行問題解決，等問題解決後再恢復其網路連線。

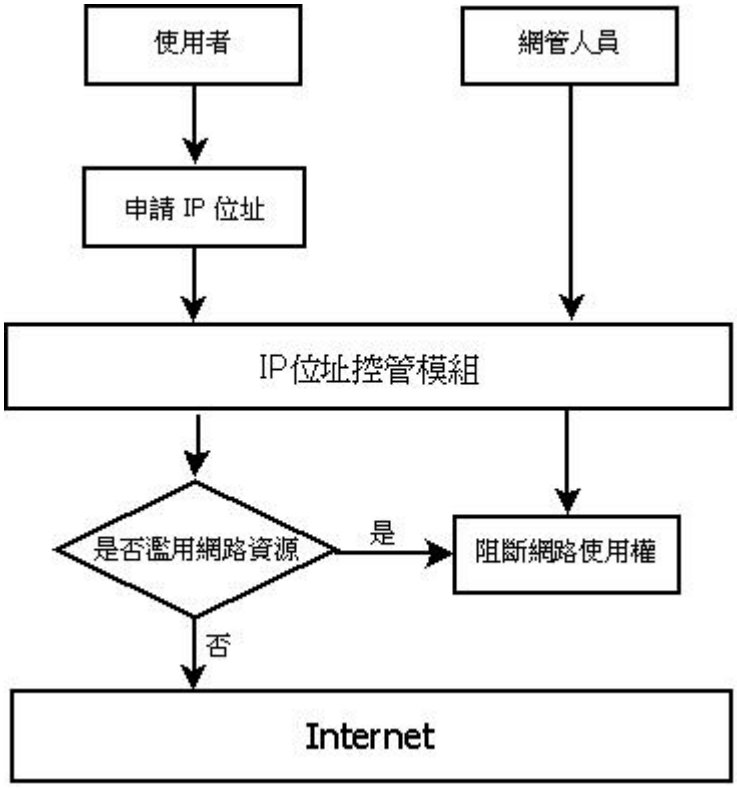

圖 4 - 7 IP 位址管控模組流程

6、IP 位址歷史紀錄模組(IP Log Module, IPLM)：

工作內容：

(1)列出過往所有 IP 位址的使用紀錄。

(2)可依時間、IP 位址與帳號排序。

設計理念：

使用者取得 IP 位址並不是永遠固定的，所以系統必須保留 IP 位址曾被哪位使用者在哪使用過，這樣日後要處理資安問題時，才可以有明確的依據可循。IP 位址歷史紀錄資料表結構如表 4-4。

欄位名稱	欄位型態	欄位說明
ip	char	IP 位址
mac	char	MAC 位址
user_id	varchar	使用者帳號
where_use	varchar	使用單位
start_time	datetime	網路權開通時間
end_time	datetime	網路權結束時間

表 4 - 4 IP 位址歷史紀錄資料表結構

4.3 CIASPA 運作流程

本節針對前一節所提結合身分認證之校園 IP 管理系統架構的運作流程做說明，並將系統運作分為使用者申請程序和管理者控管方面進行介紹，且詳細的描述使用者在透過結合身分認證之校園 IP 管理系統申請網路使用權之便利性。

