# CERIO Corporation

# CenOS 5.0 韌體

## 無線基地台操作使用手冊

# FCC Warning

This device has been tested and found to comply with limits for a Class A digital device, pursuant to Part 2 and 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiates radio frequency energy and, if not installed and used in accordance with the user's manual, may cause interference in which case user will be required to correct the interference at his own expense.

# CE Mark Warning

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user many be required to take adequate measures.

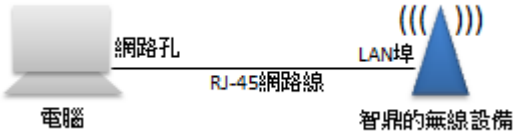
# 內容

# 1. 產品登入設定

## 1.1 網路設定

智鼎的 CenOS5.0 無線基地台設備採用網頁管理方式，當架構建置完成，可以透過瀏覽器輸入 192.168.2.254(預設 IP 位置)進入管理，當進入頁面後輸入正確的帳號密碼即可管理設備功能，接下來請依照以下步驟繼續設定您的電腦以便可以讓您的電腦與 CenOS5.0 軟體互相連接。

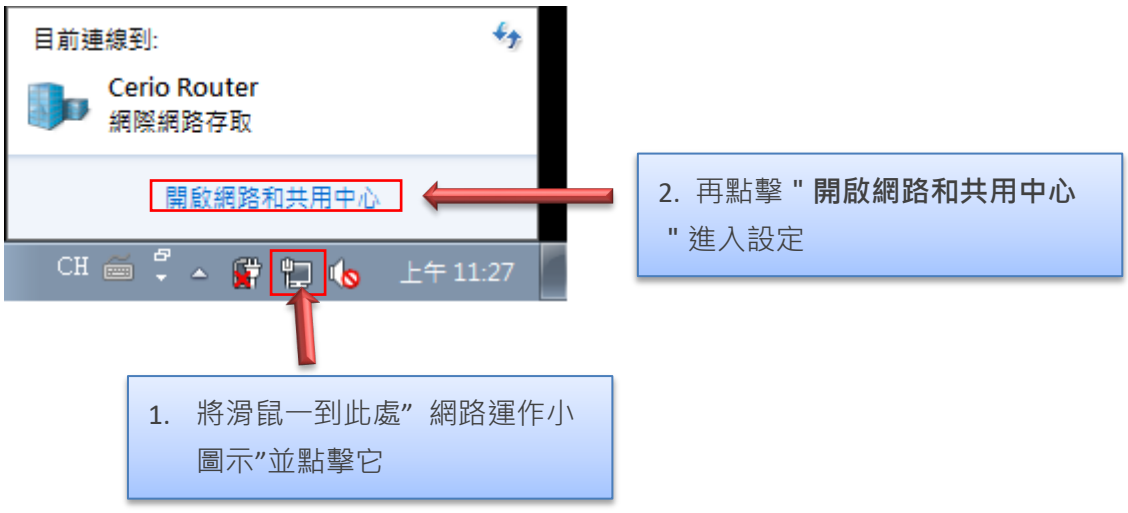
| Notice | 若選購無線路由設備，請使用網路線去連接設備的 LAN 埠與 PC 的網路孔，並直接參考 1.2 項目的登入無線基地台的 WEB 管理頁面 |
|---|---|




### Windows 7 作業系統為例

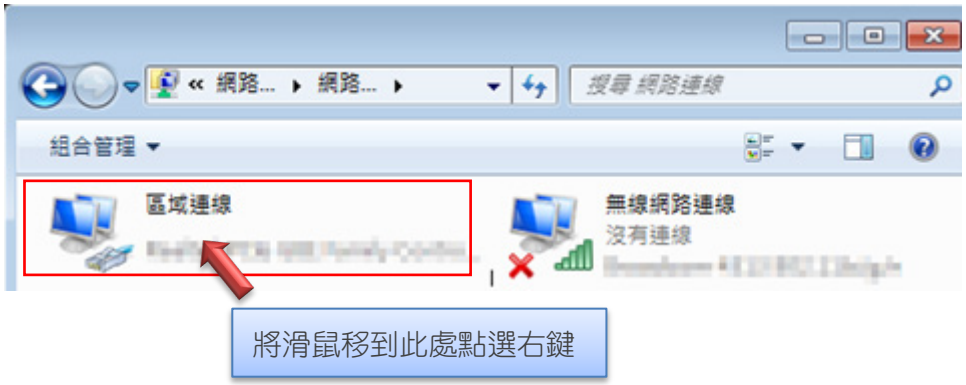
為了進入 Cerio CenOS 軟體的管理頁面，則電腦 IP 網段必須與 Cerio CenOS 軟體的網段相同，才有辦法透過瀏覽器登入管理頁面進行設定。而手動設定 IP 時您必須先至使用者電腦中變更 TCP/IP 協定，但請注意 PC / NOTEBOOK 的 IP 位址千萬不可與 Cerio CenOS 軟體的本機區域網路中的網路設備或 PC / NOTEBOOK 使用相同的 IP 位址，以免發生 IP 位址衝突的狀況。以下步驟將協助您完成登入 Cerio CenOS 軟體的設定頁面。

**步驟 1：** 請點擊螢幕右下方的網路運作小圖示，如下圖，再點擊 " **開啟網路和共用中心** " ，進入設定頁面

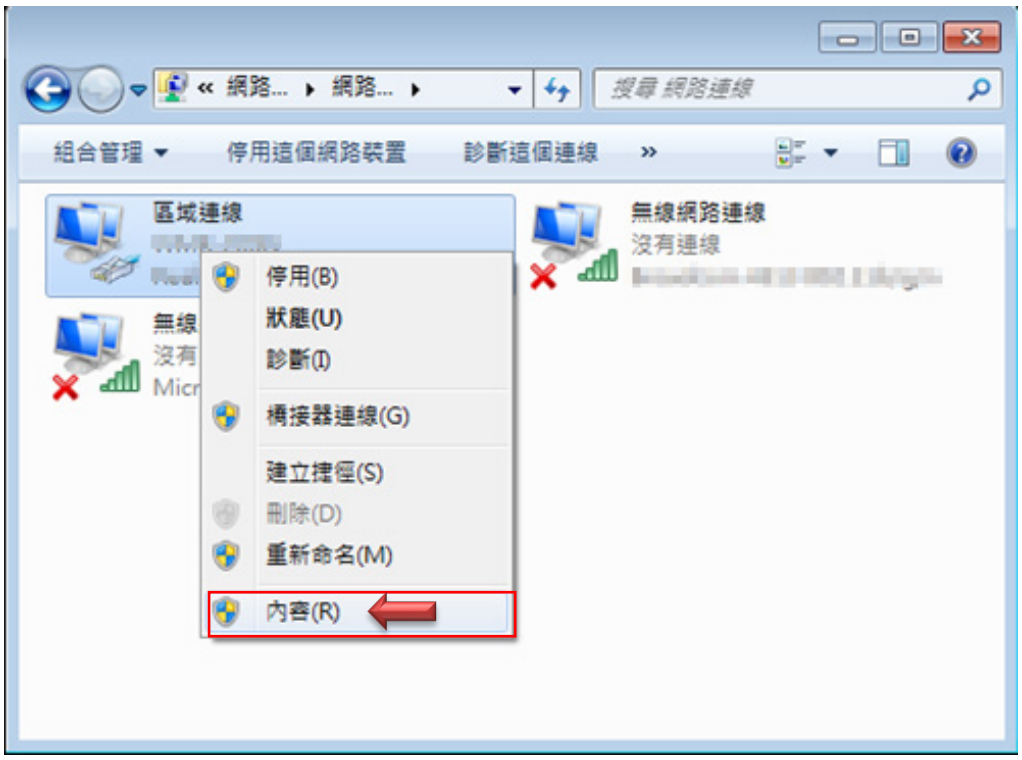


**步驟 2：** 當進入網路共用中心後，在左邊目錄部分找出＂**變更介面卡設定**＂點擊進入

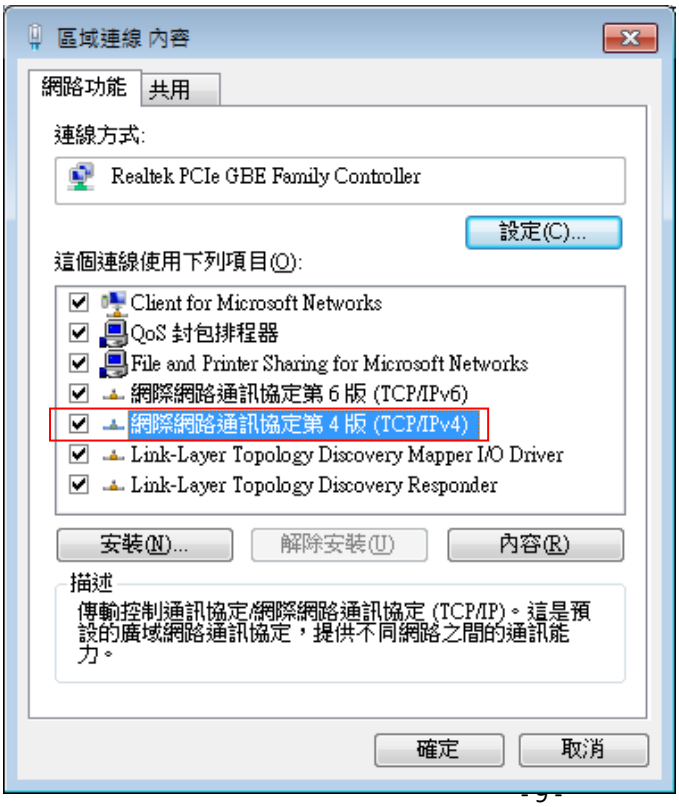

**步驟 3：** 進入變更介面卡設定則會出現以下圖示，將滑鼠移到＂**區域連線**＂後按下右鍵點擊內容



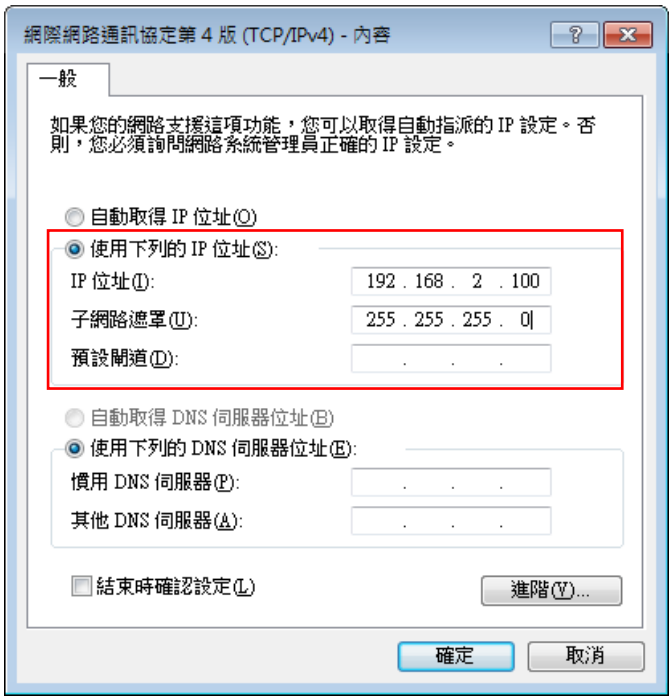
**步驟 4：**出現右鍵選單後，點擊選單下方的 " **內容** " (如下圖所示)將進入設定 TCP/IP。




**步驟 5：**進入後再 " **這個連線使用下列項目** " 內找出 " **網際網路通訊協定第 4 版(TCP/IPv4)** " 選項點擊兩下進入編輯。



**步驟 6：**點擊 TCP/IPv4 將進入 PC 或筆電的 IP 位址設定頁面，預設為自動取得 IP 位址，我們將它改為"使用以下的 IP 位址"，並在 IP 欄位打入與 Cerio CenOS 軟體的同網段 IP 位址，例如 Cerio CenOS 軟體的預設 IP 為 192.168.2.254，則 PC 或筆電的 IP 為者可以設定 192.168.2.x ，x 可設定 1~至 253 之間的數值。以下圖為例，完成設定。

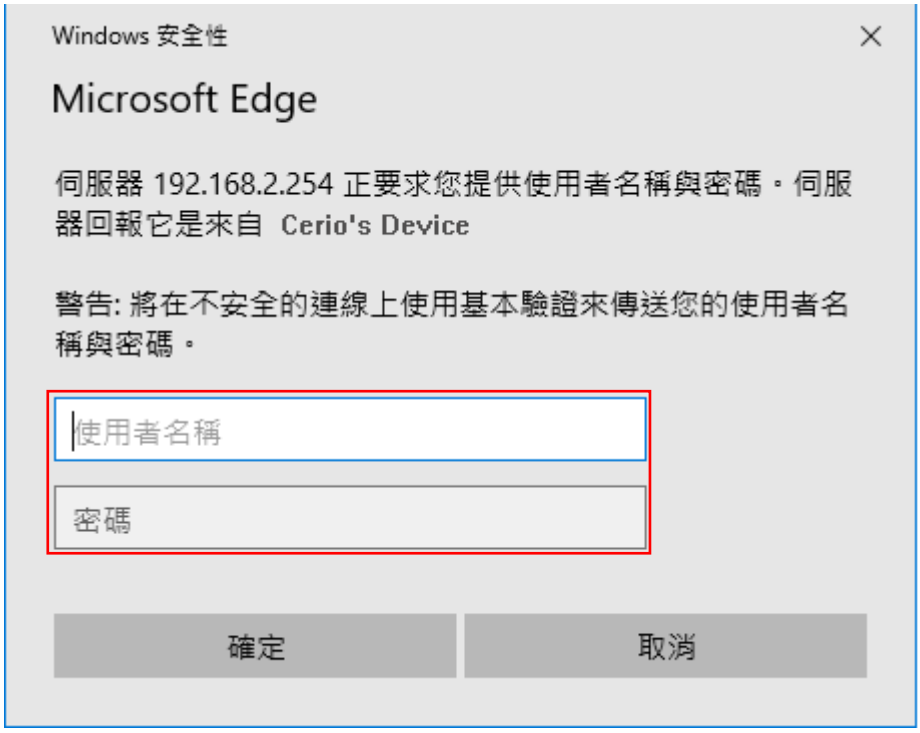



接下來請開啟您的 Internet Explorer 或 Firefox 瀏覽器並於 URL 網址列中輸入 CenOS5.0 軟體的預設的 IP 位址:http://192.168.2.254，然後按下鍵盤「Enter」鍵以開啟 CenOS5.0 軟體的 WEB 管理介面。

## 1.2 登入基地台的 WEB 管理頁面

接下來請開啟您的 Internet Explorer 或 Firefox 瀏覽器並於 URL 網址列中輸入基地台預設的 IP 位址：http://192.168.2.254，然後按下鍵盤「**Enter**」鍵以開啟基地台的 WEB 管理介面。


- 成功登入管理介面後將出現基地台的登入畫面，請在使用者名稱欄位中輸入〝**root**〞，密碼鍵入〝**default**〞，然後按「**確定**」即可登入管理介面。




請使用預設使用者名稱**" root"** 與 預設密碼 **" default "** 進行登入管理頁面

| Notice | 當設定完成後, 請務必回到 1.1 項目的步驟 6, 將電腦的 IP 改回自動取得 IP 位址, 或是設定為環境中相同的區域網路位址 |
|---|---|

# 2. 設定 CenOS5.0 軟體功能

## 2.1 中文化界面設定

若管理者需要使用中文頁面，管理者可以直接進入基地台管理頁面的系統內變更管理頁面的介面語系。

無線基地台的預設值啟動為英文語系操作介面下，請依照以下方式變更介面語系：

1. 點選進入「**System**」系統頁面。
2. 再點選進入「**Management**」管理頁面。
3. 點選「**System Language**」選項，並在「Language」下拉式選單中，選取「繁體中文」選項。

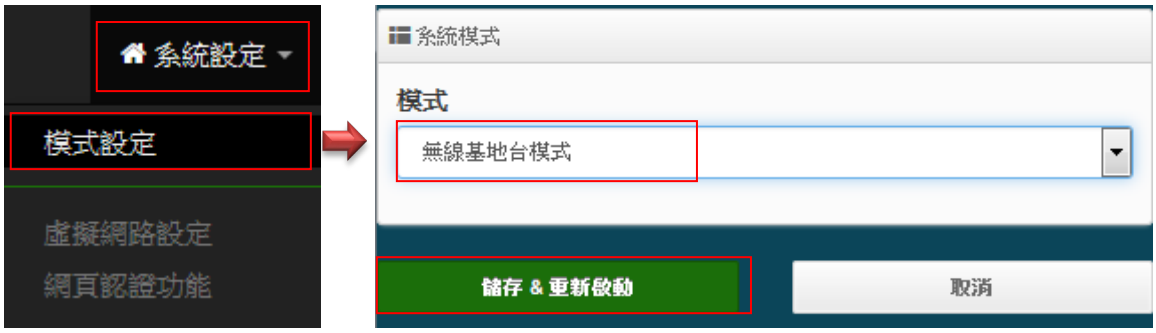

確認變更為「正體中文」後，請按下「**Save**」鍵儲存該項設定。

## 2.2 操作模式設定及說明

CERIO 無線基地台設備提供多選擇模式服務，可依不同模式廣泛應用在不同的環境，如下說明模式應用。

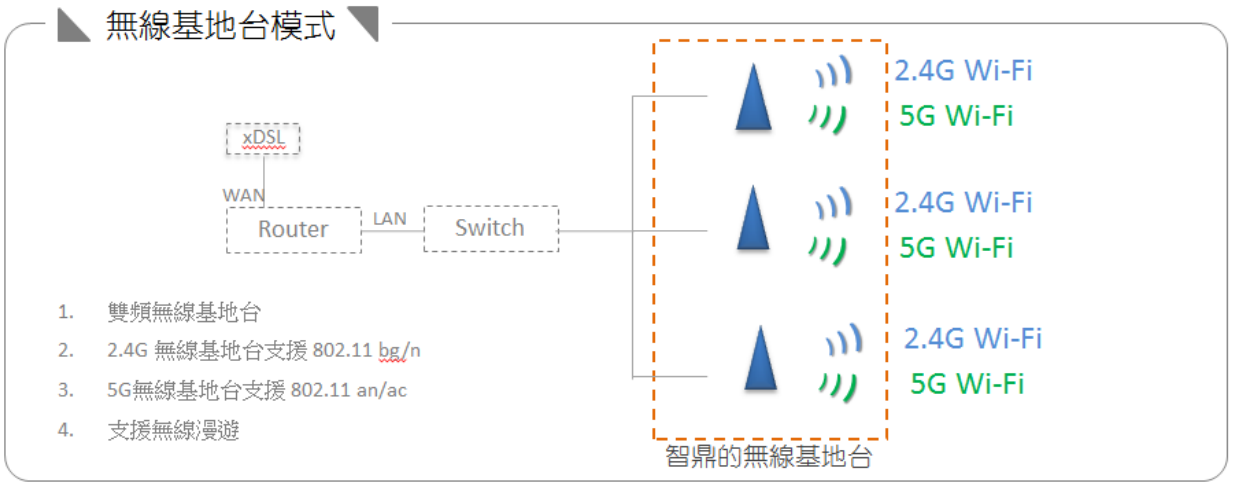
### 無線基地台 AP 模式

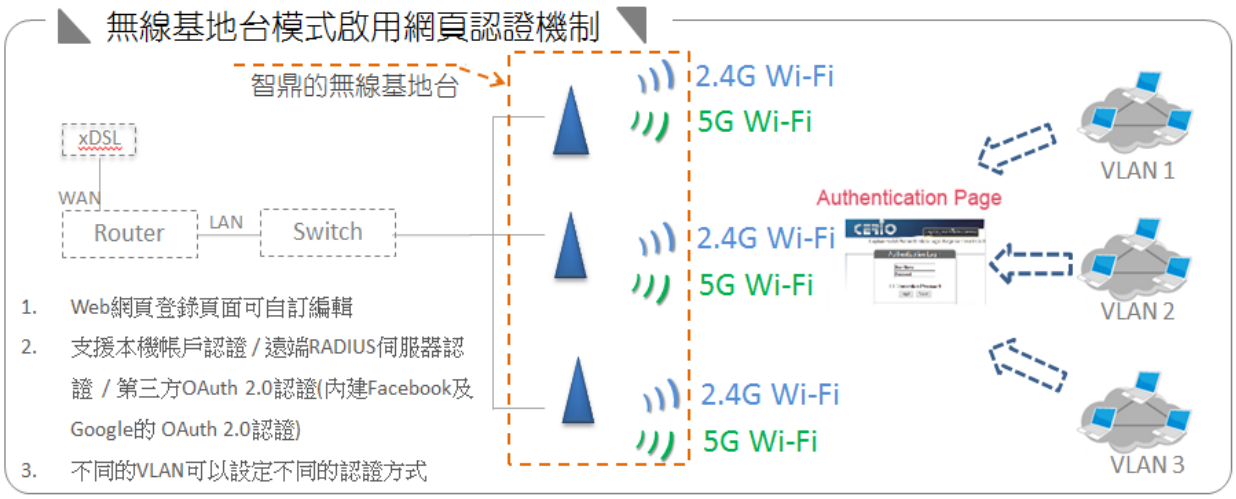
請點選**"系統設定" ➔ "模式設定"**，選擇無線基地台模式，確認後 **" 按下儲存&重新啟動 "** 按鈕即可完成模式切換。




當管理者啟動為基地台模式後，無線基地台可同時提供 2.4GHz 和 5G 無線服務，管理者設定完無線基地台相關設定後，直接透過網路線連接至區域網路即可完成無線 WiFi 使用。

在 AP 模式下可做網頁登入認證應用，認證方式支援 RADIUS Server，本機帳戶認證及支援網路 OAuth2.0 第三方認證，預設可設定 Facebook 和 Google 社群認證管理。本機內建 RADIUS 伺服器功能。

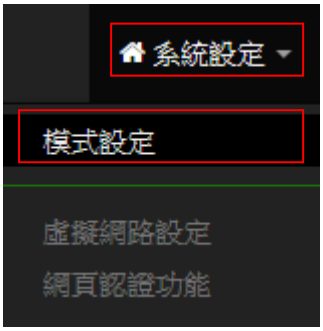


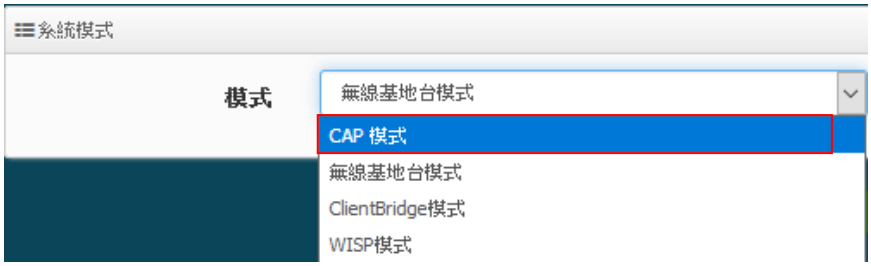



## CAP 無線基地台管理模式

當切換 CAP 此種模式本身是沒有無線基地台的功能，單純只做無線基地台的集中管理。

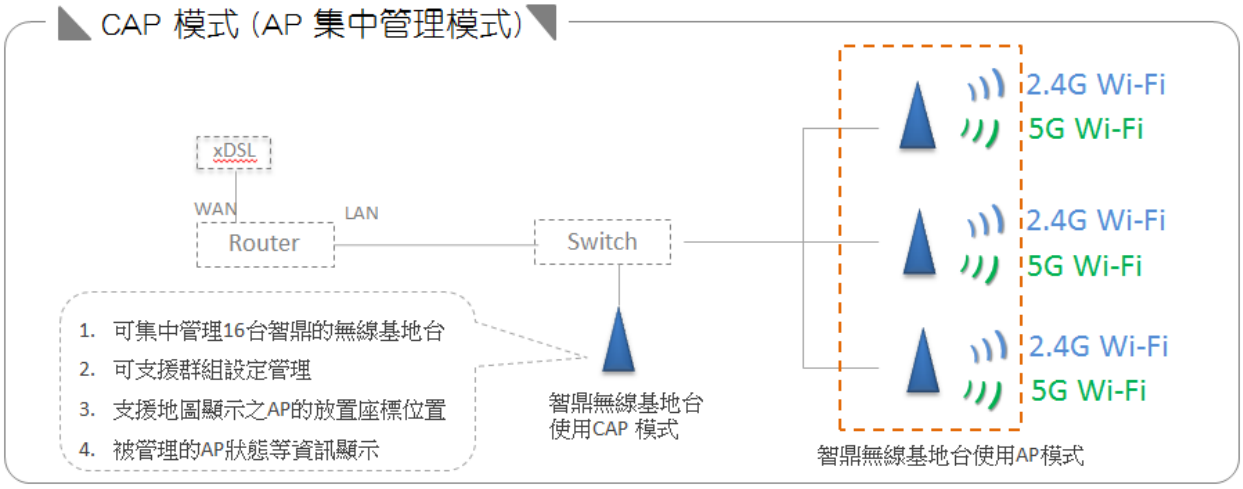
請點選**"系統設定" ➔ "模式設定"**，選擇 CAP 模式後儲存並重新啟動系統。



