國 立 交 通 大 學

資訊學院 資訊學程

碩 士 論 文

智慧型行動熱點系統

Intelligent Portable Hotspot System

研 究 生： 賴文聖

指導教授： 蔡文能 教授

林正中 教授

中 華 民 國 一0一 年 七 月

智慧型動行熱點系統

Intelligent Portable Hotspot System

研 究 生：賴文聖　　Student：Wen-Sheng Lai
指導教授：蔡文能　　Advisor：Dr. Wen-Nung Tsai
林正中　　Dr. Cheng-Chung Lin

國 立 交 通 大 學
資訊學院 資訊學程
碩 士 論 文

A Thesis
Submitted to College of Computer Science
National Chiao Tung University
in partial Fulfillment of the Requirements
for the Degree of
Master of Science
in
Computer Science
July 2012

Hsinchu, Taiwan, Republic of China

中華民國一０一年七月

智慧型行動熱點系統

學生：賴文聖　　指導教授：蔡文能教授
林正中教授

國立交通大學　資訊學院　資訊學程　碩士班

摘　要

近年來具有高速運算能力的行動裝置不斷地推陳出新，擁有二個以上行動裝置的使用者不在少數；加上網際網路應用的演進與行動產業的改變，使得網路流量需求遠大於無線頻寬技術提升的速度。原有的電信網路設備不僅要提供語音通話服務，對於資料傳輸的頻寬需求也正快速地增加，行動網路基地台負擔也因此變得越來越沈重。為了因應各種行動設備的上網需求，但又不想擴大行動網路建置成本的情形之下，可以利用 multihomed 系統中負載平衡(load balance)與備援(failover)的概念來達到負載移轉(offload)之目的，讓網路流量可以分流到其它網路。

本研究主要是透過其它異質網路的佈建，把行動裝置的網際網路流量分散到不同的異質網路上。讓行動網路基地台不會因為人口密集度過高，而導致服務品質下降。例如在公共區域佈建無線熱點(hotspot)，提供各種行動裝置的網際網路資料傳輸的需求。

本研究設計了智慧型行動熱點系統，本系統在網際網路端整合了多種異質網路，利用本研究所設計的軟體框架來管理異質網路的連線行為，提供網路環境感知與自動轉換各種網際網路的連線能力。我們利用 IEEE 802.11 無線網路技術的普及性與佈建成本較低的特點，以無線熱點建設為基礎，提供網路流量負載移轉(offload)的能力，並整合了無線網路熱點自動認證功能，讓各種行動裝置都能輕鬆又方便地共享網路資源。在戶外的行動裝置可以透過本系統所成形的獨立行動區域網路直接通訊，相對於行動設備直接與外界通連的情況，本研究成果可以提供使用者多一層網路安全的保障。

關鍵字：無線網路、熱點、備援、流量負載移轉、異質網路

Intelligent Portable Hotspot System

student:Wen-Sheng Lai Advisor:Dr. Wen-Nung Tsai
Dr. Cheng-Chung Lin

Degree Program of Computer Science
National Chiao Tung University

ABSTRACT

In recent years, lots of powerful mobile computing devices had been introduced. Many people do own more than one mobile device. They use these devices to access Internet services such as email, instant message, watching movices or listening music, updating social network status and downloading mobile applications. The bandwidth requirements are much more than the evolution of wireless technology can provide. Network traffic congestion is now a serious problem for carriers, especially in the populated areas during peak usage times.

The purpose of this study is to find a way to offload the traffic from mobile networks.We make use of the properties of multi-homed networks to design the Intelligent PortableHotspot System (IPHS). This is a network management frameowork for heterogeneous network which provides network aware perception, management and hotspot authentication.

In our study, we integrated heterogeneous network interfaces to extend the accessibility of the network services. Based on the WiFi hotspot infrastructure with low-cost wireless broadband service, the experimental results show that our system can offload the traffic automatically in the densely populated areas.

Keywords: Wireless Network, Hotspot, failover, offload, Heterogeneous Networks

誌　　謝

本論文得以完成首先要感謝的是我的指導老師 蔡文能教授，您在研究方面給了我最佳的指引，尤其是每次論文研究的會議中提供各種建議與指導，讓原本對論文毫無頭緒的學生我終於能夠逐步往正確的方向邁進。在您耐心的指導與不厭其煩的反覆討論的過程中，最終本論文得以順利完成。

在學習的過程中，感謝學校老師們在課堂上的細心教學，讓學生重拾對讀書的信心與樂趣，在不同的領域得到新的知識，許多寶貴的經驗使學生獲益良多。同時要感謝我的同學以及同事們在這段時間給予的協助，讓我在學業與工作上可以順利兼顧。最後我想感謝我親愛的家人們，感謝你們這一路走來的體諒與支持，讓我在生活事務上無後顧之憂。需要感謝的人還有很多，僅以此論文獻給所有關心我的人，希望自己過去的努力沒讓你們失望，再次感謝大家並祝福大家身體健康，萬事如意。

賴文聖 謹誌

2012年7月

目　　錄

表目錄

圖目錄

一、緒　　論

網際網路早期的營運模式是以入口網站（portal website）的方式，提供使用者綜合性的資訊服務。但隨著網路頻寬日漸提升與雲端技術的普及，網路服務經歷了許多變革。內容的提供者不再是特定的公司或組織，進而演變成使用者與使用者之間的訊息傳遞和分享上面，而提供這類服務的網站形成了所謂的社群網路（Social Network）。

近年來由於手持式硬體設備的進步，具有高速運算能力的行動裝置不斷地推陳出新，行動裝置使用網際網路服務成為了基本功能，人們對於網路服務的黏著度也顯著提高許多。這一點大大地改變了人類的生活溝通、娛樂方式以及消費模式等，因此行動上網顯然已經成為人們日常生活不可缺少的一環，無論身處何處，總是習慣地能即時地瀏覽網頁取得資訊，或分享與記錄個人當下正在發生的人事物。但是這樣的便利性也為使用者與網路服務提供者帶來了難題。

由於行動設備所提供的上網介面有限，加上 3G 行動網路模組成本較高的情況，除了智慧型手機或較高階的平板電腦，許多行動裝置的無線網路介面仍是以 IEEE 802.11 技術的規格為主。另外行動網路的存取服務大都採取用戶帳號綁定的方式，使得消費者必須為不同的行動設備分別申請門號，才能同時連上網際網路。消費者除了多一筆花費之外，行動設備之間的資源也不易共享。而網路服務提供者方面也面臨資源不足的窘境，在單一基地台的服務區域內，行動上網的人口如果太過於密集，局端設備為了服務多用戶與語音話務的需求，基地台會無法同時負荷如此大量的行動頻寬上網需求，這將導致網路服務的品質降低，客訴問題也將層出不窮。如果選擇投資更多的電信設備，這不僅需要龐大的金額，佈建基地台也會面臨不少的難題。因此，未來電信業者可能會採取以頻寬大小或流量來分段計費，並在公共場所、商圈景點等人口較稠密的區域，以佈署無線熱點(WiFi Hotspot)的方式來分擔行動網路基地台的流量。

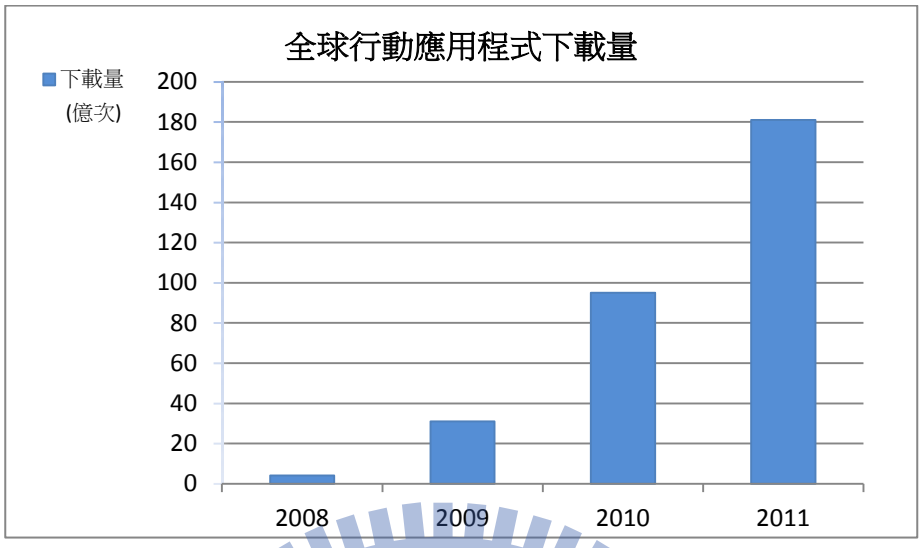
本篇論文將針對這二方面的難題提出解決方案，本研究將實作具有IPHS（Intelligent Portable Hotspot System）系統功能的IP分享器，提供大多數行動設備都支援的網路介面，以因應各種異質網路介面的上網需求。IPHS是一種容易客製化和移植的系統，提供使用者及網路服務提供者不同的需求，在客製化的條件設定之下，可以自動地為使用者找尋找較佳的網路服務，以達到頻寬分流(offload)的目的。讓使用者能無感地使用各種異質網路，不用去思考目前應該要使用什麼介面上網或者需要手動去切換不同的上網方式。本研究將採用現有的無線網路技術，在不需要修改現存網路架構之下為前提，對於各種行動設備及異質網路都能達到良好的整合與支援。冀望對於頻寬分流與自動化網路服務的研究上能有所貢獻。

1.1 研究動機

IT研究與顧問公司(Gartner)公佈了2010年全球手機終端銷售量達到了16億支，而智慧型手機正快速興起，急起直追，因為它比去年的銷售量成長了72.1個百分比，佔整體行動通訊設備銷售比重達19個百分比。並預估在2015年，全球智慧型手機的市佔率將超過一半。而手機產業轉變所形成的生態圈，其軟體市集的概念推出之後，根據統計全球行動應用程式下載量在2011年時高達到181億次，歷年統計資料(表 1)中顯示是去年下載量的將近二倍之多。市場研究機構In-Stat更是預估智慧型手機應用程式將於2015年時下載量將可能達到480億下次。

早期行動裝置(如PDA,Palm等)軟體是以提供商用服務為主要目的，但近年來的下載類別研究報告統計中(圖 1)，社群網路與新聞多媒體娛樂類所佔的比例高達66個百分比。統計數據意味著行動應用程式不在是以商務導向為大宗的軟體程式，而是與大眾生活更貼近的資訊與娛樂相關的應用程式。這樣的趨勢使得網路頻寬的需求不斷提升，大量的行動裝置同時連上行動基地台將招致頻寬不足的災難，而電信網路系統也會變得更加擁塞，這種情況會讓行動裝置應用程式無用武之地。

表 1 全球行動應用程式下載統計



智慧型手機的資料傳輸量是普通手機的 24 倍。行動裝置產業在不久的未來即將面臨頻寬不足的災難，人口稠密地區和尖峰時刻的流量將呈爆炸性倍增，這會迫使電信業者調高費率、限制使用者資料傳輸的上限。這結果反而不是大家所樂見的，因為無論是雲端服務、行動應用程式、網站瀏覽、多媒體影音串流..等都需要網路頻寬，所以使用者、應用程式開發者、電信公司和設備製造商反而都有可能深受其害。

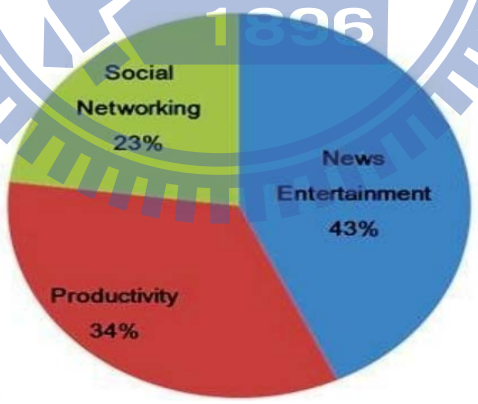


圖 1 2011 年行動應用程式下載類別與比例
資料來源：In-Stat

如果電信業者一直擴充行動網路通訊設備，大量投資大型基礎建設，在滿足消費者的傳輸量需求之前，行動網路業者很快就會開始面臨虧損命運。有鑑於 DSL(Digital Subscriber Line) 和 Cable modem 等固網技術的發展，讓最後一哩(last mile)的寬頻解決方案獲得莫大的成功。因此，本研究思考

是否可藉由既有的固接網路,配合區域性的無線熱點來卸載(offload)流量到不同的網路上，讓行動網路使用者與電信服務商雙贏的局面。

1.2 研究目標

本研究的目的在利用既存的硬體設備及網路環境，以不改變使用者上網習慣、不增加行動網路基地台等條件之下，以網路資源共享、降低費用為主要的研究方向，當然也要兼顧使用者經驗、網路安全性及易於部署等考量，提出智慧型行動熱點的系統架構。此系統架構預期可提供下列功能：

- 異質網路管理

  隨著無線技術的進步和行動裝置的發展，使得行動裝置可以同時內建不同的無線技術。例如，IEEE 802.11、UMTS、WiMAX和LTE等。如何控制、管理和支援這些異質行動網路介面是本系統研究的目標之一。
- 網路感知與自動選擇

  當行動裝置具有多重網路介面時，為了達到自動切換上網介面，必需有一套方法可以偵測網路環境，並自動為使用者選擇符合需求的網路。
- 行動網路頻寬共享

  本系統除了可以在無線熱點範圍內把網路負載分流至該當區所提供的無線網路之外，還提供了行動區域網路的概念，可以提供各種不同的行動裝置同時存取網際網路服務或本地端互相通訊的能力。
- 無線熱點自動認證

  本系統將內建自動熱點認證的功能，因為公共區域的熱點服務除了與無線網路AP的建立連線之外，通常還需要經過用戶登入的動作才能真正地存取網際網路資源，本系統將自動地幫助使用者登入無線熱點服務，讓使用者在使用熱點服務時可以無感，有如在家裡使用無線網路一般。

本系統整合了異質網路，在不同網路環境之下使用的情境如圖 2。目標是可以在各種環境都能提供良好且一致性的網際網路服務。

圖 2 IPHS使用情境

1.3 論文架構

本論文有六個章節，第一章緒論，首先說明本篇論文研究的動機，以及預計系統能達成的目標。第二章為背景知識，說明設計本系統時所需要的背景知識與技術，內容著重於無線網路、無線網路安全與熱點認證等相關技術的介紹。第三章相關研究將介紹專家學者們所提出的研究技術與文獻，包含異質網路管理、無線熱點認證的架構與方法以及家用閘道器的設計等。

第四章將說明本研究－智慧型行動熱點系統(IPHS)的系統架構與各個模組功能，參考背景知識和相關研究中所探討的技術和概念加以整合之後，實作本研究以達成系統的需求。第五章是本系統的建置與分析，首先會介紹本研究在開發時所使用的軟硬體平台，以及若干個重要的應用程式介紹。接著是系統建置完成後的實測成果，針對系統的功能擬定實驗方法並評估其效能。最後，第六章將依據本系統的實作成果，分析本系統功能與其所達成的目標，並說明本研究的結論以及未來的研究方向。

二、背景知識

本系統整合了有線網路、無線網路及行動網路等技術，並配合佈建在公共區域的無線熱點作為行動網路流量卸載的目標，因此為了解本系統實作與實際的應用，本章內容將著重於介紹無線網路相關的背景知識，內容包含IEEE 802.11 無線區域網路技術、IEEE 802.11i 認證標準以及 Wi-Fi 聯盟為無線熱點漫遊機制所制訂的標準-WISPr 等。行動網路也是本系統主要的網路介面之一，本章最後一節將簡介行動網路相關的知識與發展現況。

2.1 IEEE 802.11 無線區域網路概論

在1997電機電子工程師學會（Institute of Electrical and Electronics Engineers，IEEE）制定出無線網路通訊標準的第一個版本—IEEE 802.11[10]標準。IEEE 802.11標準定義的範圍主要是著重在無線區域網路（WLAN）中實體層（PHY）和媒體存取控制層（MAC）的通訊協定。

IEEE 802.11標準使用ISM(Industrial,Scientific and Medical)頻帶(如圖 3)，其優點是使用者不需要事先申請執照，任何人都可以自行架設無線區域網路，所以當IEEE 802.11標準推出之後就獲得市場的廣大支持。

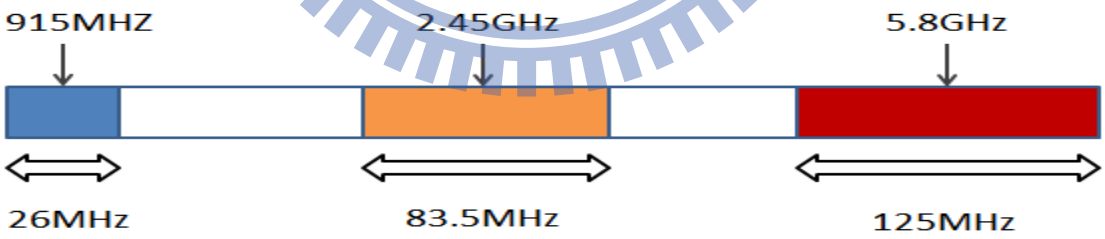


圖 3 ISM 頻帶

為了推動IEEE 802.11還有另一個常見的WLAN認證標準-Wi-Fi[11]，它是一個非營利組織－Wi-Fi聯盟(Wi-Fi Alliance) 所有擁有的商標，該聯盟成立於1999年，主要的工作是負責認證各種WLAN產品是否有遵循IEEE 802.11的標準規範，以避免市面上的產品有不相容的情況。

IEEE 802.11 網路基本架構

IEEE 802.11無線區域網路中定義了兩種基本服務組合(Basic Service Set，BSS)與延展型服務組合(ESS)，其網路架構分別如圖 4所示。

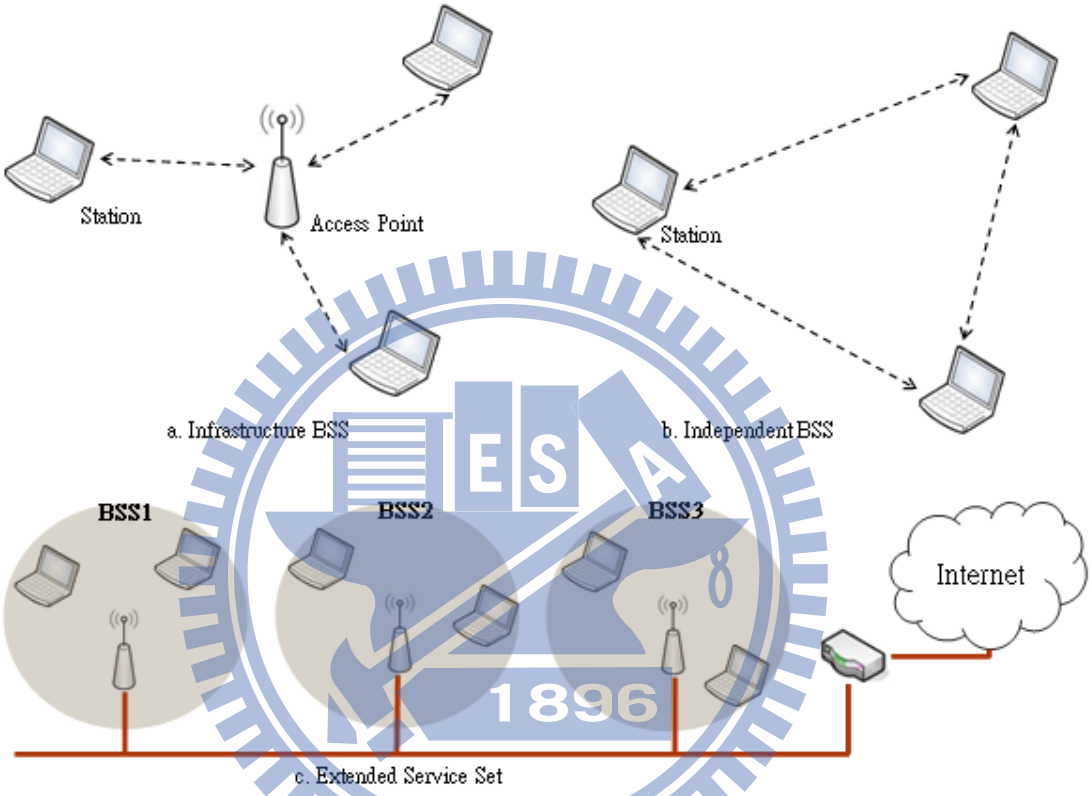


圖 4 IEEE 802.11 網路基本架構

- 基礎結構型基本服務組合(Infrastructure BSS)
  在圖 4.a中AP扮演著最重要的中間角色。網路內的STA(工作站)皆需要與AP建立聯結(Associate)之後，才能享用傳輸的服務；所以當網路中STA-A需要發送封包給STA-B時，STA-A必須先將封包送給AP，再由AP轉送給STA-B。而同一張網路卡在同一時間只能與一個AP建立聯結。

- 獨立型基本服務組合(Independent BSS)
  在圖 4.b中任二個STA只要在通訊距離內都可以直接通訊，不須靠其他工作站作轉送封包。這種獨立型服務組合又被稱之為隨意網路(Ad-Hoc network)。

- 延展型服務組合(Extended Service Set)

  圖 4.c為延展型服務組合(ESS)是由多個BSS互相串聯成為更廣大的無線區域網路，一般在AP之間會透過一個Layer2的主幹網路(backone network)互相聯結，擴展成一個較大的無線網路服務組合。

IEEE 802.11 實體層與媒體存取層

IEEE 802.11 主要目的就是要設計一套適用於無線區域網路環境之下運作的通訊協定,其中最重要的工作是要製定出實體層(PHY)和媒體存取層(MAC)的標準。IEEE 802.11 的參考模型主要分成兩部份，首先是製定出適用於所有無線網路的MAC規格,再來則是要製定出和實體傳輸媒介相關PHY的介面。

- IEEE 802.11實體層通訊協定

  實體層定義有跳頻展頻(FHSS)和直接序列展頻(DSSS)二種通訊協定，後續改版的802.11b規範了高速直接序列展頻(HR/DSSS)技術，在802.11a方面規範使用正交分頻多工(OFDM)技術，而後來的802.11g規格雖然使用OFDM技術但可以向下相容於802.11b標準。

- IEEE 802.11媒體存取層通訊協定

  由於無線電波在傳送的過程中要偵測碰撞(collision)相當不易，因此IEEE 802.11 採用不同於Ethernet的載波偵測多重存取/碰撞避免(CSMA/CD)機制。而是利用CSMA/CA的方法來傳送資料，STA傳送資料前會先偵測頻道中的電磁波能量,若電磁波能量超過基準值,即代表頻道正在被使用中，因此STA必須等待一段時間後，重新偵測頻道後才可以傳輸資料。

  對於無線媒介的存取，IEEE 802.11 MAC層規範了二種協調功能：分散式協調功能(Distributed Coordination Fucntion， DCF)和中樞協調功能(Point Coordination Function， PCF)。DCF為標準的CSMA/CA存取機制，當STA要發送資料時會先檢查頻道是否有被使用，並在延遲一段時間後頻道如果仍是淨空，即可開始發送封包。反之，STA必須隨機等待一個延遲(backoff)時間，之後再重新檢查頻道的可用性。PCF不同於DCF所採用的競爭服務，在運作過程中會有一個中樞協調者(Point Coordinator)來掌控媒

介的存取權利。它會依照輪詢名單來發送CF-POLL訊框來詢問其管轄內的STA有無須要傳送資料。因此STA不能自行傳送資料。

無線網路傳輸方面具有幾項特性，第一兩個端點之間的連線距離是有限的，且訊號的強度與距離的平方成反比，因此不同的訊號強度會影響服務的範圍；第二在開放的空間裡傳送的訊號，容易受外來雜訊干擾而影響連線品質，所以資料傳送的可靠度比有線網路式低一些；第三時常被使用於行動設備之中，為減少電力消耗太快必須要有電源管理功能；第四資料傳輸時容易被攔截和竊取，所以無線網路安全管理需要完整的身分認證及資料加密等措施。

IEEE 802.11 連線機制

無線區域網路具有不需佈線與建置成本低的特性，在網際網路接取上所扮演的角色日漸重要，而無線訊號在這開放的空間之中傳播，要如何避免被有心人士竊聽或擷取的風險，達到傳輸資料的保密性與完整性是一門重要的課題，在說明加密和認證之前，首先介紹IEEE 802.11 無線區域網路的連線機制與運作方式。

掃瞄(scaning)

工作站(station)要與AP建立連線時需要經過三個步驟，依序分別是掃瞄(scaning)、認證(authentication)和聯結(association)，其流程如圖 5。掃瞄動作會因為使用的方法不同可分為二種模式：主動掃瞄(Active scanning)和被動掃瞄(Passive scanning)；其說明分別如下：

- 主動掃瞄

  工作站會依據預先設定好的頻道清單(channel list)向各個頻道發送proble request的封包；而proble request封包也可以選擇是否指定特定的SSID；當不指定SSID時，所有非刻意隱藏的AP收到proble request封包後，都會回應probe response封包；如果probe request封包中有指定特定的SSID，則只有屬於該SSID的AP才會回應probe response封包；工作站在收集這些回應封包後就可以知道四周是否有AP存在。

- 被動掃瞄

  相對於主動掃瞄的方式，工作站使用被動掃瞄的方法是在各個預設的頻道列表中聆聽AP定期發送的beacon訊框，這種方法可以減少電波發送以節省電源，本系統也將採取被動掃瞄的方式來偵測四周環境是否有AP存。

