區域網路異常 IP 偵測技術探討

作者/資訊作戰組 陳寶騏 中校

提要

目前國軍各單位營區內電腦主機不斷增加，而資訊安全管制工作也日趨嚴格，單位資訊官要如何管制電腦 IP 位址運用，除了透過動態主機組態協定（Dynamic Host Configuration Protocol,DHCP）[1]對網路卡卡號（MAC Address,MAC）及 IP 提供一個分配的方案之外，要知道實際網路狀況只有運用掃瞄軟體來清查單位 IP 運用，但是這些共享軟體的掃瞄狀況容易受到個人電腦上所安裝的個人防火牆(Fire-wall)軟體所阻擋，而無法獲得正確的結果，本文描述以 Linux、PHP 及 PostgreSQL 所建構的網路掃瞄系統，並利用簡單網路管理協定（Simple network management protocol,SNMP）[2]取得路由器及交換器上之管理資訊庫（Management information base,MIB）[3]的訊息，並加以整理得到區域網路的電腦存活狀況，掌握單位實際的 IP 運用狀況，並從資料庫中分析出異常的 IP，可提供網路管理者解決網路問題時有利的參考資訊，進而提昇單位實體資訊安全。

壹、緒論

一、研究動機

目前各單位營區內電腦主機不斷增加，而資訊安全管制工作也日趨嚴格，單位資訊官要如何管制電腦 IP 位址運用，除了透過 DHCP 伺服器依據每個使用者的網路卡卡號設定並分配一個固定的 IP 之外，亦可運用掃瞄軟體來清查單位 IP 運用，但是這些共享軟體的掃瞄有幾個問題：

(一)容易受到個人電腦防火牆軟體的阻擋，無法正確的偵測。

(二)無法設定時間對單位電腦 IP 位址持續自動掃瞄

(三)無法記錄過去掃瞄的結果，並提供後續分析比對

亦即只能記錄掃瞄當時的網路狀況，掃瞄的記錄則無法保留下來，通常程式結束後，必須重新再開始掃瞄始可提供結果。供後續比對及查詢。

另外假設某單位資訊官獲上級單位通知，單位內有 IP10.22.33.144 疑似中毒，並嘗試感染及掃瞄其他友軍單位主機，但查詢單位 DHCP 及管制的 IP 資料庫

---

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

[2] Case, J., Fedor, M., Schoffstall, M., and Davin, J., “A Simple Network Management Protocol (SNMP),” RFC-1157, 1990.

[3] McCloghrie, K. and Rose, M., “Management Information Base for Network Management of TCP/IP-based internets: MIB-II, RFC-1213,” 1990.

中，並無此主機資料，立即使用掃瞄工具清查網路亦無所獲，單位平時雖有編組對內部網路實施弱點及資源分享掃瞄，但僅記錄違規資料，亦無此 IP 的相關資料，則該資訊官應如何處置？設定有以下的問題：

(一)該主機可能自行設定符合單位網路架構的 IP 組態，故單位 DHCP 資料庫中查無資料。

(二)掃瞄不到該主機，不能證實主機不存在，該主機可能具阻擋被掃瞄的功能。

(三)現行可獲得的掃瞄軟體不能持續記錄所掃瞄的 IP 資料，僅能表達現況。

(四)若有工具可自動掃瞄及蒐集網路的 IP 主機狀況，此時資訊官即可查詢資料庫，進一步查證該主機的實際存活記錄。

本研究即探討是否可運用簡便的方式協助單位資訊官掌握單位 IP 及網路卡卡號的狀況，進而提昇單位實體資訊安全。

二、研究目的

針對目前國軍網路上各營區的網路管理及 IP 使用及檢查的問題，我們可以依區域網路的現況區分以下幾類的營區（如表一）：

表一 國軍營區網路管理能力區分

區　　分	說　　明
A 類營區網路	內部區域網路建置完整，具有智慧型的網路交換器和路由器，並建置管理系統可協助資訊官管理內部 IP 的分配與網路卡的設定問題，使用者不得任意更改設定，每個人使用固定的 IP 及固定的交換器連接埠。
B 類營區網路	內部區域網路為一般無網管功能的交換器或集線器所構成，路由器具網管功能，可提供部分資訊，內部無管理系統可協助 IP 分配與管理，但可建置網域伺服器控管個人電腦，並設定個人電腦均採用 DHCP，使用者不得任意更改設定，每個人使用固定的 IP。
C 類營區網路	內部區域網路完全沒有任何具網管功能交換器，所有個人電腦互連在相同的網域，但可建置網域伺服器控管個人電腦，並設定個人電腦均採用 DHCP，使用者不得任意更改設定，每個人使用固定的 IP。
D 類營區網路	內部區域網路完全沒有任何具網管功能交換器，所有個人電腦互連在相同的網域，也不具備系統可以管理 IP 分配與管理。

目前本軍營區網路大部分屬於 C 類或 D 類的營區網路，現行國軍各單位大

部分均未有適當網路管理系統可提供單位區域網路的電腦持續 IP 偵測與記錄的軟體（尤其是司令部級以下單位，受限於單位預算及資訊專業人力），但是目前資訊安全問題非常多，資訊官經常要面對一個問題，某些屬於營區內的網段的IP，在國軍網路上發生問題，例如，中毒電腦去感染其他單位電腦、任意開啟資源分享遭到上級 CERT 單位稽核、使用駭客工具去掃瞄及偵測其他單位電腦等等，但是資訊官無法掌握這些 IP 屬於那些電腦使用，因為內部並無可用的網路管理工具可以限制使用者一定使用特定的 IP，所以發生問題時，也無法確定 IP 究竟為何人所使用。

本研究即希望運用 Linux 平台構建一個簡易網路管理系統，可支援不間斷掃瞄單位 IP 位址，並簡化各單位資訊官電腦 IP 管理，掌握異常 IP，並針對異常實施檢測及處置，避免影響單位資訊安全。

在管理面，本研究希望提供一套簡易 IP 偵測系統，簡化各單位資訊官對實際 IP 運用偵測作業，並掌握異常電腦 IP。在技術面，則希望：建立各種 IP 偵測技術、建立持續性 IP 與 MAC 位址的偵測記錄及建置運用共通性平台構建 IP 偵測系統。

目前大部分的網路設備都提供了 SNMP 以協助管理及監視設備本身的狀況，網路設備將網管資訊記錄在 MIB 中，本文即介紹利用 SNMP 取得路由器上的主機 IP 位址與網路卡卡號的對應表，整理得到單位網路的主機存活狀況，並透過具網路管理功能的交換器的鎖定網路卡卡號功能，來實現早期發現異常 IP 的功能，可提供網路管理者解決網路問題時有利的參考資訊。

三、研究方法與架構

本研究將透過理論及文獻探討，分析研究掌握 IP 掃瞄方式，並以實作方式，驗證可執行在通資學校的校園網路架構下。在實作部分，則運用現行免費 Linux 作業系統，架設實驗平台，包含網站 Apache、網頁程式 PHP、資料庫軟體 PostgresSQL，利用此類網頁式平台架構，可偵測單位的路由器及交換器上的網路管理資訊，並進而定時掃瞄單位 IP 網段，記錄到資料庫中，藉分析資料庫的資訊，掌握單位異常 IP 的資訊。

四、研究範圍與限制

本文研究的方式主要針對具網路管理功能路由器能詳實記錄所轉送的 IP 及網路卡卡號，有效利用這些資訊將有助於瞭解實際網路運作情形。研究將假設單位應該有具網路管理功能交換器及路由器，單位已經與國軍網路連線，部分單位可能具有可以鎖網路卡卡號的交換器（例如 Cisco 的 Catalyst 2950 等）。

