逢 甲 大 學

資 訊 工 程 學 系 專 題 報 告

Attacks on the DHCP protocol

學　　生 ： 顏 學 回(四甲)
陳 俊 德(四甲)
李 冠 宏(四甲)

指 導 教 授 ： 劉 振 緒

中 華 民 國 九 十 二 年 十 一 月

摘要

在現今的資訊科技中，由於網路的蓬勃發展使得許多原本遙不可及的夢想，得以在網路的世界中實現，但也正因為大量的使用而使得原有的資源逐漸不敷使用，其中最明顯的問題就是 IP 位址的不足，目前解決 IP 位址不足的問題，大多使用 DHCP(Dynamic Host Configuration Protocol)的機制解決，而且在許多無線網路的環境中，因為使用者的變異性極大，所以也必須使用 DHCP 的機制，由此可知 DHCP 協定在現今的網路環境中佔有非常重要的地位。

雖然 DHCP 的設計使網路可以更方便的為人們所使用，但其協定卻有安全上問題，使得 DHCP Server 可能受到不當使用者的攻擊而導致 Server 無法正常運作。本研究之目的即在於探討 DHCP 的協定及其安全上的漏洞，並嘗試可能的解決方法。

本研究所使用的程式為 ISC(Internet Software Consortium)於 2002 年研發的 DHCP Server 與 Client 端 Open Source 的程式，使用語言為 C 語言，作業系統為 Linux 或 BSD。

目　　錄

圖表目錄

第一章　緒論

1、1 研究動機

在現今網路技術的高度發展及大量使用下，已使得某些資源不敷使用，其中最明顯的問題就是 IP 位址的不足，目前亦有許多方法試圖解決這個問題，IPv6 就是解決 IP 位址不足最根本的方法，雖然有 IPv6 的技術來解決 IP 位址的不足的問題，但因為現今硬體線路及軟體支援的限制使的 ipv6 並未普及使用。因此目前最廣泛被用來解決 IP 位址不足問題的技術就是 DHCP(Dynamic Host Configuration Protocol)。DHCP 是一個可以動態配置(assign)IP 給某台主機使用的通訊協定。一個網域的使用人數可能大於這個網域的 IP 位址個數，但並非在同一時間內所有的使用者都需要連上網路，因次 DHCP 的動態配置機制可以讓有需要連上網路的使用者優先配置 IP 位址，因此可以有效的解決 IP 位址不足的問題，並且在無線網路的環境下也有使用 DHCP 的需要。

如此重要的通訊協定，但在其協定曾方面似乎仍存在著安全上的漏洞，可能導致 DHCP Server 受到不當使用者的攻擊而無法正常運作。本研究的目的即在於探討 DHCP 協定究竟出了什麼問題，為何會導致受到使用者的攻擊，並實做其攻擊過程及如何防範此種攻擊的發生。

1、2 研究方法

本研究使用的工具及其目的如下所列：

操作平台：Red Hat Linux 8.0

DHCP 軟體：ISC(Internet Software Consortium)於 2002 年所開發的 Open Source 的程式。

研究過程中：Server 端程式並未做任何修改，均使用其原始程式碼，其設定檔也是依照著一般的格式來設定，而 Client 端程式經個人修改，使其能把 server 所提供之 ip 全部要完，讓其他 client 無法向 server 取得 ip。

1、3 本文章節概述

本文章節內容概述如下：

第二章：介紹 DHCP 的封包格式、工作原理。

第三章：說明 DHCP 上的漏洞、攻擊者如何攻擊。

第四章：運用 ISC 的程式實做攻擊過程並顯示攻擊結果。

第五章：為 DHCP Server 的保護方法

第六章：總結

第二章　DHCP 的工作原理

2、1 DHCP 的封包格式

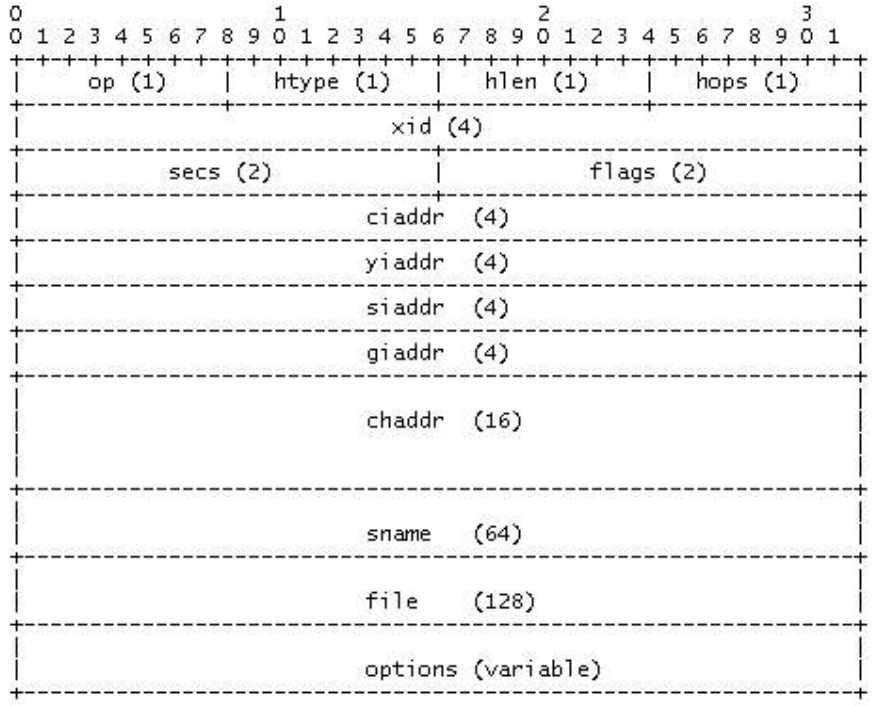


圖 2.1-1 DHCP 的封包格式

欄位	位元	說明
Op	1	Message type
Htype	1	Hardware address type
Hlen	1	Hardware address length
Hops	1	Client 端設定為 0, 大多交由 Relay agent 設定
Xid	4	Transaction ID，由 Client 隨機產生並填入
Secs	2	表示從取得 IP 到現在所經過的時間，由 Client 填入

Flags	2	旗標
ciaddr	4	Client IP address，當 Client 在 Bound、Renew、Rebinding 狀態時才會填入
yiaddr	4	“Your”(Client) IP address
siaddr	4	Server IP address
giaddr	4	Relay agent IP address
chaddr	16	Client hardware address
sname	64	Server host name
File	128	Boot file name
option	Var	Optional parameters field

2、2 DHCP 的工作原理

DHCP(Dynamic Host Configuration Protocol)是基於 TCP/IP 的網路協定中，用於暫時配置(assign)一個 IP 位址給一台機器所使用的通訊協定。DHCP 的執行必須有一台電腦執行 DHCP Server 而需要被配置 IP 的電腦則執行 DHCP Client。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：

○Client 第一次登入：

1、當 DHCP Client 為第一次登入時，發現本機上並沒有被配置(assign)IP，此時 Client 會以廣播(Broadcast)的方式發送 DHCPDISCOVER 封包來找尋網域中的 DHCP Server。

2、網域中所有的 DHCP Server 都會收到 Client 所發送的 DHCPDISCOVER，收到封包後 Server 會以 Unicast 的方式發送 DHCPOFFER 封包。在 DHCPOFFER 封包中包含所有需要告知 Client 的訊息(例如：IP address、subnet mask、gateway…等等)。

3、經過一定的時間之後 DHCP Client 應收到一個以上的 Server 所回應的 DHCPOFFER，Client 可以從多個 DHCPOFFER 中選定一個 Server 將其 Server IP 位址填入 DHCPREQUEST 封包中的 Server Identifier 中，再以廣播的方式將其發送出去。

4、網域中的 DHCP Server 會收到 Client 回應的 DHCPREQUEST 封包，但只有其 Server Identifier 與自己的 IP 位址相同的 Server 才會回應 DHCPACK 給 Client。此 DHCPACK 封包中所包含的訊息(IP、subnet mask、gateway…等)應與 DHCPOFFER 中的訊息相同。

5、當 DHCP Client 收到 DHCPACK 即表示此 Client 已被配置一個 IP，並將封包中的各個資料與作業系統做連結(bind)同時也結束一個完整的 DHCP 工作過程。

6、若 DHCP Client 收到 DHCPNAK，則表示 Server 拒絕了 Client 的請求，Client 可以重新發送 DHCPDISCOVER，此時 DHCP 的運作過程回到步驟 1

7、若 DHCP Client 收到 DHCPACK 中的 IP 已被其他機器使用，則 Client 可以回應 DHCPDECLINE，告知 Server 此一 IP 位址已被其他使用者所使用，並重新發送 DHCPDISCOVER，此時 DHCP 的運作過程回到步驟 1

○Client 第一次登入之後：

當 Client 在第一次登入之後，欲要求之前曾經獲得的 IP 時，可以省略上述某些步驟

1、DHCP Client 以 Unicast 的方式發送 DHCPREQUEST，並將欲獲得的 IP 填入 Request IP address 欄位中，Server IP 填入 Server Identifier 中。

