電信國家型計畫子計畫一期末報告

1. 中英文摘要

本計劃主要之目的，是要研究如何在多階層行動隨意網路(Multi-tier Mobile Ad Hoc Network)提供一個虛擬家網環境(Virtual Home Environment, VHE)，讓行動主機的使用者可以在不手動更改行動主機原有的環境設定(configuration)下，在任何時間、任何地點都能利用不同的存取網路(access network)連結網際網路(Internet)，並繼續享有如同家網網路(home network)環境所能提供的個人化服務。

隨著 Wireless LAN/Bluetooth、GPRS、WCDMA/cdma2000 等各種無線通訊網路的發展，與行動主機(Mobile host)軟硬體能力的提升，行動主機如能配備多階層(multi-tier)無線網路設備，就可以自由的在不同通訊協定中切換，享有不同通訊系統所提供的服務。而其他祇配備低階無線網路(如 Wireless LAN 或 Bluetooth)的主機，也可以利用行動隨意網路(Mobile Ad Hoc Networks)的多步跳躍(Multi-hop)能力，藉由別的行動主機幫忙轉送(relay)封包，利用各種不同無線網路連結網際網路。因此多階層行動隨意網路可以大大提升行動主機的的行動能力(mobility)。

然而當行動主機移動到一個新的網路環境後，如何有效地(1)利用行動主機上所支援的多階層網路設備連結網際網路、(2)登入家網網路(Home network)、(3)持續存取家網網路上的資源和設備(如資料庫、檔案系統、伺服器等)和(4)使用當地的網路環境上的資源和設備(如印表機、伺服器等)，便成為主要的研究課題。因此我們的研究主題包括同質/異質無線網路間的漫遊、安全和認證以及資源探索與分享等三大問題。

關鍵字：VPN，VHE，Multi-tier，AAA。

This project aims to develop a Virtual Home Environment (VHE) for future wireless Internet with various wireless access network technologies such as wireless LAN, GSM, GPRS, WCDMA/cdma2000, and etc. The idea of VHE is to enabling

mobile users the ability of accessing a large range of personalized and incorporated services, whatever location they reside and/or network interfaces they use. On the other hand, the concept of Virtual Private Network (VPN) makes mobile hosts appearing as they were staying at their home networks even when they are indeed visiting foreign networks. By using the techniques of VPN, we can enforce services integrity that a mobile host can have in its home network even when the mobile host is away from its home network.

Therefore, we plan to adopt the concept of VPN to provide a VHE to mobile or fixed hosts for the future wireless Internet. In our design, a host could be equipped with more than one network interface and may connect to its home VPN through whatever interface that is available or the most appropriate to it without breaking an ongoing connection.

Key word: VPN，VHE，Multi-tier，AAA。

2. 計畫研究背景

近年來，隨著第三代行動通訊系統(the 3G mobile communication system)的發展日益成熟，研究人員發現：在以 IP 為基礎之網路上的行動台(mobile node, MN)若要能隨時隨地自由存取網路上多樣化的資源，必需仰賴虛擬原網網路環境(Virtual Home Environment, VHE)的支援，否則會遭遇網路資源存取權限、使用者認證和新路徑重新路由…等問題。因此歐洲的 EURESCOM 研究計畫針對 3G 行動通訊系統 UMTS(Universal Mobile Telecommunication System)協定，提出一個 VHE 的網路架構，他們以 IETF 提出的 Mobile IP (MIP)協定為基礎，建構一個智慧型網路系統以保證 MN 使用者能夠在任何地點存取個人化服務。進一步地希望未來能夠在網路安全的前提之下，根據使用者所在的環境自動安裝並提供新的服務。VHE 已經確定是未來 3G 行動通訊的關鍵技術，由於它是以 IP 為基礎，所以未來可以整合有線 Internet 網路和其他無線網路(如 WLAN、Bluetooth、EGDE 和 cdma2000 等)提供一個 all IP 的網路環境。

虛擬家網環境(Virtual Home Environment, VHE)的概念是要讓 MN 的使用者可以在任何時間、任何地點、以任何型態的終端設備都能繼續享有如同家網網路(home network)環境所能提供的個人化服務。對於行動使用者來說，VHE 一方面必需讓網路系統商和服務提供者提供完整範圍的、因人而異的個人化服務(customized service)給每一個使用者，這些服務將不受下層網路環境(協定)變動的影響；另一方面，能夠讓行動使用者藉由簡易的下載方式很輕易地升級他們的服務。對於網路系統商來說，VHE 必需提供一個極具彈性的網路發展平台，讓他們能夠在很短的時間之內，就能針對使用者的需求設計出各式各樣的應用程式，而這些應用程式能夠在小幅度修改甚至完全不必修改之下移植到不同的網路系統。最後，對於服務提供者來說，VHE 必需提供一組建立服務的工具程式，這些工具程式能夠讓系統商建立和維護包括網路端和使用者端的所有服務的功能模組，這些功能模組包含有使用者認證、加密、網路資源的配置等功能。

