

EstiNet

IoT Network Controller User Manual

版本: 1.0
日期: 2018/12

產品目錄

1. 產品介紹	3
1.1. 產品功能	3
1.2. 產品外觀	4
1.2.1. Controller	4
1.2.2. Switch	4
2. 設備架設	6
2.1. 設備設定	7
2.1.1. EstiNet RT188T	7
2.1.2. EstiNet RT166P	9
2.2. 連接拓樸與架設	12
3. 連線操作設定	13
3.1. 登入網頁	13
3.2. Update Profile	14
3.3. 修改登入密碼	15
3.4. 登出網頁	17
3.5. Dashboard	18
4. Switches	20
4.1. Management	20
4.1.1. Overview	20
4.1.2. Probe	23
4.2. VLAN	24
4.3. Topology	25
4.4. Statistics	26
4.5. Tags	27
5. Device	28
5.1. 設備清單	28
5.1.1. 設備 Dashboard	28
5.1.2. My Group	30
5.1.3. New Devices	33
5.2. 設備內容資訊	35
5.2.1. Device Information	36
5.2.2. Switch Port	39
5.3. 設備搜尋	40
5.4. 設備資料上傳	42

6. Network	44
6.1. Subnet (Gateway)	44
6.2. Interface	47
7. Service	50
7.1. DHCP Server	50
7.2. Bandwidth Control	53
8. Security	58
8.1. 訪問模式配置	58
8.2. 白名單列表	59
8.3. 黑名單列表	61
8.4. 准入管理	63
8.5. DHCP Snooping	66
9. Policy	68
9.1. 通知警告	68
9.2. 系統議程表	71
10. System	73
10.1. Controller	73
10.2. Events	75
10.3. Backup	77
10.4. Firmware	78
10.5. Settings	81
11. Monitoring	84
11.1. 系統概況	84
11.2. Latency	86
11.2.1. Dashboard	87
11.2.2. Target	90
11.3. Uptime	92
12. 注意事項	93

1. 產品介紹

在物聯網背景下，大量的連線需求、管理需求、多樣化的頻寬管理、物聯網設備的安全性、以及相關科技所衍生出來的應用如：大數據、人工智慧(AI)等，都將對網路環境產生衝擊。

針對上述的需求，思銳科技推出網路解決方案，以思銳科技的 IoT Network Controller 為網路控制核心，搭配思銳 IoT Edge 交換機提供一個安全、可靠的網路使用環境。在思銳的解決方案中，網路管理者可以將網路設備以群組化的方式來管理網路設備。

相較於傳統網路需要每台設備單獨設定的方式，思銳的 IoT Network Controller 可讓網路管理者以簡單方式完成網路環境設定，並且能依據應用需求來動態調整網路資源配置，以達到有效率且穩定的網路功能。

1.1. 產品功能

IoT Network Controller 功能如下：

自動供裝	VLAN 自動供裝	自動設定交換器Port的VLAN
	上網設備設定自動供裝	自動偵測上網設備Port位置並套用對應的交換器設定
	IP及Port設定自動供裝	支援DHCP伺服器分派IP位址、MAC/IP位址綁定及IP Port綁定等功能
智慧診斷	網路狀態監控	網路延遲及封包遺失率監控
	異常診斷	上網設備傳輸流量或狀態異常監控
	IP 位址衝突	自動偵測IP 衝突相關設備的Port位置
	斷線警告	自動偵測交換器及Port狀況，在斷線時發出警告
	DHCP Snooping	自動阻斷非法DHCP 服務
安全管理	設備審核	支援黑/白名單及上網設備審核機制
	IP Port綁定	提供IP 位址與Port綁定功能
流量管控	Port 流量統計	即時交換器Port TX/RX流量及歷史資料查詢
	頻寬利用率	自動偵測網路拓撲及分析頻寬使用率
	頻寬保留及切片	系統可自動化設定點對點的頻寬保留，依網路狀態動態設定對內/對外頻寬保證
	頻寬限流	限制上網設備寬頻使用上限，以保障其它設備頻寬

1.2. 產品外觀

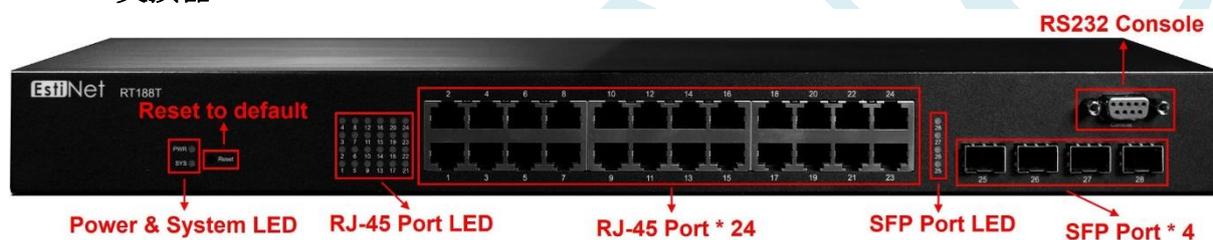
1.2.1. Controller

先將使用者所使用的 Server 或桌上型電腦安裝 ubuntu14 或 16 作業系統，再行安裝思銳 IoT Network Controller



1.2.2. Switch

RT188T 交換器



Power & System LED	電源與系統燈顯示
Reset to default	硬體還原出場設定
RJ-45 Port LED (10/100/1000 Mbps)	燈號顯示 24 個 RJ-45 Port 上下線情況
SFP Port LED(1000 Mbps)	燈號顯示 4 個 SFP Port 上下線情況
RS232 Console	CLI Console

RT166P 交換器

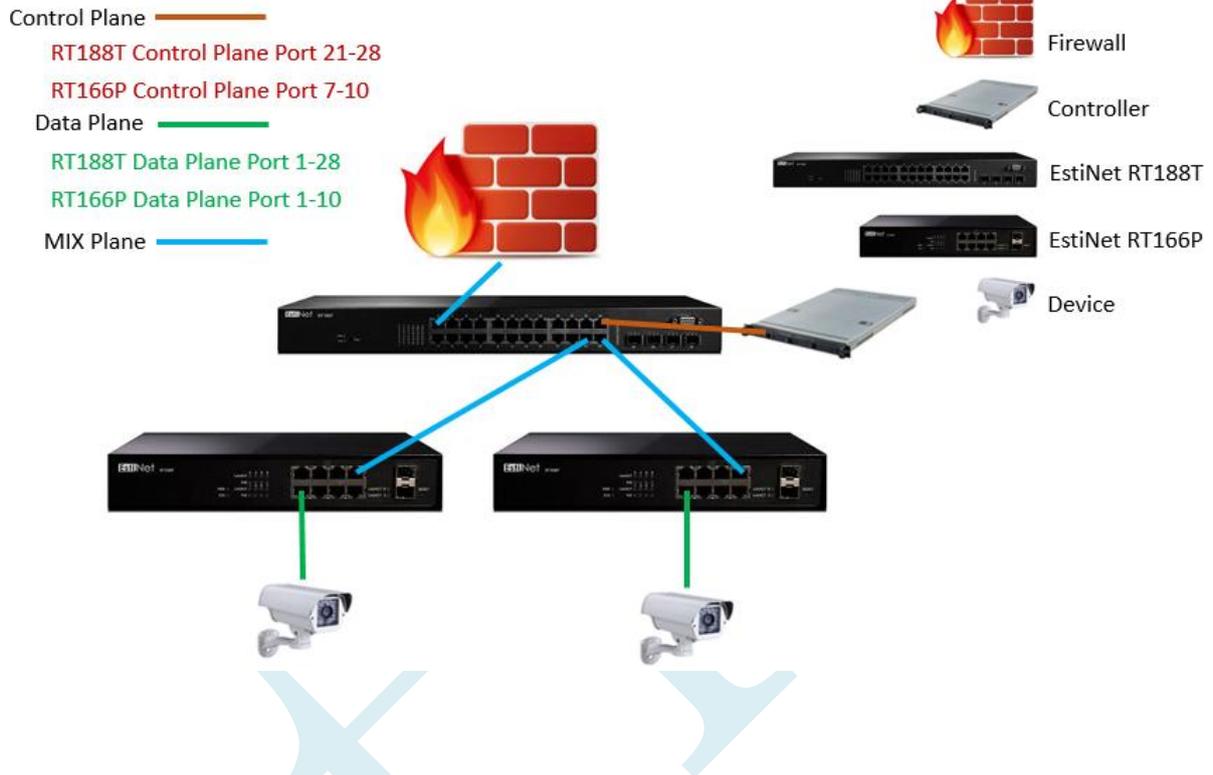


Power & System LED	電源與系統燈顯示
--------------------	----------

Reset to default	硬體還原出場設定
RJ-45 Port LED (10/100/1000 Mbps)	燈號顯示 8 個 RJ-45 Port 上下線情況以及 POE 供電顯示
SFP Port LED(1000 Mbps)	燈號顯示 2 個 SFP Port 上下線情況

2. 設備架設

本產品是在 Firewall 底下，向下監控各個交換器以及各式終端設備(如:個人電腦、攝影機、印表機、感測器設備...等等)，下圖為一簡易的拓譜環境，供客戶參考操作。詳細架設方式麻煩訊洽 Mail : fae@estinet.com



2.1. 設備設定

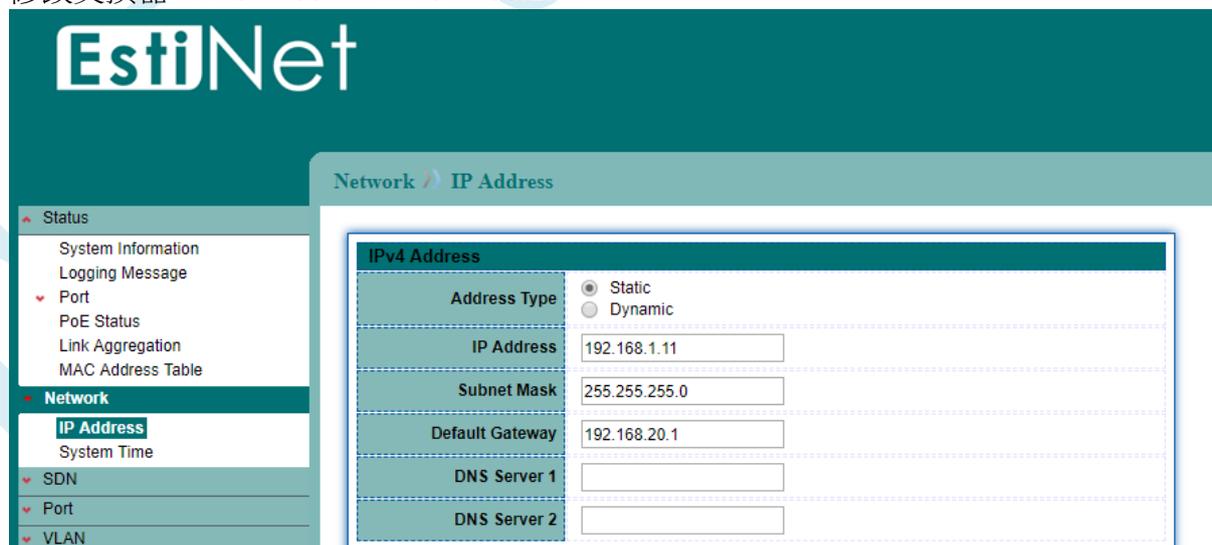
2.1.1. EstiNet RT188T

透過瀏覽器登入交換器 Default IP: 192.168.1.1，預設帳號密碼: switch/admin



標籤名稱	標籤說明
Username :	輸入帳號位置，出廠預設帳號: switch
Password :	輸入密碼位置，出廠預設密碼: admin
LOGIN	登入交換器網頁

修改交換器 IP: 192.168.1.1 -> 192.168.1.11



標籤名稱	標籤說明
Network IP Address	修改交換器的網路設定
Address Type	可選擇 Static (Static IP) 或 Dynamic (DHCP IP)
IP Address	交換器在設定 Static 下設定 IP 位址
Subnet Mask	交換器在設定 Static 下設定 Subnet Mask
Default Gateway	交換器在設定 Static 下設定 Default Gateway
DNS Server 1	交換器在設定 Static 下設定第一組 DNS Server
DNS Server 2	交換器在設定 Static 下設定第二組 DNS Server

設定好將頁面下拉並確認修改與儲存設定

The screenshot shows the 'IP Address' configuration page. At the top right, there are links for 'Save', 'Logout', 'Reboot', and 'Debug'. The breadcrumb path is 'Network > IP Address'. The 'DNS Server 2' field is visible at the top. The 'IPv6 Address' section includes 'Auto Configuration' (checked), 'DHCPv6 Client' (unchecked), and input fields for 'IPv6 Address', 'Prefix Length' (0), 'IPv6 Gateway', 'DNS Server 1', and 'DNS Server 2'. The 'Operational Status' section displays: IPv4 Address: 10.0.10.204, IPv4 Default Gateway: 10.0.10.254, IPv6 Address: fe80::20b:4ff:fe13:e8df/64, IPv6 Gateway: ::, and Link Local Address: fe80::20b:4ff:fe13:e8df/64. A 'Success.' message is shown in a dark grey box with a green checkmark. An 'Apply' button is at the bottom left.

標籤名稱	標籤說明
Apply	確認設定
Success.	輸入成功
Save	儲存交換器設定

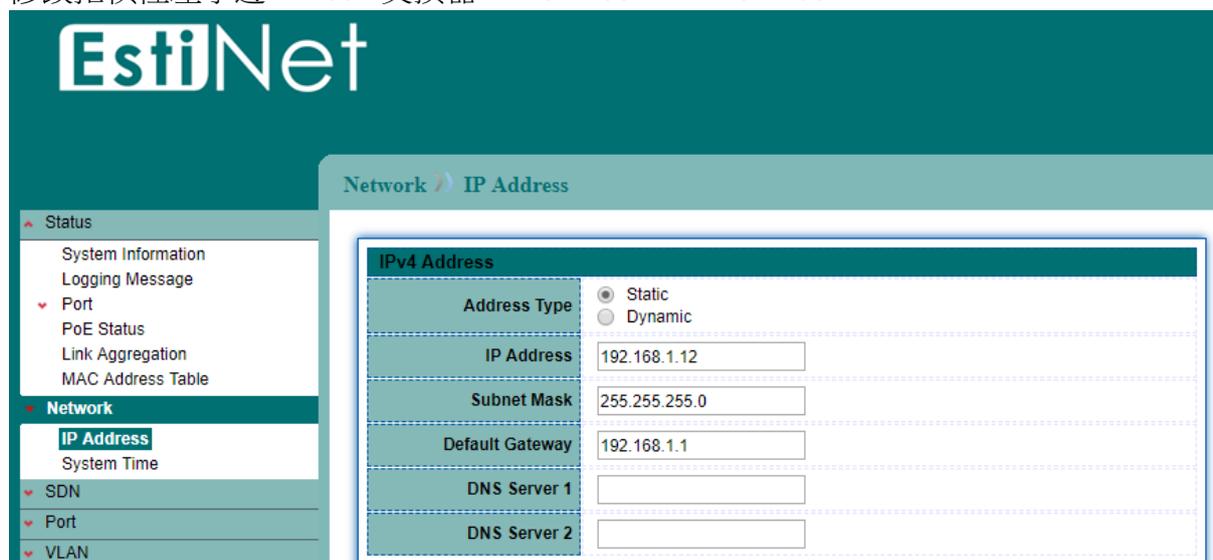
2.1.2. EstiNet RT166P

透過瀏覽器登入交換器 Default IP: 192.168.1.1，預設帳號密碼: switch/admin
 請特別注意網路拓樸中有兩台 RT166P，所以請將下列敘述的步驟針對兩台各進行一次設定

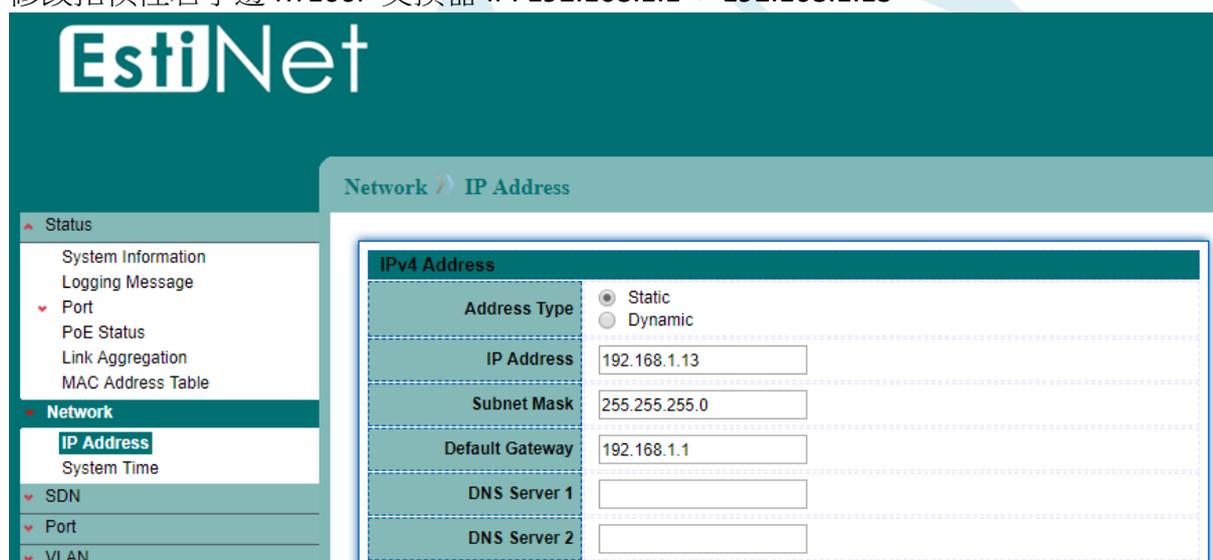


標籤名稱	標籤說明
Username :	輸入帳號位置，出廠預設帳號: switch
Password :	輸入密碼位置，出廠預設密碼: admin
LOGIN	登入交換器網頁

修改拓樸裡左手邊 RT166P 交換器 IP: 192.168.1.1 -> 192.168.1.12

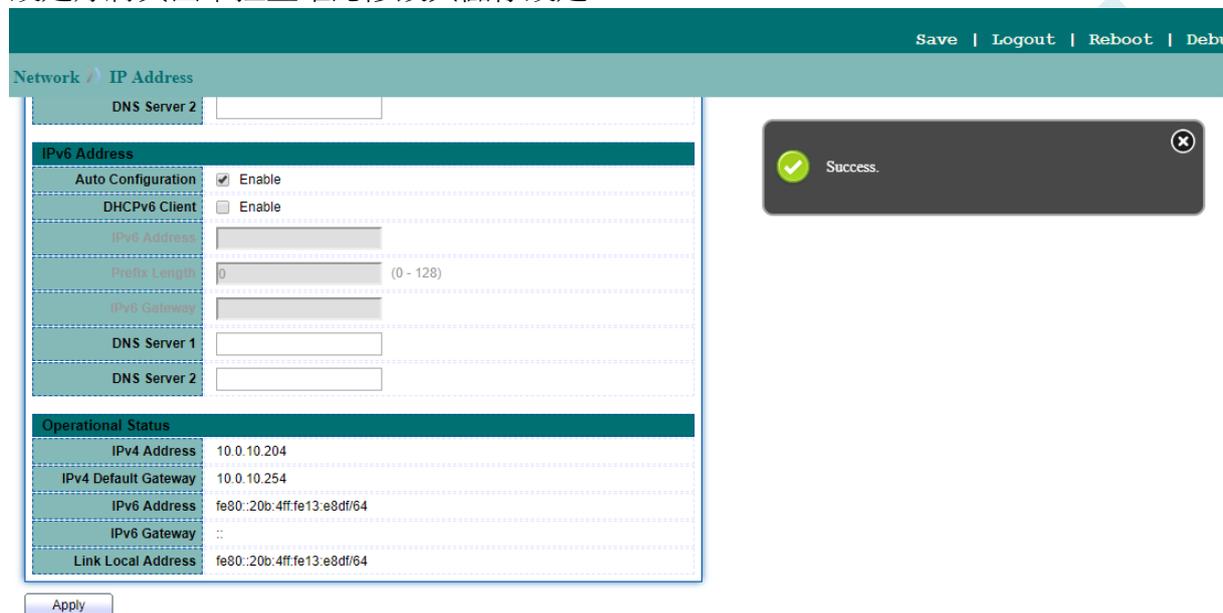


修改拓樸裡右手邊 RT166P 交換器 IP: 192.168.1.1 -> 192.168.1.13



標籤名稱	標籤說明
<ul style="list-style-type: none"> Network IP Address 	修改交換器的網路設定
Address Type	可選擇 Static (Static IP) 或 Dynamic (DHCP IP)
IP Address	交換器在設定 Static 下設定 IP 位址
Subnet Mask	交換器在設定 Static 下設定 Subnet Mask
Default Gateway	交換器在設定 Static 下設定 Default Gateway
DNS Server 1	交換器在設定 Static 下設定第一組 DNS Server
DNS Server 2	交換器在設定 Static 下設定第二組 DNS Server

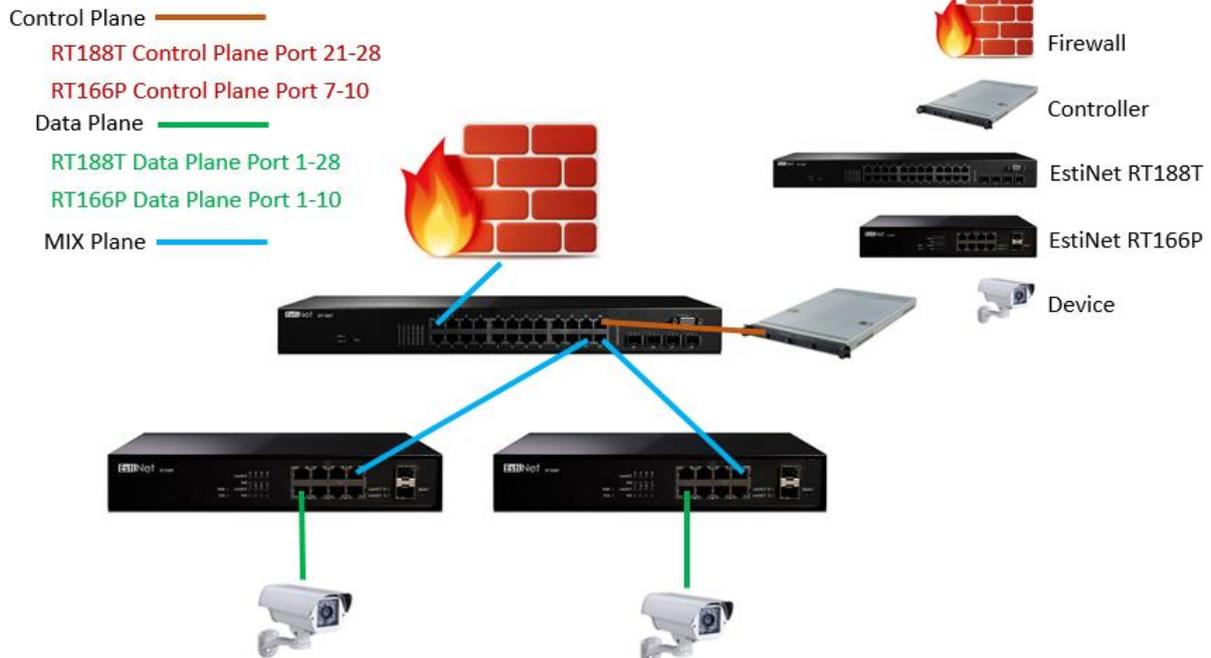
設定好將頁面下拉並確認修改與儲存設定



標籤名稱	標籤說明
	確認設定
	輸入成功
	儲存交換器設定

2.2. 連接拓樸與架設

架設拓樸如下圖：



請依上圖進行實體線路的連接，尚未接上 WAN 與設備則可依需求自行接在 RT188T 上

1. 請接一條 RJ-45 網路線在 EstiNet Controller 與 EstiNet RT188T 的 Port 24 上
(注意: EstiNet Controller 的 Port 會因使用者買的機型有所差異，請與 EstiNet 聯絡窗口確認)
2. 請接一條 RJ-45 網路線在 EstiNet RT188T 的 Port 21 與左邊 EstiNet RT166P 的 Port 8 上
3. 請接一條 RJ-45 網路線在 EstiNet RT188T 的 Port 23 與右邊 EstiNet RT166P 的 Port 8 上

基本設備建置如上，如需要其他幫助麻煩訊洽 Mail : fae@estinet.com

3. 連線操作設定

3.1. 登入網頁

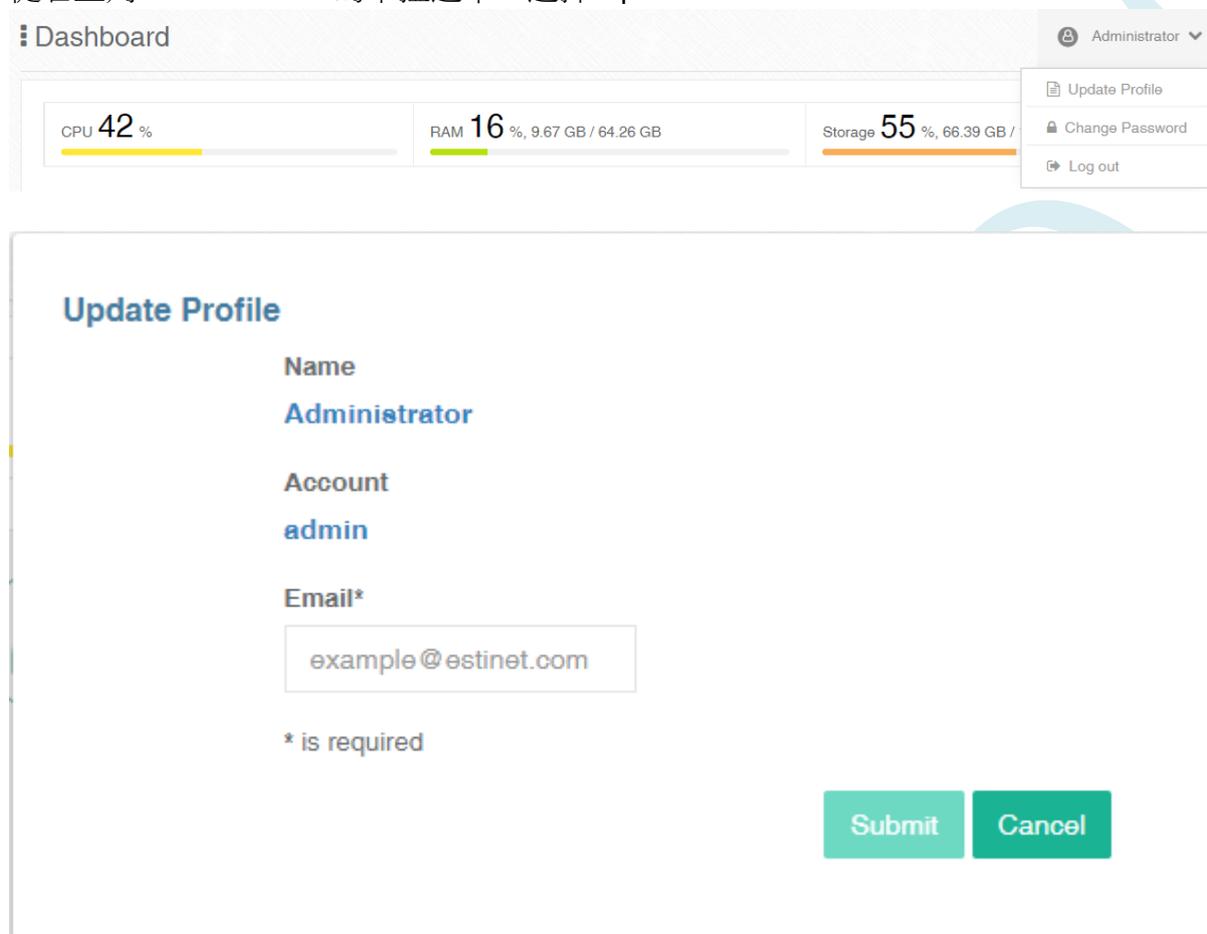
請將操作機器透過 RJ-45 線接在 Control Plane 上，由瀏覽器登入 Controller 的 WEB 介面，Default IP: 192.168.1.100:3000，預設帳號密碼: admin/EstiNet5408%\$)*