2、收到 DHCPREQUEST 的 Server 可以依據 Client 的請求回應 DHPCACK 或 DHCPNAK

3、以下步驟於前述相同

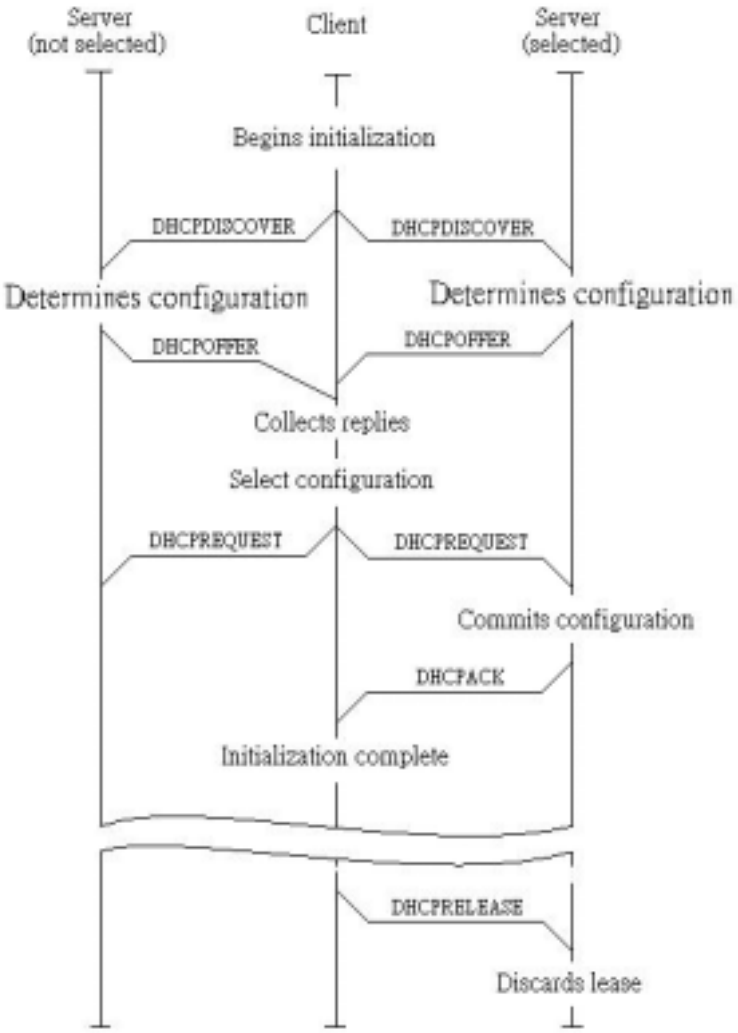


圖 2.2-1 Server 與 Client 封包傳送時間關係圖

2、3 DHCP Server Behavior

一個 DHCP Server 可能收到下列 5 種封包，本節即以下列 5 種封包說明 Server 在收到這些封包後的行為

○ DHCPDISCOVER

○ DHCPREQUEST

○ DHCPDECLINE

○ DHCPRELEASE

○ DHCPINFORM

2、3、1 DHCPDISCOVER

當 Server 收到 Client 送來的 DHPCDISVOVER，就從 IP Pool 中隨機挑選一個 IP 與租約(lease)，若所有的 IP 皆已經配置出去，無可再配置的 IP 時，程式應告知網路管理員並忽略此 DHCPDISCOVER。一旦 IP 與租約時間確定，Server 即建立一個 DHCPOFFER 封包並以收到的 DHCPDISCOVER 封包中所告知 Client 的 MAC address 以 Unicast 的方式送出封包。

2、3、2 DHCPREQUEST

若以 Server 而言，DHCPREQUEST 可能來自於下列三種情況，一是來自於回應 DHCPOFFER 的 Client，二是來自於第一次登入之後欲重新取得 IP 的 Client，三是來自於 INIT-REBOOT 的 Client，本節分別就上述三種情況論述：

○ DHCPREQUEST from Client which response DHCPOFFER：

Server 必須確定 Client 將 Server IP address 填入 Server Identifier 欄位中，ciaddr 必須為 0，Request IP address 欄位必須填入 Server 在 DHCPOFFER 中所給予的 IP。

若 Server Identifier 中的 IP address 與自己的 IP 位址不同，則 Server 忽略此 DHCPREQUEST。若上述條件均滿足，則 Server 回應 DHCPACK。

○ DHCPREQUEST from Client want to renew an IP

Server必須確定Server Identifier未被填入, Request IP address 欄位未被填入，ciaddr 必須填入 Client 自己的 IP address。若 Client 送出這種形式的封包，表示 Client 現在已經被配置一個 IP，但租約時間即將到期，Client 欲延長租約時間。若 Server 確定 Client 滿足上述條件，則 Server 應回應 DHCPACK。

○ DHCPREQUEST generated during INIT-REBOOT state

Server必須確定Server Identifier未被填入, Request IP address 欄位必須填入 Client 現在被配置的 IP，ciaddr 必須為 0，若 Client 送出這種形式的封包，表示 Client 欲確定(verify)現在使用的 IP address，若 Request IP address 中的 IP 是不正確的，則 Server 必須回應 DHCPNAK。若 Server 確定 Client 滿足上述條件，則 Server 應回應 DHCPACK。

2、3、3 DHCPDECLINE

若 Server 收到 DHCPDECLINE 表示 Client 發現 Server 所提供的 IP 已經為其他的機器所使用，Server 應立即將此 IP 標示為 ”in use ”的狀態，並通知網路管理員此一問題。

2、3、4 DHCPRELEASE

若租約尚未到期, 而 Client 已不再使用此 IP, 則 Client 可以送出 DHCPRELEASE, 當 Server 收到此封包時應立即將此 IP 標示為 ”not allocated”, 如此 Server 才可以再將此 IP 位址配置給其他的使用者。

2、3、5 DHCPINFORM

Server 收到 DHCPINFORM 後, 將必要的參數放進 Option 中, 並以 Unicast 的方式回應 DHPCACK。

2、4 DHCP Client Behavior

圖 2.4-1 為 Client 的狀態轉移圖, 以顯示 Client 於 DHPC 中的工作流程, 本節即以此圖說明 Client 的 Behavior

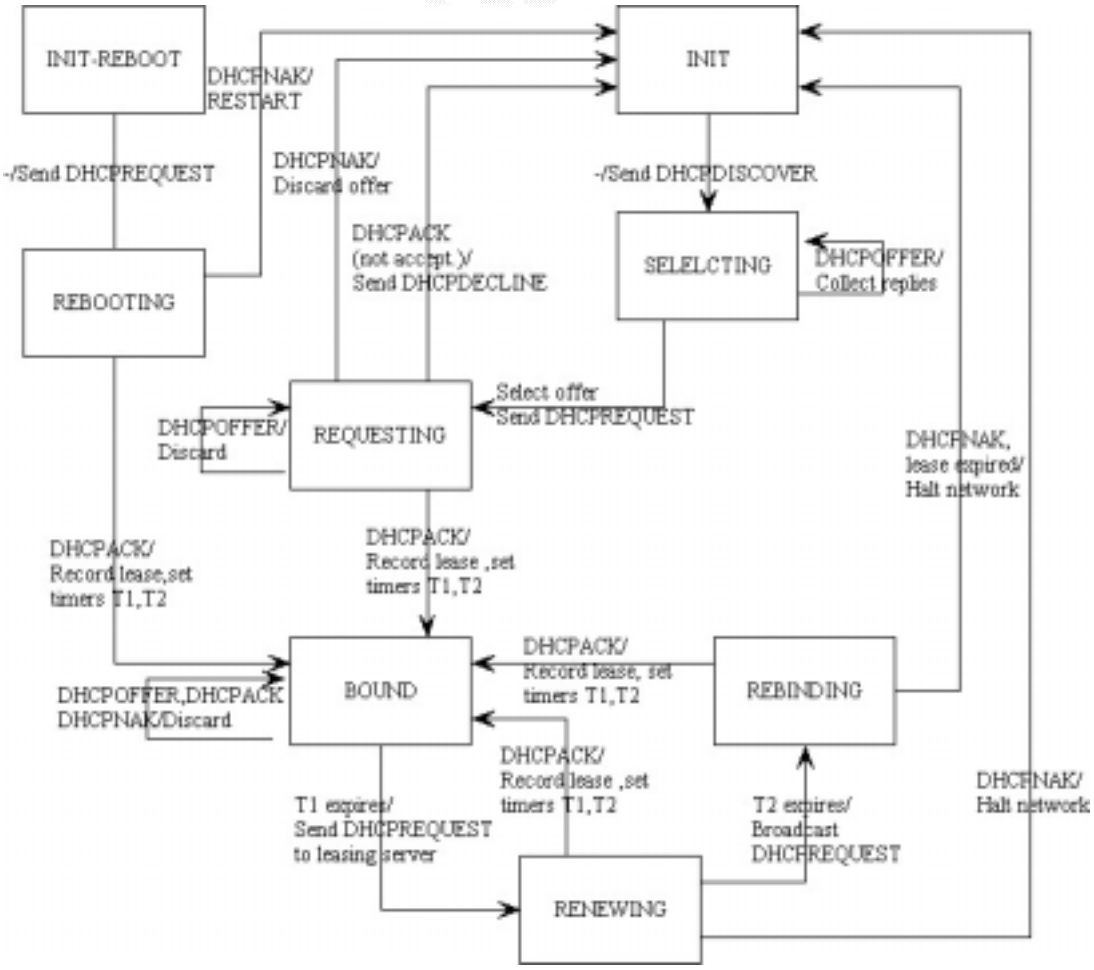


圖 2.4-1 DHCP Client 的狀態轉移圖

2、4、1 Client Begins in INIT State

在送出 DHCPDISCOVER 之前，Client 必須設定 ciaddr 為 0x00000000, 並將自己的 Hardware address 填入 chaddr, Client 也可以將欲取得的 IP 與租約(lease)時間分別放入 Request IP address 欄位與 IP address lease time 中。Client 必須隨機產生一個 transaction identifier 並把它填入 xid 中，至此 Client 可以將 DHCPDISCOVER 以廣播(broadcast)的方式發送出去，當封包送出之後，Client 由 INIT state 進入 SELECTING state。

若 Client 收到的 DHCPOFFER 封包中 xid 與送出的 DHCPDISCOVER 中的 xid 不同的話，Client 必須忽略此一封包。

在經過一定的時間之後，Client 必須選定一個 DHCPOFFER 封包並進入 REQUESTING state，在 REQUESTING state 時 ，Client 必須將 DHCPOFFER 中 Server Identifier 紀錄下來填入 DHCPREQUEST 封包中，並將 transaction identifier 填入 xid 中, 再以廣播的方式送出 DHCPREQUEST。

只要 Client 一旦收到 DHCPACK 即進入 BOUND state 完成一個 DHCP 的工作流程，一般而言，Client 在進入 BOUND state 之後應該再確定現在使用的 IP 未被其他的機器使用。若 Client 收 DHCPNAK 則重新回到 INIT state 並重新送出 DHCPDISCOVER。

2、4、2 Client Begins in INIT-REBOOT State

若 Client 是由 INIT-REBOOT 開始，Client 必須將現在的 IP 填入 Request IP address 欄位中，隨機產生一個 transaction identifier 填入 xid 中，Server Identifier 必須未被填入，而後再以廣播的方式送出 DHCPREQUEST 並進

入 REBOOTING state。

只要 Client 收到 xid 與之前送出的 xid 相同的 DHCPACK，Client 即進入 BOUND state，並記錄下租約時間。

2、4、3 Reacquisition and Expiration

因為每一配置(assign)的 IP 都有其租約(lease)時間，時間一旦到期，Server 會自動收回 IP，故 Client 為了確保機器的正常運作必須設定兩個計時器(timer)：T1、T2，T1 時間為租約時間的 0.5 倍，T2 時間為租約時間的 0.875 倍，一旦 Client 進入 BOUND state 即設定此兩個計時器，並開始計時，當 T1 時間到時，Client 即進入 RENEWING state，此時 Client 必須設定 ciaddr 為現在使用的 IP，Server Identifier 必須未被填入，再以 Unicast 的方式發送 DHCPREQUEST。

若收到 Server 回應的 DHCPACK 則 Client 回到 BOUND state。但若 Client 在 T2 時間到之前都沒有到 Server 回應的 DHCPACK，則 Client 進入 REBINDING state 並以 Broadcast 的方式送出 DHCPREQUEST 封包。

