Siraya

智慧網管
教育訓練

V2.4

主講人：陳亦詞

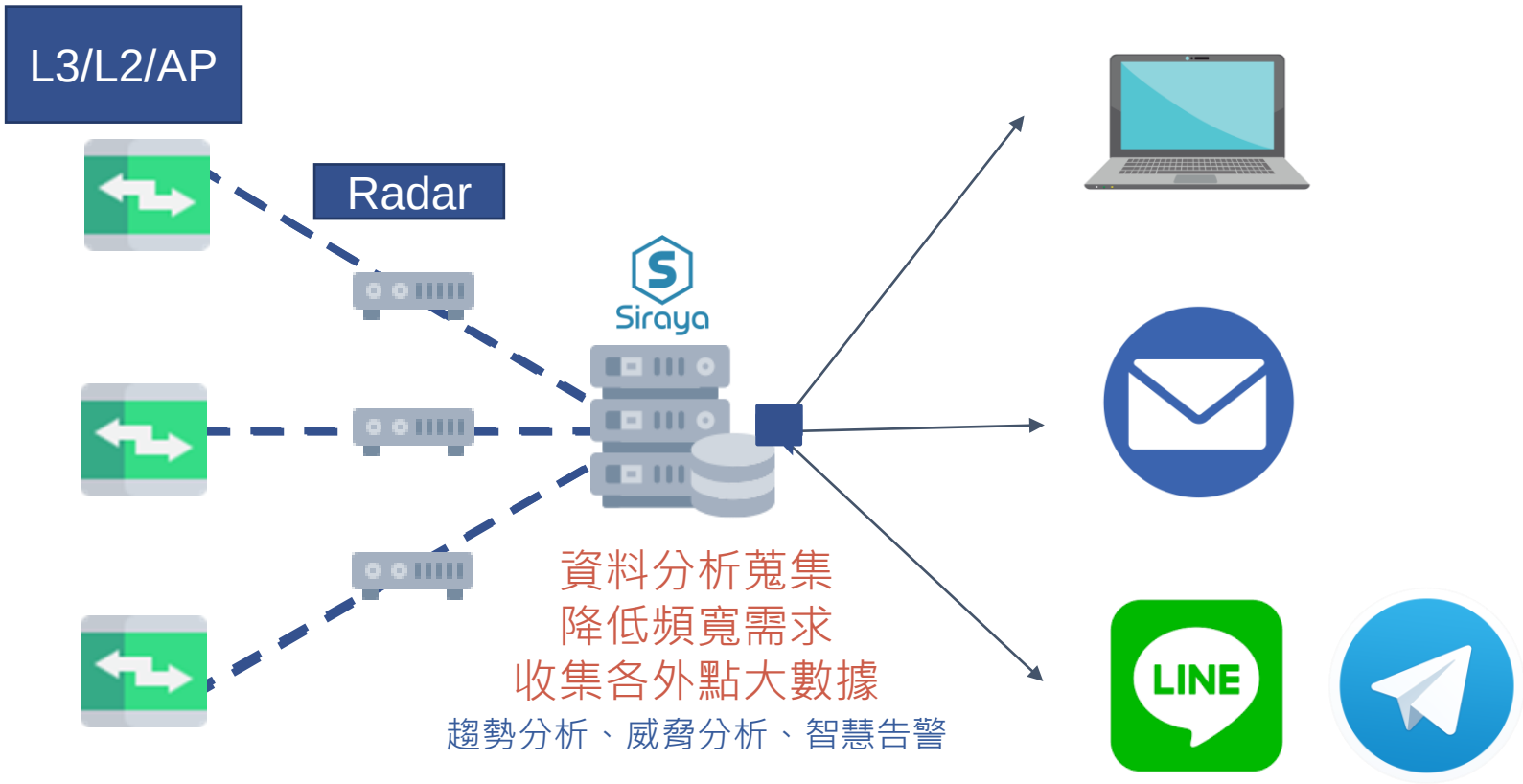
課程主題

一、Siraya 智慧網管說明

二、 實機演練

三、QA時間

資料收集


L3/L2/AP
Radar
Siraya
資料分析蒐集
降低頻寬需求
收集各外點大數據
趨勢分析、威脅分析、智慧告警
LINE

01

Siraya 智慧網管說明

校園網管常見的問題

- IP 衝突，造成學校印表機不能印...
- Loop 造成學校大區域不能上網...
- 私接AP接錯線、亂發IP，造成部分老師無法上網...
- 電腦中毒，學校網路慢...

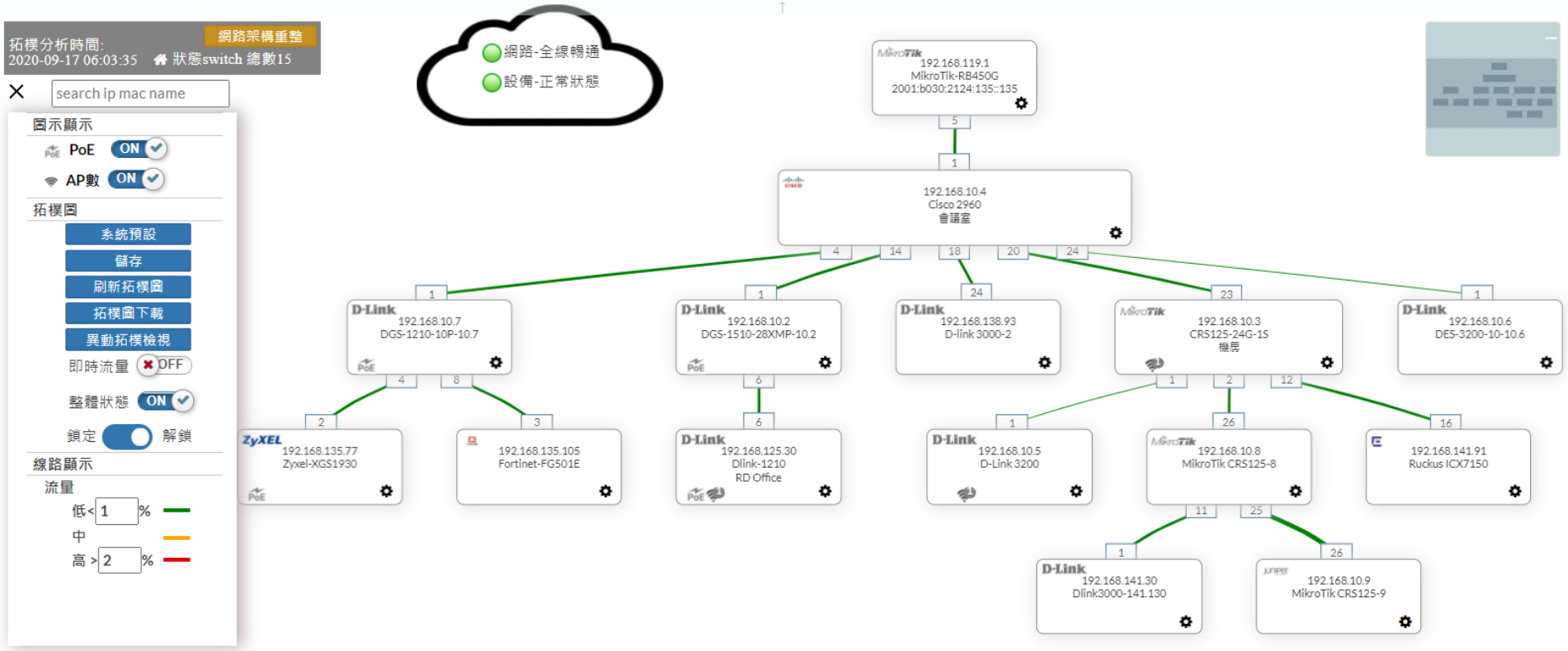
主要功能說明

登入頁

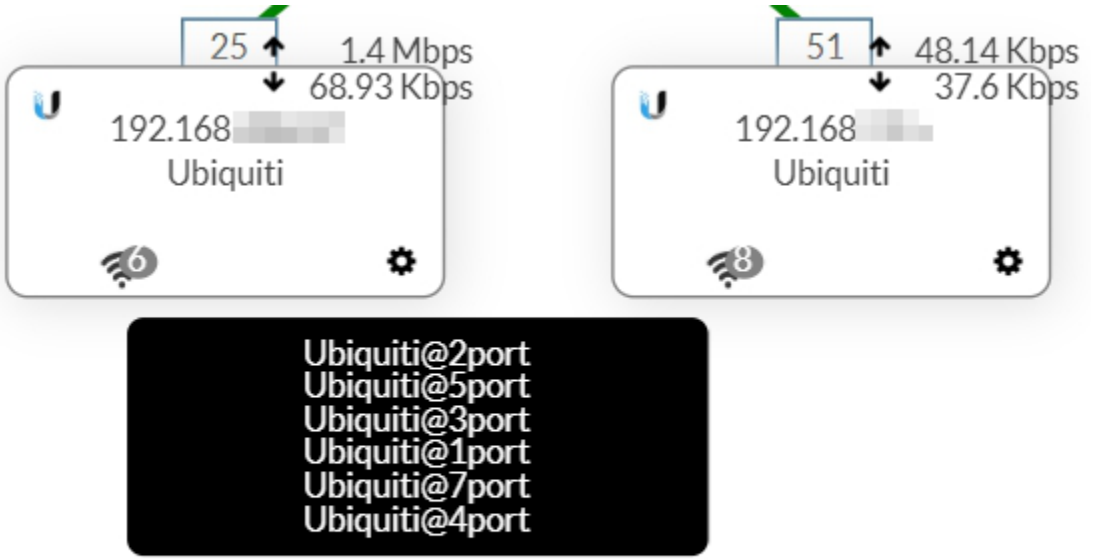
https://snm.ntct.edu.tw/

自動拓樸圖

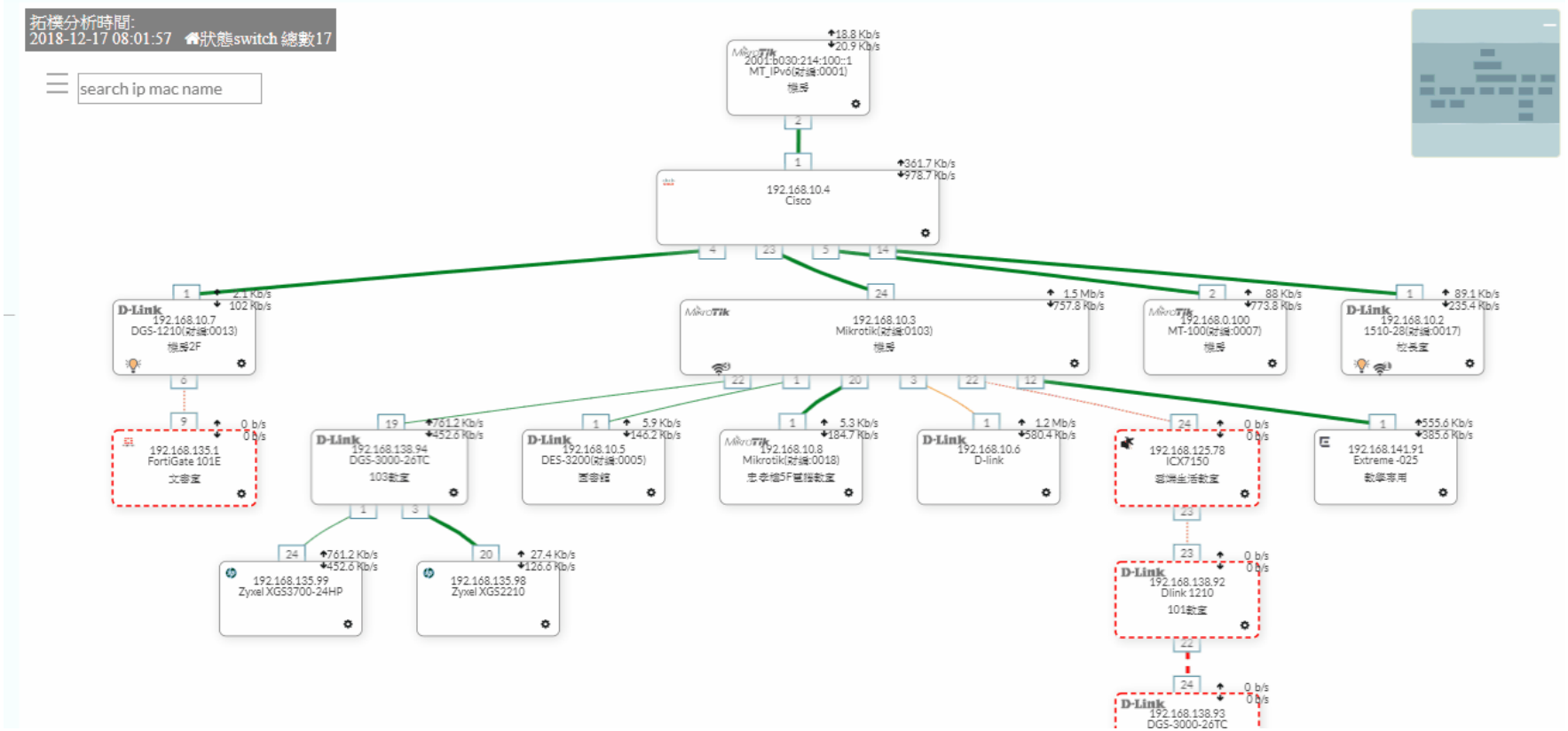
- 系統自動產生之環境架構圖
- 即時更新網路狀態
- 介接線呈現網路依擁塞程度有顏色區別

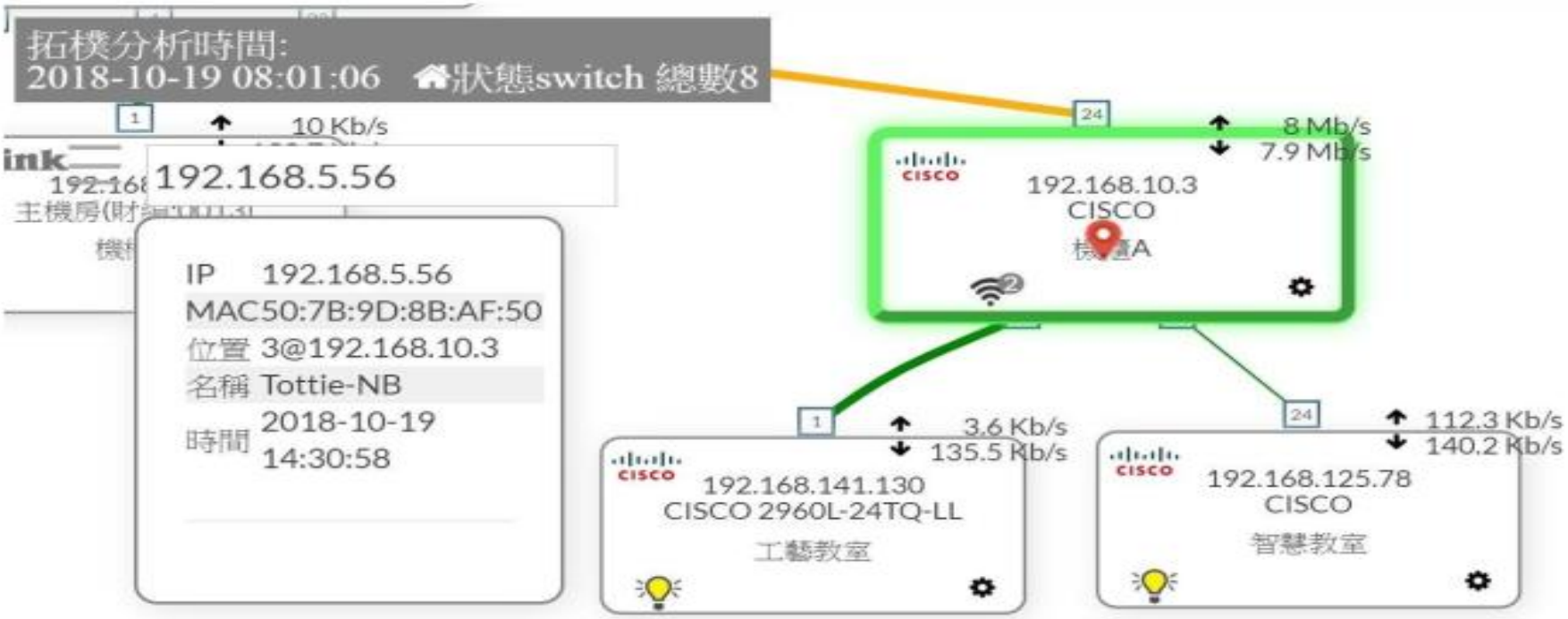


AP顯示


25
1.4 Mbps
68.93 Kbps
192.168
Ubiquiti
6
51
48.14 Kbps
37.6 Kbps
192.168
Ubiquiti
8
Ubiquiti@2port
Ubiquiti@5port
Ubiquiti@3port
Ubiquiti@1port
Ubiquiti@7port
Ubiquiti@4port

網路拓樸應用1 – 設備管理



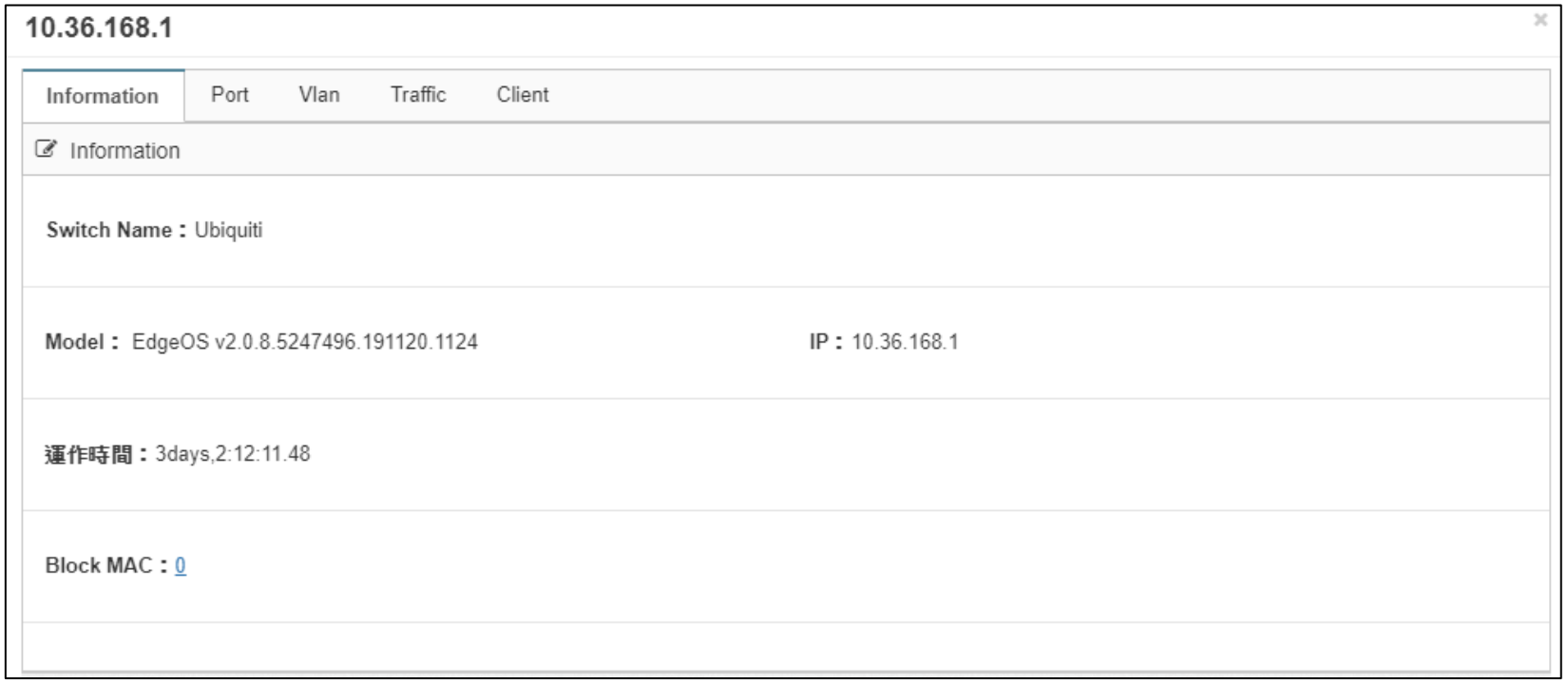


- 支援拓樸圖直接進行搜尋(IP、MAC、別名)

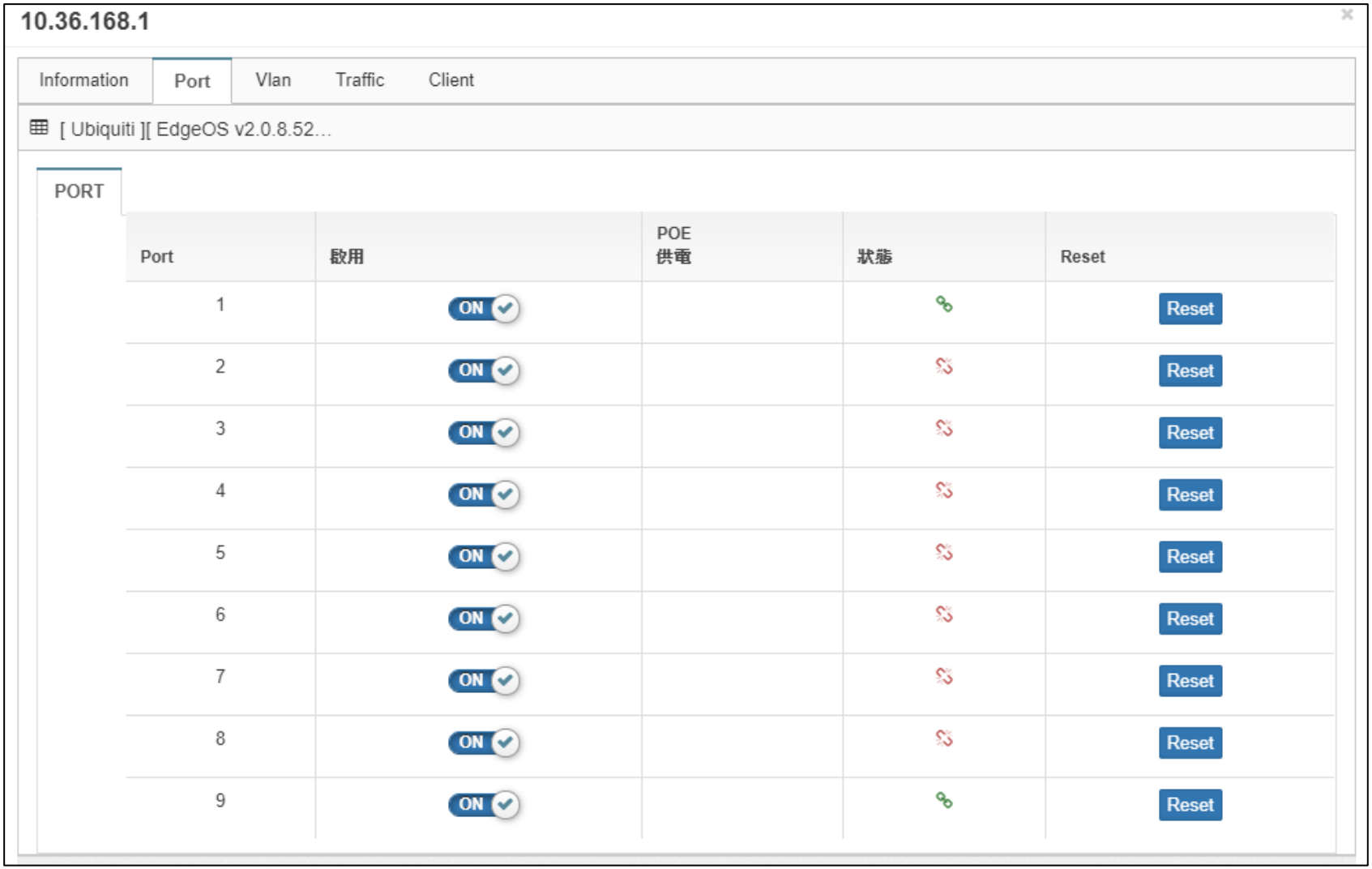
- 兩條線為堆疊狀態
- 上頭小方框為該交換器實際介接的port
- 右上數字代表該交換器uplinkport的上下載流速

