在 AAA 架構下以輕量級無線基地台為基礎之安全管理系統

王昭雄　高勝助
中興大學資訊科學所
{shawnwang, sjkao}@cs.nchu.edu.tw

摘要

IETF 所制訂的認證、授權及稽核（AAA, Authentication, Authorization and Accounting）程序描述了身份驗證、使用者網路存取授權以及計時計費程序之架構標準。在 AAA 的架構下，搭配 RADIUS（Remote Access Dial-In User Service）協定，IEEE 802.1x 標準在無線網路上的應用為區域無線使用者或漫遊使用者提供更安全的身份認證環境。然而，眾多未支援進階無線網路認證技術之無線基地台，在管理上就存在著安全的疑慮。本論文提出一套以 AAA 架構為基礎，有彈性之輕量級無線基地台安全管理機制。透過本系統導向、認證及計費模組的運作，未支援 RADIUS 協定之無線基地台網路環境得以擁有 AAA 架構之安全管理功能，更可經由後端較高效能之系統主機進行所有 AAA 架構程序，提高無線基地台的負載能力。

關鍵詞：AAA，RADIUS，輕量級無線基地台，網路管理

1. 前言

現行無線網路技術規範於 IEEE 802.11，為 IEEE 802 區域網路（LAN, Local Area Network）家族成員之一。而以 IEEE 802.11b/g [6] 標準的無線設備亦成為目前市場上的主流產品。相較於固定式有線網路，無線網路具備了行動性與機動性，為使用者提供了一個無障礙的網路存取空間；更穿透了實體建築的障礙，輕易地將內部的網路銜接至外部網路。

然而，相對於有線網路的實體線路傳輸方式，透過無線媒介進行傳輸的無線網路更容易被不法之徒所攔截而取得使用者的私密資料，凸顯了無線網路在漫遊資訊交換上的安全性 [5] [10]。因此，除了傳輸過程的加密處理之外，服務伺服器必須確認無線網路使用者的身份，進而授權給予適當的網路存取權。基於此種需求，架構於 AAA（Authenticating, Authorizing and Accounting）[2] 模組之上的 RADIUS（Remote Authentication Dial-In User Service）[8] 協定應運而生，讓網路管理者針對遠端撥入使用者進行身份驗證控管。

目前市面上無線基地台產品主要分為肥厚型無線基地台（Fat AP）以及精簡型無線基地台（Thin AP）。肥厚型無線基地台支援多種進階的無線網路技術，包括 802.1x [7]、RADIUS 協定等。精簡型無線基地台則需搭配 WLAN 交換器實現各種無線技術的支援性。然而，針對未支援 RADIUS 協定的無線基地台，我們以精簡型無線基地台為基礎，提出一套輕量級無線基地台之安全管理概念，以達到普通無線基地台對於 AAA 程序與 RADIUS 協定的支援。

第二章針對本論文所提出的輕量級無線基地台系統進行架構與概念說明。輕量級無線基地台系統測試與比較描述於第三章。最後一章為結論與未來展望。

2. 輕量級無線基地台系統架構與概念

802.1x 架構的應用，提高了無線網路的安全性；藉由無線基地台對 RADIUS 驗證伺服器與 EAP [1] 協定的支援，將申請者與認證者之間溝通的 EAPOL 封包重新封裝為 RADIUS 封包，溝通申請

者與 RADIUS 驗證伺服器之間的驗證程序。在本論文架構概念中，輕量級無線基地台將 AAA 相關程序交由後端的系統伺服器運作。

2.1 系統核心模組

系統環境區分為三組核心模組，分別為導向模組（Redirection Module）、認證模組（Authentication Module）以及計費模組（Accounting Module），各模組相關功能與運作模式描述於以下各小節。圖 1 描繪了系統三大模組之間的相依性以及各模組之中的主要元件。

