多層次校園網路監控系統之設計與實作

郭柏彰 鄭源宇 黃聖傑
蘇暉凱 博士
南華大學資訊工程學系

摘要

在現今高速寬頻網路環境，駭客入侵與病毒攻擊往往造成資料被竊取或被破壞等嚴重網安事件，因此網路監控是網路管理中一項非常重要的工作，如何在高速分封交換的環境中，提供精確且高效益的網路監控服務是一項具挑戰性的技術。本論文以校園網路環境爲基礎，提出多層次校園網路監控系統，由底層往上分爲：1. 網路設備監控、2. 網路資料流監控、3. 網路應用程式資料監控等功能。網路設備監控，監控與記錄網路設備與連線狀態；網路資料流監控，監控每台電腦的連線狀態；網路應用程式資料監控，本論文以 MSN 應用程式爲例，監控每一個 MSN 使用者的連線與通訊狀態。本系統監控結果提供網管人員重要參考數據，可以協助進行網路維護、網路資源規劃、網路安全管理等重要工作。12

關鍵詞：網路監控, 網路資料流監控, 網路應用程式監控

Abstract

In high-speed and broadband networks, attacks of hackers and viruses often cause serious network security evens. Thus, network monitoring is one important task in network management. It's a challenge to provide exact and efficient network monitoring services in high-speed transport networks. Based on the campus network, we propose a multi-level campus network monitoring system. From the low layer, the functions can be divided into three levels, such that network device monitoring, network-flow monitoring and network-application monitoring. The network device monitoring provides the operation information about network devices and links. The network-flow monitoring traces TCP/UDP connections of each host. The network-application monitoring provides a MSN application monitoring, which traces the status and communication of each MSN user. The monitoring results can help network managers to perform network main maintenance, network resource planning and network security management.

Keywords: network monitoring, network-flow monitoring, network application monitoring

1. 前言

隨著網路技術快速進步，傳輸頻寬不斷地往上提昇，加快了病毒攻擊的速度，以及造成網路資源不當使用的問題日愈嚴重，因此網路監控與網路管理工作也越來越受到重視。精確且完整的網路監控數據，可以協助網管人員了解網路資源使用狀況以及使用者網路使用行爲，以進行網路資源規劃與資訊安全處理。

以學校校園網路與宿舍網路爲例，一般常見造成網路品質不穩定或癱瘓的兩大原因：1. P2P (Peer-to-peer) 軟體不當使用，2. 病毒與木馬軟體攻擊。因此，完善的網路監控系統可以協助網管人員準確地即時了解網路狀況，以處理不當使用事件或網路資源重新規劃，將網路服務中斷的可能性降到最低。除此之外，網路監控也可以防範駭客入侵，降低資料被竊取風險。

由於網路封包交換量相當大，尤其在高速頻寬的骨幹上，如何在不影響正常網路傳輸服務的情況下，收集完整且準確的封包資訊，以提供網路管理的參考價值，是網路監控技術欲達到的目標。

目前市面上具網路管理能力的交換器 (Switch Hub)、路由器 (Router) 都內建 SNMP (Simple Network Management Protocol) 功能，因此只需要使用 SNMP 網路管理應用程式，就可以了解網路設備運作狀態，如：CPU 使用量、記憶體使用量、封包收送狀況與連線狀態。SNMP 網路管理應用程式所提供的資訊集中在網路實體層部份，因此網管人員只能了解硬體使用狀況以及匯集使用者網路使用行爲的資料。

但對於網路管理來說，僅僅了解網路設備運作狀況是不夠的，若欲進一步了解每個使用者的網路使用行爲，網路設備必須監控網路層與傳輸層 (Network Flow) 資訊，管理與記錄每一條連線的狀態，如 CISCO Router 所提供的 NetFlow 功能。然而，如果欲了解使用者網路應用傳輸的內容，就必須分析應用層協定資訊。在實作上，監控越上層的資訊，網路監控設備的負載越重，且付出成本越高。因此，如何在成本與監控效能上取得一個平衡點，以

