校園網路建置社區型 ISP 之應用

陳世賢　　李建宏
中國科技大學 資管系　　中國科技大學 計算機中心
shein@cute.edu.tw　　chienhung@cute.edu.tw

摘要

宿舍網路經營管理可說是各大學網管人員的必修課程，過去的宿網管理系統著重於自行研發宿網管理系統，或導入自由軟體使其應用於校園網路。這兩者都需要計中人員投入研發的人力與成本才能付諸實行，對於精簡人員編制的學校單位來說，看到這些宿網管理系統多只能望文生嘆，難以實行。本文以中國科大宿舍網路管理為例，我們導入一個低成本的路由器軟體，在不變動原有網路架構下，將宿舍網路以社區電信業者的方式經營，並且把宿網流量導至 ISP 業者的 FTTB 線路以減少 TANET 的負擔。此外，還可以針對使用者進行身份認證與限制流量等網管功能，而這些都不需要變動現有宿網架構，或另外花費時間撰寫宿網管理程式與介面，相較於傳統管理程式而言，功能更為強大且成本低廉。相信這樣的成功案例可作為其他學校後續宿舍網路經營管理的參考。

關鍵詞： PPPoE，宿舍網路，社區網路供應商。

1. 前言

回顧過去 TANET 論文集對宿舍網路解決方案的介紹，幾乎多屬 IP-MAC 設定管理功能、依 Netflow 資訊進行流量監控，以這兩項為主要功能的宿網管理系統。而綜觀各校宿網架構因網路設備不同，自行研發程式的結果，也造就了各個管理系統介面上的差異，這也顯示出缺乏可套用至各校宿網架構的單一宿網管理機制。此外，宿網管理長久以來也不斷受到乙太網路惡意程式廣播封包所困擾，這也不是只靠 IP-MAC 管理綁定程式就能解決的，難以採購管理系統與 ARP 病毒難以解決的結果，間接迫使各校宿網漸漸走向全部委由 ISP 業者外包的方案。

本文以中國科大為例，在不變動原有宿網硬體設備與架構下，我們藉由路由軟體設定閘道器將封包轉向業者 ISP 線路。在實際維運上，一來我們將宿網流量完全導向 ISP 業者線路，這樣可以符合 TANET 的立場。二來我們可以社區電信業者的方式經營宿網，依不同使用者收費的標準而開放不同的頻寬使用，並且視學校經營狀況動態採購對外頻寬，這樣也符合校方經營的立場。第三，我們的自建 ISP 方案，兼顧執行教育部封鎖 P2P 的要求，並非將宿網完全委外 ISP 置身事外的作法，在這中間我們仍握有主控權，相信這也符合教育部對大學宿網管理的理念。

所有的網路架構新增或異動，最擔心的就是費用成本與網管人員投注的人力時間，我們實際做到以最低的時間與成本去自建 ISP 方案，其運作穩定可節省以往網管人員在處理宿網問題的時間成本。此外，藉由商用軟體的介面便利使用與設定，大幅減少技術人員在學習自由軟體方案的進入障礙。這樣的架構與效益可提供其他學校做為校園網路或宿舍網路經營的未來發展方向。

2. 文獻探討

過去宿網解決方案，多為自行開發管理系統，以解決 ARP 問題延伸的 IP-MAC 對應或交換器 Port-MAC 對應的管理程式 [5,7,11]。其中再延伸以 Netflow 資訊進行流量控管的程式[4,6,12]，此外為以 SNMP 為主，用以監控流量[3]或 ARP 監控之網管程式[8]等。由於均屬自行研發管理系統，所以仍然缺乏共通性的整合解決方案可供參考

