

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

張慶龍 楊智淵 徐正哲

雲林科技大學資訊工程所

chang@yuntech.edu.tw

摘要

網際網路用戶數與傳輸頻寬逐年攀升，其傳輸內容亦趨於多元化，此種服務類型與傳遞內容的改變，已非單靠 IP 協定之 best-effort 封包傳送即可滿足各種服務應用的傳輸品質要求。

另一方面，網路內包羅萬象的資訊對校內學子而言，已對其正常課業的學習造成困擾。對校園網路之網管人員而言，除了致力於網路頻寬的增加外，如何對網路頻寬作有效的管理，乃是目前校園網際網路發展的重要課題。

本論文以校園網路為基礎，提出分層式之頻寬管理機制，其配合使用者認證系統、核心路由器之封包流量監視與邊緣閘道器之設計與實現，可確保骨幹網路下各個子網路使用頻寬的公平性；同時亦可確保子網路下各個使用者一定程度之網路服務品質與公平性。經由 NS2 電腦模擬之結果顯示，此分層式之頻寬管理機制可確實達到 Subnet-level 與 User-level 的公平的頻寬使用。

關鍵詞：流量監控、頻寬管理、身份認證、IP 位址盜用、Subnet-level、User-level。

Abstract

Accelerated growth in Internet bandwidth and Internet users have increased network management complexity. This issue is more pronounced in campus networks as the scale of such networks has increased dramatically. As a result of computer viruses and abnormal peer-to-peer users, some computers use a substantial amount of network bandwidth. Therefore, normal users are probably unable to obtain the correspondent quality service when using the networks. This situation can be considered an unfair allocation of bandwidth. This work proposes a novel layer-based network bandwidth management framework that significantly decreases implementation complexity, achieves fair bandwidth allocation and resolves problems associated with stolen IP addresses. Based on existing campus networks, three components are utilized— traffic measurement, user authentication server, and edge gateway—to offer cost-effective network management. The proposed framework tracks user logins, and, with information gathered by monitoring network packets, the amount of bandwidth consumed by each user and that by each subnet is estimated to provide flow-based

bandwidth management and subnet-level fair bandwidth allocations. Simulation results demonstrate that the proposed framework achieves fair bandwidth usage in the subnet and backbone.

Keywords: Campus network, fairness, traffic measurement, IP address stealing, user authentication.

1. 前言

網際網路用戶數與傳輸頻寬逐年攀升，其傳遞內容亦由文字為主轉為多媒體之資訊。由於服務類型與傳遞內容的改變，已非單靠 IP 協定之 best-effort 封包傳送來滿足各種應用服務的需求。

目前而言，雖然網路傳輸頻寬朝向 10Gbps 乙太網路的方向發展，然而對網路使用者的行為無法有效管理與控制而產生了許多問題，而這問題在校園網路尤為嚴重，其遭遇到的主要問題有：

- 1、網路服務品質無法滿足：由於 Multimedia 與 VoIP 等即時資訊傳遞的應用服務大量興起，除了加重網路負載外，亦無法滿足各個應用程式所需的網路服務品質要求。
- 2、IP 位址盜用問題：因 IP 位址設定的特性，易被竊用，除了會造成 IP 位址衝突外，若僅以 IP 位址來稽核網路使用者，其正確性亦常令人質疑，因此，當網路用戶使用行為有爭議時，將衍生不少行政上或維護上的困擾。
- 3、網路頻寬使用的不公平：在校園內雖擁有大量的傳輸頻寬，但每位使用者之網路傳輸品質確無法獲得一定程度之保障，主要原因是少數不正常的網路使用者佔據大量的網路頻寬，如：捉圖檔、MP3 或電影檔等，讓正常網路使用者反而無法得到該有的服務品質的不公平現象。
- 4、中毒電腦癱瘓整個校園網路：由於層出不窮的電腦病毒，使用者很容易在不經意間中毒而產生大量垃圾封包，當網路頻寬愈大，其產生的垃圾封包量就愈驚人，除了佔用本身網段的頻寬外，亦危害到整個骨幹網路的正常運作。

