校園無線網際網路允入控制與管理

宣拔、邱仁成、賴坤助、竇其仁

逢甲大學資訊工程學系

台中市 407 西屯區文華路 100 號

E-mails：{reihino,chad}@pluto.iecs.fcu.edu.tw, {kclai,crdow}@fcu.edu.tw

摘要

無線網路，這個技術雖然帶來了許多的便利，只要有無線網路卡，隨時隨地都可以享受無線網路的便利。但是，背後卻隱藏著一些安全性的問題，而最大的問題是如何管理無線網路下的使用者，且不能讓使用者有太多繁瑣的系統設定，就能夠在所有的系統中都能夠正常的運作。無線網路允入控制器的發展設計即是用來管理無線網路下的使用者。

關鍵詞：無線網路(Wireless Network)、RADIUS、netfilter、DHCP、iptables。

一、緒論

大部分的學校陸續建置了校園無線網路的環境，雖然提供使用者便利的網際網路服務，但是經常忽略了對使用者的管理，如果說有心人士想要從事不正當的行為，只要走到學校，把筆記型電腦插上無線網路卡，就能夠採取任何行動，最後學校必須為他的行為負責。有鑑於此，我們設計了一個能夠管理使用者的方法，並使用 RADIUS 和 DHCP 技術，讓使用者對電腦的系統設定做最小的更動，就能夠進入這個被管理的網路達到人員管理的目的。

本文主要是針對逢甲大學校園無線區域網路環境來進行討論並提出一個動態 IP 調整機制，和使用者認證和認證管理介面。我們除了實作了一個 Web-based 使用者介面的「DHCP 管理系統」，和無線網路認證管理系統外，並且探討無線區域網路環境下的相關問題，其中包含：無線網路環境中使用者上網之使用行為分析等，我們的研究具有下列的特色：

（1）實作一個具 Web-based 使用界面的「DHCP 管理系統」，具備了 DHCP 動態分配網際網路位址的功能。

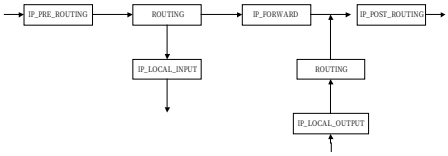
（2）提出一個認證管理的方法，讓未經授權的使用者能夠受控制，不能向外存取 Internet。並使用 RADIUS 作為認證的核心，紀錄使用者的上下線時間。

（3）實作一個無線網路認證和認證管理的介面，讓使用者能透過此介面輕鬆地和 RADIUS 伺服器要求認證服務。讓網管人員能夠透過認證管理的介面，管理經過授權的使用者。

二、相關研究

由於 IEEE 802.11 標準的出現，藉由無線區域網路的種種優勢，使得有線區域網路的型態大為改變；所以具有高移動性、不須架設線路等特性的無線區域網路，近年來在各種特殊場合大出風頭，應用有越來越普遍的趨勢。因為無線網路的便利性，造成了整個網路存取的安全性降低。與無線網路安全性相關的研究相當多，我們將針對較主要的部分 Linux netfilter 及 RADIUS，做為無線網路允入機制的理論基礎。

2.1 Linux netfilter



圖一、netfilter 架構圖

Netfilter[5]是 Linux 2.4 中所發展的一個 packet 過濾的機制，它屬於 Linux 2.4 核心中的一個子系統。能夠對每個封包做標注、過濾、偽裝以及改寫封包。它使用 iptables[6]這個使用者階層的應用程式讓使用者能夠設定核心組態。

在 netfilter 中，它具有下列的基本動作，分別是 ACCEPT 讓封包直接通過、DROP 直接丟棄封包、RETURN 直接返回以及 QUEUE 將封包交給使用者階層的應用程式處理。Netfilter 如圖一，分成了幾個內建的 chain 分別是 PREROUTING 封包進入時第一個會進入的 chain、INPUT 當封包要進入本機時所要進入的 chain、FORWARD 當封包通過 routing table 後但封包不屬於本機時所進入的 chain 以及 OUTPUT 當封包要送至網路上之前所通過的 chain。並以功能面分成三個 table 分別是 filter 專門用來過濾封包、nat 用來對封包做偽裝以及 mangle 用來修改以及標註封包。

當封包進入時，經過判斷出為正確的封包後第一個送到 IP_PRE_ROUTING 來檢查封包如果通過這個檢查，再交給 Linux 核心的 routing table 判斷這個封包要去哪裡。

