動態 IP 配置系統之安全性研究

黃鈞蔚　　徐志良　　王俊鑫
中華大學資訊工程學系
chwang@chu.edu.tw

摘要

Dynamic Host Configuration Protocol (DHCP) [9]通訊協定，被廣泛的應用在 Internet Protocol (IP) 位址的配置管理與暫緩 IP 位址不敷使用的問題，但缺乏安全的管理機制。除了使用者可不經認證，輕易的獲得 IP 的安全威脅外，更值的我們關注的是，如何防止利用 DHCP 通訊協定的特性，進行癱瘓網路與竊取機密資料的危機。在本篇論文，我們首先探討，偽造(惡意的)的 DHCP 伺服器、使用者私自設定動態 IP 位址集中的任意 IP 位址及具攻擊性，連續假造用戶端實體網路位址，重覆騙取 IP 位址等所衍生的網路安全問題。並提出了一套安全性動態 IP 分配系統架構，提供偵測異常狀態分析，若異常狀態發生時，能迅速的進行阻斷有惡意行為的網路主機，以改善與彌補傳統 DHCP 架構下所造成資訊系統安全上的漏洞。

關鍵字：DHCP, IP

1.簡介

為解決不敷使用的 IP 位址及有效的配置管理使用者 IP 位址的問題，IETF(Internet Engineering Task Force)提出動態 IP 位址分配機置(Dynamic Host Configuration Protocol, DHCP) 。如此，企業網路管理者可以利用 DHCP 動態分配機制來集中管理企業內部的主機 IP 分配，企業網路管理者只需要將 IP 位址配置規劃設定好，就可以自動將企業內部使用者所需的 IP 位址及網路相關環境設定等資訊傳送給使用者，並且自動的完成設定。使用者不需要了解到如何設定 IP 及相關網路環境設定，而需要使用到網路時；就可以直接連線至企業網路及網際網路，對於企業網路管理者簡化了繁瑣的網路設定及管理問題。

傳統 DHCP 欠缺考量安全上的機制，對於一個企業上網人數眾多的網路環境，隨便人員將網路實體線路接上網路或使用無線網路卡連線至網路後，即可輕易的獲得 IP 及網路環境資訊，如果不懷好意的人員，藉此進行竊取企業重要資源或進行網路攻擊，這將會是對於企業資訊安全上的一個重大漏洞。因此，有許多相關的技術論文[1,2,3,8]，著重於 IP 配置與認證的機制。

Komori, T 等人所提出的 DHCP 結合使用者認證方法[8]，來解決目前 DHCP 安全認證上的問題。其主要的目的是利用使用者的帳戶及密碼來防止非法取得 IP 問題。其所提出的方法是 DHCP 伺服器前端結合認證伺服器，對於每一個申請 IP 的用戶端都進行身份上的確認，當合法使用者認證過後，安全性 DHCP 系統會主動將使用者帳戶、使用者申請之 IP、用戶端網路實體位址等資訊同步至網路閘道設備中，並且同意該用戶端可以連線至網際網路。

Kaining Lu 等人[3]，提出 DHCP 結合 LDAP[6] 目錄服務認證的管理系統，該作者的主要運作環境是在校園網路中，使用 DHCP 動態分配環境並結合 LDAP 目錄服務作為校內師生使用認證後取得 IP 位址，以防止非校園內師生非法取得 IP 問題。此架構主要運作模式為，當師生要取得 IP 位址時，必需先要透過 LDAP 目錄服務伺服器認證後，才能取得 IP 位址。並透過路由器中存取控制清單 ACL(Access Control List)功能限制只允許合法 IP 位址可以瀏覽網際網路。以達成實用性、控制性、管理性等要求。

Gao Lu 等人[1]，提出設計一個整合認證、分配網路位址、封包過濾的網路設備，作者們提出一個構想，就是想要開發一個硬體在目前的寬頻服務中，提供結合認證、授權、清單(AAA)[4]認證功能

