

新世代校園無線區域網路應用實驗計畫(總計畫)

計畫類別：整合型計畫

計畫編號：NSC 91-2219-E-002-049

執行期限：2002.10.01 至 2003.09.30

總計畫主持人：蔡志宏教授

子計畫主持人：楊竹星教授、賴溪松教授、李新林教授、孫雅麗教授、  
陳志成教授、陳奕明教授

執行單位：國立台灣大學電信工程學系

一、 中英文摘要

有鑑於近年來我國 WLAN 的迅速發展，但目前在校園內大量佈設 WLAN 之學校，因受限於教育經費，數量不多。在教學方面，大部份大學僅在電腦網路課程略有提及 WLAN。而在研究計畫方面，WLAN 計畫數量亦相當有限，不足與國際發展趨勢相配合。為能充分掌握此一領域所有重要 know-how 及趨勢。電信國家型計畫為積極推動校園 WLAN 環境建置與應用技術開發，電信國家型計畫規劃本規劃建置案，依各大學專長領域規劃研究主題，以進行各項 WLAN 應用技術的研究及先導性實驗。為有別於一般國科會研究計畫，本規劃建置計畫中技術之開發研究，以能投入實際 WLAN 上網服務，提供跨校應用者為限。

本群計畫由各子計畫執行學校利用其自行建置之測試網路實機測試，並依本總計畫之分工規劃重點分別進行互連及可行性評估，而後進一步在未來完成校園成果並將擴散至國內其他有意建置 WLAN 之校園。規劃重點技術包括 Authentication/Roaming 技術、Mobile IP、入侵偵測與 Security、e-learning、video/audio multicast、PDA 應用、VoIP 以及網路管理 (含 WLAN Mobility Management)。本計畫係運用各校電算中心之資源及人力、結合各校從事 WLAN 相關研究之人力，再配合實際測試之工作，以建立校園 WLAN 公眾區域上網服務可實用的架構。本計畫執行過程中並與 WLAN 產業界技術交流，並建立技術合作模式。本計畫之應用成果十分豐富，故將本計畫做成果擴散，並把應用心得與產業界及學術界共同分享。

Abstract

In recent years, the WLAN equipment is rapidly developed, but the less school campus has deployed the infrastructure of the WLAN environment. The WLAN concept is just mentioned in the university class. The amount of the WLAN research project is also limited. In order to handle the WLAN know-how and the international trend, the National Telecommunication Program give the impetus to the WLAN campus deployment and the development of the WLAN application. In this project, some universities with the specific field are invited to propose their ideas and proceed to take some researches of the WLAN application techniques and the trial experiments. The participated universities in this project include the National Taiwan University (NTU), National Central University (NCU), National Tsing Hua University (NTHU), Chung Cheng University (CCU), National Cheng Kung University (NCKU), and National Sun Yat-sen University (NSYSU). The planned key technologies include authentication/ roaming, mobile IP, intrusion detection and security, e-learning, video/audio multicast, PDA application, VoIP, and the network management. (ex. WLAN Mobility Management) The manpower and the resource of the computer center of the participated university is also used to

operate in the coordination in this project to finish the practical trail for the feasibility study of the public WLAN in the campus environment. The research results are also shared with the industrial circle and generate some collaboration models in the technology. Besides, the experience of the deployment in the WLAN infrastructure and the development of the WLAN application have been demonstrated in some conferences and spread to many schools.

