國立交通大學

資訊工程系

碩 士 論 文

一支援跨網路預先認證的階層式移動網路之設計與實作

Design and Implementation of a Hierarchical Mobile Network with an Inter-Network Pre-Authentication Mechanism

研 究 生：方健安

指導教授：曾建超　教授

中 華 民 國 九 十 三年 七 月 十 二 日

一支援跨網路預先認證的階層式移動網路之設計與實作

研究生：方健安　　指導教授：曾建超 博士

國立交通大學

資訊工程研究所碩士班

摘要

隨著無線網路的技術發展成熟，在大眾運輸工具上利用無線網路連結網際網路，使用網際網路服務必定會成為未來的趨勢。然而大眾運輸工具會搭載許多乘客，如果使用者各自使用無線網路上網，並且利用 Mobile IP 通訊協定保持網路連線不中斷，則當大眾運輸工具移動時，使用者需自行執行 Mobile IP 的註冊，由於大眾運輸工具的移動頻繁，會造成網路交遞（handoff）的機率增加，在每次進行網路交遞時，如果每位使用者都要自行進行 Mobile IP 的註冊，則會產生大量的網路傳輸。此外網路應用程式也會因為網路交遞的機率增加，而使得網路應用程式的效能變低。

為了解決註冊封包產生大量網路傳輸量的問題，我們採用 Mobile Network（MONET）網路架構的觀念，以 Mobile Router（MR）為 MONET 的行動管理者。當 MONET 移動時，由 MR 負責整個 MONET 的 Mobile IP 註冊機制，MONET 內的網路節點則不需要再各自執行註冊的動作，以減少註冊時所造成的網路傳輸量。然而原先的 Mobile IP 通訊協定是針對單一移動節點的行動管理，對於整個 MONET 的行動管理雖有提及但並不完全適用。因此我們必須針對原先 Mobile IP 通訊協定的註冊機制稍作修改，以達成建構 MONET 的目的。另外，當一個 MONET 的行動節點(Mobile Node； MN)本身是另一個 MONET 的 MR 時，便形成一個階層式的移動網路，所以我們在建構 MONET 時，也需要考量到階層式移動網路的情況。

為了降低網路交遞對網路應用程式效能的影響，我們提出一套適用於階層式移動網路的「跨網路預先認證機制」，利用此機制可以加快 MONET 存取點的交遞，降低網路延遲，減少交遞對應用程式效能的影響。在跨網路預先認證機制中，我們會架構一台位置伺服器記錄存取點的位置，在進行交遞動作之前，MR 會根據自己目前的位置，以及位置伺服器所紀錄的存取點位置及資訊，取得可能會到達的存取點資訊，並由目前所使用的存取點轉送認證成功的訊息給這些存取點。當 MR 真正到達這些存取點時，MR 就不需要再進行後端的網路認證，而直接可使用新存取點的網際網路服務，加速交遞的速度。

最後，我們實作出一套包含階層式移動網路以及跨網路預先認證機制的系統雛型，以驗證我們的方法。實作結果證明，我們的方法確實可行。

Design and Implementation of a Hierarchical Mobile Network with an Inter-Network Pre-Authentication Mechanism

Student: Chien-An Fang Advisor: Dr. Chien-Chao Tseng

Department of Computer Science and Information Engineering

Abstract

As wireless network and terminal technologies advance, it is becoming possible for the passengers of the public transportation to access Internet using mobile devices with wireless network adapters. Besides, mobile devices may be equipped with Mobile IP (MIP) protocol to retain continuous connectivity when the public transportation moves. Therefore, when the public transportation enters the coverage area of a new access point, each mobile device needs to exercise a MIP registration procedure itself. However such MIP registration procedures may incur too much network traffic because a public transportation vehicle is likely to carry many mobile users and move frequently. Besides, the latency of MIP registrations will significantly affect the performance of network applications.

In this thesis, we adopt the concept of Mobile Network (MONET) to reduce the number of MIP registrations and a location-based pre-authentication to shorten the latency of MIP registrations. A MONET consists of a Mobile Router (MR) and all hosts attached to the MONET. The MR of a MONET is equipped with at least one wireless network adapter and provides Internet connectivity to all hosts attached to the MONET. When a MONET moves, only the MR of the MONET needs to perform MIP registration procedure. The notion of MONET helps in reducing the network traffic because the MR hides the MONET mobility from other hosts attached to the same MONET and other hosts need not exercise MIP

registrations. However, the original Mobile IP protocol is designed for a single mobile node and is not suitable for MONETs. Therefore we modify the process of MIP registration messages and present a scope-routing mechanism for MONET. Besides, a MONET may itself a mobile host attached to a second MONET, the second MONET may again attach to a third MONET, and so on, forming a hierarchy of MONETs. Therefore we also consider a hierarchy of multi-level MONETs when we design and implement a prototype of MONETs.

In order to reduce the impact of mobility on the performance of network applications, we also propose and implement a Location-based Pre-Authentication mechanism to reduce handoff latencies. The underlying idea of the Location-based Pre-Authentication mechanism is to maintain the location information of access routers (ARs), either fixed or mobile routers, in a location server. The location information of ARs can help an MN or MR to determine which AR it is likely to roam next and initiate authentication procedure before the handoff really takes place. Therefore when the MN or MR enters the coverage area of a pre-authenticated AR, it can use the services provided by the new AR directly, without waiting for a lengthy authentication with a remote server.

We have implemented a prototype of hierarchical MONETs with the location-based pre-authentication mechanism. Experimental results show that our proposals are very effective.

誌謝

首先要感謝我的指導教授－曾建超博士，提供這篇論文的構思方向，以及提供良好的研究環境，使我得以順利地完成這篇論文。另外，我要感謝徐元瑛學姊和史永健學長在這篇論文完成的過程中所給予的建議與指導。還要感謝實驗室同學、學長姊、以及學弟妹們的支持與鼓勵，讓我在兩年的碩士生涯中過得非常充實，謝謝你們。

此外，我還要感謝我的父母親、哥哥、以及我的朋友們，在我遇到挫折時，在精神面上給我的支持與鼓勵，使我得以繼續堅持下去。

僅將此結果獻給我親愛的家人、以及所有關心我的師長和朋友們。

目錄

表目錄

圖目錄

第一章　緒論

1.1 研究動機

近年來，由於 WLAN、GPRS、3G 等無線網路技術的發展已趨成熟，因此無線網路使用者在各種公共場合中無線上網已然成為未來的趨勢。假使無線網路使用者在咖啡廳、飛機場等固定場所中使用網際網路服務時，由於此時無線網路使用者的移動機會不高，因此我們可以直接使用 Mobile IPv4〔1〕通訊協定所提供的行動管理機制來管理無線網路使用者。但是，如果無線網路使用者是在大眾運輸工具上使用網際網路服務時，由於大眾運輸工具的快速移動，所以會導致底下幾個問題：

1. 增加網路傳輸量

Mobile IPv4 通訊協定的行動管理機制中，無線網路使用者只要移動到不同網域的網路環境時，無線網路使用者就必須回傳註冊訊息到家網路（Home Network）中，以便告知家網路，無線網路使用者目前所在的位置，不過因為大眾運輸工具會運載大量的無線網路使用者，而且每個無線網路使用者都需要回傳註冊訊息到家網路中，所以這樣會導致整個網路的傳輸量暴增。另外由於大眾運輸工具會頻繁地移動，使得無線網路使用者傳送註冊訊息的流程會時常發生，這樣也會導致整個網路的傳輸量暴增。

2. 增加網路延遲發生機率

由於大眾運輸工具會頻繁地移動，所以會增加網路換手發生的機率，然而只要網路進行換手時，就會造成網路的延遲，而網路的延遲將會導致許多網路應用程式的效能變低，進而影響無線網路使用者的使用觀感。

為了解決「增加網路傳輸量」的問題，我們可以在大眾運輸工具上架設一台移動路由器（Mobile Router, MR），所有經由這台 MR 來存取網際網路的網路節點所形成的網路我們就稱之為移動網路（Mobile Network, MONET）〔2〕。在 MONET 中，就只需要由 ISP 提供 MR 的架設，而且不需要每個無線網路使用者都安裝 Mobile IPv4 通訊協定的機制，只要 MR 安裝 Mobile IPv4 通訊協定的機制，就能讓大眾運輸工具內的所有無線網路使用者都可以使用網際網路服務。當運輸工具移動到不同網域的網路環境時，就只要由 MR 對家網路發出註冊的訊息，因此就可以大大地減少網路的傳輸量。

在現行的使用環境中，無線網路使用者可能會將自己擁有的數位產品使用藍芽（Bluetooth）技術互相連結而形成個人網路（Personal Area Network, PAN），並且使用一台 MR 作為對網際網路存取的行動管理者，因此這個 PAN 同時也就形成一個小型的 MONET。當這位 PAN 使用者搭乘大眾運輸工具時，

此時兩個網路就會形成階層式移動網路（Hierarchical MONET），因此 MR 的設計也需要考量到這種情況的階層式移動網路。

此外為了解決「增加網路延遲發生機率」所產生的問題，我們就必須使用快速換手（fast handoff）的機制，讓換手延遲對網路應用程式的影響降到最低。因為 MR 是整個 MONET 的行動管理，所以我們就只要在 MR 上套用快速換手的機制，就能夠讓整個 MONET 都能得到快速換手機制為網路應用程式所帶來的效能提升。

1.2 研究目標

本論文的研究目標為下列兩點：

1. 建構一個階層式移動網路的環境。
2. 使用一個記錄存取點位置資訊的位置伺服器對 MONET 下個可能會到達的存取點作預先認證（pre-authentication）的動作。

根據以上的動機，我們希望可以設計一個階層式移動網路的環境，每層移動網路都會有一台 MR 作為 MONET 存取網際網路的通訊閘。對 MONET 而言，MR 是一台標準的路由器，它會負責 MONET 內封包的繞送；對網際網路而言，MR 是一個移動的網路節點，而且這台 MR 是整個移動網路的行動管理者。

我們將使用 Mobile IPv4 通訊協定的機制來處理 MONET 的行動管理，因此 MR 就是 Mobile IPv4 通訊協定中的 Mobile Node 角色。但是，在原本 Mobile IPv4 通訊協定中所探討的都是針對單一節點移動到不同網域的網路時，對於該單一節點的行動管理機制，然而對 MONET 而言，雖然執行行動管理機制的就只有 MR，但是 MR 需服務 MONET 內部所有節點的行動管理，因此我們需要修改 Mobile IPv4 通訊協定的機制，以期適用於階層式移動網路的環境。

整個階層式移動網路會使用 IEEE 802.1x〔3〕的認證機制，當 MR 更換存取點時，MR 就必須向遠端的認證伺服器作認證動作，這樣 MR 才可以使用存取點所提供的網際網路存取服務，但是在現實的網路拓撲中，認證伺服器可能與 MR 的距離相距甚遠，所以當 MR 進行換手動作時，認證延遲的時間將會使得換手時的網路延遲時間變長。因此我們提出一套快速換手的機制，使得 MR 可以在換手到新的存取點時，進行預先認證的機制，我們將這套快速換手機制稱之為「跨網路預先認證機制」，並且這套快速換手的機制必須要能適用於階層式移動網路的環境。

在跨網路預先認證機制中，我們會建立一個位置伺服器，以記錄並管理所

有存取點的位置資訊。當 MR 要進行換手動作時，位置伺服器會根據它所記錄的存取點位置資訊，為 MR 找尋一群最有可能到達的存取點並傳回給 MR。讓 MR 對這些存取點作預先認證的動作，等 MR 移到新的存取點後，便可省去連至遠端認證伺服器做認證的時間，藉此來達到快速換手的目的。

1.3 章節簡介

這篇論文的章節內容簡述如下：

第一章： 描述這篇論文的研究動機，以及這篇論文希望達到的目標。

第二章： 說明這篇論文中相關的研究背景，包括：Mobile IPv4 通訊協定、MONET 簡介、IEEE 802.1x 認證機制、以及相關的論文研究。

第三章： 介紹我們所提出的設計方法，包括：階層式移動網路的設計方法以及跨網路預先認證機制的設計方法。

第四章： 介紹我們實作這整套系統的方式，包括：使用的軟硬體架構、修改過的封包格式、以及新增的封包格式等。

第五章： 使用幾個實例來比較分析我們所提出的跨網路預先認證機制與其它論文提出的預先認證機制，兩者之間在階層式移動網路中運作的差異性，並且舉出一個操作實例，來說明整個系統的運作狀況。

第六章： 對這篇論文作出一個總結，以及未來可繼續研究的方向。

第二章： 背景與相關研究

2.1 Mobile IPv4 簡介

Mobile IPv4 是一種可讓網際網路位址具有行動能力的網際網路通訊協定，它是由 IETF（Internet Engineering Task Force）組織所訂出的網際網路標準之一，簡單來說，在 Mobile IPv4 通訊協定中，移動節點會在家網路中使用一個固定的 IP 位址作為家位址（Home IP, HIP）。當移動節點移動到不同網域的網路環境時，移動節點就會取得一個暫時的 IP 位址，稱為 Care of Address（CoA）。發送端節點會以移動節點的家位址將封包送往移動節點，家網路的代理人就會截收此封包，然後再轉送到移動節點目前的 CoA，此時移動節點就能夠在家網路之外，收到其它節點送來的封包。

Mobile IPv4 的系統架構如圖 2.1 所示，其系統元件與相關名詞介紹如下：

1. MN（Mobile Node）：具備 IP 行動能力的網際網路節點，這個節點移動到不同網域的網路環境時，仍然可以透過其家位址進行封包的傳遞。
2. Home NW（Home Network）：原本 MN 所在的網路稱為 MN 的家網路，家網路的網域會與 MN 家位址的網域一樣。
3. HA（Home Agent）：MN 家網路內的代理人，它會負責記錄 MN 目前所在的 CoA（Care of Address），並且負責將其它節點送往 MN 的封包轉送到 MN 目前所在的位址。
4. Foreign NW（Foreign Network）：任何不是 MN 家網路的其他網路。
5. FA（Foreign Agent）：MN 在 Foreign Network 的代理人，它會與 HA 合作，完整地將網路封包傳遞給離開家網路的 MN。
6. CN（Correspondent Node）：與 MN 通訊的網路節點。

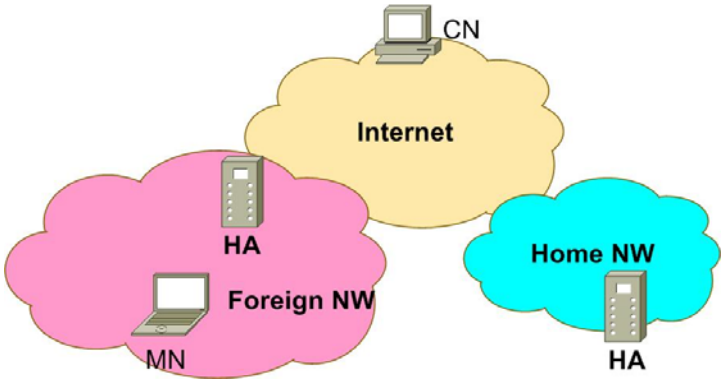

圖 2.1 Mobile IPv4 系統架構

Mobile IPv4 運作流程，如圖 2.2 所示：

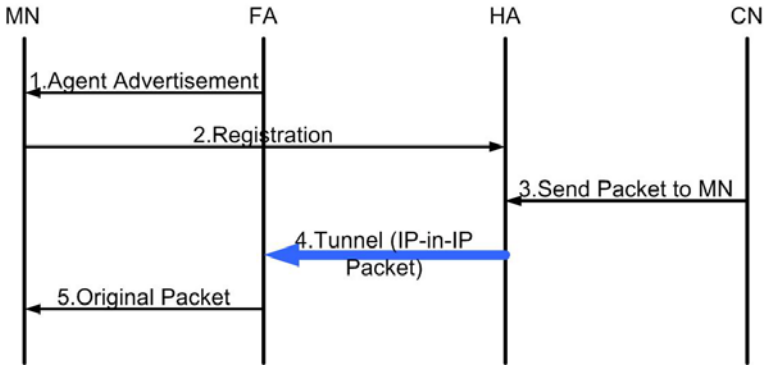

圖 2.2　Mobile IPv4 運作流程（使用 FA-CoA）

1. 當 MN 移到不同網域的網路環境時，MN 將收到 FA 廣播之 Agent Advertisement 訊息，藉此訊息 MN 可得知 FA-CoA。

2. MN 透過 FA 轉送註冊訊息給 HA，並告知 HA 目前的 FA-CoA，此時 HA 將該 MN 的 FA-CoA 記錄在 binding list 中，並產生一個由 HA 到 FA 的通道（Tunnel）。

3. 當有 CN 傳送封包給 MN 時，該封包會送到 MN 的家網路，並由 HA 接收該封包。

4. HA 透過適才建立的通道，將該封包包裝成 IP-in-IP 的封包（外層 IP 為 MN 的 FA-CoA，內層 IP 為 MN 的家位址），然後轉送給 FA。

5. 當 FA 收到 IP-in-IP 封包後，FA 將先解開外層 IP header，再將內層 IP 封包轉送至 MN。

上面所敘述的是有 FA 存在的環境，Mobile IPv4 通訊協定中也提到可以由 MN 本身與 HA 建立通道機制，由 MN 自行解開由 HA 轉送的 IP-in-IP 封包，此時，HA 所記錄的 CoA 就不稱為 FA-CoA，而稱之為 Colocated-CoA（Co-CoA）。Co-CoA 的運作流程圖，如圖 2.3 所示：

1. 當 MN 移動到不同網域的網路環境時，MN 會取得當地網域的 Co-CoA，然後 MN 轉送註冊訊息給 HA，並告知 HA 目前的 Co-CoA，此時 HA 將該 MN 的 Co-CoA 記錄在 binding list 中，並產生一個由 HA 到 MN 的通道。

2. 當有 CN 傳送封包給 MN 時，該封包會送到 MN 的家網路，並由 HA 接收該封包。

3. HA 透過適才建立的通道，將該封包包裝成 IP-in-IP 的封包（外層 IP 為

MN 的 Co-CoA，內層 IP 為 MN 的家位址），然後直接送往 MN。MN 收到 IP-in-IP 封包後，將先解開外層 IP header，解開後的封包即為 CN 送往 MN 的原封包。

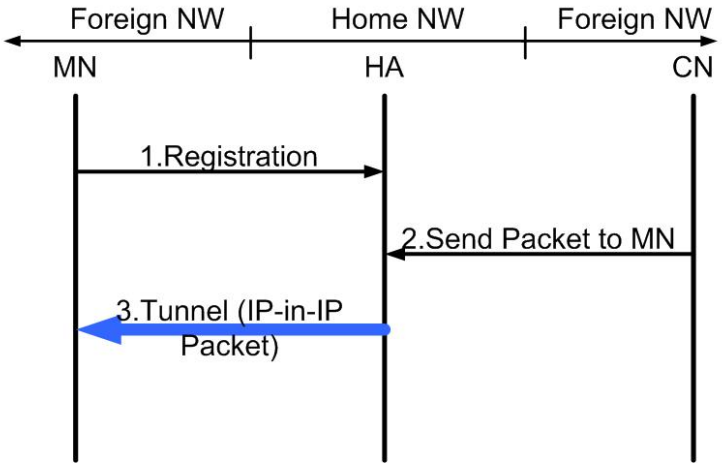

圖 2.3　Mobile IPv4 運作流程（使用 Co-CoA）

2.2　Mobile Network (MONET)

現有的網路環境中，網際網路的拓撲幾乎都是固定不動，雖然目前有許多的技術與通訊協定有針對單一節點移動所產生的問題來做討論，例如：Ad-hoc 網路或 Mobile IP 通訊協定等，但是這些討論都只研究單一節點的移動，對於整個網路的移動則未多加著墨，然而目前無線網路技術的發展成熟，無線網路的連線範圍與連線速率都不斷地提升，所以整個網路一同移動的情形想必在未來必定是個趨勢。因此 IETF 組織成立了一個工作群組－Network Mobility（NEMO），而這個工作群組成立的目的就是為了解決整個網路移動時所會產生的問題。

