國立交通大學

電機資訊學院 資訊學程

碩士論文

無線網路 802.11F 通道模式的無接縫漫遊

Seamless Roaming in 802.11F WLAN by Tunneling

研 究 生：楊志民

指導教授：曾煜棋　教授

中 華 民 國 九 十 三 年 十 月

無線網路 802.11F 通道模式的無接縫漫遊
Seamless Roaming in 802.11F WLAN by Tunneling

研 究 生：楊志民　　Student：Chih-Min Yang

指導教授：曾煜棋　　Advisor：Yu-Chee Tseng

國 立 交 通 大 學

電機資訊學院 資訊學程

碩 士 論 文

A Thesis

Submitted to Degree Program of Electrical Engineering and Computer Science

College of Electrical Engineering and Computer Science

National Chiao Tung University

in Partial Fulfillment of the Requirements

for the Degree of

Master of Science

in

Computer Science

September 2004

Hsinchu, Taiwan, Republic of China

中華民國九十三年十月

博碩士論文授權書

本授權書所授權之論文為本人在 國立交通 大學(學院) 電機資訊學院 系所
資訊 組 93 學年度第 1 學期取得 碩 士學位之論文。

論文名稱： 無線網路 802.11F 通道模式的無接縫漫遊

指導教授： 曾煜棋教授

1. ■同意 □不同意

本人具有著作財產權之上列論文全文(含摘要)資料，授予行政院國家科學委員會科學技術資料中心(或改制後之機構)，得不限地域、時間與次數以微縮、光碟或數位化等各種方式重製後散布發行或上載網路。

本論文為本人向經濟部智慧財產局申請專利(未申請者本條款請不予理會)的附件之一，申請文號為:_____，註明文號者請將全文資料延後半年再公開。

2. ■同意 □不同意

本人具有著作財產權之上列論文全文(含摘要)資料，授予教育部指定送繳之圖書館及國立交通大學圖書館，基於推動讀者間「資源共享、互惠合作」之理念，與回饋社會及學術研究之目的，教育部指定送繳之圖書館及國立交通大學圖書館得以紙本收錄、重製與利用；於著作權法合理使用範圍內，不限地域與時間，讀者得進行閱覽或列印。

本論文為本人向經濟部智慧財產局申請專利(未申請者本條款請不予理會)的附件之一，申請文號為:_____，註明文號者請將全文資料延後半年再公開。

3. ■同意 □不同意

本人具有著作財產權之上列論文全文(含摘要)，授予國立交通大學與台灣聯合大學系統圖書館，基於推動讀者間「資源共享、互惠合作」之理念，與回饋社會及學術研究之目的，國立交通大學圖書館及台灣聯合大學系統圖書館得不限地域、時間與次數，以微縮、光碟或其他各種數位化方式將上列論文重製，並得將數位化之上列論文及論文電子檔以上載網路方式，於著作權法合理使用範圍內，讀者得進行線上檢索、閱覽、下載或列印。

論文全文上載網路公開之範圍及時間 –

本校及台灣聯合大學系統區域網路： 94 年 1 月 1 日公開

校外網際網路： 94 年 1 月 1 日公開

上述授權內容均無須訂立讓與及授權契約書。依本授權之發行權為非專屬性發行權利。依本授權所為之收錄、重製、發行及學術研發利用均為無償。上述同意與不同意之欄位若未鈎選，本人同意視同授權。

研究生簽名： 楊志民 學號： 9067597

（親筆正楷） （務必填寫）

日期： 93 年 10 月 20 日

---

1. 本授權書請以黑筆撰寫並影印裝訂於書名頁之次頁。

國家圖書館博碩士論文電子檔案上網授權書

本授權書所授權之論文為本人在 國立交通 大學(學院) 電機資訊學院 系所
資訊 組 93 學年度第 1 學期取得 碩 士學位之論文。
論文名稱： 無線網路 802.11F 通道模式的無接縫漫遊

指導教授： 曾煜棋教授

■同意　　□不同意

本人具有著作財產權之上列論文全文(含摘要)，以非專屬、無償授權國家圖書館，不限地域、時間與次數，以微縮、光碟或其他各種數位化方式將上列論文重製，並得將數位化之上列論文及論文電子檔以上載網路方式，提供讀者基於個人非營利性質之線上檢索、閱覽、下載或列印。

上述授權內容均無須訂立讓與及授權契約書。依本授權之發行權為非專屬性發行權利。依本授權所為之收錄、重製、發行及學術研發利用均為無償。上述同意與不同意之欄位若未鉤選，本人同意視同授權。

研究生簽名： 楊志民　　學號： 9067597
（親筆正楷）　　（務必填寫）

日期：民國 93 年 10 月 20 日

---

1. 本授權書請以黑筆撰寫，並列印二份，其中一份影印裝訂於附錄三之一(博碩士論文授權書)之次頁；另一份於辦理離校時繳交給系所助理，由圖書館彙總寄交國家圖書館。

無線網路 802.11F 通道模式的無接縫漫遊

學生：楊志民　　指導教授：曾煜棋 教授

國立交通大學電機資訊學院 資訊學程（研究所）碩士班

摘　　要

近年來區域網路的使用趨勢，已經從傳統的有線乙太網路演變到無線網路，由於無線區域網路設備成本的降低及可快速建置的優點，市場上可以看到愈來愈多支援無線區域網路標準的行動裝置，加上許多廠商積極投入 WLAN，使得 WLAN 建置成本愈來愈低。隨著無線網路的日趨普及與大量應用，無線傳輸的安全性，儼然成為個人與企業用戶關注的焦點。由於無線網路技術被大量應用在生活與辦公室環境裡，對於個人隱私與企業機密資料的保密性上，就有其需要探究與加強的部分。

然而無線區域網路（WLAN ）的標準 802.11 提出時只是簡單的區域網路架構，在被廠商推行應用之前並未考量且制定好完整的移動性 (mobility) 以及安全性(security)的機制，因此在移動性與安全性兩者必須兼顧的需求下，漫遊時如何避免資料傳輸的中斷是一個值得重視的課題。

IEEE 在 2003 年 7 月公佈了 WLAN 的漫遊標準 802.11F，並且在 2004 年公佈新一代 WLAN 安全標準 802.11i，來確保無線網路內發送的資訊安全加密，不會中途遭第三者攔截甚至解密。為長期以來一直為安全問題所詬病的無線區域網路(WLANs)提出一個解決方案。

在本論文中，我們針對 802.11F 提出一個改善方案，以一個通道(Tunneling) 的技術使得當 802.11F 與 802.11i 同時存在於 WLAN 的環境時，在 Roaming 過程中資料傳輸不會中斷的 Seamless Roaming 的方法。

目　　錄

一、 導論

目前使用手持式終端設備與筆記型電腦之無線網路使用者與日俱增，而無線網路不受建築與線路侷限的特性，隱含的安全威脅遠高於實體網路。因此網路安全的顧慮更受無線網路使用者的重視，在移動性與安全性兩者必須兼顧的需求下，802.11F 與 802.11i 勢必將同時存在於 WLAN 的環境中，因此如何在漫遊過程中達到 Seamless 的目標是一個值得重視的課題。

就移動性的需求而言，IEEE 在 2003 年 7 月公佈了 WLAN 的漫遊 (Roaming) 標準 802.11F，提供了所有的 AP 廠商一個共同遵循的漫遊標準；就 WLAN 的安全性而言，早期 IEEE 所制定的標準 802.11 是利用固定的 WEP Key 作為加密機制，這樣的加密方式主要是透過 RC4 配合 64 bits 與 128 bits Key 兩種不同長度的 WEP Key 作為加密保護，原本無線網路在 WEP Key 所採用的 IV 值都是以 24 bits 的長度，而且只有 IV 值是變動的，之後 40 bits 或是 104 bits 的 Key 都是固定不變的。由於 IV 的長度過小，對於要有心人士而言，只要可以累積相同的 IV 值封包，就可以進行對 IV 值之後 40 bits 或是 104 bits 加密 Key 的破解。

有鑑於 WEP 機制不夠安全，IEEE 於 2004 年提出新一代的無線網路安全標準 802.11i，針對無線網路原本所具備的弱點加以補強，以建構出一個符合現今需求，具備更進一步安全性的無線網路環境。

在 802.11i 中，Access Point 與每個各別的使用者端通訊使用的是 Session Key，由於每個使用者端的 Session Key 都不同，所以可以確保每個不同使用者端一定程度的安全機制，而對於要廣播給在這區域內所有使用者的資訊，就可以透過 Group Key 傳遞。並且在每一次的重新認證過程皆會產生新的 Session Key，這把 Session Key 是以動態的方式更新以達到更安全的目的，不過這樣的安全機制使得原本漫遊的機制受到了影響，當 Station 漫遊到 New AP 時，必須與 New AP 認證並且建立新的 Session Key，在此過程中，資料傳輸將會面臨短暫中斷的問題。

在本論文中，我們針對 802.11F 提出一個改善方案，以一個通道(Tunneling) 的概念將漫遊時，802.1x 認證與建立 Session Key 所造成的時間延遲以 Tunnel 加以克服，這篇論文並不是提出一個快速的漫遊機制，而是提出一個方法來避免在漫遊時因 802.1x 認證與重新建立 Session Key 所造成的資料傳輸中斷，以達到 Seamless Roaming 的目的。

當 Station 從 Old AP Roaming 到 New AP 期間，Old AP 與 New AP 間會建立一個 IAPP Tunnel，當資料從 DS 欲傳送給 Station 時，data 先由 Old AP 接收，並以 Old session key 加密，然後藉由 IAPP Tunnel 傳到 New AP，再由 New AP 轉送給 Station， Station 便可以用 Old session key 解密，此過程中加解密的端點為 Station 與 Old AP。反之，當 Station 欲傳送資料到 DS 時，Station 以 old session key