- 滑鼠移至交換器上 ⚙ 後，跳出更進階的選單

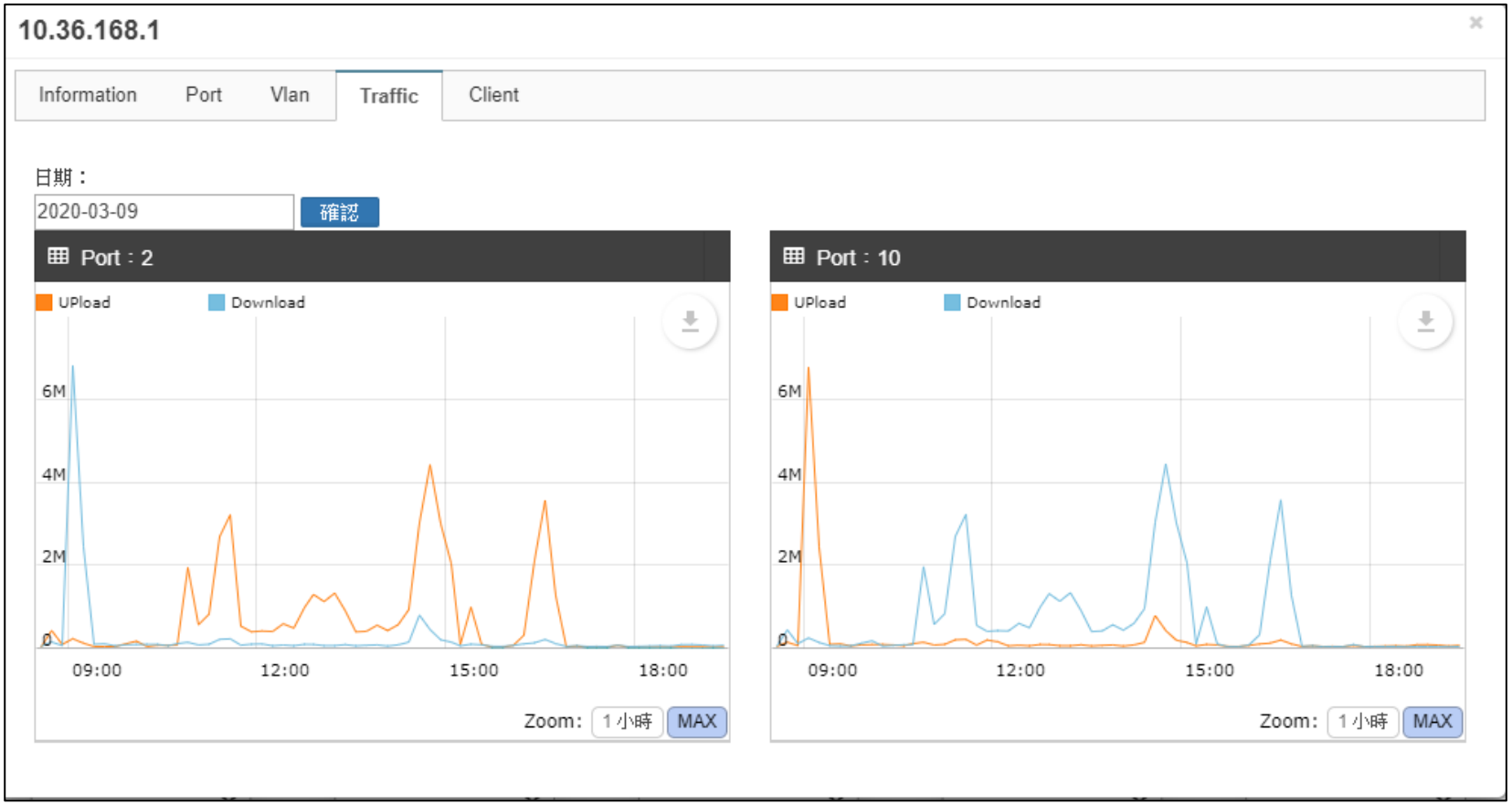
Information



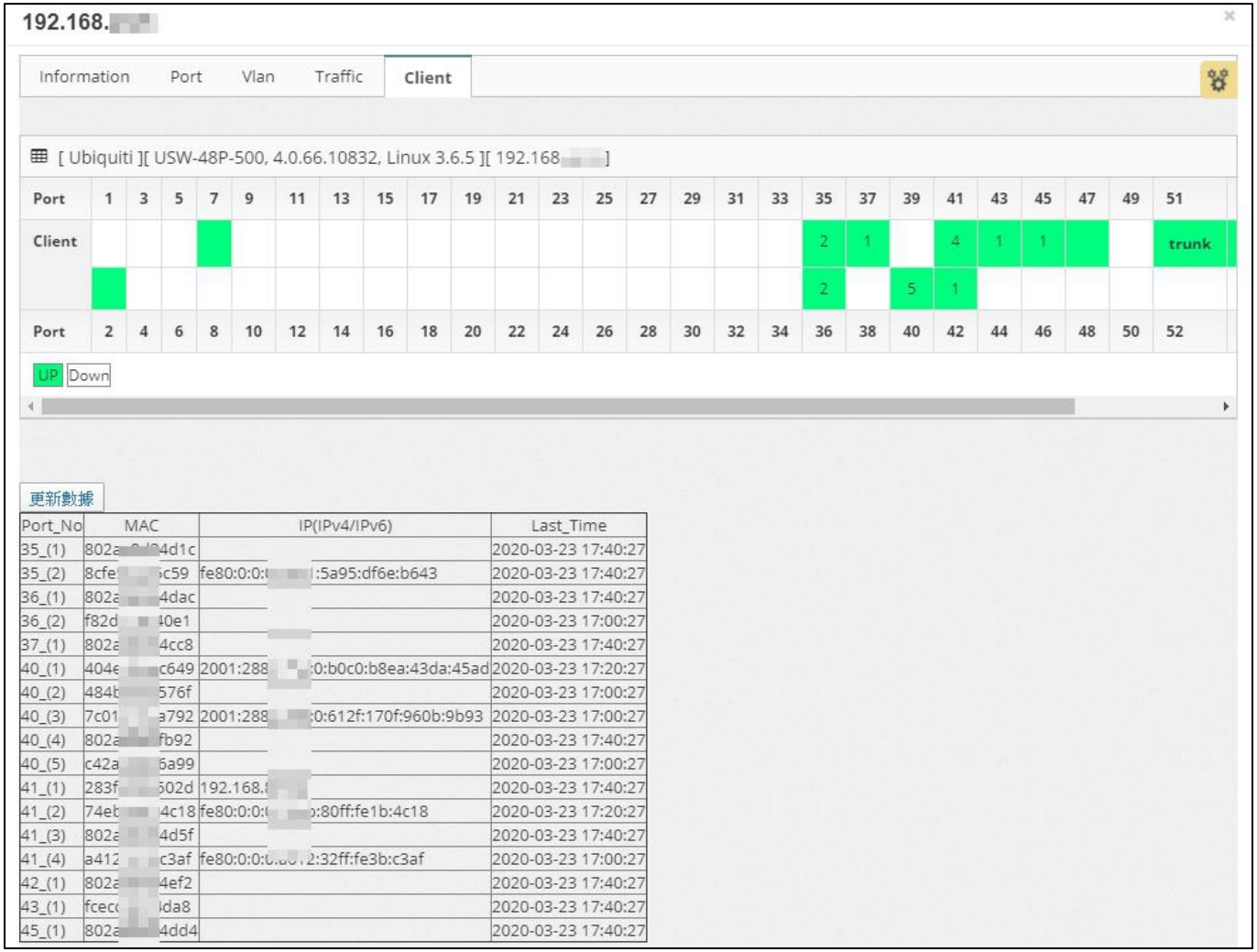
Port


10.36.168.1
Information
Port
Vlan
Traffic
Client
[Ubiquiti][EdgeOS v2.0.8.52...
PORT
Port
啟用
POE 供電
狀態
Reset
1 ON Reset
2 ON Reset
3 ON Reset
4 ON Reset
5 ON Reset
6 ON Reset
7 ON Reset
8 ON Reset
9 ON Reset

Traffic

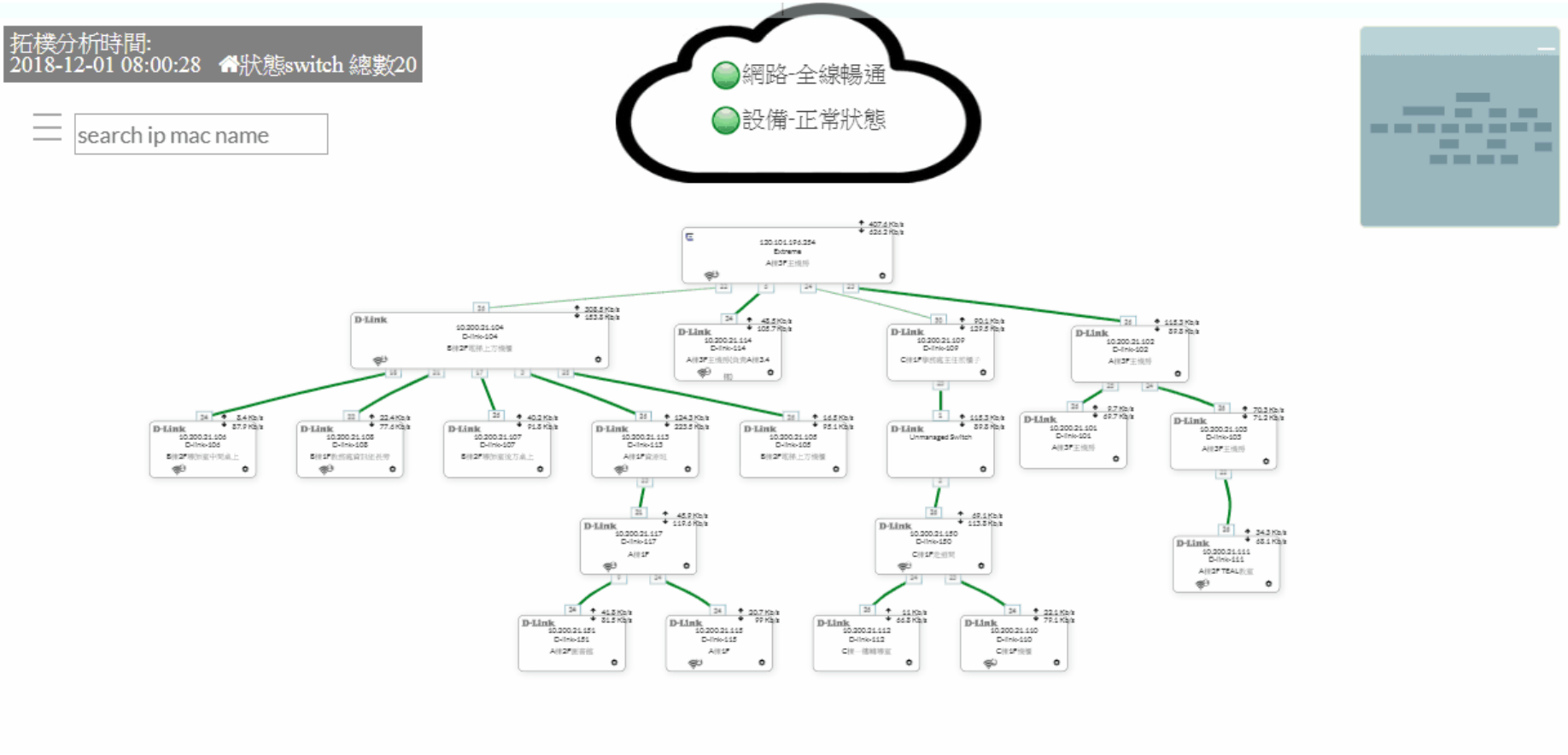

10.36.168.1
Information
Port
Vlan
Traffic
Client
日期：
2020-03-09
確認
Port : 2
UPload
Download
6M
4M
2M
0
09:00
12:00
15:00
18:00
Zoom:
1 小時
MAX
Port : 10
UPload
Download
6M
4M
2M
0
09:00
12:00
15:00
18:00
Zoom:
1 小時
MAX

Client

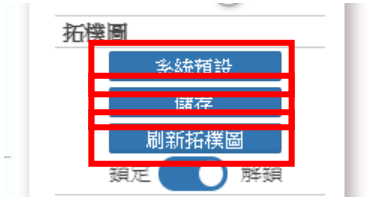


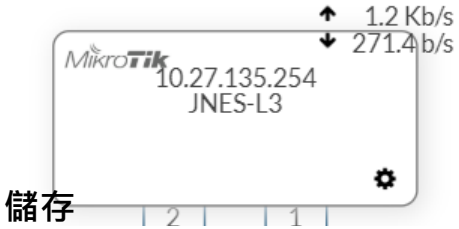
Port_No	MAC	IP(IPv4/IPv6)	Last_Time
35_(1)	802a 24d1c		2020-03-23 17:40:27
35_(2)	8cfe c59	fe80:0:0: :5a95:df6e:b643	2020-03-23 17:40:27
36_(1)	802a 4dac		2020-03-23 17:40:27
36_(2)	f82d 40e1		2020-03-23 17:00:27
37_(1)	802a 4cc8		2020-03-23 17:40:27
40_(1)	404e c649	2001:288 :0:b0c0:b8ea:43da:45ad	2020-03-23 17:20:27
40_(2)	484b 576f		2020-03-23 17:00:27
40_(3)	7c01 a792	2001:288 :0:612f:170f:960b:9b93	2020-03-23 17:00:27
40_(4)	802a fb92		2020-03-23 17:40:27
40_(5)	c42a 6a99		2020-03-23 17:00:27
41_(1)	283f 502d	192.168.8	2020-03-23 17:40:27
41_(2)	74eb 4c18	fe80:0:0: :80ff:fe1b:4c18	2020-03-23 17:20:27
41_(3)	802a 4d5f		2020-03-23 17:40:27
41_(4)	a412 c3af	fe80:0:0: 2:32ff:fe3b:c3af	2020-03-23 17:00:27
42_(1)	802a 4ef2		2020-03-23 17:40:27
43_(1)	fcec da8		2020-03-23 17:40:27
45_(1)	802a 4dd4		2020-03-23 17:40:27