2.2.1　MONET 簡介

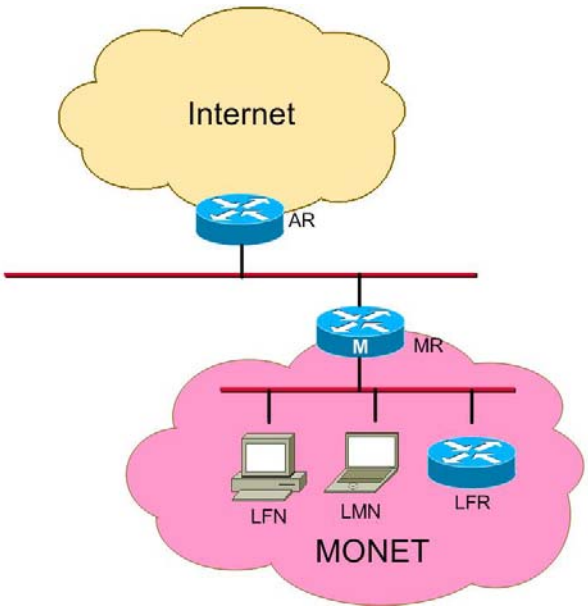

圖 2.4　MONET 系統架構

MONET 系統架構如圖 2.4 所示，其系統元件與相關名詞介紹如下：

1. Mobile Network（MONET）：一群透過 MR 來連結網際網路的網路節點，這些節點會與 MR 一同移動到不同的網路環境中，MR 與這些節點所形成的網路即稱之為 MONET。

2. Mobile Router（MR）：一台可提供網際網路存取與行動管理機制的路由器即稱之為 Mobile Router。MR 需要維護整個 MONET 對網際網路的連線，它的作用就像一台通訊閘道負責繞送網際網路與 MONET 之間的網路封包。MR 至少需要包含兩個網路介面，分別為外送介面（egress interface）與內送介面（ingress interface），外送介面是 MONET 對外的介面，當 MONET 位於家網路時，外送介面就會連接到家網路的連結，當 MONET 位於家網路之外的網路時，外送介面就會連接到其他網路的連結，而內送介面則是連接到 MONET 內部的連結。

3. Access Router（AR）：AR 本身就是一台路由器，它是一個能讓 MONET 連上網際網路的存取點。

4. Local Fixed Node（LFN）：一台永遠位於 MONET 內的主機，這個網路節點不會變更所連結的網際網路存取點。

5. Local Fixed Router（LFR）：一台永遠位於 MONET 內的路由器，這個網路節點不會變更所連結的網際網路存取點。

6. Local Mobile Node（LMN）：一個以 MONET 為家網路的移動節點，。LMN

可以在 MONET 中移動，也可以移出整個 MONET 環境。

7. Mobile Network Node（MNN）：任何位於 MONET 內的主機或路由器都可稱之為 MNN。（包含 LMN、LFN、LFR 和 MR）

2.2.2 階層式移動網路

當 MONET 內的路由器（包括 LFR 與 MR）作為 AR 使用，並有其它 MN 或 MONET 連接到此路由器時，整個網路就會成為階層式移動網路。

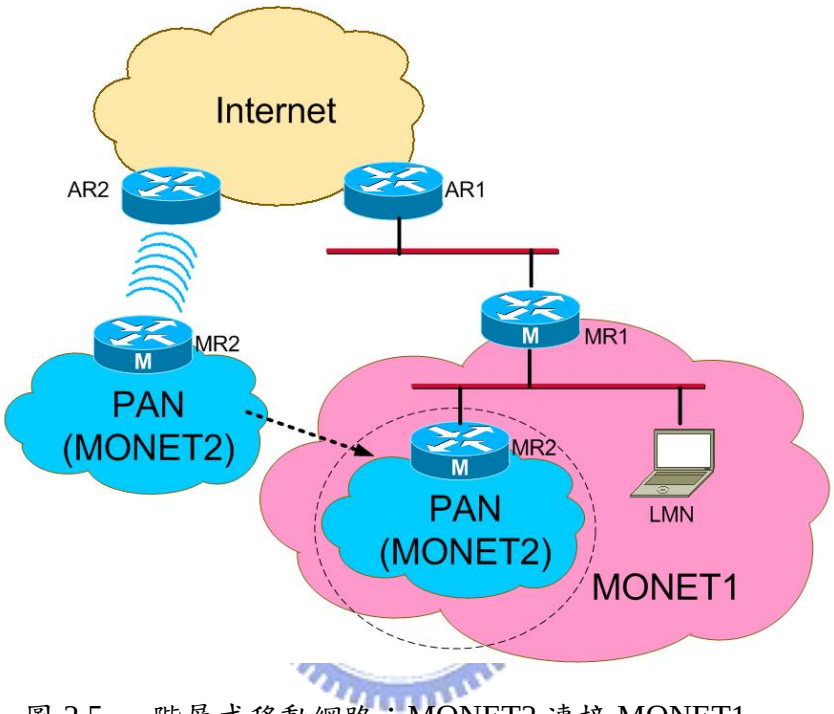

圖 2.5 階層式移動網路：MONET2 連接 MONET1

以圖 2.5 為例，某位使用者擁有一個 PAN 網路，並且 PAN 網路是透過 MR2 來存取網際網路服務，因此這個 PAN 網路與 MR2 就形成一個移動網路 MONET2，當這位使用者搭上一台火車時，MONET2 網路與火車所形成的 MONET1 網路就形成階層式移動網路，在大眾運輸工具行進的同時，MONET2 會隨著 MONET1 網路一同移動，然而當這位使用者下車時，MONET2 網路則會和 MONET1 網路分開移動。因此階層式移動網路的特點就在於每個階層的移動節點（MN）或移動網路（MONET）就是一個獨立的移動單位，而每個移動單位可一同移動，也可分開地移動。

2.2.3 MONET defined in Mobile IPv4

由單一節點所形成的階層式移動網路使用 Mobile IPv4 通訊協定的示意圖如圖 2.6 所示：

當 MR 使用 AR1 作網際網路存取服務時，AR1 就成為 MR 的 FA，所以

MR 的 HA 就會記錄 MR 的 FA-CoA 為 AR1 的 IP 位址。另外當 MN 進入 MONET 形成階層式移動網路後，MR 就成為 MN 的 FA，因此 MN 的 HA 就會記錄 MN 的 FA-CoA 為 MR 的家位址。在圖 2.6 中，MR 與 MN 的 HA 為同一台機器，因此 HA 的 binding list 中就會有兩筆資料，一筆是記錄 MR 目前所在的 FA-CoA，也就是 AR1 的 IP 位址；另一筆則是記錄 MN 目前所在的 FA-CoA，也就是 MR 的家位址。

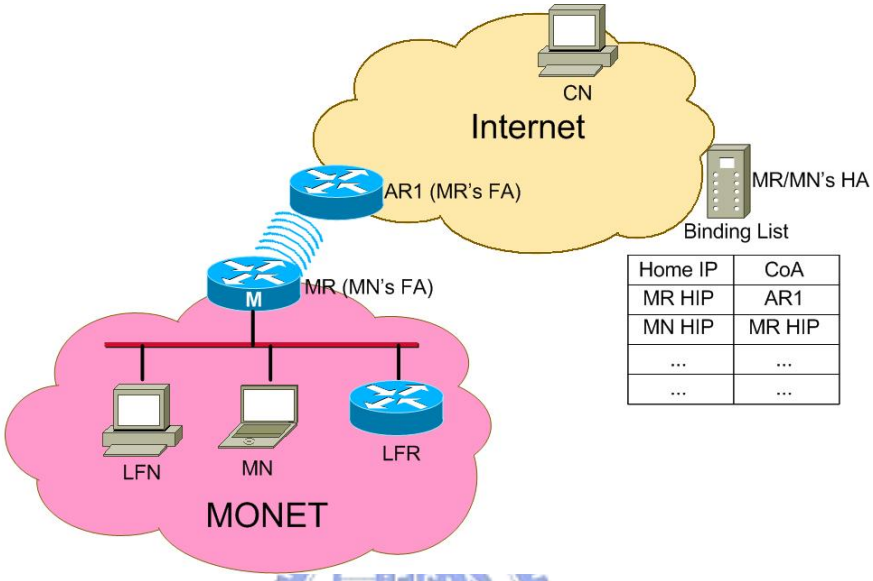

圖 2.6　MONET 內的 MN 之 MIPv4 運作示意圖

當 CN 傳送封包給 MN 時，其運作流程如圖 2.7 所示：

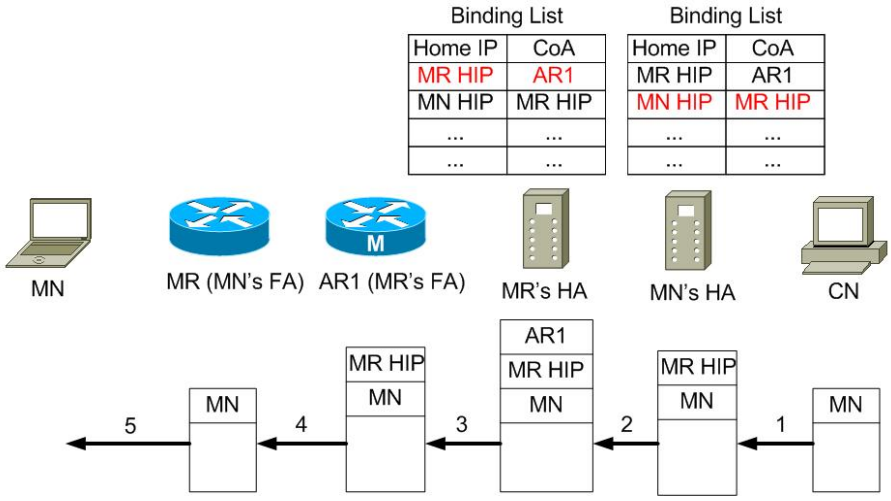

圖 2.7　MONET 內的 MN 之 MIPv4 運作流程圖

1. CN 傳送封包給 MN 家位址。

2. MN 的 HA 截收到這個封包，並對照 binding list 表，將封包包裝成 IP-in-IP

封包，其中外層目的地 IP 為 MR 的家位址。

3. MR 的 HA 截收到這個目的地 IP 為 MR 家位址的 IP-in-IP 封包，並對照 binding list 表，將該封包再包裝成 IP-in-IP 封包，其中最外層目的地 IP 為 AR1 的 IP 位址。

4. AR1 接收到這個封包，解開第一層 IP-in-IP 封包，此時，目的地 IP 即為 MR 的家位址。

5. MR 接收到這個封包，再解開一層 IP-in-IP 封包，此時，目的地 IP 即為 MN 家位址，最後，MN 就能收到 CN 傳送過來的封包。

雖然單一移動節點可以使用 Mobile IPv4 通訊協定原先所定義的方式來正常運作，但如果是 CN 傳送到封包給位於 MONET 內的 LFN，HA 會因為 binding list 裡沒有 LFN 的 CoA 資料，因此這個送往 LFN 的封包將會無法做通道機制（Tunneling）的動作，也就無法將封包轉送到這些固定節點中。然而 Mobile IPv4 通訊協定針對 MONET 環境所遭遇的問題提出了底下兩種解決方法，分述如下：

1. 方法一：將 MONET 內的所有 MNN 都視為 MN

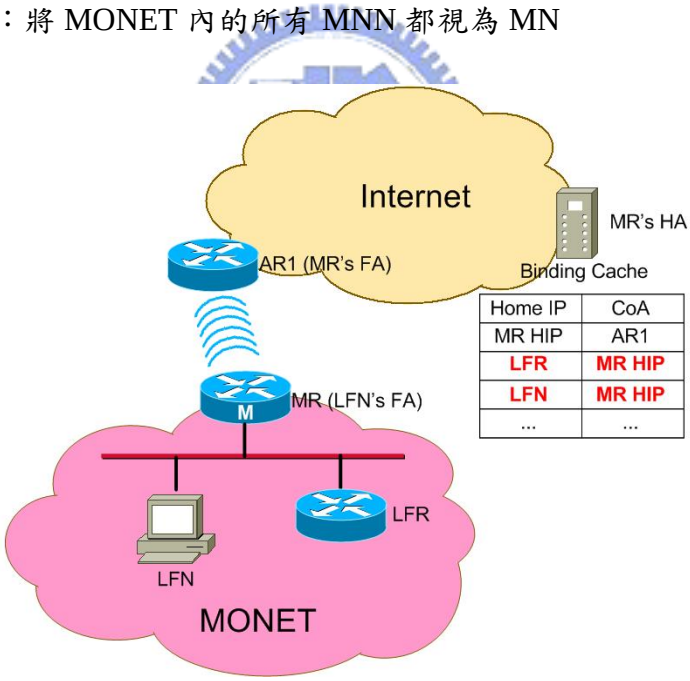

圖 2.8　MONET in MIPv4 方法一

如圖 2.8 所示，MONET 內所有的 MNN 的 FA-CoA 都會設定為 MR 的家位址，此時，MR 就能成為所有 MNN 的 FA，如此一來，傳送到這些固定節點的封包才會由 MR 的 HA 所截收，並且進行通道機制，然後再轉送到 MONET 目前所在的位置。其運作流程如圖 2.9 所示：

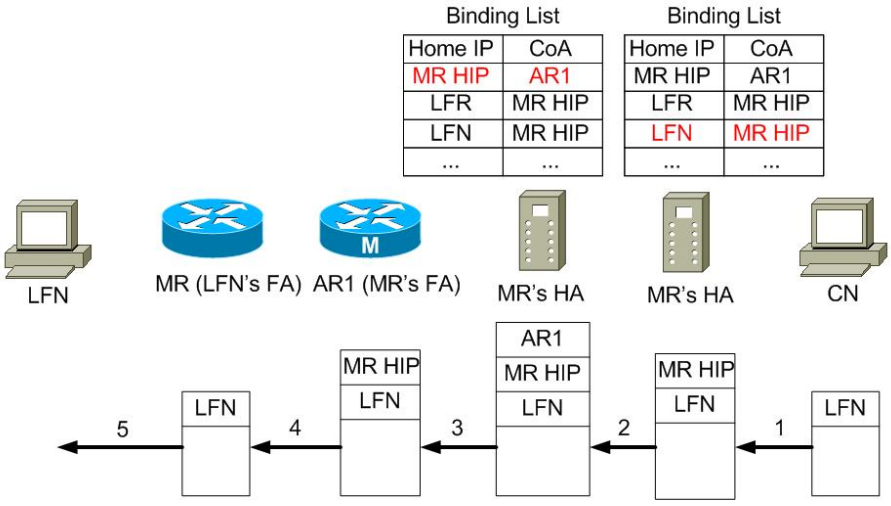

圖 2.9　方法一 MONET 內的 LFN 之 MIPv4 運作流程圖

1. CN 傳送封包給 LFN。
2. MR 的 HA 截收到這個封包，並對照 binding list 表，將封包包裝成 IP-in-IP 封包，其中外層目的地 IP 為 MR 的家位址。
3. MR 的 HA 截收到這個目的地 IP 為 MR 家位址的 IP-in-IP 封包，並對照 binding list 表，將該封包再包裝成 IP-in-IP 封包，其中最外層目的地 IP 為 AR1 的 IP 位址。
4. AR1 接收到這個封包，解開第一層 IP-in-IP 封包，此時，目的地 IP 即為 MR 的家位址。
5. MR 接收到這個封包，再解開一層 IP-in-IP 封包，此時，目的地 IP 即為 MN 家位址，最後，MN 就能收到 CN 傳送過來的封包。

使用這個方法將使得通道變成有階層式的關係如圖 2.10 所示，而封包每透過一層的通道都需要經過 IP-in-IP 的包裝，所以 IP header 的長度也會隨之而變長，此外 HA 中還必須記錄每個位於 MONET 內固定節點，如果 MONET 所含有的固定節點很多，HA 的負載量就會跟著加重。

圖 2.10　階層式通道示意圖

2. 方法二：MR 透過 HA 與 MR 之間的雙向通道（Bi-directional tunnel）廣播 Routing Infomation Protocol（RIP）訊息

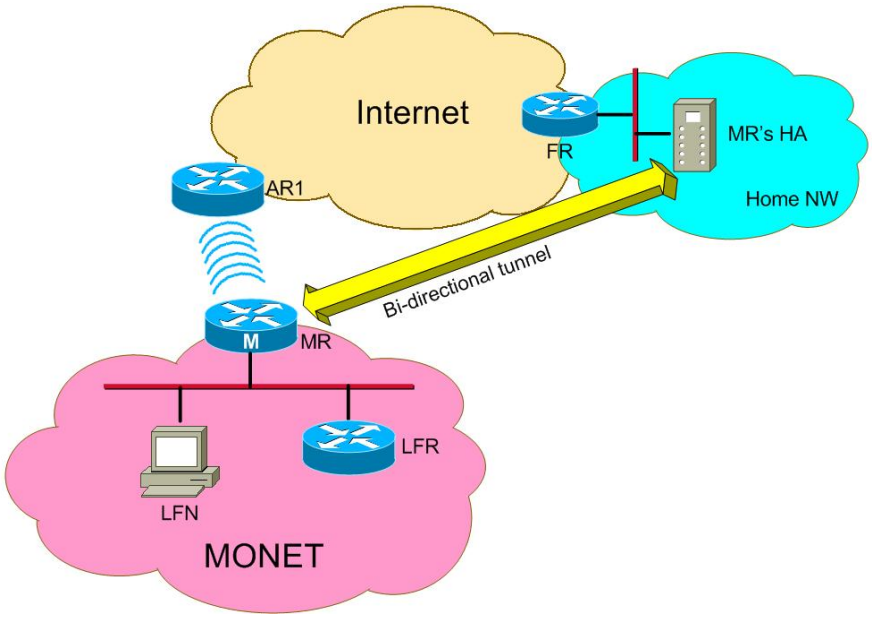

圖 2.11　MONET in MIPv4 方法二

如圖 2.11 所示，MR 使用 AR1 作為網際網路存取服務時，MR 會向 HA 註冊，並且與 MR 的 HA 建立一條雙向的通道，也就是 MR 所發出的封包會先經由這條通道傳回到家網路，再由 MR 的 HA 解開 IP-in-IP 封包之後，最後，將該封包傳送到正確的位置。在這個方法中，MR 必須將 RIP 的廣播訊息也傳回到家網路中，目的是為了讓家網路的路由器可以繼續維護送往 MONET 內部節點的路由路徑。當 CN 傳送封包到 MONET 內的 LFN 時，該封包會先傳送到 MR 家網路中的路由器（即圖 2.11 中的 FR），經由路由表得知該封包要傳往 MR，家網路的路由器就會發出 ARP 請求，而 MR 的 HA 會執行 Mobile IPv4 中的 Proxy ARP 功能，所以 MR 的 HA 可以截收到 CN 送往 LFN 的封包，不過由於這個封包的第三層目的地 IP 為 LFN 的 IP 位址，MR 的 HA 並不會幫忙 LFN 的 IP 位址封裝 IP-in-IP 封包，因此 MR 的 HA 必須也要解開 MR 送過來的 RIP 訊息，以記錄 MONET 內的網域位址，並且幫這些網域位址封裝 IP-in-IP 封包。

使用這個方法雖然不像方法一會形成階層式的通道，而且 HA 也不用記錄 MONET 內的每個固定節點，但是，MR 的 HA 必須要作修改，使其能認得 RIP 訊息封包，並且記錄 MONET 內的網域位址，因此我們還需要去了解 RIP 訊息封包格式，並解析 RIP 訊息封包，所以在實作上將會比較難達成目標。

