

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

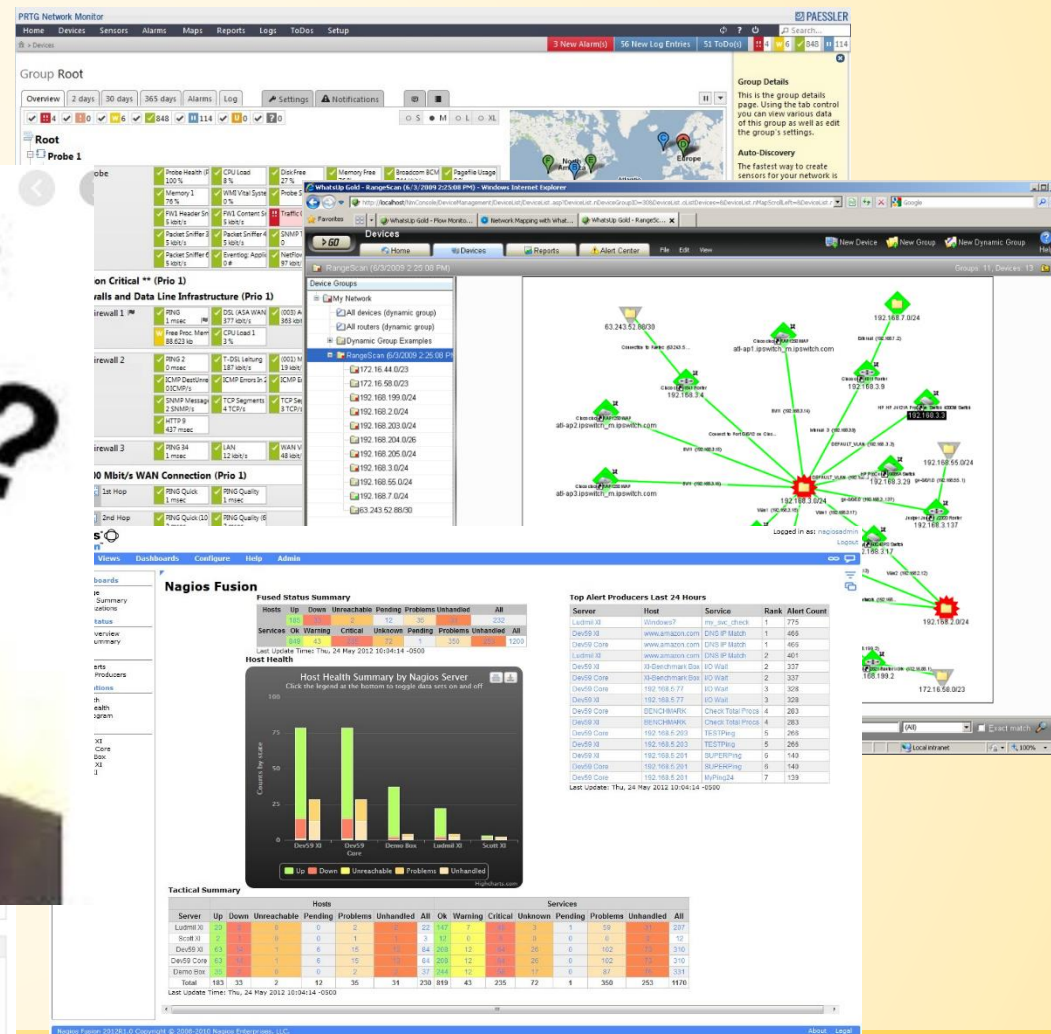
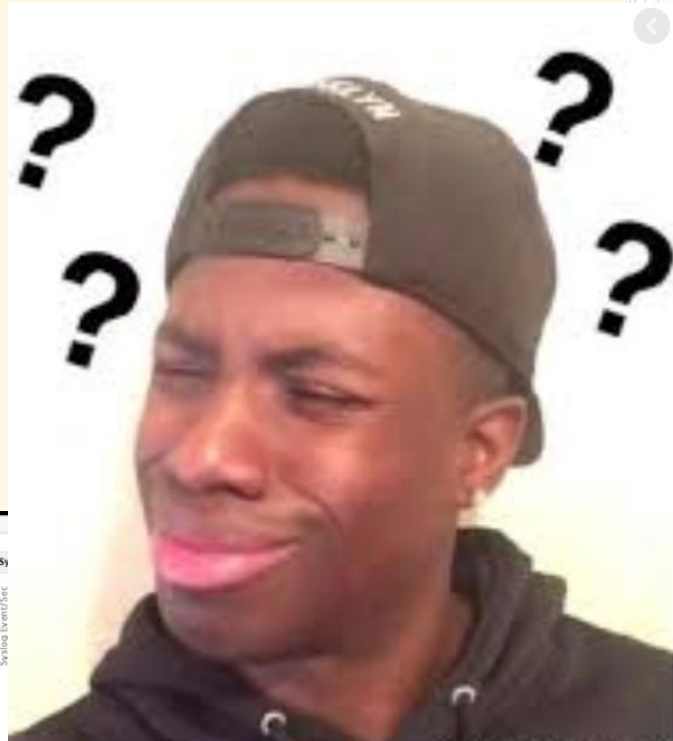
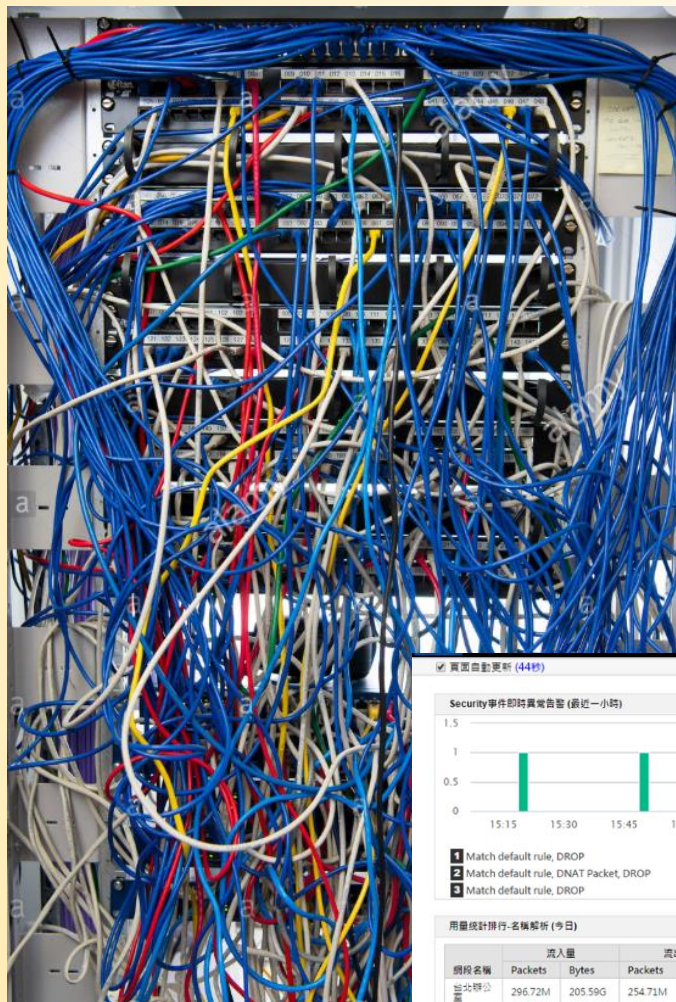
- 加註設備所在位置
- 尋找與加入設備：手動新增、搜尋新增

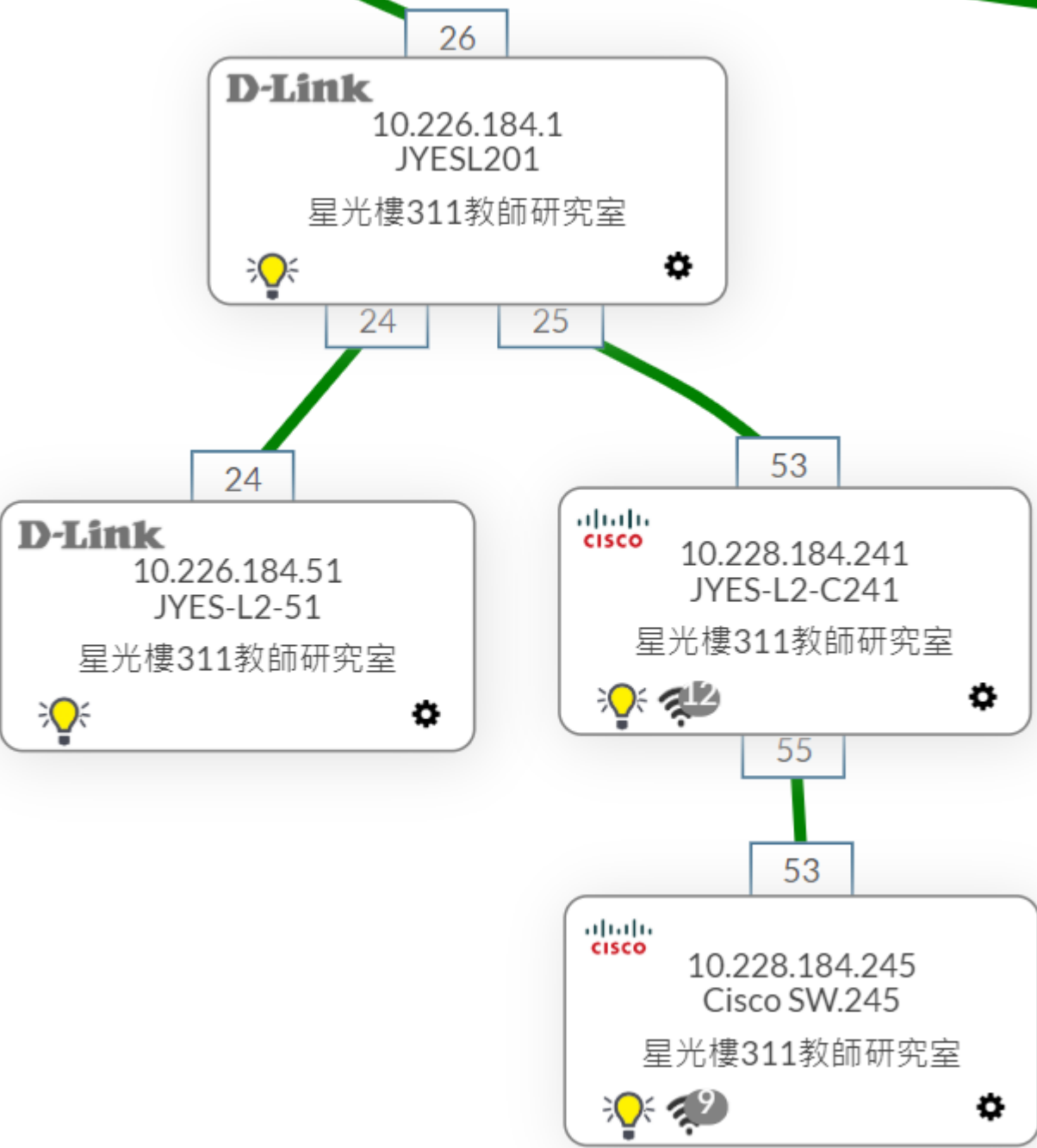
■監控與追蹤管理設備

■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？是做什么用的？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
10.226.184.3
JYESL203
正義樓3樓管道間機櫃