簡而言之，VHE 的目標就是要建構一個可跨網路協定的個人網路環境，利用一致性的使用者介面讓使用者感覺不出網路環境(介面)的切換，順暢地在同質或異質網路區域間安全地漫遊，感覺有如同使用家網網路的固定主機一般。為了達到此目標，3GPP 也有制定相關的標準，因為 3GPP 主要是電信廠商主導，是以電信環境互通為主，本計畫則是以網際網路為目標，無線的存取網路可以是不同通訊設備（如 WLAN、PHS、GPRS 等）所組成的「異質網路（Heterogeneous Networks）」。計畫的目的是要研究如何在含行動隨意網(Mobile Ad-hoc Network)的多階層異質網路(Multi-tier Heterogeneous Networks)提供一個虛擬家網環境(Virtual Home Environment, VHE)，讓行動主機的使用者可以在不手動更改行動主機原有的環境設定(configuration)下，在任何時間、任何地點都能利用不同的存取網路(access network)連結網際網路(Internet)，並繼續享有如同家網網路(home network)環境所能提供的個人化服務。

我們採用網際網路的技術，加強目前已有或甚至設計新的協定。我們預計以 Mobile IP 的行動管理機制，結合 IP-based VPN (Virtual Private Network)相關的協

定;如 PPTP(Point-to-Point Tunneling Protocol)、L2TP (Layer Two Tunneling Protocol)、IPsec 等，以及 NAT (Network Address Translation)、Authentication (如 AAA)和資源探索(如 Directory services) 等協定或技術，以達成上述目標。

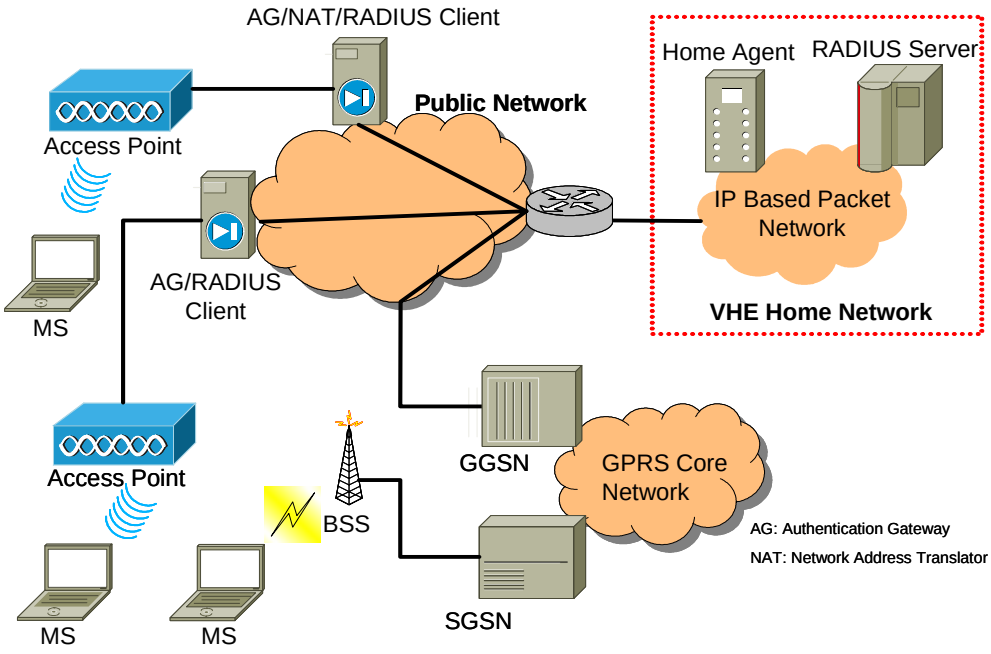
3. 系統架構與功能

系統主要可分成兩個部分：(1)Two-tier Mobile Terminal Server and Client (2)Authentication Gateway and Radius/AD Server。

