智慧網管系統

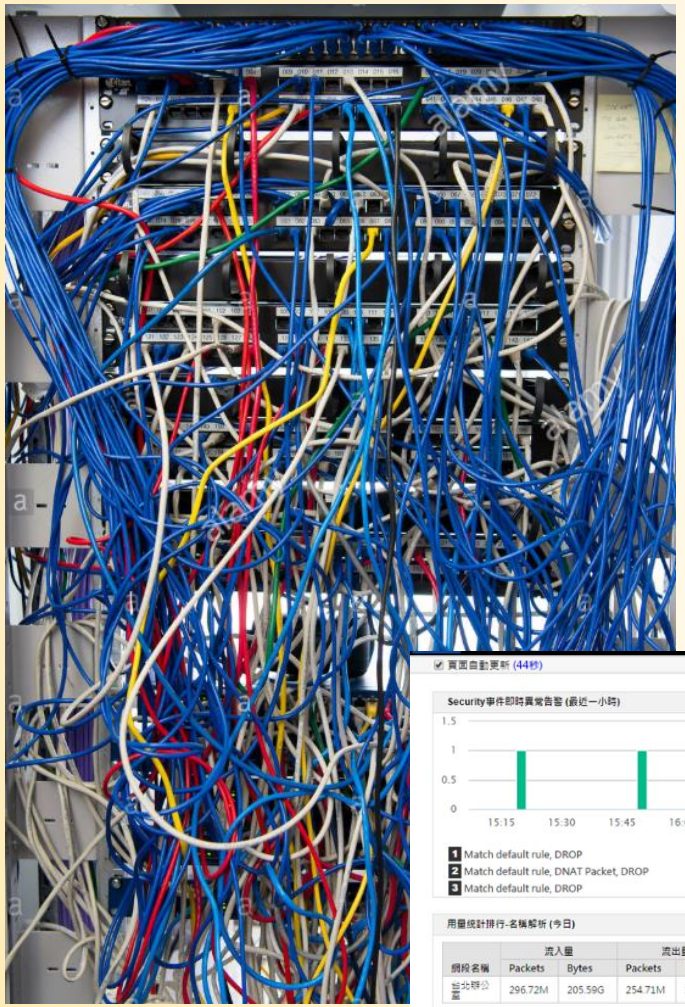
https://nms.ntpc.edu.tw

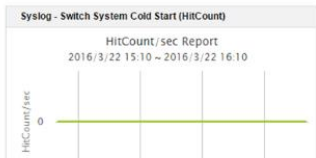
地點：教研中心電腦教室
時間：2020 年 11 月 10日

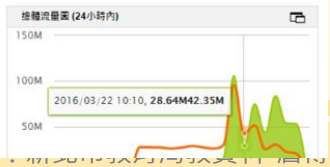
簡報大綱

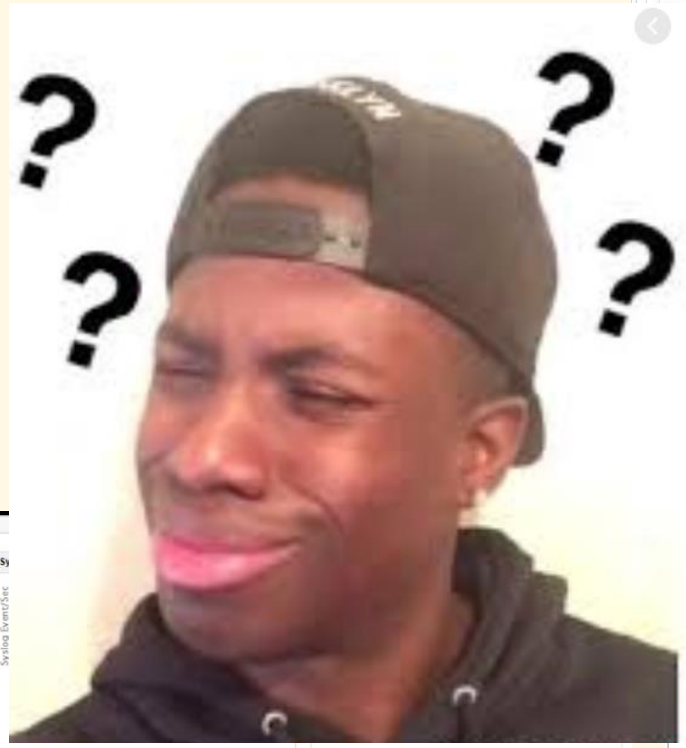
- 瞭解學校網路架構圖與實體位置
  - 加註設備所在位置
  - 尋找與加入設備：手動新增、搜尋新增
- 監控與追蹤管理設備
- 查詢與封鎖設備
  - 查詢學校有哪些網段
  - 封鎖來路不明設備

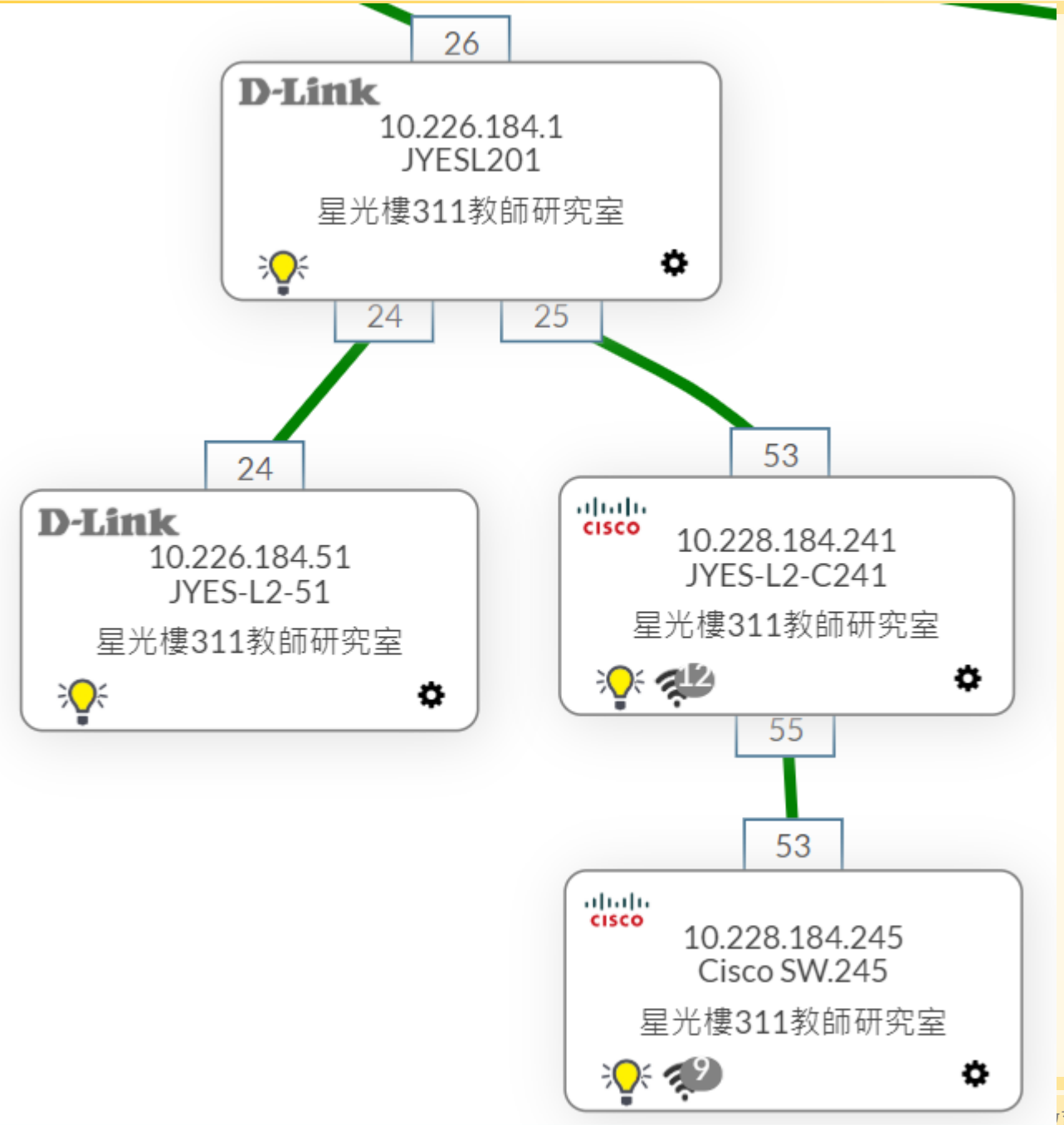
1.這麼亂的機櫃，這麼多的線路與交換器，我該如何整理？
2.每一條線到底接到哪裏?是做什麼用的?真的每條線都有在使用嗎？
3.這麼多台交換器，通通放在一起，究竟是串接在一起，還是分開的呢？

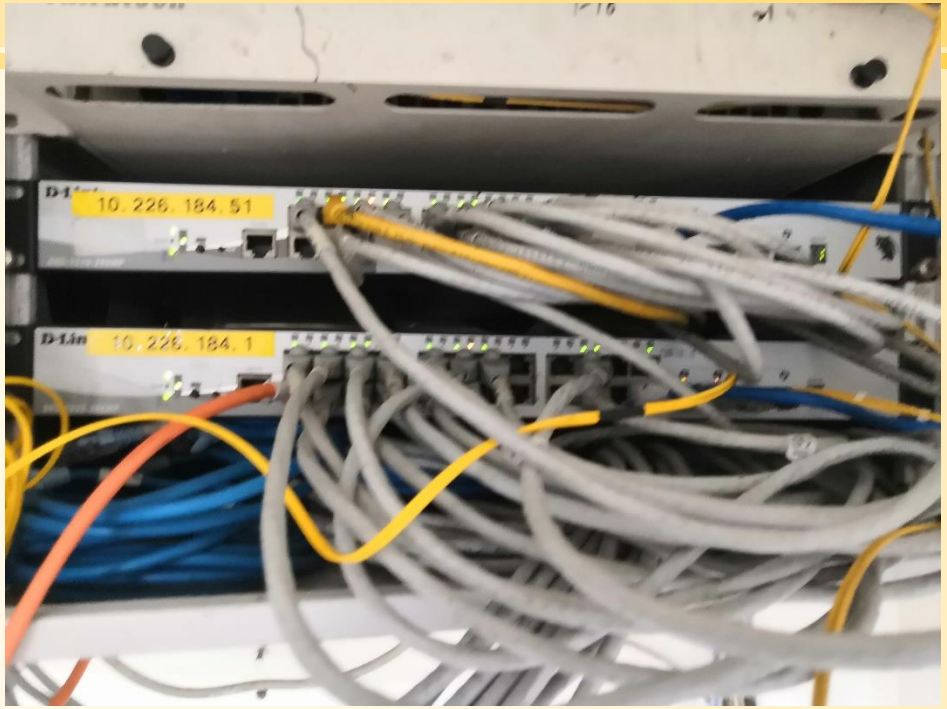


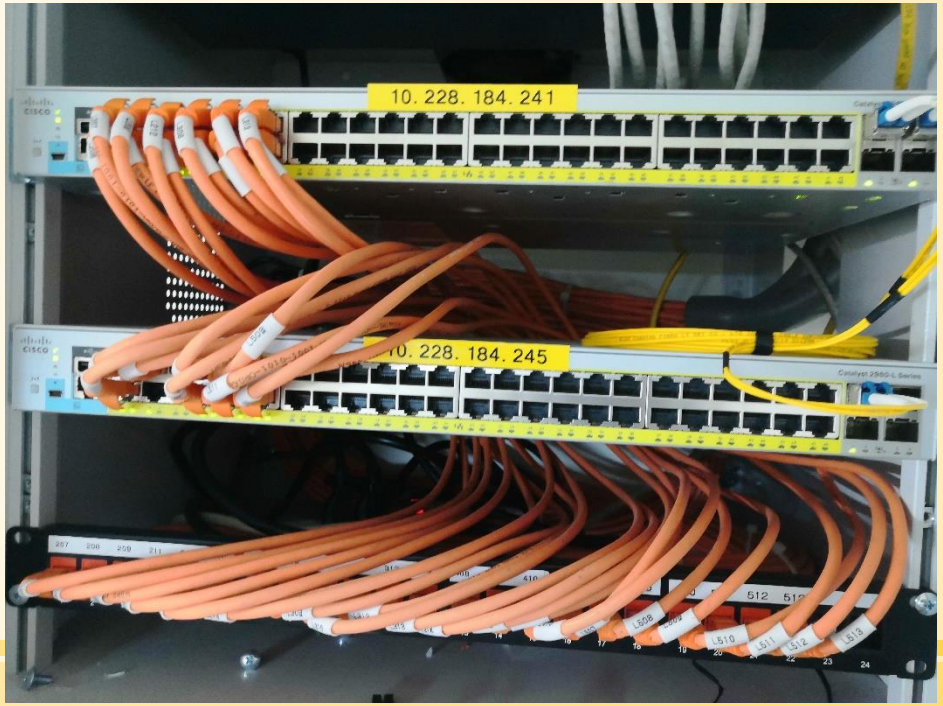


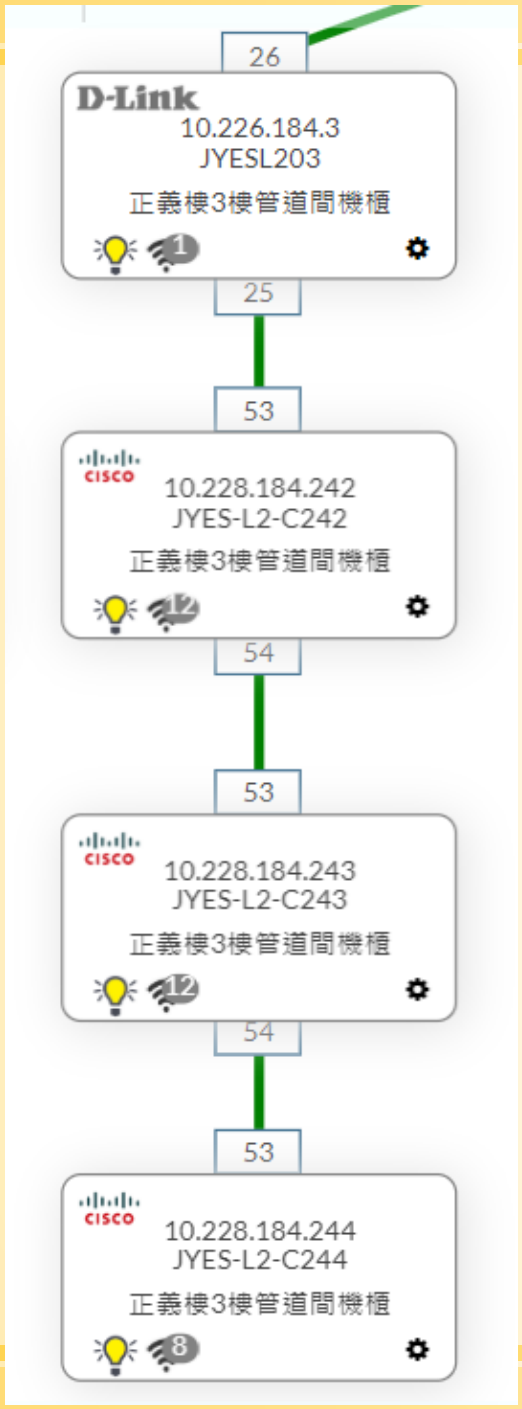





26
D-Link
10.226.184.1
JYESL201
星光樓311教師研究室
24
25
24
D-Link
10.226.184.51
JYES-L2-51
星光樓311教師研究室
53
CISCO
10.228.184.241
JYES-L2-C241
星光樓311教師研究室
55
53
CISCO
10.228.184.245
Cisco SW.245
星光樓311教師研究室


10. 226. 184. 51
10. 226. 184. 1

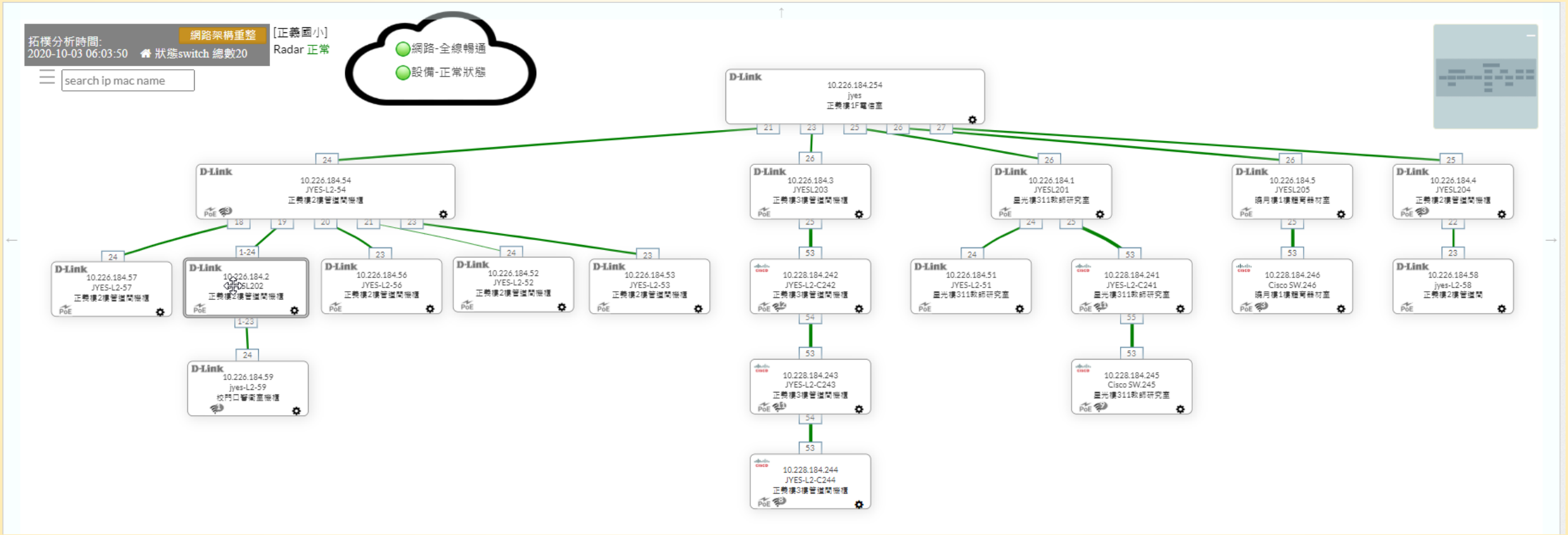

10. 228. 184. 241
10. 228. 184. 245


26
D-Link
10.226.184.3
JYESL203
正義棧3棟管道間機櫃
25
53
CISCO
10.228.184.242
JYES-L2-C242
正義棧3棟管道間機櫃
54
53
CISCO
10.228.184.243
JYES-L2-C243
正義棧3棟管道間機櫃
54
53
CISCO
10.228.184.244
JYES-L2-C244
正義棧3棟管道間機櫃


