行政院及所屬各機關出國報告
(出國類別：實習)

實習『WCDMA 無線接取網路優化輔助分析設備』

服務機關：中華電信研究所
出國人 職　　稱：助理研究員
姓　　名：劉威廷
出國地區：香港
出國期間：92 年 10 月 19 日至 92 年 10 月 25 日
報告日期：92 年 11 月 21 日

系統識別號:C09204274

公 務 出 國 報 告 提 要

頁數: 26　含附件: 否

報告名稱:

實習WCDMA無線接取網路優化輔助分析設備

主辦機關:

中華電信研究所

聯絡人／電話:

楊學文／03-4244218

出國人員:

劉威廷　中華電信研究所　無線通信技術研究室　助理研究員

出國類別: 實習

出國地區: 香港

出國期間: 民國 92 年 10 月 19 日 -民國 92 年 10 月 25 日

報告日期: 民國 92 年 11 月 21 日

分類號/目: H6／電信　／

關鍵詞: WCDMA,無線接取,網路,分析設備

內容摘要: 異質無線網路的漫遊對3G開台後與WLAN網路間之整合及應用服務開發有非常密切的關連性。開發應用服務前須對異質無線網路漫遊機制與設備的使用有全盤了解，並對異質網路運作進行必要的測試及分析；以求用戶可便利地接取異質網路所提供的各種服務。由於本公司第三代行動通信系統即將開始營運，再加上目前寬頻網路中WLAN網路的使用量大增且來勢洶洶。因此，此次實習的目的即在於充分了解WCDMA系統無線網路如何在不影響原有架構下進行與WLAN網路間的漫遊，有助於本公司第三代行動網路無縫隙式的與WLAN網路間進行漫遊與在無線通信應用服務方面之發展。此次赴香港的實習課程包含：「Mobile IP Training」及「Heterogeneous Network Integration and Security Consideration for 3G & WLAN Integration」兩部分；除了概述異質網路漫遊之機制與要點，並對異質網路間使用Mobile IP時的架構進行探討，有助於異質網路漫遊規劃與應用服務所需考量的要點。本文內容章節安排如下，首先爲研習目的、研習過程及研習內容，最後爲研習心得及建議。

本文電子檔已上傳至出國報告資訊網

赴香港實習『WCDMA 無線接取網路優化輔助分析設備』出國報告

摘　要

異質無線網路的漫遊對3G開台後與WLAN網路間之整合及應用服務開發有非常密切的關連性。開發應用服務前須對異質無線網路漫遊機制與設備的使用有全盤了解，並對異質網路運作進行必要的測試及分析；以求用戶可便利地接取異質網路所提供的各種服務。

由於本公司第三代行動通信系統即將開始營運，再加上目前寬頻網路中WLAN網路的使用量大增且來勢洶洶。因此，此次實習的目的即在於充分了解WCDMA系統無線網路如何在不影響原有架構下進行與WLAN網路間的漫遊，有助於本公司第三代行動網路無縫隙式的與WLAN網路間進行漫遊與在無線通信應用服務方面之發展。

此次赴香港的實習課程包含：「Mobile IP Training」及「Heterogeneous Network Integration and Security Consideration for 3G & WLAN Integration」兩部分；除了概述異質網路漫遊之機制與要點，並對異質網路間使用Mobile IP時的架構進行探討，有助於異質網路漫遊規劃與應用服務所需考量的要點。本文內容章節安排如下，首先為研習目的、研習過程及研習內容，最後為研習心得及建議。

目　　錄

1. 實習目的

本公司第三代行動通信系統即將開始營運，再加上目前寬頻網路中WLAN網路的使用者激增且來勢洶洶；因此，此次實習的目的即在於充分了解WCDMA系統無線網路如何在不影響原有架構下進行與WLAN網路間的漫遊，有助於本公司第三代行動網路無間隙的與WLAN網路間漫遊機制與提供無線通信應用服務之發展。

2. 實習過程及內容

職於民國92年10月19日搭乘長榮航空班機由桃園中正機場起飛，於香港當地時間10月19日到達香港赤臘角國際機場，次日前往京華飯店，研習時間從10月20日至10月24日。實習過程及課程內容如下：

日　期	研習課程及工作記要
92.10.19-92.10.19	行程，桃園中正機場→香港
92.10.20-92.10.24	(1) Mobile IP Training (2) Heterogeneous Network Integration and Security Consideration for 3G & WLAN Integration
92.10.25-92.10.25	回程，香港→桃園中正機場

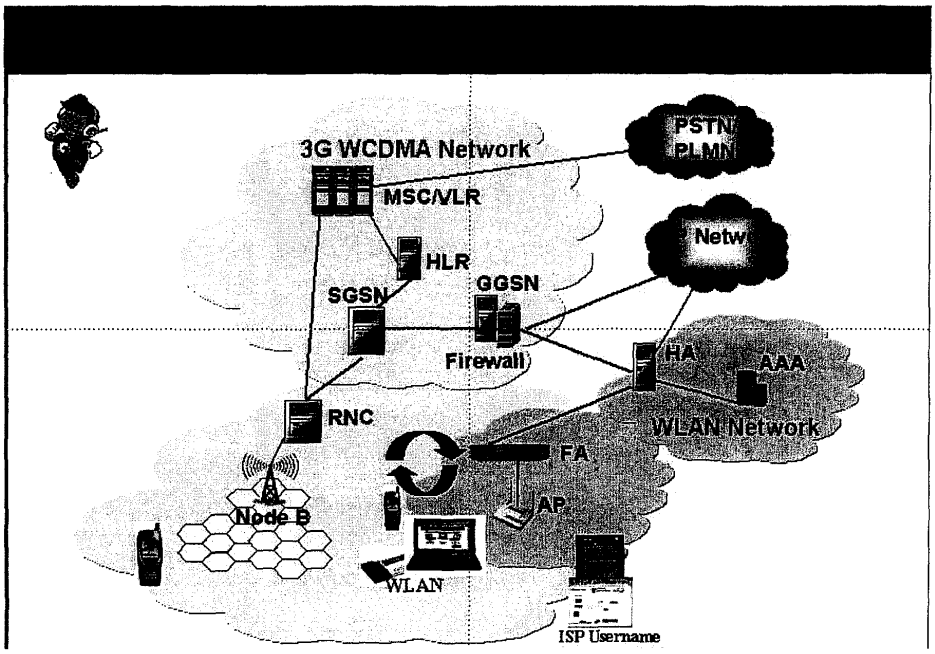
研習課程包含：「Mobile IP Training」及「Heterogeneous Network Integration and Security Consideration for 3G & WLAN Integration」兩部分。除了概述異質網路漫遊之機制與要點，並對異質網路間使用Mobile IP時的架構進行探討，有助於異質網路漫遊規劃與應用服務所需考量的要點。研習過程主要利用投影片進行講解，同時利用Notebook架設成FA

(Foreign Agent，境外代理伺服器)與HA (Home Agent，境內代理伺服器)。由於本公司與國內目前仍無異質網路和3G整合的商業營運，因此如何在此次的設備與軟體採買後，進行首批的網路整合漫遊與機制十分重要。本文將提出WCDMA無線接取網路優化輔助分析設備研習成果報告，以提供本公司在異質網路整合應用與雙網計畫中的規劃做為參考。

