



桃園縣成功高級工商職業學校

Private Chen-kung Senior Industrial & Commercial Vocational School

TANET新世代骨幹網路



大綱說明

- 緣由

- 各項規範

- 1.教育部校園網路使用規範及處理機制
- 2.流量統計圖
- 3.前 30 名 IP Address IN/OUT 流量排名
- 4.聯絡 E-Mail 帳號
- 5.IP 使用及異動作業登記管理
- 6.廣告信件或網路攻擊行為的反應處理機制，並建立處理現況及公告網頁
- 7.網路不當資訊(含犯罪與色情)過濾系統及防制處理機制建置方式
- 8.申請連線計劃書相關事宜是否經學校或單位主管確認

- 網路架構

- 發展目標



緣由：

- 一、當初本校已趨近高速網路連線之架構，因尚未達到教育部頒定的連線規範標準，雖有寬頻之硬體建設仍然未能核准以高速頻寬連線，當初僅以T1(1.544Mbps)連接使用 TANET 網路骨幹。
- 二、校園骨幹設備線路已有基礎之架構，因應整體學術網路之發展，仍需以主流趨勢的架構與設備做改善。
- 三、本校網路建設均逐步朝向「教與學數位化」的目標前進，為了跟上數位學習平台。對於降低授課成本、提升教學品質、發展學校招生形象，尚待進一步研擬可行的方案，逐步建設完成，用以滿足將來的需求。



規範 (1) :

