本體論支援多重代理人技術之主動式智慧型網路管理系統的研發

Developing an Active Intelligent Network Management System with Ontology-based and Multi-Agent Techniques

楊勝源
聖約翰科技大學 電通系
Email: ysy@mail.sju.edu.tw

張譯仁
聖約翰科技大學 電機系
Email: 96N05018@student.sju.edu.tw

摘要—本系統透過智慧型代理人軟體間的合作與協調，進行相關網路資訊的擷取。系統經過分析後提出警示，俾能監控網路上被管控物件間可能產生的錯誤徵兆，藉以管控網路已發生或預測可能發生的錯誤，成為一植基於多重代理人技術之主動式智慧型網路管理系統。本技術引用本體論概念結合 Ethereal 及 Cacti 相關自由軟體，將相關網路管理運作資訊完整儲存於後端資料庫；再整合智慧型代理人技術，提供後端監控系統做進一步分析處理，呈現出圖形化網路監控系統之相關動態資訊量化圖。初步系統呈現及實驗結果驗證本技術對於網路設備即時狀態之瀏覽、分析、研判與處理及網路使用行為分析不僅故障警示精準，針對故障處理時程更縮短為傳統處理時程的61%。

關鍵詞—智慧型代理人、圖形化監控系統、網路管理、網路流量擷取。

Abstract—The system operated the information fetching through the cooperation and coordinate of the intelligent agent software. In addition, the system also provided warnings after analysis so as to monitor and predict some possible error portents generated among controlled objects in the network, and such operating mode, so to speak, an active and intelligent network management system with multi-agent techniques. This technique derived from the ontology combining with related free software - Cacti which stored the operating information of network management perfectly into the backend database; furthermore, integrated intelligent agent techniques to provide backend monitoring system with further analysis so as to present related quantification figures of dynamic information of graphic network monitoring system. The experimental outcomes of the system prototype proved that the techniques implemented in this thesis could not only precisely recognize error alarms but also indeed reduce the recovery time to 61% of traditional processing time for network troubleshooting when real-time browsing, analyzing, estimating, handling, and engaging to behavior analysis of using network.

Keywords—Intelligent Agents, Graphic Monitoring Systems, Network Management, Network Flow Fetching.

一、緒論

網際網路的迅速發展，使得網路日益複雜及龐大，如何有效管理網路上各種不同的網路區段及設備，了解問題症狀並適時以直覺式圖形化介面來提出警示，藉以提升網路的服務品質與效能，早已成為近代網路管理中一項非常重要的課題[2]；況且，網路環境也從以往單一廠商的封閉式環境轉變為多個廠商的開放式異質環境。各式不同廠牌、類型的網路設備及軟體整合在一起，造成網路產生問題的機率相對提高，監控的困難度亦日益加深。然而，現有的網路管理系統不僅在設備及流量上皆有不同的管理應用程式；更嚴重的是現有的網管軟體均不夠人性化和缺乏彈性的監控機制，必須個別學習、維護及管理，當問題發生時，只有網管人員看得懂監控資料[10]，無法真正滿足使用者端之實務需求。

針對上述問題，市場上雖有各式不同的解決方案，諸如 HP OpenView、CA Unicenter TNG 或 IBM Tivoli 等軟體符合上述強大的異質性網路管理，然而其採購建置費用龐大，造成企業不小的負擔；即使是小而美的網控軟體，例如 WhatsUP、NetVCR 等，其模組化架構或是限制管控設備數量，卻也直接造成企業及網管人員的困擾，諸如：如何由複雜的網路結構中便捷地整合歸類出問題；無法透過單一平台提供智慧型動態資訊整合，分享關聯性查找問題；異質性網管產品資訊鬆散不同步，無法提供高智慧性整合數據等。

本論文即探討如何因應各式企業環境需求亦能有效地整合不同網路設備間的資訊，簡易達成網路監控管理系統。首先，藉由本體論（Ontology）建構自

由軟體 Cacti 與外掛 Scripts 來實作各式監控圖表；搭配分散式智慧型代理人機制加以分析整合[6]，建立出完整且準確的整體性網路資料，並存入後端 My SQL 資料庫；最後，透過系統網頁呈現分析出有效且高品質的直覺式動態網路資訊量化圖[7]。這種作法的意義在於：提供便捷、具深度、且貼近於使用者之網路相關問題解答；不僅縛節企業軟體成本與降低網路管理人員被諮詢的工作負擔，更可讓一般使用者直接透過系統網頁提供的動態網路資訊量化圖瞭解目前所使用的網路狀況。

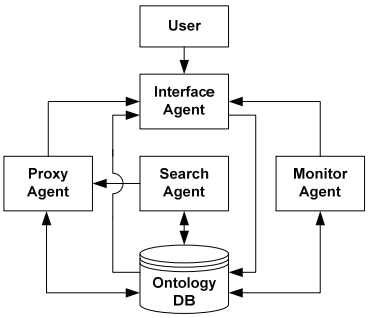


圖 1. 圖形化監控代理人架構圖

圖 1 例示出本系統的架構。介面代理人（Interface Agent）扮演使用者與系統間的溝通橋樑，傳遞人機間所有的訊息溝通；並透過操作介面之功能設定，來提供使用者的查詢結果；代取代理人（Proxy Agent）則扮演介面代理人與後端蒐集代理人（Search Agent）間之中介者，可有效降低後端伺服器資料庫的擷取負擔；監控代理人（Monitor Agent）能同時運行即時地對多個網路設備進行監控，負責擷取與收集來自設備之不同的資訊，並存成本體論主導之動態網路資料庫，方便系統直接存取並輸出監控結果；最後，蒐集代理人藉由本體論支援的網站模式，執行及時且兼顧使用者導向與領域相關的網路資訊擷取，達成植基於多重代理人技術之主動式智慧型網路管理系統的真諦。

綜言之，本論文提出並整合下列資訊技術：本體論（Ontology）、資料整合及代取（Proxy）機制，並勾勒出圖形化監控代理人於網路維運效能服務系統的四個主要組件：介面代理人、代取代理人、監控代理人與蒐集代理人的系統架構，俾能從上述四個觀點，有效地提昇與改善網路監控品質，達成主動式網路管理模式之智慧型網路管理系統。本系統 NPM（Network Performance Monitoring）的應用領域是監控廣域網路及區域網路底層架構、直觀設備及網路營運狀態，除了讓網管人員及時瞭解故障資訊，同時便於使用者獲取訊息並有效地共用知識，縮短網路相關問題的解決時間。初步系統呈現及實驗結果驗證本技術對於網路設備即時狀態之瀏覽、分析、研判與處理及網路使用行為分析確能減少問題故障之復歸時間（Recovery Time）[16]。

二、背景知識與相關開發技術

2.1 本體論

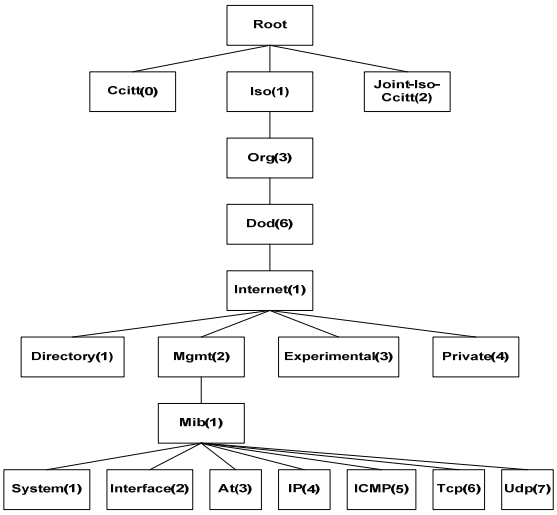


圖 2. MIB 定義 SNMP 部分本體論

本體論原本是哲學領域中的論點，主要探討生命或現實事物的知識本質。本體論能提供完整的語意模型，透過本體論來描述知識內容的架構，可以完整地呈現一個特定領域的知識核心，自動地瞭解相關領域資訊、溝通及存取，甚或更進一步推論出新的知識與結果，對於資訊系統的建立與維護，是個非常有力的工具[27]。圖 2 就是一個常用網路協定知識的部分領域本體論，主要定義網路設備間各種資訊儲存架構的相關基本知識[3]。本系統採用 Protégé-3.1.1 [25]做為本體論的建構工具。