宿網流量全部導向 TANET 有其適當性的議題。劉大川等人認為，宿網應由共用頻寬的 Ethernet 轉型為

獨用頻寬的 FTTB [12]。而且目前 TANET 出國頻寬速度在不及電信業者的線路速度下，學校可以較經濟的方式承租電信業者FTTB的方式提供更好的連線速度。

3. 架構與實作

3.1 路由器軟體 RouterOS 介紹

由於我們在去年已經成功將 PPPoE 導入學生宿網[9]，在後續擴充應用上，也成功的把宿網封包導向 ISP 業者的 FTTB (光世代)線路，這些都可以藉由 Linux 自由軟體方案完成。然而我們發現自由軟體在經過這樣的應用組合拼裝之後，雖然功能強大，但是各式應用的組態設定在進行互相關聯與整合時，顯得不易操作與維護，一旦問題發生，在追查個別功能之間的關聯性問題時，顯得額外困難，也造成自由軟體方案應用在宿舍網路時的不便之處。

因此，如何簡化設定程序，讓網管人員可以輕易地使用設定與維護的工作，這對於自由軟體方案而言，實在是一條困難又艱辛的道路。而且，各大學網管人員精簡人力的情況下，也難以投入時間成本去研究與導入宿網的自由軟體解決方案。

我們一開始在網路上發現RouterOS這套路由器軟體，是抱著測試的心態去購買使用(美金 250 元)。RouterOS 是由 MikroTik [1]無線路由器廠商出產的路由器軟體，其封包傳輸處理概念與 Linux 的 Netfilter 運作架構相似，但不同的是其設定以物件操作為主，擺脫 Linux 指令式操作介面與各種 conf 組態檔設定的技術障礙。在設定與使用上，它已經將所有相關功能整合起來，以整體服務的角度去進行設定。由於整合功能齊全、易於使用、效能良好，無論國內外已經有許多電訊業者以 RouterOS 架設社區網路的實例。

經過我們實測結果良好，因此本文站在提供校園網路解決方案的角度來介紹，我們可以用一般機架式伺服器，加上一個路由器軟體，就可以輕易將校園網路改造成小型 ISP 供應商。加上 RouterOS 低成本、高效能與穩定性都有很好的表現。事實上，本文技術架構全是由我們自行建置，中間並沒有代理商提供技術支援或服務，而且我們也沒必要特別去推銷一套美金 250 元的軟體。下圖為 RouterOS 圖型化物件操作介面。

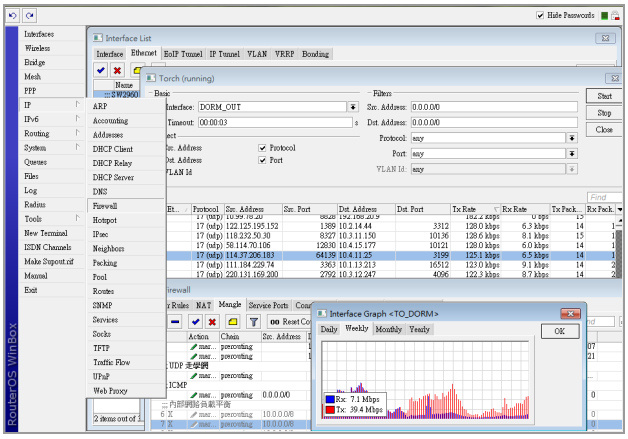

圖 1　RouterOS 使用介面

3.2 宿網架構簡介

中國科大新竹校區住宿學生約 1000 人，分為四棟建物，我們將這四棟建物依照不同樓層，區分不同的 Vlan，例如一宿 A 棟六樓的網路號碼為 10.1.6.0/24，這樣編排出了 25 個 Vlan 組成宿網。以最經濟的方式建設硬體架構，在各樓層間以 D-Link DES-1228 交換器 1000M FE 接上該棟建物之唯一集中交換器 D-link DGS-3100，最後這四棟 DGS-3100 以光纖方式接回電算中心機房 Cisco 3550 交換器內。

