建置以雙入口與角色為基礎的校園無線區域網路管理系統

周文正
國立清華大學
計算機與通訊中心
wjchou@cc.nthu.edu.tw

林平梓
國立清華大學
計算機與通訊中心
ptlin@cc.nthu.edu.tw

唐傳義
國立清華大學
資訊工程學系
cytang@cs.nthu.edu.tw

摘要

無線區域網路 (WLAN) 在新一代校園 e 化與資訊應用整合上扮演重要的角色，因此如何建置一個兼顧使用方便性與資訊安全性的無線區域網路實為一重要課題。目前各校認證方式不同與認證協定之不相容，讓 Web-based 網頁認證之漫遊用戶在 802.1x 認證之學校無法回原學校進行身份認證，因此，本文將探討如何以開放原始碼軟體為基礎，利用安全閘道建構一個以 IEEE 802.1x 及 Web-based 並存之雙入口校園無線區域網路，除了滿足國內大部分網頁認證方式，也迎合 802.1x 認證機制之世界潮流，以提供國內外無線漫遊認證服務。此外配合新的架構的形成與安全閘道之功能，進行開發以用戶授權角色為主之無線網路管理系統，以期提高無線網路管理績效與網路資源運用，亦提供實務經驗供 WLAN 系統建置與管理人員參考。

關鍵字：網路管理、無線認證、角色授權、WLAN 交換器、RADIUS

Abstract

Wireless Local Area Network (WLAN) plays an important role in either modern e-campus or integration of information systems, therefore how to build a convenient and secure WLAN has become an important issue. IEEE 802.1x - PEAP combination is very proper to be used in campus WLAN. However different schools adopt different protocols and authentication methods. The problem is: if a user who has registered in a campus using Web portal, is roaming in other 802.1x used domain then it can not be redirected back to its home domain for authentication. In this paper, we create a scheme for implementing a campus WLAN system with dual portal for both 802.1x and web-based on the base of WLAN switch mechanism to provide both home campus members and roaming users a convenient and secure wireless network environment. A role-based wireless network management system will be deployed in order to effectively and securely manage network resources. Implementing practices of setting up this system will be open to public for reference.

Keywords: Network Management, Authentication, Role-based Authorization, WLAN switch, RADIUS

1. 前言

無線區域網路(WLAN)在新一代校園 e 化與資訊應用整合上扮演著相當重要的角色，透過 WLAN 可將網際網路的觸角延展至校園的每個角落，讓校園網路實現於過去實體網路不易佈建之區域，因此如何建構一個適合學校師生的無線區域網路環境，已經成為校園 e 化的的重要課題。

在 2005 年，清華大學以 IEEE 802.1x [9]為基礎，採用 PEAP 協定[4]，配合無線網路帳號與密碼的認證，建置了以 802.1x 及 PEAP 為基礎的校園無線區域網路 [2]，以提供用戶較安全的無線網路環境。其中我們選擇 FreeRADIUS 作為 WLAN 的認證主機，除了開放原始碼軟體之經濟考量外，其具有支援 PAP/CHAP、EAP-MD5、EAP-TLS、EAP-TTLS、EAP-PEAP 與 EAP-SIM 等多功能認證方式，相當符合整合校內各單位帳號，達成單一帳號於校內自由無線上網之需求，亦能達成校際無線網路帳號漫遊認證之目的。然而，目前各校認證方式不同，認證互通互連時，例如 802.1x(PEAP)、Web-based（PAP）等認證協定的不相容。往往讓網頁認證之漫遊用戶在 802.1x 認證之學校無法回原單位進行身份認證，使校際帳號漫遊之美意成效打折。需要另外建置來賓帳號才能在本校使用 802.1x 的無線網路。此外在 802.1x 的無線網路環境初次使用時，尚未有連上網路的能力就需要下載安裝本校無線區域網路數位憑證，多少造成使用上的不便與困擾。

因此重新尋求同時兼顧連線方便性與網路安全性的解決方案，讓全方位用戶皆能方便使用無線網路以及提高 WLAN 維運績效，成為我們調整建置校園無線區域網路的主要努力方向。就現況而言，建置 802.1x 與 Web-based 雙入口無線區域網路系統有其必要性，除了滿足現階段國內大部分單位之網頁認證方式之外，也迎合 802.1x 認證機制之世界潮流，以提供國內外用戶無線漫遊認證服務。