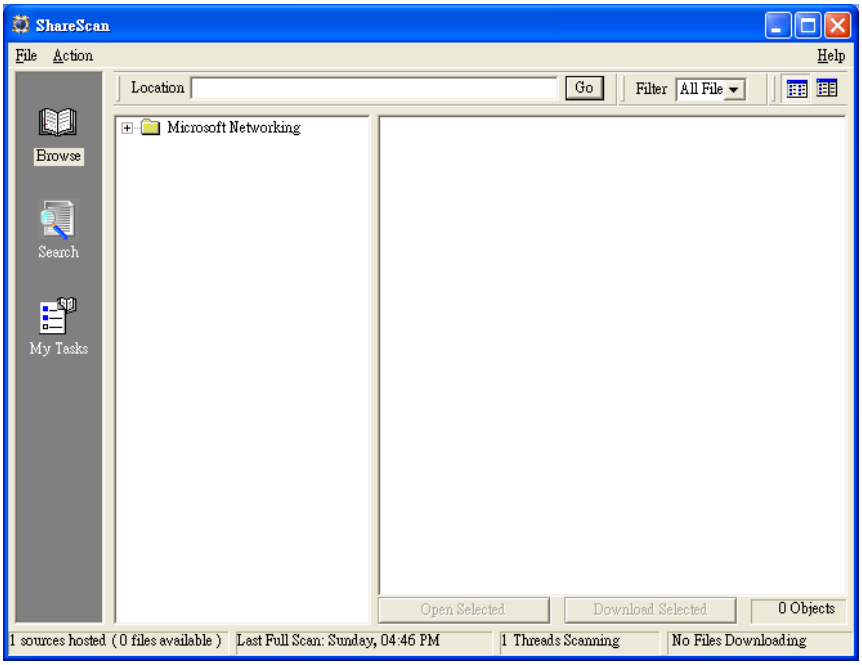
若單位僅有無網管功能路由器連外，則將限制無法取得真實的網路存活主

機狀況，僅能藉由主動偵測主機方式實施記錄，無法蒐集到正確的 IP 與 MAC 資訊，部分電腦可以阻擋偵測封包，造成「隱形」的效果，使偵測程式無法正常運作。

貳、本文

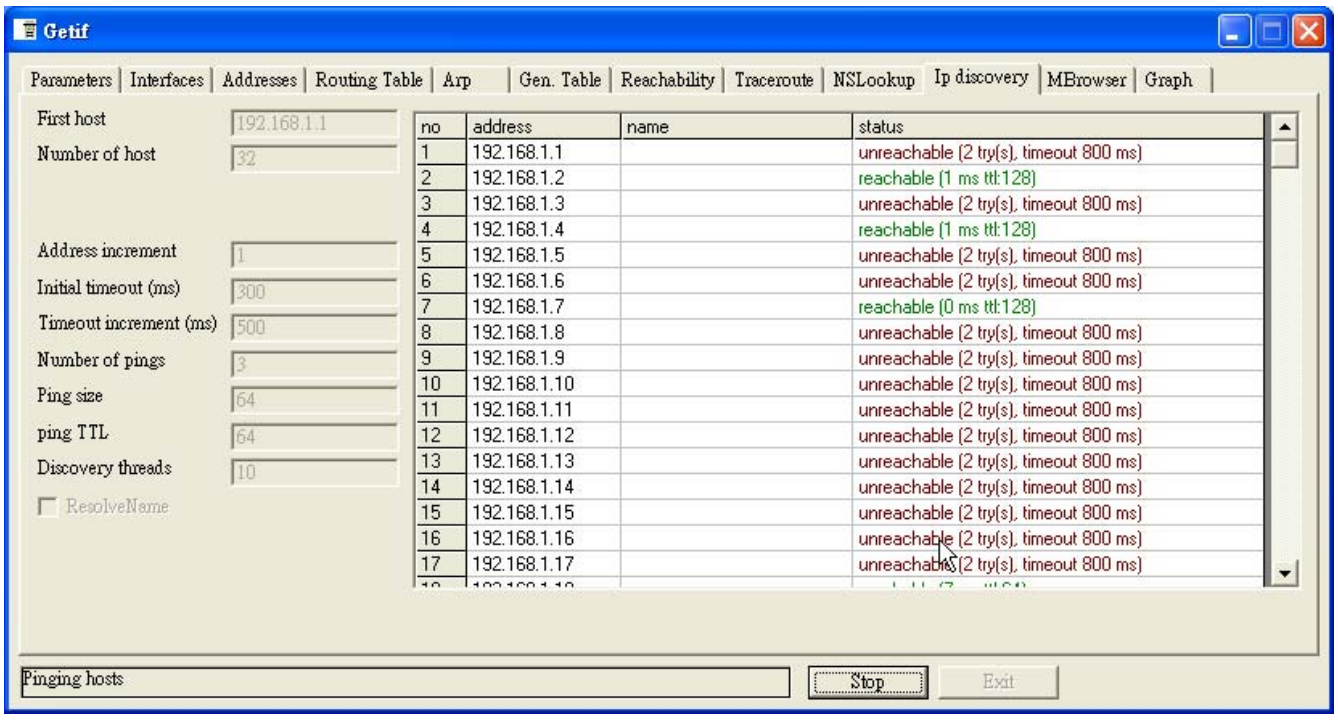
一、營區網路IP偵測問題

目前國軍各營區內資訊設備不斷增加，資訊設備的掌握也比較困難，而這些主機及網路設備的 IP 經常因為使用者不熟悉的因素，可能經常變動，另營區內若網路節點及資訊埠也漸漸成長，一般各營區若使用 1 個 Class C 的網域，便約有 250 資訊設備可以用，平常即開機使用者，並無法確認其數量。目前有部分軟體可以支援區域網路網段的掃瞄，如：sharescan（如圖一），而且支援對網路芳鄰資源分享資料夾的偵測，有利於單位資訊官掌握單位內部主機運作情況，對於非法之資源分享行為也能有效偵測。