使用者申請程序共分九個步驟，管理者控管方面共分四模組，以下先分別說明使用者申請程序的每一個步驟，其運作流程如圖所示：

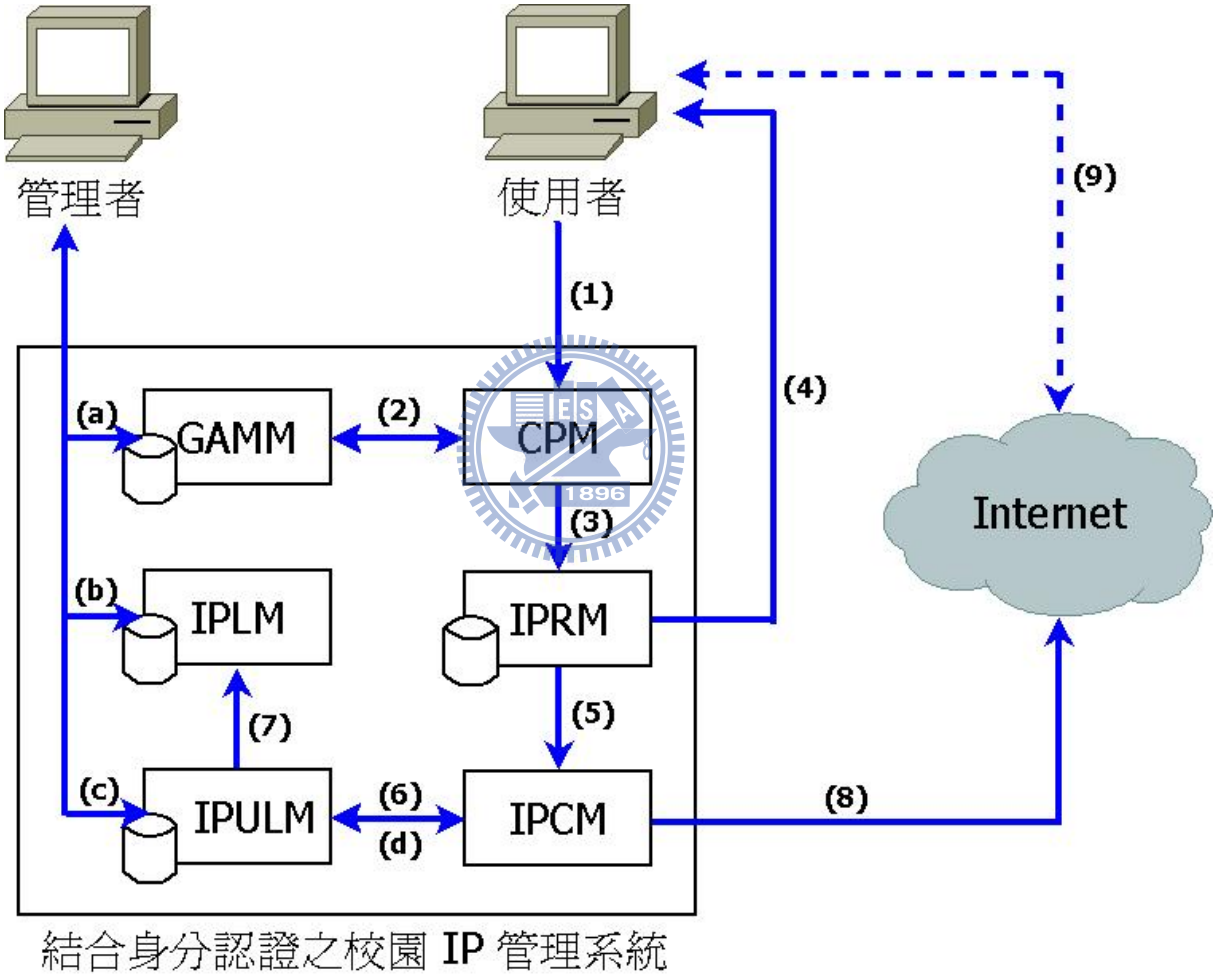

圖 4 - 8 結合身分認證之校園 IP 管理系統流程圖

(1) 使用者 → CPM（網頁認證模組）

使用者打開瀏覽器，不管使用者的網址連往何處，該網址經過 DNS 解析後，通通被導向 CPM 進行認證。

(2) CPM（網頁認證模組）→ GAMM（來賓帳號管理模組）

使用者在 CPM 輸入帳號和密碼進行登入，CPM 會將使用者的帳號和密碼傳送去

GAMM 進行認證，如果不是來賓帳號則進行 Email 認證，並將認證結果傳回 CPM 處理。

(3) CPM（網頁認證模組）→ IPRM（IP 位址註冊模組）

認證成功後，CPM 將畫面轉向 IPRM 讓使用者註冊 IP 資訊，IPRM 會自動抓取使用者的 IP 位址和 MAC 位址呈現在網頁上，讓使用者免去查詢這些資訊的手續而增加操作的簡易性。

(4) IPRM（IP 位址註冊模組）→ 使用者

在 IPRM 中，為了操作上的便利，使用者只需選擇註冊的有效時間和輸入使用單位即可。

(5) IPRM（IP 位址註冊模組）→ IPCM（IP 位址控管模組）

當使用者輸入完畢送出後，系統將這些資訊送往 IPCM 進行網路使用權開通處理；防火牆則會增加該位使用者 IP 位址的網路使用權放行規則，此時使用者的網路使用權將不受阻擋。

(6) IPCM（IP 位址控管模組）→ IPULM（IP 位址使用列表模組）

當 IPCM 處理完網路使用權的開通程序後，即會將這註冊資訊送往 IPULM 進行資料庫儲存，讓網管人員可以線上即可從 IPULM 查詢目前最新最正確的 IP 使用資訊。

(7) IPULM（IP 位址使用列表模組）→IPLM（IP 位址歷史紀錄模組）

在 IPULM 將註冊資訊儲存至資料庫中時，也會將此註冊資訊送往 IPLM 儲存至資料庫中做成歷史紀錄供日後查詢，此歷史紀錄是累加的，能夠一直被保留下來。

(8) IPCM（IP 位址控管模組）→ Internet

使用者的網路使用權在 IPCM 開通後，即可連線至 Internet 存取任何服務，而 IPCM 則會隨時待命接受網管人員的管理命令。

(9) 使用者 → Internet

使用者與 Internet 開始連線，完成 IP 位址註冊動作。

在管理者控管方面，共有四個模組可提供管理者線上控制管理，並直接影響使用者的申請與網路使用權，以下分別說明管理模組與其他模組運作的關係：

(a) 管理者 → GAMM（來賓帳號管理模組）

使用者認證來源在 CPM 中可為單一 Email 伺服器認證，亦可多個 Email 伺服器同時進行認證，為了方便性，此 Email 認證一個帳號可同時開通多部電腦的網路使用權。除了 Email 認證外，網管人員亦可在 GAMM 中進行來賓帳號的產生與列印，為了顧及安全性和容易管理，此來賓帳號有一定的有效期限，此帳號過了期限後則無法被使用，沒過期的一經使用者開通後就不可再被其

