IP 位址指派之監測與管理
Monitoring of IP Address Assignment

范恭達[*]　陳彥錚[*]　李思宏[**]
[*]國立暨南國際大學 資訊管理學系
[**]國立暨南國際大學 資訊工程研究所
E-mail: {s9213031, ycchen, leeh}@ncnu.edu.tw

摘要

每一台電腦上網前必須指定一個唯一的 IP 位址。早期，IP 位址是由人工手動設定， 確保 IP 位址之唯一性只能經由網管人員的管理；目前大部份的單位都改用 DHCP 伺服器來自動分配電腦所使用的 IP 位址，以避免人工設定時，兩台電腦 IP 位址相同，造成不能上網的情形。然而，在網管經驗上，即使在採用 DHCP 的環境中，IP 位址衝突的情形仍偶有發生，這是因為在採用 DHCP 的網路，使用者仍可經由手動設定自己電腦的 IP 位址，不理會 DHCP 所分配的網段，這種情況在校園網路屢見不鮮，這種 IP 位址指派問題漸成為網路管理上的新問題。本篇論文提出一個 IP 位址指派之監測機制，此監測機制透過 SNMP 網路管理協定至路由器設備檢查網路中 IP 位址的使用情形，並透過 DHCP 存錄的分析，找出違反規定使用 IP 位址的電腦，解決 IP 位址盜用與位址衝突之問題，可以有效降低網管人員的負擔。

關鍵詞：DHCP, IP 位址衝突, SNMP。

Abstract

A unique IP address should be assigned to each host in a network. In early days, the assignment of IP addresses is accomplished manually. Network managers guarantee the uniqueness of IP addresses. Nowadays, most networks use DHCP to automatically assign unique IP addresses. Nevertheless, the IP address conflict problem still exists. This is because users can freely change their own IP addresses even DHCP is applied in the network. How to effectively detect the mistaken use of IP addresses is an important issue for network managers. In this paper, we propose an effective monitoring mechanism of IP address assignments. Since active IP addresses can be observed in routers, we can use SNMP to retrieve those IP addresses and their corresponding MAC addresses. By the analysis of DHCP logs, we can identify the hosts using illegal IP addresses. Consequently, the IP address conflict problem can be effectively solved. The burden of network management can be significantly reduced.

Keywords: DHCP, IP address conflict, SNMP.

1. 前言

IP 位址管理一直為網路管理之重要議題，網管人員必須確保網路上之每一電腦均有獨一無二的 IP 位址，以避免 IP 位址衝突所造成部份電腦無法上網之障礙。在早期網路不發達以及網路技術未成熟的環境，電腦的 IP 位址與相關組態設定是經由人工手動完成，管理上非常不便。拜 DHCP (Dynamic Host Configuration Protocol) [6]發明之賜，目前大部份的網路都改用 DHCP 伺服器來自動分配電腦所使用的 IP 位址，一方面可以避免人工設定不當所造成 IP 位址衝突情形，亦可提高 IP 位址的利用率。此外，經由 DHCP 伺服器分配 IP 位址，網管人員也方便控管網路中電腦所使用的網段，將網路劃分一般使用者所使用的 IP 範圍和為了網路管理而使用的 IP 範圍。儘管 DHCP 解決了 IP 位址管理上許多問題，然而一般使用者使用電腦上網時，除了可以透過 DHCP 分配取得 IP 位址，仍可以經由手動設定自己的 IP 位址，而不理會 DHCP 所分配的網段，也就是說，即使全面採用 DHCP 的網路環境，也沒有任何強制性措施可以限制使用者對其網路組態設定做任何變更。因此，IP 位址的非法使用及可能帶來的 IP 位址衝突問題，在 DHCP 環境仍為一個值得研究的課題。使用者放棄使用 DHCP 改採手動設定 IP 位址之原因，可能在於對網路技術之不了解，或是搬動電腦位置所致，但也有因使用者為穿越防火牆的封包過濾，蓄意使用公用網路伺服器或代理伺服器(Proxy)IP 位址之情事，這些違反 IP 位址使用規定的情況，是網管人員在網路管理上之一大負擔，在缺乏即時的監控機制下，通常網管人員很難在事後找出問題所在，且這種問題也容易被誤認為其他網路障礙而被忽略。