0. 228. 184. 242
Catalyst 2960-L Series

1.剛接任或到新學校，如何快速瞭解學校網路環境呢？

Ans: 可以透過nms 的網路架構瞭解交換器連接情形

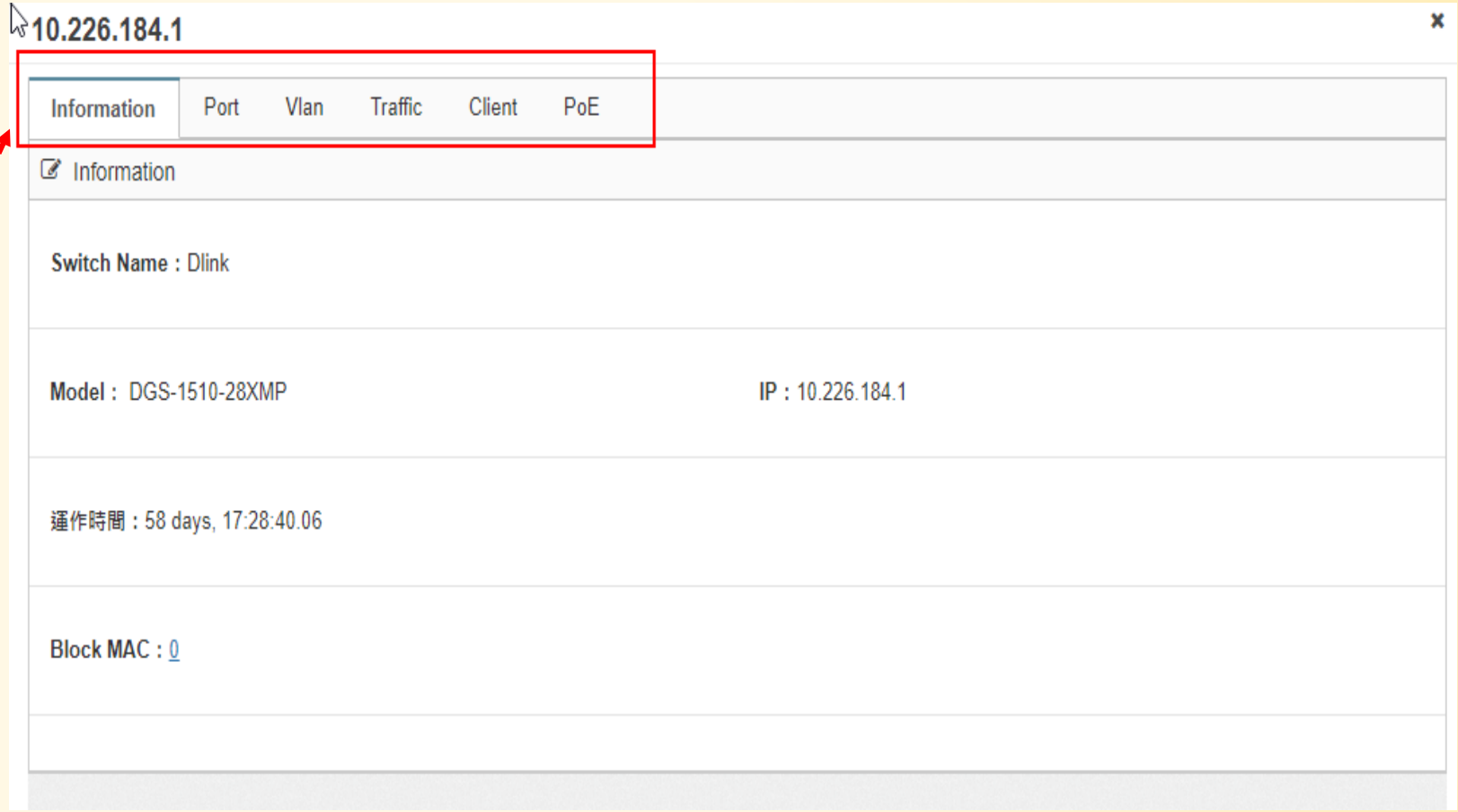


Ans: 可以透過nms 的網路架構瞭解交換器連接情形

網路拓樸圖顯示設定

利用IP 或 MAC 搜尋，可快速找到所在的交換器

Ans: 點選交換器右下角的 ⚙ 可以獲得相關資訊



- 找到現場(機房與機櫃位置)，比對網路架構圖。
- 貼上標籤貼紙。

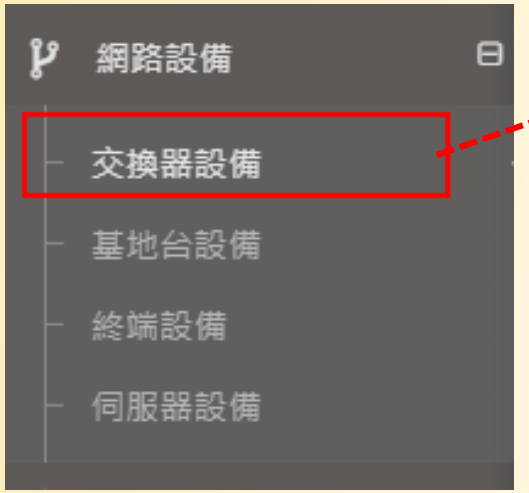
名稱：Jyes-L2-59

機型：DGS-1210-24P

ＩＰ：10.226.X.X

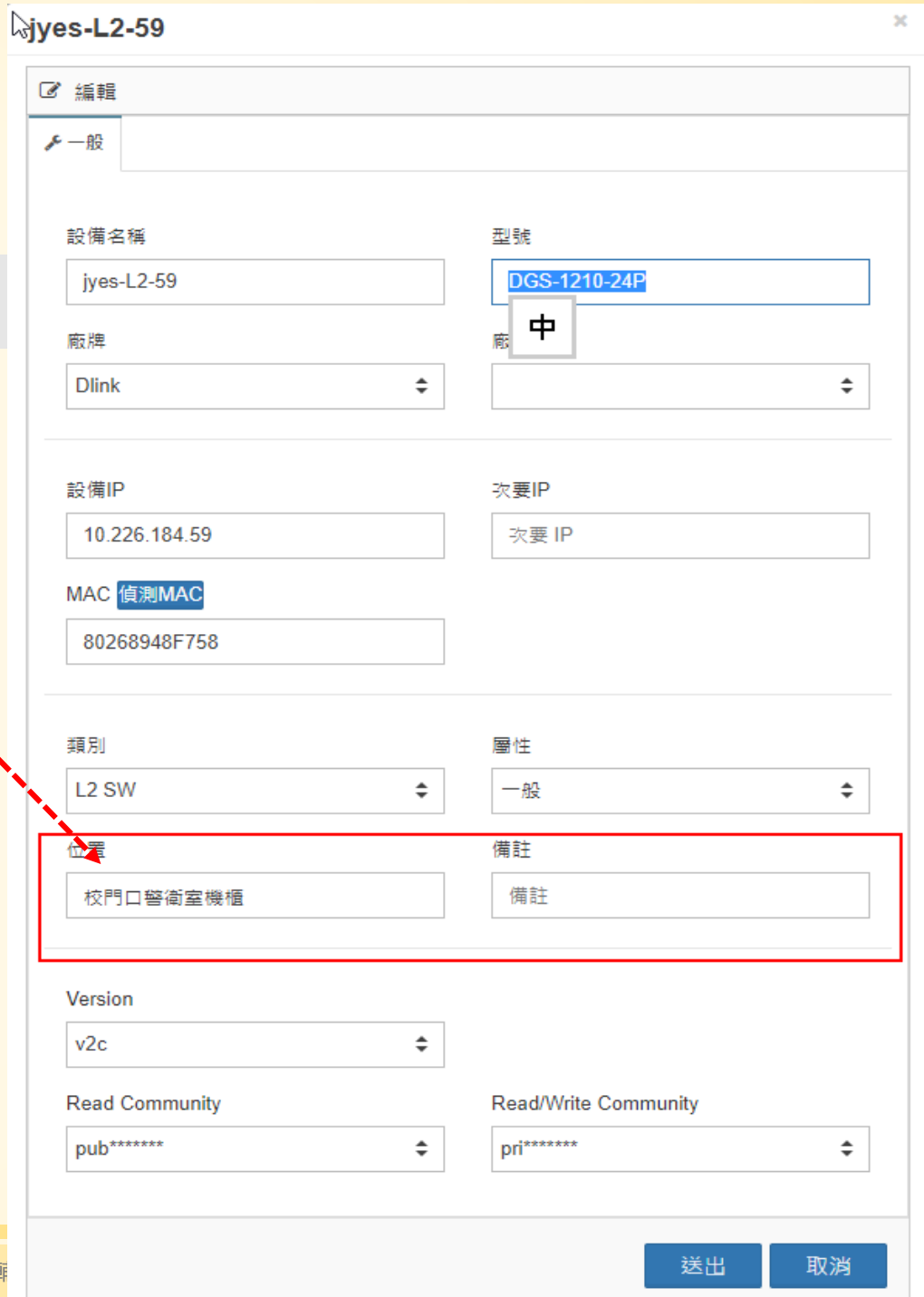
Vlan：1-9 :163 10-12:10.241

➢ 平台註記交換器說明。



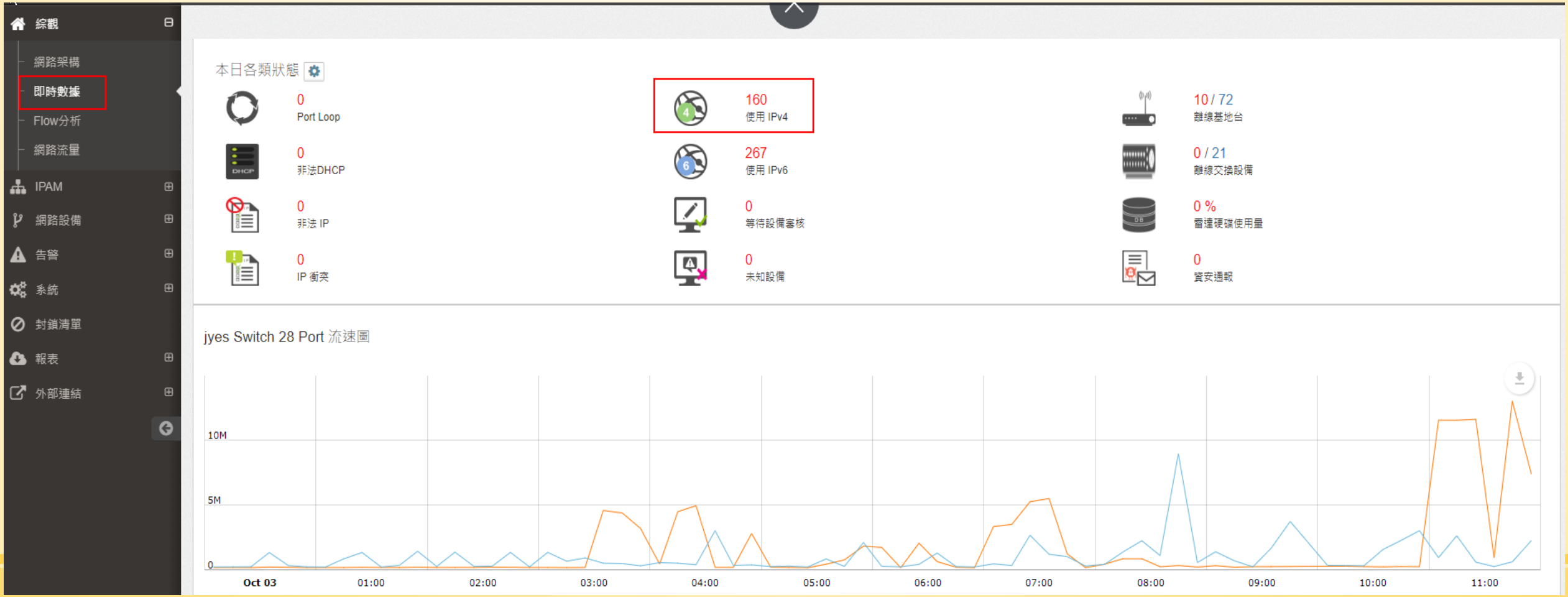
點選交換器

輸入放置位置:



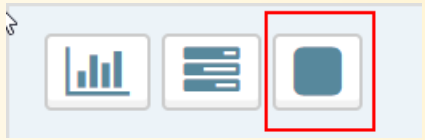
2.現在有哪些設備在使用中呢？

Ans: 利用即時數據，可得知目前網路設備現況



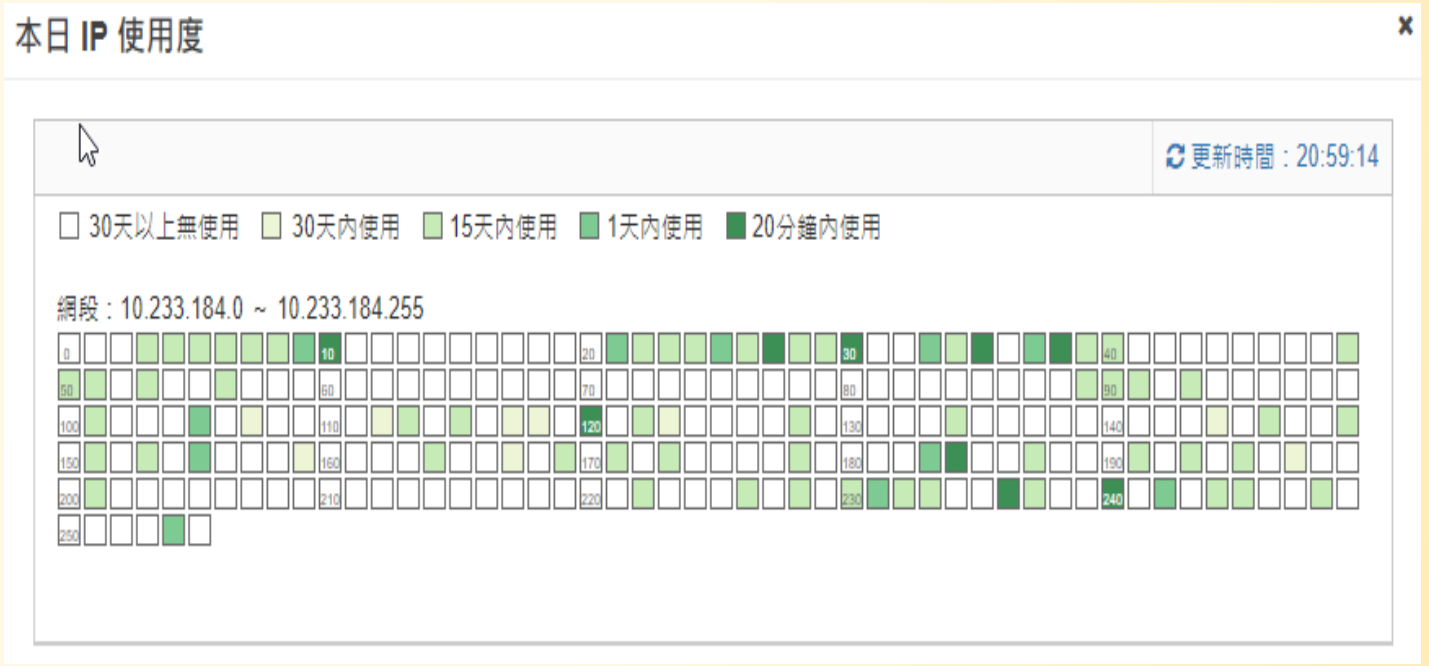
3.校內有哪些網段呢？網段使用情形是如何？

Ans: 透過IPAM->網段使用狀況，可得知各網段使用情形。



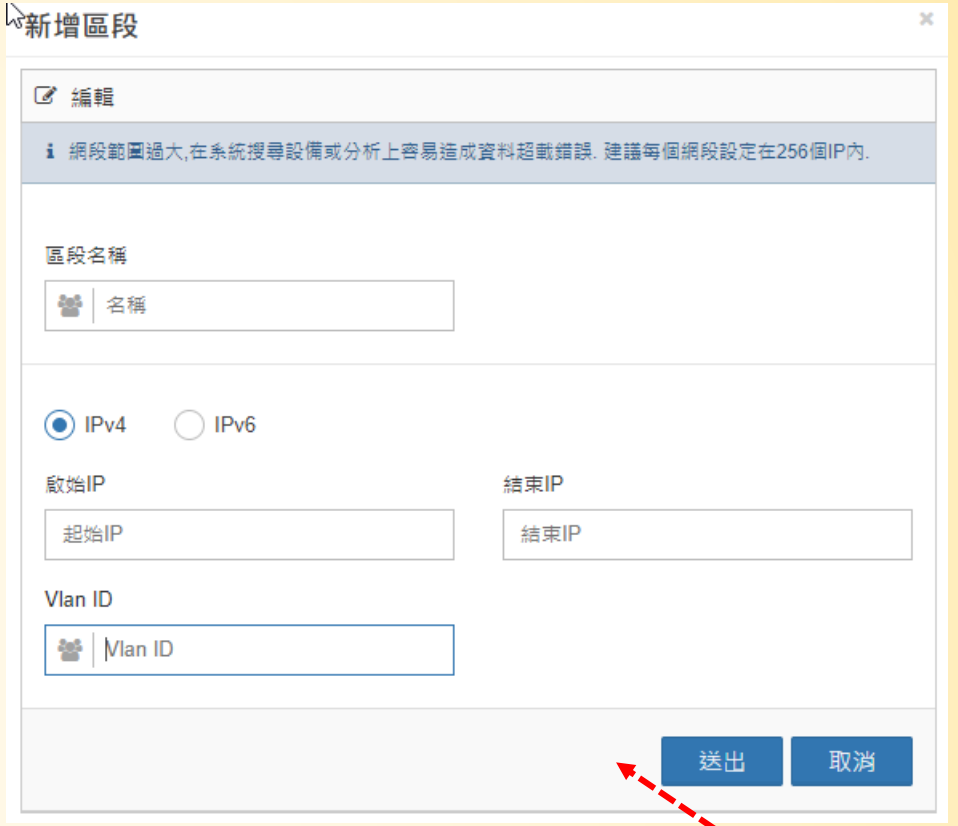
163.20.X.X：學校實體網段
10.241.X.X：班級教室網段
10.231.X.X：電腦教室網段

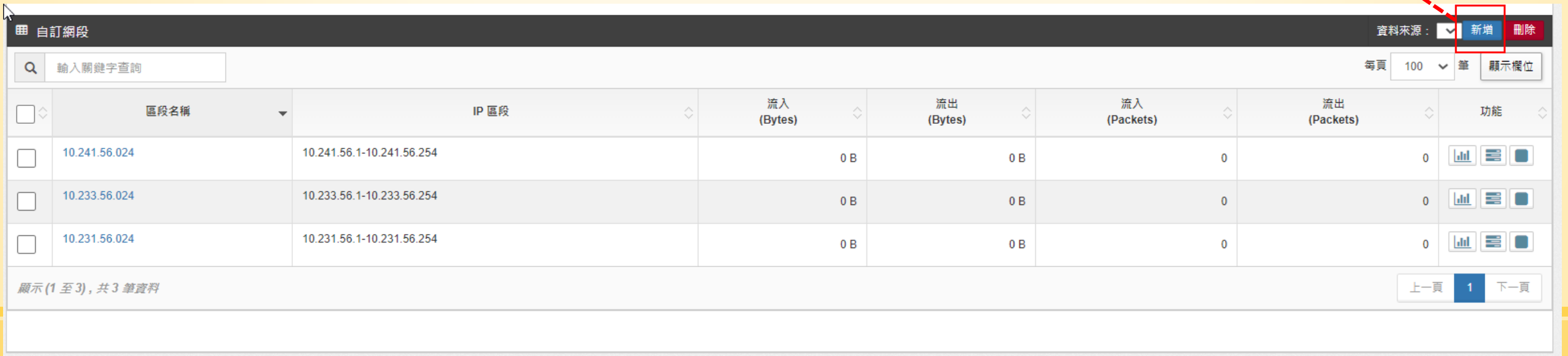
10.226.X.X：大同的交換器
10.228.X.X：華電的交換器



4. 新申請的網段如何納管監控呢?