[1]本研究由國科會贊助，計畫編號 NSC 95-2218-E-343-002。

[2]感謝南華大學資訊室協助提供實驗環境。

滿足網路監控需求，是一項具備挑戰的技術。

本論文以校園網路爲實驗環境，利用網路設備內建的 SNMP 與 NetFlow 功能，配合自行發展的 Passive Application Sniffer Agent，以監控 MSN Application 資料，提出多層次校園網路監控系統。本系統以階層式架構爲基礎，具備高度彈性與擴充性，系統元件可以監控需求與效能考量增加與調整。本系統依監控內容由底層往上可分爲：網路設備監控、網路資料流監控、網路應用程式資料監控等功能。在監控資料處理流程上可分爲：校園網路環境、資料收集與分析、資料儲存與管理、資料呈現(網管程式介面)。希望本研究成果，可以提供網管人員重要參考數據，協助進行網路維護、網路資源管理、網路安全管理等重要工作。

2. 相關技術

2.1 簡單網路管理協定 (SNMP)

SNMP (Simple Network Management Protocol) 被稱爲簡單網路管理協定，SNMP 由 IETF 所提出，用來管理位於 IP 網路上的各個節點[6]-[8]。一般具備網路管理能力的網路設備會提供 SNMP Agent 與 MIB 功能，網路設備在運作當中會不斷地收集與統計網管資訊，並更新到 MIB。SNMP 網路管理應用程式 (SNMP Manager) 可以在遠端透過 SNMP 通訊協定與網路設備 SNMP Agent 通訊，抓取 (Get) 或設定 (Set) 網路設備之 MIB 參數。因此，SNMP 網路管理應用程式可以週期性收集網路上所有網路設備狀態，並彙整成專業報表或圖表，提供網路管理人員參考。

2.2 CISCO NetFlow

NetFlow 是一套網路流量統計協定[1]-[4]，主要的原理是封包傳輸時，連續相鄰的封包通常是往相同目的地 IP 位址傳送的特性，配合快取機制 (Cache)，當網路管理者開啓路由器介面的 NetFlow 功能時，路由器介面會在接收網路封包時，分析封包的標頭部分來取得流量資料，並將所接到的封包資料流資訊 (TCP/UDP Connection) 彙整成一筆一筆的 Flow。

支援 NetFlow 功能的網路設備將其所收集到的 Flow 資訊以 UDP 封包送往預設好的流量接收主機，配合 NetFlow 等相關軟體收集資料，如 CISCO 的 NetFlow，FlowCollector 或公開原始碼軟體 Flow-tools，將這些原始流量資料做適當的處理、儲存以提供後續的相關應用。

2.3 MSN Messenger 通訊協定

MSN (MicroSoft Network) Messenger 爲 MicroSoft 所開發的一套即時通訊系統，它是以 Windows Message 爲發展起點，接著在開發出大眾所知的 MSN 即時通訊，至今 MSN 已推出了多種通用版本，但是核心的控制協定是不變的。MSN 之通訊協定有許多種版本，最主要有分 Server 跟 Client 之版本。不過大家最常討論的 MSN Messenger Protocol 是針對爲 Server 所討論[9]-[10]。

MSN Messenger Protocol 是依據 RFC 2278 的概念實現，協定內定埠號爲 1863。首先，它會先辨別 Client 端之版本，再評估是否可以與 Server 端版本相容，經判斷後如果可以與 Server 版本相容，則會給予連結。連結成功後，MSN Messenger Protocol 會先連線至 NS (Notification Server)，此時 NS 再依據 Client 端來決定要將連線導向其地方之 SBS (Switchboard Server)，連結上 SBS 後，連線就算完成，也就是所謂之『上線』。因此，監控通訊埠 1863，並解析 MSN Messenger Protocol，我們可以得到每一個 MSN 使用者的狀態與訊息交換內容。