本論文致力於校園網路頻寬管理系統之設計與實現，提出一分散式網路監控、管理架構，將骨幹網路之監控、管理負擔分散到各個邊緣閘道器，以減少設計之複雜度。利用認證系統，讓每位使用者在使用網路之前必需先通過身份認證方可取得使用網路之權限，達到以人為管理對象而非以 IP 位址。另一方面，配合認證方式，將校園網路使用

者分成 Good-user、Bad-user 與 Discard-user 等三類，而邊緣閘道器則依不同類別的使用者封包做 flow-based 的頻寬管理，以讓 Good-user 可享有正常的網路傳輸品質。

本論文之架構組成說明如下：第二節將介紹目前在頻寬管理部份相關文獻之探討；本論文所提之分層式頻寬管理架構將於第三節詳細介紹；第四節則介紹邊緣閘道器所使用之 flow-based 頻寬管理演算法；第五節是介紹認證伺服器之相關資料庫維護細節；第六節著重於如何提供公平的子網域層級之頻寬分配演算法；而 NS2 之系統模擬結果則於第七節加以探討；第八節將對本論文所提出的解決方案、實作與模擬結果作一個簡單結論。

2. 相關文獻探討

目前已有多篇關於公平的網路頻寬的論文提出，如 Ion Stoica 等[8]所提的 CSFQ 架構，其依功能將 Router 分為 Edge Router 與 Core Router 兩種。Edge Router 負責監控每個 flow 目前所傳送的速率，並以指數平均方式得出每個 flow 的平均傳輸速率，將此平均速率(flow rate)記錄在所屬 flow 的封包標頭上；而 Core Router 則監控整個骨幹網路的平均傳輸速率，以決定各個子網路的可用頻寬值(公平分享值)，並依此數據與各個封包所貼的 flow rate 比較，決定該封包丟棄的機率，以達到絕對頻寬公平共享的效果。

而 Xiaobo Zhou 和 Cheng-Zhong Xu 所提出的 Harmonic Proportional Scheme[3] 可保證每個 streaming 要求最低的頻寬(channel)使用，若系統有多餘的頻寬時，則按照 requests 的等級(weighting)來分配，等級越高的 flow 得到越多的頻寬。

Maria-Dolores Cano 和 Fernando Cerdan[9]則是以 Diff-Serv 為架構，發展出 Marking (CB) 與 Policing (NPF) 演算法，在 Edge 端監控各個使用者的傳輸速率與其所租用的傳輸速率(Contracted Target Rate)比對，適當地做出 Marking 與 Dropping 的動作，以保證使用者所租用的傳輸速率。

上述之相關論文中，分別以不同角度來提供絕對公平或是相對公平(Weights or Contracted Target Rate)的頻寬管理機制，然而這些機制都需修改現有的路由設備以達到公平分享頻寬目的。有別於目前相關文獻所提之方法，本論文是架構在現有的網路設備下，以分散式架構，提出一低成本的分層式頻寬管理機制，以達到網路頻寬使用的相對公平性。

3. 分層式之頻寬管理架構

圖 1 為本論文所提之分層式頻寬管理架構，其在現有網路環境下，加入認證伺服器(authorization server)、邊緣閘道器(edge gateway)與流量監視器

