精誠中學申請介接 TANet 新世代骨幹網路

連線計劃書

壹、前言

精誠中學依校園發展規劃藍圖，將於本學年度開始著手建置網路教學平台，因此欲提升目前之網路頻寬，擬申請新世代骨幹網路介接。精誠中學網路頻寬申請依據教育網路 TANet 中區網路管理中心—中興大學審核辦法提出申請，並說明未來學校提昇頻寬所辦理事宜。

目前精誠中學網路 TANet 連外頻寬使用二路 ADSL 頻寬合計為 1 M bps，計劃申請高速乙太線路連線頻寬為 20 M bps，以下為本校針對申請辦法八大項提出說明。

貳、連線申請說明

一、訂定校園網路使用規範

本校於 93 年 11 月 2 日行政會議審議修正通過「校園網路委員會組織章程」、「校園網路使用規範」、「對違反校園網路使用之學生懲處」。相關規範全文如下：

■ 校園網路委員會組織章程

一、目的:為確實執行教育部「校園網路使用規範」，充分發揮校園網路功能，普及尊重法治觀念，特設置「校園網路委員會」(以下簡稱本會)。

二、依據: 教育部台（90）電字第 90187600 號函訂頒之教育部「校園網路使用規範」。

三、委員之聘任:本會之委員由校長於每學年開始，聘請各處室主任、學科召集人、學科與資訊教師代表若干人組成之，委員任期為一學年。

四、權責與分工：

(一)校長為主任委員，負責召集並主持會議。

(二)本會設執行秘書一人，由教務主任兼任，秉承主任委員指示，執行本會之決議，推動各項業務及工作。

(三)本校校園網路執行管理單位（簡稱網管單位）為資訊組，其權責及管理事項明訂於本校「校園網路使用規範」。

五、工作項目：

(一)處理校園網路相關法律問題。

(二)採取適當措施以維護校園網路安全,

(三)研訂與校園網路使用規範有關之校規。

(四)宣導校園網路使用規範，引導師生正確使用網路資源，遵守網路相關法令規定及禮節。

(五)其他與網路有關之事項。

六、本會每學年開會一至二次，必要時得召開臨時會議。

七、本會研議專案，如有需要得邀請有關單位或個人提供諮商與指導。

八、本章程經行政會報通過後，陳請校長公佈實施，修正時亦同。

校園網路使用規範

一、目的：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。

二、依據：教育部台（90）電字第 90187600 號函訂頒之教育部「校園網路使用規範」。

三、權責與分工

(一) 設置「校園網路委員會」(組織章程另訂)，辦理下列事項：

1. 處理網路相關法律問題。
2. 採取適當措施以維護網路安全
3. 研訂與網路使用規範有關之校規。
4. 宣導網路使用規範，引導師生正確使用網路資源，遵守網路相關法令規定及禮節。
5. 其他與網路有關之事項。

(二) 本校執行網路管理單位（以下簡稱網管單位）為圖書館資訊媒體組，辦理下列事項：

1. 設置專人管理、維護校內各網站及 BBS 站。
2. 建立網路使用者自律機制，對網路流量應為適當之區隔與管控。
3. 對於違反本規範或影響網路正常運作者，得刪除其文章或停止該使用者使用之權利，其情節重大違反校規或法令者，應即轉請學校處置。
4. 其他有關網路管理之事項。

(三) 使用者若發現網路系統安全有任何缺陷，應儘速通報網管單位。

四、規範對象:本規範所稱網路使用者，係指全體教職員工生以及使用本校網路資源之校外人士。

五、規範事項

(一)尊重智慧財產權：網路使用者應避免下列可能涉及侵害智慧財產權之行為

1. 使用未經授權之電腦程式。
2. 違法下載、拷貝受著作權法保護之著作。
3. 未經著作權人之同意，將受著作權法保護之著作上傳於公開之網站上。

4. BBS 或其他線上討論區上之文章，經作者明示禁止轉載，而仍任意轉載。
5. 架設網站供公眾違法下載受著作權法保護之著作。
6. 其他可能涉及侵害智慧財產權之行為。

(二)禁止濫用網路系統：網路使用者不得有下列之行為

1. 散佈電腦病毒或其他干擾或破壞系統機能之程式。
2. 擅自截取網路傳輸訊息。
3. 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。
4. 相互轉借帳號、隱藏或使用虛假帳號，但經明確授權得匿名使用者不在此限。
5. 窺伺他人之電子郵件或檔案。
6. 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。
7. 以電子郵件、線上留言、線上討論、電子佈告欄（BBS）或類似功能之方法，從事非法軟體交易，或傳送不實資訊，或發表人身攻擊、詐欺、誹謗、侮辱、猥褻、騷擾之言論。
8. 利用學校之網路資源從事非教學研究等相關之活動或違法行為。

(三)隱私權之保護：網管單位應尊重網路隱私權，不得任意窺伺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。

1. 為維護或檢查系統安全。
2. 依合理之根據，懷疑有違反網路使用規範之情事時，為取得證據或調查不當行為。
3. 為配合司法機關之調查。
4. 其他依法令之行為。