網路資源有效運用與資通安全是近年來網路管理相當重要的議題，為滿足全方位用戶能使用優質的無線網路，我們選擇利用 WLAN 交換器安全閘道之角色導向管控功能，配合多個 SSID 之 ThinAP 並與現有 FatAP 整合，並開發以用戶角色為基礎(Role-Based)的無線網路管理系統(Wireless Network Management System, WNMS)， 使其在安

控管理與網路維運方面扮演重要的利器。雙入口與用戶角色為基礎的校園無線區域網路系統其架構如圖(1)所示，

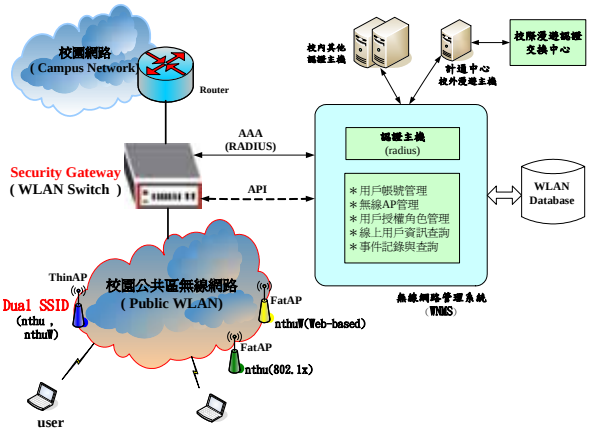

圖 1 雙入口與校園無線區域網路之架構圖

在下一節中，我們將詳述無線區域網路雙入口認證的運作架構。在第 3 節中，我們將說明系統實際建置的步驟。這次建置更新案所獲得的心得與檢討將在第 4 節中說明，最後則為本文的結論。

2. 無線區域網路雙入口認證之運作架構

在本節中我們將簡述無線區域網路雙入口認證之運作架構，以作為後續系統實際建置與無線網路管理系統開發的基礎。

2.1 802.1x 與 Web-based 認證方式之比較

一般採用 802.1x 之認證方式，係先通過認證後再取得 IP 上網，存取控制點在無線 AP；而 web-based 的認證方式，係先取得 IP 後再上網認證，存取控制端在認證閘道器，802.1x 與 Web-based 認證方式之比較參考表（1）。因此建置 802.1x 與 Web-based 雙入口認證之無線網路系統，若需整合現有 FatAP，則安全閘道 (Security Gateway, SG)至少應有對 802.1x EAP 具有透通性(Transparent)之功能，才能使 802.1x 用戶端與現有 FatAP 能透過 SG 至認證主機正常進行認證程序。若只整合 ThinAP 時，則存取控制點皆落在 SG 上。

表 1　802.1x 與 Web-based 認證方式之比較

比較項目	Web-based	802.1x + PEAP
用戶端	只需瀏覽器	需 802.1x 之用戶端軟硬體
安裝設置	無	步驟較多，初次使用時須安裝設定主機端憑證
控制點(NAS)	網路存取閘道器	無線基地台(AP)
每次使用	需透過瀏覽器，輸入使用者 ID 與密碼	以上一次認證成功之帳號與密碼，自動連線認證使用
IP 取得	先取得 IP 再認證上網	先網路認證後再取得 IP 上網
AP 假冒風險	有	無(雙向認證)
加密	無	動態 WEP Key
安全性	弱	強

2.2 FatAP 在 802.1x 下之 AAA 資料流程

就 FatAP(802.1x)與 SG 配合運作時之 AAA 流程圖如圖 2 所示，其中用戶認證時是由 FatAP 產生認證要求(Auth)，當 RADIUS Server 回應認證成功時，SG 會依回應屬性設定不同用戶角色，由此可見此時管控點由 FatAP 轉為 SG。至於 Accounting Start/Stop 要求皆是由 SG 負責，這是不同於一般無配合 SG 作業時是由 FatAP 所產生。當用戶端斷線時，SG 仍會停留在連線角色，待 idle-time out 後才真正進入斷線狀態。