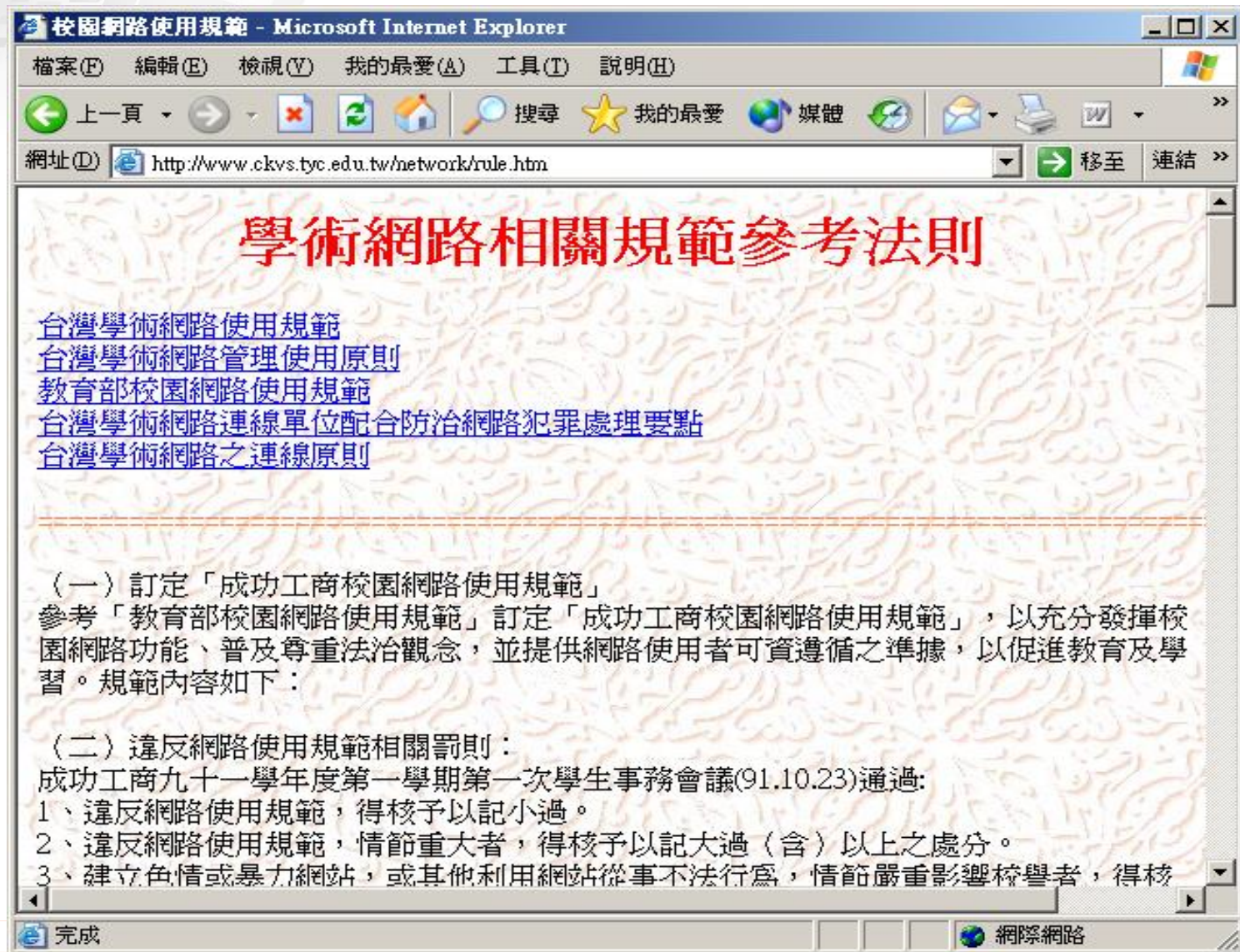
教育部校園網路使用規範及處理機制：

依教育部提供之資料納入校規規範處理，
並於以下網站位址公告說明！

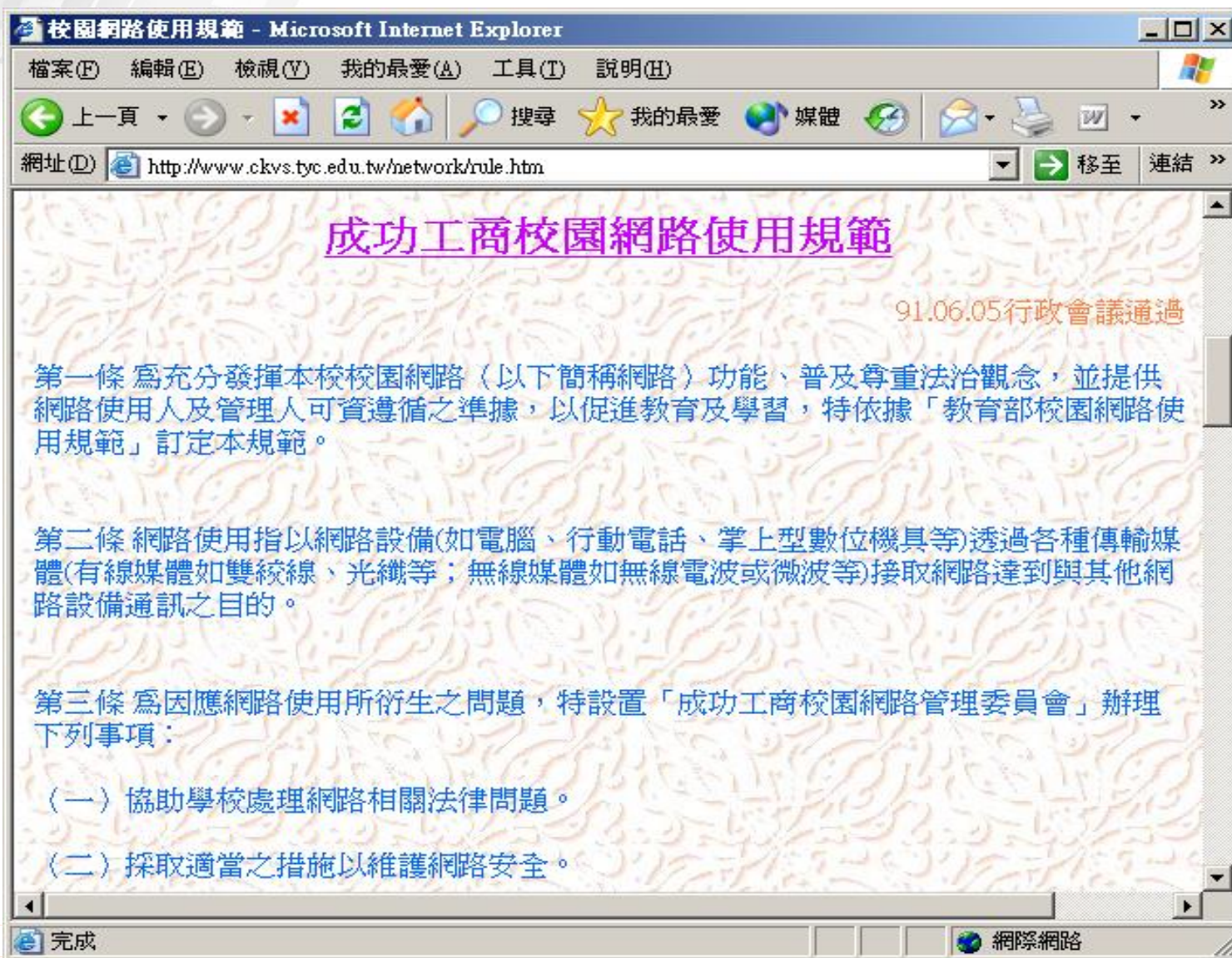
<http://www.ckvs.tyc.edu.tw/network/rule.htm>



範例 (1) :



範例 (2) :



規範 (2) :

網路流量統計：

(學校電算中心管轄主要Router及Switch的MRTG流量圖)

