

教育部北區不當資訊系統說明會

系統運作概況介紹

豪勉科技 曾國興

2004/6/24

不當資訊系統網路硬體設備

1.Bluecoat SG800 Web Security Appliance



- ◆ SG800-0 Series Port 80 security appliances
 - CacheOS
(Custom-built OS, not Unix, Windows, Linux or Net BSD-based)
 - Fault tolerant
(最多可裝 4條RAM和4顆HD)
 - 1U rack mountable
 - 512MB ECC-RAM / 18GB SCSI HDD
(目前北區各點已陸續開始upgrade到 1G RAM / 73G HDD)

2. Alteon Application Switch

Alteon 2424



- 24 10/100 BASE-T ports
- 4 SFP-GBIC ports
- Up to 2M concurrent sessions
- 64K+ Layer 4 sessions/sec*
- Support RIP1 、 OSPF 、 BGP
- Small form factor (1U)

Alteon AD3



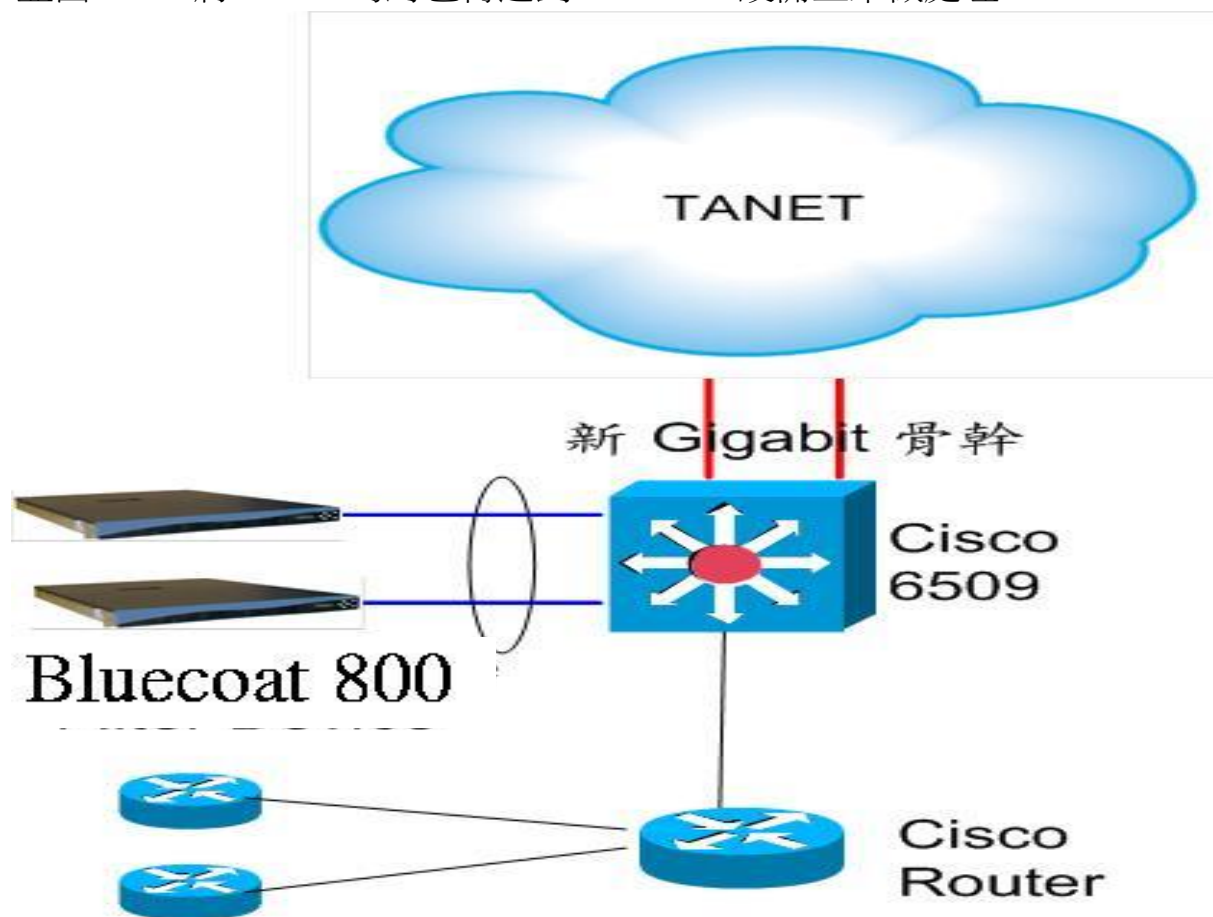
- 8 10/100 BASE-T ports
- 1 SX Giga port
- 2 MB memory per port
- Up to 224 packet filtering rule per switch
- Up to 256 real servers support

