國立草屯高級商工職業學校

申請 TANet 新世代骨幹網路

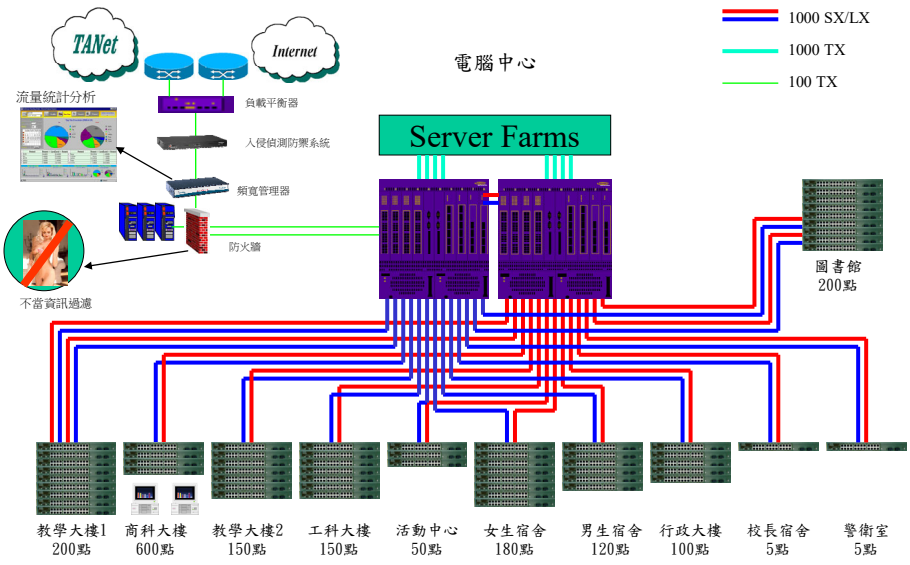
連線申請書

壹、前言

隨著 TANet 骨幹頻寬的更新擴充，使得 TANet 跨向了超高速乙太網路(Gigabit/FastEthernet)的新世代。而在此超高速乙太網路的新環境下使得 TANet 的應用將朝更多元化及更迅速的方向發展。因此，TANet 正積極開放讓各校申請新世代網路的連線。然而，在各校相繼以 Gigabit 或 FastEthernet 連接到 TANet 後，由於網路頻寬遠大於過去連線頻寬，因而將使過去 TANet 上所產生的問題更形嚴重，而這些問題的解決也更具急迫性。這些問題包括：一、地下網站或下載軟體更無限制的大量佔用骨幹流量，二、網路攻擊行為或 Code Red 等病毒攻擊將因頻寬的大量增加而造成更大的損害，三、廣告信件等垃圾郵件問題將因頻寬充裕而更加嚴重，四、不當(色情、暴力、犯罪、毒品)網站將更輕易的進入校園，污染學習環境。為解決這些問題，在 91/03/26 教育部所建議所修訂的◤TANet 新世代骨幹網路實驗計畫網路連接規範◢中，訂定數項規範，以便各校有所依循。本校為落實 TANet 網路資源合理使用及防範不當資訊在 TANet 散播的精神，全力配合，並執行本規範的相關規定，茲將本校執行本規定各項工作詳述於后。

貳、本校校園網路及申請說明

國立草屯商工網路骨幹架構圖



圖一

圖一顯示本校校園網路架構。本校校園網路骨幹目前以兩台 Extreme Black Diamond 6808 作為校園網路主交換機，並採用 Gigabit Ethernet 為校園網

路骨幹。目前本校擬申請 NetScreen 204 Firewall 等設備與 TANet 骨幹以 FastEthernet 連線。本校為執行 TANet 網路連接規範之相關規定，在由 Extreme Black Diamond 6808 至與 TANet 網路連接的路徑上，擺設了 NetScreen 204 Firewall、BandKeeper 頻寬管理器，NetKeeper 網路攻擊入侵偵測防禦系統等，並採用了 WebSence 網路濾淨資料庫以過濾不當資訊。以下將詳述本校執行，相關規定的詳細細節。