由於任何一台電腦連上網路時，其 IP 位址及網卡位址(即 MAC 位址)均會被此電腦的預設閘道器(Default Gateway)所觀察到，而如果此電腦之 IP 位址是由 DHCP 伺服器所指派的，則 DHCP 伺服器之存錄(log)也會有一筆對應的租賃記錄，記錄內容也包括 IP 位址及 MAC 位址資料，因此，倘若我們能夠有效地即時搜集這些資訊，我們便能從中確定 IP 位址之指派與 IP 位址之實際使用情況是否具一致性，進而發現問題。基於上述的觀察，本篇論文提出一個 IP 位址指派之自動監測機制，此監測機制

利用幾乎所有網路設備都有支援的 SNMP[2]網路管理協定週期性地至各路由器查詢目前網路上出現的 IP 位址及其 MAC 位址，並透過 DHCP 伺服器存錄分析，以檢查網路中是否有不透過 DHCP 伺服器取得的 IP 位址以及 IP 位址與 MAC 位址對應不一致之情況，進而找出妨害網路正常運作之來源。此外，此監測機制尚包括一個自動斷網模組，可針對違反 IP 位址使用規定之電腦，依其 MAC 位址至其連接的交換器直接進行阻斷，即時有效解決 IP 位址衝突問題。

本篇論文其他章節分述如下，第 2 節簡介 DHCP 與 SNMP 原理，第 3 節描述 IP 位址指派監測系統之架構，第 4 節介紹系統實際運作過程，第 5 節為結語及未來展望。

2. 相關技術探討

2.1 DHCP

眾所週知，一台電腦要正常地使用網路，在電腦上要設定該電腦的 IP 位址、預設閘道、子網路遮罩(subnet mask)、以及所要使用的領域名稱伺服器(DNS)。這些設定，在幾年前網路尚未像目前如此發達時，這些設定是透過人工手動進行設定的，除了設定麻煩外，如果事先沒有進行 IP 位址分配的協調，還有可能會發生兩台電腦設定相同 IP 位址的情況，此即 IP 位址衝突問題。DHCP (Dynamic Host Configuration Protocol) [6]協定就是為了解決以上問題而產生的，網管人員可以透過 DHCP 的組態檔設定，決定哪一段 IP 位址可以透過 DHCP 分配，哪一段保留作為網路管理或伺服器使用，同時因為透過 DHCP 進行 IP 位址分配，幾乎不會有同時分配給兩台電腦相同 IP 位址之問題。而經由 DHCP 統一控管，網管人員在網路的設定要進行變更時，也只要更改 DHCP 伺服器的設定，不需要個別通知網路中每一台電腦的使用者執行新的網路組態設定，因此 DHCP 是 IP 位址組態管理中一個很好的解決方案。

DHCP 的前身是 BOOTP(Bootstrap Protocol) [4]，本來是設計給無磁碟主機透過網路開機使用的協定，透過在電腦開機時，送出廣播封包的方式，尋找提供開機所需啟動檔案的機制，後來經過修改，成為目前的 DHCP，二者網路封包的格式極為相似，所以目前有的 DHCP Server 同時也支援 BOOTP 通訊協定。 DHCP 的發明，主要是為了節省設定每一台電腦上網設定的時間，讓每一台使用者端的電腦(DHCP Client) 在開機時，透過廣播封包自動尋找 DHCP 伺服器的位置、向 DHCP 伺服器要求租用 IP 位址和設定上網相關設定，其設計主要是為了節省網管人員的負擔而開發出來的。在邏輯上，DHCP 整個架構可以分為 3 個部分：

(1). ***DHCP 伺服器 (Server)***：

提供 DHCP 服務的電腦，擔任 IP 位址分配中的「借方」角色，負責處理 IP 位址的出租和收回，保持在同一個時間內，某一組 IP 只有一台電腦可以租用。

(2). ***DHCP 用戶端 (Client)***：

即一般普通使用者的電腦，在使用 DHCP 服務的環境中，擔任 IP 的「貸方」角色。在設定作業系統時，網路設定應設定為「自動取得 IP」，此設定也是 Windows 系列作業系統的預設值。