若 ThinAP 配合 SG 作業時，則所有要求皆由 SG 負責產生，其餘流程與 FatAP 在 802.1x 下之 AAA 資料流程相同。

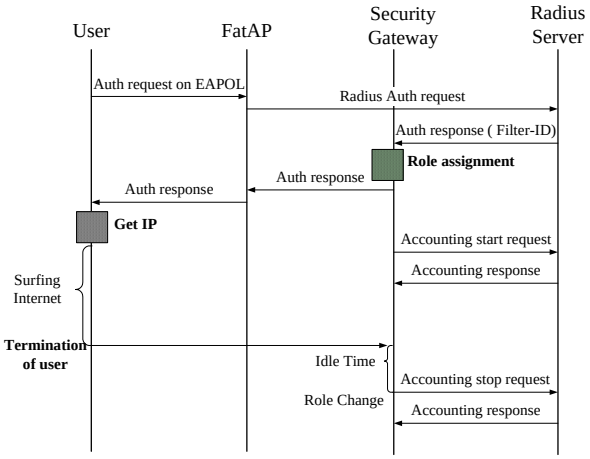

圖 2 SG 整合 FatAP(802.1x)時之 AAA 流程圖

2.3 使用者認證授權管理

由於無線網路強調高度行動方便性與安全性，因此常會希望依無線網路使用的群組類別加以管控[10]，例如包含各部門的員工、約聘員工、合約廠商、產學合作員工、來賓等等。將這些不同群組類別的使用者設定不同的存取權限。

在實際應用上，SG 一般可利用外部 RADIUS 認證主機回傳之屬性(Attribute)，以區分使用者群組，此過程可以動態讓不同角色身份的使用者以不同的權限登入無線網路系統。其中一個角色可由多個獨立政策(policy) 所組成；一個政策可由多個命令規則(rule)所組成。授權角色-政策-命令規則之間

的關鏈如圖(3)所示。同樣的用戶角色，亦可依用戶當時所使用 802.1x 或使用 Web -Based 方式之不同授與不同的權限。例如有必要時對使用 Web -Based 方式認證的使用者做必要的存取資源限制，以降低表(1)所述無加密的風險。

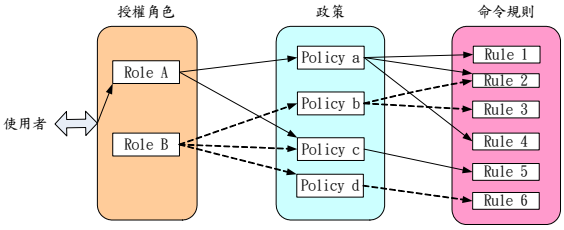

圖 3 授權角色-政策-命令規則之間的關鏈

2.4 WLAN 交換器與 ThinAP 架構

傳統分散式的無線網路 FatAP，一般負責管理、政策、漫遊、加密、認證與 RF 訊號傳遞等功能，必須每台 AP 逐一進行相關設定，例如設定 SSID、加密機制、Shared Secret、頻率頻道等。如果擴充 AP 的數量，將造成 AP 越來越難管理。此外例如 AP 功率及頻道的調整、干擾問題的偵測避免、AP 故障的備援及負載平衡等，此缺乏中央控管 AP 的機制，是提升整體 WLAN 佈置與維運績效之隱憂。

WLAN 交換器配合 ThinAP 改變了傳統無線 AP 結構，ThinAP 只負責 RF 訊號傳遞；WLAN 交換器負責管理、政策、漫遊、加密、認證等功能，且能在未改變既有的有線網路連結架構下，利用 Tunnel 技術將用戶端資料流導入無線網路網段，此集中式的控管，分散式的舖設無線 AP，不僅提高管理績效，也延展無線網路應用平台的彈性空間。同時提供了高度的漫遊特性，讓資源的存取凌駕於現有固定式的網路架構。WLAN 交換器與 ThinAP 架構之硬體成本較高，但整體校園 WLAN 維運成本與優質無線網路之使用品質，應有受公評的優勢。

3. 系統應用與實作

為提供了一個全方位用戶認證的無線網路環境，利用 Aruba Mobility Controller (MC) 安全閘道之角色導向管控功能，配合支援多個 SSID 之 ThinAP(AP61)與現有單 SSID 之 FatAP(ZyXEL B-1000)整合，建構一個以 IEEE 802.1x 及 Web-based 並存之雙入口的校園無線區域網路，此環境每個 SSID 設定一種用戶認證方式，可讓使用者於電腦開機後，用戶即可透過 SSID 來選擇所要使用的認證方式以連接無線網路。若前一次已以 802.1x(例如 SSID=nthu)成功上網，也會如同使用固接區域網路(如：Fast Ethernet)一般，自動連線校園無線區域網路，若 PC 無 802.1x 環境無法自動連網，即可選擇 Web-Based(例如 SSID=nthuW)手動開啟瀏覽器後登入認證畫面，方可進行網路連線。