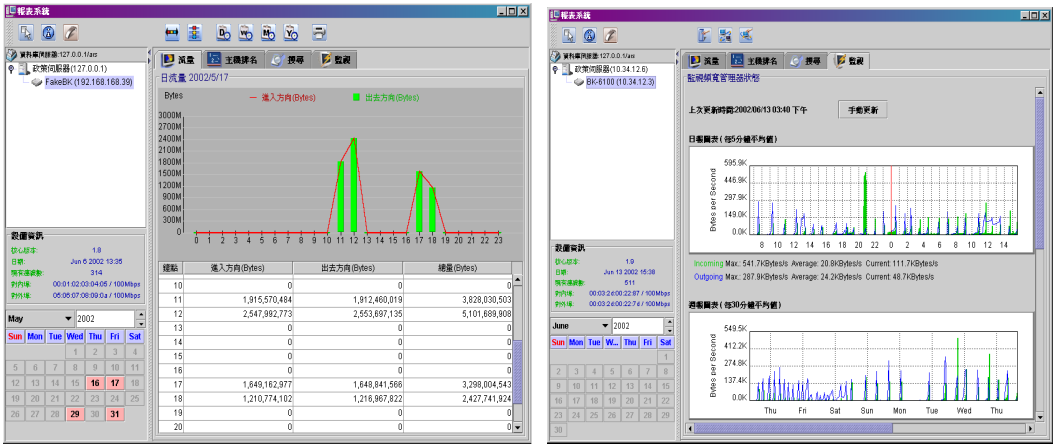
參、本校執行 TANet 網路連接規範相關規定之說明

一、需將本部頒定之◤教育部校園網路使用規範◢納入學校或機關實施的相關規範中。

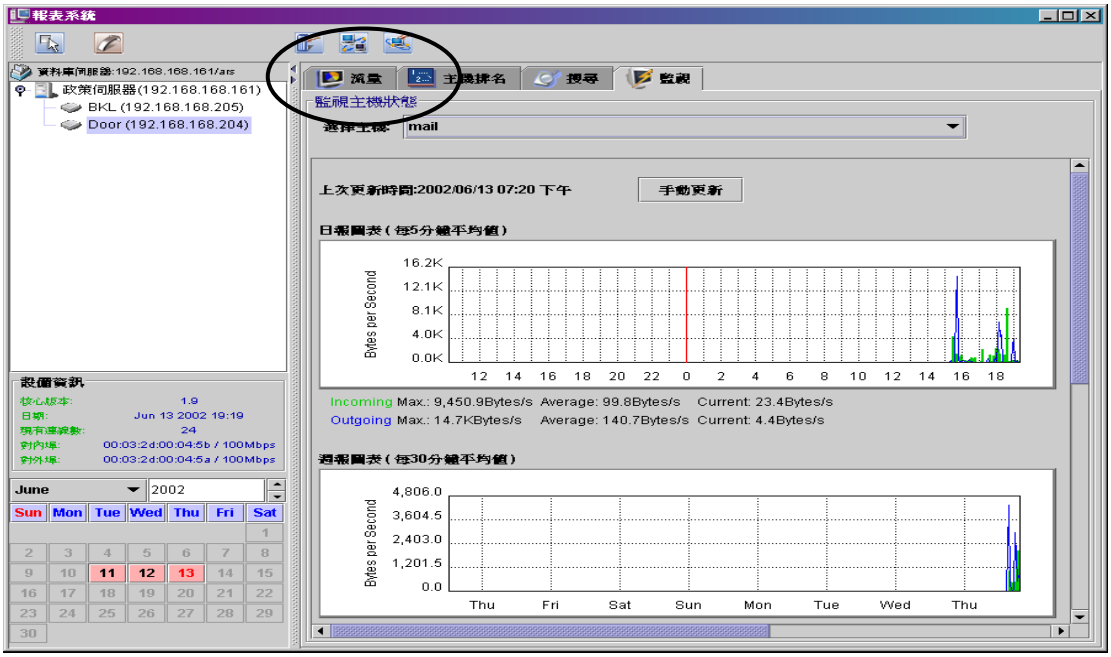
本校已於根據教育部所頒佈之◤教育部校園網路使用規範◢制定出◤校園網路使用規範◢。經由本校行政會議通過上述規範，並公佈於本校網站 http://163.22.44.3/tanet/rule.htm 實施。

二、需製作使用單位之流量統計圖，供相關管理人員參考。

本校所採用的 BandKeeper 頻寬管理器，除可提供整體 In/Out 的流量使用統計圖及頻寬使用統計圖外，更可針對單獨 IP 提供頻寬使用統計圖，因而可供管理人員針對整體網路流量，頻寬使用情形及個別 IP 頻寬使用變化情形進行監看。圖二，可顯示整體對外連線的流量使用情形及頻寬使用情形統計圖；圖三，則可為針對某一單獨 IP 進行頻寬使用情形監看，所產生此 IP 之頻寬使用變化圖。



