

校園無線環境的升級與整合：從 WiFi 到 WiMAX

唐可忠 黃偉航

國家高速網路與計算中心

kevin@nchc.org.tw ; a00whl00@nchc.org.tw

蔡志宏

國立台灣大學電信工程學研究所

ztsai@cc.ee.ntu.edu.tw

摘要

台灣校園 WiFi 無線環境的建置普及率已經達到 90% 以上，加入校園無線漫遊環境的單位也超過 110 個，足見 WiFi 應用及漫遊環境已經相當普及，但對於 WiMAX 技術的興起，校園是否已經做好準備了呢？本文乃根據校園無線網路現況並參考 WiMAX 相關規範整理出 WiFi 與 WiMAX 整合升級時的參考方案。本文所提出之參考方案考量無線漫遊機制現況，允許校園在整合 WiFi 與 WiMAX 環境後，使用者仍然能夠繼續享受單一帳號登入 WiFi、WiMAX 無線網路以及跨校 WiFi、跨校及跨網 WiMAX 漫遊等服務。最後，本文也提出與其他可選用方案之技術比較與結論。

關鍵詞：WiMAX、無線漫遊、EAP-TTLS、RADIUS

Abstract

There are over 90% of 163 colleges with established 802.11 WLAN environment in Taiwan. It is show now that the WLAN has become a universal services in campuses. In the future, the WiMAX technology may widely deployed in campuses, but have campuses made ready for WiMAX yet? In this paper, we introduce an architecture of a WiFi/WiMAX co-existing environment, as a reference solution to the WiFi access and authentication environment in campuses and WiMAX campus network based on standards from WiMAX forum and IEEE. Based on this architecture, original WiFi users can continue to enjoy WiFi/WiMAX cross-campus roaming with the same single account. At last, We also present the comparison of the reference solution and other alternatives, and the final conclusions.

Keywords: WiMAX, Roaming, EAP-TTLS, RADIUS

1. 前言

WiMAX(Worldwide Interoperability for Micro wave Access，全球互通微波存取)[7]，是基於 IEEE 802.16 的無線通訊技術，同時也是近年來相當被看好的無線網路技術，不少人也認為 WiMAX 將是演進至 4G 的代表技術之一。目前的市場上的 WiMAX

設備主要規格有兩種，分別為 IEEE 在 2004 年制訂的 802.16-2004 標準，其前身為 802.16d，又稱 Fixed WiMAX，顧名思義就是固定式的 WiMAX；另外一種是 IEEE 在 2005 年制訂的 802.16-2005，前身為 802.16e，又稱為 Mobile WiMAX，可支援行動式的相關無線應用。

Fixed WiMAX 一般應用於骨幹或橋接用途，可使用免執照頻段，例如大樓之間的網路連接，避免實體佈線的麻煩；或是作為 WiFi 環境的回程線路，臨時網路的架設等等。故一般校園大樓的實體有線 ADSL 或光纖網路，未來也可能部份改採用 Fixed WiMAX 來接取，以節省實體光纖線路佈建成本。Mobile WiMAX 的終端則主要是一般個人用戶，Mobile WiMAX 提供了媲美 3G 技術的行動通訊能力，以及 WiFi 環境的親和力，除了長程傳輸能力、高傳輸頻寬的特點外，還能夠支援現有的 IP 相關應用，因此 Mobile WiMAX 也是被各界所看好的一塊大餅。但由於其重要頻段為第一類電信業者使用之頻段，故校園若擬建置 Mobile WiMAX 環境，其實驗頻道問題要優先解決。

看著 WiMAX 產業的日漸成熟發展，回首過去的 WiFi 歷史腳步，從當時 WiFi 設備的奇貨可居，到現在校園 WiFi 無線網路環境的普及，WiFi 與 WiMAX 共存網路是否會成為未來校園無線環境的主流呢？