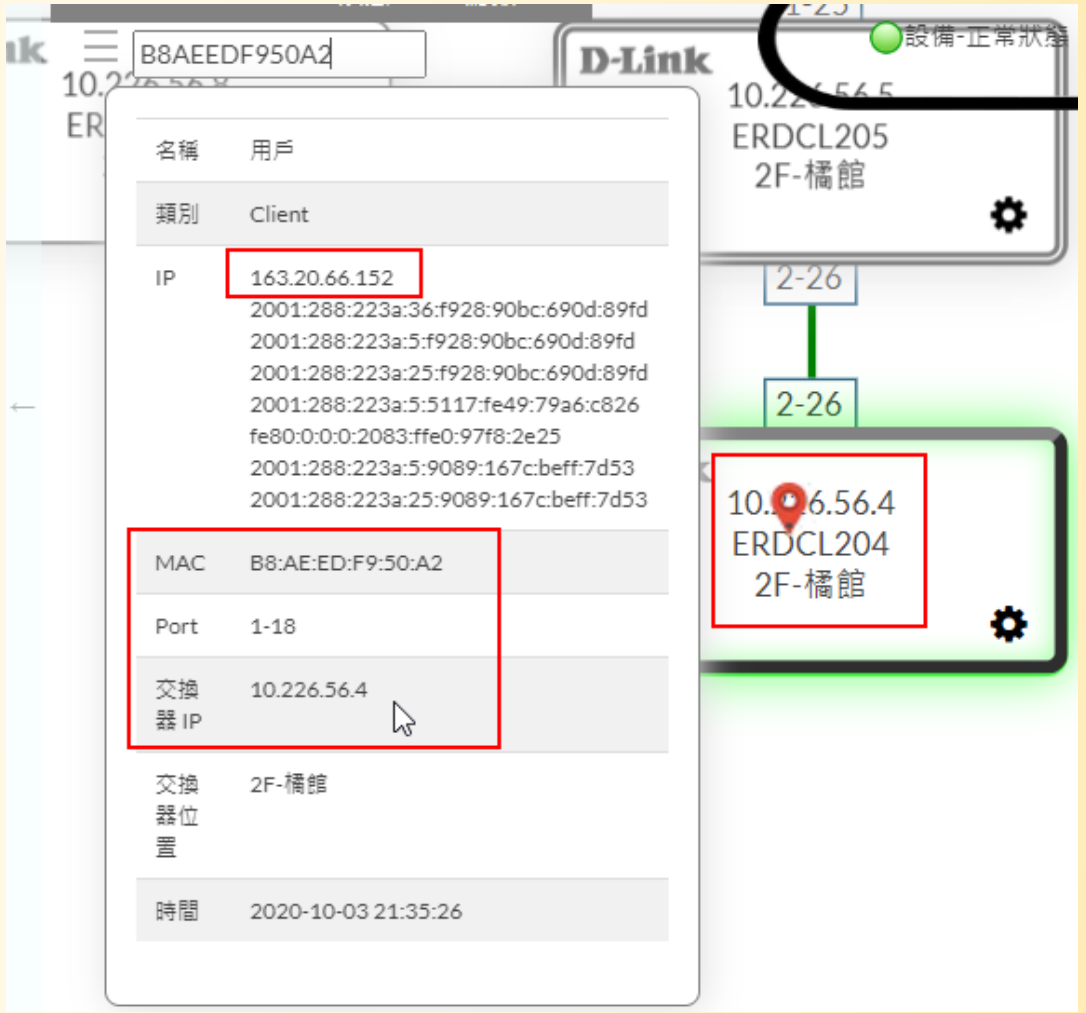
Ans: 利用自訂網段方式，
增加一個網段。





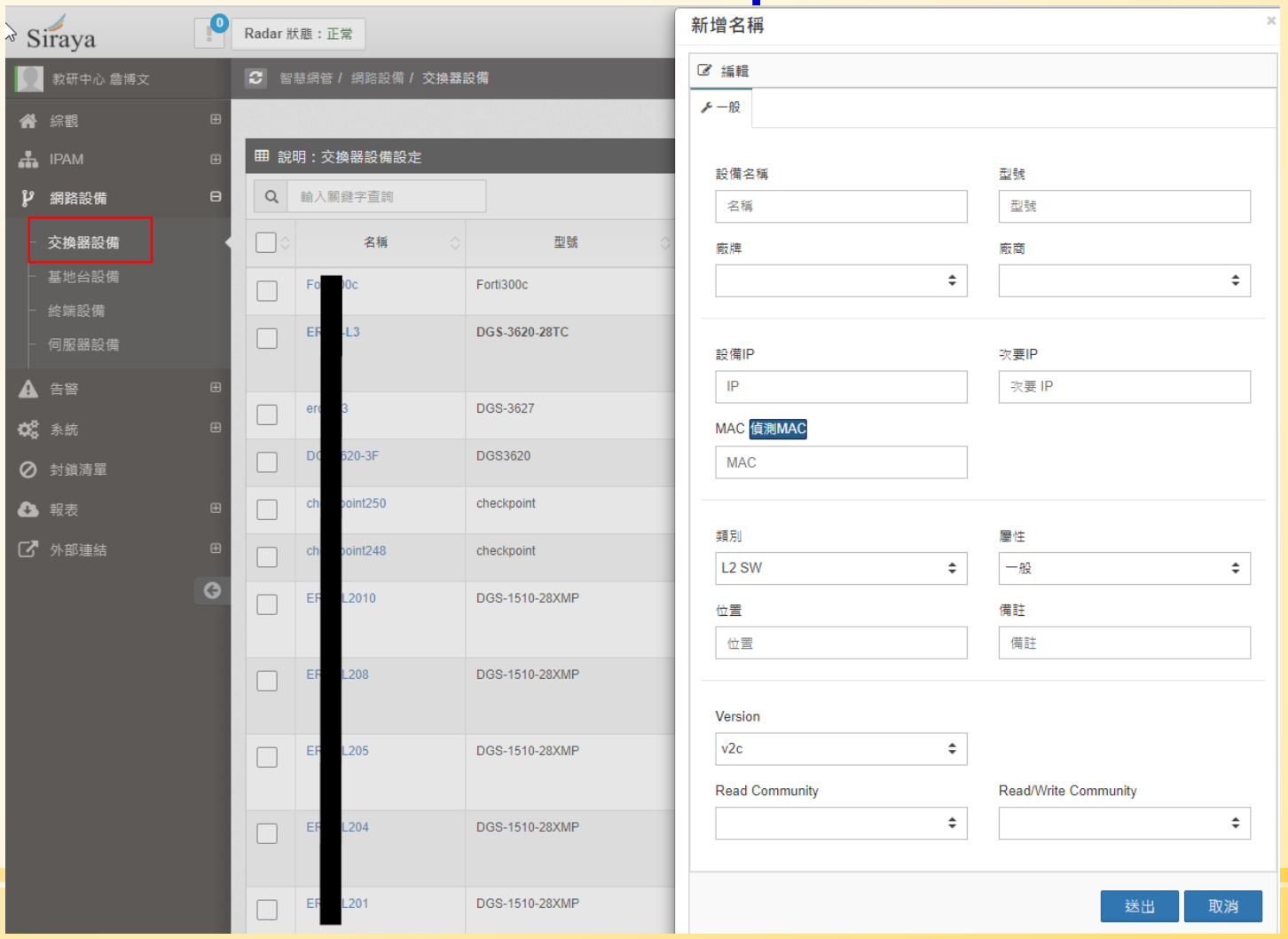
5 .班級電腦網路不通，網路發生驚嘆號，怎麼辦？

Ans: 透過MAC 搜尋在哪一台交換器哪一個port上，再到那台交換器上查看該port狀況 (是否亮燈)。



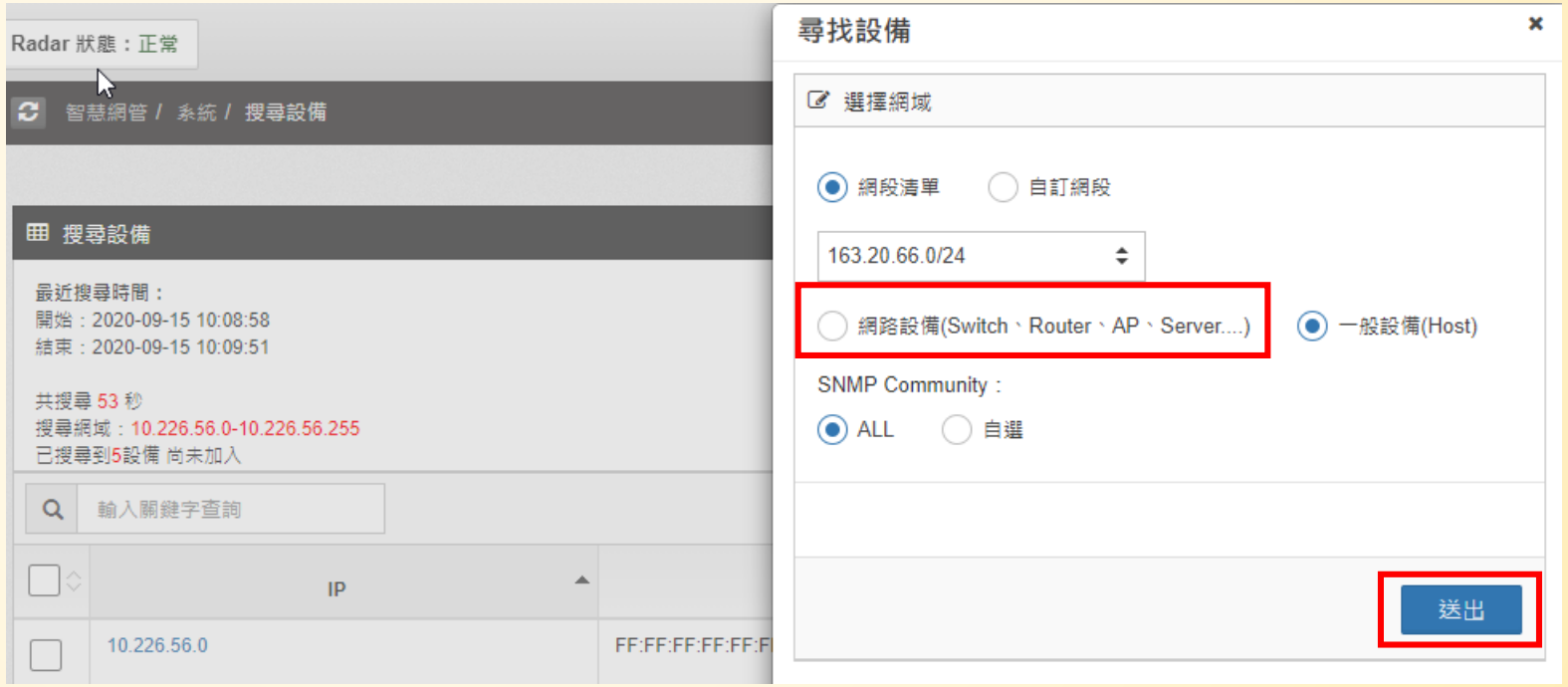
6-1.新添購的交換器設備，要如何納管呢？

Ans: (1) 將交換器上架、連網、開啟snmp通訊。
(2) 網路設備->交換器設備, [新增]
(3) 輸入設備名稱與IP、MAC及放置位置.



6-2.新添購的交換器設備，要如何納管呢？

Ans: (1) 將交換器上架、連網、開啟snmp通訊。
(2) 系統->搜尋設備-> [搜尋設備]
(3) 如有找到新設備，則勾選後，按下 [新增]
(4) 輸入設備名稱與IP、MAC及放置位置.



7.地震預警系統連線到交換器上，該怎麼辦？

Ans: (1) 地震預警系統必須走實體ＩＰ，因此，必須先確認哪個實體ＩＰ沒在使用。

(2) 設備連接上交換器後，應在網路線貼上標籤，並在交換器該port上標註說明. (網路設備->交換器設備，[port 編輯])

8.各班教室無線AP，可以納管嗎？

Ans:

(1) 可以的，各班教室AP應以納管到nms中，在網路設備->基地台設備中。

(2) 可利用[設備清單匯出]功能，匯出後，編輯名稱和裝設位置，再利用 [批次匯入] 功能，匯入"基地台設備"中。

18	fhjhAP206_輔導處	10.226.[redacted]	C8:[redacted]90	DAP-2690	Dlink	5	2	public	private	輔導處

9.整合控制器內的安卓電腦，也能納管嗎？

Ans:

(1) 可以的，利用系統->搜尋設備，搜尋10.241.X.X網段，或貴校班級教室的網段。

(2) 將搜尋到的設備，名稱為shuttle加入到一般設備中，即可納管監控。

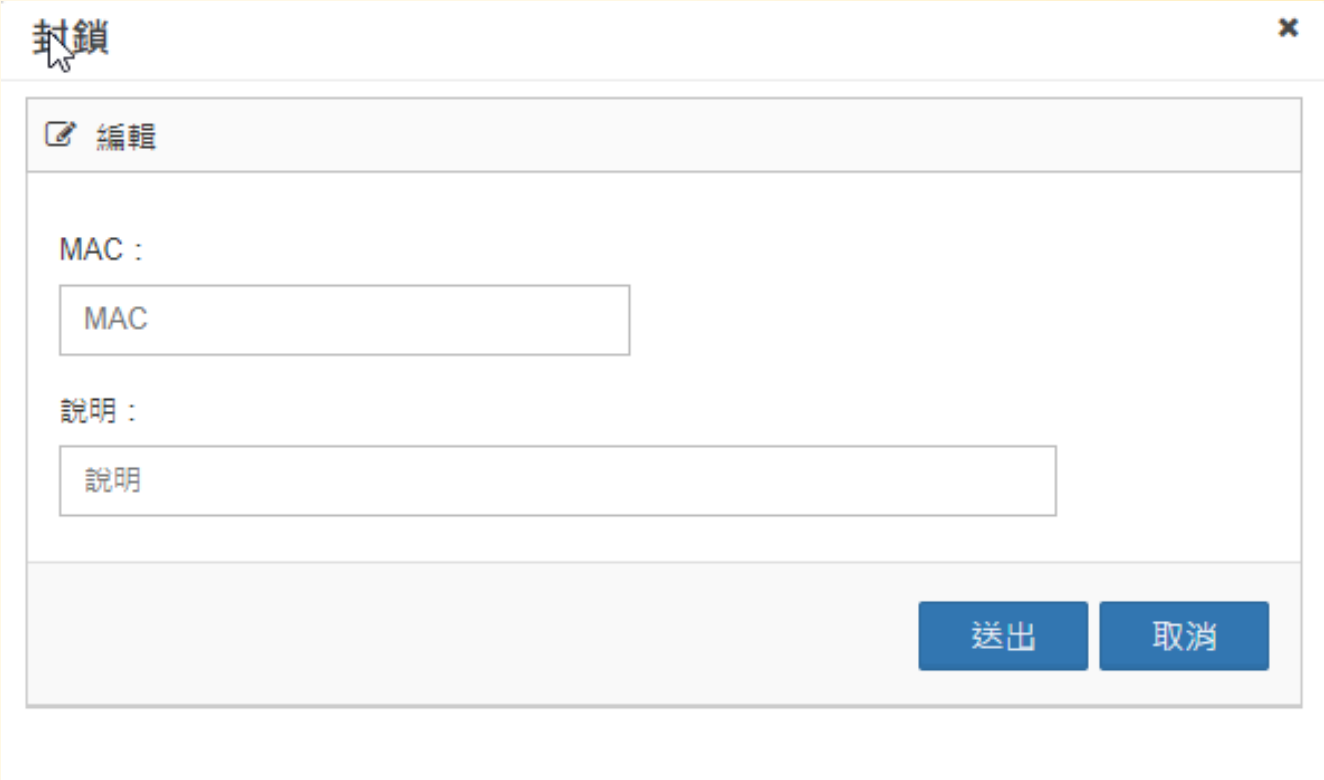
10.當收到局端告知某IP中毒或成為殭屍電腦時，該如何處理？

Ans:

(1) 利用智慧網管，找到該IP的電腦MAC與連接的交換器port 號。

(2) 封鎖清單，[新增]。

(3) 將該電腦重新還原，並安裝防毒與windows update



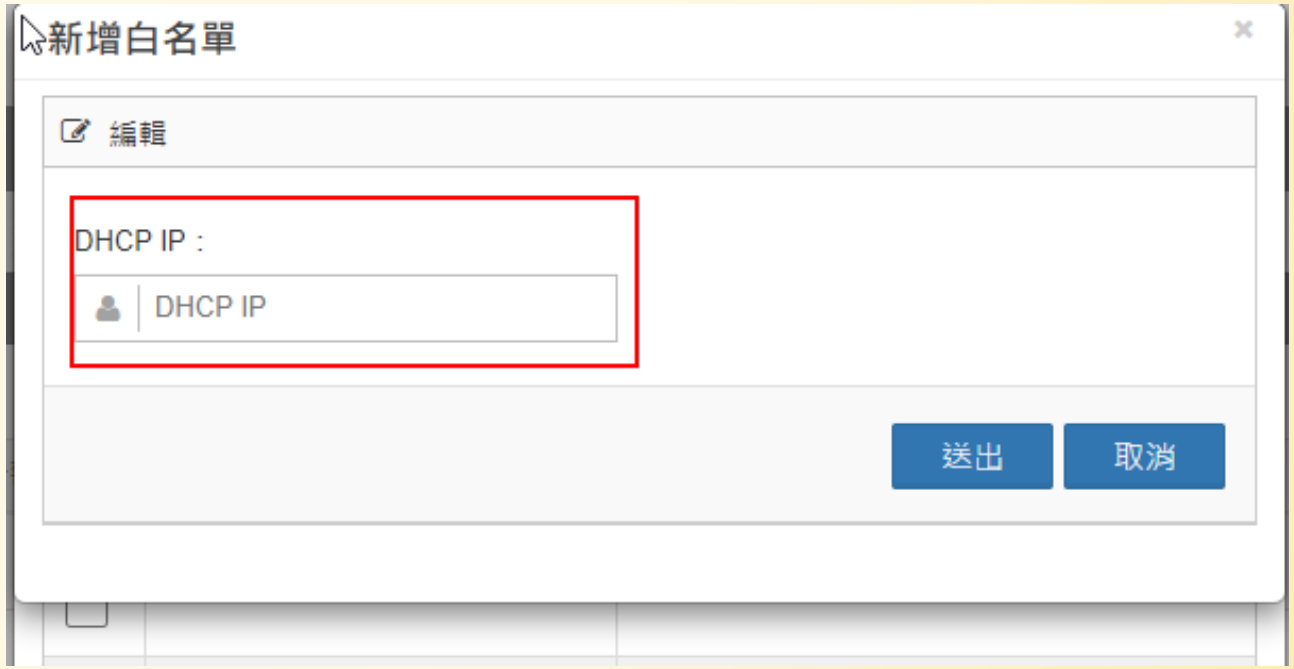
11.電腦教室的EVO Server 要如何設定不告警？

Ans:

(1) 找出EVO Server 主機的IP。

(2) 告警->告警設定->非法DHCP ，[白名單][新增]。

(3)輸入主機IP， [送出]



12.當收到IP衝突告警時，該如何處理？

Ans:

(1) 告警->告警記錄，找尋最近的告警(3-5天)。

(2) 如果是兩台PC，設定相同ＩＰ，則將其中一台ＩＰ調整即可，如果是交換器配發DHCP問題，則到ＣＣ平台報修，通知相關廠商處理。

[作業1] : Mdm 主機如何加入智慧網管內？

[作業2]：智慧教室內的 白色 Dlink AP 如何納管？

[作業 3]: 整合控制器安卓主機如何納管？

[作業４]：檢查網路架構圖是否與學校現況符合？

使用智慧網管前後分析

無智慧網管	
項目	佔據時間
校園網路管理	60%
教課與備課	30%
處理行政業務	10%

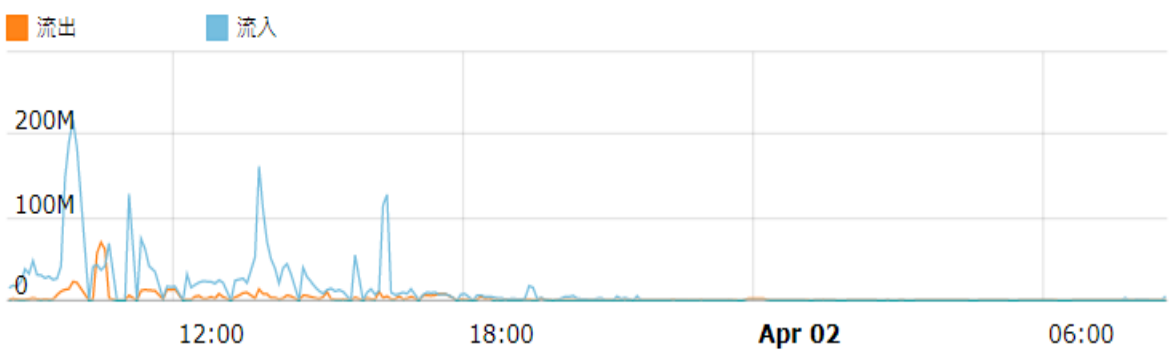
使用智慧網管	
項目	佔據時間
校園網路管理	20%
教課與備課	50%
處理行政業務	30%

