CERIO Corporation

DR-5000

Multi WAN 2.5Gigabit VPN 路由閘道器

使用手冊

Web管理頁面 / 登入資訊	
預設IP 位址	192.168.2.1
使用者名稱	root
登入密碼	defaul

1.系統管理及主體相關說明

1.1 主體外觀功能

1. DC 電源輸入孔 (電源輸入-選擇 1)
2. LED 狀態顯示燈 ：

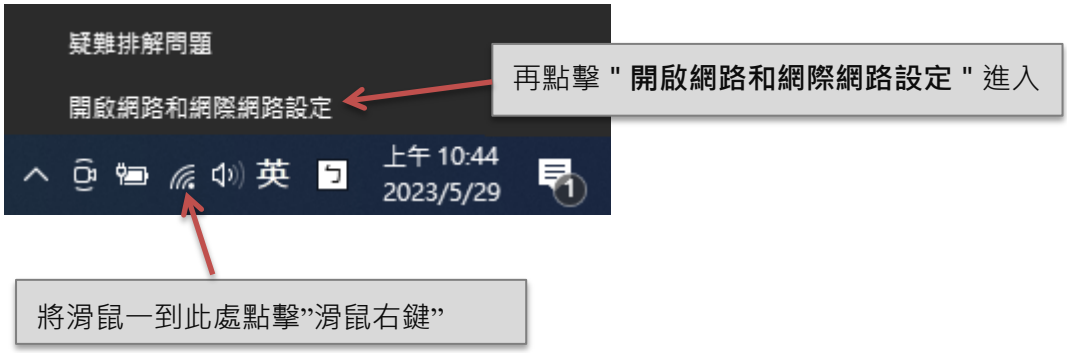
	PWR 作用燈: 當確認 PoE 輸入或 DC 輸入供電主板有受電情況下開機恆亮。
	Fail 作用燈:主機系統問題警示燈（OS 儲存無法被正常存取與異常時恆亮）。
	Online 作用燈:工作運行中燈（ 系統開機起動過程以閃爍顯示當系統順利啟動完畢且確實後則以恆亮表示成功 Ready 中狀態 ）。
	網路埠作用燈 ：ETH1 埠至 ETH4 埠 Link/Act 連線燈。

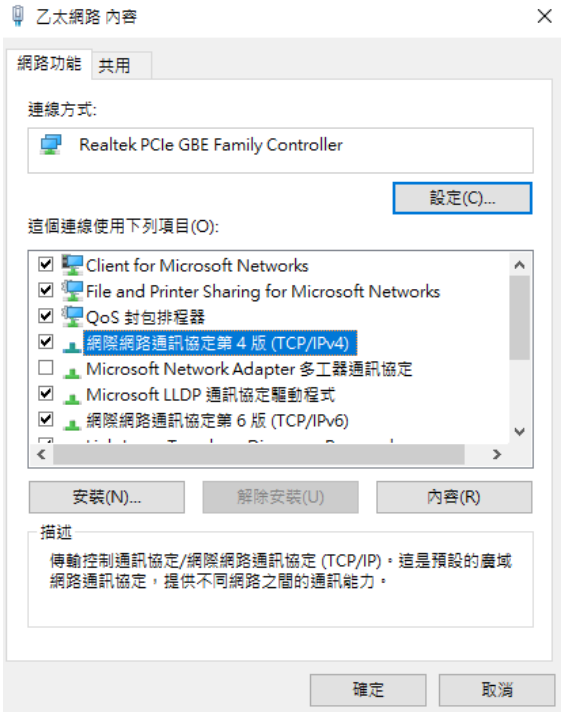
3. Reset 按鈕 (回復出廠預設值, 請按壓約 10-15 秒後，可視 Online LED 與 Fail LED 這兩個已同時產生閃爍，表示已確認，按鍵即可脫離放開等待系統回復預設值)

4. 2.5Gigabit / ETH1(POE)網路連接埠,可透過軟體變更 WAN 或 LAN 埠 (電源輸入-選擇 2)
5. Gigabit / ETH2(POE)網路連接埠,可透過軟體變更 WAN 或 LAN 埠 (電源輸入-選擇 3)
6. Gigabit / ETH3 網路連接埠,可透過軟體變更 WAN 或 LAN 埠
7. Gigabit / ETH4 網路連接埠,可透過軟體變更 WAN 或 LAN 埠
8. GND 裝置接地螺絲接點

1.2 系統登入前設定

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 192.168.2.1 (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，在連接此設備之前，電腦端需先設置與此設備相同的 IP 網段才能順利連接，請參考以下步驟設定您的電腦。





- 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

DR-5000 支援網頁管理介面，可開啟瀏覽器並輸入以下資訊即可登入管理介面。

以下為 DR-5000 登入預設值 Router 模式時頁面資訊

- **預設 IP 位址**: 192.168.2.1
- **遮罩**: 255.255.255.0
- **預設帳密: 如下表**

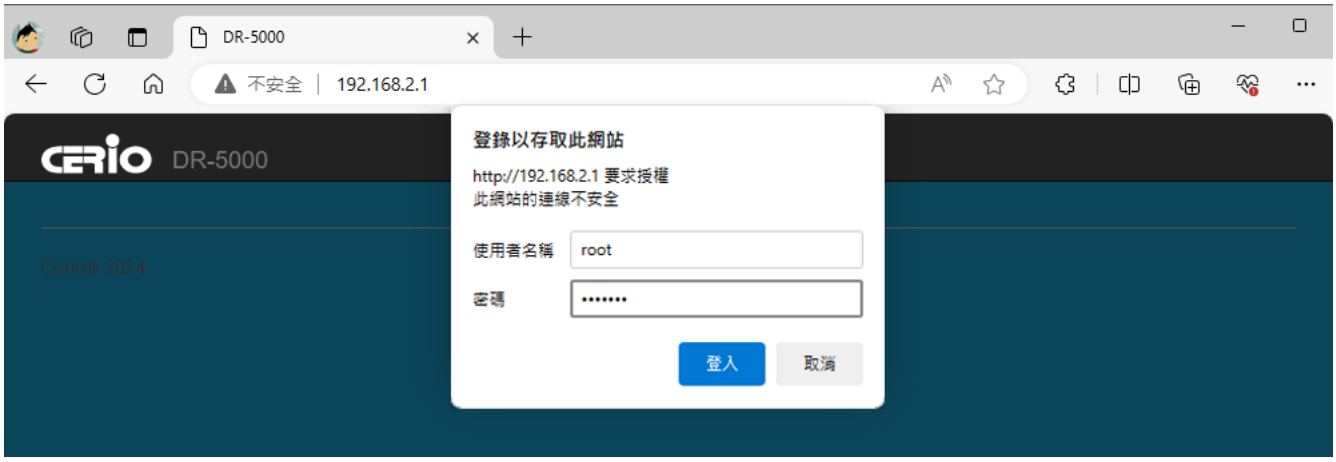
MODE	Router mode	
Management Account	Root Account	
Username	root	
Password	default	

Notice

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 192.168.2.1 的 IP 位址進行存取管理。

瀏覽器登入

開啟 IE 瀏覽器或其他如 Firefox、Chrome、Edge 瀏覽器，並於 URL 網址列中輸入此設備預設的 IP 位址：http://192.168.2.1，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。

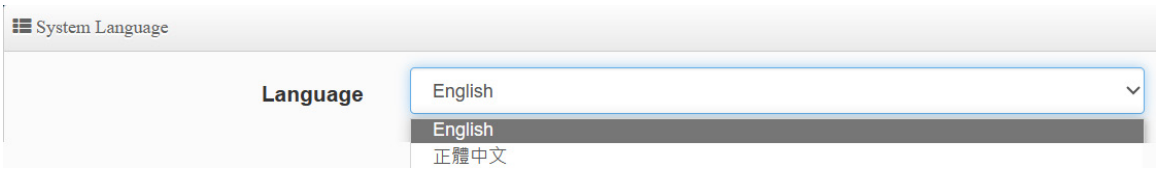
2.初次登入系統管理介面設定

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。

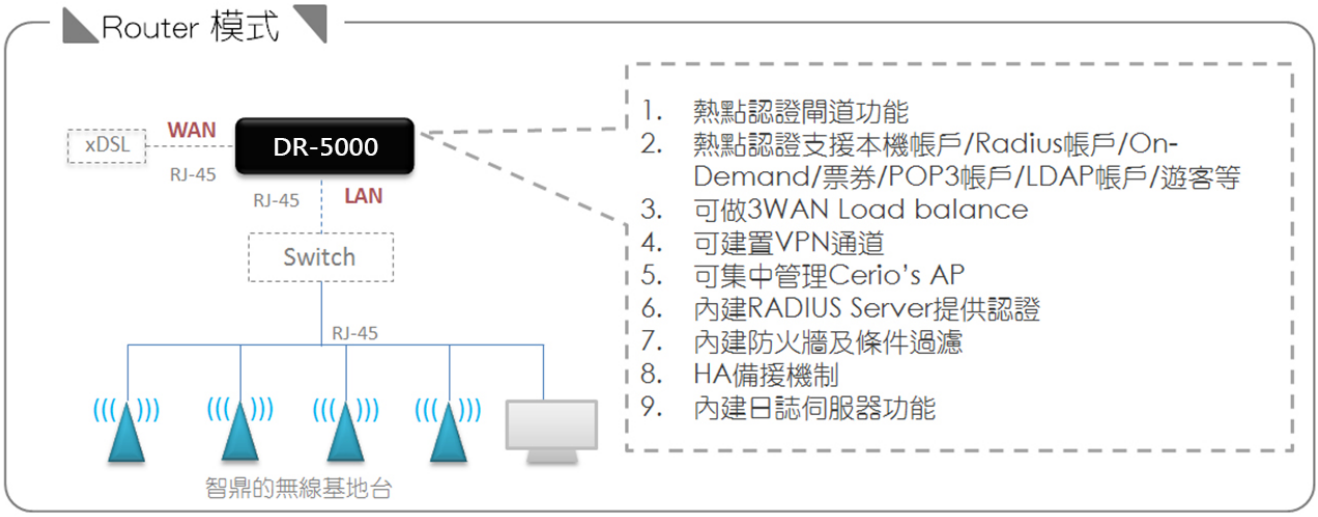
【預設啟動操作介面為英文】



2.2 基本架構與應用模式說明

2.2.1 Router 模式 (預設值模式)

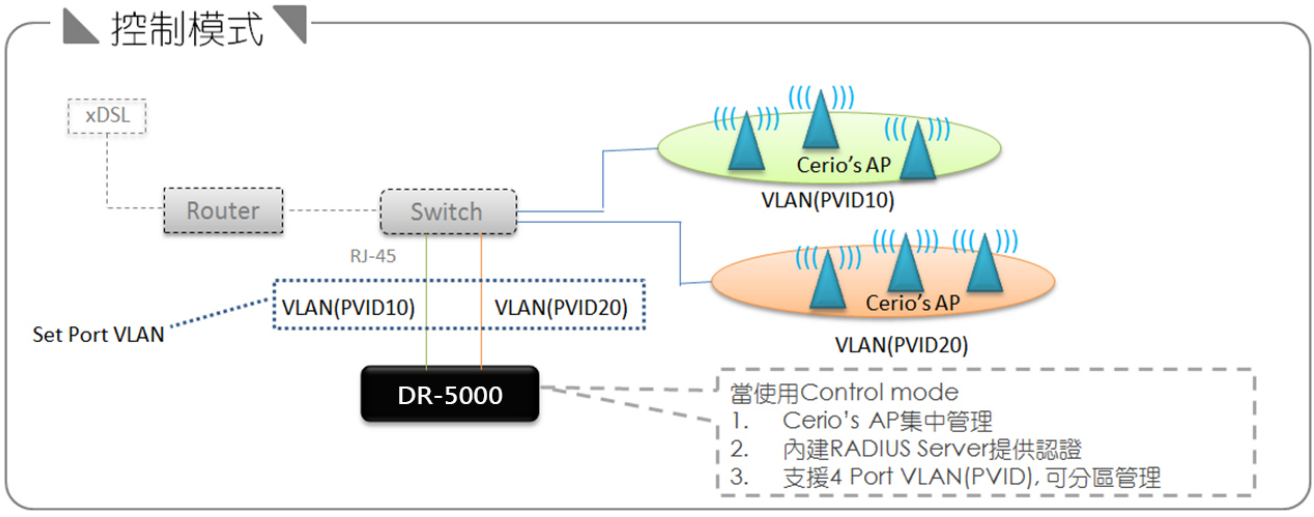
當切換成 Router 模式時，可設定 1WAN 路由設備或是多 WAN 的附載平衡機制，除此之外將可啟用熱點認證功能，在設備底下的所有用戶都可被攔截認證，此模式除了是路由設備外，同時具備基地台集中管理功能並兼具基本防火牆及 RADIUS 伺服器等完整多功能應用



若環境架構中沒有 Router/Firewall 設備，但又想建置網頁熱點認證應用，則可採用此 Router 模式，就能簡單完成應用需求

2.2.2 Captive portal 模式

當切換成 Captive Portal 模式時,屬於旁側狀態，為熱點認證機制，差別在此模式並無 Router 路由功能(此模式預設 IP 同樣為 192.168.2.1 ,但與 Router 模式 IP 位置不連動設計，當切換至此模式時請確保連線電腦的 IP 網段也相同為 192.168.2.X，已順利進入此模式)



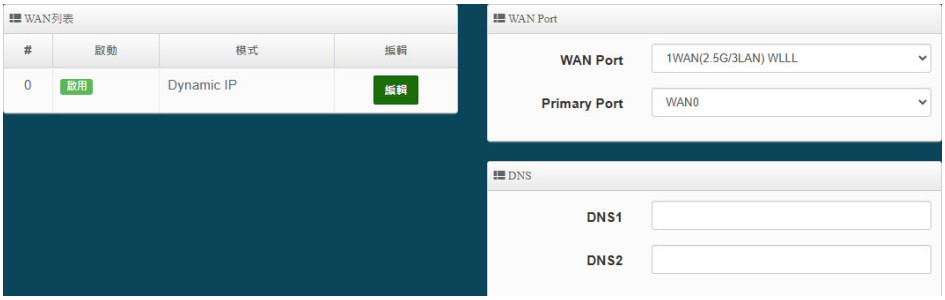
3. 系統設定

CERIO 的 DR-5000 是多功能認證閘道器，支持多 WAN 出站負載平衡，並可集中管理 CenOS5.0 AP。DR-5000 內建硬體獨立 VPN 引擎管理員可以在網絡環境中建置安全隧道，並支持高可用性，以確保網路的正常工作。

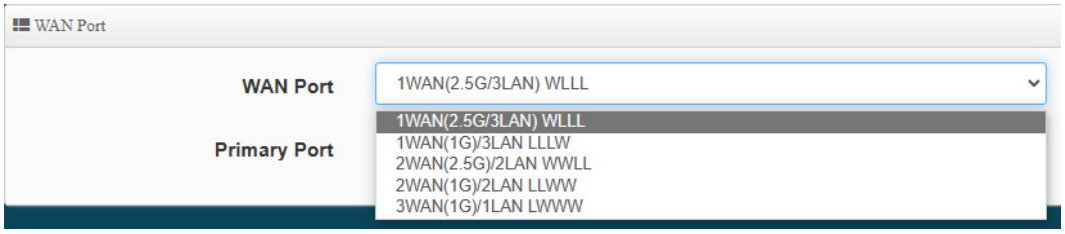
3.1 WAN 設定

此功能只在 Router 模式下運作, 管理員可以在 WAN 設置功能中設置一個 WAN 或多 WAN 負載平衡。

請點擊 System ➔ WAN Setup

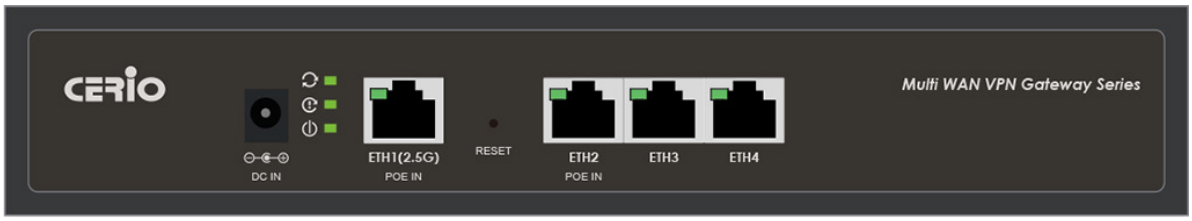


WAN Port 設定



- **WAN Port:** 管理員可以選擇設定型態為 1WAN(2.5Gb)/3LAN 或 3LAN/1WAN 或 2WAN(2.5Gb+1Gb)/2LAN 或 2LAN/2WAN 或 1LAN/3WAN,預設值為 1WAN(2.5Gb)/3LAN

實體網路埠設定不同 WAN 與 LAN 埠定義詳細列表:



Ethernet Speed		2.5Gb	1Gb	1Gb	1Gb
Mode / Port		ETH1	ETH2	ETH3	ETH4
1(預設)	1WAN(2.5Gb)/3LAN(1Gb+1Gb+1Gb) / WLLL	WAN	LAN	LAN	LAN
2	3LAN(2.5Gb+1Gb+1Gb)/1WAN(1Gb) / LLLW	LAN	LAN	LAN	WAN
3	2WAN(2.5Gb+1Gb)/2LAN(1Gb+1Gb) / WWLL	WAN	WAN	LAN	LAN
4	2LAN(2.5Gb+1Gb)/2WAN(1Gb+1Gb) / LLWW	LAN	LAN	WAN	WAN
5	1LAN(2.5Gb)/3WAN(1Gb+1Gb+1Gb) / LWWW	LAN	WAN	WAN	WAN

- WAN List：當選擇多 WAN 時, 則可顯示 WAN Priority 設定,請按下儲存按鈕，同時系統將會顯示多 WAN 的列表

Notice	當選擇 2WAN 以上, 則可在 WAN 流量設定功能頁面去設定負載平衡的優先等級設定

- **WAN Priority**：系統將先判斷 3WAN 的優先等級，數值越小優先等級越高，若設為 1/1/2 即其 WAN0/WAN1 Load Balance(負載平衡), WAN2 為 Backup, 若設為 1/1 即其 WAN0/WAN1 Load Balance, 若設為 1/2 即其 WAN2 為 Backup.

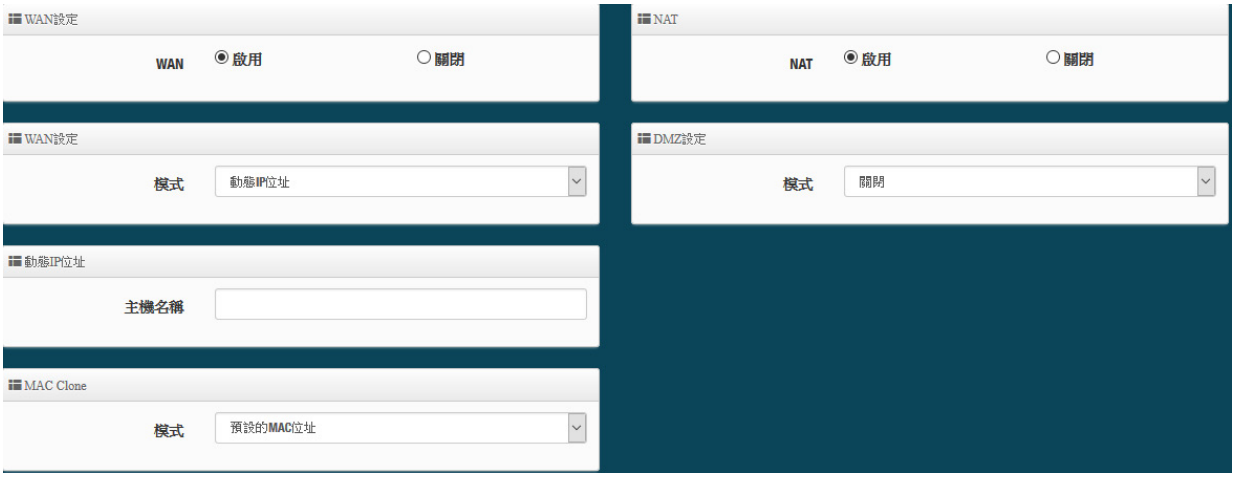
- **Primary Port:** 系統使用 WAN 埠指定設定，主要是讓系統透過設定指定的 WAN 埠去使用對外的訪問, 例如系統時間校正或是 DNS 訪問等等，若無特殊應用此設定預設值設定 WAN0 即可。
- **NAT Engine:** 啟用此功能將會自動關閉防火牆/路由等相關規則, 讓 DR-5000 能提高效能增加 NAT 使用速度, **若須使用本機的防火牆/路由等規則設定,請將此功能設定為" 關閉" 狀態。**

WAN List

管理員可以為 WAN 端口設置四種連接類型：靜態 IP，動態 IP，PPPoE 和 PPTP，同時還可以啟用或禁用 NAT 或 DMZ 功能。

請點擊 WAN 列表中的編輯按鈕。

➢ **編輯:** 管理人員可以點擊此按鈕進入 WAN 的連接設定頁面

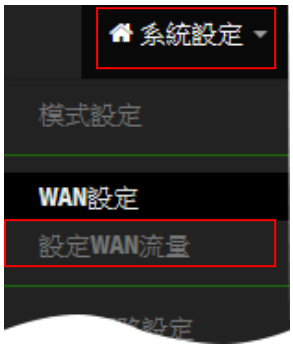


- **WAN:** 管理員可以啟用或關閉此 WAN 的功能.
- **WAN 設定:** 管理員可以選擇設定 WAN 屬於靜態 IP/動態 IP/PPPoE 或 PPTP 連接方式
- **MAC Clone:** MAC 位址對外顯示，預設為 DR-5000 的 MAC，若有些環境需要 MAC 驗證後方可上網，而驗證須以 PC 端的 MAC 位址，則管理人員可以手動指定設定去選擇使用 Manual MAC 位址，輸入 PC 或欲自行指定其他的 MAC 即可。
- **NAT:** 管理員可以選擇啟動或關閉系統的NAT服務，建議使用預設值，**若環境有特殊需求，必須手動設定路由，則請關閉此 NAT 功能。**
- **DMZ:** 此 DMZ 功能屬於軟體切割一個 DMZ 安全區域，管理員可以設定一組區域網路上的伺服器 IP 位址對外服務，必須配合虛擬網路設定。

3.2 設定 WAN 流量

WAN 的流量設定主要能改善對外連接網路的流量品質負載平衡,此頁管理可以設定 WAN 的權重，依照權重分配可讓整個網路均衡分散流量，避免單一 WAN 埠流量過載。

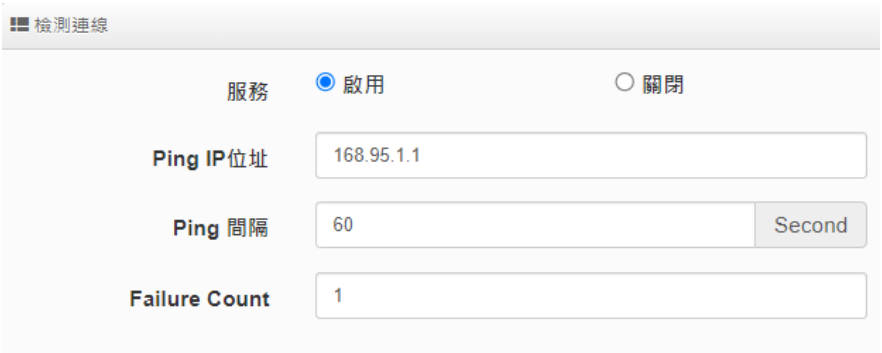
請點擊 “系統設定” ➔ “設定 WAN 流量” 進入管理



- **模式:** 如果設置多 WAN，管理員可以選擇通過分配重量或線速度重量的負載平衡。
  - **分配權重:** WAN 分配權重功能可以設置處理更多請求和處理更少的請求。 為 WAN 分配權重允許 DR-5000 設備確定每個 WAN 負載平衡服務器可以處理多少流量，從而更有效地平衡負載。 重量設置最大值 = 10 單位。

  - **Line Speed Weight:** 此功能主要以 WAN 的速度來分配優先順序

- **檢測連線:** 啟用檢測連線，設定輸入指定 Ping 的對象 IP，並設定每次 Ping 的間隔週期時間” 秒” ，設定 Failure Count (失敗次數)後以確實達到 WAN 負載平衡的啟用。



3.3 虛擬網路設定

預設值 Router 模式內支援 16 組虛擬網路服務，預設每個虛擬網路都支援 802.1Q Tag VLAN 功能，管理員只要點擊啟用，系統將能完成設定 802.1Q Tag VLAN。

虛擬網路列表

#	虛擬網路服務	旗標	IP位址	子網路遮罩	執行
0	啟用	Native	192.168.2.1	255.255.255.0	網路
1	停用	VLAN TAG: 101	192.168.101.254	255.255.255.0	網路
2	停用	VLAN TAG: 102	192.168.102.254	255.255.255.0	網路
3	停用	VLAN TAG: 103	192.168.103.254	255.255.255.0	網路
4	停用	VLAN TAG: 104	192.168.104.254	255.255.255.0	網路
5	停用	VLAN TAG: 105	192.168.105.254	255.255.255.0	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。
- **旗標**：顯示實體網路孔預設運作使用哪個虛擬網路資訊，當顯示 " Native " 表示預設使用的虛擬網路，同時可顯示每個虛擬網路所使用的 802.1Q Tag 號碼。
- **IP 位址**：顯示每個虛擬網路的 IP 位址。
- **子網路遮罩**：顯示每個虛擬網路的子網路遮罩。
- **執行**：點擊 網路 的按鈕，進入 LAN 的設定頁面，點擊 網路 下拉箭頭則可設定”頻寬控制:及” DHCP 伺服器” 功能設定。

3.3.1 網路設定(按鈕)

網路：點擊 網路 按鈕進入設定虛擬網路相關功能。

- **虛擬網路服務**：可選擇啟用或關閉虛擬網路服務。
- **IP 位址**：設定虛擬網路的 IP 位址。
- **子網路遮罩**：設定虛擬網路 IP 位址的子網路遮罩。

Notice 虛擬網路服務及 IP 位址至少需要有一組 VLAN 服務可以正常登入管理，**請勿將預設的一組的虛擬網路服務(VLAN)功能關閉(等於無 LAN 狀態)，造成必須回復預設值後始能再次正常登入管理頁面進行管理。**

- **VLAN Tag:** 設定此 VLAN 網路為 802.1Q Tag VLAN

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

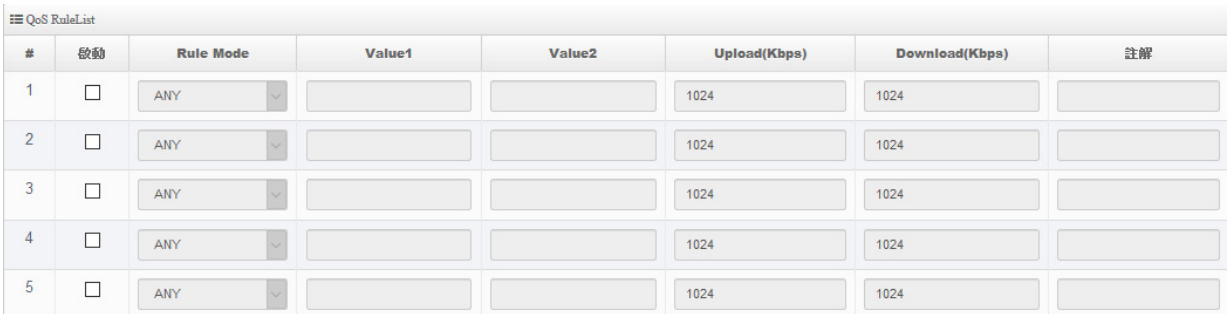
3.3.2 頻寬控制

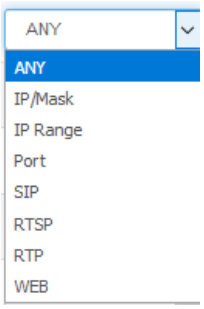
可管理 VLAN 或是用戶端的使用最大/小頻寬, 用戶頻寬管理可限制 IP/MASK , IP Range, Port(Service), SIP, RTP/RTSP, WEB 等等的頻寬限制。

- **模式:** 管理員可以選擇啟用或關閉頻寬控制功能。
- **Session Limit Per IP:** 針對此 VLAN 的所有的每一個 IP 限制連線的最大 Session 數，預設值為每一個使用者 IP 限制使用為 1024 條 Session(連線數)。
- **Total bandwidth Control:** 針對此 VLAN 限制總頻寬流量。管理者可設定最大總上載及下載的頻寬限制。

QoS Rule List: 可建置 10 筆 QoS 規則

管理者可針對 IP/MASK , IP Range, Port(Service), SIP, RTP/RTSP, WEB 等協議管理頻寬流量



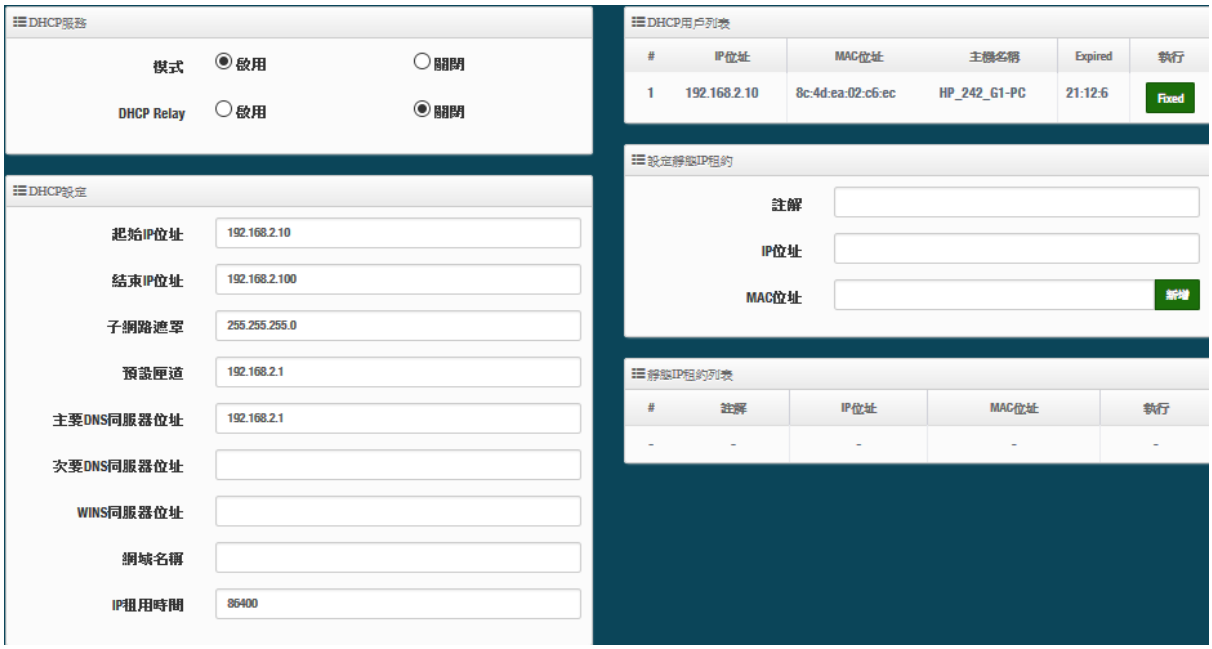


- **Any:** 表示所設定限制的上下載頻寬用於所有的協議
- **IP/Mask:** 針對特定的一個網段做頻寬的限制
- **IP Range:** 針對一個區間的 IP 位址做頻寬的限制
- **Port:** 針對特定的網路服務(Port)做頻寬的限制,(如 20,21 port 等等)
- **SIP:** 針對 Session Initiation Protocol (SIP)做頻寬的限制
- **RTSP/RTP:** 針對 Streaming 做頻寬限制
- **WEB:** 針對所有網站做頻寬的限制

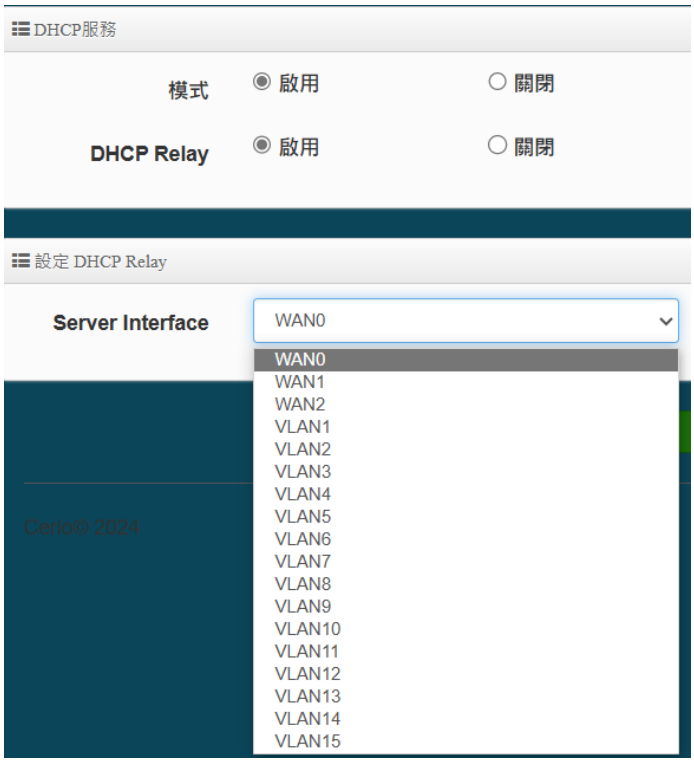
3.3.3 DHCP 伺服器設定(下拉式功能)

點擊 

下拉式按鈕設定 DHCP 伺服器。



- **模式**：管理員可以選擇啟用或關閉 DHCP 伺服器功能。
- **DHCP Relay**：管理員可以選擇啟用或關閉 DHCP Relay 功能。



- **Server Interface:** 此功能可以選擇要 DHCP Relay 跟隨介面，可以選擇開啟的 WAN0~2 介面，或選擇其他 VLAN 介面 VLAN1~VLAN15 的 DHCP 設定.