第三章　Attacks on the DHCP

3、1 DHCP 協定之漏洞

在第二章中我們已詳細說明 Server 與 Client 的 Behavior 及封包的各個欄位，在這眾多的欄位中我們可以發現只有 chaddr(Client Hardware Address)與 xid(transaction identifier)是 Server 唯一可以用來識別 Client 的兩個欄位，但 xid 是由 Client 隨機產生的，在安全性上無法發揮功能，如此一來，Server 只有靠 Hardware Address 來區別各個 Client 端的請求，換句話說，即使我們只有一台電腦，只要送出的兩個封包中 chaddr 的值各不相同，則 Server 就會將這兩個封包當作是兩個 Client 端的請求來處理，故 Server 會配置(assign)兩個 IP 給我們，依此類推，只要我們能夠不斷送出不同 chaddr 的封包，Server 就會不斷的配置 IP 給我們，直到 Server 再也沒有可用的 IP 為止，如此真正有需要使用 IP 的其他用戶即無法從 Server 取得 IP，即可達到癱瘓 Server 的目的

但上述的做法尚且只能達到暫時性的癱瘓 Server，因為 IP 皆有其租約時間，只要時間一到期，client 沒有繼續向 server 提出續約，IP 即會被 Server 收回，Server 又可以恢復正常的運作，因此攻擊者的程式尚需要能夠針對其所取得的 IP 一個一個做如章節 2、4、3 所述 Reacquisition(Renew)的動作

3、2 如何攻擊 DHCP Server

在說明攻擊 DHCP 之前我們必須先了解網路卡上的 Promiscuous Mode。網路卡在一般的模式下，只有封包上 MAC address 與網路卡上的 MAC address 相同的封包才能通過網

路卡，但若網路卡是 Promiscuous Mode 下，則不論封包的 MAC address 為何，此封包皆可以通過網路卡進入主機內。

如 3、1 節所述，因為 Hardware address 是 Server 唯一可以用來識別 Client 的依據，所以只要 Client 的程式可以隨機產生一個 Hardware address 並將它放進 DHCPDISCOVER 封包中，此外我們還必須設定一個 dhcpdiscover_counter 變數，用於紀錄我們送出的 DHCPDISCOVER 封包個數，若我們已經連續送 4 個 DHCPDISCOVER 但 Server 均未再回應 DHCPOFFER 則我們就認為 Server 已經沒有可在配置的 IP，藉此來判斷攻擊的成功與否。當我們收到 DHCPOFFER 時再依照其訊息送出 DHCPREQUEST，此處要注意的是 DHCPREQUEST 的 chaddr 的值必須與 DHCPDISCOVER 一致，如此才可以通過 Server 的檢試，只要一收到 DHCPACK 即表示我們已經從 Server 端取得一個 IP，我們只要再重複上述的動作，Server 就會不斷配置 IP 給我們，如此即可以達到攻擊 Server 的目的，但取得 IP 的過程中，我們必須將取得的 IP 與其所以對應的 Hardware address 紀錄下來以供稍後我們要做 Renew 時所需的資訊。圖 3.2-1 顯示攻擊程式的執行流程。

在開始攻擊之前我們必須確定我們的網路卡已經開到 Promiscuous Mode，因為 Server 的回應均是以 Unicast 的方式回應的，所以 Server 會針對我們隨機產生的 Hardware address 回應封包，若我們未將 Promiscuous Mode 打開則我們就沒有辦法收到 Server 回應的訊息。

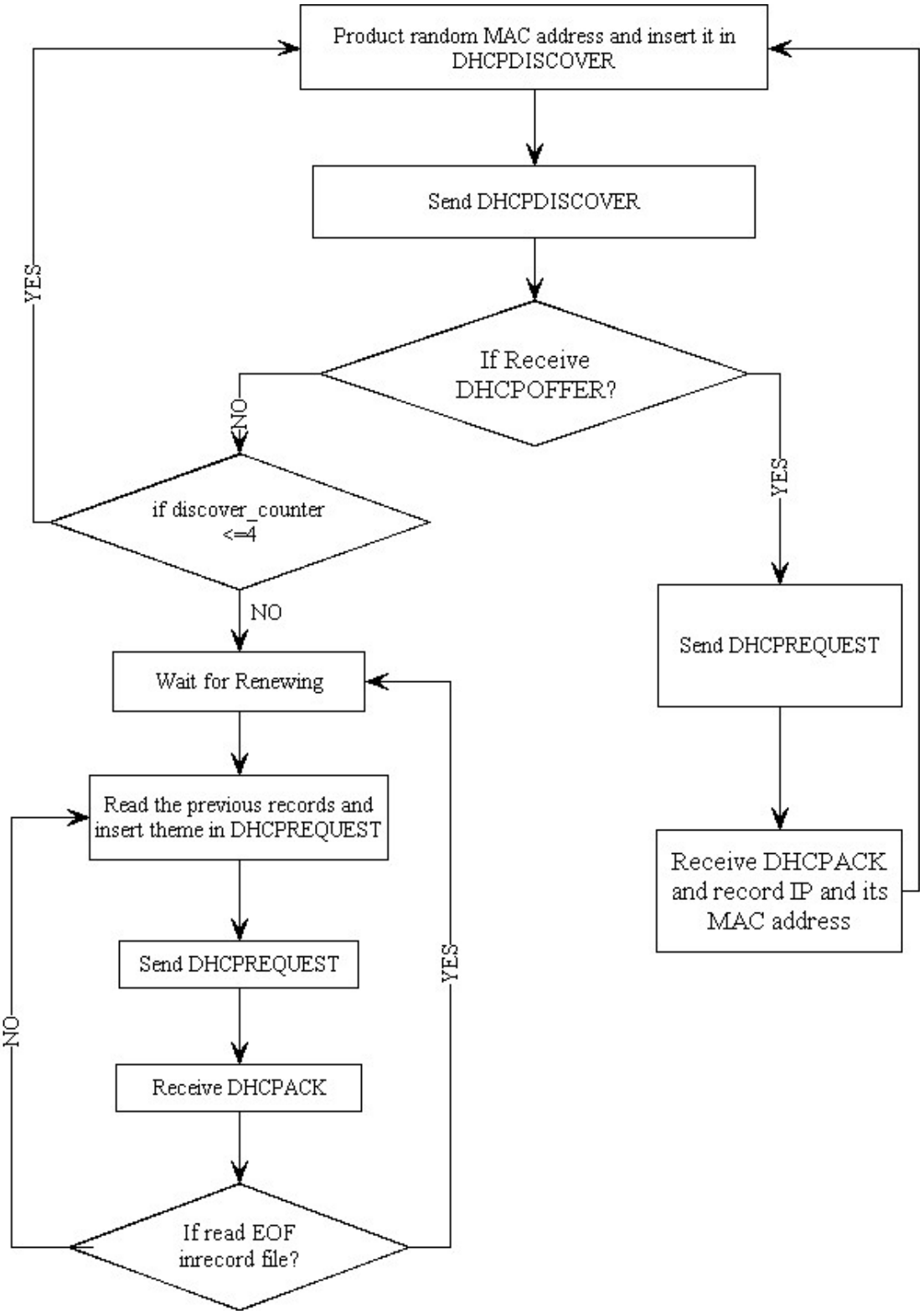


圖 3.2-1 攻擊程式的執行流程圖

3、3 DHCP Server 攻擊的實做

本研究所使用的程式為 ISC(Internet Software Consortium)於 2002 年所開發的 DHCP Server 與 Client 端程式。Server 的程式未經任何修改，而 Client 端程式已修改成可以利用第三章所描述之漏洞攻擊 Server，其攻擊目的在於取得 Server 端的所有 IP，使其無可用的 IP address 配置給其他的 Client 端用戶。以下圖片為攻擊程式執行的過程及執行結果

