Vigor2928 系列

安全防護路由器

使用手冊

版本: 1.0

韌體版本: V5.4.2

日期: 2026 年 8 月 6 日

智慧財產資訊

版權資訊

版權資訊

本手冊內容使用以下商標:

- Microsoft 為微軟公司註冊商標
- Windows 視窗系列，包括 Windows 8, 10 以及其 Explorer 均屬微軟公司商標
- Apple 以及 Mac OS 均屬蘋果電腦公司的註冊商標
- 其他產品則為各自生產廠商之註冊商標

安全說明和保固

安全說明

- 在設置前請先閱讀安裝說明。
- 由於路由器是複雜的電子產品，請勿自行拆除或是維修本產品。
- 請勿把路由器置於潮濕的環境中，例如浴室。
- 請將本產品放置在足以遮風避雨之處，適合溫度在攝氏 0 度到 40 度之間。
- 請勿將本產品暴露在陽光或是其他熱源下，否則外殼以及零件可能遭到破壞。
- 請勿將 LAN 網線置於戶外，以防電擊危險。
- 儲存設定或韌體升級時，請勿關閉設備電源，否則可能會立即損壞資料。當 TR-069/ACS 伺服器管理路由器時，請在關閉路由器電源前，先中斷路由器的網路連線。
- 請將本產品放置在小孩無法觸及之處。
- 若您想棄置本產品時，請遵守當地的保護環境的法律法規。

保固

自使用者購買日起二年內為保固期限(保固: 原廠一年，需線上註冊加給一年,合計二年)，請將您的購買收據保存二年，因為它可以證明您的購買日期。當本產品發生故障乃導因於製作及(或)零件上的錯誤，只要使用者在保固期間內出示購買證明，居易科技將採取可使產品恢復正常之修理或更換有瑕疵的產品(或零件)，且不收取任何費用。居易科技可自行決定使用全新的或是同等價值且功能相當的再製產品。下列狀況不在本產品的保固範圍內：(1)若產品遭修改、錯誤(不當)使用、不可抗力之外力損害，或不正常的使用，而發生的故障；(2) 隨附軟體或是其他供應商提供的授權軟體；(3) 未嚴重影響產品堪用性的瑕疵。

成為一個註冊用戶

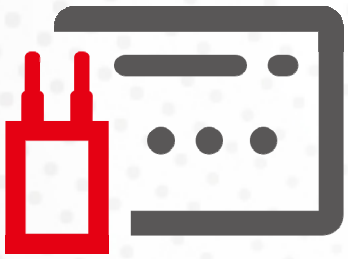
建議在 Web 介面進行註冊。您可以到 https://myvigor.draytek.com 註冊您的 Vigor 路由器。

韌體及工具的更新

請造訪 DrayTek 主頁以獲取有關最新韌體、工具及檔案文件的資訊。
https://www.draytek.com/zh/

目錄

第一章 安装

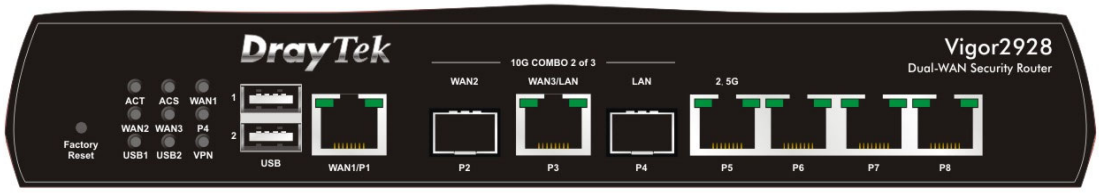


I-1 簡介

不同機種路由器之 LED 顯示面板以及背板連接介面有些許的差異，詳列如下：

I-1-1 Vigor2928 指示燈與介面說明

LED 燈號



LED	狀態	說明
ACT	閃爍	路由器已開機並可正常運作。
	熄燈	路由器已關機。
ACS	亮燈	路由器已註冊且連上 VigorACS 伺服器。
	熄燈	路由器尚未連上 VigorACS 伺服器。
WAN1~3	亮燈	網路介面已透過設定>>WAN 連線啟用。
	熄燈	網際網路尚未預備妥當。
	閃爍	正在傳輸資料中。
USB1~2	亮燈	USB 裝置已連接。
	熄燈	USB 裝置未連接。
	閃爍	正在傳輸資料中。
P4	亮燈	LAN 介面網路已連接。
	熄燈	LAN 介面網路未連接。
	閃爍	正在傳輸資料中。
VPN	亮燈	VPN 通道已建立。
	熄燈	VPN 服務已停用。
	閃爍	資料透過 VPN 通道傳輸中。
WAN1/P1		
Left LED	亮燈	介面網路已連接。
	熄燈	介面網路未連接。
	閃爍	正在傳輸資料中。
Right LED	亮燈	介面的連接速度為 1000 Mbps。
	熄燈	介面的連接速度為 10/100 Mbps。

WAN3/LAN/P3		
Left LED	亮燈	介面網路已連接。
	熄燈	介面網路未連接。
	閃爍	正在傳輸資料中。
Right LED	亮燈	介面的連接速度為 2.5/5/10 Gbps。
	熄燈	介面的連接速度為 10/100Mbps。
LAN P5		
Left LED	亮燈	介面網路已連接。
	熄燈	介面網路未連接。
	閃爍	正在傳輸資料中。
Right LED	亮燈	介面的連接速度為 2.5 Gbps。
	熄燈	介面的連接速度為 10/100Mbps。
LAN P6-P8		
Left LED	亮燈	介面網路已連接。
	熄燈	介面網路未連接。
	閃爍	正在傳輸資料中。
Right LED	亮燈	介面的連接速度為 1000Mbps。
	熄燈	介面的連接速度為 10/100Mbps。

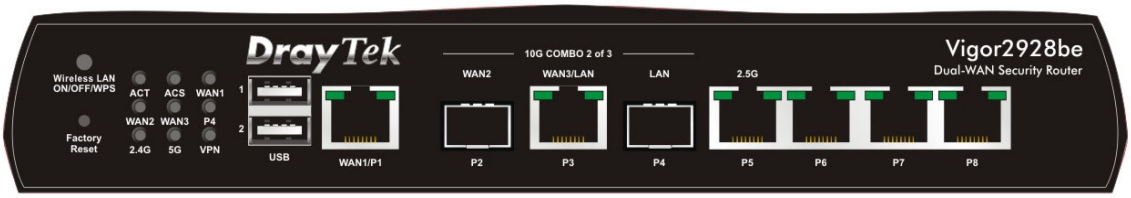
連接器

介面	說明
Factory Reset(出廠預設值按鈕)	還原成出廠預設值。 使用方法：開啟路由器（ACT LED 閃動）。用圓珠筆按下小孔內的按鈕，然後維持 5 秒左右。當您發現 ACT LED 快速閃動時，請鬆開按鈕。路由器隨後將重新啟動，並回復出廠預設值。
USB1~2	連接到 USB 3G/4G 數據機、印表機或是環境溫度計。
WAN1 / P1	連接到本機網路裝置或是數據機裝置。
10G COMBO 2 of 3	可自由選擇任兩個埠口作為 WAN(SPF+ 或 Ethernet)及 LAN 埠口。在此設定中 P2(SPF+)指定為 WAN 埠口；而 P4(SPF+)指定為 LAN 埠口。僅 P3 為可切換功能的乙太網路埠口，亦即該埠口可當 WAN 埠口也可當 LAN 埠口連線。 舉例而言,

	選擇 P2/P3: P2 為 WAN2 埠口; P3 為 LAN 埠口。 選擇 P3/P4: P3 為 WAN3 埠口; P4 為 LAN 埠口。 WAN# - 可連接數據機以便存取網際網路。 LAN - 可連接本機網路設備。
LAN P5~ P8	連接到電腦或網路設備。其中僅 P5 可用於 2.5G 連線。
PWR	連接電源變壓器。
ON/OFF	電源開關。

I-1-2 Vigor2928be 指示燈與介面說明

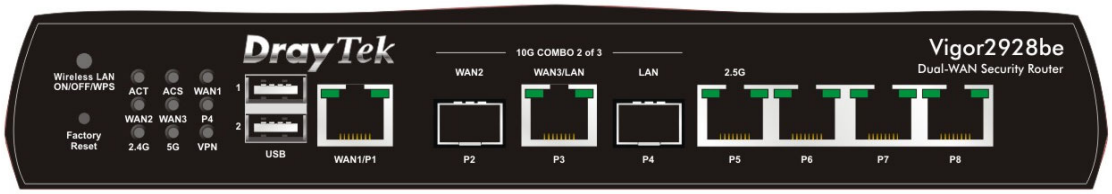
LED 燈號

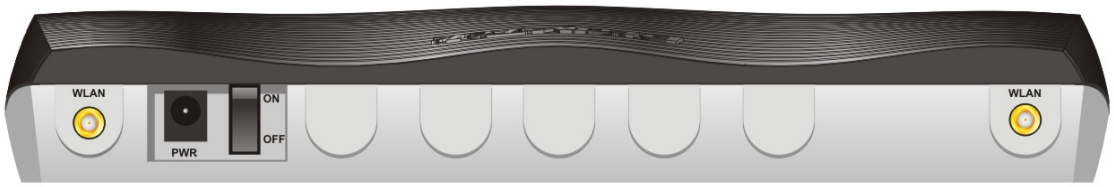


LED	狀態	說明
ACT	閃爍	路由器已開機並可正常運作。
	熄燈	路由器已關機。
ACS	亮燈	路由器已註冊且連上 VigorACS 伺服器。
	熄燈	路由器尚未連上 VigorACS 伺服器。
WAN1~3	亮燈	網路介面已透過設定>>WAN 連線啟用。
	熄燈	網際網路尚未預備妥當。
	閃爍	正在傳輸資料中。
P4	亮燈	LAN 介面網路已連接。
	熄燈	LAN 介面網路未連接。
	閃爍	正在傳輸資料中。
2.4G/5G	亮燈	2.4G/5G: 支援 2.4GHz/5GHz 頻段的無線基地台已準備就緒。 WLAN: 無線基地台已準備就緒。
	熄燈	無線功能已停用。
	閃爍	無線傳輸過程中，指示燈會緩慢閃爍。 當 WPS 運作時，ACT 和 2.4G/5G 指示燈會快速同步閃爍，兩分鐘後恢復正常。(您需要在兩分鐘內完成 WPS 設定)。
VPN	亮燈	VPN 通道已建立。
	熄燈	VPN 服務已停用。
	閃爍	資料透過 VPN 通道傳輸中。
WAN1/P1		
Left LED	亮燈	介面網路已連接。
	熄燈	介面網路未連接。
	閃爍	正在傳輸資料中。
Right LED	亮燈	介面的連接速度為 1000 Mbps。
	熄燈	介面的連接速度為 10/100 Mbps。
WAN3/LAN/P3		
Left LED	亮燈	介面網路已連接。
	熄燈	介面網路未連接。

	閃爍	正在傳輸資料中。
Right LED	亮燈	介面的連接速度為 2.5/5/10 Gbps。
	熄燈	介面的連接速度為 10/100Mbps。
LAN P5		
Left LED	亮燈	介面網路已連接。
	熄燈	介面網路未連接。
	閃爍	正在傳輸資料中。
Right LED	亮燈	介面的連接速度為 2.5 Gbps。
	熄燈	介面的連接速度為 10/100Mbps。
LAN P6-P8		
Left LED	亮燈	介面網路已連接。
	熄燈	介面網路未連接。
	閃爍	正在傳輸資料中。
Right LED	亮燈	介面的連接速度為 1000Mbps。
	熄燈	介面的連接速度為 10/100Mbps。

連接器





介面	說明
Wireless LAN ON/OFF/WPS	無線頻段可透過按鈕按壓與放開等方式進行切換與變更，例如： ● 2.4G (亮燈) 5G (亮燈) – 預設值。 ● 2.4G (熄燈) 5G (亮燈) – 按下並放開按鈕一次。 ● 2.4G (亮燈) 與 5G (熄燈) –按下並放開按鈕二次。 ● 2.4G (熄燈) 與 5G (熄燈) –按下並放開按鈕三次。 當透過網頁使用者介面啟用 WPS 功能時，按住此按鈕 2 秒以上，等待用戶端裝置透過 WPS 與此裝置建立網路連線。
Factory Reset(出廠預設值按鈕)	還原成出廠預設值。 使用方法：開啟路由器(ACT LED 閃動)。用圓珠筆按下小孔內的按鈕，然後維持 5 秒左右。當您發現 ACT LED 快速閃動時，請鬆開按鈕。路由器隨後將重新啟動，並回復出廠預設值。
USB1~2	連接到 USB 3G/4G 數據機、印表機或是環境溫度計。
WAN1 / P1	連接到本機網路裝置或是數據機裝置。

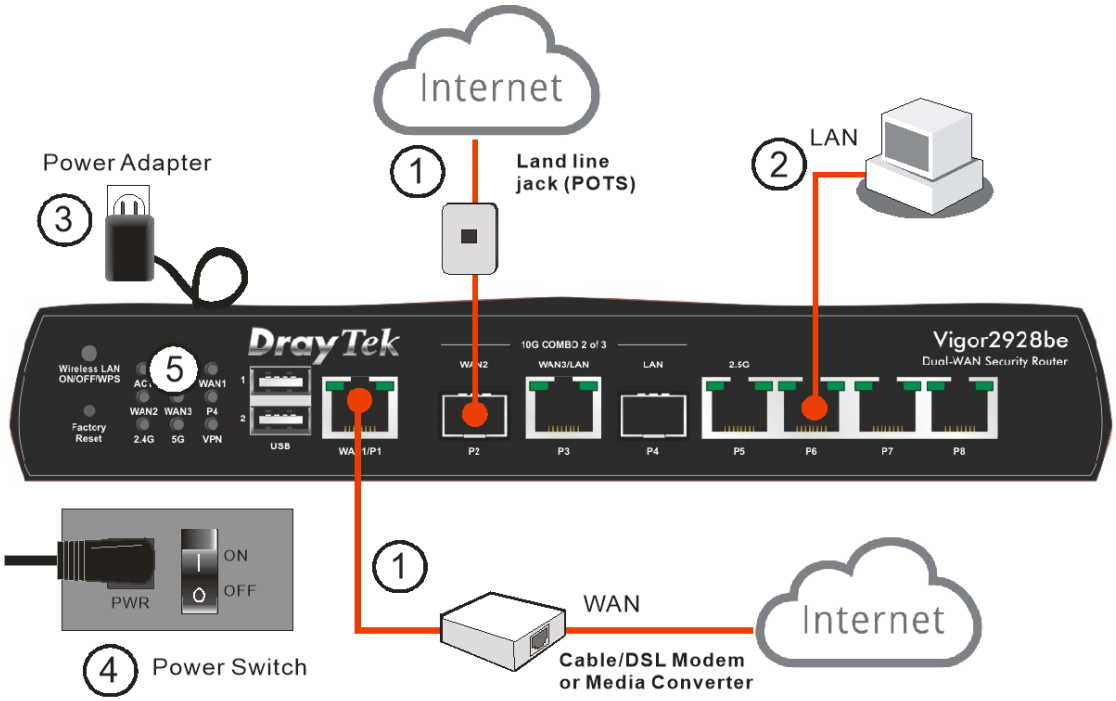
10G COMBO 2 of 3	可自由選擇任兩個埠口作為 WAN(SPF+ 或 Ethernet)及 LAN 埠口。在此設定中 P2(SPF+)指定為 WAN 埠口；而 P4(SPF+)指定為 LAN 埠口。僅 P3 為可切換功能的乙太網路埠口，亦即該埠口可當 WAN 埠口也可當 LAN 埠口連線。 舉例而言, 選擇 P2/P3: P2 為 WAN2 埠口; P3 為 LAN 埠口。 選擇 P3/P4: P3 為 WAN3 埠口; P4 為 LAN 埠口。 WAN# - 可連接數據機以便存取網際網路。 LAN - 可連接本機網路設備。
LAN P5~ P8	連接到電腦或網路設備。其中僅 P5 可用於 2.5G 連線。
PWR	連接電源變壓器。
ON/OFF	電源開關。

I-2 硬體安裝

本節引導您透過硬體連線安裝路由器。

I-2-1 網路連線

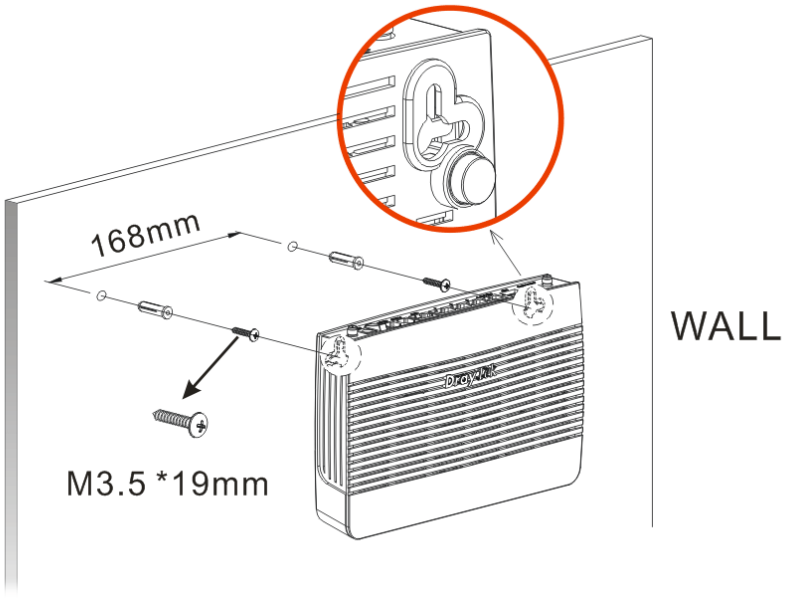
1. 利用乙太網路纜線(RJ-45)連接纜線數據機/DSL 數據機/媒體轉換器至路由器的 WAN 埠口。
2. 利用 RJ-45 纜線連接路由器(LAN 連接埠中選定其中一個)與您的電腦。
3. 將電源轉換器一端連接至路由器，另一端則連至牆上電源輸出孔。
4. 開啟路由器電源。
5. 系統開始初始化，完成測試後，檢查 **ACT** 燈號是否亮燈以確保連線無誤。(有關 LED 狀態的詳細資訊請參考章節 2 面板說明)



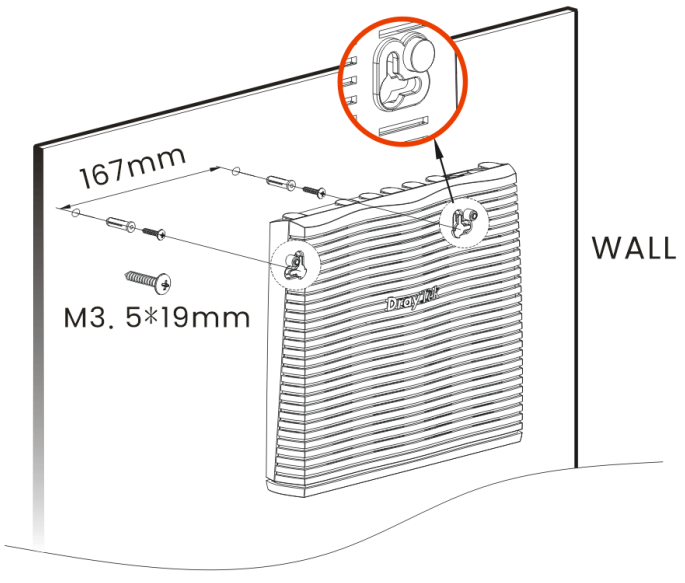
I-2-2 壁掛安裝

Vigor 路由器的背面有鎖孔式的安裝插槽，方便壁掛安裝使用。

1. 請於牆面上鑽鑿孔洞，二孔間的距離如下圖所示。
2. 使用適當類型的螺絲套管鎖進牆壁。
3. 將螺絲穿進路由器然後固定在套管上。



Vigor2928



Vigor2928be

ⓘ附註

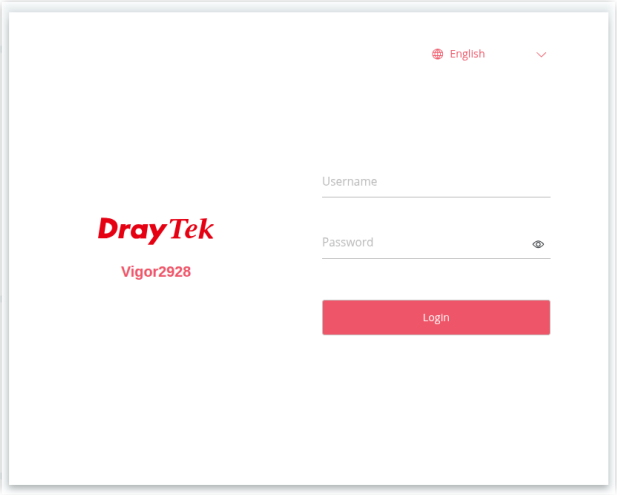
建議的孔洞尺寸為 6.5 釐米(1/4 吋)。

4. 完成上述步驟後，路由器及可穩妥安置在牆壁上。

I-3 進入設定網頁

路由器的功能與設定都可透過網頁使用者介面進行調整，請開啟慣用的網路瀏覽器。

1. 確保您的電腦已經和路由器正確的連接。
2. 開啟網頁瀏覽器並輸入位址 http://192.168.1.1，登入視窗將會出現，並要求輸入帳號與密碼。請輸入 “admin/admin” 並按下登入(**Login**)。



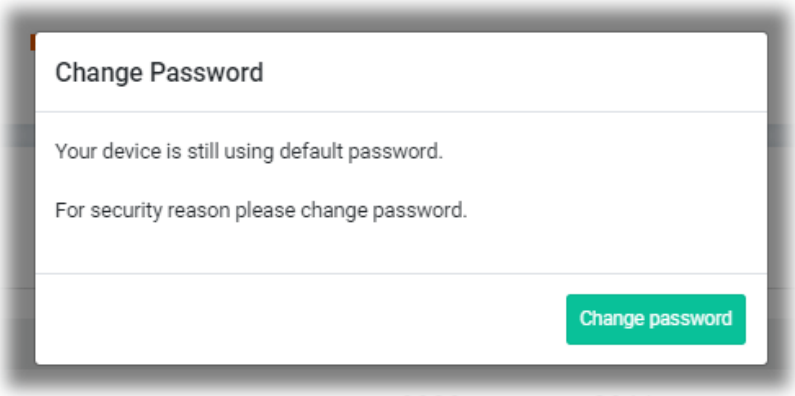
注意:

您可以選擇直接設定電腦的網路設定為動態取得 IP 位址（DHCP），或者是將 IP 設定為和 IP 分享器的預設 IP 位址（**192.168.1.1**）於同一個子網路。如需更多訊息，請參考後面的章節 – 疑難排解。