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

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。

固定 IP 設定

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，此 MAC Address 綁定 IP 位址的功能最大可綁定設定 100 組設定。

固定 IP 列表

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

3.4網頁認證功能(熱點認證)

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

請點選”**系統設定”➔＂網頁認證功能＂**

點擊”**網頁認證功能**”後，將顯示認證列表,如下圖範例，此認證列表將對應不同的(虛擬網路(VLAN)，在不同的 VLAN 下可設定不同的認證方式

Notice

當預想要啟用網頁認證功能時，請務必要確認 WAN 是否能確實上網，假若無法連線至網路則網頁認證功能將無法正常運作

- **虛擬網路服務:** 顯示目前已啟用的虛擬網路服務。(可參照" 3.3 虛擬網路設定")
- **網頁認證功能:** 顯示每個虛擬網路服務是否開啟網頁認證功能
- **執行:** 可點擊按鈕進入啟用或關閉及設定相關網頁認證功能

Notice

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

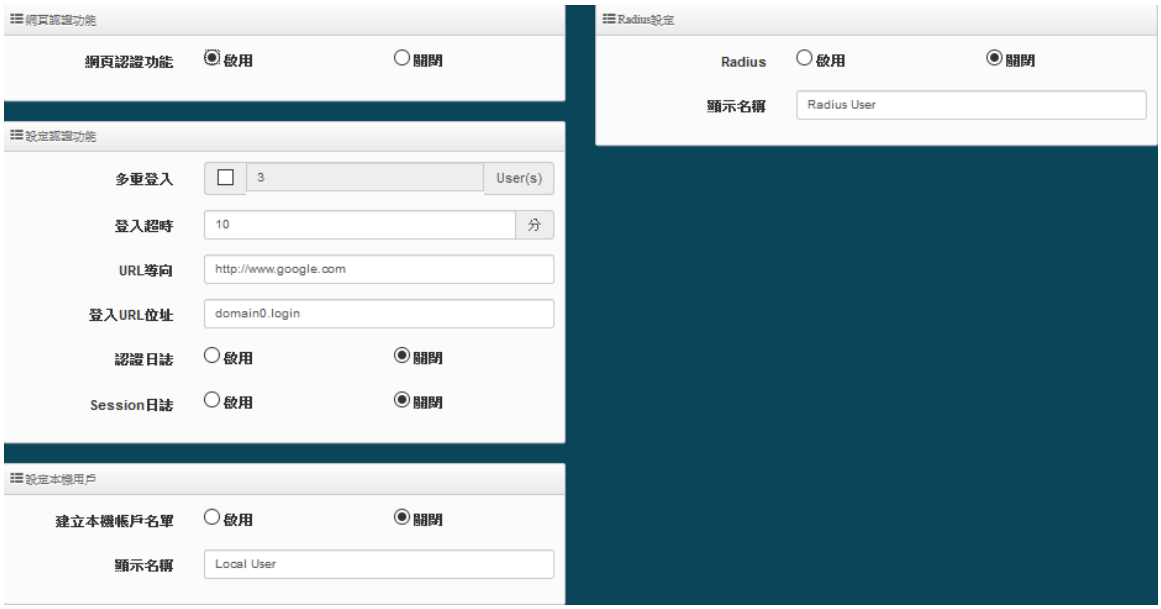
※ **以下說明認證功能操作方式**

3.4.1 啟動網頁認證功能

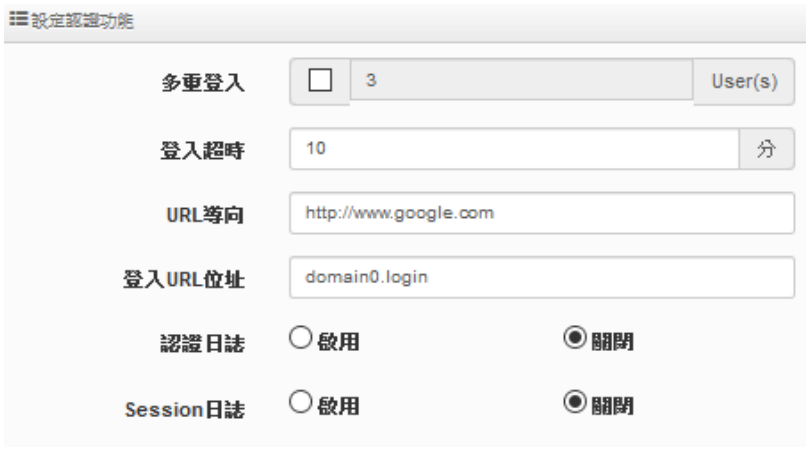
主要能設定啟用認證功能服務及認證方式，同時可設定頻寬控制等相關功能

請點擊 網頁認證功能 按鈕進入設定頁面

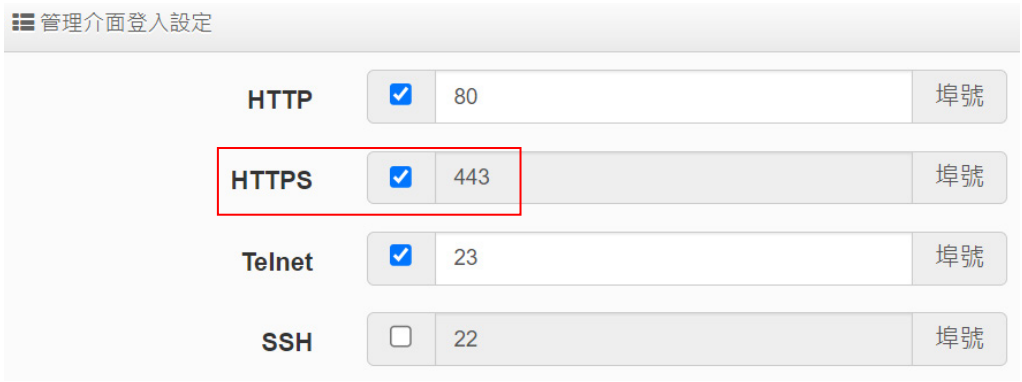
- **網頁認證功能：**可選擇" **啟用**" 或" **關閉**" 認證服務。
  當點擊啟用，則如下頁面操作說明

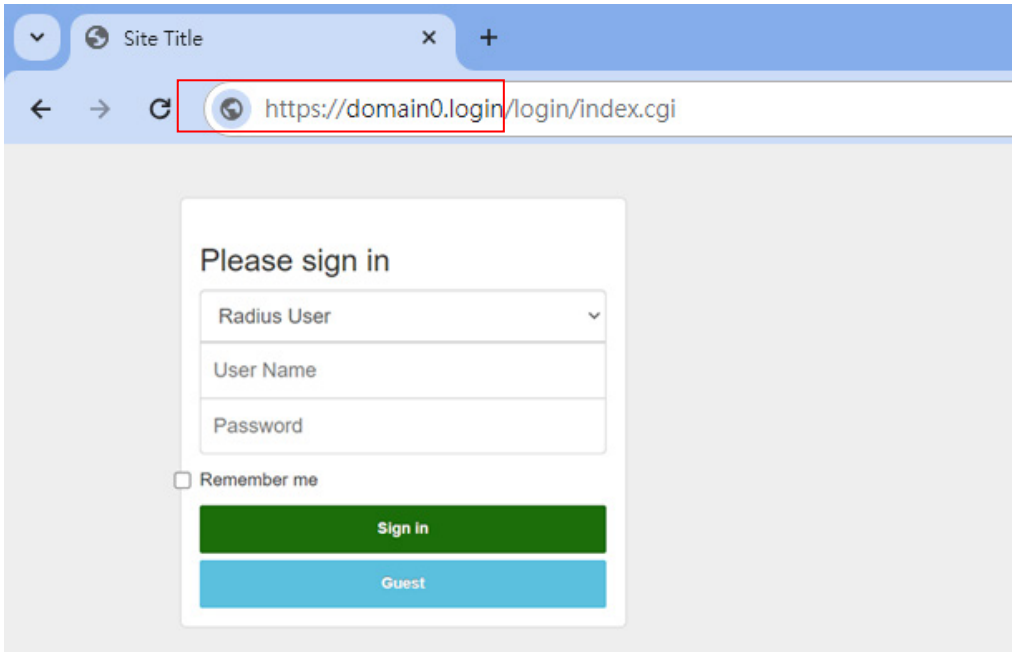


※ 設定認證功能



- **多重登入：**當勾選啟用此功能，則同一個帳號能給多人同時登入，同時登入人數可由管理者自行設定，0 為不限制。
- **登入超時：**當使用者登入後，無進行任何網路行為，無任何流量下，停滯幾分後系統自動讓使用者登出。(預設值為 10 分鐘，可填入 0-720 分鐘，0 為無限制)
- **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 3.13 系統管理➔管理介面登入設定 ，或如下圖示提示**





- **認證日誌:** 可選擇啟用或關閉，啟用可將使用者的認證資訊存放至本裝置的 SysLog 伺服器上。
- **Session Log**：可選擇啟用或關閉，啟用可將使用者的上網 Session 資訊存放至至本裝置的 SysLog 伺服器上。

Notice

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

※ 設定本機用戶

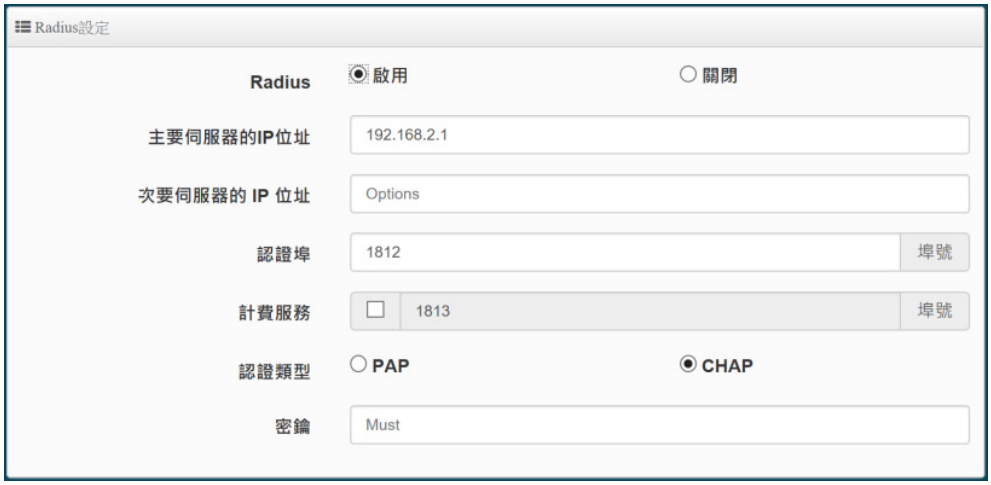
- **本機帳號**：可選擇" **啟用**" 或" **關閉**" 使用本機帳號認證登入。

Notice

當啟用本機帳號後，請務必至 " **本機帳戶** " 功能選單去建立認證用戶帳密。請參考 3.4.2 **認證功能設定➔本機帳戶**。

※ RADIUS 設定

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



- **Radius**：可設定”**啟用**”或”**關閉**”此認證服務。
- **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。

3.4.2 認證功能設定

請點擊 

下拉功能選單，可設定提供給”遊客”使用、本機帳號、OAuth2.0 認證、PoP3/IMAP 協定認證、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。

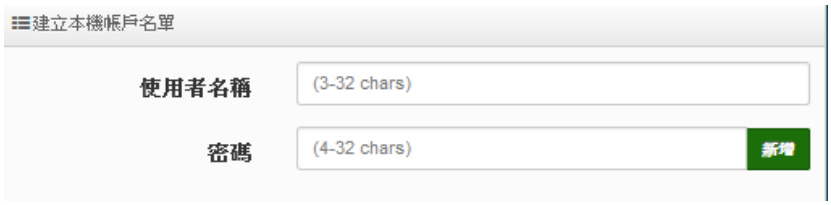
[遊客]認證

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

- **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，從遊客登入開始計算時間，就算遊客在時間內登出，系統時間依然計算。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有 10 分鐘的上網時間，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。
- **計數限制**：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。

[本機帳戶]認證

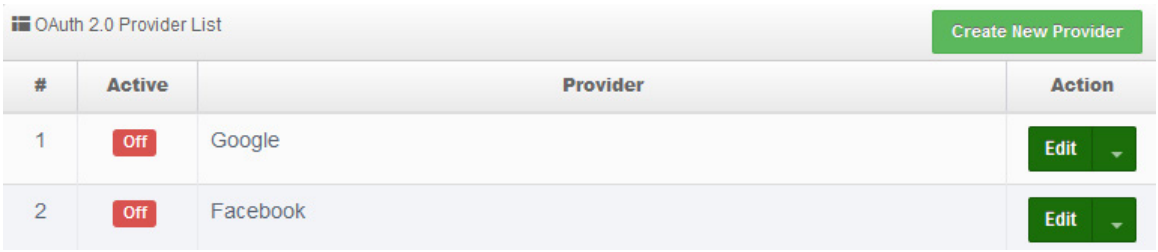
可在本機上建立網頁認證的登入帳密，最多 10 筆資料。



- **使用者名稱**：輸入使用者帳戶名稱。
- **密碼：輸入使用者的帳戶密碼。**
- **本機用戶列表**：將顯示所建立的所有帳戶帳號。

[OAuth2.0]認證

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。



-> [Google]認證程序

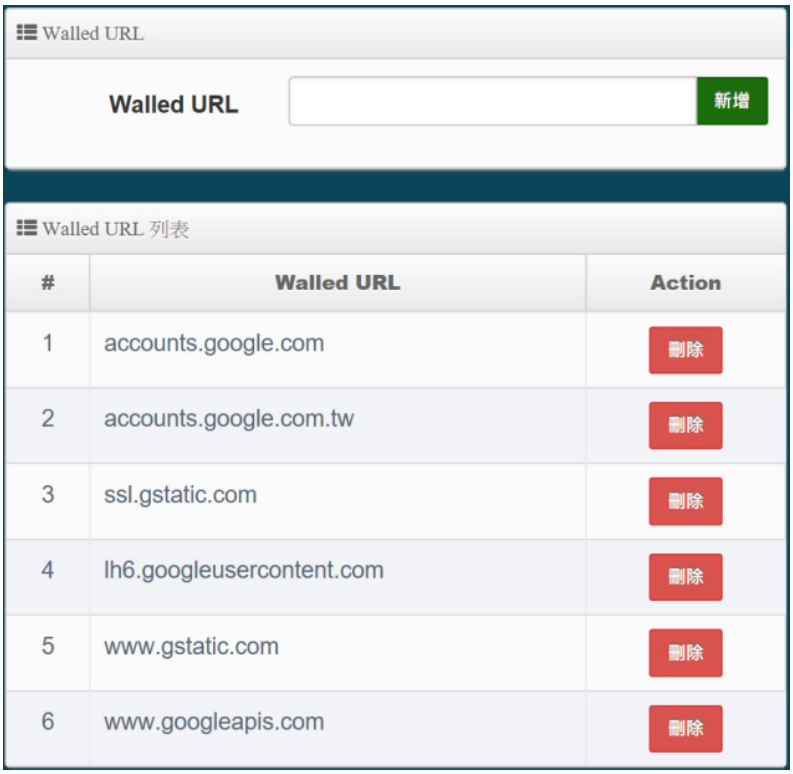
➢ **Edit:** 設定 google 的帳戶

Notice	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。

- **用戶端 ID:** 輸入 Google 的帳戶
- **用戶端密碼:** 輸入 Google 的帳戶密碼
- **進階:** 此按鈕將設定第 3 方認證伺服器的路徑及相關範圍

Notice	在系統上進階的認證路徑範圍在預設已經設定完成 Google 和 Facebook, 管理者無須再去變動它, 若要加入其他第三方認證, 再參考其他第三方的 OAuth2.0 設定資訊

以下資訊為 Pass 網站入口位置, 此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 OAuth2.0 則無需再設定。



Google 的 OAuth2.0 設定服務頁面相關程序說明

Notice	以下流程有可能變動, 須以第三方伺服器說明為主, 本章節僅供參考

1. **請登入至 google 的 API 管理介面去建立一個 OAuth 用戶端 ID, 可參考以下申請網址**
   https://accounts.google.com

2. 選擇網路應用程式

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

Notice

管理者必須確定 Google Developers 的 **"Redirect URI"** 和 **"JavaScript ORGINS"** 的位址必須與系統的 Login URL 所設定的 **"JavaScript ORGINS"** 要一樣才能正常運作

請確認 **3.4.1 啟動網頁認證功能的" 設定認證功能欄位"** 設定登入 URL 位址

將所設定的**登入 URL 位址複製到 Google 的 JavaScript ORGINS 欄位**

http://domain0.login.com/login/callback.cgi 請複製到 Google 的**已授權的重新導向 URI 的欄位**

例如: 在 Google 的帳戶認證設定頁面下，設定如下位址

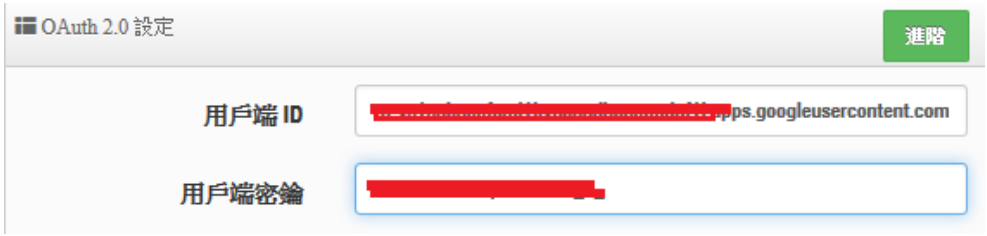
JavaScript ORGINS: http://domain0.login.com

已授權的重新導向 URI :

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

4. **確認申請完成後, Google 將給予一組 ID 與密鑰**

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



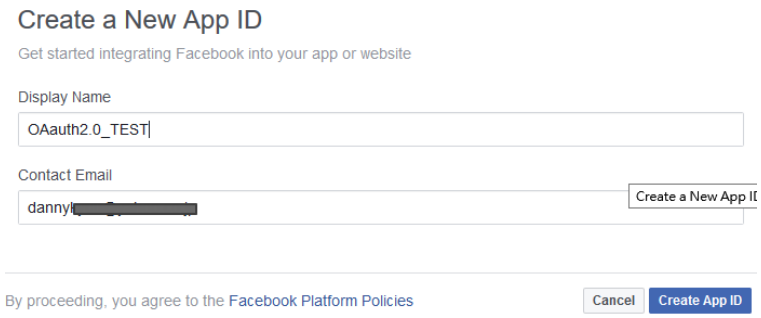
-> [Facebook]認證程序

Notice	管理者需先至 Facebook 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。

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

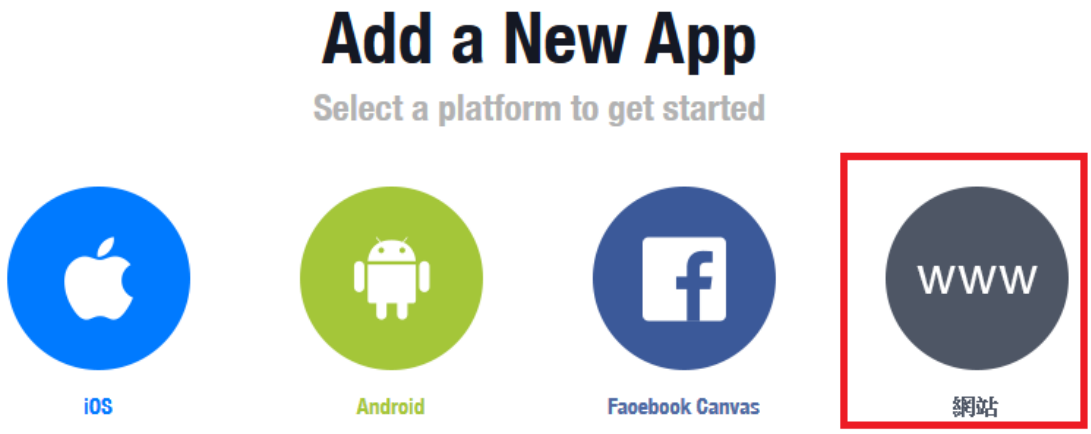
https://developers.facebook.com

Notice	以下流程有可能變動，須以第三方伺服器說明為主，本章節僅供參考

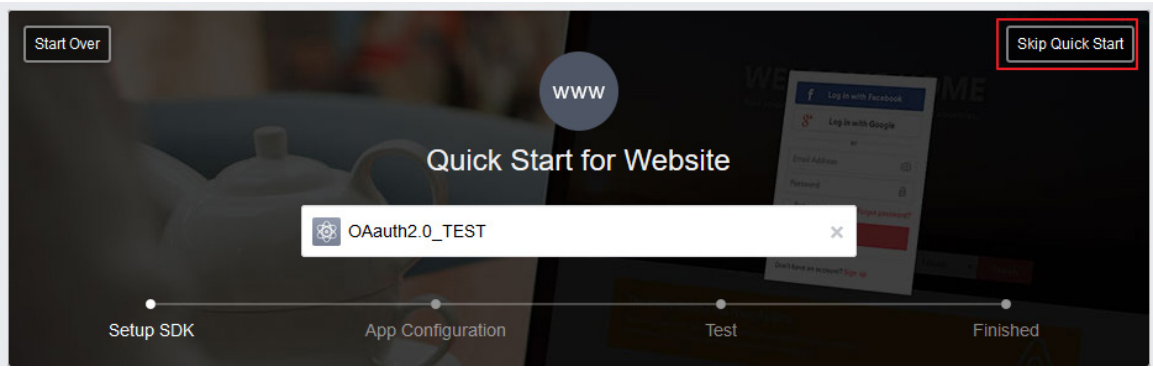


2. 申請確認後可在右下角選擇應用程式的平台

3. 設定此應用程式屬性，為 WWW 網站



4. 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



5. 回設定主頁, 點擊設定進入去設定基本資料

在應用程式網域輸入 3.4.1 啟動網頁認證功能下的 URL 導向, 建議使用 xxxx.xxx.com 網址

例如 danny.tast-login.com

在網站網址請輸入: http:// danny.tast-login.com/login/callback.cgi

如下圖描述

6. 回設定主頁, 點擊應用程式審查進入啟用對外公開上線

7. 回設定主頁, 點擊新增產品並在右邊找 Facebook 登入

8. Facebook 登入設定

啟用”用戶 OAuth 登入”及”網路 OAuth 登入”

設定完成後即可使用 Facebook 的 OAuth2.0 方式進行網頁認證

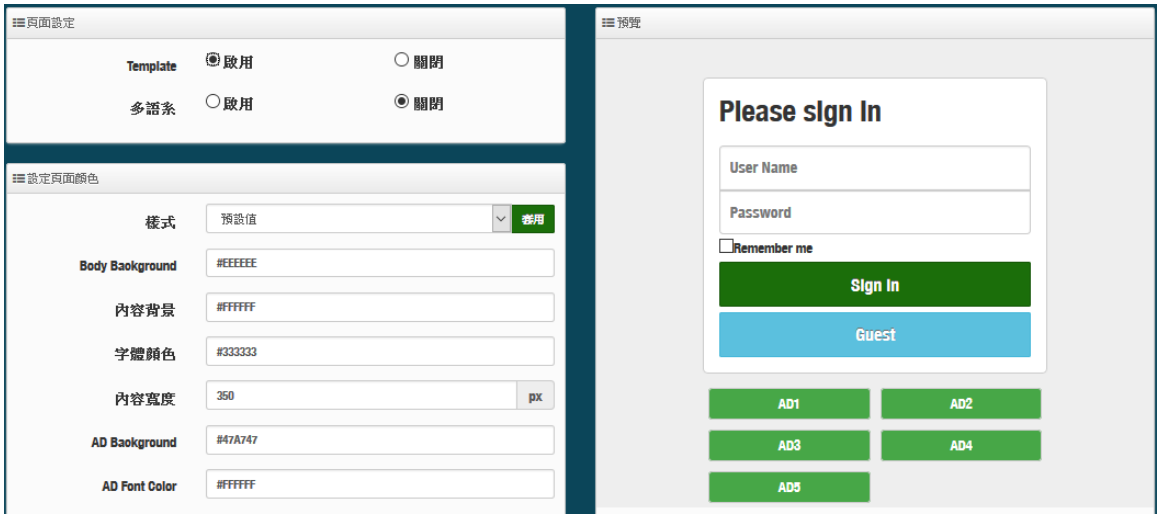
[POP3 /IMAP Server]認證

網頁認證方式支援遠端 POP3 帳戶認證，此功能認證啟用可以將網頁認證的帳戶指向 POP3 伺服器，由現有的 POP3 伺服器內的帳戶資料做網頁登入認證使用。

- **服務**：可”啟動”或”關閉”POP3 Server 帳戶認證功能服務。
- **顯示名稱**：輸入所想要顯示的名稱。
- **Host**：POP3 伺服器的網址或 IP 位址。
- **埠號**：POP3 伺服器所使用的服務埠號碼。
- **連線類型**：選擇 POP3 伺服器的連結類型 STARTTLS 或 SSL/TTL 或 None。
- **POP3 伺服器測試**：可以輸入一組電子郵件帳號及密碼來測試 POP3 伺服器設定是否正確。

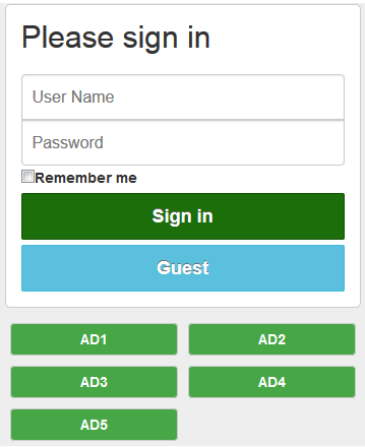
[客製化頁面] 功能編輯

這功能主要可以編輯認證的網頁登入頁面。可以自行編輯去支援多國語系，也可以透過 HTML 和 CSS 語法讓使用者自行編輯認證的登入頁面。



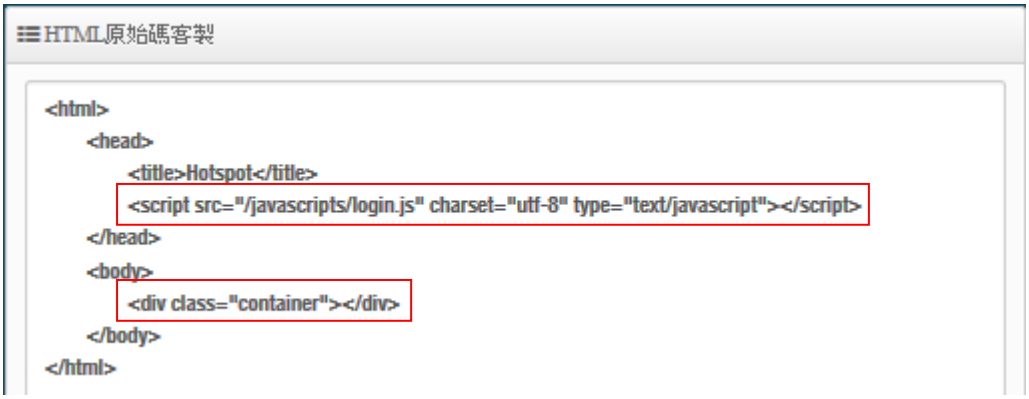
- **Template**：管理人員可選擇 Template(範本)啟用或關閉，啟用時可套用系統預設版面進行顏色修訂，若選擇關閉則可透過 html 語法做編輯。

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



管理者可透過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

確認編輯完成後，請點擊”**儲存**”按鈕後即可點擊”**預覽**”按鈕”進行預覽所編輯的網頁如下編輯完成後的示意圖

Notice

1. 若在 Login 欲想崁入遠端 web 伺服器的圖檔或其他相關資訊，請在系統的 **Walled Garden** 功能去增加 web 伺服器 IP 位址

[語系] 功能編輯

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

➢ 建立新的語系：點擊此按鈕可新增不同的語言顯示，如下說明

語言設定比對參考說明

如圖完成後所呈現畫面

[Walled Garden] 功能編輯

此功能是設定開放使用網站，若有開啟網頁認證登入功能如(3.4.1 啟用認證功能)時，則無線連接的使用者還未登入認證頁面前，所有的使用者都可以使用此 Walled Garden 功能所設定的網站。

- **顯示名稱：**設定要辨識的網站名稱。
- **IP 網址/網域：**設定網站的 IP 位址或網站的網址。
- **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。

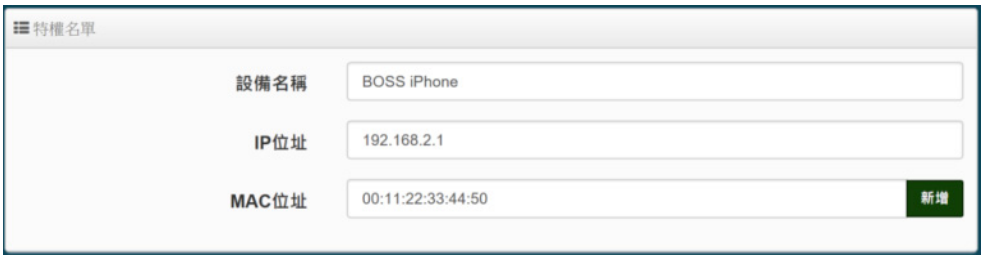
表單內最多可建置 10 筆網站名單。

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

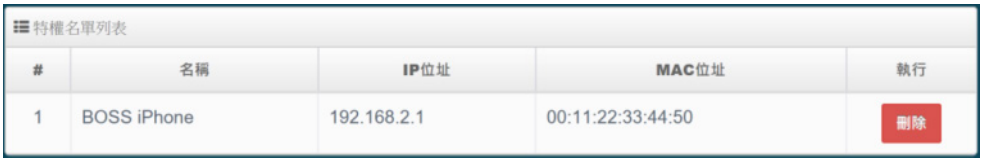
[特權名單] 功能編輯

此特權名單功能主要是當開啟網頁認證功能後，所有的有線網路使用者連接 DR-4000 後都必須透過網頁認證方可使用網路，而在此特權名單內綁定 IP/MAC 位置的設備則不需經過網頁認證就能自由

的使用上網服務。



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



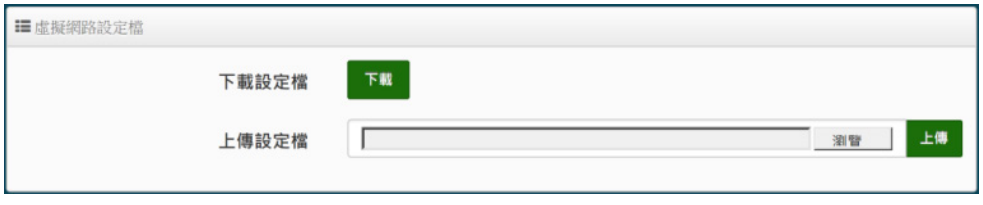
按下新增後，將所設定的網站列入表單內。

表單內最多可建置 10 筆網站名單。

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

[設定檔] 功能

此功能主要能將以設定好的 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。



3.5 High Availability

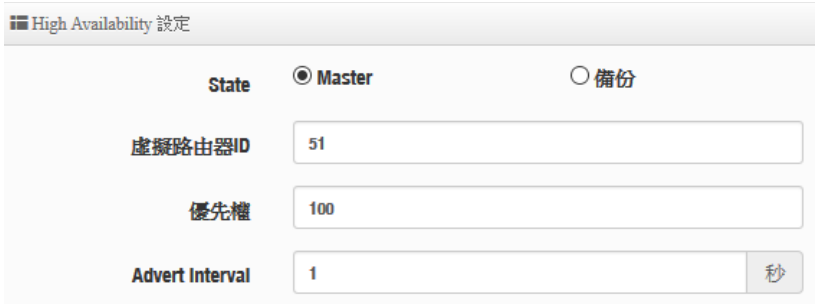
當頭端 DR-5000 設備在網路環境因不明原因導致停止工作時，則所有網絡將無法正常上網工作。如果管理員設置的高可用性功能(HA)系統備援機制，則將能夠避免網絡的意外中斷，防止使用端無法使用網路。

此 HA 功能主要能在同一個環境下架設多台的 DR-5000 做備援機制，HA 的機制主要能即時互相備援 DR-5000 的設定檔資料，當主要的 DR-5000 因不明原因導致停止工作則 HA 機制能在第一時間內啟動備援設備銜接，不會讓整個網路停止服務。

請點擊 **“系統設定”** ➔ **“High Availability”** 進入設定 HA 管理功能.