MC 對於 WNMS 來說是一個可管控的網路設備，MC 經過設定發揮 WLAN 交換器之應用功能(SSID 認證方式、用戶授權政策等)後，用戶被授權之角色行為與追蹤，動態由 WNMS 之各 ASM(Application Specific Module)決定。

以下各小節除了說明如何簡化無線網路 PEAP 認證作業程序之外，將詳細說明 WNMS 之用戶角色授權、動態轉變用戶角色之應用流程、NAS/AP 管理、單位來賓帳號管理、使用者線上之資訊查詢、及事件紀錄與查詢。

3.1 簡化無線網路 PEAP 認證作業程序

我們採用 FreeRADIUS v1.16 [7]作為我們的認證主機 RADIUS server，系統建構在 Linux 作業系統上，硬體則是採用 PC 伺服器架構，成本相當低廉。在軟體的建置上，除安裝 FreeRADIUS 外，主要步驟在於憑證的安裝與系統檔案的設定。PEAP 只使用主機端的憑證(server certificates)來認證主機端，因此只需產生主機端的憑證即可。主機端的憑證係由 CA (certification authority)所核發，若該 CA 是用戶端信任的憑證核發者，則主機憑證可被自動信任而完成連線，在使用上可說相當方便。若無法從既有信任 CA 得到主機憑證，則可利用 OpenSSL 產生 self-signed certificates[2]。為簡化無線網路 PEAP 認證作業部分，讓 PEAP 用戶初次使用時，省略下載安裝本校原有無線區域網路數位憑證(self-signed)。我們向 HiTRUST 租購"動態加密型伺服器數位憑證"[8]，以方便 PEAP 用戶上網。

完成憑證之產生後，即可進行系統檔案之設定，包含 radiusd.conf、eap.conf、clients.conf、acct_users 及 users 等。其設定範例請參考[2] ，

3.2 用戶角色授權

WNMS 可依使用者之政策性管理設定資料，在授權模組階段決定使用者允許做些什麼：包括當時「日期時間」、能上網多久、能否同一帳號同時上網或其同時上網個數以及用戶授權角色等。例如使用者之政策性管理設定資料範例如圖(4)。此範例代表該使用者可用期間為 96/08/02 09:12 至 96/10/31 23:59 之間；每週可用時間為週一至週五之 08:00-23:30 及週六整天及週日 13:00 至隔天 06:00。因此，假如該用戶在可用期間內之星期一 23:00 要求認證授權，則 RADIUS 會回應 SG "Session-Timeout=1800"，致使用戶只能使用 30 分鐘（1800 秒）後由 MC 自動斷線，並產生事件記錄。當用戶認證成功後，MC 依認證主機所設定之授權角色，管控該用戶之使用行為。

管理者在設定用戶授權角色之前，可利用 CLI 線上查詢 MC 各授權角色之實際內容，例如查詢授權角色" Role-Guest"內容 範例如圖(5)，其中說明角色 Role-Guest 之用戶只能存取 Internet，不能存取校園網路，只能使用 HTTP、Mail 且只能使用 256Kbps 的頻寬等。

圖 4 使用者之授權管理設定資料之範例說明

圖 5 WNMS 查詢用戶授權角色之內容頁面

3.3 以動態轉變用戶角色之應用流程

MC 設定每一用戶類別之內定授權角色，當 MC 向 Radius 認證主機要求認證時，若身份確認正確，認證主機會參考當時使用者之授權角色，以 Radius「Filter-ID= Role-Name」屬性回應 MC，由 MC 依回應屬性值，進行匹配授權角色(role policies)以進行政策實現(policy enforcement)" 命令規則。

例如當用戶電腦因 Internet worm 或 ARP attack 等造成網路威脅時[11]，若使用 ThipAP 可利用"stm sta-dos-prevention enable"以 CLI 方式執行 "stm add-dos-sta User'sMAC" 功能立即 MC 斷網措施。若使用 FatAP 則可執行動態設定用戶角色，以改變用戶使用路徑，其應用驗證過程(如圖 6 所示)如下：

