跨層之網路管理系統：以輔仁大學為實例

謝昇晃　劉惠英
輔仁大學電子工程學系
anderson@mail.fju.edu.tw
hiliu@mail.fju.edu.tw

摘要

網路管理一直是網路研究一項重要的課題，本文設計實作了一個具跨層管理功能的網管系統，該系統將網路管理者的管理方法與模式，轉換成自動化的管理方式，如此有助於增加網路營運管理的穩定性。一般的管理者自行研發網管系統往往藉由第二層的交換器進行異常的處理，鮮少結合第二層與第三層協同處理，本文中對異常處理，提供跨層管理的功能，如此對於網路環境異質度高的系統，提供了更有效率並更具彈性的作法。經實際上線啟用，證實此系統能更快速處理使用者 IP 位址使用問題、校內蠕蟲發作及校內外異常連線等問題，並有效節省管理者對其他異常處理判斷的時間。

關鍵詞：網路營運、網路管理。

1　前言

網際網路的快速發展，產生許多的問題，例如：盜用 IP 位址(Internet Protocol Address)、流量異常、IP 欺騙（IP Spoofing)、蠕蟲發作或內外部網路的攻擊以及網路設備設定被異常更動…等等，這些問題不但會影響網路的正常運作，嚴重的甚至可癱瘓整個網路，因此網路管理一直是網路系統研究中一項相當重要的議題，許多網路系統廠商紛紛推出許多網路管理系統，然而一般的網管系統無法完全合乎不同實際網路環境的需求，往往需要搭配固定硬體設備或是更動網路架構，最令人困擾的莫過於改變使用者習慣。有鑑於此，在不改變現狀的大原則下，以輔仁大學網路環境為藍本，實做一跨層管理功能之網路管理系統。以下先簡介輔大校園網路的架構。

輔大的校園網路架構如圖 1 所示，校園網路內部劃分為三層：核心層、分散層與存取層。其中核心層主要管校外路由，亦即整個校園網路的出口，分散層主要是使用者端的閘道與路由，由核心端連接至各主要大樓，存取層則是直接與各個使用者連接，主要的設備為乙太網路的交換器和集線器。

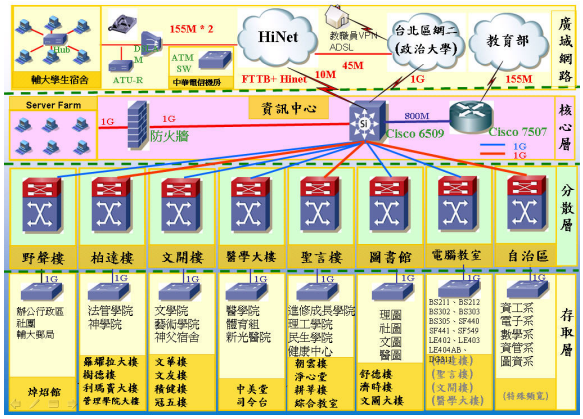

圖 1 輔大校園網路架構圖

依據輔大校園網路之暨有規劃，有下列幾項設計網管系統應注意的問題：首先全校所使用的 IP 位址全部為實體 IP 位址，其中大部分使用固定 IP 位址，其餘的使用動態取得 IP 位址。因為有使用動態取得 IP 位址的原因，因此 IP 位址與網路卡實體位址（以下簡稱 MAC 位址）無法固定一對一的對應。另外存取層中網路設備在廠牌、功能與設定有很大的差異。除了已經新汰換新的設備，可以使用簡單網路管理通訊協定（Simple Network Management Protocol，以下簡稱 SNMP）做控制，其餘的設備無法做到控制。

依照不改變現狀的原則下，開發結合分散層與存取層協同運作的跨層之網管系統，所以將該系統命名為--無痛跨層網路管理系統（painless cross-layer network management system，簡稱 PCNMS)，在 PCNMS 中，主要針對 IP 位址使用、流量過大、分散層設備負載異常、IP 欺騙、分散層設備設定被更動以及新增設備或使用者問題，提出具體作法，並且說明在第二層網路設備異質度高時，處理異常的彈性作法，供網路管理者做一個參考。

