建置整合式校園電腦教室網路管理系統

黃文聰
高苑科技大學
資訊管理系副教授兼電算中心主任
wtsung@cc.kyu.edu.tw

陳琮霖
高苑科技大學
資訊管理系
a794a1019@mail.kyu.edu.tw

莊美玲
高苑科技大學
資訊管理系
a794a122@mail.kyu.edu.tw

摘要

本研究將針對複雜的校園網路環境，整合目前各單位不同的管理方式，開發一套可以協助學校各單位管理電腦教室的網路管理系統，本研究所開發的系統將提供管理者對電腦教室來進行頻寬管理，系統可利用流量管理模組查詢個別或群體的特定時間的流量並加總後自動管制異常流量，系統管理員亦可以隨時監控目前各網路節點連線情況，該功能更可管理於電腦教室的設備編號、課程時段、及座位表，並利用個人化的電子郵件帳號作為登入時的網路身分辨識，有效的解決公用電腦使用時不易辨認確實身分的窘境，系統的維修管理功能也提供線上報修作業、維修知識庫建立、故障分析與維修進度查詢，網管人員更可利用備援管理透過本研究的整合平台來查看每天設定的排程備份狀態。

關鍵詞：網路管理系統、頻寬管理、網路身分辨識、維修管理。

Abstract

The purpose of this research is to integrate different management approach of each department for complicated network environment at campus, to develop a network management system which can help manage the network management system of each department's computer classroom. The system developed by this research will provide manager with broadband management for computer classroom. It can utilize flow management module to inquiry individual flow or grouping flow at specific time and can control abnormal flow after summing it up. The administrator of system can also monitor the connection status of each network node from time to time. Moreover, this function can combine the equipment numbering, classroom time, seat table and uses individualized email as network status identification while users' login. As a result, to effectively solve the problem of uneasy to identify accurate status when public computers were applied. The function of system maintenance management can supply with on-line maintenance reporting, the establishment of maintenance knowledgebase, analysis of malfunction and the inquiry of maintenance progress. The administrator of network can utilize backup management through the integrated platform of this research to check up the backup status of daily schedule。

Keyword：Network Management System、Broadband Management 、 Network Status Identification、Maintenance Management.

1. 前言

網路普及引導著全球化的資訊流通，也帶來快速傳播及便利，但伴隨而來的網路問題，如網路型電腦病毒及駭客的攻擊、垃圾郵件的困擾、資料被竊取的危險性等，使得各單位需加重網路管理的防範來應付以上隨之而來的問題。然而為了因應現今網路環境複雜所帶來的網路安全問題日益受到威脅的情況下，各單位所採用的網路設備、網管工具或安全防範機制也不盡相同，另一方面在網路的建置過程中，管理者面臨最大的挑戰，就是在管理眾多

網路設備及各類通訊協定上，都有它各自所屬的管理模式與提供的服務特性，使得網管人員必須有能力整合不同的網路設備並發揮該設備的最高使用效率[4][21]。

2. 文獻探討

本研究的文獻分析主要將探討網路流量管理、網路身份驗證、防火牆架設、入侵偵測、電子郵件整合、資料儲存與備援系統、網路管理的理論技術。沈榮華[13]指出為了確保網路系統的安全性，於脆弱的環節必須即時得知有入侵或攻擊行為，並有效予以修補與防治，才可以有效保證網路系統的安全。本研究中將探討網路管理者在網路管理監控時，對於內部網路系統不易偵測的漏洞，並研討相關的入侵者常運用的管道與方法，而在建置監測機制時做適當的修補與改進，提出用有效的監測與防範方式，以保障內部網路安全與重要伺服器資訊的安全。

2.1 網路流量偵測

網路流量監控的首要目標，就是要詳細了解頻寬的目前使用情形，以降低頻寬使用的建置與維護成本，而使整體企業頻寬能善加的使用[25]。流量監視為防範安全威脅提供了更多方法，如果沒有對該網路環境的流量的充分的理解，就不能對流量劃分此策略和防火牆政策有最佳的設定。當然，要提升網路的效能、降低網路壅塞程度，這都需要透過相關網路監控機制蒐集相關資訊，主動找出問題點並加以解決[8]。雖然網路流量可以利用簡易網路管理協定（Simple Network Management Protocol，SNMP）中的介面流量來搜集[19]，產做出像MRTG之流量圖表，但是無法偵測出單一主機的流量值[26]，亦無法提供出更完整更細微的數據來做判別。

蘇俊憲[34]指出，網路管理人員若能夠於第一時間內發現到有異常網路存取行為，並且通知管理者，系統透過分散式的網路設備做到即時阻擋的動作，也就不會讓更大量的網路異常行為持續發生，更進而導致網路重大異常情況，甚至癱瘓整個網路，適當的利用網路設備所提供的 NetFlow 與 sFlow 偵測網路異常行為的工具，監控網路上使用者或應用程式的情況，掌握目前所管轄網路的狀態，進一步藉此改善並提升網路設備的效能以及發揮最大效益，透過建立一個正常網路使用的流量基準，當發現網路活動明顯偏離基準時，就會發出警告資訊息，從而做到有效地識別破壞和入侵現象。另一方面，系統統計出來的紀錄與報表不因只用來監測單一使用者的網路使用行為，在細部化與標準化之後，一旦有資訊安全漏洞產生，在發生的當下立刻可以得知。

2.2 網路身份認證

在現今目前的網際網路環境中，IP 位址的盜用成為許多人頭痛的問題，其 IP 位址的盜用主要是為了逃避網際網路計費，或者是其他非正常目的使用而隱藏自身身分 [28]。為了能降低風險及防止駭客入侵系統所造成的衝擊與傷害，一個良好的網路控管系統是必要的[24]，像是身份認證系統（Authentication System），一方面可減低駭客攻擊，另一方面亦可有效的管理，以及適度的使用資源。唐可忠等[17]指出，就目前在各個校園中最常見的無線網路認證方式就是以 Web-based 網頁認證，以及少部分單位則採用 802.1xEAP-MD5、EAP-PEAP（Protected EAP）及 TTLS（Tunneled TLS Authentication Protocol）的認證方式，其網頁認證的方式大部份還是以帳號密碼 PAP（Password Authentication Protocol）來實現，使用者透過網頁式輸入帳號密碼來做身份驗證的依據，這可以支援許多種後端使用者帳號管理系統，像是輕量級目錄存取協定 LDAP（Lightweight Directory Access Protocol，LDAP）、網路存取資料庫帳號認証（SQL Server）伺服器等。

除此之外，在使用者帳號上的管理，隨著使用者數量的增加，許多相關的限制就會產生，如系統帳號數量最多只能建置 3~4 萬個。

LDAP 的做法，除可解決上述限制，同時透過集中且具安全性的使用者認證，針對不同使用者提供不同的使用存取權限[23]。LDAP 的協定模型，是在定義出 TCP/IP 的網路環境中，用戶端與伺服器間，一連串的服務要求與回應之訊息的交換過程[35]。

2.3 防火牆建置

防火牆的架設通常是於內部網路與外部網路間的出入口進行管理也較有效率性的。為了避免有問題的封包影響到主機的安全，以防止不法人事對資料的存取，以及防止病毒攻擊或是破壞方面，網路上所使用的防火牆乃是在兩個或兩個以上的網路設備之間隔出一條界線的電腦軟硬體裝置，防火牆是一雙向之安全理機制，能防止外來攻擊，亦能限制內部主機對外的通訊。不論是外部或內部的封包，經過防火牆設備時，都必須通過防火牆所設定的安全規則和政策的程序[33]。

架設防火牆主要是因為它提供了多種的安全機制，可以達到保護內部的作用。主要功能有以下三項：1.封包過濾 2.網路位置轉譯 3.存取服務或主機管理[1]：透過這些防火牆的安全機制，並利用網路位址轉譯（Network Address Transform，NAT）功能來達到防護的作用。保護主機與資料不被竄改、竊取與破壞。將主機隱藏在內部網路下，則會減少直接攻擊的可能性與禁止未經允許的封包進出內部，亦可保護內部主機的不受可疑封包的攻擊，達到內部網路的安全。而有效運用防火牆系統日誌提供之資訊，對防火牆系統日誌線上的分析功能之研究，可以減少對網路速度的影響，使防火牆系統具有攻擊偵測之能力，提昇防火牆系統安全性與稽核效能[32]。

2.4 入侵偵測之防護性

目前造成資訊安全危機的各種不同攻擊手段是更具自動化、快速、與多樣性，因此，在防禦這些攻擊的困難度也是與日俱增，通常入侵偵測系統還需要與防火牆、安全策略、網路弱點稽查[40]、權限稽核相結合，才能對整個網域做完整的保護措施。而大部份的入侵偵測系統都是以特徵模式（Signatures）來辨別是否為蓄意的入侵或有攻擊的意圖，在網路封包的分析上，也開始走向網路通訊協定的比對。