（1） 如果是要送給本機的，則將封包傳送給 IP_LOCAL_INPUT 來檢查。

（2）如果封包是要從一個實體介面傳遞到另一個實體介面則交給 IP_FORWARD 檢查，也就是說經過 routing table 的比對後，封包不屬於本機則送至 IP_FORWARD。

（3） 當封包通過之前的檢查後，最後交給 IP_POST_ROUTING 檢查，最後傳送到實體層的傳輸媒體上。

（4） 如果封包是由本機產生的，則交給 IP_LOCAL_OUTPUT 來檢查。

當封包和某個規則相符合時，它就會依照該規則的規定處理，而以下的規則將不再比對。

2.2 RADIUS

RADIUS[3-4,10]的主要特色如下

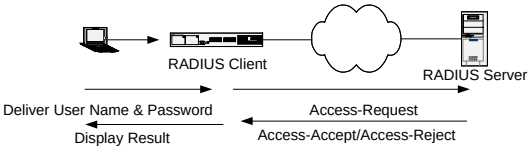
（1） Client / Server Model：RADIUS client 主要任務是傳送客戶的資訊給 RADIUS server 以及對 RADIUS server 的回應採取一些相關的動作。RADIUS server 負責接收 client 的要求、對客戶作認證、以及回應一些相關的設定訊息給 RADIUS client，RADIUS client 再以這些回應的資料對客戶開啟服務。RADIUS server 也可以以 proxy client 的形式存在於 RADIUS server 和 client 之間。當 RADIUS Server 當機或毀損時，RADIUS client 可以在選擇其他台 RADIUS Server (連接在同一使用者資料庫)要求認證服務。

（2） Network Security：Client 和 RADIUS Server 之間存在一組 shared secret，而這組 shared secret 並不會被傳送到 Internet。Client 和 Server 之間都會把資料經過加密才送至不安全的 Internet 傳送至對方，這樣的機制能降低資料再傳遞時被一些惡意的竊聽者將資料攔截。

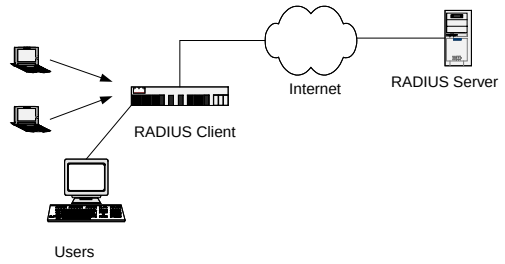
（3） Flexibility Authentication Mechanism：RADIUS 提供許多種的方式來對客戶作認證，當客戶使用他們的使用者名稱和密碼作認證時，RADIUS 可支援 PPP、PAP、CHAP、UNIX Login，和其他的認證方式幫使用者做認證。

RADIUS 架構如圖三，RADIUS 認證過程如圖二，當使用者向 RADIUS Client 要求服務時，則 RADIUS Client 會將使用者的使用者名稱和使用者密碼傳送給 RADIUS Server，讓 RADIUS Server 來對這個使用者做驗證，當通

過驗證時，則會回應一個訊息，其中包含了該使用者的服務類型。RADIUS client 一收到這個訊息，就依照回應的內容，提供該使用者所應有的服務。



圖二、RADIUS 過程



圖三、RADIUS 架構

三、系統架構

本節將要介紹無線網路允入控制器的架構，以及建置時的拓樸。

3.1 校園無線網路的規劃

由於逢甲校園獨特，屬於都會區建築物密度較高的學校，為能有效規劃無線網路，並達到最佳化服務品質的效果。因此我們在規劃無線網路建置地點前先針對室內、室外的無線特性進行測試，測試項目包含有樓層與樓層的無線有效範圍量測、建築物與建築物的無線有效範圍量測、校園內空曠地點之無線有效範圍量測及 AP 與 AP 之間漫遊之量測，經過分析後再依環境及需求的不同，考量下列因素後，規劃出最佳化網路品質的無線網路建置地點。

無線網路實際安裝考量：

（1）需要性：室內外各種不同需求環境

（2）公平性：各大樓，系所，樓層

（3）安全性：避免設備遺失

（4）美觀性：Access points 與 Power lines

（5）方便維護性

（6）其他：（含建置成本考量）

3.2 設備需求

無線網路設備基本上包括兩個部份，一是存取主機，也就是所謂的無線橋接器（Access Point，AP），連接有線的區域網路，在有線的乙太網路和無線的連結之間進行轉換的動作；AP 包括了連接到區域網路的集線器或交換器的 10Base-T 網路線連接埠、通訊和加密軟體，以及一個無線電收發器。另一個部份為使用者端的網路配接器，一般是單片無線網路卡的形式，安裝在攜帶性的通訊裝置上。