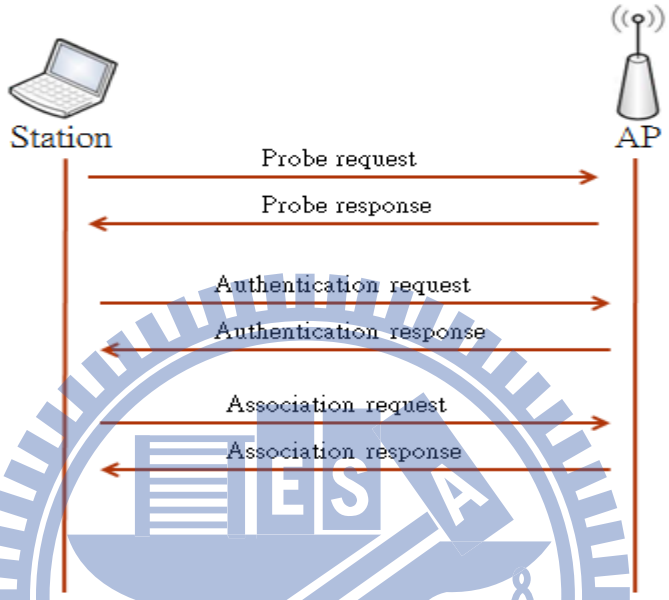


圖 5 無線AP連線流程

認證(authenticate)

傳統上使用有線傳輸時如果想要竊取網路的傳輸資料，必需要連接實際線路或設備才能監聽；而無線電磁波傳輸是在開放的空間，在傳輸資料的過程中很難避免不被第三方所截取。為了防止不合法的工作站存取無線網路資源以及保護資料傳送的安全，當工作站向有安全性設置的AP要求連線之前，必須要取得AP的認證。

聯結(associate)

當認證完成之後，工作站就可以向AP發出關聯要求(association request)的封包，如果AP同意其關聯要求就會回應註冊狀態成功的封包；如果註冊失敗則會回應錯誤狀態碼並且結束此次註冊的動作。完成聯結動作之後，AP就可以開始為工作站提供封包傳輸的服務。

2.2 IEEE 802.11i 無線安全標準介紹

初期無線網路是使用 WEP(Wired Equivalent Privacy)作為加密的標準，這樣的加密方式主要是透過 RC4 配合 64 位元與 128 位元兩種不同長度的 WEP Key 作為加密的密鑰，密鑰中的 24 位元會被用來作為 IV(Initial Vector)值。只有 IV 是變動的，之後剩下的 40 位元或 104 位元的 Key 都是固定不變的。所以要破解 WEP 加密機制，基本上只要截取足夠相同 IV 值的封包，就可以進行 WEP Key 的破解。由於安全性不佳，後續制訂 IEEE 802.11i 標準的目的就是為了彌補原來 WEP 安全性不足的弱點。IEEE 802.11i 主要包含有下面幾個重要單元如圖 6，其中與本研究無線熱點認證相關的重點說明如下。

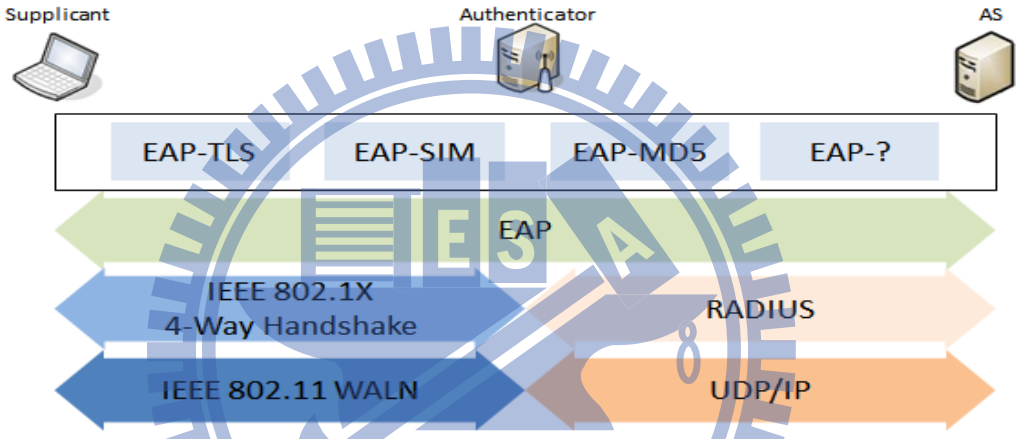


圖 6 IEEE 802.11i 主要單元

- EAP encapsulation over LAN (EAPOL)

可延伸認證協定(Extensible Authentication Protocol，EAP)最早規範於 RFC 2284[12]，設計的目的是為了讓 PPP 協定能夠支援各種認證機制。此標準於 2004 年時被 RFC3748[13]的標準所取代，除了部分定義修正之外，EAP 將可以被使用於有線或無線網路上，不再侷限於 PPP 協定來傳輸。EAP 是一種認證機制的框架，特色在於認證時不用預設使用特定的認證演算法，驗證者(authenticator)與客戶端(supplicant)之間可以相互溝通並協調出彼此都接受的認證機制。

EAP 認證過程中可以把認證封包送往在後端(backend)的認證伺服器做驗證的動作。因此前端的驗證者只需要關心認證結果的成功與否，而不用了解認證機制的細節，使得認證機制更有彈性。EAP 的封包內容定義相當簡潔，封包格式如所示圖 7。其欄位所代表的意義如下表 2。

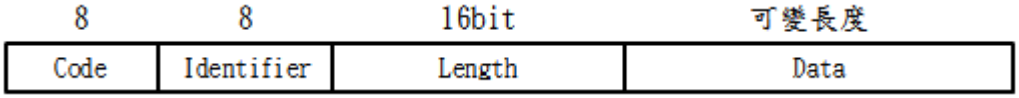


圖 7 EAP 封包格式

表 2 EAP 封包欄位

封包欄位	說明
Code	代表封包的種類： 1 要求(Request)：由驗證者發送要求給被驗證方 2 回應(Response)：客戶端/請求者回應 3 成功(Success)：認證成功 4 失敗(Failure)：認證失敗
Identifier	通常是流水號用來區分成對的要求封包與回應封包
Length	封包長度資訊，計算包括Code、Identifier、Length與Data等欄位。
Data	EAP 資料。長度由零到多個位元組(octets)

EAPOL(Extensible Authentication Protocol over LAN)是為了把EAP封裝於乙太網路封包所發展的版本，它被使用於IEEE 802.1X所定義的有線網路或無線網路的認證環境之中，其認證框架仍源自於EAP的規範，主要差別在於EAP封包被封裝在不同的資料連結層上做傳輸，階層關係及封裝方式如圖 8，封包格式與欄位說明如下圖 9和表 3所示。

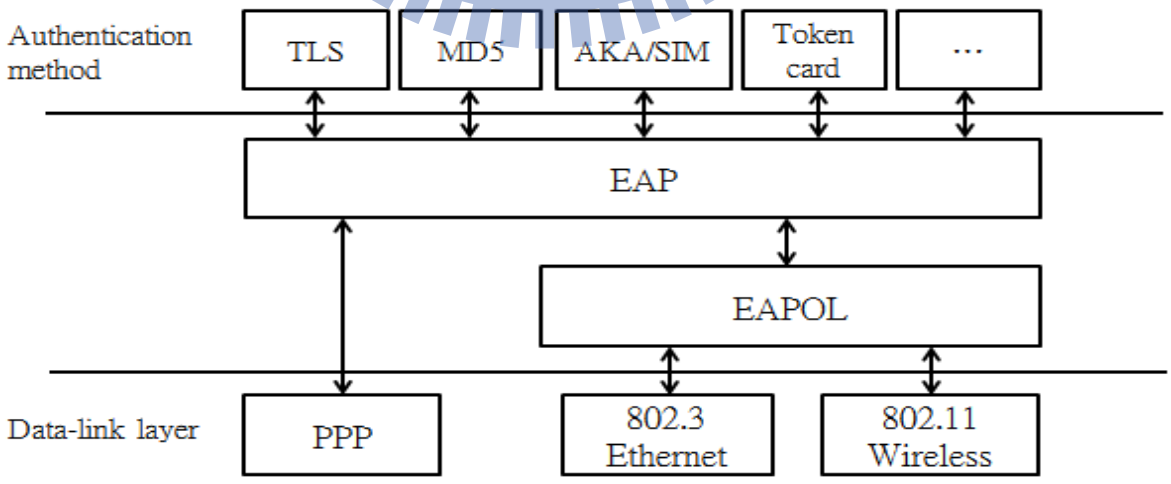


圖 8 EAPOL示意圖

6	6	2	1	1	2	可變長度
Destination address	Source address	Ethernet Type	Version	Packet Type	Packet Body Length	Packet Body

圖 9 EAPOL封裝格式

表 3 EAPOL 封包欄位

封 包 欄 位	說 明
MAC Header	Ethernet的目的和來源位置
Ethernet Type	Ethernet封包類型，EAPOL為0x888E
Version	EAPOL的版本號，目前為第一版設為1
Packet Type	EAPOL訊息種類
Body Length	EAPOL資料長度
Packet Body	EAPOL資料

- IEEE 802.1X 與RADIUS

隨著有線和無線寬頻網路的建設規模快速擴大，為了因應大規模數量急劇增加的使用者和多樣性寬頻業務的要求，數據網路通訊(Datacomm)急需如電信通訊(Telecom)所定義完整的AAA認證系統。IEEE 802.1X 具有用戶認證和管理能力，能適用於商業網路的服務的計費、認證、運營等要求。是一種基於連接埠的網路存取控制的認證機制(PNAC-Port-based Network Access Control)。

所謂的連接埠並不一定是實體的交換器的網路孔，它可以延伸解釋如無線網路中AP與STA之間的點對點的連線。所以IEEE 802.1X可適用於有線或無線的網路環境。其主要認證機制在於用戶還未通過驗證之前，是無法透過連接埠存取網路上資源。此認證機制定義了三種角色：

- Supplicant：要求加入網路的一方。
- Authenticator：擁有網路資源存取的控制權。
- Authentication Server：負責用戶資料的驗證工作。

RADIUS(Remote Authentication Dial In User Service)是一種Client/Server架構的AAA網路認證協定。圖10為IEEE 802.1X與RADIUS的運作方式。

IEEE 802.1X 連線認證步驟：

1.使用者發起連線到Authenticator要求連線

2.Authenticator要求使用者帳號及密碼

3.使用者回應帳號和密碼

4.Authenticator把使用者資訊送到RADIUS認證伺服器

5.RADIUS回應認證結果-Accept、Reject or Challenge

6.Authenticator回應使用者認證的結果；認證成功後即可開通網路服務。

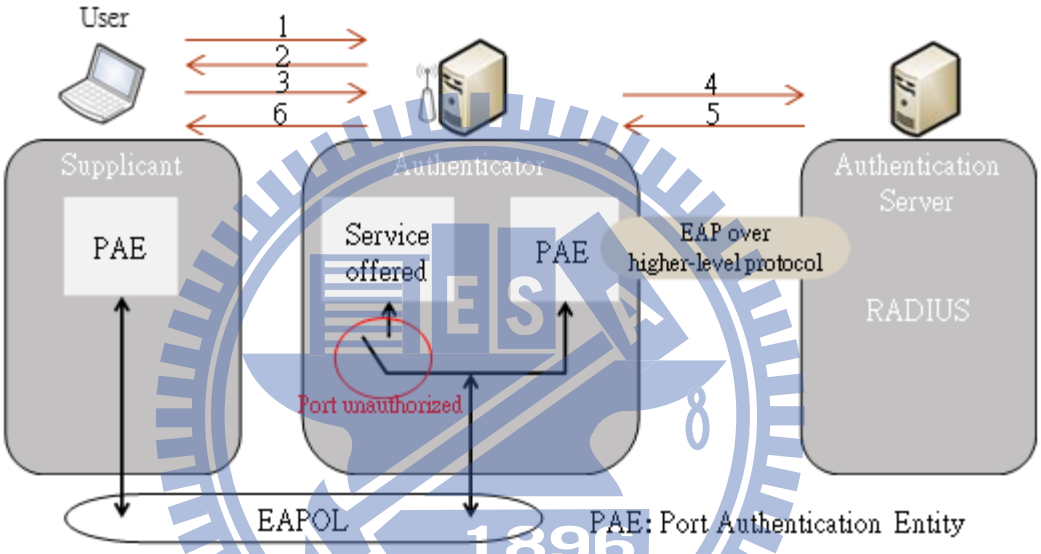


圖 10 IEEE 802.1X 的運作方式

2.3 WISPr - Wireless Internet Service Provider roaming

隨著無線區域網路的盛行，越來越多公共場所和商店開始建置無線熱點服務，提供一般民眾或消費者可以在公共空間存取網際網路。網路公司為了保障無線區域網路的安全和營運也紛紛提供了相對應認證與收費措施。無線熱點的安全性認證方法，目前普遍使用的機制是所謂Web-based的UAM (Universal Access Method)方法。當行動裝置連上無線熱點並取得網路位址之後，用戶必須再透過瀏覽器輸入帳號和密碼的認證程序才能開通與網際網路的連線。

雖然使用瀏覽器認證機制比較容易建置和實作，但此認證機制有三個主要的缺點：第一手持式行動設備通常螢幕較小且不方便輸入太多文字，尤其是密

碼的輸入往往令使用者備感不適；第二個缺點是各家網路公司所設計的認證網頁 表單沒有統一格式，每當使用者到一個新的熱點區域時，就必須要重新輸入認證資料，沒辦法實踐標準的自動化認證與漫遊的機制。第三個缺點是部分手持式裝置由於內建的瀏覽器相容性不佳而無法通過網頁驗證。

為此無線寬頻聯盟(Wireless Broadband Alliance，WBA)和無線聯盟(Wi-Fi Alliance)合作致力於改善跨營運商的無線熱點漫遊業務，為了把熱點認證機制標準化開始著手制訂了WISPr規範。WISPr標準使用二種既有的技術－HTTP/HTTPS和XML，提供一個共通的認證機制，使客戶端的行動裝置可以透過WIPSr的認證機制能夠漫遊存取各家網路公司的無線熱點網路。相對於IEEE 802.1X認證機制，WISPr是屬於第三層以上的認證協定。認證時所定義的角色與IEEE802.1X相當類似，其定義如下圖 11：

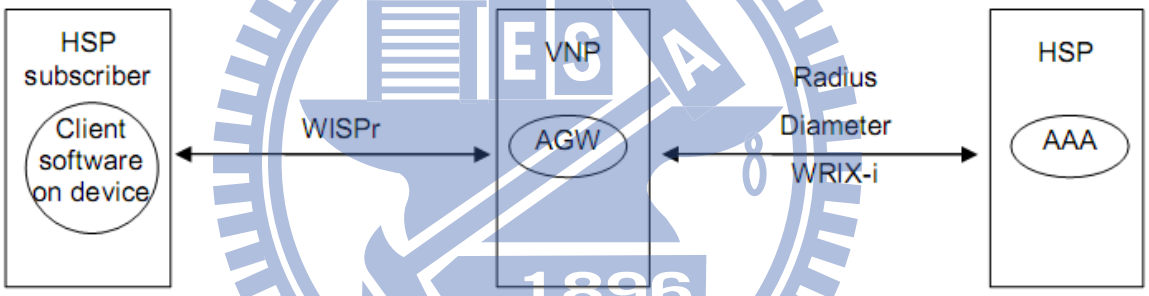


圖 11 WISPr與AAA認證協定、公眾WLAN漫遊的關係

資料來源：WISPr 2.0 specification

HSP：Home Server Provider

VNP：Visited NetworkProvider

AGW：Access Gateway

WRIX：Wireless Roaming Intermediary eXchange

WISPr使用XML格式定義了認證時所需要的標籤，然後透過HTTP/HTTPS的GET和POST方法傳送經由XML包裝好的認證參數，達到認證資訊交換的目的。下面舉例說明WISPr其中一種認證登入與登出的基本流程。

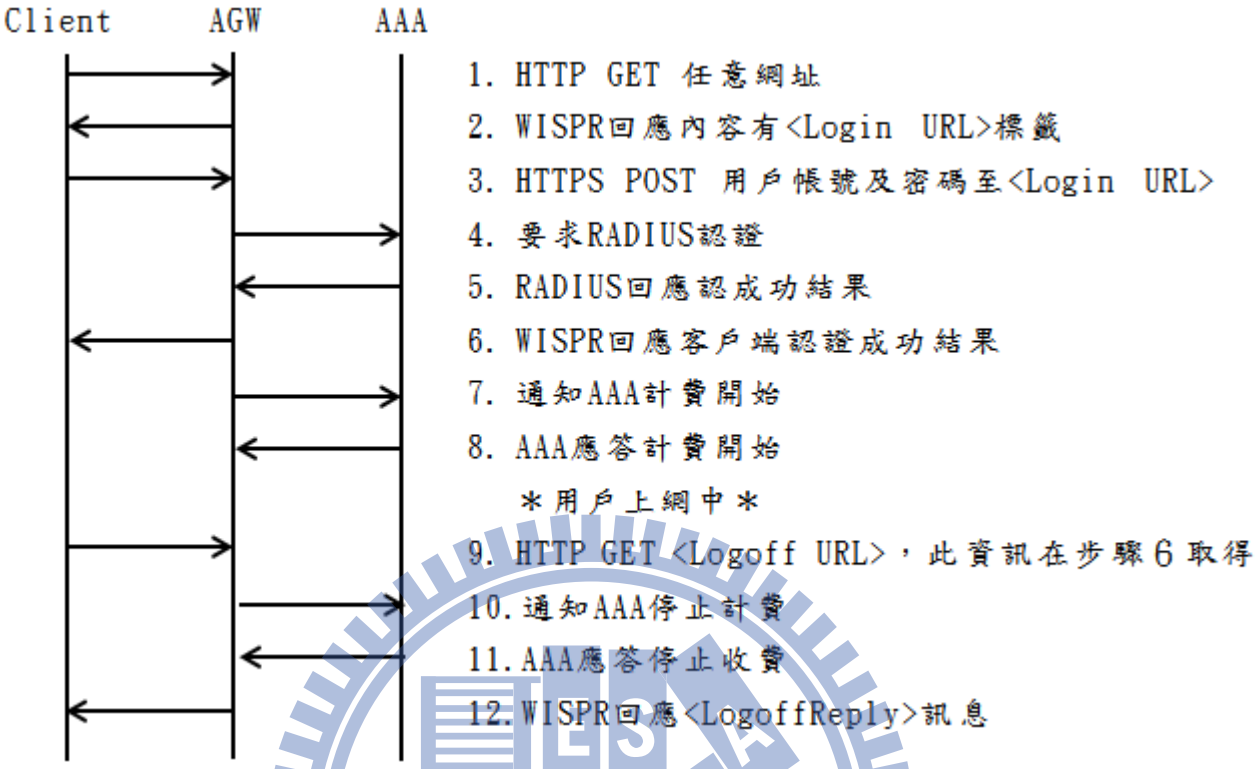


圖 12 WISPr 認證登入與登出的流程

2.4 行動網路簡介

所謂行動網路指長距離使用無線技術的行動通訊技術，可以讓行動裝置可以在固定位置的基地台之間移動，並在訊號可及的範圍內使用網路資源。基地台傳輸電波的強度會隨著距離增加而衰減，所以每個基地台服務的範圍是有限的。在每個服務區域的中心設置基地台，這樣可提延伸訊號的涵蓋範圍，使得任何地方都可以得到基地台的服務。這些小區域的分佈形狀近似六角形與蜂巢相似，所以行動網路又被稱為蜂巢式行動通訊系統(cellular networks，如圖 13)。

早期從第一代類比式行動通訊系統(AMPS)單純只能提供話務功能，行動網路真的開始發展於第二代行動通訊技術。第二代行動通訊系統稱為 GSM (Global System for Mobile Communication)，是目前應用最為廣泛的行動通訊標準，與前一代最大的不同是採用數位式技術，因此通話品質較第一代系統為佳，頻譜利用率相對提高，同時也改善了保密性等問題。

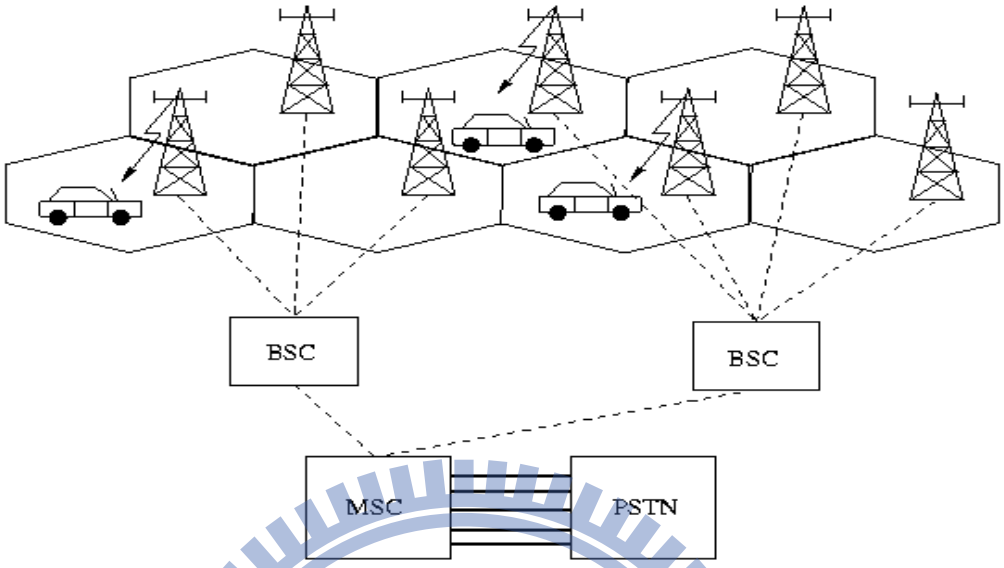


圖 13 蜂巢式行動通訊系統

資料來源：LO Walters and PS Kritzinger, "Cellular Networks Past, Present and Future"

但是由於多媒體服務與網際網路的快速發展，2G 行動通訊系統已經無法滿足高速數據傳輸上的需求以及對於多媒體行動通訊的應用，因此 ITU 為了滿足高速傳輸的需求提出了第三代行動通訊技術－CDMA(Code Division Multiple Access)，全球目前有三大主流標準有歐洲、日本為主的 W-CDMA、美國主導的 CDMA2000 以及中國的特有的 TD-SCDMA 等。三種主流標準的比較表如下。

表 4 全球第三代行動通訊標準

技術標準	W-CDMA	CDMA2000	TD-SCDMA
理論速率	下行：14.4Mbps 上行：5.76Mbps	下行：3.1Mbps 上行：1.8Mbps	下行：2.8Mbps 上行:0.56~2.24Mbps
核心網路	基於 GSM-MAP	基於 ANSI-41	基於 GSM-MAP
雙工模式	FDD	FDD	TDD
技術演進	GSM → GPRS → EDGE → WCDMA → HSDPA/HSUPA → HSPA+ →LTE FDD	CDMA → CDMA1X → CDMA2000 EV-DO Rev.0 → Rev.A → LTE FDD	TD-SCDMA → TD-HSDPA/TD-HSUPA → TD-HSPA+ → LTE TDD

W-CDMA 是 GSM 通訊技術的升級，同時也是全球 3G 通訊技術中用戶最多(原因是 GSM 系統在全球擁有高達 85%的用戶)，技術和商業應用最成熟的。W-CDMA 技術將遵循 W-CDMA、HSPA、LTE 演進路線。其中 HSPA 還有一個 HSPA+技術的演進版本，其速率高達 21Mbps 也已經開始在澳大利亞、新加坡、台灣等地開始佈署提供更高速度的行動網路服務。

EV-DO 是 CDMA2000 通訊技術的升級版本，相對於 GSM/W-CDMA，使用 CDMA/EV-DO 技術的電信服務商少很多，設備廠家和終端廠商也較少，主要的服務地區在北美，產業供應鏈基本上是由美國高通(Qualcomm)公司所主導。

TD-SCDMA 是中國自主的 3G 標準，2000 年 5 月，ITU(國際電信聯盟)公佈 TD-SCDMA 正式成為 ITU 第三代行動通信標準，與歐洲 WCDMA、美國 CDMA2000 並列為全球三大主流 3G 國際標準，並於 2008 年 4 月 1 日開始試營運。TD-SCDMA 最大特色在於有限頻譜的情況下，透過智慧天線提高頻譜利用率，使用智慧天線多通道技術可以使兩個用戶在不同的空間享同一個碼資源。

全球 CDMA 通訊設備的投資開始急速萎縮，因為 CDMA 通信技術的演進基本上電信業者已經達成共識，除了一部分的行動網路系統建設轉換至 HSPA+技術之外，絕大部分的 CDMA 電信運營商最終還是會升級至以 LTE 技術為主的通信技術，以提供速度更快的行動數據服務。LTE-A(LTE-Advanced)為 3GPP 的第十版標準，理論上可以提供 1Gbps/500 Mbps 的下上載速率。這個規格剛好符合 IMT-Advanced 所規範 4G 網路要求的 1Gbps 下載速率。LTE-A 架構有 Carrier aggregation、MIMO、全 IP 網路等特色，頻譜使用上更有彈性，在相同的資料傳輸速率之下也改善了 SINR 值；使用 Carrier aggregation 可以讓一些零散的頻寬聚合再一起，有如擁有一段較大的頻寬，使得頻譜能夠有效地被利用；MIMO 則是利用多根天線傳送技術來增加訊號傳送品質，加上 Beamforming 技術也可以減少與其它用戶之間的干擾。以目前 LTE 的發展現況來說，它將會是未來 4G 行動網路的標準。