## 二. 緣由與目的

我國無線區域網路設備的製造能力，在過去幾年間延續我國 Ethernet 區域網路的量產能力，已經突飛猛進。不論是無線接取點 (Access Point) 或是無線網路卡 (NIC) 等硬體，台灣皆已逐步成為全球第一的生產重鎮。下一步的發展重點則應朝向屬於軟體為主的無線區域網路應用服務，以及無線區域網路閘道器 (WLAN Gateway) 等高附加價值之產品。

此外，近年來由於我國早已成為筆記型電腦的主要生產國，因此不少筆記型電腦大廠早已投入相關設備研發。但是在與服務及應用必須充分整合的軟體部分，仍有許多追趕的空間。同樣地，近年來在行動電話或寬頻網路電信服務市場以積極擴展有成的電信業者或 ISP，如中華電信等，亦均已參照國外發展狀況，開始在國內廣佈公眾上網用的 WLAN。雖然我國國內產業界對 WLAN 反應熱烈，但在教育及學術界對 WLAN 之推廣、應用、教育、研究工作，均仍有擴大加強之必要。

以實際佈建而言，目前在校園內大量佈設 WLAN 之學校，因受限於教育經費，數量不多。在教學方面，大部份大學僅在電腦網路課程略有提及 WLAN。而在研究計畫方面，WLAN 計畫數量亦相當有限，不足與國際發展趨勢相配合。但由於有多項 WLAN 研究議題都與我國無線產業發展息息相關。我國學術研究單位及各網路中心，各校執行電信國家型科技計畫及追求卓越計畫單位均有必要投入先期研究，並共同分工整合，以充分掌握此一領域所有重要 know-how 及趨勢。

## 三. 達成之計畫成果

為能充分掌握此無線區域網路中所有重要技術及趨勢。電信國家型計畫積極推動校園 WLAN 環境建置與應用技術開發，並依各大學專長領域規劃研究主題，以進行各項 WLAN 應用技術的研究及先導性實驗。在本計畫中所規劃的重點技術包括 Authentication/Roaming 技術、Mobile IP、入侵偵測與 Security 控管、e-learning、PDA、video/audio multicast、VoIP 以及網路管理 (含 WLAN Mobility Management) 等。在經過一年計畫的執行後，各項子計畫成果均十分豐富。各子計畫所達成成果詳述如後。

### 子計畫一：在跨校漫遊與安全控管防護環境下支援個人化網路通訊系統

隨著網際網路的蓬勃發展，與無線區域網路技術的成熟，為了進一步推廣無線區域網路與吸引大眾主動的使用，各系統商所設計與建構之無線區域網路環境的便利性、安全性與互通性，則可視為左右其成敗的最大因素。如何設計與建構一兼具便利、安全、互通性的無線區域網路環境為此間最重要的課題。有鑑於此，本子計畫主要在探討支援異質性漫遊環境之無線區域網路安全控管系統的設計與實作。

本計畫目前之成果可運用在 multi-domain 架構與跨 ISP 的大規模漫遊需求的無線區域網路環境之建置與管理，其最大的特色在於可支援異質性的他網無線區域網路認證平台之使用者漫遊、可跨作業系統平台安裝的系統程式、可擴充、容錯的系統架構。此外，可外掛具有自動化與自主性的異常行為防禦反應的子系統 (如：入侵行為、網路病毒事件的及時偵測、反應與處理)。

此外，為配合於年初一月四日起的國家電信型第一期期末展示計畫之展示活動，除原計畫中預定之成果 (目前皆已完成)：

- (1) 提供一具使用者透通性與支援異質性認證平台之校際無線區域漫遊機制。
- (2) 提供校園公眾無線區域網路環境安全控管防護機制

擬在系統中加入多項新增之特色：

- (1) 入侵者偵測及防禦反應子系統
- (2) 整合性中央管理系統 (包含無線區域網路與入侵偵測防禦)

- (3) PDA 版整合性中央管理系統
- (4) 大區域無線網路導覽系統(市區、觀光景點導覽)

#### 子計畫二：無線群播網路影音串流技術與應用平台建置

本計畫無線群播網路之影音串流技術與應用平台建置的主要目標，是要以 NBEN/TANET 網路為基礎，在 Intra-campus 方面先以成大校園建制一 Wireless 網路系統架構，並以此系統架構為基礎，進一步發展與建置多媒體群播無線網路應用系統。在 Inter-campus 方面在與中正大學等學校合作建立一跨校 Wireless 網路系統架構並在此架構上發展多媒體群播網路應用系統。

