

# 國立交通大學

資訊學院 資訊學程

## 碩士論文

確保合法使用 IP 位址之 IP 管理機制的設計與實作

Design and Implementation of an IP Management Scheme  
to Enforce Legal Use of IP Addresses

研究生：李雨龍

指導教授：曾建超 教授

中華民國九十八年七月

確保合法使用 IP 位址之 IP 管理機制的設計與實作

Design and Implementation of an IP Management Scheme to  
Enforce Legal Use of IP Addresses

研究生：李雨龍

Student：Yu-Lung Lee

指導教授：曾建超

Advisor：Chien-Chao Tseng

國立交通大學

資訊學院 資訊學程



A Thesis

Submitted to College of Computer Science  
National Chiao Tung University  
in partial Fulfillment of the Requirements  
for the Degree of  
Master  
in  
Computer Science  
July 2009  
Hsinchu, Taiwan, Republic of China

中華民國九十八年七月

# 確保合法使用 IP 位址之 IP 管理機制的設計與實作

研究生：李雨龍

指導教授：曾建超 教授

國立交通大學 資訊學院 資訊學程碩士班

## 摘要

為確保使用者在 IP 網路中合法使用 IP Address 的權益，本論文提出一套 IP 管理機制。由於 IP 網路上是使用 IP Address 當作是網路設備的識別，因此每個網路設備需要一個唯一的 IP Address，以便能跟網路上的其他網路設備做溝通。當同個網域內有多個網路設備使用相同的 IP Address 時，會造成 IP Address 衝突的問題，可能導致合法擁有 IP Address 的網路設備無法使用 IP 網路。因此，我們提出一套能管理網域內全部的 IP Address 並且控制每個 IP Address 使用權的 IP 管理機制，來解決 IP Address 衝突的問題，本機制不僅保證合法使用者存取 IP 網路的權利，對非法使用的 IP Address 也會進行封鎖；並且允許在事先沒有註冊 IP Address 使用的情況下，可以使用手動或動態的方式設定網路設備的 IP Address。

本機制基本概念是動態地綁定使用者帳號、IP Address、MAC Address 和 Port Number，以便即使 IP Address 沒有之前綁定的資訊，也可以管理全部的 IP Address 和控制每個 IP Address 的使用權。並且為了解決 IP Address 衝突的問題，本機制會利用 Authenticator 將非法使用者封鎖，此 Authenticator 可以是 Ethernet switch，或是無線環境下的 Access Point。

本機制使用 IP Management Server 來管理所有的 IP Address，並且利用 Authenticator 來限制只有使用正確 IP Address 的合法使用者的 traffic 可以通過。在 Authenticator 和 IP Management Server 之間透過延伸 Dynamic Host Control Protocol (DHCP) 做溝通，來提供使用 IP Address 的最大彈性。

IP Management Server 會將 IP Address 和使用者帳號、MAC Address 做綁定，並紀錄在 IP Management Server 的 IP Address Assignment Table 中，IP Address 和使用者帳號的綁定可以是手動或動態的，即使用者可以事先註冊固定使用的 IP Address，或是當需要使用 IP Address 時，動態地取得 IP Address；另一方面，IP Address 和 MAC Address 的綁定是動態的，當 IP Management Server 收到合法使用者的 IP Assignment request 時，會將 MAC Address 和分配給使用者使用的 IP Address，動態的綁定在 IP Address Assignment Table 中。

不同於 802.1X 中的 Authenticator，本機制的 Authenticator 會將使用者帳號和 IP Address、MAC Address 和 Port Number 做綁定，並紀錄在 Authenticator 的 Supplicant State Table 中，透過 Supplicant State Table 的使用，Authenticator 可以確保 IP Address 合法的被使用，並且能夠保障合法使用者，以及封鎖非法使用者。

最後我們透過實作來驗證本機制的可行性，實作結果顯示本機制確實可以在最大的彈性下，確保合法的使用 IP Address。

**關鍵詞：**IP 網路、DHCP、IP 管理、動態 IP 分配、訊息交換、IP 衝突

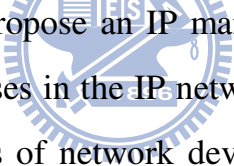
# Design and Implementation of an IP Management Scheme to Enforce Legal Use of IP Addresses

Student : Yu-Lung Lee

Advisor : Dr. Chien-Chao Tseng

Degree Program of Computer Science  
National Chiao Tung University

## Abstract



In this thesis, we propose an IP management scheme to enforce the legal use of IP addresses in the IP network. The IP network uses IP addresses as the identities of network devices. Therefore, each device needs a unique IP address so that devices can communicate with one another in the network. When two or more devices use the same IP address in the same network domain, an IP Conflict problem occurs and the host with a legal IP address may not be able to access the IP network. Therefore, we propose an IP management scheme that can resolve the IP Conflict problem by managing all IP addresses and controlling the use of each IP address. As a consequence, it can not only assure the access right of legal users but also block the illegal use of IP addresses. Furthermore, it allows a device to configure its IP address

either statically or dynamically without registering the address beforehand.

The basic idea of the proposed scheme is to bind users, IP addresses, MAC addresses and port numbers dynamically so that we can manage all IP addresses and control the use of each IP address without a priori information on the bindings. Furthermore, in order to resolve the IP conflict problem the proposed scheme will also block illegal users at network entry points, namely Authenticators, which could be situated at Ethernet switches or wireless access points.

The proposed scheme employs an IP Management Server to management all IP addresses and augments Authenticators to allow only the traffic from legal users with correct IP addresses. Furthermore, the proposed scheme also adopts an extended Dynamic Host Control Protocol (DHCP) for Authenticators to communicate with the IP Management Server to offer the maximum flexibility in using IP addresses.

The IP Management Server records the bindings of IP addresses with both user accounts and MAC addresses in an IP Address Assignment Table. The bindings between IP address and user accounts could be statically or dynamically; that is, a user could either pre-subscribe permanently or acquire dynamically an IP address when needs. On the other hand, the binding between an IP address and a MAC address is done dynamically by the IP Management Server when the server receives an IP Assignment request from the MAC address

used by a legal user.

Different from the Authenticator in 802.1X, the Authenticator in our scheme bind user accounts to IP addresses, MAC addresses and Port numbers in their Supplicant State Tables. With Supplicant State Tables, Authenticators can ensure legal use of IP addresses, protecting legal users but blocking illegal users.

We have implemented the proposed scheme to verify its effectiveness. The experimental results show that the proposed scheme indeed can enforce legal use of IP addresses with maximum flexibility.

**Keywords :** IP Networks 、 DHCP 、 IP Management 、 Dynamic IP assignment 、 Message Exchange 、 IP Conflict



## 誌 謝

本論文能夠順利地完成，不是單單只倚靠個人的辛苦以及努力，而是要歸功於許多人的指導、協助。在此，希望以我最誠摯的心意，向你們說聲「謝謝」。

首先感謝我的指導教授曾建超教授，由於他不吝於分享其豐富的經驗與知識，給予我論文上認真地指導與細心地協助、耐心地傾聽我的想法、關心我的狀況。感謝口試委員嚴力行教授、曹孝櫟教授與張弘鑫教授對於本論文詳細的指正與建議，使得本篇論文內容能更加完善。

特別感謝史永健學長的熱心指導，在學長的督促鼓勵與共同討論下，使得本篇論文能順利完成，在此預祝史永健學長能順利取得博士學位。

最後要感謝我的老婆 佳雯，雖然正值懷孕和生產期間，但是妳仍能體諒我因為課業而無法常陪伴在妳身旁，有了妳的支持與體諒，我才能專心完成學業，妳的鼓勵是我精神上最大的支柱。

最後，僅以此文獻給我的父母，感謝你們在背後無私的支持，讓我能有堅定的信心，向前邁進並勇敢迎接未來。





# 目 錄

摘 要.....	iii
Abstract.....	v
誌 謝.....	viii
目 錄.....	ix
圖目錄.....	xii
第一章 緒論.....	1
1.1 研究動機.....	1
1.2 研究目的.....	2
1.3 章節簡介.....	3
第二章 背景知識及相關議題介紹.....	4
2.1 User Authentication.....	4
2.1.1 Web Login + RADIUS.....	4
2.1.1.1 RADIUS 簡介.....	5
2.1.1.2 RADIUS 封包格式.....	6
2.1.1.3 RADIUS 工作原理.....	7
2.1.2 IEEE 802.1X.....	8
2.1.2.1 EAP 封包格式.....	10
2.1.2.2 EAPOL 封包格式.....	11
2.1.2.3 IEEE 802.1X 工作原理.....	12
2.1.3 IEEE 802.11i.....	14

2.2	Dynamic Host Configuration Protocol (DHCP) .....	15
2.2.1	DHCP Server Behavior.....	16
2.2.2	DHCP Client Behavior .....	17
2.2.3	DHCP 封包格式 .....	17
2.2.4	DHCP 工作原理 .....	19
第三章 相關研究 .....		22
3.1	研究背景.....	22
3.2	IP/MAC Binding on DHCP Server .....	22
3.3	IP/MAC Binding on Switch or AP.....	23
3.4	NCTU Dormitory Network Management System.....	24
3.5	IEEE 802.1X with IP Address Management .....	26
3.6	自動化宿舍網路註冊管理系統.....	27
3.7	總結 .....	28
第四章 確保合法使用 IP 位址之 IP 管理機制 .....		30
4.1	簡介 .....	30
4.1.1	Supplicant State Table .....	32
4.1.2	IP Address Assignment Table.....	34
4.1.3	Dynamic IP Assignment Mechanism .....	36
4.1.4	Extended DHCP Message.....	39
4.2	Analysis of Proposed Scheme.....	40
4.2.1	IP Address Assignment and Access Control.....	41
4.2.1.1	Static IP Address Configuration.....	41

4.2.1.1.1	Static IP Address with Pre-subscribed.....	41
4.2.1.1.2	Static IP Address without Pre-subscribed.....	43
4.2.1.1.3	Static conflicting IP Address with Non-subscribed .....	45
4.2.1.1.4	Static Non-conflicting IP Address with Non-subscribed.....	48
4.2.1.2	Dynamic IP Address Acquisition .....	50
4.2.1.2.1	Pre-subscribed IP Address .....	50
4.2.1.2.2	Non-subscribed IP Address.....	53
4.2.2	IP Address Releasing.....	55
4.3	單元總結.....	57
第五章 確保合法使用 IP 位址之 IP 管理機制的設計與實作 .....		58
5.1	實作方法.....	58
5.2	實作網路環境與系統.....	59
5.3	User 註冊流程說明.....	60
5.4	Supplicant 登入網路流程說明 .....	61
5.5	Authenticator 系統設計說明 .....	62
5.6	DHCP Server 系統設計說明.....	65
第六章 結論與未來工作.....		68
6.1	結論 .....	68
6.2	未來工作.....	70
參考文獻.....		71

# 圖目錄

Figure 2-1 Web Login for User Authenticator .....	5
Figure 2-2 RADIUS Packet Format .....	6
Figure 2-3 RADIUS Authentication Flow .....	7
Figure 2-4 IEEE 802.1X Authentication Flow .....	9
Figure 2-5 EAP Packet Format.....	10
Figure 2-6 EAPOL Packet Format.....	11
Figure 2-7 IEEE 802.1X EAP-MD5 Authentication Flow .....	13
Figure 2-8 IEEE 802.11i Authentication Flow.....	15
Figure 2-9 DHCP Packet Format.....	18
Figure 2-10 DHCP Packet Flow.....	20
Figure 3-1 IP/MAC Address Binding (引自 [22] ) .....	22
Figure 3-2 NCTU Dormitory Network IP Address Apply Flow .....	25
Figure 3-3 IEEE 802.1X with IP Address Management Scheme.....	26
Figure 3-4 自動化宿舍網路註冊管理系統 (引自 [24] ).....	27
Figure 4-1 IP Management Scheme concept overview .....	32
Figure 4-2 Supplicant State Table on Authenticator.....	32
Figure 4-3 IP Address Assignment Table on IP Management Server.....	35

Figure 4-4 IP Management Protocol with Extended DHCP Scheme .....	37
Figure 4-5 Extended DHCP Message Format.....	39
Figure 4-6 Static IP Address with Pre-subscribed IP Address.....	42
Figure 4-7 Static IP Address without Pre-subscribed IP Address.....	44
Figure 4-8 Static conflicting IP Address with Non-subscribed IP Address ....	46
Figure 4-9 Static Non-conflicting IP Address with Non-subscribed IP Address .....	49
Figure 4-10 User acquires subscribed IP Address with Dynamic IP Address Acquisition.....	51
Figure 4-11 User acquires IP Address with Dynamic IP Address Acquisition	53
Figure 4-12 IP Address Releasing .....	56
Figure 5-1 System architecture of proposed scheme implementation.....	58
Figure 5-2 Network Environment of proposed scheme implementation.....	59
Figure 5-3 User Account Apply Flow .....	60
Figure 5-4 Supplicant Login Flow.....	61
Figure 5-5 Authenticator System Flow of proposed scheme implementation	63
Figure 5-6 DHCP Server System Flow of proposed scheme implementation	66

# 第一章 緒論

## 1.1 研究動機

隨著網路技術的蓬勃發展，無論是企業、機關甚至是家庭、個人等，網際網路(Internet)都已經是現代人生活或工作上不可分割的一環，透過網路設備(network device)的使用，舉凡網路查詢資料、e-mail 收發、網路購物、利用電子銀行進行交易、用 Skype 講電話等都能輕易的達成，帶給我們許多的便利，而網路設備在我們使用網際網路上，扮演一個很重要的角色，也因此網路設備能正常且穩定的提供使用者使用網路上的服務和資源，就變成是一個很重要的課題。

在現今 IP Network 的環境上，每個網路設備都使用 IP Address 來當成唯一識別的 ID，供彼此辨識身分使用，因此當在同一個網域(network domain)中，同時存在兩個以上的網路設備使用相同的 IP Address 時，由於其他網路設備無法正確識別這兩個使用相同 IP Address 的網路設備，會導致所謂 IP Address 互相衝突的問題發生，而造成相同 IP Address 的網路設備無法順利使用網路上的服務和資源，進而影響使用者使用網路的權利。甚至更有惡意者利用此問題的特性，發動相關攻擊，使得合法的使用者無法使用網路，並造成網路環境混亂的問題。

為了解決上述問題，目前已經有一些 IP 管理的機制，例如限定某個網路設備只能固定使用某個 IP Address，或是網路設備均使用動態取得 IP Address 的機制，由 Dynamic Host Configuration Protocol (DHCP)[1] Server 統一管理所有的 IP Address 等等，雖然可達到基本預防 IP Address 衝突的問題，可是一旦有使用者不遵守相關設定，或是設定上有錯，同樣會造成 IP Address 衝突和網路環境混亂的問題，而且前述作法不具備彈性，無法同時支援使用者手動設定 (static configuration)或動態取得(dynamic acquisition) IP Address 的方式，在應用上並不

方便，反而容易因此衍生出其他的問題，也無法保障網路設備使用合法取得 IP Address 的權利。

## 1.2 研究目的

由於上述所提到的問題，因此本篇論文考量目前實際應用的 IP Network 環境上，所有使用 IP Address 的網路設備，基於使用者是否事先透過合法程序註冊使用者網路設備使用的 IP Address，以及使用者使用 IP Address 時，網路設備 IP Address 手動設定和動態取得的不同下，所可能產生的問題，並探討其他研究在上述問題的解決方法，期望能在不失安全性且兼具彈性的情況下，提出一套網路設備 IP Address 的管理機制，來達到下列目的：

- 可以確保每個使用者都能使用合法的 IP Address。
- 可以讓網路端完全管理所有的 Routable IP Address。
- 可以保證在網路設備使用者還沒經過網路端同意之前，不能隨意更換使用中的 IP Address。
- 可以阻止不合法的使用者進入網路使用相關服務和資源。
- 當使用者事先透過合法程序註冊使用者網路設備使用的 IP Address 時，可以保證使用者無論使用手動設定或動態取得 IP Address 的方式，都可以使用已經註冊的 IP Address。
- 可以保障網路設備使用者能正常使用合法取得的 IP Address。
- 當使用者沒有事先透過合法程序註冊使用者網路設備使用的 IP Address，卻手動設定使用 IP Address 時，如果該 IP Address 目前沒有使用者使用，且沒有事先註冊給其他使用者使用，則可以保障使用者能正常使用該手動設定的 IP Address。

- 當使用者沒有事先透過合法程序註冊使用者網路設備使用的 IP Address，可以保障使用者能透過動態取得 IP Address 的方式，取得合法能使用的 IP Address。

## 1.3 章節簡介

- 第一章 緒論  
簡介本篇論文的研究動機及目的
- 第二章 背景知識及相關議題介紹  
相關背景知識介紹以及研究議題探討
- 第三章 相關研究  
介紹相關領域的研究概況
- 第四章 確保合法使用 IP 位址之 IP 管理機制  
闡述本篇論文所提出的 IP 管理機制。
- 第五章 確保合法使用 IP 位址之 IP 管理機制的設計與實作  
描述實作網路環境、參數設定，以及各個網路設備的流程與運作機制。
- 第六章 結論與未來工作  
結論、本篇論文的總結以及未來可進行的研究方向。





## 第二章 背景知識及相關議題介紹

在現今 IP Network 的環境下，MAC Address 可以輕易的被偽造，使得非法使用者可以濫用網路上的服務和資源，以及造成網路環境的混亂，因此安全性會是一個很重要的考量，在本章節會介紹現有的認證機制，透過對使用者的認證，並且綁定該使用者正在使用的網路設備，來確認使用者的合法性。

另外，在 IP Network 上的 IP Address 的管理也是一個很重要的議題，有效的 IP Address 管理可保障合法使用者使用 IP Address 的權利，同時也可以避免非法者冒用合法者的 IP Address 和 MAC Address，在本章節會介紹目前 IP Network 上最常被使用的動態 IP Address 管理機制 - Dynamic Host Configuration Protocol (DHCP)，透過動態取得 IP Address 的方式，來分配可使用的 IP Address 給網路設備使用，達到 IP Address 的基本管理。

### 2.1 User Authentication



在這個章節裡，我們將先介紹一些目前存在使用者認證機制的背景知識，最主要是為了要確認使用者身份的合法性，並且綁定該使用者正在使用的網路設備。

#### 2.1.1 Web Login + RADIUS

這一節我們要先介紹 Web Login + Remote Authentication Dial In User Service (RADIUS)[2] 的認證機制，如 Figure 2-1 所顯示，一開始使用者先連到某個特定的 Web Server，輸入使用者的帳號和密碼後，系統會將使用者的帳號和密碼讀取，利用 RADIUS protocol 傳送給 RADIUS Server 做身份認證，以確定使用者身

份的合法性，而 RADIUS Server 同樣會將認證結果使用 RADIUS protocol 回傳給 Web Server，Web Server 則根據回傳結果對該使用者作相對應的行為，來達成使用者身份的認證機制，以下針對 RADIUS protocol 作介紹：

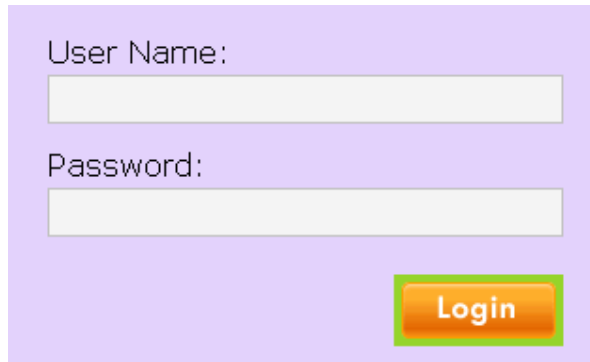
A screenshot of a web login form. The form has a light purple background. It contains two text input fields: the first is labeled "User Name:" and the second is labeled "Password:". Below the password field is a green "Login" button with a yellow border.