建立〔流量統計伺服器〕連結至 TANET 骨幹網路之流量

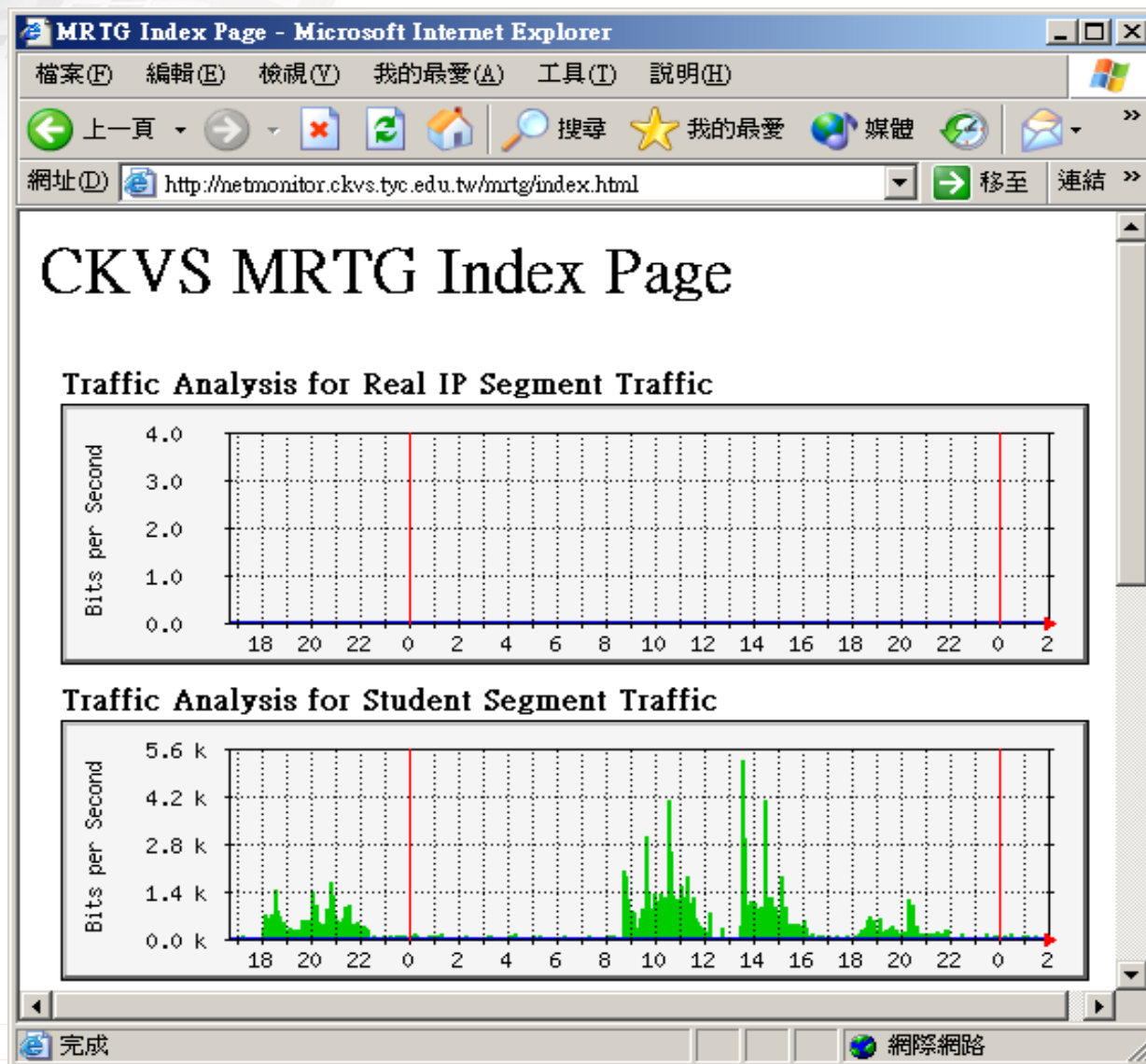
情形，以利掌握網路使用狀況。

並於以下網站位址公告說明！

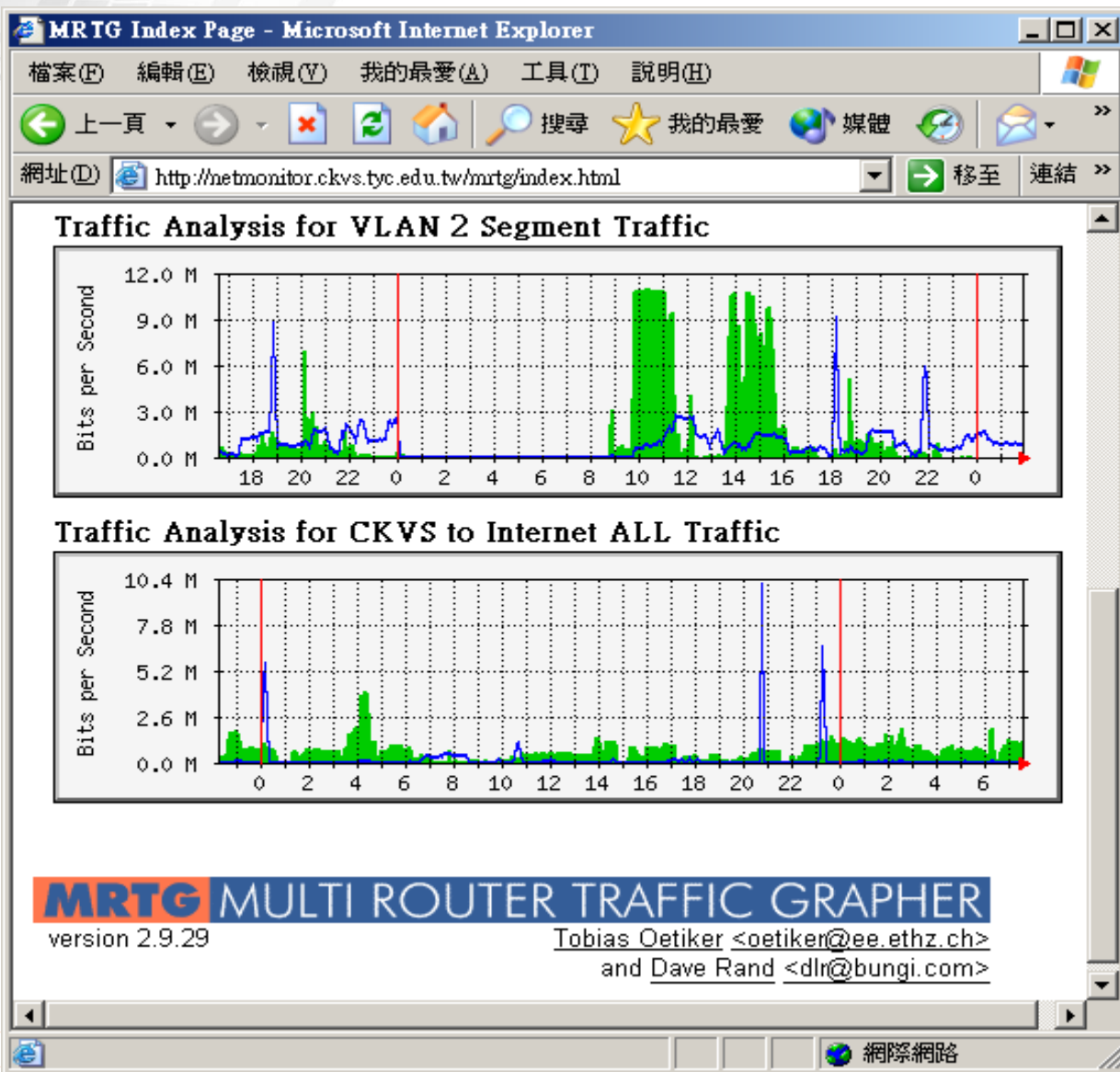
<http://netmonitor.ckvs.tyc.edu.tw/mrtg/index.html>



範例 (1) :



範例 (2) :



範例 (3)：

網路使用流量前三十名IP Address排行：
(學校對TANET流量In/Out排名)

建立「流量統計伺服器」連結至 TANET 骨幹網路之流量分配情形，以利掌握網路使用狀況。

<http://netmonitor.ckvs.tyc.edu.tw/nm/index.html>



規範 (3) :



範例 (1) :

成功工商網路流量統計 - Microsoft Internet Explorer

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

← 上一頁 → 搜尋 我的最愛 媒體 移至 連結 >>

網址(D) <http://netmonitor.ckvs.tyc.edu.tw/nm/hour.html>

按流出量 (位元組數) 排序

Number	IP	Bytes (Flow Inside)	Bytes (Flow Outside)	Packets (Flow Inside)	Packets (Flow Outside)	Average B/sec (Flow Inside)	Average B/sec (Flow Outside)
1	210.60.160.48	13,763,098	425,149,375	201,080	387,665	3,823	118,097
2	210.60.160.200	2,455,266	1,713,292	23,931	24,328	682	475
3	210.60.160.5	380,953	1,293,117	1,624	2,184	105	359
4	210.60.160.7	121,595	324,026	638	678	33	90
5	210.60.160.252	163,234	166,279	1,877	1,890	45	46
6	210.60.160.4	253,128	157,060	640	648	70	43
7	210.60.160.251	58,914	92,886	453	445	16	25
8	210.60.160.1	73,419	58,355	339	298	20	16
9	210.60.160.254	56,692	57,132	500	494	15	15
10	210.60.160.11	52,038	50,616	464	444	14	14
11	210.60.160.253	27,392	27,332	245	245	7	7
12	210.60.160.45	27,164	26,790	240	235	7	7
13	210.60.160.202	17,689	15,814	132	135	4	4
14	210.60.160.250	12,754	12,426	113	109	3	3
15	210.60.160.20	12,730	12,426	113	109	3	3
16	210.60.160.6	12,430	12,198	110	107	3	3
17	210.60.160.91	55,822	0	492	0	15	0
18	210.60.160.10	51,874	0	459	0	14	0
19	210.60.160.13	51,718	0	455	0	14	0
20	210.60.160.111	51,536	0	454	0	14	0

完成 網際網路



規範 (4) :

Abuse及security電子郵件帳號管理與問題處理 :