網路拓撲圖 – 可拖移

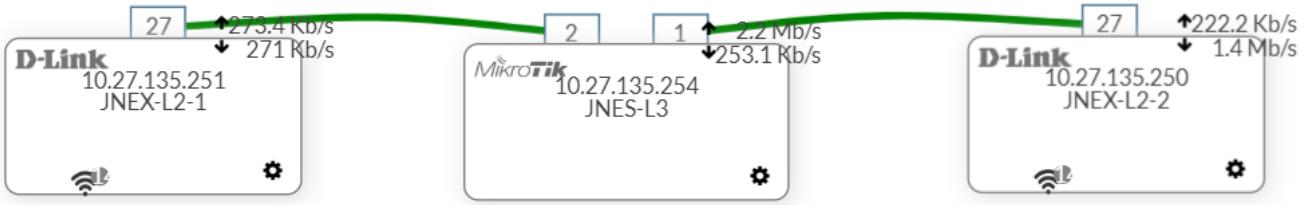

拓樸分析時間:
2018-12-01 08:00:28
狀態switch 總數20
search ip mac name
網路-全線暢通
設備-正常狀態

網路拓撲圖 – 儲存





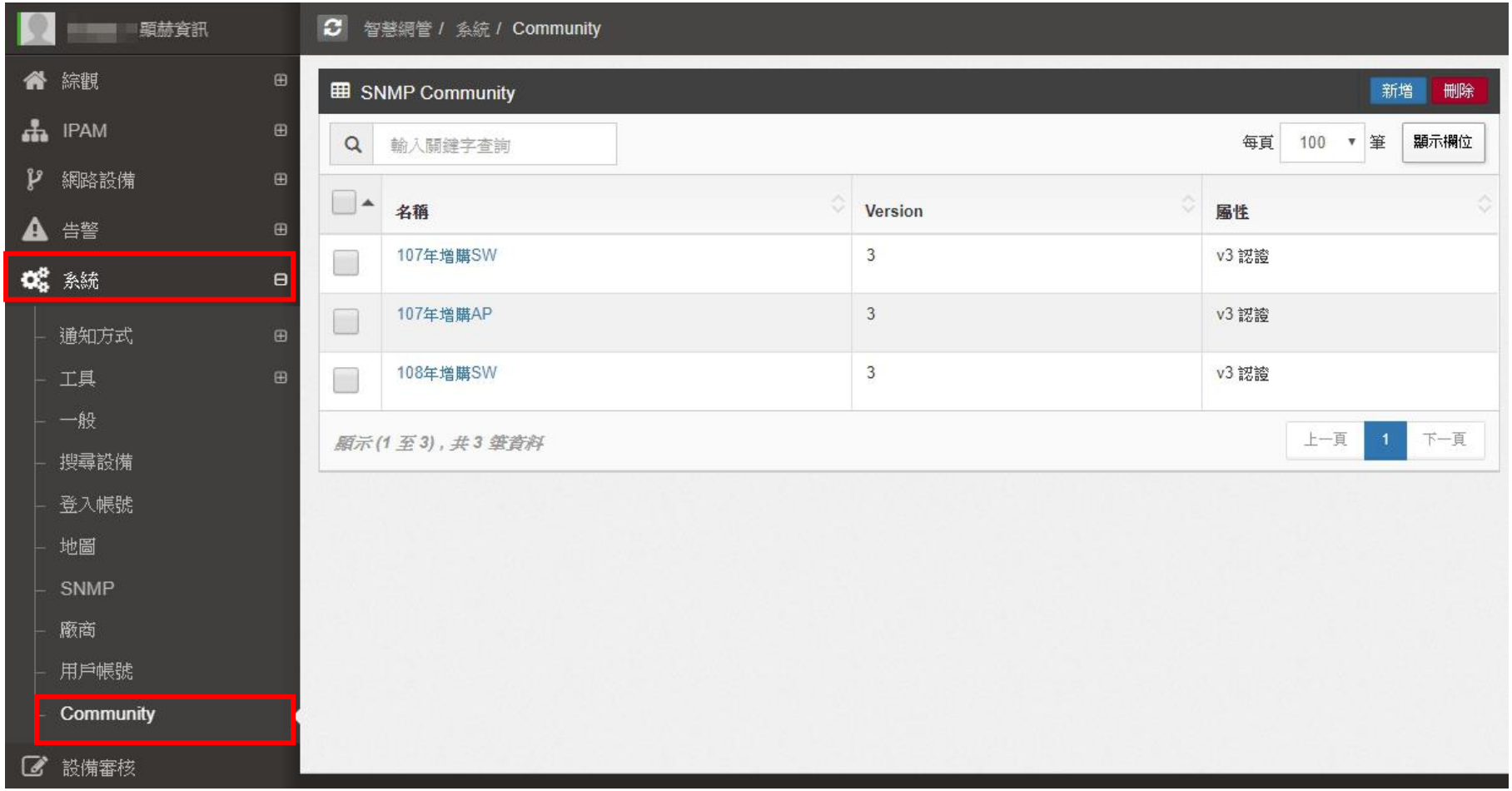
儲存



行政大樓　　忠孝樓　　仁愛樓

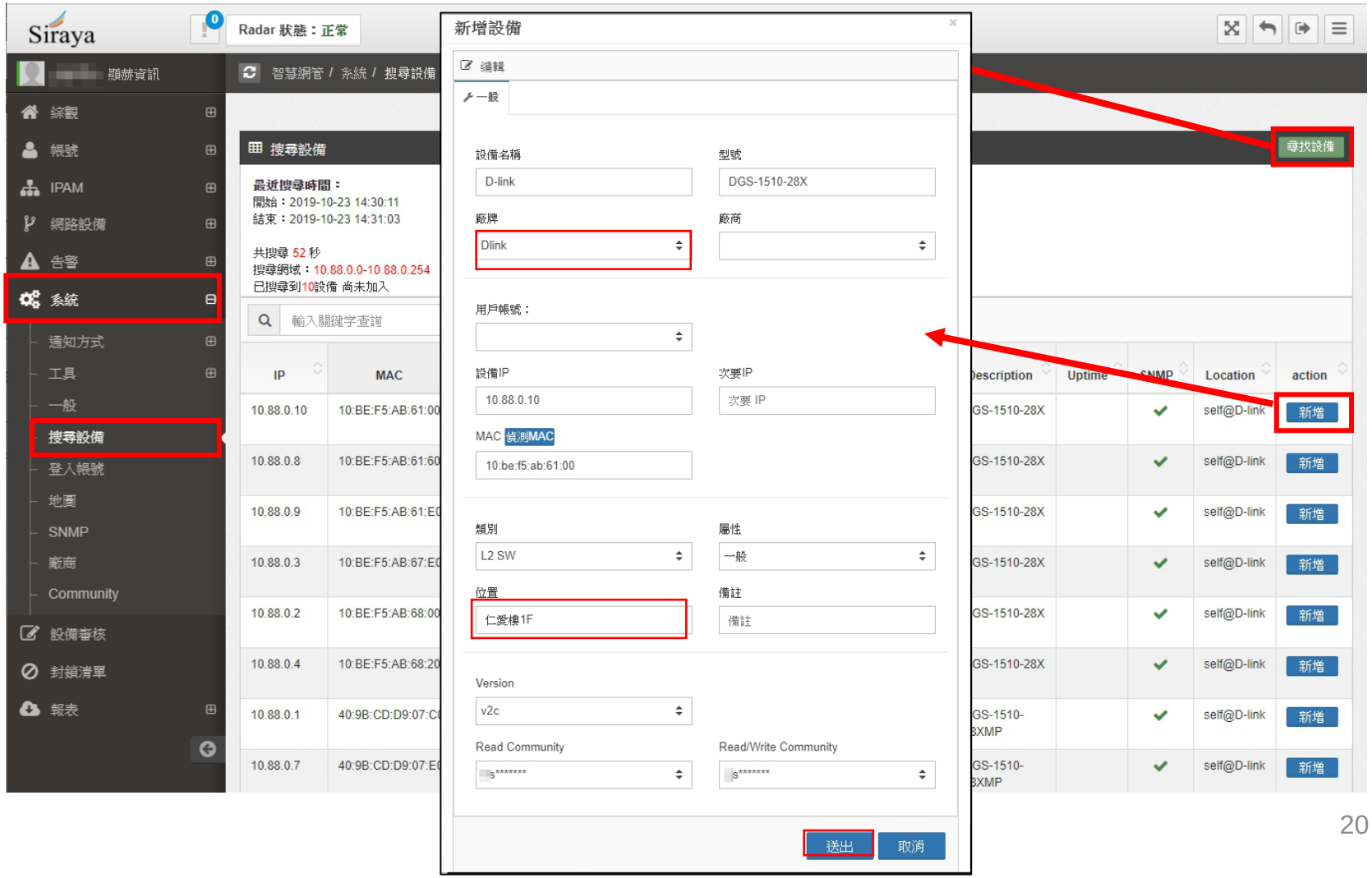
自購設備新增SNMP

系統 ➔ Community

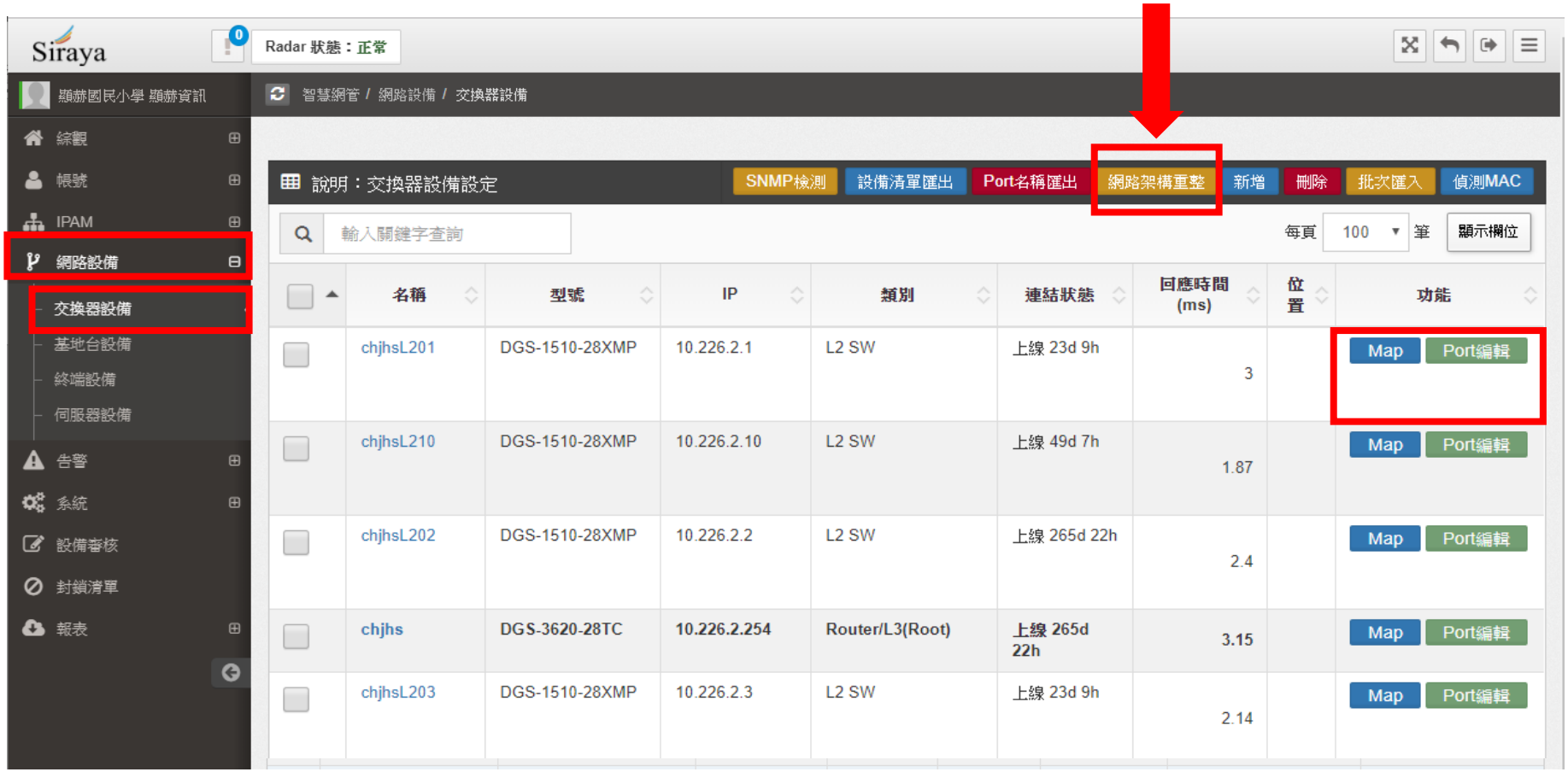


交換器與基地台納管方式

系統 ➔ 搜尋設備 ➔尋找設備

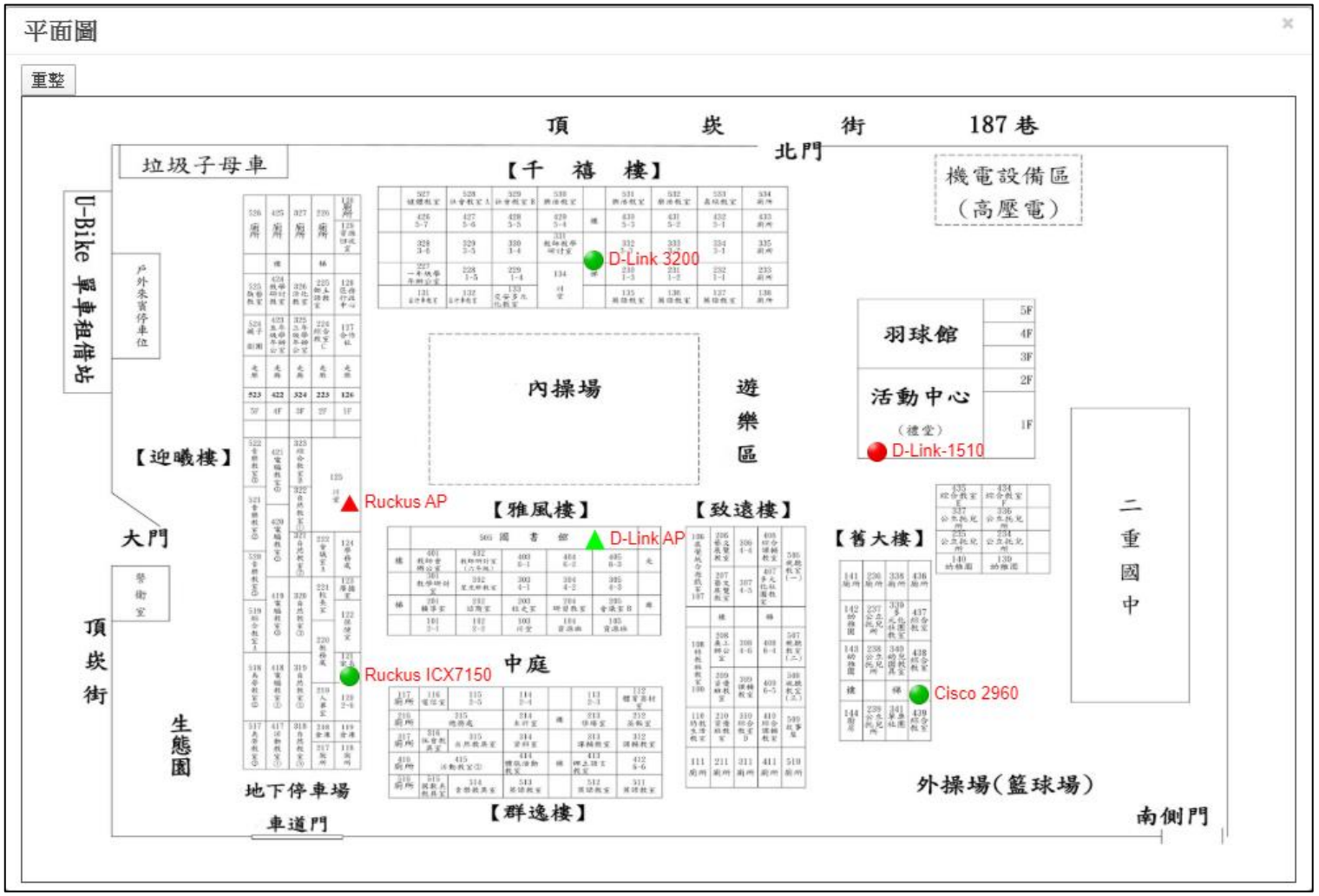


已納管之交換器清單


Siraya
Radar 狀態：正常
顯赫國民小學 顯赫資訊
智慧網管 / 網路設備 / 交換器設備
綜觀
帳號
IPAM
網路設備
交換器設備
基地台設備
終端設備
伺服器設備
告警
系統
設備審核
封鎖清單
報表
說明：交換器設備設定
SNMP檢測
設備清單匯出
Port名稱匯出
網路架構重整
新增
刪除
批次匯入
偵測MAC
輸入關鍵字查詢
每頁 100 筆
顯示欄位
名稱
型號
IP
類別
連結狀態
回應時間 (ms)
位置
功能
chjhsL201 DGS-1510-28XMP 10.226.2.1 L2 SW 上線 23d 9h 3 Map Port編輯
chjhsL210 DGS-1510-28XMP 10.226.2.10 L2 SW 上線 49d 7h 1.87 Map Port編輯
chjhsL202 DGS-1510-28XMP 10.226.2.2 L2 SW 上線 265d 22h 2.4 Map Port編輯
chjhs DGS-3620-28TC 10.226.2.254 Router/L3(Root) 上線 265d 22h 3.15 Map Port編輯
chjhsL203 DGS-1510-28XMP 10.226.2.3 L2 SW 上線 23d 9h 2.14 Map Port編輯

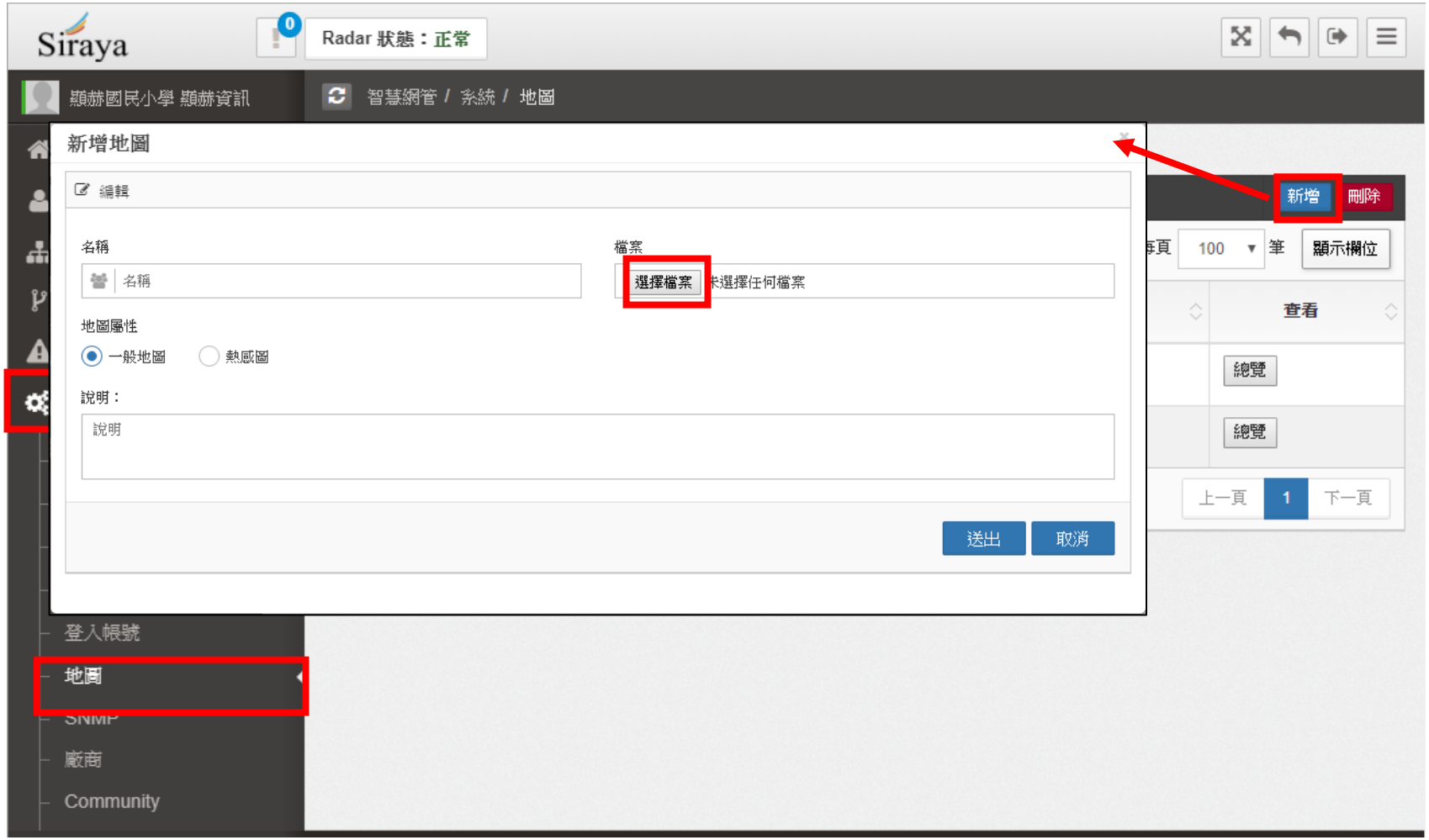
Map

設備顯示於平面圖上，清楚得知實際位置。



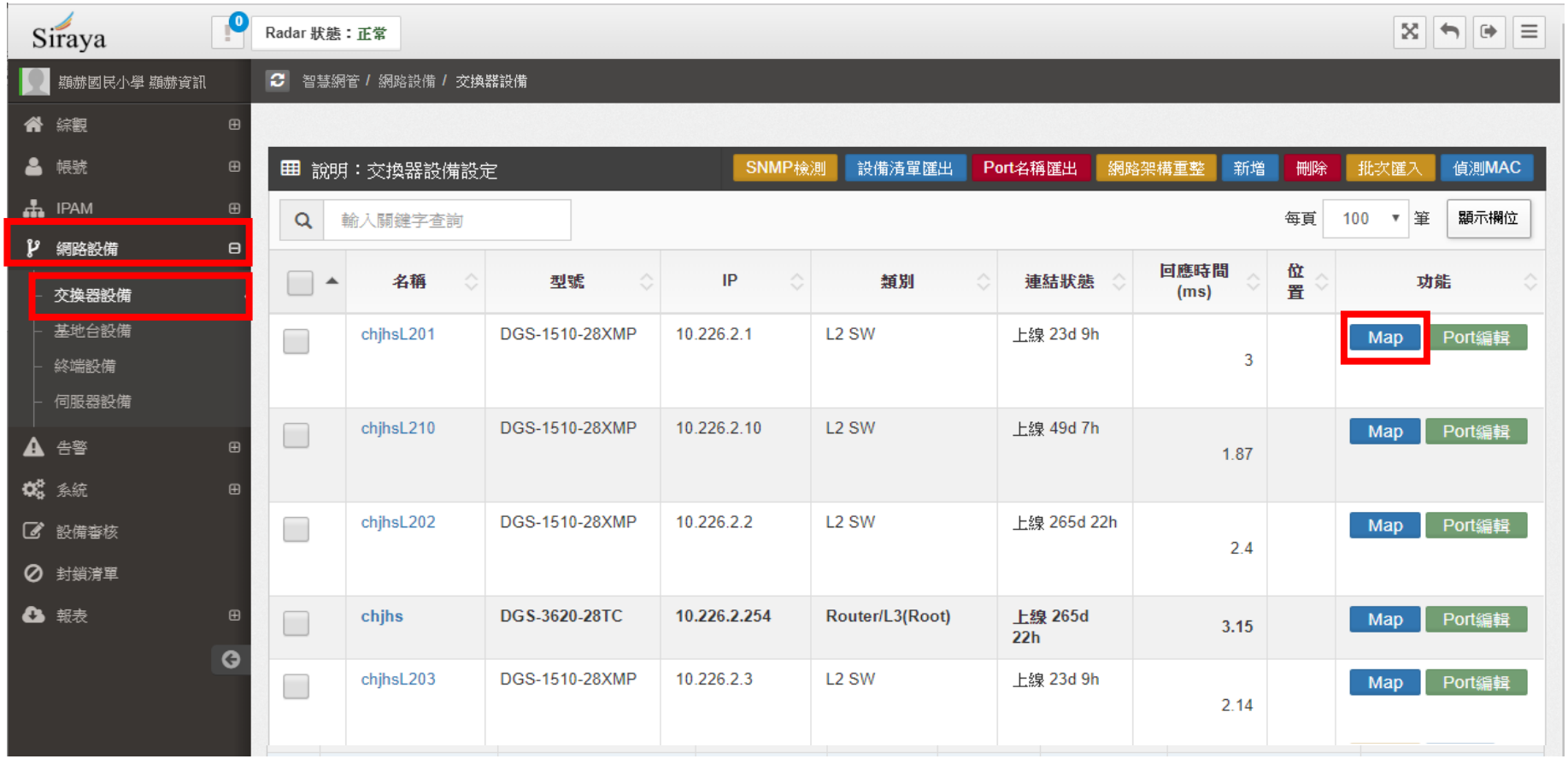
新增學校平面圖

系統➔地圖



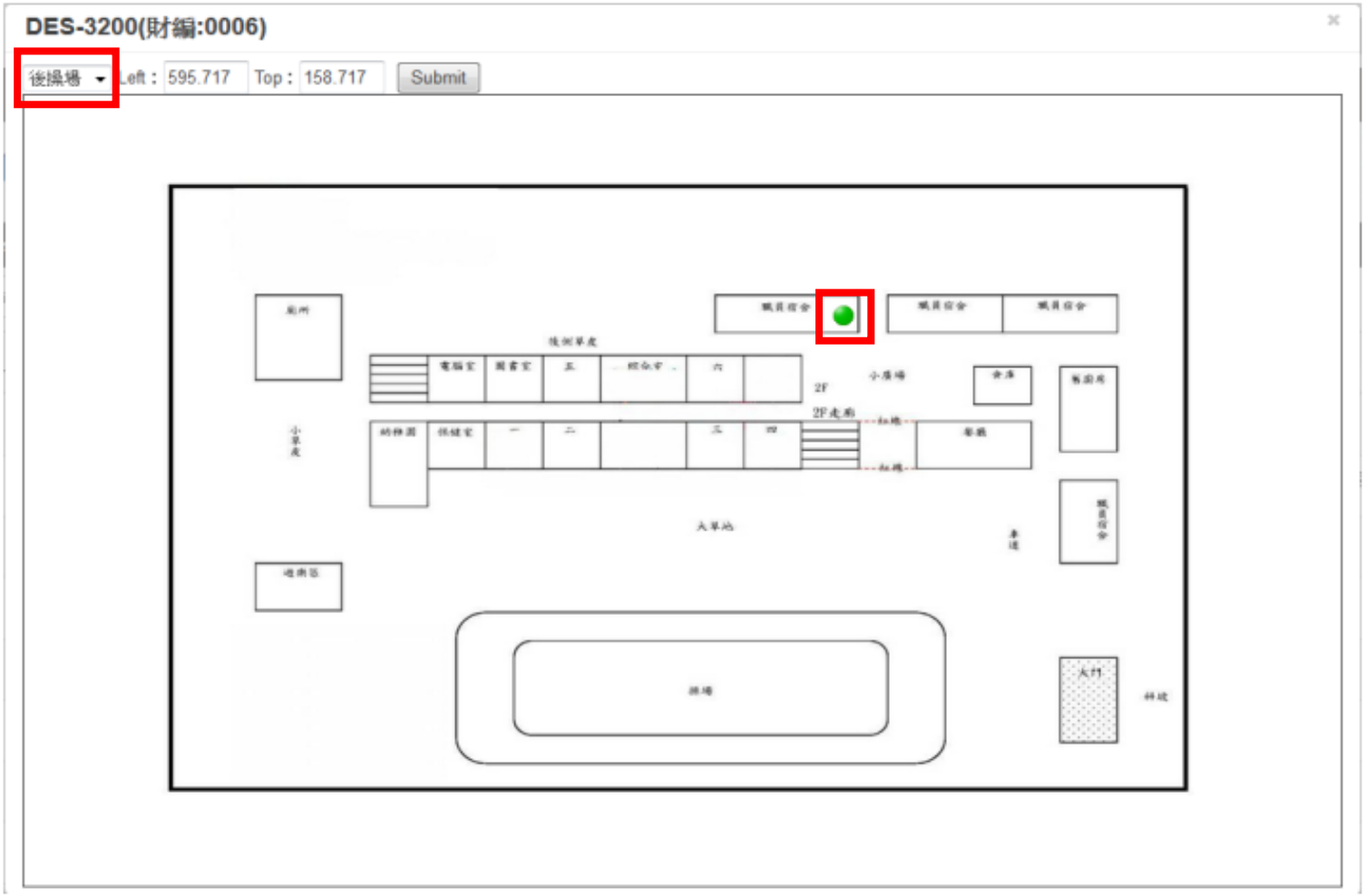
Map

如何定義設備位置?