他電腦重複使用。

(b) 管理者 → IPLM（IP 位址歷史紀錄模組）

不當使用網路資源的使用者如果不是當下發現處理，而是過了許久才被發現需要調 IP 位址紀錄時，網管人員即可以透過 IPLM 進行線上搜尋調閱，快速找到有問題的 IP 位址是誰使用的。

(c) 管理者 → IPULM（IP 位址使用列表模組）

網管人員如需要得知校園目前 IP 位址資訊，即可以在網頁上透過 IPULM 列表出來。

(d) IPULM（IP 位址使用列表模組）→IPCM（IP 位址控管模組）

在 IPULM 可詳細的列出所有使用的 IP 位址資訊，如哪個 IP 位址濫用網路資源，網管人員即可在 IPULM 選擇該 IP 位址進入 IPCM 進行網路使用權的阻擋管理。

第五章 系統建置與實作

經過第四章詳細的介紹系統規劃與設計重點之後，本章節將所有的想法付諸實現，依照設計的理念逐步建置完成，之後再說明系統的成效。因此本章節將先介紹本系統的建置環境，接著對系統模組開發所需要的技術做說明，並以實作出來的畫面展示本系統的成果，最後再對本系統實作後的結果與前述系統做比較。

5.1 系統建置環境

本研究在不更動現有的環境設備下，如圖 5-1，希望能以校園中原有的伺服器來安裝本系統，減少硬體經費的支出，接著考量到跨平台的特性，在選擇網頁伺服器軟體時就必須考量系統相容性的問題，而系統的建置成本也是要考量在其中，所以我們選用自由軟體來節省軟體購置的經費，因此本系統在網頁伺服器選擇，採用免費且穩定的 Apache Server 來建置。

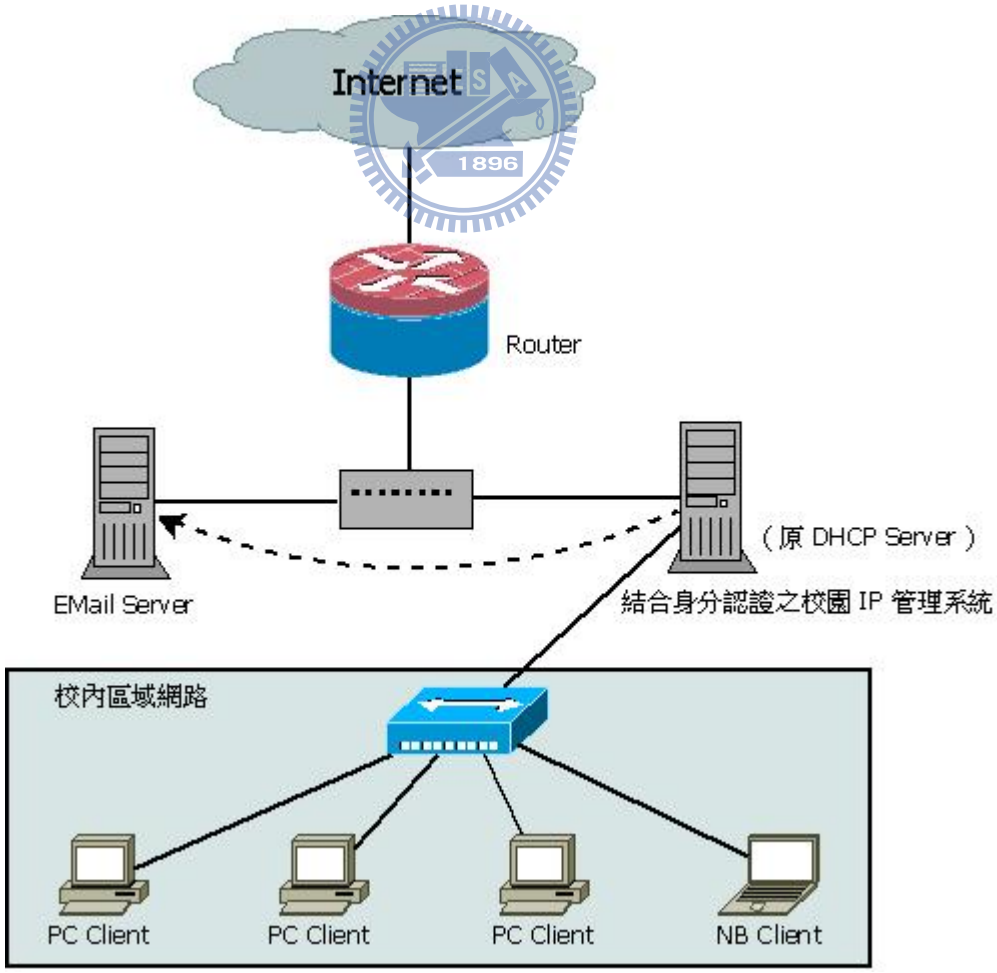

圖 5 - 1 校園網路架構圖

由於 Apache Server 可以在許多平台上執行，但在經費拮据情況下，和考慮到系統整體的運作效能與穩定性，我們採用了 Unix-like 的作業系統 FreeBSD 作為開發平台，在 IP 位址管理方面，使用了 DHCP Server 作為 IP 位址自動分配管理和 IPFW 防火牆管理網路封包的進出和網址導向，在網頁程式語言方面，則配合 Apache Server 使用免費的 PHP 作為程式開發語言，最後在資料儲存上，採用免費的且操作簡易的 MySQL 作為資料庫管理系統。而本系統所採用的硬體及軟體套件版本詳列如表 5-1，可供系統建置之參考。