標籤名稱	標籤說明
	輸入帳號位置，預設帳號: admin
	輸入密碼位置，預設密碼: EstiNet5408%\$)*
	登入 Controller 控制器頁面
	透過帳號和 Email 補發密碼

3.2. Update Profile

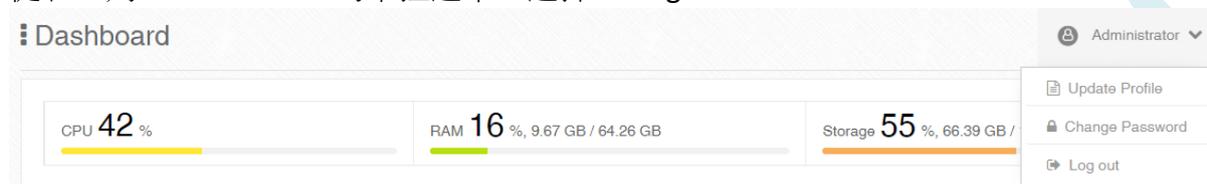
從右上角 Administrator 的下拉選單，選擇 Update Profile



標籤名稱	標籤說明
Name Administrator	登入的帳號權限
Account admin	登入的帳號
Email* <input type="text" value="example@estinet.com"/>	帳號配對的 Email
<input type="button" value="Submit"/>	確認修改 Profile
<input type="button" value="Cancel"/>	取消修改 Profile

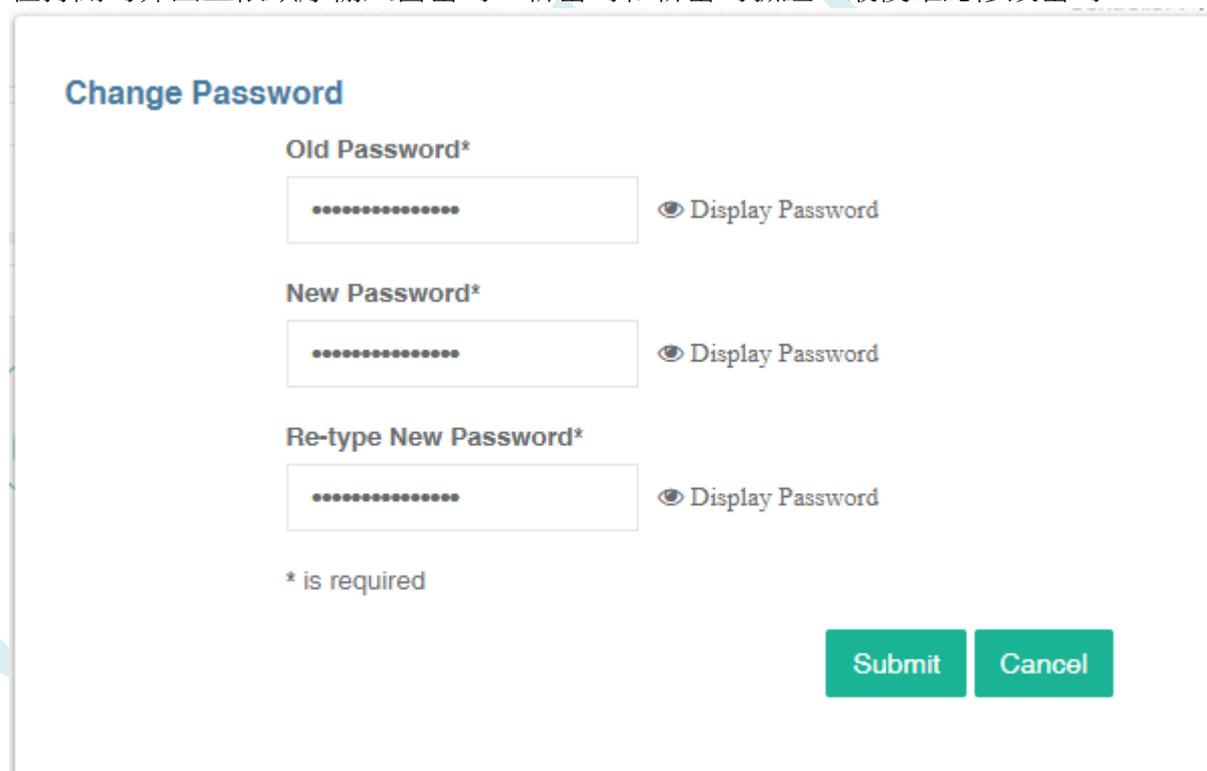
3.3. 修改登入密碼

從右上角 Administrator 的下拉選單，選擇 Change Password



標籤名稱	標籤說明
	更新使用者資訊
	修改密碼
	登出系統

在打開的介面上依順序輸入舊密碼、新密碼和新密碼驗證，最後確認修改密碼

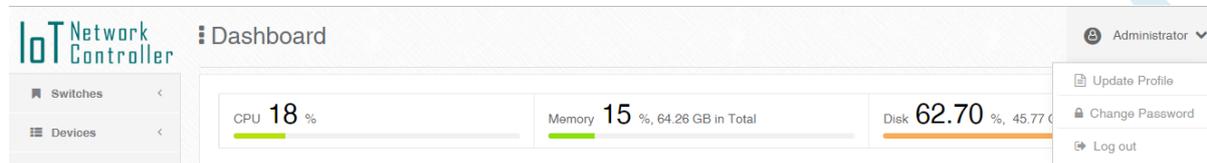


標籤名稱	標籤說明
Old Password*	輸入舊密碼

New Password*	輸入新密碼
Re-type New Password*	再次輸入新密碼
Submit	確認修改密碼
Cancel	取消修改密碼

3.4. 登出網頁

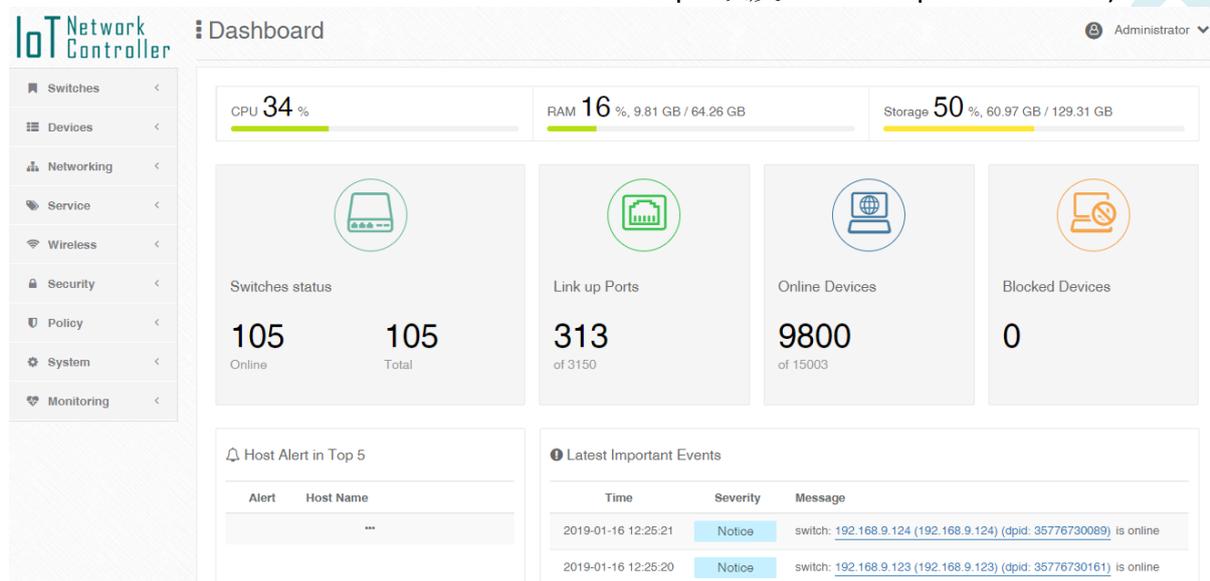
從右上角 Administrator 的下拉選單，選擇 Log out



標籤名稱	標籤說明
 Update Profile	更新使用者資訊
 Change Password	修改密碼
 Log out	登出系統

3.5. Dashboard

點擊左上角 IoT Network Controller 的 Logo 進入 Dashboard 頁面，頁面包含 Controller 目前資源使用狀況(CPU、RAM、Storage)、設備的情況 (Switches status、Link up Ports、Online Devices、Blocked Devices、Host Alert in Top5 以及 Latest Important Events)



標籤名稱	標籤說明
CPU	Controller CPU 的使用情況
RAM	Controller RAM 的使用情況
Storage	Controller Storage 的使用情況
	Switches status 交換器上線的數量
	Link up Ports 交換器 Port 的使用數量
	Online Devices 設備上線的數量

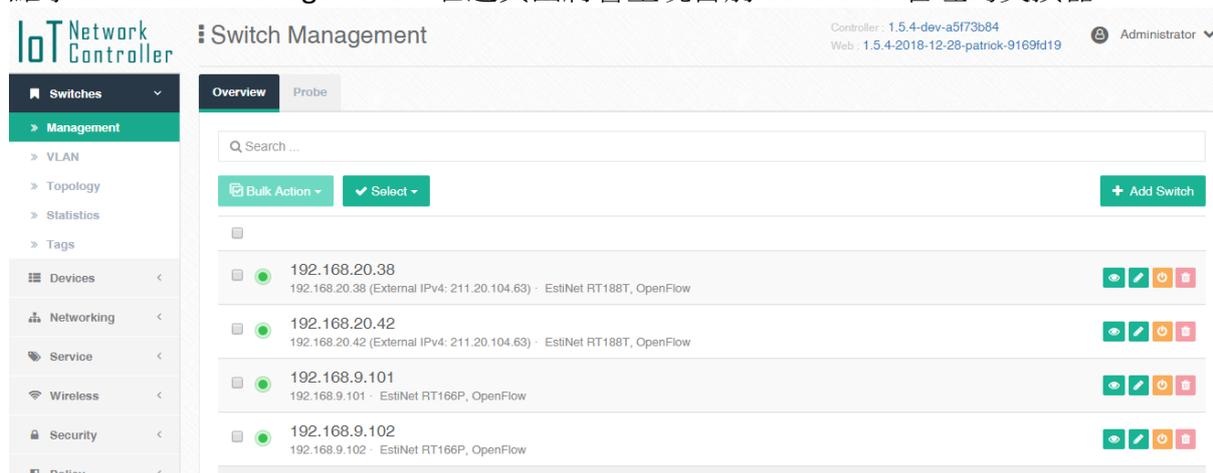
	Blocked Devices 拒絕設備上線的數量
🔔 Host Alert in Top 5	安全警告數量為前五名的設備
📢 Latest Important Events	最新的重要系統訊息

4. Switches

4.1. Management

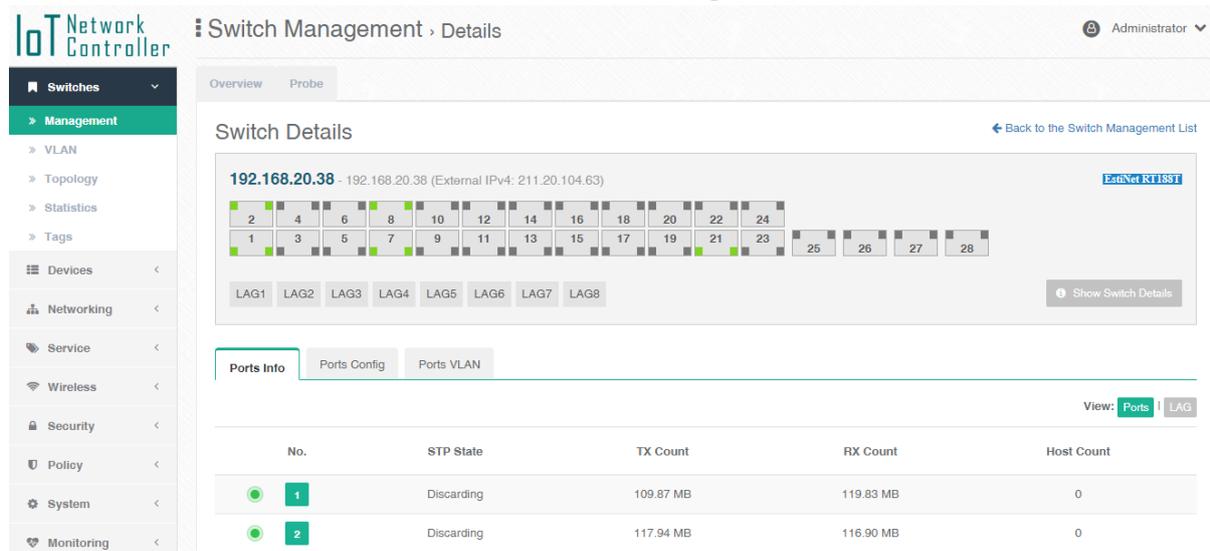
4.1.1. Overview

點擊 Switches > Management，右邊頁面將會呈現目前 Controller 管理的交換器



標籤名稱	標籤說明
 Search ...	用 IP 或名稱來搜尋交換器
 Bulk Action ▾	執行 Tag、Pin、重新命名、重啟交換機和刪除交換器等動作
 Select ▾	透過交換器的 Model、Tag、Pinned 和狀態等選取交換器
 Add Switch	增加交換機
	觀看交換器的詳細資料
	修改交換器的名稱及 Tag
	重啟交換器
	移除離線的交換器

功能包含觀看交換器詳細內容、交換器 Ports Config 設定、交換器 VLAN 設定



標籤名稱	標籤說明
← Back to the Switch Management List	回到 Overview 的頁面
交換器資訊	
	Port 的流量圖
	LAG1 的流量圖
	交換器詳細內容
交換器各項功能設定	
	Port 的 STP 狀態、TX、RX 和 Host 數量
	開啟或關閉 Port 的功能: Security、Link Detection、VLAN Provisioning 和 Via WIFI-Mesh
	設定 VLAN 設定
	Port 和 LAG 資訊確認

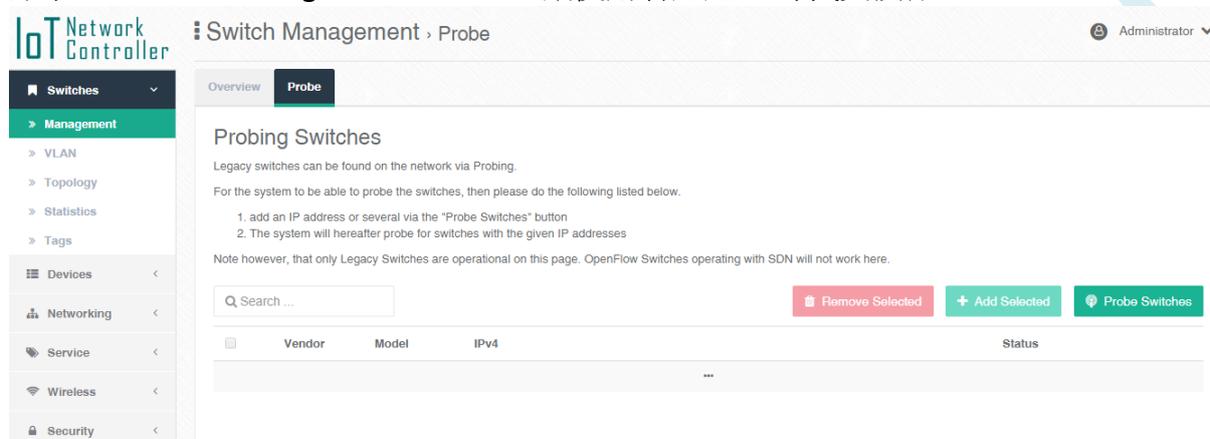
點擊 Port 的流量圖的功能包含 Static MAC、Device List 和 Event Log



標籤名稱	標籤說明
Statistics	Port 的 Static TX 和 RX
Static MAC	設定 Port 的 Static MAC(For Device)
Device List	Port 所有的 Device 名單
Log	Port 的 Event Log

4.1.2. Probe

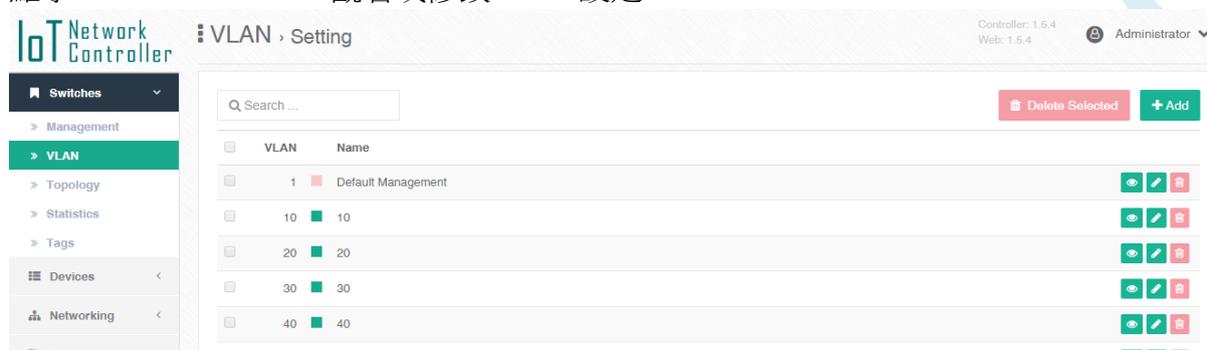
點擊 Switches > Management > Probe，讓使用者透過 IP 尋找交換器



標籤名稱	標籤說明
	<p>可以通過探測在網絡上找到傳統交換器 為了啟動探測功能，請執行以下列出的操作</p> <ol style="list-style-type: none"> 1. 通過 Probe Switches 按鈕添加一個或多個 IP 地址 2. 系統將以輸入的 IP 來探測交換器 <p>請注意探測的功能僅適用於傳統交換器，使用 SDN 的 OpenFlow 交換器不適用這功能。</p>
<input type="text" value="Search ..."/>	搜尋由 Probe 功能搜尋的交換器
<button>Remove Selected</button>	刪除由 Probe 功能搜尋的交換器
<button>+ Add Selected</button>	新增由 Probe 功能搜尋的交換器到管理頁面
<button>Probe Switches</button>	以 IP 對網路環境進行交換器搜尋
Vendor	交換器的廠商
Model	交換器的型號
IPv4	交換器的 IP
Status	交換器的狀態

4.2. VLAN

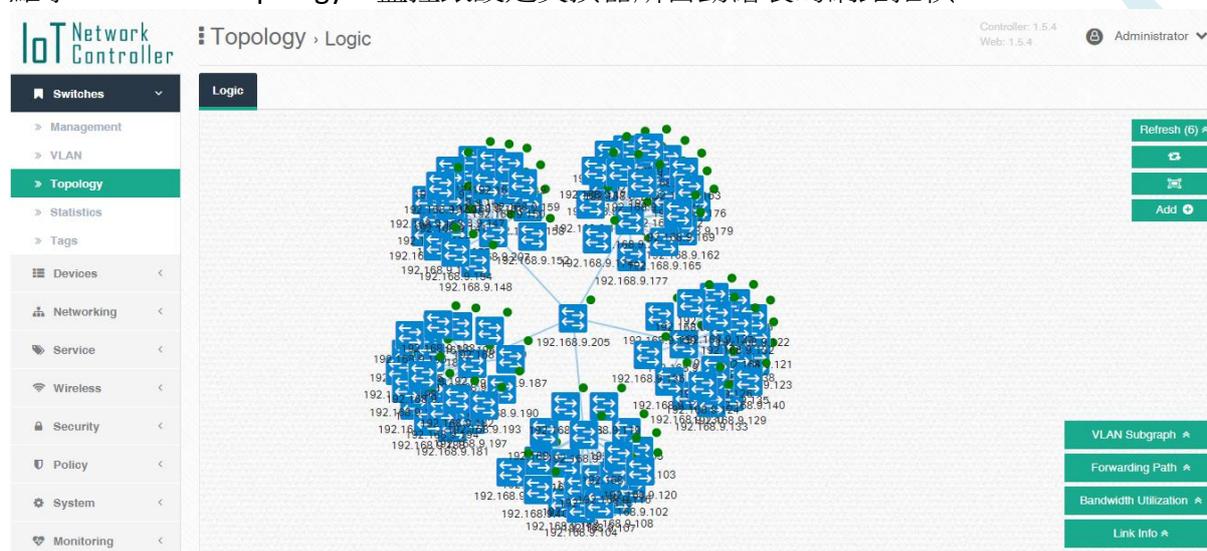
點擊 Switches > VLAN，觀看或修改 VLAN 設定



標籤名稱	標籤說明
 Search ...	搜尋已新增的 VLAN
 Delete Selected	刪除已選定的 VLAN
	新增一組 VLAN ID、ID 顏色和名稱
VLAN	VLAN ID
Name	VLAN 的名稱
	觀看 VLAN 的詳細資料
	修改 VLAN 的名稱與顏色
	移除 VLAN ID，功能必須在無任何 Port 使用的情況下進行刪除

4.3. Topology

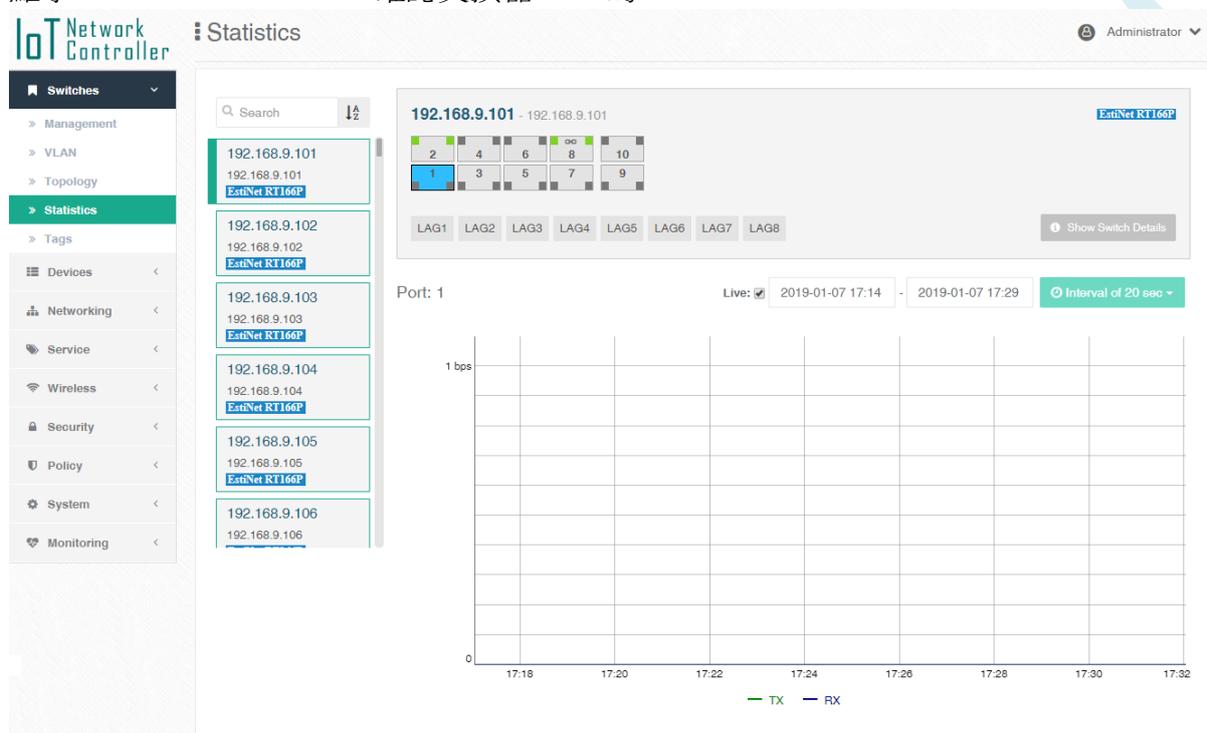
點擊 Switches > Topology，監控跟設定交換器所自動繪製的網路拓樸



標籤名稱	標籤說明
	每十五秒自動更新一次網路拓樸，可停止更新和馬上更新
	自動布置網路拓樸
	把網路拓樸移至中心
	手動新增交換器(Switch)、AP(Access Point)、防火牆(GI200)和連線(Link)
	顯示選定的 VLAN 子拓樸
	顯示來源 IP(Source IP)與目的 IP(Destination IP)經過的拓樸路徑
	網路拓樸的頻寬使用率百分比
	顯示連線詳細資訊