本文後續編排方式如下：第二節對網路管理相關問題做討論。第三節說明 PCNMS 架構。第四節提出實做 PCNMS 並檢視系統上線後的效果。第五節則是結論。

2　網路管理系統相關介紹

2.1 文獻探討

關於網路管理的議題，先前有許多研究的成果簡單介紹如下，首先是流量管控部分，「流量管理及病毒攻擊防禦整合系統之建置」[7]，使用固定位址解析協定(Static Address Resolution Protocol)，來將 IP 位址與 MAC 位址做對應，這樣可以避免使用者更改 IP 位址的問題，但是校園內基於教學的原因，常常造成 MAC 位址的移動，所以在此方法相對不適用；在文中有提到對於超過流量的 IP 位址切斷其對外傳輸，仍使其可以使用校內服務的作法立意甚好，惟必須搭配額外特定之負載平衡器來處理，在實做上也有其困難；但其對於校內 MAC 位址資料的收集的方法，即被本系統所採用。

此外，避免蠕蟲的爆發也是校園網路管理一項重要的課題，從 2001 年就有先進開始用 netflow 來做蠕蟲的偵測，如「利用 netflow 建置 Code Red Worm 偵測系統」[4]，一直到 2006 年的「利用 netflow 及時偵測蠕蟲攻擊」[3]，可以確定從 netflow 吐出的資料中可以得到許多資料流的資訊，但這個方法除了對超過門檻值做判斷，為了避免誤判現今盛行的點對點（peer-to-peer，簡稱 P2P）軟體，還加入了 TCP 旗標欄位來判斷純屬異常的流量；但本校不論發生疑似蠕蟲攻擊，或是使用 P2P 軟體都是要進行處理的，所以利用本校網路設備管理人員以往在分散層設備中執行 show ip cache flow 的指令可以獲取到類似 netflow 吐出的資料格式，來判斷是哪些 IP 位址有問題造成網路異常，即進行鎖定該 IP 位址所使用的 MAC 位址，處理後網路即恢復正常運作，所以目前採用了本校之前處理的指令，將其自動化來進行，可以減少網管人員對 PCNMS 採用新作法的疑慮。

此外，先前的研究對於異常處理時，大都採用 SNMP 的控制將該使用者的連接埠關閉，這樣的作法僅適用於當該埠僅有一個使用者時，本校在辦公室續接小型集線器是相當平常的事情，這種例外情形，則無法用上述的方法處理之，不過在 PCNMS 中這些都是納入考慮的。

基於上述的原因，放棄了將暨有的網路管理系統架構與方法移植至輔大的想法，而是參考並學習先進們的相關方法減少不必要的錯誤與嘗試，重新建立本校網路管理系統應有的功能與作法在調整修改後，以符合本校的網路架構及使用環境進行實做。

2.2 網管問題分析

網路管理有許多常見的問題，整理說明如下：

1. IP 位址使用問題：因輔大早期 IP 位址發放制度未統一加上人員異動的頻繁，造成 IP 位址資料上的不準確，進而導致包含 IP 位址相衝、未發放 IP 位址遭盜用等問題。
2. 流量過大問題：避免網路使用不公平，造成其他網路使用者的速度的變慢，適當的管理個人的網路流量是必要的。並且在處理經驗中，流量過大往往伴隨著病毒或蠕蟲爆發與使用者不當侵權之行為一併發生。
3. 網路設備負載異常問題：根據 PCNMS 的收集數據顯示，一般設備的中央處理器(Central Processing Unit，以下簡稱 CPU)的平均使用率很低，一旦中央處理器的平均使用率突然升高時，通常是網路上有異常的情況，大部分是蠕蟲爆發或改變網路架構造成迴圈（loop）所導致。
4. IP 欺騙問題：在網路設備中會看到一個 MAC 位址使用多個 IP 位址的情形，被使用到的 IP 位址或是此 MAC 位址與鄰道 IP 位址相衝時，將導致受害網段網路無法使用。
5. 設備設定異常更動問題：由於設備設定對整體網路的效能有相當的影響，然而大型單位中網管人員通常很多，因此設定檔被更動時應通知確認，以防被駭客更動而不自知。
6. 新增設備或使用者問題：在管理的經驗中，在穩定的網路中，除了病毒或蠕蟲的爆發造成的問題，網路的狀態通常會處於持續可使用的狀態，但往往在突然加入新的設備後才產生使用上的問題，所以我們希望能在新的設備或使用者加入網路後，能迅速的掌握狀況釐清問題發生的原因。

