

CERIO Corporation CenOS 5.0 使用手冊

CW-500 R1

eXtreme High Power WiFi6 Dual-Radio AX1800

功能型掛式 PoE 高速無線基地台 (500mW)



NCC 警語

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 $1\text{mW}/\text{cm}^2$ ，本產品使用時建議應距離人體 35cm」。

內容

NCC 警語.....	2
1. 系統管理及主體相關說明	7
1-1. 主體天線與功能套件	7
1-2. 系統登入前置設定.....	8
1-3. 登入 WEB 管理介面	10
2. 初次登入系統管理介面設定.....	11
2-1. 變更使用者介面語系	11
2-2. 基本架構與運作模式說明	11
2-2-1. 無線基地台模式 (預設值模式).....	11
2-2-2. ClientBridge 模式	13
2-2-3. WISP 模式	14
2-2-4. CAP 模式.....	15
3. 系統設定.....	16
3-1. 系統管理.....	16
3-2. 時間伺服器	19
3-3. SNMP	20
3-4. 時間規則.....	22
4. 無線基地台模式(AP Mode)	23
4-1. 模式設定.....	23
4-2. 虛擬網路設定	23
4-2-1. 虛擬無線基地台網路設定.....	24
4-2-2. DHCP 伺服器	26
4-2-3. 頻寬控制	28
4-2-4. 無線基地台 Radio 0(2.4G) / Radio 1(5G)設定	29
4-2-5. MAC 過濾	35
4-2-6. 802.11r Fast Roaming.....	36
4-3. 網頁認證功能	38
4-3-1. 遊客	42
4-3-2. 建立本機使用者帳戶名單.....	42

4-3-3.	OAuth 2.0.....	43
#	Google 的 OAuth2.0 服務頁面設定說明	44
#	Facebook 的 OAuth2.0 服務頁面設定說明	46
4-3-4.	POP3/IMAP Server.....	49
4-3-5.	客製化頁面	49
4-3-6.	語系	52
4-3-7.	Walled Garden	54
4-3-8.	特權名單.....	54
4-3-9.	Bulk MAC Address	55
4-3-10.	設定檔	56
4-4.	Radius 伺服器	56
4-5.	Radius 帳戶設定	57
4-6.	無線設定.....	57
4-6-1.	Radio 0 (2.4G).....	57
4-6-2.	Radio 1 (5G).....	60
4-6-3.	進階設定.....	62
4-6-4.	WMM 頻寬最佳化設定	64
4-6-5.	WDS 設定	65
4-6-6.	WDS 狀態	67
5.	Client Bridge 模式.....	68
5-1.	模式設定.....	68
5-2.	區域網路設定	68
5-3.	DHCP 設定	70
5-4.	無線設定.....	71
#	無線基地台橋接及訊號延伸(Repeater AP)設定步驟，可協助管理人員建立與上端 AP 橋接及延伸無線基地台應用。	71
5-4-1.	Radio 0 (2.4G).....	73
5-4-2.	Radio 1 (5G).....	76
5-4-3.	進階設定.....	78
5-4-4.	WMM 頻寬最佳化設定	80

5-4-5.	基地台橋接設定	81
5-4-6.	Station Profile Setup	84
5-4-7.	Repeater AP 設定.....	86
5-4-8.	MAC 過濾	87
5-4-9.	802.11r Fast Roaming.....	87
6.	WISP 模式.....	90
6-1.	模式設定.....	90
6-2.	WAN 設定	90
6-3.	區域網路設定	93
6-4.	DHCP 設定	94
6-5.	無線設定.....	96
	#無線基地台橋接及訊號延伸(Repeater AP)設定步驟，可協助管理人員建立與上端 AP 橋接及延伸無線基地台應用。	96
6-5-1.	Radio 0 (2.4G).....	98
6-5-2.	Radio 1 (5G).....	101
6-5-3.	進階設定.....	103
6-5-4.	WMM 頻寬最佳化設定	105
6-5-5.	基地台橋接設定	106
6-5-6.	Station Profile Setup	109
6-5-7.	Repeater AP 設定.....	111
6-5-8.	MAC 過濾	111
6-5-9.	802.11r Fast Roaming.....	112
6-6.	進階 (WISP 模式下適用)	115
6-6-1.	DMZ	115
6-6-2.	IP 過濾.....	115
6-6-3.	MAC 過濾設定	117
6-6-4.	虛擬伺服器	118
6-6-5.	存取控制.....	119
7.	CAP 模式.....	120
7-1.	模式設定.....	120

7-2.	虛擬網路設定	121
7-3.	AP Control	123
7-3-1.	掃描無線基地台	123
	#掃描操作程序說明：	123
7-3-2.	批次設定	124
7-3-3.	AP 設定	125
7-3-4.	群組設定	126
7-3-5.	MAP 設定	126
7-3-6.	認證設定檔(Profile)	129
7-3-7.	系統狀態	130
8.	工具	131
8-1.	系統設定管理	131
8-2.	韌體升級	131
8-3.	網路測試工具	132
8-4.	重新啟動	133
9.	系統狀態	134
9-1.	系統狀態	134
9-2.	無線用戶狀態	136
9-3.	線上使用者	136
9-4.	認證日誌	137
9-5.	系統紀錄	137
10.	相關技術文件參考	138
10-1.	Fast Roaming 802.11r 快速漫遊的引導設定	138
10-2.	點對點或點對多 WDS 相關設定	147
10-3.	套用 CERIO 網頁認證登入頁面操作	148
10-4.	地區 5Ghz WiFi 頻道相關・國家/地區 DFS(動態頻率選擇) 列表資訊	153
	Appendix A. WEB GUI Valid Characters	154

1. 系統管理及主體相關說明

1-1. 主體天線與功能套件



1-2. 系統登入前置設定

智鼎 CenOS 5.0 採網頁管理方式，當架構建置完成，透過瀏覽器輸入 192.168.2.254 (預設 IP 位置) 進入管理頁面及正確帳號密碼，即可管理設備功能，在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，請參考以下步驟設定您的電腦。



再點擊 " 開啟網路和網際網路設定 " 進入

將滑鼠一到此處點擊" 滑鼠右鍵"



乙太網路

無法辨識的網路
沒有網際網路

相關設定

[變更介面卡選項](#)

[變更進階共用選項](#)

[網路和共用中心](#)

[Windows 防火牆](#)

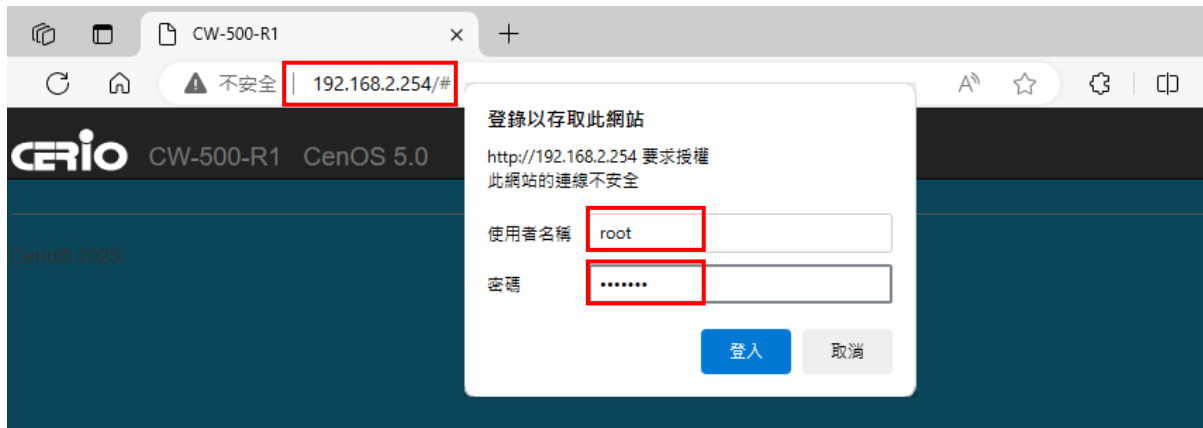
進入開啟網路和網際網路設定頁面後，在左目錄點擊 " 乙太網路 "，右邊點擊 " 變更頁面卡選項 " (以下為使用網路線連接 AP 的網路卡為案例)



- ◆ 於 " 乙太網路 " 小圖示按右鍵，進入網路功能頁面，選擇(TCP/IP4)開啟變更網段
- ◆ 選擇" 使用下列的 IP 位址" 輸入與 AP 同網段 IP，如範例使用 192.168.2.20，子網路遮罩 255.255.255.0
- ◆ 設定完後，按確認即完成設定

1-3. 登入 WEB 管理介面

開啟 IE 瀏覽器或其他如 Firefox、Chrome、Edge 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>，開啟 WEB 管理介面。



- 成功進入管理登入介面後，在使用者名稱欄位中輸入「**root**」，密碼鍵入「**default**」，按「**確定**」即可登入管理介面。



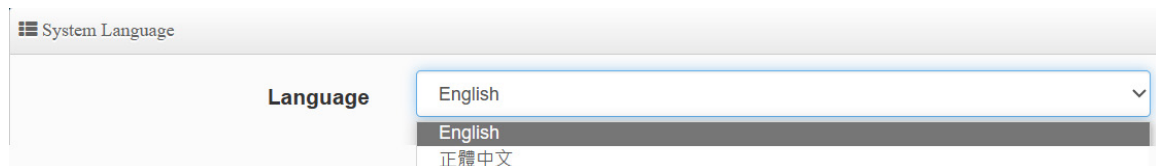
2. 初次登入系統管理介面設定

2-1. 變更使用者介面語系

若管理者需使用中文介面，可直接進入管理頁面的系統選項，變更管理介面語系。

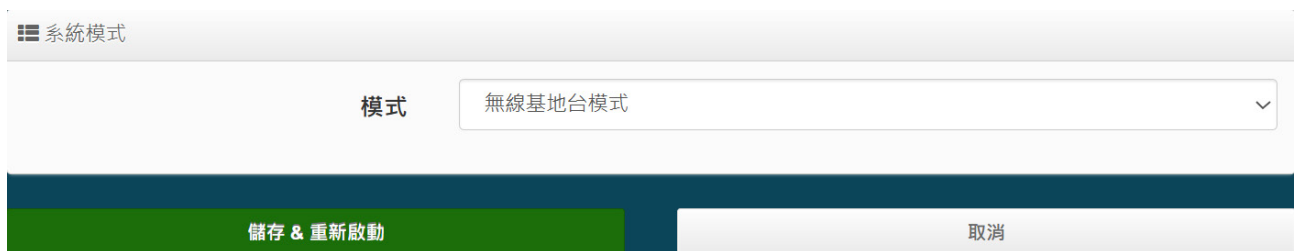
於 UI 介面右上方點選 System→Management→System Language 做語系切換。

【預設啟動操作介面為英文】



2-2. 基本架構與運作模式說明

2-2-1. 無線基地台模式（預設值模式）



當環境已完成建置有線上網服務後，若想利用無線方式進行上網，可將設備轉換為無線基地台模式，只需將網路線連接至設備並設定好無線基地台相關設定，即可達成使用無線上網之應用。

- 支援傳統無線基地台功能
- 內建 DHCP 伺服器，可自動分配 IP 位址給連線用戶
- 支援 WDS 連線，且設定支援 AES 加密
- 支援單一入口網頁認證
- 認證模式支援本機內建帳戶認證、802.1x RADIUS 伺服器帳戶認證、OAuth 2.0 開放性同步帳戶認證等方式

無線基地台模式 (Access Point mode)



無線基地台模式+認證入口功能(AAP) (AP mode + Authentication)



※ 無線基地台模式使用 WDS 功能之應用

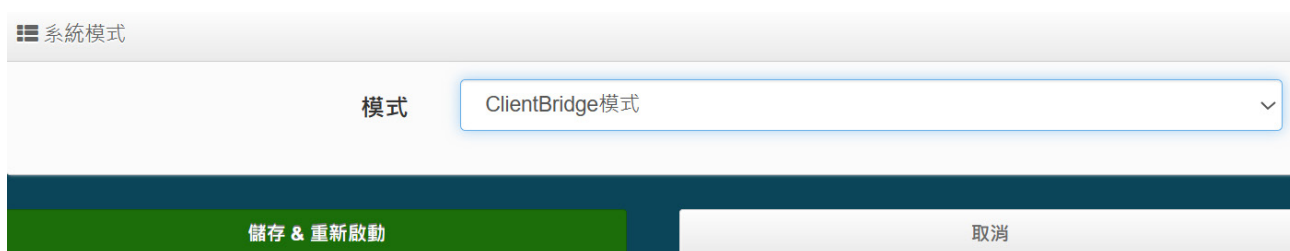
所謂 WDS 功能，可想成其為一條網路線，差別在是透過無線方式行連接，戶外型使用 WDS 點對點橋接強調長距離連接與維持穩定之技術，於此 WDS 不單只做長距離點對點橋接，也能做長距離點對多點之應用。

可在無線基地台下啟用 WDS 功能 (即 AP+WDS 應用)，設備除了一樣可使用 AP Station 之服務外，其中又能透過 WDS 方式與另一台 AP 做長距離橋接應用。

無線基地台模式+WDS功能 (AP mode + WDS function)



2-2-2. ClientBridge 模式



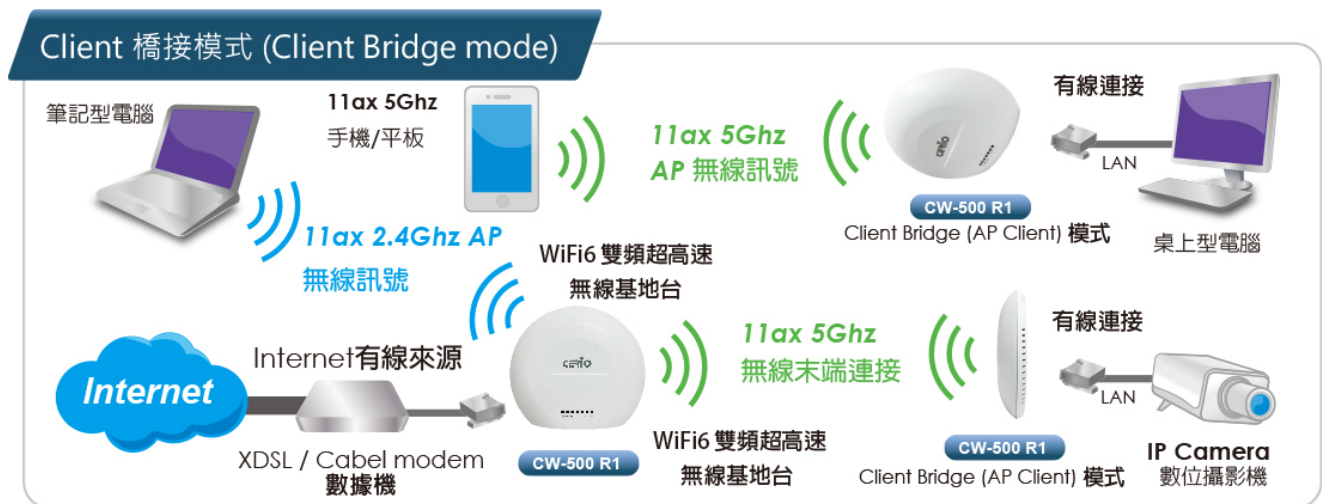
C

Client Bridge 模式，可將其想像成一個外接式無線網卡，專門負責與上端無線基地台(AP)做無線連線。切換 Client Bridge 模式後則設備必須與上端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。

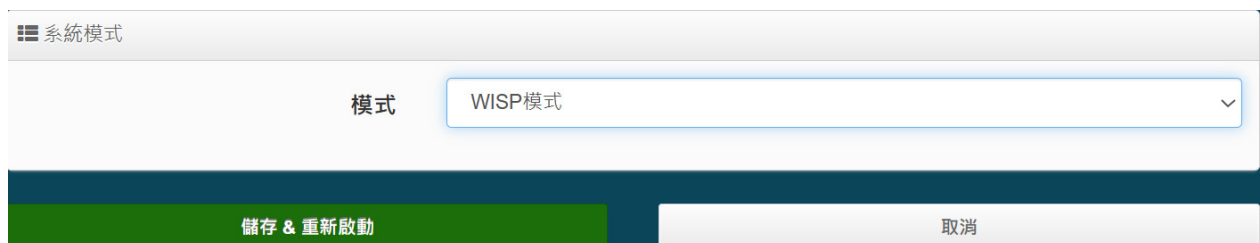
Client 橋接模式 + 延伸無線基地台功能 (Client Bridge mode + Repeater AP)



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，即為訊號再延生產生無線基地台訊號機制。



2-2-3. WISP 模式



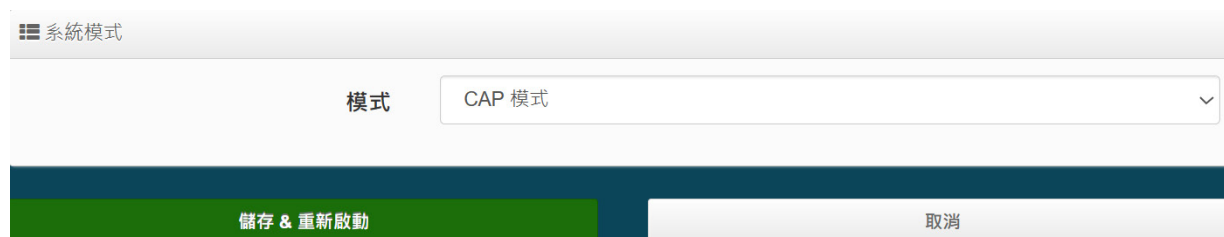
切換此模式，WAN 端撥接方式將使用 Wireless 方式與上端無線 xDSL 做橋接。WISP 模式是 (Wireless Internet Service Provide) 的簡稱，WISP 的 WAN 端是以無線方式橋接 xDSL 基地台，連線方式支援動態 IP、靜態 IP、PPPoE 及 PPTP 等。

透過 NAT 方式分享到所有的 LAN 端，在使用 WISP 模式時，本機實體網路埠為 LAN 運作(分別為 LAN1 與 LAN2)，而在 WISP 模式啟用 Repeater AP 功能時，本機的 LAN 將產生無線基地台供無線用戶使用。

WISP模式 + 延伸無線基地台功能 (WISP mode + Repeater AP)



2-2-4. CAP 模式



切換 CAP 模式後成為一台中央集中管理器，負責集中管理多台 AP 模式的無線基地台，主要能集中設定，VLAN 管理，基地台監測等。

CAP模式 (CAP mode)集中式控管平台

利用 CAP 集中控管平台對 AAP 基地台進行集中控管 (最大可控管 x 32 APs 台)



3. 系統設定

3-1. 系統管理

於 UI 介面點擊系統設定選單，選擇系統管理進入頁面



The screenshot displays two sections of the system management interface. The first section, titled '系統語系' (System Language), contains a dropdown menu labeled '語系' (Language) with '正體中文' (Traditional Chinese) selected. The second section, titled '系統資訊' (System Information), contains three input fields: '系統名稱' (System Name) with the value 'CW-500-R1', '系統描述' (System Description) with the value 'eXtreme High Power WiFi6 Dual-Radio PoE Bridge/AP', and '裝置位置' (Device Location) which is currently empty.

- **系統語系**：支援正體中文和英文兩種語系，管理者可在此管理介面進行設定。
- **系統資訊**
 - **系統名稱**：管理者可自訂編輯設備之系統名稱。
 - **系統描述**：管理者可自訂編輯設備之系統描述。
 - **裝置位置**：管理者可在此輸入目前 AP 安裝位置等資訊，管理時可輕鬆辨識裝置所在位置。



The screenshot displays two sections of the system management interface. The first section, titled '設定系統管理員 (登入名稱[root])密碼' (Set System Administrator (Login Name [root]) Password), contains two input fields: '新密碼' (New Password) and '確認新密碼' (Confirm New Password). The second section, titled 'LED控制' (LED Control), contains three radio buttons: '關閉LED' (Turn off LED), '啟用' (Enable), and '關閉' (Turn off), with the '關閉' option selected.

- **設定系統管理員(登入名稱[root])密碼**：帳號為 root，可修改系統登入密碼。
- **LED 控制**：可啟用或關閉 AP 系統在執行時的 LED 閃爍狀態。

Ping Watchdog

☒

IP位址

Interval

60

秒

Delay

100

秒

Times of faults

3

times

- **Ping Watchdog**：可透過設定讓系統自動判斷運作是否正常，若 ping 規則成立，系統自動重啟。
- **Interval**：間隔多少時間去 ping IP 位址一次
 - **Delay**：當 ping 不通後要延遲多久再 ping 一次
 - **Times of faults**：當以上條件成立幾次後，讓系統重新啟動。

管理介面登入設定

HTTP
☒

80

埠號

HTTPS
☐

443

埠號

Telnet
☒

23

埠號

SSH
☐

22

埠號

主機憑證金鑰內容

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDtiBcHpTCI

產生SSH憑證金鑰

- **管理者介面登入**：管理這可以選擇登入管理頁面方式。
- **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。
 - **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。
 - **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。
 - **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。
 - **主機憑證金鑰內容**：可點擊產生 SSH 憑證金鑰。
 - **Access WAN**：存取管理介面開放除以 LAN 方式外也可以通過 WAN 實體 IP 方式進行

存取能力，選擇啟用或關閉（此功能使用限於當模式切換至具有 NAT 性質的 WISP 模式時產生作用）

系統記錄設定

遠端伺服器 ☐

埠號 埠號

The diagram illustrates the data flow for system logs. On the left, a 'System Log Server' (represented by a server icon) sends 'Log data' (indicated by a curved arrow) to an 'Access Point' (represented by a triangle icon). A vertical line separates the server from the access point, with the data flow crossing it.

- **系統紀錄設定：**倘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，將本機系統資訊往伺服器上備存，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，預設為智鼎 AP 管理控制器內建的日誌中心相對 514 埠。



Notice

若搭配使用智鼎公司的 AP 管理控制器產品內建的日誌伺服器功能，則請使用預設的 514 的遠端伺服器連接埠進行指定連接。智鼎公司所搭配的 AP 管理控制器的內建日誌伺服器對其智鼎公司的無線 AP 裝置提供了完善的日誌格式與所有完整格式資訊，建議搭配使用以利完整掌握環境 AP 使用時的所有狀態留底資訊。

自動重新啟動

方式

關閉
每日
每週
月

- **自動重新啟動：**此功能可依照管理者需求及時間規劃安排進行系統重新啟動，可選擇每日、每週或每月進行。
 - **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。

3-2. 時間伺服器

於 UI 介面點擊系統設定選單，選擇時間伺服器進入頁面


Notice

為能正確取得 Internet 標準時間並確實紀錄各項資訊所發生時間點，可以透過網際網路方式與網際網路上的時間伺服器，進行時間同步作業。

☰ 系統時間
☰ 手動指定系統時間

目前本地端時間

2021/06/02 07:03:14

模式

☐ NTP伺服器
 ☒ 手動

日期(年/月/日)

時間(時:分:秒)

(GMT+8:00)

Set Time

☰ NTP伺服器

預設NTP伺服器

time.stdtime.gov.tw

NTP伺服器

time.stdtime.gov.tw

時區

(GMT+08:00) 北京, 香港, 新加坡, 台灣

啟用日光節約時間

☐ 啟用
 ☒ 關閉

➤ 系統時間

- 目前本地端時間：此欄位顯示目前系統的時間。
- 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。

➤ NTP 伺服器

- 預設 NTP 伺服器：可選擇預先設定好的 NTP 伺服器，也可自定 NTP 伺服器。
- NTP 伺服器：需填入所選擇的 NTP 伺服器地址，例如如下選擇網路上 **cerio.com.tw** 的時間伺服器來作為 NTP 時間的校准依據。

- **時區**：可儲存並修改所想選擇的 GMT 時間。
 - **啟用日光節約時間**：此為歐美國家的夏令時間，可選擇啟用或關閉。
- **手動指定系統時間**：手動設定完時間請按 Set Time 即完成時間設定不須再按儲存。



Notice

1. 本產品支援硬體電池記憶時間設計，當選擇“手動更新”時間並得以儲存至硬體記憶體內，若無法儲存時間且總會無效回到預設時間時，則須更換硬體機板電池。
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 伺服器設定是否正常。

3-3. SNMP

於 UI 介面點擊系統設定選單，選擇 SNMP 進入頁面。此功能將可啟動 AP 的 SNMP 功能，管理者可依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**：可在此設定一組密碼給只能讀取的管理人員使用。
 - ✓ **RW Community**：可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 ☐ 啟用 ☒ 關閉

RO Username

RO Password

RW Username

RW Password

➤ SNMP V3

- ✓ 啟動：啟動或關閉 SNMP v3 支援。
- ✓ RO Username：管理者可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：管理者可在此設定一組帳號給可讀取和寫入的管理人員使用。
- ✓ RW Password：管理者可在此設定一組密碼給可讀取和寫入的管理人員使用。

SNMP Trap

啟動 ☐ 啟用 ☒ 關閉

Community

IP 1

IP 2

IP 3

IP 4

- SNMP Trap：此功能可利用無線基地台的內建代理程式，將 SNMP Trap 訊息主動告知遠端 SNMP 監控主機，讓遠端啟動 SNMP 監控主機可即時知道目前無線基地台最新狀態。
- ✓ 啟動：您可在此選擇啟用 SNMP Trap 功能。
- ✓ Community：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：輸入遠端啟動 SNMP 監控程式的主機 IP 位址。

3-4. 時間規則

時間規則列表			
#	註解	模式	編輯
1	Policy 1	On Schedule	編輯
2	Policy 2	On Schedule	編輯
3	Policy 3	On Schedule	編輯
4	Policy 4	On Schedule	編輯
5	Policy 5	On Schedule	編輯

- 管理人員可設定時間排成，當設定好時間排成規則後，可套用至相關功能進行定時執行功能應用，例如無線訊號透過此則自動啟用關閉，共可設定 1~10 組時間規則。
- 點擊編輯方塊可設定時間規則。

時間規則

註解

Policy 1

模式

☒ 依照時間表
 ☐ 依照時間表之外

- **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。

時間規則列表

#

日

一

二

三

四

五

六

時間

執行

-

-

-

-

-

-

-

-

-

-

建立新規則

時間規則

Day of Week

☒ 日
 ☒ 一
 ☒ 二
 ☒ 三
 ☒ 四
 ☒ 五
 ☒ 六

開始時間

00

00

結束時間

23

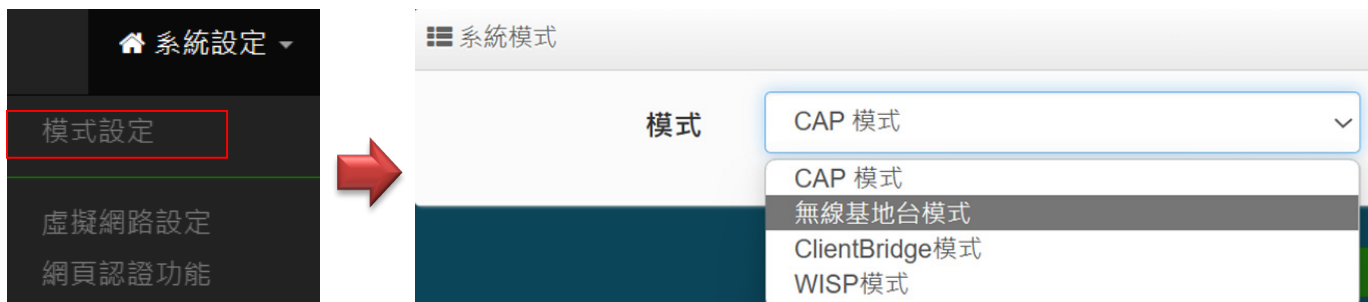
59

- 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. 模式設定

於 UI 介面點擊系統設定→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。



Notice

1. 每個模式下的 LAN IP 位址並不互相繼承沿襲使用，請就每個模式下自己的初始 LAN 預設值 IP 192.168.2.254 的 IP 位址進行存取管理。
2. Cerio's 雙頻無線基地台，支援 16 個 VLAN 及 32 個 SSIDs(每個 VLAN 各自支援 2.4Ghz SSID x1 與 5Ghz 頻段 SSID x1)。

4-2. 虛擬網路設定

虛擬網路設定

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 ETH1	Native ETH2 存取控制	192.168.2.254	255.255.255.0	2.4G_0_0	5G_0_1	網路
1	停用	ETH1.101	ETH2.101	-	-	2.4G_1_0	5G_1_1	網路
2	停用	ETH1.102	ETH2.102	-	-	2.4G_2_0	5G_2_1	網路
3	停用	ETH1.103	ETH2.103	-	-	2.4G_3_0	5G_3_1	網路

The screenshot shows a web-based configuration interface. At the top, there's a section titled '預設閘道' (Default Gateway) with a text input field containing '192.168.2.1'. Below this is a section titled 'DNS' with two text input fields: 'DNS1' containing '192.168.2.1' and 'DNS2' which is empty.