3.3 無線網路認証的建置

逢甲校園無線網路建置完成後，校內會議室的無線含蓋率已可達 100%，室外無線漫遊範圍亦可含蓋約校園的 70%左右，也就是在校園的許多地方都可以隨時利用無線來上網，某些 AP 位置的漫遊範圍甚至可以含蓋到校外區域，所以如果沒有對無線上網作任何的限制，任何人只要帶著筆記型電腦插上無線網路卡，在訊號接收範圍內就都可以自由的上網，當然這也包含可能是非學校人員利用學校無線網路資源直接上網，因此無線網路使用的管理就更加的重要。

目前在無線網路使用的管理分三方面[1]：

（1） 無線網路卡的管理：我們設立一部認證伺服器(RADUIS Server)來對網路卡進行認證，在每一片無線網路卡上皆有唯一的 Mac Address，因此在認證上為對無線網路卡的 Mac Address 進行查驗，所有要進入無線網路者，其網路卡的資料都必須在認證伺服器有登記才可以使用。在無線網路卡方面可分為學校免費提供租借及使用者自備兩種。

（2） 在網路的管理方面：現在所有的 AP 都

可支援 SNMP，所以可將無線網路納入校園網路監視系統中，透過網管系統監控無線網路設備的狀況，若有任何一部 AP 發生問題時都可很快的發現，並前往處理。另外 AP 本身亦提供了一個管理軟體，透過這個管理介面我們可以知道這個 AP 的網路流量、連線的機器、連線的品質等等，透過對這些資料的分析可以有效的對無線網路設備進行管理。

（3） 無線網路 IP 的管理：為了有效管理全校 IP 位址的使用，並讓全校師生帶著他們的筆記型電腦便能隨時且輕鬆的連上網路，使用 DHCP[2,7-8]架構動態的配置 IP 位址給使用者，並透過 AP 管理軟體，管理 IP 的使用及網路卡 Mac Address 的設定；如此，網路管理者不但可集中管理 IP 位址，而且只要將 IP 位址配置資料規劃設定好，就可自動將使用者所需 IP 位址及網路環境資料傳送給使用者，並自動設定完成，使用者不須做任何設定即可連上網際網路，不僅簡化繁瑣的網路設定，更可減輕網路管理者的負擔。

3.4 使用無線網路允入控制器

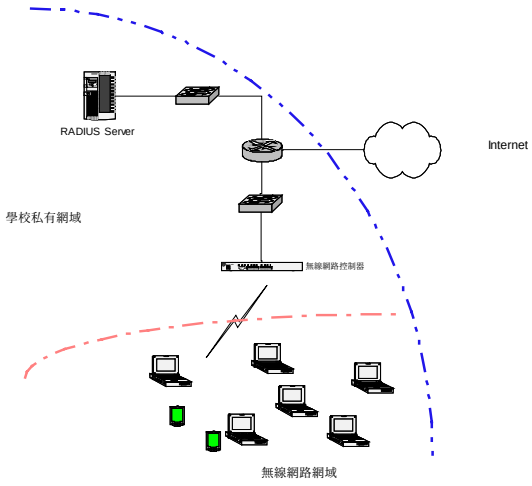
管理使用者存取無線網路，透過 RADIUS Server 和一個記錄著使用者名稱和密碼的使用者資料庫，所有的無線網路使用者都必須要經過 Web-based 的認證方式，向 RADIUS Server 請求認證，當無線網路控制器收到 RADIUS 的回應，如果認證成功則將該使用者的存取權開放，反之則否。這樣一來只要維持資料庫裡的使用者資料以及上下線時間紀錄，完全不需要考慮無線網路卡 MAC Address 的問題。

3.5 系統簡介

無線網路允入控制器，是以嵌入式 Linux 為基礎，燒錄在 ROM 上的一個小型的系統，並且能在傳統無線網路系統下提供無線網路認證管理，不讓使用者能夠任意使用網路資源，以及能夠管理網路頻寬，讓使用者能夠在有品質的頻寬下，使用網路資源，並使用 NAT 技術來減少對真實 IP 的需要。由於機器上並無硬碟等容易損壞的設備，硬體故障率低，節省置換硬體的成本。