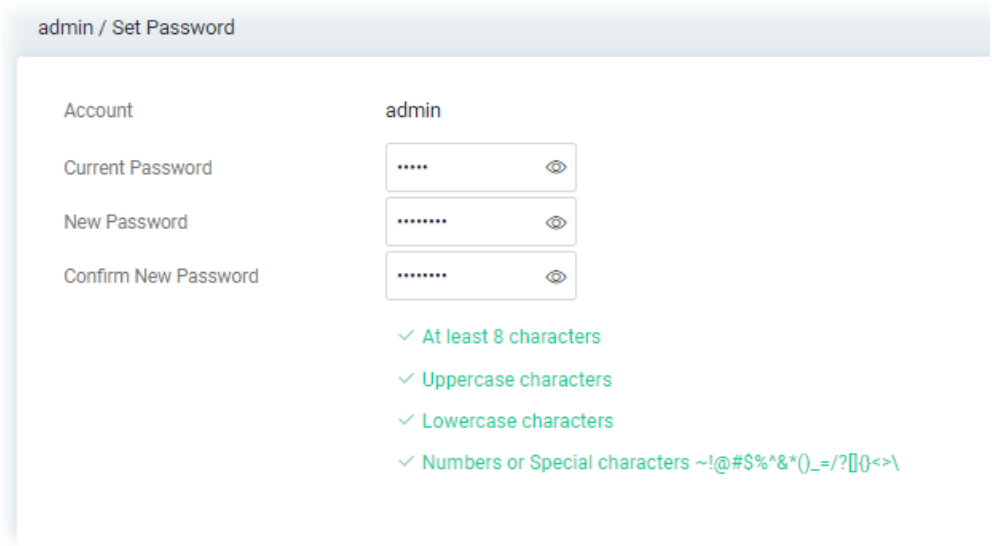
如果您無法進入網頁設定畫面，請參考“疑難排解”以解決您所面臨的問題。

---

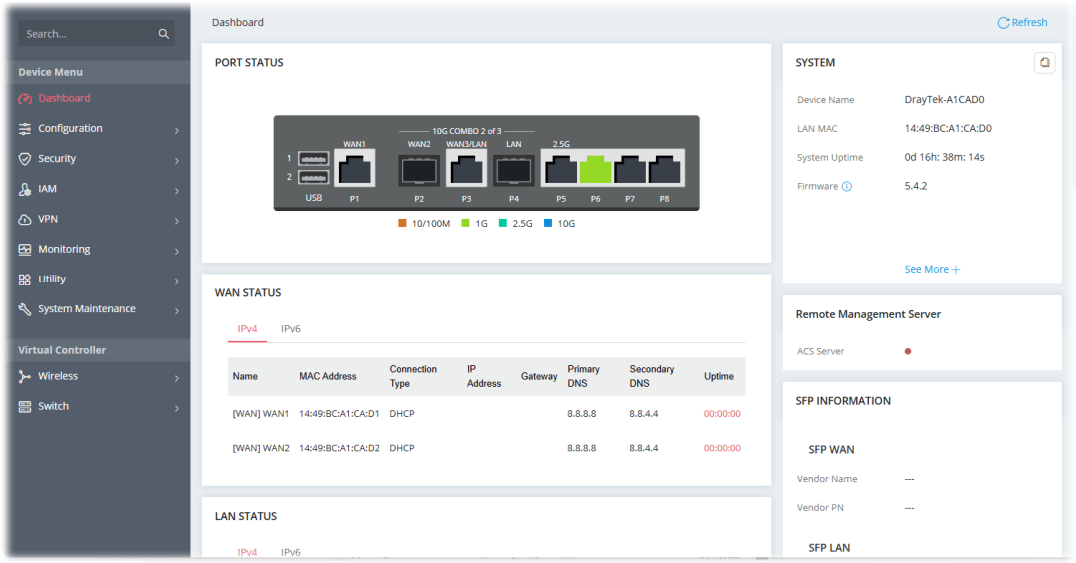
3. 接著，如下的對話盒將會出現，引導您先變更登入密碼。



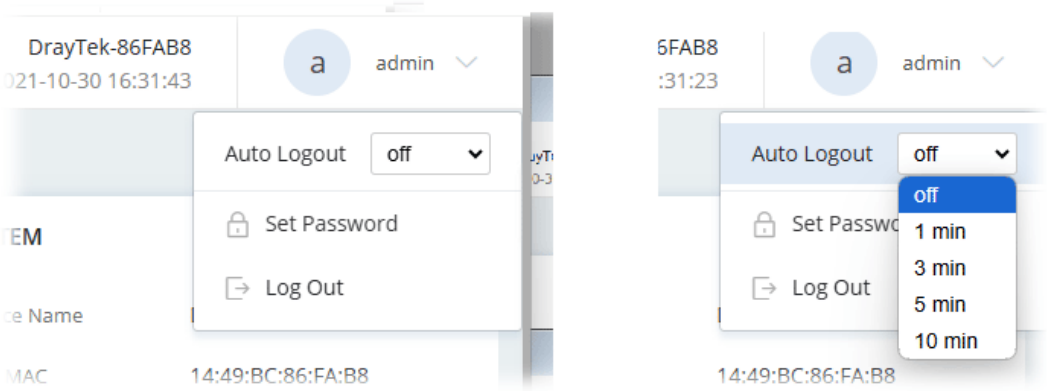
4. 為了網路安全性之故，在您存取路由器的使用者介面之前，您**必須**變更登入密碼。請輸入新密碼。



5. 按下**套用(Apply)**之後，首頁畫面將會呈現如下：



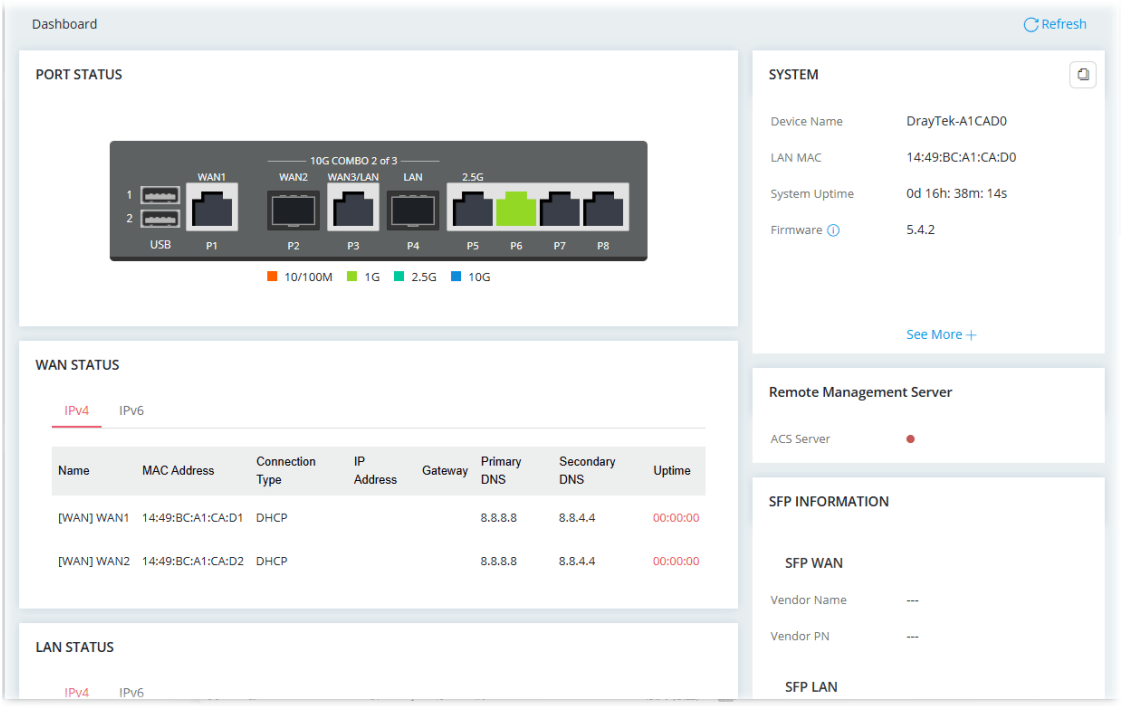
6. 使用者可以透過右上方的**登出(Log Out)**功能或是依照選擇的條件離開設定頁面。預設值通常為自動登出，意即若使用者沒有進行任何動作時，網頁會在 5 分鐘後自動離開，如有需要，您可以變更自動登出的時間設定。



I-4 儀表板簡介

儀表板(Dashboard)顯示各種連線狀態，諸如系統資訊、IPv4 網際網路連線、IPv6 網際網路連線、介面(實體連線)、安全性設定與快速存取等等。

自左手邊的主選單上按下**儀表板(Dashboard)**功能。



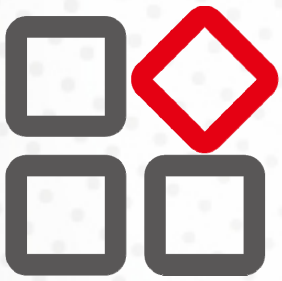
注意:

點擊這兩個圖示即可切換它們。

 - 表示"啟用(Enable)"。

 - 表示"停用(Disable)"。

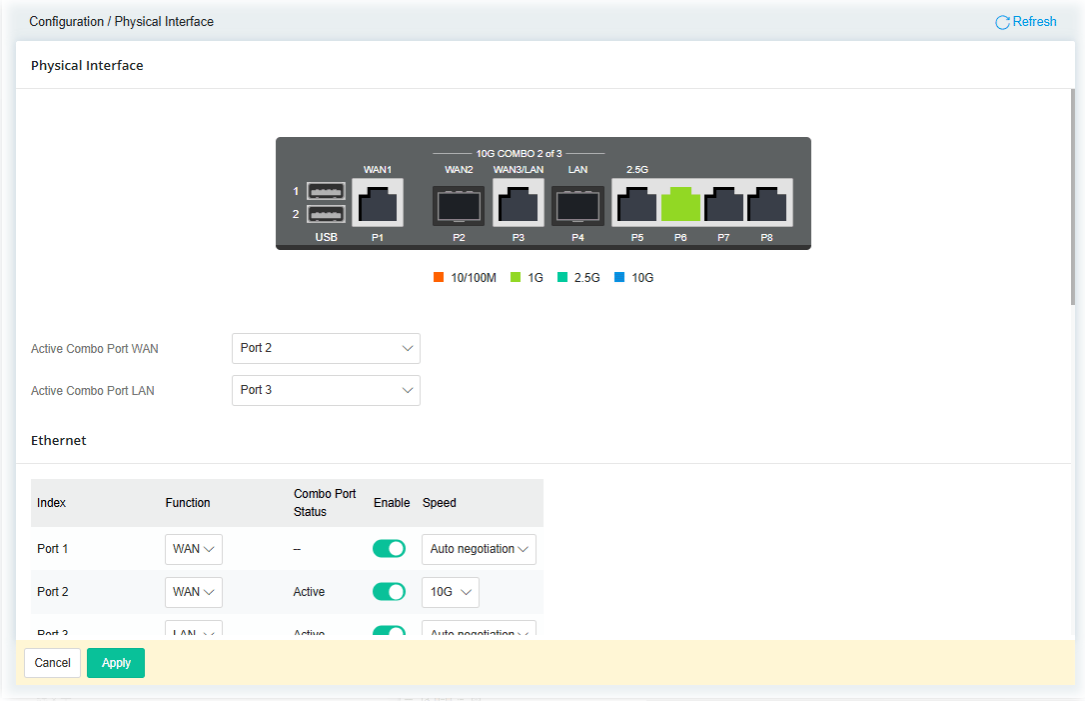
第二章 連線設定



II-1 配置設定(Configuration)

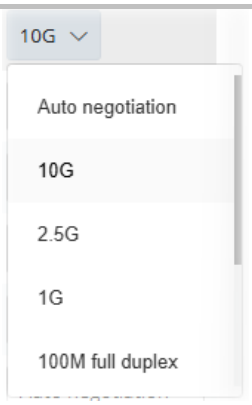
II-1-1 實體介面(Physical Interface)

配置可用介面的一般設定。開啟**設定>>實體介面(Configuration>>Physical Interface)**。



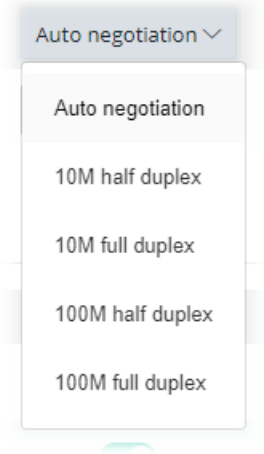
可用設定說明如下：

項目	說明
使用中的 Combo WAN 埠/使用中的 Combo LAN 埠(Active Combo Port WAN & Active Combo Port LAN)	選擇任兩個連接埠口分別作為廣域網路(WAN)埠口（SPF+或乙太網路）和區域網路(LAN)埠口。 在此配置中，連接埠口 2 (SPF+) 被指定為 WAN 埠口，連接埠口 4 (SPF+) 被指定為 LAN 埠口。只有連接埠口 3 是可切換的乙太網路埠口，可用於 WAN 或 LAN 連接。
乙太網路(Ethernet)	
索引編號(Index)	顯示此裝置可用的介面。
功能(Function)	顯示介面類型（WAN 或 LAN）。
Combo Port 狀態 (Combo Port Status)	顯示介面的目前運作狀態（活動或非活動中）。
啟用(Enable)	切換開關以啟用或停用該介面。
速度(Speed)	設定每個介面的連接埠速度能力。



埠口 2 與埠口 4

埠口 5



埠口 1、6、7、8

連接埠速度能力：

自動協商(Auto negotiation) - 自動切換速度，具備所有功能。

10G - 強制使用 10G 連線速率。

2.5G - 強制使用 2.5G 連線速率。

1G - 強制使用 1G 連線速率。

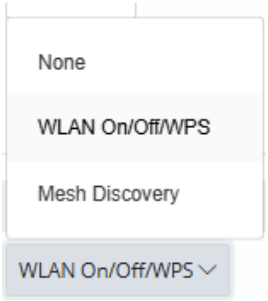
10M 半雙工 - 強制使用 10Mbps 連線速率(單向)。

10M 全雙工 - 強制使用 10Mbps 連線速率(雙向)。

100M 半雙工 - 強制使用 100Mbps 連線速率(單向)。

100M 全雙工 - 強制使用 100Mbps 連線速率(雙向)。

選擇「自動協商」模式後，可讓一個連接埠與對等連接埠自動協商，以獲得雙方都支援的連線速度和雙工模式。啟用自動協商後，路由器上的連接埠會自動與對方協商，以確定連線速度和雙工模式。如果對方連接埠不支援自動

	協商或關閉此功能，路由器將透過偵測電纜上的訊號並使用半雙工模式來確定連線速度。 當路由器的自動協商功能關閉時，連接埠在建立連線時會使用預先設定的速度和雙工模式，因此需要確保對等連接埠的設定相同才能連線。
無線(Wireless)	
介面(Interface)	顯示此裝置可用的無線介面(2.4GHz/5GHz)。
功能(Function)	顯示介面類型(WAN 或 LAN)。 介面可設定為 WAN 或 LAN 以滿足不同需求。使用下拉式選單將指定介面設定為 LAN 或 WAN。
啟用(Enable)	切換開關即可啟用或停用該介面。
USB	
介面(Interface)	顯示此裝置可用的 USB 介面。
啟用(Enable)	切換開關即可啟用或停用該介面。
LED	
介面(Interface)	顯示前面板上的所有 LED 指示燈。
LED Sleep Schedule	根據所選排程（於設定>>物件下定義）設定檔中的設置，可以開啟或關閉 LED，以滿足特定要求。 當 LED 燈處於睡眠狀態時，可透過以下方式喚醒： • 前面板上的 Factory Reset 按鈕 • 此設定頁面上的喚醒 LED 按鈕 請注意，如果將排程設定為重複類型並套用到此處，則裝置上的 LED 燈將在指定時間中，定期自動開啟和關閉。
啟用(Enable)	預設情況下，裝置上的 LED 指示燈始終是亮燈。 但是，為了滿足特定要求，LED 指示燈可以在指定的時間(數分鐘後)開啟或關閉。 為此，請切換開關以啟用此設定。
按鈕(Button)	
介面(Interface)	顯示此裝置的可用按鈕(無線/重置)。
用法(Usage)	**WLAN On/Off/WPS** – 預設是啟用的。如果未啟用，無線按鈕將失去對 WLAN 和 WPS 功能的控制。 **搜尋無線網狀網路(Mesh Discovery)** – 點擊以尋找可用的無線網狀網路節點。掃描結果可在系統日誌中查看。 

設定重置按鈕 (Configuration Reset Button)	切換此開關即可啟用或停用出廠預設值功能。
啟用(Enable)	切換開關即可啟用或停用按鈕功能。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

注意:

點擊這兩個圖示即可切換啟用與停用。

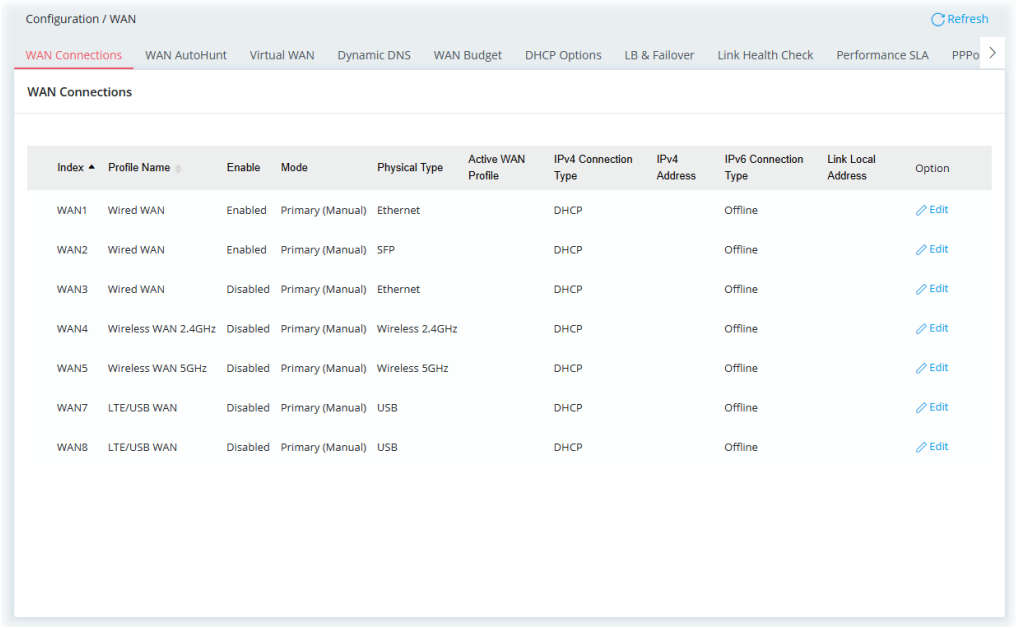
 - 表示"啟用(Enable)"。

 - 表示"停用(Disable)"。

II-1-2 WAN 設定

II-1-2-1 WAN 連線(WAN Connections)

本頁面用於設定廣域網路 WAN 連線的基本設定。



可用設定說明如下：

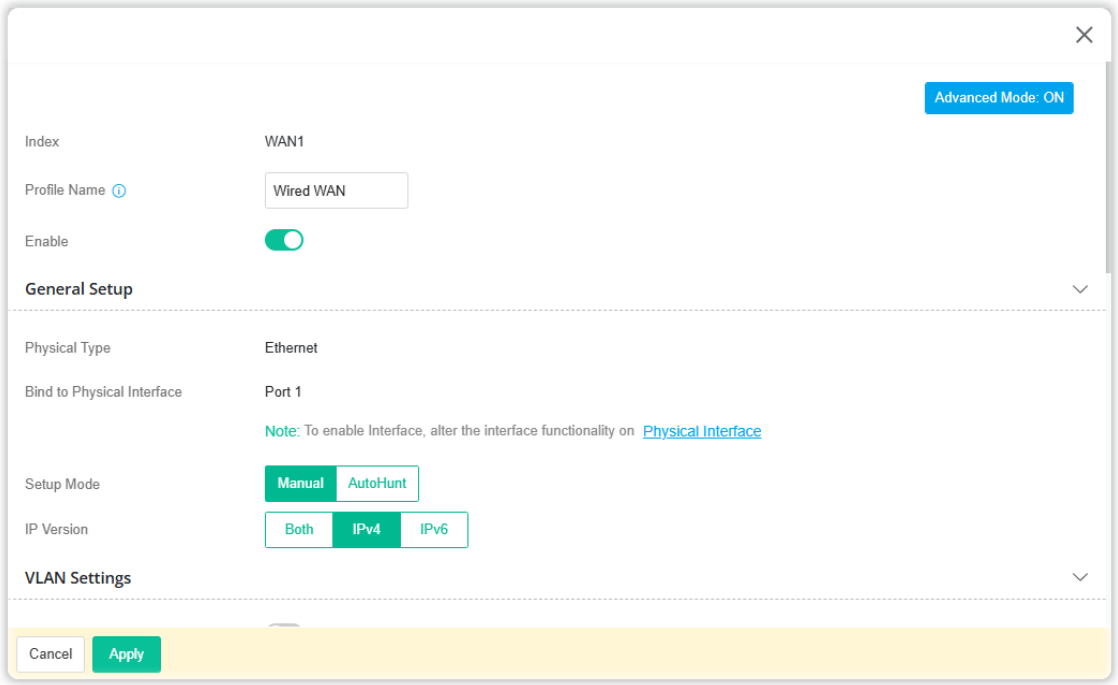
項目	說明
設定檔名稱 (Profile Name)	顯示介面的名稱。
啟用(Enable)	顯示此 WAN 介面是否啟用或停用。
模式(Mode)	顯示 WAN 介面是主要介面還是被原介面。
傳送資料模式 (Physical Type)	顯示 WAN 介面的實體類型(例如，乙太網路、無線 2.4GHz、無線 5GHz 或 LTE 等等)。
啟用 WAN 設定檔(Active WAN Profile)	顯示此 WAN 介面套用的 WAN 設定檔。
IPv4 連接類型 (IPv4 Connection Type)	顯示 WAN 介面所使用的 IPv4 連線類型 (例如靜態 IP、DHCP 等)。
IPv4 位址 (IPv4 Address)	顯示 DHCP 伺服器分派的 IP 位址或手動指定的靜態 IP 位址。
IPv6 連線類型 (IPv6 Connection Type)	顯示 WAN 介面所使用的 IPv6 連線類型。
鏈結本機位址 (Link Local Address)	顯示 IPv6 連線類型的 IPv6 位址。
選項(Option)	**編輯(Edit)** - 修改介面名稱和實體連線模式。

若要設定所選 WAN 介面的詳細設定(因實體連線類型而異)，請按一下位於各個 WAN 介面右側的編輯鏈結。

傳送資料模式為乙太網路

對於靜態 IP 存取模式，您通常會從有線網路服務供應商取得固定的真實 IP 位址或真實子網，也就是多個真實 IP 位址。大多數情況下，有線網路服務供應商會提供一個固定的真實 IP 位址。如果您擁有真實子網，則可以為 WAN 介面指派一個或多個 IP 位址。

按下 WAN1 或 WAN3 的**編輯(Edit)**連結開啟以下頁面。



可用設定說明如下：

項目	說明
進階模式:開啟/關閉 (Advanced Mode:ON/OFF)	按此顯示或隱藏 WAN 介面之進階設定(諸如伺服器名稱、PPP 驗證、IP 分派、對外流量 DNS 查詢 IP、IP 別名與 WAN MAC 位址等等)。
索引編號(Index)	顯示目前廣域網路 WAN 介面。
設定檔名稱(Profile Name)	顯示設定檔名稱。
啟用(Enable)	切換開關即可啟用或停用此功能。
基本設定(General Setup)	
傳送資料模式 (Physical Type)	顯示此介面使用的實體類型。
綁定至實體介面(Bind to Physical Interface)	選擇實體介面（乙太網路）。
設定模式(Setup Mode)	根據 AutoHunt 設定檔，逐一確認在設定頁面建立的 WAN 連線或自動建立的 WAN 連線。 **手動(Manual)** – 如果選此項，WAN 連線將按照此頁面中配置的設定執行。