已建立

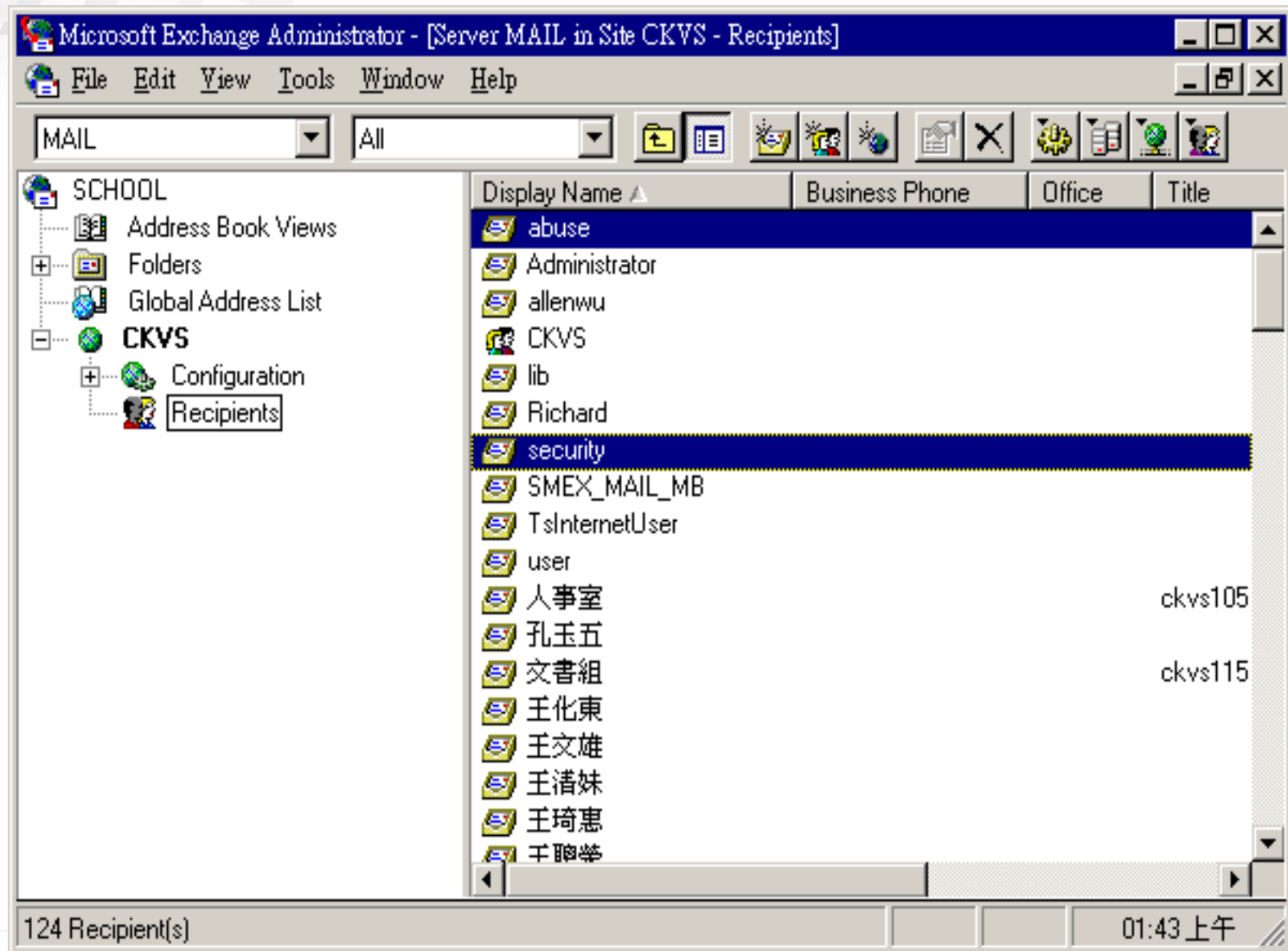
abuse@ckvs.tyc.edu.tw，security@ckvs.tyc.edu.tw
等二個帳號，並有專人負責處理帳號之信件，abuse帳號由
電子郵件管理者負責，security帳號由資訊安全管理人員
負責。處理信件之時效以不超過三個工作天為原則。

Mail Account 建立於校內郵件伺服器：

Mail.ckvs.tyc.edu.tw



範例 (1) :



範例 (2) :

網路狀況反應及通報 E-MAIL 帳號

網路狀況	通報E-MAIL 帳號
spam或攻擊等不當使用	abuse@ckvs.tyc.edu.tw
資通安全通報	security@ckvs.tyc.edu.tw

**** 負責人員：張秀春** jschun@ckvs.tyc.edu.tw

[回上頁](#)



規範 (5)：

IP 使用及異動作業登記管理：

校內所使用之IP位址均由電算中心管理，並統一負責登記分配行政、教學、研究單位使用。

並於以下網站位址公告說明！

<http://www.ckvs.tyc.edu.tw/network/ip.htm>



範例 (1) :

成功工商 IP 使用分配表 - Microsoft Internet Explorer

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

← 上一頁 → 搜尋 ★ 我的最愛 媒體 → 移至 連結 >>

網址(D) <http://www.ckvs.tyc.edu.tw/network/ip.htm>

成功工商 IP 使用分配表

IP 位址	使用單位 (功能)	IP 位址	使用單位 (功能)
210.60.160.1	資訊中心 (Web Mail伺服器)	210.60.160.128	none
210.60.160.2	資訊中心 (郵件伺服器)	210.60.160.129	none
210.60.160.3	none	210.60.160.130	none
210.60.160.4	資訊中心 (Domain Controller)	210.60.160.131	none
210.60.160.5	資訊中心 (DNS/WEB/SMTP 伺服器)	210.60.160.132	none
210.60.160.6	資訊中心(CKSER1)	210.60.160.133	none
210.60.160.7	福利社 (進銷存系統 ELIFE)	210.60.160.134	none
210.60.160.8	圖書館 (圖書系統 CC-PC51)	210.60.160.135	none
210.60.160.9	進修補校 (CC-PC7)	210.60.160.136	none
210.60.160.10	公文主機 (CKVS)	210.60.160.137	none
210.60.160.11	資訊中心(e-Course)	210.60.160.138	none

完成 網際網路



規範 (6) :

廣告信件或網路攻擊行為的反應處理機制，
並建立處理現況及公告網頁：

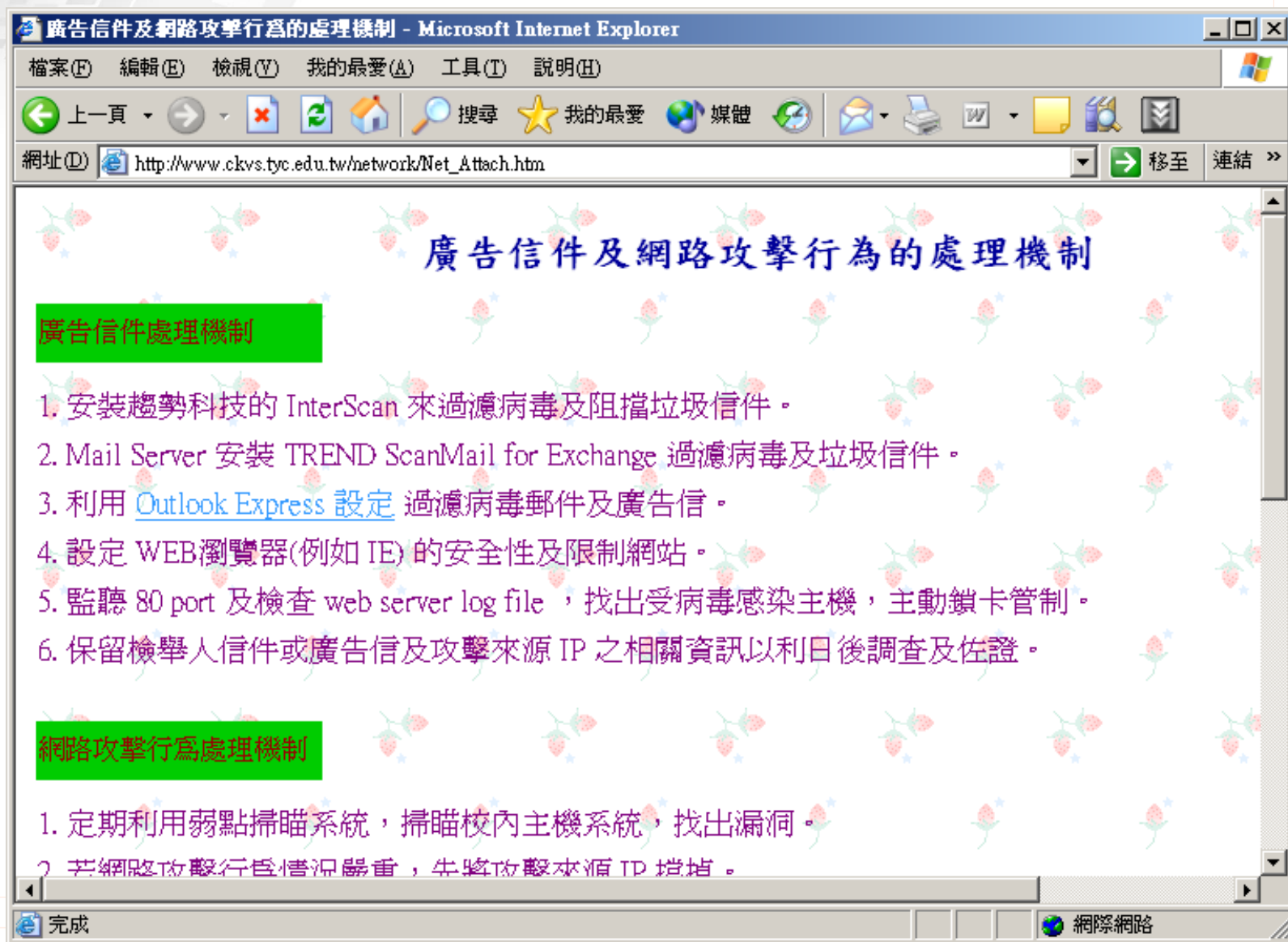
http://www.ckvs.tyc.edu.tw/network/Net_Attach.htm