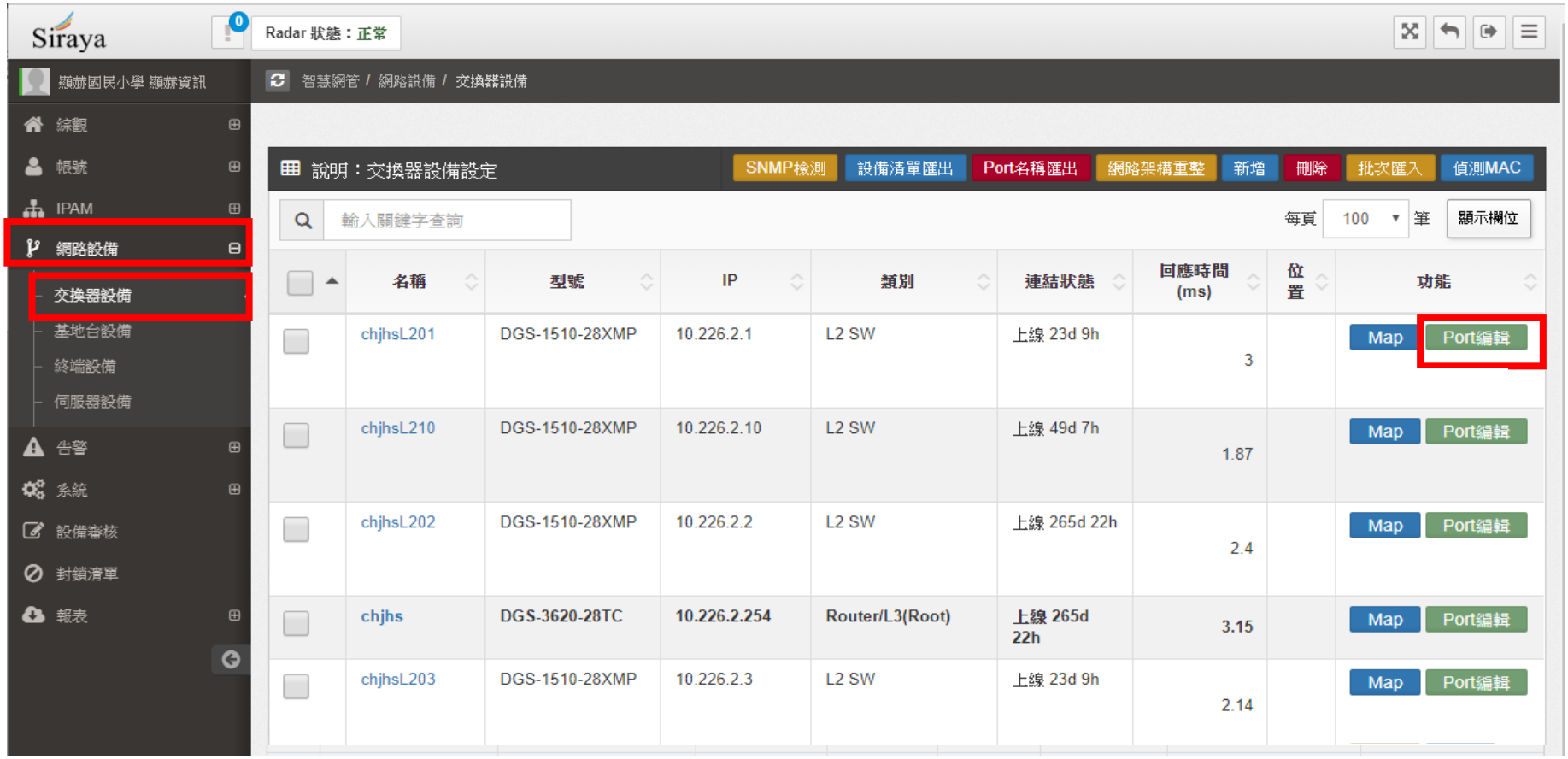


Map

拖移設備至正確的平面圖上，已標示正確所在位置。

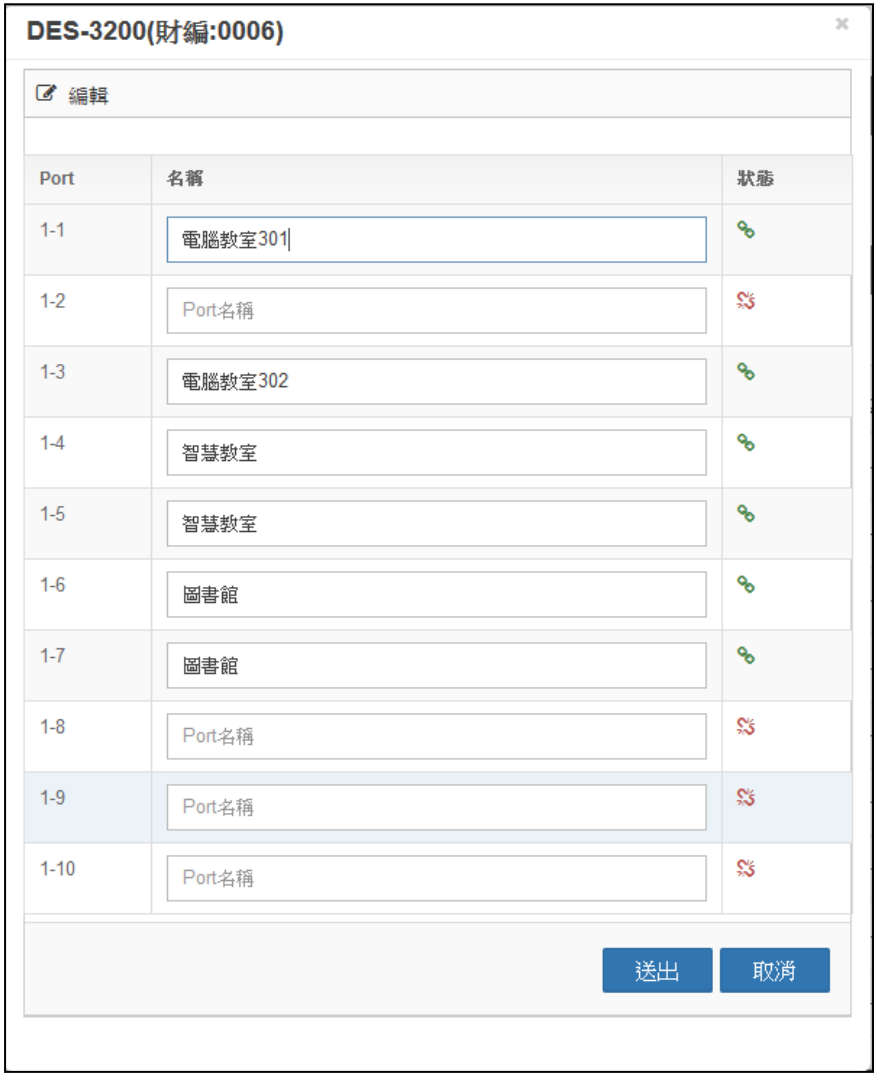


Port編輯

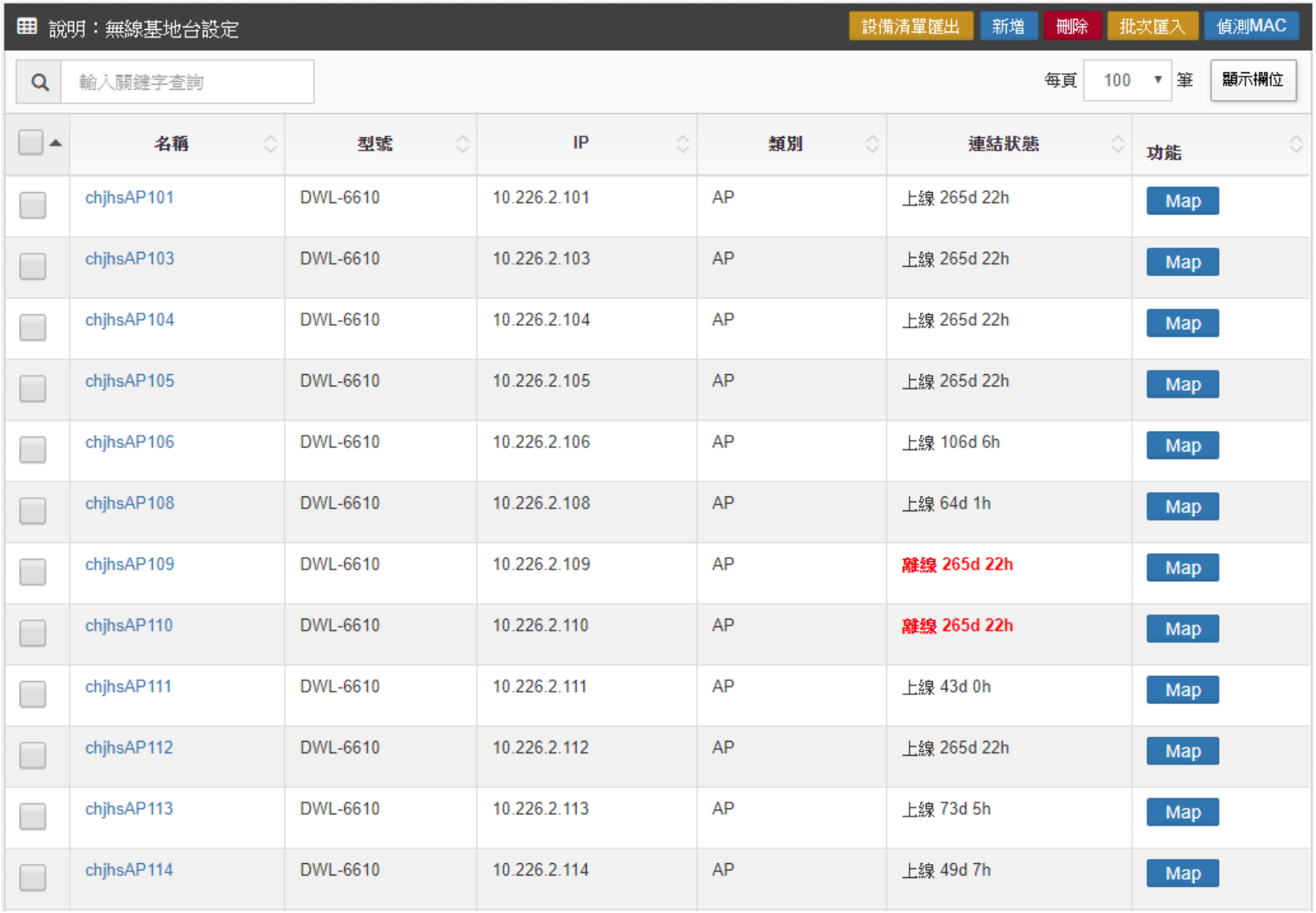

Siraya
Radar 狀態：正常
顯赫國民小學 顯赫資訊
智慧網管 / 網路設備 / 交換器設備
綜觀
帳號
IPAM
網路設備
交換器設備
基地台設備
終端設備
伺服器設備
告警
系統
設備審核
封鎖清單
報表
說明：交換器設備設定
SNMP檢測
設備清單匯出
Port名稱匯出
網路架構重整
新增
刪除
批次匯入
偵測MAC
輸入關鍵字查詢
每頁 100 筆
顯示欄位
名稱
型號
IP
類別
連結狀態
回應時間 (ms)
位置
功能
chjhsL201 DGS-1510-28XMP 10.226.2.1 L2 SW 上線 23d 9h 3 Map Port編輯
chjhsL210 DGS-1510-28XMP 10.226.2.10 L2 SW 上線 49d 7h 1.87 Map Port編輯
chjhsL202 DGS-1510-28XMP 10.226.2.2 L2 SW 上線 265d 22h 2.4 Map Port編輯
chjhs DGS-3620-28TC 10.226.2.254 Router/L3(Root) 上線 265d 22h 3.15 Map Port編輯
chjhsL203 DGS-1510-28XMP 10.226.2.3 L2 SW 上線 23d 9h 2.14 Map Port編輯

Port編輯

可自行註記每一個Port的用途、地點。



已納管之基地台清單

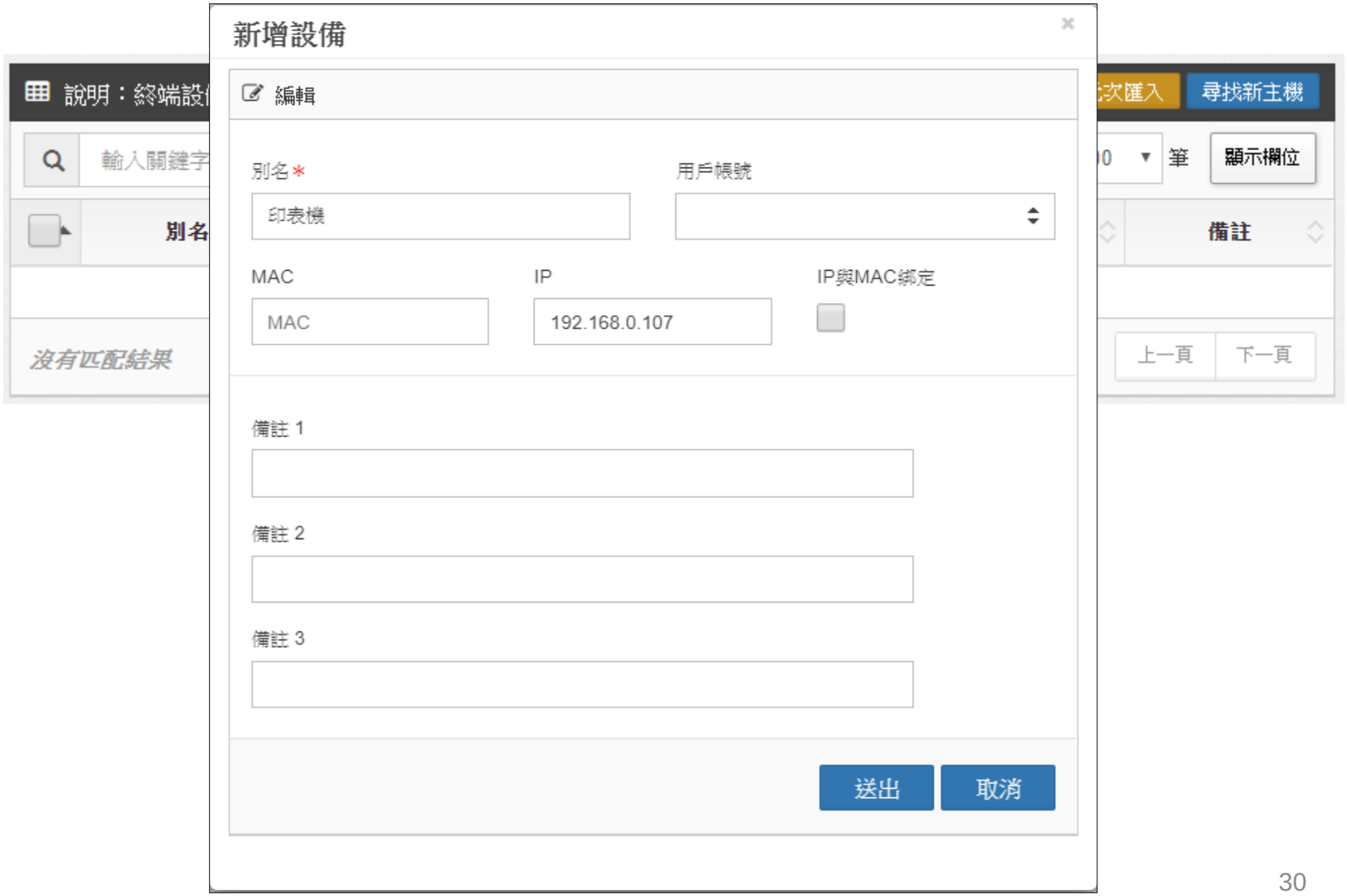


名稱	型號	IP	類別	連結狀態	功能
chjhsAP101	DWL-6610	10.226.2.101	AP	上線 265d 22h	Map
chjhsAP103	DWL-6610	10.226.2.103	AP	上線 265d 22h	Map
chjhsAP104	DWL-6610	10.226.2.104	AP	上線 265d 22h	Map
chjhsAP105	DWL-6610	10.226.2.105	AP	上線 265d 22h	Map
chjhsAP106	DWL-6610	10.226.2.106	AP	上線 106d 6h	Map
chjhsAP108	DWL-6610	10.226.2.108	AP	上線 64d 1h	Map
chjhsAP109	DWL-6610	10.226.2.109	AP	離線 265d 22h	Map
chjhsAP110	DWL-6610	10.226.2.110	AP	離線 265d 22h	Map
chjhsAP111	DWL-6610	10.226.2.111	AP	上線 43d 0h	Map
chjhsAP112	DWL-6610	10.226.2.112	AP	上線 265d 22h	Map
chjhsAP113	DWL-6610	10.226.2.113	AP	上線 73d 5h	Map
chjhsAP114	DWL-6610	10.226.2.114	AP	上線 49d 7h	Map

終端設備

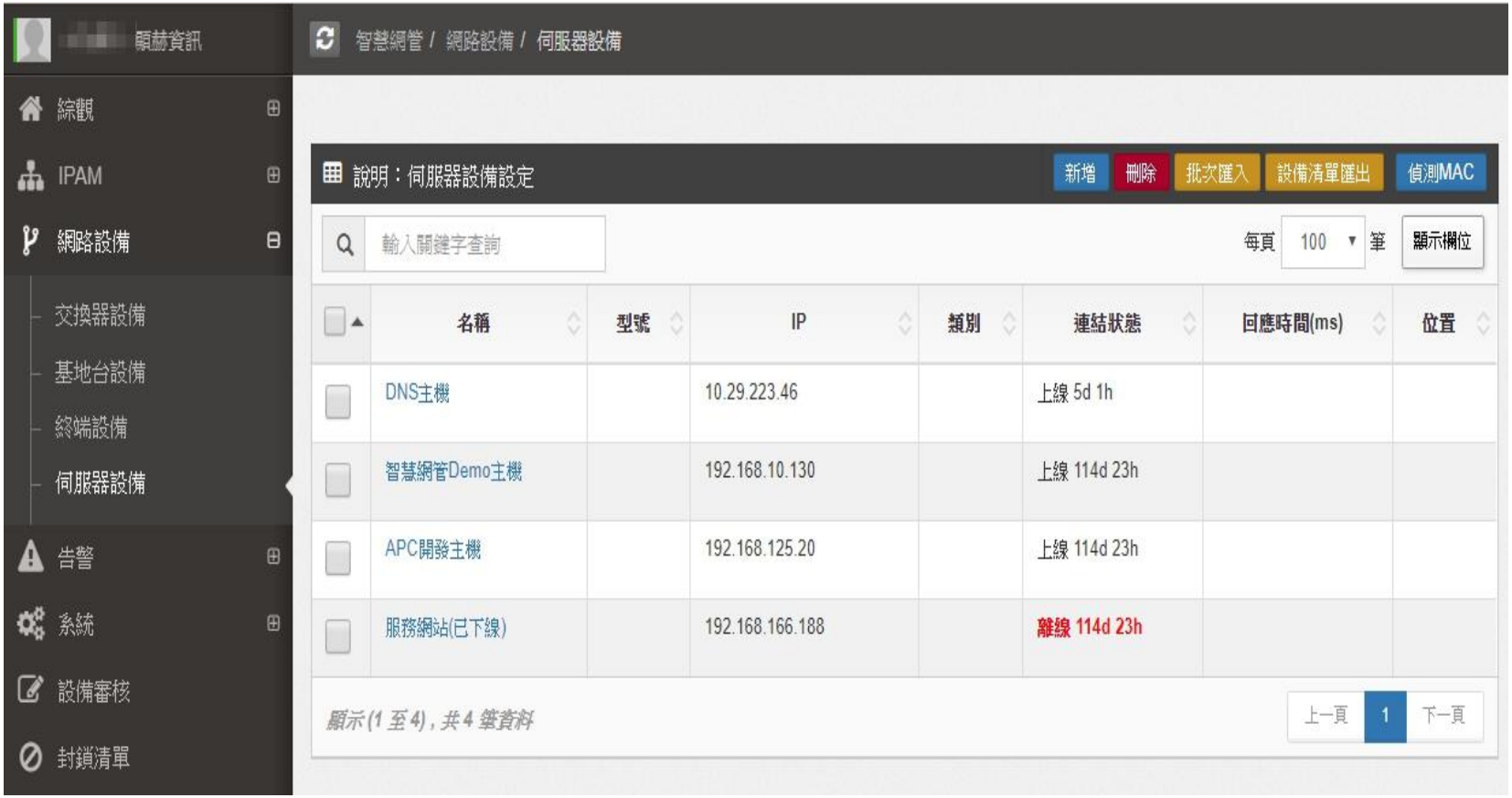
納管的終端設備於此顯示。

如何新增終端設備別名?


