可擴充頻寬的學生宿舍網路架構

翁仁芳　林義芳　林靖烽
明新科技大學電算中心
E-mail：jfw@must.edu.tw

摘要

本文將目前大專院校中學生宿舍網路，使用虛擬網路架構時頻寬不足的問題，提供一個便宜又有效的解決方案，利用 Freeware IPCop 為核心的 NAT 設備，讓管理者可以依學生的使用量隨時增加設備，避免宿舍網路擁擠的情形。

關鍵詞：宿舍網路、IPCop、虛擬網路、NAT。

Abstract

Dormitory network of universities and colleges, at present this text, the frequently wide and insufficient question, offer a cheap and effective solution while using private network structure, utilize Freeware IPCop to enable the administrator to increase the equipment at any time in accordance with students' consumption as central NAT equipment, avoid the crowded situation of the dormitory network.
Keywords: Dormitory network、IPCop、Private Network、NAT.

1. 前言

網際網路的發達與學習的需要，使得大專院校內的學生宿舍必須有網路給學生使用，以因應教學上的需要，除少數的學校外，各校皆有網路 IP 不足的問題，為能讓宿舍學生能有足夠的網路 IP 位址，只能使用虛擬 IP 方式透過 NAT 設備連接網際網路。但因學生在宿舍網路中，毫無限制使用網路的情況下，造成 NAT 設備的負擔過重，而產生網路擁塞，甚至癱瘓無法使用等問題。

為解決此問題，只有購買幾十萬的 NAT 設備來滿足宿舍網路的需求，但當有殺手級的應用程式（P2P 軟體）被普遍使用後，NAT 設備就會因負擔過重而發生網路問題，此時只有購買更大型的設備來滿足宿舍的需求，雖然滿足了需求，可是也造成原先設備上的浪費，對私立學校來說是一筆不小的負擔，透過此一架構可以有效的解決宿網，因 NAT 設備所造成頻寬不足的問題。

這樣的架構在本校已經運作二年，學生宿網除校外網路所衍生的問題外，使用上普遍滿足學生的使用需求，也減少電算中心管理上的問題，為此將經驗透過本文，提供心得讓宿舍網路管理者參考。

虛擬位址的採用已是不可避免的趨勢，我們將一些規劃網路架構的重點及需求列舉如下：

A. 成本上的考量，如果以穩定度的考量，宿舍網路 NAT 應採用 Router 級或 Core Switch 級的網路硬體設備，但這些等級的設備，不是一般私立學校可以負擔的，因此我們傾向使用個人電腦或工作站以軟體的方式進行轉換。
B. 在效能的考量上，NAT 設備不應該成為網路流量的瓶頸，為滿足現有的網路環境，NAT 設備應採用 Gigabit Ethernet，而不能僅支援到 Fast Ethernet 界面。
C. 宿舍網路虛擬 IP 位址，在校園內應視為的校園 IP 位址，校園內的伺服器可紀錄宿網用戶端的 IP 位址，不管是真實 IP 位址還是虛擬 IP 位址。
D. 宿舍網路只有在出校園的 WAN 端時，才透過 NAT 轉換設備，讀取校園內相關教學網站，要能直接存取不透過 NAT 轉換，且網路架構需簡單易維護。
E. 在流量統計的應用時，必須紀錄 NAT 轉換之前的流量，而不是紀錄 NAT 轉換之後的流量，如此才能對宿舍學生的流量做管理。
F. 備援機制，為避免 NAT 設備的故障，造成宿舍網路斷線，造成學生的抱怨。
G. NAT 軟體必須穩定且便宜，在安裝過程與管理上，要簡單快速。
H. 因應宿舍網路流量增加，可以很快擴充 NAT 的設備分擔流量，避免因設備頻寬不足，所造成的網路問題。
I. 電腦病毒容易發生大量感染，因此每棟宿舍的網路均為獨立 VLAN，以避免每棟宿舍網路間，互相影響的問題發生。
J. 在建置規劃上，應該也要考慮未來的擴充性及網路應用。例如：如果需要在校內 WAN 端出入閘口加裝 P2P 流量管制設備時，要能容易地整合進來。