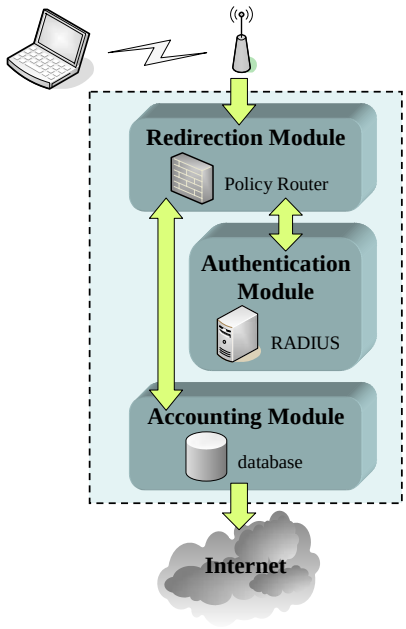

圖 1、系統核心模組示意圖

2.1.1 導向模組架構

導向模組（Redirection Module）為系統安全性與使用者網路存取權監控做了第一道重要把關。在使用者通過身份認證之前，導向模組僅開放對外的網域名稱（Domain Name）查詢。除此之外，所有的網路存取動作皆會經由建立於 Policy Router 中的封包過濾（Packet Filter）機制的判斷及過濾動作進行導向處理。

導向目標主要分為三類，若導向模組中的判斷元件偵測為未認證之使用者，使用者流程將被導向至認證伺服器進行認證動作。若偵測為已認證之合法使用者，導向模組將使其獲得對外部網域之存取權。最後一類導向目標為特殊情況之導向選擇，使用者將只獲得特定限制的網路存取權。舉例來說，無線網路服務提供者與某家銀行合作進行使用者線上刷卡或購買上網點數，若使用者帳務欠繳或上網點數不足時，將會限制使用者的部分存取，並導向使用者至外部特定網域（例如：銀行繳款系統）進行付費等帳戶續用程序。

2.1.2 認證模組架構

認證模組（Authentication Module）由 RADIUS 驗證伺服器所主導，配合支援 SSL 安全加密傳輸之瀏覽器，提供使用者安全且明確的操作方式進行身份認證。

當使用者進入認證模組時，首先存取內部網域中的網頁伺服器（Web Server），網頁伺服器透過 SSL 加密處理的頁面相互溝通使用者與後端 RADIUS 驗證伺服器。

2.1.3 計費模組架構

計費模組（Accounting Module）監控使用者的無線網路使用紀錄。自使用者認證通過獲得合法 IP 位址後開始計費動作，於使用者選擇登出無線網路之後終止計費動作並結算此次無線網路存取的總時數。

SQL 資料庫中的預存程序元件掌控計費模組的運作。透過網頁伺服器的呼叫，預存程序針對不同狀態的線上使用者在 SQL 資料庫進行不同的紀錄動作，包括為新登入之使用者新增紀錄，或為持續存取無線網路之使用者更新存取時間等動作。

2.2 系統整體架構

圖 2 所示為系統架構圖，結合了三大模組以及

其他元件的運作。架構圖中主要分為兩種資料流，分別為模組控制資料流（module control flow）與使用者控制資料流（user control flow）。模組控制資料流包括網頁伺服器與 RADIUS 驗證伺服器之間的認證模組程序以及計費步驟與 SQL 資料庫之間的計費模組程序。使用者控制資料流則包括了 DNS 網域名稱查詢以及 Policy Router 對使用者的導向選擇。

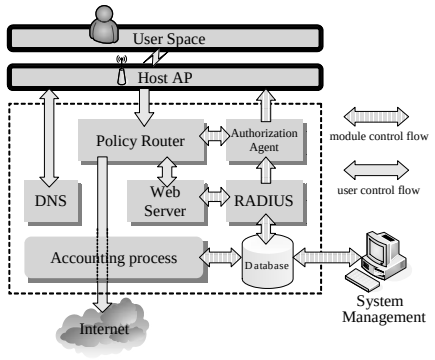

圖 2、系統架構圖

2.2.1 無線基地台

Host AP 無線基地台位於系統前端，在使用者與系統架構模組之間扮演資料傳遞與重新封裝的中介角色。藉由可程式化無線基地台，我們將無線基地台的狀態模式定位為橋接式（bridged Host AP），即所謂的輕量級無線基地台（Lightweight Host AP）；將導向、認證以及計費流程轉送給後端各系統模組執行。

