CERIO Corporation

CenOS 5.0 使用手冊

OW-200 A1 / OW-218 A1 機種適用

NCC 警語

低功率電波輻射性電機管理辦法

第十二條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。

前項合法通信，指依電信法規定作業之無線電通信。

低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

1. 使用此產品時應避免影響附近雷達系統之操作。
2. 高增益指向性天線只得應用於固定式點對點系統。
3. 此器材須經專業安裝並限用於固定式點對點操作。
4. 本器材須經專業工程人員安裝及設定，始得設置使用，且不得直接販售給一般消費者。
5. 隱私權警語標示：「為維護隱私權，請妥適使用」。
6. 「電磁波曝露量MPE標準值1mW/cm^2，本產品使用時建議應距離人體 35cm」。

1. 初始登入系統管理及主體相關說明

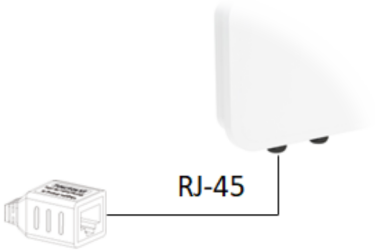
1.1 主體及 RJ-45 功能套件說明

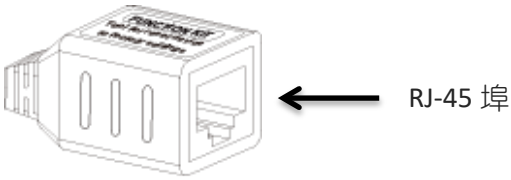
主體說明

Notice

1. 當設備無線訊號輸出，使用 1T1R 時，則主要訊號輸出位置在 ANT1，而 ANT2 將無訊號輸出，請留意。可參考 4.5.1 RADIO 0 設定說明
2. 主機本體不加入硬體式回復出廠預設值按鈕，設計以透過 RJ-45 功能套件來做回復出廠預設值用，使用方式在設備運作下，請利用 RJ-45 網路線連接主體 ETH2 與 RJ-45 功能套件約 5 秒後，拔除 RJ-45 功能套件即回復出廠值，如下圖範例

RJ-45 功能套件

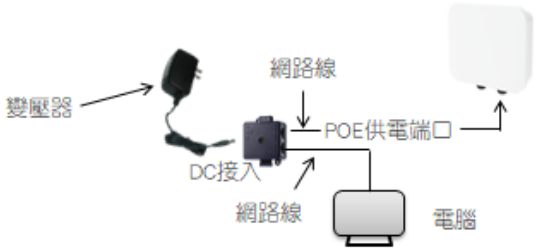




1.2 無線基地台登入設定前置作業

智鼎無線基地台的 CenOS 5.0 採用網頁管理方式，當架構建置完成，可以透過瀏覽器登入管理，當進入頁面後輸入正確的帳號密碼即可管理設備功能，再連接無線基地台之前，電腦端需先設置與無線基地台相同 IP 網段，才能順利連接至無線基地台，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。

基本連接示意圖

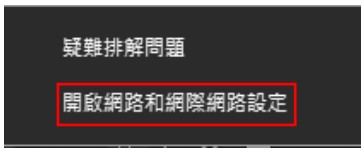


Windows 作業系統為例

為了進入 CenOS 5.0 軟體的管理頁面，則電腦 IP 網段必須與 CenOS 5.0 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 CenOS 5.0 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 CenOS 5.0 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，再點擊 **”開啟網路和共用中心”**，進入設定頁面。

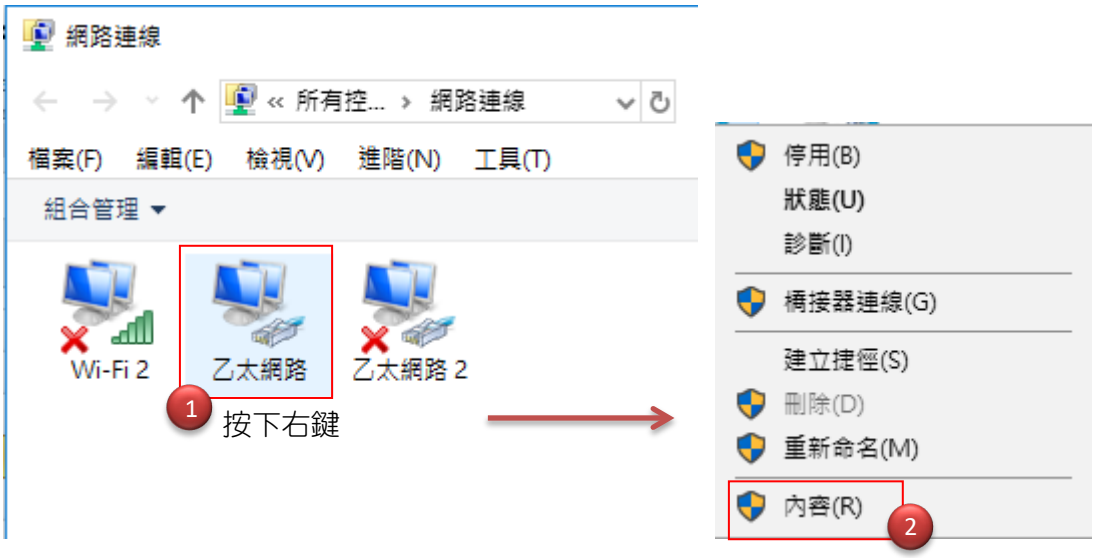
將滑鼠移到此處” **網路運作小圖示**”並按下滑鼠右鍵



再點擊 **”開啟網路和網際網路設定”** 開啟設定頁面

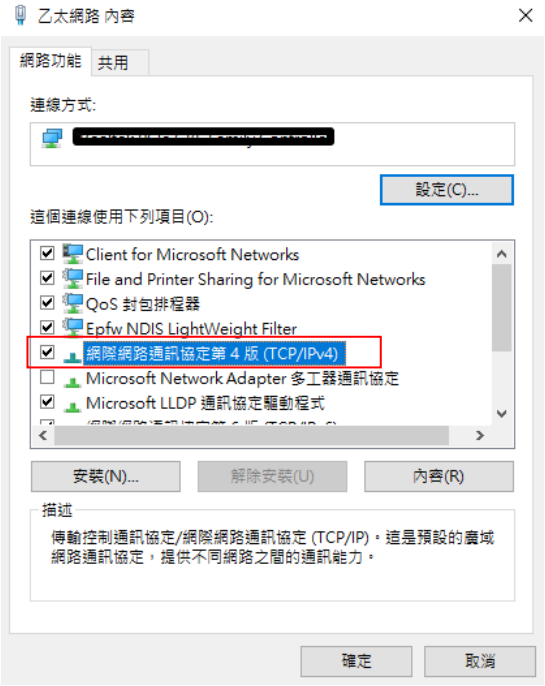
步驟 2： 當開啟網路和網際網路設定頁面後，在左邊目錄點擊 ”**乙太網路**” 並在右邊選項點擊”變更介面卡選項”進入設定。

步驟 3：進入變更介面卡設定則會出現以下圖示，將滑鼠移到到正確的 ”**乙太網路**” 後按下右鍵點擊內容。



點擊內容進入設定 IP 位址

步驟 4：完成步驟 3 後，將跳出如下設定頁面，選擇**網際網路通訊協定第 4 版(TCP/IPv4)**點兩下，或是按下確認，進入設定 IP 位址。

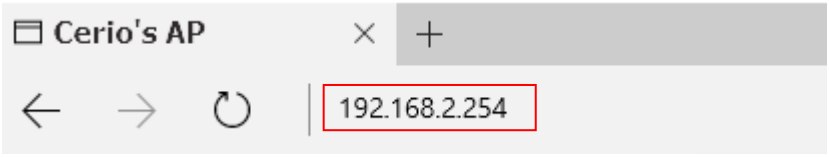


步驟 5：點擊 TCP/IPv4 將進入 PC 或筆電的 IP 位址設定頁面，預設為自動取得 IP 位址，我們將它改為"使用以下的 IP 位址"，並在 IP 欄位打入與 CenOS 5.0 軟體的同網段 IP 位址，例如 CenOS 5.0 軟體的預設 IP 為 192.168.2.254，則 PC 或筆電的 IP 為者可以設定 192.168.2.x ，x 可設定 1~至 253 之間的數值。以下圖為例，完成設定。

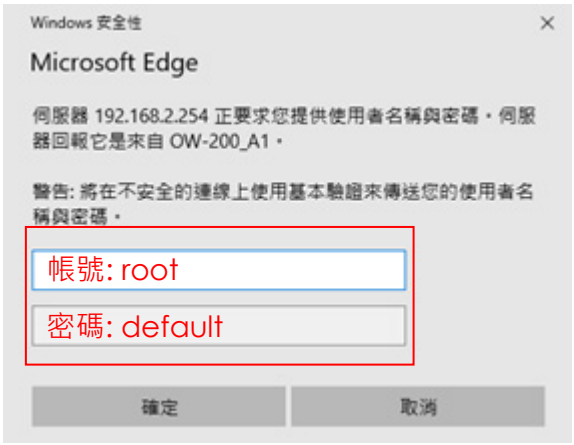
以上程序將完成電腦與無線基地台的連接與溝通，接下來請參考手冊 1.3 登入程序

1.3 登入基地台的 WEB 管理頁面

接下來請開啟您的 IE 瀏覽器或其他如 Firefox、Chrome 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。

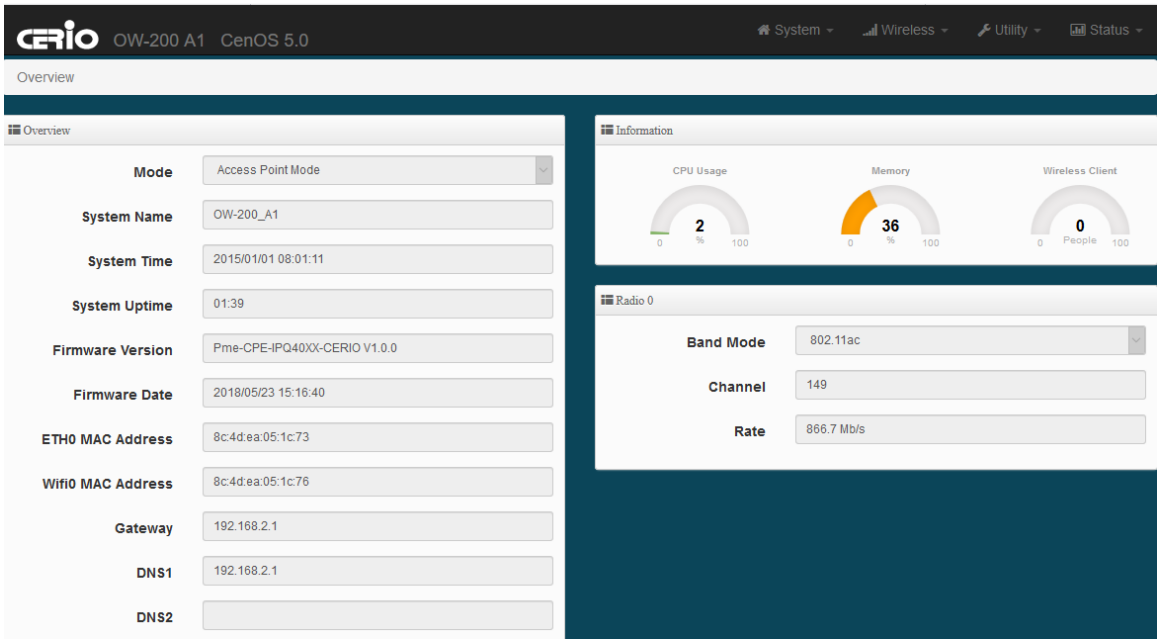


成功登入管理介面後將出現基地台的登入畫面，請在使用者名稱欄位中輸入〝**root**〞，密碼鍵入〝**default**〞，然後按「**確定**」即可登入管理介面。



請使用預設使用者名稱為” root” 與 預設密碼 “ default “ 進行入。

 # 登入成功後將顯示畫面如下畫面，預設畫面將顯示無線基地台的狀態頁面



2. 初次登入系統管理頁面設定

智鼎的 OW-200 A1 與 OW-218 A 所使用的軟體版本均為 CenOS 5.0 核心，在設定之功能將完全相同，而以下的所有功能應用說明等，將以 OW-200 A1 作為範例

Notice

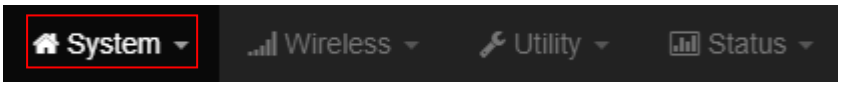
系統初次登入之預設語系皆為英文介面，若要切換至中文介面，請參考手冊 2.1 程序將協助管理者轉換為中文介面

2.1 變更使用中文介面語系

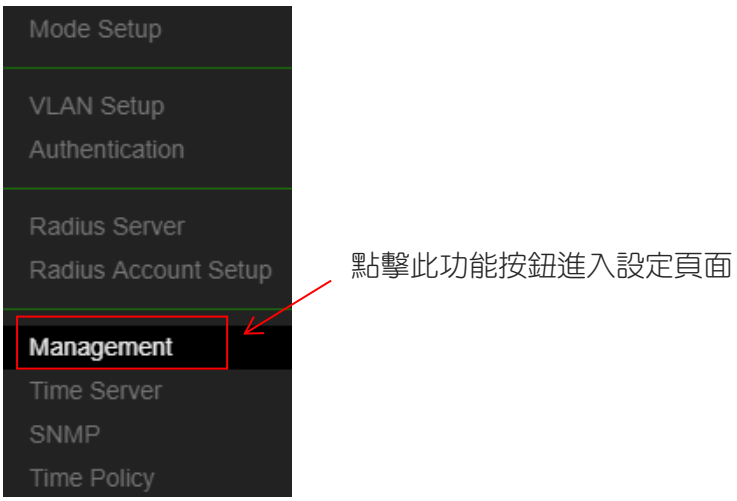
若管理者需要使用中文頁面，管理者可以直接進入基地台管理頁面的系統內變更管理頁面的介面語系。

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：

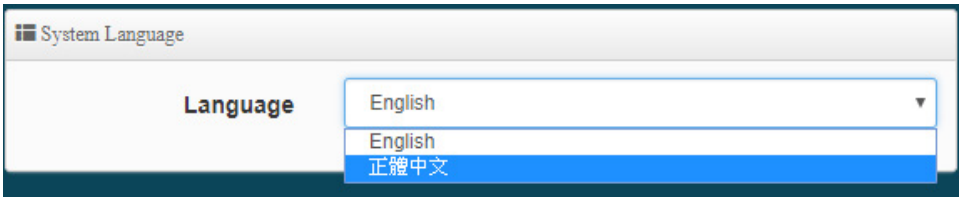
1. 在選單點擊「**System**」下拉式選單。



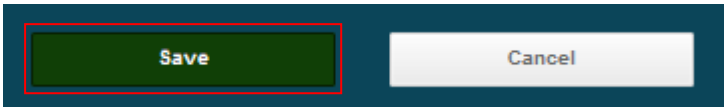
2. 在下拉式選單中找出「**Management**」功能選項。



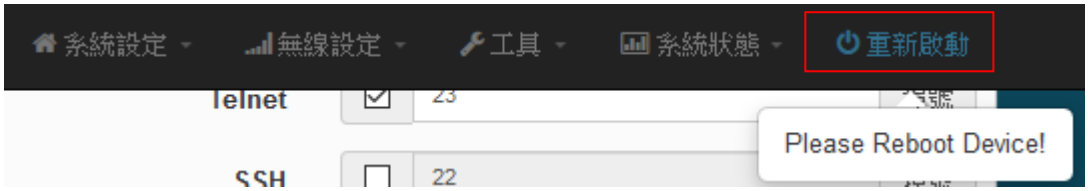
3. 在第一個欄位上「**System Language**」選項，並在「Language」下拉式選單中，選取「正體中文」選項。



4. 確認選取正體中文後，請點擊頁面最下方的 Save 按鈕將剛選取的設定儲存下來



5. 再點擊頁面最右上方的重新啟動(Reboot)按鈕，並確認重新啟動後系統將完成中文介面



2.2 選擇正確的操作模式使用

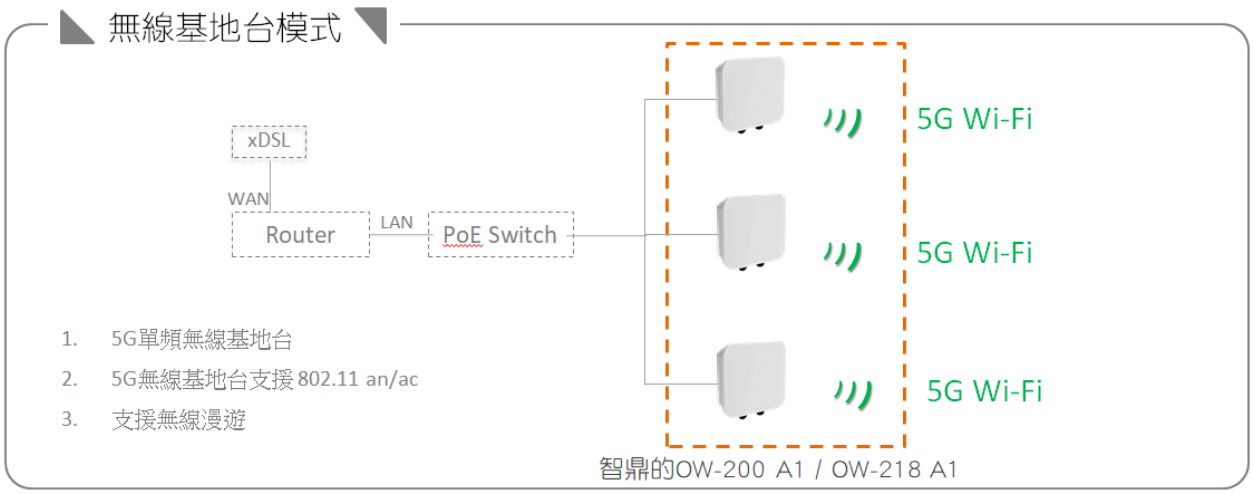
Notice

系統初次登入之模式為"**無線基地台模式**"，請依照應用需求決定要選擇使用的模式，可參考以下的模式應用示意圖說明，以確保使用正確的應用模式

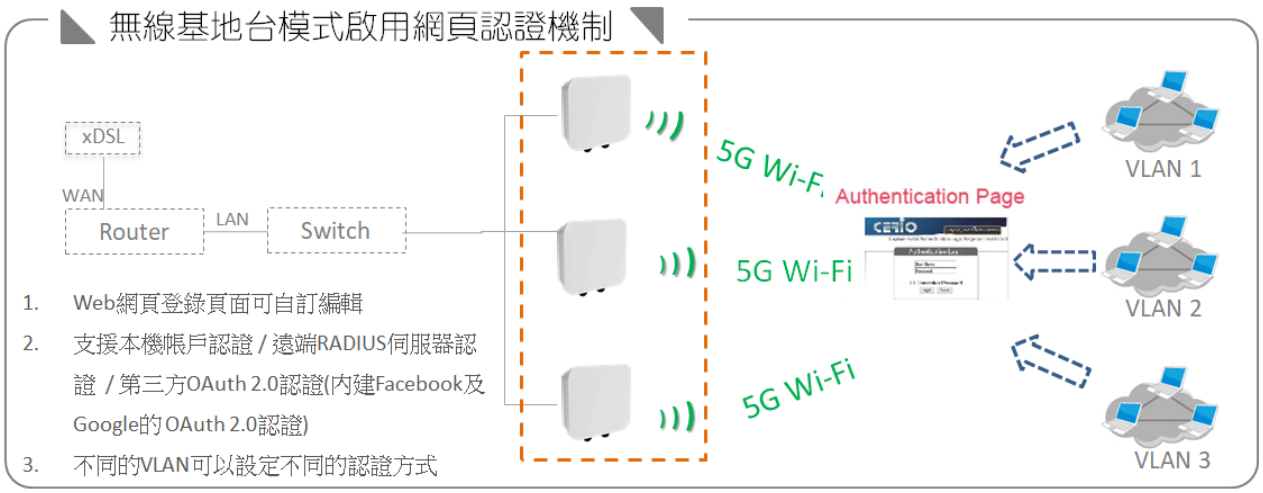
管理人員若需要切換模式，可在選單中"系統管理➔模式"下進行更換模式應用，如何正確選擇模式使用請參考以下圖解說明來決定採用正確模式(以下僅供參考)