為與業界的 Content Provider 進行整合，使上述之以 NBEN/TANET 為基礎的群播無線網路平台得以推廣與建置於各大院校校園網路環境中，本計畫中將以 windows media server 為測試商業多媒體展示系統，利用一系列的實驗測試 multicast 項目加以分析建議，以提高與業界結合之彈性與整合。

本計畫設計了單一路由器、多個路由器等相關實驗場景，完成了以下項目：

- (1) 高傳輸率無線串流群播在接收端接收訊號強的實驗
- (2) 低傳輸率無線串流群播在接收端接收訊號強的實驗
- (3) 高傳輸率無線串流群播在接收端接收訊號弱的實驗
- (4) 低傳輸率無線串流群播在接收端接收訊號弱的實驗

由於多媒體以使用 multicast 技術傳輸為最有效益，但在 multicast 傳輸中，封包的轉送是不可靠傳輸，因此封包遺失情形將會影響多媒體的接收播放情形，我們以 Windows Media Server 為網路傳輸廣播站來傳輸多媒體，包括影像與聲音，經由多媒體傳輸可觀察：

- (1) 無線傳輸封包遺失情形
- (2) 無線傳輸封包遺失對多媒體接收情形
- (3) 切割最適封包大小以減低無線封包遺失情形

我們也積極與外界合作藉以提供多元化的內容以提高使用者的意願，目前已與 Kiss Radio 簽約三

年，得以使用其廣播的內容，使得群播的來源多元化以達到產學合作的趨勢。

#### 子計畫三：發展 e 化校園之無線域網路技術

本計畫之主要目的是希望利用 WLAN 技術，加強校園在無線通訊的技術應用及整合。主要的工作方向是除加強現有無線通訊安全性及將現行本校使用 e-learning 教學平台 m-化，對於校園的無線多點傳輸及一些行動載具的應用，也做了許多的技術開發及應用，完成 的各項主要工作分述於下。

- (1) 校園無線上網：利用 Free RADIUS Proxy 建立校園內及跨校漫遊認證，並實作一實驗系統使用 VPN client 的軟體連往校園內部，VPN 加強無線通訊安全，及統計個人使用流量及連線時間。
- (2) 網路教學平台 m-化：將本校自行發展通過 SCROM 標準的 e-learning 教學平台，配合行動載具，及自行設計的討論平台 e-board，建置一個無線網路學習環境。
- (3) 無線傳輸技術的研發：此方面我們對於在廣?校園內提供了如何利用 ad-hoc 及無線 infrastructure 進行多點傳輸，並對於使用者在處於多個 AP 的環境下，自動轉換至訊號最強 AP 的系統功能開發。
- (4) 無線通訊在 PDA 上的應用：利用無線通訊功能，結合 PDA 將資料庫由遠端傳輸，進行校園內違規車輛的管理及註記。本項計畫之實施，使參與者除了全盤了解在校園 m-化方面的工作外，對於未來許多值得繼續努力的方向有了更明確的方向，如教學平台 m-化；如何配合最新的 client 端軟體更新功能；在廣?校園內，如何利用多點傳輸，使校園內的無線通訊仍能有效運作；各式的應用如何結合校園生活，使其更為便利。由於無線通訊技術不斷提升及普及，未來校園 m-化的發展是必然的趨勢，本計畫之執行使參與者在此方面獲益良多。

#### 子計畫四：無線區域網路實驗計畫

本研究計劃的目的在於研究 WLAN Management 之相關研究議題以及應用管理軟體。研究議題包括：Access Point (無線網路的接取節點) 之管理、Auto Network Topology Discovery (網路拓模自動搜尋)