2.2.2 授權代理者

系統架構圖中除了前面章節所提到的三大模組外，另外包含了授權代理者（Authorization Agent）元件，為本系統的重要元件之一。就 AAA 架構觀點而言，授權代理者相當於 AAA 架構中的網路存取伺服器（NAS, Network Access Server）。授權代理者橫跨導向、認證以及計費三大模組，詳細描述於第三章內容中。

2.3 集中式系統延伸架構

系統架構可區分內部網域與外部網域的系統元件。內部網域的系統元件組成主要以 Policy Router 為主之導向模組。外部網域的系統元件組成包括 RADIUS 驗證伺服器所控制的認證模組以及預存程序與 SQL 資料庫所控制的計費模組。因此，在不同網域中可各自建構適合既有環境之導向模組；而認證與計費程序則可交由集中式認證與計費模組進行，如此可達成不同網域之間的漫遊機制。圖 3 所示為集中式系統延伸架構。

在延伸架構中，各網域之無線網路管理者可以彈性地依據網域內的需求建立導向模組，並將使用者認證與計費交由集中式模組架構，而不需要在各網域中建立各自的認證與計費模組。如此可使漫遊系統建置便利；使用者紀錄皆透過集中式的計費模組統一管理，也可使稽核管理獲得效率。

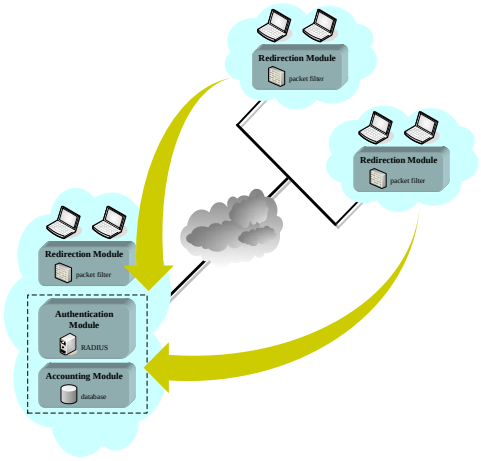

圖 3、集中式系統延伸架構

3. 輕量級無線基地台系統測試與比較

本章節中，我們將針對本論文所提出之認證管理架構進行系統測試，以驗證此方法之可行性。我們亦將系統測試細分為三類，分別為導向、認證以及計費模組測試三大主題，依次介紹於以下各章節。最後將針對不同無線基地台系統進行比較。

3.1 導向模組測試

顧名思義，導向模組必須判斷無線使用者的身份合法性並決定是否允許無線網路使用者對外的存取。我們利用 Linux 系統內建的 iptables [3] [4] 工具所提供的 C 語言函式庫撰寫了圖 2 系統架構圖中的授權代理者（Authorization Agent）；在導向模組中，授權代理者負責使用者授權存取、DHCP 觸發以及 DHCP 查詢三大功能。

若使用者尚未通過認證，其對外的瀏覽器連線動作將會被導向系統的認證位址，如圖 4 所示，其導向規則如圖 5 所示：

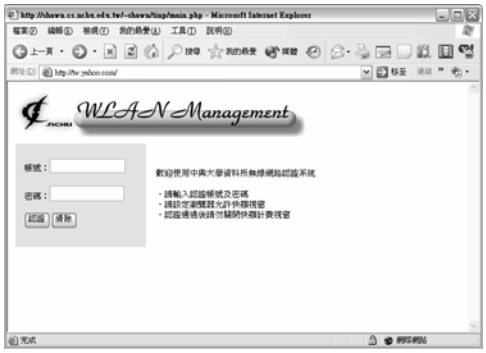

圖 4、未認證之導向頁面

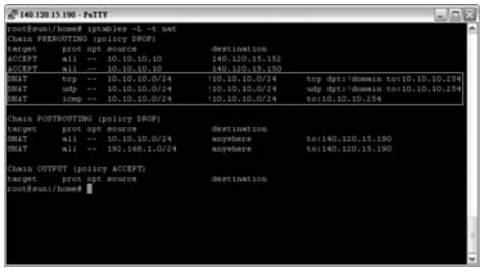

圖 5、未認證使用者導向規則

一旦使用者完成認證，授權代理者將於 Policy Router 動態即時加入允許使用者對外存取之規則，如圖 6 所示。反之，當使用者登出無線網路後，授權代理者將從導向規則中刪除此 IP 位址之存取權。