用途	套件名稱及版本
硬體環境	
- CPU	Intel(R) Pentium(R) 4 CPU 3.00GHz
- RAM	1G
- HD	80G
- 對內網路卡	Marvell/SysKonnect Yukon II Gigabit Ethernet
- 對外網路卡	RealTek 8129/8139
作業系統	FreeBSD 7.2-Release
防火牆	ipfw
IP 位址管理軟體	isc-dhcp 3.0.7
伺服器軟體	
- 網頁伺服器	Apache 2.2.14
- 資料庫	MySQL 5.1.41
開發工具	
- 伺服器端網頁程式語言	PHP 5.2.11
- 資料庫管理介面	phpMyAdmin 3.1.3.2

表 5 - 1 系統建置硬體及軟體套件版本

5.2 系統模組開發

本系統是一套能滿足國中小網管人員管理校園 IP 位址業務需求的結合身分認證之校園 IP 管理系統，所以在模組開發上，我們採用 Web-Based 作為系統的介面，以方便使用者與管理者操作。使用者在申請 IP 位址進行網路使用權開通時，認證後只需填入使用單位和選擇使用期限即可，IP 位址和 MAC 位址則由系統自動抓取，不增加申請的難度，如圖 5-2 為使用者 IP 位址申請畫面。而管理者在系統基本設定完成後，可隨時線上查詢 IP 位址使用資訊，不必時時擔心 IP 位址資訊是否有問題，如圖 5-3 為管理者操作畫面。

圖 5 - 2 使用者 IP 位址申請畫面

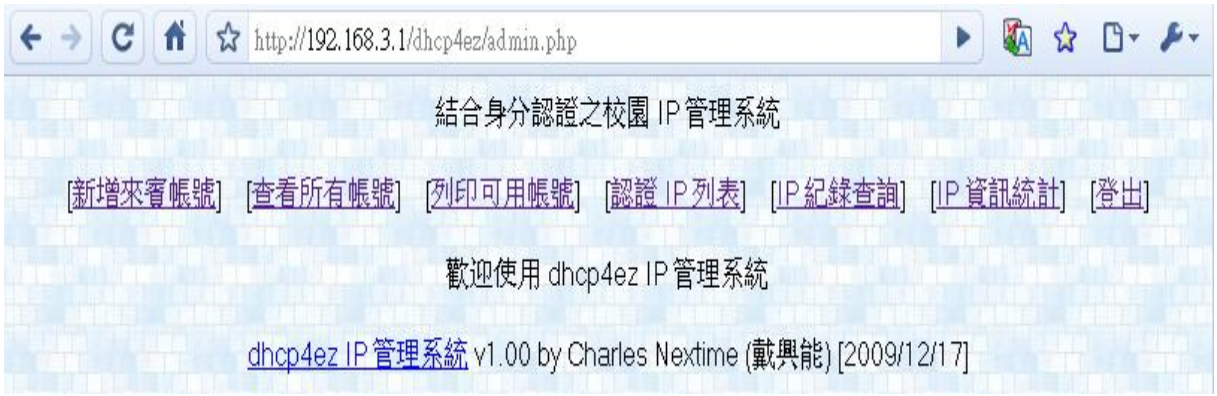

圖 5 - 3 管理者操作畫面

下面我們就針對各模組的開發逐一的介紹：

1、網頁認證模組(Captive Portal Module, CPM)：

由於本系統要阻斷未申請 IP 位址的使用者之網路使用權，並將其網頁強制導向認證網頁，所以必須在防火牆的設定著手，使未申請者的網路封包通通導向認證伺服器主機中。如圖 5-4 為 IPFW 將未認證的封包通通導向認證主機設定。

```
${fwcmd} 5700 fwd 192.168.3.1 tcp from 192.168.3.0/24 to any
${fwcmd} 5800 skipto 6000 udp from 192.168.3.0/24 to any 53 out
${fwcmd} 5900 fwd 192.168.3.1 udp from 192.168.3.0/24 to any
${fwcmd} 6000 divert natd all from any to any in via ${oif}
```

圖 5 - 4 IPFW 將未認證的封包通通導向認證伺服器主機設定

本系統網頁認證模組能夠將未申請 IP 位址的使用者之任可網頁導向認證網頁，如圖 5-5 所示，這是因為透過 Apache Server 本身功能來設定直接重導向，除了能導向網址為網域名稱(Fully Qualified Domain Name, FQDN)或 IP 位址，也能正確的導向前述網址中含有參數的，改良「HTTP 302 重導向」的 HTTP 狀態 302 可能被瀏覽器誤認為非法連線的問題，如圖 5-6 為 Apache 重導向設定。