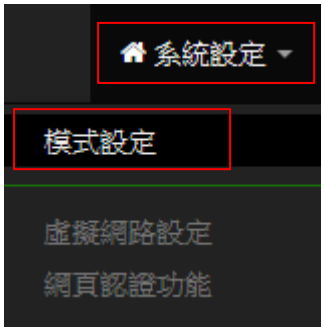

此 CAP 模式的 AP Control 主要是可以集中控管所有 CenOS5.0 核心的無線基地台。負責集中管理多台 AP 模式的無線基地台,能集中設定, VLAN 管理, 基地台監測等等。

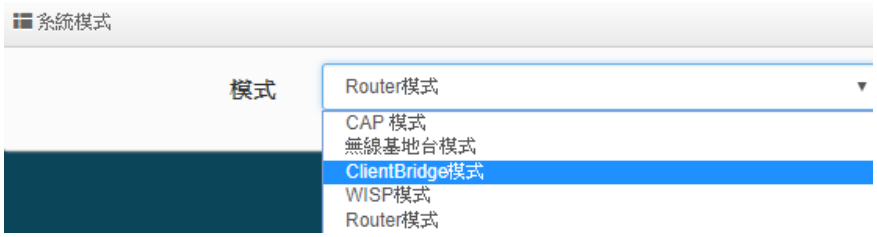
(集中管理無線基地台數量將依照產品型號有所不同, 請確認產品規格書說明)



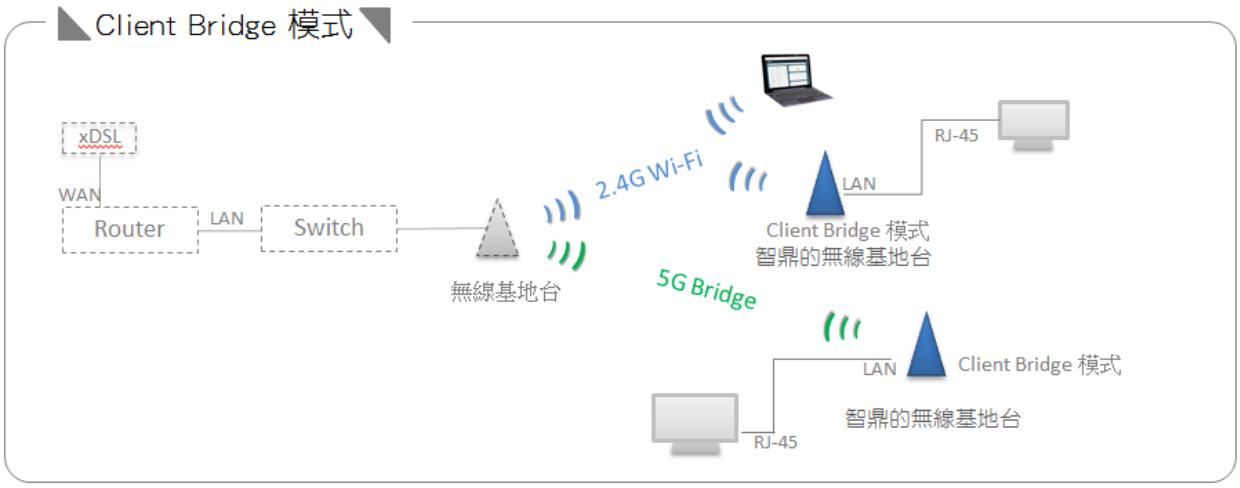
### Client Bridge 模式

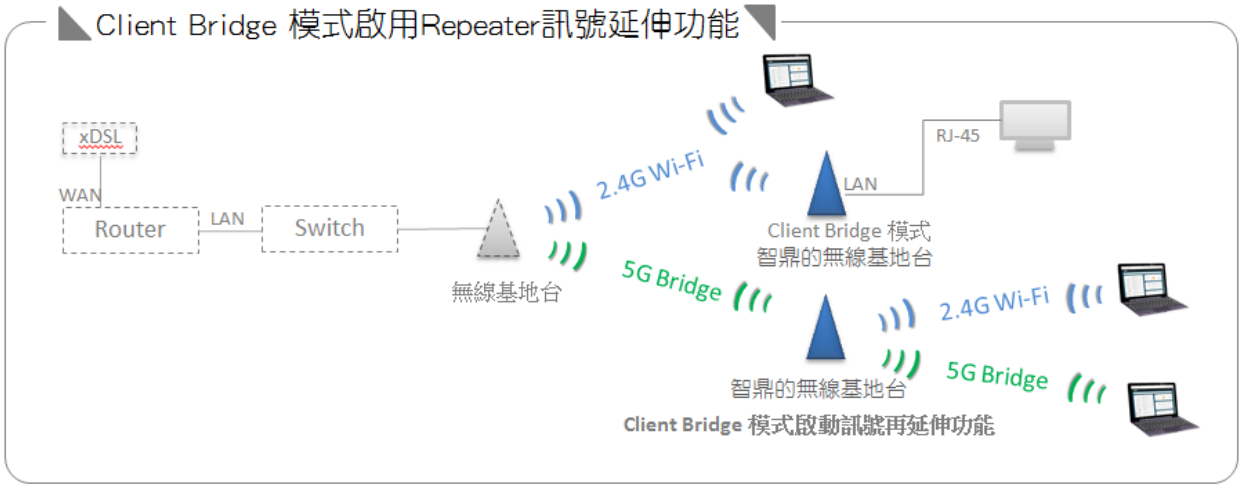
請點擊**"系統設定"➔"模式設定"**，選擇使用 Client Bridge 功能後儲存並重新啟動系統。




切換為 Client Bridge 模式後，則設備必須要與上端的基地台做橋接方可正常運作，而與上端 AP 橋接之後 Repeater 延伸基地台才可正常使用

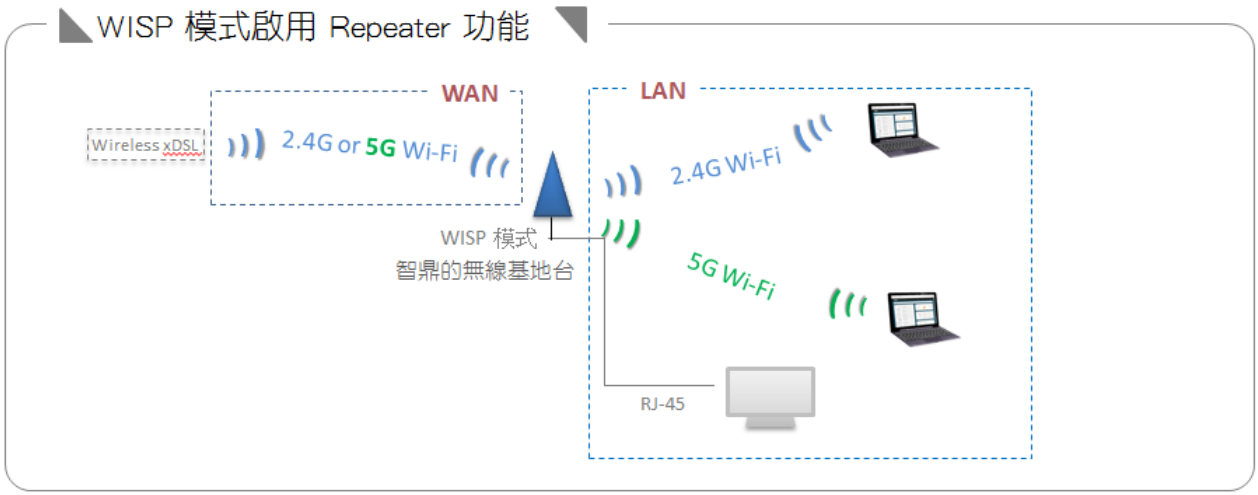


### WISP 模式

請點擊**"系統設定"➔"模式設定"**, 進選擇使用 WISP 模式後儲存並重新啟動系統。


切換此模式，WAN 端撥接方式將使用 Wireless 方式與上端無線 xDSL 做橋接

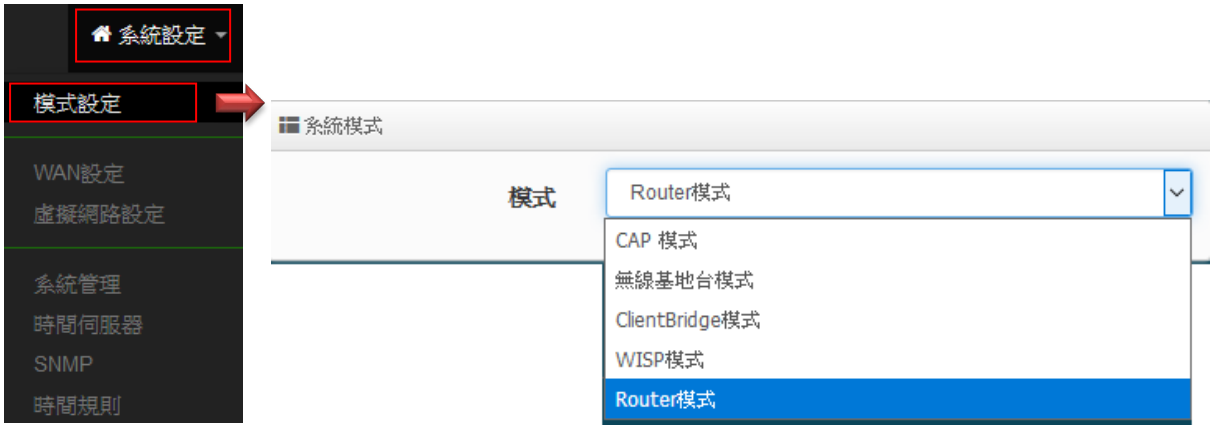


### Router 路由模式

當管理員啟動 Router AP 模式時，此系統可提供能連接上端 ISP，例如：PPPoE ADSL 或 Cable Modem 等，並可提供 NAT 功能及 DHCP 伺服器讓多人可以分享網際網路頻寬。

| Notice | 並非每個智鼎無線基地台設備都支援 Router 模式，請確認產品規格說明所支援模式 |
|---|---|

請先點選**"系統設定" ➔ "模式設定"** 進選擇使用 Router 模式後儲存並重新啟動系統。




確認選擇為 Router 模式後，請點擊 " **儲存＆重新啟動** " 完成變更操作模式。

當您啟動了 Router AP 模式後， WAN 埠連接上端 ISP 的 DSL 裝置，例如：PPPoE ADSL / Cable Modem / 固定制 ADSL 等，同時設備自動啟動 NAT 與 DHCP 功能以提供下層有線或無線使用者連結，並內建相當進階的功能，使用者可以依照需求進行網路連線管制、DMZ 以及虛擬伺服器規則設定等。

# 3. [ 系統設定 ]

## 3.1 WAN 設定

應用在 **Router** 或是 **WISP 模式**下運作，當切換成 **Router 或是 WISP 模式**後, WAN 設定可選擇設定”動態 IP” /”靜態 IP / PPPoE / PPTP 等四種設定方式。

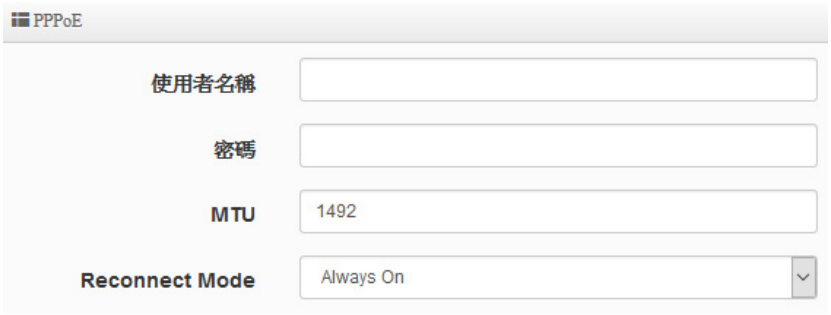

- **靜態 IP 位址**：若環境是使用 xDSL 或是上端網路有提供您固定的 IP 位址，管理人員可以使用此模式進行連線。


  - **IP 位址**：請輸入由您的 ISP 所提供的實體 IP 位址給 WAN 端介面使用。
  - **子網路遮罩**：請輸入由您的 ISP 所提供的子網路遮罩給 WAN 端介面使用。
  - **預設閘道**：請輸入由您的 ISP 所提供的預設閘道位址給 WAN 端介面使用。

- **動態 IP 位址(自動取得 IP)**：若您的 WISP 或是上端網路使用 DHCP 模式提供 WAN 端可連線的 IP 位址，您可以選擇使用此種連線方式。


  - **主機名稱:** 可設定主機使用名稱。

- **PPPoE**：主要設定 PPPoE 撥號連線帳號與密碼等，此帳密由 ISP 業者提供。



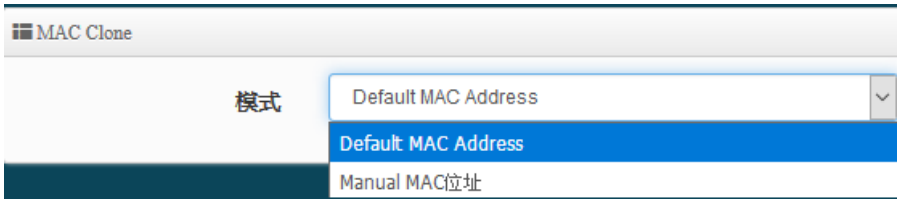

- **使用者名稱**：請輸入 ISP 所提供給你的 PPPoE 使用者帳號。
- **密碼**：請輸入 ISP 所提供給你的 PPPoE 使用者密碼。
- **MTU :** MTU 為 Maximum Transmission Unit 的縮寫。主要是 PPPoE 傳送封包的大小，通常為 1492 或 1500 長度為最佳值。(視 xDSL modem 決定)
- **Reconnect Mode**：可分為三種連線方式
  - ✓ **Always On:** 當 WAN 成功撥號連線後，將不自動斷線。
  - ✓ **On Demand**：可設定當 WAN 閒置時間多久後，WAN 自動離線。
  - ✓ **手動 :** WAN 不管是要連線或要斷線，都必須由管理者登入管理頁面進行撥號連線或離線動作

➢ **PPTP**：點對點的通道協議設定，假若 ISP 使用 PPTP 通道連接，則 WAN 也須設定為此協議進行連線。


- **使用者名稱**：輸入 PPTP 驗證的使用者名稱。
- **密碼**：輸入 PPTP 驗證的密碼。
- **PPTP**：輸入遠端連接的 PPTP 伺服器位址。
- **WAN IP**：輸入連接使用的 IP 位址。
- **子網路遮罩**：輸入 WAN IP 的子網路遮罩。

- **MTU**：PPTP 使用最佳的封包長度，預設為 1460。
- **MPPE40**：點對點的加密使用 40 位元。
- **MPPE128**：點對點的加密使用 128 位元。
- **Reconnect Mode:** 可分為 Always On / On demand / 手動等 3 種模式
  - ✓ **Always On:** 當 WAN 成功撥號連線後，將不自動斷線。
  - ✓ **On Demand**：可設定當 WAN 閒置時間多久後，WAN 自動離線。
  - ✓ **手動**：WAN 不管是要連線或要斷線，都必須由管理者登入管理頁面進行撥號連線或離線動作。

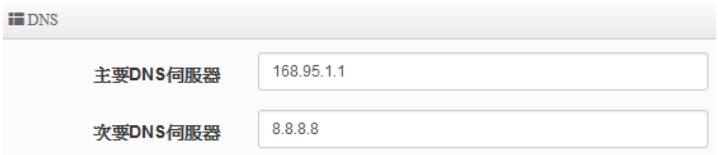
➢ **MAC Clone**：**連接 ISP 至網記網路所**註冊網卡卡號位址。




- **Default MAC Address**：使用預設本機 MAC 位址對**所**註冊網卡卡號。
- **Manual MAC 位址** ：由管理者選擇設定一組 PC 對外 ISP 的 MAC 位址。*(有些 ISP 將鎖定某特定電腦的 MAC 位址方可註冊, 例如社區網路等)*

  步驟說明: 請先確認所註冊的 PC 透過網路線連接至智鼎的無線基地台後, 在此功能頁面選擇 Manual MAC 位址即可顯示 PC 的 MAC 卡號


➢ **DNS**：設定 Domain Name 的網址解析伺服器位址。*(例如中華電信 168.95.1.1 或 168.95.192.1)*

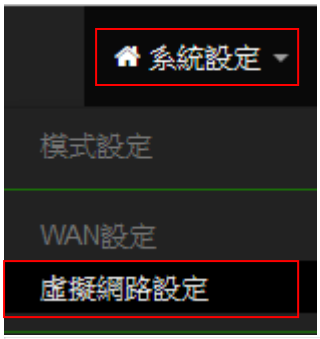



➢ **NAT Engine:** 啟動本機 NAT 路由加速引擎功能, 主要能加速 WAN 與 VLAN 之間的封包運算轉換速度, 但若啟用此 NAT 加速引擎之功能則一些防火牆功能將失效, 預設為開啟, 若管理者必須使用防火牆功能, 則建議須關閉此 NAT 加速。


以上功能設定完成後，請點擊 " **儲存** " 按鈕後記得須點擊 " **重新啟動** " ，完成功能運作。

## 3.2 VLAN 虛擬網路設定

應用在 **Router 模式** / **無線基地台模式**及 **CAP 模式**下運作，**而在 CAP 模式下將沒有無線基地台功能設定**，可支援多組虛擬網路服務(*依不同產品規格有所不同，請確認產品規格書*)，預設每個虛擬網路都支援 802.1Q Tag VLAN 功能， 管理員只要點擊啟用，系統將能完成設定 802.1Q Tag VLAN。




點擊"**虛擬網路設定**"後將顯示虛擬網路列表，依照不同型號將顯示不同 VLAN 筆數，如下圖範例

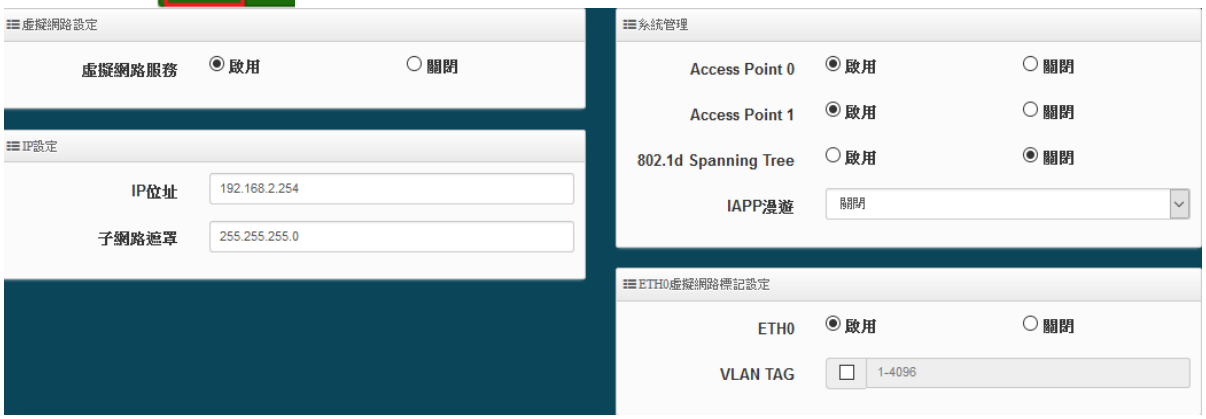
虛擬網路列表

| # | 虛擬網路服務 | 旗標 | IP位址 | 子網路遮罩 | Radio 0 | Radio 1 | 執行 |
|---|---|---|---|---|---|---|---|
| 0 | 啟用 | Native ETH0 | 192.168.2.254 | 255.255.255.0 | 2.4G_0_0 | 5G_0_1 | 網路 |
| 1 | 停用 | ETH0.101 | 192.168.101.254 | 255.255.255.0 | 2.4G_1_0 | 5G_1_1 | 網路 |
| 2 | 停用 | ETH0.102 | 192.168.102.254 | 255.255.255.0 | 2.4G_2_0 | 5G_2_1 | 網路 |
| 3 | 停用 | ETH0.103 | 192.168.103.254 | 255.255.255.0 | 2.4G_3_0 | 5G_3_1 | 網路 |
| 4 | 停用 | ETH0.104 | 192.168.104.254 | 255.255.255.0 | 2.4G_4_0 | 5G_4_1 | 網路 |
| 5 | 停用 | ETH0.105 | 192.168.105.254 | 255.255.255.0 | 2.4G_5_0 | 5G_5_1 | 網路 |
| 6 | 停用 | ETH0.106 | 192.168.106.254 | 255.255.255.0 | 2.4G_6_0 | 5G_6_1 | 網路 |
| 7 | 停用 | ETH0.107 | 192.168.107.254 | 255.255.255.0 | 2.4G_7_0 | 5G_7_1 | 網路 |

- **#：**顯示虛擬網路組別，共多組 802.1Q 虛擬網路。(依照不同功能或不同型號而不同,請參閱產品規格書)
- **虛擬網路服務：**顯示每組的虛擬網路目前是否啟用或停用。
- **旗標：**顯示實體網路孔預設運作使用哪個虛擬網路資訊，當顯示 " Native " 表示預設使用的虛擬網路，同時可顯示每個虛擬網路所使用的 802.1Q Tag 號碼。
- **IP 位址：**顯示每個虛擬網路的 IP 位址。
- **子網路遮罩：**顯示每個虛擬網路的子網路遮罩。
- **Radio 0：**顯示 2.4G 的 SSID 名稱及 2.4G Wi-Fi 是否運作(綠色為運作，紅色為停用)。
- **Radio 1：**顯示 5G 的 SSID 名稱及 5G Wi-Fi 是否運作(綠色為運作，紅色為停用)。
  *(請參考產品規格書說明是否有支援 Radio 1 之 5G 頻段，將依照不同產品決定)*
- **執行：**點擊 網路 的按鈕，進入 VLAN 的設定頁面，點擊 網路 下拉箭頭則可設定 DHCP 伺服器及無線基地台功能設定。

### 3.2.1 網路設定(按鈕)


➢ **網路**：點擊 網路 按鈕進入設定虛擬網路相關功能。




✓ **虛擬網路服務**：可選擇啟用或關閉虛擬網路服務。

Notice

虛擬網路服務及 IP 位址至少需要有一組 VLAN 服務正常啟用，請勿將整個虛擬網路服務(VLAN)功能全關閉，以免造成無法登入管理頁面進行管理，必須回復預設值。

✓ **IP 位址**：設定虛擬網路的 IP 位址。

✓ **子網路遮罩**：設定虛擬網路 IP 位址的子網路遮罩。

✓ **Access Point 0**：是否要啟用或停用此虛擬網路的無線基地台(2.4G)。

✓ **Access Point 1**：是否要啟用或停用此虛擬網路的無線基地台(5G)。

*(請參考產品規格書說明是否有支援 Radio 1 之 5G 頻段，將依照不同產品決定)*

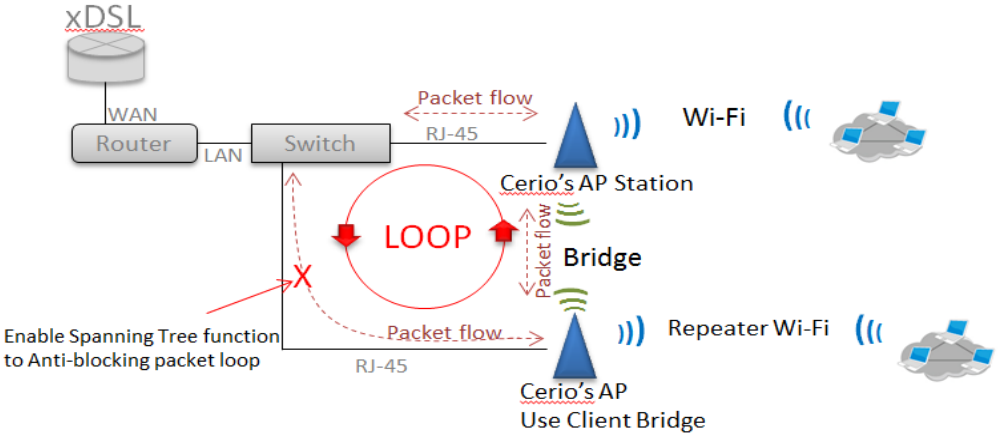
✓ **預設閘道:** 請正確輸入預設的閘道 IP 位址。( 在無線基地台模式下 )