(traffic monitoring)，以達到骨幹網路下各個子網路頻寬使用的公平性與子網路下 flow-based 之使用者頻寬管理。

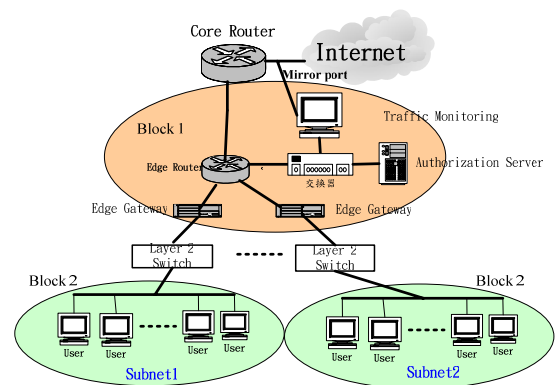


圖 1 分層式頻寬管理架構

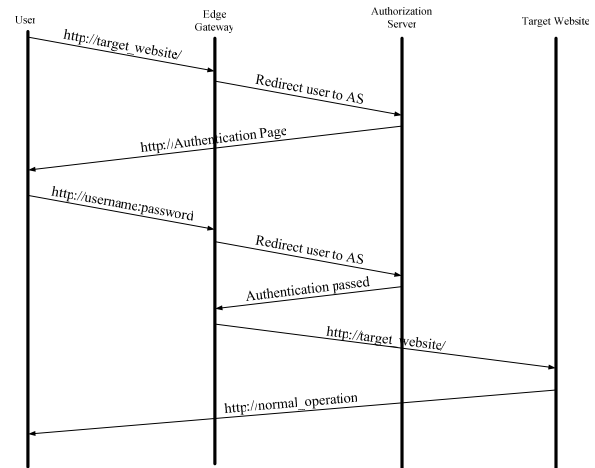


圖 2、Web-based 認證流程示意圖

如圖 1 所示，於 Core router 對外之線路設一 mirror port，將對外之封包 mirror 一份到流量監視器，以計算各個子網路之傳輸流量；於邊緣路由器與 Layer2 Switch 之間，設計一邊緣閘道器，負責該子網路之 flow-based 的頻寬管理工作；設計一認證伺服器，提供網路使用者之認證工作與紀錄使用者之資訊傳輸量，其系統運作的流程說明如下。

當使用者要使用網路時，需先經過身份認證的動作，目前主要認證技術有 802.1x [13]與 Web-based 界面兩種，由於並非所有 client 端的機器皆具有 802.1x 軟體，所以本論文是採用 Web-based 方式來提供認證。圖 2 為此管理系統之認證流程，在 Web-based 環境下，其 client 端只需利用瀏覽器，開啟某一網頁時，若該使用者未經過認證，則會被邊緣閘道器轉向到認證伺服器，作認證動作。

待認證通過後，認證伺服器會告知邊緣閘道器此通過認證的使用者其服務等級為何(Good-user、Bad-user 或 Discard-user)。邊緣閘道器則依此 user

目前所使用的 IP 位址與服務等級加以管理，達到以人為對象的頻寬管理而非以 IP 位址。

流量監視器主要工作是由 mirror port 週期性的統計往 Internet 封包中，各個 subnet 佔多少頻寬，每個 user 在這段時間傳輸的資料量。流量監視器依當時的統計結果，以公平為原則，決定每個 subnet 可送到骨幹網路的頻寬，並將此值回報給邊緣閘道器；邊緣閘道器則依此頻寬限制值決定其送到骨幹網路的資料量。

流量監視器亦週期性的將每個使用者的傳輸量回報給認證伺服器。認證伺服器除了做網路使用者之登入認證外，亦透過流量監視器的回報資訊來決定每位使用者之服務等級。每位使用者在一天開始時皆為 Good-user 等級，若網路使用者瞬間送出太大的資料量，則會由 Good-user 降為 Bad-user，倘若網路使用者當日累積的傳輸量超過某一門檻值時(如：3Gbyte)，則將其降為 Discard-user，該使用者當天無法再使用網路。當有網路使用者其服務等級被改變時，認證伺服器即將此資訊回報給所屬網域之邊緣路由器，以限制其資料傳輸量。

如上所述，此分層式頻寬管理架構，將整個頻寬管理工作分散到流量監視、認證伺服器與邊緣閘道器，其將網路使用者適度分類，以保證正常網路使用者的服務品質以及避免中毒電腦產生的封包癱瘓骨幹網路之運作，達到 User-level 的公平性，同時亦保證各個 subnet 應有的頻寬，達到 Subnet-level 的公平性。

4. 邊緣路由器(Edge Gateway)

邊緣閘道器內部主要分成三部分：分類器(Classifier)、緩衝區管理(Buffer management)和頻寬分配機制(Output scheduling)。分類器主要工作為判定所收進來的封包是屬於何使用者的封包，該使用者是否已經通過身份認證，以及使用者等級為何等資訊；緩衝區管理機制則依登入的使用者人數來分配封包記憶體大小；頻寬分配機制則採用 WRR[1] 排程機制來實現。