🔦 📶 ⚙️

25

53

CISCO
10.228.184.242
JYES-L2-C242
正義樓3樓管道間機櫃

🔦 📶 ⚙️

54

53

CISCO
10.228.184.243
JYES-L2-C243
正義樓3樓管道間機櫃

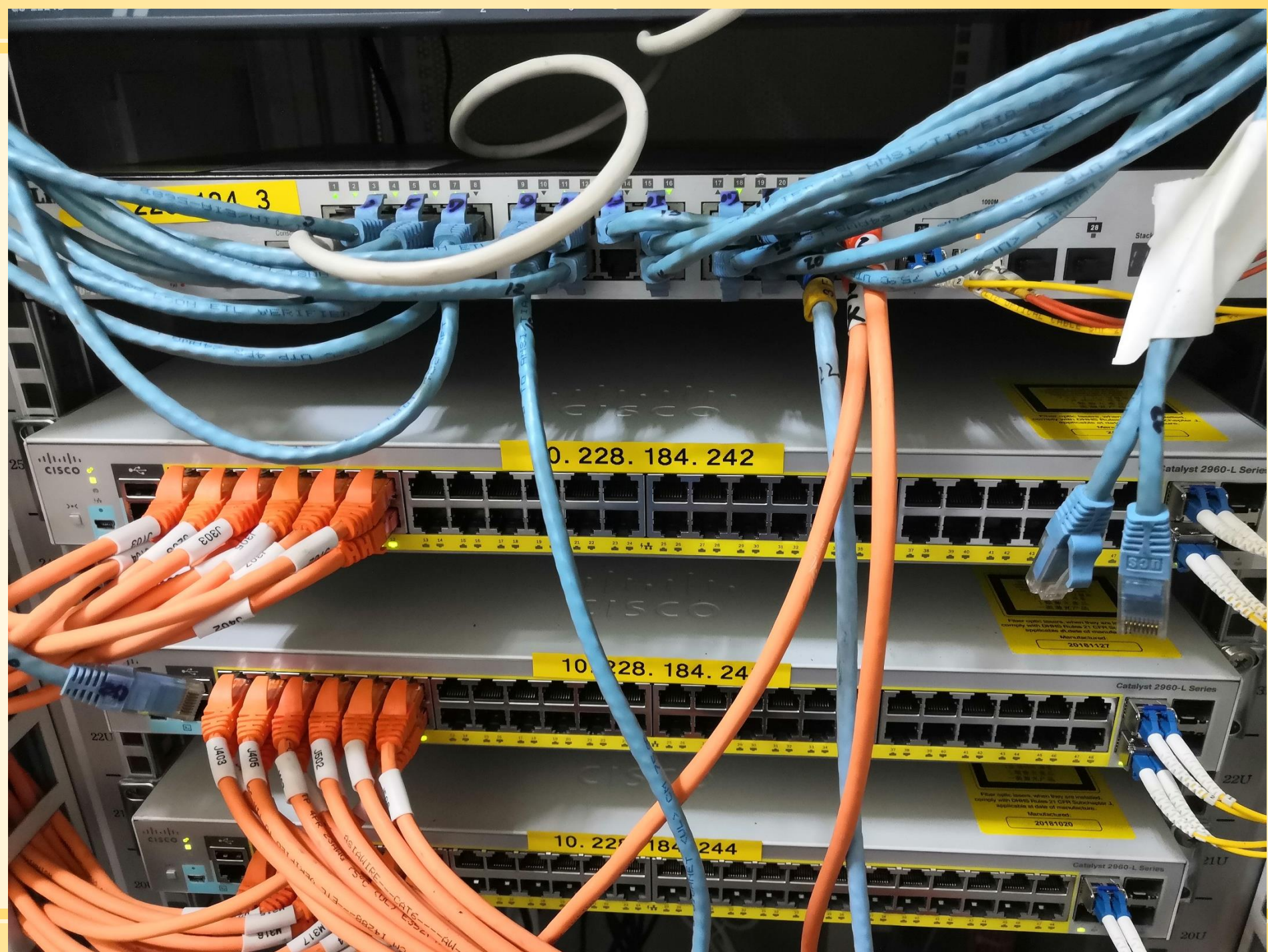
🔦 📶 ⚙️

54

53

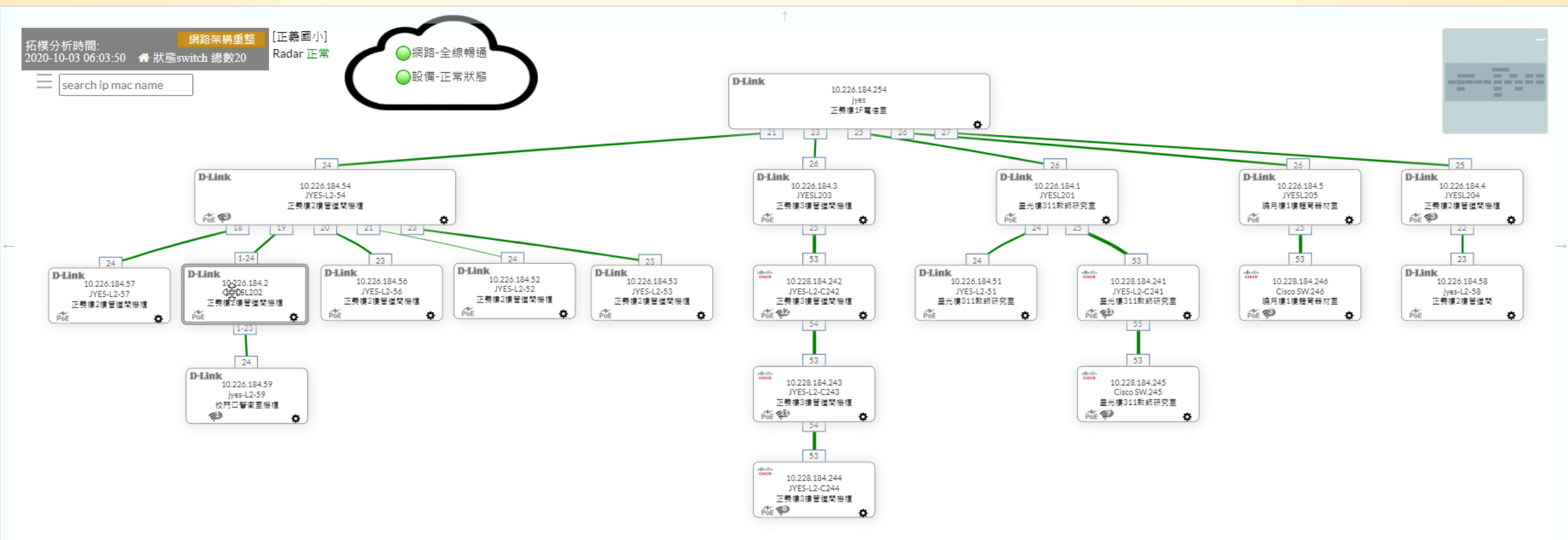
CISCO
10.228.184.244
JYES-L2-C244
正義樓3樓管道間機櫃

🔦 📶 8 ⚙️



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

The image shows a network management interface. On the left, a D-Link switch is displayed with the following information: IP address 10.226.184.1, model JYESL201, and location 星光樓311教師研究室. A red dashed arrow points from a gear icon in the bottom right corner of the switch to the configuration page on the right. The configuration page is titled 10.226.184.1 and has tabs for Information, Port, Vlan, Traffic, Client, and PoE. The Information tab is selected, showing details such as Switch Name: Dlink, Model: DGS-1510-28XMP, IP: 10.226.184.1, and Uptime: 運作時間: 58 days, 17:28:40.06.

10.226.184.1

Information	Port	Vlan	Traffic	Client	PoE
Information					
Switch Name : Dlink					
Model : DGS-1510-28XMP			IP : 10.226.184.1		
運作時間 : 58 days, 17:28:40.06					
Block MAC : 0					

- 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

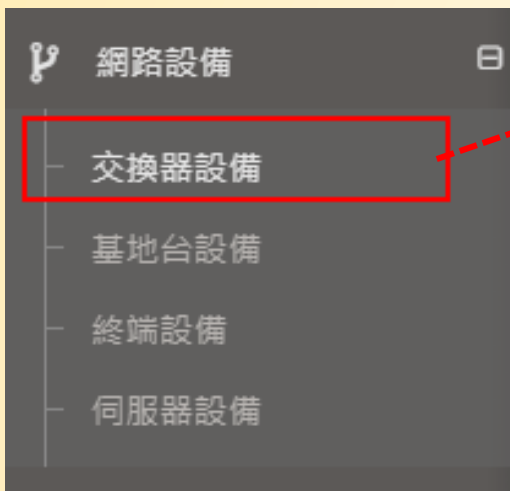
機型：DGS-1210-24P

I P：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:

A screenshot of the configuration form for a device named 'jyes-L2-59'. The form has a title bar 'jyes-L2-59' and a tab '編輯' (Edit). The '一般' (General) tab is selected. The form contains several fields: '設備名稱' (Device Name) with value 'jyes-L2-59', '型號' (Model) with value 'DGS-1210-24P', '廠牌' (Manufacturer) with a dropdown showing 'Dlink', '設備IP' (Device IP) with value '10.226.184.59', '次要IP' (Secondary IP) with a placeholder '次要 IP', 'MAC' with a button '偵測MAC' and value '80268948F758', '類別' (Category) with a dropdown showing 'L2 SW', '屬性' (Property) with a dropdown showing '一般', '位置' (Location) with a text input field containing '校門口警衛室機櫃' (highlighted with a red box), '備註' (Remarks) with a text input field containing '備註', 'Version' with a dropdown showing 'v2c', 'Read Community' with a dropdown showing 'pub*****', and 'Read/Write Community' with a dropdown showing 'pri*****'. At the bottom right are buttons '送出' (Submit) and '取消' (Cancel).

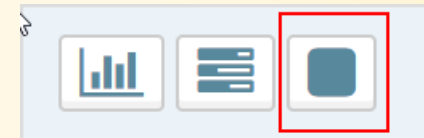
2.現在有哪些設備在使用中呢？

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

本日 IP 使用度



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。

新增區段

編輯

網段範圍過大,在系統搜尋設備或分析上容易造成資料超載錯誤. 建議每個網段設定在256個IP內.

區段名稱

名稱

IPv4

IPv6

啟用IP

結束IP

起始IP

結束IP

Vlan ID

Vlan ID

送出

取消

自訂網段

資料來源：

新增

刪除

每頁 100 顯示欄位

	區段名稱	IP 區段	流入 (Bytes)	流出 (Bytes)	流入 (Packets)	流出 (Packets)	功能
☐	10.241.56.0/24	10.241.56.1-10.241.56.254	0 B	0 B	0	0	
☐	10.233.56.0/24	10.233.56.1-10.233.56.254	0 B	0 B	0	0	
☐	10.231.56.0/24	10.231.56.1-10.231.56.254	0 B	0 B	0	0	

顯示 (1 至 3), 共 3 筆資料

上一頁

1

下一頁

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.

The screenshot displays the Siraya network management interface. On the left, a sidebar menu shows '交換器設備' (Switch Equipment) highlighted. The main area shows a table of existing switch equipment with columns for '名稱' (Name) and '型號' (Model). A vertical black bar obscures the '名稱' column. The '新增名稱' (Add Name) dialog box is open on the right, showing fields for '設備名稱' (Device Name), '型號' (Model), '廠牌' (Manufacturer), '設備IP' (Device IP), '次要IP' (Secondary IP), 'MAC' (with a '偵測MAC' button), '類別' (Category), '屬性' (Property), '位置' (Location), '備註' (Remarks), 'Version', 'Read Community', and 'Read/Write Community'. The '送出' (Submit) and '取消' (Cancel) buttons are at the bottom right.

名稱	型號
Forti300c	Forti300c
DGS-3620-28TC	DGS-3620-28TC
DGS-3627	DGS-3627
DGS3620	DGS3620
checkpoint	checkpoint
checkpoint	checkpoint
DGS-1510-28XMP	DGS-1510-28XMP
DGS-1510-28XMP	DGS-1510-28XMP
DGS-1510-28XMP	DGS-1510-28XMP
DGS-1510-28XMP	DGS-1510-28XMP
DGS-1510-28XMP	DGS-1510-28XMP

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.

The screenshot displays the '尋找設備' (Search Equipment) dialog box in a network management system. The main window shows the 'Radar 狀態：正常' (Radar Status: Normal) and the '智慧網管 / 系統 / 搜尋設備' (Smart Network Management / System / Search Equipment) path. The '搜尋設備' (Search Equipment) section displays search results, including the start and end times of the search (2020-09-15 10:08:58 to 2020-09-15 10:09:51), the search duration (53 seconds), the search range (10.226.56.0-10.226.56.255), and the number of devices found (5). Below this, there is a search bar and a table with columns for IP and MAC address. The '尋找設備' dialog box is open, showing the '選擇網域' (Select Domain) section with radio buttons for '網段清單' (Selected) and '自訂網段' (Custom). The '網段清單' option is selected, and the IP range '163.20.66.0/24' is entered. Below this, there are radio buttons for '網路設備(Switch、Router、AP、Server...)' (Network Equipment) and '一般設備(Host)' (General Equipment). The '一般設備(Host)' option is selected. The 'SNMP Community' section has radio buttons for 'ALL' and '自選' (Custom), with 'ALL' selected. A red box highlights the '網路設備(Switch、Router、AP、Server...)' option, and another red box highlights the '送出' (Send) button at the bottom right of the dialog box.