2.3 IEEE802.1x－連接埠網路存取控制(Port-Based Network Access Control)

最近幾年，無線網路的發展已逐漸成熟，無線網路也逐漸成為我們生活中不可或缺的角色，但是無線網路最令人詬病的問題還是在於無線網路的安全性問題。有鑑於此，電子電機工程師協會（IEEE）提出了一套標準－IEEE 802.1x 連接埠網路存取控制〔3〕，這個標準會在鏈結層（link layer）中為 IEEE 802 網路的網路使用者做身分認證的機制，其中，IEEE 802 網路包含有 Ethernet（IEEE 802.3）網路與 WLAN（IEEE 802.11）網路。IEEE 802.1x 不僅可以利用「使用者帳號/密碼」或「數位憑證」來做使用者身份的認證，也可以支援動態網路封包加密金鑰的配送。

圖 2.12 為 IEEE 802.1x 的示意圖，IEEE 802.1x 使用控制連接埠的方式來做安全管理，當申請者移動到網路存取點時，申請者就只能透過網路存取點中未被授權的連接埠來傳送認證的訊息。當申請者通過認證伺服器（如：RADIUS〔6〕伺服器）的認證後，申請者才可使用網路存取點中被授權的連接埠來存取網路的資料，網路存取點可透過認證的結果，針對不同的申請者開啟不同的連接埠，以供申請者使用。

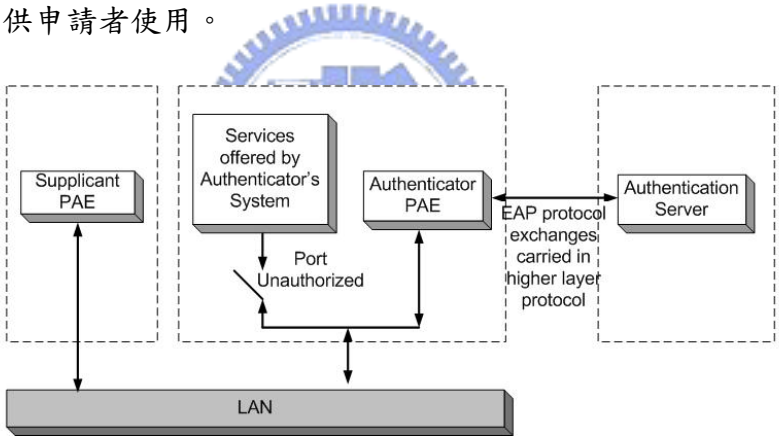

圖 2.12　IEEE 802.1x 示意圖

2.3.1 IEEE 802.1x 系統架構

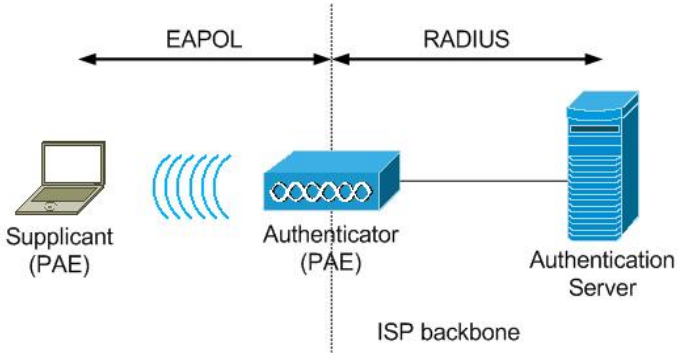

圖 2.13　IEEE 802.1x 系統架構

系統元件與相關名詞介紹如下：

1. Supplicant：請求網路存取權的實體。
2. Authenticator：具有要求認證機制的實體，這個實體可以接受未受信任端網路節點的認證請求，並控制 Supplicant 存取網路所用的連接埠。
3. Authentication Server：幫助 Authenticator 做身分認證服務的實體，這個實體可能會與 Authenticator 同時存在於一台主機中，不過大多數的狀況下它是一台獨立的伺服器。
4. Port Access Entity（PAE）：擁有存取埠的一個實體，這個實體具有 Authenticator、Supplicant 或兩者的功能。
5. EAP over LAN（EAPOL）：為 Supplicant 與 Authenticator 之間所使用的認證通訊協定。
6. RADIUS：為 Authenticator 與 Authentication Server 之間所使用的認證通訊協定。

IEEE 802.1x 只是一個架構，並非一套完整的規格。實際的認證機制，其實是透過認證伺服器（Authentication Server）來完成。IEEE 802.1x 所提供的機制，主要是用來發出認證盤查（EAP Challenge）以及確認或拒絕存取的訊息，實際上並不負責判斷對方是否有權存取。

2.3.2　可延伸認證協定（Extensible Authentication Protocol）

IEEE 802.1x 的基礎是可延伸認證協定（Extensible Authentication Protocol, EAP）〔4〕，EAP 是由 IETF 所規範的一套標準，它是一種簡單的封裝方式，可以執行於任何的鏈結層上。EAP 的基本架構如圖 2.14 所示，這個架構的主

要目的是為了能夠執行於任何的鏈結層，並且能夠使用各種的身分認證方式。

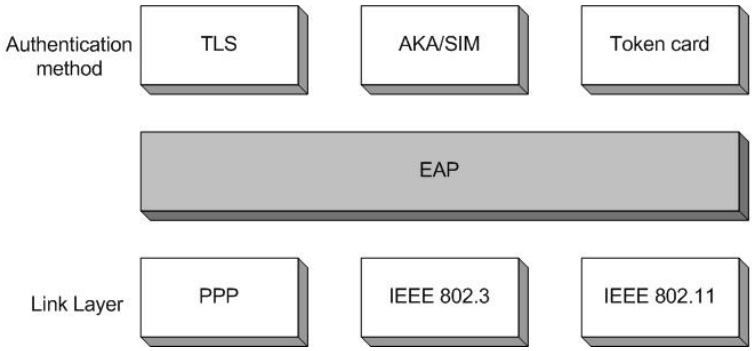

圖 2.14　EAP 系統架構

EAP 運作流程是一連串的認證步驟，以認證要求訊息為開端，並以認證成功或失敗為結束，其運作流程如圖 2.15 所示：

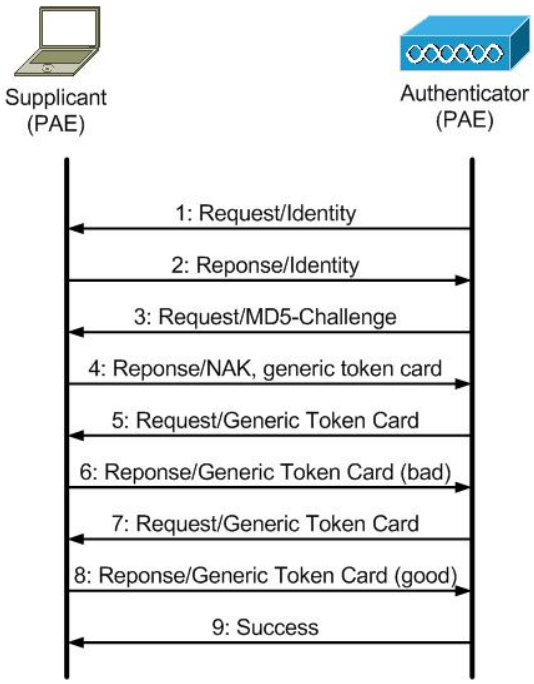

圖 2.15　EAP 運作流程

1. 認證者（Authenticator）發出 Request/Identity 封包以辨識使用者身份。
2. 申請者（Supplicant）要求使用者輸入識別碼，然後將使用者識別碼以 Response/Identity 訊息送出。
3. 一旦認出該使用者，認證者隨即送出認證盤查。圖 2.15 中認證者送出 MD-5 的認證盤查給使用者。

4. 申請者設定以標記卡（token card）進行身分認證，因此會送出一個 Response/NAK 訊息，提議以一般標記卡（Generic Token Card）作為認證機制。

5. 認證者送出一個 Request/Generic Token Card 的認證盤查，要求取得卡號（numerical sequence on the card）。

6. 使用者鍵入卡號，透過 Response/Generic Token Card 訊息送回。

7. 當使用者的答覆不正確，因此認證失敗，但是有許多 EAP 的實作允許多次認證的機會，所以認證者會再送一次 Request/Generic Token Card 的認證盤查。

8. 使用者再度以 Response/Generic Token Card 訊息答覆。

9. 此次的答覆正確，因此認證者就會發出一個 EAP Success 的訊息。

2.3.3 IEEE 802.1x 運作流程

IEEE 802.1x 運作流程與 EAP 運作流程幾乎一模一樣，主要的差別在於，申請者（Supplicant）可以主動發送 EAPOL-Start 訊息，藉此訊息來啟動整個 EAP 運作流程。如果不再需要使用網路，還可以用 EAPOL-Logoff 訊息，將連接埠還原成未授權的狀態。其運作流程如圖 2.16 所示：

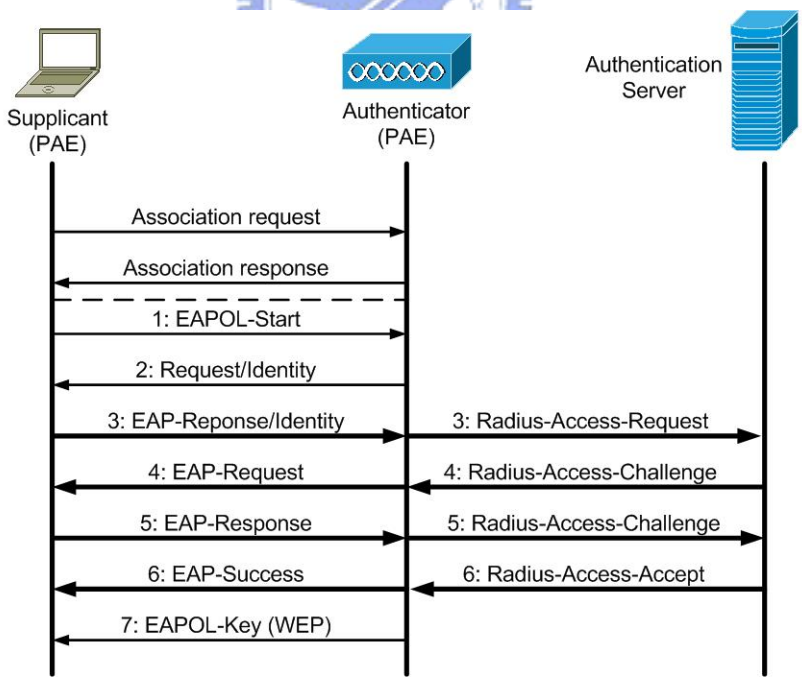

圖 2.16　IEEE 802.1x 運作流程

IEEE 802.1x 運作流程如下：

1. 申請者以一個 EAPOL-Start 訊息開始 IEEE 802.1x 運作流程。

2. 開始 EAP 的運作流程。認證者會發出一個 EAP-Request/Identity 訊息。

3. 申請者回應一個 EAP-Response/Identity 訊息，此訊息會被轉送給認證伺服器，作為 Radius-Access-Request 封包。

4. RADIUS 伺服器回應一個 Radius-Access-Challenge 封包，此封包會隨即被當作 EAP-Request 轉送給申請者，其中包含相關的認證盤查訊息。

5. 申請者從使用者取得答覆，然後再送回 EAP-Response 訊息。此訊息會由認證者轉換為 Radius-Access-Request，其中包含一個資料欄位作為認證盤查訊息的答覆。

6. Radius 伺服器以一個 Radius-Access-Accept 訊息核准申請者存取網路，然後，認證者發出 EAP-Success 訊息。該連接埠得到授權後，使用者便可以開始存取網路。

7. 認證者賦予申請者一把 WEP（Wired Equivalent Protocol）鑰匙，完成 IEEE 802.1x 認證流程。

IEEE 802.1x 認證不一定是由申請者以 EAPOL-Start 訊息啟動，在任何時刻，認證者都可以發出一個 EAP-Request/Identity 訊息來啟動 IEEE 802.1x 的認證程序，以更新認證資料。

2.4 相關論文研究

2.4.1 Pre-Authenticated Fast Handoff in a Public Wireless LAN Based on IEEE 802.1x Model

這篇論文〔5〕是由 Sangheon Pack 與 Yanghee Choi 兩位所提出，主要目的是提出一個快速換手的機制，讓無線網路使用者在與目前存取點做連結動作（association）時，除了對目前存取點作 IEEE 802.1x 認證之外，同時也對鄰近的存取點作預先認證，使得無線網路使用者抵達新存取點時，不需要再經過認證機制就可以直接使用存取點的網際網路存取服務。

這篇論文主要分成兩個部分，分別為：選取鄰近存取點、以及修改 IEEE 802.1x 認證機制中的金鑰分配。

第一部分是選取鄰近存取點，這篇論文使用兩個參數，分別為：在存取點 *i* 與存取點 *j* 之間發生換手的次數（*N(i,j)*）、以及兩個存取點換手時停留在目前存取點的時間（*R(i,j)*）。由底下方程式可決定兩存取點之間的移動機率（*H(i,j)*）：

$$H(i,j)=\frac{N(i,j)}{R(i,j)}$$

最後，根據計算出的換手機率來選取一些可能會到達的存取點。

第二部分是修改 IEEE 802.1x 認證機制中的金鑰分配，由於 IEEE 802.1x 的認證機制都只支援一對一的訊息傳遞，因為作者要將認證成功的訊息傳遞給所有鄰近的存取點，所以作者需要將原本一對一的訊息傳遞，更改為一對多的訊息傳遞，如此一來，就可以將多個認證成功的訊息，預先傳遞給所有的存取點，以達到預先認證的目標。

這篇論文執行預先認證機制的時機是在與存取點做 association 動作時，不過在 MONET 中存取點會移動，所以在 association 動作中所選取的鄰近存取點，可能已經移動到其它位置。另外由於 MONET 中存取點會移動，所以選取鄰近存取點所使用的兩個參數－存取點之間發生換手的次數以及兩個存取點換手時停留在目前存取點的時間，可能會因為網路拓撲的改變而變得不準確，因此會造成選取的錯誤率提高，所以這篇論文所提出的方式並不適用於 MONET 環境中。

第三章： 跨網路預先認證的階層式移動網路之設計、架構與方法

在本章節中，我們會先建構出整套系統的基礎架構－階層式移動網路，我們將詳細地描述階層式移動網路的整體架構，並且說明階層式移動網路中每個元件的設計方法與原則，包括 MR 與 HA 的設計原則，當階層式移動網路建構完成後，我們將繼續說明跨網路預先認證機制的系統架構，以及這套機制如何在階層式移動網路中運作，並說明跨網路預先認證機制的三個設計步驟。

3.1 階層式移動網路之設計架構

階層式移動網路的系統架構中，每個 MONET 都會有一台對外的通訊閘－Mobile Router，而這台 MR 本身會有一個 HA 來做為 MR 的行動管理者，兩個 MONET 之間互相連結，就形成了階層式移動網路。如圖 3.1 所示，透過 MR1 存取網際網路服務的網路形成 MONET1，同樣地，透過 MR2 與 MR3 存取網際網路服務的網路形成 MONET2 與 MONET3，而圖 3.1 中 MONET1、MONET2 與 MONET3 就形成階層式移動網路，而 MR1 就是整個階層式移動網路的第一階層，MR2 為第二階層，依此類推。

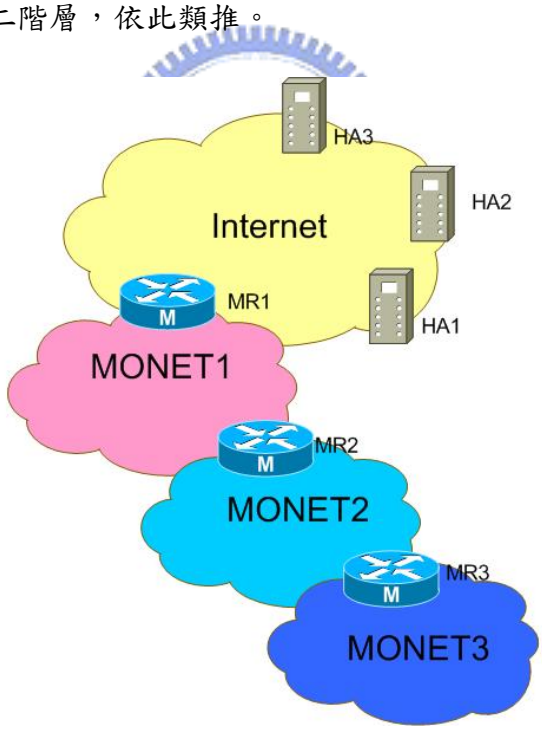

圖 3.1 階層式移動網路系統架構

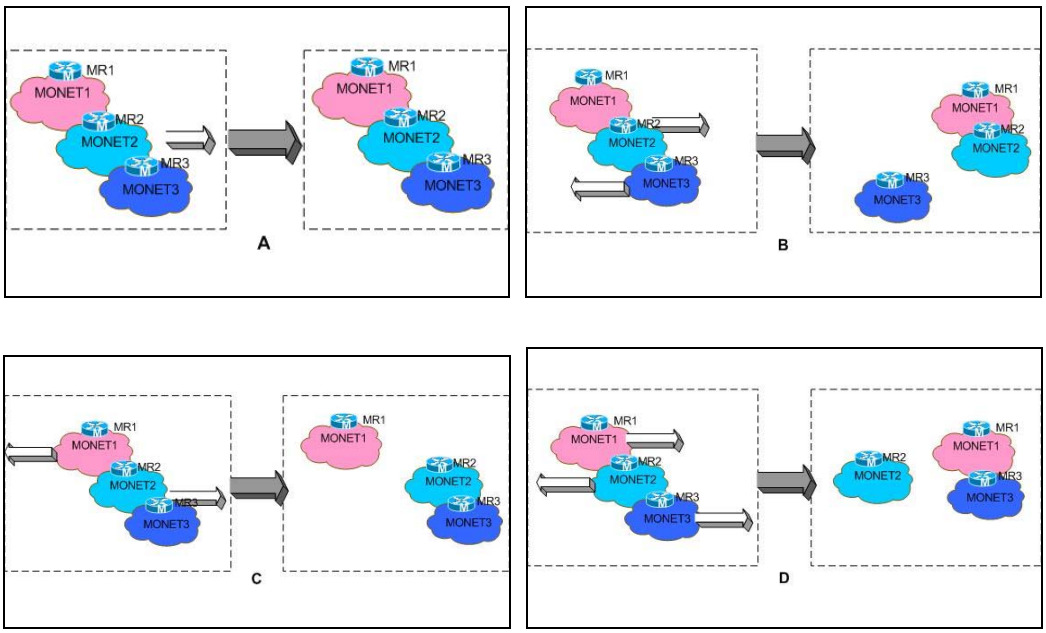

圖 3.2　階層式移動網路的相對移動

階層式移動網路最大的特點在於階層式移動網路之間的相對移動，圖 3.2 說明各種情況的相對移動，雖然階層式移動網路有很多種情況的相對移動，但是最主要還是分成兩種類型的相對移動：

1. 與父階層同向移動：以圖 3.2.D 為例，MR1 為 MR3 的父階層，並且 MR1 與 MR3 兩者往相同的方向移動，因此我們稱 MR1 與 MR3 同向移動。

2. 與父階層反向移動：以圖 3.2.D 為例，MR1 為 MR2 的父階層，MR2 為 MR3 的父階層，並且 MR1 與 MR2，以及 MR2 與 MR3 兩者都往相反的方向一定，因此我們稱 MR1 與 MR2 反向移動，MR2 也與 MR3 反向移動。