Notice

若預設閘道位址設置錯誤，將導致無法上網或無法顯示 ESSID 名稱，請務必確實輸入正確

✓ **DNS:** 請輸入名稱解析的伺服器位址，可設置閘道器的 IP 位址或外部的 DNS IP 位址(如中華電信為範例 168.95.1.1 或 168.95.192.1) ( 在無線基地台模式下 )

✓ **802.1d Spanning Tree**：**Spanning Tree Protocol** 簡稱為 STP，啟用此功能應用在整個區域網路使用迴圈架構時，將可以避免迴圈架構導致網路癱瘓，如下圖描述。




- ✓ **管理埠:** 此無線基地台是否需要被 Cerio 的管理器集中管理。*(無線基地台模式下)*
- ✓ **IAPP 漫遊：**可選擇使用 2.4G 或 5G 的 IAPP 無線漫遊。*( IAPP 漫遊條件為 SSID 需一樣，無線加密需使用 WPA2-PSK 以及使用 AES 的加密演算方式 )*
- ✓ **ETH #虛擬網路標記設定:** 主要設定實體網路埠使用 802.1Q 的 tag 轉 PVID，管理人員可設定是否要啟用或停用埠。*(此功能將依照不同型號產品所使用的網路連接埠多寡有所不同，可參考產品規格書)*

| Notice | 注意假如 ETH0 設定 VLAN Tag 時，則 AP **就只會聽取特定** VLAN Tag 的封包，其他不同的 VLAN 則將阻絕。 |
|---|---|

設定完成後，請點擊 " **儲存** " 按鈕後記得須點擊 " **重新啟動** " ，完成功能運作。

### 3.2.2 網路設定(下拉式功能)

點擊"網路"旁下拉式按鈕 

設定 DHCP 伺服器，頻寬控制及無線基地台功能等。


| Notice | Radio 1 (5G 無線頻率)設定，將依照是否有支援 5G 產品決定，請參閱產品的規格書說明確認是否支援。 |
|---|---|

## # DHCP 伺服器

設定 IP 位址自動派送給使用者之功能，請正確設定 IP 位址的派送區間和正確輸入網路的閘道位址及 DNS 伺服器位址



- **DHCP 服務:** 管理人員可以選擇啟動或關閉此服務，當關閉此功能則系統將不會自動派送 IP 位址給使用者。

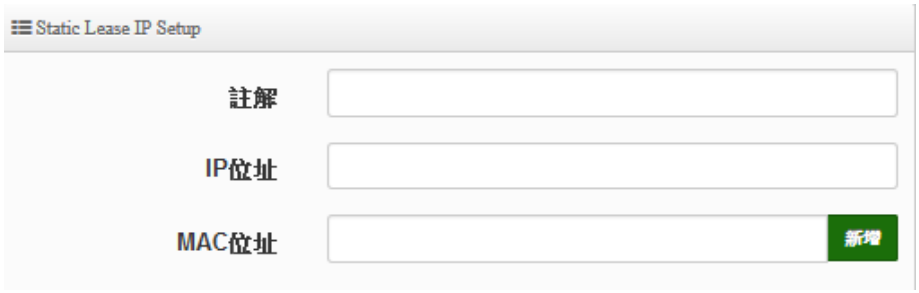

- **起始 IP 位址**：設定 DHCP 伺服器要派送 IP 的起始位址。
- **結束 IP 位址**：設定 DHCP 伺服器派送 IP 的結束位址。
- **子網路遮罩**：設定 DHCP 伺服器派送的 IP 子網路遮罩。
- **預設閘道**：設定要透過 DHCP 伺服器派送網路閘道 IP 位址。
- **主/次要 DNS 伺服器**：設定要透過 DHCP 伺服器派送 DNS 位址。
- **WINS 伺服器位址**：假若網域中有架設 WINS 伺服器，可在此設定 WINS 伺服器 IP 位址。
- **Domain**：當網域有設定網域名稱，可在此輸入網域的名稱。
- **IP 租用時間**：可設定派送 IP 的租用時間，預設 86400 秒(1 天)。若在公共區域架設此產品，建議可以縮短 IP 租用時間，例如 3600 秒為 1 小時

- **DHCP 用戶列表:** 顯示目前已派送至使用者的 IP 位址列表

DHCP用戶列表

| # | IP位址 | MAC位址 | 主機名稱 | Expired | 執行 |
|---|---|---|---|---|---|
| - | - | - | - | - | |

- **Static Lease IP Setup:** 設置 DHCP 伺服器的 IP 位址綁定於特定 PC 使用。




- **Static Lease IP List:** 當確認設定 DHCP 伺服器的 IP 位址綁定後，將顯示至此列表欄位上。

Static Lease IP List

| # | 註解 | IP位址 | MAC位址 | 執行 |
|---|---|---|---|---|
| - | - | - | - | - |

## # 頻寬控制

限制 VLAN 的使用或是用戶端的最大/小頻寬，用戶頻寬管理可限制 IP/MASK , IP Range, Port(Service), SIP, RTP/RTSP, WEB 等等的頻寬限制。

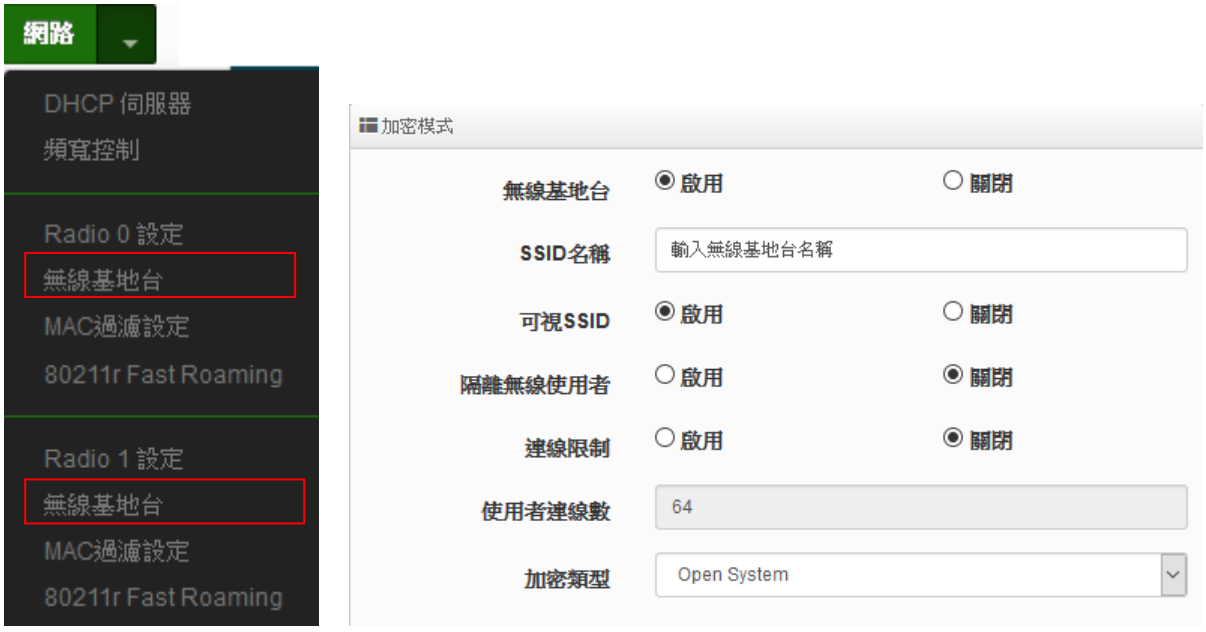

管理人員可以選擇啟用或關閉此頻寬管理之功能

- **Total Bandwidth Control:** 管理人員可限制此 VLAN 的總上傳與下載的頻寬速率
- **QoS Rule List:** 管理人員可以限制 IP/MASK , IP Range, Port(Service), SIP, RTP/RTSP, WEB 等協議, 每個 VLAN 共可設定 10 筆 QoS 規則

## # [2.4 / 5G]無線基地台設定

**Radio 0 (2.4G) / 1(5G) :** 無線基地台設定

| Notice | Radio 1 (5G 無線頻率)設定, 將依照是否有支援 5G 產品決定, 請參閱產品的規格書說明確認是否支援。 |
|---|---|




- **無線基地台：**可針對特定的"虛擬網路(0~7)"啟用或關閉無線基地台訊號。
- **SSID 名稱：**顯示此虛擬網路的無線 SSID 名稱。
- **可視 SSID：**預設為開啟，點選「關閉」後此無線服務將會隱藏 SSID 顯示功能。
- **隔離無線使用者：**點選「啟用」後，將阻隔無線使用者與無線使用者之間的溝通，不含有線。
- **連線限制：**針對一個 SSID 最大可連線的無線使用者數量，最大支援同時 64 個使用者存取同一個 SSID。

| Notice | 建議最佳 2.4G 的最大連線數 40 人，5G 最大連線數 60 人 |
|---|---|

- **加密類型：**管理者可設定 WPA-PSK/WPA2-PSK Personal 和 WPA/WAP2-Enterprise 及 802.1x 等 3 種加密模式。

### WPA-PSK/WPA2-PSK Personal


- **WPA 模式**：可選擇系統自動判斷去使用 WPA 或 WPA2 加密模式, 或者可單一固定使用 WPA 或單一使用 WPA2 等 3 種選擇。
- **加密演算法**：使用者可選擇 AES 或 TKIP 兩種加密演算法，出廠預設值 AES，此加密演算法，將影響傳送速率，建議使用 AES。
- **主要金鑰群組更新時間**：使用者可設定主要金鑰群組重新編碼更新時間，出廠預設值為 600 秒。
- **金鑰**：管理者設定此虛擬無線網路 SSID 連線密碼。
- **WPS**：啟用後將可點擊 Push button。假若 WiFi Client 設備有 WPS 功能鍵，可透過此功能直接偵測互相連接，就無須再輸入設定及密碼即可馬上完成連接動作。

### WPA/WAP2-Enterprise


- **WPA 模式**：可選擇系統自動判斷去使用 WPA 或 WPA2 加密模式, 或者可單一固定使用 WPA 或單一使用 WPA2 等 3 種選擇。
- **加密演算法**：使用者可選擇 AES 或 TKIP 兩種加密演算法，出廠預設值 AES，此加密演算法，將影響傳送速率，建議使用 AES。

- **主要金鑰群組更新時間**：使用者可設定主要金鑰群組重新編碼更新時間，出廠預設值為 600 秒。
- **Radius 伺服器**：設定遠端 Radius 伺服器 IP 位址。
- **Radius 埠**：主要設定遠端 Radius 伺服器所用的 Port 號。預設的 RADIUS 伺服器 port 號為 1812。
- **Radius Secret**：輸入 RADIUS 伺服器的登入碼。

### 802.1x 認證

當使用者啟用 WEB 802.1X，請參考動態 WEP 設定及 RADIUS 伺服器設定以利完整設定。


- **金鑰長度**：您可以選擇使用 64bits 或 128bits 金鑰長度，系統將會針對所選的位元來演算金鑰。
- **Radius 伺服器**：設定遠端 Radius 伺服器 IP 位址。
- **Radius 埠**：主要設定遠端 Radius 伺服器所用的 Port 號。預設的 RADIUS 伺服器 port 號為 1812。
- **Radius Secret**：輸入 RADIUS 伺服器的登入碼。

設定完成後，請點擊 " **儲存** " 按鈕後記得須點擊 " **重新啟動** " ，完成功能運作。

## # [2.4/5G]無線 MAC 過濾


Notice

Radio 1 (5G 無線頻率)設定, 將依照是否有支援 5G 產品決定, 請參閱產品的規格書說明確認是否支援。

點選 2.4G 或 5G 的「MAC 過濾設定」將可以進入「ACL 存取控制」設定頁面。過濾規則可分為兩部分 分別是

(1) 只阻擋 MAC 表單內的位址連線，其他設備將可以連接無線基地台。

(2) 只允許 MAC 表單內的位址連線，其他設備將無法連接無線基地台。




- **規則 ：** 可選擇關閉過濾 / 開放或阻擋 MAC 的表單位址。
- **MAC 位址：**輸入要管理的 MAC 位址。
- **MAC 位址列表：**當建置設備的 MAC 位址後，將列入表單內。

設定完成後，請點擊 " **儲存** " 按鈕後記得須點擊 " **重新啟動** " ，完成功能運作。

## # [2.4/5G]的 802.11r 快速漫遊


IEEE 802.11r/11k 的技術，作用是將整個區域網路佈建的無線基地台所涵蓋的訊號範圍之間，讓無線用戶端遊走無線基地台，迅速轉跳最佳的無線基地台連接，在轉跳過程不中斷。


- **快速漫遊**：啟動或關閉漫遊功能。
- **Mobility Domain**：設第一組共享網域，所有的 AP 在同一個網域內能共享一個相同的 SSID，目的可在一個 STA 之間可以使用快速 BSS 轉換。

| Notice | 此設定必須為 2 組 16 進位碼。 |
|---|---|

- **R0 Key Lifetime：設定** PMK-R0 的使用壽命，預設為 10000，可設定 1~65535 內的值。
- **Reassoc deadline**：重新連接的截止時間，預設為 1000，可設定 1000~65535 內的值。
- **R0/NAS Identifier**：當使用 802.11r 時，在 nas_identifier 上是必須設定的，可設定 1~48 位元字串
- **R1 Identifier**：PMK-R1 的 key 標識，設定 12 個字元，以 16 進位方式。
- **R1 Push :** 將 R1 資訊導給 R0, 建議啟用。

**R0 Key holders :** 輸入要轉跳的另一端無線基地台的 R0 認證資訊。

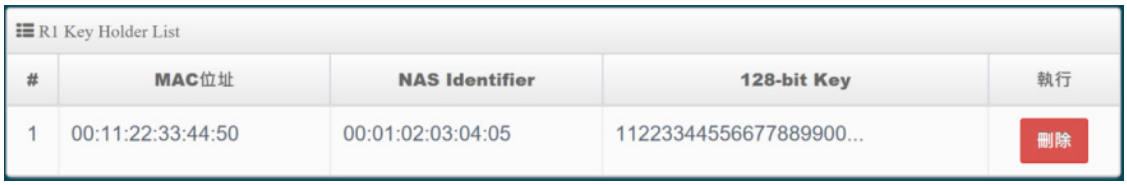

- **MAC 位址**：輸入另一端無線基地台的無線網卡卡號。
- **NAS Identifler**：輸入 AP 的 NAS Identifler 網域名稱。
- **128-bit Key**：輸入一組共用的 128-bit Key 碼。

輸入確認後將列入以下 R0 Key 表單內，如下圖


**R1 Key holders :** 輸入統一認證的無線基地台的 R1 資訊。


- **MAC 位址**：輸入另一端無線基地台的無線網卡卡號。
- **R1 Identifler**：輸入 AP 的 R1 Identifler 網域名稱。
- **128-bit Key**：輸入一組共用的 128-bit Key 碼。

輸入確認後將列入以下 R0 Key 表單內，如下圖

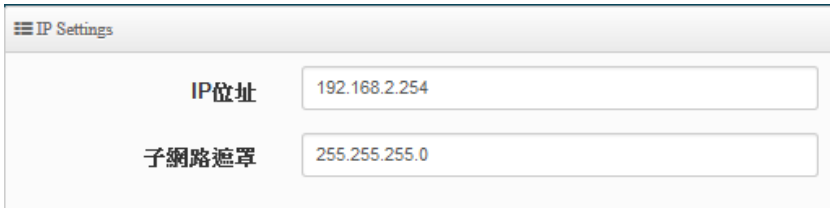



設定完成後，請點擊 " **儲存** " 按鈕後記得須點擊 " **重新啟動** " ，完成功能運作。

## 3.3 LAN 區域網路設定

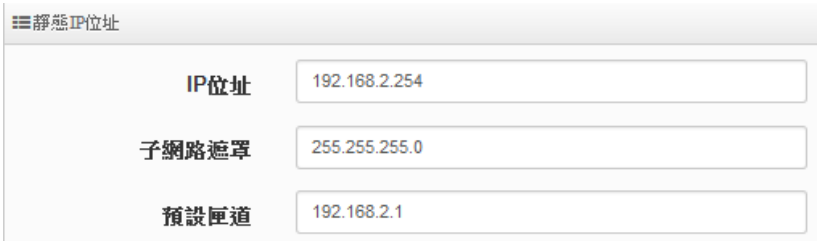
應用在 **Client Bridge** 及 **WISP 模式** 下運作，將顯示區域網路功能，當切換為 Client Bridge 模式時管理者可設定產品的區域網路的連線類型 / IP 位址 / DNS / DHCP forward / STP 等等功能，而在 WISP 模式下則可設定 IP 位址及 STP 等兩項功能。


**以下為 WISP 模式之設定頁面，主要設置設備的 IP 位址**



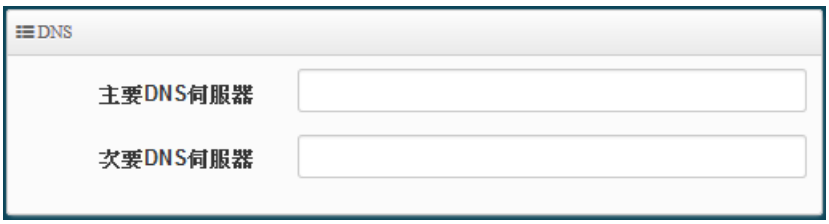

**以下為 Client Bridge 模式之設定頁面**


- **模式:** 管理人員可以為系統設定使用靜態 IP 位址或動態 IP 位址
  - **靜態 IP 位址：**可手動設定一組固定 IP 位址給系統使用。




    - ✓ **IP 位址:** 設定系統的 IP 位址。
    - ✓ **子網路遮罩:** 設定 IP 的子網路遮罩。
    - ✓ **預設閘道:** 設定網域的閘道位址。
  - **動態 IP 位址：**假若上端已有 DHCP 伺服器，則可使用動態 IP 位址可讓系統自動取得一組 IP

| Notice | 使用動態 IP 位址請注意，因系統會自動取得上端派送的 IP 位址，而所派的 IP 位址將由上端 DHCP 伺服器運算確認後派送， IP 位址則使用不固定，若管理人員要進入系統管理，可由上端 DHCP 伺服器去查詢目前系統所取得的 IP 位址。 |
|---|---|

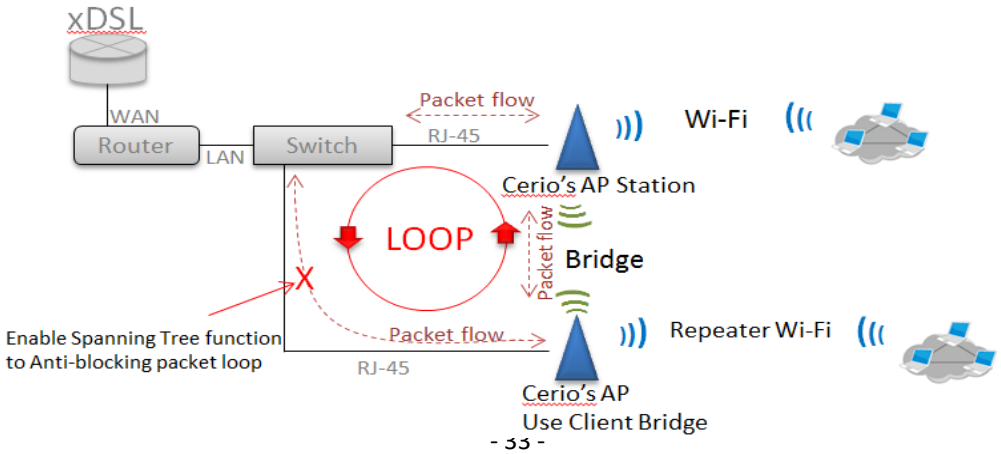



- **DNS:** 請輸入名稱解析的伺服器位址，可設置閘道器的 IP 位址或外部的 DNS IP 位址(如中華電信為範例 168.95.1.1 或 168.95.192.1)


- **DHCP Forward:** 當系統有啟用 DHCP 伺服器功能時，則需啟用此功能，系統才能協助轉派 IP 位址。


- **ETH #虛擬網路標記設定:** 主要設定實體網路埠使用 802.1Q 的 tag 轉 PVID，管理人員可設定是否要啟用或停用埠。*(此功能將依照不同型號產品所使用的網路連接埠多寡有所不同，可參考產品規格書)*

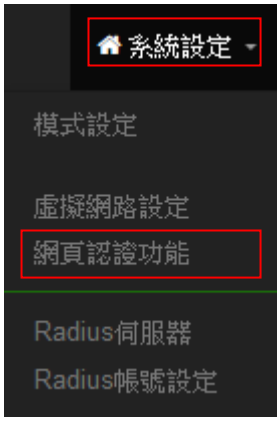

- **802.1d Spanning Tree：Spanning Tree Protocol** 簡稱為 STP，啟用此功能應用在整個區域網路使用迴圈架構時，將可以避免迴圈架構導致網路癱瘓，如下圖描述。



## 3.4 網頁認證功能

此功能頁面主要在"無線基地台模式"下，當啟動並設定完成後將出現熱點網頁身份驗證，當網頁驗證成功後，才能進行使用網路服務相關資源，而認證成功的使用者將會在 " 系統資訊 " 功能頁面中顯示使用者認證相關資訊。

請點選"系統設定"➔ " 網頁認證功能 "




點擊"**網頁認證功能**"後，將顯示認證列表，依照不同型號將顯示不同筆數，如下圖範例，此認證列表將對應不同的(虛擬網路(VLAN)，在不同的 VLAN 下可設定不同的認證方式

Notice

**當預想要啟用網頁認證功能時，請務必要確認無線基地台設備必須能連線至閘道器，請參考 3.2 虛擬網路設定確實設定閘道位址及 DNS 等功能，假若閘道位址錯誤，網頁認證功能將無法正常運作**

虛擬網路列表

| # | 虛擬網路服務 | 網頁認證功能 | 執行 |
|---|---|---|---|
| 0 | 啟用 | 停用 | 網頁認證功能 |
| 1 | 停用 | 停用 | 網頁認證功能 |
| 2 | 停用 | 停用 | 網頁認證功能 |
| 3 | 停用 | 停用 | 網頁認證功能 |
| 4 | 停用 | 停用 | 網頁認證功能 |
| 5 | 停用 | 停用 | 網頁認證功能 |
| 6 | 停用 | 停用 | 網頁認證功能 |
| 7 | 停用 | 停用 | 網頁認證功能 |

- **虛擬網路服務:** 顯示目前已啟用的虛擬網路服務。(可參照"3.2 虛擬網路設定")
- **網頁認證功能:** 顯示每個虛擬網路服務是否開啟網頁認證功能
- **執行:** 可點擊按鈕進入啟用或關閉及設定相關網頁認證功能

Notice

1. 網頁認證功能 按鈕，主要能設定啟用認證功能服務及相關認證服務等
2. 網頁認證功能 下拉功能選單，可設定提供給"遊客"使用、本機帳號、OAuth2.0 認證、網頁登入頁面客製化、登入頁面語系、Walled Garden、特權名單以及將認證功能的設定檔備份或存回套用等等。