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 I P ，因此，必須先確認哪個實體 I P 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])



6	Port名稱	OFF	
7	地震預警系統	ON	

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	10.226.67.236	C8:DE:12:FF:FE: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。

☐	10.241.184.146	74:██████:93	Elitegroup	→ 教室電腦	4@JYESL203	新增
☐	10.241.184.147	74:2██████:E4	Elitegroup		11@JYES-L2-57	新增
☐	10.241.184.152	80:EE:72:E3:02:FE	Shuttle	→ 安卓主機	7@JYES-L2-57	新增
☐	10.241.184.163	80:██████:02:D8	Shuttle		2@JYES-L2-56	新增
☐	10.241.184.214	C0:██████:15:45:D8	Elitegroup		3@JYES-L2-51	新增

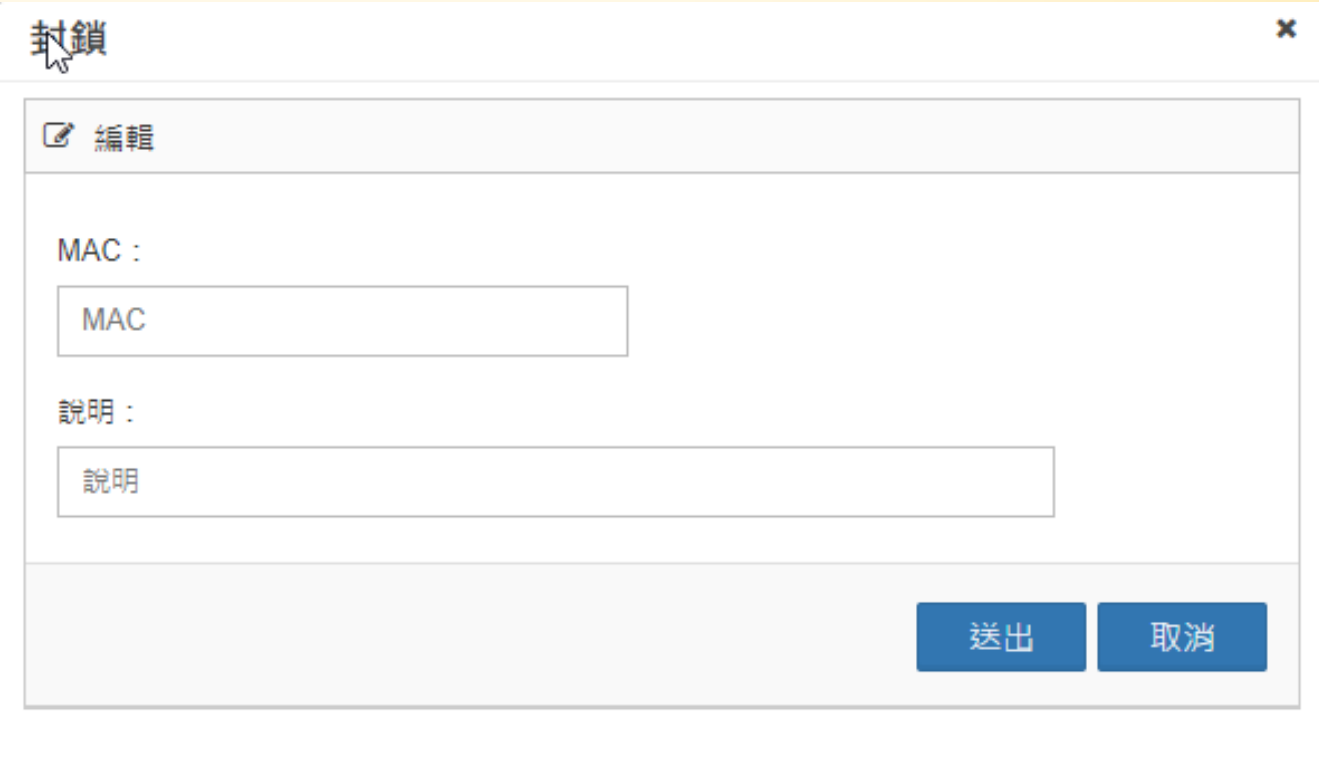
10.當收到局端告知某IP中毒或成為殭屍電腦時，該如何處理？

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

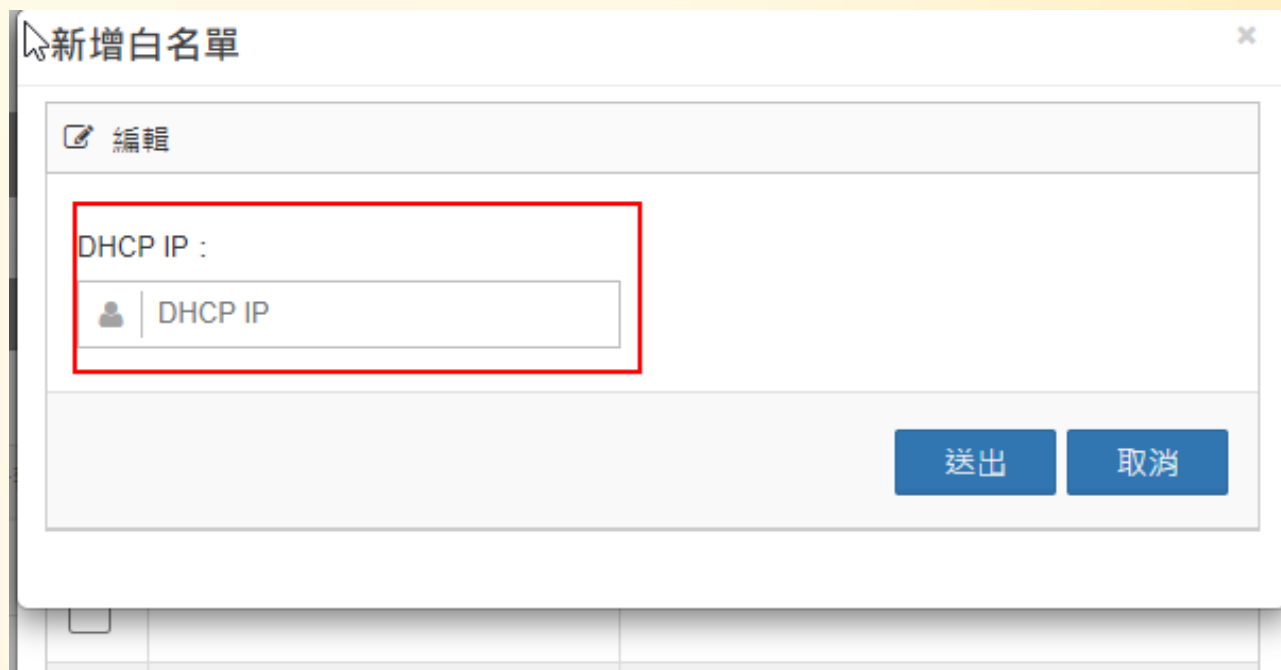


The screenshot shows a web-based interface for managing a blocklist. The title bar at the top says '封鎖' (Block) with a close button. Below the title bar is a tab labeled '編輯' (Edit) with a pencil icon. The main form area contains two input fields: 'MAC :' followed by a text box containing 'MAC', and '說明 :' followed by a larger text box containing '說明'. At the bottom right of the form are two buttons: '送出' (Submit) and '取消' (Cancel).

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]



新增白名單

編輯

DHCP IP :

DHCP IP

送出 取消

1 2.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 I P，則將其中一台 I P 調整即可，如果是交換器配發DHCP問題，則到 C C 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

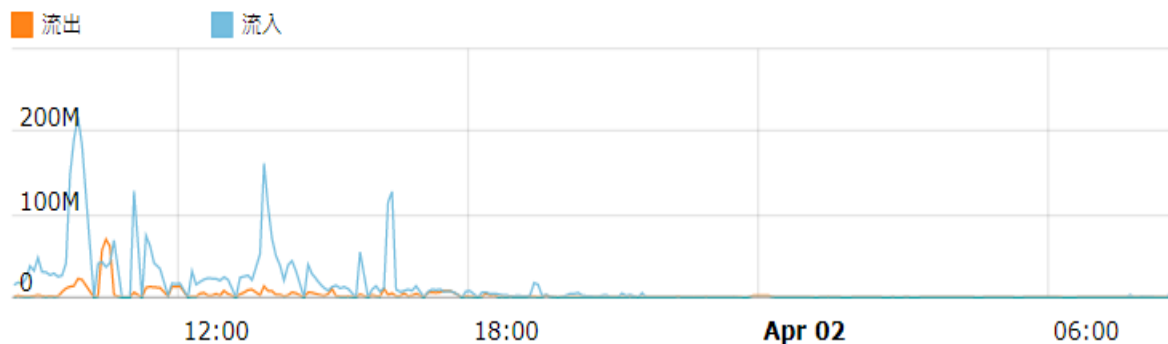
項目	佔據時間
校園網路管理	20%
教課與備課	50%
處理行政業務	30%

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

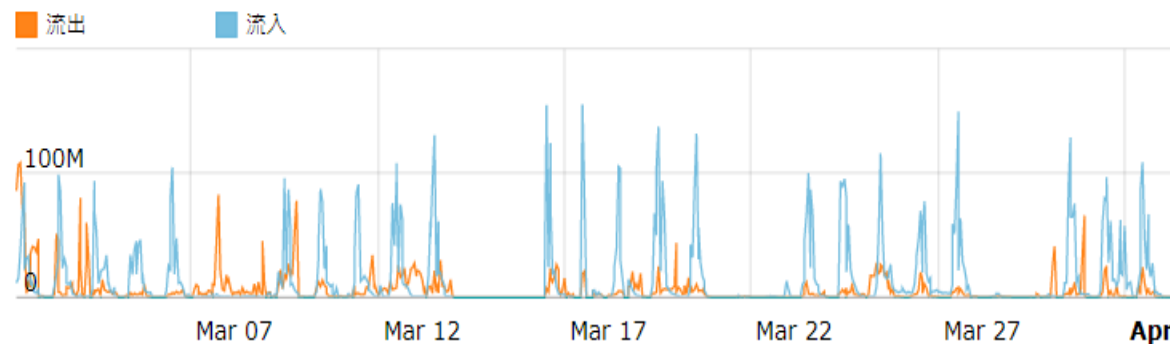
顯示時間：2020年04月02日 08時35分

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%)

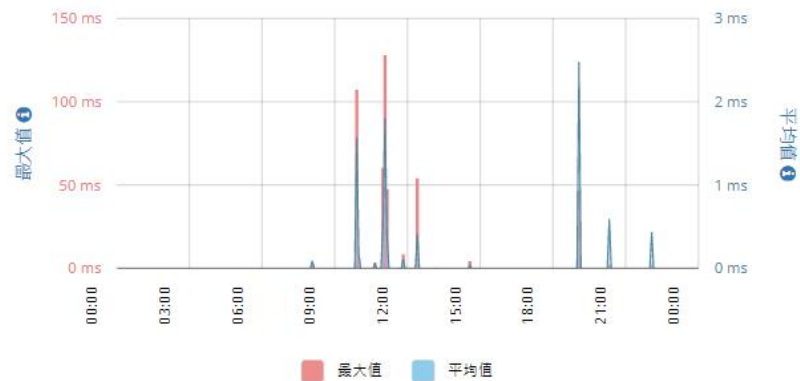
被動式網路服務品質分析(2)