圖 3.3-1 啟動 DHCP Server

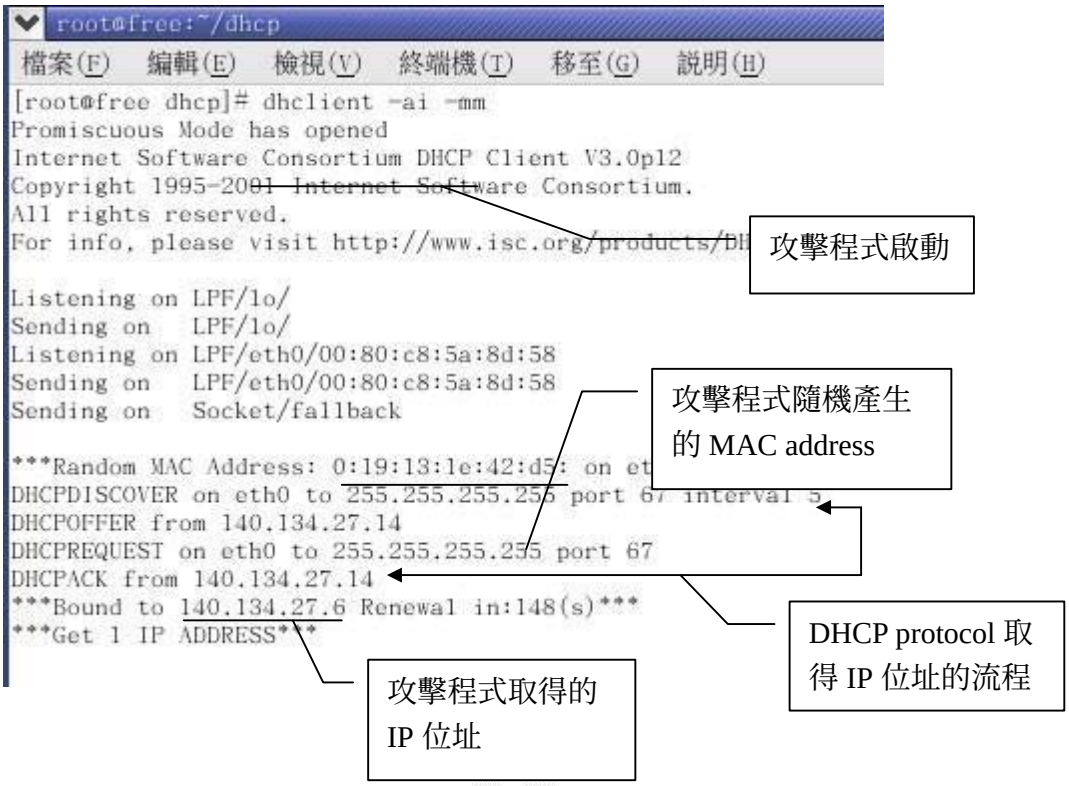


圖 3.3-2 攻擊程式取得第一個 IP 位址

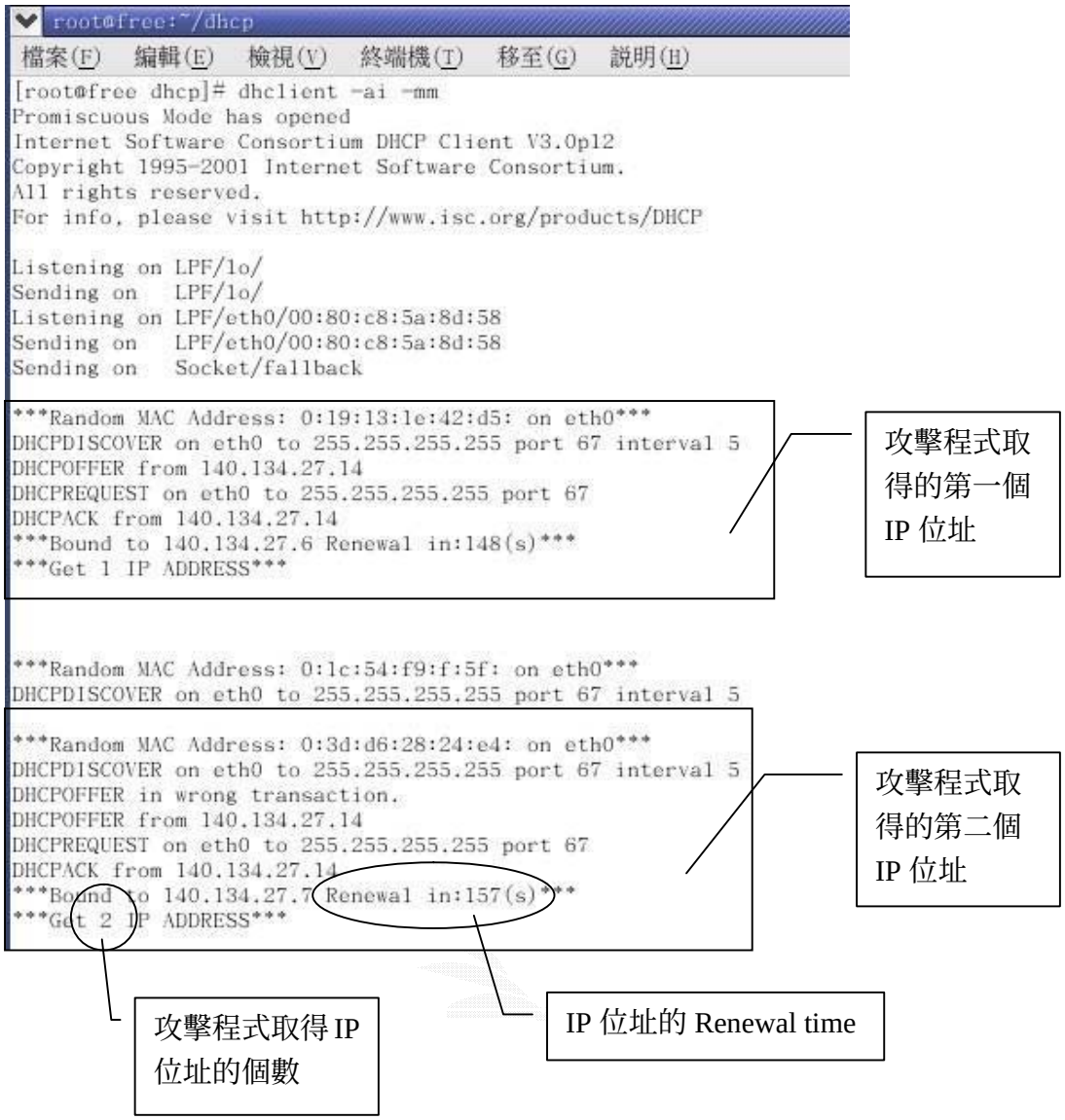


圖 3.3-3 攻擊程式取得第二個 IP 位址

第三個以後的 IP 取得方式均與圖 3.3-2 與圖 3.3-3 的取得過程相同，因此本文在此不將攻擊程式每一個 IP 位置的取得過程一一說明。

在攻擊程式中以連續送出四個 DHCPDISCOVER 封包但未收到 Server 回應的 DHCPOFFER 封包作為攻擊結束與否的依據。在 Server 端程式的畫面中可以清楚的看到 Server 印出”no free lease”的訊息，表示 Server 所有可用的 IP 位址已被攻擊程式取走，故無 IP 可用。