2. 校園無線網路現況

目前台灣大學院的無線網路環境的建置以 802.11a/b/g 的 WiFi 環境為主，無線環境普及率大約在 90% 以上，近幾年來經由國家高速網路與計算中心、資策會配合政府 M-Taiwan 計畫推動的無線漫遊互通機制^[1]，已經有超過 61% 的學校加入，同時也大幅擴展了各校師生的行動運算能力。

在電信國家型科技計畫的支持下，中央大學與暨南大學共同成立了 WiMAX 開放實驗室，專責進行 WiMAX 的效能量測、應用服務實驗以及網路管

*本論文為電信國家型科技計畫「校園無線漫遊網路環境建置與安全升級計畫(II)」研究成果，國科會計畫編號：NSC 96-2219-E-492-001。

理建置等工作[3]，並在台大、中大、清大、交大、暨大等校園投入 WiMAX 網路實驗建置。另外淡江大學、宜蘭大學與台灣大學也與廠商合作建置校園 WiMAX 網路，以期作為產品測試及應用服務開發平台，換言之，WiMAX 的普及化正逐漸展開。

3. WiFi 與 WiMAX 應用環境

目前在校園內建置的 WiMAX 實驗環境多以 ISM 頻段之 802.16d 為主，也就是 Fixed WiMAX。此技術一般作為大樓之間的網路接取或是作為 WiFi 環境的後端線路，當然我們也不可完全排除 802.16d 用於移動用戶的可能性。考量現有 WiMAX 產業大部分朝向 802.16e 發展，因此本文的重點將著眼於 WiFi 與 Mobile WiMAX 共存的環境。

目前談到 WiMAX 眾人的印象不外乎就是範圍廣，頻寬大的一種無線網路技術，就建置架構上來看，似乎比起現行的 WiFi 環境或者是 WiFi Mesh 似乎來得更容易管理。但在應用服務方面則相當不同，SIP/VoIP 原是在 WiFi 環境下經常被提起的一種應用服務，雖然這類產品市面上風行已久，但在校園內總是不那麼熱絡，其原因在於各個校園無線網路的認證機制以及無線閘道設備實作標準的不同，限制了 WiFi 手機的行動力。配合 Mobile WiMAX，以及 WiMAX 採用的 PKMv2 (Privacy Key Management version 2) 認證機制，這將使得 SIP/VoIP 在校園內普及更有機會踏實。

我們預期 WiFi 並無法由 WiMAX 直接取代，因 WiFi 仍然可以作為一般存取網路或是非即時性通訊的管道。透過支援 WiFi 與 WiMAX 的雙模網路卡，也能夠讓用戶在 WiFi 與 WiMAX 之間選擇，看個人的使用需求而定。

下圖 1 中顯示了校園自建 WiFi 與 WiMAX 環境並存的時可能提供的應用服務，但在建置或升級 WiMAX 環境時，如何兼顧原有的 WiFi 環境呢？

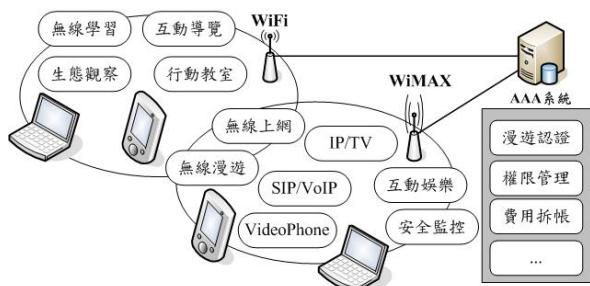


圖 1 WiFi 與 WiMAX 整合環境示意圖

無論未來是 WiMAX 取代 WiFi，或是 WiFi 與 WiMAX 攜手並進的情況，除非建置全新的無線及認證環境，否則校園管理者都將面臨著無線使用者的認證機制以及後端 AAA 系統的轉換及整合問題。