: 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 ETH1** **Native ETH2** 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 2.4Ghz 基地台，可顯示每個虛擬網路中 2.4Ghz 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。
- **Radio 1**：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。
- **DNS**：設定 DNS 解析的 IP 位址。

4-2-1. 虛擬無線基地台網路設定

點擊“網路”按鈕進入設定虛擬網路相關功能 **網路**

預設匣道

預設匣道

192.168.2.1

DNS

DNS1

192.168.2.1

DNS2

8.8.8.8

- **虛擬網路服務**：可啟用或關閉虛擬網路功能，預設值是指啟用虛擬網路 0。
- **IP 設定**：可啟用/關閉虛擬網路區域的 VLAN IP, 或修改虛擬網路的 IP 位址/子網路遮罩。



虛擬網路服務(VLAN)功能，系統會自動保留一組 VLAN 作為管理使用。

系統管理

Access Point 0

☒ 啟用

☐ 關閉

Access Point 1

☒ 啟用

☐ 關閉

802.1d Spanning Tree

☐ 啟用

☒ 關閉

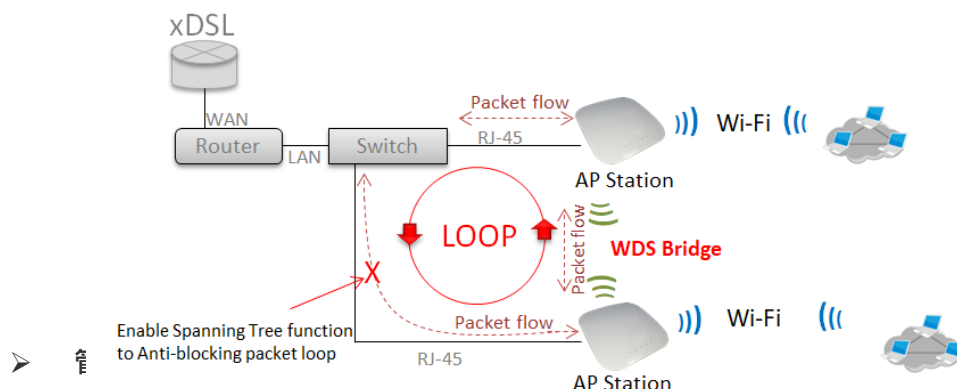
管理埠

☒ 啟用

☐ 關閉

系統管理：

- **Access Point 0 (2.4G)**：可針對虛擬網路(VLAN 下的 2.4G 無線基地台)啟用或關閉。
- **Access Point 1 (5G)**：可針對虛擬網路(VLAN 下的 5G 無線基地台)啟用或關閉。
- **802.1d Spanning Tree**：簡稱為 STP，可啟用或關閉 Spanning Tree 功能，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。



- **VLAN Tag 設定:** 設定 VLAN 使用的相對 tags。

ETH1 虛擬網路標記設定：

ETH1 虛擬網路標記設定

VLAN TAG

☐ 1-4096

- **網路埠 VLAN Tag Setup：** 使用標準 802.1Q 規範，可關閉或啟用功能。可自行定義對應 ETH1 實體網路埠的 tag，可設置 1~4096。

ETH2 虛擬網路標記設定：

ETH2 虛擬網路標記設定

VLAN TAG

☐ 1-4096

- **網路埠 VLAN Tag Setup：** 使用標準 802.1Q 規範，可關閉或啟用功能。可自行定義對應 ETH2 實體網路埠的 tag，可設置 1~4096。



注意：倘若 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。

設定完成後請點選儲存設定，並按下「重新啟動」按鈕，完成套用新設定。

4-2-2. DHCP 伺服器

網路設定(下拉式選單功能)：於虛擬網路列表上，點擊“網路”按鈕旁小箭頭，可設定 DHCP 伺服器、頻寬控制、Radio 0(2.4G) 或 Radio 1(5G)無線基地台等功能。

DHCP服務

模式

☒ 啟用
 ☐ 關閉

- **DHCP 伺服器：**可啟用或關閉 DHCP 伺服器服務。

DHCP設定	
起始IP位址	192.168.2.10
結束IP位址	192.168.2.100
子網路遮罩	255.255.255.0
預設閘道	192.168.2.254
主要DNS伺服器位址	192.168.2.254
次要DNS伺服器位址	
WINS伺服器位址	
網域名稱	
IP租用時間	86400

- **起始 IP 位址：**設定 DHCP 所派發的起始 IP 位址。
- **結束 IP 位址：**設定 DHCP 結束派發的 IP 位址。
- **子網路遮罩：**設定 IP 的子網路遮罩。
- **預設閘道：**設定 DHCP 派發的預設閘道位址。
- **DNS 伺服器位址：**設定 DHCP 派發的 DNS 伺服器位址。
- **WINS 伺服器位址：**若網路環境有架設 WINS 解析伺服器，可在此設定 WINS 的 IP 位址
- **Domain：**設定網域名稱。
- **IP 租用時間：**當 DHCP 伺服器派發 IP 後，可設定多久時間結束租用拿回 IP 位址，預設值為 86400 秒。



Notice

1. 若網路架構中無 DHCP 伺服器或者是架構中想利用第二台 DHCP 伺服器去分派 IP 時，管理者就可以啟用此功能，來設定網段去分派 IP 位址。
2. 若網路環境有 2 台 DHCP 伺服器，須注意 IP 位址的派送請勿重複，避免造成 IP 衝突。

DHCP用戶列表					
#	IP位址	MAC位址	主機名稱	Expired	執行
-	-	-	-	-	-

➤ **DHCP 用戶列表**：當 DHCP 伺服器派發出去的 IP 位址將記錄在此列表上。

- ✓ **IP 位址**：顯示已派送出去給設備使用的 IP 位址
- ✓ **MAC 位址**：顯示設備的 MAC 位址
- ✓ **主機名稱**：顯示連接之主機名稱
- ✓ **Expired**：顯示 IP 租用的到期時間
- ✓ **執行**：是否要將此設備(MAC)列為固定 IP 位址的配送

Static Lease IP Setup				
註解				
IP位址				
MAC位址				新增

Static Lease IP List				
#	註解	IP位址	MAC位址	執行
-	-	-	-	-

➤ **固定 IP 設置**

- ✓ **Static Lease IP Setup**：若有特定設備需取得 DHCP 伺服器固定派發的 IP 位址，可在此上面設定設備的 MAC 位址以及固定要取得的派送 IP 位址即可。
- ✓ **Static Lease IP List**：當設定完成 Static Lease IP Setup 後，資訊將列入此名單內。

4-2-3. 頻寬控制

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

頻寬控制

模式

☒ 啟用
 ☐ 關閉

Airtime Fairness

☐ 啟用
 ☒ 關閉

Total Bandwidth Control

模式

☐ 啟用
 ☒ 關閉

上傳

10240

Kbps

下載

10240

Kbps

- 頻寬控制 / Total Bandwidth Control
- **模式:** 管理員可以選擇啟用此虛擬網路(VLAN)的頻寬管理。
 - **Airtime Fairness:** 能讓 TX/RX 流量平衡, 不至於讓上下載落差太大(此功能應用在 AP+Client 橋接或 WDS 橋接上)。
 - **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 RuleList							
#	啟動	Rule Mode	Value1	Value2	Upload(Kbps)	Download(Kbps)	註解
1	☐	ANY			1024	1024	
2	☐	ANY			1024	1024	
3	☐	ANY			1024	1024	

- **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。

設定完成記得儲存&系統重新啟動才可正常運行。

4-2-4. 無線基地台 Radio 0(2.4G) / Radio 1(5G)設定

加密模式

無線基地台 ☒ 啟用 ☐ 關閉

SSID名稱

可視SSID ☒ 啟用 ☐ 關閉

隔離無線使用者 ☒ 啟用 ☐ 關閉

連線限制 ☒ 啟用 ☐ 關閉

使用者連線數

加密類型

➤ 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，最大設定支援同時 128 個使用者存取同一個 SSID。

➤ 加密類型：管理者可設定 WEP、WPA / WPA2-Personal、WPA / WPA2-Enterprise、WPA3 及 802.1x 等 5 種加密模式。

加密類型

WEW

Open System

WEW

WPA/WPA2 Personal

WPA/WPA2 Enterprise

WPA3

802.1x



請注意：WEP 加密模式目前已知並非為最安全無線加密方式，且選用 WEP 加密方式將無法支援 802.11ac/ax 以上速率，不建議您繼續使用此種 WEP 加密模式，建議您至少改用符合 802.11ac/ax 速率相對應支援的 WPA / WPA2 以上的加密模式，以增加您無線網路安全性。

- **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)。

WEP Settings

WEP Auth Method

Open system

WEP Length

64 bits

WEP Key

.....

Key Index

2

● WEP :

- ✓ **WEP Auth Method 模式**：選取您欲使用的 WEP 無線認證方式，可選擇 WEP Open system 開放認證方式或選擇 WEP Shared 密碼認證方式。
- ✓ **WEP Length**：可選擇 64bits、128bits、156bits 三種加密長度，選取您欲使用的無線加密金鑰長度，目前您可以選擇使用 64bits、128bits 與 152bits 等三種加密金鑰長度，但您必須要先確定您的無線用戶端使用的無線網路卡也支援相對應的無線金鑰長度。
- ✓ **WEP Key**：輸入 16 位元 (HEX) 的金鑰數值，共有四組可選擇設定。
- ✓ **Key Index**：可為您的 WEP 預先設定 4 組 WEP Key(金鑰數值)。未來無線用戶端若要進行連線，可選擇要使用哪一組無線金鑰作加密連線建立。



Notice

請注意：若您選擇使用 WEP 加密模式，請依照以下需求輸入相對應的 WEP 金鑰數值。

64bits：

10 組 Hex 十六進位字元 (0~9、A~F 與 a~f 都可以使用)

5 組 ASCII 字元 (0~9、A~Z 與 a~z 都可以使用)

128bits：

26 組 Hex 十六進位字元 (0~9、A~F 與 a~f 都可以使用)

13 組 ASCII 字元 (0~9、A~Z 與 a~z 都可以使用)

152bits:

32 組 Hex 十六進位字元 (0~9、A~F 與 a~f 都可以使用)

16 組 ASCII 字元 (0~9、A~Z 與 a~z 都可以使用)



密碼設定

WPA模式

自動 (WPA或WPA2)

加密演算法

自動

主要金鑰群組更新時間

600

秒

金鑰

WPS

☐ 啟用
 ☒ 關閉

WPS Push Button

Push Button

- **WPA / WPA2-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。



Notice

請注意：設定 WEP 或 TKIP 加密時，資料速率不會超過 54 Mbps，IEEE 802.11n 協定起禁止使用具有 WEP 或 TKIP 的高輸送量作為單播金鑰。如果您使用這些加密方法（例如 WEP、WPA-TKIP、WPA2-TKIP），您的資料速率將降至 54 Mbps，或若是和商業上刻意需求，例如藉此控制末端使用者不能以高於 54Mbps 速率連接無線時的應用。

- ✓ **主要金鑰群組更新時間：**使用者可設定主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。

Radius伺服器設定

WPA模式

自動 (WPA或WPA2)

加密演算法

自動

主要金鑰群組更新時間

600

秒

Radius伺服器

Radius埠

1812

埠號

Radius 密鑰

- **WPA / WPA2-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。



Notice

請注意：設定 WEP 或 TKIP 加密時，資料速率不會超過 54 Mbps，IEEE 802.11n 協定起禁止使用具有 WEP 或 TKIP 的高輸送量作為單播金鑰。如果您使用這些加密方法（例如 WEP、WPA-TKIP、WPA2-TKIP），您的資料速率將降至 54 Mbps，或若是和商業上刻意需求，例如藉此控制末端使用者不能以高於 54Mbps 速率連接無線時的應用。

- ✓ **主要金鑰群組更新時間：**使用者可設定主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。

WPA3 Settings

SAE Password

新增

SAE PWE

☐ 啟用
 ☒ 關閉

SAE MFP

☐ 啟用
 ☒ 關閉

- **WPA3 :**

802.11ax 對等實體同時驗證模式(通過認證密碼訊息，用密碼進行身分驗證)，有別於 Pre-Shared Key(預先共享金鑰密碼，密碼導出方式)。

- ✓ **SAE Password :** 管理者設定此虛擬無線網路 SSID 使用 WPA3 演算時 SAE 至少 8 字元連線密碼。
- ✓ **SAE PWE :** 選擇性啟用 SAE PWE (密碼元素) 功能，在交換 SAE 身份驗證消息之前，雙方將會生成一個私密元素 PWE (密碼元素) 和兩個私密值 (rand 和掩碼) 方式進行進階驗證交換。
- ✓ **SAE MFP :** SAE 密碼認證機制加入更安全防竊防窺防側錄密碼的管理幀保護 (MFP)，此模式若在 AP 上啟用請確保在此模式下運行的 AP 和客戶端都需要管理幀保護 (MFP) 支援。



WPA3 是目前可用於 Wi-Fi 設備的最新、最安全的協議。它適用於所有支持 Wi-Fi 6 (802.11ax) 的存取端網卡設備，使用時必須無線存取網卡同步支援，倘若無線存取端網卡不支援 WPA3 演算模式，建議您調整使用為 WPA2 / AES 演算模式。

Radius伺服器設定

金鑰長度

☒ 64位元
 ☐ 128位元

Radius伺服器

Radius埠

1812

埠號

Radius 密鑰

- **802.1x**

- ✓ **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。

4-2-5. MAC 過濾

於 UI 介面點選「MAC 過濾設定」，可進入「ACL 存取控制」設定頁面。使用者可設定 ACL 加以控制用戶端連結，點選無線設定，點選虛擬 AP 設定，點選所要設定 ESSID 的 ACL 設定進入頁面，設定方式如下列：

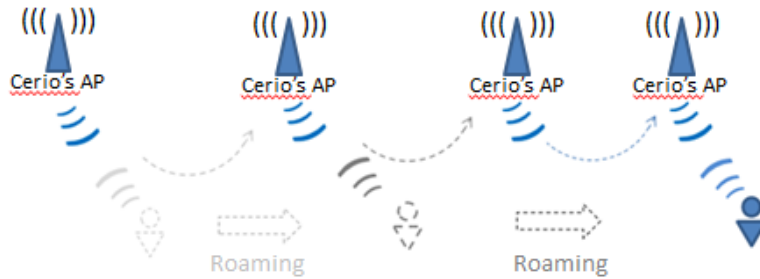
- **規則:** 使用者可從下拉清單選取設定，可設定關閉、只阻擋 MAC 清單或只允許 MAC 清單等，使用方式如下：
 - **關閉：** 關閉存取控制設定功能，所有無線使用者皆可以連線至無線基地台。
 - **只阻擋 MAC 清單：** 啟用此功能，若無線用戶端 MAC 位址設定於列表中則該無線用戶端則此 MAC 的清單之無線設備是不允許連線至此無線基地台。
 - **只允許 MAC 清單：** 啟用此功能，若無線用戶端 MAC 位址設定於列表中則該無線用戶端則此只有以下的 MAC 清單之無線設備允許連線至此無線基地台。
- **新增 MAC 位址：** 輸入要管理的使用者設備中 MAC 位址。

- **MAC 位址列表：** 被管理設備的 MAC 位址將列出至表單內。

MAC位址列表					
#	MAC位址	執行	#	MAC位址	執行
1	aa:bc:dd:ef:11:23	刪除	2	aa:bc:dd:ed:11:24	刪除

設定完成記得儲存&系統重新啟動才可正常運行。

4-2-6. 802.11r Fast Roaming



IEEE 802.11r 的技術，作用是將整個區域網路佈建的無線基地台所涵蓋之訊號範圍，讓無線使用端遊走無線基地台之間，迅速轉跳較佳的無線基地台連接，轉跳過程不中斷。



當建置 802.11r 無線漫遊平台時，無線使用者設備須有支援 802.11k 功能，才能正常的運作。

802.11r/802.11k 快速漫遊

快速漫遊

☒ 啟用

☐ 關閉

- **快速漫遊：**啟動或關閉漫遊功能。

快速漫遊設定

Mobility Domain

a1b2

R0 Key Lifetime

10000

Reassoc期限

1000

R0/NAS Identifier

ap.example.com

R1 Identifier

000102030405

R1 Push

☐ 啟用

☒ 關閉

- **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。

- **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**：自動連接 R1 Key Holders

R0 Key holders

MAC位址

目的端 MAC 位址

NAS Identifier

(1-48 octets)

128-bit Key

128-bit key as hex string

新增

- **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 Identifier**：輸入 AP 的 NAS Identifier 網域名稱。
 - **128-bit Key**：輸入一組共用的 128-bit Key 碼。

R0 Key Holder List				
#	MAC位址	NAS Identifier	128-bit Key	執行
1	8c:4d:ea:00:11:22	cerio.com.tw	8c4dea00112233445566...	刪除

輸入確認後將列入以下 R0 Key 表單內，如上圖輸入

R1 Key Holders

MAC位址

目的端 MAC 位址

R1 Identifier

R1 Identifier

128-bit Key

128-bit key as hex string

新增

- **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 Identifier**：輸入 AP 的 R1 Identifier 網域名稱。
 - **128-bit Key**：輸入一組共用的 128-bit Key 碼。

R1 Key Holder List				
#	MAC位址	NAS Identifier	128-bit Key	執行
1	00:11:22:33:44:50	00:01:02:03:04:05	11223344556677889900...	刪除

輸入確認後將列入以下 R1 Key 表單內，如上圖輸入

4-3. 網頁認證功能

此功能主要為啟動熱點網頁身份驗證，支援本機帳戶認證 / RADIUS 伺服器帳戶認證 / OAuth 2.0 開放性帳戶認證及訪客認證。當網頁驗證成功後，才能進行使用網路服務相關資源。

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 ▾


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。

- #：顯示虛擬網路可設定之組別。(例如 0 表示 VLAN0 之虛擬網路)
- 虛擬網路服務：顯示每組的虛擬網路目前是否啟用或停用。
- 網頁認證功能：顯示每組的網頁認證功能目前是否啟用或停用。

網頁認證功能	
網頁認證功能	☒ 啟用 ☐ 關閉

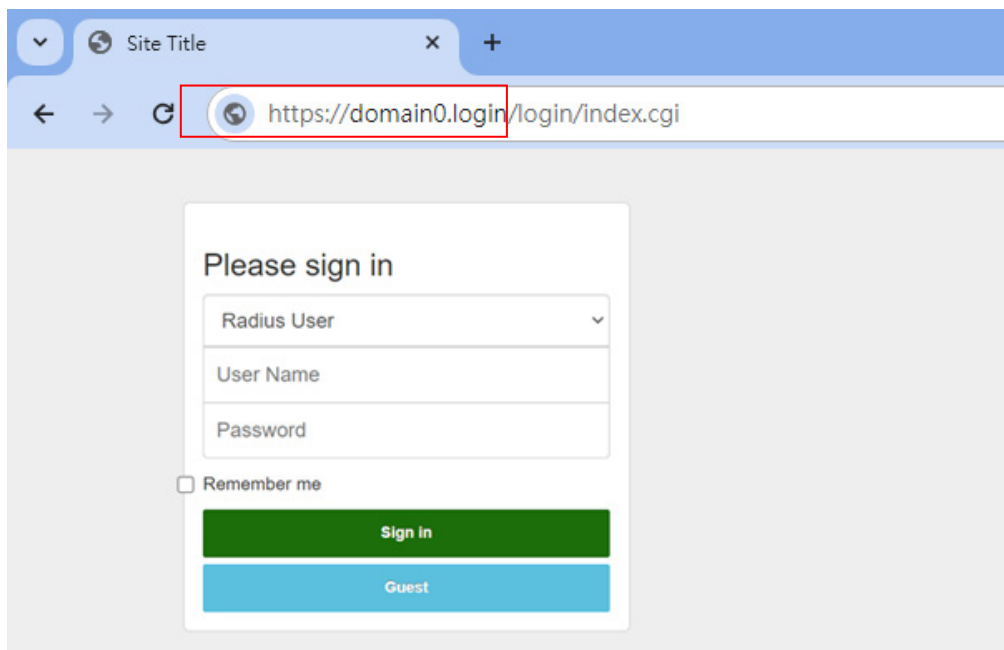
設定認證功能

多重登入	☐ 3	User(s)
登入超時	10	Minutes
URL 導向	http://www.google.com	
登入URL位址	domain0.login	
認證日誌	☐ 啟用 ☒ 關閉	
Session Log	☐ 啟用 ☒ 關閉	

- **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**：設定自動觸發登入頁面的網頁位址。當啟動網頁欲登入觸發或直接輸入預設值的登入頁面網址 <http://domain0.login> 即可快速跳轉至完整的登入認證登入起始頁面 <http://domain0.login/login/index.cgi>，若您希望使用 <https://domain0.login> 則請務必確認“管理介面登入設定是否有開啟 HTTPS 登入開放使用，請參考 3-1 系統管理➡管理介面登入設定，或如下圖示提示

管理介面登入設定

HTTP	☒	80	埠號
HTTPS	☒	443	埠號
Telnet	☒	23	埠號
SSH	☐	22	埠號



- **認證日誌**：可選擇啟用或關閉，啟用可記錄使用者登入登出資訊存放至 SysLog 伺服器上，（此部分管理控制器日誌伺服器功能請參考 智鼎公司 相關“AP 管理控制器”系列產品手冊內“認證日誌”詳細說明）。
- **Session Log**：可選擇啟用或關閉，啟用可記錄使用者的上網 Session 資訊存放至遠端管理控制器的 Sysme Log Server 日誌伺服器上備存，（此部分管理控制器日誌伺服器功能請參考 智鼎公司 相關“AP 管理控制器”系列產品手冊內“Session 日誌”詳細說明）。



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 伺服器上。

※ **設定本機用戶**：可選擇“啟用”或“關閉”使用本機帳號認證登入。

設定本機用戶

建立本機帳戶名單

☐ 啟用
 ☒ 關閉

顯示名稱

Local User



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。

- ※ **RADIUS 設定**：網頁認證方式支援遠端 RADIUS 伺服器認證，若環境中已有使用 RADIUS 伺服器做安全認證帳戶，此功能啟用可將網頁認證之帳戶指向內部的 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設定