1. 當用偵測系統感應用戶端電腦造成網路威脅時，WNMS 以該 IP 得知當時之使用名稱(UID)。
2. WNMS 動態設定該使用者之新的授權角色，並記錄此事件。
3. WNMS 藉 MC CLI 及時將該使用者斷線(例如 aaa user delete name UID)。
4. 當使用者被斷線後，透過 MC 重新以 PEAP 或網頁認證時，Radius 以 Reject 禁用或 Acceept 新角色回應 MC(例如 Destination NAT 將所有 Web 連線導向固定網站)。
5. WNMS 紀錄使用者認證使用資料。
6. 用戶以新的授權角色連網。

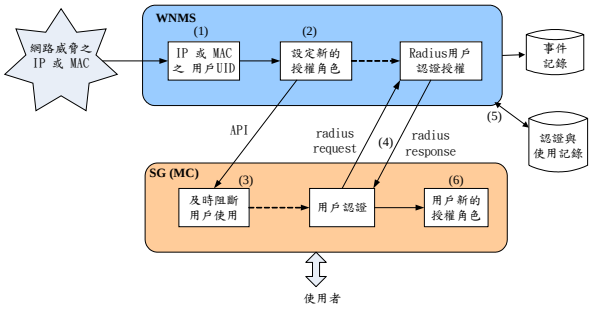

圖 6 以動態轉變用戶角色之應用流程

3.4 NAS/AP 管理

NAS/AP 管理包含設備佈置資訊與運作查詢。NAS/AP 管理功能範例如圖(7)所示，其佈置資訊包含：FatAP 放置位置(單位,樓層,編號),ThinAP Location ID、IP 位址、MAC 位址、認證主機連結密碼、SSID、FatAP Channel（1、6、11）、品牌型號、異動時間、是否啟用等。此新增、異動、刪除介面提供管理者能隨時掌控 NAS/AP 資訊，藉此資訊可輕鬆佈設所管理之 NAS/AP 設備。尤其在設備監測與位置查詢應用上，提供重要參照資訊。

圖 7 NAS/AP 管理功能頁面

3.5 單位來賓帳號管理

近年來學術交流頻繁，產學合作日趨密切，各單位無跨校漫遊帳號之來賓，如何使用校園無線網路以及來賓之管理，帶來各單位管理者諸多不便，因此系統提供各單位管理者線上建置及管理所屬之來賓帳號，以解決無跨校漫遊帳號之來賓使用校園無線網路的問題，單位來賓帳號管理功能範例如圖(8)所示。

系所單位管理者建置所需之來賓帳號時，可針對不同的帳號設定不同的使用期限，當帳號時效過期，使用該帳號的來賓將自動被登出系統，並且無法再登入使用無線網路。管理者亦可線上登錄來賓的相關基本資料，以便隨時掌握帳號之使

用狀況，必要時以作為用戶追踪之依據。藉由帳號分散式處理集中式管理、各單位分層負責、網頁式操作介面以及完整的帳號資訊異動歷史記錄存查等功能 ，可提高帳號管理績效。

圖 8 單位來賓帳號管理功能頁面

3.6 使用者線上之資訊查詢

我們將 MC 與 Radius 認證主機之間所有用戶認證、授權與帳務之 AAA 互動資訊，整合為單一查詢介面，提供維運人員能即時得到使用者之上線資訊，以利協助解決使用者之請求。

當使用者認證成功上網之後，即可能建置使用者線上資訊查詢，其資訊包含：用戶基本資料、使用認證型態（例如 WEB、PEAP、TTLS 等）、用戶授權角色、上線地點（IP/ThinAP Location ID）、時間、無線網路卡號及所使用 IP、帳號漫遊資訊（本地帳號從非本地主機回到本地認證或是非本地帳號借本地上網）、是否收到帳務相關資料等資訊。尤其應讓服務人員能快速掌握使用者當時 MC 安全閘道所實施該使用者之管制策略。因此系統以 CLI 即時至 MC 安全閘道搜尋整理該授權角色之詳細政策規則，輔助研判說明使用者之真實現況，如同圖(5)所示。