4. WiFi 與 WiMAX 之認證整合

一個無線環境的建立，包括了前端的使用者認證規劃，中間的認證流程路徑以及後端的使用者帳號系統建置及 AAA 機制的建立等細節，同時也必須考量並存環境下的設備管理問題。如果校園內 WiFi 與 WiMAX 環境的 AAA 機制都是獨立運作的系統，用戶以不同的帳號使用不同的服務，那可能就沒有所謂的整合問題，但這樣的架構可能會造成使用者帳號及無線網路設備管理上的麻煩。最顯而易見的例子就是單一使用者擁有多個帳號的狀況，不僅使用者在認證時會困擾，管理者在處理使用者記錄時也會有整合上的難處。

校園內 WiFi 與 WiMAX 整合的方式可能會有下列幾種：

1. 校園自行佈建 WiMAX 環境並整合現有 WiFi 架構。
2. 校園租用 WiMAX 業者服務，整合校園 WiFi 環境。
 - a、委託業者管理帳號及帳務
 - b、透過 proxy 使用校內帳號

以目前的產業界模式、WiMAX 相關標準以及 WiMAX 執照發放的情況來看，與業者合作的可能性也許會比較高一些。屆時校園內提供的室內 WiFi 環境也能夠補足 WiMAX 業者在室內訊號不足之處，當然這中間牽涉到校園與業者之間資源分配的問題，如何規劃公平的互惠機制將是一個重點，不過這暫時不在本文的討論範圍之內。

無論採用什麼樣的整合方式，我們的目標是希望在 WiFi 與 WiMAX 共存的環境下，使用者仍然能夠以單一帳號進行無線網路認證，並且能繼續享受跨校無線漫遊的服務；同時管理者也能夠因為單一帳號以及整合過後的認證架構，獲得較佳的管理效率。在本文中我們將以架構最簡單的校園自建 WiMAX 環境來說明 WiMAX 與 WiFi 整合的議題。

4.1 WiFi 使用者認證機制介紹

目前在各個校園中最常見的 WiFi 無線網路認證方式為網頁認證，少部分單位則採用 802.1x[4] /EAP-PEAP(Protected EAP) 及 802.1x/EAP-TTLS (Tunneled TLS Authentication Protocol) 認證方式[2]。

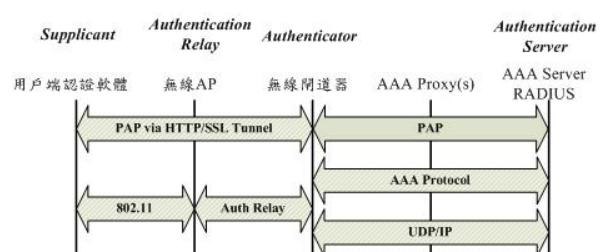


圖 2 WiFi 用戶端網頁認證流程

網頁認證機制的好處在於支援多種使用者帳號系統，使用者只需要網頁瀏覽器便可進行身份認證，不過身份認證機制採用 PAP 方式，因此使用者的密碼會直接以明文的形式在網路上傳送。如圖 2 所示為 WiFi 用戶透過網頁認證的流程。

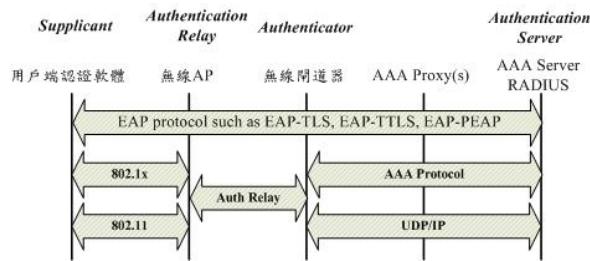


圖 3 WiFi 用戶端 802.1x 認證流程

如圖 3 所示為 WiFi 環境使用 802.1x 認證的流程，常用的 802.1x EAP 認證類型，包括 PEAP 與 TTLS 均屬於 TLS 加密通道式的協定，認證前會先以 TLS 建立加密通道後，再以一般常用的身份驗證機制進行驗證，如 MS-CHAPv2、PAP 等，因此可以保證使用者個人密碼的安全[2]。下表 1 為網頁認證、EAP-PEAP 與 EAP-TTLS 認證機制的特性比較。