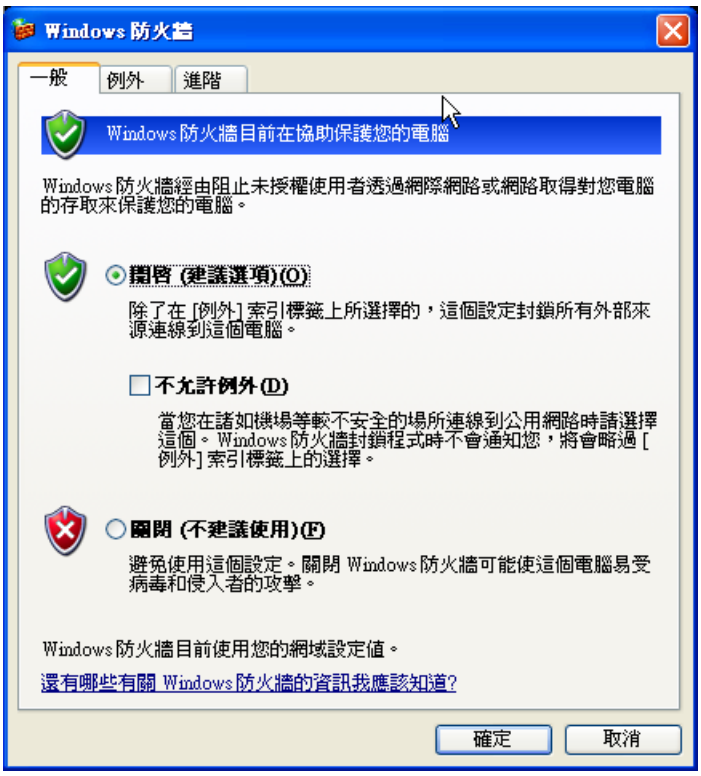
圖一 sharescan

另外，也可以下載許多掃瞄的工具程式，例如可提供網管功能的 getif。可針對特定區域主機實施掃瞄（如圖二）。



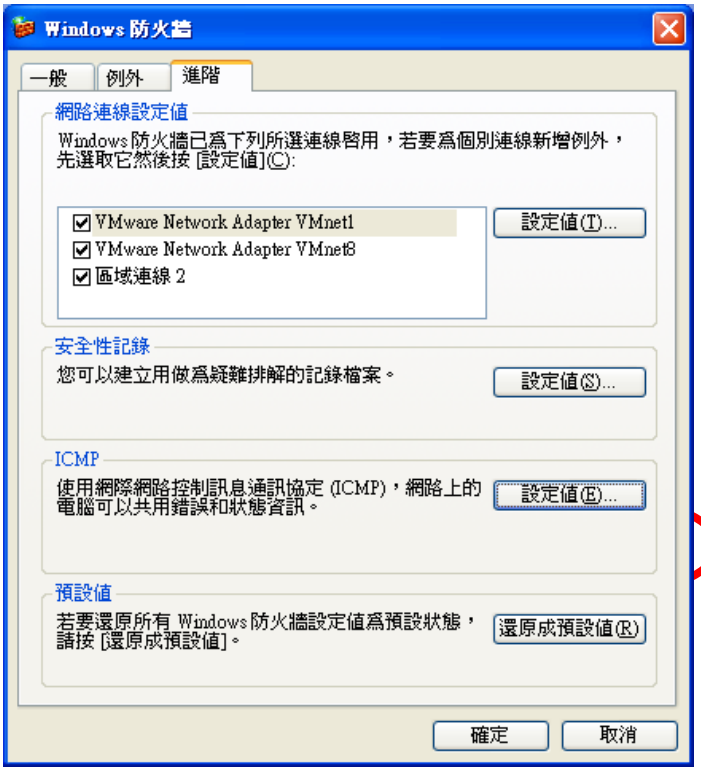
圖二 利用 getif 掃瞄某 IP 網段

這些偵測到的資料，只是單純顯示了目前網路上可偵測到的存活主機的狀況，沒有顯示主機所在的位置，也無法瞭解這個主機先前存在的狀況，若主機更改電腦名稱或主機更改 IP 位址，將無從判斷主機相關的資訊。假定惡意的使用者熟知單位內部的網域參數、如 IP 位址的範圍、交換器及路由器的架構等、預設閘道器位址，那麼他將可以不斷更改 IP 位址以逃避這些掃瞄及檢查，而且惡意的使用者也能運用個人電腦的內建的防火牆或另外安裝個人防火牆，來防止軟體對電腦的偵測，使電腦幾乎隱形。目前在作業系統的部分，可利用 Windows XP 內建之防火牆來阻擋其他電腦的偵測，如圖三所示，Windows XP 的使用者只要啟動 Windows 防火牆，其預設值即無法對電腦實施偵測。

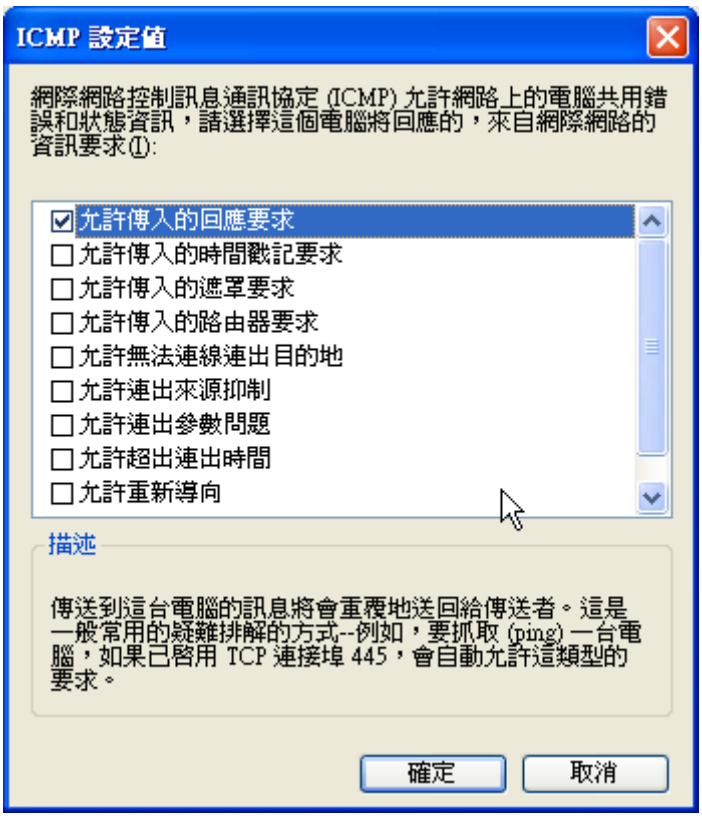


圖三　啟動作業系統內建的防火牆

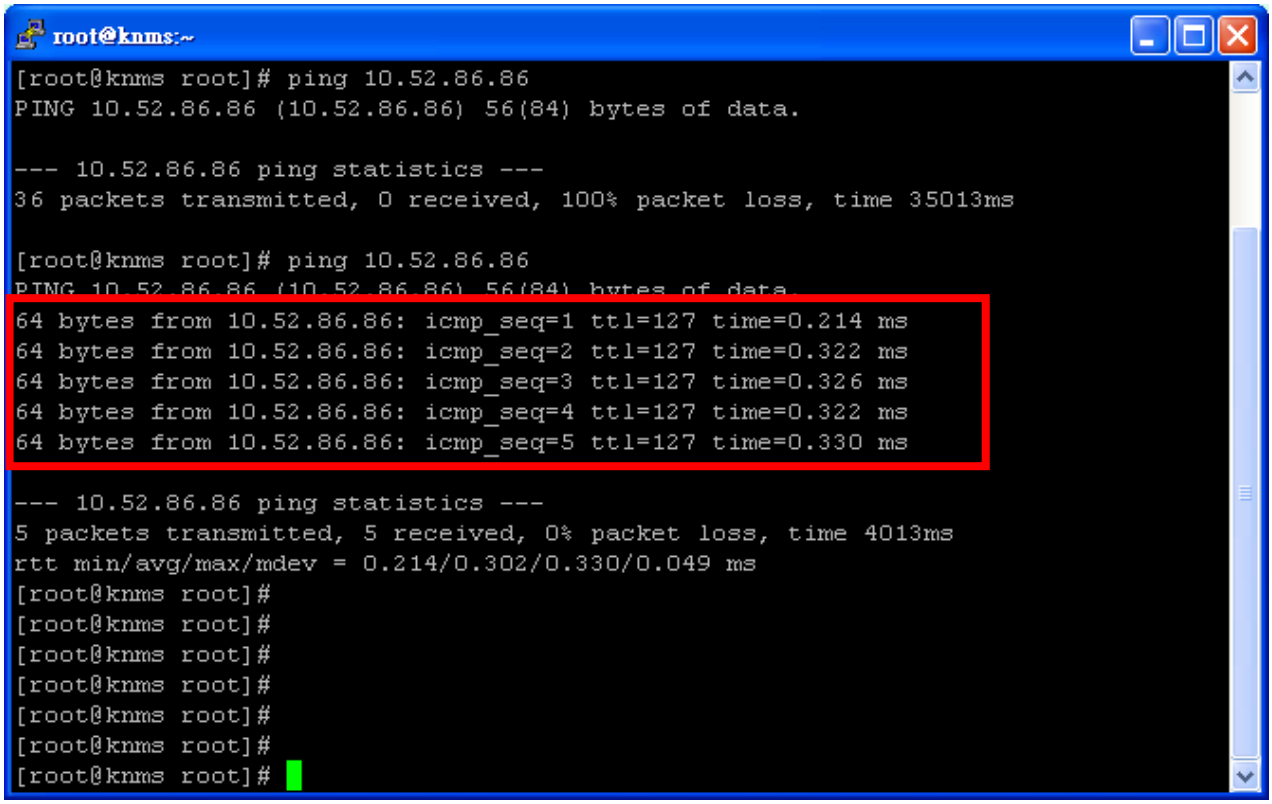
若更改設定值，設定「允許傳入的回應要求」，如圖四及圖五，則將開放讓電腦可以被其他主機以 ping 的指令來進行偵測，如圖六。