當邊緣閘道器收到一個封包時，依據該封包的來源 IP 位址到使用者狀態表做搜尋的動作，以取得該使用者封包的相關資訊(如使用者是否登入、權重為 Good 或 Bad 等)。由於邊緣閘道器僅負責該 subnet 的管理，一般而言，一個 subnet 的網路大小為一組 class C (255 個 user)，所以用來源 IP 位址為索引的 Table 大小僅需 255 個 entries。

而頻寬分配機制是依據使用者等級，執行差異式服務流量控制，而在時間 t_i 期間，服務等級 c 所能傳輸的頻寬 $BW_c(t_i)$ 為

$$BW_c(t_i) = \frac{w_c}{\sum_{j=1}^N w_j} \times Limit_BW(t_i) \quad (1)$$

$$W_c = \sum_1^{N_c} Weight_c \quad (2)$$

其中 $c \in \{\text{Good-user, Bad-user}\}$ ， N_c 為目前已登錄使用者中屬於 Class c 之人數， W_c 為服務等級 c 之權重值， $Weight_c$ 為服務等級 c 之每位使用者所分配到的權重值， $Limit_BW(t_i)$ 為 t_i 期間流量監視器允許此 subnet 使用之網路頻寬。

5. 認證伺服器(Authentication Server)

認證伺服器主要工作為使用者認證與決定該使用者之服務等級。其中服務等級之決定是依流量監視器所回報之每位使用者在 t_i 時間之傳輸量來決定。認證伺服器依下列式子得出每位使用者在 t_i 時間所佔用之骨幹網路頻寬與到目前為止該使用者之網路傳輸量。

$$Total_x(t_i) = Total_x(t_{i-1}) + T_x(t_i) \quad (3)$$

$$r_x(t_i) = \frac{T_x(t_i)}{t_i} \quad (4)$$

$$R_x(t_i) = \alpha R_x(t_{i-1}) + (1-\alpha) r_x(t_i) \quad (5)$$

式子(3)到(5)中， $T_x(t_i)$ 為 t_i 期間內使用者 x 之網路傳輸量， $Total_x(t_i)$ 為到 t_i 時間為止使用者 x 的總傳輸量， $r_x(t_i)$ 為使用者 x 在 t_i 期間內所使用之頻寬， $R_x(t_i)$ 為使用者 x 指數平均傳輸速率。

根據式子(3)與(5)，我們設定兩個門檻值，分別為 T_{max} 及 R_{max} 來， T_{max} 為網路使用者一天的最大網路傳輸量； R_{max} 為網路使用者之最大的平均傳輸速率。當 $Total_x(t_i) > T_{max}$ 時，則使用者 x 將成為 Discard-user；若 $R_x(t_i) > R_{max}$ 時，使用者 x 將由 Good-user 降級為 Bad-user。

圖 3 為認證伺服器維護每位使用者狀態之連線狀態機，以隨時掌握每位使用者目前所屬的連線狀態，每位使用者之狀態分別為 G-user(G)、B-user(B) 及 Discard-user(D)。其狀態轉換條件說明如下：