表 1、網頁認證/PEAP/TTLS 比較表

	網頁認證	PEAP	TTLS
認證軟體	瀏覽器	專用軟體	專用軟體
認證協定	PAP	MS-CHAPv2/ EAP-TLS	PAP/CHAP/MS -CHAPv2/EAP
漫遊認證	支援	支援	支援
帳號隱藏	無	有	有
傳輸安全	無	動態 WEP	動態 WEP

以目前的 WiFi 身份認證現況而言，使用者若要採用 PEAP 與 TTLS 驗證，均需要透過專用的認證軟體，像是 Windows 內建的 PEAP 軟體、SecureW2、Xsupplicant、WIRE1x 等軟體。此外，PEAP 對於帳號系統的要求也比較嚴格，可能會影響認證環境的整合，這部份本文稍後會做說明。

4.2 WiMAX 使用者認證機制

WiMAX 採用 PKMv2 作為認證的基礎，與 WiFi 環境下的 802.1x 機制有許多類似的地方，且兩者均採用 EAP 作為認證訊息交換的標準。根據 WiMAX Forum 發佈的 Stage3[7] 文件中的規範，WiMAX Mobile Station(MS) 至少必須支援 EAP-TTLS 或 EAP-AKA 認證，但 EAP-AKA 在校園內應用的機會並不高。雖然 WiMAX Forum 規範文件中並沒有把 PEAP 納入，但 PEAP 挾著強大的作業系統內建優勢，因此也是可能被採用的 EAP 認證協定之一。如圖 4 所示為 WiMAX 使用者的認證流程。

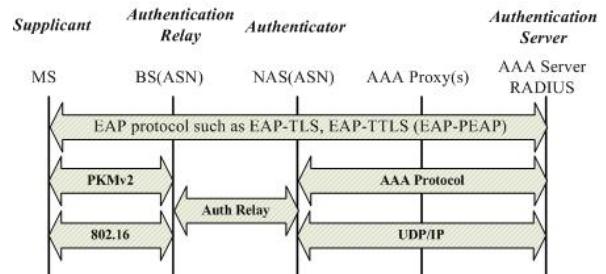


圖 4 WiMAX 使用者身份認證流程

因此考量 WiFi 與 WiMAX 網路並存環境下，我們可以列出如表 2 的認證機制搭配方案。

表 2 WiFi 與 WiMAX 用戶端認證機制

	WiFi	WiMAX
認證機制	網頁認證 PAP (802.1x)EAP-TTLS or EAP-PEAP	(PKMv2) EAP-TTLS or EAP-PEAP

在 WiFi 與 WiMAX 整合環境中，考量整合度與安全性的情況下，我們建議應該統一採用能夠支援 EAP 認證的機制。由於 WiMAX 本身已經規範採 EAP 認證，因此在 WiFi/WiMAX 共存環境中，WiFi 應強制採用 EAP 認證並搭配 WPA/WPA2 以強化連線安全。

如果考量 WiFi 環境是用來作為非敏感性資料傳輸或一般訪客上網之用，WiFi 也許可考慮繼續沿用方便簡單，卻不夠安全的網頁認證機制。只是使用者可能會對於選擇何種認證方式無所適從。不過使用者認證機制能否順利運作，還必須看後端帳號系統是否能支援而定，這部份我們將在後面的章節中說明。

4.3 帳號系統的認證支援

使用者帳號系統能夠支援的認證協定種類，可能會因為帳號系統本身的特性而受到限制。一般在校園 WiFi 環境中常見的帳號系統為 UNIX 系統帳號、LDAP 以及 SQL 伺服器等，也有少部分學校採用 POP3 認證。