※ 以下說明認證功能操作方式

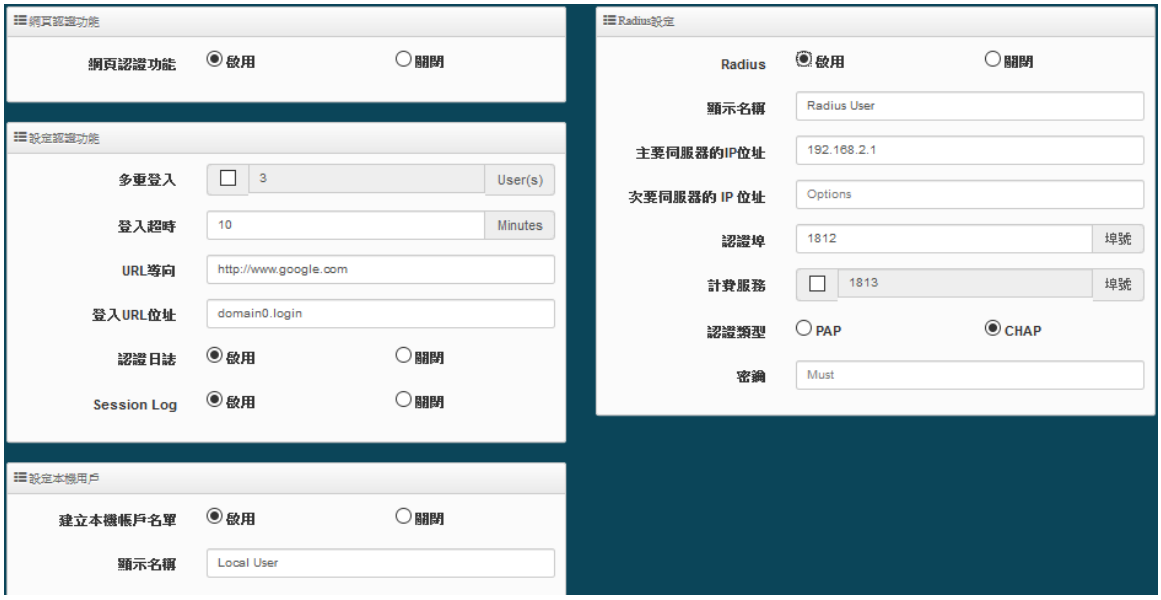
### 3.4.1 啟動網頁認證功能

主要能設定啟用認證功能服務及認證方式，同時可設定頻寬控制等相關功能

請點擊 網頁認證功能 按鈕進入設定頁面


➢ **網頁認證功能：**可選擇**"啟用"**或**"關閉"**認證服務。

當點擊啟用，則如下頁面操作說明




**※設定認證功能**

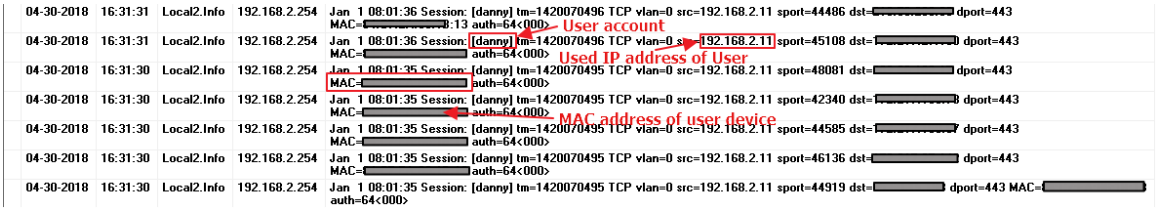

➢ **多重登入：**當勾選啟用此功能，則同一個帳號能給多人同時登入，同時登入人數可由管理者自行設定，0為不限制。

➢ **登入超時：**當使用者登入後，無進行任何網路行為，無任何流量下，停滯幾分後系統自動讓使用者登出。

- **URL 導向**：使用者網頁登入後，系統自動導向到此設定網站位置。
- **登入 URL 位址**：設定登入頁面的網頁位址。
- **Session Log**：可選擇啟用或關閉，啟用主要是將使用者的上網 Session 資訊存放至 SysLog 伺服器上。

> Notice
> **啟用後必須至系統設定➔系統管理下設定"系統紀錄設定"去指定環境中的** SysLog 伺服器的 IP 位址及埠號，方可讓 session 的 log 訊息往 server 備存。

**System Log server information: 提供參考**




### ※ 設定本機用戶


- **本機帳號**：可選擇**"啟用"**或**"關閉"**使用本機帳號認證登入

> Notice
> 當啟用本機帳號後，請務必至 **" 本機帳戶 "** 功能選單去建立認證用戶帳密，請參考 3.4.1 **認證功能設定➔本機帳戶**

### ※ RADIUS 設定

網頁認證方式支援遠端 RADIUS 伺服器認證，假若環境中已經有使用 RADIUS 伺服器做安全認證帳戶，此功能認證啟用可以將網頁認證的帳戶指向內部的 RADIUS 伺服器，由現有的 RADIUS 伺服器內的帳戶資料做網頁登入認證使用。

- **Radius：** 可設定**"啟用"**或**"關閉"**此認證服務。
- **主要伺服器的 IP 位址 ：** 設定遠端 RADIUS 伺服器的 IP 位址。
- **次要的伺服器 IP 位址 ：** 設定備用的 RADIUS 伺服器 IP 位址。(依照環境需求設定)
- **認證埠 ：** 設定 RADIUS 伺服器使用的通訊埠號。
- **計費服務：**假若遠端 RADIUS 伺服器有啟用計費服務(如統計流量等等)之功能，可在此設定遠端 RADIUS 伺服器的計費服務埠。
- **認證類型：**可選擇 PAP 或 CHAP 的認證類型。
- **密鑰：**輸入連接遠端 RADIUS 伺服器的密鑰。

※ **頻寬控制**


- **單一使用者：**可以啟動或關閉單一頻寬控制，針對每個所有使用者去限制上下傳頻寬。
- **總計：**可以啟動或關閉總計頻寬控制，限制總流量頻寬提供給下端所有使用者去使用。

### 3.4.2 網頁認證功能設定

請點擊 

下拉功能選單，可設定提供給"遊客"使用、本機帳號、OAuth2.0 認證、PoP3/IMAP Server 認證、網頁登入頁面客製化、登入頁面語系、Walled Garden、特權名單、Bulk MAC Address 以及將認證功能的設定檔備份或存回套用等等。


➢ **# 遊客**

可啟用或停用此服務，此功能主要可以設定網頁認證的遊客免輸入帳密就能享受網路服務資源，管理者則可以限制同時有多少遊客使用，限制遊客時間及使用流量管理等等。


- **服務**：可**"啟動"**或**"關閉"**遊客功能服務。
- **登入類型**：可選擇遊客使用網路服務的時間類型
  - ✓ **一次性**：所謂一次性就是若給遊客使用 10 分鐘，從遊客登入開始的同時時間就開始計算，一直到 10 分鐘後結束。
  - ✓ **Multiple Time**：為多次性登入，也就是說假設給遊客 10 分鐘的時間，當遊客在 10 分鐘內登出，時間將停止不再計算，直到下次登入再由上次停止時間繼續計算。
- **Count Limit**：設定開放遊客的連線人數。
- **登入時間**：設定遊客使用時間。
- **QoS**：可啟用或關閉遊客的使用上下載流量控制。

➢ **# 建立本機帳戶名單**

可在本機上建立網頁認證的登入帳密，最多 20 筆資料。



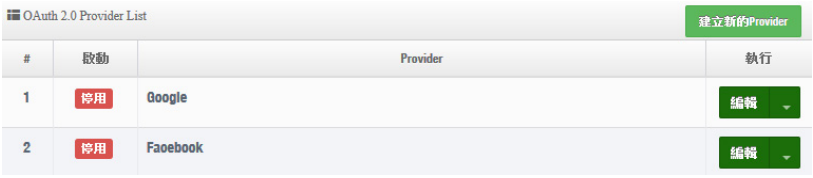
- **使用者名稱**：輸入使用者帳戶名稱
- **密碼：輸入使用者的帳戶密碼**

**#　本機用戶列表**：將顯示所建立的所有帳戶帳號

➢ **# OAuth2.0**

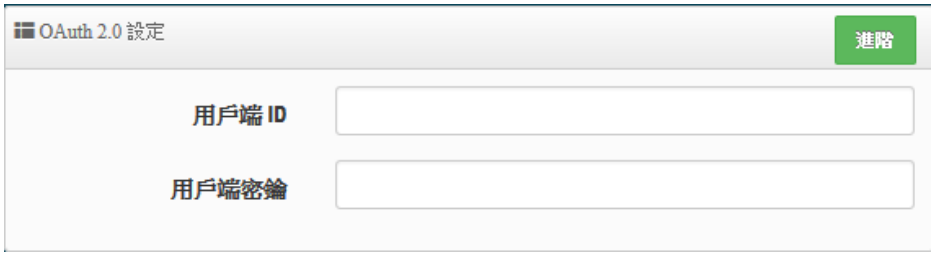
開放第三方認證伺服器，可透過如 facebook 或 google 等的使用這戶作為網頁認證登入機制使用，此系統預設可使用 facebook 或 google 的認證設定。



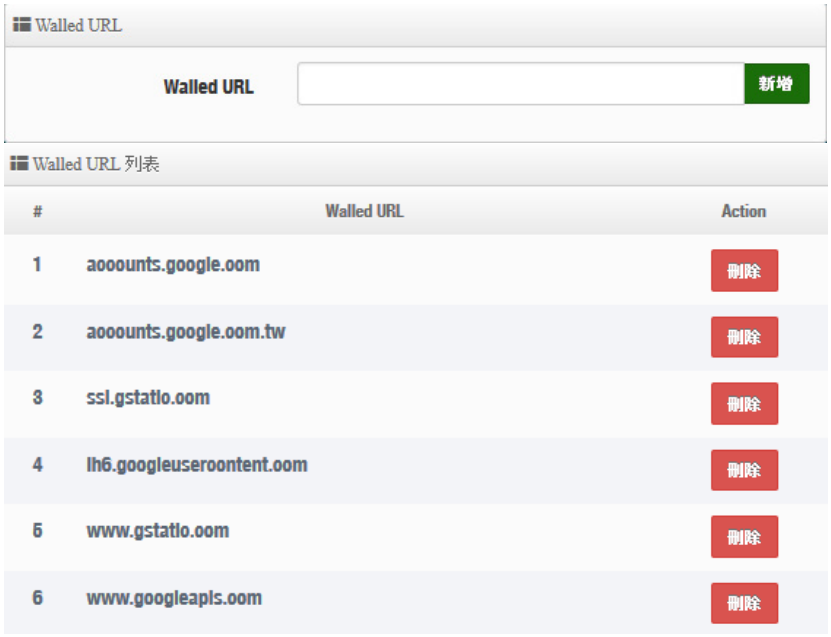



Notice **以下申請流程屬於第三方伺服器，若有所變動將以第三方官方網站發布為主**

**# Google：** 管理者需先至 Google 的 OAth2.0 服務頁面申請帳戶，將申請後的帳戶 ID 及密鑰輸入於欄位中。




以下資訊功能無須在增加或刪除，在預設值中已經將 Google 的設定認證資訊頁面位址增加到此欄位，若使用 Google 的 Oath2.0 則無需再設定。




## # Google 的 OAth2.0 服務頁面設定說明

**1. 請登入至 google 的 API 管理介面去建立一個 OAuth 用戶端 ID**


2. 選擇網路應用程式


3. 設定 JavaScript 來源及 REDIRECT URI 授權重新導向 URI 的位址，如下

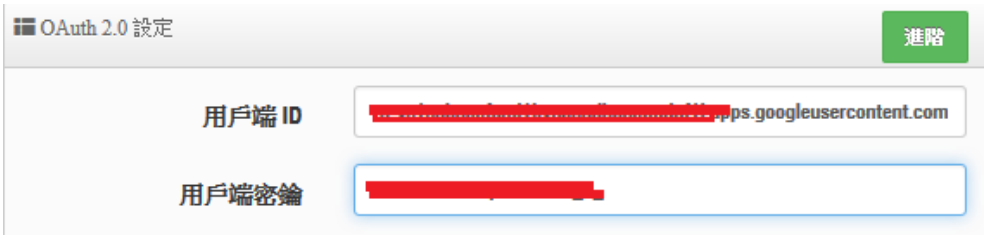

Notice

管理者必須確定 Google Developers 的 **“Redirect URI”** 和 **“JavaScript ORGINS”**的位址必須與系統的 Login URL 所設定的**“JavaScript ORGINS”** 要一樣才能正常運作。請回 **3.4.1.啟動網頁認證功能的”設定認證功能欄位”設定，例如:** 在 Google 的帳戶認證設定頁面下，設定如下位址

**JavaScript ORGINS:** http://domain0.login.com
**REDIRECT URI :** http://domain0.login.com/login/index.cgi?cgi=CALLBACK
而在系統上的 Login URL 必須與 Google 的 **JavaScript ORGINS** 一樣

4. 確認建立後將得到一組 ID 與密鑰

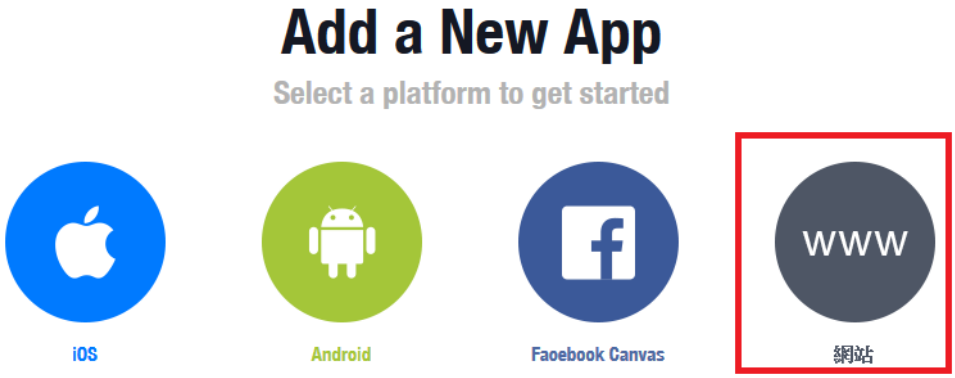

5. 將 ID 與密鑰貼入系統的 google 編輯內的 OAuth2.0 設定下，確認及完成




## # Facebook 的 OAth2.0 服務頁面設定說明

1. 先至 facebook 的 developers 頁面去，點擊 " 製作新應用程式 " 申請一組帳戶


2. 設定此應用程式屬性，為 WWW 網站



3. 建立此應用程式的名稱，之後可依照下一步進行設定，或直接跳過資訊


4. 之後可在基本設定內設定網址，新增一筆 URL
http://domain0.login.com/login/index.cgi?cgi=CALLBACK


5. 確認 Facebook 的 APP 認證設定完成，記住請至 " 應用程式審查 " 功能去啟用您的 APP


6. 在系統上的 Login URL 必須與 Facebook 的網址一樣(前面的 domain)
*http://domain0.login.com/*

7. 管理者將申請後的帳戶 ID 及密鑰輸入於系統的 facebook 內的欄位中。


在回系統上設定 Facebook 的用戶 ID 及密鑰

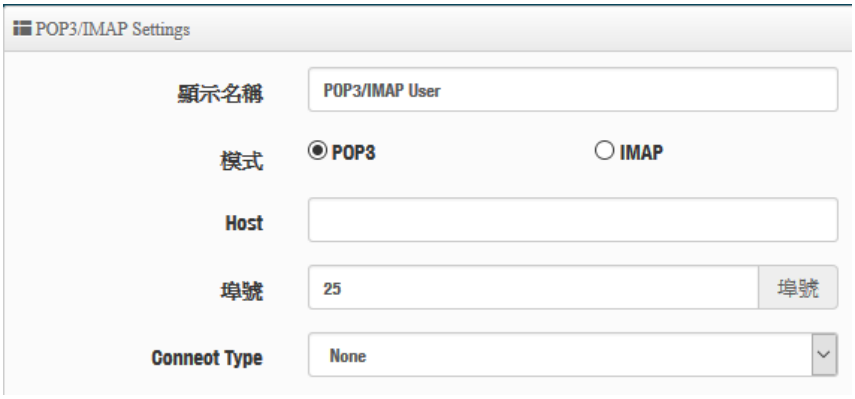

設定完成後，請點擊＂**儲存**＂按鈕後記得須點擊＂**重新啟動**＂，完成功能運作。

➢ **# PoP3/IMAP Server 認證**

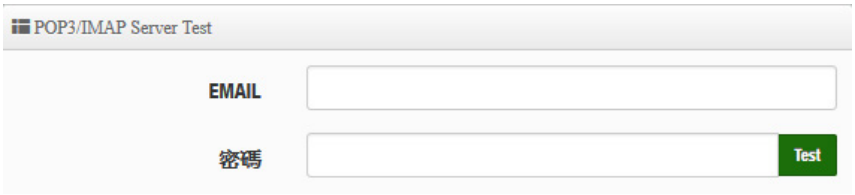
驗證帳戶可以指向 PoP3/IMAP 伺服器進行驗證



- **服務:** 管理員可以選擇啟動或關閉此功能



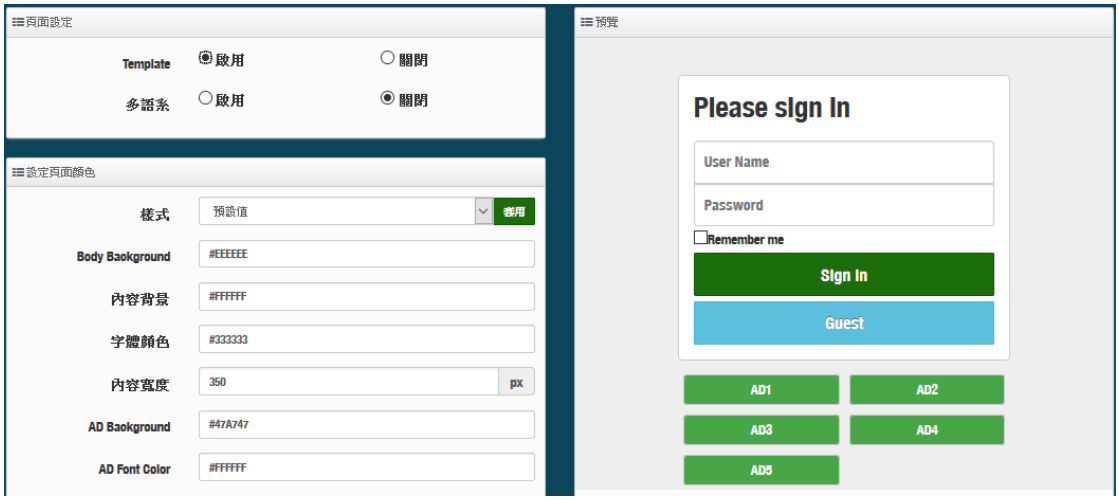

- **顯示名稱:** 管理人員可以自行定義此服務名稱。
- **模式：**選擇 Mail server 的驗證方式
- **Host：**輸入 Mail 伺服器的位址
- **埠號：**輸入 Mail 驗證所使用的埠號
- **Connect Type：**選擇 Mail 伺服器使用的加密類型




- **PoP3/IMAP Server Test:** 當以上資訊設定完成後，可透過此功能進行測試，驗證所設定的伺服器是否正常運作

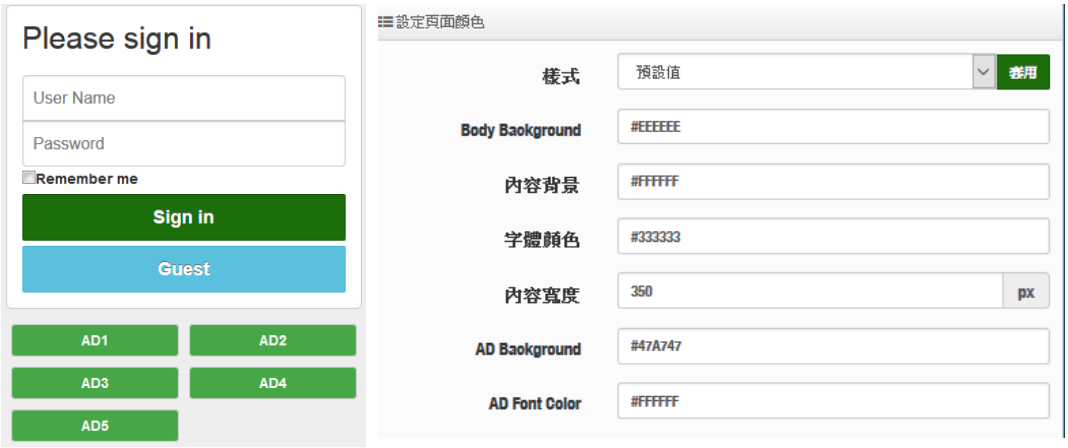
### 3.4.3 客製化頁面


這功能主要可以編輯系統內建的認證網頁登入頁面. 管理人員也可以透過 HTML 和 CSS 語法自行去客製化認證的登入頁面



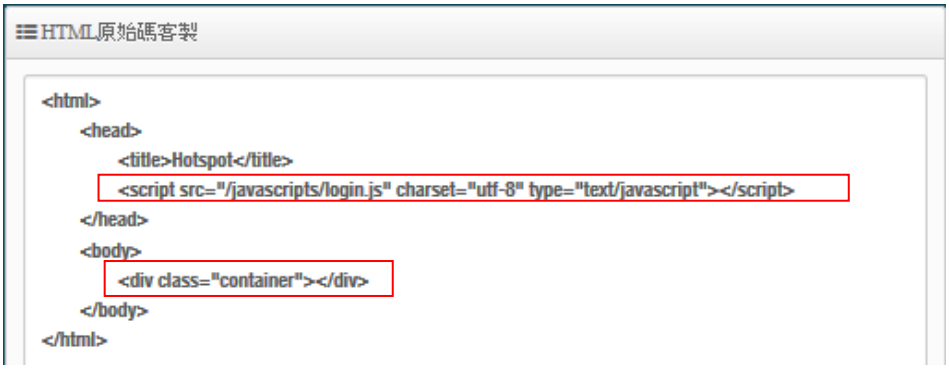

➢ **Template**：管理人員可選擇 Template(範本)啟用或關閉，啟用時可套用系統預設版面進行顏色修訂，若選擇關閉則可透過 html 語法做編輯

# 當選擇啟用則登入頁面將使用系統預設的格式.當關閉範本則會跳出 HTML 語法，可透過語法自行去編輯登入頁面

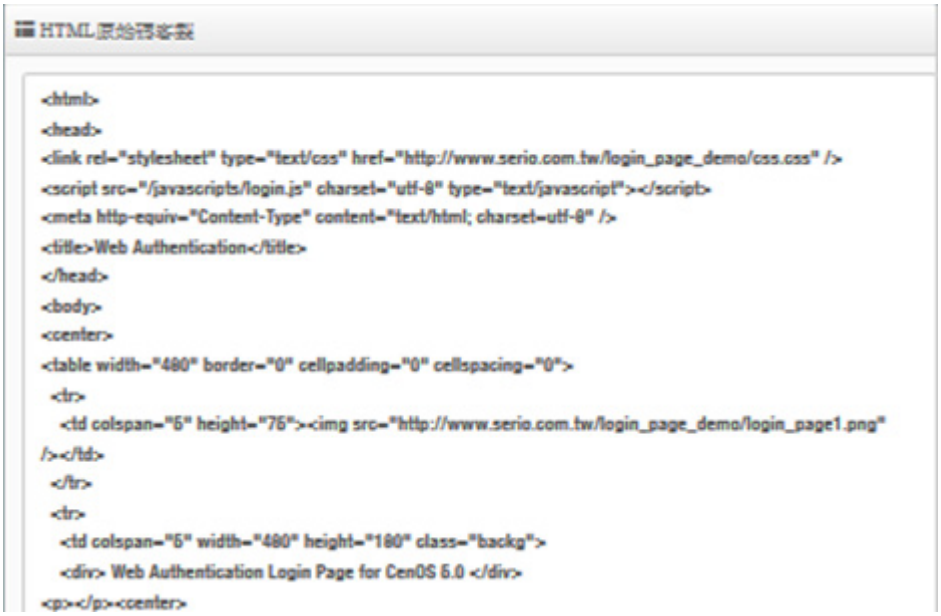



管理者可透過 html 的顏色語法設定頁面色彩及版型大小等

# 當選擇關閉，則欄位將跳出 HTML 原始碼客製欄位提供管理者去編輯




預設的原始碼紅色框框部分請勿刪除，其他部分則可透過 html 語法或 css 方式進行網頁編輯，如下範例:



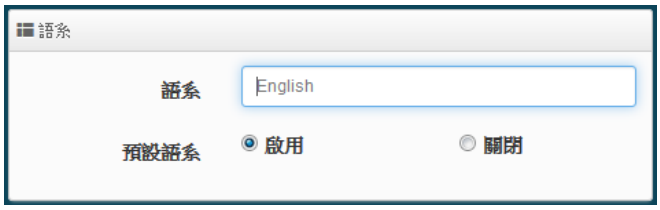

確認編輯完成後，請點擊**”儲存”**按鈕後即可點擊**”預覽”**按鈕”進行預覽所編輯的網頁


| Notice | 1. 本編輯 html 系統有一定的長度限制，同時也無法上傳圖檔至系統內，所以若有 CSS 語法或圖檔，建議先上傳至網站伺服器，透過超連結方式去連結圖檔<br>2. 在系統的 **Walled Garden** 功能必須增加上傳圖檔或 CSS 檔案的伺服器 IP 位址 |
|---|---|

