基於使用者分群的校園網路頻寬管理系統設計與實作

林保庭
國立中興大學資訊科學與工程學系
katz.lin@msa.hinet.net

高勝助
國立中興大學資訊科學與工程學系
sjkso@cs.nchu.edu.tw

摘要

校園網路環境下常見的網路頻寬使用問題有：(1)P2P 使用者造成頻寬資源濫用(2)即時性服務因沒有頻寬保證造成使用效果不彰(3)同區段多人同時上網造成低優先權使用者保證頻寬被佔用，而目前普遍使用的頻寬管理方法無法有效的解決上述問題。本論文提出基於使用者分群的頻寬管理架構，先將使用者分成三類，透過三部頻寬管理器，給予各類使用者不同的保證頻寬及優先權，採用允入機制保障已連線使用者皆可獲得最小保證頻寬，子網路間並可藉由頻寬借用演算法，動態借用剩餘頻寬。系統實作顯示可有效限制 P2P 的使用者，對即時性服務以及已連線的低優先權使用者提供最小保證頻寬，並且經由子網路間剩餘頻寬借用的實作，有效提昇頻寬使用率。

關鍵詞：校園網路，頻寬管理，即時性服務，P2P。

Abstract

The common network bandwidth using problems under a campus network environment are as follows: (1) the bandwidth resources abuse caused by P2P users, (2) the use of the real-time services is unsatisfactory without bandwidth guarantee, and (3) many people are surfing the internet at the same segment at the same time, resulting in the bandwidth of lower priority users is preempted; presently, the generally used bandwidth management method can not solve the above-mentioned problems effectively. The dissertation proposed the bandwidth management framework based on user clustering, divided the users into three categories, gave the users of each category different guaranteed bandwidth and priority via three bandwidth management devices, adopted the admission control mechanism to ensure that the users who are already online can get the minimum guaranteed bandwidth, and the excess bandwidth can be borrowed dynamically among the subnets by means of bandwidth borrowing algorithm. The system implementation showed that it can restrict P2P users effectually, provide the minimum bandwidth guarantee for the real-time service and the low priority users that are already online, and promote the bandwidth utility rate efficaciously through the implementation of excess bandwidth borrowing among subnets.

Keywords:Campus network, bandwidth management, real-time service, P2P.

1. 前言

本單元將區分為以下章節敘述如下：1.1 節探討校園網路頻寬管理的現況及問題，1.2 節敘述本論文的研究動機，1.3 節說明本論文的章節大綱。

1.1 現況概要

隨著網路科技的普及發展，加上政府對校園資訊化的重視與推廣，現今國內的校園中幾乎都已建置有線網路環境，甚至許多學校也已建置無線網路環境，網路基礎建設的普及化對於校園整體教學品質及行政效率的提升有明顯的助益。然而，近年來網際網路上的服務發展迅速，愈來愈多樣化的網路服務以及日漸便宜的電腦與週邊設備的價格，使得校園網路的使用者及電腦設備的數量不斷增加，造成原來有限的校園網路頻寬開始呈現捉襟見肘的情形。目前校園網路主要的頻寬管理問題如下：

■未規劃使用者頻寬管理機制

網路 BE(best-effort)的 IP 封包傳送機制會讓少數喜歡私下使用 P2P(peer-to-peer)軟體的使用者佔用了大多數的頻寬，如果有數個使用者同時進行 P2P 下載時，很容易造成該網段頻寬的擁塞，同時造成其他網路使用者無法獲得正常的網路服務品質。這種不公平、沒有控管的網路使用方式需要一套有效的使用者頻寬

管理機制來預防[1][2]。

■即時性服務(real-time service)無法保證頻寬

在政府大力推動行政及教學資訊化政策下，愈來愈多的教師開始嘗試運用資訊媒體科技融入教學中，比如運用網路線上影音多媒體影片融入教學，學校行政單位也開始採用網路電話與傳統電話並用的方式來節省電話費。然而，由於 VoIP(Voice over Internet Protocol)及影音串流(Video streaming)這些網路即時性服務對於連線品質的要求較高，一旦網路發生擁塞時，如果沒有事先針對這些即時性服務予以保留足夠的頻寬，服務的品質將會受到影響而無法正常運作[3]，這些影響也將讓使用者運用這些服務的意願大為降低。

■網路架構未經妥善規劃

校園網路環境中，行政區的使用者眾多，行政業務對於校務運作有著重要的影響，加上行政業務使用者使用網路的頻率最高、時間最長、使用的網路服務類型也最廣，因此最需要保持網路暢通；教學區的網路使用者主要是教師，同一時段的使用者不多，但其使用網路的目的主要是於課堂中進行資訊融入教學，因此也需維持一定的網路品質；電腦教室區主要的網路使用者為學生，使用網路的人數最多，但通常會有集中在固定的時段上網的特性，使用的網路服務類型也較少，相較於行政區及教學區的使用者而言，對於網路的迫切性較低。然而，由於校園網路在建置時若未經妥善的規劃，常會造成多數使用者集中在同一區域或同一時段使用網路的情形，該網段的網路設備就容易發生頻寬擁塞，造成使用者的上網速度變得緩慢，進而影響到行政及教學的正常進行。

■頻寬管理備設備功能不足

大部份學校採用上級單位配發的網路設備進行運用，然而配發的設備多屬具備頻寬管理功能的防火牆，在頻寬管理的功能上明顯不足。而市面上功能較強的中高階頻寬管理器，價格動輒數十、數百萬，一般學校礙於經費有限，也無法加以採購來運用[4]。

1.2 研究動機

校園網路頻寬管理的相關研究方向大多以 HTB(Hierarchical Token Bucket)佇列演算法實作在單一頻寬管理器，其動態頻寬借用功能多是運用 HTB 的 Link- Sharing 機制針對不同類別(class)間進行動態借用[4][5][6]，然而 HTB 演算法效能雖較 CBQ(Class Based Queuing)高[7]，但若在類別上設定太多的頻寬借用，容易造成頻寬借用過於頻繁，使系統的運作負載加重[8]。採用多台頻寬管理器分層管理的架構[9]可有效解決單一頻寬管理器負載的問題，然而在子網路頻寬借用演算演及 CBQ 演算法上還有可改良之處。另外，以上研究皆未採取允入控制機制(admission control)對網路上的使用人數上進行控管，一旦使用者過多時，也無法有效保障使用者的保證頻寬[10]。

本論文著眼於解決現今校園網路的頻寬運用及管理問題，對於 P2P 的使用者能有效的管制其頻寬；對於即時性的網路服務要能保證頻寬，並給予較高的優先權(priority)，使服務能正常的運作；對於不同等級的使用者要有不同的保證頻寬外，即使是低優先權的使用者在網路繁忙的情形下，仍可獲得維持上網正常運作的最小保證頻寬；對於頻寬不足的網段能夠借用頻寬多餘網段的頻寬使用。在不變更現有校園網路架構，及考量學校經費有限的原則下，我們採用免費的作業系統及軟體，使用一般的電腦設備來建置系統，以期達到同樣的效果。

本論文參考論文[9]的方法，提出基於使用者分群的頻寬管理架構，事先針對校園網路使用者的類型、每小時平均使用者人數，以及使用網路的特性進行分析，將使用者分成三個群組：行政、教師及學生，每個群組各自劃分於一個子網路，每個子網路由一台頻寬管理器進行控管以減輕系統負載。針對網路上同一時間的使用人數使用允入控制機制，以確保每種類型的使用者不論何時上網，皆可獲得最小保證頻寬。改良子網路頻寬借用演算法運用在頻寬管理器上，以設定每個子網路的最大可借出頻寬及借用優先權，避免使用者較少，子網路頻寬多餘時造成的浪費，並保證高優先權使用者能借得較多的剩餘頻寬。此外，採用一台頻寬管理主控台，以網頁介面提供管理者設定子網路及使用者的頻寬參數，並藉以了解每個子網路使用者的登入情形、子網路的頻寬借用情形、以及子網路的即時上下載流量，以方便管理者對於所有子網路的頻寬管理器進行集中式的管理。

1.3 章節大綱

本論文的架構說明如下：第 1 章敘述本論文的研究動機及目的，第 2 章介紹本論文所需的相關背景，包括：頻寬管理器的簡介、Linux 的 QoS 機制、核心處理封包的流程、HTB(Hierarchical Token Bucket)佇列演算法、Link-Sharing 機制、Iptables 及 Netfilter 介紹、允入控制機制、串流多媒體。第 3 章就本論文提出的頻寬管理架構及組成元件做詳細的介紹，第 4 章為系統實作及操作介面介紹，第 5 章介紹系統的測試環境，並針對測試的項目及結果做說明。第 6 章對本論文所提之頻寬管理系統作歸納總結，並提出未來可繼續研究的方向。

2. 主要內容

為了有效管理頻寬資源，Internet Engineering Tast Force(IETF)提出許相關的研究和方法，如採 IntServ[11]及 Diffserv[12]的架構來解決，然而這些方法需要網路上的設備皆支援相同的機制才能有效達成，對於一般中小型單位而言實施的困難度較高，而以網路匣道器為基礎的頻寬管理架構，只需在單一設備上建立頻寬管理機制，就可以有效達成對使用者的頻寬管理目的，許多研究也相繼針對在 Linux 上實施頻寬管理進行探討。

本單元將於 2.1 節介紹有關校園網路頻寬管理的相關論文，2.2 節介紹頻寬管理器的概念及原理，2.2 節詳細說明 Linux 的 Qos 機制，2.3 節介紹 iptables 及 Netfilter 的語法及功能，2.4 節對允入控制機制做說明。

2.1 頻寬管理器簡介

網路上的資料是以封包(packet)的型式傳送，不同類型的網路服務會產生不同的封包，但因目前網路傳輸採 best-effor 方式，依網路負載狀況以最佳傳輸量及速率傳送資料，資料封包可能會延遲(delay)或遺失(loss)，因為沒有優先順序的關係，各種服務的封包在會競相搶奪網路頻寬，造成服務品質無法保證。當頻寬擁擠時，就好像是連續假期的高速公路上，各式各樣的車子湧上高速公路造成大塞車一樣。