加密，透過 New AP 傳到 Old AP，由 Old AP 解密後再傳至 DS，直到 Station 與 New AP 的漫遊程序完成。

二、 背景知識

2-1 Inter-Access Point Protocol (IAPP) 簡介

IAPP (Inter-Access Point Protocol) 設計了一個機制使得在一個 Extended Service Set (ESS) 中，station 能在不同的AP間作漫遊，其定義了當station 從一AP 漫遊到另一AP 時，前後AP 之間的一些訊息交換，這些訊息包含該 station 在前後AP的 security context [1]。

如圖 2-1-1 所示，當 STA 從 AP1 漫遊到 AP2 時，STA 發送 Reassociation Request frame [2] 給 AP2 要求 Association，IAPP 的程序便由此展開。

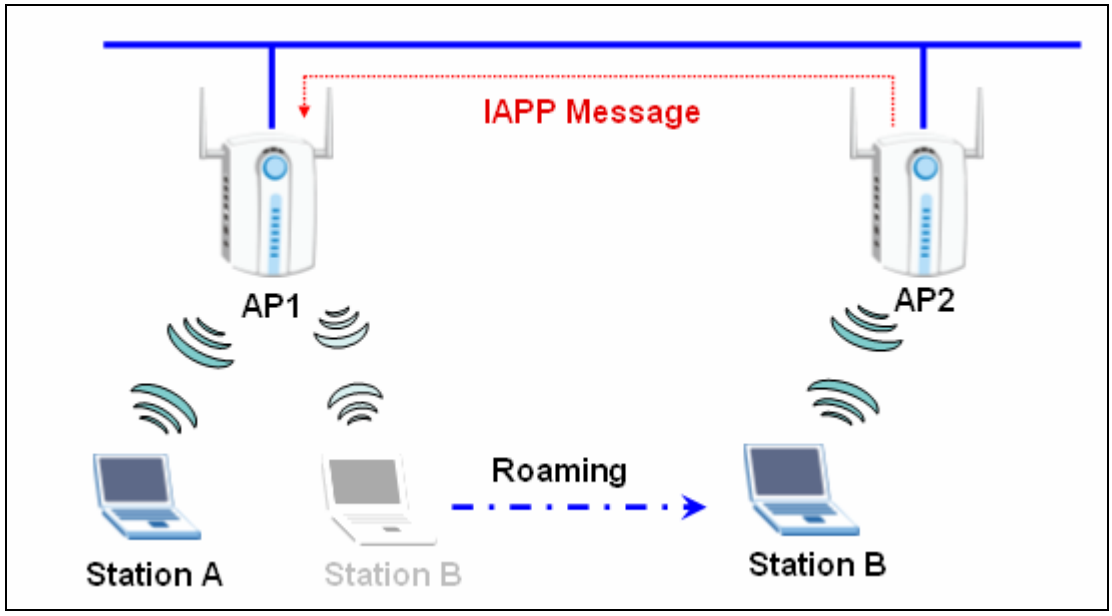
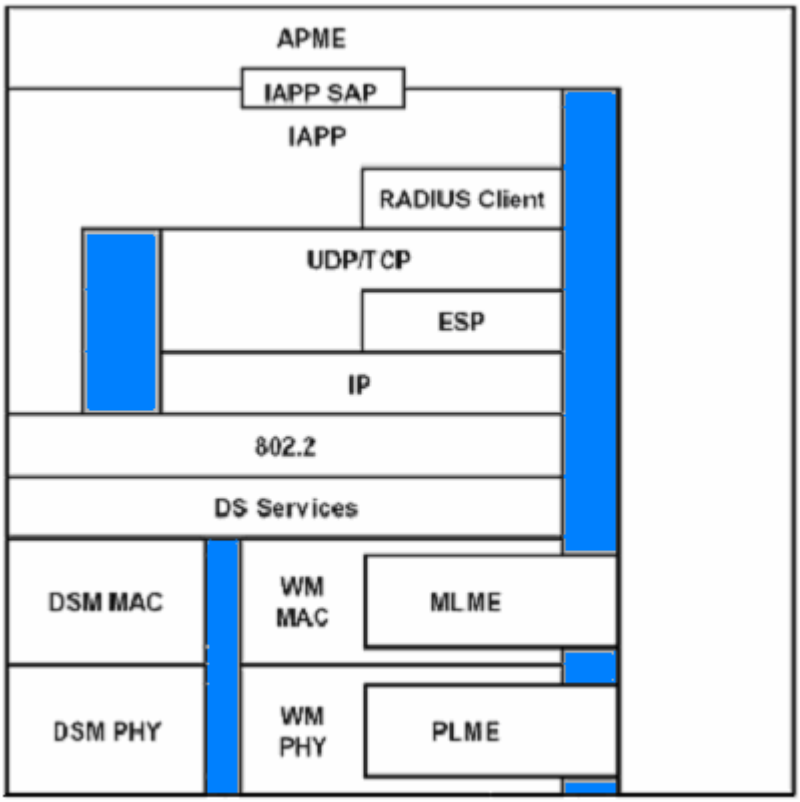


圖2-1-1

在 802.11F 中定義了 service access point (SAP)， service primitives，一個 protocol 和一些 function，使得在一個共同DS 的 APs 可以藉由 TCP/IP 來交換 IAPP 封包，AP 也可以透過Remote Authentication Dial- in User Service (RADIUS) 取得關於其他AP 的資訊。

圖2-1-2 描繪出一個AP 中 IAPP 的架構，AP management entity" (APME) 是AP的一個主要的 function，APME 透過 IAPP service primitives 要求 IAPP service 做一些事像與其他 AP 或 RADIUS server 交換資料。圖中深色部分隔開了部分的區塊，表示這些區塊 (Functions) 無法直接溝通。



AP Architecture with IAPP

圖2-1-2

Note:

APME: AP Management Entity
MLME: MAC Layer Management Entity
PLME: PHY Layer Management Entity
DSM: Distribution System Medium
WM: Wireless Medium

IAPP Service definition

IAPP SAP 允許management entity (APMP) 去呼叫 IAPP services，並且接受從其他AP傳來的請求。在SAP中定義了四種 service primitives : requests，confirms，indications，和responses。Service requests 和 responses 由 較高層的 entity (APME) 傳送到 the IAPP entity，而IAPP則傳送 Service confirms和indications 到 APME。圖2-1-3 顯示這些service primitives 的關係圖。

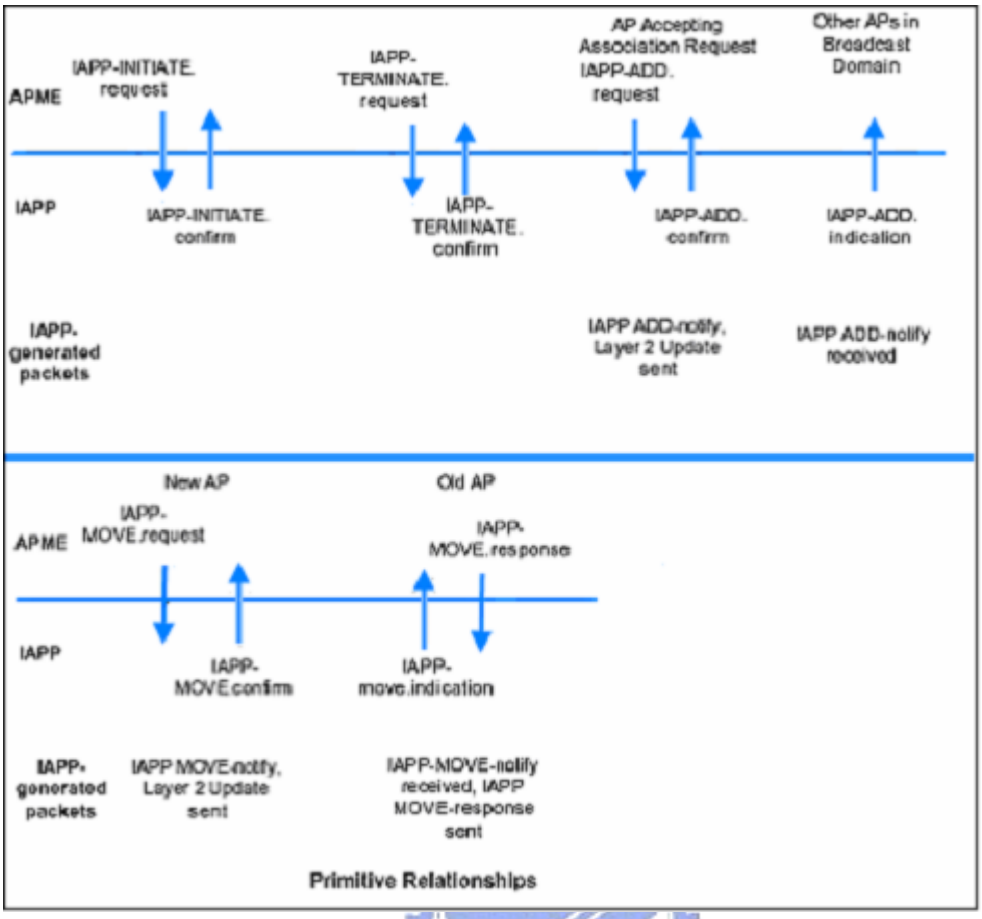


圖 2-1-3

IAPP Protocol Overview

802.11F 目前定義了三種 protocol sequences : IAPP-ADD，IAPP-MOVE以及 IAPP-CACHE。

1. IAPP-ADD

當 SAT associate 到一個 AP，APME 會以 IAPP-ADD.request 要求 IAPP 送一個 IAPP ADD-notify packet 到一個 multicast address (224.0.1.178)。在 IAPP ADD-notify packet 中包含 STA 的 MAC address 及此 STA Association 的 Sequence number ，當其他 AP 收到此 packet 後，會以 APME 檢查此 STA 是否存在於 Association Table 中，若存在則將其從 Association Table 刪除。