Radius

☒ 啟用
 ☐ 關閉

顯示名稱

Radius User

主要伺服器的IP位址

192.168.2.1

次要伺服器的 IP 位址

Options

認證埠

1812

埠號

計費服務

☐ 1813

埠號

認證類型

☐ PAP
 ☒ CHAP

密鑰

Must



- **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。

4-3-1. 遊客

可啟用或停用此服務，此功能主要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，管理者可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。

遊客

服務

☒ 啟用
 ☐ 關閉

登入類型

☒ 一次性
 ☐ Multiple Time

Count Limit

10

登入時間

10

Minutes

QoS

☐ 啟用
 ☒ 關閉

上傳

512

Kbps

下載

512

Kbps

- **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。

4-3-2. 建立本機使用者帳戶名單

可在此頁面可簡易與快速建立網頁認證需要時的“ 本機使用者” 登入帳密，此為簡單方式的使用者帳密建立使用功能，最多 10 筆資料。

建立本機使用者

使用者名稱

Local User

密碼

(4-32 chars)

新增

本機使用者列表

#	名稱	執行
1	user-1	刪除
2	user-2	刪除

- 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。
- # 本機使用者列表：將顯示所建立的所有帳戶帳號。

4-3-3. OAuth 2.0

- 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。

OAuth 2.0 Provider List				建立新的Provider
#	啟動	Provider	執行	
1	停用	Google	編輯	
2	停用	Facebook	編輯	

Google：管理者需先至 Google 的 OAuth2.0 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。

OAuth 2.0

Provider

Google

啟動

☒ 啟用
 ☐ 關閉

OAuth 2.0 設定

用戶端 ID

用戶端密鑰

進階

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。

Walled URL		
Walled URL		新增
Walled URL 列表		
#	Walled URL	Action
1	accounts.google.com	刪除
2	accounts.google.com.tw	刪除
3	ssl.gstatic.com	刪除
4	lh6.googleusercontent.com	刪除

Google 的 OAuth2.0 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

API 管理員	憑證
總覽	憑證 OAuth 同意畫面 網域驗證
憑證	API 憑證 您需有憑證才能存取 API。請啟用您要使用的 API，然後再建立這些 API 所需的憑證。取決於 API，您可能需要 API 金鑰、服務帳戶或 OAuth 2.0 用戶端 ID。詳情請參閱 API 說明文件。 建立憑證

OAuth 用戶端 ID

要求使用者同意您的應用程式存取其資料。
適用於 Google 日曆等 API。

2. 選擇網路應用程式

應用程式類型

- ☒ 網路應用程式
- ☐ Android [瞭解詳情](#)
- ☐ Chrome 應用程式 [瞭解詳情](#)
- ☐ iOS [瞭解詳情](#)
- ☐ PlayStation 4
- ☐ 其他

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

已授權的 JavaScript 來源

這是用戶端應用程式的來源 URI，可用於瀏覽器發出的要求。其中不得包含萬用字元 (http://*.example.com) 或是路徑 (<http://example.com/subdir>)。如果您使用的是非標準的通訊埠，就必須把這個通訊埠包含在來源 URI 中。

<http://domain0.login.com>

×

<http://www.example.com>

已授權的重新導向 URI

重新導向 URI 用於網路伺服器發出的要求。使用者透過 Google 進行驗證後，系統就會將他們重新導向至應用程式中的這個路徑。此路徑會附帶存取的授權碼。路徑中必須含有通訊協定，不得含有網址片段或相對路徑，而且不能是公開的 IP 位址。

<http://domain0.login.com/login/callback.cgi>



Notice

管理者必須確定 Google Developers 的 “Redirect URI” 和 “JavaScript ORIGINS” 的位址必須與系統的 Login URL 所設定的 “JavaScript ORIGINS” 要一樣才能正常運作請回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 ORIGINS: <http://domain0.login.com>

REDIRECT URI : <http://domain0.login.com/login/callback.cgi>

而在系統上的 Login URL 必須與 Google 的 JavaScript ORIGINS 一樣

設定認證功能

多重登入

☐ 3
 User(s)

登入超時

10
 Minutes

URL 導向

<http://www.google.com>

登入URL位址

domain0.login.com

Session Log

☒ 啟用
 ☐ 關閉

4. 確認建立後將得到一組 ID 與密鑰

OAuth 用戶端

這是您的用戶端 ID

您的用戶端密鑰如下

確定

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

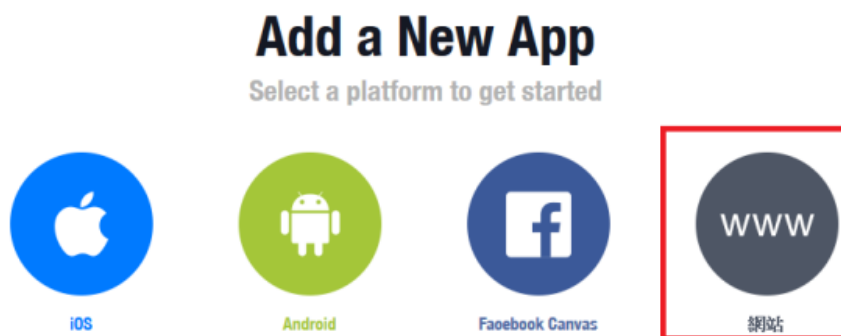
請注意，此為第三方認證功能，認證規則將以第三方公告為主

Facebook 的 OAuth2.0 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

Create a New App ID

Create **OAuth-TEST** App?

聯絡電子郵件

用於應用程式相關的重要溝通事宜

類別

選擇類別 ▾

一旦繼續，就代表你同意 **Facebook** 開放平台政策

取消

建立應用程式編號

4. 之後可在基本設定內設定網址，新增一筆 URL

<http://domain0.login.com/login/callback.cgi>

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/>

設定認證功能

多重登入

☐ 3
 User(s)

登入超時

10
 Minutes

URL導向

<http://www.google.com>

登入URL位址

domain0.login.com

Session Log

☒ 啟用
 ☐ 關閉

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。

OAuth 2.0

Provider

[Facebook](#)

啟動

☒ 啟用
 ☐ 關閉

OAuth 2.0 設定

用戶端 ID

用戶端密鑰

進階

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。



上述步驟是依照 Google 及 Facebook 步驟申請及設定(僅供參考，詳細則以第三方說明為主)
第三方認證伺服器(如 Google 及 Facebook)申請確認後，將產生客戶端 ID 及客戶端密鑰。

檢查線上認證使用者

此資訊頁面主要可以即時檢查目前在線的認證使用者資訊。

請點擊"系統狀態" → "線上使用者" 檢查認證成功的使用者。

■ 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
0	ON	2	1384	1079	1.77MB	68.18KB	詳細
1	OFF	0	0	0	0B	0B	-
2	OFF	0	0	0	0B	0B	-
3	OFF	0	0	0	0B	0B	-

■ Authentication Zone 0 Online Users

#	認證方式	Username	IP位址	MAC位址	登入時間	下載封包	上傳封包	下載位元	上傳位元	執行
1	Local	danny	192.168.2.20		2016/01/01 00:39:28	285	362	96.98KB	69.02KB	登出
2	Local	test	192.168.2.22		2016/01/01 00:39:46	22807	21410	31.17MB	1.25MB	登出

認證日誌

此資訊頁面紀錄所有認證使用者的登入帳號及登入/登出的時間外，並統計認證使用者在使用的時間內所使用多少上下傳流量。

請點擊"系統狀態" → "認證資訊" 檢查認證成功的使用者。

#	日期時間	系統狀態	使用者	IP位址	MAC位址	下載封包	上傳封包	下載位元	上傳位元
1	2016/01/01 00:13:35	LOGIN		192.168.2.23		0	0	0B	0B
2	2016/01/01 00:14:26	LOGOUT		192.168.2.23		66	58	18.62KB	20.56KB
3	2016/01/01 00:14:55	LOGIN	test	192.168.2.24		0	0	0B	0B
4	2016/01/01 00:17:01	LOGOUT	test	192.168.2.24		1966	1687	1.95MB	167.13KB
5	2016/01/01 00:29:38	LOGIN	danny	192.168.2.21		0	0	0B	0B

4-3-4. POP3/IMAP Server

POP3/IMAP Server

服務 ☒ 啟用 ☐ 關閉

POP3/IMAP Settings

顯示名稱

模式 ☒ POP3 ☐ IMAP

Host

埠號 埠號

Connect Type

- 服務：可啟動或關閉 POP Server 帳戶認證功能服務。
- 顯示名稱：輸入所想要顯示的名稱。
- 模式：POP3 及 IMAP 兩種型態設定。
- Host：POP 伺服器的網址或 IP 位址。
- 埠號：POP 伺服器所使用的服務埠號碼。
- Connect Type：選擇 POP 伺服器的連結類型 STARTTLS 或 SSL/TTL 或 None。
- POP3 伺服器測試：設定完成後儲存後，可以輸入一組電子郵件帳號及密碼來測試 POP 伺服器設定是否正確。

4-3-5. 客製化頁面

此功能主要可以編輯認證的網頁登入頁面。可自行編輯去支援多國語系，也可透過 HTML 和 CSS 語法自行去客製化認證的登入頁面。

頁面設定

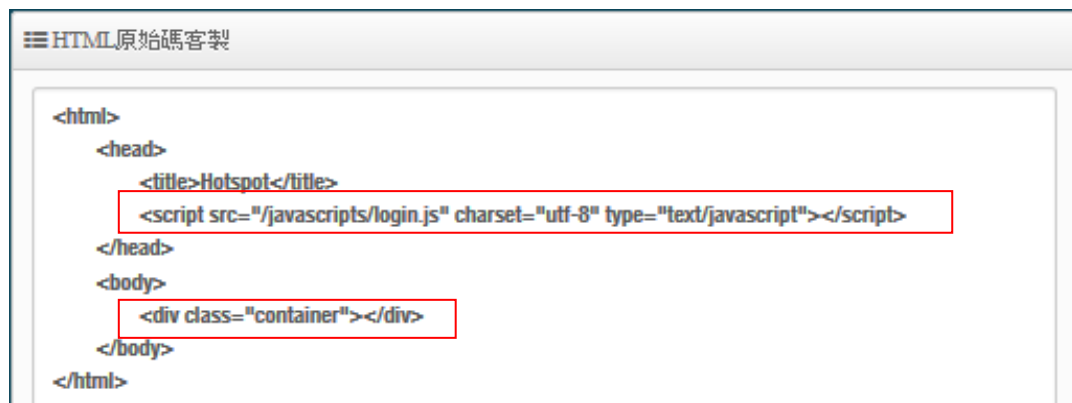
Template ☒ 啟用 ☐ 關閉

多語系 ☐ 啟用 ☒ 關閉

- **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。
- 管理者可透過設定頁面去修改登入頁面的背景及字體顏色等。



- 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，編輯 html 原始碼最多可輸入 4096 字元，如下範例：

```

HTML 原始碼編輯器

<html>
<head>
<link rel="stylesheet" type="text/css" href="http://www.cerio.com.tw/login_page_demo/css.css" />
<script src="/javascripts/login.js" charset="utf-8" type="text/javascript"></script>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Web Authentication</title>
</head>
<body>
<center>
<table width="480" border="0" cellpadding="0" cellspacing="0">
<tr>
<td colspan="6" height="76"></td>
</tr>
<tr>
<td colspan="6" height="180" class="backg">
<div> Web Authentication Login Page for CenOS 5.0 </div>
<div id="windows1">
<div class="win_font">Sign in</div>
<div class="container"></div>
</div></td></tr>
<tr>
<td colspan="6">
<div id="abc" style="display:none" mce_style="display:none">
<a href="http://www.google.com.tw" class="css_btn_class">Google</a>
<a href="http://www.yahoo.com.tw" class="css_btn_class">Yahoo</a>
<a href="http://www.cerio.com.tw" class="css_btn_class">CERIO</a>
</div>
</td></tr>
</table>
</body>
</center>
</html>
    
```

預覽 儲存



Notice

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，本公司不支援協助教導語法的使用，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。

確認編輯完成後，請點擊儲存鈕後，即可點擊預覽進行所編輯之網頁樣式





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，必須先上傳至網站伺服器，透過超連結方式去連結圖檔。
2. 在系統的 Walled Garden 功能必須增加要上傳圖檔或 CSS 檔案的伺服器 IP 位址。

4-3-6. 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。

語系列表				建立新的語系
#	預設值	語系		執行
1	★	English		編輯

- 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

基本語言	
網站標題	CenOS4.0頁面
登入標題	CERIO登入頁面
使用者名稱	使用者名稱
密碼	密碼
記得我	勾選記住我的帳密
登入	確認登入
訪客	訪客登入

Please sign in

User Name

Password

☐ Remember me

CERIO登入頁面

使用者名稱

密碼

☐ 勾選記住我的帳密



如圖完成後所呈現畫面

依訪客為例

Hello	您好	您好,
登入時間	登入時間	登入時間
Session Time	連接時間	2015/01/01 08:00:35
Traffic Volume	使用流量	10分
登出	登出	登出

4-3-7. Walled Garden

此功能是設定開放使用網站，當使用者連接 AP 模式的無線基地台後，若有開啟網頁認證登入功能如(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。

Walled Garden

顯示名稱

CERIO

IP位址/網域

www.cerio.com.tw

完整的 URL

http://www.cerio.com.tw

新增

Walled Garden 列表

#	名稱	IP位址/網域	執行
1	CERIO	www.cerio.com.tw	刪除

- **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 位址或網站的網址。
- **Full URL**：設定網站的 URL 網址。

※ 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。

當設定完成後點擊“新增”按鈕完成設定，並重新啟動系統讓功能正常運作。

4-3-8. 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 AAP 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。

特權名單

設備名稱

BOSS iPhone

IP位址

192.168.2.1

MAC位址

00:11:22:33:44:50

新增

特權名單列表

#	名稱	IP位址	MAC位址	執行
1	BOSS iPhone	192.168.2.1	00:11:22:33:44:50	刪除

- **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。

※ 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。

當設定完成後點擊“新增”按鈕完成設定，並重新啟動系統讓功能正常運作。

4-3-9. Bulk MAC Address

此功能與特權名單相類似，差異在這功能只驗證 MAC 位址，且 MAC 名單只允許透過上傳方式批量建置，當開啟此功能，只要 MAC 名單上的設備將不需做網頁驗證及可直接使用上網服務。

MAC 過濾規則

規則

關閉

儲存

Upload MAC Address

選擇檔案

沒有選擇檔案

上傳

沒有選擇檔案

- **規則：**管理員可啟用或關閉此功能。
- **Upload MAC Address:** 選擇 MAC 資料檔的位置，並按下上傳，即可將表單的 MAC 為只會入至此功能上進行系統判斷。

MAC位址列表

#	MAC位址	#	MAC位址	#	MAC位址	#	MAC位址	#	MAC位址
1	8C:4D:EA:04:A6:6F	2	8C:4D:EA:04:A6:62	3	8C:4D:EA:04:A6:65	4	8C:4D:EA:04:A6:68	5	8C:4D:EA:04:A6:6B
6	8C:4D:EA:04:A6:6E	7	8C:4D:EA:04:A6:71	8	8C:4D:EA:04:A6:74	9	8C:4D:EA:04:A6:77	10	8C:4D:EA:04:A6:7A
11	8C:4D:EA:04:A6:7D	12	8C:4D:EA:04:A6:80	13	8C:4D:EA:04:A6:83	14	8C:4D:EA:04:A6:86	15	8C:4D:EA:04:A6:89
16	8C:4D:EA:04:A6:8C	17	8C:4D:EA:04:A6:8F	18	8C:4D:EA:04:A6:92	19	8C:4D:EA:04:A6:95	20	8C:4D:EA:04:A6:98
21	8C:4D:EA:04:A6:9B	22	8C:4D:EA:04:A6:9E	23	8C:4D:EA:04:A6:A1	24	8C:4D:EA:04:A6:A4	25	8C:4D:EA:04:A6:A7

當確定完成後點擊重新啟動系統讓功能正常運作。

4-3-10. 設定檔

此功能主要能將已設定好的 VLAN#認證的設定值和 html 網頁登入的自定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

下載設定檔

下載

上傳設定檔

選擇檔案 沒有選擇檔案

上傳

虛擬網路客制化頁面

下載客製化頁面

下載

上傳客製化頁面

選擇檔案 沒有選擇檔案

上傳

4-4. Radius 伺服器

Radius 伺服器

服務

☒ 啟用
☐ 關閉

Radius 埠

1812

Radius 密鑰

(4-32 chars)

- 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。

4-5. Radius 帳戶設定

Radius用戶

使用者名稱

(3-32 chars)

密碼

(4-32 chars)

新增

匯出/匯入 使用者

匯出使用者檔案

匯出

從PC匯入

選擇檔案 沒有選擇檔案

匯入

Radius列表

#	名稱	執行	#	名稱	執行
-	-	-	-	-	-

- 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。

4-6. 無線設定

4-6-1. Radio 0 (2.4G)

一般設定

MAC位址

8c:4d:ea:05:1c:82

區域設定

Taiwan

無線運作模式

802.11ax

自動頻道

☐ 啟用
 ☒ 關閉

頻道

5 (2432 Mhz)

無線傳輸功率設定

等級 9

Slot Time

9

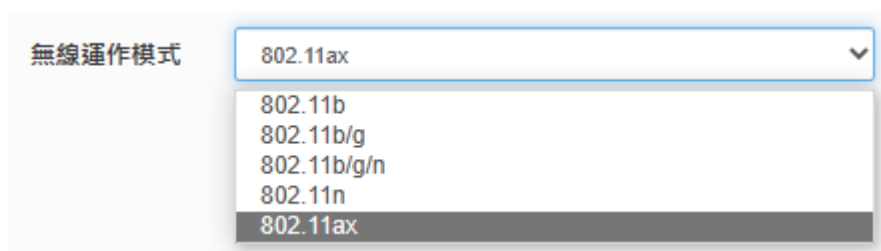
距離

ACK Timeout

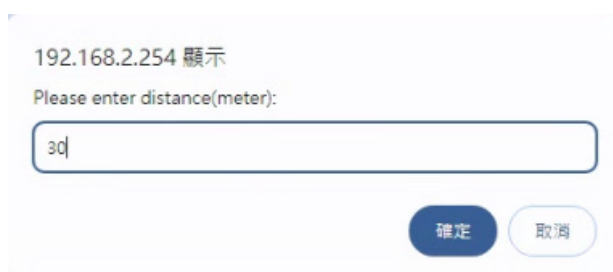
64

● 一般設定

- **MAC 位址**：顯示 2.4G (Radio 0)無線 MAC 位址。
- **區域設定**：可設定符合該設備安裝國家之區域，支援「US」、「EU」、「Japan」、「Taiwan」。
- **無線運作模式**：支援「802.11b」、「802.11b/g」、「802.11b/g/n」、「802.11n」、「802.11ax」五種模式，使用者可依需求使用做選擇。



- **自動頻道**：啟用時自動搜尋良好頻道進行連線，關閉時可依環境需求手動調整。
- **頻道**：依法規於不同地區之無線運作模式下有不同選擇，可配合向上/向下延伸。
- **無線傳輸功率設定**：可依所在環境需求，設置 RF 等級 1~等級 9 之功率。
- **Slot Time**：您可在此輸入 slot time 數值，當距離遠近，等待封包傳送時間將可調整快與慢。
- **距離**：當點下“**距離**”按鈕，將可以輸入點對點的橋接距離，系統會自動計算出該 Slot Time 與 ACK Timeout 的理想參考建議值，輸入距離以單位(公尺)計算。



- **ACK timeout**：當等待“ACKnowledgment frame”間隔太長而不被接收，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

設定 ACK Timeout 能加強長距離連線，更改數值能有最佳化設定，數值太低會使傳輸降低，數值太高可能有斷線的可能，建議保持預設值使用。

● HP Physical Mode

HT Physical Mode

TX/RX Stream	2T2R
頻道模式	20/40
延伸頻道	☐ 向上 ☒ 向下
Min MCS	4
Max MCS	11
Short GI	☒ 啟用 ☐ 關閉
封包聚合	☒ 啟用 ☐ 關閉
Aggregation Frames	32
封包聚合大小	50000

- **TX/RX Stream**：出廠傳送/接收預設值為 2T2R，可依特殊應用選擇調整 1T1R。



本產品 2.4Ghz 天線已是為內建 2x2 (2T2R)，若無特殊應需求時請保持此 2T2R 預設值的設定值。

- **頻道模式**：2.4G 可選擇 20 或 20/40Mhz 做為基地台與無線用戶間傳輸資料速度。
- **延伸頻道**：此功能僅於頻道模式選擇「20/40 Mhz」時，才可做上/下延伸選擇。
- **MIN MCS**：MCS 編譯是 802.11ax 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。
- **MAX MCS**：最大 MCS 編譯設定值，須注意 Max MCS 值須大於 Min MCS 值。
- **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**：將多個封包整合為一在傳送，主要為控制封包傳輸時過量，出廠預設值為啟用狀態，建議勿關閉。
- **Aggregation Frames**：封包聚集訊框大小。
- **封包聚合大小**：封包聚集的大小。

4-6-2. Radio 1 (5G)

一般設定

MAC位址

8c:4d:ea:05:1c:81

區域設定

Taiwan

無線運作模式

802.11ax

自動頻道

☐ 啟用
 ☒ 關閉

頻道

36 (5180 Mhz)

無線傳輸功率設定

等級 9

Slot Time

9

距離

ACK Timeout

64

● 一般設定

- **MAC 位址**：顯示 5G (Radio 1)無線 MAC 位址。
- **區域設定**：可設定符合該設備安裝國家之區域，支援「US」、「EU」、「Japan」、「Taiwan」。
- **無線運作模式**：支援 802.11a、802.11a/n、802.11n、802.11ac、802.11ax 五種模式，使用者可依需求使用做選擇。

無線運作模式

802.11ax

802.11a

802.11a/n

802.11n

802.11ac

802.11ax

- **自動頻道**：啟用時自動搜尋良好頻道進行連線，關閉時可依環境需求手動調整。
- **頻道**：依法規於不同地區之無線運作模式下有不同選擇。

****根據 NCC 釋出資料規範，台灣開放以下三種 5G 頻段供使用****

- 5250 ~ 5350MHz (CH52 5260MHz、CH56 5280MHz、CH60 5300MHz、CH64 5320MHz)
- 5470 ~ 5725MHz (CH100 5500MHz、CH104 5520MHz、CH108 5540MHz、CH112 5560MHz、CH116 5580MHz、CH120 5600MHz、CH124 5620MHz、CH128 5640MHz、CH132 5660MHz、CH136 5680MHz、CH140 5700MHz)
- 5725 ~ 5825MHz (CH149 5745MHz、CH153 5765MHz、CH157 5785MHz、CH161 5805MHz、CH165 5825MHz)



請注意：5470 ~ 5725MHz 頻段與軍方/氣象用的都普勒雷達頻率相衝突，在軍方優先民間次之的邏輯下，本主機符合設計若要使用這些頻率，設計搭載配合了 DFS(雷達掃描區) 和 TPC (EIRP 值大於 500mW 之設備) 功能，本主機當感測到目前頻率有其它人在使用時，會依照規範軟體自行跳開改採其它頻率；而 5250 ~ 5350MHz 只能在室內使用。
(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**：可依所在環境需求，設置 RF 等級 1~等級 9 之功率。
- **Slot Time**：您可在此輸入 slot time 數值，當距離遠近，等待封包傳送時間將可調整快與慢。
- **距離**：當點下“ **距離** ”按鈕，將可以輸入點對點的橋接距離，系統會自動計算出該 Slot Time 與 ACK Timeout 的理想參考建議值，輸入距離以單位(公尺)計算。

- **ACK timeout**：當等待“ACKnowledgment frame”間隔太長而不被接收，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。

● HP Physical Mode

- **TX/RX Stream**：出廠傳送/接收預設值為 2T2R，可依特殊應用選擇調整 1T1R。



本產品 5Ghz 天線已是為內建 2x2 (2T2R)，若無特殊應需求時請保持此 2T2R 預設值的設定值。

- **頻道模式**：5G 可選擇 20 或 20/40 Mhz 或 11ac/ax 80Mhz 做為基地台與無線用戶間傳輸資料速度。
- **MIN MCS**：MCS 編譯是 802.11ax 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。
- **MAX MCS**：最大 MCS 編譯設定值，須注意 Max MCS 值須大於 Min MCS 值。
- **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**：將多個封包整合為一在傳送，主要為控制封包傳輸時過量，出廠預設值為啟用狀態，建議勿關閉。
- **Aggregation Frames**：封包聚集訊框大小。
- **封包聚合大小**：封包聚集的大小。

4-6-3. 進階設定

進階設定

Beacon Interval	100	
DTIM 間隔	1	
Fragment Threshold	2346	
RTS Threshold	2346	
Short Preamble	☒ 啟用	☐ 關閉
IGMP Snooping	☒ 啟用	☐ 關閉
Greenfield	☒ 啟用	☐ 關閉
5G優先連線	☐ 10	RSSI Limit
RF on/off by Schedule	Always	
Location Tracking Log	☐ 600	秒

- **Beacon Interval**：輸入數值從 10 到 5000 sec，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。建議使用預設值
- **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。建議使用預設值
- **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。建議使用預設值
- **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。建議使用預設值
- **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。建議使用預設值
- **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。建議使用預設值
- **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。建議使用預設值
- **5G 優先連線(Band Steering)**：2.4GHz 與 5GHz 的網路同時存在時，自動以 5GHz 的用戶端連線至 5GHz 的網路為主要連接，以提升效能。可於“RSSI Limit”設定值內鍵入 2.4 GHz 連接最低的連接 RSSI 的門檻值，以此作為 5GHz 優先連線的介定值，也就是說以此介定當雙頻(2.4/5GHz)無線用戶與 AP 的 5GHz 訊號優於 2.4GHz 連線 RSSI 所設定的介定值，則本機將促使無線用戶自動以 5GHz 連線為優先。