三、相關研究

本章節在探討實現本系統所參考的相關技術與研究，相關文獻依系統功能模組的需求共分為三個小節，第一節介紹多網(Multihoming)系統的網路管理之研究，探討如何管理異質網路以達到網路備援及負載平衡的功能，進而把研究中的概念運用到本系統之中，提供異質網管理功能與加速發動換手的決策動作；第二小節將介紹無線網路認證相關的研究，了解網路認證環境的建構可分區為集中式管理以及分散式管理二種模式，研究內容將有助於本系統研究熱點認證方面的工作。第三節相關研究的部分將介紹如何利用開放 Linux 嵌入式系統建構出具有路由功能的家庭閘道器，進而把研究中的軟體架構知識運用到本研究之中。

3.1 多網(Multihoming)系統網路管理之研究

多網(Multihoming)系統是指單一個主機(host)擁有二個以上的線路可以連接到網際網路上的一種網路架構(圖 14)。它的目的主要是依不同的目的而有不同的應用方式。依功能需求可分為下面幾類：負載備援(Redundancy)、負載平衡(Load balance)、頻寬整合(Bandwidth boding)、使用者導向(User define) [3]等。

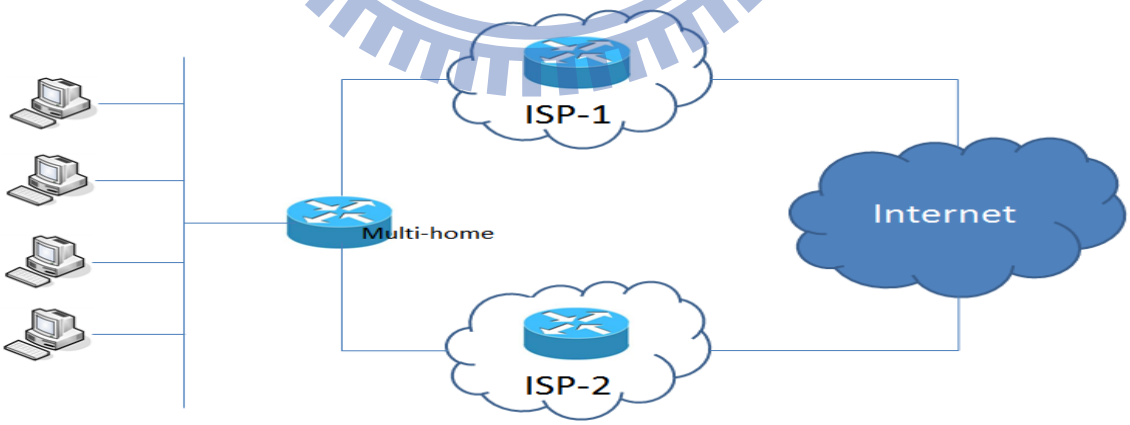


圖 14 多網(Multi-homing)系統網路架構

在 Multihoming 的系統中都會定義不同的傳輸管理規則，並針對不同的網路介面的特性，制訂不同的運作模式。在[1]研究中使用了三種傳輸管理政

策，分別是(i)Round Robin，根據網路介面的數量，依序選擇每個網路介面來傳輸，來達到循環輪迴傳送的功能；(ii)Least Load First Transmission，在選擇路由介面時，是以封包已傳送的量作為考量。在做資料傳輸時將選擇當下傳輸累積量較少介面來做為傳送介面；(iii)Fast Speed First Trans-mission，在選擇傳送介面時以傳送速度作為考量，依據當下 RTT(Round Trip time)最小的介面當作下一個傳輸線路。

在負載備援方面[1]的方法是運用 ICMPv6 協定，在對應的網路介面發送 Router Solicitation 封包到上游路由器，當上鏈路由器接收後會回應相對的封包。當上鏈路由器沒有回應時，就代表此網路已經不能使用，必需選擇另外一個傳輸介面。作者藉由這樣機制用來偵測網路連線的狀態。

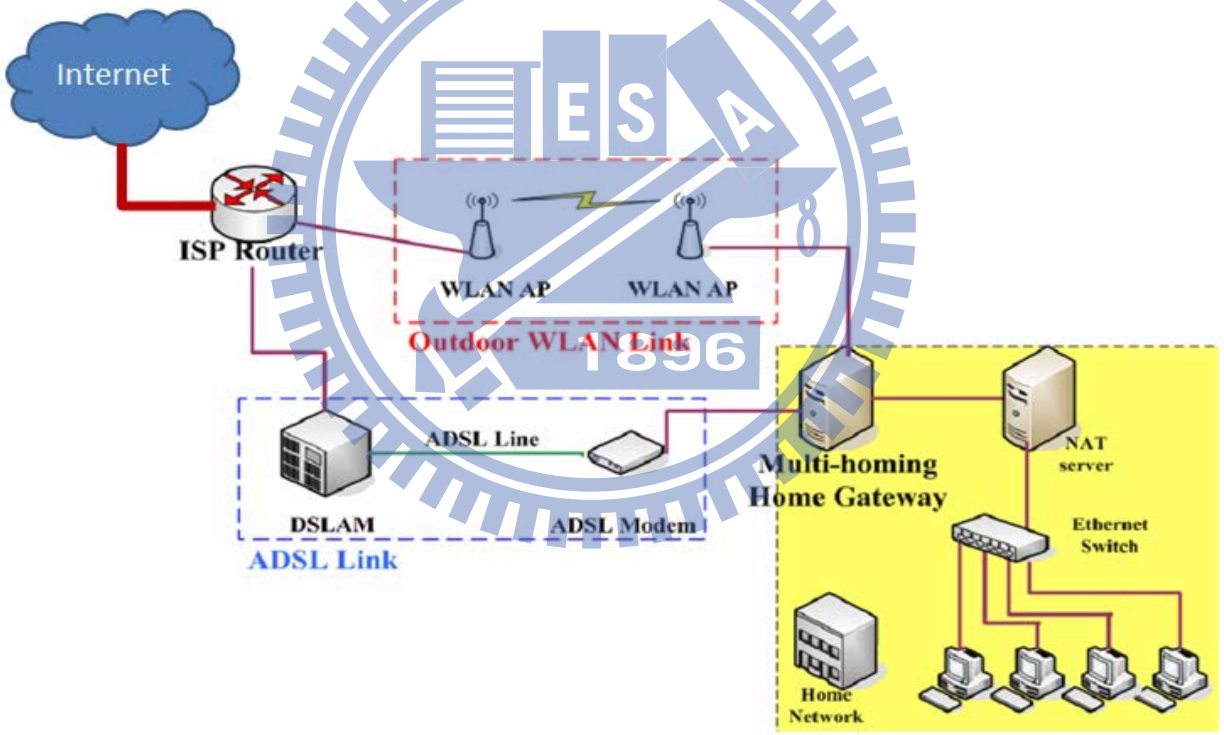


圖 15 多網家庭閘道器系統架構
資料來源：[2]多網家庭閘道器之設計與實作

異質網路除了有線固接的網路之外，無線網路也是相當成熟的網路技術。在[2]的研究中提出如何利用無線 IEEE 802.11 和有線 ADSL 二種異質網路，設計了一套名為 LoBRA(Load Balancing Routing Algorithm)的系統，其系統架構如圖 15，實作異質網路負載平衡與頻寬整合的應用。由於 IEEE 802.11

的分散式協調功能(Distributed Coordination Function, DCF)是使用CSMA/CA的協定來決定主機(station)如何傳送無線訊框(frame)。因此，在DCF模式下因為CSMA/CA通訊協定的機制，無線網路節點會互相競爭傳送訊框的機會。在這種情況之下，處在不同位置的主機在傳送資料時，會使得較遠的主機發生傳送飢餓(starvation)的現象。每個主機實際能使用的頻寬量就會不同，使得頻寬無法保證公平被分配。而ADSL具有上行頻寬較小和下行頻寬較大的不對稱性。因此，在此研究中根據不同的網路特性來設計路由演算法來整合這二種異質網路。

為了解決不同網路介面的路由問題，利用了IP通道(IP-in-IP tunnel)和IP alias的概念(如圖 16)，讓資料可以分流至不同的網路介面。使用這種方法一方面可以維持來源端IP／PORT與目的端IP／PORT的End-to-End連線，達到無縫的換手而不影響原來的連線傳輸；另一方面就是封裝過後的封包經過IP通道解封裝之後，可以通過ISP路由器上防火牆的外出(egress)或進入(ingress)過濾規則的檢查，以避免封包被丟棄可能。

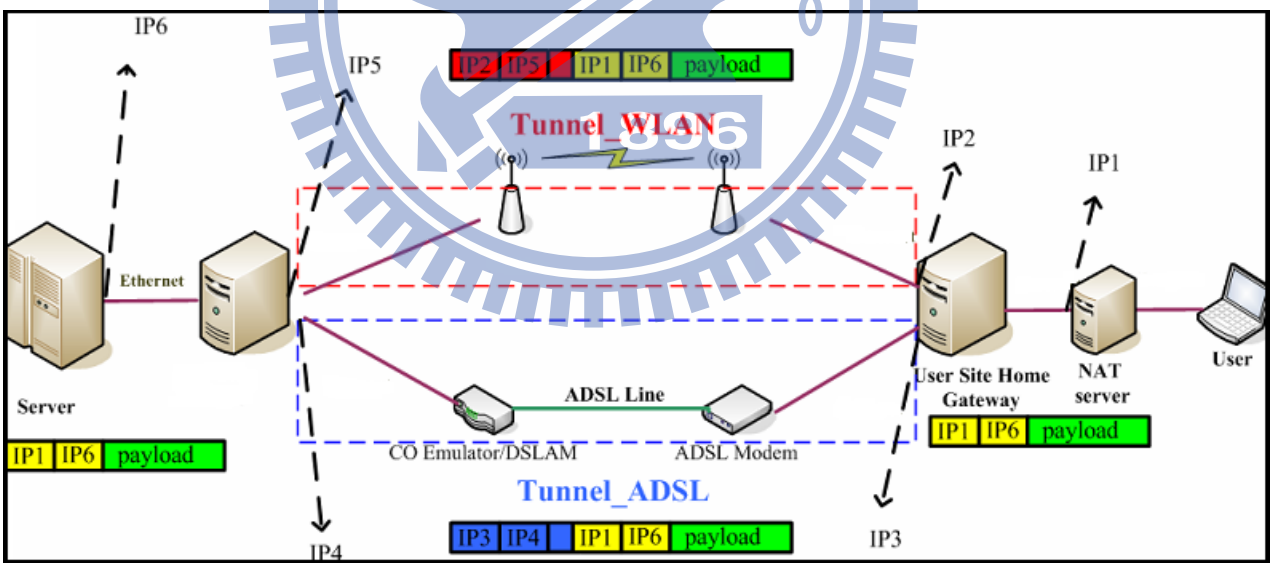


圖 16 多網家庭閘道器 IP tunneling
資料來源：[2]多網家庭閘道器之設計與實作

由於同時支援多種網路介面的行動設備越來越普遍，為了管理多種異質網路介面，必須要設計一套有效的管理系統，在2011年，研究[4]在Linux系統上提出了多網路介面管理系統與事件通知機制(MIME)。目的是希望能設計一套介

面事件主動通知的機制，讓網路介面管理系統可以快速反應各種網路狀態，例如，偵測網路卡的新增、移除、連線與斷線等。如此一來在網路斷線或移除時，可以加速轉換到另一個網路介面上，減少使用者連上網際網路的等待時間。在此論文的研究成果中網路管理的效率確實比原來的內建在Linux系中的網路管理程式要來的好。MIME統架構分別是由MIME-IM、MIME-PM、MIME-NM等三個主要模組所組成，如圖 17所示。

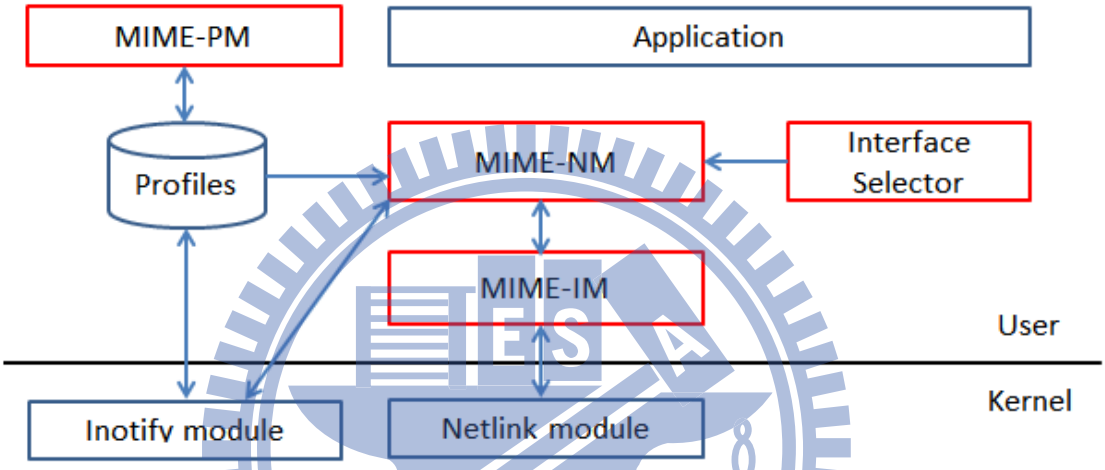


圖 17 MIME Architecture

資料來源：[4]多網路介面之網路管理系統與事件通知機制的設計與實作

- MIME-IM (Interface Manager)

  利用Linux Kernel中的netlink機制，提供一個標準的中介層(middle-wave)。當網路介面發生改變時，可以讓網路管理應用程式可以快速收到通知，增進網路管理效率。其中包含網路介面的Plug In、Plug Out、Link Up與Link Down等狀態改變的事件通知。

- MIME-PM (Profile Manager)

  主要的工作是提供MIME系統的設定介面，讓使用者可以針對不同的網路介面設定多個Profiles，使其能夠支援不同網路之問的錯誤後轉移(failover)及錯誤後回復(failback)等功能。另外使用者也可以透過這個模組檢視目前網路連線的狀況。

- MIME-NM (Network Manager)

  主要是用來管理所有的網路介面，這部分會與MIME-IM和MIME-PM這二個模組互相協同運作。當網路介面發生變化時，會做出相對應的動作，快速載入設定檔並重新更新網路連線。

3.2 無線網路認證之研究

無線區網路的佈設將越來越普遍，電信公司在各飲食餐廳、大賣場、便利商店等都有提供付費的無線熱點上網服務。現在政府單位，如台北市政府在民國一百年六月八日推出了「Taipei Free -台北公眾費無線上網服務」，無線AP高達4000個，佈署區域包含了公共場所部分有市府市政大樓、12個區行政中心、市立圖書館及各分館、市立聯合醫院各院區、臺北捷運車站及捷運地下街等場所；室外公共場所部分，則包括市區主要幹道、主要住商區域及人口密集區之公共場所。另外，行政院研考會也在同年推出「iTaiwan」免費的無線上網服務，其佈建的服務範圍是以全國公家機關的室內為主，例如各地鄉市鎮公所、圖書館、郵局、台鐵車站等。

由此可知無線熱點上網服務是未來的趨勢，因為它具有佈建方便、簡單易用、設備便宜等特性，用來卸載(offload)3G基地台的負載是最合適的方法之一。但IEEE 802.11無線區域網路不像GSM/UMTS系統有定義明確的認證系統，因此本章節將要介紹無線區域網路認證的相關研究以及其認證架構。對於規模較大的無線熱點的建置，不論要收於費用與否，必定要設計一套良好的AAA (Authentication, Authorization and Accounting)管理機制，否則一旦發生資訊安全問題時，將難以維護網路資源和保護使用者的資料。

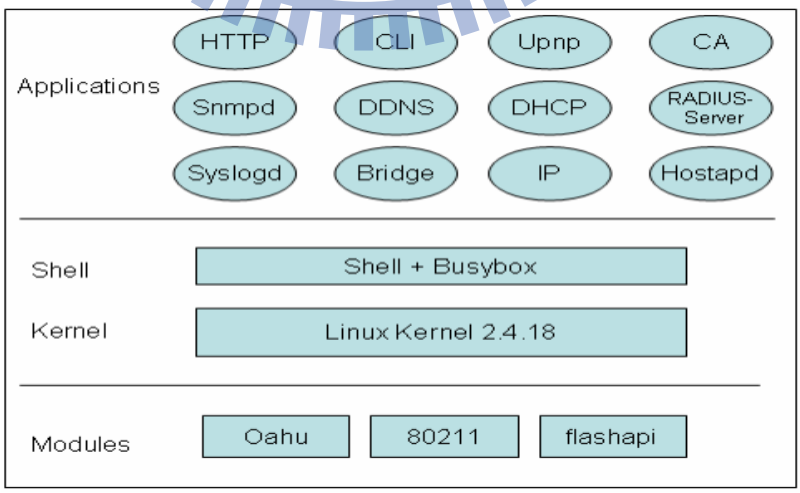


圖 18 整合憑證認證之無線網路路由器的軟體架構

資料來源：[6] 設計與實作以憑證為認證基礎的無線網路路由器

在研究[6]中實作出以憑證為基礎的路由器，主要的特色是把認證伺服器(Authetication Server)與憑證認證(CA，Certificate Authority)的功能整合到無線網路路由器之中，其系統架構如圖 18所示。可以由軟體架構知道在應用程式區塊中整合了三個主要認證模組CA、RADIUS-Server和HTTP-Server。作者對IEEE 802.1x的EAP-TLS系統架構上做了改進，以避免因為網路斷線造成的錯誤，提高系統的可信賴度，而且在使用與維護的複雜度也減少了許多。

為了解決各家業者無線熱點認證與授權的問題，在[8]Mauro Brunato等人發展一套取名為WilmaGate的系統，它是一個基於Open Access Network所發展的無線區域網路熱點管理系統。作者希望能夠解決在各種不相容的認證標準之下，能提供單一入口而多樣性的無線熱點AAA認證服務。圖 19是WilmaGate在網路拓樸所扮演的角色，可以知道當MN(mobile node)需要認證的時候，此系統將可以經由Internet存取各家ISP所提供的各種認證服務。

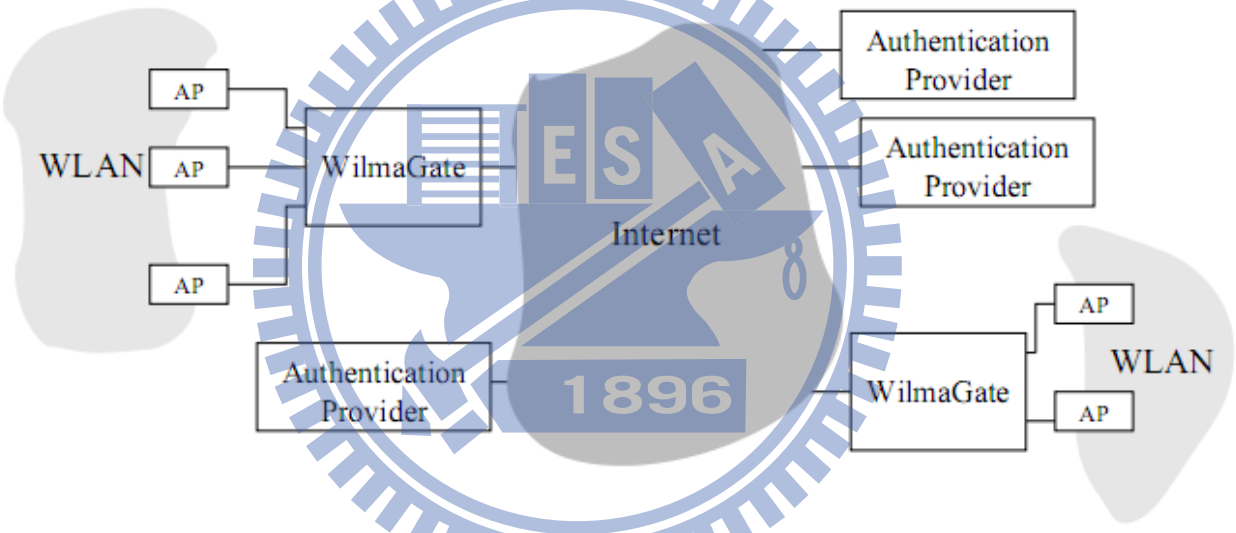


圖 19 Overview of WilmaGate
資料來源：[8] WilmaGate

在系統區塊圖(圖 20)中的佈局可以知道系統分成二個主要部分：

- Gateway 模組
  此模組的功能是管理包含至少二個以上的網路介面(LAN和WAN)，並根據IP和MAC的授權記錄表，監控網路封包並且會把未經過授權的使用者封包加以攔阻。而未經授權的使用者封包將會被送往Gatekeep作進一步的處理。

- Gatekeep 模組
  此模組負責維護用戶端的認證狀態，管理DHCP和IP與MAC認證授權清單。當用戶端透過Captive Portal驗證之後，它便會下命令通知Gateway模

組此用戶的IP與MAC已授權的狀態，之後此用戶便能使用網際網路資源。

WilmaGate還有一個特色就是它可以經由不同的設定改變其系統的拓樸結構，這個特色讓它可以很彈性地融入現有的網路架構之中，提供授權和認證的服務。下面將來介紹該究研中的三種網路設置：

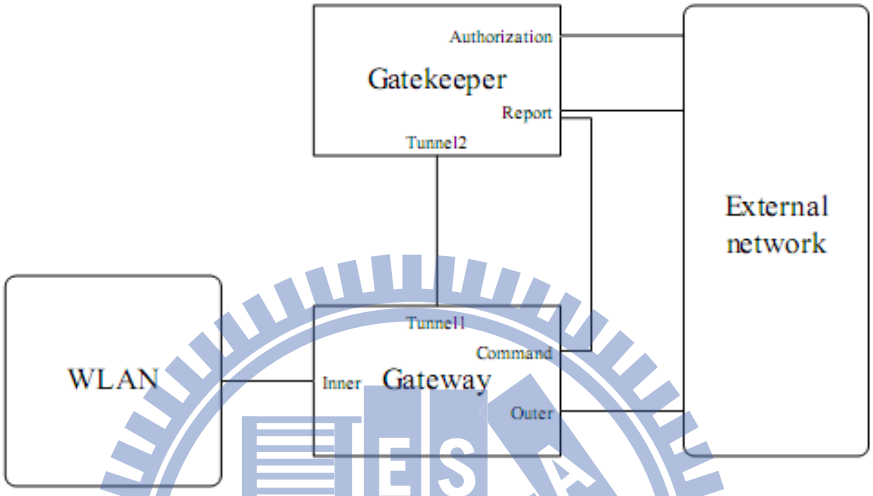


圖 20 Block diagram of WilmaGate system
資料來源：[8] WilmaGate

- All in one
Gateway和Gatekeep模組設置在同一台主機，這種設置適合小型的熱點服務或SOHO使用，其架設方式如圖 21。

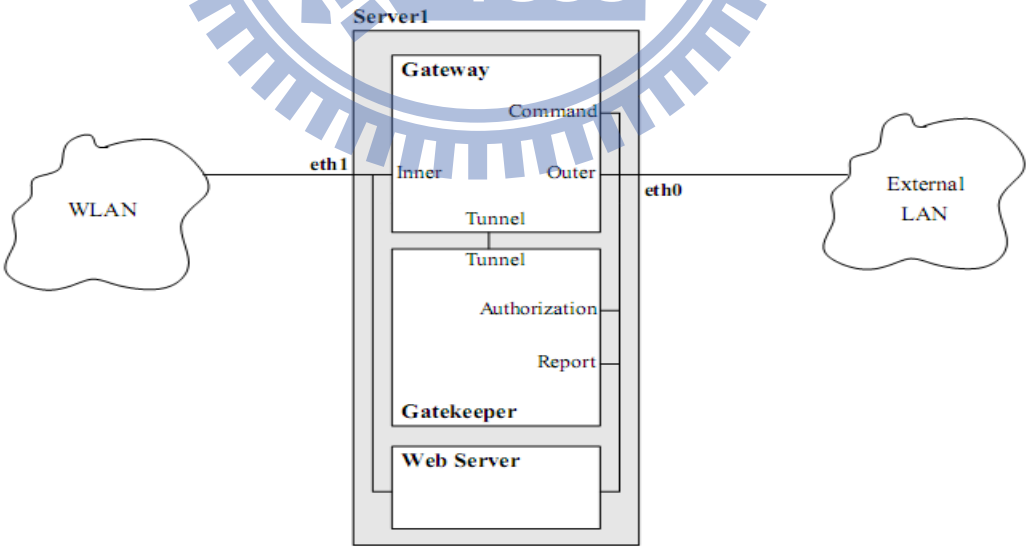


圖 21 All in one 的設置方式
資料來源：[8] WilmaGate

- Tandem
  Gateway和Gatekeep分別設置在不同的主機，二個模組可以獨立存取外部網路。此架設方式適合用於提供高網路流量需求的時候，其架設方式如圖22。