使用者線上資訊查詢範例如圖(9)，其中顯而易見，使用者認證使用之情形。其中 ThinAP 以 Location ID(1.3.2)至 AP 資料庫得知 ThinAP 之 IP 與位置；而 FatAP(PEAP)認證時，能將以 FatAP 之 IP 至 AP 資料庫得知 FatAP 位置。當用戶離線時，會「即時」產生用戶計時與計量之結算，並另產生當日使用之累計，以供歷史紀錄查詢或下次連線認證之授權參考。

圖 9 使用者線上資訊查詢

3.7 事件紀錄與查詢

系統紀錄用戶認證授權時之異狀事項（event log），以提供用戶與管理者網路查詢，異狀事件列舉如下：未在授權日期範圍內使用、未在授權時間範圍內使用、MAC 未授權使用、已超過同時上線數、禁用中等類別，事件查詢功能範例如圖(9)。此用戶之認證異狀歷史記錄，可依據異狀事件、用戶編號、NasIP 及上線時間等條件進行組合查詢，有助於提供管理者面對用戶諮詢時之重要參考資訊。

圖 10 事件查詢功能頁面

4. 心得與檢討

從利用 Aruba MC 建構一個以 IEEE 802.1x 與 Web-based 之雙入口校園無線區域網路，以及研發校園無線區域網路管理系統的過程中，我們獲得許許多多的寶貴經驗，茲將幾個我們初步獲得心得與檢討條列如下：

1. 同時支援 802.1x 及 web-based 認證機制的無線網路環境，除了滿足國內大部分學校之漫遊認證方式，也迎合 802.1x 認證機制之世界潮流，可照顧到更多的使用者。此外系統也提供各單位管理者線上建置及管理所屬之來賓帳號，以解決無跨校漫遊帳號之來賓使用校園無線網路的問題。
2. 採用 802.1x 之認證方式，係先通過認證後再取得 IP 上網，存取控制點在無線 AP，一般需下載並安裝設定校園無線區域網路數位憑證，以免在認證過程中會有 AP 假冒之風險。然而在初次使用時，尚未有連上網路的能力就需要下載安裝本校無線區域網路數位憑證，多少造成使用上的不便與困擾，因此可向 HiTRUST 租購"動態加密型伺服器數位憑證"，使主機憑證變成 Windows XP SP2 預置之信任 CA 所核發，讓用戶初次使用時，省略下載安裝無線區域網路數位憑證。
3. 若 MC 需要同時支援 ThinAP 與 FatAP 時，就用戶使用之穩定性與系統管理的考量，FatAP 可集中於 Web-based 認證區，同一區欲支援 802.1x 與 Web-based 認證，以支援多 SSID 之 ThinAP 為佳。
4. 傳統 FatAP(PEAP)並不會將所謂用戶 IP「Framed-IP-Address」傳給 Radius Server，但會記載用戶無線網卡之 MAC 位址「Calling-Station-ID」，若欲想記錄當時用戶無線上網之 MAC 與 IP，以 Calling-Station-ID 從 DCHP LOG 比對攫取 IP 是不可靠的，畢竟使用者待 PEAP 認證後由 DHCP 取得 IP 後，可直接以靜態指定一個已知合法 IP 使用。因此系統管理程式可由 router 之 ARP table 取得該用戶