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。

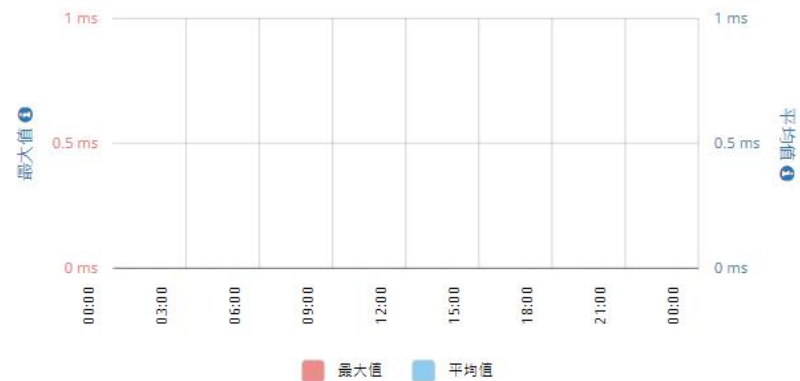
2020-03-31

選擇圖表

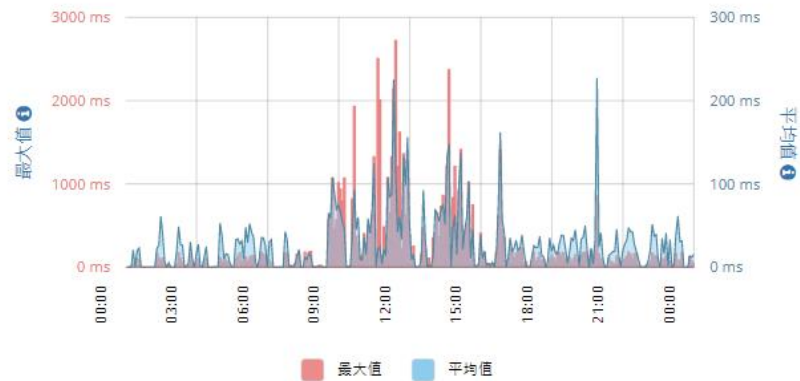
YOUTUBE



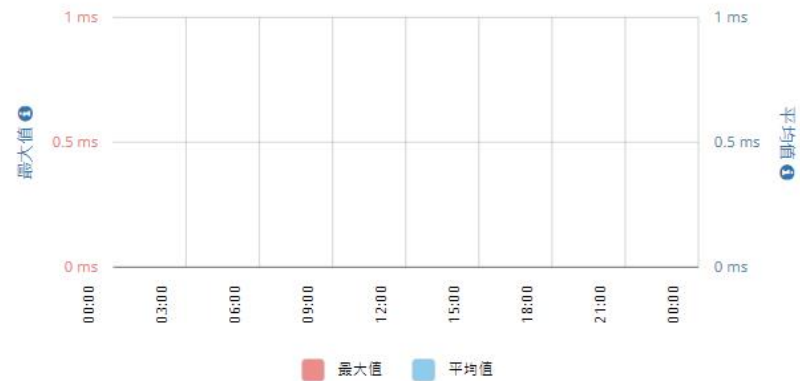
GMAIL



MICROSOFT UPDATE



GOOGLE 雲端硬碟



監控與追蹤管理設備(3)



告警



告警設定



網路交換器

基地台

IP/MAC

非法DHCP

IP流量

Syslog

伺服器

告警記錄

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

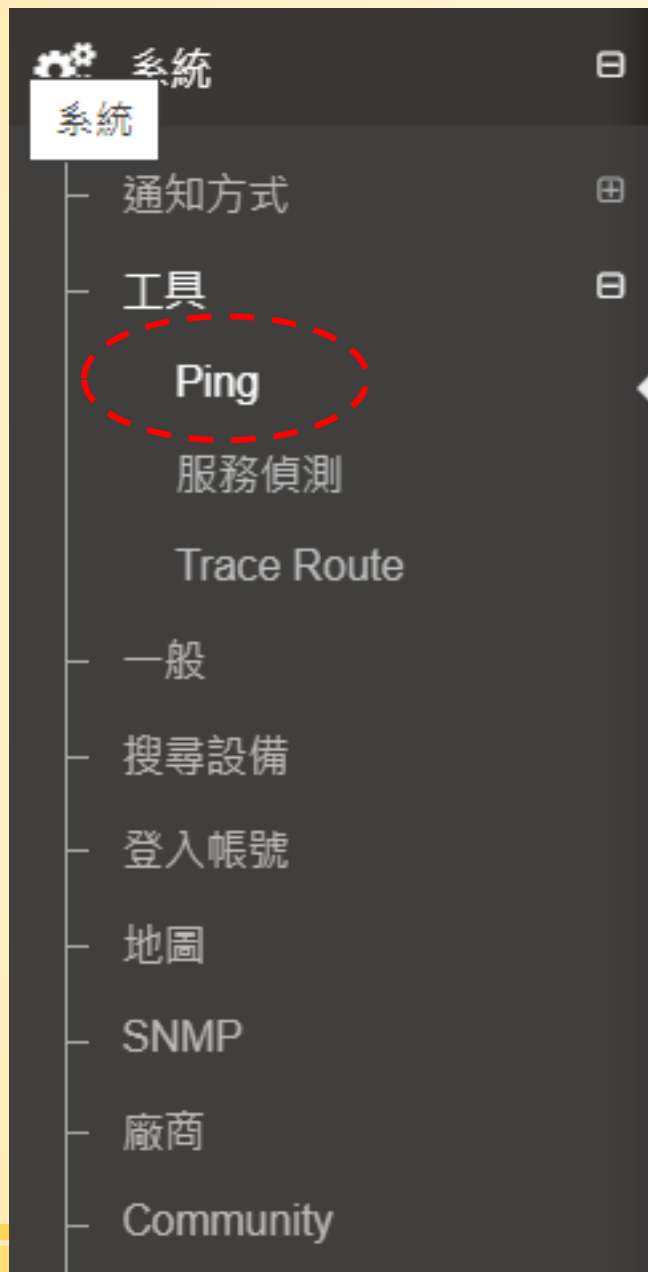


輸入關鍵字查詢

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

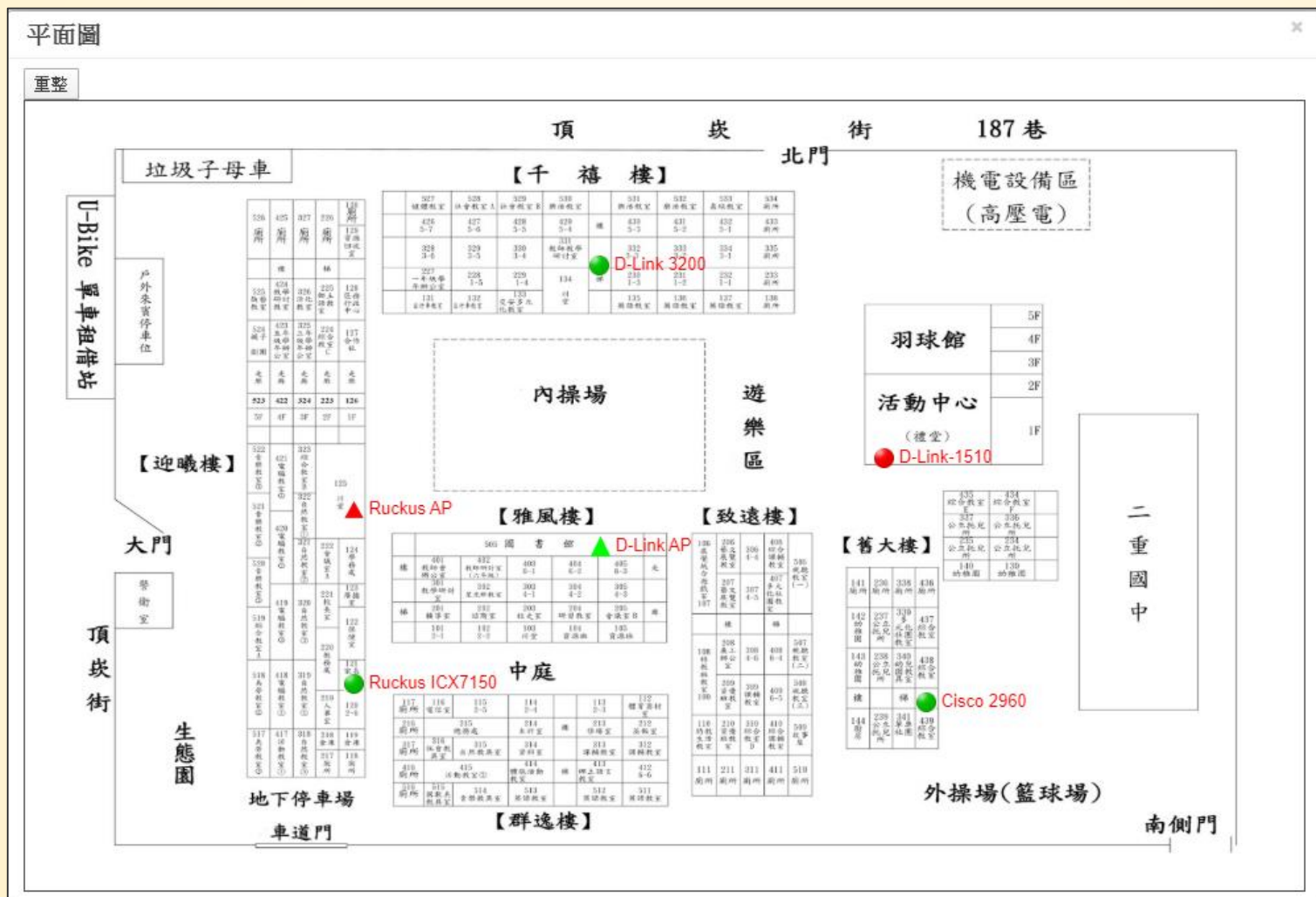
--- 163.20.85.2 ping statistics ---

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

Siraya

0 Radar 狀態：正常

顯赫國民小學 顯赫資訊

智慧網管 / 系統 / 地圖

新增地圖

編輯

名稱 名稱

檔案 選擇檔案 來選擇任何檔案

地圖屬性

☒ 一般地圖 ☐ 熱感圖

說明：

說明

送出 取消

新增 刪除

每頁 100 筆 顯示欄位

查看

總覽

總覽

上一頁 1 下一頁

登入帳號

地圖

SNMP

廠商

Community

Map

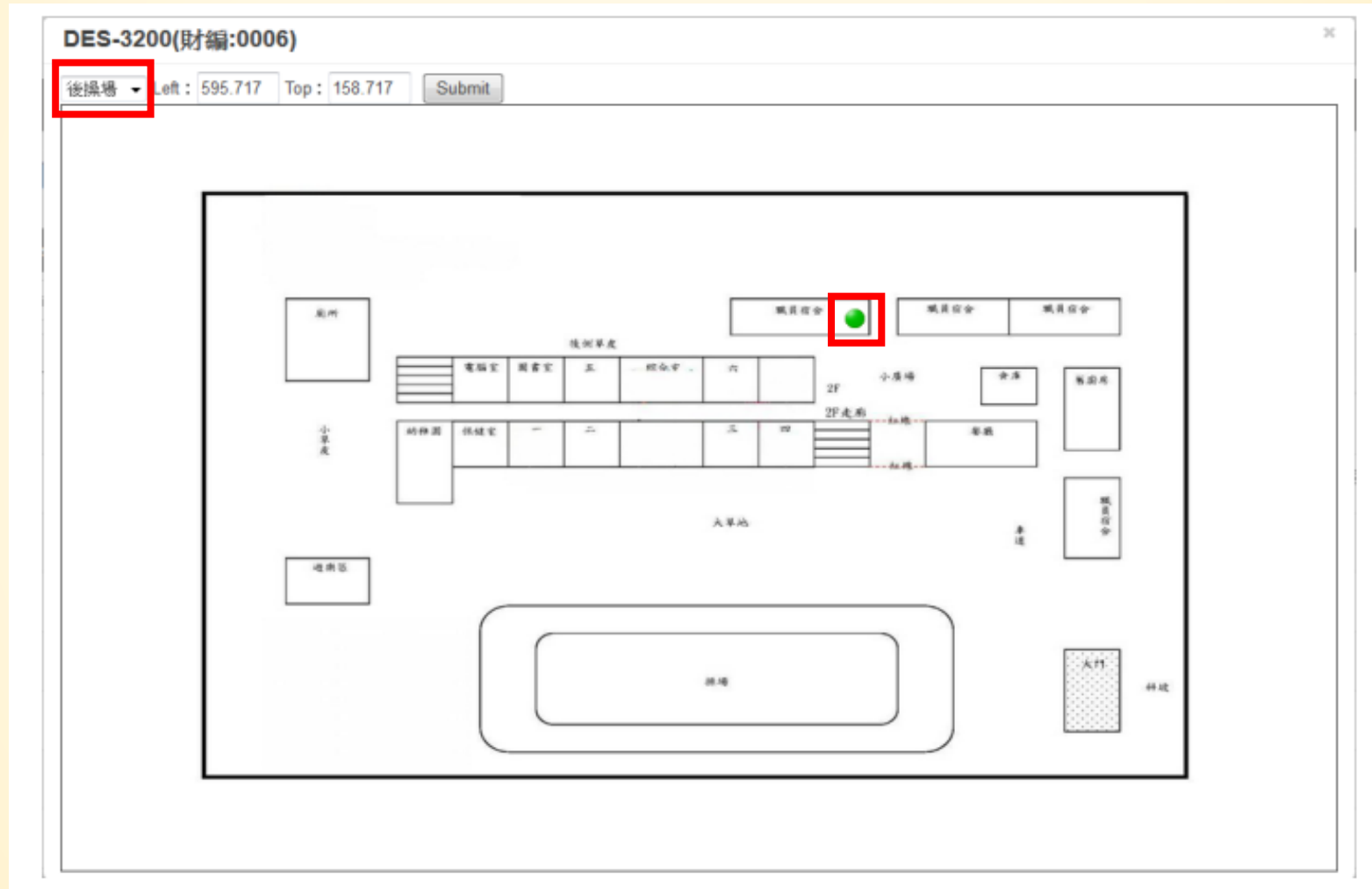
如何定義設備位置?