常見的網路型入侵偵測系統它是以監控網路封包為主；另外，主機型入侵偵測系統它是以監控系統紀錄檔來做判斷[27]。現行的主機型入侵偵測系統也有在特定的 port 上進行網路封包檢查，算是結合主機型與網路型入侵偵測系統功能的一種方式，而網路型與主機型相互結合也是入侵偵測系統發展的趨勢之一。本研究中就目前廣泛入侵偵測系統偵測方法，將各種偵測方法進行分析與探討其特質，分別有異常行為偵測、錯誤行為偵測、特徵比對偵測、異常通訊協定偵測。林鳳銘等[15]指出，在這幾年來主動性的入侵偵測系統，儼然成為重要的發展方向之一，透過入侵偵測了解網路攻擊行動，進而找出攻擊的特性，可以提供預防性的入侵防禦機制，同時結合資料探勘技術，提供更為完整的入侵偵測系統功能。

2.5 電子郵件安全

目前收件者常受到干擾的垃圾郵件，分別為病毒郵件與廣告郵件，病毒郵件是透過郵件夾帶方式夾帶會傷害電腦、盜取資料的有害程式，如木馬程式、後門程式等。廣告郵件只是強迫的推銷產品、色情媒體，或者是無寄信來源、無標題等假造的郵件[20]。然而，垃圾郵件會如此的氾濫帶來許多的困擾，是因為 E-mail 的傳輸協定簡易郵件傳輸協定（Simple Mail Transfer Protocol，SMTP）過於簡單，並未做好寄件者身分驗證的工作，加上免費的郵件地址取得容易與寄信的低成本產生垃圾郵件如此的嚴重[2]。

對於垃圾郵件的資安問題，目前大多採用過濾技術來進行阻絕垃圾郵件，目前主要的防制方法是利用過濾技術是分別在伺服器及用

戶端進行篩選[10]。伺服器（Server）端所需要的過濾（Filter）是儘早將系統辨認可能的垃圾郵件（Mail Spamming）阻擋下來。但有些情形必須在客戶端（Client）過濾，例如：每個人的白名單（White List）都不太一樣，比較難在伺服器（Server）端統一做個整體的白名單（White List）[3]。

2.6 資料儲存與備援系統

謝昆霖等[29]指出依據我國產業界的研究報告指出，如果資訊系統停擺一小時，會有 39%的公司發生核心活動全面停擺的危機，如果資訊系統停止 2 至 3 周，將會有 88%的企業將全面停擺無法運作，僅有 4%以下的公司還可以利用人工作業來維持公司的運作。當組織要保持運作不中斷以及維持資料的安全性、完整性，建立備援系統是有效的一個方式，擁有一個好的備援系統對組織來講是很重要的，因為它可縮短系統當機的時間，系統當機時間越短，組織損失的成本也就越少。

「保護資料，維持營運不中斷」已經是企業內部普遍的共識，由於現今災難頻傳，所以如有一套完整的資料儲存與備援計劃，再加上資產管理的相互配合，這將是各式各樣的企業都所會去採用的，這樣儲存裝置才能有效去執行它的功能[14]。而目前資料儲存的系統可分為：1.直接連接儲存（Direct Attached Storage，DAS）、2.網路連接儲存（Network Attached Storage，NAS）、3.儲存區域網路（Storage Area Networks，SAN）[16]。比較傳統的 DAS 備份目前已不敷使用，而現今 NAS 和 SAN 是比較有效的資料儲存系統，這兩種最主要的目地是減少管理上的複雜度以及提供更有效率的儲存媒體拓樸架構[18]。

而現今的資訊備援可分為三種類型：（1）、基本資料備援：定期使用磁帶或是光碟媒體備分企業資料，並且將備分媒體運往另一個安全的保管處，是低成本又簡單的一種備分方式，且建置技術門檻相當低。（2）遠端伺服器主機備援：使用遠端的儲存設備與寬頻網路，以同步或非同步的方式備分企業資料，是目前異地備援方式的主流。（3）專屬設備備援：是在另一個地點建置一個相同的主機系統、關鍵電腦周邊、操作系統與應用系統，就如同一個小型的分公司，並且採用同步的方式進行備分，技術門檻與撤除門檻都相當高[11]。

另一方面在主機維護此方面一直是系統管理者日常最重要之例行性資訊管理工作，然而，系統管理的複雜度、效率和所管理的範圍、主機數、主機型態都息息相關，因此，記錄檔(LOG)的概念被廣泛使用在系統管理上，透過 LOG 檔機制，主機系統運作之軌跡能夠被有效的記錄，也讓系統管理者　能夠循跡找出問題癥結，對於系統管理者而言，LOG 檔案的存在性是絕對必要[5]。

2.7 網路管理

蘇俊維[33]指出，網路管理上我們必須隨時注意網路架構與應用的變化及網路安全的管理方式與安全策略，也應該適時地調整並加強監控網路內部未經授權的服務與安全較薄弱的節點，必要時檢查與分析網路封包，找出異常的網路行為或攻擊，予以拒絕。並在使用者進行網路行為之前，先進行身分的認證，配合防火牆相關的網路設備等通訊記錄檔，有效的掌握著每位使用者的網路活動，以預防當發生網路異常時可以進行查看[22]。

網路管理的複雜度，主要的評估是以網路環境的範圍大小與設備種類多寡而定。然而，在現今網路環境中混合著諸多廠牌的網路設備，組成復雜的異質網路架構，要如何能有效地管理是一門深奧的學問。儘管如此，針對網路管理不同角度的銓釋也會有著不一樣的定義。例如網管人員而言，期望透過目標清晰的管理並監控其所有連接到網路的設備。就企業個體、工廠而言，重視著導入網管工具後所節省的資料與時間甚至停工時的耗損成本。就學校而言，是在現有的設備裏，必須有能力整合

網路設備並發揮網路頻寬最高使用效率[6][8]。

確保資訊之流通，網路管理人員均透過網路管理系統來管理及控制網路之正常運作，而網路管理系統的任務是提供網路管理者一個簡單、方便、快速的機制以監測與管理整個網路系統運作[31]。然而，對於目前各廠商所推出的管理系統必須透過特定的工作平台才能監控網路的情形，這對於一個網管人員而言限制了對網路異常處理的即時性。因此，網路管理系統應該能整合不同管理平台、網路系統與網路協定並具有一個標準介面就能監督與管理網路的各種狀況[21]。

李進興[12]指出，在組織中，若一開始未能規劃好完善健全的網管體制，或由於當時需求、成本等因素，使企業內同時擁有許多不同廠商的軟硬體設備並存著，而造成有兩個以上的網管系統同時進行管理，然而這些網管系統間卻無法溝通與合作。建置一整合的網路管理統合異質網路架構並可與其它網管系統溝通，將能提高網路資源的利用，還能維持管理資訊的一致性，更重要的是企業更新管理技術或增添設備時，舊有系統不致因無法相容遭到淘汰而造成浪費[9]。

3. 研究設計

3.1 研究架構

本研究將透過文獻探討的理論基礎，設計一整合性的網路管理平台，並針對目前校園網路環境所面臨的安全性（Security）、可靠性（Reliable Performance）、擴充性（Fiexibility）與連結性（Connectivity）予以考量，在系統開發過程中將與各單位的電腦教室管理員者做深入訪談，分析與探討目前網路環境的背景，也收集目前的管理資訊與技術資訊、探索實際的網路特性、找出使用者在網路使用上的安全行為與線上報修需求功能，於系統設計方面，本研究將著重在在實驗網路架構、系統功能、系統流程、資料庫結構與整合式管理平台操作介面設計之五個項目，並於系統的發展過程中利用網路程式語言建立五個主要系統功能模組與整合管理平台，導入後再依其功能的廣泛適用性進行效益分析比對其設計目標。

3.2 系統需求與探討

3.2.1 背景分析與探討

本研究的環境是以高苑科技大學電算中心所管理的 16 間電腦教室及資訊管理系的專業教室為實驗背景，並以使用這些教室的上課用電腦及師生為研究對象。由於本研究教室目前編排多門課程於不同的授課教師及授課學生在指定的時間內使用，而每位授課學生於課堂上使用網路進行的教學活動也不盡相同，時常會出現因學生不當的使用網路進行下載，導致教室內網路下載過量的情況，進而影響到校園的網路效能。該網路實驗教室主要是提供給資管系的師生於上課教學所使用，但除了依照課程所編排的時間來開放教室外，也規劃於課餘時間給學生進行自由上機練習。

在網路管理方面，雖然能夠透過學校目前的網路流量管理系統與 MRTG（Multi Router Traffic Grapher）得知各時段網路流量狀況，但卻無法正確的得知造成此問題的學生名單及使用的設備，只能透過張貼公告或口頭上警告方式來加以勸導，然而這樣的勸導方式卻無法達到來源落實追蹤的效果。