在原先的架構下，一開始就註定了我們沒辦法在宿網管理上走向 802.1x 管理路線，我們只能在硬體設備維持現況不動的情況下，推出我們的 ISP 自建方案。

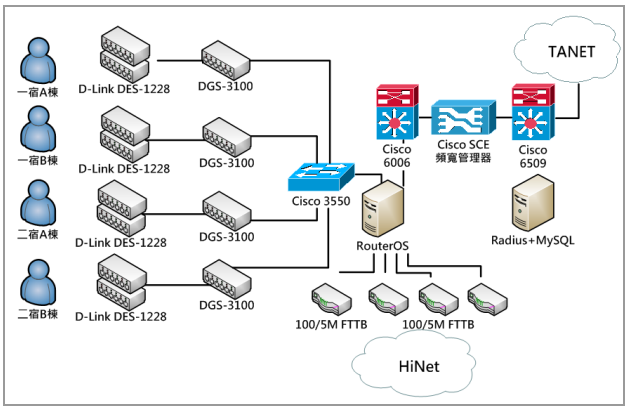

圖 2　中國科大宿網架構圖

我們去年導入 PPPoE 自由軟體方案時，僅使用一台

IBM X3550 作為伺服器，現在則直接以 RouterOS 取代 Rp-PPPoE 軟體，因此不再需要另外增購伺服器。因為原伺服器沒有特別擴充網路卡，所以申請的四路獨立對外的 FTTB 線路我們把它接在 Cisco 6006 的 FE port 上，以 Vlan 的使用方式，讓 RouterOS 透過 Trunk 線路將流量導向這四條線上。

使用 FTTB 線路首先要克服的是使用者的上傳/下載集縮比的問題，由於我們一棟建物只用一條 100M/5M 的線路，所以限定個人 PC 頻寬為 10M/128k 的流量限制。我們發現 FTTB 雖然下載 10M 足夠使用，但使用者會不自覺開啟某些佔用上傳頻寬的應用程式，如果在上傳 5M 流量達臨界值時，會直接影響下載的速度表現。為了使用上感覺更順暢，我們將 UDP 封包導向學術網路。這是一條過去宿網走的路線，它仍然是受到頻寬管理器(Cisco SCE)的限制，將封鎖所有 P2P 傳輸封包。這個 UDP 封包分流的方式是我們特有的作法，並不是必要的功能選項，未來各校可視情況增設 FTTB 線路或維持全部導向原有 FTTB 線路。

3.3 PPPoE 封裝傳輸

宿網改用 PPPoE 的最大好處在於排除區網 L2 廣播的問題，尤其是宿網到了後期，各式廣播型病毒成了宿網經營者的惡夢，無論使用 IP 綁定 MAC，或 MAC 綁交換器 Port 的方式，都無法擺脫 L2 廣播惡意程式的痛苦。這樣的問題已沉痾難解，而使用者只會責怪校方宿網龜速，不可能去怪罪自己電腦如何中毒，這都使得網管人員有苦難言。

使用 PPPoE 封裝格式，可避免傳統 Ethernet 網路協定的困擾，消除 ARP、DHCP 欺騙等問題，亦不需藉由 IP-MAC 綁定作業而發展相關 802.1x 或 SNMP 等管控之類技術，尤其是 802.1X 認證技術，還需要全面更換宿網交換器，改為單一 PC 對應至交換器單一 Port 的方式，這需要挹注大筆的硬體投資才能完成。

我們採用 ISP 業者的執行方式，以 PPPoE 將 Client 封包完全導向路由器，將使用者視為單一獨立個體傳輸封包。統一集中控管的另一個好處，還可以避免傳統宿舍內部影音資料分享所衍生的其他問題。在我們使用 PPPoE 技術後，宿網原先聘請的三位宿網經理從過去疲於奔命處理各個 Vlan 的 PC 廣播風暴與中毒的問題，到現在改採 PPPoE 時期處理 PC 問題的工作量幾乎是天壤之別。