監控與追蹤管理設備(1)

透過每日圖表分析，可以瞭解學校在哪個時段網路流量特別高

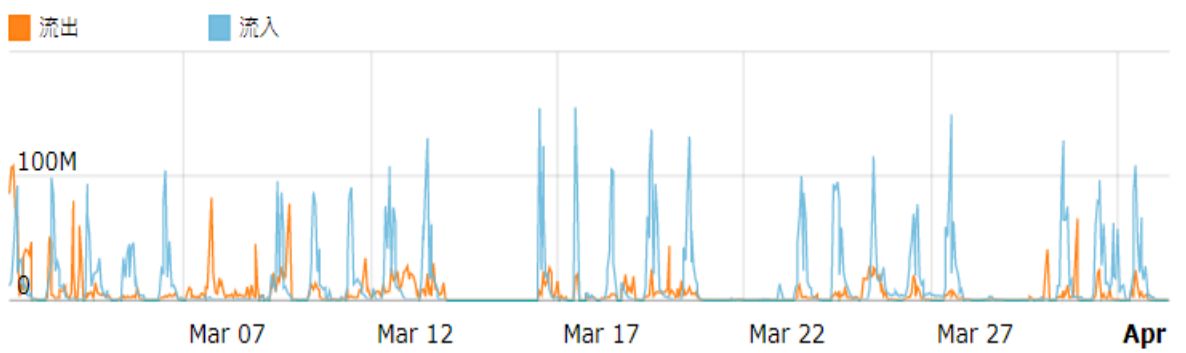
顯示時間：2020年04月02日 08時35分

每日圖表（5分鐘平均）



	最大	平均	目前
流入	217.34 Mbps (217.34%)	13.57 Mbps (13.57%)	609.91 kbps (0.61%)
流出	70.05 Mbps (70.05%)	2.77 Mbps (2.77%)	583.17 kbps (0.58%)

每月圖表（1小時平均）

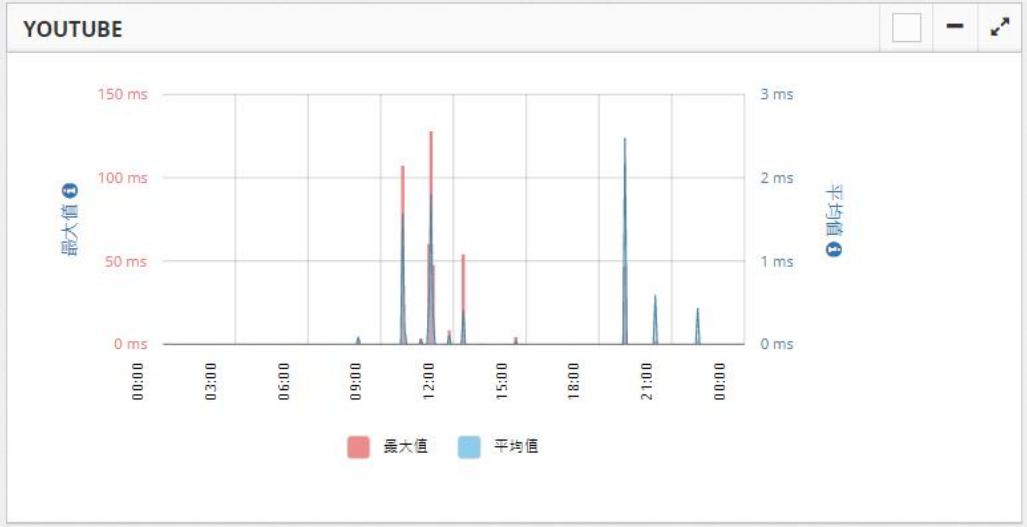


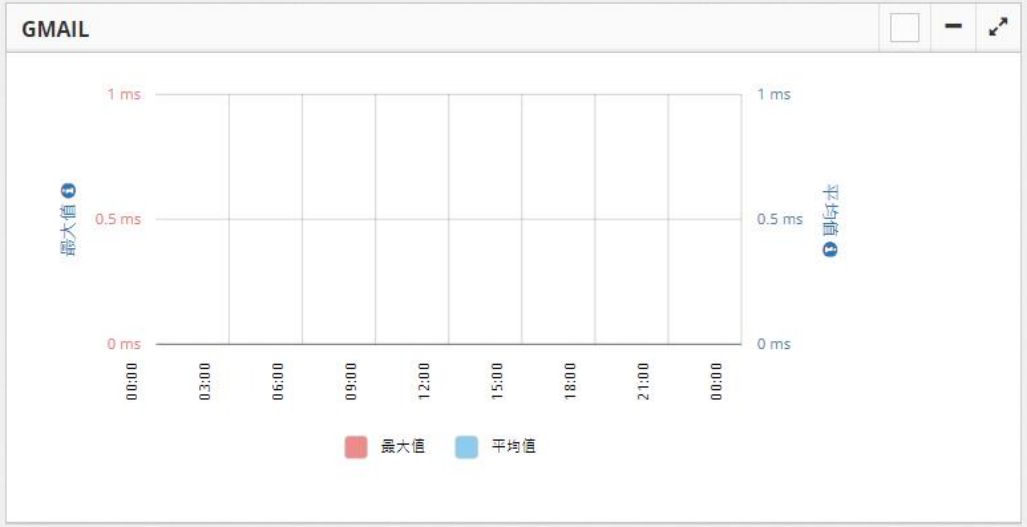
	最大	平均	目前
流入	155 Mbps (155%)	15.6 Mbps (15.6%)	678.21 kbps (0.68%)
流出	108.19 Mbps (108.19%)	6.65 Mbps (6.65%)	217.87 kbps (0.22%)

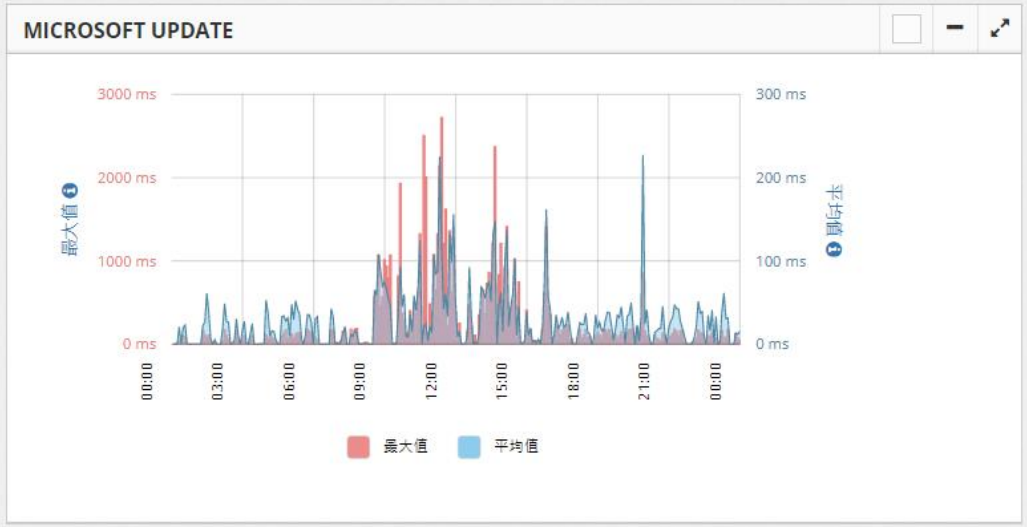
被動式網路服務品質分析(2)

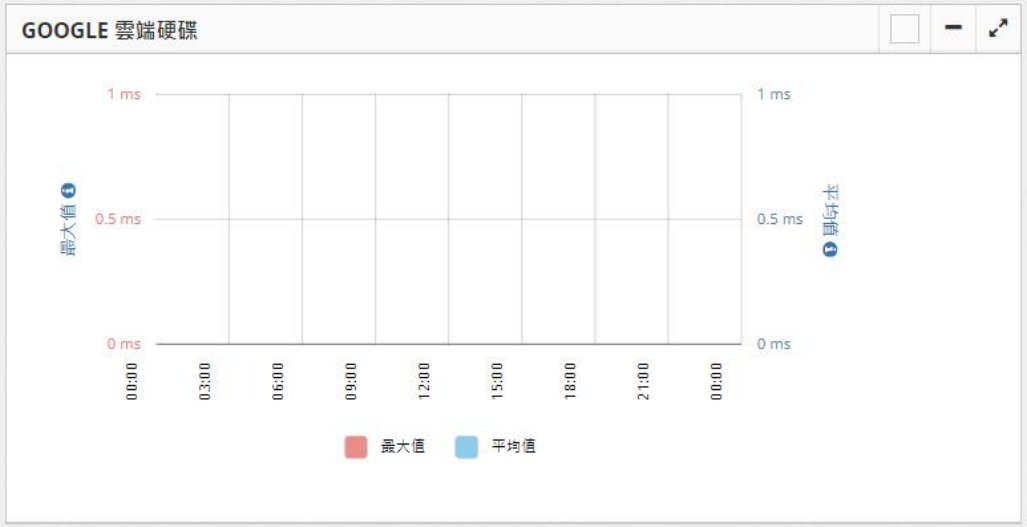
由實際網路流量分析上網服務狀況，無須產生額外偵測流量來監測。

2020-03-31 選擇圖表









監控與追蹤管理設備(3)

告警記錄

啟始： 2020-03-31 ~ 結束： 2020-04-02 告警類別： ALL 確認

明細紀錄 統計紀錄

所有

輸入關鍵字查詢

單位	時間	事件類別	告警內容
正義國小	2020-04-01 18:52:44	IP衝突	IP=10.241.184.194, 衝突MAC=80:EE:73:E6:5B:85，80:EE:73:E5:99:86
正義國小	2020-04-01 14:11:58	IP衝突	IP=10.228.184.152, 衝突MAC=00:CD:88:60:26:AD，00:CD:88:60:21:70
正義國小	2020-04-01 13:35:59	IP衝突	IP=10.241.184.57, 衝突MAC=74:27:EA:DA:2B:0B，00:23:24:D9:67:9B
正義國小	2020-04-01 13:25:36	IP衝突	IP=10.241.184.151, 衝突MAC=74:27:EA:DA:6E:F6，80:EE:73:E5:8F:CA
正義國小	2020-04-01 13:16:53	IP衝突	IP=10.241.184.119, 衝突MAC=74:27:EA:DA:6A:C1，00:23:24:D9:66:80
正義國小	2020-03-31 18:47:47	IP衝突	IP=10.241.184.194, 衝突MAC=80:EE:73:E5:99:86，80:EE:73:E6:5B:85
正義國小	2020-03-31 13:35:02	IP衝突	IP=10.241.184.57, 衝突MAC=00:23:24:D9:67:9B，74:27:EA:DA:2B:0B
正義國小	2020-03-31 13:30:00	IP衝突	IP=10.228.184.152, 衝突MAC=00:CD:88:60:21:70，00:CD:88:60:26:AD
正義國小	2020-03-31 13:13:53	IP衝突	IP=10.241.184.119, 衝突MAC=00:23:24:D9:66:80，74:27:EA:DA:6A:C1
正義國小	2020-03-31 13:13:52	IP衝突	IP=10.241.184.151, 衝突MAC=80:EE:73:E5:8F:CA，74:27:EA:DA:6E:F6
正義國小	2020-03-31 09:50:01	IP衝突	IP=10.228.184.152, 衝突MAC=00:CD:88:60:21:70，00:CD:88:60:26:AD
正義國小	2020-03-31 08:12:27	IP衝突	IP=10.241.184.119, 衝突MAC=74:27:EA:DA:6A:C1，00:23:24:D9:66:80
正義國小	2020-03-31 08:07:59	IP衝突	IP=10.241.184.151, 衝突MAC=80:EE:73:E5:8F:CA，74:27:EA:DA:6E:F6

顯示 (1 至 13)，共 13 筆資料

監控與追蹤管理設備(4)

說明：從Radar端 執行Ping測試指定IP的連線狀況。

IP： 163.20.85.2 Ping次數： 5 次 送出

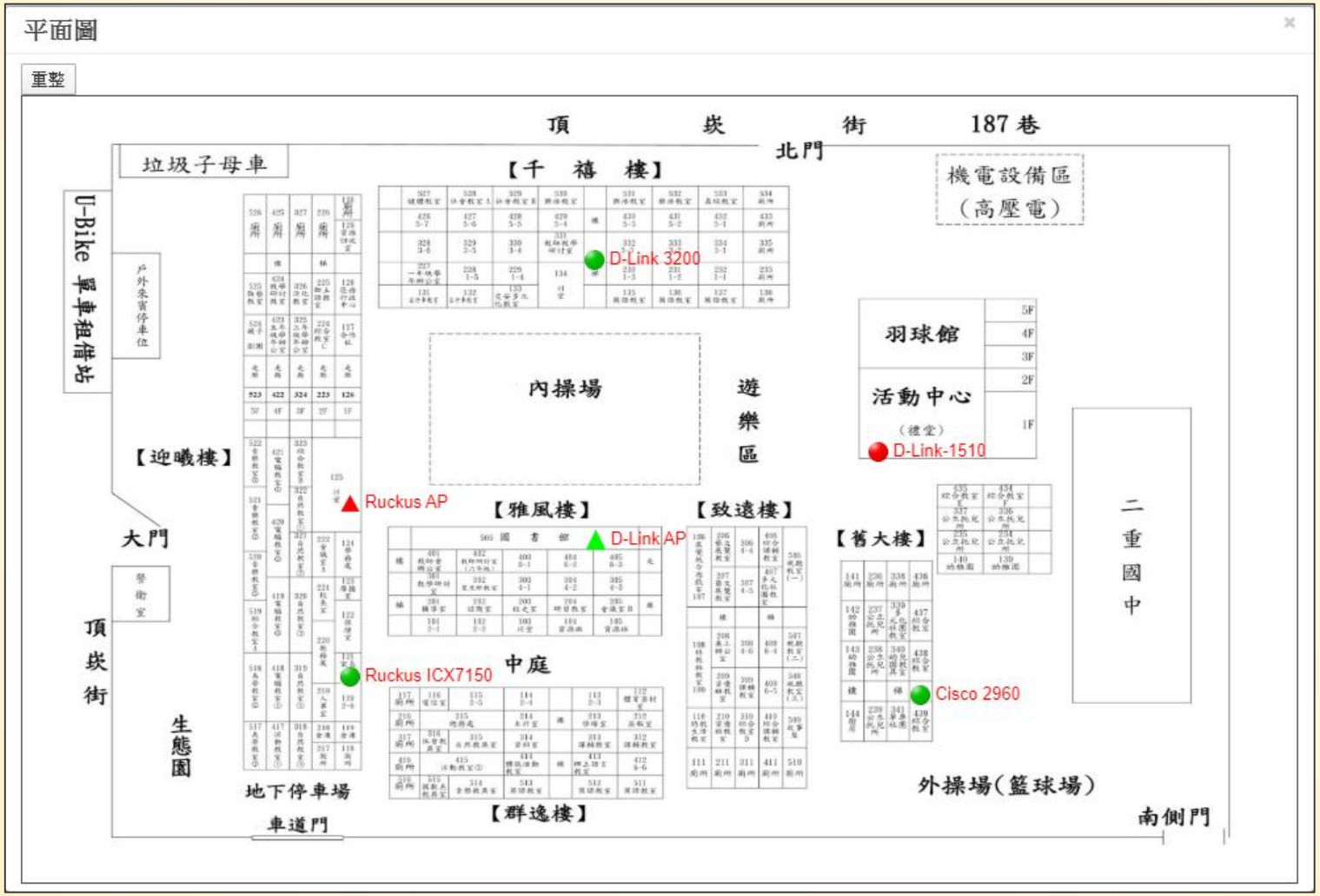
結果

```
PING 163.20.85.2 (163.20.85.2) 56(84) bytes of data.
64 bytes from 163.20.85.2: icmp_seq=1 ttl=127 time=0.689 ms
64 bytes from 163.20.85.2: icmp_seq=2 ttl=127 time=0.502 ms
64 bytes from 163.20.85.2: icmp_seq=3 ttl=127 time=0.559 ms
64 bytes from 163.20.85.2: icmp_seq=4 ttl=127 time=0.539 ms
64 bytes from 163.20.85.2: icmp_seq=5 ttl=127 time=0.767 ms

--- 163.20.85.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4187ms
rtt min/avg/max/mdev = 0.502/0.611/0.767/0.101 ms
```