無線基地台模式

當環境已完成建置有線上網的服務後，預想要利用無線方式進行上網，則可將設備轉換為無線基地台模式，只要網路線連接至設備，設定好無線基地台的相關設定，將可達成使用無線上網之應用。



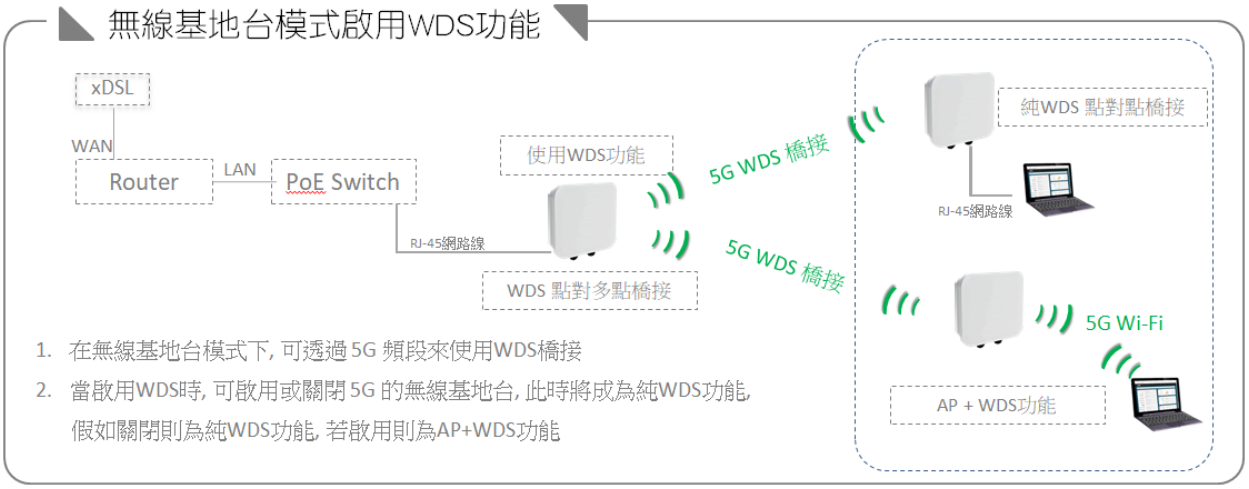
無線基地台模式使用網頁認證功能之應用



無線基地台模式使用 WDS 功能之應用

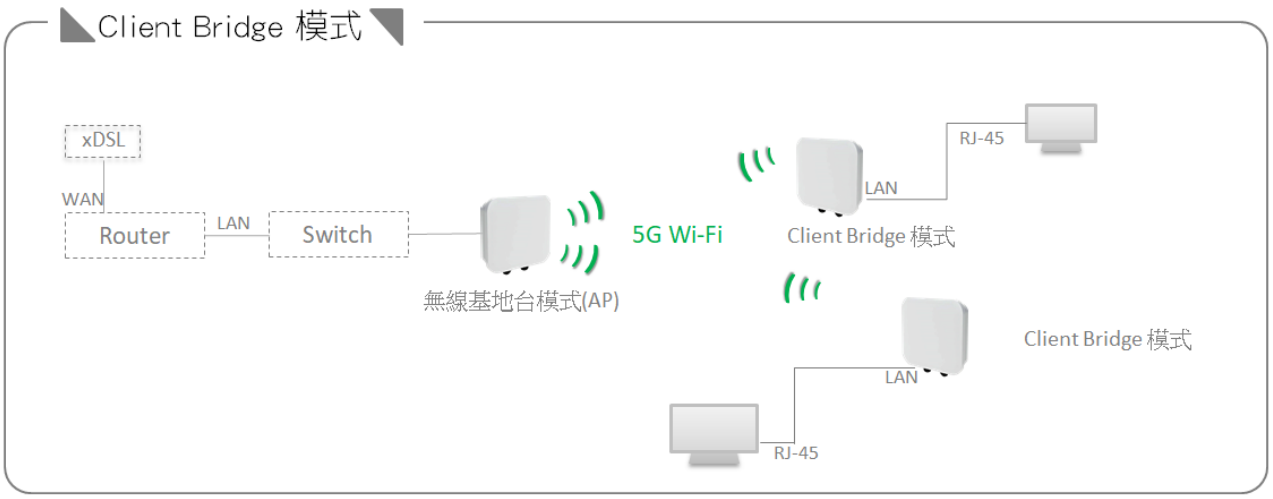
所謂的 WDS 功能，可想成它是一條網路線，差別在他是透過無線的方式行連接，通常就俗稱為 WDS 點對點橋接之應用，而 WDS 不單只是做點對點橋接，他也能做點對多點之應用

在無線基地台下啟用 WDS 功能，則為 AP+WDS 之應用，也就是說設備一樣可以使用 AP 之服務外，其中又能透過 WDS 方式與另一台 AP 做橋接應用



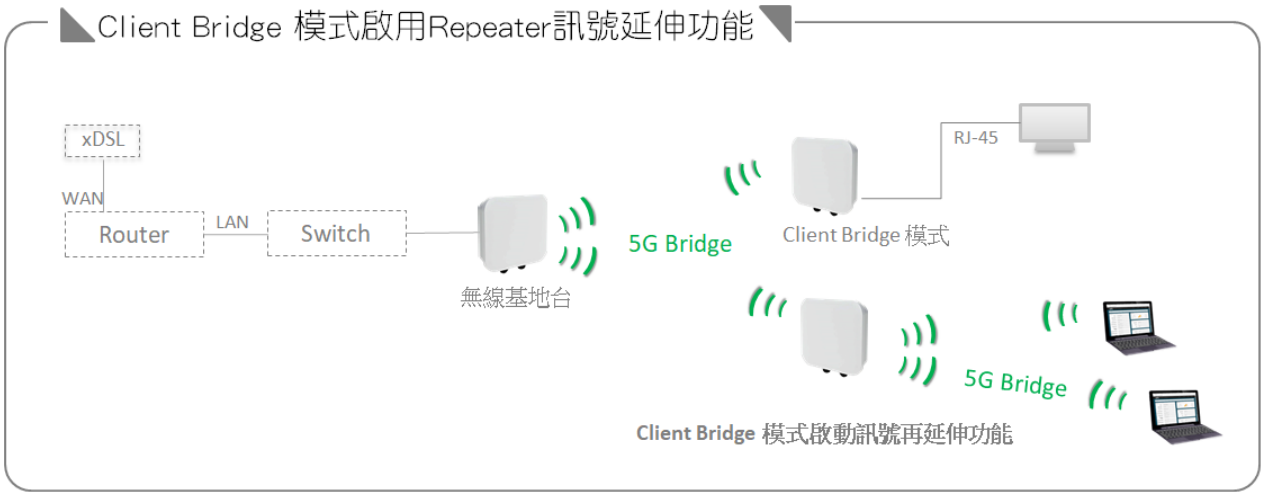
Client Bridge 模式

所謂 Client Bridge 模式，可以把它想像成它是一個外接式的無線網卡，專門負責與上端無線基地台(AP)做無線連線。



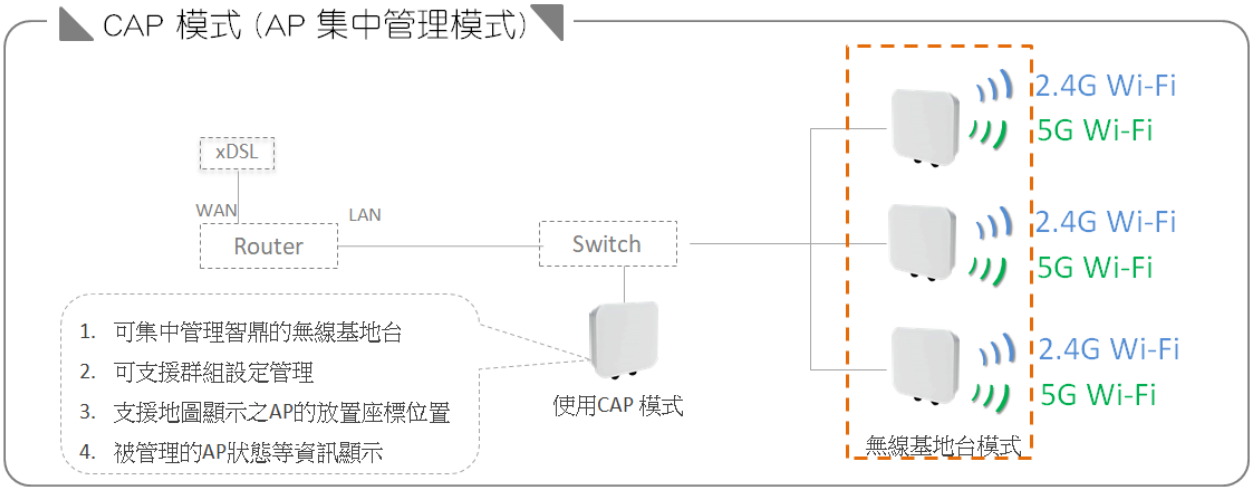
Client Bridge 模式+ Repeater AP 之應用

所謂 Repeater AP 功能，則表示當 Client Bridge 確實與上端 AP 做連接後，自己本身可在建置出無線基地台，俗稱訊號再延生機制。



CAP 模式

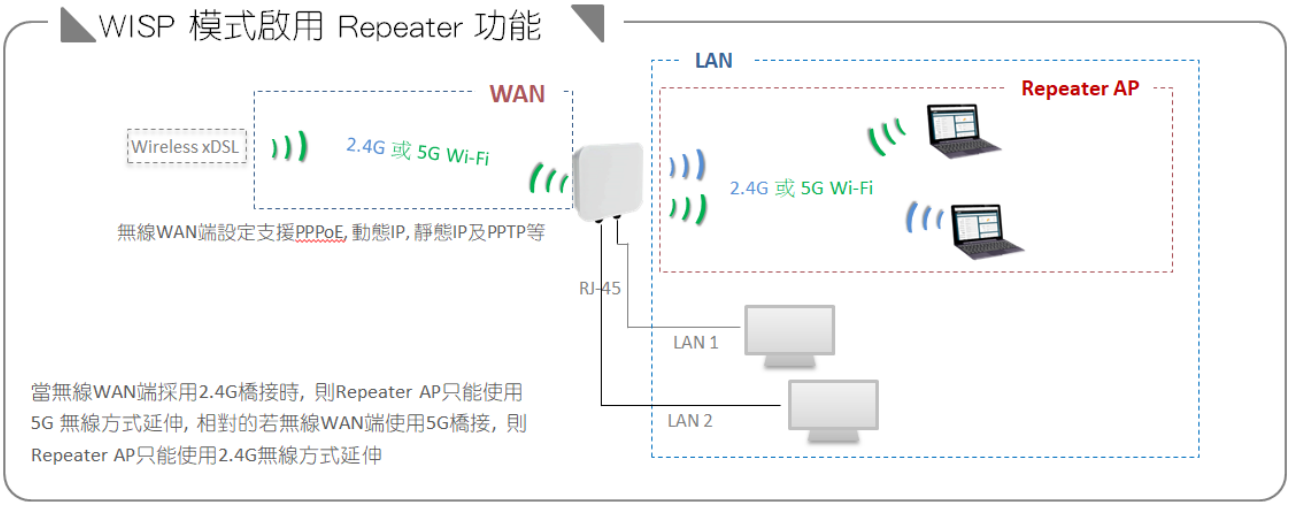
此功能非常特殊，專屬於智鼎資訊獨家傭有的一項技術，它的應用是當切換此功能後，此設備將改變成一台集中式控制器，而非無線基地台，它的工作將負責把同一個網域中的所有智鼎資訊的無線基地台設備集中統一控制管理。也就是說，環境中有多台智鼎的無線設備必須要設定時，只要在這管理器上設定好確認送出，底下多台的無線設備將全部設定完成。



WISP 模式

WISP 模式是(Wireless Internet Service Provide)的簡稱，WISP 的 WAN 端是以無線方式橋接上端的 xDSL 基地台，連線方式支援動態 IP、靜態 IP、PPPoE 及 PPTP 等。而在透過 NAT 方式分享到所有的 LAN 端，在使用 WISP 模式時本機的實體網路埠為 LAN 運作(分別為 LAN1 與 LAN2 網路功能埠)，而在 WISP 模式啟用 Repeater AP 功能時，本機的 LAN 將產生無線基地台提供給無線用戶使用。可參考下圖說明。

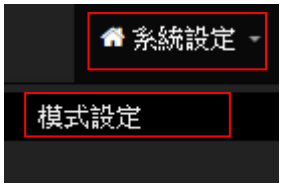
WISP 模式需要啟動 Repeater AP(延伸無線基地台功能)，此模式下無線 WAN 端確實正常運作後，則 Repeater AP(Wi-Fi 基地台)功能才可正常運作,提供使用者無線存取使用.(預設為啟用)

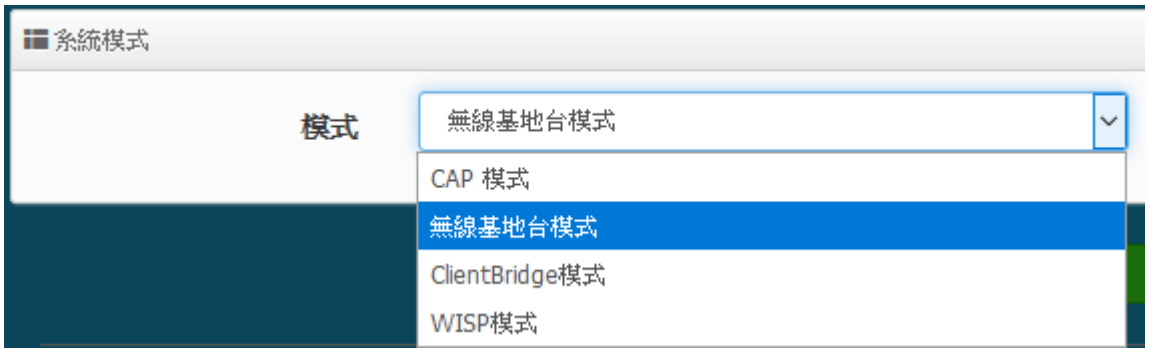


3. 系統設定

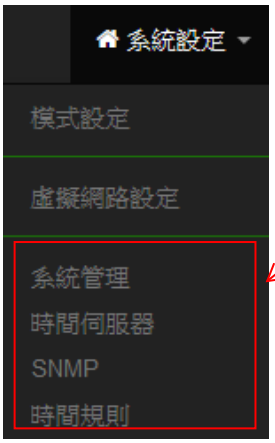
3.1 模式設定

在管理介面下，點擊選項中**"系統設定" ➔ "模式設定"**，選擇欲想要應用之模式，確認後 **" 按下儲存&重新啟動 "** 按鈕即可完成模式切換。





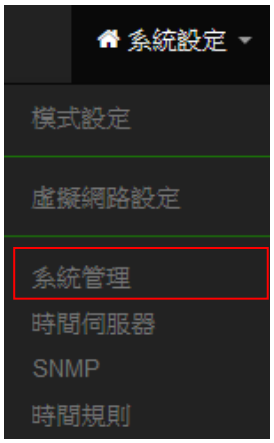
Notice



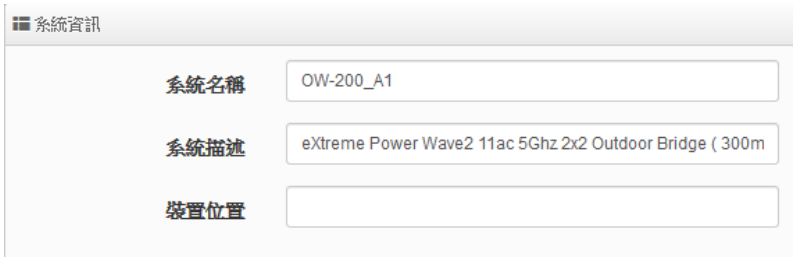
在任何模式下的"**系統管理**", "**時間伺服器**", "**SNMP**", 及"**時間規則**"等管理功能為共用設定區域，以下章節先介紹共用設定區域之說明

3.2 系統管理

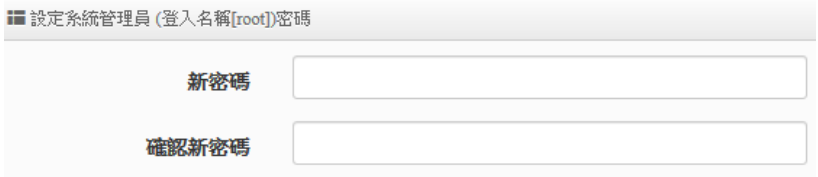
此管理頁面主要設定介面語系，設備名稱及描述，或登入者密碼變更及相關登入協定等，同時能設定系統自動重啟功能設定遠端 System Log Server 連接及 Ethernet 特殊應用等功能，假若設備不需要 LED 燈號顯示也能在此頁面進行關閉。



- **語系:** 本設備支援中英兩種語系，管理者可在此切換管理頁面之語系

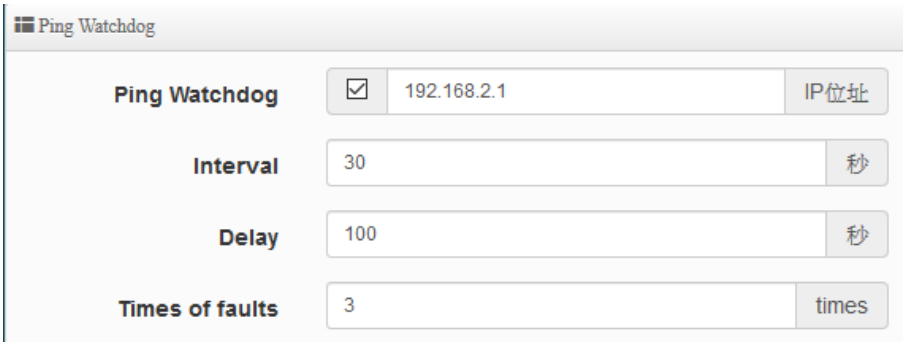


- **系統名稱:** 管理者可自訂編輯設備的系統名稱。
- **系統描述:** 管理者可自訂編輯設備的系統名稱。
- **裝置位置:** 管理者可自行描述設備的裝置位置資訊。



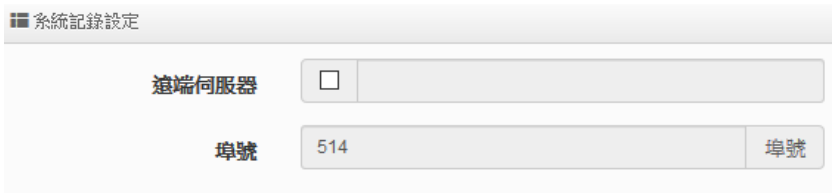
- **新密碼:** 可設定要修改的 root 登入密碼
- **確認新密碼:** 再輸入一次要修改的 root 登入密碼做確認動作

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

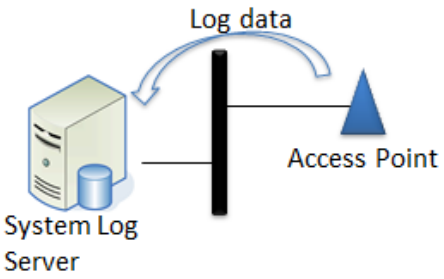


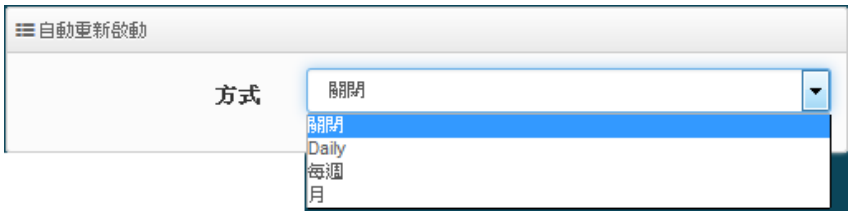
- **Ping Watchdog:** 輸入遠端設備的 IP 位址(建議輸入的 IP 位址是確認不會失聯的主機 IP 位址)
- **Interval:** 設定 Ping 的間隔時間，最少 30 秒
- **Delay:** 設定系統重新開機後延遲多久才開始 ping
- **Times of faults:** 當 ping 錯誤達到設的值後，系統自動重新起動