The screenshot shows the Siraya network management interface. On the left sidebar, the '網路設備' (Network Devices) menu is highlighted, and the '交換器設備' (Switch Devices) sub-menu is selected. The main content area displays a table of switch devices. The first device, 'chjhsL201', has a 'Map' button highlighted in the '位置' (Location) column. The table includes columns for Name, Model, IP, Category, Connection Status, Response Time, Location, and Function.

	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

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。

The screenshot displays the Siraya network management interface. The left sidebar shows the navigation menu with '告警' (Alert) highlighted. The main content area shows the '告警設定' (Alert Setting) page for '網路交換器' (Network Switch). A table lists various network devices, including 'Cisco 2960'. A red box highlights the 'Cisco 2960' entry, and a red arrow points to the configuration modal that appears. The modal shows settings for 'Cisco 2960', including '離線偵測' (Offline Detection) set to 'ON', '觸發次數' (Trigger Count) set to 2, and '通知方式' (Notification Method) set to '佈告欄' (Bulletin Board), 'LINE', and 'Telegram'. The '重複通知' (Repeat Notification) is set to 'NO'.

設備名稱	IP	位置	離線偵測	CPU負載偵測	Port流量偵測
Cisco 2960	192.168.10.4	會議室	ON	OFF	OFF
CRS125-24G-1S	192.168.10.3				
D-link 3000-2	192.168.138.93				
DES-3200-10-10.5	192.168.10.5				
DES-3200-10-10.6	192.168.10.6				
DGS-1210-10P-10.7	192.168.10.7				
DGS-1510-28XMP-10.2	192.168.10.2				
Dlink3000-141.130	192.168.141.30				

Cisco 2960

離線偵測 觸發次數：1次為五分鐘

觸發次數: 2

通知方式: ☒ 佈告欄 ☐ E-mail ☒ LINE ☐ Telegram

重複通知: ☒ NO

送出 取消

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

The screenshot displays the Siraya network management interface. On the left sidebar, the '告警' (Alerts) menu item is highlighted with a red box, and the 'IP/MAC' sub-menu item is also highlighted with a red box. The main content area shows the 'IP衝突偵測' (IP Conflict Detection) settings. A modal window titled 'IP衝突偵測' is open, displaying the following information:

- 說明:** 當發現多台設備使用相同IP時的通知方式。
- IP 衝突告警方式設定**
- 通知方式:** ☒ 佈告欄 ☐ E-mail ☐ LINE ☐ Telegram
- 重複告警週期(秒):** 86400
- 一天通知一次** (written in blue text)
- Buttons: 送出 (Send), 取消 (Cancel)

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

The screenshot displays the Siraya network management system interface. The left sidebar contains a menu with items: 綜觀, 帳號, IPAM, 網路設備, 告警 (highlighted with a red box), 告警設定 (highlighted with a red box), 網路交換器, 基地台, IP/MAC, 非法DHCP, IP流量 (highlighted with a red box), Syslog, 伺服器, and 告警記錄. The main content area is titled '智慧網管 / 告警 / 告警設定 / IP流量'. It features a search bar with the placeholder '輸入關鍵字查詢'. Below the search bar is a table with the following columns: IP, 資料來源, 告警類別, 告警值, 時間區段, and 通知方式. The table contains four rows of data:

IP	資料來源	告警類別	告警值	時間區段	通知方式
IPv4 Any	192.168.119.1	Flow筆數上限	6666	5 分鐘	LINE通知
IPv6 Any	192.168.119.1	流量上限	500 MB	5 分鐘	LINE通知
192.168.5.22	192.168.119.1	流量上限	1 MB	5 分鐘	佈告欄通知
IPv6 Any	192.168.119.1	流量上限	1988 MB	當日	LINE通知

Below the table, it says '顯示 (1 至 4), 共 4 筆資料'. At the bottom of the interface, there is a footer with 'Siraya 2.4 © 2019'.

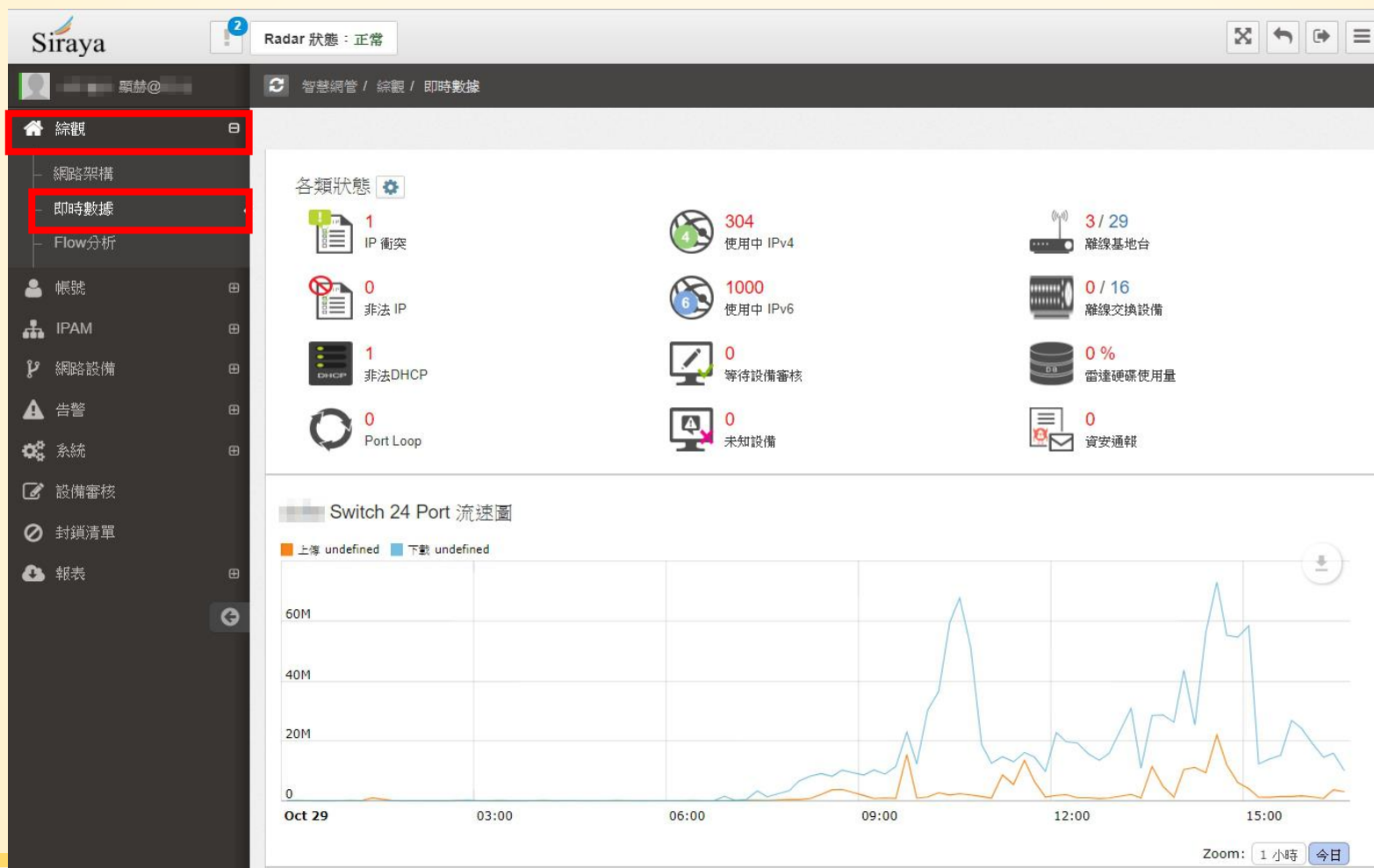
系統流量

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。

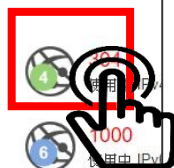


adar 狀態：正常

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

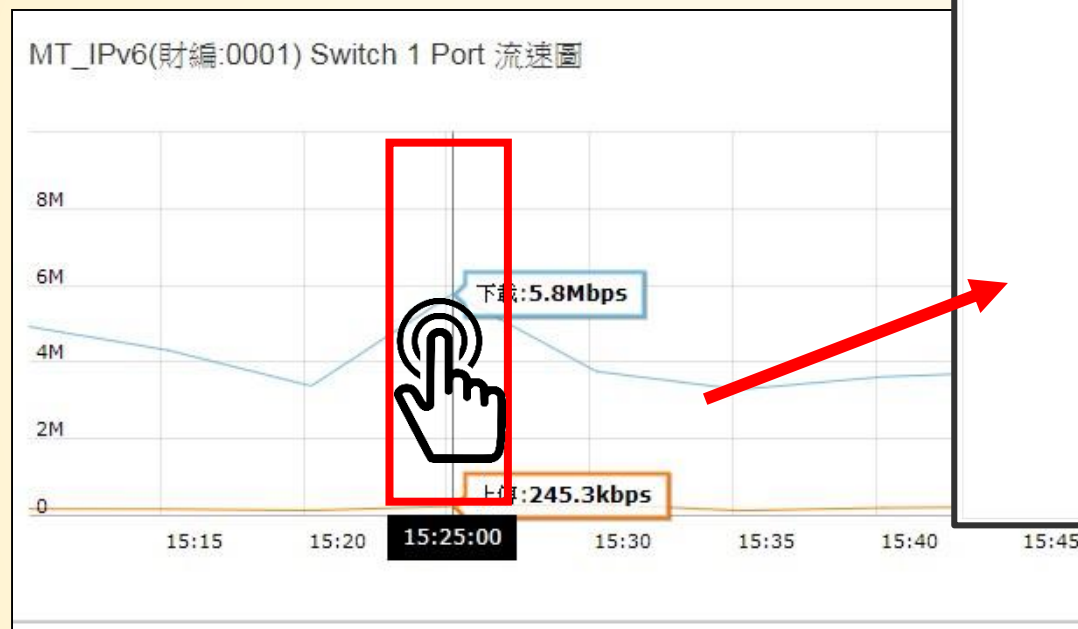
每頁 100 ▾ 筆 顯示欄位

IP	別名	今日累積數據				活動分鐘數 ⓘ ▾
		流入 (Bytes) ▾	流出 (Bytes) ▾	流入 (Packets) ▾	流出 (Packets) ▾	
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流速圖表頁