2.2 管理訊息資料庫（MIB）

管理訊息資料庫MIB（Management Information Base），架構於網路中監控與被監控的設備上，可用來儲存各式各樣的SNMP物件。因為不同種類或使用不同通訊協定之網路設備，均有其獨特的網路管理模式，故每種網管模式都會有其自身的MIB物件集合，諸如設備之網路界面、路由表格、IP封包之傳送接收等，本系統將這些資訊統稱為SNMP物件，並以標準格式儲存於MIB本體論資料庫中，藉以進一步管理監控網路上的各項設備之相關管理資訊。

2.3 SNMP 協定

SNMP 是簡易網路管理通信協定（Simple Network Management Protocol）的簡稱，也是網際網路的協定標準之一。它能讓網路上不同的設備，有共通標準，並可提供網路管理的資料。這些資料，可進一步由網管應用程式來讀取或進行監控。換言之，每

一被監控的系統上均運行一稱為代理人的軟體元件，且透過 SNMP 對管理系統報告資訊，只要網路設備上擁有 SNMP 代理人機制，系統即可使用網路管理軟體，透過這些代理人，檢視或監控其設備上的相關網管資訊。

2.4 相關開發工具與技術

Cacti 是一種利用 PHP 程式語言編寫運用 SNMP 採集資料，結合 RRDtool、SNMP、MySQL、Apache 等多種工具組合而成[15]。它是一種圖形化呈現的網路監控軟體，能儲存相關監控資訊及其時間序列（time-series）；並具備多項強大的特色：幾乎支援所有的網路協定、豐富的過濾語言、易於查看 TCP 交談等，是目前全世界最廣泛的專業網管效能監控軟體之一[19]。它的元件可建構一個以本體論為基礎的網路通訊協定分析系統，且建置完成之本體論資料庫可適用於其它網管軟體讀取分析；也可直接匯入資料庫系統，如 MySQL，支援的功能較其它網路監控工具來得完整。本系統採用版本為 0.8.7。

RRDtool 指的是環狀資料庫工具（Round-Robin Database）。它是一套可將數據轉換成圖表，並可動態更新圖表的程式[26]。RRDtool 可用於網頁瀏覽器中顯示 PNG 格式的圖像，這些 PNG 圖像來自動態資料的收集，它可以是網路平均使用率、峰值等，最適合儲存時間序列的資料，圖表以時間為 x 軸、流量為 y 軸來表示。

MySQL 是一開放源碼的小型關聯式資料庫管理系統，開發者為瑞典 MySQL AB 公司[24]。目前 MySQL 被廣泛地應用在 Internet 的中小型網站。由於其體積小、速度快、成本低，許多中小型網站為了降低網站總體擁有成本而選擇它作為網站資料庫。SQL（Structured Query Language）則是一種常見的關聯式資料庫查詢語言，用來取得資料庫中的資料。

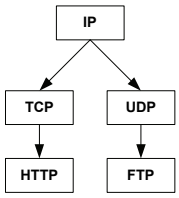


圖3. Ethereal封包解析協定樹概略圖

Ethereal由Gerald Combs開發，是一個開放原始碼免費的網路分析系統軟體，也是目前最好的網路通訊協定分析器之一[20]，支援Linux和MS Windows平台，架構採用協定樹的方式，示如圖3。在國際標準組織ISO的OSI（Open System Interconnection）7層網路協定模型，網路封包資料是從上到下封裝後發送的，因此，對於協定分析需要從下至上進行。首先，對網路層的協定識別後，進行封包還原，然後脫去網路層協定表頭，將裡面的資料交給傳輸層分析，如此循環進行直到應用層為止。由於程式採取開放原始碼的方式，更新通訊協定迅速，支援不同軟體匯出的封包擷取檔案格式，最後，透過圖形介面來表示，清晰易懂，為目前廣為世界各地專業網管使用，本系統安裝版本為0.10。

本系統使用Ethereal內含的WinPcap工具，包含核心的封包過濾，一個低階動態聯結函式庫，和一個高階系統函式庫的Pattern來定義一個過濾的正規表示法[29]。如此，即可直接存取封包應用程式界面來分類通訊協定、儲存記錄，用以提升分類的及時性及其精準度。WinPcap是一個可在Win32環境下用來擷取封包的工具，同時也可讓使用者運用高階應用程式介面去執行一些較低階的擷取功能，因此，在開發有關封包擷取的軟體時，WinPcap是一個相當理想的選擇。WinPcap的基本架構大體上可分為三部分，包含了一核心層次的封包過濾器（Netgroup Packet Filter, NPF）；在使用者層次則提供兩個動態連結函式庫：一個較低階的動態聯結函式庫（Dynamic Link Library）；以及一個高階並且獨立於作業系統的聯結函式庫（System-independent Library）。在核心層部分，最主要的工作就是擷取網路卡收到的封包，以及過濾與監聽封包；在擷取封包的過程中，必須要繞過網路協定堆疊，擷取在網路中傳輸的封包，此部分必須運作在作業系統核心中，並且能與網路驅動介面做直接的互動；亦即必須在WinPcap定義NPF來達成上述核心層的工作。在使用者層，packet.dll是一個動態鏈結函式庫，其提供較低階存取的API（Application Programming Interface）可供存取硬體層之參數。packet.dll為Win32平台提供了一個公共介面，不同版本的Windows系統均有其對應核心，來解決系統核心間的差異問題，使得動態鏈結packet.dll的程式可運作在不同版本的Win32平台上，而無需重新編譯。至於wpcap.dll則是一個在擷取程式內的靜態函式庫，內含諸多的系統函式，這些函式與硬體型號或是作業系統版本無關，提供一個高階且方便的途徑去擷取封包，如圖4所示。

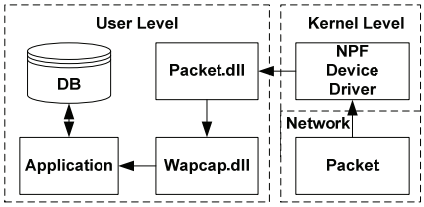


圖4. WinPcap運作流程圖

多重代理人系統（Multi-Agent System：MAS），係指多種代理人所形成的分散式環境。有鑒於目前許多的軟體或資訊系統，皆由許多不同的代理人程式所

組成的趨勢，在多重代理人系統環境中，各種類型的代理人可協同其個別技術、知識、目標和計劃來整合解決分散式問題，展現出多重代理人的異質性（Heterogeneity）與多重代理人間的溝通特性[5]。本論文即運用多重代理人來完成相關網路效能的監控及直覺式圖表繪製與更新的智慧型網路資訊控管系統。它會在監控網路上，主動於既定規則與授權範圍內活動，在沒有時間與空間的限制下，協助其委託人進行網路資訊蒐集、過濾、整理、分析與呈現。