- **管理介面登入設定** ：
  - **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。
    - ✓ **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。
    - ✓ **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。
    - ✓ **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。
    - ✓ **主機憑證金鑰內容:** 若 SSH 服務需要提供金鑰，可在此產生 SSH 使用金鑰。
    - ✓ **ACCESS WAN:** 此功能主要讓遠端設備是否能連接至本設備進行管理，預設為關閉



- **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將往伺服器上備存，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。



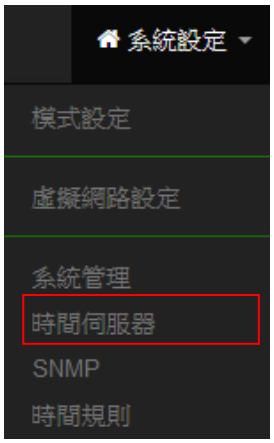


此功能可以依照管理者需求，依照管理者所安排之時間規則進行系統的重新啟動

- 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

設定完成後，記得按下儲存按鈕並重新啟動系統讓功能正常運作

3.3 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 的閘道 IP 位址與 DNS 伺服器設定是否正確。

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。

3.4 SNMP

請點選「**系統設定**」→「**SNMP**」進入 SNMP 設定頁面，此頁面功能將可以讓您啟動 **AP** 的 SNMP 功能，管理者可以依照實際需求開啟或關閉此功能，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。此 SNMP 支援 V2c 版, V3 版及 SNMP Trap 等

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。

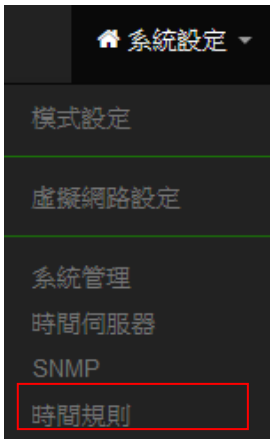
SNMP Trap

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。

3.5 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。

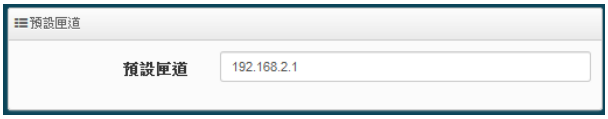
設定完成後，請點擊”**儲存**”按鈕後記得須點擊”**重新啟動**”，完成功能運作。

4. 無線基地台模式(AP Mode)

4.1 虛擬網路設定

此設備預設支援 16 組 VLAN 功能，每個 VLAN 都符合 802.1q tag VALN，在虛擬網路功能頁面將可設定每個 VLAN 的 IP 位址, Gateway(閘道)位址, DHCP 伺服器，頻寬管理，網頁認證，虛擬無線基地台等等相關應用

- **#** ：顯示虛擬網路組別。
- **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**：顯示虛擬網路使用的 Tag ID 資訊，當顯示 **Native ETH0** 表示目前主要的有線連接是以此虛擬網路為主要登入系統。
- **IP 位址**：顯示每個虛擬網路所設定的 IP 位址。
- **子網路遮罩**：顯示每個虛擬網路所設定的子網路遮罩。
- **Radio 0** ：為 5Ghz 基地台，可顯示每個虛擬網路中 5Ghz 的 SSID 名稱以及是否啟用(綠色為啟用，紅色代表停用)。
- **執行**：點擊 **網路** 的按鈕，進入 LAN 的設定頁面， 點擊 **網路** 下拉箭頭則顯示無線設定功能列表。
- **預設閘道**：設定閘道器 IP 位址。



Notice

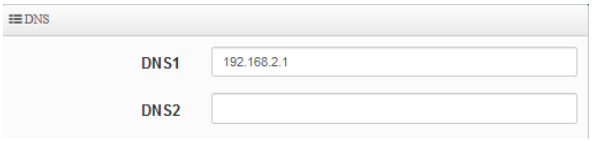
若預設閘道位址設置錯誤，將導致無法上網或無法顯示 ESSID 名稱，請務必確實輸入正確

- **Port Isolate:** 啟用或關閉虛擬 Ethernet 功能，預設為關閉。

  啟用或關閉虛擬 Ethernet 功能，若網頁認證服務啟動，並需要實體有線及無線用戶上網服務都必須攔截認證，則需要啟用它，假若指攔截無限用戶，則可關閉，預設為關閉。

  - **啟用**：若選擇啟用則系統將透過軟體自動在實體乙太網路主控制晶片上建立出虛擬 Ethernet 連接埠。當啟用此功能則虛擬網路(VLAN)將只有一組提供服務。
  - **關閉**：若選擇關閉則系統將以實體乙太網路主控制晶片為主，不建立虛擬 Ethernet，此時將可有多組虛擬網路(VLAN)服務

- **DNS**：設定 DNS 解析的 IP 位址。



Notice

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)

網路設定

點擊**"網路"**按鈕進入設定虛擬網路相關功能 

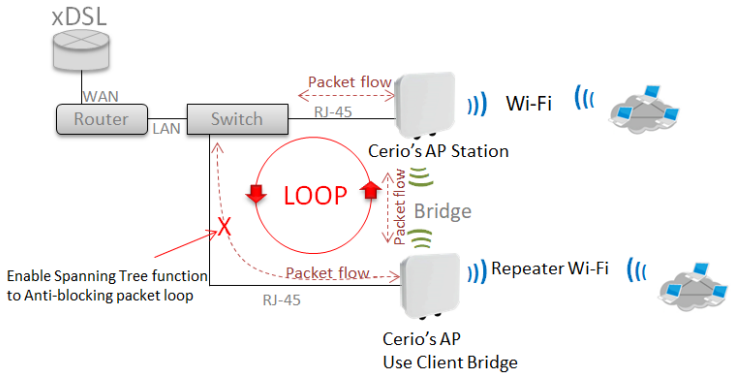
- **虛擬網路服務**：可啟用或關閉虛擬網路功能，預設值指開啟**"虛擬網路 0"**。
- **IP 設定**：可啟用/關閉**"虛擬網路"**的 VLAN IP，或修改虛擬網路的 IP 位址/子網路遮罩。

Notice

虛擬網路服務及 IP 位址至少需要有一組 VLAN 服務可以正常登入管理，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。

系統管理：

- **Access Point 0**：可針對此 VLAN 的虛擬網路啟用或關閉發射 5G 的訊號。
- **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**：可啟用或關閉此無線基地台是否要被管理器管理。
- **IAPP**：可選擇啟用或關閉 IAPP 無線漫遊。

Notice

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）

ETH0 虛擬網路標記設定

- **VLAN Tag:** 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。

Notice

注意假如 ETH0 設定使用 VLAN Tag 時，則進入管理介面就必須與 tag 相同之 VLAN 才可進入管理設定，非此 VLAN 網域則完全阻絕。

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。

網路設定(下拉式功能)

點擊"網路"按鈕旁下拉式按鈕 

設定 DHCP 伺服器，頻寬控制及無線基地台功能等。

4.1.1 DHCP 伺服器

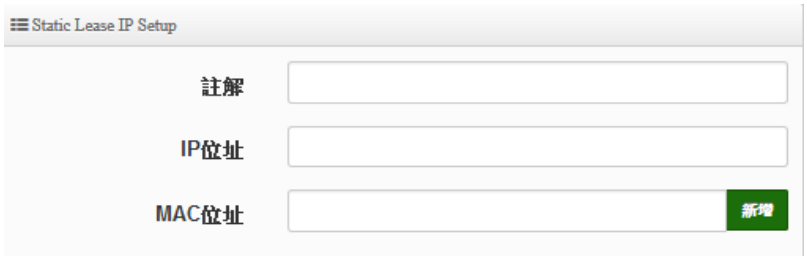
設定 IP 位址自動派送給使用者之功能，請正確設定 IP 位址的派送區間和正確輸入網路的閘道位址及 DNS 伺服器位址

- **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。
- **網域名稱**：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 位址列表將顯示與欄位內

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

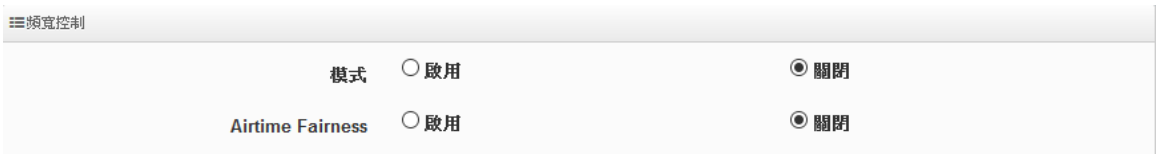


➢ **Static Lease IP List:** 當確認設定 DHCP 伺服器的 IP 位址綁定後，將顯示至此列表欄位上。

4.1.2 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

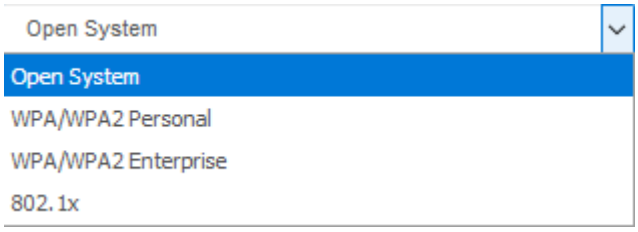


- **模式:** 管理員可以選擇啟用頻寬控制
- **Airtime Fairness:** 能讓 TX/RX 流量能接近平衡，不至於讓上下載流量落差太大(此功能應用較常見的是兩台對等的設備使用 AP+Client 橋接之應用)

- **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

4.1.3 Radio 0(5G)無線基地台

- **無線基地台**：可針對特定的”虛擬網路”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。
- **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。



- **Open System:** 表示此無線基地台不做加密動作。當無線用戶連接至此基地台時，將無須輸入密碼(不建議選用)。

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 Push Button**：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，若選擇 TKIP 加密演算法，將影響 802.11n 的傳送速率，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

- **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。

設定完成後按下「**儲存**」鍵儲存設定，可設定多項功能後再一次性重新啟動，將套用新設定。

4.1.4 MAC 過濾

點選「MAC 過濾設定」將可以進入「MAC 存取控制」設定頁面。過濾規則可分為兩部分

(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。

4.1.5 802.11r 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。

Notice

當建置 802.11r 無線漫遊平台時，此功能啟用則無線使用者設備必須有支援 802.11k 功能，才能正常的運作

在快速漫遊設定這欄位上，需每台 AP 都設相同的值，這樣 AP 與 AP 之間才會認定同一區域

- **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 2 組 16 進為碼，例如輸入 8c4d
- **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 期限**：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。

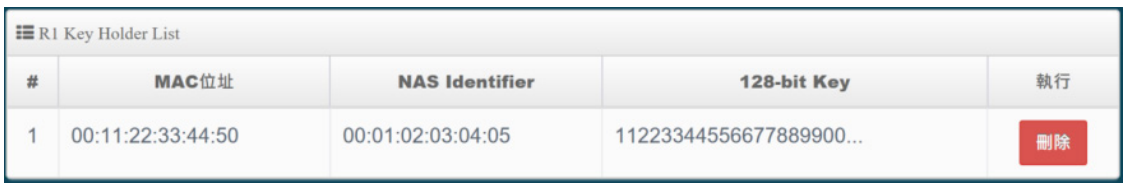
- **MAC 位址**：輸入另一端無線基地台的無線網卡卡號。
- **NAS Identifler**：輸入 AP 的共通 NAS Identifler 網域名稱。
- **128-bit Key**：輸入一組共用的 128-bit Key 碼。

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

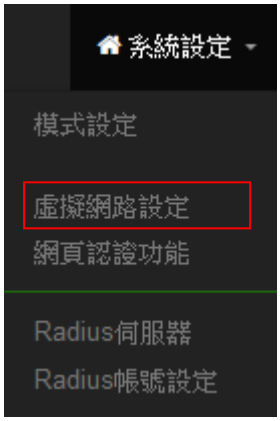


設定完成後，請點擊”**儲存**”按鈕後記得須點擊”**重新啟動**”，完成功能運作。

4.2 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** " 進入設定



Notice

當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 4.1 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

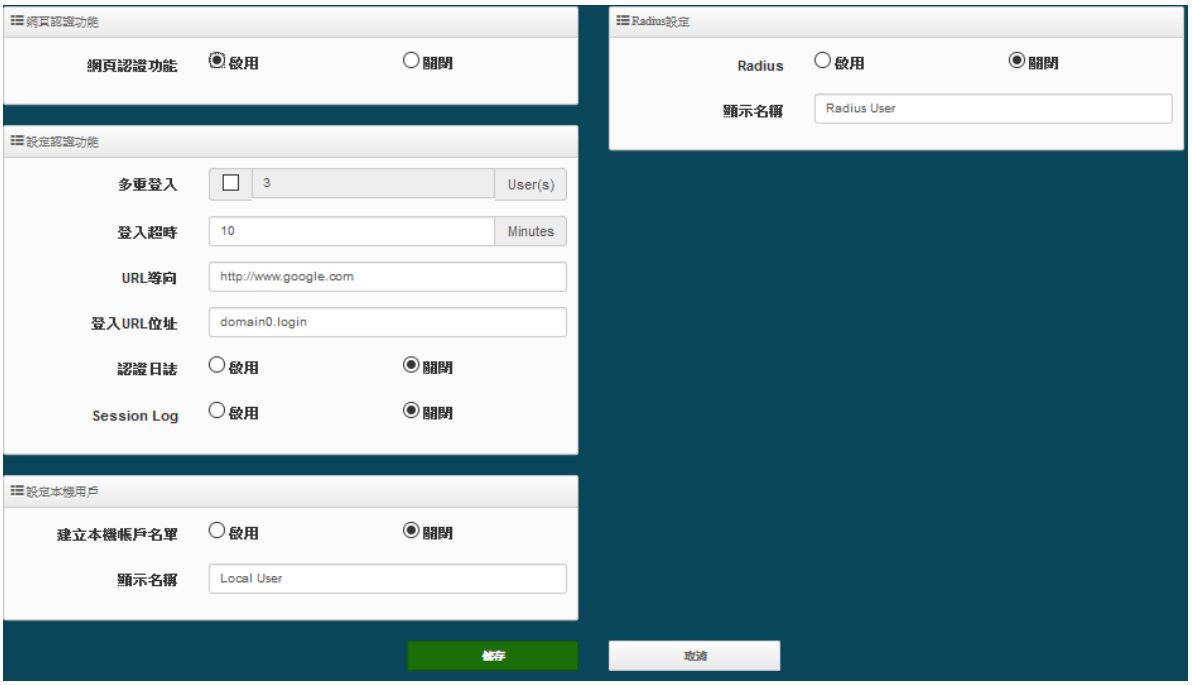
Notice

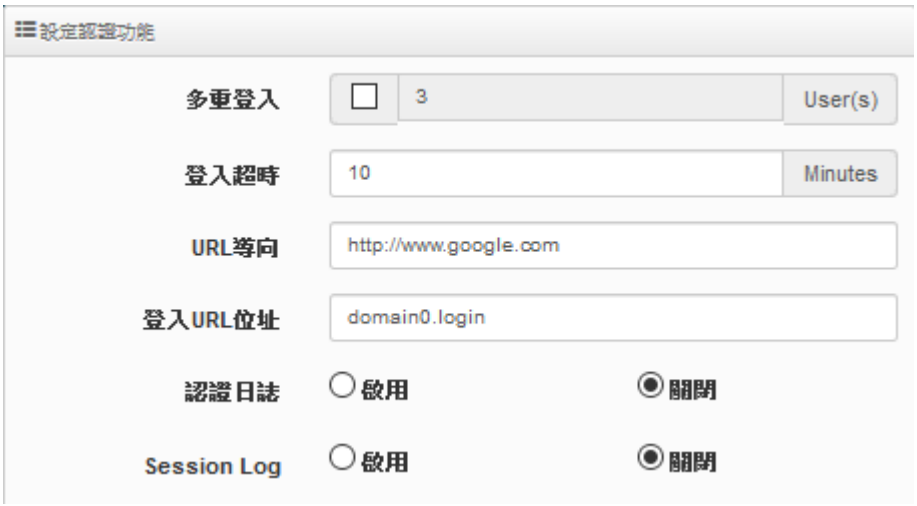
1. 網頁認證功能 按鈕，主要能設定啟用認證功能服務及相關認證服務等
2. 網頁認證功能 下拉功能選單，可設定提供給"遊客"使用、本機帳號、OAuth2.0 認證、網頁登入頁面客製化、登入頁面語系、Walled Garden、特權名單以及將認證功能的設定檔備份或存回套用等等。

4.2.1 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等相關功能

請點擊 網頁認證功能 按鈕進入設定頁面，而當點擊啟用，則如下頁面操作說明

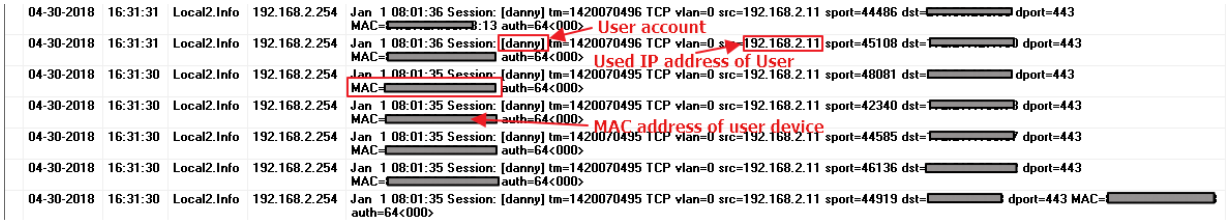




- **多重登入**：當勾選啟用此功能，則同一個帳號能給多人同時登入，同時登入人數可由管理者自行設定， 0 為不限制。
- **登入超時**：當使用者登入後，無進行任何網路行為，無任何流量下，停滯幾分後系統自動讓使用者登出。
- **URL 導向**：使用者網頁登入後，系統自動導向到此設定網站位置。
- **登入 URL 位址**：設定登入頁面的網頁位址。
- **認證日誌:** 當啟用後，所有認證日誌訊息將會發送至遠端 System Log Server 做備份

- **Session Log**：可選擇啟用或關閉，啟用主要是將使用者的上網 Session 資訊存放至遠端 System Log Server 做備份。

認證日誌/Session Log 備存訊息如下提供參考



- **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 4.2.2 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。
- **顯示名稱:** 可設定要顯示至認證畫面的名稱
- **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。

4.2.2 網頁認證功能設定

請點擊 **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、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

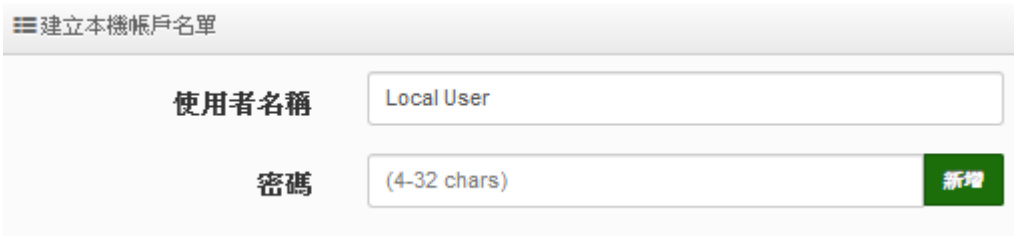
可啟用或停用此服務，此功能主要可以設定網頁認證的遊客免輸入帳密就能享受網路服務資源，管理者則可以限制同時有多少遊客使用，限制遊客時間及使用流量管理等等。

- 服務: 可選擇啟用或關閉此遊客帳戶
- 登入類型: 可選擇一次性或 Multiple Time(多次性)登入
  - **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：**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，直到時間用完。
- **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。

