Web Based 區域網路 IP 位址監視系統
A Web Based of IP Monitor System in LAN

羅啟文* 黃圳柏* 邱基峰** 黃文祥*
國立高雄應用科技大學電機系* 國立成功大學電機工程研究所**

摘 要

近幾年來網際網路的蓬勃發展及資訊教育的發達，人們使用網路來找尋資料、追求新知的比例大幅地上升，這使得上網人數近幾年成倍數增加；然而 TCP/IP 網路架構中的 IP 位址有限，以致於 IP 位址嚴重不足。在校園中網路是老師與學生獲得知識的重要途徑，因此連上 Internet 來探索其中奧秘是很普遍的學術研究方法，但由於校園內 IP 位址的日漸不足，使得許多學生在此情況下以 DHCP (Dynamic Host Configuration Protocol)共享 IP 的方式連上 Internet。因為校園內之 IP 位址大多已分配給特定的使用者，如果因學生用 DHCP 方式動態取得 IP 位址或 IP 被竊用，則使得原 IP 的擁有者無法使用 Internet，嚴重影響網路秩序。本文於區域(乙太)網路中實作出一監視系上網路系統，利用擷取封包並加以分析的方式實現。系統中網路管理者可迅速、方便得知網域內 IP 位址之使用狀況，進而有效管理網路資源。文中將針對系統的實作詳述說明並加以討論。

關鍵詞：乙太網路，Sniffer，TCP/IP，網路管理

1. 簡 介

近年來 Internet 上網人數急速的成長，其魅力風靡於國內各大專院校中，老師與學生可以利用網路尋找所需要的資料、分享研究成果、網路繳交電子檔作業等，使得網路與學術研究緊密的結合。由於網路如此的便利，每個人都希望能經由 Internet 獲得自己的需求，因此造成校園內使用網路人數大幅成長，然而目前校園內大多是使用 TCP/IP 協定，其中 IPV4 位址在有範圍之限制下，並非所有人都能取得 IP 而連上 Internet。因此在 IP 位址僧多粥少的情況下，學生擁有 IP 位址的比例相對降低，造成許多學生以私自設定一個未使用中之 IP 位址來連接 Internet，或以 DHCP 動態地取得未使用中之 IP 位址。雖然近幾年許多因 IP 位址不足而提出的許多解決方案如 IPV6，但由於目前許多設備並無完全支援 IPV6 的功能而未能普及，另其相容性的問題也需逐一地克服，因此現階段 IPV4 仍為最普遍之技術。

當有兩台主機同時設定同一 IP，較晚登入網路之主機將因為其 IP 位址在網路上已被佔用而導致該主機無法連接 Internet。但往往較晚登入網路的主機才是該 IP 位址的擁有者，於是乎形成 IP 位址的被竊用，造成網路管理上相當困擾的問題。而在一般常見的網路管理軟體中，大都針對網路主機流量的監控，而至於盜用 IP 位址等資訊的軟體卻很少。事實上，不論是在宿舍網路或是校園網路中，IP 位址的管理也是網管人員所要處理的課題。若網管人員能在隨時可掌握其管轄範圍內 IP 位址的使用狀況並紀錄之，則對於追查非正常使用 IP 位址之工作將會有很大的幫助；有鑑於此，我們研製了一套自動取得IP位址使用資訊的IP位址監視系統。此系統中，我們利用擷取網域上所有的封包，並加以分析了解網域內 IP 位址之使用狀況，配合已建立好的使用者資訊庫，以 Web 模式顯示出分析之結果，提供雙向互動式的即時查詢系統。本文將對該系統作詳細的描述與討論。

2. 相關背景

電腦擷取封包的技術，已經不是很困難的技術，現在有許多的工具可以進行擷取封包的工作，而再此我們使用了 Linux packet capture 的函式庫作為我們的工具，來實作出 IP 位置監視系統。