- **服務:** 管理員可以選擇啟用或停用此服務。

High Availability Setup

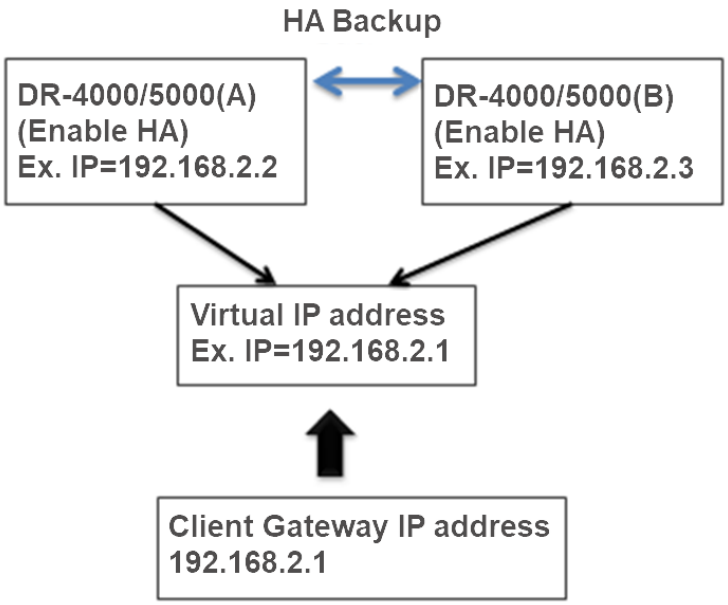


- **State:** 管理員可以選擇指定此 DR-5000 的 HA 是屬於主要的運作還是備份。
- **虛擬路由器 ID:** 管理員必須設定每一台 DR-5000 所有 HA 設備中使用相同的虛擬路由器 ID
- **優先權:** 設定優先權等級
- **Advert Interval:** 當主要的 HA 故障後，經過多少秒後回復。

設定虛擬 IP: 管理員可以在不同的 VLAN 中設置 HA 功能。請點擊” 編輯” 按鈕進入設定。

- **Virtual IP:** HA 機制中，必須先設置一組共用的虛擬閘道 IP 位址，透過此虛擬的閘道位址後系統將自動判斷主要與次要的 DR-5000 設備, 如下圖說明

(The following concepts)

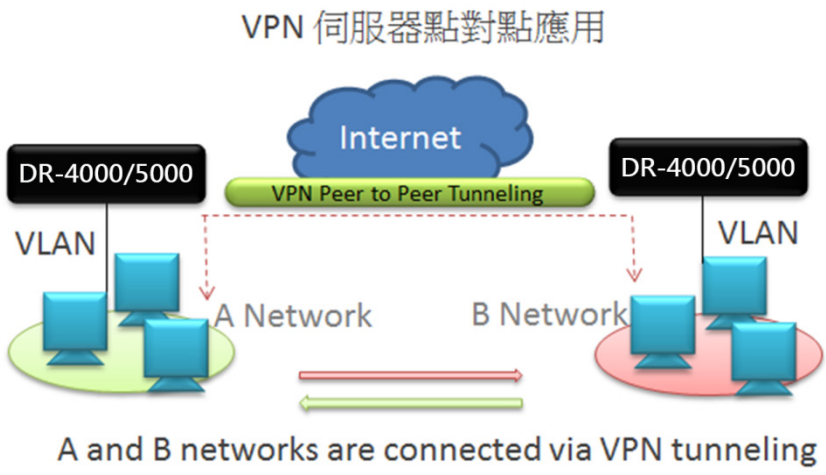


- **認證類型:** 管理員可以選擇 PASS 或 AH 的安全加密方式來保護虛擬閘道位址。
- **密碼:** 設置此虛擬閘道的安全保護密碼。

3.6 VPN 伺服器設定

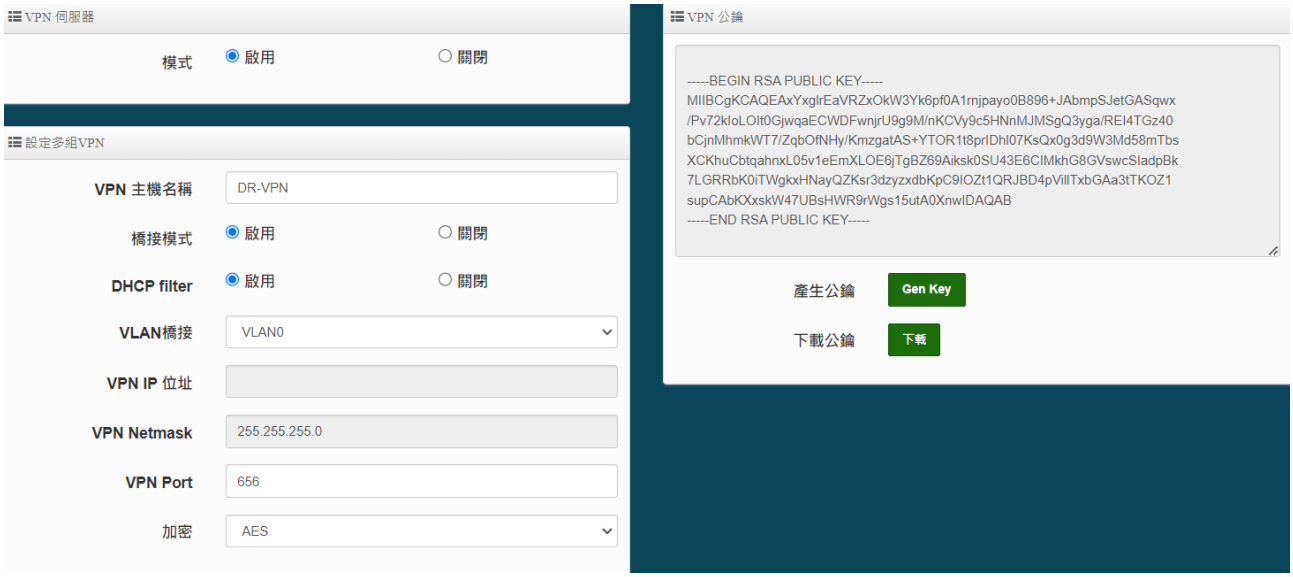
Notice	**VPN 伺服器、PPTP/L2TP 以及 IPsec 的 VPN 通道等多種 VPN 模式無法同時啟用，整台 VPN 只能擇一模式啟用 VPN,若使用 VPN 伺服器連線，則須關閉 PPTP/L2TPD 和 IPsec 通道連線**

主要應用在 VPN P2P 點對點連接，請點擊 **“系統設定”➔”VPN 伺服器設定”** 建置 VPN 通道



VPN 服務

➢ **模式:** 管理員可以選擇啟用或關閉 VPN 服務。



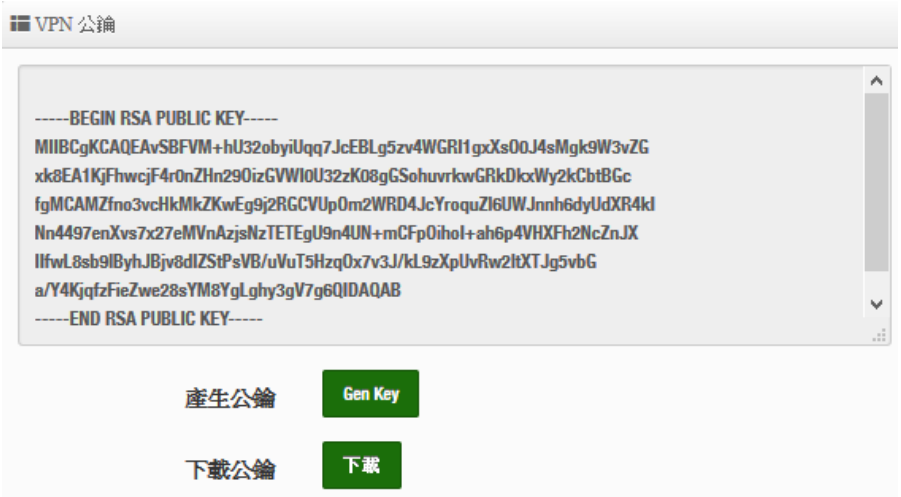
設定多組 VPN

- **VPN 主機名稱:** 管理人員可以設定 VPN 的名稱
- **橋接模式:** 管理人員可以啟用去選擇使用 VLAN# 作 VPN 通道，或者是關閉採用手動建立 VPN 的 IP 位址通道。
- **DHCP filter : 可以選擇啟用或關閉,開啟時可以避免兩端實體區網的 DHCP Server IP 互相越界派發 IP 的產生。**(只需單邊啟用此一功能. **若兩端皆開啟 DHCP filter 時將會導致網路邏輯錯誤無法 VPN 成功連線**)
- **VLAN 橋接:** 如果橋接模式選擇啟用，則可在此欄位選擇要使用哪個 VLAN 作 VPN 通道。
- **VPN IP 位址/Netmask:**假如橋接模式選擇關閉可手動輸入本機 VLAN 的 IP 位址及 IP 遮罩
- **VPN Port:** 設置 VPN 使用的連接埠。
- Encryption: 設定 VPN 加密方式, 支援 blowfish , AES 及 3DES 等, 建議可以選擇使用 AES

Notice	1. 假如選擇使用 VLAN 橋接模式, 則 VPN 兩端的 network VLAN 網段需相同 2. 若 VPN 兩端的 VLAN 網段不同, 則建議關閉 VLAN 橋接模式, 改為手動設定 IP 位址, 並手動設定 VPN IP 的路由

VPN 公鑰

系統將可透過此功能生成此端點的VPN 憑證公鑰, 若建置 VPN 點對點通道, 則兩端點的公鑰須交換確認



- **產生公鑰:** 管理員可以點擊” Gen Key” 按鈕來產生新的 VPN 公鑰。
- **下載公鑰:** 可點擊” 下載” 按鈕將 VPN 的公鑰下載存放至 PC。

3.7 設定 VPN Peer

Notice	**當 3.6 VPN 伺服器設定完成後，則須在此功能頁面設定另外一端的真實 IP 位址以及上傳公鑰憑證**

此功能為 Peer to Peer 端點 VPN 通道連接，主要將兩端點的資訊互設即可，管理員可以在 VPN Peer 功能建置 VPN 連接。

請點擊 “**系統設定**” ➔” 設定 **VPN Peer**”

進入後請點擊**建立新的 Peer** 按鈕進入設定 Peer 條件，最大可建置 20 組 VPN Peer 設定。

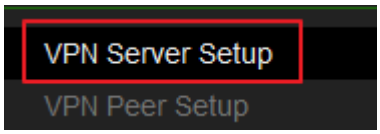
- **模式:** 選擇啟用或關閉 Client VPN 功能。
- **HostName:** 設定遠端的 VPN 主機的名稱，注意兩端點的主機名稱不可一樣。
- **真實 IP/Domain:** 設定遠端 VPN 主機的真實 IP 位址或可被解析過後的 Domain 網址位址。。
- **VPN Port:** 設定 VPN 主機的使用埠，需一致。
- **Description:** 可設定此 VPN 連接的描述。(此部份可以選擇性填入設定，將不影響 VPN 連線設定)

設定程序基本說明

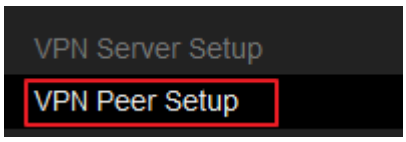
以 A 和 B 兩端點做範例, 注意當建置兩端 VPN Peer to peer 時, 兩端的網域需相同且 IP 位址不可重複

1. 設定 A 端的 VPN Server, 並將 VPN Public Key 下載儲存, 待上傳給 B 端點認證, B 端點的 VPN

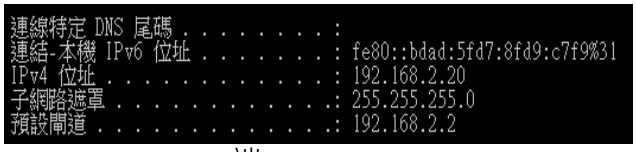
Server 也是如此



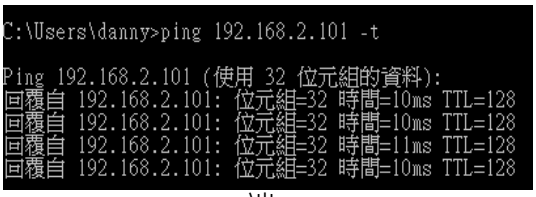
2. 在設定 VPN Peer，此頁面主要是建立遠端的 VPN Server 資訊，並將遠端的 Public Key 上傳至此



3. 建置完成後，可透過 Ping 指令確認 A 和 B 兩端的區網是可以互相得到回應，如下圖示，由 A 端點的區域網路去 Ping 到 B 端的區域網路的 IP 位址是可互相回應



A 端



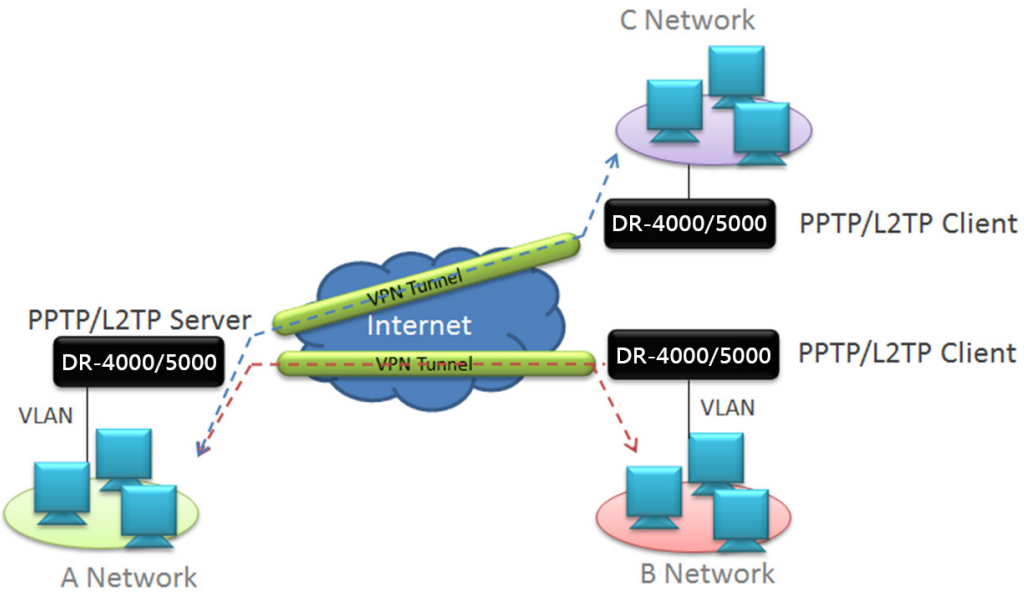
B 端

4. **請特別注意,兩邊最終 VPN 伺服器與 VPN Peer 設定的各別 Client 設置，都必須啟用讓 VPN Peer 連線成功。**
5. 貼心提醒您，請妥善設定啟用 DHCP filter 功能，可以**針對環境開啟使用 DHCP Server 派發 IP 時，避免兩端實體區網互相越界派發 IP 導致取得的 IP 並非真實本地端之 DHCP Server 派發 IP 造成之後無法正常上網，您必須兩端擇一開啟過濾阻擋非本地 DHCP Server 派發 IP 來避免越界派發，此部分請特別注意不要兩端皆開啟此一功能，若兩端皆開啟 DHCP filter 時將會導致網路邏輯錯誤無法 VPN 成功連線。**

3.8 PPTP 伺服器設定

Notice	**VPN 伺服器、PPTP/L2TP 以及 IPsec 的 VPN 通道設定只能啟用一種模式，若建置 PPTP/L2TP 的 VPN 連線，則須關閉 VPN 伺服器和 IPsec 通道連線**

建置 VPN 通道使用 PPTP Server 方式，讓遠端使用 PPTP Client 透過 VPN 通道連接



此功能的 VPN 建置方式採用 Server 與 Client 方式連接

請點擊 “系統設定” ➔” **PPTP Server 設定**”

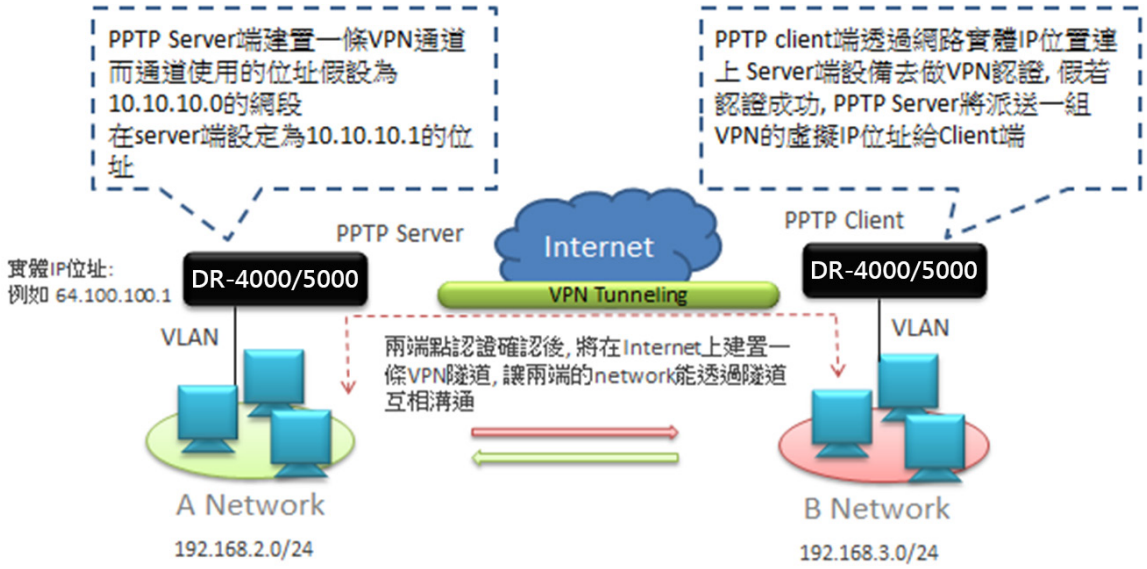
- **Connections**: 設定 VPN Client 的連線數
- **本地端 IP 位址**: 設定一組本地端的虛擬 VPN IP 位址

Notice **此 IP 位址設定為 VPN 使用的虛擬 IP 通道，請勿與 WAN IP 和 Network IP 相同網段**

- **Remote Start IP Address**: 設定 IP 的起始位址，要給 VPN Client 端點自動取得
- **Remote End IP Address**: 設定 IP 的結束位址
- **MPPE40/128**: 可選擇要求加密使用 40 或 128 bit.
-

如下設定範例:

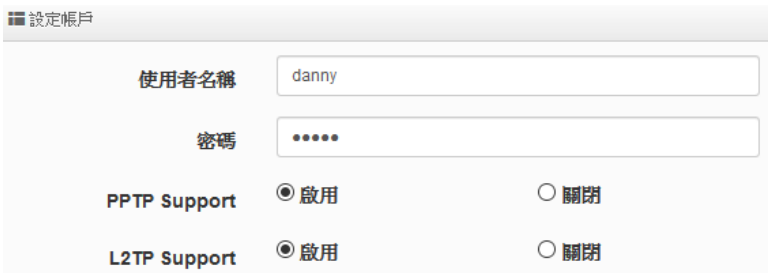
建立 VPN 通道使用 PPTP Server 與 Client 座橋接,假設 Server IP 使用 10.10.10.1，而 Client 端則自動派送 IP 位址，由 10.10.10.10~15 的位址. 概念圖如下



PPTP Server 端

1. 啟用 PPTP Server 並進入頁面設定, 參考以上應用圖, 如下設定

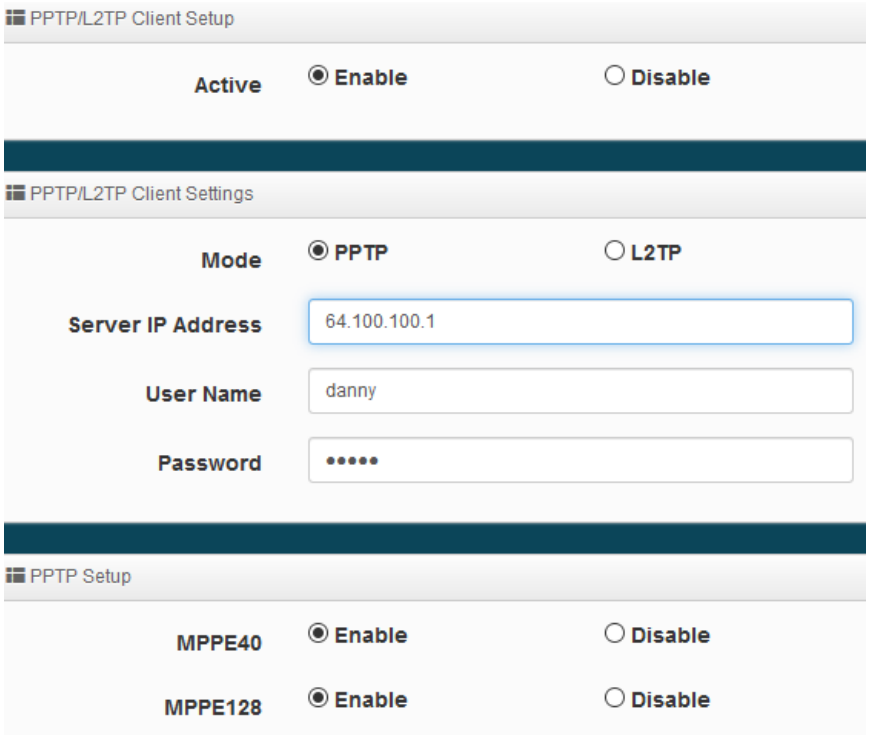
2. 建置 Client 認證帳戶



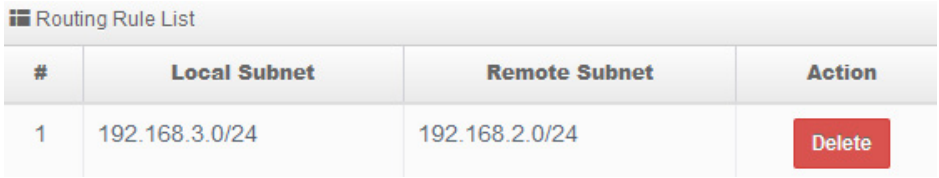
設定兩端的 network 路由網段

PPTP Client 端

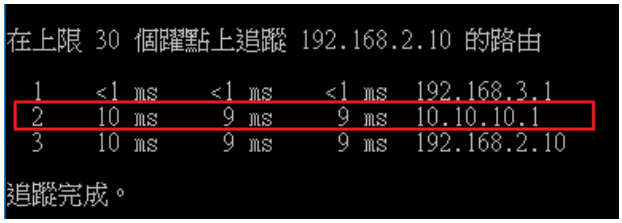
1. 在 Client 端設定 Server 端的實體 IP 位址，並設置認證帳戶及密碼



2. 設置兩端的 network 路由



設定完後即可完成 VPN 通道連線，可追蹤路由，將發現兩端是走 VPN 的虛擬 IP 通道



注意: 以上圖示為了建置手冊之範例，所以當追蹤路由時 VPN 通道刻意顯示出來，而實際狀況 VPN 通道將會是隱藏不顯示追蹤資訊

3.9 L2TP 伺服器設定

Notice

VPN 伺服器、PPTP/L2TP 以及 IPsec 的 VPN 通道設定只能啟用一種模式,
若建置 PPTP/L2TP 的 VPN 連線, 則須關閉 VPN 伺服器和 IPsec 通道連線

同 PPTP 伺服器運作概念, 而此 VPN 連線建置主要採用的是 L2TP 協定, 設定應用範例可參考 PPTP 的設定範例

請點擊 "系統設定" ➔" **L2TP Server 設定**"

- **本地端 IP 位址:** 設定一組本地端的虛擬 VPN IP 位址

Notice

此 IP 位址設定為 VPN 使用的虛擬 IP 通道, 請勿與 WAN IP 和 Network IP 相同網段

- **Remote Start IP Address:** 設定 IP 的起始位址, 要給 VPN Client 端點自動取得
- **Remote End IP Address:** 設定 IP 的結束位址

是否要透過 IPSec 方式使用 Pre-shared key 並固定 Client 的 IP 位址

- **模式:** 可選擇啟用或關閉此功能
- **Pre-shared key:** 可輸入一組金鑰
- **Client IP:** 設定 Client 端的固定 IP 位址
- **WAN ID:** 選擇使用一個 WAN 端

3.10 PPTPD/L2TPD Account Setup

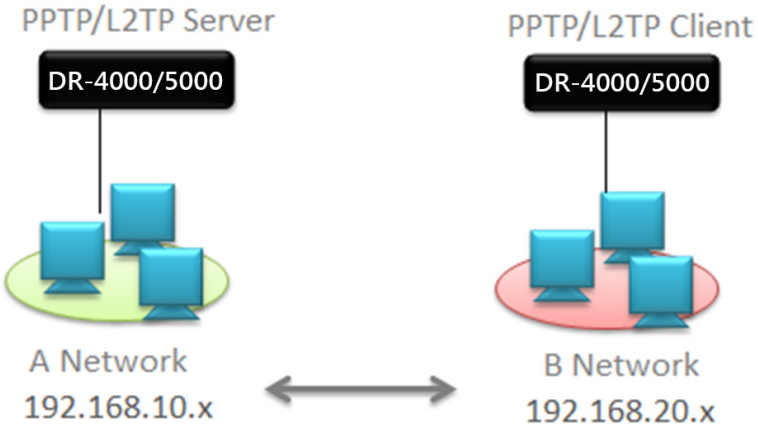
主要建置 PPTP/L2TP 的連接驗證帳戶, 最大可建置 60 筆 VPN 帳戶數

請點擊 “系統設定” ➔” PPTPD/L2TPD Account Setup”

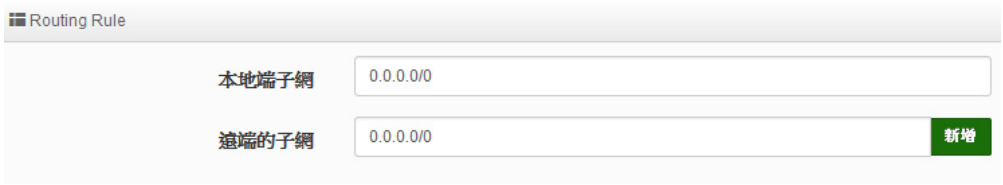
進入後請點擊 Create Account 按鈕建立認證帳戶

- **使用者名稱:** 輸入要建立的 VPN 帳戶
- **密碼:** 輸入 VPN 帳戶的密碼
- **PPTP / L2TP Support:** 選擇 VPN 認證帳戶使用的協定

路由規則： 設定兩個網路的路由，如下圖基本示意圖, 本地端為 Server 端點, 遠端為 Client 端點



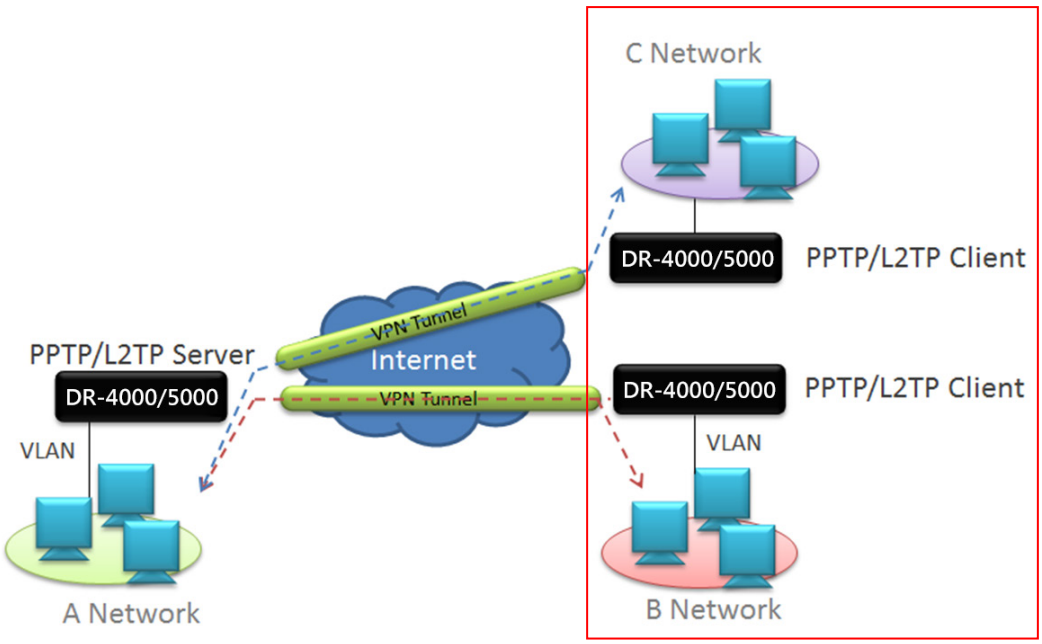
範例:
本地端: 192.168.10.0/24
遠端: 192.168.20.0/24