3. 異質網路漫遊機制

3.1 前言

本公司 3G WCDMA 系統即將正式開始營運，而在寬頻網路中，WLAN 網路也已儼然成為大量使用的無線網路之一。以涵蓋區域而言，3G 毫無疑問的遠大於 WLAN 網路，且綿密程度亦可達 2G 網路之程度，然而在網路的傳輸速度與價格方面，卻又以 WLAN 佔較大的優勢，因此如何妥善的增進兩者互補的關係，而非互相牽制，進而營造出雙贏的局面，是目前的重要議題和方向。行政院和相關研究人員所提出與共同合作的『雙網』計畫所指的正是 3G 與 WLAN 網路，目前也由業界與研究單位積極的研究與進行中，為趕上這股潮流與進行相關的規劃和評估，異質網路漫遊的機制與實現的設備有必要進行先期的瞭解與測試。異質網路的整體架構圖如圖(1)所示，包含 3G WCDMA 網路與 WLAN 網路，本報告討論的重點將著重於網路漫遊時所採用的規約與漫遊時的整體架構研究，以供雙網漫遊時的參考使用。



圖(1) 異質網路架構示意圖

3.2 欣建通之異質網路漫遊時使用的主要規約

有別於一般的 Internet IP 網路，當使用者在異質網路漫遊時所使用的機制除了原本的 IP 架構之外，需使用到定義於 IETF RFC 規約中之 Mobile IP 的型式。在 RFC 中與 Mobile IP 相關的規約包括 3344，3519，3012，3024 等規約，欣建通公司也是依據以上所提之規約進行軟體設計與建立整體漫遊的機制。

接下來的章節中將根據 Mobile IP 的主要觀念與特性、名詞用語、提供的服務與操作的機制進行討論。

3.2.1 Mobile IP 的主要觀念與特性

Mobile IP 定義來自於 IETF RFC3220 的文件中，最主要的原意在於讓一個 IPv4 的用戶節點(Node or Host) 可以使用一個固定的 IP 位址，然後讓這個節點可以在持續使用這個固定 IP 位址的情況下，改變連接到 Internet 的位址，而且在改變連接位置的過程中，不會影響節點上其他正在執行的 TCP 連接的使用。而 IP 的主要的目的原本即是如何將 Routing 正確繞至節點和在傳輸與應用層的終端節點之 ID 驗證，因此 Mobile IP 亦將維持原有 IP 的功能達到在移動中的使用。且 Mobile IP 並不會在原有 IP 規約上加諸限制，換言之在鏈結層（link layer）無須再加上額外的變動，即使網路上其他地方使用的是一般 IP，而非 Mobile IP，依然可以正常通行與工作。

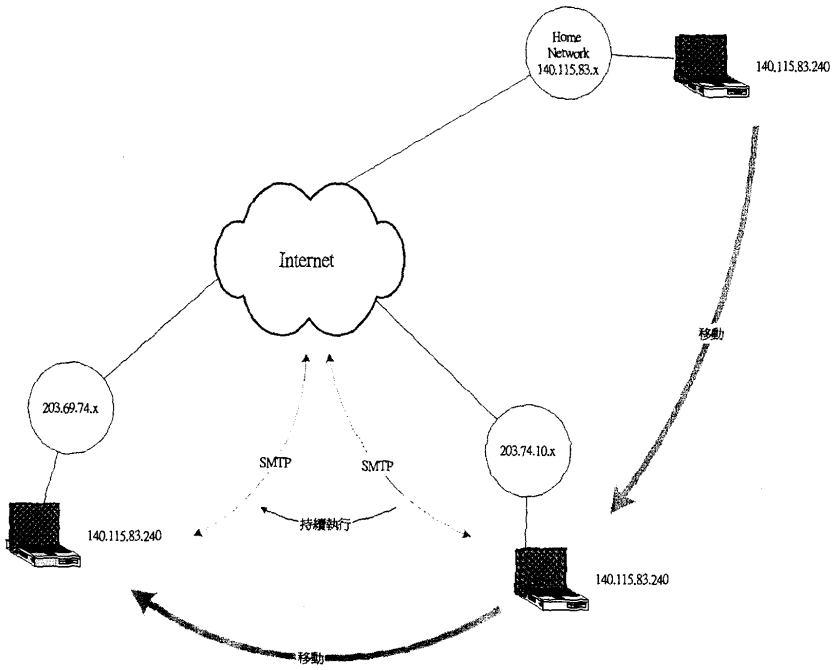


圖 (2) Mobile IP 的示意圖

如圖(2)，舉例而言， 某一個節點的 IP 位址為 140.115.83.240 ，屬於一個 140.115.83.x 的網段。這個節點是一個 Notebook 的行動用戶，使用者會帶著這個 Notebook 到客戶的公司去進行簡報，當用戶把 Notebook 帶到客戶的公司去後，客戶公司的內部網路可能為 203.74.10.x ，而 Mobile IP 的用戶只要將 Notebook 接上當時的區域網路之後，可以同樣的使用自己原有的 IP 位址 140.115.83.240 ，透過客戶的企業內部網段 203.74.10.x ，連接上 Internet 。

節點原本所屬的網路下，可能有一些 Server 所提供的服務，會針對內部用戶鎖定其 IP 位址來提供服務，例如像 SMTP 的服務。這些服務，儘管節點已經移動到 Internet 上面的其他網段上，因為節點使用的 IP 還是固定為 140.115.83.240 ，因此內部的 SMTP 還是可以針對這個節點用戶提供服務。

假設，剛好節點用戶所到的客戶公司有兩棟大樓，而且有另一個獨自的網段 203.69.73.x ，且兩個大樓各自的網段都是使用 WLAN 的設備，而節點用戶自己的 notebook 也使用 WLAN 網卡與該企業的 WLAN 連接。當節點用戶在 203.74.10.x 網段中執行了一個 SMTP 進行郵件傳送，傳送一個很大容量的郵件，需要一段很長的時間，而此時節點用戶因為必須馬上去另一棟大樓，而又不希望中斷 SMTP 的傳送，此時節點用戶只要帶著 Notebook 馬上移動到第二棟大樓的 203.69.73.x 的網段中， Mobile IP 的協定會讓節點用戶持續使用固定的 140.115.83.240 的 IP ，同時也不會讓這個已經啟動的 SMTP 連接中斷。

當然，要達到這樣個功能，必須在節點、原始網段、外部網段中，增加一些額外的設備或者 Server 模組，才能完成 Mobile IP 的服務提供。

3.2.2 Mobile IP 的名詞用語

Mobile Node – (MN)

行動節點，一部 PC 、PDA 或手機等的 TCP/IP 節點，這個節點可以隨時改變它所連結上網的網路位置，而在改變不同的網路連結過程中，行動節點本身所使用的 IP 的並不會改變；移動的過程中，網際網路上其他與行動節點通訊的任何網路節點，都不會因為行動節點改變網路連結位置而造成通訊中斷。

Home Address

原始位址或內網位址，行動節點在移動過程中所持續使用的固定 IP 位址，這個 IP 在行動節點的移動漫遊過程中不會更改。行動節點每次執行漫遊行程，不一定需要使用同一個固定 IP，但是同一個漫遊行程（Session）中會是固定的。