Figure 2-1 Web Login for User Authenticator

### 2.1.1.1 RADIUS 簡介

RADIUS 定義在 RFC2865[2]、RFC2866[3] 中，是一種在網路接入(network entrance)設備和認證伺服器(authentication server)間承載認證(authentication)、授權(authorization)、計費(accounting)和配置信息的協議，使用 User Datagram Protocol (UDP)[4] 為傳輸協定，認證授權 Port 為 1812、計費 Port 為 1813，目前為認證、授權、計費方面應用最廣泛的協議之一，具以下特點：

- **使用 Client/Server 架構:** Network Access Server (NAS, 網路連結伺服器) 為 RADIUS Server 的 Client，主要負責將用戶的訊息傳遞給 RADIUS Server，並回覆用戶取得的相關信息，而 RADIUS Server 則負責認證及回傳所有必要的訊息。
- **具備網路安全:** 採用共享密鑰(Shared Secret Key)保證網路傳輸安全性，Client/Server 各自先設定相同的密鑰，因此密鑰不會在網路上傳輸，

且 Client/Server 間的封包發送都需要進行加密過程。

- **良好的可擴展性:** 所有的屬性值都是由不同長度的【屬性—長度—值】構成，因此新的屬性值的加入不會影響到原有協議的執行。

### 2.1.1.2 RADIUS 封包格式

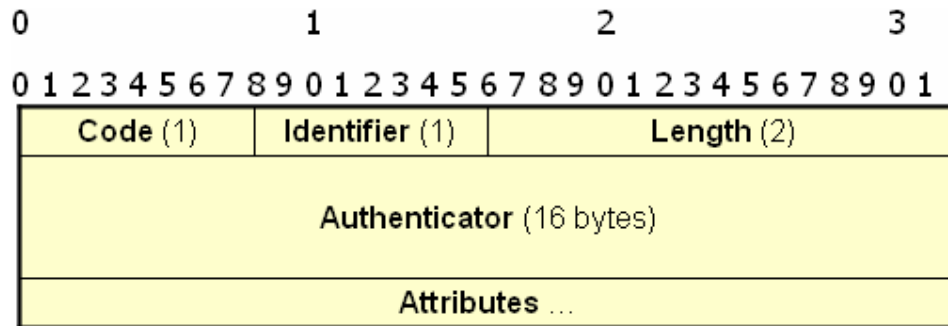


Figure 2-2 RADIUS Packet Format

RADIUS 的封包格式如 Figure 2-2 所示，各欄位定義分別介紹如下：

- **Code:** 長度為 1 個位元組，用於標明 RADIUS 的類型。
  - **1: Access-Request**，NAS 用來跟 Radius Server 認證使用者之用。
  - **2: Access-Accept**，表示該使用者通過認證，為合法使用者。
  - **3: Access-Reject**，表示該使用者沒通過認證，不為合法使用者。
  - **11: Access-Challenge**，Radius Server 用來跟 RADIUS Client 要求進行認證。
- **Identifier:** 長度為 1 個位元組，用於輔助 Server/Client 間傳送的封包。
- **Length:** 長度為 2 個位元組，用來表示封包的長度。
- **Authenticator:** 長度為 16 個位元組，用於認證 Server 和 Client 之間訊

息的有效性。

- **Attributes:** 長度是可變的，它是多個由【Type, Length, Value】組成的屬性所形成的，以下列出常用的 Type。[5]
  - **1:** User-Name, Length 為  $\geq 3$ , 表示用戶名稱。
  - **2:** User-Password, Length 為 18-130, 表示用戶密碼。
  - **4:** NAS-IP-Address, Length 為 6, 表示 NAS IP Address。
  - **8:** Framed-IP-Address, Length 為 6, 表示用戶 IP Address。
  - **18:** Reply-Message, Length 為  $\geq 3$ , 表示回覆 RADIUS Client 訊息。
  - **26:** Vendor-Specific, Length 為  $\geq 7$ , 提供給廠商擴充之用。

### 2.1.1.3 RADIUS 工作原理

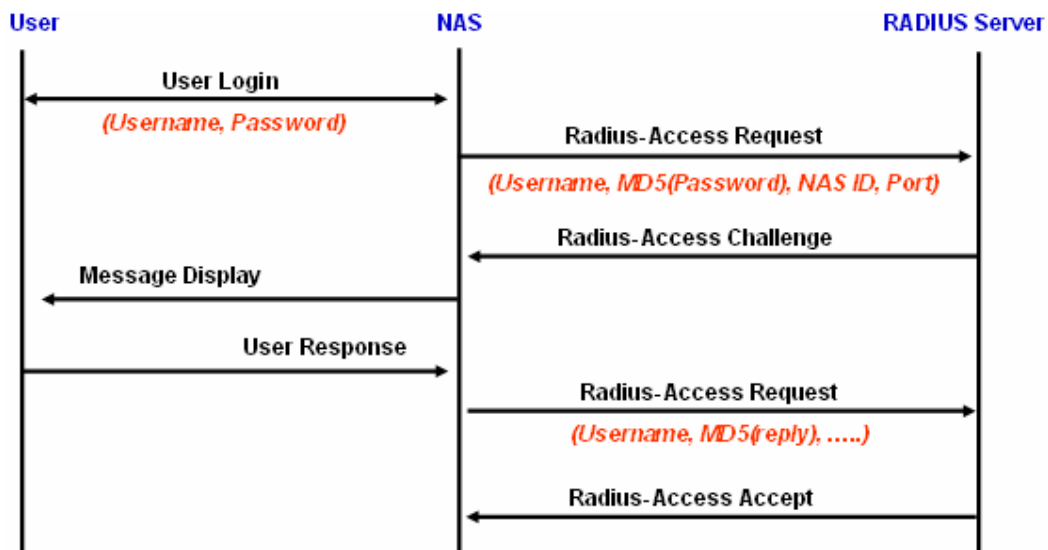


Figure 2-3 RADIUS Authentication Flow

Figure 2-3 所示為 RADIUS Authentication Flow，使用者撥接到提供 RADIUS 用戶端的 NAS，NAS 會從使用者收集到使用者的帳號和密碼，然後使用 UDP/IP 傳送加密過的 Access-Request 給 RADIUS 伺服器。這個 Message 包含一些屬性，例如 Username、Message-Digest algorithm 5 (MD5)[6] 過的 Password、NAS port ID

和 IP Address 等。RADIUS Server 會去檢查本身資料庫內是否有這個使用者的資料，如果沒有符合的資料，則 RADIUS Server 會回傳 Access-Reject 給 NAS，並且可能會在此 Message 中，利用 Type18 的 Reply-Message 將認證失敗的原因回傳給 NAS。NAS 收到後會通知使用者認證失敗。如果 RADIUS Server 有找到這個使用者的資料而且密碼正確，RADIUS Server 會傳回 Access-Accept 給 NAS，連同其它完成連線所需要的額外設定資料，如分配給使用者的 IP Address 等，一起傳回給 NAS。[7]

## 2.1.2 IEEE 802.1X

IEEE 802.1X[8] 是一個認證協定，定義了網路連接埠的接入控制 (Port-Based Network Access Control)，連接埠可以是一個物理埠，也可以是一個邏輯埠，例如 Virtual Local Area Network (VLAN)[9]，主要是以使用者帳號或使用者設備為基礎之網路連接埠認證標準。IEEE 802.1X 認證的最終目的就是確認網路使用者是否有權使用網路，對於網路連接埠來說，如果使用者認證成功，則表示開啟此連接埠，允許所有的封包通過；如果使用者認證失敗，則表示關閉此連接埠，除了 IEEE 802.1X 的認證封包 Extensible Authentication Protocol over LAN (EAPOL) 通過，其他封包均封鎖。[10]

這種認證程序稱為「連接埠層級認證」(Port-Level Authentication)，利用 RADIUS 將 IEEE 802.1X 認證的網路設備區分成三種角色：Supplicant、Authenticator、以及 Authentication Server。[11]

- **Supplicant:** 即是所謂的客戶端，要求向 Authenticator 作認證，並透過 Authenticator 存取網路上服務與資源，在 Supplicant 上必須執行 IEEE 802.1X 客戶端程式，如 Microsoft Windows XP 等。[12]

- **Authenticator:** 即是根據 Supplicant 的認證狀態來決定該 Supplicant 是否有權利存取網路上服務與資源的網路設備，位於 Supplicant 和 Authentication Server 間充當認證代理角色。Authenticator 會要求 Supplicant 提供相關資訊，再將資訊傳送給 Authentication Server 作認證，Authenticator 則根據認證結果決定該連接埠是否開啟或關閉，即對 Supplicant 的封包放行或封鎖。
- **Authentication Server:** 對 Supplicant 進行實際認證，並通知 Authenticator 是否允許該 Supplicant 存取網路上服務與資源的網路設備。Authentication Server 接受 Authenticator 傳送的認證需求，並在對 Supplicant 認證完成後，將結果回傳給 Authenticator，以達到對網路連接埠的管理。

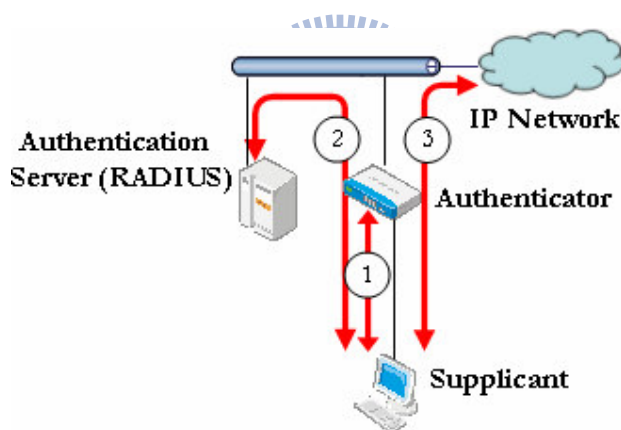


Figure 2-4 IEEE 802.1X Authentication Flow

Figure 2-4 所示為一般 IEEE 802.1X Authentication Flow，當 Supplicant 連接到 Authenticator 時 (①)，Authenticator 會要求 Supplicant 提供認證資料，並將這些認證資料，轉傳給 Authentication Server 做認證 (②)，如果認證成功，則 Authenticator 會允許 Supplicant 透過 Authenticator 使用網路上的資源 (③)，否則會封鎖 Supplicant 的 traffic，使其無法透過 Authenticator 到達網路。

為了要提供 IEEE 802.1X 的標準驗證機制，因此 IEEE 選擇了「可延伸驗證通訊協定」(EAP, Extensible Authentication Protocol)[13]。EAP 是一種「點對點通訊協定」(PPP, Point-to-Point Protocol)[14] 架構的驗證技術，通常使用於點對點的網路區段上。由於 EAP 訊息原來是定義作為 PPP 傳輸資料中的有效傳輸單元，所以 IEEE 802.1X 定義了區域網路上的 EAP (EAPOL, EAP over LAN) 技術，這是一種經過封裝程序的 EAP 訊息，以便在乙太網路或無線區域網路上傳送的方法。

### 2.1.2.1 EAP 封包格式

IEEE 802.1X 使用 EAP 在認證過程中交換資訊，主要用來在 PPP 中提供額外的認證機制，以提供遠端登入的認證機制。EAP 的封包格式如 Figure 2-5 所示，各欄位定義分別介紹如下：[15]

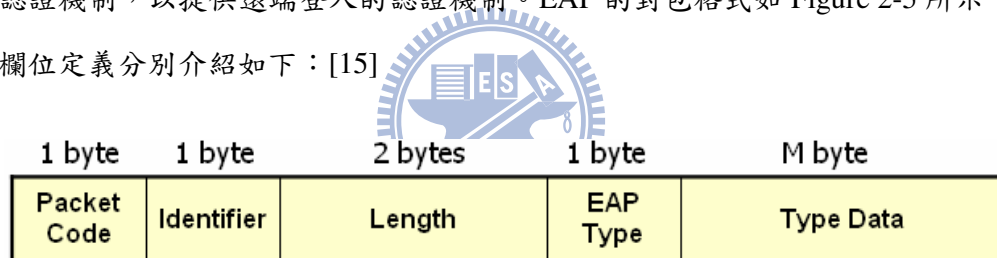


Figure 2-5 EAP Packet Format

- **Packet Code:** 長度為 1 個位元組，用於標明 EAP 封包的類型。
  - **1:** 表示為 EAP Request。
  - **2:** 表示為 EAP Response。
  - **3:** 表示為 EAP Success。
  - **4:** 表示為 EAP Failure。
- **Identifier:** 長度為 1 個位元組，用於輔助 Request/Response 間傳送的封包。

- **Length:** 長度為 2 個位元組，用於表示 EAP 封包的長度。
- **EAP Type:** 長度為 1 個位元組，一個 EAP 封包只會包含一個 EAP Type，共有以下七種類型：
  - **0x01:** Identity。
  - **0x02:** Notification。
  - **0x03:** Nak (Response Only)。
  - **0x04:** MD5-Challenge。
  - **0x05:** One-Time Password (OTP)。
  - **0x06:** Generic Token Card。
  - **0x07:** Transport Level Security (TLS)。

## 2.1.2.2 EAPOL 封包格式

EAPOL 是屬於網路協定中 IP 層以下的通訊協定，主要定義在 IEEE 802.1X 的 7.6 節中，目的是讓使用者在未經過 EAP 認證以前的封包，可以透過 EAPOL 的傳送，經由 Authenticator 與後端認證伺服器進行認證。Supplicant 尚未認證前只有 EAPOL 的封包可以通過 Authenticator，因此 Authenticator 會去檢查封包的 Ethernet Type 欄位，如果為 0x888E，表示此為 EAPOL 的封包，就會放行通過，其他類型的封包則會封鎖。EAPOL 的封包格式如 Figure 2-6 所示，各欄位定義分別介紹如下：[15]

1 byte	1 byte	2 bytes	N byte
Protocol Version	Packet Type	Packet Body Length	Packet Body

Figure 2-6 EAPOL Packet Format



- **Protocol Version:** 長度為 1 個位元組，表示協定版本，在 IEEE 802.1X 中，此欄位的值為 0x01。
- **Packet Type:** 長度為 1 個位元組，用來確認 EAPOL 封包是夾帶 EAP 封包，或用來進行一般 EAPOL 的程序，有下列幾類：
  - **0x00:** EAP-Packet，表示用來夾帶 EAP 資料的封包，Packet Body Length 是包含後面 Packet Body 資料長度，而 Packet Body 為所夾帶的 EAP 封包內容。
  - **0x01:** EAPOL-Start，表示 EAPOL 開始的封包，不會夾帶 EAP 的資料，Packet Length 為 0。
  - **0x02:** EAPOL-LogOff，表示 EAPOL 登出環境的封包，不會夾帶 EAP 的資料，Packet Length 為 0。
  - **0x03:** EAPOL- Key，表示 EAPOL 交換 Key 使用的封包，不會夾帶 EAP 的資料，Packet Length 為 0。
- **Packet Body Length:** 長度為 2 個位元組，表示 Packet Body 資料長度，當 Packet Type 不為 0x00 時，Packet Length 為 0。
- **Packet Body:** 長度不定，當 Packet Type 為 0x00 時，表示夾帶 EAP 的資料。

### 2.1.2.3 IEEE 802.1X 工作原理

基於 IEEE 802.1X 的認證協定，Supplicant 和 Authenticator 之間使用 EAPOL 格式封裝 EAP 協定傳送認證的資訊，Authenticator 與 Authentication Server 之間通過 RADIUS 協定傳送認證資訊。由於 EAP 協定的可擴展性，使用 EAP 協定的

認證系統可以使用多種不同的認證演算法，如 EAP-MD5、EAP-TLS[16]、EAP-TTLS[17] 以及 EAP-AKA[18] 等認證方法。

EAP-MD5 是一種單向認證機制，可以完成網路對用戶的認證，但認證過程不支援加密密鑰的生成。Figure 2-7 所示為以 EAP-MD5 為例的認證流程，認證流程如下：

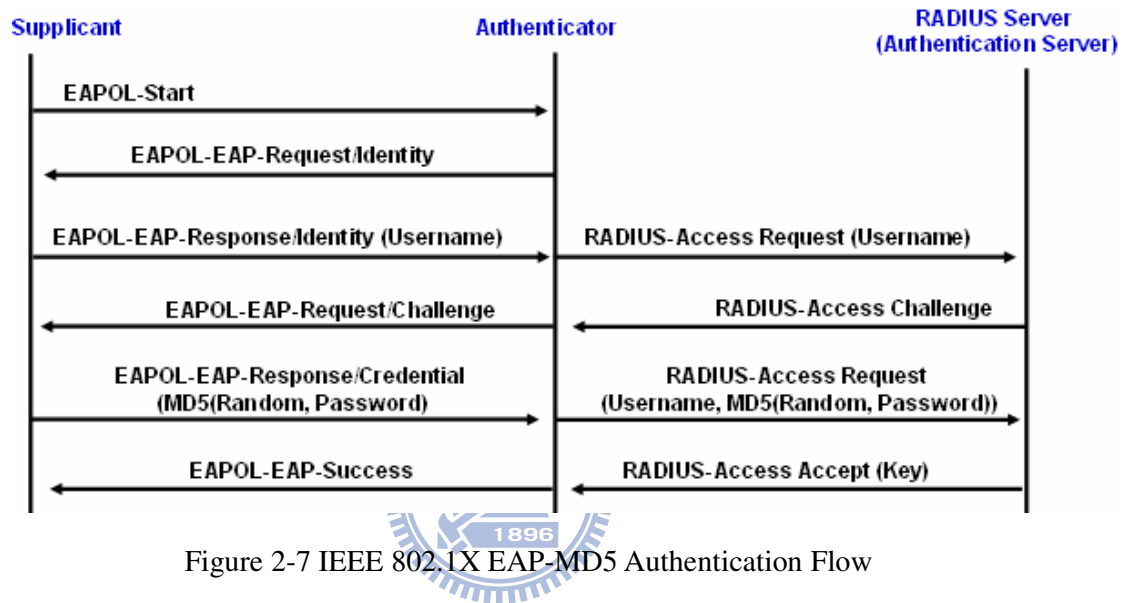


Figure 2-7 IEEE 802.1X EAP-MD5 Authentication Flow

- Supplicant 向 Authenticator 發送 EAPOL-Start 封包，開始 IEEE 802.1X 認證機制。
- Authenticator 向 Supplicant 發送 EAPOL-EAP-Request/Identity 封包，要求 Supplicant 傳送 Username 給 Authenticator。
- Supplicant 將 Username 包含在 EAPOL-EAP-Response/Identity 封包中，回傳給 Authenticator 的請求。
- Authenticator 將 EAPOL-EAP-Response/Identity 封包封裝到 RADIUS Access-Request 封包中，發送給 Authentication Server。

- Authentication Server 會產生一個 Challenge，將包含 EAP-Request/MD5-Challenge 的 RADIUS Access-Challenge 封包回傳給 Authenticator。
- Authenticator 將 EAPOL-EAP-Request/MD5-Challenge 封包發送給 Supplicant，要求 Supplicant 進行認證。
- Supplicant 收到 EAPOL-EAP-Request/MD5-Challenge 封包後，將密碼和收到的 Challenge 做 MD5 演算法，並把所得到的 Challenged-Password 放到 EAPoL-EAP-Response/MD5-Challenge 封包中回傳給 Authenticator。
- Authenticator 將 Challenge、Challenged Password 和 Username，利用 RADIUS Access-Request 封包 送到 Authentication Server，由 Authentication Server 進行認證。
- Authentication Server 根據取得的資訊，做 MD5 演算法，判斷 Supplicant 是否合法，然後回應 RADIUS Access-Accept 或 RADIUS Access-Reject 封包到 Authenticator。
- Authenticator 根據 Authentication Server 回傳的封包內容，發送 EAPOL-EAP Success 或 EAPOL-EAP Failure 給 Supplicant，並對該連接埠開啟或關閉，以及提供相對應的設定與網路服務。

### 2.1.3 IEEE 802.11i

IEEE 802.11i[19] 是一種無線網路上新一代的安全標準，定義了 Robust Security Network (RSN) 的概念。RSN 是目前公認最安全的架構，包含了使用者認證和資料加密傳輸，認證部分主要透過原本 IEEE 802.1X 所定義的 EAPOL 封包格式傳送上層 EAP 認證程序封包；資料加密傳輸部分則以 Temporal Key

Integrity Protocol (TKIP) 和 Advanced Encryption Standard (AES) 作為加密的方法，使用 IEEE 802.11i 新訂定不同於 IEEE 802.1X 之 EAPOL-Key 封包格式，進行加解密金鑰的交換程序 (4-Way Pairwise-Key Handshaking and Two-Way Group-Key Handshaking)。

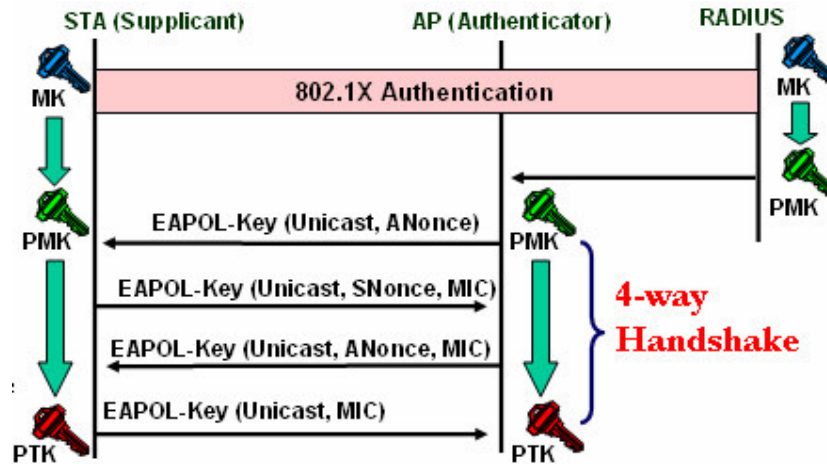


Figure 2-8 IEEE 802.11i Authentication Flow

Figure 2-8 所示為 IEEE 802.11i Authentication Flow，當 STA 作完 IEEE 802.1X 的認證後，STA 和 AP 會有一把共同的 Pairwise Master Key (PMK)，透過 4-way handshake 的方式，產生 Pairwise Transient Key Security Association (PTKSA)，PTKSA 包含有 Pairwise Transient Key (PTK)、STA MAC Address、AP MAC Address 等資訊，因此對於 STA 和 AP 來說，PTKSA 是連結彼此唯一的憑證。