4.4. Statistics

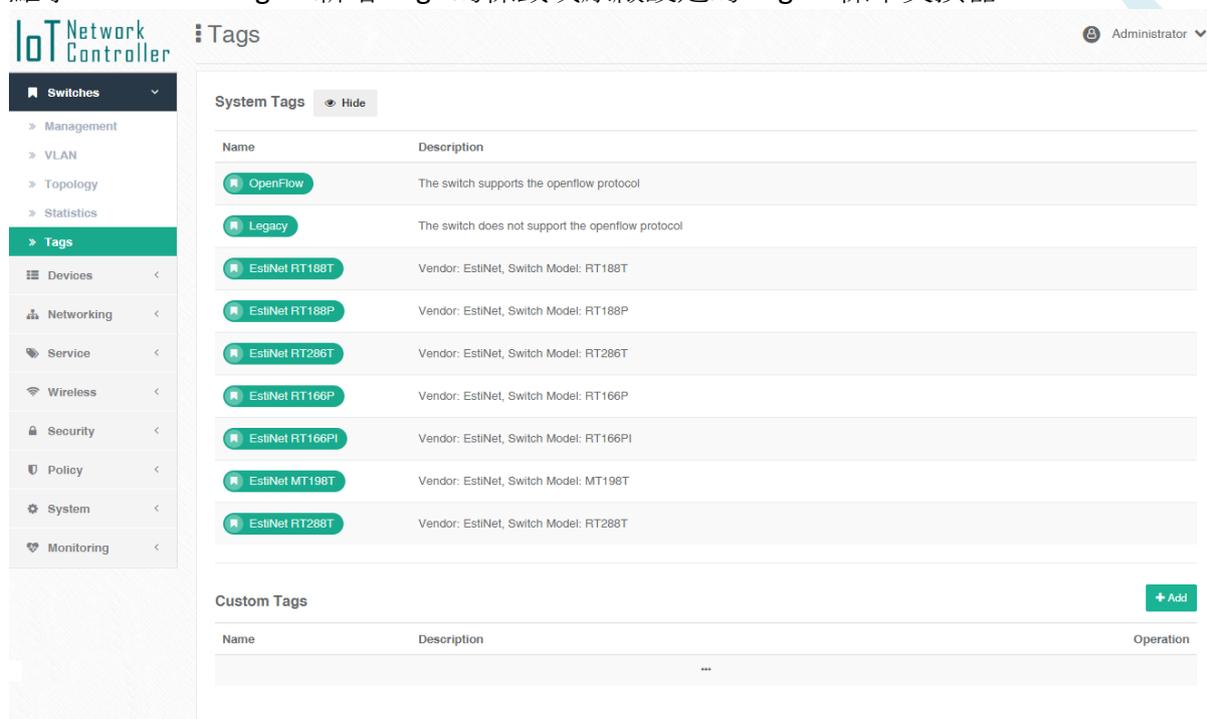
點擊 Switches > Statistics，確認交換器 Port 的 Statistics



標籤名稱	標籤說明
	收尋交換器並透過交換器的名字、廠商以及 IP 進行排列
	選擇查看 Statistics 的交換器
	查看 Port 的 Statistics
	查看 LAG 的 Statistics
	交換器的詳細內容
	勾選時會自動更新流量
	手動設定顯示 Statistics 的時間範圍
	設定 Statistics 每點的區間間隔

4.5. Tags

點擊 Switches > Tags，新增 Tags 的標籤或原廠設定的 Tags，標示交換器



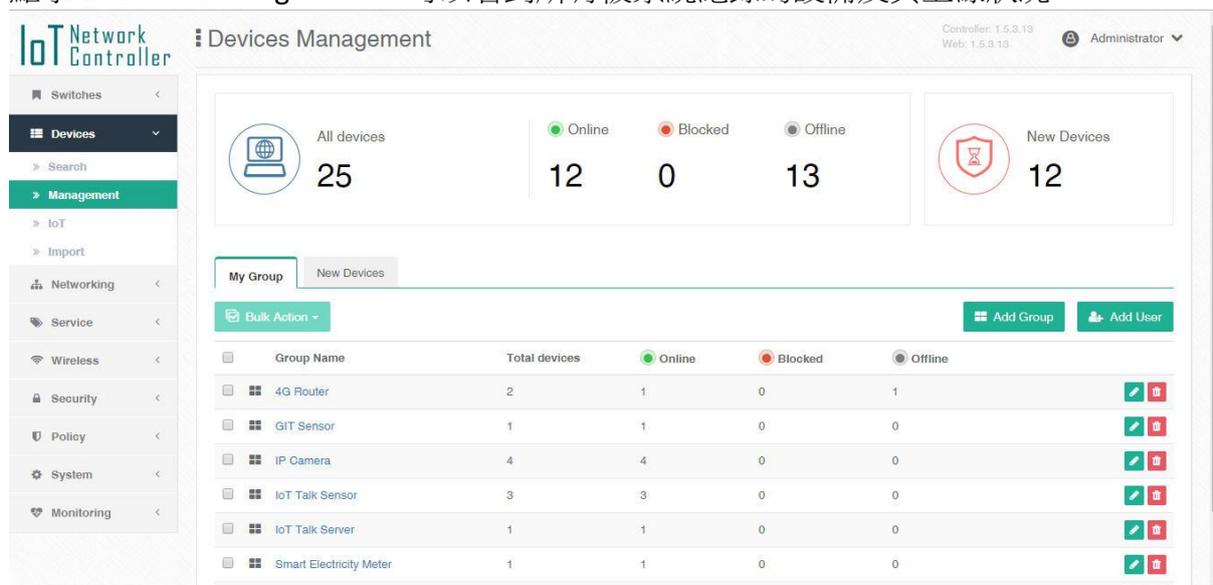
標籤名稱	標籤說明
System Tags	
 Hide	隱藏或顯示系統預設的 Tags
Name	Tag 的名稱
Description	Tag 的描述
 Legacy	標籤的名稱與顏色
Custom Tags	
 Add Tag	新增自訂的 tag
Name	Tag 的名稱
Description	Tag 的描述
Operation	可以對 TAG 進行修改跟刪除
	修改 Tag 的名稱、描述和顏色
	刪除 Tag

5. Device

5.1. 設備清單

5.1.1. 設備 Dashboard

點擊 Device > Management，可以看到所有被系統紀錄的設備及其上線狀況

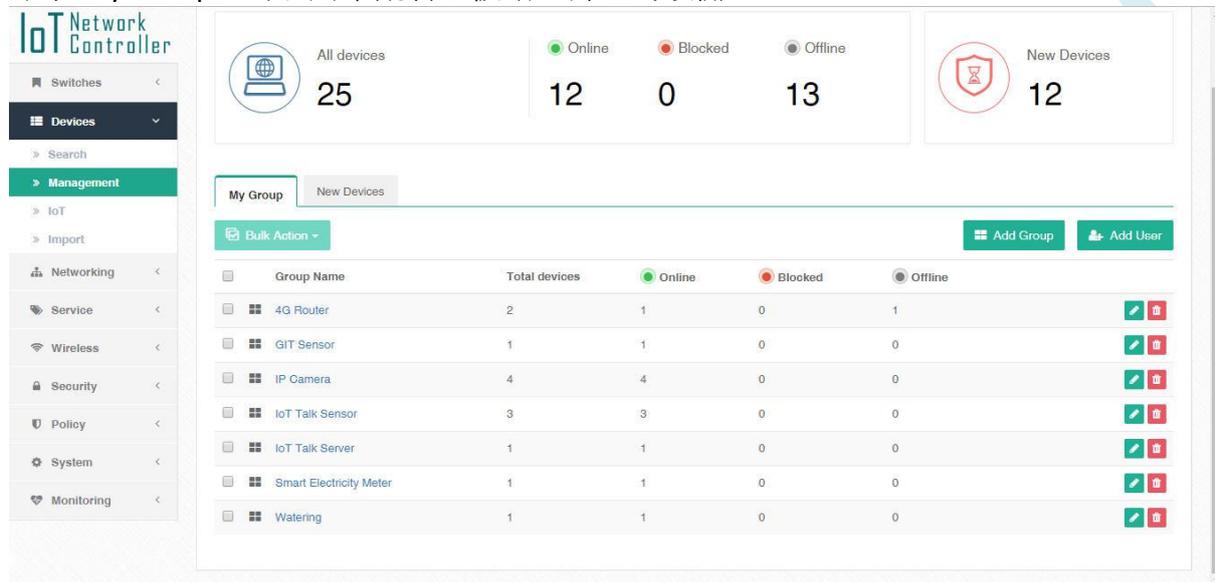


標籤名稱	標籤說明
所有被系統紀錄的設備及其上線狀況	
 <p>All devices 25</p>	全部上線過的設備數量
<p>● Online 12</p>	上線的設備數量
<p>● Blocked 0</p>	被拒絕上線的設備數量
<p>● Offline 13</p>	目前下線的設備數量

 <p>New Devices 12</p>	<p>沒有被編進去 Group 裡的設備數量</p>
<p>群組及新設備</p>	
<p>My Group</p>	<p>已編入群組裡的設備</p>
<p>New Devices</p>	<p>尚未編入群組裡的設備</p>

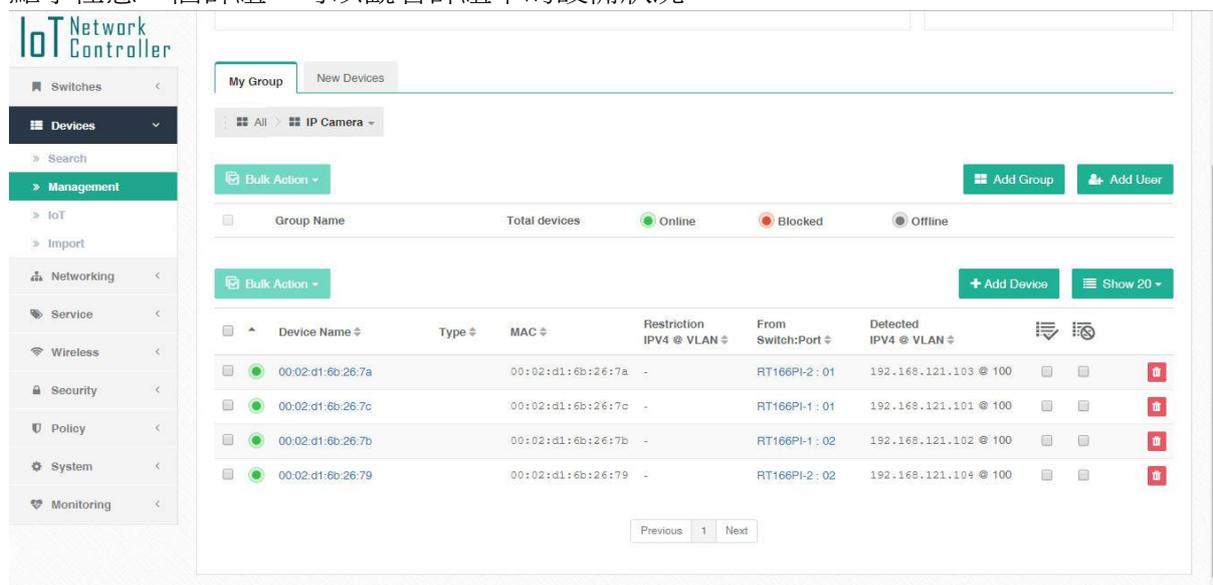
5.1.2. My Group

點擊 My Group，可以用來觀看已被編入群組的設備



標籤名稱	標籤說明
新增群組	
	新增一個群組
群組設備的數量及其上下線狀況	
Group Name	群組名稱
Total devices	該群組裡面的設備總數量
Online	群組上線設備的數量
Blocked	該群組裡面目前被拒絕上線的設備數量
Offline	該群組裡面目前下線的設備數量
	變更群組名稱
	刪除群組

點擊任意一個群組，可以觀看群組中的設備狀況

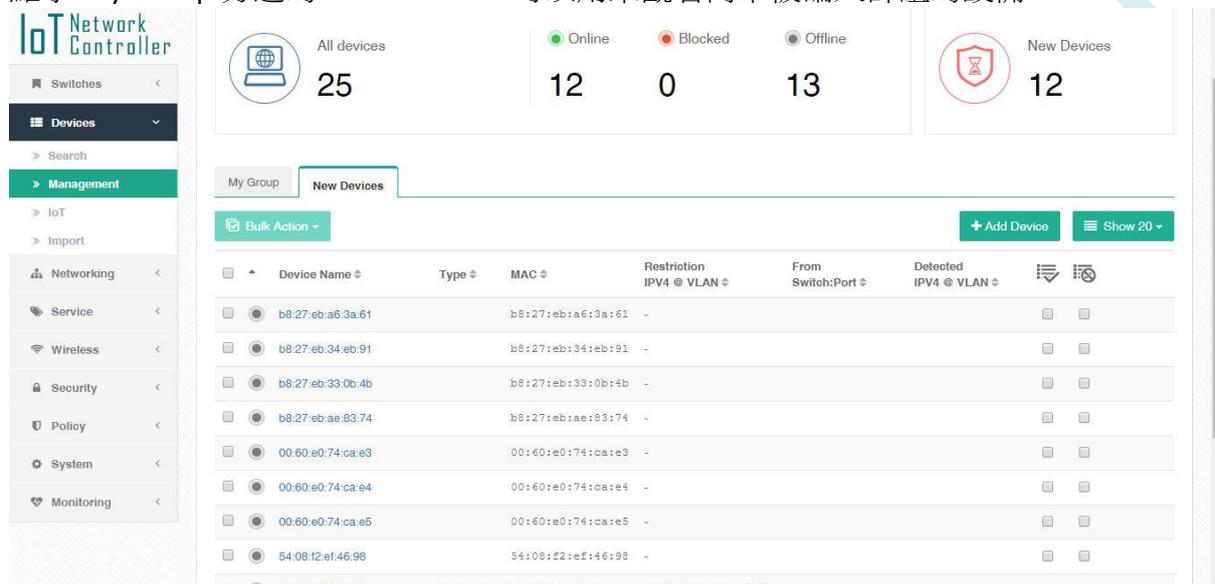


標籤名稱	標籤說明
觀看的群組	
	當前所觀看的組別
新增設備及展示	
	新增一個設備
	在此頁面中，展示 10, 20, 50, 100 個群組設備
該群組中的設備狀況	
	該設備名稱，可以點進去查看或修改設備詳細資訊 ● 為上線，● 為下線，● 為被拒絕上線
	該設備的類型(如:PC、IP Camera、Server)
	該設備的 Mac 位址
	限制此設備的 IP 位址與 VLAN

	此設備是透過哪一台交換機的 Port 連線
	系統偵測到此設備的 IP 位址與 VLAN
	勾選將此設備加入白名單
	勾選將此設備加入黑名單
	按下將此設備由群組中刪除

5.1.3. New Devices

點擊 My Group 旁邊的 New Device，可以用來觀看尚未被編入群組的設備



標籤名稱	標籤說明
新增設備及展示	
	新增一個設備
	在此頁面中，展示 10, 20, 50, 100 個群組設備
該群組中的設備狀況	
	該設備名稱，可以點進去修改(預設名稱是 Mac 位址) 為上線， 為下線， 為被拒絕上線
	該設備的類型(如:PC、IP Camera、Server)
	該設備的 Mac 位址
	限制此設備的 IP 位址與 VLAN
	此設備是透過哪一台交換機的 Port 連線

	系統偵測到此設備的 IP 位址與 VLAN
	勾選將此設備加入白名單
	勾選將此設備加入黑名單

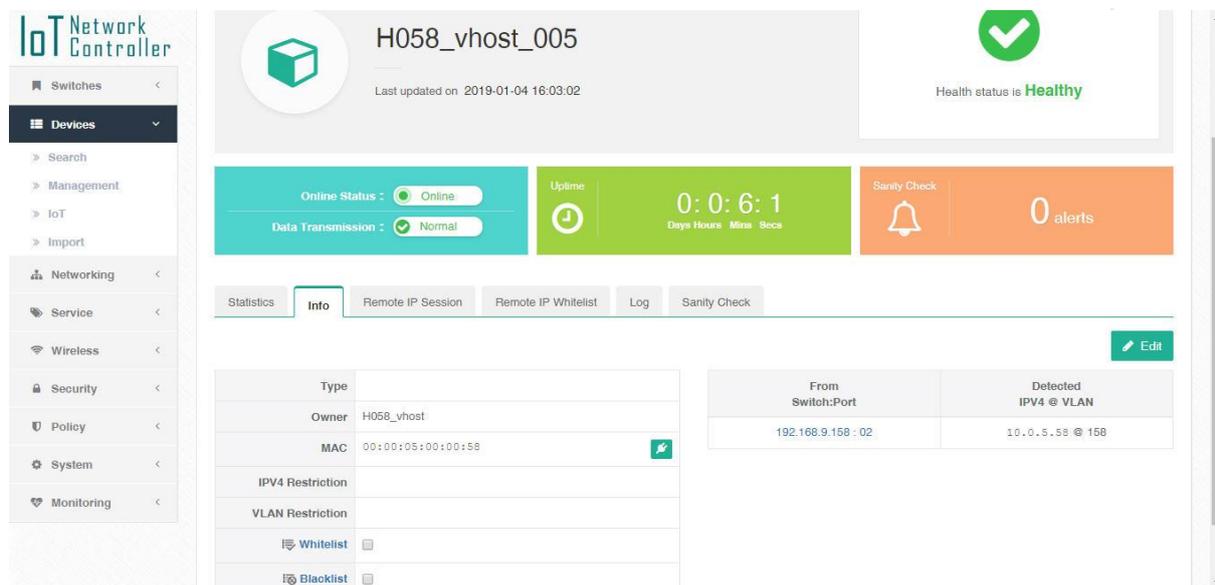
5.2. 設備內容資訊

點選任一設備的 Device Name，會進入 Device Information；點選 Switch Port 便會切換至該設備使用的交換機管理頁面

The screenshot displays the 'IoT Network Controller' interface. On the left is a sidebar with a menu including 'Switches', 'Devices', 'Management', 'IoT', 'Import', 'Networking', 'Service', 'Wireless', 'Security', 'Policy', 'System', and 'Monitoring'. The main area shows a group named 'H001_vhost'. Below this, there is a table of devices. The table has columns for 'Device Name', 'Type', 'MAC', 'Restriction', 'From Switch:Port', and 'Detected IPv4 @ VLAN'. Each row represents a device, such as 'H001_vhost_095', 'H001_vhost_001', etc., with their respective MAC addresses and network configurations. There are also buttons for 'Bulk Action', 'Add Group', 'Add User', 'Add Device', and 'Show 20'.

Device Name	Type	MAC	Restriction	From	Detected
			IPV4 @ VLAN	Switch:Port	IPV4 @ VLAN
H001_vhost_095		00:00:5f:00:00:01	-	192.168.9.101:02	10.0.95.1 @ 101
H001_vhost_001		00:00:01:00:00:01	-	192.168.9.101:02	10.0.1.1 @ 101
H001_vhost_009		00:00:09:00:00:01	-	192.168.9.101:02	10.0.9.1 @ 101
H001_vhost_038		00:00:26:00:00:01	-	192.168.9.101:02	10.0.38.1 @ 101
H001_vhost_028		00:00:1e:00:00:01	-	192.168.9.101:02	10.0.28.1 @ 101
H001_vhost_088		00:00:58:00:00:01	-	192.168.9.101:02	10.0.88.1 @ 101
H001_vhost_039		00:00:27:00:00:01	-	192.168.9.101:02	10.0.39.1 @ 101
H001_vhost_043		00:00:2b:00:00:01	-	192.168.9.101:02	10.0.43.1 @ 101
H001_vhost_079		00:00:4f:00:00:01	-	192.168.9.101:02	10.0.79.1 @ 101

5.2.1. Device Information



標籤名稱	標籤說明
新增設備及展示	
	該設備的類型(如:None、PC、IP Camera、Printer...)，可由設定者自己去 更改
H058_vhost_005	可以在這裡點選修改 Device 名稱，預設為 Mac 位址
	該設備在線的健康程度
設備狀況	
	在線狀態及資料傳輸狀態
	該設備的在線時間
	該設備的安全警告
設備細項資訊	

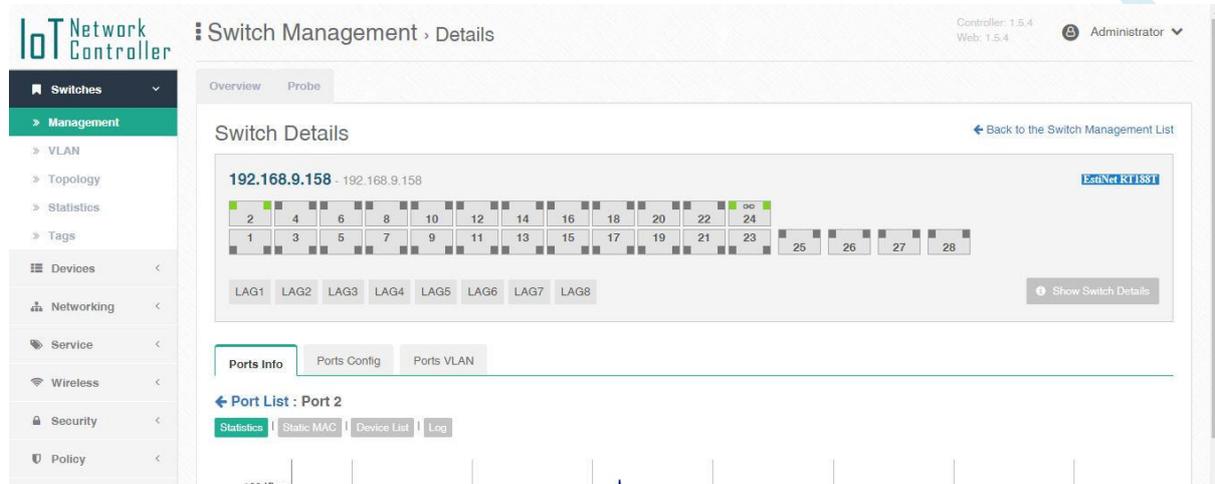
<p style="text-align: center;">Statistics</p>	<p>設備發送與接收的流量統計</p>
<p style="text-align: center;">Info</p>	<p>設備基本訊息</p> <p>Type : 該設備的類型</p> <p>Owner : 該設備的群組</p> <p>MAC : 該設備的 Mac 位址</p> <p>IPV4 Restriction : 限制連線此設備的 IPv4</p> <p>VLAN Restriction : 限制連線此設備的 VLAN</p> <p> : 設定 Static MAC</p> <p> Whitelist : 勾選加入白名單</p> <p> Blacklist : 勾選加入黑名單</p> <p>From</p> <p>Switch:Port : 連接此設備的交換機跟 Port 號</p> <p>Detected</p> <p>IPV4 @ VLAN : 系統偵測到此設備所使用的 IP 與 VLAN</p>
<p style="text-align: center;">Remote IP Session</p>	<p>遠端連線此設備的 Session 數量</p>
<p style="text-align: center;">Remote IP Whitelist</p>	<p>遠端連線此設備的白名單</p>
<p style="text-align: center;">Log</p>	<p>此設備的 Log 紀錄資料</p>
<p style="text-align: center;">Sanity Check</p>	<p>連線此設備的健全性檢查</p> <p> Add Rule : 新增四項 Alert 通知</p> <p>Traffic Alert  Add : 新增流量通知</p> <p>Offline Alert  Add : 新增下線通知</p> <p>High Latency  Add : 新增高 Latency 通知</p> <p>IP Session Exceed  Add : 新增 IP Session 過多通知</p> <p>Alerts : 已經發生 Alert 的數量</p> <p>Rule Type : Alert 的總類</p> <p>Rule/Threshold : Rule 的內容</p> <p>Action : 發生 Alert 時啟動的行為</p> <p>Send notification : 是否發 Mail 通知</p>

	 : 删除 Rule
--	---

EstiNet

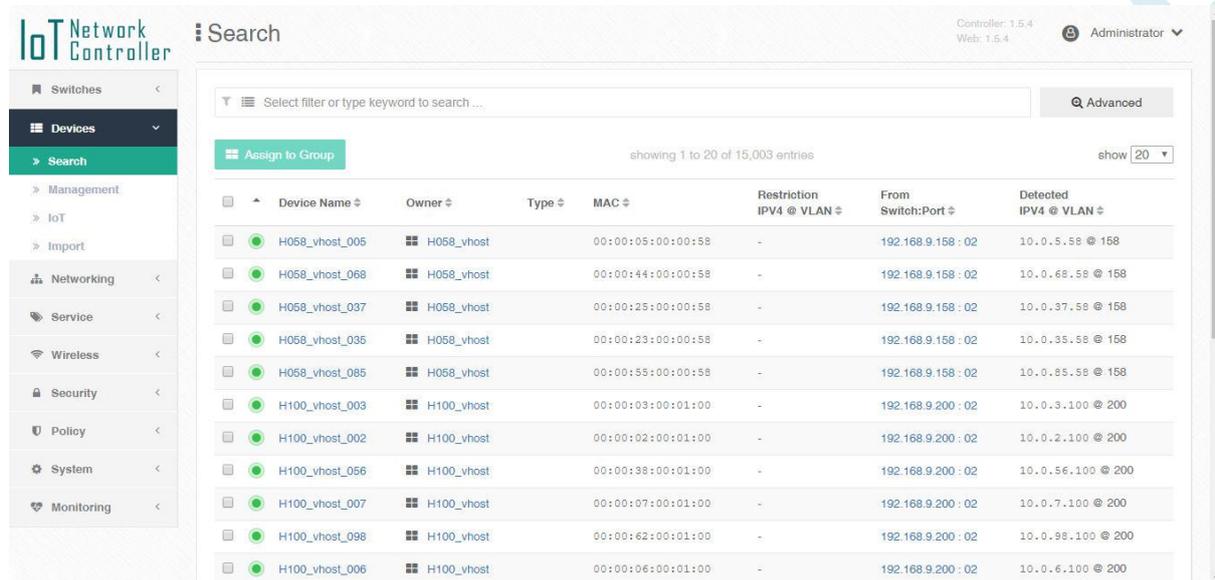
5.2.2. Switch Port

點選 Switch Port，就會進入交換機管理頁面，可以去配置交換機 Port 上的設定

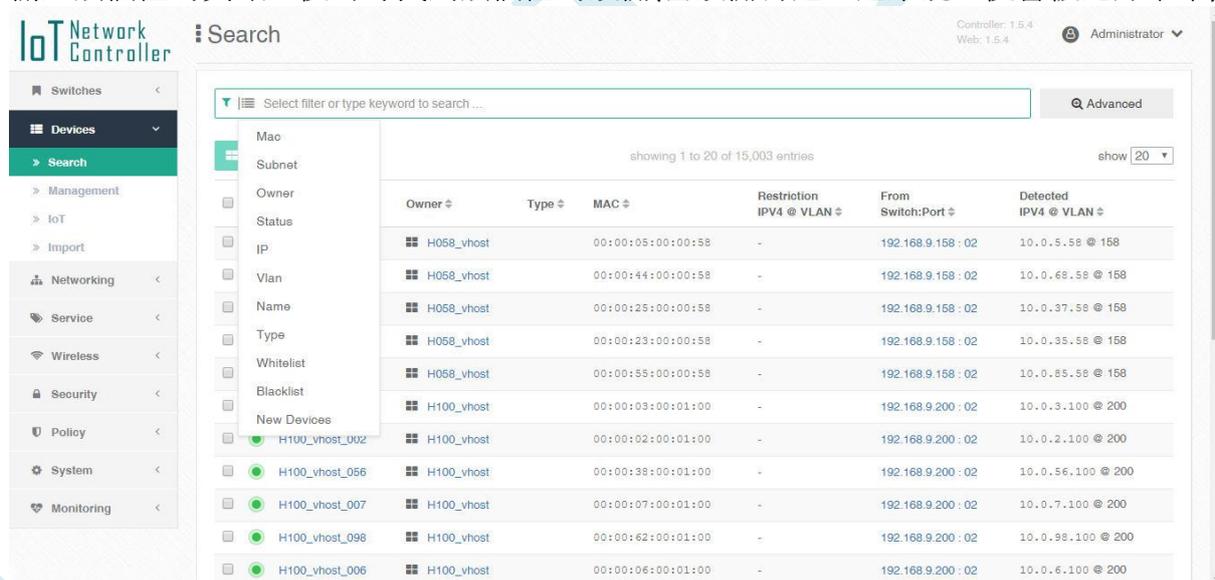


5.3. 設備搜尋

點擊左邊 Device > Search，可以看 Device 的搜索頁面



點擊上方的搜索欄位，便可出現要搜索的欄目(如:Mac、Subnet、Owner、Status...等)，輸入該欄位的資訊，便可尋找到該欄位的設備(當設備有連上過系統，便會被記錄下來)