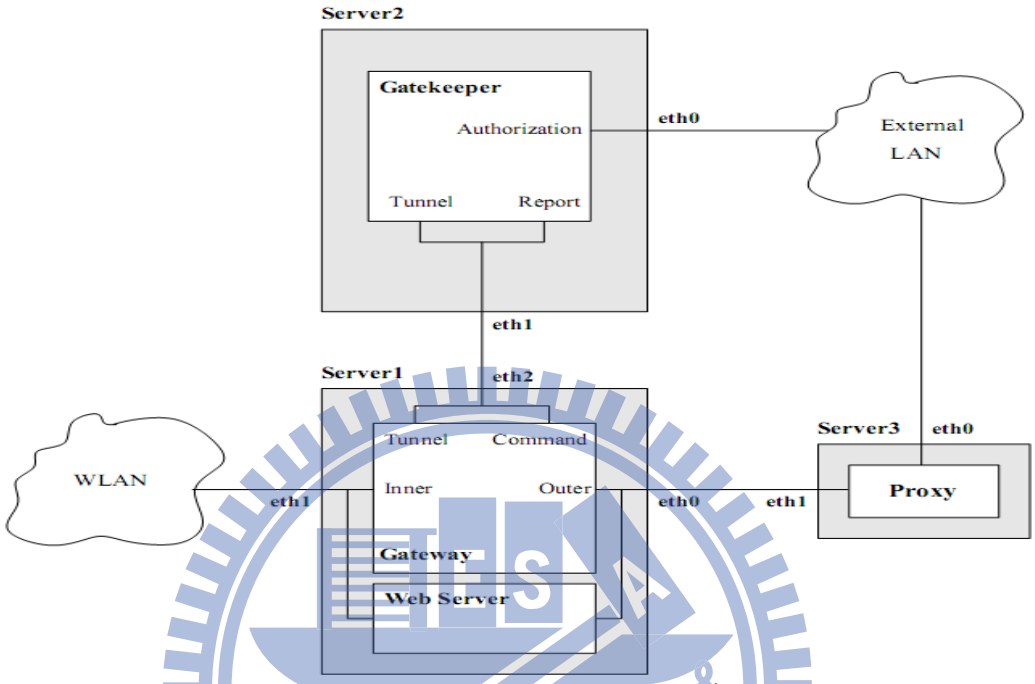


圖 22 Tandem 的設置方式
資料來源：[8] WilmaGate

- Front-end
  Gateway和Gatekeep模組也分別設置在不同的主機，但Gateway與Gatekeep串接之後，只有Gatekeep才可以存取外部網路，適合用於用戶只有一個對外IP的時候，其架設方式如圖 23。

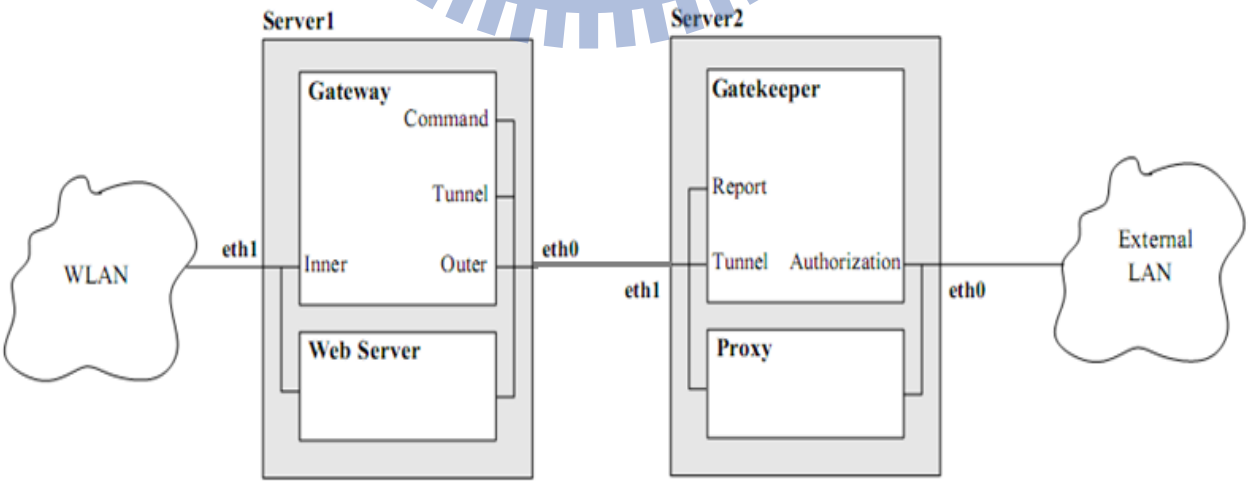


圖 23 Front-end 設置方式
資料來源：[8] WilmaGate

3.3 家用閘道器設計之研究

家用閘道器(Home Gateway)又稱為IP分享器，目的是為能讓使用者透過置設在家裡的閘道器，使得家中的網路裝置能夠相互溝通和分享網際網路的資源。家用閘道器針對內部網路和外部網路分別提供不同的網路協定，基本上具有網路路由和橋接的功能，加上最重要的能力是網路位址轉換功能；對內提供私有網路位址自成一個區域網路(LAN)；對外則是扮演私有網路位址轉換成公有網路位址的功能。家用閘道器[20]其所扮演的角色與使用情境如圖 24。

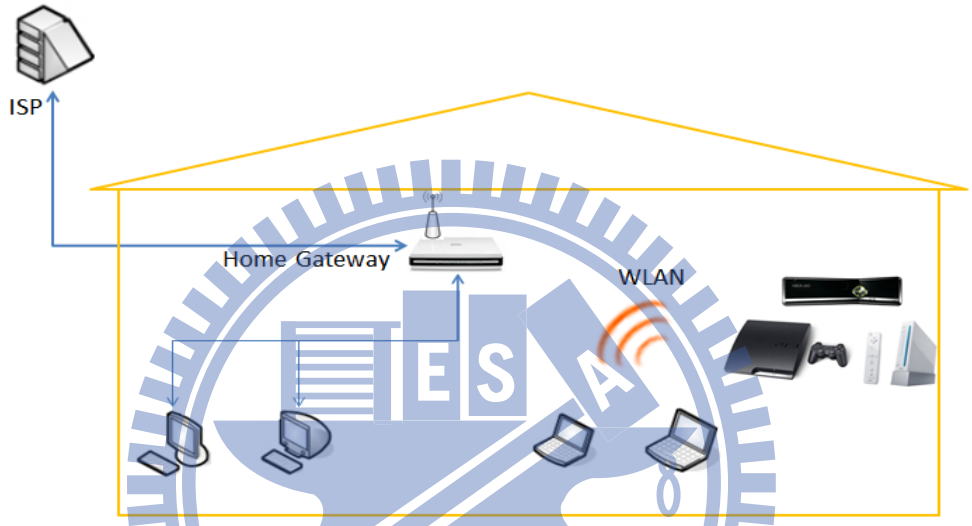


圖 24 家庭閘道器使用情境

一般家用閘道器的設計與硬體組成元件如圖 25，[16]包括中央處理單元負責執行網路協定、封包的轉送與應用程式。快閃記憶體負責儲存執行所需要軟/韌體以及系統設定等，以嵌入式Linux作業系統為例，它可以存放如Boot-loader、Linux kernel和root filesystem等資料。而數位訊號處理器(DSP)為選擇性配備，專門負責處理特定的功能，例如xDSL數據機前端的類比/數位調變和解調變功能、VoIP聲音的編碼處理等。硬體加速引擎也是選擇性配備，主要為了加速運算處理能力，例如資料加密與解密功能、影像和聲音的編碼、NAT(Network Address Translation)加速功能等。周邊的輸出與輸入負責提供各種匯流排(BUS)介面，例如MII為802.3 MAC層與實體層的介面、某些平台應因不同需求與應用也會提供例如PCI、SDIO和USB等介面。

家用閘道器為了提供與外部網路介接的能力，會依據網路環境提供各種介接方式，例如，乙太網路、無線區域網路、xDSL(泛指各種Digital Subscriber Loop的技術)、電力線通信(Power line communication, PLC)[15]與以有線電視(CATV)電纜為介質的傳輸技術。

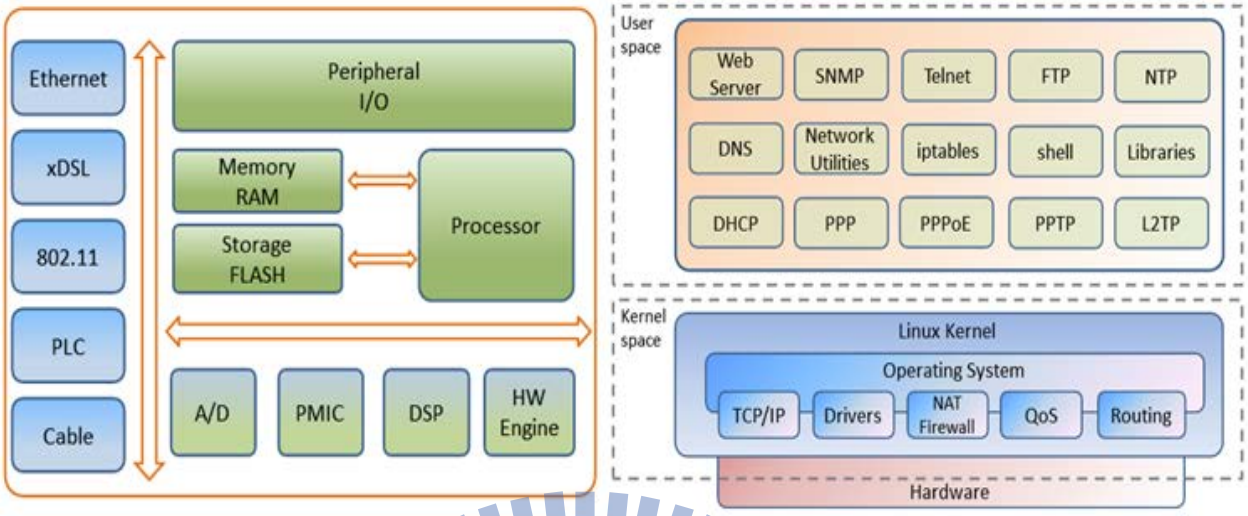


圖 25 家用閘道器的硬體和軟體

在軟體組成方面，由於SoC的發展與進步，從早期封閉的網路作業系統架構，迄今，使用最廣泛的系統是以Linux為基礎的嵌入式Linux系統，藉著開放原始碼的力量，使得網路通訊廠商可以很快速地提供各種不同應用的家用閘道器。Linux作業系統可以提供記憶體管理與配置、行程的管理、系統資源分配、控制輸入與輸出裝置、網路功能與檔案系統管理、硬體裝置的驅動程式等多樣性的功能。在[15][16][17][18]的研究報告中即以Linux作業系統為基礎的家用閘道器，其共同基本的軟硬體架構如圖 25，以下就幾個重要的軟體功能區塊來說明。

網頁伺服器(Web Server)作為家用閘道器的圖形化使用者管理介面；SNMP、Telnet等可以提供遠端網路管理與系統除錯能力；對於沒有內建電池和RTC (real time clock)的嵌入式系統，則可以利用NTP協定透過網路來同步時間；封包過濾與防火牆功能可藉由iptables及kernel裡的Netfilter來實現；還有幾個常見的網路協定，如DHCP、PPP、PPTP與L2TP等協則是用來登入ISP的網路並取得上網所需的IP位址。

在寬頻網路的發展與普及之下，家用閘道器儼然成為每個家庭必備的網路設備，為了提升家用閘道器的功能，把各種不同的新技術整合在一起，提供多樣性的服務與應用變成一種趨勢。例如在[15]研究中整合了家庭用電設備控制及用電情形監視等功能，並驗證了智慧型插座的概念；在[18]研究則整合了P2P以及UPnP AV等網路功能，讓家用閘道器成為家裡的多媒體中心，達成影音分享的目的。

四、智慧型行動熱點系統(IPHS)

目前市面上所銷售的行動寬頻設備中，大都以 3G 網路卡或行動網路搭配 AP 的方式，讓消費者的行動設備可以使用 3G 行動網路，但對於無外接其它週邊能力的行動設備而言並無法使用這一類的網路卡擴充的便利性；雖然行動 AP 可以解決這個問題，但是它缺乏多種網路接取的能力，在無線熱點方面也沒有整合其應用方式。在此章節將要說明如何設計與實作本系統-智慧型行動熱點系統(Intelligent Portable Hotspot System, IPHS)。透過本系統可以整合多種異質網路，提供網路環境感知、自動切換與熱點自動認證等機制，讓行動裝置不論是在家裡、辦公室、公共場所或行動中都能保持一致性的上網經驗。

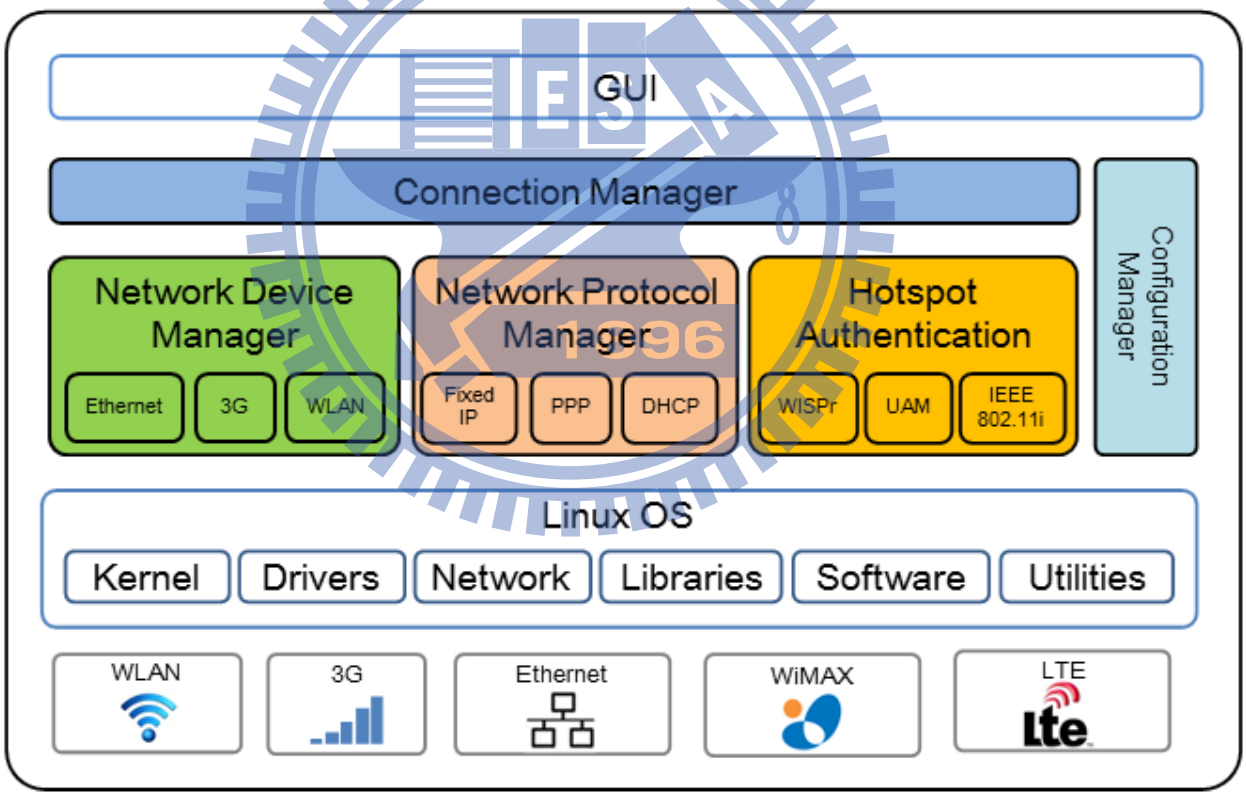


圖 26 IPHS 系統架構

4.1 IPHS 系統架構

IPHS系統架構如圖 26所示，本研究我們將著重於網路裝置控管與連線建立的整合性設計，利用系統平台資源如Linux作業系統、硬體周邊與各種網路

介面等，提供異質網路自動化連線服務。每一個功能都將採取模組化設計，其特色是可以讓IPHS系統具有較佳的移植性與擴充性，讓本系統易於移到任何支援異質網路的硬體平台上面。當然為了讓本系統發揮功效，在硬體選擇方面除了必須支援多樣性網路介面與可電池供給電源之外，在軟/硬體平台的選擇方面並沒有限定。另外，由於本系統也是一種行動網路設備，在電源管理方面依使用狀態採取以下策略，讓系統能有效率地使用電源以延長系統使用時間。

- 啟動狀態

即本系統設備中啟動網路連線服務的狀態，除了無線網路設備所規範的省電標準之外，還會依據無線網路傳輸距離的遠近和網路傳輸的流量，自動調整電波發送功率以調節電源的使用量。

- 閒置狀態

本系統在沒有用戶連線的情況之下則會進入閒置(idle)狀態，此時本系統會要求系統元件及網路介面進入閒置狀態。在此狀態之下，網路介面不會進行任何處理或傳遞資料的訊務。此機制可以省掉不必要的耗電，讓能源能更有效地被利用。當無線網路偵測到用戶行動裝置要求連線時，便會喚醒系統回到啟動狀態並開始提供網路服務。因此，本系統具備偵測網路狀態，自動進入閒置或啟動狀態轉變的能力

- 停止狀態

本系統在停止狀態時將關掉大部分的周邊電源供應，系統設備不會提供任何服務，此時只會留下些許電源給小部分的周邊元件，如電源管理 IC(PMIC)及 RTC 等。用戶必須使用外部開關手動喚醒本系統才能夠回到啟動狀態。這種狀態最為省電，可以延長本系統的使用時間。

本系統實作包含以下幾個功能模組，包含連線管理模組(Connection Manager)、網路裝置管理模組(Network Device Manager)、網路連線協定管理模組(Network Protocol Manager)、熱點認證模組(Hotspot Authentication)和系統設定管理模組(Configuration Manager)等，其詳細說明分別如下：

● 連線管理模組(Connection Manager, CM)

連線管理模組(以下簡稱 CM)是本系統的主要的網路連線協調者，它負責的任務是管理所有網路硬體裝置連線與上層網路協定連線的邏輯控制。當設定管理介面操作本系統時，除了會把設定值傳送給系統設定值模組做資料的儲存之外，還會通知連線管理模組設定值有異動。CM 則會依最新的命令與設定值開始運作並更新目前的狀態。CM 的網路介面管控與網路連建立線需要協調的三個模組，這些模組包括網路裝置管理模組、網路協定管理模組與無線

熱點認證模組。CM 必須監控這些模組的狀態，依據網路環境以及使用者需求提供最佳的連線服務。

下圖 27 為 CM 與其它系統模組的關係。為了因應未來功能模組擴充的需求，CM 設計了統一的模組化管理介面，分別為各個模組定義了一套標準的管理框架，CM 可以透過這個管理框架與模組之間互相溝通。標準化介面的優點是一方面可以提供模組實作的準則，讓各個模組在發展其所屬的功能時把實作內容封裝起來，使各個模組都能保持一貫性的操作介面而不限制實作方法；另一方面在模組客製化時，將有利於新增或關閉某些子模組功能，但不會影響到整體的功能。因此本研究特別設計了統一標準框架，好處是未來要新增功能或模組時，可以專注於功能模組內的實作，而不用重新考慮與 CM 銜接的介面，同時也不用擔心增減功能模組時會影響到原有系統的運作。

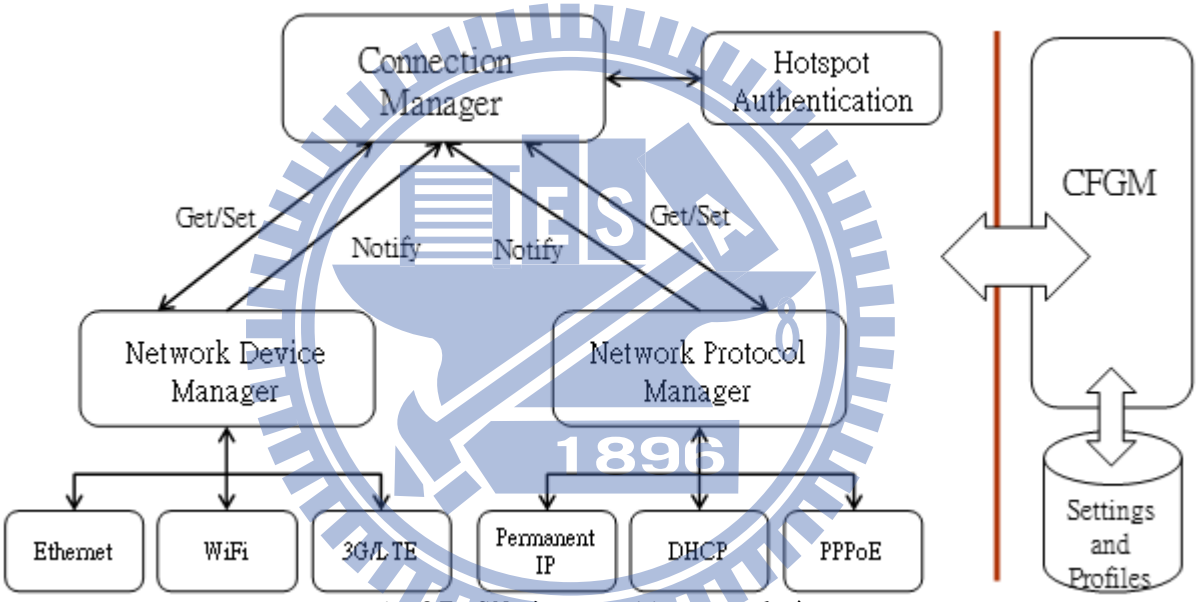


圖 27 CM 與功能模組的關係

- 網路裝置管理模組(Network Device Manager, NETDEV)

網路裝置管理模組主要任務是管理實體的網路介面，支援動態裝置偵測與網路介面狀態的監控。由於不同的網路介面具有不同的操作屬性，本模組會把他們實作的方法封裝起來，各自擁有獨立的狀態偵測以及操作方法；例如，有線網路關心的是網路線是否有接上網路設備；無線區域網路則著重在網路環境的感知，在區域空間內經由掃瞄程序之後，確認是否能找到合適的AP可以聯結(associate)；而3G行動網路則是先確認SIM卡的狀態與基地台的註冊狀況，成功之後才可以建立資料傳輸的通道。因此為了統一管理這些異質網路裝置，設計了一套雙向的溝通機制。從網路裝置模組自動發送的狀態回報稱之為Notify；而CM則可以透過Get與Set來改變或存取網路裝置模組的狀態或設置。

➢ 網路裝置狀態通知(Notify)：

當網路裝置發生改變的時候，裝置模組會主動地回報狀況給上層CM。讓CM盡快知道網路介面的狀態已經異動，CM則會依回報內容的做相對應的處理。下表 5為各種狀態通知的說明。

表 5 網路裝置狀態回報

狀態名稱	NETDEV_PNPIN	使用者	NETDEV
內容說明	針對USB介面考慮支援隨插即用(Plug&Play)的網路設備，分別定義了網路裝置的安裝以及移除二種狀態。當偵測到網路裝置時會NETDEV_PNPIN通知給CM模組。		
狀態名稱	NETDEV_PNPOUT	使用者	NETDEV
內容說明	當偵測到網路裝置移除時，網路裝置會發送此訊息，通知CM網路裝置已經被移除了。		
狀態名稱	NETDEV_LINKDOWN	使用者	NETDEV
內容說明	因為不同的網路裝置有其特定實體層建立連線的方式，為了讓上層CM的可以統一管理，把建立連線分為二個部分，在實體網路未建立連線或不能傳輸資料的狀態稱之為NETDEV_LINKDOWN；其狀態分別如下，無線區域網路在掃瞄階段或尚未通過認證和聯結之前的狀態就歸屬於NETDEV_LINKDOWN；而3G行動網路在SIM卡尚未與基地台建立註冊關係之前也是屬於NETDEV_LINKDOWN狀態。		
狀態名稱	NETDEV_LINKUP	使用者	NETDEV
內容說明	當實體層連線已經建立完成並可以用來傳輸資料的狀態稱之為NETDEV_LINKUP。在網路裝置在這個狀態下時，會發送此訊息給上層的CM。		
狀態名稱	NETDEV_EVENTNOTIFY	使用者	NETDEV
內容說明	網路裝置除了上述的主要狀態回報之外，對於網路品質的監控與管理的資訊可由這個Event Notify回報給上層的CM，例如無線訊號的改變、封包傳送的統計資料、掃瞄結果等。Event列表如下：NETDEV_EVT_LOCKED、NETDEV_EVT_UNLOCK_FAILED、NETDEV_EVT_SCAN_RESULT、NETDEV_EVT_RSSI。		

➢ 網路裝置存取操作：

網路裝置存取操作是一組用來存取與設定於CM模組下層實體網路裝置的程式介面，例如取得實體連線狀態、改變網路裝置的設定以及實體網路連線相關的操作，表 6為此模組基本存取操作的相關說明。

表 6 網路裝置存取操作

命令名稱	NETDEV_GET_STATUS	使用者	CM
內容說明	用來取得網路連線狀態與統計資料。		
命令名稱	NETDEV_SET_CONFIG	使用者	CM
內容說明	當使用者改變網路裝置的設定時，用來通知網路介面更新其設定值。		
命令名稱	NETDEV_PRIV_CONTROL	使用者	CM
內容說明	用來存取網路裝置的特定屬性。例如，無線區域網路的掃瞄機制、天線發送功率等。		
命令名稱	NETDEV_NET_SCAN	使用者	CM
內容說明	驅動無線區域網路執行掃瞄動作。		
命令名稱	NETDEV_NET_SCAN_RESULT	使用者	CM
內容說明	在下達NETDEV_NET_SCAN命令之後，CM可以使用NETDEV_NET_SCAN_RESULT來取得掃瞄結果。		
命令名稱	NETDEV_NET_RECONNECT	使用者	CM
內容說明	要求無線區域網路立即重新建立連線。		
命令名稱	NETDEV_SIM_PIN_PROTECT	使用者	CM
內容說明	用來設定啟動SIM卡的PIN碼保護機制，下次系統啟動使用3G行動網路之前，必須要解鎖PIN碼之後才能與基地台連線。		
命令名稱	NETDEV_SIM_PIN_UNLOCK	使用者	CM
內容說明	設定解鎖SIM卡的PIN碼保護機制。		
命令名稱	NETDEV_SIM_PUK_UNLOCK	使用者	CM
內容說明	當使用者不小心連續輸入三次錯誤的PIN碼之後SIM卡的將會被鎖住無法使用，這時候可以用輸入PUK碼來解除這樣的狀況。		