Home Network

原始網段，原始位址所屬的網路區段(IP Subnet)。這個網段可以是一個虛擬的，所謂的虛擬是指這個網段實際上並沒有一個實體的區域網路存在，而只是透過 Router (此時就是 Home Agent) 設備所維護管理，這個虛擬網段唯一的進入點就是 Router 設備的 IP 接入口。所有要傳遞給行動節點的資料，都會透過標準的 IPv4 封包繞路機制傳遞到這個原始網段。或更簡潔的描述為一 IP 位址前三碼與 MN 之原始位址相同之網路皆為原始網段。

Foreign Network

外網，home network 以外的任何標準 IPv4 網域，行動節點會到這些外網進行連結，透過外網來使用行動節點的原始位址 IP 。

Home Agent – (HA)

境內代理伺服器或稱為內網代理器，存在於原始網段的一個 Router (路由器) ，負責將原本要傳遞給行動節點的 TCP/IP 訊息透過通道技術 (Tunnel) 傳遞給身處於原始網路以外其他網段的行動節點。

Foreign Agent – (FA)

境外代理伺服器或外網代理器，存在於行動節點當時所在網段下的一個 Router (路由器) ，負責將來自內網代理器傳遞給行動節點的 TCP/IP 訊息解通道(de-tunnel)之後轉送給行動節點，也負責提供行動節點對外的路徑處理。

Mobility Agent

移動代理器，泛指內網代理器以及外網代理器。

Agent Advertisement(代理器廣播)

從 IPv4 中的路由器網播訊息的格式擴充而來，用來讓代理器針對其所服務的網段廣播訊息，行動節點在網段上收到這些廣播訊息之後可以用來判斷，行動節點自己目前所在的位置，以及有哪些代理器可以提供服務。

Care-of Address – COA (看管位址)

看管位址是資料從內網經通道技術往移動節點傳遞時，通道的終點。 在這個通訊協定中，看管位址有兩種，外網代理器看管位址 "FA-COA: foreign agent care-of address" (就是行動節點當時所在的外網代理程式的 IP 位址)與聯合看管位址 "CCOA: co-located care-of address" (就是行動節點，在外網時指定給自己網路介面的當地 IP 位址)，在 CCOA 的架構中，MN 必須自行處理 Tunnel 的 encapsulate 和 de-capsulate，且無須 FA 的存在。唯此次欣建通公司提供的架構為全面 FA-COA 的架構，無論是在 3G 或 WLAN 的網路中均如此。

Correspondent Node – (CN)

與行動節點通訊的另一個 node ，這個節點可以是一個傳統的 IPv4 節點，也可以是一個 Mobile IP 的行動節點。

Link-Layer

資料鏈結層，網路層以下的硬體網路設備與媒體。例如 Ethernet 就是一種 Link ，而 GPRS 也是一種 Link ，這兩種 Link 都可以讓 TCP/IP 這種邏輯網路層的網路在上面執行。

Link-Layer Address

在實體層網路 Link 中用來識別節點身份的位址，通常就是 Media Access Control (MAC) address 資料鏈結層位址，如 MAC 硬體網路位址。

Mobility Binding

移動繫結，原始位址與其目前所在的看管位址的紀錄，同時維護這個繫結剩餘的持續時間資訊。

RADIUS

符合標準 RFC2138, RFC2865 的 AAA (Authentication, Authorization, Accounting) 伺服器，可以提供絕大部分 ISP 實務應用時的 AAA 處理。

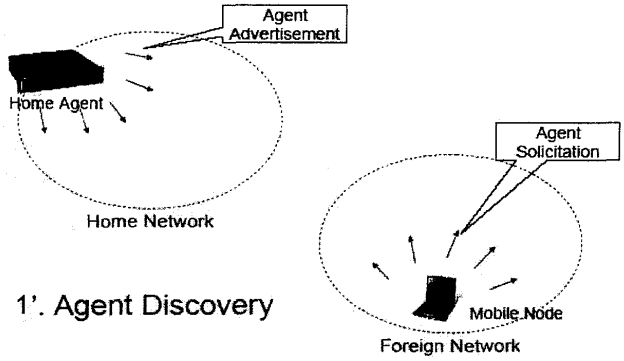
3.2.3 Mobil IP 的運作方式

整個 Mobile IP 的主要理論依據以及標準，來自 IETF RFC3220 的文件，Mobile IP 的執行運作過程，主要可以分成三個階段：

① ***Agent Discovery*** – 代理器尋找階段

如圖(3)，代理器 **HA** 與 **FA** 會透過 ICMP Agent Discovery 訊息，於存在的實體層網路上廣播代理器存在的事實，同時也透過這些廣播訊息通知當時在這些實體層網路上的 **MN** ， **MN** 可以由這些訊息知道許多相關訊息。如果 **MN** 到了一個外網中，卻沒有收到來自代理器廣播的訊息，**MN** 可以主動發出 ICMP Agent Solicitation 訊息來找尋代理器的存在。

代理器尋找的處理過程，是擴充自 ICMP Router Discovery Protocol (**IRDP**) 的處理邏輯，因此整個處理過程與 Router Discovery 的概念完全相同，而 Mobile IP 的 Agent Discovery 只是在 **IRDP** 的 Advertisement 以及 Solicitation 訊息中加上有關 Mobile IP 專用的擴充欄位，用來傳遞一些相關的訊息，例如 **FA** 可以把自己的 Foreign Agent COA 透過廣播訊息，告訴在這個網段上的 **MN** ，**MN** 也可以從收到的廣播訊息中知道 **FA** 的實體層位址，提供 **MN** 與 **FA** 之間的直接資料報傳遞。



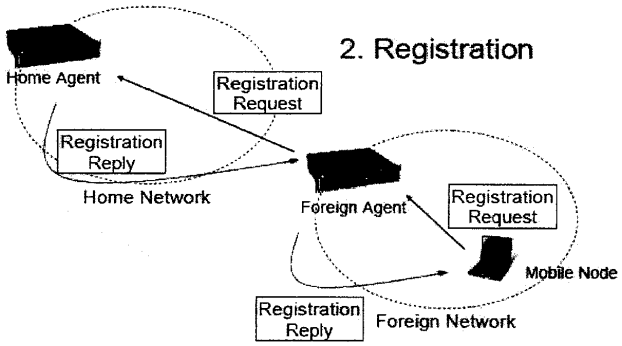
圖(3) 代理器尋找階段示意圖

② ***Registration*** – Mobile IP 註冊階段

如圖(4)，**MN** 在移動到某一個新的網路上的時候，透過 Agent Discovery 的處理知道其目前所在網段上的代理器資訊，接著就必須對當時網段上的代理器進行 Mobile IP 註冊的要求動作。

註冊要求的訊息，會由 **MN** 以 UDP 封包傳遞，**FA** 與 **HA** 會以 UDP 的 Port （如 port 434）接收來自 **MN** 的註冊要求訊息 Registration Request ，而 **FA** 或 **HA** 在完成對 **MN** 所提出的註冊要求處理之後，會回應給 **MN** 一個 Registration Reply 訊息，通知 **MN** 註冊要求的處理結果。