以下為主要的蒐集資訊：

1. 背景概況與現況：主要是針對電腦教室使用了哪些網路設備以及電腦教室位址(Internet Protocol，IP)的分配方式，接著調查電腦教室如何連結至校園網路而出網際網路（Internet）、以及目前電腦教室網路頻寬的使用情況、使用哪些通訊協定，還有管理電腦教室所使用的應用程式，最後當電腦教室發生問題，是如何獲得支援等主要的調查內容。

2. 網路流量分析：由於這些實驗教室主要是提供給教師教學及學生實習來使用，當使用者使用網路時會有封包在網路上進行互相傳遞之動作，而主要是透過流量收集、分析來了解目前網路流量使用狀況，當發生流量異常發生的情況，可以透過流量統計圖得知在哪一時段流量超額並將使用者使用情形加以記錄，透過 WEB 管理畫面能正確的查出哪一個使用者所使用的流量超額，進而針對該使用者提出警告的訊息。

3. 網路應用服務：
   - 郵件服務：目前資管系提供給該師生每人100MB容量是當教師課堂上於有重要訊息要告知與某班級或單位，可以像是群組轉寄方式將訊息傳送給一群組的收件者。
   - 檔案傳輸協定（File Transfer Protocol，FTP）服務：主要是提供給學生及教師一個資料上傳的存取空間，此外 FTP Server 裡的所有檔案目前已利用拷貝的方式做資料的備份，來防止資訊的遺失。
   - 教學廣播系統：該系統主要是提供給老師在教學上一種更方便的教學方式，透過教學廣播的應用程式可以讓所有的學生電腦進入到廣播的狀態，也能夠更清楚的看到老師所進行的操作步驟或是上課內容的進度。
   - 教學用應用程式：目前教室內的電腦設備皆會安裝較常使用的應用程式，像是文書處理軟體、繪圖軟體等等的應用程式，並會依照老師上課教材所需要使用到的應該程式進行安裝增加，來提供給老師上課時使用。
   - 校內學生資訊系統服務：該教室目前學生除了使用 Internet 瀏覽各網站外，學生亦常用即時通軟體，此外，學生亦於上課中使用「數位學院」、「學生網路學習平台」、「遠距教室」取得上課教材與繳交作業。

4. 使用者的安全考量：根據系統內使用者的管理機制，使用上的安全性大致上皆是以確認身份及權限分配為主要目的。將習實須利用網路連線資源的學生，皆須通過身份認證系統才可使用資源，並且使用權限管理方式可以有效控管學生的使用範圍。

5. 資料備份與備援：了解目前在管理電腦教室內提供同學儲存檔案或文件的磁碟空間，以及該教室內的相關伺服器的學生使用通訊記錄檔和系統的程式碼是如何進行備份，而備份的時程又如何規劃[30]。

6. 維修服務的管理需求：了解各間電腦教室內，當發生電腦損壞、故障時，通常都透過什麼樣的方式來通知管理者，以及在整個維修的時間上是否會因為不當的報修通知程序，而延遲維修時間，進而影響學生上課的權益。

3.2.2 需求分析

1. 收集管理資訊：系統將針對每台電腦上依序分配電腦編號、電腦位址（Internet Protocol，IP）、節點編號進行對應，不論是問題異常狀況或是維修還是在查詢主機資訊方面時，能夠較快速且明確的掌握目標位置。然而，當使用者啟動瀏覽器時，根據使用者所註冊的學生帳號密碼資料與系統上做身份辨認動作，並由其登入後所取得的權限來決定能夠允許使用的服務項目，系統也會將使用者的相關使用情況記錄下來，有利於事後查詢問題的方便性。

2. 收集技術資訊：本研究主要是蒐集教室內的網路環境概況、人員使用電腦之情形、電腦連線效能及目前該電腦教室的網路管理方式，透過訪談該實驗教室管理人員發現目前各網路節點的電腦不管透過有線或無線網路的連線，皆需透過帳號認證技術進行人員的認證並記錄使用者在網路上的使用情況。而為了整個網路環境架構中必須有安全上的防護，教室內部所被分配到的電腦 IP 將透過環境中所建置的防火牆設備利用網路位址轉譯（Network Address

Translation，NAT）的方式分配靜態虛擬 IP（Static Vitual IP），以防止內部設備暴露在網際網路下，當封包資訊在互相傳送時，經由入侵偵測系統的監控與收集，解讀封包是否含有攻擊或異常的行為，而降低危害到教室內電腦主機安全的徵兆，並再利用防火牆的過濾規則來做到阻擋的動作。

3. 探索網路特性：探索網路的特性，將所規劃的一個網路環境，當在正常運作模式下，評估網路所使用的狀況，可靠度是否穩定，評估是否會有問題產生，當使用者在使用應用程式時，是否會造成網路壅塞、負載過大、流量超額等等效能瓶頸，透過系統工具、通訊協定的方針，讓管理員比較有效了解網路的特性。

4. 使用上的安全分析：雖然網路帶給使用者相當多的便利性，不過也夾帶著大量不安全的因素，這種情況於校園環境下也是一樣，針對網路管理系統而言，提供眾多的不同服務與限制，不過將這個網路管理系統架設起來，運用在實際網路環境上，其實應考量幾項安全上的漏洞，作業系統、軟硬體設計、通訊協定、管理不當等等，由於這些的漏洞，造成有心人士入侵資訊系統，導致使用上的安全受到威脅，因此安全上的管理工作需要嚴謹的防範措施。

5. 維修管理需求：當網路發生異常現象時，例如像教室網路突然斷線、設備出現警訊、網路變慢壅塞等等問題時，造成提供給學生上課教學的應用服務無法使用，此時，如何能以最快速的時間，讓管理者得知，以最迅速時間的了解問題點，並進行處理而讓網路恢復正常運作，這時便必須運用到維修管理，提供使用者填寫報修單，詳細描述發生原因的情形，讓管理員查詢到時，能清楚判斷問題可能發生的地方，而以最快速前來處理。

6. 找出網路特性步驟[38]：主要的目的是為了解使用中的應用程式、衡量網路的效能、網路的可靠性、通訊協定、運用到的網路工具、設備狀態..等等網路特性上的分析，給予符合使用者需求最好的方案。

3.3 系統分析與設計

經由以上的需求分析後，本研究進行以下幾項重要規劃重點進行考量：

- 使用者在使用網路實驗教室前，需進行身分辨認以及紀錄使用者的使用行為。
- 針對使用者登入的身份，提供所擁有的權限及允許使用的相關服務。
- 能立即的掌握整個網路教室的頻寬使用情況及流量分析狀態。
- 當網路實驗教室設備產生異常狀況，能迅速得知所發生的原因而進行處理。
- 將學校（系）所提供的郵件服務，能方便跟網路管理系統帳號同步使用。
- 針對網路實驗教室內使用者的重要檔案以及電子文件檔進行定期的備份工作。
- 提供使用者線上的報修功能，讓管理者能夠快速的得知教室設備損壞或異常的資訊，並進行維護工作。

本研究所考量的資料來源計有：個人電腦、伺服器、資料庫、應用系統、電子郵件，網路建構的目標將整合：組態管理（Configuration Management）、錯誤管理（Fault Management）、效能管理（Performance Management）、安全管理（Security Management）、帳號管理（Accounting Management），而本研究依訪談結果歸納以下各點以滿足目前電腦教室管理者之需求：網路流量分析、網路異常行為分析、網路節點管理、身分辨認與權限、郵件服務管理的平台設計，並針對目前實體網路環境提出具有擴充性（Flexibility）、可靠性（Reliable Performance）、安全性（Security）、連結性（Connectivity）的發展架構，系統整體發展架構設計(如圖 1)所示。

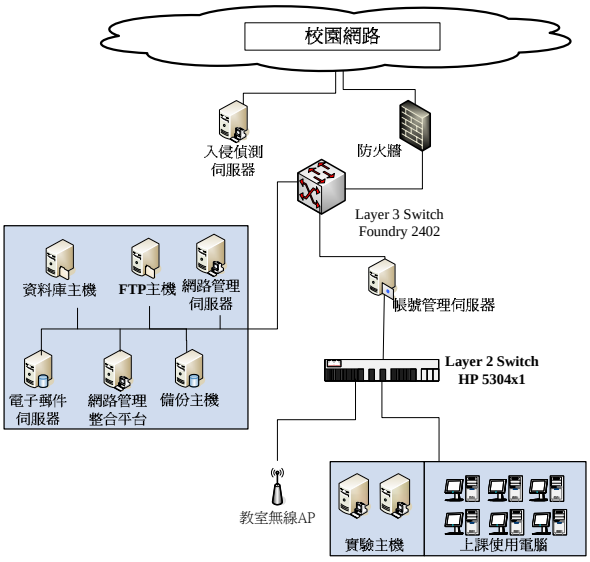

圖 1: 整合式網路管理架構圖

3.3.1 系統功能設計

本研究所規劃出來的整合式管理平台，主要的功能項目分別為：「網路流量管理」、「節點管理」、「帳號管理」、「維修管理」、「備援管理」。在「網路流量管理」方面，主要是提供管理者來了進行頻寬管理，系統可查詢目前及過去的流量記錄，也可以限定個別或整體的總流量並對違規事件進行管理；在「網路節點管理」方面，則是可以監控目前網路架構環境中各管理的網路節點連線情況，該功能更可整合於電腦教室的設備編號及座位表；另一方面，「帳號管理」主要是針對身份辨認、帳號資訊、課程作業、群組管理、郵件帳號整合、郵件管理以及權限管理等項目功能；再者，「維修管理」功能則是提供資訊化的報修作業，管理階層可以透過這個功能來進行網路維修工作的分配或是線上填寫維修記錄；最後，「備援管理」功能則是提供管理者可以方便去了解目前環境中資料的備份情況以及備份下來的記錄資料。