---

*本論文研究為中華大學重點教學與研究計畫之研究成果, 計畫編號 CHU-93-TR-010

及動態分配 IP 位址、封包過濾於一身的集中控制器(Concentrator)。

Jenq-Haur Wang 等人[2]，提出加強式 Intranet 動態分配 IP 環境管理概念，除了原有的 DHCP Server 外，再加上 ACL Server，當使用者向 DHCP Server 要求取得 IP 時，由 DHCP Server 更新 ACL Server 的內容，並由 ACL Server 透過 RS232 介面更新 MAC Bridge 上的 Filter Data Base，當流經 MAC Bridge 的封包符合 Filter Data Base 中的記錄時，才允許使用者連線至網際網路，否則由 MAC Bridge 丟棄，以增加企業網路的安全性。

縱觀上述的 DHCP 技術相關論文，均著重在結合認證整合方面，然而卻忽略了傳統 DHCP 架構上，所產生對於網路安全性上的威脅，如偽造(惡意的)的 DHCP 伺服器、使用者私自設定動態環境範圍中的 IP 位址及具攻擊性，連續假造用戶端實體網路位址，重覆騙取 IP 位址等所衍生的網路安全問題，茲分述如下:

狀況一: 蓄意假造 DHCP 伺服器或甚至無心的啟用 DHCP 伺服器，影響正常 DHCP 用戶端無法獲取內部正確網路位址，使得大部份企業 DHCP 用戶端會獲取到假造 DHCP 伺服器所給予的錯誤網路位址，進而影響企業用戶端無法進行正常性工作、生產、銷貨等，因而達成癱瘓公司運作之目的。或是利用錯誤的網路位址及網路閘道(Gateway)，來收集或監聽用戶端的訊息資訊，以達到竊取商業機密之目的。

狀況二：私自定義 DHCP 位址集中的 IP 位置，以影響某一位用戶端使用正常 DHCP 申請所獲得的網路位址，使得該用戶端由於 IP 相衝突的原因導致雙方用戶端均無法使用到網路資源，進而影響該正常用戶端無法進行正常性工作或生產，如果有心人士就此問題進行反覆性產生時，如利用電腦病毒的模式來大量產生問題，則影響到的用戶端數量將會很多，因此就會達成癱瘓公司運作之目的。

狀況三：利用作業系統之漏洞，植入自行開發的後門程式或攻擊程式，對企業網路中的 DHCP 伺服器進行攻擊，其攻擊手法是使用程式一直變造 DHCP 封包內申請 IP 位址之來源實體位址(MAC Address)，向企業網路中的 DHCP 伺服器騙取 IP 位址資訊，由於每次來向 DHCP 伺服器所要 IP 位址資訊的用戶端實體位址均不同，所以 DHCP 伺服器會認為是來自於不同的用戶端做 IP 位址的申請，而立即回應不同 IP 位址資訊給該用戶端，事實上都是來自於同一台主機的申請，因而耗盡 DHCP 伺服器中所有的 IP 資源，使得正常用戶端無法獲取到 IP 位址資訊，導致企業用戶端無法進行正常性工作或生產，達癱瘓公司運作之目的。

因此，在本篇論文中我們將針對 DHCP 架構上，所產生對於網路安全性上的威脅，提出一個安全性的系統架構，利用系統中偵測系統來查覺是否有異常網路行為產生，當偵測有任何異常行為發生時，立即進行異常行為之阻斷，並且通知系統管理者，以建置一個具安全性的動態 IP 配置系統。