不當資訊系統網路運作架構

1.透過Catalyst 6509轉送封包

建置地點：東華大學、花蓮師院、台東師院、花蓮縣網、台東縣網、金門縣網、連江縣網(共7點)。

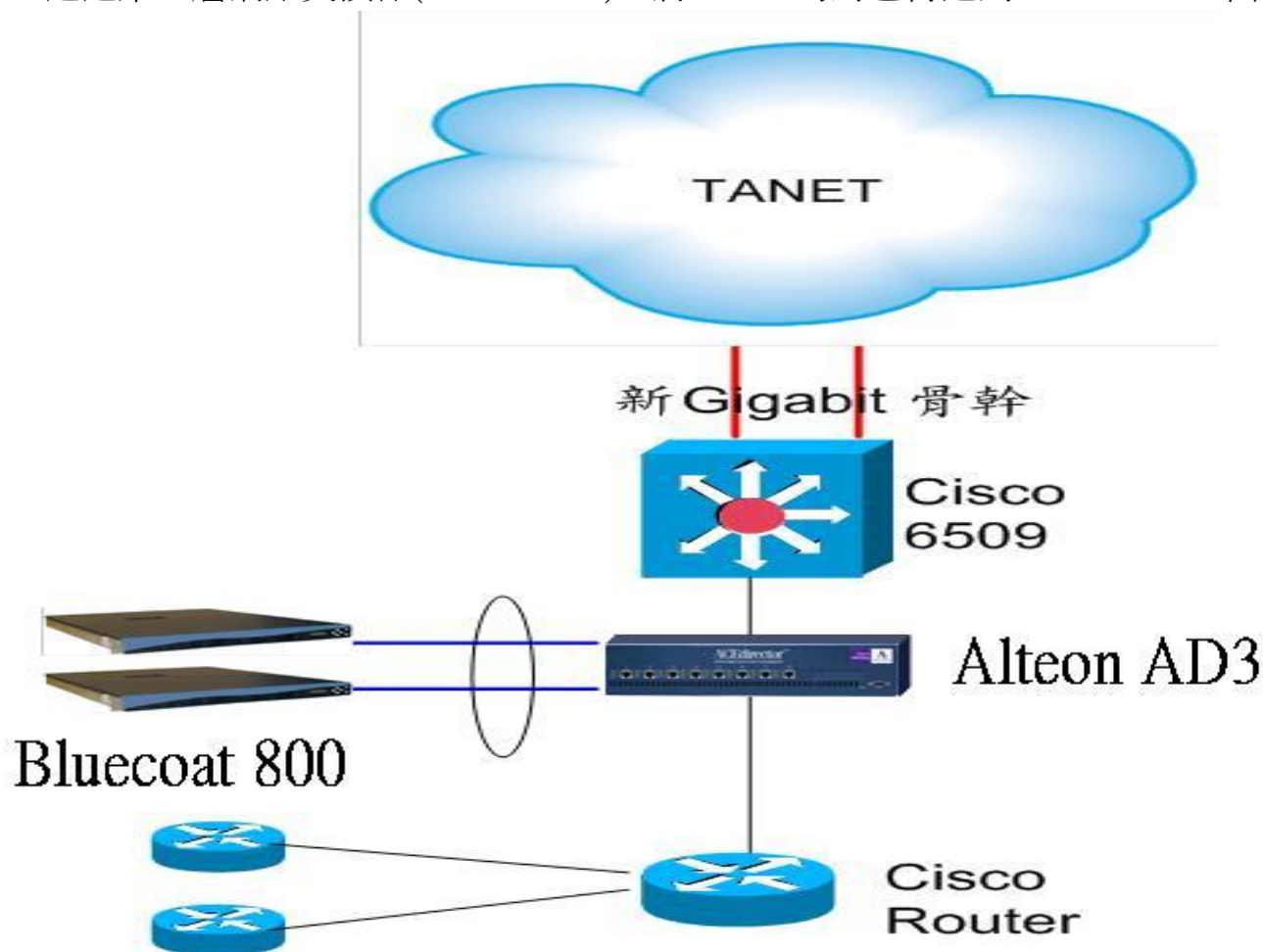
架構說明：從下圖可以得知連接到區縣網路中心的流量，都會透過Cisco Catalyst 6509 來連接新骨幹，因此我們利用 6509 作為 HTTP 封包轉送的設備。啟動 6509 和 Bluecoat 的 WCCP 功能，並由 6509 將 HTTP 的封包轉送到 Bluecoat 設備上來做處理