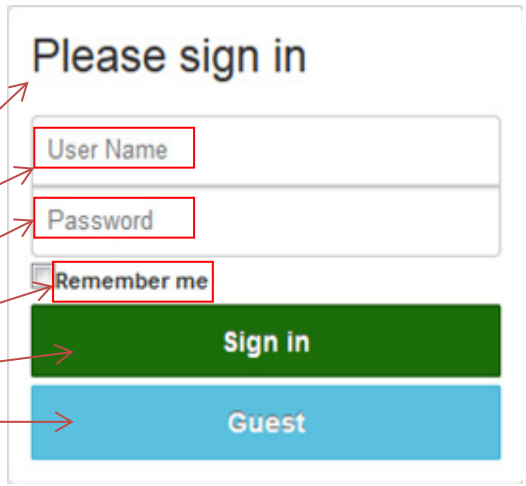
### 3.4.4 語系


此功能主要是若使用預設的登入頁面時，可以自行加入編輯出登入網頁需認證所顯示的語系，依照需求顯示不同語系，預設為英文


➢ **建立新的語系**：點擊此按鈕可新增不同的語言顯示，如下說明




**語言設定比對參考說明**



如圖完成後所呈現畫面

### 3.4.5 Walled Garden


此功能是設定開放使用網站，當使用者連接 AAP 模式的無線基地台後，若有開啟網頁認證登入功能如(2.2.3 啟用認證功能)時，則無線連接的使用者還未登入認證頁面，所有的使用者都可以使用此 Walled Garden 功能所設定的網站。


- **顯示名稱:** 設定要辨識的網站名稱
- **IP 網址/網域:** 設定網站的 IP 位址或網域名稱(例如 www.cerio.com.tw)
- **Full URL:** 設定網站的 URL 網址

如下範例

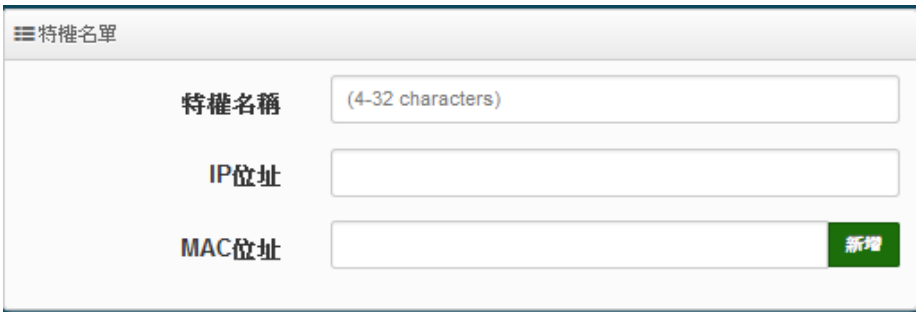

**按下新增後，將所設定的網站列入表單內**


表單內最多可建置 10 筆網站名單

當設定完成後請點擊**"新增"**按鈕，確認後記得 " **重請啟動** " 系統來完成作業程序

### 3.4.6 特權名單


此特權名單功能主要是當開啟網頁認證功能後，所有的無線使用者連接 AP 的無線基地台後都必須透過網頁認證方可使用網路，而在此特權名單內綁定 IP/MAC 位置的設備則不需經過網頁認證就能自由的使用上網服務。



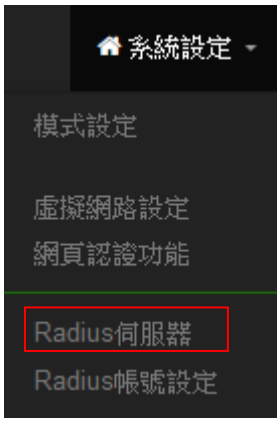

- **特權名稱:** 輸入設備的名稱來辨識使用者。
- **IP 位址:** 輸入設備所使用的 IP 位址。
- **MAC 位址:** 輸入設備所使用的網卡卡號(MAC)位址。

當設定完成後點擊”新增”按鈕來完成設定，確認後記得重新啟動系統讓功能正常運作

### 3.4.7 設定檔


此功能主要能將以設定好網頁登入的設定值原始碼等資料備份出至 PC，同時也能從 PC 再回存至系統

## 3.5 RADIUS 伺服器



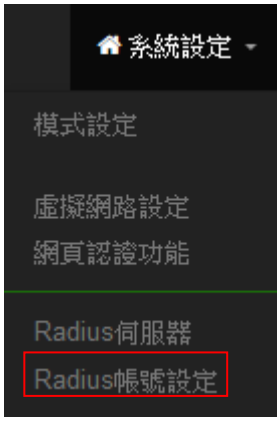

Notice 此功能只支援在**"無線基地台模式"**下運作

在無線基地台模式下系統已內建標準的 RADIUS 伺服器，且為了讓管理者輕鬆就能架設完成一台 RADIUS 伺服器，已將複雜的架設規則全部由系統自行完成，管理者只要啟用功能則就完成架設一台標準的 RADIUS 伺服器。


- **服務**：可選擇啟用或停用 RADIUS 伺服器
- **Radius 埠**：在標準的 Radius 伺服器預設都是使用的是 1812 埠，若無特殊應用建議無須修改
- **Radius 密鑰**：輸入此伺服器的登入密鑰

設定完成後，記得重新啟動系統讓功能正常運作

## 3.6 RADIUS 帳戶設定



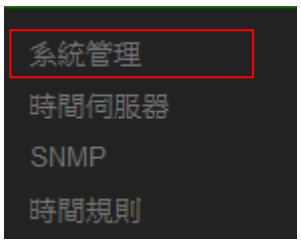

Notice 此功能只支援在**"無線基地台模式"**下運作

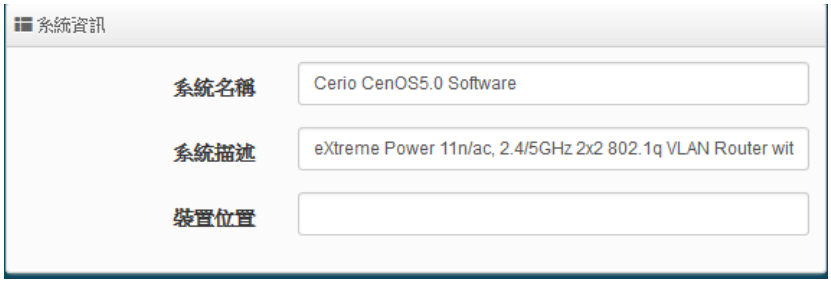
當啟用 RADIUS 伺服器後，則 RADIUS 的認證帳戶可在此新增建立。帳戶最多可建置 50 筆認證用戶。


- **使用者名稱**：建立用戶的使用帳號。
- **密碼**：輸入帳號的密碼。
- **匯出使用者檔案**：當建立多筆帳戶後，可利用此功能將帳戶備份匯出，儲存至電腦。
- **從 PC 匯入**：當帳戶匯出的檔案，可透過此功能重新匯入。
- **Radius 列表**：列出所有建立的帳戶名單。

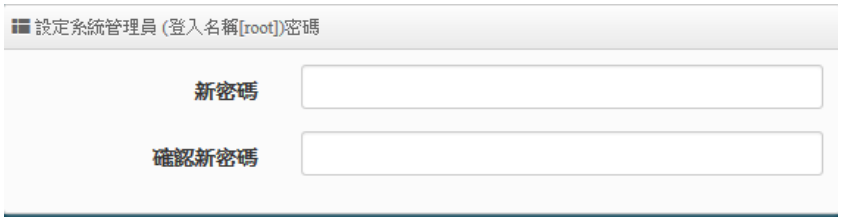
設定完成後, 記得重新啟動系統讓功能正常運作

## 3.7 系統管理




- **系統名稱**：管理者可以在此輸入預設的系統名稱。
- **描述**：請在此輸入系統的描述說明文字。
- **裝置位置**：管理可以在此輸入目前 **AP** 的安裝位置等資訊，讓網路管理員在管理時可以輕鬆辨識裝置所在位置。
- **系統管理員登入密碼 :**帳號為 root 可修改登入系統的密碼。

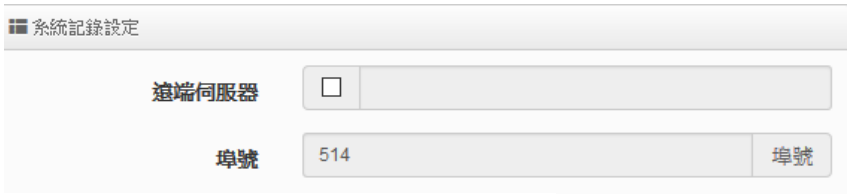


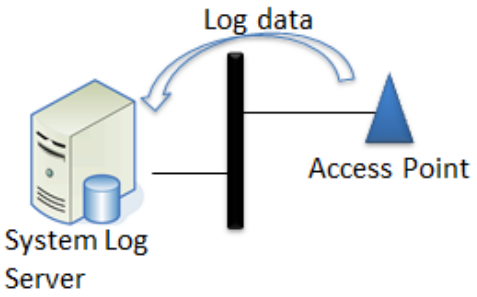

- **LED 控制**：管理者可啟用或關閉 AP 系統在執行工作時的 LED 閃燈狀態。


- **管理員介面登入設定**：管理這可以選擇登入管理頁面方式。

- **開啟 HTTP 管理**：勾選此項目將可以啟動 WEB 介面進入管理介面。預設為 80 埠，建議您使用 1025 ~ 65535 之間的埠號。
- **開啟 HTTPS 管理**：勾選此項目將可以啟動 WEB 介面進入管理介面。預設為 443 埠，建議您使用 1025 ~ 65535 之間的埠號。
- **開啟 Telnet 管理**：勾選此項目將可以啟動 Telnet 進入管理介面。預設為 23 埠，建議您使用 1025 ~ 65535 之間的埠號。
- **開啟 SSH 管理**：勾選此項目將可以啟動 SSH 進入管理介面。預設為 22 埠，建議您使用 1025 ~ 65535 之間的埠號。

➢ **系統紀錄設定**：假若架構環境中有一台系統紀錄伺服器，此功能可以指向到系統伺服器上，將本機的系統資訊檔往伺服器上備存，方便管理者未來除錯用。




- **遠端伺服器**：設定遠端系統資料伺服器的 IP 位址。
- **埠號**：設定遠端系統資料伺服器的埠號，預設為 514。

➢ **自動重新啟動**


- **Daily**：規劃每日固定時間重新啟動系統
- **每週**：規劃每週日期及時間重新啟動系統
- **每月**：規劃每月日期及時間重新啟動系統

## 3.8 時間伺服器


請點選「**系統設定**」→「**時間伺服器**」進入設定頁面，在系統時間為了能夠正確取得標準時間並確實的紀錄各項資訊所發生的時間點，故建議選擇 NTP 伺服器更新，透過網際網路的方式與網際網路上的時間伺服器進行時間同步作業。


- **目前本地端時間**：此欄位顯示出目前系統的時間。
- **模式**：可設定使用網際網路 NTP 伺服器即時線上更新時間，或是可用手動方式直接抓取 PC 的時間，也可以透過選擇欄位自訂日期與時間。

Notice

1. 當使用手動更新時間後，若系統重新啟動，則時間將會回到預設時間。
2. 若是使用 NTP 伺服器更新，而系統時間一直無法正確顯示目前時間，建議您重新檢查您的**網路設定**以及您的**時區設定**是否正確。或確認 AP 的 DNS 伺服器設定是否輸入正確 IP 位址

設定完成後，請點擊 " **儲存** " 按鈕後記得須點擊 " **重新啟動** " ，完成功能運作。

## 3.9 SNMP


請點選「**系統設定**」→「**SNMP**」進入 SNMP 設定頁面，此頁面功能將可設定 SNMP V2c 版, V3 版及 SNMP Trap 等功能，管理者可以依照實際需求開啟或關閉，請在欄位中輸入正確的 SNMP 資訊以便您的 SNMP 代理程式可以取得正確的系統資訊。


**SNMP V2c**

- **啟動**：啟動或關閉 SNMP v2c 支援。
- **RO Community**：您可以在此設定一組密碼給只能讀取的管理人員使用。
- **RW Community**：您可以在此設定一組密碼給可以讀取和寫入的管理人員使用。


**SNMP V3**

- **啟動**：啟動或關閉 SNMP v3 支援。
- **RO Username**：管理者可以在此設定一組帳號給只能讀取的管理人員使用。
- **RO Password**：管理者可以在此設定一組密碼給只能讀取的管理人員使用。
- **RW Username**：管理者可以在此設定一組帳號給可以讀取和寫入的管理人員使用。
- **RW Password**：管理者可以在此設定一組密碼給可以讀取和寫入的管理人員使用。


**SNMP Trap**

SNMP Trap 功能可以利用本機無線基地台內建的代理程式，將 SNMP Trap 訊息主動告知遠端 SNMP 監控主機，讓遠端啟動 SNMP 監控主機可以即時的知道目前本機無線基地台的最新狀態。

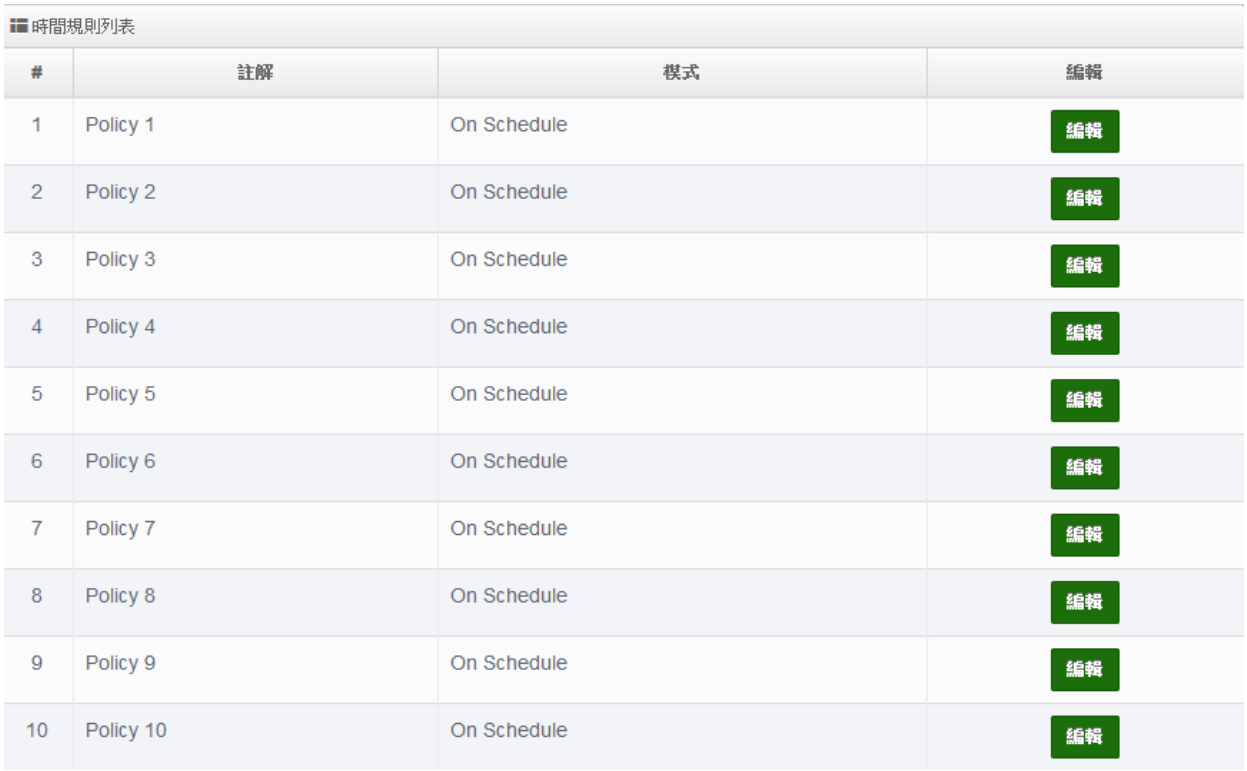
- **啟動**：您可以在此選擇啟用 SNMP Trap 功能。
- **Community**：請輸入一組字串讓遠端 SNMP 監控主機與本機無線基地台進行身份驗證用。
- **IP 1～4**：請輸入遠端啟動 SNMP 監控程式的主機 IP 位址。

設定完成後，請點擊 " **儲存** " 按鈕後記得須點擊 " **重新啟動** " ，完成功能運作。

## 3.10 時間規則


管理人員可設定時間排成，當設定好時間排成之規則後，可套用至相關功能進行定時的執行功能應用。共可設定 1~10 組時間規則

請點擊 " 系統設定 " ➔ " 時間規則 " 進入規則設定列表，在列表上點擊 " **編輯** " 按鈕進入時間設定頁面

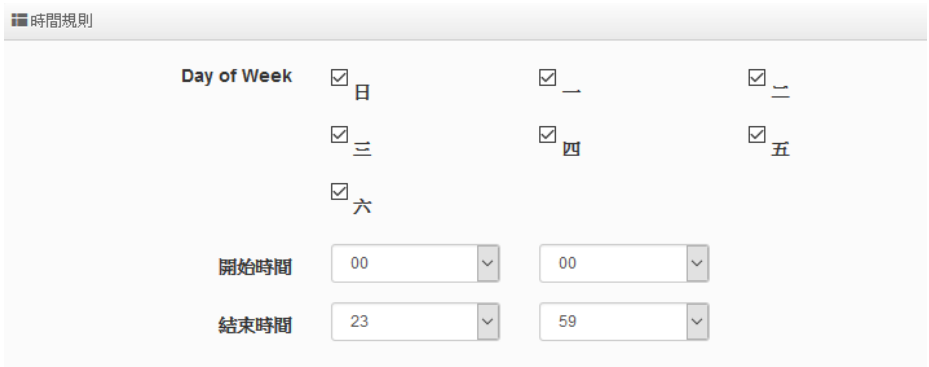




**模式:**

- **依照時間表:** 系統將依照所設定的時間執行。
- **依照時間表之外:** 表示排除所設定的時間表內不執行


- **建立新規則:** 當管理者點擊建立新則按鈕，則可進入設定時間表，可建置多個時間點。




設定完成後，請點擊 " **儲存** " 按鈕後記得須點擊 " **重新啟動** " ，完成功能運作。

# 4. [ 無線設定 ]

此功能選單將依照不同模式有所差異, 請確認所需的應用模式(可參考 2.2 操作模式設定及說明)

## 4.1 Radio 0 (2.4G 頻段)


- **MAC 位址 ：** 顯示 2.4G 無線 MAC 的位址。
- **區域設定：**使用者可設定符合該設備安裝國家之區域，支援「US」、「ETSI」、「Taiwan」
- **無線運作模式：**支援 802.11b , 802.11 b/g , 802.11b/g/n, 802.11n 四種模式，使用者可依需求選擇。
- **自動頻道：**啟用時系統將自動搜尋良好的頻道進行連線，關閉時管理者可依照自己環境需求手動調整。
- **頻道：**會依照法規在不同地區不同無線運作模式有不同的頻道選擇，可配合延伸頻道功能，選擇往上或往下頻道
- **無線傳輸功率設定：**
  使用者可依所在環境需求設定”等級 1” ~ ”等級 9”傳輸功率，最大為等級 9 ，依照不同的環境需求可自行調整降低或提高輸出功率，預設為”等級 9”。

### HT Physical Mode

- **TX/RX Stream**：出廠預設值為 2 傳送及 2 接收。
- **頻道模式**：使用 2.4Ghz 為 20Mhz 或 20/40Mhz，作為基地台與無線用戶之間傳輸的資料速度。
- **延伸頻道**：訊號延伸設定，可向上或向下延伸。
- **MCS:** MCS 編譯是 802.11n 在 WLAN 的通訊速率上提出的一種表示。而 MCS 編譯值將影響通訊速率的主要因素，在 MCS 值是與頻道頻寬做相對應，在 MCS 對應速率表上若以頻道頻寬為 20 時，則最高速率可達 150Mbps，假若頻道頻寬為 40 時，則最高速率將可達到 300Mbps，而最高速率將取決於單向或雙向的流量(Stream)
- **Short Gi :** 短保護間隔，無線信號在空間傳輸會因多方傳輸等因素在接收時造成延遲，如果後續數據發送過快，會和前一個數據形成干擾，而 Guard Interval 就是使用來減少並規避干擾的一項功能，出廠預設值為「啟用」。
- **封包聚合**：將多個封包合而為一，一起傳送出去。主要還是減少大量封包傳輸時，控制封包過量，出廠預設值為「啟用」。

設定完成後，請點擊 " **儲存** " 按鈕後記得須點擊 " **重新啟動** " ，完成功能運作。

## 4.2 Radio 1 (5G 頻段)

| Notice | 並非每個產品都支援 5G 頻段，請確認產品規格書說明是否有支援 |
|---|---|


- **MAC 位址**：顯示 5G 無線 MAC 的位址。
- **區域設定**：使用者可設定符合該設備安裝國家之區域，支援「US」、「ETSI」、「Taiwan」
- **無線運作模式**：主要可以選擇 802.11a / 802.11an / 802.11n(5G)/及最新的 802.11ac 等
- **自動頻道**：啟用時系統將自動搜尋良好的頻道進行連線，關閉時管理者可依照自己環境需求手動調整。
- **頻道**：會依照法規在不同國家地區不同無線運作模式有不同的頻道選擇

Notice

根據 NCC 釋出的資料，台灣開放下列 3 個 5GHz 頻段：

1. 5280 ~ 5350MHz（CH56 5280MHz、CH60 5300MHz、CH64 5320MHz）
2. 5470 ~ 5725MHz（CH100 5500MHz、CH104 5520MHz、CH108 5540MHz、CH112 5560MHz、CH116 5580MHz、CH120 5600MHz、CH124 5620MHz、CH128 5640MHz、CH132 5660MHz、CH136 5680MHz、CH140 5700MHz）
3. 5725 ~ 5825MHz（CH149 5745MHz、CH153 5765MHz、CH157 5785MHz、CH161 5805MHz、CH165 5825MHz）

其中 5470 ~ 5725MHz 這個頻段與軍方和氣象用都普勒雷達頻率相衝突，在軍方優先民間次之的邏輯下，若是要使用這些頻率，配合搭載啟動 DFS 和 TPC（EIRP 值大於 500mW 之設備）功能，當裝置感測到目前頻率有軍方其它人在使用時，DFS 會自動能夠跳開改採其它頻率； 5250 ~ 5350MHz 開放室內使用。(台灣相關規範可上 NCC 搜尋「低功率射頻電機技術規範」)

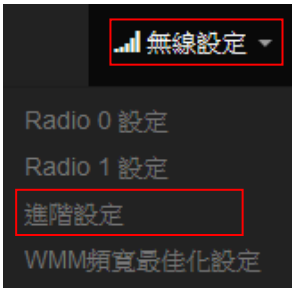
- **無線傳輸功率設定：**使用者可依所在環境需求設定”等級 1” ~ ”等級 9”傳輸功率，最大為等級 9 ，依照不同的環境需求可自行調整降低或提高輸出功率，預設為”等級 9”。

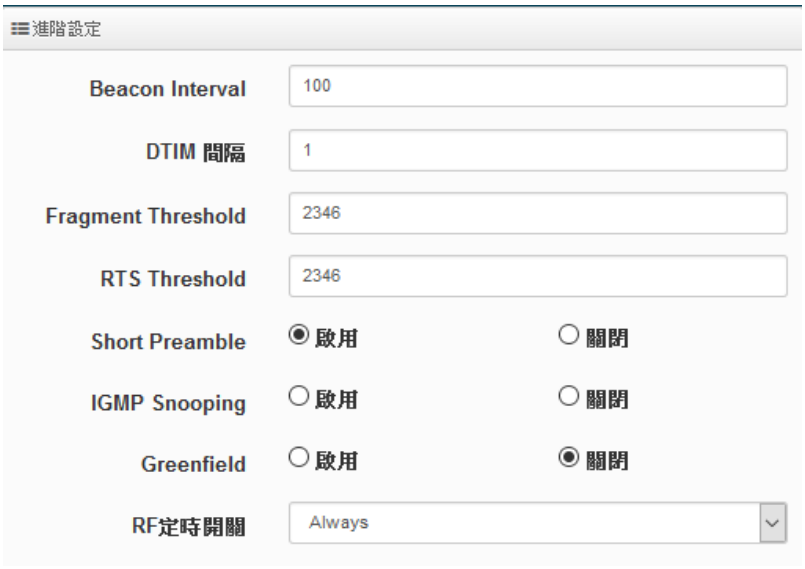
### HT Physical Mode


- **TX/RX Stream：**出廠預設值為 2 傳送及 2 接收。
- **頻道模式：**使用 20Mhz /40Mhz/或 802.11ac 的 80 作為基地台與無線用戶之間傳輸的資料速度。
- **Short Gi：** 短保護間隔，無線信號在空間傳輸會因多方傳輸等因素在接收時造成延遲，如果後續數據發送過快，會和前一個數據形成干擾，而 Guard Interval 就是使用來減少並規避干擾的一項功能，出廠預設值為「啟用」。
- **封包聚合：**將多個封包合而為一，一起傳送出去。主要還是減少大量封包傳輸時，控制封包過量, 出廠預設值為「啟用」。