三、系統架構及處理流程

3.1 系統開發及運作

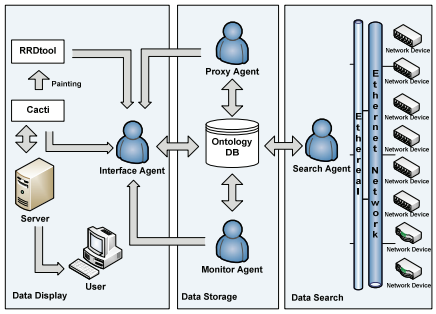


圖5. 系統運作架構圖

圖 5 為本系統運作架構，系統後端伺服器作業系統採用 Windows 2003 Server 版本及 IIS 6.0 [11]。智慧型代理人系統則使用 Java 來開發其相關作業環境[17]，並常駐佈建於主機的電腦上執行；再利用各代理人間的合作機制，以 KQML（Knowledge Query Manipulation Language）的標準語言彼此溝通、協調與分工合作，藉以蒐集相關網路之動態封包通訊協定及數據，並將數據資料存入後端 MySQL 資料庫，藉以建立該領域的本體論；最後，安裝自由軟體 Ethereal 及 Cacti，Cacti 搭配 RRDtool、Net-snmp 等套件來協助實作各式網路流量圖及狀態圖，使監控圖表的代理人及本體論相結合，用以支援該領域的網路流量統計分析與通訊協定與 IP 分析[14]。使用者之前端網頁則使用 PHP 語法來呈現出相關的數據及狀態，讓系統監控能力更加完整，同時亦簡化了系統安裝及設定流程，大幅降低本系統實務導入時的困難度[23]。相關多重代理人之角色及任務與完整群組之詳細工作流程，茲分述如后。

3.2 介面代理人

圖6即為本介面代理人的細部架構與其它相關代理人的關係圖，其內容模組可以區分為User Login（使用者身份確認掌握）；User Manager Program（管理使用者的功能存取權限）；Personalized Web（個人化網頁呈現）；Painting Component Model（數據繪圖模組），Webpage Processor（預先下載與處理直覺化圖型相關網頁）。

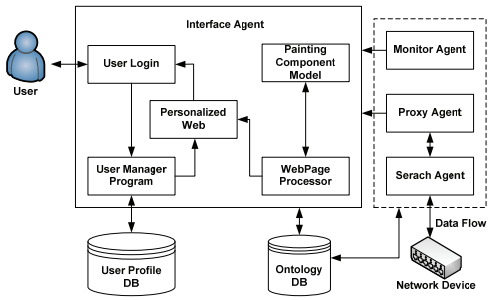


圖6. 介面代理人的架構圖

當介面代理人收到使用者的登入查詢請求，為驗證每一個登入使用者的身份及給予瀏覽權限來進行帳戶分級管理，經由User Manager Program接收到使用者帳號及密碼後，轉向後端使用者個人資料庫（User Profile DB）搜尋使用者資訊。使用者管理程式認證流程說明如下：在資料庫裡，設置不同用戶存取權限之使用者資料，使用者管理程式去讀取使用者模組資料庫帳號權限進行比對，並對內部資料表格依序讀取下列四種記錄類型：

(1) Auth：對使用者所提供的帳號認證資訊做驗證；
(2) Account：非認證方面的帳號管理，比如檢查帳號密碼的期限是否過期等；
(3) Password：對使用者所提供的密碼認證資訊做驗證；
(4) Session：與使用者在存取服務前後所需執行的一些工作有關聯，比如紀錄掛載目錄的資訊、限制使用者的資源使用等。

針對上述資料庫的記錄來搜尋符合登入使用者的瀏覽權限，一旦驗證成功，使用者管理程式則依據其登入的帳號作權限管制，完成整個認證過程，並將認證結果傳回給Personalized Web，分別呼叫所使用的個人化網頁機制，來產生對應的個人化權限網頁機制[12]，運作流程詳如圖7。

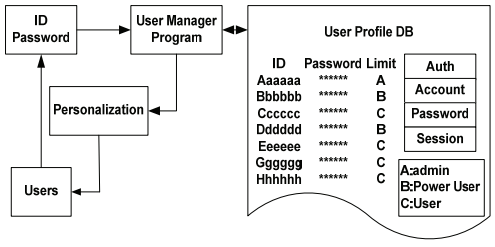


圖7. 使用者帳號認證架構圖

Painting Component Model使用Cacti的RRDTool模組套件，可定時透過監控代理人及代取代理人對網路設備間收集相關網路流量的資料並繪製成圖表，如圖8所示。

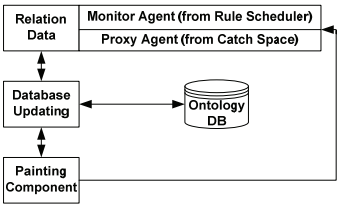


圖8. 繪圖模組流程圖

```
<?
      $corder=@$HTTP_GET_VARS['color'];
      $width=@$HTTP_GET_VARS['width'];
      $height=@$HTTP_GET_VARS['height'];

      if ($corder=='') {$corder='000000';}
      if ($width=='') {$width=20;}
      if ($height=='') {$height=20;}

      if ($width<=0) {$width=1;}
      if ($height<=0) {$height=1;}

      $im=imagecreate($width,$height);
      $back_color=$corder;


$black=imagecolorallocate($im,hexdec(substr($back_color,0,2)),
hexdec(substr($back_color,2,2)),hexdec(substr($back_color,4,2)));

      imagefill ($im,0,0,$black);
      imagepng($im);
      imagedestory($im);
?>
```

圖9. PHP圖型顯示部份語法

領域本體論資料庫（Ontology Database）的建立，則分別將每日所產生的圖示數據資料分開存放[1]。由監控代理人及代取代理人傳送過來的數據資料進行訊息接收，待Relation Data（關聯資料）例如：IP流量排名及日期時間相關流量數據等，完成關聯網路流量圖示化資訊數據後，則進行Database Updating（更新數據庫），並利用Cacti的流量背景樣板圖型依接收的資料（由Database Updating來源輸出的資料）及PHP繪製通訊協定分析、IP流量排名的整合資料，其部分撰寫語法如圖9所示，透過Painting Component Model來繪出相關監控圖表，並一直循環執行。最後，透過介面代理人的執行流程，以網頁呈現企業內部網路系統的整合監控運作情況，並以Webpage Processor來呈現出相關即時網路監控直覺式圖形，例如：流量數據圖、設備狀態圖，並可週期性更新畫面上各項設備的即時狀態，提高企業內部網路監控資料整合的效益及相關資訊服務的品質。

3.3 代取代理人

本代取架構係改良傳統的功能架構，發展出一套主動式代取代理人機制，其元件係由Proxy Space（網頁資料暫存區用來儲存預取的資料）；Refresher（自動按照定義的Data Display Model時間間隔刷新資料）；Data Display Model（資料顯示模組）；Scheduler（提供定時到資料庫讀取資料）四個部份組成，如圖10所示。

代取功能結合代取代理人機制，透過Data Display Model（資料顯示模組），其組成元件為Data Connection（資料連接）、Data Integration（資料整合）、Data Updating（資料更新）、Data Record（資料記錄），如圖11所示。由Scheduler應用程式定時呼叫Data Display Model的Data Connection，透過標準的SQL語言資料查詢方式，將資料查詢的語法傳遞給Ontology DB資料庫，並解析出使用者查詢語法中所夾帶的資料來源位置，向資料庫來源進行相關資料讀取，其執行相關步驟為：

