

網頁式校園宿舍網路管理資訊系統規劃與建置

¹姜文忠 ²廖述益 ²施銘亮

¹修平技術學院資訊管理系 ²修平技術學院電子計算機中心

E-mail: { wcchiang,iven,andystar}@mail.hit.edu.tw

摘要

隨著網際網路應用的日漸普及與多樣化，大學生使用電腦上網率高達百分之百。然而，經由網管分析得知，網路上所傳輸的訊息以多媒體資料居多，網路使用者的行為模式也越來越複雜，如：P2P(Peer-to-Peer)、網路電視、串流影音...等，學生守法觀念薄弱與自主意識高漲，使得校園網路管理變得更加地困難。因此，結合有效的管理政策以及合適的管理系統，用以解決上述問題將是資訊部門所必須面對的重大議題。本研究以中部某技術學院學生宿舍網路為對象，開發一套能協助網路管理者有效控管 IP(Internet Protocol)和流量異常的網路管理系統，經實務證明，此系統可有效解決宿舍網路管理所遭遇的：1.學生免除設定 IP 的困擾、2.避免 IP 衝突、3.自動阻擋流量異常之 IP、4.限制單一 IP 每天的流量。

關鍵字：流量異常，盜用 IP，阻擋導流

1. 簡介

如何讓有限的網路頻寬被有效地使用是網路管理者的基本職責，但如何做到讓使用者對其傳輸速率滿意則是網路管理者所迫切需要解決的問題，一直擴展網路頻寬相對的付出成本也勢必提高。所以如何在即有的網路頻寬下，讓網路頻寬充分被使用是當務之急。目前網際網路多以 P2P 軟體傳送數位影音資料為主，例如 MP3(MPEG Audio Layer III)音樂及 MPEG(Motion Picture Experts Group)電影檔及網路線上遊戲...等。這些行為都是網路頻寬最大殺手。要使網路頻寬能有效地被使用，必需要定出一套可行的宿網使用規範與管理機制，讓使用者可遵循校園網路使用規範使用網路，若使用者違反使用規範時，應給予適當處置，共同維持網路的通暢。

本論文期望實作出一套能協助網路管理者分析流量，偵測出流量異常者，再搭配網路設備所具備之過濾(Filter)功能，給予暫時終止其網路用權的處置。

本網路管理輔助資訊系統預計達到的目標：

(一)扮演輔助者角色

本系統主要是輔助管理者進行流量蒐集、分析，阻擋流量異常之 IP 等等這些繁瑣的事。

(二)記錄網路使用者基本資料

所有網路使用者，需經宿網註冊，登錄正確的 MAC(Media Access Control)後，才能正常上網。唯有資料齊全，才能提供往後辨別身份正確的資訊。

(三)自動發放床號對應 IP 給使用者

系統會將宿網註冊資料自動轉換成 DHCP(Dynamic Host Configuration Protocol) Service 的設定檔，發給使用者 IP，讓使用者免除 IP 設定的困擾。

(四)IP-MAC 對應

系統會將宿網註冊的 MAC 與床號所對應之 IP 記錄在網路設備上，避免 IP 盜用的情況發生。

(五)流量分析，自動阻擋流量異常

系統整合了 Flow-Tools 做流量分析，如發現流量異常之 IP 立即在網路設備上自動阻擋此 IP，保持網路之暢通。

(六)阻擋導流

透過系統之 DNS(Domain Name Server)設定，讓被阻擋的使用者，開瀏覽器時，自動導引到阻擋說明網頁，並告知阻擋原因和解決方法。

(七)網路使用狀況資料保存

系統會將分析完成的流量資訊儲存到資料庫中，以便管理者和使用者查詢相關流量資訊。

2. 背景及相關研究

2.1 背景

每學期當學生進住到宿舍，學生都要自己設定 IP，但大部分學生因網路概念與網路設定能力不足（不會設定或設定錯誤），造成不能上網。雖然在宿舍公佈欄有公告設定說明，也成立宿網管理小組協助處理，但遇到的問題千奇百怪有網卡故障、網路線不通、電腦遭受病毒感染、網路連線設定有誤...等，迫使管理者在這段時間內需協助解決，造成人力損耗。