六、違反之效果

違反本規範之網路使用者，將受到下列之處分：

(一)停止使用網路資源，刪除已發表之文章或資料。

(二)學生違規情節重大者，由網管單位移送校規處置。

(三)教職員工違規情節重大者，由網管單位陳請校長處理。

(四)網管人員違規者，應加重其處分。

(五)依上列各項規定之處分者，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。

七、處理原則及程序

(一)對學生違反本規範之處分，另行明訂於校規中。

(二)違反本規範之行為人對所受之處分，應依正當法律程序提出申訴和救濟。

(三)前列校規及網管單位所採取之各項處分與管制措施應符合必要原則、比例原則及法律保留原則。

(四)本校處理相關網路申訴或救濟程序之權責單位，應徵詢校園網路委員會或指定專人之意見。

八、本章程經行政會報通過後，陳請校長公佈實施，修正時亦同。

■ 對違反校園網路使用之學生懲處

網路規範獎懲實施要點

一、合於左列規定情事之一者，記警告：

（一）、使用校園網路違犯下列侵害智慧財產權或濫用網路系統之行為者：

1 使用未經授權之電腦程式。

2 違法下載、拷貝受著作權法保護之著作。

3 未經著作權人之同意，將受著作權法保護之著作上傳於公開之網站上。

4 ＢＢＳ或其他線上討論區上文章，經作者明示禁止轉載，而仍任意轉載。

5 擅自截取網路傳輸訊息。

6 窺伺他人之電子郵件或檔案。

7 以破解、盜用或冒用他人帳號及密碼或使用虛假帳號等方式，未經授權使用網路資源者，但經明確授權得匿名使用者不在此限。

8 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。

上列各項規定之處分如情節重大者，得改記小過一次，其另有違法行為時，尚應依民法、刑法、著作權法或他相關法令負法律責任。

二、合於左列規定情事之一者，記小過：

（一）、學生使用校園網路，發生下列情形之一者：

1 架設網站供公眾違法下載受著作權法保護之著作。

2 散佈電腦病毒或其他干擾或破壞系統機能之程式。

3 以電子郵件、線上留言、線上討論、電子佈告欄（ＢＢＳ）或類似功能之方法，從事非法軟體交易，或傳送不實資訊，或發表人身攻擊、詐欺、誹謗、侮辱、猥褻、騷擾之言論。

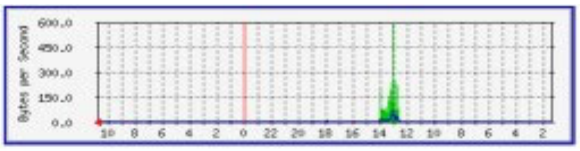
4 利用學校之網路資源從事違法之活動或行為。

上列各項規定之處分如情節重大者，得改記大過一次，其另有違法行為時，尚應依民法、刑法、著作權法或他相關法令負法律責任。

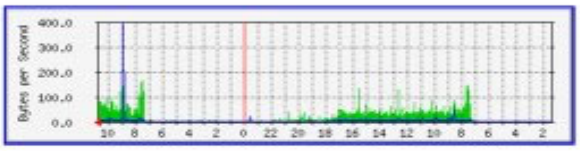
二、流量統計圖（學校電算中心管轄主要 Router 及 Switch 的 MRTG 流量圖 MRTG）

本校流量統計之 MRTG 網址為：https://163.23.124.23:10000/mrtg/，主要分析校內網路主設備 core switch 之流量，含全校行政端、學生端、電腦教室、教師辦公室所有校園網路。

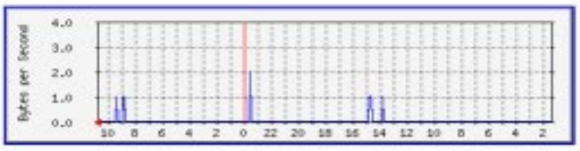
Description: Vlan60
ifType: propVirtual (53)
ifName: Vl60
Max Speed: 125.0 MBytes/s
Ipc 192.168.60.254 ()



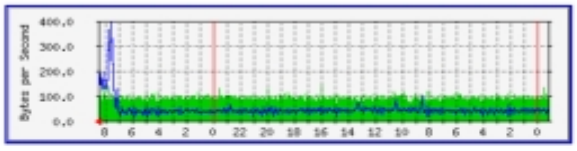
Description: Vlan65
ifType: propVirtual (53)
ifName: Vl65
Max Speed: 125.0 MBytes/s
Ipc 163.23.124.158 ()



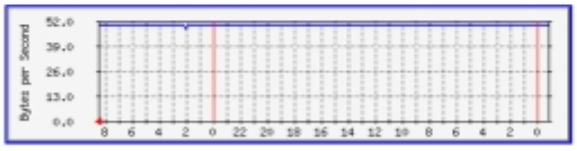
Description: Vlan70
ifType: propVirtual (53)
ifName: Vl70
Max Speed: 125.0 MBytes/s
Ipc 192.168.70.254 ()



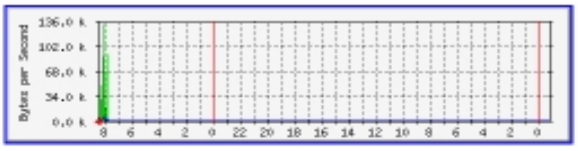
Description: Vlan99
ifType: propVirtual (53)
ifName: Vl99
Max Speed: 125.0 MBytes/s
Ip: 163.23.124.30 ()