圖四 修改電腦內建防火牆對 ICMP 的設定值

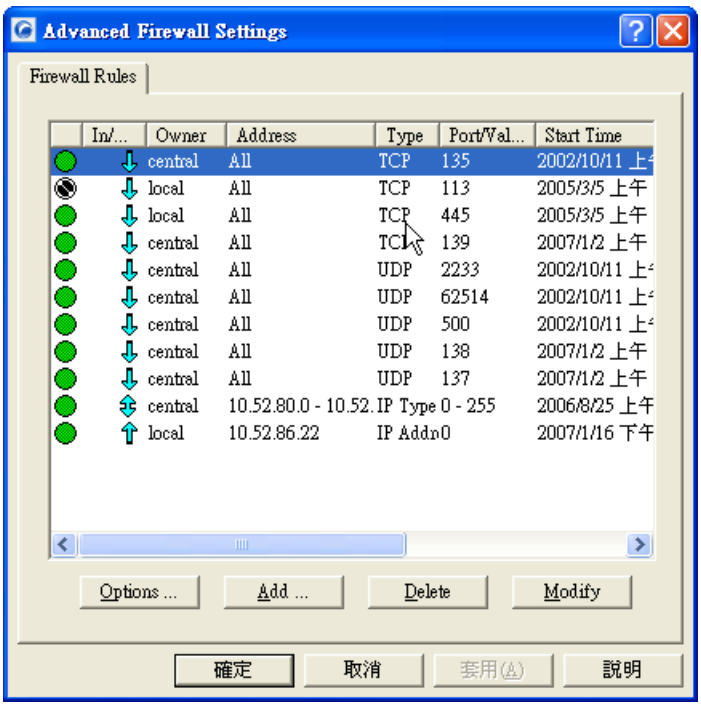


圖五



圖六 以 ping 指令執行對個人電腦存活的偵測

另外，也可以使用個人防火牆如 BlackICE 等，封鎖電腦對於其他主機所傳入的 ICMP 回應要求，即可讓電腦不被其他主機偵測，如圖七。



圖七 個人防火牆 BlackICE

目前在營區中可用的 IP 控管技術包含：

(一)DHCP 控管技術

利用自建資料庫結合 Windows 的 DHCP 伺服器，配合利用 AD 網域技術控管，並結合存取 DHCP 伺服器登錄資料功能，將實際所偵測到網路的狀況與 DHCP 登錄資料實施比對，可以得到更多的訊息。

(二)利用交換器直接鎖定使用者的網路卡卡號

部分較新式的交換器（如 Cisco Catalyst 2950、3750 等型號的交換器）已經支援可以設定使用者的卡號，將之指派給特定的交換器上某個埠，使得使用者不能任意更換交換器的埠號，必須在指定的埠才能正常連線使用，如此可以避免非授權人員連入網路內，造成不可預期的損壞。

但是以上這些控管技術必須由去管理者去完整設定後，方能有效果，若區域網路環境無相關可供網路管理設備，亦無強制使用者不能任意更改電腦設定，則網路內將有漏洞產生，為強化資訊安全，網路管理者仍應對網路實施掃瞄，並記錄各主機 IP 使用狀況，以備問題發生時，能有歷史記錄進行查詢。以下便說明如何對網路上的主機實施偵測。

二、IP主機偵測技術

(一)主機偵測技術

主機偵測技術依黃耀文[4]的區分有下列幾種方法：

[4] 黃耀文，黃世昆，網路對映技術探討與評估，資訊安全通訊，Vol. 7，No. 2，2001，頁 52-75。

1.Ping Sweep。

2.Non-Echo ICMP Sweep。

3.ICMP Error Sweep。

4.ICMP Broadcast Sweep。

5.TCP and UDP Sweep。

其中只有「Ping Sweep」及「TCP Sweep」能提供較高的可用度，為通用的主機偵測方法，其他方法只能用在 TCP/IP 實作完整的網路設備，並不適用在大量偵測整個網路主機可到達的狀況。

「Ping Sweep」的方式主要送出 ICMP 的回應請求封包（ICMP Echo，Type 8）給待測主機位址，如果收到一個 ICMP 的回應回覆封包（ICMP Echo Reply，type 0），那麼我們便認定該主機位址是在網路上並且可以到達的。

「TCP Sweep」的方式則是利用 TCP 連線前先進行「三段式交握」的原理，傳送一個「SYN」封包到待測主機位址上的任何一個服務埠，如果該主機的服務埠的狀態是開啟的（listening），我們將可從這個目標收到一個「SYN ACK」回應。如果該主機的服務埠的狀態是關閉的，我們將收到一個「RESET」的回應封包。

由於 PHP 不提供 ICMP 相關的函式，所以在本研究中，我們利用了 PHP 所提供的 Socket 函式中的 fsockopen()的功能，利用「TCP Sweep」的原理， 用 fsockopen()送出 TCP 的封包，設定逾時參數為 0.01 秒，試圖與目標主機的某個服務埠連線，如果能完成連線，表示目標主機可到達，如果接收到目標主機的錯誤訊息（通常是 ICMP 封包，表示服務埠不存在等訊息），那麼我們也可以知道目標主機是可到達。如果過了設定的時間，或者收到鄰近路由器所傳回的錯誤訊息（目標網路不可到達），我們便可判斷目標主機不可到達。利用這個方法，也可以達到偵測主機的效果，而且 fsockopen()函式提供逾時參數，配合待偵測網路的狀況，我們可以設定適當的逾時參數，以提昇主機偵測的效率。

(二)動態主機組態協定 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 [5]協

[5] 同註 1。

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。

由於每個電腦用戶端會向DHCP伺服器取得IP，因此DHCP伺服器上也會保留目前網路上大部分的用戶端設定，這些資訊有助於我們瞭解目前網路的狀況，我們可以從DHCP伺服器上取得IP資料與MAC位址資料，但是如果使用者是自行設定主機的IP組態，則DHCP伺服器便無法提供可用的參考資訊。

(三)簡單網路管理協定 SNMP

簡單網路管理協定 (Simple Network Management Protocol, SNMP)[6] 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、SNMPv2、SNMPv3，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。