時間: 2018-12-19 09:45:00 - 2018-12-19 09:55:00

資料來源: 中心流量取樣

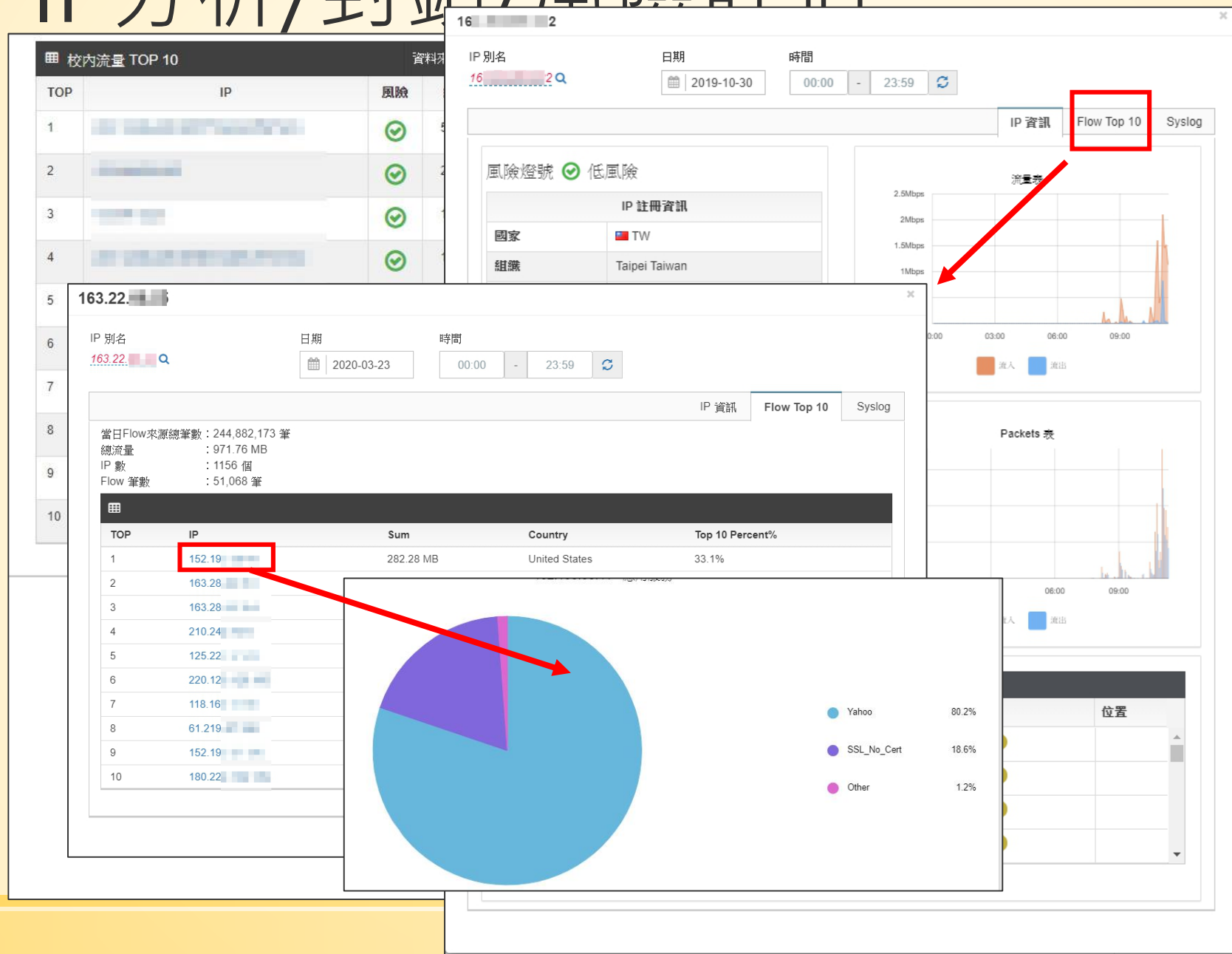
IP比例圖 詳細資料

用 IP 流量

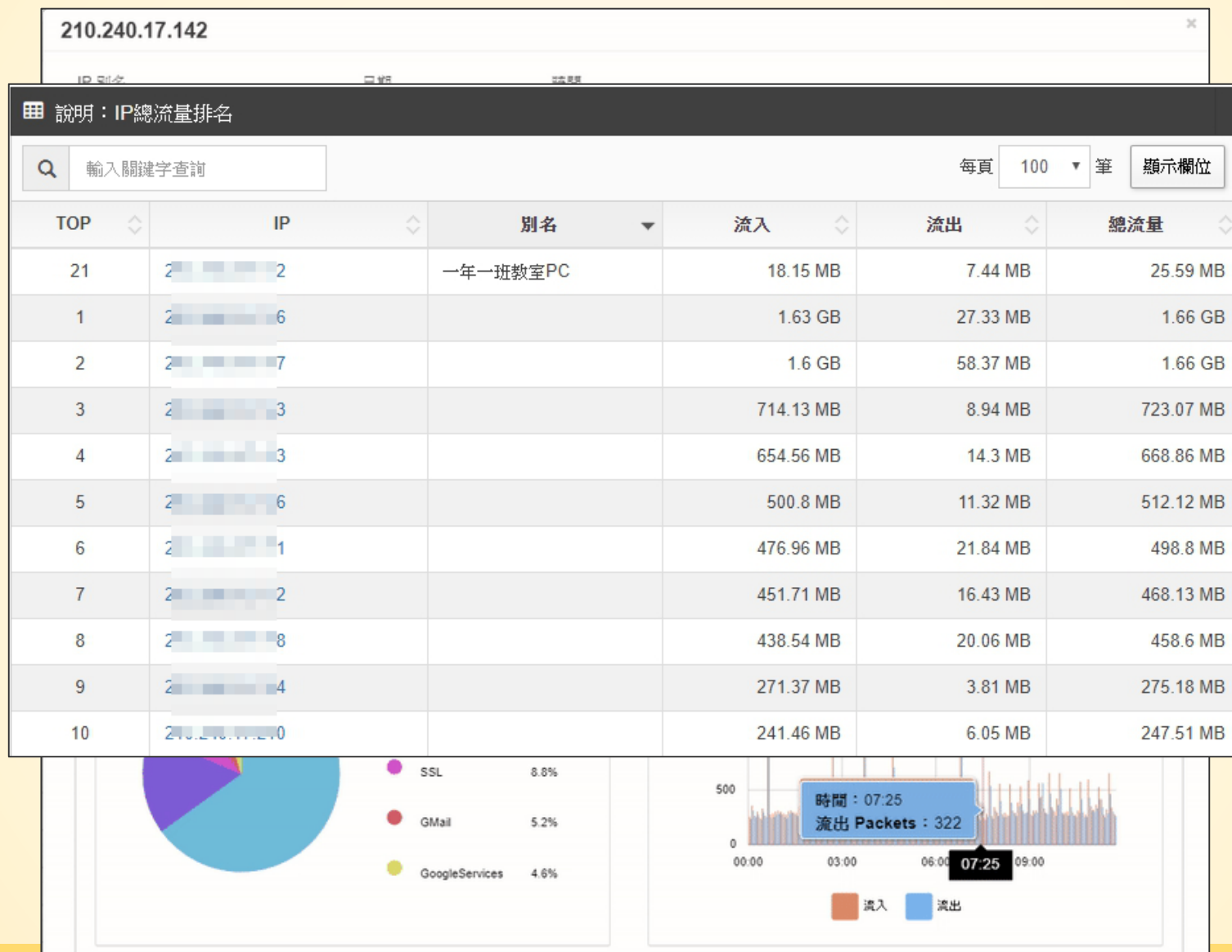
輸入關鍵字查詢 每頁 100 顯示欄位

帳號	IP	名稱	總流量
N/A	163.27.135.79		1.61 GB
N/A	163.27.135.29		489.94 MB
N/A	163.28.5.34		351.07 MB
N/A	163.27.135.56		84.27 MB
N/A	61.218.251.74		84.21 MB
N/A	163.27.135.57		71.78 MB
N/A	220.130.123.59		64.68 MB
N/A	163.27.135.59		56.59 MB
N/A	175.181.185.149		50.59 MB
N/A	122.118.216.64		42.28 MB
N/A	172.217.160.106		41.4 MB
N/A	49.159.229.27		40.62 MB
N/A	202.169.173.206		36.25 MB
N/A	163.27.135.197		36.19 MB
N/A	1.172.111.169		35.99 MB
N/A	163.27.135.123		35.98 MB
N/A	111.184.22.37		34.98 MB