- 網路連線協定管理模組(Network Protocol Manager, NETPROTO)

此模組所負責管理各種網路連線協定，當網路裝置與欲連線的端點要求建立實體資料傳輸的通道時，必須根據網路業者所要求的方法向網路服務提供者(ISP)取得上網的資訊，這些基本資訊包含 IP 位址、子網路遮罩、預設

閘道的 IP 位址以及網域名稱服務伺服器的 IP 位址等。此模組則依不同的網路服務使用特定的網路連線協定去取得上述的網路基本資訊。但各種協定的連線方式有不同的特性，為了方便管理這些的網路連線協定，此模組也將不同的網路連線協定的管理與操作都封裝起來，CM 模組則可以透過這個統一的介面來管理第三層網路連線能力，表 7 將說明這些操作介面所定義的動作。

表 7 網路連線協定操作介面

介面名稱	NETPROTO_SETUP	使用者	CM
內容說明	設置網路連線時所需要的參數。		
介面名稱	NETPROTO_CONNECT	使用者	CM
內容說明	命令網路連線協定進行網路登入與取得 IP 位址的程序。		
介面名稱	NETPROTO_CONNECTING	使用者	NETPROTO
內容說明	當 CM 發起取得 IP 位址的程序之後，如果不能即時取得 IP 位址時，NETPROTO 將會回應此訊息給 CM 模組示意連線正在進行中。		
介面名稱	NETPROTO_CONNECTED	使用者	NETPROTO
內容說明	當 NETPROTO 取得 IP 之後，NETPROTO 會發送此訊息給 CM 模組通知已經取得上網資訊連線已經完成。		
介面名稱	NETPROTO_DISCONNECT	使用者	CM
內容說明	此訊息由 CM 模組主動發送，目的在要求 NETPROTO 中斷目前在連線中或已連線的狀態。		
介面名稱	NETPROTO_DISCONNECTED	使用者	NETPROTO
內容說明	此訊息由 NETPROTO 模組主動發送，目的在通知上層的 CM 連線失敗或已連線的狀態被中斷了。		
介面名稱	NETPROTO_GET_IPINFO	使用者	CM
內容說明	此操作可以獲取目前網路連線的相關資訊。例如，IP 位址、子網路遮罩、預設閘道位址及網域名稱伺服器位址(DNS)等資訊。		

- 熱點認證模組(Hotspot Authentication)

以無線區域網路技術的熱點服務雖然已經存在一段時間了，但一直到現在關於使用者認證的方式各家業者仍沒有統一的認證標準；目前台灣的無線熱點

服務，雖有少部分熱點支援WISPr標準但大部份仍是採取Web-Based Portal UAM (Captive Portal)的認證方式。雖然這種方式有安全性不足的缺點，但由於這種認證方法在網路架設和使用上具有相當方便的優勢，所以仍被許多網路業者所採用。

由於網路業者之間互相少有訂定漫遊契約的情形之下，當使用者擁有不同的熱點帳戶時，行動設備會在移動後會重新連線，依連線服務這時候必須要採取不同的登入方式，然後重新再做一次網路認證的動作。否則使用者的行動設備會看似連上無線熱點的AP，但事實上行動裝置會因為IEEE 802.1X的機制是無法存取網際網路的資源的。為了解決這個問題，在本系統特別獨立設計了一個熱點認證模組。主要功能是當網路的連線服務需要特定的認證流程時，此模組將負責與不同的無線熱點服務進行認證的工作，可以免除使用者每次都要手動登入認證的麻煩。

- 系統設定管理模組(Configuration Manager, CFGM)

系統設定管理模組主要的目的是提供使用者管理系統設定值，讓系統參數設定可以被儲存和備份。管理模組提供了統一的 API 介面支援設定值的新增、修改與刪除的能力。除了實作設定值支援不同型別和儲存空間的要求之外，此模組還具備一些系統輔助管理的功能，其功能特色介紹如下：

設定值管理：

不同的嵌入式平台會有不同的媒體儲存能力，為了降低平台的依賴性，本系統不使用特定的資料庫系統或檔案系統，就可以提供不同系統的存放能力，例如在有檔案系統的平台，設定值則可以使用檔案方式來存放；反之，無提供檔案系統的平台則支援讀寫快閃記憶體(flash memrory)功能，以原始資料(raw data)的方式儲存在記憶體裡面。

流量統計：

流量統計會依不同的網路介面與網路設定檔分別統計，讓使用者可以了解目前系統各個網路服務的使用狀況。對於有限制使用量的網路服務可以提供節約的功能，例如，用戶可以設定行動網路流量，當到達設定上限後就會自動限制該網路的連線服務。

連線記錄追蹤：

考慮消費者在使用本系統時必須裝載SIM卡及輸入連線認證必要的的帳號資訊，為了保障使用者的帳戶資料，特別設計一套連線記錄追蹤的機制。此機制可以讓本系統在遺失的時候能夠被追蹤。本系統的回報機制可以把目前的網路位址並附帶相關網路資訊通知失主，以利後續處理的佐證資料。

4.2 IPHS 多網(Multihoming)連線切換機制

本系統從實體連線至取得IP位址的過程主要由二個模組負責：網路裝置模組(NETDEV)負責實體連線接取的部分；網路連線協定(NETPROTO)負責取得上網的IP位址。當系統啟動後，NETDEV先會有一個偵測裝置的處理程序，它可以接收外接網路介面的PNP訊息或內建網路介面驅動程式備妥的訊息。對於省電方面，如果系統內網無線AP端無任何裝置連線時，在閒置一段時間後系統將自動切斷對外網路，並進入閒置狀態以節省電源，直到有連線需求時再重新啟動網路偵測與連線機制。以下將依不同的網路類型說明其連線的流程。

行動網路(Wireless Cellular Network)：

行動網路裝置的連線流程如圖 28說明如下。

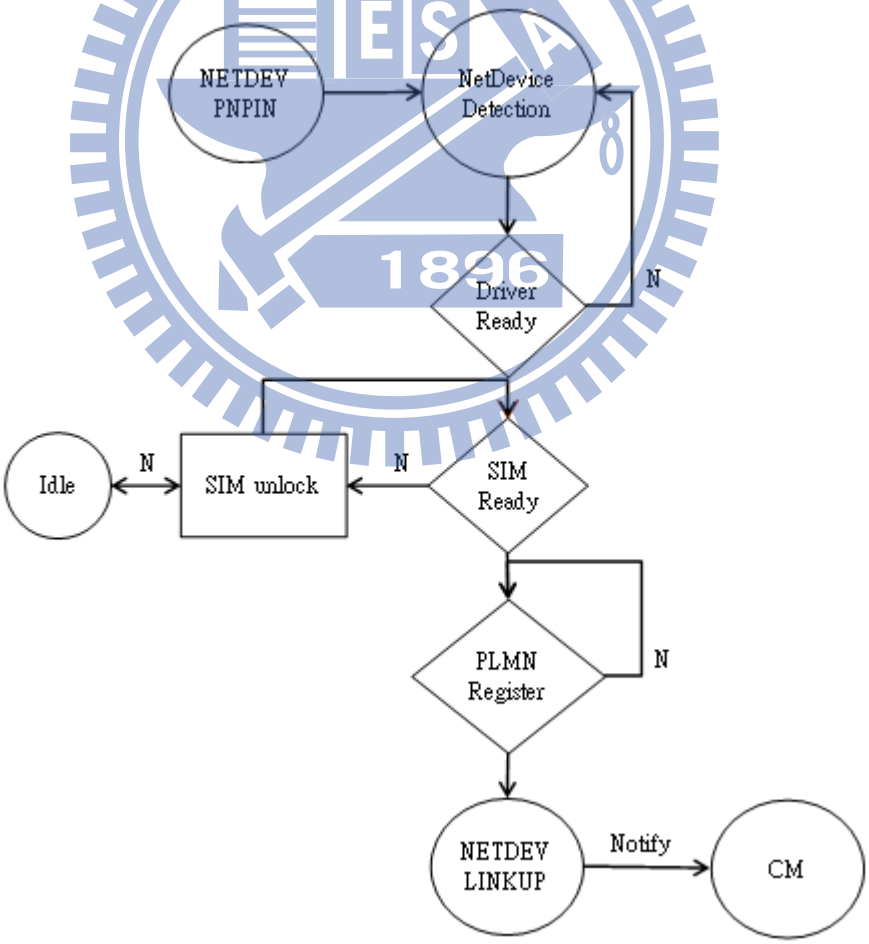


圖 28行動網路裝置連線流程

- 偵測網路設備的存在，等待驅動程式初始化完成。
- 檢查SIM卡的狀態，如果是鎖定的狀態則依系統設定來解鎖；反之當無法解鎖或解鎖失敗時，回報NETDEV_EVT_LOCKED或NETDEV_EVT_UNLOCK_FAILED，之後便會進到閒置狀態(Idle)，等待輸入正確的PIN碼。
- 解鎖成功之後，便會等待並確認是否已經註冊到PLMN(Public land mobile network)網路。
- 註冊成功之後，回報NETDEV_LINKUP狀態給CM模組。
- 在已連線的狀態轉變成連線中斷時，先回報NETDEV_LINKDOWN狀態給CM。NETDEV再重新回到偵測網路設備的狀態。

無線區域網路(IEEE 802.11, WLAN)：

無線區域網路裝置的連線多了掃瞄與比對的動作，流程如圖 29。

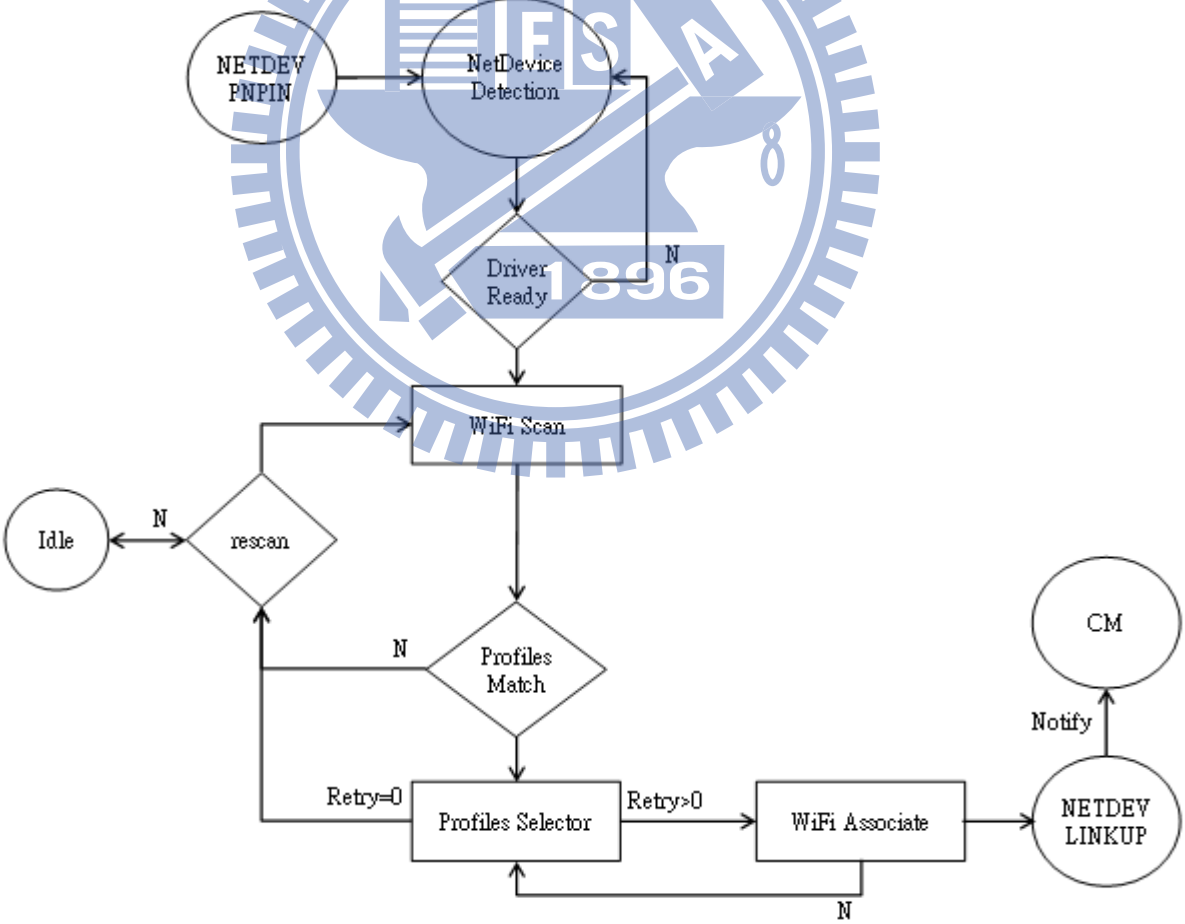


圖 29無線區域網路裝置連線流程

- 初始狀態為偵測網路設備的存在，之後便等待驅動程式初始化完成。
- 取得無線網路設定檔(profile)依設定啟動無線掃瞄動作。掃瞄動作分成主動掃瞄(active scan)和被動式掃瞄(passive scan)二種模式。當沒有任何掃瞄記錄或掃瞄記錄過時，第一次會採取主動式掃瞄模式，之後的掃瞄方法則會採取被動式掃瞄模式。
- 啟動狀態開始會經過三次連續地掃瞄，若無任何符合記錄的AP存在，則會進入到閒置狀態(Idle)。
- 在閒置狀態時，若系統內網無線AP有行動裝置連線存在時，則會周期性每6秒自動掃瞄頻道，首次掃瞄頻道1、5、6、9、11、13，下一輪則以全頻道掃瞄方式，如此循環下去。
- 若有搜尋到符合的AP時，依據使用者喜好設定開始與AP連線；當連線發生問題時則逐一選擇次要的AP來連線。
- 當成功與AP完成關聯(associated)之後就會回報NETDEV_LINKUP狀態給CM模組。
- 若在已連線的狀態如果連線中斷了，則會先回報NETDEV_LINKDOWN狀態給CM。NETDEV再重新回到偵測網路設備的狀態。

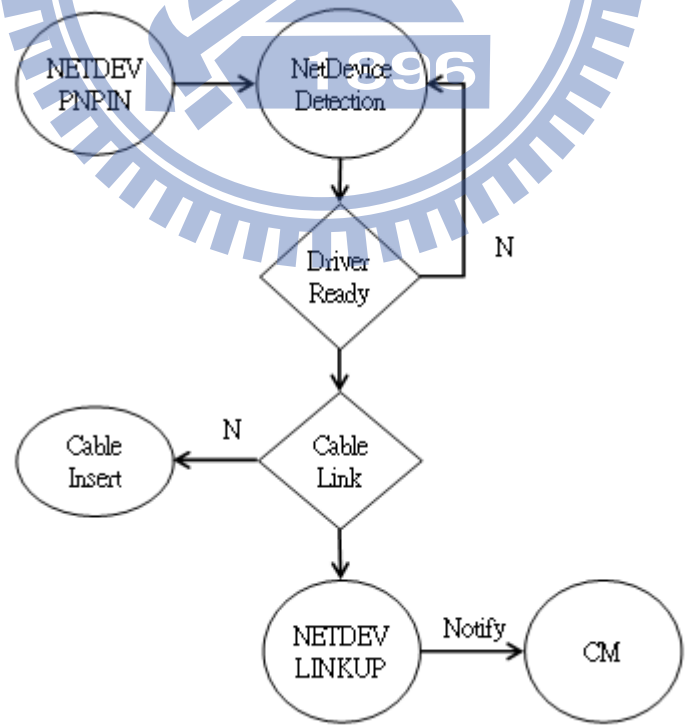


圖 30 有線網路裝置連線流程

有線網路(IEEE 802.3, ETHERNET)：

有線網路裝置的連線流程比無線網路單純，如圖 30所示。

- 先偵測網路設備的存在，等待驅動程式初始化完成。
- 之後偵測網路實體線路是否有效(active)，當偵測成功之後則會回報NETDEV_LINKUP狀態給CM模組。
- 在已連線的狀態如果網路線被移除連線中斷了，會回報NETDEV_LINKDOWN的狀態給CM模組。NETDEV再重新回到偵測網路設備的狀態。

當存在多重對外網路的時候連線切換機制便會啟動，預設情況會依據網路的速度、可靠度和費用來依序切換網路連線，切換機制運作如下說明(圖 31)：

1. 當IPHS系統啟動之後，各個網路裝置模組會同時進入網路裝置偵測程序的準備動作。
2. 網路裝置模組偵測到網路裝置時，便會對它初始化並依據使用者設定來決定是否進行實體層及資料連結層的連線程序。
3. 完成實體成連線之後，便會發送LINKUP訊息通知上層CM做進一步的動作。
4. CM收到網路裝置模組的回報後，再去設定網路連線所需要的資料，開始進行IP取得的動作。
5. CM依據設定啟動對應的網路協定模組連線動作進行取得IP的連線步驟。
6. 網路協定模組取得IP位址後立即發送已連線(NETPROTO_CONNECTED)的訊息給CM。
7. CM會依據下列策略來設定不同的對外的連線。

- 如果此連線是目前唯一的連線：

  對此連線設定成預設的路由閘道，讓IPHS所服務的後端裝置能透過此連線使用網際網路。

- 如果原來已經存在對外的連線：

  依系統設定有二種模式可以選擇，單一路由模式和多重路由模式。

  單一路由模式－只會存在單一的對外預設路由閘道，優點是可以幫助使用者節省網路通信費，並自動選擇可靠度較高網路連線、其優先次序為有線網路，無線區域網路，最後為行動網路。其切換方法分成二種方式。第一種是立即切換預設閘道，會立刻把預設閘道設定成新的連線並中斷舊有連線，往後對外的封包將往新的閘道出去；另一種方式是新舊連線會並存一段時間，並把路由設置到優先次多較高的網路介面，對於優先次序較低的

連線會監測它的網路流量，延遲一段時間後再切斷其網路連線，避免正在傳輸中的session因此而中斷。

多重路由模式－使用多重路由模式時可以允許存在多個對外的網際網路連線，每個對外連線可以設定不同的權重，可作為負載平衡的用途，適合行動網路通信流量無上限的的使用者。預設權重是有線網為5，無線區域網路為3，行動網路為2。

8. 檢查IP是否衝突，由於IPHS系統的對外網路是採用NAT方式提供LAN端的私有網路位址可以共享網際網路資源，所以在取得上網IP位址的時候有可能被分配到與IPHS系統相同子網路的私有網路位址。這樣的情況尤其會發生在使用公眾無線熱點的情境之下。衝突解決辦法首先避免把私有區域網路中的DHCP伺服器中的租用時間設定太長；再來，動態改變LAN端的私有網路位址，並強迫LAN端的裝置斷線，讓LAN端設備重新取得新的私有網路位址。
9. 如果連線的網路種類是無線區域網路時，則會依據SSID決定是否發動自動熱點認證機制。

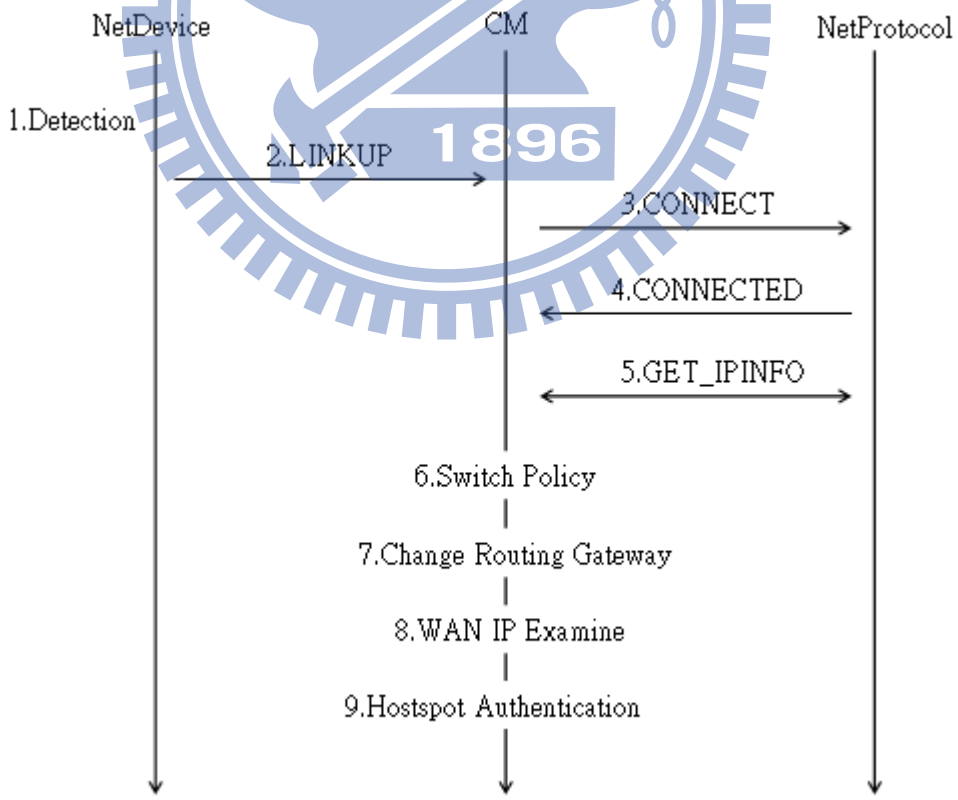


圖 31 基本連線程序

當存在兩個以上的網路連線時，圖 32 說明 IPHS 如何切換不同的對外網路連線。

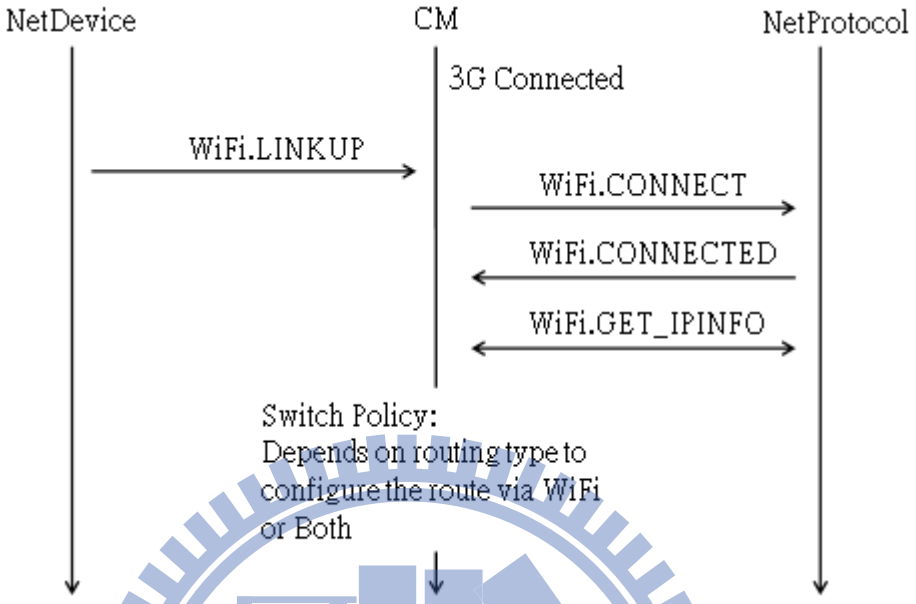


圖 32 多重連線切換

為了加速無線網路斷線後的連線速度，會預先做掃瞄的動作找出下一個更合適的網路。預設行為是以相同的ESSID(Extended Service Set Identifier)為主要連接對象，其次再依設定的優先次序來連線。當連線成功之後會記錄當下的訊號強度(Received Signal Strength Indication, RSSI)當作本系統移動偵測的基準，連線模組會持續記錄RSSI值的上升或下降的趨勢，當RSSI值低於門檻值(預設值為-75dBm)時，便會預先發動掃瞄的動作，把多次掃瞄的結果依RSSI值排序，並記錄每次掃瞄後其RSSI的變化，之後找出符合系統設定的AP並預設其為下次換手的候選對象之一。

圖 33為預測無線網路環境即將改變，本系統所要採取的切換流程的情況。透過無線網路訊號的遞減來決定是否發動無線掃瞄的機制。當環境中掃瞄結果存在訊號較佳的無線AP的時候，只要目前無線網路的訊號低於門檻值就會轉換連線至其它的無線AP。