符合 SNMP 標準架構之網管包括四個構成元素，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

[6] 同註 2。

援 TCP/IP 通信協定之網路設備，均會支援標準的 MIB-II 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[7]。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。

(四)利用 MIB 資料找出 IP 位址存活狀態

MIB II 屬於標準的 MIB 資料庫，在整個 MIB 中被定義在 1.3.6.1.2.1 的位置，主要是為了路由器的控制管理所設計的。MIB II 共分為 system、interface、at、ip、icmp、tcp、udp、egp、transmission、snmp 共 10 個類別，記錄各種控制、傳輸、路由等資訊，這裡我們所關心的是它的第二個類別 interface 和第四個類別 ip。

Interface 類別下有一個 Interface Table，Interface Table 可以告訴我們這台路由器每一個通訊埠現在的使用狀況。在 ip 類別下，我們可以取得 Routing Table 及 Net to Media Table。Routing Table 紀錄了不同的 ip address 應該送往那一個節點轉送，而 Net to Media Table 告訴我們 Router 的每一個埠和哪些機器直接相連[8]。Routing Table 及 Net to Media Table 詳細的欄位內容分別列於表二及表三。

表二　Routing Table 欄位說明

欄位名稱	資料型態	說明
ipRouteDest	IPAddress	destination IP address
ipRouteIfIndex	INTEGER	經由那個 port 路由
ipRouteMetric1	INTEGER	primary routing metric(和 iprouteproto 有關)
ipRouteMetric2	INTEGER	routing metric 替代方案
ipRouteMetric3	INTEGER	routing metric 第三個方案
ipRouteMetric4	INTEGER	routing metric 第四個方案
ipRouteNextHop	IPAddress	下一個 hop 的 IP 位址
ipRouteType	INTEGER	route 方式(直接給誰/還要轉接)
ipRouteProto	INTEGER	路由使用的通訊協定
ipRouteAge	INTEGER	這一個路由記錄上一次修改現在經過幾秒
ipRouteMask	IPAddress	路由位址的 Net Mask

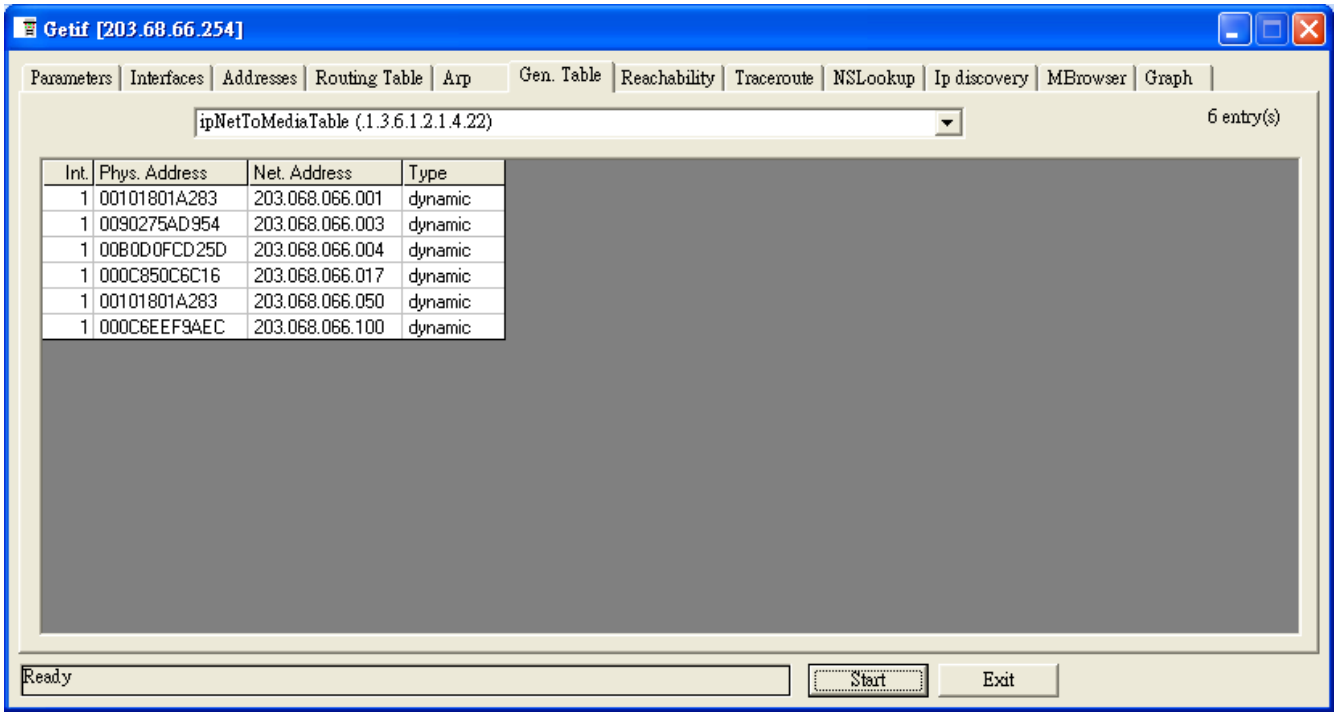
表三　Net To Media Table 欄位說明

欄位名稱	資料型態	說明
ipNetToMediaIfIndex	INTEGER	interface 的索引值
ipNetToMediaPhysAddress	OCTET STRING	和 interface 直接相連機器的 MAC 位址
ipNetToMediaNetAddress	IpAddress	和 interface 直接相連機器的 IP 位址
ipNetToMediaType	INTEGER	ipNetToMedia 記錄的型態

[7] 范恭達，陳彥錚，李思宏，「IP 位址指派之監測與管理」，2003 年台灣網際網路研討會，頁 1-3。
[8] 孫文駿，林盈達，「網域拓撲探測與延遲測量」，1999。

(五)取得路由器上的 IP 與 MAC 位址對照表

路由器的 MIB 包含了 system、interfaces、ip 等群組，由 ipAddrTable 得到指定給路由器介面的 IP 位址，ipRouteTable 得到路由器所設定所學習的路徑表，ipNetToMediaTable 暫存了路由器上 IP 位址與網路卡位址的對照表，如圖八。