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。

建立本機帳戶

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

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。

OAuth2.0

本系統有設計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。

以下提供基本概念圖示說明

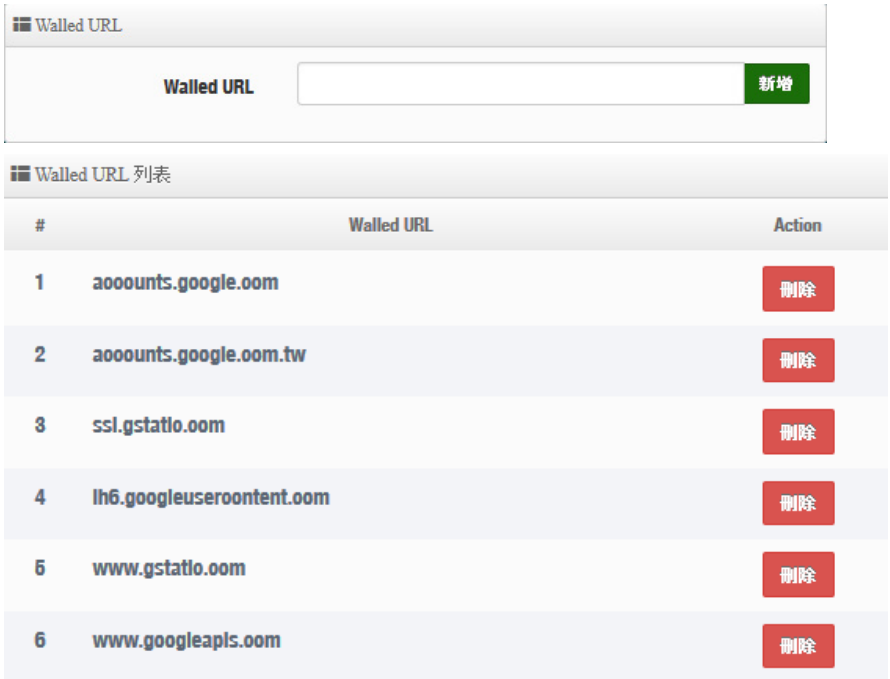
Notice

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 的 OAth2.0 服務頁面設定說明

 # 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。



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

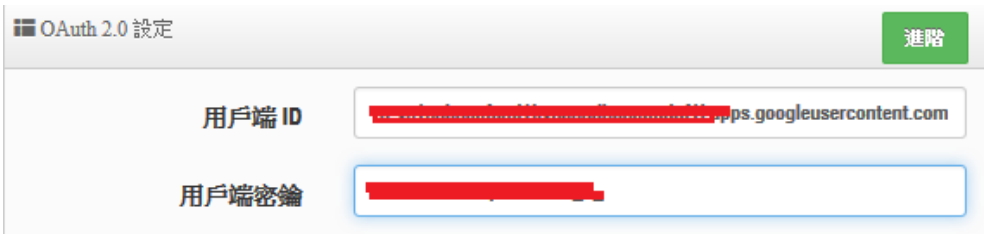
JavaScript ORGINS: http://domain0.login.com

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

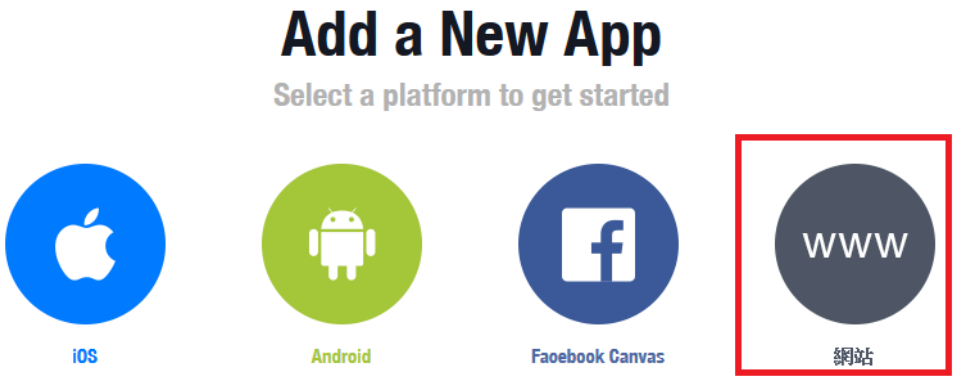
5. 將 ID 與密鑰貼入系統的 google 編輯內的 OAuth2.0 設定下，確認及完成



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。

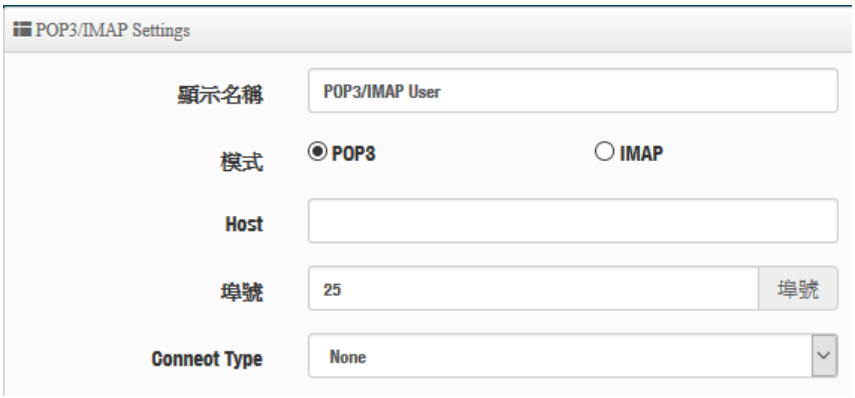
在回系統上設定 Facebook 的用戶 ID 及密鑰

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:

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

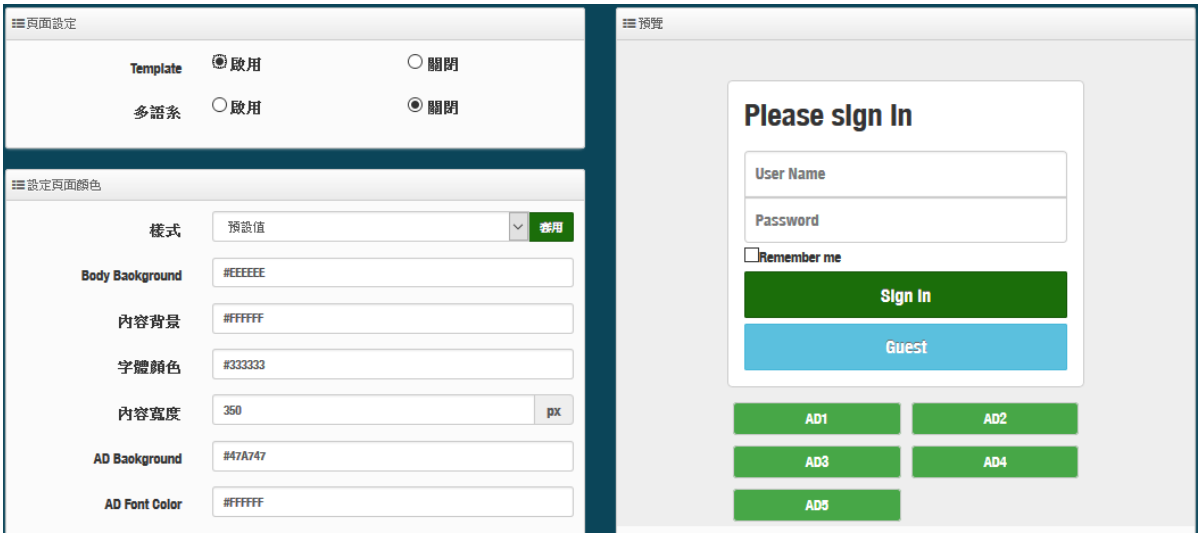


- **顯示名稱:** 管理人員可以自行定義此服務名稱。
- **模式**：選擇 Mail server 的驗證方式
- **Host**：輸入 Mail 伺服器的位址
- **埠號**：輸入 Mail 驗證所使用的埠號
- **Connect Type**：選擇 Mail 伺服器使用的加密類型，系統支援 STARTTLS 和 SSL/TLS 加密

- **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

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

Notice

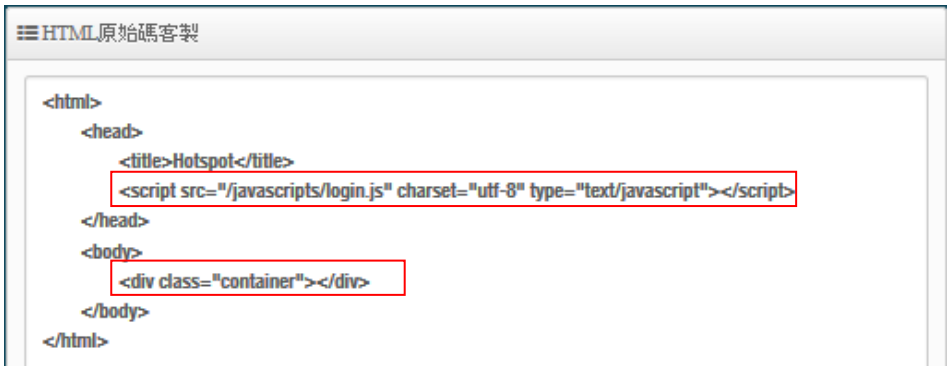
當選擇"啟用"則登入頁面將使用系統預設的格式. 當"關閉"範本則會跳出 HTML 語法，可透過語法自行去編輯登入頁面

- 選擇啟用時，以下對照表提供參考

- 選擇關閉時，可使用 html 和 css 等語法進行編輯

Notice

1. 若當使用 html 和 css 等語法編輯時，建議編輯者有 html 和 css 等的編輯能力，本要公司不支援協助教導語法的使用
2. 自欄位必須在 190 行間之內，若撰寫的 HTML/CSS 等原始碼超過一定的行間下，建議將 CSS 原始碼存放至遠端 Web Server，然後將遠端 web server 的 IP 位址輸入至 Walled Garden 內



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，可參考手冊最下方的技術文件說明

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

語系

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

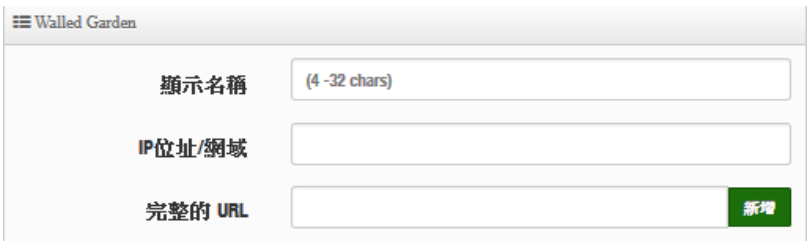
➢ **建立新的語系**：點擊此按鈕可新增不同的語言顯示，如下中文語系基本範例

依訪客為例

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

 # 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(4.2.1 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

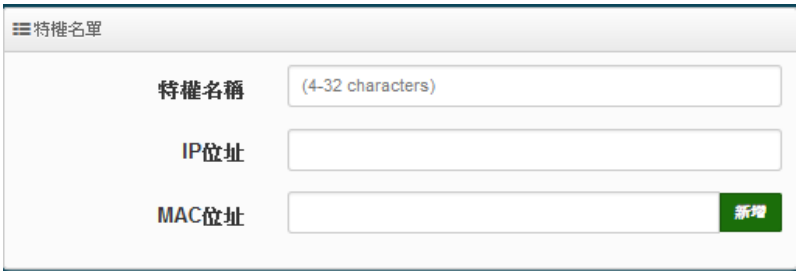
按下新增後，將所設定的網站列入表單內

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

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。

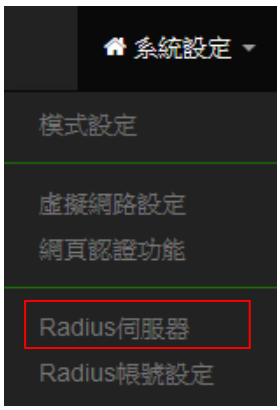
當設定完成後點擊”新增”按鈕來完成設定，確認後記得重新啟動系統讓功能正常運作

設定檔

此功能主要能將已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

- **虛擬網路設定檔:** 每個不同的虛擬網路都有一組個別的網頁認證設定環境，此區主要是備份或者是上傳這虛擬網路所設定的網頁認證的設定值
- **虛擬網路客製化頁面:** 不同虛擬網路的網頁認證頁面，都可以有不同的展示畫面，相對每個認證頁面的語法編輯各有不同，此區主要是備份或者是上傳這虛擬網路所設定的 html 語法.

4.3 RADIUS 伺服器



Notice

此功能只支援在**"無線基地台模式"**下運作

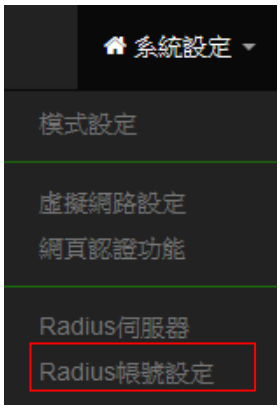
在無線基地台模式下系統已內建標準的 RADIUS 伺服器，且為了讓管理者輕鬆就能架設完成一台 RADIUS 伺服器，已將複雜的架設規則全部由系統自行完成，管理者只要啟用功能則就完成架設一台標準的 RADIUS 伺服器。

- **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，記得按下儲存按鈕並重新啟動系統讓功能正常運作

4.4 RADIUS 帳號設定

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。



Notice

此功能只支援在**"無線基地台模式"**下運作

- **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**：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，並可透過名單進行帳戶刪除動作。

設定完成後，記得按下儲存按鈕並重新啟動系統讓功能正常運作

4.5 無線設定

主要設定 5G 無線基台的運作模式，頻道，無線進階設定，WMM 及 WDS 功能設定等等

4.5.1 Radio 0 設定

- **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**：將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 頻段分別：

1. 5150～5350MHz（CH36、CH40、CH44、CH48、CH56、CH60 、CH64）
2. 5470～5725MHz（CH100、CH104、CH108、CH112、CH116、CH120、CH124、CH128、CH132、CH136、CH140）
3. 5725～5825MHz（CH149、CH153、CH157、CH161、CH165）

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 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；而在 5150～5350MHz 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"。
- **Slot Time:** 若使用點對點橋接下，在不同距離將有不同的等待傳送值，這個值會影響傳送的速率，在系統的設計下內建了公式運算，系統會自動計算出理想值。
  - **距離：**當點下"**距離**"按鈕，將可以輸入點對點的橋接之間的距離,輸入距離以單位(公尺)計算。
- **ACK Timeout**：這與 Slot Time 相關，若等待〝ACKnowledgment frame〞間隔太長將而不被接收，ACK 會重新傳輸，較高的 ACK Timeout 會減少封包 lost，但傳輸效率會較差。

Notice

更改 **Slot Time 和 ACK Timeout** 將會影響傳輸速率，若點對點距離在 1Km 以下建議先不去改變它，可使用預設嘗試。以現場環境為主

HT Physical Mode

- **TX/RX Stream**：出廠預設值為 2 傳送及 2 接收，假若選擇使用 1T1R 時,採用 OW-200 A1 設備請注意外接 N-type 接頭兩個將會有一個無訊號輸出，如下圖說明，請確實安裝

- **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」。

Notice

若非特殊必要，請勿關閉此功能，這將影響傳輸速率品質

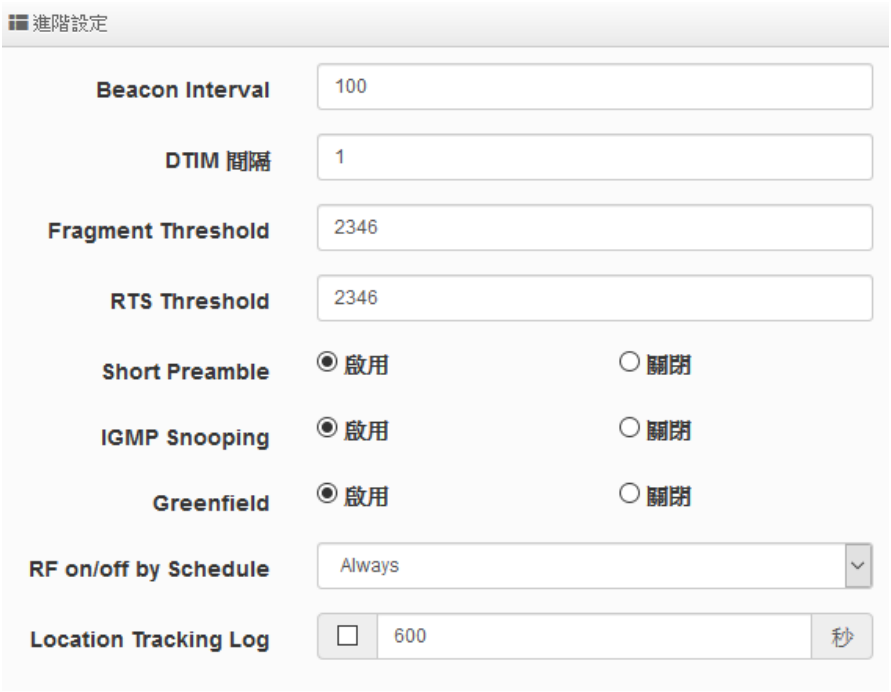
- **Aggregation Frames**：調整封包聚集的訊框大小。
- **封包聚合大小**：調整封包聚集的大小。

Notice

Aggregation Frames / Size 若非特殊必要，請勿修改原先預設值，這將影響傳輸速率品質

設定完成後，記得按下儲存按鈕並重新啟動系統讓功能正常運作

4.5.2 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**：在無線傳輸下用來支援在 layer2 建立和維護 MAC 的 Multicast 地址表，以達到在 layer2 也進行 Multicast。
- **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 on/off by Schedule:** 此功能可以套用時間表讓無線訊號依照時間表自動開啟或關閉, 時間標規則定義請至"系統設定"➔"時間規則"去編輯它。
- **Location Tracking Log:** 此功能可將無線用戶與本機無線基地台之距離(RSSI 計算)資訊提供給遠端數據庫做分析。管理者可設定多少秒傳送一次資訊給數據庫。

```
Jan  1 08:28:00 Wifilogd: tm=1420072080 vlan=0 radio=0 bssid=8c:4d:ea:05:1c:7a climac=[redacted] rssi=-67
Jan  1 08:27:00 Wifilogd: tm=1420072020 vlan=0 radio=0 bssid=8c:4d:ea:05:1c:7a climac=[redacted] rssi=-68
Jan  1 08:26:00 Wifilogd: tm=1420071960 vlan=0 radio=0 bssid=8c:4d:ea:05:1c:7a climac=[redacted] rssi=-67
```

Notice

Location Tracking Log 只負責提供無線用戶位置資訊給數據庫，此應用可由無線用戶的所在位置反推出本機無線基地台的方位。

設定完成後，記得按下儲存按鈕並重新啟動系統讓功能正常運作

4.5.3 WMM 頻寬最佳化設定

- **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。

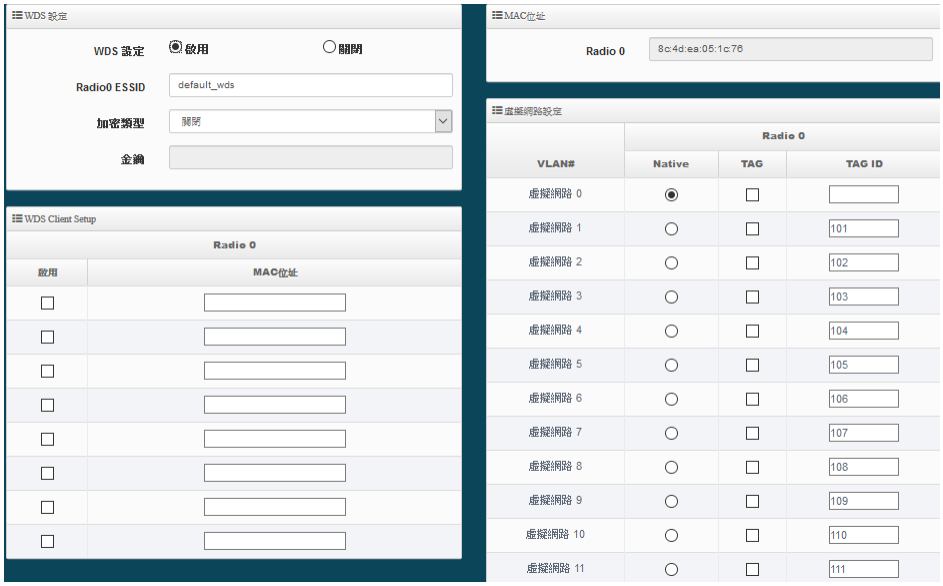
- **TxOP Limit**：Transmission Opportunity，這個傳送機會，對於在資料傳輸中需要較高優先權的 AC_VI 與 AC_VO，您可以設定較大的數值以便取得較高的傳送優先權。
- **ACM bit**：Admission Control Mandatory，ACM 只適用於 AC_VI 及 AC_VO,當這個功能沒有被選取時,則由連接中的無線基地台來負責 ACM,反之 ,當這個功能被選取時,則由用戶端來負責。
- **No ACK policy bit**：不選取時，表示無線基地台透過無線連線傳輸 WMM 封包時，將會回應傳輸需求，可確保對方一定收到 WMM 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，記得按下儲存按鈕並重新啟動系統讓功能正常運作