安裝趨勢科技的IMSS來過濾病毒及阻擋垃圾信件。

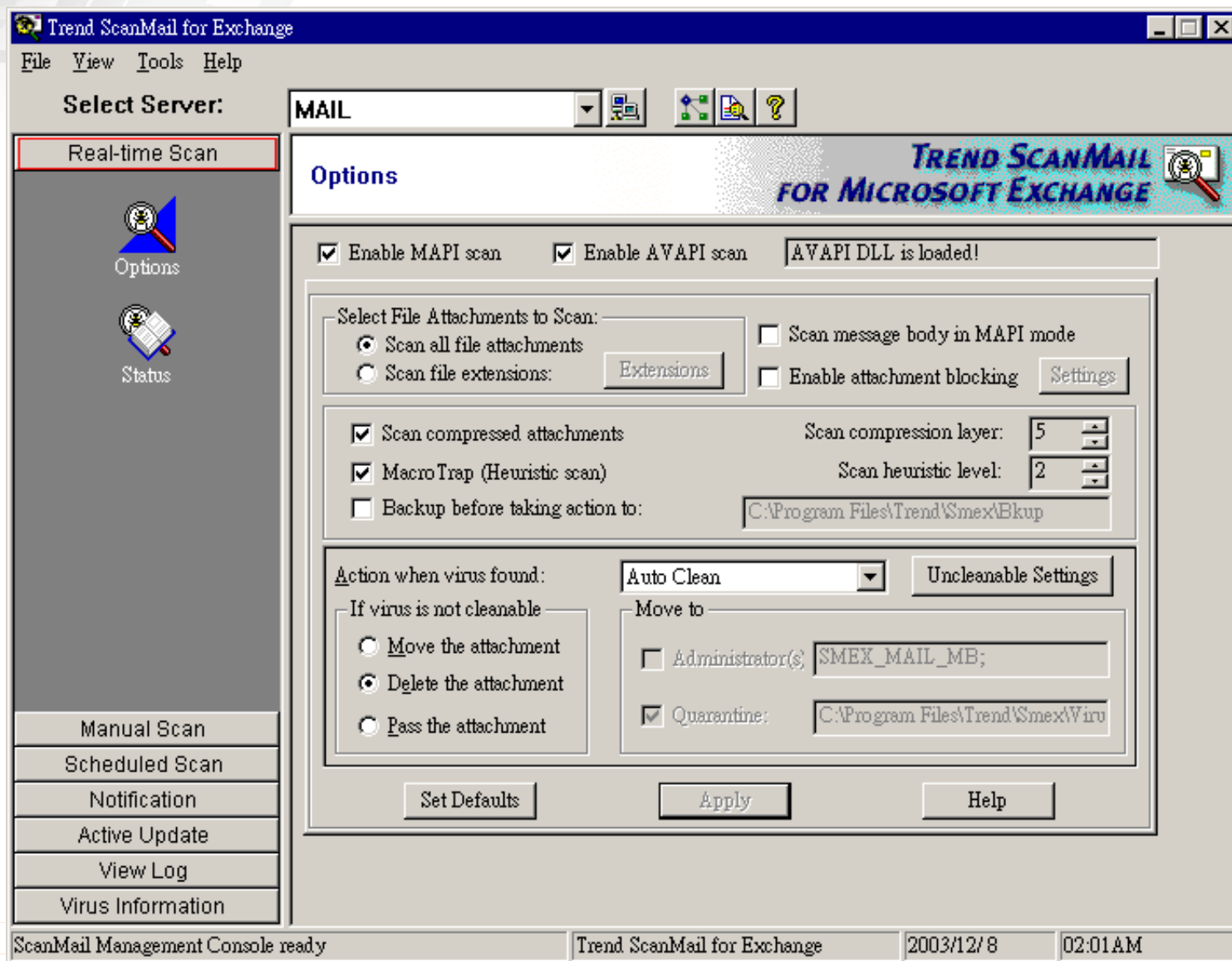
1. Mail Server安裝ScanMail for Exchange過濾病毒及垃圾信。
2. 利用 Outlook Express 設定 過濾病毒郵件及廣告信。
3. 設定 WEB瀏覽器(例如 IE) 的安全性及限制網站。
4. 監看 80 port 及檢查 web server log file ，找出受病毒感染主機，主動鎖卡管制。
5. 保留檢舉人信件或廣告信及攻擊來源 IP 之相關資訊以利日後調查及佐證。