經過實際的上線測試與調校，本文宿舍網路連線架構，不僅可以同時滿足上述的需求，而且建置成本也不甚高，非常適合宿舍網路使用虛擬 IP 的學校作為參考。

2. 架構說明

設備與軟體的選擇，為能利用最低成本達到最好的頻寬供應，在設備的選擇時，我們考量以市面

上，最容易購買到的設備，此架構會用到路由器、防火牆硬體、防火牆軟體等，這些軟硬體建置時均以成本與效能為考量重點。

本文宿舍網路規劃架構如圖 1 所示，架構中把宿舍網路的流量，針對校內與對外流量，透過靜態路由方式，將所有的流量經過路由器的轉送，靜態路由的好處是容易設定，管理上也非常容易，除非你的宿舍網路或是網路拓樸龐大，不然靜態路由是非常好的選擇，簡單又不容易出錯。

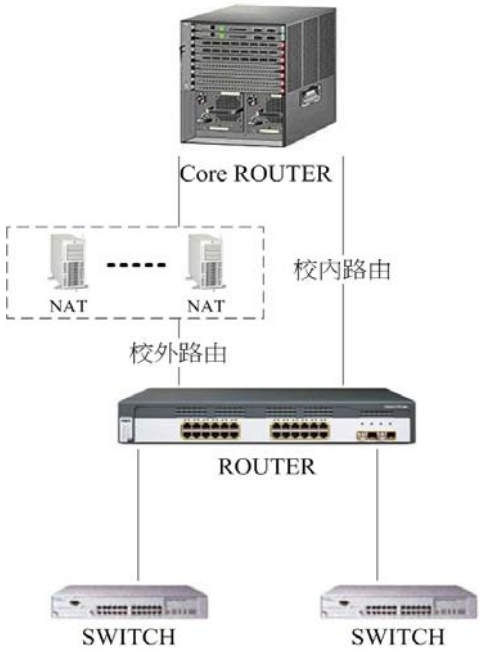

圖 1

2.1 路由器

本校使用 CISCO 的 3750 系列路由器做為宿舍網路路由器，Cisco 的 Cisco Catalyst 3750 系列交換器是一個全新的產品系列，它結合易用性和最高的備援性，提升了堆疊式交換器在區域網路中的工作效率。這個新的交換器系列採用了最新的 Cisco StackWise 技術，可進行高達 32 Gbps 的堆疊互聯，使若干獨立的交換器在堆疊時集成在一起，便於使用者建立一個統一、高靈活度的交換系統－就好像是一台交換器一樣，如果宿舍網路需要擴充時，只要把兩台 3750 堆疊一起，可以方便管理。而且它的價格並不昂貴，以中信局的成交價，12PORT 全光界面（含十二顆 Cisco 原廠 MiniGBIC）才 21 萬左右。

另外這一系列的產品，有宿舍網路最需要的功能 Shaped Round Robin（SRR），藉由此功能流量可以透過智慧處理入口佇列與出口佇列，對封包流量排定不同的優先順序，有這樣的功能，我們才能達到流量分散的目的，設定非常的簡單，只要把對路由器的對外設定，加入”ip route 0.0.0.0 0.0.0.0〈Next-hop router〉”有幾台就加幾行，對管理者來說非常容易，複雜的工作就交由路器處理。當然也可以使用高階的路由器，透過 Policy routing 來做，但是這會減緩 router 處理速度，而且它的設定太複雜，對管理者來說是一大負擔，這樣的路由器也不便宜，不是一般學校所能負擔。

2.2 硬體平台

在一般大專院校網路中，學生宿舍網路的流量對整體的流量來說，是學校對外流量的主要來源之一，規劃時因學生使用量大，所以我們假設學生宿舍網路，會用掉全校一半流量作為依據，以本校當時 200 Mb/s 的流量計算，學生宿舍網路應該會有 100 Mb/s 左右的流量。

除了流量是我們需要考慮外，還有一個重要的參數是我們必須考慮的”連線數（session）”問題，當 NAT 設備可提供的連線數不足時，會造成宿舍網路內的電腦對外連線失敗；可能發生情形，學生剛剛可以連上網路，但因有人使用 P2P 軟體下載檔案，此時造成 NAT 設備連線數不足，產生無法連結網站現象，但下載檔案完成後，NAT 設備連線數又足夠，不能上網的同學又能使用了，這時同學會認為宿舍網路不穩定時常斷線，而會經常抱怨電算中心，造成管理上的問題。

從本校骨幹的 IDS/IDP 的設備上，我們知道全校對外同時連線數（Concurrent Sessions）有 32 萬左右，同樣我們預估宿舍佔有一半的貢獻量，會有 16 萬同時連線數發生，由於軟體 NAT 的限制，每台僅能提供 6 萬個連線數，所以我至少要有三台的 NAT 設備給學生宿舍使用，另外避免發生中毒時，產生大量連線數造成網路不通，因此我們將 NAT 設備數量增加一台到四台，以避免可能造成網路不通的情形。