新增設備
編輯
別名 *
印表機
用戶帳號
MAC
MAC
IP
192.168.0.107
IP與MAC綁定
備註 1
備註 2
備註 3
送出
取消
說明：終端設
輸入關鍵字
別名
沒有匹配結果
尋找新主機
顯示欄位
筆
備註
上一頁
下一頁

伺服器設備

納管的伺服器設備於此顯示。



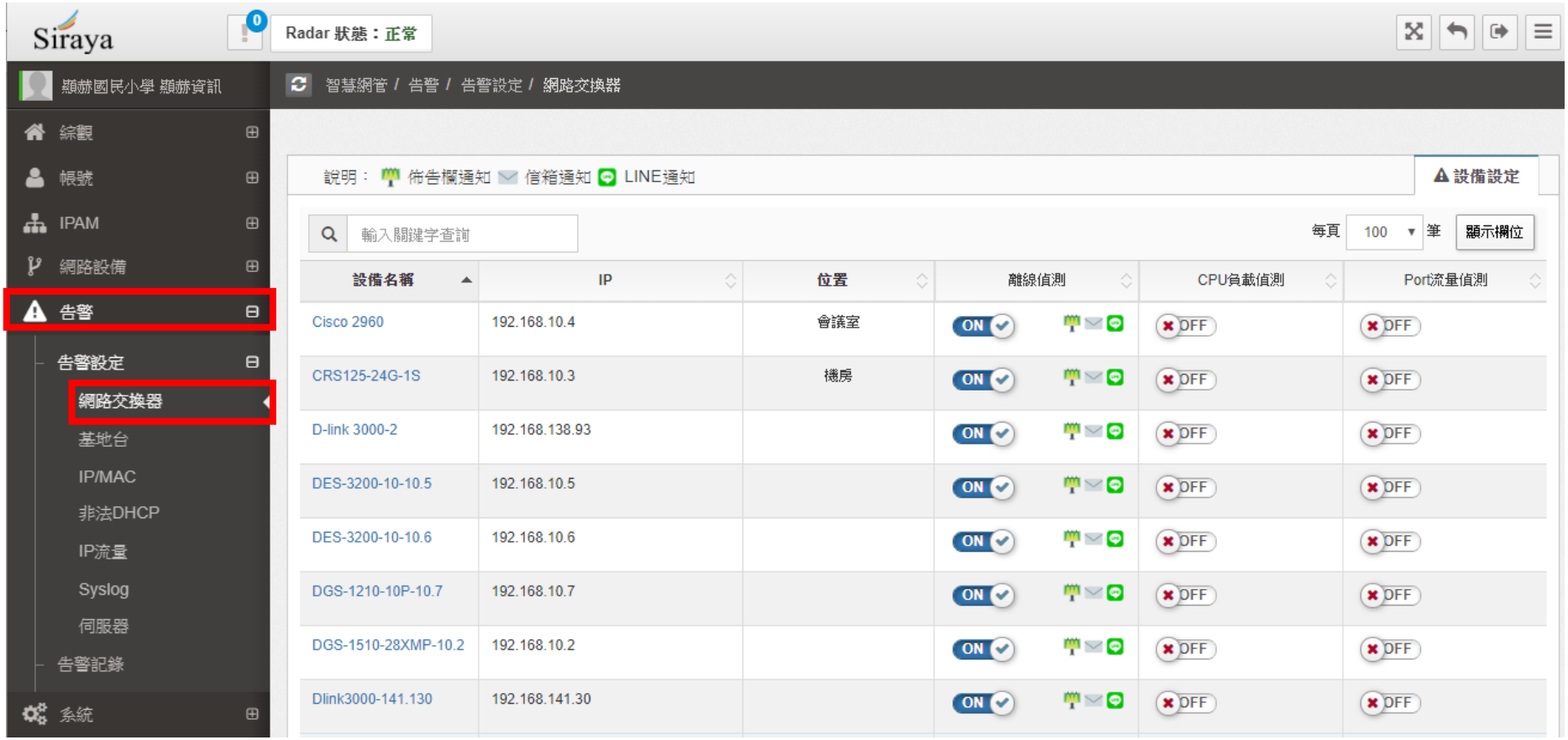
告警設定

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

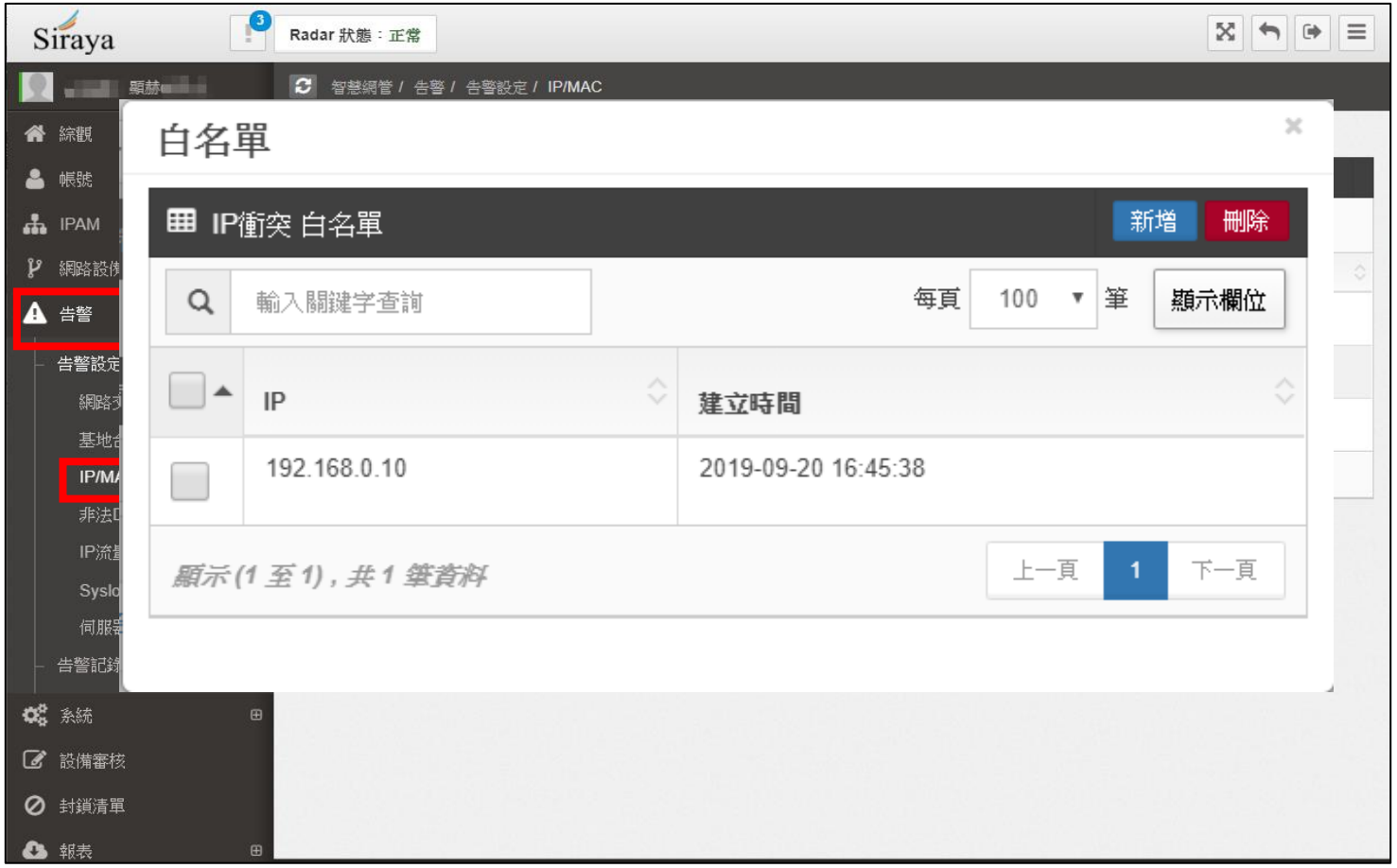
針對網路交換器進行**離線偵測**、**CPU 負載**、**Port 流量偵測**。