1. 流量管理：系統實施整體網路頻寬監控主要是收集核心交換機（Foundry 2402）及帳號管理伺服器之網路流量，以 sFlow 封包為收集基礎之流量監控[44]，分析網路封包，依實施監控條件、監控的地點、以封包訊務量特徵的辨識方式及異常的連線活動等來監控整體網路頻寬運作情形[網]，再加以蒐集相關數據與資訊，確認或制止可疑的入侵與攻擊行為，以維護管理單位網路傳輸品質或他人使用權利，本研究將設計以下四個模組來進行：

● 流量蒐集模組（Flow Collector Module）：收集 sFlow[41] [42] [43]流量資料之設備（Router 有支援 sFlow 監控模組之網路設備），並將 sFlow Agent 收集之流量資料（Flow Records）傳送至流量資料庫(如圖 2)。此外，根據設定，將 sFlow Agent 所取得的原始資料（Raw Data）儲存，以方便日後追蹤及回溯分析。

```
startDatagram =================================
datagramSourceIP 192.168.9.11
datagramSize 132
unixSecondsUTC 1166856071
datagramVersion 2
agent 192.168.9.11
packetSequenceNo 72177
sysUpTime 360144900
samplesInPacket 1
startSample ----------------------
sampleType_tag 0:2
sampleType COUNTERSSAMPLE
sampleSequenceNo 1224
sourceId 0:9
statsSamplingInterval 300
counterBlockVersion 1
ifIndex 9
networkType 62
ifSpeed 100000000
ifDirection 1
ifStatus 3
ifInOctets 198389901
ifInUcastPkts 1649336
ifInMulticastPkts 273
ifInBroadcastPkts 22829
ifInDiscards 0
ifInErrors 261
ifInUnknownProtos 0
ifOutOctets 3816494118
ifOutUcastPkts 3272648
ifOutMulticastPkts 19468
ifOutBroadcastPkts 133492
ifOutDiscards 0
ifOutErrors 0
ifPromiscuousMode 1
endSample   ----------------------
endDatagram   =================================
```

圖 2: 流量蒐集

● 流量分析模組（Flow Analyzer Module）此模組主要針對流量蒐集模組 Flow Collector Module 傳送過來之 Flow 資料作運算與分析，使用者可再透過流量監測模組 Flow Monitor Module 所提供之 Web 介面去傳送欲監控之節點、區域，依據所設定之條件過濾 sFlow Agent 輸出之流量資料，將符合監控條件（Filter）流量資料作分類與統計，並將分析結果存入流量資料庫中(如圖 3)。

圖 3: 流量分析

● 流量監測模組（Flow Monitor Module）:從資料庫裡讀取監控條件(Filter)之即時流量圖、流量查詢等，本研究利用 PHP 程式撰寫，透過網頁介面提供使用者一個標準化 Web 型式之系統存取操作界面，以執行監控及查詢之動作。透過此監測模組，使用者可隨時隨地透過網頁瀏覽器登入系統，並可自行定義流量資料的管理條件與監控範圍， 連結流量管理主機至流量資料庫擷取倉儲資料，並產生即時性之 HTML 網頁做流量歷史查詢及即時流量圖表(如圖 4)。

圖 4: 流量監測

● 異常事件管理模組：本研究透過以流量統計資訊、入侵偵測系統（CA e-Trust）事件、資訊與系統環境弱點，建立入侵偵測事件的分析機制[7]，以提高偵測準確度與降低誤判率，並應用於實際的網路環境中收集網路存取資訊(如圖 5)。

圖 5: 異常事件管理

2. 節點管理：利用節點查看的方式，儘速的得知學生於網路實驗教室中的使用情形，以及了解網路實驗教室內其網路設備的運作，來查看是否有發生異常或是停止運作的狀況，以便能夠保持教室內網路持續連線的功能[12]。除此之外，為了往後能方便的管理電腦教室，在節點管理的部份中，首先紀錄節點的相關資訊，並找出該節點所對應到的設備或是主機的相關資料，方便在往後的資料查看上，可以快速得知節點的資訊。而對於學生進入教室所使用的設備，也會針對學生使用主機所進行的網路行為來加以記錄。除了可以提供往後問題發生可以有一個查詢的依據，也可以利用這些記錄來了解學生的使用情況，並且加以規範。然而，也配合系上所規劃出來的課程，依照課程的使用時間與學生的使用記錄來進行核對，提供各個節點更多的資料，在往後的查詢上便能夠更清楚的了解節點的使用資訊(如圖 6)。

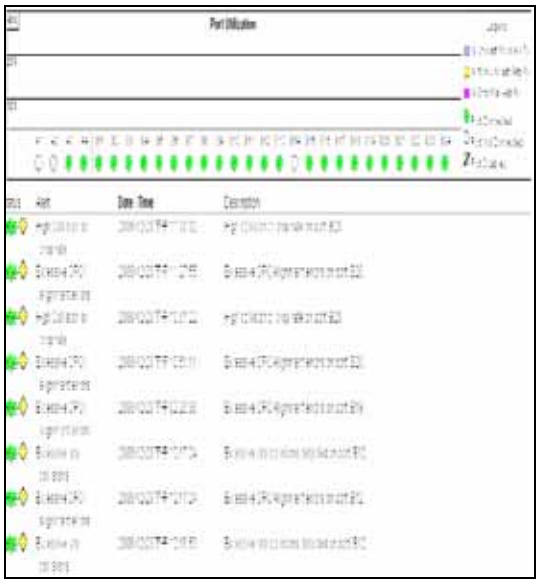

圖 6: 節點管理

3. 帳號管理：首先我們先規劃使用者的帳號資料以進行身分辨認的設計，並建立功能項目來維護使用者的帳號資訊。接著，設計其課程作業，與教室內所修之課程可相互呼應並根據使用者帳號規劃其群組，將使用者歸類於所修之課程群組中。再者將使用者帳號與郵件帳號以及網管系統結合以達成帳號同步機制，並針對使用者的信箱容量來加以控管。最後針對帳號權限的等級加以設置，以搭配環境的需求來達到管理效能的提升[37]。以下幾點為帳號管理的七項主要功能設計：

- 身份辨認：

當使用者透過瀏覽器提出驗證請求時，系統即會提供 Web 登入畫面要求使用者輸入合法帳號及密碼做驗證程序（如圖 17）。而 Server 端資料比對正確後，會回應給 Client 端驗證通過的畫面。

- 帳號資訊：

在帳號新增功能設計上，我們考慮到使用者帳號必須經由管理者來建立於 Account Server 中，以確保資料安全及重複性，因此，我們設計當使用者提出註冊申請時，所註冊的 Session 會暫存於資料庫中以待管理者核准建立新增。而在帳號的刪除功能方面，則是提供管理者針對使用者未來該帳號已停用或該帳號資料錯誤必須撤銷使用者帳號而設計。另外，帳號的修改功能則是當使用者或管理者在帳號資料上有資料須更正或錯誤時，提供給予使用者及管理者做帳號資料的修改與維護。

- 課程作業：

課程作業主要就是針對電腦教室編排之課表而設計的，在此方面的設計上，我們是以資料庫來建置其課程資料，將各個不同於該電腦教室內課程的使用時間以及該課程教師編輯於系統內成為一個群組，管理者是以鍵入的方式將課程資料鍵入系統中，接著再將其課程對應各個不同資料庫。

- 群組管理：

群組的規劃是以一個課程為一群組，將使用者所選修之不同課程使用不同之權限等級。且於電腦教室內，相同使用者帳號，但選修不同時間之課程的問題，使之無法掌握該帳號所使用之電腦編號亦可由群組的管理來劃分其規範。

- 郵件帳號同步：

當該帳號與 Account Server 通過驗證之後會帶出所輸入的驗證值，並與 Mail Server 該帳號驗證，然後提取該帳號的郵件檔案，並呈現於郵件服務平台上，來達成整個網管系統帳號的同步效率，無須在登入網管系統之後，並在輸入個別帳號資料再驗證一次，使得管理者能集中式的帳號管理並且也讓使用者能方便的使用服務。

- 郵件容量管理：

郵件容量管理，主要是將郵件容量分配給學生與教職員使用，當使用者使用郵件容量到達限制額度時，這些使用者將會被列為容量超額，網管平台將會把這些超額的使用者帳號、使用量、寬限時間等等詳細資訊呈現於 Web 平台上，以供管理者提出警告或告知處理。