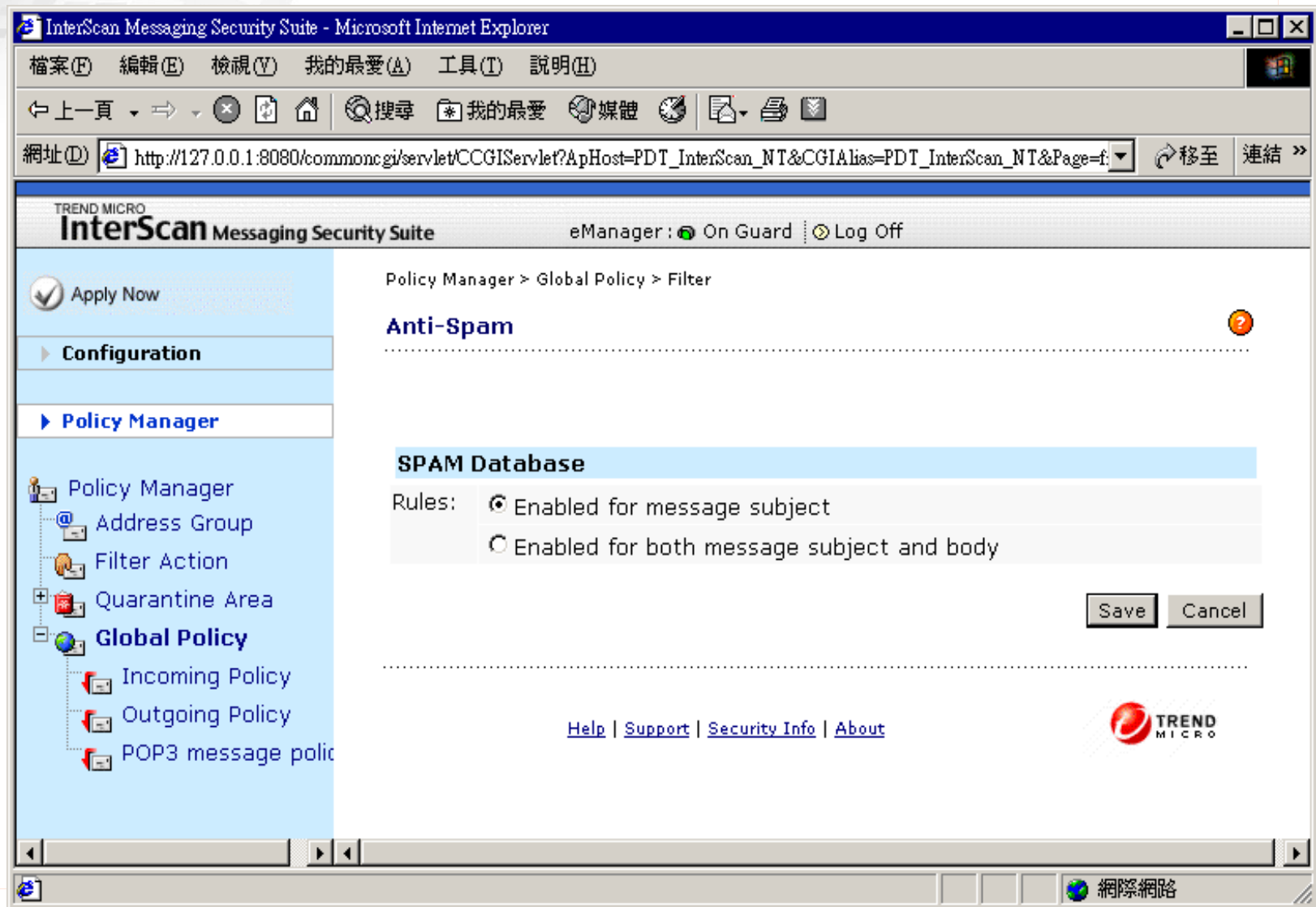
範例 (1) :



範例 (2) :



範例 (3) :



規範 (6-1) :

網路攻擊行為處理機制：

1. 定期利用弱點掃描系統，掃描校內主機系統，找出漏洞。
2. 若網路攻擊行為情況嚴重，先將攻擊來源 IP 擋掉。
3. 依照「IP 使用分配表」找到當事人並以電話連絡或以E-mail通知，請當事人說明被檢舉的情事。
4. 依照校園電腦網路使用遵守規範及獎懲辦法予以當事人適當之懲處，並停權處分以茲眾人警惕。
5. 保留檢舉人信件或廣告信及攻擊來源 IP 之相關資訊以利日後調查及佐證。



規範 (6-1)：

網路攻擊行為處理機制：

6. 定時安排透過網管工具、網路流量分析軟體及網路安全網站查詢分析網路攻擊及中毒行為，即時於路由器及防火牆設定 ACL 阻擋功能。先阻擋攻擊之 IP Address(ACL)。再做調查是否為主動或是被入侵。如果主動攻擊將送交相關單位處理，如果被入侵，等系統修復後才釋放ACL。

公告網址

http://www.ckvs.tyc.edu.tw/network/Net_Manage.htm



範例 (1) :

校園網路管理停權公告 - Microsoft Internet Explorer

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

← 上一頁 → 搜尋 ★ 我的最愛 媒體

網址(D) http://www.ckvs.tyc.edu.tw/network/Net_Manage.htm 移至 連結 >>

校園網路管理停權公告

網路停權-禁用帳號

帳號	使用者	所屬單位	IP	停權時間	停權原因
Student21	學生	電腦教室	10.1.2.21	92.08.21	擅自架設站台
Student27	學生	電腦教室	10.1.2.27	92.08.21	擅自架設站台

完成 網際網路



規範 (7) :

網路不當資訊(含犯罪與色情)過濾系統 及防制處理機制建置方式：

本校針對色情網站進行阻擋服務，其實施方式如下：

1. 目前連線至 TANet 以防止不良網站閘道器 (Web Leach) 實施管制以防止不正常網路行為。硬體式「防色e晶片」，裝置於 TANET 與校園網路出入口處成為不當資訊防治主機，透過硬體方式之過濾機制，可提升執行效率與穩定性，晶片可透過網路於每日定時自動更新不當資訊之網址資料庫(Vision Next)，管理者並可依IP、使用者、群組、阻擋類型、網域、URL、進(出)流量大小等進行查詢，列出上網網址和上網資料佔用頻寬等報表，本校所有對外80 Port 均導向不當資訊防治主機，因此能有效防治校內所有使用者對外接取不當之資訊，效果可達80%以上。



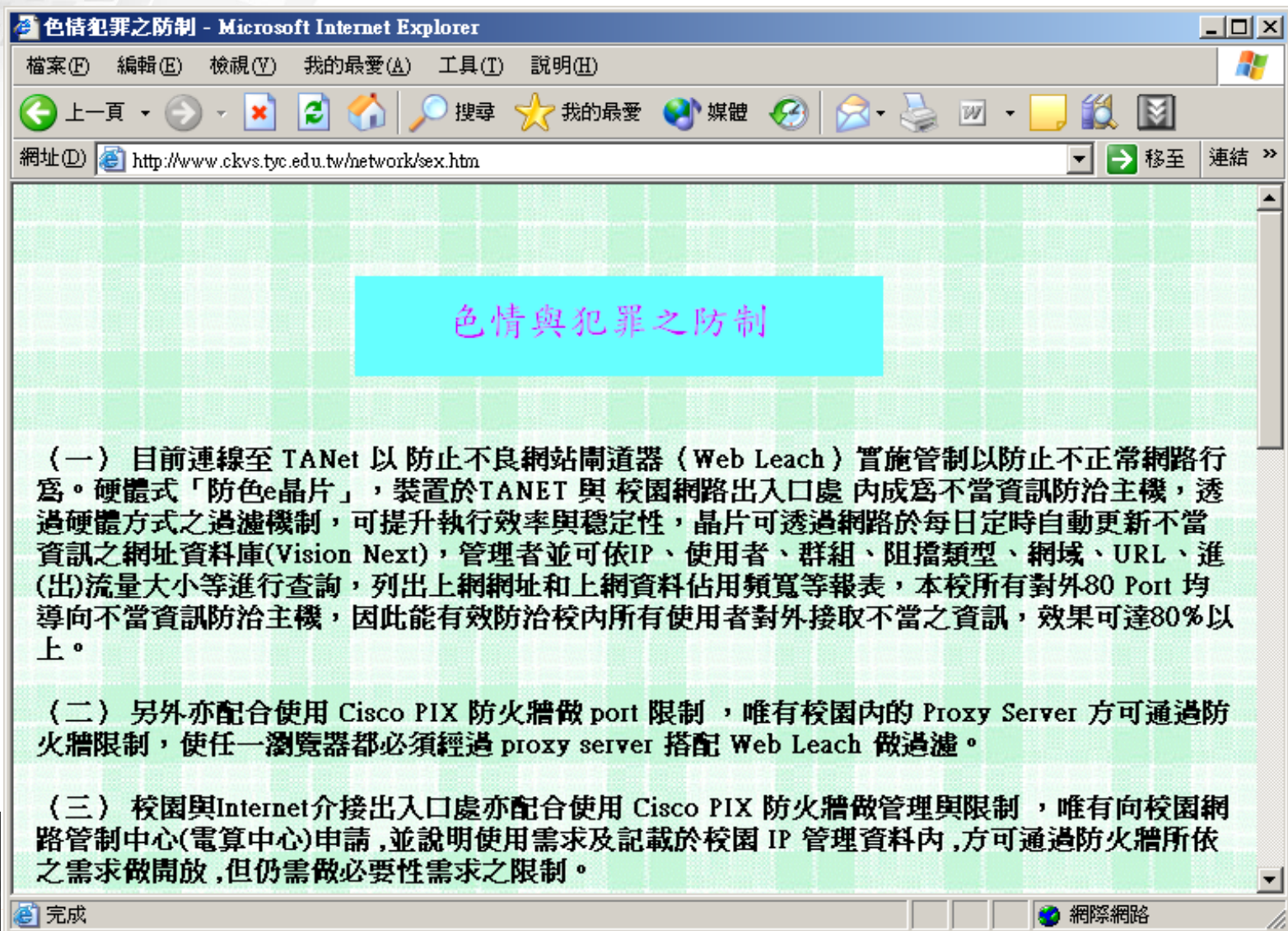
規範 (7) :