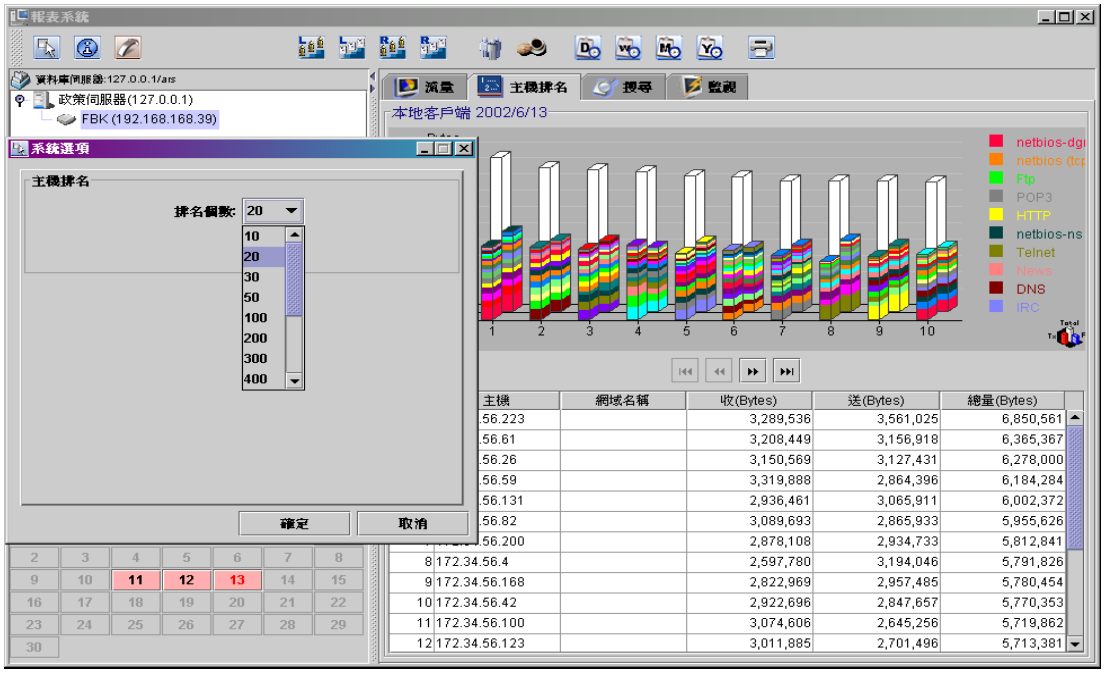
圖二



圖三

三、需公佈單位內對 TANet 前三十名 IP Adderss 使用量排行，並列出該 IP 使用之網路流量及該校流量平均值

本校所 BandKeeper 頻寬管理器，可提供 Top N 的 IP 流量使用排行及統計，同時可將此 ToP N 的 IP 流量所使用的應用分佈情形繪出，如圖四所顯示。管理者可根據此統計圖表，採取適當的措施。本校將 Top N 的使用排行，公佈於 http://163.22.44.3/taner/topn.html



圖四

四、需建立 abuse、security 這兩個 E-mail 帳號作為連絡使用(abuse 主要作為 spam 或攻擊等不當使用之反應帳號；security 用為資通安全通報使用)，並派專人處理此一帳號之信件。

本校已於 mail server 上建立 abuse 及 security 兩個 mail 帳號，以分別作為 spam mail，攻擊事件；及資通安全通報之連絡反應帳號，並以指派專人負責處理。abuse 及 security 兩個 E-mail 信箱均會轉寄到相關負責人的信箱，以隨時處理相關事件。有關人員亦可由本校學術網路網頁，http://163.22.44.3/tanet 發信到這兩個信箱。

五、應對學校或機關內至少以 Class C 為單位的 IP 使用及異動作登記管理，登記內容至少包含使用單位、管理人員及網段內提供服務之伺服器主機等項目。

本校已針對校內各單位 IP 使用範圍進行分配，並於各網段指定專人管理。將本校各單位所使用的 IP 範圍，負責人電話及 E-mail 信箱，以及各網段伺服器主機之 IP 繪製成表，以便於管理。本表亦已公佈於本校網站上，http://163.22.44.3/tanet/ipmap.htm