上述六點是許多中大型網路常見的問題，輔大的網路管理上也常發生，因此 PCNMS 將解決上述問題為主要課題。

3 PCNMS 的架構與方法

PCNMS 管理系統包含三個元件分別是資料庫主機、網路管理主機和維運管理主機，如圖 2，除資料庫獨立主機外，又依功能區分成六個模組：

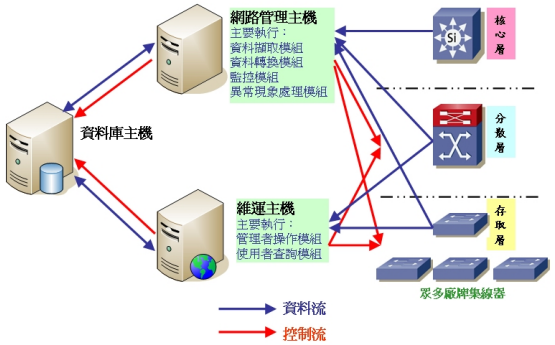

圖 2 系統架構圖

其中網路管理主機包含資料擷取、資料轉換、監控與異常處理等四個檢控管理的模組，維運管理主機

則負責管理者操作與使用者查詢等與維運相關的工作。六個模組主要對於本校網路三層設備進行資料收集、異常監控與管理，各模組之間控制流與資料流傳遞關係如圖 3 所示，目前因可控制之存取層網路設備數量有限，故以分散層為主要運作中心，未來數量增加後運作比重將會改變。以下分別介紹六個模組的功能。

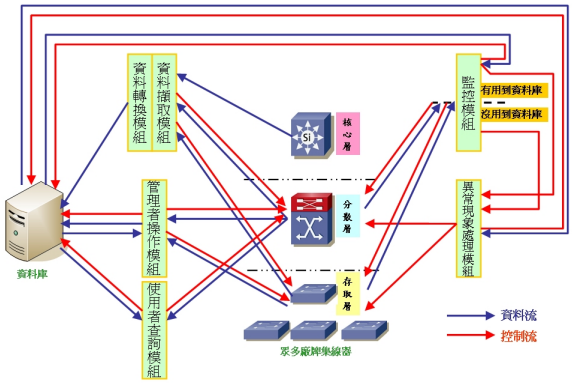

圖 3 控制流與資料流傳遞關係圖

3.1 資料擷取模組

主要是對所有網路設備進行資料蒐集，然而不同層級的設備，功能不同，因此所蒐集的資料與方法不同。分別說明如下：

核心層設備：核心層設備主要採用 netflow，進行資料蒐集，而網管主機再透過 flow-tool 取得資料，其原始資料為檔案格式，可以做為流量計算及監控異常連線的分析。

分散層設備：對分散層設備所蒐集的資料有，CPU 使用率與 IP/MAC 位址之對應，這兩者是用網管主機對所有分散層設備以終端機連線(telnet)形式蒐集。CPU 使用率收集，目前除了可做為判斷異常的依據外，還可以看出各使用區域的使用情況，供管理者衡量是否要進行區域整合、分割或是設備更換，另外，PCNMS 還可依照此數據，評估其餘模組執行的頻率。IP/MAC 位址對應的收集，則是藉著長期的收集，將目前已存在及已使用的 IP/MAC 位址情況記錄下來。

存取層設備：對存取層設備則是透過 SNMP 協定蒐集，蒐集 MAC 位址/連接埠之對應。

除 netflow 所蒐集的資料外，其餘所有蒐集的資料進入資料庫中。

3.2 資料轉換模組

資料轉換模組主要將擷取模組收集到的原始資料經過篩選與整理後，轉換成後續模組可直接使用的資料，經這模組轉換的資料包括：

netflow 原始資料。每日將 netflow 原始資料，依照 IP 位址將每日校內外互傳流量佳總整理並匯入資料庫中，此外，為了加速流量資料查詢的速度，預先將每日的流量較常查詢的資料預先處理。這部分除了加速了查詢流量的時間，也縮短對違反流量規則所需的判斷時間，但犧牲了少部分資料儲存的空間。