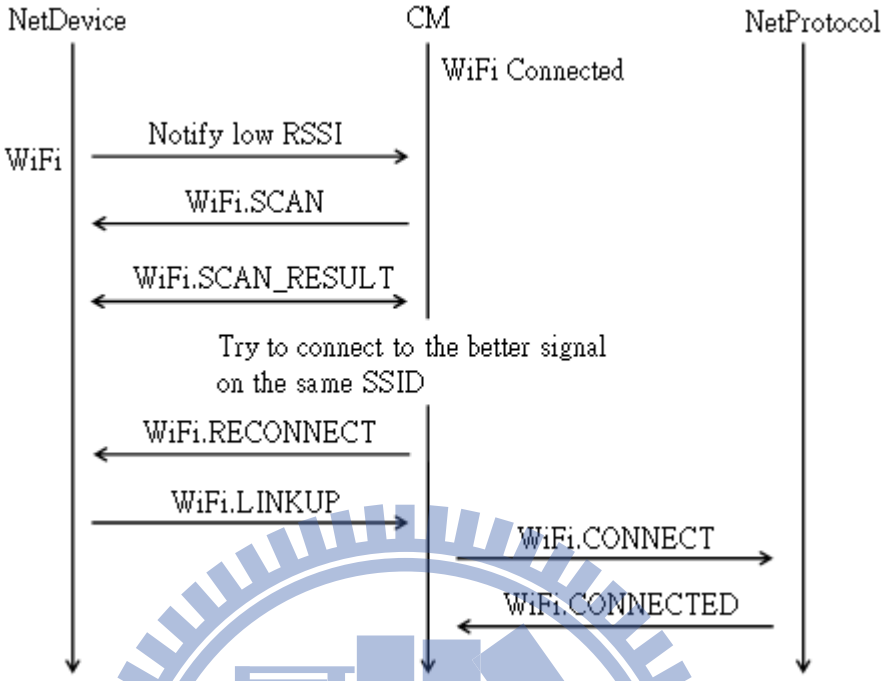


圖 33 連線切換-WiF→WiFi

下圖 34為無線區域網路連線失敗的程序。在環境中無法找到合適的無線網路時，進而轉換回到行動網路連線。

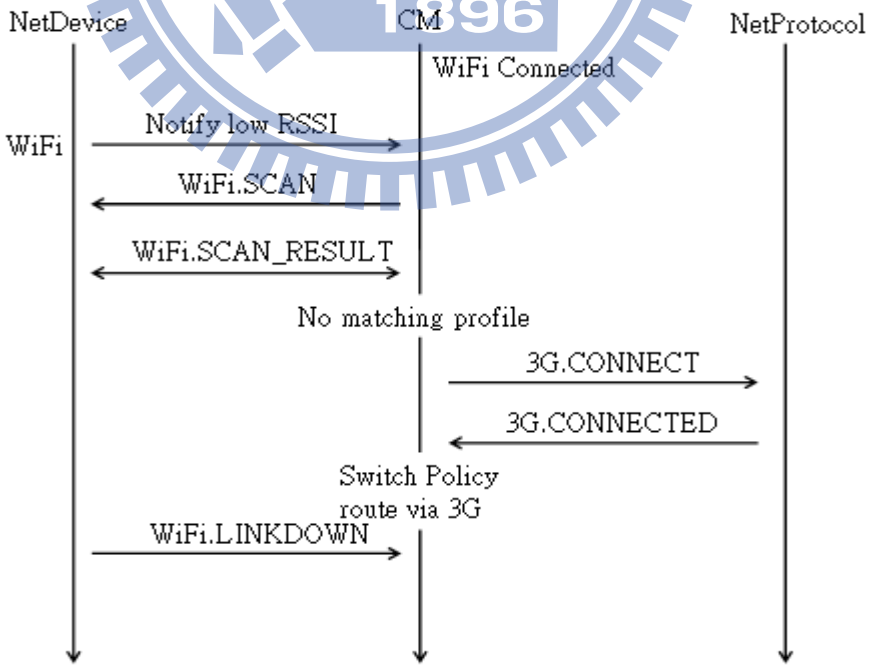


圖 34 連線切換-WiFi→3G

圖 35為無線網路連線完成之後，視連線對象AP的設定來判別是否要啟動無線熱點自動認證的程序。

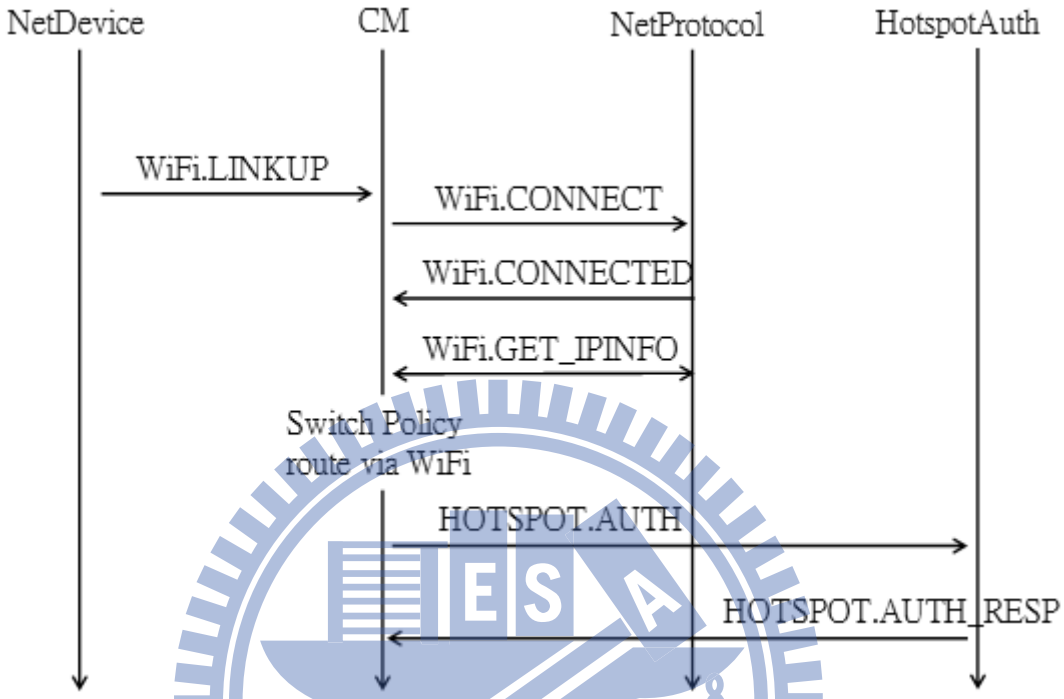


圖 35連線切換-WiFi與熱點認證

4.3 IPHS 系統開發

在本小節將說明如何利用嵌入式Linux系統平台實作本系統，內容包括連線管理模組、網路裝置模組、網路協定模組、系統設定管理模組與熱點認證模組等模組的軟體開發與實作內容。

4.3.1 連線機制實作

連線管組管理模組(CM)主要的功能是提供軟體架構並負責統合管理網路裝置管理模組(NETDEV)、網路協定管理模組(NETPROTO)與熱點自動認證等功能模組，依據網路環境與系統設定來執行連線切換的政策。

連線功能的框架實作於Linux平台的示意圖如圖 36。由於採取模組化的設計，所以本系統據有易於移植的特性，針對系統平台與硬體相依的部分做修改即可建構在各種的軟/硬體平台之上。在同樣的軟體框架與操作方法之下，每一個模組都可以利用平台的特性與能力，實踐同樣的異質網路連線管理能力。

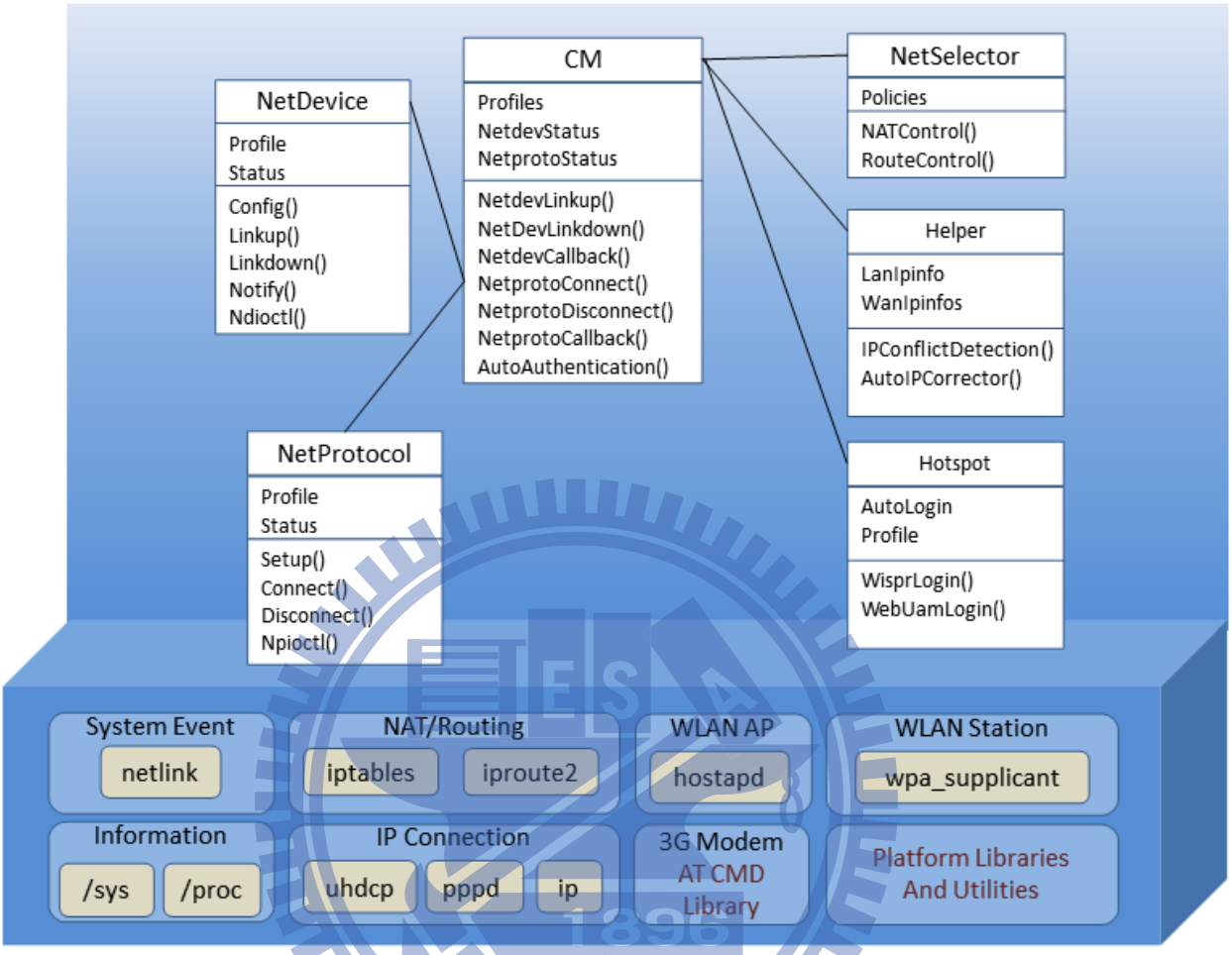


圖 36 IPHS系統框架實作

連線管組管理模組(CM)

- 路由管理-利用Linux的iproute2應用程式來設定多重路由模式或單一路由模式，其參考指令範例如下：

多重路由模式：

#ip route add default scope global nexthop via 192.168.1.254 dev eth0 weight 5 nexthop via 223.138.20.202 rmnet0 weight 2

單一路由模式：

#ip route add default scope global nexthop via 192.168.1.254 dev eth0 weight 1

- NAT管理 - 利用iptables/Netfilter中的MASQUERADE模組來實現。

- IP自動修正 - 當WAN端和LAN端IP具有相同的子網路時，會暫時性地自動修改LAN的IP位子和子網路設定。

網路裝置管理模組(NETDEV)

此模組的主要任務是管理實際的網路介面。利用 Linux Netlink 機制實踐不同的實體網路管理功能。

- 偵測外接網路卡-網路裝置分為平台內建與USB外接二種，內建的網路裝置可以省去硬體存在與否的偵測動作；外接裝置則是需要利用Linux核心的Netlink機制來獲得網路介面卡新增或移除的狀態。
- 管理實體網路卡連線-利用netlink通知機制與Linux系統sys/class/net中的資訊獲得網路介面裝置的狀態；實體網路連線則依不同的網路裝置使用不同的方法去控制連線。

網路協定管理模組(NETPROTO)

網路協定管理負責維護網路層的連線並取得IP相關資訊的部分，這些資訊包含IP位址、子網路遮罩、預設閘道器位址、網域名稱伺服器位址等。本系統目前實作了固定IP、DHCP、PPP和PPPoE等四種網路協定模組。

- 固定IP子模組-只須把使用者設定利用ip或ifconfig指令設定網路介面。
- DHCP子模組-使用busybox中的udhcpc程式去取得IP相關資訊。
- PPP子模組-則是利用pppd程式根據使用者設定產生3G數據機連線必要的設定值，如連線的初始化設定、帳號、密碼、與認證方法等。3G USB網路卡的實體介面通常會以串列埠(usb serial)的方式來呈現，所以要利用PPP與AT指令集跟3G網路卡(數據機)來溝通，以開通實體的網路連線。
- PPPoE子模組-則是使用pppd中的pppoe外掛模組(plugin)來實現，與PPP模組不同的地方是PPPoE的實體介面通常是乙太網路(Ethernet)介面或無線區域網路(IEEE 802.11)介面。

4.3.2 熱點認證模組

無線熱點認證模組，本系統實作支援三種方式：IEEE802.11i、WISPr與網頁認證(web-based portal UAM)等方式。其中IEEE 802.11i認證方式將利用開源軟體wpa_supplicant應用程式來實作，它支援許多EAP的認證演算法，依據網路認證的需求把認證資訊填入組態檔之中，下面將舉例二種常用的EAP認證組態的設定。

- EAP-TLS組態設定

在組態設定中可以指定EAP-TLS認證所需要的id和公開金鑰演算的公鑰和私鑰等資訊。

```
network={
    ssid="ssid_of_eap_tls"
    scan_ssid=1
```

```
    key_mgmt=WPA-EAP
    pairwise=CCMP TKIP
    group=CCMP TKIP
    eap=TLS
    identity="username@domain.com"
    ca_cert="/pathto/cert/ca.pem"
    client_cert="/pathto/cert/user.pem"
    private_key="/pathto/cert/user.prv"
    private_key_passwd="yourpassword"
}
```

- EAP-PEAP組態設定

```
network={
        ssid="ssid_of_eap_peap"
        scan_ssid=1
        key_mgmt=WPA-EAP
        pairwise=CCMP TKIP
        group=CCMP TKIP
        eap=PEAP
        identity="username@domain.com"
        password="yourpassword "
        ca_cert="/pathto/certs/cacert.pem"
        phase1="peapver=0"
        phase2="MSCHAPV2"
}
```

在WISPr熱點認證方面，本系統模組則依據”WiFi Aliance-Wireless ISP Roaming (WISPr v1.0)”規格書中”The Smart Client to Access Gateway Interface Protocol”的說明，實作wispr_client應用程式，本模組的WISPr認證流程如圖 37所示，有偵測、認證、連線完成等程序。

另外，對於採用網頁登入來驗證使用者的權限的熱點服務，由於沒有統一的規則或標準可以遵循，所以網頁的表單設計會依各家網路系統業者的需求會有不同參數設定。因此，為了支援目前市面上這一類的熱點服務，網頁自動認證模組的實作方式將依各家熱點服務設計了不同的認證子程序，依無線網路AP的SSID名稱來分辨不同的熱點服務，其認證的程序則會對應到不同的認證程序模組。認證子模組將被設計成對應到不同的熱點認證方法，這種方式將有利於未來可以擴充或修改，讓本系統的自動認證模組增加了許多彈性。

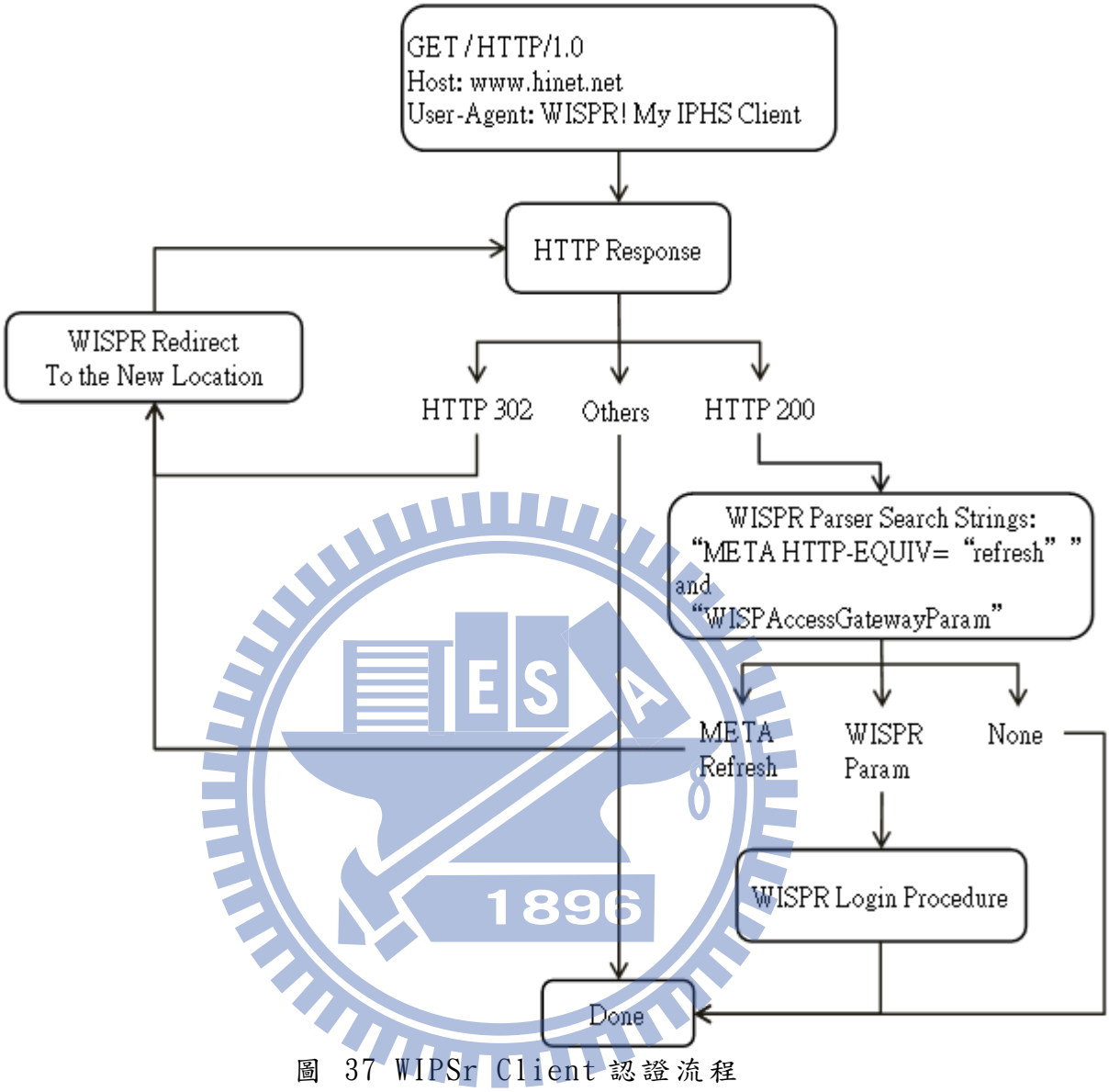


圖 37 WIPSr Client 認證流程

本系統網頁自動認證模組的實作方式，首先要分析各家系統業者的網頁的表單內容，並利用Fiddler Web Debugger這一套軟體去攔截瀏覽器所送出的認證資料，此資訊通常會在HTTPS POST的封包之中。之後再把記錄下來的認證步驟及表單的參數實作到自動認證的子模組中。

當無線區域網路連線成功的時候，自動認證程序會先偵測並判斷是否需要額外的登入程序，並根據不同的SSID名稱來判別是哪一種無線網路熱點服務。再為此特定的熱點服務執行自動登入的動作。以下將舉例說明本研究所實作的三種網頁式熱點認證所採取的方法，其認證資訊規格如下。

交大校園無線網路的認證資訊：

交大校園無線網路	ESSID=NCTU-Wireless
HTTP POST 認 證 內 容	
POST **http://140.113.191.254/auth/index.html** HTTP/1.1 Host: 140.113.191.254 (Partial HTTP HEADER did not display) **user**=D2Account%40@nctu.edu.tw&**password**=YourPasswd&**cmd**=authenticate &Login=Log+In	
說 明	表單動作(ACTION) https://140.113.191.254/auth/index.html 表單資料 user:交大Email帳號 password:密碼 cmd=authenticate

台灣免費的公共區域無線熱點的認證資訊：

中央行政機關室內 公共區域免費無線上網	ESSID=iTaiwan
POST **https://wlanac.hinet.net/loginpages/userlogin.shtml** HTTP/1.1 Host: wlanac.hinet.net Origin: http://auth.itaiwan.gov.tw Content-Type: application/x-www-form-urlencoded (Partial HTTP HEADER did not display) **clt_user**=YourPhoneNumber&**clt_pass**=YourPasswd&type=0&**username**= itw_itw/YourPhoneNumber@itw&**passwd**=YourPasswd &**session**=SIFur6Amf7RKc6BSe5R-f3UjPGhie6xWg6BWj%2FxXx6RWh7hWh8wHiIE jT9Byg5hui065	
說 明	表單動作(ACTION) https://wlanac.hinet.net/loginpages/userlogin.shtml 表單資料 clt_user:輸入表單的帳號(即手機號碼) clt_pass:密碼

	type:0~2 0=iTaiwan,1=TPE-Free,2=NewTaipei username:"prefix"+clt_user+帳號分類; 帳號種類: 當type=0,"itw_itw/" + clt_user + "@itw" 當type=1,"tpe_itw/" + clt_user + ".tpe@itw" 當type=2,"ntpc_itw/" + clt_user + "@itw" passwd:密碼 session=在轉址的過程中可以取得

中華電信無線熱點的認證資訊：

中華電信Hinet	ESSID=CHT WiFi(Hinet)
POST **https://wlanac.hinet.net/loginpages/userlogin.shtml** HTTP/1.1 Host: wlanac.hinet.net Origin: http://auth.itaiwan.gov.tw Content-Type: application/x-www-form-urlencoded (Partial HTTP HEADER did not display) **cht_user**=YourPhoneNumber&**passwd**=YourPasswd&&**username**=username@emome.net&**password**=YourPasswd&**session**=SIFur6Amf7RKc6BSe5R-f3UjPGhie6xWg6BWj%2FxXx6RWh7hWh8wHiIEjT9Byg5hui065&**custom**=cht	
說　明	表單動作(ACTION) https://wlanac.hinet.net/loginpages/userlogin.shtml 表單資料 cht_user:輸入表單的帳號 passwd:密碼 usrname: 帳號+帳號種類，例如emome.net password:密碼 session:在轉址的過程中可以取得 custom:cht為固定資訊

4.3.3 系統設定管理模組

系統管理模組為了讓系統易於移植與設定，外部應用程式可以透過此模組提供的 IPC 介面與本系統互相溝通，方便地管理 IPHS 及監看系統狀態，包含行動網路的設定、無線區域網路的設定、連線切換機制的設定、內部網路服務的設定、管理者密碼的設定、流量統計、系統記錄，連線追蹤等功能。本研究在嵌入式 Linux 平台仍採用 UNIX domain socket 作為 IPC 的底層介面，透過事先定義好的資料結構即可以存取本系統相關資訊。

以內置的網頁伺服器作為使用者介面為例，網頁伺服器的 CGI 程式可以透過本模組的 IPC 介面管理本系統。設定資料將經由 IPC 送至後台的系統管理模組裡，此管理模組便會通知資料相關的功能模組更新其功能設定，其運作示意如圖 38。

IPC 函式庫在系統移植部分扮演著相當重要的角色，因為它可以很彈性地任意替換成其它的使用者前端介面。只要前端程式內部仍根據 IPC 函式庫的呼叫規則，不需要修改本系統內部結構就可以無縫地轉換使用者前端介面。另一方面在移植其它平台的時候，只要 IPC 函式庫內部依照該平台的特性客製化，就可以讓該系統平台擁有存取和控制本系統的能力，如此一來提高了本系統對其它平台的的可移植性。

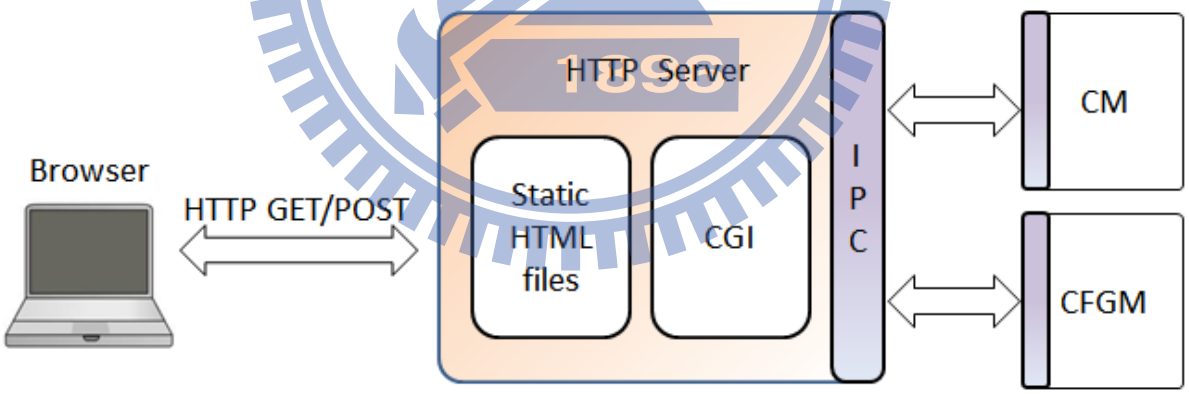


圖 38 系統管理之 IPC 運作方式

系統管理模組除了提供上述與外部溝通的介面之外，還具備以下輔助功能。

設定值管理：

為了減少嵌入式系統平台的儲存能力的相依性，本系統設計了一套自有的設定值管理機制，實作上採用二維串列的方法來實現設定值的新增、修改與刪除。對於系統相依性較高的部分依系統平台的能力實作不同的載入(load)與儲存(save)的方法。圖 39為設定值管理機制的示意圖。