## 2.2 Dynamic Host Configuration Protocol (DHCP)

在 IP Network 中，每個連接上的網路設備都需要使用唯一的 IP Address，當 IP Address 的數量不敷使用，透過 Dynamic Host Configuration Protocol (DHCP，動態主機設定協定)[1] 的機制可以動態的分配 IP Address 給網路上的網路設

備，使得 IP Address 的運用更有彈性，它主要分為兩種角色：一個是伺服器端 (DHCP Server)，另一個是客戶端(DHCP Client)。DHCP Server 主要負責所有 IP Network 上網路設備設定資料的集中管理，並負責處理 DHCP Client 的 DHCP 要求；DHCP Client 則透過 DHCP 要求，取得並使用從 DHCP Server 分配下來的 IP 環境資料，並且透過“租約”的運用，可使 DHCP Server 能更有效且動態的分配 DHCP Client 的 網路組態設定。

## 2.2.1 DHCP Server Behavior

DHCP Server 可能收到下列五種封包，分別說明如下：

- **DHCP DISCOVER:** 當 DHCP Client 第一次登錄網路的時候，也就是發現本機上並沒有被配置 IP Address 的時候，用來取得 IP Address 使用。
- **DHCP REQUEST:** 可能來自於回應 DHCP OFFER 的 DHCP Client，或是第一次登入之後欲重新取得 IP 的 DHCP Client。
- **DHCP DECLINE:** 當 DHCP Client 發現 DHCP Server 所提供的 IP Address 已經為其他的機器所使用，會主動使用此封包來拒絕 DHCP Server 的 DHCP OFFER，並重新發送 DHCP DISCOVER 取得其他可使用的 IP Address。
- **DHCP RELEASE:** 若 IP Address 的租約尚未到期，而 DHCP Client 已不再使用此 IP Address，則 DHCP Client 可以送出此封包通知 DHCP Server，如此 DHCP Server 才可以再將此 IP Address 配置給其他的使用者使用。
- **DHCP INFORM:** 當 DHCP Server 收到此封包時，會將必要的參數放進

Option 欄位中，並以 Unicast 的方式回應 DHCP ACK 給 DHCP Client。

## 2.2.2 DHCP Client Behavior

DHCP Client 可能收到下列三種封包，分別說明如下：

- **DHCP OFFER:** DHCP Server 以 Unicast 的方式回覆 DHCP Client 的 DHCP DISCOVER 封包，包含 IP Address 等網路設定。
- **DHCP ACK:** 當 DHCP Server 接收到 DHCP Client 的 DHCP REQUEST 或 DHCP INFORM 之後，若封包中 Server Identifier 與自己的 IP Address 相同，會回應此封包給 DHCP Client。
- **DHCP NACK:** 表示 DHCP Server 拒絕 DHCP Client 的請求，Client 可以重新發送 DHCP DISCOVER 取得 IP Address。[20]

## 2.2.3 DHCP 封包格式

DHCP 的封包格式如 Figure 2-9 所示，各欄位定義分別介紹如下：

- **op:** 長度為 1 個位元組，若為 DHCP Client 送給 DHCP Server 的封包，設為 1，反向為 2。
- **htype:** 長度為 1 個位元組，表示硬體類別，Ethernet 為 1。
- **hlen:** 長度為 1 個位元組，表示硬體位址長度，Ethernet 為 6。
- **hops:** 長度為 1 個位元組，若封包需經過網路設備傳送，每經過一個網路設備則 hops 會被加 1，若在同一個網域內，則為 0。

- **xid:** 長度為 4 個位元組，DHCP REQUEST 時產生的數值，用來作 DHCP REPLY 時的依據。

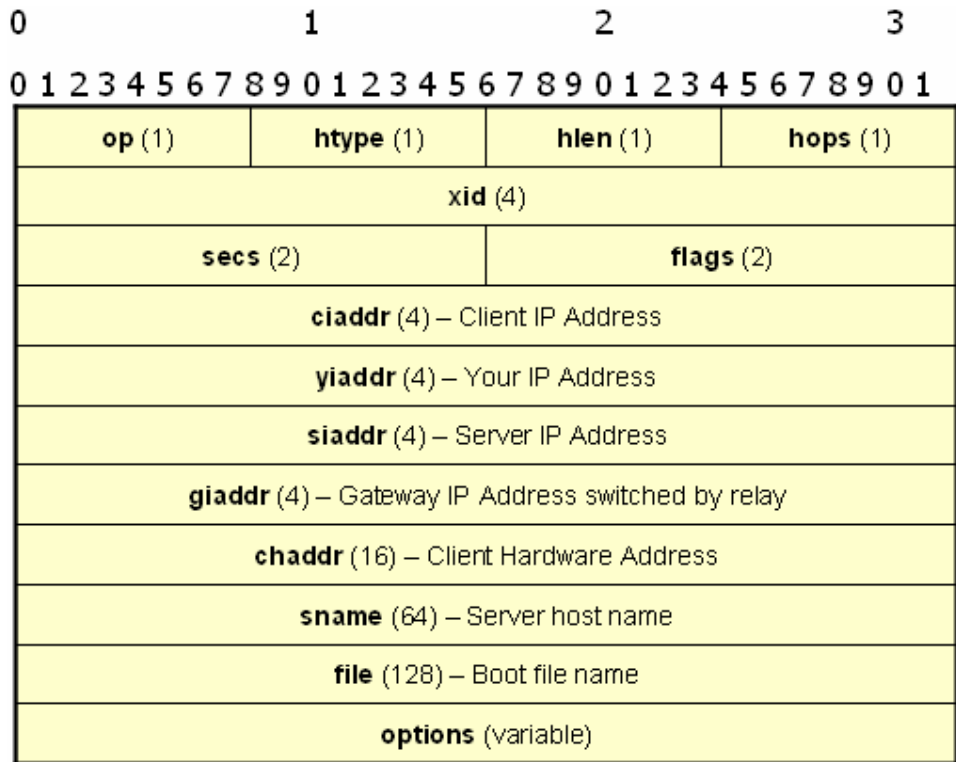


Figure 2-9 DHCP Packet Format

- **flags:** 長度為 2 個位元組，最左邊的 bit 為 1 時，表示 DHCP Server 將以 Broadcast 方式傳送封包給 DHCP Client，其餘尚未使用。
- **ciaddr:** 長度為 4 個位元組，為 DHCP Client 想繼續使用之前取得的 IP Address。
- **yiaddr:** 長度為 4 個位元組，為 DHCP Server 在回傳給 DHCP Client 的 DHCP OFFER 與 DHCP ACK 封包中，填寫分配給 DHCP Client 的 IP Address。
- **siaddr:** 長度為 4 個位元組，若 DHCP Client 需透過網路開機，在 DHCP

Server 傳送的 DHCP OFFER、DHCPACK 和 DHCP NACK 封包中，填寫開機程式碼所在 Server 的 IP Address。

- **giaddr:** 長度為 4 個位元組，若需跨網域進行 DHCP 的發放，則填寫 Relay Agent 的 IP Address，否則為 0。
- **chaddr:** 長度為 16 個位元組，為 DHCP Client 的硬體位址 (MAC Address)。
- **sname:** 長度為 64 個位元組，為 DHCP Server 的名稱字串，以 0x00 結尾。
- **file:** 長度為 128 個位元組，若 DHCP Client 需要透過網路開機，則填寫開機程式名稱，稍後以 Trivial File Transfer Protocol (TFTP)[21] 傳送。
- **options:** 長度不定，允許廠商定義選項 (Vendor-Specific Area)，以提供更多設定資訊 (如：Netmask、Gateway、DNS 等)。

## 2.2.4 DHCP 工作原理

Figure 2-10 所顯示的是 DHCP 的封包流程，因為 DHCP Client 是否為第一次登入會影響到 DHCP 的運作，故分別於下列兩點論述。

- 當 DHCP Client 第一次登入 DHCP Server 時:
  - 當 DHCP Client 為第一次登入時，發現本機上並沒有被配置 IP Address，此時 DHCP Client 會以 Broadcast 的方式發送 DHCP DISCOVER 封包來找尋網域中的 DHCP Server。
  - 網域中所有的 DHCP Server 都會收到 DHCP Client 所發送的 DHCP DISCOVER，DHCP Server 會在 DHCP OFFER 封包中包含所有需



要告知 DHCP Client 的訊息 (例如：IP Address 等等)，並以 Unicast 的方式回傳給 DHCP Client。

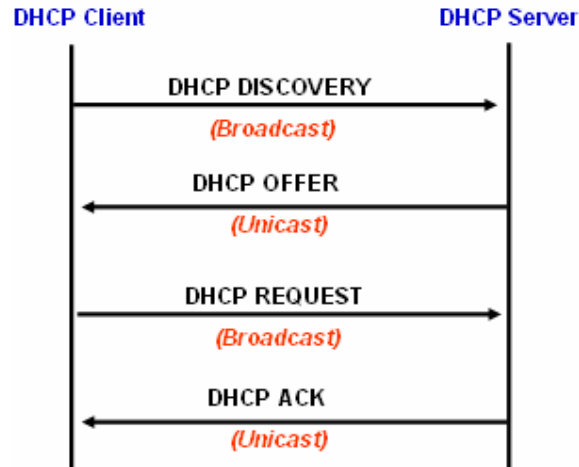
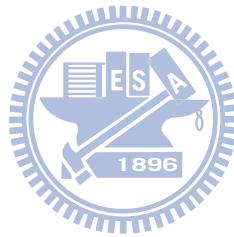


Figure 2-10 DHCP Packet Flow

- 若 DHCP Client 在一段時間後收到一個以上的 DHCP Server 所回應的 DHCP OFFER，則 DHCP Client 會從中選定一個 DHCP Server，將 DHCP Server IP Address 填入 DHCP REQUEST 封包中的 Server Identifier，再以 Broadcast 的方式將其發送出去。
  - 網域中的 DHCP Server 收到 DHCP Client 回應的 DHCP REQUEST 封包時，只有封包中 Server Identifier 與自己的 IP Address 相同的 DHCP Server，才會回應 DHCP ACK 給 DHCP Client。此 DHCP ACK 封包中所包含的訊息應與 DHCP OFFER 中的相同。
  - 當 DHCP Client 收到 DHCP ACK 時，即表示此 DHCP Client 已被配置一個 IP Address，並將封包中的各個資料作設定，完成一個完整的 DHCP 工作過程。
- 當 DHCP Client 第一次登入 DHCP Server 後：

- 當 DHCP Client 在第一次登入後，若想取得之前曾獲得的 IP Address 時，可以以 Unicast 的方式發送 DHCP REQUEST，並將想取得的 IP Address 填入 Request IP Address 欄位中，DHCP Server IP Address 填入 Server Identifier 中。
- 收到 DHCP REQUEST 的 DHCP Server，可以依據 DHCP Client 的請求回應 DHCP ACK 或 DHCP NAK。

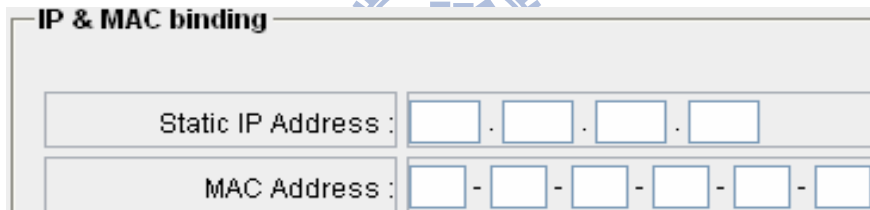


## 第三章 相關研究

### 3.1 研究背景

在現今 IP Network 的環境應用越來越普及，每個網路設備主要是使用 IP Address 來當成唯一識別的 ID，因此當在同一個網域中，同時存在兩個以上的網路設備使用相同的 IP Address 時，會導致有 IP Address 互相衝突的問題發生，而造成相同 IP Address 的網路設備無法順利使用網路上的服務和資源。因此目前針對上述問題已經有一些作法提出，期望能透過 IP 管理的機制，來預防類似的情形發生，分別在以下列出討論。

### 3.2 IP/MAC Binding on DHCP Server



The image shows a configuration window titled "IP & MAC binding". It contains two input fields: "Static IP Address" and "MAC Address". The "Static IP Address" field is a dotted decimal format with four empty boxes separated by dots. The "MAC Address" field is a hexadecimal format with six empty boxes separated by hyphens. A blue arc with arrows is positioned above the "Static IP Address" field.

Figure 3-1 IP/MAC Address Binding (引自[22])

Figure 3-1 所顯示為 IP/MAC Address Binding，主要是利用 IP Address 和 MAC Address 的對應關係，來限制網路設備只能固定使用設定好的 IP Address，並禁止網路設備任意更換 IP Address，透過這種 IP 管理的機制，來達到網路上預防 IP Address 互相衝突的問題發生。

由於 DHCP Server 是動態分配 IP Address 的伺服器，因此若 IP & MAC Binding 在 DHCP Server 上執行時，DHCP Server 可以根據設定，將固定的 IP Address 分配給固定的 MAC Address，提供管理者對連接上的網路設備作管制，而該 MAC

Address 的網路設備透過動態取得 IP Address 的機制，只會得到相同的 IP Address，以達成預防 IP Address 互相衝突，而造成網路環境混亂的問題發生。

此方法在現有網路環境的缺點：

- 不夠有彈性。必須先註冊要使用的網路設備 MAC Address，以及可使用的 IP Address，否則無法使用。
- 網路設備使用者只能使用動態取得 IP Address 的方式，否則無法取得正確的 IP Address，進而無法使用網路上的服務和資源，造成使用者的困擾和不便。
- 必須要限制網路設備使用者不能使用手動設定 IP Address 的機制。如果沒有作限制，或是 Switch/AP 沒有對於手動設定 IP Address 的機制做處理，則因為 IP Address 互相衝突，而造成網路環境混亂的問題仍然有可能會發生。
- 安全性不夠。只要冒用 MAC Address 並使用動態取得 IP Address 的方式，即可取得 IP/MAC Address Binding rule 的合法 IP Address，進而使用網路上的服務和資源。



### 3.3 IP/MAC Binding on Switch or AP

如同 Figure 3-1 所顯示，由於 Switch/AP 是 Supplicant 連上網路時，會連接到  
的網路設備，因此若 IP & MAC Binding 在 Switch/AP 上執行時，Switch/AP 可以  
提供管理者對連接上的網路設備作管制，將固定的 IP Address 對應給固定的 MAC  
Address，該 MAC Address 的網路設備只能使用固定的 IP Address 連上  
Switch/AP，確認後再透過 Switch/AP 使用網路上的服務和資源；當該 MAC

Address 的網路設備不是使用設定在 Switch/AP 上的固定 IP Address 時，則 Switch/AP 會把該網路設備封鎖，以達成因為 IP Address 互相衝突，而造成網路環境混亂的問題發生。

此方法在現有網路環境的缺點：

- 不夠有彈性。必須先設定好要使用的網路設備 MAC Address，以及可使用的 IP Address，否則無法使用。
- 網路設備使用者只能使用手動設定 IP Address 的方式，如果設定有錯誤，或是使用者忘記自己的 IP Address，則會無法使用網路上的服務和資源，造成使用者的困擾和不便。
- 安全性不夠。在現今 IP Address 和 MAC Address 很容易就被冒用的情況下，只對 IP Address 和 MAC Address 作對應，雖然對預防 IP Address 互相衝突的問題發生有效果，但卻無法真正保障合法使用者使用網路上的服務和資源的權利。



### 3.4 NCTU Dormitory Network Management System

Figure 3-2 所顯示為交通大學的宿舍網路管理辦法[23] 中，使用者 IP Address 的申請流程，使用者一開始進入宿網申請網頁，使用學號和密碼當作帳號，申請登記宿網 IP Address，在申請頁面上輸入使用者所使用的宿舍網路孔，以及使用的網路設備 MAC Address，之後選擇要使用的網路區段，以及選擇要註冊使用的 IP Address，即完成宿舍網路註冊程序。

之後再將申請之 IP Address 手動設定到使用者使用的網路設備上，並輸入子網路遮罩 (Netmask)、預設閘道 (Gateway) 與位址解析伺服器 (Domain Name

Server, DNS) 等相關資訊，即可利用此 IP Address 使用宿舍網路。

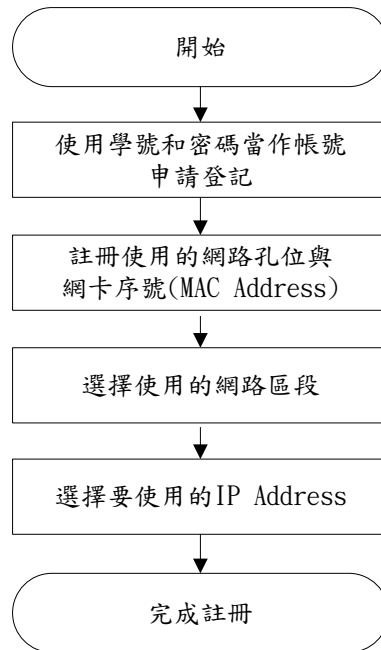


Figure 3-2 NCTU Dormitory Network IP Address Apply Flow

此方法在現有網路環境的缺點:

- 不夠有彈性。使用者必須要利用使用者的網路設備和要使用的網路孔，事先註冊一組 IP Address 使用，此 IP Address 只能利用使用者註冊的網路設備在註冊的網路孔使用，無法透過註冊的 IP Address 和 MAC Address，在任何地方都能使用；另外使用者必須手動設定 IP Address，如果設定有錯誤或變更，或是使用者忘記自己的 IP Address，則會無法使用網路上的服務和資源，造成使用者的困擾和不便。
- 必須要限制使用者不能使用動態取得 IP Address 的機制。如果沒有限制，或是 Switch/AP 沒有對動態取得 IP Address 的機制做處理，則因為 IP Address 互相衝突，而造成網路環境混亂的問題仍然有可能會發生。

- 安全性不夠。在現今 IP Address 和 MAC Address 很容易就被冒用的情況下，只對 IP Address 和 MAC Address 作對應，雖然對預防 IP Address 互相衝突的問題發生有效果，但卻無法保障真正合法使用者使用網路上的服務和資源的權利。

### 3.5 IEEE 802.1X with IP Address Management

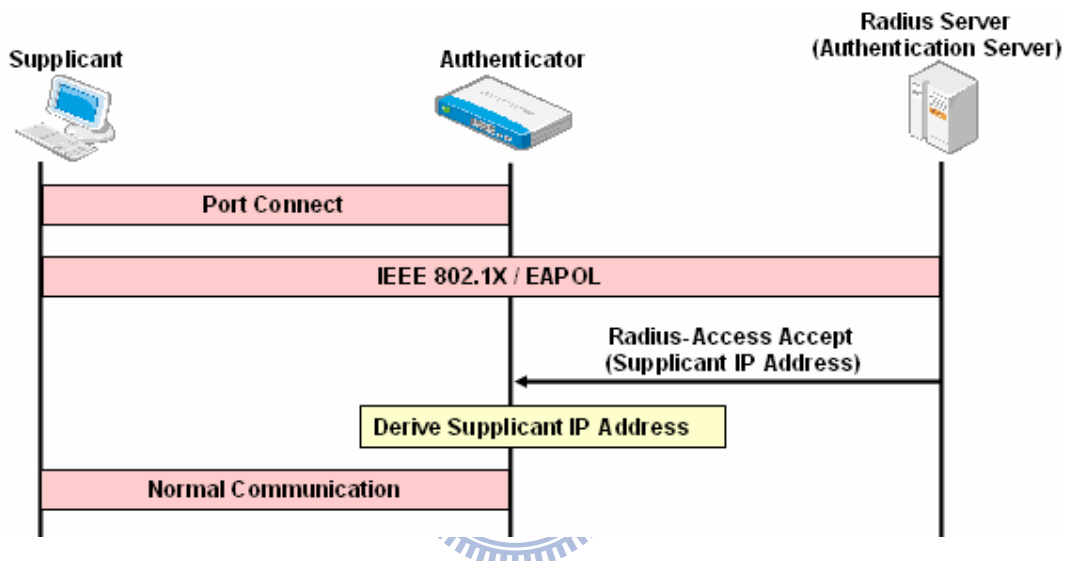


Figure 3-3 IEEE 802.1X with IP Address Management Scheme

Figure 3-3 所顯示為 IEEE 802.1X with IP Address Management Scheme，在 Supplicant 使用者使用網路資源前，必須要先執行 IEEE 802.1X 的認證程序，當認證通過之後，Radius Server 會將 Supplicant 使用者合法可以使用的 IP Address，利用 Radius Protocol 的 Access Accept 訊息傳送給 Authenticator，而 Authenticator 則會利用此 IP Address 來判斷 Supplicant 所使用的 IP Address 是否合法，來決定放行或封鎖 Supplicant 的封包。[7]