圖 5 - 5 未申請者的網頁自動導向認證網頁

```
# 設定本機管理 ip，此 ip 不會強迫導向 dhcp4ez 認證
<VirtualHost 192.168.3.1:80>
    DocumentRoot /usr/local/www/apache22/data
</VirtualHost>

# 連往其他 ip 則通通強迫導向 dhcp4ez 認證
<VirtualHost *:80>
    DocumentRoot /usr/local/www/apache22/data/dhcp4ez
</VirtualHost>

# 網址有誤時，導向根目錄
ErrorDocument 404 "/"
```

圖 5 - 6 Apache 重導向設定

此網頁認證模組可以提供來賓帳號和跨校 Email 認證機制，是先透過 PHP 語法判斷帳號身分別為何，再進行對應的認證程序。如圖 5-7 為跨校 Email 認證機制陣列設定。

```
// ==================== 認證伺服器 相關設定 ======================
$AuthMailHost = array ( // 第一筆為預設認證伺服器，帳號不用打 @host
    "mail.abc.edu.tw" => "192.168.3.2:pop3:110",
    "mail.cdf.edu.tw" => "192.168.4.1:pop3:110",
    "home" => "192.168.3.2:pop3:110"
  );  // "EMail host" => " Auth IP:pop3:110", (pop3:110, imap:143)
```

圖 5 - 7 跨校 Email 認證機制陣列設定

2、IP 位址註冊模組(IP Register Module, IPRM)：

本模組為了能讓使用者方便的進行 IP 位址註冊程序，系統透過伺服器網頁資訊($_SERVER['REMOTE_ADDR'])和 arp 指令自動化查詢使用者的 IP 位址和 MAC 位址，如圖 5-8 為使用者申請 IP 位址畫面，使用者只要簡單的輸入使用單位即可註冊完成，在有效期限內網路使用權為一直開通不須再註冊，不會造成太多的使用負擔，而使用單位那項是屬於使用者自行管理的項目，如果遇到問題時，網管人員得依據認證的帳號進行詢問，並會同使用者前往處理有問題的電腦。

圖 5 - 8 使用者申請 IP 位址畫面

註冊完成後，在三秒內系統會自動化將網路使用權開通，大大減少使用者等待開通時間和網管人員作業負擔，如圖 5-9 為 IP 位址申請後畫面。開通後，本模組會依據使用者未認證前原本的網址進行自動轉址，此技術為透過伺服器網頁資訊抓取 $_SERVER["SERVER_NAME"] 與 $_SERVER["REQUEST_URI"] 達成自動化轉址服務。

圖 5 - 9 IP 位址申請後畫面

3、來賓帳號管理模組(Guest Account Management Module, GAMM)：

本系統提供跨校 EMail 伺服器認證服務，管理者可以設定許多組 POP3 Server 來同時進行認證，使用者只要在帳號欄位輸入完整的 EMail 信箱，系統就會自動判斷去設定好的 POP3 Server 認證，雖然可以方便的進行設定，但有

時候其他學校不提供 POP3 Server 時，就無法進行註冊打開網路使用權了，所以本模組提供臨時的來賓帳號服務，讓認證方式更彈性化，服務更周全。圖 5-10 為建立來賓帳號畫面，可以選擇一次建立多少組來賓帳號和開通後有效時間，而在系統內部管理者可調整來賓帳號要用什麼字串為開頭、流水帳號為幾位數、密碼共幾位數和密碼開頭英文字母等設定，如圖 5-11 為來賓帳號系統設定細項。

圖 5 – 10 建立來賓帳號畫面

```
$GuestAcc = "guest";                          // 來賓帳號開頭
$GuestMaxNum = "4";                           // 流水帳號最大位數(最大爲 7)
$GuestMaxPwd = "5";                           // 來賓密碼個數
$GuestDelDay = "7";                           // guest 有效天數
$GuestAddNum = "10";                          // 預設建立幾組 guest 帳號
$PwdStart = "a c d e f h j k m p s t u w x y"; // 密碼以什麼開頭
```

圖 5 – 11 來賓帳號系統設定細項

圖 5-12 為來賓帳號建立完成畫面，可以看見帳號以 guest 開頭並加上 4 位數的流水號，如果建立到 9999 時則會從 0001 開始重新使用，使用過或未使用而到期的帳號，將會被系統自動刪除，減少資源的浪費，在密碼部分考慮到方便性和安全性，則以單一字母為開頭，後面接 4 個數字作為簡易型拋棄密碼使用。

圖 5 - 12 來賓帳號建立完成畫面

4、IP 位址使用列表模組(IP Using List Module, IPULM)：

此模組可以列出目前已註冊的 IP 位址資訊，包含 IP 位址、MAC 位址、使用者、使用單位、開通時間和重新認證時間等項目，如圖 5-13 為已申請 IP 位址的使用列表，在此列表中，網管人員可以清楚了解目前校園 IP 位址被使用的情形，隨時掌握 IP 位址使用量。