完成註冊處理之後，**HA** 就會知道 **MN** 目前所在位置的相關資訊，而針對 **MN** 提供 Tunnel 的通道技術繞路服務。



圖(4) ***Registration*** 示意圖

③ Data Routing – 繞路階段

當 **HA** 透過 Registration 的過程知道了 **MN** 目前的 COA ，所有在 Internet 上面的 **CN** 要傳遞給 **MN** 的 IP 封包都會先傳遞到 Home Network 上，而 Home Network 上面的 **HA** 會代替 **MN** 將些封包收下，然後以通道技術用另一層 IP 標頭把這個收到的 IP 封包完完整整的包裝起來，這個外層包裝的 IP 標頭，目的位址會填入此時 **MN** 所註冊的 COA 。因此，經過通道包裝過的 IP 封包，就會透過傳統的 IP 封包繞路技術傳遞到 IP 為這個 COA 的節點上，在 Foreign Agent COA 的情形下，這個節點就是 **FA** ；在 Co-Located COA 的情形下，這個節點就是 **MN** 本身。

如果 **MN** 回到了 Home Network ， **MN** 對 **HA** 所傳送的 Registration Request 最主要的目的是在於通知 **HA** ，MN 已經回到 Home Network 而不需要 Tunnel 的繞路服務。因此，通常 **MN** 在 Home network 下所執行的 Registration Request 也會叫做 deregistration ，這個動作會讓 **HA** 把 **MN** 的移動繫結給清除掉，也就是說不在提供 Tunnel 的繞路服務給 **MN** ，而 **MN** 則以傳統的 IPv4 的繞路方式進行。

(A) Mobile IP 繞路處理

(1) MN 在 Home Network 時 (如圖 (5)所示)

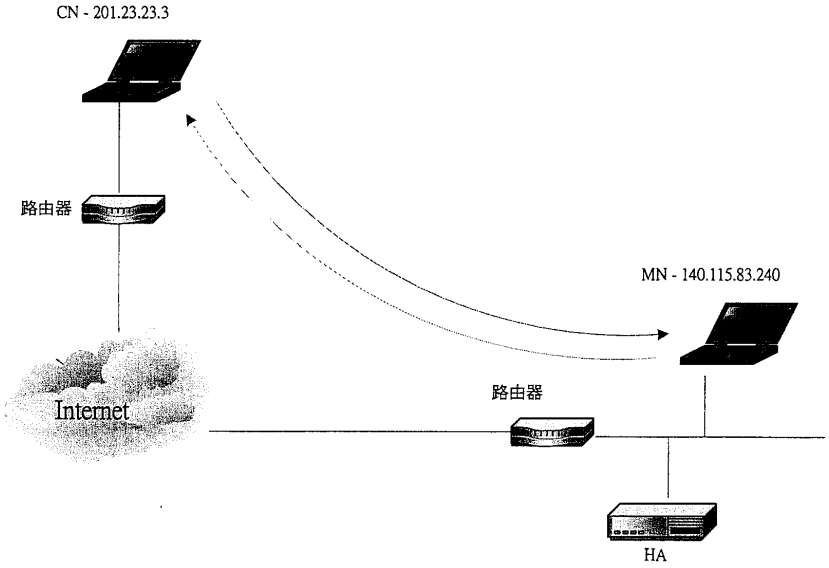


圖 (5) MN 在 Home Network 時的示意圖

當 **MN** 在 Home Network 下啟動 Mobile IP 的 Client 軟體，或者從外網漫遊回到內網 Home Network 的時候，**MN** 對內網上面的 HA 會執行 deregistration 的處理，由 **MN** 對 **HA** 的 UDP 特定（如 434） Port 傳送一個 Mobile IP 的 Registration Request 訊息，**HA** 在收到這個註冊要求訊息之後，會將 **HA** 目前 **MN** 所要求使用的內網位址 IP 還存在的所有移動繫結紀錄給清除掉，也就是這個 IP 位址目前所紀錄的 Tunnel 服務全部取消掉，如果之前確實存在著 Tunnel (表示 MN 剛剛是從外網漫遊回內網) ，**HA** 還必須同時取消掉其網路介面為 **MN** 的內網 IP 位址所進行的 Proxy ARP 與 Gratuitous ARP 的動作，讓 **MN** 可以在 Home Network 中取得這個 IP 的使用權。

回到 Home Network 的 **MN** ，並不需要 **HA** 為其提供任何輔助，只需要透過 Home Network 當時的網路環境，如 Router 的

設定、DNS 的設定等等，就可以直接以標準的 IPv4 協定讓 **MN** 與 Internet 上的任何 **CN** 進行通訊。

當然，**HA** 設備有時會與 Router 設備結合在一起，這個時候 Home Network 下的 default Router 的功能會直接由 **HA** 來執行取代。

(2) MN 在 Foreign Network 的時候

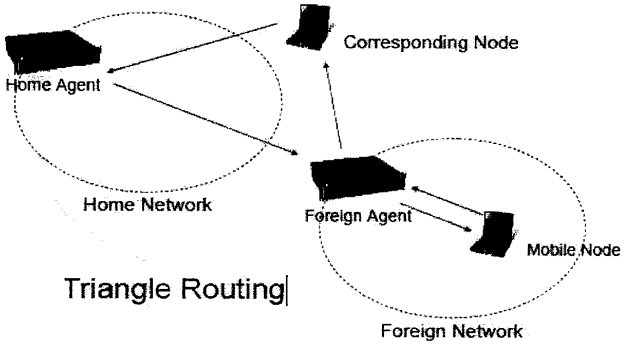


圖 (6) Triangle Routing 的示意圖

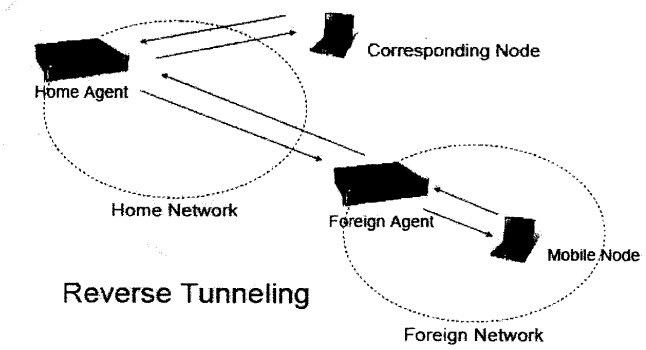


圖 (7) Reverse Tunneling 的示意圖

當 **MN** 在外網的時候，同樣的在完成 Registration 的程序之後，**MN** 與 **CN** 的封包繞路方式有兩種: Triangle Routing、Reverse Tunnel 兩種。

(a) Triangle Routing

如圖(6)，Triangle Routing 的方式下，**MN** 傳遞給 **CN** 的所有 IP 封包，會透過 **MN** 自己或者 **FA** 直接以外網當時的網路環境傳遞出去。**MN** 傳遞給 **CN** 的 IP 封包，會如同 **MN** 在 Home Network 下面時，填寫標準 IPv4 的標頭訊息，然後透過外網當地的 Router 將這個 IP 封包傳遞出去。這是因為，IPv4 的規定中，IP 封包的繞路是根據 IP 標頭的目的地位址以及目的網路遮罩，而不會因為來源處的 IP 位址欄而有所影響。

CN 要傳遞給 **MN** 的 IP 封包，則是會以標準的 IPv4 封包繞路傳遞到 Home Network 網段中，此時因為 **MN** 完成 Registration 之後， **HA** 為 **MN** 所使用的 IP 位址完成一個移動繫結，同時也會在這個 Home Network 網段上，透過 Proxy ARP 以及 Gratuitous ARP 的功能，讓 **HA** 的網路介面可透過標準 TCP/IP 的協定，替 MN 把這些 IP 封包擷取下來。(換句話說，**HA** 這時其實就是代替 **MN** 在 Home Network 中使用 **MN** 的原始 IP 來運作)