下表 3 為在 WiFi 環境中，以 FreeRADIUS[6] 作為認證伺服器時，使用者帳號系統與認證方式支援能力的比較列表。

表 3 WiFi 環境認證方式與帳號系統的支援

	UNIX	LDAP	SQL	POP3
PAP	V	V	V	V*
EAP-TTLS	V	V	V	V*
EAP-PEAP	X	V	V	X

PAP 認證是最簡單的認證方式，因此各種帳號系統都能夠支援。PEAP 強制用戶端採用 MS-CHAPv2 來驗證密碼，因此若帳號系統以不可逆演算法將個人密碼編碼，將無法支援 PEAP，像

是 UNIX 系統帳號就無法支援 PEAP。另外 POP3 協定並無提供取出密碼的能力，因此也不可能支援 PEAP。相較之下 TTLS 的驗證機制比 PEAP 靈活，幾乎各種帳號系統都能夠支援，非常適合用來整合校園無線網路的 EAP 認證環境。

由於 WiMAX Forum 規範了 MS 端的認證機制必須支援 EAP 認證，因此 WiMAX 使用者的帳號系統也理所當然必須支援所選用的 EAP 認證類型。不管是在 WiFi 或是 WiMAX 環境，EAP 認證的本質特性是不會改變的，因此我們仍可以參考表 3 的資料，只不過 PAP 機制就不在支援之列了。

為了配合各校後端帳號系統的 EAP 支援能力，以及考慮跨校漫遊認證的方便，我們建議規劃 WiFi 及 WiMAX 環境認證時，應以採用 EAP-TTLS 為主，並視情況支援 EAP-PEAP 認證。在 WiFi 的網頁認證方面，我們也建議最好至少升級到 802.1x 認證。

4.4 認證伺服器軟體的選擇

在我們瞭解了使用者認證機制與後端帳號系統的關係後，認證伺服器的選擇將是讓整個認證流程運作起來的關鍵。

一般校園常用的 WiFi 閘道設備可能透過 LDAP 直接查詢帳號資料庫、或透過 POP3 驗證用戶身份。以本計畫協助各校建置無線漫遊的經驗來看，多數的學校都採用 RADIUS 搭配使用者帳號系統來做驗證。

根據 WiMAX Forum 的規範，WiMAX AAA 架構應符合 IETF 標準，例如符合 RFC2865、RFC2866 等標準的 RADIUS 或 Diameter 系統。幾乎所有的 WiFi 閘道設備都支援透過 RADIUS 來驗證使用者身份，但不一定支援 Diameter。因此考量在統一 WiFi 與 WiMAX 認證環境的前提下，我們建議採用 RADIUS 作為認證伺服器，未來再考視需求慮轉換為 Diameter。

目前在校園內運作的 RADIUS 系統大致上有有 Merit RADIUS、GNU RADIUS、FreeRADIUS、Cisco ACS、Microsoft IAS 等，除了 Cisco ACS 與 IAS 外都是自由軟體(Free Software)。表 4 為校園常見 RADIUS 支援的認證機制種類，其中以 FreeRADIUS 的支援能力最好，不過設定上也比其他 RADIUS 複雜一些。

表 4 RADIUS 認證協定支援表

	PAP/CHAP	PEAP	TTLS
Cisco ACS	V	V	X
MS IAS	V	V	X
M/RADIUS	V	X	X
G/RADIUS	V	X	X
F/RADIUS	V	V	V

上表中 Merit RADIUS 的開發目前已經停擺，而 GNU RADIUS 開發速度緩慢，且功能有限，都無法支援 EAP 認證。因此除了商業版本的 RADIUS 外，最強大的 RADIUS 系統莫過於 FreeRADIUS，且 FreeRADIUS 在校園內的普及率也是最高的。