	設定自動偵測(AutoHunt) – Vigor 路由器將自動連接到乙太網路 WAN 連接埠。連接並開啟電源後，路由器將運行一系列網路連線設定 (基於設定自動偵測設定檔 AutoHunt) 以確定是否可以建立連線。如果連接失敗，路由器將繼續嘗試下一個 ISP 設置，直到獲得 IP 位址。 如果選擇了 **AutoHunt**，可設定以下項目： ● **設定自動偵測設定檔(AutoHunt Profile)** – 選擇一個設定檔。 ● **+新增(+Add)** – 按此以指定自動搜尋設定檔。 ● **啟用 WAN 設定檔(Active WAN Profile)** – 顯示套用於此 WAN 介面的自動偵測設定檔。連線過程中，將顯示目前正在嘗試連線的自動偵測設定檔。如果所有設定檔都失敗，則顯示最後一個嘗試的設定檔。
IP 版本(IP Version)	設定此 WAN 介面所使用的協定 (IPv4 或 IPv6 或兩者都用) 。
	VLAN 設定(VLAN Settings)
顧客 VLAN (Customer VLAN)	切換此開關以啟用或停用帶有標籤的 VLAN 功能。如果啟用，請輸入標籤和優先權值。 **標籤(Tag)** – 輸入 VLAN ID 號碼。範圍為 0 到 4094。 **優先權(Priority)** – 輸入該 VLAN 的封包優先編號。範圍為 0 到 7。
服務 VLAN (Service VLAN)	切換此開關以啟用或停用帶有標籤的 VLAN 功能。如果啟用，請輸入標籤和優先權值。 **標籤(Tag)** – 輸入 VLAN ID 號碼。範圍為 0 到 4094。 **優先權(Priority)** – 輸入該 VLAN 的封包優先編號。範圍為 0 到 7。
	IPv4
IPv4 連接類型(IPv4 Connection Type)	當選擇兩者(Both)或 IPv4 作為 IP 版本時，可使用此功能。 **PPPoE** – 將存取模式設定為 PPPoE。 ● **使用者名稱(Username)** – ISP 提供的 PPPoE 驗證的使用者名稱。 ● **密碼(Password)** – ISP 提供的 PPPoE 驗證的密碼。 ● **WAN DNS** – 選擇**自動(Auto)**或**手動(Manual)**。 如果選擇了手動(Manual)，需指定主要與次要 DNS 伺服器。 **IPv4 主要 DNS(IPv4 Primary DNS)** – 輸入主要 DNS 伺服器位址。 **IPv4 次要 DNS(IPv4 Secondary DNS)** - 輸入次要 DNS 伺服器位址。 ● **服務名稱(Service Name)** – PPP 服務名稱標籤。部分 ISP 需要此項目。除非您的 ISP 另有指示，否則請留空。此功能僅在啟用進階模式時可用。 ● **PPP 驗證(PPP Authentication)** – 用於 PPP 驗證的協定。**PAP 或 CHAP** - PAP 和 CHAP (詢問握手認證協定) 皆可用於 PPP 認證。路由器會與 PPTP 或 L2TP 伺服器協商以確定使用哪種協定。此功能僅在進階模式啟用時可用。 ● **IP 分派(IP Assignment)** – 此功能僅在啟用進階模式時可用。當選擇 PPPoE 作為 IPv4 連線類型時，即可使用此功能。 **DHCP** - 位址是動態分配的。 **靜態 IP (Static IP)** - 您的網路服務供應商已指派一個固定的廣域網路 IP 位址。請輸入 IP 位址。 **DHCP** – 路由器從 DHCP 伺服器接收 IP 設定資訊。

	• **WAN DNS** – 選擇**自動(Auto)**或**手動(Manual)**。 如果選擇了手動(Manual)，需指定主要與次要 DNS 伺服器。 **IPv4 主要 DNS(IPv4 Primary DNS)** – 輸入主要 DNS 伺服器位址。 **IPv4 次要 DNS(IPv4 Secondary DNS)** - 輸入次要 DNS 伺服器位址。 **靜態 IP (Static IP)** – 將存取模式設定為靜態 IP。 • **IP 位址 (IP Address)** – 由網際網路服務供應商 (ISP) 指派的廣域網路 IP 位址。 • **子網遮罩(Subnet Mask)** – WAN 子網路遮罩。 • **閘道 IP(Gateway IP)** – WAN 閘道的 IP 位址。 • **IPv4 主要 DNS (IPv4 Primary DNS)** – 主要 DNS 伺服器的 IP 位址。 • **IPv4 次要 DNS (IPv4 Secondary DNS**) – 次要 DNS 伺服器的 IP 位址。 **對外流量 DNS 查詢 IP (Outbound DNS Query IP)** - 此功能僅在啟用進階模式時可用。請指定路由器用於發送 DNS 查詢的來源 IP 位址。 • **預設 IP (Default IP)** – 查詢 IP 由 Vigor 路由器自動設定。 • **別名 IP (Alias IP)** – 輸入使用者自訂的用於 DNS 查詢的 IP 位址。
WAN 連線偵測(WAN Connection Detection)	
模式(Mode)	設定如何監控廣域網路連線。 **永遠連線(Always On)** - 路由器假定廣域網路連線始終處於作用中狀態。 **ARP 偵測(ARP Detect)** - 路由器每 5 秒廣播一次 ARP 請求。如果在 30 秒內沒有收到回應，則認為 WAN 連線失敗。 **Ping 偵測(Ping Detect)** - 路由器會根據 ping 間隔設置，向 Ping 閘道 IP 欄位中指定的位址的主機發送 ICMP (Internet 控制訊息協定) 回應請求，以驗證 WAN 連線。如果遠端主機在指定秒數 (由 ping 間隔定義) 內沒有回應，則認為 WAN 連線失敗。 如果你選擇 **Ping 偵測(Ping Detect)**作為檢測模式，您需要輸入以下項目的必要設定。 • **Ping 閘道 IP (Ping Gateway IP)** - 切換此開關以啟用/使用目前 WAN 閘道 IP 位址進行 ping 測試。透過 ping 測試 IP 位址，Vigor 路由器可以檢查 WAN 連線是否已開啟。 • **TTL** – 存活時間 (Time To Live) ，即到達 ping 目標位址允許的最大跳數。有效值範圍為 1 到 255。 • **Ping 間隔(5-3600 秒) (Ping Interval (Sec, 5-3600))** – 輸入系統執行 PING 操作的間隔。 • **Ping 重試次數(Ping Retry)** - 輸入在判定 WAN 斷開連線之前，系統允許執行 PING 操作的次數。
IP 別名(IP Alias)	**IPv4 別名(IPv4 Alias)** - 如果您有多個真實 IP 位址，並希望在 WAN 介面上使用它們，請使用 WAN IP 別名。除了目前正在使用的真實 IP 位址之外，您最多可以設定 8 個真實 IP 位址。 **+新增(+Add)** – 按下**+新增(+Add)** 輸入 IPv4 位址作為 IPv4 別名。
IPv6	
IPv6 連線類型(IPv6 Connection Type)	當選擇兩者(Both)或 IPv6 作為 IP 版本時，可使用此功能。 **斷線(Offline)** – 選擇離線時，IPv6 連線將會停用。 • **WAN DNS** – 選擇**自動(Auto)**或**手動(Manual)**。 如果選擇了手動(Manual)，需指定主要與次要 DNS 伺服器。 **IPv6 主要 DNS(IPv6 Primary DNS)** – 輸入主要 DNS 伺服器位址。

IPv6 次要 DNS(IPv6 Secondary DNS) - 輸入次要 DNS 伺服器位址。

PPP – 在 PPPoE 協商過程中，IPv6 WAN 位址會與 IPv4 WAN 位址一起指派。這種 IPv6 存取模式會要求 IPv4 使用 PPPoE 協定。

- **WAN DNS** – 選擇**自動(Auto)**或**手動(Manual)**。

  如果選擇了手動(Manual)，需指定主要與次要 DNS 伺服器。

  IPv6 主要 DNS(IPv6 Primary DNS) – 輸入主要 DNS 伺服器位址。

  IPv6 次要 DNS(IPv6 Secondary DNS) - 輸入次要 DNS 伺服器位址。

靜態(Static) – 設定 ISP 分配的靜態 IPv6 設定。

- **+新增(+Add)** – 按一下此按鈕，將 IPv6 位址和前置碼長度欄位中的值新增至全球位址表(Global Address Table)。
- **IPv6 全球位址(IPv6 Global Address)** – 由網際網路服務供應商 (ISP) 指派的廣域網路 IPv6 位址。
- **前置碼長度(Prefix Length) – IPv6** 前置碼的長度。
- **閘道位址(Gateway Address) –** ISP 閘道的 IPv6 位址。
- **IPv6 主要 DNS (IPv6 Primary DNS)** –主要 DNS 伺服器的 IP 位址。
- **IPv6 次要 DNS (IPv6 Secondary DNS)** - 次要 DNS 伺服器的 IP 位址。

DHCPv6 – 使用 DHCPv6 協定從伺服器取得 IPv6 位址。

- **DUID** – 顯示此 WAN 介面所使用的 DHCP 唯一 ID。
- **IAID** – 用於識別此 WAN 介面的唯一整數。
- **驗證通訊協定(Authentication Protocol)** - 此協定用於用戶端在存取網際網路之前透過 DHCPv6 伺服器進行身份驗證。可以指定三種類型：**重新設定金鑰(Reconfigure Key)**，**延遲(Delayed)**和**無(None)**。通常情況下，預設為**無(None)**。
  - **重新設定金鑰(Reconfigure Key)** – 在連線過程中，DHCPv6 伺服器將自動對用戶端進行身份驗證。
  - **延遲(Delayed)** - 在連線過程中，DHCPv6 伺服器將根據這些欄位中指定的金鑰 ID、領域和秘鑰資訊對用戶端進行身份驗證和識別。
    金鑰 ID (Key ID) – 輸入一個值 (範圍從 1 到 65535)，該值將用於產生 HMAC-MD5 值。
    領域(Realm) – 在此輸入的名稱 (1 到 31 個字元) 將標識產生 HMAC-MD5 值的密鑰。
    密鑰(Secret) – 輸入一段文字 (1 到 31 個字元) 作為每個 DHCP 伺服器上每個用戶端的唯一識別碼。
- **WAN DNS** – 選擇**自動(Auto)** 或是**手動(Manual)**。

  如果選擇了手動(Manual)，需指定主要與次要 DNS 伺服器。

  IPv6 主要 DNS(IPv6 Primary DNS) – 輸入主要 DNS 伺服器位址。

  IPv6 次要 DNS(IPv6 Secondary DNS) - 輸入次要 DNS 伺服器位址。

TSPC - 通道建立協定用戶端（TSPC）是一款可以幫助您輕鬆連接到 IPv6 網路的應用程式。

請確保您的 IPv4 WAN 連線正常，並從 hexago 申請免費帳戶 (http://gogonet.gogo6.com/page/freenet6-account 在您嘗試使用 TSPC 進行網路連線之前，請先進行設定。TSPC 會連線到通道代理，並根據設定檔中的規格請求通道。它會從通道代理程式取得公用 IPv6 位址和 IPv6 前置碼，然後在背景監控通道的狀態。

在取得 IPv6 前置碼並啟動路由器通告守護程式（RADVD）後，該路由器後面的 PC 可以直接連接到 IPv6 網際網路。

- **通道代理伺服器位址(Tunnel Broker Address)** – 輸入位址通道代

理 IP 位址、FQDN 或選用連接埠號碼。

- **使用者名稱(Username)** – 建議您使用另一個使用者名稱和密碼。http://gogonet.gogo6.com/page/freenet6-account。
- **密碼(Password)** -輸入與使用者名稱關聯的密碼。
- **WAN DNS** – 選擇**自動(Auto)** 或是**手動(Manual)**。

  如果選擇了手動(Manual)，需指定主要與次要 DNS 伺服器。

  IPv6 主要 DNS(IPv6 Primary DNS) – 輸入主要 DNS 伺服器位址。

  IPv6 次要 DNS(IPv6 Secondary DNS) - 輸入次要 DNS 伺服器位址。

6in4 – 為 WAN 介面設定 6in4 靜態通道。

然而，6in4 提供了一個 2002::0/16 之外的前置碼。如此一來，您可以使用固定端點，而不是任何類型轉換端點。這種模式更加可靠。

- **啟用 IPv4 WAN Ping 存取 6in4/6rd 通道 (Enable IPv4 WAN Ping Access for 6in4/6rd Tunnel)** – 若要使用此 6in4 連線類型，必須允許 IPv4 WAN 存取，且防火牆必須允許通道代理 IP 位址通過。
- **遠端終點 IPv4 位址(Remote Endpoint IPv4 Address)** – 由通道提供者指派的 WAN IPv6 位址。
- **6in4 IPv6 位址(6in4 IPv6 Address)** – 由通道提供者指派的 WAN IPv6 位址。
- **6in4 IPv6 前置碼長度(6in4 IPv6 Prefix Length) –** 通道提供者指派的 WAN IPv6 前置碼長度。
- **LAN 路由前置碼(LAN Routed Prefix) –** 區域網路 IPv6 位址前置碼。
- **LAN 路由前置碼長度(LAN Routed Prefix Length) –**區域網路 IPv6 位址前置碼長度。
- **通道 TTL (Tunnel TTL) –** 存活時間值，即允許到達端點的最大躍點數。
- **WAN DNS** – 選擇**自動(Auto)** 或是**手動(Manual)**。

  如果選擇了手動(Manual)，需指定主要與次要 DNS 伺服器。

  IPv6 主要 DNS(IPv6 Primary DNS) – 輸入主要 DNS 伺服器位址。

  IPv6 次要 DNS(IPv6 Secondary DNS) - 輸入次要 DNS 伺服器位址。

6rd – 為 WAN 介面設定 6rd。

- **啟用 IPv4 WAN Ping 存取 6in4/6rd 通道(Enable IPv4 WAN Ping Access for 6in4/6rd Tunnel)** – 要使用 6rd 連線類型，必須允許 IPv4 WAN 訪問，且防火牆必須允許通道代理 IP 位址通過。
- **模式(Mode)** – 兩種選項 : **自動(Auto)**和**靜態(Static)**態。**自動(Auto)** - 路由器與 DHCPv4 搭配使用時，會自動使用選項 212 設定 IPv6。**靜態(Static)**- IPv6 設定資訊是手動輸入的。**若是**選取**靜態(Static)**，須設定以下內容：
  - **IPv4 邊界中繼(IPv4 Border Relay)** – 輸入給予 6rd 網域的 6rd 邊界中繼的 IPv4 位址。
  - **6rd 前置碼(6rd Prefix)** – 輸入 6rd IPv6 位址。
  - **6rd 前置碼長度(6rd Prefix Length)** - 輸入 6rd IPv6 前置碼長度（以位元為單位）。
- **WAN DNS** – 選擇**自動(Auto)** 或是**手動(Manual)**。

  如果選擇了手動(Manual)，需指定主要與次要 DNS 伺服器。

  IPv6 主要 DNS(IPv6 Primary DNS) – 輸入主要 DNS 伺服器位址。

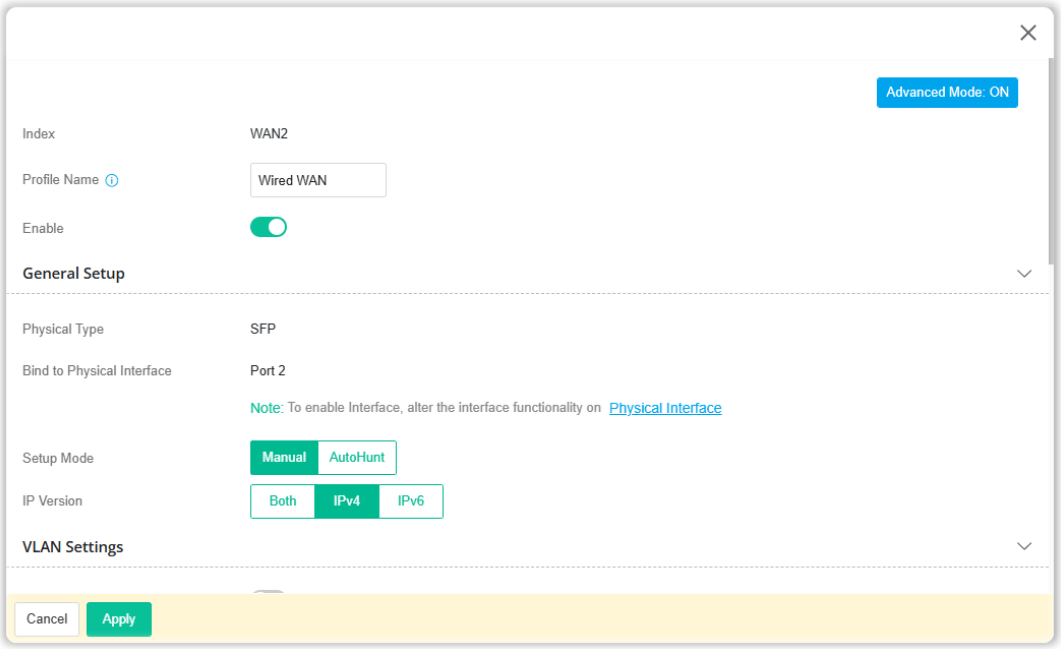
  IPv6 次要 DNS(IPv6 Secondary DNS) - 輸入次要 DNS 伺服器位址。

IPv6 WAN 連線偵測(IPv6 WAN Connection Detection)	
模式(Mode)	**永遠連線(Always On) -** 路由器假定廣域網路連線始終處於作用中狀態。 **NS 偵測(NS Detect) -** 路由器透過發出鄰居請求封包來驗證連線。 **Ping 偵測(Ping Detect)** -路由器會根據 ping 間隔設置,向 Ping 閘道 IP 欄位中指定的位址的主機發送 ICMP (Internet 控制訊息協定) 回應請求,以驗證 WAN 連線。如果遠端主機在指定秒數 (由 ping 間隔定義) 內沒有回應,則認為 WAN 連線失敗。 如果你選擇 **Ping 偵測(Ping Detect)**作為檢測模式,您需要輸入以下項目的必要設定。 ● **主要 Ping IP (Primary Ping IP)** – 在此欄位中輸入要 ping 的 IP 位址。 ● **次要 Ping IP (Secondary Ping IP)** - 請在此欄位中輸入要 ping 的 IP 位址。 ● **TTL** – 存活時間 (Time To Live) ,即到達 ping 目標位址允許的最大跳數。有效值範圍為 1 到 255。 ● **Ping 間隔(10-3600 秒) (Ping Interval (Sec, 10-3600))** – 輸入系統執行 PING 操作的間隔。 ● **Ping 重試次數(Ping Retry) -** 輸入在判定 WAN 斷開連線之前,系統允許執行 PING 操作的次數。
MTU	
MTU	最大傳輸單元 (MTU) 是指可以傳送到廣域網路 (WAN) 的最大資料封包的大小 (以位元組為單位) 。最大值為 1500。對於 PPPoE 連線而言,因為 PPPoE 連線會額外增加 8 位元組的封包標頭,因此原本 Ethernet 的最大 MTU 1500 位元組需要扣掉這 8 位元組,所以 PPPoE 的最大 MTU 為 1492 位元組。
WAN MAC 位址(WAN MAC Address)	
模式(Mode)	**預設值(Default)** – 使用 WAN 連接埠的預設 MAC 位址。 **客製化(Customized) -** 如果您的 ISP 透過 MAC 位址進行驗證,請選擇此選項。 ● **MAC -** 為 WAN 乙太網路連接埠指定 MAC 位址。
MAC	顯示此裝置的 MAC 位址。
取消(Cancel)	捨棄目前設定並回到前一頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後,按下套用(Apply)按鈕儲存相關設定。

傳送資料模式為 SFP 光纖模式

按下 WAN2 的**編輯(Edit)**連結開啟以下頁面。



可用設定說明如下：

項目	說明
進階模式:開啟/關閉 (Advanced Mode:ON/OFF)	按此顯示或隱藏 WAN 介面之進階設定(諸如伺服器名稱、PPP 驗證、IP 分派、對外流量 DNS 查詢 IP、IP 別名與 WAN MAC 位址等等)。
索引編號(Index)	顯示目前廣域網路 WAN 介面。
設定檔名稱(Profile Name)	顯示設定檔名稱。
啟用(Enable)	切換開關即可啟用或停用此功能。
基本設定(General Setup)	
傳送資料模式 (Physical Type)	顯示此介面使用的實體類型。
綁定至實體介面(Bind to Physical Interface)	顯示實體介面名稱。
設定模式(Setup Mode)	根據 AutoHunt 設定檔，逐一確認在設定頁面建立的 WAN 連線或自動建立的 WAN 連線。 **手動(Manual)** – 如果選此項，WAN 連線將按照此頁面中配置的設定執行。 **設定自動偵測(AutoHunt)** – Vigor 路由器將自動連接到乙太網路 WAN 連接埠。連接並開啟電源後，路由器將運行一系列網路連線設定 (基於設定自動偵測設定檔 AutoHunt) 以確定是否可以建立連線。如果連接失敗，路由器將繼續嘗試下一個 ISP 設置，直到獲得 IP 位址。 如果選擇了 **AutoHunt**，可設定以下項目： ● **設定自動偵測設定檔(AutoHunt Profile)** – 選擇一個設定檔。

	• **+新增(+Add)** – 按此以指定自動搜尋設定檔。 • **啟用 WAN 設定檔(Active WAN Profile)** – 顯示套用於此 WAN 介面的自動偵測設定檔。連線過程中，將顯示目前正在嘗試連線的自動偵測設定檔。如果所有設定檔都失敗，則顯示最後一個嘗試的設定檔。
IP 版本(IP Version)	設定此 WAN 介面所使用的協定（IPv4 或 IPv6 或兩者都用）。
	VLAN 設定(VLAN Settings)
顧客 VLAN (Customer VLAN)	切換此開關以啟用或停用帶有標籤的 VLAN 功能。如果啟用，請輸入標籤和優先權值。 **標籤(Tag)** – 輸入 VLAN ID 號碼。範圍為 0 到 4094。 **優先權(Priority)** – 輸入該 VLAN 的封包優先編號。範圍為 0 到 7。
服務 VLAN (Service VLAN)	切換此開關以啟用或停用帶有標籤的 VLAN 功能。如果啟用，請輸入標籤和優先權值。 **標籤(Tag)** – 輸入 VLAN ID 號碼。範圍為 0 到 4094。 **優先權(Priority)** – 輸入該 VLAN 的封包優先編號。範圍為 0 到 7。
	IPv4
IPv4 連接類型(IPv4 Connection Type)	當選擇兩者(Both)或 IPv4 作為 IP 版本時，可使用此功能。 **PPPoE** – 將存取模式設定為 PPPoE。 • **使用者名稱(Username)** – ISP 提供的 PPPoE 驗證的使用者名稱。 • **密碼(Password)** – ISP 提供的 PPPoE 驗證的密碼。 • **WAN DNS** – 選擇**自動(Auto)**或**手動(Manual)**。 如果選擇了手動(Manual)，需指定主要與次要 DNS 伺服器。 **IPv4 主要 DNS(IPv4 Primary DNS)** – 輸入主要 DNS 伺服器位址。 **IPv4 次要 DNS(IPv4 Secondary DNS)** - 輸入次要 DNS 伺服器位址。 • **服務名稱(Service Name)** – PPP 服務名稱標籤。部分 ISP 需要此項目。除非您的 ISP 另有指示，否則請留空。此功能僅在啟用進階模式時可用。 • **PPP 驗證(PPP Authentication)** – 用於 PPP 驗證的協定。**PAP 或 CHAP** - PAP 和 CHAP（詢問握手認證協定）皆可用於 PPP 認證。路由器會與 PPTP 或 L2TP 伺服器協商以確定使用哪種協定。此功能僅在進階模式啟用時可用。 • **IP 分派(IP Assignment)** – 此功能僅在啟用進階模式時可用。當選擇 PPPoE 作為 IPv4 連線類型時，即可使用此功能。 **DHCP** - 位址是動態分配的。 **靜態 IP (Static IP)** - 您的網路服務供應商已指派一個固定的廣域網路 IP 位址。請輸入 IP 位址。 **DHCP** – 路由器從 DHCP 伺服器接收 IP 設定資訊。 • **WAN DNS** – 選擇**自動(Auto)**或**手動(Manual)**。 如果選擇了手動(Manual)，需指定主要與次要 DNS 伺服器。 **IPv4 主要 DNS(IPv4 Primary DNS)** – 輸入主要 DNS 伺服器位址。 **IPv4 次要 DNS(IPv4 Secondary DNS)** - 輸入次要 DNS 伺服器位址。 **靜態 IP (Static IP)** – 將存取模式設定為靜態 IP。 • **IP 位址 (IP Address)** – 由網際網路服務供應商 (ISP) 指派的廣域