【Band Steering 功能只限於雙頻無線網卡(至少具有 2.4G 與 5G 同時存的無線網卡配合存取使用)，若 Band Steering 打開，主要連接使用 5GHz 11ac/11ax，若雙頻無線網卡無支援此功能或是其他不明因素，會導致無線使用者無法正常連線。】

- **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。



【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。】

4-6-4. 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 Parameters 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	☐

- **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, 當此功能沒有被選取時, 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。

4-6-5. 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，可選擇啟用或停用。

WDS 設定

WDS 設定

☒ 啟用
 ☐ 關閉

Radio0 ESSID

default_wds0

Radio1 ESSID

default_wds1

加密類型

關閉

金鑰

MAC位址

Radio 0

8c:4d:ea:05:1c:82

Radio 1

8c:4d:ea:05:1c:81

當啟用 WDS 功能，可設定使用 Radio 0(2.4G) 或 Radio 1(5G) 做 WDS 等，而最大橋接於 2.4G+5G 共可設定 **16 組**，在 WDS 功能支援 VLAN tag 傳送，若在網域內有設定 Tag 時，WDS over Tag 將可把多組 Tag 帶至另一個橋接端點。

WDS Client Setup			
Radio 0		Radio 1	
啟用	MAC位址	啟用	MAC位址
☐		☐	
☐		☐	
☐		☐	
☐		☐	
☐		☐	
☐		☐	
☐		☐	
☐		☐	
☐		☐	

虛擬網路設定						
VLAN#	Radio 0			Radio 1		
	Native	TAG	TAG ID	Native	TAG	TAG ID
虛擬網路 0	☒	☐		☒	☐	
虛擬網路 1	☐	☐	101	☐	☐	101
虛擬網路 2	☐	☐	102	☐	☐	102

- **Radio ESSID**：依要使用連接的 Radio，請每台都輸入相同的 SSID 名稱。
- **加密類型**：關閉或啟動 AES 128bit 加密或 AES 256bit 加密功能，AES 加密自訂金鑰可輸入 0~9 數字或 A~Z 大小寫英文格式，支援可輸入 8~32 個字元金鑰加密演算在每台 WDS AP 彼此之間做安全加密傳輸互相連線。
- **金鑰**：設定符合格式的共享密鑰。
- **WDS 連接設定**：可設定使用 Radio 0(2.4G)做 WDS 或 Radio 1(5G) 做 WDS 無線訊號來做 WDS 橋接，請在 WDS Client Setup 此欄位中輸入橋接端的無線基地台 MAC 位址。



【WDS 注意事項】

1. 兩台無線基地台要使用 WDS 連線時，則兩台的頻道需要相同。
2. 假若兩台基地台分別 A 與 B，則 A 台的 WDS Client Setup 需設定 B 台的無線 MAC 位址，相對的 B 台的 WDS Client Setup 需設定 A 台的無線 MAC 位址。
3. 假若架構中必須使用 tag，2 邊的基地台可在虛擬網路設定的項目勾選多組 tag。
4. 用戶自行選擇是否使用 AES 加密進行 WDS 連線安全加密。

- **MAC 位址**：顯示此設備的可設定使用 Radio 0(2.4G) 或 Radio 1(5G) 的無線網卡位址。
- **虛擬網路設定：(WDS)**
 - **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。

4-6-6. WDS 狀態

Radio0連線用戶		
MAC位址	Rate(RX/TX)	RSSI
-	-	-
Radio1連線用戶		
MAC位址	Rate(RX/TX)	RSSI
-	-	-

顯示 Radio 0(2.4G) 或 Radio 1(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(RX 接收/TX 傳送)流量資訊。
- **RSSI**：顯示與另一端 WDS 連接中的無線訊號數品質。

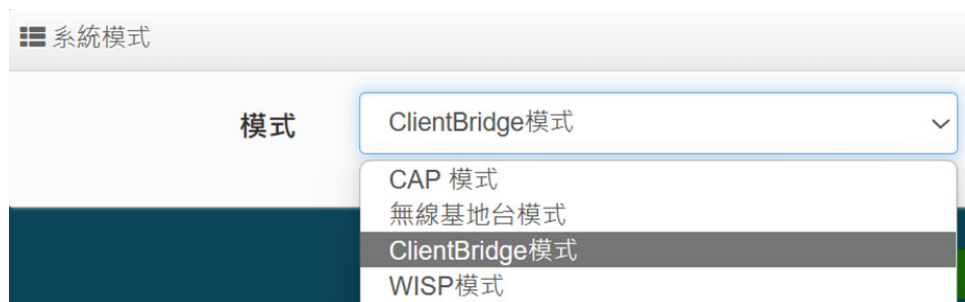


本產品 RSSI 訊號品質顯示以訊號強度衡量方式進行表示，最終以“數值正數”為大且表示為佳之方式。

5. Client Bridge 模式

若管理者需橋接或延伸無線基地台訊號時，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。

5-1. 模式設定



系統模式

模式

ClientBridge模式

CAP 模式

無線基地台模式

ClientBridge模式

WISP模式

5-2. 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

☒ 靜態IP位址

☐ 動態IP位址

靜態IP位址

IP位址

192.168.2.254

子網路遮罩

255.255.255.0

預設匣道

192.168.2.1

➤ 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。



使用動態 IP 位址須注意：因系統會自動取得 DHCP 派送的 IP 位址，而所取的 IP 位址將由上端 DHCP 伺服器運算確認後得到，取得 IP 位址則非固定，若管理人員要進入系統管理，必須由上端 DHCP 伺服器去查詢目前系統所取得的 IP 位址。

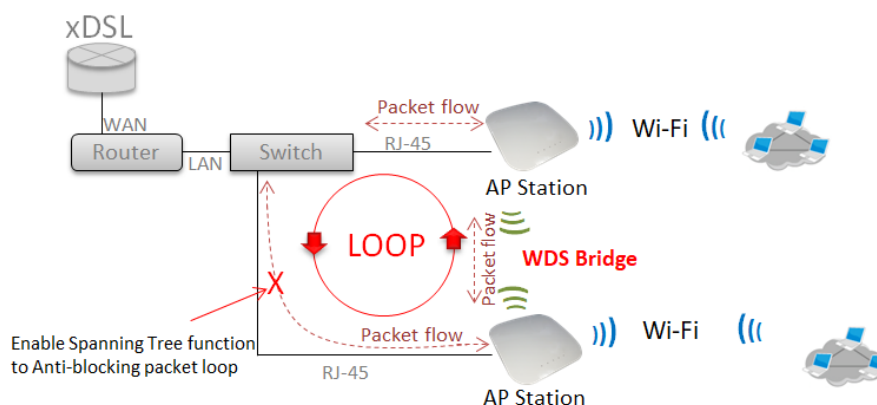
➤ **靜態 IP 位址：**

- **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。

The screenshot shows a web-based configuration interface with three sections:

- DNS:** Contains two input fields for '主要DNS伺服器' (Primary DNS Server) and '次要DNS伺服器' (Secondary DNS Server).
- 802.1d Spanning Tree:** Shows the '802.1d Spanning Tree' setting with two radio buttons: '啟用' (Enabled) and '關閉' (Disabled). The '關閉' option is selected.
- DHCP Forward:** Shows the 'DHCP Forward' setting with two radio buttons: '啟用' (Enabled) and '關閉' (Disabled). The '關閉' option is selected.

- **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 IP 位址採用動態 IP 取得，並啟用 Repeater 功能時，則需開啟 Forward 功能。



5-3. DHCP 設定

DHCP服務

模式

☒ 啟用
☐ 關閉

DHCP設定

起始IP位址	192.168.2.10
結束IP位址	192.168.2.100
子網路遮罩	255.255.255.0
預設閘道	192.168.2.254
主要DNS伺服器位址	192.168.2.254
次要DNS伺服器位址	
WINS伺服器位址	
網域名稱	
IP租用時間	86400

- 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)。

5-4. 無線設定

#無線基地台橋接及訊號延伸(Repeater AP)設定步驟，可協助管理人員建立與上端 AP 橋接及延伸無線基地台應用。

步驟 1：管理人員請先確認是要使用 2.4G 或 5G 頻段使用 Client 方式去連接上端無線基地台，假若上端 AP 是使用 2.4G 的頻段，則管理員需以 2.4G 頻段去搜尋站台。

以下使用 5G 為範例，至無線設定→ Radio 1 去啟用基地台模式，啟用後將會以 5G 頻段搜尋基地台。

一般設定

MAC位址

8c:4d:ea:05:1c:81

區域設定

Taiwan

無線運作模式

802.11ax

自動頻道

☐ 啟用
 ☒ 關閉

頻道

36 (5180 Mhz)

無線傳輸功率設定

等級 9

Slot Time

9

距離

ACK Timeout

64

步驟 2：進入至“無線設定”→“基地台橋接設定”後點擊“搜尋站台”按鈕開始搜尋附近的所有站台。

無線站台列表					搜尋站台
頻道	Signal	BSSID	ESSID	加密模式	設定
11	-74%		CerioGuard	WPA/WPA2 Personal	設定
9	-62%		Cerio_AP	None	設定
10	-77%		Guard	WPA/WPA2 Personal	設定
11	-73%		CerioGuest	None	設定

步驟 3：搜尋完成後，附近所有的無線基地台將會列出至表單內，請確實找出預想連線的 BSSID 名稱，並

點擊“設定”按鈕來設定此 BSSID 的帳號與密碼。

基地台橋接連線設定

SSID名稱

加密類型

WPA/WPA2 Personal

WPS Push Button

Push Button

密碼設定

加密模式

自動 (WPA或WPA2)

加密演算法

自動

金鑰



請注意站台的訊號值，假若所連接無線基地台的訊號值低於 40%表示此設備與上端無線基地台的連線訊號品質很差，建議請改善連線的訊號品質

當確認基地台橋接已設定完成後，請重新啟動系統並在“系統狀態”下檢查 **Radio 0 或 1** 橋接上端站台的資訊，若資訊有出現 BSSID 及速率等表示成功與 AP 連接。



如果步驟 2 完成後，在系統狀態下無出現 BSSID 及速率，有可能與上端的 IP 位址是不同網段，或是無法與上端 AP 正常連線。需確認上端 AP 或本機設定

步驟 4: 假若要設定延伸基地台，則可以開啟 Repeater AP 功能，管理人員可以點擊 “無線設定” → “Repeater AP 設定” 啟用功能並設定無線基地台資訊。預設值為開啟

加密模式

無線基地台

☒ 啟用
 ☐ 關閉

SSID名稱

default

可視SSID

☒ 啟用
 ☐ 關閉

隔離無線使用者

☒ 啟用
 ☐ 關閉

連線限制

☐ 啟用
 ☒ 關閉

使用者連線數

128

加密類型

Open System



當與上端 AP 做橋接時，切記 IP 位址不能衝突，以免造成網路不正常無法運作。

設定完成後，請點擊儲存並重新啟動完成其功能運作。

5-4-1. Radio 0 (2.4G)

一般設定

MAC位址

8c:4d:ea:05:1c:82

區域設定

Taiwan

無線運作模式

802.11ax

自動頻道

☐ 啟用
 ☒ 關閉

頻道

5 (2432 Mhz)

無線傳輸功率設定

等級 9

Slot Time

9

距離

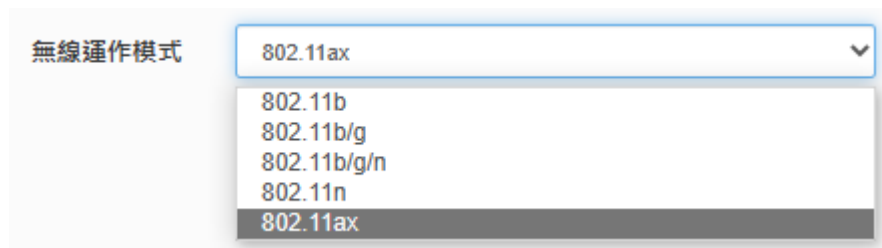
ACK Timeout

64



● 一般設定

- **MAC 位址：**顯示 2.4G (Radio 0)無線 MAC 位址。
- **區域設定：**可設定符合該設備安裝國家之區域，支援「US」、「EU」、「Japan」、「Taiwan」。
- **無線運作模式：**支援「802.11b」、「802.11b/g」、「802.11b/g/n」、「802.11n」、「802.11ax」五種模式，使用者可依需求使用做選擇。



- **自動頻道：**啟用時自動搜尋良好頻道進行連線，關閉時可依環境需求手動調整。
- **頻道：**依法規於不同地區之無線運作模式下有不同選擇，可配合向上/向下延伸。
- **無線傳輸功率設定：**可依所在環境需求，設置 RF 等級 1~等級 9 之功率。
- **Slot Time:** 您可在此輸入 slot time 數值，當距離遠近，等待封包傳送時間將可調整快與慢。
- **距離：**當點下“**距離**”按鈕，將可以輸入點對點的橋接距離，系統會自動計算出該 Slot Time 與 ACK Timeout 的理想參考建議值，輸入距離以單位(公尺)計算。



- **ACK timeout：**當等待“ACKnowledgment frame”間隔太長而不被接收，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

設定 ACK Timeout 能加強長距離連線，更改數值能有最佳化設定，數值太低會使傳輸降低，數值太高可能會有斷線的可能，建議保持預設值使用。

● HP Physical Mode

HT Physical Mode

TX/RX Stream

2T2R

頻道模式

20/40

延伸頻道

☐ 向上
 ☒ 向下

Min MCS

4

Max MCS

11

Short GI

☒ 啟用
 ☐ 關閉

封包聚合

☒ 啟用
 ☐ 關閉

Aggregation Frames

32

封包聚合大小

50000

- **TX/RX Stream**：出廠傳送/接收預設值為 2T2R，可依特殊應用選擇調整 1T1R。



本產品 2.4Ghz 天線已是為內建 2x2 (2T2R)，若無特殊應需求時請保持此 2T2R 預設值的設定值。

- **頻道模式**：2.4G 可選擇 20 或 20/40Mhz 做為基地台與無線用戶間傳輸資料速度。
- **延伸頻道**：此功能僅於頻道模式選擇「20/40 Mhz」時，才可做上/下延伸選擇。
- **MIN MCS**：MCS 編譯是 802.11ax 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。
- **MAX MCS**：最大 MCS 編譯設定值，須注意 Max MCS 值須大於 Min MCS 值。
- **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**：將多個封包整合為一在傳送，主要為控制封包傳輸時過量，出廠預設值為啟用狀態，建議勿關閉。
- **Aggregation Frames**：封包聚集訊框大小。
- **封包聚合大小**：封包聚集的大小。

5-4-2. Radio 1 (5G)

一般設定

MAC位址

8c:4d:ea:05:1c:81

區域設定

Taiwan

無線運作模式

802.11ax

自動頻道

☐ 啟用
 ☒ 關閉

頻道

36 (5180 Mhz)

無線傳輸功率設定

等級 9

Slot Time

9

距離

ACK Timeout

64

● 一般設定

- **MAC 位址**：顯示 5G (Radio 1)無線 MAC 位址。
- **區域設定**：可設定符合該設備安裝國家之區域，支援「US」、「EU」、「Japan」、「Taiwan」。
- **無線運作模式**：支援 802.11a、802.11a/n、802.11n、802.11ac、802.11ax 五種模式，使用者可依需求使用做選擇。

無線運作模式

802.11ax

802.11a

802.11a/n

802.11n

802.11ac

802.11ax

- **自動頻道**：啟用時自動搜尋良好頻道進行連線，關閉時可依環境需求手動調整。
- **頻道**：依法規於不同地區之無線運作模式下有不同選擇。

****根據 NCC 釋出資料規範，台灣開放以下三種 5G 頻段供使用****

- 5250 ~ 5350MHz (CH52 5260MHz、CH56 5280MHz、CH60 5300MHz、CH64 5320MHz)
- 5470 ~ 5725MHz (CH100 5500MHz、CH104 5520MHz、CH108 5540MHz、CH112 5560MHz、CH116 5580MHz、CH120 5600MHz、CH124 5620MHz、CH128 5640MHz、CH132 5660MHz、CH136 5680MHz、CH140 5700MHz)
- 5725 ~ 5825MHz (CH149 5745MHz、CH153 5765MHz、CH157 5785MHz、CH161 5805MHz、CH165 5825MHz)



請注意：5470 ~ 5725MHz 頻段與軍方/氣象用的都普勒雷達頻率相衝突，在軍方優先民間次之的邏輯下，本主機符合設計若要使用這些頻率，設計搭載配合了 DFS(雷達掃描區) 和 TPC (EIRP 值大於 500mW 之設備) 功能，本主機當感測到目前頻率有其它人在使用時，會依照規範軟體自行跳開改採其它頻率；而 5250 ~ 5350MHz 只能在室內使用。
(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**：可依所在環境需求，設置 RF 等級 1~等級 9 之功率。
- **Slot Time**：您可在此輸入 slot time 數值，當距離遠近，等待封包傳送時間將可調整快與慢。
- **距離**：當點下“**距離**”按鈕，將可以輸入點對點的橋接距離，系統會自動計算出該 Slot Time 與 ACK Timeout 的理想參考建議值，輸入距離以單位(公尺)計算。

- **ACK timeout**：當等待“ACKnowledgment frame”間隔太長而不被接收，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。

● HP Physical Mode

- **TX/RX Stream**：出廠傳送/接收預設值為 2T2R，可依特殊應用選擇調整 1T1R。



本產品 5Ghz 天線已是為內建 2x2 (2T2R)，若無特殊應需求時請保持此 2T2R 預設值的設定值。

- **頻道模式**：5G 可選擇 20 或 20/40 Mhz 或 11ac/ax 80Mhz 做為基地台與無線用戶間傳輸資料速度。
- **MIN MCS**：MCS 編譯是 802.11ax 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。
- **MAX MCS**：最大 MCS 編譯設定值，須注意 Max MCS 值須大於 Min MCS 值。
- **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**：將多個封包整合為一在傳送，主要為控制封包傳輸時過量，出廠預設值為啟用狀態，建議勿關閉。
- **Aggregation Frames**：封包聚集訊框大小。
- **封包聚合大小**：封包聚集的大小。

5-4-3. 進階設定

進階設定

Beacon Interval	100
DTIM 間隔	1
Fragment Threshold	2346
RTS Threshold	2346
Short Preamble	☒ 啟用 ☐ 關閉
IGMP Snooping	☒ 啟用 ☐ 關閉
Greenfield	☒ 啟用 ☐ 關閉
RF on/off by Schedule	Always
Location Tracking Log	☐ 600 秒

- **Beacon Interval**：輸入數值從 10 到 5000 sec，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。建議使用預設值
- **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。建議使用預設值
- **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。建議使用預設值
- **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。建議使用預設值
- **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。建議使用預設值
- **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。建議使用預設值
- **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。建議使用預設值
- **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。



【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。】

5-4-4. 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 Parameters 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 Parameters 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,當此功能沒有被選取時,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。

5-4-5. 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，則可設定要橋接地無線站台資訊，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。

無線站台列表					搜尋站台
頻道	Signal	BSSID	ESSID	加密模式	設定
-	-	-	-	-	-

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”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。

無線站台列表					搜尋站台
頻道	Signal	BSSID	ESSID	加密模式	設定
1	-80%			WPA/WPA2 Personal	設定
9	-62%		Cerio_AP_2.4G	None	設定
10	-77%			WPA/WPA2 Personal	設定
11	-73%		CerioGuest-2.4G	None	設定
11	-74%		CerioGuard-2.4G	WPA/WPA2 Personal	設定

- **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，並設定相對應加密的連線密碼。

基地台橋接連線設定

SSID名稱

CerioGuard-2.4G

加密類型

WPA/WPA2 Personal

WPS Push Button

Push Button

密碼設定

加密模式

自動 (WPA或WPA2)

加密演算法

自動

金鑰

- **基地台橋接連線設定**：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。
- **WEP Setting**：此功能配置移動式站台應用作為 Client Bridge 移動性橋接沿線連接眾多橋接基地台(站台)時進階 Roaming 漫遊細節功能指定的設定，若為非移動式固定 Client Bridge 連接橋接基地台(站台)時，此功能不須啟用。

WEP Settings

加密方式

☐ 關閉
 ☒ 啟用

Key Settings

Key Type

☐ HEX
 ☒ ASCII

金鑰長度

☒ 64位元
 ☐ 128位元

Key Index

1

Network Key

- **WEP Type**：選擇輸入 16 位元 (HEX) 或 ASCII 的金鑰數值，共各別有四組可選設。
- **WEP Length**：可選擇 64bits、128bits 二種加密長度，選取您欲使用的無線加密金鑰長度，目前您可以選擇使用 64bits、128bits 二種加密金鑰長度，但您必須要先確定您的無線用戶端使用的無線網路卡也支援相對應的無線金鑰長度。
- **Key Index**：可為您的 WEP 預先設定 4 組 WEP Key(金鑰數值)。未來無線用戶端若要進行連線，可選擇要使用哪一組無線金鑰作加密連線建立。
- **Network Key**：自訂自己需要設定的加密金鑰。



Notice

請注意：若您選擇使用 WEP 加密模式，請依照以下需求輸入相對應的 WEP 金鑰數值。

64bits：

10 組 Hex 十六進位字元 (0~9、A~F 與 a~f 都可以使用)

5 組 ASCII 字元 (0~9、A~Z 與 a~z 都可以使用)

128bits：

26 組 Hex 十六進位字元 (0~9、A~F 與 a~f 都可以使用)

13 組 ASCII 字元 (0~9、A~Z 與 a~z 都可以使用)

152bits:

32 組 Hex 十六進位字元 (0~9、A~F 與 a~f 都可以使用)

16 組 ASCII 字元 (0~9、A~Z 與 a~z 都可以使用)

● Roaming Setting：

此功能配置移動式站台應用作為 Client Bridge 移動性橋接沿線連接眾多橋接基地台(站台)時進階 Roaming 漫遊細節功能指定的設定，若為非移動式固定 Client Bridge 連接橋接基地台(站台)時，此功能不須啟用。

Roaming Settings

Roaming

☐ 關閉 ☒ 啟用

Min RSSI

Stable Time

秒

Scan Interval

秒

Check Time

秒

Scan Queue

Use Profiles

☒ 關閉 ☐ 啟用

- **Roaming**：選擇啟用或關閉。
- **Min RSSI**：設定移動時偵測最低連線的接收信號強度指示器 RSSI 門檻，預設值 Min RSSI 40，低於此設定的 RSSI 數值的橋接基地台(站台)時將不予連線。
- **Stable Time**：穩定連線等待時間設定，預設值為 60 秒，不同設備晶片無線連接反應溝通時間差異，這裡可以適度更改適合您配置環境的等待秒數。當超過等待時間之內與橋接基地台(站台)尚未自動連線成功，將改與其他設定可連線的橋接基地台(站台)連線。
- **Scan Interval**：當對橋接基地台(站台)接入點的信號惡化時，工作 Client Bridge AP 會掃描備用接入點，如果此掃描不成功（即未找到信號更好的接入點），則此處輸入的秒數將作為下一次掃描嘗試的間隔。此部分設定的設定可以依工作 Client Bridge AP 於環境實際移動速度進站與沿線橋接基地台(站台)間格距離進行優化調整設定。
- **Check Time**：對橋接基地台(站台)訊號的檢查時間，預設值 30 秒。
- **Scan Queue**：工作 Client Bridge AP 對橋接基地台(站台)掃描結果儲列，預設值為 10 次。
- **Use Profiles**：選擇啟用使用預先建立設定要連接的目標基地台設定檔 Profile。

5-4-6. Station Profile Setup

可以為您的工作 Client Bridge AP 連接設定建立設定多筆設定檔，並可選擇是否單筆或多筆同時啟用，當移動時，會自動對接收信號強度指示器 RSSI 品質足夠的橋接基地台(站台)無線連線，且系統會自動對於列表內有啟用的橋接基地台(站台)進行自動連線。

Station Profile List						建立新的設定檔
#	啟用	註解	SSID名稱	加密類型	執行	
-	-	-	-	-	-	

- **建立新的設定檔：**選擇新增建立新的橋接基地台設定。

基地台橋接連線設定

啟用 ☐ 關閉 ☒ 啟用

Roaming Match ☒ Whole ☐ Start with

SSID名稱

加密類型

註解

WEP Settings

加密方式 ☒ 關閉 ☐ 啟用

● 基地台橋接連線設定

- **啟用：**選擇此筆“設定檔”啟用或關閉。
- **Roaming Match：**針對所有的橋接基地台(站台)漫遊 SSID 接受格式的設置要求。
 - **Whole：**只接受無線自動連接完全一致相同的橋接基地台(站台)SSID 名稱。
 - **Start with:**可以接受無線自動連接橋接基地台(站台)SSID 不同但前綴相同的 SSID 名稱格式，例如沿線所有橋接基地台(站台)SSID 名稱可以分別為 station_01、station_02、station_03 等各自不同站台區隔 SSID 格式名稱。
- **SSID 名稱：**設定要橋接連接的無線基地台(站台)名稱。
- **加密類型：**選擇要對橋接基地台(站台)連線相對應的加密資訊。
- **註解：**可以為您的每一個設定檔進行各別備註標示。

5-4-7. Repeater AP 設定

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 Repeater AP 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。

☰ 加密模式

無線基地台	☒ 啟用	☐ 關閉
SSID名稱	default	
可視SSID	☒ 啟用	☐ 關閉
隔離無線使用者	☒ 啟用	☐ 關閉
連線限制	☐ 啟用	☒ 關閉
使用者連線數	128	
加密類型	Open System	