- 權限管理：

權限的管理是針對不同的使用者來區分其何種服務可使用，經由所驗證之欄位根據 Server 端的帳號資料做比對並判斷出該使用者於網管平台所使用的權限，根據資料庫比對之結果，將該帳號所屬之職位及所設置之權限一併取出可使用之資源，並顯示呈現於使用者頁面上。

4. 維修管理：主要是提供使用者報修功能可直接上網填寫維修單提出故障報修記錄，管理人員可以即得知節點故障情況可做即時的處理；為了讓維修人員有效率的來達到維修管理的目的，可善用行動裝置的便利性搭配無線網路，維修人員可藉由維修管理網站來得知當日的維修行程，所以提供派工作業的管理，讓管理人員在維修人員、區域和維修單管理等做適當的排程設定，以方便管理維修排程的進度；網管人員將維修時常碰到維修的相關資訊蒐集並儲存至維修資訊，以方便當維修人員遇到無法處理的情形時，可查看維修資訊，來做適當的維修處理動作，並且將維修情況做記錄，讓網管人員可依照維修記錄情形做適當的故障管理，並將維修單記錄做為統計報表的輸出、和歷史記錄的查詢(如圖7)。

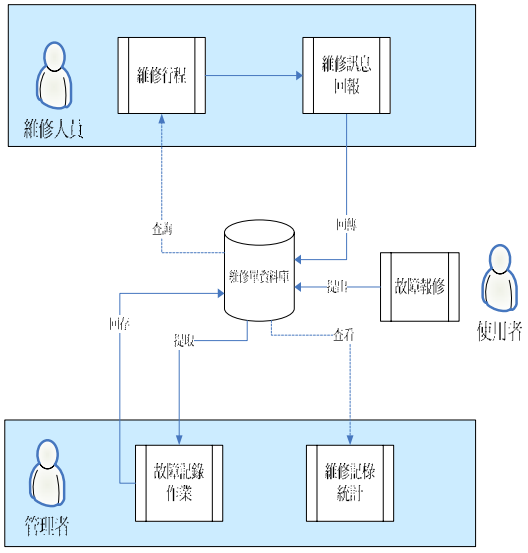

圖 7: 維修管理

5. 備援管理：本研究的備份作業可分為應用層面（Application Layer）、設備層面（Equipment Layer）、管理層面（Management Layer）三部份，主要是針對使用者登入紀錄檔與系統主機檔案、使用者文件檔等，經由備份的流程導向進行規劃。

- 應用層面：由於校園裡的各個電腦教室使用率頻繁，因此本研究的備份服務主要是針對電腦教室裡使用的電腦主機作業系統做備份動作。
- 設備層面：主要是利用排程去備份這些於設備或伺服器上的暫存檔案，以本研究目前主要備份的主機如下：流量監控伺服器、郵件服務伺服器、帳號伺服器、FTP伺服器。
- 管理層面：備份主機在做完任何運作後，都會將運作的結果紀錄儲存到資料庫中，此記錄都是詳細說明備份的結果是否成功，而此資料庫中的資料可供管理者調閱，因此內容可判斷備份主機是否有按照設定來動作。

3.3.2 系統流程設計

本研究所建置的整合式網路管理平台作業流程，主要分為前端的驗證作業與後端的管理作業。在前端的驗證作業上，是當使用者或管理者要使用網路資源或網路管理平台時，皆必須先經由登入畫面來輸入所申請的帳號密碼[36]，而系統會將輸入的帳號密碼與 Account Server 做身分驗證比對，並在比對完後將驗證結果回傳，告知使用者是否驗證成功。驗證失敗則返回登入畫面，成功則透過該使用者的權限來分配所使用的平台功能服務。若使用者還未取得帳號資料時，可以透過註冊程序，來取得屬於使用者個人的帳號資料並做登入動作。

另外，本研究所提供的各項管理服務的作業能呈現於平台上，使用者經由驗證比對後判定是否進入網路管理平台提供五大項管理服務，而各項管理服務的作業皆是經由網管資料

庫來存取網路管理系統的數據及使用行為，並透過網路設備所支援的 SNMP Agent，即時收集網路設備上的詳細資訊，以及傳回資料庫儲存，並呈現於網管平台供使用者查詢以及管理者來維護的結果。然而，使用者使用時，發現設備出現異常或損壞，可經由線上填寫報修單，讓維修人員得知前來維護與管理(如圖 8)。

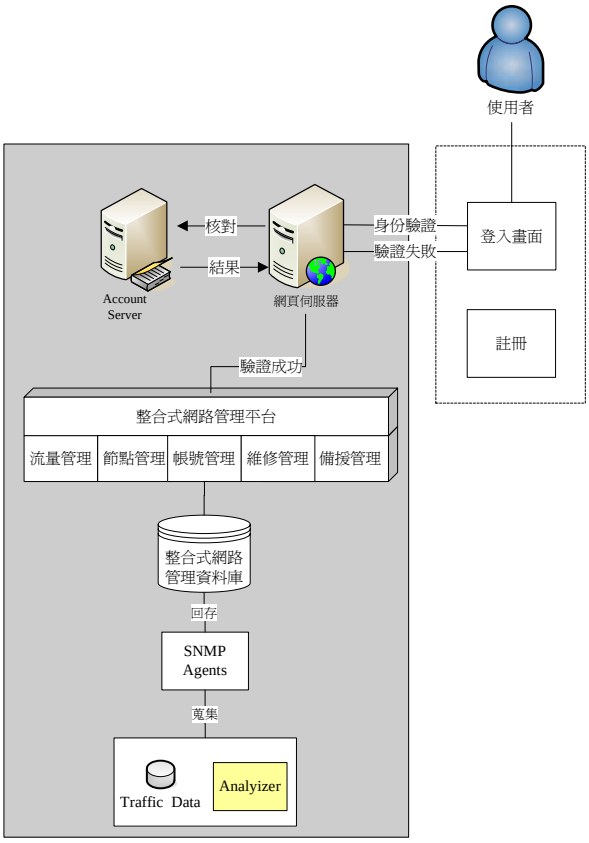

圖 8: 整合式網路管理系統作業流程圖

4. 系統實作

為了維持管理網路之正常運作，藉由網管系統所收集、分析到的監控數據就是規劃的重要參考。本研究利用流量分析系統來監視、監測、控制、管理及維護網路的正常運作，並針對流量異常使用者進行行為分析，即時對於使用者的不當使用或異常使用進行管制，經由資產管理監控重要網路設備，並且可以掌控公司內部所有軟體資產的狀況，提供資產查詢及異動等功能，減少人力時間的成本耗費，提升資產評估的效益及可靠性，增加管理上的彈性。網路管理不只是要維護運作，最重要的也要考慮到在發生人為或天然災害時，能夠在最短時間內使服務重新啟動，本研究的實驗平台設計配合異地備份的功能隨時掌握備份完整性，使得資料保存更有保障。

整合式校園電腦教室網路管理系統的設計，考量了校園網路環境中所發生的種種網路相關問題以及環境需求，根據各個電腦教室環境的不同性質，本研究設計使用以 Web 為介面來提供一般使用者的前端網路流量查詢、維修申請、進度查詢，另外，可提供電腦教室管理員的流量管理、節點管理、維修管理，系統管理員的帳號管理、備援管理、組態設定、基本資料維護、網路設備監控（如圖 9）。

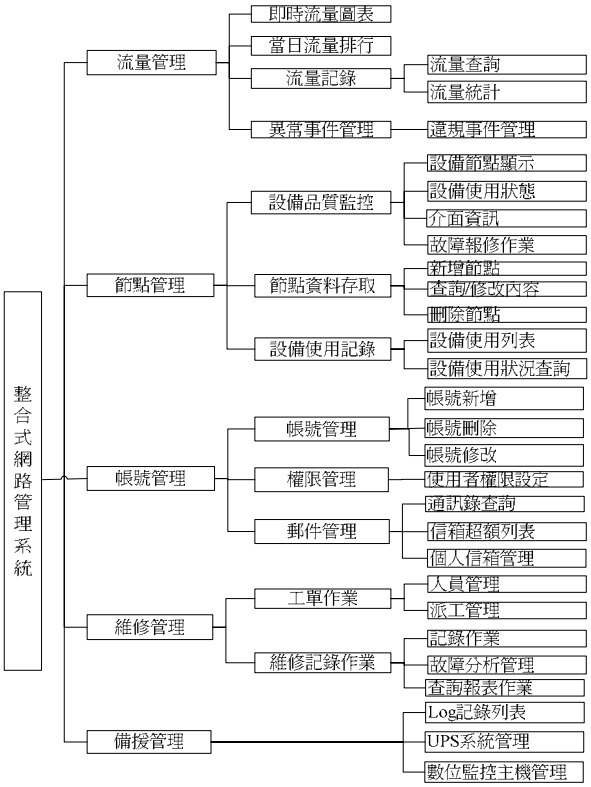

圖 9: 整合式網路管理系統架構圖

4.1 流量管理

本研究在實行流量蒐集時將網路流量狀況資料存在資料庫中，待資料累積了一段時間後，儲存數據，流量管理系統就可以將這些資料取出來分析與監控（如圖 10），並可找出有問題的網路節點並加以改善。本研究使用