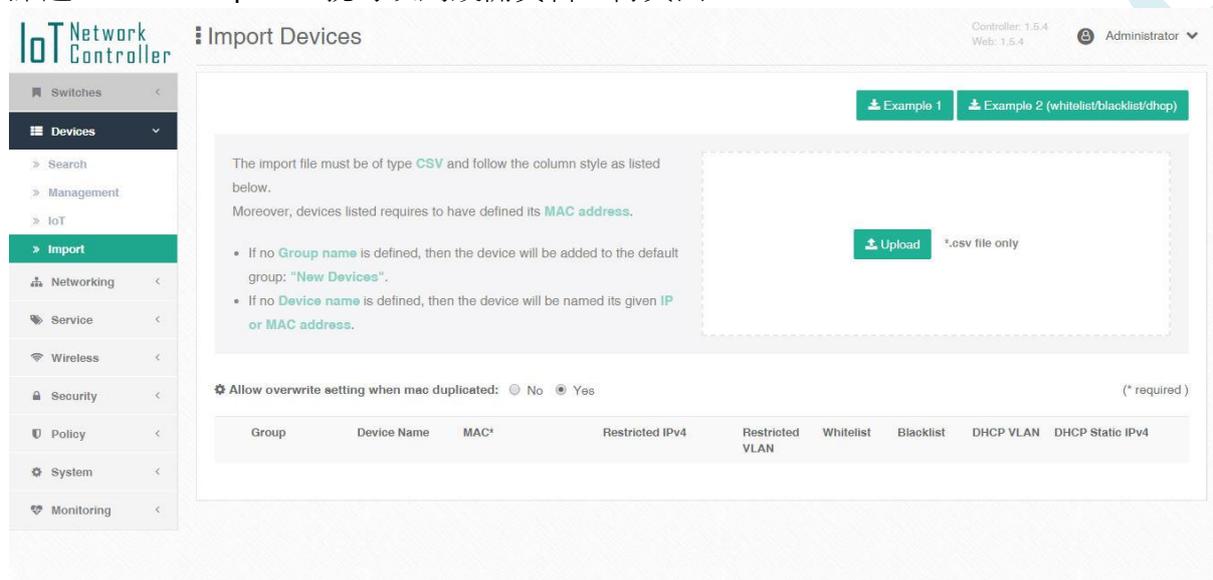


標籤名稱	標籤說明
設備展示	
show 20 ▼	在此頁面中，展示 10, 20, 50, 100 個群組設備
該群組中的設備狀況	

Device Name ⇅	該設備名稱，可以點進去修改(預設名稱是 Mac 位址) <input checked="" type="radio"/> 為上線， <input type="radio"/> 為下線
Owner ^	該設備的群組名稱
Type ⇅	該設備的類型(如:PC、IP Camera、Server)
MAC ⇅	該設備的 Mac 位址
Restriction IPV4 @ VLAN ⇅	限制此設備的 IP 位址與 VLAN
From Switch:Port ⇅	此設備是透過哪一台交換機的 Port 連線
Detected IPV4 @ VLAN ⇅	系統偵測到此設備的 IP 位址與 VLAN

5.4. 設備資料上傳

點選 Device > Import，就可以到設備資料上傳頁面



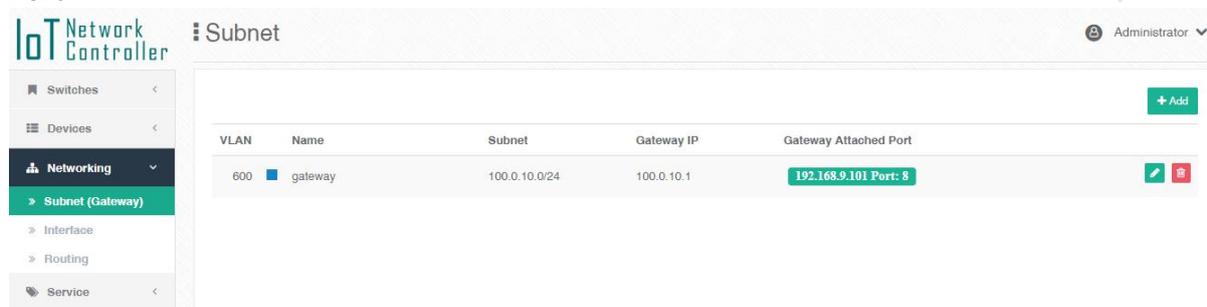
標籤名稱	標籤說明
設備上傳格式	
<ol style="list-style-type: none"> 1. 要上傳的設備資料必須符合 CSV 檔案格式，可由旁邊的 Example1 跟 Example 2(whilelist/blacklist/dhcp)當作參考格式使用 2. 設備清單必須包含設備的 Mac 位址 3. 如果沒填入群組名稱(Group Name)，則設備會被建置在新設備(New Device)上 4. 如果沒填入設備名稱(Device Name)，則設備會以 IP 或 Mac 位址做命名 5. Allow overwrite setting when mac duplicated: 選擇是否 Mac 位址一樣時，允許覆寫設定 	
設備資料	
Group	設備群組
Device Name	設備名稱
MAC*	設備的 MAC 位址(此欄位必須要有)
Restricted IPv4	限制此設備連線的 IPv4
Restricted VLAN	限制此設備連線的 VLAN

Whitelist	白名單
Blacklist	黑名單
DHCP VLAN	DHCP 派發 IP 所使用的 VLAN
DHCP Static IPv4	DHCP 下使用固定的 IPv4
 Upload	點擊上傳，僅適用 CSV 檔

6. Network

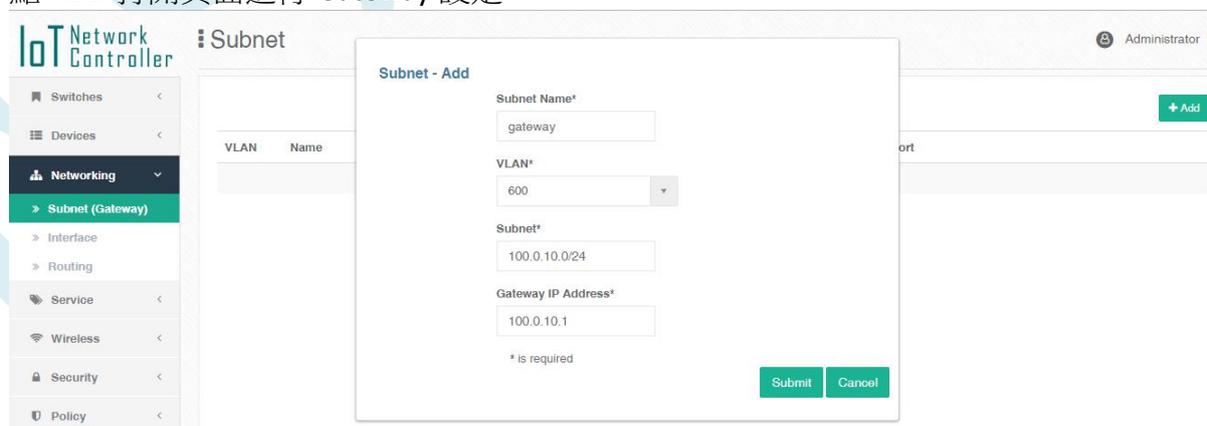
6.1. Subnet (Gateway)

點選 Networking > Subnet (Gateway)，設定 VLAN 的 IP subnet、Gateway IP 與 Gateway Port



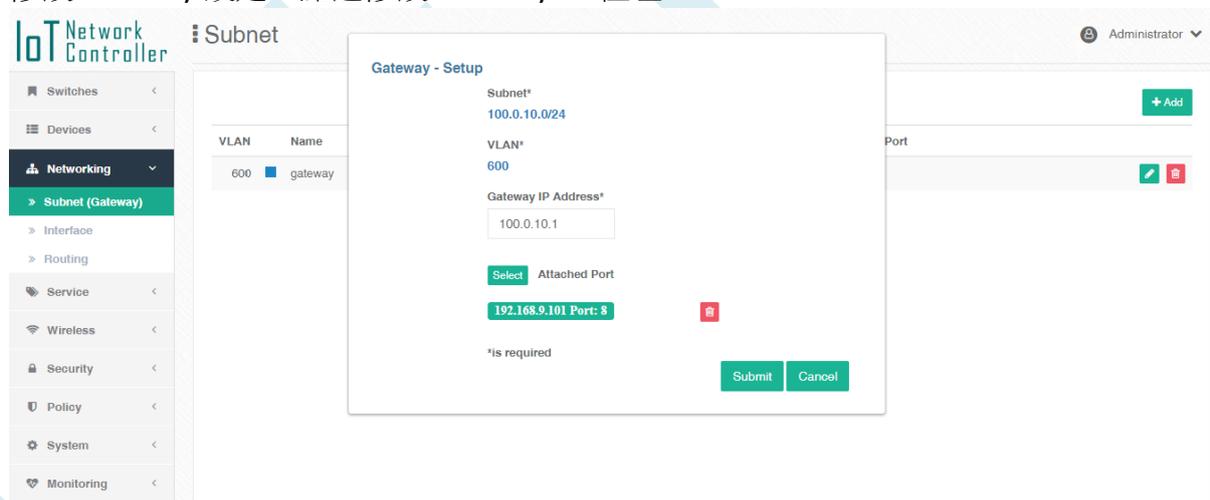
標籤名稱	標籤說明
VLAN	顯示 VLAN ID
Name	顯示名稱
Subnet	顯示 Subnet
Gateway IP	顯示該 Subnet 的 Gateway IP
Gateway Attached Port	顯示 Gateway IP 的 Gateway Attached Port
	新增 Subnet 設定
	修改 Subnet 設定 (可新增/修改 Gateway attached port 設定)
	刪除 Subnet 的設定

點選 ADD 打開頁面進行 Gateway 設定



標籤名稱	標籤說明
Subnet Name* <input type="text" value="gateway"/>	設定 Subnet 的名稱
VLAN* <input type="text" value="600"/>	設定 Subnet 的 VLAN ID
Subnet* <input type="text" value="100.0.10.0/24"/>	設定 VLAN 的 IP subnet
Gateway IP Address* <input type="text" value="100.0.10.1"/>	設定 Gateway IP 位址
<input type="button" value="Submit"/>	確認設定
<input type="button" value="Cancel"/>	取消設定

修改 Gateway 設定，點選修改 Gateway IP 位址

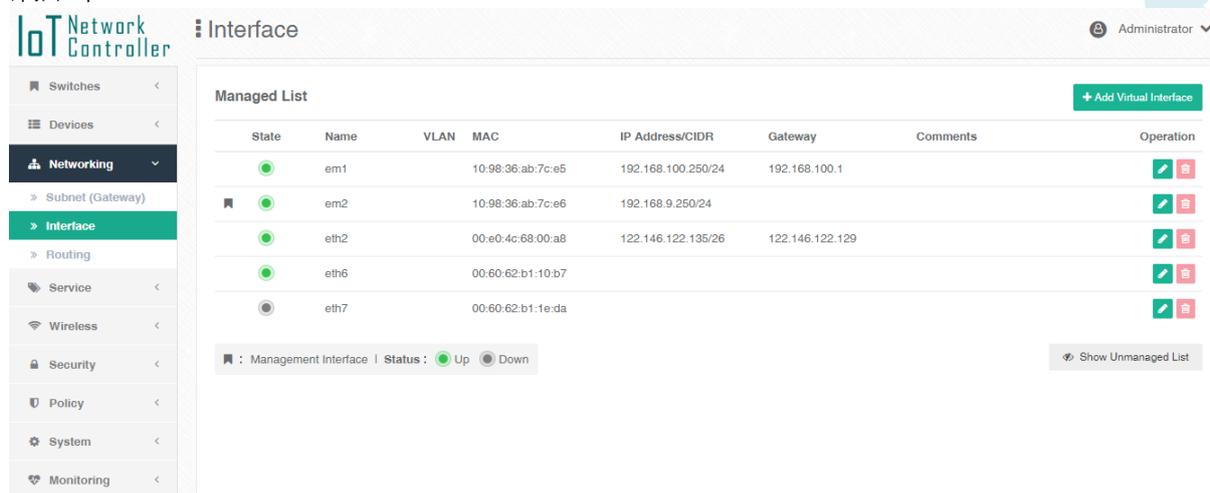


標籤名稱	標籤說明
Gateway IP Address* <input type="text" value="100.0.10.1"/>	設定 Gateway IP 位址
<input type="button" value="Select"/> Attached Port	設定連接著該 VLAN 的 Gateway Port

	移除 Gateway Port
	確認設定
	取消設定

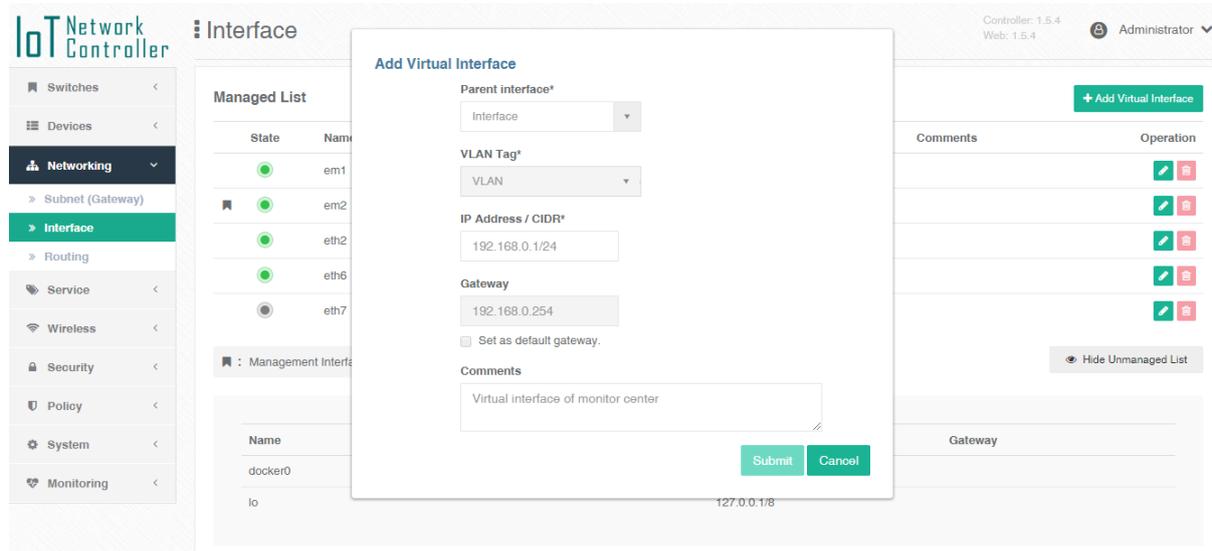
6.2. Interface

點選 Networking > interface，觀看 Controller 本身所有網路卡的設定，可新增刪除虛擬網路卡



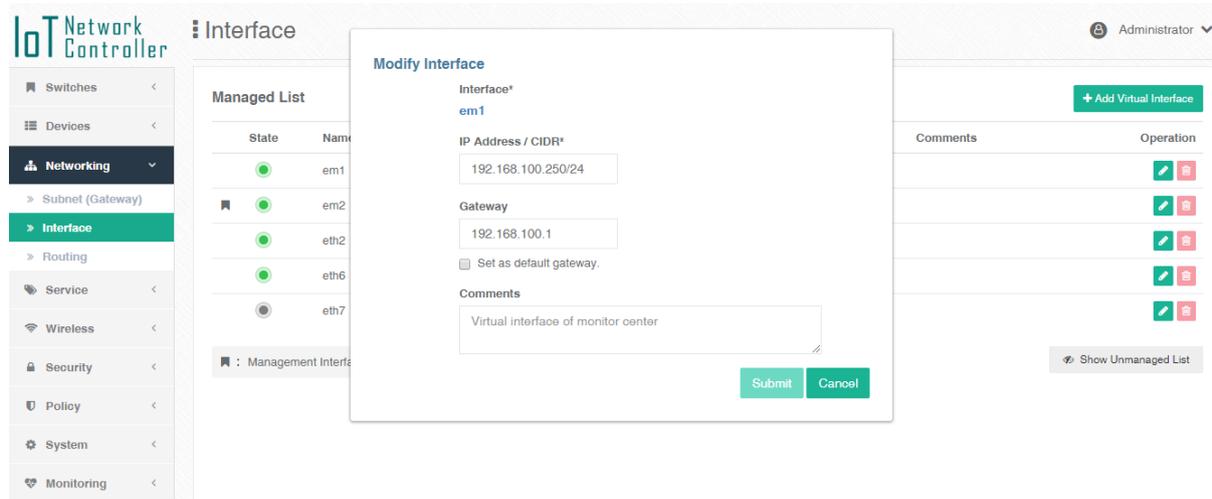
標籤名稱	標籤說明
	新增一張虛擬網路卡
State	網路卡的狀態
Name	網路卡的名稱
VLAN	網路卡的 VLAN ID
MAC	網路卡的 MAC
IP Address/CIDR	網路卡的 IP
Gateway	網路卡的 Gateway
Comments	網路卡的說明
Operation	可以進行修改予刪除
	修改網路卡的設定如 IP 位址和 Gateway 設定
	刪除一張虛擬網路卡，無法刪除實體網路卡
	展示其他類型的虛擬網路卡如 docker 產生的網路卡或 lo

點擊右上角新增虛擬網路卡，新增虛擬網路卡



標籤名稱	標籤說明
Parent interface* <input type="text" value="Interface"/>	選擇要虛擬網路卡建立於實體網路卡
VLAN Tag* <input type="text" value="VLAN"/>	選擇虛擬網路卡的 VLAN ID
IP Address / CIDR* <input type="text" value="192.168.0.1/24"/>	設定虛擬網路卡的 IP 位址
Gateway <input type="text" value="192.168.0.254"/>	設定虛擬網路卡的 Gateway IP 位址
<input type="checkbox"/> Set as default gateway.	選定虛擬網路卡為 Default Gateway
Comments <input type="text" value="Virtual interface of monitor center"/>	新增虛擬網路卡的說明
<input type="button" value="Submit"/>	確認設定
<input type="button" value="Cancel"/>	取消設定

修改虛擬網路卡或實體網路卡的設定



標籤名稱	標籤說明
Interface* em1	網路卡名稱
IP Address / CIDR* 192.168.100.250/24	修改虛擬網路卡的 IP 位址
Gateway 192.168.100.1	修改虛擬網路卡的 Gateway IP 位址
<input type="checkbox"/> Set as default gateway.	選定該虛擬網路卡的 Gateway 為 Default Gateway
Comments Virtual interface of monitor	修改虛擬網路卡的說明
Submit	確認設定
Cancel	取消設定

7. Service

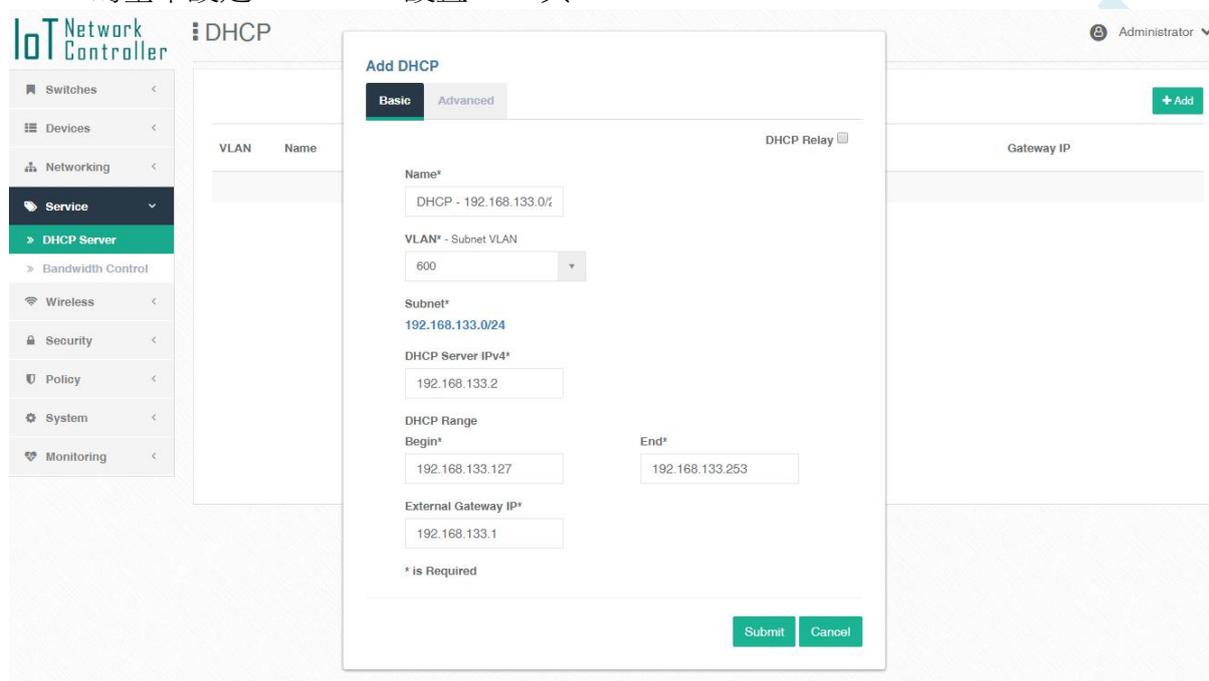
7.1. DHCP Server

點選 Service > DHCP Server，新增 DHCP 服務功能



標籤名稱	標籤說明
	新增一個 DHCP Service
VLAN	DHCP 的 VLAN ID
Name	DHCP 的名稱
Subnet	DHCP 支援的 subnet
IPv4 (DHCP Server Address)	DHCP Server 的 IP
Range	DHCP 支援的 IP Range
Gateway IP	DHCP 配發 Gateway IP
DHCP - 192.168.133.0/24	可查看、修改和刪除 DHCP Service 的詳細設定

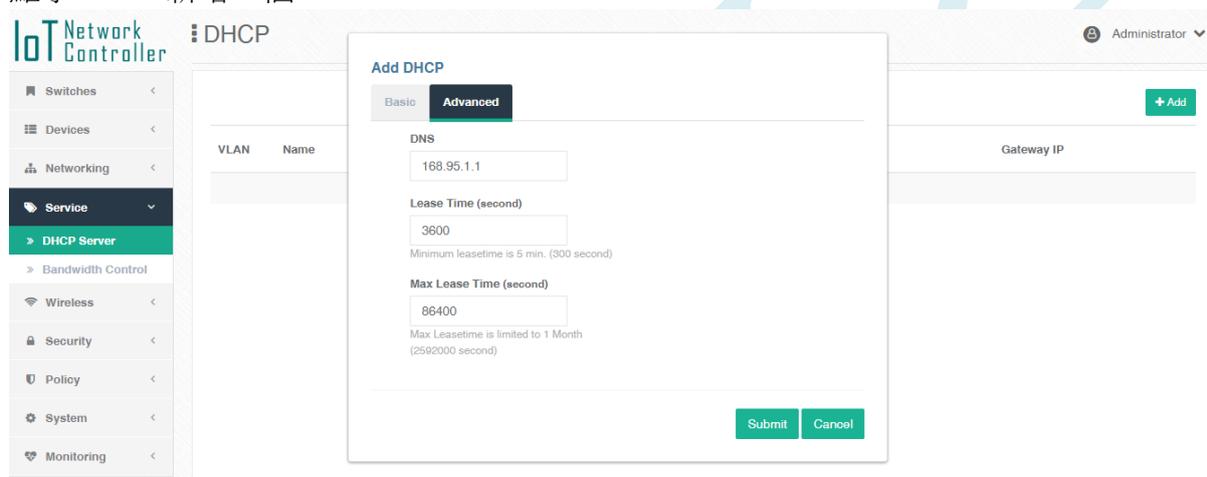
新增 DHCP 設定，點選 ADD 進行設定，設定分成兩部分 Basic 與 Advanced，Basic 設置 DHCP 的基本設定，Advance 設置 DNS 與 Lease Time



標籤名稱	標籤說明
DHCP Relay <input type="checkbox"/>	設定 DHCP Relay
Name* DHCP - 192.168.133.0/24	設定 DHCP Server 的名稱
VLAN* - Subnet VLAN 600	設定 DHCP Server 的 VLAN ID
Subnet* 192.168.133.0/24	確認 DHCP Server 的 Subnet
DHCP Server IPv4* 192.168.133.2	設定 DHCP Server 的 IP
Begin* 192.168.133.127	設定 DHCP Server 發放的 IP，從 Begin 開始發放 IP
End* 192.168.133.253	設定 DHCP Server 發放的 IP，End 為最後發放的 IP

External Gateway IP* <input type="text" value="192.168.133.1"/>	設定 DHCP IP 的 Gateway IP 位址
<input type="button" value="Submit"/>	確認設定
<input type="button" value="Cancel"/>	取消設定

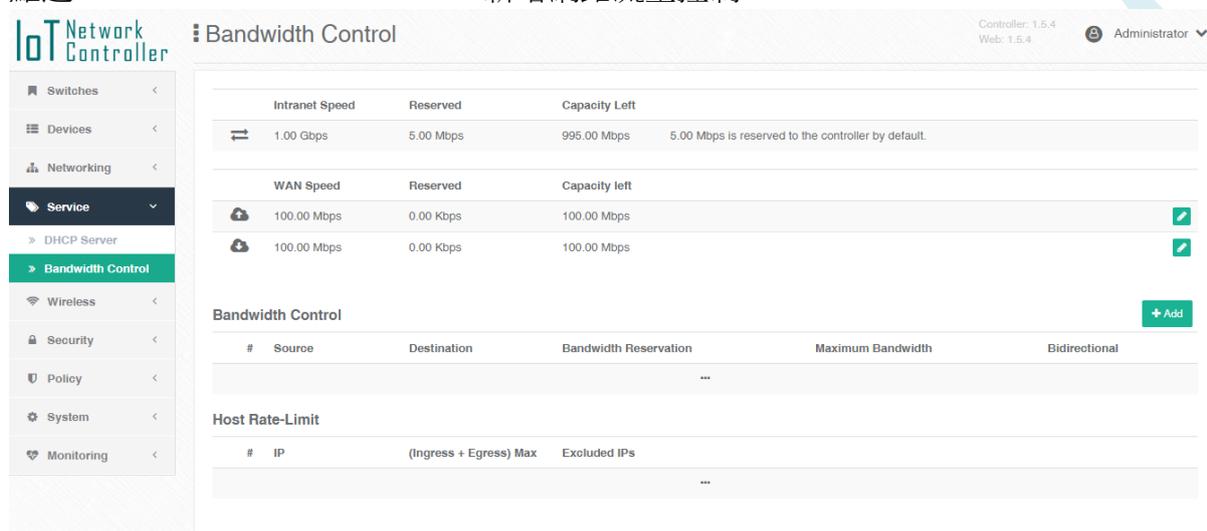
點擊 Add，新增一個 DHCP Server



標籤名稱	標籤說明
DNS <input type="text" value="168.95.1.1"/>	設定 DHCP Server 設定的 DNS
Lease Time (second) <input type="text" value="3600"/> <small>Minimum leasetime is 5 min. (300 second)</small>	設定 DHCP 他的最小註冊時間
Max Lease Time (second) <input type="text" value="86400"/> <small>Max Leasetime is limited to 1 Month (2592000 second)</small>	設定 DHCP 他的最大註冊時間
<input type="button" value="Submit"/>	確認設定
<input type="button" value="Cancel"/>	取消設定