IP 位址/MAC 位址對應資料。可將半年期間每日收集的資料，轉換成一個 IP 位址與多個 MAC 位址對應的處理（以下稱 IM 表）與一個 MAC 位址對應多個 IP 位址的處理（以下稱 MI 表）的兩張對應表，以目前使用者的資料做為合法使用的依據，對動態取得 IP 部分則加入旗標做為辨識，這是監控模組所需使用的資料來源。

最後，更新每日收集到存取層的 MAC 位址/連接埠使用的資料，以便做為 3.4 異常現象處理時，判斷該埠是否為單獨的 MAC 位址所使用的依據。

PCNMS 的資料轉換模組會定期進行資料的轉換作為後續處理的依據，其模組可適當改變或增加，以便針對不同現象來做追蹤與分析。

3.3 監控模組

監控模組又分成線上獨立監控、線上搭配資料庫監控與 netflow 資料監控三部分，主要是針對分散層與存取層的設備做監控，對於監控到異常現象的處理步驟，第一步驟就是使用電子郵件方式來通知管理者。第二步驟，依原因將記錄存入資料庫中，並且呼叫 3.4 所介紹的異常現象處理模組來處理。下面就對這三個部分做說明。

3.3.1 獨立監控

以上經由資料擷取與資料轉換模組所收集的資料追蹤分析，如追蹤 CPU 使用率可得知正常運作與異常現象的均值，因此資料庫系統可建立異常現象的系統流量、CPU 使用率等資料，以便後續的監控與判斷。

獨立監控指不需妹和其他資料，可獨立做判斷與監控，此部分有下列幾項監控重點：

CPU 使用率：監控分散層所有設備的使用率，一旦有異常的現象(如超過系統設定的門檻值)，則進一步分辨出問題的網段，以便做後續處理。

IP 連結：監控模組會定期或有某些異常現象(如經上述的 CPU 使用率觀察而得)啟動，來觀察個別 IP 的連結，當有某個 IP 對其他連續 IP 的連線，當有某個 IP 對其他連續 IP 做連結，此現象通常是有異常，將此來源 IP 交由異常現象處理模組做後續處理。

IP/MAC 對應：監控所有網段的 IP/MAC 對應，當有單一 MAC 短時間對應到多個 IP 時，則為 IP 欺騙的現象，同樣將此 MAC 交由異常現象處理模組來做處理。

此模組可以根據分散層設備本身以及網路管理主機的負擔，衡量要集中控管或是進行分散式處理，甚至常出問題的區域，配合擷取模組所得到 CPU 使用率，評估增加執行頻率加強監控，這些都是可以彈性考量的。

3.3.2 搭配資料庫監控

由上述獨立監控所得的資料，可搭配原有資料庫中 IM 表作比較，如當有 IP 位址沒有對應的 MAC 時，這種狀況絕大部分是發生 IP 位址被盜用，所以 PCNMS 認定其為異常，並進行相關的處理。

此外亦可與資料庫中 MI 表比較，當發現了沒有出現過的 MAC 位址時，此時 PCNMS 認定網路上增加了新的設備，並進行後續的處理。

最後將分散層設備的各個設定檔與資料庫比對有異動時，立即通知所有管理者確認是何人修改過，以確認資料庫是否要更新或是遭到他人異動。

由於這部分在監控比對為定期處理，由於有用到資料庫的資料，所以在執行頻率上必須考量到資料庫的負擔。

3.3.3 netflow 資料監控

這一部份的監控，主要對 IP 流量異常與連線異常進行監控，其中 IP 流量異常是監控個別 IP 的使用量，此可根據轉換模組產生的流量資料進行結算，找出使用流量違反規定者之 IP 位址，將其紀錄於資料庫中，並啟動異常處理模組進行後續的處理。

對於連線異常的部份，PCNMS 可由管理者設定分析時間長度、受監控之未使用 IP 位址與異常連線的門檻值。此處監控未使用的 IP 指系統保留部分 IP 專門做為陷阱，以監控是否有不當的連線，當一個 IP 對受監控之未使用 IP 的連線數量(對同一個 IP 只算一次）超過門檻值時，就認定此 IP 位址有異常連結的行為，在此針對異常的校內 IP 才啟動異常處理模組進行後續處理。因為校外 IP 的異常連結，經過網際網路層層傳送的原因，對於校內設備負擔的影響不大，反觀校內 IP 發生異常連結現象，往往造成設備負擔大增，所以僅對校內 IP 做後續異常處理。PCNMS 在實做過程中觀察到幾個現象，第一：受監控之未使用 IP 位址最好是連續的，如果無法連續，分析的時間需要拉長。第二：受監控之未使用 IP 位址建議在同一 C 級網段，跨多個 C 級網段的未使用 IP 位址，在原本分析的時間內看不出此異常現象。第三：若欲使用之前有使用過的 IP 位址，尤其是伺服器使用過的 IP 作為受監控之未使用 IP 位址，最好停用一段時間，不然此 IP 位址的連線次數將較未使用過的 IP 位址頻繁，對於異常的判定效果將會降低。