	網路 IP 位址。 ● **子網遮罩(Subnet Mask)** – WAN 子網路遮罩。 ● **閘道 IP(Gateway IP)** – WAN 閘道的 IP 位址。 ● **IPv4 主要 DNS (IPv4 Primary DNS)** – 主要 DNS 伺服器的 IP 位址。 ● **IPv4 次要 DNS (IPv4 Secondary DNS)** – 次要 DNS 伺服器的 IP 位址。
WAN 連線偵測(WAN Connection Detection)	
模式(Mode)	設定如何監控廣域網路連線。 **永遠連線(Always On) -** 路由器假定廣域網路連線始終處於作用中狀態。 **ARP 偵測(ARP Detect)** - 路由器每 5 秒廣播一次 ARP 請求。如果在 30 秒內沒有收到回應，則認為 WAN 連線失敗。 **Ping 偵測(Ping Detect)** - 路由器會根據 ping 間隔設置，向 Ping 閘道 IP 欄位中指定的位址的主機發送 ICMP (Internet 控制訊息協定) 回應請求，以驗證 WAN 連線。如果遠端主機在指定秒數 (由 ping 間隔定義) 內沒有回應，則認為 WAN 連線失敗。 如果你選擇 **Ping 偵測(Ping Detect)**作為檢測模式，您需要輸入以下項目的必要設定。 ● **Ping 閘道 IP (Ping Gateway IP)** - 切換此開關以啟用/使用目前 WAN 閘道 IP 位址進行 ping 測試。透過 ping 測試 IP 位址，Vigor 路由器可以檢查 WAN 連線是否已開啟。 ● **TTL** – 存活時間 (Time To Live) ，即到達 ping 目標位址允許的最大跳數。有效值範圍為 1 到 255。 ● **Ping 間隔(5-3600 秒) (Ping Interval (Sec, 5-3600))** – 輸入系統執行 PING 操作的間隔。 ● **Ping 重試次數(Ping Retry)** - 輸入在判定 WAN 斷開連線之前，系統允許執行 PING 操作的次數。
IP 別名(IP Alias)	**IPv4 別名(IPv4 Alias)** - 如果您有多個真實 IP 位址，並希望在 WAN 介面上使用它們，請使用 WAN IP 別名。除了目前正在使用的真實 IP 位址之外，您最多可以設定 8 個真實 IP 位址。 **+新增(+Add)** – 按下**+新增(+Add)** 輸入 IPv4 位址作為 IPv4 別名。
IPv6	
IPv6 連線類型(IPv6 Connection Type)	當選擇兩者(Both)或 IPv6 作為 IP 版本時，可使用此功能。 **斷線(Offline)** – 選擇離線時，IPv6 連線將會停用。 ● **WAN DNS** – 選擇**自動(Auto)**或**手動(Manual)**。 如果選擇了手動(Manual)，需指定主要與次要 DNS 伺服器。 **IPv6 主要 DNS(IPv6 Primary DNS)** – 輸入主要 DNS 伺服器位址。 **IPv6 次要 DNS(IPv6 Secondary DNS)** - 輸入次要 DNS 伺服器位址。 **PPP** – 在 PPPoE 協商過程中，IPv6 WAN 位址會與 IPv4 WAN 位址一起指派。這種 IPv6 存取模式會要求 IPv4 使用 PPPoE 協定。 ● **WAN DNS** – 選擇**自動(Auto)**或**手動(Manual)**。 如果選擇了手動(Manual)，需指定主要與次要 DNS 伺服器。 **IPv6 主要 DNS(IPv6 Primary DNS)** – 輸入主要 DNS 伺服器位址。 **IPv6 次要 DNS(IPv6 Secondary DNS)** - 輸入次要 DNS 伺服器位址。 **靜態(Static)** – 設定 ISP 分配的靜態 IPv6 設定。 ● **+新增(+Add)** – 按一下此按鈕，將 IPv6 位址和前置碼長度欄位中的值新增至全球位址表(Global Address Table)。

- **IPv6 全球位址(IPv6 Global Address)** – 由網際網路服務供應商 (ISP) 指派的廣域網路 IPv6 位址。
- **前置碼長度(Prefix Length)** – IPv6 前置碼的長度。
- **閘道位址(Gateway Address)** – ISP 閘道的 IPv6 位址。
- **IPv6 主要 DNS (IPv6 Primary DNS)** –主要 DNS 伺服器的 IP 位址。
- **IPv6 次要 DNS (IPv6 Secondary DNS)** – 次要 DNS 伺服器的 IP 位址。

DHCPv6 – 使用 DHCPv6 協定從伺服器取得 IPv6 位址。

- **DUID** – 顯示此 WAN 介面所使用的 DHCP 唯一 ID。
- **IAID** – 用於識別此 WAN 介面的唯一整數。
- **驗證通訊協定(Authentication Protocol)** – 此協定用於用戶端在存取網際網路之前透過 DHCPv6 伺服器進行身份驗證。可以指定三種類型：**重新設定金鑰(Reconfigure Key)**，**延遲(Delayed)**和**無(None)**。通常情況下，預設為**無(None)**。
  - **重新設定金鑰(Reconfigure Key)** – 在連線過程中，DHCPv6 伺服器將自動對用戶端進行身份驗證。
  - **延遲(Delayed)** – 在連線過程中，DHCPv6 伺服器將根據這些欄位中指定的金鑰 ID、領域和秘鑰資訊對用戶端進行身份驗證和識別。
    金鑰 ID (Key ID) – 輸入一個值 (範圍從 1 到 65535)，該值將用於產生 HMAC-MD5 值。
    領域(Realm) – 在此輸入的名稱 (1 到 31 個字元) 將標識產生 HMAC-MD5 值的密鑰。
    密鑰(Secret) – 輸入一段文字 (1 到 31 個字元) 作為每個 DHCP 伺服器上每個用戶端的唯一識別碼。
- **WAN DNS** – 選擇**自動(Auto)** 或是**手動(Manual)**。

  如果選擇了手動(Manual)，需指定主要與次要 DNS 伺服器。

  IPv6 主要 DNS(IPv6 Primary DNS) – 輸入主要 DNS 伺服器位址。

  IPv6 次要 DNS(IPv6 Secondary DNS) - 輸入次要 DNS 伺服器位址。

TSPC – 通道建立協定用戶端（TSPC）是一款可以幫助您輕鬆連接到 IPv6 網路的應用程式。

請確保您的 IPv4 WAN 連線正常，並從 hexago 申請免費帳戶 (http://gogonet.gogo6.com/page/freenet6-account 在您嘗試使用 TSPC 進行網路連線之前，請先進行設定。TSPC 會連線到通道代理，並根據設定檔中的規格請求通道。它會從通道代理程式取得公用 IPv6 位址和 IPv6 前置碼，然後在背景監控通道的狀態。

在取得 IPv6 前置碼並啟動路由器通告守護程式（RADVD）後，該路由器後面的 PC 可以直接連接到 IPv6 網際網路。

- **通道代理伺服器位址(Tunnel Broker Address)** – 輸入位址通道代理 IP 位址、FQDN 或選用連接埠號碼。
- **使用者名稱(Username)** – 建議您使用另一個使用者名稱和密碼。http://gogonet.gogo6.com/page/freenet6-account。
- **密碼(Password)** -輸入與使用者名稱關聯的密碼。
- **WAN DNS** – 選擇**自動(Auto)** 或是**手動(Manual)**。

  如果選擇了手動(Manual)，需指定主要與次要 DNS 伺服器。

  IPv6 主要 DNS(IPv6 Primary DNS) – 輸入主要 DNS 伺服器位址。

  IPv6 次要 DNS(IPv6 Secondary DNS) - 輸入次要 DNS 伺服器位址。

6in4 – 為 WAN 介面設定 6in4 靜態通道。

然而，6in4 提供了一個 2002::0/16 之外的前置碼。如此一來，您可以使

	用固定端點，而不是任何類型轉換端點。這種模式更加可靠。 • **啟用 IPv4 WAN Ping 存取 6in4/6rd 通道 (Enable IPv4 WAN Ping Access for 6in4/6rd Tunnel)** – 若要使用此 6in4 連線類型，必須允許 IPv4 WAN 存取，且防火牆必須允許通道代理 IP 位址通過。 • **遠端終點 IPv4 位址(Remote Endpoint IPv4 Address)** – 由通道提供者指派的 WAN IPv6 位址。 • **6in4 IPv6 位址(6in4 IPv6 Address)** – 由通道提供者指派的 WAN IPv6 位址。 • **6in4 IPv6 前置碼長度(6in4 IPv6 Prefix Length) –** 通道提供者指派的 WAN IPv6 前置碼長度。 • **LAN 路由前置碼(LAN Routed Prefix) –** 區域網路 IPv6 位址前置碼。 • **LAN 路由前置碼長度(LAN Routed Prefix Length) –**區域網路 IPv6 位址前置碼長度。 • **通道 TTL (Tunnel TTL) –** 存活時間值，即允許到達端點的最大躍點數。 • **WAN DNS** – 選擇**自動(Auto)** 或是**手動(Manual)**。 如果選擇了手動(Manual)，需指定主要與次要 DNS 伺服器。 **IPv6 主要 DNS(IPv6 Primary DNS)** – 輸入主要 DNS 伺服器位址。 **IPv6 次要 DNS(IPv6 Secondary DNS)** - 輸入次要 DNS 伺服器位址。 **6rd** – 為 WAN 介面設定 6rd。 • **啟用 IPv4 WAN Ping 存取 6in4/6rd 通道(Enable IPv4 WAN Ping Access for 6in4/6rd Tunnel)** – 要使用 6rd 連線類型，必須允許 IPv4 WAN 訪問，且防火牆必須允許通道代理 IP 位址通過。 • **模式(Mode)** – 兩種選項 : **自動(Auto)**和**靜態(Static)**態。**自動(Auto)** - 路由器與 DHCPv4 搭配使用時，會自動使用選項 212 設定 IPv6。**靜態(Static)**- IPv6 設定資訊是手動輸入的。**若是**選取**靜態(Static)**，須設定以下內容： - **IPv4 邊界中繼(IPv4 Border Relay)** – 輸入給予 6rd 網域的 6rd 邊界中繼的 IPv4 位址。 - **6rd 前置碼(6rd Prefix)** – 輸入 6rd IPv6 位址。 - **6rd 前置碼長度(6rd Prefix Length)** - 輸入 6rd IPv6 前置碼長度（以位元為單位）。 • **WAN DNS** – 選擇**自動(Auto)** 或是**手動(Manual)**。 如果選擇了手動(Manual)，需指定主要與次要 DNS 伺服器。 **IPv6 主要 DNS(IPv6 Primary DNS)** – 輸入主要 DNS 伺服器位址。 **IPv6 次要 DNS(IPv6 Secondary DNS)** - 輸入次要 DNS 伺服器位址。
IPv6 WAN 連線偵測(IPv6 WAN Connection Detection)	
模式(Mode)	**永遠連線(Always On)** - 路由器假定廣域網路連線始終處於作用中狀態。 **NS 偵測(NS Detect)** - 路由器透過發出鄰居請求封包來驗證連線。 **Ping 偵測(Ping Detect)** -路由器會根據 ping 間隔設置，向 Ping 閘道 IP 欄位中指定的位址的主機發送 ICMP（Internet 控制訊息協定）回應請求，以驗證 WAN 連線。如果遠端主機在指定秒數（由 ping 間隔定義）內沒有回應，則認為 WAN 連線失敗。 如果你選擇 **Ping 偵測(Ping Detect)**作為檢測模式，您需要輸入以下項目的必要設定。 • **主要 Ping IP (Primary Ping IP)** – 在此欄位中輸入要 ping 的 IP 位址。 • **次要 Ping IP (Secondary Ping IP)** – 請在此欄位中輸入要 ping 的

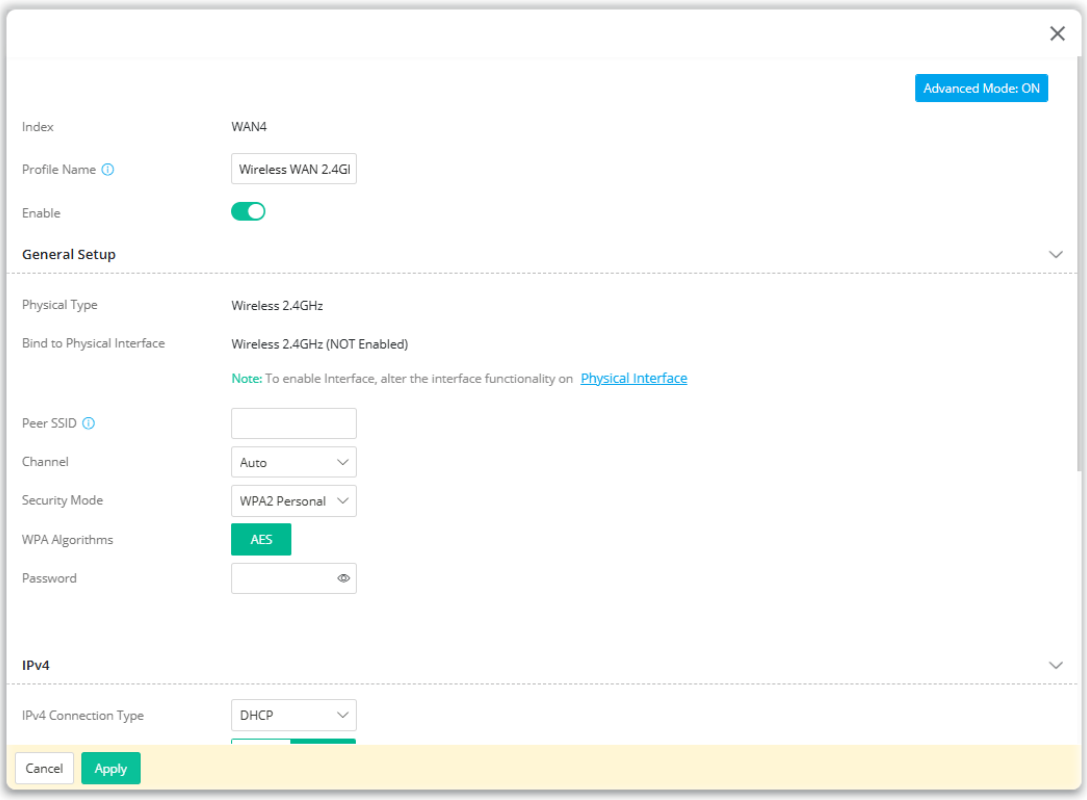
	IP 位址。 • **TTL** – 存活時間（Time To Live），即到達 ping 目標位址允許的最大跳數。有效值範圍為 1 到 255。 • **Ping 間隔(10-3600 秒) (Ping Interval (Sec, 10-3600))** – 輸入系統執行 PING 操作的間隔。 • **Ping 重試次數(Ping Retry)** - 輸入在判定 WAN 斷開連線之前，系統允許執行 PING 操作的次數。
MTU	
MTU	最大傳輸單元 (MTU) 是指可以傳送到廣域網路 (WAN) 的最大資料封包的大小（以位元組為單位）。最大值為 1500。對於 PPPoE 連線而言，因為 PPPoE 連線會額外增加 8 位元組的封包標頭，因此原本 Ethernet 的最大 MTU 1500 位元組需要扣掉這 8 位元組，所以 PPPoE 的最大 MTU 為 1492 位元組。
WAN MAC 位址(WAN MAC Address)	
模式(Mode)	**預設值(Default)** – 使用 WAN 連接埠的預設 MAC 位址。 **客製化(Customized)** - 如果您的 ISP 透過 MAC 位址進行驗證，請選擇此選項。 • **MAC** - 為 WAN 乙太網路連接埠指定 MAC 位址。
MAC	顯示此裝置的 MAC 位址。
取消(Cancel)	捨棄目前設定並回到前一頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

傳送資料模式為無線 2.4GHz

當選擇無線 2.4G 作為傳送資料模式時，WAN 介面將採用無線站點模式存取網際網路。路由器可作為 2.4GHz 無線站點，並連接到指定的無線基地台(AP)。

按下 WAN4 的**編輯(Edit)**鏈結，即可開啟如下頁面。



可用設定說明如下：

項目	說明
進階模式:開啟/關閉 (Advanced Mode:ON/OFF)	按此顯示或隱藏 WAN 介面的進階設定(如 WAN MAC 位址)。
索引(Index)	顯示目前廣域網路 WAN 介面。
設定檔名稱(Profile Name)	顯示設定檔名稱。
啟用(Enable)	切換開關即可啟用或停用此功能。
基本設定(General Setup)	
傳送資料模式 (Physical Type)	顯示此介面使用的傳送資料模式。
綁定至實體介面(Bind to Physical Interface)	目前，僅 WAN3 支援 2.4GHz 無線連線。
對方 SSID (Peer SSID)	輸入無線裝置的識別碼。
頻道(Channel)	選擇裝置的頻率頻道。

安全性模式(Security Mode)	我們提供了多種模式供您選擇。每種模式都會顯示不同的參數（例如，網路安全性金鑰）供您設定。 **WPA3 個人版 (WPA3 Personal)** – 路由器以 WPA3 用戶端身分連接到無線 AP，加密金鑰應以 PSK 格式輸入。 **WPA2 個人版 (WPA2 Personal)** – 路由器以 WPA2 用戶端身分連接至無線 AP，加密金鑰應以 PSK 格式輸入。 **開放(OPEN)** – 加密機制已關閉。
WPA 演算法(WPA Algorithms)	選擇 AES 作為 WPA 加密演算法。
密碼(Password)	進入 **8~64**ASCII 字元，例如 012345678..（或以 0x 開頭的 64 個十六進位數字，例如 "0x321253abcde..." ）。
IPv4	
IPv4 連接類型(IPv4 Connection Type)	當選擇兩者(Both)或 IPv4 作為 IP 版本時，可使用此功能。 **DHCP** – 路由器從 DHCP 伺服器接收 IP 設定資訊。 ● **WAN DNS** – 選擇**自動(Auto)**或**手動(Manual)**。 如果選擇了手動(Manual)，需指定主要與次要 DNS 伺服器。 **IPv4 主要 DNS(IPv4 Primary DNS)** – 輸入主要 DNS 伺服器位址。 **IPv4 次要 DNS(IPv4 Secondary DNS)** - 輸入次要 DNS 伺服器位址。. **靜態 IP (Static IP)** – 將存取模式設定為靜態 IP。 ● **IP 位址 (IP Address)** – 由網際網路服務供應商 (ISP) 指派的廣域網路 IP 位址。 ● **子網遮罩(Subnet Mask)** – WAN 子網路遮罩。 ● **閘道 IP(Gateway IP)** – WAN 閘道的 IP 位址。 ● **IPv4 主要 DNS (IPv4 Primary DNS)** – 主要 DNS 伺服器的 IP 位址。 ● **IPv4 次要 DNS (IPv4 Secondary DNS)** – 次要 DNS 伺服器的 IP 位址。
WAN 連線偵測(WAN Connection Detection)	
模式(Mode)	設定如何監控廣域網路連線。 **永遠連線(Always On) -** 路由器假定廣域網路連線始終處於作用中狀態。 **ARP 偵測(ARP Detect)** - 路由器每 5 秒廣播一次 ARP 請求。如果在 30 秒內沒有收到回應，則認為 WAN 連線失敗。 **Ping 偵測(Ping Detect)** - 路由器會根據 ping 間隔設置，向 Ping 閘道 IP 欄位中指定的位址的主機發送 ICMP（Internet 控制訊息協定）回應請求，以驗證 WAN 連線。如果遠端主機在指定秒數（由 ping 間隔定義）內沒有回應，則認為 WAN 連線失敗。 如果你選擇 **Ping 偵測(Ping Detect)**作為檢測模式，您需要輸入以下項目的必要設定。 ● **Ping 閘道 IP (Ping Gateway IP)** - 切換此開關以啟用/使用目前 WAN 閘道 IP 位址進行 ping 測試。透過 ping 測試 IP 位址，Vigor 路由器可以檢查 WAN 連線是否已開啟。 ● **TTL** – 存活時間（Time To Live），即到達 ping 目標位址允許的最大跳數。有效值範圍為 1 到 255。 ● **Ping 間隔(5-3600 秒) (Ping Interval (Sec, 5-3600))** – 輸入系統執行 PING 操作的間隔。 ● **Ping 重試次數(Ping Retry)** - 輸入在判定 WAN 斷開連線之前，系統允許執行 PING 操作的次數。

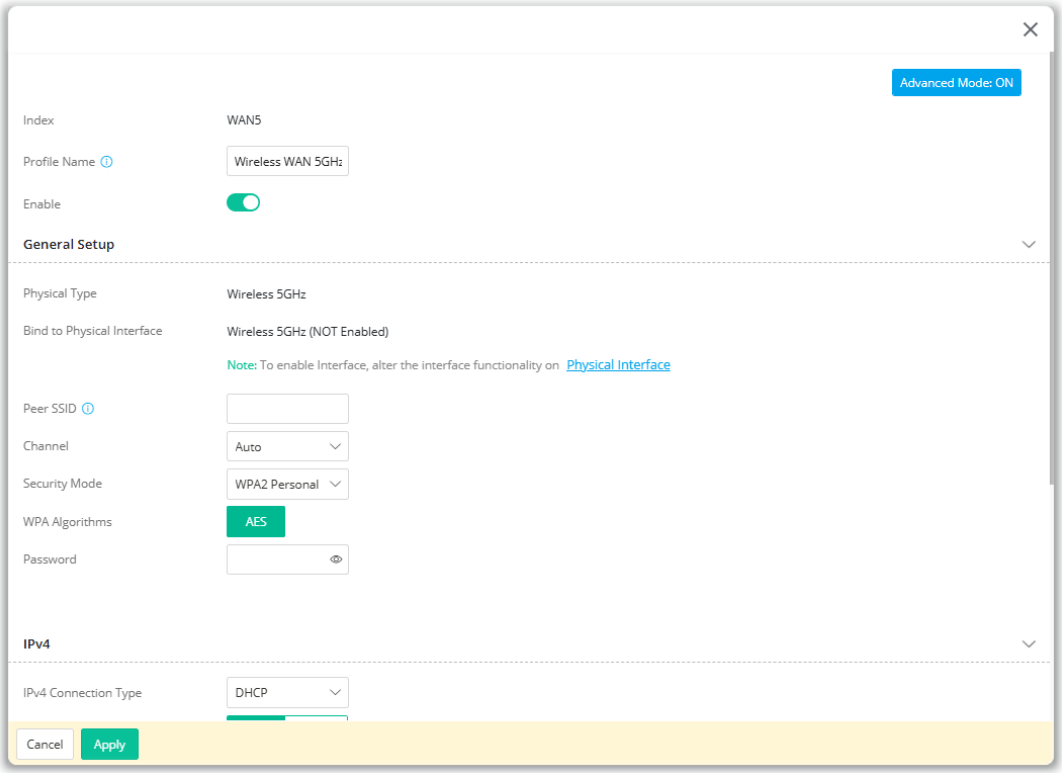
MTU	
MTU	最大傳輸單元 (MTU) 是指可以傳送到廣域網路 (WAN) 的最大資料封包的大小（以位元組為單位）。最大值為 1500。
WAN MAC 位址(WAN MAC Address)	
模式(Mode)	此功能僅在進階模式啟用時可用。 **預設值(Default)** – 使用無線廣域網路的預設 MAC 位址。 **客製化(Customized)** - 如果您的 ISP 透過 MAC 位址進行驗證，請選擇此選項。 • **MAC** - 為無線廣域網路指定 MAC 位址。
取消(Cancel)	捨棄目前設定並回到前一頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