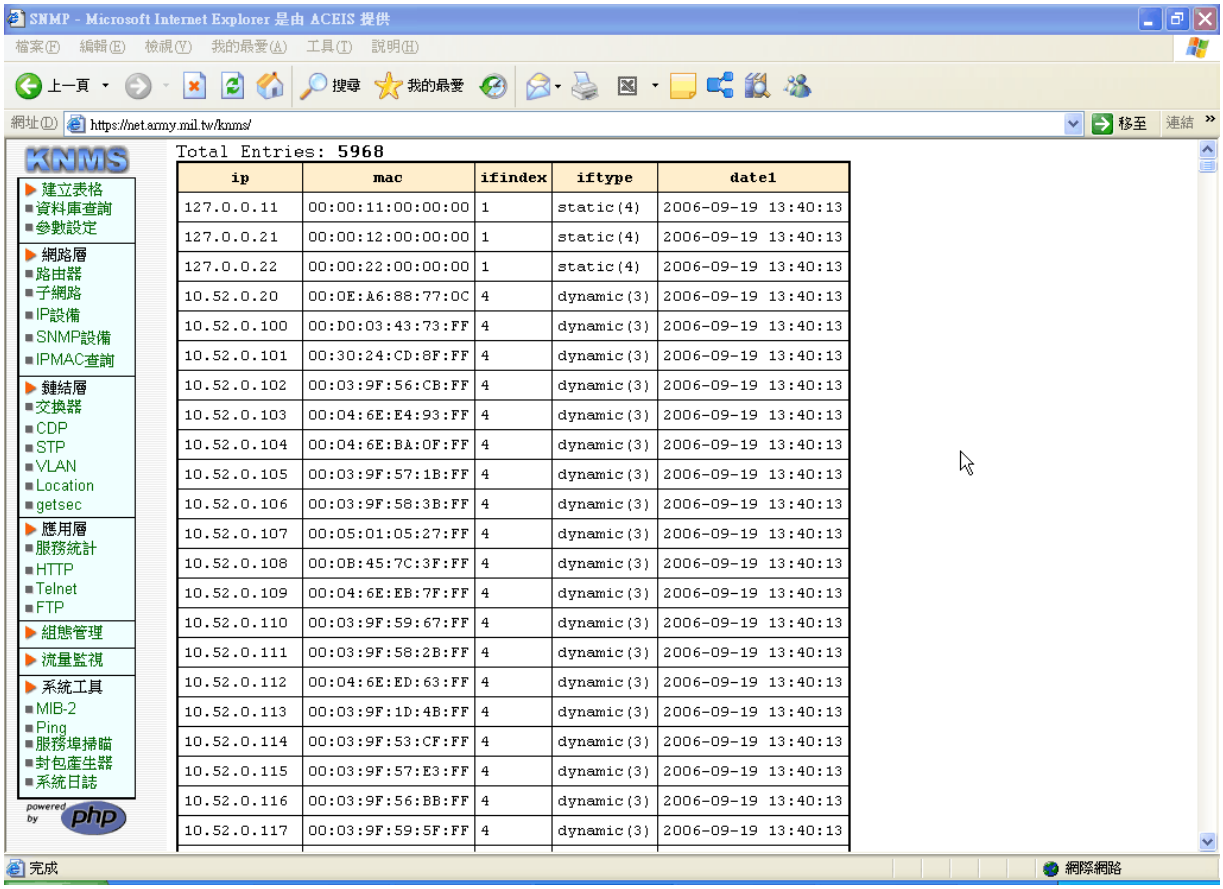


圖八 利用 getif 取得路由器上的 ipNetToMediaTable

具備網路管理功能的路由器會記錄通過它的主機位址及網路卡的卡號，並記錄在 ipNetToMediaTable 這個內部的資料表中，我們可以把它取出來，放在資料庫中，並加上時間的記錄，便可以提供後續的資料比對。

我們可以逐一取得單位網路上主要路由器 MIB 中的 IP 位址與 MAC 位址的對照表 ipNetToMediaTable 來加以分析，以瞭解該網路環境實際連接的網路設備（如主機或是電腦），並儲存到資料庫中。

其記錄到資料庫的演算法則是，對於每筆 ipNetToMediaTable 的資料，我們在儲存前，先查詢資料庫中是否已經有相同 IP 與 MAC 的記錄，如果有，便不重複儲存，如果不相同，便新增一筆記錄，並註記發現的日期，並設定系統每日定期取得路由器上最新的資料並存入資料庫。我們可以透過資料庫查詢的功能，比對資料庫中 IP 位址或 MAC 位址重複的狀況，便可以得知網路異常 IP 位址設定情形。圖九顯示取得路由器 ipNetToMediaTable 的範例。



圖九 取得路由器上的 ipNetToMediaTable

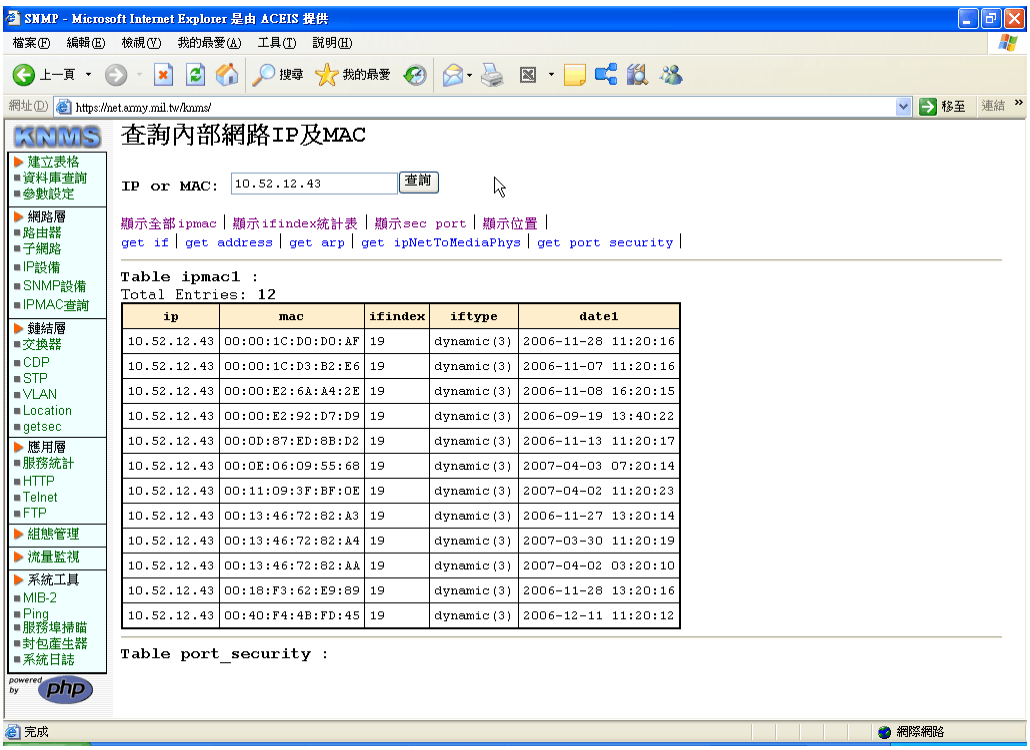
三、如何運用資料庫進行比對

透過 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，我們可以過濾出以下二種異常情形[9]：

(一)IP 位址相同， MAC 位址不同

表示有一台電腦已經更換網卡，或者有某部電腦自行設定 IP 位址，而此 IP 位址實際上已分配給某一合法使用者。如圖十所示，某一電腦主機其 IP 位址為 10.52.12.43，MAC 位址自 2006-09-19 開始，不斷更換，有異常的行為，網路管理人員可依據記錄來查詢該 IP 主機的運用情形。