HA 收到之後，會利用 Tunnel 技術，把 **CN** 傳遞給 **MN** 的 IP 封包完完整整的包裝在另一個 IP 封包裡面，稱之為 IP-in-IP 。這個包裝的外層 IP 標頭，可以讓這個 IP 封包透過標準的 IPv4 繞路機制，在 Internet 上面把這個封包傳遞到 **MN** 在 Registration 所登記的 COA 節點上。如果 **MN** 當時所在的外網有 **FA** 而且 **MN** 是透過 **FA** 代為對 **HA** 進行 Registration 時， 這時的 COA 叫做 Foreign Agent COA ，其實就是 **FA** 的網路介面 IP 。如果 **MN** 當時所在的外網並沒有 **FA** ，**MN** 會先透過當時外網的 DHCP 服務取得外網中可用的 IP 位址，當作 Co-located COA ，這個 COA 其實也就是 **MN**

的另一個 IP 位址，這個 IP 位址可以提供 **MN** 在外網中以傳統標準的 IPv4 協定連接上 Internet 。

HA 以 COA 作為外層 Tunnel 封裝時 IP 封包標頭的目的 IP 欄位，讓這個經過 Tunnel 封裝的 IP-in-IP 封包可以透過 Internet 傳遞到使用 COA 這個 IP 位址的節點上(**FA** 或 **MN**)。收到這個 Tunnel 封包的節點，會把外層 Tunnel 的 IP 標頭取消掉，然後把內部包裝的封包完完整整的取出來，然後傳遞給 **MN** 。

如果是 **FA** 收到 **HA** 來的 Tunnel 封包，在解除外層包裝之後，**FA** 會直接透過實體網路層的通訊協定，把解出來的封包傳遞 **MN**；如果是 **MN** 自己收到 **HA** 來的 Tunnel 封包，那麼解除外層的 Tunnel 封裝之後，MN 就可以直接取得這個原來的 IP 封包。

(b) Reverse Tunnel

如圖(7)，在 Reverse Tunnel 的方式下，**CN** 要傳送給 **MN** 的 IP 封包與 Triangle Routing 方式的做法相同。唯一不同的是，**MN** 要傳送給 **CN** 的封包，會同樣以 Tunnel 的方式進行封裝，而這一次封裝的方向是從 **MN**(或 **FA**) 到 **HA** ，因此叫做 Reverse Tunnel。

如果 **MN** 當時是直接與 **HA** 進行通連，那麼這個 Tunnel 的封裝執行工作就是由 **MN** 自己處理，如果 **MN** 是透過 **FA** 與 **HA** 進行通連，那麼 **MN** 會把原始的 IP 封包，透過實體網路層的通訊協定，先傳遞給 **FA**，然後由 **FA** 進行 Tunnel 的封裝與傳遞的處理工作。

HA 在收到這個 Tunnel 封包之後，同樣的會截除外層 Tunnel 封裝的 IP 標頭，將原始的 IP 封包取出，然後透過 Home Network 的網路環境，以標準的 IPv4 繞路機制傳遞給 **CN**。

(B) Foreign Agent COA 與 Co-located COA

從 Mobile IP 的運作原理來看，**MN** 本身並不一定需要有 **FA** 才可以對 **HA** 取得 Mobile IP 的服務，可是因為某些因素，使用 Foreign Agent 有時是必須的：

許多 **MN** 可以同時使用同一個 Foreign Agent COA。在現在 IP 位址不足的趨勢下，許多 ISP 業者在提供網際網路使用服務時，都會考慮 IP 位址的問題。因為 **FA** 與 **MN** 之間是可以直接透過實體網路層進行通訊，因此 **MN** 到外網的時候，並不需要去佔用一個 IP 位址，而 **FA** 只要使用一個 Public IP 位址就可以提供眾多的 **MN** 共同使用。

MN 自己執行 Tunnel 處理時，會耗費系統資源。 **MN** 如果不透過 **FA** 來對 **HA** 使用 Mobile IP 服務，那麼 **MN** 就必須處理與 **HA** 之間的 Tunnel 通道處理工作，這樣會讓 **MN** 自己造成執行上的效能負擔。

因此，在實際的建置與應用上，是否需要使用 **FA** 是可以根據不同的環境條件進行配置的，此次欣建通公司提供的為全部具備 **FA** 的架構。

(C) seamless 的漫遊

RFC 3220 在定義 Mobile IP 時就提到，主要的應用環境是針對越來越受歡迎的無線通訊網路，為了配合無線通訊網路應用的先天上頻寬都較低的特性，因此特別著重在 Registration 處理過程中 UDP 訊息格式的設計。

Mobile IP 把 Registration 的訊息設計的很精簡，讓 Registration 的訊息可以很快的在網路上傳遞，同時讓 Registration 的處理動作可以在非常短的時間之內完成。

RFC 3220 的標準，會讓 **FA** 與 **HA** 在一秒鐘之內，發送出三個 ICMP Agent Advertisement 訊息，而 **MN** 在收到這些訊息之後，也可以在最短的時間內把 Registration 的訊息處理完成。通常在網路品質良好的情況下，當 **MN** 移動到另一個網路上去時，可以在 1－2 秒鐘之內，完成 Registration 的處理。

如果這時候 **MN** 與 **CN** 之間的通訊應用是採用 TCP 的方式，透過 TCP 原本的 Acknowledgement 的機制，就可以確保整個 TCP 的通訊不會中斷。

主要的原因在於 **MN** 使用了一個固定的 IP ，對於 **CN** 的 TCP/IP 通訊模組來講，他並不知道 **MN** 目前到底是否在 Home Network 或者在其他外網。**CN** 傳遞給 **HA** 的封包仍舊會正常的到達 Home Network 然後由 **HA** 以 Tunnel 封裝技術，傳遞給 **MN** 。 TCP 通訊本身具有 Acknowledgement 與 Sliding Window 的逾時重送機制，會在通訊對方沒有回應前一個 TCP 封包的 Acknowledgement 的時候，重新傳送一次之前的封包。這個動作會根據當時的網路上封包傳遞的統計時間進行分析而重複執行數次，有時也可以透過參數來調整這些時間參數。一般情況下，一個 TCP 通連通常都可以承受 10 秒鐘以內的中斷時間。

因此，在 **MN** 漫遊的過程中，**MN** 會持續對 **HA** 執行 Registration 的處理，而 **HA** 在收到 **HA** 的 Registration 要求之後，會將 **MN** 的移動繫結紀錄重新登記為目前 **MN** 最新的 COA ，然後讓 **HA** 的 Tunnel 處理模組馬上把接下來的 IP 封包都透過 Tunnel 傳遞到最新的 COA 位址上。只要 HA 在處理這個接換動作的時間可以在數秒之內完成，就

算 **CN** 傳遞給 **MN** 的封包因為傳遞到舊的 COA 去而遺失的時候，**CN** 也會因為沒有收到 **MN** 回應的 Acknowledgement 而重傳一次丟失的封包，如此就可以保持 TCP 的通訊不會中斷。