網路不當資訊(含犯罪與色情)過濾系統 及防制處理機制建置方式 :

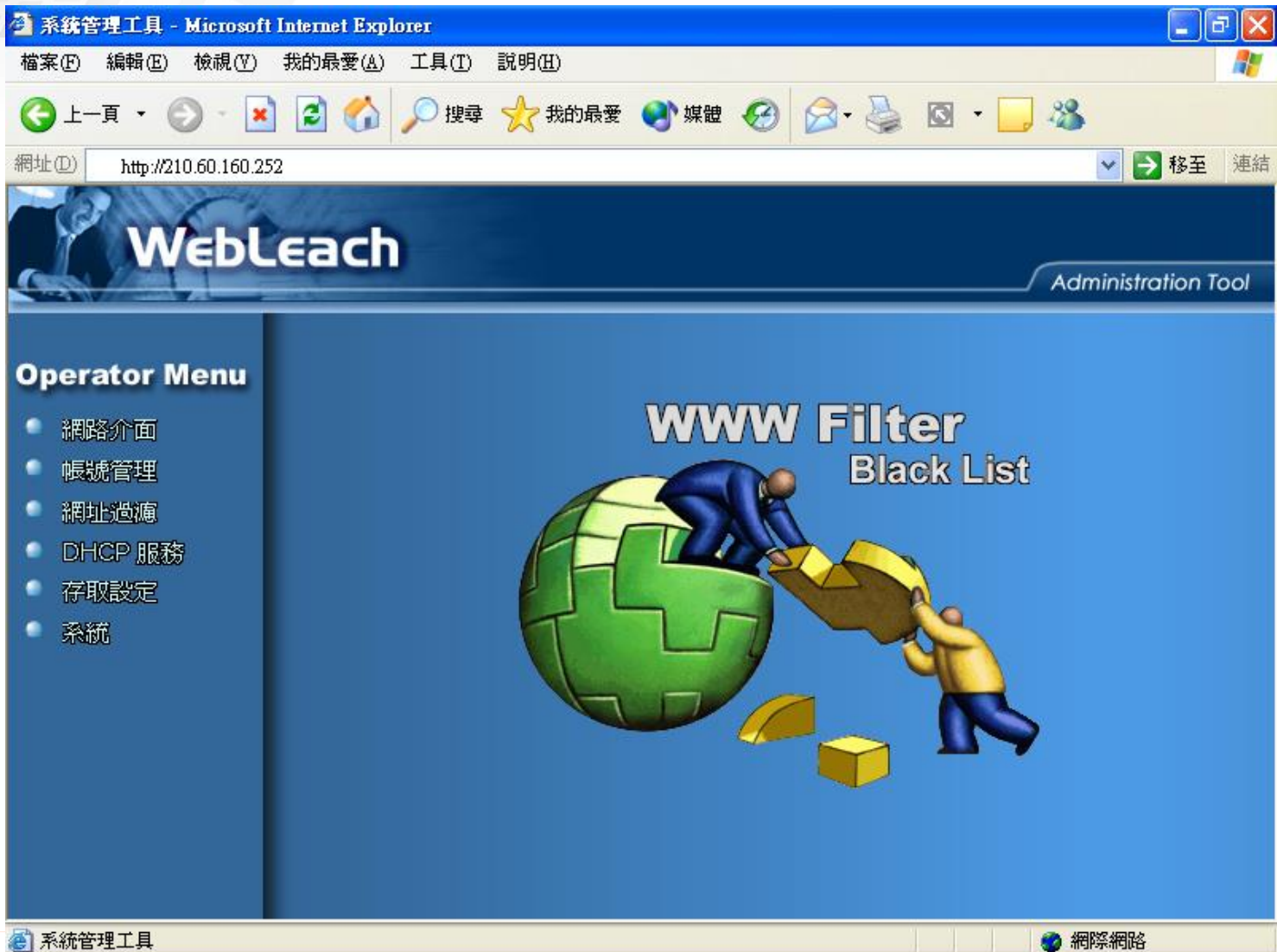
2. 另外亦配合使用 Cisco PIX 防火牆做 port 限制，唯有校園內的 Proxy Server 方可通過防火牆限制，使任一瀏覽器都必須經過 proxy server 搭配 Web Leach 做過濾。
3. 校園與Internet介接出入口處亦配合使用 Cisco PIX 防火牆做管理與限制，唯有向校園網路管制中心(電算中心)申請，並說明使用需求及記載於校園 IP 管理資料內，方可通過防火牆依所需求做開放，但仍需做必要性需求之限制。