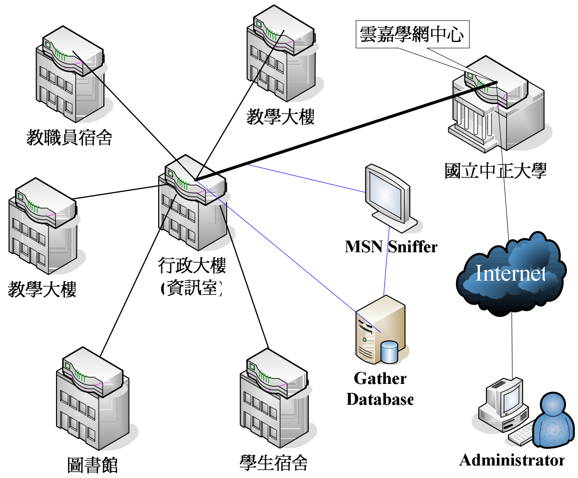

圖 1 校園網路與系統環境

3. 系統元件設計

3.1 系統架構

圖 1爲校園中網路連結概況圖，所有校園內的教學大樓、教職員學生宿舍等之建築物網路均連結至位於行政大樓裡的資訊室，統一由骨幹資訊室對外與位於中正大學雲嘉學術網路中心連結。本系統除了監控與記錄來自各大樓的路由與交換器的 SNMP 狀態資訊外，在骨幹網路上的路由器也開啓 NetFlow 網路資料流，也將骨幹的光纖網路使用分光技術，分析特定的網段記錄網路應用程式資料。

本系統架構如圖 2 所示，系統環境依橫向角度可以區分爲 Campus Networks (校園網路)、Data Collector and Analyzer (資料收集與分析)、Data Storage (資料儲存) 與 Network Management Application (網路管理應用程式) 四個部份。系統功能依縱向角度可以分爲 Network Application Monitoring (網路應用程

式資料監控）、Network Flow Monitoring (網路資料流監控)、Network Device Monitoring (網路設備監控) 等功能。

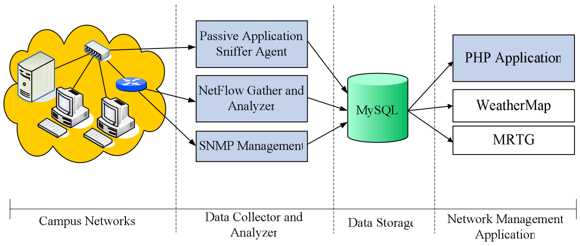

圖 2 多層次網路監控系統架構圖

1. Campus Networks: 為校園網路基礎建設設備，本系統將利用具網路管理能力之網路設備，在不影響校園網路正常運作的情況下，提供網路管理資料。
2. Data Collector and Analyzer: 依功能包含 Passive Application Sniffer Agent、NetFlow Gather and Analyzer 與 SNMP Management。本系統 Passive Application
3. Sniffer Agent 以監控 MSN Application 為第一階段目標，利用網路設備 Mirror Port 功能，收集與分析有興趣的網路區段之 MSN 封包資料。NetFlow Gather and Analyzer 與 SNMP Management 利用 NetFlow 與 SNMP 通訊協定收集網路 Network Flow 資訊與網路設備運作資訊，此兩元件以公開原始碼軟體 Flow-tools 與 SNMP 為基礎，並加強資料分析與資料庫連結功能。
4. Data Storage: 本系統以 Open Source MySQL 資料庫系統，儲存與管理網路監控數據資料。
5. Network Management Application: 整合 MRTG 與 WeatherMap 資料呈現功能，並利用 PHP 網頁發展技術5自行開發網路管理應用程式。

3.2 元件設計

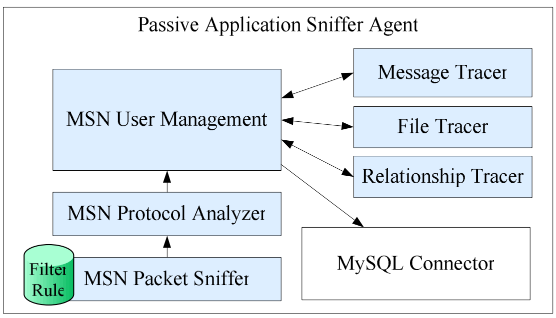

圖 3 被動應用程式監控代理器之功能方塊圖

被動應用程式監控代理器之功能方塊圖如圖 3所示，淡藍色方塊功能為本論文所設計，白色方塊功能為引用 Open Source 或其他開放函式庫。在本系統裡以 MSN 為例，監控 MSN 之相關封包，不相關之封包則不處理。MSN Packet Sniffer 依據 Filter Rule 擷取有關 MSN 之所有封包，接著 MSN Protocol Analyzer 則分析 MSN 之相關封包，最主要先分析使用者狀態 (MSN User Management)，根據使用者狀況，再從中分析好友狀態 (Relationship Tracer)、語音對話與文字聊天內容 (Message Tracer) 及檔案傳送 (File Tracer)。分析完畢後則儲存在資料庫 (MySQL)，管理者便可從資料庫裡讀取擷取到之 MSN 訊息。