4.5.4 WDS 設定

使用 AP+WDS 功能時兩端的無線基地台必須同時都要支援 WDS 功能，且**兩端無線基地台必須互相設定對方的無線介面的 MAC 位址**，換句話說每一個基地台都必須包含需要 WDS 連線的各點基地台 MAC 位址，同時您必須確認各 WDS 基地台都必須使用**相同無線網路名稱**、**頻道**以及**無線加密方式**。

當啟用 WDS 功能時最多橋接數共 8 組，在 WDS 功能支援 VLAN tag 傳送，若在網域內有設定 Tag 時，WDS 將可把多組 Tag 帶至另一個橋接端點。



- **Radio 0 ESSID:** 可設定 WDS 識別名稱
- **加密類型:** WDS 點對點傳輸可使用 AES 加密方式。
- **WDS Client Setup**：欄位中輸入橋接端的無線基地台 MAC 位址。
  例如 A 與 B 點個無線基地台做 WDS 點對點傳輸，則 A 點須設定 B 點的 MAC 位址，相對的 B 點設定 A 點的 MAC 位址。
- **虛擬網路設定**:此欄位主要是在架構中可能有多個 VLAN Tag 需透過此 WDS 點對點傳輸，請確認勾選要傳輸的 VLAN Tag 碼，此時 VLAN Tag 才能順利在 WDS 中分辨
  - **VLAN#**：顯示 AP 的所有的虛擬網路。
  - **Native**：可選擇要使用哪個虛擬網路來做 WDS 橋接。
  - **TAG**：可勾選多組 tag 的封包。
  - **TAG ID**：設定 VLAN Tag 的 ID 值。

設定完成後，記得按下儲存按鈕並重新啟動系統讓功能正常運作

4.5.5 WDS 狀態

顯示 5G 的 WDS 連線狀態資訊

- **MAC 位址**：顯示另外一端的無線基地台 MAC 位址資訊。
- **Rate(TX/RX)**：顯示 WDS 的上/下載流量資訊。
- **RSSI:** 顯示點對點橋接的連線訊號品質，數值越高表示連接訊號越強

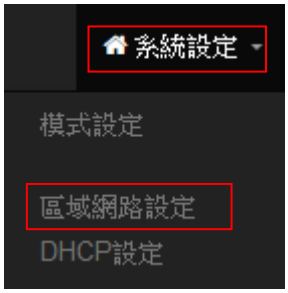
Notice

RSSI 值過高，表示無線基地台太近對設備和傳輸速率將其反效果，若 RSSI 值太低表示訊號對應不良，則傳輸品質相對較差，建議 RSSI 值在 40~60 之間是最好的

5. Client Bridge 模式

若管理者需要橋接或延伸無線基地台訊號時，假若設備不支援 WDS 橋接功能，管理者可啟動為 Client Bridge 模式，利用此模式與上端 AP 做網路連接後在透過 Repeater AP 功能去延伸無線基地台。以下介紹 Client Bridge 模式及 Repeater AP 設定。

5.1 區域網路設定



當切換為 Client Bridge 模式後，管理者必須先設定系統的 IP 位址，網段必須與內部網域相同，而 IP 位址不可衝突。

區域網路連線類型

- **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。
  - **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。

靜態 IP 位址：

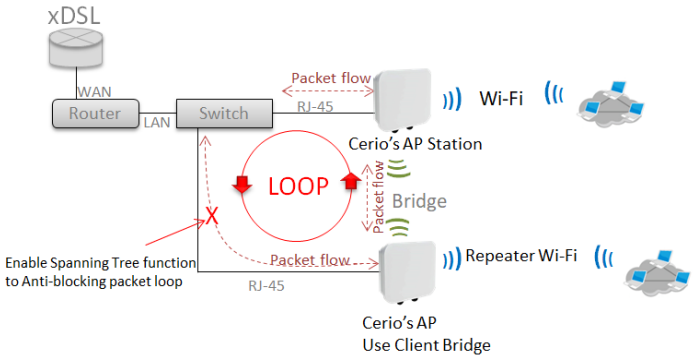
- **IP 位址**：設定系統的 IP 位址。
- **子網路遮罩**：設定 IP 的子網路遮罩。
- **預設閘道**：設定網域的閘道位址。

DNS：

- **主要/次要 DNS 伺服器**：可設定網域名稱解析的 IP 位址。

802.1d Spanning Tree：

➢ 可啟用或關閉 Spanning Tree 功能。**802.1d Spanning Tree** 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。



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。

5.2 DHCP 設定

CERIO 的 CenOS5.0 軟體內建 DHCP 伺服器，管理人員可透過此功能派送 IP 位址給使用者。假若環境已確實有 DHCP 伺服器在派送 IP 時，為了避免衝突，可將系統的 DHCP 伺服器功能關閉，或是啟用分派 DHCP 的 IP 位址。假若環境內無任何 DHCP 伺服器，則可透過此功能啟用，進行虛擬 IP 派發。

請點選 **”系統設定”➔”DHCP 設定”** 下啟用 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

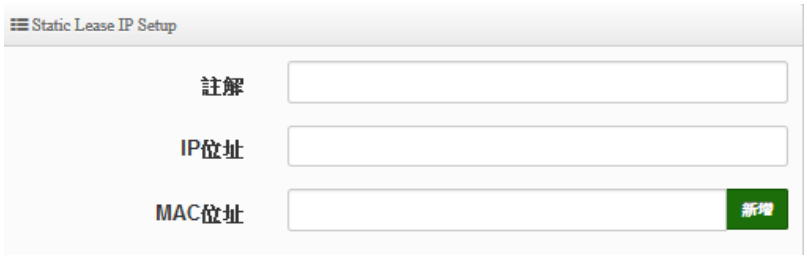
- **DHCP 服務:** 管理人員可以選擇啟動或關閉此服務，當關閉此功能則系統將不會自動派送 IP 位址給使用者。

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。
- **網域名稱**：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 位址列表將顯示與欄位內

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



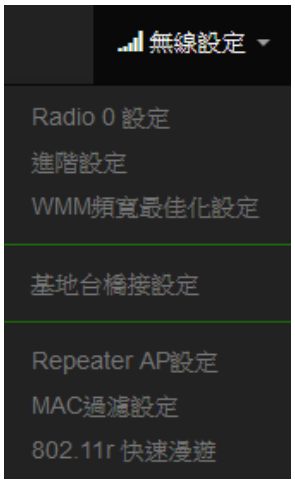
- **Static Lease IP List:** 當確認設定 DHCP 伺服器的 IP 位址綁定後，將顯示至此列表欄位上。

Static Lease IP List

#	註解	IP位址	MAC位址	執行
-	-	-	-	-

5.3 無線設定

當使用 Client Bridge 模式後，此功能頁面主要設定與上端 AP 連接的一些基本設定值，若有需要將設備建立虛擬的無線基地台，則可在此選單上啟用 Repeater AP 功能，達到訊號再延伸之概念
可參考手冊 2.2 項的 Client Bridge + Repeater AP 之基本應用圖解



Notice

1. 當 Client Bridge 與 AP 做連接時，請注意本設備的 IP 位址需要與 AP 端區網相同，且 IP 位址請勿相同造成衝突
2. Repeater AP 與 Client Bridge 屬於父子關係，也就是說，當要使用 Repeater AP 功能時必須確認 Client Bridge 跟 AP 間是正常運作, Repeater AP 才可正常，否則 Repeater AP 將不成立

5.3.1 Radio 0

- **MAC 位址:** 顯示本機的無線網卡 MAC 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。
- **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，最大功率為等級 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"。

- **Slot Time:** 若使用點對點橋接下，在不同距離將有不同的等待傳送值，這個值會影響傳送的速率，在系統的設計下內建了公式運算，系統會自動計算出理想值。
  - **距離：**當點下”**距離**”按鈕，將可以輸入點對點的橋接之間的距離,輸入距離以單位(公尺)計算。
- **ACK Timeout**：這與 Slot Time 相關，若等待〝ACKnowledgment frame〞間隔太長將而不被接收，ACK 會重新傳輸，較高的 ACK Timeout 會減少封包 lost，但傳輸效率會較差。

Notice

更改 **Slot Time 和 ACK Timeout** 將會影響傳輸速率，若點對點距離在 1Km 以下建議先不去改變它，可使用預設嘗試。以現場環境為主

HT Physical Mode

- **TX/RX Stream**：出廠預設值為 2 傳送及 2 接收，假若選擇使用 1T1R 時，請注意外接 N-type 接頭兩個將會有一個無訊號輸出，如下圖說明，請確實安裝

- **頻道模式：**使用 5Ghz 在標準規範下將提供 20Mhz 或 20/40 和 80Mhz 選擇，作為基地台與無線用戶之間傳輸的頻帶頻寬與速度。
- **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」。

Notice

若非特殊必要，請勿關閉此功能，這將影響傳輸速率品質

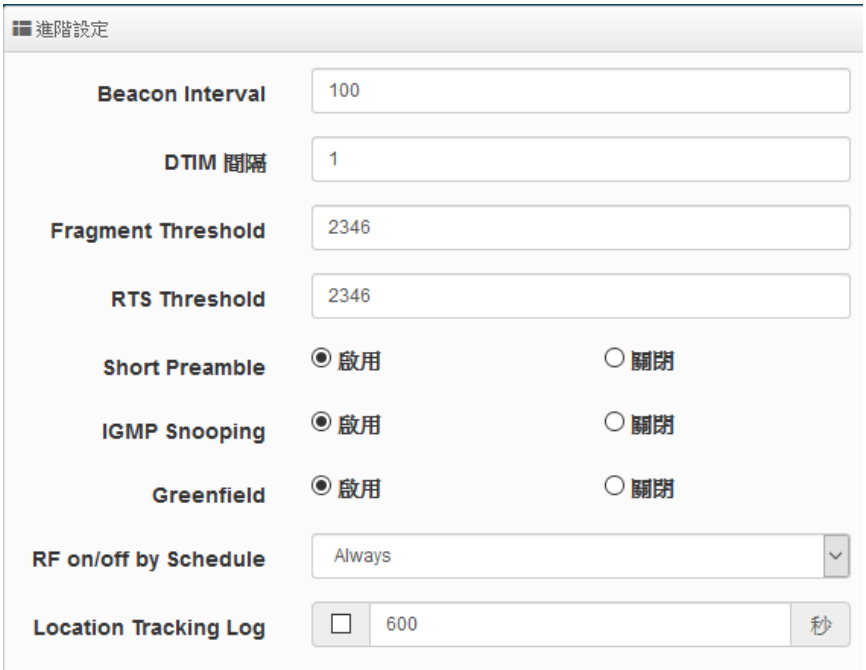
- **Aggregation Frames**：調整封包聚集的訊框大小。
- **封包聚合大小**：調整封包聚集的大小。

Notice

Aggregation Frames / Size 若非特殊必要，請勿修改原先預設值，這將影響傳輸速率品質

設定完成後，記得按下儲存按鈕並重新啟動系統讓功能正常運作

5.3.2 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 間隔**：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**：在無線傳輸下用來支援在 layer2 建立和維護 MAC 的 Multicast 地址表，以達到在 layer2 也進行 Multicast。

- **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 on/off by Schedule:** 此功能可以套用時間表讓無線訊號依照時間表自動開啟或關閉，時間標規則定義請至"系統設定"➔"時間規則"去編輯它。
- **Location Tracking Log:** 此功能可將無線用戶與本機無線基地台之距離(RSSI 計算)資訊提供給遠端數據庫做分析。管理者可設定多少秒傳送一次資訊給數據庫。

```
Jan  1 08:28:00 Wifilogd: tm=1420072080 vlan=0 radio=0 bssid=8c:4d:ea:05:1c:7a climac=[redacted] rssi=-67
Jan  1 08:27:00 Wifilogd: tm=1420072020 vlan=0 radio=0 bssid=8c:4d:ea:05:1c:7a climac=[redacted] rssi=-68
Jan  1 08:26:00 Wifilogd: tm=1420071960 vlan=0 radio=0 bssid=8c:4d:ea:05:1c:7a climac=[redacted] rssi=-67
```

Notice

Location Tracking Log 只負責提供無線用戶位置資訊給數據庫，此應用可由無線用戶的所在位置反推出本機無線基地台的方位。

5.3.3 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。

5.3.4 基地台橋接設定

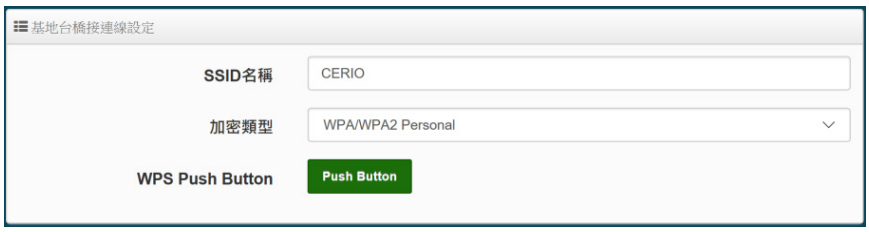
可點選**"搜尋站台"**按鈕選擇欲想要連接的無線基地台，找到要連接的無線站台後點擊**"設定"**按鈕，則可設定要橋接的無線站台資訊，如設定連接密碼等。若管理人員已經知道無線站台的 SSID 名稱及加密方式等，可不需透過**搜尋站台功能**，可直接手動增加無線基地台的 SSID 及加密方式等。

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**：顯示實際環境中無線基地台的名稱(大多數是基地台的無線 MAC)。
- **ESSID**：顯示無線基地台名稱。
- **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，不透過搜尋站台功能，則管理者可手動輸入已知的 SSID 名稱及密碼至欄位即可。



Pass Phrase Settings：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。

- **WPA 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。

5.3.5 Repeater AP 設定

Notice

1. Repeater AP 功能若要正常運作基本前提須要確認 Client Bridge 是正常的與 AP 連接並正常運作
2. Repeater AP 功能在預設值下是啟用，若只單純做 Client Bridge 橋接,不想使用 Repeater AP 這功能，建議關閉

- **無線基地台**：關閉或啟用 Repeater AP(延伸基地台)功能服務。預設為開啟
- **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，最大支援同時 64 個使用者存取同一個 SSID。建議最高連線人數 60 人以下。
- **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。

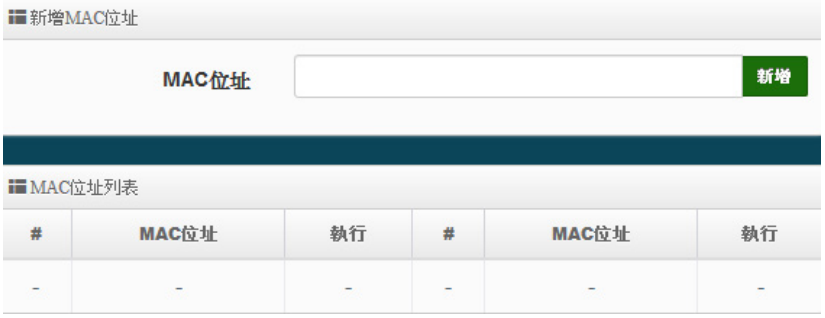
5.3.6 MAC 位址過濾

此無線的 MAC 過濾只針對無線 Client 要連上 Repeater AP 時做 MAC 的過濾條件

MAC 過濾條件分別有兩種類型

(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。

5.3.7 802.11r 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。

Notice

當建置 802.11r 無線漫遊平台時，此功能啟用則無線使用者設備必須有支援 802.11k 功能，才能正常的運作

在快速漫遊設定這欄位上，需每台 AP 都設相同的值，這樣 AP 與 AP 之間才會認定同一區域

- **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 2 組 16 進為碼，例如輸入 8c4d
- **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 期限**：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。

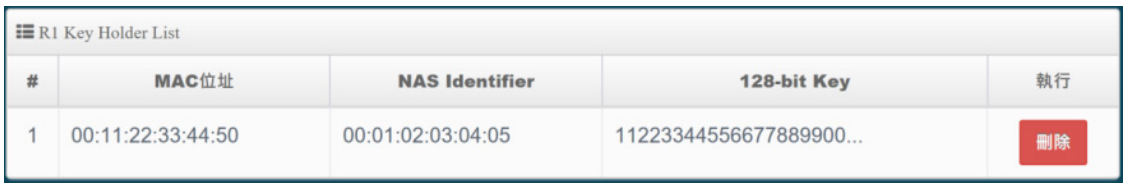
- **128-bit Key**：輸入一組共用的 128-bit Key 碼。

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



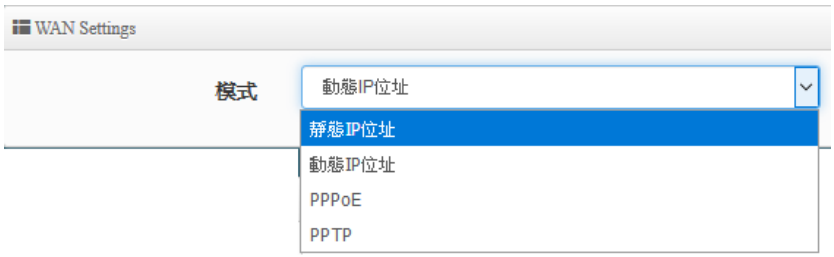
設定完成後，請點擊”**儲存**”按鈕後記得須點擊”**重新啟動**”，完成功能運作。

6. WISP 模式

啟動了 WISP 模式後，則系統將改變為 Router 功能，不同地方是 WAN 連接方式則是透過無線方式做連接，其他運作方式與 Router 相同。

6.1 WAN 設定

當切換成 WISP 模式後，無線訊號的橋接為 WAN 端，WAN 設定可選擇”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。

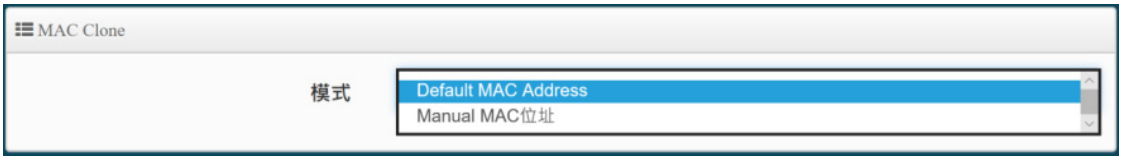
➢ **PPPoE**：主要設定 PPPoE 撥號連線帳號與密碼等，此帳密由 ISP 業者提供

- **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 長度為最佳值。
- **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。