MAC 與 IP 之配對值。

5. 在此雙入口認證架構之下，不管 Web-based 或 PEAP 認證方式，MC 會紀錄用戶 IP Framed-IP-Address 傳給 Radius Server。若用戶經認證後擅自由目前 IPa 改成 IPb，則 MC 將視 IPb 為新的 session，須再經認證成功後才能上網，並且記錄於 Framed-IP-Address。待 IPa 之 session 進入 idle-timeout 狀態， MC 送 Acct_stop 以結束 IPa 認證使用程序。
6. FatAP(PEAP)與 Radius 間之 shared secret 需相同於 Aruba MC 與 Radius 間之 shared secret，不然，當用戶端透過 FatAP(PEAP)經 Radius Server 通過認證處於連線狀態後，仍須經過網頁重新認證才能使用 WLAN。
7. 對 FatAP(PEAP)而言， MC 不只是 pass through, 還監看(Stateful 802.1x)RADIUS 封包，可以抓到 RADIUS 回應屬性，將用戶指派到某個 Role。不過 linux 需要停用 "Path Maximum Transfer Unit(Path MTU) discovery " 功能，即在 /etc/sysctl.conf 檔案中設定 net.ipv4.ip_no_pmtu_disc = 1，不然 MC 無法攫取 Radius Accept 相關資訊，致使 FatAP(PEAP)已處於連線狀態，MC 仍處於"logon"狀態，須再經過 Web 重新認證才能使用 WLAN。
8. FatAP(PEAP) 認證時，認證 Auth 要求由 FatAP 產生，帳務 Acct 由 MC 產生。然而單一 SSID 多個 FatAP(PEAP)時，多個 FatAP(PEAP)有時會產生多個 FatAP(auth) 認證要求，Radius 認證主機若起動用戶同時使用次數限制(Simultaneous-Use)，會造成檢測功能失準。應透過 API 至 MC 存取上線用戶為依據。
9. FatAP(Web)認證時，無法像 FatAP(PEAP)能將 AP 之 IP(即 Client-IP-Address 屬性)送到 Radius Server，管理系統無法得知用戶之位置。然而使用 ThinAP 時，可藉 ARUBA_LOCATION_ID 屬性傳遞用戶位置。
10. 諸如 Aruba MC 之 WLAN 交換器與 Thin AP 架構，改變了傳統無線 AP 之結構與管理思維，可在未改變既有網路連結架構下，進行分散式的鋪設無線 AP，集中式的控管，不僅提高管理績效，也延展無線網路應用平台之彈性空間至無限的可能。且 ThinAP 迎合客觀環境的變化，隨之自我調整的能力提升(例如頻道與功率，負載平衡)，無形提高無線網路之使用品質。

5. 結論

本文探討如何建置 802.1x 與 Web-based 雙入口無線區域網路系統，讓用戶可透過 SSID 來選擇所要使用的認證方式以連接無線網路。.就現況而言，除了帶來來賓方便以網頁認證使用網路，以及滿足現階段國內大部分單位之網頁認證方式之外，也迎合 802.1x 認證機制之世界潮流，以提供國內外用戶無線漫遊認證服務。

現今 WLAN 交換器與 Thin AP 之運作模式，已改變了傳統無線 AP 之結構與管理思維，能在未改變既有的有線網路連結架構下，進行建置管理。我們利用 WLAN 交換器功能，所發展之以用戶角色為基礎的無線網路管理系統，在安控管理與網路維運方面已扮演重要的利器，仍需持續進行功能加強與使用者介面的改善。

用戶以網頁認證固然方便，但是畢竟經過認證後之網路存取行為還是存在有被竊聽的風險，因此 802.1x 仍是無線認證之最佳機制。雙入口無線區域網路系統是滿足國內大部分網頁認證漫遊現況之過渡期解決方案，期待國內漫遊單位皆能持續朝向 802.1x 架構邁進，以建置符合國際趨勢的無線網路使用環境。

參考文獻

[1] 周文正, 王晉良,“校園無線區域網路 AAA 系統設計與實作,” TANET 2003, pp.173-178.

[2] 周文正, 賴守全,” 建置以 802.1x 及 PEAP 為基礎的校園無線區域網路” TANET’ 2005

[3] Aruba Network . http://www.arubanetworks.com/

[4] A. Palekar et al., “Protected EAP Protocol (PEAP) Version2,” draft-josefsson-pppext-eap-tls-eap-10.txt, Internet draft (working in progress), October 2004.

[5] Christoph Rensing, Hasan, Martin Karsten , Burkhard Stiller, “AAA:A Survey and a Policy-Based Architecture and Framework” IEEE Network November/December 2002 p22-p27

[6] Dakshi Agrawal, Seraphin Calo, etc. “Policy Management for Networked Systems and Applications”, Integrated Network Management 2005(IM2005).

[7] FreeRADUIS, http://www.FreeRADIUS.org.

[8] HiTRUST, http://www.hitrust.com.tw/

[9 IEEE Standard 802.1x, “IEEE Standard for Local and Metropolitan area networks – Port-Based Network Access Control,” October 2001.

[10] Ravi S. Sandhu, etc. “Role-based access control models”, IEEE computer February 1996

[11] Shou-Chuan Lai, Wen-Chu Kou, Mu-Cheng Hsieh,”Defending against Internet Worm-like Infestations”, 18th International Conference on Advanced Information Networking and Applications (AINA'04)