3.4 使用者身份驗證與限頻管制

使用者即時頻寬限制與每日總量管制，為各校宿網基本功能需求，雖然 RouterOS 已內建頻寬管理功能。但是由於不同使用者需要不同等級的頻寬與總量 quota 限制，這需要透過 Radius 伺服器配合 SQL server 來完成 AAA 驗證、授權 (RFC-2865)、帳戶處理 (RFC-2866)等管理功能。以本校而言，我們將老師帳號與學生帳號設定不同的頻寬限制。由於這是一個標準網路協定，所以我們只要以單一伺服器架好 Radius 及 MySQL 即可，接下來 RouterOS 會自動依據 Radius 資料庫記錄給予使用者不同的 Quota 與頻寬限制。

驗證 (Authentication)：在這段實際應用上，我們可以寫一個簡易的宿網管理程式，每學期將住宿學生學號(username)轉入 Radius 資料庫內，要求 Radius 轉向學校 LDAP 主機進行密碼認證。這一部份如果不撰寫管理程式，也可以簡單的用 SQL 語法將資料轉進資料庫內即可。

使用 Radius 認證方式也可以設定依 Username 綁定指定網路卡 MAC 後分配指定特定 IP，達成 Username = MAC = IP Address 三種綁定作業。不過目前我們認為 Radius 已經有很好的 Accounting 功能，網路 NAT 轉換資訊也都記錄到 Netflow 資料內，就不必要再進行綁定 MAC 的設定工作。

授權 (Authorization)：驗證通過後依 Radius 資料表內使用者等級給予頻寬限制的授權作業。這一點在未來應用發展上很重要，我們可以把學校當作是 ISP 供應商或社區電信業者，未來住宿學生可依收費情況給予不同頻寬使用，當學校取得經費來源後可再繼續擴充 FTTB 對外頻寬線路。這可視學校經營方式而定。Radius 使用者等級資料表如下圖所示：

radgroupreply
radpostauth
radreply
report
uselog
usergroup

id	GroupName	Attribute	op	Value
10	student-level-3	Mikrotik-Rate-Limit	==	128k/10M
11	teacher-level-1	Mikrotik-Rate-Limit	==	128k/10M
9	student-level-2	Mikrotik-Rate-Limit	==	128k/3M
8	student-level-1	Mikrotik-Rate-Limit	==	64k/1024k
12	teacher-level-2	Mikrotik-Rate-Limit	==	128k/10M
13	teacher-level-3	Mikrotik-Rate-Limit	==	128k/10M

圖 3　RADIUS 資料庫表格欄位

帳戶管理(Accounting)：為了刻意懲罰超量使用者，我們在資料庫端撰寫自動化執行程式，每日計算 Radius Accounting 資料庫內，使用者 In/Out Total Bytes 數，一旦程式發現超量使用者，將變更其 Radius 資料庫之使用者等級欄位，待懲罰日期過後再恢復原等級。下圖為我們宿網管理的唯一資料庫程式概圖。

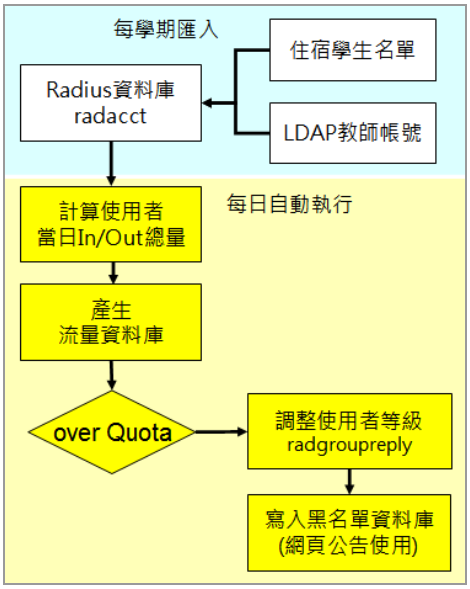

圖 4　宿網資料庫程式運作

刻意懲罰超量使用者，是我們特別測試做為 AAA 的使用功能，這並不是系統運作的必要項目，在使用上也僅是改變 Radius 資料庫的欄位值即可。

3.5　NAT 轉址

對於 PPPoE 的使用者封包轉向 ADSL 線路，RouterOS 會自動進行 NAT 轉址服務。此外，RouterOS 也可以設定為單純提供 NAT 服務設備，這樣的作法與翁仁芳[5]等人利用 IPCop 軟體做全宿舍的 NAT 服務的結果是一樣的。