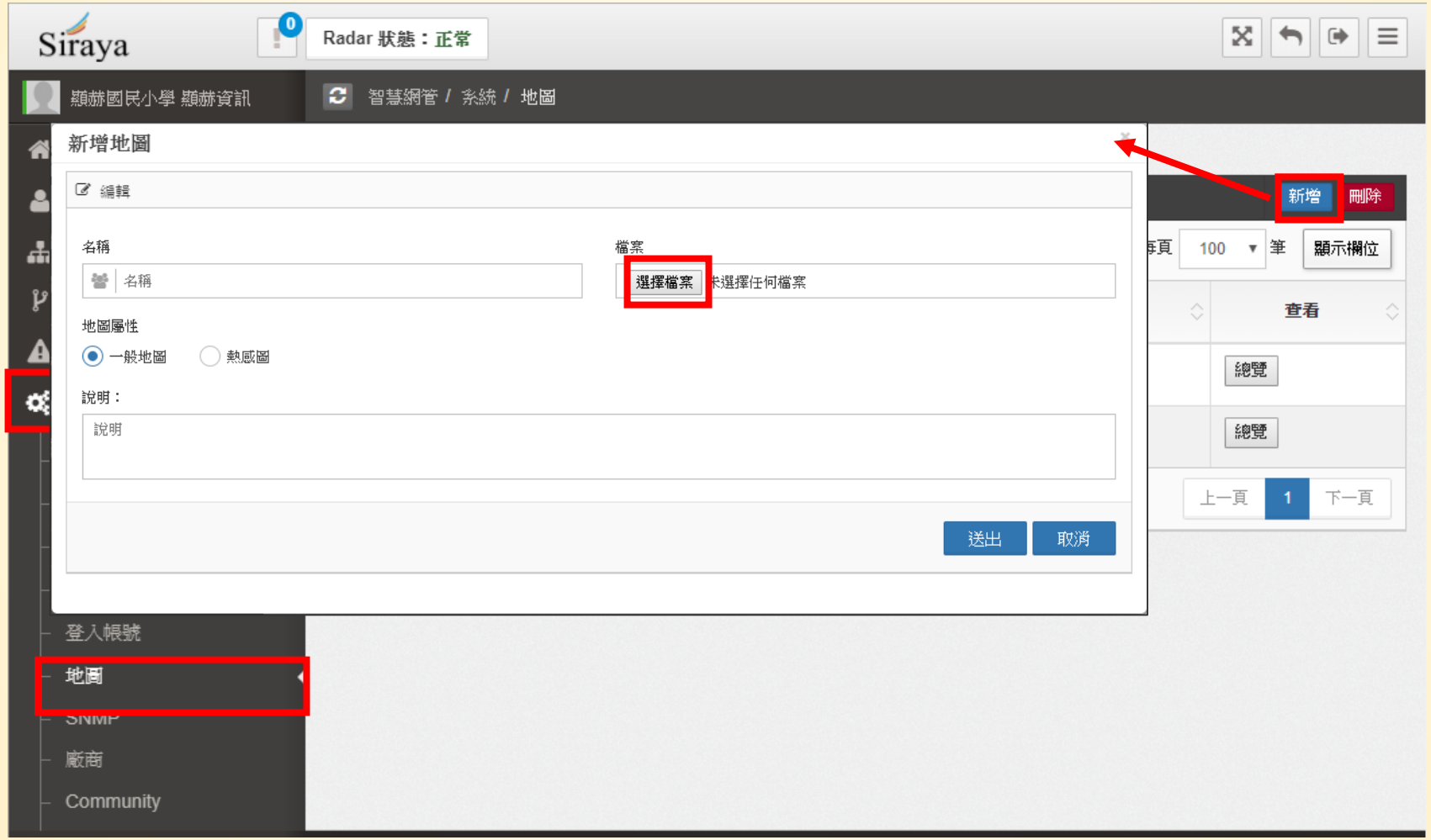
Map

設備顯示於平面圖上，清楚得知實際位置。



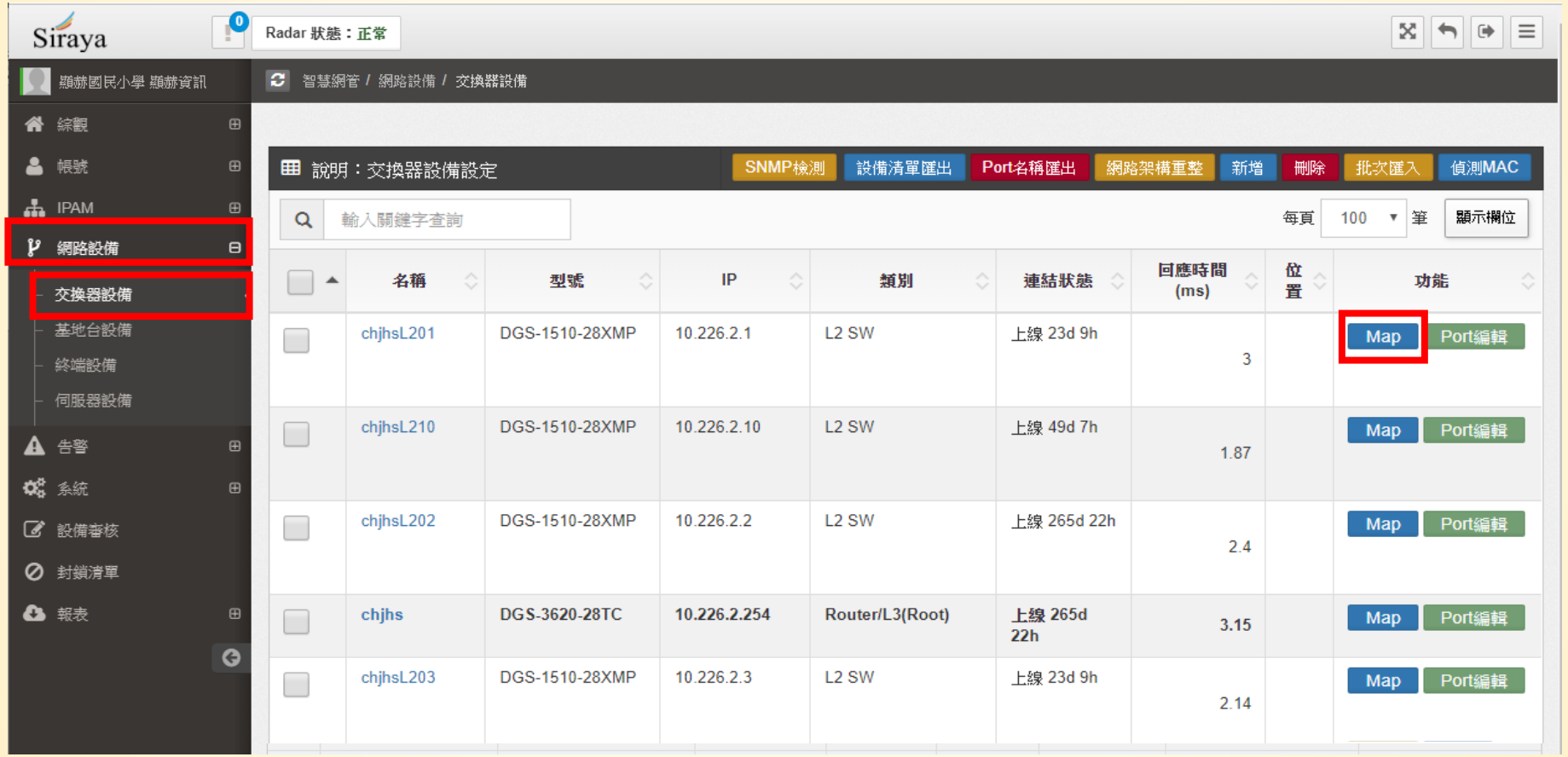
新增學校平面圖

系統➔地圖



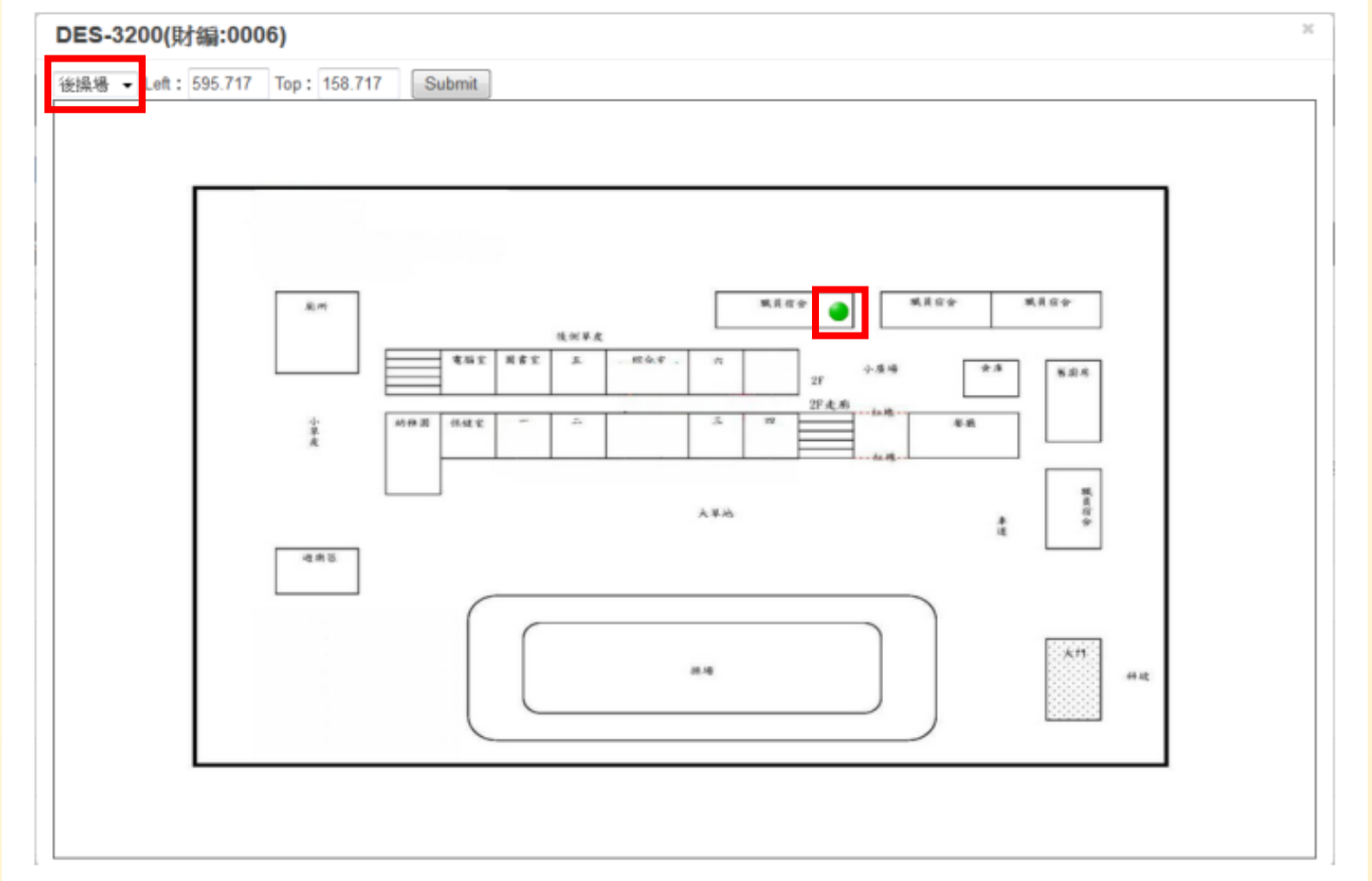
Map

如何定義設備位置?



Map

拖移設備至正確的平面圖上，已標示正確所在位置。



告警設定

系統相關告警設定方式

設備偵測

告警 ➔ 告警設定 ➔網路交換器

針對網路交換器進行**離線偵測、CPU 負載、Port 流量偵測**。

全域設定

告警 ➔ 告警設定 ➔IP/MAC

針對網路環境進行 **IP衝突、未知設備、非法IP** 偵測

全域設定

告警 ➔ 告警設定 ➔IP流量

對網段或是單一 IP 進行**IP流量**偵測

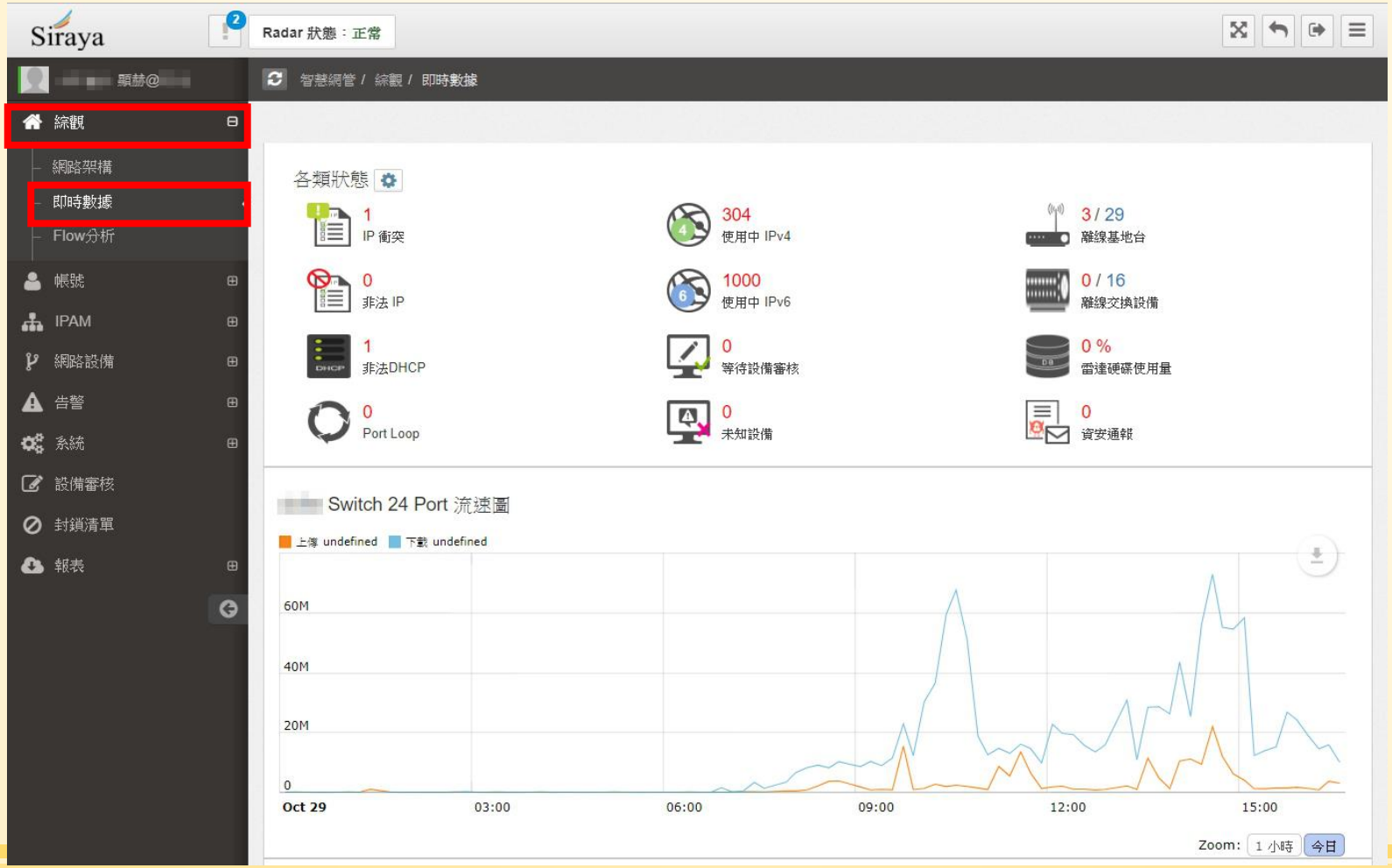
系統流量

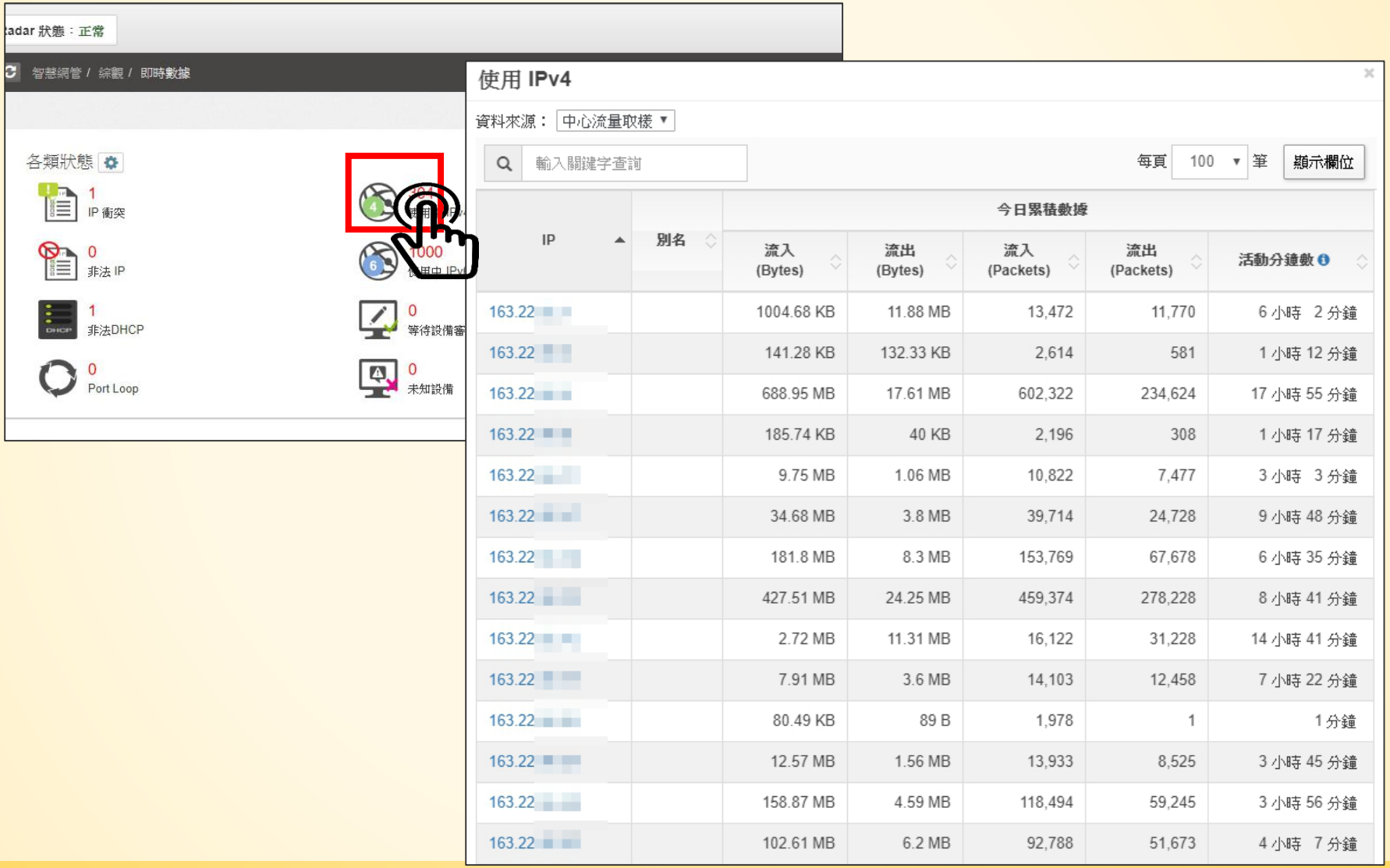
相關資訊說明

即時數據

綜觀 ➔ 即時數據

本區顯示眾多即時指標數據，管理者可在此查看目前系統監測狀態總覽，包含單位整理的流量資訊、交換器等設備偵測狀態、流量排名分析。

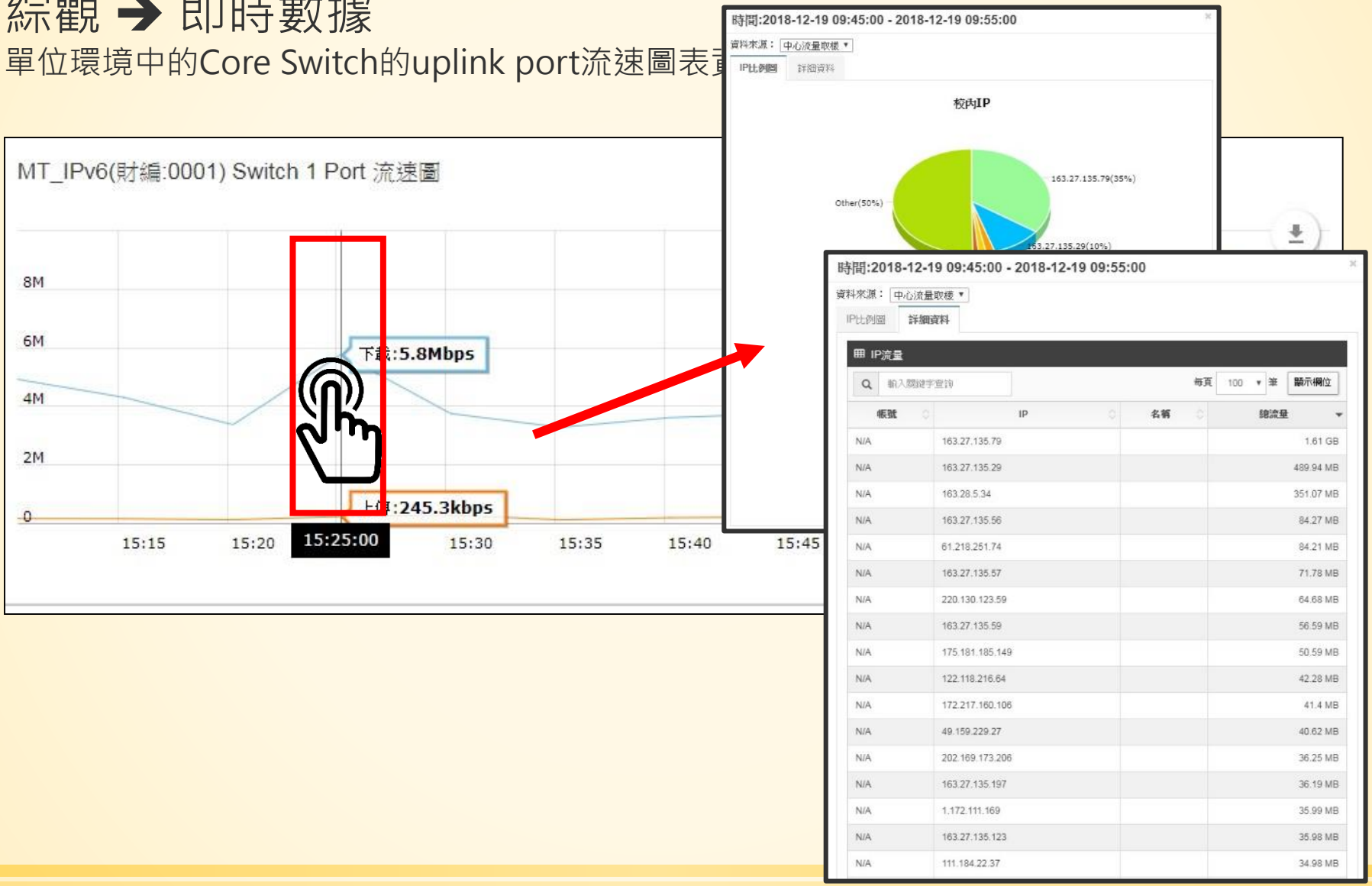



adar 狀態：正常
智慧網管 / 綜觀 / 即時數據
各類狀態
1
IP 衝突
0
非法 IP
1
非法DHCP
0
Port Loop
0
等待設備審
0
未知設備
使用 IPv4
資料來源：
中心流量取樣
輸入關鍵字查詢
每頁
100
筆
顯示欄位
今日累積數據
IP
別名
流入 (Bytes)
流出 (Bytes)
流入 (Packets)
流出 (Packets)
活動分鐘數
163.22 1004.68 KB 11.88 MB 13,472 11,770 6 小時 2 分鐘
163.22 141.28 KB 132.33 KB 2,614 581 1 小時 12 分鐘
163.22 688.95 MB 17.61 MB 602,322 234,624 17 小時 55 分鐘
163.22 185.74 KB 40 KB 2,196 308 1 小時 17 分鐘
163.22 9.75 MB 1.06 MB 10,822 7,477 3 小時 3 分鐘
163.22 34.68 MB 3.8 MB 39,714 24,728 9 小時 48 分鐘
163.22 181.8 MB 8.3 MB 153,769 67,678 6 小時 35 分鐘
163.22 427.51 MB 24.25 MB 459,374 278,228 8 小時 41 分鐘
163.22 2.72 MB 11.31 MB 16,122 31,228 14 小時 41 分鐘
163.22 7.91 MB 3.6 MB 14,103 12,458 7 小時 22 分鐘
163.22 80.49 KB 89 B 1,978 1 1 分鐘
163.22 12.57 MB 1.56 MB 13,933 8,525 3 小時 45 分鐘
163.22 158.87 MB 4.59 MB 118,494 59,245 3 小時 56 分鐘
163.22 102.61 MB 6.2 MB 92,788 51,673 4 小時 7 分鐘