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



IP 衝突偵測 ：環境中出現兩個相同 IP 即產生告警。

未知設備偵測: 單位內非納管之設備進行偵測告警。

非法IP 偵測 ：若環境中出現與納管既有設備之相同 IP，即產生告警。

全域設定

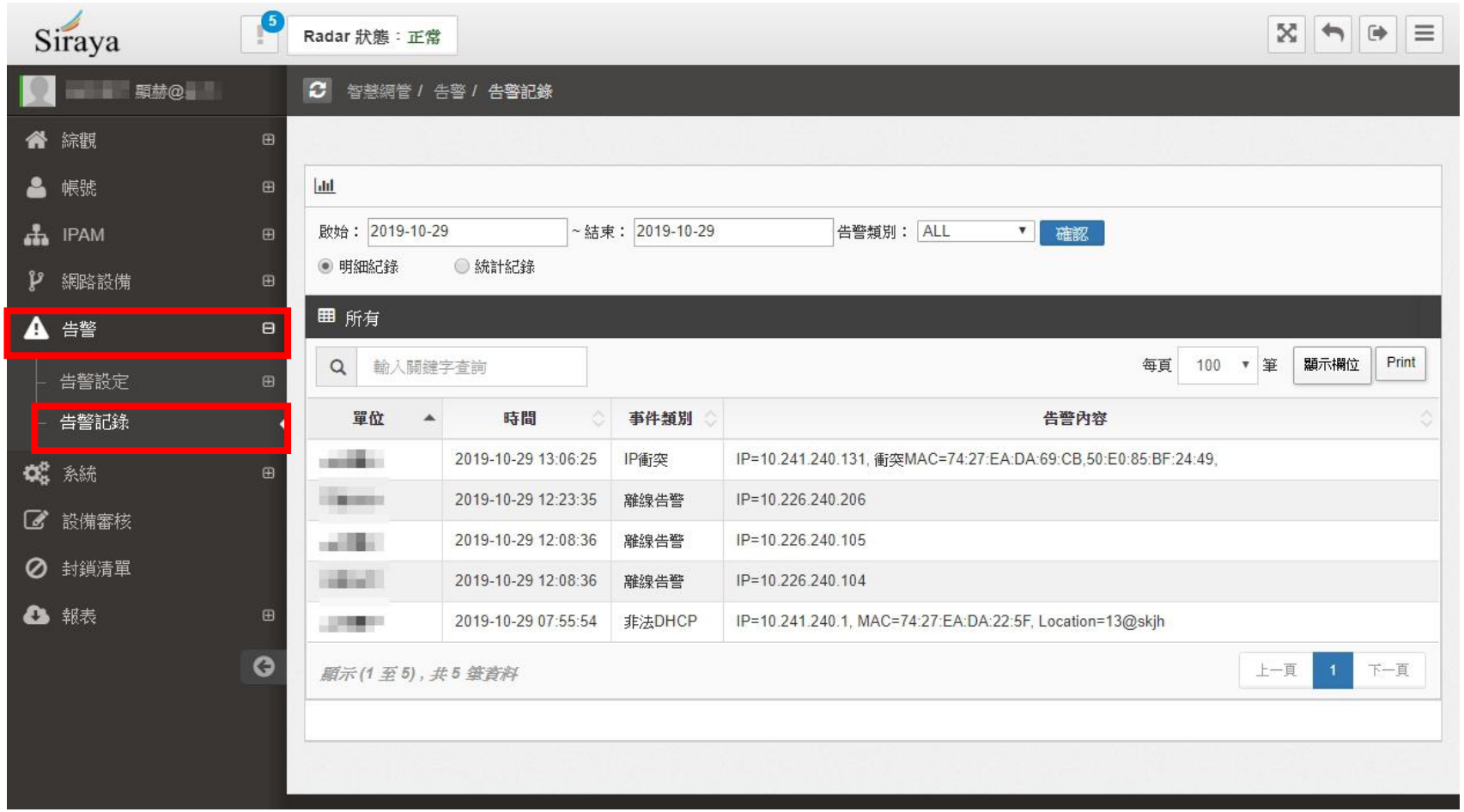
告警 ➔ 告警設定 ➔IP流量

對網段或是單一 IP 進行**IP流量**偵測

告警記錄

告警 ➔ 告警紀錄

產生的相關紀錄留存查詢。



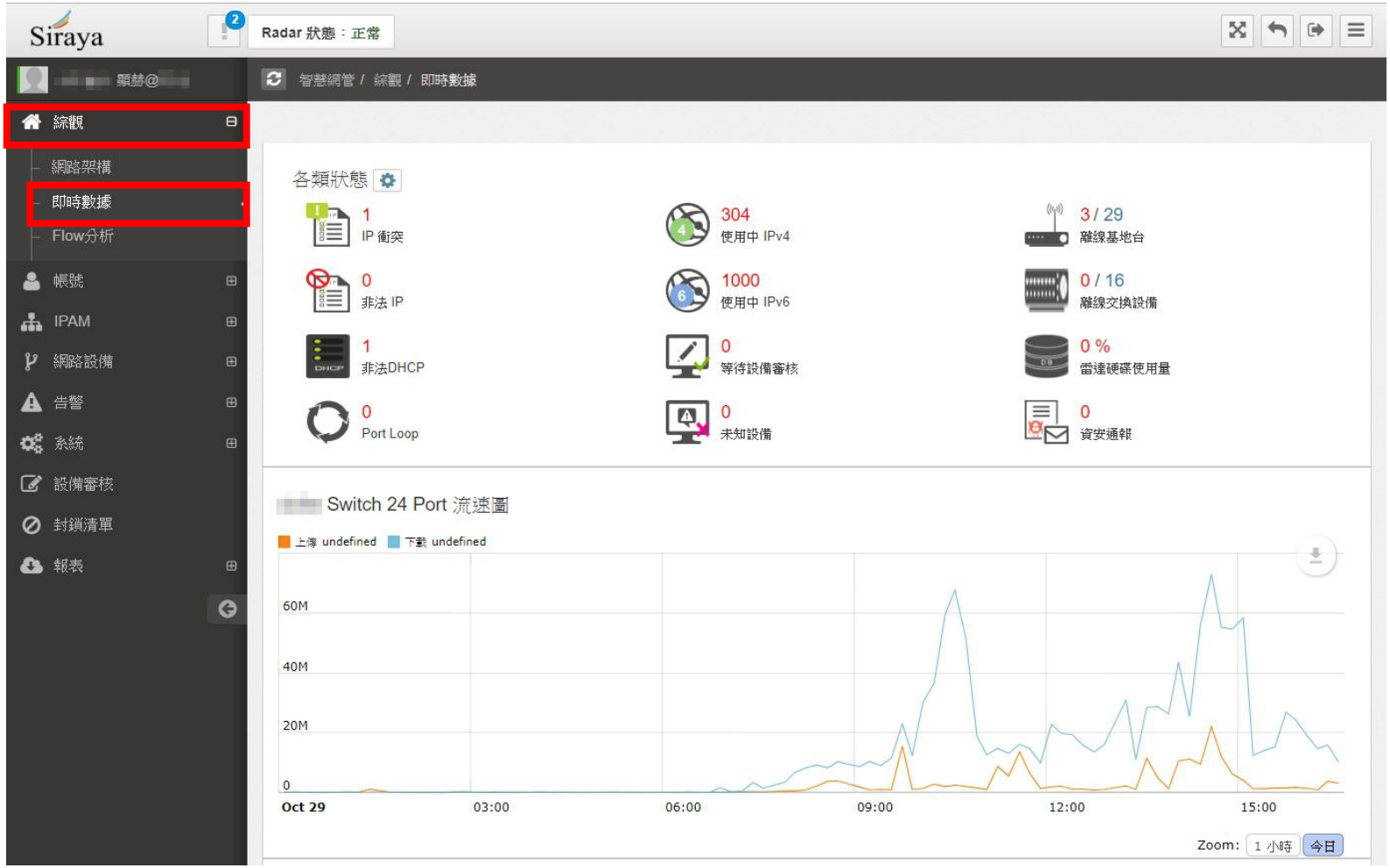
系統流量

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。



使用 IPv4

資料來源： 中心流量取樣

輸入關鍵字查詢

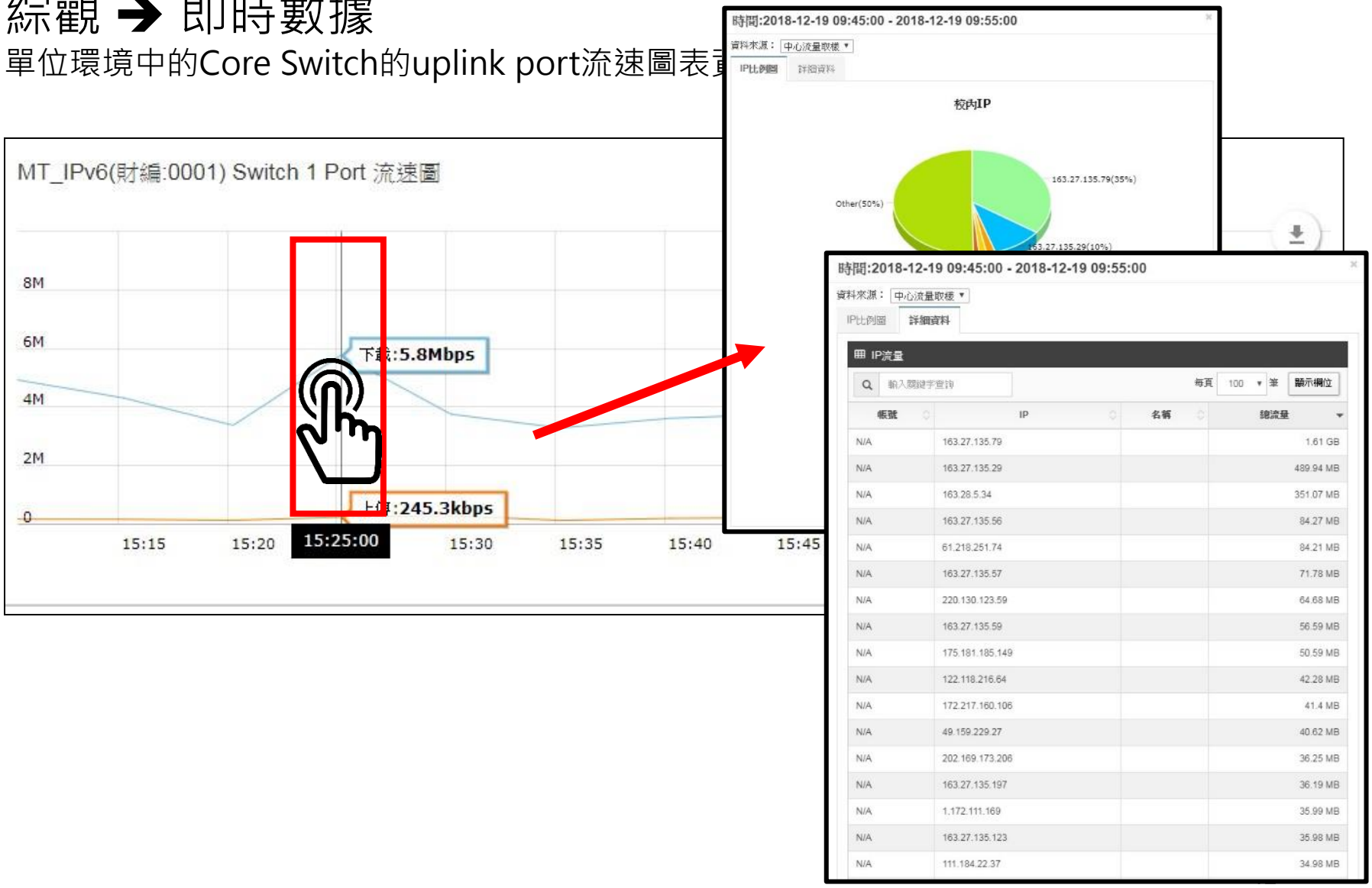
每頁 100 筆 顯示欄位

IP	別名	今日累積數據				
		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

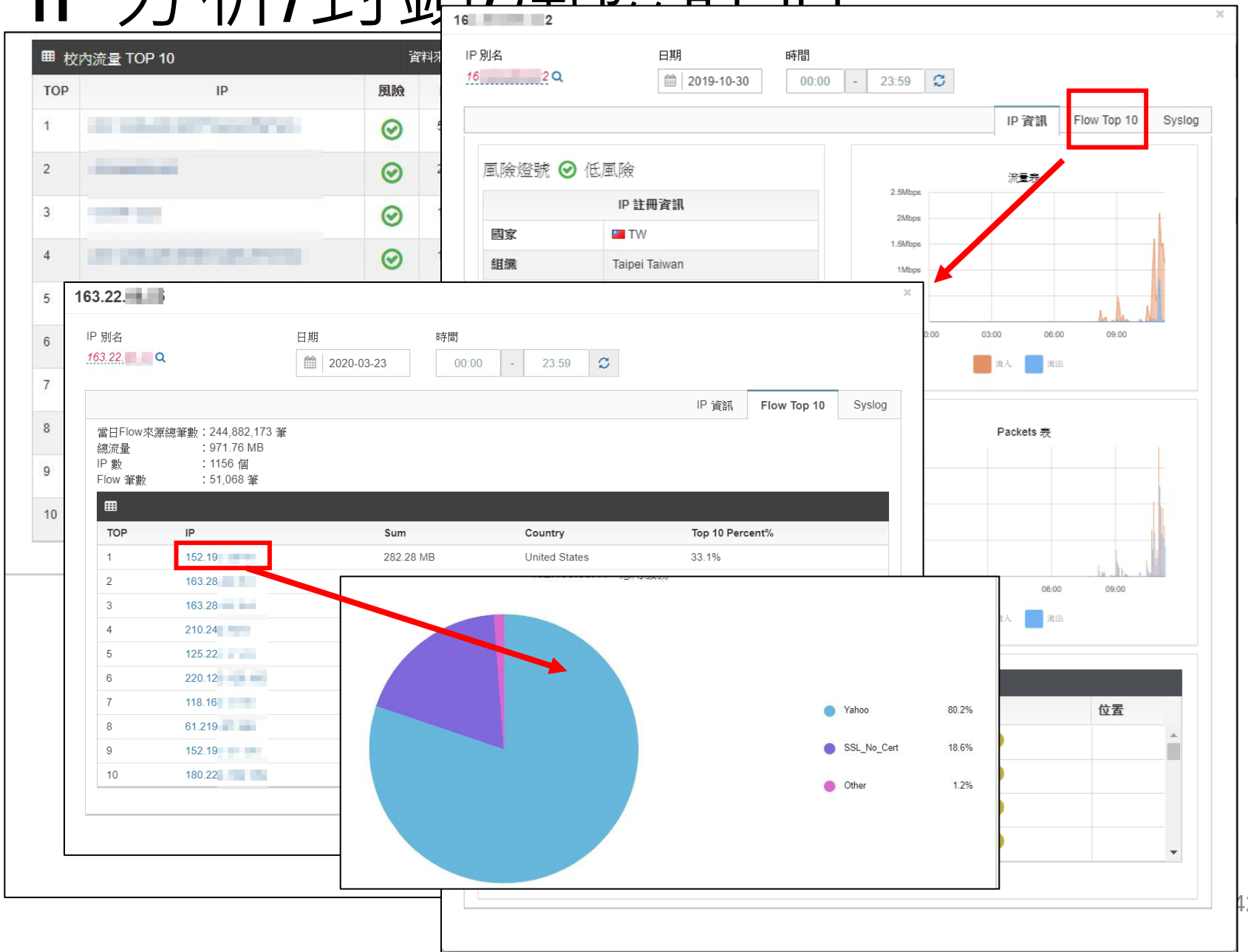
即時數據

綜觀 ➔ 即時數據

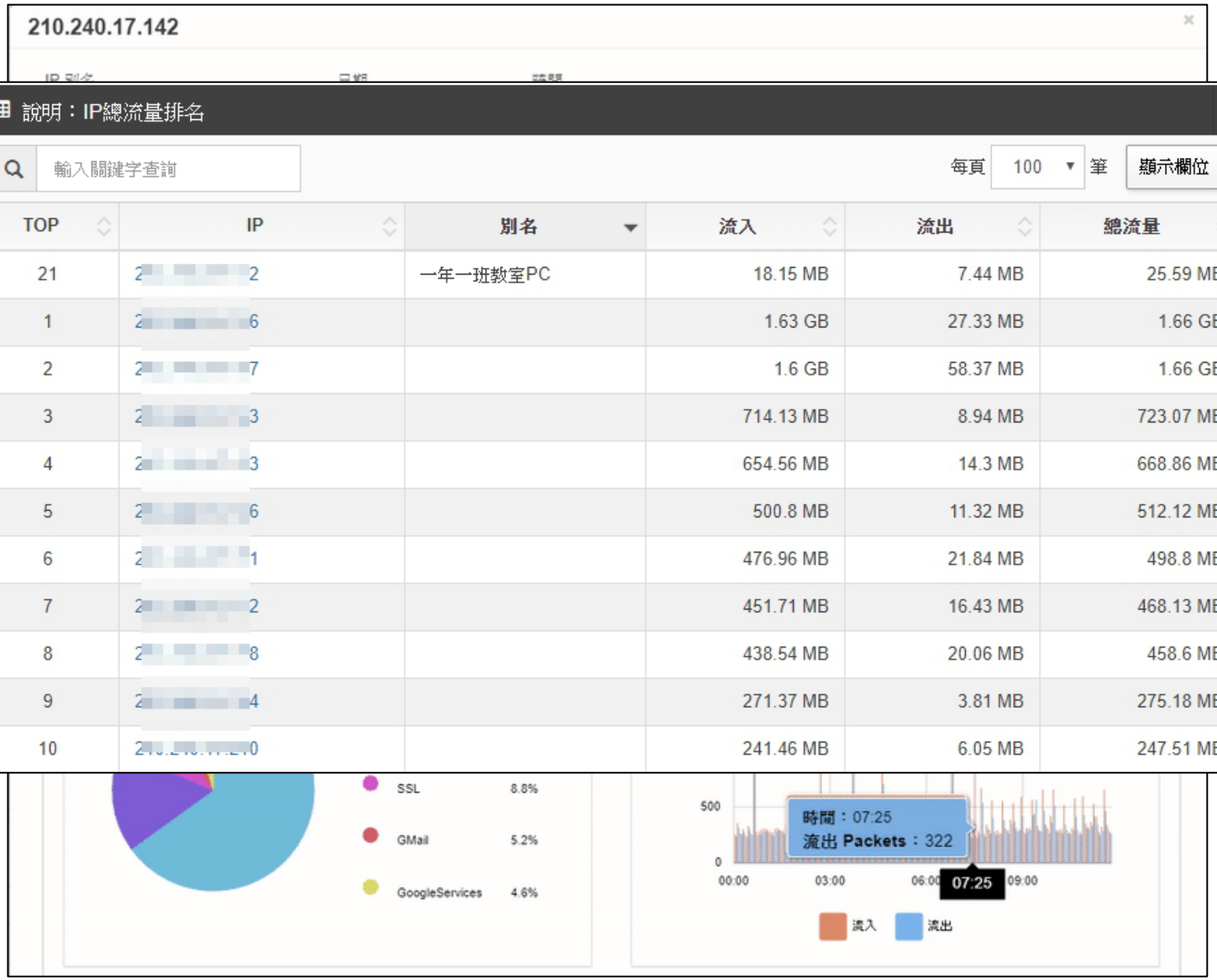
單位環境中的Core Switch的uplink port流速圖表資



IP分析/封鎖/風險評估

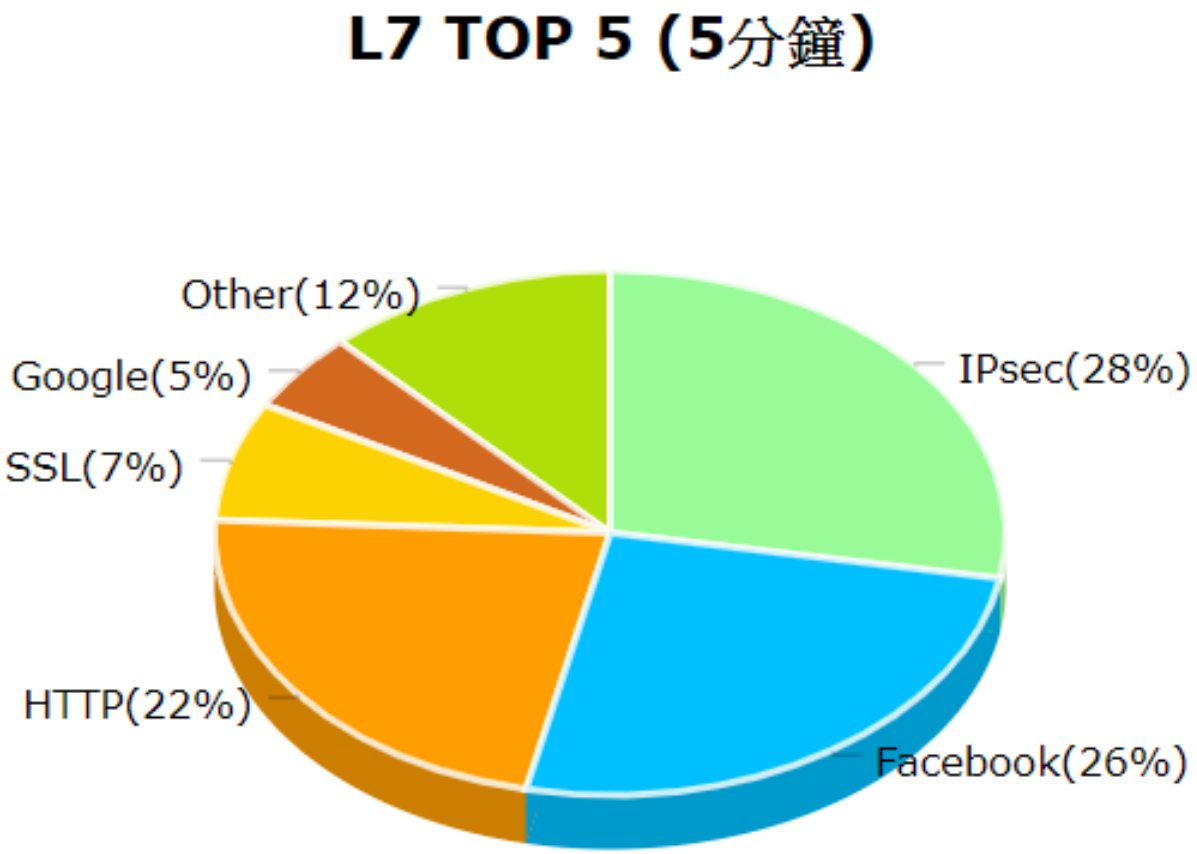

校內流量 TOP 10
TOP
IP
風險
IP 別名
日期
2019-10-30
時間
00:00
23:59
IP 資訊
Flow Top 10
Syslog
風險燈號 低風險
IP 註冊資訊
國家
TW
組織
Taipei Taiwan
163.22.
2020-03-23
當日Flow來源總筆數：244,882,173 筆
總流量 ：971.76 MB
IP 數 ：1156 個
Flow 筆數 ：51,068 筆
Sum
Country
Top 10 Percent%
1 152.19 282.28 MB United States 33.1%
2 163.28
3 163.28
4 210.24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

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

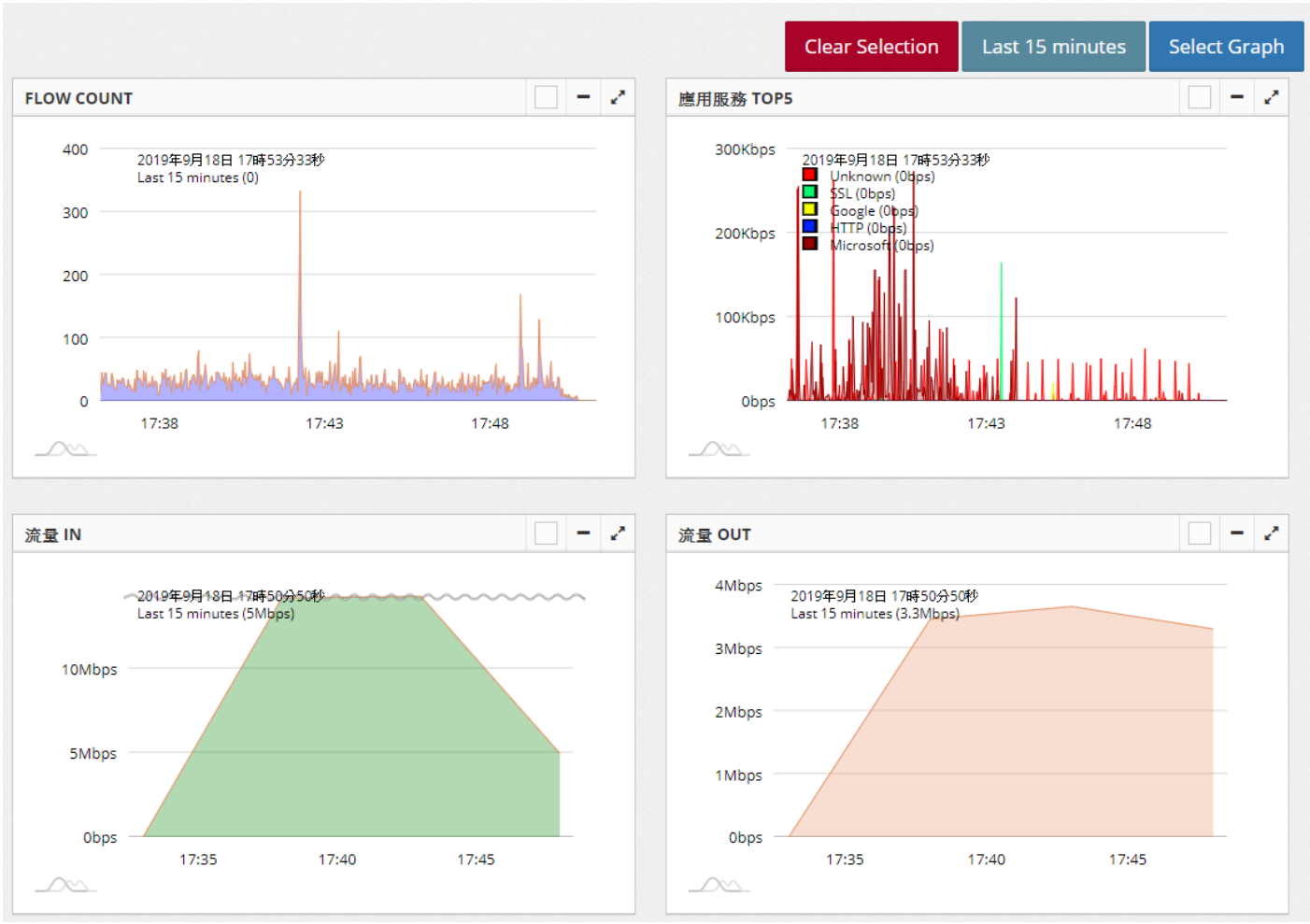
第七層服務前五名分析，針對整體流量進行第七層分析，並以圓餅圖呈現。



Flow分析

綜觀 ➔ Flow分析

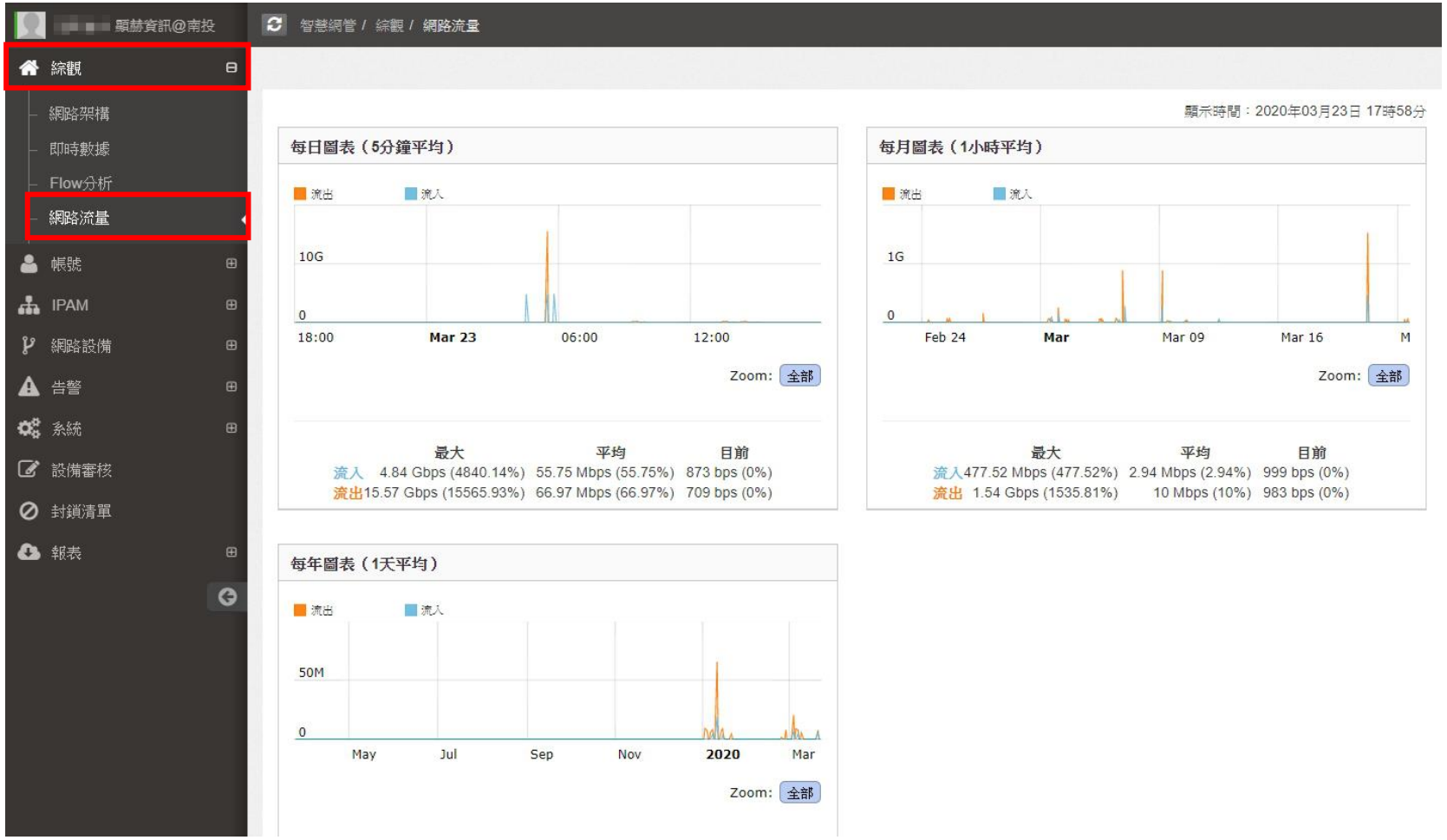
本校IP流量圖表分析總覽/流量資訊排名/圖表式佔比，圖表可作區間放大。



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)。



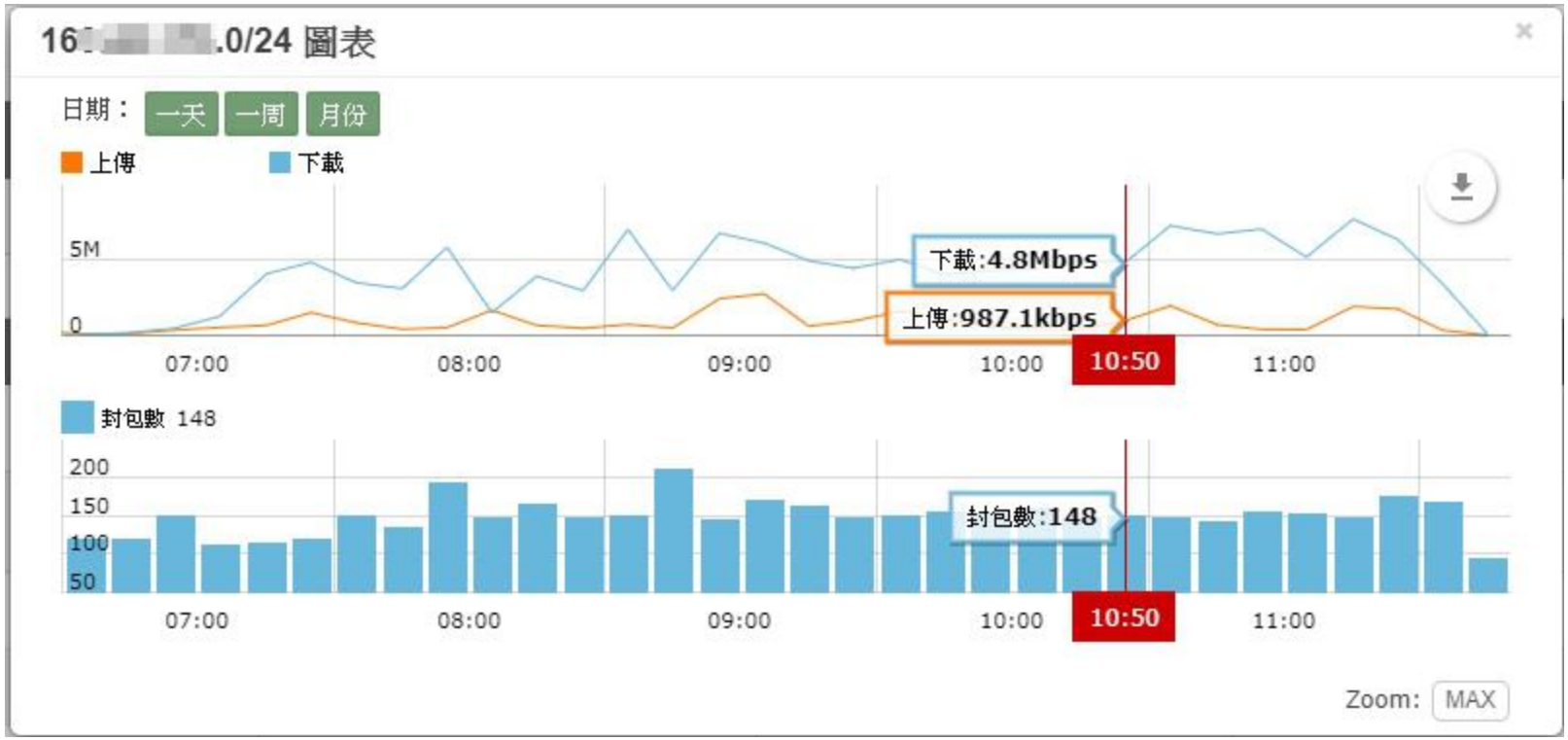
IPAM

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。

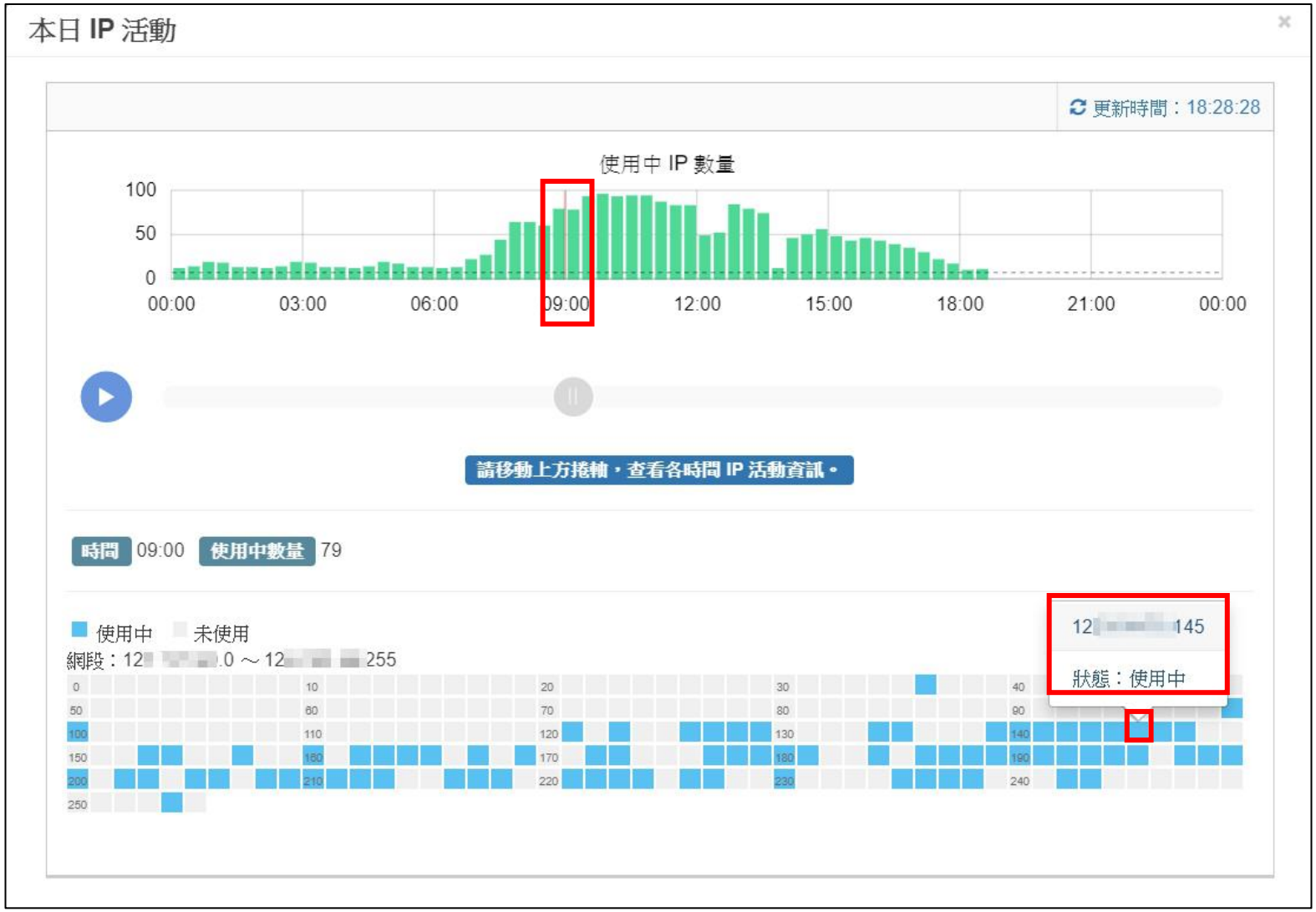
IPAM

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？

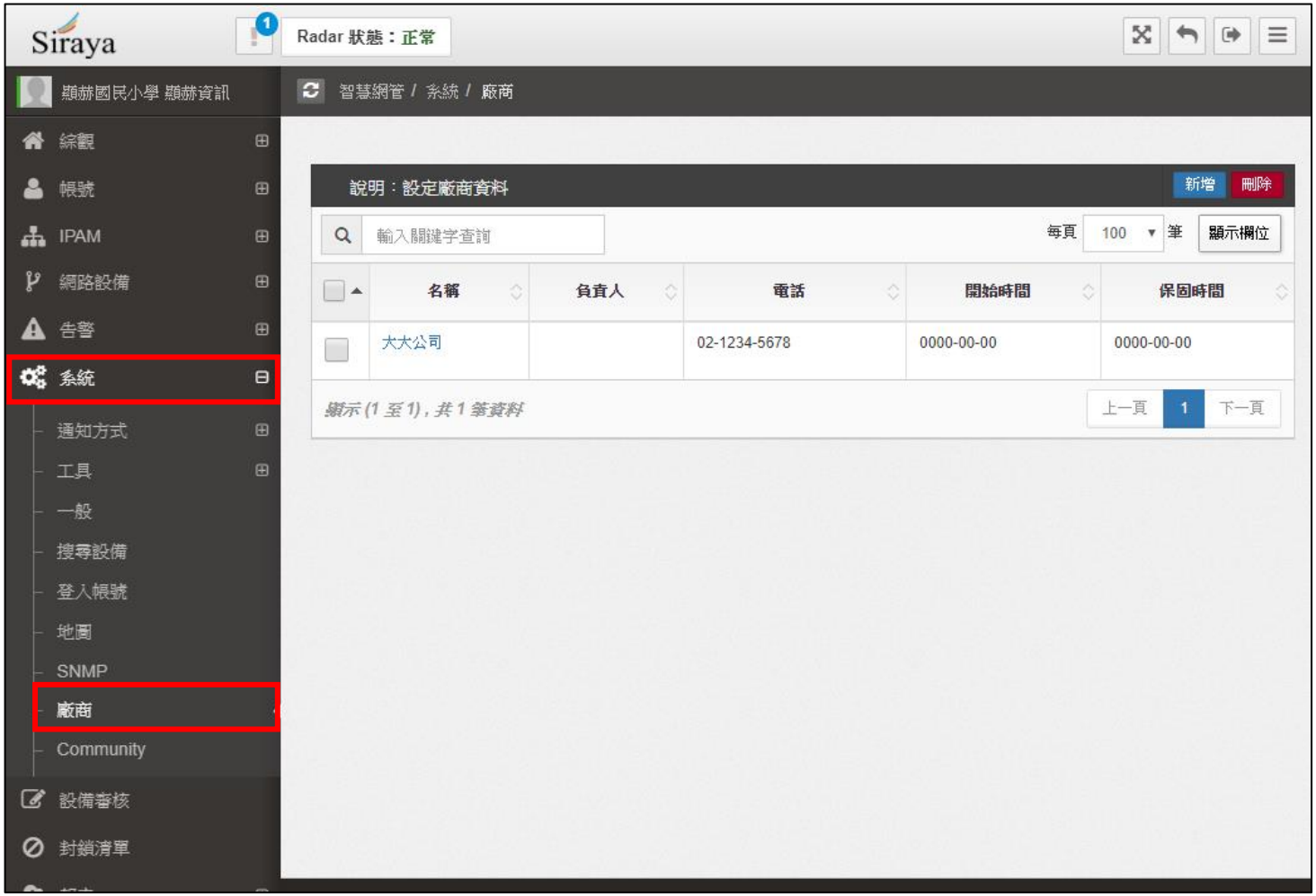
臨時找不到可用 IP，可於系統查找一個月內未使用的 IP，來使用。

IP 未妥善紀錄
臨時也不知道哪一組可以使用?