3.4 異常現象處理模組

在異常現象的處理上，是透過 3.3 監控模組或是 3.5 管理者操作模組的呼叫來執行，主要做的就是將判定有異常行為的 IP 位址或 MAC 位址，自資料庫中取出，限制或是停止其繼續使用網路資源，在處理的流程上，會依照由下列優先順序處理之：

1. 對於異常行為的 MAC，若其所使用的埠為單一對應時，則直接關閉該埠。此關閉的控制可透過 SNMP 協定完成之。
2. 對異常行為的 MAC，若其所使用的埠為非單一對應，即該埠有許多 MAC 使用，則僅於該埠單獨鎖住此異常行為的 MAC。此鎖定的動作透過 SNMP 協定設定存取列表來完成。
3. 對於異常行為的 MAC 位址，無法在存取層進行上述兩項處理時，則在分散層中鎖住其 MAC 位址，此封鎖透過 telnet 方式，執行封鎖 MAC 位址指令。
4. 當發生異常行為的 IP 位址，無法取的其對應的 MAC 位址時，則在分散層設備限制其 IP 位址之使用，此限制透過 telnet 方式，執行增加限制 IP 位址存取列表的指令。

異常處理的流程如圖 4，在此可以確定當異常發生時，在分散層封鎖 MAC 位址或 IP 位址動作的其中一個，一定可以執行，因為這是呼叫這模組所必須要的資料。

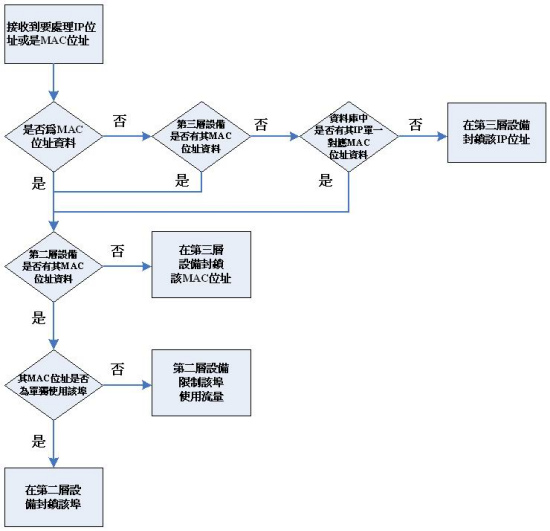

圖 4 異常處理流程圖

最後，將處理的結果，詳實的記錄於資料庫中，讓未來在處理解鎖動作時，能依據資料在正確的位置解除鎖定。

3.5 管理者操作模組

管理者操作模組共分三個小模組，包括：

資料查詢模組：主要用來協助管理者判斷，所以都是設備上及資料庫內資料的查詢，以存取層搜尋 MAC 位址出現的位置為例，如圖 5 所示：

網管指令執行模組：讓管理者透過操作介面，輸入或選擇相關資料並決定要執行的動作。當網路上層管理單位要處理的異常 IP 位址、或是將未使用 IP 位址限制存取列表重新修正等。都是透過此模組執行。