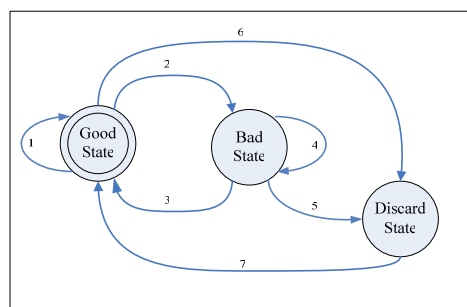


圖 3 使用者連線狀態機

1. 當使用者一直正常使用網路時則維持於 G 狀態；即 $Total_x(t_i) < T_{max}$ 且 $R_x(t_i) < R_{max}$ 。

2. 當使用者瞬間佔據大量網路頻寬 (例: 如中毒後產生大量的垃圾封包); 即 $Total_x(t_i) < T_{max}$ 但 $R_x(t_i) > R_{max}$, 此時由 G 狀態改為 B 狀態。
3. 在 B 狀態時, 若使用者正常使用頻寬一段時間後, 使其 $R_x(t_i)$ 降於 R_{max} 之下時且 $Total_x(t_i) < T_{max}$, 則由 B 狀態回到 G 狀態。
4. 使用者仍然持續異常使用網路, 即 $Total_x(t_i) < T_{max}$ 但 $R_x(t_i) > R_{max}$ 條件持續成立, 則維持於 B 狀態。
5. 在 B 狀態時, 若其 $Total_x(t_i) > T_{max}$, 表示該使用者已超過當天網路傳輸的上限值, 即由 B 狀態跳到 D 狀態, 無法繼續使用網路。
6. 在正常使用網路下, 但當天網路使用流量已超過門檻值, 即 $Total_x(t_i) > T_{max}$ 但 $R_x(t_i) < R_{max}$, 則由 G 狀態跳到 D 狀態。
7. 當一天的開始時, 每位使用者皆是 Good-user, 即在 G 狀態。

6. Subnet-level 頻寬分配演算法

本論文除了致力於使用者使用頻寬的公平性 (User-level) 外, 亦以骨幹的角度, 提供子網路間使用網路的公平性 (Subnet-level)。所謂 Subnet-level 公平頻寬分配乃是依據子網路下已登入的使用者人數多寡來平均分配, 其分配方式如下式所示。

$$Subnet_s = \frac{N_s}{\sum_{j=1}^n N_j} \times LineRate \quad (6)$$

其中 $Subnet_s$ 為分配給子網路 s 之頻寬, N_s 為子網路 s 已登入之使用者人數, $LineRate$ 為骨幹網路對外到 Internet 的頻寬。

當流量監視器啟動時, 先主動向認證伺服器詢問各個子網路目前已登入的使用者人數為何, 再根據式(6)決定各個子網路所分配頻寬, 將分配到的頻寬值通知給邊緣路由器, 邊緣路由器再依所分配到的頻寬做 flow-based 的頻寬管理。

除了公平考量外, 流量監視器亦希望將對外可用頻寬有做最有效運用; 即某子網路用不完所配給的頻寬時, 可將剩餘頻寬平均分配給需要更多頻寬的子網路使用。為了達到此動態頻寬分配之目的, 流量監視器藉由週期性地統計從 mirror port 所送過來的 packets 中, 等知各個 subnet 實際使用的頻寬情形, 與配給的頻寬值做比對, 將沒用完的頻寬於下一次頻寬分配中平均分配給其他子網路使用, 如式(7)所示, 直到分配穩定為止。

$$B_s(t_{i+1}) = B_s(t_i) - (B_s(t_i) - E_s(t_i)) + \sum_{m=1, m \neq s}^n (B_m(t_i) - E_m(t_i)) / (n-1) \quad (7)$$

其中 $B_s(t_{i+1})$ 為時間 t_{i+1} 分配給子網路 s 之頻寬, $E_s(t_i)$ 為流量監視器監測到子網路 s 之實際使用頻寬, n 為子網路的個數。

7. Simulation

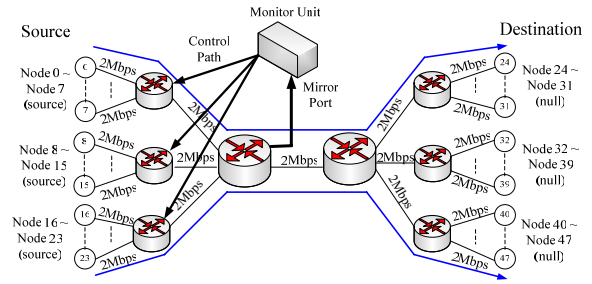


圖 4 模擬環境

本論文採用 NS-2 模擬軟體, 以模擬方式來驗證所提之分層式頻寬管理機制, 模擬環境設定如圖 4 所示, 不管是 Edge 或 Core 部分, 其實體網路頻寬皆為 2Mbps, 左邊網路為來源端, 其有 3 個子網路, 每個子網路下有 8 個使用者, 每個使用者皆為 Pareto on/off distribution, 其 on 週期為 200ms, off 週期為 100ms, 每個封包長度設為 500bytes, 流量監視器的頻寬量測週期為 0.1s, Node0 到 Node23 為來源端, Node24 到 Node47 分別為目的端。