的技術、網路中不合法 AP 的偵測方法。

- (1) AP2000 是一套管理單一 Access Point，提供 Web-based 介面來即時監控 AP 的系統，主要分為 Configuration(監控、更改 AP 的設定)、Management(觀看網管資訊及統計網路流量)、Command(即時對 Device 下指令)三個部分，而能夠使得 AP 的控管，無論在 Network、Interface、Bridge、Security 各方面，皆達到管理者的需求。
- (2) Auto Network Topology Discovery 之技術方法提供管理者關於所轄網域內的所有網路設備的資訊。透過演算法設計以及 SNMP (Simple Network Management Protocol, 簡單網路管理協定) 工具，可以自動找尋出所轄網路下的所有網路設備，並且針對網路層 (Network Layer) 以及鏈結層 (Data Link Layer) 繪出其網路拓模 (Network Topology)。此段探討其演算方法及優劣、拓模發現之困難與解決方法、SNMP 工具的配合使用以及實際應用於網路上之成果。配合圖形化的介面設計此系統可以讓管理者更方便的管轄區域網路內各種設備的狀態，並隨時作追蹤，以提供網路管理者最迅速的協助。
- (3) 私自架設一個不屬於原有企業網路架構中的 Access Point，提供透過 Wireless 端存取網路的服務，即是所謂的 Rogue AP，這將會造成企業網路安全上的疑慮。因此 Rogue AP Discovery 是當今無線區域網路管理上的重要議題之一，我們的做法分為以下兩部份：一、如何透過在 Wired 端、接續 Network Topology 演算法而繼續對於可能為 AP 的 Device 作 Query 的方法；二、在 Wireless 端定期掃描 Rogue AP 發送的無線訊號的方法。由此雙管齊下發現 Rogue AP。

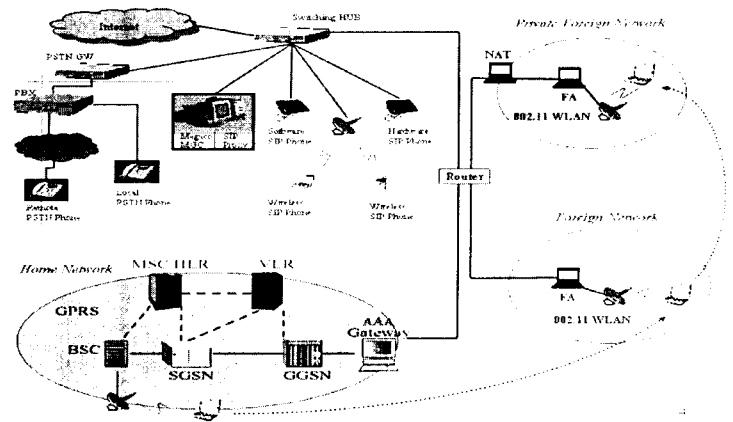
#### 子計畫五：視訊會議在無線區域網路與 Mobile IPv6 中之建置測試及分析

本計畫目前已完成一 IPv6 之校內網路環境建立，並且安裝了 Mobile IPv6 系統；另外我們也建立一個以 SIP 為連線訊號協定、做到流量控制且加入視訊會議之系統。

同時，為了完成一 wireless VoIP 之校內的網路環境

建立，我們準備了 hardware 與 software 之 SIP phones 以提供給使用者測試。在計畫中，我們進行了各項 VoIP 與視訊會議在有線與無線網路上使用情形之測試與分析，並提出量測數據。

本計畫所建置的 Testbed 的架構說明，如圖一，左下方為工研院所開發的 GPRS 系統，右下角為 Wireless LAN，右上角為 NAT，左上方也是工研院所開發的 VONTEL VoIP 系統。透過 Gateway 的連結以及 IP-in-UDP Tunnel 的機制，Mobile Node 得以順暢地漫遊於 GPRS, WLAN, 以及 NAT 之間；此外透過 PSTN Gateway 的介接，在 Testbed 上的視訊會議系統可以延伸至一般的市內電話或者手機等。



圖一

#### 子計畫六：從入侵者角度檢驗 Wireless LAN 安全問題的實驗計畫

近年來，隨著國內無線區域網路產品大幅降價，802.11 無線區域網路在國內迅速普及，但隨之而來的網路安全問題也隨之受到大眾矚目。跟隨此網路發展趨勢，本計畫即由網路入侵者的角度來檢視無線區域網路的安全問題，我們的目的是希望從理論和實務的觀點，探討現有無線區域網路安全機制部署的弱點在哪裡？有哪些地方可以事先予以防範？目前，我們得到的成果可以分成三大部分：