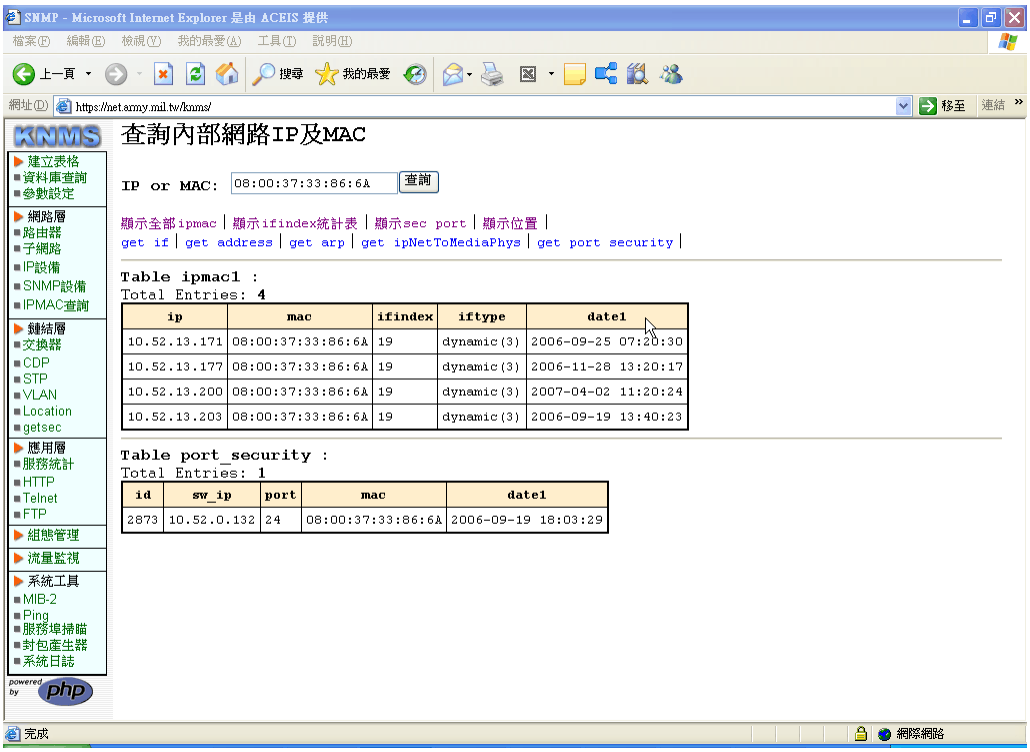
[9] 同註 7。



圖十　IP 位址相同，但 MAC 位址不同

(二)MAC 位址相同的， IP 位址不同

表示有一使用者自行設定 IP 位址，或者自 DHCP 獲得另一合法 IP 位址。如圖十一所示，查詢 MAC 位址：08:00:37:33:86:6A，系統可顯示其分別在四個不同的日期，更換了四個不同的 IP 位址，有異常的網路操作情形，網路管理人員可依據此一記錄，瞭解使用者是否合法更新 IP 位址，或者有其他的問題。



圖十一　系統提供查詢 IP 與 MAC 位址記錄

上述二種情形中，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，通常第二種狀況是我們比較需要觀察的對象。

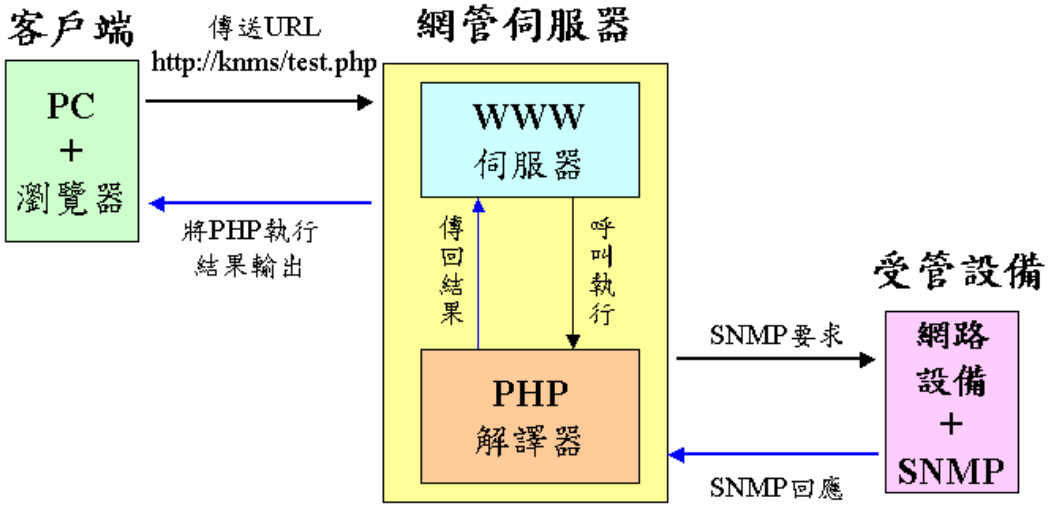
在找出違法使用 IP 位址之電腦後，如果這些 IP 位址的違法使用危及網路之正常運作，我們可以進一步使用 SNMP 至連接這些電腦交換器逕行實施斷網之措施，以維合法使用者之權益。各交換器為第二層設備，因此均支援 RFC 1493 之 BridgeMIB ， 我們可以 SNMP 設定交換器上之 dot1dTpFdbTable 物件，使交換器拒絕轉送違法使用 IP 位址之電腦。dot1dTpFdb Table 物件之設定必須使用電腦之 MAC 位址， 我們從先前的 ipNetToMediaTable 已可得知各電腦之 MAC 位址，因此斷網的工作非常容易完成。

四、實作系統架構

(一)網頁描述語言 PHP

PHP 是一個伺服器端、跨平台的超文字連結語言（hyper text markup language， HTML）及嵌入命令稿語言（embedded scripting language）。大部分的語法很類似 C、Java 和 Perl。其發展的目的在允許網站的發展者快速地撰寫動態的網頁。PHP 獨立於瀏覽器；是伺服器端語言，PHP 程式碼在伺服器端執行，結果送給瀏覽器，在瀏覽器中檢視原始檔，看不到 PHP 的程式片段。PHP 從 1994 年就開始發展，目前發展到 PHP5，加入 Zend Engine，以提昇整體運作的效能。

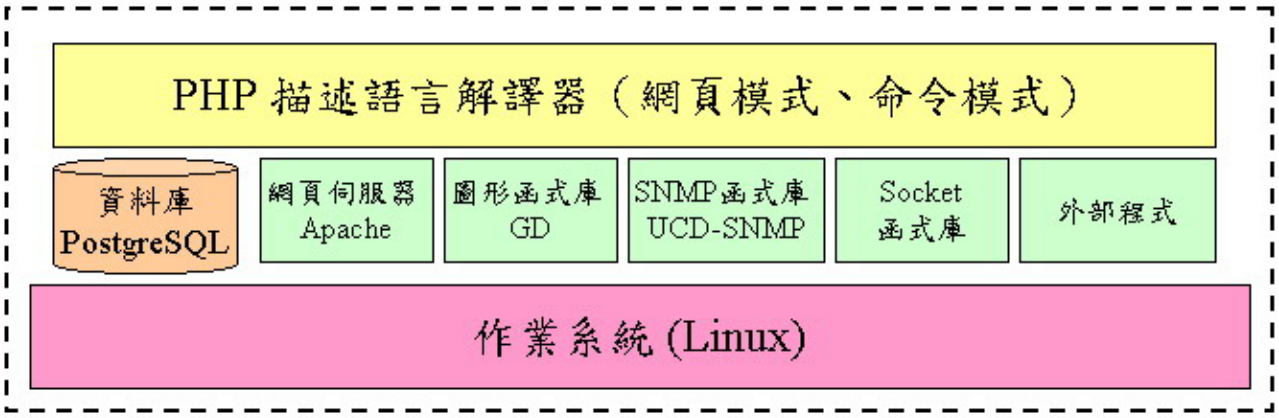
PHP 經過適當的組態及編譯，能夠支援資料庫、SNMP、Graph 及 Socket 的操作。圖十二為 PHP 在 WWW 伺服器上執行網管程式的架構圖。



圖十二 PHP 執行網管工作示意圖

(二)系統架構與實驗環境

本系統架構區分為軟體架構及硬體架構。軟體架構如圖十三。各模組均以 PHP 完成。



圖十三 系統軟體架構圖

而系統硬體主要由網管伺服器及一般電腦所組成，在網管伺服器上安裝網頁伺服器、圖形函式庫、SNMP 函式庫、資料庫管理系統及本系統的程式組，由一般電腦開啟瀏覽器連上網管伺服器上的網頁，透過網管伺服器來探索網路、查詢資料、管理網路及偵測網路。