第一部份是 Two-tier Mobile Terminal Server and Client，Two-tier Mobile Terminal Server 提供 Mobile IP with NAT 機制，能夠接受並管理 Two-tier Mobile Terminal Client 的註冊；而 Client 端為網路環境的建構，包含無線區域網路的設置，及使用 GPRS 裝置連接 Internet，還有 Mobile IP 環境的設立，負責在網路切換時通知 Server 端，提供順暢換手 (smooth hand-off) 機制，讓使用者達成漫遊時自動切換使用裝置與連線不中斷的理想。

第二部分則為 Authentication Gateway and Radius/AD Server，負責使用者登記和認證動作，使得使用者在切換網路後仍然能夠使用原來網路的資源，不需要重新作登記及認證動作。其中 Authentication Gateway 主要的功能有如一個加入認證功能 Gateway，但其中並不內建帳號，帳號之維護以及建立和刪除是利用單一個 Radius Server 達成，如此一來就不會有各個 Authentication Gateway 各自內建帳號之維護的問題，也可以輕易達到 AAA (Authentication Authorization Accounting) 的管理功能。

下圖是系統的整體架構圖，在圖中我們可以看到使用者先在原始網路中向 Authentication Gateway 登記，通過認證後便可以藉由我們的系統，帶著其可攜式的電腦漫遊於不同網段的網路環境，並於適當的時機使用最合適的裝置連接 Internet，並且原來的網路並不會因此斷線。