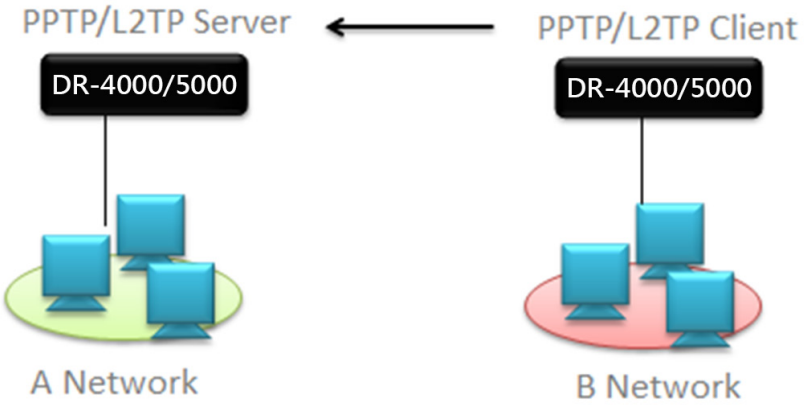


- **本地端子網** ：設定本地網路子網
- **遠端的子網** ：設定遠地網路子網

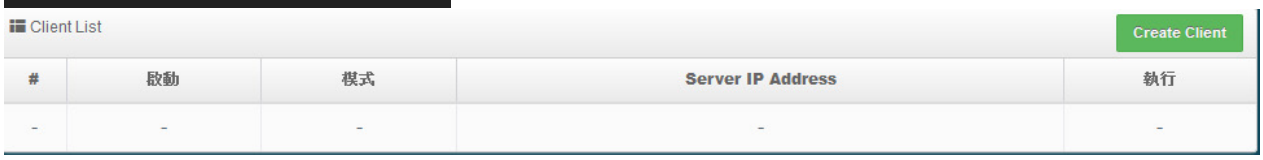
3.11 PPTP/L2TP Client Setup

當上端 VPN 設備使用 PPTP 或 L2TP 伺服器協定時, 若要連接上端 VPN 伺服器則必須啟用 PPTP 或 L2TP 的 Client 模式, 此功能主要是去連接上端的 VPN 是使用 PPTP 或 L2TP 伺服器之應用





請點擊 “系統設定” ➔” PPTPD/L2TPD Client Setup”



進入後請點擊 Create Client 按鈕進入設定 Client 條件，，最大可建置 60 筆 Client 筆數

- **模式:** 選擇上端 VPN 建置使用 PPTP 或 L2TP Server 協定
- **Server IP Address:** 輸入 Server 端的 IP 位址
- **使用者名稱 / 密碼: 輸入** PPTP 或 L2TP Server 所建置的認證帳戶名稱與密碼

假若使用 PPTP 協定，則請選擇加密類型，如下圖

- **MPPE40/128:** 基於使用遠端 VPN 伺服器的安全性選擇啟用或關閉。

假若使用 L2TP 協定，則請輸入 Pre-share Key(金鑰)，並確認使用那個 WAN 對外做 VPN 通道，如下圖

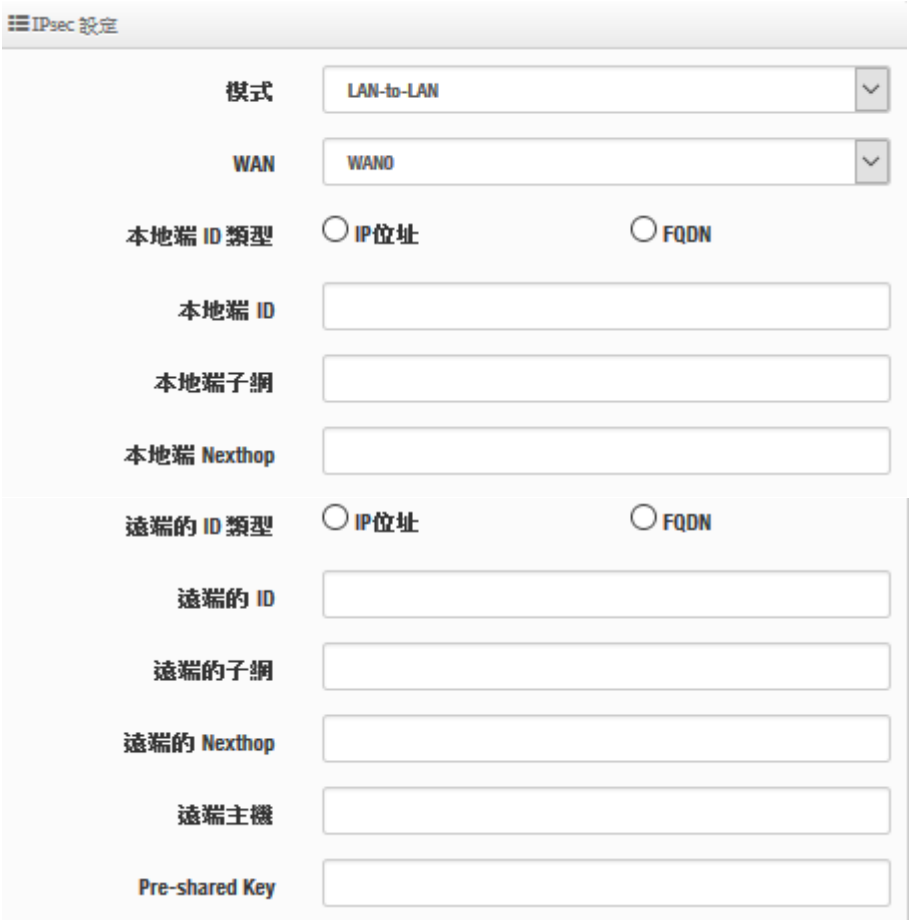
- **Over IPsec :** 選擇啟用或關閉使用 **Over IPsec VPN 協議**。
- **Pre- shared Key :** 可輸入一組金鑰
- **WAN :** 選擇 L2TP VPN 要經過相對 WAN 的使用介面。

3.12 IPSec 設定

Notice	**VPN 伺服器、PPTP/L2TP 以及 IPsec 的 VPN 通道設定只能啟用一種模式， 若建置 PPTP/L2TP 的 VPN 連線，則須關閉 VPN 伺服器和 IPsec 通道連線**

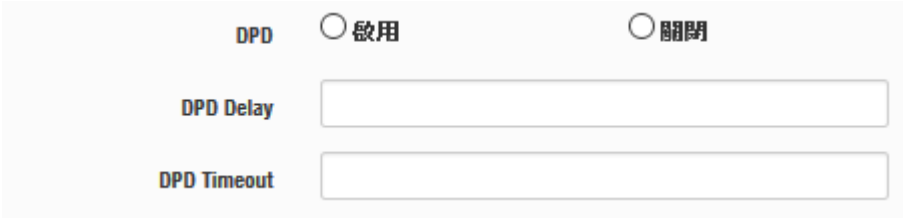
此功能的 VPN 連線將以 LAN to LAN 或是 Client to LAN 的架構模式連接。
請點擊 “系統設定” ➔” **IPSec 設定**”

- **服務:** 可選擇啟用或者關閉此功能服務



- **模式:** 管理人員可以選擇使用 LAN to LAN 方式或是 Client to LAN 方式進行 VPN 通道連線。
- **WAN:** 管理人員可以選擇使用哪個 WAN 端口對外連接 VPN 通道。
- **本地端 ID 類型:** 管理員可以選擇 VPN 通道是使用 IP 方式或是 FQDN 方式進行通道連接。
- **本地端 ID:** 若選擇使用 FQDN 方式連接，則須建立此本機的 ID。
- **本地端子網:** 設定本地端的 IP 子網遮罩，例如 192.168.2.0/24.

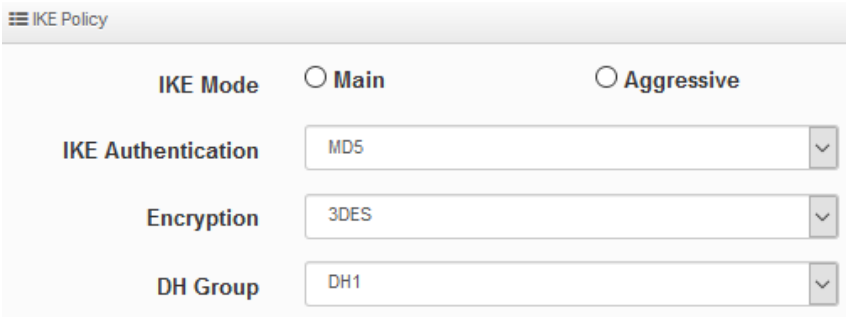
- **本地端 Nexthop:** 若網路架構環境有 2 台 Gateway，可設定本地端的下一個 Gateway 位址，若無，可直接設定 0.0.0.0 即可。
- **遠端 ID 類型:** 選擇設定遠端 VPN 使用 IP 或 FQDN 的類型.
- **遠端的 ID:** 假如使用 FQDN 類型，需在此輸入遠端的 ID。
- **遠端的子網:** 設定遠端的 IP 子網遮罩，例如 192.168.2.0/24.
- **遠端的 Nexthop:** 若遠端網路架構環境有 2 台 Gateway，可設定遠端的下一個 Gateway 位址，若無，可直接設定 0.0.0.0 即可。
- **Pre-shared Key:** 輸入 VPN 連接的 Pre-shared Key 碼。



- **DPD:** DPD (Dead peer detection) 是網絡設備用於驗證遠端 VPN 設備與當前 VPN 主機若一端斷開時可能產生存在的不再自動 VPN 連線的狀態的解決與可用性的方法。DPD 的功能成立必須兩端 VPN 主機皆做了啟用設定始予功能成立，單邊系統可以等待來自遠端固定設的 Delay 時間封包訪問予以給以封包回應來讓主機確保認知雙方皆是存活的正常狀態，當存在設定超過 **Timeout 時間而得不到對向主機回應封包時則主機將可採取 DPD 機制予以自動啟動 VPN 重新連線程序**，此功能預設值開啟，建議管理者使用此功能以避免 VPN 可能的斷開後不再自動複連的可能現象。
- **DPD Delay:** 管理員可以設定遠端 VPN 回應的等待時間。(預設值 30 秒予以封包訪問對向 VPN 主機) 。
- **DPD Timeout:** 管理員可以設定多久時間後超時斷開。(預設值 120 秒時對向主機未按 Delay 設定的訪問對向週期每次正常回應時.即自動啟動 DPD 自動 VPN 連線程序)。

IKE Policy:

此功能主要是驗證身分，在 VPN 要跟對方建立連接則必須要做認證去建立彼此的信任關係，此 IKE 支援 KE Phase 1/2

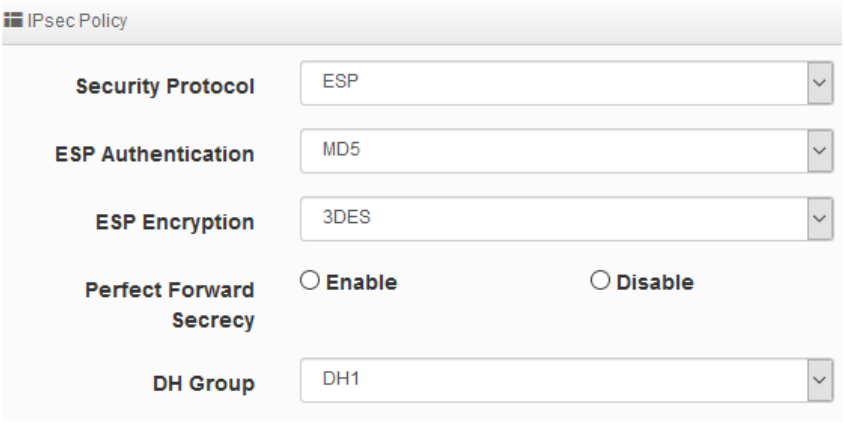


- **IKE Mode:** 可選擇使用 Main 或是 Aggressive 模式，當設備使用路由器則建議採用 Main 主

要模式較安全

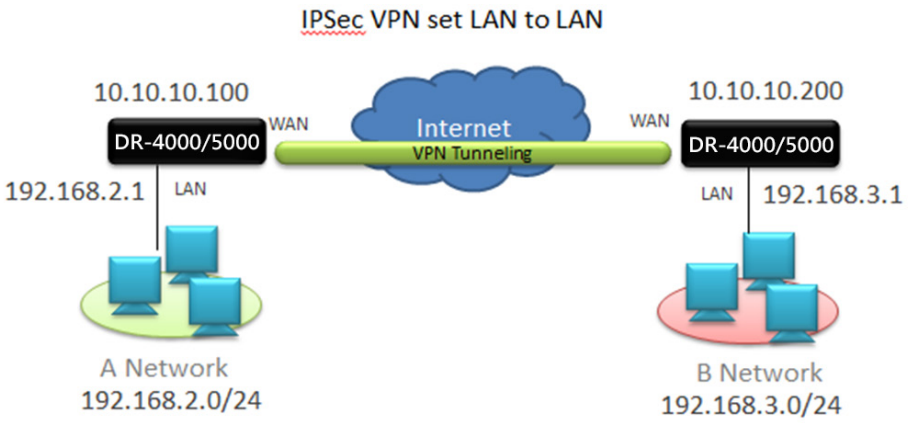
- **IKE Authentication:** 選擇 IKE 的加密演算方法，支援 MD5, SHA1, SHA2_256 等
- **Encryption:** 可選擇加密方式，支援 3DES 及 AES128/192/256
- **DH Group:** Diffie-Hellma 為密鑰的交換，支援 DH1/2/5/14. 此功能主要是讓兩方在完全沒有對方任何資訊的條件下，透過不安全的通道下雙方建立起一個密鑰。

IPSec Policy:

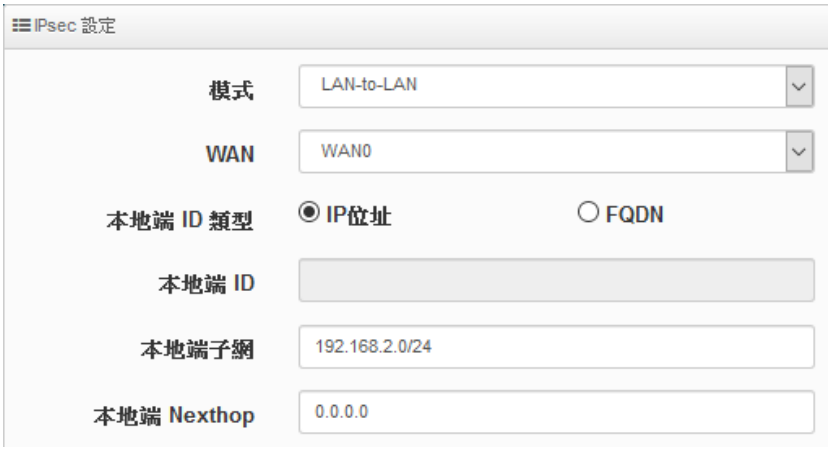


- **Security Protocol:** 可同時提供訊息來源鑑定與資料加密。
- **ESP Authentication:** 選擇 ESP 的加密演算方法，支援 MD5, SHA1, SHA2_256 等
- **ESP Encryption:** 選擇加密方式，支援 3DES 及 AES128/192/256
- **Perfect Forward Secrecy:** 可選擇是否啟用 DH 密鑰交換
- **DH Group:** Diffie-Hellma 為密鑰的交換，支援 DH1/2/5/14. 此功能主要是讓兩方在完全沒有對方任何資訊的條件下，透過不安全的通道下雙方建立起一個密鑰。

基本設定範例:



在 A 端點設置如下



本地端子網設定 192.168.2.0/24，而 Nexthop 可設定 0.0.0.0

遠端的子網須設定 B 端的子網如 192.168.3.0/24，而主機請設置遠端的實體 IP 位置，在 Pre-shared Key 則兩端點需要一致即可

而 IKE 及 IPSec policy 設定只要兩端點的機密類型都一致即可完成

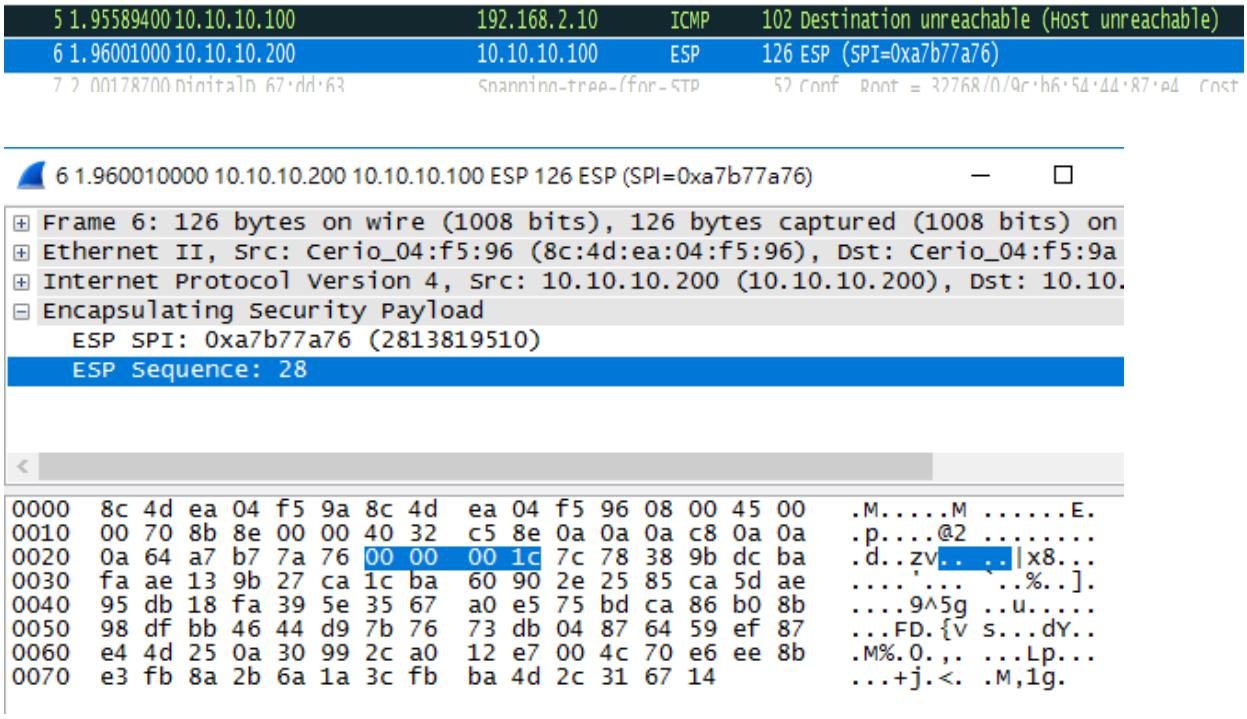
在 B 端點設置只差在本地端與遠端相反其餘都一樣即可完成

以下可看出，兩端點 LAN 已使用 VPN IPSec 連接

從 192.168.3.0/24 網域(B 端點)直接找 192.168.2.0/24(A 端點)的設備，很清楚發現兩端已經透過 VPN 隧道路由成功.

注意: 以上圖示為了建置手冊之範例，所以當追蹤路由時 VPN 通道刻意顯示出來，而實際狀況 VPN 通道將會是隱藏不顯示追蹤資訊

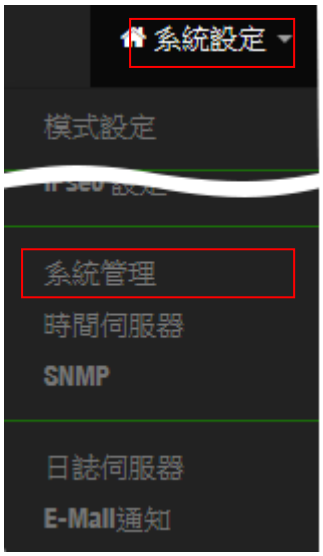
檢查兩端點的封包，將發現已確實被加密，表示 VPN IPSec 以確實完成.

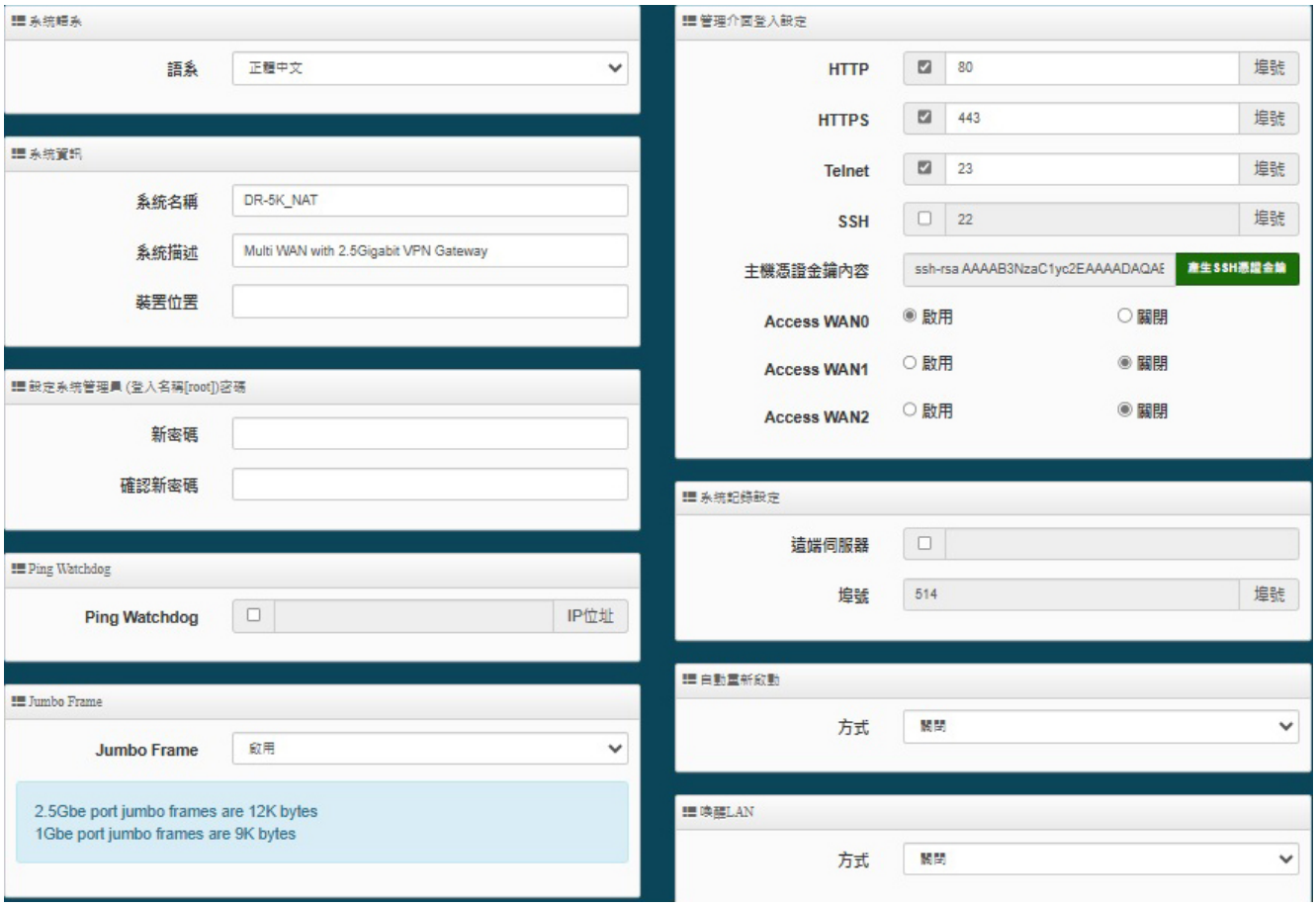


3.13 系統管理

管理員可以通過此管理頁面中設定系統的位置描述等等，並修改系統管理者的登錄密碼，還可選擇使用系統登錄協議 80,443,23,22 端口。在這管理頁面可啟用 syslog 服務器功能和系統自動重啟功能。

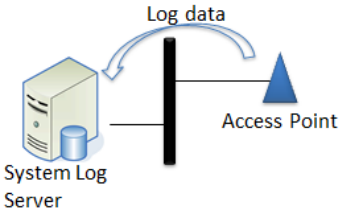
請點擊”**系統設定**”➔”**系統管理**”進入設定頁面



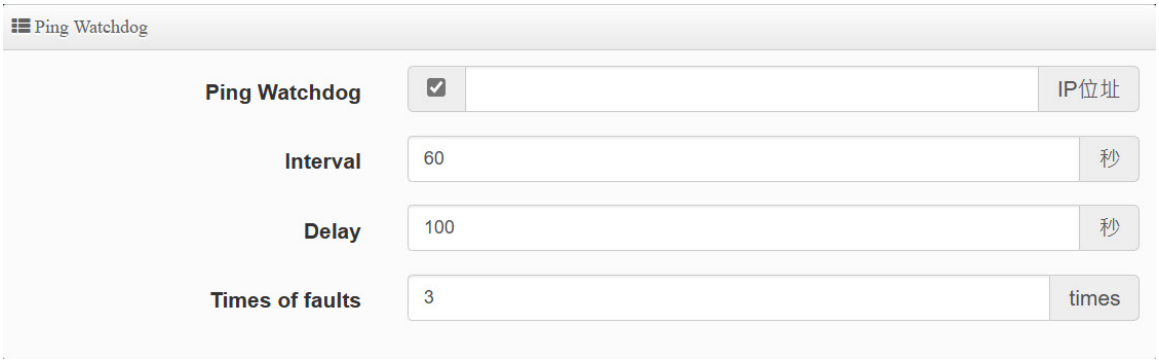


- **系統語系:** 管理員可以選擇更換中文或英文系統的語系.
- **系統資訊:** 管理員可修改此系統的名稱及描述等資訊，讓管理者方便辨識。
- **設定系統管理元登入密碼:** 管理員可以修改登入系統的密碼，預設為 default。
- **系統紀錄設定:** 倘若架構環境中有一台系統紀錄伺服器，此功能可以指向到系統伺服器上，將本機系統資訊往伺服器上備存，方便管理者未來除錯用，此功能主要能將 DR-5000 的 Log 資訊即時備份到 Syslog 伺服器。

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

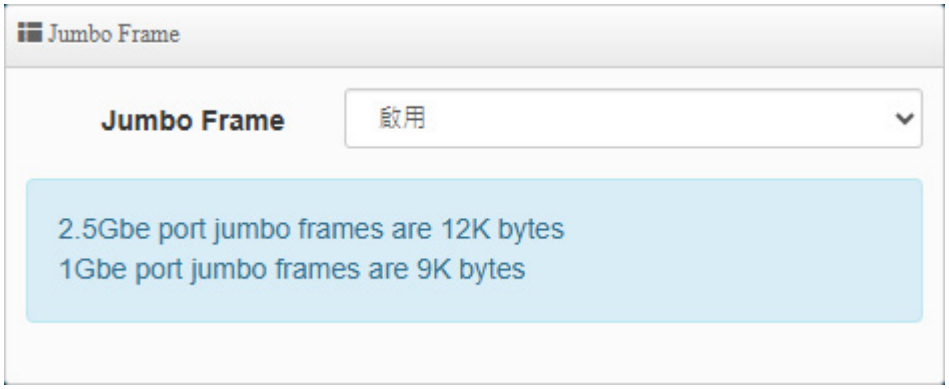


➢ **Ping Watchdog**：可透過設定讓系統自動判斷運作是否正常，若 ping 規則成立，系統自動重啟。.

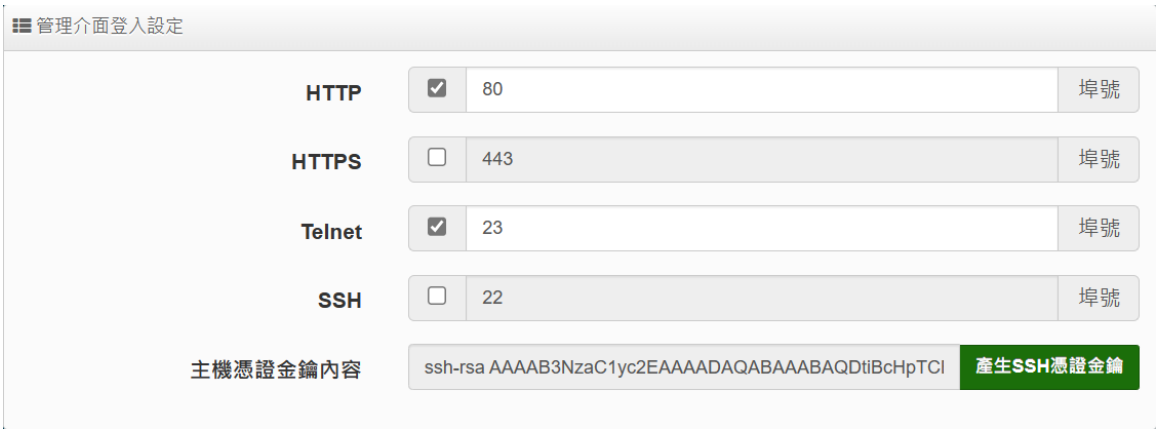


- **Ping Watchdog**：設定填入要監 ping 的 IP 位址
- **Interval**：間隔多少時間去 ping IP 位址一次
- **Delay**：當 ping 不通後要延遲多久再 ping 一次
- **Times of faults**：當以上條件成立幾次後, 讓系統重新啟動。

➢ **Jumbo Frame**：可啟用或停用以確定實體乙太網路連接埠是否使用 2.5Gbe 至 12K 和 1Gb 至 9K Jumbo Frame 作為主要封包傳輸格式。.



