

國立交通大學

資訊工程系

碩士論文

在行動虛擬私人網路下以行動代理人為基礎之無縫交遞

Mobile Agent-based Seamless Handoff for Mobile VPN



研究生：吳科慶

指導教授：曾建超 教授

中華民國九十四年六月

在行動虛擬私人網路下以行動代理人為基礎之無縫交遞

Mobile Agent-based Seamless Handoff for Mobile VPN

研究生：吳科慶

Student：Ko-Ching Wu

指導教授：曾建超

Advisor：Chien-Chao Tseng

國立交通大學
資訊工程系
碩士論文

A Thesis

Submitted to Department of Computer Science and Information Engineering

College of Electrical Engineering and Computer Science

National Chiao Tung University

in partial Fulfillment of the Requirements

for the Degree of

Master

in

Computer Science and Information Engineering

June 2005

Hsinchu, Taiwan, Republic of China

中華民國九十四年六月

在行動虛擬私人網路下以行動代理人為基礎之無縫交遞

研究生：吳科慶

指導教授：曾建超 博士

國立交通大學

資訊工程學系碩士班

摘 要

本論文之基本動機在於同時提供行動性與安全性。要達成這個目標有許多方法，如結合兩個網路協定，讓他們各自負責行動性與安全性。然而單純地結合兩個協定雖然可避免部署新的網路元件，或降低重寫程式的麻煩，但卻犧牲了使用的效能，因為兩個網路層協定在結合時，通常會有不必要繼續存在的協定要素。

除了重複動作的資源浪費外，協定之間還可能有彼此衝突的情況發生，為了完成某協定的程序，可能要犧牲另一協定的功能，或是額外作一些動作來配合。

另外，為了行動性與安全性，當行動端 (Mobile Node) 在切換所在的網域或是改變 IP 位址的時候，所花的時間將會非常長，使用者可明顯感到連線被中斷，而且有時還會造成通訊或網路協定上的逾時 (timeout)，不符合實際應用。

於是我在原本企業所使用的虛擬私人網路 (Virtual Private Network, VPN) 架構上，加上行動代理人 (Mobile Agent) 的技術與一些 Mobile IP 機制來同時提供行動性與安全性。

Mobile Agent 代替行動端進行預先認證與協調的動作，並搭配 Multicast 以及 Mobile IP 的 binding list 要素，使行動端在切換網域之後，可立即接續之前的連線；VPN 的架構除了保障安全性之外，還讓行動端省去第三層換手的動作。如此在傳輸效能與安全性上將與僅使用 VPN 一樣，而交遞卻比 Mobile IP 快速且無間斷，使本系統得以支援即時通訊的應用程式。

Mobile Agent-based Seamless Handoff for Mobile VPN

Student: Ko-Ching Wu

Advisor: Dr. Chien-Chao Tseng

Department of Computer Science and Information Engineering

National Chiao Tung University

ABSTRACT

Supporting mobility and security simultaneously is the basic motivation of this thesis. An intuitive solution may be the combination of two internet protocols, providing mobility and security respectively. Despite direct merging of two protocols reusing existent software and network hardware, reduced system efficiency is further caused by redundant elements shared by both protocols.

Besides the resource squander of duplicate proceedings, a conflict may be break out between two protocols. Sacrifice or extra actions of one protocol for processes of other protocols may be caused.

When Mobile Node changes its network domain or IP address, it usually needs a lot of procedures for supporting mobility and security. User would feel the break off of the connection, and the communication or internet protocol would suffer timeout in realistic applications.

This thesis provides a method and system for mobility and security, comprising Virtual Private Network (VPN), Mobile Agent and some Mobile IP mechanisms.

The mobile agent acts as a representative of mobile node, and executes pre-authentication and pre-negotiation with the multicast mechanism and the binding list of Mobile IP protocol to make mobile node continue the previously communication after changing network domain. VPN architecture not only provides security, but saves the handoff latency for mobile node. Therefore, the transmission performance and security of this system are the same as VPN, and the handoff latency is less than Mobile IP to make this system suit real-time protocols.

誌 謝

本篇論文的完成，首先要感謝我的指導教授 – 曾建超博士，感謝老師開啟我對這領域的認識，並細心修正我的研究方向，以及在論文的完成與口試階段給予的費心指導。還有學長 – 楊人順博士，從專題一路帶領我前進，啟發和引導我的研究內容，並在過程中不斷地鼓勵與建議。若是沒有老師和學長的協助，我不可能完成此論文。

還要感謝實驗室所有學長姊、同學、學弟妹的支持與幫忙，讓我在這段實驗室的日子裡過得非常充實愉快。

此外要謝謝家人給我良好的學習環境，讓我得以無後顧之憂地專心研究。還有大學同學及社團夥伴於精神上的支援，使我能夠在最佳狀態堅持下去。

僅以此研究成果，獻給所有關心我的家人、師長和朋友們。



目錄

中文摘要	i
英文摘要	ii
誌謝	iii
目錄	iv
圖目錄	vi
第一章 緒論	- 1 -
1.1 研究動機	- 1 -
1.2 研究目標	- 2 -
1.3 章節簡介	- 2 -
第二章 背景與相關研究	- 4 -
2.1 Virtual Private Network (VPN) 基本概念	- 4 -
2.2 Layer Two Tunneling Protocol (L2TP)	- 5 -
2.2.1 L2TP Message	- 5 -
2.3 Mobile IP簡介	- 6 -
2.4 Mobile IP與虛擬私人網路的結合	- 7 -
2.4.1 問題描述	- 7 -
2.4.2 Mobile IPv4 Traversal Across IPsec-based VPN Gateways	- 9 -
2.5 行動代理人	- 11 -
第三章 在行動虛擬私人網路下以行動代理人為基礎之無縫交遞	- 13 -
3.1 行動虛擬私人網路之基本架構	- 13 -
3.2 行動虛擬私人網路之設計方法	- 14 -
3.3 以行動代理人為基礎之無縫交遞機制	- 15 -
3.4 以行動代理人為基礎之無縫交遞機制的設計方法	- 15 -
3.4.1 偵測訊號並送出行動代理人	- 15 -
3.4.2 行動代理人的動作	- 16 -
3.4.3 第二層換手之後續動作	- 19 -
3.5 在行動虛擬私人網路下以行動代理人為基礎之無縫交遞流程	- 22 -

第四章 在行動虛擬私人網路下以行動代理人為基礎之無縫交遞實作 .	- 26 -
4.1 系統之軟硬體需求	- 26 -
4.2 偵測ESSID	- 27 -
4.3 Mobile Agent	- 27 -
4.4 Multicasting	- 29 -
第五章 效能分析	- 30 -
5.1 交遞效能分析	- 30 -
第六章 結論與未來工作	- 32 -
6.1 結論	- 32 -
6.2 未來工作	- 32 -
參考文獻	- 33 -



圖目錄

圖 2.1	VPN基本架構 1	- 4 -
圖 2.2	VPN基本架構 2	- 5 -
圖 2.3	L2TP Packet Format.....	- 5 -
圖 2.4	Mobile IP系統架構	- 7 -
圖 2.5	Mobile IPv4 Traversal Across IPsec-based VPN Gateways架構圖	- 9 -
圖 2.6	Mobile IPv4 Traversal Across IPsec-based VPN Gateways訊息流	- 10 -
圖 2.7	Mobile IPv4 Traversal Across IPsec-based VPN Gateways封包格式	- 11 -
圖 3.1	行動虛擬私人網路基本架構	- 13 -
圖 3.2	虛擬私人網路通道傳輸	- 15 -
圖 3.3	MN偵測訊號並送出行動代理人.....	- 16 -
圖 3.4	行動代理人之認證與授權	- 17 -
圖 3.5	Multi-homing.....	- 18 -
圖 3.6	積極式Oakley鑰匙交換法.....	- 19 -
圖 3.7	L2 Handoff	- 20 -
圖 3.8	Location Binding Update	- 21 -
圖 3.9	在行動虛擬私人網路下以行動代理人為基礎之無縫交遞機制運作圖	- 22 -
圖 3.10	Message Flow	- 24 -
圖 5.1	交遞效能比較	- 30 -

第一章 緒論

1.1 研究動機

近年來行動裝置的使用愈來愈普遍，通訊的行動性 (mobility) 已是不可缺少，而在講求方便的同時，安全性 (security) 逐漸為大家所重視，同時提供行動性與安全性似乎已經勢在必行。要達成這個目標有許多方法，較直覺的如個人用的行動網際網路協定 (Mobile IP) [1] 加上網際網路協定安全 (IPSec) [2]、企業的虛擬私人網路 (Virtual Private Network, VPN) 加上 Mobile IP [3][11]，然而單純地結合兩個協定雖然可避免部署新的網路元件，或降低重寫程式的麻煩，但卻犧牲了使用的效能，因為兩個網路層協定在結合時，通常會有不必要繼續存在的協定要素，例如 VPN 通道 (tunnel) 與 Mobile IP 通道的重複性。

除了重複動作的資源浪費外，協定之間還可能有彼此衝突的情況發生 [4][10]，為了完成某協定的程序，可能要犧牲另一協定的功能，或是額外作一些動作來配合。

IETF (Internet Engineering Task Force) 雖然有提出 Mobile VPN 的設計方案 [11]，但它使用了兩層 Mobile IP 與一層 VPN 封裝，這將大幅降低網路傳輸效能，也提高了使用者系統的負擔。

另外，一般在提供行動端 (Mobile Node) 行動性時，在切換所在的網域或是改變 IP 位址的時候，都必須要進行第三層換手 (Layer 3 handoff)，這樣才能讓行動端的連線得以導向新的、正確的位址。這個換手的動作至少包含了：

- 在新網域取得新的 IP 位址，並更新路由表 (routing table)。
- 通知家網代理人 (Home Agent) 或代理伺服器 (Proxy)，以改變連線路徑。

如果要再考量安全性的提供，還得再加上：

- 連線前的安全性認證、授權。
- 重新建立安全連線。

還有在換手後資料從代理伺服器轉送經新路徑到達新位置的時間。

這樣所花的時間將會非常長，使用者可明顯感到連線被中斷，而且有時還會造成通訊或網路協定上的逾時 (timeout)，不符合實際應用。

1.2 研究目標

本論文主要目標有：

- 提供一個可兼顧安全性的無縫交遞 (seamless handoff) 機制。
- 在兼顧行動性與安全性的前提下，盡可能降低網路負擔。
- 在行動性與安全性之外也注重擴充性。

於是我希望能在原本企業所使用的 VPN 架構上，加上行動代理人 (Mobile Agent) 的技術與一些 Mobile IP 機制來同時提供行動性與安全性。Mobile Agent 不僅增加行動交遞的效率，也加強了 VPN 的安全與掌控性，並可提供如服務品質保證(Quality of Service, QoS)的擴充性服務；VPN 的架構亦被利用來大幅提昇交遞效能。行動性與安全性不再彼此牽制，反而相輔相成，如此在傳輸效能與安全性上將與僅使用 VPN 一樣，而交遞卻比 Mobile IP 快速且無間斷，使本系統得以支援即時通訊的應用程式。

除此之外，在系統設計上不會追求程序的完整性，反而盡可能減少所需要的動作，這是希望在實際應用時，可以將現在業界所使用的各個系統 – 如行動代理人系統、安全性機制、服務品質保證、認證等等，鑲嵌在這套系統架構之中，而只需要做到這裡所要求的少數幾個動作，即可達成本系統之功能。