本篇論文，第二章將說明的安全性動態 IP 配置系統架構，在第三章介紹系統的設計原理及實作方式，最後第四章就本論文所提出的架構作一個總結。

2.系統架構

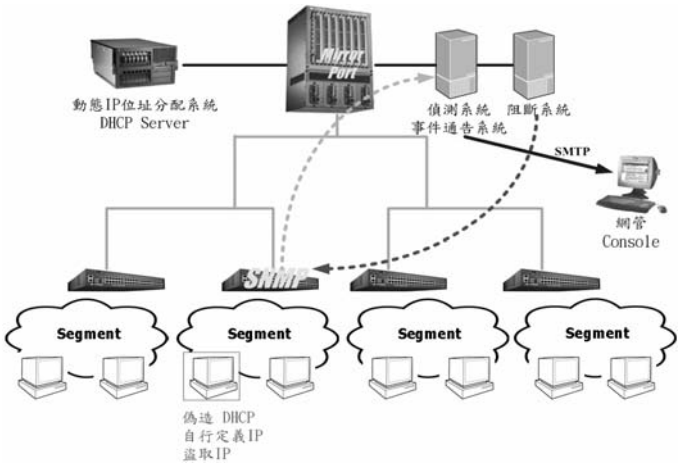

圖 2-1 安全性動態分配架構圖

在這個章節，將介紹我們所提出的一種安全性動態分配 IP 位址的系統架構，以解決目前 DHCP 運作上所造成資訊安全上的漏洞，使得企業網路管理者在面對 DHCP 環境時，不必再擔心會有因 DHCP 在 IP 管理上所造成資訊安全上的漏洞。

本系統之架構如圖 2-1 所示，分為三大部份，第一部份為安全漏洞偵測系統，它主要的任務負責監聽網路上有關於 DHCP 及 IP 層的相關行為，隨時掌控任何最新的網路入侵破壞行為狀況。當有發生入侵破壞行為時，偵測系統會偵測到此入侵手法，並將此來源位址記錄以及隨即通知阻斷系統，

進行入侵行為之阻斷，最後會啟動通知系統，利用郵件方式通知系統管理員，何時發生入侵行為及入侵手法、來源位址等相關訊息。第二部份為動態主機 IP 位址分配系統，主要是提供用戶端 IP 位址配置與管理功能，當用戶端有 IP 位址需求時，位址分配系統會從可用的 IP 位址集合中(IP Pool)，找出一個可用的 IP 位址，配置給用戶端，並通知用戶端租用此 IP 位址的期間為多久等。第三部份則為阻斷系統，當偵測系統通知有入侵行為產生時，阻斷系統會將此入侵來源位址，透過 Simple Network Management Protocol (SNMP)[7]去尋找每一台 Edge Switch 交換器內的 MAC Table 實體位址記錄表，查尋出入侵來源位址主機是接到那一台的交換器中的那一個 Port 端口，當找到入侵來源之後，再利用相同的 SNMP 手法，將入侵來源所在交換器的端口進行關閉，以有效阻斷入侵行為的發生。

3.系統設計及實作

為了有效阻止入侵或攻擊事件的發生，以及達成安全事故處理流程的自動化，我們設計了整合偵測、通知、阻斷、分配位址於一體的安全性動態 IP 位址分配架構。本章節將說明安全性動態 IP 位址分配架構，以及各系統之設計概念及原理。將分別就位址分配、入侵破壞偵測、自動警告通知、入侵破壞來源阻斷等，說明系統設計概念以及各系統之運作原理。

3.1 位址分配機制及建置

在我們的實作環境之中，將使用一台 DHCP 伺服器，其作業系統平台為微軟 Windows 2000 作業系統，並搭配一套微軟所提供的 DHCP 伺服器，作為本安全性網路架構中動態分配 IP 位址之角色。本架構實作系統規劃如圖 3-1。

3.2 入侵、異常狀況偵測

本架構中的偵測系統，主要是針對現有傳統 DHCP 環境中作異常性分析。其中我們要探討的問題是『什麼樣的狀態行為稱為異常狀態或是攻擊狀態』。我們將依照現有傳統 DHCP 環境中已知的異