頻寬管理器的概念就是將頻寬劃分成不同的傳輸路徑，讓不同類型的封包依據規劃好的路徑傳輸，就像在高速公路上劃分不同的專用道，讓慢速車走慢車道，高速車走快車道，救護車走緊急車道一樣，目的是要在有限的頻寬資源內，讓網路頻寬發揮最大的效用。

2.1.1 頻寬管理器的位置

目前大多數校園頻寬管理器的架設位置[8]常置於 Internet 與 LAN 之間，用於對於內部所有使用者的頻寬進行集中管理，如圖 2-1 所示；另外也可以架設於內部網路瓶頸處，用來對網路瓶頸處的頻寬進行控管，如圖 2-2。

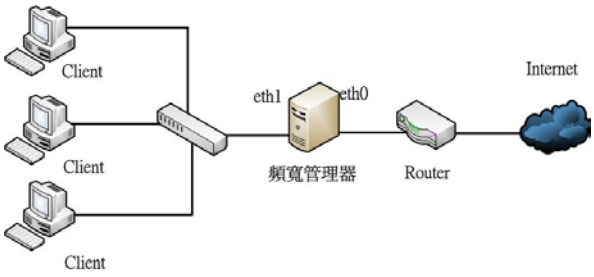

圖 2-1 頻寬管理器置於 Internet 與 LAN 之間

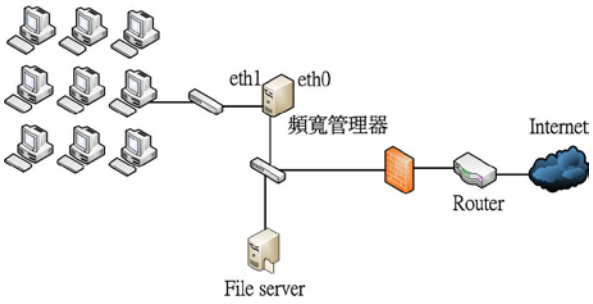

圖 2-2 頻寬管理器置於 LAN 內

2.1.2 頻寬管理器運作原理

頻寬管理器的運作過程如圖 2-3，首先利用分類器(packet classifier)對網路封包做分類，分類的方式可依據 IP address、Port number、Protocol type，分類後的封包會被送至不同的佇列(queue)中等待傳送，之後會依規劃好的排程從佇列中被取出處理，最後則是對封包進形整形的工作，調整封包的傳送速率以避免擁塞。

圖 2-3 頻寬管理器的運作過程

2.2 Linux 的 Qos 機制

Linux自核心版本2.1.90 後開始提供流量控制架構[12]，如圖2-4。架構中包含了三個重要的元件：Queueing Discipline、Class、與Filter，我們可以利用這三個元件的組合變化來設定各種頻寬管理策略。

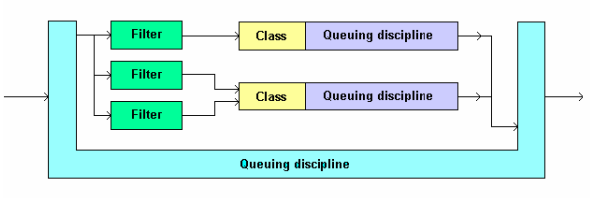

圖 2-4 Linux 的 Qos 機制

以下為三個元件的介紹：

- Qdisc

Qdisc(Queuing Discipline)是佇列規則的縮寫，主要的功能為決定封包排程及傳送方式，它本身就是一個佇列演算法。核心要對外發送封包時，會依照網路介面所配置的Qdisc的演算法來處理封包，比如決定封包送出的先後順序，或是丟棄(drop)該封包等處理動作。目前Linux 核心中提供了許多不同的Qdisc，如FIFO、WRR、SFQ、CBQ、HTB…等，部份的Qdisc如CBQ、HTB內部可再劃分成多個Class，組成階層式的架構。

- Class

Class為類別，可以將它視為一個邏輯群組。在某些Qdisc中可以包含一些類別，並且可以針對每個類別設定不同的屬性，不同的頻寬。最底層的類別可以有自己的Qdisc，當封包經由Filter歸類到該類別時，就能以自己的Qdisc方式將封包傳送出去，因此，透過不同類別以及其下不同Qdisc的組合，就可以彈性的產生不同的頻寬管理方式。

- Filter

主要的功能為將封包檔頭(Header)依Filter設定的規則進行過濾，並且送到不同的類別中產生分類的效果。Linux核心在Filter中提供了許多分類器來做封包過濾，如fw、u32、rsvp、rsvp6…等。

fw分類器可以與iptables配合，利用 iptables先對特定的的封包進行標識，再由fw分類器進行分類。fw分類器的指令範例如下：

```
tc filter add dev eth1 parent 10: protocol ip prio
100 handle 10 fw classid 10:10
```

2.2.1 Linux核心處理封包流程

如圖2-5所示，當封包進入到輸入介面(Input Interface)時，會先傳送到輸入多路分配器(Input De-multiplexing)，如果是要送往本機的封包，則會被送到Upper Layers層處理，再依封包的類型分別送給相對應的應用程式處理。如果目標位址不是本機的封包，則會先送到Forwarding，由Forwarding負責選擇輸出的介面，決定封包的下一個目的，然後封包會被送到Output Queuing中等待被提取，而Linux的Traffic Control主要也是對Output Queuing的封包做處理，如排隊、丟棄、延遲…等，進而達到流量控制的功能。

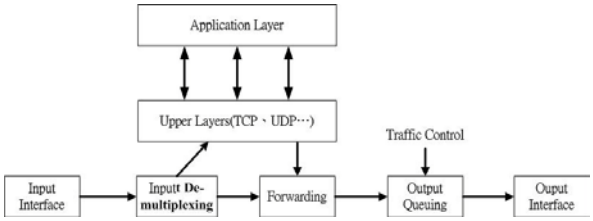

圖 2-5 Linux 核心處理封包流程圖

2.2.2 HTB

HTB[13]是CBQ[14]的改良版本，兩者皆可實現Link Sharing架構，然而HTB較CBQ有更多的優點，如：對於頻寬的保證準確性比CBQ好，可以保證每個類別的最小頻寬及最大頻寬，同一層級類別數增加時，處理封包的時間較短，在參數的設定上也較CBQ來的簡單。

HTB的相關參數介紹如下：

- rate：用來設定class的基本保證頻寬，在設定上所有子類別(child class)的rate總和須小於或等於其父類別(parent class)的rate值。
- ceil：用來設定class的最大頻寬，當ceil的設定值大於rate的設定值時，等於設定class外借頻寬的範圍為rate減ceil的值。
- prio：是priority的縮寫，可以實現對流量進行優先順序管理，只有高優先順序類別的封包全部發送完畢，才會發送低優先順序類別的封包。Prio的值從0~7，預設為0，當有多個class競爭剩餘頻寬時，prio值最低的將佔用所有剩餘頻寬。
- default class：當封包不符合所有filter設定的規則時，會被導入預設的類別中。

2.2.3 Link Sharing

Link Sharing 機制是由 Sally Folyd 於 1993

年提出[15]，主要的目的在於有效分配頻寬給類別中的每一個使用者，並且結合可分類的佇列規則，建立階層式的連結共享架構，讓不同類別的頻寬能夠彈性的被運用。

假設有 3 個使用者 A、B、C，各分配到總頻寬的 30%、50%、20%，而每個 user 又依應用程式不同的需要，將頻寬分配給不同的應用程式使用，如圖 2-6。當 user B 發起 real-time 服務時，系統即動態的分配符合該 real-time 服務頻寬需求的頻寬給 user B，並且將 user B 的使用者等級提昇為 real-time 服務使用者所設定的頻寬 50%。一旦 user B 停止該網路 real-time 服務，系統即立刻將分配給該 real-time 服務的 20%頻寬收回，並將 user B 的使用者等級降為原本的使用者等級及該等級最大的可用頻寬 30%，以以將未使用的即時性服務 20%的頻寬提供其他應用程式及使用者使用。

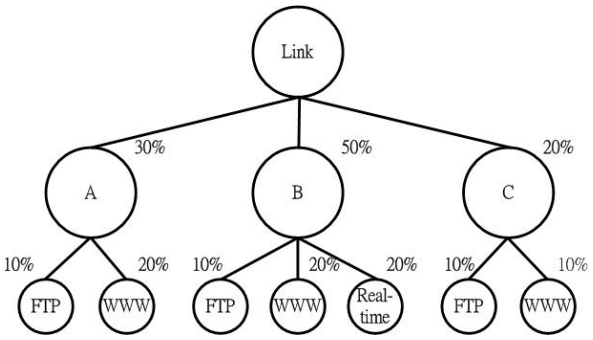

圖 2-6 Link Sharing 架構

2.3 Iptables& Netfilter

在Linux 2.4以上的版本已將iptables[16][17]及Netfilter加入核心中。iptables是屬於應用層的使用者介面，讓使用者將防火牆規則加入Netfilter中，讓系統依使用者設定的規則過濾封包。iptables定義了幾個不同的table， nat可以用來轉譯封包位址資訊、mangle用來修改或標註封包、filter用來過濾通過本機的封包，每個table中又包含許多內建的規則鏈(chains)，包括PREROUTING、INPUT、FORWARD、OUTPUT、POSTROUTING分別對應到Netfilter的五個檢查點(HOOK)，如圖2-7。