決定 NAT 設備數量後，我們接著決定硬體規格，在考量 NAT 設備硬體平台時，有幾個部份是我們在意的，如硬體效能、網路卡的選擇、記憶體容量大小等，以下針對這些部份提出我們的想法：

A. 硬體效能，設備本身主要是做為 NAT 使用，因此 I/O 部分是主要的考量，至少我要有符合 PCI 2.3 規範的主機板，目前的主機板都有支援，這樣才能提供兩片 1Gb 網路卡的足夠的頻寬，儘量使用南北橋獨立晶片的主機板，避免使用南北橋整合之晶片組，否則 I/O 效能不足，會影響到整體效能，其他部分只要效能不要太差就足夠應付。
B. 網路卡的選擇，必須要挑選效能好的晶片，建議使用 INTEL 或是 3Com 的網路卡，這在各單位使用已經有很好的使用實績，可以省下我們不少解決問題的時間，重要的是軟體相容性高。
C. 記憶體容量，經過我們實際使用的結果，系統在正常運作時，不會超過 512MB，但是為避免宿舍網路中毒，造成 NAT 設備發生負載過重的問題，因此我們建議 RAM 為 2GB 以應付突發狀況。

2.3 IPCop

在網際網路裡，有很多基於 Linux 環境的路由器，防火牆軟體可供選擇，例如 m0n0wall、Smoothwall Express、LEAF-Bering uClibc 和 ClarkConnect 等，這些防火牆軟體在網路或其他媒體上都有許多功能及應用方面的介紹。但在我們評估 IPCop 時，它的主要目的是「讓不良資料包到此為止」，引起我們的注意力，透過測試後，發覺它是功能強大的整合性軟體。

IPCop 它是一套自由軟體，有眾多的功能，包括 Web 管理介面、NAT 功能、支援 SSH 登入、支援多網卡、上下行流量管制、伺服器日誌管理等功能，是一個功能強大的軟體防火牆，而且安裝上很容易且快速，只要硬體準備好，十分鐘內就能將它安裝完成，這樣的安裝特性讓我們決定使用它，作為我 NAT 設備上的防火牆軟體，如果設備發生問題時，我們可以在短時間內將設備復原，將衝擊減到最少。IPCop 也有很多好用外掛套件，有興趣可以參考它的網站，有詳細的說明。

3. 實作

3.1 路由器設定

為能讓宿舍網路虛擬 IP 位址，在校園被視為的校內 IP 位址，必須分別在 Core 6509 上及宿舍的路由器設定，方式如下：

- ✓ Core 6509 路由設定部份，將宿舍的虛擬 IP 位址，導向宿舍的 3750 上。
- ✓ 宿舍 3750 路由設定部份，將學校的真實 IP 位址，導向 Core 6509 的上。

如此兩台路由器，就可以知道這些 IP 位址，該往那個路由器傳送，宿舍的電腦就能透過 Core 6509 與校內的其他路由器上的伺服器或電腦溝通，不會通過 NAT 設備，存取校園內網路資源，而是直接經由路由器存取，宛如校園內真實 IP 位址運作模式。部份設定如下：

```
ip route 203.68.229.0 255.255.255.0 172.29.255.254
ip route 203.68.230.0 255.255.255.0 172.29.255.254
ip route 203.68.231.0 255.255.255.0 172.29.255.254
ip route 203.68.232.0 255.255.255.0 172.29.255.254
ip route 203.68.233.0 255.255.255.0 172.29.255.254
```

校內 IP 位址部分是使用靜態路由直接將封包送到 cisco6509（172.29.255.254），經由 6509 再轉送到其他網段。宿舍網路只有在出校園的 WAN 端時，才透過 NAT 轉換設備，為能滿足宿舍網路內學生頻寬需求，我們利用 CISCO 3750 內建 Round Robin 的功能，將 4 台 NAT 設備連結到對外線路上，設定方法如下所示，172.19.31.1~4 是 NAT 設備 Local 端 IP 位址。如果還需要增加設備，只要再加上一行 ip route 0.0.0.0 0.0.0.0 172.19.31.X 就能達到擴充的目的，而且有 4 台 NAT 設備，彼此可以達到備援的功能。

```
ip route 0.0.0.0 0.0.0.0 172.19.31.1
ip route 0.0.0.0 0.0.0.0 172.19.31.2
ip route 0.0.0.0 0.0.0.0 172.19.31.3
ip route 0.0.0.0 0.0.0.0 172.19.31.4
```