此方法在現有網路環境的缺點：

- 不夠有彈性。Supplicant 使用者必須要事先註冊使用的 IP Address，並且

Supplicant 使用者只能使用手動設定 IP Address，如果設定有錯誤，或是使用者忘記自己的 IP Address，則會無法使用網路上的服務和資源，造成使用者的困擾和不便。

### 3.6 自動化宿舍網路註冊管理系統

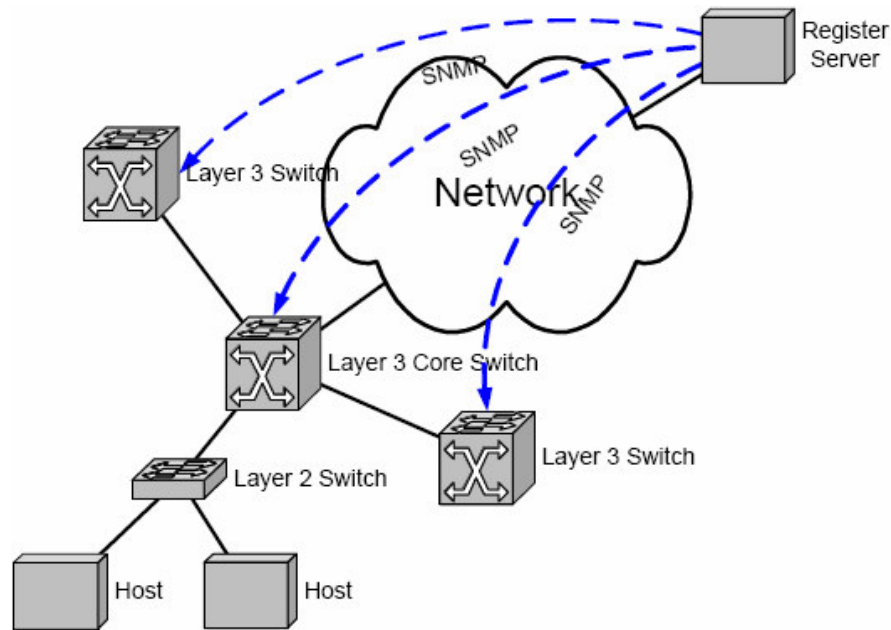


Figure 3-4 自動化宿舍網路註冊管理系統 (引自[24])

此機制為其他文章所提出的自動化宿舍網路註冊管理系統，在一開始註冊階段，網路設備使用者先使用 DHCP 機制取得一組未認證的 IP Address，確認此 IP Address 為宿舍網路內的 IP Address 後，利用此 IP Address 和使用者使用的網路設備 MAC Address，以及網路設備使用者個人資料，去取得一個註冊的 IP Address，成功之後如 Figure 3-4 所示，會將該 IP Address 和 MAC Address 透過 Simple Network Management Protocol (SNMP)寫入 Layer 3 Switch，並在 Layer 3 Switch 上利用 Access Control List (ACL)做管控，沒註冊的使用者只允許連接到註冊伺服器，而 IP Address 和 MAC Address 兩者都符合的網路設備使用者則能使用網路的



服務和資源。

此方法在現有網路環境的缺點:

- 不夠有彈性。網路設備使用者除了要事先註冊使用的 IP Address，而且網路設備使用者只能使用手動設定 IP Address，如果設定有錯誤，或是使用者忘記自己的 IP Address，則會無法使用網路上的服務和資源，造成使用者的困擾和不便。
- 網路設備使用者使用動態 機制取得的 IP Address，只能暫時使用來註冊，無法透過動態取得 IP Address 的機制，即取得可以使用網路上服務和資源的 IP Address。
- 安全性不夠。雖然註冊階段有使用網路設備使用者的個人資料和使用的網路設備 MAC Address 作安全性的認證，但註冊後只針對 IP Address 和 MAC Address 做比對，只要冒用 IP Address 和 MAC Address 即可使用網路上的服務和資源。



### 3.7 總結

總結本節所述，雖然上述所提出的方法上各有特點，在特定的情境和限制下，也可以預防在同一網域上，網路設備的 IP Address 互相衝突，而造成網路環境混亂的問題發生，但在使用上多所限制，不夠彈性，無法同時支援網路設備使用者使用手動設定 IP Address 和動態取得 IP Address，容易造成使用者使用上的困擾和不便；再者安全性不夠，大部分方法多透過 IP Address 和 MAC Address 的對應關係，來達到期望的目的，但卻忽略在現今的網路環境下，IP Address 和 MAC Address 的冒用是很容易即可以做到，以至於網路上的服務和資源被濫用，對使

用者使用網路的權利造成影響。



## 第四章 確保合法使用 IP 位址之 IP 管理機制

### 4.1 簡介

綜合前面章節的介紹，目前雖然有一些作法，但我們可以發現每種 IP 管理機制均無法同時滿足以下的情況：

- 同時支援使用者使用手動設定或動態的方式取得 IP Address。
- 同時支援使用者使用已經事先註冊的 IP Address，或自己手動設定沒有衝突的 IP Address，來使用網路服務與資源時。
- 確保使用者事先註冊的 IP Address 不會被冒用。

因此本論文希望能達到以下目的：

- 確保 IP Address 能合法的被使用：
  - 保障合法的 IP Address 使用者不會有 IP Address 衝突的問題發生。
  - 管理所有的 IP Address，對於非法的使用者進行封鎖。
- 提供彈性的使用 IP Address
  - 可同時支援使用者使用手動設定或動態的方式取得 IP Address。
  - 可同時支援使用者使用已經事先註冊的 IP Address，或自己手動設定沒有衝突的 IP Address，來使用網路服務與資源時。

因此我們提出下列機制，來達到我們所期望的目的：

- **Table-based IP management mechanism**

透過在 Authenticator 和 IP Management Server 上建立 Table，來確保無論是使用者事先註冊的 IP Address，或是利用動態取得的 IP Address，均能合法的被使用。

■ **Supplicant State Table:** 在 Authenticator 上建立 Supplicant State Table，用來對連接到 Authenticator 的 Supplicant 的合法性和行為進行管控。

■ **IP Address Assignment Table:** 在 IP Management Server 上建立 IP Address Assignment Table，主要目的是用來對連接到 Authenticator 的 Supplicant 作 IP Address 的分配與管理。

- **Dynamic IP assignment mechanism**

透過 Dynamic IP assignment 的機制，Authenticator 和 IP Management Server 之間利用 IP Management Protocol 做溝通，來達到彈性使用 IP Address 的目的。



Figure 4-1 所顯示的為本論文方法的 concept overview，當 Supplicant 連接到 Authenticator 時，會自動在 Authenticator 上會建立 Supplicant State Table，用來管控連接到 Authenticator 的 Supplicant 的合法性和行為；在 IP Management Server 上會事先建立 IP Address Assignment Table，主要目的是用來對連接到 Authenticator 的 Supplicant 作 IP Address 的分配與管理，當 Supplicant 透過 Authenticator 跟 Authentication Server 做認證時，Authenticator 會從中取得 Supplicant 的 User Account，當認證成功之後，會將此 User Account 放到 IP Management Protocol 中使用，用以連結使用者以及使用者所使用的網路設備，達到保障合法使用者使用網路的權利。

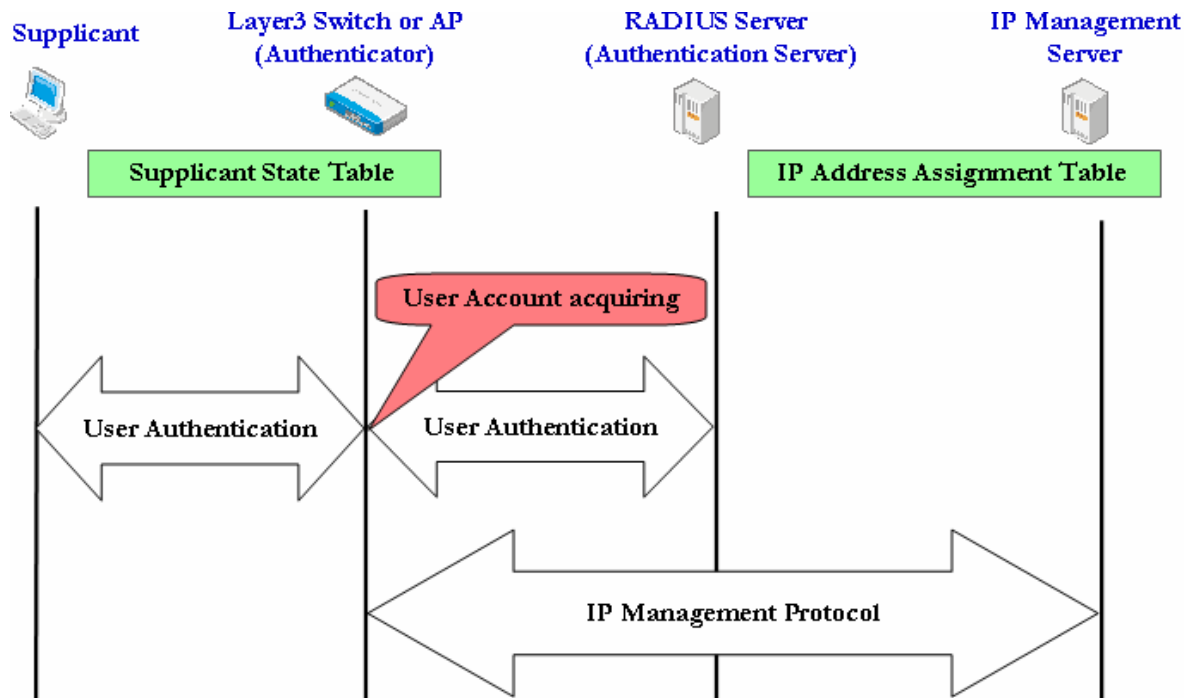


Figure 4-1 IP Management Scheme concept overview

### 4.1.1 Supplicant State Table

User Account	IP Address	MAC Address	Port	Status
User1		MAC_1	Port1	Auth
User2	IP_2	MAC_2	Port2	Static
User3	IP_3	MAC_3	PTKSA1	Dynamic

Figure 4-2 Supplicant State Table on Authenticator

為了能管控所有連接到 Authenticator 的 Supplicant 的合法性和行為，因此在 Authenticator 上需要建立一個相對應的表格，記錄 Supplicant 的資訊和狀態，以提供 Authenticator 判斷和管理 Supplicant，這個表格在 Supplicant 連上 Authenticator 時候會自動建立。

Figure 4-2 所顯示的為 Authenticator 上的 Supplicant Status Table，相關欄位說明如下：

- **User Account:**

Table 中的欄位 User Account 記錄 Supplicant 的 User Account，用來傳送給 IP Management Server 作確認之用，此欄位為當 Supplicant 作 User Authentication 時記錄到 Table 中。

- **IP Address:**

Table 中的欄位 IP Address 記錄 Supplicant 的 IP Address，用來對 Supplicant 是否可連接到網路作基本的判斷確認，此欄位為當 IP Management Server 回傳 Supplicant 合法的 IP Address 時記錄。

- **MAC Address:**

Table 中的欄位 MAC Address 記錄 Supplicant 的 MAC Address，用來對 Supplicant 是否可連接到網路作基本的判斷確認，此欄位為當 Supplicant 連接上 Authenticator 時即會記錄。

- **Port:**

本論文提出的方法，除可使用在有線網路的環境下，同樣也可以使用在無線網路的環境，但由於無線網路沒有實際的 Port 連接，因此為了增加安全性，預防不合法 Supplicant 使用者進入網路端，在無線網路的環境下，會記錄 Pairwise Transient Key Security Association (PTKSA)，來對 Supplicant 進行管控。如果 Supplicant 連接上 Authenticator 的網路環境為 Wired，則會在 Port 欄位記錄 Supplicant 連接上 Authenticator 的 Port Number; 如果網路環境為 Wireless，則會在 Port 欄位記錄 Supplicant 和 Authenticator 經過 Four Way Handshake 之後所得到的 PTKSA，此欄位最主要的功能為增加安全性，預防不合法 Supplicant 使用者進入網路端。

- **Status:**



■ Table 中的欄位 Status 則用來記錄連接的 Supplicant 目前狀態，以方便判斷和管理 Supplicant，並決定 Supplicant 的封包是否放行或封鎖，共有以下幾種 Status：

◆ **Connected:** 此狀態為 Supplicant 連接上 Authenticator，但尚未經過身分驗證，此時該 Supplicant 尚無法經由 Authenticator 使用網路上的資源。

◆ **Auth:** 此狀態為 Supplicant 連接上 Authenticator 後已經經過身分驗證成功，但尚未取得合法 IP Address，此時該 Supplicant 尚無法經由 Authenticator 使用網路上的資源。

◆ **Static:** 此狀態為 Supplicant 使用 Static IP Address 連接上 Authenticator 後已經經過身分驗證成功，並且確認使用的 IP Address 為該 Supplicant 合法可使用的 IP Address。

◆ **Dynamic:** 此狀態為 Supplicant 連接上 Authenticator 後已經經過身分驗證成功，並且使用動態機制取得該 Supplicant 合法可使用的 IP Address。

## 4.1.2 IP Address Assignment Table

為了能對所有連接到 Authenticator 的 Supplicant 作 IP Address 的分配與管理，因此在 IP Management Server 上需要事先建立一個相對應的表格，記錄 Supplicant 取得 IP Address 的資訊和連接狀態，以提供 IP Management Server 在分配與管理 IP Address 時的判斷。

IP Address Assignment Table 中的記錄可分為 static 和 dynamic 兩種情況，static 即是指 Supplicant 使用者透過合法程序註冊使用的 IP Address，會事先將該資訊

記錄在 Table 中，而 dynamic 則是指其餘未註冊使用的 IP Address 的 Supplicant 使用者，會等到使用動態機制的方式取得合法可用 IP Address 時，才會將該資訊記錄在 Table 中。

User Account	IP Address	MAC Address	Status
User1	IP_1		Inactive
User2	IP_2	MAC_2	Subscribed
.....			
User3	IP_3	MAC_3	Non-Subscribed
User2	IP_D	MAC_D	Non-Subscribed

Figure 4-3 IP Address Assignment Table on IP Management Server

Figure 4-3 所顯示的為 IP Management Server 上的 IP Address Assignment Table，相關欄位說明如下：

- **User Account:**

Table 中的欄位 User Account 記錄使用者透過合法程序註冊的帳號，此帳號需與使用者在 Authentication Server 註冊的帳號相同，用來對 Supplicant 使用者是否有註冊使用的 IP Address 作基本的判斷確認;或是記錄未註冊使用的 IP Address 的 Supplicant 使用者的帳號。

- **IP Address:**

Table 中的欄位 IP Address 記錄 Supplicant 使用者透過合法程序註冊使用的 IP Address，用來對 Supplicant 使用者是否有註冊使用的 IP Address 作基本的判斷確認;或是記錄未註冊使用的 IP Address 的 Supplicant 使用者，所分配到的 IP Address。

- **MAC Address:**

Table 中的欄位 MAC Address 記錄使用者在使用 IP Address 時 Supplicant



的 MAC Address。

- **Status:**

- Table 中的欄位 Status 則用來記錄 Supplicant 使用者取得 IP Address 的方式和目前的狀態，用來方便管理 Supplicant 使用者的 IP Address，以及 Supplicant 使用者在 IP Address Release 時，判斷是否保留該記錄之用，若該記錄為使用者透過合法程序註冊使用，則保留該記錄；若為使用者透過動態機制向 IP Management Server 取得的動態 IP Address，則刪除該記錄。共有以下幾種 Status：

- ◆ **Inactive:** 此狀態當此記錄為 static，即 Supplicant 使用者已經透過合法程序註冊使用的 IP Address，但尚未連接上 Authenticator。

- ◆ **Subscribed:** 此狀態當此記錄為 static，即 Supplicant 使用者已經透過合法程序註冊使用的 IP Address，已經連接上 Authenticator 且取得該 IP Address 使用中。

- ◆ **Non-Subscribed:** 此狀態當此記錄為 dynamic，即 Supplicant 使用者沒有註冊使用的 IP Address，但透過動態的機制向 IP Management Server 取得合法可以使用的 IP Address。

### 4.1.3 Dynamic IP Assignment Mechanism

在 Dynamic IP Assignment Mechanism 中，本論文利用延伸 DHCP Message Format 作為 Authenticator 和 IP Management Server 之間的 IP Management Protocol 來做探討，在此 DHCP Server 即為 IP Management Server。

Figure 4-4 所顯示的為利用延伸 DHCP Message Format 來做到 IP Management

Protocol，當要執行 IP Management Protocol 之前，User Account 必須已經認證成功，且 Authenticator 已經將 User Account 記錄到 Supplicant State Table 中。

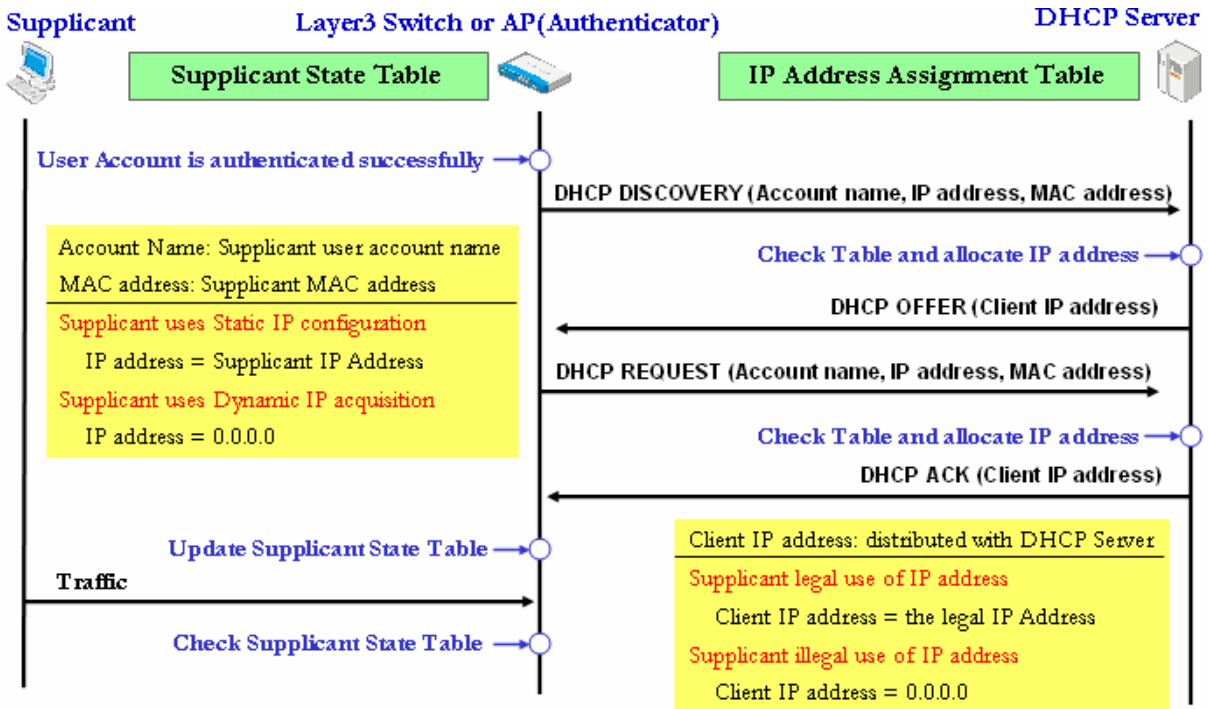


Figure 4-4 IP Management Protocol with Extended DHCP Scheme

當 Supplicant 連接到 Authenticator 時，即會在 Authenticator 的 Supplicant Status Table 上建立 Supplicant 的 MAC Address 等相關資料，並且如果 Supplicant 連接上 Authenticator 的網路環境為 Wired，則會在 Port 欄位記錄 Supplicant 連接上 Authenticator 的 Port Number; 如果網路環境為 Wireless，則會在 Port 欄位記錄 Supplicant 和 Authenticator 經過 4-Way Handshake 之後所得到的 PTKSA。

在 User 身分認證完後，此時 Authenticator 已經可以確認 Supplicant 使用者的身分是否合法，若不合法，將對該 Supplicant 使用者作封鎖；若合法則 Authenticator 會將 Supplicant 使用者帳號記錄下來，並在之後將該帳號加入要傳送給 DHCP Server 的 DHCP Message 中。