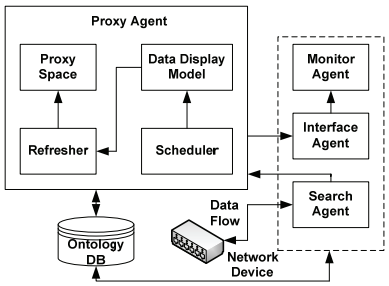


圖10. 代取代理人架構圖

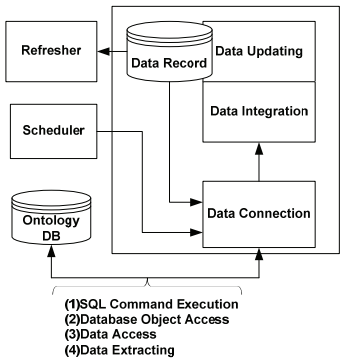


圖11. Data Display Model架構圖

(1) SQL Command Execution：執行SQL命令列；
(2) Database Object Access：搜尋相關的資料表格工作；
(3) Data Access：執行資料庫資料讀取；
(4) Data Extracting：把所需資料擷取出來。

將所查詢到的資料例如：IP（含Source及Destination）、通訊協定、流量數據、日期時間，一一傳送到Data Display Model的Data Integration，做資料關聯整合及準備數據呈現，例如：Source IP對應的Destination IP位置、通訊協定的歸納等；透過Data Updating更新資料移入Data Record成為新的資料記錄，並將整合完成的數據處理結果回傳給資料庫，做為歷史查詢的數據資料，來維持資料的一致性；再將數據資料透過Refresher元件進行內部資料的更新後暫存到Proxy Space，用來暫時儲存固定被要求的資料；再由介面代理人的Painting Component Model來向Proxy Space讀取資料。當有使用者提出瀏覽需求時，則透過介面代理人傳送給瀏覽器，完成這一連串監控資訊整合過程，藉以提高監控資訊瀏覽速度與相關處

理效率，以減少監控資訊存取時間。因此，本代取代理人可依據使用者的真正資訊需求，務實地縮短使用者至資料庫的查詢時間，進而達成查詢係以使用者導向之的。

3.4 監控代理人

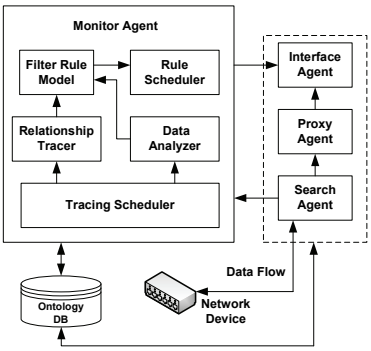


圖12. 監控代理人架構圖

本代理人係透過結合相關監控及運算機制，將資料及數據先行彙整，並經集中處理運算後，主動提供即時、符合使用者需求且適性化的監控資訊內容；監控代理人更能同時對網路流量及設備的監控行為做更有效率的分派、協調，如此更能在兼顧資料的變動情形與系統資源有限的前提下，提供主動且有效率的監控資訊服務[4]。本系統設計以監控網路流量示警及網路設備為主要功能，如圖12所示，包括：Tracing Scheduler（定時將資料庫資料讀取）、Relationship Tracer （網路通訊埠關聯）、Data Analyzer（分析擷取流量數據）、Filter Rule Model （示警運算模組）及Rule Scheduler（所得結果定時送至介面代理人）。首先，利用Tracing Scheduler元件定時讀取資料庫所需要的資訊數據，因資料庫記錄檔的資料非常繁雜，需透過Relationship Tracer及Data Analyzer去分析讀取資料庫不同來源的記錄檔，將需要的資訊區塊讀取出來，如：網路設備的介面通訊埠、流量數據及日期，來做資料的關聯整合，並透過Filter Rule Model（如圖13所示）進行數據資料讀取Data Reading（From Relationship Tracer and Data Analyzer）、數據分析及診斷（Data Analysis and Diagnosis）、數據處理（Data Processing）、故障警示（Error Alarm）及正常狀態（Normal State），以下說明Filter Rule Model運作流程。

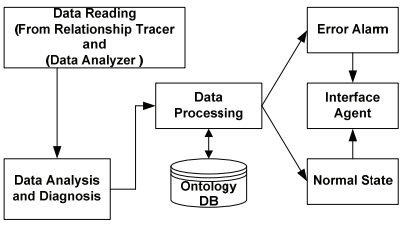


圖13. Filter Rule Model架構圖

首先，Filter Rule Model從Relationship Tracer取得各網路通訊埠狀態訊息，例如：運行狀況是Up或Down，再從Data Analyzer取得相關數據資料，例如：取得網路設備通訊埠上各流量數據，本代理人透過這兩者數據分析及診斷後；再將處理後的數據按使用者的要求，系統加權計算後，算出最後的結果，例如：x<=40表綠色正常、80=>x>=41表黃色示警、x>=81表紅色示警；最後，系統據此透過介面代理人做出適當的警示。這種作法不僅即時產生數據做處理，同時儲存於資料庫；一則針對歷史紀錄，做資料流量的分析，以利後續的歷史資料查詢；再則依據管理者事先設定好的訊息處理做出適合的回應。

綜言之，本代理人係根據所得到的結果來判斷臨界值是否符合管理者的設定，藉以判定設備現有的狀況，來反應為故障警示或正常狀態結果，並觸發相關的警訊處理兼顧增強偵測被管理物件異常狀態與示警通知能力；隨後透過介面代理人模組，將接收到設備狀態數據結合繪圖模組處理，以直覺式圖型表示並週期性更新畫面上各項設備的即時狀態。使用者亦可透過瀏覽器隨時觀看整個網路與設備之連線狀態，進而得知監控設備與網路頻寬的即時狀況。因此，網路管理者不僅可輕易地判斷網路異常，如流量過大、線路中斷等，更可快速找到故障事件點儘速隔離及排除，務實縮短問題故障之復歸時間[8]。這種作法不僅減少使用者監看的資料量，更能增進網路監控系統的效能。

3.5 蒐集代理人

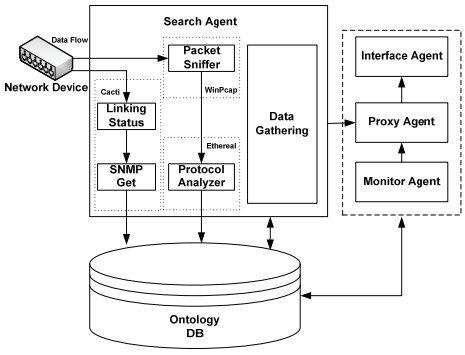


圖14. 蒐集代理人架構圖

網路監控所需蒐集的資料因地制宜，支援監控代理人所產生的資料格式及內容也截然不同。本蒐集代理人為觀察整個網路與設備之連線狀況，引用相關領域本體論、Cacti 及 Ethereal 等開放源碼之相關函式庫，建構在 SNMP 核心之上，包括 Linking Status（連線狀況）；Packet Sniffer（封包收集）；Data Gathering（資料採集）及 Protocol Analyzer（協定分析），完整架構詳如圖 14 所示。整體運作分為封包收集和網路流量收集。前者，將網路設備啟用監控（Monitor）

通訊埠功能，利用 Ethereal 內建封包採集函式所產生的 Packet Sniffer，來收集網路上所有傳輸封包，並透過 Protocol Analyzer 分析通訊協定及其對應 IP；後者，則透過 Cacti 的 SNMP Get 通訊協定來收集整體網路流量數據[21]。相關元件的功能及運作，茲分述如后。