➢ **管理介面登入設定:** 系統可支援多種協定登入管理，包含 http / https / Telnet / SSH 等。



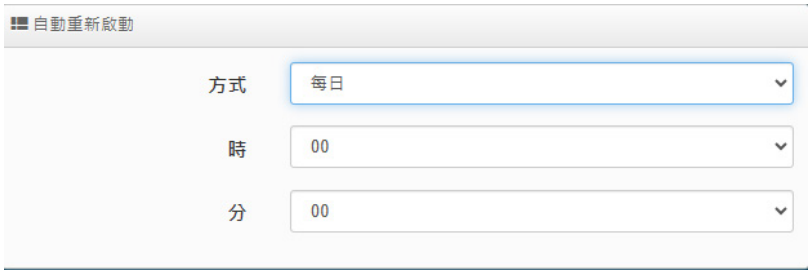
- **HTTP 管理**：勾選此項目將可以啟動 WEB 介面進入管理介面。預設為 80 埠，建議您使用 1025～65535 之間的埠號。

- **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。

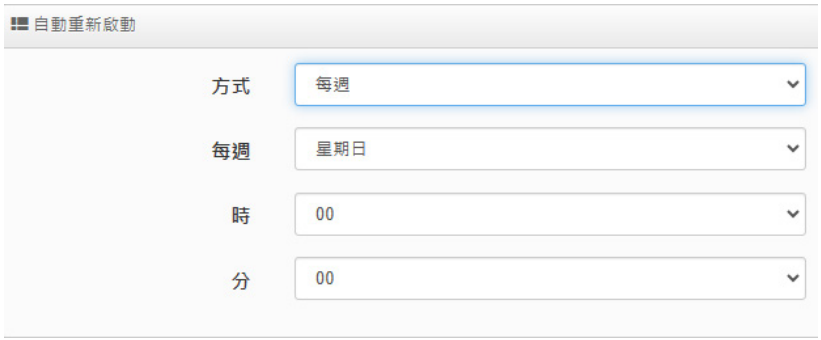
➢ **Access WAN#:** 管理者可啟用或關閉外部是否可以透過 WAN 端進入 DR-5000 的管理介面。(此功能需在 Router 模式才能使用)

➢ **自動重新啟動:** 此功能可以設定系統自動重新啟動。

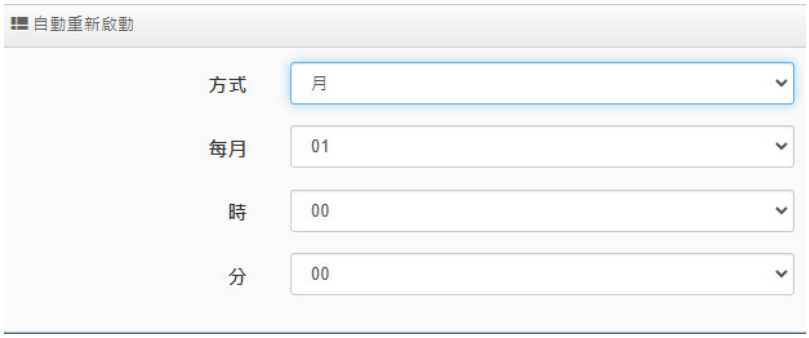
- **每日：** 可設定每日一個時間讓系統自動重新啟動。



- **每週：** 可設定一週中的某一天重新啟動系統。



- **每月:** 可設定每週的某一天讓系統自動重新啟動。



➢ **喚醒 LAN:** 此功能可以輸入遠端 MAC 網卡位址讓系統即時或去定時喚醒遠端某一台網路 MAC 位址設備。

- **每日：** 可設定每日一個時間讓系統去喚醒遠端某一台網路 MAC 位址設備。

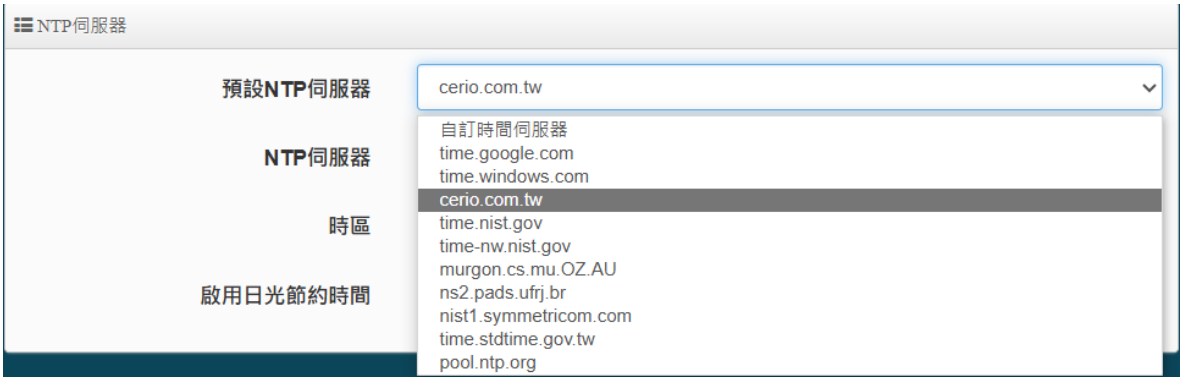
- **每週：** 可設定一週中的某一天讓系統去喚醒遠端某一台網路 MAC 位址設備。

- **每月:** 可設定每週的某一天讓系統去喚醒遠端某一台網路 MAC 位址設備。

3.14 時間伺服器

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

- **目前本地端時間**：此欄位顯示出目前系統的時間。
- **模式**：可設定使用網際網路 NTP 伺服器即時線上更新時間，或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電源供應給 RTC (Real Time Clock Module) IC 即時時鐘記憶儲存模組設計，當選擇" 手動更新" ，若無法儲存時間且總會無效回到預設時間時，則須檢查並更換機板硬體電池。 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 DR-4000 裝置的 DNS 伺服器設定是否正常。

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

3.15 SNMP

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

請點擊" 系統設定" ➔" SNMP" 進入設定

SNMP V2c

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

SNMP V3

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

SNMP Trap

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

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

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

3.16 DDNS

Dynamic Domain Name Server，簡稱 DDNS 動態 DNS 的技術。根據網際網路的域名訂立規則，域名必須跟從固定的 IP 位址。但動態 DNS 系統為動態網域提供一個固定的名稱伺服器（Name server），透過即時更新，使外界用戶能夠連上動態用戶的網址。

本系統內建支援 2 個提供廠商，分別 dyndns 和 no-ip 兩家服務商

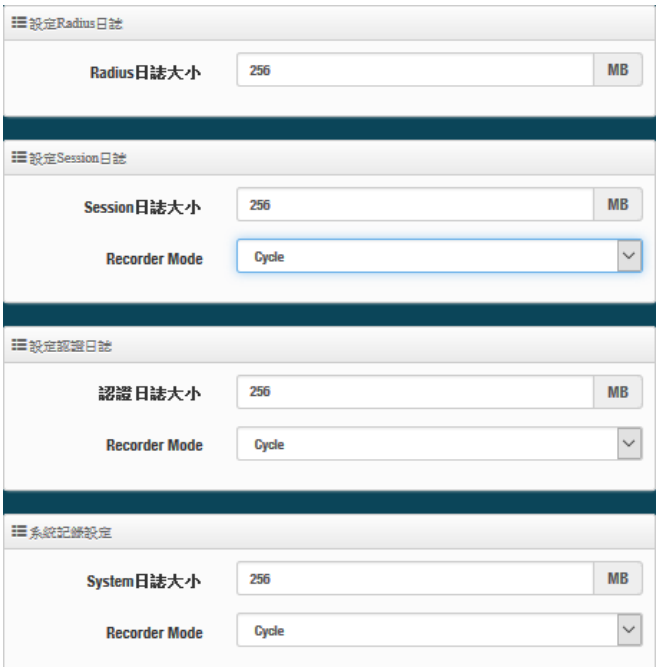
請點擊 "系統設定" ➔" DDNS"

進入後依照所需對應 WAN 選擇編輯設定，共可支援 3 組對應 WAN IP 設定。

- **啟動:** 選擇啟用或關閉啟功能
- **Provider:** 選擇服務廠商
- **WAN:** 選擇本機對外連線的連接埠
- **主機名稱:** 輸入主機名稱
- **用戶名稱/密碼:** 輸入 DDNS 服務廠商所申請的帳戶密碼
- **Interval:** 輸入主機自動向 DDNS 服務廠商提供實體位址的間隔

3.17 日誌伺服器

如果設備使用 CERIO 產品並有支援 syslog 服務功能，則 CERIO 設備的 Log 資訊可以傳送到此服務器並記錄以便日後稽核或是除錯，Log 的紀錄資訊支援 RADIOS/Session/網頁認證及系統資訊等 Log。 此日誌伺服器可管理儲存空間大小及保留 Log 的時間，也能透過 E-Mail 方式寄出。



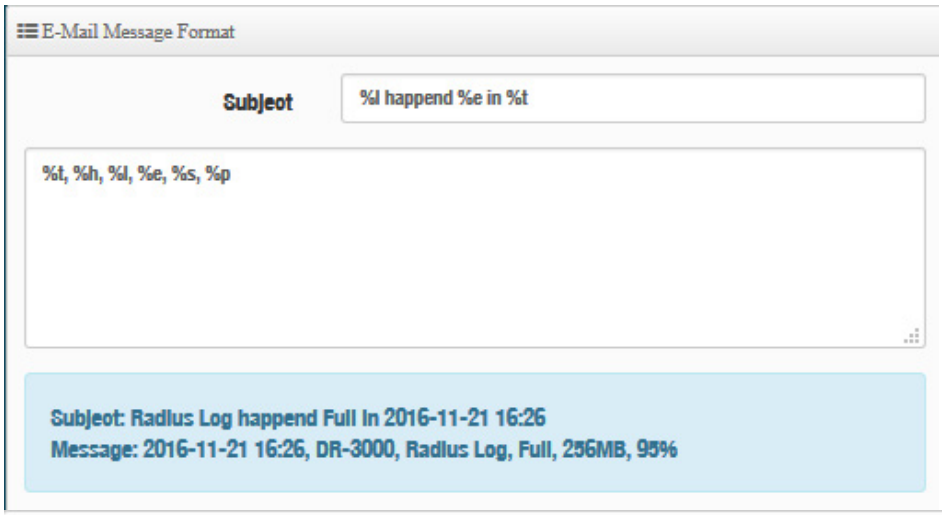
- **日誌大小:** 管理人員可以設定日誌的儲存空間的大小，包含 RADIUS/session/網頁認證及系統 log.(最大空間可設定 512MB)
- **Recorder Mode:** 日誌保留期限方式，此選項可以管理日誌保留期限或是關閉限制。
  - **Cycle:** 此功能是週期性的日誌保留，當儲存空間已滿時，則系統會自動刪除最先前的日誌資訊持續記錄最新的資訊，循環紀錄日誌。
  - **Retention Period:** 此功能管理主要是限制日誌保留天數，當資訊保留到設定的天數後，系統將會自動刪除最先前的一天資訊，持續的循環紀錄。最大設定 90 天。

Notice	**當日誌的紀錄檔案超過設定空間的大小時，系統會停止紀錄，所以務必計算保留天數及空間大小。例如：保留天數設定 7 天，但在第 3 天時儲存空間已滿，則當下系統將自動停止紀錄。**

  - **終止服務:** 終止日誌保留限制，若終止限制，則系統會一直儲存日誌，直到空間已滿後停止在記錄。

電子郵件訊息的格式

若啟用 **3.18 E-Mail 通知功能** 則管理人員可以在此設定寄送日誌資訊的格式.



Message Format

Format	Description
%h	Hostname
%t	Time
%l	Log Type(Radius Log/Session Log/Authentication Log/System Log)
%s	File Size
%p	File Percentage
%e	Event Type(Full/ Stop Service/ Start Service)

代號說明：

- %h: 顯示主機名稱。
- %t: 顯示日誌的時間。
- %l: 顯示日誌的類型,例如 RADIUS/Session..等日誌
- %s: 顯示日誌的檔案大小。
- %p: 顯示日誌的檔案百分比。
- %e: 顯示事件類型如(已滿/停止服務/啟動服務)

假若管理人員想利用系統自動以 E-Mail 方式寄出，並希望只看特定的訊息，可以在消息欄位輸入代號，例如：管理人員想看到主機名稱及日誌時間和類型，可以輸入%h,%t,%l 即可, 以逗號分開

3.18 E-Mail 通知設定

此功能可以設定系統要使用哪個 E-Mail 伺服器去寄送日誌給特定的 E-Mail 帳戶。

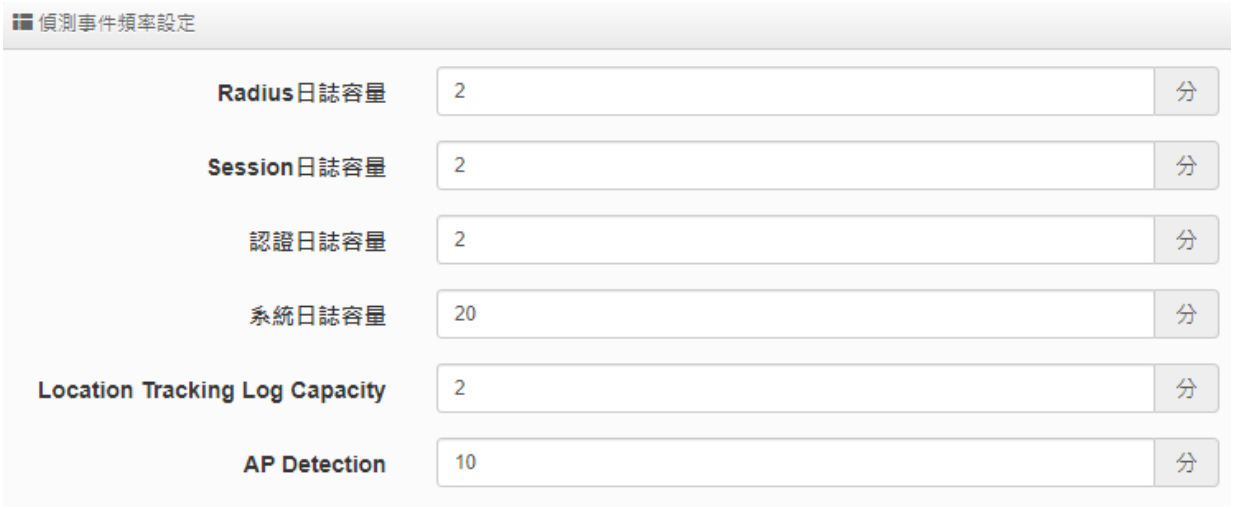
請點擊 **“系統設定” ➔ “E-Mail 通知”**，共可設置 2 組 SMTP 的寄送帳戶。

- **SMTP 1/2 服務:** 此功能可設定 2 組 SMTP 寄送的 E-Mail 帳戶

- **送件人:** 設定發送的郵件帳戶
- **TEST 按鈕:** 當 SMTP 資訊設定完成後，可按下 TEST 按鈕，系統將自動測試此 SMTP 是否能正常運作。
- **SMTP 伺服器:** 設定 SMTP 寄件伺服器位址。
- **Port:** 設定 SMTP 寄件伺服器的使用埠號。
- **加密:** 選擇 SMTP 伺服器的使用加密方式。
- **SMTP 認證:** 設定 SMTP 伺服器(E-Mail)使用的帳號及密碼。

偵測事件頻率設定

主要可以設定每多少分鐘去偵測 1 次日誌的容量，預設為每 30 分鐘去偵測一次儲存空間，當觸發偵測後，系統將透過 SMTP 信箱發送資訊給所設定的收件者。可以設定 Radius, Session, 認證，系統日誌容量，Location Tracking Log Capacity, AP Detection 頻率。並按" 儲存" 完成設定。



接收的 E-Mail 列表

管理人員可以設定要接收資訊的 E-Mail 帳戶，並可選擇要發送哪些警訊通知。請點擊 " 建立 Receiver E-Mail " 按鈕進入新增 E-Mail 帳戶。

- **接收的 E-Mail:** 設定收信帳戶 E-Mail 位址。
- **編輯：**可以**停用/啟用 Radius, 網頁認證功能, Session, Syslog, Location Tracking** 位置追蹤, **AP Detection** AP 偵測.

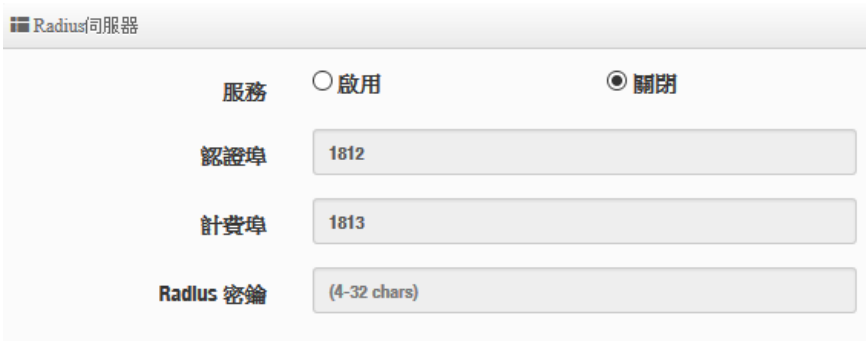
刪除 E-mail：透過”執行”下的”編輯”功能可以直接刪除設定好的某個 “E-mail” 的通知設定。

4. 帳戶認證

此功能是一個 AAA 認證 RADIUS 服務器，可允許受管 Cerio AP 使用 RADIUS 服務器認證，且認證方式支援多種類型。當受管的 Cerio AP 設定外部 RADIUS 服務器啟用身份驗證時，必須將驗證的位址設定 DR-5000 的 IP 地址，以正確重定向認證客戶端。(可參考 Cerio CenOS5.0 AP 的使用手冊)

Cerio 的 DR-5000 RADIUS 認證伺服器包括預生產票和遠端 LDAP（AD）身份驗證類型，管理員必須先啟動 RADIUS 伺服器運作並設置認證帳戶。

4.1 RADIUS 伺服器



- **服務:** 管理人員可以啟動或關閉 RADIUS 伺服器功能。
- **認證埠:** 此為標準的 RADIUS 伺服器，管理人員可以為此 RADIUS 伺服器設定埠號，建議使用預設標準的 1812 埠.
- **計費埠:** 此為標準的 RADIUS 伺服器統計/計費使用埠號，管理人員可以設定埠號，建議使用預設標準的 1813 埠.
- **Radius 密鑰:** 若啟動此服務管理人員須設定 RADIUS 伺服器的使用密鑰(Secret key)。

4.2 遠端 LDAP 設定

遠端 LDAP 認證，主要是 RADIUS 伺服器的帳戶是向遠端 LDAP 伺服器詢問，也就是說受管理的 Cerio AP 使用外部認證需設定指向 DR-5000 的 RADIUS 伺服器認證，而帳戶則由 DR-5000 去訪問遠端 LDAP 伺服器的帳戶，如下示意圖。目的是假如在現有環境中已經有 AD 或是 LDAP 伺服器，則 DR-5000 無須再重複建置認證帳戶的資料庫，可直接與現有的 AD 或是 LDAP 伺服器整合。

- **服務:** 管理人員可以選擇啟動或關閉此服務。
- **LDAP 埠 ：** 設定遠端 LDAP 使用的埠號
- **LDAP 密鑰:** 設定登入遠端 LDAP 伺服器的密鑰。

- **編輯:** 點擊”**編輯**”進入設定欲想連接遠端 LDAP 的資訊

- **服務:** 啟動或關閉此服務。
- **IP 位址:** 設定遠端 LDAP(AD)伺服器的 IP 位址。
- **埠號:** 設定遠端 LDAP(AD)伺服器所使用的埠號。
- **用戶名稱:** 設定可登入遠端 LDAP(AD)伺服器的帳戶。
- **密碼:** 設定可登入遠端 LDAP(AD)伺服器的帳戶密碼。
- **Base DN:** 設定遠端 LDAP(AD)伺服器的網域 DN 路徑。
- **帳戶屬性:** 設定遠端 LDAP(AD)伺服器登入的帳戶屬性。
- Identity: 設定帳戶所屬的身分。

LDAP 設定

此功能可以設定認證逾時時間/時間限制級網路超時等

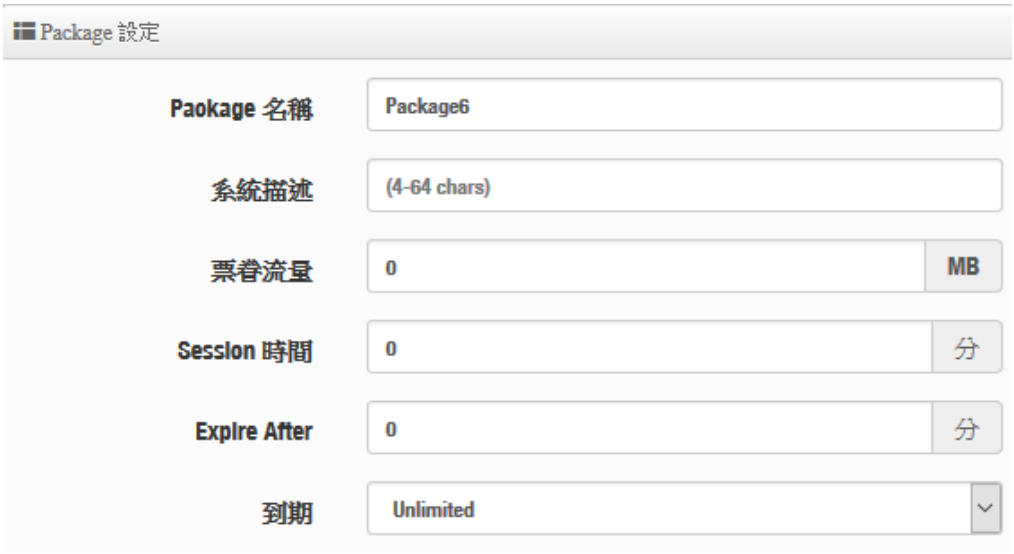
4.3 Package 設定

此功能為建置票券規則，每個票券規則可針對 session/流量/到期日等等上網限制，同時可設定系統自動產生的密碼規則，此票券管理可搭配智鼎的帳戶票卷輸出器 POS 系統，讓系統自動產生的認證帳戶透過熱感式印表機列印出來。

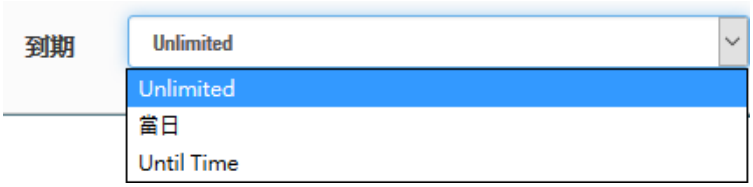
#	名稱	系統描述	Session 時間	票卷流量	Expire After	到期	執行
0	Test-1	test1		60.00MB			編輯
1	Test-2	Test-2	20Minute(s)	0B			編輯
2	Test-3	Test-3		0B	1Hour(s)		編輯
3	Test-4	Test-4		0B		Per 1day 00:00	編輯
4	Test-5	Test-5		0B		Per 0day 17:00	編輯
5	Test-6			0B		Until 0day 14:00	編輯

➢ **建立新的 Package:** 管理人員可以點擊此按鈕來建置新的票券規則。

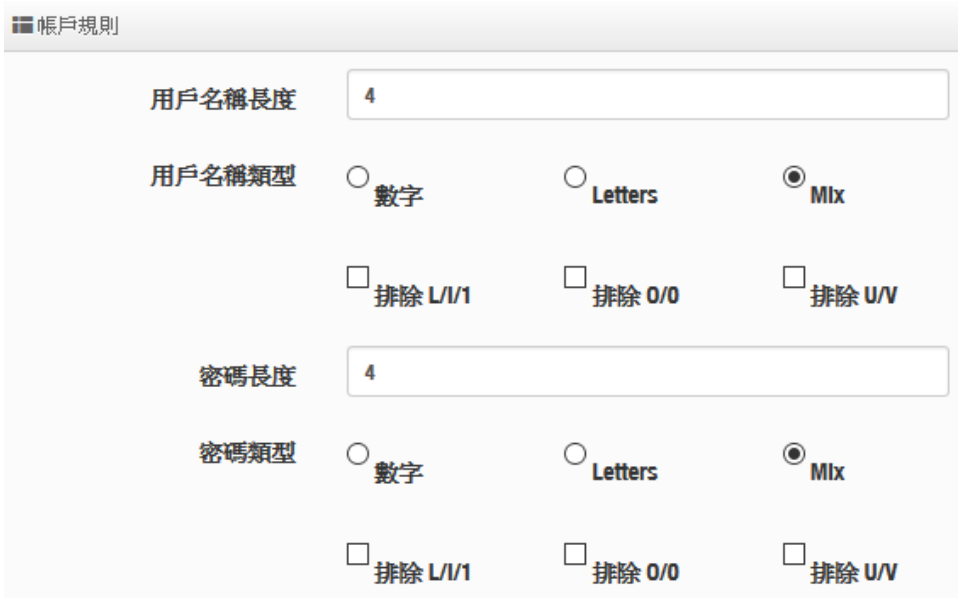
進入 Package 設定



- **Package 名稱：**設定此票券規則名稱。
- **系統描述：**可簡單描述此規則概述。
- **票券流量：**設定帳戶上網的使用流量限制。
- **Session 時間:**設定帳戶上網的 Session 時數限制，當登入後開始計時，登出後則停止計時，等下次登入時繼續計時直到時數用完為止。
- **Expire After：**設定帳戶登入後開始計時，直到設定的時數用完則停止。
- **到期：**設定到期時間。



- ✓ **Unlimited**：無限制
- ✓ **當日**：設定一個截止時間，當帳戶登入後開始計時，直到截止日到期將停止。
  例如：設定 1 天時間，若帳戶在下午 3 點開通，則將在隔天下午 3 點截止。
- ✓ **Until Time**：設定一個使用的時間點，不管帳戶有沒有登入，只要所設定的時間點到就停止。
  例如：設定 1 天時間，不管帳戶什麼時間點開通，只要 00:00 點時間一到就停止。



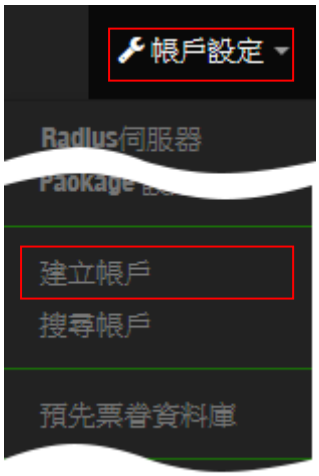
- **用戶名稱/密碼長度**：設定系統自動產生帳戶名稱/密碼的長度。
- **用戶名稱/密碼類型**：設定系統自動產生帳戶/密碼的類型規則。
  - ✓ **數字**：表示系統產生的帳戶只為數字。
  - ✓ **Letters**：表示系統產生的帳戶只為英文字母。
  - ✓ **Mix**：表示系統產生的帳戶為數字與字母混和。

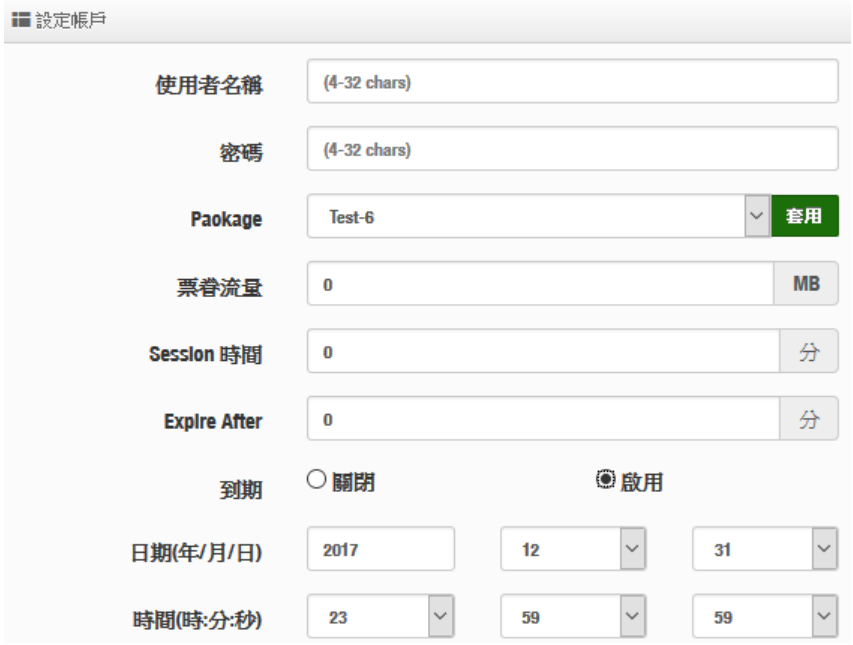
➢ **#：** 在列表上的(0~9)數字是提供給網路控制伺服器(SP-800) 去選擇要列印哪一筆票券的規則

4.4 建立帳戶(RADIUS 帳戶)

管理人員可以手動建置 RADIUS 伺服器的帳戶名稱與密碼，同時可以限制所建置的帳戶使用期限限制，也能套用票券規則的設定值去套用。

請點擊 **“帳戶設定”➔”建立帳戶”進入設定**



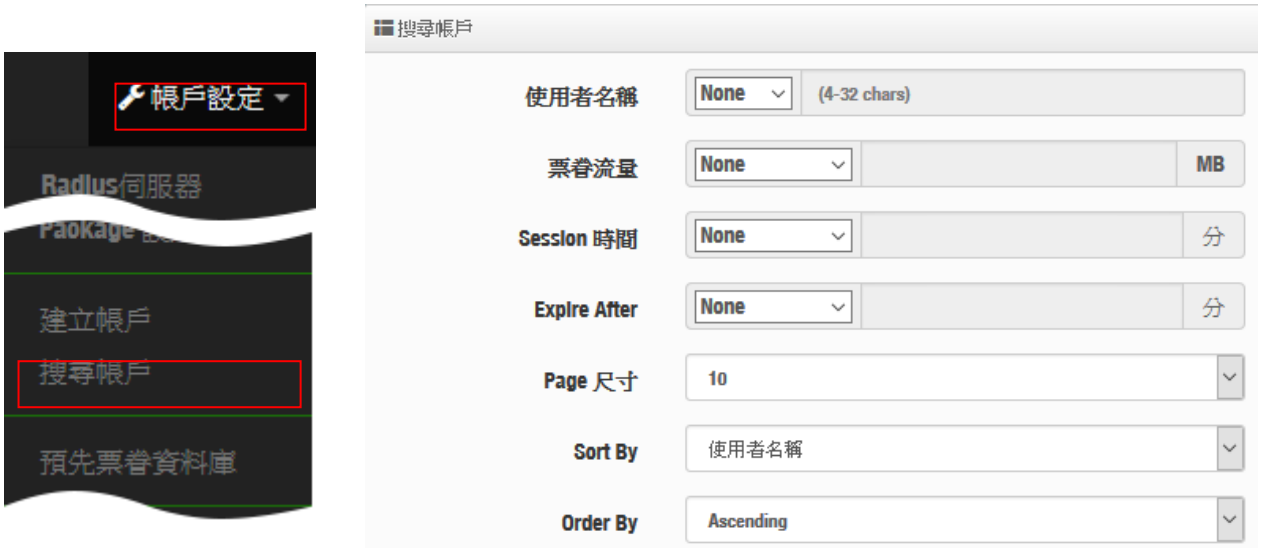


- **使用者名稱**：建立 RADIUS 伺服器的使用帳戶。
- **密碼**：建立 RADIUS 伺服器的帳戶密碼。
- **Package:** 管理員可以選擇是否要套用票券的規則。
- **票券流量:** 管理人員可以限制此帳戶的使用流量，一但流量使用完畢將停止此帳戶的服務。
- **Session 時間**：設定帳戶上網的 Session 時數限制，當登入後開始計時，登出後則停止計時，等下次登入時繼續計時直到時數用完為止。
- **Expire After**：設定帳戶登入後開始計時，直到設定的時數用完則停止。
- **到期**：設定到期日期，不管帳戶有沒有登入，只要所設定的時間點到就停止。