- **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**：針對一個 SSID 最大可連線的無線使用者數量，最大設定支援同時 128 個使用者存取同一個 SSID。
- **認證**：管理者可設定 WEP、WPA-PSK/WPA2-PSK Personal 和 WPA/WAP2-Enterprise、WPA3 及 802.1x 等 5 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。

5-4-8. MAC 過濾

點選「MAC 過濾設定」將可以進入「ACL 存取控制」設定頁面。使用者可設定 ACL 加以控制用戶端連結，點選無線設定，點選虛擬 AP 設定，點選所要設定 ESSID 的 ACL 設定進入頁面，設定方式如下列：

MAC 過濾規則

規則

➤ **規則：**使用者可從下拉清單選取設定，可設定關閉、只阻擋 MAC 清單或只允許 MAC 清單等，使用方式如下：

- **關閉：**關閉存取控制設定功能，所有無線使用者皆可以連線至無線基地台。
- **只阻擋 MAC 清單：**啟用此功能，若無線用戶端 MAC 位址設定於列表中則該無線用戶端則此 MAC 的清單之無線設備是不允許連線至此無線基地台。
- **只允許 MAC 清單：**啟用此功能，若無線用戶端 MAC 位址設定於列表中則該無線用戶端則此只有以下的 MAC 清單之無線設備允許連線至此無線基地台。

➤ **新增 MAC 位址：**輸入要管理的使用者設備中 MAC 位址。

新增MAC位址

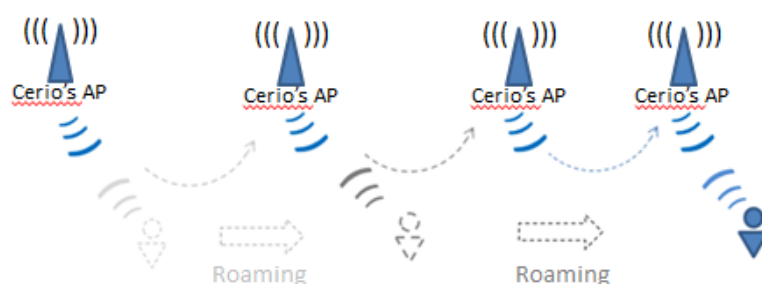
MAC位址

➤ **MAC 位址列表：**被管理設備的 MAC 位址將列出至表單內。

MAC位址列表					
#	MAC位址	執行	#	MAC位址	執行
1	aa:bc:dd:ef:11:23	刪除	2	aa:bc:dd:ed:11:24	刪除

設定完成記得儲存&系統重新啟動才可正常運行。

5-4-9. 802.11r Fast Roaming



IEEE 802.11r 的技術，作用是將整個區域網路佈建的無線基地台所涵蓋之訊號範圍，讓無線使用端遊走無線基地台之間，迅速轉跳較佳的無線基地台連接，轉跳過程不中斷。



當建置 802.11r 無線漫遊平台時，無線使用者設備須有支援 802.11k 功能，才能正常的運作。

802.11r/802.11k 快速漫遊

快速漫遊

☒ 啟用

☐ 關閉

- **快速漫遊：**啟動或關閉漫遊功能。

快速漫遊設定

Mobility Domain

a1b2

R0 Key Lifetime

10000

Reassoc期限

1000

R0/NAS Identifier

ap.example.com

R1 Identifier

000102030405

R1 Push

☐ 啟用

☒ 關閉

- **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。

➤



MobilityDomain 設定必須為 2 組 16 進位碼。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 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：**自動連接 R1 Key Holders



R0 Key holders

MAC位址

目的端 MAC 位址

NAS Identifier

(1-48 octets)

128-bit Key

128-bit key as hex string

新增

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 Identifier**：輸入 AP 的 NAS Identifier 網域名稱。
- **128-bit Key**：輸入一組共用的 128-bit Key 碼。

R0 Key Holder List				
#	MAC位址	NAS Identifier	128-bit Key	執行
1	8c:4d:ea:00:11:22	cerio.com.tw	8c4dea00112233445566...	刪除

輸入確認後將列入以下 R0 Key 表單內，如上圖輸入

R1 Key holders：輸入統一認證的無線基地台的 R1 資訊。

R1 Key Holders

MAC位址

目的端 MAC 位址

R1 Identifier

R1 Identifier

128-bit Key

128-bit key as hex string

新增

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

R1 Key Holder List				
#	MAC位址	NAS Identifier	128-bit Key	執行
1	00:11:22:33:44:50	00:01:02:03:04:05	11223344556677889900...	刪除

輸入確認後將列入以下 R1 Key 表單內，如上圖輸入

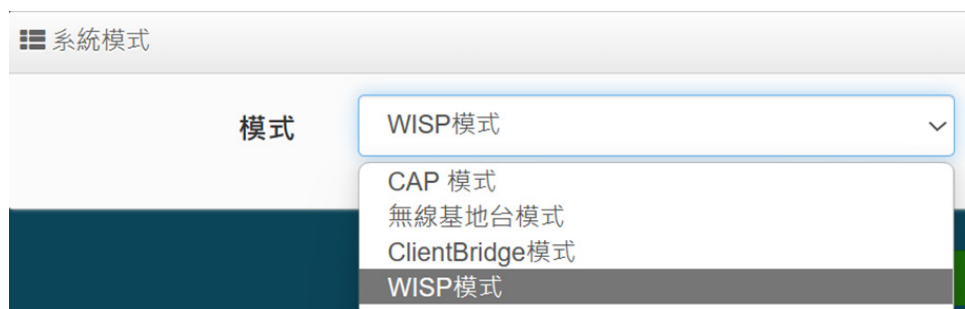
6. WISP 模式

6-1. 模式設定

當您啟動了 WISP 模式後，則系統將改變為 NAT Router 功能，但 WAN 連接方式則是透過無線方式做連接，同時系統將自動啟動 NAT 與 DHCP 功能以提供下層有線或無線使用者使用，您可以透過本章節說明進行細部設定啟動 WISP 功能。



若 WISP 是利用 2.4G 頻段連線上端設備時，則 Repeater AP 功能只能使用 5G 的頻段，相對的假若 WISP 是利用 5G 頻段連接上端設備時，則 Repeater AP 只能使用 2.4G 的頻段。



6-2. 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

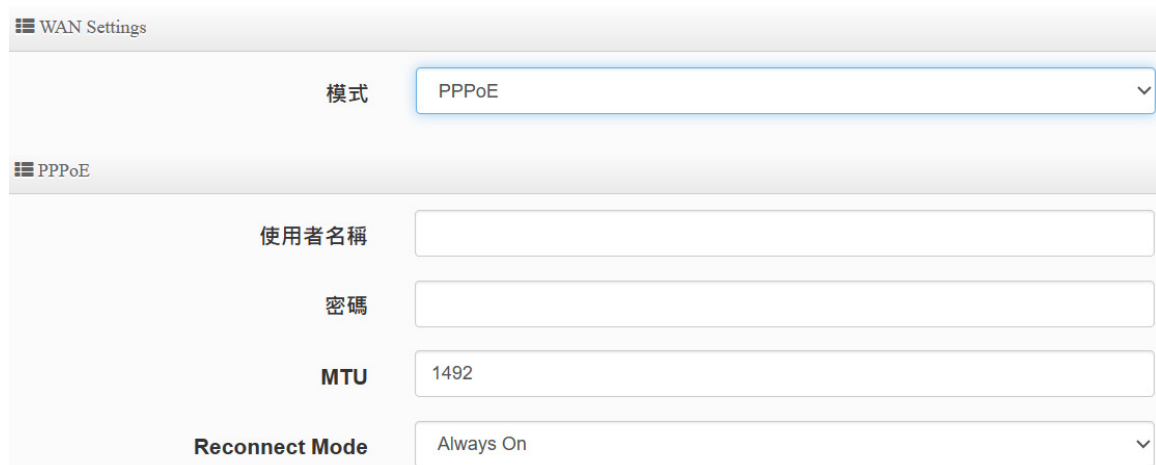
- **IP 位址**：請輸入由您的 ISP 所提供的實體 IP 位址給 WAN 端介面使用。
- **子網路遮罩**：請輸入由您的 ISP 所提供的子網路遮罩給 WAN 端介面使用。
- **預設閘道**：請輸入由您的 ISP 所提供的預設閘道位址給 WAN 端介面使用。



The screenshot shows the 'WAN Settings' interface. Under the 'Dynamic IP' section, the 'Mode' is set to 'Dynamic IP'. The 'Host Name' field is empty.

- **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。



The screenshot shows the 'WAN Settings' interface. Under the 'PPPoE' section, the 'Mode' is set to 'PPPoE'. The 'Username' and 'Password' fields are empty. The 'MTU' is set to 1492. The 'Reconnect Mode' is set to 'Always On'.

- **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

使用者名稱

密碼

PPTP Server IP

WAN IP

子網路遮罩

MTU

MPPE40

☐ 啟用
☒ 關閉

MPPE128

☐ 啟用
☒ 關閉

Reconnect Mode

➤ **PPTP**：點對點通道協議設定，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

模式

Default MAC Address

Manual MAC位址

➤ **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

主要DNS伺服器

次要DNS伺服器

➤ **DNS**：設定網址解析的伺服器位址。

6-3. 區域網路設定

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**" ➔ "**區域網路設定**" 進入頁面設定

IP Settings

IP位址

子網路遮罩

802.1d Spanning Tree

802.1d Spanning Tree

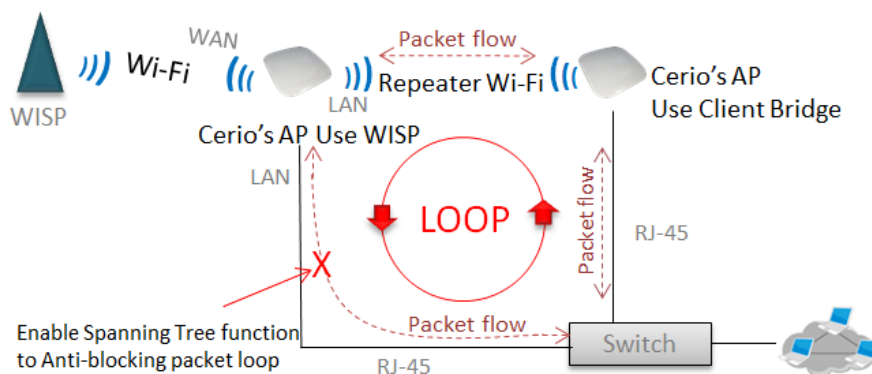
☐ 啟用
 ☒ 關閉

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



6-4. DHCP 設定

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 " 進入頁面設置

DHCP服務

模式
☒ 啟用
☐ 關閉

DHCP設定

起始IP位址	192.168.2.10
結束IP位址	192.168.2.100
子網路遮罩	255.255.255.0
預設匣道	192.168.2.254
主要DNS伺服器位址	192.168.2.254
次要DNS伺服器位址	
WINS伺服器位址	
網域名稱	
IP租用時間	86400

DHCP 設定/用戶列表

- **起始/結束 IP 位址**：設定 DHCP 伺服器要派送 IP 的起始/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)。當 DHCP 伺服器派發出去的 IP 位址，將記錄在列表上。

固定 IP 設定/列表

- **Static Lease IP Setup**：若有特定設備需要取得 DHCP 伺服器所固定派發的 IP 位址，可在此上面設定設備的 MAC 位址以及固定要取得的派送 IP 位址即可。

Static Lease IP Setup

註解

IP位址

MAC位址

新增

- **Static Lease IP List**：當設定完成 Static Lease IP Setup 後，資訊將列入此名單內。

Static Lease IP List				
#	註解	IP位址	MAC位址	執行
-	-	-	-	-

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. 無線設定

#無線基地台橋接及訊號延伸(Repeater AP)設定步驟，可協助管理人員建立與上端 AP 橋接及延伸無線基地台應用。

步驟 1：管理人員請先確認是要使用 2.4G 或 5G 頻段使用 Client 方式去連接上端無線基地台，假若上端 AP 是使用 2.4G 的頻段，則管理員需以 2.4G 頻段去搜尋站台。

以下使用 5G 為範例，至無線設定→ Radio 1 去啟用基地台模式，啟用後將會以 5G 頻段搜尋基地台。

一般設定

MAC位址

8c:4d:ea:05:1c:81

區域設定

Taiwan

無線運作模式

802.11ax

自動頻道

☐ 啟用
 ☒ 關閉

頻道

36 (5180 Mhz)

無線傳輸功率設定

等級 9

Slot Time

9

距離

ACK Timeout

64

步驟 2：進入至“無線設定”→“基地台橋接設定”後點擊“搜尋站台”按鈕開始搜尋附近的所有站台。

無線站台列表					搜尋站台
頻道	Signal	BSSID	ESSID	加密模式	設定
11	-74%		CerioGuard	WPA/WPA2 Personal	設定
9	-62%		Cerio_AP	None	設定
10	-77%		Guard	WPA/WPA2 Personal	設定
11	-73%		CerioGuest	None	設定

步驟 3: 搜尋完成後，附近所有的無線基地台將會列出至表單內，請確實找出預想連線的 BSSID 名稱，並點擊“設定”按鈕來設定此 BSSID 的帳號與密碼。

基地台橋接連線設定

SSID名稱

加密類型

WPA/WPA2 Personal

WPS Push Button

Push Button

密碼設定

加密模式

自動 (WPA或WPA2)

加密演算法

自動

金鑰



請注意站台的訊號值，假若所連接無線基地台的訊號值低於 40%表示此設備與上端無線基地台的連線訊號品質很差，建議請改善連線的訊號品質

當確認基地台橋接已設定完成後，請重新啟動系統並在“系統狀態”下檢查 **Radio 0 或 1** 橋接上端站台的資訊，若資訊有出現 BSSID 及速率等表示成功與 AP 連接。



如果步驟 2 完成後，在系統狀態下無出現 BSSID 及速率，有可能與上端的 IP 位址是不同網段，或是無法與上端 AP 正常連線。需確認上端 AP 或本機設定

步驟 4: 假若要設定延伸基地台，則可以開啟 Repeater AP 功能，管理人員可以點擊 “無線設定” → “Repeater AP 設定” 啟用功能並設定無線基地台資訊。預設值為開啟

加密模式

無線基地台

☒ 啟用
 ☐ 關閉

SSID名稱

default

可視SSID

☒ 啟用
 ☐ 關閉

隔離無線使用者

☒ 啟用
 ☐ 關閉

連線限制

☐ 啟用
 ☒ 關閉

使用者連線數

128

加密類型

Open System



當與上端 AP 做橋接時，切記 IP 位址不能衝突，以免造成網路不正常無法運作。

設定完成後，請點擊儲存並重新啟動完成其功能運作。

6-5-1. Radio 0 (2.4G)

一般設定

MAC位址

8c:4d:ea:05:1c:82

區域設定

Taiwan

無線運作模式

802.11ax

自動頻道

☐ 啟用
 ☒ 關閉

頻道

5 (2432 Mhz)

無線傳輸功率設定

等級 9

Slot Time

9

距離

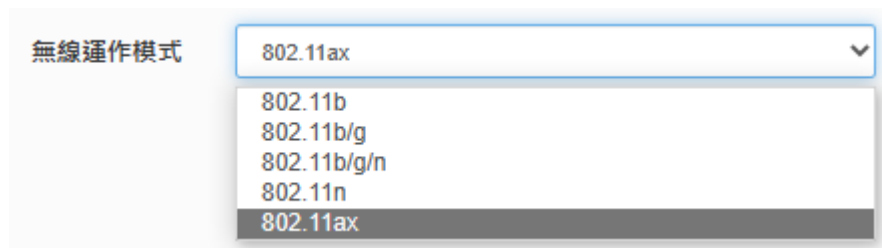
ACK Timeout

64



● 一般設定

- **MAC 位址：**顯示 2.4G (Radio 0)無線 MAC 位址。
- **區域設定：**可設定符合該設備安裝國家之區域，支援「US」、「EU」、「Japan」、「Taiwan」。
- **無線運作模式：**支援「802.11b」、「802.11b/g」、「802.11b/g/n」、「802.11n」、「802.11ax」五種模式，使用者可依需求使用做選擇。



- **自動頻道：**啟用時自動搜尋良好頻道進行連線，關閉時可依環境需求手動調整。
- **頻道：**依法規於不同地區之無線運作模式下有不同選擇，可配合向上/向下延伸。
- **無線傳輸功率設定：**可依所在環境需求，設置 RF 等級 1~等級 9 之功率。
- **Slot Time:** 您可在此輸入 slot time 數值，當距離遠近，等待封包傳送時間將可調整快與慢。
- **距離：**當點下“**距離**”按鈕，將可以輸入點對點的橋接距離，系統會自動計算出該 Slot Time 與 ACK Timeout 的理想參考建議值，輸入距離以單位(公尺)計算。



- **ACK timeout：**當等待“ACKnowledgment frame”間隔太長而不被接收，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。



設定 ACK Timeout 能加強長距離連線，更改數值能有最佳化設定，數值太低會使傳輸降低，數值太高可能有斷線的可能，建議保持預設值使用。

● HP Physical Mode

HT Physical Mode

TX/RX Stream

2T2R

頻道模式

20/40

延伸頻道

☐ 向上
 ☒ 向下

Min MCS

4

Max MCS

11

Short GI

☒ 啟用
 ☐ 關閉

封包聚合

☒ 啟用
 ☐ 關閉

Aggregation Frames

32

封包聚合大小

50000

- **TX/RX Stream**：出廠傳送/接收預設值為 2T2R，可依特殊應用選擇調整 1T1R。



本產品 2.4Ghz 天線已是為內建 2x2 (2T2R)，若無特殊應需求時請保持此 2T2R 預設值的設定值。

- **頻道模式**：2.4G 可選擇 20 或 20/40Mhz 做為基地台與無線用戶間傳輸資料速度。
- **延伸頻道**：此功能僅於頻道模式選擇「20/40 Mhz」時，才可做上/下延伸選擇。
- **MIN MCS**：MCS 編譯是 802.11ax 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。
- **MAX MCS**：最大 MCS 編譯設定值，須注意 Max MCS 值須大於 Min MCS 值。
- **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**：將多個封包整合為一在傳送，主要為控制封包傳輸時過量，出廠預設值為啟用狀態，建議勿關閉。
- **Aggregation Frames**：封包聚集訊框大小。
- **封包聚合大小**：封包聚集的大小。



6-5-2. Radio 1 (5G)

☰ 一般設定

MAC位址	8c:4d:ea:05:1c:81
區域設定	Taiwan
無線運作模式	802.11ax
自動頻道	☐ 啟用 ☒ 關閉
頻道	36 (5180 Mhz)
無線傳輸功率設定	等級 9
Slot Time	9 距離
ACK Timeout	64

● 一般設定

- **MAC 位址**：顯示 5G (Radio 1)無線 MAC 位址。
- **區域設定**：可設定符合該設備安裝國家之區域，支援「US」、「EU」、「Japan」、「Taiwan」。
- **無線運作模式**：支援 802.11a、802.11a/n、802.11n、802.11ac、802.11ax 五種模式，使用者可依需求使用做選擇。

無線運作模式

802.11ax
802.11a
802.11a/n
802.11n
802.11ac
802.11ax

- **自動頻道**：啟用時自動搜尋良好頻道進行連線，關閉時可依環境需求手動調整。
- **頻道**：依法規於不同地區之無線運作模式下有不同選擇。

****根據 NCC 釋出資料規範，台灣開放以下三種 5G 頻段供使用****

- 5250 ~ 5350MHz (CH52 5260MHz、CH56 5280MHz、CH60 5300MHz、CH64 5320MHz)
- 5470 ~ 5725MHz (CH100 5500MHz、CH104 5520MHz、CH108 5540MHz、CH112 5560MHz、CH116 5580MHz、CH120 5600MHz、CH124 5620MHz、CH128 5640MHz、CH132 5660MHz、CH136 5680MHz、CH140 5700MHz)
- 5725 ~ 5825MHz (CH149 5745MHz、CH153 5765MHz、CH157 5785MHz、CH161 5805MHz、CH165 5825MHz)



請注意：5470 ~ 5725MHz 頻段與軍方/氣象用的都普勒雷達頻率相衝突，在軍方優先民間次之的邏輯下，本主機符合設計若要使用這些頻率，設計搭載配合了 DFS(雷達掃描區) 和 TPC (EIRP 值大於 500mW 之設備) 功能，本主機當感測到目前頻率有其它人在使用時，會依照規範軟體自行跳開改採其它頻率；而 5250 ~ 5350MHz 只能在室內使用。
(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**：可依所在環境需求，設置 RF 等級 1~等級 9 之功率。
- **Slot Time**：您可在此輸入 slot time 數值，當距離遠近，等待封包傳送時間將可調整快與慢。
- **距離**：當點下“**距離**”按鈕，將可以輸入點對點的橋接距離，系統會自動計算出該 Slot Time 與 ACK Timeout 的理想參考建議值，輸入距離以單位(公尺)計算。

- **ACK timeout**：當等待“ACKnowledgment frame”間隔太長而不被接收，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。

● HP Physical Mode

- **TX/RX Stream**：出廠傳送/接收預設值為 2T2R，可依特殊應用選擇調整 1T1R。


Notice

本產品 5Ghz 天線已是為內建 2x2 (2T2R)，若無特殊應需求時請保持此 2T2R 預設值的設定值。

- **頻道模式**：5G 可選擇 20 或 20/40 Mhz 或 11ac/ax 80Mhz 做為基地台與無線用戶間傳輸資料速度。
- **MIN MCS**：MCS 編譯是 802.11ax 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。
- **MAX MCS**：最大 MCS 編譯設定值，須注意 Max MCS 值須大於 Min MCS 值。
- **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**：將多個封包整合為一在傳送，主要為控制封包傳輸時過量，出廠預設值為啟用狀態，建議勿關閉。
- **Aggregation Frames**：封包聚集訊框大小。
- **封包聚合大小**：封包聚集的大小。

6-5-3. 進階設定

進階設定

Beacon Interval	100
DTIM 間隔	1
Fragment Threshold	2346
RTS Threshold	2346
Short Preamble	☒ 啟用 ☐ 關閉
IGMP Snooping	☒ 啟用 ☐ 關閉
Greenfield	☒ 啟用 ☐ 關閉
RF on/off by Schedule	Always
Location Tracking Log	☐ 600 秒

- **Beacon Interval**：輸入數值從 10 到 5000 sec，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。建議使用預設值

- **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。建議使用預設值
- **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。建議使用預設值
- **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。建議使用預設值
- **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。建議使用預設值
- **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 Multicast。建議使用預設值
- **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。建議使用預設值
- **5G 優先連線(Band Steering)**：2.4GHz 與 5GHz 的網路同時存在時，自動以 5GHz 的用戶端連線至 5GHz 的網路為主要連接，以提升效能。可於“RSSI Limit”設定值內鍵入 2.4 GHz 連接最低的連接 RSSI 的門檻值，以此作為 5GHz 優先連線的介定值，也就是說以此介定當雙頻(2.4/5GHz)無線用戶與 AP 的 5GHz 訊號優於 2.4GHz 連線 RSSI 所設定的介定值，則本機將促使無線用戶自動以 5GHz 連線為優先。



【Band Steering 功能只限於雙頻無線網卡(至少具有 2.4G 與 5G 同時存的無線網卡配合存取使用)，若 Band Steering 打開，主要連接使用 5Ghz 11ac/11ax，若雙頻無線網卡無支援此功能或是其他不明因素，會導致無線使用者無法正常連線。】

- **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。



【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。】

6-5-4. 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 Parameters 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 Parameters 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, 當此功能沒有被選取時, 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。

6-5-5. 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，則可設定要橋接地無線站台資訊，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。

無線站台列表					搜尋站台
頻道	Signal	BSSID	ESSID	加密模式	設定
-	-	-	-	-	-

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”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。

無線站台列表					搜尋站台
頻道	Signal	BSSID	ESSID	加密模式	設定
1	-80%			WPA/WPA2 Personal	設定
9	-62%		Cerio_AP_2.4G	None	設定
10	-77%			WPA/WPA2 Personal	設定
11	-73%		CerioGuest-2.4G	None	設定
11	-74%		CerioGuard-2.4G	WPA/WPA2 Personal	設定

- **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，並設定相對應加密的連線密碼。

基地台橋接連線設定

SSID名稱

CerioGuard-2.4G

加密類型

WPA/WPA2 Personal

WPS Push Button

Push Button

密碼設定

加密模式

自動 (WPA或WPA2)

加密演算法

自動

金鑰

- **基地台橋接連線設定：**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。
- **WEP Setting:**此功能配置移動式站台應用作為 WISP 移動性橋接沿線連接眾多橋接基地台(站台)時進階 Roaming 漫遊細節功能指定的設定，若為非移動式固定 WISP 連接橋接基地台(站台)時，此功能不須啟用。

WEP Settings

加密方式

☐ 關閉
 ☒ 啟用

Key Settings

Key Type

☐ HEX
 ☒ ASCII

金鑰長度

☒ 64位元
 ☐ 128位元

Key Index

1

Network Key

- **WEP Type**：選擇輸入 16 位元 (HEX) 或 ASCII 的金鑰數值，共各別有四組可選設。
- **WEP Length**：可選擇 64bits、128bits 二種加密長度，選取您欲使用的無線加密金鑰長度，目前您可以選擇使用 64bits、128bits 二種加密金鑰長度，但您必須要先確定您的無線用戶端使用的無線網路卡也支援相對應的無線金鑰長度。
- **Key Index**：可為您的 WEP 預先設定 4 組 WEP Key(金鑰數值)。未來無線用戶端若要進行連線，可選擇要使用哪一組無線金鑰作加密連線建立。
- **Network Key**：自訂自己需要設定的加密金鑰。