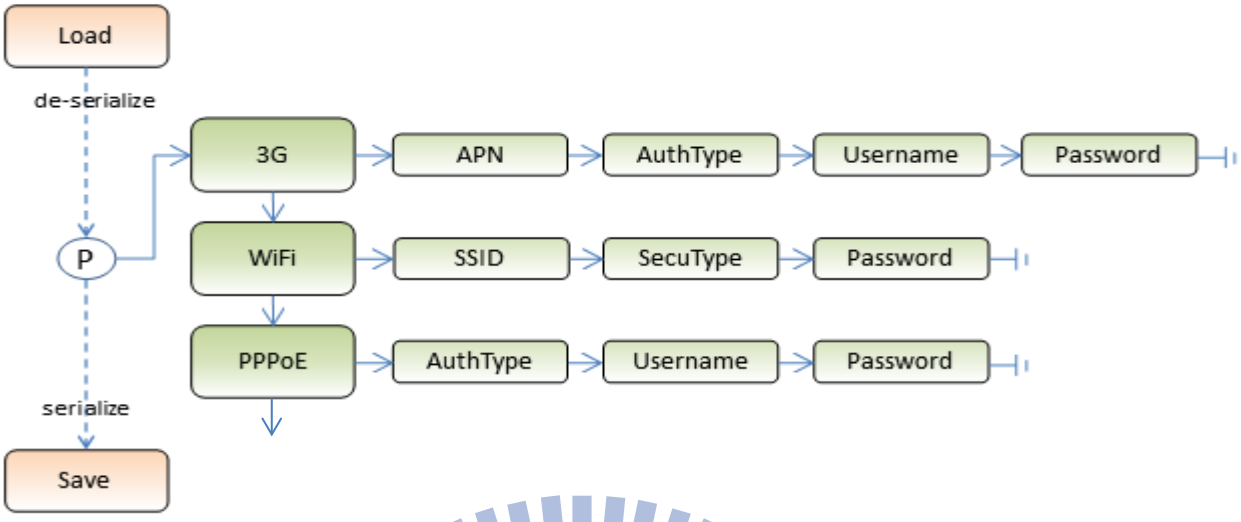


圖 39 系統設定值管理機制

流量統計：

流量統計依使用的網路介面與設定檔來統計，讓使用者可以了解本系統目前各個網路服務的使用狀況。記錄方式為每次連線和斷線的時候各記錄一次，如果有設定限額傳輸量的網路超過指定的傳輸量時將會被標記；然後依據使用者的設定決定是否立刻斷線或者持續連線直到斷線為止。本系統有一個常駐程式會持續監視於Linux上特有的/proc/net/dev這個系統檔案，以達到流量統計的功能。

連線記錄追蹤：

本系統為了保障使用者的帳號安全，特別設計了一套追蹤網路設備的功能。利用trace routing與email的機制。在本系統連上網際網路的時候即可發動這個機制。實作方法是從本系統內部向特定網站發出trace routing的封包，並逐一蒐集這些回應的封包確認本系統的路由路徑(hop)，然後搜集部分系統相關的資訊，如：IMSI資訊和無線網路的設定等。之後利用SMTP協定把內容寄送到使用者指定的Email信箱。

使用者在遺失本系統的情況之下，便可以利用這些資訊追蹤本系統的大概位置，然後可以進一步提供這些資訊給警政單位協助尋找失物。當然如果使用者擔心個人資料外洩，也可以禁用本系統所提供的功能。

系統韌體更新：

由於網路服務的變化很快，尤其是無線熱點認證方面，為了提供更好、更豐富的網路連線服務，本系統可以透過這個模組來更新系統功能。

五、系統建置與分析

經由上一章IPHS系統架構與開發的說明，我們將依據IPHS的設計理念來建置一套完整的系統，本章節將評估本系統的實用價值與實測結果。首先介紹本系統軟體和硬體的開發環境，以及本系統開發時所選用的開放原始碼軟體；接著量測不同情境下的網路連線切換效能。最後，於實際網路環境應用本系統的自動熱點認證的功能。

5.1 系統建置環境

本研究是以開放原始碼的嵌入式Linux作業系統作為實作平台，本小節首先介紹本系統開發時所使用的軟體和硬體環境；接著說明系統所使用幾個重要的開放原始碼軟體以及相關的函式庫。

5.1.1 開發環境介紹

本系統實作使用的硬體平台是由高通(Qualcomm)公司所開發Snapdragon S1系列的MSM7x27 SURF開發板；此系統平台包含了二個ARM處理器核心、行動基頻處理器、二個無線區域網路晶片分別對應AP模式以及Station模式、圖形處理器、電源控制IC以及容量為1600mAh的鋰電池等；硬體平台相關資訊如下表 8。

表 8 IPHS 開發硬體平台

功 能 元 件	規 格
應用處理器	核心：ARM1136JF-S™ 速度：600MHz 指令集：ARMv6 DSP：QDSP5000 320 MHz
行動數據處理器	核心：ARM926EJ-S 速度：400MHz 指令集：ARMv5TEJ DSP：QDSP4000 122.88 MHz
記憶體	256MB
儲存空間	128MB NAND Flash
繪圖處理器	Adreno 200
行動網路	支援 GSM/GPRS/EDGE、UMTS/WCDMA、HSPA
無線區域網路	Atheros AR6002 IEEE 802.11 chip
電池	鋰電池1600mAh
周邊介面	USIM、USB2.0、UART、SDIO等

平台上所提供軟體開發環境為Android 1.6版，它是一種以Linux核心為基礎的開放原始碼作業系統，主要被使用於行動裝置如智慧型手機、平板電腦等。雖然此平台提供Android開發環境，但基於系統未來移植的考量並不會利用Android所提供的軟體框架(JVM framework)，所以實作方式將視此平台為一個標準的嵌入式Linux作業系統的開發環境，程式開發實作上則直接使用C語言作為主要的程式開發語言，並且根據Linux所提供的方法與系統核心來溝通，本系統開發環境與相關設置如下表。

表 9 開發環境與相關設置

電腦備配	Notebook：ASUS U6Vc CPU：Intel Core 2 Duo T9400 2.53G RAM：DDR2 4GB HDD：320GB Network：Intel® PRO/Wireless 4965ABN Ethernet 10/100/100Mbps USB Port：3個
作業系統	Ubuntu 10.10
開發輔助軟體	git-core、gnupg、flex、bison、gperf、zip、curl、build-essential、zliblg-dev、gcc-multilib、g++-multilib、libc6-dev-i386、lib32z-dev、lib32ncurses5-dev、ia32-libs、x11proto-core-dev、libx11-dev、lib32readline5-dev、repo、bash、samba、minicom
編譯工具鏈	CodeSourcery ARM toolchain： arm-2006q3-27-arm-none-linux-gnueabi-i686-pc-linux-gnu.tar.bz2 JDK： jdk-1_5_0_xx-linux-i586.bin
Linux BSP	於Code Aurora Forum下載MSM/QS系列的開放原始碼包裝，加上高通公司獨有的Patch安裝包

開發過程中為了加速開發流程通常會使用Android提供的特有工具ADB，全名為Android Debug Bridge，是開發Android時很常用到的工具。使用者可以從Android官方網站下載SDK，並在platform-tools目錄中找到它。ADB是一種採Client-Server的RPC架構，開發端電腦可以透過USB介面經由ADB的協定可以登入到開發目標設備裡，類似於使用Telnet登入工作站的方法，可協助程式執行與除錯。不過ADB提供更多的功能。例如，把檔案上傳至開發目標設備的檔案系統中或者從目標設備的檔案系統中取出檔案等。本系統在開發階段一般都會採用這樣的流程，以避免大範圍NAND區塊的更新與燒錄動作，減少每次除錯時的驗證時間。

5.1.2 使用的軟體與程式庫介紹

系統功能開發使用了幾個重要的開放原始碼軟體程式，以輔助實現本系統部分的功能，本小節將介紹本系統所使用的開放原始碼軟體程式。

WPA Supplicant

早期Linux系統對於無線區域網路的設定非常不友善，使用者通常要使用如iwconfig、iwpriv、iwlist等相關命令設定無線網路，指令和參數不但不容易記憶且缺乏良好的AP設定檔的管理機制。不過在wpa_supplicant[21]管理工具推出之後便解決了上述的問題。wpa_supplicant的無線區域網路的連線能力支援IEEE 802.11i與多種EAP加密方法，其功能特色支援列表如下表 10；透過設定檔功能可以管理多組AP設定並具有自動掃瞄與連線功能，這些功能對於使用者來說相當便利。

Hostapd

hostapd[22]與wpa_supplicant是系出同門的工具程式，但它的功能定位屬於無線區域網路AP端的軟體程式，其功能特色與wpa_supplicant相同，但hostapd所扮演的角色正好與supplicant相互對應。hostapd可以控制特定的無線網路卡驅動程式，讓無線網路卡提供無線AP服務的能力。本系統的無線網路卡支援此工具程式，AP相關設置可以透過此工具程式來達到目的。

表 10 WPA Supplicant 與 Hostapd 的功能特色

WPA/ IEEE 802.11i	WPA-PSK ("WPA-Personal") WPA with EAP ("WPA-Enterprise") key management for CCMP, TKIP, WEP104, WEP40 WPA and full IEEE 802.11i/RSN/WPA2 RSN: PMKSA caching, pre-authentication IEEE 802.11r、IEEE 802.11w Wi-Fi Protected Setup (WPS)
EAP methods	EAP-TLS、EAP-PEAP/MSCHAPv2、EAP-PEAP/TLS、EAP-PEAP/GTC、EAP-PEAP/OTP、EAP-PEAP/MD5-Challenge、EAP-TTLS/EAP-MD5-Challenge、EAP-TTLS/EAP-GTC、EAP-TTLS/EAP-OTP、EAP-TTLS/EAP-MSCHAPv2、EAP-TTLS/EAP-TLS、EAP-TTLS/MSCHAPv2、EAP-TTLS/MSCHAP、EAP-TTLS/PAP、EAP-TTLS/CHAP、EAP-SIM、EAP-AKA、EAP-PSK、EAP-FAST

Busybox

BusyBox最初是由布魯士·伯倫斯(Bruce Perens)在1996年為Debian GNU/Linux安裝光碟所編寫的工具程式，其原始構想是希望在一張軟碟片上能放入一個開機系統且能提供基本的功能。BusyBox把UNIX系統中常用的工具指令，如sh、cp、mv、mkdir、chmod、find和grep等，經過精簡化之後結合成一個單一可執行的檔案，命名為busybox。busybox雖然容量小但功能足以媲美原始大型系統裡的工具程式。隨著嵌入式Linux系統的發展，busybox的功能也趨於完備，可以為任何小型或嵌入式系統提供一個相當完整的shell操作環境。因為Android裡toolbox相對地比busybox功能要來得少，為了讓Android系統更貼近於標準的Linux系統，本系統特別把它列入開發必要的軟體之一。

Iptables

Iptables[24]是一個用來設定Linux防火牆的應用程式，系統管理者可利用此工具程式配置kernel中Netfiler模組的鏈表和規則，Netfilter模組是一種軟體框架，它掛載(hook)於核心的網路層，可用來監視封包的流進、流出與轉送，封包流動與Netfilter的關係如圖 40。透過Netfilter的軟體框架可以無限地擴充它的功能模組，使得Linux作業系統可以支援各種網路封包過濾、連線標記、SNAT以及DNAT等功能。本系統設計便使用了MASQUERADE與MARK等擴充模組實現NAT與連線追蹤的能力。

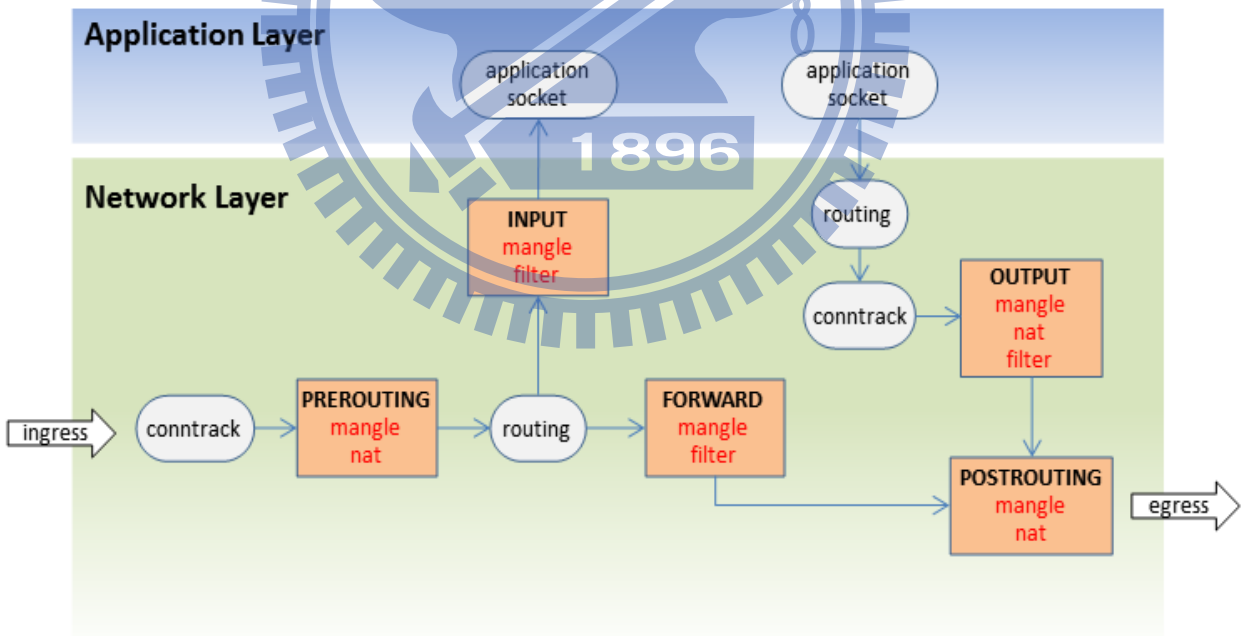


圖 40 封包流向與 Netfilter 關係

OpenSSL

OpenSSL是一個開放原始碼且功能齊全的SSL程式庫，實作了諸如雜湊演算法 (Hash algorithms)、加解密演算法(Encryption/Decryption algorithms)以及Secure Sockets Layer(SSL v2/v3)和Transport Layer Security(TLS v1)

等協定。本系統的無線熱點認證模組將需要此程式庫的支援，以實現HTTPS的連線能力。

Iproute2

Iproute2一套網路工具程式集，它可以提供比傳統工具程式更進階的功能，例如本系統需要設定多重路由功能必須借助此工具來達成。下表是iproute2與傳統net-tools工具程式的比較表。

表 11 iproute2 與傳統 net-tools 工具程式的比較表

功　能	傳統 net-tools	iproute2
Address and link configuration	ifconfig	ip addr, ip link
Routing tables	route	ip route
Neighbors	arp	ip neigh
VLAN	vconfig	ip link
Tunnels	iptunnel	ip tunnel
Multicast	ipmaddr	ip maddr
Statistics	netstat	ss

資料來源：http://en.wikipedia.org/wiki/Iproute2

PPP daemon

PPP協定在Linux系統實作分成二個部分，在核心中的PPP驅動程式負責傳遞封包到指定的實體網路介面與產生虛擬網路裝置(如，ppp0)；而pppd(PPP daemon) [27]則是使用者層的應用程式，用來與核心驅動程式溝通。使用者可以把連線所需要的資料填入PPP設定檔之後，pppd將負責與PPP伺服器協商認證和網路層資訊的交涉等動作，待連線建立之後將持續維護與PPP伺服器的連線。本系統的NETPROTO模組則是利用此應用程式實踐PPPoE(PPP over Ethernet)、PPTP(Point-to-Point Tunneling Protocol)等網路存取協定，以及外接3G行動網路卡時的PPP撥號連線能力。

5.2 IPHS 評估分析

在本論文的第四章說明了IPHS的系統架構與實作重點，本節將驗證本系統的開發成果。IPHS系統的評估分析分成二個部分，第一個部分是連線切換的效能評估，包含各別網路介面從待機狀態連上網際網路的時間、行動網路對無線區域網路之間的切換、無線區域網路之間的切換、有線網路熱插拔偵測與切換等；第二個部分著重於無線熱點自動認證的實測，將前往實際的公共環境去驗證熱點自動認證的運作情況。我們期望藉由這些驗證結果確認所有功能模組都能達到本研究所預期的目標。

5.2.1 系統連線效能分析

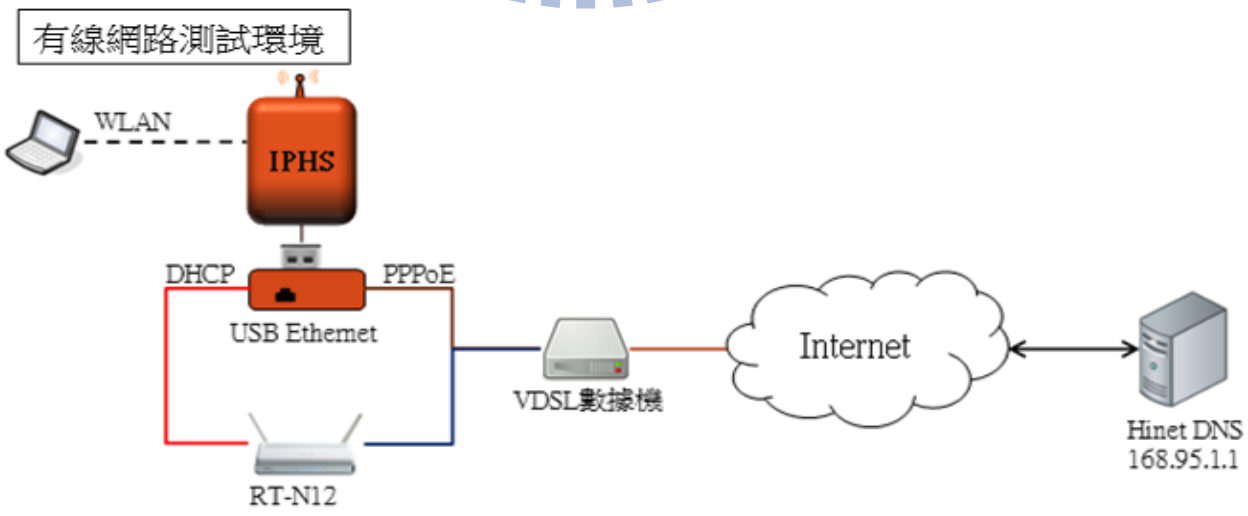
本研究主要的測試項目將使用實際的網際網路環境來驗證成果，準備的測試設備如下。

1. 中華電信 3G 行動網路 SIM 卡。
2. 二台家用閘道器分別為 ASUS RT-N12 無線路由器與 D-Link DIR-619L 無線路由器和一台 L2 交換器(switch)。
3. 中華電信光世代 VDSL 數據機作為 ASUS RT-N12 的對外網際網路。
4. USB 2.0 介面的 Ethernet 網路卡(晶片為 10/100,ASIX AX88772)，用來測試有線網路的連線效能及網路介面熱插拔偵測的功能。
5. 筆記型電腦二台，作業系統分別為 Windows 7 家用白金版與專業版二種。

- **各別網路介面從待機狀態連上網際網路之測試**

此項目是量測在各別網路介面從待機狀態連上網際網路的時間，讓我們了解本研究在各種網路介面單獨的連線效能。測試步驟如下：

1. 首先讓系統進入待機狀態，此時無任何行動設備與 IPHS 連接。
2. 讓未與 IPHS 連線的筆記型電腦先執行 PING Tester 程式並持續 ping 中華電信的 DNS(168.95.1.1)，此時網路是不通的狀態。
3. 讓筆記型電腦的無線網路與 IPHS 連接，驅使 IPHS 回復到啟動狀態開始對外連線。
4. 當筆記型電腦的無線網路連線成功後便開始計時，直到 ping 得到正確的回應為止。



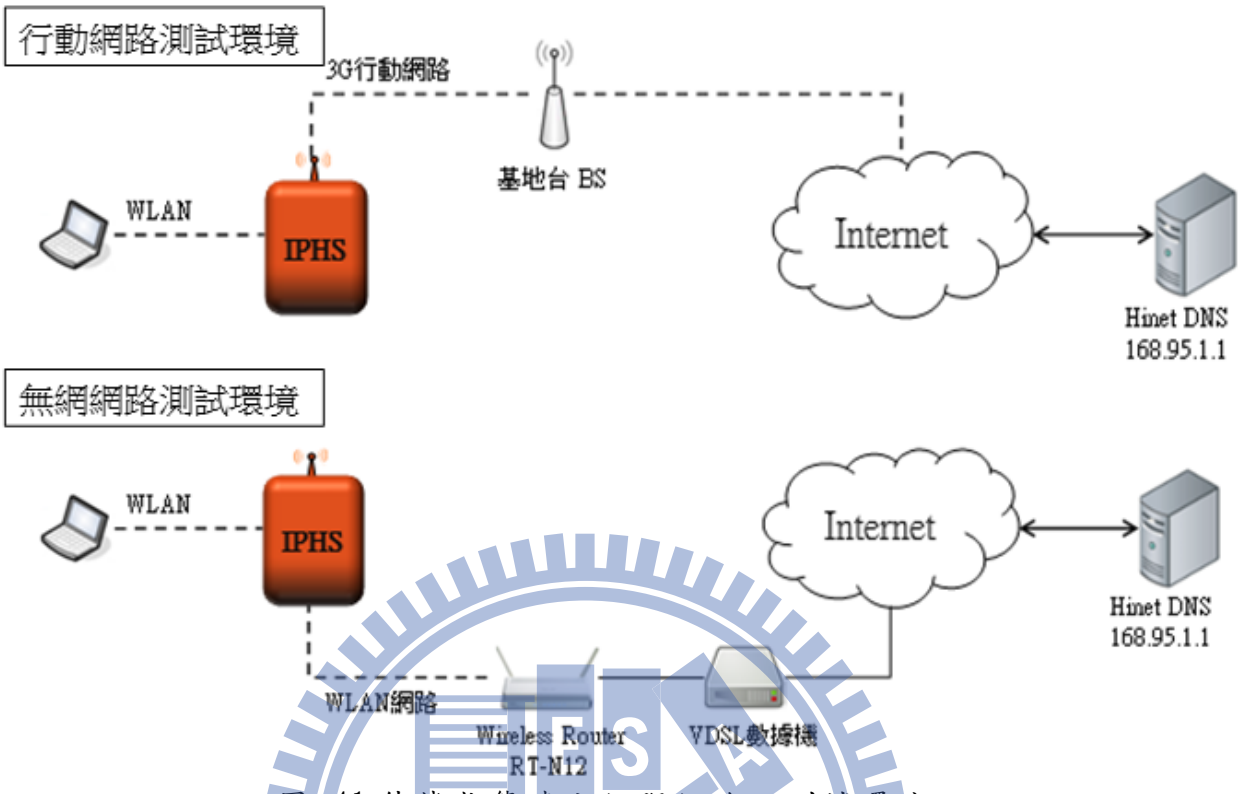


圖 41 待機狀態連上網際網路之測試環境

圖 42 待機狀態連上網際網路之測試流程

每個測試項目依圖 42 的流程，實驗 100 次之後的結果如圖 43 所示。實驗數據顯示有線網路的連線最快且較穩定，行動網路次之，最後是無線區域網路，連線平均速度的快慢依序是有線 DHCP 約 4 秒、有線 PPPoE 約 6 秒、3G 行動網路約 8 秒、無線區域網路約 9 秒。無線區域網路之所以比較慢的原因，查看連線記錄發現經過多次反覆的待機與連線，造成從待機狀態回復的瞬間，掃瞄結果會有不穩定的現象，以及驅動程式內的掃瞄列表過期需要更新較久的時間。另外在測試的過程中因為長時間多次讓筆記型電腦的無線網路不斷地重覆連線和斷線的動作，造成 Windows 7 的網路連線會變得比較不穩定，這時必須把電腦重開機才可以改善這個問題。

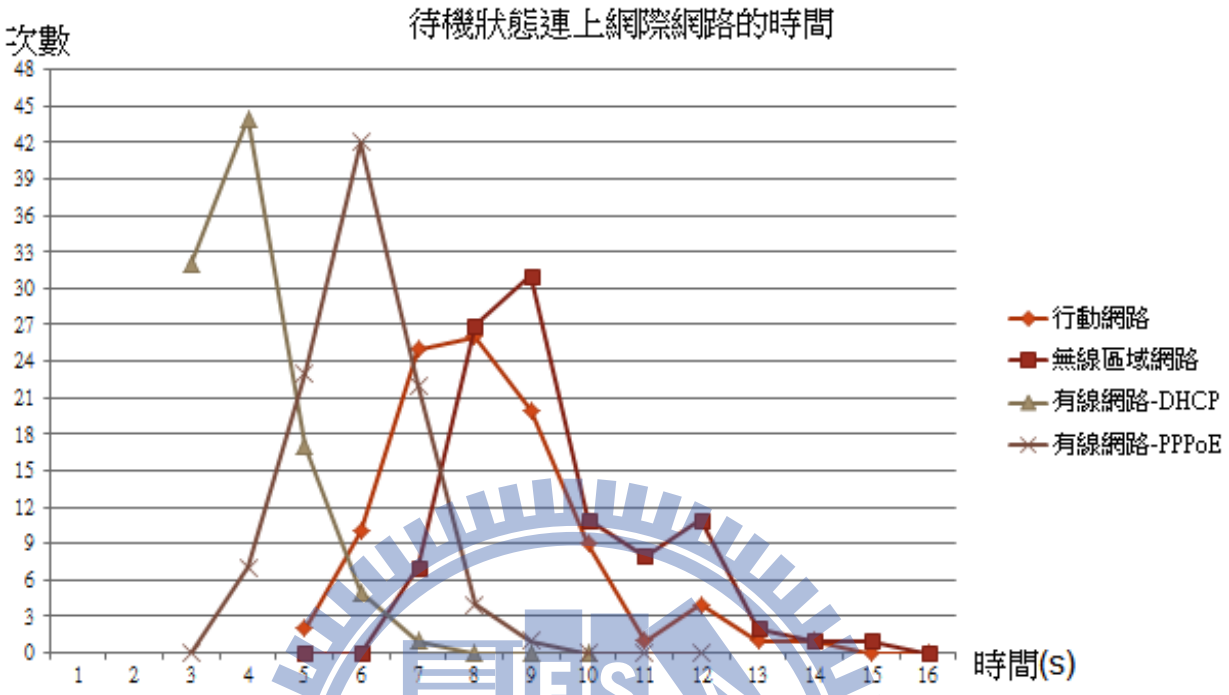


圖 43 待機狀態連線之測試結果

- **行動網路、無線區域網路與有線網路連線切換之測試**

此項目是在驗證網路環境的感知功能與連線效能，以本研究的預設優先次序是有線網路、無線區域網路、3G 行動網路。在現實環境中行動網路除了傳輸速度與費用讓人不甚滿意之外，最大優勢是它的網路服務是無所不在的(ubiquitous)的。所以我們測試的條件設定是 3G 行動網路總是會先連上網際網路，之後會營造環境中無線區域網路的出現與消失，驗證 IPHS 系統是否可以切換至無線區域網路；再來就是接上 USB 介面的乙太網路卡，驗證系統的熱插拔偵測與有線網路的連線功能，同時它也是優先次序最高的網路介面。測試環境設置如圖 44，測試方法如下：