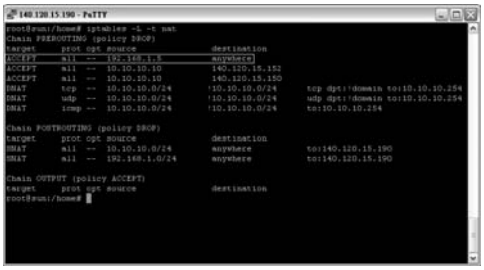

圖 6、認證通過之使用者權限規則

3.2 認證模組測試

認證模組中我們採用 FreeRADIUS 軟體，搭配 MSSQL 資料庫以及 CNR(Cisco Network Registrar) DHCP 伺服器共同運作。圖 7 所示為認證模組資料交換流程。

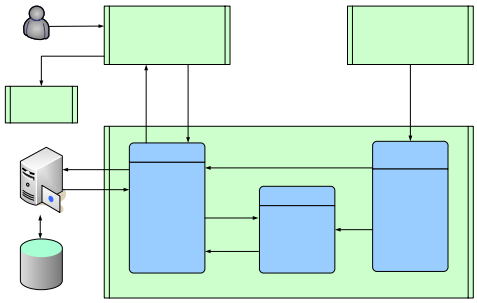

圖 7、認證程序資料交換流程

authentication.php 即為未認證使用者所被導向之瀏覽器頁面。瀏覽器首先透過 SSL 加密處理取得使用者之帳號密碼，隨後利用 authentication.sub 副程序將使用者資訊依照 RADIUS 協定標準封裝，並建立 socket 與驗證伺服器溝通進行身份驗證，以確保認證的安全性。

在 RADIUS 協定的封裝標準中，我們採用 PAP（Password Authentication Protocol）認證方式，透過網頁伺服器 PHP 函式將 RADIUS 的共享金鑰（shared secret）與隨機產生之認證碼（authenticator）進行 MD5 [9] 運算，將結果再與使用者密碼進行 XOR 運算。

若使用者通過身份驗證，授權代理者將呼叫 CNR 伺服器針對此位使用者之 MAC 位址配予合

法 IP 位址，其指令模式如圖 8 所示。反之，若使用者選擇離開無線網路，授權代理者同樣將呼叫 CNR 伺服器將此位使用者之合法 IP 位址收回。

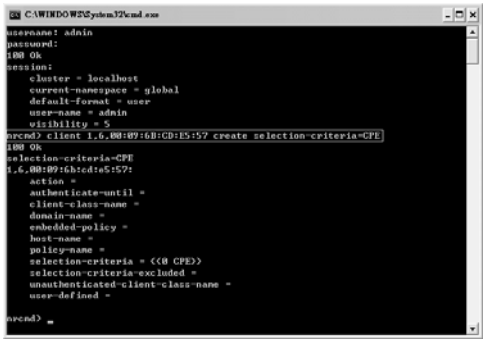

圖 8、授權代理者呼叫 CNR 伺服器

3.3 計費模組測試

計費模組由 MSSQL 資料庫所實作，我們利用 MSSQL 資料庫所具備的預存程序（Stored Procedure）進行計費模組的流程控制。

當使用者成功驗證身份之後，其瀏覽器將開啟計費視窗，此視窗定時與資料庫的預存程序聯繫，藉此預存程序可確保使用者仍於線上，並定時紀錄使用者在線上的使用時間，以提供帳務人員進行無線網路使用的稽核管理。

在資料庫表格中，wireless_account 資料表紀錄使用者各項資訊，包括使用者帳號、IP 位址、MAC 位址、無線網路存取時間等。資料表格型態描述於表 1 中。

表 1、wireless_account 資料表欄位定義

Name	Type	Length	Key
cpe_mac	char	17	
cpe_id	char	8	
cpe_ip	char	15	
time_start	datetime	8	
time_stop	datetime	8	
time_interval	int	4	

3.4 系統比較

傳統無線基地台具有精簡型無線基地台（Thin AP）以及肥厚型無線基地台（Fat AP）兩大類型。表 2 所列為輕量級無線基地台與傳統無線基地台之比較。

表 2、系統比較

	Fat AP	Thin AP	Lightweight AP
AP 內建功能	多	少	少
系統管理方式	分散式	集中式	集中式
進階技術擴充性	低	中	高
進階技術擴充成本	高	中	低
AP 擴充管理人力	高	低	低