- (1) 我們已整理出目前無線區域網路安全問題的關鍵。我們發現除了因管理不善造成的安全問題之外，以 ARP spoofing 技術來進行的 man-in-the-middle 攻擊對無線區域網路造成最大的安全威脅。我們以實驗證明，目前常見的以 web 介面進行使用者身份

認證的機制，將可以讓駭客輕易地假冒無線存取節點 (AP) 而取得使用者的連線資訊，包括 https 以及 ssh 加密過的資訊。

(2) 我們已發展出結合入侵偵測系統與防火牆兩種功能的入侵偵測與預防系統 (IDPS)，並將此系統的雛形建置在 host AP 上，使 AP 能夠及早發現無線區域網路上的異常活動，並及時予以阻絕，避免造成進一步的損害。

(3) 本計畫也和中央大學電算中心密切合作，持續地以所獲得的知識與技術，改進校園無線區域網路的安全。

綜合來說，本計畫已大致達成原訂的目標。我們從入侵者的角度，將網路上現成的工具加以整合與改寫利用後，的確發現現有無線區域網路的安全機制有許多漏洞而有可趁之機。我們的研究結論是目前公眾場所所佈建的無線區域網路，仍容易受到 man-in-the-middle 攻擊，因此在 AP 端需要有偵測機制，才能及早偵測攻擊事件是否發生。我們對此入侵偵測系統做了研究並發展一套 IDPS 雛形系統，未來值得為此系統的有效性與效能進行後續的研究。

#### 四. 結語

隨著無線網路通訊技術的快速發展與校園公眾無線區域網路的普及化，校際間無線網路資源整合與各類應用的需求在近幾年間將以驚人的速度快速成長。有鑑於此，電信國家型計畫積極推動校園 WLAN 環境建置與各項新的網路應用技術開發，並依各大學專長領域邀集相關負責教授，包括台大、清大、中央、中正、中山、成大等，與國家實驗網路人員共同參與此項計畫，以 NBEN/TANET/TANET 2 網路為基礎，建制一橫跨各參與計畫大學之 Wireless 網路系統架構，使各項 WLAN 應用技術的研究及先導性實驗得以在此平台上順利開展。

在此計畫中我們建立一個新世代跨校園的無線網路應用雛型，具有 IEEE 802.1x 安全漫遊能力，支援多元服務，並在網路安全議題上整理出目前無線區域網路安全上所遭遇到問題的關鍵，和發展出結合入侵偵測系統與防火牆兩種功能的入侵偵測與預防系統 (IDPS)，使得在無線區域網路上的異常活動能及早發現，並及時予以阻絕，避免造成進一步的損害。

在推廣校園無線網路應用方面，本計畫對於無線區域網路的相關技術議題上，提供了網路管理、視訊會議、移動式 IPv6、e-Learning、群播技術、隨選視訊、認證方式等技術與應用的研究指引與解決方針，各項成果也陸續推廣於個校園中使用，獲得相當的成果。

以上此計畫所獲得相關之網路建置與各項主要多媒體應用系統之架設技術均建立了完整的技術手冊與參考資料，短期內可作為 NBEN 骨幹網路應用平台與其它各研究機構在推廣無線網路建設之重要參考依據。長期而言也為我國在下一代網路建設之奠定了重要基礎。

最後本計畫之成果已於 TANET2003 研討會及 NTP 成果發表會上展示各項建置之網路應用，各子計畫之研發項目亦有多篇相關論文發表。此外，在計畫成果推廣上，除了積極在國內各校園推廣外，並已主動對 WLAN 相關的產業界進行介紹並建立彼此之合作關係，期望能將此計畫各項成果順利的移轉至產業界以提昇國內廠商在無線區域網路上之競爭力。