廠商

系統➔ 廠商

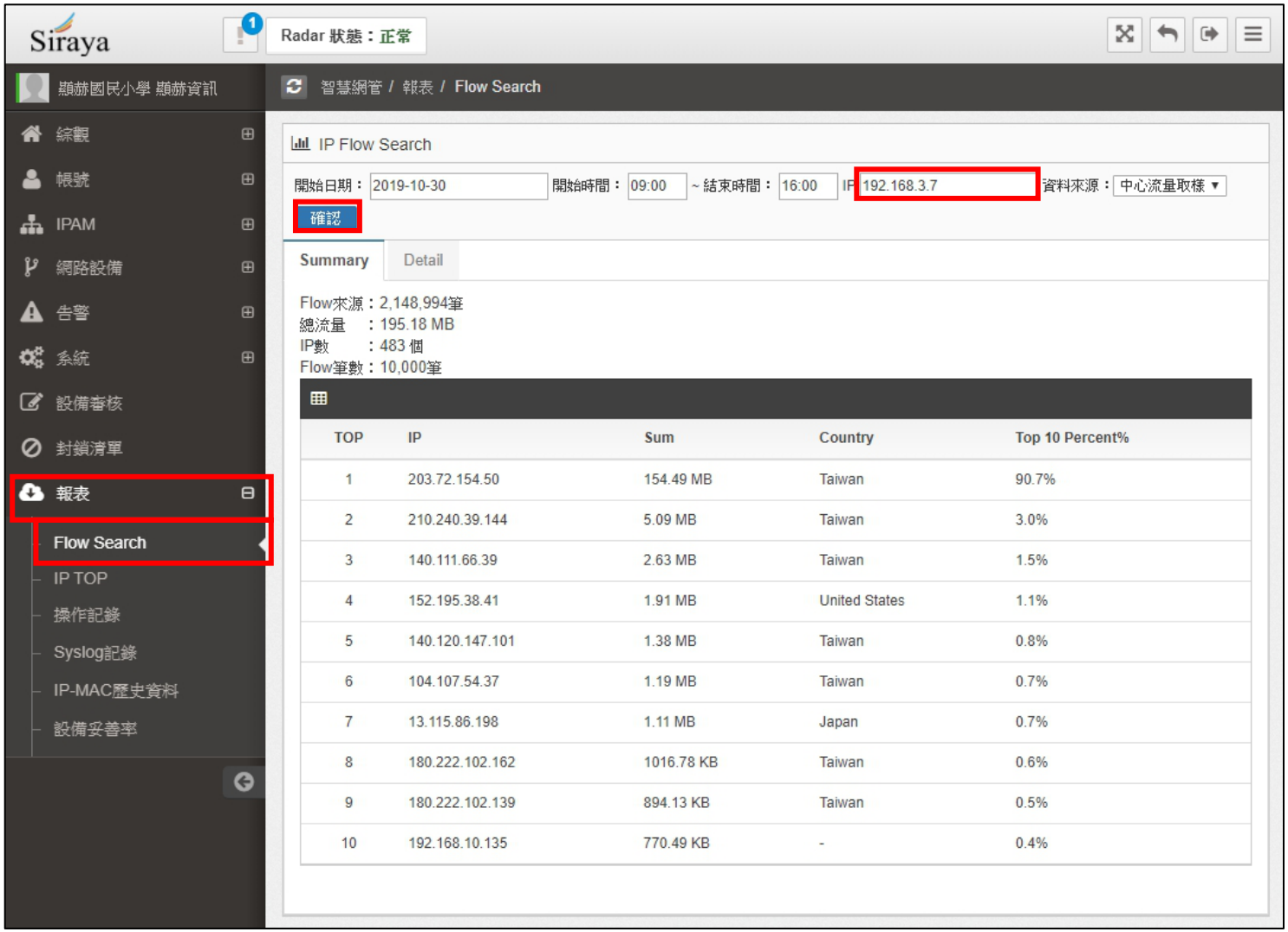
老師可將維護設備廠商資訊在此新增，可於每次增購設備中，選擇相對應的廠商資料。



報表

報表➔ FlowSearch

可於此搜尋整個系統內存的IP資訊。

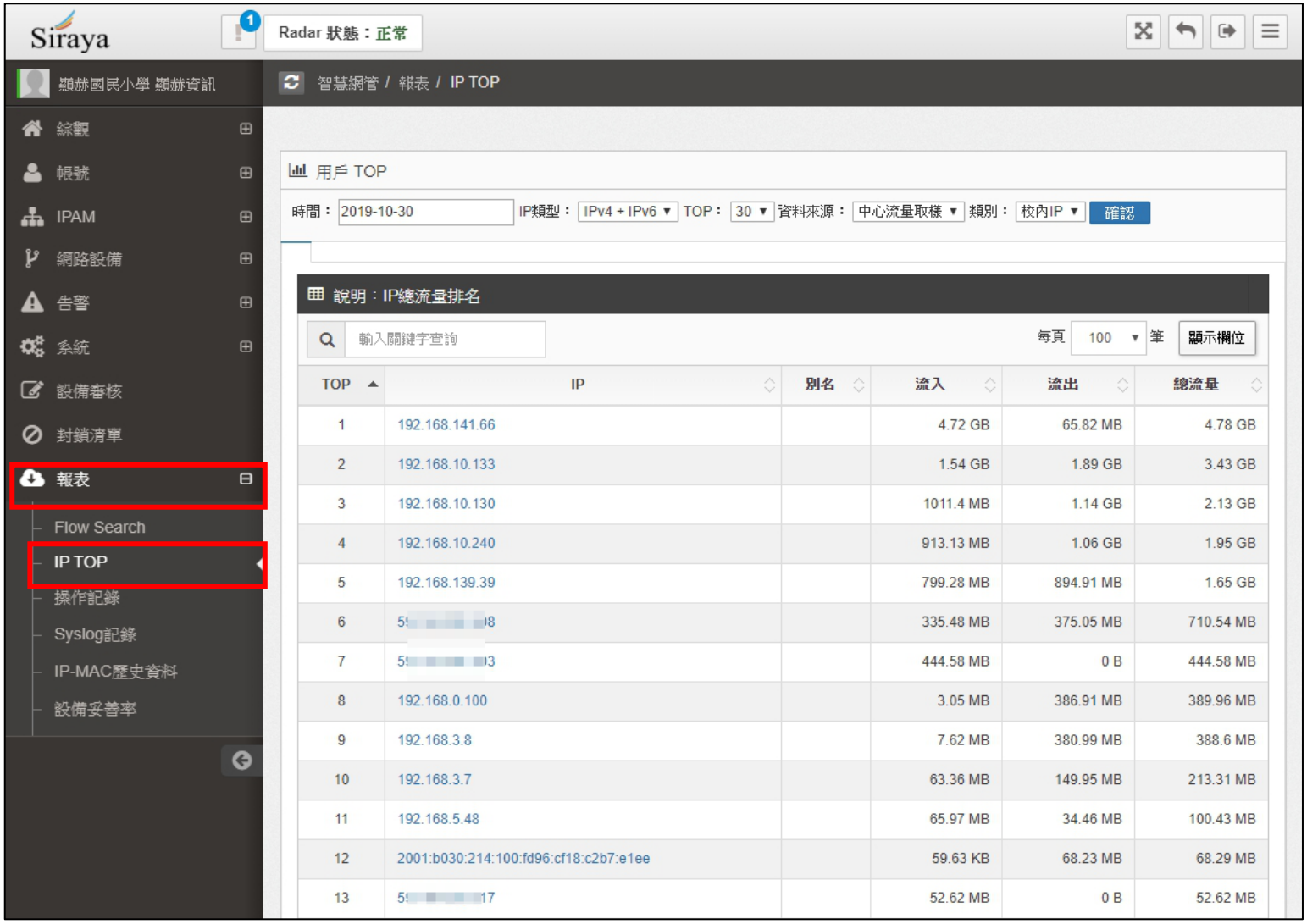


TOP	IP	Sum	Country	Top 10 Percent%
1	203.72.154.50	154.49 MB	Taiwan	90.7%
2	210.240.39.144	5.09 MB	Taiwan	3.0%
3	140.111.66.39	2.63 MB	Taiwan	1.5%
4	152.195.38.41	1.91 MB	United States	1.1%
5	140.120.147.101	1.38 MB	Taiwan	0.8%
6	104.107.54.37	1.19 MB	Taiwan	0.7%
7	13.115.86.198	1.11 MB	Japan	0.7%
8	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。