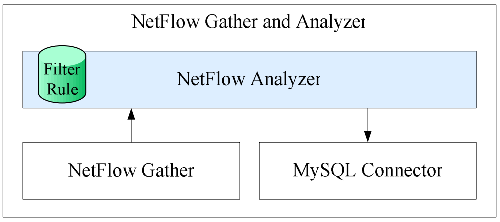

圖 4 NetFlow 收集與分析之功能方塊圖

圖 4 為 NetFlow 功能方塊設計圖。NetFlow 之資訊每個欄位所表達之封包意義各不同，所以當有支援 NetFlow 之 CISCO Router 送出 NetFlow 之封包訊息時，NetFlow Analyzer 會先依據 Filter Rule 來擷取 NetFlow 之封包，並且在依照欄位分別輸入在資料庫裡，管理者就可以從資料庫裡觀察 NetFlow 之訊息，間接知道網路是否有遭受 DDos (分散阻絕攻擊) 攻擊或不當的佔用頻寬。

圖 5 為 SNMP 之功能方塊設計圖。SNMP 之元件在本系統裡為最重要之元件。其中之 Link Status 與 Device Status 為觀察整個網路與設備之連線狀況，它依附 SNMP 之核心架構上，所以可直接由 SNMP Management 來觀看或設定 Link 與 Device 之狀態。Link Status 與 Device Status 所記錄到之數據都會藉由 SNMP Management 記錄在資料庫裡，使用者便可觀察其狀態而得知本系統之設備與網路頻寬之狀況。

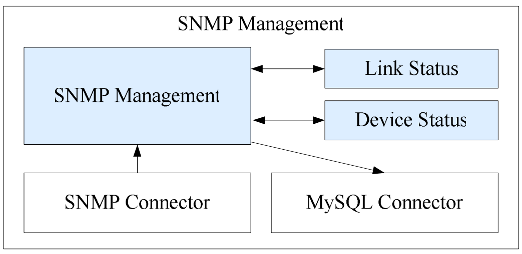

圖 5 SNMP 管理器之功能架構圖

3.3 MSN Packet Sniffer 設計原理

MSN Packet Sniffer 是本系統一大特色，補足 SNMP 與 NetFlow 無法觀察的網路行為。根據數據顯示，全球的通訊軟體，MSN 佔全球使用者 61%，換句話說，全球大部分使用者都使用 MSN。MSN 功能強大，可以做文字訊息傳遞，傳遞檔案與語音交談。

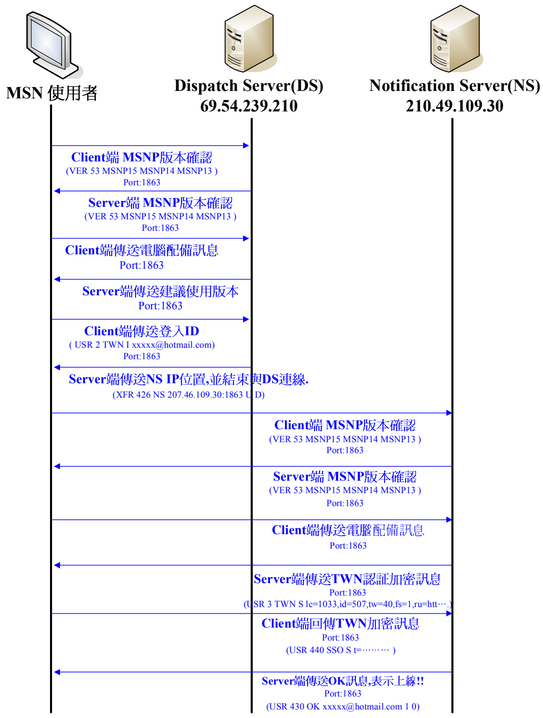

圖 6 MSN 上線流程

透過 MSN Packet Sniffer 監控，我們可以建立出使用者的量化網狀關係，例如：A 使用者與 B 使用者的好友關係是 0.7，但 A 使用者與 C 使用者的好有關係是 -0.9，因此當 A 使用者大量傳送封包給 C 使用者，我們可以判斷為不正常傳輸。除此之外，我們可以透過聊天訊息的監控，自動過濾 MSN 病毒散佈，不合法網址與檔案交換予以攔截。