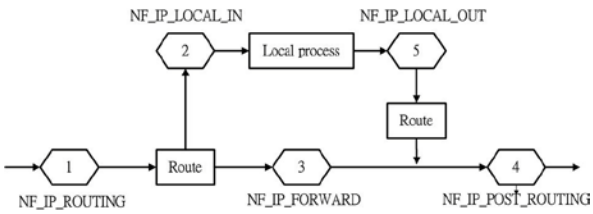

圖2-7 Netfilter的五個檢查點

當封包符合規則鏈設定的過濾規則時，就可以對封包做相對應的處理。iptables的使用範例如下表2-1：

表2-1 iptables使用範例

#iptables –t nat –A PREROUTING –p tcp –dport 80 –s 192.168.10.0.24 –j DNAT –to 163.x.x.x:80 說明：將來自192.168.10.0網段，目地port為80的封包改變封包位址至163.x.x.x的80port。 #iptables –t nat –A POSTROUTING –s eth1 –o eth0 –j MASQUERADE 說明：將來自網卡eth1，到網卡eth0離開的封包做NAT。

2.3.1 L7-filter

L7-filter[18]是Netfilter的分類器，主要是針對OSI模型的第七層，也就是應用層的網路服務所設計，可以對每個封包所使用的通訊協定做分類 ，讓Netfilter對特定的通訊協定進行阻擋或頻寬控管。它採用字串比對的方式辨識封包，當一個連線建立時，會分析該連線的前八個封包，當封包分析後的內容與系統內建的特徵值符合時，便在connection tracking[19]模組相對應的連線記錄標記應用程式的名稱。L7-filter支援的protocol類型有很多[20]，對於Video streaming、VoIP支援的協定如表2-2。表2-3為採用L7-filter針對應用層的網路服務程式進行封包阻擋的iptables指令範例。

表2-2 L7-filter支援即時性服務的協定種類

Streaming video	http-rtsp、rtp、rtsp、pplive
VoIP	h323、skypeout、skypetoskype、teamspeak、ventrilo

表2-3 L7-filter封鎖skypetoskype的指令範例

#iptables -A FORWARD -m layer7 --l7proto skypetoskype -j DROP

2.4 允入控制機制

對於有QoS要求的網路系統而言允入控制機制是相當重要的，如果將網路頻寬以公速公路做比喻的話，允入控制就好比匝道管制系

統，當網路處於重負載的情況下，需要有允入控制系統根據系統的狀況，決定是否讓新的使用者進入系統，以保障已連線使用者的QoS品質，避免系統超出負載（overload）。

在這裏我們先對允入控制做一個簡單的描述：當收到一個要求建立新的連線的封包時，必須考慮已建立的連線目前所佔用的系統資源，扣掉這一部份，即是系統所剩餘的能提供給新的連線使用的資源，假設剩餘的資源能夠滿足新的連線的要求，就會允許建立，反之，就必須拒絕（reject）新的連線建立。

如果系統允許超過它可以容納的連線建立，這些連線會彼此競爭系統資源，且系統在同一個時間內將會收到大量的封包，卻無法馬上進行處理，這些無法馬上被處理的封包會被暫存在buffer中，一直到buffer無多餘的空間，則接下來的封包將會被丟棄，對於即時性服務的封包來說，對於延遲相當的敏感，buffer如果時間過久，造成delay時間過久，便無法滿足服務所要求的QoS。對於非即時性服務來說，一旦有封包被丟棄，使用者和伺服器之間必須重新傳輸流失的封包，如此一來將會造成網路資源的嚴重浪費。

相反的，若是系統只允許少數的連線建立，則大部份的系統資源都會處於閒置（idle）的狀態，卻有許多的使用者在等待系統允許他們的連線建立，雖然如此可以減低傳輸失敗的機會，但是系統的資源將無法充份的被利用。綜合上述的說明，我們可以知道，一個最理想的允入控制機制應該在不影響服務品質下，盡可能的充份利用系統資源，允許最多的連線建立。

3. 系統架構

本單元將分為以下章節分別敘述，第 1 節針對系統架構及系統運作流程做詳細的說明，第 2 節則對本系統的各個模組功能做介紹。

3.1 系統架構說明

圖 3-1 為本論文提出的基於使用者分群的頻寬管理架構，其中包含三個子網路 subnet1、subnet2，及 subnet3、一個頻寬管理主控台，以及三台頻寬管理器。三個子網路中分別擁有不同數量的電腦及使用者，連接到各自的 Layer2 switch 上，最後再連接到各子網路的頻寬管理器，由這三台頻寬管理器進行該子網路下所有使用者的網路服務及頻寬控管工作。

Subnet1 劃分作行政區，Subnet2 劃分作教學區，Subnet3 劃分作電腦教室區。

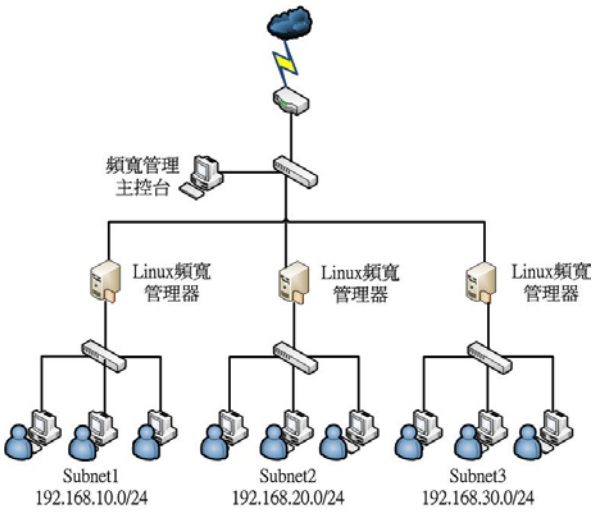

圖 3-1 分散式頻寬管理架構圖

以下為針對頻寬管理主控台、頻寬管理器的詳細說明。

3.1.1 頻寬管理主控台

頻寬管理主控台的主要功能為利用 WEB 介面，讓管理者設定各子網路的可用網路服務，如：WWW、FTP、SSH 等，設定子網路的頻寬配置及借用規則，如：最大上傳及下載頻寬、最大可借出頻寬、借用優先權，設定使用者及即時性服務的保證上傳及下載頻寬、最大上傳及下載頻寬、優先權。另外，頻寬管理主控台每隔五秒鐘會自動捉取三台頻寬管理器的流量資料，經過計算後顯示目前各子網路的上傳及下載流量，同時顯示各子網路的使用者登入人數，方便管理者了解實際的網路流量及子網路頻寬借用情形。

3.1.2 頻寬管理器

頻寬管理器主要採 NAT[24]模式，以 DHCP 配發下層使用者的 IP 位址，並負責接收頻寬管理主控台的頻寬管理及防火牆配置規則，以管理下層使用者的網路頻寬及網路服務。當下層子網路的使用者開啟瀏覽器時，會自動將網路連線 redirect 至使用者認證畫面，使用者輸入的帳號、密碼經過與使用者資料庫比對無誤後，頻寬管理器會下達 iptables 指令，開啟該使用者網路位址的對外連線封鎖限制，並依照該子網路使用者允許使用的網路服務功能及流量限制，限制該使用者的可用網路

服務及流量。系統的詳細運作流程如圖 3-2。

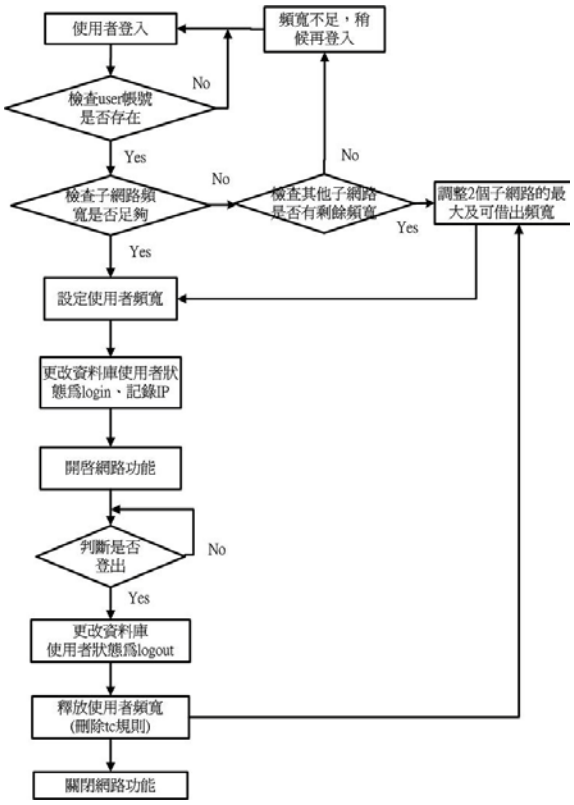

圖 3-2 系統運作流程圖

3.2 模組功能說明

本論文在實作上總共包含六個模組，模組架構如圖 3-3。

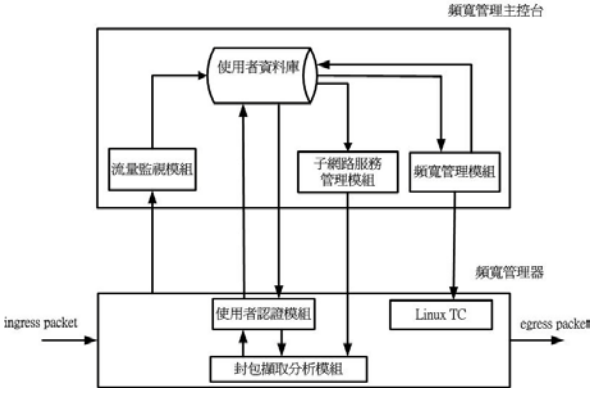

圖 3-3 模組功能架構圖

3.2.1 封包擷取分析模組

主要的功能為將使用者的網路連線 redirect 至使用者認證模組，分析進入頻寬管理器的封包資訊，判斷封包來源所屬於的網路服務類別或來源 IP 位址，加以分類後由頻寬管理器限制網路服務或使用者頻寬。

3.2.2 使用者認證模組

接收來自頻寬管理器的使用者認證要求，以 Web-base 的方式，提供使用者輸入認證資料並與使用者資料庫比對，認證成功後再與頻寬管理模組上的使用者保證頻寬及子網路最大可用頻寬資料比對，若該子網路的頻寬足以配置給該使用者，即在資料庫中記錄該使用者的名稱、網路位址、使用者保證頻寬，及登入狀態。