網路資源的豐富帶給使用者便捷資料的取得，由於它的便利與不可見性，少部份宿網使用者往往濫用網路資源而不自覺，導致「部分使用者不了解網際網路成文與不成文的規範，造成使用者在網路上，交換無合法版權軟體、MP3 音樂、或電影 VCD 的資料傳輸行為常常發生，很輕易地就能將寶貴的頻寬消耗殆盡」[18]，最近幾年網路被駭客及病毒肆虐成災越來越嚴重，電腦不斷的被病毒嘗試感染及被駭客嘗試入侵，這樣的問題一直反覆著發生，造成管理者需要經常去查閱防火牆的記錄檔，判斷是否有流量過大或中毒跡象，如果是就進行手動阻擋。但也有可能誤判的情況產生。且要記錄阻擋時間，經由學校懲罰性的行為後又得手動解除阻擋，如果超過時間解除又會造成使用者的反彈，所以管理者時時刻刻都要注意網路上的流量和解除阻擋之時間。

宿網使用者如果意圖大量下載數位內容、感染網路型病毒、發送龐大的網路訊息或佔用大量網路頻寬時，被管理者阻擋，都會任意更改 IP，造成 IP 衝突，管理者必須連線到網路設備上，查出 IP 在網路設備的那一個介面，再到現場去查看連線到那個資訊插座，進而查出盜用 IP 的使用者，如此會造成管理者人力損耗。

2.2 相關研究

學校對於宿舍網路管理模式大略分成：1.利用學校既有的網路頻寬，委外由 ISP(Internet Service Provide)業者管理 2.宿網對外頻寬和管理都由 ISP 業者提供 3.宿網管理及對外頻寬都由學校管理。第

一種及第二種模式對於學校在宿網管理基本上不太需要付出人力損耗，但學生上網的行為無法管制，第三種模式雖然對學校的人力支出較大但本著教育學生的原則，學生的行為舉止學校有監督及教育的義務，本校採用第三種模式期望能管制使用者上網行為。

良好的宿網輔助管理系統功能必需包含流量異常自動阻擋、防止 IP 盜用、自動發配床號所對應的 IP 給使用者、限制使用者日流量在區網中心所規定內、防止使用者使用 P2P 軟體下載有版權的數位內容、阻擋導流及阻擋後自動解除阻擋。

(一)偉智和王明輝[11]，是利用 Cisco Netflow 資料進行即時偵測蠕蟲攻擊的方法，利用這個方法，可以在蠕蟲發動掃描攻擊時，有效辨識出發動攻擊的電腦 IP 位址，接著就可以在路由器上將發動攻擊的 IP 位址阻擋掉。此系統只針對蠕蟲攻擊做處理，無法對流量大的使用者加以限制。

(二)李宇峰等[10]，透過 ARP(Address Resolution Protocol)、SNMP(Simple Network Management Protocol)等技術勾勒並實作出一個 IP 管理自動化的架構，解決大部份網管人員長久以來之困擾並有效降低管理成本。但此系統發配 IP 時並無法發配床號所對應之 IP。

(三)任善隆等 [7]，此系統將超過限制流量的 IP 導向違規伺服器，限制流量伺服器會依照網路連線方式顯示違規 IP 相關資料。此系統無自動解除阻擋機制，會造成管理者要時時刻刻去注意什麼時候要解除阻擋。

本系統結合了 NetFlow、Flow-Tools、DHCP 及 DNS 設定檔和網路設備所提供的 Filter 和 ARP Table 功能，開發出一套具流量異常自動阻擋、防止 IP 盜用、自動發配床號所對應的 IP 給使用者、限制使用者日流量在區網中心所規定內、阻擋導流及阻擋後自動解除阻擋的宿網輔助管理系統。