Notice

請注意：若您選擇使用 WEP 加密模式，請依照以下需求輸入相對應的 WEP 金鑰數值。

64bits：

10 組 Hex 十六進位字元 (0~9、A~F 與 a~f 都可以使用)

5 組 ASCII 字元 (0~9、A~Z 與 a~z 都可以使用)

128bits：

26 組 Hex 十六進位字元 (0~9、A~F 與 a~f 都可以使用)

13 組 ASCII 字元 (0~9、A~Z 與 a~z 都可以使用)

152bits:

32 組 Hex 十六進位字元 (0~9、A~F 與 a~f 都可以使用)

16 組 ASCII 字元 (0~9、A~Z 與 a~z 都可以使用)

● Roaming Setting：

此功能配置移動式站台應用作為 WISP 移動性橋接沿線連接眾多橋接基地台(站台)時進階 Roaming 漫遊細節功能指定的設定，若為非移動式固定 WISP 連接橋接基地台(站台)時，此功能不須啟用。

Roaming Settings

Roaming

☐ 關閉
 ☒ 啟用

Min RSSI

40

Stable Time

60

秒

Scan Interval

3

秒

Check Time

30

秒

Scan Queue

10

Use Profiles

☒ 關閉
 ☐ 啟用

- **Roaming**：選擇啟用或關閉。
- **Min RSSI**：設定移動時偵測最低連線的接收信號強度指示器 RSSI 門檻，預設值 Min RSSI 40，低於此設定的 RSSI 數值的橋接基地台(站台)時將不予連線。
- **Stable Time**：穩定連線等待時間設定，預設值為 60 秒，不同設備晶片無線連接反應溝通時間差異，這裡可以適度更改適合您配置環境的等待秒數。當超過等待時間之內與橋接基地台(站台)尚未自動連線成功，將改與其他設定可連線的橋接基地台(站台)連線。
- **Scan Interval**：當對橋接基地台(站台)接入點的信號惡化時，工作 WISP AP 會掃描備用接入點，如果此掃描不成功（即未找到信號更好的接入點），則此處輸入的秒數將作為下一次掃描嘗試的間隔。此部分設定的設定可以依工作 WISP AP 於環境實際移動速度進站與沿線橋接基地台(站台)間格距離進行優化調整設定。
- **Check Time**：對橋接基地台(站台)訊號的檢查時間，預設值 30 秒。
- **Scan Queue**：工作 WISP AP 對橋接基地台(站台)掃描結果儲列，預設值為 10 次。
- **Use Profiles**：選擇啟用使用預先建立設定要連接的目標基地台設定檔 Profile。

6-5-6. Station Profile Setup

可以為您的工作 WISP AP 連接設定建立設定多筆設定檔，並可選擇是否單筆或多筆同時啟用，當移動時，會自動對接收信號強度指示器 RSSI 品質足夠的橋接基地台(站台)無線連線，且系統會自動對於列表內有啟用的橋接基地台(站台)進行自動連線。

Station Profile List						建立新的設定檔
#	啟用	註解	SSID名稱	加密類型	執行	
-	-	-	-	-	-	

- **建立新的設定檔：**選擇新增建立新的橋接基地台設定。

基地台橋接連線設定

啟用 ☐ 關閉 ☒ 啟用

Roaming Match ☒ Whole ☐ Start with

SSID名稱

加密類型

註解

WEP Settings

加密方式 ☒ 關閉 ☐ 啟用

● 基地台橋接連線設定

- **啟用：**選擇此筆“設定檔”啟用或關閉。
- **Roaming Match：**針對所有的橋接基地台(站台)漫遊 SSID 接受格式的設置要求。
 - **Whole：**只接受無線自動連接完全一致相同的橋接基地台(站台)SSID 名稱。
 - **Start with:**可以接受無線自動連接橋接基地台(站台)SSID 不同但前綴相同的 SSID 名稱格式，例如沿線所有橋接基地台(站台)SSID 名稱可以分別為 station_01、station_02、station_03 等各自不同站台區隔 SSID 格式名稱。
- **SSID 名稱：**設定要橋接連接的無線基地台(站台)名稱。
- **加密類型：**選擇要對橋接基地台(站台)連線相對應的加密資訊。
- **註解：**可以為您的每一個設定檔進行各別備註標示。

6-5-7. Repeater AP 設定

當基地台橋接成功(WISP)確認已經與上端 AP 連接後，則可以選擇啟用 Repeater AP 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。

加密模式

無線基地台

☒ 啟用
 ☐ 關閉

SSID名稱

default

可視SSID

☒ 啟用
 ☐ 關閉

隔離無線使用者

☒ 啟用
 ☐ 關閉

連線限制

☐ 啟用
 ☒ 關閉

使用者連線數

128

加密類型

Open System

- 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間無法溝通連線。
- 連線限制：針對一個 SSID 最大可連線的無線使用者數量，最大設定支援同時 128 個使用者存取同一個 SSID。
- 認證：管理者可設定 WEP、WPA-PSK/WPA2-PSK Personal 和 WPA/WAP2-Enterprise、WPA3 及 802.1x 等 5 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。

6-5-8. MAC 過濾

點選「MAC 過濾設定」將可以進入「ACL 存取控制」設定頁面。使用者可設定 ACL 加以控制用戶端連結，點選無線設定，點選虛擬 AP 設定，點選所要設定 ESSID 的 ACL 設定進入頁

面，設定方式如下列：

MAC 過濾規則

規則

關閉

儲存

- **規則：**使用者可從下拉清單選取設定，可設定關閉、只阻擋 MAC 清單或只允許 MAC 清單等，使用方式如下：
 - **關閉：**關閉存取控制設定功能，所有無線使用者皆可以連線至無線基地台。
 - **只阻擋 MAC 清單：**啟用此功能，若無線用戶端 MAC 位址設定於列表中則該無線用戶端則此 MAC 的清單之無線設備是不允許連線至此無線基地台。
 - **只允許 MAC 清單：**啟用此功能，若無線用戶端 MAC 位址設定於列表中則該無線用戶端則此只有以下的 MAC 清單之無線設備允許連線至此無線基地台。
- **新增 MAC 位址：**輸入要管理的使用者設備中 MAC 位址。

新增MAC位址

MAC位址

aabcddee1123

×

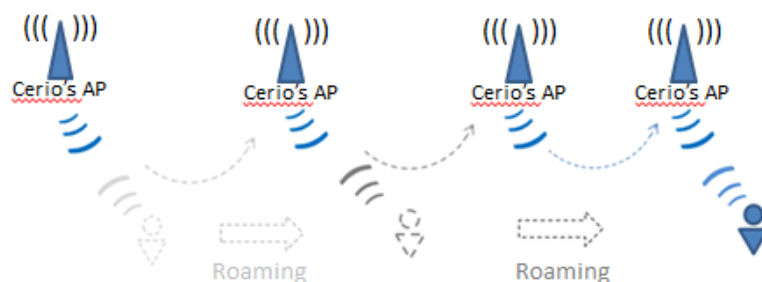
新增

- **MAC 位址列表：**被管理設備的 MAC 位址將列出至表單內。

MAC位址列表					
#	MAC位址	執行	#	MAC位址	執行
1	aa:bc:dd:ef:11:23	刪除	2	aa:bc:dd:ed:11:24	刪除

設定完成記得儲存&系統重新啟動才可正常運行

6-5-9. 802.11r Fast Roaming



IEEE 802.11r 的技術，作用是將整個區域網路佈建的無線基地台所涵蓋之訊號範圍，讓無線使

用端遊走無線基地台之間，迅速轉跳較佳的無線基地台連接，轉跳過程不中斷。



當建置 802.11r 無線漫遊平台時，無線使用者設備須有支援 802.11k 功能，才能正常的運作。

802.11r/802.11k 快速漫遊

快速漫遊

☒ 啟用

☐ 關閉

- **快速漫遊**：啟動或關閉漫遊功能。

快速漫遊設定

Mobility Domain

a1b2

R0 Key Lifetime

10000

Reassoc期限

1000

R0/NAS Identifier

ap.example.com

R1 Identifier

000102030405

R1 Push

☐ 啟用

☒ 關閉

- **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。



MobilityDomain 設定必須為 2 組 16 進位碼。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 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**：自動連接 R1 Key Holders

R0 Key holders

MAC位址

目的端 MAC 位址

NAS Identifier

(1-48 octets)

128-bit Key

128-bit key as hex string

新增

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 Identifier**：輸入 AP 的 NAS Identifier 網域名稱。
- **128-bit Key**：輸入一組共用的 128-bit Key 碼。

R0 Key Holder List				
#	MAC位址	NAS Identifier	128-bit Key	執行
1	8c:4d:ea:00:11:22	cerio.com.tw	8c4dea00112233445566...	刪除

輸入確認後將列入以下 R0 Key 表單內，如上圖輸入

R1 Key Holders

MAC位址

目的端 MAC 位址

R1 Identifier

R1 Identifier

128-bit Key

128-bit key as hex string

新增

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 Identifier**：輸入 AP 的 R1 Identifier 網域名稱。
- **128-bit Key**：輸入一組共用的 128-bit Key 碼。

R1 Key Holder List				
#	MAC位址	NAS Identifier	128-bit Key	執行
1	00:11:22:33:44:50	00:01:02:03:04:05	11223344556677889900...	刪除

輸入確認後將列入以下 R1 Key 表單內，如上圖輸入

6-6. 進階 (WISP 模式下適用)

6-6-1. DMZ

DMZ設定

模式

關閉

關閉

Automatic Assignment

靜態分配

- 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。

 **Notice** 本系統有 Automatic Assignment(自動分配)及 Static Assignment(靜態分配) 二種 DMZ 類型

- **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。

6-6-2. IP 過濾

IP過濾列表

#	啟動	註解	通訊協定	流入/流出	執行	來源位址/Mask	來源埠	目的位址/Mask	目的埠	編輯
1	InActive	-	ALL	In	Deny	-	-	-	-	編輯
2	InActive	-	ALL	In	Deny	-	-	-	-	編輯
3	InActive	-	ALL	In	Deny	-	-	-	-	編輯

IP過濾規則

啟動

☐ 啟用
 ☒ 關閉

註解

- **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。

IP過濾規則

政策

☒ 拒絕
 ☐ Pass

流入/流出

☒ 流入
 ☐ 流出

通訊協定

ALL

- **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。

IP過濾規則

來源位址/Mask

來源埠

(min:1, max:65535 or Range xxxxx:xxxxx)

目的位址/Mask

目的埠

(min:1, max:65535 or Range xxxxx:xxxxx)

Listen

☒ 啟用
 ☐ 關閉

介面

☒ WAN
 ☐ LAN

時間表

Always

- **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。

6-6-3. MAC 過濾設定

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。

MAC過濾規則

模式

關閉

關閉

拒絕

允許

- **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。
- **啟動**：選擇設定的 MAC 條例是否要作用開啟或關閉，管理者可以為設定的 MAC 條例進行說明註解。

MAC過濾列表

#	啟動	註解	MAC位址	政策
1	☐			Always Run
2	☐			Always Run
3	☐			Always Run

- **MAC 位址**：輸入要被 MAC 過濾管理的使用者的 MAC 位址。
- **政策**：可依照時間規則來設定時間點進行運 (要使用此功能請先將時間規則列表進行設定，詳細請參考手冊 3.4"時間規則"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。

6-6-5. 存取控制

存取控制列表				
#	啟動	註解	通訊協定	編輯
1	InActive	-	ANY	編輯
2	InActive	-	ANY	編輯
3	InActive	-	ANY	編輯

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。

存取控制規則

啟動

☐ 啟用
 ☒ 關閉

註解

通訊協定

ANY

時間表

Always

存取控制規則：

- **啟動：**可選擇啟動或關閉功能。
- **註解：**可輸入此規則描述。
- **通訊協定：**可選擇要過濾的通訊協定。
- **時間表：**可選擇時間制定規則【[詳細設定方式，參考手冊章節 3“系統設定” 功能](#)】

通訊協定

ANY

ANY

TCP

UDP

ICMP

內容關鍵字過濾

網域名稱過濾

IP P2P

- **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
- **內容關鍵字過濾:** 可針對「關鍵字」進行規則設定。
 - ✓ **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)。
 - ✓ **Keyword:** 輸入要過濾的內容英文關鍵字。(請注意，本系統不支援繁體字元關鍵字輸入格式)。
- **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。
- **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。

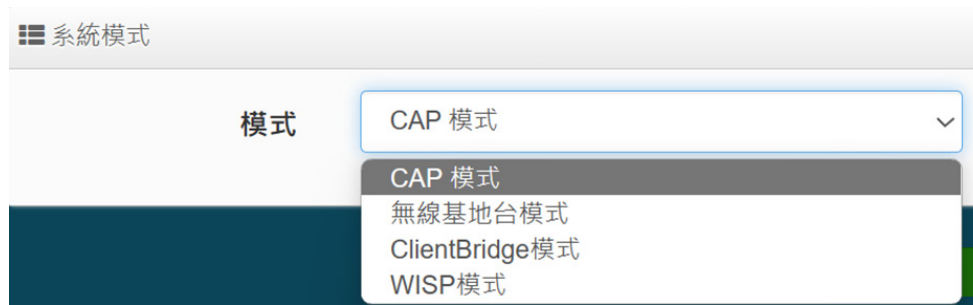
7. CAP 模式



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。如下進入 CAP 切換方式。

7-1. 模式設定

此功能設定本機控制器的 LAN 或 VLAN 的 IP 位址、閘道位址、DNS、VLAN Tag 和 spanning Tree 等等。



- 選擇為 CAP 模式後，儲存並重新啟動系統


Notice

每個模式 LAN IP 位址並不相互繼承沿襲使用，請就每個模式下自己 IP 位址進行存取管理。

7-2. 虛擬網路設定

#	系統狀態	旗標	IP位址	子網路遮罩	執行
0	啟用	Native ETH1 Native ETH2	192.168.2.254	255.255.255.0	網路
1	停用	ETH1.101 ETH2.101	192.168.101.254	255.255.255.0	網路
2	停用	ETH1.102 ETH2.102	192.168.102.254	255.255.255.0	網路
3	停用	ETH1.103 ETH2.103	192.168.103.254	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 ETH1** **Native ETH2** 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。
- **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


Notice

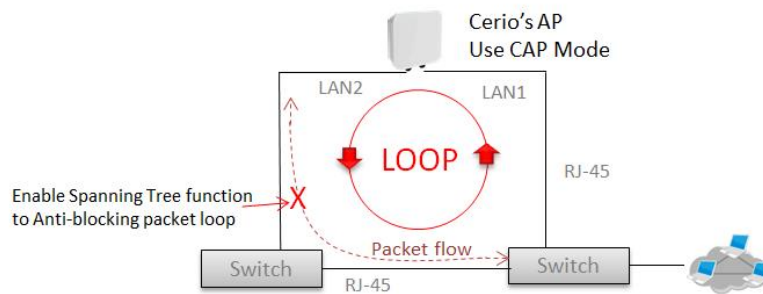
虛擬網路服務(VLAN)功能，系統會自動保留一組 VLAN 作為管理使用。

系統管理

802.1d Spanning Tree

☐ 啟用
 ☒ 關閉

- **802.1d Spanning Tree**：可以避免網路架構迴圈機制，例如：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



ETH1 虛擬網路標記設定

VLAN TAG

☐ 1-4096

ETH2 虛擬網路標記設定

ETH2

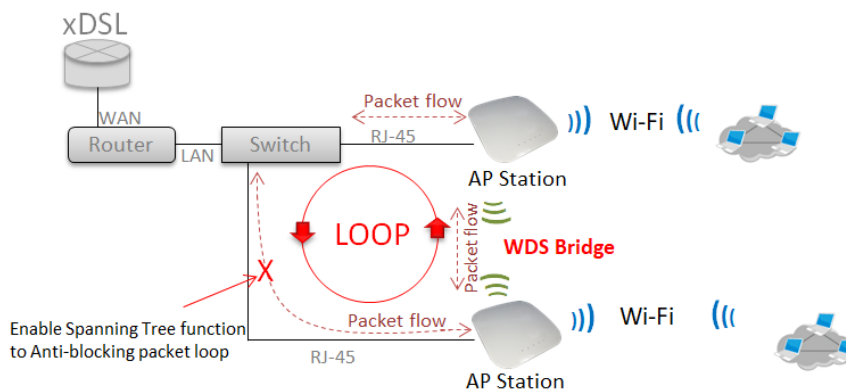
☒ 啟用
 ☐ 關閉

VLAN TAG

☐ 1-4096

- **ETH1 虛擬網路標記設定**：可設定 ETH1 此連接埠的 VLAN tag。
- **ETH2 虛擬網路標記設定**：可設定 ETH2 是否啟用或關閉並設定此連接埠的 VLAN tag。

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。



7-3. AP Control

此 CAP 模式的 AP Control 功能，主要是控制管理所有 CenOS5.0 的無線基地台。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、AAP 認證設定檔及被管理 AP 的系統狀態。

7-3-1. 掃描無線基地台

裝置過濾

VLAN#

VLAN 0 (192.168.101.0/24)

預設密碼

.....

Sort

IP位址

偵測掃描

#掃描操作程序說明：

1. 裝置過濾：

- **VLAN**：主要選擇要掃描的 VLAN 網段，其他非相關的網段則過濾掉。若在“虛擬網路設定”有啟用多組 VLAN 網路，則此選項將會依造“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 CenOS5.0 被管 AP 的系統登入密碼有修改過，此欄位則須輸入被修改過的密碼。(預設值為 default)
- **Sort**：可選擇掃描結果後，採用 IP 位址排序或是 MAC 位址排序列出。

掃描結果						預設值	匯入
#	Device	MAC位址	密碼	IP位址	子網路遮罩	執行	
-	-	-	-	-	-	-	

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或單一的無線基地台。
- **MAC 位址**：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。
- **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：**確認修改以上單一無線基地台設定後，可按下儲存並重新啟動，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，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。

7-3-2. 批次設定

此功能主要是集中控制管理 CenOS5.0 的無線基地台模式無線基地台的無線功能，除可管理同時也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。

虛擬網路列表

VLAN	VLAN 0 (192.168.101.0/24)	▼
群組	None	▼
批次設定	虛擬網路設定	▼

- **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 Radio 0(2.4G) 或 Radio 1(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”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。
- **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。

AP設備列表				選擇全部
選取	VLAN#	IP位址	系統狀態	
-	-	-	-	

7-3-3. 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。

虛擬網路列表

VLAN

All

AP設備列表

選擇全部

刪除

更新

VLAN#	Device	系統狀態	系統名稱	IP位址	MAC位址	連線時間	執行
-	-	-	-	-	-	-	-

- ◆ **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。

7-3-4. 群組設定

群組列表

#

VLAN

名稱

系統描述

執行

-

-

-

-

-

編輯群組

VLAN

VLAN 0 (192.168.101.0/24)

群組名稱

系統描述

建立新群組

可以在同一個 VLAN 下去建置多筆的群組。

- **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。

7-3-5. MAP 設定

可放置平面圖，將所有被管理 AP 的架設位置定位擺放，讓管理者可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。

Map 列表

#

名稱

系統描述

執行

-

-

-

-

編輯Map

Map 名稱

Map0

圖檔的 URL 位址

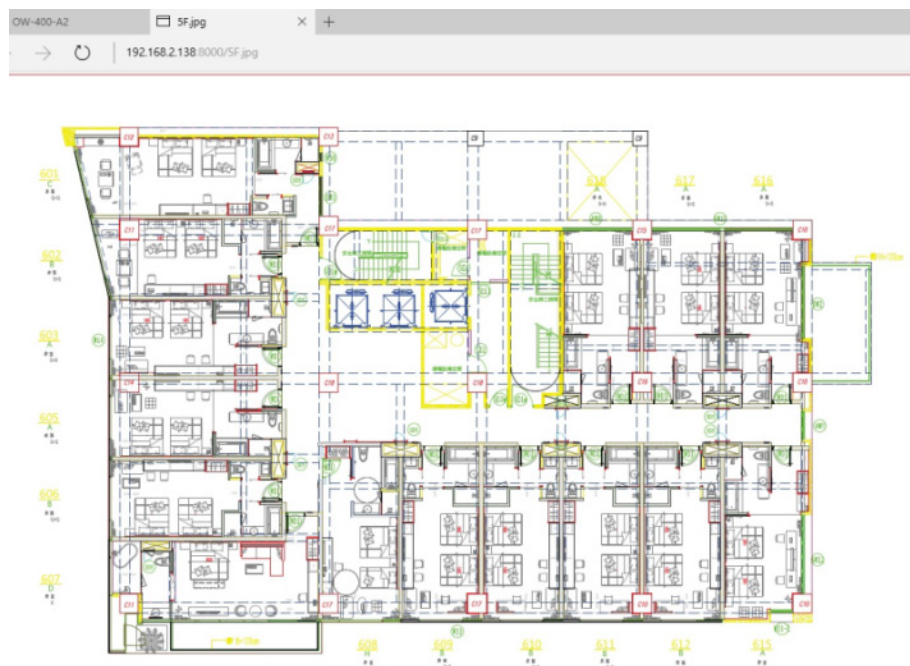
系統描述

圖檔

檢視

建立新地圖

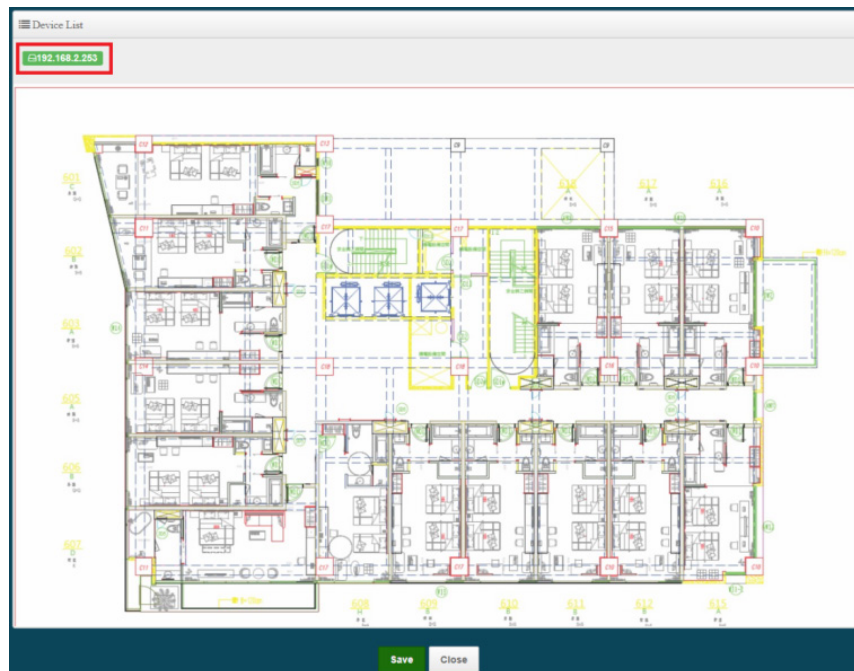
- Map 名稱：輸入此地圖的代號名稱。
- 圖檔的 URL 位址：圖檔需上傳到某 web 伺服器，之後將圖檔的 URL 位置輸入此欄位，該 web 伺服器需另外自行架設或利用現有的 web 伺服器。
- 系統描述：輸入此圖檔的詳細描述。
- 檢視：當確認 URL 路徑後可以點擊此按鈕，檢視圖檔是否正確，假如圖檔路徑正確將會出現所加入的圖檔畫面



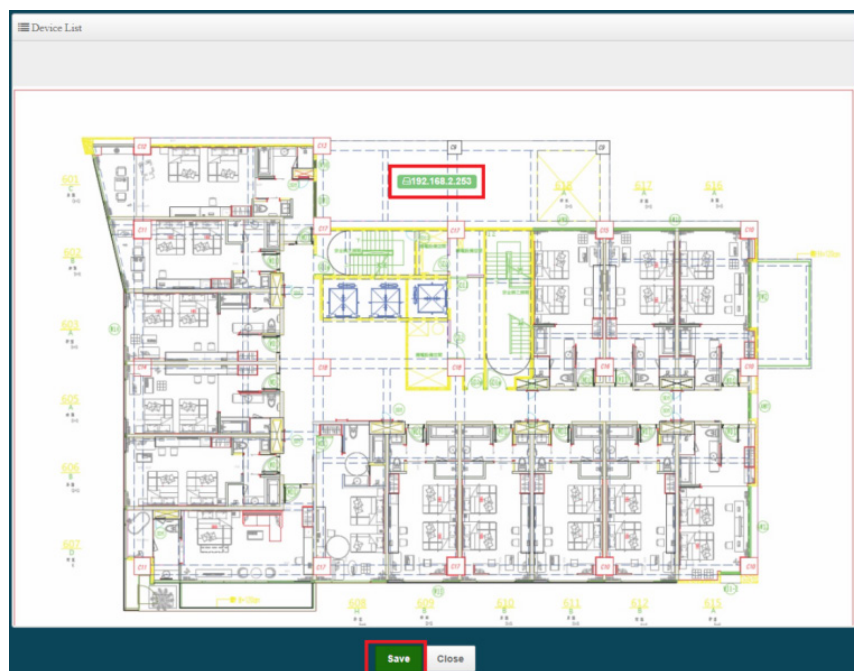
確認後點擊“儲存”按鈕儲存設定並將系統重新啟動讓地圖生效。系統重新啟動後，Map 列表會出現剛剛儲存的地圖資訊。

Map 列表				建立新地圖
#	名稱	系統描述	執行	
1	5F.jpg	測試		檢視

點選檢視框旁的下拉式選單選擇 Layout，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。

Map 列表				建立新地圖
#	名稱	系統描述	執行	
1	5f.jpg	測試	檢視	

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。

Device Status	
IP Address	192.168.2.253
MAC Address	00:22:ab:00:00:00
Hostname	Cerio's AP
Uptime	16:15
Channel	11
Rate	300.0 Mb/s
Client	0

7-3-6. 認證設定檔(Profile)

認證設定檔列表(Profile List)						建立新的設定檔
#	名稱	系統描述	網頁認證功能	編輯	執行	
-	-	-	-	-	-	

系統設定管理

設定檔名稱

系統描述

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“ 批次設定” 內去選擇套用。

認證設定檔列表(Profile List)						a 建立新的設定檔
b #	c 名稱	系統描述	d 網頁認證功能	編輯	執行	
1	TEST1	Authenticate Profile...	停用	e 網頁認證功能	f Setup	刪除

遊客
 建立本機帳戶名單
 OAuth 2.0
 客製化頁面
 語系
 Walled Garden
 特權名單
 設定檔

- 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“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

7-3-7. 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。

AP設備列表								
VLAN#	系統狀態	系統名稱	IP位址	連線時間	Radio Information	接收(位元)	傳送(位元)	User(s)
VLAN0		CW-400NAC-E1	192.168.2.253	33	5(11.0 Mb/s) / 100(0.0 Mb/s)	622B	664B	0

- **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

8-1. 系統設定管理

系統設定管理

您可以將目前的設定存成一個設定備份檔案，當有需要時可利用的設定備份檔恢復至您先前的設定，您也可以在此選擇還原至原廠預設值。

下載系統設定備份檔案

儲存

回存系統設定備份檔案

選擇檔案

沒有選擇檔案

上傳

還原系統預設值

預設值

從電腦上傳SSL憑證檔案

憑證檔案

選擇檔案

沒有選擇檔案

沒有選擇檔案

上傳

- 管理者可備份/還原此系統現行環境之所有設定資料及恢復系統預設值等功能。

8-2. 韌體升級

韌體資訊

我們支援韌體更新,請選擇由您的存放於您的電腦的最新版本韌體執行更新,(升級韌體乃危險過程升級失敗可能導致系統無法正常運作,請在升級韌體時千萬不要關閉電源並以有線的方式將無線基地台與電腦直接連線,升級過程中保持本機與基地台之間網路持續連線以免發生更新失敗的問題.)