(3). ***範疇(Scope)***：

即為「出租物」之範圍。每一台 DHCP Server 至少要管理一組 IP 位址，這組 IP 位址便是 Scope。當 DHCP Client 透過網路要求 IP 位址時，DHCP Server 便會在所管理的 IP 位址 中找出一組目前處理閒置狀態的 IP 位址，出租給 DHCP 用戶端，並告知用戶端合法租用期間。

整個 DHCP 運作的過程，可以區分為以下四個步驟：

(1). ***DHCP 用戶端要求租用 IP 位址***:

DHCP 用戶端送出 目的 MAC 位址為 FF:FF:FF:FF:FF:FF 及 IP 位址 為 255.255.255.255 的 DHCPDiscover 廣播封包。

(2). ***DHCP 伺服器提供可租用的 IP 位址***:

DHCP 伺服器收到廣播封包後，會在自己所維護的 Scope 中找出可供租用的 IP 位址，並決定租借時間的長短，放在 DHCPOffer 封包內，再用廣播的方式回送給 DHCP 用戶端。

(3). ***DHCP 用戶端確認 IP 位址租約***:

在網路上同時存在多台 DHCP 伺服器時，每一台伺服器在收到用戶端所廣播的 DHCPDiscover 封包時，都會送出 DHCPOffer 封包，依照系統預設值，用戶端只會接受最先收到的 DHCPOffer 封包，其他的封包則不予理會。在用戶端決定要使用的 IP 位址後，會再使用廣播的方式送出 DHCPRequest 封包，與所挑選的 DHCP 伺服器確認租約，與其他 DHCP 伺服器的租約則沒有成立。若用戶端不同意伺服器所提供的 IP 位址，會送出 DHCPDecline 封包，重新回到第 1 個步驟。

(4). ***DHCP 伺服器同意 IP 位址租約***:

當 DHCP 伺服器收到用戶端所廣播的 DHCPRequest 封包後，如果同意該 IP 位址的租借，會再以廣播送出 DHCPAck 封包，並開始計算租用的時間。若不同意，該送出 DHCPNack 封包，重新回到第 1 個步驟。

在以上的 IP 位址租賃過程中，用戶端除了 DHCP 封包的收送外，還會利用 ARP (Address Resolution Protocol) [9] Request 確認 IP 位址之唯一

性，此動作恰好可提供路由器最新的 IP 位址與 MAC 位址對應資訊，也因此，本論文研究所利用之路由器 ARP 快取資料是即時正確的，可以不用擔心因快取資料過時所導致的錯誤。此外，對於經常使用網路之合法使用者，即使租約過期再重新分配之 IP 位址也多與先前所使用之 IP 位址相同，因此，在路由器所觀察到之 IP 位址與 MAC 位址對應資料，正常情況下並不會有太大的改變。

2.2 SNMP

SNMP (Simple Network Management Protocol, SNMP) [2]是 1986 年由美國的一位 Jeff Case 教授所提出的，當時設計的目的是為了建立一套適用 TCP/IP 網路環境的網管通訊協定，方便網路管理人員以標準統一的方式監測網路的狀況以及控制網路設備的運作，隨著網路技術的演進以及網路管理的需求日增，SNMP 至目前共發展了三個版本，分別是 SNMPv1 [2]、SNMPv2 [3]、SNMPv3 [7]，其中 SNMPv1 因為架構簡單，實作容易，目前大部分的網路設備都有支援，微軟 Windows 2000 和 Windows XP 也都有提供 SNMP 的程式，讓普通的電腦可以透過 SNMP，遠端管理電腦的網路卡介面，得到電腦的網路流量統計等資料。