圖 6 裡表示使用者上線時跟伺服器的封包傳遞訊息，但過濾時不必給個封包監控，因為有些封包則是 MSN 內部程式之指令，要注意的是最後一個封包，因為上線程序都許穀才會發此封包，因此截取此封包便可知道上線情形，MSN 之伺服器也會通知其他使用者為上線。

圖 7表示表示 MSN 傳送訊息的流程。標上紅框部分，即是傳送訊息的內容，本系統也將針對這個部分進行分析並將分析後的資料匯入資料庫儲存，以供網管人員封鎖或進行後續動作。

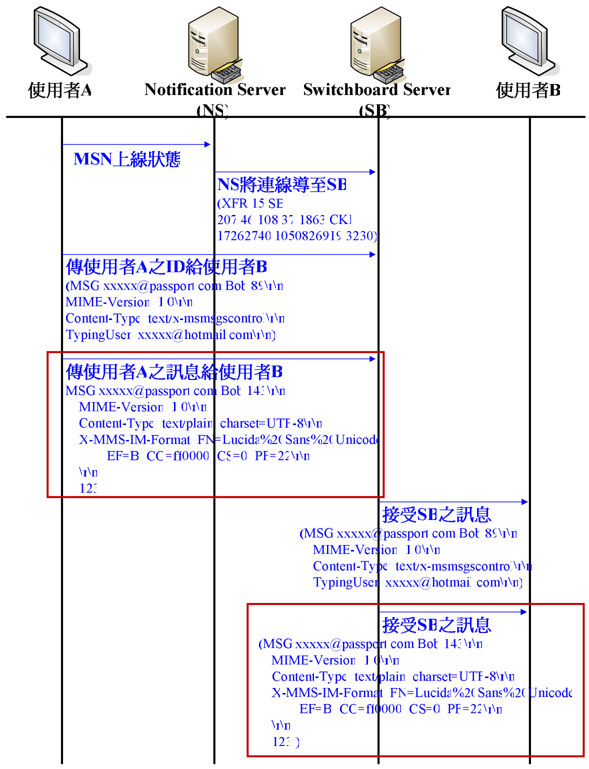

圖 7 MSN 訊息傳送

MSN 為本系統是第一個監控的應用服務，未來希望以此設計原理，將其他網路應用服務監控模組嵌入到本系統，本系統將可以提供更多網路監控資訊。

3.4 資料庫設計

本系統以關聯式資料庫儲存與管理分析後的監控資料，提供前端網路管理系統呈現與查詢監控數據。網路資料流與網路設備之 ER 圖。

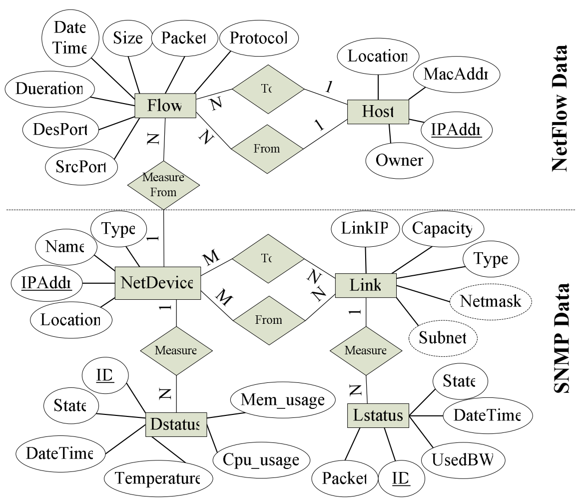

圖 8 網路資料流與網路設備 ER 設計圖

設計圖如圖 8所示，上半部為 NetFlow 監控數據，下半部為 SNMP 監控數據。設計內容說明

如下：

1. 實體：Flow (網路流量)。
   屬性：SrcPort、DesPort、Dueration、DateTime、Size、Packet、Protocol。
   關係：它與 Host 有兩種關係。To：同一時間可能有多個封包傳送到一台主機，因此關係是 N：1。From：同一時間可能有好幾個封包從一台主機傳送過來，因此關係是 N：1。它與 NetDevice 有 MeasureFrom (測量) 關係，好幾個 Flow 的訊息可以被一個 NetDevice 測量，因此關係是 N：1。
2. 實體：Host (主機)。
   屬性：Location、MacAddr、IPAddr、Owner。
   關係：它與 Flow 有兩種關係。To：同一時間一台主機可能有好幾個封包傳送出去，因此關係是 1：N。From：同一時間一台主機可能有好幾個封包傳送過來，因此關係是 1：N。
3. 實體：NetDevice (網路裝置)。
   屬性：Type、Name、IPAddr、Location。
   關係：它與 Flow 有 MeasureFrom (測量) 關係，一個 NetDevice 可以測量好幾個 Flow 的訊息，因此關係是 1：N。它與 Link 有兩種關係。To：同一時間可能有多個網路裝置連線到多個不同的 port 上，因此關係是 M：N。From：同一時間多個網路裝置可能被多個網路連線過來，因此關係是 M：N。它與 Dstatus 有 MeasureFrom(測量)關係，一個 NetDevice 可以被好幾個測量裝置測量，因此關係是 1：N。
4. 實體：Link (連線)。
   屬性：LinkIP、Capcity、Type。
   弱屬性：netmask、subnet。
   關係：它與 NetDevice 有兩種關係。To：多個連線可以連到多個網路裝置，因此關係是 N：M。From：多個 port 可被多個網路裝置連線，因此關係是 N：M。它與 Lstatus 有 MeasureFrom(測量)關係，一個 Link 可被多個 Lstatus 裝置測量，因此關係是 1：N。