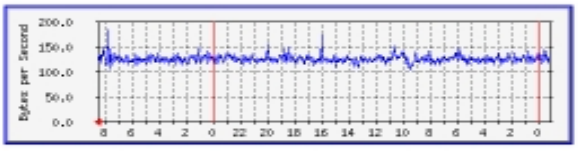
Description: GigabitEthernet1/0/1
ifType: ethernetCsmacd (6)
ifName: Gi1/0/1
Max Speed: 12.5 MBytes/s



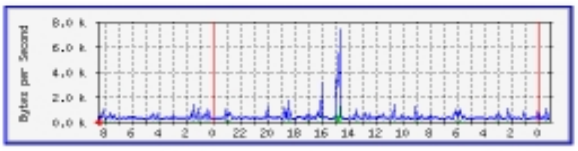
Description: GigabitEthernet1/0/5
ifType: ethernetCsmacd (6)
ifName: Gi1/0/5
Max Speed: 125.0 MBytes/s



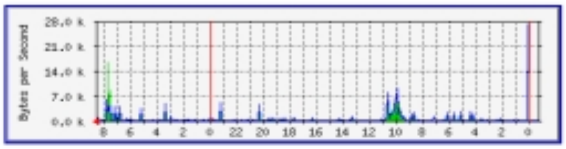
Description: GigabitEthernet1/0/6
ifType: ethernetCsmacd (6)
ifName: Gi1/0/6
Max Speed: 12.5 MBytes/s



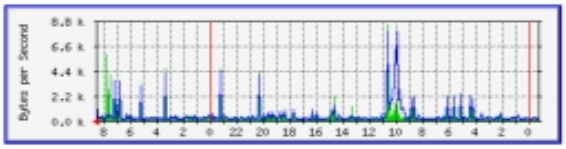
Description: GigabitEthernet1/0/7
ifType: ethernetCsmacd (6)
ifName: Gi1/0/7
Max Speed: 12.5 MBytes/s



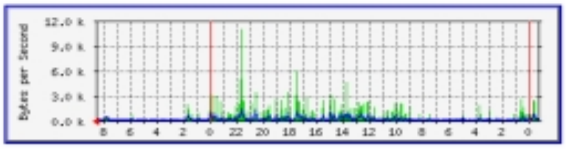
Description: GigabitEthernet1/0/10
ifType: ethernetCsmacd (6)
ifName: Gi1/0/10
Max Speed: 12.5 MBytes/s



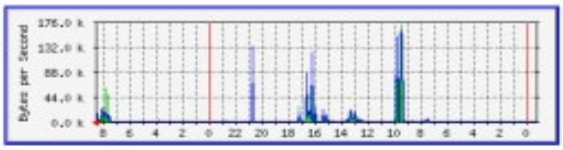
Description: GigabitEthernet1/0/11
ifType: ethernetCsmacd (6)
ifName: Gi1/0/11
Max Speed: 125.0 MBytes/s



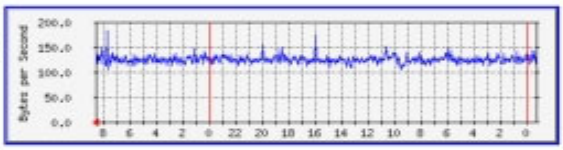
Description: GigabitEthernet1/0/12
ifType: ethernetCsmacd (6)
ifName: Gi1/0/12
Max Speed: 12.5 MBytes/s



Description: GigabitEthernet1/0/13
ifType: ethernetCsmacd (6)
ifName: Gi1/0/13
Max Speed: 12.5 MBytes/s

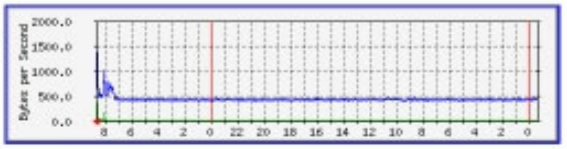


Description: GigabitEthernet1/0/14
ifType: ethernetCsmacd (6)
ifName: Gi1/0/14
Max Speed: 12.5 MBytes/s

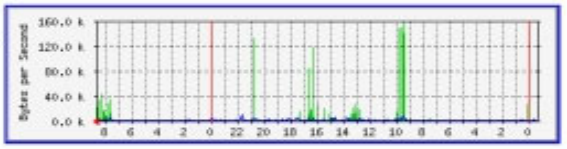


Max Speed: 12.5 MBytes/s
Max Speed: 12.5 MBytes/s
Max Speed: 12.5 MBytes/s
Max Speed: 12.5 MBytes/s
Max Speed: 12.5 MBytes/s
Max Speed: 12.5 MBytes/s

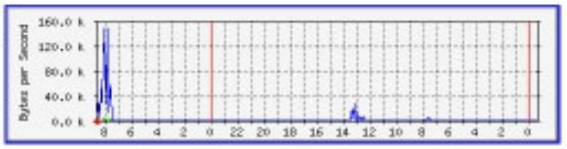
Description: GigabitEthernet1/0/23
ifType: ethernetCsmacd (6)
ifName: Gi1/0/23
Max Speed: 12.5 MBytes/s



Description: GigabitEthernet1/0/24
ifType: ethernetCsmacd (6)
ifName: Gi1/0/24
Max Speed: 12.5 MBytes/s