7.2. Bandwidth Control

點選 Service > Bandwidth Control，新增網路流量控制

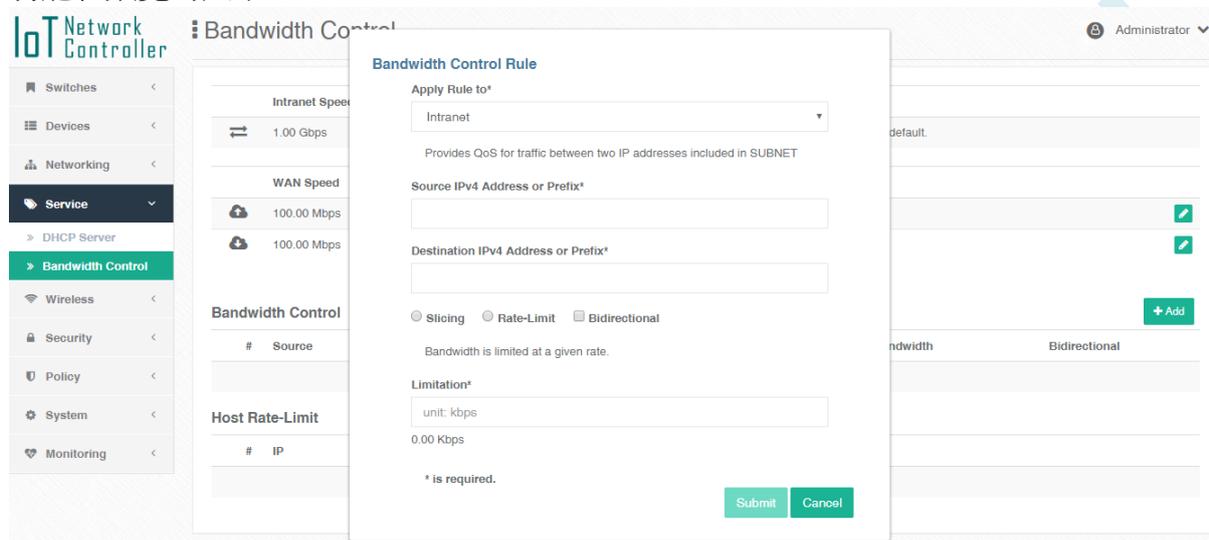


標籤名稱	標籤說明
Intranet Speed	網際網路頻寬
Reserved	保留頻寬
Capacity Left	可用頻寬
Intranet Speed	內聯網(或局域網)頻寬
Reserved	上傳保留頻寬
Capacity Left	上傳剩餘頻寬
WAN Speed	外聯網(或網際網路)頻寬
Reserved	下載保留頻寬
Capacity Left	下載剩餘頻寬
	設定上傳網際網路的頻寬上限

	設定下載網際網路的頻寬上限																												
<div data-bbox="229 376 1417 573"> <p>Bandwidth Control + Add</p> <table border="1"> <thead> <tr> <th>#</th> <th>Source</th> <th>Destination</th> <th>Bandwidth Reservation</th> <th>Maximum Bandwidth</th> <th>Bidirectional</th> <th></th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Internet</td> <td>10.10.20.142</td> <td>10.00 Mbps</td> <td></td> <td>No</td> <td> </td> </tr> <tr> <td>2</td> <td>10.10.20.142</td> <td>Internet</td> <td>6.00 Mbps</td> <td>6.00 Mbps</td> <td>No</td> <td> </td> </tr> <tr> <td>3</td> <td>Internet</td> <td>10.10.20.129</td> <td>10.00 Mbps</td> <td>10.00 Mbps</td> <td>No</td> <td> </td> </tr> </tbody> </table> </div>		#	Source	Destination	Bandwidth Reservation	Maximum Bandwidth	Bidirectional		1	Internet	10.10.20.142	10.00 Mbps		No	 	2	10.10.20.142	Internet	6.00 Mbps	6.00 Mbps	No	 	3	Internet	10.10.20.129	10.00 Mbps	10.00 Mbps	No	 
#	Source	Destination	Bandwidth Reservation	Maximum Bandwidth	Bidirectional																								
1	Internet	10.10.20.142	10.00 Mbps		No	 																							
2	10.10.20.142	Internet	6.00 Mbps	6.00 Mbps	No	 																							
3	Internet	10.10.20.129	10.00 Mbps	10.00 Mbps	No	 																							
	新增一條頻寬控制的設定																												
Source	來源 IP																												
Destination	目的 IP																												
Bandwidth Reservation	頻寬保留																												
Maximum Bandwidth	最大頻寬																												
Bidirectional	是否雙向設定																												
	修改頻寬設定																												
	刪除頻寬設定																												
<div data-bbox="229 1339 1417 1473"> <p>Host Rate-Limit</p> <table border="1"> <thead> <tr> <th>#</th> <th>IP</th> <th>(Ingress + Egress) Max</th> <th>Excluded IPs</th> <th></th> </tr> </thead> <tbody> <tr> <td>1</td> <td>100.0.10.0/24</td> <td>4.00 Mbps</td> <td></td> <td> </td> </tr> </tbody> </table> </div>		#	IP	(Ingress + Egress) Max	Excluded IPs		1	100.0.10.0/24	4.00 Mbps		 																		
#	IP	(Ingress + Egress) Max	Excluded IPs																										
1	100.0.10.0/24	4.00 Mbps		 																									
IP	限制的 IP Address																												
(Ingress + Egress) Max	最大流量																												
Excluded IPs	被拒絕的 IP Address																												
	修改頻寬設定																												
	刪除頻寬設定																												

EstiNet

點選 **Add** 設定網路頻寬設定，請依序設定：套用規則的種類、來源目的、頻寬設定的功能和頻寬的大小



標籤名稱	標籤說明
Apply Rule to* Intranet	選擇頻寬的總類: Internet、Internet Download、Internet Upload 和 Host Rate limite
Source IPv4 Address or Prefix*	設定頻寬的來源端 IP
Destination IPv4 Address or Prefix*	設定頻寬的目的端 IP
<input type="radio"/> Slicing	設定保留頻寬與限制頻寬
<input type="radio"/> Rate-Limit	設定限制頻寬
<input type="checkbox"/> Bidirectional	設定來源 IP 與目的 IP 的頻寬控制為雙向
<input type="radio"/> Reservation	設定保留頻寬
Limitation* unit: kbps	設定頻寬控制流量，單位為 Kbps
Exclude IPs	被排除的 IP Address

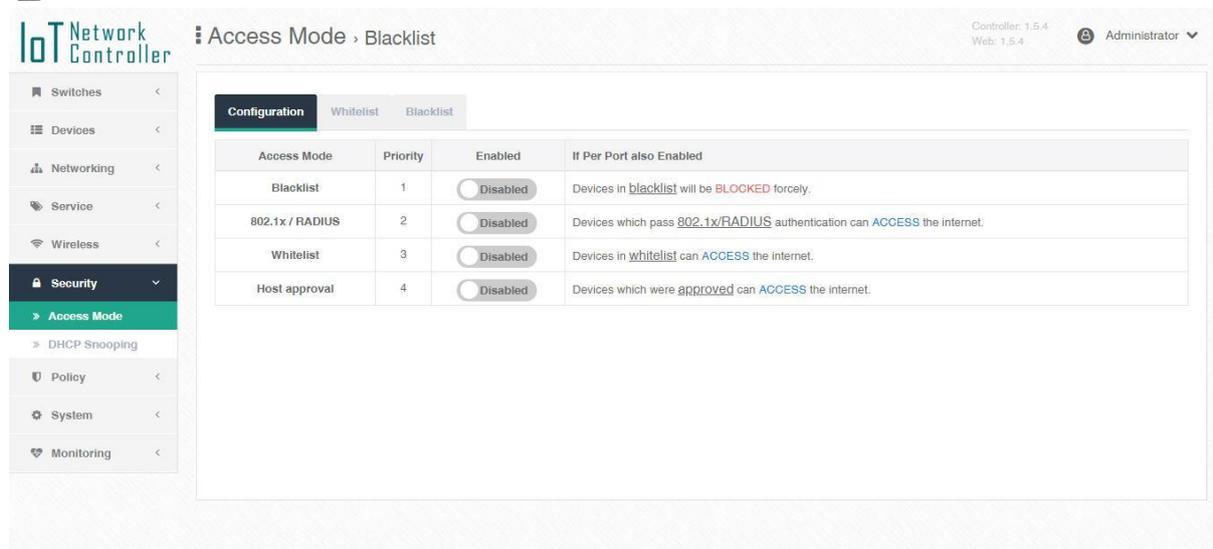
<input type="button" value="Submit"/>	確認設定
<input type="button" value="Cancel"/>	取消設定

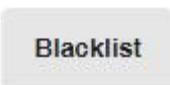
EstiNet

8. Security

8.1. 訪問模式配置

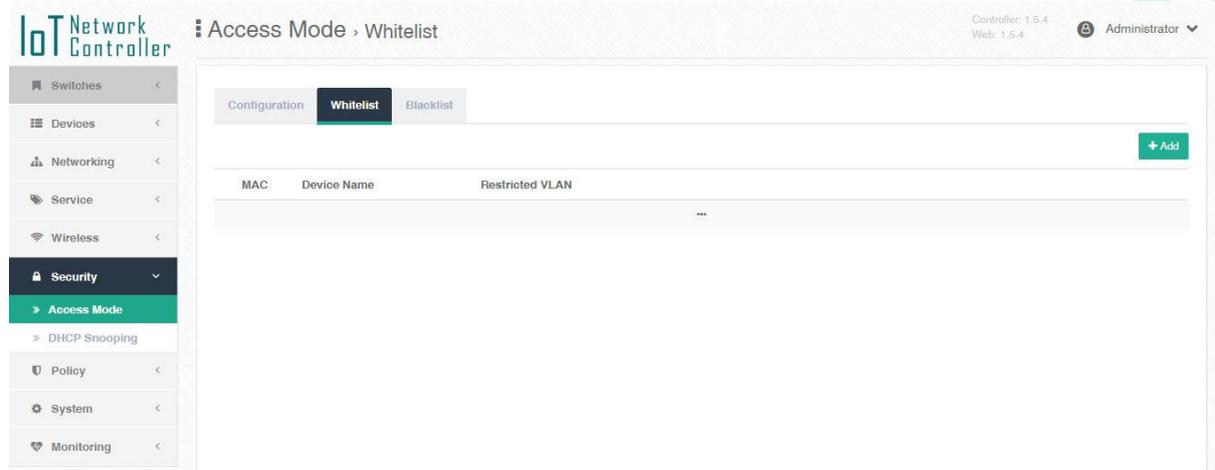
點選 Security > Access Mode，去設定開啟黑名單、802.1x / RADIUS、白名單以及准入管理



標籤名稱	標籤說明
安全設定配置	
Blacklist: 在黑名單裡的設備將強制拒絕上線	
802.1x / RADIUS: 通過 802.1x / RADIUS 身份驗證的設備可以訪問網路	
Whitelist: 在白名單裡的設備將可訪問網路	
Host approval: 被允許進入的設備才可以訪問網路	
配置頁面	
	<p>Access Mode : 訪問模式</p> <p>Priority : 權重</p> <p>Enabled : 點選開啟該訪問模式</p> <p>If Per Port also Enabled : 描述該訪問模式開啟後該 Port 的情況</p>
	白名單列表
	黑名單列表

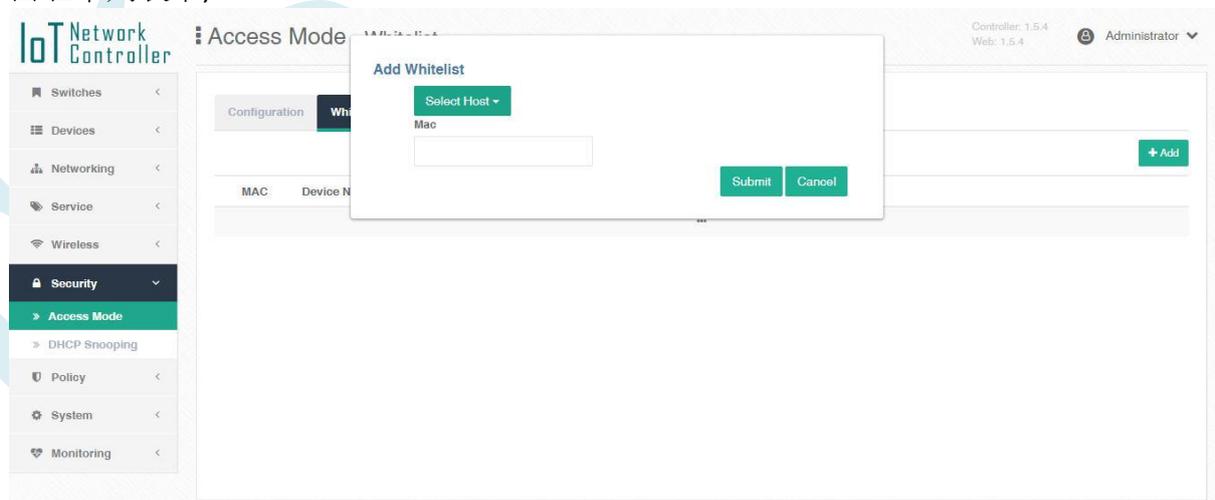
8.2. 白名單列表

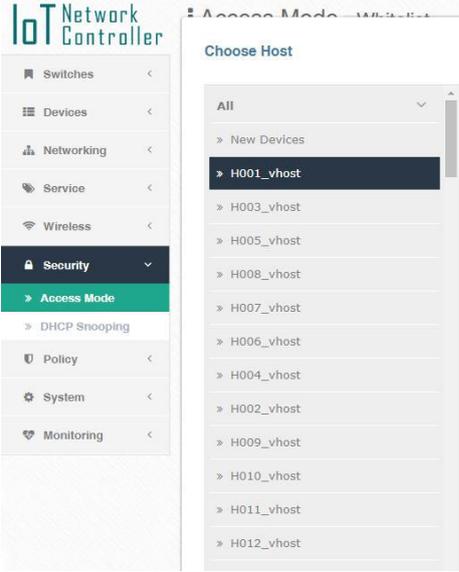
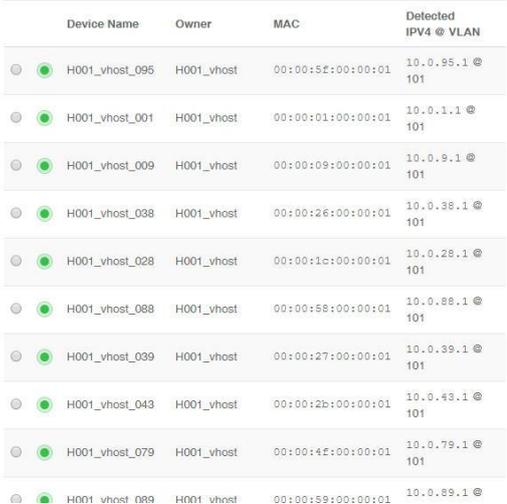
在白名單功能開啟時，只有加入白名單列表的設備才允許使用網路



標籤名稱	標籤說明
配置頁面	
	新設備加入白名單
	設備的 Mac 位址
	設備的名稱
	設備所限制的 VLAN

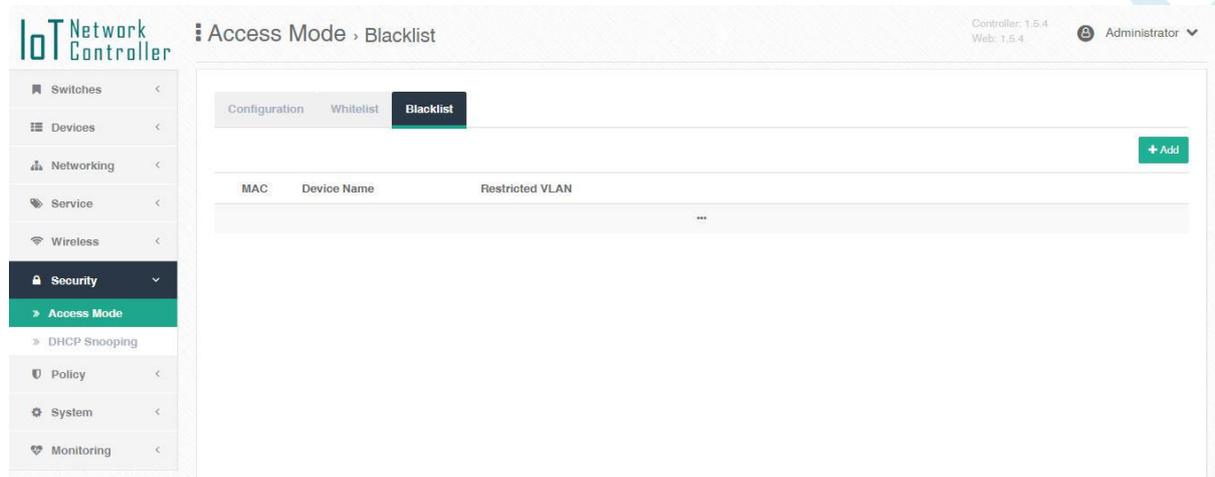
點選 Add，增加白名單列表(由 Device 頁面將單一設備加入白名單，也會同步出現在此白名單列表中)



標籤名稱	標籤說明																																												
配置頁面																																													
	下拉選單選擇要加入白名單的設備(已被系統紀錄下來的)，如下圖																																												
	 <table border="1" data-bbox="683 589 1190 1093"> <thead> <tr> <th>Device Name</th> <th>Owner</th> <th>MAC</th> <th>Detected IPV4 @ VLAN</th> </tr> </thead> <tbody> <tr><td>H001_vhost_096</td><td>H001_vhost</td><td>00:00:5E:00:00:01</td><td>10.0.95.1 @ 101</td></tr> <tr><td>H001_vhost_001</td><td>H001_vhost</td><td>00:00:01:00:00:01</td><td>10.0.1.1 @ 101</td></tr> <tr><td>H001_vhost_009</td><td>H001_vhost</td><td>00:00:09:00:00:01</td><td>10.0.9.1 @ 101</td></tr> <tr><td>H001_vhost_038</td><td>H001_vhost</td><td>00:00:26:00:00:01</td><td>10.0.38.1 @ 101</td></tr> <tr><td>H001_vhost_028</td><td>H001_vhost</td><td>00:00:10:00:00:01</td><td>10.0.28.1 @ 101</td></tr> <tr><td>H001_vhost_088</td><td>H001_vhost</td><td>00:00:58:00:00:01</td><td>10.0.88.1 @ 101</td></tr> <tr><td>H001_vhost_039</td><td>H001_vhost</td><td>00:00:27:00:00:01</td><td>10.0.39.1 @ 101</td></tr> <tr><td>H001_vhost_043</td><td>H001_vhost</td><td>00:00:2b:00:00:01</td><td>10.0.43.1 @ 101</td></tr> <tr><td>H001_vhost_079</td><td>H001_vhost</td><td>00:00:4f:00:00:01</td><td>10.0.79.1 @ 101</td></tr> <tr><td>H001_vhost_089</td><td>H001_vhost</td><td>00:00:59:00:00:01</td><td>10.0.89.1 @ 101</td></tr> </tbody> </table>	Device Name	Owner	MAC	Detected IPV4 @ VLAN	H001_vhost_096	H001_vhost	00:00:5E:00:00:01	10.0.95.1 @ 101	H001_vhost_001	H001_vhost	00:00:01:00:00:01	10.0.1.1 @ 101	H001_vhost_009	H001_vhost	00:00:09:00:00:01	10.0.9.1 @ 101	H001_vhost_038	H001_vhost	00:00:26:00:00:01	10.0.38.1 @ 101	H001_vhost_028	H001_vhost	00:00:10:00:00:01	10.0.28.1 @ 101	H001_vhost_088	H001_vhost	00:00:58:00:00:01	10.0.88.1 @ 101	H001_vhost_039	H001_vhost	00:00:27:00:00:01	10.0.39.1 @ 101	H001_vhost_043	H001_vhost	00:00:2b:00:00:01	10.0.43.1 @ 101	H001_vhost_079	H001_vhost	00:00:4f:00:00:01	10.0.79.1 @ 101	H001_vhost_089	H001_vhost	00:00:59:00:00:01	10.0.89.1 @ 101
Device Name	Owner	MAC	Detected IPV4 @ VLAN																																										
H001_vhost_096	H001_vhost	00:00:5E:00:00:01	10.0.95.1 @ 101																																										
H001_vhost_001	H001_vhost	00:00:01:00:00:01	10.0.1.1 @ 101																																										
H001_vhost_009	H001_vhost	00:00:09:00:00:01	10.0.9.1 @ 101																																										
H001_vhost_038	H001_vhost	00:00:26:00:00:01	10.0.38.1 @ 101																																										
H001_vhost_028	H001_vhost	00:00:10:00:00:01	10.0.28.1 @ 101																																										
H001_vhost_088	H001_vhost	00:00:58:00:00:01	10.0.88.1 @ 101																																										
H001_vhost_039	H001_vhost	00:00:27:00:00:01	10.0.39.1 @ 101																																										
H001_vhost_043	H001_vhost	00:00:2b:00:00:01	10.0.43.1 @ 101																																										
H001_vhost_079	H001_vhost	00:00:4f:00:00:01	10.0.79.1 @ 101																																										
H001_vhost_089	H001_vhost	00:00:59:00:00:01	10.0.89.1 @ 101																																										
	輸入已知的 Mac 位址加入白名單																																												
	點選確定加入白名單																																												

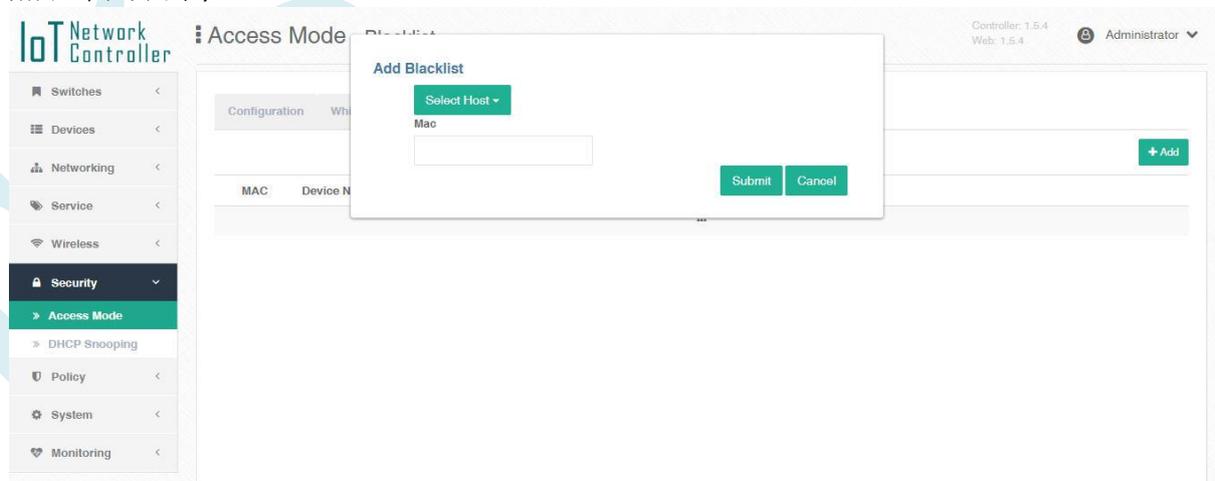
8.3. 黑名單列表

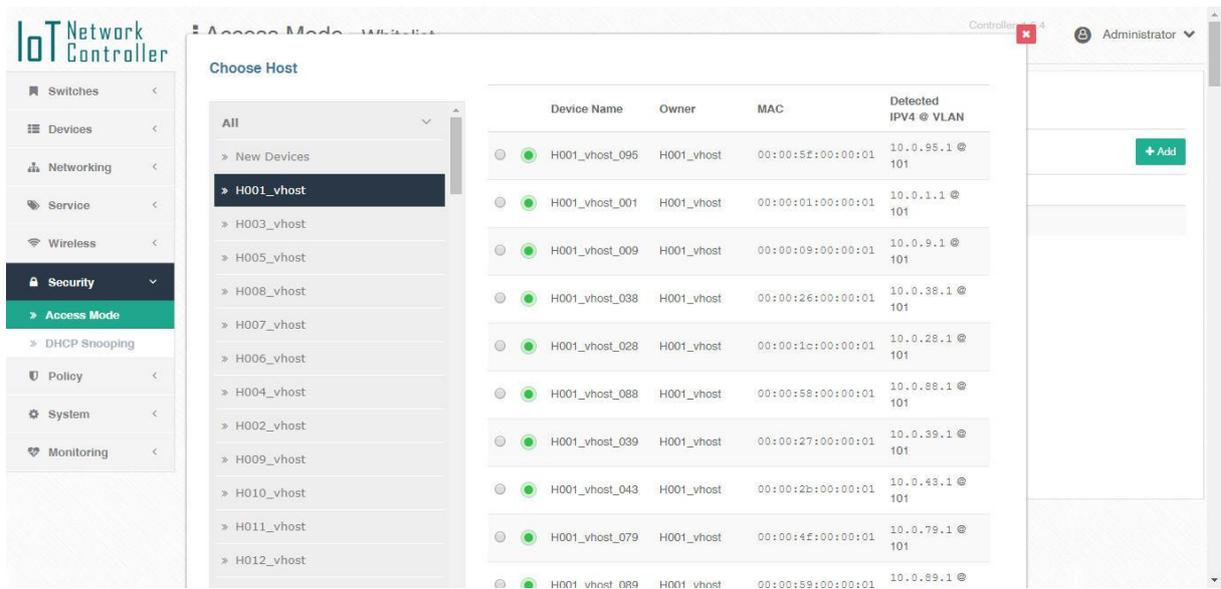
在黑名單功能開啟時，被加入黑名單的設備將會被拒絕上線



標籤名稱	標籤說明
配置頁面	
	新設備加入黑名單
	設備的 Mac 位址
	設備的名稱
	設備所受限制的 VLAN

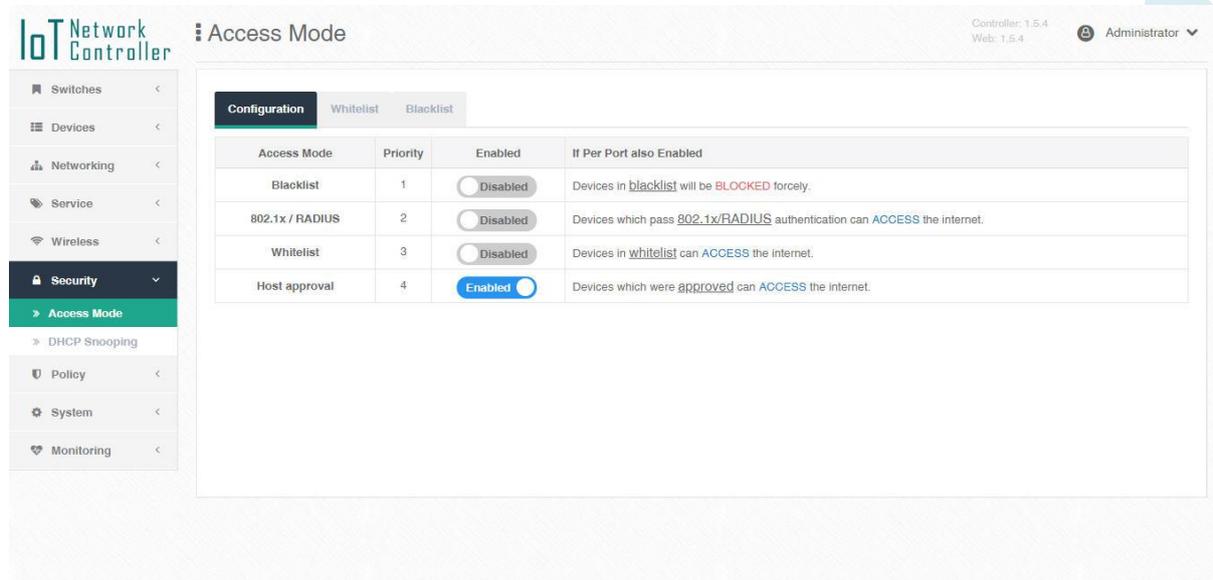
點選 Add，增加黑名單列表(由 Device 頁面將單一設備加入黑名單，也會同步出現在此黑名單列表中)