為了能夠符合大多數 WiFi 與 WiMAX 並存環境的認證需求，並且考量各種新舊帳號資料庫的支援問題，我們強烈推薦採用 FreeRADIUS 作為校園無線網路認證的主要認證伺服器軟體。

4.5 RADIUS Accounting

由於 WiFi 閘道器均支援 RFC2866，且 WiMAX Forum 也規範 WiMAX ASN 閘道器必須支援 RFC2866，因此若無特殊需求，WiFi 與 WiMAX 閘道設備所產生的 RADIUS Accounting 資料將可送至同一部 Accounting 伺服器處理，如此可以避免多套 Accounting 伺服器所產生的成本及記錄管理問題，同時記錄整理工具也需要一套便可處理所有的記錄即可。其運作示意圖如圖 5 所示。

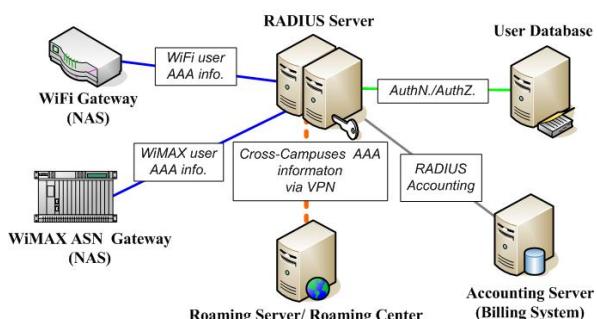


圖 5 Accounting 整合架構圖

以上我們介紹了認證機制、認證伺服器以及使用者帳號系統之間的關係以及配核能力，綜合來說採用 FreeRADIUS 結合 EAP-TTLS 認證環境，將能夠有最佳的整合效果。

5. WiFi 與 WiMAX 整合環境之建置

本章節將介紹由現有的 WiFi 認證架構轉換至 WiMAX 並存或相容架構的流程。

首先介紹校園內常見的無線網路認證架構，下圖 6 為常見的網頁認證架構圖。一般網頁認證採 PAP 認證，經由無線閘道器做存取控管，使用者認證則交由後端的 RADIUS 配合使用者帳號系統作處理。有的校園會直接以無線閘道器連接帳號系統做認證，如 POP3 伺服器、LDAP 伺服器等，這時 RADIUS 系統可能就不負責認證工作，而僅作為記帳之用。