設定完成後，請點擊 " **儲存** " 按鈕後記得須點擊 " **重新啟動** " ，完成功能運作。

## 4.3 進階設定



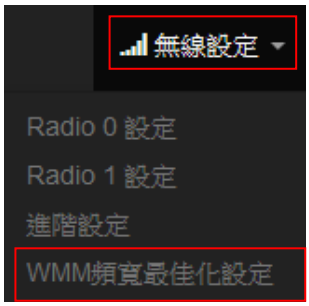




- **Beacon Interval**：輸入數值從 10 到 5000 msec，預設值是 100，輸入的數值越高，有助於無線用戶端省電，輸入的數值越低，連結無線網路的速度越快。
- **DTIM Interval**：輸入 DTIM Interval 數值，數值越高，用戶端網卡越省電，數值越低，效能越好，但也較不省電。
- **fragment threshold**：用來調整每個訊框大小，基本上訊框的值越大，在無線的傳送的穩定性相較高，預設值為 2346。
- **RTS Threshold**：輸入數值從 1 至 2346，無干擾的環境下，可設定越高數值，建議正常狀況下無需調整此設定。
- **Short Preamble**：使用者可點選啟用設定 56-bit 改善傳輸效能，關閉則使用 128-bit。
- **IGMP Snooping :** 用來支援在 layer2 建立和維護 MAC 的 Multicast 地址表，以達到在 layer2 也進行 Mutlicast。
- **Greenfield(綠燈模式) :** 若整體無線環境下都是使用 802.11n 模式下作運行，則可啟動綠燈模式，讓所有 11n 標準的客戶端可以全速通行。
- **RF 定時開關:** 可套用時間政策讓系統自動啟動或關閉無線訊號。

| Notice | 若要使用時間政策讓系統自動開關無線訊號時，務必確認系統時間是正確，系統時間設定必須使用 NTP 校時，同時要確保無線基地台的系統能透過網際網路連線至 NTP 伺服器，以下注意幾個關鍵點設定<br>**1.** 虛擬網路設定必須設定正確的 Gateway. **2.** DNS 伺服器建議手動設定 IP 位置 |
|---|---|

設定完成後，請點擊 " **儲存** " 按鈕後記得須點擊 " **重新啟動** " ，完成功能運作。

## 4.4 WMM 頻寬最佳化設定




WMM頻寬最佳化設定

WMM頻寬最佳化 ◉ 啟用 ○ 關閉

WMM Parmameters of Access Point

| AC Type | CWmin | CWmax | AIFS | TxOp Limit | No ACK Policy bit |
|---|---|---|---|---|---|
| AC_BE(0) | 4 | 6 | 3 | 0 | ☐ |
| AC_BK(1) | 4 | 10 | 7 | 0 | ☐ |
| AC_VI(2) | 3 | 4 | 1 | 3008 | ☐ |
| AC_VO(3) | 2 | 3 | 1 | 1504 | ☐ |

WMM Parmameters of Station

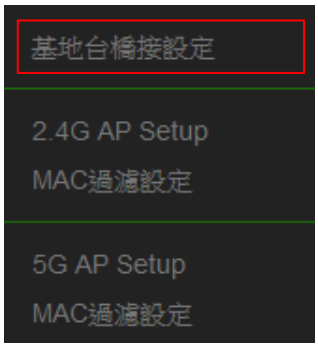
| AC Type | CWmin | CWmax | AIFS | TxOp Limit | ACM bit |
|---|---|---|---|---|---|
| AC_BE(0) | 4 | 10 | 3 | 0 | ☐ |
| AC_BK(1) | 4 | 10 | 7 | 0 | ☐ |
| AC_VI(2) | 3 | 4 | 2 | 3008 | ☐ |
| AC_VO(3) | 2 | 3 | 2 | 1504 | ☐ |

- **AC Type**：Access Category 的優先權區分為 Voice(VO), Video(VI), Best-effort(BE)及 Back-ground(BK)等四級。
- **CWmin**：Minimum Contention Window，這個數值會影響 WMM 存取類型的延遲時間。
- **CWmax**：Maximum Contention Window，這個數值會影響 WMM 存取類型的延遲時間，注意 CWMax 一值必須大於或等於 CWMin。
- **AIFS**：Arbitration Inter-Frame Spacing Number，這個數值可控制用戶等待每筆資料傳輸的時間。

- **TxOP Limit**：Transmission Opportunity，這個傳送機會，對於在資料傳輸中需要較高優先權的 AC_VI 與 AC_VO，您可以設定較大的數值以便取得較高的傳送優先權。
- **ACM bit**：Admission Control Mandatory，ACM 只適用於 AC_VI 及 AC_VO,當這個功能沒有被選取時,則由連接中的無線基地台來負責 ACM,反之 ,當這個功能被選取時,則由用戶端來負責。
- **No ACK policy bit**：不選取時，表示無線基地台透過無線連線傳輸 WMM 封包時，將會回應傳輸需求，可確保對方一定收到 WMM 封包。選取時，表示無線基地台透過無線連線傳輸 WMM 封包時，不會回應任何傳輸需求，成效雖然較好但是可靠性較低。

設定完成後，請點擊 " **儲存** " 按鈕後記得須點擊 " **重新啟動** " ，完成功能運作。

## 4.5 基地台橋接設定

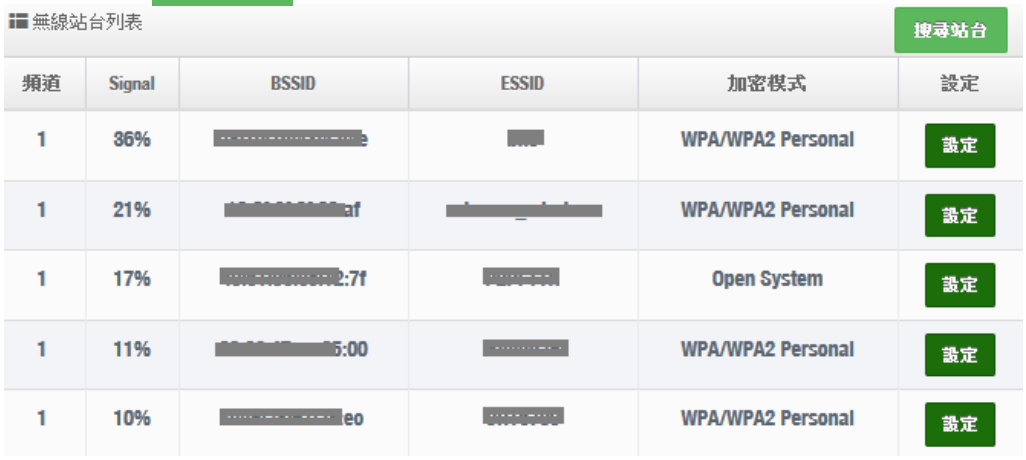



Notice 此功能僅支援 Client Bridge / WISP 模式下運作

可點選**"搜尋站台"**按鈕選擇欲想要連接的無線基地台，找到要連接的無線站台後點擊 " **設定** " 按鈕, 則可設定要橋接地無線站台資訊，如設定連接密碼等。
建議管理人員手動方式設定 SSID 名稱及加密方式。

搜尋無線站台請先點擊 **搜尋站台** 按鈕，再找出環境中要連接的無線基地台，確認後點擊 " **設定** " 按鈕即可以在右邊欄位輸入連接密碼，確認完成後點擊 " **儲存** " 按鈕並重新啟動系統即可完成連接

- **點擊** **搜尋站台** ：開始尋找環境中的無線基地台，並列表。




- **頻道**：顯示無線基地台的使用頻道。
- **Signal**：顯示目前與無線基地台的訊號強度，百分比越高訊號接受強度越好。
- **BSSID**：顯示環境中無線基地台的名稱。
- **ESSID**：顯示基地台名稱。
- **加密模式**：顯示基地台的認證加密方式。
- **設定**：點擊可選取要連線的無線基地台，並設定連線密碼

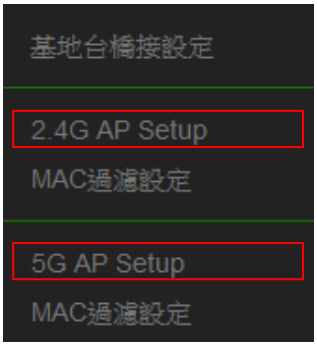
**基地台橋接連接設定**：當管理人員點擊無線站台列表的設定按鈕後，該無線基地台資訊將顯示此欄位。假若管理者已確認無線站台名稱與密碼，可不需透過搜尋站台功能，管理者可手動輸入已知的 SSID 名稱及密碼至欄位即可。


- **SSID 名稱:** 若再搜尋站台列表上所搜尋出來的站台後點擊設定後, SSID 名稱將自動套用此欄位, 管理者也可以手動自行輸入已知的 SSID 名稱。
- **加密類型：顯示站台的加密類型，管理者也可手動自行選擇。**


- **密碼設定**：可選擇無線基地台的加密模式及密碼演算方式，並輸入連接無線基地台的正確密碼。管理者必須手動正確的輸入加密模式/演算方式及 SSID 密碼
  - **加密模式**：選擇無線基地台的加密模式。
  - **加密演算法**：選擇無線基地台加密模式的演算法。
  - **金鑰**：輸入無線基地台的連接密碼。

設定完成後，請點擊 " **儲存** " 按鈕後記得須點擊 " **重新啟動** " ，完成功能運作。

## 4.6 2.4G / 5G AP Setup (訊號再延伸)



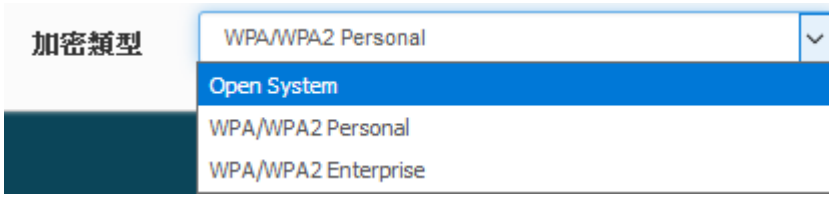

此功能應用主要是 2.4G/5G 的訊號再延伸(Repeater)功能，可參考 *2.2 項的操作模式設定及說明之應用圖解*

| Notice | 此功能僅支援 Client Bridge / WISP 模式下運作 |
|---|---|

當基地台橋接成功(Client Bridge)確認已經與上端 AP 連接後，則可以選擇啟用此 2.4G 和 5G 訊號延伸功能或停用延伸基地台功能 ，選擇啟用後設備將成為無線基地台讓訊號延伸再提供給使用者連接。

| Notice | 基地台橋接與訊號延伸為父子關係，所以假若 Client Bridge(基地台橋接)不成立，則延伸基地台功能將無法使用 |
|---|---|


- **無線基地台**：關閉或啟用 Repeater AP(延伸基地台)功能服務。
- **SSID 名稱**：設定 Repeater AP(延伸基地台)的 SSID 名稱。
- **可視 SSID**：設定啟用或關閉 Repeater AP(延伸基地台)的 SSID 名稱是否要隱藏。
- **隔離無線使用者**：設定是否要隔離 Repeater AP(延伸基地台)下的無線使用者。也就是說無線用戶端依然可以正常連線 Internet，但無線使用者與無線使用者之間是無法溝通連線。
- **連線限制**：設定無線基地台的 SSID 最大可連線的無線使用者數量，預設最大支援同時 64 個使用者存取同一個 SSID。*建議若使用 2.4G 頻段最高連線人數 40 人以下，若使用 5G 頻段最高連線人數 60 人以下。*
- **認證** ：管理者可設定 WPA-PSK/WPA2-PSK Personal 和 WPA/WAP2-Enterprise 等認證模式。



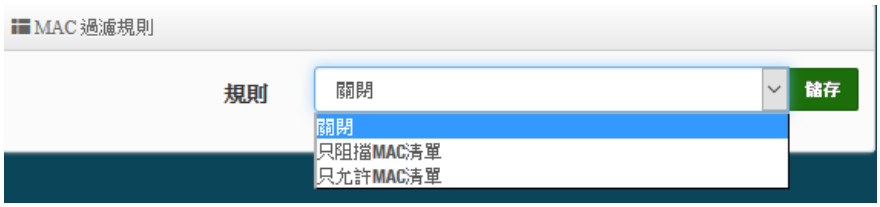

設定完成後，請點擊 " **儲存** " 按鈕後記得須點擊 " **重新啟動** " ，完成功能運作。

## 4.7 MAC 位址過濾


Notice 此功能僅支援 Client Bridge / WISP 模式下運作

點選「MAC 過濾設定」將可以進入設定頁面。過濾規則可分為兩部分，分別是：

1) 只阻擋 MAC 表單內的位址連線，其他設備將可以連接無線基地台。
2) 只允許 MAC 表單內的位址連線，其他設備將無法連接無線基地台。

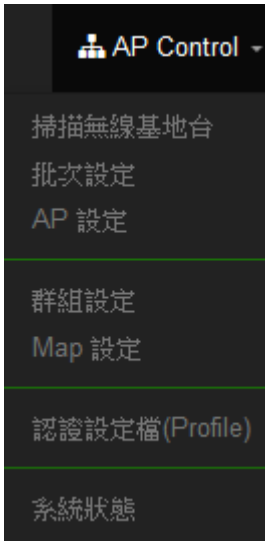




- **規則**：可選擇關閉過濾 / 開放或阻擋 MAC 的表單位址。
- **MAC 位址**：輸入要管理的 MAC 位址。
- **MAC 位址列表**：當建置設備的 MAC 位址後，將列入表單內。

設定完成後，請點擊 " **儲存** " 按鈕後記得須點擊 " **重新啟動** " ，完成功能運作。

# 5. [ AP Control ]




Notice 此功能只在**"CAP 模式"**下運作

此 CAP 模式的 AP Control 的功能主要是控制管理所有 CenOS5.0 的 AP 模式之無線基地台。集中管理無線基地台功能包含能完整找出**網域中有架設 CenOS5.0 核心的基地台**、集中設定被管理 AP 之**批次設定**、**AP 功能設定**、**群組設定**、**Map**、**AP 認證設定檔**及被管理 AP 的**系統狀態**。

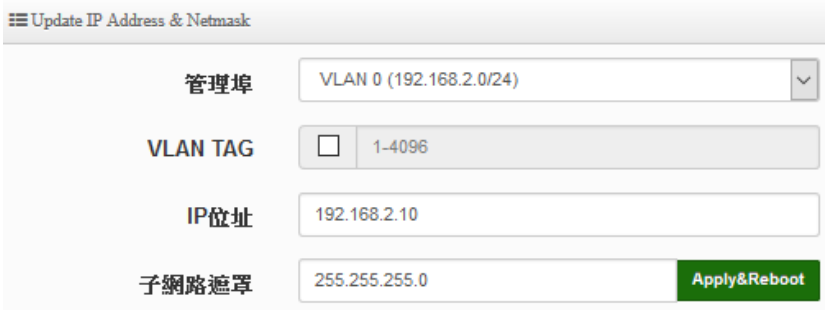
## 5.1 掃描無線基地台


使用此功能主要可以尋找整個網路環境下所有使用 CenOS5.0 軟體的 AP 無線基地台，當確認被尋找出來的 AP 將能一次性的去設定所有 AP 的 IP 位址、閘道位址等，當所有被管理的無線基地台的 IP 為位址都分配完成後，確認即可匯入資料庫進行集中管理無線基地台，同時也能將 AP 還原出廠預設值

初次集中管理步驟說明:

1. 先確認 CAP 模式下的系統 IP 位址不可與被管理的 AP 之 IP 位址有衝突，例如 Cerio 預設出廠 AP 的 IP 位址是 192.168.2.254，所以此 CAP 模式下的系統 IP 位址可設定 102.168.2.2
2. 將所有要管理的 CERIO AP 全部接上同區域網路後，按下偵測掃描按鈕，控制器將進行偵查整個區域網路內的 Cerio AP

3. 掃描完成後 Cerio 的 AP 將全部進入清單內，開始設定每一台被管理 AP 的系統 IP 位址(預設每一台都是 192.168.2.254)，在清單內勾取全選並在 Update IP Address & Netmask 欄位設定起始 IP 位址，系統將會依照起始 IP 位址遞增上去，例如起始 IP 位址是 192.168.2.10，則會從 10,11,12….一直新增上去修改所有 AP 的 IP 位址

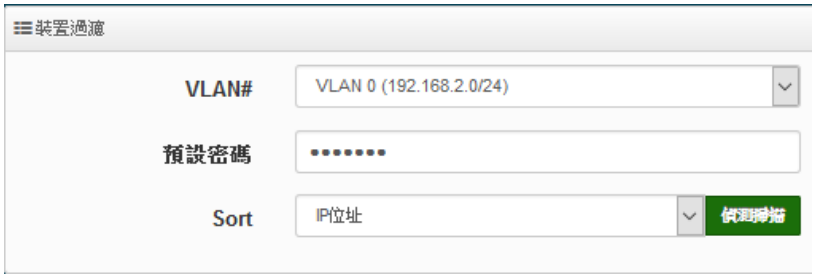



4. 按下 Apply&Reboot 按鈕，所有被管理 AP 將會被儲存 IP 位址並自動重新啟動 AP 設備

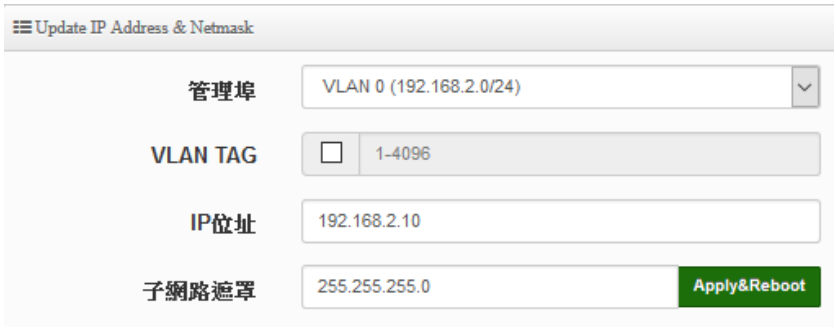
5. 等待約 1 分鐘後，重新再掃描一次被管理 AP 後，在清單內將發現所有被管 AP 的 IP 位址已經全部被改變

6. 在清單表內勾全選，並按下 匯入 按鈕，將全部的被管理 AP 全會入資料庫進行集中管理

詳細功能說明如下說明




- **LAVN**：選擇要掃描的區域網段，若環境中有設定多組 VLAN 網路，則此選項將會依造**"3.2 虛擬網路設定"**所啟用的 VLAN 做選擇。
- **預設密碼**：當網路環境中所有 ConOS5.0 被管 AP 的系統登入密碼有修改過，則此欄位則須輸入被修改過的密碼。(預設值為 default)
- **Sort**：可選擇 IP 位址排序或是 MAC 位址排序




- **管理埠**：可選擇 AP 要切換至某特定 VLAN 下做管理
- **VLAN Tag**：若 AP 是架設在 VLAN Tag 環境下，可在此設定 Tag ID。

- **IP 位址**：設定多台被管理無線基地台的 IP 位址時，此功能 IP 位址將會遞增上去到所有的被管理無線基地台上。
- **子網路遮罩**：設定被管理無線基地台的網路遮罩。


- **Device**：可勾選欄位上的所有被管理的無線基地台，或單一的無線基地台。
- **IP 位址**：顯示目前已掃描到被管理無線基地台 IP 位址。
- **MAC 位址**：顯示目前已掃描到被管理無線基地台 MAC 位址。
- **密碼**：可在欄位上單獨修改被管理無線基地台的密碼。
- **Host Name**：顯示目前已掃描到被管理無線基地台的系統名稱。
- **F/W Version**：顯示目前已掃描到被管理無線基地台的韌體版本。
- **F/W Date**：顯示目前已掃描到被管理無線基地台的韌體釋出日期。
- **IP 位址**：可單一修改已掃描到被管理無線基地台的 IP 位址。
- **子網路遮罩**：可單一修改已掃描到被管理無線基地台的子網路遮罩。
- **執行**：確認修改以上單一的無線基地台設定後，可按下儲存並重新啟動此被管的無線基地台設定將完成修改。

## 5.2 批次設定


此頁面主要是集中控制管理 CenOS5.0 的 AP 模式無線基地台的無線功能，除了可以管理同時能強制更改整個被管理無線基地台所使用的模式，在這功能下可以整批集中管理無線基地台的群組管理/LVAN Tag 設定/IP 位址/設定檔套用/設定 Gateway 和 DNS 位址/被管理 AP 的系統時間/系統管理設定/無線的設定/無線進階設定/WMM 設定/韌體更新及重新啟動所有無線基地台等等。


- **VLAN**：選擇要管理特定 VLAN 下環境的 AP。
- **群組**：若在**"群組設定"**功能上，有規劃群組，此 VLAN 網段將可以選擇 AP 要歸納哪個群組上
- **批次設定**：主要設定所有被管理無線基地台的所有功能，包括 LAN/無線設定/網頁認證/系統等等。


- **虛擬網路設定**：設定被管理 AP 的 2.4G/5G 的無線訊號啟用或關閉、Tag ID、IP 位址等等功能
- **認證設定檔(Profile)**：若已經編輯完成**"5.6 認證設定檔"**功能，則可在此選擇套用。
- **Gateway & DNS**：設定被管理無線基地台的閘道器及 DNS 位址。
- **時間伺服器**：設定被管 AP 的系統時間。
- **系統管理設定**：設定被管 AP 的登入密碼、主機名稱、啟用日誌紀錄、登入管理的連接埠以及設定系動自動重新啟動功能等。
- **無線基本設定**：設定被管理 AP 的模式、頻道、輸出功率等等
  ***(請參考項目 4 無線設定)***, *依照不同產品型號所支援的功能進行設定, 其他不支援之功能可不理會*
- **無線進階設定**：設定被管理 AP 的無線進階功能***(可參考 4.3 進階設定的功能說明 )***
- **VAP 設定**：設定被管理無線基地台的 SSID 名稱，限制連線人數及加密等等
- **從 TFTP 伺服器升級韌體**：可透過 TFTP 伺服器做整批更新所有被管理 AP 的韌體
  ***(可參考 7.2 韌體升級的功能說明)***
- **從 HTTP 伺服器升級韌體**：可透過 web 伺服器做整批更新所有被管理 AP 的韌體
  ***(可參考 7.2 韌體升級的功能說明)***

- **重新啟動**：當所有被管理的 AP 都設定完成後，需在此進行所有被管理 AP 的系統重新啟動，才能完成修改設定檔


➢ **AP 設備列表**：顯示 VLAN 下的所有已經被管理 AP 的列表。當某特定 AP 或是全部 AP 要進行批次設定，請在此列表上勾選被管理的 AP

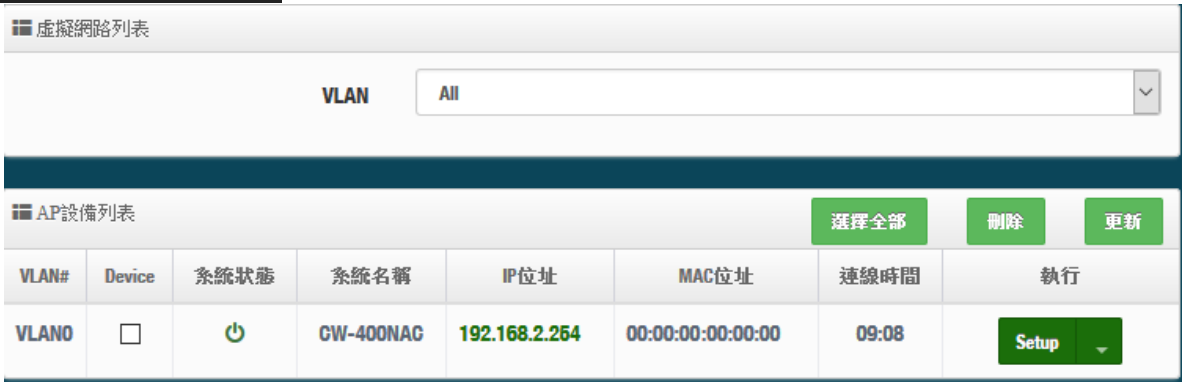
Notice

1. 每設定完成一項功能，必須在功能頁右上角的套用按鈕確實點擊套用才可生效，如下圖範例


2. 全部設定完成後一定要讓被管 AP 重新啟動

## 5.3 AP 設定


主要可以顯示 VLAN 下所有被管理 AP 的狀態是屬於離線還是上線，也能將特定的被管理無線基地台踢出管理等



- **VLAN#**：顯示被管理 AP 屬於哪個 VLAN 網域。
- **Device**：選擇特定的被管理 AP。
- **系統狀態**：顯示被管理 AP 目前是離線或在線。
- **系統名稱**：顯示被管理 AP 的系統名稱。
- **IP 位址**：顯示目前被管理 AP 的 IP 位址。
- **MAC 位址**：顯示目前被管理 AP 的 MAC 位址。
- **連線時間**：顯示目前被管理 AP 系統的啟動時間。
- **執行**：可以刪除被管理 AP 在管理資料庫名單，或修改被管理 AP 的 IP 位址及資訊等等。