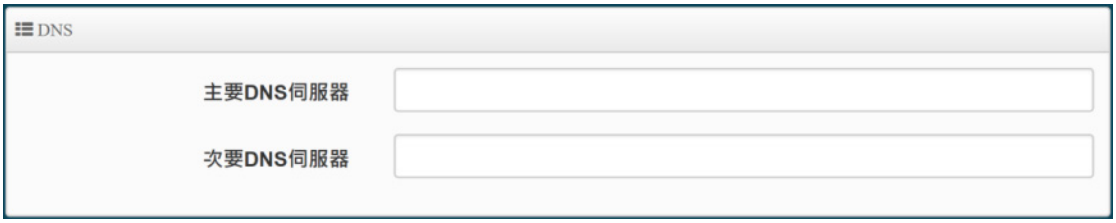
- **使用者名稱**：輸入 PPTP 驗證的使用者名稱。
- **密碼**：輸入 PPTP 驗證的密碼。
- **PPTP**：輸入遠端連接的 PPTP 伺服器位址。
- **WAN IP**：輸入連接使用的 IP 位址。
- **子網路遮罩**：輸入 WAN IP 的子網路遮罩。
- **MTU**：PPTP 使用最佳的封包長度，預設為 1460。
- **MPPE40**：點對點的加密使用 40 位元。
- **MPPE128**：點對點的加密使用 128 位元。
- **Reconnect Mode:** 可分為 Always On / On demand / 手動等 3 種模式。
  - ✓ **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**：網卡卡號共用分享。



- **Default MAC Address**：使用預設本機 MAC 位址對外。
- **手動指定 MAC 位址** ：由管理者自行設定一組對外 MAC 位址。

➢ **DNS :** 設定網址解析的伺服器位址。

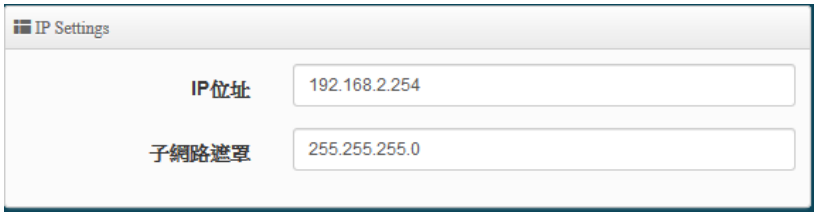


設定完成後，請點擊”**儲存**”按鈕後記得須點擊”**重新啟動**”，完成功能運作。

6.2 區域網路

區域網路設定頁面主要設置本機的 LAN IP 位址及子網路遮罩，在 LAN 應用上也支援 802.1d Spanning Tree 功能。

請點擊”**系統設定**” ➔ ”**LAN 設定**”進入頁面設定



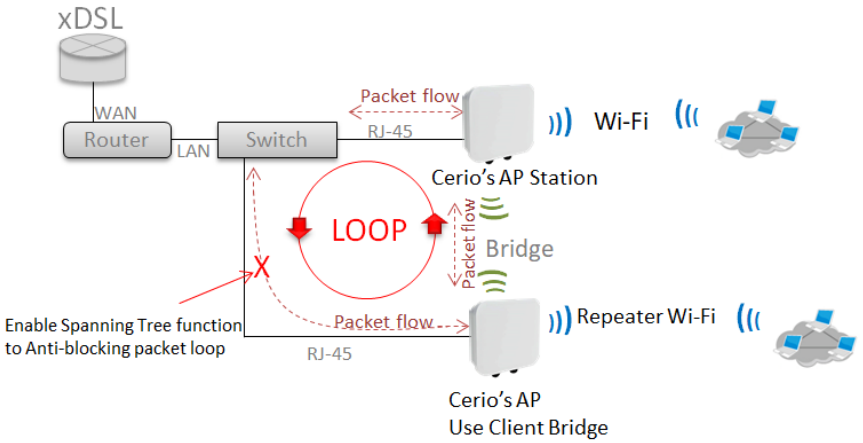
IP Settings:

➢**IP 位址**：設定本機主要的 LAN IP 位址。

➢**子網路遮罩**：設定 LAN IP 的子網路遮罩，出廠預設值為 255.255.255.0。

802.1d Spanning Tree：

Spanning Tree Protocol 簡稱為 STP，啟用此功能需要上端或是與基地台相連接的網路設備都有支援此通訊協定，主要避免基地台乙太網路線雙重連接至相同的一台網路設備時導致網路傳送資料迴圈，而將會造成整個網路無法正常運作，例如：當管理者使用 WDS 功能與其他遠端的無線基地台互相連結時發生迴圈造成網路無法正常運作（如下圖所示），開啟此功能將可以避免此問題發生。



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 DHCP 設定

假若環境已確實有 DHCP 伺服器在派送 IP 時，為了避免衝突，可將系統的 DHCP 伺服器功能關閉，或是啟用分派 DHCP 的 IP 位址。假若環境內無任何 DHCP 伺服器，則可透過此功能啟用，進行虛擬 IP 派發。

請點選”**系統設定**”➔”**DHCP 設定**”下啟用 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

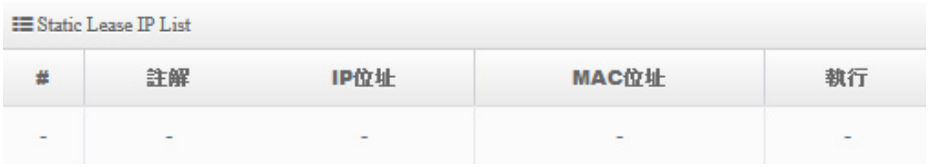
- **DHCP 服務:** 管理人員可以選擇啟動或關閉此服務，當關閉此功能則系統將不會自動派送 IP 位址給使用者。

  - **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。
  - **網域名稱**：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 位址列表將顯示與欄位內

- **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。



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 無線設定

此功能頁面主要設定連線 Wi-Fi WAN 端的無線橋接方式，管理者可選擇要使用 5G 的頻率與上端基地台橋接(依照上端頻率決定)，調整無線基地台的相關功能，同時可設定 Repeater AP(LAN)無線基地台的功能，及使用 MAC 過濾和無線快速漫遊等功能。

6.4.1 Radio 0

- **MAC 位址:** 顯示本機的無線網卡 MAC 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。
- **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，最大功率為等級 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”。
- **Slot Time:** 若使用點對點橋接下，在不同距離將有不同的等待傳送值，這個值會影響傳送的速率，在系統的設計下內建了公式運算，系統會自動計算出理想值。
  - **距離：**當點下” **距離**”按鈕，將可以輸入點對點的橋接之間的距離,輸入距離以單位(公尺)計算。

- **ACK Timeout**：這與 Slot Time 相關，若等待〝ACKnowledgment frame〞間隔太長將而不被接收，ACK 會重新傳輸，較高的 ACK Timeout 會減少封包 lost，但傳輸效率會較差。

Notice

更改 **Slot Time 和 ACK Timeout** 將會影響傳輸速率，若點對點距離在 1Km 以下建議先不去改變它，可使用預設嘗試。以現場環境為主

HT Physical Mode

- **TX/RX Stream**：出廠預設值為 2 傳送及 2 接收，假若選擇使用 1T1R 時，請注意外接 N-type 接頭兩個將會有一個無訊號輸出，如下圖說明，請確實安裝

- **頻道模式**：使用 5Ghz 在標準規範下將提供 20Mhz 或 20/40 和 80Mhz 選擇，作為基地台與無線用戶之間傳輸的頻帶頻寬與速度。
- **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」。

Notice

若非特殊必要，請勿關閉此功能，這將影響傳輸速率品質

- **Aggregation Frames**：調整封包聚集的訊框大小。

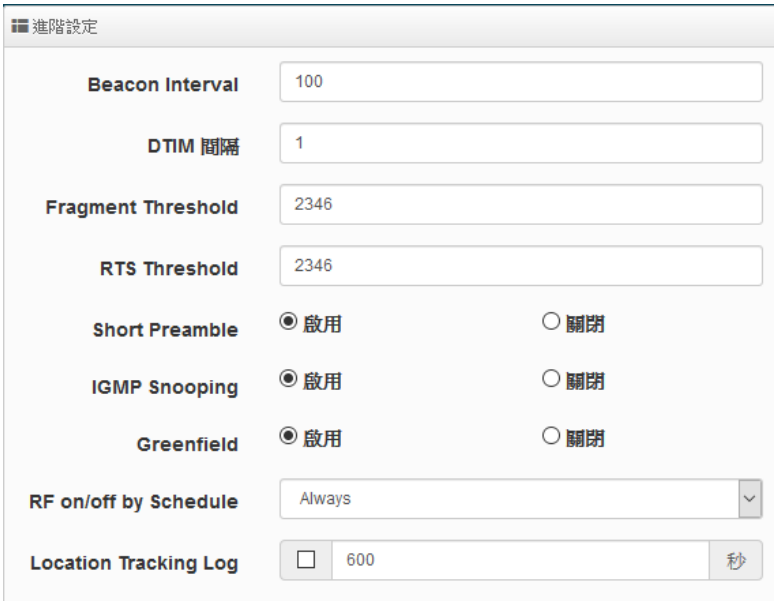
- **封包聚合大小：**調整封包聚集的大小。

Notice

Aggregation Frames / Size 若非特殊必要，請勿修改原先預設值，這將影響傳輸速率品質

設定完成後，記得按下儲存按鈕並重新啟動系統讓功能正常運作

6.4.2 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 間隔**：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**：在無線傳輸下用來支援在 layer2 建立和維護 MAC 的 Multicast 地址表，以達到在 layer2 也進行 Multicast。
- **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 on/off by Schedule:** 此功能可以套用時間表讓無線訊號依照時間表自動開啟或關閉，時間標規則定義請至”系統設定”➔”時間規則”去編輯它。
- **Location Tracking Log:** 此功能可將無線用戶與本機無線基地台之距離(RSSI 計算)資訊提供給遠端數據庫做分析。管理者可設定多少秒傳送一次資訊給數據庫。

```
Jan  1 08:28:00 Wifilogd: tm=1420072080 vlan=0 radio=0 bssid=8c:4d:ea:05:1c:7a climac=[redacted] rssi=-67
Jan  1 08:27:00 Wifilogd: tm=1420072020 vlan=0 radio=0 bssid=8c:4d:ea:05:1c:7a climac=[redacted] rssi=-68
Jan  1 08:26:00 Wifilogd: tm=1420071960 vlan=0 radio=0 bssid=8c:4d:ea:05:1c:7a climac=[redacted] rssi=-67
```

Notice

Location Tracking Log 只負責提供無線用戶位置資訊給數據庫，此應用可由無線用戶的所在位置反推出本機無線基地台的方位。

設定完成後，記得按下儲存按鈕並重新啟動系統讓功能正常運作

6.4.3 WMM 頻寬最佳化設定

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。

6.4.4 基地台橋接設定

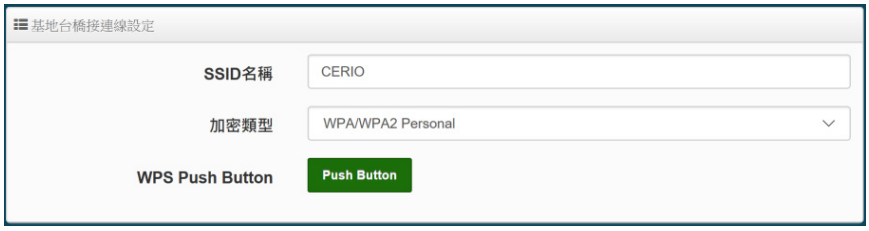
可點選**"搜尋站台"**按鈕選擇欲想要連接的無線基地台(xDSL)，找到要連接的無線站台後點擊 **"設定"** 按鈕，則可設定要橋接的無線站台資訊，如設定連接密碼等。若管理人員已經知道無線站台的 SSID 名稱及加密方式等，可不需透過**搜尋站台功能**，可直接手動增加無線基地台的 SSID 及加密方式等。

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：**顯示實際環境中無線基地台的名稱(大多數是基地台的無線 MAC)。
- **ESSID：**顯示無線基地台名稱。
- **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，不透過搜尋站台功能，則管理者可手動輸入已知的 SSID 名稱及密碼至欄位即可。



Pass Phrase Settings：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。

- **WPA 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。

6.4.5 Repeater AP 設定

Notice

1. Repeater AP 功能若要正常運作基本前提須要確認 Client Bridge 是正常的與 AP 連接並正常運作
2. Repeater AP 功能在預設值下是啟用，若只單純做 Client Bridge 橋接,不想使用 Repeater AP 這功能，建議關閉

- **無線基地台**：關閉或啟用 Repeater AP(延伸基地台)功能服務。預設為開啟
- **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，最大支援同時 64 個使用者存取同一個 SSID。建議最高連線人數 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。

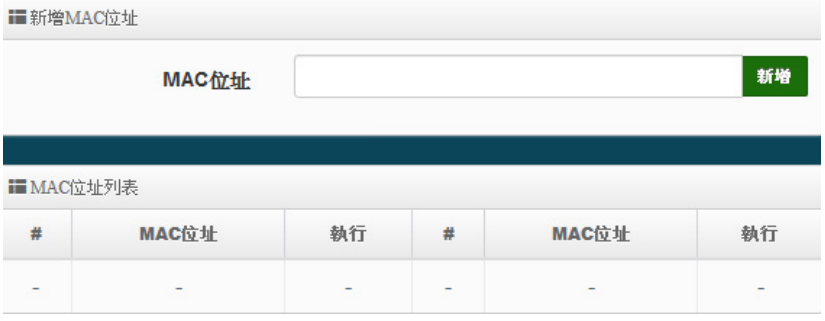
6.4.6 MAC 位址過濾

此無線的 MAC 過濾只針對無線 Client 要連上 Repeater AP 時做 MAC 的過濾條件

MAC 過濾條件分別有兩種類型

(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。

6.4.7 802.11r 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。

Notice

當建置 802.11r 無線漫遊平台時，此功能啟用則無線使用者設備必須有支援 802.11k 功能，才能正常的運作

在快速漫遊設定這欄位上，需每台 AP 都設相同的值，這樣 AP 與 AP 之間才會認定同一區域

- **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 2 組 16 進為碼，例如輸入 8c4d
- **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 期限**：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。

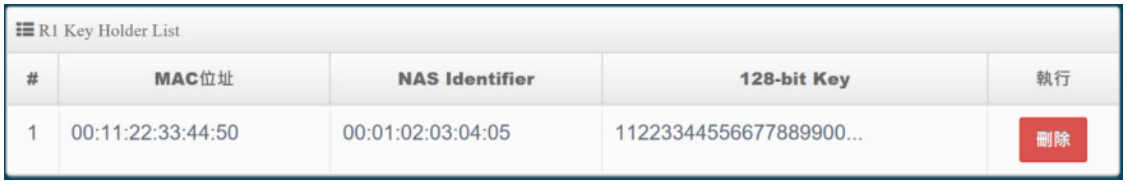
- **128-bit Key**：輸入一組共用的 128-bit Key 碼。

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



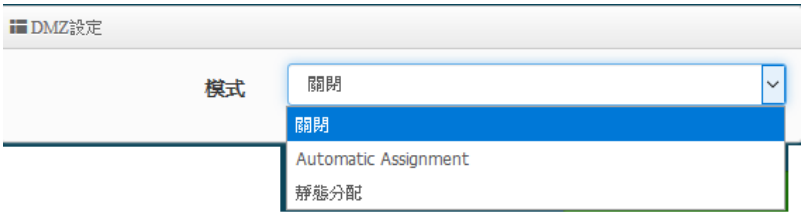
設定完成後，請點擊”**儲存**”按鈕後記得須點擊”**重新啟動**”，完成功能運作。

6.5 進階

主要設定基本的路由安全功能，包含 DMZ / IP 和 MAC 過濾 / 虛擬伺服器及相關存取控制管理(基本防火牆規則)等等

6.5.1 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。



本系統有 2 種 DMZ 類型，分別為 Automatic Assignment(自動分配) 及 Static Assignment(靜態分配)等。

- **Automatic Assignment**：自動分配主要是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。

6.5.2 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。

點擊編輯按鈕進入設定過濾條件

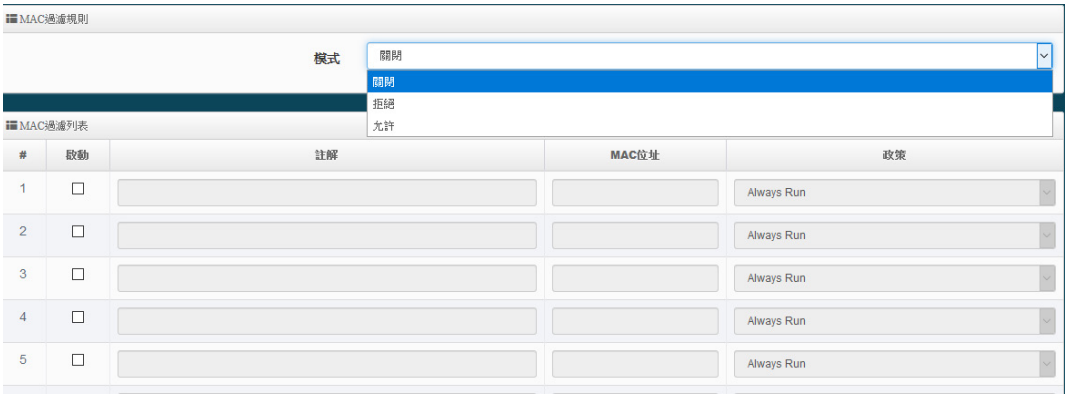
- **啟動**：管理人員可以啟動或關閉 IP 過濾條件。
- **註解**：管理人員可設定此條件的描述。
- **政策**：管理人員可設定此條件是要阻擋或是通行。
- **流入/流出**：管理人員可以選擇 IP 流向屬於流入或是流出。
- **通訊協定**：可選擇網路通訊協定屬性。

- **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。

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。

6.5.3 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。
- **政策**：可依照時間規則來設定時間點進行運作。

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。

6.5.4 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。


虛擬伺服器列表

#	啟動	註解	通訊協定	外部公共埠號	內部伺服器IP位址	內部伺服器埠號	編輯
1	InActive	-	TCP	-	-	-	編輯
2	InActive	-	TCP	-	-	-	編輯
3	InActive	-	TCP	-	-	-	編輯
4	InActive	-	TCP	-	-	-	編輯
5	InActive	-	TCP	-	-	-	編輯

- **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。

6.5.5 存取控制

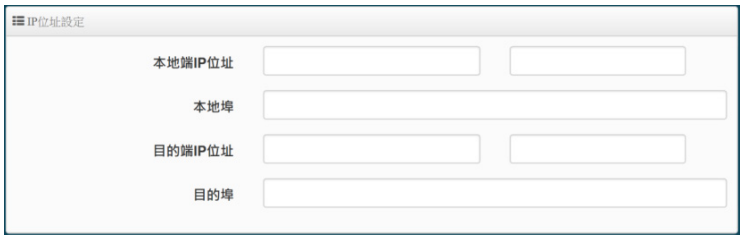
此功能將可以讓網管人員限制或允許網路使用者成員或公司員工上網行為，透過此基本防火牆規則方式進行以「通訊協定」、「網域或關鍵字」或是「應用程式」進行阻擋或允許。可設定 20 筆管理規則。

管理員可點擊 **編輯** 按鈕，進入設定頁面。

存取控制規則：

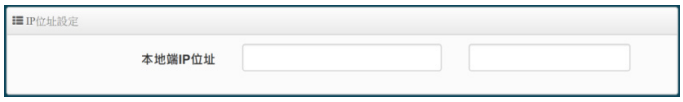
- **啟動**：可選擇啟動或關閉功能。
- **描述**：可輸入此規則描述。
- **通訊協定**：可選擇要過濾的通訊協定。

- **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。



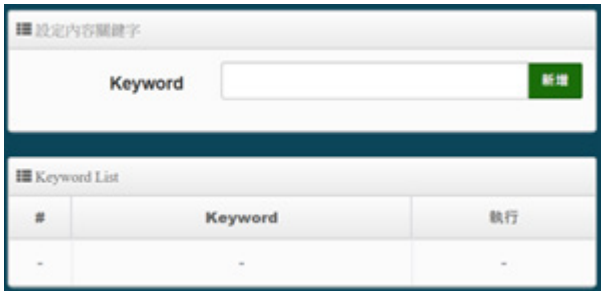
- ✓ **本地端 IP 位址:** 輸入要管理的本地端 IP 位址或 IP 區間。
- ✓ **本地埠**：輸入要管理的本地埠，若要設定區間可用”**:**”表示，例如(1:65535)。
- ✓ **目的端 IP 位址**：輸入目的端 IP 位址或 IP 區間。
- ✓ **目的埠**：輸入要管理的目的埠，若要設定區間可用”**:**”表示，例如(1:65535)。