資料輸入及修正模組。讓管理者可以手動新增刪除修改資料庫內的資料，以達到資料的準確性。

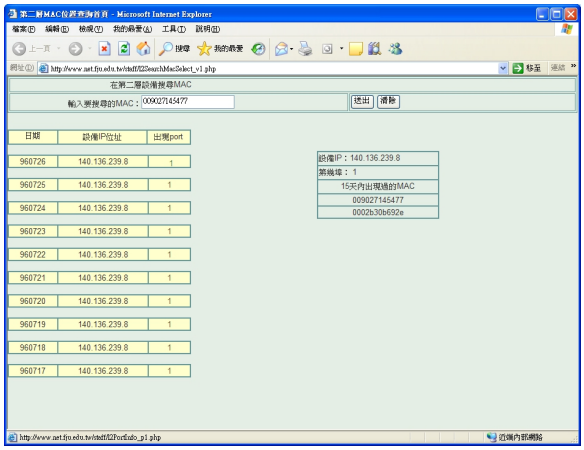

圖 5 搜尋該 MAC 位址出現的位置

3.6 使用者查詢模組

目前僅可以查詢有關流量資料及 IP 位址或 MAC 位址被封鎖的訊息。

4 成效分析

PCNMS 的實做開發，在背景執行時主要以 Practical Extraction and Report Language（以下簡稱：Perl）程式語言為主，對於管理者操作或使用者查詢則提供網頁介面，使用 PHP: Hypertext Preprocessor（以下簡稱 PHP）撰寫透過瀏覽器來操作，資料庫的部分則使用 MySQL。

在實際上線後，對於遭遇網路問題時，PCNMS 處理的情況，做一個目標與效能的評估，以下就是根據 2.1 所述目前遭遇到的問題一項一項來檢視系統是否能解決或改善，達到原本設定的目標。

4.1 IP 位址使用問題

在上線的三個月內，雖未發生 IP 位址相衝的問題，需要管理者使用 PCNMS 收集資料來處理，但卻發生過數次使用者在重灌電腦後忘記自己原本 IP 位址的問題，而原本發放 IP 位址中並未登錄此使用者資料，經查資料庫內的資料，成功幫助使用者找回原本 IP。由於未使用 IP 位址已被存取列表限制，盜用的 IP 位址僅能針對已經發放的 IP 位址方可使用，而 PCNMS 又已經定期將 MAC 位址與 IP 位址做紀錄，相信只要發生 IP 位址相衝，一定能確認盜用者的 MAC 位址，再透過管理者操作模組交由異常現象處理模組來處理。

4.2 流量過大問題

PCNMS 可以成功的依照本校流量制訂之規定，自動的封鎖流量過大的使用者，並在封鎖日期結束後，再將其自動的開啟。

4.3 第三層設備負載異常問題

在校內使用者爆發異常連線時，造成分散層設備 CPU 使用率異常升高，PCNMS 成功降低 CPU 使用率，有效維持網路營運。

4.4 IP 欺騙問題

在上線這段期間，IP 欺騙這個問題剛好有發生，PCNMS 未能於爆發時立即發現，而是在定時的監控後才發現，而該區域目前存取層並非 PCNMS 所能控制，故在問題發現後將其 MAC 位址封鎖於分散層，然而在封鎖後該區域仍有多位使用者無法正常使用網路，經管理者介入後，發現必須在存取層設備上拔掉其連上的線路，並清除分散層上的地址解析協議表（Address Resolution Protocol table，以下簡稱 ARP table）後，其他正常的使用者才能恢復使用，目前研判應是分散層的 ARP table，已將其 IP 位址對應到錯誤的 MAC 位址，所以正常使用者仍無法使用，所以 PCNMS 的功能是能夠發現 IP 欺騙的行為與其對應的 MAC 位址，但 PCNMS 卻無法完成後續的動作，這樣的效果實在還是不夠減輕管理者的負擔，所以正嘗試加入後續的動作來處理。

4.5 第三層設備設定更動問題

目前僅被動式的告知所有管理者，設定已經被更動，然後要求更改設定的管理者確認，這個功能是能正常運作。

4.6 新增設備或使用者問題

PCNMS 功能正常運作卻沒達到任何的效果，原

因是因為沒有辦法要求使用者，一台電腦就一定要申請一個 IP 位址，所以只要 IP 位址不衝突，就算有新的 MAC 位址進入本校的網路，系統會通知管理者，除非加入的時間點恰巧有網路問題發生，這時此項功能才會被凸顯。

4.7 其他成效與發現

PCNMS 在上線後，除上述問題大都能有效處理外，在系統的處理過程中，也有三項額外的發現：

發現校外異常連結：原本透過 netflow 的分析欲發現校內異常連結，分析後卻發現有許多校外的 IP 位址，異常的對本校 IP 位址做連結的動作。故在分散層中動態增加限制存取列表之後再定期清空[7]。