韌體版本

Pme-CPE-IPQ60XX-CERIO V0.0.1

韌體釋出日期

2024/01/02 16:10:44

從本機電腦升級韌體

選擇檔案

選擇檔案

沒有選擇檔案

上傳

從TFTP伺服器升級韌體

TFTP伺服器IP位址

檔案名稱

上傳

從HTTP連接位址升級韌體

URL連接網址

上傳

當 CERIO 有釋出新的韌體，管理者若有需要更新系統韌體，可至本公司網站(<http://www.cerio.com.tw>) 瀏覽是否有提供更新韌體並下載進行系統更新，若您有任何更新產品上的問題，歡迎隨時致電本公司洽詢詳細的操作步驟。



Notice

我們強烈的建議您務必遵守以下步驟和規範，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，切勿使用無線連線方式進行。
2. 更新過程中請勿關閉或切斷系統的電源，且務必使用相容的 WEB 瀏覽器進行更新，以免發生更新失敗問題。
3. 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。
4. 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。
5. 倘若您的無線基地台平常時間運作正常，且沒有發生任何相容性問題，我們建議不要輕易更新系統韌體。
6. 更新韌體是個有風險的動作，更新失敗可能導致系統無法正常運作而損毀，若無特殊需求下建議您勿隨意更新。
7. 請務必從本公司網站下載相關韌體檔案，若您使用非本公司釋出且不明來源之檔案，導致系統無法正常運作或喪失某部分功能，本公司將不負此產品任何後續維修服務，請見諒！

8-3. 網路測試工具

PING測試工具

遠端IP位址/URL位址

回應時間

Ping



- **Ping 測試工具：**此工具可協助您以 PING 的指令測試遠端設備與系統的連線狀態，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。

路由跟蹤

目的地的主機

開始

Max. Hops

停止

- **路由跟蹤：**此工具可協助您以 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。
 - **目的地的主機：**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. Hops：**您可以在此輸入所需要顯示 Hop 的數量。

8-4. 重新啟動

重新啟動

有時系統會發生無法正常運作的問題，您可以透過重新啟動將系統恢復至正常狀態，重新啟動系統將不會變更或遺失已完成的系統設定，請按下「重新啟動」鍵並稍候數秒系統將會自動重新開機。

重新啟動

- 網路管理員可用「重新啟動」鍵輕鬆重啟系統，重啟完成時間約需 1~2 分鐘。
- 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

9-1. 系統狀態

☰ 系統狀態

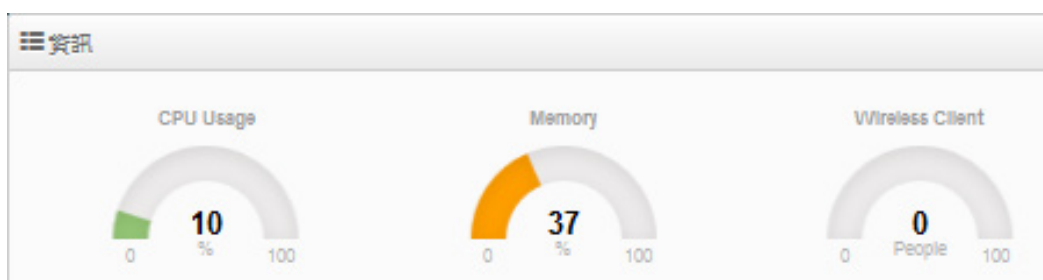
模式	無線基地台模式 ▼
系統名稱	CW-500-R1
系統時間	2021/06/01 08:50:22
系統啟用時間	43:22
韌體版本	Pme-CPE-IPQ60XX-CERIO V0.0.2
韌體釋出日期	2024/05/06 12:45:19
ETH1 MAC位址	8c:4d:ea:05:1c:6b
ETH2 MAC位址	8c:4d:ea:05:1c:6c
WiFi0 MAC位址	8c:4d:ea:05:1c:6e
WiFi1 MAC位址	8c:4d:ea:05:1c:6d
預設匣道	192.168.2.1
DNS1	192.168.2.1
DNS2	
Port Link	ETH2 ETH1

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、網卡位址及網路埠接通圖示相關狀態等資訊。

資訊：

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



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

Radio 0

無線運作模式

802.11ax

頻道

5

速率

573.5 Mb/s

Radio 1

無線運作模式

802.11ax

頻道

36

速率

1201.0 Mb/s

9-2. 無線用戶狀態

LAN						
無線基地台	MAC位址	RSSI	Rate(RX/TX)	Bytes(RX/TX)	Packet(RX/TX)	SEQ(RX/TX)
-	-	-	-	-	-	-

※ 顯示 Radio 連線使用者相關資訊

- 無線基地台：無線使用者連接 Radio 0(2.4G)或 Radio 1(5G)的狀態。
- MAC 位址：無線使用者 MAC 位址。
- RSSI：無線使用者與 AP 間之訊號值。
- Rate(RX/TX)：使用者上/下載連線數。
- Byte(RX/TX)：傳送/接收總位元量。
- Packet(RX/TX)：封包傳送/接收流量。
- SEQ(RX/TX)：傳送/接收序列。

9-3. 線上使用者

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
-	-	-	-	-	-	-	-



1. 此功能在無線基地台模式下運作。
2. 管理員可監控用戶的身分驗證帳號登入/登出時間和帳戶驗證類型。

- VLAN#：顯示用戶所使用之 VLAN 區域。
- 網頁認證功能：顯示用戶認證之功能類型。
- 使用者數量：顯示用戶目前在線認證數量，若啟用一帳戶可多台登入，將顯示複數。
- 下載/上傳封包：顯示用戶上傳/下載封包量。
- 下載/上傳位元：顯示用戶上傳/下載 Mbps 流量。

9-4. 認證日誌

☰ 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**：可點擊進入查看各行列資訊

9-5. 系統紀錄

☰ 系統紀錄 更新 清除			
時間	服務名稱	服務等級	訊息
2021-06-01 08:00:26	System	Info	started: BusyBox v1.24.2
2021-06-01 00:00:26	Wireless	Info	wds1: IEEE 802.11 driver had channel switch: freq=5180, ht=1, vht_ch=0x0, offset=1, width=5 (160 MHz), cf1=5250, cf2=0
2021-06-01 00:00:27	Wireless	Info	ath01: IEEE 802.11 driver had channel switch: freq=5180, ht=1, vht_ch=0x0, offset=1, width=5 (160 MHz), cf1=5250, cf2=0



1. 此頁面將會記錄無線基地台從開機到當下所有系統處理狀態及詳細資訊。
2. 可協助系統管理者針對問題進行除錯。

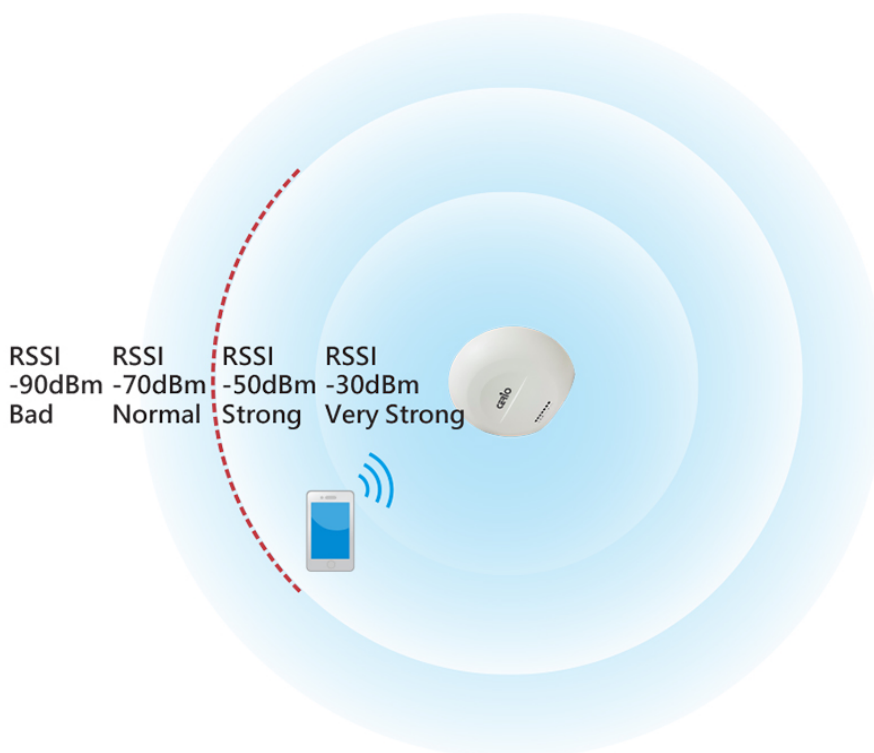
- **日期**：紀錄事件發生的日期和時間。
- **服務名稱**：可幫助識別事件來源，如系統或用戶來源。
- **服務等級**：與特定事件關聯的服務等級，如訊息、錯誤、報告。
- **訊息**：事件描述。
- **更新**：點擊以更新日誌最新狀態。
- **清除**：點擊以清除當下所有紀錄。

10. 相關技術文件參考

10-1. Fast Roaming 802.11r 快速漫遊的引導設定

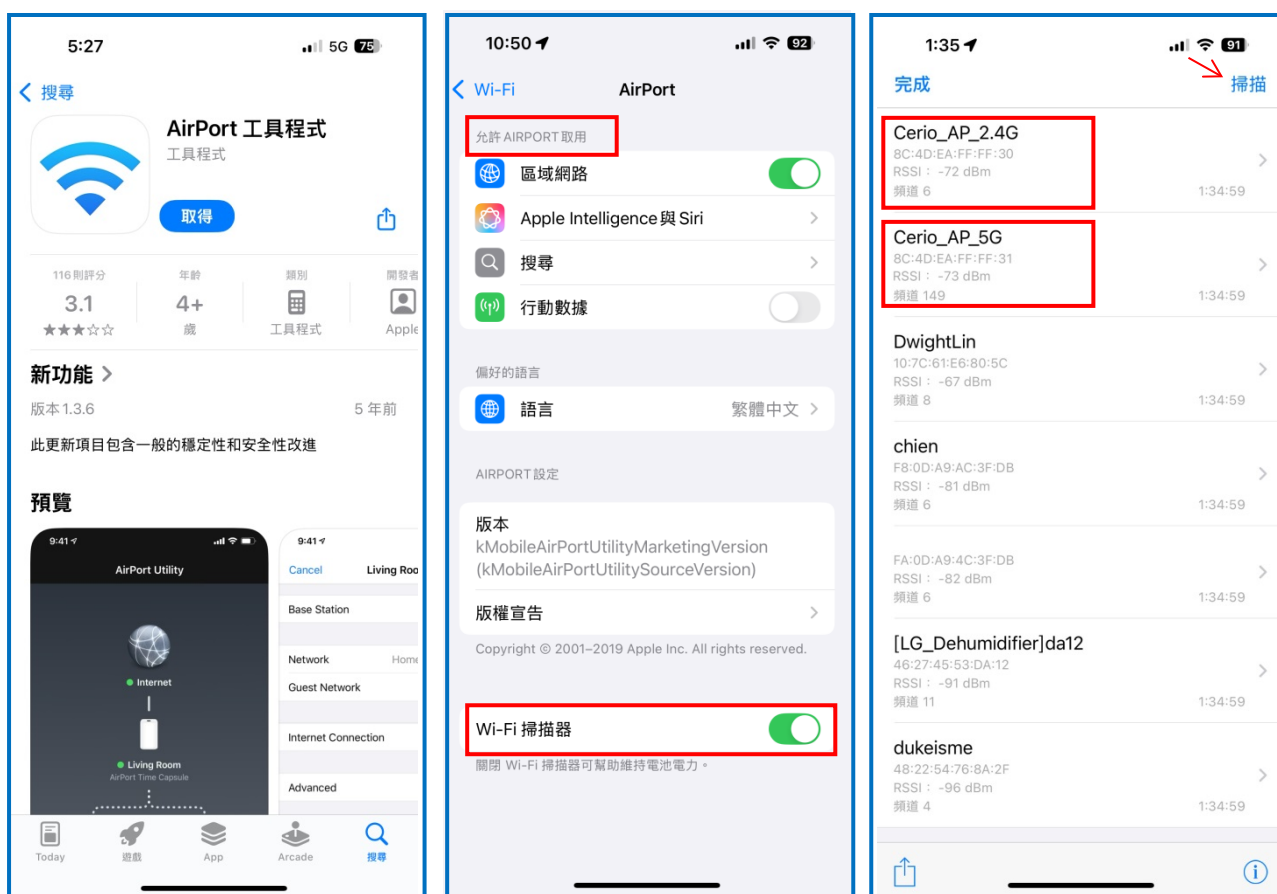
802.11r 的漫遊機制,完全取決於用戶端的設備決定，WiFi 漫遊指的是以在一個 ESS (ESSID=無線網路的名稱)內從一個 BSS (BSSID =WiFi AP 的 MAC 位址)接入到另外一個 BSS(BSSID =WiFi AP 的 MAC 位址)，而快速漫遊允許客戶端網路卡設備(例如對於移動時需要無縫連接的手持式 WiFi 客戶端設備或 WiFi 筆電等)在從一個 Cerio WiFi AP 接入點轉換到另一個 Cerio WiFi AP 接入點時保持連續的無線連接，可不必重新連線就可以繼續保持傳輸，802.11r 快速漫遊的支援解決了 WiFi 客戶端設備不會和舊 AP(原連線之 AP)提早觸發斷連，即不會提早主動向舊 AP(原連線之 AP)發送解連線關聯或解除認證提報，因無任何機制或有漫遊鄰居清單列表可做依據，因此導致可能連到底直至無法傳輸後才予以跳換可用 WiFi AP 接入點現象，其過程就是無接縫漫遊的狀態。

利用每台 AP 的 802.11r/802.11k 快速漫遊啟用,進行設定給 “WiFi 客戶端網路卡設備” 所需的 R0 /R1Key Holders 等相關鄰居 AP 的清單，當 “WiFi 客戶端網路卡設備” 一旦連線透過每台已設定好的 “R0 /R1Key Holders 等相關鄰居清單” 的取得，當 “WiFi 客戶端網路卡設備” 移動至與 Cerio WiFi AP 接入點的訊號(RSSI) 到達 “臨界值” 時即可自己進行無縫轉換連接(AP 視為換手程序)下一台 WiFi AP 接入點。



步驟-1：WiFi AP 設定前先完成 AP 佈點位置規劃：

WiFi 客戶端網路卡設備連接 WiFi AP 接入點的訊號 RSSI 值(接收信號強度指示單位)會依環境障礙格局不同會有不同訊號結果，RSSI 值(接收信號強度指示單位)越接近 0 將會是最好的。且 WiFi 客戶端網路卡設備自身設計驅動啟動漫遊換手的“臨界值”普遍是定義在 RSSI -70 至-80 之間，且不同的 WiFi 客戶端網路卡設備(例如手機 WiFi 功率低)，與不同功率能力的 WiFi AP 接入點都會產生不同的 RSSI 品質可能結果，於 Cerio WiFi AP 設定之前，請確實佈置適合自己環境中每台 Cerio WiFi AP 適當位置相對訊號發射功率(Power Level)，了解自己 WiFi 客戶端網路卡設備與 WiFi AP 的相對距離與可達 RSSI 狀態，可以利用例如 iPhone 手機 Apple Store 下載使用 AirPort 於 APP 設定內開啟“WiFi 掃描器”功能進行先行佈置。



多台 Cerio WiFi AP 接入點的彼此訊號必須互相產生互相重疊的“漫遊末端訊號”，此訊號通常指的就是 WiFi 客戶端網路卡與 Cerio WiFi AP 接入點連接後於 RSSI -70 至-80 之間，當 WiFi 客戶端網路卡的驅動自行機制偵測到自己與 WiFi AP 接入點的 RSSI 已達“臨界值”(RSSI -70 至-80 之間)時，將會依照先前由 WiFi AP 接入點取得的“R0 /R1Key Holders 等其他相關 AP 鄰居清單”進行漫遊更換其他更佳的 WiFi AP 鄰居，於漫遊設定前去適當的為每台 WiFi AP 接入點進行必要的“漫遊末端的重疊訊號”佈置點規劃是相對必要的。

彼此不恰當過近或過遠的 WiFi AP 位置佈置，將可能導致自己設計佈置規劃的“無縫漫遊”效果不佳或甚漫遊不成功，此提醒“無縫漫遊的前提是：

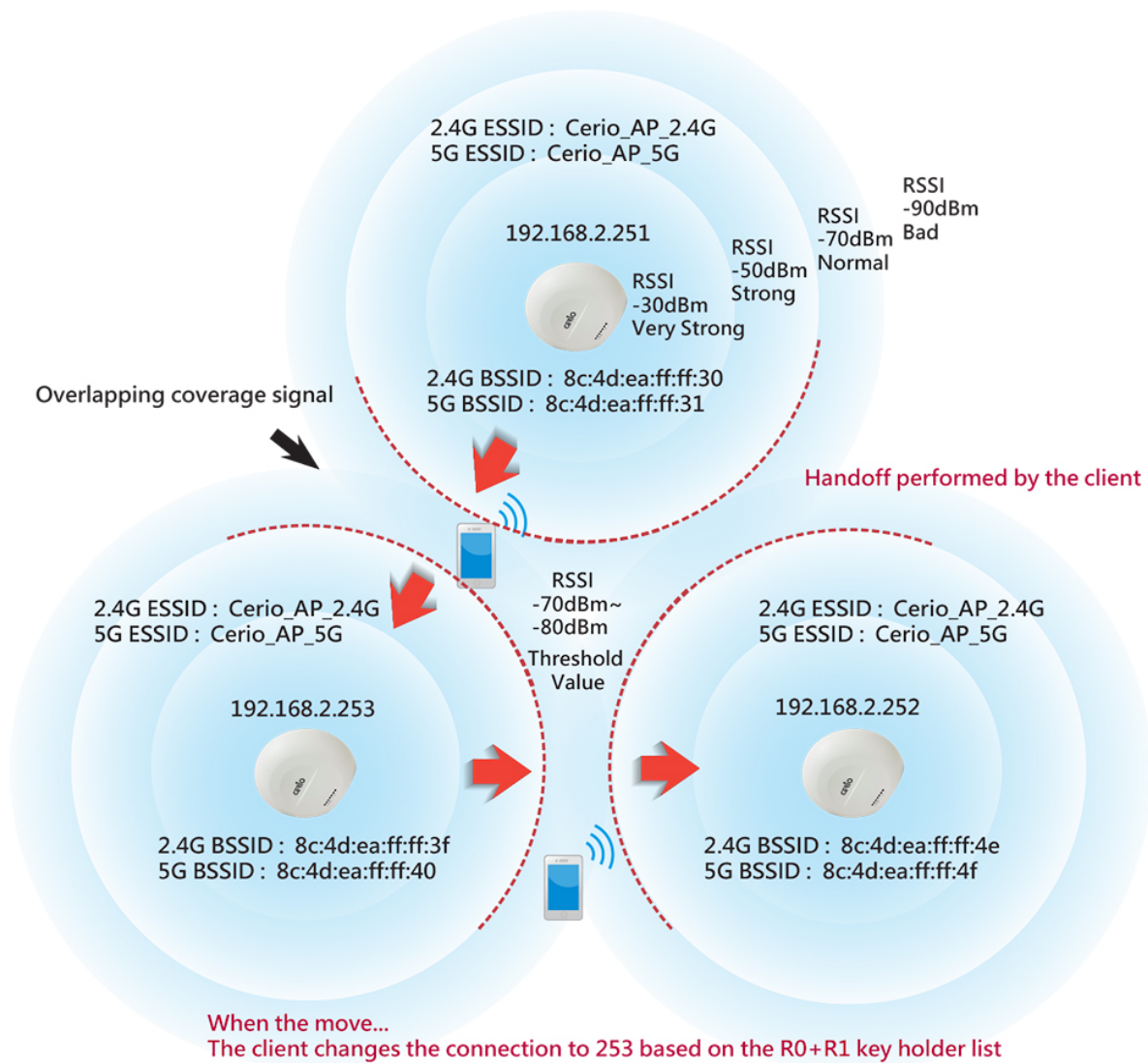
1. 環境每台 Cerio WiFi AP “彼此都已佈置有“漫遊末端的重疊訊號”。
2. 每台 Cerio WiFi AP 使用相同頻道與相同 SSID 名稱(ESSID) 與相同的 WiFi 加密。
3. 為每台 Cerio WiFi AP”設定自己相對的“R0 /R1Key Holders 等其他相關 AP 鄰居清單”。
4. 連接 Cerio WiFi AP 的 WiFi 客戶端網路卡(Client)也必須有支援相同 802.11r/k 漫遊協定。

步驟-2：確認漫遊環境中要設定的每台 WiFi AP 的 BSSID

以下圖例例舉三台 IP 為 251.與 252 與 253 各為鄰居且各自 BSSID(MAC 位址 ID)如下:

	AP unit 1	AP unit 2	AP unit 3
LAN IP	192.168.2.251	192.168.2.252	192.168.2.253
Radio-0(2.4G) BSSID	8c:4d:ea:ff:ff:30	8c:4d:ea:ff:ff:3f	8c:4d:ea:ff:ff:4e
Radio-1(5G) BSSID	8c:4d:ea:ff:ff:31	8c:4d:ea:ff:ff:40	8c:4d:ea:ff:ff:4f

AP distance/power level is based on client connection RSSI threshold.