3.6 封鎖 P2P 傳輸與不當資訊防治

RouterOS 可辨識部份 P2P 傳輸封包，我們只需要在 RouterOS 的防火牆內設定丟棄 P2P 封包即可。如有需要進行不當網頁資訊防治，可參考我們過去的作法[10]，直接在申請的 FTTB 線路加上色情守門員即可。

3.7 強制導向使用者讀取校園訊息公告

我們利用 RouterOS 對封包標記(mark)的功能，當有重大訊息需要公告時，我們可以強制將使用者 http 封包先行導向我們要公告的網站，待 30 秒閱讀時間過後使用者才能正常瀏覽其他網站，而且我們設定僅強制閱讀一次，不會造成使用者在後續使用上的不便。

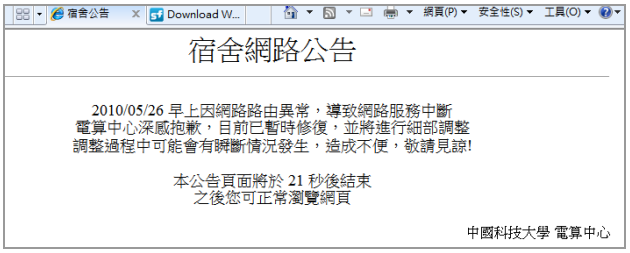

圖 5　強制讀取校園訊息公告

3.8 強制導向 Proxy

我們可以在 Cisco 路由器上設定 Policy Route 強制導向 Proxy 伺服器，而這個 Proxy Server 就是 RouterOS 本身，這是它的內建功能，只需勾選服務項目即可。為此我們又再另外採購一套 RouterOS，移作學校 Proxy Server 之用，強制全校 WWW 流量導向至 RouterOS，並再將 WWW 封包以 NAT 方式轉至另一線獨立的 100/5M FTTB 專線，網管部份改以 Netflow 記錄方式留存記錄。這些都可以勾選欄位方式設定即可。

3.9 對外 ISP 線路整合與備援

我們使用四路光世代 100M/5M FTTB 線路對外連線，支撐新竹校區宿網 1000 人使用者，我們將這四路線路分屬不同 Vlan 透過交換器接上 RouterOS，並於 RouterOS 路由設定各線路互為備援使用，當第一線路故障中斷後，自動將流量導向第二線路，除非 ISP 業者提供的四路線路全部中斷才無法繼續提供服務。我們可設定由系統自動偵測線路復原時間，一旦復原立即將封包導向原來線路使用。

雖然 RouterOS 可支援線路負載平衡，但是實際運作上發現宿網使用者在執行線上遊戲時會斷線的問題，所以我們改採行獨立建築物以個別線路的方式來處理，避免這樣的斷線問題。

3.10 網路管理

RouterOS 內建 Cisco Netflow 統計封包格式，我們可延續使用傳統 Netflow 路由器統計封包方式，將 NAT 的通聯記錄保存至遠端主機，作為後續記錄分析或網管稽核的工作。亦如同所有的網路設備一般，RouterOS 支援 SNMP 協定可讓我們針對各介面 I/O 流量或 CPU、Memory 等進行 MRTG 繪製工作。此外，支援 Cisco AAA MIB 格式，可將 PPP 使用者總數或個別 PPP 使用者資訊繪製圖表或監控即時使用者人數之用。我們將 PPP 使用人數繪製成即時 MRTG 圖，可看出六月間的尖峰時段約 400 人次同時使用網路。