Packet Sniffer 封包蒐集器透過 WinPcap 工具從網路上接收傳來的流量封包，然後使用以 Ethereal 為基礎的 Protocol Analyzer 來做協定分析，將傳送來的封包根據對 IP 封包所屬之資料流（Data Flow），做多重通訊協定分類，依封包標頭的五個欄位（Source IP、Destination IP、Protocol、Source Port、Destination Port）來分類封包的資料流。依據封包的標頭與內容、進行過濾的動作，來辨別出所使用的 Protocol、IP 及 Port，並將流經的每條資料流基本資料以及設備的相關資訊狀態儲存於 Ontology DB 本體論資料庫中。另 Linking Status 元件週期性運用 Windows Ping 方式偵測設備的最新的狀態，為每個網路設備通訊埠進行連線狀態的維持偵測，同時引用 Cacti 的 SNMP Get 通訊協定週期性收集網路即時流量資訊，負責連線資訊的紀錄與流量數據的抓取，其所記錄到之相關網路監控資料及數據，都會藉由 SNMP Get 儲存在 Ontology DB 本體論資料庫。透過 Data Gathering（資料採集）元件加強資料分析與對應資料庫連結功能，根據每條資料流的識別碼，可至本體論資料庫中尋找對應的資料流紀錄[13]。例如：SMTP、HTTP、TCP、UDP、ICMP 協定對應到的 IP。直接把定義監控資料從資料庫按分類讀取出來，根據對應 IP 彙整相關監控資訊，並同步更新資料庫的資訊；根據代取代理人所訂定的顯示資料，來檢視封包的標頭找出符合的規則。最後，傳送完整的監控資訊到代取代理人，方便使用者透過介面代理人來讀取欲查詢之相關監控訊息，快速、精準且及時地觀察相關網路狀態，包括網路設備、使用通訊協定、IP 與網路頻寬之運作資訊及其相關狀態。

3.6 知識塑模及本體論資料庫建置

本系統選擇史丹佛大學醫學中心所研發的 Protégé-3.1.1 作為本體論建置工具。它不僅擁有 Java-Based 的特性，具備支援多種平台的版本，尚可外掛載入視覺化階層架構圖（TGVizTab）來延伸建置功能，方便檢視本體論內容的一致性（Consistency）。綜言之，其最大特色是透過多類元件進行知識本體的編輯與製作，讓知識工作者可以建構一個以本體論為基礎的知識管理系統，且建置完成之本體論不但可轉換成各種不同的本體論格式，諸如 RDF(S)、OWL、XML 等；亦可直接匯入資料庫系統，譬如 MySQL 及 MS SQL Server，支援的功能較其它本體論建置工具來的完整。

首先利用 OWL 語言描述 MIB 資訊及定義，接著再透過已建置完成的 MIB 本體論做結構性分類，也就是利用 MIB 的層級概念來表達各階層之關係，其所建構的本體論架構來分析各種封包中所包含的意義，並將這些意義記錄到對應本體論中而形成不同分類群組，概念如圖 15 所示。

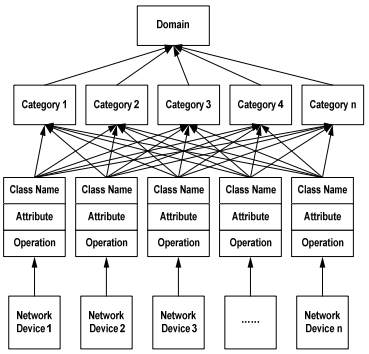


圖 15. 本體論概觀圖

表 1. 類別與標號的對應

類別	標號	所包含的訊息
System	（1）	主機或路由器的作業系統
Interfaces	（2）	各種網路介面及它們的測定通信量
Address Translation	（3）	位址轉換
IP	（4）	IP 分組統計
ICMP	（5）	已收到 ICMP 消息的統計
UDP	（6）	演算法、參數和統計
EGP	（7）	外部閘道協議通信量統計

上圖說明一個區域網路透過封包蒐集器蒐集資料所形成的本體論的概觀圖，Domain 表示一個可執行 SNMP 的網路元件上運作的軟體，可蒐集網路封包及流量數據的 SNMP 要求的根（root）；Category[1…n]表示可執行在特定管理信息庫中定義資訊和管理功能的子類別；Class Name 表示 Category 的子類別，其中包含每個封包相關內容，舉例來說：一個管理信息庫有主代理的資訊、配置主代理的參數、回應管理者的要求、產生警告等子類別，而上述的定義資訊又有 System、Interfaces、Address Translation、IP、ICMP、TCP、UDP、EGP 等的子類別，而每個子類別的屬性均有標號，如表 1 所示。

每一個階層的運作代表連結（Link）。本系統透過 MIB 蒐集多種目前常被使用到的通訊協定與應用服務。了解訊息格式在封包標頭與應用層內容中的特性與規格。歸納出分類封包時需要使用到的比對特徵，進而設計出 MIB 本體論資料庫。它具有網路 OSI 七層內容檢視、動態的通訊協定狀態紀錄與維持，根據多種常見的通訊協定與應用服務規格，包含足夠的比對參數種類，歸納出檢視封包標頭與 OSI 七層內容時會使用的比對特徵；利用 Ethereal 工具以提供狀態內容分類引擎（Statefully Content-Based Classification

Engine）做為封包分類時的依據，來滿足便利與彈性的需求。如此，涵蓋足夠的比對參數種類，才能描述出各式的通訊協定或應用服務。最後，將其統計彙整進而建立可供搜尋的資料庫。換言之，系統利用建置好的網路協定本體論資料庫，支援蒐集代理人進行相關網路協定封包的蒐集，支援系統進行分類處理。針對的蒐集代理人而言，本體論引領領域封包蒐集指引；對分類功能來說，本體論則是更進一步由特性去細分類別，並設定出諸多類別樣式當作通訊協定分類的依據。因此，我們只建構單一領域本體論去支援蒐集代理人，但卻必須設置數個不同型樣的本體論去支援分類功能。透過此本體論概觀圖，可以自動的判讀資訊的關聯，本系統之本體論資料庫的建置包括：網路協定相關概念統計與分析及本體論資料庫的建立兩階段，茲細述如后。

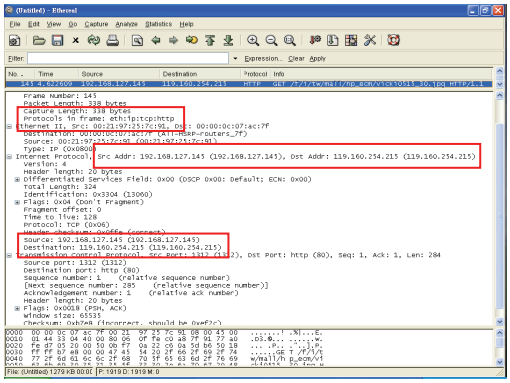


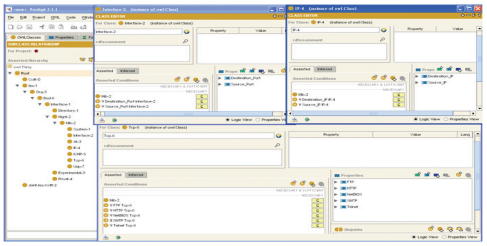
圖 16. 封包內容

首先，我們蒐集網路協定相關概念關鍵字及其對應封包格式，如圖 16 所示。系統根據網路協定相關概念關鍵字將其對應的標準封包格式，則按分類型樣進行相關資訊分類，方便蒐集代理人進行監控資訊引用，並具備比對通訊協定封包內容。換言之，假使比對符合欲監控之對應通訊協定概念，且其封包格式亦正確，系統則據以判斷此蒐集之網路封包的通訊協定符合蒐集歸類的標的，並將此資訊附掛於 MIB 本體論資料庫的分類標的之下，藉以蒐集真實資料案例，增強系統判斷資料的精準度。