7.1 子網路(Subnet-level)頻寬使用公平性之驗證

為了驗證此分層式頻寬管理系統對子網路間頻寬使用的公平與否, 本論文乃採用 Jain's fairness index[11]式子來判斷 Subnet-level 之公平式, 式子(8)為此 fairness index 的計算方式。

$$f(x_1, x_2, \dots, x_N) = \frac{(\sum_{s=1}^N x_s)^2}{N \sum_{s=1}^N x_s^2} \quad (8)$$

其中 N 為子網路各數, x_s 為子網路 s 下每位使用者之平均使用頻寬, 其計算方式為

$$x_s = \frac{Tavg_s}{U_s} \quad (9)$$

其中 $Tavg_s$ 為子網路 s 之平均 Throughput, U_s 為子網路 s 之使用者人數。

Case1: 相同使用者於相同時間登入時, 各個子網路所使用的頻寬量模擬。圖 5 為每個子網路皆有 8 位使用者之模擬結果, 而圖 6 為子網路一有 2 位使用者登入、子網路二有 3 位使用者登入, 而子網路三有 8 位使用者登入之模擬結果。由圖 5 與圖 6 知, 若 Core router 僅使用簡單之 FIFO 方式來傳送封包, 則大部份的網路頻寬將被某一 subnet 搶去, 形成很不公平現象, 其 fairness index 約皆僅有 0.6621。反之, 本論文所提之機制下, 其 fairness index 值皆可趨近 1, 確實可達到 Subnet-level 之公平性。

Case 2：使用者登入時間不同時，各個子網路所使用的頻寬量模擬。圖 7 為每個子網路皆有 8 位使用者之結果，而圖 8 為子網路一有 2 位使用者登入，子網路二有 3 位使用者登入，而子網路三有 8 位使用者登入之模擬結果。由圖 7 與圖 8 結果中可計算出，本論文所提之方式其 fairness index 值亦趨近於 1，可提供非常公平之 Subnet-level 頻寬使用。

由圖 7 與圖 8 知，雖然新使用者登入時間有所差異，但當認證伺服器通知流量監視器使用者人數的最新資訊而啟動頻寬重新分配後，亦可達到 Subnet-level 之頻寬使用的公平性。

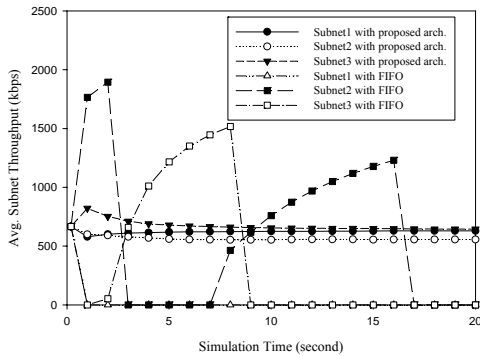


圖 5 相同使用者下各子網路所使用之平均 Throughput 比較

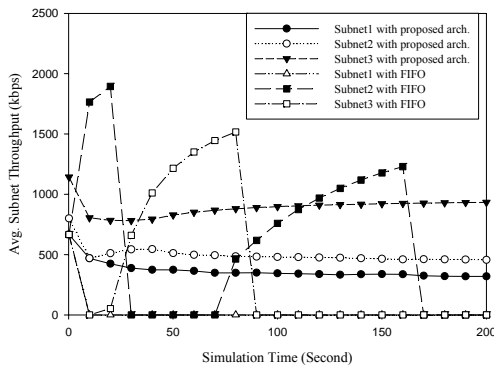


圖 6 各子網路所使用之平均 Throughput 比較(2)