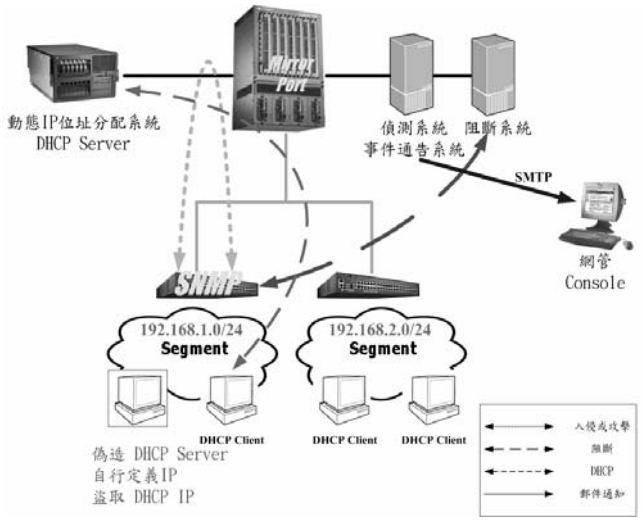

圖 3-1 實作架構圖

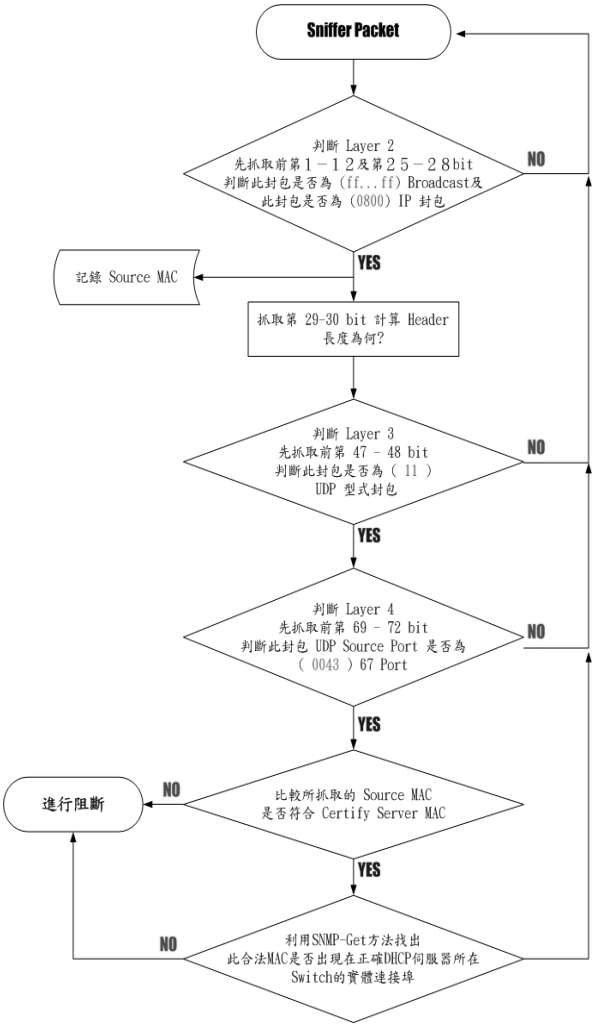

圖 3-2 偵測假造 DHCP 伺服器流程圖

常行為及可能的攻擊方法，進行狀態行為分析。

各企業目前在運作 DHCP 環境中所最常發生以及可能會發生的異常狀況有三種。而我們就以三種狀況進行分析及辨識異常行為，開發出偵測模

組。再進一步整合所有的偵測模組，即可成為安全性動態分配架構中的偵測系統。各偵測模組分述如下:

3.2.1. 偽造網路上動態分配 IP 的 DHCP 伺服器

要偵測網路上是否有出現偽造的 DHCP 伺服器，則必須就網路上的 DHCP 伺服器發送的 DHCP OFFER 廣播訊息進行監聽，再分析此 DHCP OFFER 訊息內的伺服器位址(IP 與 MAC)，是否為企業網路內部所定義的正確 DHCP 伺服器，若比對不合，則認定為偽造的 DHCP 伺服器；若比對相同時，則暫視為正常狀況，因假造之 DHCP 伺服器依然有可能會偽裝其來源 MAC 及來源 IP 位址為企業網路內部所真正 DHCP 伺服器的 MAC 及 IP 位址，所以為了避免這樣的漏洞，我們可以利用 SNMP-Get 方法，抓取每台 Switch 的 MAC Table，找出偽造 DHCP 伺服器的 MAC 出現在那一台的 Switch 之中，若發現該 MAC 出現在不是正確 DHCP 伺服器所在 Switch 的實體連接埠時，則也認定為異常狀況，偵測的流程如圖 3-2。