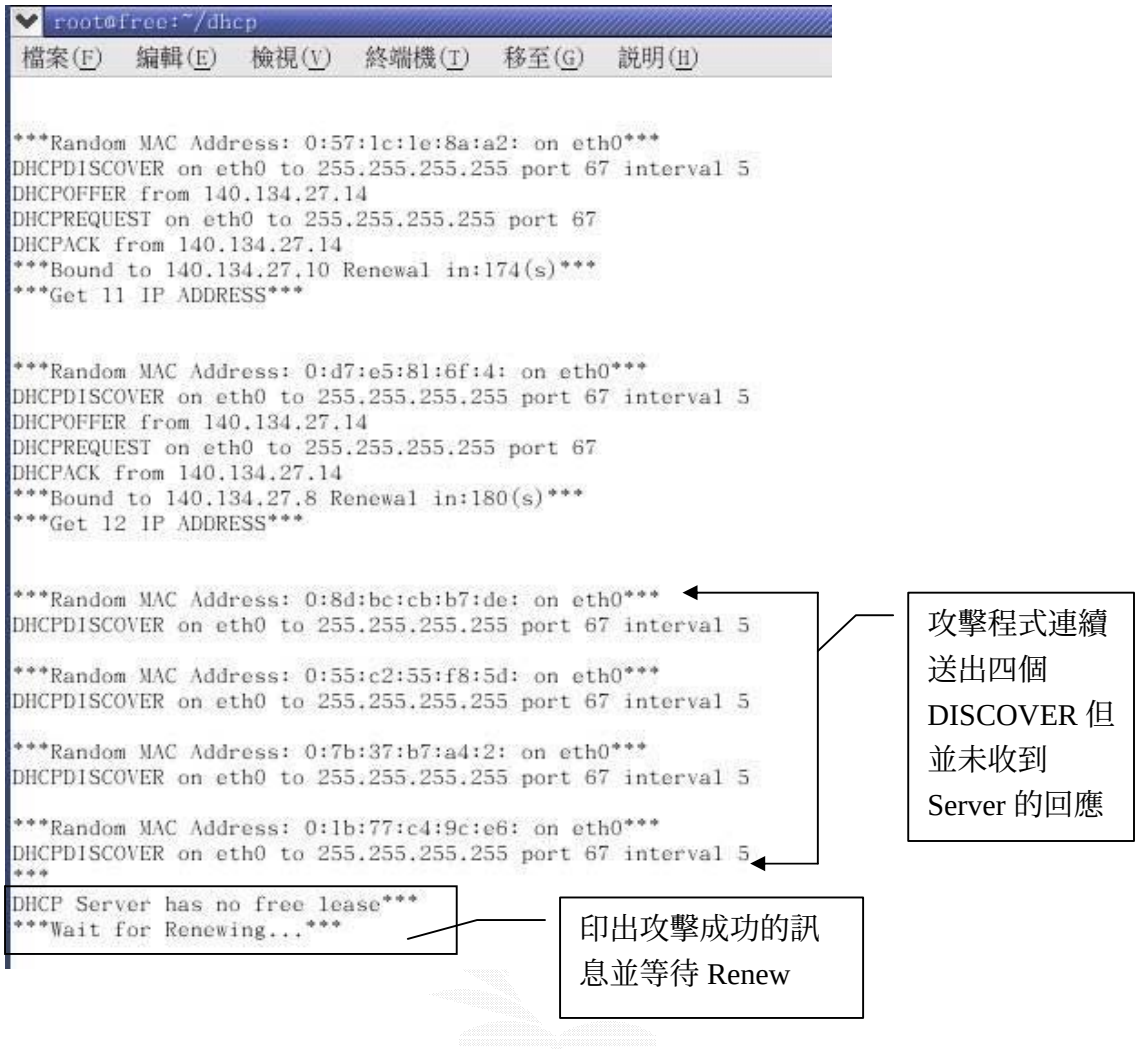


圖 3.3-4 攻擊程式成功取得所有 IP 位址

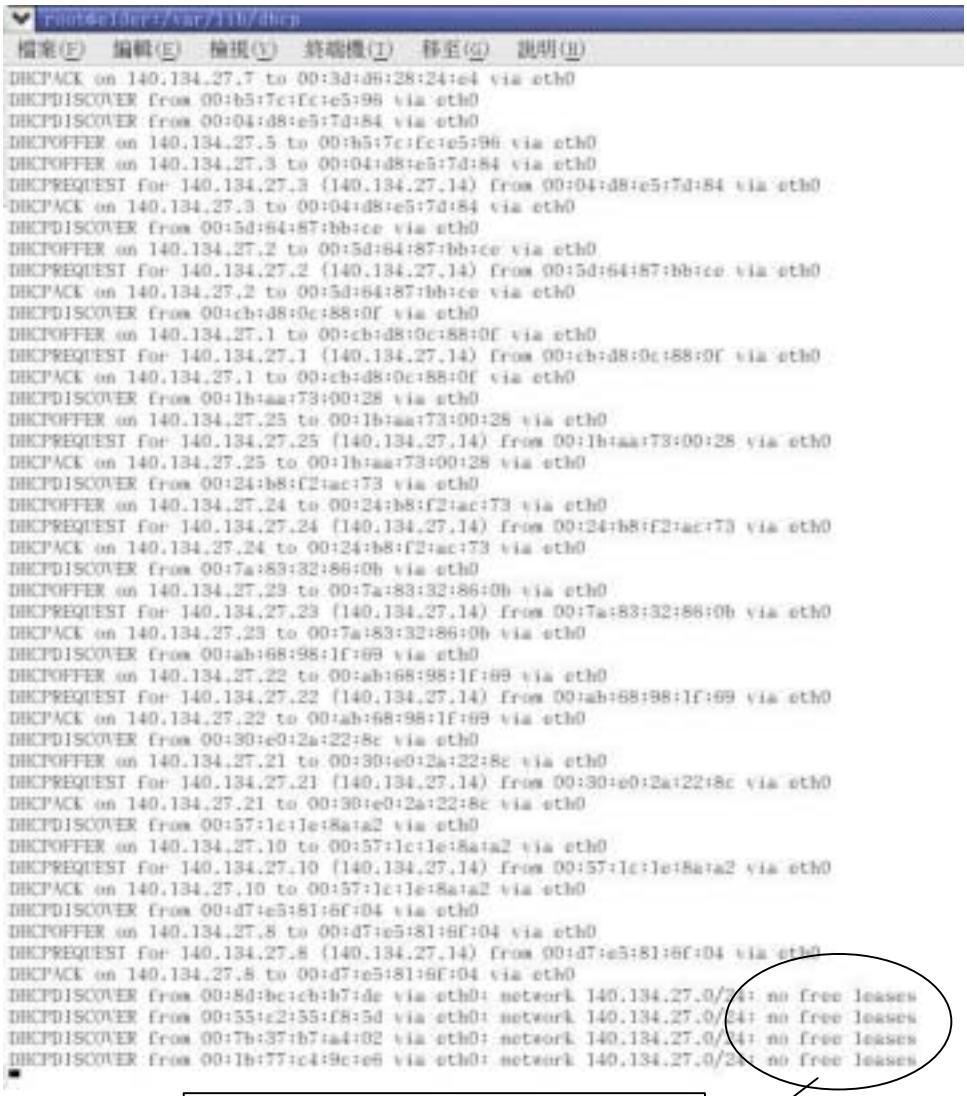


圖 3.3-5 攻擊後的 DHCP Server

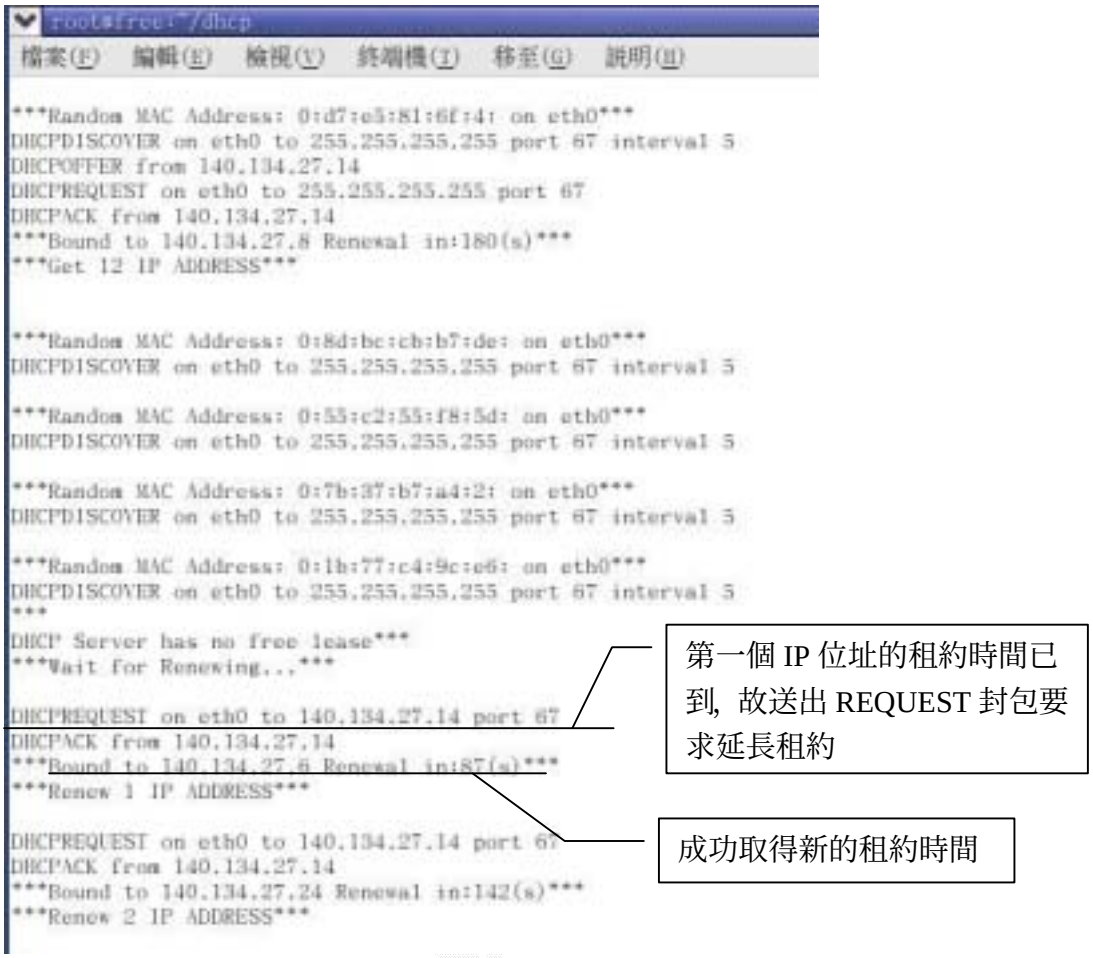


圖 3.3-6 攻擊程式執行 Renew 功能

第四章 DHCP Server 的保護

本研究所探討的 DHCP 漏洞乃因為 Hardware address 為 Server 唯一可識別 Client 的依據，但 Hardware address 又是 Client 端程式可以隨機產生的，故我們無法從協定的角度來做防護，只有利用 DHCP 以外的機制來彌補漏洞。本研究在此提出下列幾種可能的 DHCP Server 保護的方法。

4、1 網路卡實體位址（MAC ADDRESS）管理

基本上 DHCP protocol 中並沒有針對"使用者"來認證，而是針對網路卡來認證，大部分的 DHCP Server 都可以設定僅僅接受某些卡號的連線，網路卡號必須先由網路管理者註冊後方可使用該無線網路基地台。以 ISC 提供的程式為例，它提供一個 Server 的設定檔，使網路管理員可以設定哪些 IP 只能配置給哪些特定的 Hardware address，如此即使 Client 可以隨機產生 MAC address 但因其隨機的 MAC address 無法與設定檔中所指定的 MAC address 相吻合，故 Server 不會將 IP 配置給 Client，故可達到保護 Server 的目的。

4、2 802.1x 使用者認證

IEEE 802.1x 於 2001 年七月獲 IEEE 核可，是目前無線網路上最理想的身分認證與密鑰管理協定。透過 802.1x 能將無法通過認證的使用者隔絕於網路之外，使其無法利用任何網路資源。802.1x 原本是為了"有線"的乙太網路來設計以"埠"(port)為基礎的認證機制，而在無線網路的應用上，利用其認證機制(可結合後端之 RADIUS(Remote Access Dial

In User Service)認證伺服器)來確認使用者之身分，並利用"動態"WEP 加密來防止資料被竊聽。

802.1x 的主要成員包括下列四者：

○ Authenticator：

要求並且接受未受信任端網路節點的認證請求的實體。

○ Supplicant：

請求網路存取權，並且需接受 Authenticator 的認證稽核。

○ Port Access Entity(PAE)：

具有 Authenticator，Supplicant 或兩者的功能（也是指 AP 的初始狀態，因為 AP 本身也要通過 RADIUS 認證才能夠當作 Authenticator)。

○ Authentication Server：

對 Authenticator 提供身分認證服務的實體，可能與 Authenticator 存在同一主機內，但大多數的狀況下是一台獨立的伺服器。

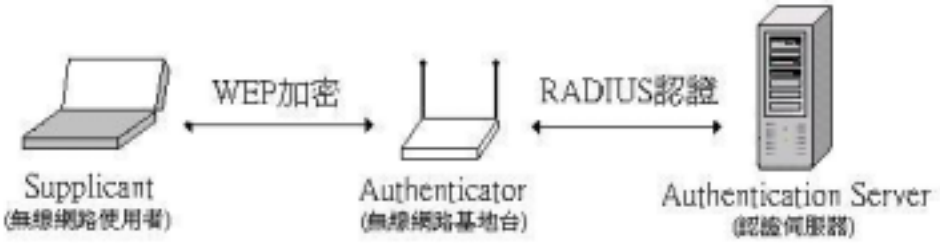


圖 4.2-1 802.1x 的架構

在正式介紹無線網路的認證機制之前，在無線網路安全架構下(802.11i)將會引入 802.1x Port-Based Network Access Control 的機制。當 Access Point 與 Radius Server

進行 Radius Protocol 的協議流程時，如果 Access Point 收到 Access-Reject 的封包，就表示該使用者認證失敗，被 Radius Server 拒絕登入，如果 Access Point 收到 Access-Accept，就表示該使用者認證成功，Radius Server 同意其登入網域，之後只要是由該使用者經過認證的主機所送出的封包，經過 Access Point 時就會放行通過，此種機制即稱作 Port-Based Network Access Control。透過這樣的機制，Access Point 可以用來過濾沒有經過後端認證伺服器(Radius Server)許可的使用者封包。

無線網路認證的機制包含著 EAPOL、EAP 與 Radius Protocol。以下就以這三種機制分別敘述：

1 EAPOL(EAP Over Lan)：

EAPOL 是屬於無線網路協定裡 IP Layer 以下的通訊協定，可以讓使用者在未經過 EAP 認證登入以前的封包，透過 EAPOL 傳送，經由 Access Point 與後端 AAA (Authentication, Authorization, and Accounting) Server 進行認證。

2 EAP(Extensible Authentication Protocol)：

EAP 是 PPP(Point-to-Point Protocol) 的延伸，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，基於不同的安全需求與使用考量，EAP 提供了不同的認證方式，主要有 MD5-Challenge、TLS(Transport Level Security)。

○EAP-MD5 CHAP(Extensible Authentication Protocol- Message Digest5 Challenge Handshake Authentication Protocol)：

其中 Client 端一開始會先送出 EAPOL-Start 的訊息，如果網路上有支援 802.1x 服務的 Access Point，該 Access Point 一收到 EAPOL-Start 的訊息就會透過 EAPOL 送出 EAP-Packet，也就是 EAP-Identity 用來要求使用者確認身份，使用者端程式收到 EAP-Identity 之後，就會要求使用者輸入帳號與密碼。

使用者輸入之後，就會先把帳號送給 Access Point，Access Point 與後端網路上的 Radius Server 使用的通訊協定為 Radius Protocol，在收到使用者的 EAP 訊息後，就會把 EAP 訊息加到 Radius Protocol 的 Attribute 後送出給 Radius Server。再來 Radius Server 會送出 Access-Challenge(Radius Protocol) 給使用者，使用者端的程式收到後，就會把使用者的密碼經由 Hash 後產生的結果透過 Access Point 以 Access-Request 送回給 Radius Server。在 Radius Server 端收到這項要求後，就會根據自己所管理的使用者帳號，根據其密碼也同樣經過 Hash 處理比對兩者是否一致，如果一致的話，就會送出 Access-Accept 的訊息給 Access Point，如果兩者不同，表示該使用者的身份確認上有誤，就會送出 Access-Reject 給 Access Point，當 Access Point 收到該訊息後，就會對使用者送出 EAPOL-Fail 的訊息，此時使用者端的 802.1x 程式就會顯示出無法登入的訊息，並且要求使用者再次輸入正確的使用者帳號與密碼，便於進行下一次的登入嘗試。圖 4.2-2 顯示整個 EAP-MD5 的運作流程。