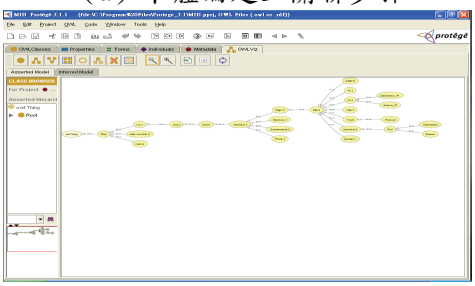
本系統利用 Protégé-3.1.1 OWL [9]編輯器建置完成本體論建置的第二階段：MIB 本體論資料庫，詳如圖 17 所示。

系統搭配本體論和比對規則，規則格式為：網路協定、來源和目標的 IP 位址、來源和目標的通訊埠。當系統比對出對應關鍵字，這些關鍵字就是一個本體論的概念所形成的集合，藉此判斷出對應的通訊協定，再經對應封包格式的比對，即可輕易判斷出何種協定的特定封包格式，來支援上述代理人間的系統運作。本階段主要是將建置於 Protégé-3.1.1 中的本體論轉換成 My SQL 資料庫，方便系統精準引用本體論資訊，步驟如下：

(1) 將Protégé知識庫所建置好的檔案匯出成XML檔，這正是Protégé的強大知識再用性與快速知識嵌入能力的明證。
(2) 最後再將XML匯入My SQL資料庫，方便系統相關元件的存取，完成本體論資料的建置，如圖18所示。



（a）本體論建立關聯步驟



（b）本體論階層圖

圖 17. Protégé 建置領域本體論

圖18. 網路協定本體論資料庫轉換流程

四、系統呈現與驗證

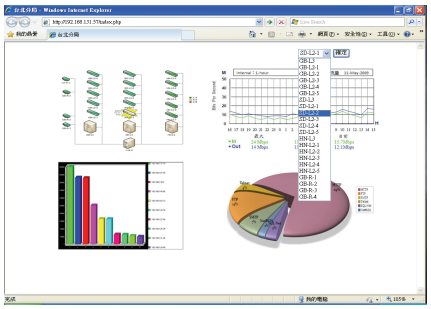


圖19. 本系統網路監控第一層主畫面

爲了讓使用者清楚了解網路狀況，本系統首頁呈現方式採階層式概念設計，包括以網路設備為主體的網路設備狀態圖、網路設備流量圖、流量排行及協定流量排行等四大部分。第二層為網路設備詳細狀況，包含所有相關之設備、連線狀態、協定通訊資料等，如圖 19 所示出系統擷取的網路監控主畫面。茲將相關監控細節分述如后。

4.1 使用者介面

本系統為直覺式圖型化監控模式，為方便系統管控網頁瀏覽權限，使用者分成三種類型，包括：User、Power user 及 Admin 三種身份。User 登入後只能在網路瀏覽系統提供的第一層監控主畫面；Power user 可以進入第二層之進階畫面瀏覽；Admin 除了可以瀏覽上述兩者外，尚可設定網路設備及使用者權限，相關設定功能分述如后。

(1) Device：新增、刪除網路設備 IP，詳如圖 20 所示。當網路設備 IP 設定新增後，其下方 IP Address List 則顯示出方才設定好的 IP 位置；若要查詢這一台設備有多少介面通訊埠受到系統監控，則須選擇欄位 Interface 對應之查詢按鈕，如圖 21 所示。

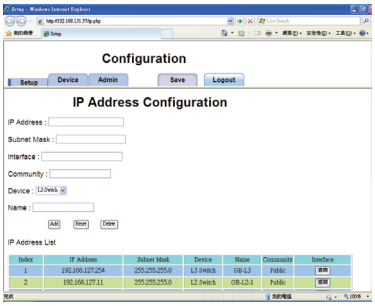


圖 20. 網路設備新增移除設定

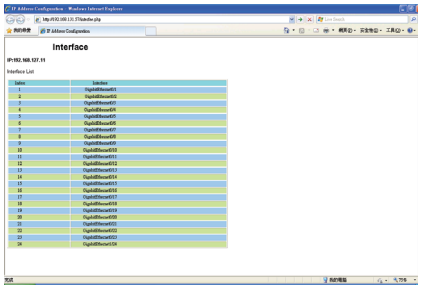


圖 21. Interface 設定顯示

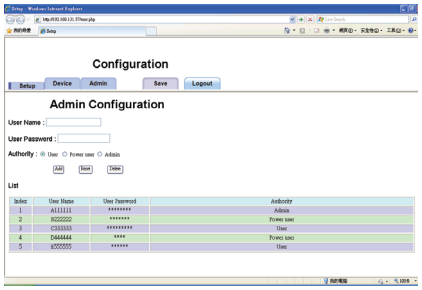


圖 22. 帳號密碼新增移除設定

(2) Admin：新增、刪除使用者帳號及密碼，如圖 22 所示。當新增帳號完成後，則可在 List 下顯示出新設定的帳號、密碼及其相關網頁瀏覽權限。

4.2 網路流量排行榜

圖 19 左下角顯示出流量排行榜統計能讓使用者得知那些主機佔據頻寬使用網路的最大流量。若想要知道那些相對應主機間造成的流量，亦可點選對應網頁圖示，即可輕易顯示進階狀態，如圖 23 所示。

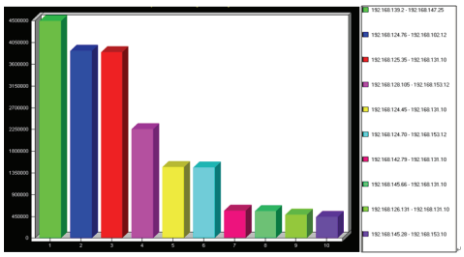


圖23. 網路流量進階分析

4.3 協定流量

圖 19 右下角顯示出每個應用協定頻寬使用的情況，系統分析網路佔滿頻寬的應用程式為何？並能清楚羅列出使用的連線方式及其頻寬使用率方便使用者觀看與查詢，協助使用者便瞭解那些軟體系統佔用電腦的最大的網路頻寬。

4.4 網路流量趨勢

圖 19 右上角則以圖形化顯示整個網路的流量分析圖。系統可統計當日或過去任意時段的網路流量，利用最大頻寬的臨界值警告，主動監控網路流量。系統能在網路中斷時或頻寬滿載時自動發出預警，讓使用者能儘早發現，即時處理事件，從而避免故障時間，讓使用者隨時追蹤掌握事件狀況。

4.5 網路設備狀態圖

本系統能顯示出監控網路基礎架構下相關設備的狀態圖，如圖 19 左上角所示。當設備或連線狀況出現障礙時，及時將設備狀態反應於連線圖示上。系統會根據障礙點判斷並以顏色變化標示狀態，例如紅色表故障、黃色為警告、綠色則為正常。將所有異常事件皆歸屬於其所屬網路設備，除呈現顏色狀態變化外，並顯示出發生時間。讓使用者更容易了解網路狀況。本系統亦針對監控網路設備的狀況，可進一步點擊該圖示了解其設備之詳細狀況，如圖 24 所示。針對整個網路的每一個埠上，觀察其第 2-4 層的流量，提供進階使用者知道該網路問題出在基礎架構的那個部份，更能瞭解那些業務受到影響[22]。