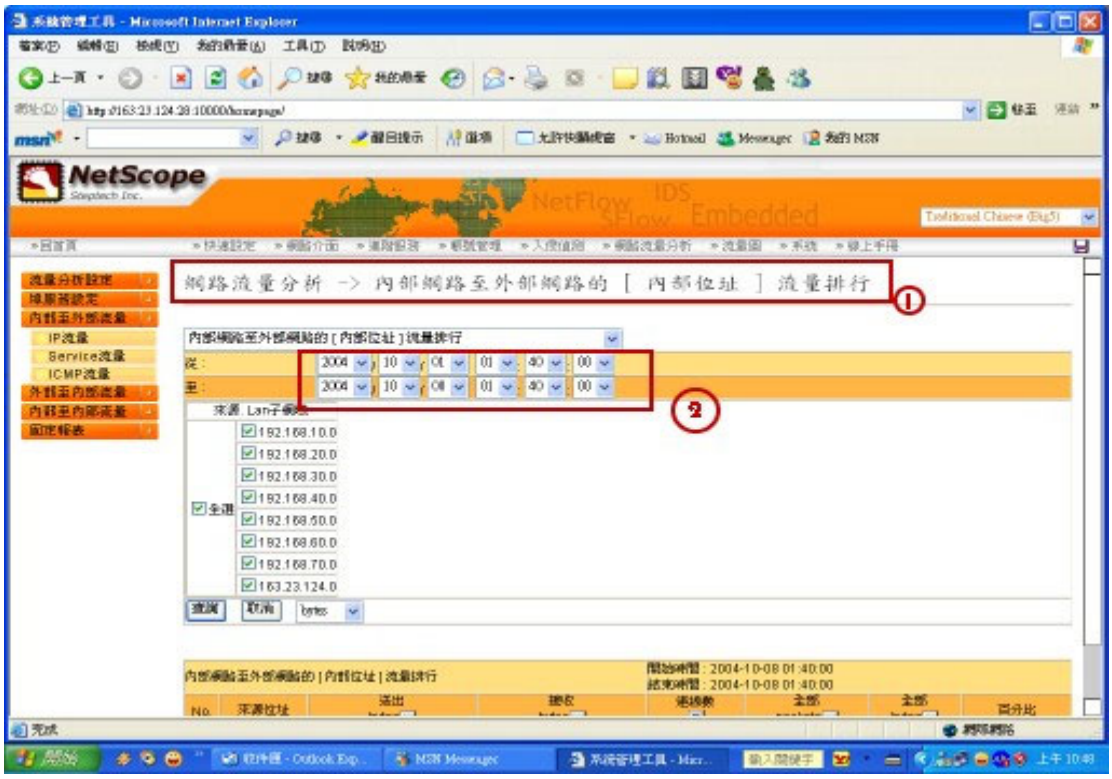
Description: GigabitEthernet1/0/25
ifType: ethernetCsmacd (6)
ifName: Gi1/0/25
Max Speed: 125.0 MBytes/s