Ethernet 表頭	IP 表頭	TCP 表頭	應用程式資料	乙太網路表尾

圖一、簡易封包格式

圖一為簡易模式封包格式，其最外層為 Ethernet 之訊框表頭表尾內記錄 Sender 及 Receiver 的網路卡實體位址 MAC (media access control)，其後緊接著 IP 表頭 (header)記錄著 sender 和 receiver 的 IP 位址，當我們擷取到封包時，欲取得 MAC 與 IP 位置必須先了解協定的格式，才能從正確的位置中取得這些資訊。本節將介紹 IP 位址監視系統中使用到的相關背景知識，如 IP header 格式、Ethernet Frame 格式等，至於使用的平台技術則在此不贅述。

2.1 媒體存取控制位址

媒體存取控制 MAC (media access control)位址，又稱實體位址，它是封包真正在網路上傳輸所使用的位址，它與 IP 位址間的關係可經由 ARP(Address Resolution Protocol) 或 RARP

(Reverse Address Protocol)對映查得。在 IEEE802 標準下，每一種區域網路技術都擁有自己實體定址的方法，這些定址之位址均與 IP 位址無關。在乙太網路中，每一個裝置都有一個 48 位元之 MAC 位址，以十六進位值表示，前三個位元組代表此 Ethernet 裝置之製造廠商，其餘的位元組為一有如序號且獨一無二之識別碼。製造廠商有責任為其所生產的 Ethernet 裝置建立永久的 MAC 位址，製造商代碼與獨有之序列號碼之組合將可確保所有的 Ethernet 裝置不會用到重複之 MAC 位址，MAC 位址被紀錄於封包之 Ethernet 訊框表頭(Frame header)中，其格式如圖二所示。由其協定型態欄位可判斷封包內上層資料的類型，如：IP、IPX ...等。

目的地端網路卡位置	來源端網路卡位址	協定型類
6 bytes	6 bytes	2 bytes

圖二、乙太網路的訊框表頭

2.2 IP 表頭

每部以 TCP/IP 通訊協定為基礎的主機，必須擁有一個用來識別主機位址的 IP 位址。也就是說 Internet 是利用 IP 位址作為傳輸封包的主機識別，Internet 網路上資料得以跨網路傳送至世界的任一端主機所依賴便是這 32 個位元的地址，包含這地址及其它重要網路所需資訊的便是所謂的 IP 表頭(Header)，圖三即為 IP header 的格式。

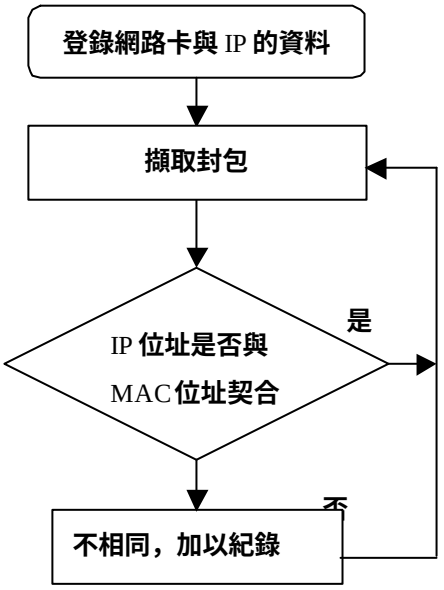
4 位元版本	4 位元標頭長度	8 位元的服務類型(TOS)	16 位元總長度(以位元組計算)	
16 位元認證			3 位元旗標	13 位元區段位移
8 位元存活時間(TTL)	8 位元通訊協定		16 位元標頭總和檢查	
32 位元來源端 IP 位址				
32 位元目的端 IP 位址				
選項(如過有的話)				
資料				

圖三、IP 的訊框表頭

3. IP 位址監視系統

在前一章節中，描述了擷取封包，並依照網路協定的格式取出了 MAC 位址與 IP 位址等資訊後，我們就對這些資訊加以分析即整理並存入資料庫中。藉由查詢資料庫中主機之 IP 位址擁有者的網路卡與 IP 封包的是否相同，來驗證 IP 位址是否遭到非法使用，進而透過網路主動警告網路管理者。本文提出的系統功能除可提供 IP 位址資訊外，並能追縱了解 IP 位址被哪些主機使用過，以方便追蹤誰是盜用者。欲隨時了解 IP 之資訊，最好的方法就是取得網路上的封包，並觀察之。封包的協定表頭裡即包含這些相關資訊。Ethernet 訊框內之來源端 MAC 位址與 IP 表頭內來源端 IP 位址代表著來源端主機之資訊。因為 IP 位址為軟體設定，隨時可以變更，不利於利用此作為對照之基礎；MAC 位址乃由硬體設定，因此主機所送出之封包於此網域內其 MAC 位址將對應於此主機。本文藉由觀察此相關欄位得知 IP 位址是否被佔用之。