六、需建立對廣告信件或網路攻擊行為的反應處理機制，並提出具體之管理辦法及措施。

基於落實網路資源合理使用的概念，本校針對不當耗費網路資源的 SPAM 廣告信件或 CodeRed 等網路病蟲攻擊以及其他有意/無意之網路攻擊行為已採取適當的措施加以管理防制。茲說明如下。

針對廣告信件 SPAM 行為，本校採取下列管理辦法及措施：

- 對於校內已登記的合法 Mail Server，加強管理，增加 Mail Server 的安全性，避免被當成 Mail Relay。
- 經由 abuse 所舉報的 SPAM 主機
  - 若為校內已登記之 Mail 主機，則以 BandKeeper 頻寬管理器限制該對外之 SMTP (Port 25)服最大使用頻寬為 1Mbps，每日最大傳送流量限流為 100MB，同一時間對外連線數(Concurrent Connections)限制不超過 2 條，並通知該網段管理人員，限期於一個月內改善，並回報。若一個月後未見改善，則以 BandKeeper 頻寬管理器，關閉該主機對外之所有連線，直到改善為止。
  - 若為校內未登記之地下站台或 PC，則以 BandKeeper 頻寬管理器關閉該地下主機或 PC 對外之所有連線三個月，並於三個月

開放後，限制該主機或 PC 一年內每天流量不超過 200MB，並公告於本校網頁 http://163.22.44.3/tanet/spam.htm

- ■ 若為校外主機，則本校將以 BandKeeper 頻寬管理器，關閉該主機與本校內部之 SMTP 服務，並以 Mail 通知該主機之管理者，直到該校外主機改善後才再開放雙方之 SMTP 服務。

- ➢ 若經由本校之所發覺校外的 SPAM，則將主動透過 abuse 帳號通知教育部，台中區網及鄰近各校。
- ➢ 圖五，顯示 BandKeeper 頻寬管理器用以限頻及限流的機制。