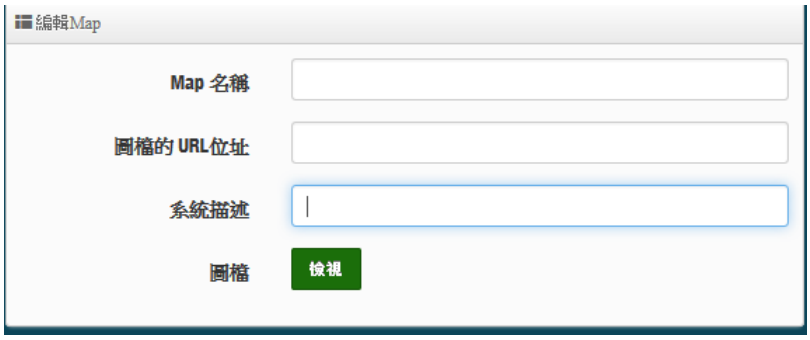
## 5.4 群組設定


此功能主要能在同一個 VLAN 下去建置多筆的群組，利用群組去管理特定的 AP

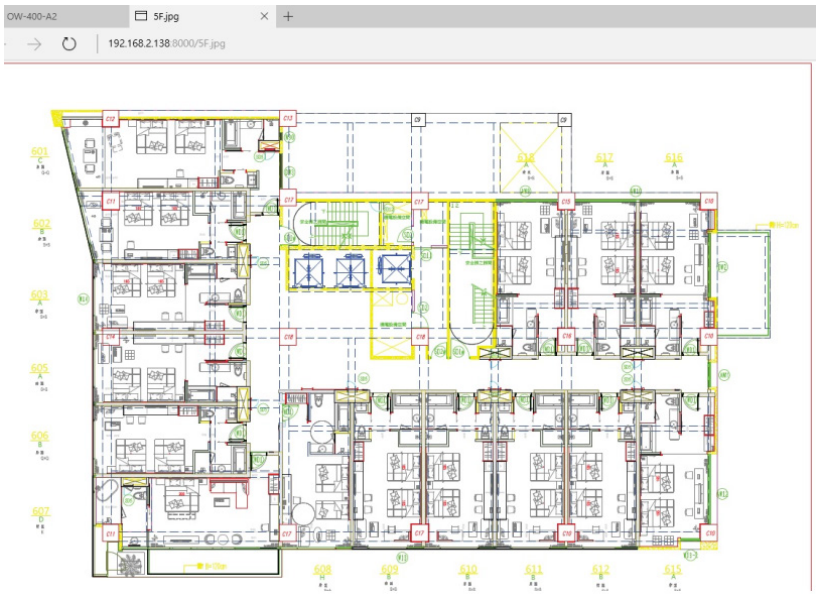

- **VLAN**：若有建置多組 VLAN，可在此選擇其他 VLAN
- **建立新群組**：此按鈕可以在一個 VLAN 下創建多個群組，方便利用群組去管理無線基地台
- **Device**：此按鈕將可以選擇被管理 AP 要納入特定群組

## 5.5 Map 設定


可放置平面圖，將所有的被管理 AP 的架設位置定位擺放，讓管理者可以透過位置圖知道特定的 AP 所架設的位置在哪個地方，方便管理。




- **Map 名稱：輸**入此地圖的代號名稱。
- **圖檔的 URL 位址：**圖檔需上傳到某 web 伺服器，之後將圖檔的 URL 位置輸入此欄位
- **系統描述：**輸入此圖檔的詳細描述。
- **檢視：**當確認 URL 路徑後可以點擊此按鈕，檢視圖檔是否正確。

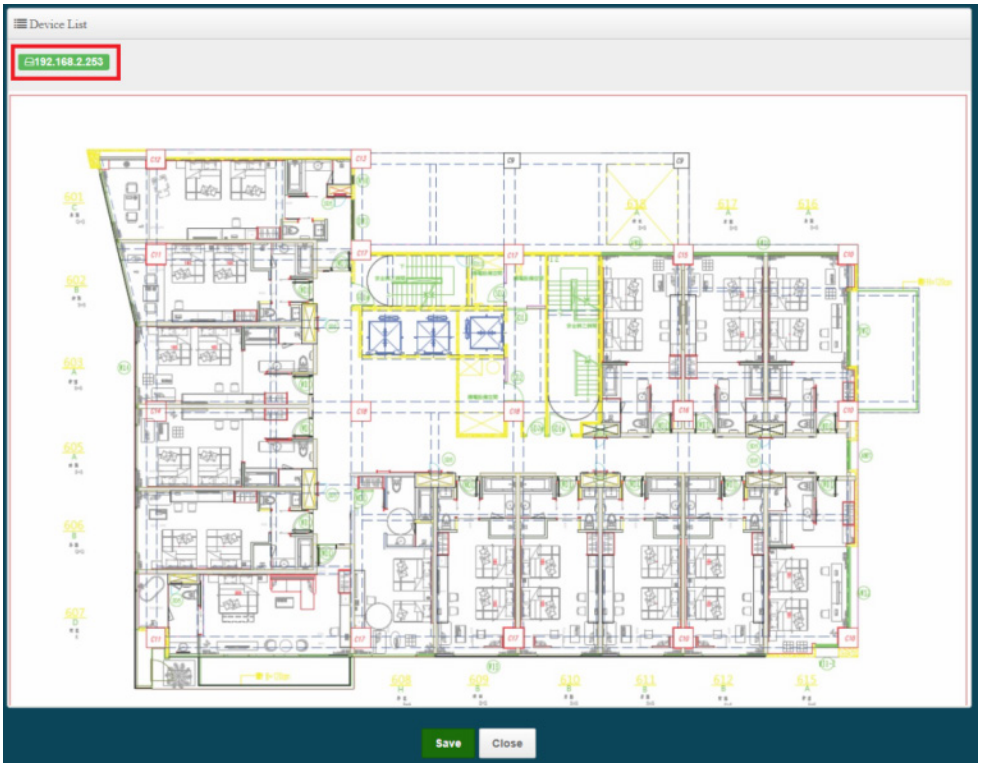



確認後點擊”儲存”按鈕儲存設定並將系統重新啟動讓地圖生效。

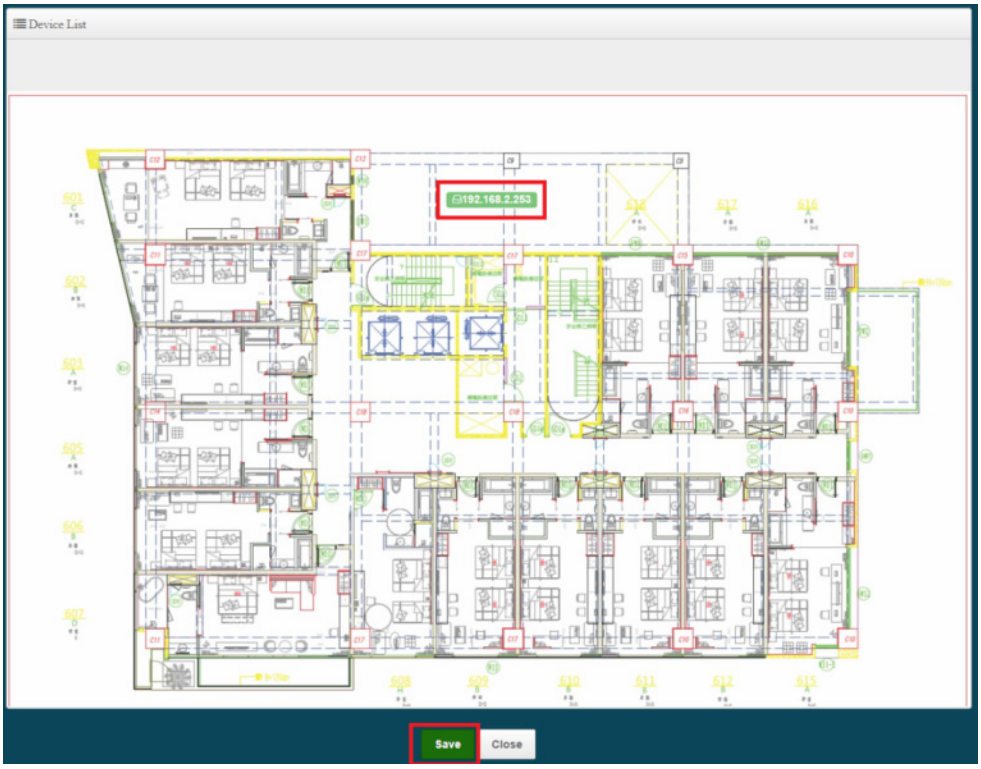
系統重新啟動後，Map 列表會出現剛剛儲存的地圖資訊。


點選下圖紅框所示的下拉式選單並點選”Layout”。


點選後將會出現地圖視窗，並在上方會出現 AP 圖示。

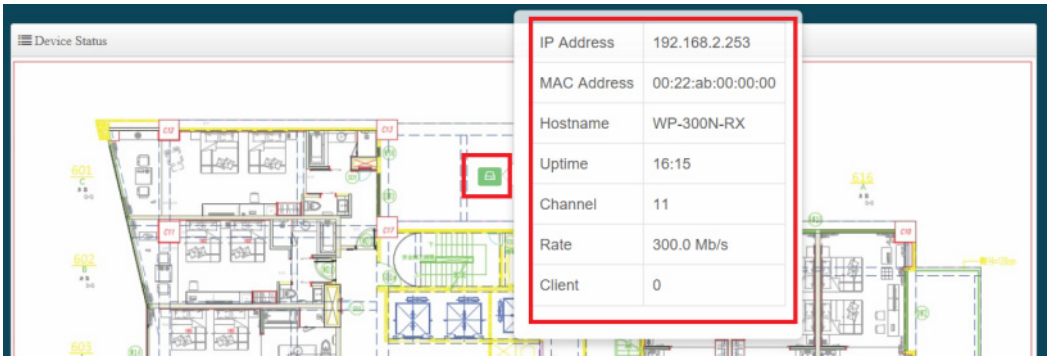



將 AP 圖示拖曳至地圖上欲設定的位置，完成後點選”Save”儲存設定再點選”Close”關閉視窗。




點選”檢視”按鈕，檢視地圖。


開啟地圖視窗後，將滑鼠移至地圖上的 AP 圖示後將會出現 AP 目前資訊。



## 5.6 認證設定檔(Profile)


當所有 AP 需要啟用網頁認證功能，而網頁認證的條件規則，可以先在此建立一個設定檔，完成後即可以在至 5.2 批次設定內去選擇套用。


**a:** 建立一個認證設定檔，名稱及描述等。

**b:** 顯示認證設定檔的名稱。

**c:** 顯示設定檔的描述。

**d:** 顯示此設定檔的網頁認證功能是否要啟用。

**e:** 編輯網頁認證的功能條件，當此條件設定後，在 5.2 批次設定就能去套用給多台被管理 AP 的設定值，讓所有的被管理 AP 的網頁認證條件，都使用此設定檔。

***(設定認證功能的說明，可參考 3.4 網頁認證功能)***

**f:** 可刪除此設定檔或修改這設定檔的名稱描述。

## 5.7 系統狀態


主要可以顯示每個 VLAN 底下所有被管理 AP 的狀態，並能詳細檢查每個被管理 AP 流量及無線使用者連線人數和相關資訊等。


- **VLAN#**：顯示被管理 AP 所屬的虛擬區域網路資訊。
- **系統狀態**：顯示被管理 AP 的運作狀態，是否離線或上線。
- **系統名稱**：顯示被管理 AP 的名稱資訊。
- **IP 位址**：顯示被管理 AP 的使用 IP 位址資訊。
- **連線時間**：顯示被管理 AP 的運作時間。
- **Radio information**：顯示被管理 AP 所啟用的頻率與頻道資訊。
- **接收**：顯示被管理 AP 所接收多少封包流量。
- **傳送**：顯示被管理 AP 所傳送出多少封包流量。
- **User(s)**：顯示被管理 AP 目前 Wi-Fi 連接人數。

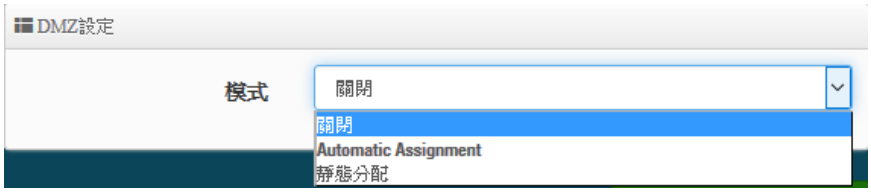
# 6. [ 進階 ]

本進階設定內容適用於 **WISP / Router 模式**，其他如 AP 模式、Client Bridge 模式、CAP 模式等非 NAT 功能的模式下將不支援以下之功能。

## 6.1 DMZ

DMZ (Demilitarized Zone)縮寫，DMZ 功能是在區域網路內另外在隔開一個特殊小區域，目的是希望在區域網路內的特定伺服器能給外部網路存取資料，且不允許外部網路偵測到內部其他非開放對外的伺服器，所以只要開放對外的伺服器放置 DMZ 區，讓外部連線只能限制讀取 DMZ 區域內的伺服器，可保護內部的區域網路不受外部連線的偵測，降低風險。

此系統設計 2 種 DMZ 類型，分別為 Automatic Assignment 及 Static Assignment 等。


- **Automatic Assignment**：讓所有外部的網路都能讀取 DMZ 內的伺服器所開放的服務。


  - **內部 IP 位址**：輸入要放置 DMZ 區域的伺服器 IP 位址。
- **靜態分配**：限制讓特定的外部 IP 位址可以連線到 DMZ 區域，其他外部 IP 位址將無法連線至 DMZ 區域。

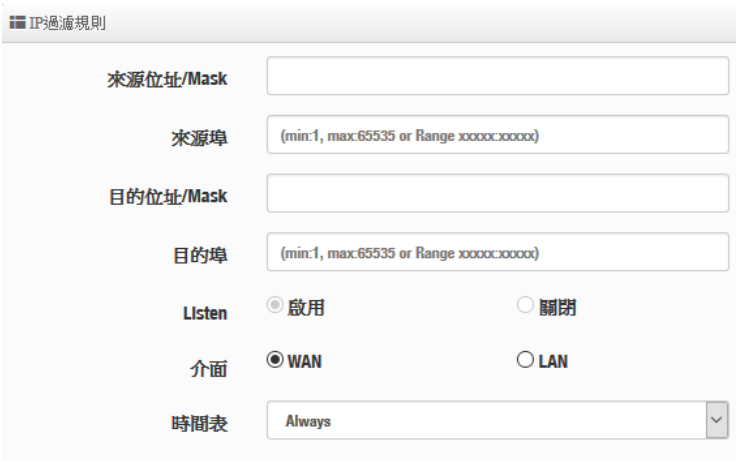

  - **外部 IP 地址**：輸入外部的 IP 位址。
  - **內部 IP 地址**：輸入要放置 DMZ 區的伺服器 IP 位址。

設定完成後，請點擊 " **儲存** " 按鈕後記得須點擊 " **重新啟動** " ，完成功能運作。

## 6.2 IP 過濾

管理者可以在此管理 WAN 到 LAN 或是 LAN 到 WAN 的 IP 流向及服務端口讀取控制，可增加網路安全機制。IP 過濾可建置 20 筆條件。


- **啟動**：管理人員可以啟動或關閉 IP 過濾條件。
- **註解**：管理人員可設定此條件的描述。
- **政策**：管理人員可設定此條件是要阻擋或是通行。
- **流入/流出**：管理人員可以選擇 IP 流向屬於流入或是流出。
- **通訊協定**：可選擇網路協定屬性。




- **來源位址/Mask**：設定來源端的 IP 位址及網路遮罩。
- **來源埠**：設定來源端的服務埠，可設定區間。
- **目的位址/Mask**：設定目的端的 IP 位址及網路遮罩。
- **目的埠**：設定目的端的服務埠，可設定區間。
- **Listen**：若選擇 TCP 則系統會強制監聽。
- **介面**：選擇條件執行的介面。
- **時間表**：是否要套用時間表進行自動執行或關閉條件。(可參考 3.10 項目時間規則)

**如下提供簡單設定範例:**

假設要阻擋某一個 IP 不能使用 80 Port(網站), 可設定如下即可完成阻擋

來源位址/Mask : 192.168.2.10/32 以及來源埠: 設定全部(1:65535)

目的位址/Mask: 0.0.0.0/0 以及目的埠: 80

介面為 LAN

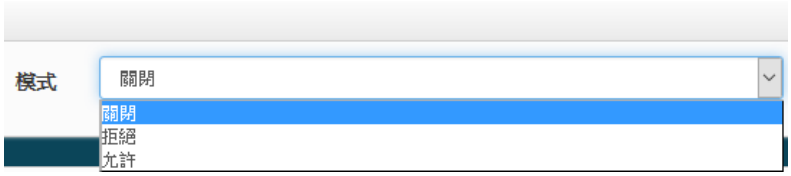
以下詳細頁面顯示


其他 IP 過濾等相關應用設定, 建議請上網尋找相關防火牆 IP 過濾規則等資訊

設定完成後，請點擊 " **儲存** " 按鈕後記得須點擊 " **重新啟動** " ，完成功能運作。

## 6.3 MAC 過濾

管理人員可以利用此頁面功能直接針對使用者的 MAC 位址進行網際網路的存取管制。此系統最大可設定 20 筆 MAC 位址。

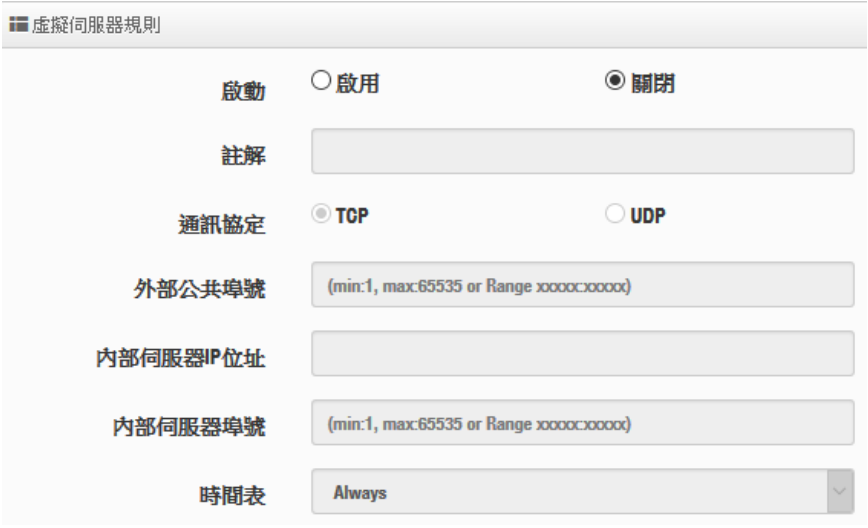




- **拒絕**：只阻擋 MAC 表單內的 MAC 位址，其他 MAC 將可以連線上網。
- **允許**：只開放 MAC 表單內的 MAC 位址，其他 MAC 將無法連線上網。

設定完成後，請點擊 " **儲存** " 按鈕後記得須點擊 " **重新啟動** " ，完成功能運作。

## 6.4 虛擬伺服器

如果管理人員希望外部可以讀取區網內開放的特定服務如 IP 網路攝影機、網頁伺服器、FTP 伺服器等讓服務透過通訊埠(Port)對外連接，可設定此功能。此設備可設定 20 筆虛擬伺服器規則。


- **啟動**：管理員可設定虛擬伺服器規則啟動或關閉。
- **註解**：可描述此規則用途。
- **通訊協定**：選擇服務欲使用的通訊協定類型。
- **外部公共埠**：設定外部通訊協定的服務埠號
- **內部伺服器 IP 位址**：設定區域網路的開放伺服器的 IP 位址。
- **內部伺服器埠**：設定區域網路的開放伺服器的使用服務埠號。
- **時間表**：是否要套用時間表進行自動執行或關閉條件。

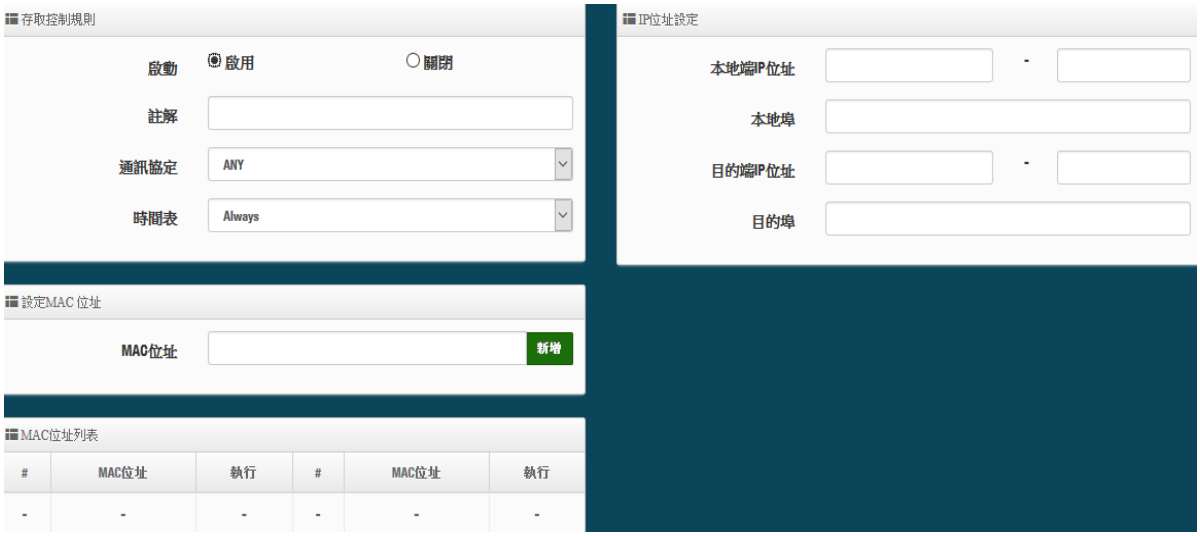
設定完成後，請點擊 " **儲存** " 按鈕後記得須點擊 " **重新啟動** " ，完成功能運作。

## 6.5 存取控制

此功能將可以讓網管人員限制或允許網路使用者成員或公司員工上網行為，利用此規則進行以「通訊協定」、「網域或關鍵字」或是「應用程式」進行阻擋或允許。可設定 20 筆管理規則

若只是單純要阻擋特定人員上網, 建議可以直接在 5.2 IP 過濾進行限制管理即可。

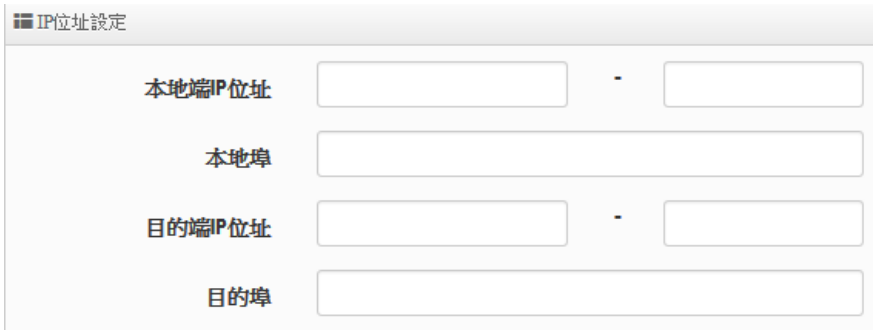

管理員可點擊 編輯 按鈕，進入設定頁面。




## 存取控制規則：


- **啟動**：可選擇啟動或關閉功能
- **描述**：可輸入此規則描述
- **通訊協定**：可選擇要過濾的通訊協定


- **ANY**：針對所有的通訊協定做規則管理。
- **TCP**：只針對 TCP 的通訊協定做規則管理
- **UDP**：只針對 UDP 的通訊協定做規則管理