在 802.1x 環境下的認證機制採用 EAP 認證，且後端必須搭配至少一套 RADIUS 系統才能夠支援 EAP，如圖 7 所示。

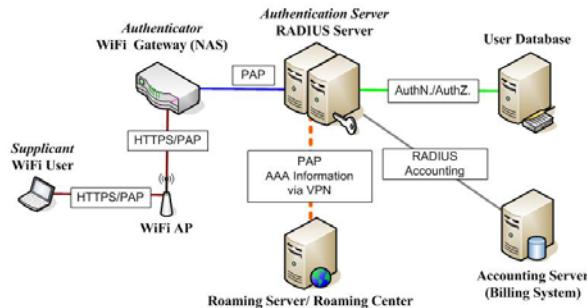


圖 6 校園 WiFi 環境使用網頁認證

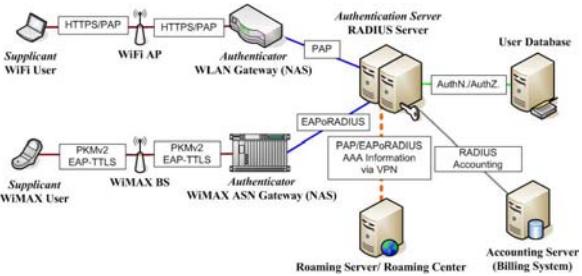


圖 9 WiFi 與 WiMAX 採用網頁與 EAP 認證

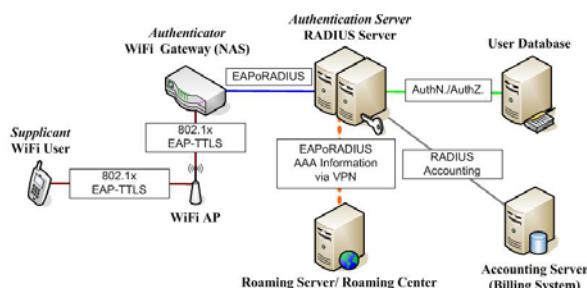


圖 7 校園 WiFi 環境使用 EAP 認證

下圖 8 為 WiMAX 獨立環境可能採用的認證架構圖，由於 WiMAX 採用 PKMv2 EAP 認證，因此架構與 WiFi 使用 802.1x EAP 的架構相當類似，最主要的關鍵是後端的 AAA 系統要能夠支援 EAP。

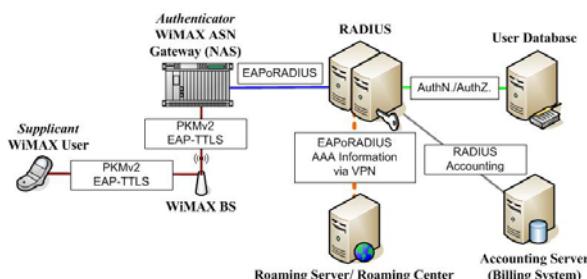


圖 8 校園 WiMAX 網路認證

在瞭解 WiFi 與 WiMAX 無線認證環境之後，我們便能夠很清楚的找出兩種認證架構能夠結合的地方，並進行整合。

5.1 WiFi 網頁認證與 WiMAX 的整合

我們的第一個考量是 WiFi 沿用網頁認證方式，並佈建全新 WiMAX 網路的情況，如圖 9 所示。

其實這樣的架構會比較混亂，也因此必須注意使用者選擇不同網路時該採用的認證協定。簡而言之，使用者使用 WiFi 網路時只要開瀏覽器即可認證，連線到 WiMAX 網路時，使用者也必須透過認證軟體進行認證，因此必須特別注意使用者的教育訓練問題，否則一般使用者通常都很難分得清楚何時該選用何種認證機制。

5.2 WiFi 802.1x 環境與 WiMAX 的整合

我們建議的整合架構是根據目前校園 WiFi 無線網路現況，並參考 WiMAX Forum 相關文件而提出。在這個架構中，WiFi 與 WiMAX 環境均採用統一的認證協定，例如 EAP-TTLS，其整合認證架構圖如圖 10 所示。

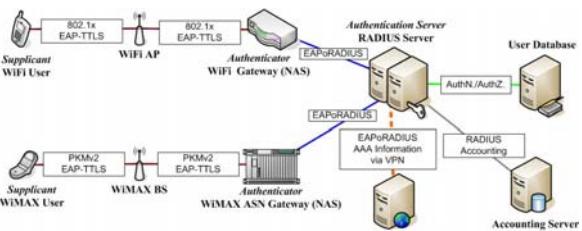


圖 10 WiFi 與 WiMAX 並存使用 EAP 認證

WiFi 與 WiMAX 共同採用 EAP 協定，由於使用者操作的都是一個外加的認證軟體，因此使用者在進行無線認證時的使用經驗落差會比較小。但很遺憾的，目前似乎尚無能夠整合 WiFi 與 WiMAX 的用戶端認證軟體出現，因此這部份能著墨的地方並不多。在 WiFi 環境下我們可以用 SecureW2、Xsupplicant、Wire1x 等軟體來使用 EAP-TTLS 認證，但這些軟體目前並不支援 WiMAX 的 PKMv2 協定。

另外此架構一律採用 EAP 認證，WiMAX 的安全性當然不在話下，最主要的是 EAP 環境也提高了 WiFi 環境採用 WPA/WPA2 的可能性。部分單位可能由於 WiFi 設備或少部分行動裝置老舊因而無法開啟完整的 WPA/WPA2，這並非使用者之福。