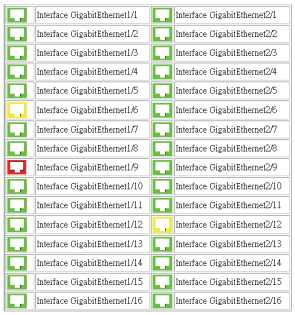


圖24. 網路設備進階監控圖

4.6 示警監控

網路監控系統在障礙管理及效能管理中，有諸多

監控項目的異常判定是藉由量測數據跟基準臨界值的比較來決定的，例如流量。然而量測數據往往會因應不同環境、時刻與用戶行為而產生不同的合理變量範圍。本系統因採微軟的作業系統，則利用 Windows Ping 指令來診斷網路連線狀態與連線品質，此一指令依據 RFC 792 透過 ICMP（Internet Control Message Protocol）協定的 Echo 功能，來檢查網路連線狀態。小型的封包被送到網路上的 IP 位址，接著就等待其回應的封包及數據，假使網路連線沒問題，網路設備也正常開啟運作，送出端將會收到完好回應封包及回應的數據，依此數據來作為封包行程所需耗費的時間。本系統利用流量分析的高度彈性及模組化的監控參數與複合式的監控條件組成過濾條件，來進行流量分析訂定一數據標準[18]，其公式如下：

〔Reply time（1）＋Reply time（2）＋Reply time（3）＋Reply time（4）/4〕＝Average 值
Reply time：設備回應時間數據
Average：計算後所呈現的數據

若回應數據的時間平均值 X，其值為小於等於 40ms 出現正常的綠色狀態；大於或等於 41ms 且小於或等於 80ms，則出現黃色警示狀態；若是 X 值無回應或大於等於 81ms 以上，則出現紅色的警示狀態，藉以判斷現存網路效能的高低，方便系統進一步作為網路故障排除的示警依據。

4.7 效能驗證

4.7.1 示警判斷的正確性

本實驗主要目的在於測試流量功能示警及封包蒐集分類判斷的正確性。系統實作環境的實體拓撲（Topology）網路架構，採用封閉式的區域網路。我們蒐集中央健康保險局某分局資訊室對機房主機兩星期內網域上所有的流量封包，並加以分析了解網域內 IP 位址之使用狀況，配合系統事先建立之對應使用者資訊庫，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。網路封包、流量數據及網路效能當成正常的訓練和測試封包，其網路效能方面是以監控代理人程式的 Ping 做測試，封包是用 ICMP 的格式，測量出兩端點間的網路流量回應時間，除測試傳送流量之餘，亦能監測網路設備運作是否穩定？此外，更在網路設備上設鏡像（Mirror）埠方便封包蒐集，網路流量數據則透過蒐集代理人蒐集，其示警結果詳如圖 25 所示。圖中，分別顯示各時間點的示警分佈，X 軸為日期時間，Y 軸為當時本系統監控資訊室到機房網路設備往返兩端點間產生之回應平均數據。透過對照整理後得到細部及時監測的流量數據圖表，詳如圖 26 所示。圖中能精準地顯示在上述發生之示警日期時間均有較高的流量，而影響到網路傳輸的效率，示警精準度幾乎 100%。

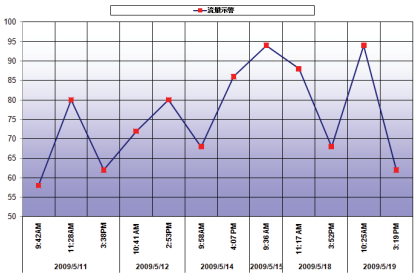


圖 25. 流量示警圖

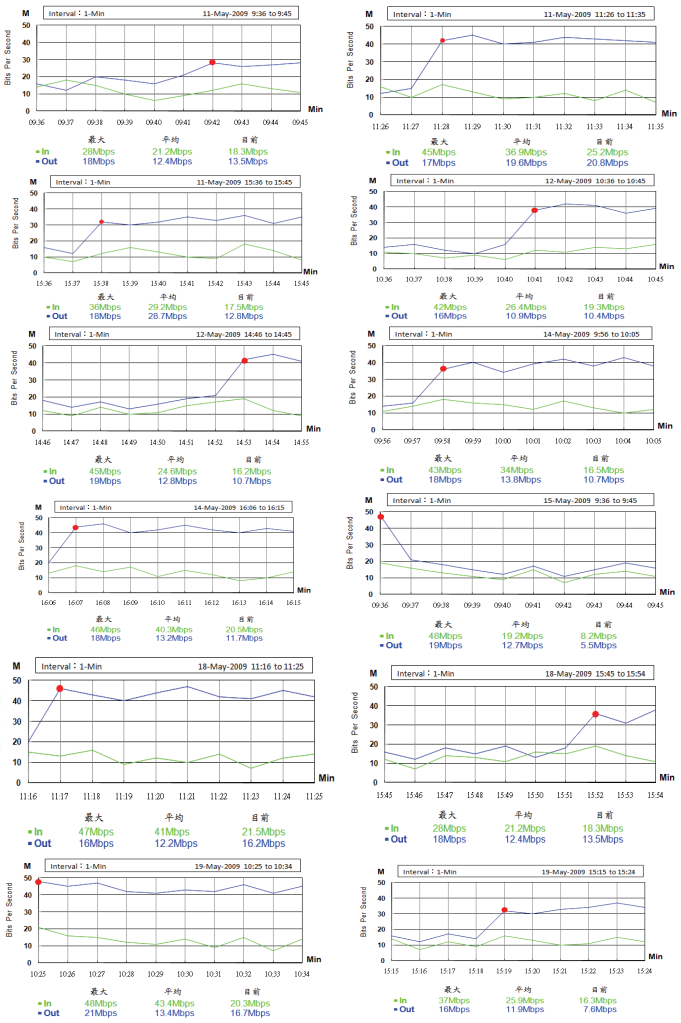


圖 26. 示警細部流量圖

4.7.2 系統處理的時效性

早期的網路故障處理，都是由使用者口述網路問題，但管理者經常遇到使用者敘述不清或無法精準釐清網路使用上的問題時，網管人員只能憑藉網路設備架構，依照標準作業程序一步步地循序檢查，造成網路管理者處理時間過久；特別當遇上大型網路架構，耗費的時程更是令人不敢輕易嘗試，深怕牽一髮而動全身。往往從網路故障到檢查確定與排除，花費的時間都在一個小時以上。然而，在這個凡事都講求效率及服務至上的資訊時代，傳統方式的處理時效性早已

無法滿足實際的需求。網管人員往往在查測過程不僅花盡心力，更要忍受使用者的詢問關愛，最重要的是無法即時的分析處理相關網路問題。在實測環境中導入本系統兩個星期，一方面訓練使用者如何操作本系統，包括觀看網路設備及流量狀態；讓使用者事先清楚瞭解自己的網路環境，當使用者遇到問題時，可先釐清是網路或是其它問題所造成？若是網路問題，使用者不僅可即時觀看是那一段網路出現問題，相關網路設備目前狀況如何？網管人員更可透過本系統來瞭解是那一個網路設備節點出現問題，進而及時排除相關網路狀況。圖 27 整理出三項常發生問題：網路設備故障、網路線路問題及流量過大問題，處理時程分析後，網路設備故障縮短為 67%（30/45=67%）；網路線路問題縮短為 50%（10/20=50%）；網路線路問題縮短為 67%（20/30=67%），平均處理時程縮短為傳統作法的 61%。引用本系統不僅簡易操作，當故障發生時示警精準更具效率，對使用者及管理者都有極大的幫助。