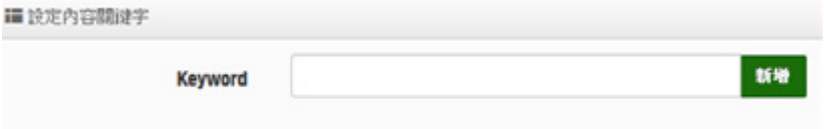

- ✓ **本地端 IP 位址:** 輸入要管理的本地端 IP 位址或 IP 區間。
- ✓ **本地埠：**輸入要管理的本地埠，若要設定區間可用”**:**”表示，例如(1:65535)
- ✓ **目的端 IP 位址：**輸入目的端 IP 位址或 IP 區間。
- ✓ **目的埠：**輸入要管理的目的埠，若要設定區間可用”**:**”表示，例如(1:65535)

- **ICMP：**只針對 ICMP 的通訊協定做規則管理


- ✓ **本地端 IP 位址:** 輸入要管理的本地端 IP 位址或 IP 區間。

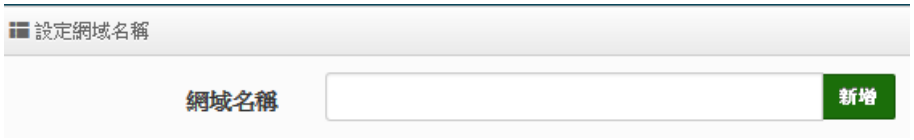
- **內容過濾：**可針對「關鍵字」進行規則設定，請在「關鍵字」欄位中輸入「關鍵字」後按下「新增」鍵，若要刪除請按「移除」鍵


- ✓ **本地端 IP 位址:** 輸入要管理的本地端 IP 位址或 IP 區間。
- ✓ **本地埠：**輸入要管理的本地埠，若要設定區間可用”**:**”表示，例如(1:65535)
- ✓ **目的端 IP 位址：**輸入目的端 IP 位址或 IP 區間。
- ✓ **目的埠：**輸入要管理的目的埠，若要設定區間可用”**:**”表示，例如(1:65535)
- ✓ **關鍵字：**輸入要過濾的內容關鍵字。(目前只支援英文關鍵字)

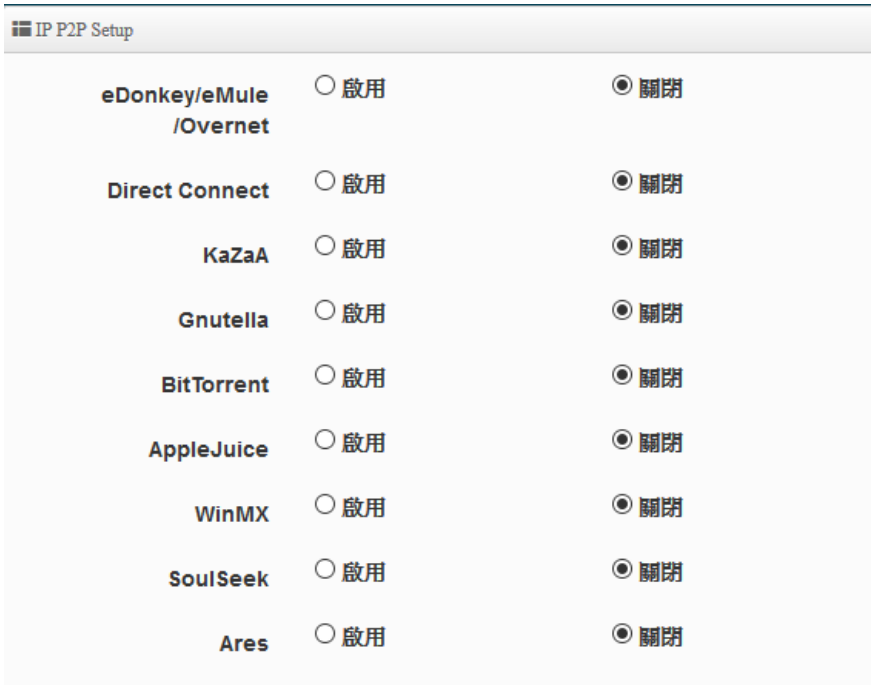



- **網域名稱過濾：**

管理員可針對「網域名稱」進行規則設定，請在「網域」欄位中輸入要過濾的網域名稱後按下「新增」鍵即可，若要刪除請按「移除」鍵




- **IP P2P:** 阻擋使用下載的應用程式，系統已內建多筆目前較常用的下載軟體進行阻擋



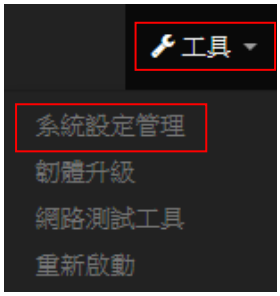

➢ **設定 MAC 位址：**管理員可針對特定的 MAC 去做條件過濾。


設定完成後，請點擊 " **儲存** " 按鈕後記得須點擊 " **重新啟動** " ，完成功能運作。

# 7. [ 工具 ]

網路管理員可在此管理系統設定，包含系統設定管理、韌體升級、網路測試工具、資料庫格式化及重新啟動本機無線基地台。

## 7.1 系統設定管理




管理者可以在備份此系統現行環境的設定資料或還原備份設定或回復系統預設值等功能，請先點選「**工具**」→「**系統設定管理**」進入頁面。


- **下載系統設定備份檔案**：點選「**儲存**」鍵即可開始備份整個系統的設定值，請指定儲存備份的「**系統設定檔**」至你所指定的電腦磁碟裝置中，日後可透過此設定檔回復系統設定值。
- **回存系統設定備份檔案**：請先點選「**瀏覽**」鍵選取一個先前您曾經備份過得設定檔，再點選「**上傳**」，即可回復至先前的備份設定。
- **還原系統預設值**：請直接點選「**預設值**」鍵，系統將會直接還原出廠預設值，還原完成後，系統將出現提示告知您還原成功，此時請重新啟動系統即可。
- **從電腦上常傳 SSL 憑證檔案 ：**若架構環境中，管理單位有屬於自己單位的 SSL 安全憑證時，可透過此功能將該單位的 SSL 安全憑證上傳至本機上運作。

## 7.2 韌體升級

假若 CERIO 有釋出新的韌體，管理者若有必要去更新系統的韌體時，管理者可以至本公司網站（http://www.cerio.com.tw）瀏覽是否有提供更新的韌體，可以從我們網站中下載並進行系統更新。


我們強烈建議您：若您的**無線基地台**在平常時間運作正常且沒有發生任何相容性的問題，我們通常建議使用者不要輕易更新您的系統韌體，若必要更新切勿利用無線的方式更新韌體，更新韌體是一個有風險的動作，當更新失敗了可能會導致整個系統無法正常運作，而損毀，若沒有特殊需求下建議您不要隨意更新，請務必從本公司網站下載相關的韌體檔案，若您使用了一個非本公司釋出且不明來源的檔案，導致系統無法正常運作或喪失某些功能時，本公司將不負責此產品的任何後續維修服務，請您見諒！


- **從本機電腦升級韌體 ： 將**最新韌體儲存至個人 PC 上，再點選瀏覽找尋韌體存放位置，確認位置後點選升級，將開始執行韌體更新升級動作。
- **從 TFTP 伺服器升級韌體 ：** 將更新之韌體檔案放置 TFTP 伺服器上，然後在此功能頁面上輸入 TFTP 伺服器位址，並輸入確認韌體的檔案名稱，點選升級將開始執行韌體更新升級動作。
- **從 HTTP 連接位址升級韌體 ：** 將更新韌體放置在網站上，透過功能頁面的 URL 連接網址，輸入韌體放置路徑後，點選升級將開始執行韌體更新升級動作。

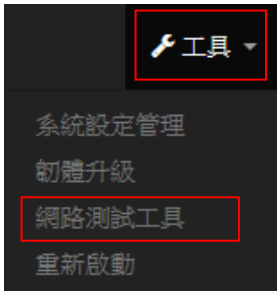
Notice

*我們強烈的建議您務必遵守以下步驟進行韌體更新：*

1. *請使用* ***RJ-45 網路線連接您的電腦以及無線基地台進行更新動作****，切勿使用無線連線的方式進行韌體更新作業。*
2. *更新過程中****請勿關閉或是切斷系統的電源****。*
3. *建議更新韌體前先清除瀏覽器歷史紀錄資料*
4. *更新完成後務必執行恢復原廠預設值動作並重新啟動您的無線基地台。*
5. *若未依照以上步驟進行更新作業，當發生更新失敗導致系統無法提供服務或是無法正常運作，請恕本公司會將此狀況判定為人為疏失，您將會失去您的產品保固服務，維修時將會向您收取相對的維修費用。*
6. *若您有任何更新產品上的問題歡迎您隨時致電本公司洽詢詳細的操作步驟後再進行。*

## 7.3 網路測試工具

請點選「工具」→「網路測試工具」頁面使用 Ping 的動作檢查目前的網路連線，網路管理員可以透過本工具診斷目前的網路狀態進行除錯。





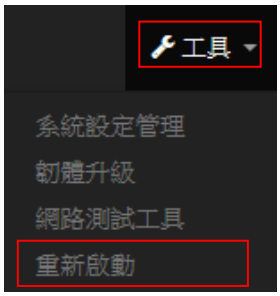
- **Ping**：此工具可以協助您以 PING 的指令測試遠端設備與系統的連線狀態，PING 工具是使用利用傳送 ICMP 封包的方式嘗試與遠端主機進行兩個網路節點之間的連線能力以及反應時間的測試程式，結果將顯示於「結果」欄位中。
  - **遠端 IP 位址 / URL 位址**：請在此欄位中輸入一組遠端的 IP 位址或網域名稱，再按下「PING」鍵進行測試。

- **回應時間**：您可以在此輸入所需要測試的次數，次數可輸入 1～50 的數值。

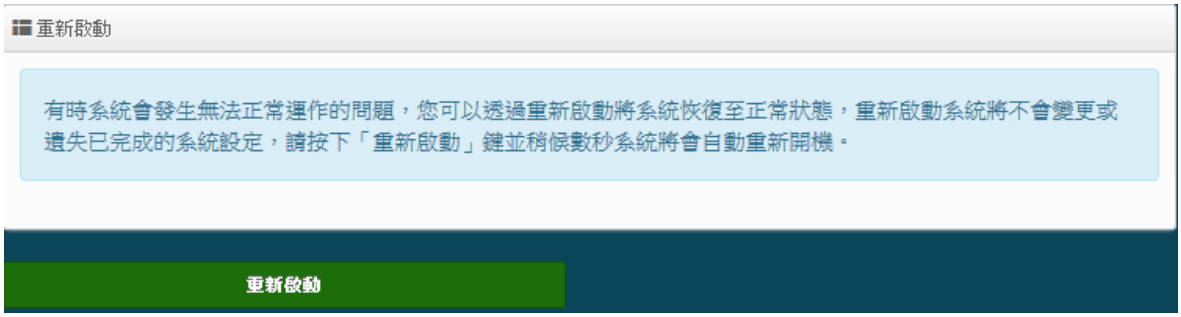
➢ **Traceroute**：此工具可以協助您以 Traceroute 的指令測試遠端設備與系統用來顯示路由封包到達目的位址的情形，結果將顯示於「結果」欄位中。

- **Destination Host**：請在此欄位中輸入一組遠端的 IP 位址或網域名稱，再按下「開始」鍵進行測試。
- **MAX Hop**：您可以在此輸入所需要顯示 Hop 的數量。

## 7.4 重新啟動




網路管理員可用「重新啟動」鍵輕鬆重新啟動系統，重新啟動完成約需一分鐘的時間。

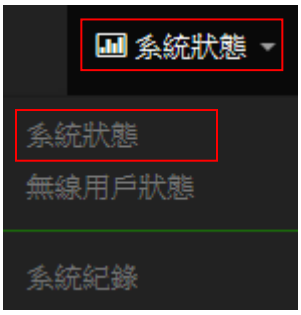



當您按下「**重新啟動**」鍵後系統將會跳出一視窗告知您目前還需要多少時間才能完成系統的啟動作業，請您稍待約 50 秒的時間切勿於重新啟動期間切斷系統電源以免發生系統錯誤。

# 8. [ 系統狀態 ]

系統狀態主要顯示系統相關資訊，包含系統網路資訊，無線基地台資訊，及無線使用者連線資訊等等

## 8.1 系統狀態

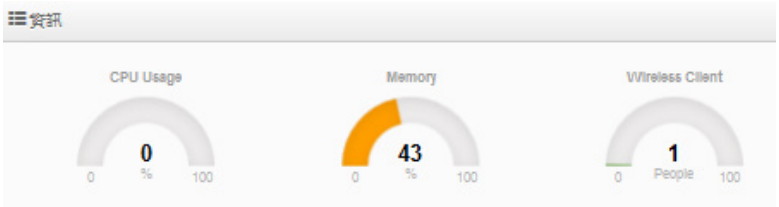




**系統狀態：**

主要顯示系統目前使用的模式，名稱，時間，韌體版本，網卡位址及相關網路設定等資訊。

**資訊：**




顯示目前系統已使用的 CPU 目前處裡的效能/Memory 的使用量及無線使用者目前的連線人數等。

**Radio 0 (2.4G) / Radio 1 (5G) :** 顯示目前 2.4G/5G 無線基地台的基本運作模式資訊

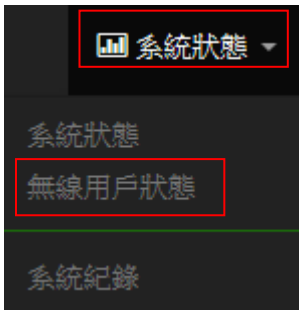
在 **Router** / **無線基地台模式**顯示如下


- **無線運作模式:** 顯示目前所無線使用是屬於 802.11 bg/n 或 ac/an 等(請確認項目 4.無線設定內所設定的模式)
- **頻道:** 顯示目前無線基地台所使用的頻道
- **速率:** 顯示目前使用的無線頻寬最大速率值，無線設定將會影響速率值，如加密方式及加密演算，無線運作模式等等都會影響

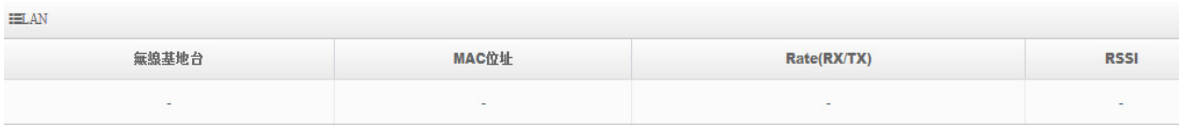
在 **Client** / **WISP 模式**顯示如下

- **模式:** 顯示 2.4/5G 的無線使用是 **Station 或 Repeater**，若顯示 Station 表示此無線(2.4G 或 5G)是與上端的 AP 站台做無線橋接，若顯示 Repeater AP 表示此無線(2.4G 或 5G)啟用的訊號再延伸功能。

## 8.2 無線用戶狀態




顯示 2.4/5G 的無線連線使用者的相關資訊




- **無線基地台**：顯示無線使用者所連接是屬於 2.4G 或 5G 的無線站台
- **MAC 位址**：顯示無線使用者的無線 MAC 位址
- **Rate(Tx/Rx)**：顯示使用者上下載的連線數
- **RSSI**：顯示無線使用者與 AP 之間的訊號值

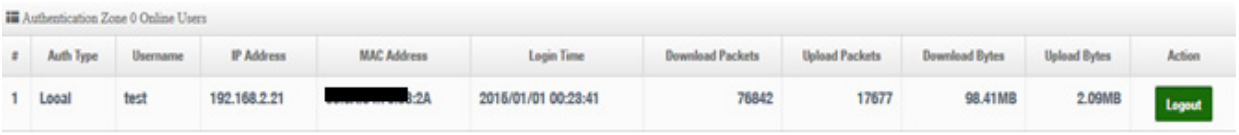
## 8.3 線上使用者


Notice 此狀態僅在無線基地台模式下顯示

當開啟網頁認證功能(參考項目 3.4 網頁認證)，將會顯示已通過線上網頁認證(Captive Portal)用戶。

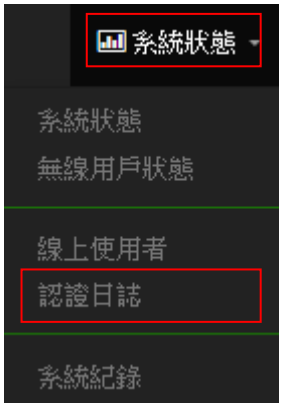
管理員可以監控用戶的身份驗證帳戶的登錄/登出時間和帳戶認證類型。


- **VALN#**：顯示用戶所使用的 VLAN 區域.
- **網頁認證功能**：顯示用戶認證的功能類型。
- **使用者數量**：顯示此用戶目前再線的認證數量，假若啟用一個帳戶可多台登入將會出現複數
- **下載封包**： 顯示此用戶的總下載封包量
- **上傳封包**：顯示此用戶的總上傳封包量
- **下載位元**：顯示此用戶下載多少 Mbps 的流量
- **上傳位元**：顯示此用戶上傳多少 Mbps 的流量
- **執行**：管理人員可以點擊 **“執行”** 按鈕去觀看更詳細的用戶使用資訊




- **Auth Type**：顯示用戶登入認證類型
- **User name**：顯示用戶的登入使用帳號
- **IP Address**：顯示用戶使用的 IP 位址
- **MAC Address**：顯示用戶的 MAC 位址
- **Login Time:** 顯示用戶所登入網頁認證的時間
- **Download Packets**：顯示此用戶的總下載封包量
- **Upload Packets**：顯示此用戶的總上傳封包量
- **Download Bytes**：顯示此用戶下載多少 Mbps 的流量
- **Upload Bytes**：顯示此用戶上傳多少 Mbps 的流量
- **Logout:** 將此認證用戶踢出

## 8.4 認證日誌

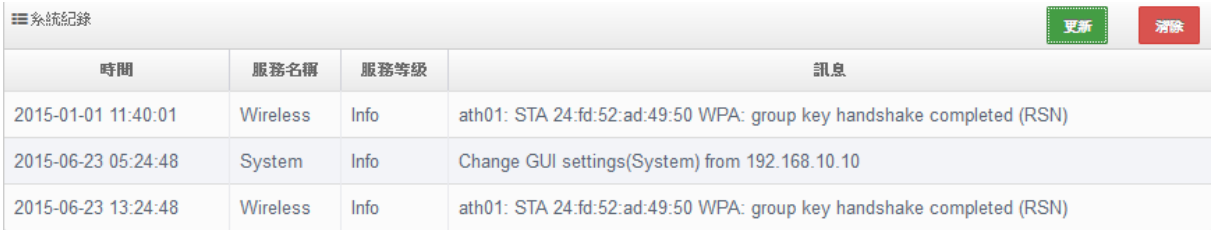



Notice 此狀態僅在無線基地台模式下顯示

認證日誌可以紀錄所有 VLAN 及帳戶登錄/登出及認證類型和帳戶使用時間。


## 8.5 系統紀錄


此頁面將會記錄無線基地台由開機到現在所有的系統處理狀態以及詳細資訊，此處的進階資訊將可以協助系統管理針對系統的問題進行除錯。




| 時間 | 服務名稱 | 服務等級 | 訊息 |
|---|---|---|---|
| 2015-01-01 11:40:01 | Wireless | Info | ath01: STA 24:fd:52:ad:49:50 WPA: group key handshake completed (RSN) |
| 2015-06-23 05:24:48 | System | Info | Change GUI settings(System) from 192.168.10.10 |
| 2015-06-23 13:24:48 | Wireless | Info | ath01: STA 24:fd:52:ad:49:50 WPA: group key handshake completed (RSN) |

# Appendix A. WEB GUI Valid Characters

***Table B WEB GUI Valid Characters***

| Block | Field | Valid Characters |
|---|---|---|
| **LAN** | IP Address | IP Format; 1-254 |
| | IP Netmask | 128.0.0.0 ~ 255.255.255.252 |
| | IP Gateway | IP Format; 1-254 |
| | Primary DNS | IP Format; 1-254 |
| | Secondary DNS | IP Format; 1-254 |
| | Hostname | Length : 32<br>0-9, A-Z, a-z<br>~ ! @ # $ % ^ * ( ) _ + - { } \| : < > ? [ ] / ; `, . = |
| **DHCP Server** | Start IP | IP Format; 1-254 |
| | End IP | IP Format; 1-254 |
| | DNS1 IP | IP Format; 1-254 |
| | DNS2 IP | IP Format; 1-254 |
| | WINS IP | IP Format; 1-254 |
| | Domain | Length : 32<br>0-9, A-Z, a-z<br>~ ! @ # $ % ^ * ( ) _ + - { } \| : < > ? [ ] / ; `, . = |
| | Lease Time | 600 ~ 99999999 |

*Table B WEB GUI Valid Characters (continued)*

| Block | Field | Valid Characters |
|---|---|---|
| **Management** | System Name/ Location | Length : 32<br>0-9, A-Z, a-z<br>Space<br>~ ! @ # $ % ^ * ( ) _ + - { } \| : < > ? [ ] / ; `, . = |
| | Description | 32 chars |
| | Password | Length : 4 ~ 30<br>0-9, A-Z, a-z<br>~ ! @ # $ % ^ * ( ) _ + - { } \| : < > ? [ ] / ; `, . = |
| | HTTP/ HTTPS Port | 1 ~ 65535 |
| | Telnet/ SSH Port | 1 ~ 65535 |
| **SNMP** | RO/RW community | Length : 32<br>0-9, A-Z, a-z<br>~ ! @ # $ % ^ * ( ) _ + - { } \| : < > ? [ ] ; `, . = |
| | RO/RW user | Length : 31<br>0-9, A-Z, a-z<br>~ ! @ # $ % ^ * ( ) _ + - { } \| : < > ? [ ] ; `, . = |
| | RO/RW password | Length : 8 ~ 32<br>0-9, A-Z, a-z<br>~ ! @ # $ % ^ * ( ) _ + - { } \| : < > ? [ ] ; `, . = |
| | Community | Length : 32<br>0-9, A-Z, a-z<br>~ ! @ # $ % ^ * ( ) _ + - { } \| : < > ? [ ] ; `, . = |
| | IP | IP Format; 1-254 |
| **General Setup** | Tx Power | 1-100 % |
| **Wireless Profile** | Profile Name | 32 chars |
| | ESSID | Length : 31<br>Space<br>0-9, A-Z, a-z<br>~ ! @ # $ % ^ * ( ) _ + - { } \| : < > ? [ ] / ; `, . = |
| | WEP Key | 10, 26 HEX chars or 5, 13 ASCII chars |
| | Pre-shared Key | 8 ~ 63 ASCII chars; 64 HEX chars |
| **Advanced Setup** | Beacon Interval | 20 ~ 1024 |
| | Date Beacon Rate | 1 ~ 255 |
| | Fragment Threshold | 256 ~ 2346 |
| | RTS Threshold | 1 ~ 2347 |

*Table B WEB GUI Valid Characters (continued)*

| Block | Field | Valid Characters |
|---|---|---|
| **Virtual AP Setup** | ESSID | Length : 31<br>Space<br>0-9, A-Z, a-z<br>~ ! @ # $ % ^ * ( ) _ + - { } \| : < > ? [ ] / ; `, . = |
| | Maximum Clients | 1 ~ 32 |
| | VLAN ID | 1 ~ 4094 |
| | WEP Key | 10, 26 HEX chars or 5, 13 ASCII chars |
| | Group Key Update Period | >=60 seconds |
| | PMK Cache Period | > 0 minute |
| | Pre-Shared Key | 8 ~ 63 ASCII chars; 64 HEX chars |
| | Radius Server IP | IP Format; 1-254 |
| | Radius Port | 1 ~ 65535 |
| | Shared Secret | 8 ~ 64 characters |
| | Session Timeout | >= 60 seconds; 0 is disable |
| **IP Filter** | Source Address | IP Format; 1-254 |
| | Source Mask | 0 ~ 32 |
| | Source Port | 1 ~ 65535 |
| | Destination Address | IP Format; 1-254 |
| | Destination Mask | 0 ~ 32 |
| | Destination Port | 1 ~ 65535 |
| **MAC Filter** | MAC address | MAC Format; 12 HEX chars |
| **Virtual Server** | Description | 32 chars |
| | Private IP | IP Formate; 1-254 |
| | Private/ Public Port | 1 ~ 65535 |