IAPP ADD-notify packet 的目的用來讓其他 AP 更新 Association table 及 Forwarding table。

2. IAPP-MOVE

當SAT Reassociate 到一個 AP， APME 會以IAPP-MOVE.request 要求 IAPP 送一個 IAPP MOVE -notify packet 到此 STA 原先 associate 的AP，原AP 會回覆 IAPP MOVE-Response，IAPP MOVE-Response 可以包含STA 從原AP 連上新AP 時所需要的Context block。

交換 IAPP MOVE-notify and MOVE-response packets 的目的在於允許新舊 AP 交換 Station 的 Context Information，這可以加速 Station Reauthentication 的認證程序。

IAPP MOVE-Notify 和 MOVE-Response 的傳送是藉由新舊 AP 間的 TCP session，由於RADIUS server 上保持一份 BSSID 與 IP address 的對應表，新AP 必須能向 RADIUS server 查詢到舊AP的 IP addresss。

基於安全的考量，如果 IAPP MOVE-response packet 被要求加密，RADIUS 會提供足夠的訊息給新舊 AP，使得新舊 AP 之間 IAPP MOVE packet 的 Security Blocks 交換是建立在加密的連結之上。

3. IAPP-CACHE-NOTIFY

Proactive Caching 是目的是減少在漫遊過程中，兩個 AP 間及 AP 與 RADIUS server 由於交換 IAPP message 所造成的 delay。

Proactive Caching 提供一個 Fast Roaming 的方法，預先在 STA 可能會漫遊到的 AP 上，將漫遊時 STA 與 New AP 所需要的交換的 message 預先存放在 neighbor AP 上。要達到此目的，AP 必須先動態地學習到鄰近有哪些 AP，並且維護一個 Neighboring Graph，當 STA 從舊 AP 漫遊到新 AP 之前，舊 AP 已經透過 IAPP-CACHE-NOTIFY 傳送 STA 的 Security Context 到所有的 Neighboring AP 上。

一旦 STA Reassociated 或 Associated 到一個AP，此AP的 IAPP Entity 會從 APME收到 IAPP-CACHE-NOTIFY.request 後，IAPP entity 應該將收到的 Context 藉由CACHE-notiry packet 傳送到 Neighboring AP Graph 中的其他AP，使neighbor graph 中的所有APs將CACHE-notify的context放入cache中。而 Neighboring AP 收到 CACHE-notify packet 後，其 IAPP entity 會傳遞一個 IAPP-CACHE-NOTIFY. indication 到上層的 APME，使得APME 更新STA context cache 並回送CACHE-

response packet 給舊AP。當舊AP 的 IAPP entity 收到CACHE-response packet，其 IAPP entity 會傳遞 IAPP-CACHE-NOTIFY.confirm 給上層的 APME 。 如果有 Neighboring graph 中的 AP 未在一定時間內回傳 CACHE-response packets，IAPP entity 會將此AP 從neighboring graph 中刪除，如果所有的neighboring AP 都未能在時間內回傳 CACHE-response packets， IAPP entity 會傳遞一 IAPP-CACHE-NOTIFY.confirm {Status=TIMEOUT} 給上層的 APME。

2-2 問題描述

802.11i 定義了以 IEEE 802.1x 為基礎的認證程序與 Key的交換機制，Station 必須先以 Open System [2] 的認證 Associate 到 AP ，接著 Station 與 AP 進行協商以瞭解彼此所能支援的加密機制與功能，所以一個支援802.11i標準的 Access Point在發出Beacon Frame 與回應Probe Response 時，就必須要在所傳回的 Frame 中填入 Information Element，也就是說透過 Information Element所定義的OUI 欄位，使用者端可以知道目前所屬網域 Access Point 所具備的加密機制，再根據使用者端本身的設定選擇對應的方式加入Access Point。而對於Access Point端而言，每一個使用者端的網卡要連上該網域時亦會發出 Association Request ，Access Point 端就可以透過 Association Request Frame 中的 Information Element 中所具備的 OUI 欄位，知道目前連上 Access Point 的使用者端所具備的加密機制與能力，再根據本身是否支援來決定是否允許使用者連線上來 [3]。

接著 AP 會對 Station 作 802.1x 認證 ，在完成 802.1x 認證後， Station 與 Authentication Server (Radius Server) [4] 會利用協商中交換的訊息建立相同的 Pairwise Master Key (PMK) [5]。 Authentication Server (RADIUS Server) 會將此 PMK 傳送給 AP。 對於 AP而言，與每個各別的使用者端通訊使用的是Session Key，由於每個使用者端的Session Key 都不同，所以可以確保每個不同使用者端一定程度的安全機制，而對於要廣播給在這區域內所有使用者的資訊，就可以透過 Group Key 傳遞。當AP 收到 Authentication Server (Radius Server) 傳送來的 PMK，AP 會利用此PMK 與 Station 進行 4-way Handshake 以產生Pairwise Transient Key (PTK)以及 Group Key 2-way Handshake以產生 Group Transient Key (GTK)。 當PTK 及 GTK 順利產生後， Station 與 AP 之間的資料傳輸即可利用此兩把 Key 做為 Unicast /Multicast 之加解密之用。

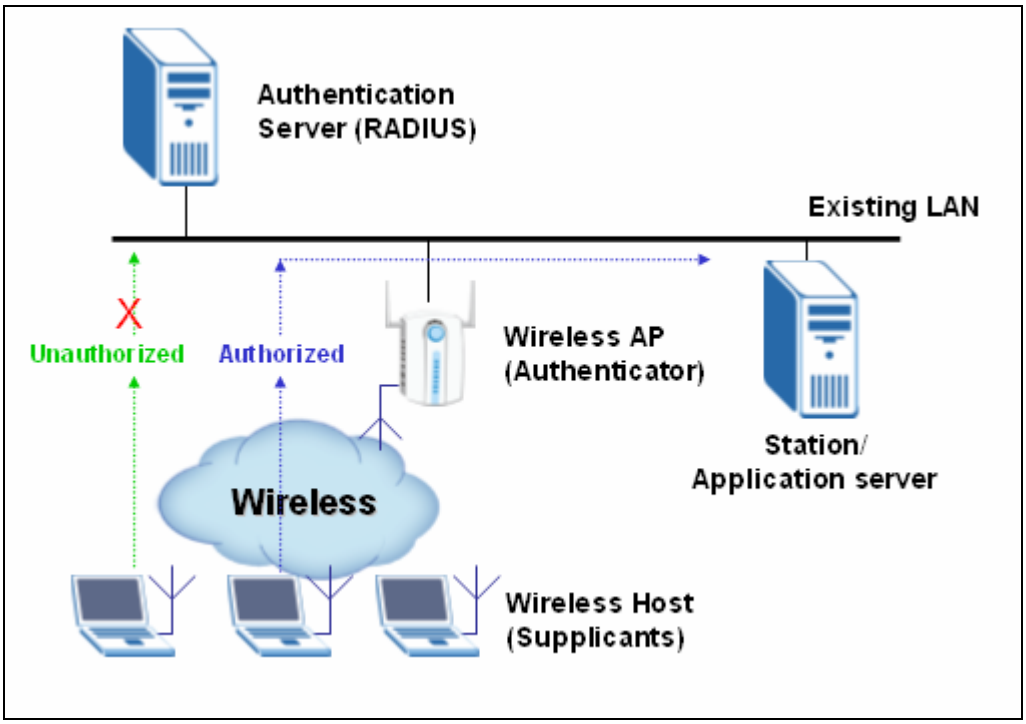


圖 2-2-1

在每一次的 802.11x [6] 認證程序中，皆會以此機制產生新的 PTK 以及 GTK，這樣動態的方式更新 Key [7] 解決了 Static WEP Key 不安全的問題，不過由於這樣的機制使得原本漫遊的機制受到了影響，當 Station 漫遊到 New AP 時，必須先與 New AP 進行認證並且建立新的 PTK 及 GTK，在此過程中，資料傳輸將會面臨短暫中斷的問題。

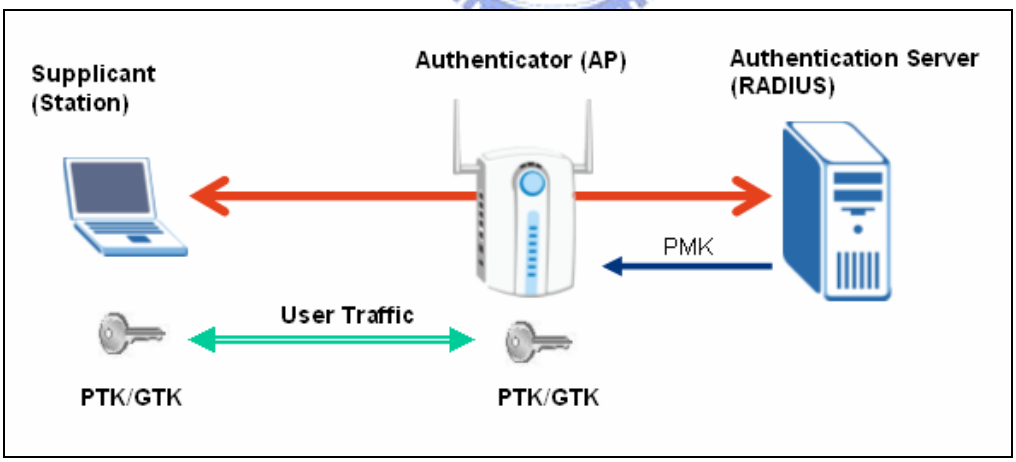


圖 2-2-2

目前 802.11F 雖可以利用 Proactive Caching 及 Pre-Authentication [8] 的機制達到 Fast Roaming，預先在STA可能會漫遊到的AP上。 將漫遊時STA 與 New AP 所需要的交換的用來加密的 Pairwise Transient Key (PTK) 及 Group Transient Key (GTK)，預先以 IAPP–CACHE 傳送到 Neighbor AP [9] 上，但是利用 Proactive Caching的機制有幾個缺點:

1. PTK 與 GTK 須在經常在網路上被交換，較不安全
2. 由於 Key 當 AP 與 Station 的數量比較多的時候，許多額外的 Traffic 產生。例如在一個 ESS 中有 N 個 AP，每個 AP 上有 M 個 Station associate，第一次所有 Station associate 上 AP 需要 M*N 個 PMK 及 GTK 的交換，每當一個 Station 的 PMK 更換時，又另外需要 N 個 PMK 的交換，即使 Station 不會有 Roaming 的行為，PMK 仍然被傳送所有到 neighbor AP 中。
3. 每個 AP 必須維護 Proactive Cache。
4. 所有 AP 需要維護 Neighborhood graph 。
5. Station 必須以 Pre-Authentication 預先向所有可能會漫遊的 AP 完成認證程序。

下一章節將提供一個較佳的方法—在 802.11F 增加一個 Tunnel 機制以達到 Seamless Roaming 的目的。

三、 Seamless Roaming by Tunneling

在 802.11i 的環境下，為了使漫遊期間資料傳輸不致中斷，必須在 Station 從 Old AP 移動至 New AP 後，而 New PTK 與 GTK 尚未產生前，Station 與 New AP 間資料的傳輸能繼續使用 Old PTK 與 GTK，直到 Station 與 New AP 之間的 New PTK、GTK 建立完成。

本論文提出一個新的概念，當 Station 從 Old AP 漫遊到 New AP 期間，在 Old AP 與 New AP 間建立一個 IAPP Tunnel，當資料從 DS 欲傳送給 Station 時，由於 Station 在 New AP 上的 802.1x port 尚未開啟，因此 data 先由 Old AP 接收，並以 Old PTK (或 GTK) 加密，然後藉由 IAPP Tunnel 傳到 New AP，再由 New AP 轉送給 Station。 Station 便可以用 Old PTK 解密，此過程中加解密的端點為 Station 與 Old AP。 反之，當 Station 欲傳送資料到 DS 時，Station 以 old PTK 加密，透過 New AP 傳到 Old AP，由 Old AP 解密後再傳至 DS，直到 Station Authentication 完成且與 New AP 間的 PTK 與 GTK 建立，802.1x port 開啟後，New AP 將通知 Old AP 將 IAPP Tunnel 中斷，從此所有與 Station 的資料傳輸改由 New AP 負責接收。

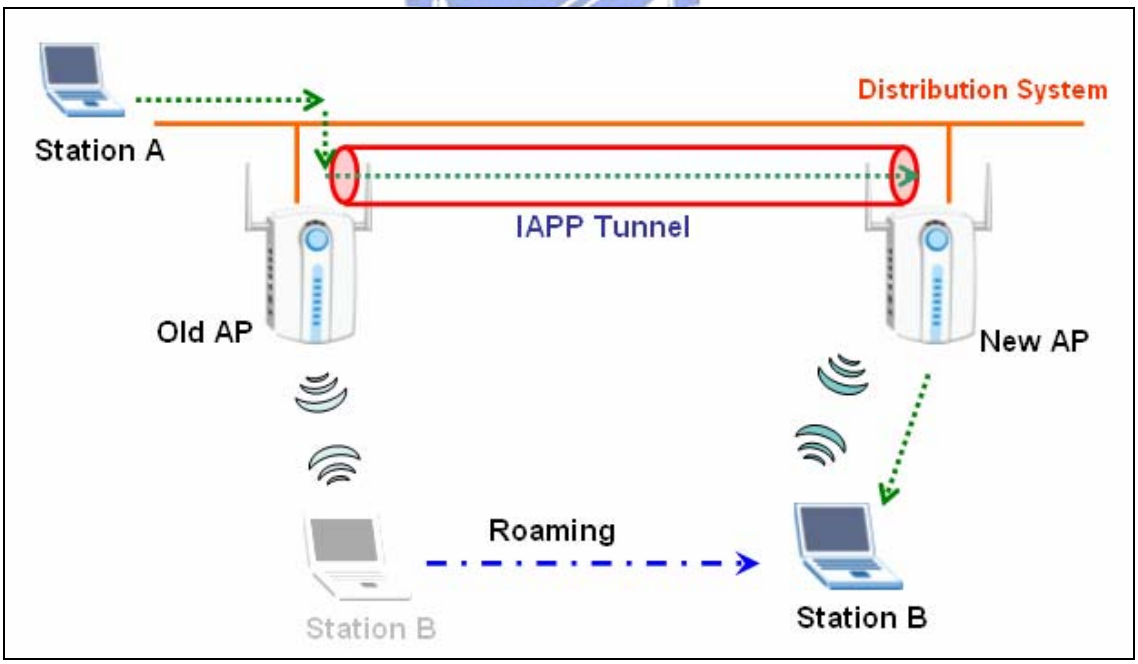


圖 3-1

IAPP-TUNNEL 機制必須在 IAPP 原有三個 protocol sequences : IAPP-ADD，IAPP-MOVE 以及 IAPP-CACHE 以外再加上 IAPP-TUNNEL 作為新舊 AP 間 Tunnel 之建立，中止與 data 傳送。

3.1 New IAPP Services for 802.11F

3.1.1 IAPP-TUNNEL-NOTIFY.request

當AP收到802.11i/WPA enabled 的Station 發出 Reassociation Request frame，APME 會以 IAPP-TUNNEL-NOTIFY.request primitive 要求 IAPP 傳送 IAPP TUNNEL-notify packet到該Station原先Associated 的 AP，讓原 AP 知道 Station 的 reassociation 並且及要求與原 AP 建立 IAPP Tunnel。

IAPP-TUNNEL-NOTIFY.request primitive 有下列的 semantics

IAPP-TUNNEL-NOTIFY.request {
MAC Address，
Sequence Number，
Old AP，
Timeout
}

MAC Address 是 reassociated 到此AP 的 station 的 MAC Address。

Sequence Number是來自於station 發出 Reassociation Request frame 中的Sequence Number field。

Old AP是Reassociated到此AP的station 上一個Associated AP的WM MAC address，APME 可以從Station 發出 Reassociation Request frame 中的 Current AP Address field 取得。

Timeout 是以秒為單位，從 IAPP TUNNEL-notify packet 送出去直到 IAPP TUNNEL-response packet 收到所預期的時間，若超過這個時間仍未收到 IAPP TUNNEL-response packet 則視為 Timeout。

當 IAPP 收到這個 service primitive 後，IAPP entity 要藉由原 AP 的 MAC address 取得其 DSM 的 IP address，並傳送 IAPP TUNNEL-NOTIFY packet 給原 AP 告知 Station 的 Reassociation 並要求建立 IAPP Tunnel。

3.1.2 IAPP-TUNNEL-NOTIFY.confirm

當 New AP 收到從Old AP 傳來的 IAPP TUNNEL-response packet 或者尚未收到 IAPP TUNNEL-response packet，但已到達 IAPP-TUNNEL.request primitive 上指定的Timeout 時間，IAPP會以此 service primitive 用來回覆 APME 其 IAPP-TUNNEL-NOTIFY.request 之處理結果。

IAPP-TUNNEL-NOTIFY.confirm primitive 有下列的 semantics

IAPP-TUNNEL-NOTIFY.confirm {
MAC Address，
Sequence Number，
Old AP，
New BSSID，
Status
}

MAC Address 是依據 IAPP-TUNNEL-NOTIFY.request 中指示 reassociated 到此 AP 的 station 的 MAC Address。

Sequence Number是來自於station 發出 Reassociation Request frame 中的Sequence Number field。

Old AP 是 reassociated 到此AP 的 station 上一個 associated AP 的 WM MAC address。

New BSSID 是 station reassociated 的 New AP 的 WM MAC address。

Status 用來指示 IAPP-TUNNEL.request. 的結果，結果可能為 SUCCESSFUL，FAIL，DENIED 或 TIMEOUT。SUCCESSFUL 表示 IAPP Tunnel 已成功地建立，FAIL 表示 RADIUS 不接受查詢 Old AP 的 IP Address 的要求。
DENIED 表示 IAPP-TUNNEL.requsest 所指定的Old AP無法被驗證或者因其他理由不被允許建立 IAPP Tunnel， TIMEOUT 表示未能在 timeout 時間內收到 IAPP TUNNEL-response packet。

當 APME 收到的 status 為 SUCCESSFUL，IAPP 可以開始將station 傳給 DS 的 data 透過 IAPP Tunnel 傳給 Old AP，以及接受從 Old AP 透過 IAPP Tunnel 傳來的 data，若 APME 收到的 status 不是 SUCCESSFUL，則 IAPP

Tunnel 無法被建立。

3.1.3 IAPP-TUNNEL-NOTIFY.indication

當 AP 收到 IAPP TUNNEL-notify packet 後，IAPP 會產生 IAPP-TUNNEL-NOTIFY.indication 用來告訴 APME 有一個 Station 已經 Reassociated 到另一個 AP (New AP)，APME應該回覆一個 IAPP-TUNNEL.response packet 給該New AP。

IAPP-TUNNEL-NOTIFY.indication primitive 有下列的 semantics

IAPP-TUNNEL-NOTIFY.indication {
MAC Address，
New BSSID
Sequence Number，
AP Address，
}

MAC Address 是依據 IAPP TUNNEL-notify packet 中所指示 reassociated 到 New AP 的 station 的 MAC Address。

New BSSID 是 station reassociated 的 New AP 的 WM MAC address。

Sequence Number是來自於station 發出 Reassociation Request frame 中的Sequence Number field。

AP Address 是New AP的DSM IP address，也就是傳送IAPP TUNNEL-notify packet 的 AP 的 IP address。

3.1.4 IAPP-TUNNEL-NOTIFY.response

當APME 收到 IAPP-TUNNEL-NOTIFY.indication 後，APME 會回覆IAPP-TUNNEL.response 給 IAPP，指示 IAPP-TUNNEL-NOTIFY.indication 的處理結果。IAPP收到 IAPP-TUNNEL-NOTIFY.response 後，會將 Status 透過 IAPP TUNNEL-response packet 傳送給 New AP。