在判斷使用者使用的是 Static IP Address configuration 或是 Dynamic IP Address acquisition 上，Authenticator 是以收到 Supplicant 封包為判斷基準，若收到的封包已經包含 IP Address，則認定 Supplicant 使用的是 Static IP Address configuration; 若收到的封包為 Supplicant 使用 DHCP 機制發送的 DHCP DISCOVERY 或 DHCP REQUEST，則認定 Supplicant 使用的是 Dynamic IP Address acquisition。

透過以上所得的資訊，當 Supplicant 欲透過 Authenticator 使用網路上的資源時，Authenticator 會將上述 Supplicant 所使用的 IP Address，MAC Address 和使用者帳號，利用 DHCP Message 的 DHCP DISCOVERY 或 DHCP REQUEST 傳送給 DHCP Server 作確認，若認定 Supplicant 使用的是 Static IP Address configuration，則傳送的 IP Address 會填入 Supplicant 使用的 Static IP Address; 若認定 Supplicant 使用的是 Dynamic IP Address acquisition，則傳送的 IP Address 會填入“0.0.0.0”。

DHCP Server 收到 DHCP DISCOVERY 或 DHCP REQUEST 後，會取出 IP Address，MAC Address 和使用者帳號，跟自身的 IP Address Assignment Table 做比對，並把 Supplicant 可以使用的 IP Address 傳回給 Authenticator，若 Supplicant 使用的是合法 IP Address，則傳送的 IP Address 會填入該 IP Address; 若 Supplicant 使用的是不合法 IP Address，則傳送的 IP Address 會填入“0.0.0.0”。

Authenticator 則根據 DHCP Server 所傳回 DHCP Message 中的 Client IP Address，來判斷 Supplicant 所使用的 IP Address 是否合法可用，並更新 Supplicant State Table，透過對 IP Address、MAC Address 和 Port 欄位的比對，對該 Supplicant 作相對應的管控。

## 4.1.4 Extended DHCP Message

Figure 4-5 所顯示的為延伸 DHCP Message 後的 Format，主要是利用原本定義好的“ciaddr”、“yiaddr”和“chaddr”欄位，以及自行定義在 options 的“uaname”欄位，來存放 Authenticator 和 DHCP Server 之間溝通驗證的資訊，分別介紹如下：

op (1)	htype (1)	hlen (1)	hops (1)
<b>xid (4)</b>			
<b>secs (2)</b>		<b>flags (2)</b>	
<b>ciaddr (4) – Client IP Address</b>			
<b>yiaddr (4) – Your IP Address</b>			
<b>siaddr (4) – IP Address of next server to use in bootstrap</b>			
<b>giaddr (4) – Gateway IP Address switched by relay</b>			
<b>chaddr (16) – Client Hardware Address</b>			
<b>sname (64) – Server host name</b>			
<b>file (128) – Boot file name</b>			
<b>uaname (64) – User Account name</b>			
<b>options (variable)</b>			

Figure 4-5 Extended DHCP Message Format

- **ciaddr:** 原本是用來存放 DHCP Client 想要繼續使用的 IP Address，本方法則是用來存放 Supplicant 的 IP Address。
- **yiaddr:** 原本是用來存放 DHCP Client 的要分配給 DHCP Client 使用的 IP Address，本方法則是用來存放 DHCP Server 在確認 IP Address Assignment Table 後，Supplicant 可使用的 IP Address，此欄位只會在

DHCP OFFER 和 DHCP ACK 中使用。

- **chaddr:** 原本是用來存放 DHCP Client 的 Hardware Address，本方法則是用來存放 Supplicant 的 Hardware Address。
- **uaname:** 本方法中新增的欄位，用來存放 Supplicant 的 User Account。

## 4.2 Analysis of Proposed Scheme

本章節中將逐一介紹本篇論文所提出的解決方案，並依照不同的情境，說明本方法如何利用延伸 DHCP Message Format 來達到 IP Address 的統一分配與管理，以及如何在 Authenticator 上達到對 Supplicant 的管控。情境說明如下：

- **IP Address Assignment and Access Control**

- **使用者使用 Static IP Address configuration 連上 Authenticator:**

- ◆ 使用者手動設定的 IP Address 為事先透過合法程序註冊使用的 IP Address。
- ◆ 使用者手動設定的 IP Address 不為事先透過合法程序註冊使用的 IP Address。
- ◆ 使用者手動設定的 IP Address 並沒有事先透過合法程序註冊使用，但沒有跟其他註冊或正在使用的 IP Address 衝突。
- ◆ 使用者手動設定的 IP Address 並沒有事先透過合法程序註冊使用，但跟其他註冊或正在使用的 IP Address 衝突。

- **使用者使用 Dynamic IP Address acquisition 連上 Authenticator:**

- ◆ 使用者設定 Supplicant 為使用 DHCP 機制取得 Dynamic IP Address 連上 Authenticator，並且事先已經透過合法程序註冊

使用的 IP Address。

- ◆使用者設定 Supplicant 為使用 DHCP 機制取得 Dynamic IP Address 連上 Authenticator，但事先並沒有透過合法程序註冊使用的 IP Address。

- **IP Address Releasing**

## **4.2.1 IP Address Assignment and Access Control**

使用者在連上 Authenticator 時，透過本論文方法取得 IP Address，在這種情況下，本論文根據使用者使用的是 Static IP Address configuration 或 Dynamic IP Address acquisition 來分別討論。

### **4.2.1.1 Static IP Address Configuration**

使用者在連上 Authenticator 時，手動設定 Static IP Address configuration，在這種情況下，本論文再根據該使用者是否事先透過合法程序註冊使用的 IP Address，以及手動設定的 Static IP Address 是否合法分別討論。

#### **4.2.1.1.1 Static IP Address with Pre-subscribed**

在此情境中，使用者已經事先透過合法程序註冊使用的 IP Address，並且手動設定該 IP Address 在 Supplicant 上使用。

Figure 4-6 所顯示的為 Supplicant 使用者手動設定的 IP Address，和事先註冊使用的 IP Address 相同時，整個 Message 交換的流程圖，分別說明如下：

- ① 當 Supplicant 連接到 Authenticator 時，Authenticator 會要求 Supplicant 提供認證資料，並將這些認證資料，轉傳給 Authentication Server 做認證。
- ② 在使用者身份認證完後，此時 Authenticator 已經可以確認 Supplicant 使用者的身分，當 Authenticator 收到 Supplicant 第一筆可以取得 Supplicant 的 IP Address 封包時，Authenticator 確認 Supplicant 使用者為手動設定 IP Address 使用。

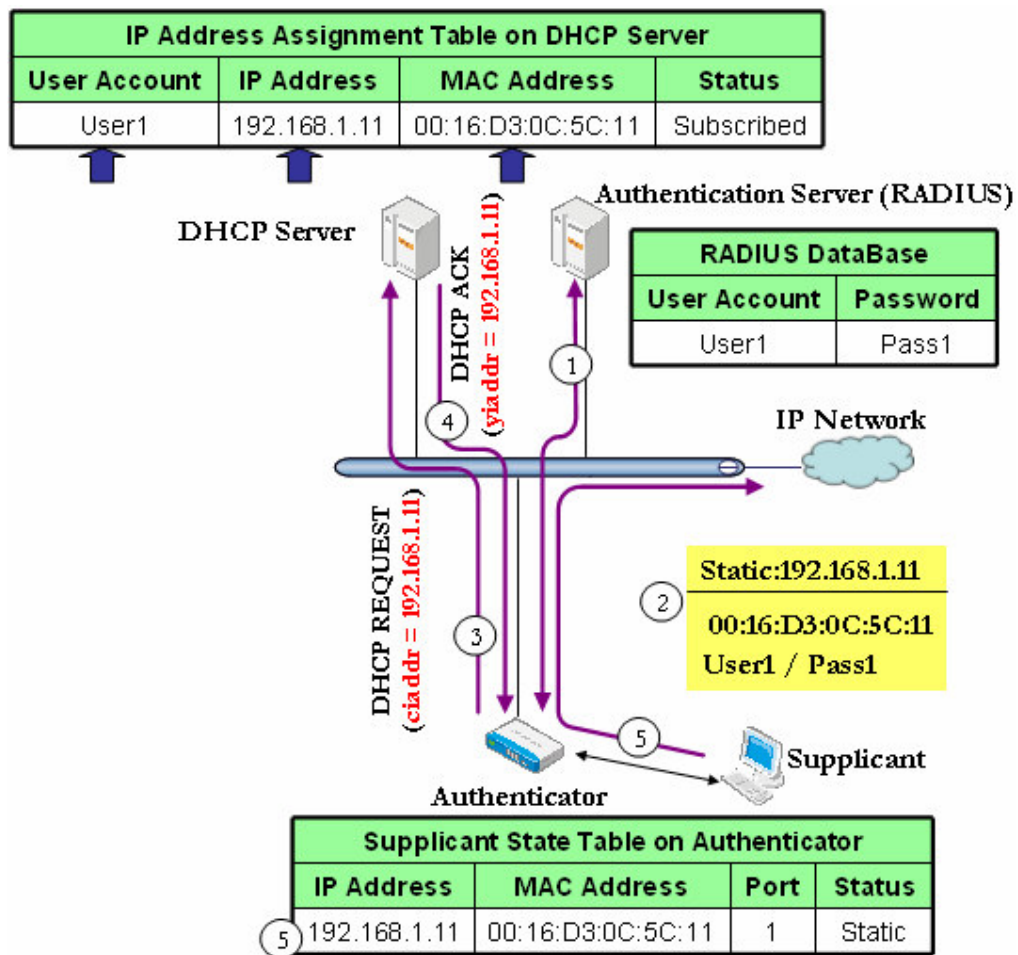


Figure 4-6 Static IP Address with Pre-subscribed IP Address

- ③ Authenticator 會發送 DHCP REQUEST 給支援本論文方法的 DHCP Server 作確認，把 Supplicant 使用的 IP Address 和 MAC Address 分別填入 DHCP

Message 的“ciaddr”和“chaddr”欄位中，並把使用者身份認證的帳號填入“uname”欄位中。

- ④ 當 DHCP Server 收到 DHCP DISCOVERY 時，DHCP Server 會從 DHCP Message 的“uname”和“chaddr”欄位取得 Supplicant 使用者使用的帳號和 MAC Address，用來跟本身的 IP Address Assignment Table 中的記錄做比對，以取得 Supplicant 使用者註冊的 IP Address，在此情境下，由於 Supplicant 使用者已經事先透過合法程序註冊使用的 IP Address，因此經由帳號的比對，從 IP Address Assignment Table 中取得 Supplicant 使用者註冊的 IP Address，會和從 DHCP Message 的“ciaddr”欄位取得的 IP Address 相同，此時 DHCP Server 會把該記錄的 Status 欄位的值更改為 Subscribed，把從“chaddr”欄位取得的 MAC Address 填入該記錄的 MAC Address 欄位，並把此 IP Address 填入 DHCP ACK 的“yiaddr”欄位後回傳給 Authenticator。
- ⑤ Authenticator 在收到 DHCP ACK 後，會將“yiaddr”欄位中的值和之前傳送 DHCP REQUEST 的“ciaddr”欄位比對是否相同，在此情境下，“yiaddr”欄位比對結果會相同，表示 Supplicant 使用者使用的 IP Address 沒有衝突，因此會將“yiaddr”欄位中的 IP Address 記錄在本身的 Supplicant State Table 中該 Supplicant 使用者的 IP Address 欄位，並且 Status 欄位設定 Static，之後會允許該 Supplicant 的 traffic 通過。

#### 4.2.1.1.2 Static IP Address without Pre-subscribed

在此情境中，使用者已經透過合法程序註冊使用的 IP Address，但是手動設定在 Supplicant 上使用的 Static IP Address 卻不是該 IP Address。



Figure 4-7 所顯示的為 Supplicant 使用者手動設定的 IP Address，和事先註冊使用的 IP Address 不相同時，整個 Message 交換的流程圖，分別說明如下：

- ① 當 Supplicant 連接到 Authenticator 時，Authenticator 會要求 Supplicant 提供認證資料，並將這些認證資料，轉傳給 Authentication Server 做認證。

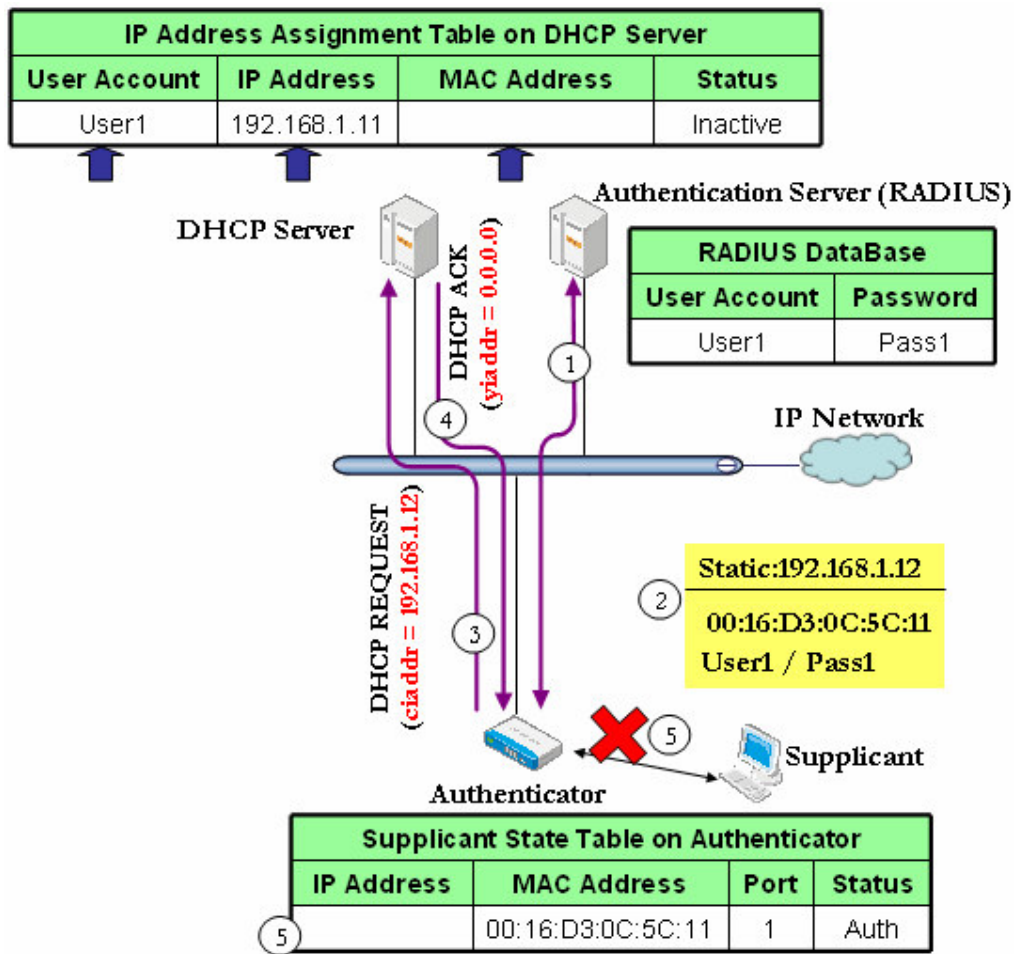


Figure 4-7 Static IP Address without Pre-subscribed IP Address

- ② 在使用者身份認證完後，此時 Authenticator 已經可以確認 Supplicant 使用者的身分，當 Authenticator 收到 Supplicant 第一筆可以取得 Supplicant 的 IP Address 封包時，Authenticator 確認 Supplicant 使用者為手動設定 IP Address 使用。

- ③ Authenticator 會發送 DHCP REQUEST 給支援本論文方法的 DHCP Server 作確認,把 Supplicant 使用的 IP Address 和 MAC Address 分別填入 DHCP Message 的“ciaddr”和“chaddr”欄位中, 並把使用者身份認證的帳號填入“uname”欄位中。
- ④ 當 DHCP Server 收到 DHCP DISCOVERY 時, DHCP Server 會從 DHCP Message 的“uname”和“chaddr”欄位取得 Supplicant 使用者使用的帳號和 MAC Address, 用來跟本身的 IP Address Assignment Table 中的記錄做比對, 以取得 Supplicant 使用者註冊的 IP Address, 在此情境下, 由於 Supplicant 使用者已經事先透過合法程序註冊使用的 IP Address, 但使用的卻不是該註冊的 IP Address, 因此經由帳號的比對, 從 IP Address Assignment Table 中取得 Supplicant 使用者註冊的 IP Address, 會和從 DHCP Message 的“ciaddr”欄位取得的 IP Address 不相同, 此時 DHCP Server 會把 0.0.0.0 填入 DHCP ACK 的“yiaddr”欄位後回傳給 Authenticator。
- ⑤ Authenticator 在收到 DHCP ACK 後, 會將“yiaddr”欄位中的值和之前傳送 DHCP REQUEST 的“ciaddr”欄位比對是否相同, 在此情境下, “yiaddr”欄位的值為 0.0.0.0, 表示 Supplicant 使用者使用的 IP Address 有衝突, 因此不會將“yiaddr”欄位中的 IP Address 記錄在本身的 Supplicant State Table 中該 Supplicant 使用者的 IP Address 欄位, 並且會對該 Supplicant 的 traffic 封鎖。

#### 4.2.1.1.3 Static conflicting IP Address with Non-subscribed

在此情境中, 使用者沒有透過合法程序註冊使用的 IP Address, 例如 guest

user，但手動設定在 Supplicant 上使用的 Static IP Address，卻和 DHCP Server 的 IP Address Assignment Table 中所記錄的 IP Address 有所衝突。

Figure 4-8 所顯示的為 Supplicant 使用者手動設定的 IP Address，和 DHCP Server 的 IP Address Assignment Table 中所記錄的 IP Address 有所衝突時，整個 Message 交換的流程圖，分別說明如下：

- ① 當 Supplicant 連接到 Authenticator 時，Authenticator 會要求 Supplicant 提供認證資料，並將這些認證資料，轉傳給 Authentication Server 做認證。

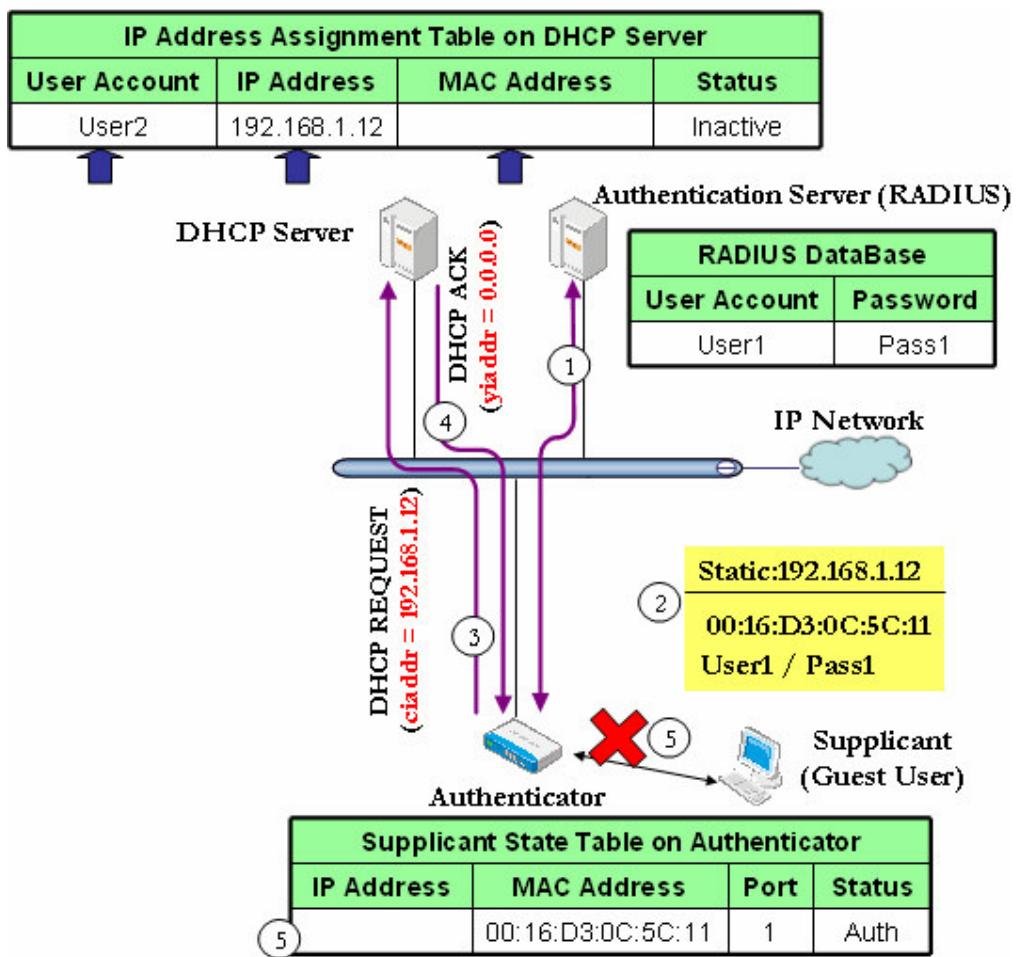


Figure 4-8 Static conflicting IP Address with Non-subscribed IP Address

- ② 在使用者身份認證完後，此時 Authenticator 已經可以確認 Supplicant 使用者的身分，當 Authenticator 收到 Supplicant 第一筆可以取得 Supplicant 的 IP Address 封包時，Authenticator 確認 Supplicant 使用者為手動設定 IP Address 使用。
- ③ Authenticator 會發送 DHCP REQUEST 給支援本論文方法的 DHCP Server 作確認，把 Supplicant 使用的 IP Address 和 MAC Address 分別填入 DHCP Message 的“ciaddr”和“chaddr”欄位中，並把使用者身份認證的帳號填入“uname”欄位中。
- ④ 當 DHCP Server 收到 DHCP DISCOVERY 時，DHCP Server 會從 DHCP Message 的“uname”和“chaddr”欄位取得 Supplicant 使用者使用的帳號和 MAC Address，用來跟本身的 IP Address Assignment Table 中的記錄做比對，以取得 Supplicant 使用者註冊的 IP Address，在此情境下，由於 Supplicant 使用者沒有透過合法程序註冊使用的 IP Address，無法經由帳號的比對，從本身 IP Address Assignment Table 中的記錄取得使用者註冊的 IP Address，因此會從 DHCP Message 的“ciaddr”欄位取得 Supplicant 使用者使用的 IP Address，和所有已經註冊使用的 IP Address，以及其他目前正在使用的 IP Address 做比對，由於 Supplicant 使用者使用的 IP Address 和其他使用者使用的 IP Address 發現衝突，因此 DHCP Server 會把 0.0.0.0 填入 DHCP ACK 的“yiaddr”欄位後回傳給 Authenticator。
- ⑤ Authenticator 在收到 DHCP ACK 後，會將“yiaddr”欄位中的值和之前傳送 DHCP REQUEST 的“ciaddr”欄位比對是否相同，在此情境下，“yiaddr”欄位的值為 0.0.0.0，表示 Supplicant 使用者使用的 IP Address 有衝突，因此不會將“yiaddr”欄位中的 IP Address 記錄在本身的 Supplicant State Table 中該 Supplicant 使用者的 IP Address 欄位，並且會對該 Supplicant 的 traffic