3.6 認證機制建置

將無線網路允入控制器安置在無線網路的出口點如圖四，以控制整個網路的出入，將 RADIUS Server 安置在校內網路或是 Internet 上，以接受無線網路控制器的認證要求。使用者透過控制器本身的 DHCP Server 取得 IP Address，當使用者欲使用瀏覽器瀏覽網頁時，都會被強制導向到一個預設的認證畫面，經由輸入



圖四、允入控制器安裝架構

使用者名稱和密碼，以及 RADIUS Server 的驗證，確定使用者的身分，才能夠讓使用者存取無線網路以外的網路資源。當使用者使用網路對外存取網站時，無論如何，他都只能連接到“無線網路登入畫面”，要求使用者輸入正確的使用者名稱以及密碼，或只能在允許的網路範圍裡活動(預設逢甲首頁)，當使用者輸入資料後，經過內建的使用者資料庫比對，或透過內建的 RADIUS Client 程式向外面的 RADIUS 伺服器要求認證，如果回應是正確

的，則將給予存取權，反之則否。當管理員進入“無線網路認證管理畫面”時，可以看到目前在線上的使用者，故可以對使用者作強制斷線的動作，也就是說強制中斷使用者使用連外頻寬的權利。如果使用內建使用者資料庫作為認證方式時，則會多出一個使用者和密碼的對應表，以便管理者維護內建的使用者名稱以及密碼對應表。

四、系統雛形

這裡將介紹無線網路允入管理器的運作以及使用者介面。

4.1 使用者登入與管理

當所有的使用者經由無線網路允入控制器中的 DHCP 服務中取得 IP 位址後，使用者一開啟瀏覽器，無論連到何處，就只能在我們允取的範圍，以及無線網路認證登入的畫面活動，直到使用者經過無線網路認證登入的畫面(如圖五)輸入使用者名稱以及密碼，通過 RADIUS Server 的驗證，才能存取 Internet 或是限定的網路區域。

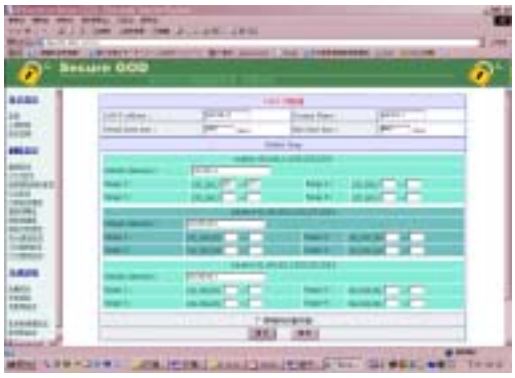
網路管理員可以透過無線網路允入控制器裡的無線認證管理介面(如圖六)，來對已經登入的使用者加以管理。包含了強制使用者登出，以及 RADIUS 設定，和認證方式切換。目前的認證方式有 RADIUS 以及內建使用者資料庫這兩種模式。

圖五、無線網路認證登入

圖六、無線網路認證管理

4.2 DHCP Server 管理

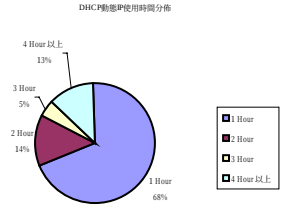
網路管理員可以透過 DHCP 管理的介面如圖七，來設定無線網路允入控制器內建的 DHCP Serve，可支援多重區域網路，每個網路可支援 4 個 DHCP 區段。



圖七、DHCP 管理

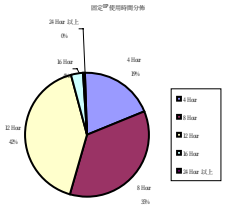
五、實驗分析

主要是觀察無線網路中 DHCP 使用者的使用時間分析，並且和固定 IP 使用者的使用時間做一個比較。以圖書館為統計分析之環境，利用 ping 程式收集了四個星期中圖書館 IP 位址的使用資料，並將其使用記錄儲存於資料庫，分別對 DHCP 動態 IP 位址及固定 IP 位址進行統計分析。我們以 ping 程式定期偵測動態 IP 之使用情形，並記錄每個 IP 位址每次租用之實際使用時間長度，產生如圖八所示之統計圖表，從其中資料可以得知無線環境下使用者之行為習慣。