- **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。



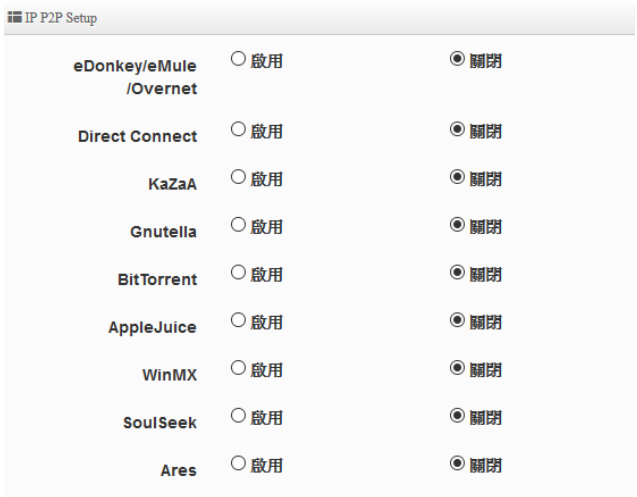
- ✓ **本地端 IP 位址:** 輸入要管理的本地端 IP 位址或 IP 區間。
- ✓ **本地埠**：輸入要管理的本地埠，若要設定區間可用”**:**”表示，例如(1:65535)。
- ✓ **目的端 IP 位址**：輸入目的端 IP 位址或 IP 區間。

- ✓ **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)

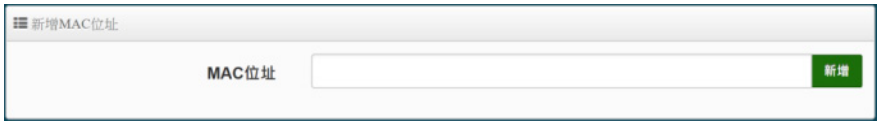
- **網域名稱過濾：**

  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**：系統已預設有多筆 P2P 應用程式，管理人員可針對特定 P2P 軟體進行管理應用程式。



- ➢ **設定 MAC 位址**：管理員可針對特定的 MAC 去做條件過濾。

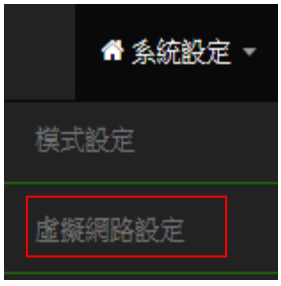


設定完成後，請點擊”**儲存**”按鈕後記得須點擊”**重新啟動**”，完成功能運作。

7. CAP 模式

此 CAP 模式主要是可以集中控管所有 CenOS5.0 核心的無線基地台。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。

7.1 虛擬網路設定



此頁面可啟用或關閉多組的虛擬區域網路並設定閘道位址、DNS 、VLAN Tag 和 spanning Tree 等等相關功能。

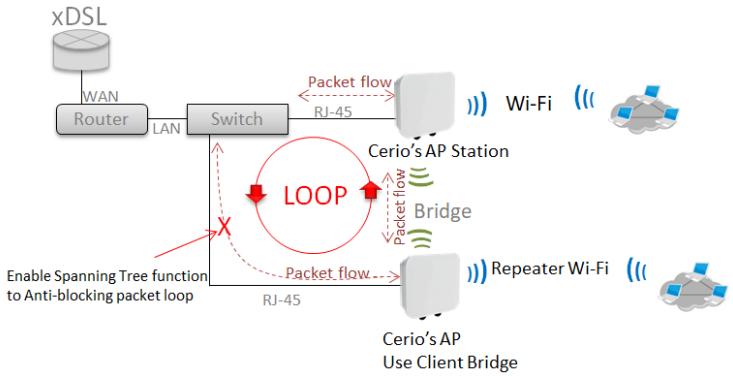
虛擬網路列表

#	系統狀態	旗標	IP位址	子網路遮罩	執行
0	啟用	Native ETH0	192.168.2.254	255.255.255.0	網路
1	停用	ETH0.101	192.168.101.254	255.255.255.0	網路
2	停用	ETH0.102	192.168.102.254	255.255.255.0	網路
3	停用	ETH0.103	192.168.103.254	255.255.255.0	網路
4	停用	ETH0.104	192.168.104.254	255.255.255.0	網路
5	停用	ETH0.105	192.168.105.254	255.255.255.0	網路

- **系統狀態**：顯示啟用或關閉虛擬網路資訊。
- **旗標**：顯示虛擬網路使用的 tag ID 資訊，當顯示 Native ETH0 表示目前主要的有線連接是以此虛擬網路為主要登入系統。
- **IP 位址**：顯示該虛擬網路的 IP 位址。
- **子網路遮罩**：顯示該虛擬網路的子網路遮罩。
- **預設閘道**：設定頭端 Gateway 的 IP 位址。
- **DNS**：設定網域名稱解析伺服器，可設定兩組，DNS1 為主要的伺服器解析位址。
- **執行**：可點擊 網路 按鈕進入設定此虛擬網路之相關設定。

※ 如下進入”網路”設定頁面

- **虛擬網路服務**：可選擇”**啟用**”或”**關閉**”虛擬網路服務。
- **IP 位址**：設定該虛擬網路服務的 IP 位址。
- **子網路遮罩**：設定該虛擬網路服務的子網路遮罩。
- **802.1d Spanning Tree**：可以避免網路架構迴圈機制，例如：可以避免當您使用 WDS 功能與其他遠端的無線基地台互相連結時發生迴圈造成網路無法正常運作（如下圖所示），開啟此功能將可以避免此問題發生。



- **ETH0 虛擬網路標記設定**：
  - ✓ **ETH0**：可設定 ETH0 該網路埠是否啟用或關閉這連接埠的 VLAN tag。
  - ✓ **ETH0 Tag:** 當 ETH0 啟用後，可設定該網路埠的 Tag VLAN ID。

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。

7.2 AP Control

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**掃描網域中的 CenOS5.0 核心的基地台**、**批次設定**、**AP 設定**、**群組設定**、**Map**、**AP 網頁認證設定檔**及被管理 AP 的**系統狀態**。

7.2.1 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。

1. **裝置過濾：**

- **LAVN**：選擇要掃描的區域網段，若在**"4.1 虛擬網路設定"**有啟用多組 VLAN 網路，則此選項將會依造**"4.1 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**：可選擇透過 IP 方式去排列顯示，或選擇 MAC 方式排列顯示。

2. **掃描結果**：當掃描後，所有的無線基地台將會列出至此列表欄位。

- **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。

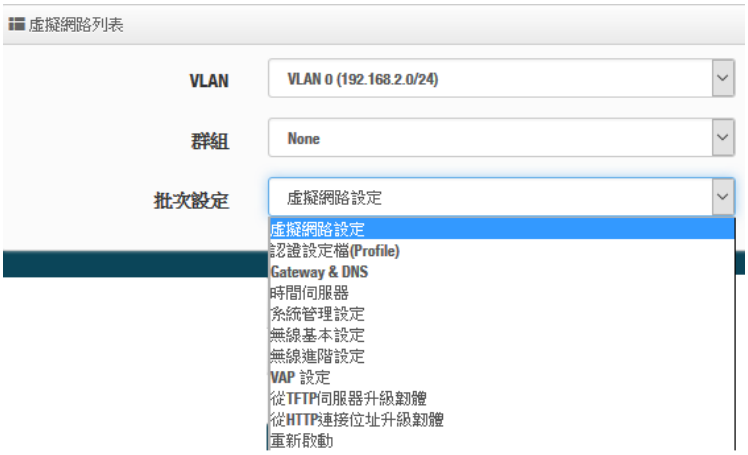
3. **Update IP Address & Netmask**：當在 Device 上是勾選多台以上或全選時，則可在此欄位功能上，設定整批無線基地台的 IP 位址或是 VLAN Tag 等。

- **管理埠**：可選擇修改 AP 要被管理的 VLAN 網段。
- **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。

設定完成確認後，則可點擊 Apply&Reboor 按鈕讓所有的被管理無線基地台儲存並重新啟動。

7.2.2 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**：選擇要管理的 VLAN 環境。
- **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**"認證設定檔(Profile)"**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***(可參考 4.5 的無線設定功能)***
- **無線進階設定**：設定被管理 AP 的無線進階。***(可參考 4.5.2 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。***(可參考 4.1.3 無線基地台功能設定)***
- **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。
- **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。
- **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**:顯示此 VLAN 的所有已經被管理 AP 的列表，可透過列表選擇需要被修改的無線基地台。

7.2.3 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移出管理等。

➢ **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。

7.2.4 群組設定

可以在同一個 VLAN 下去建置多筆的群組做管理，在不同的 VLAN 可設定多個 Group。

- **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。

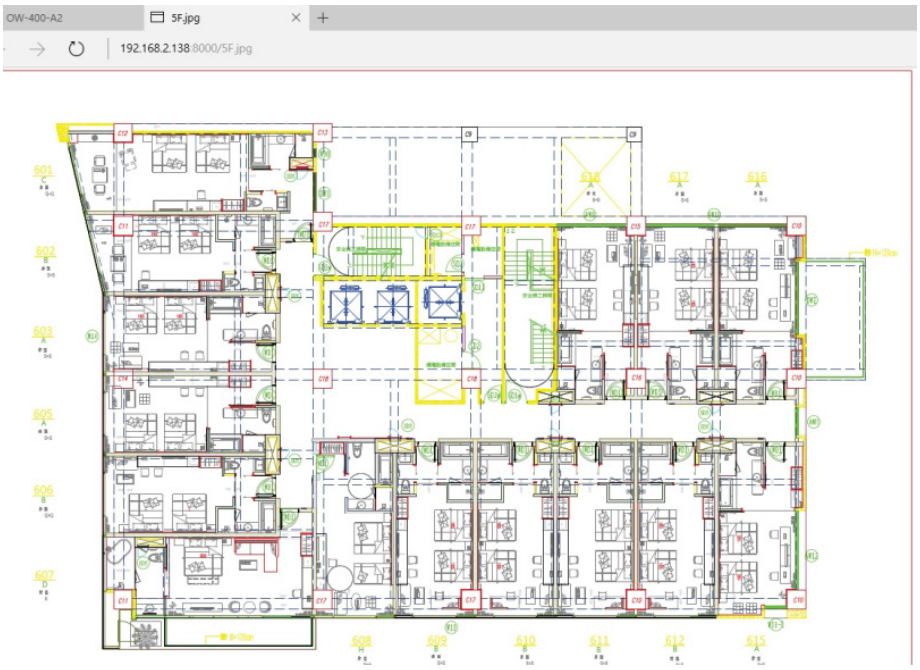
7.2.5 Map 設定

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。請先點選”建立新地圖”按鈕。

點選後將會進入新地圖設定頁面。

- **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，該 web 伺服器需另外自行架設或利用現有的 web 伺服器。
- **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。

假如圖檔路徑正確將會出現所加入的圖檔畫面

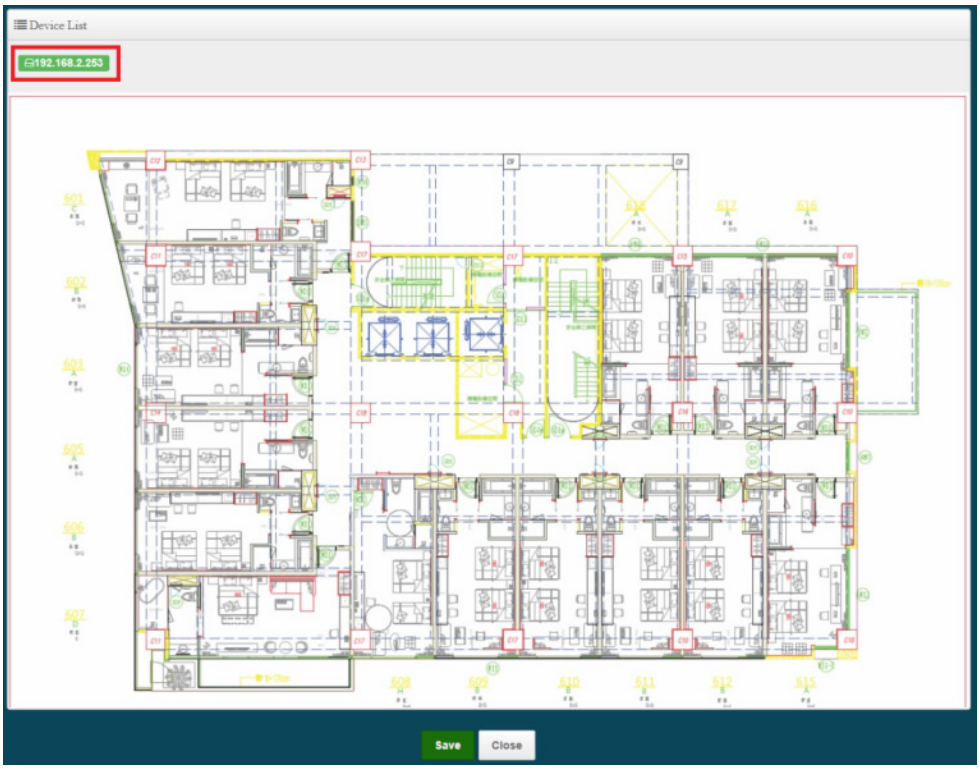


確認後點擊"**儲存**"按鈕儲存設定並將系統重新啟動讓地圖生效。

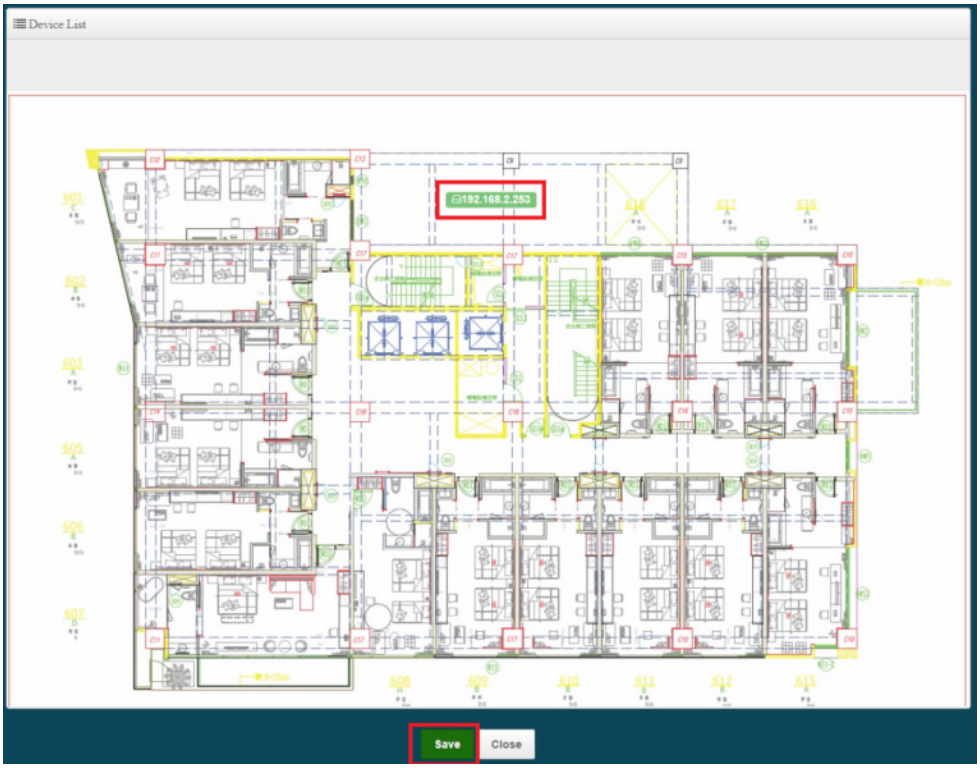
系統重新啟動後，Map 列表會出現剛剛儲存的地圖資訊。

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。

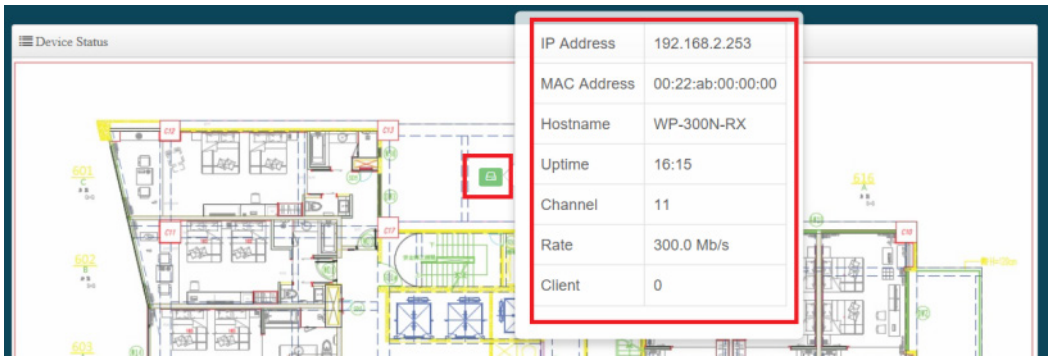


將 AP 圖示拖曳至地圖上欲設定的位置，完成後點選”Save”儲存設定再點選”Close”關閉視窗。



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。

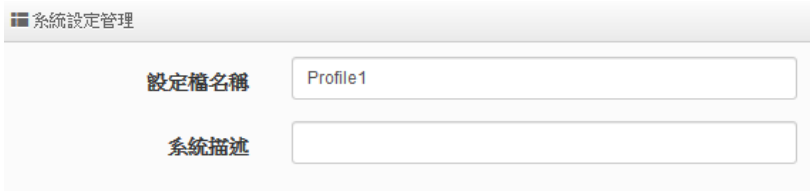


7.2.6 認證設定檔(Profile)

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 7.2.2 批次設定內去選擇套用。

應用步驟

1. 先點擊右上方”**建立新的設定檔**”按鈕進入新增 Profile
2. 進入後請設定 Profile 的名稱與描述



3. 確認後回到認證頁定檔主頁面，將出現剛設定的資訊

4. 在編輯框點擊網頁認證功能按鈕可進入先預設認證功能，請參考手冊 4.2.1 項說明

5. 在編輯框點擊網頁認證功能按鈕旁的下拉式選單可進入先預設認證相關功能，請參考手冊 4.2.2 項說明

以上步驟將完成 Profile 的設定檔，後只需要在手冊 7.2.2 批次設定下去套用即可

6. 若要修改或刪除 Profile 資料檔，可在執行欄位上，點即設定或下拉式功能去刪除

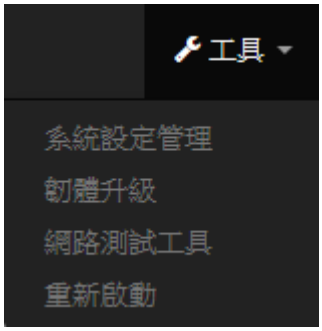
7.2.7 系統狀態

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。

8. 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。



8.1 系統設定管理

管理者可以在備份此系統現行環境的所有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。

8.2 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

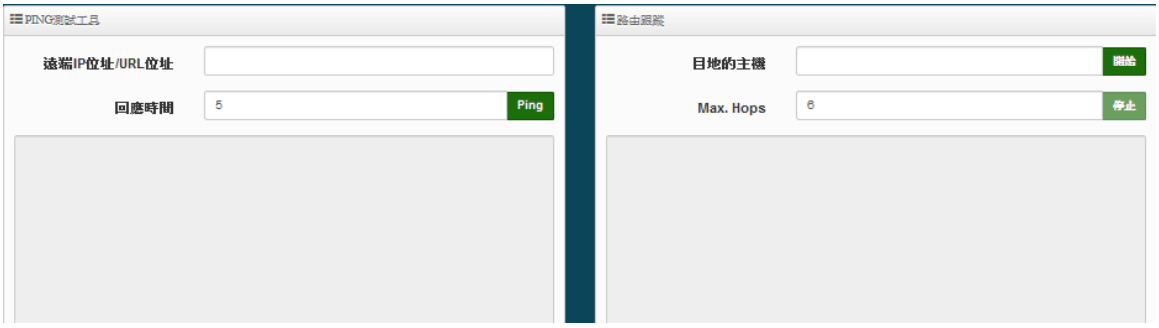
我們強烈的建議您務必遵守以下步驟進行韌體更新：

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. *務必使用相容的 WEB 瀏覽器進行更新以免發生更新失敗的問題。*
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。*