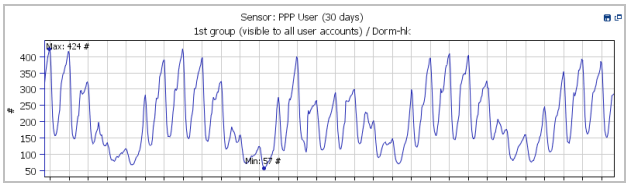

圖 6　即時監控 PPP 使用人數 (30 天)

3.11 效能表現

我們讓 RouterOS 做 PPP 認證、頻寬限制、導向 FTTB 的 NAT 處理、UDP 分流導向、封鎖 P2P 封包、Netflow 傳輸等等工作，其伺服器的 CPU 表現都在 10% 以內，其效能表現比去年只做 RP-PPPoE 而已卻佔用 10-20%的情況要好多了，這也表示出 RouterOS 相較於一般自由軟體有較高效率的處理能力。

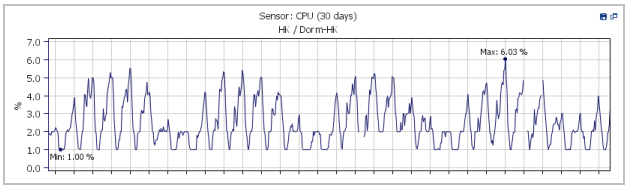

圖 7　伺服器 CPU 效能圖 (30 天)

CPU 實際運作效能是一個指標，我們實際以一台機架式伺服器(中信局契約價 15 萬)加上一個近萬元的路由器軟體，就能在現有校園網路架構下，建構一個服務宿舍學生的社區網路服務供應商的方案。

4. 結論

我們提供的宿網解決方案與過去各大學宿網管理系統的概念不同，這可做為一個用來取代現有各校網路架構的整套解決方案，不需要另外自建或購買專屬的宿網管理系統，也不需要換購原有網路交換器設備，同時可以將宿網流量導至電信業者 FTTB 線路，減輕學術網路負擔。並可藉由管理介面設定使用者身份認證、P2P 封鎖與限制頻寬流量等控管作業，做到實際將宿舍網路以社區電信業者的方式經營運作，以期達到教育部、學校、學生三方共贏的局面。

參考文獻

[1] MikroTik RouterOS , http://www.mikrotik.com

[2] 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”, TANET 2005

[3] 周文正 “學生宿舍網路管理與頻寬調節系統之研製”, TANET 1999研討會

[4] 姜文忠,廖述益,施銘亮 “網頁式校園宿舍網路管理資訊系統規劃與建置”, TANET 2007研討會

[5] 翁仁芳,林義芳,林靖烽 “可擴充頻寬的學生宿舍網路架構”, TANET 2007 研討會

[6] 張安平,黃世銘 “新世紀宿舍網路管理系統”, TANET 2003研討會

[7] 張凱賀,簡國斌,陳建宏,陳偉銘,陳懷恩 “學生宿舍網路註冊系統及網路管理程式”, TANET 2008

[8] 郭蕭禎,謝進利,許忠強 “以 SNMP 偵測阻斷區域網路 ARP 欺騙行為”, TANET 2008研討會

[9] 陳世賢,李建宏 “PPPoE 技術的校園網路應用”, TANET 2009 研討會

[10] 陳世賢,李建宏,蘇世昌 “校園不當資訊過濾機制—以中國科大為例”, TANET 2009 研討會

[11] 楊志強,蘇俊憲,孫學智 “宿舍網路管理系統之建置”, TANET 2002研討會

[12] 劉大川,陳昌盛 “規劃新一代的校園宿舍網路”, TANET 2008 研討會

[13] 蘇建郡,廖哲毅,陳序豪 “宿網管理與校務資訊系統之整合設計”, TANET 2004研討會