3.2.3 流量監視模組

流量監視模組建置於頻寬管理主控台上，每隔 5 秒鐘以 awk[25]指令週期性的擷取各子網路頻寬管理器對外網卡的流量資訊，經過計算後顯示目前各子網路的下載及上傳流量於頻寬管理主控台，方便管理者即時監控子網路的流量狀況。

3.2.4 子網路服務管理模組

子網路服務管理模組建置於頻寬管理主控台上，將管理者於頻寬管理主控台設定的各子網路使用者允許使用的網路服務，設定到各子網路的頻寬管理器，用來限制使用者可用的網路服務。

3.2.5 頻寬管理模組

頻寬管理模組建置於頻寬管理主控台上，用來設定子網路、使用者、即時性服務的保證上傳及下載頻寬、最大上傳及下載頻寬、優先權，子網路的最大可借用頻寬及借用優先權，並套用至各子網路的頻寬管理器。每個使用者登入時，使用者認證模組會確認頻寬管理模組的子網路頻寬配置情形，若該子網路頻寬已不足以借用，會依各子網路的頻寬借用優先權向其他有多餘頻寬的子網路借用，並將更新的子網路頻寬配置參數重新設定至頻寬管理器。

3.2.6 子網路頻寬借用演算法

假設骨幹網路的總頻寬為 Bw，有三個子網路 s1、s2、s3，每個子網路的預設的最大頻

寬為 Bw_s1、Bw_s2、Bw_s3，每個子網路使用者群組預設的保證頻寬為 Ubs1、Ubs2、Ubs3。在時間為 ti 時，每個子網路的實際上線總人數為 Ns1(ti)、Ns2(ti)、Ns2(ti)，ti 時每個子網路使用的總保證頻寬為 $B_{guarantee}$-s1(ti)、$B_{guarantee}$-s2(ti)、$B_{guarantee}$-s3(ti)，在一般未使用即時性服務的情形下：

$B_{guarantee\_}s1(ti)= \sum_{j=1}^{n} Ns1(ti)$*Ubs1-----(1)

$B_{guarantee\_}s2(ti)= \sum_{j=1}^{n} Ns2(ti)$*Ubs2-----(2)

$B_{guarantee\_}s3(ti)= \sum_{j=1}^{n} Ns3(ti)$*Ubs3-----(3)

假設 ti 時在 s1 內有 M 個使用者發起即時影音串流服務，有 L 個使用者發起 VoIP 服務，Streaming Video 的預設保證頻寬為 $B_{streaming}$，VoIP 的預設保證頻寬為 B_{VoIP}，這時子網路 s1 的總保證頻寬為：

$B_{guarantee\_}s1(ti)= \sum_{j=1}^{n} Ns1(ti)$*Ubs1+$\sum_{j=1}^{n} M(ti)$ * $B_{streaming}$+$\sum_{j=1}^{n} L(ti)$* B_{VoIP} -----(4)

此時會有兩種情形，當有新使用者登入時，假設子網路 s1 在 ti 時間的總保證頻寬 $B_{guarantee}$-s1(ti)≤子網路 s1 的預設的最大頻寬 Bw_s1 時，也就是 Bw_s1- $B_{guarantee}$-s1(ti) ≥0，代表該子網路的頻寬足以供使用者的保證頻寬使用，因此子網路頻寬借用機制將不會運作，該使用者可成功登入。若是 $B_{guarantee}$-s1(ti) > Bw_s1 時，也就是 Bw_s1- $B_{guarantee}$-s1(ti)<0，代表子網路 s1 的預設最大頻寬已不足以提供該子網路下使用者及服務的總保證頻寬，這時子網路頻寬借用模組將依照以下式子來實施子網路間的頻寬借用。

$B_{borrow\_}s1(ti)= B_{guarantee}$-s1(ti) – Bw_s1-----(5)

$B_{borrow_}s1(ti)$為子網路 s1 在 ti 時，需向其他子網路借用的頻寬。之後，子網路頻寬借用模組尚需利用以下式子檢查其他子網路是否有剩餘頻寬足以借用。

Bw_s2- $B_{guarantee}$-s2(ti) ≥ $B_{borrow_}$s1(ti)-----(6)

Bw_s3- $B_{guarantee}$-s3(ti) ≥ $B_{borrow_}$s1(ti) ----- (7)

我們依照各個子網路的不同的重要性給予 0~2 的優先權值，0 代表最高優先權，2 代表最低優先權，優先權值高的可以向較低優先權的子網路借用頻寬，另外，我們也設定各子網路的最大可借出頻寬，分別為 B_{lend} _s1、B_{lend} _s2、B_{lend} _s3。假設子網路間優先權順序為 s1>s2>s3，則 s1 可向 s2、s3 借用頻寬，s2 可向 s3 借用頻寬，而 s3 則不可借用其他子網路的頻寬。假設這時候子網路 s2 及 s3 皆有多餘的頻寬可借用，因 s3 的優先權較低，所以 s1 會優先向 s3 借用頻寬，子網路 s3 在 ti 時的新頻寬為 NB_s3(ti)，子網路 s1 借用頻寬後的新頻寬變成 NB_s1(ti)。子網路頻寬借用模組會將計算出來新的子網路最大頻寬設定給有變動的子網路 s1、s3，完成子網路間的頻寬借用。

NB_s3(ti)=Bw_s1- $B_{borrow_}$s1(ti)-----(8)

NB_s1(ti)=Bw_s1+ $B_{borrow_}$s1(ti)-----(9)

此時 s3 的最大可借出頻寬 $B_{lend_}$s3(ti)就會變成

$B_{lend\_}s3(ti)= B_{lend}$ _s3- $B_{borrow_}$s1(ti)-----(10)

3.2.7 允入控制機制

允入控制流程如圖 3-4，若 s1 仍有新的使用者要登入，而 s1 的頻寬仍不足以分配給新使用者時，則會先判斷 s3 的最大可借出頻寬是否仍足夠，若 s3 已不足夠，則會依序向 s2 借用。若在 ti 時其他的子網路的頻寬皆不足以借用，則系統會給予新登入者一個警告訊息，告知目前的頻寬已滿載，請稍候再登入。

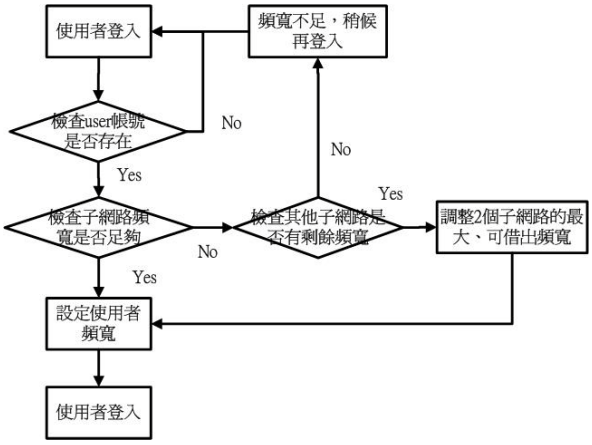

圖 3-4 允入控制流程圖

4. 系統實作

本章節的 4.1 節將介紹本系統的開發平台；4.2 節說明頻寬管理主控台管理介面的操作方式；第三小節說明頻寬管理器的相關設定及功能。

4.1 系統環境

為了證實本論文所提出的方法在校園網

路環境中的可行性，在實作部份採用一般的電腦設備來安裝系統，捨去學校難以使用的高階網路伺服器。頻寬管理主控台以及頻寬管理器的規格如下：CPU-Intel Celeron 2.4G、記憶體 512MB、作業系統為 Fedora Core 9。

頻寬管理主控台提供管理者以 PHP 程式製作的 Web 操作介面，需啟動 Apache 服務並安裝 Mysql 資料庫，此外，頻寬管理主控台與三台頻寬管理器之間需具備不用密碼即可以 ssh 相互登入的功能[26]。頻寬管理主控台安裝的相關模組及套件如下：

- linux-2.6.25
- php 5.2.9
- mysql 5.0

頻寬管理器採 NAT 模式，並以 DHCP 配發 IP 給子網路的使用者，因此需另外設定 NAT 及 DHCP，另外為了使系統支援 Layer7-filter 功能，頻寬管理器的核心必需重新編譯，並安裝 L7-filter 相關模組。本系統實作所重新編譯及安裝的相關套件及模組如下：

- linux-2.6.25
- Iptables-1.4.2
- netfilter-layer7-v2.20
- l7-protocols-2009-05-28

4.2 頻寬管理主控台實作

管理者在輸入頻寬管理主控台的 IP 位址後，會先進入管理者登入畫面，需輸入正確的管理者帳號、密碼後才可以登入，登入畫面如圖 4-1。

圖 4-1 頻寬管理主控台-登入畫面

登入後，需先在子網路設定頁面中設定三個子網路的名稱及頻寬管理器的 IP 位址，因頻寬管理器安裝二塊網路卡，一張對外，一張對內，這裡的 IP 位址是指對外的真實 IP 位址。對內 IP 位址已於程式中預設為 192.168.10.254、192.168.20.254 及 192.168.30.254，所以不需設定。子網路設定畫面如圖 4-2。

圖 4-2 頻寬管理主控台-子網路設定畫面

接著管理者可以在使用者帳號設定頁面中新增、刪除或修改不同子網路使用者的帳號及密碼。設定畫面如圖 4-3。

圖 4-3 頻寬管理主控台-使用者帳號設定畫面

Qos 設定畫面如圖 4-4，主要可分為四個設定項目，分別敘述如下：

■ **子網路頻寬設定**

用來設定每個子網路的最大下載、最大上傳頻寬、最大借出頻寬，以及借用優先權，借用優先權的數字愈小，代表優先權愈高，優先權愈高的子網路可以向優先權低的子網路借用最大可借出頻寬。