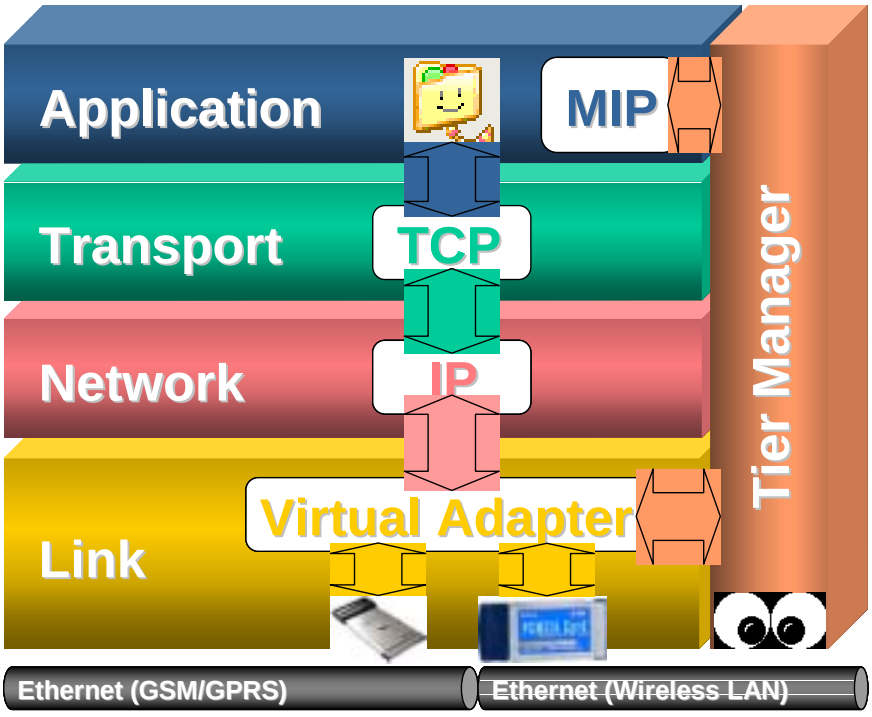


系統架構圖

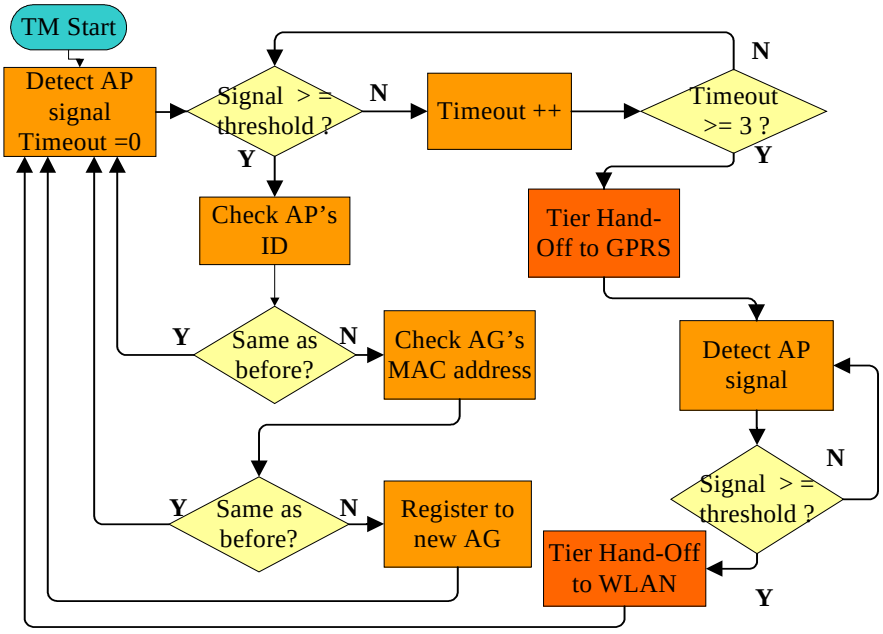
其元件說明如下：

- **VHE Home Network**：當 MN 不在 Home Network 時，仍可藉由 VHE 的機制獲得如 Home Network 般的服務環境，或者可連回 VHE Home Network 存取 Home network 的資源。
- **Home Agent**：當 MN 離開 Home Network 時，利用 MIP 機制代替 MN 接收封包並轉送到 MN 目前所在網段的伺服器。
- **AG/NAT/RADIUS Client**：AG/NAT/RADIUS Client 為一個加入 NAT, DHCP 功能的 Authentication Gateway，使用者要經過授權認證後才可經由此 AG 連結上網，其中 AAA 的部分是採用 RADIUS 的管理。
- **RADIUS Server**：多個 Authentication Gateway 的認證資料庫，帳號密碼都儲存於這裡，可達到中央式的管理以及使系統的擴展性(scalability)加強。
- **GGSN**：Gateway GPRS Support Node，架設在基地台中心的閘道節點，負責處理各基地台回傳的上網資料。
- **SGSN**：Serving GPRS Support Node，負責封包傳輸部分的資料處理。

另外，支援階層間換手的虛擬介面(Virtual Interface)，我門分別用下面兩個圖說明建立於 MN 中的換手虛擬介面協定架構，其中 virtual adapter 能夠根據無線信號的強度，選擇適當的無線網路介面以建立鏈結層的連線。另外，MIP 可以根據新的無線網路連線和對應的 IP address，向 Home Agent 作位置更新的動作，已確保上層的連線，如 TCP session 或 SIP session…等，不會因為作 tier handoff 而產生斷線。



階層間換手虛擬介面協定架構



虛擬介面自動切換訊號流程圖

4. 子計畫一第一年成果

本子計畫在第一年的系統功能包括：(1)跨網域漫遊的使用者登認證及帳號之稽核管理；(2)階層間的透通換手機制(transparent handoff)；(3)Mobile IP 在實際網路的部署(deployment)機制。其詳細內容將在下面敘述。

(1) 跨網域漫遊的使用者登認證及帳號之稽核管理

使用者登入、認證和授權 (Authentication Authorization Accounting；AAA) 的管理功能是 VHE 的基本功能，藉由使用者登記和認證動作，可以提供 VHE 網路在客戶端之基本存取權管制，避免非法使用者入侵。另外，也要讓使得使用者在切換網路後仍然能夠使用原來網路的資源，不需要重新作登記及認證動作。我們所採用的方法是：在每一個低階層之無線區域網路的部分安裝 Authentication Gateway(AG)，其主要的功能有如一個加入認證功能 Gateway，但並不內建帳號，帳號之維護利用單一個、位於 VHE Home 網路的 Radius Server 達成，如此一來就不會有各個 AG 各自內建帳號之維護的問題。至於在高階層無線廣域網路的部分則直接利用其原有的 AAA 機制。

(2) 階層間的透通換手機制(transparent handoff)

為了提供上層網路協定透通換手的能力，我們將在多種網路介面的驅動程式和上層協定之間建構一個虛擬設備介面(Virtual Device Interface)，稍後在圖 2 說明，此虛擬設備介面是介面管理者，可以根據網路介面(如 Wireless LAN)所測量到的訊號強度和服務品質來決定連接的網路設備介面，以及經由哪一個網路介面收送封包，介面管理能夠維持上層網路協定的連線在設備介面切換時不致中斷(倚靠 Session handoff manager 和 Session forwarding buffer 來達成)。Tunneling Device 則可以執行封包的 encapsulation 和 decpsulation 是實作多階層 Mobile IP 系統的必要機制。