2.在Cisco Router及Catalyst 6509之間架設 第四層網路交換器轉送封包

建置地點：台灣大學、政治大學、中央大學(共3點)。

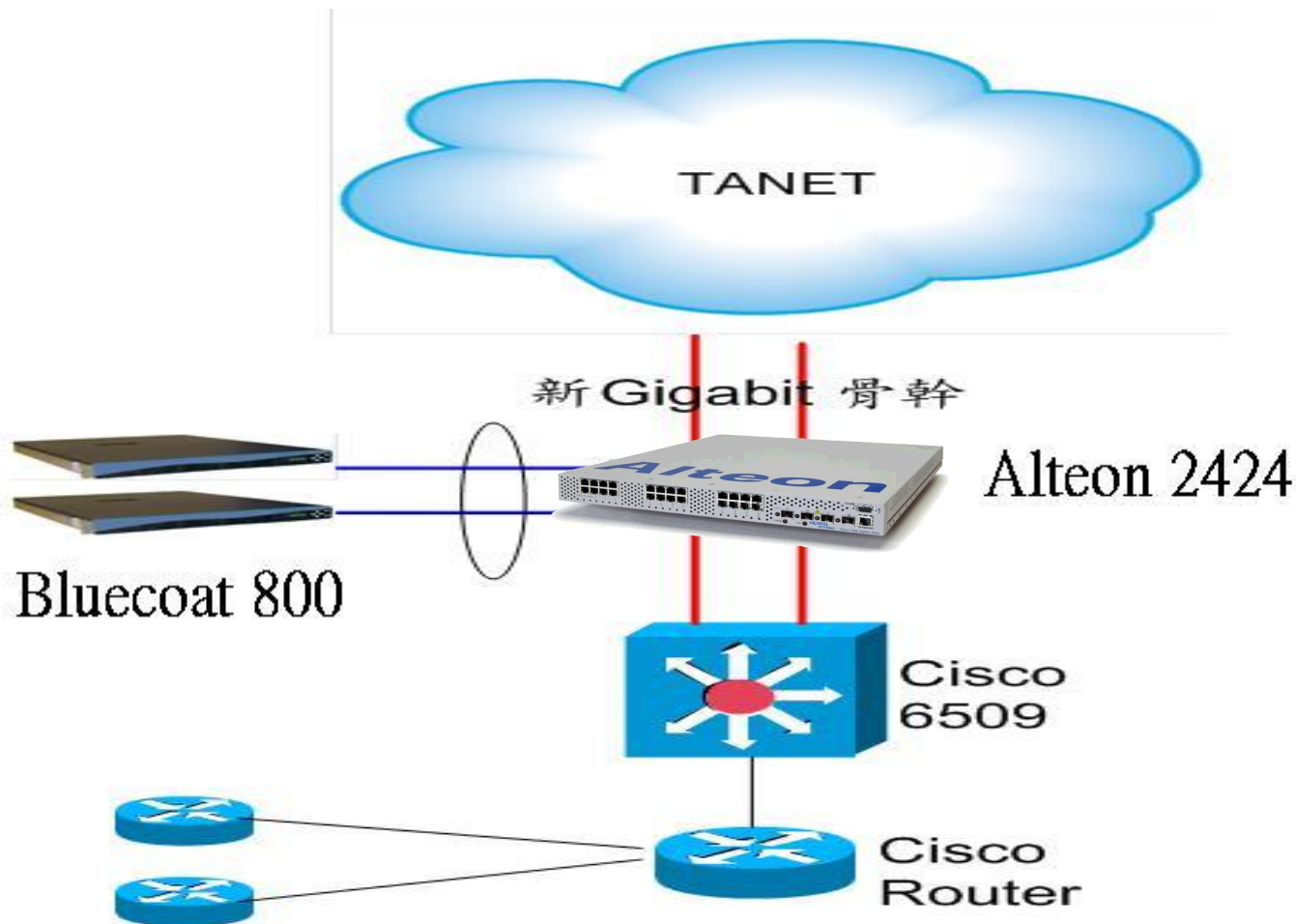
架構說明：針對介接於台大、政大、中大底下但尚未通過新世代骨幹網路升級之學校，提供過濾機制，透過第四層網路交換器(Alteon AD3)，將 HTTP 的封包轉送到 Bluecoat 上來做處理。



3.Catalyst 6509出口處架設第四層網路交換器 轉送封包

建置地點：台北市網、台北縣網、基隆市網、桃園縣網、宜蘭縣網(共5點)。

架構說明：在建置點的 Catalyst 6509 對外兩條 Gigabit Ethernet 電路上安裝第四層網路交換器(Alteon 2424)，對外出口處將HTTP封包導向 Bluecoat 設備進行過濾。



不當資訊系統網路運作現況

1.Bluecoat如何進行過濾？

1.取得Filter

Bluecoat原廠提供的pattern

```
; HTTP CONNECT
[Regular-expression]
https://.*:(443|80) service=yes
https://.*:[0-9]+/ service=no

; SPAM
[/^]+:25/$ service=no

; Nimda.A
http://www/ service=no
/[Rr][Ee][Aa][Dd][Mm][Ee]\.[Ee][Xx][Ee] service=no
/system32/cmd\.\exe\?[/root\.\exe\?[/readme\.\eml$) service=no

; Code Red
(?i)/.*\.ida\?.{230} service=no cache=no

; Slapper
http://.*/*mod_ssl:error:HTTP-request.* service=no