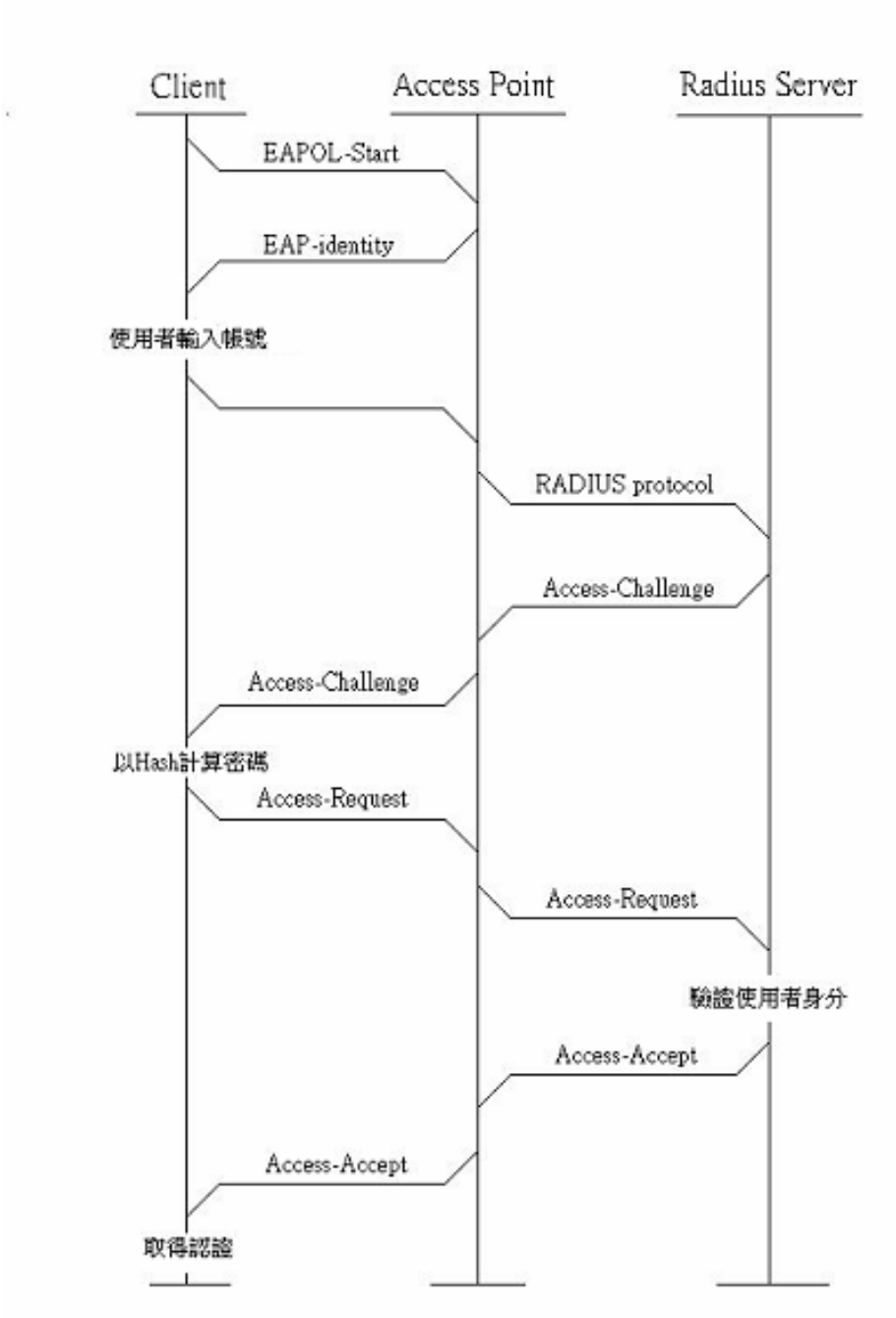


圖 4.2-2 EAP-MD5 的運作流程

○EAP-TLS(Extensible Authentication Protocol-Transport Level security)：

EAP-TLS 以 Certificate 方式認證，也就是說每個使用者在使用 EAP-TLS 認證的服務以前，都必須要先取得網路上負責認證 CA 的 Certificate，Certificate 的存放可以透過 Smart Card，磁片 或是經由網路下載後安裝。

EAP-TLS 的好處在於使用者端與 Radius Server 端可以共同產生一把用來加密無線網路資料的 WEP Session-Key，Access Point 端收到 Radius-Acess 的訊息時，其中就會有一個欄位夾帶著 Session Key，Access Point 端要透過與 Radius Server 彼此共同擁有的 Shared Key 與其他資料，來解開這把 Session Key。之後根據要指定使用者使用不同的 Brocast Key 與 Session Key 的考量，分別送出設定使用者這兩把 Key 的 EAPOL 封包。

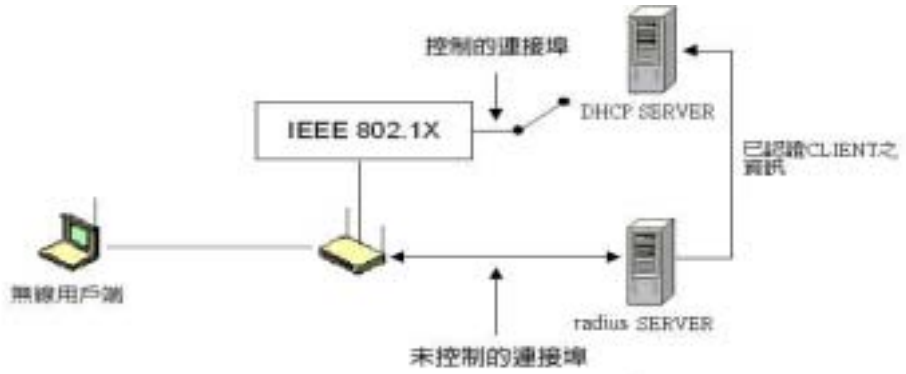
之後使用者端與 Access Point 就會透過設定好的 WEP Key 來加密通訊資料，所以說透過這樣的方式，我們可以定義出動態設定 WEP Key 的機制，也就是說可以週期性的送出要 求更改 WEP Key 的 EAPOL 封包，讓使用者端與 Access Point 兩邊彼此都擁有不固定的 WEP Key 加密機制。

3 Radius(Remote Authentication Dial In User Service) Protocol：

主要用來提供 Authentication 機制，用來辨認使用者的身份與密碼，確認通過之後，經由 Authorization 授權使用者登入網域使用相關資源，並可提供

Accounting 機制，保存使用者在網路上的活動記錄。RADIUS 以 MAC address 的作為使用認證資訊以批准或拒絕進入網路。Access Point 的作用如同一個 RADIUS 用戶，它可收集用戶認證資訊並把這些資訊傳送到指定的 RADIUS 伺服器上。RADIUS 伺服器的作用一是接收用戶的各種連接請求；二是處理各種請求以鑒別用戶；三是通過向用戶提供服務所必須的資訊對 Access Point 做出回應。Access Point 對 RADIUS 伺服器的回復回應起作用，許可或拒絕對網路的接入。各種認證特徵內嵌於 RADIUS 伺服器中。在 Access Point 和 RADIUS 伺服器之間的各種處理程式都通過使用一個從不在網路上傳送的共用密碼進行認證，而各種密碼都是經過加密的。

當 Client 經由上述的方法向 RADIUS Server 取得認證的同時，RADIUS Server 也將其認證資訊(如：Client 端的 MAC address、通過認證的 Ticket)傳送給 DHCP Server，以告知 DHCP Server 某個 Client 的 MAC address 必須對應到 RADIUS 所發出的 Ticket，如此即使攻擊程式可以產生隨機的 MAC address 但因為這些 MAC address 並沒有經過 RADIUS 認證所以沒有可通行的 Ticket，所以 DHCP Server 也不會配置 IP 位址給 Client, 如此以達到保護 DHCP Server 的目的。



802.1X 之保護架構圖

4、3 Authentication for DHCP Messages：

RFC 3118 定義了一種新的 DHCP 認證方式，可同時提供實體認證(entity authentication)和訊息認證(message authentication)，來確保

DHCP message 的來源和內容能正確無誤以避免一些常見的攻擊。

DHCP message 的格式和欄位在前面已經介紹過了，其中有一個欄位稱為 options, 是 DHCP protocol 指派給用戶端的位址設定參數。雖然該擴充選項可以由廠商或使用者自行新增, 但是大部分的內容均已事先根據 RFC 1542 所定義的選項參數完成定義。而 RFC 3118 所討論的即是對這欄位加以應用，將所謂的 DHCP 認證選項(DHCP authentication option)塞進 options 欄位裡, 來實做 DHCP 的認證。

○DHCP 認證選項的格式(Format of DHCP authentication option)：

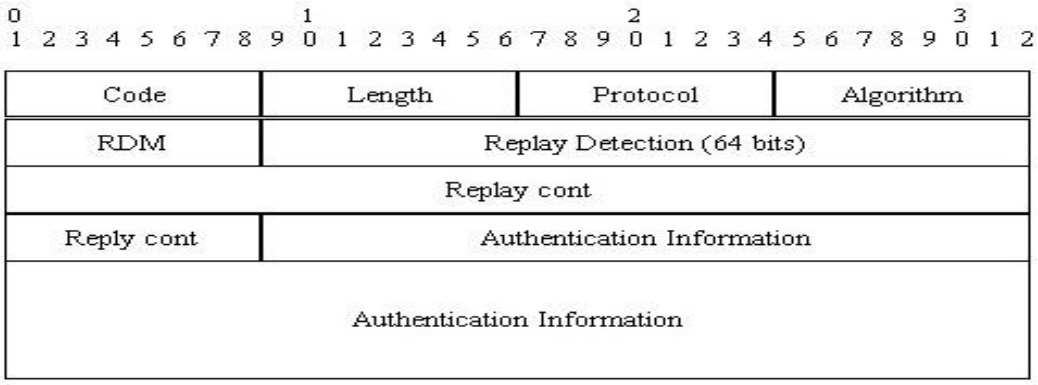


圖 4.3-1 Format of DHCP authentication option

Filed	Description
Code	For authentication option is 90.
Length	Contain the length of Protocol, RDM, Algorithm, Replay Detection and Authentication Information fields in octets.
Protocol	Define the particular technique for authentication option.
Algorithm	Define the specific algorithm according to the Protocol field.
RDM	Determine the type of replay

(Replay Detection Method)	detection used in the Replay Detection field.
Replay Detection	The field is per the RDM in use.
Authentication Information	The field is per the Protocol in use.