圖 5 - 13 已申請 IP 位址的使用列表

5、IP 位址控管模組(IP Control Module, IPCM)：

在 IP 位址使用列表模組中，如果想對某個 IP 位址進行管控時，只要點選該 IP 位址即可進入 IP 位址控管模組，如圖 5-14 為單一 IP 位址的網路使用權設定。對於使用者濫用網路資源經勸導無效時，此模組中可以設定此 IP 位址禁用和限速的天數，讓校園網路隨時保持通暢。

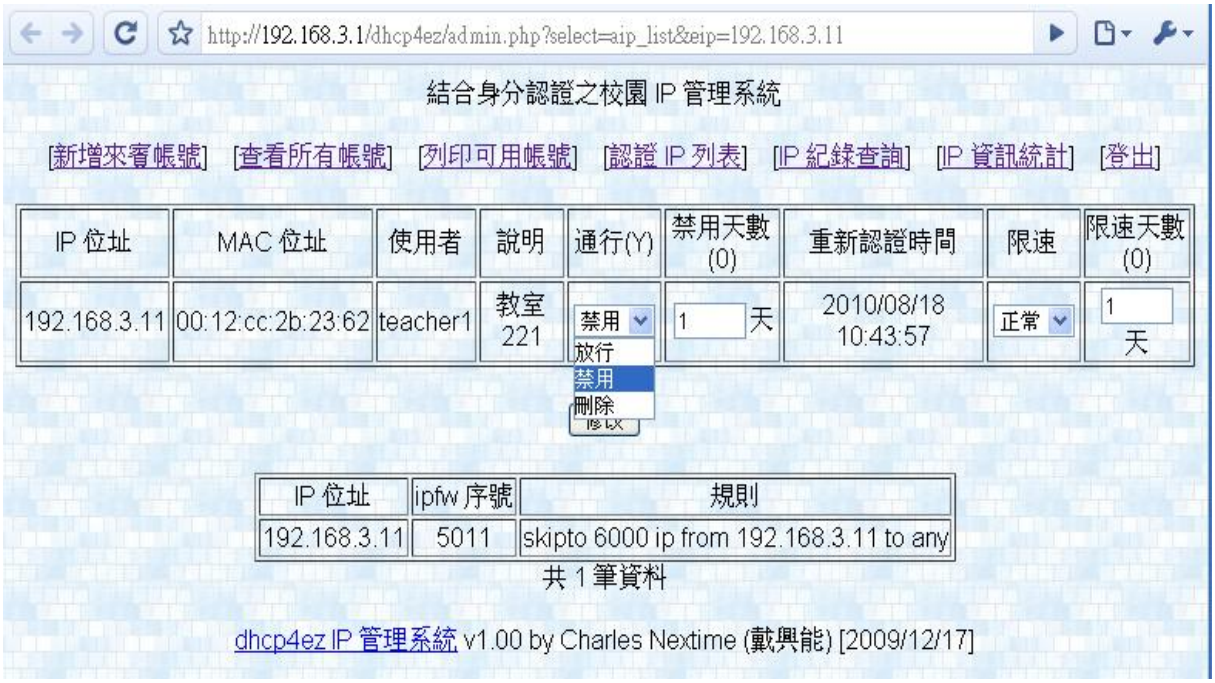

圖 5 - 14 單一 IP 位址的網路使用權設定

6、IP 位址歷史紀錄模組(IP Log Module, IPLM)：

當使用者認證進行 IP 位址註冊後，系統即會將相關資料即時的存入資料庫中，如果未來有資安問題時可以隨時查詢 IP 位址歷史紀錄，如圖 5-15 為查詢 IP 位址紀錄畫面。

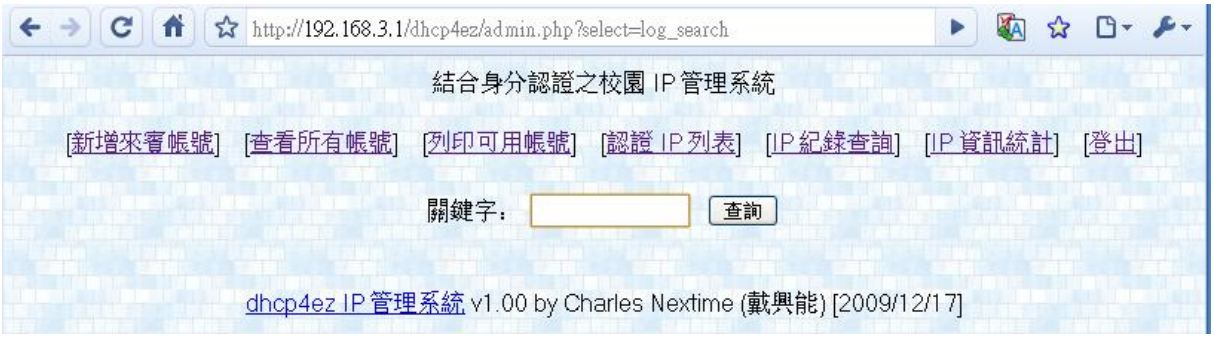

圖 5 - 15 查詢 IP 位址紀錄畫面

在此模組中，可以輸入要查詢的關鍵字進行篩選，或是不輸入任何文字進行全部輸出，假定我們以「科任」為關鍵字進行查詢，如圖 5-16 為查詢 IP 位址紀錄結果畫面，我們可以清楚看到欄位中含有「科任」的 IP 位址會被篩選出來，在這 IP 位址歷史紀錄中，包含了使用者、IP 位址、MAC 位址、使用單位、申請時間和結束時間等資訊供查詢使用。