1. 先讓 IPHS 連上 3G 網路再讓電腦的無線網路連上 IPHS 系統，並持續用 Ping Tester 程式 ping 中華電信的 DNS(168.95.1.1)。
2. 無線路由器的電源打開，待路由器上的無線指示燈亮時開始計算時間。
3. 無線路由器的電源關閉，計算切換回 3G 行動網路的時間。
4. 把 USB 介面的乙太網路卡接到 IPHS 系統，等網路卡 Link 燈亮起之後開始計算時間。
5. 移除 USB 介面的乙太網路，計算切換至 3G 行動網路的時間。

6. 關閉行動網路並插拔 USB 介面的乙太網路卡來測試無線網路與有線網路的連線切換能力。

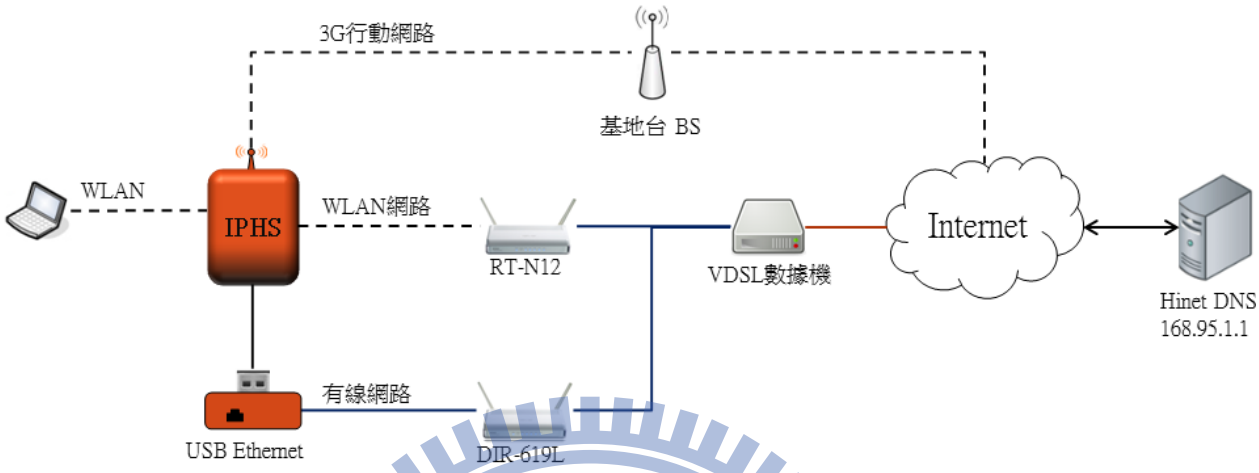


圖 44 行動網路與無線區域網路連線測試環境

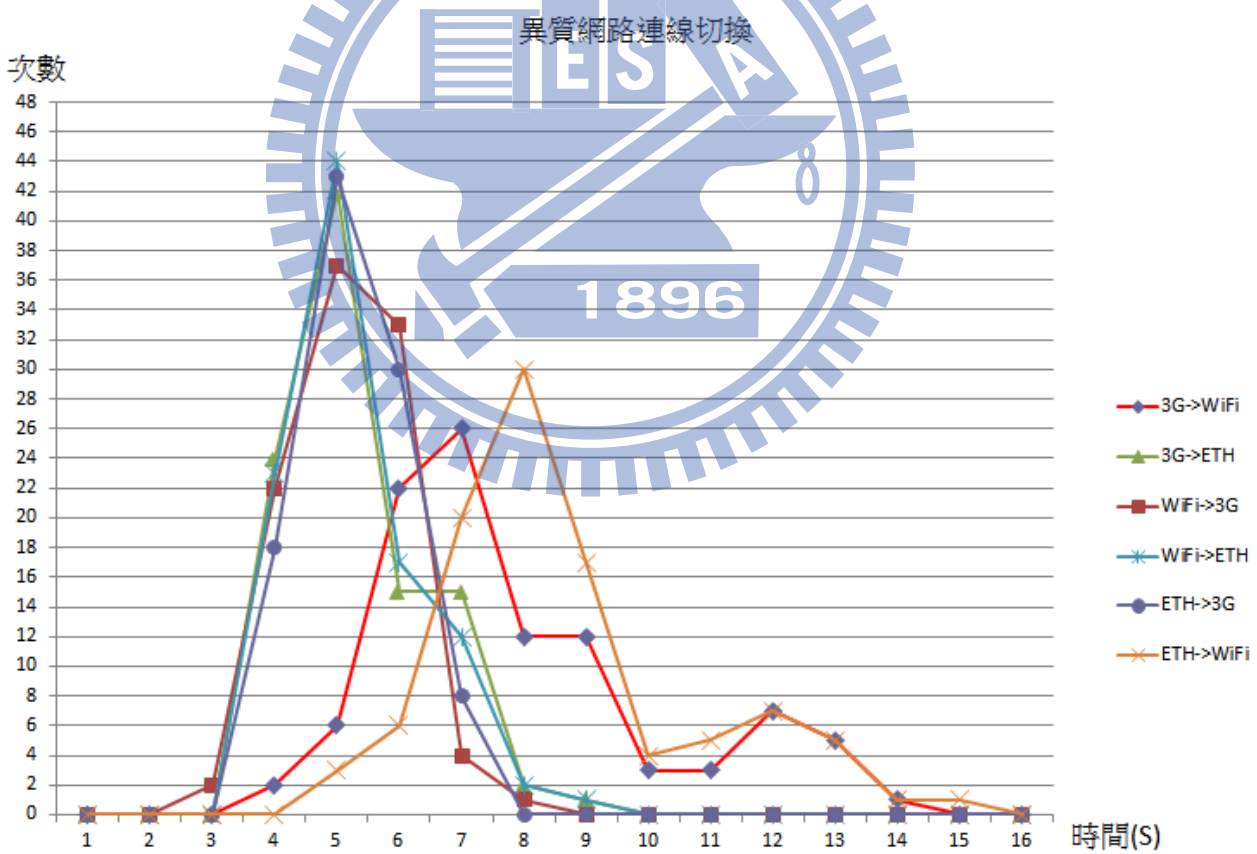


圖 45 靜態的異質網路連線切換之測試結果

每個項目經過 100 次的測試結果如圖 45，實驗數據顯示無論是無線區域網路或者有線乙太網路切換回 3G 行動網路的時間，大部分約略在 5 秒內可以

完成，最慢的部分在 7 秒內都可以完成切換回到 3G 行動網路的動作。這比從待機中狀態的 3G 行動網路的連線時間稍為快一些。其中有線網路的連線切換時間比待機狀態連線切換慢，其原因是多了 USB 驅動程式載入動作與網路裝置的偵測。而無線區域網路由於使用輪詢(polling)的方式來掃瞄，當以 6 秒為間距的情況之下，大致上能在 9 秒內完成連線切換。最差的情況是會經過二次的輪詢掃瞄，所以有少部分會延遲到 12 到 13 秒之後才能完成連線切換的動作。綜合平均測試時間和原來從待機狀態連線的數據相比較之下可以得到相同的使用經驗。

- 移動中無線網路之間的連線切換之測試

此項目在測試 IPHS 系統在移動中行動網路與無線區域網路之間的連線切換效能，系統會依據目前無線網路的訊號強弱來預測是否要啟動連線切換的機制，模擬在現實環境中轉換網路環境的情況提早做連線切換的準備工作，以減少移動時網路斷線的時間。測試行為有二種狀況包含 3G 行動網路與無線區域網路的連線切換與不同無線區域網路之間的連線切換動作。其中要注意的地方是要二台無線路由器設置，配合本系統設定其訊號強度在邊緣的交集區域之處約略控制在 75-85dBm 左右。測試環境設置分別為圖 46 與圖 47。

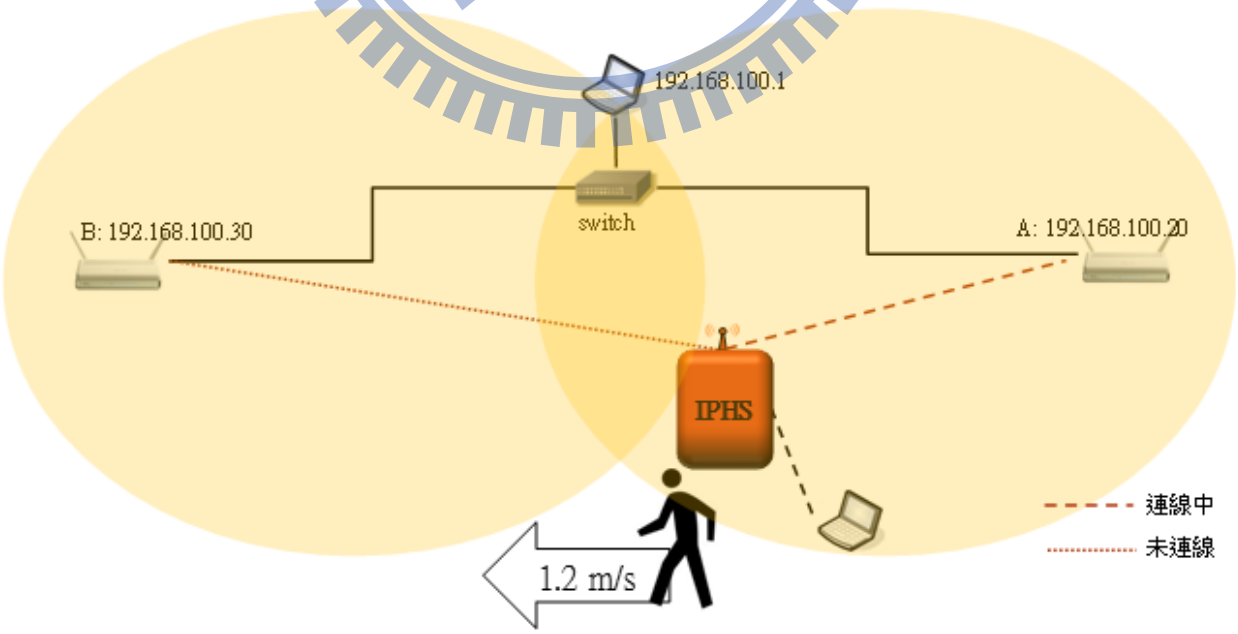


圖 46無線區域網路之間的移動測試

移動切換的測試方法如下說明：

1.先讓IPHS連上其中一台無線路由器，再讓電腦的無線網路連上IPHS系統，並持續用Ping Tester程式ping中華電信的DNS(168.95.1.1)來確認連線正常。

2.IPHS以一般步行的速度(約1.2m/s)移動，遠離目前連線中的無線路由器。

3.計算ping封包在切換的過程中計算總共會失去多少封包。

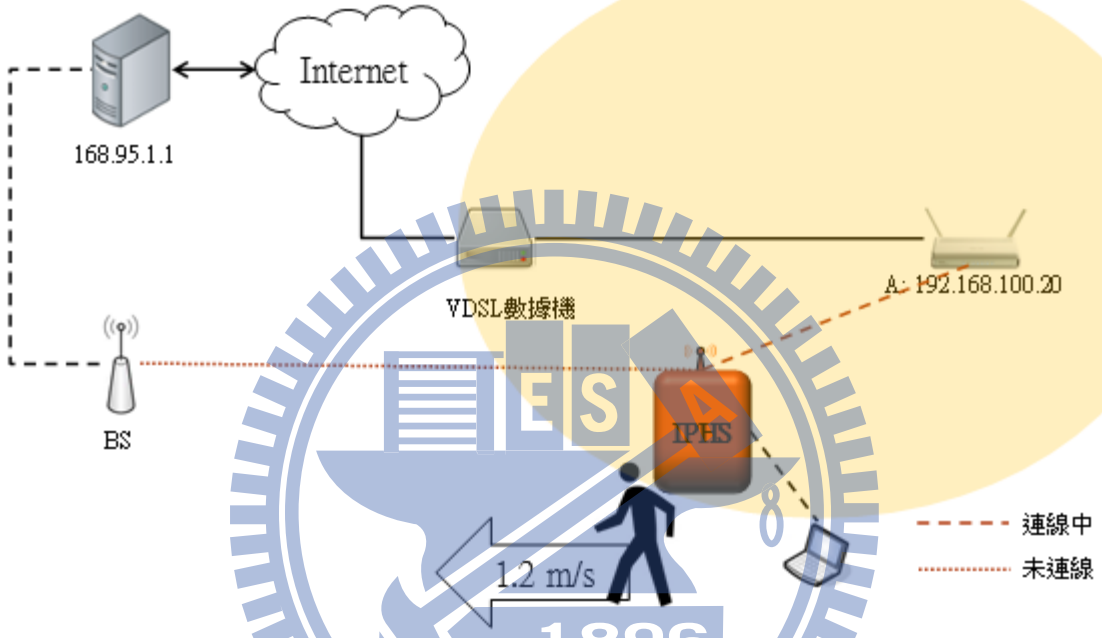


圖 47行動網路與無線區域網路的移動測試

圖 48為每個測試項目分別測試60次的結果，WiFi對WiFi的連線切換測試，封包損失大部分落在15以內。由於無線網路訊號的偵測不太穩定以及移動速度不易控制的影響，造成訊號衰減判斷時間過長，測試結果會有封包損失高達約20多個的情形。這部分的實驗結果是有待加強與改善的。

本系統因為使用者移動造成網路環境會不斷地在改變，在現實的網路環境中根據使用者的經驗，移動過程將會是以行動網路為主的連線方式。IPHS系統在移動過程中如果沒有偵測到無線區域網路的訊號，本系統會保持在3G行動網路的連線狀態。3G行動網路對WiFi的連線切換則表示使用者正停留在一個有提供無線區域網路的環境；而WiFi對3G行動網路的連線切換通常發生在使用者正要離開無線網路服務的使用範圍。因此，本測試結果雖然沒有定點網路切換效率來得好，但綜合使用者行為模式、實際的網路環境與行動軟體的設計不至於造成不良的影響。

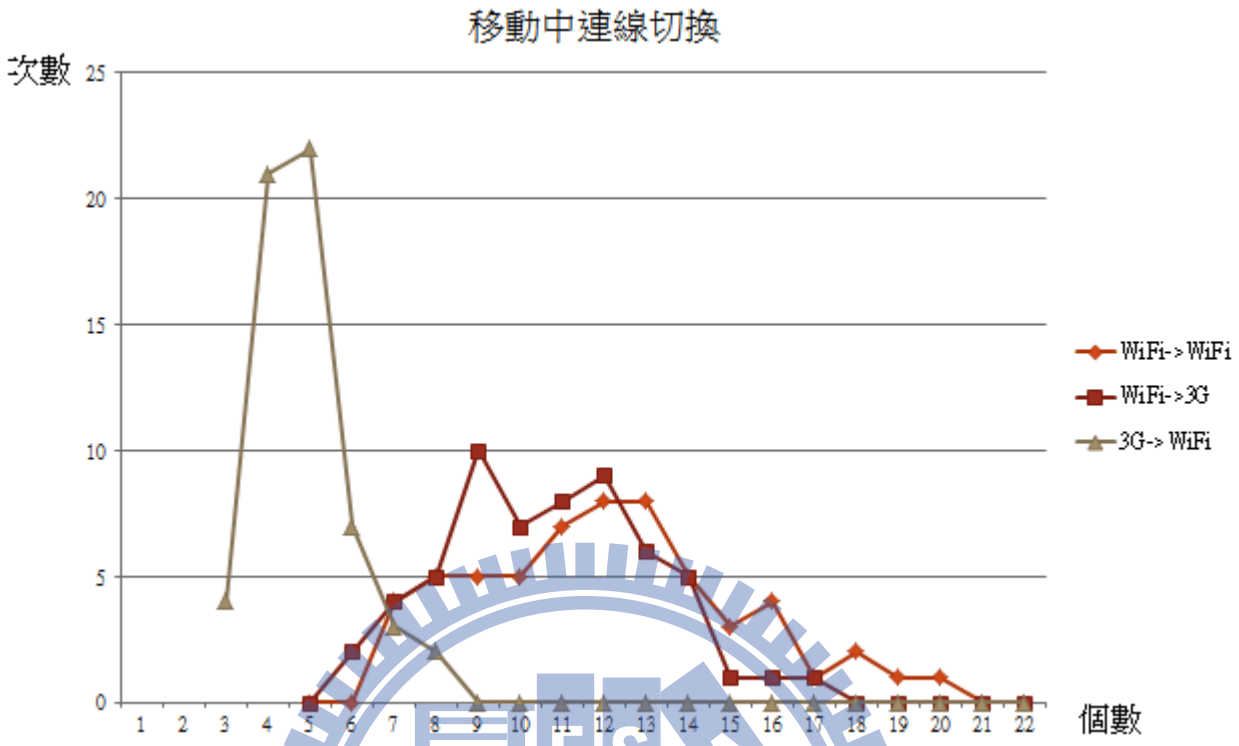


圖 48移動中連線切換之測試結果

5.2.2 熱點自動認證實測結果

此測試項目在驗證本系統熱點自動認證的實作成果，驗證方法是實際拿本系統前往提供無線熱點的公共場所實地測試。待無線網路連線完成後，測試是否可以透過本系統直接連上網際網路，不用再另外手動輸入帳戶資料。每一個地點將反覆測試 20 次其結果如下列表。由以下測試結果得知本系統的自動熱點認證模組可以達到預期目標，可以提供自動化的認證功能，避免行動裝置使用無線熱點時的不便之處。

表 12 交大校園無線熱點測試結果

縣 市	地 點	測試結果
新竹市	工三館 1F	OK
新竹市	工三館 4F	OK
新竹市	工四館 1F	OK

表 13 iTaiwan 無線熱點測試結果

縣 市	地 點	測試結果
新竹市	臺鐵局新竹站候車大廳	OK
新竹市	新竹區監理所新竹市監理站	OK
新竹市	新竹民生路郵局	OK
新竹市	新竹民主路郵局	OK

新竹市	新竹建中郵局	OK
新竹市	交通大學郵局	OK
新竹市	新竹武昌街郵局	OK

表 14 中華電信無線熱點測試結果

縣 市	地 點	測試結果
新竹市	統一超商 7-11 新揚門市	OK
新竹市	三民公園(公共電話亭)	OK
新竹市	統一超商 7-11 公學門市	OK
新竹市	萊爾富 武昌店	OK
新竹市	統一超商-竹運門市	OK

六、結論與未來工作

由於行動通訊技術的蓬勃發展使得人們可以擺脫有線網路的束縛，利用無線網路享受無所不在(ubiquity)網路服務，在任何時間、任意地點都能透過網路取得所需要的資訊或與他人通訊。當然這與具有高速運算能力的行動設備日漸普及且價格便宜的趨勢有關，加上全球社群網路的快速發展與電信產業生態鏈的改變，行動通訊相關的應用已廣泛被大眾所接受。人們對於網際網路的依賴程度逐漸提高，不但可以從網際網路取得豐富又多元的資訊，也可以即時分享個人目前正在發生的人事物，大大地影響人類的生活方式與溝通型態。

為了結合各種異質網路，在不同網路環境之下提供一致性的上網服務，利用本研究的系統可以帶來以下好處：(1)支援性，提供無線區域網路轉接其它異質網路的能力，讓只有基本無線區域網路能力的行動設備，可以接取如3G或有線網路的可能。(2)便利性，支援不同的網路介面，可以適用於大部分的網路環境，例如在家裡可以透過有線網路經由數據機連上網際網路，在戶外移動的過程之中可以使用行動網路；當在有提供熱點服務的環境時，將自動轉換無線熱點服務。網路環境改變的過程中無須為行動設備做任何設定上的改變。(3)資源共享，提供類似行動區域網路的概念，讓行動設備之間可以互相溝通並共享網際網路資源。(4)流量卸載(offload)，當越來越的服務與應用都需要網路頻寬時，基於營運成本和環境的考量，不可能大量建置基地台情況之下，行動網路的速度永遠跟不上使用者的需求。如果利用本系統將可以自動把流量卸載到建置成本較低的無線熱點服務。(5)安全性，經由本系統網路的轉接，可以避免行動裝置直接曝露在公眾網路上，減少被惡意攻擊或入侵的危險。

本研究所提出之系統功能依然有未盡完美之處，未來工作有幾個方面可以進一步加強。由於系統本身即為一個行動路由器設備，在電源管理機制方面希望能提出的較好的解決方案，以增加系統待機與使用時間；對於無線熱點自動認證的支援可以與網路業者合作，導入更多的服務項目。另外IPv6網路服務全球目前正積極地推動和佈署中，未來期望可以提供IPv4與IPv6雙重的連線能力，以因應未來IP網路的需求。

參考文獻

[1] 許健飛,"以Linux嵌入式系統為基礎具多重連結功能之家庭路由器實作",國立中正大學,碩士論文,2005

[2] 趙丁漢,"多網家庭閘道器之設計與實作",國立台灣大學,碩士論文,2006

[3] 許君,"使用者導向之異質行動管理",國立台灣大學,碩士論文,2009

[4] 高榮裕,"多網路介面之網路管理系統與事件通知機制的設計與實作",國立交通大學,碩士論文,2011

[5] Jani Puttonen, Gabor Fèkete, Tapio Väärämäki and Timo Hämäläinen ,"Multiple Interface Management of Multihomed Mobile Hosts in Heterogeneous Wireless Environments",Eighth International Conference on Networks,2009

[6] 鄭宗益,"設計與實作以憑證為認證基礎的無線網路路由器",國立交通大學,碩士論文,2004

[7] 黃威鳴,"無瀏覽器裝置之無網路認證設計",國立交通大學,碩士論文,2011

[8] Mauro Brunato,Danilo Severina," WilmaGate - a new open access gateway for hotspot management",WMASH'05 Proceedings of the 3rd ACM international workshop on Wireless mobile applications and services on WLAN hotspots,2005

[9] 謝志遠," 異質無線網路中根據偏好值之網路選擇機制",國立交通大學,碩士論文,2009

[10]IEEE Standards Association,Available:http://standards.ieee.org [Accessed 2012/04/10]

[11]Wi-Fi Alliance,Available:http://www.wi-fi.org [Accessed 2012/04/10]

[12]RFC2284:"PPP Extensible Authentication Protocol",Available: http://www.ietf.org/rfc/rfc2284.txt [Accessed 2012/04/10]

[13]RFC3748:"Extensible Authentication Protocol",Available: http://www.ietf.org/rfc/rfc3748.txt [Accessed 2012/04/10]

[14]Wireless Broadband Alliance,Available:http://www.wballiance.com

[15]吳宗憲,"整合嵌入式系統與電力線通訊於智慧家庭應用之研究",國立成功大學,碩士論文,2009

[16]HU Hao,GU Xin, "Design and implementation of embedded gateway based on S3C4510B", Computer Engineering and Design, School of Computer Science,Xidian University,Xi’an 710071,China, 2008.

[17]李海芳, 潘志安, 何海鵬, "基於S3C2410的家庭閘道Web伺服器的研究與實現", 電腦開發與應用COMPUTER DEVELOPMENT & APPLICATIONS, 2010年第23卷第1期

[18]林信成,"整合P2P與UPnP內容分享服務之家用多媒體閘道器：設計與實作",國立中央大學,碩士論文,2012

[19]Wan-Ki Park,Chang-Sic Choi, Haeryong Lee, Kwang-Roh Park, "Energy Efficient Home Gateway Based on User Service Traffic in Always-On Home Network Environment", Advances in Electronics and Micro-electronics, 2008. ENICS ’08. International Conference on, On page(s): 121 - 125.

[20]Satish Gupta,"Home Gateway White Paper of Wipro Technologies", broadcastpapers. com, 2004

[21]WPA Supplicant, Available:http://hostap.epitest.fi/wpa_supplicant [Accessed 2012/04/10]

[22]Hostapd,Available:http://hostap.epitest.fi/hostapd [Accessed 2012/04/10]

[23]Busybox,Available:http://www.busybox.net [Accessed 2012/04/11]

[24]Netfilter/iptables,Available:http://www.netfilter.org [Accessed 2012/04/15]

[25]OpenSSL,Available:http://www.openssl.org [Accessed 2012/05/25]

[26]Iproute2,Available:http://en.wikipedia.org/wiki/Iproute2 [Accessed 2012/05/26]

[27]PPP daemon,Available:http://ppp.samba.org [Accessed 2012/05/26]