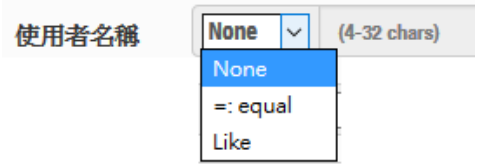
4.5 搜尋帳戶

管理員可以透過此智慧型搜尋引擎功能在資料庫中搜索所有帳戶。 利用此智慧型搜尋引擎可以透過條件式或關鍵字等查詢帳戶資料。

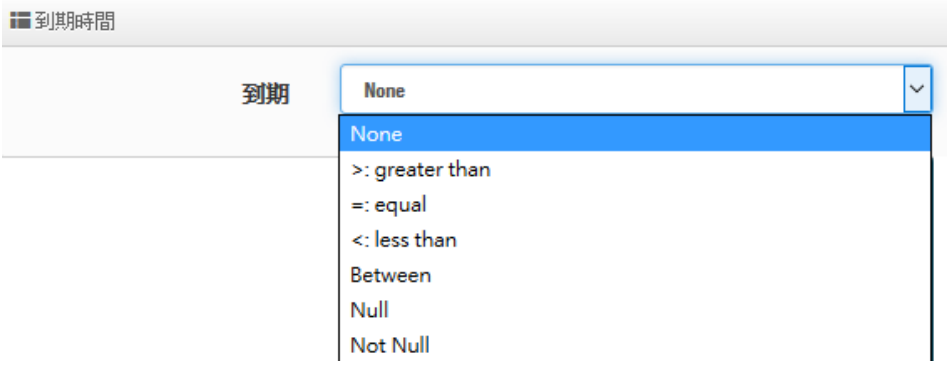
請點擊 **“帳戶設定”➔”搜尋帳戶”** 進入搜尋



管理員可以在搜索引擎中選擇不同的數據類型關鍵查詢。

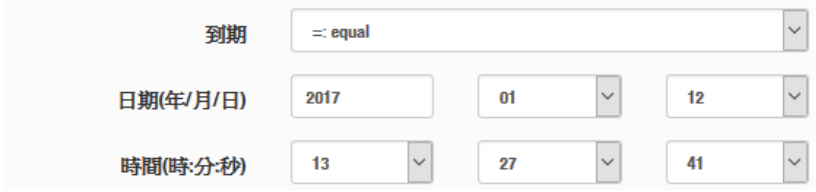


- **None**：表示不判斷條件搜尋全部帳戶。
- **Like**：關鍵字搜尋。

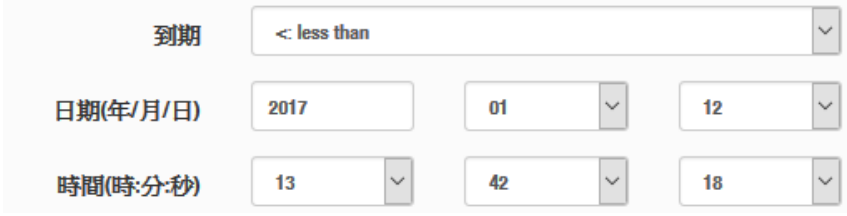


- **Greater then**：搜尋帳戶到期日大於以下設定的日期．

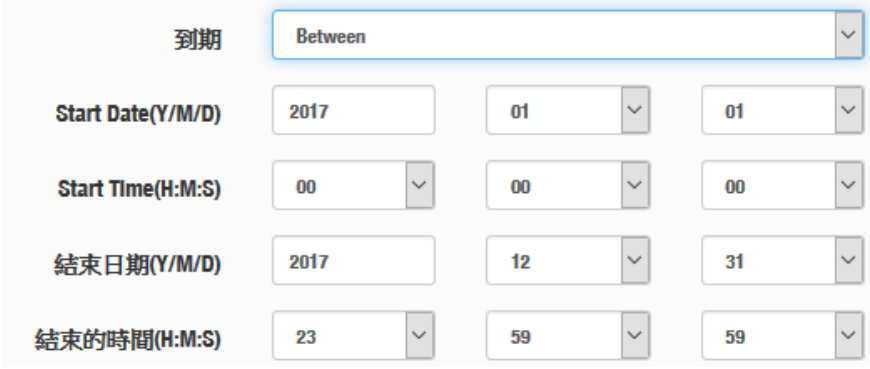
- **Equal**：搜尋帳戶到期日等於以下設定的日期。



- **Less then：** 搜尋帳戶到期日小於以下設定的日期。



- **Between：** 搜尋帳戶到期日的起始/結束區間的日期。

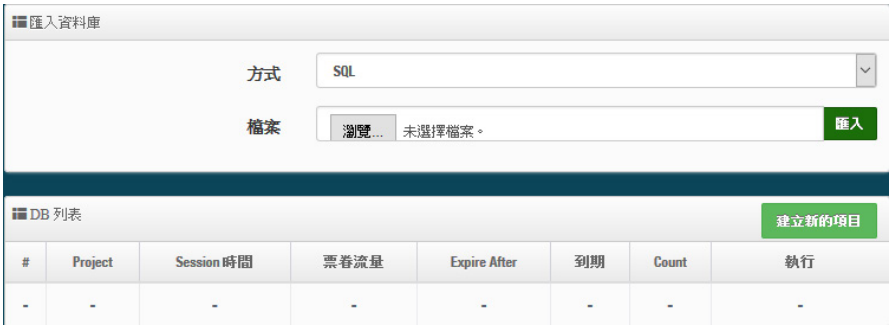


- **Null：** 搜尋沒有設定到期日的所有帳戶。
- **Not Null：**搜尋有設定到期日的所有帳戶。

4.6 預先票券資料庫

此功能為預先設定票券，管理人員可以在這功能頁面上一次產生多筆帳戶

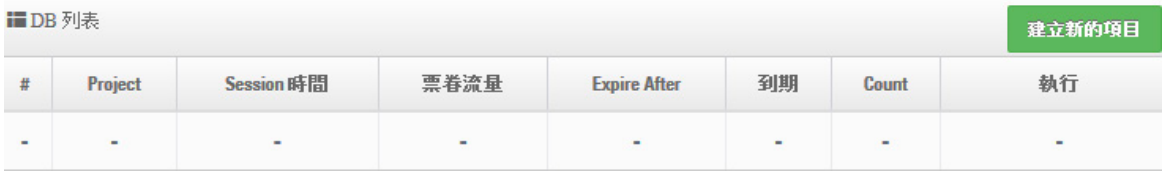
請點擊 **“帳戶設定”➔”預先票券資料庫”**新增多筆帳戶資料庫



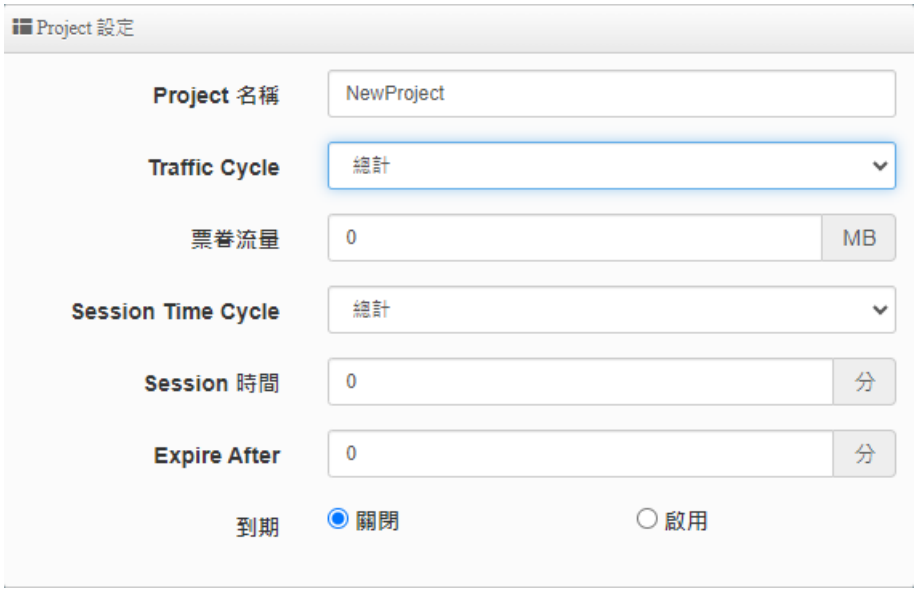
匯入資料庫：假若先前已經有建立過資料庫，並將資料庫匯出檔案，可在此復原資料庫內的帳戶。

- **方式**：選擇要復原資料庫的檔案類型。
- **檔案**：選擇要要復原的資料庫檔案。

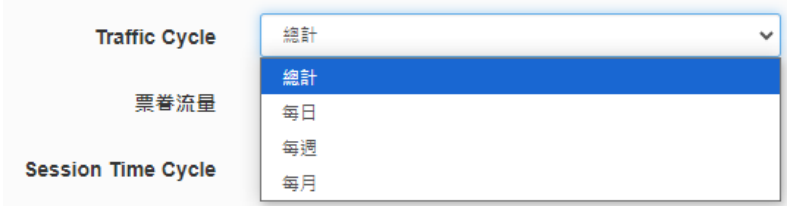
DB 列表: 可顯示資料庫表單以及新建資料庫。



管理人員請點擊**"建立新的項目"**按鈕，可建立多筆帳戶的資料庫



- **Project 名稱:** 設定新增的帳戶資料庫名稱。

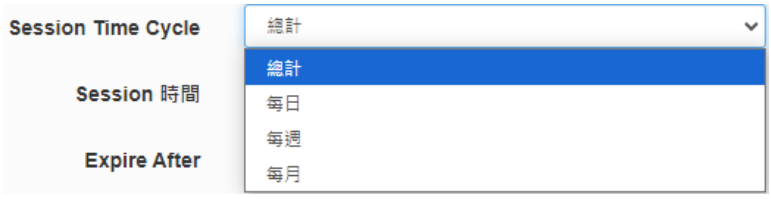


- **Traffic Cycel: 流量使用清零重置週期，預先票卷帳密將因此重置週期而獲得重複可再活躍使用資格。**
  - ✓ **總計**：依一次性總計計算，預先票卷帳密流量總計額度用完將無法再使用。
  - ✓ **每日**：設定" 日" 為限額流量重置歸零循環期，系統固定每日 00:00 為" 日" 重置跨點。
  - ✓ **每週**：設定" 週" 為限額流量重置歸零循環期，系統固定每週日 00:00 為" 週" 重

置跨點。

- ✓ **每月:**設定" 月" 為限額流量重置歸零循環期,系統固定每月底最後一日 00:00 為" 月" 重置跨點。

➢ **票券流量:** 配合 Cycle 設定為"總計"時,管理人員可以設定此資料庫的帳戶所能使用多少流量。



➢ **Session Cycel:** Session 時間使用清零重置週期,預先票卷帳密將因此重置週期而獲得重複可再活躍使用資格。

- ✓ **總計:**依一次性總計計算,預先票卷帳密 Session 時間總計到期用完將無法再使用。
- ✓ **每日:**設定" 日" 為 Session 可用時間重置歸零循環期,系統固定每日 00:00 為" 日" 重置跨點。
- ✓ **每週:**設定" 週" 為 Session 可用時間重置歸零循環期,系統固定每週日 00:00 為" 週" 重置跨點。
- ✓ **每月:**設定" 月" 為 Session 可用時間重置歸零循環期,系統固定每月底最後一日 00:00 為" 月" 重置跨點。

➢ **Session 時間:** 配合 Session Cycle 設定為"總計"時,管理人員可以設定此資料庫的帳戶上網 Session 時數限制,當登入後開始計時,登出後則停止計時,等下次登入時繼續計時直到時數用完為止。

➢ **Expire After:** 設定帳戶登入後開始計時,直到設定的時數用完則停止。

➢ **到期**: 設定此資料庫的帳戶使用網路到期時間。

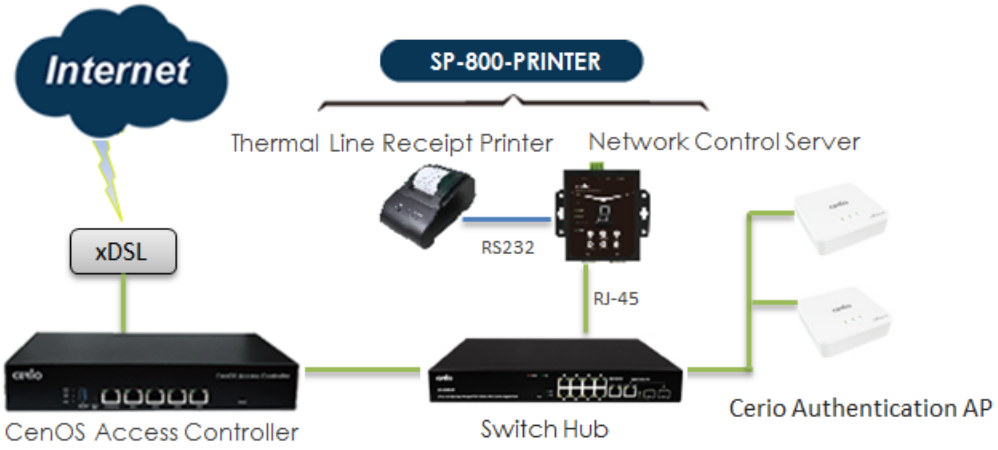
- **用戶名稱/密碼長度**：設定系統自動產生帳戶名稱/密碼的長度。
- **用戶名稱/密碼類型**：設定系統自動產生帳戶/密碼的類型規則。
  - **數字**：表示系統產生的帳戶只為數字。
  - **Letters**：表示系統產生的帳戶只為英文字母。
  - **Mix**：表示系統產生的帳戶為數字與字母混和。

4.7 設定熱感式印表機

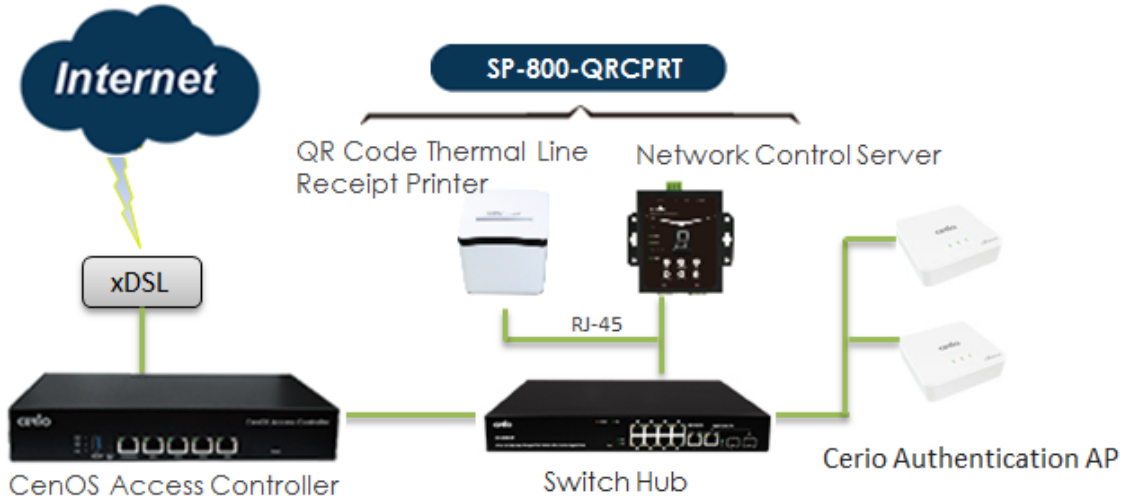
此功能須搭配智鼎的帳戶票卷輸出器 POS 系統，主要是設定整合智鼎的 POS 系統讓 DR-5000 自動產生一組帳戶並透過帳戶票卷輸出器 POS 系統列印出來，帳戶的產生則由本章節"5.3 Package 設定"

熱感式印表機可搭載兩種款式，分別普通型及 QR Code 型熱感式印表機，如下建置架構說明

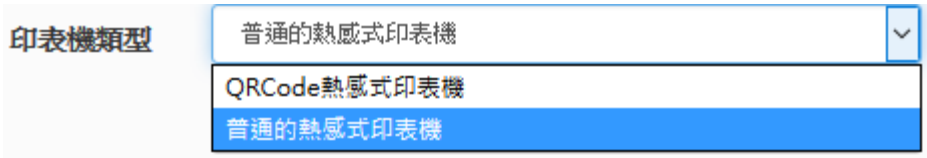
 # 搭載 SP-800-PRINTER（普通型熱感式印表機）



 # 搭載 SP-800-QRCPRT（QR Code 型熱感式印表機）

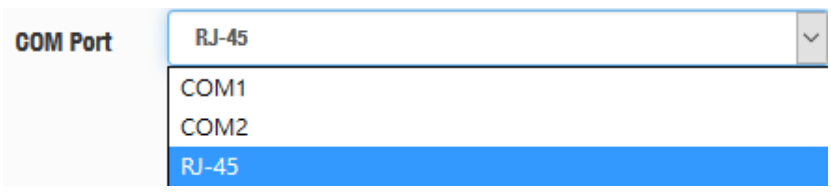


- **IP 位址** 設定網路控制伺服器的 IP 位址 (SP-800)
- Command Port: 設定網路控制伺服器的埠號(SP-800)
- **印表機類型:** 選擇所使用的熱感式印表機。



  - **QRCode 熱感式印表機:** 若採購智鼎 SP-800-QRCPRT POS 系統則選擇此設定。
  - **普通的熱感式印表機:** 若採購智鼎 SP-800-PRINTER POS 系統則選擇此設定。
- **COM Port:** 選擇熱感式印表機所連接到 SP-800 的 COM 埠

Notice 若使用 QRCode 熱感式印表機並以 RJ-45 連接至內部網路, 則必須選擇 RJ-45



- ✓ **印表機 IP 位址:** 設定 QR Code 熱感式印表機的 IP 位址
- ✓ **印表機 Port:** 設定 QR Code 熱感式印表機的使用連接埠號
- ✓ **QR Code 類型:** 可設定要列印出 RQ Code 碼的大小或關閉。

➢ **New Look Password:** 設定 SP-800 的按鍵鎖密碼，預設為 1234

➢ **描述:** 可自行設定此描述說明。

Package 列表

當設定完成"5.3 Package"規則後則會在此欄位顯示筆數，依照需求勾選，被勾選的 Package 數字將會顯示在 SP-800 上，假若在 SP-800 選擇 3，則系統將會自動產生一筆帳戶列印出來並套用 Package3 的規則。

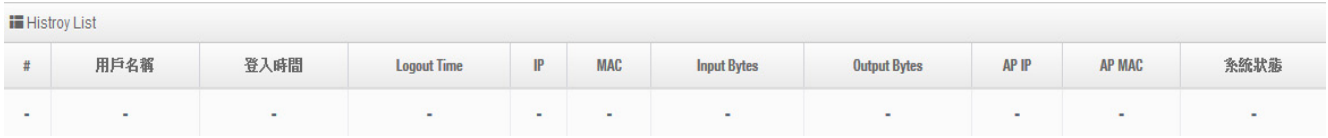
Package 列表

Package#	啟用	名稱	系統描述
0	☐	Test-1	no limit
1	☐	TEST-2	Flow limit
2	☐	TEST-3	Session limit
3	☐	TEST-4	only 60 min
4	☐	TEST-5	Per day
5	☐	Paokage5	

比如選擇 3，則 DR-4000/5000 系統將會自動產生一筆 Package3 規則的帳戶並列印出來

4.8 歷史日誌

能調閱所有帳戶的歷史紀錄，包含帳戶的使用流量，登出/登入訊息，帳戶的使用 IP/MAC 位址，及帳戶連接的 AP 等等資訊


Histroy List

#	用戶名稱	登入時間	Logout Time	IP	MAC	Input Bytes	Output Bytes	AP IP	AP MAC	系統狀態
-	-	-	-	-	-	-	-	-	-	-

4.9 線上日誌

此功能可檢視所有目前在線的帳戶名單資訊

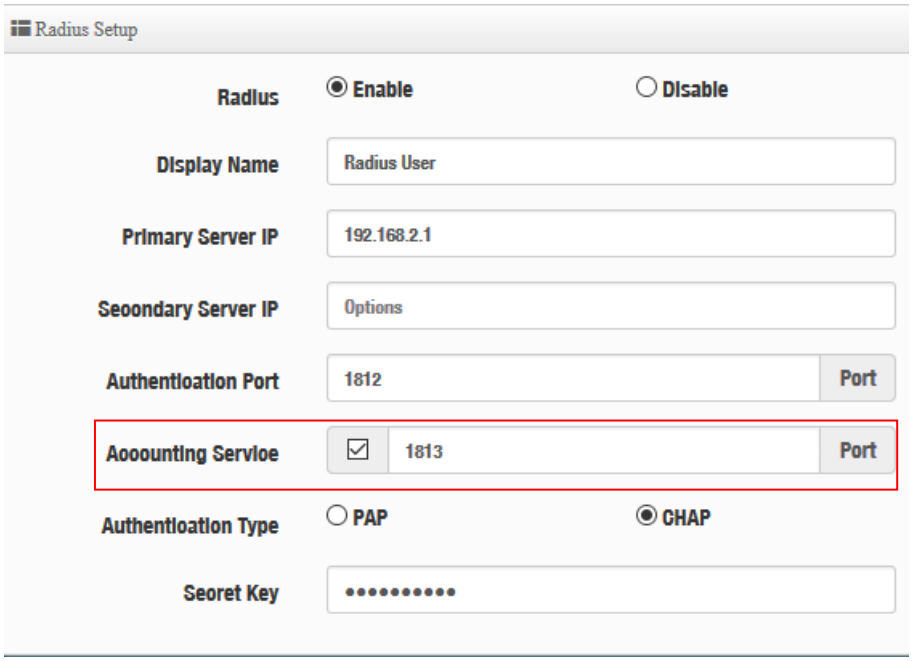

Online Log

Online Log

#	Username	Login Time	Session Time	IP	MAC	Input Bytes	Output Bytes	AP IP	AP MAC
-	-	-	-	-	-	-	-	-	-

若要記錄即時線上帳戶資訊功能，則必須要配合智鼎 AP 的網頁認證功能設定啟用 RADIUS 認證並啟用 Accounting 服務才能完整記錄即時線上帳戶的所以資訊，如下圖所示

 # 智鼎 AP 的認證功能介面（ 使用 CenOS5.0 核心）



4.10 資料庫維護

主要可清除資料庫內帳戶的資料，包含已經到期的帳戶，預先票券的帳戶或所有的帳戶刪除

Notice 當按下清除按鈕後，系統將立即清除帳戶，當清除後則無法復原帳戶，請注意確認後再執行

5.進階

5.1 IP 過濾設定

管理者可以在此管理來源端到目的端或是目的端到來源的 IP 流向及服務端口(Port)讀取控制，並可套用 IP 群組或埠群組限制，同時可啟用封包監聽功能，增加網路安全機制。此 IP 過濾規則最大可建置 64 筆資料

請點擊**"進階"➔"IP 過濾設定"**進入列表，並在列表上點擊**"編輯"**按鈕進入設定

➢ 點擊編輯進入設定頁面

➢ **啟動:** 管理員可以選擇啟用或關閉此規則

➢ **註解:** 可輸入此規則的註解描述。

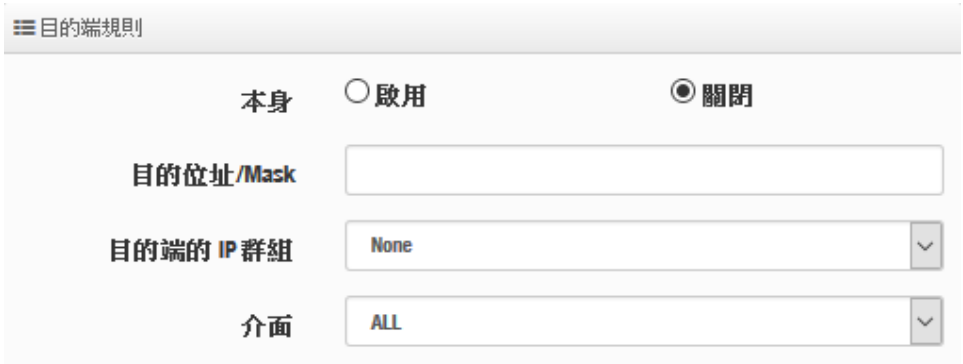
IP 過濾規則

- **政策:** 可選擇此規則是要拒絕或是通行。
- **通訊協定:** 可選擇通訊埠(Port)的協定屬性
- **時間表:** 可套用時間表的規則，透過時間表決定使用特定的時間點去拒絕或通行。

來源規則：設定來源端位址

- **本身:** 假若來源端為本機，管理員則可以直接選擇啟用。
- **來源位址/Mask:** 設定來源端 IP 位址及 MASK 遮罩。
- **來源 IP 群組:** 假若是要過濾整個 IP 區間，可先建置 IP 群組，再將群組套用至此即可。
- **介面:** 可選擇來源端介面是 WAN 或 LAN

目的端規則：設定目的端位址



- **本身:** 假若目的端為本機，管理員則可以直接選擇啟用。
- **目的位址/Mask:** 設定目的端 IP 位址及 MASK 遮罩。
- **目的端 IP 群組:** 假若是要過濾整個 IP 區間，可先建置 IP 群組，再將群組套用至此即可。
- **介面:** 可選擇目的端介面是 WAN 或 LAN

5.2 IP 群組設定

管理員可在此建置多組的 IP 位址組成一個群組，主要能在 IP 過濾設定功能上進行套用此 IP 群組做為安全管控。共可建置 20 筆 IP 位址群組管理。

請點擊**"編輯"**按鈕進入編輯 IP 群組設定

➢ **註解:** 輸入此 IP 位址群組的註解。

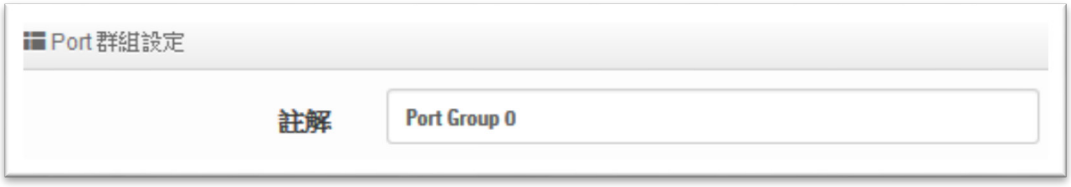
➢ **IP 位址類型:** 管理人員可以選擇加入單一 IP 位址/IP 位址的範圍區間或是整個區域網域等

- **單一 IP 位址:** 輸入單一個 IP 位址
- **範圍:** 輸入 IP 位址的起始/結束範圍區間
- **Subnet:** 輸入一個區域網域，例如 192.168.2.0/24 表示 Class C 網段

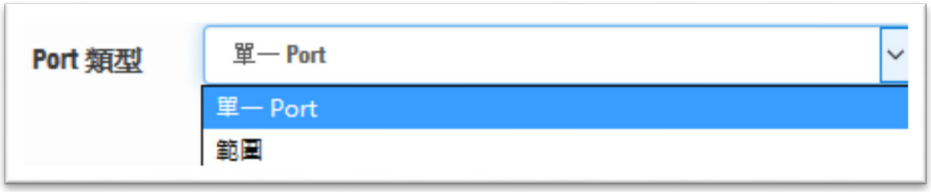
5.3 Port 群組設定

管理員可在此建置多組的 Port 組成一個群組，主要能在 IP 過濾設定功能上進行套用此 Port 群組做為安全管控。共可建置 20 筆 Port 群組

請點擊**"編輯"**按鈕進入編輯 Port 群組



- **註解:** 輸入此 Port 群組的註解。



- **單一 Port:** 管理員可以新增一個 Port 號。
- **範圍:** 管理員可以新增一組 Port 號範圍區間。

5.4 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 64 筆 MAC 位址。

- **模式:** 管理員可以選擇 MAC 過濾條件為拒絕或允許通過.
  - **拒絕:** 當選擇為拒絕則 MAC 位址的名單將會拒絕通行，表單以外的 MAC 位址允許通行.
  - **允許:** 當選擇為允許則 MAC 位址的名單將會允許通行，表單以外的 MAC 位址拒絕通行.
- **註解:** 輸入 MAC 位址的註解。
- **MAC 位址:** 輸入 MAC 位址。(可省略**":"**符號，例如 MAC 位址 8c:4d:ea:11:22:33 則可直接輸入 8c4dea112233，以上兩種格式均可)
- **政策:** 政策管理主要可套用時間規則，目的可以在某特定的時間點做過濾的動作。

5.5 虛擬伺服器設定

如果管理人員希望外部可以讀取區網內開放的特定服務如 IP 網路攝影機、網頁伺服器、FTP 伺服器等讓服務透過通訊埠(Port)對外連接，可設定此功能。此虛擬伺服器可建置 64 筆規則。

請點擊**"編輯"**按鈕進入虛擬伺服器設定

- **啟動:** 管理人員可以啟動或關閉此筆虛擬伺服器規則。
- **註解:** 可描述此規則說明.
- **通訊協定:** 請選擇使用 TCP 或 UDP 的通訊協定.
- **介面:** 選擇一個對外網路的介面.
- **外部公共埠號:** 設定外部連線至內部伺服器所使用的埠號。
- **內部伺服器 IP 位址:** 輸入要對外的內部伺服器 IP 位址
- **內部伺服器埠號:** 設定內部伺服器所使用的埠號。
- **時間表 :** 管理員可套用**"時間規則"**，透過時間規則可在特定的時間點開啟或關閉服務。

5.6 存取控制設定

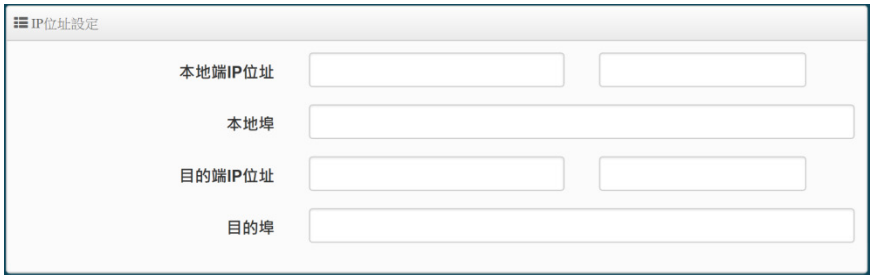
此功能將可以讓網管人員限制或允許網路使用者成員或公司員工上網行為，利用此規則進行以「通訊協定」、「網域或關鍵字」或是「應用程式」進行阻擋或允許。可設定 64 筆管理規則。

請點擊**"編輯"**按鈕進入設定管理

存取控制規則：

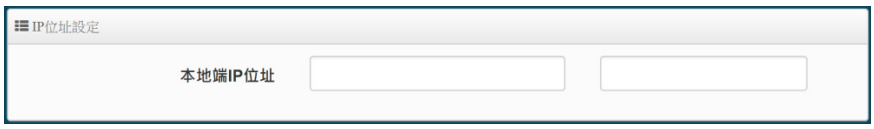
- **啟動**：可選擇啟動或關閉功能。
- **描述**：可輸入此規則描述。
- **通訊協定**：可選擇要過濾的通訊協定。

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



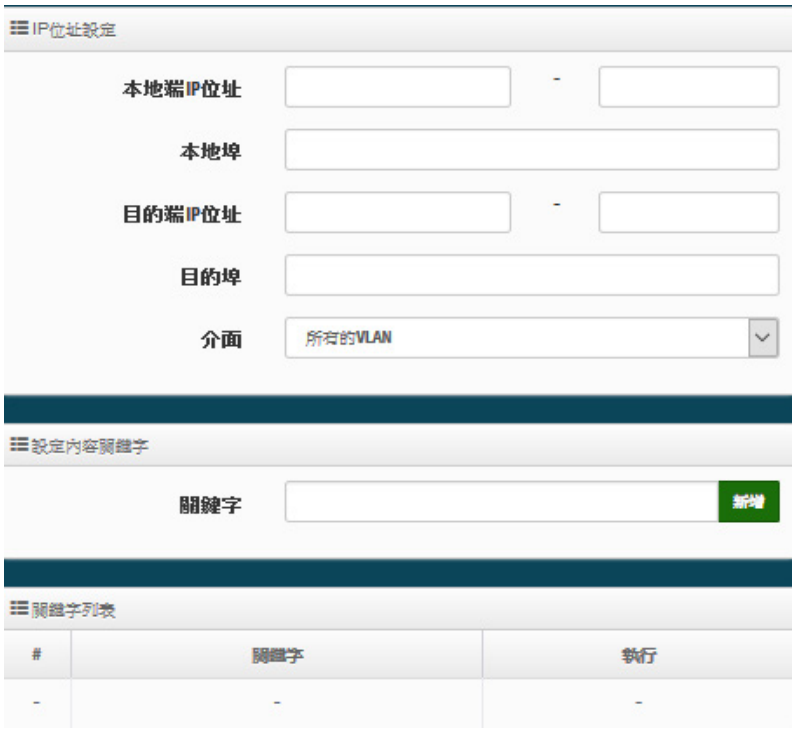
- ✓ **本地端 IP 位址:** 輸入要管理的本地端 IP 位址或 IP 區間。
- ✓ **本地埠**：輸入要管理的本地埠，若要設定區間可用”**:**”表示，例如(1:65535)。
- ✓ **目的端 IP 位址**：輸入目的端 IP 位址或 IP 區間。
- ✓ **目的埠**：輸入要管理的目的埠，若要設定區間可用”**:**”表示，例如(1:65535)。