圖 5 - 16 查詢 IP 位址紀錄結果畫面

5.3 系統成效與比較

本研究所提的結合身分認證之校園 IP 管理系統是在不變更使用者環境、不增加額外費用的情況下，希望能藉此簡化網管人員管理 IP 位址的業務、提高行政效率。不管是使用者或是網管人員的使用界面都採用網頁式操作，更方便、更有親和力，所以使用者不必額外教育即可馬上進行 IP 位址的申請，達到 IP 位址管理的成效，使校園網路保持暢通。

校園 IP 址位管理隨著科技進步與網路環境的影響，管理的方式就不同，本系統提供了許多便利服務與優點，以下將說明採用本系統後所產生的成效，接著將本系統與第三章各學者所提的系統做比較。

系統成效：

未使用本系統之前，校園 IP 位址的管理雖然是採 DHCP 自動取得分配給使用者，但網管人員並不知這些 IP 位址分別被哪個使用者所使用，遇到 IP 位址問題時，一般的管網人員只能束手無策，而進階的網管人員可以利用 IP 位址查詢小軟體找到 IP 位址與電腦名稱的對應，但每部電腦的電腦名稱是可以隨使用者的設定而更動，並不是百分之分正確，所以常常要花許多時間去核對 IP 位址與使用者的正確性，網管人員在此花費時間是一種無效率的浪費。

使用本系統之後，校園 IP 位址的管理依然採 DHCP 自動取得分配的方式給使用者，但使用者要使用網路權時，必須透過網頁認證並註冊後才可通行，如此網管人員可在本系統隨時查詢最新最正確的 IP 位址使用資訊，遇到 IP 位址問題時，只要進入管理模式，馬上得知有問題的 IP 位址是誰所註冊，減少找依 IP 位址找電腦的時間，增加問題解決的效率，如圖 5-17 為使用本系統前後，網管人員依 IP 位址找電腦花費時間成效圖。

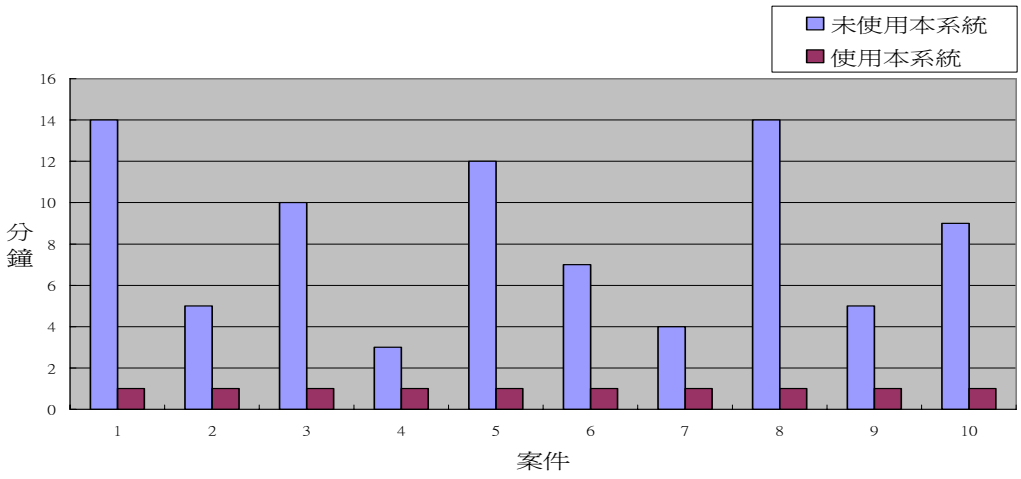

圖 5 - 17 依 IP 位址找電腦花費時間成效圖

系統比較：

本系統與第三章各學者所提的系統做比較，如表 5-2 為本研究系統與各學者所提的 IP 位址管理系統比較表。

	本研究的系統	劉則明等三人（2005）	曾憲民（2007）	楊有信（2008）
認證配合方式	POP3/來賓帳號	填寫註冊單	填寫註冊單	AD Server
阻擋未認證者之網路使用權	是	是	否	是
自動開通網路使用權	是	否	否	是
支援來賓設定	是	否	否	否
對使用者限制網路流量	是	否	否	否
支援網路使用權開通期限	是	否	否	否
網路環境建置	簡單	困難	簡單	困難
線上管控網路使用權	是	是	是	否

表 5 - 2 本研究系統與各學者所提的 IP 位址管理系統比較表

第六章 結論與未來方向

近年來各學校電腦數量愈來愈多，隨之而來的 IP 位址管理問題和網路使用權管制方式，都一直困擾者許多網管人員，雖然各單位都有自己的一套政策來管理，對問題的處理也各有所異，但網路環境設備和操作方式則為各校選用的重要考量，對於經費拮据的國中小學來說，如果要額外採購許多網路設備來達成，實為一筆很大的負擔，本研究採用自由軟體實作一套結合身分認證之校園 IP 管理系統，以極低的成本達到 IP 位址管理和網路使用權管制效果。