■ **子網路頻寬細部設定**

用來設定各子網所有使用者，以及即時性服務的保證下載、最大下載、保證上傳、最大上傳頻寬以及優先權值，也就是 TC 樹狀架構中第 2 層的參數值，如 subnet1-user 的保證下載頻寬為 4500k，最大下載頻寬為 9000k，優先權值為 1，subnet1-service 的保證下載頻寬為 4500k，最大下載頻寬為 4500k，優先權值為 0，代表 subnet1 的使用者當即時性服務未用到 4500k 時，可以借用即時性服務的頻寬，最大可用到全部 9000k 的頻寬，然而因即時性服務的優先權值較高，一旦即時性服務使用時，可

以優先保證使用到 4500k 的頻寬，但無法超過 4500k。

■ **使用者群組頻寬設定**

用來設定各子網路中單一使用者的保證下載、最大下載、保證上傳、最大上傳頻寬、以及優先權值，也就是 TC 樹狀架構中的最底層參數，優先權值是用來和單一使用者的即時性服務的優先權值做比較。如 subnet1 的使用者保證下載頻寬 150k，代表單一使用者的保證下載頻寬為 150k，最大下載頻寬 9000k，代表使用者在頻寬多餘的情況下，最多可使用整個 subnet1 的所有頻寬，而其優先權值為 1，代表當使用者同時使用一般網路服務與即時性服務時，由於即時性服務的優先權值為 0，所以，即時性服務可以優先得到保證頻寬。

■ **即時性服務頻寬設定**

用來設定即時性服務的保證下載、保證上傳、最大下載、最大上傳頻寬，在這裡我們僅設定二種常用的即時性服務：Video streaming 及 VoIP，由於 Video streaming 通常需要較大的頻寬才可保證觀看時的流暢度，所以我們設定保證頻寬及最大頻寬為 100k，VoIP 的部份我們設定 50k，即時性服務的優先權值皆為 0，以使即時性服務擁有最高優先權。

圖 4-4 頻寬管理主控台-Qos 設定畫面

在網路服務設定頁面，可以針對不同子網路來設定使用者可用的網路服務類型，預設可使用的網路服務類型有 HTTP、FTP、POP3、SMTP、SSH、VoIP 及 Video streaming。在尚未套用網路服務設定前，頻寬管理器預設規則為拒絕所有對外連線，當按下更新鈕時，會將新的規則分別套用至三個子網路的頻寬管理器中。網路服務設定的畫面如圖 4-5。

圖 4-5 頻寬管理主控台-網路服務設定畫面

在頻寬使用狀況頁面顯示每個子網路目前的登入人數、子網路使用者的保證下載頻寬、即時性服務的保證下載頻寬、目前分配頻寬、子網路的實際上傳及下載流量。在子網路實際上傳及下載流量部份，採用 awk 指令每隔 5 秒鐘週期性的從三台頻寬管理器的 /proc/net/dev 擷取對外網卡 eth1 的流量，經過計算後顯示於畫面中[27]。透過這個畫面管理者可以清楚的了解每個子網路的登入人數，頻寬分配情形，以及實際的流量。頻寬使用狀況頁面如圖 4-6。

圖 4-6 頻寬管理主控台-頻寬使用狀況畫面

使用者登入狀況頁面，主要用來查詢不同子網路目前所有已註冊使用者的帳號、登入狀態以及使用的 IP 位址。使用登入狀況頁面如圖 4-7。

圖 4-7 頻寬管理主控台-使用者登入狀況畫面

4.3 頻寬管理器實作

為了使整體網路頻寬能有效分配，我們事先針對校園網路中的使用者進行統計分析，如圖 4-8~10。

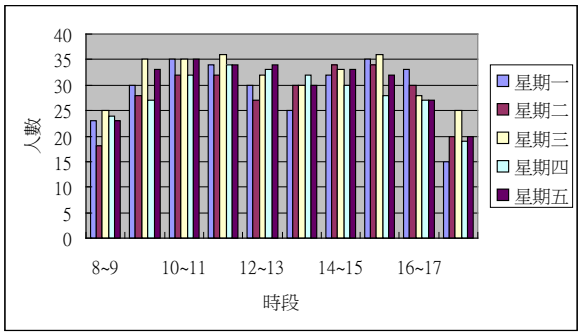

圖 4-8 行政區上網人數統計圖

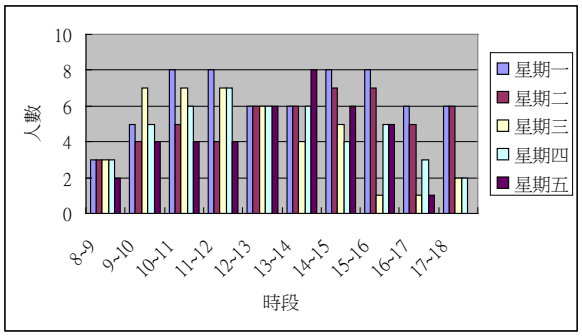

圖 4-9 教學區上網人數統計圖

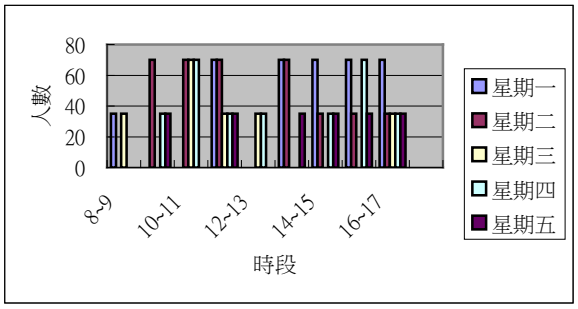

圖 4-10 電腦教室上網人數統計圖

我們將使用者依類型、每小時平均使用者人數、及使用網路的特性劃分成三種群組：行政人員、教師、學生，並將不同群組的使用者以不同的子網路區隔，每個群組預設的最大頻寬則依不同群組使用者上網的重要性、特性來分配，如 subnet1 為行政區，最大頻寬設為 9000kb，subnet2 為教學區，最大頻寬設為 1500kb，sunbet3 為電腦教室區，最大頻寬設為 9500kb，整體網路的總頻寬為 2,0000kbits。預設的頻寬規劃如下表 4-1~2。

從圖 4-8 可以發現行政區的使用者每小時上網人數較為平均，我們取每小時上網人數的平均值 30 人做為預設值。從圖 4-9 可以發現教學區的使用者於使用網路進行教學時每小時的上網人數較少，我們亦取其平均值 5 人做為預設值，從圖 4-10 可發現電腦教室區每小時的上網人數落差很大，上網人數最大值 70 人，為避免其他兩個子網路在電腦教室使用者滿載時無法借用頻寬，我們取其最大值加上 10 人做為預設值。

表 4-1 各子網路頻寬規劃表

子網路	網段	最大可用頻寬(kbits)	每小時平均上網人數
Subnet1	192.168.10.0/24	9000	30
Subnet2	192.168.20.0/24	1500	5
Subnet3	192.168.30.0/24	9500	80

每個子網路所屬使用者預設的最小保證頻寬及最大可用頻寬則依表 4-1，等於最大可用頻寬除以平均上網人數，並依不同群組的重要性給予 1~3 的優先權值，預設的使用者頻寬規劃如下表 4-2。

表 4-2 使用者頻寬規劃表

群組名稱	最小保證頻寬(kbits)	最大可借出頻寬(kbits)	優先權
Group1	300k	0	1
Group2	300k	600	2
Group3	118k	4750	3

依照表 4-1 及表 4-2 我們可以分別規劃出頻寬管理器上傳的 TC 架構，如圖 4-11~13，並以此設定其 TC 指令及參數，因頻寬管理器的下載 TC 架構圖與上傳大致相同，我們便予以省略不再列出。

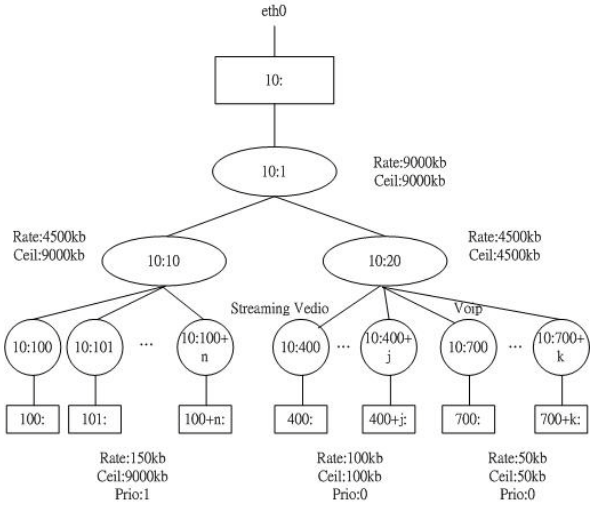

圖 4-11　subnet1 的上傳 TC 規劃圖

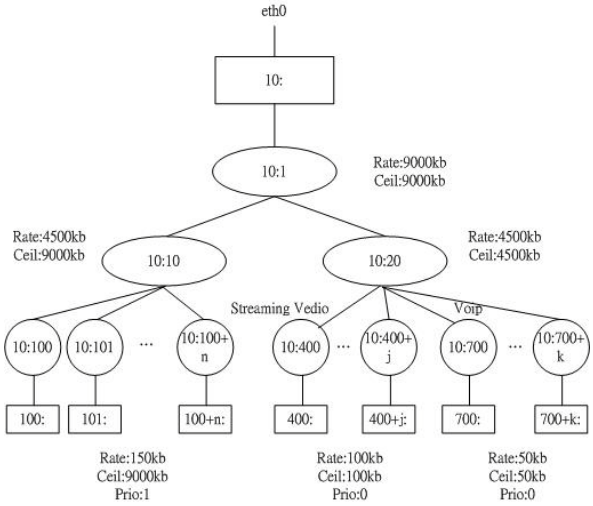

圖 4-12　subnet2 的上傳 TC 規劃圖

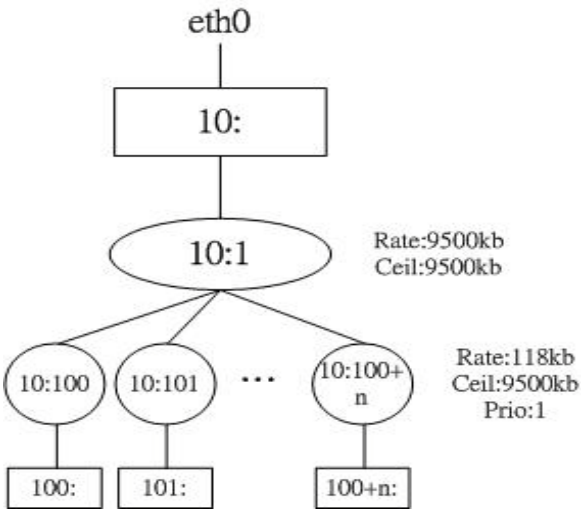

圖 4-13　subnet3 的上傳 TC 規劃圖

另外，頻寬管理器必須先讓下層使用者在尚未認證成功前無法使用網路，所以在 iptables 的設定預設對外封包全部封鎖，並且將使用者的瀏覽器產生的封包導至頻寬管理器的使用者登入畫面，iptables 設定如表 4-3，使用者登入畫面如圖 4-14。