- **ICMP**：只針對 ICMP 的通訊協定做規則管理。



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

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



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

- **應用程式：**系統已預設有多筆應用程式，管理人員可點擊下拉選單去選擇要過濾的應用程式。

- **網域名稱過濾：**

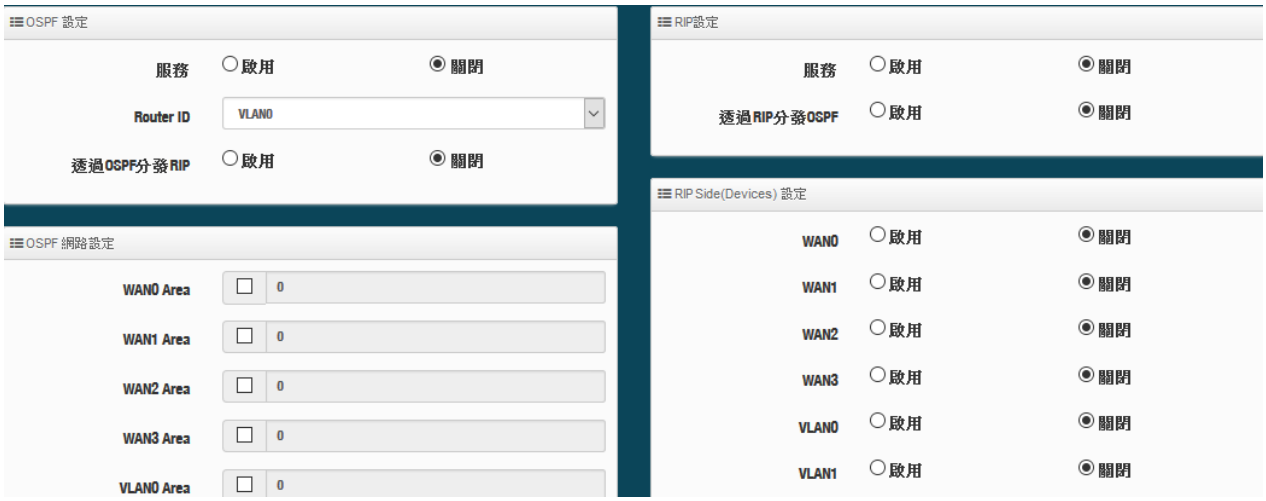
管理員可針對「網域名稱」進行規則設定，請在「網域」欄位中輸入要過濾的網域名稱後按下「新增」鍵即可，若要刪除請按「移除」鍵。

➢ **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。

5.7 IP Routing 設定

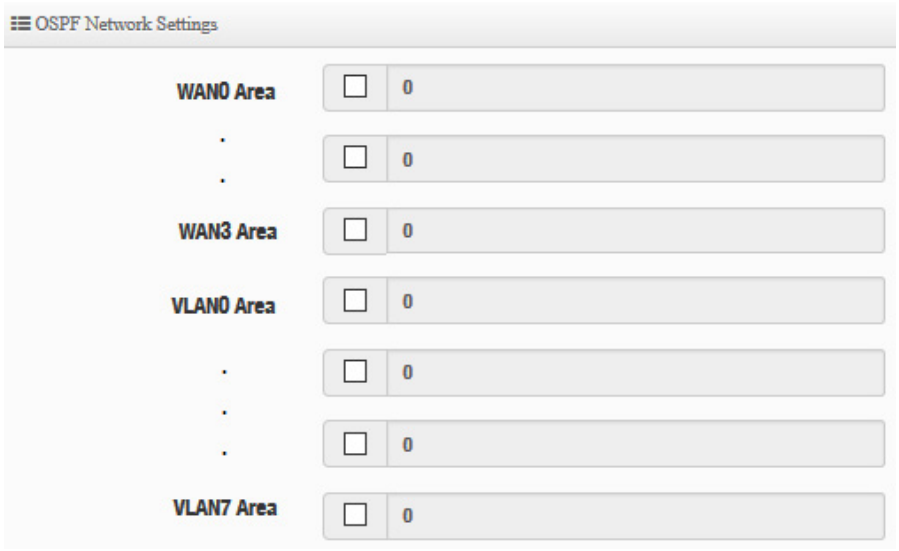
IP 路由設置主要設定 RIP（路由信息協議）和 OSPF（開放最短路徑優先）路由等協議。



➢ **OSPF 設定 :**

- **服務:** 管理員可以設定啟用或關閉 OSPF 協議
- **Route ID:** 標示 OSPF 的 Router ID，每台的 Router ID 都必須有不同的 Router ID
- **透過 OSPF 分發 RIP:** 管理員可以選擇啟用或關閉。

OSPF Network Setting



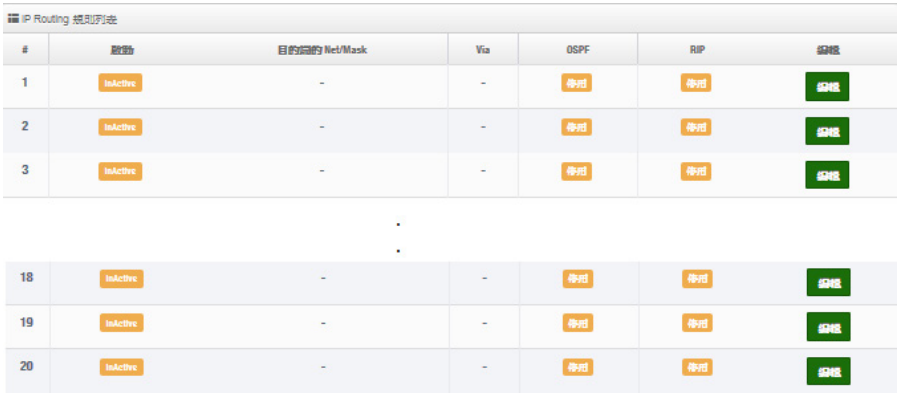
✓ **#Area:** 表示 OSPF 路由協議的區域代碼，可以是十進制中的任意數字，默認值為 0。

➢ **RIP 設定**

- **服務:** 管理員可以設定啟用或關閉 RIP 協議
- **透過 RIP 分發 OSPF:** 管理員可以選擇啟用或關閉。

✓ **RIP Side(Devices) 設定:** 管理員可以設定 Router RIP 路由協定，其中 WAN/LAN 代表的是路由器(本機)所連接的其他網路區段。

5.8 IP Routing 規則設定



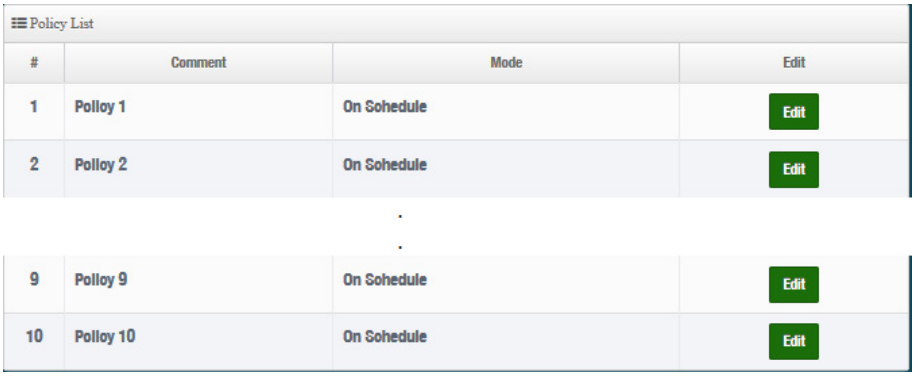
請點擊**"編輯"**按鈕進入 Routing 設定

- **服務:** 管理員可以選擇啟動或關閉此筆的路由規則。
- **目的端的 Net/Mask:** 設定目的端的 Net / Mask 網域。
- **Via:** 可選擇手動輸入閘道位址或是選擇本機的介面位址。
- **OSPF/RIP:** 管理人員可以選擇是否要啟用 OSPF 或 RIP 協議。

5.9 時間規則

管理者可以定義時間規則去管理 IP 過濾，MAC 過濾和虛擬服務器等條件，透過時間規則進行啟用或停止。系統預設可建置 10 筆時間政策(Time Policy)，並於每筆時間政策(Time Policy)下支援 300 筆時間規則。

請先點選「進階設定」→「時間規則」進入頁面。



請點擊**"編輯"**按鈕進入時間規則設定頁面

- **描述**：管理員可輸入此規則描述。
- **模式**：可選擇依照時間表內執行或依照時間表外執行等。
- **時間規則點**：可點擊 " 建立 " 按鈕設定時間表。

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. 工具

6.1 系統設定管理

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

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

6.2 韌體升級

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

我們強烈建議您：若您的 **DR-5000** 在平常時間運作正常且沒有發生任何相容性的問題，我們通常建議使用者不要輕易更新您的系統韌體，更新韌體是一個有風險的動作，當更新失敗了可能會導致整個系統無法正常運作，而損毀，若沒有特殊需求下建議您不要隨意更新，請務必從本公司網站下載相關的韌體檔案，若您使用了一個非本公司釋出且不明來源的檔案，導致系統無法正常運作或喪失某些功能時，本公司將不負責此產品的任何後續維修服務，請您見諒！

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

Notice

我們強烈的建議您務必遵守以下步驟進行韌體更新：

1. *更新過程中**請勿關閉或是切斷系統的電源**。*
2. *務必使用相容的 WEB 瀏覽器進行更新以免發生更新失敗的問題。*
3. *若未依照以上步驟進行更新作業，當發生更新失敗導致系統無法提供服務或是無法正常運作，請恕本公司會將此狀況判定為人為疏失，您將會失去您的產品保固服務，維修時將會向您收取相對的維修費用。*
4. *若您有任何更新產品上的問題歡迎您隨時致電本公司洽詢詳細的操作步驟。*

6.3 網路測試工具

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

- **Ping**：此工具可以協助您以 PING 的指令測試遠端設備與系統的連線狀態，PING 工具是使用利用傳送 ICMP 封包的方式嘗試與遠端主機進行兩個網路節點之間的連線能力以及反應時間的測試程式，結果將顯示於「結果」欄位中。
  - **遠端 IP 位址 / URL 位址**：請在此欄位中輸入一組遠端的 IP 位址或網域名稱，再按下「PING」鍵進行測試。
  - **回應時間**：您可以在此輸入所需要測試的次數，次數可輸入 1 ~ 50 的數值。

- **Traceroute**：此工具可以協助您以 Traceroute 的指令測試遠端設備與系統用來顯示路由封包到達目的位址的情形，結果將顯示於「結果」欄位中。
  - **Destination Host**：請在此欄位中輸入一組遠端的 IP 位址或網域名稱，再按下「開始」鍵進行測試。
  - **MAX Hop**：您可以在此輸入所需要顯示 Hop 的數量。

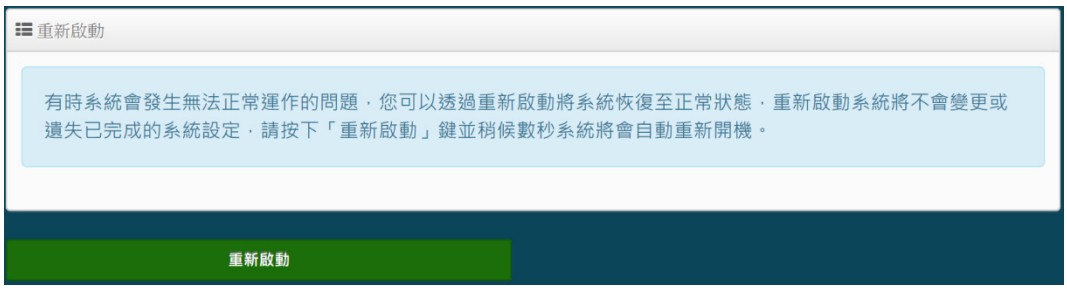
6.4 日誌維護

管理員可以監視 Session/認證和系統的日誌存儲容量狀態，並可透過此功能刪除特定日期的日誌檔。

- **檔案大小/百分比:** 顯示目前日誌使用容量及占用空間的百分比。
- **Keep Date:** 設定保留日期。
  - **刪除:** 刪除日誌

6.5 重新啟動

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



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

7. 系統狀態

7.1 系統狀態

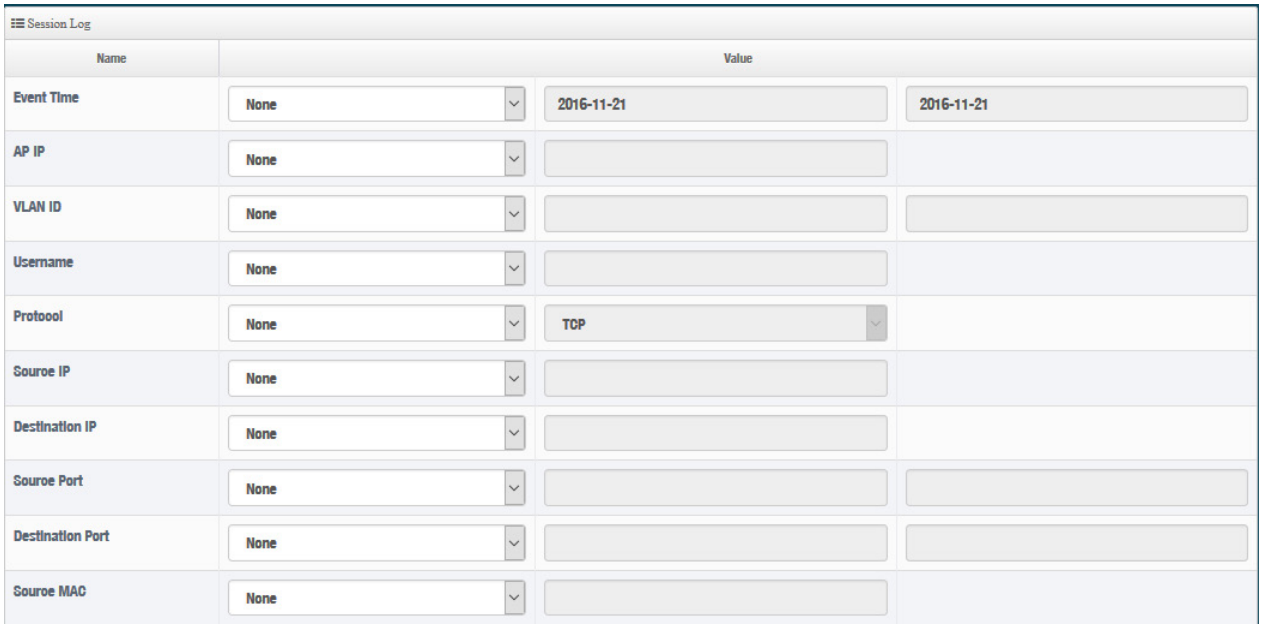
系統狀態主要顯示系統相關資訊，包含系統網路資訊，系統 CPU/memory/Log 等資訊及 WAN 連線資訊。

7.2 本機系統日誌

系統日誌主要是紀錄系統啟動和運行時顯示系統事件。 此外，當系統中遇到問題時，它作為故障排除工具非常有用。

7.3 Session 日誌

此為系統日誌伺服器的日誌紀錄，同時也可將網路環境架構中有使用 CERIO 的 AP 並啟用 syslog 功能也將 CERIO AP 的 Session 的日誌存至此日誌伺服器，該頁面同時也可以記錄 CERIO AP 的 session 日誌以供整體架構管理。 此功能頁面內建智能搜索功能，管理員可以使用關鍵字或日期方法詳細搜尋設備的 session 資料。



管理員可在這智能搜尋引擎依照需求選擇或輸入條件，進行 session 日誌資料搜索。

- **None:** 不設條件限制，搜尋全部資料
- **Greater then:** 搜尋大於所定義值的資料。
- **Equal:** 搜尋絕對等於所定義值的資料。
- **Less then:** 搜尋小於所定義值的資料。
- **Between:** 搜尋一個區間內所定義值的資料。
- **Like:** 搜尋跟設定值相關的資料。
-

Session Log List

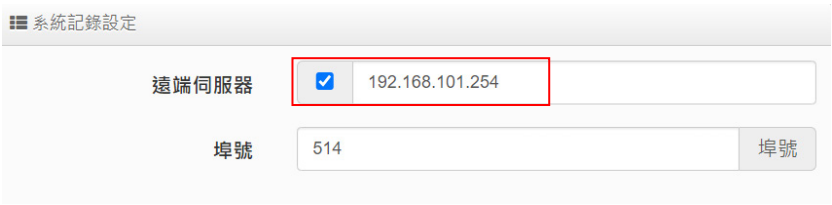
#	Event Time	AP IP	VLAN ID	Username	Protocol	Source IP	Destination IP	Source Port	Destination Port	Source MAC
1	2015-01-01 08:01:41	192.168.2.254	0	test	UDP	192.168.2.10		62461	1900	8C:4D:EA:02:C6:EC
2	2015-01-01 08:01:41	192.168.2.254	0	test	TCP	192.168.2.10		62362	443	8C:4D:EA:02:C6:EC
3	2015-01-01 08:01:42	192.168.2.254	0	test	UDP	192.168.2.10		59448	53	8C:4D:EA:02:C6:EC
4	2015-01-01 08:01:42	192.168.2.254	0	test	UDP	192.168.2.10		54064	53	8C:4D:EA:02:C6:EC
5	2015-01-01 08:01:42	192.168.2.254	0	test	UDP	192.168.2.10		53759	53	8C:4D:EA:02:C6:EC
6	2015-01-01 08:01:42	192.168.2.254	0	test	TCP	192.168.2.10		62364	443	8C:4D:EA:02:C6:EC
7	2015-01-01 08:01:44	192.168.2.254	0	test	UDP	192.168.2.10		62461	1900	8C:4D:EA:02:C6:EC
8	2015-01-01 08:01:46	192.168.2.254	0	test	TCP	192.168.2.10		62366	443	8C:4D:EA:02:C6:EC
9	2015-01-01 08:01:46	192.168.2.254	0	test	UDP	192.168.2.10		57436	53	8C:4D:EA:02:C6:EC
10	2015-01-01 08:01:46	192.168.2.254	0	test	TCP	192.168.2.10		62367	5222	8C:4D:EA:02:C6:EC
11	2015-01-01 08:01:47	192.168.2.254	0	test	UDP	192.168.2.10		62461	1900	8C:4D:EA:02:C6:EC
12	2015-01-01 08:01:48	192.168.2.254	0	test	TCP	192.168.2.10		62368	80	8C:4D:EA:02:C6:EC

您可以將 Cerio AP 的”Session log”日誌儲存到此 Session 日誌伺服器，請進入 Cerio AP 的管理設定並設定「系統日誌設定」將 IP 指向本主機 IP 位址並啟用 Cerio AP 功能的 Session log 功能。

 # 以下為 Cerio AP 的相關設定簡易說明。

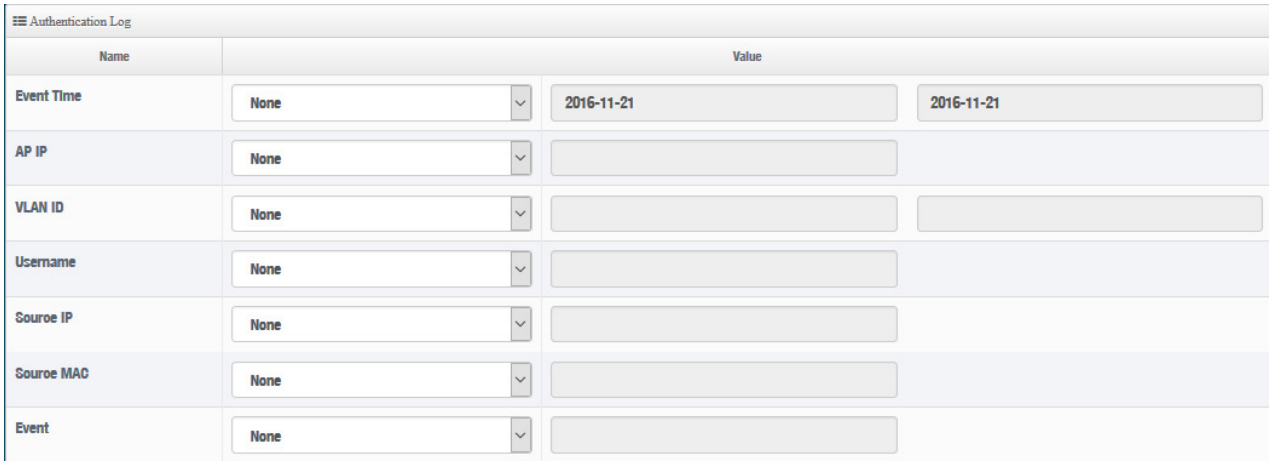
#相關設定 1： 請點選 Cerio AP 的**“系統”➔”網頁認證功能”** 啟用”Session Log” 設定。.

#相關設定 2： 請點選 Cerio AP 的**“系統管理”➔”系統紀錄設定”** 勾選啟用”遠端伺服器”並填入指定本機器(AP 的遠端伺服器)的 IP 位置設定。.



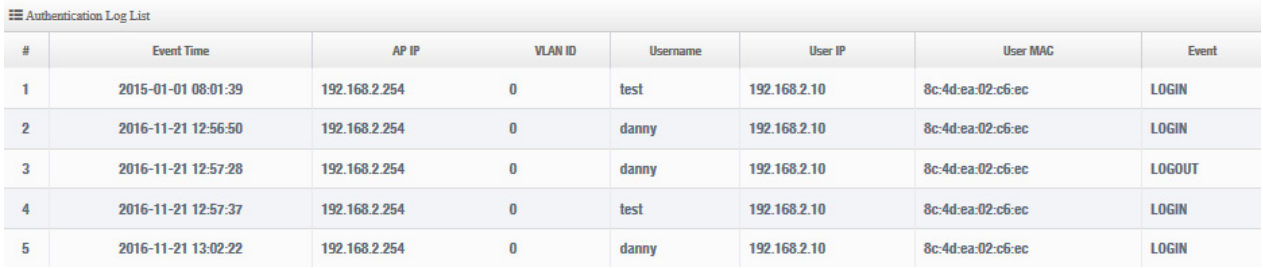
7.4 認證日誌

此為系統日誌伺服器的日誌紀錄，同時也可將網路環境架構中有使用 CERIO 的 AP 並啟用 syslog 功能將認證功能的認證相關日誌存至此日誌伺服器，該頁面可以記錄 CERIO AP 的網頁認證日誌。 此功能頁面內建智能搜索功能，管理員可以使用關鍵字或日期方法詳細搜尋網頁認證的帳戶紀錄資料。



管理員可在這智能搜尋引擎依照需求選擇或輸入條件，進行網頁認證帳戶日誌資料搜索。

- **None:** 不設條件限制，搜尋全部資料
- **Greater then:** 搜尋大於所定義值的資料。
- **Equal:** 搜尋絕對等於所定義值的資料。
- **Less then:** 搜尋小於所定義值的資料。
- **Between:** 搜尋一個區間內所定義值的資料。
- **Like:** 搜尋跟設定值相關的資料。



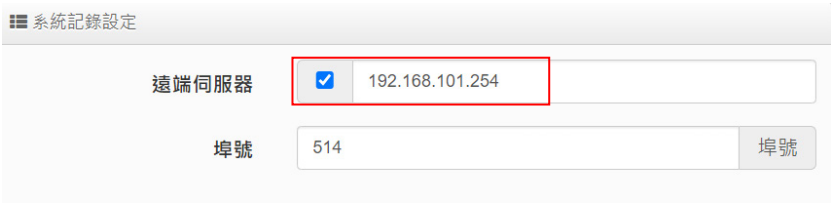
#	Event Time	AP IP	VLAN ID	Username	User IP	User MAC	Event
1	2015-01-01 08:01:39	192.168.2.254	0	test	192.168.2.10	8c:4d:ea:02:c6:ec	LOGIN
2	2016-11-21 12:56:50	192.168.2.254	0	danny	192.168.2.10	8c:4d:ea:02:c6:ec	LOGIN
3	2016-11-21 12:57:28	192.168.2.254	0	danny	192.168.2.10	8c:4d:ea:02:c6:ec	LOGOUT
4	2016-11-21 12:57:37	192.168.2.254	0	test	192.168.2.10	8c:4d:ea:02:c6:ec	LOGIN
5	2016-11-21 13:02:22	192.168.2.254	0	danny	192.168.2.10	8c:4d:ea:02:c6:ec	LOGIN

您可以將 Cerio AP 的”認證日誌”儲存到此認證日誌伺服器內，請進入 Cerio AP 的管理設定並設定「系統日誌設定」將 IP 指向本主機 IP 位址並啟用 Cerio AP 功能的 Session log 功能。

 # 以下為 Cerio AP 的相關設定簡易說明。

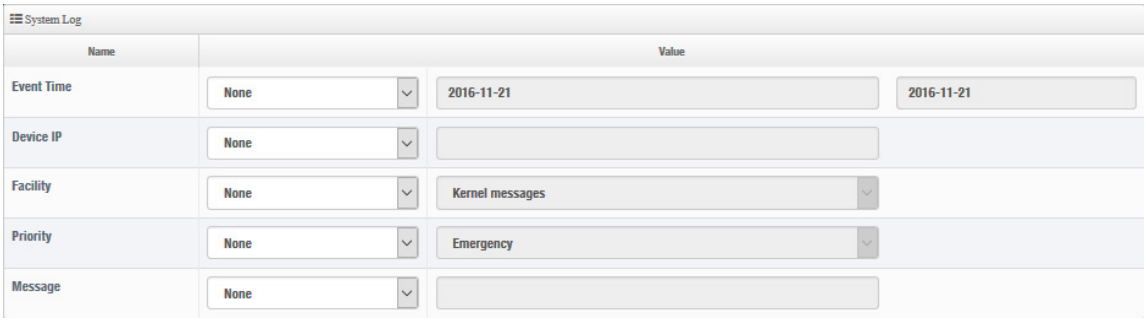
#相關設定 1： 請點選 Cerio AP 的“**系統”➔”網頁認證功能”** 啟用”認證日誌”設定。.

#相關設定 2： 請點選 Cerio AP 的**“系統管理”➔”系統紀錄設定”** 勾選啟用”遠端伺服器”並填入指定本機器(AP 的遠端伺服器)的 IP 位置設定。.



7.5 遠端系統日誌

此為系統日誌伺服器的日誌紀錄，同時也可將網路環境架構中有使用 CERIO 的 AP 並啟用 syslog 功能將設備的系統日誌資料存至此日誌伺服器，該頁面同時也可以記錄 CERIO AP 的系統日誌。 此功能頁面內建智能搜索功能，管理員可以使用關鍵字或日期方法詳細搜尋設備的系統日誌資料。



管理員可在這智能搜尋引擎依照需求選擇或輸入條件，進行設備的系統日誌資料搜索。

- **None:** 不設條件限制，搜尋全部資料
- **Greater then:** 搜尋大於所定義值的資料。

- **Equal:** 搜尋絕對等於所定義值的資料。
- **Less then:** 搜尋小於所定義值的資料。
- **Between:** 搜尋一個區間內所定義值的資料。
- **Like:** 搜尋跟設定值相關的資料。

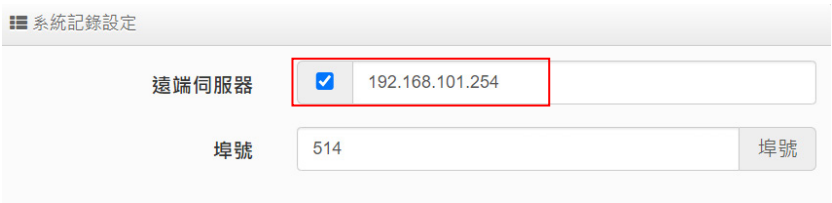
System Log List

#	Event Time	AP IP	Facility	Priority	Message
1	2016-01-01 08:00:00	192.168.2.254	user	Informational	PPP BSD Compression module registered
2	2016-01-01 08:00:00	192.168.2.254	user	Informational	PPP MPPE Compression module registered
3	2016-01-01 08:00:00	192.168.2.254	user	Informational	NET: Registered protocol family 24
4	2016-01-01 08:00:00	192.168.2.254	local0	Informational	started, version 2.22 cachesize 150
5	2016-01-01 08:00:00	192.168.2.254	local0	Informational	cleared cache
6	2016-01-01 08:00:00	192.168.2.254	local0	Informational	reading /etc/resolv.conf
7	2016-01-01 08:00:00	192.168.2.254	local0	Informational	using nameserver 192.168.2.1#53
8	2016-01-01 08:00:00	192.168.2.254	user	Informational	PPPoL2TP kernel driver, V1.0

您可以將 Cerio AP 的”系統日誌”儲存到此”遠端系統日誌伺服器”，請進入 Cerio AP 的管理設定並設定「系統日誌設定」將 IP 指向本主機 IP 位址功能。

 # 以下為 Cerio AP 的相關設定簡易說明。

#相關設定 1： 請點選 Cerio AP 的“**系統管理”➔”系統紀錄設定”** 勾選啟用”遠端伺服器”並填入指定本機器(AP 的遠端伺服器)的 IP 位置設定。.