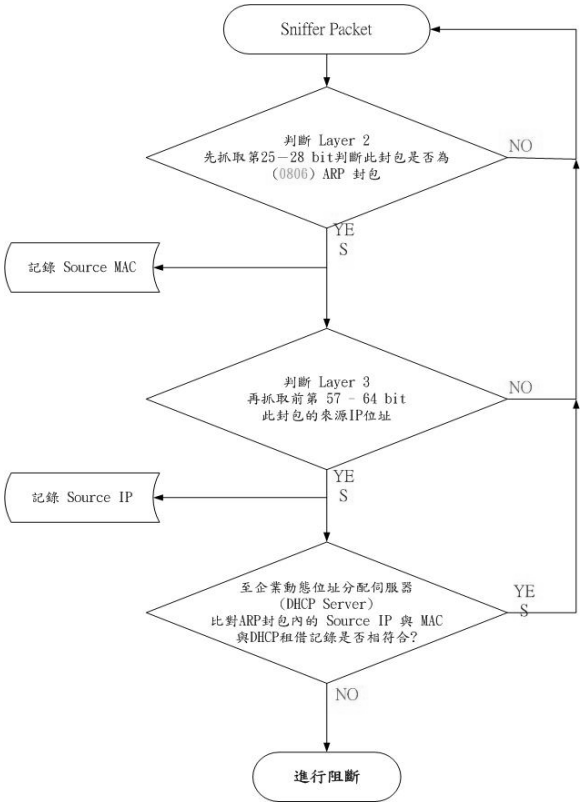

圖 3-3 偵測私定 IP 位址流程圖

3.2.2. 私自定義動態環境範圍中的 IP 位址

要偵測出是否有用戶端主機，私自定義企業動態網路環境中，動態 IP 位址集中的任何一個 IP 位址。我們可以藉由監聽網路上的 Address Resolution Protocol (ARP)[5]封包來進行分析比對。由於 IP 的運作方式，若主機要與同網段中的另一部主機進行資訊傳遞時，須利用 ARP 方式來獲取對方主機之 MAC 位址。就基於此特性，我們可以監聽 ARP 封包內的來源 MAC 位址及 IP 位址，若與企業 DHCP 伺服器中租借資料庫記錄不符合時，就可以發現有用戶端主機，私自定義企業中動態 IP 位址，判定此種狀態為異常，偵測的流程如圖 3-3。

3.2.3. 具攻擊性，連續性假造用戶端實體網路位址，重覆騙取 IP 位址

要偵測出是否有惡意的用戶端主機利用修改來源實體位址，重覆向 DHCP 伺服器要求 IP 資源。為了要偵測此種惡意行為，則首先利用偵測系統找出用戶端所發出的 DHCP Request 訊息，並解析包含此訊息其 Layer 2 的來源實體位址(Source MAC)並記錄之，再配合解析 DHCP Request 訊息中用戶端實體位址(Client MAC)，比對 layer 2 所記錄的 Source MAC 與 DHCP-Request 訊息中所記錄的 Client MAC 是否相符，若不相符合就視為一種異常狀況，並立即進行阻斷。但若相符則暫判定為 DHCP 正常行為，再進行進一步分析，判斷駭客是否有同時修改 layer 2 與 DHCP-Request 訊息中來源實體位址，判斷方法是利用在正常的 Edge 網路設備中(如 switch)，每一個用戶端所實際連接的網路實體連接埠，在短時間內不會有大量的 DHCP 申請封包出現(但 Up-Link 連接埠除外)，若同一個實體連接埠在一定時間範圍內出現大量 DHCP-Request 封包，則也判定此狀況為異常，偵測的流程如圖 3-4。

3.3 異常訊息通知

本架構的自動通知系統，是整合在異常偵測系統中。通知系統是利用一支外掛發信程式(Postie Mail Client)，如圖 3-5，此發信程式主要是一種命令式(Command Line)發信方法，使用一連串指令方可寄信。訊息通知系統主要的運作方式，是當偵測

