彰化私立達德商工「TANet 新世代骨幹網路實驗計畫」

連線申請書

電腦中心網路組　　九十四年五月三日

連線申請說明

一、*訂定校園網路使用規範*

本校於 91 年 09 月 09 日主管會議初審 91 年 12 月 30 日教務會議通過「校園網路使用規範」。規範全文如下：(網址為　http://www.tdvs.chc.edu.tw/statute.htm)：

達德商工校園網路使用規範

一、 依據

教育部校園網路使用規範 【教育部 90 電創 184016 號文 中華民國 90 年 12 月 26 日核定】

二、規範目的

（一） 本校為恪遵台灣學術網路(TANet)管理公約。

（二） 使用校園網路資源之個人與單位皆適用此規範。

（三） 為充分發揮校園網路（以下簡稱網路）功能、普及尊重法治觀念，並提供網路使用者可資遵循之準據，以促進教育及學習，特訂定本規範。

三、尊重智慧財產權

本校校園網路使用者應尊重智慧財產權，避免下列可能涉及侵害智慧財產權之行為：

（一）使用未經授權之電腦程式。

（二）違法下載、拷貝受著作權法保護之著作。

（三）未經著作權人之同意，將受保護之著作上傳於公開之網站上。

（四）BBS 或其他線上討論區上之文章，經作者明示禁止轉載，而仍然任意轉載。

（五）架設網站供公眾違法下載受保護之著作。

（六）其他可能涉及侵害智慧財產權之行為。

四、禁止濫用網路系統
本校校園網路使用者應使用者不得為下列行為：
（一） 散布電腦病毒或其他干擾或破壞系統機能之程式。
（二） 擅自截取網路傳輸訊息。
（四） 以破解、盜用或冒用他人帳號及密碼等方式，未經授權使用網路資源，或無故洩漏他
人之帳號及密碼。
（五） 禁止將帳號借予、買賣，並不得私設或竄改校園網路節點上任何電腦之網際網路位址
（IP Adress 簡稱 IP）與他人使用。
（六） 隱藏帳號或使用虛假帳號。〔但經明確授權得匿名使用者不在此限〕
（七） 窺視他人之電子郵件或檔案。
（八） 以任何方式濫用網路資源，包括以電子郵件大量傳送廣告信、連鎖信或無用之信息，
或以灌爆信箱、掠奪資源等方式，影響系統之正常運作。
（九） 以電子郵件、留言版、討論區、線上談話、電子佈告欄（BBS）或類似功能之方法散
布詐欺、誹謗、侮辱、猥褻、騷擾、非法軟體交易或其他違法之訊息。
（十） 禁止散佈及瀏覽色情寫真、違背善良道德資訊、賭博、驚悚、暴力、配對、援交、一
夜情、違禁藥物、毒品交易、軍火、犯罪教學、自殺、線上買賣證券期貨等網站。
（十一）利用學校之網路資源從事非教學研究等相關之活動〔如商業性之行為〕或違法行為。
（十二）任何不合法之套裝軟體不得安裝、儲存、使用於校園網路系統內。
（十三）非法入侵他人主機或資料庫，進行盜拷竄改毀損重要資料、攻擊破壞干擾系統作業
等行為。

五、網路之管理
本校為執行教育部校園網路規範之內容，其有關校園網路之管理事項如下：
（一）協助網路使用者建立自律機制。
（二）對網路流量應為適當之區隔與管控。
（三）對於違反教育部校園網路規範或影響網路正常運作者，得暫停該使用者使用之權利，
情節重大、違反校規或法令者，將轉請學校處置。
（四）BBS 及其他網站設置專人負責管理、維護。違反網站使用規則者，負責人得刪除其文
章或暫停其使用。情節重大、違反校規或法令者，將轉請訓導處或司法機關處置。
（五）使用者若發現系統安全有任何缺陷，應儘速報告學校網路管理單位處理。

六、網路隱私權之保護
本校尊重網路隱私權，網管者不得任意窺視使用者之個人資料或有其他侵犯隱私權之行為。但有下列情形之一者，不在此限：
（一）為維護或檢查系統安全。
（二）依合理之根據，懷疑有違反校規之情事時，為取得證據或調查不當行為。
（三）為配合司法機關之調查。
（四）其他依法令之行為。