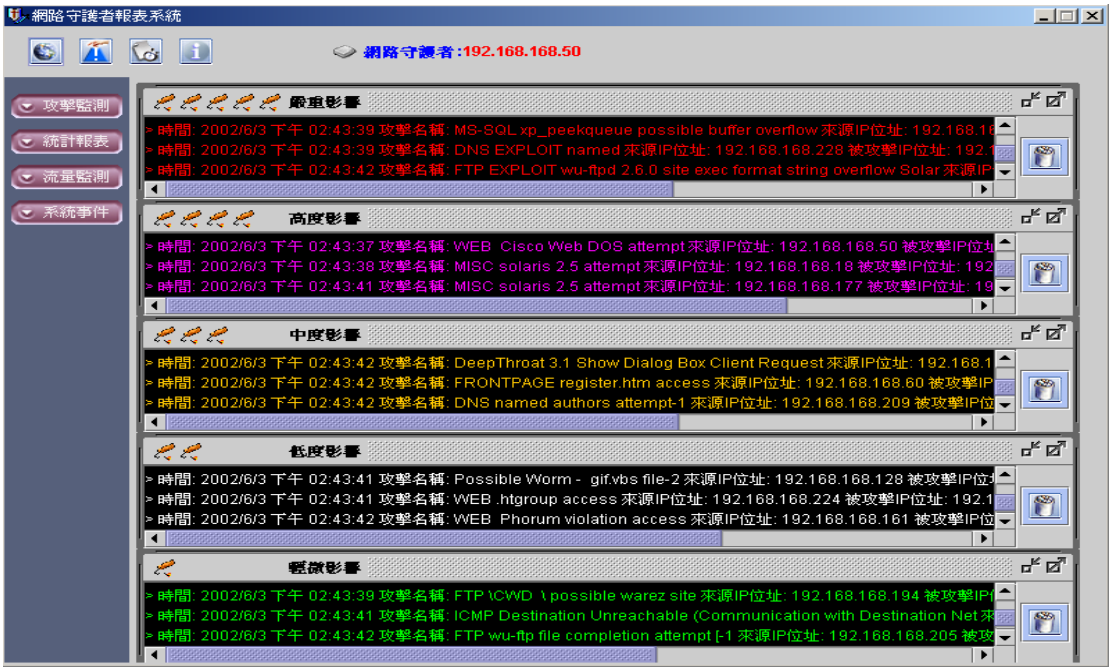
圖五

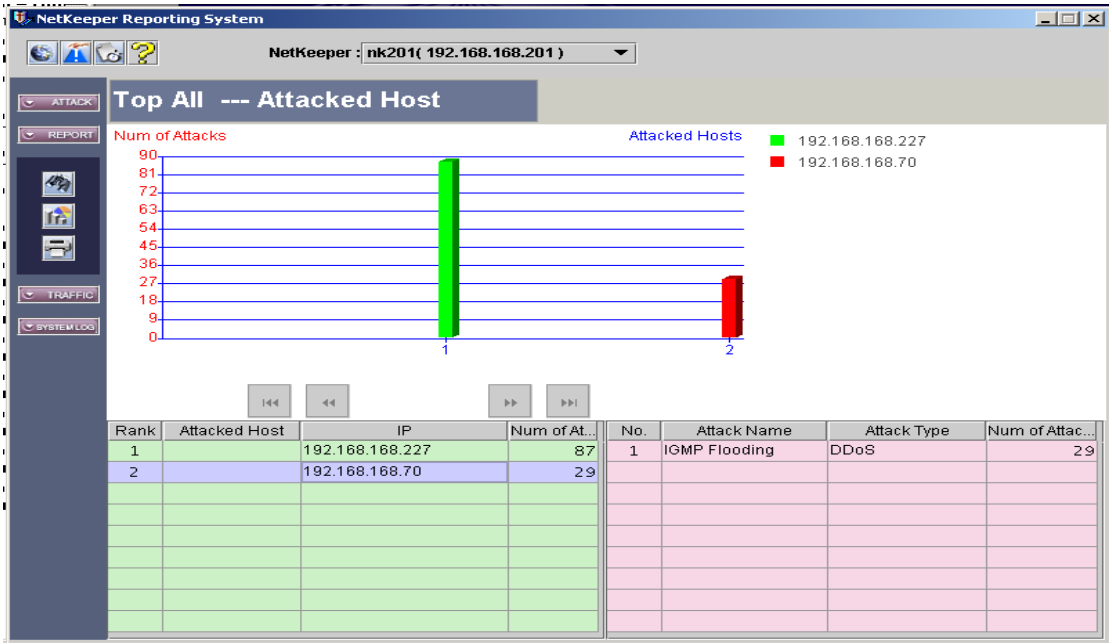
針對 CodeRed 等網路病蟲攻擊或其他有意/無意之網路攻擊行為，本校所採取的管理防制措施如下：

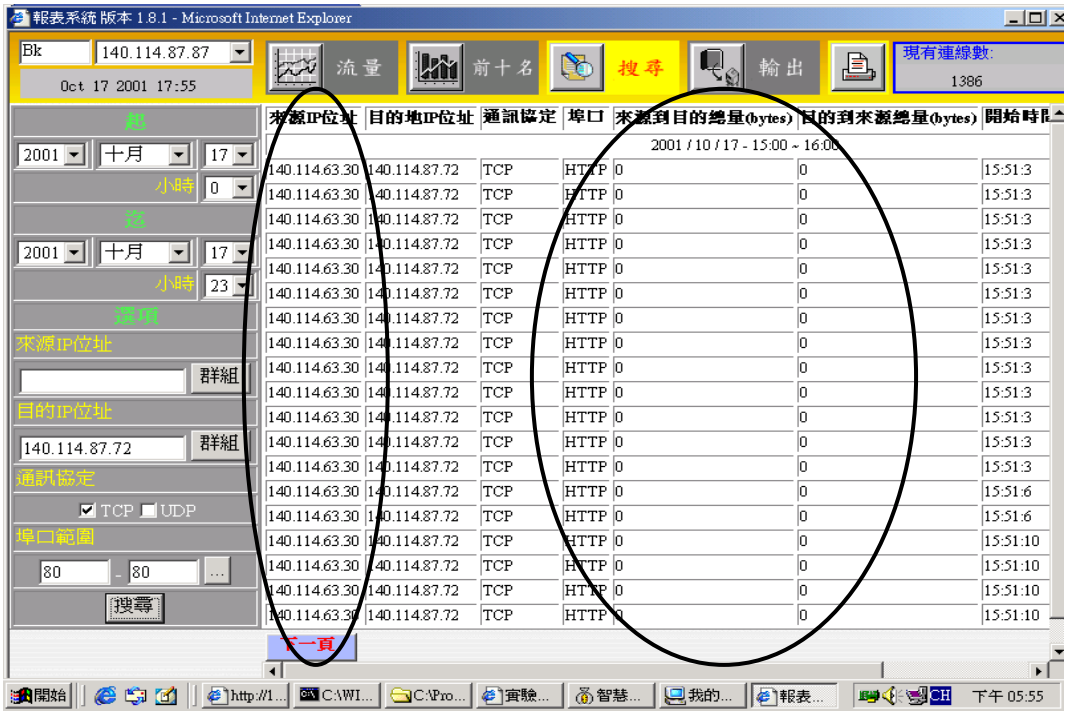
- ➢ 本校採用 NetKeeper 網路入侵攻擊測防禦系統來防制由校園網路到 TANet 或由外部進入校園網路之網路攻擊。本系統可選擇採取雙向或單邊防禦，並可有效防禦包括 CodeRed 網路在內的大約一千種的有意/無意之網路攻擊。而此，防禦系統更有及時監看及事後通報記錄追查之功能。圖六，是 NetKeeper 所偵測到的網路攻擊情形，及相關報表記錄。
- ➢ 本校除採用 NetKeeper 採取主動防範網路攻擊事件外，更以 BandKeeper 配合偵測及管制受 CodeRed 網路病的 PC。相關措施如下：
  - ■ 由 BandKeeper 的報表系統(如圖七)及 NetKeeper 的偵測中，本校管理人員可偵測出內部受到 CodeRed 網路病蟲感染的 PC 及外部攻擊至本校的來源。
  - ■ 對於內部受感染的 PC，本校管理人員會 BandKeeper 的頻寬管