系統偵測到網路封包符合異常的定義條件時，則判定此網路上發生異常狀況，此時偵測系統立即使用命令方式，發送郵件通知系統管理者目前網路發生什麼樣的異常狀況。

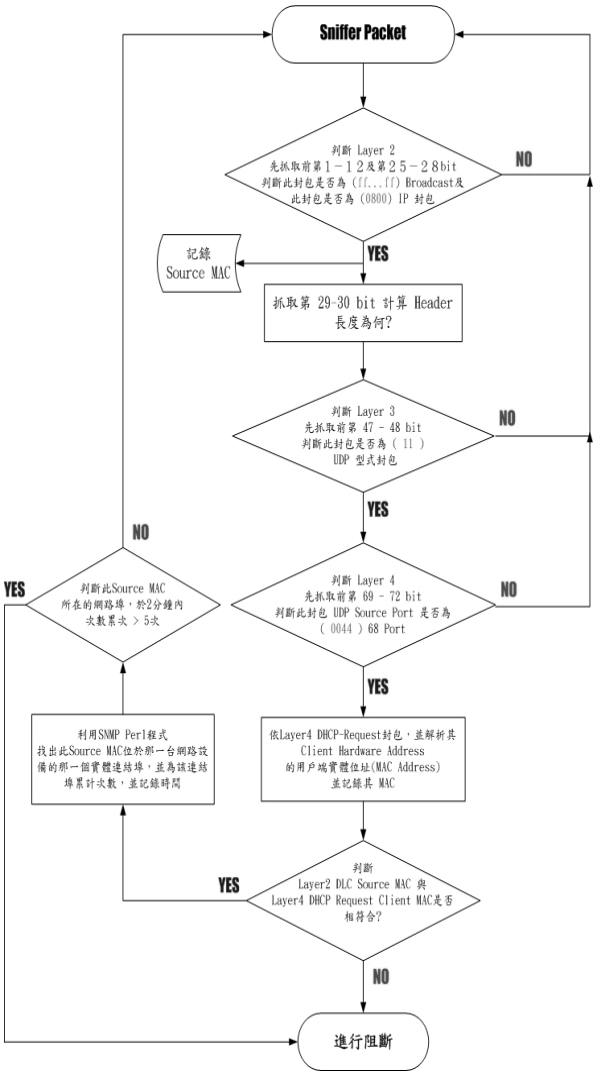

圖 3-4 偵測假造來源位址流程圖

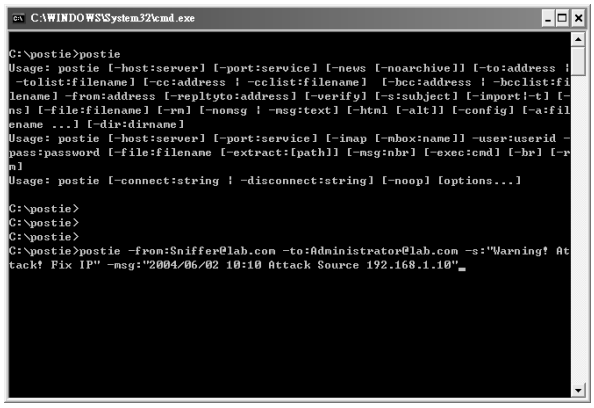

圖 3-5　Postie Command Line Mail Client

3.4 異常狀態阻斷

實際實施網路阻斷必須考量的是如何選擇最有效的阻斷點，選擇何種的網路設備進行阻斷最為有效。

本架構中的阻斷系統，主要的阻斷位置及運用的阻斷網路設備就是距離用戶端最近的網路交換器，由於現今大部份的網路設備均具備有網路管理機制(SNMP)，就是基於此特性，我們自行開發了一套 SNMP-Base 的 Perl 網路阻斷程式。而此程式有使用兩個 SNMP 函式庫(Basic Encoding Rules)及(SNMP Request/Response Handling)。阻斷程式其運作方法，是因為每一台網路交換器中都支援 SNMP 網路管理，而阻斷程式就是利用 SNMP-Get 的方法，取出各網路交換設備中的 MAC Table，因為 MAC Table 是記錄交換設備每一個網路通訊埠與所連接網路用戶端的對應表，所以當偵測系統發現到有異常主機出現時，則會使用通訊連結方法，立即通知阻斷程式其查到的異常主機網路實體位址(MAC Address)。接下來阻斷程式將會比較各網路交換設備中的 MAC Table 是否有符合的網路位址，如此，將會很快得知異常主機的正確位置為何，查尋流程如圖 3-6。