5. 實體：Lstatus (連線狀態)。
   屬性：ID、State、DateTime、Temperature、Cpu_usage、Mem_usage。
   關係：它與 Link 有 MeasureFrom (測量) 關係，多個 Lstatus 可測量一個 Link，因此關係是 N：1。
6. 實體：Dstatus (裝置狀態)。
   屬性：State、DateTime、UsedBW、ID、Packet。
   關係：它與 NetDevice 有 MeasureFrom (測量) 關係，多個 Dstatus 可測量一個 NetDevice，因此關係是 N：1。

圖 9為 MSN 監控資料之 ER 設計圖，設計內容說明如下：

1. 實體：User (使用者)。
   屬性：AliasName、UserID、FriendNum、State。
   弱屬性：Class。
   關係：它與 Chat 有兩種關係。To：多個 User 可以發送多個 Chat，Chat 資料庫全程對應，因此關係是 M：N。From：一個使用者可接收多個訊息，Chat 資料庫全程對應，因此關係是 1：N。它與 Present-state 有 State(狀況)關係，一個 User 可擁有多個 Present-state，Present-state 資料庫全程對應，因此關係是 1：N。它與 Talk 有兩種關係；To：一個 User 可以發送多個 Talk，因此關係是 1：N。From：一個 User 可接收多個 Talk，因此關係是 1：N。它與 FileTran 有兩種關係；To：一個 User 可以發送多個 FileTran，因此關係是 1：N。From：一個 User 可接收多個 FileTran，因此關係是 1：N。
2. 實體：Chat (聊天訊息)。
   屬性：ID、UserID、Content、DateTime、State。
   關係：它與 User 有兩種關係。To：多個 Chat 可以發送給多個 User，Chat 資料庫全程對應，因此關係是 N：M。From：多個 Chat 可被一個 User 發送，Chat 資料庫全程對應，因此關係是 N：1。
3. 實體：Present-state (使用者狀態)。
   屬性：ID、UserID、DataTime、State。
   關係：它與 User 有 State(狀況)關係，多個 Present-state 可被一個 User 擁有，Present-state 資料庫全程對應，因此關係是 N：1。
4. 實體：Talk (語音交談)。
   屬性：State、ID、Wav、UserID、TalkTime。
   關係：它與 User 有兩種關係。To：多個 Talk 可以發送給一個 User，因此關係是 N：1。From：多個 Talk 可被一個 User 發送，因此關係是 N：1。
5. 實體：File Transship (資料傳送)。
   屬性：State、DateTime、DataClient、ID。
   關係：它與 User 有兩種關係。To：多個 FileTran 可以傳送給一個 User，因此