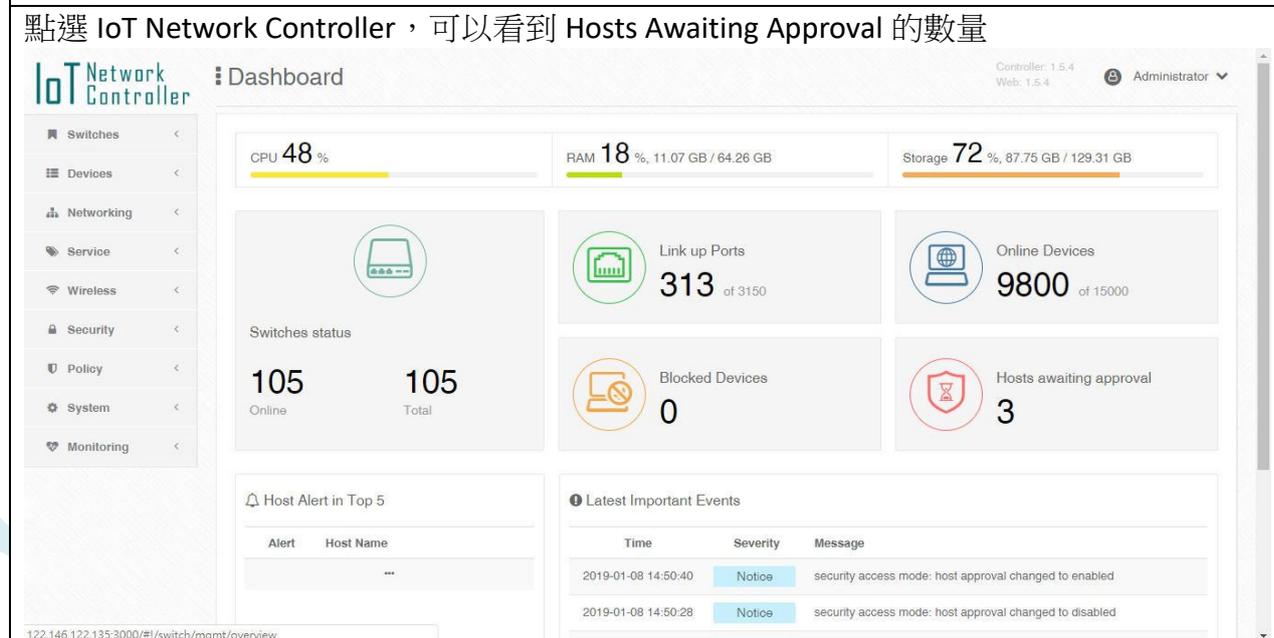
<p>標籤名稱</p>	<p>標籤說明</p>
<p>配置頁面</p>	
<p>Select Host ▾</p>	<p>下拉選單選擇要加入黑名單的設備(已被系統紀錄下來的)，如下圖</p>
	
<p>Mac</p>	<p>輸入已知的 Mac 位址加入黑名單</p>
<p>Submit</p>	<p>點選確定加入黑名單</p>

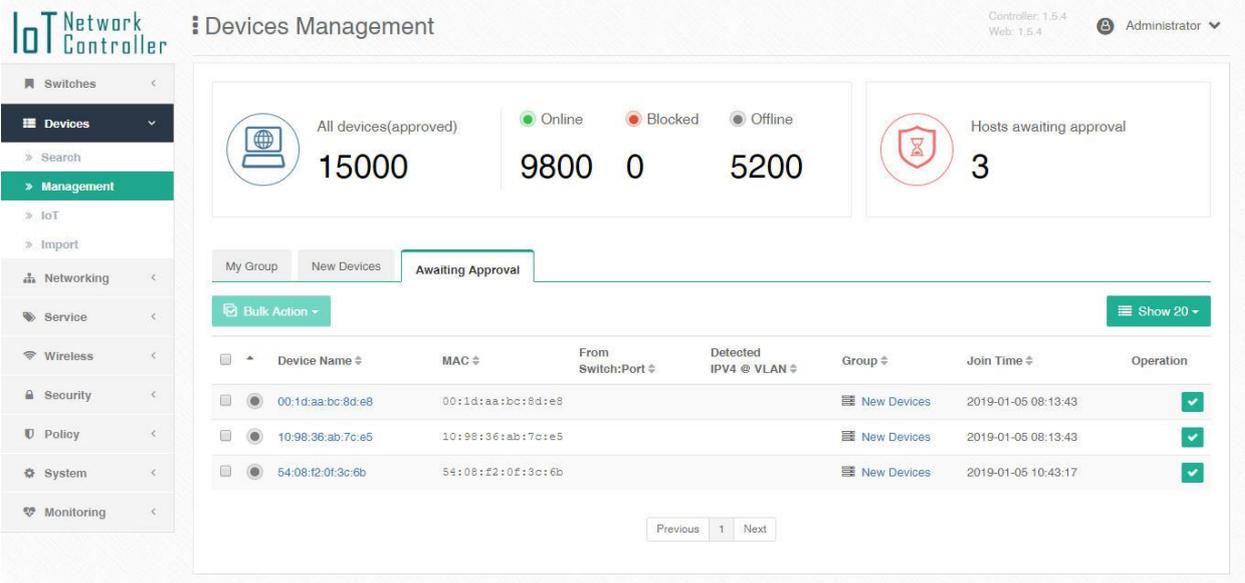
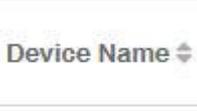
8.4. 准入管理

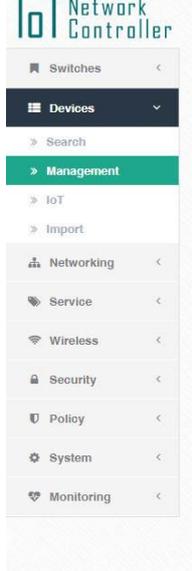
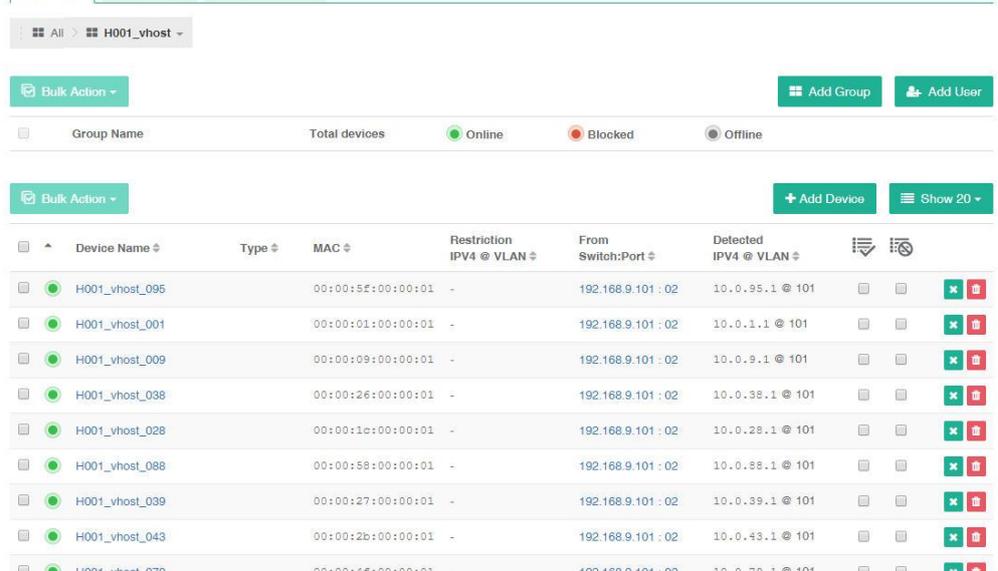
當 Host Approval 開啟時，所有設備將會在 Hosts Awaiting Approval 等待允許上線，當設備被允許上線了，才會出現在 My Group 跟 New Device



標籤名稱	標籤說明
顯示頁面	點選 IoT Network Controller，可以看到 Hosts Awaiting Approval 的數量
	目前有多少設備處於 Hosts Awaiting Approval

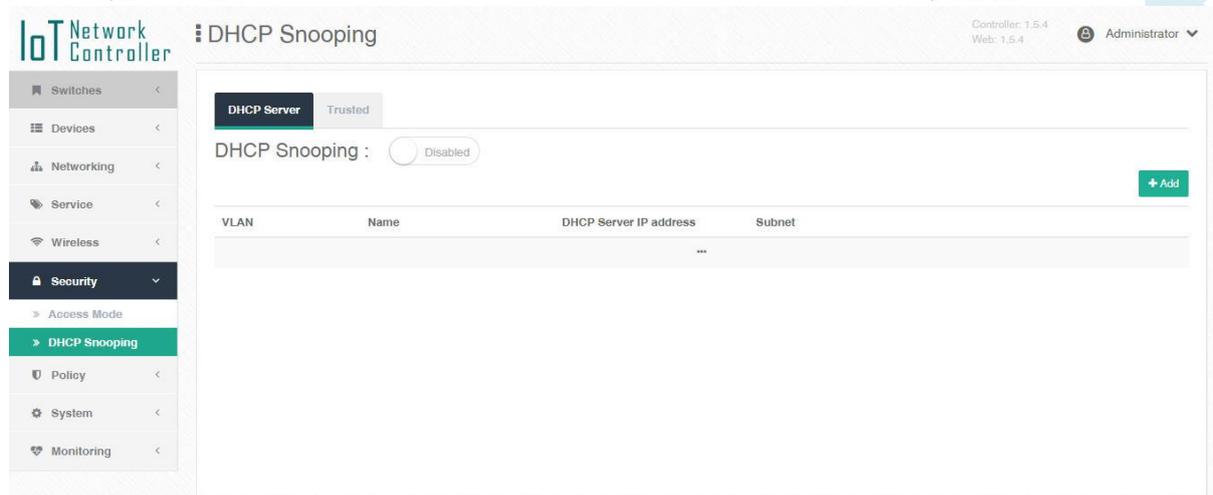


配置頁面	
<p>點選 Device > Management > Awaiting Approval，可以觀看處於等待允許上線的設備</p> 	
	目前有多少設備處於 Hosts Awaiting Approval
	在此頁面中，展示 10, 20, 50, 100 個群組設備
	該設備名稱，可以點進去修改(預設名稱是 Mac 位址)  為上線，  為下線
	該設備的 Mac 位址
	此設備是透過哪一台交換機的 Port 連線
	系統偵測到此設備的 IP 位址與 VLAN
	該設備的群組名稱
	此設備被記錄下進入到系統的時間

	<p>運作狀態</p> <p>: 點擊允許設備進入</p> <p>**允許進入的設備將會出現在 My Group 或 New Device 中**</p>																																																																																										
<p>在 My Group 或 New Device 中，可以讓設備回到 Hosts Awaiting Approval</p>																																																																																											
	 <table border="1"> <thead> <tr> <th>Device Name</th> <th>Type</th> <th>MAC</th> <th>Restriction IPV4 @ VLAN</th> <th>From Switch:Port</th> <th>Detected IPV4 @ VLAN</th> <th></th> <th></th> <th></th> </tr> </thead> <tbody> <tr> <td>H001_vhost_095</td> <td></td> <td>00:00:5f:00:00:01</td> <td>-</td> <td>192.168.9.101:02</td> <td>10.0.95.1 @ 101</td> <td></td> <td></td> <td></td> </tr> <tr> <td>H001_vhost_001</td> <td></td> <td>00:00:01:00:00:01</td> <td>-</td> <td>192.168.9.101:02</td> <td>10.0.1.1 @ 101</td> <td></td> <td></td> <td></td> </tr> <tr> <td>H001_vhost_009</td> <td></td> <td>00:00:09:00:00:01</td> <td>-</td> <td>192.168.9.101:02</td> <td>10.0.9.1 @ 101</td> <td></td> <td></td> <td></td> </tr> <tr> <td>H001_vhost_038</td> <td></td> <td>00:00:26:00:00:01</td> <td>-</td> <td>192.168.9.101:02</td> <td>10.0.38.1 @ 101</td> <td></td> <td></td> <td></td> </tr> <tr> <td>H001_vhost_028</td> <td></td> <td>00:00:1e:00:00:01</td> <td>-</td> <td>192.168.9.101:02</td> <td>10.0.28.1 @ 101</td> <td></td> <td></td> <td></td> </tr> <tr> <td>H001_vhost_088</td> <td></td> <td>00:00:58:00:00:01</td> <td>-</td> <td>192.168.9.101:02</td> <td>10.0.88.1 @ 101</td> <td></td> <td></td> <td></td> </tr> <tr> <td>H001_vhost_039</td> <td></td> <td>00:00:27:00:00:01</td> <td>-</td> <td>192.168.9.101:02</td> <td>10.0.39.1 @ 101</td> <td></td> <td></td> <td></td> </tr> <tr> <td>H001_vhost_043</td> <td></td> <td>00:00:2b:00:00:01</td> <td>-</td> <td>192.168.9.101:02</td> <td>10.0.43.1 @ 101</td> <td></td> <td></td> <td></td> </tr> <tr> <td>H001_vhost_079</td> <td></td> <td>00:00:4f:00:00:01</td> <td>-</td> <td>192.168.9.101:02</td> <td>10.0.79.1 @ 101</td> <td></td> <td></td> <td></td> </tr> </tbody> </table>	Device Name	Type	MAC	Restriction IPV4 @ VLAN	From Switch:Port	Detected IPV4 @ VLAN				H001_vhost_095		00:00:5f:00:00:01	-	192.168.9.101:02	10.0.95.1 @ 101				H001_vhost_001		00:00:01:00:00:01	-	192.168.9.101:02	10.0.1.1 @ 101				H001_vhost_009		00:00:09:00:00:01	-	192.168.9.101:02	10.0.9.1 @ 101				H001_vhost_038		00:00:26:00:00:01	-	192.168.9.101:02	10.0.38.1 @ 101				H001_vhost_028		00:00:1e:00:00:01	-	192.168.9.101:02	10.0.28.1 @ 101				H001_vhost_088		00:00:58:00:00:01	-	192.168.9.101:02	10.0.88.1 @ 101				H001_vhost_039		00:00:27:00:00:01	-	192.168.9.101:02	10.0.39.1 @ 101				H001_vhost_043		00:00:2b:00:00:01	-	192.168.9.101:02	10.0.43.1 @ 101				H001_vhost_079		00:00:4f:00:00:01	-	192.168.9.101:02	10.0.79.1 @ 101			
Device Name	Type	MAC	Restriction IPV4 @ VLAN	From Switch:Port	Detected IPV4 @ VLAN																																																																																						
H001_vhost_095		00:00:5f:00:00:01	-	192.168.9.101:02	10.0.95.1 @ 101																																																																																						
H001_vhost_001		00:00:01:00:00:01	-	192.168.9.101:02	10.0.1.1 @ 101																																																																																						
H001_vhost_009		00:00:09:00:00:01	-	192.168.9.101:02	10.0.9.1 @ 101																																																																																						
H001_vhost_038		00:00:26:00:00:01	-	192.168.9.101:02	10.0.38.1 @ 101																																																																																						
H001_vhost_028		00:00:1e:00:00:01	-	192.168.9.101:02	10.0.28.1 @ 101																																																																																						
H001_vhost_088		00:00:58:00:00:01	-	192.168.9.101:02	10.0.88.1 @ 101																																																																																						
H001_vhost_039		00:00:27:00:00:01	-	192.168.9.101:02	10.0.39.1 @ 101																																																																																						
H001_vhost_043		00:00:2b:00:00:01	-	192.168.9.101:02	10.0.43.1 @ 101																																																																																						
H001_vhost_079		00:00:4f:00:00:01	-	192.168.9.101:02	10.0.79.1 @ 101																																																																																						
	<p>點擊後讓該設備回到 Awaiting Approval 狀態</p>																																																																																										
	<p>點擊將設備從群組中刪除</p>																																																																																										

8.5. DHCP Snooping

DHCP Snooping 開啟後，從本系統建立的 DHCP Server 將會自動加入 Trusted 列表中，如果以其他設備當作 DHCP Server，請點擊 Add 將其加入，否則將會被阻擋掉



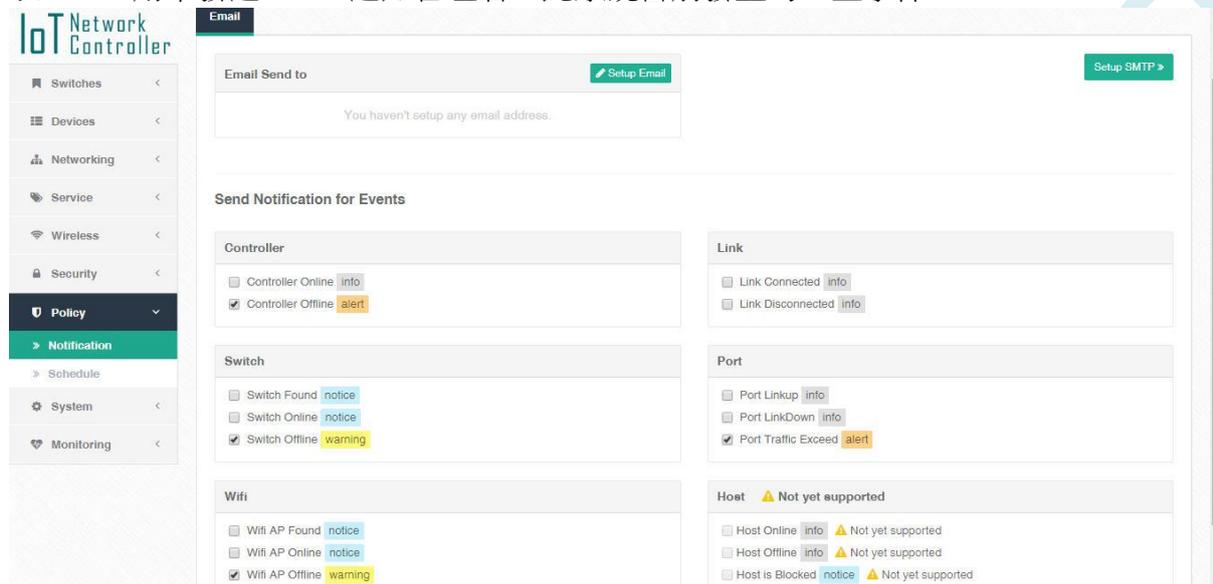
標籤名稱	標籤說明
配置頁面	
	將未知的 DHCP Server 加入，已獲取系統信任 **建議: 同一 Subnet 底下使用一個 DHCP Server 就好**
DHCP Snooping : 	點擊開啟 DHCP Snooping
	DHCP Server 所使用的 VLAN
	DHCP Server 的名稱
	DHCP Server 的 IP 位址
	DHCP Server 所使用的子網域
	加入可信任 DHCP Server，如下圖

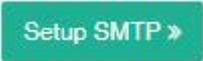
<h3>DHCP Server</h3> <p>Subnet Name*</p> <input type="text" value="My DHCP Server"/> VLAN* - Subnet VLAN <input type="text" value="VLAN"/> Subnet* <input type="text" value="192.168.1.0/24"/> DHCP Server IP Address* <input type="text" value="192.168.1.1"/> <p><i>* is Required</i></p> <p><input type="button" value="Submit"/> <input type="button" value="Cancel"/></p>	
<input type="button" value="Trusted"/>	系統信任的 DHCP Server 列表(從本系統建立的 DHCP Server 會自動加入)

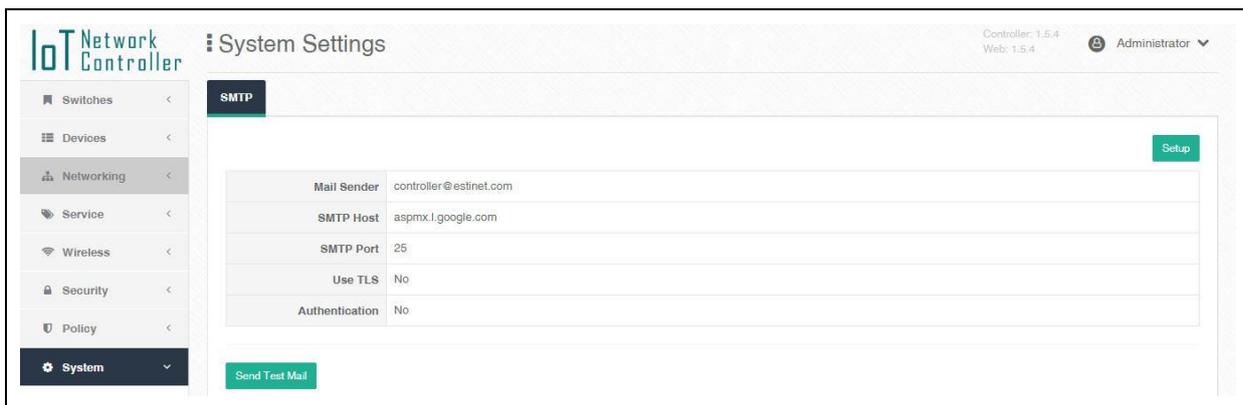
9. Policy

9.1. 通知警告

以 SMTP 用來發送 email 通知管理者，此系統目前發生的一些事件

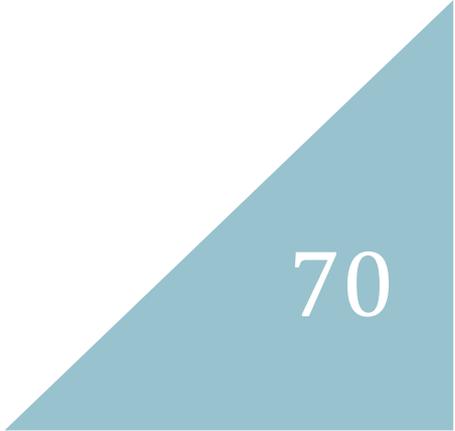


標籤名稱	標籤說明
Email 及通知事件配置頁面	
	點擊 Setup Email 設定 Email 信箱，如果要設定多組的 email，請用 space(空白鍵)、commas(逗號)、enter(輸入鍵)作區隔
space(空白鍵)	111@estient.com 222@estinet.com
commas(逗號)	111@estient.com,222@estinet.com
enter(輸入鍵)	111@estient.com 222@estinet.com
	點擊切換至 System > Setting 中，設定 SMTP，如下圖



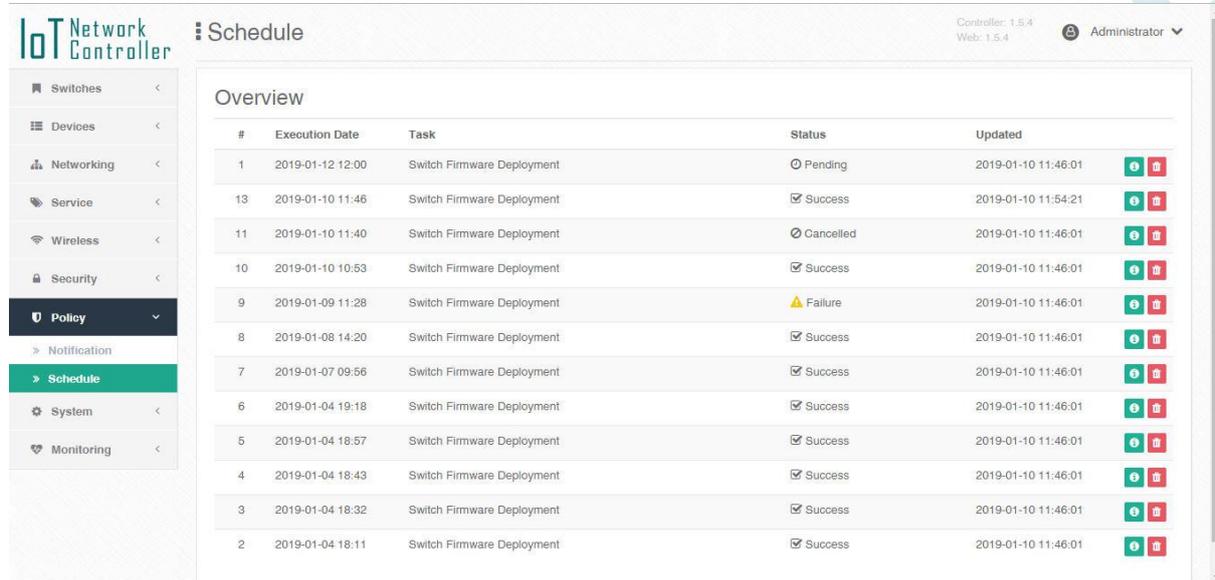
<p>Controller</p>	<p>可以勾選 Controller Online 的資訊、Controller Offline 的警告，當事件發生時，會發送至使用者的 Email</p>
<p>Link</p>	<p>可以勾選 Link Connected、Link Disconnected 的資訊，當事件發生時，會發送至使用者的 Email</p>
<p>Switch</p>	<p>可以勾選 Switch Found、Switch Online 的通知、Switch Offline 的警告，當事件發生時，會發送至使用者的 Email</p>
<p>Port</p>	<p>可以勾選 Port Linkup、Port Linkdown 的資訊、Port Traffic Exceed 的警告，當事件發生時，會發送至使用者的 Email</p>