表 4.3-1 Fields of DHCP authentication option

其中 Protocol filed 主要有兩個數值分別是 0 和 1，各自代表兩種

不同的認證方式。描述如下：

○If Protocol is 0：

此時 Authentication Information field 握有一簡易的組態標記(configuration token)，該組態標記是個不透明的(opaque)，未加以編碼的(unencoded)的值(value)，發送端和接收端(sender and receiver，在此先不管是 Client 或 Server)之間都能知道該值。發送端將 configuration token 插入 DHCP message，接收端收到後從 DHCP message 取出該 configuration token 並配對(match)為共享標記(shared token)，這樣以後，如果有來自任何發送端的 DHCP message 其 configuration

token 如未與 shared token 符合的話，接收端將丟棄該 DHCP message。事實上 Configuration token 可能使用了純文字的符號密碼，只提供了陽春的 entity authentication，而且沒有提供 message authentication，不能做到完整的保護。

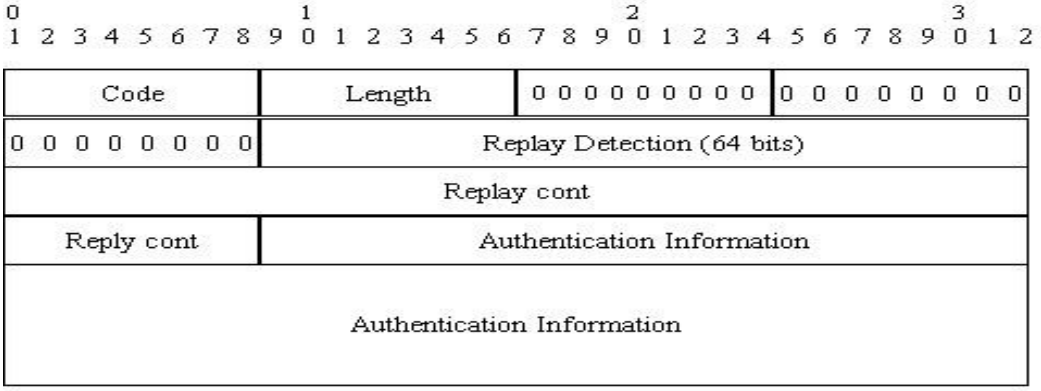


圖 4.3-2 when protocol field is 0

○If Protocol is 1：

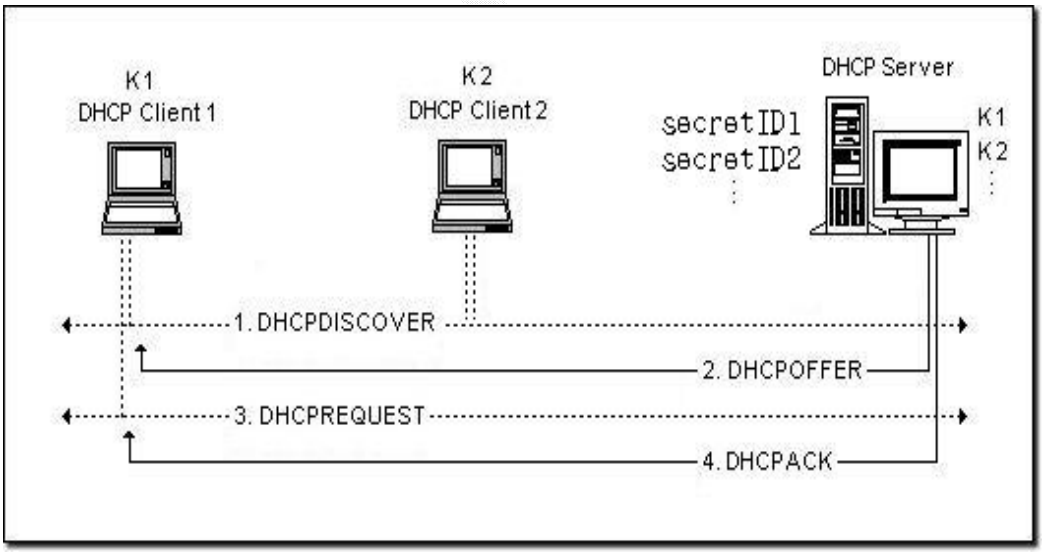


圖 4.3-3 Interation between DHCP Client and Server using protocol 1

在該 Protocol 裡，DHCP message 使用了一種稱為延遲認證(delayed authentication)的機制。以下就 Server 和 Client 之間的行為來分別描述 DHCP message：

1.DHCPDISCOVER：

一開始，Client 會藉由發送 DHCPDISCOVER 和一個能夠向 Server 證明 Client 本身是獨一無二的的 ”client identifier option ”(文中並未說明是如何傳遞該 client identifier option 給 Server)來向 Server 要求認證(authentication)。

2.DHCPOFFER：

Server 收到 DHCPDISCOVER 並確認為獨一無二後，會先針對該 Client 選擇一個唯一的 key，K，每一個 K 有一個唯一的 secret ID, 也就是 unique identifier, Server 會將 K 和 unique identifier 紀錄在本機電腦，並透過 ”特殊安全管道(out-of-band) ” 的方式將 K 傳送給 Client，再來會使用 K 來編碼(encode)一個臨時值(nonce value)來作為訊息認證碼(message authentication code, MAC)，該訊息認證碼可使用 K 及 HMAC generation algorithm 和 the MD5 hash function 來計算出。然後送出包含 Authentication Information 的

DHCPOFFER 給 Client。

3.DHCPREQUEST：

Client 收到 DHCPOFFER 後, 會使用 K 來解碼 DHCPOFFER 的 Authentication Information，並進行所謂的 Message validation test，也就是算出 Authentication Information 裡面的 MAC 值, 如果算出來的 MAC 與本機算出的 MAC 不符的話, Client 會丟棄該封包；否則 Client 將選擇該 DHCPOFFER 提供的組態配置(configurations)，並使用 K 編碼(encode)一個包含 Authentication Information 的 DHCPREQUEST 並送給 Server。

4.DHCPACK：

Server 收到 DHCPREQUEST 後利用 secret ID 來得知是哪個 K，再來同樣使用 K 來進行 Message validation test，如果通過，Server 同樣使用該 K 編碼一個包含 Authentication Information 的 DHCPACK 並送出給 Client。

Client 在收到 DHCPACK 後同樣使用 K 來進行 Message validation test，如果通過，Client 則使用 Server 提供的 configuration。

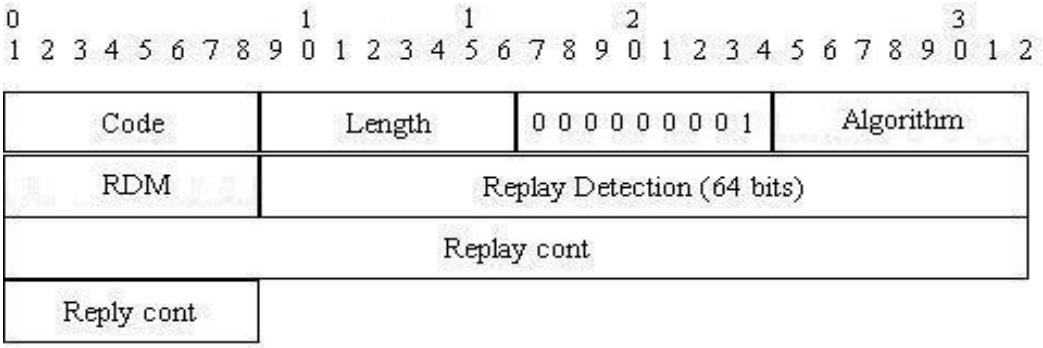


圖 4.3-4 The format of the authentication request in a DHCPDISCOVER or a DHCPINFORM

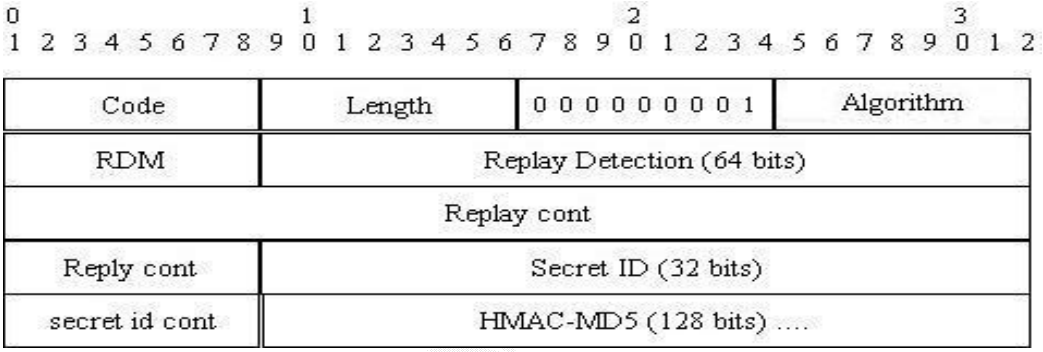


圖 4.3-5 The format of the authentication information in a DHCPOFFER, DHCPREQUEST or DHCPACK

Field	Description
K	A secret value shared between the source and destination of the message; each secret value has a unique identifier (secret ID).

Secret ID	The unique identifier for the secret value used to generate the MAC for this message.
HMAC-MD5	The MAC generating function.

表 4.3-2 key words used in protocol 1

5.Client 的其他狀態：

不管是在 INIT-REBOOT state、RENEWING state、REBINDING state、或 DHCPRELEASE message，Client 都必須使用 K 來產生有 Authentication Information 的 DHCP message 並送出給 Server。

4、4 DHCP Server 保護的結論

在上述章節中，本研究提出了三種 DHCP Server 保護的方法，其中第一種是利用網路卡號的管理作為保護，第二是利用 IEEE 802.1x 協定作為保護，第三是 RFC3118 所提出的認證機制。

在這三種方法中，第二種方法需要多餘應體設備支援(如：Access Point)，且在 802.1x 中並未定義 RADIUS Server 如何與 DHCP Server 傳送訊息，因此使用 802.1x 作為認證方法可能導致 DHCP Server 無法知道 RADIUS 的認證訊息以及 Server 與 Client 間分享的 key 值為何。

第三種方法雖然的確可以在現有的協定上做到認證的功能，但至今為止尚無人將 RFC3118 中所提到的機制寫成可用

的程式，因此 RFC3118 至今仍純屬理論，而無實際的產品出現。

綜觀以上除了第一種方法外，其他的保護方式似乎都仍有不足。而第一種方法雖然可以做到保護 Server 的目的，但這項功能並非在 RFC2131 中明確規定必須提供的功能，因此也無法保證所有的 DHCP 程式都有支援此項功能，況且以網路卡號管理作為保護的方法，過程繁瑣且易於出錯，因此這些種種的問題都還有待相關的研究機構解決。

4、5 DHCP Server 保護的實做

本研究在此共提出了三種 DHCP Server 保護的機制，但因 IEEE 802.1x 與 Authentication for DHCP message 此兩種方法仍然存在著許多問題，因此本研究僅實做以網路卡號管理作為保護的方法。以下即是實做過程。