表 4-3 頻寬管理器的 Iptables 設定

```
iptables -P INPUT      DROP
iptables -P OUTPUT    ACCEPT
iptables -P FORWARD DROP
iptables -t nat -P PREROUTING    ACCEPT
iptables -t nat -P POSTROUTING ACCEPT
iptables -t nat -P OUTPUT          ACCEPT
iptables -A INPUT -i lo -j ACCEPT
iptables -t nat -A POSTROUTING -s
$INNET -o $EXTIF -j MASQUERADE
iptables -A FORWARD -m layer7 --l7proto
$Layer7Service -j REJECT
iptables -t nat -A PREROUTING -p tcp
--dport 80 -s $INNET -j DNAT --to
$EXTIP:80
```

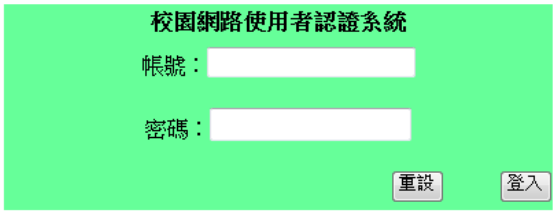

圖 4-14 使用者登入畫面

待使用者登入成功後，會顯示登入成功的畫面，並將使用者的帳號、網路位址、登入狀態寫入頻寬管理主控台的使用者資料表後，下達 iptables 指令開啟該使用者 IP 的網路功能，iptables 指令如表 4-4。

表 4-4 開啟使用者上網功能的 iptables 指令

```
iptables -A FORWARD -s $userip -j ACCEPT
iptables -t nat -A PREROUTING -s $userip -j
ACCEPT
```

5. 系統測試與驗證

本章將就論文提出的基於使用者分群的頻寬管理架構做相關測試，在測試部份採用比較簡單的 2 個子網路的環境來測試系統的功能是否可有效運作，並可藉此引證在 3 個子網路的情形下，本系統仍具有同樣的效能。系統測試環境的架構如下圖 5-1，2 台頻寬管理器分別管理 2 個 Subnet 的使用者，Subnet1 的網段為

192.168.10.0/255.255.255.0，Subnet2 的網段為 192.168.20.0/255.255.255.0，頻寬管理器安裝 2 張網卡，對內網卡 IP 為 192.168.10.254，192.168.20.254。

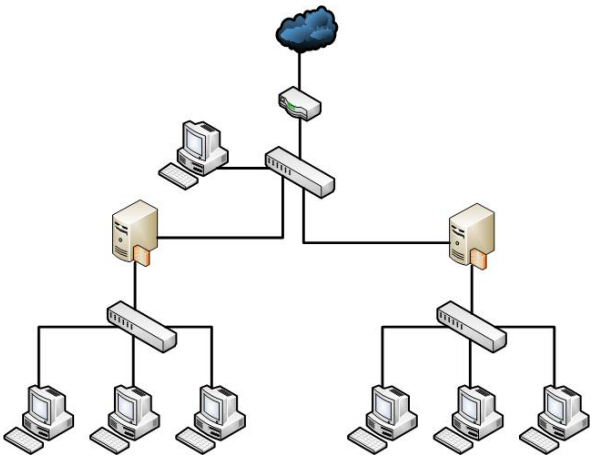

圖 5-1 測試環境架構圖

5.1 網路服務限制功能測試

本實驗的目的是要測試頻寬管理器對於該子網路使用者是否能有效限制其可使用的網路服務。我們以一台 PC 做為 Subnet 下的使用者，一開始我們取消頻寬管理器上該子網路所有可使用的網路服務，然後每隔一段時間依序啟用 WWW、FTP、POP3、SMTP、SSH、VoIP、Video streaming 服務的功能，並於使用者電腦開啟對應的網路服務程式，記錄該服務使用的流量，以測試該網路服務是否可正常使用，對於 WWW 的部份我們以 IE 瀏覽器，FTP 以檔案管理員進行下載，POP3 及 SMTP 則以 Outlook 進行收發信，VoIP 以 Skype 做通話測試，Video streaming 則以 Media Player 播放網路上的 mms 服務進行測試，實驗結果如圖 5-2。

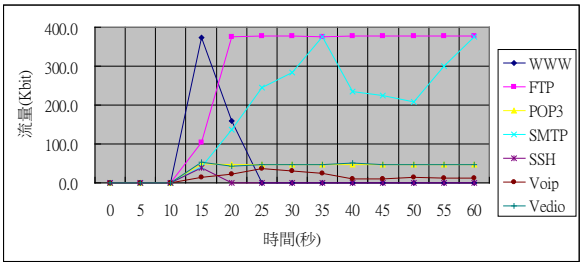

圖 5-2 網路服務限制功能測試

由上圖可以發現，在頻寬管理器未開啟各項網路服務的功能前，每種網路服務的流量皆為 0，且該網路服務皆無法使用。在依序開啟每種服務的限制，並於使用者開啟對應的網路服務時，網路服務皆可正運作，並依據不同網路服務的特性產生下載流量。由以上實驗可證明頻寬管理器對於子網路使用者的網路服務確實可以有效的限制。

5.2 使用者保證頻寬測試

本實驗的目的是要測試頻寬管理器當使用者不多時，單一使用者是否可使用多餘的網路頻寬；在多人登入使用網路服務時，單一使用者的保證頻寬功能是否有效，我們將子網路的最大可用頻寬設為 400k，使用者的保證頻寬設為 100k，最大可用頻寬設為 400k。

剛開始所有的使用者先進行登入，但未使用任何網路服務，因子網路最大可用頻寬僅有 400k，而每個使用者的保證頻寬為 100k，所以當第 user5 要進行登入時，頻寬管理器因判斷可用頻寬已不足，因此拒絕 user5 的登入要求。接著，我們讓 user1 開始使用 FTP 進行下載，其下載的流量值約可保持在 375k，可見當僅有一個使用者時，該使用者的確可以使用子網路的所有頻寬。

我們依序於第 30 秒、60 秒、90 秒、120 秒時讓 user2、user3、user4、user5 也開始利用 FTP 進行下載，可以發現當第 30 秒 user2 開始下載後，user1 和 user2 的下載流量皆降至 200k 以下，當第 60 秒 user3 也開始下載後，user1、user2、user3 的下載流量皆降至 125k 以下，當第 90 秒 user4 開始下載後，所有 user 的下載流量皆降至 100k 以下，第 120 秒 user5 因沒有登入成功，所以無法進行下載，因而流量為 0。測試結果如圖 5-3。

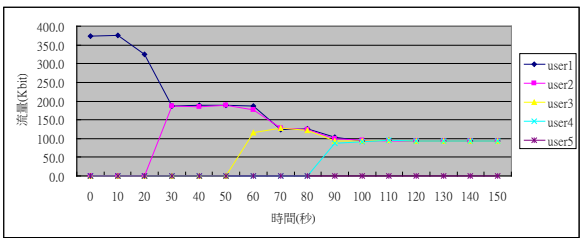

圖 5-3 使用者保證頻寬及頻寬借用測試

從以上實驗可證明頻寬管理器對於單一使用者的頻寬可有效的保證在 100k，而當子網路頻寬有多餘時，使用者亦可使用多餘的頻寬，不至造成浪費。

5.3 P2P 下載流量限制測試

本實驗的目的是要測試本系統能否針對

P2P 使用者有效達到下載流量的管制。子網路的最大下載頻寬設為 400k，使用者的保證下載頻寬為 200k，最大 400k，我們使用 BitComet1.16 做為測試的 P2P 軟體。一開始 user1、user2 皆在已登入的狀態，user1 從一開始即使用 BitComet 軟體進行下載，第 60 秒時，user2 才開始使用 FTP 進行下載。

當 user1 進行 P2P 下載時，同一子網路的其他使用者因沒有使用網路服務，因此 user1 可下載流量達到最大 391k，而當第 60 秒 user2 開始使用 FTP 下載時，user1 的 P2P 流量逐漸下降至 200k 以下，user2 的下載流量亦可達到約 200k。測試的結果如圖 5-4。