由於 MONET 所形成的階層式移動網路會相對移動，所以網路的拓撲也會隨著階層式移動網路的相對移動而跟著變動，因此當我們要執行預先認證機制時，MONET 的行動管理就會變得十分重要。

3.2　階層式移動網路之設計方法

根據 2.2.3 節的討論，我們可以知道在 MONET 內的 MN 節點，可以適用於原先 Mobile IPv4 通訊協定所規範的運作流程。至於 MONET 內的 LFN 節點，Mobile IPv4 通訊協定也針對此時 MONET 的設計提出了兩種方法，但是這兩種方法都有其缺點，我們將這兩種方法的設計缺點，簡述如下：

1. 方法一：將 MONET 內的所有 MNN 都視為 MN

HA 需要為每個固定節點記錄其 CoA（即 MR 的家位址），而且還必須使用到階層式的通道，因此不僅會增加 HA 的負載量，並且每通過一層通道，封包就會增加一層 IP-in-IP 的封裝，所以整個封包的 IP header 長度就會隨著變長

2. 方法二：MR 透過 HA 與 MR 之間的雙向通道廣播 RIP 訊息

MR 的 HA 必須要能認得 RIP 訊息封包，並且記錄 MONET 內的網域位址，才能使得 CN 送往 MR 的封包得以經過通道機制轉送到 MR。因此我們還需要去了解 RIP 訊息封包格式，並解析 RIP 訊息封包，所以在實作上將會比較難達成目標。

而我們的設計方法是修改 MR 送給 HA 的註冊封包，使註冊封包含有 MONET 內部的網域資料，HA 透過這個註冊封包，取得 MONET 的內部網域資料，並將這些網域資料儲存於 HA 的路由表中。藉由我們所修改的註冊封包，HA 可以取得 MONET 內所含有的網域資料，HA 只要在路由表中新增多筆路由路徑，將這些送往 MONET 內部網域的封包都傳送到這條通道。如此一來，傳送到 MONET 內的封包就會封裝成 IP-in-IP 封包送往 MR 目前所在的位置，接著當 MR 接收到這個 IP-in-IP 封包後，MR 會先解開外層 IP header，並將內部封包傳送給內部節點。

如圖 3.3 所示，當 MR 以 Co-CoA 向 HA 註冊之後，HA 就會新增一個通道網路介面，也就是圖 3.3 中的 TUNL 網路介面，並且 HA 除了新增一筆路由路徑，這筆路徑會將目的地 IP 位址為 MR 家位址的封包送往 TUNL 網路介面之外，HA 還需要新增多筆路由路徑，將 MONET 的網域也送往 TUNL 網路介面。

當 CN 傳送封包給 LFN 時，HA 會在家網路中截收到這個封包，然後 HA 會對照路由表的路由規則，由於搜尋到 MONET 的網域正好與 LFN 所在的網域相同，因此就將此封包送往 TUNL 通道網路介面。TUNL 通道網路介面就將這個封包封裝成 IP-in-IP 的封包，其中外層的目的地 IP 位址為 MR 的 Co-CoA 位址，MR 截收到此封包之後，就會解開 IP-in-IP 封包，最後該封包就會根據 MONET 內部的路由規則送往 LFN 節點。

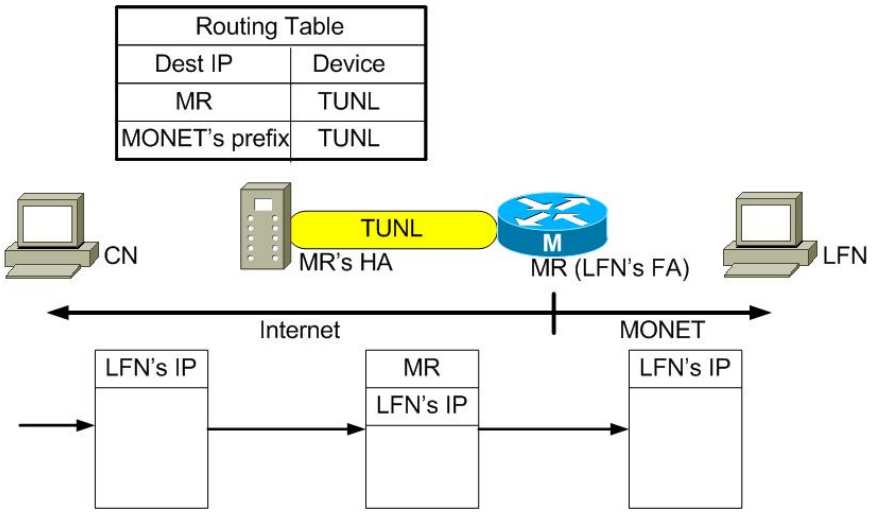

圖 3.3　階層式移動網路之設計方法

上述的設計方法使得送往 MONET 的封包就只需要封裝一層 IP-in-IP 的 header，所以很自然地可以解決方法一（將 MONET 內的所有 MNN 都視為 MN）會形成階層式通道的缺點，然而我們使用記錄 MONET 的網域來取代記錄所有固定節點，所以也能夠解決方法一的另一項缺點－需要記錄 MONET 內的所有固定節點。雖然 MONET 內可能會有多個網域，不過比起記錄所有固定節點，使用記錄網域的方式，將可大大地減輕 HA 的負載量。

方法二（MR 透過 HA 與 MR 之間的雙向通道廣播 RIP 訊息）中 MR 會透過雙向通道廣播 RIP 訊息，其目的是為了維護家網路路由器送往 MONET 內部節點的路由路徑，由於使用我們的設計方法，HA 會在路由表中記錄 MONET 內所有節點的網域，所以只要在 HA 與家網路的路由器之間藉著使用 RIP 通訊協定，交換兩台路由器之間的網域資訊，家網路的路由器就能維護送往 MONET 內部節點的路由路徑，因此我們只要讓 HA 可以收送 RIP 訊息即可達到要求。方法二的缺點在於 HA 需要解析 RIP 訊息封包，然而使用我們設計的方法，不需要解析 RIP 訊息封包，只要收送 RIP 訊息封包，所以實作上就會變得較為容易。

以下我們列出經過修改後的詳細註冊，以及傳送封包的流程。

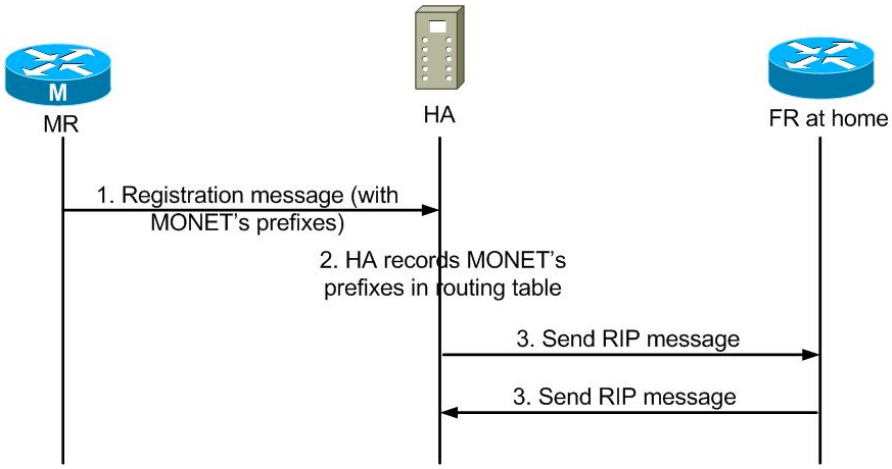

圖 3.4　階層式移動網路的註冊流程圖

如圖 3.4 所示，階層式移動網路的註冊流程為：

1. MR 藉由註冊封包將 MONET 所含有的網域告知 HA。
2. HA 將接收到的網域資訊記錄起來，並設定為所有來自這些網域的封包都傳送到 MR 與 HA 之間的通道。
3. HA 開啟交換 RIP 訊息的功能，使得 MR 不在家網路時，HA 可以與家網路下的路由器交換 RIP 訊息，藉此來維護送往 MONET 的路由設定。

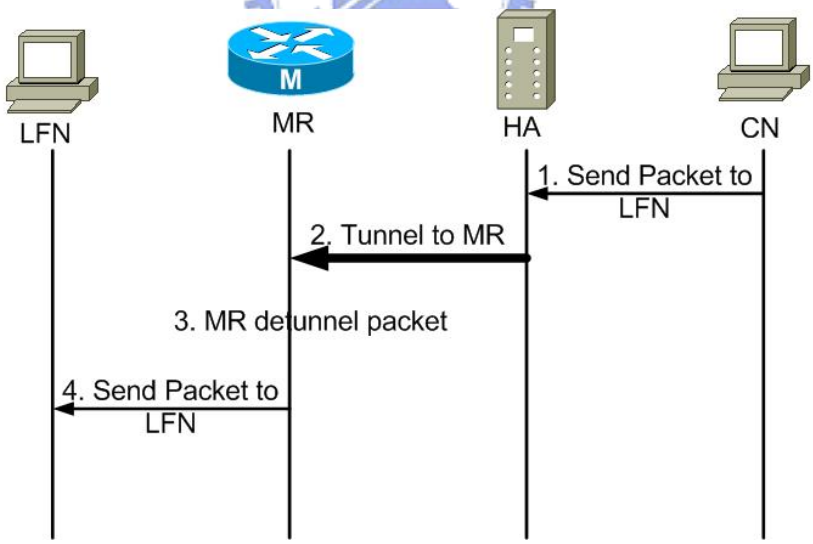

圖 3.5　階層式移動網路的封包傳送流程圖

如圖 3.5 所示，階層式移動網路的封包傳送流程為：

1. CN 傳送封包到 MONET 下的網路節點 LFN。

2. HA 截收到此封包，並將該封包丟往 MR 與 HA 之間的通道，然後將 IP-in-IP 封包送往 MR 目前所在的位置。

3. MR 解開 IP-in-IP 封包，繼續送達 MONET 的內部網路中。

4. 根據 MONET 內部的路由規則，將封包送達目的地節點。

3.2.1 Mobile Router 之設計原則

根據上述的設計方法，MR 需要扮演兩種角色，對 Internet 而言，MR 所扮演的角色為一台 MN，由家網路下的 HA 幫忙 MR 做行動管理；對 MONET 內部而言，MR 所扮演的角色為 MONET 的 FA，MR 需要將家網路所送來的 IP-in-IP 封包解開一層 IP header，接著傳送到 MONET，然後經由 MONET 本身的路由繞送規則，將封包送達目的地節點。因此 MR 必須使用 Co-CoA 的方式對 HA 做註冊的動作，使用 Co-CoA 的話，MR 就能夠有解開 IP-in-IP 封包的功能，如此一來，MR 就能自然地扮演這兩種角色。

另外在此階層式移動網路中，HA 除了需要記錄 MR 的 Co-CoA 之外，還需要記錄 MONET 下所含有的網域資訊，因此 MR 做註冊動作時，除了要告知 MR 本身的 Co-CoA 之外，MR 還需要向 HA 告知 MONET 內所含有的網域，所以 MR 所發出註冊訊息中，必須做些許的更改，使得註冊訊息中夾帶 MONET 內所含有的網域資訊，相同地，HA 也必須跟著做更改，使其能認得更改過的註冊訊息。

我們將 Mobile Router 的設計原則，整理如下：

1. 路由器功能：MONET 內部的路由規則，必須先經由 MR 的路由器功能來完成，這樣封包才得以在 MONET 內部繞送。

2. MIPv4 的 MN 功能：整個 MONET 的行動管理，都是經由 MR 的 MN 功能來完成，並且 MR 要設定為使用 Co-CoA 來執行，因為 MR 必須有解開 IP-in-IP 封包的功能。

3. 傳送 MONET 網域功能：MR 需告知 HA 整個 MONET 下所含有的網域，這個功能可以在註冊封包中增加網域資訊的欄位來完成。

3.2.2 Home Agent 之設計原則

在我們的階層式移動網路設計方法中，HA 的功能不僅是 MR 的行動管理者，同時也是整個 MONET 的行動管理者，所有傳送到 MONET 的封包都需要經由 HA 來轉送，雖然 HA 是整個 MONET 的行動管理者，但是 HA 並不用像 MONET defined in MIPv4 方法一，需要記錄所有 MONET 固定節點的資訊，HA 只要記錄 MONET 所含有的網域即可，因此可以大大地減輕 HA 的負載量。

HA 除了作為 MONET 的行動管理者之外，它還必須擔任路由器代理人的角色，當 MR 移出家網路時，HA 必須開啟傳送 RIP 訊息的功能，幫助 MR 與家網路下的路由器交換路由規則，這樣送往 MONET 的封包才能繼續地送往 MONET 中。

我們將 Home Agent 的設計原則，整理如下：

1. MIPv4 的 HA 功能：當 MONET 移出家網路時，HA 正是藉由 MIPv4 的 HA 功能幫忙轉送封包到 MONET 目前的所在位置。

2. 記錄 MONET 網域的功能：MR 會經由註冊封包告知 MONET 所含有的網域資訊，而 HA 必須認得這個更新過的註冊封包，並且將網域資訊記錄起來，這些網域資訊除了可以用在 HA 轉送封包到 MONET 目前所在位置的用途外，這些資訊還需要用在與家網路的路由器交換路由規則。

3. 路由器代理人的功能：HA 必須有能力可以和家網路的路由器交換 RIP 訊息，由於持續地交換 RIP 訊息，所以家網路的路由器才能將傳送到 MONET 的封包繞送到 MONET 的家網路中。

3.3 動態之跨網路預先認證機制

為了達到快速換手的目的，因此我們將在移動網路移動到下個存取點之前，對下個存取點採用預先認證的機制，當移動網路確實地移動到該存取點時，移動網路可以不必再向網際網路遠端的認證伺服器做認證的動作，就能夠直接使用該存取點的各項服務，所以使用預先認證的機制將能大大地節省移動網路向認證伺服器認證的時間，藉此將能減少更換存取點時發生網路存取中斷的時間。在我們對下個存取點採用預先認證機制之前，我們必須先搜尋下個可能會到達的存取點位置，因此我們需要有一套位置管理的系統，來幫助我們尋得這些存取點的位置，又因為移動網路隨時會移動的特性，所以這套位置管理的系統必須要能夠適用於這種隨時會變更網路拓撲的移動網路。

基於上述的幾項理由，動態之跨網路預先認證機制的系統架構，如圖 3.6 所示：

1. Location Server：管理整個階層式移動網路位置資訊的伺服器，當 MR 啟動預先認證機制之前，MR 需要向位置伺服器發出 Next AR Discover 的訊息，然後，位置伺服器再根據所記錄的各個存取點的位置資訊，選取最可能會到達的存取點，並將這些存取點資訊回應告給 MR。

2. AAA Server：為 IEEE 802.1x 認證機制中的認證伺服器，MR 要透過存取點來存取網際網路的各項服務之前，都需要先經過 AAA Server 的認證才可以使用。

3. Access Router：用來存取網際網路的存取點，Access Router 屬於 IEEE 802.1x 認證機制中的認證者（Authenticator），MR 本身或者 MONET 內的存取點都可以擔任 Access Router 的角色。圖 3.6 的 AR1 為 MR 目前用來存取網際網路的存取點，而 AR2 與 AR3 為下個可能會到達的存取點。

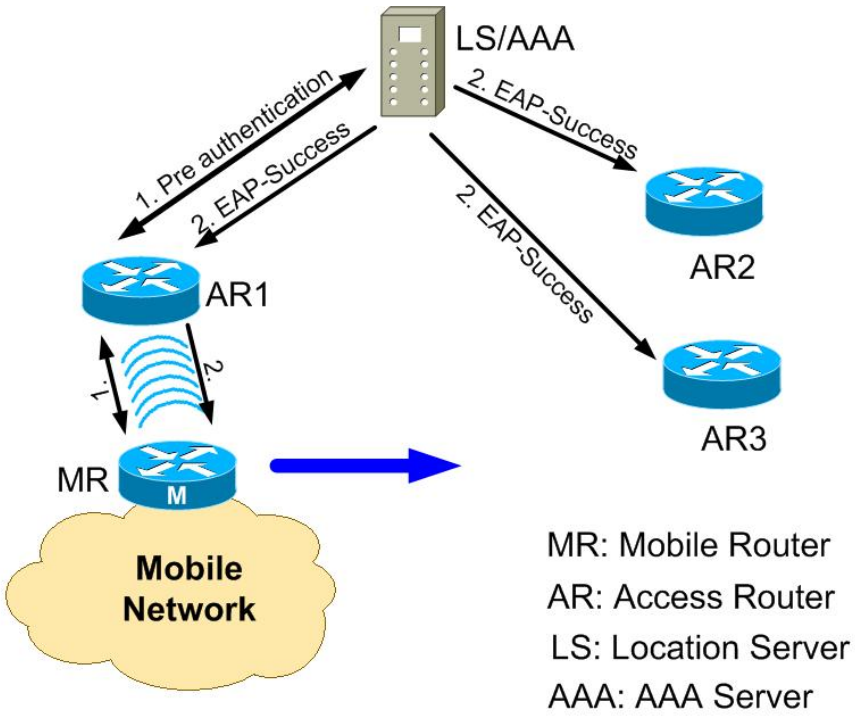

圖 3.6　跨網路預先認證機制的系統架構

如圖 3.6，當 MR 偵測到 AR1 訊號變弱時，MR 就會發出 Pre-Authentication request 訊息向 LS/AAA 伺服器詢問下個可能會到達的存取點，LS/AAA 伺服器在尋得一群候選存取點之後，會先與 MR 作一連串的 EAP 認證機制，最後 LS/AAA 伺服器會將 EAP-Success 的預先認證成功訊息傳送給搜尋到的候選存取點以及 MR。當 MR 到達 AR3 時，MR 就會向 AR3 做 Re-association 的步驟，並由 MR 送出 Update Location 訊息給位置伺服器，讓位置伺服器得以更新位置表內的位置資訊。

整個系統架構中，位置伺服器扮演的角色最為重要，因為位置伺服器不僅需要維護整個階層式移動網路的位置資訊，位置伺服器還需要根據 MR 所發出的 Pre-Authentication request 訊息來尋找下個最有可能會到達的存取點，而且選取這些存取點的準確率越高，預先認證機制的功能對於整個階層式移動網路快速換手的幫助就越大。

3.4　動態之跨網路預先認證機制的設計方法

跨網路預先認證機制的設計方法分成三個步驟，分別為：

1. Pre-Authentication 步驟：

在這個步驟中，我們必須考慮到何種情況要開始觸發跨網路預先認證機制，以及如何向下個可能會到達的存取點預先做認證。

2. Re-association 步驟：

當移動網路到達新的存取點時，就會進入 Re-association 的步驟，在這個步驟中，我們必須考慮到如何讓已經預先認證過的存取點，不用再向後端的認證伺服器做認證的動作。

3. Location Management 步驟：

Location Management 步驟主要在維護存取點的最新位置，因此在 Pre-Authentication 步驟與 Re-association 步驟時，都需要執行適當的動作。在 Pre-Authentication 步驟時，需要負責選取下個可能會到達的存取點，在 Re-association 步驟時，就必須要執行位置更新的處理流程。

底下幾個章節將詳細地介紹這三個步驟的設計方法。

3.4.1 Pre-Authentication 步驟

在 Pre-Authentication 步驟中，第一個要考慮的問題是何時開始觸發跨網路預先認證機制，我們都知道執行預先認證機制的目的是為了在變更存取點時執行快速換手，進而讓即時網路應用程式能夠盡快地使用網際網路的服務，因此在與目前存取點斷線之前，我們就必須向下個存取點執行預先認證機制，也就是說，跨網路預先認證機制的觸發時機就是在目前存取點斷線之前就要開始執行。然而判斷目前的存取訊號強弱，我們就能決定是否會與目前存取點斷線，當存取訊號變弱時，則代表我們正要離開目前存取點的服務範圍，因此我們就應該開始執行跨網路預先認證機制。所以當存取訊號減弱到某個低點時，就需要執行跨網路預先認證機制。