IAPP-TUNNEL-NOTIFY.response primitive 有下列的 semantics

IAPP-TUNNEL-NOTIFY.response {
MAC Address，
New BSSID
Sequence Number，
AP Address，
Status
}

MAC Address 是依據 IAPP TUNNEL-notify packet 中所指示 reassociated 到New AP 的 station 的 MAC Address。

New BSSID 是 station reassociated 的 New AP 的 WM MAC address。

Sequence Number是來自於 station發出 Reassociation Request frame 中的Sequence Number field。

AP Address是New AP的DSM IP address，也就是傳送 IAPP TUNNEL-notify packet 的 AP 的 IP address。

Status 用來指示 IAPP-TUNNEL-NOTIFY.indication 的結果，結果可能為 SUCCESSFUL 或 DENIED。SUCCESSFUL 表示處理結果正確無誤，允許 IAPP Tunnel 的建立。
DENIED表示IAPP-TUNNEL-NOTIFY.indication 所指定的AP無法被驗證或者因其他理由不被允許建立IAPP Tunnel。

3.1.5 IAPP-TUNNEL-DATA.request

當 IAPP Tunnel 已經建立，而有 data 欲透過 IAPP Tunnel 傳送到 Remote AP 時， APME 會以這個 IAPP-TUNNEL-DATA.request 要求 IAPP entity 將此 frame透過 IAPP Tunnel機制傳給 Remote AP，IAPP 收到 IAPP-TUNNEL.DATA. rsponse 後，會將整個 802.11 frame 封裝到 IAPP-TUNNEL.DATA中，然後透過 IAPP TUNNEL傳送給 Remote AP。

IAPP-TUNNEL-DATA.request primitive 包含下列的 semantics

IAPP- TUNNEL-DATA {
MAC Address，
Sequence Number，
Peer BSSID，
Local BSSID，
Data
}

MAC Address 是 station 的 MAC Address。

Sequence Number 與 Reassociation Request frame 中的 Sequence Number 相同。

Peer BSSID 是 remote AP的 WM MAC address。

Local BSSID是 AP 自己的 WM MAC address。

Data 是整個 802.11 frame。

3.1.6 IAPP-TUNNEL-DATA.confirm

這個 service primitive 是 IAPP用來將 IAPP-TUNNEL-DATA.request 處理結果回覆給 APME，APME 可透過 IAPP-TUNNEL-NOTIFY.confirm 中的 Status field 得到處理結果。

The IAPP-TUNNEL-NOTIFY.confirm primitive 包含下列的 semantics

IAPP-TUNNEL-NOTIFY.confirm {
MAC Address，
Sequence Number，
Peer BSSID，
Local BSSID，
Status
}

MAC Address 是 station 的 MAC Address。

Sequence Number 與 Reassociation Request frame 中的 Sequence Number 相同。

Peer BSSID 是 Remote AP的 WM MAC address。

Local BSSID是 Local AP 的 WM MAC address。

Status用來指示IAPP-TUNNEL-DATA.request 的結果，結果可能為 SUCCESSFUL 或 FAIL。 SUCCESSFUL 表示 data 已經 透過 IAPP Tunnel 傳送給remote AP，FAIL 表示無法找到相對應的 IAPP Tunnel。

3.1.7 IAPP-TUNNEL-DATA.indication

當 AP 收到來自於 IAPP Tunnel 的 data 時，IAPP 會以IAPP-TUNNEL-DATA.indication 通知 APME 有 Data 從 IAPP Tunnel 的另一端的 AP 傳來，APME 收到 IAPP-TUNNEL-DATA.indication 後，會將 data 部分交由 MLME 處理。

IAPP-TUNNEL-DATA.indication primitive 包含下列的 semantics

IAPP-TUNNEL.indication {
MAC Address，
Sequence Number，
Peer BSSID，
Local BSSID，
Peer IP Address，
Local IP Address，
Data
}

MAC Address 是 station 的 MAC Address。

Sequence Number 與 Reassociation Request frame 中的 Sequence Number 相同。

Peer BSSID 是 Remote AP的 WM MAC address。

Local BSSID是 Local AP 的 WM MAC address。

Peer IP 是 Remote AP 的 DSM IP address。

Local IP 是 Local AP 的 DSM IP address。

Data 是整個 802.11 frame。

3.1.8 IAPP-TUNNEL-DATA.response

當 APME 收到 IAPP-TUNNEL-DATA.indication 後， APME 會以 IAPP-TUNNEL-DATA.response 將處理結果回覆給IAPP，IAPP 可透過 IAPP-TUNNEL-DATA.response 中的 Status field 得到其處理結果。

The IAPP-TUNNEL.response primitive has the following semantics

IAPP-TUNNEL.response {
MAC Address，
Sequence Number，
Local BSSID，
Peer BSSID，
Local IP Address，
Peer IP Address，
Status
}

MAC Address 是 station 的 MAC Address。

Sequence Number 與 Reassociation Request frame 中的 Sequence Number 相同。

Peer BSSID 是 Remote AP的 WM MAC address。

Local BSSID是 Local AP 的 WM MAC address。

Peer IP 是 Remote AP 的 DSM IP address。

Local IP 是 Local AP 的 DSM IP address。

Data 是整個 802.11 frame。

Status 用來指示 IAPP-TUNNEL-DATA.indication.request 的結果，結果可能為 SUCCESSFUL 或 FAIL，SUCCESSFUL 表示 data 已經順利地交由MLME 處理，FAIL 表示無法找到相對應的 IAPP Tunnel。

3.1.9 IAPP-TUNNEL-TERMINATE.request

當 station 與 New AP 的 802.1x 認證程序完成以及 PTK，GTK 產生後，APME 會產生 IAPP-TUNNEL-TERMINATE.request 來要求 IAPP 終止 IAPP Tunnel。IAPP 收到 IAPP-TUNNEL-TERMINATE.request 後會傳送 TUNNEL-Terminate packets 到 Remote AP 並將 IAPP Tunnel 終止。

IAPP-TUNNEL-TERMINATE.request primitive 有下列的 semantics

IAPP-TUNNEL-TERMINATE.request {
MAC Address，
Sequence Number，
Old AP，
}

MAC Address 是 reassociated 到此AP 的 station 的 MAC Address。

Sequence Number 是來自於 station 發出 Reassociation Request frame 中的 Sequence Number field。

Old AP 是 Reassociated 到此 AP 的 Station 上一個 Associated AP 的 WM MAC address，APME 可以從 station 發出 Reassociation Request frame 中的 Current AP Address field 取得。

3.1.10 IAPP-TUNNEL-TERMINATE.confirm

IAPP 收到 IAPP-TUNNEL-TERMINATE.request 後會以 IAPP-TUNNEL-TERMINATE.confirm 來回覆APME 其處理結果，APME 可透過 IAPP-TUNNEL-TERMINATE.confirm 的 Status field 得到處理結果。

IAPP-TUNNEL-TERMINATE.confirm primitive 有下列的 semantics

IAPP-TUNNEL-NOTIFY.confirm {
MAC Address，
Sequence Number，
Old AP，
Status
}

MAC Address 是 station 的 MAC Address。

Sequence Number是來自於Station 發出 Reassociation Request frame 中的Sequence Number field。

Old AP 是 Reassociated 到此AP 的 Station 上一個 Associated AP 的 WM MAC address，APME 可以從 station 發出 Reassociation Request frame 中的 Current AP Address field 取得。

Status 用來指示 IAPP-TUNNEL.request 的結果，結果可能為 SUCCESSFUL 或 FAIL， SUCCESSFUL 表示 IAPP Tunnel 已終止，FAIL 表示 無法找到對應的 IAPP Tunnel。

3.1.11 IAPP-TUNNEL.TERMINATE.indication

當 IAPP 收到 IAPP TUNNEL-TERNAMATE packet 後，會以IAPP-TUNNEL. indication 告訴 APME 已經收到一個終止IAPP Tunnel 的 packet 從 Remote AP 傳來這個 IAPP Tunnel 即將被終止。

IAPP-TUNNEL.indication primitive 有下列的 semantics

IAPP-TUNNEL.TERMANATE.indication {
MAC Address，
New BSSID
Sequence Number，
AP Address，
}

MAC Address 是依據 IAPP TUNNEL-NOTIFY packet 中所指示 reassociated 到 New AP 的 station 的 MAC Address。

New BSSID 是 station reassociated 的 New AP 的 WM MAC address。

Sequence Number是來自於station 發出 Reassociation Request frame 中的Sequence Number field。

AP Address是New AP的DSM IP address，也就是傳送IAPP TUNNEL-TERMINATE packet 的 AP 的 IP address。

3.1.12 IAPP-TUNNEL.response

當 APME 收到 IAPP-TUNNEL.TERMINATE.indication 後， APME 會以 IAPP-TUNNEL.response 來回覆 IAPP 其處理結果，這個 IAPP Tunnel 即被終止。

IAPP-TUNNEL.response primitive 有下列的 semantics

IAPP-TUNNEL.response {
MAC Address，
New BSSID
Sequence Number，
AP Address，
Status
}

MAC Address是依據IAPP TUNNEL-NOTIFY packet中所指示 Reassociated 到New AP 的 station 的 MAC Address。

New BSSID 是 station reassociated 的 New AP 的 WM MAC address。

Sequence Number 是來自於Station發出 Reassociation Request frame 中的Sequence Number field。

AP Address 是 New AP 的 DSM IP address，也就是傳送 IAPP TUNNEL-NOTIFY packet 的 AP 的 IP address。