Mobile IP 確實無法保證 UDP 訊息在 **MN** 進行漫遊的過程中遺失封包，然而 UDP 通訊的本質就是可以允許通訊過程中 UDP 封包的遺失，因此實際應用上 UDP 的都是用在如 Streaming 或者 Video On Demand 這一類語音資料的應用系統上。這一類應用系統可以容許部分的 UDP 封包遺失，而不至於導致應用系統無法運作。

(D) Mobile IP 的 AAA 處理

RFC 3220 中並沒有針對 AAA 的真正實作方式有所定義，只是簡單的定義了 Registration 的處理架構以及訊息的框架格式。

Registration 的訊息中，除了標準的 Mobile IP 進行 Tunnel 紀錄所需的一些欄位之外，後面全部是透過所謂的 Authentication Extension 來讓系統實作者進行必要的 AAA 架構設計。

RFC 3220 中定義了三種基本的 Authentication Extension， MN-HA，MN-FA, FA-HA ，分別用來讓 **MN** 與 **HA** 之間，**MN** 與 **FA** 之間，**FA** 與 **HA** 之間作 AAA 處理。

3.3 雙網網路整合與安全性考量

3.3.1 同異質網路漫遊的整合架構

此次實習中分別提出不同的漫遊架構，包括在同質網路和異質網路間的狀況，其中 IP 的移動管理必須在整合的網路架構中做到:

(A) 不同 WLAN 網路中的交遞

(B) 3G 與 WLAN 網路間的交遞（漫遊）

為達到此一目的，第三層 (Layer 3) 的無縫隙漫遊需成功。圖(8)與圖(9)分別表示欣建通於同質與異質網路中進行漫遊時的架構，此時所需達到的漫遊機制包括：

(1) 從一網路的領域中進入另一不同網路領域

(2) 兩種網路可能是用不同的方式進行無線進接存取

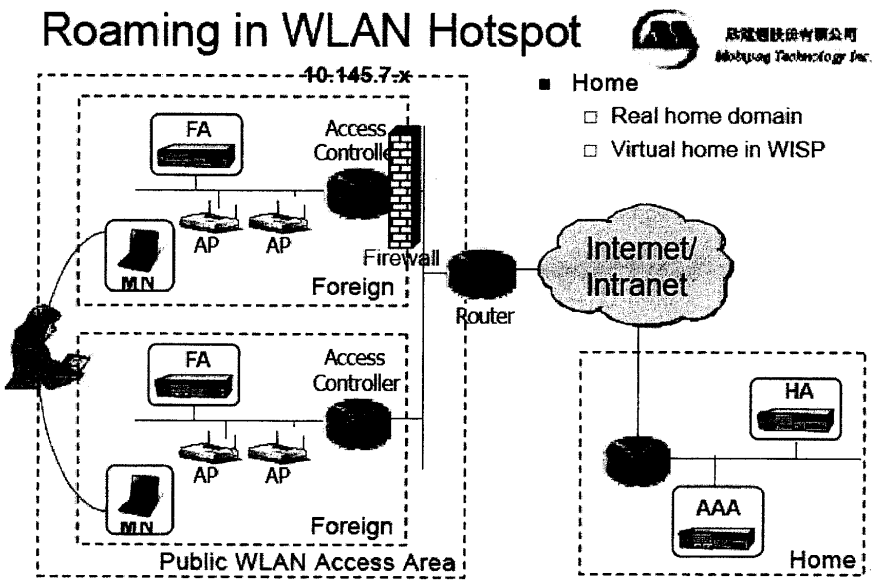
(3) 原本服務中的連結不斷

(4) 第二層 (MAC 層) 的交遞是必須但可不用考慮

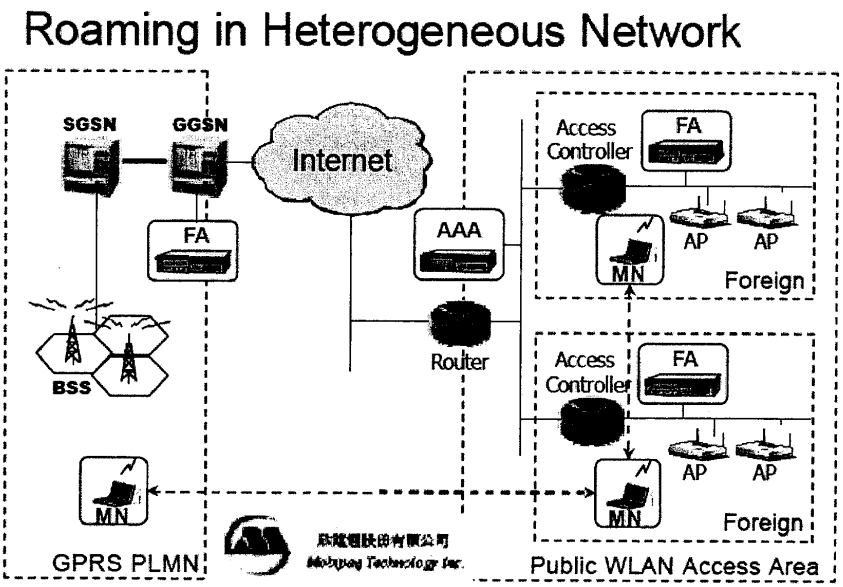
(5) IETF 之 Mobile IP 的定義是指第三層的無縫隙漫遊

圖(10) 所示則為本次購案中，欣建通公司提供本所漫遊的架構圖，為了與實際營運模式相同，FA 無法放置於 3G 網路內，且欣建通公司無法同時擁有 FA-COA 與 CCOA 的並存架構之軟體。故本所此次購案中的機制皆為 FA-COA，與先前和別家廠商測量不同的地方為：該架構中，3G 裡的 MN 仍為 FA-COA 狀態。欣建通公司原先的解決方案全為 CCOA 的架構，但為符合本所不侵入 3G 網路中的要求，又全數改為 FA-COA，且因 FA 在透過防火牆才與 MN 介接的方式並非屬於 Mobile IP 的規範，故該機制屬於欣建通公司的專利 (Proprietary)，而並非完全相等於原 Mobile IP 規範所定義的架構。此點因涉及公司的軟體機密，故本次並未詳加描述。

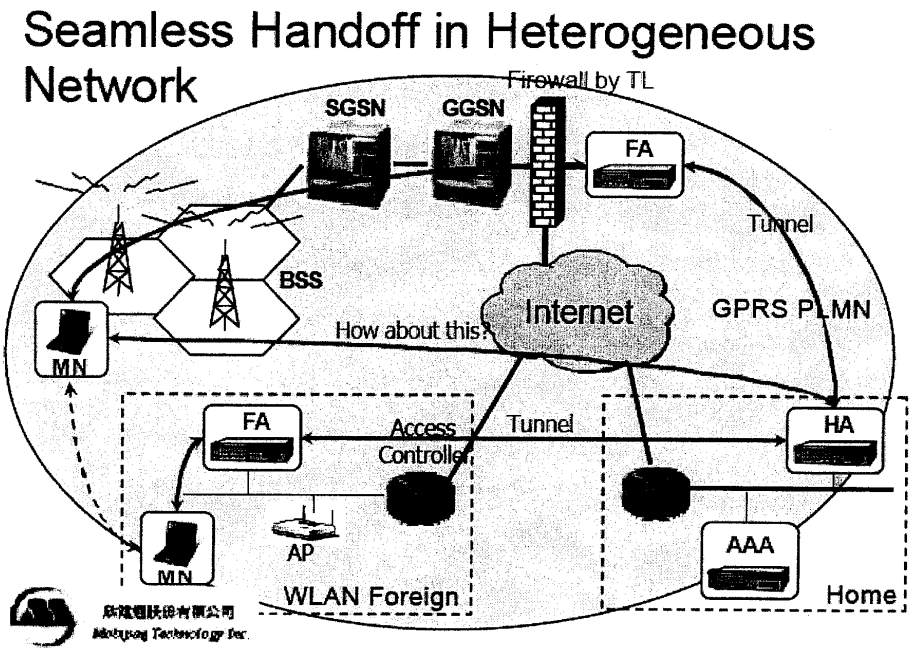
另外，欣建通公司針對 NAT 也根據 Mobile IP 的機制來設計軟體，故在 NAT 存在的架構中，仍能順利漫遊成功，針對本所與 NAT 架構的漫游圖示如圖(11)，而吾人所習知的的通透防火牆的架構圖則如圖(12)，可觀察出與本所架構不同處在於該 FA 的位置在 GPRS 的網路架構中是位於防火牆內，與本所放置於防火牆外有所不同，此為符合 Mobile IP 之架構。