如圖 3.7 所示，在跨網路預先認證機制的系統架構中，位置伺服器的功能是用來管理整個階層式移動網路的位置資訊，因此在執行跨網路預先認證機制時，MR 需要先請求位置伺服器根據這些位置資訊，找出 MR 下個可能會到達的存取點位置，然而為了讓位置伺服器能有個參考座標以便找出下個存取點，所以 MR 必須將自己目前所在的位置告知位置伺服器，然後，位置伺服器會根據 MR 所傳來的位置資訊，在 Location Management 步驟中，以適當的程序找出下個可能到達的存取點，至於找尋下個存取點的方式，將會在 3.4.3 節中詳細地討論。

LS/AAA 伺服器根據 Location Management 步驟找出的候選存取點之後，LS/AAA 伺服器會先與 MR 執行一連串的 EAP 認證，當 LS/AAA 伺服器認證成功之後，LS/AAA 伺服器除了將 EAP-Success 訊息回傳給 MR 之外，LS/AAA 伺服器還會將 EAP-Success 訊息傳給適才選取出來的候選存取點。而每台候選的存取點接收到預先認證成功的訊息之後，必須記錄這些預先認證成功的訊

息，並且設定一個計時器來維護預先認證成功的訊息，當計時器超過時間，候選的存取點如果還未服務該 MR 時，就代表 MR 並未移動到這個存取點，那麼該存取點就必須將 MR 預先認證成功的訊息移除。

整個 Pre-Authentication 步驟的示意圖，如下：

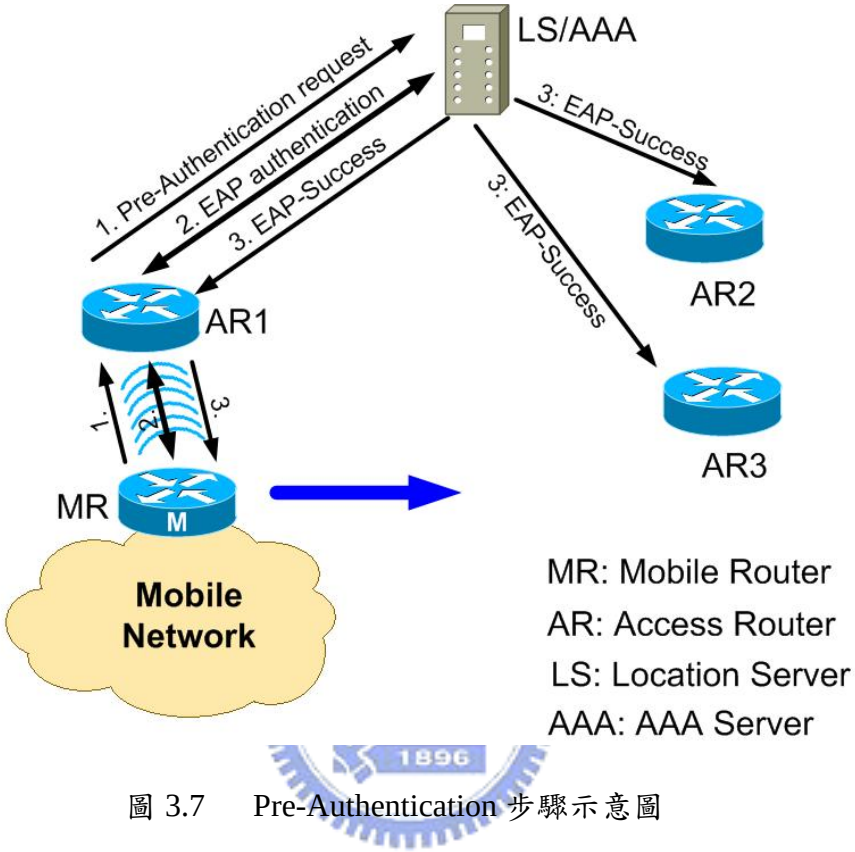

圖 3.7　Pre-Authentication 步驟示意圖

整個 Pre-Authentication 步驟的運作流程圖，如下：

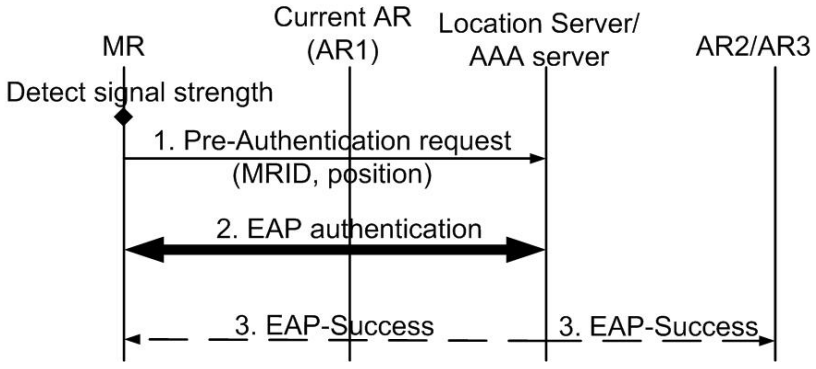

圖 3.8　Pre-Authentication 步驟運作流程圖

如圖 3.8 所示，Pre-Authentication 步驟的運作流程如下所示：

1. MR 偵測到 AR1 的訊號強度變弱到某個低值，則開始執行跨網路預先認

證機制，MR 會透過 AR1 傳送 Pre-Authentication request 訊息給位置伺服器。

2. 位置伺服器取得 Pre-Authentication request 訊息後，取得訊息中 MR 目前所在的位置作為位置參考點，算得下個可能到達的存取點為 AR2 和 AR3，接著由 AAA 伺服器會與 MR 執行一連串的 EAP 認證。

3. AAA 伺服器將預先認證成功的訊息傳送給 MR 之外，還會將預先認證成功的訊息轉送給候選的存取點（亦即 AR2 與 AR3 等）。而 AR2 與 AR3 會以計時器來維護預先認證成功的訊息，當計時器超過指定時間，代表 MR 將不會使用 AR2 或 AR3 的存取點服務，因此就需要將該 MR 的預先認證成功訊息移除。

3.4.2 Re-association 步驟

2.3.4 節所提到的 IEEE 802.1x 認證流程中，認證者（Authenticator）會先向申請者（Supplicant）發出一個 EAP-Request/Identity 訊息，而申請者會回應一個 EAP-Response/Identity 訊息，經由這個 Identity 訊息，認證者就能夠知道申請者的身分，然後，認證者再根據這個身分向認證伺服器（AAA Server）執行一連串認證的動作。

如圖 3.2 所示，階層式移動網路中，AR 即為認證者的角色，MR 即為申請者的角色，當 MONET 移動到新存取點（AR2）時，跨網路預先認證機制就會進入 Re-association 步驟，首先，AR2 會先向 MR 發出一個 EAP-Request/Identity 訊息，MR 也同樣地回應一個 EAP-Response/Identity 訊息，當新存取點接收到回覆訊息後，新存取點就能認得 MR 的身分，假使新存取點有 MR 預先認證成功的記錄，新存取點就不會再向認證伺服器執行一連串認證的動作，而直接讓 MR 使用新存取點的各項服務；假使新存取點沒有任何 MR 預先認證成功的記錄，則新存取點就必須促使 MR 與認證伺服器執行原先的 IEEE 802.1x 認證動作。

位置伺服器必須管理整個階層式移動網路的位置資訊，當 MR 移動到新存取點時，MR 必須告知位置伺服器它的新位置資訊，因此當 MR 向新存取點認證成功，並且已經可以使用新存取點的各項服務時，MR 還必須傳送一個 Update Location 訊息來告知位置伺服器目前所在的位置，當位置伺服器收到該訊息後，位置伺服器就會執行一連串更新階層式移動網路位置的動作，至於如何更新整個階層式移動網路，將會在 3.4.3 節－Location Management 步驟中詳細地作探討。

整個 Re-association 步驟的示意圖，如圖 3.9 所示：

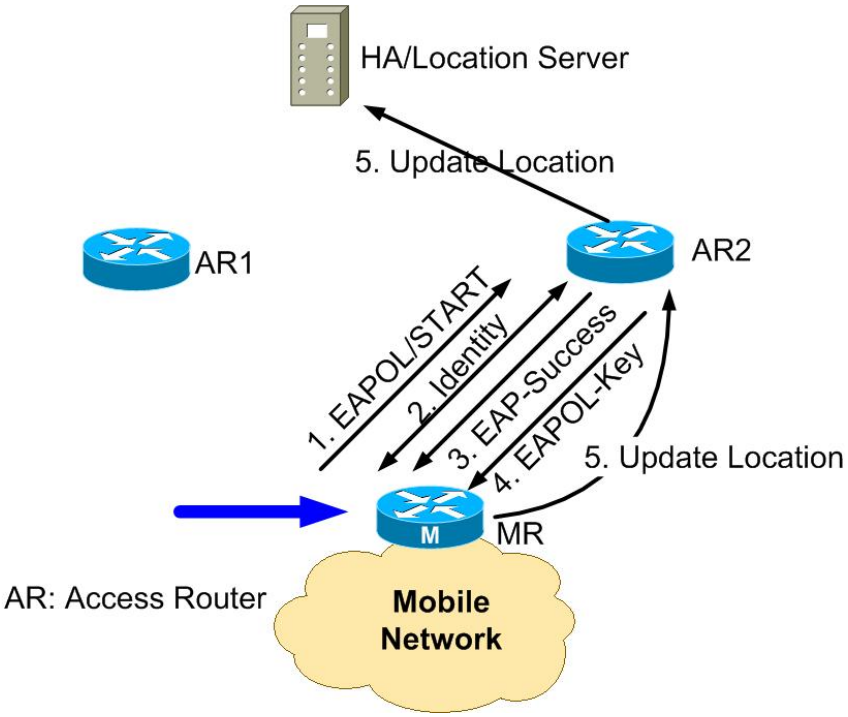

圖 3.9　Re-association 步驟示意圖

整個 Pre-Authentication 步驟的運作流程圖，如圖 3.10：

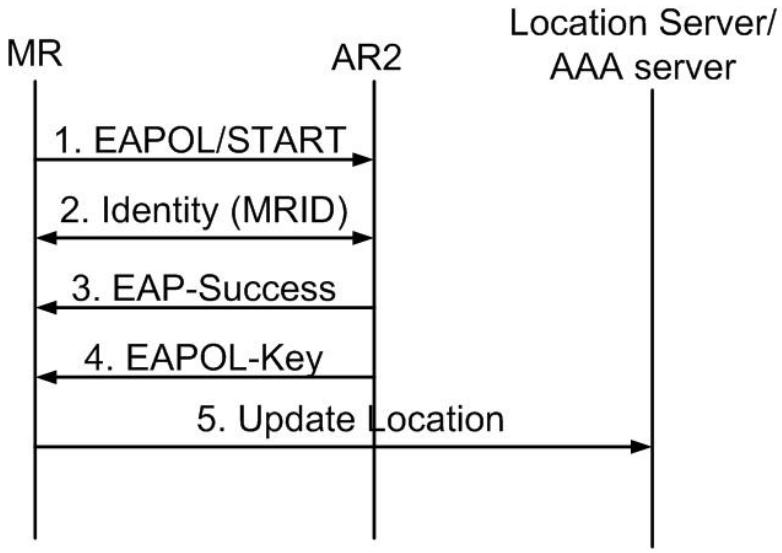

圖 3.10　Re-association 步驟運作流程圖

如圖 3.9 與圖 3.10 所示，Re-association 步驟的運作流程如下所示：

1. MR 以一個 EAPOL-Start 訊息開始 IEEE 802.1x 認證動作的運作流程，AR2 會發出一個 EAP-Request/Identity 訊息請求 MR 告知身分。
2. MR 回應一個 EAP-Response/Identity 訊息給 AR2，此時，AR2 就能得知

MR 的身分。

3. 因為 MR 已經對 AR2 執行過跨網路預先認證的機制，因此 AR2 會直接向 MR 發出 EAP-Success 的認證成功訊息，AR2 不需要再對後端的認證伺服器執行認證動作，就能直接允許 MR 使用 AR2 的各項網際網路服務。

4. 接著 AR2 會傳送 EAPOL 的金鑰給 MR，往後 MR 傳送封包時，MR 都會以這把金鑰來進行加密封包的動作。

5. 最後，MR 會發出一個 Update Location 訊息給位置伺服器，藉此訊息來讓階層式移動網路移動到新存取點時，位置伺服器能夠將階層式移動網路內所有受位置伺服器管理的節點作更新位置的動作。

3.4.3 Location Management 步驟

跨網路預先認證機制中，最重要的步驟就是 Location Management 步驟，不論是 Pre-Authentication 步驟中尋找下個可能會到達的存取點，又或者是 Re-association 步驟中更新位置伺服器內的位置資訊，都需要藉由 Location Management 步驟來協助處理。Location Management 步驟簡單來說就是執行位置伺服器的運作機制，我們所設計的位置伺服器除了會記錄固定存取點之外，還記錄階層式移動網路中所有具有存取點功能的節點（包括 MR 與 LFR 等）。位置管理設計可以分成三個設計重點，分別為：位置表的資料結構、尋找存取點的策略、更新位置表的程序，以下三個小節，我們將針對這三個設計重點，來介紹我們的位置管理設計方法。

3.4.3.1 位置表的資料結構

Pre-Authentication 步驟中 AAA 伺服器需要負責傳送預先認證成功的訊息給所有候選的存取點，因此位置表內必須記錄存取點的 IP 位址，才能讓 AAA 伺服器知道候選存取點在網際網路上的位址。

另外，在位置伺服器尋找存取點的程序中，位置伺服器需要透過存取點的位置資訊來執行尋找存取點程序，所以位置表內一定要記錄存取點的位置。另外，位置伺服器在尋找存取點程序中會使用到 MR 的移動速率作為選取的依據，我們雖然可以由位置資訊取得 MR 的移動距離，但是我們還必須再記錄時間資訊才可算出 MR 的移動時間，進一步才可計算出 MR 的移動速率。

由於位置伺服器需要記錄所有存取點的資訊，包括階層式移動網路內的存取點，因此位置伺服器必須記錄這種階層性的關係，才能讓位置伺服器可以順利地更新所有移動過的存取點位置資訊，然而記錄階層性的方式有兩種，第一種方式是由父存取點記錄所有子存取點的資訊；第二種方式是由子存取點記錄單一父存取點的資訊，如果使用第一種記錄的方式，父存取點就需要記錄多個

子存取點的資料，所以我們使用第二種記錄的方式，也就是讓每個存取點只記錄父存取點資訊，由於每個存取點都會記錄目前幫忙服務的父存取點，因此階層性的關係就自然而然地能夠被記錄在位置伺服器中。

所以位置表資料結構需要含有五個資料欄位，分別為：存取點 ID、存取點 IP 位址、存取點絕對位置、存取點更新時間、以及父存取點 ID。

A. 存取點 ID（ARID）：存取點的 MAC 位址。

B. 存取點 IP 位址（ARIP）：當 AAA 伺服器要傳送預先認證的訊息給候選存取點時，需要由這個存取點 IP 位址，才能將預先認證的訊息傳給候選存取點。

C. 存取點絕對位置（Position）：存取點實際環境中的絕對位置。

D. 存取點更新時間（Update time）：這個欄位將記錄存取點更新的時間，藉由這個欄位的儲存值，可以讓位置伺服器算出 MR 的移動速率以便使用在尋找存取點的策略中（見 3.4.3.2 節）。

E. 父存取點 ID（PARID）：父存取點的 MAC 位址，藉由這個欄位的儲存值，可以讓位置伺服器記錄整個階層式移動網路的階層式關係。

以圖 3.11 的階層式移動網路拓撲而言，位置表的資料結構如表 3.1 所示。

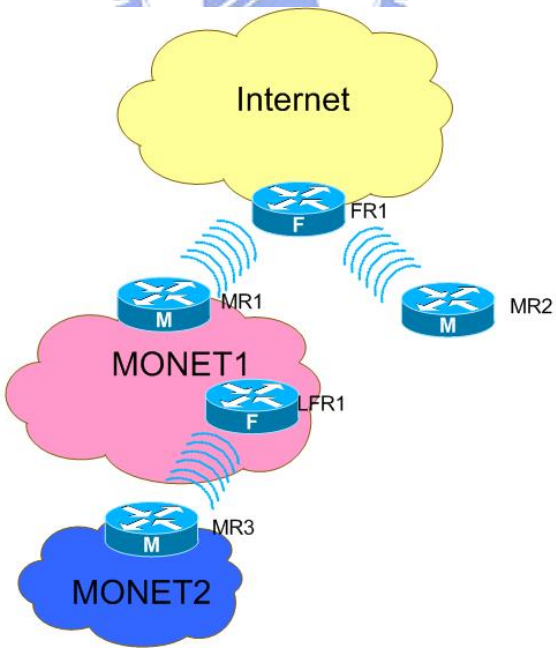

圖 3.11　階層式移動網路的網路拓撲

Location Table				
ARID	MRIP	Position	Update Time	PARID
FR1 MAC	FR1 IP	FR1 position	FR1 time	N/A
MR1 MAC	MR1 IP	MR1 position	MR1 time	FR1 MAC
MR2 MAC	MR2 IP	MR2 position	MR2 time	FR1 MAC
MR3 MAC	MR3 IP	MR3 position	MR3 time	LFR1 MAC
LFR1 MAC	LFR1 IP	LFR1 position	LFR1 time	MR1 MAC

表 3.1　位置伺服器的位置表

3.4.3.2 尋找存取點的策略

位置伺服器的位置表會記錄 MR 進入存取點時的絕對位置和時間資訊，然而在 Pre-Authentication 步驟中，MR 如果偵測到目前使用的存取點訊號強度變弱時，MR 會發出 Pre-Authentication request 訊息，並且將 MR 目前的所在位置告知位置伺服器，因此位置伺服器就會有 MR 的兩個參考點位置，分別為：位置表內所記錄的參考點位置，以及 Pre-Authentication request 訊息內的參考點位置。經由這兩個參考點位置，位置伺服器就能夠取得 MR 的移動方向與移動距離，另外，位置伺服器會根據 Pre-Authentication 訊息送來的時間，與位置表內 MR 進入存取點時的時間資訊，計算出兩個參考點之間的時間差距，因此位置伺服器就能使用 MR 的移動距離和時間差距算出 MR 的移動速率。藉由 MR 移動速率的資訊就可以定出兩個參數－選取半徑（r）與選取角度（θ），並進而算出一目標扇形區域（如圖 3.12）。

選取半徑與選取角度兩個參數值根據不同的狀況，會有不同的設定值，有兩個因素會影響參數值的設定，分別為：MR 的移動速率，以及存取點的服務涵蓋範圍。MR 移動速率越快，則代表下個可能會使用的存取點距離會較遠，因此選取半徑的設定值就要隨之增加，至於，選取角度則不會受到 MR 移動速率的影響；存取點的服務涵蓋範圍越大，則代表可以選取較遠的存取點來做為下個服務的存取點，因此選取半徑的設定值就會隨之增加，同時，也代表周圍可以服務的存取點增多，也就是，選取角度的設定值可以隨之增加。根據上面的討論，我們可以將選取半徑和選取角度，與 MR 移動速率和存取點服務範圍，由以下兩個數學式表示：

$$\begin{cases} \gamma = \kappa_1 \times v \times c \\ \theta = \kappa_2 \times c \end{cases}$$