(3) Mobile IP 在實際網路的部署(deployment)機制

因為 Mobile IP (MIP)採用 IP-in-IP 包裝的 IP 封包，將封包經由 Home Agent (HA)在 Corresponding Node (CN)端和 MN 之間的利用隧道(tunnel)的方式傳輸。因此 MIP 在現有網路環境使用會遭遇相當多的問題，例如 Network Address Translator (NAT)和封包加密的問題。由於 AG 一般而言都會支援 NAT 協定，以便自由使用 private IP address 而不受目前 IP address 不足的限制(GPRS 也有同樣的問題。然而，在 NAT 的機制下，MIP 機制中的 Home Agent 無法將封包路由到 MN。所以我們要修改 MIP 協定，讓 MIP 的封包其能夠穿越 NAT Gateway。

5. 子計畫一第二、三年的預定研究項目：

第二年研究項目：

(1) 完成 Mobile IP 與 VPN 的整合。

(2) 完成多階層 VPN 網路的架構與設計。

(3) 設計實作支援階層間無縫換手(seamless handoff)的機制。

(4) 研究如何利用 VPN 的特性，加強行動管理的能力。

(5) 整合 authentication 和 MIP 的流程，用以減低原先認證和授權獨立於 MIP 註

冊之外，所造成的延遲。

第三年研究項目：

(1) 設計 VHE 的網路資源延展與分享機制。

(2) 設計家網 VPN 和他網 VPN 之間的資源分享機制。

(3) 完成地點導向的服務探索與資源分享機制。

(4) 完成行動主機的自動環境組態設定與配置機制。

6. 文獻參考:

[1] Morand L. et al, “First Step toward an IP-based VHE,” IEE conference: 3G Mobile Communication Technologies, March 2001.

[2] EURESCOM Project P920 – UMTS Network aspects, http://www.eurescom.de/public/projects/P900-series/p920/P920.htm.

[3] 3GPP TR 23.922, “Architecture for an All-IP network,” v.4.0.0, March 2001.

[4] EURESCOM Project P920 – UMTS Network aspects, 2000, “VHE comcept description, scenario and protocol”, Project results D1.

[5] EURESCOM Project P1013 - “First Step toward UMTS: Mobile IP services, a European tesbed,”
http://www.eurescom.de/public/project/P900-series/p1013/P1013.htm

[6] Townsley W. et al, “Layer Two Tunneling Protocol "L2TP",” IETF RFC 2661, August 1999.

[7] Simpson W., “The Point-to-Point Protocol (PPP),” IETF RFC 1661, July 1994.

[8] Rand D., “PPP Reliable Transmission,” IETF RFC1663, July 1994.

[9] Rekhter Y., Moskowitz B., Karrenberg D., de Groot G. and E. Lear, “Address Allocation for Private Internets,” IETF 1918, February 1996.

[10] Valencia A., Littlewood M. and T. Kolar, “Cisco Layer Two Forwarding (Protocol) L2F,” RFC 2341, May 1998.

[11] Kent S. and R. Atkinson, “Security Architecture for the Internet Protocol,” RFC 2401, November 1998.

[12] Hamzeh K., Pall G., Verthein W., Taarud J., Little W. and G. Zorn, “Point-to-Point Tunneling Protocol (PPTP),” IETF RFC 2637, July 1999.

[13] M. Carugi, et al., “Service Requirements for Provider Provisioned Virtual Private Networks,” IETF DRAFT draft – ietf – ppvpn – requirements -01.txt, June 2001.

[14] G. Heron, et al., “Requirements for Virtual Private Switched Networks,” IETF DRAFT draft – heron-ppvpn-vpsn-reqmts-00.txt, July 2001.

[15] B. Gleeson, et al, “A Framework for IP Based Virtual Private Network,” IETF RFC 2764, February 2000.

[16] L. Andersson, et al. “Label Distribution Protocol Specification,” IETF RFC 3036, January 2001.

[17] B. Gleeson, A. Lin, J. Heinanen, G. Armitage, A. Malis. “A Framework for IP Based Virtual Private Networks,” IETF RFC 2764, February 2000.

[18] V. Kompella et al. “Virtual Private Switched Network Services over an MPLS Network,” draft-vkompella-ppvpn-vpsn-mpls-00.txt, October 2001

[19] 3G TS 23.108: “Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); Mobile radio interface layer 3 specification; Core Network Protocols - Stage 2 (Release 4),” v.4.0.0, March 2001.

[20] 3GPP, “Open Service Access (OSA); Application Programming Interface(API),” Tech. spec. 3GPP TS 29.198 5.1.0, Sep. 2002.

[21] 3GPP, "VHE Home Environment/Open Service Access (OSA)," Tech. spec.3GPP TS 23.127 v5.1.0 Sep. 2002.