封鎖。

#### 4.2.1.1.4 Static Non-conflicting IP Address with Non-subscribed

在此情境中，使用者沒有透過合法程序註冊使用的 IP Address，例如 guest user，手動設定在 Supplicant 上使用的 Static IP Address，沒有和 DHCP Server 的 IP Address Assignment Table 中所記錄的 IP Address 有所衝突。

Figure 4-9 所顯示的為 Supplicant 使用者手動設定的 IP Address，沒有和 DHCP Server 的 IP Address Assignment Table 中所記錄的 IP Address 有所衝突時，整個 Message 交換的流程圖，分別說明如下：

- ① 當 Supplicant 連接到 Authenticator 時，Authenticator 會要求 Supplicant 提供認證資料，並將這些認證資料，轉傳給 Authentication Server 做認證。
- ② 在使用者身份認證完後，此時 Authenticator 已經可以確認 Supplicant 使用者的身分，當 Authenticator 收到 Supplicant 第一筆可以取得 Supplicant 的 IP Address 封包時，Authenticator 確認 Supplicant 使用者為手動設定 IP Address 使用。
- ③ Authenticator 會發送 DHCP REQUEST 給支援本論文方法的 DHCP Server 作確認，把 Supplicant 使用的 IP Address 和 MAC Address 分別填入 DHCP Message 的“ciaddr”和“chaddr”欄位中，並把使用者身份認證的帳號填入“uname”欄位中。

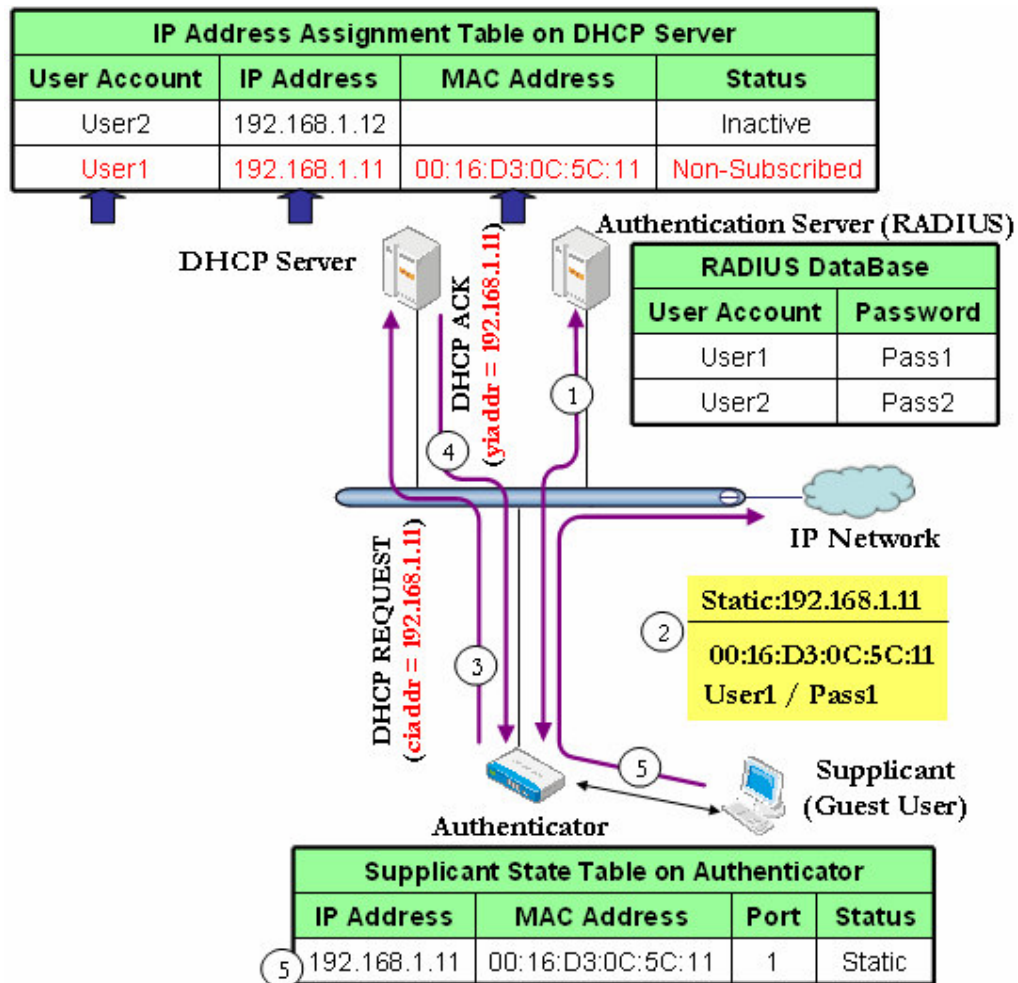


Figure 4-9 Static Non-conflicting IP Address with Non-subscribed IP Address

- ④ 當 DHCP Server 收到 DHCP DISCOVERY 時，DHCP Server 會從 DHCP Message 的“uname”和“chaddr”欄位取得 Supplicant 使用者使用的帳號和 MAC Address，用來跟本身的 IP Address Assignment Table 中的記錄做比對，以取得 Supplicant 使用者註冊的 IP Address，在此情境下，由於 Supplicant 使用者沒有透過合法程序註冊使用的 IP Address，無法經由帳號的比對，從本身 IP Address Assignment Table 中的記錄取得使用者註冊的 IP Address，因此會從 DHCP Message 的“ciaddr”欄位取得 Supplicant

使用者使用的 IP Address，和所有已經註冊使用的 IP Address，以及其他目前正在使用的 IP Address 做比對，由於 Supplicant 使用者使用的 IP Address 沒有和其他使用者使用的 IP Address 發現衝突，因此 DHCP Server 會把此 Supplicant 的 User Account，IP Address 和 MAC Address 資訊新增記錄到本身的 Table 中，並且將此記錄的 Status 欄位設定為 Non-Subscribed，之後 DHCP Server 會將從 DHCP Message 的“ciaddr”欄位取得 Supplicant 使用者使用的 IP Address，填入 DHCP ACK 的“yiaddr”欄位後回傳給 Authenticator。

- ⑤ Authenticator 在收到 DHCP ACK 後，會將“yiaddr”欄位中的值和之前傳送 DHCP REQUEST 的“ciaddr”欄位比對是否相同，在此情境下，“yiaddr”欄位比對結果會相同，表示 Supplicant 使用者使用的 IP Address 沒有衝突，因此會將“yiaddr”欄位中的 IP Address 記錄在本身的 Supplicant State Table 中該 Supplicant 使用者的 IP Address 欄位，並且 Status 欄位設定 Static，之後會允許該 Supplicant 的 traffic 通過。

## 4.2.1.2 Dynamic IP Address Acquisition

使用者在連上 Authenticator 時，設定使用 DHCP 機制取得 Dynamic IP Address，在這種情況下，本論文根據該使用者是否事先透過合法程序註冊使用的 IP Address 分別討論。

### 4.2.1.2.1 Pre-subscribed IP Address

在此情境中，使用者已經透過合法程序註冊使用的 IP Address，並且設定使用 DHCP 機制取得 Dynamic IP Address 在 Supplicant 上使用。



Figure 4-10 所顯示的為 Supplicant 使用者設定使用 DHCP 機制取得透過合法程序註冊使用的 IP Address 時，整個 Message 交換的流程圖，分別說明如下：

- ① 當 Supplicant 連接到 Authenticator 時，Authenticator 會要求 Supplicant 提供認證資料，並將這些認證資料，轉傳給 Authentication Server 做認證。

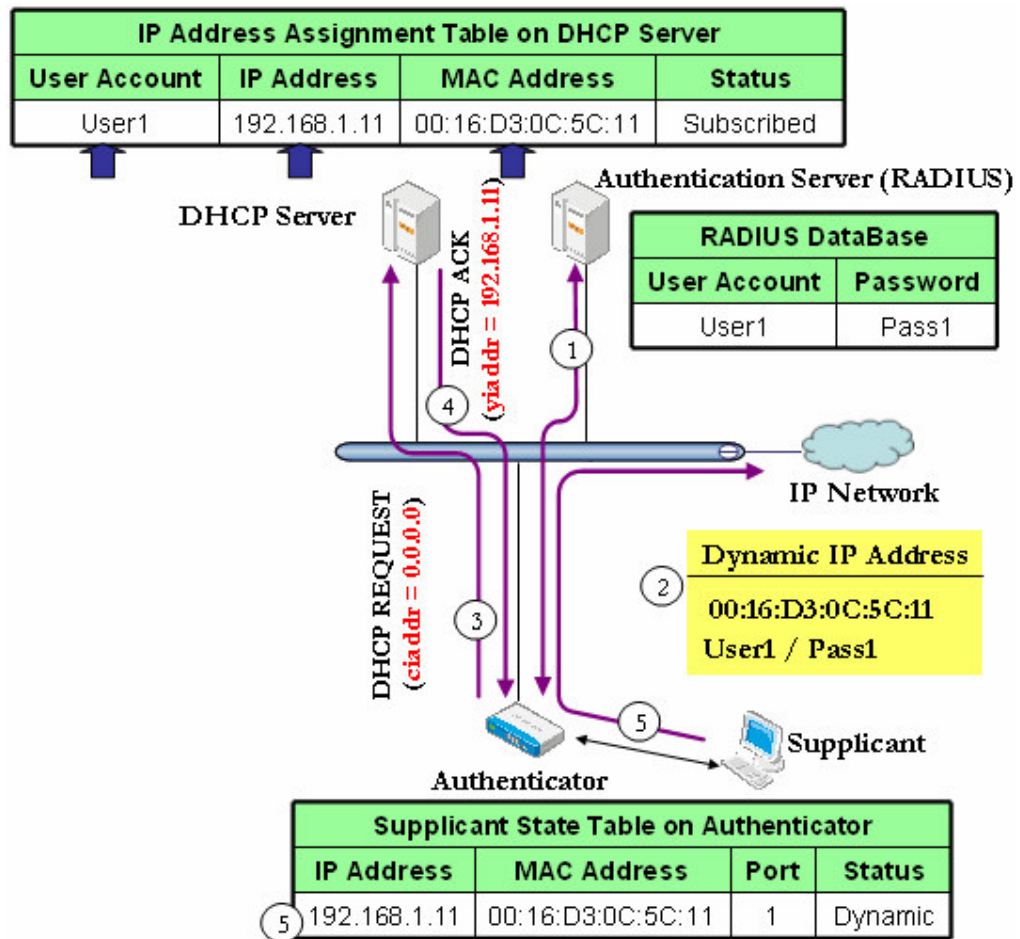


Figure 4-10 User acquires subscribed IP Address with Dynamic IP Address Acquisition

- ② 在使用者身份認證完後，此時 Authenticator 已經可以確認 Supplicant 使用者的身分，由於 Supplicant 使用者設定使用 DHCP 機制取得 Dynamic IP Address，因此當 Authenticator 收到 Supplicant 發出的 DHCP DISCOVERY



封包時, Authenticator 確認 Supplicant 使用者為動態取得 IP Address 使用。

- ③ Authenticator 會發送 DHCP REQUEST 給支援本論文方法的 DHCP Server 作確認, 把 Supplicant 使用的 MAC Address 填入 DHCP Message 的“chaddr”欄位中, 並把使用者身份認證的帳號填入“uname”欄位中, 並把“ciaddr”欄位填入 0.0.0.0, 表示 Supplicant 使用者使用的是 DHCP 機制。
- ④ 當 DHCP Server 收到 DHCP DISCOVERY 時, DHCP Server 會從 DHCP Message 的“uname”和“chaddr”欄位取得 Supplicant 使用者使用的帳號和 MAC Address, 用來跟本身的 IP Address Assignment Table 中的記錄做比對, 以取得 Supplicant 使用者註冊的 IP Address, 在此情境下, 由於 Supplicant 使用者已經事先透過合法程序註冊使用的 IP Address, 因此經由帳號的比對, 從 IP Address Assignment Table 中取得 Supplicant 使用者註冊的 IP Address, 由於 DHCP Message 的“ciaddr”欄位設定為 0.0.0.0, 因此 DHCP Server 會把該記錄的 Status 欄位的值更改為 Subscribed, 把從“chaddr”欄位取得的 MAC Address 填入該記錄的 MAC Address 欄位, 並把從 Table 中取得 Supplicant 使用者註冊的 IP Address 填入 DHCP ACK 的“yiaddr”欄位後回傳給 Authenticator。
- ⑤ Authenticator 在收到 DHCP ACK 後, 會將“yiaddr”欄位中的值和之前傳送 DHCP REQUEST 的“ciaddr”欄位比對是否相同, 在此情境下, 由於 Supplicant 使用者使用的是 DHCP 機制, “ciaddr”欄位為 0.0.0.0, 因此如果“yiaddr”欄位有值, 則表示 Supplicant 使用者可以使用“yiaddr”欄位中的 IP Address, 因此會將“yiaddr”欄位中的 IP Address 記錄在本身的 Supplicant State Table 中該 Supplicant 使用者的 IP Address 欄位, 並且 Status 欄位設定 Dynamic, 之後會允許該 Supplicant 的 traffic 通過。

## 4.2.1.2.2 Non-subscribed IP Address

在此情境中，使用者沒有透過合法程序註冊使用的 IP Address，例如 guest user，並且設定使用 DHCP 機制取得 Dynamic IP Address 在 Supplicant 上使用。

Figure 4-11 所顯示的為 Supplicant 使用者設定使用 DHCP 機制取得 Dynamic IP Address 時，整個 Message 交換的流程圖，分別說明如下：

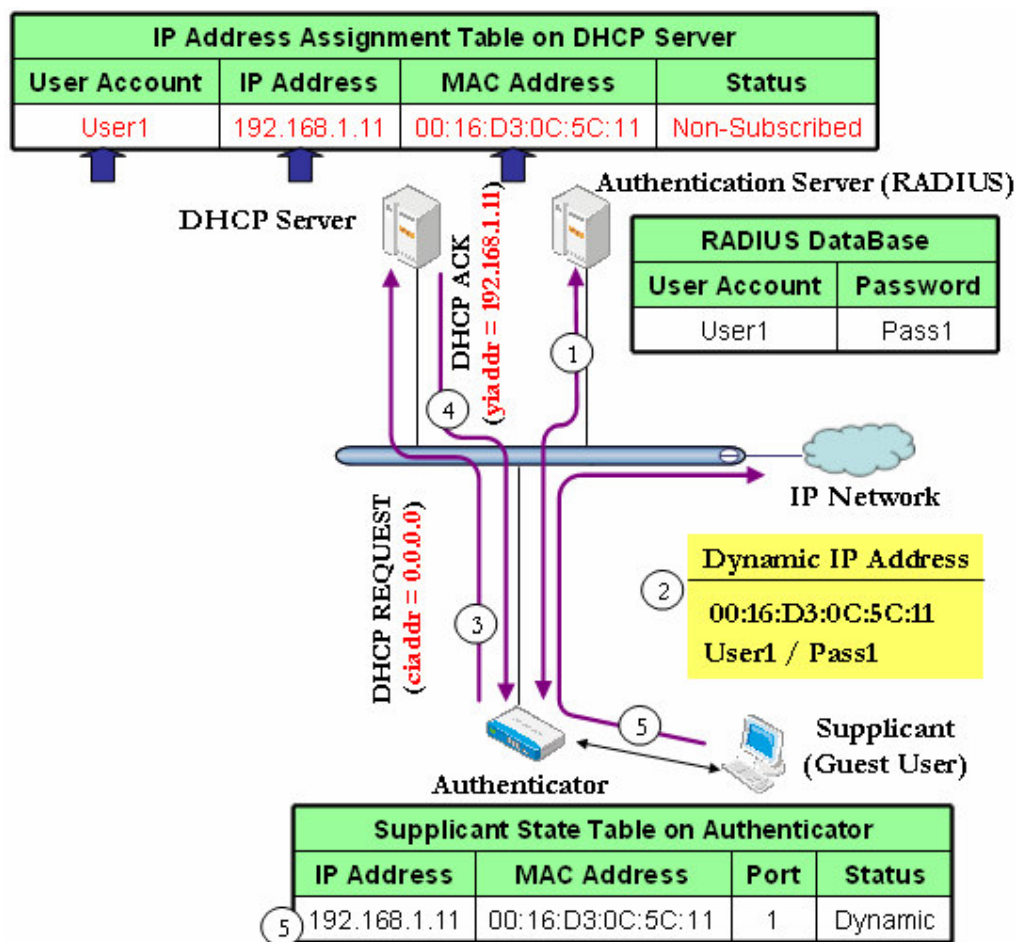


Figure 4-11 User acquires IP Address with Dynamic IP Address Acquisition

① 當 Supplicant 連接到 Authenticator 時，Authenticator 會要求 Supplicant 提

供認證資料，並將這些認證資料，轉傳給 Authentication Server 做認證。

- ② 在使用者身份認證完後，此時 Authenticator 已經可以確認 Supplicant 使用者的身分，由於 Supplicant 使用者設定使用 DHCP 機制取得 Dynamic IP Address，因此當 Authenticator 收到 Supplicant 發出的 DHCP DISCOVERY 封包時，Authenticator 確認 Supplicant 使用者為動態取得 IP Address 使用。
- ③ Authenticator 會發送 DHCP REQUEST 給支援本論文方法的 DHCP Server 作確認，把 Supplicant 使用的 MAC Address 填入 DHCP Message 的“chaddr”欄位中，並把使用者身份認證的帳號填入“uname”欄位中，並把“ciaddr”欄位填入 0.0.0.0，表示 Supplicant 使用者使用的是 DHCP 機制。
- ④ 當 DHCP Server 收到 DHCP DISCOVERY 時，DHCP Server 會從 DHCP Message 的“uname”和“chaddr”欄位取得 Supplicant 使用者使用的帳號和 MAC Address，用來跟本身的 IP Address Assignment Table 中的記錄做比對，以取得 Supplicant 使用者註冊的 IP Address，在此情境下，由於 Supplicant 使用者沒有透過合法程序註冊使用的 IP Address，因此經由帳號的比對，無法從 IP Address Assignment Table 中取得 Supplicant 使用者註冊的 IP Address，且由於 DHCP Message 的“ciaddr”欄位設定為 0.0.0.0，因此 DHCP Server 會從沒有分配給使用者使用的 IP Address，以及目前沒有在使用的 IP Address 中，取出一個 IP Address 填入 DHCP ACK 的“yiaddr”欄位後回傳給 Authenticator，並把此 Supplicant 的 User Account 和 MAC Address，以及分配到的 IP Address 資訊新增記錄到本身的 Table 中，並且將此記錄的 Status 欄位設定為 Non-Subscribed。
- ⑤ Authenticator 在收到 DHCP ACK 後，會將“yiaddr”欄位中的值和之前傳送 DHCP REQUEST 的“ciaddr”欄位比對是否相同，在此情境下，由於