下圖即為 DHCP Server 的設定檔

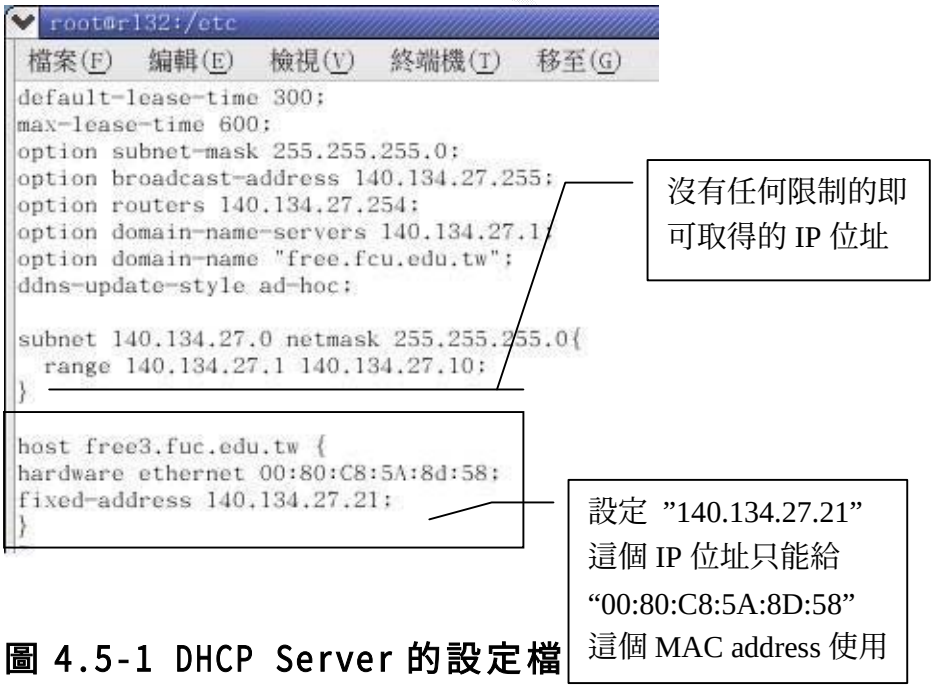


圖 4.5-1 DHCP Server 的設定檔

在上圖中 DHCP Server 的設定檔中可以明確的看到"140.134.27.21"這個 IP 位址只能給"00:80:C8:5A:8D:58"這個 MAC address 使用，因此攻擊程式僅能拿到 "140.134.27.1"到"140.134.27.10"這個範圍裡面的 IP 位址。

圖 4.5-2 攻擊程式攻擊有保護的 DHCP Server

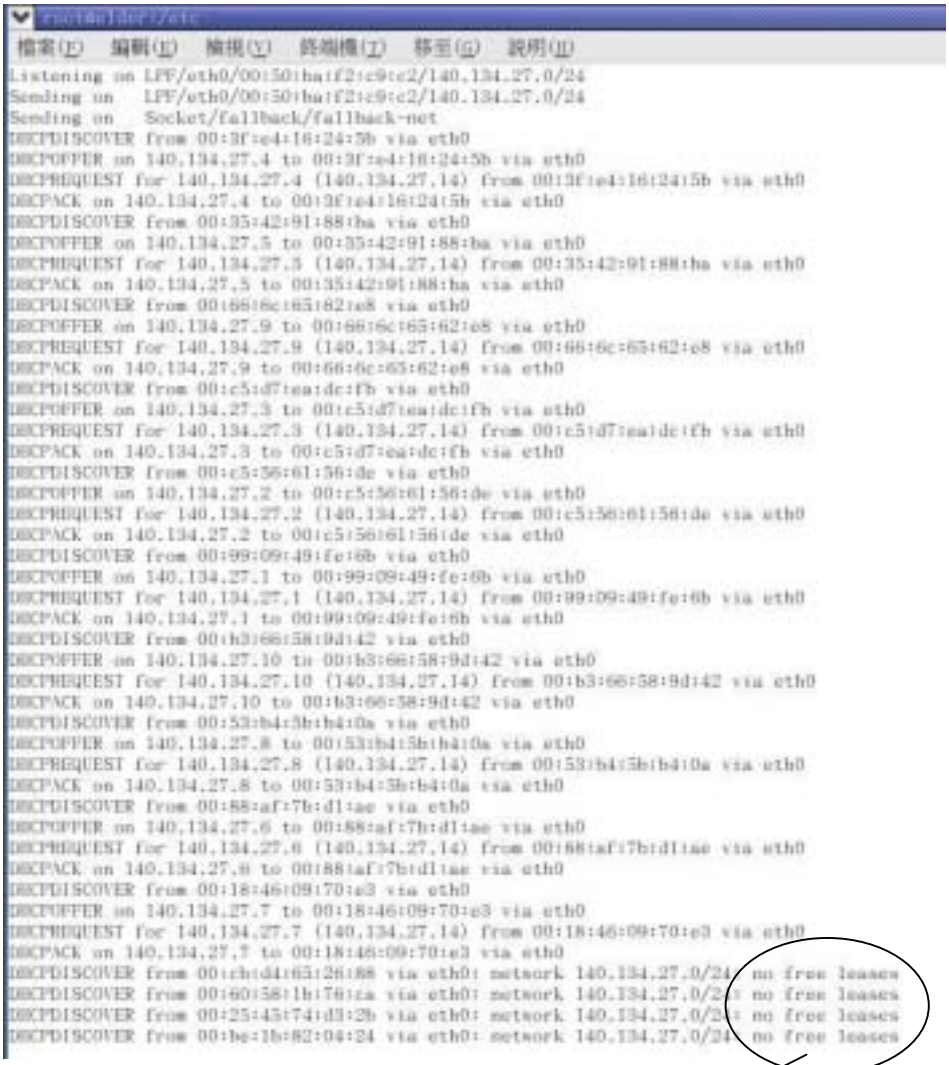


圖 4.5-3 被攻擊後的 Server

圖 4.5-4 取得 IP 位址的合法 Client

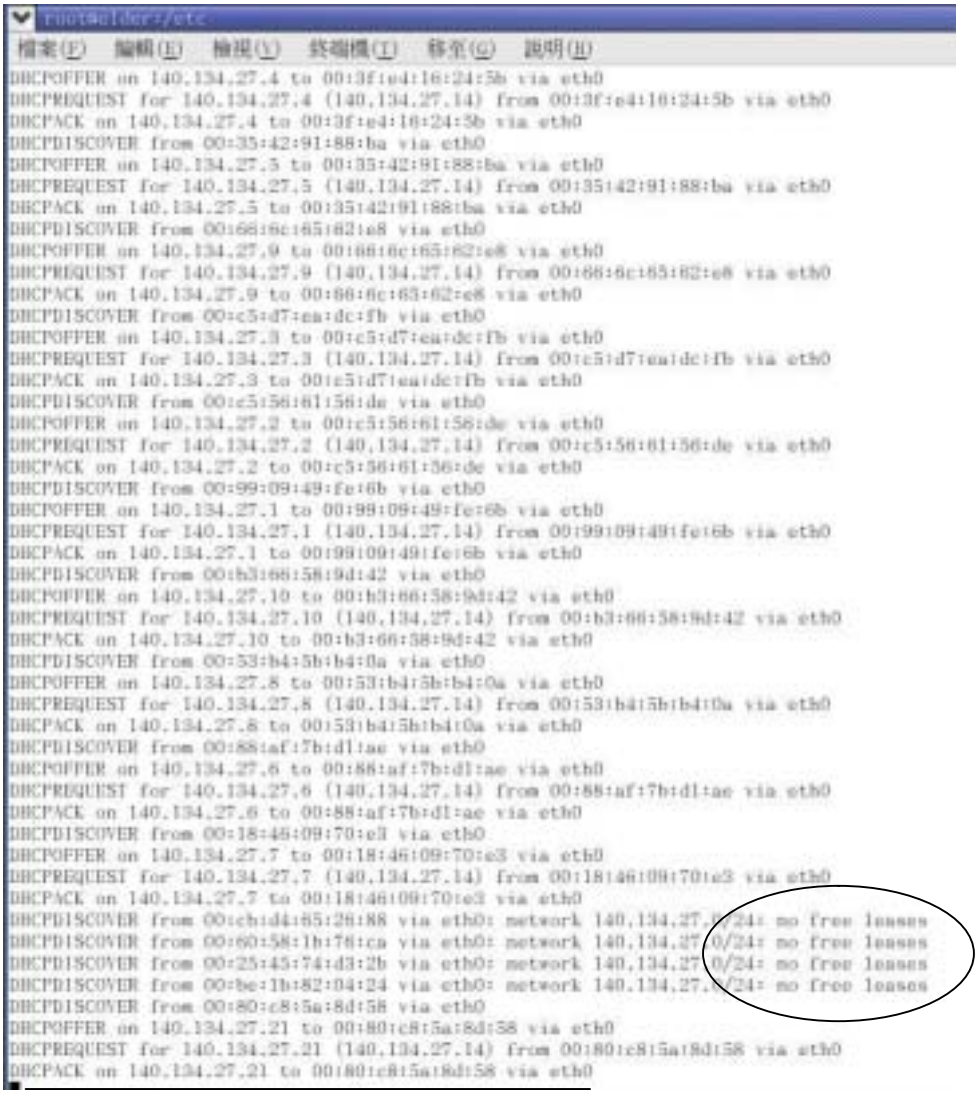


圖 4.5-5 保護下的 Server 仍可運作

在上圖中我們可以發現, 即使 Server 已經沒有可用的 IP 位址，但因為攻擊程式隨機產生 MAC address 無法取得設定檔中已經鎖死的 IP 位址 ”140.134.27.21 ”因此當合法的 Client 進入 DHCP Server 時它仍可取得 IP 位址, 因此 Server 提供的服務才不至於中斷。

第六章　結論

DHCP 已經是目前最常被使用的動態 IP 調適機制，其能夠動態配置 IP 的特性大幅的解決 IP 位址不足的問題，亦對於網路的使用者帶來莫大的便利性，但 DHCP protocol 卻因無有效的認證機制使得 Server 所能夠提供的 IP 位址可能被同一個 Client 拿走，導致 Server 提供服務的功能中斷。這一點在本文的第三章已經有明確的實做。

關於此一安全性的問題，雖有許多人士提出可能的解決方法，但除了利用網路卡號管理作為保護的方法外，其他的方式都仍有待討論。這也是目前 DHCP protocol 中最大的隱憂。也因為如此，本研究在此希望在短期之內可將網路卡號管理納入 DHCP protocol 的一部分以暫時提供網路管理人員解決此一問題的方法。但就長遠來看，DHCP protocol 還是必須把 Server 與 Client 間的認證機制當作協定層的一部分來設計，如此方可提供有效且完整解決方法。

參考文獻

[1] R. Droms , “ Dynamic Host Configuration Protocol ” ,RFC2131, March 1997

[2] S. Alexander, R. Droms , “ DHCP Options and BOOTP Vendor Extensions ” , RFC2132, March 1997

[3] C. Rigney, S. Willens, A. Rubens, W. Simpson, “ Remote Authentication Dial In User Service (RADIUS) ” , RFC2865, June 2000

[4] R. Droms, W. Arbaugh , “ Authentication for DHCP Messages ” , RFC3118, June 2001

[5] http://www.isc.org/products/DHCP/

[6]Felix Lindner, “ Attacks on the DHCP Protocol ” , http://www.nruns.com/filebase/download/wp/exploiting_dor

[7] http://www.ringchain.com.tw/products/index_3.asp

[8] http://home.kimo.com.tw/hunglinchou/WirelesSecurity.htm

[9]http://www.ieee802.org/1/files/public/docs2003/EAP-1X-Machines-0307.pdf

[10] http://www.informit.com/

[11] R. Droms, W. Arbaugh, draft-ietf-dhc-authentication, “ Authentication for DHCP Messages ” , June 1999