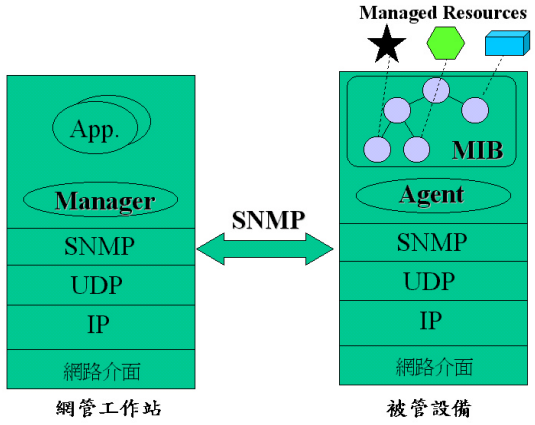

圖 1 SNMP 網管架構

符合 SNMP 標準架構之網管包括四個構成元素，如圖 1 所示，分別為管理者、代理者、網管通訊協定、以及管理資訊庫。管理者為各項網管應用程式，負責網管監控主要工作；代理者為被管設備端的程式，接受管理者的指令及發送通報給管理者；網管通訊協定(即 SNMP 本身)提供管理者與代理者間標準的通訊程序與格式，計有 Get-Request、GetNext-Request、Set-Request、Get-Response、及 Trap 五種訊息；而管理資訊庫(Management Information Base, MIB)則為網管資訊的集合。基本上，SNMP 的架構簡單，但不同的網路設備提供的 MIB 不同，各自有其不同的網管目的。每個 MIB 是由許多個別的物件所組成，每個物件對應至網路設備的網管資訊或狀態，在 SNMP 的網管模型下，網路管理工作便是對 MIB 物件的讀取與設定。誠如先前所述，不同的網路設備提供的 MIB 不同，但只要支援 TCP/IP 通信協定之網路設備，均會支援標準的 MIB-II [8]物件，提供網際網路一些基本通信協定之監測管理資訊。另外，各式第二層的橋接器或交換器也會支援 Bridge MIB [5]。本論文所提利用 SNMP 蒐集 IP 位址使用資訊，便是從標準的 MIB-II 取得 IP 位址與 MAC 位址資料，另外並利用 Bridge MIB 實施斷網工作。因此，在實務上我們所提 IP 位址指派監測機制是一實際可行的解決方案。

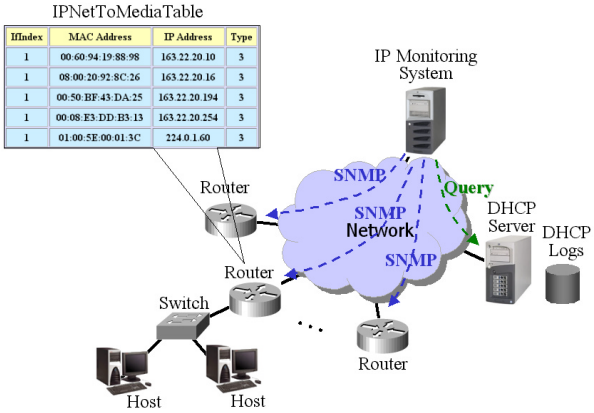

圖 2 IP 位址指派監測系統架構

3. 系統架構

本論文提出一個利用 SNMP 與 DHCP 存錄分析的 IP 位址指派監測機制，圖 2 顯示其系統架構。此監測機制包括一個 IP 位址監測器，負責週期性地使用 SNMP 至各路由器讀取最近連上網路的電腦之 IP 位址與 MAC 位址。各路由器為了迅速轉送封包至各電腦，均會記錄與其連結的電腦之 IP 位址與 MAC 位址，即 ARP 快取資料，以避免重複地使用 ARP 詢問 MAC 位址。以 SNMP 的觀點，ARP 快取資料存於 MIB-II 中的 ipNetToMediaTable，表 1 為 ipNetToMediaTable 之實例，每一筆記錄包括路由器介面卡編號、電腦 MAC 位址、電腦 IP 位址、及此位址對應型態。位址對應型態值為整數，可為 other(1)、invalid(2)、dynamic(3)、 static(4)四個數值。我們可分析那些位址對應型態為 dynamic 的記錄，即動態對應的位址資料，當我們分析後發現某筆位址對應資料是非法設定 IP 位址所造成時，我們可將該筆記錄資料之位址對應型態設為 invalid，藉此告知路由器必須重新取得正確的位址對應資料。因此，IP 位址監測器以固定週期方式透過 SNMP 取得路由器中的 ipNetToMediaTable 便可得知此路由器所控管的網段中正在活動的電腦。由於 ipNetToMediaTable 定義於 MIB-II 標準，幾乎所有支援 SNMP 的網路設備均提供 MIB-II 網管資訊，對路由器設備而言，MIB-II 之 ipNetToMediaTable 更是必備之網管資訊，因此 IP 位址監測器可以完全掌握網路中所有電腦的位址對應資料。