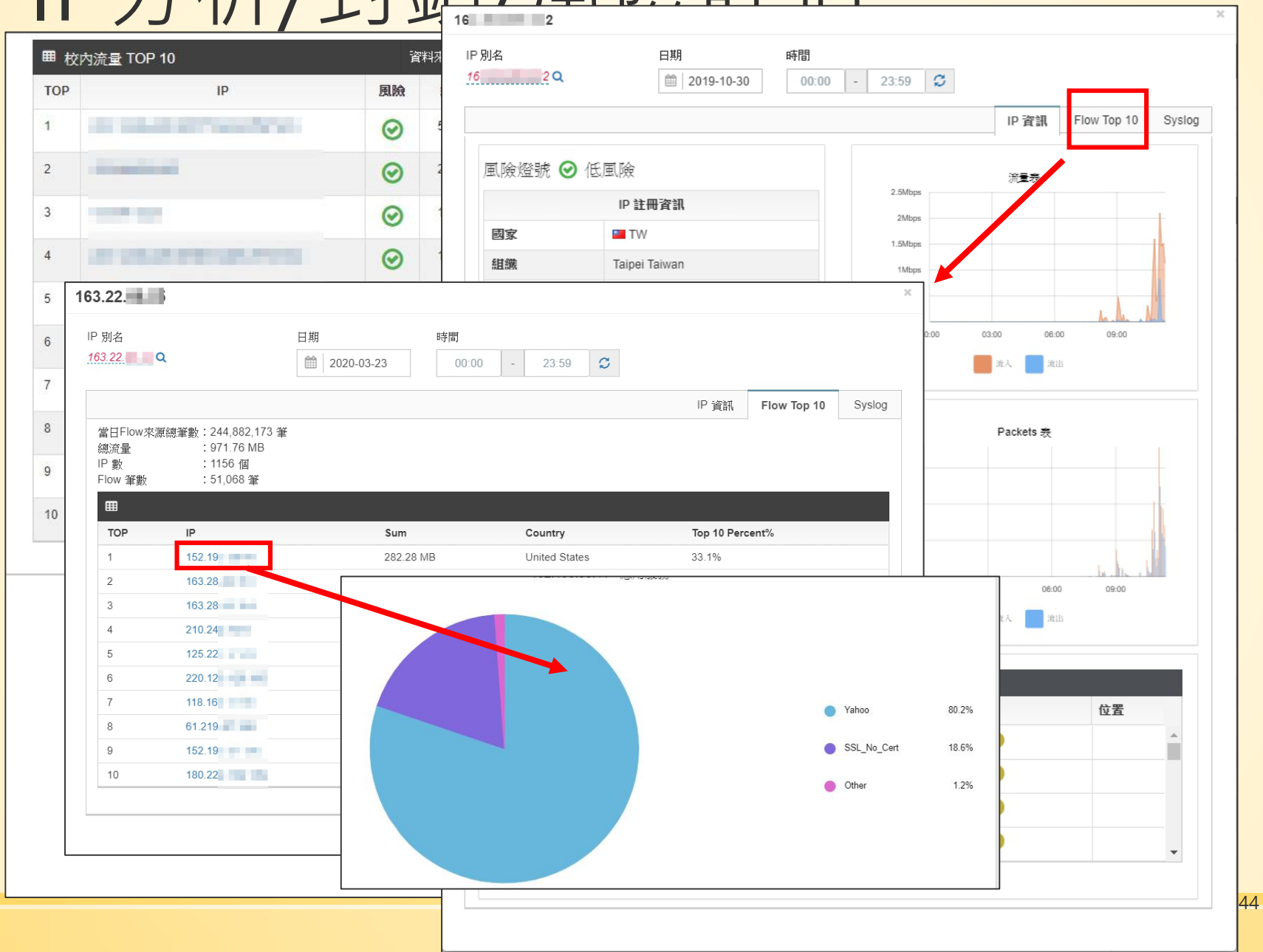
即時數據

綜觀 ➔ 即時數據

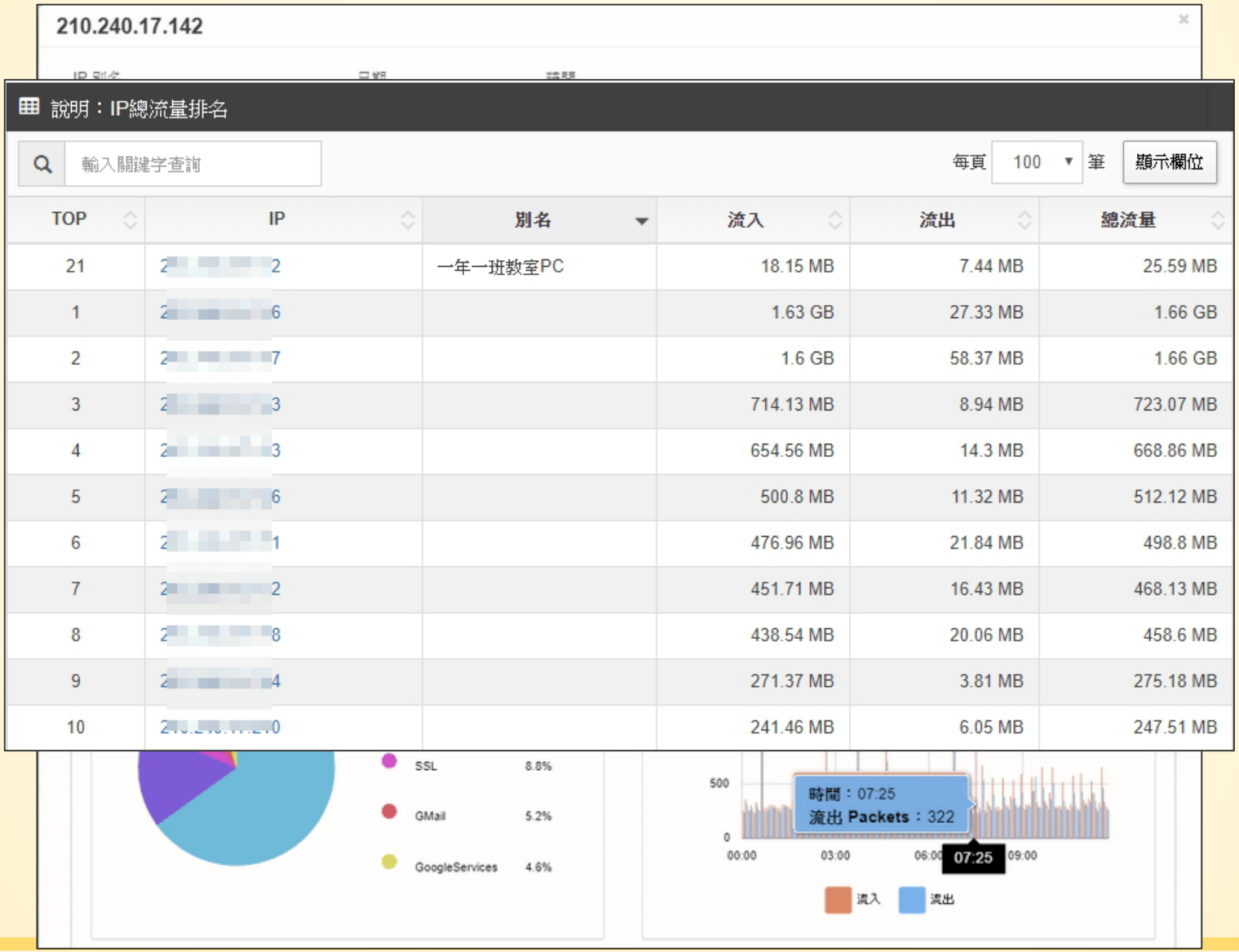
單位環境中的Core Switch的uplink port流速圖表



IP分析/封鎖/風險評估

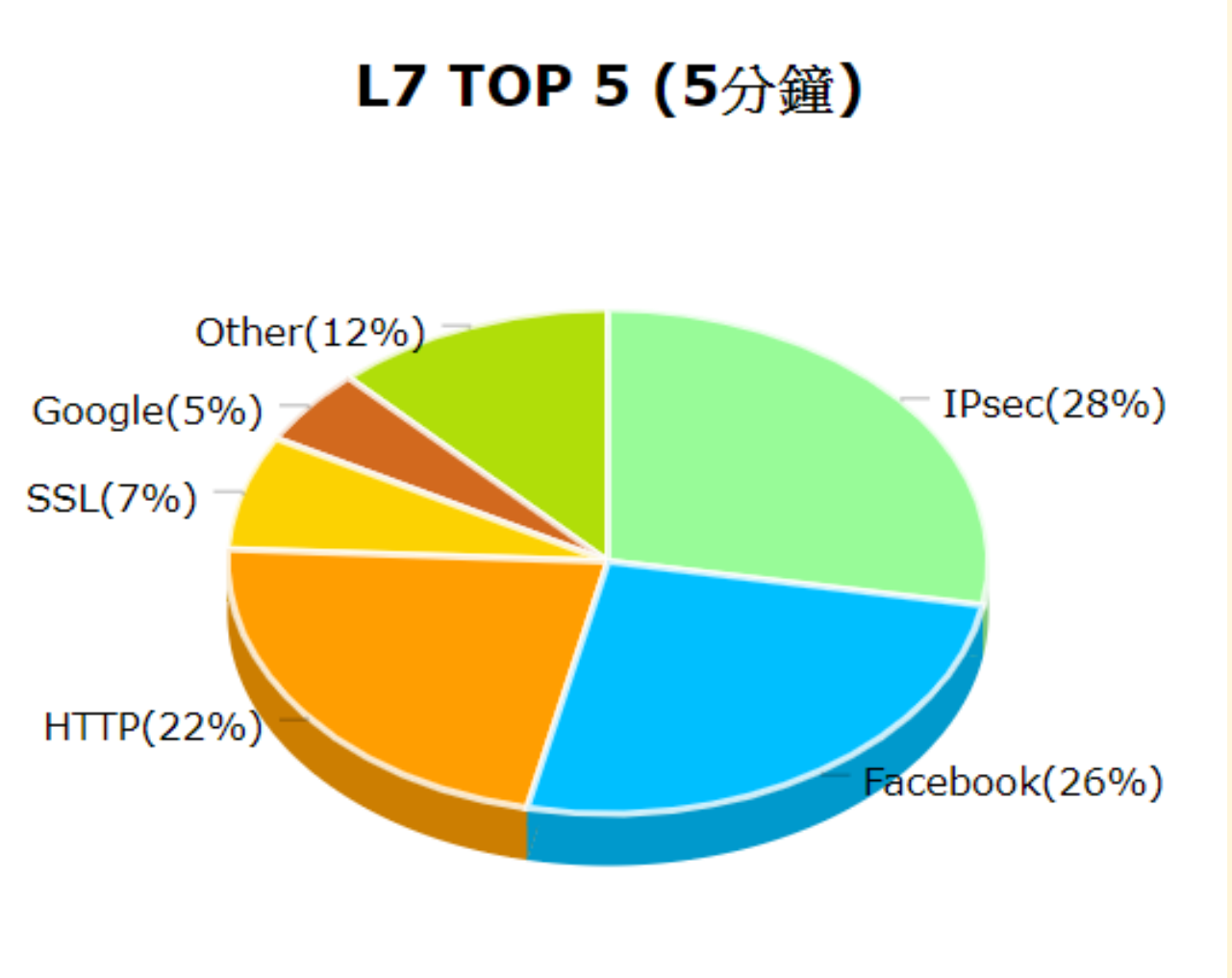

校內流量 TOP 10
TOP
IP
風險
IP 別名
日期
2019-10-30
時間
00:00
23:59
IP 資訊
Flow Top 10
Syslog
風險燈號
低風險
IP 註冊資訊
國家
TW
組織
Taipei Taiwan
流量表
2.5Mbps
2Mbps
1.5Mbps
1Mbps
163.22.
2020-03-23
當日Flow來源總筆數：244,882,173 筆
總流量 ：971.76 MB
IP 數 ：1156 個
Flow 筆數 ：51,068 筆
Sum
Country
Top 10 Percent%
1 152.19 282.28 MB United States 33.1%
2 163.28
3 163.28
4 210.24
5 125.22
6 220.12
7 118.16
8 61.219
9 152.19
10 180.22
Packets 表
位置
Yahoo 80.2%
SSL_No_Cert 18.6%
Other 1.2%

IP別名


210.240.17.142
說明：IP總流量排名
輸入關鍵字查詢
每頁 100 筆
顯示欄位
TOP
IP
別名
流入
流出
總流量
21 2 2 一年一班教室PC 18.15 MB 7.44 MB 25.59 MB
1 2 6 1.63 GB 27.33 MB 1.66 GB
2 2 7 1.6 GB 58.37 MB 1.66 GB
3 2 3 714.13 MB 8.94 MB 723.07 MB
4 2 3 654.56 MB 14.3 MB 668.86 MB
5 2 6 500.8 MB 11.32 MB 512.12 MB
6 2 1 476.96 MB 21.84 MB 498.8 MB
7 2 2 451.71 MB 16.43 MB 468.13 MB
8 2 8 438.54 MB 20.06 MB 458.6 MB
9 2 4 271.37 MB 3.81 MB 275.18 MB
10 241.46 MB 6.05 MB 247.51 MB
SSL 8.8%
GMail 5.2%
GoogleServices 4.6%
500
0
時間：07:25
流出 Packets：322
00:00
03:00
06:00
07:25
09:00
流入
流出