關係是 N：1。From：多個 FileTran 可被一個 User 傳送，因此關係是 N：1。

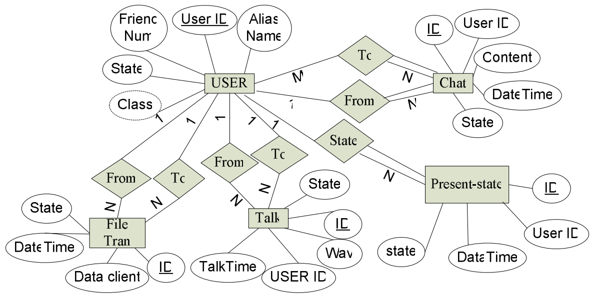

圖 9 MSN 監控資料 ER 設計圖

4. 系統雛型與成果展示

4.1 系統介面架構

如圖 10，本系統介面由 html 與 PHP 所設計、建構出來的網站介面，將提供一般使用者以及網管人員所需的相關資訊，在網站選項裡依序由左而右分為訪客瀏覽 (Guest)、網管人員瀏覽 (Login)。

尚未登入的使用者可查詢由 SNMP 提供的設備與網路連線的狀態資訊，網管人員登入後可進一步提供每筆傳送網路資料流更詳細的訊息，也可進行網路應用層的監控。

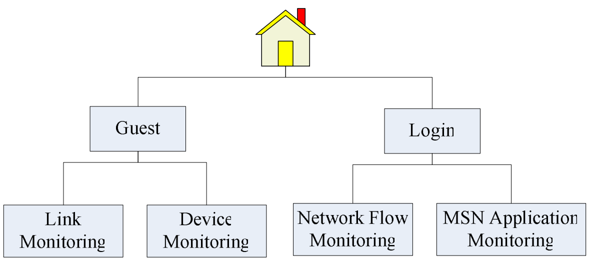

圖 10 多層次校園網路監控系統網站架構圖

成果展示

本節介紹本系統網站呈現與介面。由上而下依序為使用 SNMP 的網路設備監控，採用 CSICO NetFlow 的網路資料流監控與實現網路應用程式資料監控的 MSN 使用者監控等。

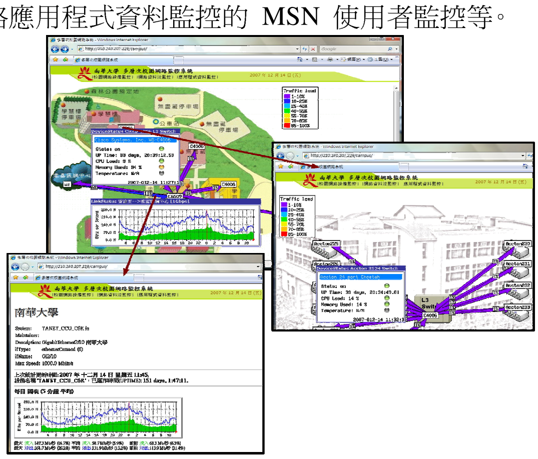

圖 11 校園網路設備監控展示圖

如圖 11，在主頁上預設直接進入校園網路設備監控，使用者可透過由 WeatherMap 所建構的直覺式網頁介面點選，進行網路設備狀態的查詢與網路流量 MRTG 監看等。網路資料流(Network Flow) 與 MSN 監視 (MSN Monitoring) 等選項，可分別顯示圖 5以及圖 8中實體以及其鍵值屬性的相關資料。

網路設備監控在頁面的呈現有別於以往的網路監控系統。為使其有更直覺的操作方式，於是讓資訊漂浮於頁面上。當滑鼠游標經過虛擬的校園地圖上網路連接路徑或建築物時，即浮現當前設備的狀態或流量資訊等，網路流量可進一步點選查看 MRTG 更完整的資訊。

圖 12，點選網路資料流監控即出現需要帳號與密碼的登入視窗，網管人員登入後即可查詢網路資料流監控與應用程式資料監控的部份。網路資料流可依日期查詢當天流量排行榜或特定協定百分比等資訊。未來朝向過濾出病毒或是木馬攻擊的 IP 位置等更為詳細的資訊供網管人員進行預防與維護網路安全的工作。