3. 系統架構

本系統是利用具備網管功能的網路設備所提供的功能和特性加以開發的宿網管理系統。在此先介紹宿舍網路架構後，再詳述系統架構。

3.1 宿舍網路架構圖

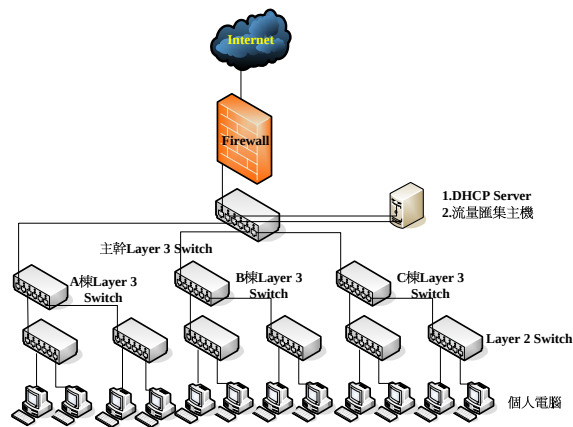


圖 1 宿舍網路架構圖

如圖 1 每一棟(A 棟、B 棟、C 棟...等)宿舍各有一台 Layer 3 Switch 分別連接至數台 Layer 2 Switch，再到個人電腦，宿網佈線採用單一配線系統(Single Cabling System: SCS)，包含配線端子板、資訊插座、跳接線、連接線及 UTP 線等構成的整體配線系統。每棟宿舍的 Layer 3 Switch 分別為每一層樓設定一個 VLAN(Virtual Local Area Network)，可以有效的控制廣播封包不會轉發到其他 VLAN 中。系統在執行 IP-MAC 對應和自動阻擋時，管理者只需於每棟宿舍的 Layer 3 Switch 上下達管理指令即可，方便控制流量、簡化網路管理、提高網路的安全性。而在流量匯整及分析方面，則在主幹 Layer 3 Switch 上用 Mirror 的方式，將對外網路連接埠之流量複製到系統主機上。

3.2 系統架構圖

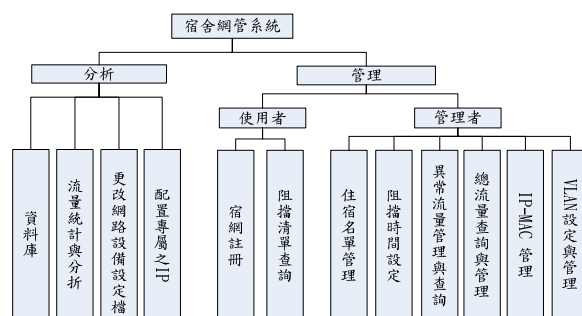


圖 2 系統架構圖

如圖 2 系統部份主要分成二類，分別為管理模組和分析模組：

(一)分析模組：其功能分別是流量統計與分析，分析後之結果存放至資料庫、修改網路設備的設定檔、更改 DHCP 的設定檔，使用者可以正確取得床

號所對應之 IP，以 Perl 語言撰寫。

(二)管理模組：分別提供給使用者宿網註冊和阻擋清單查詢及提供給管理者住宿名單管理、阻擋時間設定、流量異常管理與查詢、總流量查詢與管理、IP-MAC 管理及 VLAN 設定與管理，以 PHP 語言撰寫 WEB Base 系統架構。

4. 實驗結果

下例是以台中某技術學完之宿舍網路所做的實例

4.1 宿網 IP 分配原理

主要是說明 DHCP 發 IP 給學生之規則。由於宿網對於沒有註冊的電腦僅提供瀏覽校內網站及進行宿網註冊動作，因此，DHCP 需提供一段 IP 給學生宿網註冊使用。對於已註冊的電腦，DHCP 會依學生註冊的 MAC 號碼發給所對應的 IP(如圖 3)，即可正常上網。以下(表 1)是未註冊 IP 與已註冊 IP 的差異

表 1：未註冊 IP 與已註冊 IP 的差異表

	未註冊 IP	已註冊 IP
IP	10.棟別+樓層.65.1	10.棟別+樓層.房號.床號
IP 例子	10.12.65.1	10.12.1.1(201 號房第一床位)
限制	只限瀏覽校內網站	IP 和 MAC 對應

VLAN	樓層	學號	姓名	系級	班級	TEL	註冊	IP	MAC	流量限制	設定日期	上次修改	保留	
資訊二樓	學法	200707171505	王嘉瑞	資訊管理	1			10.12.4.2	00-0D-03-43-5A-13	3096 MB	0	2007-07-17 15:05	☐	☐
資訊二樓	學法	200707171605	王嘉瑞	資訊管理	1			10.12.1.1	00-13-04-9A-CE-23	3096 MB	0	2007-07-17 16:05	☐	☐
資訊二樓	學法	200707171605	王嘉瑞	資訊管理	1	010-11-09-30		10.12.4.1	00-13-04-9C-EA-15	3096 MB	0	2007-07-17 16:05	☐	☐
資訊二樓	學法	200707171605	王嘉瑞	資訊管理	1			10.12.2.2	00-16-05-0A-EA-18	3096 MB	0	2007-07-17 16:05	☐	☐
資訊二樓	學法	200707171605	王嘉瑞	資訊管理	1			10.12.2.1	00-4D-F4-6E-83-21	3096 MB	0	2007-07-17 16:05	☐	☐
資訊二樓	學法	200707171605	王嘉瑞	資訊管理	1	010-11-09-30		10.11.19.4	00-2D-ED-4E-AE-24	3096 MB	0	2007-07-17 16:05	☐	☐