發現使用者 IP 位址的誤用：因為同一個 MAC 位址使用了多個 IP 位址，而這些 IP 位址分別對應不同的域名（Domain Name），可以揣測使用者應該用虛擬主機（Virtual Server）的方式處理，而非使用此一對應方式。將一一釐清後更正使用者錯誤的使用方式，回收更多可使用之 IP 位址。

發現 MAC 位址集體移動：由於校內辦公空間的遷移，造成同一個 MAC 位址，在不同時期使用了不同 C 級網段的 IP 位址。原本不知情的網管單位，在 PCNMS 啟用後發現，進而回收不再使用的 IP 位址。

這些的發現，將更有助於網路管理者判斷校外 IP 位址潛在威脅與更有效率的管控 IP 位址。

在其他成效方面，以往提供給使用者的資訊，更新速度十分緩慢，常常造成使用者的誤解，在 PCNMS 上線後，管理者可以傳遞比以往更即時的訊息給使用者，以網卡被鎖定的即時資訊如圖 6 所示。

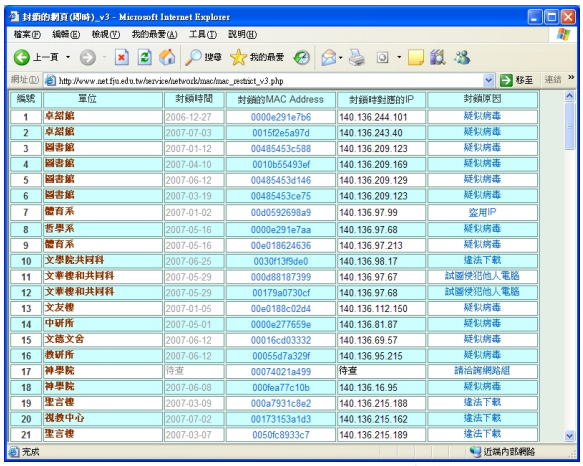

圖 6 MAC 位址被封鎖的即時資訊

另外，在遇到災害發生時，管理者可以利用在資料庫中設備的設定資料，在短時間之內進行災害重建的工作，這些成效都是當初沒有預期到的。

5 結論

不論是 IP 位址的管理、流量的異常及其他影響網路穩定的種種現象，網路管理者往往透過單一層設備，甚至不同種類的單一設備來解決其所遇到之問題，但在網路技術的突飛猛進的今日，傳輸介面與速度更替的頻繁，將造成原本管理設備無法使用，導致管理出現斷層，PCNMS 將這些管理問題分散在原本就使用的第二層與第三層設備來協同運作，此一問題即可避免，還可將負擔分散到個個設備，即使校園骨幹傳輸介面升級或校園出口頻寬提升，也不置於影響到此一管理架構，符合不改變現狀的原則外，並達成網路管理系統持續營運的目標。PCNMS 使用內建指令來操作第三層設備，在第二層設備則透過 SNMP 協定來控制，實際上線證實此系統運作正常且達到幫助網路管理者縮短問題處理的時間。

最後，由上線的結果得知，PCNMS 尚有功能有待加強，未來將不斷的研究與改進，秉持著不改變現狀的原則，讓此系統可以更完善，讓管理者更佳順利的維持網路營運。

參考文獻

[1] 任善隆、許俊萍、孫際宇、張勝欽、林世哲、吳承益。宿舍網路維運與 IP 流量限制方案。TANET2005。

[2] 李宇峰、劉柏汎、楊慶隆、紀新洲。自動化 IP 管理系統。TANET2005。

[3] 徐偉智、王明輝。利用 netflow 及時偵測蠕蟲攻擊。TANET2006。

[4] 黃文穗、林守仁。利用 netflow 建置 Code Red Worm 偵測系統。TANET2001。

[5] 蔣安平、史明輝、嚴天峻、潘東名、黃顯樺、王元凱、邱瑞科、林宏彥。全程即時自動化宿舍網路申請暨管理系統。TANET2001。

[6] 劉柏汎。FreeBSD 異質系統及網路管理整合應用(出版日 2005.09.16)。松崗電腦圖書資料股份有限公司。

[7] 嚴嘉錚、楊靖宇。流量管理及病毒攻擊防禦整合系統之建置。TANET2003。

[8] http://www.mibdepot.com/。

[9] http://www.ethereal.com/。