傳送資料模式為無線 5GHz

當選擇無線 5G 作為傳送資料模式時，WAN 介面將採用無線站點模式存取網際網路。路由器可作為 5GHz 無線站點，並連接到指定的無線基地台(AP)。

按下 WAN5 的**編輯(Edit)**鏈結，即可開啟如下頁面。



可用設定說明如下：

項目	說明
進階模式:開啟/關閉 (Advanced Mode:ON/OFF)	按此顯示或隱藏 WAN 介面的進階設定(如 WAN MAC 位址)。

索引(Index)	顯示目前廣域網路 WAN 介面。
設定檔名稱(Profile Name)	顯示設定檔名稱。
啟用(Enable)	切換開關即可啟用或停用此功能。
基本設定(General Setup)	
傳送資料模式 (Physical Type)	顯示此介面使用的傳送資料模式。
綁定至實體介面(Bind to Physical Interface)	目前，WAN5 支援 5GHz 無限連線。
對方 SSID (Peer SSID)	輸入無線裝置的識別碼。
頻道(Channel)	選擇裝置的頻率頻道。
安全性模式(Security Mode)	我們提供了多種模式供您選擇。每種模式都會顯示不同的參數 (例如，網路安全性金鑰) 供您設定。 **WPA3 個人版 (WPA3 Personal)** – 路由器以 WPA3 用戶端身分連接到無線 AP，加密金鑰應以 PSK 格式輸入。 **WPA2 個人版 (WPA2 Personal)** – 路由器以 WPA2 用戶端身分連接至無線 AP，加密金鑰應以 PSK 格式輸入。 **開放(OPEN)** – 加密機制已關閉。
WPA 演算法(WPA Algorithms)	選擇 AES 作為 WPA 加密演算法。
密碼(Password)	進入 **8~64**ASCII 字元，例如 012345678.. (或以 0x 開頭的 64 個十六進位數字，例如 “0x321253abcde...”) 。
IPv4	
IPv4 連接類型(IPv4 Connection Type)	當選擇兩者(Both)或 IPv4 作為 IP 版本時，可使用此功能。 **DHCP** – 路由器從 DHCP 伺服器接收 IP 設定資訊。 ● **WAN DNS** – 選擇**自動(Auto)**或**手動(Manual)**。 如果選擇了手動(Manual)，需指定主要與次要 DNS 伺服器。 **IPv4 主要 DNS(IPv4 Primary DNS)** – 輸入主要 DNS 伺服器位址。 **IPv4 次要 DNS(IPv4 Secondary DNS)** - 輸入次要 DNS 伺服器位址。. **靜態 IP (Static IP)** – 將存取模式設定為靜態 IP。 ● **IP 位址 (IP Address)** – 由網際網路服務供應商 (ISP) 指派的廣域網路 IP 位址。 ● **子網遮罩(Subnet Mask)** – WAN 子網路遮罩。 ● **閘道 IP(Gateway IP)** – WAN 閘道的 IP 位址。 ● **IPv4 主要 DNS (IPv4 Primary DNS)** – 主要 DNS 伺服器的 IP 位址。 ● **IPv4 次要 DNS (IPv4 Secondary DNS)** – 次要 DNS 伺服器的 IP 位址。
WAN 連線偵測(WAN Connection Detection)	
模式(Mode)	設定如何監控廣域網路連線。 **永遠連線(Always On) -** 路由器假定廣域網路連線始終處於作用中狀態。 **ARP 偵測(ARP Detect)** - 路由器每 5 秒廣播一次 ARP 請求。如果在 30 秒內沒有收到回應，則認為 WAN 連線失敗。

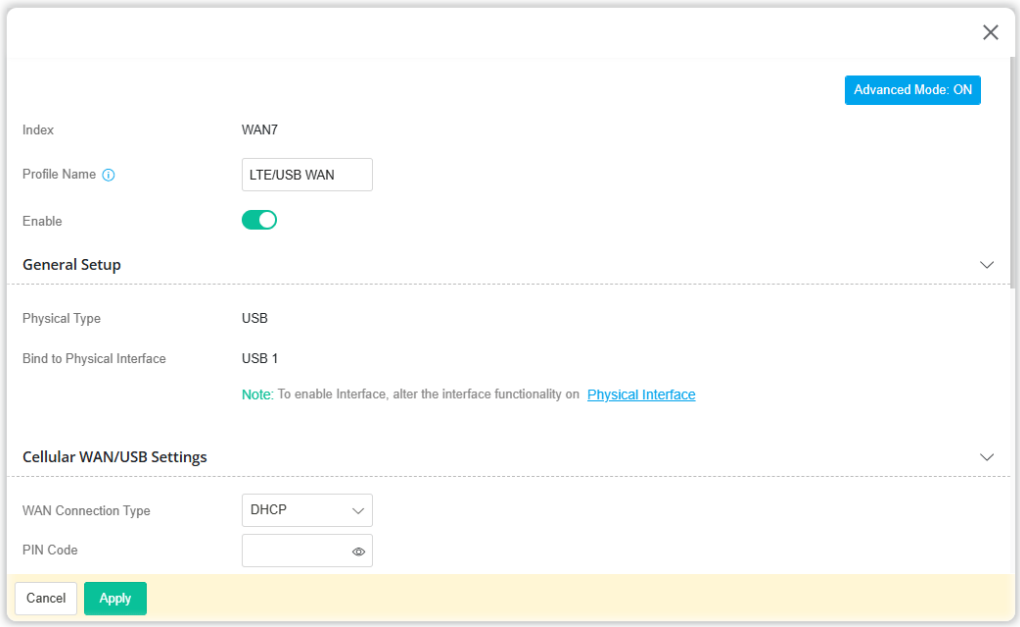
	Ping 偵測(Ping Detect) - 路由器會根據 ping 間隔設置，向 Ping 閘道 IP 欄位中指定的位址的主機發送 ICMP（Internet 控制訊息協定）回應請求，以驗證 WAN 連線。如果遠端主機在指定秒數（由 ping 間隔定義）內沒有回應，則認為 WAN 連線失敗。 如果你選擇 **Ping 偵測(Ping Detect)**作為檢測模式，您需要輸入以下項目的必要設定。 ● **Ping 閘道 IP (Ping Gateway IP)** - 切換此開關以啟用/使用目前 WAN 閘道 IP 位址進行 ping 測試。透過 ping 測試 IP 位址，Vigor 路由器可以檢查 WAN 連線是否已開啟。 ● **TTL** – 存活時間（Time To Live），即到達 ping 目標位址允許的最大跳數。有效值範圍為 1 到 255。 ● **Ping 間隔(10-3600 秒) (Ping Interval (Sec, 10-3600))** – 輸入系統執行 PING 操作的間隔。 ● **Ping 重試次數(Ping Retry)** - 輸入在判定 WAN 斷開連線之前，系統允許執行 PING 操作的次數。
MTU	
MTU	最大傳輸單元 (MTU) 是指可以傳送到廣域網路 (WAN) 的最大資料封包的大小（以位元組為單位）。最大值為 1500。
WAN MAC 位址(WAN MAC Address)	
模式(Mode)	此功能僅在進階模式啟用時可用。 **預設值(Default)** – 使用無線廣域網路的預設 MAC 位址。 **客製化(Customized)** - 如果您的 ISP 透過 MAC 位址進行驗證，請選擇此選項。 ● **MAC** - 為無線廣域網路指定 MAC 位址。
取消(Cancel)	捨棄目前設定並回到前一頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

傳送資料模式為 USB

僅適用於 USB 數據機連線。

按下 WAN7 或 WAN8 的**編輯(Edit)**鏈結，即可開啟如下頁面。



可用設定說明如下：

項目	說明
進階模式:開啟/關閉 (Advanced Mode:ON/OFF)	按此顯示或隱藏 WAN 介面的進階設定(如 WAN MAC 位址)。
索引(Index)	顯示目前廣域網路 WAN 介面。
設定檔名稱(Profile Name)	顯示設定檔名稱。
啟用(Enable)	切換開關即可啟用或停用此功能。
基本設定(General Setup)	
傳送資料模式 (Physical Type)	顯示此介面使用的傳送資料模式。
IP 版本(IP Version)	設定此 WAN 介面所使用的協定（IPv4 或 IPv6 或兩者都用）。
行動網路 WAN/ USB 設定 (Cellular WAN/USB Settings)	
WAN 連線類型(WAN Connection Type)	**DHCP** – 使用動態主機設定協定 (DHP) 建立連線。 ● **PIN 碼 (PIN Code)** – 數據機中 SIM 卡的 PIN 碼。 PIN 碼最大長度為 15 個字元。 ● **啟用使用者名稱/密碼/驗證 (Enable Username/Password Authentication)** –切換開關即可啟用或停用此功能。 **驗證(Authentication)** – 選擇用於 PPP 身份驗證的協定。 **限用 PAP (PAP only)** – 僅使用 PAP（密碼驗證協定）。 **PAP 或 CHAP (PAP or CHAP)** – PAP 和 CHAP（詢問握手驗證協定）皆可用於 PPP 認證。路由器與 PPTP 或 L2TP 伺服器協商以確定使用哪種協定。

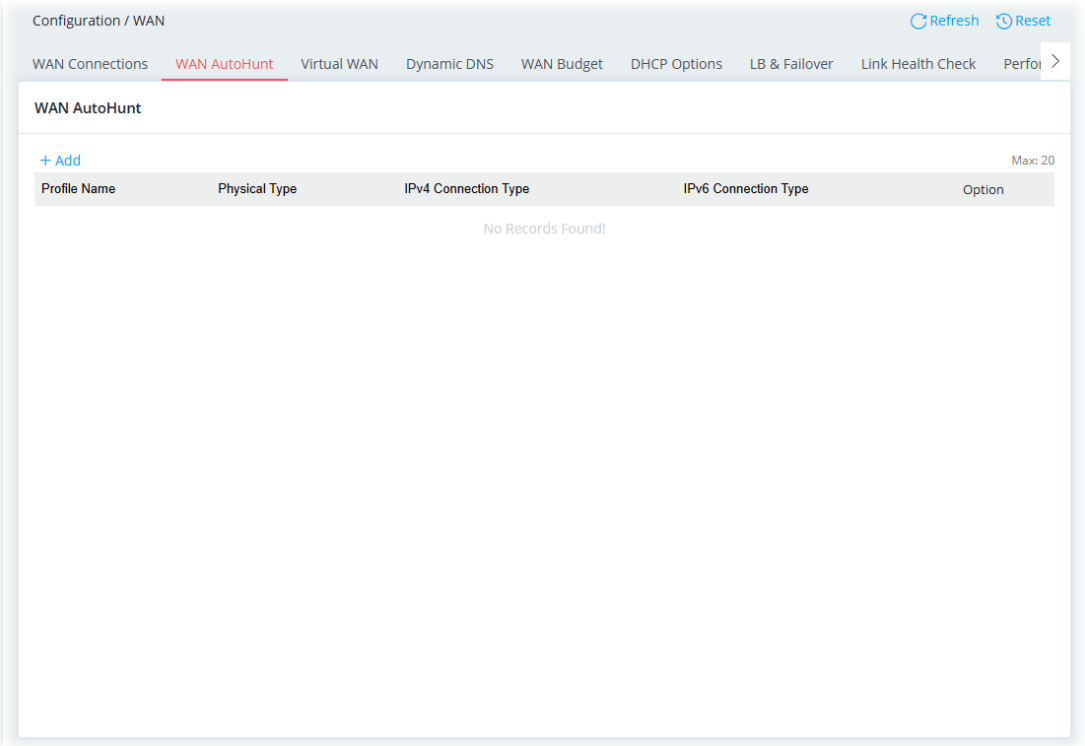
	使用者名稱(Username) – ISP 提供的用於身份驗證的使用者名稱(選項設定)。 **密碼(Password)** - ISP 提供的用於身份驗證的密碼(選項設定)。 ● **自動 APN 名稱(Auto APN Name)**–用於連線的存取點名稱(Access Point Name)。請聯絡您的網際網路服務供應商或電信商以取得正確的名稱。 ● **網路模式(Network Mode)** – 強制 Vigor 路由器以此處指定的模式連接網際網路。如果您選擇 5G/4G/3G 作為網路模式，路由器將依照實際無線訊號自動選擇適當的模式。 **PPP** - 使用點對點協定建立連線。 ● **PIN 碼 (PIN Code)** – 數據機中 SIM 卡的 PIN 碼。 PIN 碼最大長度為 15 個字元。 ● **啟用使用者名稱/密碼/驗證 (Enable Username/Password Authentication)** –切換開關即可啟用或停用此功能。 **驗證(Authentication)** – 選擇用於 PPP 身份驗證的協定。 **限用 PAP (PAP only)** – 僅使用 PAP (密碼驗證協定) 。 **PAP 或 CHAP (PAP or CHAP)** – PAP 和 CHAP (詢問握手驗證協定) 皆可用於 PPP 認證。路由器與 PPTP 或 L2TP 伺服器協商以確定使用哪種協定。 **使用者名稱(Username)** – ISP 提供的用於身份驗證的使用者名稱(選項設定)。 **密碼(Password)** - ISP 提供的用於身份驗證的密碼(選項設定)。 ● **產生數據機初始化字串方式(Generate Modem Initial String by)** – 選擇產生數據機初始字串的方法。 **依循 APN 名稱(Following APN Name)** – 使用 APN 名稱作為數據機的初始字串。 **客製化字串(Customized String)** – 將一個字串設定為數據機的初始字串。 **數據機初始化字串(選項設定) (Modem Initial String (Optional))** – 用於初始化 USB 數據機。請聯絡您的網路服務供應商。 ● **自動 APN 名稱(Auto APN Name)** –用於連線的存取點名稱(Access Point Name)。請聯絡您的網際網路服務供應商或電信商以取得正確的名稱。 ● **數據機初始化字串 2(選項設定) (Modem Initial String2 (Optional))** – 初始字串 1 與 APN 共用。在某些情況下，使用者可能需要另一個初始 AT 指令來限制 3G 頻段或進行任何特殊設定。 ● **數據機撥號字串(選項設定)(Modem Dial String (Optional))** – 用於透過 USB 模式撥號。請使用預設值。如有任何疑問，請聯絡您的網路服務供應商 (ISP)。 ● **Service Name (Optional)** – PPP 服務名稱標籤。部分 ISP 需要此項目。除非您的 ISP 另有指示，否則請留空。此功能僅在啟用進階模式時可用。
IPv4 – WAN 連線偵測(WAN Connection Detection)	
WAN DNS	選擇**自動(Auto)**或**手動(Manual)**。 如果選擇了手動(Manual)，需指定主要與次要 DNS 伺服器。 ● **IPv4 主要 DNS(IPv4 Primary DNS)** – 輸入主要 DNS 伺服器位址。 ● **IPv4 次要 DNS(IPv4 Secondary DNS)** - 輸入次要 DNS 伺服器位址。
模式(Mode)	設定如何監控廣域網路連線。 **永遠連線(Always On)** - 路由器假定廣域網路連線始終處於作用中狀態。 **Ping 偵測(Ping Detect)** –路由器會根據 ping 間隔設置，向 Ping 閘道 IP 欄位中指定的位址的主機發送 ICMP (Internet 控制訊息協定) 回應請求，以驗證 WAN 連線。如果遠端主機在指定秒數 (由 ping 間隔定義) 內沒

	有回應，則認為 WAN 連線失敗。 如果你選擇 **Ping 偵測(Ping Detect)**作為檢測模式，您需要輸入以下項目的必要設定。 ● **Ping 閘道 IP (Ping Gateway IP)** – 切換此開關以啟用/使用目前 WAN 閘道 IP 位址進行 ping 測試。透過 ping 測試 IP 位址，Vigor 路由器可以檢查 WAN 連線是否已開啟。 ● **TTL** – 存活時間（Time To Live），即到達 ping 目標位址允許的最大跳數。有效值範圍為 1 到 255。 ● **Ping 間隔(10-3600 秒) (Ping Interval (Sec, 10-3600))** – 輸入系統執行 PING 操作的間隔。 ● **Ping 重試次數(Ping Retry)** - 輸入在判定 WAN 斷開連線之前，系統允許執行 PING 操作的次數。
MTU	
MTU	最大傳輸單元 (MTU) 是指可以傳送到廣域網路 (WAN) 的最大資料封包的大小（以位元組為單位）。最大值為 1500。對於 PPPoE 連線而言，因為 PPPoE 連線會額外增加 8 位元組的封包標頭，因此原本 Ethernet 的最大 MTU 1500 位元組需要扣掉這 8 位元組，所以 PPPoE 的最大 MTU 為 1492 位元組。
WAN MAC 位址(WAN MAC Address)	
模式(Mode)	**預設值(Default)** – 使用 WAN 連接埠的預設 MAC 位址。 **客製化(Customized)** - 如果您的 ISP 透過 MAC 位址進行驗證，請選擇此選項。 ● **MAC** - 為 WAN 乙太網路連接埠指定 MAC 位址。
取消(Cancel)	捨棄目前設定並回到前一頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-1-2-2 WAN 設定自動偵測(WAN AutoHunt)

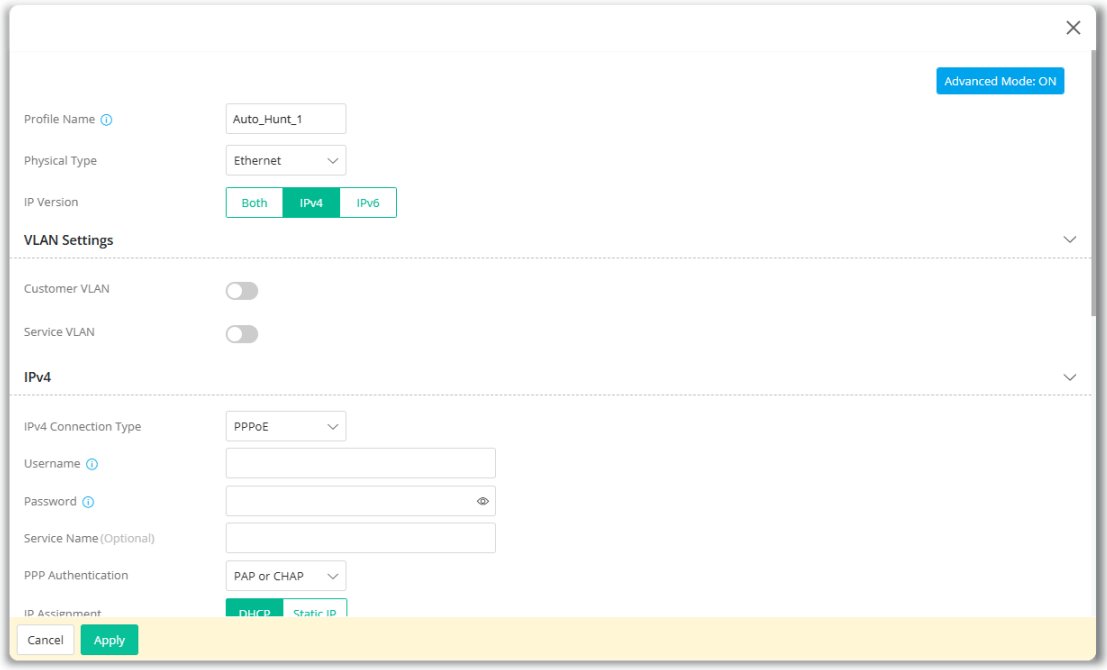
Vigor 路由器將自動連接到乙太網路 WAN 連接埠。連接並通電後，路由器將運行一系列網路連線設定（基於自動偵測設定檔）以確定是否可以建立連線。如果連接失敗，路由器將繼續嘗試下一個 ISP 設置，直到獲得 IP 位址。



項目	說明
重置(Reset)	按下清除所有設定文件，回復出廠設定值。
+新增(+Add)	按一下以開啟虛擬 WAN 設定檔（最多 5 個）的設定頁面。

乙太網路傳送資料模式之自動偵測

欲新增自動偵測設定檔，請按**+新增(+Add)**鏈結即可開啟如下頁面。



可用設定說明如下：

項目	說明
進階模式:開啟/關閉 (Advanced Mode:ON/OFF)	按此顯示或隱藏 WAN 介面的進階設定(如 IP 別名與 WAN MAC 位址)。
設定檔名稱(Profile Name)	輸入字串作為設定檔名稱，供辨識使用。
傳送資料模式 (Physical Type)	顯示 WAN 介面的傳送資料模式。
IP 版本(IP Version)	為此 WAN 介面選擇 IP 版本(IPv4、IPv6 或二者)。
VLAN Settings	
顧客 VLAN (Customer VLAN)	切換此開關以啟用或停用帶有標籤的 VLAN 功能。如果啟用，請輸入標籤和優先權值。 **標籤(Tag)** – 輸入 VLAN ID 號碼。範圍為 0 到 4094。 **優先權(Priority)** – 輸入該 VLAN 的封包優先編號。範圍為 0 到 7。
服務 VLAN (Service VLAN)	切換此開關以啟用或停用帶有標籤的 VLAN 功能。如果啟用，請輸入標籤和優先權值。 **標籤(Tag)** – 輸入 VLAN ID 號碼。範圍為 0 到 4094。 **優先權(Priority)** – 輸入該 VLAN 的封包優先編號。範圍為 0 到 7。
IPv4	
IPv4 連接類型(IPv4 Connection Type)	當選擇兩者(Both)或 IPv4 作為 IP 版本時，可使用此功能。 **PPPoE** – 將存取模式設定為 PPPoE。 ● **使用者名稱(Username)** – ISP 提供的 PPPoE 驗證的使用者名稱。 ● **密碼(Password)** – ISP 提供的 PPPoE 驗證的密碼。 ● **服務名稱(Service Name)** – PPP 服務名稱標籤。部分 ISP 需要此項目。除非您的 ISP 另有指示，否則請留空。此功能僅在啟用進階模式時可用。 **PPP 驗證(PPP Authentication)** – 用於 PPP 驗證的協定。**PAP 或 CHAP** - PAP 和 CHAP (詢問握手認證協定) 皆可用於 PPP 認證。路由器會與 PPTP 或 L2TP 伺服器協商以確定使用哪種協定。此功能僅在進階模式啟用時可用。 ● **IP 分派(IP Assignment)** – 此功能僅在啟用進階模式時可用。當選擇 PPPoE 作為 IPv4 連線類型時，即可使用此功能。 **DHCP** - 位址是動態分配的。 **靜態 IP (Static IP)** - 您的網路服務供應商已指派一個固定的廣域網路 IP 位址。請輸入 IP 位址。 ● **WAN DNS** – 選擇**自動(Auto)**或**手動(Manual)**。 如果選擇了手動(Manual)，需指定主要與次要 DNS 伺服器。 **IPv4 主要 DNS(IPv4 Primary DNS)** – 輸入主要 DNS 伺服器位址。 **IPv4 次要 DNS(IPv4 Secondary DNS)** - 輸入次要 DNS 伺服器位址。 **DHCP** – 路由器從 DHCP 伺服器接收 IP 設定資訊。 ● **WAN DNS** – Select **Auto** or **Manual**. ● **WAN DNS** – 選擇**自動(Auto)**或**手動(Manual)**。 如果選擇了手動(Manual)，需指定主要與次要 DNS 伺服器。 **IPv4 主要 DNS(IPv4 Primary DNS)** – 輸入主要 DNS 伺服器位址。