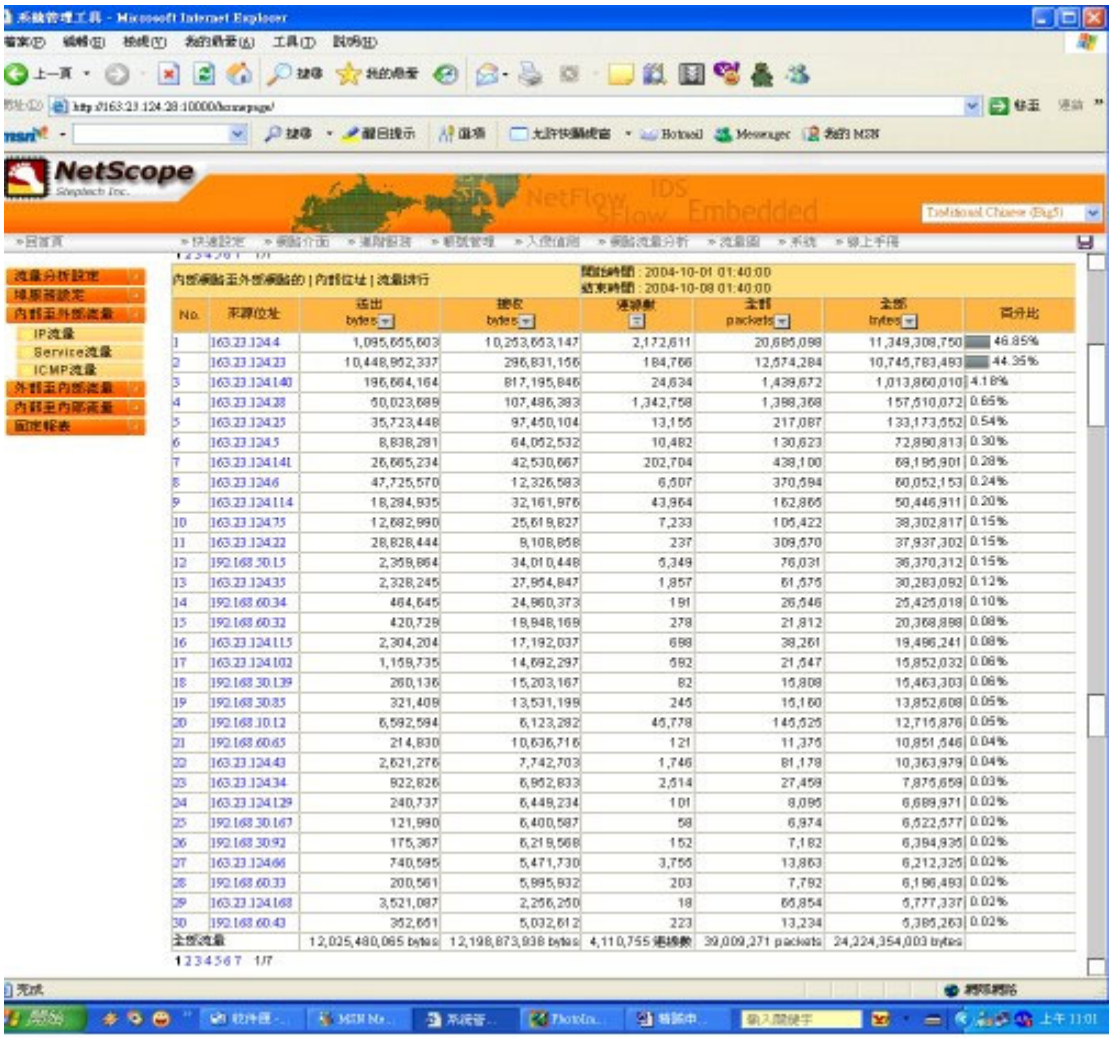


三、 前三十名 IP Address 使用量（學校對 TANet 流量 In/Out 排名）

網頁網址：http://163.23.124.28:10000/

Top IP 30 之分析可分為：內部對外部、外部對內部、內部對內部之分析再分別根據 IP、SERVICE 等流量分析，定義分析日期間距後可得報表，IP 分析完若覺得某 IP 流量有問量可再深入探究該 IP 連接的 IP 為何及所使用的服務為何。





系統管理工具 - Microsoft Internet Explorer

NetScope
Simplestech Inc.

流量分析設定
排除器設定
內部至外部流量
IP流量
Service流量
ICMP流量
外部至內部流量
內部至內部流量
固定報表

內部網路至外部網路的 | 內部位址 | 流量排行

開始時間 : 2004-10-01 01:40:00
結束時間 : 2004-10-08 01:40:00

No.	來源位址	送出 bytes	接收 bytes	連線數	全部 packets	全部 bytes	百分比
1	163.23.124.4	1,095,655,603	10,253,653,147	2,172,611	20,685,098	11,349,308,750	46.85%
2	163.23.124.23	10,448,952,337	296,831,156	184,766	12,574,284	10,745,783,493	44.35%
3	163.23.124.140	196,664,164	817,195,846	24,634	1,439,672	1,013,860,010	4.18%
4	163.23.124.28	60,023,689	107,486,383	1,342,758	1,398,368	157,510,072	0.65%
5	163.23.124.25	35,723,448	97,450,104	13,156	217,087	133,173,552	0.54%
6	163.23.124.5	8,838,281	64,052,532	10,482	130,623	72,890,813	0.30%
7	163.23.124.141	26,665,234	42,530,667	202,704	438,100	69,195,901	0.28%
8	163.23.124.6	47,725,570	12,326,583	6,507	370,594	60,052,153	0.24%
9	163.23.124.114	18,284,935	32,161,976	43,964	162,865	50,446,911	0.20%
10	163.23.124.75	12,682,990	25,619,827	7,233	105,422	38,302,817	0.15%
11	163.23.124.22	28,828,444	9,108,858	237	309,570	37,937,302	0.15%
12	192.168.30.15	2,358,864	34,010,448	5,349	76,031	36,370,312	0.15%
13	163.23.124.35	2,328,245	27,954,847	1,857	61,575	30,283,092	0.12%
14	192.168.60.34	464,645	24,960,373	191	26,546	25,425,018	0.10%
15	192.168.60.32	420,728	19,948,169	278	21,812	20,368,898	0.08%
16	163.23.124.115	2,304,204	17,192,037	698	38,261	19,496,241	0.08%
17	163.23.124.102	1,159,735	14,692,297	592	21,547	15,852,032	0.06%
18	192.168.30.139	260,136	15,203,167	82	16,808	15,463,303	0.06%
19	192.168.30.85	321,409	13,531,199	245	16,160	13,852,608	0.05%
20	192.168.10.12	6,592,594	6,123,282	46,778	146,525	12,716,876	0.05%
21	192.168.60.65	214,830	10,636,716	121	11,375	10,851,546	0.04%
22	163.23.124.43	2,621,276	7,742,703	1,746	81,178	10,363,979	0.04%
23	163.23.124.34	922,826	6,952,833	2,514	27,459	7,875,659	0.03%
24	163.23.124.129	240,737	6,448,234	101	8,095	6,689,971	0.02%
25	192.168.30.167	121,990	6,400,587	58	6,974	6,522,577	0.02%
26	192.168.30.92	175,367	6,218,568	152	7,182	6,394,935	0.02%
27	163.23.124.66	740,595	5,471,730	3,755	13,863	6,212,325	0.02%
28	192.168.60.33	200,561	5,995,932	203	7,792	6,196,493	0.02%
29	163.23.124.168	3,521,087	2,256,250	18	66,854	5,777,337	0.02%
30	192.168.60.43	352,651	5,032,612	223	13,234	5,385,263	0.02%
全部流量		12,025,480,065 bytes	12,198,873,938 bytes	4,110,755 連線數	39,009,271 packets	24,224,354,003 bytes	