1.3 章節簡介

這篇論文的章節簡述如下：

- **第一章、緒論**

簡述這篇論文的動機，以及所希望達成的目標。

- **第二章、背景與相關研究**

說明此論文用到的背景知識，如虛擬私人網路 (VPN)、行動網際網路協定 (Mobile IP)、行動代理人 (Mobile Agent)；與相關的論文研究。

- **第三章、在行動虛擬私人網路下以行動代理人為基礎之無縫交遞**

介紹本論文提出的架構、機制與設計方法，包含行動虛擬私人網路與如何利用行動代理人達到無縫交遞 (seamless handoff) 的目標。

- **第四章、在行動虛擬私人網路下以行動代理人為基礎之無縫交遞實作**

本系統之實作方法，以功能區分為幾個大部分，並描述如何做到這些功能。

- **第五章、效能分析**

- **第六章、結論與未來工作**



第二章 背景與相關研究

2.1 Virtual Private Network (VPN) 基本概念

自成一個網域而與外界 (如網際網路 Internet) 隔絕的稱為私密網路 (private network)，這網域與外界的聯繫需經過防火牆，以確保內部安全性，通常見於企業網路，又稱為 Intranet。而身在公司外的公司成員想連接 Intranet 存取資源時，可以拉專線或直接撥接到公司內部。也就是說 private network 具有實體部署上的私密性。

然而這對於遠端存取資源的成本太高，距離太遠的話專線受限於物理傳遞限制而需轉接，佈線成本亦隨距離大幅增加；使用長途撥接的電話費也很高。至於跨海跨洲的成本更是限制其可使用性。

虛擬私人網路 (Virtual Private Network, VPN) 則是利用幾乎無所不在的 Internet 來大幅降低成本，且能達到 private network 的私密安全性。單一遠端使用者會向虛擬私人網路閘道器 (VPN Gateway) 建立一條通道 (tunnel)，此 tunnel 可以是點對點通道協定 (Point-to-Point Tunneling Protocol, PPTP)、第二層通道協定 (Layer Two Tunneling Protocol, L2TP) [5]、網際網路安全性協定 (Internet Protocol Security, IPSec) 等協定，此 tunnel 不僅使遠端使用者在系統架構上如同在 Intranet 內一般，也保障這段通訊的私密安全性。除單一使用者外，也有母子公司的架構，即兩個 VPN Gateway 間建立 tunnel，將兩個網域連成一個，兩 Gateway 通常有主從關係，如 L2TP 協定中的 L2TP 網路伺服器 (L2TP Network Server, LNS) 與 L2TP 存取集線器 (L2TP Access Concentrator, LAC)。

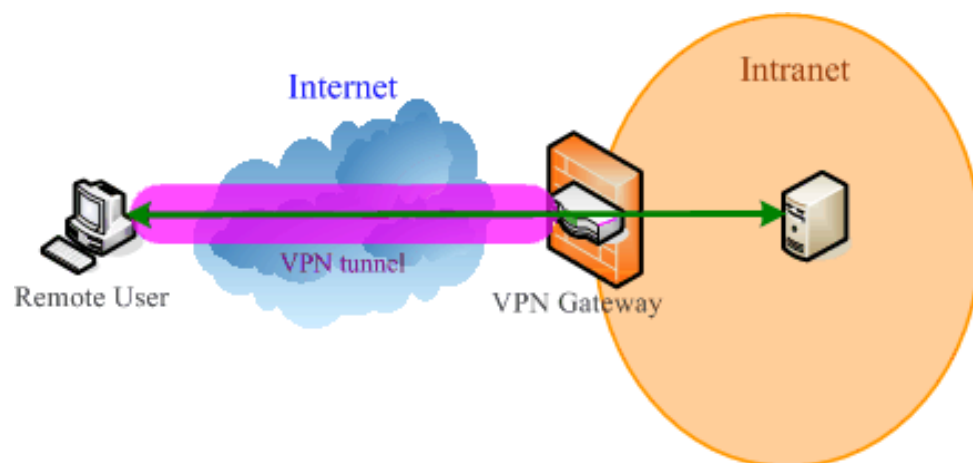


圖 2.1 VPN 基本架構 1

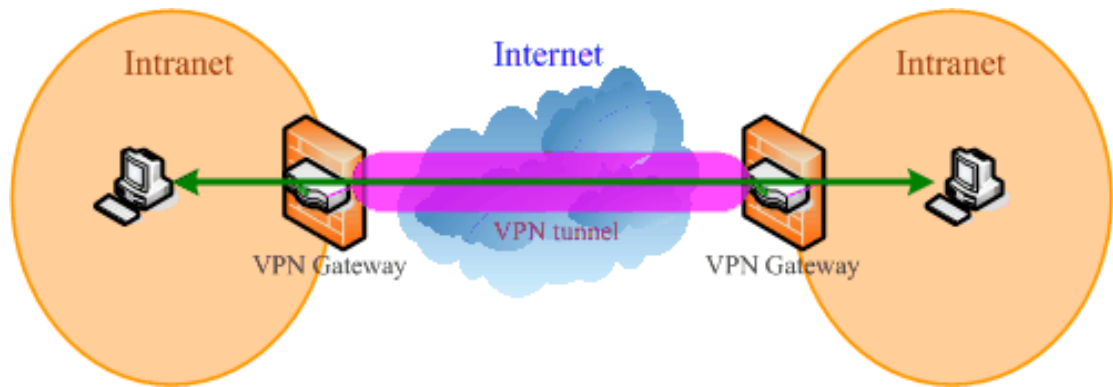


圖 2.2 VPN 基本架構 2

2.2 Layer Two Tunneling Protocol (L2TP)

[6] PPTP (Point-to-Point Tunneling Protocol) 是由 Microsoft、3COM、U.S. Robotics、Ascend、ECI Telematics 等企業所聯合發展，屬於 OSI 架構中第二層的協定，目的是在遠端使用者與網路伺服器之間提供虛擬私有網路。

同時 Cisco 也獨力發展了第二層轉遞協定 (Layer 2 Forwarding, L2F)，而後在 Internet 特別工程小組 (Internet Engineering Task Force, IETF) 的協調下，Cisco 與發展 PPTP 的公司共同擬定第二層通道協定 (Layer Two Tunneling Protocol, L2TP)，結合 PPTP 與 L2F 的優點，RFC 編號 2661 [5]。

L2TP 本身並不提供對資料的加密安全性，所以文獻建議搭配 IPsec 作加密機制 [15]。

L2TP tunnel 的兩端，在伺服器或母公司端的是 L2TP Network Server (LNS)，使用者或子公司端為 L2TP Access Concentrator (LAC)。

2.2.1 L2TP Message

下圖為 L2TP 封裝的格式，先以 PPP tunnel 包裝，再加上 L2TP 的 header，然後是一般 UDP 與 IP header，UDP header 指定送給 port 1701。



圖 2.3 L2TP Packet Format

而其中 L2TP Header 的格式為：

12 bits												4 bits	16 bits			
T	L	X	X	S	X	O	P	X	X	X	X	Ver	Length (option)			
Tunnel ID												Session ID				
Ns (option)												Nr (option)				
Offset Size (option)												Offset Pad ... (option)				

T：0 為資料訊息，1 為控制訊息。L：1 代表有 Length 這一欄位，控制訊息一定要設成 1。S：1 表示有 Ns、Nr 欄位，控制訊息一定要設成 1。O：1 表示有 Offset Size 這欄，控制訊息一定要設成 0。P：若設成 1，則在候伺與傳輸時，將獲得優先處理。Ver：L2TP 版本，目前為 2。Tunnel ID：L2TP tunnel 的 ID。Session ID：L2TP session 的 ID。Ns：此訊息的 sequence number。Nr：下一個預期收到訊息的 sequence number。

2.3 Mobile IP 簡介

行動網際網路協定 (Mobile IP) 是讓 IP 位址得以具備行動能力的一種通訊協定，它讓移動節點 (Mobile Node, MN) 在網際網路上漫遊時，仍可使用固定的 IP 位址來與其他網路節點進行通訊，這是由 IETF (Internet Engineering Task Force) 組織制訂出來的網路標準之一 [1]。

當 MN 移動到一個新網域時，他會在當地取得一個 IP 位址，這被稱為 Care of Address (CoA)，MN 會告知家網域 (Home Network) 的家代理人 (Home Agent, HA)，HA 則在 Home Network 代替 MN 接收來自通訊節點 (Correspondent Node, CN) 的封包，並經由通道 (tunnel) 轉送至 CoA。

MN 通訊時所固定使用的家網域 IP 位址稱為家位址 (Home IP)，HA 在家網域利用 ARP 通訊協定來接收給 Home IP 的封包，轉送至 Foreign Network (非 Home Network 之外地網域)。

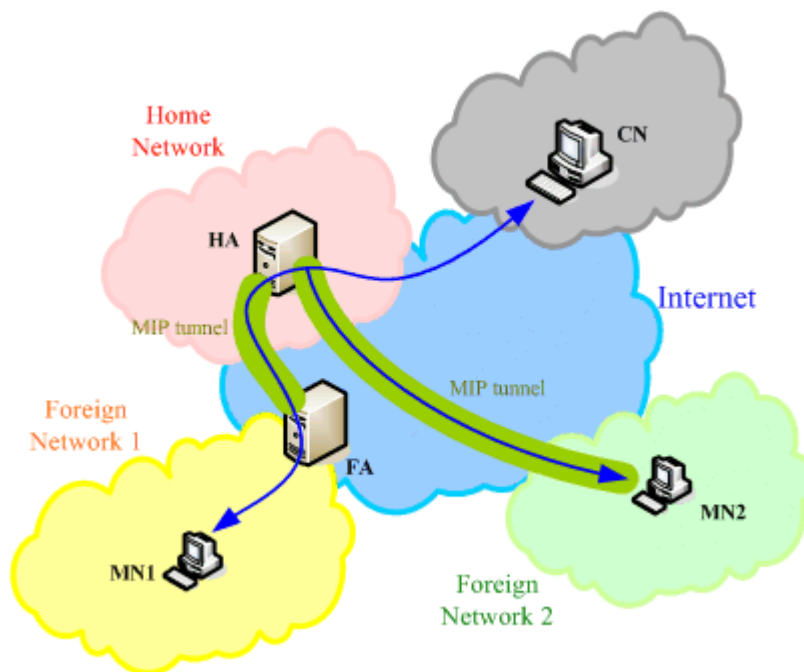


圖 2.4 Mobile IP 系統架構

圖 2.4 是 Mobile IP 的系統架構圖，其中 MN1 使用的是 FA-CoA，FA (Foreign Agent) 為 Foreign Network 中支援 Mobile IP 的伺服器，它管轄 Foreign Network，在其下的 MN1 所使用的 CoA 即 FA 的位址，被稱為 FA-CoA。FA 收到從 HA 傳來的封包後，根據 Home IP 來決定轉給底下哪個 MN (利用 MAC 位址)。

而 MN2 使用的是 Co-located-CoA (Co-CoA)，MN2 直接向 HA 建立 IP-in-IP 通道，HA 那裡所記錄的就是 MN2 在當地網路使用的 IP 位址，稱為 Co-located-CoA。

2.4 Mobile IP 與虛擬私人網路的結合

IETF 在 Internet Draft 中提出了 Mobile IP 與虛擬私人網路 (VPN) 結合時，所會發生的問題以及需要考慮的事情 [4][10]，還有它所訂定的解決方案 [3][11]。

2.4.1 問題描述

依照 IETF 的文獻 [4][10] 指出，討論 Mobile IP 與 VPN 的結合時，可依 Home Agent (HA) 的所在位置大致區分五種模型，再分別探討不同的封包格式及 Foreign Agent (FA) 存在與否所會造成的問題。

- **模型一、MIPv4 HA(s) Inside the Intranet behind a VPN Gateway**

當 HA 放在 intranet 中，被 VPN Gateway 保護著的時候，MIPv4 必需被封裝 (encapsulate) 在 VPN tunnel (以下以 IP Security (IPSec) 協定為例) 之內。由於 FA 無法辨認被 IPSec 所保護的內容，且 MN 不接受未經 IPSec 封裝的 Advertisement，故在此模型中並不能使用 FA。若採用 Co-located mode，則每當 MN 改變網路位置時，VPN tunnel 就必需做 re-negotiate 的動作。