; Blaster
^http://\d+\.\d+\.\d+\.\d+/$ service=no
```

資料庫廠商提供的Filters

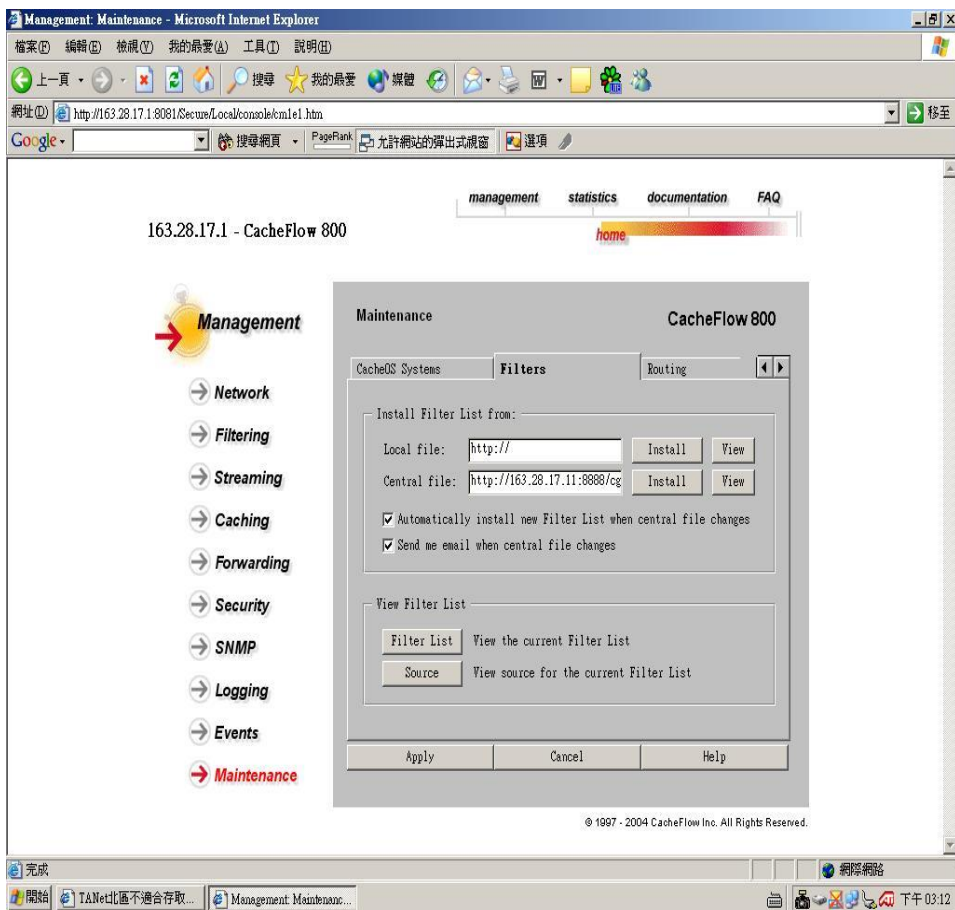
```
http://66.115.143.129 service=no cache=no
http://195.10.44.23 service=no cache=no
http://66.203.198.106 service=no cache=no
http://66.212.225.149 service=no cache=no
http://66.110.189.30 service=no cache=no
http://207.219.111.152 service=no cache=no
http://69.44.58.23 service=no cache=no
http://195.10.46.40 service=no cache=no
http://209.47.15.254 service=no cache=no
http://66.212.226.138 service=no cache=no
http://www.casino.com/common service=no cache=no
http://www.cashsurfers.com/images service=no cache=no
http://www.asian-xxx-girls.com service=no cache=no
http://www.asianapples.com service=no cache=no
http://www.asianbare.com service=no cache=no
http://www.asianclassmates.com service=no cache=no
```