	IPv4 次要 DNS(IPv4 Secondary DNS) - 輸入次要 DNS 伺服器位址。 **靜態 IP (Static IP)** – 將存取模式設定為靜態 IP。 ● **IP 位址 (IP Address)** – 由網際網路服務供應商 (ISP) 指派的廣域網路 IP 位址。 ● **子網遮罩(Subnet Mask)** – WAN 子網路遮罩。 ● **閘道 IP(Gateway IP)** – WAN 閘道的 IP 位址。 ● **IPv4 主要 DNS (IPv4 Primary DNS)** – 主要 DNS 伺服器的 IP 位址。 ● **IPv4 次要 DNS (IPv4 Secondary DNS)** – 次要 DNS 伺服器的 IP 位址。 **對外流量 DNS 查詢 IP (Outbound DNS Query IP)** - 此功能僅在啟用進階模式時可用。請指定路由器用於發送 DNS 查詢的來源 IP 位址。 ● **預設 IP (Default IP)** – 查詢 IP 由 Vigor 路由器自動設定。 ● **別名 IP (Alias IP)** – 輸入使用者自訂的用於 DNS 查詢的 IP 位址。
	WAN 連線偵測(WAN Connection Detection)
模式(Mode)	設定如何監控廣域網路連線。 **永遠連線(Always On)** - 路由器假定廣域網路連線始終處於作用中狀態。 **ARP 偵測(ARP Detect)** - 路由器每 5 秒廣播一次 ARP 請求。如果在 30 秒內沒有收到回應，則認為 WAN 連線失敗。 **Ping 偵測(Ping Detect)** - 路由器會根據 ping 間隔設置，向 Ping 閘道 IP 欄位中指定的位址的主機發送 ICMP (Internet 控制訊息協定) 回應請求，以驗證 WAN 連線。如果遠端主機在指定秒數 (由 ping 間隔定義) 內沒有回應，則認為 WAN 連線失敗。 如果你選擇 **Ping 偵測(Ping Detect)**作為檢測模式，您需要輸入以下項目的必要設定。 ● **Ping 閘道 IP (Ping Gateway IP)** - 切換此開關以啟用/使用目前 WAN 閘道 IP 位址進行 ping 測試。透過 ping 測試 IP 位址，Vigor 路由器可以檢查 WAN 連線是否已開啟。 ● **TTL** – 存活時間 (Time To Live) ，即到達 ping 目標位址允許的最大跳數。有效值範圍為 1 到 255。 ● **Ping 間隔(5-3600 秒) (Ping Interval (Sec, 5-3600))** – 輸入系統執行 PING 操作的間隔。 ● **Ping 重試次數(Ping Retry)** - 輸入在判定 WAN 斷開連線之前，系統允許執行 PING 操作的次數。
IP 別名(IP Alias)	**IPv4 別名(IPv4 Alias)** - 如果您有多個真實 IP 位址，並希望在 WAN 介面上使用它們，請使用 WAN IP 別名。除了目前正在使用的真實 IP 位址之外，您最多可以設定 8 個真實 IP 位址。 **+新增(+Add)** – 按下**+新增(+Add)** 輸入 IPv4 位址作為 IPv4 別名。
	IPv6
IPv6 連線類型(IPv6 Connection Type)	當選擇兩者(Both)或 IPv6 作為 IP 版本時，可使用此功能。 **斷線(Offline)** – 選擇離線時，IPv6 連線將會停用。 **PPP** – 在 PPPoE 協商過程中，IPv6 WAN 位址會與 IPv4 WAN 位址一起指派。這種 IPv6 存取模式會要求 IPv4 使用 PPPoE 協定。 **靜態(Static)** – 設定 ISP 分配的靜態 IPv6 設定。 ● **+新增(+Add)** – 按一下此按鈕，將 IPv6 位址和前置碼長度欄位中的值新增至全球位址表(Global Address Table)。 ● **IPv6 全球位址(IPv6 Global Address)** – 由網際網路服務供應商 (ISP) 指派的廣域網路 IPv6 位址。 ● **前置碼長度(Prefix Length)** – IPv6 前置碼的長度。

- **閘道位址(Gateway Address) –** ISP 閘道的 IPv6 位址。

DHCPv6 – 使用 DHCPv6 協定從伺服器取得 IPv6 位址。

- **DUID** – 顯示此 WAN 介面所使用的 DHCP 唯一 ID。
- **IAID** – 用於識別此 WAN 介面的唯一整數。
- **驗證通訊協定(Authentication Protocol)** - 此協定用於用戶端在存取網際網路之前透過 DHCPv6 伺服器進行身份驗證。可以指定三種類型：**重新設定金鑰(Reconfigure Key)**，**延遲(Delayed)**和**無(None)**。通常情況下，預設為**無(None)**。
  - **重新設定金鑰(Reconfigure Key)** – 在連線過程中，DHCPv6 伺服器將自動對用戶端進行身份驗證。
  - **延遲(Delayed)** - 在連線過程中，DHCPv6 伺服器將根據這些欄位中指定的金鑰 ID、領域和秘鑰資訊對用戶端進行身份驗證和識別。
    金鑰 ID (Key ID) – 輸入一個值 (範圍從 1 到 65535)，該值將用於產生 HMAC-MD5 值。
    領域(Realm) – 在此輸入的名稱 (1 到 31 個字元) 將標識產生 HMAC-MD5 值的密鑰。
    密鑰(Secret) – 輸入一段文字 (1 到 31 個字元) 作為每個 DHCP 伺服器上每個用戶端的唯一識別碼。

TSPC -通道建立協定用戶端（TSPC）是一款可以幫助您輕鬆連接到 IPv6 網路的應用程式。

請確保您的 IPv4 WAN 連線正常，並從 hexago 申請免費帳戶（http://gogonet.gogo6.com/page/freenet6-account 在您嘗試使用 TSPC 進行網路連線之前，請先進行設定。TSPC 會連線到通道代理，並根據設定檔中的規格請求通道。它會從通道代理程式取得公用 IPv6 位址和 IPv6 前置碼，然後在背景監控通道的狀態。

在取得 IPv6 前置碼並啟動路由器通告守護程式（RADVD）後，該路由器後面的 PC 可以直接連接到 IPv6 網際網路。

- **通道代理伺服器位址(Tunnel Broker Address)** – 輸入位址通道代理 IP 位址、FQDN 或選用連接埠號碼。
- **使用者名稱(Username)** – 建議您使用另一個使用者名稱和密碼。http://gogonet.gogo6.com/page/freenet6-account。
- **密碼(Password)** -輸入與使用者名稱關聯的密碼。

6in4 –為 WAN 介面設定 6in4 靜態通道。

然而，6in4 提供了一個 2002::0/16 之外的前置碼。如此一來，您可以使用固定端點，而不是任何類型轉換端點。這種模式更加可靠。

- **啟用 IPv4 WAN Ping 存取 6in4/6rd 通道 (Enable IPv4 WAN Ping Access for 6in4/6rd Tunnel)** – 若要使用此 6in4 連線類型，必須允許 IPv4 WAN 存取，且防火牆必須允許通道代理 IP 位址通過。
- **遠端終點 IPv4 位址(Remote Endpoint IPv4 Address)** – 由通道提供者指派的 WAN IPv6 位址。
- **6in4 IPv6 位址(6in4 IPv6 Address)** – 由通道提供者指派的 WAN IPv6 位址。
- **6in4 IPv6 前置碼長度(6in4 IPv6 Prefix Length) –** 通道提供者指派的 WAN IPv6 前置碼長度。
- **LAN 路由前置碼(LAN Routed Prefix) –** 區域網路 IPv6 位址前置碼。
- **LAN 路由前置碼長度(LAN Routed Prefix Length) –**區域網路 IPv6 位址前置碼長度。
- **通道 TTL (Tunnel TTL) –** 存活時間值，即允許到達端點的最大躍點數。

6rd -為 WAN 介面設定 6rd。

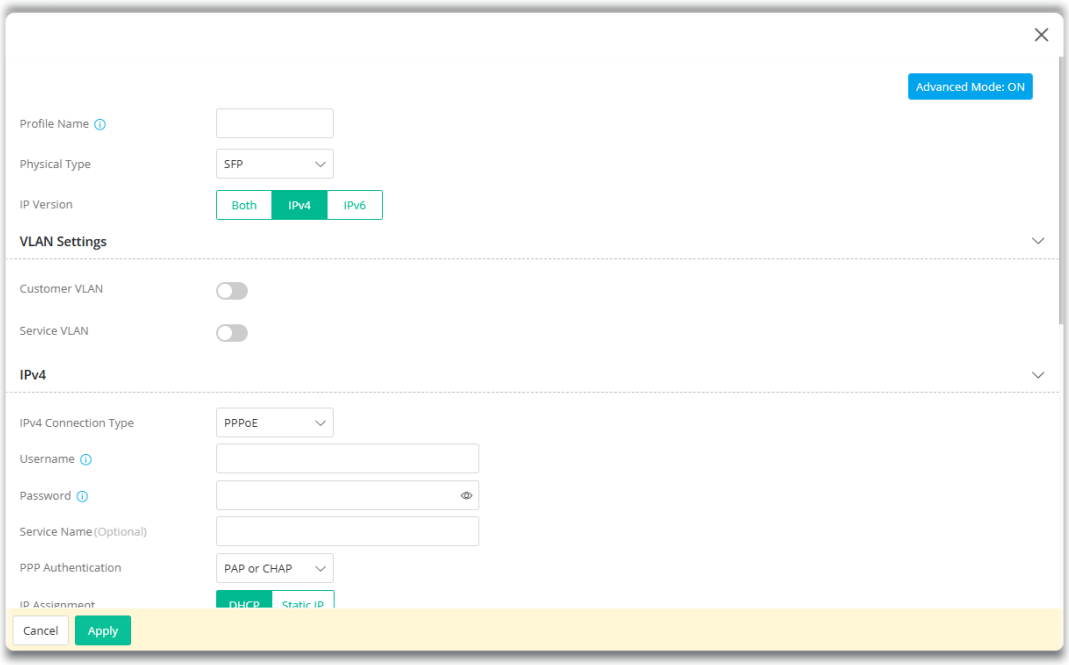
- **啟用 IPv4 WAN Ping 存取 6in4/6rd 通道(Enable IPv4 WAN Ping**

	Access for 6in4/6rd Tunnel) – 要使用 6rd 連線類型，必須允許 IPv4 WAN 訪問，且防火牆必須允許通道代理 IP 位址通過。 • **模式(Mode)** – 兩種選項 : **自動(Auto)**和**靜態(Static)**態。**自動(Auto)** - 路由器與 DHCPv4 搭配使用時，會自動使用選項 212 設定 IPv6。**靜態(Static)**- IPv6 設定資訊是手動輸入的。**若是**選取**靜態(Static)**，須設定以下內容： - **IPv4 邊界中繼(IPv4 Border Relay)** – 輸入給予 6rd 網域的 6rd 邊界中繼的 IPv4 位址。 - **6rd 前置碼(6rd Prefix)** – 輸入 6rd IPv6 位址。 - **6rd 前置碼長度(6rd Prefix Length)** - 輸入 6rd IPv6 前置碼長度（以位元為單位）。 • **WAN DNS** – 選擇**自動(Auto)** 或是**手動(Manual)**。 如果選擇了手動(Manual)，需指定主要與次要 DNS 伺服器。 **IPv6 主要 DNS(IPv6 Primary DNS)** – 輸入主要 DNS 伺服器位址。 **IPV6 次要 DNS(IPv6 Secondary DNS)** - 輸入次要 DNS 伺服器位址。
IPv6 WAN 連線偵測(IPv6 WAN Connection Detection)	
模式(Mode)	設定如何監控廣域網路連線。 **永遠連線(Always On)** - 路由器假定廣域網路連線始終處於作用中狀態。 **NS 偵測(NS Detect)** - 路由器透過發出鄰居請求封包來驗證連線。 **Ping 偵測(Ping Detect)** –路由器會根據 ping 間隔設置，向 Ping 閘道 IP 欄位中指定的位址的主機發送 ICMP（Internet 控制訊息協定）回應請求，以驗證 WAN 連線。如果遠端主機在指定秒數（由 ping 間隔定義）內沒有回應，則認為 WAN 連線失敗。 如果你選擇 **Ping 偵測(Ping Detect)**作為檢測模式，您需要輸入以下項目的必要設定。 • **主要 Ping IP (Primary Ping IP)** – 在此欄位中輸入要 ping 的 IP 位址。 • **次要 Ping IP (Secondary Ping IP)** - 請在此欄位中輸入要 ping 的 IP 位址。 • **TTL** – 存活時間（Time To Live），即到達 ping 目標位址允許的最大跳數。有效值範圍為 1 到 255。 • **Ping 間隔(10-3600 秒) (Ping Interval (Sec, 10-3600))** – 輸入系統執行 PING 操作的間隔。 • **Ping 重試次數(Ping Retry)** - 輸入在判定 WAN 斷開連線之前，系統允許執行 PING 操作的次數。
MTU	
MTU	最大傳輸單元 (MTU) 是指可以傳送到廣域網路 (WAN) 的最大資料封包的大小（以位元組為單位）。最大值為 1500。對於 PPPoE 連線而言，因為 PPPoE 連線會額外增加 8 位元組的封包標頭，因此原本 Ethernet 的最大 MTU 1500 位元組需要扣掉這 8 位元組，所以 PPPoE 的最大 MTU 為 1492 位元組。
WAN MAC Address	
模式(Mode)	**預設值(Default)** – 使用 WAN 連接埠的預設 MAC 位址。 **客製化(Customized)** - 如果您的 ISP 透過 MAC 位址進行驗證，請選擇此選項。 • **MAC** - 為 WAN 乙太網路連接埠指定 MAC 位址。
MAC	顯示裝置的 MAC 位址。

取消(Cancel)	捨棄目前設定並回到前一頁面。
套用(Apply)	儲存目前設定並離開此頁面。

光纖 SFP 傳送資料模式之自動偵測

欲新增自動偵測設定檔，請按**+新增(+Add)**鏈結即可開啟如下頁面。



可用設定說明如下：

項目	**說明**
進階模式:開啟/關閉 (Advanced Mode:ON/OFF)	按此顯示或隱藏 WAN 介面的進階設定(如 IP 別名與 WAN MAC 位址)。
設定檔名稱(Profile Name)	輸入字串作為設定檔名稱，供辨識使用。
傳送資料模式 (Physical Type)	顯示 WAN 介面的傳送資料模式。
IP 版本(IP Version)	為此 WAN 介面選擇 IP 版本(IPv4、IPv6 或二者)。
VLAN Settings	
顧客 VLAN (Customer VLAN)	切換此開關以啟用或停用帶有標籤的 VLAN 功能。如果啟用，請輸入標籤和優先權值。 **標籤(Tag)** - 輸入 VLAN ID 號碼。範圍為 0 到 4094。 **優先權(Priority)** - 輸入該 VLAN 的封包優先編號。範圍為 0 到 7。
服務 VLAN (Service VLAN)	切換此開關以啟用或停用帶有標籤的 VLAN 功能。如果啟用，請輸入標籤和優先權值。 **標籤(Tag)** - 輸入 VLAN ID 號碼。範圍為 0 到 4094。 **優先權(Priority)** - 輸入該 VLAN 的封包優先編號。範圍為 0 到 7。

IPv4	
IPv4 連接類型(IPv4 Connection Type)	當選擇兩者(Both)或 IPv4 作為 IP 版本時，可使用此功能。 **PPPoE** – 將存取模式設定為 PPPoE。 ● **使用者名稱(Username)** – ISP 提供的 PPPoE 驗證的使用者名稱。 ● **密碼(Password)** – ISP 提供的 PPPoE 驗證的密碼。 ● **服務名稱(Service Name)** – PPP 服務名稱標籤。部分 ISP 需要此項目。除非您的 ISP 另有指示，否則請留空。此功能僅在啟用進階模式時可用。 **PPP 驗證(PPP Authentication)** – 用於 PPP 驗證的協定。**PAP 或 CHAP** - PAP 和 CHAP（詢問握手認證協定）皆可用於 PPP 認證。路由器會與 PPTP 或 L2TP 伺服器協商以確定使用哪種協定。此功能僅在進階模式啟用時可用。 ● **IP 分派(IP Assignment)** – 此功能僅在啟用進階模式時可用。當選擇 PPPoE 作為 IPv4 連線類型時，即可使用此功能。 **DHCP** - 位址是動態分配的。 **靜態 IP (Static IP)** - 您的網路服務供應商已指派一個固定的廣域網路 IP 位址。請輸入 IP 位址。 ● **WAN DNS** – 選擇**自動(Auto)**或**手動(Manual)**。 如果選擇了手動(Manual)，需指定主要與次要 DNS 伺服器。 **IPv4 主要 DNS(IPv4 Primary DNS)** – 輸入主要 DNS 伺服器位址。 **IPv4 次要 DNS(IPv4 Secondary DNS)** - 輸入次要 DNS 伺服器位址。 **DHCP** – 路由器從 DHCP 伺服器接收 IP 設定資訊。 ● **WAN DNS** – Select **Auto** or **Manual**. ● **WAN DNS** – 選擇**自動(Auto)**或**手動(Manual)**。 如果選擇了手動(Manual)，需指定主要與次要 DNS 伺服器。 **IPv4 主要 DNS(IPv4 Primary DNS)** – 輸入主要 DNS 伺服器位址。 **IPv4 次要 DNS(IPv4 Secondary DNS)** - 輸入次要 DNS 伺服器位址。 **靜態 IP (Static IP)** – 將存取模式設定為靜態 IP。 ● **IP 位址 (IP Address)** – 由網際網路服務供應商 (ISP) 指派的廣域網路 IP 位址。 ● **子網遮罩(Subnet Mask)** – WAN 子網路遮罩。 ● **閘道 IP(Gateway IP)** – WAN 閘道的 IP 位址。 ● **IPv4 主要 DNS (IPv4 Primary DNS)** – 主要 DNS 伺服器的 IP 位址。 ● **IPv4 次要 DNS (IPv4 Secondary DNS)** – 次要 DNS 伺服器的 IP 位址。
WAN 連線偵測(WAN Connection Detection)	
模式(Mode)	設定如何監控廣域網路連線。 **永遠連線(Always On)** - 路由器假定廣域網路連線始終處於作用中狀態。 **ARP 偵測(ARP Detect)** - 路由器每 5 秒廣播一次 ARP 請求。如果在 30 秒內沒有收到回應，則認為 WAN 連線失敗。 **PPP 偵測(PPP Detect)** – 偵測路由器與 ISP 之間的 PPP 連線成功與否的方式。 **Ping 偵測(Ping Detect)** - 路由器會根據 ping 間隔設置，向 Ping 閘道 IP 欄位中指定的位址的主機發送 ICMP（Internet 控制訊息協定）回應請求，以驗證 WAN 連線。如果遠端主機在指定秒數（由 ping 間隔定義）內沒有回應，則認為 WAN 連線失敗。 如果你選擇 **Ping 偵測(Ping Detect)**作為檢測模式，您需要輸入以下項目的

	必要設定。 ● **Ping 閘道 IP (Ping Gateway IP)** - 切換此開關以啟用/使用目前 WAN 閘道 IP 位址進行 ping 測試。透過 ping 測試 IP 位址，Vigor 路由器可以檢查 WAN 連線是否已開啟。 ● **TTL** – 存活時間（Time To Live），即到達 ping 目標位址允許的最大跳數。有效值範圍為 1 到 255。 ● **Ping 間隔(5-3600 秒) (Ping Interval (Sec, 5-3600))** – 輸入系統執行 PING 操作的間隔。 ● **Ping 重試次數(Ping Retry)** - 輸入在判定 WAN 斷開連線之前，系統允許執行 PING 操作的次數。
IP 別名(IP Alias)	**進階模式**啟用時，可使用此功能。 **IPv4 別名(IPv4 Alias)** - 如果您有多個真實 IP 位址，並希望在 WAN 介面上使用它們，請使用 WAN IP 別名。除了目前正在使用的真實 IP 位址之外，您最多可以設定 8 個真實 IP 位址。 **+新增(+Add)** – 按下**+新增(+Add)** 輸入 IPv4 位址作為 IPv4 別名。
	IPv6
IPv6 連線類型(IPv6 Connection Type)	當選擇兩者(Both)或 IPv6 作為 IP 版本時，可使用此功能。 **斷線(Offline)** – 選擇離線時，IPv6 連線將會停用。 **PPP** – 在 PPPoE 協商過程中，IPv6 WAN 位址會與 IPv4 WAN 位址一起指派。這種 IPv6 存取模式會要求 IPv4 使用 PPPoE 協定。 **靜態(Static)** – 設定 ISP 分配的靜態 IPv6 設定。 ● **+新增(+Add)** – 按一下此按鈕，將 IPv6 位址和前置碼長度欄位中的值新增至全球位址表(Global Address Table)。 ● **IPv6 全球位址(IPv6 Global Address)** – 由網際網路服務供應商 (ISP) 指派的廣域網路 IPv6 位址。 ● **前置碼長度(Prefix Length)** – IPv6 前置碼的長度。 ● **閘道位址(Gateway Address)** - ISP 閘道的 IPv6 位址。 **DHCPv6** – 使用 DHCPv6 協定從伺服器取得 IPv6 位址。 ● **DUID** – 顯示此 WAN 介面所使用的 DHCP 唯一 ID。 ● **IAID** – 用於識別此 WAN 介面的唯一整數。 ● **驗證通訊協定(Authentication Protocol)** - 此協定用於用戶端在存取網際網路之前透過 DHCPv6 伺服器進行身份驗證。可以指定三種類型：**重新設定金鑰(Reconfigure Key)**，**延遲(Delayed)**和**無(None)**。通常情況下，預設為**無(None)**。 - **重新設定金鑰(Reconfigure Key)** – 在連線過程中，DHCPv6 伺服器將自動對用戶端進行身份驗證。 - **延遲(Delayed)** - 在連線過程中，DHCPv6 伺服器將根據這些欄位中指定的金鑰 ID、領域和秘鑰資訊對用戶端進行身份驗證和識別。 **金鑰 ID (Key ID)** – 輸入一個值（範圍從 1 到 65535），該值將用於產生 HMAC-MD5 值。 **領域(Realm)** – 在此輸入的名稱（1 到 31 個字元）將標識產生 HMAC-MD5 值的密鑰。 **密鑰(Secret)** – 輸入一段文字（1 到 31 個字元）作為每個 DHCP 伺服器上每個用戶端的唯一識別碼。 **TSPC** -通道建立協定用戶端（TSPC）是一款可以幫助您輕鬆連接到 IPv6 網路的應用程式。 請確保您的 IPv4 WAN 連線正常，並從 hexago 申請免費帳戶（http://gogonet.gogo6.com/page/freenet6-account 在您嘗試使用 TSPC 進行網路連線之前，請先進行設定。TSPC 會連線到通道代理，並根據設定檔中的規格請求通道。它會從通道代理程式取得公用 IPv6 位址