本校住宿學生電腦數量大約有 1200 台左右，如果沒有做適當的切割，網路的效能會不好，學生的電腦也容易互相干擾，一但遭受網路病毒攻擊時，災害會相當的嚴重，因此我們將宿舍網路切成多個 VLAN 使用，避免一個大的 VLAN，降低受害的範圍，也可以減少廣播封包，增進傳輸速度與效能。VLAN 的切割以每棟宿舍為基本，依住宿學生人數不同而對每棟使用不同子遮罩（netmask），這樣做是受限於光纖建置的問題。
以下是 3750 VLAN 的部份設定內容。

```
interface Vlan803
 description ### 第 3,4 宿舍 ##
 ip address 172.19.0.254 255.255.255.0
!
interface Vlan804
 description ### 第 5,6 宿舍 ##
 ip address 172.19.1.254 255.255.255.0
!
interface Vlan808
 description ### 女生宿舍 ##
 ip address 172.19.11.254 255.255.252.0
 !
```

3.2 IPcop 設定

IPcop 對網路連接介面定義，分為有以下三種，Red 代表外部網路、Orange 代表 DMZ、Green 代表內部網路，做為單純的 NAT 設備，我們只會使用到 Red 與 Green 這兩個連接介面，這兩個 Red 與 Green 介面所代表的網路千萬不要搞錯，不然網路是不會通的，這些連接介面分別各自為獨立的 VLAN，這樣對於各種介面下的使用者，於病毒發作或是有其他的攻擊行為時，可以在 VLAN 上作為即時的阻斷，避免影響到其他網路使用者的連線。

IPcop 安裝非常容易，有基本網路知識的人，照著步驟一步一步來就能安裝完成，整個過程不到 10 分鐘，在安裝由於我們是使用兩片網卡，請注意請選擇如圖 2 所示 GREEN+RED 這一項。

圖 2

圖 3

圖 3 為 IPcop 安裝完成後的畫面，此時 IPcop 就可以使用，但因為在我們宿舍網路架構中，它的下層是 3750 路由器，我們必須要告訴 IPcop 該如何回去，也就當宿舍網路內部電腦連線到校外網站後，網站的資料封包要會回到宿舍網路內部這台電腦，這條路徑必須連結起來。

由於 IPcop 並不知道它下層的 IP 網段有那些，因此登入本機手動設定路由，才能有完整的路徑，否則所有的封包會往 Default 的閘道丟給 eth1 也就是 6509，再由 6509 經由校內的路由回到宿舍 3750 再丟給使用者（流量路徑如圖 4 所示），增加整個網路的負擔。

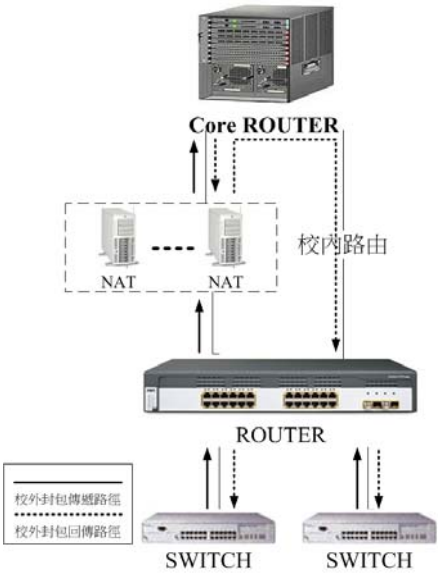

圖 4

IPCop 路由原始設定如下：

172.19.31.0	255.255.255.0	eth0
203.68.223.0	255.255.255.0	eth1
Default	ce254.must.edu.tw	eth1

使用此路由設定檔的情況，所有的流量回來時，都會在 NAT 上全部轉向校外路由（圖 5），而再透過校內路由回到宿舍內部（圖 6）。

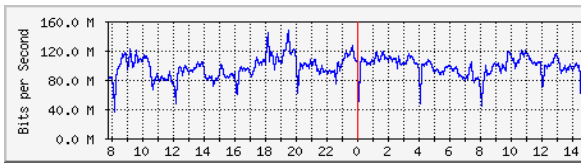

圖 5

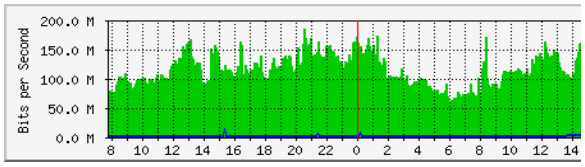

圖 6

為避免此一情形，而在 IPCop 上多加一行指令，增加一筆靜態路由設定，如下指令：
Route add –net 172.19.0.0 netmask 255.255.240.0 dev eth0