圖 3 床號與 IP 對應表

4.2 統計 IP 流量

本系統是利用網路設備本身所提供的 Mirror 功能將對外之流量複製到網管伺服器上，系統利用 NetFlow 接收後，使用 Flow-Tools 做分析和統計出總流量和流量異常(如圖 4)。

全校 2007年 07月17日 TopN 日排行榜												
排名	ip	校外->校内			校内->校外			校内<->校外			size	
		flow	pkts	size	flow	pkts	size	flow	pkts	size		
1	64.66	886,303	20,943,834	24,665,243,003	888,168	14,080,876	1,767,745,457	1,774,471	35,024,710	26,432,969,280		
2	64.32	36,290	5,337,637	615,524,968	36,271	7,361,946	7,852,817,571	70,563	12,719,593	8,466,342,539		
3	76.30	312	2,383,088	96,553,976	301	4,791,005	6,678,630,736	612	7,174,093	6,775,184,715		
4	74.219	28,921	3,020,133	2,781,188,245	29,858	3,151,217	3,045,680,528	58,779	6,171,350	5,826,866,773		
5	71.76	69,353	3,415,620	4,400,464,908	76,606	2,519,159	149,491,343	145,958	5,934,779	4,549,956,250		

圖 4 每日總流量

4.3 阻擋導流

本系統如果發現流量異常或日流量超過 2GB 之 IP，系統會自動更改網路設備的設定檔將異常 IP 阻擋，並將此 IP 導到阻擋說明網頁(如圖 5)，告知阻擋原因、解除阻擋時間和基本解決方法(如圖 6)。

技術學院電算中心

注意

您已被阻斷，無法使用全部網路資源

可能原因:

- 流量超過上限
- 流速異常
- 管理者阻斷

詳情請點此處。

Generated Tue, 17 Jul 2007 07:56:02 GMT by netflowdb (Squid/2.4.STABLE6)

圖 5 阻擋網頁

超過限制流量與異常清單									
已遭封鎖IP同學，請洽宿舍網路管理委員會解除封鎖									
全部資料有 3 筆， 阻斷資料有 3 筆， 警告資料有 0 筆									
阻斷資料區									
IP address	啟動阻斷時間	開放時間	阻斷原因	流入量(M)	流出量(M)	總流量(M)	流量異常原因		
20.3	2007-07-17 08:10	2007-07-18 00:00	超過流量上限	274	2782	3056			
25.1	2007-07-15 03:20	2007-07-18 04:00	流量異常	0	0	0	session		
6.2	2007-07-17 13:20	2007-07-18 00:00	超過流量上限	866	2261	3127			

警告區

IP address 上次更新時間 警告原因 流量異常原因

圖 6 阻擋清單

4.4 宿網註冊

學生只要登入到個人資訊化系統點選宿網註冊時，系統會利用 SNMP 去抓取電腦的 MAC 號碼(如圖 7)，並讓使用者輸入連絡電話和郵件帳號後存入資料庫並且自動更改 DHCP 的設定檔和網路設備上的 ARP 表格(如圖 8)，以防止使用者盜用他人之 IP。