七、違反之處分
本校網路使用者違反校園使用規範者，將受到下列之處分：
（一）停止使用學校任何網路資源。
（二）接受校規之處分。學生則依本校〔學生獎懲辦法〕處理。
（三）網路管理者違反本規範者，應加重其處分。
（四）依前兩項規定之處分者，其另有違法行為時，行為人尚應依民法、刑法、著作權法或
其他相關法令負法律責任。其他未盡事宜，均依現行法令規定辦理。

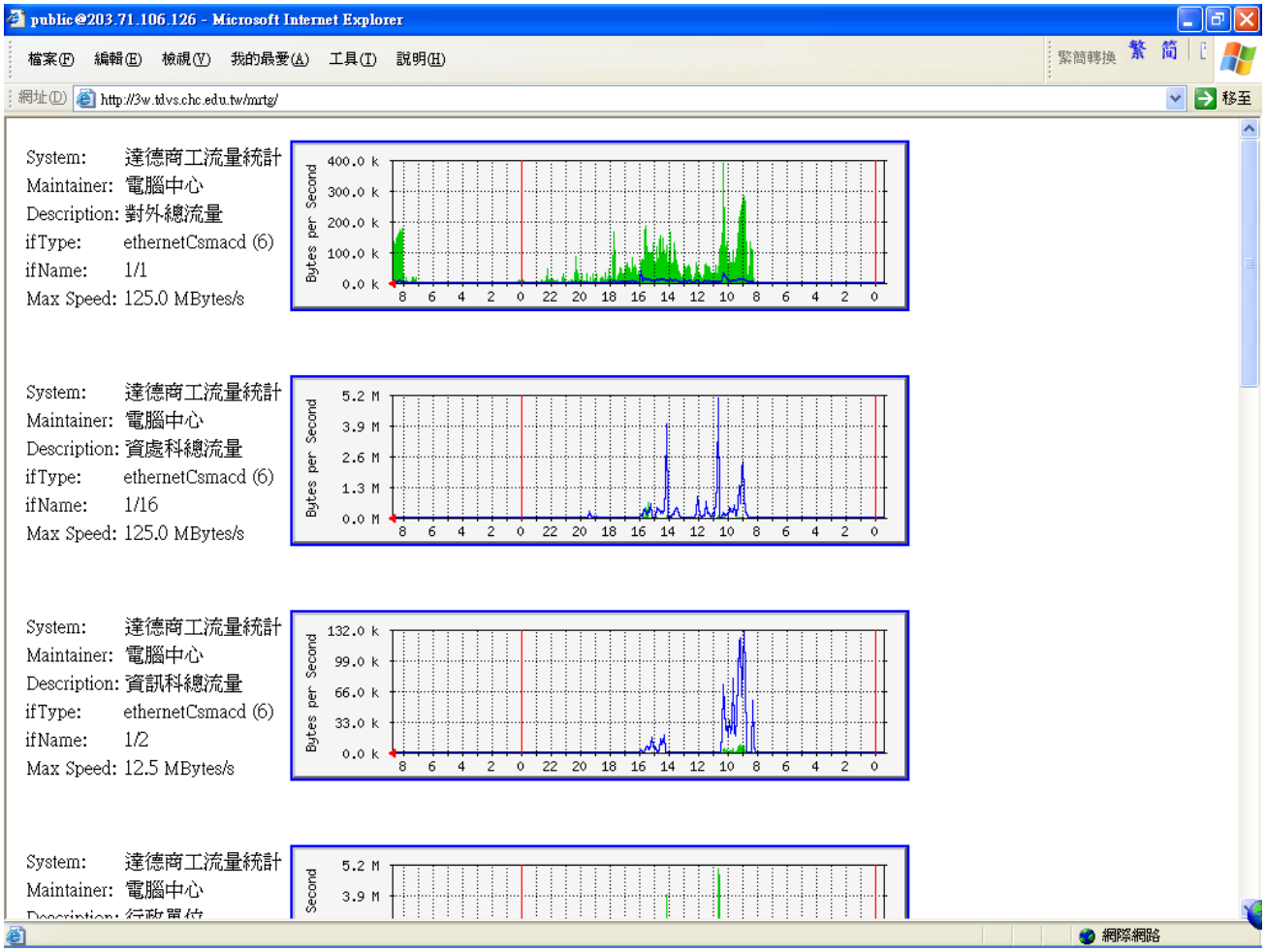
八、校園網路使用規範處理原則及程序
若違規事件經學生部分將依循學校訓育規範之原則與程序處理，教師及職工則依人評會規範程序處理。