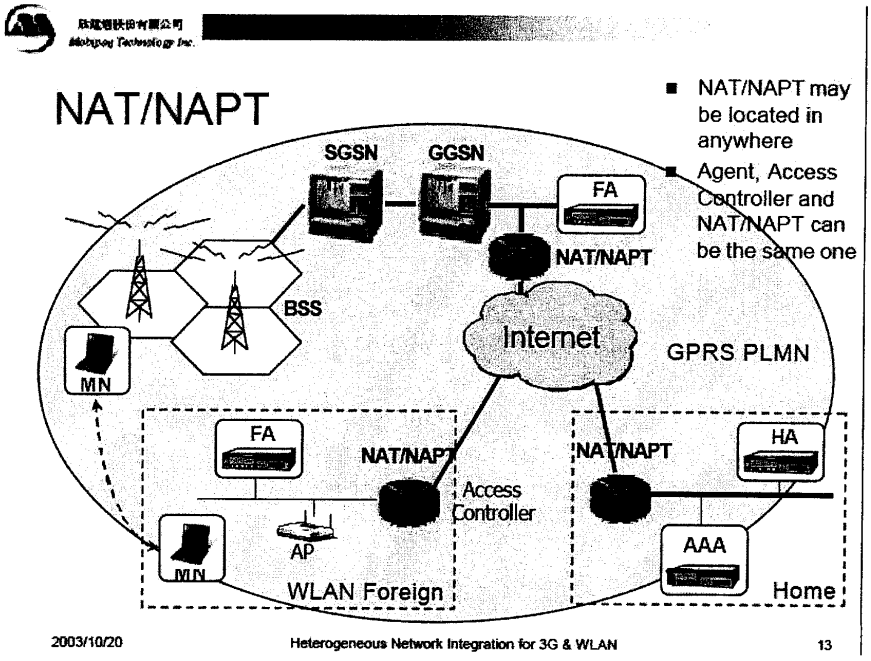
圖(8) 欣建通之同質網路間的漫遊架構



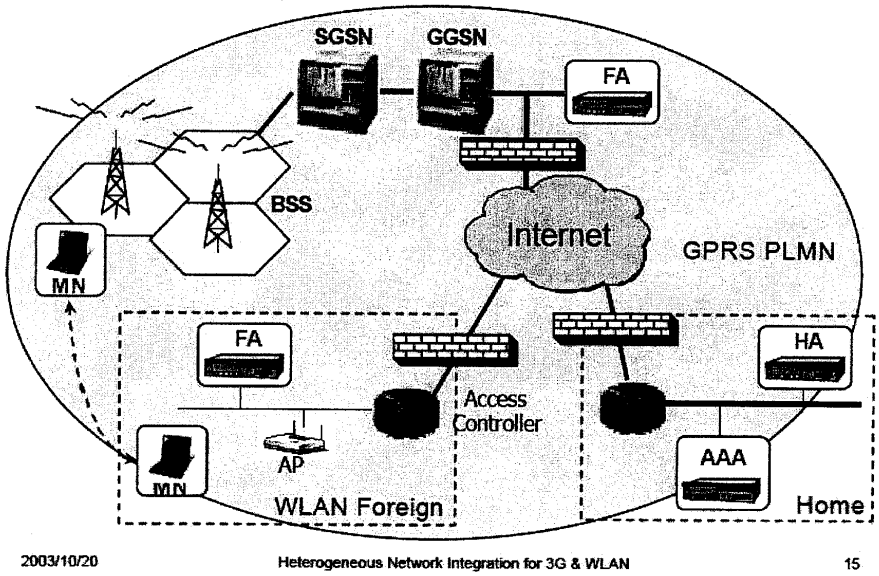
圖(9) 欣建通之異質網路間的漫遊架構



圖(10) 欣建通建置於本所的漫遊架構圖



圖(11) 欣建通建置於本所之包含 NAT 的漫遊架構圖



圖(12) 欣建通建置於本所之包含 Firewall 的漫遊架構圖

3.3.2 同異質網路漫遊的安全性

在 2.5G 與 3G 行動通信網路中均有完整的 AAA 解決方案，但在 WLAN 網路中卻欠缺此一方案。因此，目前的標準中 802.11x 是目前可用來解決 WLAN AAA 的標準之一。而對行動業者而言則可以利用行動通信(GSM/3G)中的 AAA 認證機制進而結合 WLAN 網路系統，如此一來不僅可共用用戶的管理系統，更可將收費機制統一由單一帳單出帳。如此的好處包括：

(1) 使用最少的安裝費用與降低複雜度

(2) WLAN 的服務業者可使用 GSM/GPRS 的計費和認證系統

欣建通建議在WLAN的安全標準方面有三種等級之分：

(1) 開放式介接 (Open Access): 無 Encryption，為目前的 Public WLAN 架構。

(2) 基本安全：加上 40 bit 或 128 bit 的靜態 WEP Encryption，通常使用在家庭中。

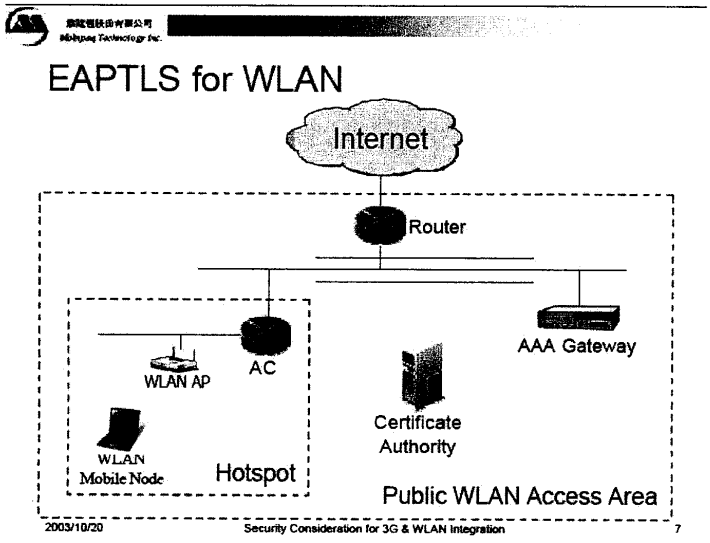
(3) 加強性的安全：包括 802.11X-based 的 authentication，TKIP 或 AES encryption，通常使用於企業界或未來的 Public WLAN。