.....

1.Bluecoat如何進行過濾？

2.設定Filter

透過WEB UI方式



透過CLI的方式

```
Bluecoat# inline filter-list central "end-267520988-inline"
```

```
http://66.115.143.129 service=no cache=no  
http://195.10.44.23 service=no cache=no  
http://209.47.15.254 service=no cache=no  
http://66.212.226.138 service=no cache=no  
http://www.asianapples.com service=no cache=no  
http://www.asianbare.com service=no cache=no  
http://www.asianclassmates.com service=no cache=no
```

```
.....  
end-267520988-inline  
Bluecoat#
```

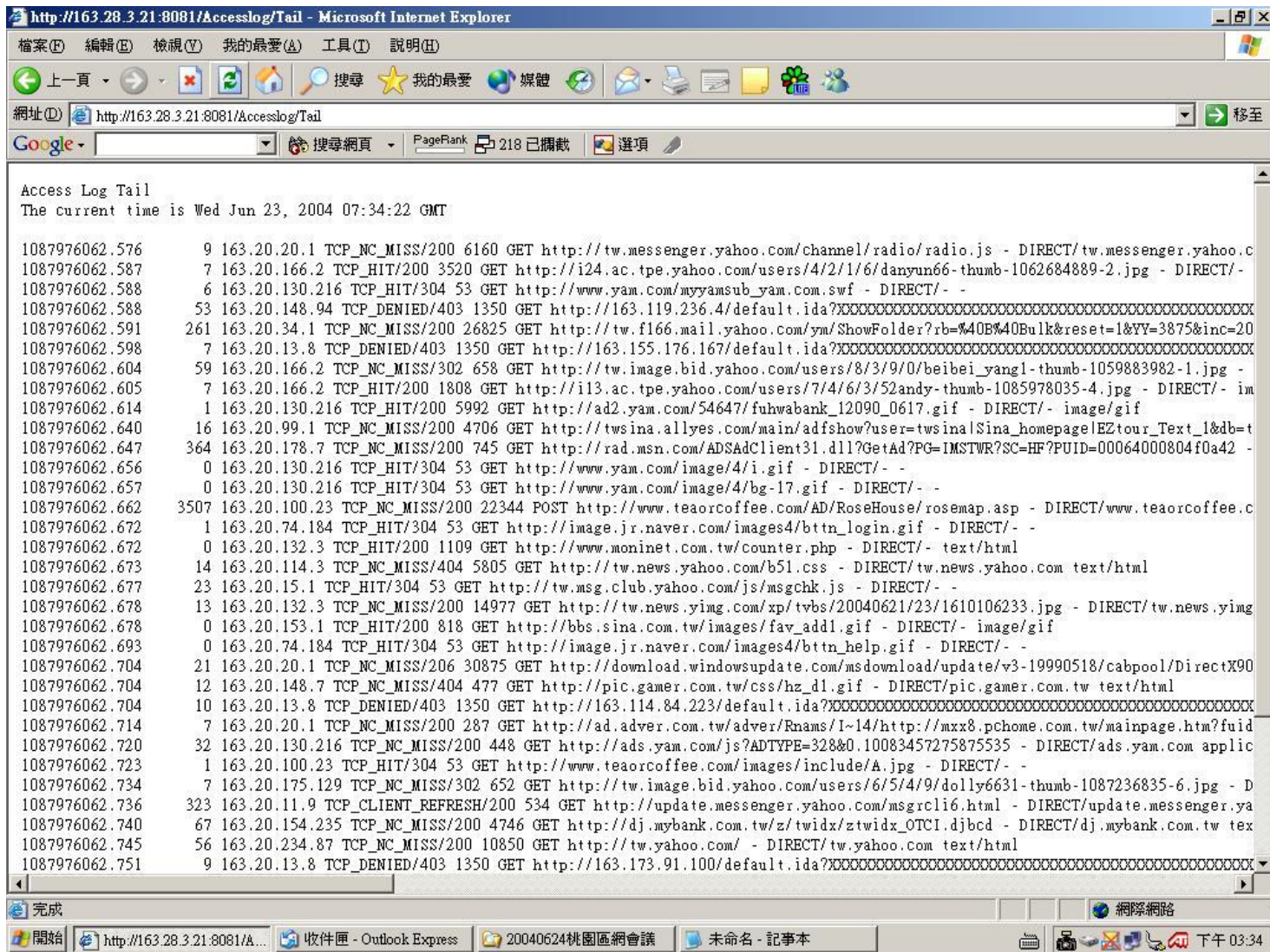
```
Bluecoat#inline filter-list local "end-267520988-inline"
```

```
; Code Red  
(?i)/.*\.ida\?.{230} service=no cache=no  
; Slapper  
http://.*mod_ssl:error:HTTP-request.* service=no  
; Blaster  
^http://\d+\.\d+\.\d+\.\d+/$ service=no
```

```
.....  
end-267520988-inline  
Bluecoat#
```