九、實施
本規範經行政會議通過，呈請校長核可後公佈施行，修訂時亦同。

建議在『學生獎懲辦法』中關於學生違反『校園網路使用規範』者的懲處規定新增如下：
★違反校園網路使用規範，情節輕微者，應予記警告。
★違反校園網路使用規範，情節嚴重者，應予記小過。
★侵害他人智慧財產權情節嚴重者，應予記大過。
★擅自侵入他人資訊系統或設備，致生重大損害者，應予記大過。
★建立色情暴力網站或其他利用網路從事不法行為者，應予記大過。
★其他違反校園網路使用規範，情節嚴重致生重大損害者，應予記大過。

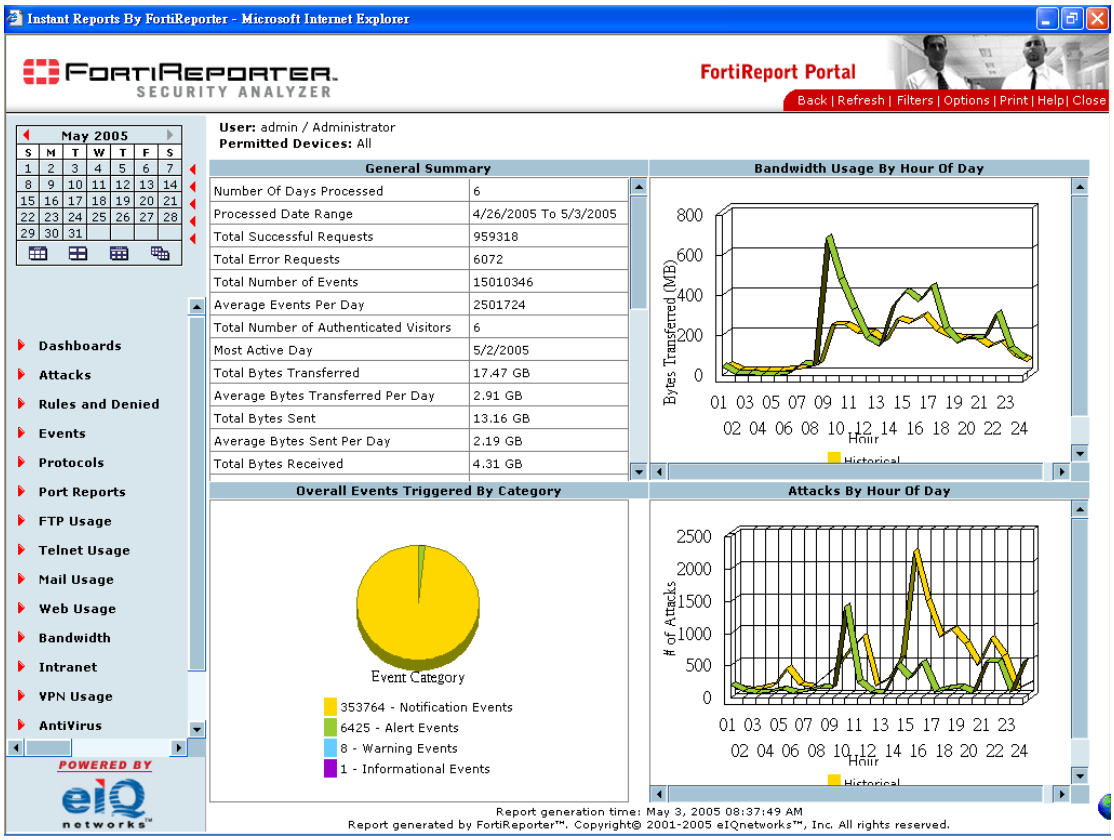
二、單位流量統計圖

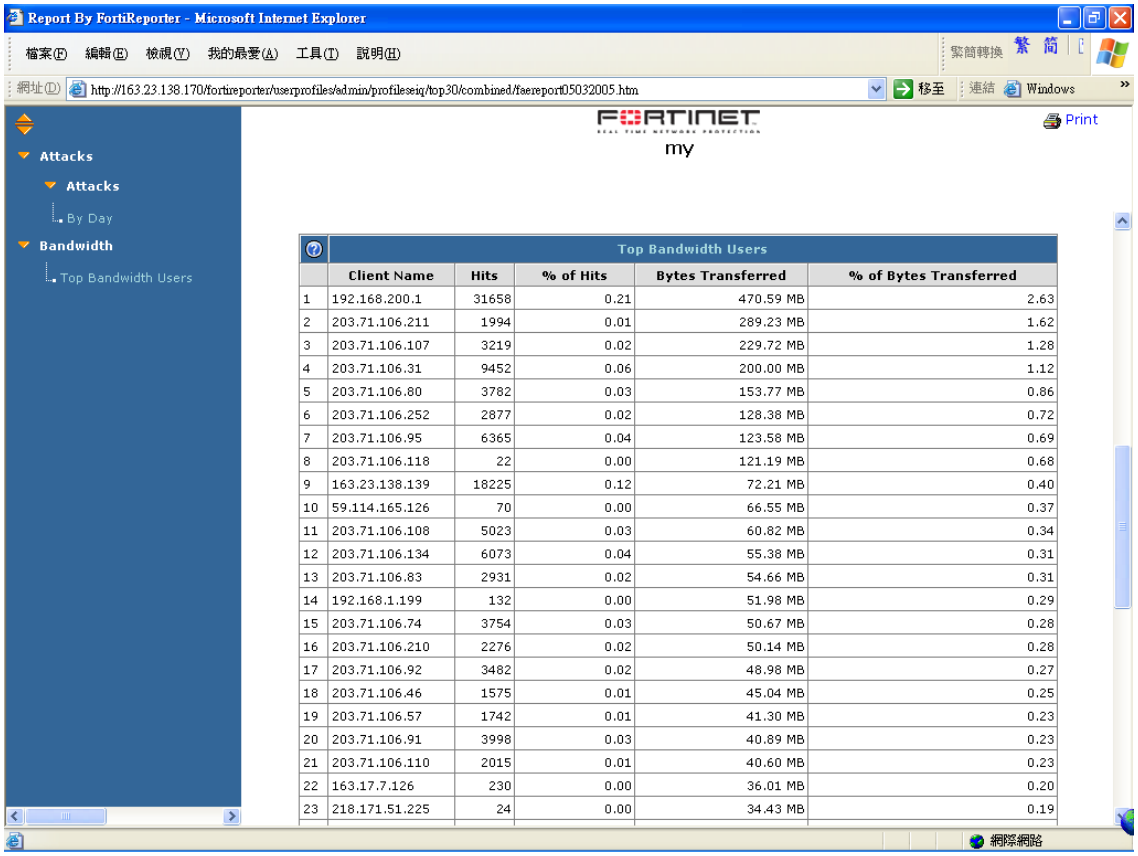
本校流量統計之 MRTG 圖網址為： http://3w.tdvs.chc.edu.tw/mrtg/



三、前三十名 IP 使用排行

本校流量排行以 FortiReporter(防火牆報表軟體)將核心交換機之 netflow 導入，分析後以報表方式呈現，網址為：http://163.23.138.170/fortireporter/