- **模型二、VPN Gateway and MIPv4 HA(s) in parallel**

VPN gateway 與 HA 一起放在 DMZ 中，代表無論 MN 在 intranet 內或 internet 上，所有 MIPv4 的封包都必需經過 DMZ (DeMilitarized Zone)。這將有安全性上的顧慮。因為 DMZ 未受到完整的防火牆保護，屬於半公開的區域，雖然封包的資料因為仍有 VPN 保護不致外洩，但是仍有被駭客執行阻絕攻擊 (Denial of Service) 的可能。

這時可再探討 MIPv4 與 IPSec 的內外關係，若將 MIPv4 封裝在 IPSec 之內，則會產生跟前一個模型相同的問題；若是 MIPv4 在 IPSec 外，則需對 HA 與 VPN Gateway 的 routing logic 做一些修改，因為原本 VPN Gateway 是對外開門，可是現在從外面 MN 來的封包得讓 HA 先解開 MIP header，再交給 VPN Gateway；送給 MN 的封包則動作相反。

- **模型三、Combined VPN Gateway and MIPv4 HA**

此模型雖解決了前一模型的 routing 問題，但違反 multi-vendor interoperability (希望 MIPv4 mobility agents、mobility clients (MN)、VPN server 與 VPN client 能由四個不同的 vendors 所提供) 的原則，因為 MIPv4 mobility agents、mobility clients (即為 MN)、VPN server 與 VPN client 必需由同一家廠商設計。

- **模型四、MIPv4 HA(s) Outside the VPN domain**

IPSec 包在 MIPv4 之內，且 HA 不受 VPN Gateway 保護，所以 MIPv4 的註冊不需先跟 VPN Gateway 建立 IPSec tunnel。但是，由於 Intranet 中沒有 HA 的存在，MN 也不能以一個不受信任的 HA 來當作代理人，故 Intranet 內無法提供 mobility。除此之外，運作上應該沒有任何技術上的問題。

- **模型五、Combined VPN Gateway and MIPv4 HA(s) on the Local Link**

VPN Gateway 兼任 NAT Gateway 的角色，與使用 private IP 的 HA 以 local link

的方式連結。若是讓 MIPv4 封裝在 IPsec 裡面，則問題與第一個模型相同；若是 MIPv4 在外，則在路由(routing)方面沒有任何技術上的問題。但是，這個模型不適合用在大型的部署上，因為安全邊界大且分散，local link 的連接將會很複雜。

2.4.2 Mobile IPv4 Traversal Across IPsec-based VPN Gateways

經過幾年來的討論與演進 [3]，IETF 在 2005 年 1 月制訂了以下的架構和機制 [11]，這篇現在仍為 Draft，尚未升為標準，它的目的在於結合 Mobile IP 與 IPsec-based VPN，以同時提供行動性與安全性，並盡可能使用現有的軟硬體，不修改原有的協定。

圖 2.5 是此系統的架構圖，防火牆右邊是 Intranet，左邊就是 Internet (External network)；中間為 DMZ (Demilitarized Zone, 非軍事區)，有著一定程度安全性且要讓外部網路 (External network) 使用者存取資源的企業網路，文獻中說現在多數企業將 VPN 的管理伺服器部署在 DMZ 之中。

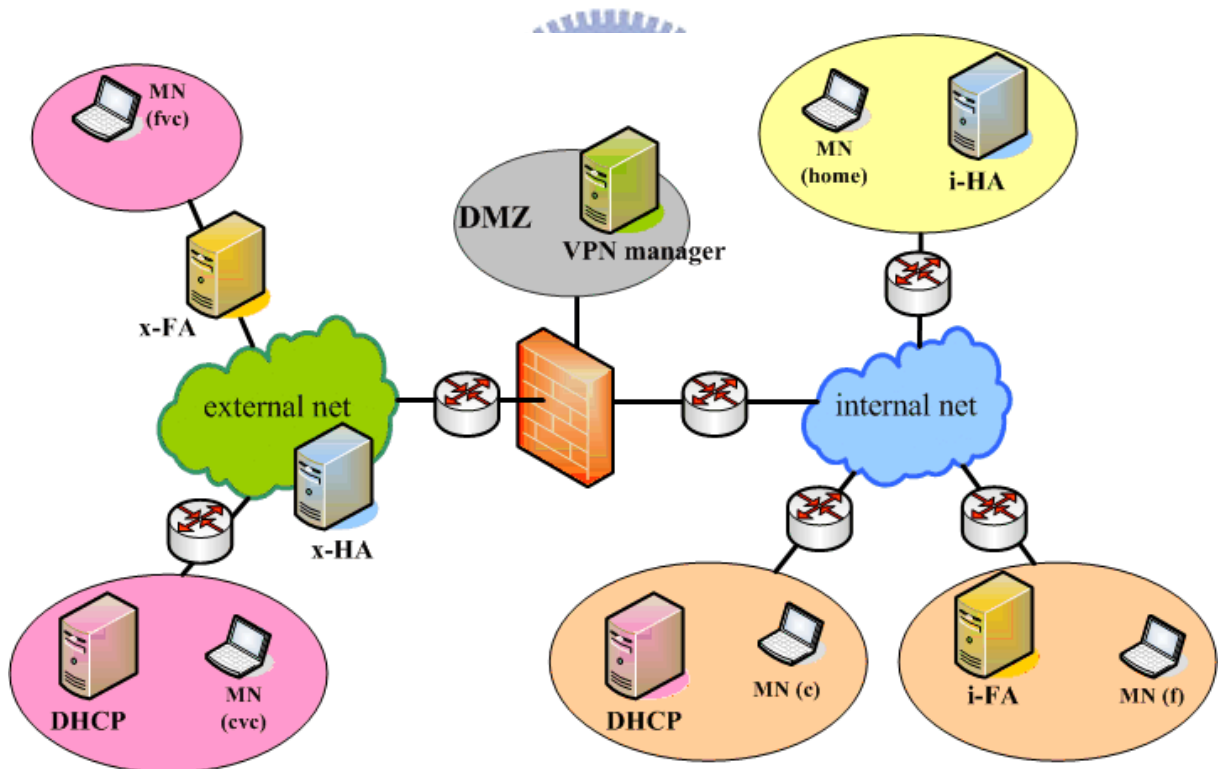


圖 2.5 Mobile IPv4 Traversal Across IPsec-based VPN Gateways 架構圖

右上角為 Home Network，MN 的 HA 所在之處，提供最內層的 Mobile IP，此 HA 被標記為 i-HA (Internal HA)。右下角兩個網域為 Intranet 中的 Foreign Network，MN 有可能在這些地方漫遊，這時 MN 只需執行最原始單純的 Mobile IP

即可，「(c)」表示使用 Co-located CoA，「(f)」則是 FA-CoA，視當地是否有 FA 而定。

左邊兩個網域屬於 External network，當 MN 在這些地方與 Intranet 通訊時，需要 IPsec 的安全性保護，而為提供 IPsec tunnel 的行動性，在最外面又加了一層 Mobile IP，這由部署在外面的 External HA (標記為 x-HA) 來提供服務。由於最外層是一般的 Mobile IP，所以可支援 Co-located 與 FA 模式。

「(fvc)」表示有三層 tunnel，最外層為 FA 模式的 Mobile IP，中間是 VPN tunnel (IPsec tunnel)，裡面為 Co-located 模式的 Mobile IP；「(cvc)」的差異在於，最外層是 Co-located 模式的 Mobile IP。