Supplicant 使用者使用的是 DHCP 機制，“ciaddr”欄位為 0.0.0.0，因此如果“yiaddr”欄位有值，則表示 Supplicant 使用者可以使用“yiaddr”欄位中的 IP Address，因此會將“yiaddr”欄位中的 IP Address 記錄在本身的 Supplicant State Table 中該 Supplicant 使用者的 IP Address 欄位，並且 Status 欄位設定 Dynamic，之後會允許該 Supplicant 的 traffic 通過。

## 4.2.2 IP Address Releasing

當 Authenticator 收到 Supplicant 的 DHCP RELEASE，或是偵測到 Supplicant 斷線時，無論 Supplicant 使用手動設定使用 Static IP Address，或是設定使用 DHCP 機制取得 Dynamic IP Address，均會透過 DHCP Message 向 DHCP Server 做 IP Address Release 的機制。

Figure 4-12 所顯示的為 Supplicant 使用者已經可以正常使用網路後，當 Authenticator 收到 Supplicant 使用者發出的斷線訊息，或是偵測到 Supplicant 斷線時，整個 Message 交換的流程圖，分別說明如下：

- ① Authenticator 收到 Supplicant 的 DHCP RELEASE，或是偵測到 Supplicant 斷線。
- ② Authenticator 會從 Supplicant State Table 中取得 Supplicant 的 IP Address 和 MAC Address 分別填入 DHCP Message 的“ciaddr”和“chaddr”欄位中，發送 DHCP RELEASE 給支援本論文方法的 DHCP Server 作確認，並把本身 Supplicant State Table 中的該記錄刪除。

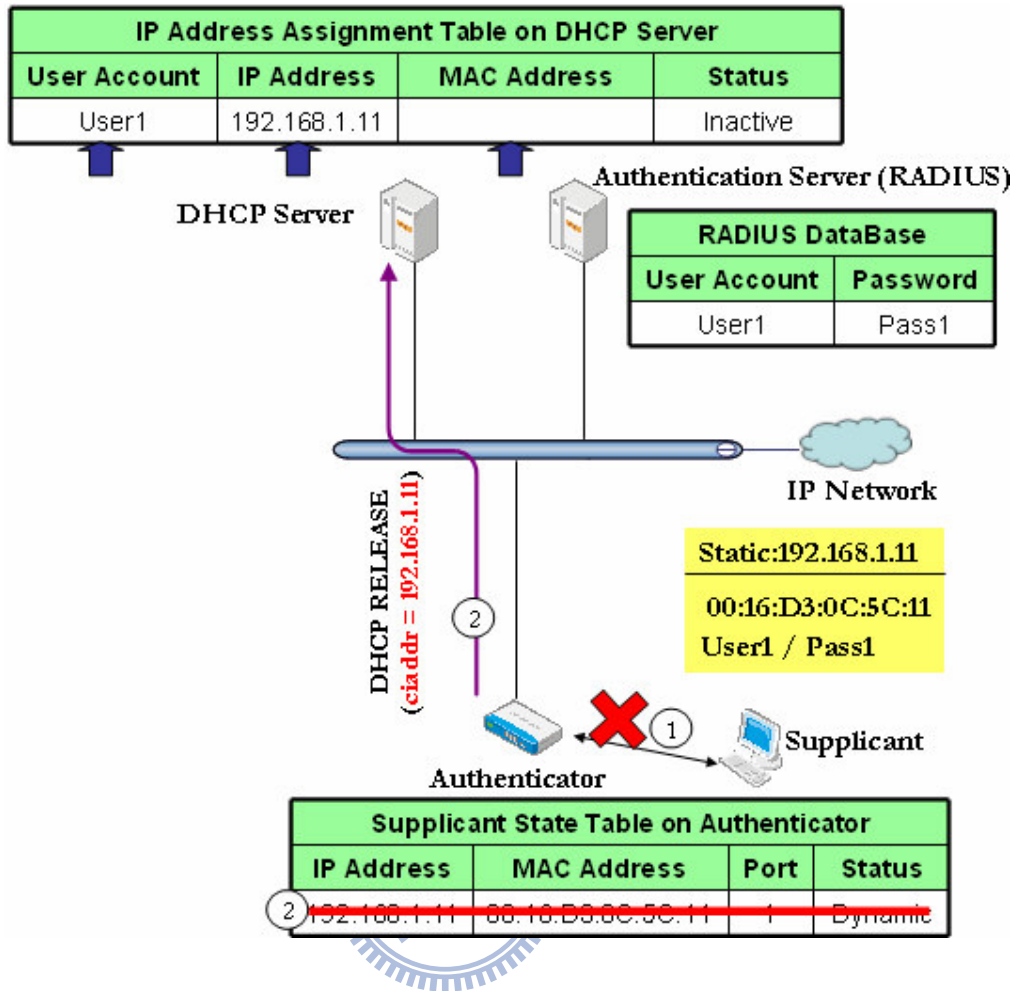


Figure 4-12 IP Address Releasing

- ③ 當 DHCP Server 收到 Authenticator 發送的 DHCP RELEASE 時， DHCP Server 會從 DHCP Message 的“ciaddr”和“chaddr”欄位取得 Supplicant 使用者使用的 IP Address 和 MAC Address，用來跟本身的 IP Address Assignment Table 中的記錄做比對，若比對成功，且該記錄為使用者透過合法程序註冊使用，則把 Table 中該記錄的 Status 欄位改為 Inactive; 若比對成功，但該記錄不為使用者註冊使用，而是透過 DHCP 機制向 DHCP Server 取得 IP Address，則把 Table 中該記錄刪除; 若比對失敗，則不理會此 DHCP Message。

## 4.3 單元總結

總結本章節所述，我們所提的 IP 管理機制包含下列幾個部分：

- 在 Authenticator 上建立 Supplicant State Table，用來管控連接到 Authenticator 的 Supplicant 的合法性和行為。
- 在 IP Management Server 上建立 IP Address Assignment Table，用來對連接到 Authenticator 的 Supplicant 作 IP Address 的分配與管理。
- 在 Dynamic IP Assignment Mechanism 中，本論文利用延伸 DHCP Message 作為 Authenticator 和 IP Management Server 之間的 IP Management Protocol 來做探討。
  - 在 Authenticator 上利用 DHCP Message 中已經定義的“ciaddr”，“chaddr”的兩個欄位，與新增 options 的“uname”欄位，將連接到 Authenticator 的 Supplicant 相關資訊傳送給 DHCP Server 做確認，並對回傳 DHCP Message 的“yiaddr”欄位作判斷，將結果記錄於 Supplicant State Table 中，以便對連接的 Supplicant 作管控。
  - 在 DHCP Server 上透過對 Authenticator 所傳送 DHCP 封包的“ciaddr”，“chaddr”，“uname”三個欄位判斷，從 IP Address Assignment Table 中，將 Supplicant 可使用的 IP Address 利用 DHCP Message 中已經定義的“yiaddr”欄位傳送回 Authenticator。

# 第五章 確保合法使用 IP 位址之 IP 管理機制的設計與實作

## 5.1 實作方法

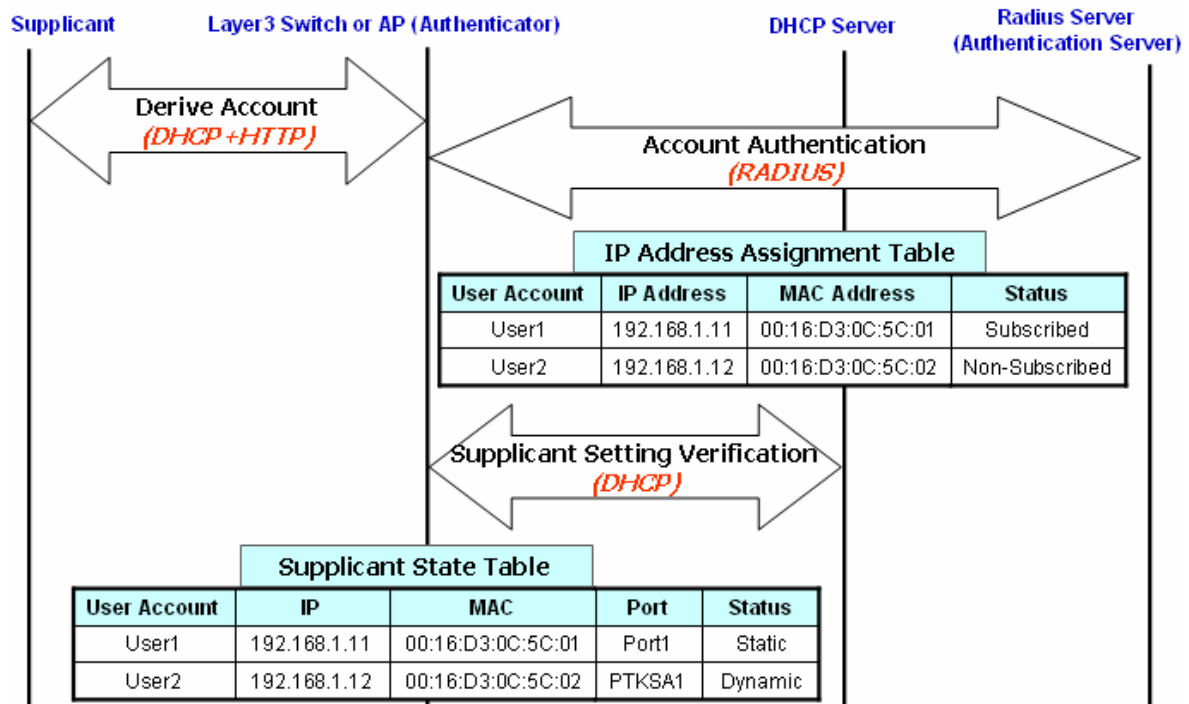


Figure 5-1 System architecture of proposed scheme implementation

本篇論文實作上，在使用者的身分認證機制方面，使用的是 Web Login + RADIUS，在此實作方法上，使用者如果設定動態取得 IP Address 時，由於此時沒有 IP Address 使用，因此無法連上 Web Server，所以 Authenticator 必須先分配一個暫時的 IP Address 給 Supplicant 使用，使其能連接上 Web Server 輸入帳號密碼，透過 RADIUS 進行身分認證。在 IP 管理的機制方面，則使用本論文提到的相關方法，先在 DHCP Server 上建立 IP Address Assignment Table，管理 Supplicant 的 IP Address，在 Supplicant 認證完成後，透過本論文的 DHCP Message 訊息交換，



根據 Supplicant 的使用者帳號，使用的網路設備 IP Address 和 MAC Address，進行是否可合法使用網路的確認，並且在 Authenticator 上建立 Supplicant State Table，對連接上的 Supplicant 作管控，整個實作的方法如同 Figure 5-1 所顯示。

## 5.2 實作網路環境與系統

本篇論文的實作環境如 Figure 5-2 所顯示，Supplicant 均連接到 Authenticator，透過 Authenticator 使用網路上的服務和資源，Authenticator 並連接 Radius Server，來做 Supplicant 使用者的身分認證，以及連接 DHCP Server，來做 Supplicant 的合法性確認。

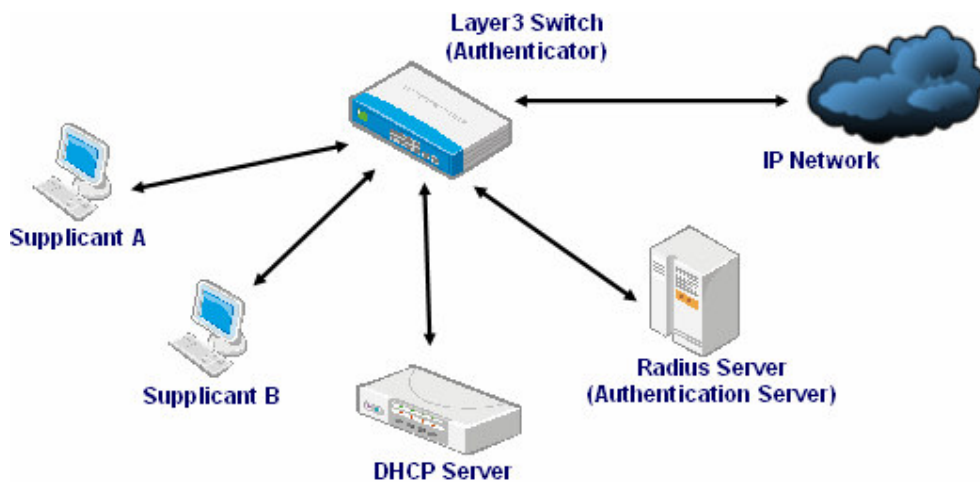


Figure 5-2 Network Environment of proposed scheme implementation

實作的基本設定上，Authenticator 的 IP Address 設定為 192.168.1.1，由於使用者如果設定動態取得 IP Address 時，Authenticator 必須先分配一個暫時的 IP Address 給 Supplicant 使用，因此 Authenticator 會有一個暫時的 DHCP IP Address，設定值為 192.168.1.11~192.168.1.20。Radius Server 的 IP Address 設定為 192.168.1.2。DHCP Server 的 IP Address 設定為 192.168.1.3，由於 DHCP Server



同樣要分配給沒有事先註冊的 Supplicant 一個合法可使用的 IP Address，因此設定值為 192.168.1.21~192.168.1.30。

實作的系統上，Supplicant 使用一般電腦即可，不需做修改或安裝任何程式，Radius Server 則是使用 Linux 上 Open Source 的 FreeRadius[25] 建構而成，而在 Authenticator 和 DHCP Server 上，則是使用實際運作的網路設備，也是本論文實作中，最主要需要修改的部份。

### 5.3 User 註冊流程說明

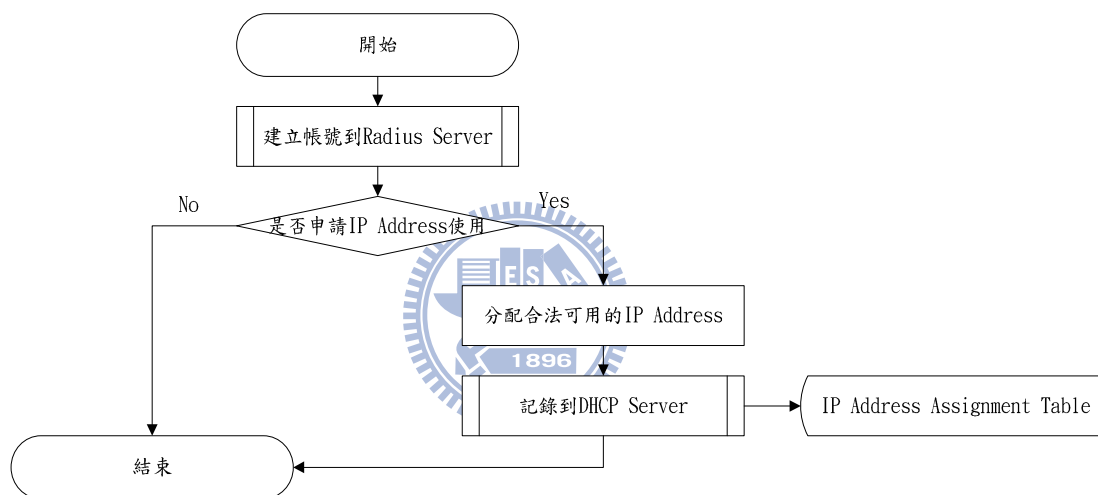


Figure 5-3 User Account Apply Flow

首先針對 User 註冊的流程進行說明。Figure 5-3 所顯示的為 User 註冊的流程，一開始先建立要使用的使用者帳號到 Radius Server 中[26]，再根據此使用者是否要註冊申請使用的 IP Address，如果要則系統會分配合法可用的 IP Address 給使用者，並把使用者帳號、註冊使用的 IP Address、以及使用此 IP Address 的網路設備 MAC Address，記錄到 DHCP Server 中的 IP Address Assignment Table，即完成整個 User 註冊的程序。

## 5.4 Supplicant 登入網路流程說明

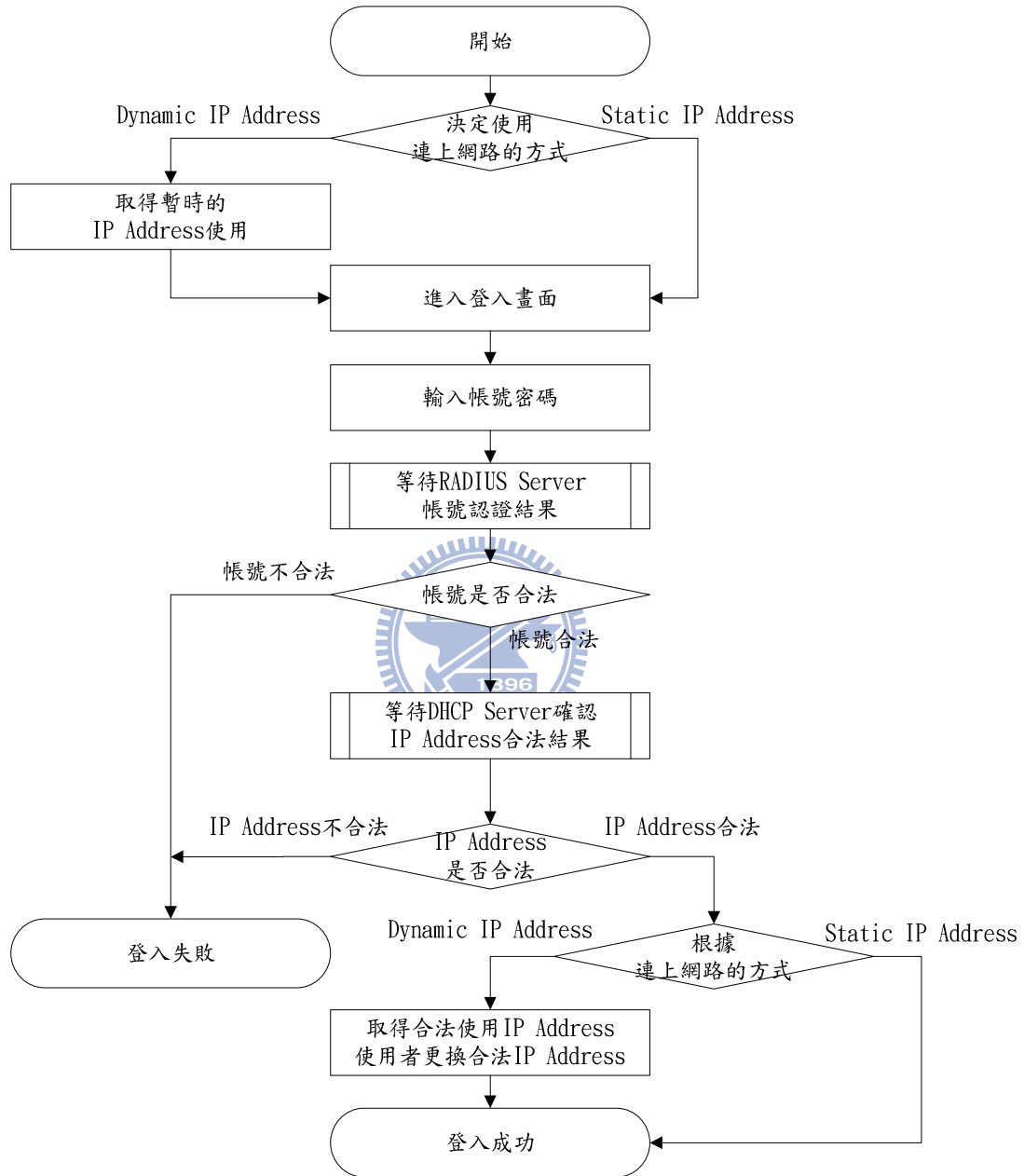


Figure 5-4 Supplicant Login Flow

Figure 5-4 所顯示的為 Supplicant 登入網路的流程，一開始 Supplicant 使用者

先決定連上網路的方式，如果是使用動態取得 IP Address 的方式，Authenticator 會先分配一組暫時的 IP Address，提供 Supplicant 連到 Authenticator 登入畫面輸入帳號密碼，之後 Authenticator 會將使用者帳號密碼傳送給 Radius Server 作身份認證，根據 Radius Server 回傳的結果，如果帳號不合法，則表示登入失敗，Supplicant 使用者的不能透過 Authenticator 使用網路上的資源和服務。