表 1 ipNetToMediaTable 實例

IfIndex	MAC Address	IP Address	Type
1	00:60:94:19:88:98	163.22.20.10	3
1	08:00:20:92:8C:26	163.22.20.16	3
1	00:50:BF:43:DA:25	163.22.20.194	3
1	00:08:E3:DD:B3:13	163.22.20.254	3
1	01:00:5E:00:01:3C	224.0.1.60	3

除了 IP 位址監測器與網路各路由器外，此 IP 位址指派監測機制還包括 DHCP 伺服器，網管人員事先依各網段自動分派 IP 位址之範圍及相關資料設定 DHCP 伺服器，當電腦向 DHCP 伺服器請求 IP 位址成功後，DHCP 伺服器便會將此電腦之 MAC 位址與所派定的 IP 位址，連同租用起始與預定終止時間一起記錄於 DHCP 存錄中，請參考表 2 所示 DHCP log 檔實例。顯然，存於 DHCP 存錄的電腦位址對應資料是合法正確的，這些資料可以作為判斷 IP 位址是否正確使用的依據，因此我們無須像以往為解決 IP 位址衝突問題自行建立與維護一個位址對應資料庫，當 IP 位址監測器從各路由器取得目前位址對應資料後，再從 DHCP 伺服器取得 DHCP 存錄資料進行進一步分析。因此，只要透過 DHCP 存錄資料與 ipNetToMediaTable 資料的交叉比對，我們便可以找出問題所在。針對 ipNetToMediaTable 中之每一筆記錄的 IP 位址與 MAC 位址，我們至 DHCP 存錄比對，可以過濾出以下三種異常情形：

(1). ***IP 位址相同的存錄， MAC 位址不同***

表示有一台電腦自行設定 IP 位址，而此 IP 位址實際上已分配給某一合法使用者。

(2). ***MAC 位址相同的存錄， IP 位址不同***

表示有一已以 DHCP 獲得合法 IP 位址之電腦，自行變更其 IP 位址。

(3). ***IP 位址及 MAC 位址均不在 DHCP 存錄***

表示有一台電腦自行設定 IP 位址，此 IP 位址目前並沒有分配給任一合法使用者。

上述三種情形中，第一種情況會導致 IP 位址衝突問題，使得合法使用者無法順利連上網路。第二與第三種情況雖不致於有立即性的威脅，但會影響 DHCP 在往後分配 IP 位址時，無法讓使用者順利獲取租約的情況。

以上之分析是針對可動態指派IP位址範圍的部分進行比對，針對網路上供伺服器使用之固定 IP 位址範圍內的比對，我們必須另外建立位址對應資料，比對分析方式大致相同，分析的結果通常只有以上第一種異常情形會發生，亦即有電腦將其 IP 位址設為伺服器所使用之固定 IP 位址。

表 2 DHCP 存錄實例

```
lease 163.22.8.52 {
  starts 3 2003/08/06 02:12:27;
  ends 4 2003/08/07 02:12:27;
  binding state active;
  next binding state free;
  hardware ethernet 00:d0:59:cc:c2:47;
  uid "\001\000\320Y\314\302G";
  client-hostname "NCNU-TEAM";
}
```