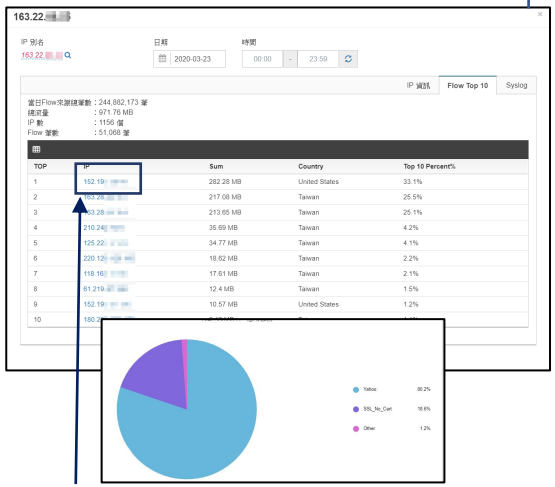
判斷IP危險程度

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

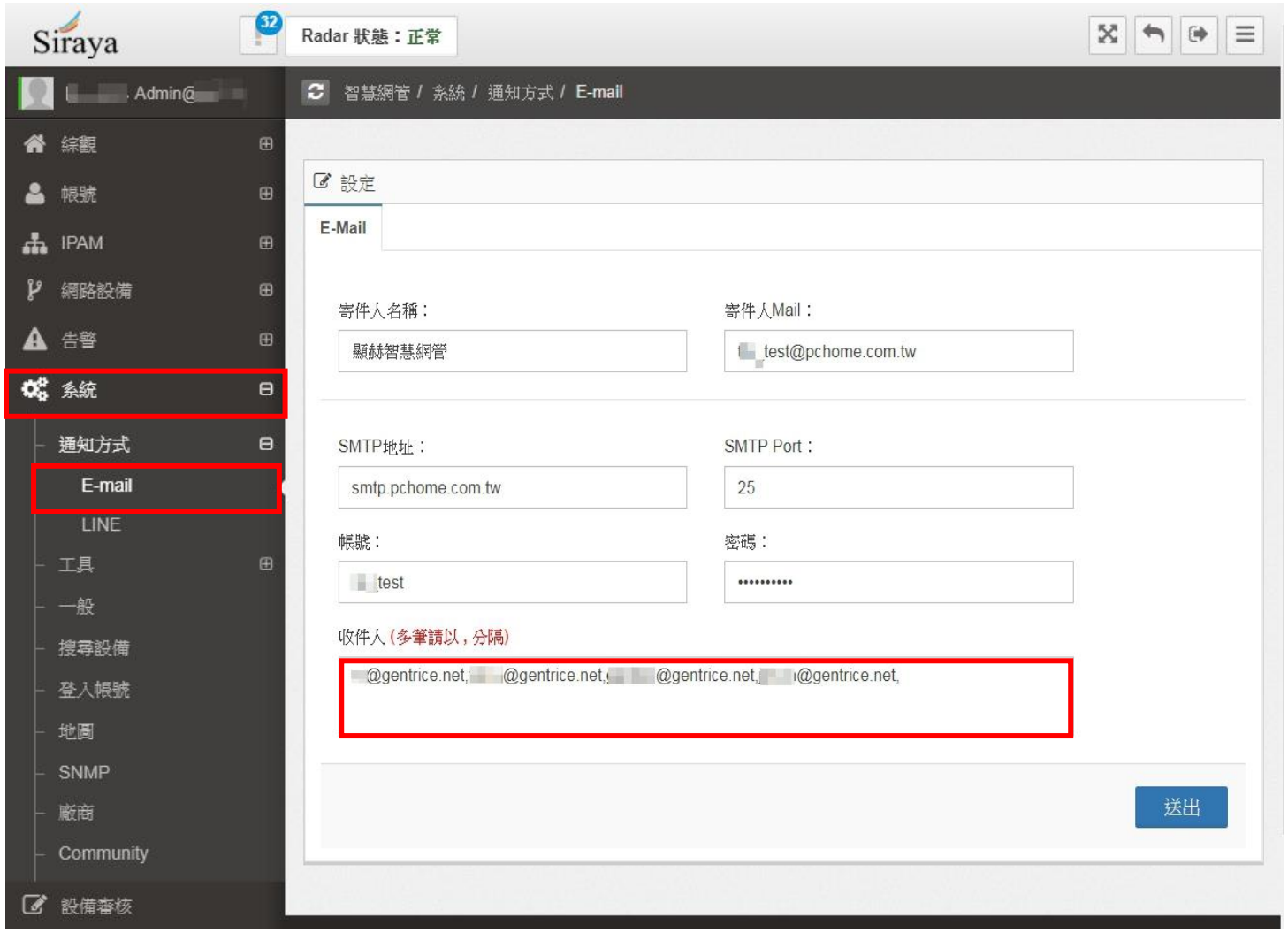


其他功能說明

通知方式

系統 ➔ 通知方式 ➔ E-mail

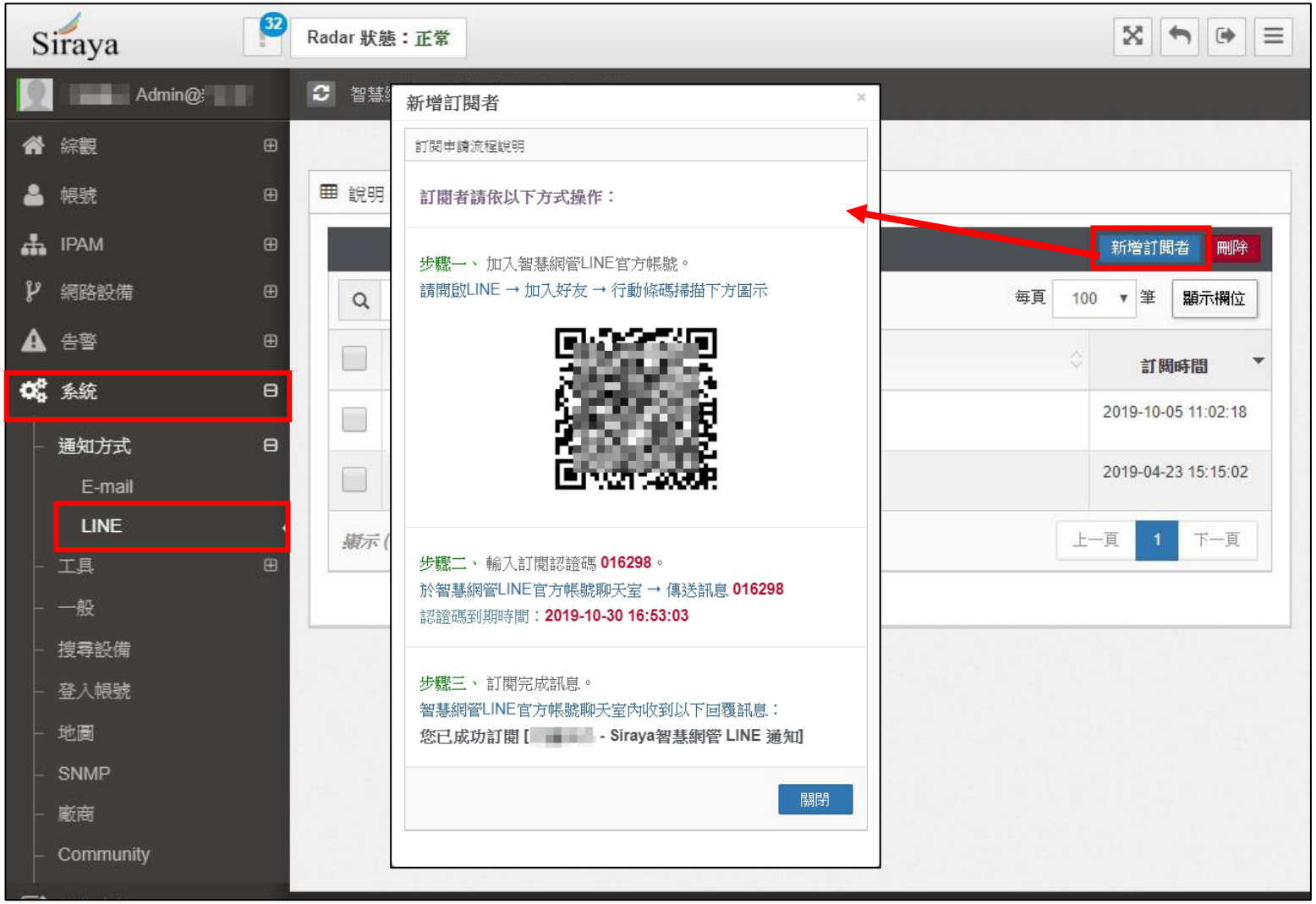
可設定SMTP位置，支援警示訊息使用Email通知管理者。



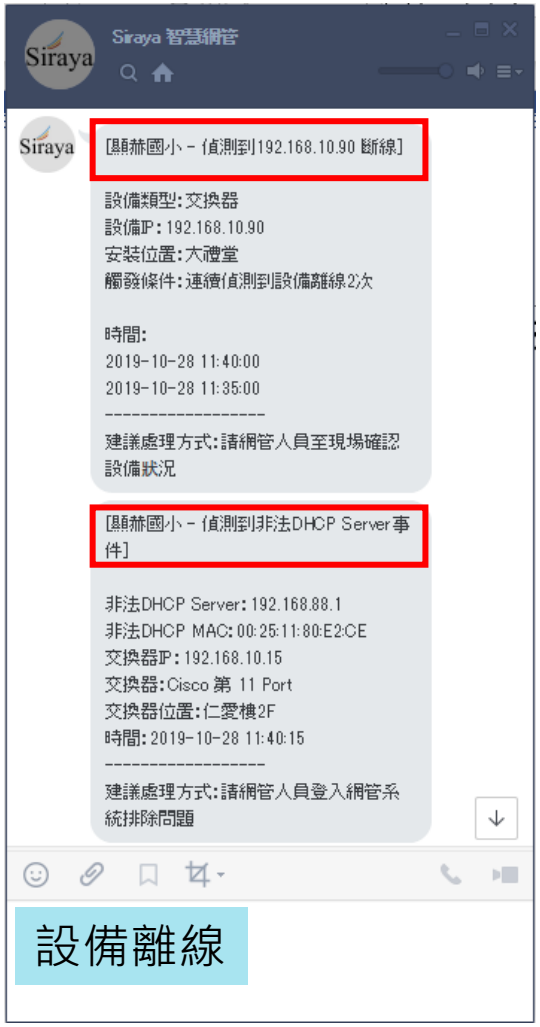
通知方式

系統 ➔ 通知方式 ➔ LINE

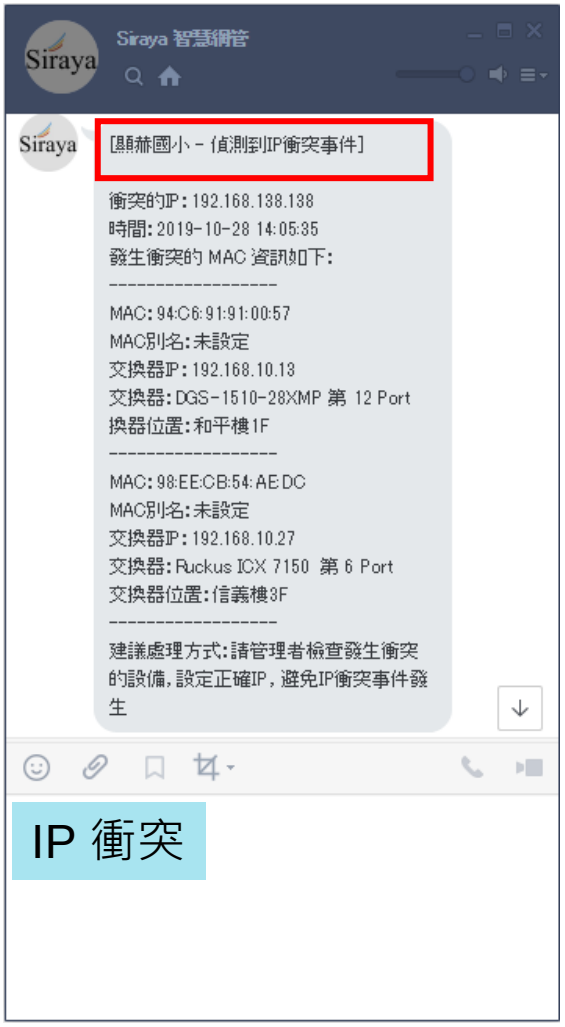
訂閱Line帳號,即可從Line立即接收學校告警的事件訊息。



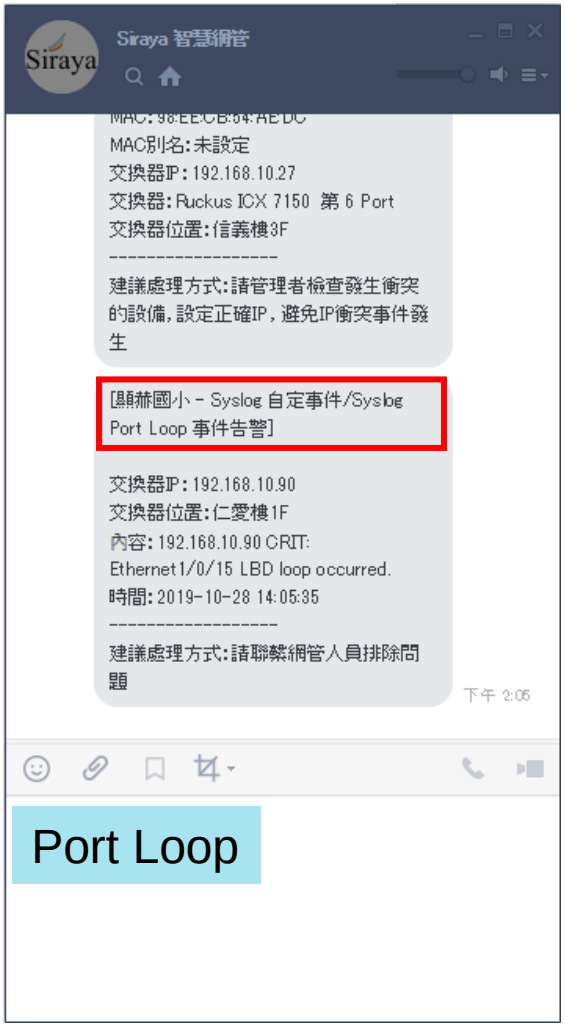
告警通報



設備離線



IP 衝突



Port Loop

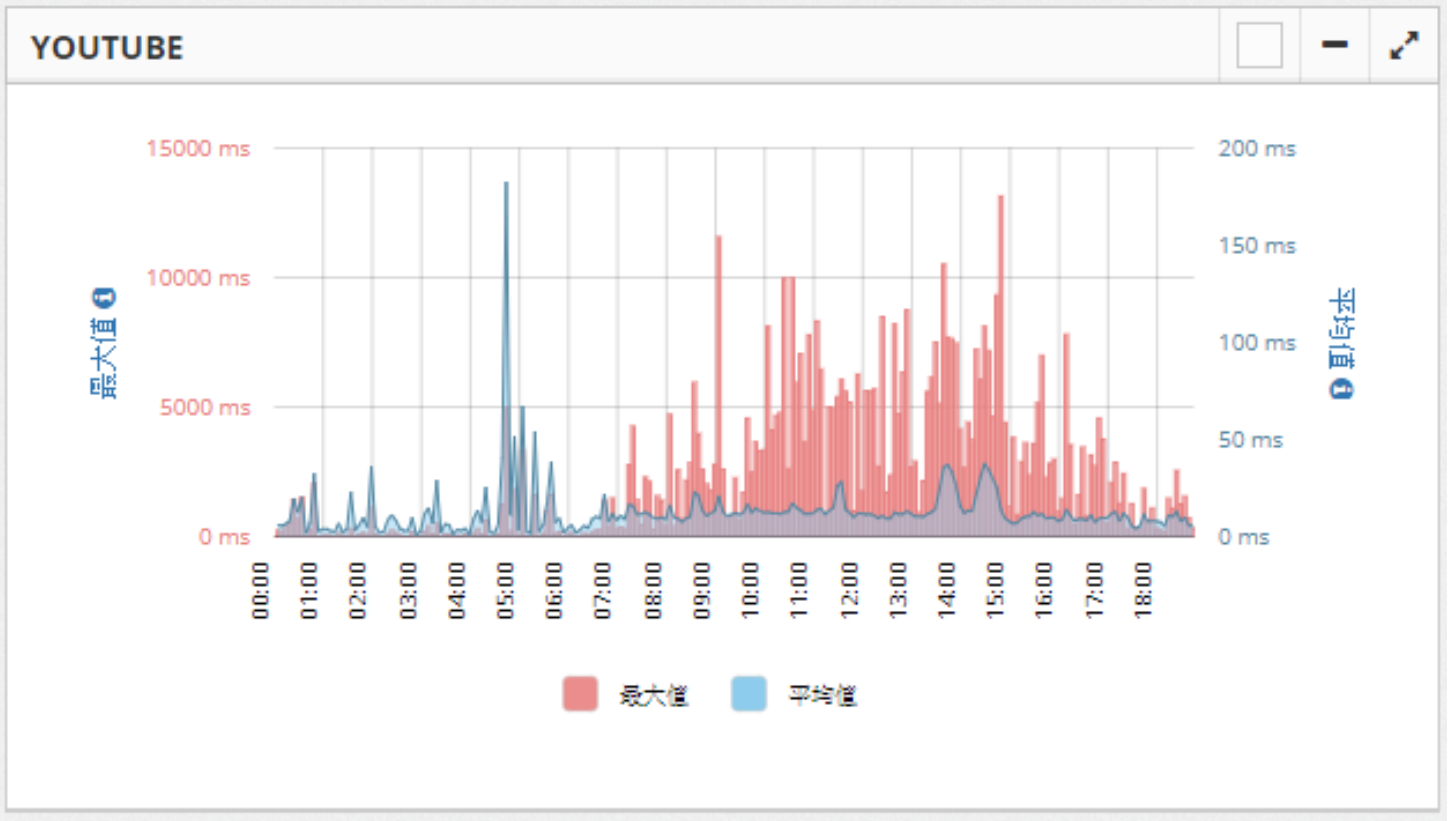
非法 DHCP Server

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。

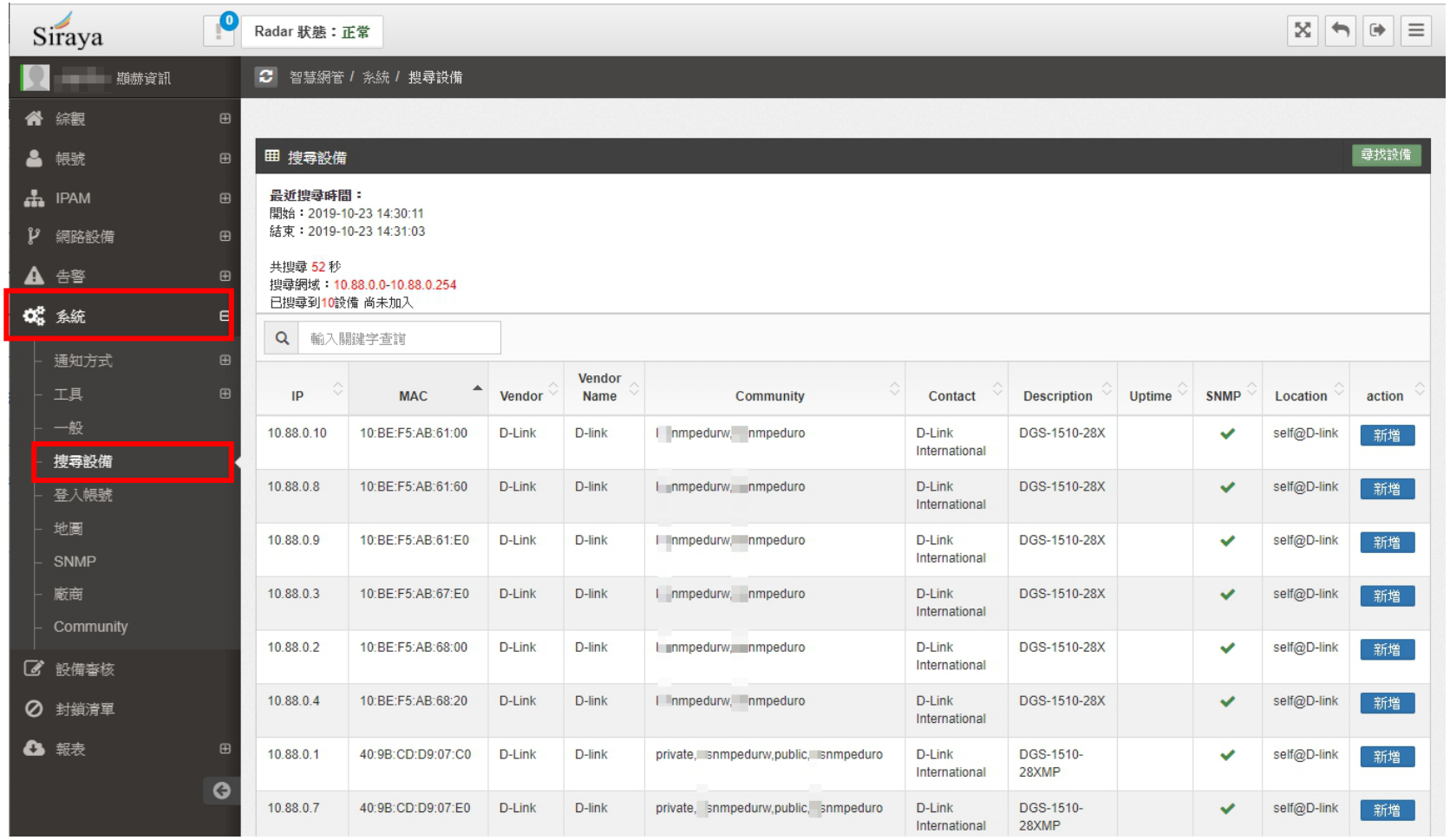
重要服務監測


YOUTUBE
15000 ms
10000 ms
5000 ms
0 ms
最大值
200 ms
150 ms
100 ms
50 ms
0 ms
平均值
00:00
01:00
02:00
03:00
04:00
05:00
06:00
07:00
08:00
09:00
10:00
11:00
12:00
13:00
14:00
15:00
16:00
17:00
18:00
最大值
平均值

搜尋設備

系統 ➔ 搜尋設備

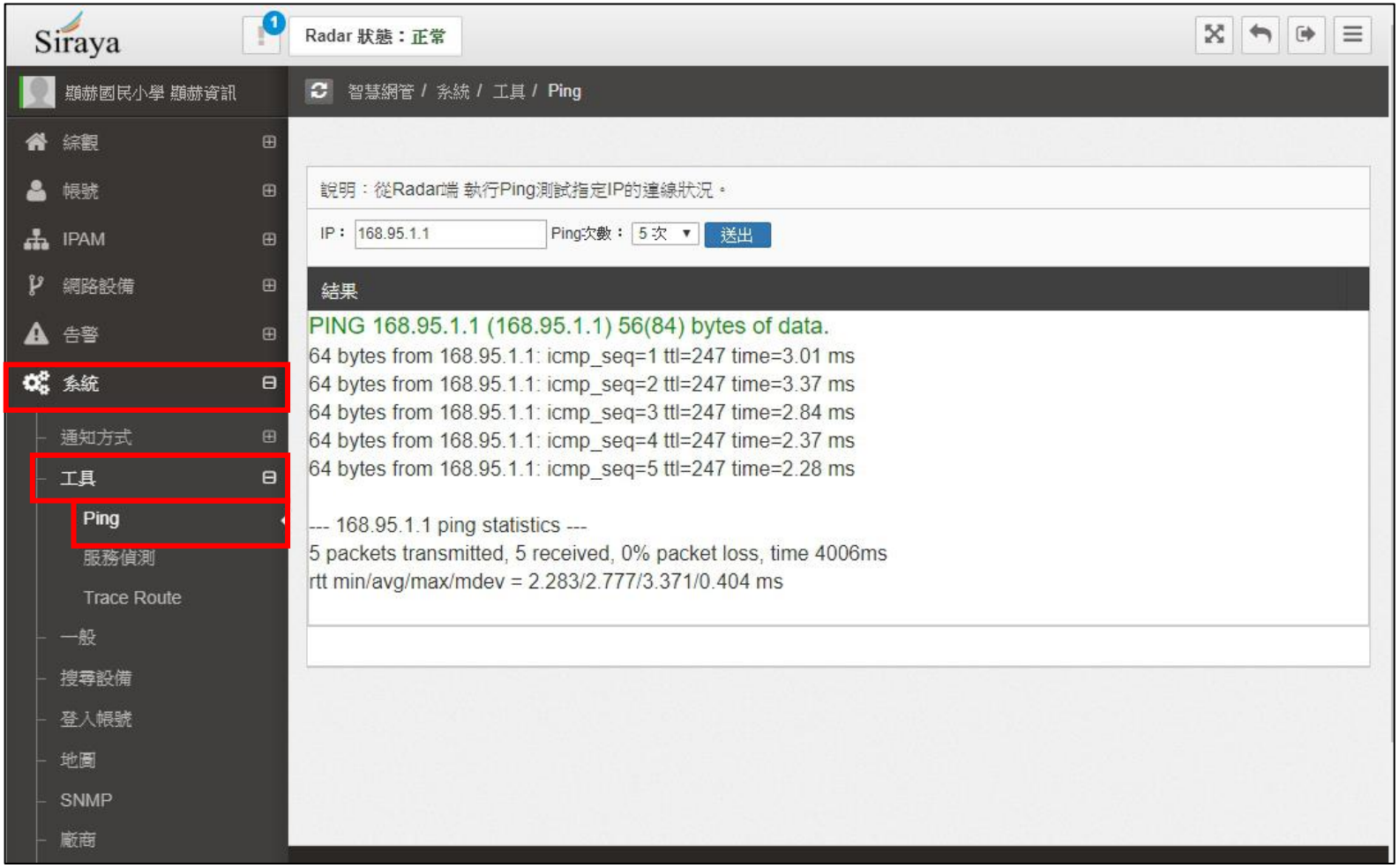
對網段內的資料找尋設備並納管。



Ping

系統 ➔工具 ➔ Ping

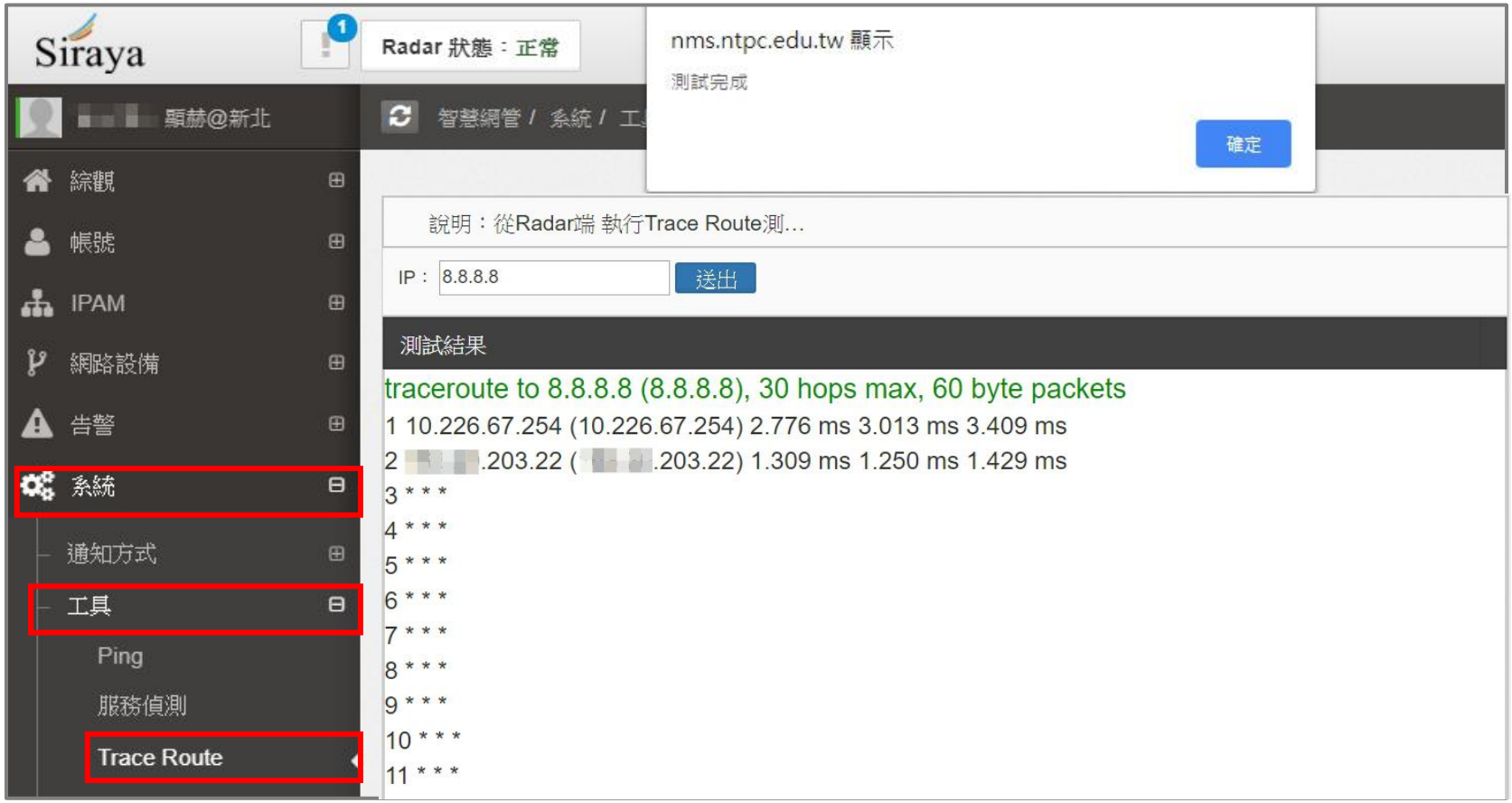
提供小工具，由學校端的雷達設備進行Ping，能自行確認由此雷達端點，至各個端點的網路狀況。



Trace Route

系統 ➔工具 ➔ Trace Route

提供小工具，由學校端的雷達設備進行Trace Route，能自行確認由此雷達端點，至各個端點的網路狀況。



服務偵測

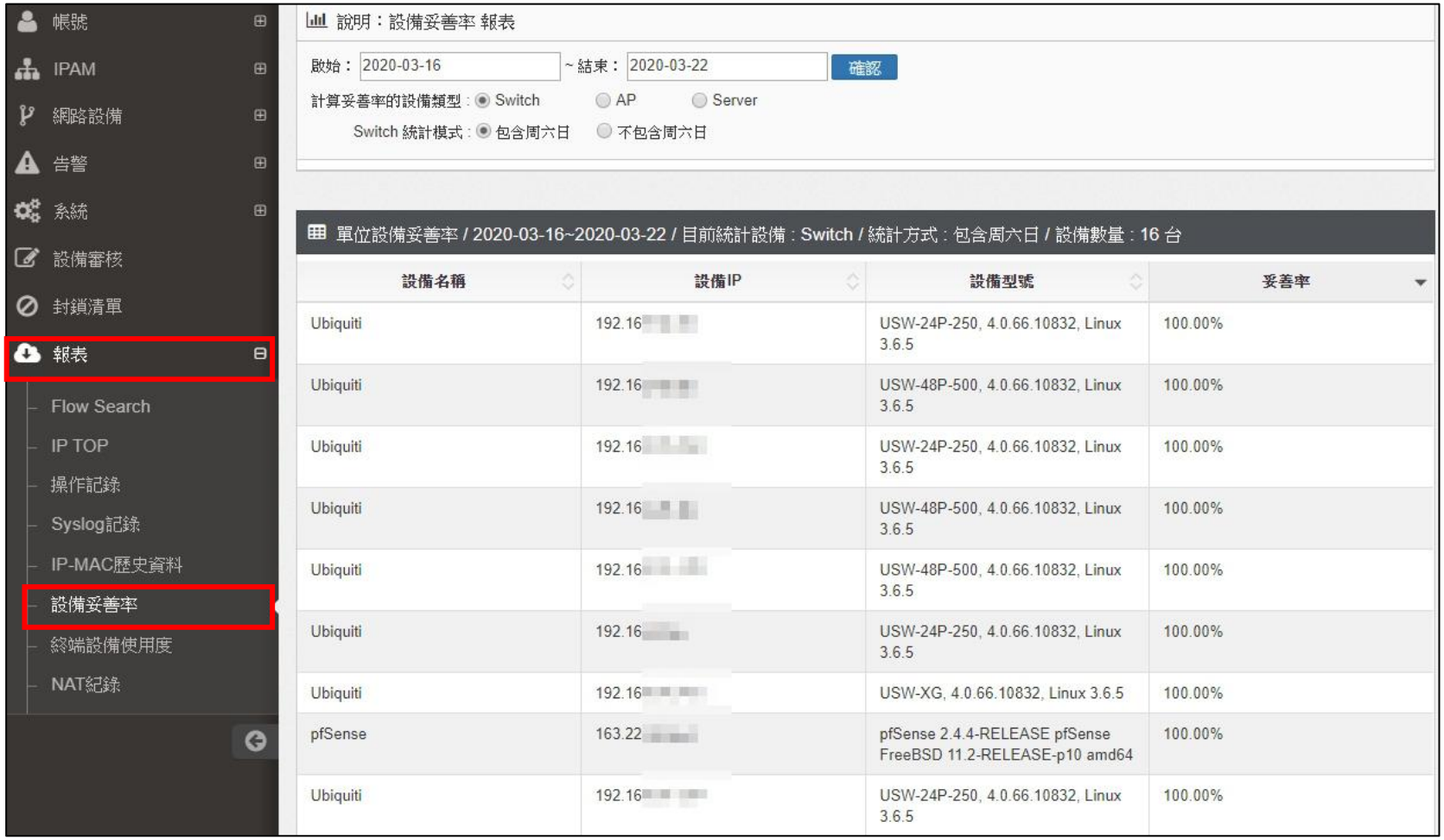
系統 ➔工具 ➔ 服務偵測

透過智慧網管去抓取偵測對象流量，來反應該服務的速度。

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。



02

實機演練

03

QA時間