Foundry 2402（支援 sFlow）來監控核心層頻寬使用量及網路活動，而改善這些問題的方法可以透過一些常見的網管協定來完成，目前本研究實驗的電腦教室其網路設備都具支援簡易 SNMP 協定，也正因 SNMP 網管協定的廣泛使用，只要網管設備能夠啟動及設定好網管的協定，再藉由網管的使用者透過 PHP 網頁傳遞控管訊息給流量管理伺服器，再由 SNMP 網管協定來初始管理資訊庫（Management Information Base，MIB） [39]，以便能精確的符合網管人員的所需，達到正確又即時的效果。


即時流量圖表 | 當日流量排行 | 流量查詢 | 流量統計 | 事件管理

資401 資402

當日統計時間			2006-12-03 從00時00分至目前14時43分		
ip	in(Kbyte)	out(Kbyte)	total(Kbyte)	total(%)	MBbyte
192.168.1.254	218542.21	125243.39	343785.60	18.36%	335.73
192.168.1.25	4155.36	86065.30	90220.66	4.82%	88.11
192.168.1.20	6390.23	79609.37	85999.61	4.59%	83.98
192.168.1.15	3608.04	78772.40	82380.44	4.40%	80.45
192.168.1.31	5362.07	76974.78	82336.85	4.40%	80.41
192.168.1.16	4343.66	72901.49	77245.15	4.12%	75.43
192.168.1.14	3665.02	73456.98	77122.00	4.12%	75.31
192.168.1.30	5002.53	71674.09	76676.62	4.09%	74.88
192.168.1.35	2148.99	71817.33	73966.32	3.95%	72.23
192.168.1.26	2680.12	70439.83	73119.95	3.90%	71.41
192.168.1.27	2157.42	69655.09	71812.52	3.83%	70.13
192.168.1.33	1769.19	69414.27	71183.46	3.80%	69.52
192.168.1.34	3247.49	67554.90	70802.39	3.78%	69.14
192.168.1.19	2578.87	67154.98	69733.85	3.72%	68.10
192.168.1.2	532.73	66631.73	67164.46	3.59%	65.59
192.168.1.22	0.00	64822.36	64822.36	3.46%	63.30
192.168.1.13	0.00	64804.58	64804.58	3.46%	63.29
192.168.1.28	0.00	64050.34	64050.34	3.42%	62.55

圖 10: 流量統計

另外，在進行流量分析與流量監控方面，本研究設計上將整合應用流量管理層面，運用 sFlow 監控核心層網路頻寬及網路活動外，在管理區域方面，只要支援 SNMP 協定的網路設備，就能利用本系統查詢網路流量、網際控制訊息協定（Internet Control Message Protocol，ICMP）等。把即時流量統計、當日統計、過量封包統計、異常網路事件等功能整合在一起（如圖 11）。使用者進入本系統前，必須輸入使用帳號及密碼，以確保資料的保密性，在身份確認後，進入流量管理查詢畫面，使用者選擇查詢管理區域、單位，即從流量資料庫中調閱相關數據，以供使用者於整合平台上即時瀏覽，並做進一步管理決策。

圖 11: 流量分析與監控

4.2 節點管理

本研究的節點管理功能設計將透過利用目前有支援 SNMP 通訊協定的網路設備，來擷取於環境中網路設備的 MIB 數值資料[12] [20]，當網路設備處於正常使用的狀態下，即可透過 SNMP 協定即可抓取到該設備中節點所對應到埠號的 MIB 數值，依照這種原理來進行查詢的話，若想要即時得知網路的節點狀況時，可以利用抓取網路設備中各個埠號的 MIB 數值，而得知其節點的連線狀態，並將所抓取到的結果呈現於 Web 平台上（如圖 12）。

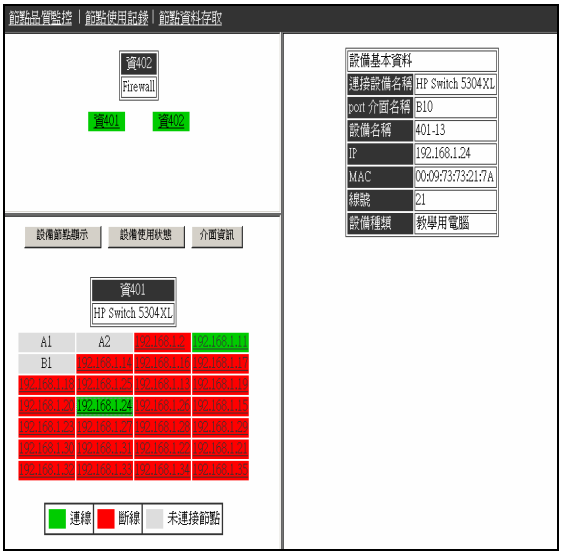

圖 12: 即時節點狀況

另外，當環境中有增加新的設備或是主機時，本系統可以利用新增節點功能來查看，或是節點所顯示的資料有作變動時可以進行節點資訊的修改等等功能。在進行異動的畫面時，必需先使用帳號來進行身份的辨認，並以管理者身份來進行修改，針對 Web 平台上所提供的節點資訊來進行增加、修改、刪除的動作，執行完相關的修改動作之後，將資訊儲存於節點資料庫內，再依照系統的編排方式，透過 Web 平台將結果呈現出來（如圖 13）。

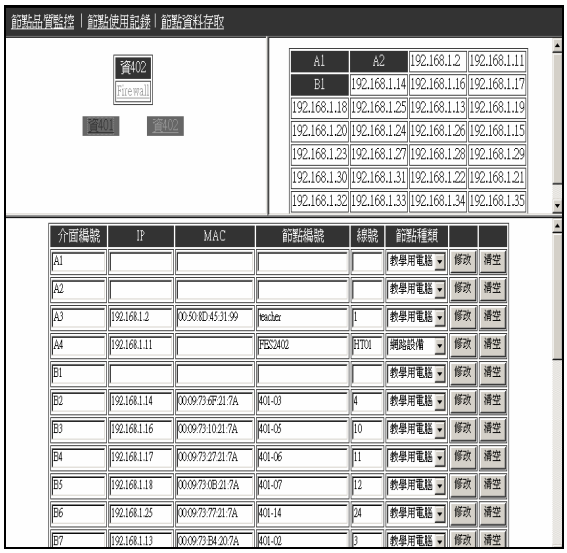

圖 13: 網路節點存取管理

另一方面，由於教室內的電腦學生須依規定登入個人的帳號方可使用網路，目的是將學生於該時段使用電腦所進行的網路行為記錄於系統中，以方便於日後查證。當管理者提出使用狀態的查詢時，系統會進入節點資料庫內先抓取查詢的相關資料，並查看使用者資料庫內是否有相關對應的資料，將所擷取到的資料進行排列，在透過網頁的方式將結果呈現出來（如圖 14）。

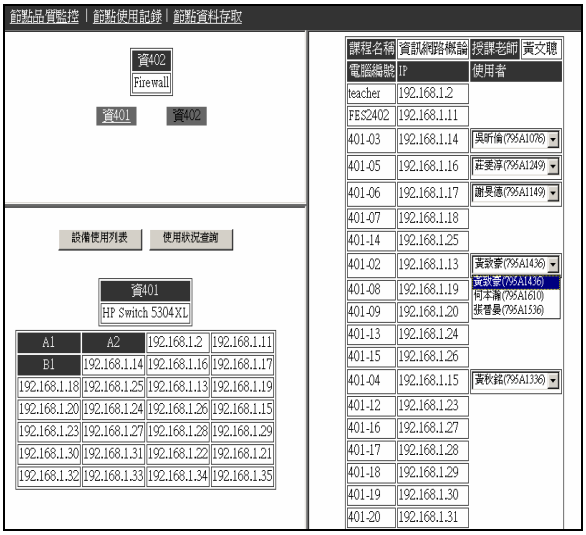

圖 14: 節點使用狀態查詢

4.3 帳號管理

當使用者使用電腦教室內的電腦開啟瀏覽器，網管系統即會自動將首頁引導至帳號認證頁面，要求使用者輸入帳號及密碼，系統會透過驗證程式與 Account Server 進行身分驗證程序，並在比對帳號資料的同時，也透過同步程式取得該帳號所屬的個人郵件檔案以及所屬權限[36]。驗證完畢後，系統會回傳驗證結果是否成功，失敗則會重新導入登入頁面要求使用者重新輸入帳號資料，成功則會開通網路服務並依驗證結果來辨認是一般使用者或系統管理者以及產生該使用者的相關 Session，依據所產生的相關 Session 辨認，系統便會得知是哪位使用者目前正在使用網路環境，若辨認出權限為一般使用者，則系統會對該使用者加以記錄使用行為，並提供該使用者的個人化網路資源。例如：郵件服務、線上報修服務..等等(如圖 15)。如權限為管理者則產生管理系統上的相關服務，例如：節點管理、流量查看、維修查詢、資料備份..等等。依照不同的使用者區分不同的使用權限，以達到帳號整合之管理方針。