1 2 3 4 5 6 7 1/7

完成


NetScope
Simptech Inc.
流量分析設定
掃描器設定
內對至外部流量
IP流量
Service流量
ICMP流量
外對至內部流量
內部至內部流量
Top Send
Top Send
Top Recieve
Top Recieve
Top Session
Top Session
Top Total packets
Top Total packets
Top Total bytes
Top Total bytes

四、E-mail 帳號（Abuse、security）

1. 本校已建立 abuse@mail.cchs.chc.edu.tw 及 security@mail.cchs.chc.edu.tw 兩個 e-mail 帳號。這兩個帳號郵件由專人負責處理，並將轉寄至資訊組邱慧玲組長信箱 iris@mail.cchs.chc.edu.tw。
2. 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。

五、IP 使用及異動作登記管理

1. 若有發現違法使用 IP 情形，將依校園網路使用規範處理
2. IP 分配依處室及教室於校園中之實際位置加以分割及配置
3. 全校 IP 之使用及管理由網管中心統籌分配管理
4. 各單位 IP 使用分配明細如下

行政單位及教師辦公室 163.23.*.*			
處室別	分配 IP 範圍	管理人	備註
資訊中心	隱藏	邱慧玲	
教務處	隱藏	陳英杰	
校長、人事、總務	隱藏	林明慧	
學務、自然科、英文科、數學科	隱藏	黃朝義	
輔導室、國文科	隱藏	邱慧玲	
未使用	隱藏	邱慧玲	
未使用	隱藏	邱慧玲	
未使用	隱藏	邱慧玲	

班級電腦及電腦教室-學生用			
地點	分配 IP 範圍	管理人	備註
電腦教室 201	192.168.10.*	邱慧玲	VLan10

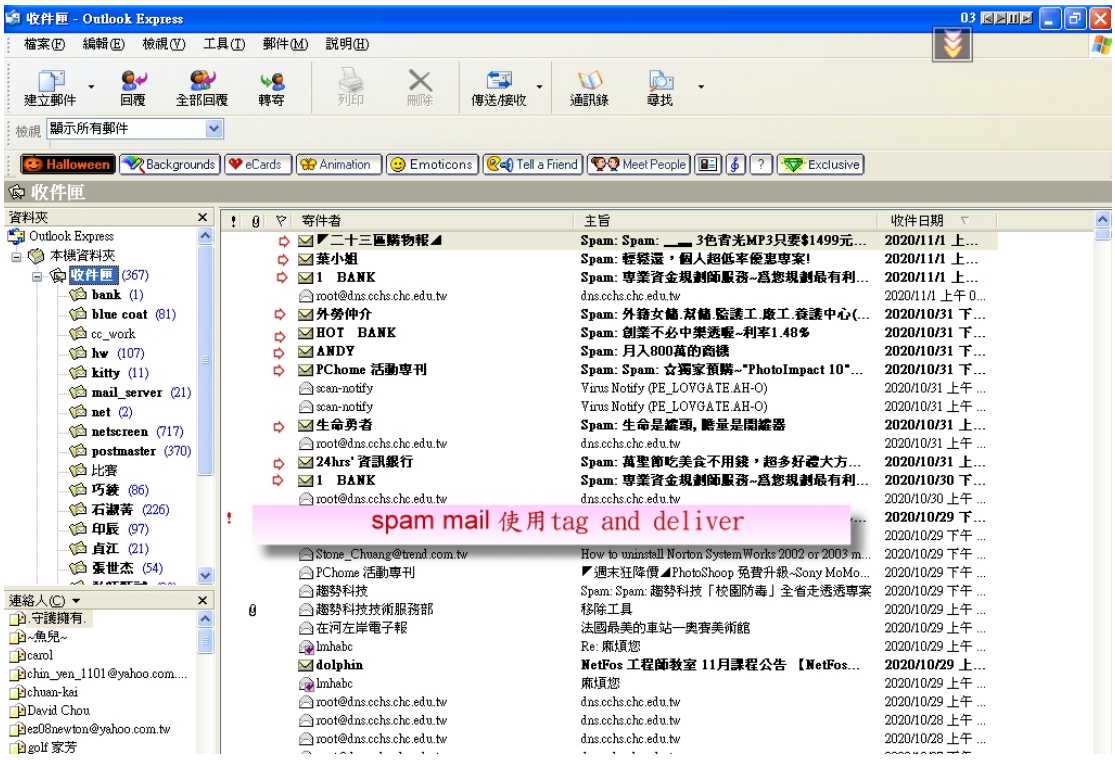
電腦教室 202	192.168.60.*	邱慧玲	VLan60
電腦教室 301	192.168.20.*	陳英杰	VLan20
電腦教室 302	192.168.30.*	陳英杰	VLan30
班級電腦前	192.168.50.*	邱鴻毅	VLan50
班級電腦後	192.168.40.*	邱鴻毅	VLan40