圖 2.6 為此架構中「(cvc)」模式的訊息流，當 MN 啟動時所需進行的動作，而移動時只需進行對 x-HA 的註冊。

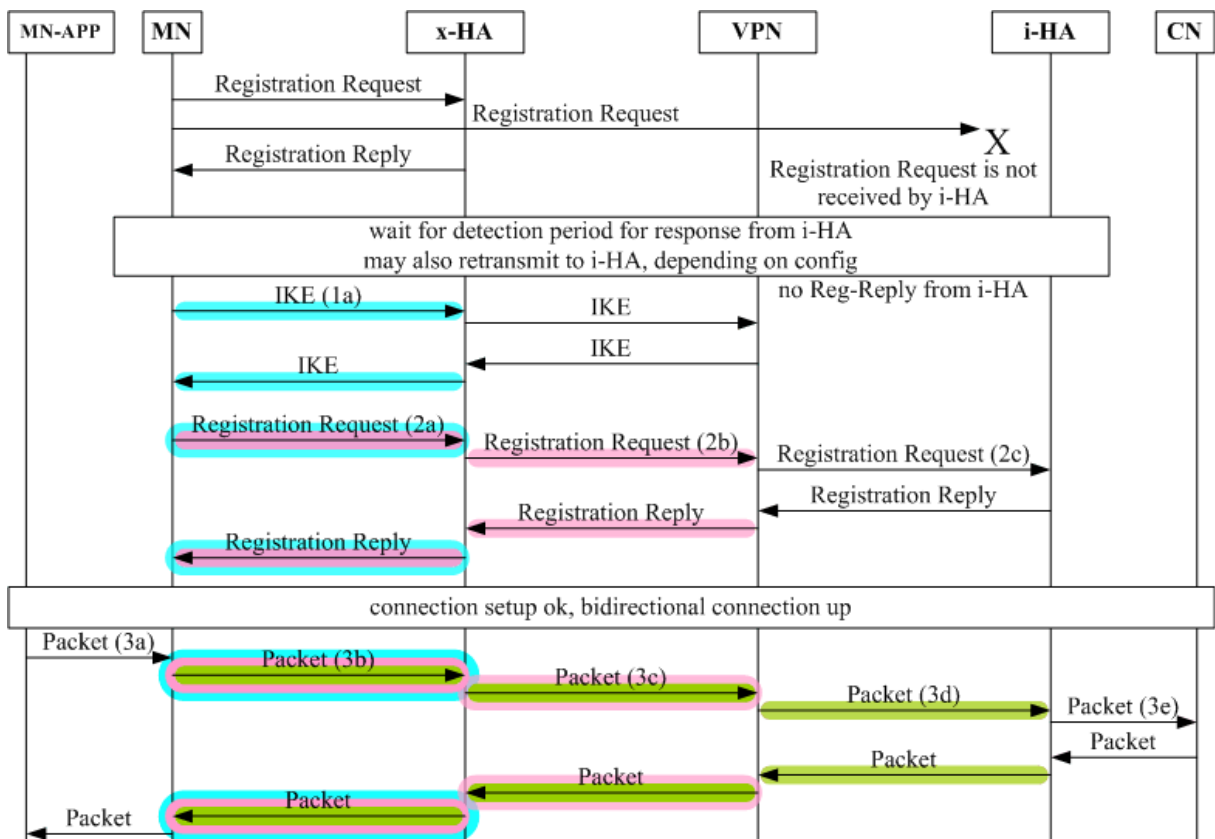


圖 2.6 Mobile IPv4 Traversal Across IPsec-based VPN Gateways 訊息流

MN 從最外層開始一層層建立通道 (tunnel)，完成以後，封包傳遞就如上圖中最下面，MN 必須處理三層的 tunnel。

圖 2.6 中在有些封包名稱之後會刮號「(1a)」，「(3c)」等等，這是對應下圖

(圖 2.7) 的封包格式。

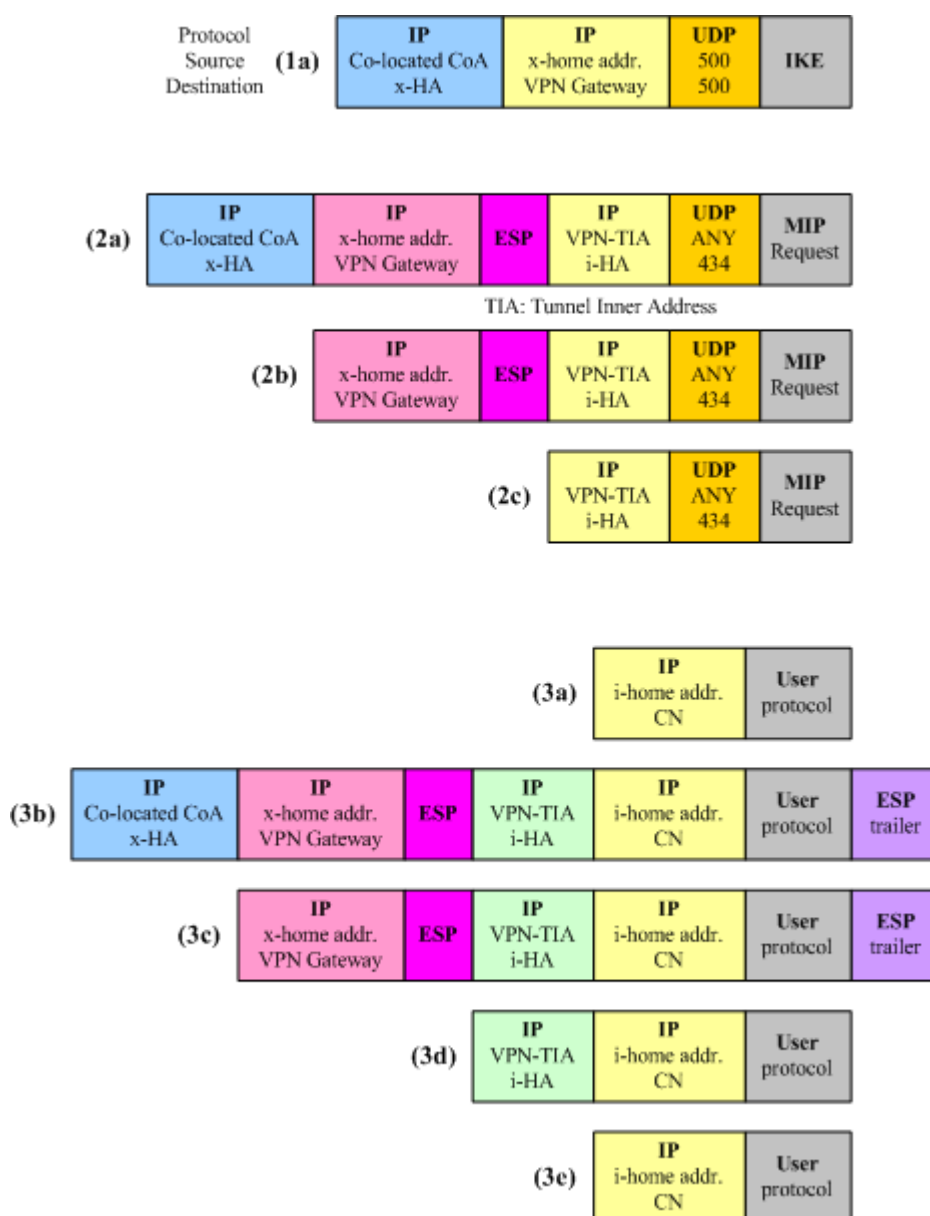


圖 2.7 Mobile IPv4 Traversal Across IPsec-based VPN Gateways 封包格式

2.5 行動代理人

行動代理人 (Mobile Agent) [8][9]，是一種可在各電腦之間移動，並同時能進行自主分散運算處理的程式。它可提高分散式計算系統的效率及便利性，也降低了傳遞延遲與電腦間的傳送次數。

行動代理人的基本原理，就是接受使用者交付的任務，並視情況於網路端點間移動，進行運算或發佈、收集資訊，最後將結果回傳給使用者。它具備自主性

(Autonomy) 與行動性 (mobility)，自主性是指代理人可掌控自己的行為與狀態，不受其他使用者或系統的干涉，它能夠獨立判斷收集到的情報，並藉此決定接下來的動作；

透過行動代理人，不需考慮網路架構就可實現分散程式設計 (distributed programming)，即使是通信失敗等例外，處理程序也可簡單化。

行動代理人可用獨自的程式語言來編譯，但也能使用現有的程式語言如 Java 等等。它可在各種不同硬體設備或 OS 的電腦上執行、移動。最主流的執行方式是使用常見的程式語言來描述行動代理人的動作，然後在執行機器上利用直譯器或虛擬機器來執行。

行動代理人有以下特性：

- **遠端分散式處理**

使用者可藉由行動代理人，壓縮分散式系統處理程式的程式碼，帶到遠端電腦上執行，如此可降低傳輸通訊量，減少網路負擔。而代理人對遠端電腦資源的使用與存取，可以提升效率和靈活性。

- **非同步處理**

傳統主從架構 (client-server paradigm) 中，client 和 server 需要一直保持連線；而行動代理人則在程式送到接收端後，傳輸的兩端就不需再保持連線，行動代理人獨自在接收端運作，大幅減低網路傳輸負擔。

行動代理人還有安全性上的顧慮，因為行動代理人可能會被經過或執行的機器所破壞，或是竊取、竄改其中的資訊；而執行的系統也會擔心被惡意的程式碼攻擊。對此已經有不少的研究方案被提出，像是限制系統資源與 API 的執行、變更程式後插入檢查碼[12]、傳送前的交互認證 [13][14]、機密資訊的加密...等等。

第三章 在行動虛擬私人網路下以行動代理人為基礎之無縫交遞

在本章節中，我會先建構出本系統的基礎架構 – 行動虛擬私人網路，並詳細描述其設定、目的與各元件的設計方法。然後繼續說明如何在行動虛擬私人網路下，以行動代理人來達成無縫交遞之目標。

3.1 行動虛擬私人網路之基本架構

圖 3.1 為本論文之系統基本架構圖，L2TP Network Server (LNS, VPN Gateway) 為 Intranet 對外唯一開道，所有進出的封包都要經由 LNS。這裡以 L2TP 作 VPN tunnel，此 tunnel 由 IPSec 保護。L2TP Access Concentrator (LAC) 管轄的範圍我們稱為 Foreign Intranet，雖不像 Intranet 具有實體部署上的安全性，但可藉認證授權與傳輸加密來取得類似的安全能力，即虛擬私人網路之概念。在 LAC 之下的行動端 (Mobile Node, MN) 經由 VPN tunnel (L2TP tunnel) 與 Intranet 之中的通訊端 (Correspondent Node, CN, 可能是伺服器或其他使用者) 連線，MN 與 LAC 之間的傳輸亦由 IPSec 保護。

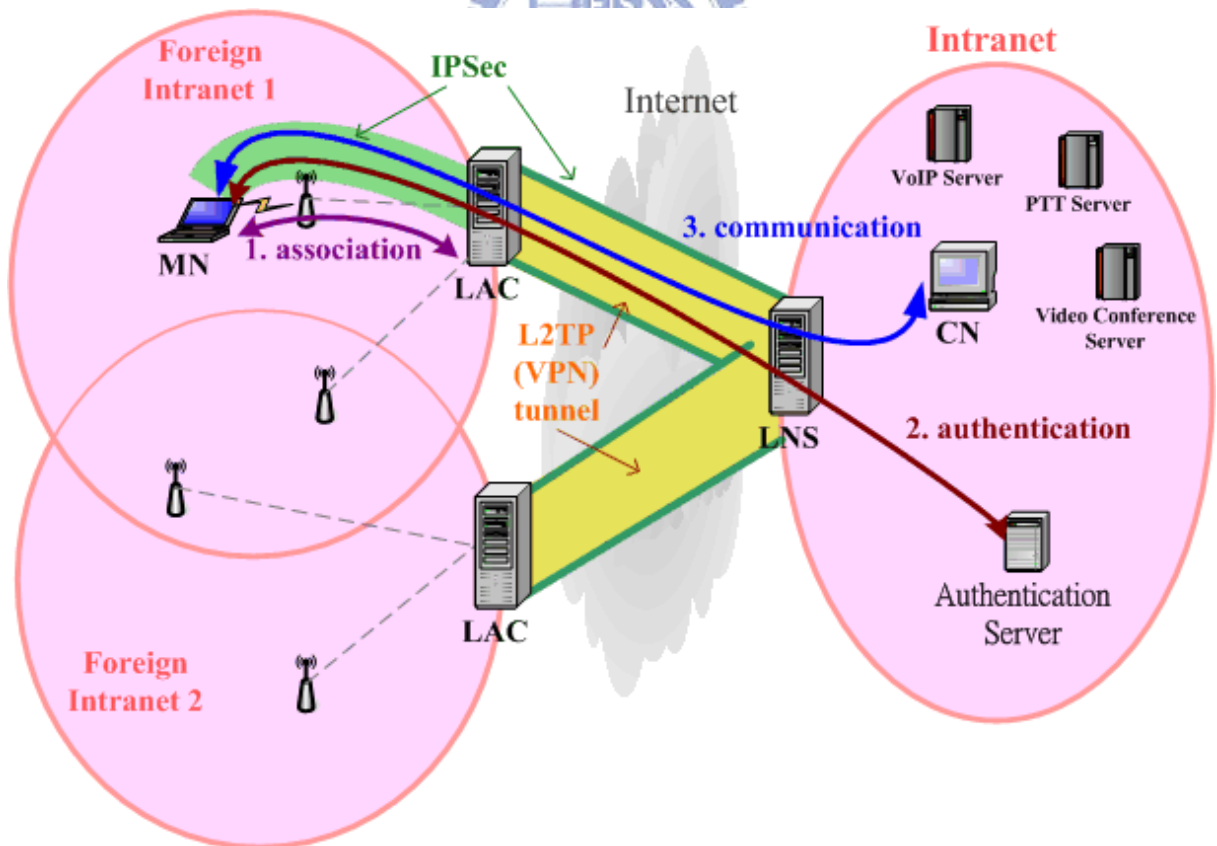


圖 3.1 行動虛擬私人網路基本架構

本系統希望讓 Mobile Node 得以漫遊於各 Foreign Intranet 以及 Intranet 之間，不但不會有連線中斷的感覺，還能保持 VPN 應有的安全性，如此可使企業成員在公司網路之外移動時，還能如同在公司內部一樣進行作業。

MN 在使用 L2TP tunnel 與 LNS 及 Intranet 內的端點連線前，必須先向認證伺服器 (Authentication Server, AS) 認證；LAC 讓未經授權的 MN 只被允許連向 AS。

3.2 行動虛擬私人網路之設計方法

本架構除了提供安全性外，這裡還利用來省去部分第三層換手 (Layer 3 handoff) 的時間，包含取得新 IP 位址、更新路由 (routing) 設定。

LNS 與 LAC 之間由固定存在且被 IPSec 保護的 L2TP tunnel 連接，在文獻規範與一般使用來說，VPN tunnel 兩端的網路位址集合只需不重複以致造成混淆即可，然而這裡我規定讓 Intranet 與 Foreign Intranet 共用一個位址集合，此集合可以是虛擬 IP 位址，如 10.*.*.*，這亦將 Intranet 與各 Foreign Intranet 連成了一個網域，IP 位址由 Intranet 管理、分配，每台機器或每個使用者均擁有專屬於自己的 IP 位址。

在這些網域移動的 Mobile Node (MN) 的 IP 位址是固定不變的，如此可避免切換到不同 LAC 網域時的第三層換手。除此之外，所有 LAC 與 LNS 對內的網路位址均相同 (例如：10.0.0.254)，省去 MN 更新 routing table 的動作。這樣一來，MN 將不會感覺到自己是在不同的網域間漫遊。

LNS 要在 Intranet 中利用 proxy ARP 代替 MN 收下封包，經由 L2TP/IPSec tunnel 轉送到 MN 所在的 LAC 下，LAC 與 MN 之間亦有 IPSec 保護；MN 也將要給 Correspondent Node (CN) 的封包以 IPSec 加密送出，LAC 收到解密後經 L2TP/IPSec tunnel 轉到 LNS，LNS 從 tunnel 中取出封包傳至 CN。如圖 3.2。