可以看到設定多了一筆路由資料（粗體為新增的路由）：

172.19.31.0	255.255.255.0	eth0
172.19.0.0	**255.255.240.0**	**eth0**
203.68.223.0	255.255.255.0	eth1
Default	ce254.must.edu.tw	eth1

新增的路由後，IPCop 已經可以認識他下層有哪些網段的 IP，IPCop 會自行將封包轉向下層去完成完整的路由的路徑（圖 7）。網路流量也正常如圖 8。

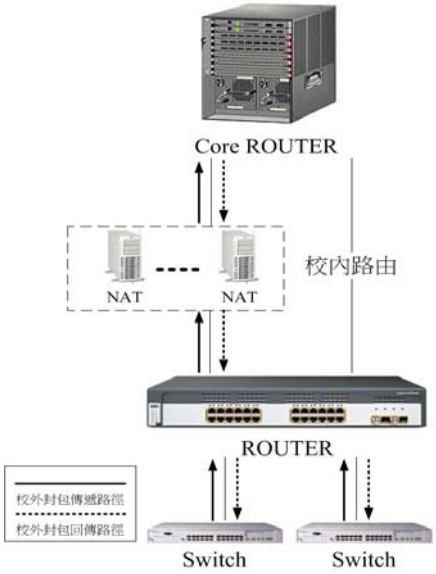

圖 7

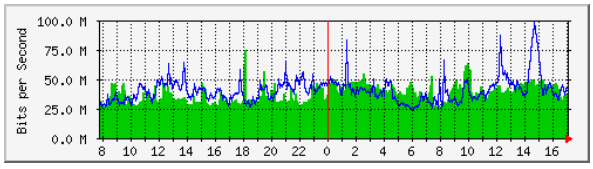

圖 8

圖 9 和圖 10 分別為兩個不同 NAT 設備端的流量圖，由圖可看出兩台設備的流量大致相等，所以這樣的架構確實可以達到分流的目的，頻寬加倍的結果，彼此達到備援的功能。

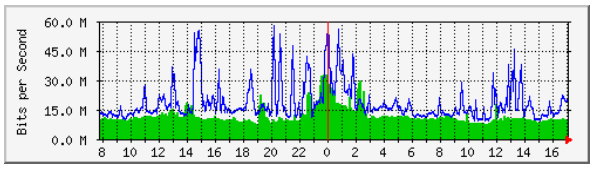

圖 9

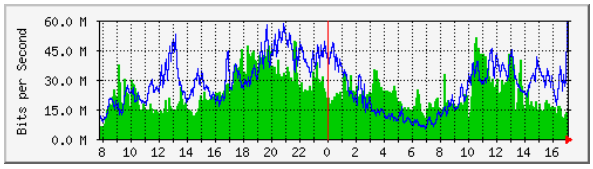

圖 10

4. 結論

這樣架構確實能解決本校學生宿舍網路的問題，採用後宿舍網路擁塞的情形不見，學校的 MRTG 圖可以看出宿舍的流量大約有 110Mb/s 與我們當初規劃時，所預估相當，而且這樣的架構足以應付學生宿舍網路的需求，整體設備加起來不到 30 萬，卻有百萬等級的頻寬，而且也有備援的功能，值得有需要的同伴試試。

由於宿舍使用 NAT 方式對外連線，因此有些網站會封鎖這些 NAT 設備的 IP，原因是因為有太多連線數來至相同 IP，被誤認為是攻擊，通常我們要跟網站的管理者通知這樣的情形，解決方式可以將單一位址改為 NAT POOL 方式，不過 IPcop 不支援這樣的功能。

至於流量監測部份，宿舍網路中使用 3750 做為路由器，我們只要對出 WAN 的 VLAN 部份做 mirror 就能對宿舍網路做 IP 流量的限制。

學生宿舍網路是所有學校管理者的痛，如何讓宿網正常的運作，是網路管理者需要面對的，希望這篇文章能協助有相同需求的人。

參考文獻

[1] http://www.cisco.com/
[2] http://www.faqs.org/rfcs/rfc1631.html
[3] http://www.ipcop.org/
[4] http://www.secureneed.com/ipcop/