其中r代表選取半徑、θ代表選取角度、v代表MR移動速率、c代表存取點服務涵蓋的範圍、以及K_1與K_2代表兩個常數值。

圖 3.12 說明尋找存取點的方式，以 MR 移動方向決定扇形中軸的方向，接著依據 MR 移動速率與存取點的服務涵蓋範圍，所定出的選取半徑與選取角度形成一個扇形區域，然而在扇形區域內的 AR2 和 AR3 即為位置伺服器所選出的候選存取點。

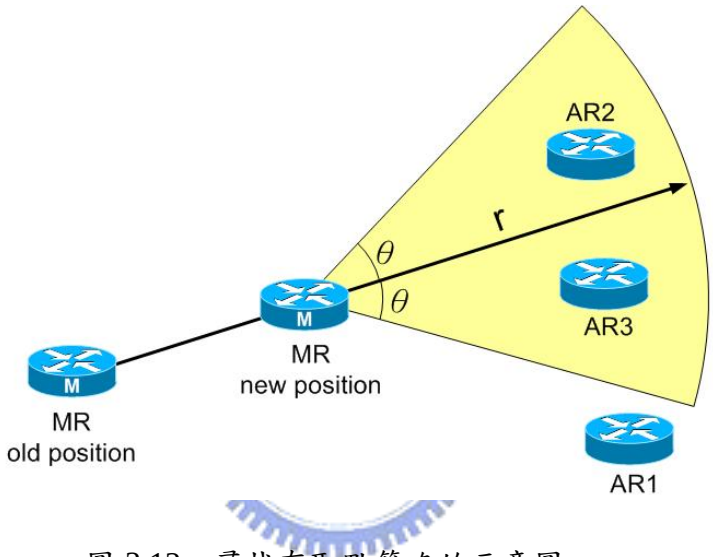

圖 3.12　尋找存取點策略的示意圖

3.4.3.3 更新位置表程序

由於位置伺服器會記錄移動網路內每台存取點的位置資訊，因此當階層式移動網路移動到不同存取點時，階層式移動網路內的所有存取點位置資訊都需要執行更新位置表程序，不過由於位置表的資料結構會記錄階層式移動網路的階層性關係，所以位置伺服器可以很清楚地知道這個階層式移動網路內包含哪些存取點，以及需要更新哪些存取點的位置資訊。也就是只要由正在更新存取點的 MR 負責在 Re-association 步驟中發出 Update Location 訊息，位置伺服器就會為 MR 之下的所有 AR 更新位置，其詳細更新方式如下：

在更新位置表程序中會先宣告一個佇列，這個佇列是用來記錄尚未經過處理的父存取點，然而發出 Update Location 訊息的 MR 正是整個移動網路的第一層父存取點，因此 MR 為第一個放入佇列中等待處理的節點。由 3.4.3.1 一節中，我們可以知道位置表內的 ARID 欄位代表這個項目的父存取點，因此當

這個項目的 ARID 欄位等於佇列中第一個節點時，則代表這個項目的父存取點為佇列中的第一個節點，也就是，這兩個節點所管理的移動網路為同向移動的兩個移動網路，所以兩個節點都需要更新位置資料，除此之外，以這個項目作為父存取點的節點也需要更新位置資料，因此這個項目也必須要放在佇列中等待處理。當佇列中所有節點都處理過後，就代表整個階層式移動網路的位置表都已經經過位置更新的程序。

更新位置表程序的流程圖，如圖 3.13 所示：

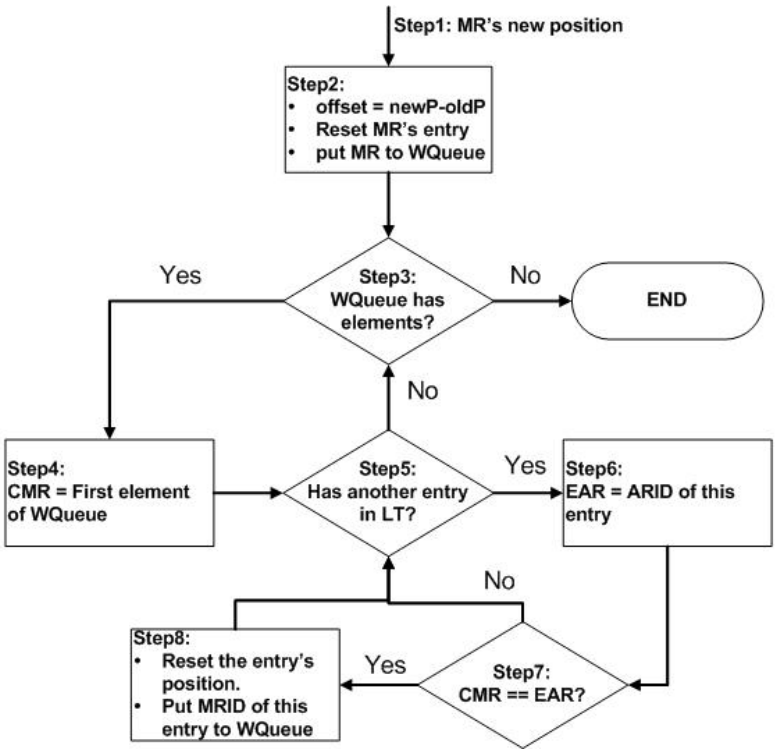

圖 3.13　更新位置表程序的流程圖

1. 位置伺服器收到由 MR 於 Re-association 步驟中發出的 Update Location 訊息，以取得 MR 的新位置。

2. 位置伺服器算出 MR 新位置與位置表內 MR 舊位置的位移值，將此位移值存於變數 *offset*，然後，更新位置表內 MR 項目的位置資料和時間資料（也就是 Position 欄位與 Time 欄位），並且，將 *MRID* 放入待處理的佇列 *WQueue*。

3. 判斷 *WQueue* 佇列內是否還有未處理的節點，如果還有未處理的節點，則繼續進行步驟 4，如果所有節點都已經處理完，則結束更新位置表程序。

4. 取出 *WQueue* 佇列內的第一個待處理的節點存於變數 *CMR* 中。

5. 判斷位置表內是否還有未處理完的項目，如果還有未處理的項目，則繼續進行步驟 6，如果位置表內所有項目都已經處理完，則代表位置表內所有以這個節點為存取點的項目都已經更新位置資訊，因此返回步驟 3 繼續處理 *WQueue* 佇列內的下個節點。

6. 從位置表取得這筆項目的 *ARID* 欄位，也就是取得這筆項目的存取點，並存於變數 *EAR* 中。

7. 判斷 *CMR* 是否等於 *EAR*，如果 *CMR* 不等於 *EAR*，則返回步驟 5 繼續處理下個項目；如果 *CMR* 等於 *EAR*，則代表這筆項目是以目前的 *CMR* 當作存取點來存取網際網路，因此必須進入步驟 8 更新位置表內的位置資訊。

8. 將 *offset* 位移值加入這筆項目的 *Position* 欄位以更新這筆項目的位置資訊，並把這筆項目的 *MRID* 放入待處理的 *WQueue* 佇列內，然後，返回步驟 5 繼續處理下個項目。

更新位置表程序的虛擬程式碼，如下所示：

```
Offset = new MR position – old MR position
ResetLTEntry(newMREntry)
Put MRID to WQueue.
CMR = MRID;
While ( CMR != EOF)
{
  EAR = FirstLTEntry(LTable);
  While (EAR != NULL)
  {
      if (CMR == EAR)
      {
          ResetLTEntry(EAREntry)
          Put EAR to WQueue
      }
      EAR = getNextLTEntry(LTable);
  }
  CMR = getNextWQElement(WQueue);
}
```

3.5 動態之跨網路預先認證機制的系統運作流程

整個跨網路預先認證機制的系統運作流程，如圖 3.14 所示：

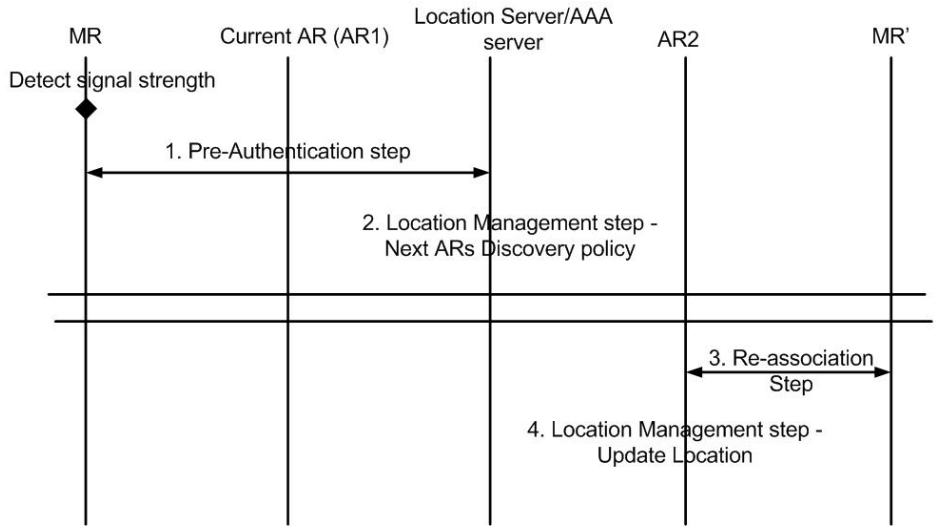

圖 3.14　跨網路預先認證機制的運作流程

1. 當 MR 偵測到存取點的訊號強度變弱時，MR 會進入到 Pre-Authentication 步驟，對下個可能會到達的存取點做預先認證的動作。

2. 位置伺服器會在 Pre-Authentication 步驟的過程中進入 Location Management 步驟的尋找存取點策略，以找尋下個可能會到達的存取點。

3. 當MR移動到新存取點時（即為圖中的MR'），MR'就會進入Re-association 步驟，以重新連結新的存取點。

4. Re-association 步驟結束後，位置伺服器就會根據 Update Location 訊息，進入 Location Management 步驟的更新位置表程序，將位置表內所有相關的存取點作更新位置的動作。

第四章： 跨網路預先認證的階層式移動網路之實作

4.1 系統之軟硬體需求

跨網路預先認證的階層式移動網路系統中，包括六項系統元件，分別為：Location Server、AAA Server、Access Router、Mobile Router、Home Agent 等，以下將分別針對這六項元件的軟硬體需求做詳細地介紹：

- Location Server：

  作業系統：Linux Red Hat 9〔14〕

  軟體需求：實作 3.4.3 節中位置表資料結構、尋找存取點策略、以及更新位置表程序的伺服器。

- AAA Server：

  作業系統：Linux Red Hat 9

  軟體需求：

  1. FreeRADIUS〔15〕：需作修改以接受並處理跨網路預先認證機制的訊息封包。

- Access Router：

  硬體設備：具有兩張網路介面的路由器。

  作業系統：Linux Red Hat 9

  軟體需求：

  1. Routed：使 Access Router 成為一台路由器。
  2. Host AP driver〔16〕：使 Access Router 成為一台 IEEE 802.11 WLAN 存取點。
  3. Host AP Daemon〔16〕(Hostapd)：使 Access Router 成為 IEEE 802.1x 認證機制中的 Authenticator 角色，並可擔任 FreeRADIUS Authentication 的用戶端，需作修改以轉送及處理跨網路預先認證機制的訊息封包。

- Mobile Router：

  硬體設備：具有兩張網路介面的移動路由器。

作業系統：Linux Red Hat 9

軟體需求：

1. Routed：使 Access Router 成為一台路由器。
2. Open1x XSupplicant〔17〕：使 Mobile Router 成為 IEEE 802.1x supplicant 的角色，需作修改以發出跨網路預先認證機制的訊息封包。
3. Dynamics HUT Mobil IP〔18〕Client：使 Mobile Router 成為 MIPv4 中 MN 的角色，需作修改以符合階層式移動網路的需求。

- Home Agent：

作業系統：Linux Red Hat 9

軟體需求：

1. Routed：當 Mobile Router 移出家網路時，負責與家網路上的路由器交換 RIP 訊息封包，以維護送往階層式移動網路的封包。
2. Dynamics HUT Mobil IP Home Agent：使其成為 MIPv4 中 HA 的角色，需作修改以符合階層式移動網路的需求。

- LFN

LFN 可以是使用任何作業系統的網路節點。

4.2 階層式移動網路之實作

階層式移動網路的實作是採用 Dynamics HUT Mobile IP 對 Mobile IPv4 的實作方法來進行進一步的修改，因此我們必須要先對 Dynamics HUT Mobile IP 的實作方式作深入地了解，然後，才能進一步的作修改以達成階層式移動網路的需求。

如圖 4.1 與圖 4.2 所示，MN 的 Home 網路網域為 192.168.2.0/24，而 Foreign 網路網域為 192.168.1.0/24，另外 MN 的家位址為 192.168.2.3，而 MN 的 HA IP 位址為 192.168.2.2。在 Dynamics HUT Mobile IP 中，當 MN 向 HA 註冊結束後，HA 會執行底下幾個重要的程序：

1. 新增一個 TUNL0 網路介面：這個網路介面正是 Mobile IPv4 中的通道機制，所有經由這個網路介面的封包，都會經過 IP-in-IP 的封包封裝。
2. 新增一條路由路徑：HA 的路由表會增加一條路由路徑，這條路由路徑的

內容為目的地封包如果為 MN 的 IP 位址（192.168.2.3）時，則將封包送往上述新增的網路介面（TUNL0）。

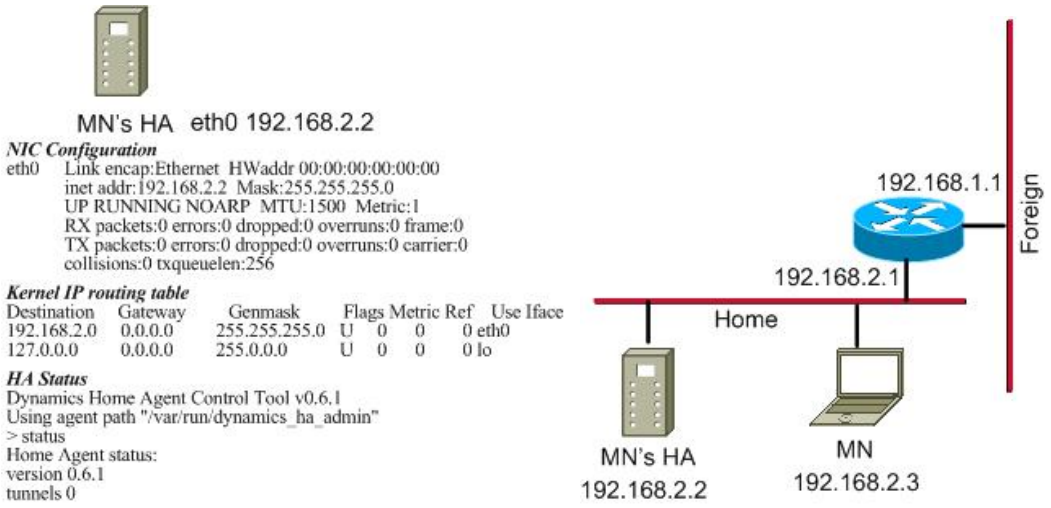

圖 4.1　HA 系統狀態 (MN 位於家網路)

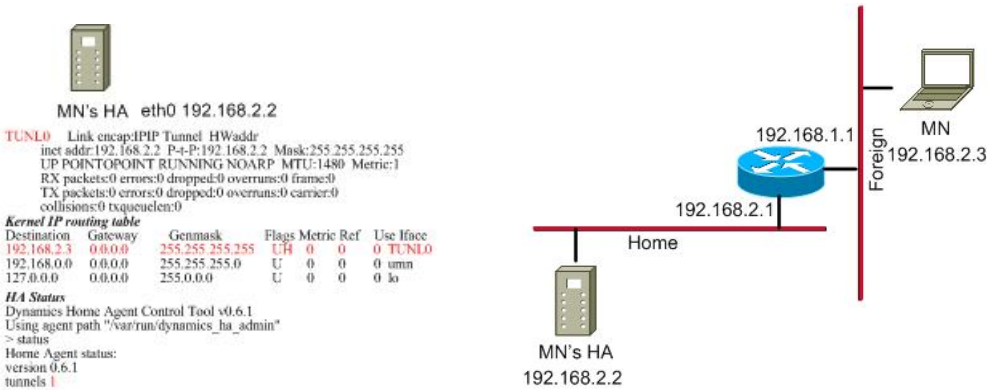

圖 4.2　HA 系統狀態 (MN 向 HA 註冊後)

因此當 CN 送封包到 MN 時，該封包運作的流程如下所述：

1. CN 送出一個目的地 IP 位址為 MN 位址的封包。
2. 由於 HA 會幫忙回應 ARP 請求，因此當封包到達 MN 家網路時，HA 就會幫忙 MN 截收這個封包。
3. HA 接收到封包後會對照其路由表，由於 HA 在 MN 註冊後所新增的路由路徑是送往 MN 的封包都轉送到 TUNL0 網路介面，因此該封包就會送往 TUNL0 網路介面中。
4. TUNL0 網路介面將封包封裝成 IP-in-IP 封包，並再次對照 HA 的路由表，將 IP-in-IP 封包送往 MN 目前所在的位置。

5. MN 解開 IP-in-IP 封包後，就會取得原 CN 送來的封包。

4.2.1 Mobile Router 之實作

根據 3.2.1 節中，我們可以整理出 MR 必須包含三種功能，分別為：路由器功能、MIPv4 的 MN 功能、以及傳送 MONET 網域功能。

1. 路由器功能：

路由器功能的目的是為了維護 MONET 內部網路的路由繞送規則，在家網路中，MR 的路由器功能會收發 RIP 訊息，以確保送往 MONET 的封包可以送達 MR。在 Linux Red Hat 9 作業系統中提供 routed 程式，這個程式可以根據路由表的資料，發出 RIP 的訊息封包，並且針對收到的 RIP 訊息，更改路由表的資料。因此 MR 必須執行 routed 程式，以達到路由器的功能。

2. MIPv4 的 MN 功能：

MR 離開家網路後的行動管理會經由 Dynamics HUT Mobile IP 中的 MN 程式來幫忙處理，MN 程式會定時接收 Agent Advertisement 封包，經由 Agent Advertisement 封包就能判斷 MR 是否位於家網路中，假使 MR 不在家網路中，MR 就會發出註冊封包向 HA 作註冊的動作，HA 就會執行相關的步驟，最後會將送往 MR 的封包轉送給 MR。

3. 傳送網域功能：

在我們的階層式移動網路的設計中，MR 必須告知 HA 整個 MONET 所連結的網域，由於 MR 只要移動到不同的網路環境時，MR 就會向 HA 發出註冊的封包，因此我們將這些網域的訊息放置於註冊封包中傳送給 HA，所以我們必須修改 Mobile IPv4 中的註冊訊息封包，以達到我們的要求。

4.2.1.1 註冊訊息的封包格式

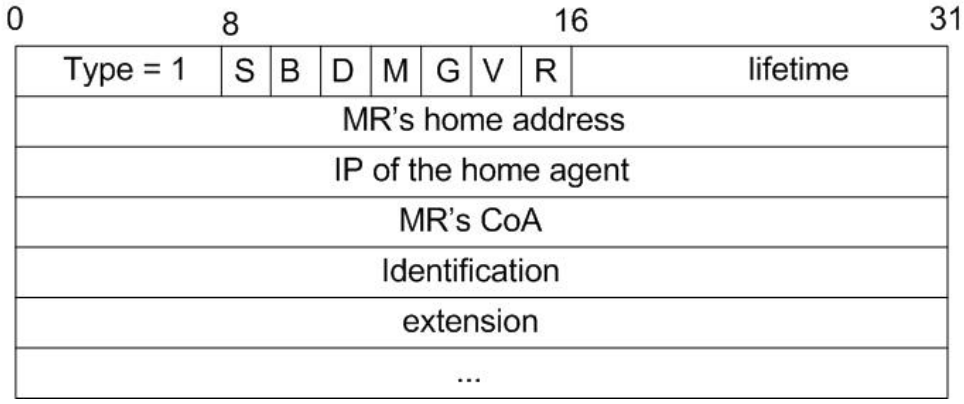

圖 4.3 MIPv4 之 MN 的註冊訊息封包格式

圖 4.3 為 Mobile IPv4 所定義的註冊訊息封包格式，其中 R 位元代表保留位元，因此我們將送出網域資料的註冊訊息封包使用 R 位元來作為區分，當註冊訊息封包含有 MONET 網域資料時，R 位元就設定為 1；相反地，當註冊訊息封包為一般的 Mobile IPv4 註冊訊息，則 R 位元就設定為 0。更改後的註冊訊息封包格式，如下所示：