資訊中心伺服器			
服務別	分配 IP	網域名稱	備註
DNS、Mail	隱藏	dns.cchs.chc.edu.tw	
WWW	隱藏	www.cchs.chc.edu.tw	
防毒	隱藏	sps.cchs.chc.edu.tw	
行政電腦化系統	隱藏		
防火牆	隱藏		
快取伺服器	隱藏	Netscope.cchs.chc.edu.tw	
網管報表	隱藏		
core	隱藏		
圖書館系統	隱藏	library.cchs.chc.edu.tw	

六、廣告信件或網路攻擊行爲的反應處理機制，並建立處理現況及公告之網頁

廣告信件處理

1. 廣告信件的處理採用趨勢科技的 Spam Prevention Solution，可以將垃圾郵件阻絕於閘道端之外的解決方案。
2. 採用智慧型啟發式技術，根據郵件的多項特徵來評量、辨識和監測現有與新型的垃圾郵件，達到精確的垃圾郵件捕捉率。
3. Spam Prevention Solution 可與防毒和內容安全解決方案整合，所以可有效防制混合型的垃圾郵件威脅，降低系統負擔及生產力的損失。
4. 對於可疑的郵件，網管人員可以設定「標記後傳送」(tag and deliver) ，或是送到預先指定的管理者信箱，或可以設定為直接刪除。



5. 本校教職員生發送廣告信件，經檢舉調查屬實後，停用帳號一個月。情節嚴重者依據校園網路使用規範處理。
6. 建立 abuse 電子郵件帳號，可供使用者檢舉廣告信件。
7. 於 mail server 亦利用貝式分析法進行二次 spam 偵測。

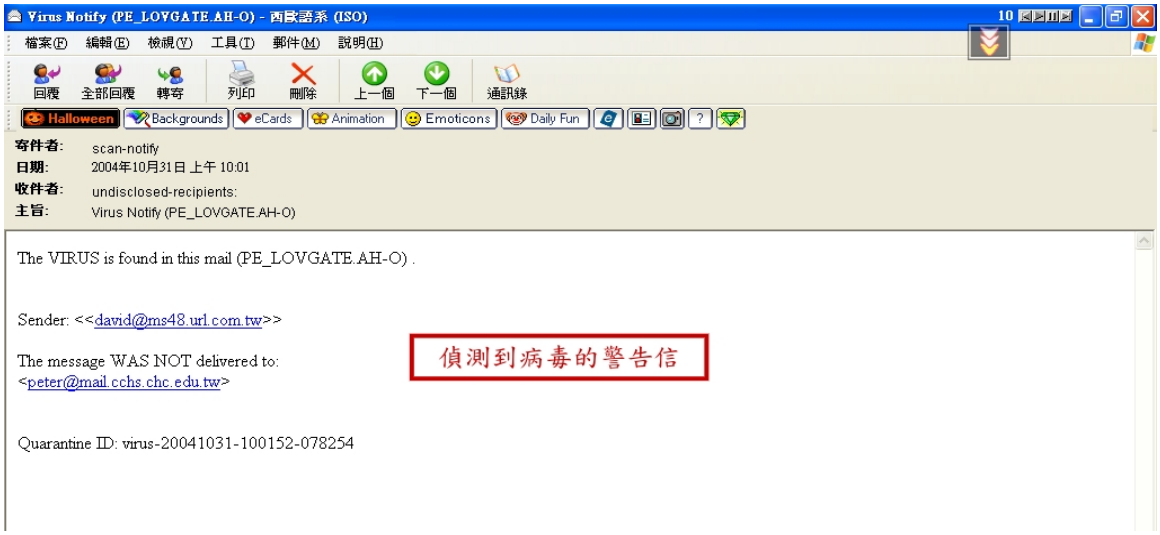
網路攻擊行為處理

1. 在防火牆上僅開放數台提供特定服務之主機提供特定服務， 其他則完全關閉外部電腦對其他校內電腦的存取動作
2. 透過流量監控晶片搭配 cisco router 及 firewall ，主動針對網路攻擊向網管人員提出網頁及郵件警示，並即時阻斷惡意連線。
3. 若發現 IP 有不正常之行為，於防火牆先阻擋攻擊之 IP (存取控制列表 ACL)。透過攻擊事件所產生的紀錄檔(Log File)，調查是否為主動或是被入侵。如果主動攻擊並涉及違法則依循相關通報管道及辦法處理，如果被入侵，等系統修復後才釋放 ACL(存取控制列表)。
4. 隨時查閱區網中心的 Spam mail 及資通安全事件之網頁（http://www.nchu.edu.tw/trnc/spam/），若發現有事件發源自本校，即刻予以處理。
5. 隨時查閱台灣電腦網路危機處理中心（http://www.cert.org.tw/cindex.htm）查閱新發現的系統漏洞，並修正之

其他網路病毒的處理機制

1. 本校所有信件，將會先寄至 Trend Interscan VirusWall 掃毒主機掃毒後，再轉

寄給收件者，以確保收件者收到的或寄出去的 E-Mail 是無病毒的。InterScan VirusWall 隨時有完整的活動紀錄檔，詳細記載每一隻攔截到的病毒以及每一件可疑的入侵事件：包括檔案來源、名稱、收件人、收到日期、病毒名稱、以及所採取的處理行動。讓管理者很容易找出問題的來源，採取適當的反應。