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。

8.3 網路測試工具

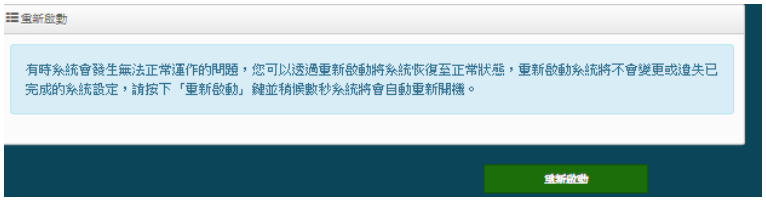
請點選「工具」→「網路測試工具」頁面使用 Ping 的動作檢查目前的網路連線，網路管理員可以透過本工具診斷目前的網路狀態進行除錯。



- **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。

8.4 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。

9. 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。

9.1 系統狀態

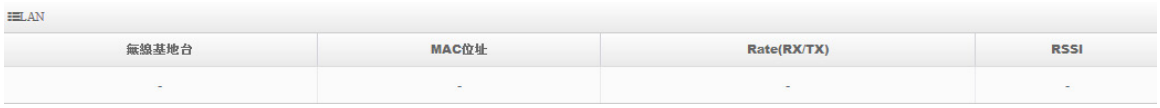
系統狀態：
主要顯示系統目前使用的模式、名稱、時間、韌體版本、網卡位址及相關網路設定等資訊。

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 無線基地台：顯示目前 Radio 0 (5GHz)無線基地台的基本運作模式資訊

9.2 無線用戶狀態

顯示 5G 的無線連線使用者的相關資訊。


LAN

無線基地台	MAC位址	Rate(RX/TX)	RSSI
-	-	-	-

- **無線基地台：**顯示無線使用者連接無線狀態。
- **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。

9.3 線上使用者

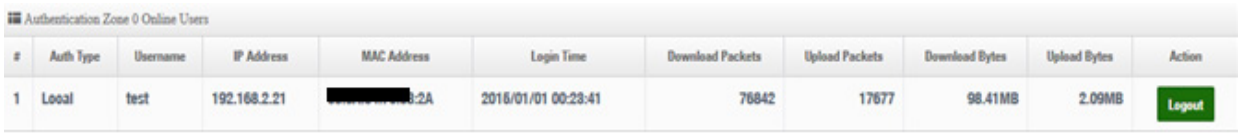
此功能建置在無線基地台模式，主要顯示目前已再線上的認證的使用者名單
當開啟網頁認證功能(參考手冊 4.2 網頁認證功能)，將會顯示已通過線上網頁認證(Captive Portal)用戶。
管理員可以監控用戶的身份驗證帳戶的登錄/登出時間和帳戶認證類型。


認證的線上使用者

VLAN#	網頁認證功能	使用者數量	下載封包	上傳封包	下載位元	上傳位元	執行
-	-	-	-	-	-	-	-

- **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


Authentication Zone 0 Online Users

#	Auth Type	Username	IP Address	MAC Address	Login Time	Download Packets	Upload Packets	Download Bytes	Upload Bytes	Action
1	Local	test	192.168.2.21	[redacted]:2A	2015/01/01 00:23:41	76842	17677	98.41MB	2.09MB	Logout

- **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:** 將此認證用戶強制登出

9.4 認證日誌

此功能建置在無線基地台模式，主要顯示目前已再線上的認證的使用者名單
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。

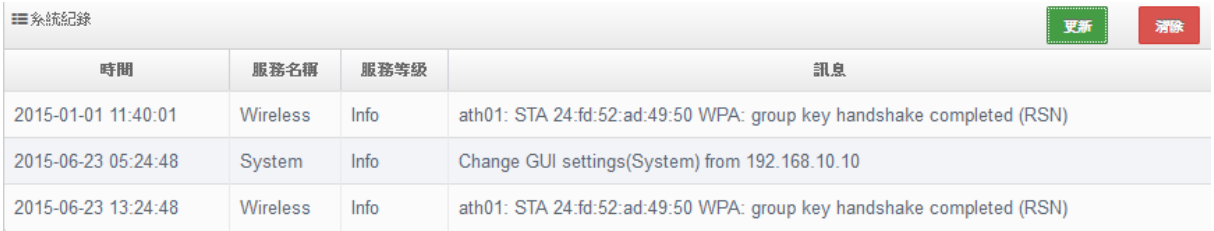

認證區日誌

日期	VLAN#	詳細
-	-	-

- **日期:** 顯示年月份日期
- **VLAN:** 可選擇顯示不同 VLAN
- **詳細**: 可點擊進入查看行系資訊

9.5 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。


系統紀錄 更新 清除

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)

10. 技術文件補充

10.1 WDS 相關設定

WDS 功能應用在無線基地台模式之下，此功能主要是做點對點無線基地台橋接，設定方法請參考手冊 4.5.4 WDS 設定說明，此相關文件主要引導 WDS 重點程序，只要依照以下流程將能輕鬆架構 WDS 點對點之應用

1) 若要點對點橋接使用 WDS 功能，建議都使用本公司產品以避免相容性問題
2) 當要 2 台無線基地台做橋接時，請確實每台的無線基地台 IP 位址需同網段不能重複
3) 請參考手冊 4.5.4 WDS 設定頁面正確設定要連接的無線基地台 MAC 位址，若以 A 和 B 兩台橋接做範例，則 A 台須設定 B 台的 MAC 位址，相對的 B 台則須設定 A 台的 MAC 位址
4) 確認後重新啟動將完成 WDS 點對點橋接，可至 4.5.5 WDS 狀態確認 RSSI 值，若為-1 表示沒有連接成功， 請重新確認設定檔是否按照以上說明，或是基地台間的訊號遭受阻隔過干擾 RSSI 值建議落在 40~60 間，太高表示 AP 與 AP 之間太近，太低表示訊號沒對好或是距離太遠

其他說明:

因為 WDS 應用是在無線基地台模式之下，所以若啟用 WDS 功能則將是 AP+WDS 之應用，倘若要純使用 WDS 功能不需要無線基地台(AP)，則可以參考手冊 4.1 虛擬網路設定說明，將無線基地台(AP)關閉即可，如下圖

10.2 套用 CERIO 網頁認證登入頁面操作

假若設備使用本公司無線基地台 CenOS 5.0，並啟用網頁認證功能，則將能自訂編輯網頁認證頁面，可參照以下步驟輕鬆完成套用樣本的登入頁面

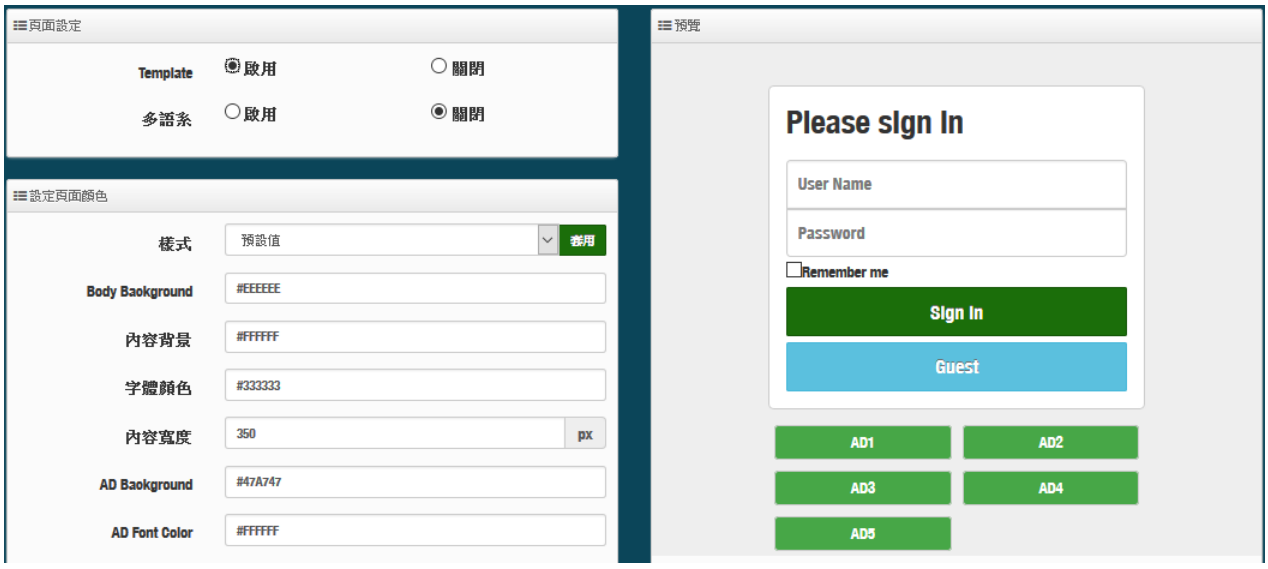
步驟一 ：先啟動網頁認證功能，在系統設定=>網頁認證功能 (可參考使用手冊 3.3)

步驟二：確認啟用後，可選擇登入帳密要採用何種類型，本步驟以”本機帳戶”為範例，將”啟用建立本機帳戶”，確認啟用後儲存，如下

步驟三: 請至認證功能的下拉功能按鈕, 進入建立帳戶名稱與密碼, 如下圖說明

PS.
若要使用系統預設的頁面請參考步驟四
若要套用本公司的範本請參考步驟五以下
若要自行編輯網頁請參考步驟七(此方式建議有 Html/CSS 編寫能力使用)本更司不教導支援

步驟四: 若要使用系統預設的認証頁面, 可參考使用手冊 3.3.4 說明, 將能設定預設的格式做顏色編輯修訂, 若需要自訂頁面並套用我司的範本請參考步驟五

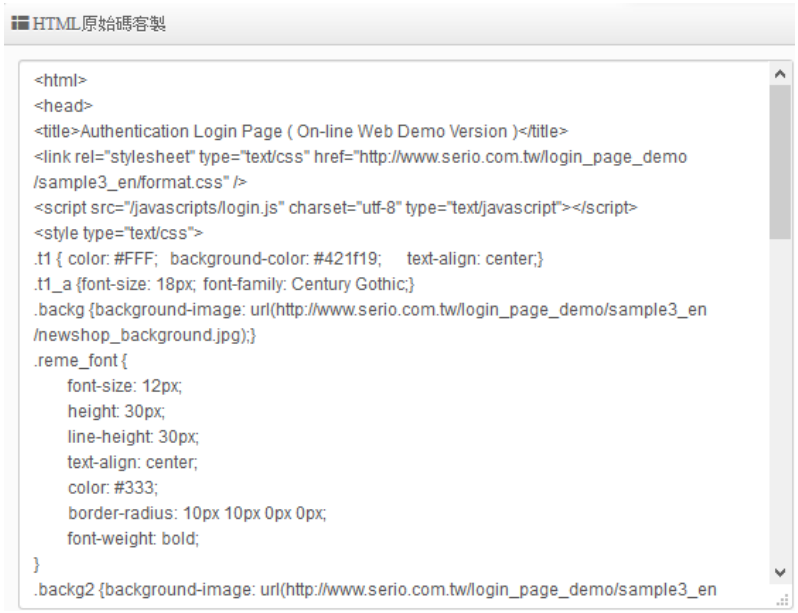


步驟五: 因為登入頁面的圖檔必須放置在網站伺服器上, 所以須將網站位址建立白名單, 此範例的背景圖存放位置在本公司第二台伺服器上, 所以請確實將以下網址輸入至 Walled Garden 內
(網址:www.serio.com.tw)

步驟六: 至本公司官方網站下載範例，解壓縮後 將裡面的 HTML 語法全選並複製，然後貼在系統的自訂編輯頁面後儲存即可，如下範例

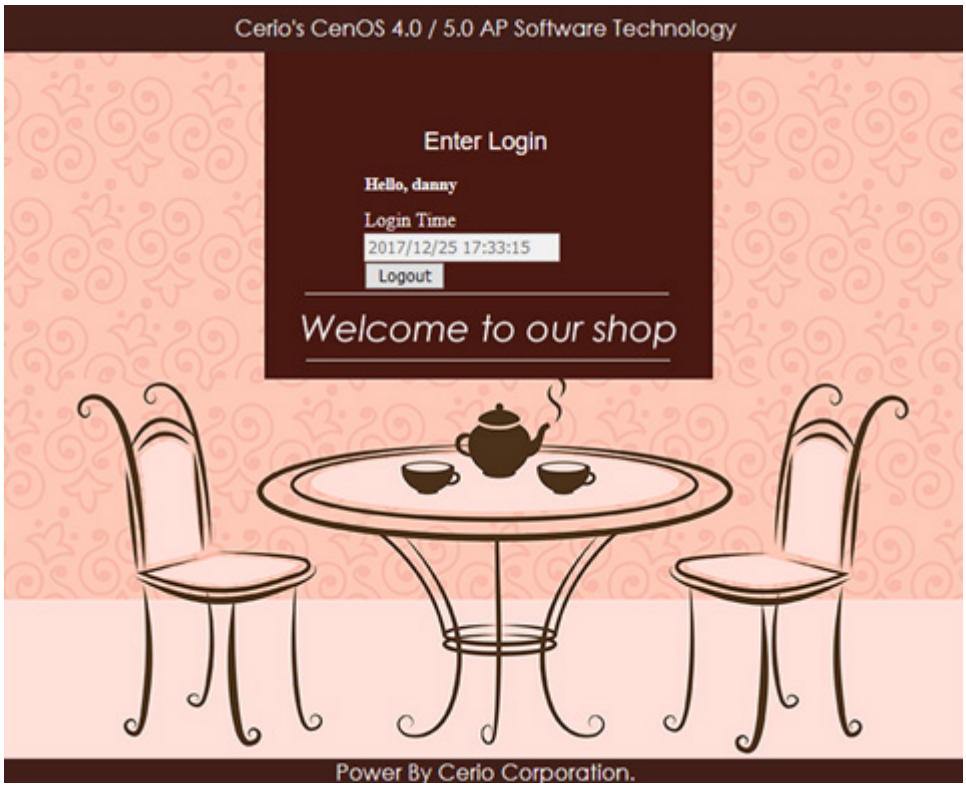
下載範例位址: https://www.cerio.com.tw/?page_id=24746

先清空 HTML 原始碼內容後，再將下載的原始碼全部貼入欄位裡面，儲存並重新啟動無線基地台，即可完成登入頁面的編輯



如下範本的登入頁面


Cerio's CenOS 4.0 / 5.0 AP Software Technology
Enter Login
Local User
User Name
Password
Remember me
Sign in
Welcome to our shop
Power By Cerio Corporation.


Cerio's CenOS 4.0 / 5.0 AP Software Technology
Enter Login
Hello, danny
Login Time
2017/12/25 17:33:15
Logout
Welcome to our shop
Power By Cerio Corporation.

步驟七: 假若自訂頁面要自行撰寫，必須保留以下紅字之原始碼不可移除，其他將能自行編寫

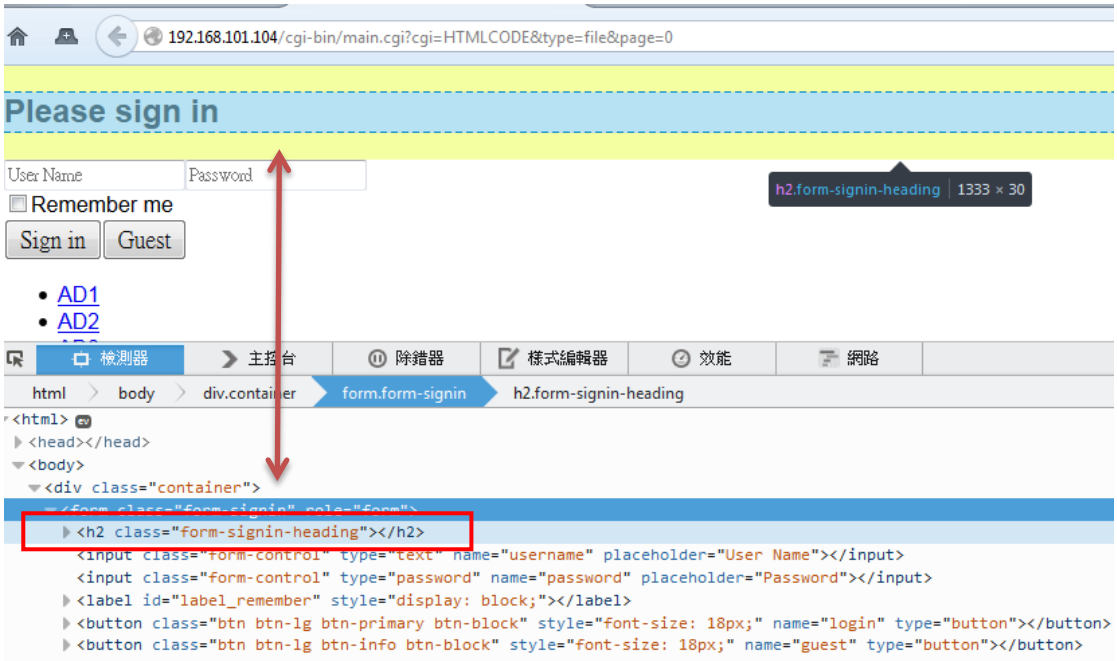
```
<html>
 <head>
      <title>Hotspot</title>
      <script src="/javascripts/login.js" charset="utf-8" type="text/javascript"></script>
 </head>
 <body>
      <div class="container"></div>
 </body>
</html>
```

注意:

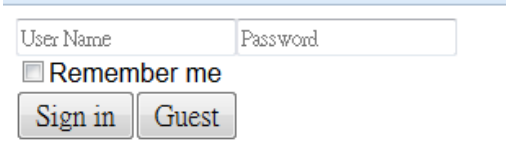
1. 此欄位必須在 190 行間之內，若撰寫的 HTML/CSS 等原始碼超過一定的行間下，建議將 CSS 原始碼存放至遠端 Web Server，然後將遠端 web server 的 IP 位址輸入至 Walled Garden 內，請參考使用手冊 3.3.6
2. 本設備不支援圖檔的存放空間，若必要請將圖檔存放至遠端 web 伺服器，透過位址呼叫近來，同上作法

步驟八: 本系統的登入欄位功能，預設是全部顯示，若有不必要的欄位將可透過 css 語法方式去隱藏特定欄位，如下說明

語法內新增<style>class 的標籤然後加入{display: none;}即可</style>如下範例，透過瀏覽器先找出要隱藏的欄位 ID 碼，例如要隱藏登入頁面中的”Please Sign in”這描述，則先找出它的 Class ID 如下圖指示



在 head 內增加<style> .form-signin-heading {display: none;}</style>即可將”Please Sign in”這描述隱藏不顯示如下圖，發現 Please Sign in 字樣不見了，依此類推



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 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; `, . =
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 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; `, . =
	Lease Time	600 ~ 99999999

Table B WEB GUI Valid Characters (continued)

Block	Field	Valid Characters
Management	System Name/ Location	Length : 32 0-9, A-Z, a-z Space ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; `, . =
	Description	32 chars
	Password	Length : 4 ~ 30 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; `, . =
	HTTP/ HTTPS Port	1 ~ 65535
	Telnet/ SSH Port	1 ~ 65535
SNMP	RO/RW community	Length : 32 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] ; `, . =
	RO/RW user	Length : 31 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] ; `, . =
	RO/RW password	Length : 8 ~ 32 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] ; `, . =
	Community	Length : 32 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] ; `, . =
	IP	IP Format; 1-254
General Setup	Tx Power	1-100 %
Wireless Profile	Profile Name	32 chars
	ESSID	Length : 31 Space 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; `, . =
	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 Space 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; `, . =
	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
WDS Setup	AES Key	8 ~ 63 ASCII chars; 64 HEX chars
	Peer's MAC Address	12 HEX chars
	Description	32 chars
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