EstiNet

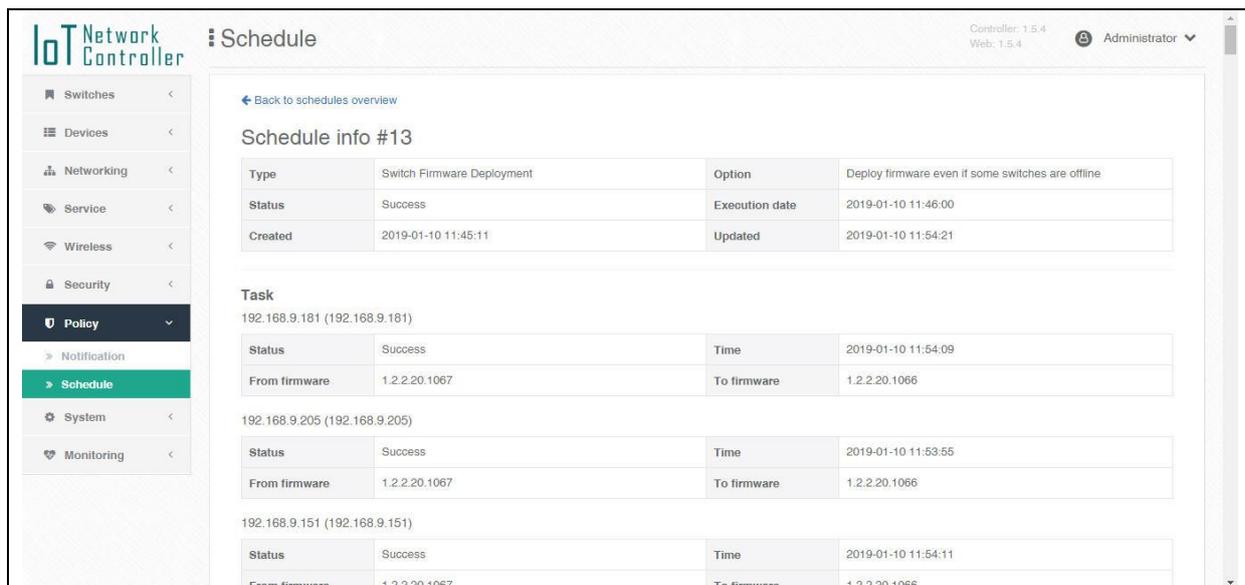


9.2. 系統議程表

主要是針對 System > firmware 的 firmware Deployment 規劃的流程表



標籤名稱	標籤說明
系統議程概觀展示頁面	
Execution Date	議程規劃的預計執行時間
Task	排程規劃的執行任務
Status	議程規劃的執行狀態 ⌚ Pending : 進行中 ✓ Success : 成功 ⌛ Cancelled : 取消 ⚠ Failure : 失敗
Updated	排程規劃的確切的更新時間
	點擊觀看該排程的細項，如下圖

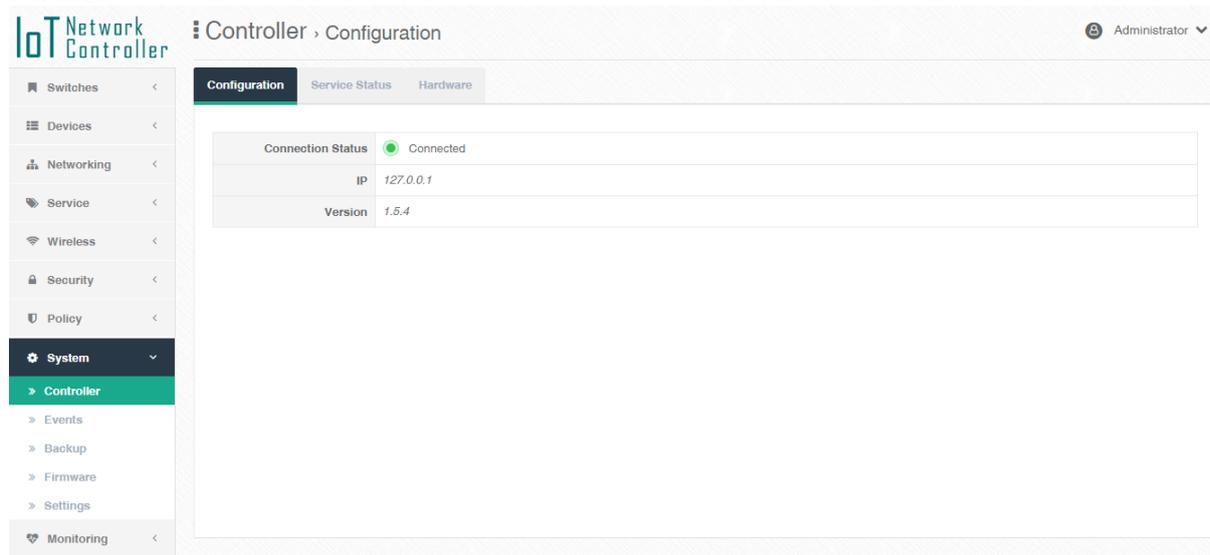


Type	Schedule 類別
Option	Schedule 說明
Status	Schedule 狀態
Execution date	Schedule 執行時間
Created	Schedule 新增的時間
Updated	Schedule 最後更新時間
Time	Task 執行時間
From firmware	原先的舊版本
To firmware	改動的新版本
	點擊刪除該排程規劃

10. System

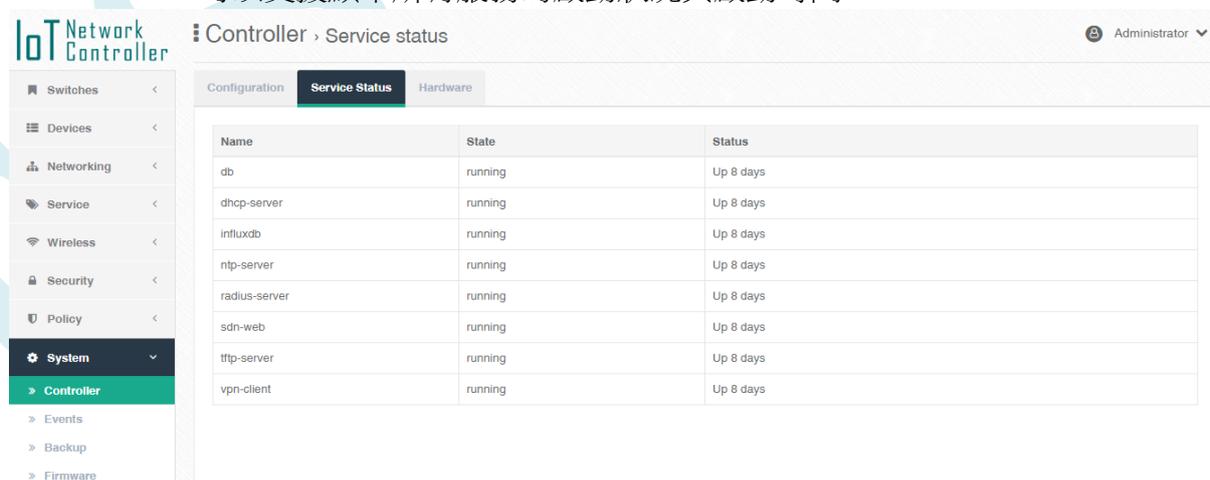
10.1. Controller

點選 System > Controller，確認 Controller 的 Configuration、執行服務狀態和硬體的情況與訊息



標籤名稱	標籤說明
Connection Status	Controller 目前是否正常連線
IP	Controller 目前的 IP
Version	Controller 目前版本

Service Status 可以支援顯示所有服務的啟動狀況與啟動時間



標籤名稱	標籤說明
Name	服務的名稱
State	服務目前運作的狀態
Status	服務已執行時間

在 Hardware 查看硬體的狀態

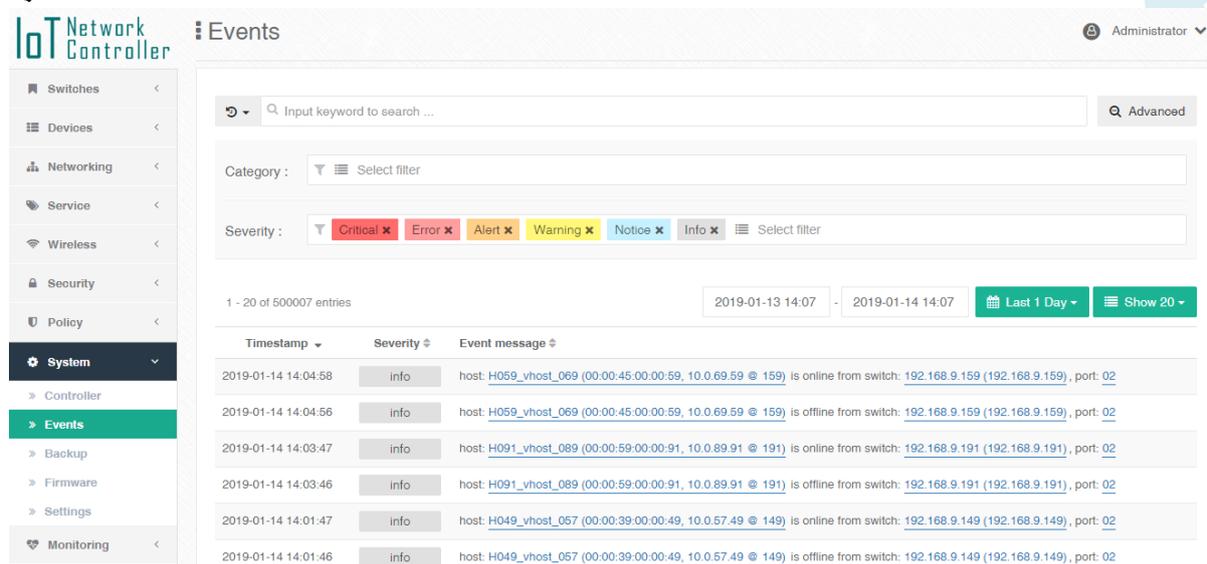
The screenshot shows the 'Controller > Hardware Information' page in the IoT Network Controller web interface. The left sidebar contains navigation options: Switches, Devices, Networking, Service, Wireless, Security, Policy, System (expanded), Controller (selected), Events, Backup, Firmware, Settings, and Monitoring. The main content area has three tabs: Configuration, Service Status, and Hardware (selected). The Hardware tab displays the following system information:

```

Machine: Type: Server System: Dell product: PowerEdge R230 v: N/A serial: Chassis:
         type: 23 serial:
         Mobo: Dell model: 0MFXTY v: A02 serial: BIOS: Dell v: 1.4.5 date: 08/09/2016
Memory: RAM: total: 62.76 GiB used: 12.97 GiB (20.7%)
         RAM Report: unknown-error: dmidecode was unable to generate data
CPU:     Topology: Quad Core model: Intel Xeon E3-1240 v5 bits: 64 type: MT MCP arch: Skylake-S
         rev: 3 L2 cache: 8192 KiB
         flags: lm nx pae sse sse2 sse3 sse4_1 sse4_2 ssse3 vmx bogomips: 56068
         Speed: 3750 MHz min/max: 800/3900 MHz Core speeds (MHz): 1: 3750 2: 3743 3: 3733
         4: 3723 5: 3771 6: 3727 7: 3738 8: 3734
Network: Message: No Device data found.
         IF-ID-1: br-nfv state: unknown speed: N/A duplex: N/A mac:
         IP v6: scope: link
         IF-ID-2: br-vintf state: up speed: 10 Mbps duplex: full mac:
         IP v6: scope: link
         IF-ID-3: dhcp_ext state: up speed: 10000 Mbps duplex: full mac:
         IF-ID-4: dhcp_int state: up speed: 10000 Mbps duplex: full mac:
         IF-ID-5: docker0 state: down mac:
         IP v4: scope: global
         IF-ID-6: em1 state: up speed: 1000 Mbps duplex: full mac:
         IP v4: scope: global
         IP v6: scope: link
         IF-ID-7: em1-vi state: up speed: 1000 Mbps duplex: full mac:
         IF-ID-8: em2 state: up speed: 1000 Mbps duplex: full mac:
         IP v4: scope: global
         IP v6: scope: link
         IF-ID-9: em2-vi state: up speed: 1000 Mbps duplex: full mac:
    
```

10.2. Events

點選 System >Event，確認系統是否出現異常、交換器、終端設備以及 Controller 上下線等 Event

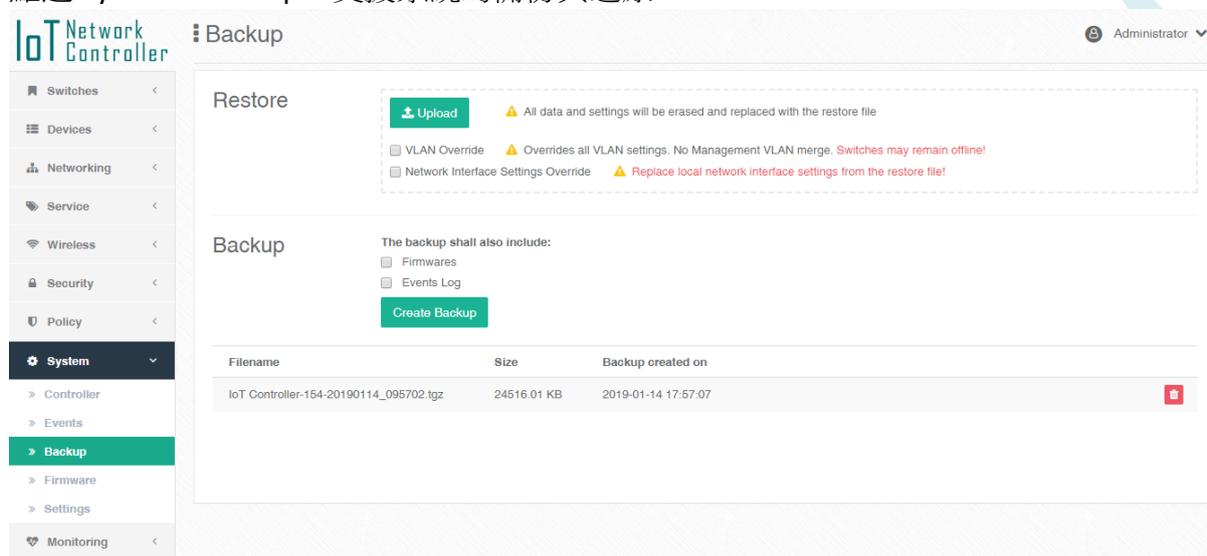


標籤名稱	標籤說明
	歷史查詢紀錄
<input type="text" value="Input keyword to search ..."/>	關鍵字搜尋 Events
<input type="button" value="Advanced"/>	開啟/關閉進階搜尋
Category : <input type="text" value="Select filter"/>	透過 Controller、Topology / Link、Switch、Port、Host 和 Traffic Alert 等來分類 Events
Severity : <input type="text" value="Select filter"/>	透過嚴重性與種類（Critical、Error、Alert、Warning、Notice 和 Info）來分類 Events
2019-01-13 14:07 - 2019-01-14 14:07	自訂時間搜尋 Events
<input type="button" value="Last 1 Day"/>	指定時間三十分鐘、一小時、兩個小時、一天、三天、一星期和無限制來搜尋 Events
<input type="button" value="Show 20"/>	每頁顯示 Events 的數量 10 個、20 個、50 個和 100 個

Timestamp ▼	Event 發生的時間
Severity ⇅	Event 的總類
Event message ⇅	Event 的 Message

10.3. Backup

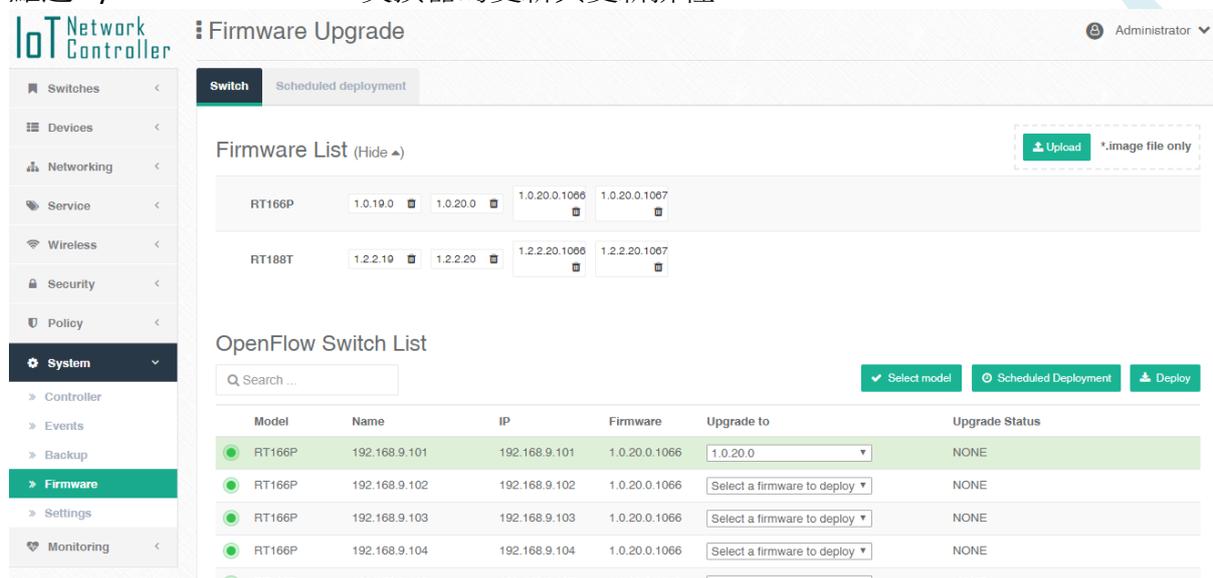
點選 System > Backup，支援系統的備份與還原



標籤名稱	標籤說明
	Upload 設定檔（設定檔來自 Backup）
<input type="checkbox"/> VLAN Override	Upload 是否覆蓋 VLAN 設定
<input type="checkbox"/> Network Interface Settings Override	Upload 是否覆蓋 Network Interface 設定
	產生 Backup 設定檔
<input type="checkbox"/> Firmwares	交換器韌體版本
<input type="checkbox"/> Events Log	是否連同 Events Log 一同備份
Filename	檔案名稱
Size	檔案大小
Backup created on	檔案產生時間
IoT Controller-154-20190114_095702.tgz	點選下載設定備份檔
	移除 Backup 設定檔

10.4. Firmware

點選 System > Firmware，交換器的更新與更新排程



標籤名稱	標籤說明
	上傳交換器的 Firmware
	刪除上傳的 Firmware
	選取交換器以及更新的版本
Model	交換器型號
Name	交換器名稱
IP	交換器 IP
Firmware	交換器版本
Upgrade to	選擇要更新的版本
Upgrade Status	目前更新狀態
	設定排程更新選定的設備韌體的時間
	立即更新選定的設備韌體

<p>Upgrade to</p> <p>1.0.20.0 ▼</p>	<p>選擇設備更新版本</p>
<p>Scheduled deployment</p>	<p>分頁連接至 Policy > Schedule</p>

Select model 指定機型與更新版本

Apply firmware version to selected model

Pick a model from the list below to select all switches of this kind, and which firmware to apply

RT188T ▼ 1.2.2.20.1067 ▼

Select only switches which are online

Submit
Cancel

標籤名稱	標籤說明
<p>RT188T ▼</p>	<p>選擇更新的機型</p>
<p>1.2.2.20.1067 ▼</p>	<p>選擇更新的版本編號</p>
<p><input type="checkbox"/> Select only switches which are online</p>	<p>是否只選擇上線的機器</p>
<p>Submit</p>	<p>確認設定</p>
<p>Cancel</p>	<p>取消設定</p>

Scheduled Deployment 設定交換器 Firmware 更新時間

Select a date to deploy firmware on

📅 Deploy firmware on

2019-01-14

^
12
v

^
00
v

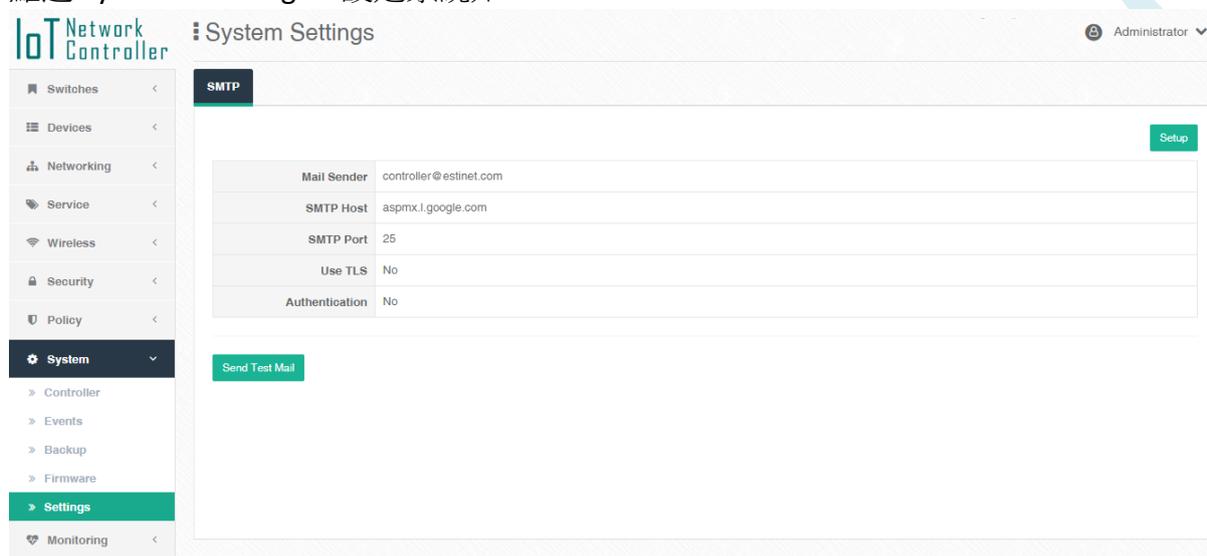
Stop firmware deployment if any switch is offline prior deployment execution

Submit
Cancel

標籤名稱	標籤說明
<div style="border: 1px solid #ccc; padding: 5px; display: flex; align-items: center;"> 📅 Deploy firmware on <div style="border: 1px solid #ccc; padding: 2px 10px;">2019-01-14</div> </div>	選擇更新的日期
^ <div style="border: 1px solid #ccc; padding: 2px 10px; display: inline-block;">12</div> : v	選擇更新的時間(時)
^ <div style="border: 1px solid #ccc; padding: 2px 10px; display: inline-block;">00</div> v	選擇更新的時間(分)
<input type="checkbox"/> Stop firmware deployment if	排程更新時如有未上線的機器是否停止排程更新
Submit	確認設定
Cancel	取消設定

10.5. Settings

點選 System > Settings，設定系統如 SMTP



標籤名稱	標籤說明
Setup	設定 SMTP 連線設定
Mail Sender	送件者
SMTP Host	SMTP Server
SMTP Port	SMTP Port
Use TLS	是否使用 TLS 加密
Authentication	是否啟用認證機制
Username	使用者帳號
Send Test Mail	發送測試郵件確認功能是否正常

Setup 在開啟後可以設定 SMTP 相關設定

Edit SMTP Setting

Mail Sender

SMTP Host

SMTP Port

Secure (TLS)
 use TLS?

Authentication
 Require Authentication?