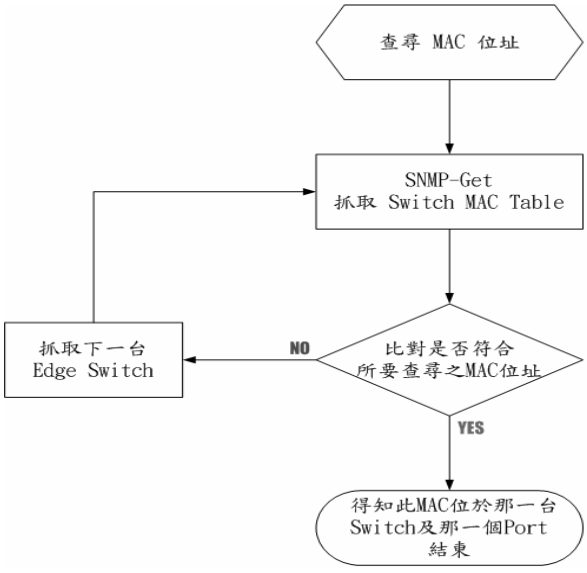

圖 3-6 查尋可疑 MAC 流程

當一旦查尋到該異常主機的正確位置之後，則阻斷程式將進行正式的網路阻斷，其方法是使用

SNMP-Set，至異常主機所連接的網路交換設備中，將異常主機所實際連接的通訊埠，作關閉通訊埠的動作(Disable Port)。使得異常主機無法再繼續對網路上發送任何網路封包。以達成最有效的阻斷方法。

4.結論

由於網際網路的快速發展，相反的對於造成網路攻擊或是異常使用的網路安全事故也愈來愈多。而且這些網路安全事故很有可能會在極短的時間內，造成公司資訊作業停擺。因此，對於事故反應的時間就更顯得重要。而對於現在企業用戶所使用最頻繁的動態位址分配環境，所造成企業資訊安全上的漏洞，是目前企業網路管理者所最關心的課題。因此我們希望藉由安全性動態 IP 分配架構的提出，能夠有效的解決現有傳統 DHCP 所造成企業網路安全性上的漏洞。

在另一方面，本架構中也提出了一項針對異常事件的阻斷功能。目的是在處理安全事故上的反應時間盡量能夠縮到最短。所以我們主張以較為積極的動作，立即阻斷會造成資訊安全上危害的異常用戶端主機，強制隔離問題源，以確實縮短處理反應時間。運用此安全性架構下，將會使得網路管理員在面對煩瑣的 IP 分配問題及資訊安全上的壓力，均一次獲得解決。

5.參考文獻

[1] Gao Lu, Ma Yan and Liu Jianbing, ”The Design for Ethernet Access Concentrator,” Info-tech and Info-net, 2001. Proceedings. ICII 2001 - Beijing. 2001 International Conferences on Volume 5, 29 Oct.-1 Nov. 2001, pp. 223-228.

[2] Jenq-Haur Wang and Tzao-Lin Lee, ” Enhanced intranet management in a DHCP-enabled environment,” Computer Software and Applications Conference, 26-29 Aug. 2002, pp. 893 – 898.

[3] Kaining Lu, Xian Yun Tu and Jun Zou, ”Design and Implementation of DHCP & LDAP Directory Service Integrated Management System,” Communications, Circuits and Systems and West Sino Expositions, IEEE International Conference on Volume 1, 29 June-1 July 2002, pp.758 - 762 .

[4] Network Working Group “AAA” RFC 2903, 2000.

[5] Network Working Group “ARP” RFC 826, 1982.

[6] Network Working Group “LDAP” RFC 1777, 1995.

[7] Network Working Group “SNMP” RFC 1157, 1990.

[8] T. Komori and T. Saito, ”The Secure DHCP System with User Authentication,” Local Computer Networks, 27th Annual IEEE Conference on 6-8 Nov. 2002, pp. 123 - 131.

[9] R. Droms, ”Dynamic Host Configuration Protocol,” RFC 2131, 1997.