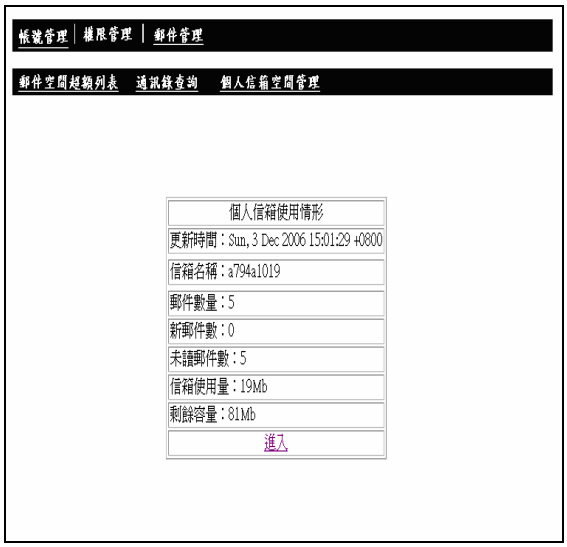

圖 15: 帳號管理

4.4 維修管理

當使用者的電腦設備發生異常狀態或故障情形時，使用者可藉由其他台電腦連上本系統進行報修申請(如圖 16)，系統首先會要求進行身份驗證的程序，驗證成功後即可上網填寫維修單和故障狀況，管理人員於後端可透過 Web 得知各電腦教室節點故障情形。

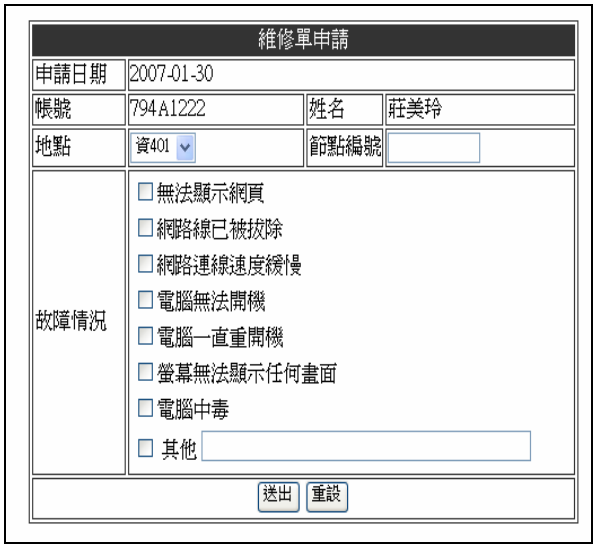

圖 16: 報修申請

維修人員可得知自己所負責的工作區域和當天維修的行程，讓維修人員可立即得知當天所須維修的節點狀況，並將維修狀況記錄回傳，讓網管人員得知現場維修狀態。另外，派工人員可以設定維修人員所負責的維修地點指定，主要是為了讓維修人員能在經由認證成功後，點選維修行程後，而顯示該負責區域的維修工單記錄，如果有遇到特殊狀況或需指定維修人員進行維護，也可依維修工單來指定特定的維修人員（如圖 17）。

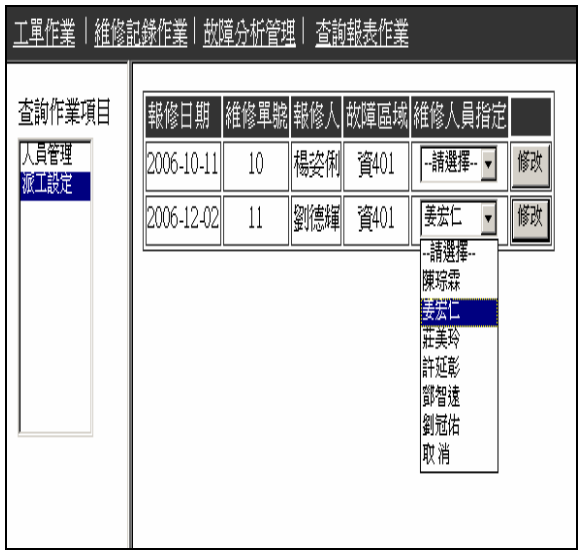

圖 17: 派工作業

最後，維修人員在執行維修工作後，必須依實際的維修處理過程線上記錄於網站上。系統將維修時所遇到的狀況處理蒐集並將整理出維修的相關資訊，以方便在維修中遇到瓶頸時可隨時查看（如圖 18）。

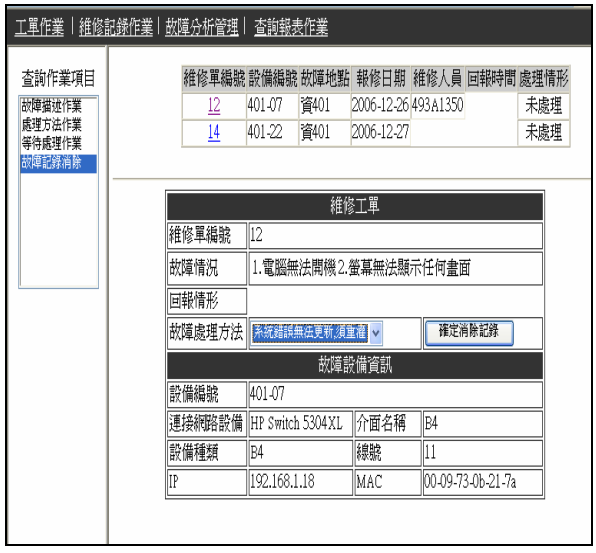

圖 18: 維修記錄存取

4.5 備援管理

本研究中，備份主機是透過備份軟體來實施備份動作，因此會在各設備主機裡安裝備份軟體的代理程式，而在機房將使用一台備份主

機，另一台備援主機則是放在另一棟大樓的相似機房內，並隨時與機房裡的備份主機做資料的同步動作。另外，機房中與放置備援主機的地方也都安裝數位監控系統來監視機房的安全。在各設備的 LOG Server，它是等待備份主機排定的排程來做備份的動作，並且備援主機會自動去探尋備份主機是否有正常動作，而所有動作都是由備份主機去備份所有的電子文件與 LOG 紀錄，備援主機再去備份主機裡備份它所有的檔案，但是當備份主機已超過預定的排程後，仍無備份的動作，此時備援主機將會自動接手備份主機的工作，以維持檔案備份的不中斷性(如圖 19)。

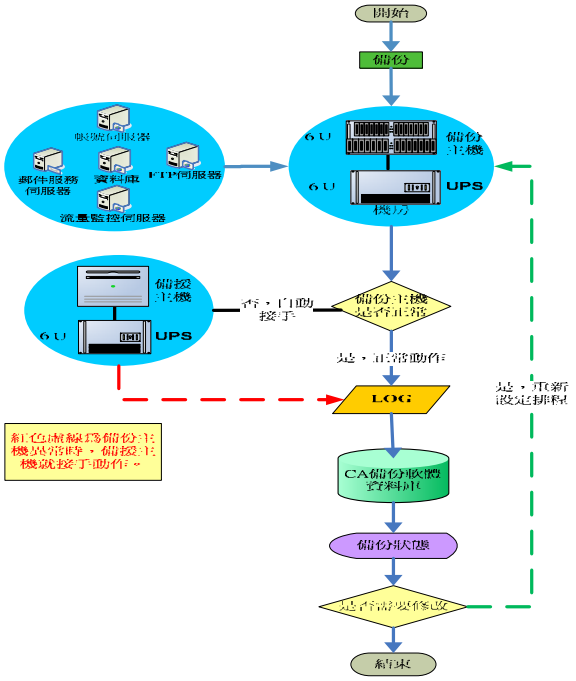

圖 19: 本系統的整體備援管理流程

最後，備份主機在完成相關作業後，會將所有備份動作的 LOG 檔傳送到備份軟體的資料庫中，而網管人員可透過本研究的整合平台來查看每天設定的排程備份狀態，整體備援管理流程(如圖 20)。