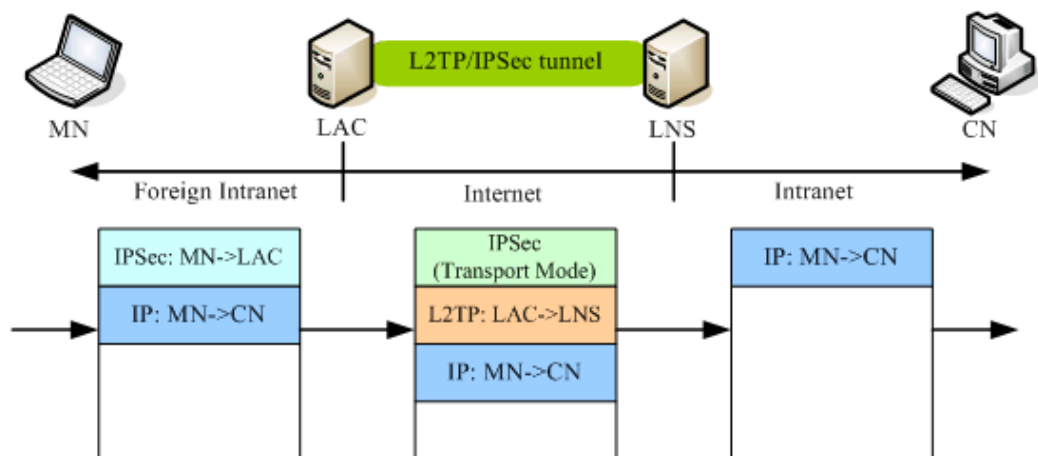


圖 3.2 虛擬私人網路通道傳輸

3.3 以行動代理人為基礎之無縫交遞機制

在第一章提到的換手時間中，還需要考慮：通知家網代理人以更新連線路徑、認證授權、建立安全連線，這部分我將使用行動代理人來進行，

在 2.5 節中，可以瞭解到行動代理人最重要的特性就是自主性和移動性，如此它可在遠端伺服器上，代替 MN 預先做出一些動作，如認證、建立連線、向 HA 註冊等等，如此這些動作將不會佔據交遞時間。

至於行動代理人最具爭議的安全性，在行動虛擬私人網路架構下，解決方案將變得簡單而不多餘，因為 MA 所經過與執行的伺服器，都屬於虛擬私人網路的一部份，而 VPN 本來就會對底下機器進行認證授權稽核，因此最麻煩的問題 -- 行動代理人與執行伺服器的互相信任，在上一節的架構之下已被自然而然解決了。傳送時的安全亦由行動虛擬私人網路所提供。

3.4 以行動代理人為基礎之無縫交遞機制的設計方法

以下我會依整個機制的流程順序來分節討論，並詳細說明各步驟中各元件需要做到的動作，以及希望達到的功能效果。

3.4.1 偵測訊號並送出行動代理人

當 MN 移動到無線訊號的邊緣時（偵測到訊號低於某設定的門檻），會啟動本交遞機制，這時 MN 開始掃瞄周遭的無線基地台，取得周圍有提供服務的 ESSID，

藉此得知附近有哪些屬於同一 VPN 的 LAC，然後送出行動代理人 (MAc) 到現在使用中的 LAC，並在行動代理人中指定那些鄰近 LAC，以及個別要送去的資料，再由現用 LAC 分送 (MAn)，這樣可節省無線網路中的傳輸量。MN 可以不知道這些 LAC 對 Internet 介面的位址 (public address)，只需指定 ESSID，讓現用的 LAC 根據對照表來轉送，此對照表需定期更新維護。

由於 MN 在連線 VPN 之前已經過認證，各 LAC 亦有 VPN 提供的認證，所以彼此間的信任沒有問題，行動代理人與執行系統在傳送與接收的階段，安全性交由 VPN 負責即可，幾乎沒有額外的負擔。至於執行時的安全性，各種行動代理人系統與機器、作業系統有各自的實作方式。

在這階段中，MN 依然保持與 CN 的連線，不需中斷，只是額外傳送了幾個行動代理人的封包。

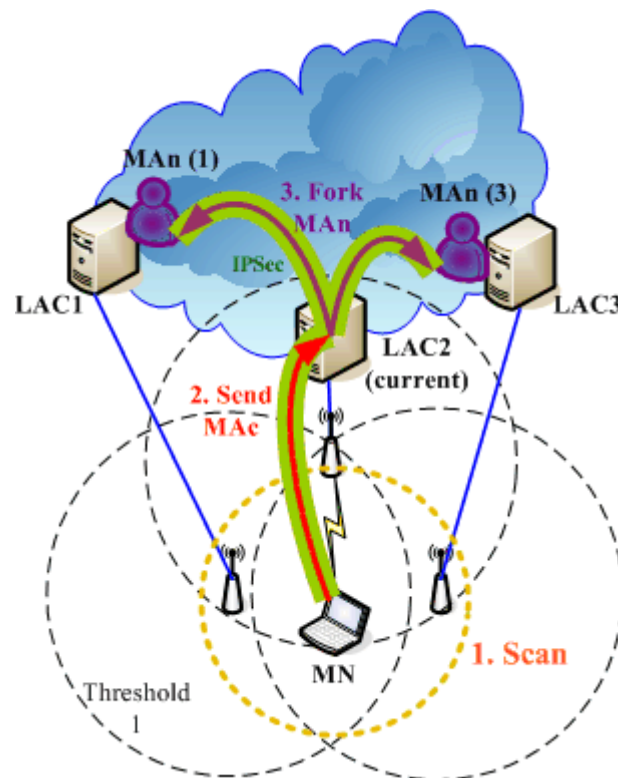


圖 3.3 MN 偵測訊號並送出行動代理人

3.4.2 行動代理人的動作

在上一節有提到，想要達成無縫交遞的目標，我們還有幾項時間必須考慮，包括認證授權、建立安全連線、通知家代理人以更新連線路徑，本系統準備利用行動代理人來預先完成這幾項動作，如此 MN 可省去這些交遞時間。

3.4.2.1 認證授權

原本是指取得 VPN 的認證授權，也就是向 Authentication Server (AS) 作完整認證動作，但 MN 在第一次連線前已經完成過一次，所以這裡的重點在於：確認行動代理人的身份，就是證明此 Mobile Agent 的確是 MN 的代理人。

為了安全性上的考量，不便讓行動代理人攜帶安全協定中的金鑰，於是這裡採用數位簽章來當作身份證明，換句話說，MN 簽署身份證明讓行動代理人得以向 AS 證明自己的身份。數位簽章所加密的內容必須是雙方都可取得、且要避免重送攻擊 (replay attack)，因此簽章內容可包含時間戳記 (timestamp)、MN 與 LAC 的 ID、一組由行動代理人一起攜帶的亂數等等，這類數位簽章的研究可在許多文獻中找到。

3.4.2.2 更新連線路徑

在 AS 通過行動代理人的認證後，會通知 LNS 與代理人所在的 LAC，讓他們曉得這個 Mobile Agent 的確是 MN 的代理人。

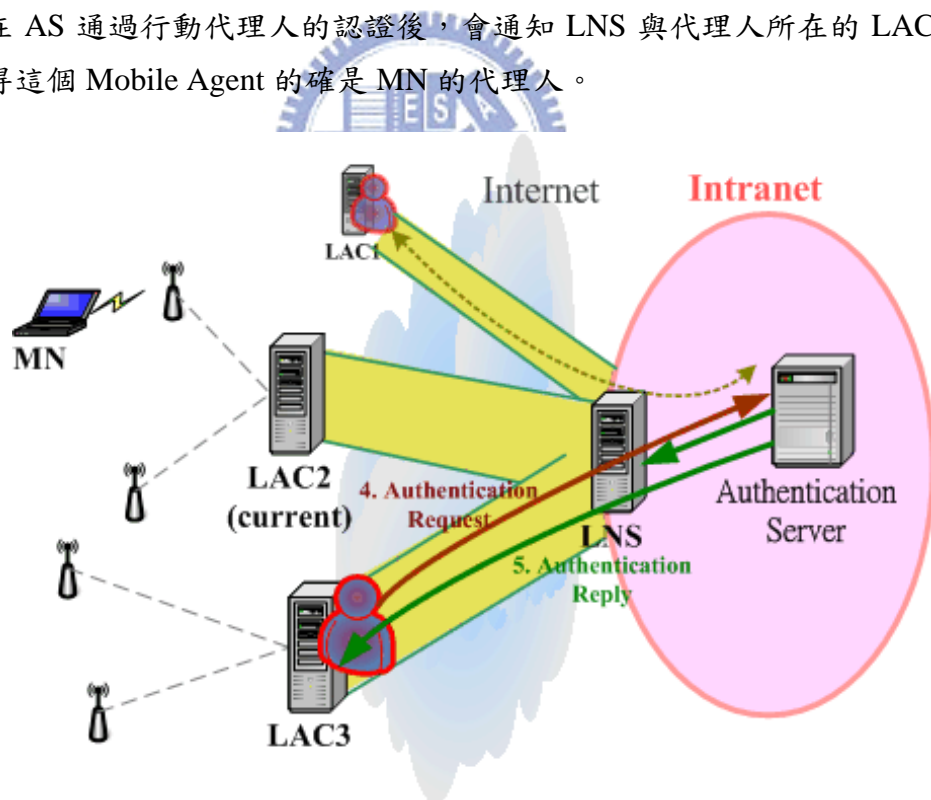


圖 3.4 行動代理人之認證與授權

LAC 會允許代理人繼續執行其他的動作，並解除對 MN 的管制，也就是讓 MN 可以透過它來連上 VPN。然後 Mobile Agent 可以繼續進行剩下的任務，如建立安全連線，與協調 QoS 等等。

在本系統中，LNS 其實就兼任了 MN 的家代理人，因此 LNS 必須要更新連線路徑，LNS 需要更新的是 binding list，在 Mobile IP 中 binding list 是記錄 MN 的 home address 與 CoA 之對照，這裡則是記著 MN 與他所在的 LAC。所以當 AS 告知 LNS 說 MA 已認證成功，LNS 就會在 binding list 中加上 MA 現在的 LAC 位址，但並未中斷之前與 MN 的連線，也就是使用 Multi-homing 的機制，讓 CN 與 MN 的連線同時繞經多條 VPN tunnel，讓 MN 只要在這些 LAC 之下，都可以保持與 CN 的連線。

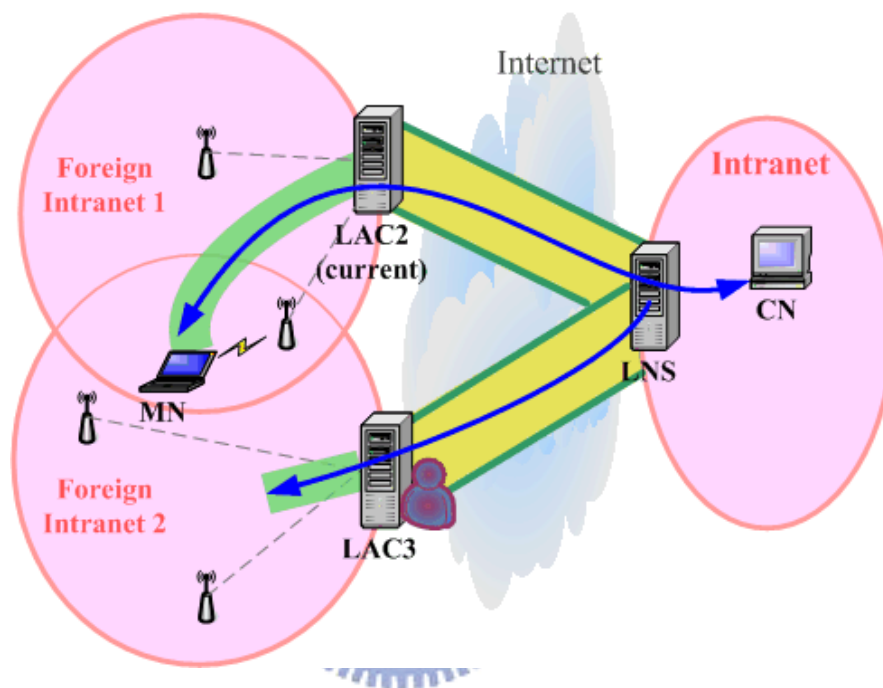


圖 3.5 Multi-homing

雖說是 Multi-homing，但只看端點位址的話其實是 Uni-casting，因為這許多路徑的兩個端點都是 LNS 與 MN。

3.4.2.3 建立安全連線

在 LAC 接受 multi-homing 之前，MA 必須先跟 LAC 建立好 IPsec association，彼此間必須交換好加解密等安全連線所需的金鑰，這樣 LAC 才能安全地轉接 LNS 與 MN 的通訊連線；MN 也才能在第二層換手 (Layer 2 handoff) 後立即用 IPsec 保護與 LAC 之間的傳輸。