Status 用來指示 IAPP-TUNNEL.TERMINATE.indication 的結果，其值為 SUCCESSFUL。

3.2 漫遊程序

在 IAPP Tunnel 機制中，圖 3.2.1，在漫遊過程中加解密的端點為 Old AP 與 Station B。

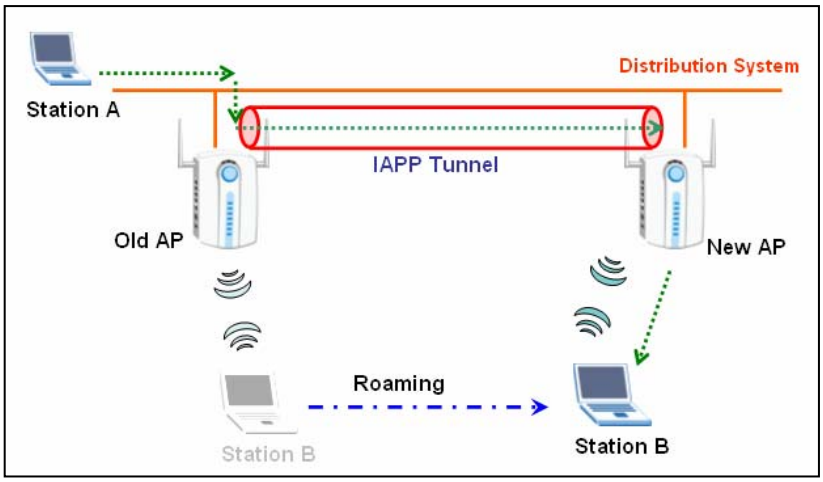


圖 3-2-1

3.2.1 Actions triggered by an IAPP-TUNNEL-NOTIFY.request

當 802.11i/WPA enabled 的 Station， Reassociate 到此 AP， APME 會以 IAPP-TUNNEL-NOTIFY.request primitive 要求IAPP 傳送 TUNNEL-notify packet 到該Station原先Associated的AP (Old AP)，讓Old AP知道此Station的Reassociation 並且要求建立 IAPP Tunnel。

IAPP收到這個 service primitive後，IAPP entity 要以 Old AP 的 MAC address 向RADIUS server查詢其DSM 的 IP address，並傳送 IAPP TUNNEL-notify packet 給Old AP 告知 station 的 reassociation 並要求建立 IAPP Tunnel，圖3-2-2。 Old AP 則以 IAPP TUNNEL-response 回覆。

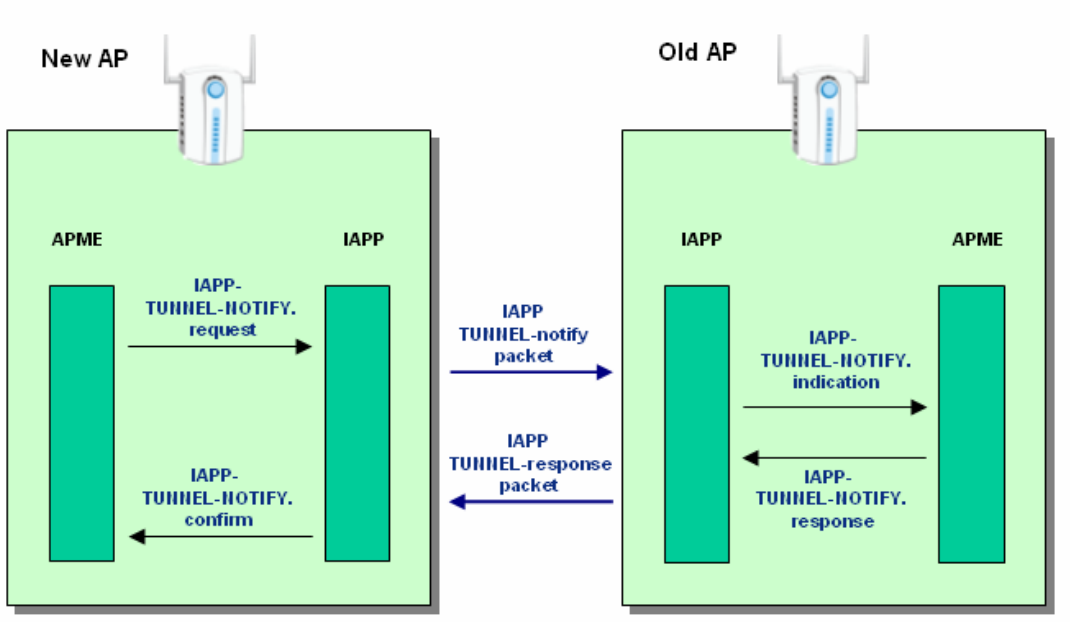


圖 3-2-2

3.2.2 Actions triggered by an IAPP-TUNNEL.DATA.request

在Station 從 Old AP 漫遊到 New AP 期間，Old AP 與 New AP 間的 IAPP Tunnel 已經建立，當資料從 DS 傳送給 Station 或從 Station 傳到 DS 皆會藉由 IAPP Tunnel 來傳送。

若 data 從 station 傳送到 DS。

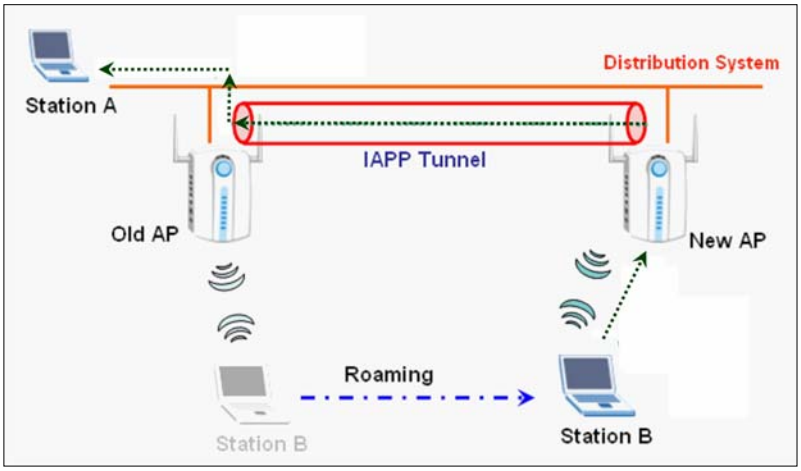


圖 3-2-3

對 New AP 而言:

當 APME 從 MLME 收到 802.11 frame 要透過 IAPP Tunnel 傳到 Remote AP (Old AP)，APME 會以這個 IAPP-TUNNEL-DATA.request 要求 IAPP entity 將此 frame 封裝至 TUNNEL-data packet 然後透過 IAPP Tunnel 傳給 Old AP。

對 Old AP 而言:

當 IAPP 收到 TUNNEL-data packet，IAPP 將 packet 中的 data 恢復其 802.11 frame 格式，透過 APME 再交由 MLME 傳給 Station。

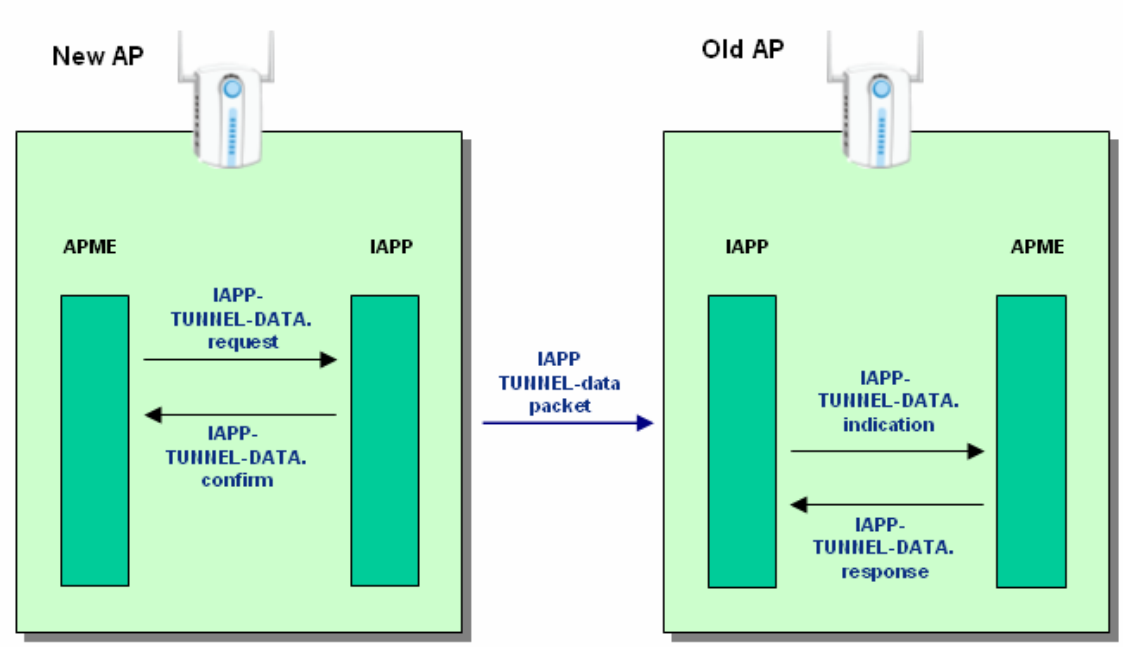


圖3-2-4

若 data 從 DS 傳送到 station。

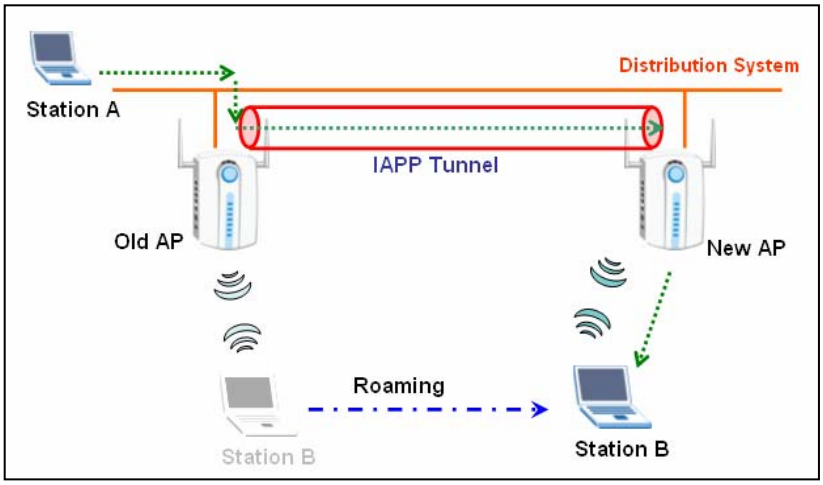


圖3-2-5

對 Old AP 而言:

當APME 從MLME 收到 802.11 frame 要透過 IAPP Tunnel 傳到 Remote AP，APME 會以這個 IAPP-TUNNEL-DATA.request 要求 IAPP entity 將此 frame 封裝至 TUNNEL-data packet 然後透過 IAPP Tunnel 傳給 New AP。

對 New AP 而言:

當IAPP 收到 TUNNEL-data packet，IAPP 將 packet 中的 data 恢復其 802.11 frame 格式，透過 APME 再交由 MLME 傳至DS。

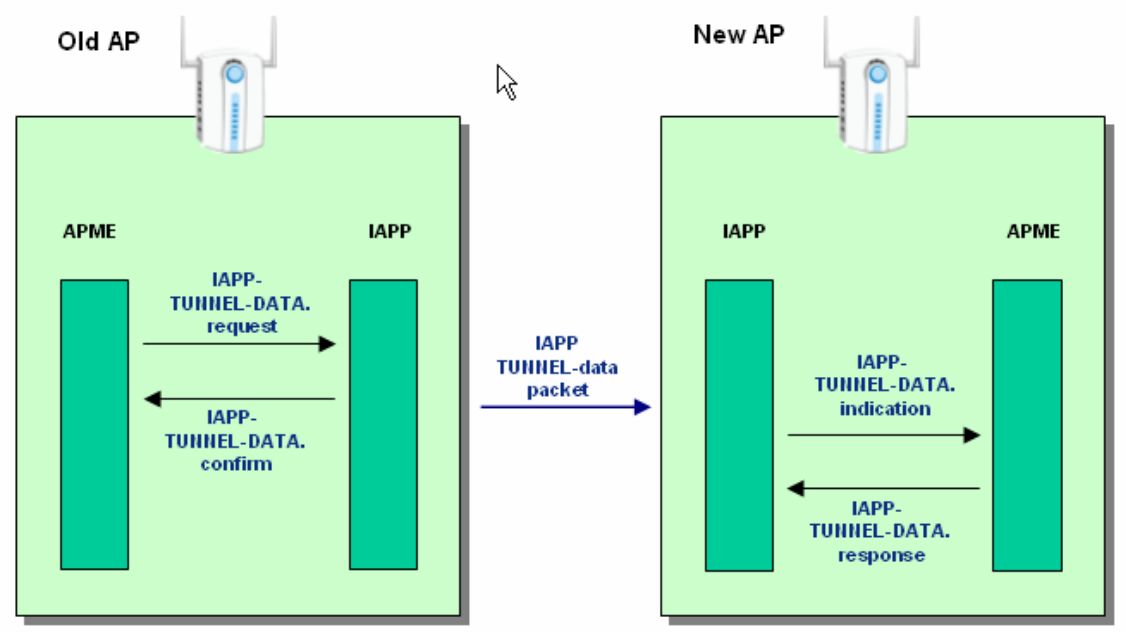


圖3-2-6

3.2.3 Actions triggered by an IAPP-TUNNEL.TERMINATE.request

當 Station 與 New AP 的 802.1x 認證程序完成以及 PTK，GTK 產生後，New AP 的 APME 會產生 IAPP-TUNNEL-TERMINATE.request 要求IAPP 終止 IAPP Tunnel，然後 IAPP 會傳送TUNNEL-Terminate packets 到 Remote AP 並將 IAPP Tunnel 終止，至此以後，該Station 的加解密以及資料傳輸皆透過 New AP。

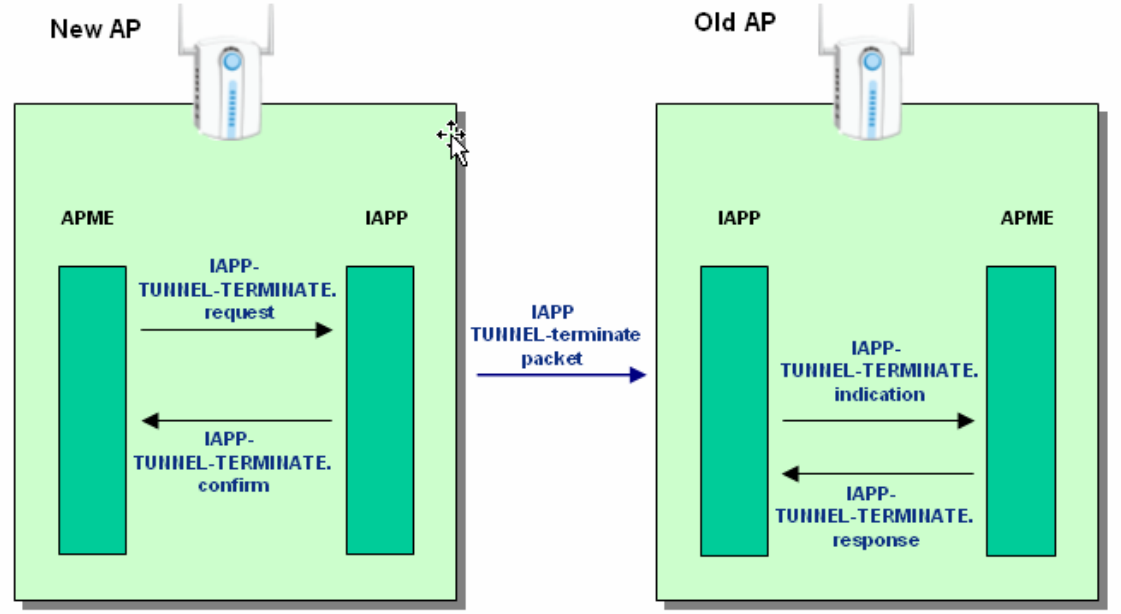

New AP
Old AP
APME
IAPP
IAPP-
TUNNEL-TERMINATE.
request
IAPP-
TUNNEL-TERMINATE.
confirm
IAPP
TUNNEL-terminate
packet
IAPP
APME
IAPP-
TUNNEL-TERMINATE.
indication
IAPP-
TUNNEL-TERMINATE.
response

圖3-2-7

3.3 Packet Formats

3.3.1 General IAPP Packet Format

圖 3-3-1 為一般的 IAPP 封包格式，IAPP 封包可以藉由 TCP 或 UDP 傳輸，其 port number 是 35173。

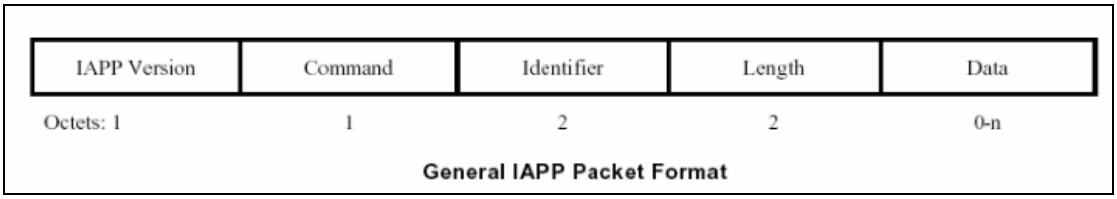


圖 3-3-1

IAPP Version 欄位長度為八個 bits，用來表示 IPAA 協定版本，“0” 用來表示目前的版本，其餘的值尚未被定義，作為保留用。

Command 欄位長度為八個 bits，其值為從 0 到 255 的整數， 用來表示 IAPP 封包的功能，表 3-3-1 為 Command 欄位的對應表，目前 802.11F 定義了七個封包種類，分別從 0 至 6，其餘的值為保留用，在 IAPP Tunneling 的設計上需用到 4 個封包種類，因此在此論文中我用了 7 到 10 作為 IAPP Tunnel 之使用。

Value	Command
0	ADD-notify
1	MOVE-notify
2	MOVE-response
3	Send-Security-Block
4	ACK-Security-Block
5	CACHE-notify
6	CACHE-response
7	TUNNEL-notify
8	TUNNEL-response
9	TUNNEL-data
10	TUNNEL-Terminate-notify
11-255	Reserved

表 3-3-1 **Command field for IAPP-TUNNEL**

Identifier 欄位長度為 16 個 bits，作為 IAPP 封包的識別用，對於 IAPP Request 封

包而言，此值必須為唯一值，IAPP Requests 和 Responses 封包以此值作為對應，此外，Identifier 也可以作為封包重複接收的偵測用，當 device 收到重複 Identifier 的封包則會將其丟棄。

Length 欄位長度為 16 個 bits，指示出整個 IAPP 封包的長度，包含 version，command，identifier，length 以及 data 欄位，當封包長度大於 Length 欄位所指定的值時，超出的部份將被忽略，若長度不及 Length 欄位所指定的值時，此封包將被丟棄。

Data 欄位是一個可變長度的欄位，其內容則依據 Command 欄位所指示的 IAPP 封包型態而定。

3.3.2 TUNNEL-notify Packet

TUNNEL-notify 封包透過 TCP 來傳輸，當 802.11i/WPA enabled 的 station reassociate 到AP時，此AP會傳送 TUNNEL-notify 封包到 station 原先 associated 的 AP (Old AP)，讓 Old AP 知道此 station 的 reassociation 並且要求建立 IAPP Tunnel，由於IAPP Tunneling的建立過程需要數個封包交換，因此較可靠的 TCP 比 UDP 更為適合，圖3-3-2 表示 TUNNEL-notify 封包的data 欄位的格式。

Address Length	Reserved	MAC Address	Sequence Number
Octet : 1	1	n = Address Length	2

圖 3-3-2

Address Length 欄位欄位為 8 個 bits 整數，用來表示 MAC address 長度的 Octect 數目，它讓 IAPP 可以擴充至 IEEE 64-bit MAC addresses。