1.Bluecoat如何進行過濾？

3.觀察Filter運作情形



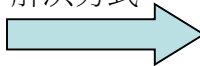
1.Bluecoat如何進行過濾？

4.Filter實際運作的特殊狀況

a.啟用防止Blaster的Filter

```
; Blaster  
^http://\d+\.\d+\.\d+\.\d+/$ service=no
```

解決方式



對於常用的IP網址設入Bluecoat的
By-pass list

```
Bluecoat#inline bypass-list local "end-267520988-inline"
```

```
134.208.0.0 255.255.0.0  
140.110.0.0 255.254.0.0  
140.112.0.0 255.240.0.0  
140.138.0.0 255.255.0.0
```

```
.....  
end-267520988-inline  
Bluecoat#
```

會導致以IP為網址的網站被過濾

b.User反應連線到網站的反應時間變慢

1.正常情況下Bluecoat回給Client的時間是很短的
除非對方網站不存在，或是網路實際連線狀況不良

2.Bluecoat能夠Handle的Client數量滿載(病毒攻擊)
Bluecoat 800-0 能夠Handle 539個Client連線

1.Bluecoat如何進行過濾？

5.申訴網頁(當使用者連結到被過濾的網頁時會出現)



2.Bluecoat設備的效能檢視

1.進入WEB UI點選Statistics的General選項，可觀察一些基本狀態

The screenshot shows a Microsoft Internet Explorer browser window displaying the Bluecoat CacheFlow 800 web interface. The address bar shows the URL `http://163.28.17.1:8081/Secure/Local/console/cm2a1.htm`. The page title is "Statistics: General - Microsoft Internet Explorer".

The main content area displays "163.28.17.1 - CacheFlow 800". At the top, there are navigation links: "management", "statistics", "documentation", and "FAQ". The "statistics" link is highlighted with a red bar and the word "home" below it.

On the left side, there is a vertical menu with the following items: "Statistics" (highlighted with a red arrow), "General" (highlighted with a red arrow), "Volume", "Resources", "Efficiency", "Contents", and "Event Viewer".

The main content area shows the "General Statistics" section for "CacheFlow 800". It has tabs for "Summary", "Environment", and "Disks 1-2". The "Summary" tab is selected.

The "Summary" tab contains two sections:

- Configuration**
 - Disks installed: 1
 - Memory installed: 512 megabytes
 - CPUs installed: 1
 - Software image: Version: CA 4.1.10 Release id: 18924
 - Serial number: 5002000084
- General status**
 - Last access log upload: 2004-06-23 02:00:00+08:00CST
 - Current access log size: 16.31 megabytes
 - System started: 2003-11-02 15:41:15+08:00CST
 - CPU utilization: 6 percent

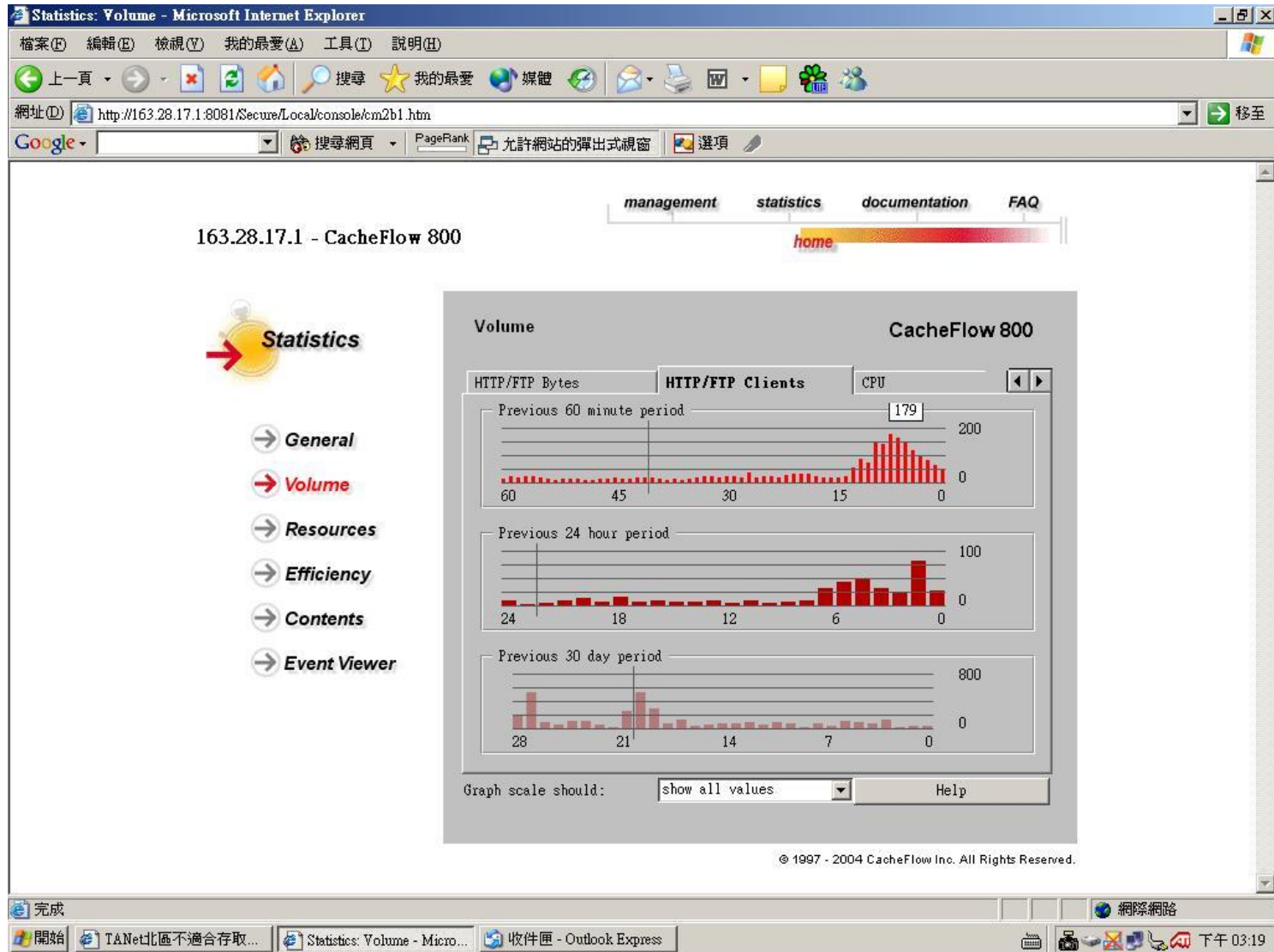
At the bottom right of the "General Statistics" section, there is a "Help" button.