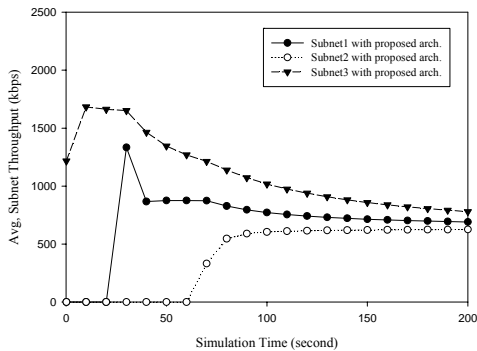


圖 7 子網域平均產量

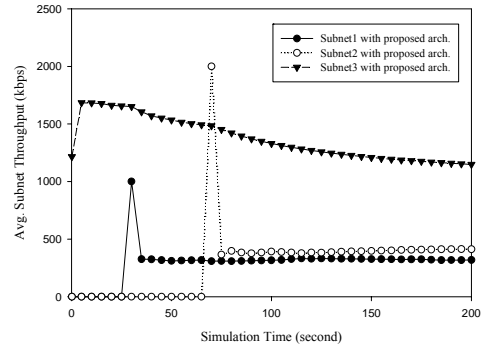


圖 8 子網域平均產量

7.2 使用者(User-level)頻寬使用公平性之驗證

本小節主要是驗證子網路下 User-level 的公平性，其中 R_{max} 參數值設定為 $Limit_BW_s(t_i)/U_s$ ， α 值設定為 0.5，流量監視器是以每 0.1 秒統計一次使用者的傳輸量，並將統計結果回報給認證伺服器，以決定每位使用者之服務等級。

如圖 4 所示，各子網路都有 8 位使用者登入，且每位使用者之始狀態皆設為 Good-user，子網路二與子網路三的使用者是以 Pareto on/off distribution 來傳輸封包，on 時間為 200ms，off 時間為 100ms，傳送速率為 2000kbps。子網路一的使用者則以 Constant Bit Rate (CBR) 的方式傳輸。

在上述條件下，流量監視器將分配每一子網路可用頻寬約為 667kbps，因子網路一有 8 位使用者登入，所以其 R_{max} 為 83.4kbps。

表 1 User-level 公平性之驗證(1)

	Generate Traffic	Average Throughput	Bad-user State
Node0	50kbps	49.02kbps	0%
Node1	50kbps	49.99kbps	0%
Node2	2000kbps	101.77kbps	99.58%
Node3	2000kbps	96.81kbps	99.48%
Node4	2000kbps	101.76kbps	99.53%
Node5	2000kbps	96.79kbps	99.48%
Node6	2000kbps	101.79kbps	99.48%
Node7	2000kbps	96.79kbps	99.48%

表 2 User-level 公平性之驗證(2)

	Generate Traffic	Average Throughput	Bad-user state
Node0	50kbps	49.31kbps	0%
Node1	90kbps	84.31kbps	51.03%
Node2	2000kbps	87.59kbps	54.55%
Node3	2000kbps	87.61kbps	54.65%
Node4	2000kbps	87.86kbps	54.55%
Node5	2000kbps	87.15kbps	53.57%
Node6	2000kbps	87.05kbps	53.88%
Node7	2000kbps	87.49kbps	54.14%

表 3 User-level 公平性之驗證(3)

	Generate Traffic	Average Throughput	Bad-user state
Node0	90kbps	78.39kbps	49.77%
Node1	90kbps	78.44kbps	49.82%
Node2	2000kbps	78.58kbps	49.92%
Node3	2000kbps	78.56kbps	49.92%
Node4	2000kbps	78.53kbps	49.82%
Node5	2000kbps	78.54kbps	49.92%
Node6	2000kbps	78.53kbps	49.92%
Node7	2000kbps	78.54kbps	49.97%

表 1~表 3 為驗證 User-level 公平性之模擬結果，由表 1 知，Node0 與 Node1 因其傳輸資料量小於 R_{max} ，整個傳輸過程皆處於 Good-user 狀態，其傳輸頻寬有被保證。而 Node2 與 Node7 因其傳輸資料量遠大於 R_{max} ，在整個傳輸過程大部份處於 Bad-user 狀態，但其所得到的網路頻寬在 Bad-user 中仍是公平的，且 Node0 與 Node1 沒用完的頻寬仍會給其它 node 使用，沒有造成頻寬的浪費。