要使用本系統首先必須將網域之 IP 擁有者與網路卡擁有者一同輸入於資料庫內。系統開始執行後，將開始擷取網域上之封包，取得封包後我們將對這些封包加以分析。首先將取出 Ethernet 訊框內來源端與目的端之 MAC 位址，再取出 IP 表頭中之來源端與目的端 IP 位址，利用 IP 位址擁有者與 MAC 位址擁有者做一一比對，如果相同即表示 IP 擁有者正使用著自己的主機上網，反之表示為該網路卡之使用者正佔據著別台主機之 IP，此時我們將必須把此資訊紀錄於資料庫中，經過長久之觀察，如果有主機不斷侵占別人 IP，則網路管理者可停用侵占 IP 位址者之網路以示懲戒，或以其他的方式處理，得以保障被侵占 IP 位址之使用者的權益。圖四為系統流程圖。



圖四、IP 監視系統流程圖

系統中將有一網域中網路卡之列表，當系統偵測到一張新的網路卡出現在網域中時，將會把此網路卡之 MAC 位址加入列表中，並觀察一段時間，假使此張新的網路卡一直設為是某台主機之 IP 位址，並且網管人員在與其主機擁有者確認後，此張

新網路卡之使用者將歸於此主機。

4. 結果與分析

本文中之 IP 監視系統於擷取封包並加以整理後分析，將以 Web 模式顯現之，於此模式下我們將系統分成底下幾個重要項目：

- **IP 列表**：列出網域內所有 IP 位址，裡面資訊將有 IP 位址、使用中網路卡位址、IP 位址之流量以及 IP 位址之擁有者，如圖五所示。
- **IP 位址資料**：包含 IP 擁有者、正在使用該 IP 位址之網路卡及其擁有者，以及曾經使用過該 IP 位址之網路卡，如圖六、圖七所示。
- **MAC 位址資料**：包含該網路卡之擁有者以及其目前設定之 IP 位址，並顯示出過去曾使用過之 IP 位址，圖八所示為網路卡使用狀況圖。

當第一次啟動系統時，系統將會自動列出網域內之所有 IP 位址，於開始擷取封包後，網路卡之 MAC 位址將對應於其所設定之 IP 位址。此例子當中，我們選定 140.127.114.5 來觀察它的相關資料，如圖七所示，裡面顯示了 IP 位址擁有者，和正在使用該 IP 位址之網路卡，以及曾經使用過該 IP 位址之網路卡。在此例子中我們發現有兩張網路卡設定過此 IP 位址，一個為此 IP 的擁有者 WWW2，另一個為 A 研究室，而且使用的時間不長。當一個 IP 被兩張網路卡設定過，代表了有下列幾種可能：

情況一：可能是網路卡有問題，拿到別台主機測試。

情況二：IP 使用者可能更換了電腦或是更換了網路卡。

情況三：非此 IP 擁有者故意設定此 IP 位置，也就是俗稱“盜用 IP”。

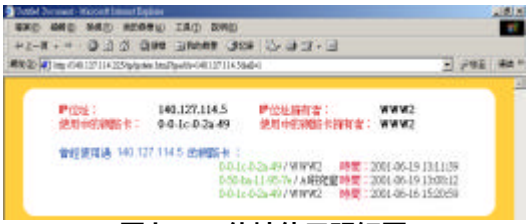
一般而言，情況一這種狀況，使用該 IP 的時間並不會太長；而情況二，該 IP 位址以後會被分配給新的網路卡，所以經過這次變動後以後，除非再換卡，否則該 IP 就會被一張網路卡設定；而情況三這種盜用的情形，一台主機沒有被分配 IP，但是使用者要使用網路，只好盜用 IP，而當不使用時，真正 IP 擁有者搶回了 IP，盜用主機欲再上網時，只好在設定其他 IP 位址。所以盜用的主機所以系統會顯示出這台主機會有設定多個 IP，且每次的時間不會太長的情形。而 WWW2 是學校的 WWW Server，都是不關機運作，不會是上述的情形一，且使用的時間只有一下子，也不會是情形二，因此可判定 A 研究室這個使用者盜用過 WWW2 的 IP 位址。