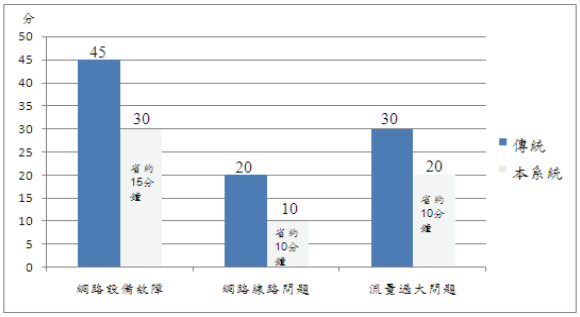


圖 27. 傳統 vs. 本系統故障處理時間比較

4.9 相關系統比較

本系統的特點在於全面監控網路設備的基礎架構，直覺化圖示監控設備營運狀態，動態監控網路狀況，及時瞭解故障資訊[28]。以下針對市面上幾種網管軟體作比較來說明本系統的優缺點。如表 2 所示 WHATSUP 無法監控遠端 IP，亦無提供直覺式圖形化介面；NETVCR 則僅能在 SNMP 協定上運作；最後一欄則是本論文採用的作法，能提供完整、有效且精準的網管功能。

表 2. 網管軟體功能比較

功能特色	WHATSUP	NETVCR	CACTI+ TEMPLATE
SNMP 監控	V	V	V
單一操作執行多請求	V	X	V
SNMP 監控支援多平台	V（軟體）	X（硬體）	V（軟體）
可即時顯示資訊	V	X	V
監控遠端 IP	X	X	V
SNMP 可自訂警告值	V	V	V
直覺式圖形化	X	X	V

五、結論與討論

本系統以管理網路設備的橋接區域網路為主，提出一本體論支援網路設備之分散式智慧型代理人軟體，整合形成一集中式網路流量資訊擷取系統。本系統透過智慧型代理人軟體間的合作與協調，來進行相關網路資訊的擷取。系統經過分析後提出警示，俾能監控網路上被管控物件間可能產生的錯誤徵兆，藉以管控網路已發生或預測可能發生的錯誤，成為一植基於多重代理人技術之主動式智慧型網路管理系統。本技術引用本體論概念結合 Ethereal 及 Cacti 相關自由軟體，將相關網路管理運作資訊完整儲存於後端資料庫；再整合智慧型代理人技術，提供後端監控系統做進一步分析處理，呈現出圖形化網路監控系統之相關動態資訊量化圖。初步系統呈現及實驗結果驗證本技術對於網路設備即時狀態之瀏覽、分析、研判與處理及網路使用行為分析不僅故障示警精準，針對故障處理時程更縮短為傳統處理時程的 61%，對使用者及管理者都有極大的幫助。

基於完全採用開放原始碼的開發工具，故系統的可塑性強。使用者能根據本系統週期性的網路監控分析，透過簡單易懂的網路圖形化使用者介面，精準瞭解與掌控網路設備之不正常的現象，準確地辨識出網路設備本身或是線路的問題，直接減輕網路管理人員的工作負擔，更間接降低相關網管維護費用與專業人員培訓成本。未來本系統將朝向兼顧操作與管理兩層次的介面發展，使管理者亦可透過此視覺化介面設定與管理各項網路設備，並進一步顯示與列印出各項分析報告與監控圖表，真正達到網路管理系統的真諦。

六、參考文獻

[1] 中華民國開放系統協會，“資料庫伺服器架設標準作業程序書”，COSA-SOP-2003-006，Version 1.00，民92。

[2] 呂崇富，網路規劃與管理實務，學貫圖書，台北，台灣，民 94。

[3] 李棟梁、楊勝源、呂思賢，“本體論支援之研究學者資訊整合推薦器之研究”，*第八屆離島資訊技術與應用研討會論文集*，金門，福建，民 98。

[4] 林韋成、伍麗樵，“User-based 行為探勘及異常偵測機制之設計”，*第七屆離島資訊技術與應用研討會論文集*，澎湖，台灣，民 97。

[5] 林揚正，應用行動代理器於分散式系統之研究與實作，碩士論文，資訊管理研究所，中國文化大學，台北，台灣，民 94。

[6] 張儀興、呂宗益，“導入智慧型代理人於適性化

學習之研究”，*TANET2006 台灣網際網路研討會論文集*，花蓮，台灣，民 95。

[7] 郭書佑、廖豐標、陳國玲，網路管理 (Network Management: Concepts and Practice, A Hands-On Approach)，碁峰圖書，台北，台灣，民 94。

[8] 陳忠祥，以代理人為基礎的網路異常監控機制，碩士論文，資訊科技研究所，台中健康管理學院，台中，台灣，民93。

[9] 陳秋娘、楊中皇，“以 OWNS 為基礎的網路犯罪偵防系統之設計與實現”，*第五屆離島資訊技術與應用研討會論文集*，金門，福建，民 95。

[10] 黃志文，網路管理通訊系統簡介，中華民國電子零件認證委員會，台北，台灣，民 97。

[11] 楊居易，IIS 6 伺服器架設與管理，文魁圖書，台北，台灣，民 93。

[12] 楊海明，一種基于 Web 的網絡管理系統的設計與實現，科技創新導報，中國宇航出版社，哈爾濱，中國，民 96。

[13] 楊素秋、曾黎明，“網路匯集點的 Flooding 訊務偵測與自動通告系統”，*TANET2007 台灣網際網路研討會論文集*，台中，台灣，民 96。

[14] 楊勝源、呂思賢，“本體論支援之研究學者資訊整合推薦器之研究”，*AIT2009 資訊科技國際研討會論文集*，台中，台灣，民 98。

[15] 劉柏汎，FreeBSD異質系統及網路管理整合應用，松崗圖書，台北，台灣，民94。

[16] 盧有志，智慧型代理人之動態網路學習系統，碩士論文，資訊管理研究所，屏東科技大學，屏東，台灣，民 92。

[17] 竇其仁、林志敏、林正敏，網路代理人，知城資訊，台北，台灣，民95。

[18] D. Baker, M. Nodine, R. Chadha, C.J. Chiang, Y. Gottleb, C.P. Hsu, R. Jaeger, G. Levin, L. Yibei, “Computing diagnostic explanations of network faults from monitoring data,” *Proc. of IEEE Military Communication Conference*, CA, USA, 2008, pp. 1-7.

[19] Cacti, The Complete RRDTool-based Graphing Solution, http://www.cacti.net/.

[20] Ethereal, The world's most popular network protocol analyzer, http://www.ethereal.com/.

[21] K.S. Shin, J.H. Jung, J.Y. Cheon, and S.B Choi, “Real-time network monitoring scheme based on SNMP for dynamic information”, *Journal of Network and Computer Applications*, 30(1), 2007, pp. 331-353.

[22] Q. Li, Q.F. Hao, L.M. Xiao, and Z.J. Li, “Vm-based architecture for network monitoring and analysis,” *Proc. of the 9th International Conference for Young Computer Scientists*, Hunan, China, 2008, pp. 1395-1400.

[23] A.R. Morffi, D.R, Paz, M.M. Hing, and L.M. González, “A Reinforcement Learning Solution for Allocating Replicated Fragments in a Distributed Database,” *ComputaciÓn y Sistemas*, 11(2), 2007, pp. 117-128.

[24] MySQL, The world's most popular open source database, http://www.mysql.com/.

[25] Protégé, Stanford University Protégé-3.1.1 Teaching website, http://protege.stanford.edu/.

[26] RRDTool, RRDTool Logging & Graphing, http://oss.oetiker.ch/rrdtool/.

[27] M. Trifan, B. Ionescu, D. Ionescu, O. Prostean, and G. Prostean, “An ontology based approach to intelligent data mining for environmental virtual warehouses of sensor data,” *IEEE Conference on Virtual Environments, Human-Computer Interfaces and Measurement Systems*, Istanbul, Turkey, 2008, pp.125-129.

[28] C. Valliyammai and S.T. Selvi, “Relational network monitoring system for grid performance optimization,” *Proc. of the sixteenth International Conference on Advanced Computing and Communications*, Chennai, India, 2008, pp. 170-173.

[29] WinPcap, The Windows Packet Capture Library, http://www.winpcap.org/.