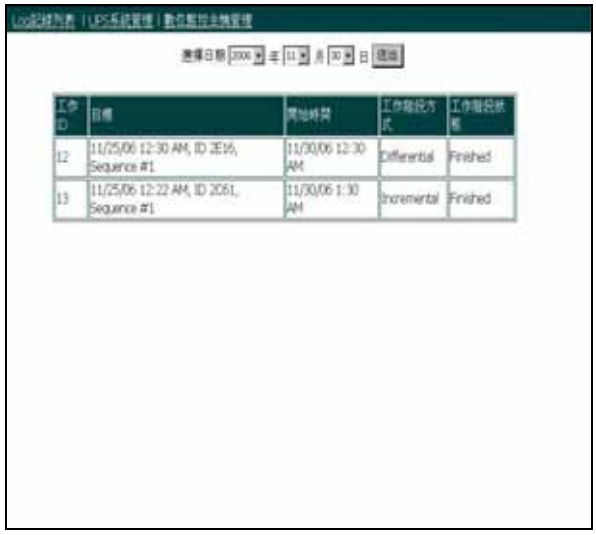

圖 20: Log 記錄列表

5. 系統評估

經由系統建置完成，並導入電腦教室進行實際的初步測試後，系統已能實際應用於電腦教室的管理上，相關設計的應用功能也都能一一的進行操作管理，而本研究建置的系統於目前已有以下幾點成果：

- 記錄學生於教室內使用之相關網路記錄，系統已整合各電腦教室地點、上課課程、課程時段、修課學生名單、座位表與連線紀錄。
- 可即時查看各教室節點，掌握住教室裡各台電腦連線狀況與頻寬管理。
- 系統提供使用者的身份辨認及權限管理，並與郵件信箱身份認證同步化。
- 利用自由軟體開發本系統，並藉由方便的 Web 介面來進行管理與登入，可降低網路管理系統開發的建置成本。
- 固定進行資料備份的排程，以防電腦教室內的電腦及伺服器發生故障後資料的遺失。
- 資訊化的維修管理可提升維修的速度並累積相關資訊建立一套網路維修知識庫。

本研究目前以高苑科技大學電算中心所管理的電腦教室與資管系專業教室為系統導入對象，目前以提升校園資訊安全與電腦教室管理的方便性。

6. 結論

校園內的電腦教室如此的眾多，而通常都是一位設備管理人員或工讀生需管理數間電腦教室，在服務的考量上除大量加人力來加強外，其維修效率及連線品質都是無法滿足目前師生上課中電腦設備與網路零故障的目標。有鑑於此，本研究設計的整合網路管理系統，系統將適用於各大學、中大型企業規模、工廠環境，並可監控與管理不同廠牌的網管型網路設備，在網路發生異常時能即時的追蹤並發現問題來源所在進而加以修復，以維持網路運作的通暢。

參考文獻

[1] 王士豪，"基於網路訊務動態基線分析之網路蠕蟲偵測機制"，***暨南國際大學資訊管理學系碩士論文***，2004。

[2] 王正豪，"向垃圾郵件說不"，***HOPENET 科技月刊***，第 103 期，pp 66-71，2004。

[3] 王正豪，"垃圾郵件攻防戰-SPAM 防治技術剖析"，***HOPENET 科技月刊***，第 93 期，pp 62-69，2004。

[4] 王佳瑞，"行動代理者應用於網路管理之研究"，***成功大學工程科學系碩士論文***，2000。

[5] 古東明、陳弘傑、沈志昌，"具電腦鑑識特性之即時遠端 LOG 蒐集監測機制"，***2006 台灣網際網路研討會論文集***，2006。

[6] 江國位，"高等校園網路應用與整合模式之研究--以大葉大學為例"，***大葉大學資訊管理學系碩士論文***，2003。

[7] 吳文政，"入侵偵測系統攻擊徵兆 MIB 設計"，***中華大學資訊工程學系碩士論文***，2003。

[8] 吳振豪，"企業網路之錯誤管理與效能分析實證研究"，***明志技術學院工程管理研究所碩士論文***，2004。

[9] 巫國吏，"下一代整合網路管理平台之研製"，***交通大學資訊工程研究所碩士論文***，2000。

[10] 李先育，"垃圾郵件防治篩選之研究"，***中國文化大學資訊管理研究所碩士論文***，2004。

[11] 李俊隆，"論災難備援計劃在資訊安全的重要性－以美商 CTS Corporation 為例"，***中山大學資訊管理學系碩士在職專班碩士論文***，2003。

[12] 李進興作，追求速效網路管理方法，***網路資訊雜誌***，第 163 期，pp 10-113，2005。

[13] 沈榮華，"網路犯罪相關問題之研究"，***國防管理學院法律研究所碩士論文***，2003。

[14] 林俊銘，"從企業資訊安全論備援系統的計劃與實務"，***中山大學管理學院國際管理研究所碩士論文***，2001。

[15] 林鳳銘、吳守豪、李蔡彥，"Intrusion Detection: a Network View"，***2001 網際網路研討會論文集***，2001。

[16] 林聖雄、黃文祥、王俊堯、魏守仁，"具 iICMPv6 管理技術的 iSCSI 儲存網路代理器之研製"，***2004 台灣網際網路研討會論文發表論文集***，2004。

[17] 唐可忠、黃偉航、蔡志宏，"校園無線漫遊認證機制安全與 802.1x PEAP/TTLS 環境建置"，***2006 台灣網際網路研討會論文集***，2006。

[18] 徐志明，"網路儲存系統之管理"，***中興大學資訊科學研究所碩士論文***，2001。

[19] 張苑蓉譯，James D. Murray (PY)著，**SNMP 網路管理協定**，美商歐萊禮股份有限公司，1999。

[20] 張傑生、唐瑤瑤、許凱平、陳啟煌、李秀惠、賴飛羆，"使用 Open Source 軟體進行 SPAM Mail 防制處理-以台灣大學電子郵件系統為例"，***2004 台灣網網路研討會論文發表論文集***， 2004。

[21] 許倬睿，"利用 Proxy Agent 技術實作之異質網路管理"，***中興大學應用數學系碩士論文***，2002。

[22] 陳通福，"改善網路管理品質資訊系統之建構－以宿舍網路為例"，***元智大學資訊管理學系碩士論文***，2002。

[23] 楊世帆、劉泳霖、方怡雯、蔡旭昇，"結

合 LDAP 之校園電子郵件系統”，***第三屆離島資訊技術與應用研討會***， 2003。

[24] 楊凱宇，”校園無線網路認證系統之建置”，***2003 台灣網際網路研討會論文集***，2003。

[25] 葉平、黃鼎鈞，”sFlow 校園流量即時監測系統之實作”，***2003 台灣網際網路研討會論文集***，2003。

[26] 蔡旭昇、吳采珍、邱紹誠、劉冠廷、黃名霜，”以 SNMP 為基礎之網頁式網路流量查詢”，*第**二屆離島資訊技術與應用研討會***，2002。

[27] 蔡博偉、李錫捷，”網路多模組監控回報系統之研究與設計”，***2003 台灣網際網路研討會論文集***， 2003。

[28] 諸葛理綉、范一鳴、方智敏、鄭秀琴，”基於身份認證的 IP 地址管理方法研究”，***計算技術與自動化***，第 24 卷，第 2 期，2005。

[29] 謝昆霖、呂易儒、郭俊賢，”非營利單位資訊災難備援機制建置之雛形研究”，***2005 台灣網際網路研討會論文集***，2005。

[30] 謝逸凡著，拆解儲存系統中的備份策略，***網路通訊雜誌***，第 168 期，pp 42-P47，2005。

[31] 羅淳譯，”具容錯能力之網路管理系統設計”，***交通大學資訊工程系所碩士論文***，2003。

[32] 嚴大中，”以防火牆日誌分析之網路攻擊偵測系統”，***2002 年台灣網際網路研討會論文集***，2002。

[33] 蘇俊維，”網路安全威脅分析與防制策略”，***東海大學資訊工程與科學研究所碩士論文***，2003。

[34] 蘇俊憲、楊志強、盧東彥，”以 Web-Based 為架構建置網路即時管制系統”，***2003 台灣網際網路研討會論文集***，2003。

[35] 鐘子杰，”應用 LDAP 於公開金鑰基礎架構之研究與實作”，***東海大學資訊工程與科學系碩士論文***，2002。

[36] Cornell W.Robinson lll 作，吳明宜譯，企業網路安全基石：認證，***網路資訊雜誌***，第 179 期，pp 98- 101，2005。

[37] Conry-Murray,Andrew 著，徐祥智譯，內賊要比外患可怕！--來自內部的安全威脅，***網路資訊雜誌***，第 168 期，pp 50-57，2005。

[38] Diane Teare，**Cisco 網路設計**，台灣培生教育出版股份有限公司， 2003。

[39] **ipMonitor Suppor Porta**l，http://support.ipmonitor.com/mibs_byoidtree.aspx。

[40] Jordon Wiens 作，徐祥智譯，”增強弱點偵測-如何選對弱點偵測產品”，***網路資訊雜誌***，第 168 期，pp 67-69，2005。

[41] **P. Phaal and S. Panchen**，http://www.sflow.org/packetSamplingBasics/index.htm。

[42] **RFC 3176**，http://www.sflow.org/rfc3176.txt。

[43] **sFlow**，http://www.sflow.org/。

[44] **Traffic Monitoring using sFlow**，http://www.sflow.org/sFlowOverview.pdf。