Top Bandwidth Users

	Client Name	Hits	% of Hits	Bytes Transferred	% of Bytes Transferred
1	192.168.200.1	31658	0.21	470.59 MB	2.63
2	203.71.106.211	1994	0.01	289.23 MB	1.62
3	203.71.106.107	3219	0.02	229.72 MB	1.28
4	203.71.106.31	9452	0.06	200.00 MB	1.12
5	203.71.106.80	3782	0.03	153.77 MB	0.86
6	203.71.106.252	2877	0.02	128.38 MB	0.72
7	203.71.106.95	6365	0.04	123.58 MB	0.69
8	203.71.106.118	22	0.00	121.19 MB	0.68
9	163.23.138.139	18225	0.12	72.21 MB	0.40
10	59.114.165.126	70	0.00	66.55 MB	0.37
11	203.71.106.108	5023	0.03	60.82 MB	0.34
12	203.71.106.134	6073	0.04	55.38 MB	0.31
13	203.71.106.83	2931	0.02	54.66 MB	0.31
14	192.168.1.199	132	0.00	51.98 MB	0.29
15	203.71.106.74	3754	0.03	50.67 MB	0.28
16	203.71.106.210	2276	0.02	50.14 MB	0.28
17	203.71.106.92	3482	0.02	48.98 MB	0.27
18	203.71.106.46	1575	0.01	45.04 MB	0.25
19	203.71.106.57	1742	0.01	41.30 MB	0.23
20	203.71.106.91	3998	0.03	40.89 MB	0.23
21	203.71.106.110	2015	0.01	40.60 MB	0.23
22	163.17.7.126	230	0.00	36.01 MB	0.20
23	218.171.51.225	24	0.00	34.43 MB	0.19

四、建立 abuse、security 之專人管理 e-mail 帳號

本校建立之帳號為 abuse@tdvs.chc.edu.tw 及 security@tdvs.chc.edu.tw 。將會轉寄電腦中心網路組由專人處理。

五、本校各單位 IP 管理及主機資料

私立彰化達德商工 IP 分配使用狀況一覽表 （校內一律採用虛擬 IP）

IP 位址	使用單位	管理人員
203.71.X.0(DHCP)	行政單位	網路組(04-8753929 轉 179)
192.168.0.0 至 192.168.12.0(DHCP)	資處科電腦教室	網路組
192.168.200.0(DHCP)	資訊科電腦教室	網路組

私立彰化達德商工伺服主機一覽表

伺服器 IP	伺服器名稱	伺服器功能
163.23.X.Y0	dns.tdvs.chc.edu.tw	學校 DNS 伺服器
163.23.X.Y1	Mail.tdvs.chc.edu.tw	行政 mail 伺服器
163.23.X. Y2	ftp.tdvs.chc.edu.tw	學校 FTP 伺服器
163.23.X.Y4	www.tdvs.chc.edu.tw	學校 Web 伺服器
163.23.X.Y5	teach.tdvs.chc.edu.tw	教師教學伺服器
163.23.X.Y6	Ms1.tdvs.chc.edu.tw	學生 mail 伺服器
163.23.X.Y7	3w.tdvs.chc.edu.tw	學生 Web 伺服器

六、廣告信件&網路攻擊之處理機制

網址：http://www.tdvs.chc.edu.tw/state.asp

廣告信反應處理機制

關閉 mail 伺服器 mail relay 功能，防止校外 IP 之信件轉寄。

利用流量分析報表軟體進行監測，如有發現異常之連線情形，便拒絕其連線。

建立 abuse 電子郵件帳號，供使用者檢舉廣告信件。

網路攻擊行為反應處理機制

利用流量分析報表軟體進行監測，如有發現異常之連線情形，便拒絕其連線。

使用 IPS，防火牆將自動偵測並防堵攻擊行為。

分析防火牆 Log File，關閉攻擊行為之相關 port 並阻絕異常連線之 IP。

建立 security 電子郵件帳號，供使用者檢舉資通安全事件。

病毒反應處理機制

各伺服器以 Symantec AntiVirus 做為防護機制。

各工作站以 Symantec AntiVirus 做為防護機制。

電子郵件以 TREND ScanMail 做為防護機制。

七、色情與犯罪資訊網頁之過濾機制

色情防制機制

網頁要求一律導向防火牆網頁過濾，並依據 sex filter 清單，做為色情過濾機制，目前已建有數萬筆資料。

利用流量分析報表軟體進行 IP 流向追蹤，如發現異常連線，經追查若為犯罪、色情 或其他不當網站，便將該網址加入防火牆網頁過濾的過濾清單中。

即時阻絕不良網站之畫面如下：

http://www.sex.com/ - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
繁簡轉換 繁
網址(D) http://www.sex.com/
移至
The URL you requested has been blocked. URL = www.sex.com
完成
網際網路