當我們再將 Node1 的傳輸速率提升至 90kbps，則 Node1 與 Node2~Node7 相同，大部分是在 Bad-user 狀態，如表 2 所示。最後我們亦將 Node0 的傳輸速率提升至 90kbps，其結果如表 3 所示，此時 Node0~Node7 的平均傳輸速率皆大於 R_{max} ，所以大部分皆在 Bad-user 狀態，但頻寬並不會被某一使用者所獨佔。

由上述之結果知，本論文所提之機制確實可達到 flow-based 的頻寬管理與頻寬使用的公平性。

8. Conclusions

本論文提出一分層式之頻寬管理機制，在不更改現有網路設備功能下，加入邊緣閘道器、認證伺服器與流量監視器三部份，其以分散式架構，將頻寬管理的負擔分散到各個部份，以提供 flow-based 的使用者頻寬管理與 subnet-based 的公平頻寬使用，可將中毒電腦對整體網路的影響限制在子網路內，有效維護骨幹網路的傳輸順暢，同時，藉由使用者認證機制，可確認 IP 位址是否有被盜用，是在何時間、為何人所盜用，解決 IP 位址與使用者對應之困擾。

經由 NS2 電腦擬模結果顯示，在不同的網路使用條件下，本論文所提之分層式頻寬管理機制皆可達到 Subnet-level 與 User-level 的頻寬使用之公平性，確保正常網路使用者之網路使用品質。

參考文獻

[1] F. Ruixue, H. Shimonishi, H. Suzuki, and M. Yoshida, "An Improvement of Weighted Round Robin Cell Scheduling in ATM networks",

GLOBECOM '97, vol. 2, pp. 1119-1123, 1997.

[2] J. Nagle, "On Packet Switches with Infinite Storage", IEEE Transactions on Communications, Volume 35, pp 435-438, 1987.

[3] Cheng-Zhong Xu and Xiaobo Zhou "Harmonic Proportional Bandwidth Allocation and Scheduling for Service Differentiation on Streaming Servers," IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 15, no. 9, pp.835-848, 2004.

[4] Intel IXP400 Software Programmer's Guide, June 2004.

[5] Intel IXP42X Product Line of Network Processors and IXC1100 Control Plane Processor Datasheet.

[6] SAMSUNG Device Solution Network USER'S MANUAL S3C2500B.

[7] D. Black, E. Davies, M. Carlson, W. Weiss, S. Blake and Z. Wang, "An Architecture for Differentiated Services", RFC 2475. December 1998.

[8] Hui Zhang, Ion Stoica and Scott Shenker, "Core-Stateless Fair Queuing: Achieving Approximately Fair Bandwidth Allocations in High Speed Networks," IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 11, NO. 1, FEBRUARY 2003.

[9] Fernando Cerdan and Maria-Dolores Cano, "Proportional Bandwidth Distribution in IP Networks Implementation the Assured Forwarding PHB," Proceeding of the 10th IEEE Symposium on Computer and Communication (ISCC 2005.)

[10] Fernando Cerdan, Joan Garcia-Haro, Josemaria Malgosa-Sanahuja and Maria-Dolores Cano, "A new proposal for Assuring Services in Internet", Proceedings of the International Conference on Internet Computing IC'02, Vol. II pp.379-384, Las Vegas, USA, June 2002.

[11] R. Jain, "The Art of Computer Systems Performance Analysis", John Wiley and Sons Inc., 1991.

[12] The Network Simulator- NS2 Notes and documentation and source code.[Online]. <http://www.isl.edu/nsnam/ns>, retrieved 2006/4/12.

[13] IEEE Std. P802.1X/D11, "Standard for Port based Network Access Control", March 2001.

[14] M. Wahl, S. Kille and T. Howes, "Lightweight Directory Access Protocol (v3)", RFC 2251, December 1997.

[15] IXIA, "IxExplore 3.80 Users Guide: General Configuration and Operation", September, 2004.

[16] 方盈, TCP/IP 通訊協定-入門與應用。博碩文化, 2000。