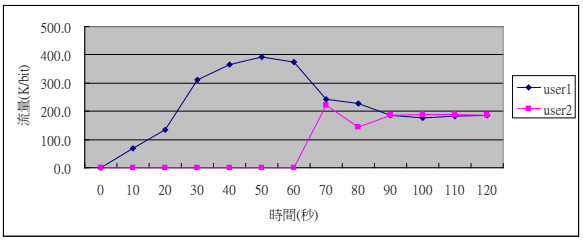

圖 5-4 P2P 下載流量限制測試

由以上實驗可證明，即使同一子網路下有使用者使用 P2P 服務，當其他使用者使用網路服務時，其流量亦會被限制，不會佔用其他使用者的網路頻寬。

5.4 即時性服務保證頻寬測試

本實驗的目的是要測試當使用者使用 VoIP 及 Video streaming 等即時性服務時，是否可有效的保證即時性服務的頻寬。使用者的保證頻寬設為 100k，優先權設為 2，使用者可用即時性服務的保證頻寬設為 100k，優先權設為 0，包含 VoIP 保證及最大皆設為 50k，Video streaming 保證及最大皆設為 50k，單一使用者可用頻寬共 200k。VoIP 測試用的軟體為 Skype，因 Skype 僅使用語音時的下載流量僅數 k，為使實驗效果明顯，我們開啟網路視訊的功能以加大流量，Video streaming 測試用的軟體為以 Media Player 播放網路上以 mms 協定傳送的影音串流影片。

一開始使用者先使用 FTP 服務進行下載，第 60 秒時開始啟用 Media Player 播放網路上的影音串流影片，第 120 秒時再開啟 Skype 進行視訊及語音通話，我們將使用者使用各種網路服務的流量記錄下來，Skype 的部份分下載及上傳兩種流量分別記錄。

由實驗結果可發現，當使用者開始使用 FTP 下載時，下降流量逐漸升至 200k，當第 60 秒使用者開啟 Media Player 時，由於即時性服務的優先權較高的原因，mms 的流量逐漸升高至 48k，而 FTP 的流量則逐漸下降至 120k。第 120 秒，當使用者使用 Skype 並建立連線後，Skype 的下載流量先逐漸升高到約 40k，再下降至 14k，而 Skype 的上傳流量則因啟用視訊的關係，於 50k 至 30k 之間振盪，上下傳流量皆未超過最大頻寬 50k，同時間 mms 的流量也穩定的保持在 50k 以下，FTP 的流量則因優先權較低的關係，逐漸降至 100k 以下。測試結果如圖 5-5。

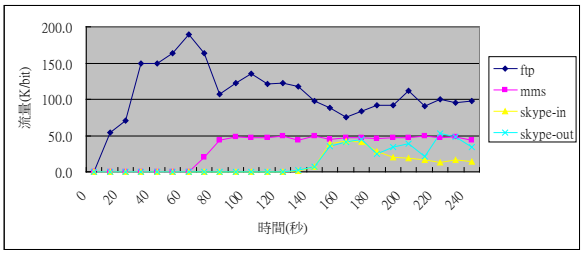

圖 5-5 即時性服務保證頻寬測試

由上面的實驗可證明，本系統確實可以有效保證特殊服務的頻寬。

5.5 子網路頻寬借用功能測試

本實驗的目的是要測試不同頻寬管理器間的頻寬借用功能是否有效。頻寬管理器 1 管理 subnet 1 下的使用者，Subnet 1 最大下載頻寬設為 400k，包含使用者保證頻寬 100k，特殊服務保證頻寬 100k(含 VoIP 及 Video streaming 各 50k)，最大可借出頻寬為 0，因此，subnet 1 不可借出頻寬，而再沒有借用其他子網路頻寬的狀態下，subnet 1 的最大可登入人數應為 2 人。頻寬管理器 2 管理 subnet 2 下的使用者，Subnet 2 最大下載頻寬設為 400k，包含使用者保證頻寬 100k，特殊服務保證頻寬 100k(含 VoIP 及 Video streaming 各 50k)，最大可借出頻寬為 200。實驗一開始 Subnet2 下的 2 位使用者 s2-user1 及 s2-user2 已先登入，並使用 FTP 進行下載，然後我們依序每隔 1 分鐘讓 subnet 1 的使用者登入，並於登入後使用 FTP 進行下載。

由圖 5-6 可發現 s2-user1、s2-user2 一開始的下載頻寬皆約為 188k， s1-user1 因 subnet1 尚未有其他使用者，因此其下載流量可達約 380k。第 60 秒時，當 s1-user2 登入並使用 FTP 下載時，s1-user1 的流量降至 188k。第 120 秒時，我們嘗試讓 s1-user3 登入，因 subnet 1 的

頻寬已全部分配給 s1-user1 及 s1-user2，因此 s1-user3 無法登入。第 180 秒時，我們將 subnet 2 的使用者 s2-user2 登出，此時 s2-user2 的流量迅速下降至 0k，而 s2-user1 的流量則迅速上升至 385k。第 240 秒時，我們試著讓 s1-user3 登入，此時因 subnet 2 有剩餘 200k，因此 subnet 1 可借用此 200k，所以 s1-user3 便可登入，流量可達約 186k。

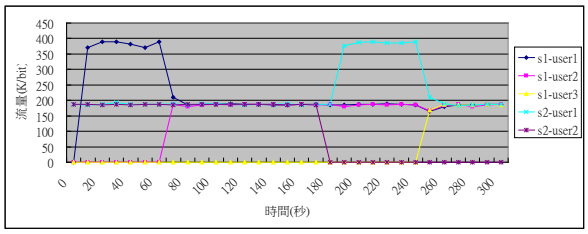

圖 5-6 子網路頻寬借用功能測試

從以上的實驗可證明，本實驗的不同頻寬管理器之間可以有效的借用多餘的頻寬。

5.6 效能比較測試

本實驗的目的是要測試未採用允入機制的單一頻寬管理器與本論文架構對於所有使用者的保證頻寬的影響。我們採用相關的頻寬條件，在單一頻寬管理器部份，最大下載及上傳頻寬皆為 1000k，使用者分為 2 個群組，Group1 為高優先權使用者，保證下載及上傳頻寬為 600k，最大下載及上傳頻寬為 1000k，也就是當系統有剩餘頻寬時，Group1 群組的使用者可以借用到最大 1000k 的頻寬，Group1 群組下的每個使用者的保證頻寬為 200k，最大下載及上傳頻寬為 1000k，優先權值為 0。Group2 為低優先權使用者，保證下載及上傳頻寬為 400k，最大下載及上傳頻寬為 400k，優先權值為 1，也就是 Group2 群組的使用者僅可使用該群組最大的頻寬 400k，無法借用剩餘頻寬，Group2 群組下的每個使用者的保證頻寬為 100k，最大下載及上傳頻寬為 400k，優先權值為 1。頻寬規劃架構如圖 5-7。

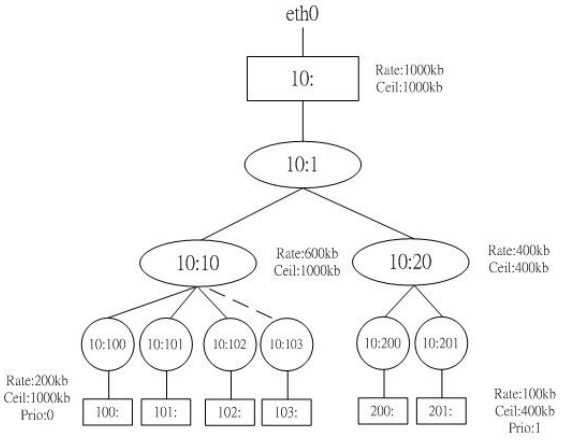

圖 5-1 單一頻寬管理器頻寬規劃架構圖

實驗一開始，我們先讓 Group1 的使用者 s1-user1~s1-user3 登入，並使用 FTP 進行下載，接著，我們讓 Group2 的使用者 s2-user1 及 s2-user2 登入，並使用 FTP 進行下載，從圖 5-8 可以發現，此時由於 Group1 及 Group2 的使用者保證頻寬總和皆未超過該群組的最大頻寬，因此，Group1 的 3 個使用者可獲得保證頻寬約 189k，Group2 的 2 個使用者可獲得保證頻寬約 187k，此時系統尚能有效保證使用者的最小保證頻寬。

接著，我們模擬未採用允入機制的情形，讓 Group1 的使用者 s1-user4 登入，因為 Group1 的使用者保證頻寬總和為 800k，大於 Group1 群組 class 的預設最大保證頻寬值 600k，此時，不僅 Group1 群組的使用者受影響，連 Group2 群組的使用者也受到影響，所有使用者的保證頻寬值開始從 0 至最大下載頻寬間發生激烈的上下振盪，所有使用者的下載頻寬仍不會超過該 class 的最大下載頻寬，然而保證頻寬機制此時等同失效。

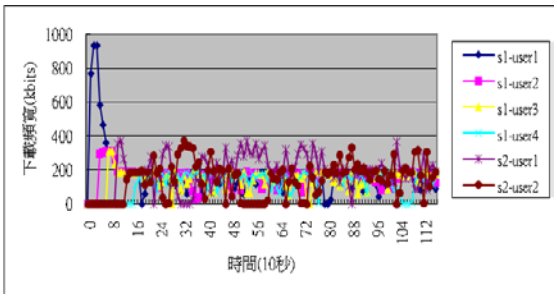

圖 5-2 未採用允入機制使用者保證下載頻寬

在本系統的部份，為證實子網路的頻寬借用功能及採用允入機制可有效保證所有使用者的最小保證頻寬，我們以兩台頻寬管理器分別管理 Group1 及 Group2 的使用者，Group1

及 Group2 的群組頻寬及使用者頻寬設定和單一頻寬管理器的設定一樣，差別在於本系統的 Group2 設定最大可借出頻寬 200k，因此在 Group2 只有 2 個 user 登入的情形下，Group1 的使用者 s1-user4 可以借用 200k 的頻寬成功登入。頻寬架構如圖 5-9 所示。