當然如下圖示可以直接進入系統狀態，即可進行查閱得知 IP 251 的 WIFI0 MAC 位址 (2.4G)的 BSSID(MAC 位址 ID) 為 8c:4d:ea:ff:ff:30,與 WIFI1 MAC 位址 (5G)的 BSSID(MAC 位址 ID) 為 8c:4d:ea:ff:ff:31 (5G) ，以此類推一併去先行得知 IP 252 與的 IP 253 的 BSSID(MAC 位址 ID) 。

***提示：**除上述透過軟體 UI 查閱方法得知之外，您也可以透過 Cerio 產品本體的機下標籤查閱快速得知每個相對 Radio 的 MAC 位址 ID 。

系統狀態

模式

無線基地台模式

系統名稱

CW-500-R1

系統時間

2025/02/04 17:00:13

系統啟用時間

16:25

韌體版本

Pme-CPE-IPQ60XX-CERIO V0.0.2

韌體釋出日期

2025/01/23 19:24:59

ETH1 MAC位址

8c:4d:ea:ff:ff:2e

ETH2 MAC位址

8c:4d:ea:ff:ff:2f

WiFi0 MAC位址

8c:4d:ea:ff:ff:30

WiFi1 MAC位址

8c:4d:ea:ff:ff:31

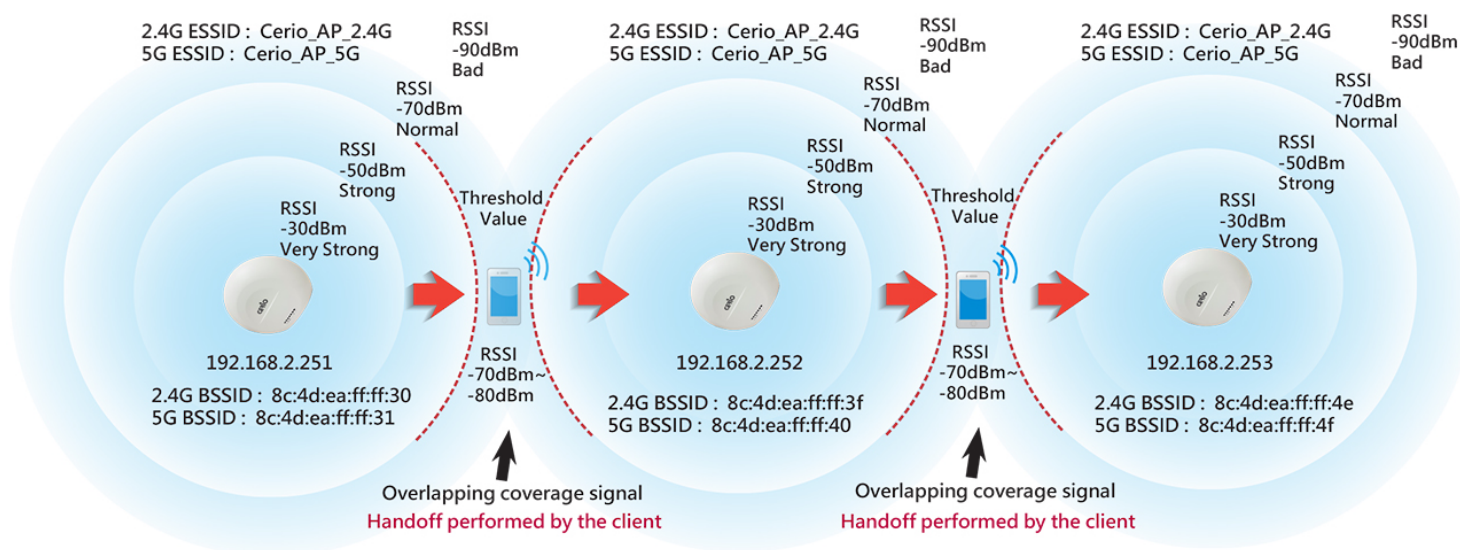
預設匯道

192.168.2.1

步驟-3： 先行瞭解每台所在 AP 的鄰居狀態.

透過自己整體規劃佈點的”漫遊末端的重疊訊號”後，得以清楚的了解每台各自的 WiFi AP 自己的”漫遊末端的重疊訊號”是那些鄰居，802.11r 的漫遊機制在 WiFi AP 的責任上是必須設定列出自己的鄰居是哪些 AP，並確實輸入新增於列表內，以利 WiFi 客戶端網路卡設備隨時連接上任一台 WiFi AP 的同時也就得到了 802.11r 漫遊協定的預先”鄰居清單”，因此 WiFi 客戶端網路卡就可以順利提早加速完成了快速漫遊換連。

AP distance/power level is based on client connection RSSI threshold.



步驟-4： 對每台 WiFi AP 進行 802.11r 設定；就上圖例作為後續相關設定範例：

1.) IP 251 WiFi AP 的相鄰鄰居是 IP 252 WiFi AP，即表示 IP251 WiFi AP 必須：

於 Radio-0(2.4G)的漫遊 11r 設定內需新增鄰居 8c:4d:ea:ff:ff:3f 於漫遊清單(R0KH 或 R1KH 清單)內。

於 Radio-1(5G)的漫遊 11r 設定內需新增鄰居 8c:4d:ea:ff:ff:40 於漫遊清單(R0KH 或 R1KH 清單)內。

2.) IP 252 WiFi AP 的相鄰鄰居是 IP 251 WiFi AP 與 IP 253 WiFi AP，即表示 IP252 WiFi AP 必須：

於 Radio-0(2.4G)的漫遊 11r 設定內需新增鄰居 8c:4d:ea:ff:ff:30 與 8c:4d:ea:ff:ff:4e 於漫遊清單(R0KH 或 R1KH 清單)內。

於 Radio-1(5G)的漫遊 11r 設定內需新增鄰居 8c:4d:ea:ff:ff:41 與 8c:4d:ea:ff:ff:4f 於漫遊清單(R0KH 或 R1KH 清單)內。

3.) IP 253 WiFi AP 的相鄰鄰居是 IP 252 WiFi AP，即表示 IP253 WiFi AP 必須：

於 Radio-0(2.4G)的漫遊 11r 設定內需新增鄰居 8c:4d:ea:ff:ff:3f 於漫遊清單(R0KH 或 R1KH 清單)內。

於 Radio-1(5G)的漫遊 11r 設定內需新增鄰居 8c:4d:ea:ff:ff:40 於漫遊清單(R0KH 或 R1KH 清單)內。

以上直至步驟 1~步驟 3，引導說明了 WiFi 客戶端網路卡設備連接 WiFi AP 接入點後

於 IEEE802.11 協會制定的 802.11r 快速漫遊的基本運作關係的理解，將快速助您後續”如何建立每台的 R0 /R1Key Holders (R0KH 或 R1KH)鄰居清單設定，以下接續以設定頁面開始引導新增漫遊清單：

1.) IP 251 WiFi AP 的相鄰鄰居是 IP 252 WiFi AP，即表示 IP251 WiFi AP 必須：

於 Radio-0(2.4G)的漫遊 11r 設定內需新增鄰居 8c:4d:ea:ff:ff:3f 於漫遊清單(R0KH 或 R1KH 清單)內。

漫遊共享域稱：
每台都必須設定取名為同一個“域稱”以利自己建立的快速漫遊環境得以區別辨識，當然您也可以直接選用預設值的域稱“a1b2”即可。

快速漫遊設定

- Mobility Domain: 8c4d
- R0 Key Lifetime: 10000
- Reassoc期限: 1000
- R0/NAS Identifier: ap.8c4d.com
- R1 Identifier: 000102030405
- R1 Push: ☒ 啟用

R0 Key holders

- MAC位址: 8c:4d:ea:ff:ff:40
- NAS Identifier: ap.8c4d.com
- 128-bit Key: 12345678901234567890123456789012

R0 Key Holder List

#	MAC位址	NAS Identifier	128-bit Key	執行
1	8c:4d:ea:ff:ff:40	ap.8c4d.com	12345678901234567890...	刪除

R1 Key Holders

- MAC位址: (empty)
- R1 Identifier: (empty)
- 128-bit Key: 128-bit key as hex string

R1 Key Holder List

#	MAC位址	NAS Identifier	128-bit Key	執行
-	-	-	-	-

新增填入鄰居的 BSSID

金鑰密碼自訂設定：
於此環境每台要建立各自的鄰居清單金鑰都需相同一致

就新增鄰居時填入

建議啟用 R1 Push 功能，意思是第二層金鑰的生成，就是 R1KH 金鑰自動透過 R0KH 現有清單內容與 WiFi 客戶網路卡溝通後自動生成，因此得以省略 R1KH 的清單建立。

建立 ROKH 鄰居清單所需用到的識別標識字符。此格式需求以網址格式自訂表示，當然您也可以直接選用預設值的標識字符 ap.example.com 即可。

新增完成了要供給 WiFi 客戶網路卡連線後取用的 ROKH 鄰居清單列表。

於 Radio-1(5G)的漫遊 11r 設定內需新增鄰居 8c:4d:ea:ff:ff:40 於漫遊清單(R0KH 或 R1KH 清單)內。

快速漫遊

- 快速漫遊: ☒ 啟用

快速漫遊設定

- Mobility Domain: (empty)
- R0 Key Lifetime: (empty)
- Reassoc期限: (empty)
- R0/NAS Identifier: (empty)
- R1 Identifier: (empty)
- R1 Push: ☒ 啟用

R0 Key holders

- MAC位址: 8c:4d:ea:ff:ff:40
- NAS Identifier: ap.8c4d.com
- 128-bit Key: 12345678901234567890123456789012

R0 Key Holder List

#	MAC位址	NAS Identifier	128-bit Key	執行
1	8c:4d:ea:ff:ff:40	ap.8c4d.com	12345678901234567890...	刪除

R1 Key Holders

- MAC位址: 目的端 MAC 位址
- R1 Identifier: (empty)
- 128-bit Key: 128-bit key as hex string

R1 Key Holder List

#	MAC位址	NAS Identifier	128-bit Key	執行
-	-	-	-	-

如上相同

新增完成了要供給 WiFi 客戶網路卡連線後取用的 ROKH 鄰居清單列表。

2.) IP 252 WiFi AP 的相鄰鄰居是 IP 251 WiFi AP 與 IP 253 WiFi AP，即表示 IP252 WiFi AP 必須：於 Radio-0(2.4G)的漫遊 11r 設定內需新增鄰居 8c:4d:ea:ff:ff:30 與 8c:4d:ea:ff:ff:4e 於漫遊清單(R0KH 或 R1KH 清單)內。

漫遊共享域稱：
每台都必須設定取名為同一個“域稱”以利自己建立的快速漫遊環境得以區別辨識，當然您也可以直接選用預設值的域稱“a1b2”即可。

快速漫遊設定

Mobility Domain: 8c4d

R0 Key Lifetime: 10000

Reassoc期限: 1000

R0/NAS Identifier: ap.8c4d.com

R1 Identifier: 000102030405

R1 Push: ☒ 啟用 ☐ 關閉

建議啟用 R1 Push 功能，意思是第二層金鑰的生成，就是 R1KH 金鑰自動透過 R0KH 現有清單內容與 WiFi 客戶網路卡溝通後自動生成，因此得以省略 R1KH 的清單建立。

R0 Key holders

MAC位址: 8c:4d:ea:ff:ff:4e

NAS Identifier: ap.8c4d.com

128-bit Key: 12345678901234567890123456789012

R0 Key Holder List

#	MAC位址	NAS Identifier	128-bit Key	執行
1	8c:4d:ea:ff:ff:31	ap.8c4d.com	12345678901234567890...	刪除
2	8c:4d:ea:ff:ff:4f	ap.8c4d.com	12345678901234567890...	刪除

R1 Key Holders

MAC位址:

R1 Identifier:

128-bit Key: 128-bit key as hex string

R1 Key Holder List

#	MAC位址	NAS Identifier	128-bit Key	執行
-	-	-	-	-

新增填入鄰居的 BSSID

金鑰密碼自訂設定：於此環境每台要建立各自的鄰居清單金鑰都需相同一致

就新增鄰居時填入

建立 R0KH 鄰居清單所需用到的識別標識字符。此格式需求以網址格式自訂表示，當然您也可以直接選用預設值的標識字符 ap.example.com 即可。

於 Radio-1(5G)的漫遊 11r 設定內需新增鄰居 8c:4d:ea:ff:ff:41 與 8c:4d:ea:ff:ff:4f 於漫遊清單(R0KH 或 R1KH 清單)內。

快速漫遊設定

Mobility Domain:

R0 Key Lifetime:

Reassoc期限:

R0/NAS Identifier:

R1 Identifier:

R1 Push: ☐ 啟用 ☒ 關閉

如上相同

R0 Key holders

MAC位址: 8c:4d:ea:ff:ff:4e

NAS Identifier: ap.8c4d.com

128-bit Key: 12345678901234567890123456789012

R0 Key Holder List

#	MAC位址	NAS Identifier	128-bit Key	執行
1	8c:4d:ea:ff:ff:30	ap.8c4d.com	12345678901234567890...	刪除
2	8c:4d:ea:ff:ff:4e	ap.8c4d.com	12345678901234567890...	刪除

R1 Key Holders

MAC位址:

R1 Identifier:

128-bit Key: 128-bit key as hex string

R1 Key Holder List

#	MAC位址	NAS Identifier	128-bit Key	執行
-	-	-	-	-

新增完成了要供給 WiFi 客戶網路卡連線後取用的 R0KH 鄰居清單列表。

3.) IP 253 WiFi AP 的相鄰鄰居是 IP 252 WiFi AP，即表示 IP253 WiFi AP 必須：

於 Radio-0(2.4G)的漫遊 11r 設定內需新增鄰居 8c:4d:ea:ff:ff:3f 於漫遊清單(R0KH 或 R1KH 清單)內。

按圖例架構此須新增的 R0KH 鄰居清單與 IP251 相同，請參考 1.) 此不在重複贅述。

於 Radio-1(5G)的漫遊 11r 設定內需新增鄰居 8c:4d:ea:ff:ff:40 於漫遊清單(R0KH 或 R1KH 清單)內。

按圖例架構此須新增的 R0KH 鄰居清單與 IP251 相同，請參考 1.) 此不在重複贅述。

” 802.11r 無縫漫遊設定成功的必要前提再次溫馨提醒如下：

1. 環境每台 Cerio WiFi AP ” 彼此都已佈置有” 漫遊末端的重疊訊號” 。
2. 每台 Cerio WiFi AP 使用相同頻道與相同 SSID 名稱(ESSID) 與相同的 WiFi 加密。
3. 為每台 Cerio WiFi AP” 設定自己相對的” R0 /R1Key Holders 等其他相關 AP 鄰居清單” 。
4. 連接 Cerio WiFi AP 的 WiFi 客戶端網路卡(Client)也必須有支援相同 802.11r/k 漫遊協定。

更多詳細設定請參考手冊” 無線基地台 SSID” 與” 頻道設定” 與 802.11r 快速漫遊 等相關章節說明。

10-2. 點對點或點對多 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，此設定方法請參考手冊“WDS 設定”說明，此此相關文件主要引導 WDS 重點程序，此只要依照以下流程將能輕鬆架構 WDS 點對點或點對多之應用

- 1) 若要點對點橋接使用 WDS 功能，此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，此請確實每台的無線基地台 IP 位址需同網段不能重複
- 3) 依照要應用於 2.4G 或 5G 之需求，此請確實每台無線基地台設定一組共同的使用頻道 (請參考手冊“無線設定”(Radio 0 或 Radio 1))
- 4) 請參考 WDS 設定頁面正確設定要連接的無線基地台 MAC 位址，此若以 A 和 B 兩台橋接做範例，此則 A 台須設定 B 台的 MAC 位址，此相對的 B 台則須設定 A 台的 MAC 位址
- 5) 確認後重新啟動將完成 WDS 點對點橋接，此可參考手冊“WDS 狀態”確認 RSSI 值，此若為-1 表示沒有連接成功，此請重新確認設定檔是否按照以上說明，此或是基地台間的訊號遭受阻隔過干擾。

補充：RSSI 值絕佳落在 30~50 間，爆高表示 AP 與 AP 之間太近，太低表示訊號沒互相對好或是距離太遠
其他說明：因 WDS 應用是在無線基地台模式之下，若啟用 WDS 功能則將是 AP+WDS 之應用，倘若要純使用 WDS 功能不需無線基地台(AP)，則可[參考手冊“虛擬無線基地台網路設定”](#)說明，將無線基地台(AP)進行關閉，如下圖



10-3. 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 CenOS5.0, 並啟用網頁認證功能，此則將能自訂編輯網頁認證頁面，此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“網頁認證”功能)

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

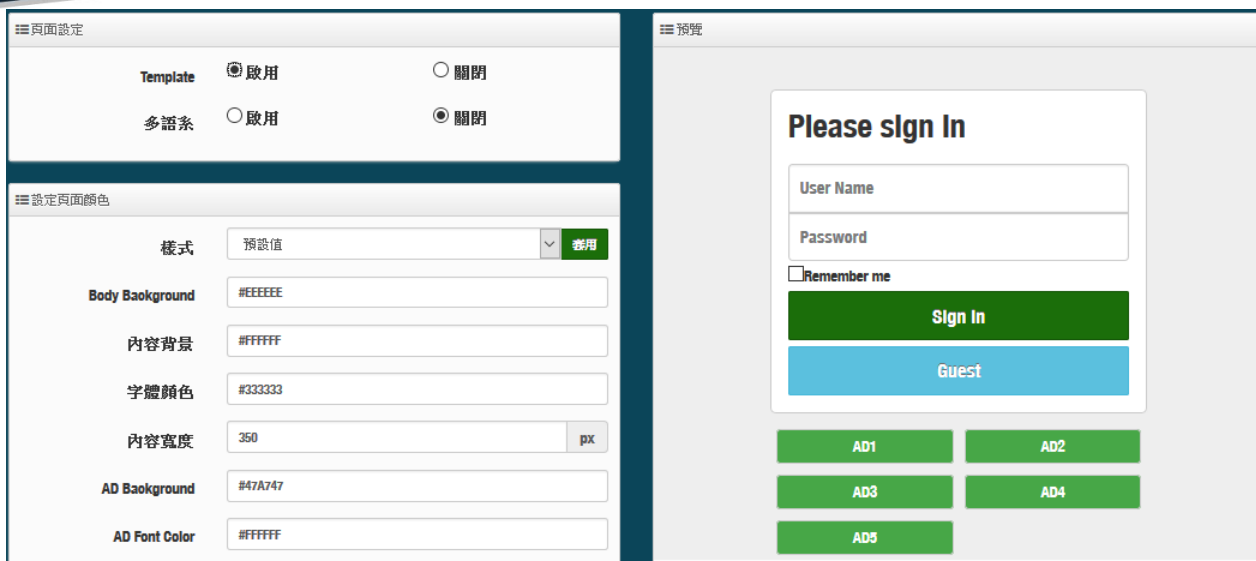
步驟三：請至認證功能的下拉功能按鈕，進入建立帳戶名稱與密碼，如下圖說明

特別補充:

- * 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**

【建議管理者本身須具有網頁 Html/CSS 編寫基本能力) 本公司無負責網頁語法指導。】

步驟四：若要使用系統預設的認證頁面，可參考使用手冊“客製化頁面”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**



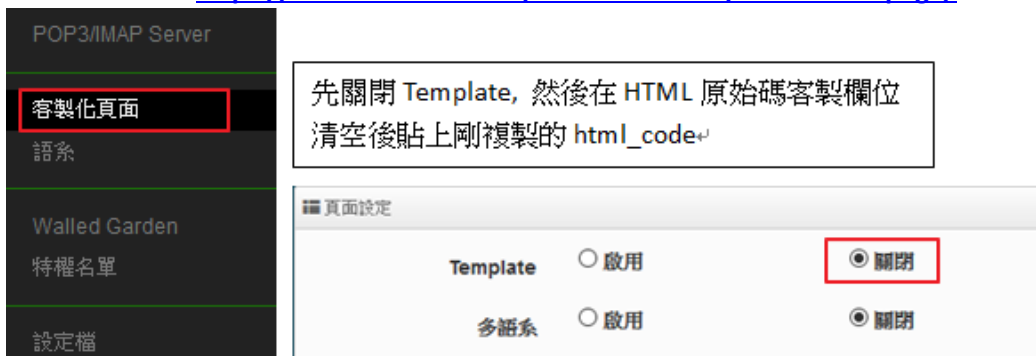
步驟五: 因登入頁面圖檔必須放置網站伺服器上，所以須將網站位址建立白名單，此範例的背景圖存放位置在本公司第二台伺服器上，所以請確實將以下網址輸入至 Walled Garden 內。

(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/extreme-indoor/customized-page/>



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

```

HTML原始碼客製
<html>
<head>
<title>Authentication Login Page ( On-line Web Demo Version )</title>
<link rel="stylesheet" type="text/css" href="http://www.serio.com.tw/login_page_demo
/sample3_en/format.css" />
<script src="/javascripts/login.js" charset="utf-8" type="text/javascript"></script>
<style type="text/css">
.t1 { color: #FFF; background-color: #421f19; text-align: center;}
.t1_a {font-size: 18px; font-family: Century Gothic;}
.backg {background-image: url(http://www.serio.com.tw/login_page_demo/sample3_en
/newshop_background.jpg);}
.reme_font {
font-size: 12px;
height: 30px;
line-height: 30px;
text-align: center;
color: #333;
border-radius: 10px 10px 0px 0px;
font-weight: bold;
}
.backg2 {background-image: url(http://www.serio.com.tw/login_page_demo/sample3_en

```

如下範本的登入頁面





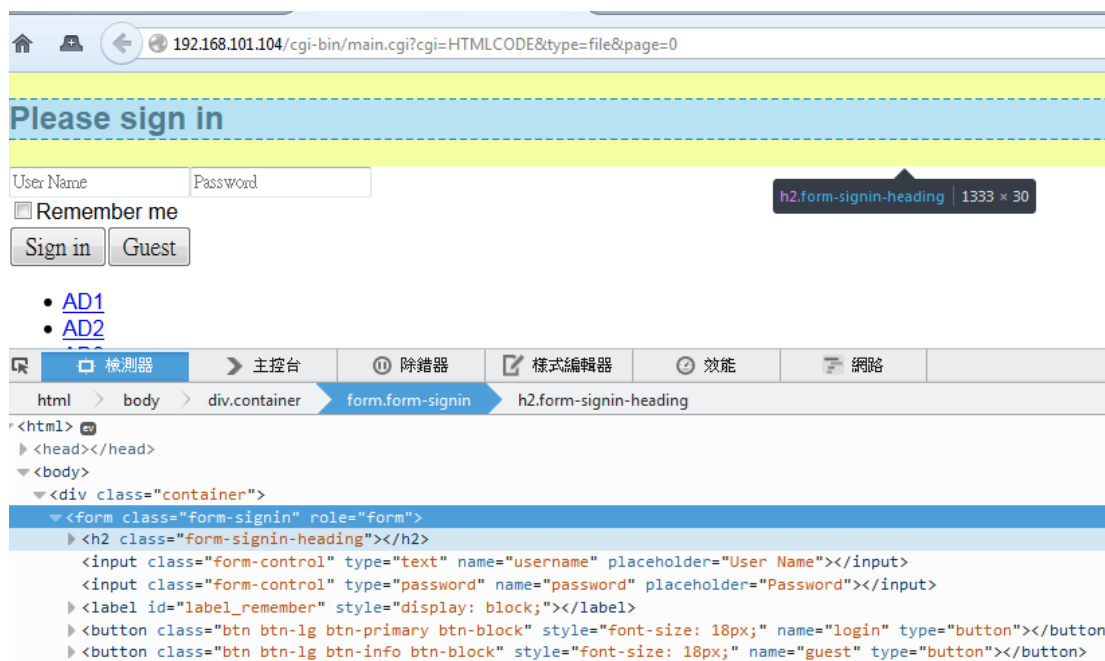
1. 此欄位必須在 190 行間之內，若撰寫的 HTML/CSS 等原始碼超過一定的行間下，建議將 CSS 原始碼存放至遠端 Web Server，然後將遠端 web server 的 IP 位址輸入至 Walled Garden 內。
(請參考手冊 “Walled Garden “設定說明)
2. 本設備不支援圖檔的存放空間，若必要請將圖檔存放至遠端 web 伺服器，透過位址呼叫近來，同上作法。

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>
```

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

☐ Remember me

10-4. 地區 5Ghz WiFi 頻道相關・國家/地區 DFS(動態頻率選擇) 列表資訊

頻段/U-NII	使用頻率 (MHz)	頻率/頻寬模式/對應使用頻道				(各國)區域性開放規範			
		20MHz	40Mhz	80Mhz	160Mhz	美國(US)	歐洲(Europe)	Japan(日本)	Taiwan(台灣)
Band1 (U-NII-1)	5180	36	36~40	36~48 (42)	36~64 (50)	YES	Indoors	Indoors	Indoors
	5200	40	(38)			YES	Indoors	Indoors	Indoors
	5220	44	44~48			YES	Indoors	Indoors	Indoors
	5240	48	(46)			YES	Indoors	Indoors	Indoors
Band2 (U-NII-2A)	5260	52	52~56	52~64 (58)		DFS	Indoors/DFS	Indoors/DFS	Indoors
	5280	56	(54)			DFS	Indoors/DFS	Indoors/DFS	Indoors
	5300	60	60~64			DFS	Indoors/DFS	Indoors/DFS	Indoors
	5320	64	(62)			DFS	Indoors/DFS	Indoors/DFS	Indoors
Band3 (U-NII-2C)	5500	100	100~104	100~112 (106)	100~128 (114)	DFS	DFS	DFS	DFS
	5520	104	(102)			DFS	DFS	DFS	DFS
	5540	108	108~112			DFS	DFS	DFS	DFS
	5560	112	(110)			DFS	DFS	DFS	DFS
	5580	116	116~120	116~128 (122)		DFS	DFS	DFS	DFS
	5600	120	(118)			DFS	DFS	DFS	DFS
	5620	124	124~128			DFS	DFS	DFS	DFS
	5640	128	(126)			DFS	DFS	DFS	DFS
	5660	132	132~136	132~144 (138)	N/A	DFS	DFS	DFS	DFS
	5680	136	(134)			DFS	DFS	DFS	DFS
	5700	140	140~144			DFS	DFS	DFS	DFS
	5720	144	(142)			DFS	NO	NO	NO
Band4 (U-NII-3)	5745	149	149~153	149~161 (155)		YES	NO	NO	NO
	5765	153	(151)			YES	NO	NO	NO
	5785	157	157~161			YES	NO	NO	NO
	5805	161	(159)			YES	NO	NO	NO
	5825	165				YES	NO	NO	NO

* DFS 頻道增加了使用者可以選擇的頻道數量。這些附加頻道是共用於特定的軍用雷達、衛星通訊、氣象雷達的頻道使用，頻道共用過程會進行使用前可用性檢查程序(Channel Availability Check process, CAC) 並遵循自動閃避跳頻道退讓機制，對於點對點或點對多的“WDS 等模式”需要綁定固定頻道的設定模式而言，當其中一個站點閃避跳頻將會造成多點對或多點的無線中斷，將需再次重新設定，若非單純的“無線基地台模式”等是為了無線網卡存取上網或“Client Bridg 模式”等跟隨頻道性的設定應用類型，建議請盡量不要選擇 DFS 共用通道使用。

Appendix A. WEB GUI Valid Characters

Table A 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
	Beacon Interval	20 ~ 1024
Advanced Setup	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