姓名 廖

帳號 93

身份 學生

宿舍別 女宿四樓

系級 二專工管科

班級 2

電話

Email 93@il.edu.tw

網路卡 MAC 00-50-BA-0B-17-01

網路卡的實體位址,格式如 00-50-BA-E3-32-BA

提出申請

圖 7 IP 申請表

```

c:\ Telnet 10.0.0.
arp 10.3.14.7 4411.1111.111d ARPA
arp 10.3.13.4 4411.1111.111d ARPA
arp 10.3.12.5 4411.1111.111d ARPA
arp 10.3.11.2 4411.1111.111d ARPA
arp 10.3.10.3 4411.1111.111d ARPA
arp 10.3.9.0 4411.1111.111d ARPA
arp 10.3.8.1 4411.1111.111d ARPA
arp 10.2.15.7 4411.1111.111d ARPA
arp 10.2.14.6 4411.1111.111d ARPA
arp 10.2.13.5 4411.1111.111d ARPA
arp 10.2.12.4 4411.1111.111d ARPA
arp 10.2.11.3 0013.d4bf.900f ARPA
arp 10.2.10.2 4411.1111.111d ARPA
arp 10.2.9.1 4411.1111.111d ARPA
arp 10.2.8.0 4411.1111.111d ARPA
arp 10.1.15.4 4411.1111.111d ARPA
arp 10.1.14.5 4411.1111.111d ARPA
arp 10.1.13.6 4411.1111.111d ARPA
arp 10.1.12.7 4411.1111.111d ARPA
arp 10.1.11.0 4411.1111.111d ARPA
arp 10.1.10.1 4411.1111.111d ARPA
arp 10.1.9.2 4411.1111.111d ARPA
arp 10.1.8.3 4411.1111.111d ARPA
arp 10.4.15.0 4411.1111.111d ARPA
--More--

```

圖 8 網路設備的 ARP 表格

5. 結論及未來發展方向

對於網路管理，限制使用者使用網路是不得已的手段，但是少部份的使用者占用大量頻寬，進而間接地影響到校園網路之正常運做。此時管理者則有其權利和義務限制該使用者之使用權。故為開發本網路管理輔助系統的意義即在於此。

本系統已達到預期之功能，使用者可隨時上網註冊，只要MAC無誤，即可正常上網。使用者的IP和MAC對應，達到防止IP盜用之目的。監控使用者之流量，防止少數使用占用大量頻寬，保障所有網路使用者之權力。

此外，本系統目前已於本校宿舍網路上使用，未來將更推廣至校學之教學單位和行政單位，使得校園網路管理更有效率。但由於此套系統尚未能針對使用者之行為加以分析統計做限制，故在未來的研究方向將朝，整合免費分析網路行為之軟體對P2P使用者加以限制與管理等方面多加努力。

6. 參考文獻

[1] Apache, <http://apache.org/>
[2] Flow-tools, <http://www.splintered.net/sw/flow-tools/>

- [3] Perl, <http://perl.hcchien.org/>
- [4] Linux, <http://linux.vbird.org/>
- [5] Perl, http://linux.tnc.edu.tw/techdoc/perl_intro/
- [6] PHP, <http://www.php.net/>
- [7] 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, 2005.07
- [8] 李國熙，許建發 “Perl程式設計/LarryWall, Tom Christiansen & Randal L. Schwartz 原著”，美商歐萊禮股份有限公司台灣分公司
- [9] 李國熙 “Perl學習手冊/ Randal L. Schwartz, Tom Christiansen原著”，聯寶總經銷
- [10] 李宇峰，劉柏汎，楊慶隆，紀新洲 “自動IP管理系統”，TANET 2005, 2005.07
- [11] 徐偉智，王明輝 “利用Netflow 即時偵測蠕蟲攻擊”，TANET 2006, 2006.07
- [12] 許鳴程 “專業PHP程式設計/Jesus Castagnetto, Harish Rawat, Sascha Schumann, Chris Scollo, Deepak Veliath 原著”，基峰資訊股份有限公司
- [13] 陳志昌 “Perl高等程式設計/Sriram Srinivasan 原著”，美商歐萊禮股份有限公司台灣分公司
- [14] 陳峰棋 “Cisco Router 設定大全/Allan Leinwand Bruce Pinsky 原著”，知城數位股份有限公司
- [15] 黃燕忠，林奕光 “Linux網路伺服器架站與管理實務大全”，博碩文化股份有限公司
- [16] 黃武隆 “校園宿舍的網路管理及建置以南華大學宿網為例”，南華大學資訊管理學研究所碩士論文, 2002.
- [17] 劉淑慧 “最近 JavaScript 語法參考辭典/Kazuhiro FURUHATA 原著”，博碩文化股份有限公司
- [18] 謝志昌，蔡哲民 “以開放原始碼做簡易網路連線流量統計”，TANET 2000, 2000.10