利用此資訊我們將得知 A 研究室之主機曾經盜用了 WWW2 之 IP 位址。在點選其 WWW2 使用明細我們將可列出該網路卡使用 IP 之時間，發現在 6 月 19 日 13 點 8 分，A 研究室搶走了此 IP，但在 13 點 11 分時，WWW2 又將此 IP 拿了回來。如圖七所示。

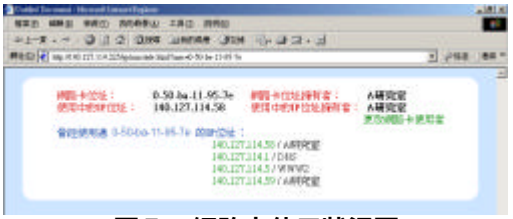
圖八為網路卡使用狀況之相關資訊，圖中表示的網路卡中，其目前所用之 IP 位址為 140.127.114.58，但是它曾經設定過 DNS、WWW2 以及 A 研究室之位址，而此網路卡乃登記屬於 A 研究室所擁有，再依照前面所提供盜用時間等歷史紀錄，因此將可看出此使用者盜用過 DNS 和 WWW2 的 IP 位址，是常常盜用他人 IP，破患網路的使用秩序。而管理者就可以根據這些資訊來對“A 研究室”這個使用者作些處置。而在經過查證之後，A 研究室只分配了 3 個 IP 位址，但裡面有 7 台電腦，所以 A 研究室才會盜用他人 IP，而現在 A 研究室以改用 NAT 的方式，讓整個研究室的電腦上網，從此 IP 監視系統中就不再出現 A 研究室盜用 IP 的紀錄。

圖五、IP 列表畫面

圖六、IP 位址使用狀態圖



圖七、IP 位址使用明細圖



圖八、網路卡使用狀況圖

5. 結論與未來研究

本文研製一 Web Based 乙太網路 IP 監視系統，系統中方便、迅速提供網管人員了解 IP 位址使用之狀況，並利用此系統所提供之資訊，對違反者作出適當的處理。文中所提出之 IP 監視系統，希望能夠作為校園內網管人員了解網域內 IP 位址使用狀態。未來我們將繼續完成其他更方便之功能，例如：提出一簡易演算法快速得知哪些為盜用 IP 位址之主機等；盜用 IP 的問題在宿舍網路中尤其嚴重，若再繼續改良程式，IP 監視系統可成為宿網管理人員的好工具。

6. 參考資料

[1] W.RICHARD STEVENS , "UNIX NETWORK PROGRAMMING" , Prentice Hall

[2] Douglas E. Comer , "Internetworking With TCP/IP" , Prentice Hall

[3] Richard Stevens 資策會譯 , "TCP/IPI llustrated 中文版" , 學貫行銷股份有限公司

[4] Paul DuBois 劉春成等編譯 , "MySQL 徹底研究" , 博碩文化

[5] Tackett & Burnett , "Linux超級手冊第五版" , 碁峰資訊有限公司

[6] Richard Stones & Neil Matthew 吳德銘譯 , "Linux程式設計教學手冊" , 碁峰資訊有限公司

[7] Jesus Castagnetto .etc 許鳴程 譯 , "專業 PHP 程式設計" , 碁峰資訊有限公司

[8] Andrew Sun 徐錦基 譯 , "PPP 網路管理" , O' REILLY

[9]Linux libpcap 說明文件

[10] " My libpcap tutorial " ,
http://www.cse.nau.edu/~mc8/Socket/Tutorials/section1.html

[11] 黃圳柏、羅啟文、黃文祥、邱基峰，" 建構在 Web 上之網路流量統計分析系統 "，TANET 2001 研討會，2001 年，下冊 415 頁。