除此之外，行動代理人也能同時進行一些溝通協調，如服務品質保證 (Quality of Service, QoS)，或其他擴充性服務。對於多媒體即時通訊，QoS 的協調十分重要。

利用行動代理人來建立安全性連線，與一般流程有些不同。在網路上建立安全連結時，必須設法避免網路上的攻擊，如重送 (replay attack)、偽裝、竊聽、截斷、破壞等等，因此在通訊時會使用許多像時戳 (timestamp)、臨時亂數 (Nonce)、加密、整體確認值 (Integrity Check Value, ICV)、識別碼等機制。但是行動代理人與執行系統的通訊全都在單機電腦上執行，只要作好系統安全，就不需顧慮到建立連結時網路傳輸的被攻擊可能。使用行動代理人不止可以提高效能，也可提升安全性。

行動代理人在安全性上的顧慮是，它要經由網路送到執行的電腦上，因此不能攜帶私密金鑰等不該出現於網路上的東西，但是上面有提到使用行動代理人可省去很多安全性步驟，這可讓代理人不需攜帶金鑰也能完成安全連結 (Security Association)。需要保護的只有傳送的行動代理人，與代理人回傳的訊息。

```
I → R: CKYI, OK_KEYX, GRP, gx, EHAO, NIDP, IDI, IDR, NI, SKI[IDI || IDR || NI || GRP || gx | EHAO]
R → I: CKYR, CKYI, OK_KEYX, GRP, gy, EHAS, NIDP, IDR, IDI, NR, NI, SKR[IDR || IDI || NR || NI || GRP || gy || gx | EHAS]
I → R: CKYI, CKYR, OK_KEYX, GRP, gx, EHAS, NIDP, IDI, IDR, NI, NR, SKI[IDI || IDR || NI || NR || GRP || gx || gy | EHAS]
```

- I = 發起者
- R = 回應者
- CKY_I, CKY_R = 發起者與回應者的 cookie
- OK_KEYX = 鑰匙交換訊息的類型
- GRP = 此交換訊息所採用的 Diffie-Hellman 群組的名稱
- g^x, g^y = 發起者與回應者的公開鑰匙；g^{xy} = 此次交換的通訊鑰匙
- EHAO, EHAS = 提供與選取的加密演算法、雜湊函數，以及確認函數
- NIDP = 用來指出不會對訊息的剩餘部分加密
- ID_I, ID_R = 發起者與回應者的 ID
- N_I, N_R = 發起者與回應者針對此次交換所產生的隨機臨時亂數
- S_{KI}[X], S_{KR}[X] = 利用發起者與回應者的私密鑰匙，對 X 簽署後所產生的簽章

圖 3.6 積極式 Oakley 鑰匙交換法

以上圖「積極式 Oakley 鑰匙交換法」[17][20] 為例，若使用行動代理人來進行，則可省去 cookie、隨機臨時亂數、簽章與加密，行動代理人只需攜帶 OK_KEYX、GRP、g_x、EHAO、ID，然後在建立安全連結後回傳 g_y、EHAS 即可，中間傳輸的加密與彼此身份的認證，則由 VPN 來負責。

3.4.3 第二層換手之後續動作

當前面的前置動作都已完成，MN 就可在第二層換手後，繼續保持原來的通訊連線，但是還有一些後續動作要作，除此之外，以下也會說明如何接續第三層連線。

3.4.3.1 維持第三層連線

因為 Multi-homing 的關係，MN 在移動到新的 LAC 下時，立刻可接收到來自 CN 的封包，同時自己傳給 CN 的封包也可被 LNS 接受。但是還有一個問題需要考慮，就是 MN 如何使用行動代理人預先建立的 IPSec 連結，也就是 MN 要怎樣在第三層與 LAC 溝通。

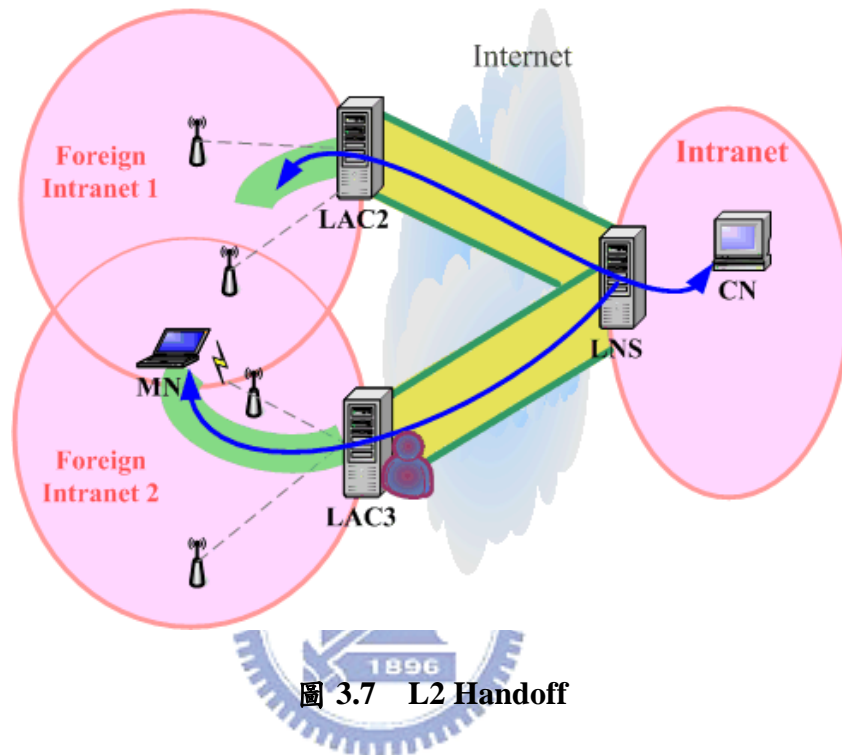


圖 3.7 L2 Handoff

IP 位址在行動虛擬私人網路的架構下不成問題，MN 不需改變 IP 層位址，而因 LAC 對內位址一致，所以也不用改路由表 (routing table)，但是 MN 與 LAC 必須使用新建立的 IPSec 通道，MN 要能選擇使用正確對應的加解密機制。

IPSec 最基本的概念是安全連結 (Security Associations, SA)，每個單向的聯繫使用一個 SA，SA 可由安全參數索引 (Security Parameters Index, SPI)、IP 目的端位址、安全協定來辨識，在本系統中，對新舊 LAC 的 IPSec 連線目的端位址是相同的，但仍可由 SPI 來辨別，所以 MN 在接收到新的 LAC 傳來的加密封包，可借封包標頭中的 SPI 來選擇使用正確的解密方式。

而 MN 在送出封包時也要選擇 SA，這可在安全連結資料庫 (SPD，用來將 IP 訊息與特定的 SA 結合在一起) 中，加入一個 ESSID 的參數來當索引。當行動代理人建立好安全連結後，回傳給 MN，MN 則在資料庫中將 SA 與 ESSID 作對應，如此就可在發送封包時選擇正確的 SA。

3.4.3.2 接受行動代理人之任務回報

行動代理人在完成任務後，應該要向委託人 MN 報告結果，除了上面的安全連結外，還有認證授權稽核等等 VPN 相關的記錄，以及 QoS 的協調結果，或其他擴充性的服務項目。

這個動作可在 MN 移動到新的 LAC 下時，由 MN 主動通知行動代理人，讓代理人回傳報告。此動作與 MN-CN 的通訊無關，是同時平行處理的。

任務回報完畢後，行動代理人可進行自我刪除。

3.4.3.3 更新位置表

上述所有動作結束後，就要作最後收尾，將狀態回復成執行本交遞機制前的樣子。MN 這時會發出位置對應更新 (Location Binding Update) 給 LNS，LNS 收到之後先轉送給所有 binding list 上 MN 所對應的 LAC，接著更新 binding list，將 MN 對應的 LAC 只留下現在所用的，並取消 Multi-homing。