The footer of the page contains the copyright notice: "© 1997 - 2004 CacheFlow Inc. All Rights Reserved."

The Windows taskbar at the bottom shows the following open applications: "完成", "開始", "TANet北區不適合存取...", "Statistics: General - Micros...", and "收件匣 - Outlook Express". The system clock shows "下午 03:19".

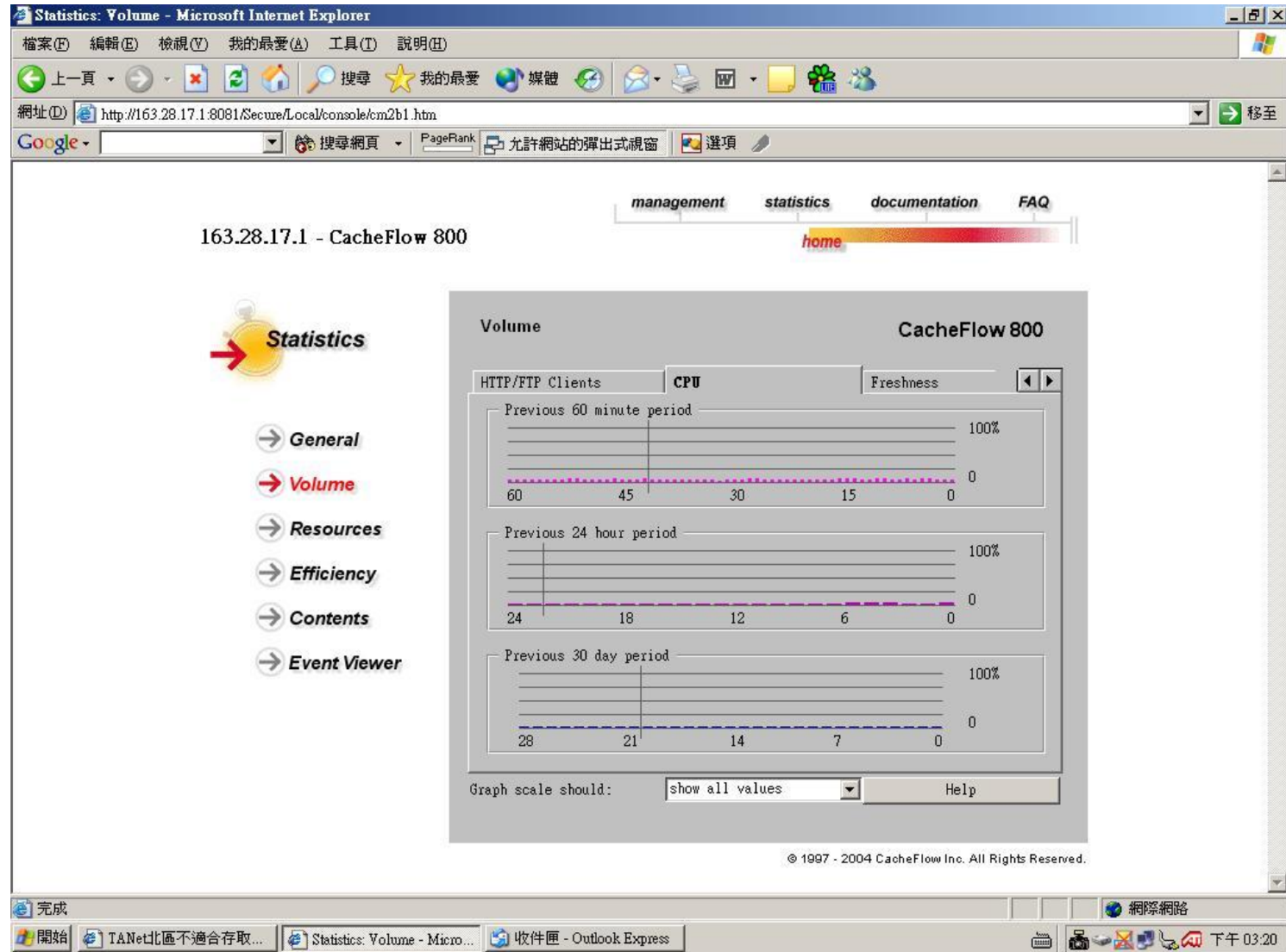
2.Bluecoat設備的效能檢視

2.點選Volumn的HTTP/FTP Client選項，可觀察Client的歷史連線數



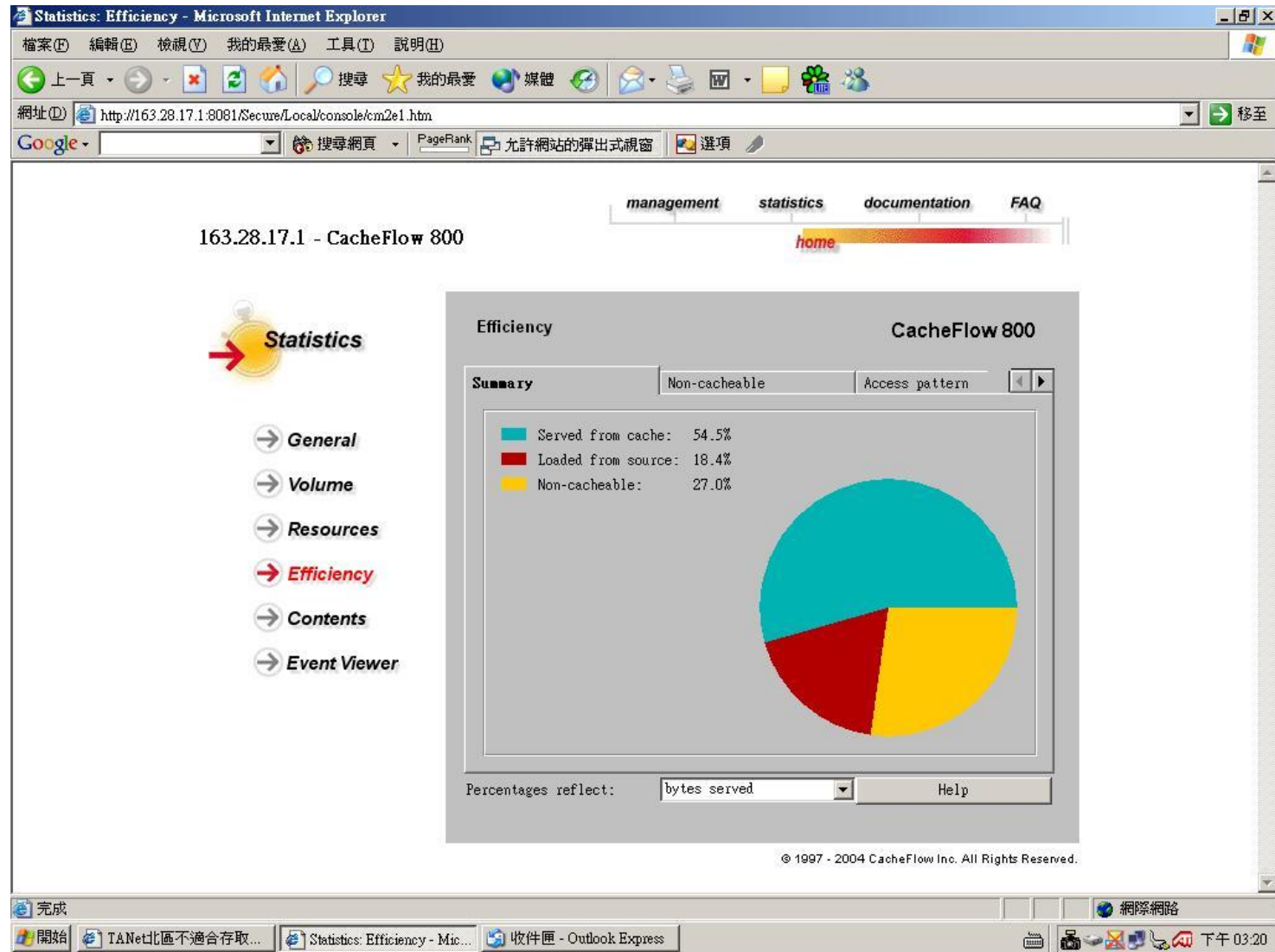
2.Bluecoat設備的效能檢視

3.點選Volumn的CPU選項，可觀察CPU值的歷史紀錄



2.Bluecoat設備的效能檢視

4.點選Efficiency的Summary選項，可觀察Client的Hit rate



2.Bluecoat設備的效能檢視

5.北區不當資訊設備狀況的首頁，可透過MRTG圖檢視設備的狀況

TANet北區不適合存取網頁過濾機制 - 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://163.28.16.18/mrtg/ 移至