IP分析/封鎖/風險評估

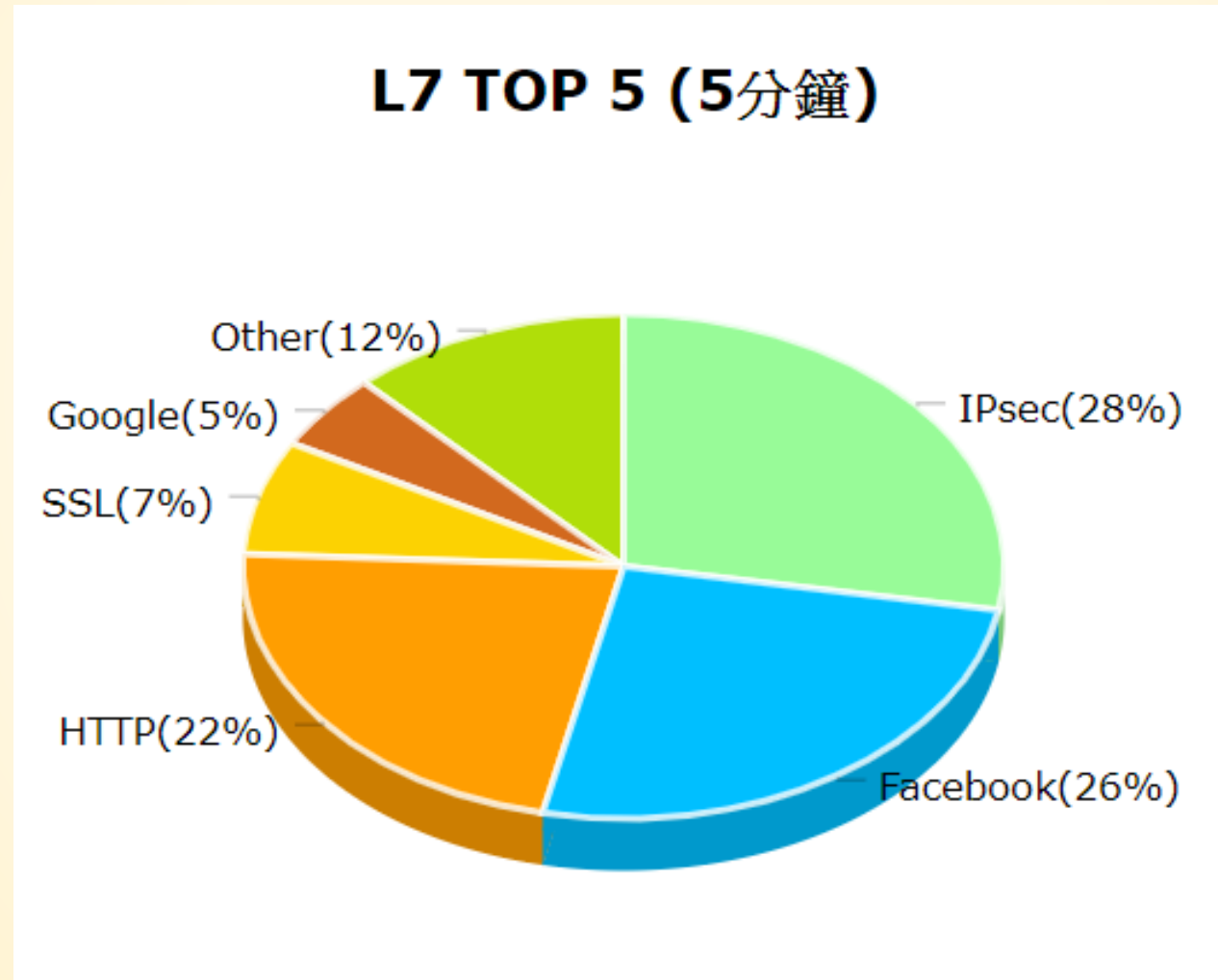


IP別名



第七層前五名分析

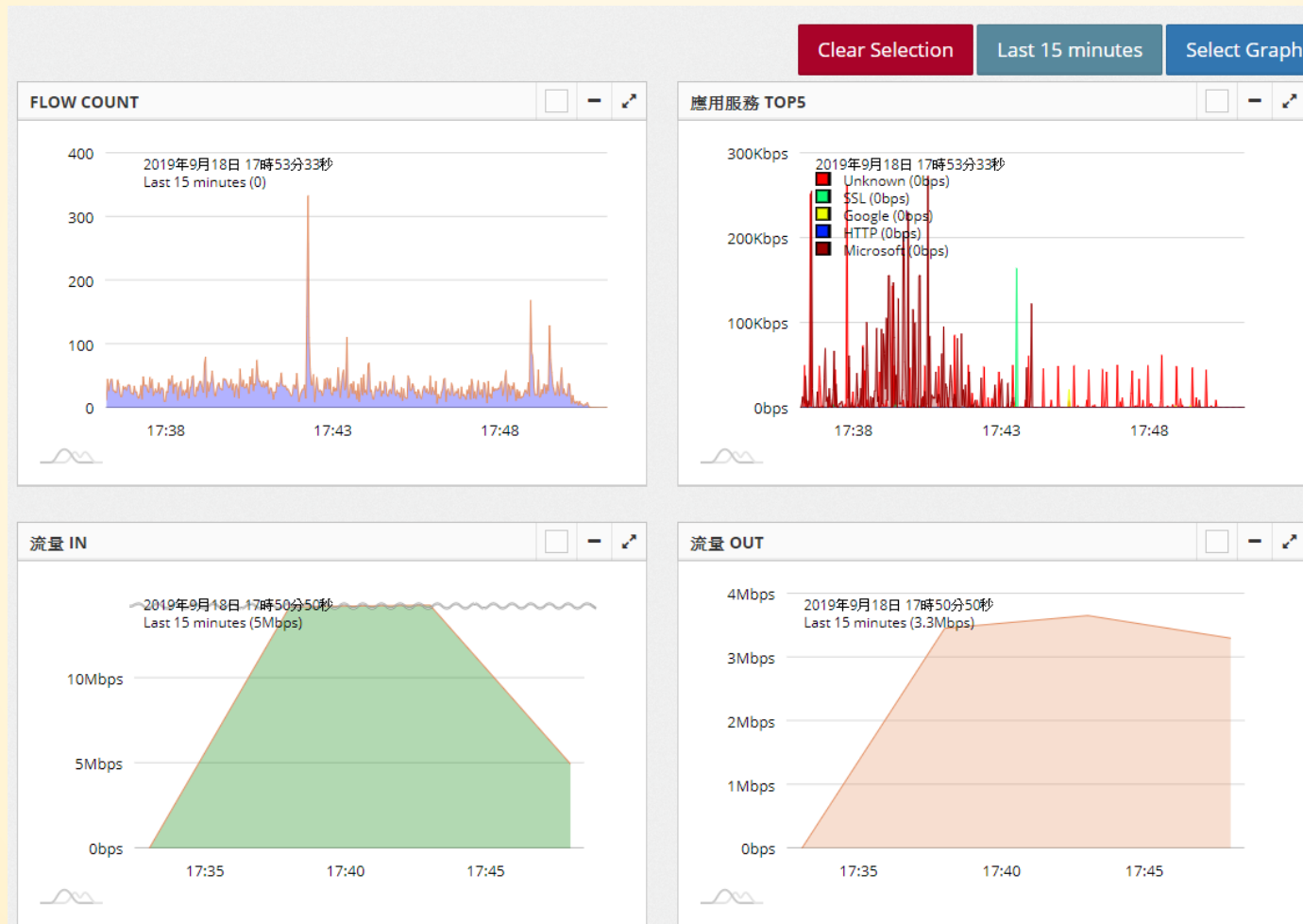
第七層服務前五名分析，針對整體流量進行第七層分析，並以圓餅圖呈現。



Flow分析

綜觀 → Flow分析

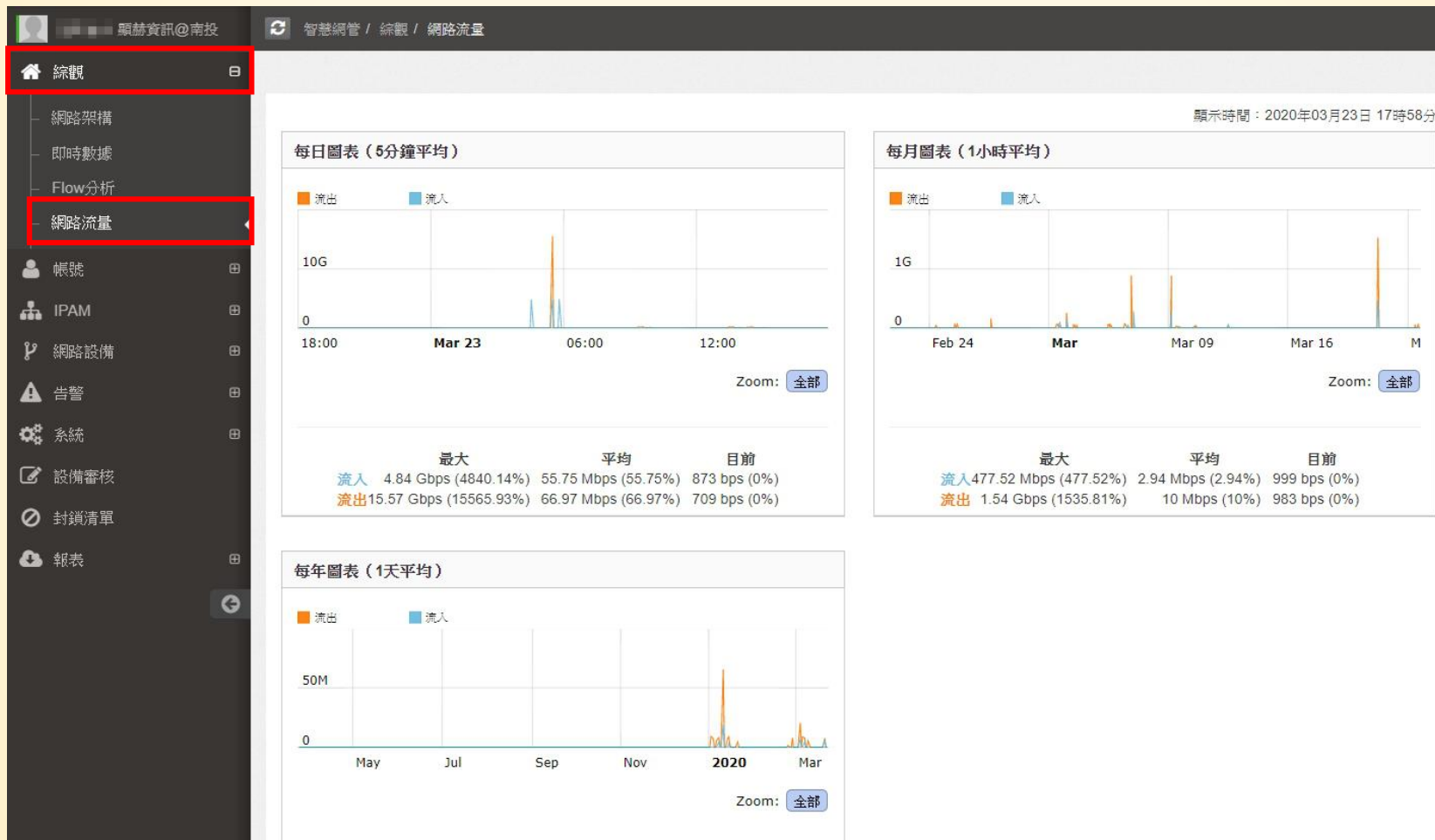
本校IP流量圖表分析總覽/流量資訊排名/圖表式佔比，圖表可作區間放大。



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

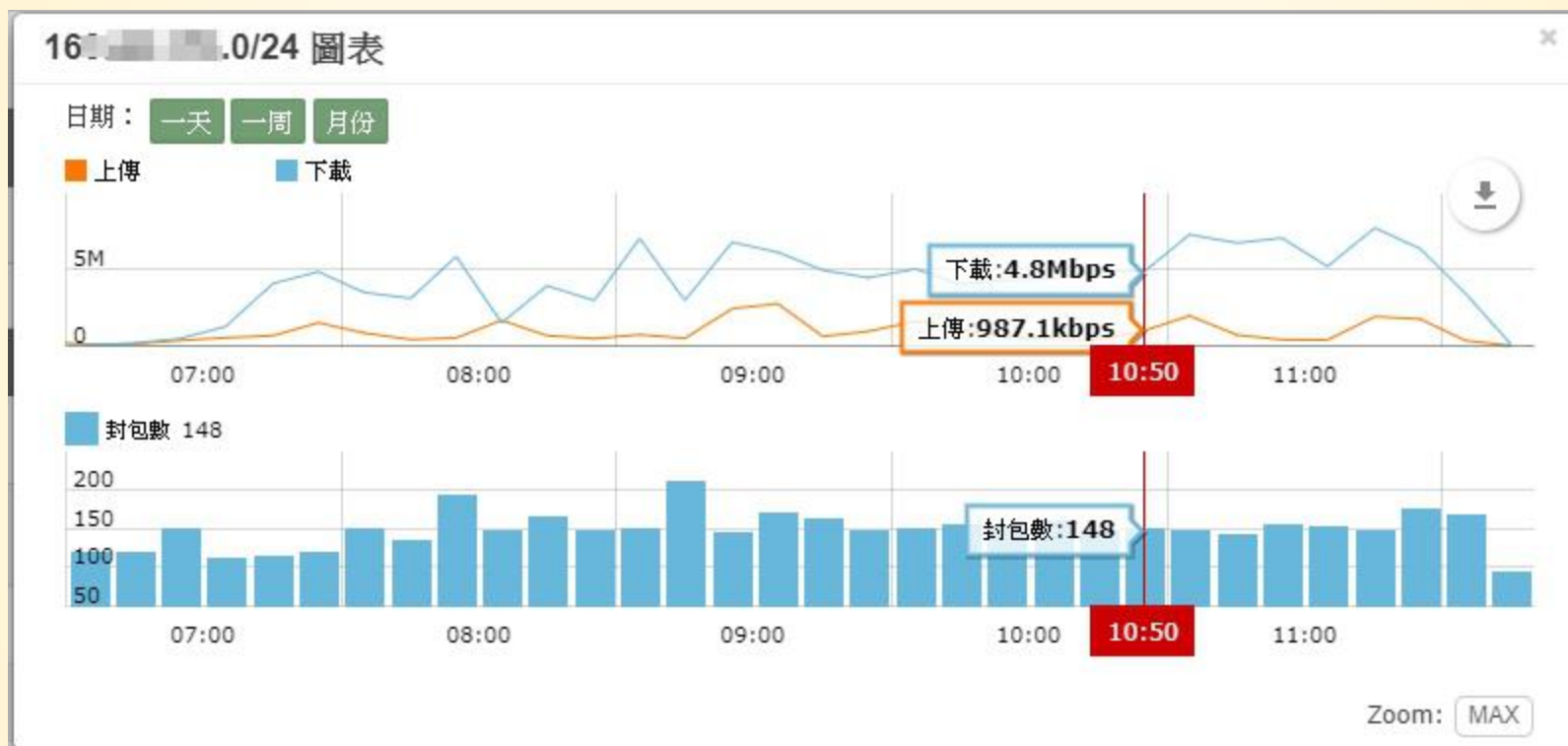
IPAM → 網段使用狀況

目前已納管至單位內的網段於此管理檢視。



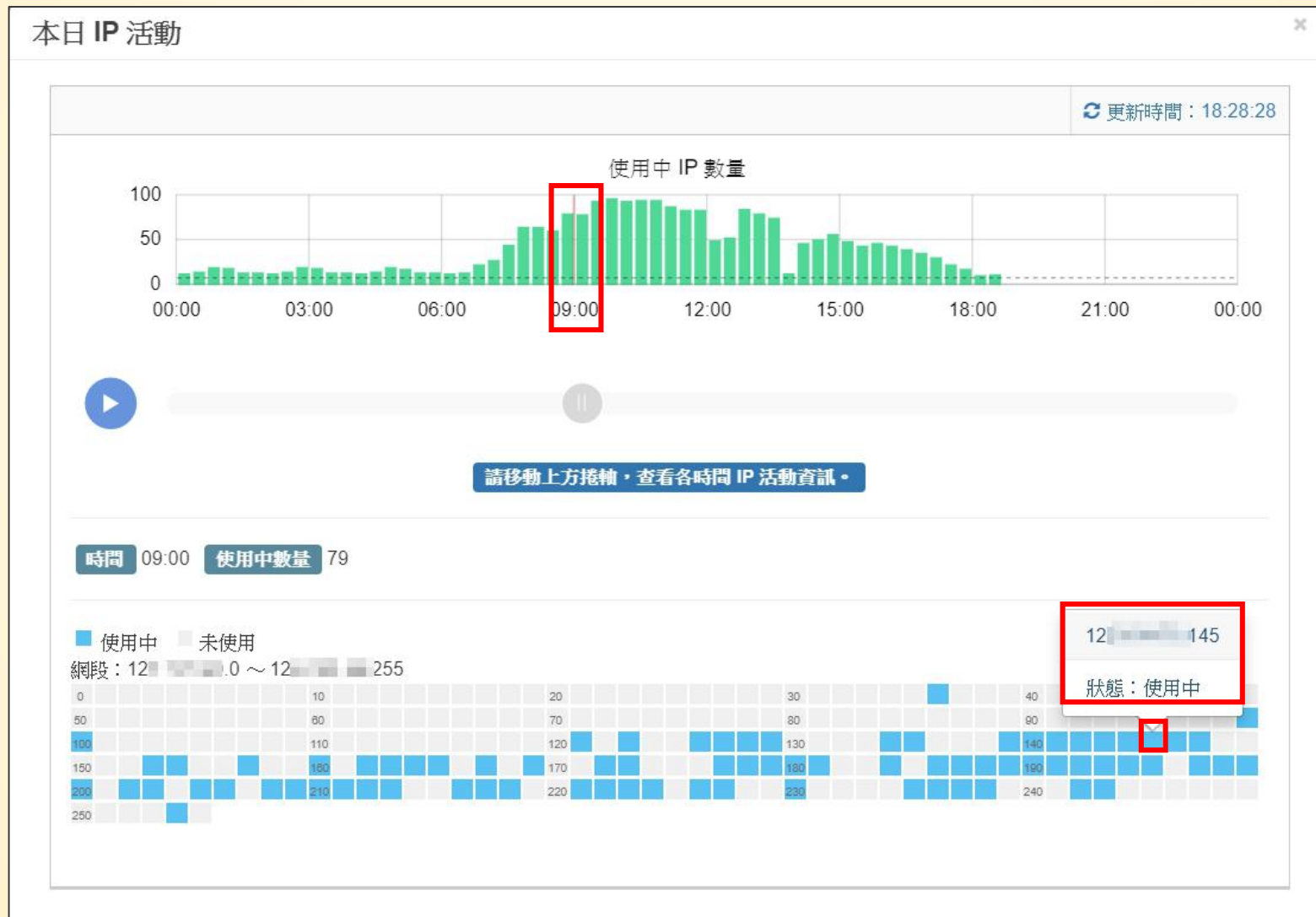
IPAM

網段流量圖表



IPAM

本日IP活動



報表

報表 → FlowSearch

可於此搜尋整個系統內存的IP資訊。

The screenshot displays the Siraya network management system's Flow Search interface. The left sidebar contains navigation options, with '報表' (Reports) and 'Flow Search' highlighted. The main area shows search criteria and a table of top 10 IP addresses by flow volume.

Search Criteria:

- 開始日期: 2019-10-30
- 開始時間: 09:00 ~ 結束時間: 16:00
- IP: 192.168.3.7
- 資料來源: 中心流量取樣

Summary:

- Flow來源: 2,148,994筆
- 總流量: 195.18 MB
- IP數: 483 個
- Flow筆數: 10,000筆

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。

Siraya

1

Radar 狀態：正常

✕ ↶ ↷ ≡

顯赫國民小學 顯赫資訊

智慧網管 / 報表 / IP TOP

🏠 綜觀

👤 帳號

👥 IPAM

🔧 網路設備

⚠️ 告警

⚙️ 系統

🔍 設備審核

🔒 封鎖清單

☁️ 報表

Flow Search

IP TOP

操作記錄

Syslog記錄

IP-MAC歷史資料

設備妥善率

📊 用戶 TOP

時間：2019-10-30 IP類型：IPv4 + IPv6 TOP：30 資料來源：中心流量取樣 類別：校內IP 確認

📋 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 ◇
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! 18		335.48 MB	375.05 MB	710.54 MB
7	5! 13		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! 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。

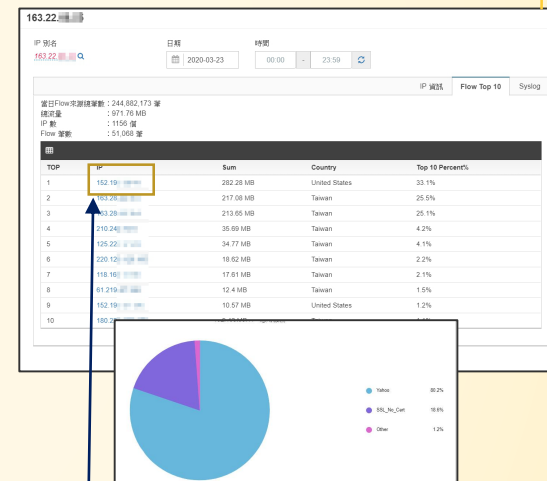
判斷IP危險程度

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。

報表

Flow Search

TOP N

操作記錄

Syslog紀錄

IP-MAC歷史資料

設備妥善率

終端設備使用度

NAT紀錄

體制外IP使用狀況

說明：Syslog 報表。支援[查詢]10000筆

◎ 詳細 ◎ Switch

啟始：2020-10-13 ~ 結束：2020-10-13 時間：0:00 ~ 10:48 IP：ALL 關鍵字(非必填)：請輸入關鍵字 確認

SysLog 查詢的IP：ALL / 資料時間：2020-10-13 00:02:08 ~ 2020-10-13 10:47:14 / 關鍵字：

每頁 10 筆

時間	設備IP	紀錄訊息
2020-10-13 00:02:08	10.226.	10.226. CRIT: MAC-based Access Control unauthenticated host(MAC: D2-4A-2A Port 21, VID: 36)
2020-10-13 00:03:40	10.226.	10.226. CRIT: MAC-based Access Control unauthenticated host(MAC: D2-4A-2A Port 23, VID: 36)
2020-10-13 00:06:56	10.226.	10.226. CRIT: MAC-based Access Control unauthenticated host(MAC: D2-4A-2A Port 21, VID: 36)
2020-10-13 00:08:56	10.226.	10.226. CRIT: MAC-based Access Control unauthenticated host(MAC: D2-4A-2A Port 23, VID: 36)
2020-10-13 00:14:28	10.226.	10.226. CRIT: MAC-based Access Control unauthenticated host(MAC: D2-4A-2A Port 23, VID: 36)
2020-10-13 00:15:42	10.226.	10.226. CRIT: MAC-based Access Control unauthenticated host(MAC: D2-4A-2A Port 21, VID: 36)
2020-10-13 02:03:11	10.226.	10.226. CRIT: MAC-based Access Control unauthenticated host(MAC: 80-26-89 Port 21, VID: 36)
2020-10-13 02:11:49	10.226.	10.226. CRIT: MAC-based Access Control unauthenticated host(MAC: D0-B1-28 Port 21, VID: 36)
2020-10-13 03:18:36	10.226.	10.226. CRIT: MAC-based Access Control unauthenticated host(MAC: D2-4A-2A Port 21, VID: 36)
2020-10-13 03:18:58	10.226.	10.226. CRIT: MAC-based Access Control unauthenticated host(MAC: D2-4A-2A Port 23, VID: 36)