5.3 WiFi 與 WiMAX 整合仍待解決的問題

其實 WiFi 與 WiMAX 環境的整合，只要帳號系統及 RADIUS 環境能夠互相配合基本上就不會有太大的難題，但在 EAP 認證環境下，最重要的元件之一就是用戶端的認證軟體，軟體的親合度將決定使用者的使用意願。一般支援 EAP 認證的無線網卡多有附送支援 EAP-TTLS/EAP-PEAP 的認證軟體，但目前 WiFi 與 WiMAX 的認證軟體是不相容的。

雖然說 WiMAX 環境下的開放源碼用戶端認證軟體目前可能還難以尋覓，但致力於此的自由軟體工作者，相信不會輕易放棄 WiMAX 用戶認證軟體之研究。故我們所關心的，是如何讓校園的後端帳號認證環境為 WiMAX 做好準備。至於可適用於 WiFi 及 WiMAX 共存校園環境之用戶端軟體，我們則建議國內 Open Source 之研究團隊來一起合作。

6. 結論

早些年前，WiMAX 原只是遙遠的技術名詞，在今年，學界、業界或政府推動的各項 WiMAX 測試、建置計畫都正在積極的規劃佈建，各 WiMAX 廠商的 WiMAX CPE 與用戶端設備也開始在市場上嶄露頭角，不難想見 WiMAX 在未來各項無線寬頻應用的重要性。

經由本文的介紹，讀者應已發現從 WiFi 環境升級到 WiMAX 或是與 WiMAX 並存的環境，最重要的關鍵在於無線網路認證後端架構對於 EAP 認證機制的支援能力。考量現有的校園無線環境及其後端架構，我們建議全面採用 FreeRADIUS 作為認證伺服器，並採用 EAP-TTLS 認證協定，一併解決前端的認證機制以及後端的帳號系統支援問題。

我國校園要廣泛佈建 WiMAX 環境還需要一段時間，但若有心打造校園 WiFi / WiMAX 環境，我們現在就可著手規劃未來整體配套，達到至少是可宣稱為 WiMAX 已有完善的準備。

7. 參考文獻

- [1] 校園無線漫遊機制整合實驗與推廣計畫網站，
Jul. 2007, <https://wlanrc.nchc.org.tw>
- [2] 唐可忠，黃偉航，蔡志宏，“校園無線漫遊認證機制安全與 802.1x PEAP/TTLS 環境建置”，TA
NET2006, Nov. 1st-3rd, 2006.
- [3] 魏學文，陳彥文，周立德，吳中實，吳曉光，陳
文雄，楊峻權，陳恒佑，吳坤熹，李天序，“802.
16 試驗網路建置與效能評估”，<http://www.nsc.gov.tw/eng/public/Attachment/762010302571.doc>
- [4] IEEE, “802.1x Port-Based Network Access Co
ntrol”, Dec. 2004, [http://standards.ieee.org/getiee
ee802/download/802.1X-2004.pdf](http://standards.ieee.org/getiee
ee802/download/802.1X-2004.pdf)
- [5] IEEE, “802.16e-2005”, [http://standards.ieee.org/
getieee802/download/802.16e-2005.pdf](http://standards.ieee.org/
getieee802/download/802.16e-2005.pdf)
- [6] The FreeRADIUS Server Project, May. 2006,
<http://www.freeradius.org/>
- [7] WiMAX Forum, “WiMAX End-to-End Networ
k Systems Architecture Stage2-3 Release 1.0.
0”, [http://www.wimaxforum.org/technology/docu
ments/WiMAXNetworkArchitectureStage2-3Rel1.
0.0.zip](http://www.wimaxforum.org/technology/docu
ments/WiMAXNetworkArchitectureStage2-3Rel1.
0.0.zip)