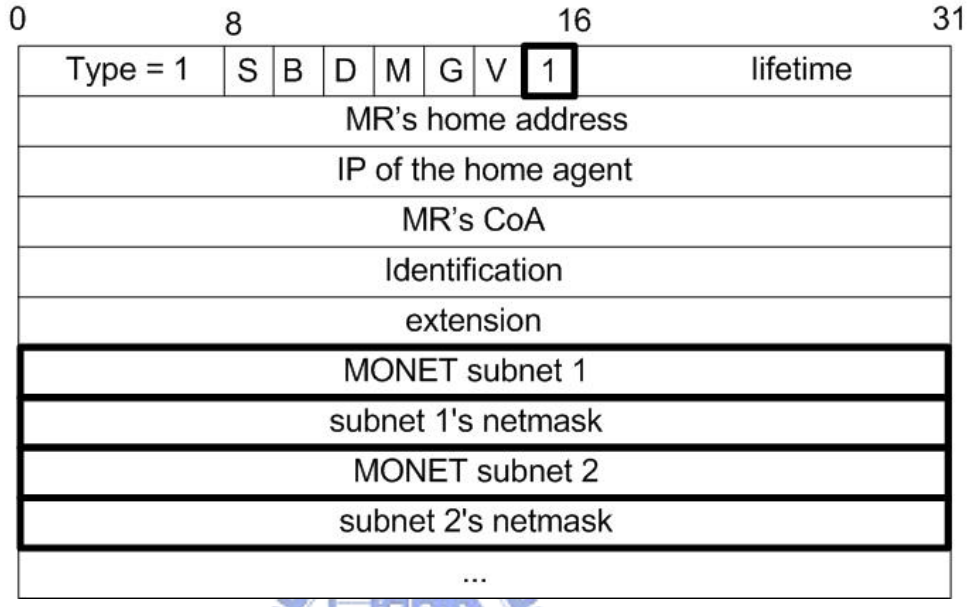

圖 4.4　MONET 之 MR 的註冊訊息封包格式

所以當 MR 離開家網路後，MR 要傳送註冊訊息封包給 HA 時，MR 除了需要封裝原先 Mobile IPv4 對註冊訊息封包格式之外，還需要執行底下幾個步驟：

1. 將 R 位元設定為 1。
2. 在 extension 之後，加入 MR 之下所管理之網域資訊，以及這些網域的遮罩。
3. 然後對註冊訊息封包的查驗作修改，以使得修改後的註冊訊息封包也能正常地送出。

4.2.2 Home Agent 之實作

根據 3.2.2 節中，我們可以整理出 MR 必須包含三種功能，分別為：MIPv4 的 HA 功能、記錄 MONET 網域的功能、以及路由器代理人的功能。

1. MIPv4 的 HA 功能：

當 MR 離開家網路時，HA 就必須經由 Dynamics HUT Mobile IP 中的 HA

程式來為 MR 作行動管理，HA 程式除了要執行原先 Mobile IPv4 的標準處理程序之外，還必須處理由 MR 所傳來被更改過的註冊訊息封包，由於，註冊訊息封包內含有 MONET 的網域資訊。HA 必須先檢查註冊封包中的 R 位元是否設定為 1，如果 R 位元設定為 1，表示該註冊封包含有 MONET 的網域資訊，然後再從這些註冊訊息封包中擷取 MONET 的網域資訊。

2. 記錄 MONET 網域的功能：

在 Dynamics HUT Mobile IP 的設計實作中，CN 傳送到 MN 的封包都是經由查詢路由表的方式來決定封包要送往哪個通道以包裝 IP-in-IP 的封包，因此我們只要在 HA 的路由表中增加多筆路由規則，將這些註冊訊息中所擷取的 MONET 網域資訊都送往 HA 與 MR 之間的通道，如此一來，不僅可以將送往 MONET 內的封包都經由通道機制轉送到 MONET，還可以由路由表來記錄 MONET 所含有的網域資料。

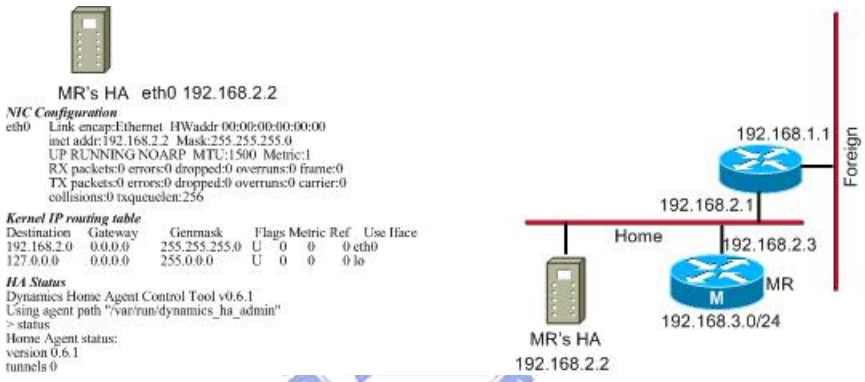

圖 4.5 HA 系統狀態 (MR 位於家網路)

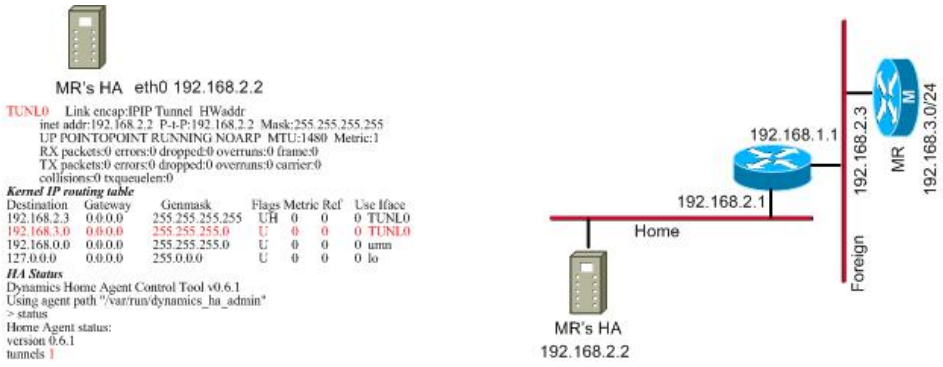

圖 4.6 HA 系統狀態 (MR 向 HA 註冊後)

如圖 4.6 所示，當 MR 移動到家網路之外的網路，並且向 HA 註冊後，HA 會新增一個 TUNL0 網路介面，並且在路由表中，除了新增一筆由 MR 的 IP 位址（192.168.2.3）到 TUNL0 網路介面的路由路徑之外，另外還需要新增一筆 MONET 內部網域（192.168.3.0/24）到 TUNL0 網路介面中。如此一來，

MONET 內部的網域資訊就會儲存於路由表中。

3. 路由器代理人的功能

兩個路由器所維護的路由表會經由 RIP 訊息的交換來動態地更新路由規則，當 MR 離開家網路時，HA 就要幫忙維護家網路的路由器之路由規則。我們會將註冊訊息中所擷取的網域資料都儲存於 HA 的路由表中，正好符合於 RIP 訊息是根據路由表來動態更新路由規則的特性，因此我們只要在 MR 離開家網路之後，在 HA 中執行 routed 程式，以此來幫忙維護家網路的路由器之路由規則即可。

4.3 動態之跨網路預先認證機制的實作

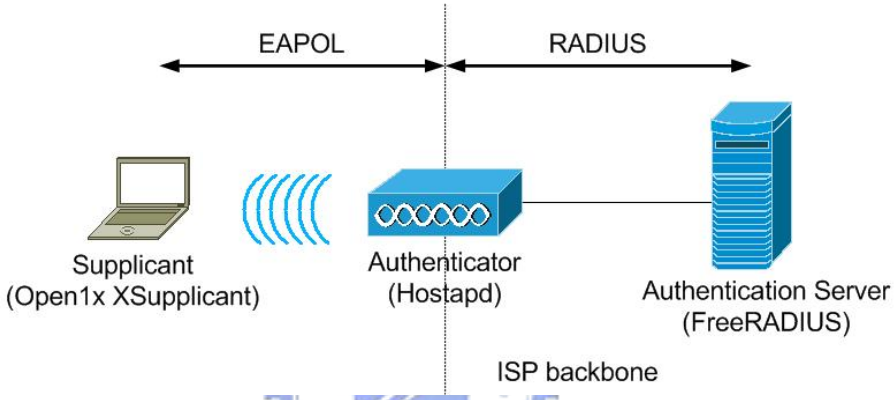

圖 4.7 IEEE 8021.x 實作示意圖

圖 4.7 列出我們實作 IEEE 802.1x 認證機制時，各元件所架設的應用軟體，Supplicant 角色我們採用 Open1x XSupplicant 應用軟體實作；Authenticator 角色也就是我們的 MR，我們採用 Hostapd 應用軟體實作；Authentication Server 角色我們採用 FreeRADIUS 應用軟體實作。其中，Authenticator 角色必須先架設 Hostap driver 應用軟體，而 IEEE 802.1x 認證機制則全都在 Hostapd 應用軟體中實作。然而 Supplicant 與 RADIUS 伺服器之間需要透過 Authenticator 來轉送認證機制，因此底下我們必須先對 Hostapd 應用軟體的運作方式作個簡介。

Hostapd 應用軟體將整個 IEEE 802.1x 認證機制分成兩部分，並且使用兩個狀態機器分別作處理，這兩個部分為：Supplicant 與 Authenticator 之間的 EAPOL 認證、以及 Authenticator 與 RADIUS 伺服器之間的 RADIUS 認證。Hostapd 應用軟體將處理 EAPOL 認證的狀態機器命名為 AUTH_PAE 狀態機器；將處理 RADIUS 認證的狀態機器命名為 BE_AUTH 狀態機器。以下將分別針對這兩個狀態機器的狀態轉換作簡單介紹。

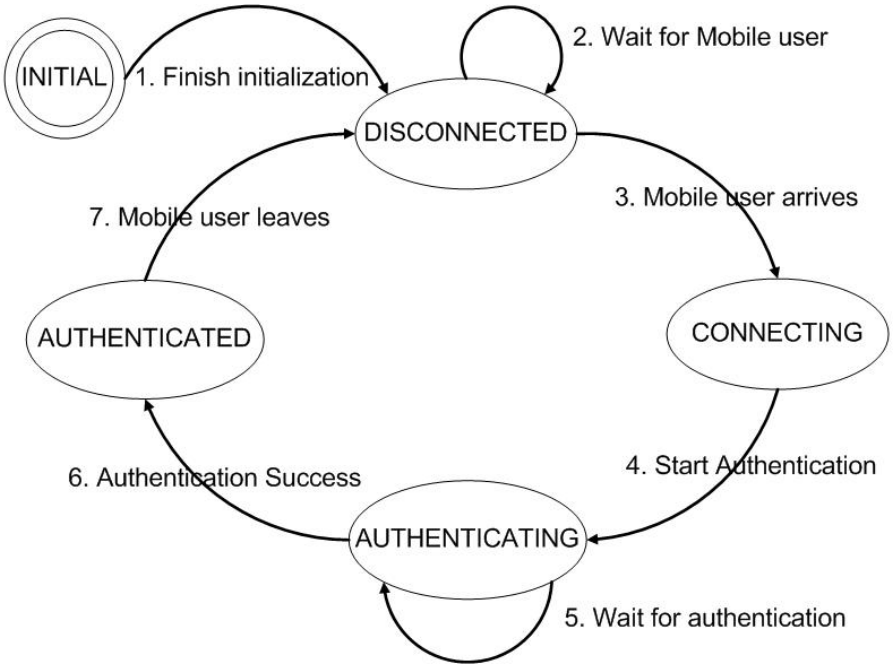

圖 4.8　AUTH_PAE 狀態機器的狀態流程圖

圖 4.8 為 AUTH_PAE 狀態機器的狀態流程圖，其流程為：

1. 執行 EAPOL 認證的初始化設定，當完成初始化設定後，則由 INITIAL 狀態進入 DISCONNECTED 狀態。
2. 如果沒有無線使用者進入，則繼續停留在 DISCONNECTED 狀態。
3. 當無線使用者進入後，則進入 CONNECTING 狀態。
4. 開始認證機制時，就會由 CONNECTING 狀態進入 AUTHENTICATING 狀態。
5. 當 RADIUS 後端認證還未完成，則會繼續停留在 AUTHENTICATIN 狀態中。
6. 當 RADIUS 後端認證完後後，則會由 ATUTHENTICATING 狀態進入 AUTHENTICATED 狀態中，此時，無線使用者就可使用該存取點的網際網路服務。
7. 等到無線網路使用者離開後，則進入 DISCONNECTED 狀態。

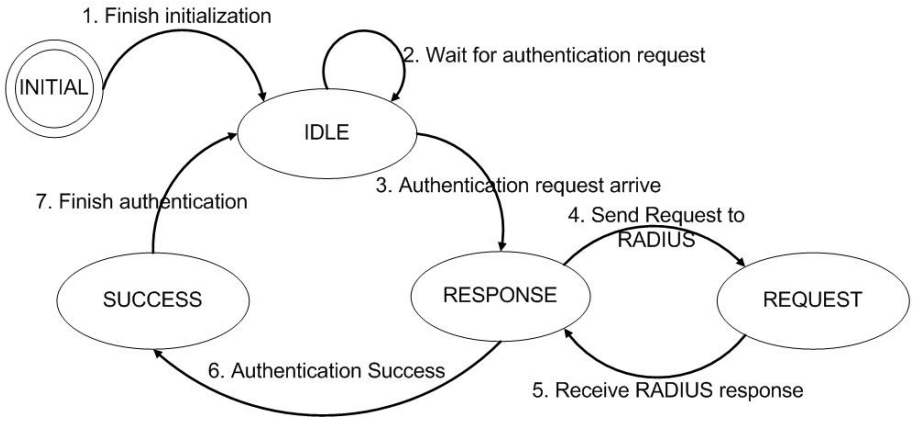

圖 4.9　BE_AUTH 狀態機器的狀態流程圖

圖 4.9 為 BE_AUTH 狀態機器的狀態流程圖，其流程為：

1. 執行 RADIUS 認證的初始化設定，當完成初始化設定後，則由 INITIAL 狀態進入 IDLE 狀態。
2. 如果不需要後端 RADIUS 認證，則繼續停留在 IDLE 狀態。
3. 如果需要後端 RADIUS 認證，則由 IDLE 狀態進入 RESPONSE 狀態。
4. 當 Authenticator 傳送 RADIUS 認證請求給 RADIUS 伺服器時，則由 RESPONSE 狀態進入 REQUEST 狀態。
5. 當 Authenticator 接收到 RADIUS 的回應訊息，則由 REQUEST 狀態進入到 RESPONSE。
6. 當 Authenticator 接收到 RADIUS 認證成功的訊息，則由 RESPONSE 狀態進入 SUCCESS。
7. 最後完成認證成功的設定後，則進入 IDLE 狀態。

4.3.1　Pre-Authentication 步驟之實作

根據 3.4 節所提出的設計方法，我們希望在 MR 與目前存取點訊號變弱後，開始執行跨網路預先認證機制，因此我們將 AUTH_PAE 狀態機器的狀態改成圖 4.10 所示：

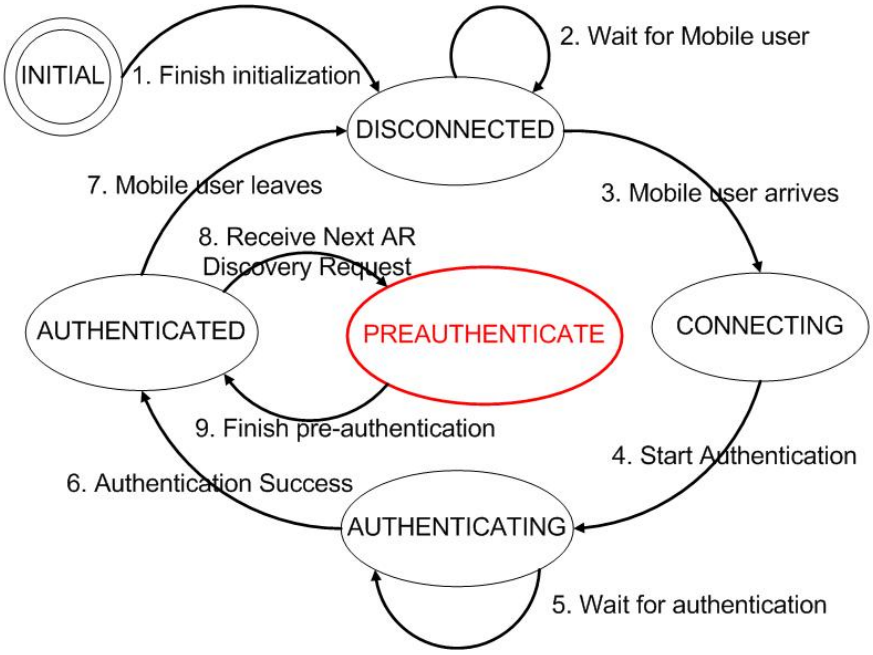

圖 4.10　AUTH_PAE 狀態機器的預先認證機制流程圖

MR 在與目前存取點認證成功之後，目前存取點內的 AUTH_PAE 狀態機器就會停留在 AUTHENTICATED 狀態中，當 MR 偵測到存取點訊號強度減弱時，MR 會送出 Pre-Authentication Request 訊息，而目前的存取點會收到 MR 送來的 Pre-Authentication Request 訊息，當存取點收到該訊息後，AUTH_PAE 狀態就會由 AUTHENTICATED 狀態進入 PREAUTHENTICATE 狀態。

此時，BE_AUTH 狀態機器也會收到認證請求的通知，然後根據圖 4.9 的狀態流程圖，BE_AUTH 狀態機器就會進入 RESPONSE 狀態，接著，目前存取點會將 Pre-Authentication Request 訊息傳送給 RADIUS 伺服器，BE_AUTH 狀態機器就會進入 REQUEST 狀態，接著 RADIUS 伺服器就會與 MR 執行一連串的 EAP 認證機制。所以 BE_AUTH 狀態機器會再 REQUEST 狀態與 RESPONSE 狀態中交互停留，然後收到認證成功的訊息，BE_AUTH 狀態機器就會進入 SUCCESS 狀態，最後，完成認證成功的設定後，BE_AUTH 狀態機器就會進入到 IDLE 狀態中。

當 BE_AUTH 狀態機器執行完後端認證之後，代表 AUTH_PAE 狀態機器的 PREAUTHENTICATE 狀態已經處理完畢，因此 AUTH_PAE 狀態機器就會再由 PREAUTHENTICATE 狀態回到 AUTHENTICATED 狀態，並完成跨網路預先認證機制中的 Pre-Authentication 步驟。