LAC 接到 LNS 轉送來的的位置對應更新，就會刪除上面執行的 MN 的行動代理人，並回復對 MN 位址的管制。

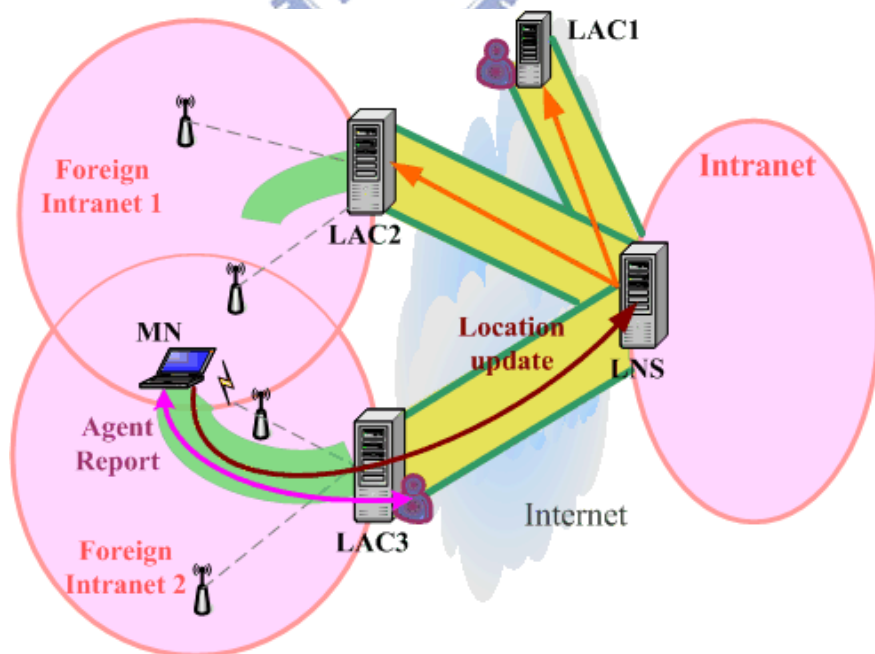


圖 3.8 Location Binding Update

3.5 在行動虛擬私人網路下以行動代理人為基礎之無縫交遞流程

完整的運作過程如下圖所示：

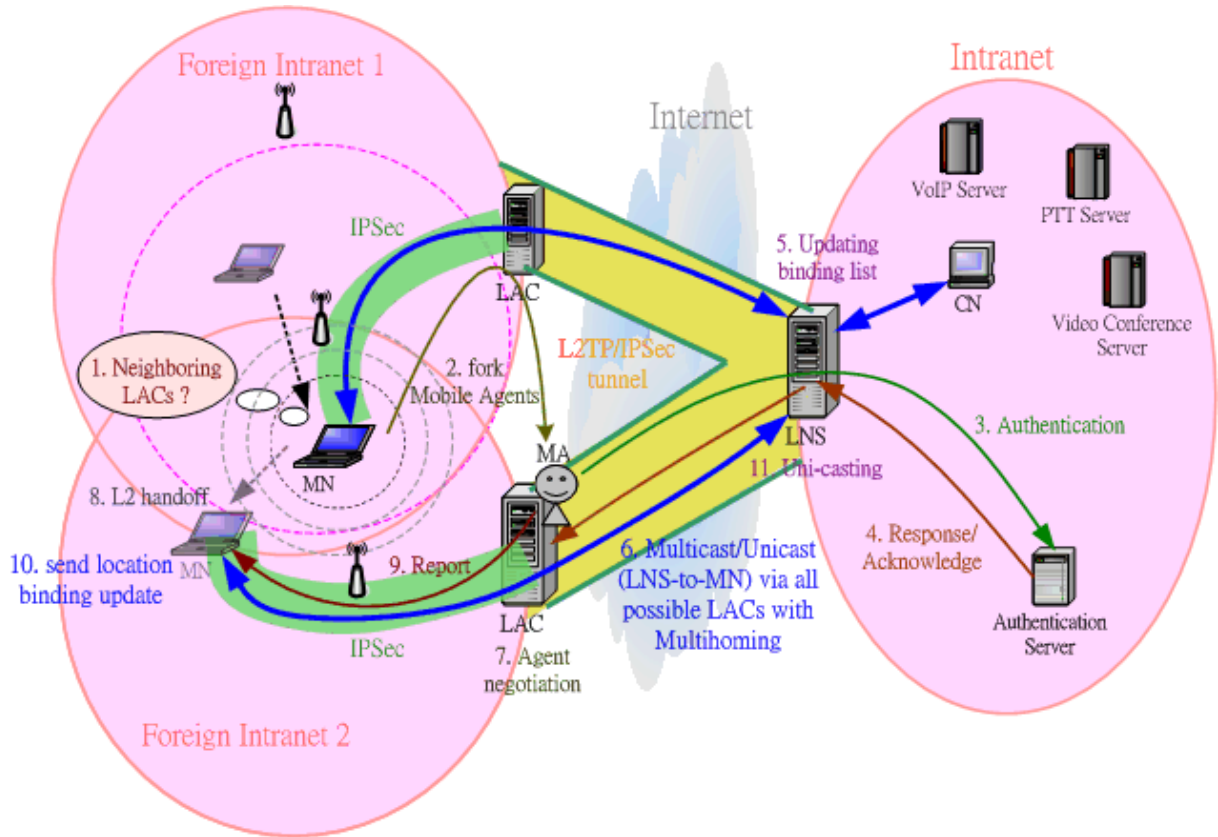


圖 3.9 在行動虛擬私人網路下以行動代理人為基礎之無縫交遞機制運作圖

1. Detect Neighboring LACs:

當 MN 發現無線訊號降低至某一門檻時，開始掃瞄周圍 AP 的 ESSID，藉此得知有哪些 LAC。

2. Fork Mobile Agent:

經由現用 LAC 轉交，MN 將行動代理人送到那些 LAC 上。

3. Authentication:

行動代理人向認證伺服器 (AS) 證明自己是 MN 的代理人。

4. Response/Acknowledge:

AS 確認 MA 的身份後，告知 LNS 與 LAC。

5. Updating binding list:

收到 AS 的通知後，LNS 更新記錄中 MN 所在的 LAC。

6. Multi-casting:

LNS 將 CN 與 MN 的連線，tunnel 經那些 binding list 中記錄的所有 LAC。

7. Agent negotiation:

行動代理人需要代表 MN 跟 LAC 建立安全連結 (Security Association)，還有協調服務品質保證 (QoS)，或其他擴充性服務。

8. L2 handoff:

在上面動作完成後，MN 即可在第二層換手完立即延續之前與 CN 的通訊，MN 會選擇正確的安全連結來與新的 LAC 連線。

9. Agent Report:

MN 移動到新的 LAC 下後，就可向當地的代理人要求任務回報，取得所需要的資訊。



10. Location binding update:

接下來 MN 需告知 LNS 他的新位置，讓 LNS 更新 binding list 並改成 Uni-casting。LNS 在更新 binding list 前先通知 list 上的所有 LAC，讓這些 LAC 可以刪除上面 MN 的行動代理人，並回復對 MN 的管制。

下圖為本系統之訊息流：

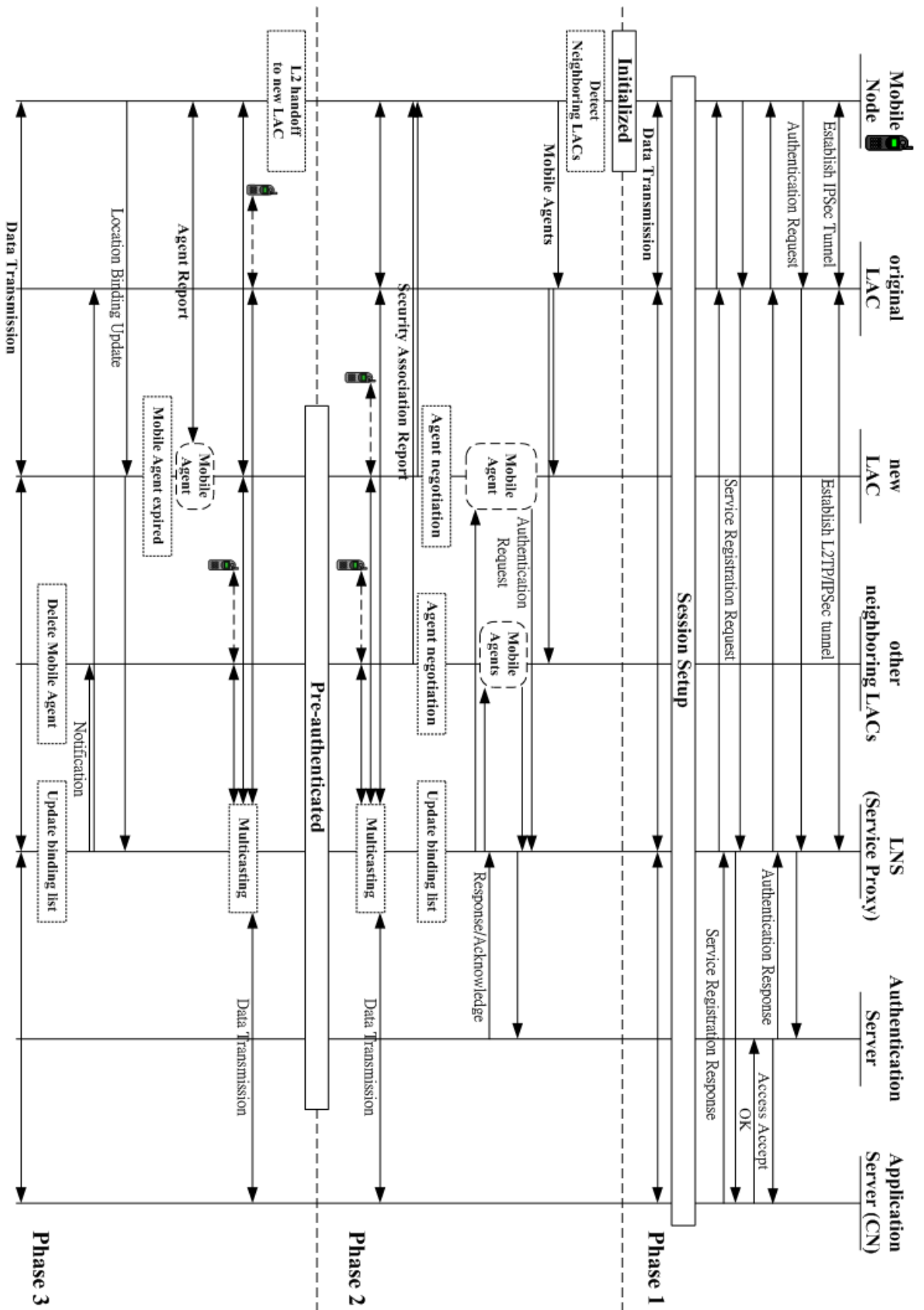


圖 3.10 Message Flow

上圖中我將流程分為三個階段，第一階段是建立行動虛擬私人網路基本架構，包含 LNS 與 LAC 間的通道設立、MN 對 AS 的認證、MN 向 CN 要求連線；第二階段為交遞流程中，在 MN 進行 L2 handoff 前的步驟，從偵測訊號變低，到行動代理人完成任務；第三階段是從 MN 的 L2 handoff 開始，到完成後續動作，回復第一階段最後的狀態。



第四章 在行動虛擬私人網路下以行動代理人為基礎之無縫交遞實作

在這一章中，我將會說明本系統的實作內容，先列出基本的軟硬體需求，然後就各項主要功能作詳細介紹。

4.1 系統之軟硬體需求

在行動虛擬私人網路下以行動代理人為基礎之無縫交遞的系統架構中，包含四個主要實體元件：Mobile Node、L2TP Network Server、L2TP Access Concentrator、Authentication Server。本節介紹這些元件的軟硬體需求：

- **Mobile Node (MN)**

硬體需求：支援無線訊號掃描的無線網路卡

作業系統：Red Hat 9.0 [18]

軟體需求：虛擬私人網路的成員

行動代理人系統之委託人

可與 LAC 建立 IPSec 通道

- **L2TP Access Concentrator (LAC)**

硬體需求：對外與對內介面的兩張網路卡

作業系統：Red Hat 9.0

軟體需求：VPN 通道的 client 端

行動代理人之執行系統

與底下機器建立 IPSec 通道

- **L2TP Network Server (LNS)**

硬體需求：對外與對內介面的兩張網路卡

作業系統：Red Hat 9.0

軟體需求：VPN Gateway (防火牆、閘道器)

VPN 通道的 server 端

Multicasting 的能力

部分 Mobile IP 中 Home Agent 的功能

- **Authentication Server (AS)**

作業系統: Red Hat 9.0

軟體需求: 為 Mobile Node 與 Mobile Agent 提供認證服務

4.2 偵測 ESSID

在較新的無線網路卡韌體中，會提供掃描周圍無線訊號的指令介面，每家公司的介面與執行動作不盡相同，以 Z-Com I-300 為例，可以使用下面的指令：

- iwlist [interface] scan

如此可得到關於無線訊號的許多訊息，然後我們必須要從裡面取出需要的東西，在此我們只需要 ESSID。為了辨識此 ESSID 是否為 Mobile VPN 的成員，ESSID 建議包含辨認用的字串。

4.3 Mobile Agent



以下先列出在這個功能項目中，系統各元件所要做到的動作，然後說明如何達成。

- **MN**

- 完成偵測動作後，送出 MA 到現用的 LAC。
- 接收 MA 回傳的安全連結參數。
- phase 3 時啟動與 MA 的 secured report。

- **LAC**

- 隨時準備幫 MN 轉送行動代理人給其他 LACs。
- 預備好平台來接收 MA，讓 MA 得以在上面執行。
- 收到 LNS 來的 location binding update 通知後刪除 MA。

- **MA**

- 夾帶足夠的資訊到 LAC 上的平台執行。
- 代表 MN 向 LAC 做出溝通與協調。
- 對 AS 進行認證流程。
- 認證完畢準備向 MN 作 secured report。

- report 結束後自我刪除。

Mobile Agent 本身使用 TLV (Type-Length-Value) 的格式，內容包含

- 目的地及自身的 ID
- 認證用 payload，如亂數、時戳、數位簽章
- 連結用程式碼

● 現用 LAC 轉送

LAC 在 private 介面的連接埠收到行動代理人時，會先依目的地分裝成多個 MA，每個 MA 攜帶要到各自目的地執行的資料。接著在內建的對應表中找出各 ESSID 的相對 Public IP Address，然後藉此轉送到目的 LAC，途中有 LAC 間的 IPsec 連線保護。