Google 搜尋網頁 PageRank 218 已擷取 選項

台灣學術網路北區不適合存取網頁過濾機制

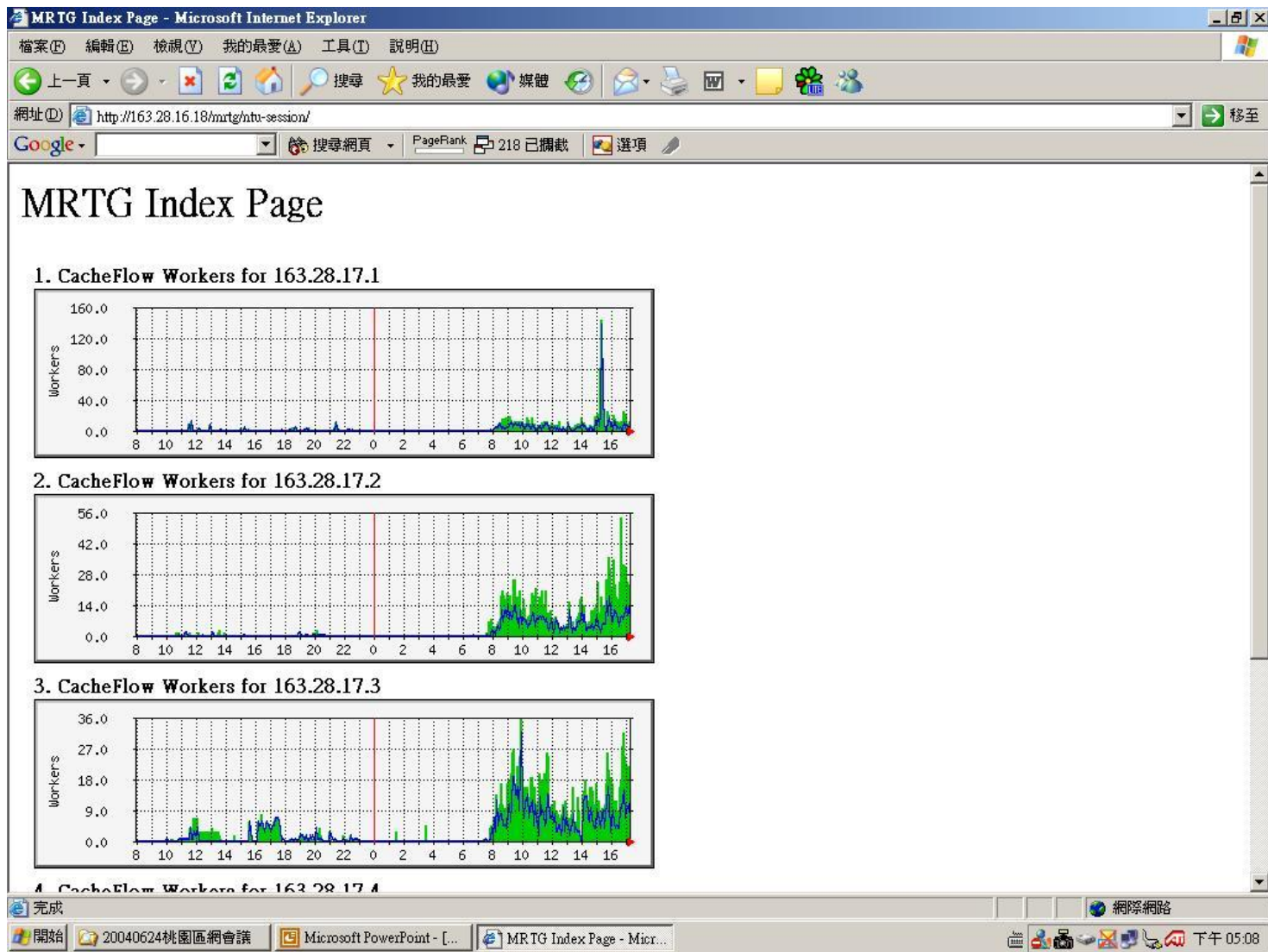
北區各建置點設備狀況

台灣大學	政治大學	中央大學	東華大學	花蓮師院
<ul style="list-style-type: none">• MRTG流量圖• BC session• 163.28.17.1, log• 163.28.17.2, log• 163.28.17.3, log• 163.28.17.4, log• NTU Alteon AD3: 流量; CPU	<ul style="list-style-type: none">• MRTG流量圖• BC session• 163.28.33.1, log• 163.28.33.2, log• 163.28.33.3, log• NCCU Alteon AD3: 流量; CPU	<ul style="list-style-type: none">• MRTG流量圖• BC session• 203.72.244.217, log• 203.72.244.218, log• 203.72.244.219, log• NCU Alteon AD3: 流量; CPU	<ul style="list-style-type: none">• MRTG流量圖• BC session• 134.208.8.58, log• 134.208.8.59, log• 6509 CPU Load	<ul style="list-style-type: none">• MRTG流量圖• BC session• 163.28.146.1, log• 163.28.146.2, log• 6509 CPU Load
台東師院	台北市教育網	台北縣教育網	基隆市教育網	宜蘭縣教育網
<ul style="list-style-type: none">• MRTG流量圖• BC session• 163.28.178.1, log• 163.28.178.2, log• 6509 CPU Load	<ul style="list-style-type: none">• MRTG流量圖• BC session• 163.28.18.226, log• 163.28.18.227, log• 163.28.18.194, log• 163.28.18.195, log• TPC Alteon 2424: 流量; CPU	<ul style="list-style-type: none">• MRTG流量圖• BC session• 163.28.3.21, log• 163.28.3.23, log• 163.28.3.25, log• 163.28.3.27, log• TPC Alteon 2424: 流量; CPU	<ul style="list-style-type: none">• MRTG流量圖• BC session• 163.28.33.252, log• 163.28.33.220, log• KL Alteon 2424: 流量; CPU	<ul style="list-style-type: none">• MRTG流量圖• BC session• 163.28.18.252, log• 163.28.18.220, log
桃園縣教育網	台東縣教育網	花蓮縣教育網	金門縣教育網	連江縣教育網
<ul style="list-style-type: none">• MRTG流量圖• BC session	<ul style="list-style-type: none">• MRTG流量圖	<ul style="list-style-type: none">• MRTG流量圖	<ul style="list-style-type: none">• MRTG流量圖	<ul style="list-style-type: none">• MRTG流量圖

開始 收件匣 - Outlook Exp... 不當資訊防制 TANet北區不適合存... MSN Messenger Microsoft Word 國際網路 下午 03:46

2.Bluecoat設備的效能檢視

6.透過MRTG圖，檢視四部Bluecoat的Client連線數



Thank You

Jackson Tseng
jacksont@hauman.com.tw
www.hauman.com.tw