由於肥厚型無線基地台集強大的功能於一身，因此適合集中式小型企業網路環境，無線網路管理者只需針對單一無線基地台進行設定維護，即可掌控所有的網路情況。反之，大型企業環境中，許多設備勢必分散於各部門，此時適用精簡型或輕量級無線基地台架構。在擴充性方面，相較於肥厚型無線基地台，可程式化之輕量級無線基地台系統具有高度的擴充性；就系統彈性而言，本系統可機動地建置於多個無線網路環境，透過集中式的認證、授權以及稽核管理，提供無線網路管理者掌控不同網域的使用者漫遊資訊。另外，當無線基地台數量擴充後，集中式管理之系統具備較有效率之管理型態。

4. 結論與未來展望

本論文以精簡型無線基地台（Thin AP）為對象，研究無線基地台安全管理需求，提供未支援 RADIUS 協定之無線基地台一個定位於 AAA 架構上的處理程序。在無線網路服務提供者（WISP, Wireless Internet Service Provider）的無線存取設備支援性尚未升級之前，我們所提出的系統架構可實

現無線網路使用者安全認證以及 AAA 認證計費程序之目標。系統中的關鍵程序由後端的三大模組所控制，分別為導向模組、認證模組以及計費模組；此三大模組實現了 AAA 架構，並將系統負載由無線基地台轉移至後端系統之中；利用後端較高等級的系統主機肩負起所有的系統程序負載，以達到輕量級無線基地台的概念。此外，以網頁為基礎的計費機制中，使用者可以獲得友善的無線網路系統程序介面而不需安裝其他額外的計費機制工具軟體。

由於認證程序的封包不再由無線基地台控管而是交由後端的可程式化系統處理，因此系統在認證上的支援性具有相當的擴充性。對於 IEEE 802.1x 標準而言，開發者可適當地加入其他可延伸認證協定（EAP, Extensible Authentication Protocol）的支援，例如 EAP/TLS 與 EAP/PEAP 等認證支援；相較於市面上已制式化的無線設備，本論文所提出的系統具有良好的擴充性。在漫遊機制方面，本系統可以擴充架構為集中式管理方式；透過建置於不同網域的導向模組，將認證與計費模組集中管理，以收使用者漫遊資訊管理之便。因此，本系統具有良好的擴充性、管理效率、系統設定以及便利的使用者存取介面，提供系統管理員在傳統無線設備升級之前的一套安全系統選擇。

參考文獻

[1] Blunk, L. and Vollbrecht, J., *"PPP Extensible Authentication Protocol (EAP),"* RFC 2284, March 1998.

[2] de Laat, C., Gross, G., Gommans, L., Vollbrecht, J. and Spence, D., *"Generic AAA Architecture,"* RFC 2903, August 2000.

[3] Gregor N. Purdy, *"LINUX iptables Pocket Reference,"* ISBN: 0-596-00569-5, O'Reilly, August 2004.

[4] Iptables Tutorial 1.1.19, http://iptables-tutorial.frozentux.net/iptables-tutorial.html

[5] Hahnsang Kim and Hossam Afifi, *"Improving Mobile Authentication with New AAA Protocols,"* IEEE International Conference on Communications, Volume: 1, Pages: 497-501, 2003.

[6] IEEE Std 802.11b-1999. *"Higher-Speed Physical Layer Extension in the 2.4GHz Band,"* Institute of Electrical and Electronics Engineering, Inc. September 1999.

[7] IEEE Std 802.1X-2001. *"Port-Based Network Access Control,"* Institute of Electrical and Electronics Engineering, Inc. June 2001.

[8] Rigney, C., Willens, S., Rubens, A. and Simpson, W., *"Remote Authentication Dial In User Service,"* RFC 2865, June 2000.

[9] Rivest, R., *"The MD5 Message-Digest Algorithm,"* RFC 1321, April 1992.

[10] Ying-Jui Lee, *"Mobile IP and AAA Architecture for Wireless LAN,"* NTUEE, June 2002.