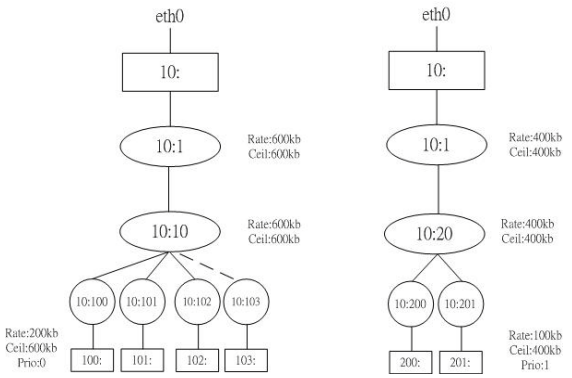

圖 5-3 2 個頻寬管理器頻寬規劃架構圖

實驗一開始，Group1 的使用者 s1-user1~s1-user3 及 Group2 的使用者 s2-user1~s2-user2 陸續登入，並以 FTP 進行下載，從圖 5-10 可以發現，當第 70 秒時，Group1 的 3 個使用者及 Group2 的 2 個使用者登入時，Group1 的使用者可以獲得保證頻寬約 187k，Group2 的使用者可以獲得保證頻寬約 187k；在第 90 秒時，我們讓 Group1 的使用者 s1-user4 登入，並使用 FTP 進行下載，此時，因為 Group1 已借用 Group2 的剩餘頻寬 200k，因此 Group1 的最大頻寬變成 800k，4 個使用者的保證頻寬各為 200k，所以使用者可有效使用保證頻寬 187k。而 Group2 因最大頻寬借出 200k，因而最大頻寬僅剩 200k，因此，Group2 的使用者的下載頻寬下降至約 94k，但仍可獲得最小保證頻寬。

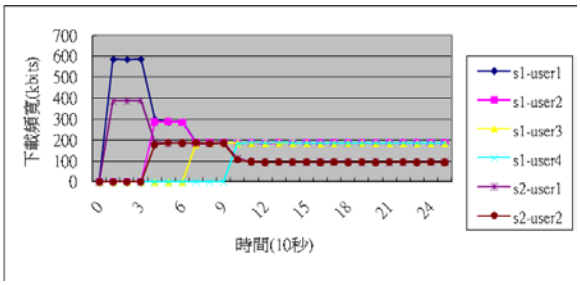

圖 5-4 採用允入機制的使用者下載頻寬

我們也將上述 2 個實驗的總下載流量進行記錄及比較，以了解此 2 種實驗的總下載流量是否有不一樣的結果。每隔 5 分鐘記錄一次，總共記錄 15 分鐘，統計結果如圖 5-11 所示。

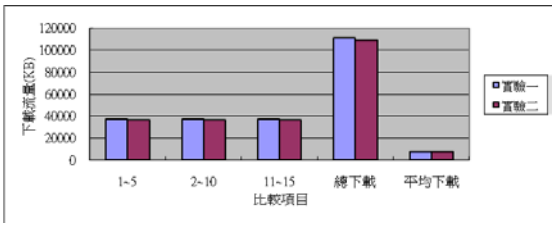

圖 5-5 下載流量比較圖

從以上實驗可以發現，單一頻寬管理器與本系統的架構在下載的流量部份差異並不大，然而，對於使用者的保證頻寬而言，本系統採用允入機制的方法相較於單一頻寬管理器未採用允入機制的作法，確實能有效保證每個使用者的最小保證頻寬。

6. 結論與未來展望

本論文提出了基於使用者分群的校園網路頻寬管理架構，事先針對網路使用者的類型、每小時平均使用人數、使用網路的特性進行分析後將使用者分成三種類型，分別設定不同的保證頻寬、優先權、最大可借出頻寬及可用網路服務，劃分於不同子網路由三台頻寬管理器分別進行頻寬管理。加入允入控制機制對於每個子網路的登入人數進行控管，避免過多使用者同時使用網路造成頻寬的壅塞，確保每個使用者都可獲得最小保證頻寬。採用子網路頻寬借用演算法，使高優先權使用者在頻寬不足時，可以借用低優先權使用者剩餘的頻寬，以提高整體的頻寬使用率。另外，以一台頻寬管理主控台對三台頻寬管理器進行集中管理，採 Web 介面方便管理者設定使用者、即時性服務及子網路的頻寬參數，了解使用者登入狀態、子網路頻寬使用情形、實際上下載流量等資訊。

實作的結果，本系統確實可有效阻絕各子網路所設定限制的網路服務，對於各子網路的使用者皆可有效保證最小頻寬，對於即時性服務可以有效保證最小頻寬 100k，對於網路上的 P2P 使用者可有效限制其下載流量於 200k，對於不同子網路間的高優先權使用者可以有效的借用低優先權使用者的剩餘頻寬 200k，並於登出時歸還。此外，相較於單一頻寬理器未採用允入機制的作法，本系統採用允入機制加上子網路間的頻寬借用，能有效避免使用者登入人數過多造成的使用者保證頻寬失效，並且讓整體的頻寬運用更有效率。然而，現今網路即時性服務愈來愈多樣，功能也愈來愈強，本論

文目前針對即時性服務的封鎖及頻寬管理僅針對 L7-filter 可支援的程式，部份新的即時性影音服務如 PPlive 在封包的辨識上仍有無法完全辨識的問題，這部份需視 L7-filter 在未來的更新版本能否加強對即時性影音辨識的效能，或自行分析即時性影音服務的封包特徵值來做為封鎖的依據，以加強封包過濾及分類的能力。此外，在頻寬管理工具部份，TCNG(Traffic Control Next Generation)[28-30]為繼 Linux TC 後發展的頻寬管理工具，有著更新的架構及語法，爾後或許可以採用 TCNG 取代 TC 做為實作及研究的工具。

參考文獻

[1] 李紹唐，"***P2P 網路流量管理系統之設計與實作***"，碩士論文，國立中山大學資訊工程學系，2008 年 2 月。

[2] Anttoni Halme, "***Peer-to-peer Traffic: Impact on ISPs and Evaluation of Traffic Management Tools***", Seminar on Internetworking ,2005.

[3] 邱家偉 and 潘仁義，"***基於 Linux 平台之 SIP 網路電話動態頻寬保證及允入控制雛型實作***"， 2006 年 10 月。

[4] 蘇建郡 and 謝仲訓，"***以 Linux TC 建置校園宿舍網路頻寬管理***"，碩士論文，南台科技大學資訊管理系，2003 年 1 月。

[5] 陳俊豪，"***基於橋接模式之校園頻寬管理器設計與實作***"，碩士論文，亞洲大學資訊工程學系，2008 年。

[6] 蔡禮文，"***一個具身份認證及動態頻寬調整之校園網路管理系統的開發***"，碩士論文，國立中興大學資訊科學與工程學系，2009 年 12 月。

[7] 何振毅，"***HTB 與 CBQ 在 Linux 上階層性頻寬分享機制實作分析和探討***"，碩士論文，大葉大學資訊工程系，2003 年。

[8] 林廷皆，"***階層式自動偵測頻寬管理系統之設計與實作***"，碩士論文，元智科技大學電機工程學系，2004 年。

[9] 楊智淵，"***以分層公平頻寬使用考量之校園網路管理架構設計與實現***"，碩士論文，國立雲林科技大學資訊工程研究所，2006 年 11 月。

[10] 呂秉諺，"***在 802.16 架構下之允入控制之研究 A Study of Admission Control in IEEE 802.16***"，碩士論文，國立中央大學通訊工程所，2005 年 7 月。

[11] R. Braden, D. Clark and S. Shenker, "RFC1633: ***Integrated Services in the Internet Architecture: an Overview***," RFC Editor United States, 1994.

[12] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang and W. Weiss. " RFC2475: ***An architecture for differentiated service***,"RFC Editor United States,1998.

[13] HTB home, Http://luxik.Cdi.cz/~devik/qos/htb/，2009 年 12 月。

[14] Class-based queueing, Http://www.Icir.org/floyd/cbq.Html，2009 年 12 月。

[15] S. Floyd and V. Jacobson, "***Link-sharing and resource management models for packet networks***," IEEE/ACM Transactions on Networking (TON), vol. 3, pp. 386, 1995.

[16] IPTABLES, Http://www.Netfilter.org/projects/iptables/index.Html，2009 年 11 月。

[17] 施威銘，***Linux Iptables 技術實務***，旗標出版社，2005 年。

[18] L7-filter, Http://l7-Filter.Sourceforge.Net/，2009 年 12 月。

[19] Iptables and Connection Tracking, Http://www.Redhat.com/docs/manuals/enterprise/RHEL-4-Manual/security-guide/s1-Firewall-State.Html，2009 年 10 月。

[20] "L7-filter Supported Protocols", Http://l7-Filter.Sourceforge.net/protocols，2009 年 11 月。

[21] Y. A. Chen, "***The Design and Implementation of Time-Shifting Mechanism for Live Streaming Multimedia***"，碩士論文，朝陽科技大學資訊工程系，2007 年 5 月。

[22] Microsoft Media Server, Http://en.Wikipedia.org/wiki/Microsoft_Media_Server，2009 年 10 月。

[23] H. Schulzrinne, A. Rao and R. Lanphier, "RFC2326: ***Real Time Streaming Protocol (RTSP)***," Internet RFCs, 1998.

[24] 鳥哥的 Linux 私房菜，"Linux 防火牆與 NAT 主機"，

Http://linux.Vbird.org/linux_server/0250simple_firewall.php#nat，2009 年 12 月。

[25] Awk，Http://www.Grymoire.com/Unix/Awk.Html，2009 年 12 月。

[26] 鳥哥的 Linux 私房菜，"ssh 伺服器"，Http://linux.Vbird.org/linux_server/0310telnetssh.php#ssh，2009 年 10 月。

[27] Linux 流量監控的三個方法，Http://www.ccidcom.com/blog/?action-viewthread-tid-48944，2009 年 12 月。

[28] Traffic Control Next Generation, Http://tcng.Sourceforge.Net/，2009 年 12 月。

[29] Traffic control using tcng and HTB HOWTO, Http://tldp.org/HOWTO/Traffic-Control-Tcng-HTB-HOWTO/，2009 年 12 月。

[30] Traffic control next generation reference manual，Http://linux-Ip.net/gl/tcng/，2009 年 12 月。