圖八、四週中 140.134.192.0 網域 - 動態 IP 使用時間分佈圖

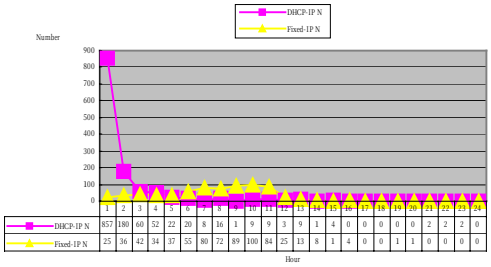
由圖八可以清楚的觀察出，DHCP 的使用者使用的時間多為一小時以下，所以使用者多半都是臨時借用 IP 然後離線。



圖九、四週中 140.134.40.0 網域 – 固定 IP 使用時間分布圖

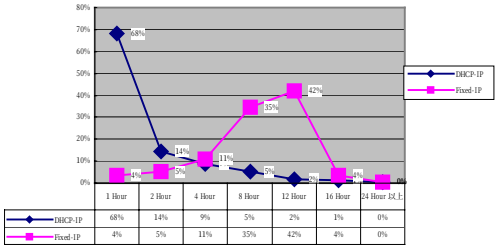
圖九則為依據圖書館四樓行政辦公室 140.134.40.0 網域四週中之固定 IP 位址使用情形，作一記錄及統計分析。根據統計結果所示，我們發現相同於 140.134.192.0 網域的固定 IP 位址使用情形，行政辦公室環境固定 IP 位址的之使用時間長度多集中於 7-11 小時，使用者使用 12 個小時以內的更高達 96%。

最後我們將動態 IP 位址及固定 IP 位址之使用情形作成圖十及十一之比較圖，經由以上的統計分析圖能夠實際了解到無線網路環境下使用者租用動態 IP 位址及固定 IP 位址使用行為之明顯不同，以做為提供網路管理者分配管理不同環境下使用者 IP 位址之參考依據。



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
DHCP-IP N	857	180	60	52	22	20	8	16	1	9	9	3	9	1	4	0	0	0	0	0	2	2	2	0
Fixed-IP N	25	36	42	34	37	55	80	72	89	100	84	25	13	8	1	4	0	0	1	1	0	0	0	0

圖十、四週中 DHCP 動態 IP 與固 IP 使用時間情形比較圖



圖十一、四週中 DHCP 動態 IP 與固定 IP 使用時間分佈比較圖

六、結論

隨著無線網路技術的發展與成熟無線網路設備的成本降低，現在慢慢的在很多地方都有提供無線網路的服務。隨著無線網路的便利性所延伸出來的問題，便是安全性不佳，以及管理不易，因為使用無線網路的人流動率都相當的高，因此不好掌握這個網域內到底有誰在使用網路。在 IEEE802.1x[9]中有定義如何來管理無線網路中的使用者，但是使用者的作業系統必須要支援 IEEE802.1x，AP 也要同時支援 IEEE802.1x，而且設定上不是相當的容易，所以設計了這個只需要利用瀏覽器、DHCP 以及 Linux netfilter 的機制，而且在傳統的無線網路系統下就能夠有效的達到管理人員的目的。在未來也能利用這種模式，使用在各種公共的場合，例如：校園、機場…等地方，只要使用者在 ISP 的 RADIUS 伺服器裡有紀錄，便能便利的使用網路資源。在加上 RADIUS 本身有計費的機制，對於使用者計費更是沒有問題。

七、參考文獻

[1] 竇其仁，林倩伶與余禎祥, “校園無線網際網路－以逢甲大學無線網路建置為例 ”。

[2] C. J. Park, S. J. Ahn, J. W. Chung and C. H. Lee, “The Improvement for Integrity for Integrity between DHCP and DNS,” IEEE, HPC Asia ’97, pp. 511-516, 2000.

[3] C. Rigney, W. Simpson and S. Willens, "Remote Authentication Dial In User Service (RADIUS),” RFC2138, April 1997.

[4] C. Rigney, “RADIUS Accounting,” RFC2866, June 2000.

[5] H. Walte and R. Russell, “Linux netfilter Hacking HOWTO,” July, 2002.

[6] R. Russell, ”Linux iptables HOWTO,” September, 1999.

[7] R. Droms, “ Automated Configuration of TCP/IP with DHCP,” IEEE Internet Computing, Vol. 34, pp. 45-53, July-Aug. 1999.

[8] T. Lemon and R. Droms, “The DHCP Handbook: Understanding, Deploying, and Managing Automated Configuration Services,” New York: Macmillan Technical Publishing, 1999.

[9] LAN/MAN Standards Committee of the IEEE Computer Society, "IEEE Standard for Local and Metropolitan Area Networks Port-Based Network Access Control," IEEE-SA Standards Board, June 2001.

[10] http://www.freeradius.org/