● 簽章認證

LAC 在 public 介面接收到後，先將認證用的 payload 取出，送給 AS，其中包含了 MN 的 ID、LAC 的 ESSID、臨時隨機亂數、timestamp，以及用前面那些資訊做出的數位簽章。

公開與私密金鑰以及簽章、認證的動作，都是使用 OpenSSL 函示庫 [19]，在 MN 剛啟動的第一次認證時（可使用任意認證方式，如 EAP-SIM），MN 會同時產生私密與公開金鑰，並將公開金鑰傳給 AS 儲存。

- 產生私密金鑰：`openssl genrsa -out [output file1]`
- 產生公開金鑰：`openssl rsa -in [私密金鑰] -pubout -out [output file2]`

簽章時先讀出私密金鑰 (Private Key)，使用 `PEM_read_RSAPrivateKey()` 函數。然後將要包裝的資訊以 OpenSSL 的 `MD5()` 雜湊函數做成文摘，再以 `RSA_sign()` 簽章此文摘。

認證時用 `PEM_read_RSA_PUBKEY()` 讀出 MN 公開金鑰 (Public Key)，根據 payload 中附的 MN ID 選擇 Key file。再來以 `MD5()` 做出文摘，再使用 `RSA_verify()` 驗證。

● 建立安全連結

通過認證後，LAC 取出程式碼的部分，將它獨立成一個檔案並編譯、執行，之後 MA 可以代替 LAC 來設定 IPSec 連結，讓 LAC 得以和 MN 溝通，但為了 LAC 的安全性，LAC 要另外提供介面給 MA 來下命令，這樣可以管制 MA 動作的合法性。

4.4 Multicasting

要做到 Multicasting，必須要攔截從 CN 過來、送給 MN 的封包，並將這些封包複製後傳進指定的 tunnel 中。

於是我們要 hook 一支 driver，截下從內部網路送來的封包，然後根據目的位址來做事。Binding list 以 ioctl 函數送給此 driver，當 driver 看到要給 MN 的封包，就會依 binding list 複製幾份，填好 IP header 後送往 LAC。送出的封包會照 routing rule 來啟動 tunnel 介面。

LAC 收到時，解開外層的 tunnel 包裝，接收 LNS 上 driver 送來的封包，取出裡面 CN 要給 MN 的封包，由 raw socket 送出。

至於 MN 給 CN 的封包則不需特殊處理。



第五章 效能分析

5.1 交遞效能分析

下圖比較了傳統 VPN 下的行動使用者、IETF 提出的 VPN 與 Mobile IP 結合之機制，以及本論文之交遞系統，在進行網域切換時的通訊中斷時間。

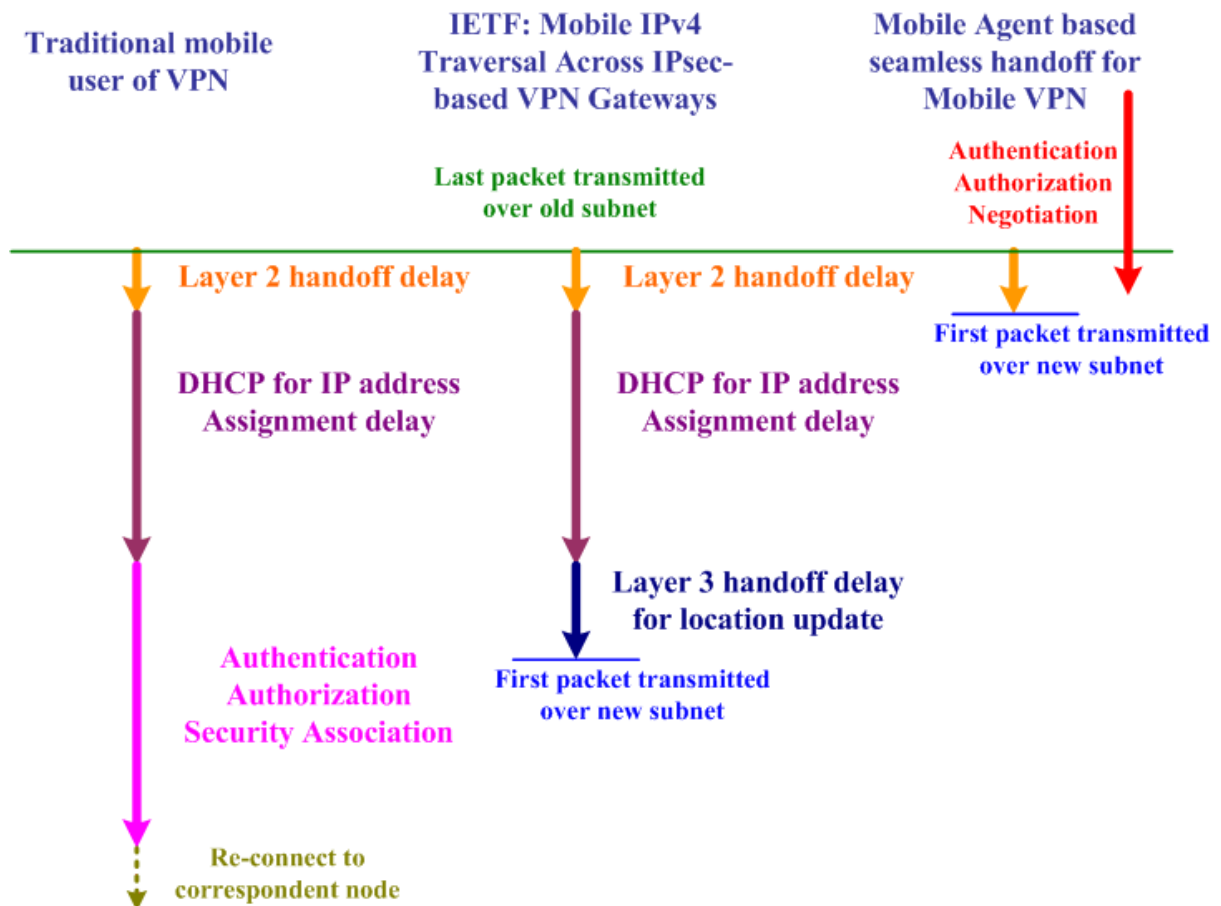


圖 5.1 交遞效能比較

傳統 VPN 使用者在更換網域時，必須先取得新的 IP 位址，然後在新網域以新位址向 VPN Gateway 認證及註冊、建立新的安全連線，而且因為使用的是新 IP 位址，所以無法保持原先的通訊連線，必須重建。

在 IETF 提出的機制中，行動端依然要先取得新網域位址，然後以這位址向最外層的 Mobile IP 註冊，但是 IPsec 安全連線因為最外層的 Mobile IP 而不需重建；與通訊端的連線則因最內層的 Mobile IP 而不需重新連線。

然而本系統的行動虛擬私人網路架構省去了第三層取得新位址的時間，另外

行動代理人代替行動端預先完成了安全認證與協調，並藉由 binding list 及 multicast 機制讓行動端一進入新網域就可以接續先前的通訊連線，所以僅有第二層換手的中斷時間。




第六章 結論與未來工作

6.1 結論

在本篇論文中，我設計了一個行動虛擬私人網路架構，並利用行動代理人、Mobile IP 機制、multicast 來實作一套可兼顧安全性的無縫交遞機制，且同時盡可能降低網路負擔。

為了保障通訊傳輸的安全，這裡採用 VPN 架構來保護所有成員，同時作了一些設定使行動端不需進行第三層換手動作，省去重新要求 IP、設定路由等時間。另外採用了行動代理人幫行動端預先完成安全性認證、協調，並以 binding list 與 multicast 來建立新的通訊管道，讓行動端一進入新網域就得以接續先前的通訊連線。如此一來，行動端感覺到的通訊中斷僅有第二層換手的時間，而且過程中都維持著安全性保障。行動代理人最大的安全性爭議，亦在虛擬私人網路架構中自然地解決。

6.2 未來工作



目前的設定是將行動代理人送到所有鄰近的 LAC 上，但是這樣一來，當 MN 數量太多時，身為行動代理人平台的 LAC 運算量會很大，LNS 與 AS 則不斷接受行動代理人的要求，同時 multicast 也會提高 VPN tunnel 中的傳輸負擔。所以我希望可以再加上行動預測的機制，預測行動端的未來移動，評估哪些 LAC 才需要送出行動代理人，如此可大幅降低行動代理人的數量，進而提高系統效能。

另外系統中有設定一個很重要的訊號門檻 (threshold)，就是啟動無縫交遞機制的時機。threshold 太高會使交遞機制啟動頻繁，甚至增加許多不必要的啟動，提高負擔；太低則可能會讓交遞機制太晚啟動而來不及完成，或影響通訊品質。所以這個值的設定需要更詳盡的計算與測量。

參考文獻

- [1] C. Perkins, Ed., “IP Mobility Support for IPv4”, IETF RFC3344, August 2002.
- [2] S. Kent and R. Atkinson, “Security architecture for the internet protocol”, IETF RFC 2401, November 1998.
- [3] S. Vaarala, et al., “Mobile IPv4 Traversal Across IPsec-based VPN Gateways (draft-ietf-mobileip-vpn-problem-solution-00)”, Internet-Draft, January 2003.
- [4] F. Adrangi, et al., "Problem Statement: Mobile IPv4 Traversal of VPN Gateways (draft-ietf-mobileip-vpn-problem-statement-req-01)", Internet-Draft, January 29, 2003.
- [5] W. Townsley, A. Valencia, A. Rubens, G. Pall, G. Zorn, and B. Palter, “Layer Two Tunneling Protocol "L2TP" “, IETF RFC2661, August 1999.
- [6] Charlie Scott, Paul Wolfe, and Mike Erwin, Virtual Private Networks, 1st edition, O’Reilly, US, March 1998.
- [7] S. Kent, R. Atkinson, “Security Architecture for the Internet Protocol”, IETF RFC 2401, November 1998.
- [8] 楊柏華，「行動代理人技術 (上)」，計算中心通訊，第 18 卷第 23 期，中央研究院計算中心，民國 91 年 11 月 4 日。
- [9] 楊柏華，「行動代理人技術 (下)」，計算中心通訊，第 18 卷第 24 期，中央研究院計算中心，民國 91 年 11 月 18 日。
- [10] F. Adrangi, Ed., “Problem Statement: Mobile IPv4 Traversal of VPN Gateways (draft-ietf-mip4-vpn-problem-statement-03)”, Internet-Draft, October 4, 2004.
- [11] S. Vaarala, et al., “Mobile IPv4 Traversal Across IPsec-based VPN Gateways (draft-ietf-mip4-vpn-problem-solution-01)”, Internet-Draft, January 5, 2005.
- [12] Wehbe, R.; Lucco, S.; Anderson, T. E.; Graham, S. L., ”Efficient Software Based Fault Isolation”, Proceedings of ACM Symposium on Operating System Principles, pp.203-216, 1993.
- [13] Eung-Gu You, Keum-Suk Lee, “A Mobile Agent Security Management”, 18th



International Conference on Advanced Information Networking and Application, 2004.

- [14] Vigana, G.(ed), “Mobile Agents and Security”, Lecture Notes in Computer Science, Vol.1419, 1998.
- [15] B. Patel, et al., “Securing L2TP using IPsec”, IETF RFC 3193, November 2001.
- [16] B. Aboba, et al, “Extensible Authentication Protocol (EAP)”, IETF RFC 3748, June 2004.
- [17] William Stallings, 密碼學與網路安全 – 原理與實務, 第二版, 巫坤品、曾志光譯, 碁峰資訊股份有限公司, 台北市, 民國九十一年一月。
- [18] Red Hat Linux, <http://www.redhat.com/>
- [19] OpenSSL, <http://www.openssl.org/>
- [20] H. Orman, “The OAKLEY Key Determination Protocol”, IETF RFC 2412, November 1998.