(三)實驗數據分析

經過測試，系統首次執行為 96 年 4 月 9 日，首次獲得 IP 為 397 部（如表四），掃描時間為 1430，此為當時電腦已開機，並通過路由器所記錄的電腦數量，系統自動記錄所獲得的 IP 與網路卡卡號，爾後每日固定時間在 1230 及 1830 各偵測乙次，隔日再掃描時，系統會比對已存入資料庫的 IP 與網路卡卡號，當 IP 與網路卡卡號不相同時，才新增到資料庫中。

系統依據網路卡的卡號，結合 IEEE 的 OUI 資料庫，可提供網路卡的製造商資料，這個資料可以協助資訊官判斷 IP 及網路卡卡號所屬的電腦(如表五)。

表四 實作測試偵測 IP 數據分析表

項　次	掃　描　日　期	掃 描　I P　數	備　　考
1	96-04-09	397	掃描 IP 數為每日偵測所增加的數量
2	96-04-10	20	
3	96-04-11	5	
4	96-04-12	4	
5	96-04-13	11	
6	96-04-14	5	
7	96-04-15	1	
8	96-04-16	7	

9	96-04-17	10	
10	96-04-18	21	
11	96-04-19	15	
12	96-04-20	14	
13	96-04-21	0	
14	96-04-22	2	
15	96-04-23	5	

表五 實作測試偵測 IP 數據分析表 (部分資料)

IP	MAC	ifindex	iftype	Date	NIC Com.
10.52.86.68	00:0C:29:62:46:99	171	dynamic(3)	2007/4/19 18:30	VMware,
10.52.86.82	00:0C:29:18:67:E1	171	dynamic(3)	2007/4/19 18:30	VMware,
10.52.86.85	00:0C:29:B9:43:CD	171	dynamic(3)	2007/4/19 23:30	VMware,
10.52.86.88	00:0F:1F:A2:04:14	171	dynamic(3)	2007/4/20 06:30	WW
10.52.86.90	00:0C:29:A1:F5:C4	171	dynamic(3)	2007/4/20 06:30	VMware,
10.52.86.91	00:0C:29:FD:04:8F	171	dynamic(3)	2007/4/20 06:30	VMware,
10.52.81.134	00:09:6B:37:78:0E	130	dynamic(3)	2007/4/20 12:30	IBM
10.52.81.140	00:0F:1F:A1:E1:C7	130	dynamic(3)	2007/4/20 12:30	WW
10.52.83.59	00:14:85:3B:D3:B1	148	dynamic(3)	2007/4/20 12:30	Giga-Byte
10.52.84.6	00:11:D8:EE:40:02	158	dynamic(3)	2007/4/20 12:30	ASUSTek
10.52.86.85	00:0F:1F:A1:9D:E2	171	dynamic(3)	2007/4/20 12:30	WW
10.52.80.66	00:0E:A6:82:AE:91	127	dynamic(3)	2007/4/20 18:30	ASUSTEK
10.52.86.70	00:20:ED:31:BC:FD	171	dynamic(3)	2007/4/20 18:30	GIGA-BYTE
10.52.86.78	00:0C:29:F1:9D:02	171	dynamic(3)	2007/4/20 18:30	VMware,
10.52.86.87	00:0F:1F:A1:9D:E2	171	dynamic(3)	2007/4/20 18:30	WW
10.52.86.93	00:0C:29:AF:91:20	171	dynamic(3)	2007/4/20 18:30	VMware,
10.52.86.94	00:0C:29:94:C0:FA	171	dynamic(3)	2007/4/20 18:30	VMware,
10.52.86.61	00:0C:29:2D:58:3F	171	dynamic(3)	2007/4/22 23:30	VMware,
10.52.86.75	00:0C:29:71:0F:C4	171	dynamic(3)	2007/4/22 23:30	VMware,
10.52.81.201	00:20:ED:32:35:C8	131	dynamic(3)	2007/4/23 12:30	GIGA-BYTE
10.52.86.64	00:0C:29:1E:6E:07	171	dynamic(3)	2007/4/23 12:30	VMware,
10.52.86.68	00:11:D8:E1:CD:D1	171	dynamic(3)	2007/4/23 12:30	ASUSTek
10.52.86.70	00:40:F4:22:49:D5	171	dynamic(3)	2007/4/23 12:30	CAMEO
10.52.86.71	00:17:31:6C:B4:DF	171	dynamic(3)	2007/4/23 12:30	ASUSTek

參、結論與建議

本文提供一個可行的方案，藉由取得單位內部網路對外路由器上的 IP 位址與 MAC 位址對照表，並儲存至資料庫中，然後比對相關資料，以獲得單位異常

IP 資訊。再配合交換器上所儲存的資料，可以找到異常 IP 所在的交換器，提供單位資訊官自動觀察網路並提供異常 IP 與 MAC 位址訊息的便利方式；系統將可協助各單位資訊官對營區內連網資訊設備實施長時間監控，並掌握單位 IP 及網路卡卡號的狀況，從中分析出異常活動的電腦，俾利早期處置，提昇單位實體資訊安全。

系統亦提供單位內部區域網路環境一個 IP 與 MAC 位址一個完整的記錄，記錄時間愈長，愈能提供資訊管理者更多參考資訊，在判斷網路問題時，提供更有利的資訊。另系統也提供了一般網路環境所需的基本網路管理的功能，如子網路及 IP 掃瞄管理等功能，可提供對一般網路環境實施偵測與記錄。

未來系統可進一步規劃擴充功能，例如：

一、提供可移植的平台：將來系統將規劃安裝於微軟的 Virtual PC 2007（Virtual PC 2007 係微軟提供，可免費下載，亦可使用 VMWare）這個虛擬作業系統平台，並提供本軍各單位使用，只要其映像檔複製到單位某一電腦內，並安裝 Virtual PC 2007，啟動映像檔直接執行，按程序調整設定即可執行，沒有重新安裝的問題。

二、提供整合查詢功能：規劃建置上層主機，可將整合各單位的所定期偵測的資料合併上傳至上層主機資料庫，可提供司令部針對有問題的 IP 進行查詢，可解決當發現問題 IP 時，能很快查詢所屬單位及 IP 存活的歷史記錄，將可加速 CERT 問題處理流程。

三、提供主動管制功能：本系統並可規劃配合智慧型網路管理交換器，利用程式控制交換器，當發現有問題的 IP 時，配合資料庫的記錄，對該 IP 所連接的交換器連線埠施予「斷網」（關閉連線埠）的處置。

四、結合資訊資產系統：本系統主要功能為發現單位內部實際 IP 執行的概況，雖然各單位可能自建資訊資產管理系統，並運用相關系統及設備管制內部 IP 及 MAC 位址，但無法確保網路上是否有非法活動的電腦存活，本系統所偵測資料將可提供一項自動化的驗證機能，可結合單位資訊資產管理系統上的主機資料，比對實際所偵測的資料，提供異常的 IP 資料。

資訊安全的管制工作廣受各單位所重視，但是其執行過程則有賴管理人員細心的注意每一個環節，本文即希望提供在繁雜的 IP 管理工作中，能有一自動化的工具軟體，協助網路管理人員更清楚單位網路的活動狀況，以提昇單位資訊安全管制工作的效能。