而在WLAN的AAA認證機制中使用的認證方式包括：

(1) 802.11x 之 EAP-based 安全認證方式

(2) 其他利用 EAP-based (Extensible Authentication Protocol)演算之認證方法： EAPTLS (Transport Layer Security)，EAPTTLS (Tunneled TLS) 和 PEAP (Protected EAP)等。

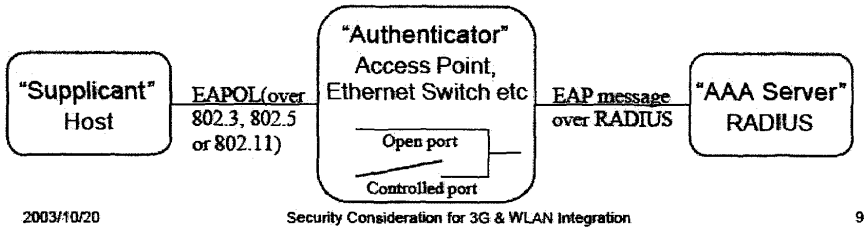
如圖(13)，為 EAPTLS 應用於 WLAN 的架構圖。



圖(13) 應用 EAPTLS 的 WLAN 網路架構圖

，針對Operator整合WLAN的網路時，亦可應用數種安全機制，主要可採用的安全機制包括原本AAA server所提供的安全認證與帳務系統上的管理。而WLAN中應用於Operator AAA上的安全機制主要為SIM-based 的機制，亦即802.11x的解決方案。

在IEEE 802.11x的定義中，主要扮演三大角色：分別為Suppliant, Authenticator, 與Authentication。為能應用於Operator的架構中，尚須增加EAP與Authentication的Server。其中EAP的功能為允許增加其他的安全認證方法加諸其上，與進行集中的使用者管理和成為開放與擴張式的標準之基本規約。其簡單的示意圖如圖(14)。



圖(14) 應用EAP的示意圖

此外，欣建通利用EAP-SIM based的解決方案則如圖(15)，圖中是以GPRS網路為規劃。根據欣建通的說法，採用EAP-SIM的主要理由如下：

(1) EAP-SIM 在管理公眾使用者時，唯一較容易實現的方法。

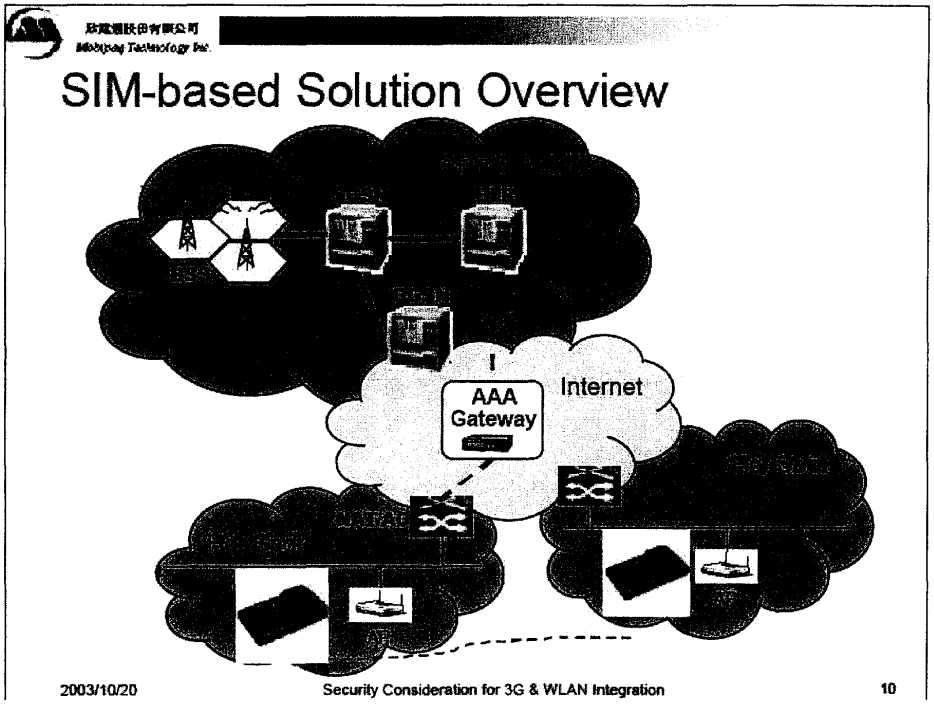
(2) SIM 卡是足以信任且攜帶方便的一安全認證實體。

(3) 可提供與 Operator 合作的良好基礎

(4) GSM SIM 卡的認證可直接由 Operator 的原有機制進行認證

根據以上的 SIM-based 之認證，OWLAN (Operator WLAN)所需的系統中

之相關元件包括：AAA/HLR Gateway，Access Controller (Authenticatior)，Wireless Access Point 與 MN（具 WLAN NIC）。



圖(15) 應用SIM-based 的整體架構圖

3.4 結論

此次赴香港的實習課程主要包含：「Mobile IP Training」及「Heterogeneous Network Integration and Security Consideration for 3G & WLAN Integration」兩部分；除了探討異質網路漫遊之機制與要點，並對異質網路間使用Mobile IP時的架構進行探討，有助於異質網路漫遊規劃與應用服務所需考量的要點。尤其在異質與同質網路的架構上的探討，可提供日後佈建時的依據，以目前的架構而言幾乎全都是以MIP為主的架構，所以MIP也成為探討異質網路整合時最重要的基本因素與實踐藍圖。

4. 實習心得與建議

高速率的數據傳輸及多樣化的服務要求與日俱增，3G系統成為目前GSM網路經營者最合適的系統選擇。但由於使用者需求的多樣化與價格上的差異，致使許多用戶在WLAN網路的使用上日益頻繁，且數量有急速上昇的趨勢，對本公司即將開始經營3G 網路而言，既可為利亦可為弊。若忽略 WLAN 網路的用戶成長量而未將其與行動通信之用戶進行整合，則勢必在許多 PWLAN (Public WLAN) 區域周圍之非WLAN涵蓋區，會因無法提供WLAN用戶使用3G而降低3G的用戶量與使用量，此則為弊。且若只看到整合時3G用量的可能減少性而不願整合（因WLAN的價錢便宜，而3G主要互補的部分為漫遊與服務不中斷特性），則其弊將會因WLAN的用戶無法與3G用戶漫遊的不方便性而擴大。反之，藉由整合用戶的資料與提供漫遊方便性，則能提高 3G的用戶量與部分的使用量。有鑑於此，如何的利用3G在WLAN網路在室內部分輔助3G網路，進而整合雙網系統之帳務與認證，使用戶在選擇之餘，仍能為行動業者所統整，實為重要之策略。

第三代行動通信服務和WLAN的網路皆以寬頻、多樣化及品質為重要的訴求，是以利用適當的漫遊機制促使兩者在整合時能順利的進行無縫隙漫遊是非常重要之目標。此次實習藉助實際操作MN，HA，FA，與AAA的設備等進行Mobile IP的實作，使吾人在網路整合的觀念與實作上均受益良多。將來在進行雙網整合前，亦可藉由此次實習的相關探討與結果，作為評估與規劃的參考。