如果帳號合法，則 Authenticator 會將使用者帳號、使用的 IP Address、以及 Supplicant 的 MAC Address，傳送給 DHCP Server 作確認，根據 DHCP Server 回傳的結果判定，如果 IP Address 不合法，則表示登入失敗，Supplicant 使用者的不能透過 Authenticator 使用網路上的資源和服務；如果 IP Address 合法，則根據 Supplicant 使用者連上網路的方式，如果是使用手動設定 IP Address 的方式，則表示登入成功，Supplicant 使用者的可以透過 Authenticator 使用網路上的資源和服務；如果是使用動態取得 IP Address 的方式，則表示取得合法可使用的 IP Address，Authenticator 此時會顯示訊息，請 Supplicant 使用者再使用動態取得 IP Address 的方式，取得合法可使用的 IP Address，並可以透過此 IP Address 使用網路上的資源和服務。

## 5.5 Authenticator 系統設計說明

Figure 5-5 所顯示的為 Authenticator 系統設計的流程，一開始 Authenticator 會建立 Supplicant State Table，用來對連接的 Supplicant 作管控。當取得連接上的 Supplicant MAC Address，以及取得 Supplicant 連接上的 Port Number，並記錄到本身的 Supplicant State Table 中，之後判斷使用者連上網路的方式，執行相對應的動作。

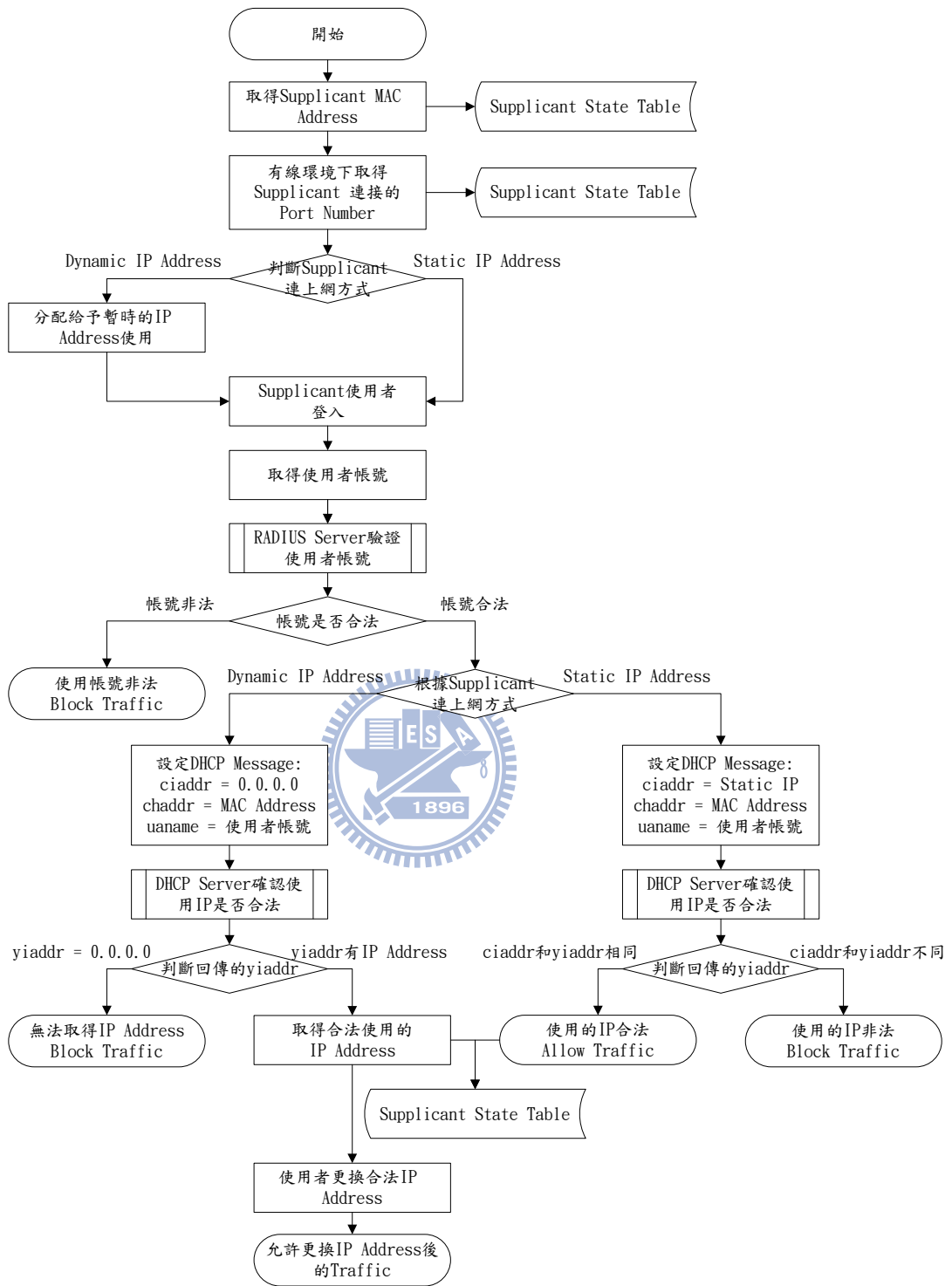


Figure 5-5 Authenticator System Flow of proposed scheme implementation

如果是使用動態取得 IP Address 的方式，則會先分配一組暫時的 IP Address，提供 Supplicant 連到 Authenticator 登入畫面輸入帳號密碼，Authenticator 取得使用者帳號密碼後，會將使用者帳號密碼傳送給 Radius Server 作身份認證，根據 Radius Server 回傳的結果，如果帳號不合法，則表示帳號非法，此時 Authenticator 會封鎖該 Supplicant 使用者的封包，使其不能透過 Authenticator 使用網路上的資源和服務；如果帳號合法，則會根據 Supplicant 使用者連上網路的方式，填入相關的 DHCP Message 欄位，傳送給 DHCP Server 確認使用者使用的 IP Address 是否合法，或是取得使用者合法可使用的 IP Address。

如果 Supplicant 使用者使用手動設定 IP Address 的方式，則會將 DHCP Message 中的“ciaddr”欄位填入手動設定的 IP Address，“chaddr”欄位填入 Supplicant 的 MAC Address，“uname”欄位填入使用者的帳號；如果 Supplicant 使用者使用動態取得 IP Address 的方式，則會將 DHCP Message 中的“ciaddr”欄位填入 0.0.0.0，“chaddr”欄位填入 Supplicant 的 MAC Address，“uname”欄位填入使用者的帳號；完成上述設定後，Authenticator 會將此 DHCP Message 使用 Unicast 的方式，發送 DHCP DISCOVERY/DHCP REQUEST 給 DHCP Server，DHCP Server 在確認後會回傳 DHCP OFFER/DHCP ACK 給 Authenticator。

如果 Supplicant 使用者使用手動設定 IP Address 的方式，且回傳 DHCP Message 中的“yiaddr”欄位填入的值與傳送的“ciaddr”欄位值不相同，則表示使用的 IP Address 非法，此時 Authenticator 會封鎖該 Supplicant 使用者的封包，使其不能透過 Authenticator 使用網路上的資源和服務；如果欄位值相同，則會把欄位的 IP Address 寫入 Supplicant State Table 中該 Supplicant 的 IP Address 欄位，並允許該 Supplicant 使用者使用網路上的資源和服務。

如果 Supplicant 使用者使用動態取得 IP Address 的方式，且回傳 DHCP Message 中的“yiaddr”欄位填入的值為 0.0.0.0，則表示無法取得合法可使用的 IP

Address，此時 Authenticator 會封鎖該 Supplicant 使用者的封包，使其不能透過 Authenticator 使用網路上的資源和服務；如果“yiaddr”欄位填入的值为 IP Address，則會把欄位的 IP Address 寫入 Supplicant State Table 中該 Supplicant 的 IP Address 欄位，並顯示訊息通知 Supplicant 使用者再使用動態取得 IP Address 的方式，取得合法可使用的 IP Address，此時 Authenticator 允許使用該 IP Address 的 Supplicant 使用者使用網路上的資源和服務。

## 5.6 DHCP Server 系統設計說明

Figure 5-6 所顯示的為 DHCP Server 系統設計的流程，一開始 DHCP Server 會建立 IP Address Assignment Table，用來對網路上的 IP Address 作管理。當收到 Authenticator 發出用來確認使用者使用 IP Address 合法性的 DHCP Message 時，會從 DHCP Message 中的“ciaddr”、“chaddr”和“uaname”欄位分別取得使用者的 IP Address、使用者 Supplicant 的 MAC Address，和使用者的帳號，透過 IP Address Assignment Table 的比對，可得知 Supplicant 使用者是否事先已經註冊用的 IP Address。

如果 Supplicant 使用者事先已經註冊使用的 IP Address，則根據“ciaddr”欄位的值是否為 IP Address，若值為 0.0.0.0，則表示 Supplicant 使用者使用動態取得 IP Address 的方式，因此把 DHCP Message 的“yiaddr”欄位值，填入 Supplicant 使用者事先已經註冊使用的 IP Address；如果“ciaddr”欄位的值为 IP Address，則表示 Supplicant 使用者使用手動設定 IP Address 的方式，因此會比對手動設定的 IP Address，是否與事先註冊使用的 IP Address 相同，若值相同，則把 DHCP Message 的“yiaddr”欄位值，填入 Supplicant 使用者事先已經註冊使用的 IP Address；若值不相同，表示 Supplicant 使用者使用的 IP Address 不合法，因此會把 DHCP Message 的“yiaddr”欄位值，填入 0.0.0.0，之後會將 填好的 DHCP Message 回傳給

Authenticator。

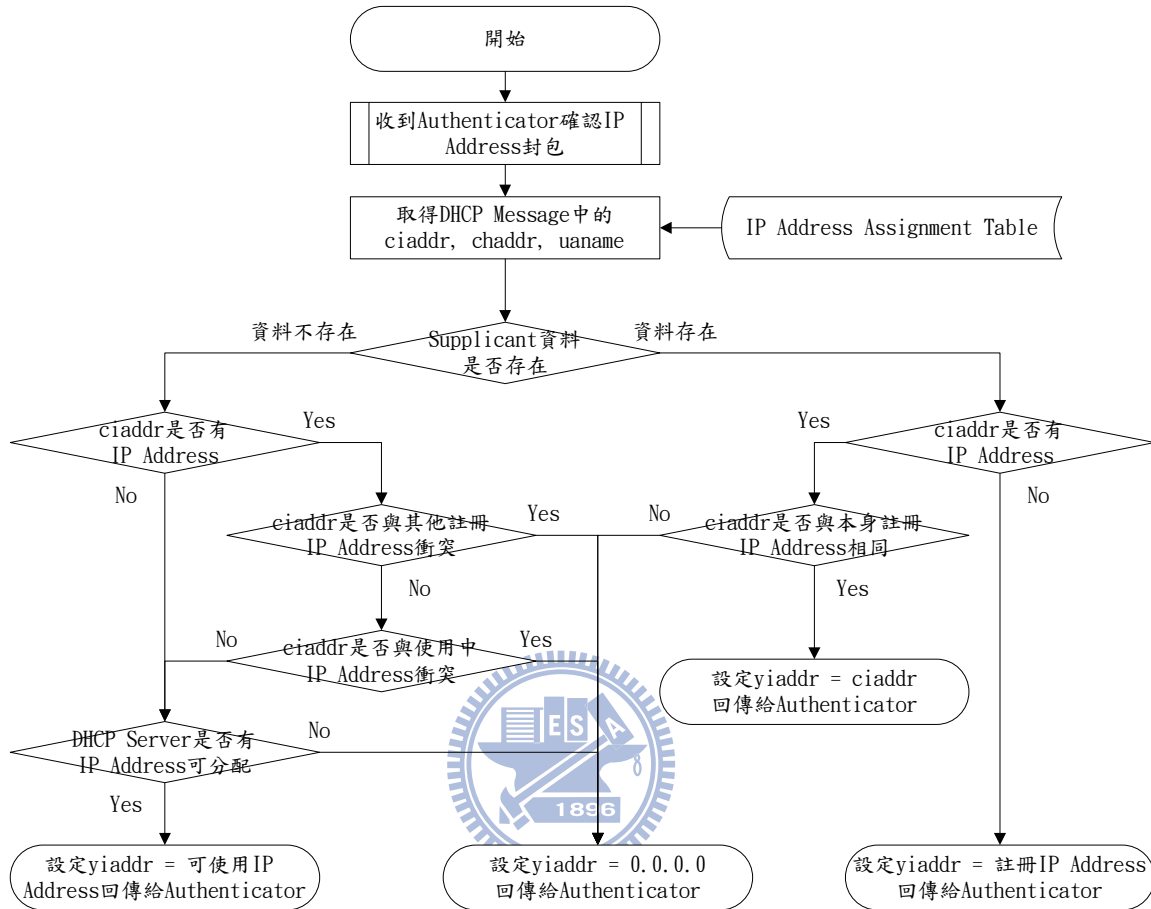


Figure 5-6 DHCP Server System Flow of proposed scheme implementation

如果 Supplicant 使用者沒有事先註冊使用的 IP Address，則無法在 IP Address Assignment Table 中查詢到資料，根據“ciaddr”欄位的值是否為 IP Address，若值為 0.0.0.0，則表示 Supplicant 使用者使用動態取得 IP Address 的方式，因此 DHCP Server 會確認是否還有非註冊給使用者，且目前沒有使用的 IP Address，若有則從中選取一個 IP Address 填入 DHCP Message 的“yiaddr”欄位；若沒有則會把 DHCP Message 的“yiaddr”欄位值，填入 0.0.0.0；如果“ciaddr”欄位的值為 IP Address，則表示 Supplicant 使用者使用手動設定 IP Address 的方式，因此會比對

手動設定的 IP Address，是否與其它事先註冊使用的 IP Address，或是正在使用的 IP Address 相衝突，若有則會把 DHCP Message 的“yiaddr”欄位值，填入 0.0.0.0；若沒有則會確認 DHCP Server 是否還有非註冊給使用者，且目前沒有使用的 IP Address，若有則從中選取一個 IP Address 填入 DHCP Message 的“yiaddr”欄位，之後會將填好的 DHCP Message 回傳給 Authenticator。





## 第六章 結論與未來工作

### 6.1 結論

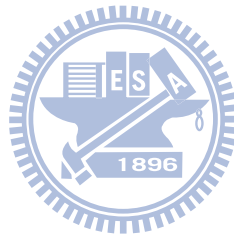
我們所提出的 IP 管理機制當中，當 Supplicant 加入網路時，其所連結的 Authenticator 即會將相關資訊記錄在 Supplicant State Table 中，並透過使用者認證機制，確認使用者的合法性。當 Authenticator 確認 Supplicant 使用者使用網路的合法性後，會再利用 Dynamic IP assignment 的機制，與 IP Management Server 作 Supplicant 使用者使用 IP Address 的合法性進行確認，而 IP Management Server 則利用建立的 IP Address Assignment Table，來確認與取得 Supplicant 使用者可使用的合法 IP Address。Authenticator 透過此機制，將取得的合法 IP Address 記錄在 Supplicant State Table 中該 Supplicant 使用者的 IP Address 欄位，利用 Supplicant State Table，來預防非法使用者使用網路資源，以及相同 IP Address 的網路設備造成的 IP 衝突問題，達成 IP 管理的目的。

我們所提出的 IP 管理機制具有以下特色：

- **預防 IP Address 衝突：**可以保證在同一個網域中，同時有兩個以上的網路設備使用相同的 IP Address 時，不會發生 IP Address 互相衝突的問題。
- **統一管理：**透過在 IP Management Server 的 IP Address Assignment Table 建立，可以讓網路端完全管理所有的 Ratable IP Address。此外，在網路設備使用者還沒經過網路端同意之前，不能隨意更換使用中的 IP Address。
- **阻擋非法：**透過在 Authenticator 的 Supplicant State Table 建立，可以阻止不合法的使用者，或在網路設定上有誤 Supplicant 進入網路使用相關

服務和資源。

- **彈性使用：**無論使用者是否事先透過合法程序註冊使用者網路設備使用的 IP Address，或是連上網路時，使用手動設定或動態取得 IP Address 的方式，都可以取得事先已經註冊的 IP Address，或是可以合法使用的 IP Address。



## 6.2 未來工作

本篇論文所提的方法是利用在 IP Management Server 上建立的 IP Address Assignment Table，透過 Table 中 User Account 欄位的比對，來判斷使用者是否事先註冊要使用的 IP Address，以及使用中的 IP Address 是否合法正確。如果使用者事先註冊要使用的 IP Address，一開始先用一台網路設備使用動態的方式取得 IP Address，此時透過 IP Address Assignment Table 中 User Account 欄位的比對，會將使用者註冊的 IP Address 分配給此使用者所使用的網路設備，若此時使用者用另外一台網路設備使用手動設定註冊的 IP Address 方式連接上 Authenticator，由於註冊的 IP Address 已經被分配給動態取得 IP Address 的網路設備，會使得使用手動設定 IP Address 的網路設備無法上網，如何解決當使用者已經事先註冊要使用的 IP Address，卻因為使用者網路設備利用手動設定註冊的 IP Address，或利用動態取得註冊 IP Address 的前後順序，造成網路設備無法順利使用網路上的資源與服務的這個問題，將會是我們未來研究的方向。

## 參考文獻

- [1] R. Droms, “Dynamic Host Configuration Protocol,” RFC 2131, March, 1997.
- [2] C. Rigney, S. Willens, A. Rubens, W. Simpson, “Remote Authentication Dial In User Service (RADIUS),” RFC 2865, June, 2000
- [3] C. Rigney, “RADIUS Accounting,” RFC 2866, June, 2000
- [4] J. Postel, “User Datagram Protocol,” RFC 768, 28, August, 1980
- [5] Radius Types. Available:  
<http://www.iana.org/assignments/radius-types>
- [6] R. Rivest, “The MD5 Message-Digest Algorithm,” RFC 1321, April, 1992
- [7] RADIUS From Wikipedia. Available:  
<http://en.wikipedia.org/wiki/RADIUS>
- [8] IEEE 802.1 Working Group, “Port-Based Network Access Control,” IEEE Standard 802.1X-2004, December 2004.
- [9] Virtual LAN From Wikipedia. Available:  
<http://en.wikipedia.org/wiki/VLAN>
- [10] IEEE 802.1X From Wikipedia. Available:  
[http://en.wikipedia.org/wiki/IEEE\\_802.1X](http://en.wikipedia.org/wiki/IEEE_802.1X)
- [11] P. Congdon, B. Aboba, A. Smith, G. Zorn, J. Roese, “IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines,” RFC 3580, September 2003
- [12] IEEE 802.1X 無線連線驗證. Available:  
<http://www.microsoft.com/taiwan/technet/community/columns/cableguy/cg0402.aspx>
- [13] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, “Extensible Authentication Protocol (EAP),” RFC 3748, June 2004
- [14] W. Simpson, “The Point-to-Point Protocol (PPP),” RFC 1661, July 1994
- [15] 無線網路安全機制剖析. Available:  
<http://loda.zhupiter.com/WirelesSecurity.htm>
- [16] D. Simon, B. Aboba, R. Hurst, “The EAP-TLS Authentication Protocol,” RFC 5216, March 2008
- [17] P. Funk, S. Blake-Wilson, “Extensible Authentication Protocol Tunneled

Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0),”  
RFC 5281, August 2008

- [18] J. Arkko, H. Haverinen, “Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA),” RFC 4187, January 2006
- [19] IEEE 802.11 Working Group, “Amendment 6: Medium Access Control (MAC) Security Enhancements,” IEEE Standard 802.11i-2004, July 2004.
- [20] Dynamic Host Configuration Protocol From Wikipedia. Available:  
<http://en.wikipedia.org/wiki/Dhcp>
- [21] K. Sollins, “THE TFTP PROTOCOL (REVISION 2),” RFC 350, July 1992
- [22] IP & MAC Address Binding. Available:  
[http://ftp.qno.cn/Doc/Technical/FVR9416\\_IP&MAC\\_Binding\\_Setting.pdf](http://ftp.qno.cn/Doc/Technical/FVR9416_IP&MAC_Binding_Setting.pdf)
- [23] NCTU Dormitory Network IP Address Apply. Available:  
[http://www.cc.nctu.edu.tw/dorm/apply\\_ip.html](http://www.cc.nctu.edu.tw/dorm/apply_ip.html)
- [24] 自動化宿舍管理系統. Available:  
<http://www.kyu.edu.tw/93/epaperv7/001.pdf>
- [25] FreeRadius 官方網站. Available:  
<http://freeradius.org/>
- [26] FreeRadius 安裝與管理. Available:  
<http://rd.tyc.edu.tw/modules.php?name=Tutorial&mode=visit&tid=10>