顯示 (1 至 10) , 共 741 筆資料

上一頁 1 2 3 4 5 ... 75 下一頁

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。

報表

Flow Search

TOP N

操作記錄

Syslog記錄

IP-MAC歷史資料

設備妥善率

終端設備使用度

NAT紀錄

體制外IP使用狀況

說明：Syslog 報表。支援[查詢]10000筆

時間：2020-10-13 確認

Switch 狀態

輸入關鍵字查詢

名稱	IP	型號	位置	Syslog 數
.201	10.226	DGS-1510-28XMP	星光樓311教師研究室	8
.202	10.226	DGS-1510-28XMP	正義樓2樓管道間機櫃	96
.203	10.226	DGS-1510-28XMP	正義樓3樓管道間機櫃	0
.204	10.226	DGS-1510-28XMP	正義樓2樓管道間機櫃	31
.205	10.226	DGS-1510-28XMP	曉月樓1樓體育器材室	27
L2-51	10.226	DGS-1510-24P	星光樓311教師研究室	0
L2-52	10.226	DGS-1510-24P	正義樓2樓管道間機櫃	0
L2-53	10.226	DGS-3100-24P	正義樓2樓管道間機櫃	0
L2-54	10.226	DGS-3100-24P	正義樓2樓管道間機櫃	0
L2-56	10.226	DGS-3100-24P	正義樓2樓管道間機櫃	0
L2-57	10.226	DGS-3100-24P	正義樓2樓管道間機櫃	0
2-58	10.226	DGS-3100-24P	正義樓2樓管道間	0

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。

帳號

IPAM

網路設備

告警

系統

設備審核

封鎖清單

報表

Flow Search

IP TOP

操作記錄

Syslog記錄

IP-MAC歷史資料

設備妥善率

終端設備使用度

NAT紀錄

說明：設備妥善率 報表

啟始：2020-03-16 ~ 結束：2020-03-22

確認

計算妥善率的設備類型：☒ Switch ☐ AP ☐ Server

Switch 統計模式：☒ 包含周六日 ☐ 不包含周六日

單位設備妥善率 / 2020-03-16~2020-03-22 / 目前統計設備：Switch / 統計方式：包含周六日 / 設備數量：16 台

設備名稱	設備IP	設備型號	妥善率
Ubiquiti	192.16	USW-24P-250, 4.0.66.10832, Linux 3.6.5	100.00%
Ubiquiti	192.16	USW-48P-500, 4.0.66.10832, Linux 3.6.5	100.00%
Ubiquiti	192.16	USW-24P-250, 4.0.66.10832, Linux 3.6.5	100.00%
Ubiquiti	192.16	USW-48P-500, 4.0.66.10832, Linux 3.6.5	100.00%
Ubiquiti	192.16	USW-48P-500, 4.0.66.10832, Linux 3.6.5	100.00%
Ubiquiti	192.16	USW-24P-250, 4.0.66.10832, Linux 3.6.5	100.00%
Ubiquiti	192.16	USW-XG, 4.0.66.10832, Linux 3.6.5	100.00%
pfSense	163.22	pfSense 2.4.4-RELEASE pfSense FreeBSD 11.2-RELEASE-p10 amd64	100.00%
Ubiquiti	192.16	USW-24P-250, 4.0.66.10832, Linux 3.6.5	100.00%

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末上線的終端設備。

報表

Flow Search

TOP N

操作記錄

Syslog記錄

IP-MAC歷史資料

設備妥善率

終端設備使用度

NAT紀錄

體制外IP使用狀況

終端設備使用度

使用天數： 確認

查詢的結果：您建立的終端設備數共 47 台，回溯近 3 天內都無上線使用的終端設備有 8 台，列示如下

每頁 100 顯示欄位 Print

設備別名	MAC	Vendor	IP
Shuttle3c2b0	80EE73E3C2B0	Shuttle	
Shuttle3c2f0	80EE73E3C2F0	Shuttle	
Shuttle3c328	80EE73E3C328	Shuttle	
Shuttle65b85	80EE73E65B85	Shuttle	
Shuttle65bc0	80EE73E65BC0	Shuttle	
Shuttle65fd6	80EE73E65FD6	Shuttle	
Shuttle667ce	80EE73E667CE	Shuttle	
Shuttle66bb6	80EE73E66BB6	Shuttle	

顯示 (1 至 8)，共 8 筆資料

上一頁 1 下一頁

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。

報表

Flow Search

TOP N

操作記錄

Syslog記錄

IP-MAC歷史資料

設備妥善率

終端設備使用度

NAT紀錄

體制外IP使用狀況

起始：2020-10-01 ~ 結束：2020-10-13 IP 或 MAC：10.226.184.245 確認

IP-MAC歷史資料 查詢的結...

輸入關鍵字查詢 每頁 100 筆 顯示欄位 Print

時間	IP	MAC
2020-10-01	10.226.184.245	B8:27:EB:DF:A7:59 81
2020-10-02	10.226.184.245	B8:27:EB:DF:A7:59 81
2020-10-03	10.226.184.245	B8:27:EB:DF:A7:59 81
2020-10-04	10.226.184.245	B8:27:EB:DF:A7:59 87
2020-10-05	10.226.184.245	B8:27:EB:DF:A7:59 76
2020-10-06	10.226.184.245	B8:27:EB:DF:A7:59 74
2020-10-07	10.226.184.245	B8:27:EB:DF:A7:59 74
2020-10-08	10.226.184.245	B8:27:EB:DF:A7:59 73
2020-10-09	10.226.184.245	B8:27:EB:DF:A7:59 82
2020-10-10	10.226.184.245	B8:27:EB:DF:A7:59 79
2020-10-11	10.226.184.245	B8:27:EB:DF:A7:59 73

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