理功能，關閉其對 TANet 之連線，並將其 IP 公告於本校網頁 http://163.22.44.3/tanet/codered.htm，並求使用者需改善後始得連上 TANet。

- 本校採用之 Netkeeper 並已設有閘道防毒功能，並將最新網路安全相關訊息公告給全校使用者。此外，如何解毒，也是本網頁服務項目之一。本網站網址為 http://163.22.44.3/tanet/security.htm。
- 由 BandKeeper 及 NetKeeper 所發覺的來自外部 PC 之 CodeRed 或其他網路攻擊。本校將透過，abuse 或 security 兩個信箱通知相關單位應變。







圖七

七、需建立過濾機制，阻擋犯罪與色情之資訊或網頁，具體辦法及相關軟硬體設施。

為致力於網路上的掃黃，掃黑工作，本校採用 WebSence 網路濾淨資料庫來淨化校園網路。本校所有使用者的 Web 瀏覽，都會被本校出口的 NetScreen Firewall 導入 WebSence 做檢查，一旦在資料庫中發現該筆瀏覽為不當網站的瀏覽時，將會拒絕使用者存取該網站，並通知該使用者。不當網站資料庫具有更新資料庫的機制，因此可保持最新最有效的過濾能力。此外，本校亦已建立不當網站檢舉信箱 badsite@ mail.ttvs.ntct.edu.tw，並公佈於本校網頁 http://163.22.44.3/tanet/ badsite.html，使用者可透過檢舉信箱向本校人員檢舉，經相關人員查證屬實後，本校相關負責人員將會將此不當網站加入資料庫中，並將此網站加入其更新伺服器中。

此外，為防範不當資訊的擴散傳播，本校針對校園網路內的地下站台，亦採取預先防範的措施：本校採用 BandKeeper 頻寬管理器，將非註測登記為校內合法伺服器的 PC，限制每日對 TANet 傳輸量不超過 500MB。此外，經檢舉或本校管理者發現架設地下不當資訊站台時，除依◤校園網路使用規範◢處理外，本校網管人員還會先限制該 IP 對 TANet 的上傳頻寬成為 20Kbps。如此，可有效防止本校校園網路內，產生不當資訊地下網站。

肆、結語

本校過去一直致力於校園網路發展，隨著校務蒸蒸日上及本校校園網路的迅速發展，曾先後不斷更新電路與頻寬，然本校校園網路骨幹已於民國 93 年初全面更新為 Gigabit Ethernet，現今對外頻寬已有不足現象。今本校已完成◤TANet 新世代骨幹網路實驗計畫◢連接規範中的各項要求，懇請◤區域網路管理委員會◢及◤台灣學術網路管理委員會◢能准許本校以 FastEthernet 介接區網中心。本校保證當一本初衷，致力執行 TANet 所制定的各項網路管理政策，以維護 TANet 運作順暢。