Username

Password

標籤名稱	標籤說明
Mail Sender <input type="text" value="controller@estinet.com"/>	設定郵件寄件者位置
SMTP Host <input type="text" value="aspmx.l.google.com"/>	設定郵寄伺服器位置
SMTP Port <input type="text" value="25"/>	設定郵寄伺服器使用的 Port
Secure (TLS) <input type="checkbox"/> use TLS?	是否使用 TLS 加密
Authentication <input checked="" type="checkbox"/> Require Authentication?	是否進行帳號認證
Username <input type="text" value="admin"/>	輸入帳號

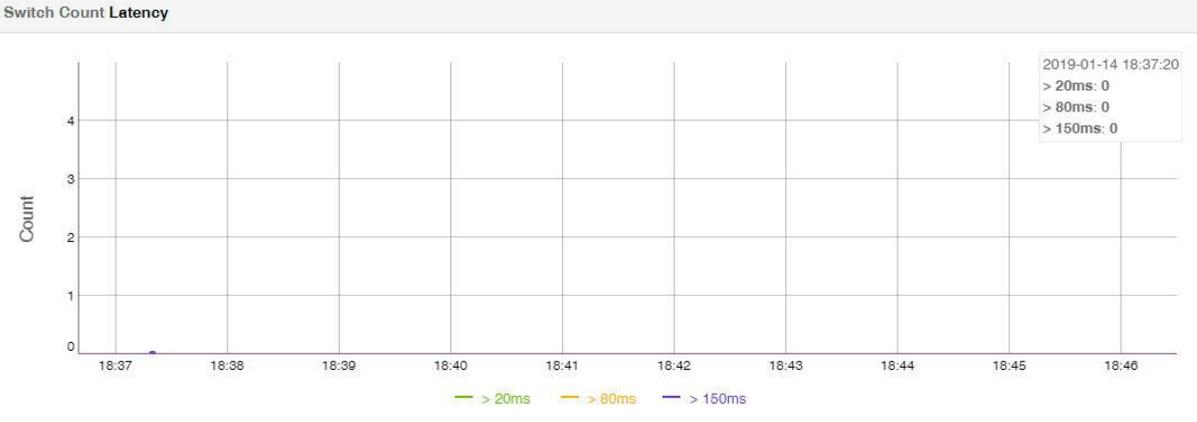
Password <input type="password" value="....."/>	輸入密碼
<input type="button" value="Submit"/>	確認設定
<input type="button" value="Cancel"/>	取消設定

11. Monitoring

11.1. 系統概況

此頁面是用來觀看 Latency(系統延遲)跟 Packet Loss(封包遺失)的狀況

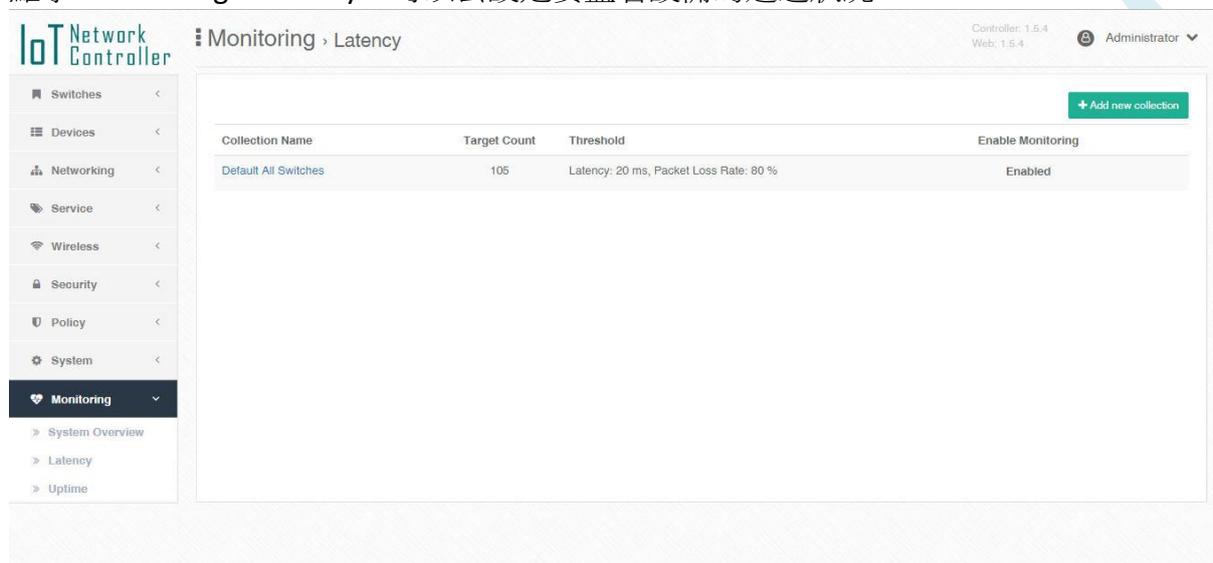


標籤名稱	標籤說明
Latency(系統延遲)	
	
<div style="border: 1px solid gray; padding: 5px; width: fit-content; margin: 0 auto;"> <p>Latency</p> </div>	<p>系統的延遲時間</p> <ul style="list-style-type: none"> — > 20ms : 顯示大於 20 毫秒 — > 80ms : 顯示大於 80 毫秒 — > 150ms : 顯示大於 150 毫秒 <div style="border: 1px solid gray; padding: 5px; width: fit-content; margin-top: 10px;"> <p>2019-01-14 17:22:00</p> <p>> 20ms: 0</p> <p>> 80ms: 0</p> <p>> 150ms: 0</p> </div> <p style="text-align: right;">: 顯示三種延遲的數量</p>



11.2. Latency

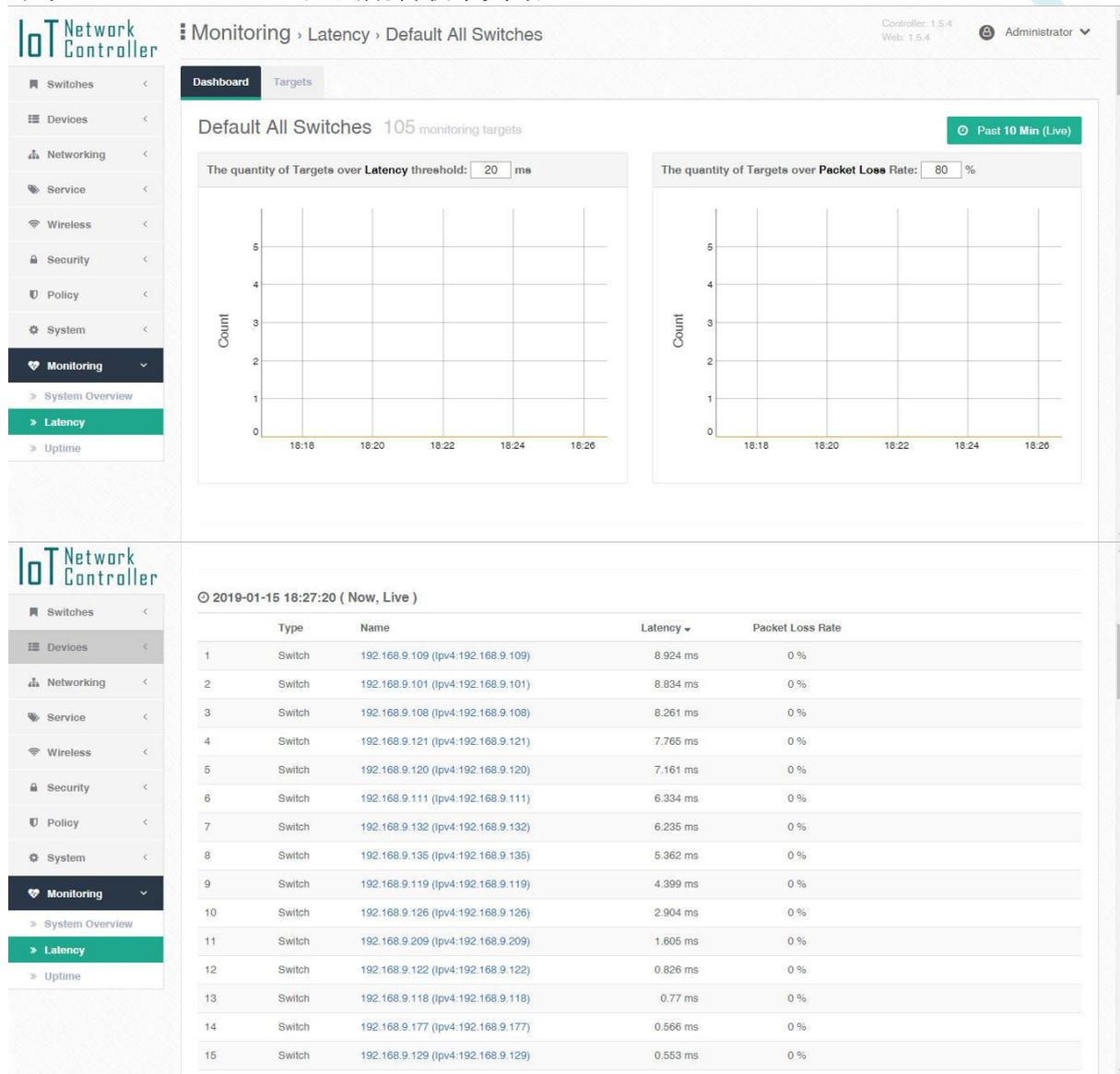
點擊 Monitoring > Latency，可以去設定要監看設備的延遲狀況



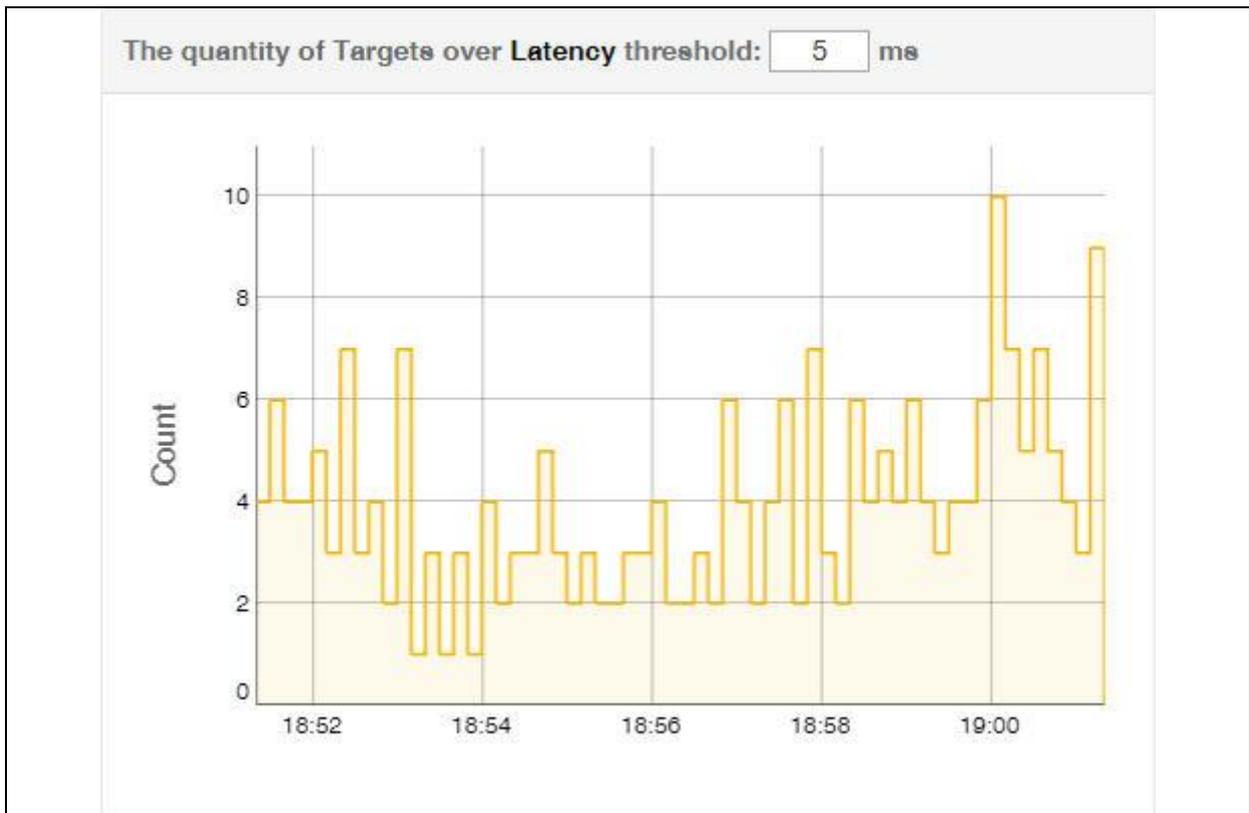
標籤名稱	標籤說明
顯示頁面	
	新增一個監看群組
<u>Collection Name</u>	監看設備的群組名稱
<u>Target Count</u>	監看設備的數量
<u>Threshold</u>	監看的門檻
<u>Enable Monitoring</u>	開啟/關閉監看

11.2.1. Dashboard

點擊 Collection Name，進去觀看收集資訊

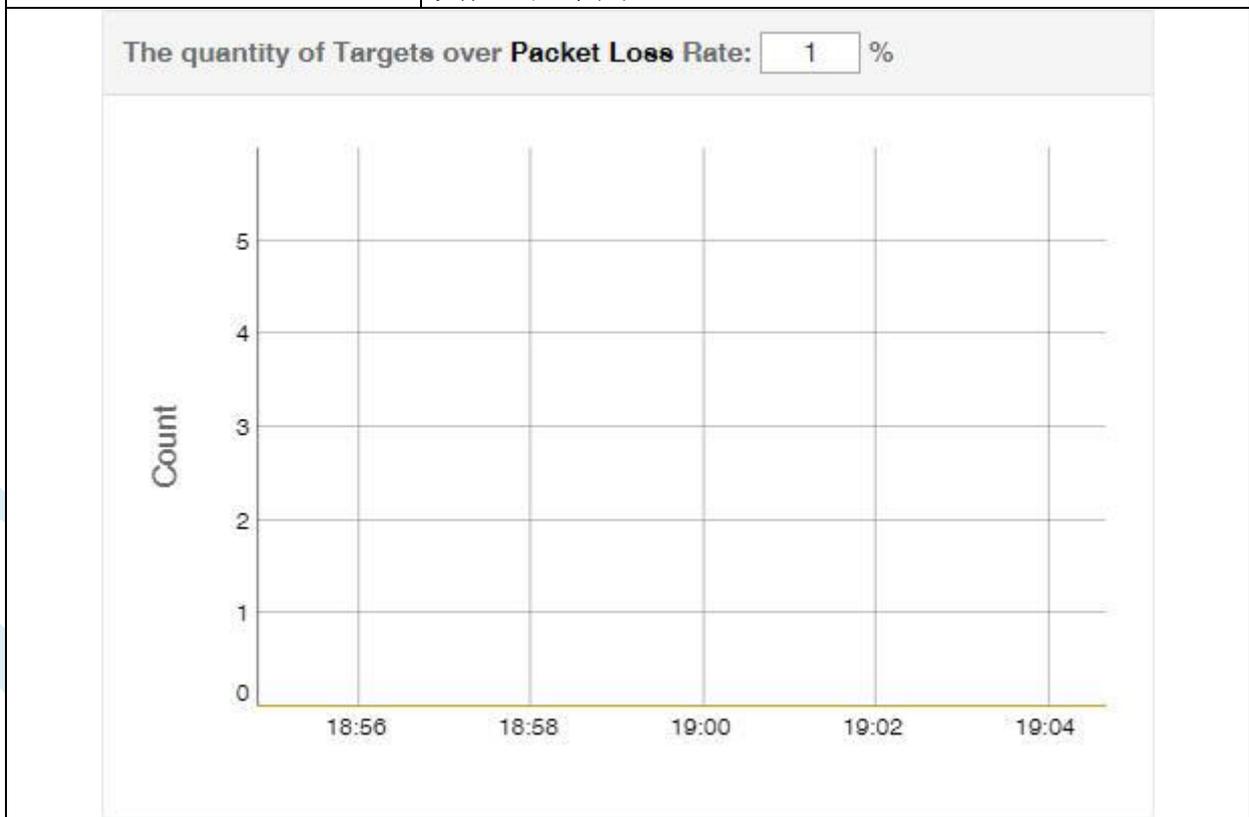


標籤名稱	標籤說明
顯示頁面	
Latency	目標的延遲量超過門檻會顯示，門檻可在 <input type="text" value="20"/> ms 設定其值，如下圖



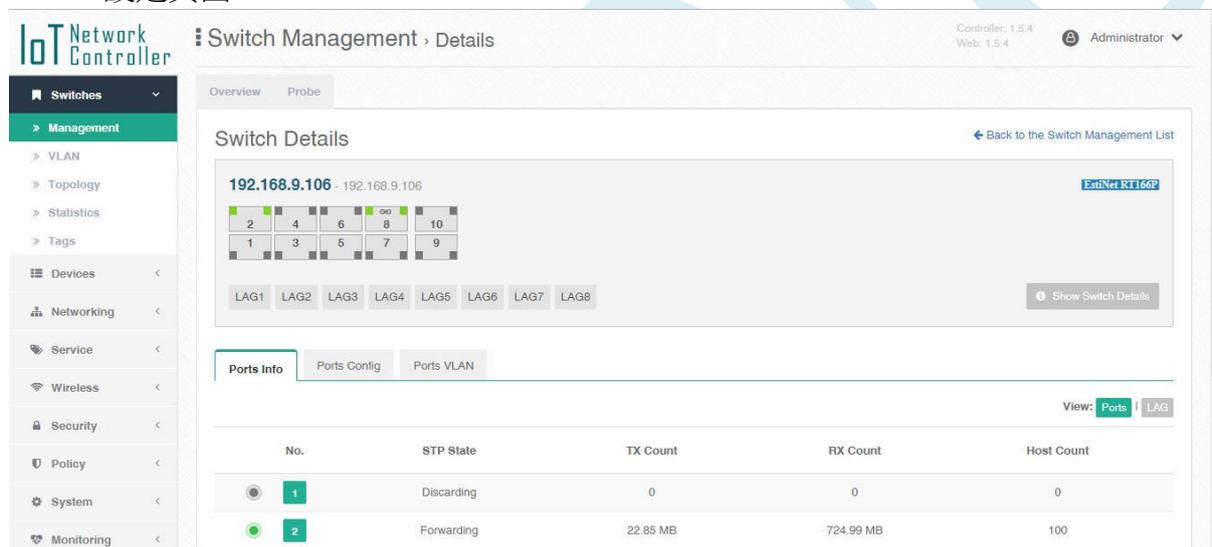
Packet Loss

目標的封包遺失率超過門檻會顯示，可在 % 設定其值，如下圖



 Past 10 Min (Live)	選擇顯示過去多少時間，如: 10 分鐘、30 分鐘、2 小時、6 小時、12 小時、1 天、2 天等
Type	監看設備類型
Name	監看的設備名稱，點擊可切換至 Switch 或 Device 設定頁面
Latency	延遲多少毫秒
Packet Loss Rate	封包遺失率

Switch 設定頁面



Switch Management · Details

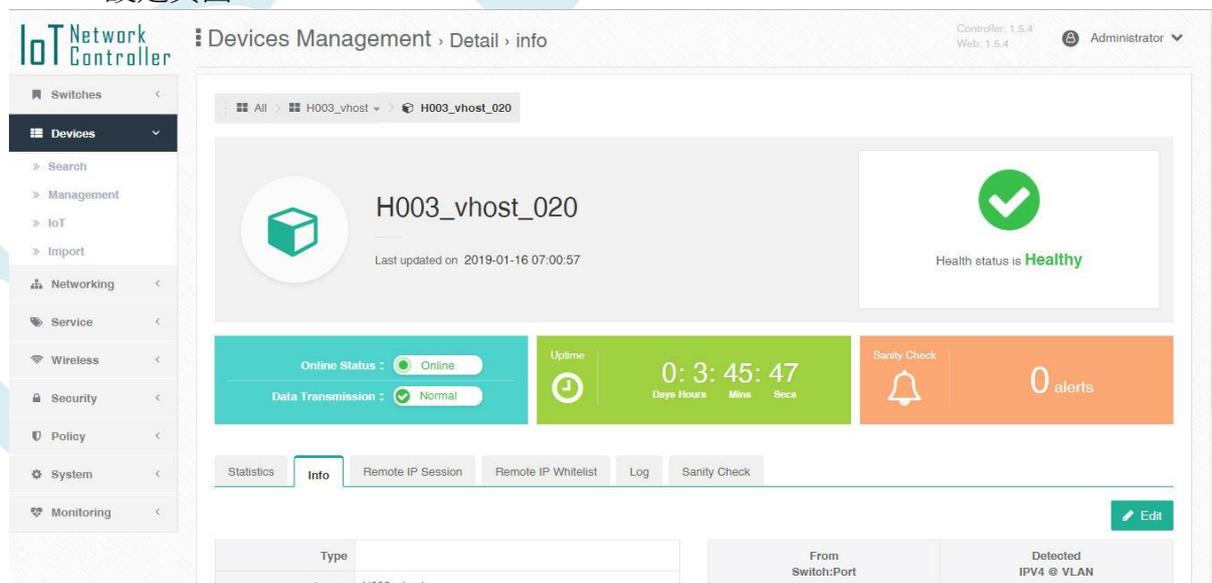
Controller: 1.5.4 Web: 1.5.4 Administrator

Switch Details

192.168.9.106 - 192.168.9.106

No.	STP State	TX Count	RX Count	Host Count
1	Discarding	0	0	0
2	Forwarding	22.85 MB	724.99 MB	100

Device 設定頁面



Devices Management · Detail · info

Controller: 1.5.4 Web: 1.5.4 Administrator

H003_vhost_020

Health status is **Healthy**

Online Status: Online Uptime: 0:3:45:47

Data Transmission: Normal 0 alerts

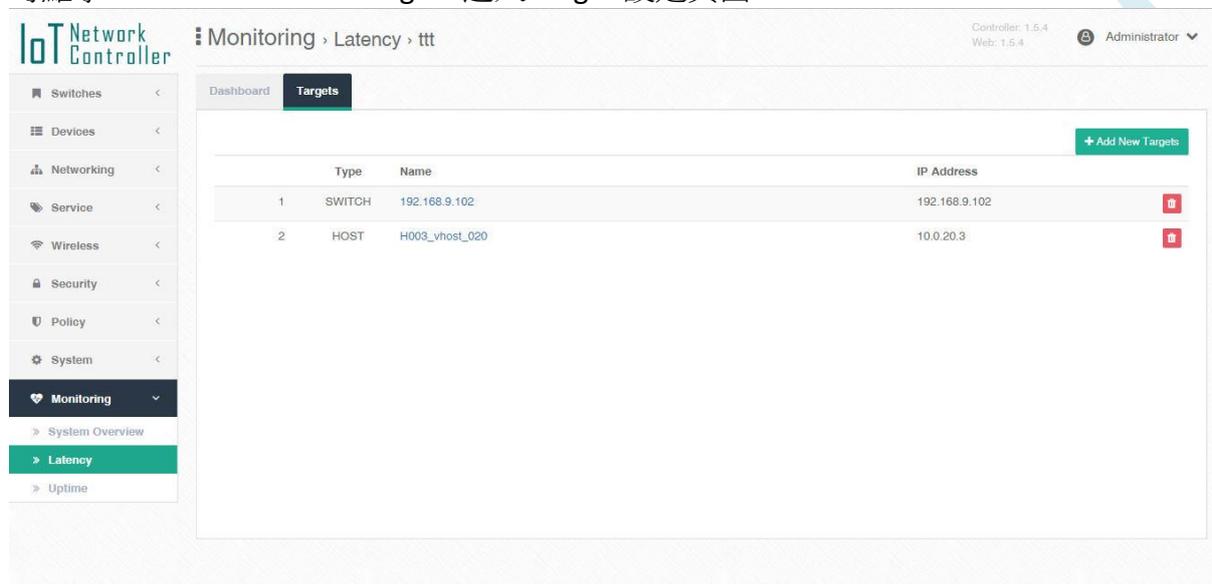
Statistics Info Remote IP Session Remote IP Whitelist Log Sanity Check

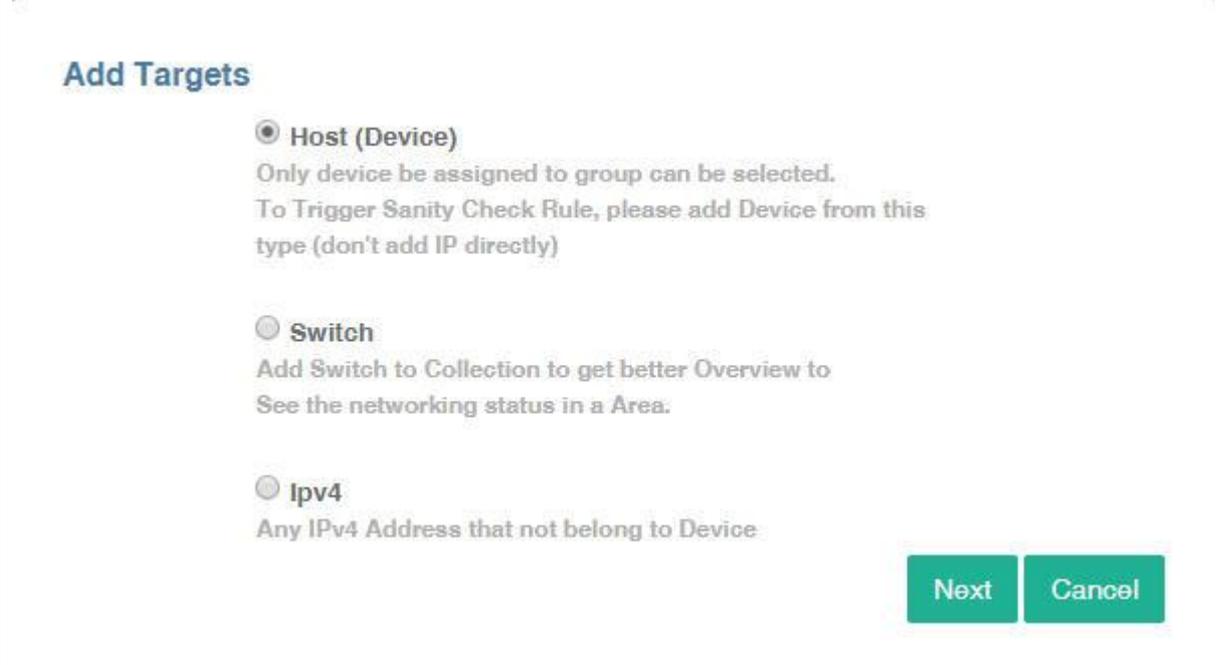
Owner: H003_vhost

From Switch:Port Detected IPV4 @ VLAN

11.2.2. Target

可點擊 Collection Name > Targets 進入 Target 設定頁面

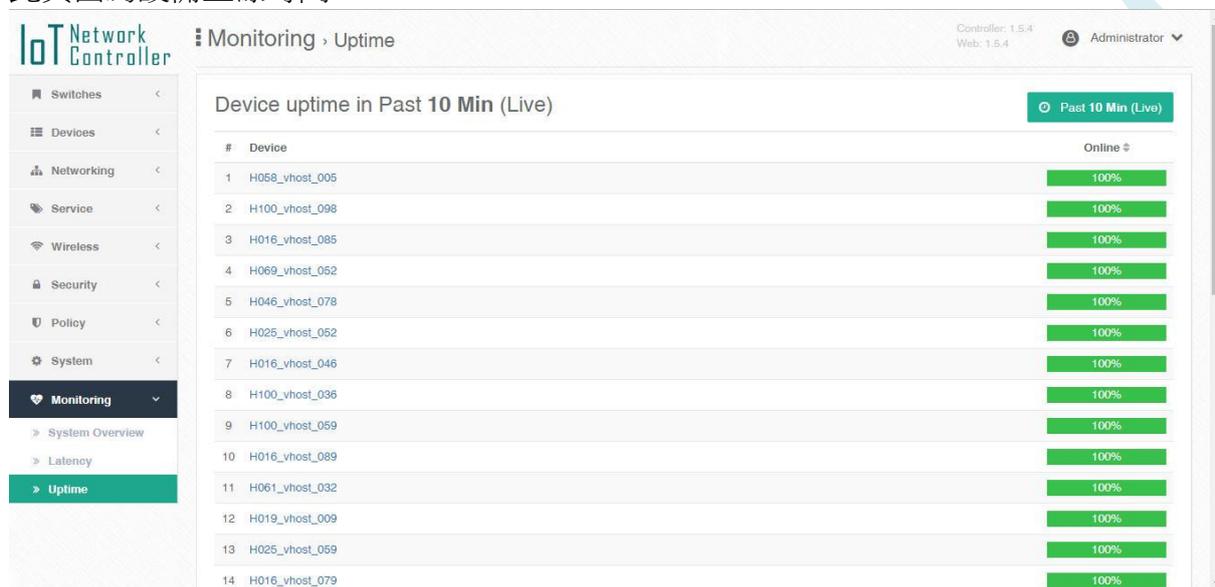


標籤名稱	標籤說明
顯示頁面	
	點擊新增監看目標，如下圖
	
	監看設備的類型

Name	監看設備的名稱
IP Address	監看的 IP 位址
	刪除監看設備

11.3. Uptime

此頁面為設備上線時間



標籤名稱	標籤說明
顯示頁面	
	選擇顯示過去多少時間，如: 10 分鐘、30 分鐘、2 小時、6 小時、12 小時、1 天、2 天等
	監看設備的編號
	監看設備的名稱
	監看目標的上線的健康程度

12. 注意事項

1. 當交換器正在更新時，請勿將電源拔除
2. DHCP Snooping 不支援 DHCP server relay
3. VLAN 的 Trunk 模式下若無設定 VLAN TAG 則會被判定為 Access 模式
4. 預設 Data Plane 為 VLAN 100，Control Plane 為 VLAN 1
5. 控制器預設 RT188T 交換器的前 1-20 Port 為 Data Plane(VLAN 100)，21-28 為 Control Plane(VLAN 1)
6. 控制器預設 RT166P 交換器的前 1-6 Port 為 Data Plane(VLAN 100)，7-10 為 Control Plane(VLAN 1)
7. 如要連線到交換器需將網路線接至 Control Plane 上
8. 控制器若無接收到 Device 的 ARP 封包，將無法顯示 Device 在控制器網頁上
9. QoS 的 Rate limit 需要設定 subnet 的功能才能使用
10. Statistics 流量統計為每分鐘一次，所以圖像僅顯示平均速度
11. Statistics 流量只保留三天
12. Security 802.1x/RADIUS 不支援 Windows 7 與之後的版本
13. Legacy 交換器在 Topology 上，必須手動建置