4.3.1.1 Pre-Authentication Request message 之封包格式

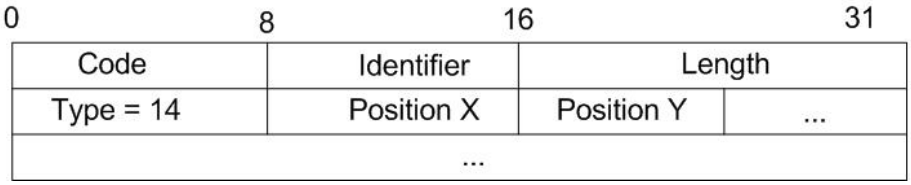

圖 4.11　Pre-Authentication Request 封包格式

Pre-Authentication Request 封包如圖 4.11 所示，我們採用 EAP 的封包格式，並且自訂一個 EAP 的類型（Type = 14）來處理我們跨網路預先認證機制的封包，由於 Pre-Authentication Request 訊息需要告知位置伺服器，MR 目前所在的絕對位置，所以在 Pre-Authentication Request 訊息封包中，會有 X 軸座標以及 Y 軸座標的資訊，以提供給位置伺服器執行尋找存取點的策略。

4.3.1.2 Pre EAP-Success message 之封包格式

根據位置伺服器所選取的候選存取點，RADIUS 伺服器就會根據位置伺服器所給予的 IP 位址，傳送多個 Pre EAP-Success 的訊息封包給所有的候選存取點，這些 Pre EAP-Success 封包格式如圖 4.12 所示：

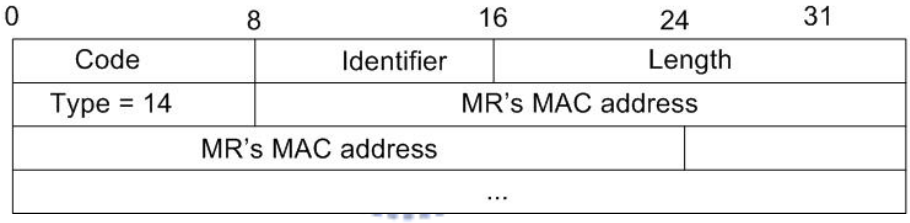

圖 4.12　Pre EAP-Success 封包格式

Pre EAP-Success 訊息封包會將預先認證過的 MR MAC 位址傳送給候選的存取點，而候選存取點會將 MR 的 MAC 位址記錄起來，並且設定一個計時器，如果在計時器已經超過時間，而 MR 還未到達這個存取點，則表示 MR 目前不會由這個候選的存取點來提供網際網路服務，因此存取點就會將這筆預先認證過的 MAC 位址刪除。

4.3.2　Re-association 步驟之實作

由 3.4.2 節中的 Re-association 步驟，我們可以知道當 MR 到達已經預先認證過的存取點時，該存取點的 AUTH_PAE 狀態機器就會由 DISCONNECT 狀態進入 CONNECTING 狀態。接著，該存取點就會開始對 MR 進行認證，此時，AUTH_PAE 狀態機器就會進入 AUTHENTICATING 狀態，存取點就會請求 MR 提供身分認證的資訊，而 MR 會回應自己的身分認證給存取點，由於 MR

所回應的身分就是 MR 的 MAC 位址，因此根據 4.3.1 節中，存取點會記錄已經預先認證過的 MR MAC 位址，存取點就能知道這個 MR 已經預先認證，此時，存取點就會回傳一個 EAP-Success 訊息，AUTH_PAE 狀態機器得知認證成功的訊息，隨即進入 AUTHENTICATED 狀態，並且讓 MR 得以使用存取點所提供的網際網路服務。

4.3.3 Location management 步驟之實作

MR 所發出的 Pre-Authentication Request 與 Next AR Discovery Response 的訊息為 EAP 格式的訊息封包，這些訊息封包都必須傳至 RADIUS 伺服器中進行處理，RADIUS 伺服器收到這些封包之後，會先解析封包中的加密部分，最後才能取得 MR 所傳遞的 EAP 封包。因此我們就將 3.4.3 節中所設計的位置伺服器實作於 RADIUS 伺服器中，如此一來，我們就不需要額外地解析 EAP 格式封包的加密部分，就能直接取得 EAP 的內容部分，並進而實作我們的設計方法。

除了實作方便之外，將位置伺服器實作於 RADIUS 伺服器中還有另一項優點，因為我們必須將多個 EAP 認證成功的訊息，由目前存取點轉送給候選存取點，我們必須要確保所有候選存取點都是 RADIUS 伺服器所信任的存取點，以免有偽裝的存取點藉此取得 MR 的資訊，因此如果我們在 RADIUS 伺服器中記錄這些候選存取點，則代表這些候選存取點都是我們所信任的存取點，所以我們就可放心地讓這些存取點接收 EAP 認證成功的訊息。

第五章： 操作實例

5.1 操作實例

我們以底下的操作實例，來驗證整個系統實作的正確性。

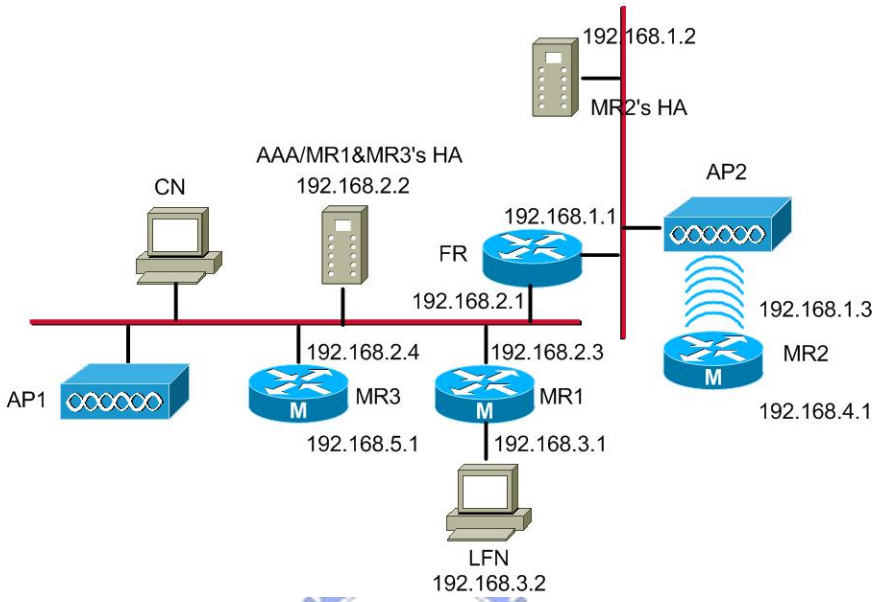

圖 5.1 操作實例原始網路架構圖

圖 5.1 為操作實例的原始網路架構圖，各網路元件的介紹如下：

1. FR：為 192.168.1.0/24 網域與 192.168.2.0/24 網域之間的路由器。
2. MR1：為 192.168.2.0/24 網域與 192.168.3.0/24 網域之間的移動路由器，其家位址為 192.168.2.3，而它的 HA 為圖中 IP 位址為 192.168.2.2 的網路節點。
3. MR2：為 192.168.1.0/24 網域與 192.168.4.0/24 網域之間的移動路由器，其家位址為 192.168.1.3，它的 HA 為圖中 IP 位址為 192.168.1.2 的網路節點。
4. MR3：為 192.168.2.0/24 網域與 192.168.5.0/24 網域之間的移動路由器，其家位址為 192.168.2.4，它的 HA 為圖中 IP 位址為 192.168.2.2 的網路節點。

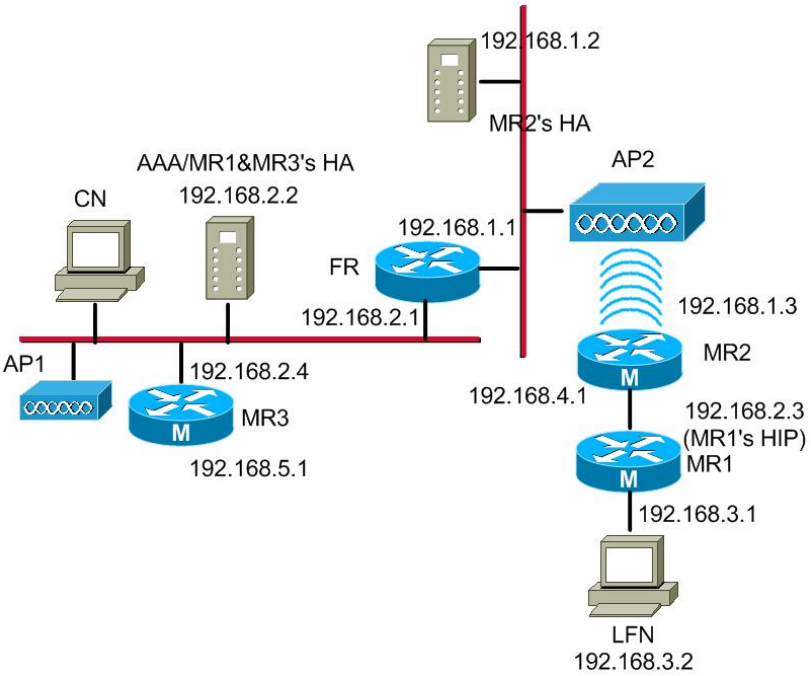

圖 5.2　操作實例－移動步驟 1

圖 5.2 為移動步驟 1 的示意圖，MR1 所形成的 MONET 移動到 MR2 所形成的 MONET，此時，觀察 CN 到 LFN 的連線有無中斷。此步驟可測試整個系統形成階層式移動網路後，網路連線是否還可維持正常。

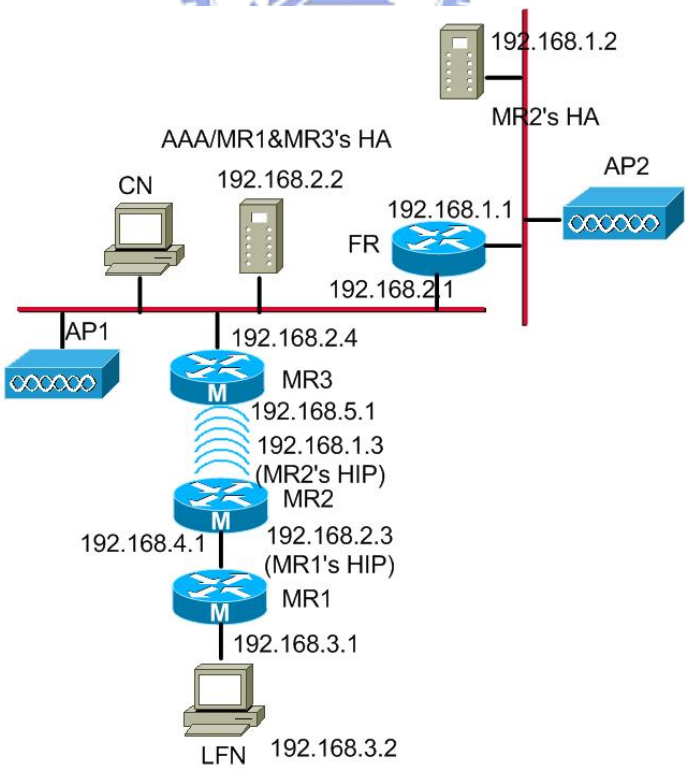

圖 5.3　操作實例－移動步驟 2

圖 5.3 為移動步驟 2 的示意圖，MR2 所形成的 MONET 移動到 MR3 所形成的 MONET。於 MR2 移動到 MR3 之前，觀察跨網路預先認證機制是否有選取 MR3 為候選存取點。於 MR2 連結到 MR3 時，觀察 MR2 是否可以不需要經過 AAA 伺服器就能直接使用 MR3 所提供的網際網路服務。此步驟可測試跨網路預先認證機制的實作是否正確。

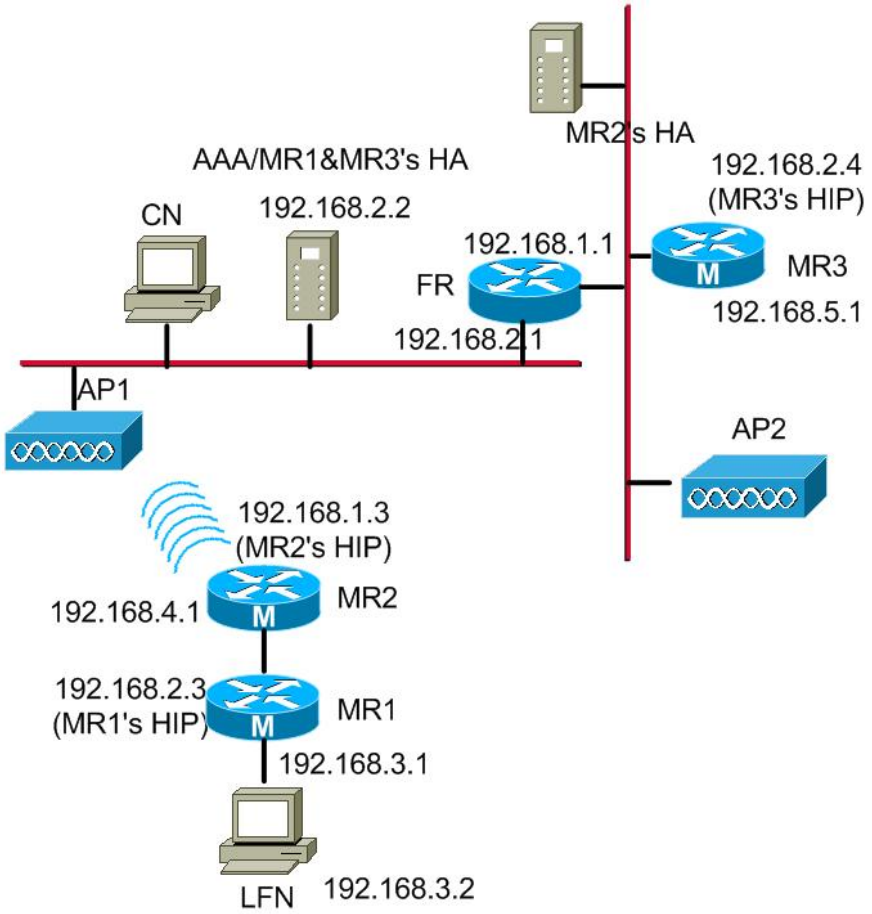

圖 5.4　操作實例－移動步驟 3

圖 5.4 為移動步驟 3 的示意圖，MR2 與 MR3 所形成的階層式移動網路中，MR3 為整個階層式移動網路的父節點，MR3 與整個階層式移動網路反向移動。此時，觀察 CN 到 LFN 的連線有無中斷。此步驟可測試位於階層式移動網路上層的存取點移動後，網路連線是否還可維持正常，並且可以在 MR3 移出階層式移動網路之前，觀察跨網路預先認證機制是否有選取 AP1 為候選存取點。在 MR2 連結到 AP1 時，觀察 MR2 是否可以不需要經過 AAA 伺服器就能直接使用 AP1 所提供的網際網路服務。此步驟還可測試跨網路預先認證機制的實作是否正確。

第六章： 結論與未來工作

6.1 結論

在這篇論文中，我們參考 Mobile IPv4 通訊協定中關於 MONET 的設計方法，並根據這些設計方法的優缺點，進而實作一個結合這些設計方法優點的階層式移動網路，這個階層式移動網路環境可以讓 MN 與 LFN 隨著 MONET 移動，還能夠保持網際網路連線不斷線，並且考量到 MONET 實際的應用環境，而做出適當的設計。

另外為了讓網路應用程式不會受到 MONET 經常換手的影響，我們提出了一套跨網路預先認證機制，期望可以在這個階層式移動網路的環境中，使用這套跨網路預先認證機制進行快速換手，以減少 MONET 經常換手對網路應用程式所造成的效能影響。在這套跨網路預先認證機制中，我們採用三個步驟的設計來達到跨網路預先認證的效果，分別為：Pre-Authentication 步驟、Re-Association 步驟、以及 Location Management 步驟。在 Location Management 步驟中，我們提出了三種類型的位置伺服器設計，分別為：位置伺服器記錄所有存取點的位置資訊、位置伺服器僅記錄固定存取點的位置資訊、以及完全由 MR 偵測存取點等。然後，先比較這三種類型的位置伺服器設計之間的差異性，再以不同的實例來說明使用這三種類型的位置伺服器設計的優缺點。

6.2 未來工作

由於階層式移動網路可以攜帶多個網域一同移動，但是就目前 IPv4 網路環境來說，IP 位址已經快要達到飽和的狀態，所以未來我們考慮將階層式移動網路運用到 IPv6〔11〕的網路環境中，以期望能夠解決 IP 位址不足夠的問題。因此我們希望可以使用 Mobile IPv6〔12〕通訊協定取代原先 Mobile IPv4 通訊協定的設計來建構階層式移動網路。

另外由於目前我們所提出的跨網路預先認證機制是採用單一位置伺服器來控管整個網路拓撲中的所有存取點，採用集中控管的位置伺服器不僅會讓位置伺服器的負擔變重，在搜尋存取點與更新位置表所花費的時間也會跟著變多。因此我們考慮將網路拓撲分成多個區域，然後使用多個分散式的位置伺服器來控管各個區域，這樣就能減輕位置伺服器的負擔，搜尋存取點與更新位置表所花費的時間也會跟著變少。不過使用分散式位置伺服器來控管的話，當 MONET 移動到不同位置伺服器所控管的區域時，該如何通知不同的位置伺服器，是否也需要使用階層式位置伺服器的觀念，這些都是我們未來可以思考的方向。

目前我們尋找存取點的策略是採用移動方向、選取半徑、以及選取角度所形成的扇形面積來決定下個可能會到達的存取點，由於我們採用位置伺服器來控管存取點，因此我們可以順便記錄這些存取點的環境記錄，例如：存取點所提供的 QoS 等。藉由這些存取點的環境記錄來增加我們預測候選存取點的準確率，以增加階層式移動網路能夠快速換手的機率。

參考文獻

[1] C. Perkins, Ed., “IP Mobility Support for IPv4” IETF RFC-3344, August 2002.

[2] Thierry Ernst, WIDE and INRIA., “Network Mobility Support Terminology” IETF Internet-Draft, May 2003.

[3] “IEEE Standards for Local and Metropolitan Area Networks－Port Based Network Access Control", IEEE Std 802.1X-2001.

[4] L. Blunk, J. Vollbrecht., “PPP Extensible Authentication Protocol (EAP)” IETF RFC-2284, March 1998.

[5] Sangheon Pack , Yanghee Choi., “Pre-Authenticated Fast Handoff in a Public Wireless LAN Based on IEEE 802.1x Model” Proceedings of the IFIP TC6/WG6.8 Working Conference on Personal Wireless Communications, p.175-182, October 23-25, 2002.

[6] C. Rigney, S. Willens, A. Rubens, W. Simpson., “Remote Authentication Dial In User Service (RADIUS)” IETF RFC-2865, June 2000.

[7] B. Aboba, P. Calhoun., “RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)” IETF RFC-3579, September 2003.

[8] H. Jonatban., “RADIUS” O’REILLY, October 2002.

[9] P. Bruce, F. Bob., “802.11 Security” O’REILLY, December 2002.

[10] Matthew S. Gast, “802.11 無線網路技術通論”, 黃裕彰, O’REILLY, May 2003.

[11] R. Hinden, S. Deering., “Internet Protocol Version 6 (IPv6) Addressing Architecture” IETF RFC-3513, April 2003.

[12] D. Johnson, C. Perkins, J. Arkko., ” Mobility Support in IPv6” IETF Internet-Draft, June 30, 2003.

[13] Pekka., “Mobile Network Prefix Delegation extension for Mobile IPv6” IETF Internet-Draft, March 2003.

[14] Red Hat Linux, http://www.redhat.com/

[15] FreeRADIUS, http://www.freeradius.org/

[16] Host AP driver, http://hostap.epitest.fi/

[17] Open Source Implementation of IEEE 802.1x, http://open1x.org/

[18] HUT Dynamics Mobile IP, http://dynamics.sourceforge.net/