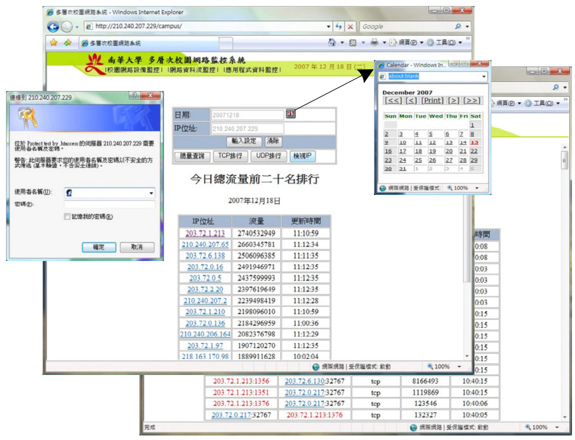

圖 12 網路資料流監控展示圖

配合網路資料流查出異常的 IP 位址，網路應用程式監視能更進一步找出問題的原因。採 MSN Sniffer 實作後確認了該部分的可實現性，如圖 13 所示。日後這部份的設計也將朝向分析與記錄 P2P 與木馬等病毒或惡意侵占頻寬的網路應用程式。

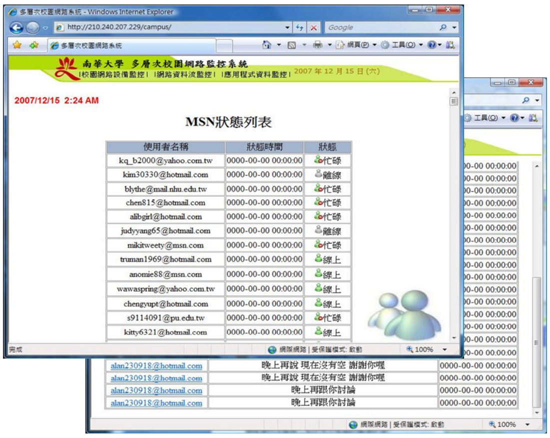

圖 13 MSN 使用者連線狀態監控展示圖

5. 結論

本論文以校園網路環境為基礎，利用網路設備內建的 SNMP 與 NetFlow 功能，配合自行發展的 Passive Application Sniffer Agent，以監控 MSN Application 資料，提出多層次校園網路監控系統。本系統以階層式架構為基礎，具備高度彈性與擴充性，系統元件可依監控需求與效能考量增加與調整。本系統依監控內容由底層往上可分為：網路設備監控、網路資料流監控、網路應用程式資料監控等功能。本系統之網路應用程式資料監控是以 MSN Application 為例，可以分析 MSN 使用者好友關係、訊息交換內容、與檔案交換內容。未來以本系統架構為基礎，可以再發展其他應用程式分析模組，分析更多網路合法與異常行為，提供網管人員重要參考數據，以協助進行網路維護、網路資源管理、網路安全管理等重要工作。

在做整體的實作時學會了團隊合作的精神和習得與每位組員的協調與溝通的能力，也在這次專題實作中接觸到更多與課堂上沒有碰過的程式語言，除了大部分底層使用基礎的 C 語言外，網頁程式的 PHP 和 JavaScript，與呈現圖片介面的 GD 繪圖的 Perl 語言，和為了有效的管理 Linux 工作時程的 ShellScript 等。也學習到 Linux 的伺服器建置與架設。都是這次專題所學習到的寶貴經驗。

參考文獻

1. 中央大學電算中心 - NetFlowExporter Project 使用 FreeBSD 掛上 Netflow 功能, http://sunsite.cc.ncu.edu.tw/NetflowExporter/
2. 台灣電腦網路危機處理暨協調中心, http://www.cert.org.tw/document/column/show.php?key=87
3. 交通大學 NetFlow 文件, http://netflow.nctu.edu.tw/netflow.htm
4. 思科 CISCO 官網-Netflow 版本與 IOS 關係 http://www.cisco.com/en/US/products/ps6601/products_white_paper0900aecd80406232.shtml
5. 廣川類, 桑村潤, PHP 5 徹底研究, 博碩文化, 2006.
6. D. Harrington, R. Presuhn and B. Wijnen, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks", STD 62, RFC 3411, December 2002.
7. J. Case, M. Fedor, M. Schoffstall and J. Davin, "The Simple Network Management Protocol", STD 15, RFC 1157, May 1990.
8. M. Rose and K. McCloghrie, "Concise MIB Definitions", STD 16, RFC 1212, March 1991.
9. MSN Messenger Protocol, http://www.hypothetic.org/docs/msn/
10. MSNPiKi, http://msnpiki.msnfanatic.com/index.php/Main_Page

.