Reserved 欄位目前此版本的 IAPP 為應為 0，並且是被忽略的，其目的是為了讓 MAC Address 欄位成為 16 bits 的整數。

MAC Address 欄位是 Reassociated 到此 AP 的 station 的 MAC Address，

Sequence Number 欄位為 0 到 4095 整數，來自於 station 發出 Reassociation Request frame 中的 Sequence Number field。

3.3.3 TUNNEL-response Packet

TUNNEL-response 封包透過 TCP 來傳輸，當 Old AP 收到 New AP 傳送過來的 TUNNEL-notify 封包後， 會以 TUNNEL-response 封包作為回覆，由於 IAPP Tunneling 的建立過程需要數個封包交換，因此較可靠的 TCP 比 UDP 更為適合，圖 3-3-3 表示 TUNNEL- response 封包的 data 欄位的格式。

TUNNEL-response Packet

Address Length	Status	MAC Address	Sequence Number
Octet : 1	1	n = Address Length	2

Status Value	Definition
0	Successful
1	Denied
2-255	Reserved

圖 3-3-3

Address Length 欄位欄位為 8 個 bits 整數，用來表示 MAC address 長度的 Octect 數目，它讓 IAPP 可以擴充至 IEEE 64-bit MAC addresses。

Status 欄位為 8 個 bits 整數。

MAC Address 欄位是 Reassociated 到此 AP 的 station 的 MAC Address。

Sequence Number 欄位為 0 到 4095 整數，來自於 station 發出 Reassociation Request frame 中的 Sequence Number field。

Suatus 欄位欄位為 8 個 bits 整數，用來表示收到 TUNNEL-notify 後的處理結果，表xx 為Status 欄位的對應表，Status 可能為 SUCCESSFUL 或 DENIED。

SUCCESSFUL 表示 TUNNEL-notify後的處理結果正確無誤，允許IAPP Tunnel 的建立，DENIED表示傳送 TUNNEL-notify的AP無法被驗證，或是 MAC address欄位所指示的 Station 並未存在於此AP的 Association Table 中，或者因其他理由不被允許建立IAPP Tunnel。

MAC Address 欄位是 Reassociated 到 New AP 的 station 的 MAC Address。

Sequence Number 欄位為 0 到 4095 整數，相同於 TUNNEL-notify 中的 Sequence Number 欄位。

3.3.4 TUNNEL-data Packet

TUNNEL-data 封包透過 TCP 來傳輸，圖 3-3-4 表示 TUNNEL-notify 封包的 data 欄位的格式。

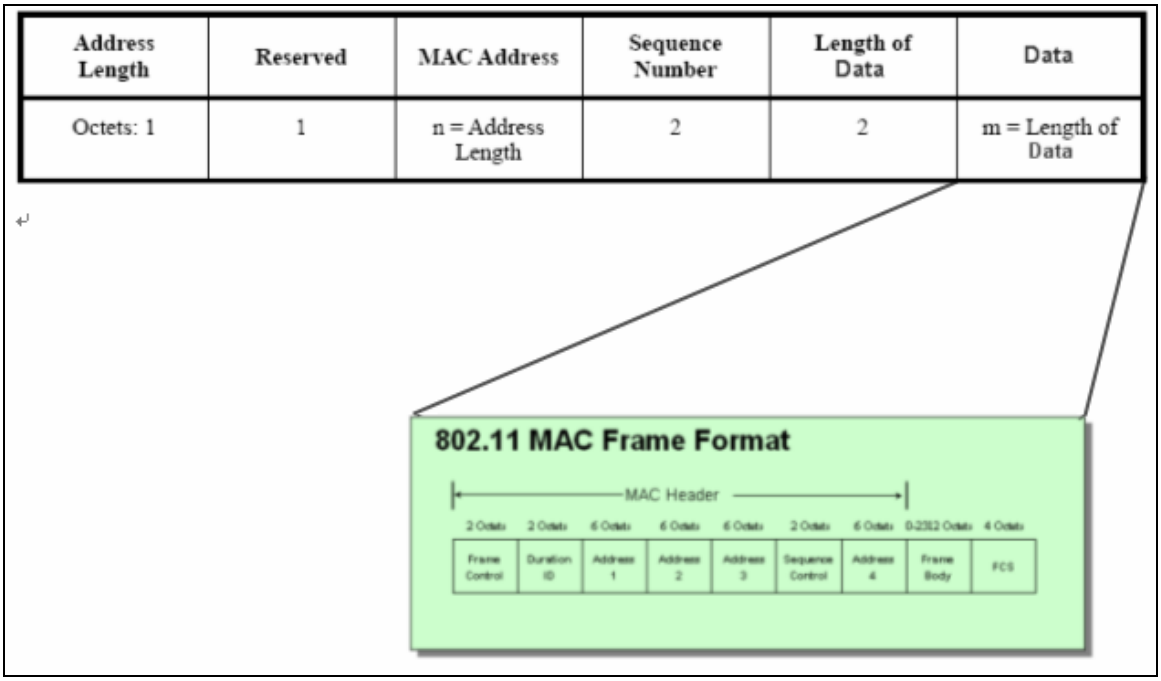


圖 3-3-4

Address Length 欄位欄位為 8 個 bits 整數，用來表示 MAC address 長度的 Octect 數目，它讓 IAPP 可以擴充至 IEEE 64-bit MAC addresses。

Reserved 欄位目前此版本的 IAPP 為應為 0，並且是被忽略的，其目的是為了讓 MAC Address 欄位成為 16bits 的整數。

MAC Address 欄位是 Reassociated 到此 AP 的 station 的 MAC Address。
Sequence Number 欄位為 0 到 4095 整數，來自於 station 發出 Reassociation Request frame 中的 Sequence Number field。

Data 是一個不定長度的欄位，它包含整個 802.11 frame 的資料，當資料從 DS 傳到 station 時，Old AP 以它的 session key 加密並將整個 802.11 frame 置於 Data 欄位透過 Tunnel 傳給 New AP，New AP 再將還原為 802.11 frame 傳給 station。反之，若資料是由 station 送往 DS 時，station 以它的 session key 加密 802.11 frame 傳給 New AP，New AP 將整個 802.11 frame 置於 Data 欄位透過 Tunnel 傳給 Old AP，Old AP 解密後傳送至 DS。

Length of Data 說明了 Data 欄位的長度。

3.3.5 TUNNEL-terminate Packet

IAPP Tunnel 機制使用 TUNNEL-Terminate 封包來告知對方將 IAPP Tunnel 終止，它並不需要傳送確認的訊息，TUNNEL-data 封包可以透過 TCP 或 UDP 來傳輸，圖 3-3-5 表示 TUNNEL-notify 封包的 data 欄位的格式。

Address Length	Reserved	MAC Address	Sequence Number
Octet : 1	1	n = Address Length	2

圖 3-3-5

Address Length 欄位欄位為 8 個 bits 整數，用來表示 MAC address 長度的 Octect 數目，它讓 IAPP 可以擴充至 IEEE 64-bit MAC addresses。

Reserved 欄位目前此版本的 IAPP 為應為 0，並且是被忽略的，其目的是為了讓 MAC Address 欄位成為 16 bits 的整數。

MAC Address 欄位是 Reassociated 到此 AP 的 station 的 MAC Address。

Sequence Number 欄位為 0 到 4095 整數，來自於 station 發出 Reassociation Request frame 中的 Sequence Number field。

第四章 結論

無線網路已經是目前的趨勢，且由於近年來 VoIP 的興起，再頻寬及價格問題逐漸解決的情況下，VoIP 將帶動一場電信革命，屆時無線網路結合 VoIP 將是主要的應用模式。隨著相關軟硬體研發廠商不斷改進產品規格與性能，以及越來越多樣化的網路服務，未來行動通訊網路將無所不在地存在於人們的生活之中。因此如何提供一個簡單、安全、有品質的無線上網環境成了一個相當重要的議題。

IEEE 802.11F 的漫遊機制延伸了無線區域網路的距離限制，而 IEEE 802.11i 是下一代強化加密機制與私密性的標準方案，802.11i 結合強化後的認證與加密機制，改善了原先 WLAN 為人詬病的安全問題。IAPP Tunnel 機制能使 802.11F 與 802.11i 聯合運作更為完善，藉由 IAPP Tunnel 讓 PTK 與 GTK 完全不需要在網路上被交換，不僅更加安全而且避免許多額外的 Traffic 產生。藉由 IAPP Tunnel 讓 AP 不需要額外維護 Proactive Cache， IAPP Tunnel 機制也讓 AP 不需要再維護 Neighborhood Graph，並且 Station 不需要預先所有可能會漫遊的 AP 完成認證程序，而能避免漫遊過程中資料傳輸中斷，達到 Seamless Roamng 的目標。

參考文獻

[1] “Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation “, IEEE 801.11F, 14 July 2003.

[2] “Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications”, ANSI/IEEE Std 802.11, LAN MAN Standards Committee of the IEEE Computer Society, 1999.

[3] Stuart J. Kerry，Al Petrick，Harry Worstell, Tim Godfrey, Dave Halasz, Jesse Walker, “Draft Amendment to STANDARD FOR Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Medium Access Control (MAC) Security Enhancements”, IEEE 802.11i D4.1, July 2003.

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

[5] Blunk, L. and Vollbrecht, J. IETF RFC 2284, PPP Extensible Authentication Protocol (EAP) , March 1998.

[6] IEEE Standard 802.1x, “IEEE Standard for Local and metropolitan area networks ─ Port-Based Network Access Control”, June 2001.

[7] Bernard Aboba, Dan Simon, IETF RFC 2716, PPP EAP TLS Authentication Protocol , October 1999.

[8] Sangheon Pack and Yanghee Choi, “Fast Inter-AP Handoff using Predictive-Authentication Scheme in a Public Wireless LAN," Networks 2002 (Joint ICN 2002 and ICWLHN 2002), Aug. 2002.

[9] Robert Moskowitz, ICSAlabs/TruSecure, “PMK Plumbing for Fast Roaming“, June 4, 2003.