第七層前五名分析

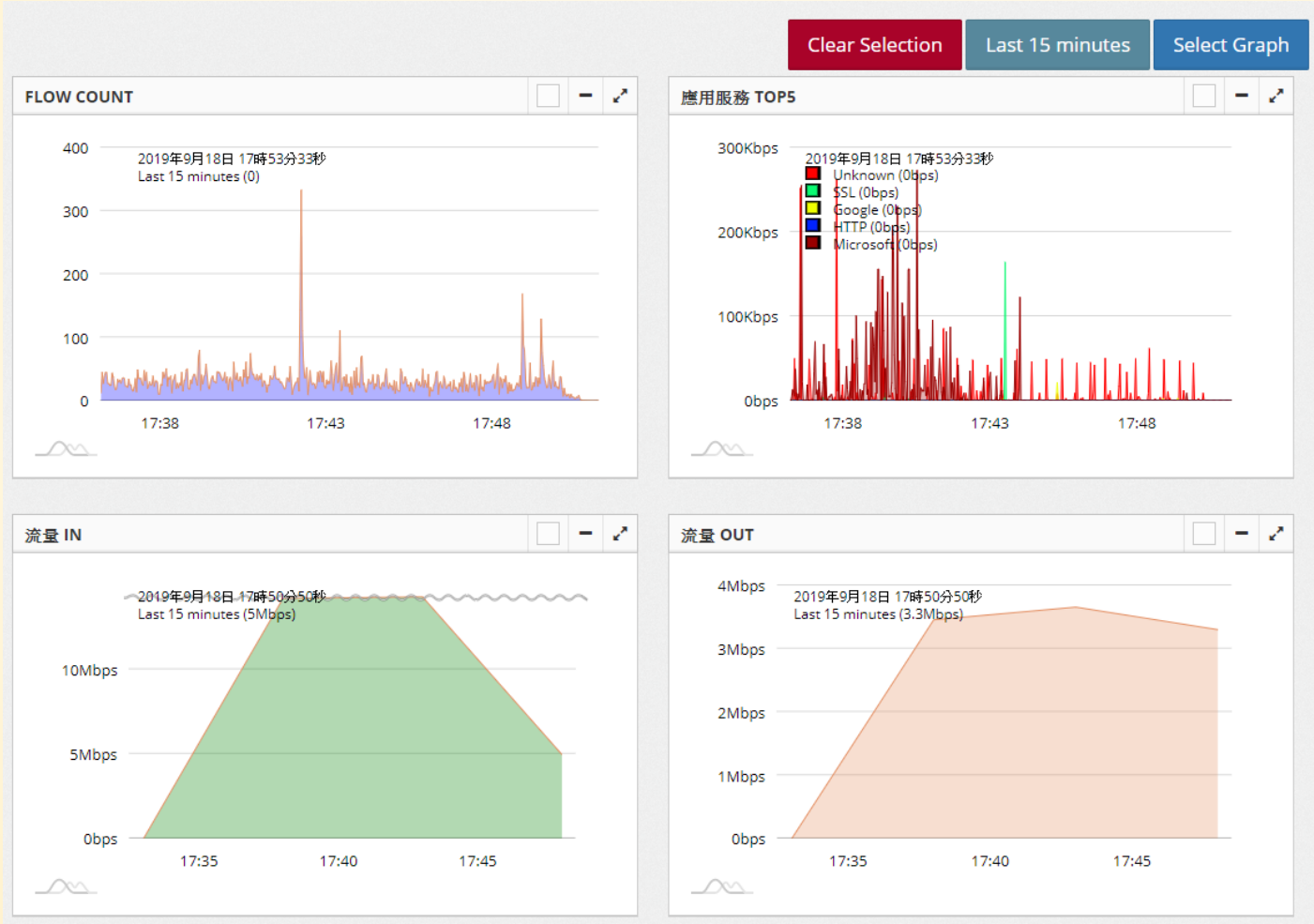
第七層服務前五名分析，針對整體流量進行第七層分析，並以圓餅圖呈現。



Flow分析

綜觀 ➔ Flow分析

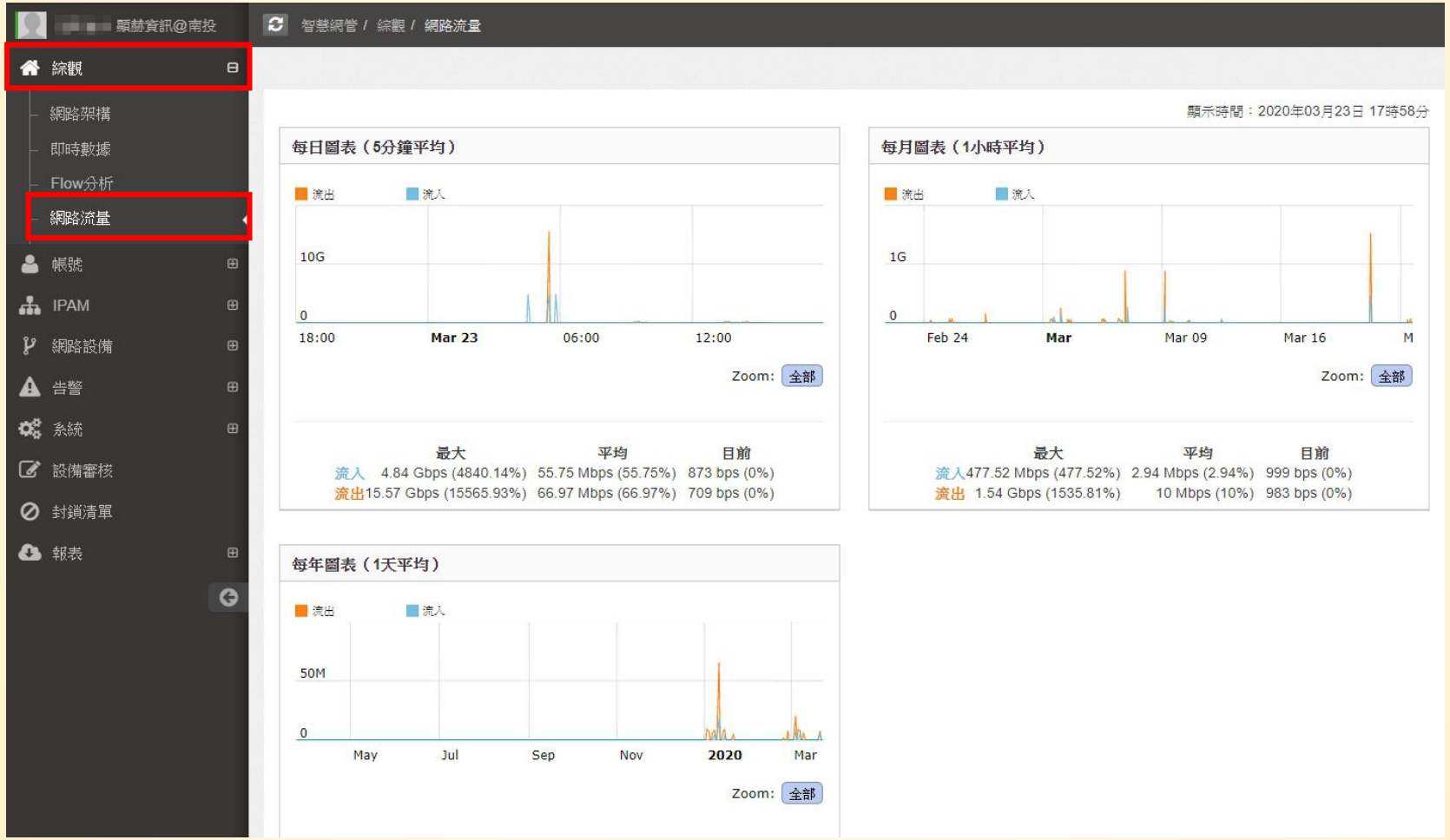
本校IP流量圖表分析總覽/流量資訊排名/圖表式佔比，圖表可作區間放大。



網路流量

綜觀 ➔ 網路流量

本區顯示L3 up link port的流量圖表(日/月/年)。



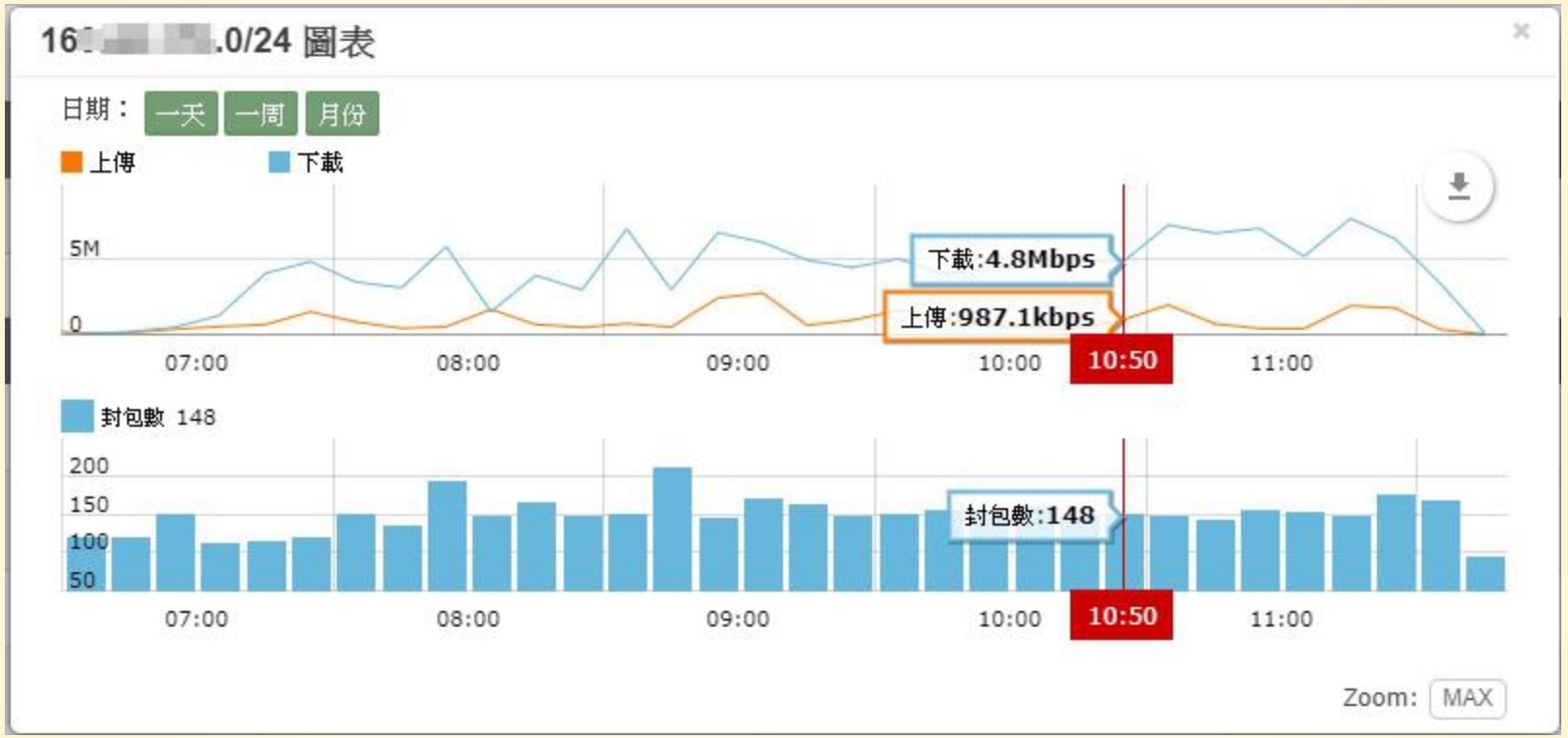
IPAM

IPAM ➔ 網段使用狀況

目前已納管至單位內的網段於此管理檢視。

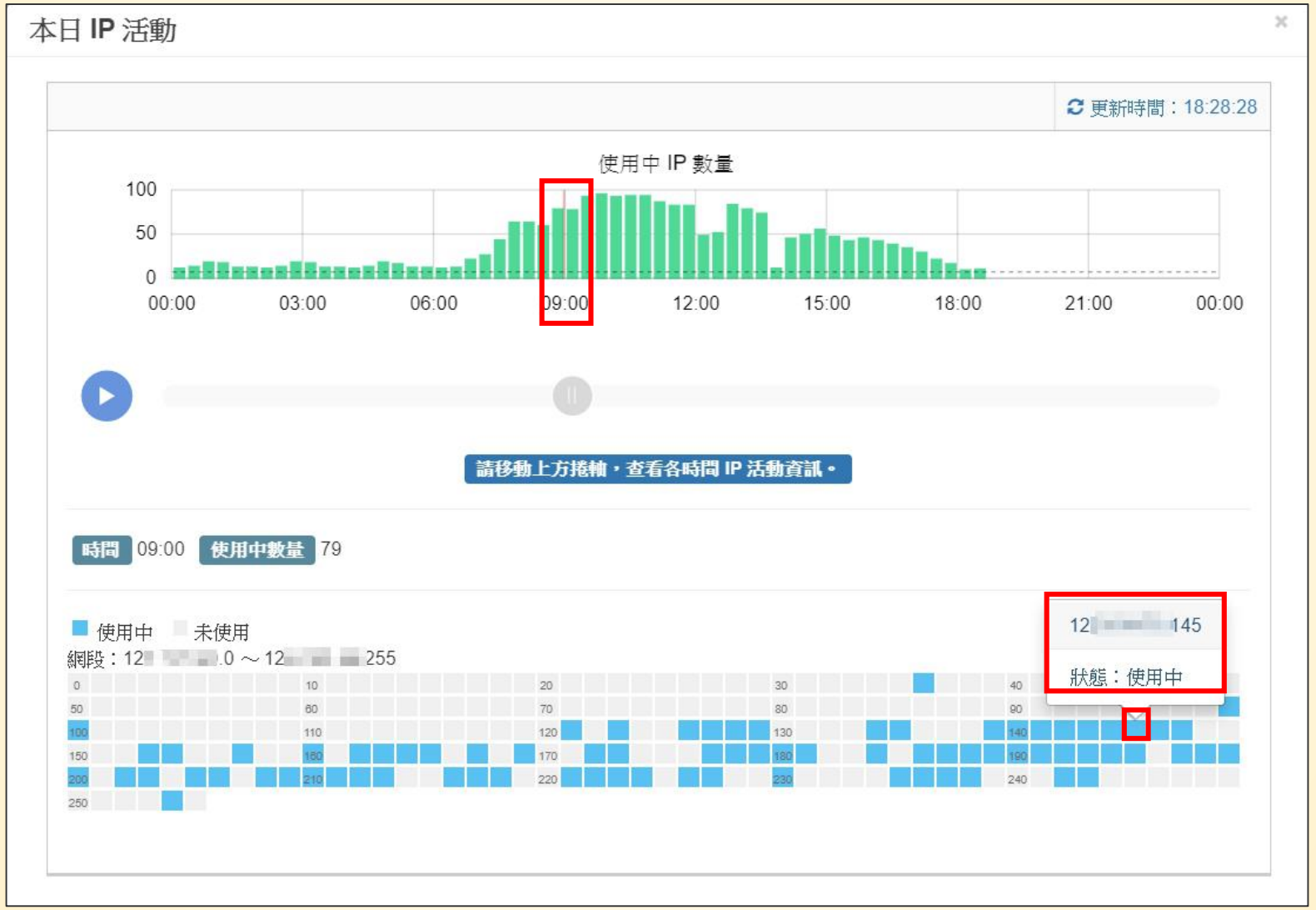
IPAM

網段流量圖表


16[redacted].0/24 圖表
日期：
一天
一周
月份
上傳
下載
5M
0
下載:4.8Mbps
上傳:987.1kbps
07:00
08:00
09:00
10:00
10:50
11:00
封包數 148
200
150
100
50
封包數:148
07:00
08:00
09:00
10:00
10:50
11:00
Zoom:
MAX

IPAM

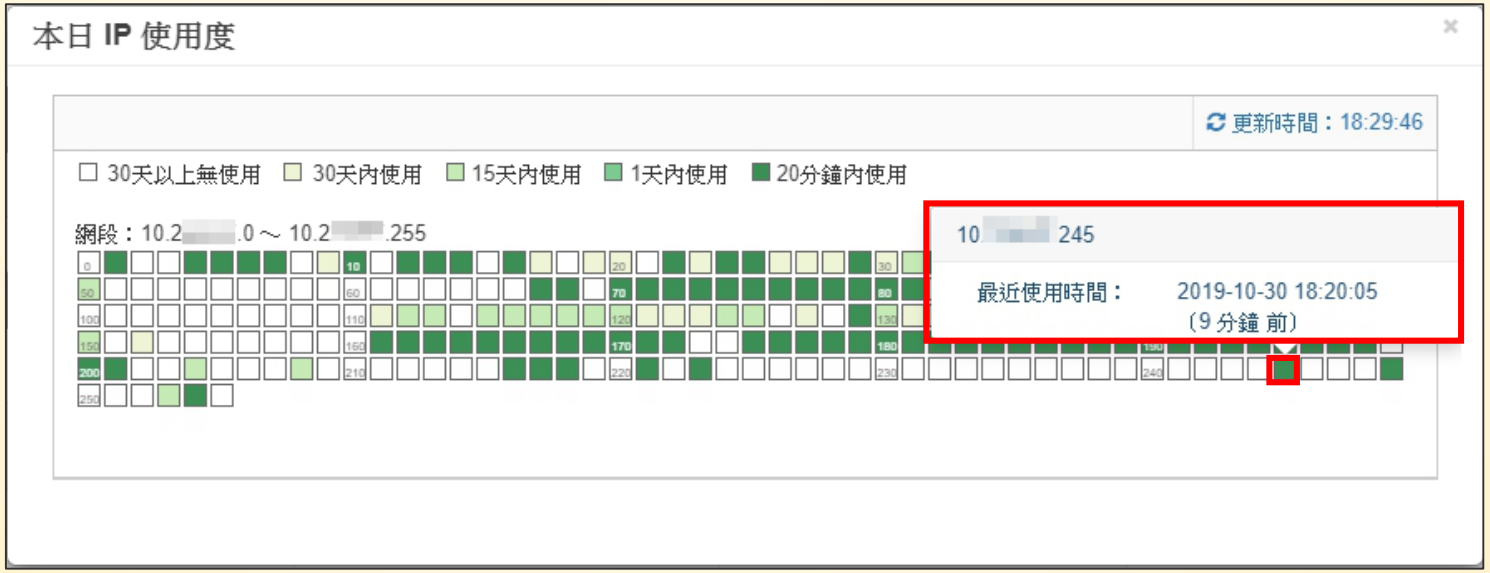
本日IP活動


本日 IP 活動
更新時間：18:28:28
使用中 IP 數量
100
50
0
00:00
03:00
06:00
09:00
12:00
15:00
18:00
21:00
00:00
請移動上方捲軸，查看各時間 IP 活動資訊。
時間 09:00
使用中數量 79
使用中
未使用
網段：12 .0 ～ 12 255
12 145
狀態：使用中

可用 IP？

臨時找不到可用 IP，可於系統查找一個月內未使用的 IP，來使用。

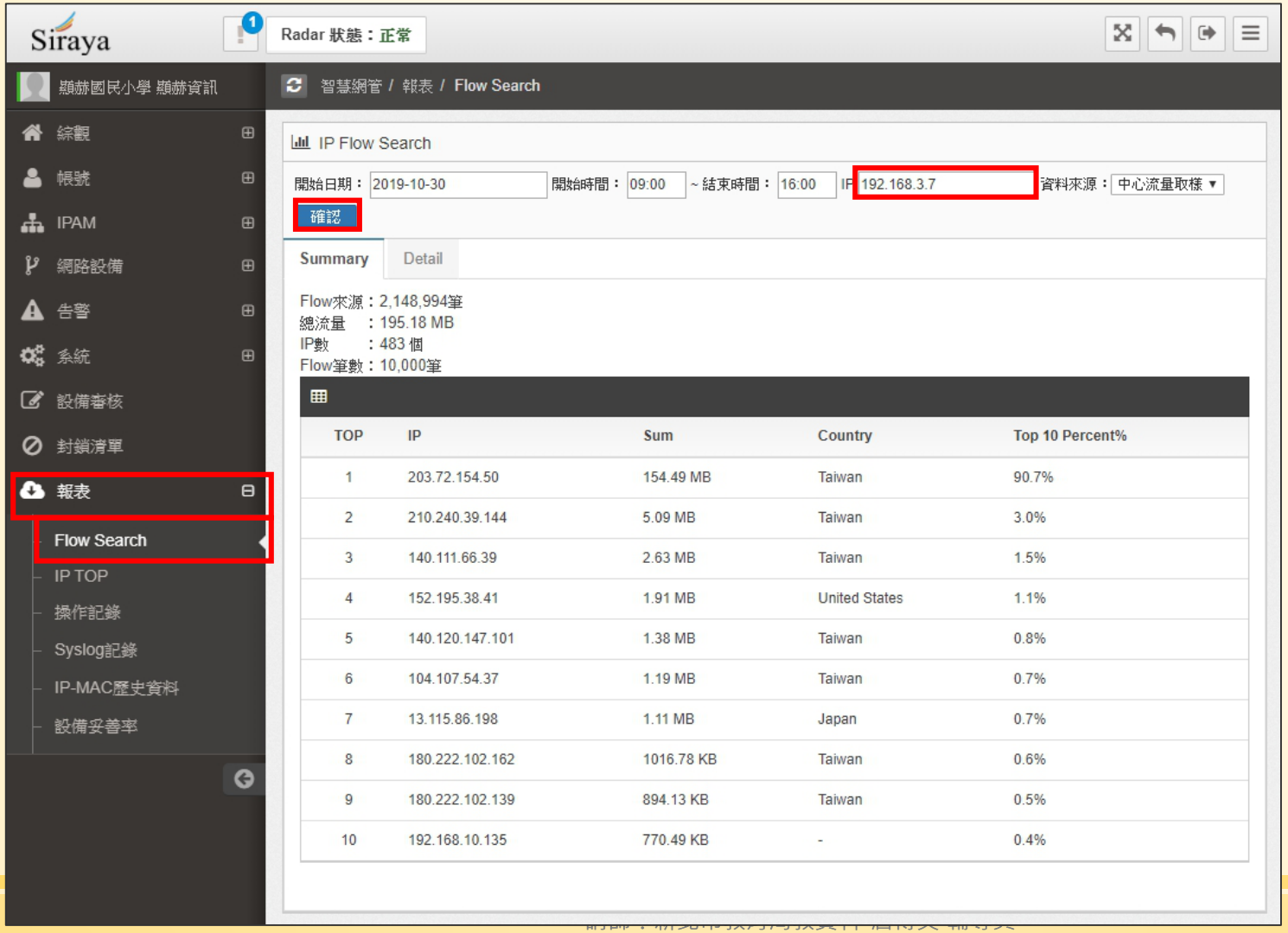
IP 未妥善紀錄
臨時也不知道哪一組可以使用?