在找出違法使用 IP 位址之電腦後，如果這些 IP 位址的違法使用危及網路之正常運作，我們可以進一步使用 SNMP 至連接這些電腦交換器逕行實施斷網之措施，以維合法使用者之權益。各交換器為第二層設備，因此均支援 RFC 1493 之 Bridge MIB，我們可以 SNMP 設定交換器上之 dot1dTpFdbTable 物件，使交換器拒絕轉送違法使用 IP 位址之電腦。dot1dTpFdb Table 物件之設定必須使用電腦之 MAC 位址，我們從先前的 ipNetToMediaTable 已可得知各電腦之 MAC 位址，因此斷網的工作非常容易完成。

4. 系統實作

基於以上的系統架構，我們以校園網路為實驗對象，實際撰寫了一個 IP 位址監測程式，此 IP 位址監測程式為一由 Java 程式語言所撰寫的 SNMP 應用程式，其中 SNMP 程式介面採用 AdventNet SNMP API [1]，IP 位址監測程式每一個週期利用 SNMP 至納管的路由器讀取 ipNetToMediaTable，圖 3 顯示此監測程式對單一路由器以表格方式所輸出之 ipNetToMediaTable 資料。由圖中我們可以觀察目前網路上正在活動電腦的 IP 位址和 MAC 位址。

SNMP ipNetToMediaTable:

ipNetToMediaIfIndex (1)	ipNetToMediaPhysAddress (2)	ipNetToMediaNetAddress (3)	ipNetToMediaType (4)
2	00:50:ba:e3:1f:5c	163.22.30.1	dynamic
2	00:50:da:b3:54:f2	163.22.30.2	dynamic
2	00:50:ba:bc:9d:99	163.22.30.9	dynamic
2	00:d0:b7:07:77:0c	163.22.30.15	dynamic
2	00:50:da:b3:56:7d	163.22.30.17	dynamic
2	00:50:ba:6a:6b:0a	163.22.30.25	dynamic
2	00:e0:18:00:00:50	163.22.30.27	dynamic
2	00:48:54:50:e0:a1	163.22.30.37	dynamic
2	00:a0:0c:c8:d0:82	163.22.30.47	dynamic

圖 3 監測程式所擷取之 ipNetToMediaTable

此外，IP 位址監測程式也會至 DHCP 伺服器讀取 DHCP 存錄，針對每筆資賃記錄擷取 IP 位址、MAC 位址、租約起始時間、租約終止時間，整理成如圖 4 所示之表格資料，以方便進一步的解析工

作。值得注意的是，在搜尋 DHCP 存錄檔的記錄時，只需找出目前系統時間介於租約起始時間及租約終止時間之間的 DHCP 存錄資料即可。以避免浪費太多時間在 DHCP 存錄讀取與分析上。

DHCP log 檔中的資料

IP Address	MAC Address	starts	ends
163.22.30.172	00:50:da:b3:80:91	2003/08/06 09:00:29	2003/08/06 21:00:29
163.22.28.213	00:50:ba:e3:1f:5b	2003/08/06 09:01:28	2003/08/06 21:01:28
163.22.23.170	00:00:e2:4f:a7:5e	2003/08/06 09:03:00	2003/08/06 21:03:00
163.22.31.217	08:04:00:00:05:81	2003/08/06 09:03:14	2003/08/06 21:03:14
163.22.9.192	00:00:e2:51:6b:af	2003/08/06 09:04:52	2003/08/06 21:04:52
163.22.30.1	00:50:ba:e3:1f:5c	2003/08/06 09:11:06	2003/08/06 21:11:06
163.22.30.2	00:50:da:b3:54:f2	2003/08/06 09:11:06	2003/08/06 21:11:06
163.22.27.187	00:80:c8:91:be:32	2003/08/06 09:11:37	2003/08/06 21:11:37
163.22.8.47	00:80:ad:b8:2f:3d	2003/08/06 09:11:50	2003/08/07 09:11:50

圖 4 監測程式所擷取之 DHCP 存錄資料

從圖 3 與圖 4 所顯示的 ipNetToMediaTable 和 DHCP 存錄檔的內容，如果電腦的 IP 位址是經由 DHCP 所分配的，那麼該電腦的 IP 位址和 MAC 位址在 DHCP 存錄檔以及 ipNetToMediaTable 中的記錄應會一致，如有不同的情況發生，即表示有手動指定電腦 IP 位址的行為。利用監測程式取得的 IP 位址和 MAC 位址，經由程式執行比對工作，可將 ipNetToMediaTable 中具一致性的資料移除，留下異常的記錄，程式執行比對的結果如圖 5 所示。