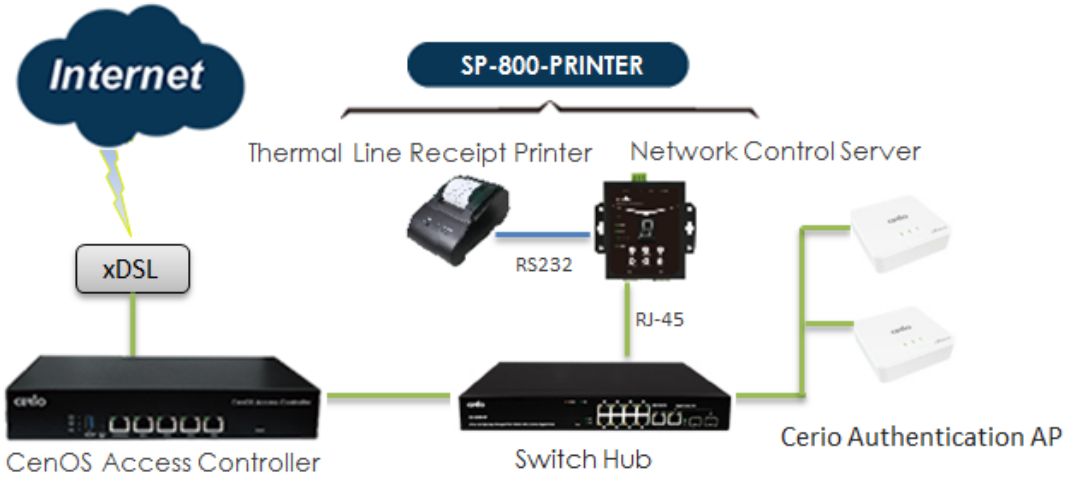


8. 技術文件

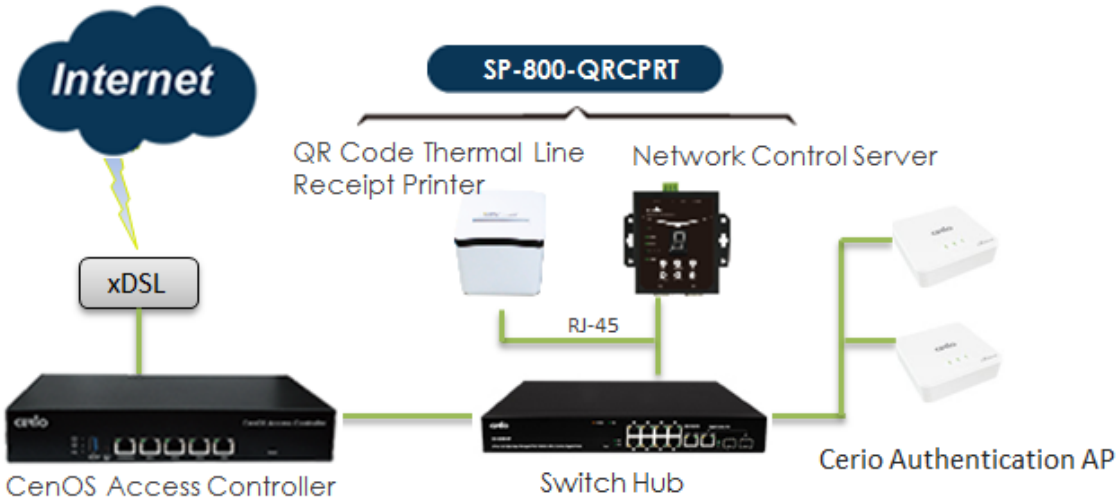
8.1 熱點認證使用 POS 系統

POS 系統為熱點認證功能專用**網路控制伺服器+熱感式印表機**，主要能可透過”**網路控制伺服器”去**控制認證設備讓 CenOS 系統自動產生認證帳戶碼，並利用熱感式印表機將產生的帳戶列印輸出成票券，”**網路控制伺服器”**可搭載普通型及 QR Code 兩種熱感式列印票券機，展現帳戶即時輸出方便作業之效能。

搭載 SP-800-PRINTER 之 POS 認證系統應用圖

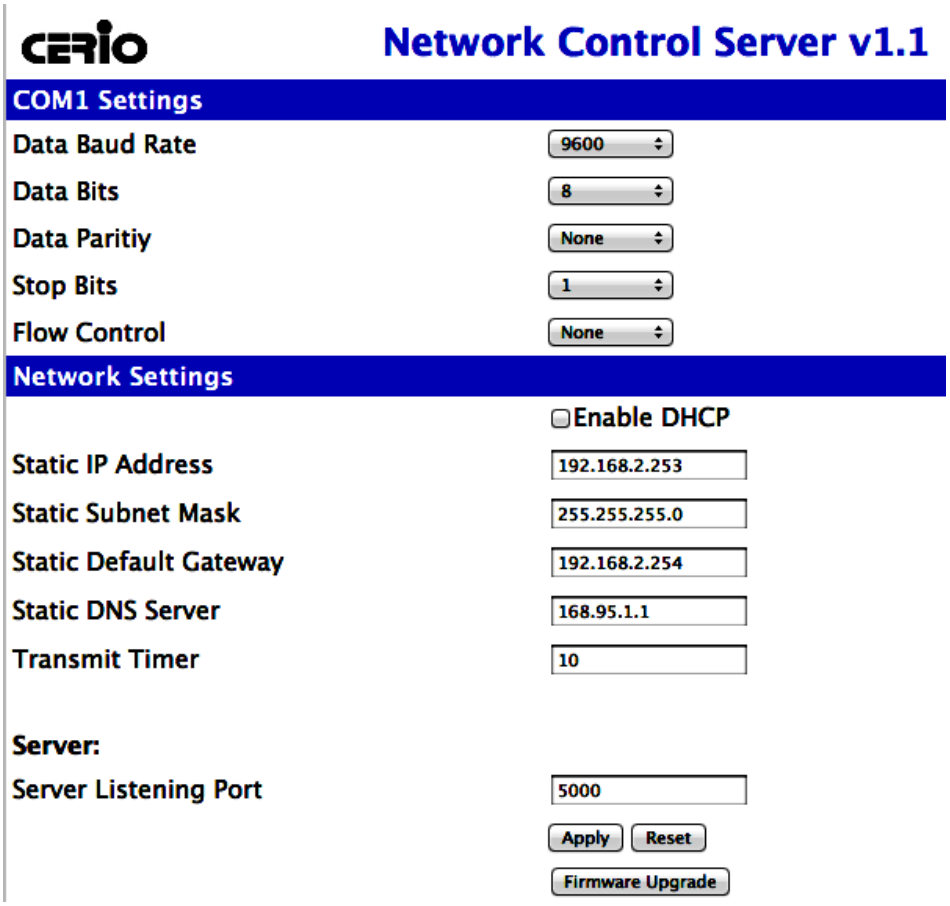


搭載 SP-800-QRCPRT 之 POS 認證系統應用圖



登入網路控制伺服器管理介面

網路控制伺服器(SP-800)內建 WEB 設定介面，當完成硬體安裝後，管理人員可透過網路線連接 PC / NB，將電腦 IP 設為 192.168.2.X 並開啟 Internet Explorer 或 Firefox 瀏覽器，即可連結登入 WEB 介面設定，開啟瀏覽器後，請輸入 **http://192.168.2.253/setting.htm** 網址進入 WEB 畫面，成功登入後將會出現如下畫面



- **COM1 Setting:** 建議使用預設值即可。
- **Network Setting:**
  - **Enable DHCP:** 此功能若啟用，系統將自動向 DHCP 伺服器索取 IP 位址，建議不啟用，管理者自行輸入 SP-800 系統的 IP 位置。
  - 輸入 IP 位址/MASK/Gateway 閘道位址等
  - **Static DNS Server:** 可輸入 DNS IP 位址。
  - **Transmit Timer:** 設定每多少毫秒偵測一次認證伺服器連線狀況，建議預設值即可。
  - **Server Listening Port:** 設定與認證伺服器連接 Port 號

確認設定完成後，請點擊 Apply 按鈕完成儲存設定

普通型熱感式印表機安裝

熱感紙安裝步驟

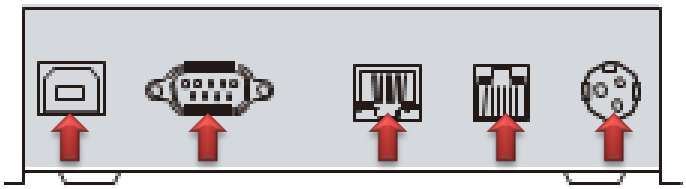
1) 掀起印表機上方蓋
2) 放入熱感紙捲並將熱感紙捲抽出一小截至外
3) 確認後將蓋上印表機上蓋，並完整夾住熱感紙

熱感式印表機安裝說明

1) 連接”**網路控制伺服器**”的 Console 埠
2) DC 直流電接孔
3) 電源開關

QR Code 熱感式印表機安裝

在 QR Code 熱感式印表機背面，可連接電源/網路線/RJ-11/Console 及 USB 介面等接孔，如下說明



USB 埠　Console 埠　RJ-45 埠　RJ-11 埠　DC in

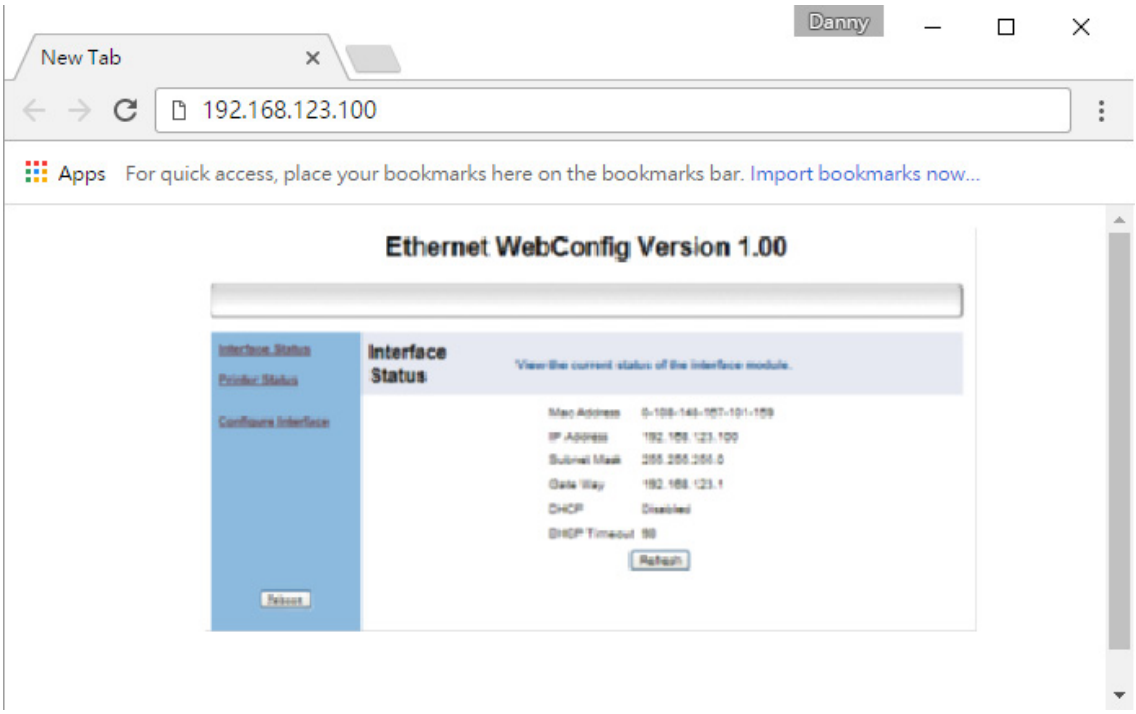
提醒: 若整體環境架設認證 POS 系統僅需連接 DC 電源及 RJ-45 埠即可

管理頁面登入設定

此 QR Code 熱感式印表機支援 Web 管理介面，管理者可先登入管理介面修改 QR Code 熱感式印表機的 IP 位址來完成架設程序。

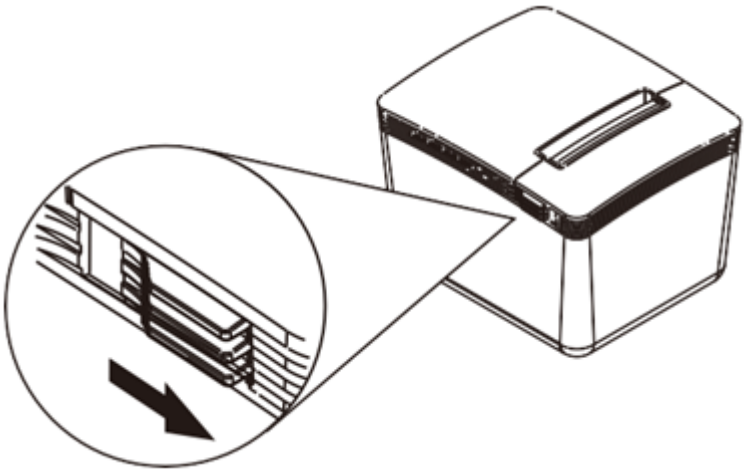
QR Code 熱感式印表機預設 IP 位址: 192.168.123.100 ，管理人員須將 PC 設定與印表機同網段之 IP 位址如:192.168.123.200 後,開啟瀏覽器並輸入印表機 IP 位址即可。

管理頁面如下圖所示

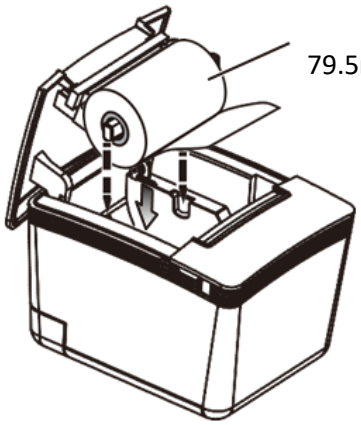


QR Code 熱感式印表機安裝說明

1) 打開 QR Code 熱感式印表機上蓋，請在左側位置將上蓋卡隼向前推壓即可開啟

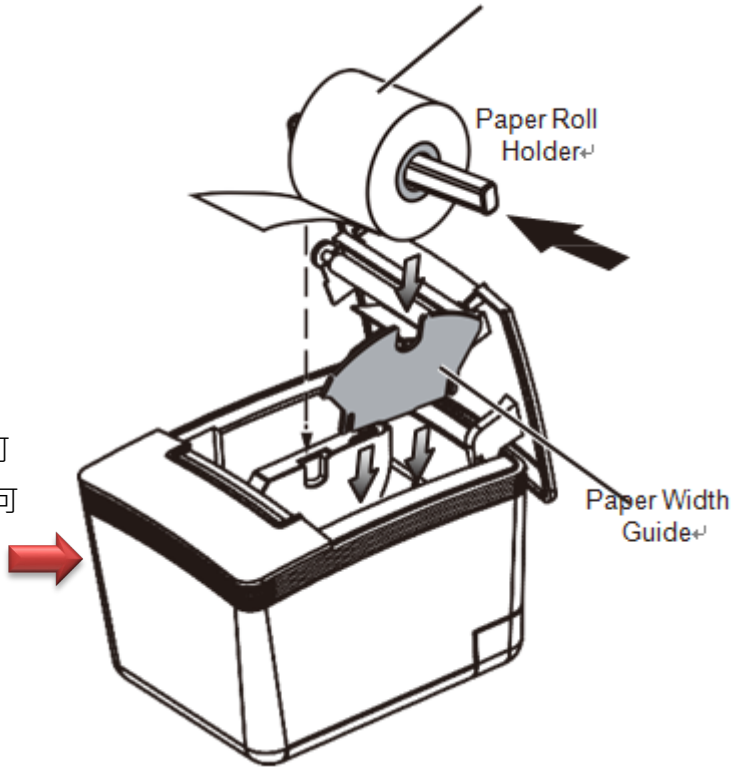


2) 此 QR Code 熱感式印表機支援 79.5mm± 0.5mm 寬度尺寸以下(包含)，請將熱感紙捲架穿過熱感紙後放入並將熱感紙捲抽出一小截至外



79.5mm 尺寸熱感紙直接放入於槽內

57.5mm 尺寸熱感紙可搭配件組裝

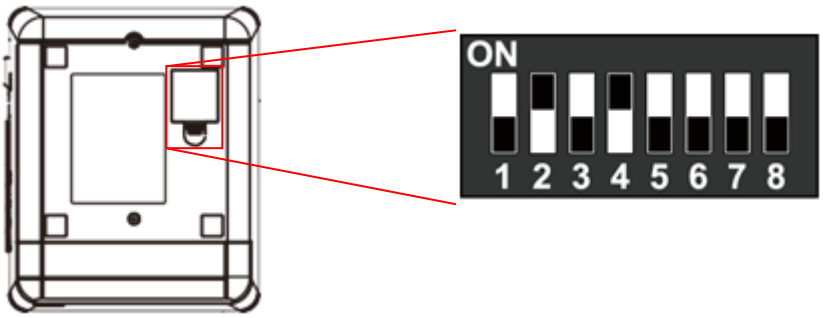


若熱感紙尺寸使用 57.5mm，則可搭配附件紙張寬度導軌片固定，可避免紙捲移動。

3) 確認後蓋上即完成熱感紙安裝

QR Code 熱感式印表機 DIP 切換設定

在印表機下方有設置 DIP 切換功能, 如下表格對照



DIP	Function	ON	OFF
1	Paper Cutter	No	Yes*
2	Audio Alarm	Yes *	No
3	Print Density	Dark	Light *
4	Two-byte Character Code	*No	Yes
5	Character Per Line	42	48 *
6	Cutter with Cash Drawer	Yes	No *
7 & 8	Baud Rate Setting	---	OFF*

認證 POS 系統架構設定步驟

帳戶票卷輸出器 POS 系統需與 CERIO 的認證管理器結合，透過”**網路控制伺服器”**讓認證管理器自動產生認證帳戶，並由印表機列印輸出，可參考”熱點認證使用 POS 系統”內的應用架構說明

架設整體的熱點認證及帳戶產生輸出 POS 系統步驟，如下

＃設定 CERIO 的 CenOS 認證管理器

(以 CERIO DR-5000 閘道認證管理控制器為例)

步驟一

先進入**”網路控制伺服器”**設定 IP 位址，非必要其他功能設定無須修改

可參考”**登入網路控制伺服器管理介面**”之操作

步驟二

若使用 QR Code 熱感式印表機，請登入 QR Code 熱感式印表機的管理介面，更改與網路環境同網段之 IP 位址

可參考"QR Code 熱感式印表機安裝"的管理頁面登入設定

步驟三

進入 CERIO DR-5000 管理頁面(可參考 DR-5000 使用手冊)開啟 RADIUS Server，並設定 RADIUS Server 的登入驗證碼。在**"帳戶設定"➔"RADIUS 伺服器"**, 如下圖所示

步驟四

進入 CERIO DR-5000 管理頁面（可參考 DR-5000 使用手冊）後，進入**"帳戶設定"➔"設定熱感式印表機"**, 如下圖 DR-5000 設定頁面

a. 若環境只架設一台**"網路控制伺服器"**，直接在第一筆欄位點擊右方的 Setup 按鈕

b. 進入後請選擇啟用功能，並開始設定

- **IP 位址:** 輸入"**網路控制伺服器**"的 IP 位址(可參考"**登入網路控制伺服器管理介面**")說明
- **Command port:** 輸入"**網路控制伺服器**"的"**Server Listening Port**"碼 (可參考"**登入網路控制伺服器管理介面**")
- **印表機類型:** 可選擇使用普通或 QR Code 型的熱感式印表機，依照採購印表機類型決定選擇。
- **選擇 QR code 的熱感式印表機：**將出現以下設定頁面

- ✓ **印表機 IP 位址：**請輸入熱感式印表機的 IP 位址(可參考"**QR Code 熱感式印表機安裝**")說明。
- ✓ **印表機 Port：**SP-800 與 QR Code 熱感式印表機使用網路溝通的 Port 號。(若採用 Cerio 所搭配的 QR Code 熱感式印表機則為 9100 Port)
- ✓ **QR Code 類型：**管理者可以選擇是否列印 QR Code，QR Code 大小可以選擇。
- **COM Port:** 選擇熱感式印表機的連接方式。

Notice

1. **若選擇普通的熱感式印表接且連接在 SP-800 的 COM1 上，則請選擇 COM1，**
2. **若選擇 QR Ccode 熱感式印表機，則建議選擇 RJ-45 方式**
3. **QR Code 熱感式印表機的 IP 位址必須與網路環境相同網段。**

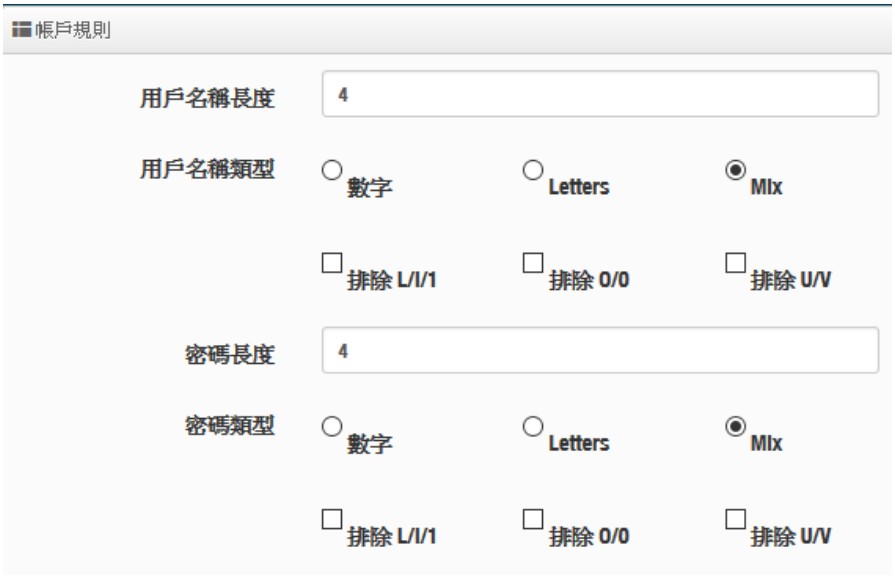
- **New Look Password：**輸入 SP-800 與 DR-5000 連結的按鈕密鑰，假如 SP-800 有啟動密碼鎖，則解鎖碼在此設定。
- **系統描述：**可輸入此設定的描述。

c. 以上設定確認後儲存，即完成帳戶票卷輸出器 POS 系統與認證管理器結合啟用

步驟五

在認證管理器(DR-5000)啟動票券帳戶功能，管理員可在認證管理器管理介面的**"帳戶設定"➔"Package 設定"**下新增建立帳戶票券的使用類型, 如下說明

- Package 名稱：輸入此規則的票券的名稱。
- 系統描述：輸入此規則的描述，方便管理者辨識。
- 票券流量/session 時間/Expire After/到期：此功能將為限制帳戶的使用時數或流量
- 帳戶規則：可設定自動產的帳戶名稱及密碼的長度和帳密的類型。



假如設定多筆票券帳戶功能完成後，將出現 Package 列表，表頭以 0~9 排序，分別就是**"網路控制伺服器"**上方所顯示的 0~9 選項，若選擇列印 0 表示熱點帳戶的帳密由 Package 0 的規則去產生出來，依此類推。如下圖

Package List

Create New Package

#	Name	Description	Session Time	Traffic Volume	Expire After	Expiration	Action
0	TEST-1	no time		0B			Edit
1	test-2	60Mbps Traffic		60.00MB			Edit
2	test-3	use 120 minutes time	2Hour(s)	0B			Edit
3	Test-4	use 120 minutes expi...		0B	2Hour(s)		Edit

以上步驟設定完成重新啟動後，將達成**"網路控制伺服器"**去控制**"認證管理器(DR-5000)"**讓系統自動產生帳戶並列印出來。

步驟六

進入設定系統時間，為了讓認證帳戶產生的時間是確實正確，必須先確實讓系統的時間與時間伺服器是一致性的，請進入**"系統設定"➔"時間伺服器"**設定。

系統時間

目前本地端時間	2016/11/23 14:39:15	
模式	◉ NTP伺服器	○ 手動

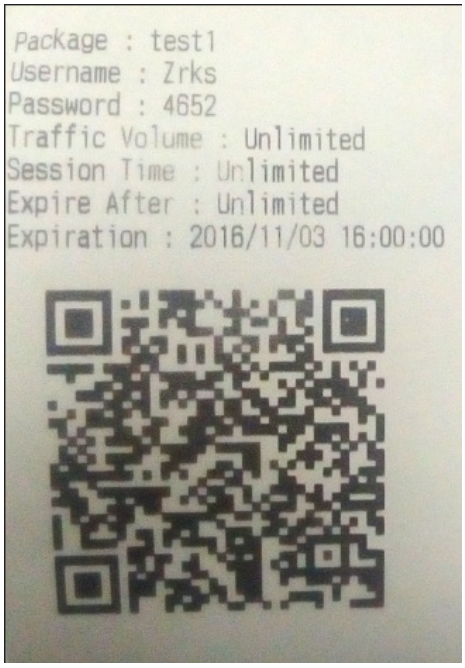
步驟七

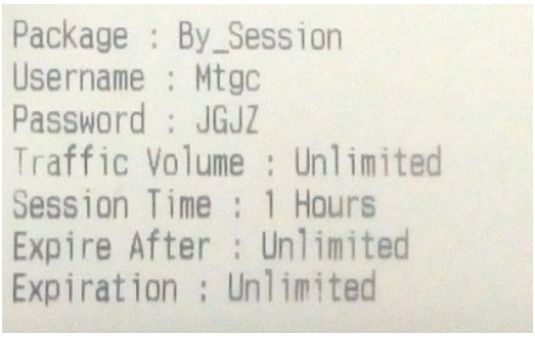
啟用網頁認證功能，請進入**"系統設定"➔"網頁認證功能"**

虛擬網路列表

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

設定完成後，可由網路控制伺服器去選擇項目，而帳密將由熱感式印表機列印呈現出票券，如下圖票券樣本



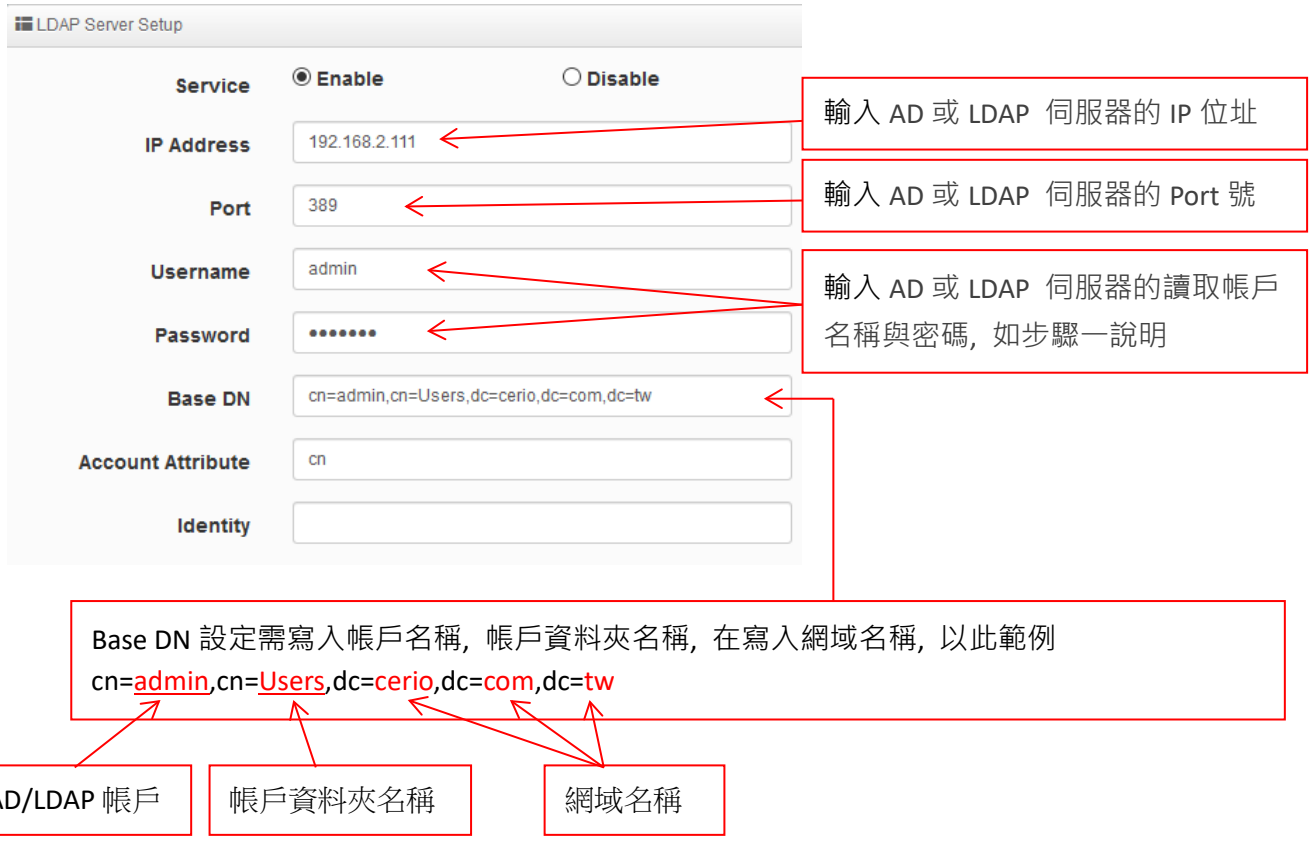


8.2 LDAP(AD)設定範例

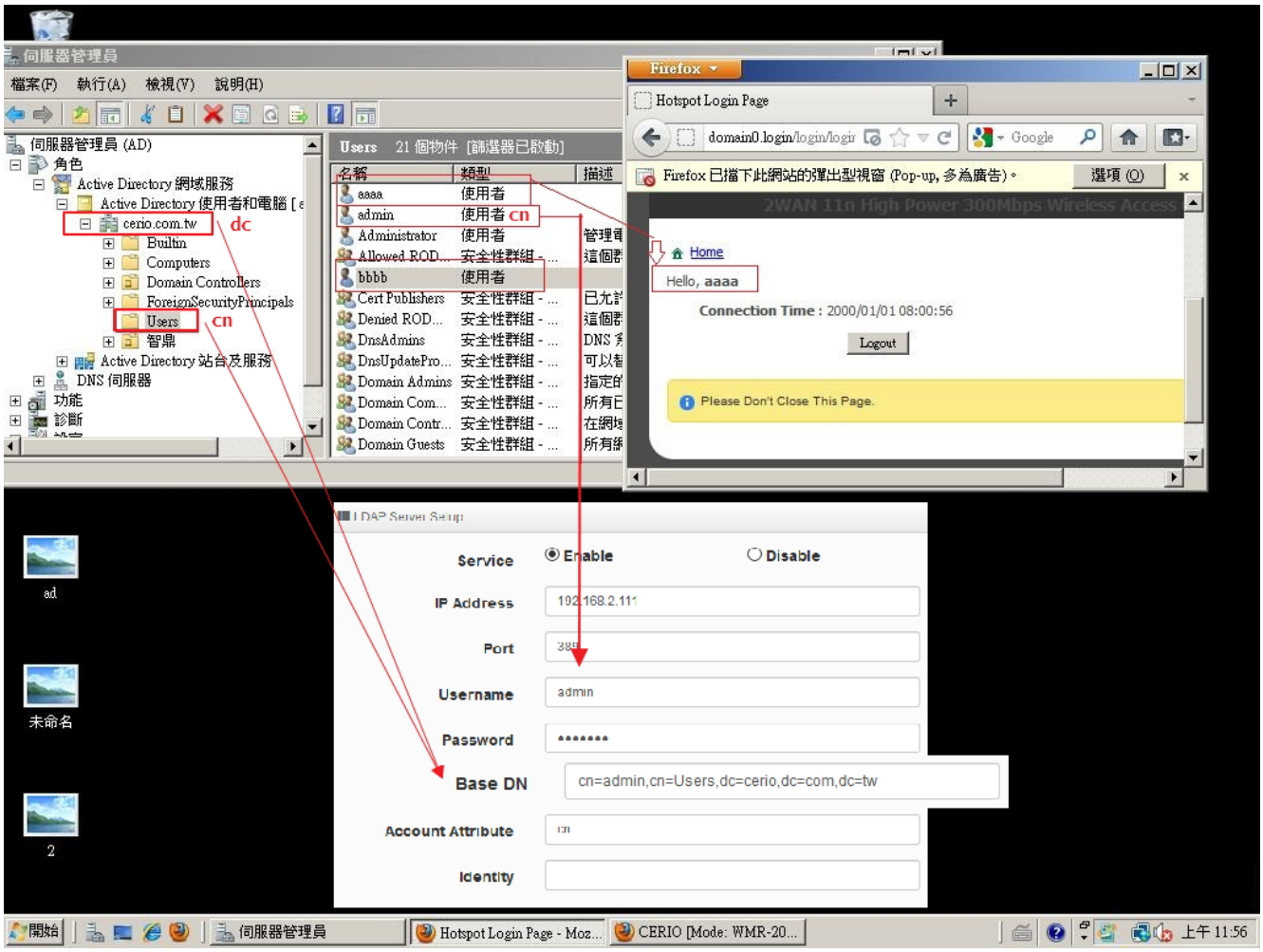
假如網路環境架構中，已經有架設一台 AD 或 LDAP 伺服器時，此 DR-5000 的 RADIUS 伺服器可以與現有的 AD 或 LDAP 伺服器整合，簡單說就是 RADIUS 伺服器會向 AD 或 LDAP 伺服器訪問，建置方式如下說明

假設 AD 或 LDAP 伺服器的網域名稱為 cerio.com.tw，而此網域的帳戶建置在 Users 資料夾內
此時我們可以先在帳戶資料夾內新增一組帳戶給 RADIUS 伺服器去讀取
步驟一:
在 AD 或 LDAP 伺服器網域的帳戶資料夾內新增一個例如**"admin"**帳戶供 RADIUS 伺服器讀取

步驟二:
確認後可至 DR-5000 的**"Account" ➔ "Remote LDAP Setup"**去建置認證，可參考本手冊的 **5.2 遠端 LDAP 設定**



如下圖詳細圖解說明


伺服器管理員
檔案(F) 執行(A) 檢視(V) 說明(H)
伺服器管理員 (AD)
角色
Active Directory 網域服務
Active Directory 使用者和電腦
cerio.com.tw
dc
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Users
cn
智鼎
Active Directory 站台及服務
DNS 伺服器
功能
診斷
Users 21 個物件 [篩選器已啟動]
名稱 類型 描述
aaaa 使用者
admin 使用者 cn
Administrator 使用者
bbbb 使用者
Cert Publishers 安全性群組 - ...
Denied ROD... 安全性群組 - ...
DnsAdmins 安全性群組 - ...
DnsUpdatePro... 安全性群組 - ...
Domain Admins 安全性群組 - ...
Domain Com... 安全性群組 - ...
Domain Contr... 安全性群組 - ...
Domain Guests 安全性群組 - ...
Firefox
Hotspot Login Page
domain0.login/login/logir
Google
Firefox 已擋下此網站的彈出型視窗 (Pop-up, 多為廣告)。
選項 (O)
2WAN 11n High Power 300Mbps Wireless Access
Home
Hello, aaaa
Connection Time : 2000/01/01 08:00:56
Logout
Please Don't Close This Page.
LDAP Server Setup
Service
Enable
Disable
IP Address
192.168.2.111
Port
389
Username
admin
Password
Base DN
cn=admin,cn=Users,dc=cerio,dc=com,dc=tw
Account Attribute
cn
Identity
ad
未命名
2
開始
伺服器管理員
Hotspot Login Page - Moz...
CERIO [Mode: WMR-20...
上午 11:56