報表

報表➔ FlowSearch

可於此搜尋整個系統內存的IP資訊。

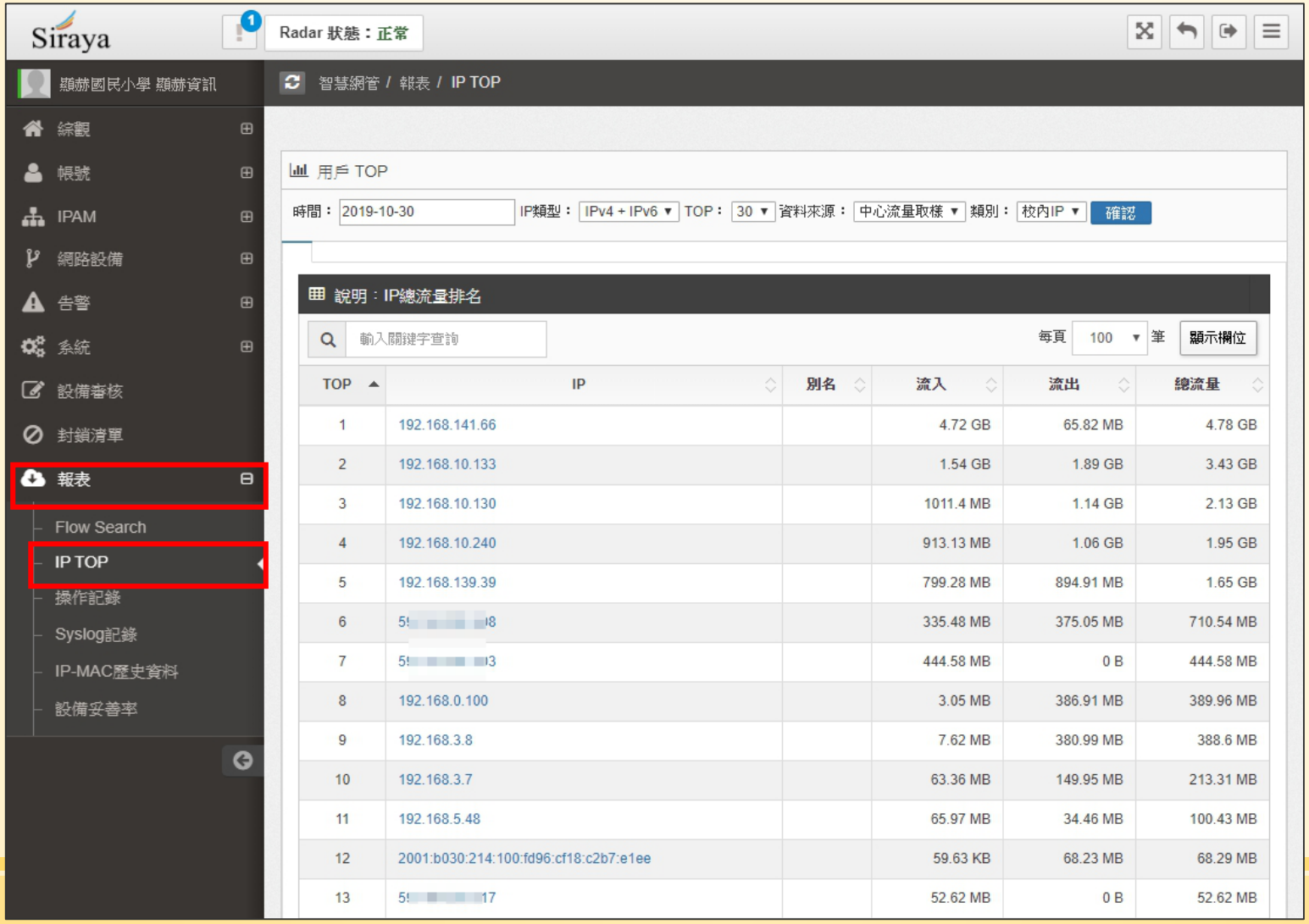


TOP	IP	Sum	Country	Top 10 Percent%
1	203.72.154.50	154.49 MB	Taiwan	90.7%
2	210.240.39.144	5.09 MB	Taiwan	3.0%
3	140.111.66.39	2.63 MB	Taiwan	1.5%
4	152.195.38.41	1.91 MB	United States	1.1%
5	140.120.147.101	1.38 MB	Taiwan	0.8%
6	104.107.54.37	1.19 MB	Taiwan	0.7%
7	13.115.86.198	1.11 MB	Japan	0.7%
8	180.222.102.162	1016.78 KB	Taiwan	0.6%
9	180.222.102.139	894.13 KB	Taiwan	0.5%
10	192.168.10.135	770.49 KB	-	0.4%

IP TOP

報表➔ IP TOP

單位內的IP使用流量排行榜。



TOP	IP	別名	流入	流出	總流量
1	192.168.141.66		4.72 GB	65.82 MB	4.78 GB
2	192.168.10.133		1.54 GB	1.89 GB	3.43 GB
3	192.168.10.130		1011.4 MB	1.14 GB	2.13 GB
4	192.168.10.240		913.13 MB	1.06 GB	1.95 GB
5	192.168.139.39		799.28 MB	894.91 MB	1.65 GB
6	5[redacted]8		335.48 MB	375.05 MB	710.54 MB
7	5[redacted]3		444.58 MB	0 B	444.58 MB
8	192.168.0.100		3.05 MB	386.91 MB	389.96 MB
9	192.168.3.8		7.62 MB	380.99 MB	388.6 MB
10	192.168.3.7		63.36 MB	149.95 MB	213.31 MB
11	192.168.5.48		65.97 MB	34.46 MB	100.43 MB
12	2001:b030:214:100:fd96:cf18:c2b7:e1ee		59.63 KB	68.23 MB	68.29 MB
13	5[redacted]17		52.62 MB	0 B	52.62 MB

IP 資訊

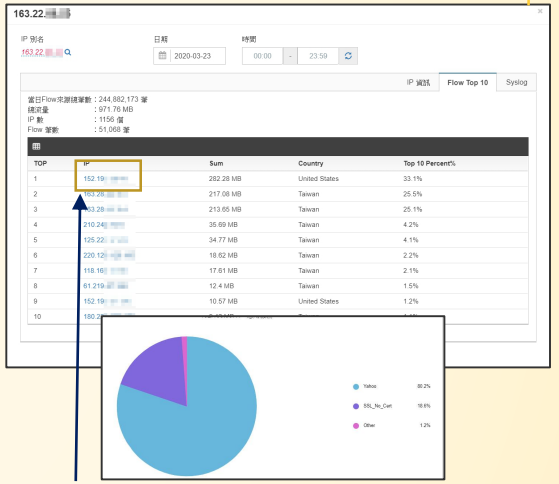
針對單一 IP 分析資料，更可以進階drill down找出與此IP有連線紀錄的Top10 IP。

判斷IP危險程度

IP第七層分析

IP MAC
位於交換器埠

進階 drill down 分析關聯IP
IP 流量圖表

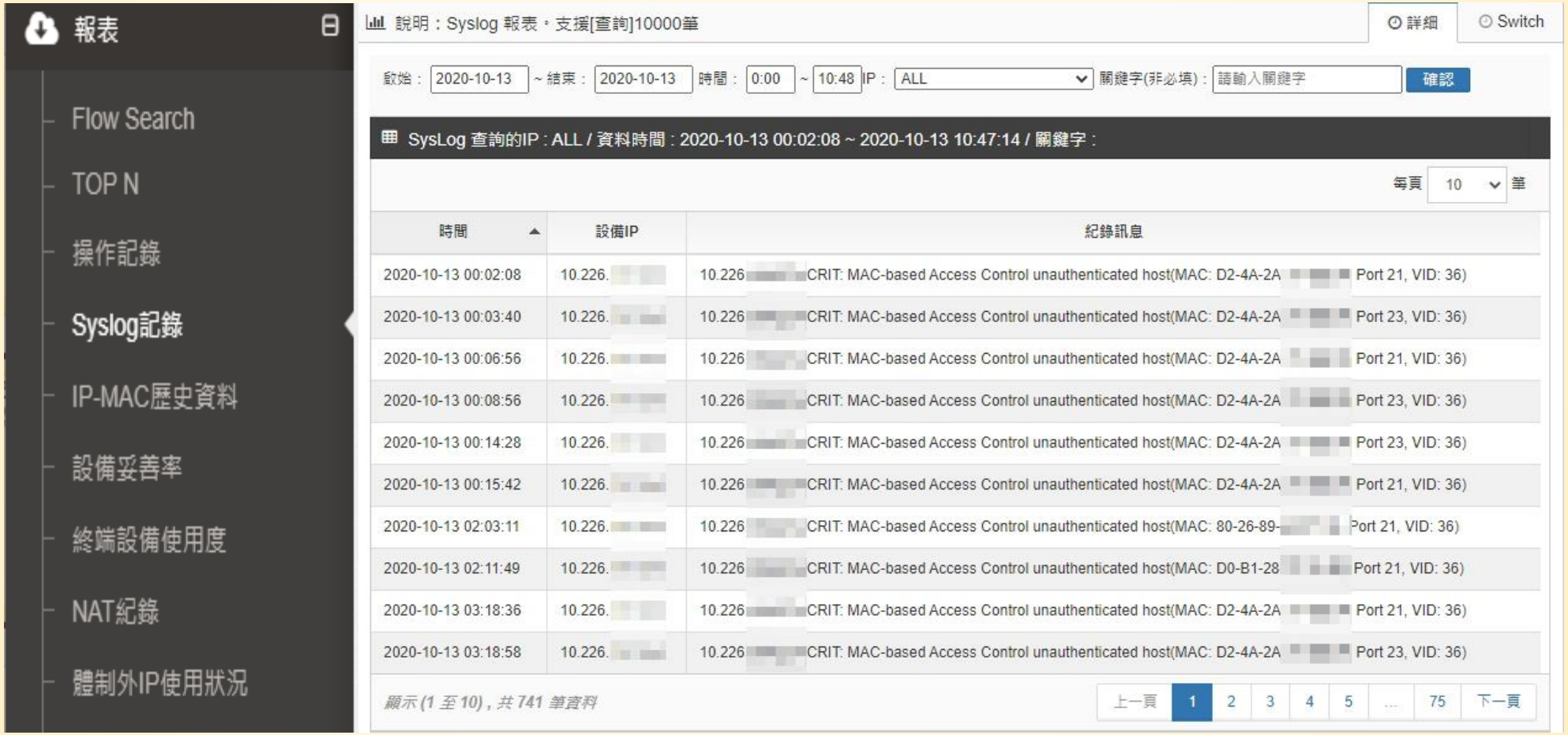


與此關連 IP 第七層分析

Syslog紀錄

報表 ➔Syslog紀錄

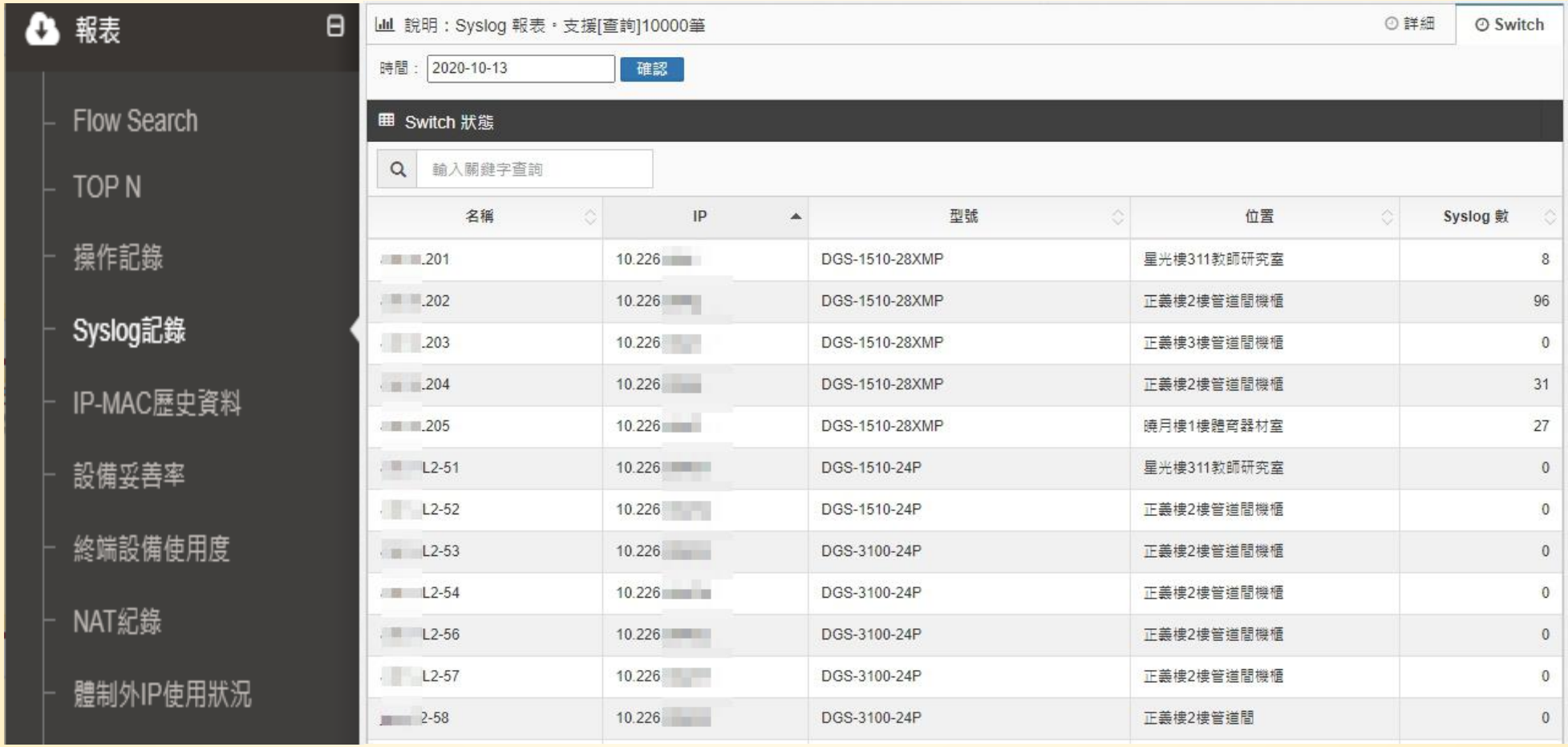
交換器先將syslog往學校的智慧網管閘道器，於系統呈現給管理者查看。



Syslog紀錄

報表 ➔Syslog紀錄

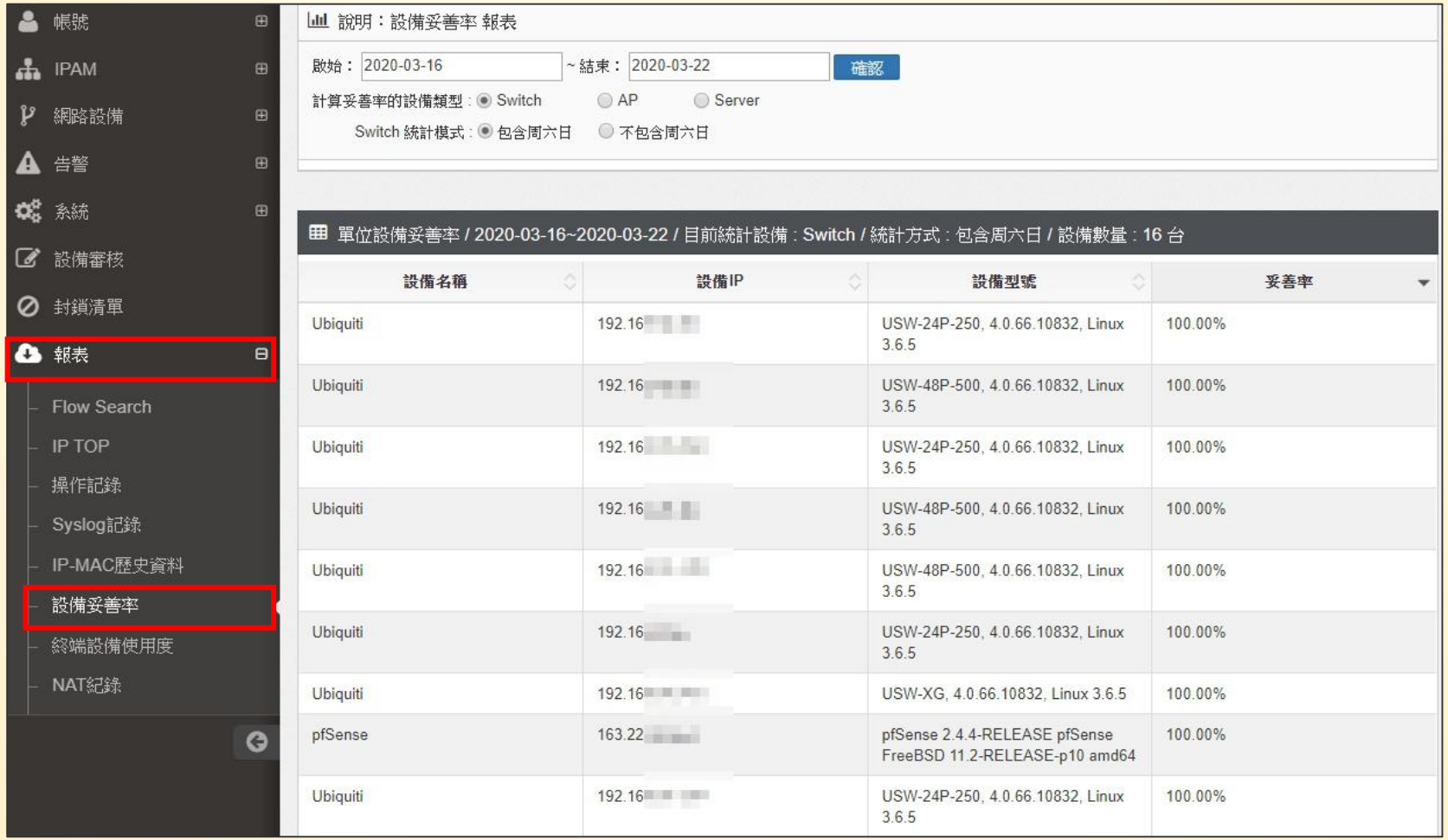
交換器先將syslog往學校的智慧網管閘道器，於系統呈現給管理者查看。



設備妥善率

報表 ➔設備妥善率

透過智慧網管去偵測設備，來反應設備妥善率。



終端設備使用度

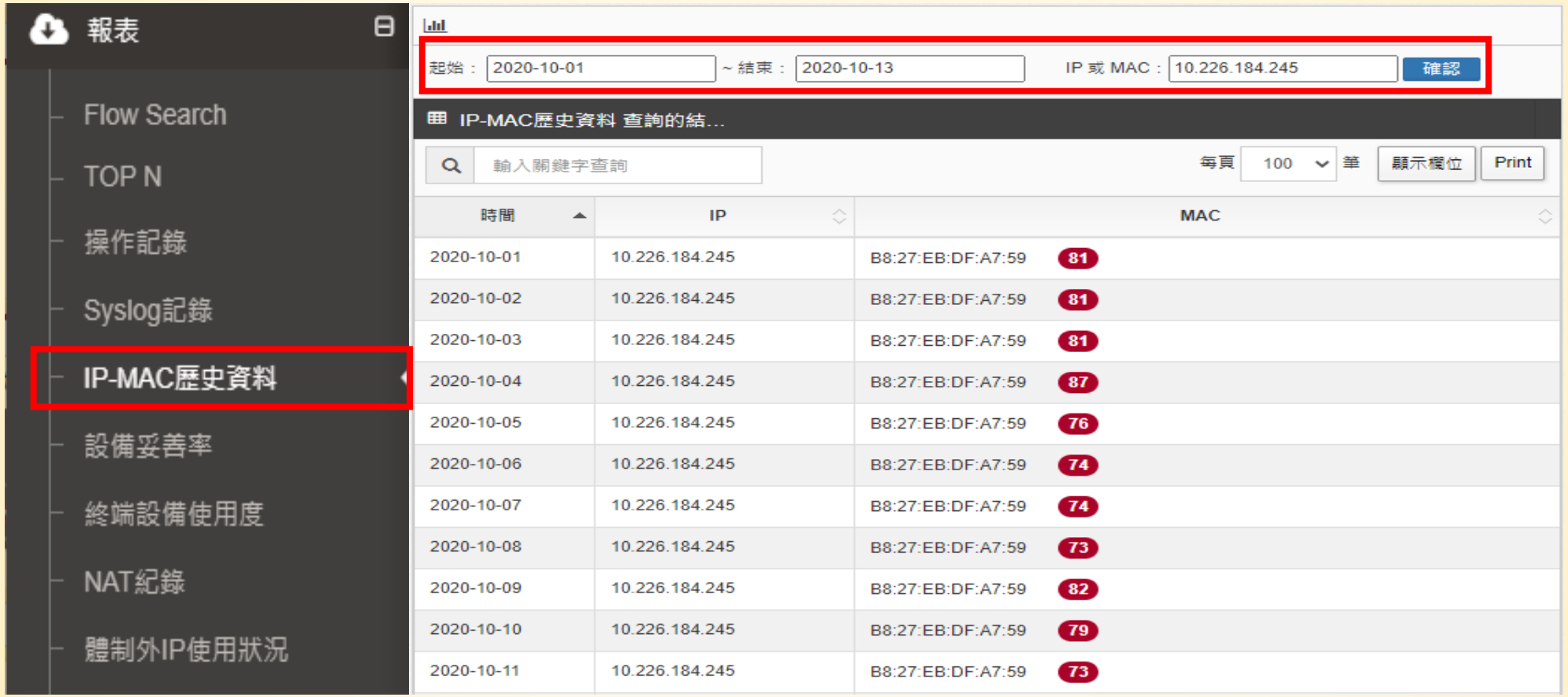
報表 ➔終端設備使用度

透過智慧網管去偵測設備，自定義天數來查找近期未上線的終端設備。

IP-MAC歷史資料

報表 ➔ IP-MAC歷史資料

自定義時間區間，想查找的IP或MAC，進行資料搜尋。



服務偵測

系統 ➔工具 ➔ 服務偵測

透過智慧網管去抓取偵測對象流量，來反應該服務的速度。

Q&A時間

如有任何建議，請踴躍提出

謝謝聆聽