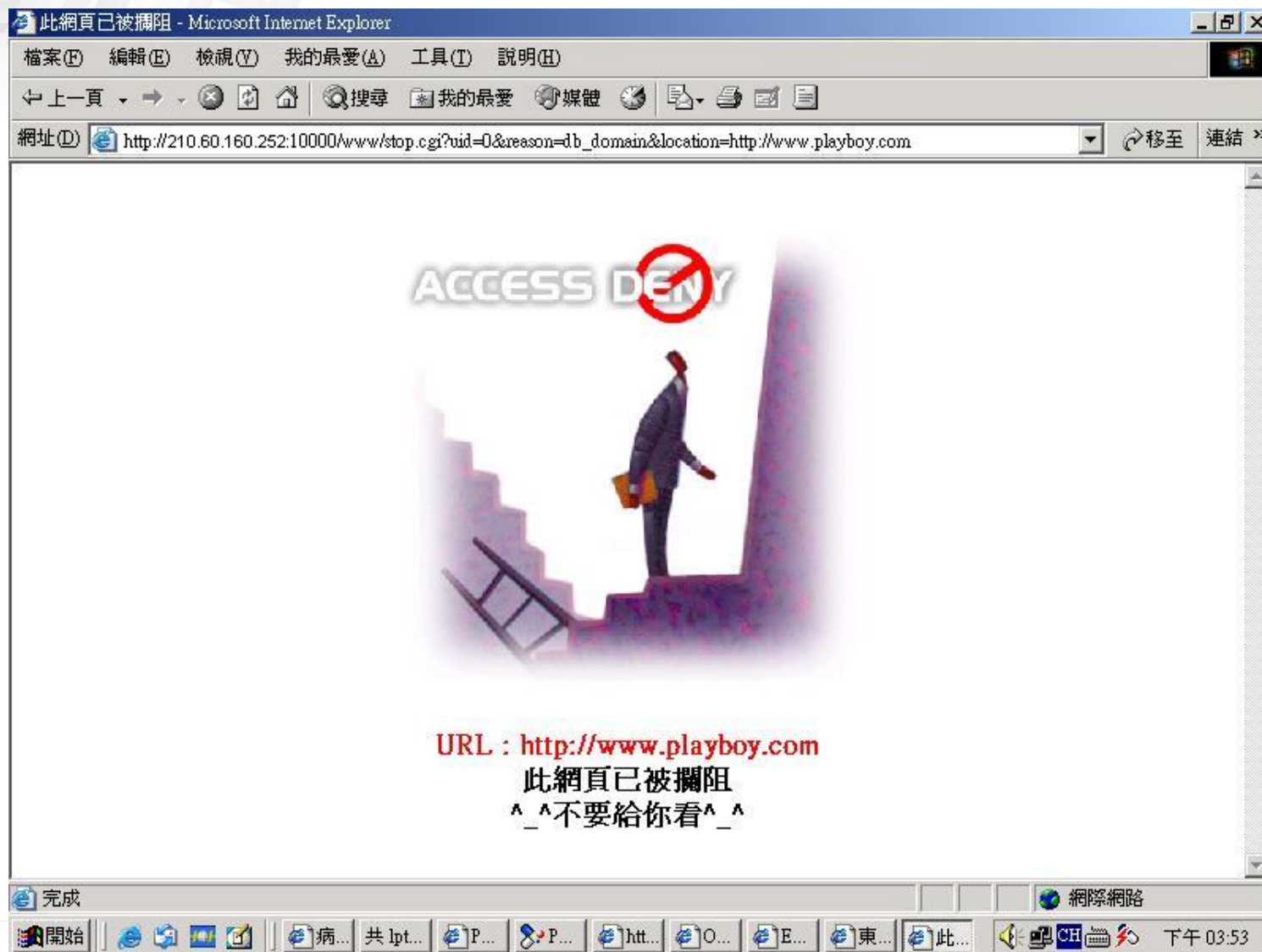
範例 (1) :



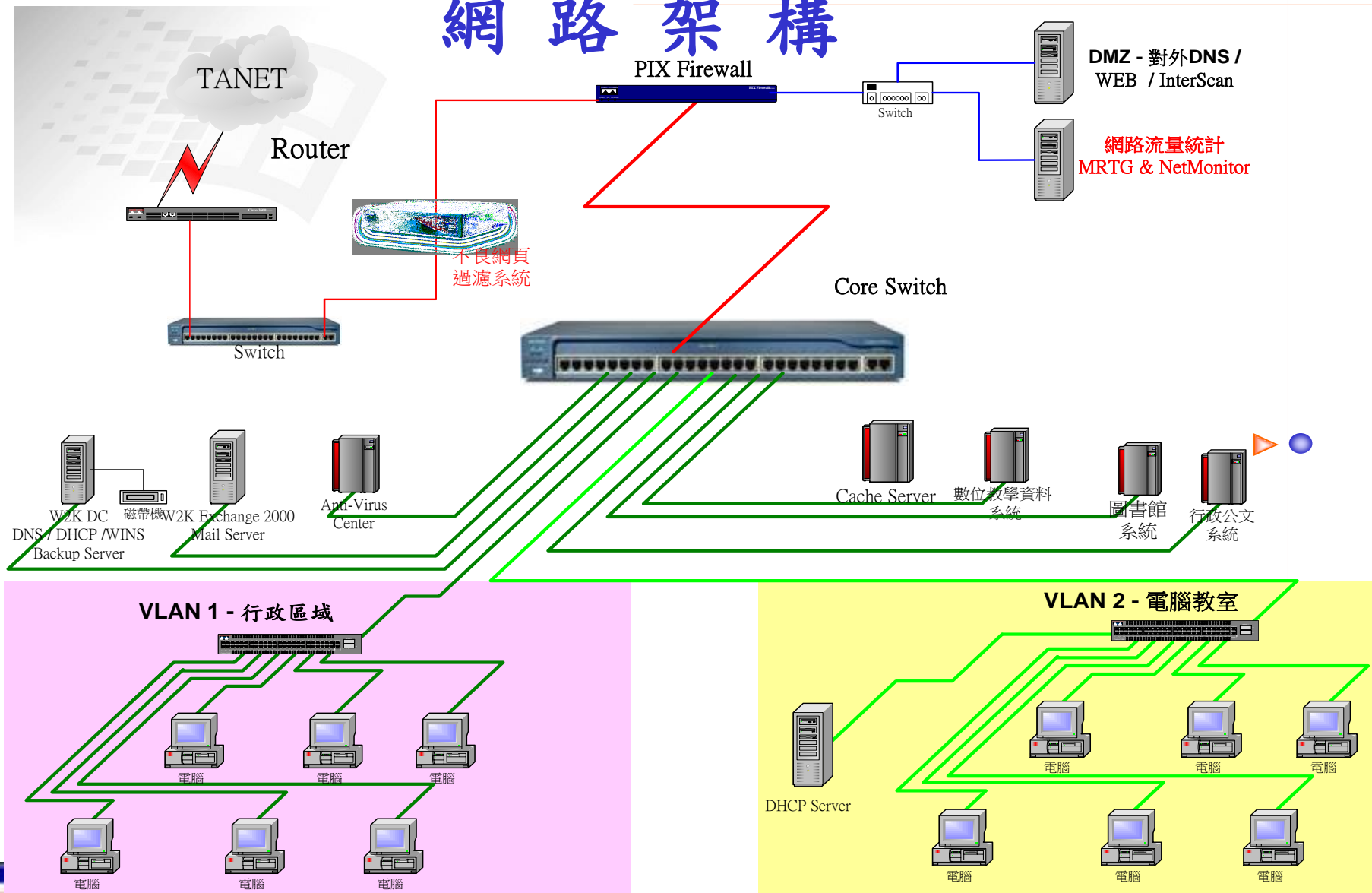
範例 (2) :



範例 (3) :



網路架構





發展目標

- 無線化校園學習環境的建立
- 整體化網路監控及管理系統的建立，針對網路安全及防範網路濫用規劃相關使用規範並安裝監控設備。





Thank You !