6.1 結論

本研究為解決 IP 位址管理問題，利用現有的硬體設備，在不變更使用者環境、不增加額外費用下，提出一個適用於國中小結合身分認證之校園 IP 管理系統，其主要目的在於：

1、解決網路使用權管制問題。

2、解決人工管理 IP 位址費時費工的問題。

3、解決 IP 位址被誤用問題。

針對這些目的，本研究所提出的解決方案分別是：

1、透過網頁認證機制，使用者在未認證前，瀏覽器的網頁會自動導向認證介面進行認證，而認證過的使用者才能有網路使用權。

2、配合認證機制，利用網頁式介面讓使用者為自己的電腦 IP 位址和 MAC 位址進行註冊，使用者只要輸入使用單位和選擇有限期限即可註冊完成，讓 IP 位址資訊保持最新最正確。

3、如果使用者私下改 IP 位址，將會導致 IP 位址發生衝突或者資安問題無法求證，所以在本系統使用 arp 指令將 IP 位址和 MAC 位址進行 arp 靜態綁定，如果亂改 IP 位址，其網路將無法連線。

除此之外，本研究根據本系統架構實作一套結合身分認證之校園 IP 管理系統，來說明本系統架構的可行性，並證明這個結合身分認證之校園 IP 管理系統的確能解決以上所提的問題。

6.2 未來方向

本論文提出的方案可以有效管理 IP 位址，但尚有未臻完美之處，未來本研究可朝三個方向進行：

1、系統跨平台安裝：

本究研的系統分內部防火牆和外部操作程式，操作介面為網頁式服務，為 Apache 網頁服務和 PHP 語言所提供，可跨平台安裝使用，但內部防火牆則是在 FreeBSD 作業系統開發而成，適用 IPFW 防火牆設定。然而有許多學校採用 Linux 作業系統，其中防火牆則為 iptable，本研究的系統在此則無法運作，日後若可加入此功能則可以更方便安裝使用。

2、系統基本設定網頁化：

在使用本研究的系統之前，網管人員需要用編輯器去調整一些系統基本設定，雖然只需調整一次即可，但對於網管人員管理設定的便利性還可以再加強，未來若將這些設定通通進入資料庫，網管人員就可以透過網頁設定，讓安裝的步驟更簡單和容易。

3、支援 IPv6：

隨著科技的發達，IP 位址逐漸不敷使用，為了解決目前 IP 位址短缺的問題，IPv6 協議將取代現行 IPv4 版本，而本研究的系統只支援 IPv4 版本，若他日能增加對 IPv6 版本的支援，其適用性將大大提高。

參考文獻

[1] Dynamic Host Configuration Protocol. Available from: http://tools.ietf.org/html/rfc2131

[2] FreeBSD. Available from: http://www.freebsd.org/

[3] Apache. Available from: http://httpd.apache.org/

[4] PHP. Available from: http://php.net/index.php

[5] MySQL. Available from: http://www.mysql.com/

[6] IPFW. Available from: http://www.freebsd.org/doc/handbook/firewalls-ipfw.html

[7] TCP/IP. Available from: http://zh.wikipedia.org/zh-tw/Tcp/ip

[8] Internet Protocol Suite. Available from: http://en.wikipedia.org/wiki/Tcp/ip

[9] OSI 模型. Available from: http://zh.wikipedia.org/zh-tw/OSI 模型

[10] DHCP. Available from: http://zh.wikipedia.org/zh-tw/DHCP

[11] 王俊斌，FreeBSD 6.0 架設管理與應用，博碩文化，台灣，2005。

[12] ARP. Available from: http://zh.wikipedia.org/zh-tw/ARP

[13] An Ethernet Address Resolution Protocol. Available from: http://tools.ietf.org/html/rfc826

[14] ARP 協定. Available from:http://www.study-area.org/network/network_ip_arp.htm

[15] 網路交換器. Available from:http://zh.wikipedia.org/zh-tw/網路交換器

[16] Access control list. Available from: http://en.wikipedia.org/wiki/Access_control_list

[17] Captive portal. Available from: http://en.wikipedia.org/wiki/Captive_portal

[18] Whitelist. Available from: http://en.wikipedia.org/wiki/Whitelist

[19] HTTP 302 Status Code. Available from: http://tools.ietf.org/html/rfc2616#page-62

[20] 林碧華，一個可調適之 IP 位址分配與管理系統，逢甲大學資訊工程學系碩士班論文，2001。

[21] 曾憲民，非法連網自動偵測與資源效能監控機制，國立東華大學資訊工程學系碩士論文，2007。

[22] 劉則明、程毓明、刁建成，自動化宿舍網路註冊管理系統，高苑學報第十一卷，2005。

[23] Robert Beck, ”Dealing with Public Ethernet Jacks – Switches, Gateways, and Authentication,” University of Alberta, USA, November 1999.

[24] 楊有信，校園網路中用戶身分認證過濾系統之實作，中華大學資訊工程學系碩士班碩士論文，2008。