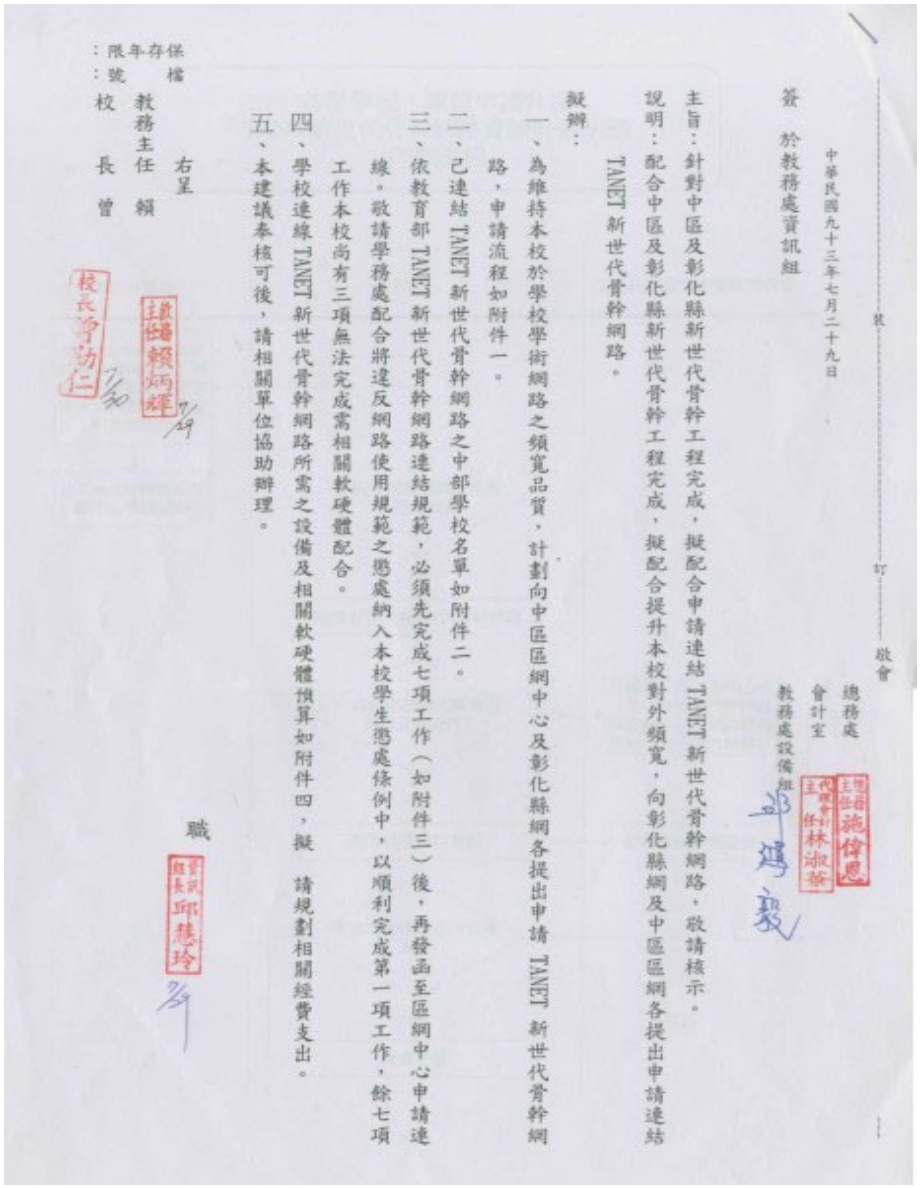
2. 架有 OfficeScan 企業版整合多種核心的安全技術，透過主從式的管理架構，提供用戶端電腦所需要的完整防護。管理者可以利用 OfficeScan 的 web 管理介面，進行網路上任何一台桌上型電腦和筆記型電腦的安全政策自動部署或軟體更新。OfficeScan 除了防止病毒的入侵外，還能針對不當入侵與間諜軟體等威脅加以防護。同時支援趨勢科技的網路防毒牆（Network VirusWall）達成校園資訊安全政策。

七、阻擋犯罪與色情之資訊或網頁，需建立處理機制並述明阻擋方式

1. 本校之阻擋犯罪與色情之資訊或網頁機制，係由硬體式快取伺服器負責，校內網路欲存取外部資訊或網頁時，core switch 會將所有的存取需求導向硬體式快取伺服器（非經由個人 pc 之 proxy 設定），硬體式快取伺服器在 catch 網頁時會先比對是否有 policy 中定義的 catch no 、service no 的網站，若有則拒絕使用者的連線要求
2. 硬體式快取伺服器 policy 中定義的 catch no service no 的網站名單係參考教育部建議之不良網站名單，另可以針對特定之網站加入 policy 的名單中．

連線到不當網站，proxy server拒絕存取回應

八、申請連線計劃書是否經學校或單位主管認可



參、結論

以上申請方案說明乃依據教育部規定，考量未來校園網路發展、成本負擔等因素而規劃，期望將來連線成功後，能順利建置規劃中之網路教學平台，並與台中區網及各中區連線學校保持更緊密聯繫，共享教學資源，讓整個教育網路發揮最大效能。