比對結果，未使用 DHCP 分配的 IP 有：

IP Address	Mac Address
163.22.30.37	00:48:54:50:e0:a1

圖 5 監測程式比對結果

由比對資料的結果，可以得知目前被佔用的 IP 位址和其 MAC 位址，網管人員可以依據此資料，使用 SNMP 網管協定改變交換器中的設定值，使交換器拒絕轉送違法使用 IP 位址之電腦所送出的封包，達成保護網路合法使用者的目的。

5. 結語

IP 位址管理是網路管理人員的一項重要工作，雖然 DHCP 的發明有效地改進 IP 位址管理問題，IP 位址衝突與位址的非法使用仍舊存在，本篇論文所提出的 IP 位址指派監測機制，利用讀取路由器的位址記錄，有效掌握了網路上所有 IP 位址的使用情況；另外，DHCP 存錄資料正可以用來判斷異常使用的 IP 位址以及其對應的 MAC 位址。由 MAC 位址，我們便能追溯導致異常的來源，在目前大部分使用交換器的網路環境，我們可以進一步控制交換器，有效阻斷這些違反規定的封包。因此，因 IP 位址衝突所導致無法上網的問題，可以在第一時間獲得解決。經由實際的系統研發與測試，證明本論文所提 IP 位址指派監測方法，確實能有效解決 IP 位址衝突問題，也能藉以貫徹 DHCP 自動分派 IP 位址的政策，大量減輕網管人員在 IP 位址管理之負擔。

為有效掌控網路所有 IP 位址之使用情形，IP 位址監測器必須經常地至路由器讀取整個 ipNetToMediaTable，雖然 SNMP 訊息長度並不長，然而 ipNetToMediaTable 資料通常並不少，為降低網管通訊之負擔，可以使用 SNMPv2 之 GetBulk 指令減少網管訊息往返次數，另外由於 IP 位址的非法使用通常會延續一段時間，我們可以提高至每一路由器讀取資料的輪詢週期，而不致影響系統的正確性。此外，我們期待未來可以發展更為方便的使用者介面，整合於網路管理系統中，讓網管人員在操作上更加容易，並且加上發出警告訊息的機制，在發現有 IP 位址使用異常時，自行發出訊息訊通知網管人員進行處理。

參考文獻

[1] AdventNet Co. Ltd., "*AdventNet SNMP API 4 – SNMP Management Applications*," URL: http://www.adventnet.com/products/snmp/index.html

[2] Case, J., Fedor, M., Schoffstall, M., and Davin. J., "*A Simple Network Management Protocol (SNMP)*," RFC 1157, May 1990.

[3] Case, J., McCloghrie, K., Rose, M., and S. Waldbusser, "*Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)*", RFC 1905, January 1996.

[4] Croft, B., and J. Gilmore, "*Bootstrap Protocol (BOOTP)*", RFC 951, Stanford and SUN Microsystems, September 1985.

[5] Decker, E., Langille, P., Rijsinghani, A., and McCloghrie, K., "*Definitions of Managed Objects for Bridges*", RFC 1493, cisco Systems, Digital Equipment Corporation, Digital Equipment Corporation, Hughes LAN Systems, July 1993

[6] Droms, R., "*Dynamic Host Configuration Protocol*", RFC 2131, Bucknell University, March 1997.

[7] Harrington, D., Presuhn, R. and B. Wijnen, "*An Architecture for Describing SNMP Management Frameworks*", RFC 2571, April 1999.

[8] McCloghrie K., and M. Rose, Editors, "*Management Information Base for Network Management of TCP/IP-based internets*", STD 17, RFC 1213, Performance Systems International, March 1991.

[9] Plummer, D., "*An Ethernet Address Resolution Protocol*", STD 37, RFC 826, MIT, November 1982.