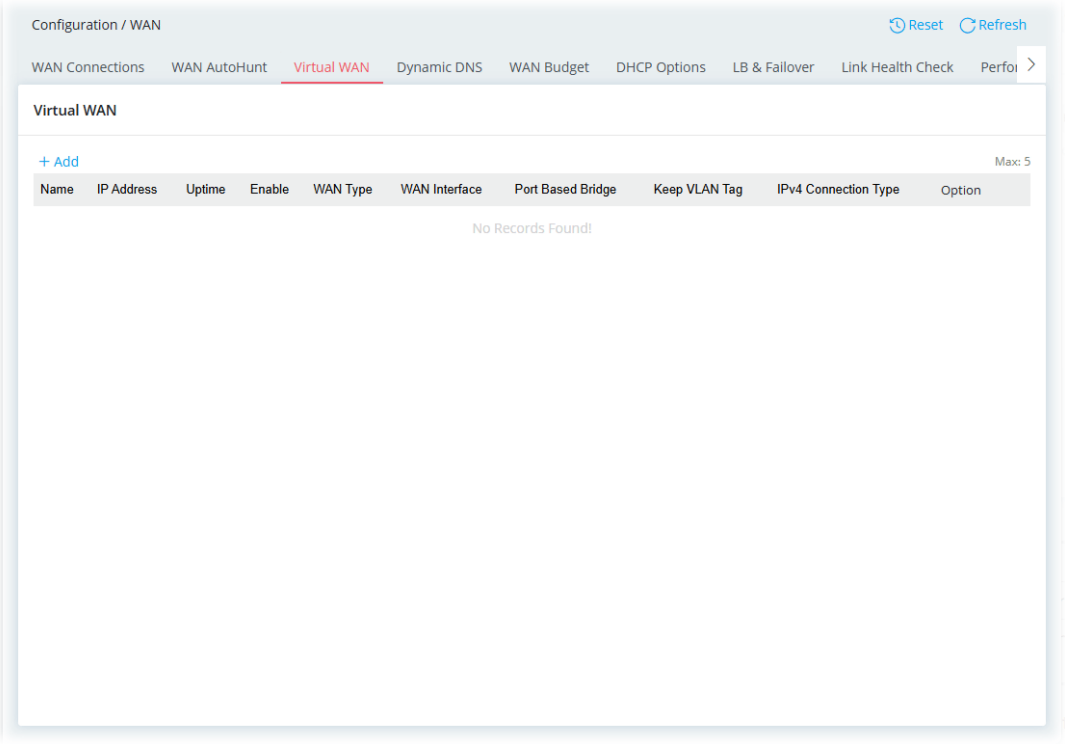
	和 IPv6 前置碼，然後在背景監控通道的狀態。 在取得 IPv6 前置碼並啟動路由器通告守護程式（RADVD）後，該路由器後面的 PC 可以直接連接到 IPv6 網際網路。 ● **通道代理伺服器位址(Tunnel Broker Address)** – 輸入位址通道代理 IP 位址、FQDN 或選用連接埠號碼。 ● **使用者名稱(Username)** – 建議您使用另一個使用者名稱和密碼。http://gogonet.gogo6.com/page/freenet6-account。 ● **密碼(Password)** –輸入與使用者名稱關聯的密碼。 **6in4** –為 WAN 介面設定 6in4 靜態通道。 然而，6in4 提供了一個 2002::0/16 之外的前置碼。如此一來，您可以使用固定端點，而不是任何類型轉換端點。這種模式更加可靠。 ● **啟用 IPv4 WAN Ping 存取 6in4/6rd 通道 (Enable IPv4 WAN Ping Access for 6in4/6rd Tunnel)** – 若要使用此 6in4 連線類型，必須允許 IPv4 WAN 存取，且防火牆必須允許通道代理 IP 位址通過。 ● **遠端終點 IPv4 位址(Remote Endpoint IPv4 Address)** – 由通道提供者指派的 WAN IPv6 位址。 ● **6in4 IPv6 位址(6in4 IPv6 Address)** – 由通道提供者指派的 WAN IPv6 位址。 ● **6in4 IPv6 前置碼長度(6in4 IPv6 Prefix Length)** – 通道提供者指派的 WAN IPv6 前置碼長度。 ● **LAN 路由前置碼(LAN Routed Prefix)** – 區域網路 IPv6 位址前置碼。 ● **LAN 路由前置碼長度(LAN Routed Prefix Length)** –區域網路 IPv6 位址前置碼長度。 ● **通道 TTL (Tunnel TTL)** – 存活時間值，即允許到達端點的最大躍點數。 **6rd** –為 WAN 介面設定 6rd。 ● **啟用 IPv4 WAN Ping 存取 6in4/6rd 通道(Enable IPv4 WAN Ping Access for 6in4/6rd Tunnel)** – 要使用 6rd 連線類型，必須允許 IPv4 WAN 訪問，且防火牆必須允許通道代理 IP 位址通過。 ● **模式(Mode)** – 兩種選項 : **自動(Auto)**和**靜態(Static)**態。**自動(Auto)** - 路由器與 DHCPv4 搭配使用時，會自動使用選項 212 設定 IPv6。**靜態(Static)**- IPv6 設定資訊是手動輸入的。**若是**選取**靜態(Static)**，須設定以下內容： - **IPv4 邊界中繼(IPv4 Border Relay)** – 輸入給予 6rd 網域的 6rd 邊界中繼的 IPv4 位址。 - **6rd 前置碼(6rd Prefix)** – 輸入 6rd IPv6 位址。 - **6rd 前置碼長度(6rd Prefix Length)** - 輸入 6rd IPv6 前置碼長度（以位元為單位）。 ● **WAN DNS** – 選擇**自動(Auto)** 或是**手動(Manual)**。 如果選擇了手動(Manual)，需指定主要與次要 DNS 伺服器。 **IPv6 主要 DNS(IPv6 Primary DNS)** – 輸入主要 DNS 伺服器位址。 **IPV6 次要 DNS(IPv6 Secondary DNS)** - 輸入次要 DNS 伺服器位址。
IPv6 WAN 連線偵測(IPv6 WAN Connection Detection)	
模式(Mode)	設定如何監控廣域網路連線。 **永遠連線(Always On)** - 路由器假定廣域網路連線始終處於作用中狀態。 **NS 偵測(NS Detect)** - 路由器透過發出鄰居請求封包來驗證連線。 **Ping 偵測(Ping Detect)** –路由器會根據 ping 間隔設置，向 Ping 閘道 IP 欄位中指定的位址的主機發送 ICMP（Internet 控制訊息協定）回應請求，以驗證 WAN 連線。如果遠端主機在指定秒數（由 ping 間隔定義）內沒有回應，則認為 WAN 連線失敗。

	如果你選擇 **Ping 偵測(Ping Detect)**作為檢測模式，您需要輸入以下項目的必要設定。 ● **主要 Ping IP (Primary Ping IP)** – 在此欄位中輸入要 ping 的 IP 位址。 ● **次要 Ping IP (Secondary Ping IP)** - 請在此欄位中輸入要 ping 的 IP 位址。 ● **TTL** – 存活時間（Time To Live），即到達 ping 目標位址允許的最大跳數。有效值範圍為 1 到 255。 ● **Ping 間隔(10-3600 秒) (Ping Interval (Sec, 10-3600))** – 輸入系統執行 PING 操作的間隔。 ● **Ping 重試次數(Ping Retry)** - 輸入在判定 WAN 斷開連線之前，系統允許執行 PING 操作的次數。
MTU	
MTU	最大傳輸單元 (MTU) 是指可以傳送到廣域網路 (WAN) 的最大資料封包的大小（以位元組為單位）。最大值為 1500。對於 PPPoE 連線而言，因為 PPPoE 連線會額外增加 8 位元組的封包標頭，因此原本 Ethernet 的最大 MTU 1500 位元組需要扣掉這 8 位元組，所以 PPPoE 的最大 MTU 為 1492 位元組。
WAN MAC Address	
模式(Mode)	**預設值(Default)** – 使用 WAN 連接埠的預設 MAC 位址。 **客製化(Customized)** - 如果您的 ISP 透過 MAC 位址進行驗證，請選擇此選項。 ● **MAC** - 為 WAN 乙太網路連接埠指定 MAC 位址。
MAC	顯示裝置的 MAC 位址。
取消(Cancel)	捨棄目前設定並回到前一頁面。
套用(Apply)	儲存目前設定並離開此頁面。

II-1-2-3 虛擬 WAN (Virtual WAN)

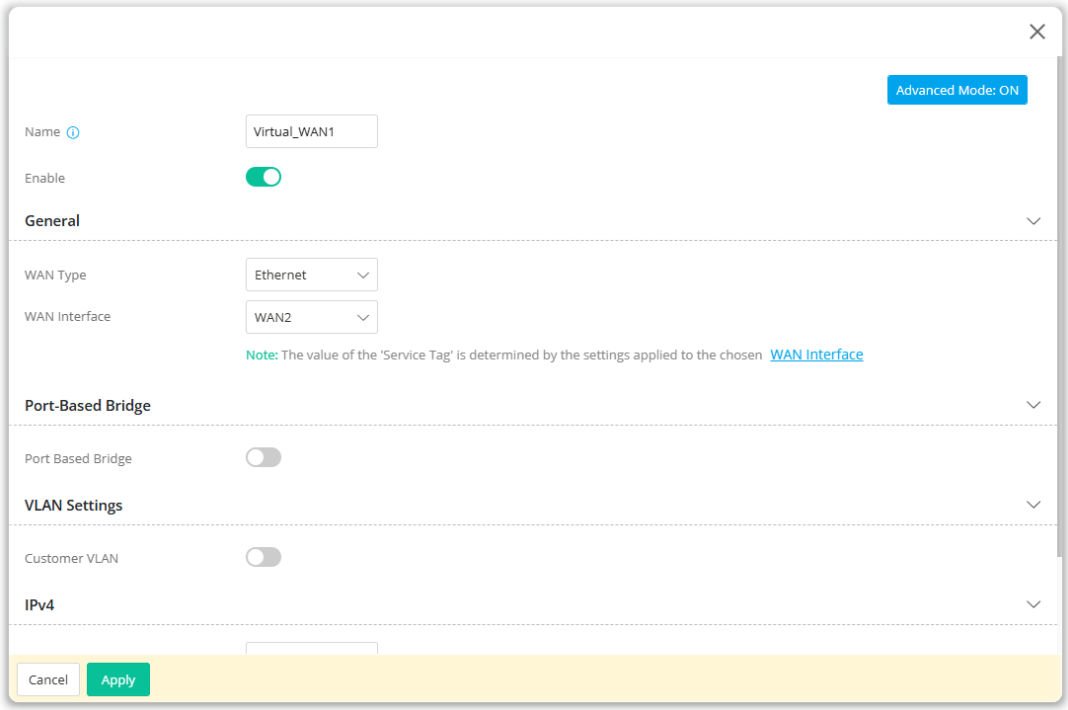
最多可以設定五個虛擬 WAN 設定文件，用於不同的應用程式。

每個設定檔都可以根據實際網路環境的要求，透過 VLAN 和綁定介面進行指定。



項目	說明
重置(Reset)	按下清除所有設定文件，恢復出廠設定。
+新增(+Add)	按一下以開啟虛擬 WAN 設定檔（最多 5 個）的設定頁面。

欲新增虛擬廣域網設定檔，請按一下**+新增(+Add)**鏈結即可開啟如下頁面。



可用設定說明如下：

項目	說明

進階模式:開啟/關閉 (Advanced Mode:ON/OFF)	按此顯示或隱藏虛擬 WAN 的進階設定
名稱(Name)	輸入字串作為設定檔名稱，供辨識使用。
啟用(Enable)	切換開關即可啟用或停用此功能。
基本(General)	
WAN 類型(WAN Type)	顯示實體介面的類型（例如，乙太網路）。
WAN 介面(WAN Interface)	選擇一個可用的 WAN 介面（在 WAN>>WAN 連線中啟用）。
埠號式橋接(Port-Based Bridge)	
埠號式橋接(Port Based Bridge)	切換開關即可啟用或停用此功能。 **綁定介面(Binding Interface)** - 選擇綁定介面。
多播串流 VLAN 轉換 (Multicast Stream VLAN Trans)	切換開關即可啟用或停用此功能。 在某些地區，多播 VLAN 標籤值可能與 IGMP VLAN 標籤值不同。這可能會導致在觀看 IPTV 節目時，IPTV 資料封包泛流到其他 VLAN 端口，從而造成資料傳輸問題。 如有需要，可將 IGMP VLAN 標籤和多播 VLAN 標籤設定為相同的值。 **下行多播 VLAN 標籤(Downstream Multicast VLAN Tag)** – 輸入用於標記多播資料封包的數值。範圍為 0 到 4094。 **上行 IGMP VLAN 標籤(Upstream IGMP VLAN Tag)** – 輸入用於標記 IGMP 封包的數值。範圍為 0 到 4094。
VLAN 設定(VLAN Settings)	
顧客 VLAN (Customer VLAN)	切換此開關以啟用或停用帶有標籤的 VLAN 功能。如果啟用，請輸入標籤和優先權值。 **標籤(Tag)** - 輸入 VLAN ID 號碼。範圍為 0 到 4094。 **優先權(Priority)** - 輸入該 VLAN 的封包優先編號。範圍為 0 到 7。 注意：如果啟用**多播流 VLAN 傳輸(Multicast Stream VLAN Trans)**，VLAN 設定將被忽略並停用。
進階模式下的選項	
IPv4	
IPv4 連接類型(IPv4 Connection Type)	**PPPoE** – 將存取模式設定為 PPPoE。 ● **使用者名稱(Username)** – ISP 提供的 PPPoE 驗證的使用者名稱。 ● **密碼(Password)** – ISP 提供的 PPPoE 驗證的密碼。 ● **PPP 驗證(PPP Authentication)** – 用於 PPP 驗證的協定。**PAP 或 CHAP** - PAP 和 CHAP(詢問握手認證協定)皆可用於 PPP 認證。路由器會與 PPTP 或 L2TP 伺服器協商以確定使用哪種協定。此功能僅在進階模式啟用時可用。 ● **IP 分派(IP Assignment)** – 此功能僅在啟用進階模式時可用。當選擇 PPPoE 作為 IPv4 連線類型時，即可使用此功能。 **DHCP** - 位址是動態分配的。 **靜態 IP (Static IP)** - 您的網路服務供應商已指派一個固定的廣域網

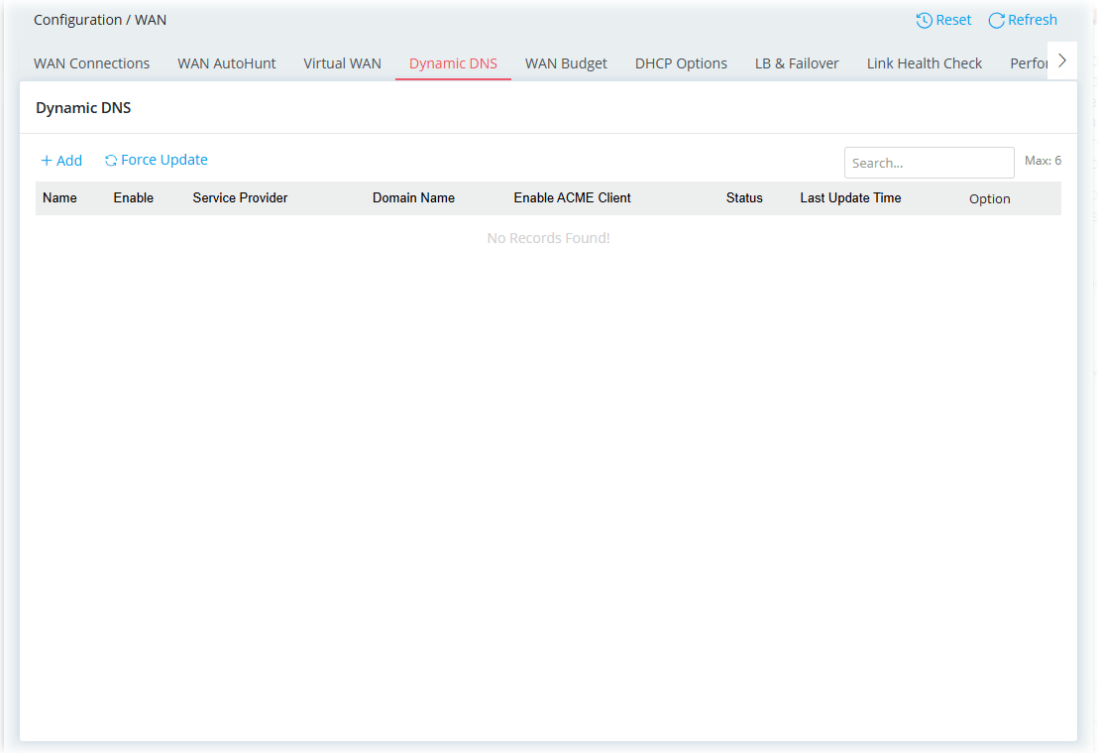
	路 IP 位址。請輸入 IP 位址。 **DHCP** – 路由器從 DHCP 伺服器接收 IP 設定資訊。 ● **路由器名稱(Router Name) -** 輸入路由器名稱。某些 ISP 需要此設定內容。 ● **網域名稱(Domain Name)-**因應路由器需要，輸入網域名稱。 當選擇靜態 DHCP 作為 IPv4 連線類型時，可使用此功能。 **靜態 IP (Static IP)** – 將存取模式設定為靜態 IP。 ● **IP 位址 (IP Address)** – 由網際網路服務供應商 (ISP) 指派的廣域網路 IP 位址。 ● **子網遮罩(Subnet Mask)** – WAN 子網路遮罩。 ● **閘道 IP(Gateway IP)** – WAN 閘道的 IP 位址。
取消(Cancel)	捨棄目前設定並回到前一頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-1-2-4 動態 DNS(Dynamic DNS)

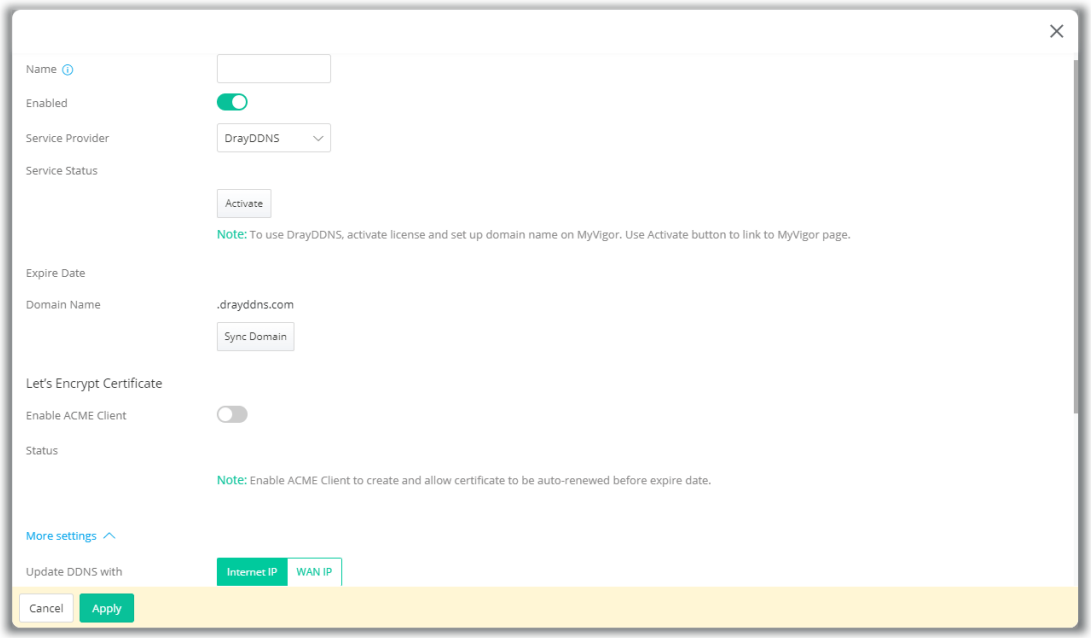
大多數網際網路服務供應商（ISP）會為客戶指派動態 WAN IP 位址。對於需要從網際網路遠端存取區域網路（LAN）服務的使用者而言，動態 IP 位址可能會帶來不便，因為 WAN IP 位址可能會在未通知的情況下變更，導致遠端連線中斷或服務無法存取。

透過向動態 DNS（DDNS）服務供應商申請服務，並在 Vigor 路由器上設定 DDNS 更新功能，您即可使用容易記憶的網域名稱存取您的網路。而當 WAN IP 位址變更時，DDNS 會自動將網域名稱更新為最新的 WAN IP 位址，確保您能持續且可靠地存取網路。



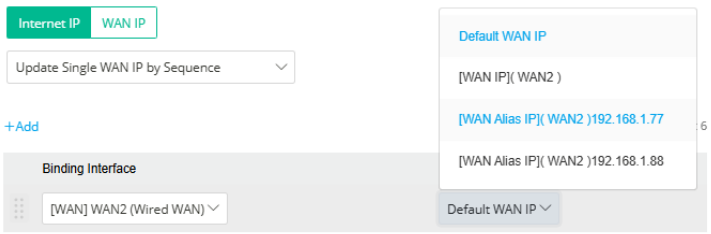
項目	說明
重置(Reset)	按下可清除所有設定文件，回復出廠設定值。
+新增(+Add)	按下可開啟 DDNS 設定檔（最多 6 個）的設定頁面。
強迫更新(Force Update)	按下即可立即連接到 DDNS 伺服器以更新 IP 位址資訊。

欲新增 DDNS 設定檔，請按一下**+新增(+Add)**鏈結即可開啟如下頁面。



可用設定說明如下：

項目	說明
名稱(Name)	請輸入字串作為設定檔名稱，以供識別。
啟用(Enabled)	切換此開關即可啟用或停用此功能。
服務供應商(Service Provider)	選擇 DDNS 服務供應商。如果您的 DDNS 服務供應商並未被列出，可選擇**使用者定義(User-Defined)**以便手動進行設定。 ● **DrayDDNS** ● **NO-IP** ● **Dyn.com** ● **58DDNS** ● **UBDDNS** ● **使用者定義(User-Defined)** ● **Let's Encrypt ACME**
當服務供應商(Service Provider)設定選擇了 DrayDDNS	**服務狀態(Service Status)** - 按下**啟動(Activate)**以便啟動該服務。 **失效日期(Expire Date)** - 顯示服務的到期日。 **網域名稱(Domain Name)** - 顯示要更新的網域和子網域。 **同步網域(Sync Domain)** – DrayDDNS 的網域已在 MyVigor 伺服器上設定。按下此按鈕以載入並取得網域名稱（如果可用）。
當服務供應商(Service Provider)設定選擇了 NO-IP, Dyn.com, 58DDNS, UBDDNS	**網域名稱(Domain Name)** - 需要更新的網域和子網域。 **帳戶名稱(Account Name)** - 輸入 DDNS 帳號的登入名稱。 **密碼(Password)** - 輸入 DDNS 帳號的密碼。
當服務供應商(Service Provider)設定選擇了使用者定義(User-Defined)	**供應商主機 URL (Provider Host URL)** – 輸入提供相關服務的主機的 IP 位址或網域名稱。 **服務 API (Service API)** – 輸入 DDNS 服務供應商提供的 API 資訊。 **伺服器回應(Server Response)** – 輸入您希望從 DDNS 伺服器接收的任何文字。 **帳戶名稱(Account Name)** – 輸入 DDNS 帳號的登入名稱。 **密碼(Password)** – 輸入 DDNS 帳號的密碼。

	驗證類型(Auth Type) – 可以使用兩種類型的身份驗證。 ● **基本(Basic)** – 後續定義的使用者名稱和密碼可以從擷取的資料封包中顯示出來。 ● **URL** – 後續定義的使用者名稱和密碼可以顯示在 URL 中。 **啟用 ACME 用戶端(Enable ACME Client)** – 切換此開關以產生 Let's Encrypt 簽發的憑證，並套用至 DDNS 帳戶。
更多設定(More settings)	
使用以下方式更新 DDNS (Update DDNS with)	如果 Vigor 路由器安裝在任何 NAT 路由器後面，您可以啟用此功能來尋找真實的 WAN IP。 當 Vigor 路由器使用的 WAN IP 為虛擬 IP 時，此功能可以偵測 NAT 路由器使用的真實 IP，並使用偵測到的 IP 位址進行 DDNS 更新。 有兩種方法供您選擇： **網際網路 IP (Internet IP)** - 將使用真實的 IP 位址。如果指派給路由器 WAN 介面的 IP 位址不是實際的外部 IP 位址，請選擇此選項。 **WAN IP** - 將使用路由器 WAN 介面的 IP 位址。
更新 WAN IP 模式 (Update WAN IP Mode)	可當 **DrayDDNS** 被設定為服務供應商，可使用此設定。 **更新所有選定的 WAN IP (Update All Selected WAN IPs)** – Vigor 路由器系統將更新所有選定的 WAN IP 位址。 **依序更新單一 WAN IP (Update Single WAN IP by Sequence)** – Vigor 路由器系統將依序更新 WAN IP。 **+新增(+Add)** – 按此以新增 IP 位址（最多 6 個）。 ● **綁定介面(Binding Interface)** – 選擇一個介面（WAN1 至 WAN6）用於傳輸流量。最多可以定義六個介面。 ● **介面 IP(Interface IP)** – 如果先前已設定 IP 別名，則此欄位中即可顯示可用項次。綁定介面中列出的第一個 IP 位址是預設 IP 位址。請選擇一個與綁定介面相符的選項。 
通訊協定(Protocol)	選擇用於回應 DDNS 服務供應商的 IP 位址之 IP 類型（IPv4 或 IPv6，或任一）。
自動更新間隔(Auto Update Interval)	路由器連接到 DDNS 伺服器以更新 IP 位址資訊的頻率(以分鐘為單位)。預設值為 14400。
取消(Cancel)	捨棄目前設定並回到前一頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

DrayDDNS 設定

DrayDDNS 是由 DrayTek 開發的動態網域名稱系統(DDNS, Dynamic Domain Name System)，可將多個廣域網路 IP 位址（IPv4/IPv6）綁定至單一網域。使用者可透過 MyVigor 方便地使用此功能，並輕鬆完成設定。每台 Vigor 路由器可至 MyVigor 註冊一個網域，有效期限為一年。

遇到如下情況時會更新 DDNS:

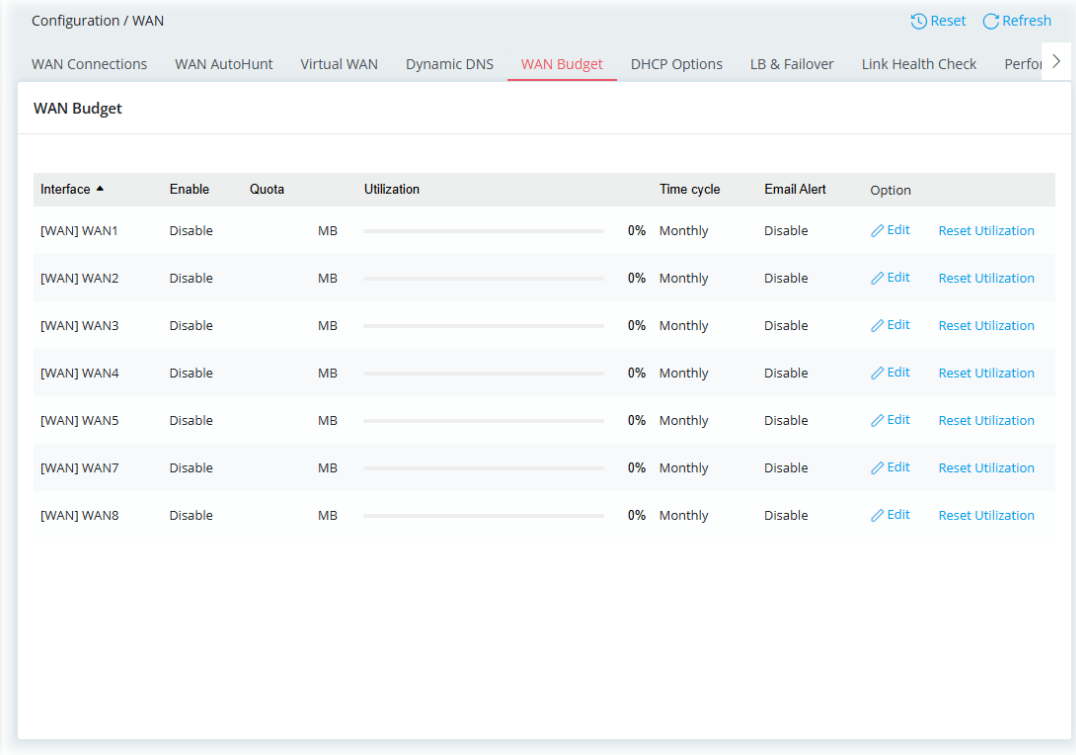
- 路由器已開機或重新啟動。
- 任何廣域網路介面的真實 IP 位址都變更了。
- WAN 介面的線上狀態變更了（從上線變為離線或反之亦然）。
- DDNS 功能已從「停用」變更為「啟用」。
- DDNS 條目已修改並啟用。
- 自動更新間隔已過。
- 按下強迫更新按鈕(Force Update)。

II-1-2-5 WAN 計量收費(WAN Budget)

此功能可分別確認各個廣域網路（WAN）介面的資料流量，以協助避免因資料傳輸超過 ISP（網際網路服務供應商）的流量方案而產生額外費用。請注意，必須先正確設定額度限制（Quota Limit）及每月計費週期日（Billing cycle day of month），才能確保相關週期的流量統計與計算結果正確無誤。

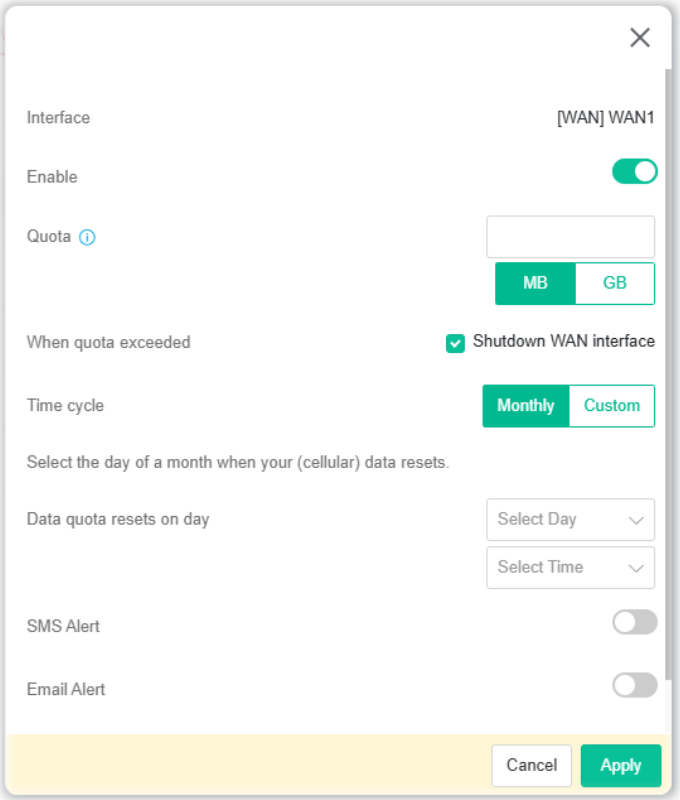
WAN 流量預算功能可讓您方便追蹤網際網路流量。您可以：

- 設定日曆週期進行監控；
- 根據你的網路服務供應商的額度限制你的上網時間；
- 設定超出額度時要採取的措施。



項目	說明
重置(Reset)	按此將每個 WAN 介面的 WAN 計量收費重設為出廠設定。
編輯(Edit)	修改 WAN 廣域網路計量收費設定檔內的內容。
重置利用(Reset Utilization)	清除所選 WAN 介面的目前資料流量（顯示在使用率(Utilization)下）。

欲新增設定檔，請按一下**+新增(+Add)**鏈結即可開啟如下頁面。



可用設定說明如下：

項目	說明
啟用(Enable)	切換此開關即可啟用或停用該設定檔。 啟用後，此介面將啟用廣域網路計量收費(WAN Budget)機制。
額度(Quota)	請輸入此廣域網路介面允許的資料流量額度。 有兩種單位（MB 和 GB）可以選擇。
當超過額度時(When quota exceed)	**關閉 WAN 介面(Shutdown WAN interface)** - 當流量超過計量收費限制時，所有透過此 WAN 介面發出的流量都將被停止。
時間循環(Time Cycle)	**每月(Monthly)** – 部分網路服務供應商可能會根據每月流量限制來設定網路流量。此設定意在提供一種機制，能每月重置流量記錄。 **客製化(Custom)** - 此設定允許使用者依照自身需求定義計費週期。WAN 計量收費將以計費週期重置。
當時間循環(Time Cycle)設定選擇了每月(Monthly)	**資料額度每隔數日重置(Data quota resets on day)** - 您可以確定一個月內的起始日期。
當時間循環(Time Cycle)設定選擇了客製化(Custom)	預設為每月。如果需要更長的週期或更短的週期，請使用**客製化(Custom)**設定，週期長度為 1 天至 30 天。您可以透過指定日期和小時數來確定週期長度。此外，您也可以指定目前週期包含哪一天。 **循環期間(日)(Cycle duration (Days))** – 定要重置流量記錄的日期（1~31）。 **循環期間(時)(Cycle duration (Hours))** – 指定重置流量記錄的時間（0~23）。 **起始日期(Start Date)** – 指定週期中的哪一天作為 Vigor 路由器重置流量

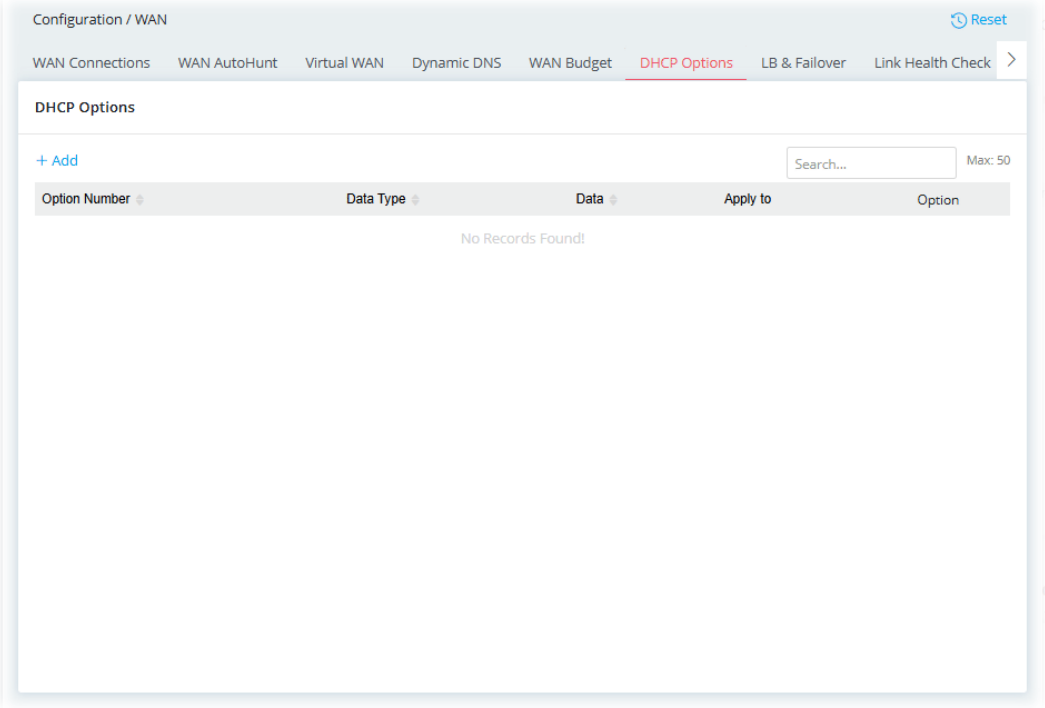
	記錄的起始點。 **起始時間(Hr:Min.)(Start Time (Hr:Min.))** - 指定資料額度重置週期的時間，作為 Vigor 路由器重置流量記錄的起始點。
簡訊警示(SMS Alert)	切換開關即可啟用或停用此功能。 **傳送警示簡訊至(Send Alert SMS to)** – 當資料額度(計費)即將用罄（少於10%）時，系統將向此處指定的用戶發送警示簡訊。
電子郵件警示(Email Alert)	切換開關即可啟用或停用此功能。 **傳送警示郵件至(Send Alert Email to)** – 當資料額度(計費)即將用罄(少於10%）時，系統會向此處指定的使用者透過郵件發送警告訊息。
取消(Cancel)	捨棄目前設定並回到前一頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

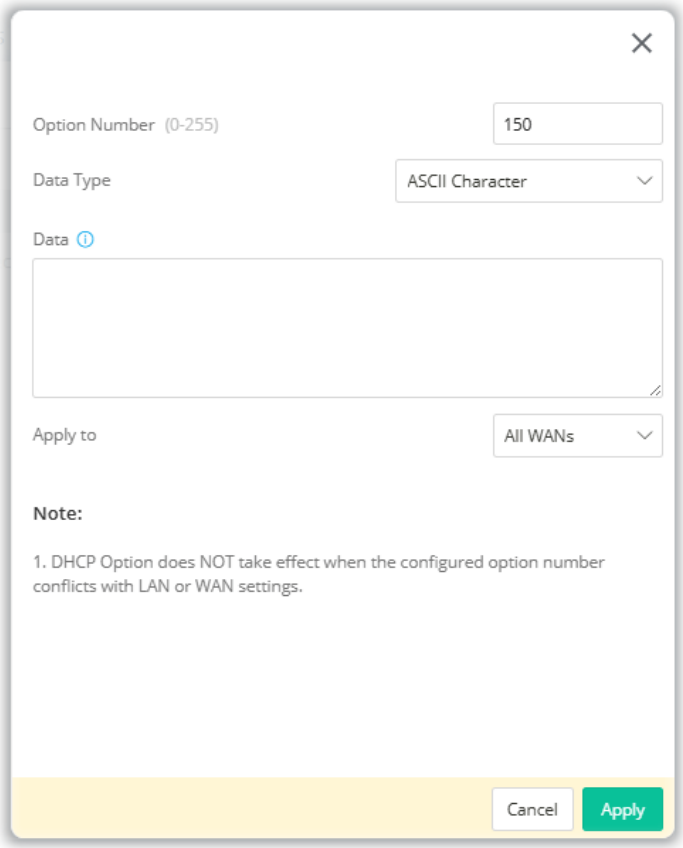
II-1-2-6 DHCP 選項(DHCP Options)

啟用並設定此功能後，可以透過新增選項編號和資料資訊來處理 DHCP 封包。

此頁面可讓您設定其他 DHCP 用戶端選項。



欲新增/編輯設定檔，請按一下**+新增/編輯(+Add/Edit)**鏈結即可開啟如下頁面。



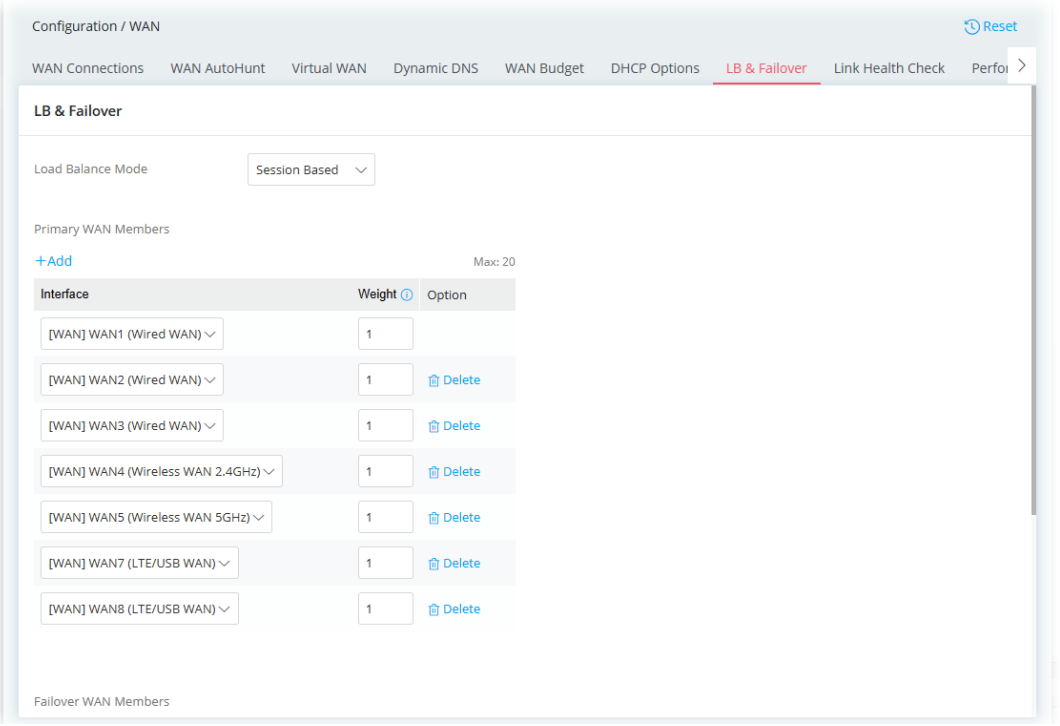
可用設定說明如下：

項目	說明
選項號碼(Option Number)	每個 DHCP 選項都由選項編號和資料組成。 請輸入一個數字。
資料類型(Data Type)	選擇要儲存的資料類型（ASCII、十六進位或位址清單）。資料欄位中的資料類型包含： ● **ASCII 字元**：文字字串。例如：/path。 ● **十六進位數字(Hexadecimal Digit)**：十六進位字串。有效字元為 0 到 9 和 a 到 f。例如：2f70617468。 ● **位址清單(Address List)**：一個或多個 IPv4 位址，以逗號分隔。
資料(Data)	輸入要透過 DHCP 選項功能處理的資料內容。
套用至(Apply to)	選擇此條目適用的 WAN 介面。
取消(Cancel)	捨棄目前設定並回到前一頁面。
套用(Apply)	儲存目前設定並離開此頁面。

II-1-2-7 備援(Failover)

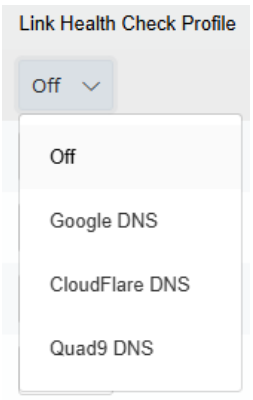
此頁面允許設定備援廣域網路。

當路由器的主要 WAN 口發生故障時，其他可用的 WAN 介面將依序接管網路連線。



可用設定說明如下：

項目	說明
負載平衡模式(Load Balance Mode)	**依 IP 位址(IP Based)** – 為了確保使用者連線數的一致性，此功能會將來自特定客戶端（列於介面/權重中）的請求導向同一伺服器。但是，如果來自相同客戶端的請求過多，則可能無法均勻分配流量。 **依工作階段(Session Based)** – 此選項透過考慮 IP 位址、完整的連線數詳情和目前負載情況，提供更均勻、更有效率的流量分配。主 WAN 介面（作為對外連線 WAN）將用於傳輸新連線數，以獲得更高的傳輸速度。雖然總處理量測試結果可能良好，但某些網站可能無法流暢打開，特別是需要身份驗證的網站，例如 FTP 網站。
主要 WAN 成員（Primary WAN Members）	**+新增(+Add) –** 按此新增條目。 **介面(Interface)** – 選擇一個 WAN 介面。預設情況下，此 WAN 將用於網路連線。但是，如果此 WAN 連線中斷，**備援** WAN 成員將依照優先權接管網路連線。 **權重(Weight)** – 選擇此條目的權重值（1 到 255）。 **選項(刪除)(Option (Delete))** – 按此移除選定的條目。
備援 WAN 成員 (Failover WAN Members)	顯示所有將作為備援 WAN 使用的啟用 WAN 介面。如果此欄位中指定的介面失去連線或偵測失敗，則可以將流量轉送至備用替代介面。 **+新增(+Add) –** 按此新增條目。

(Failover WAN Members)	介面失去連線或偵測失敗，則可以將流量轉送至備用替代介面。 **+新增(+Add) –** 按此新增條目。 **介面(Interface) –** 選擇一個廣域網路介面。此廣域網路介面旨在作為備援連接埠，當其他指定的廣域網路連接埠連接中斷時使用。 **優先權(Priority) –** 確定失效切換之廣域網路的優先順序。數值越小，越優先將其用作備援 WAN 廣域網路。 **權重(Weight) –** 選擇此條目的權重值 (1 到 255)。 **選項(刪除) (Option (Delete)) –** 刪除選定項目設定 (活動中的 WAN 介面) 。
進階設定(Advanced Settings)	
故障回復(Failback)	當原始介面發生故障時，資料封包將透過另一個介面發送或遵循另一種策略 (**失效切換至**) 一旦原始介面恢復服務 (**故障回復**) ，資料封包將立即回至原介面。 切換此開關即可啟用/停用此功能。
還原鏈結檢查(Restore Link Checks)	若啟用**故障回復(Failback)**，即可使用此功能。 請輸入一個數值以便系統決定鏈結所需的檢查次數。鏈路檢查成功後，連線將恢復。
介面鏈結健康與 SLA 協議 (Link Health Check and SLA)	切換此開關以啟用此功能。 如果停用此功能，則依照 WAN 連線設定檔中定義的 WAN 連線偵測模式來決定啟用的 WAN 介面。 啟用後，WAN 連線設定檔中定義的 WAN 連線偵測將被忽略。路由器將測量介面成員的效能，並使用鏈路健康檢查和效能 SLA 來確定啟用哪個介面。 **介面鏈結健康與 SLA 協議(Interface Link Health & SLA) –** 列出可用於設定不同健康檢查方法的 WAN 介面。 • **介面(Interface) –** 顯示 WAN 介面。 • **鏈結健康檢查設定檔(Link Health Check Profile) –** 為介面選擇一個可用的檢查設定檔 (在設定>>WAN>>鏈結健康檢查 (Configuration>>WAN>>Link Health Check)中定義) 。  • **效能 SLA (Performance SLA) –** 為介面選擇一個可用的檢查設定檔 (在設定>>WAN>>效能 SLA

	(Configuration>>WAN>>Performance SLA)中定義)。 • **失敗重試檢查(Failure Retry Checks) -** 指定系統檢查連線的次數。如果所有嘗試都失敗，系統將判定連線不穩定。
負載平衡例外清單(Load Balance Exception List)	建立例外列清單，該清單將使用固定 WAN 而非多 WAN 負載平衡。 **+新增(+Add) –** 按此新增條目(最多可設定 10 個)。 **啟用(Enable)** – 切換此開關以啟用此設定。 **註解(Comment)** – 輸入簡易說明以資識別。 **服務類型(Service Type)** – 選擇此條目適用的服務類型。服務是指使用特定協定或連接埠的預先定義或使用者自訂的流量類型。若要設定自訂服務，請選擇**客製化(Customized)**以設定服務名稱、通訊協定和埠號。 **通訊協定(Protocol)** – 選擇 TCP, UDP 或是 TCP/UDP。 **來源埠號(Source Port)** – 輸入來源 IP 位址需求之埠號。 **目的(Destination)** – 輸入目的 IP 位址。 **目的埠號(Destination Port)** – 輸入目的 IP 位址需求之埠號。 **選項(刪除) (Option (Delete))** – 刪除選定項目設定（活動中的 WAN 介面）。
取消(Cancel)	捨棄目前設定並回到前一頁面。
套用(Apply)	儲存目前設定並離開此頁面。

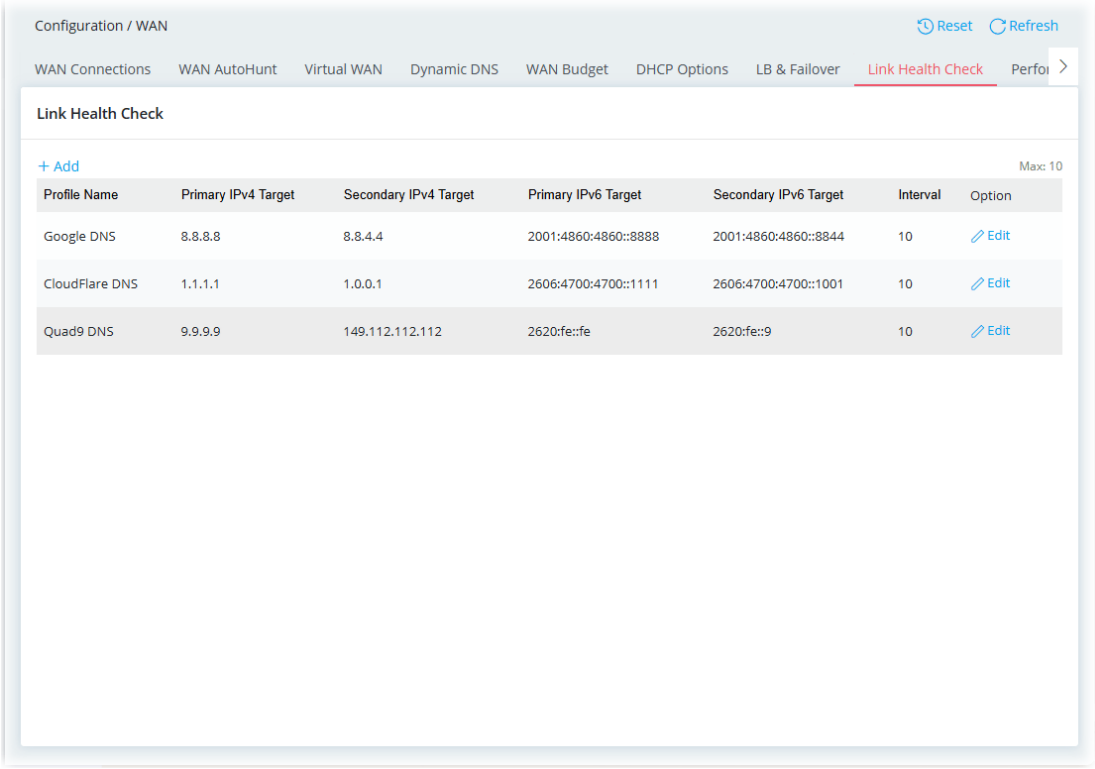
II-1-2-8 鏈結健康檢查(Link Health Check)

鏈結健康檢查用於指定需要驗證的 IP 位址（IPv4 和 IPv6），以確保透過 ping/httping 實現網路連線。

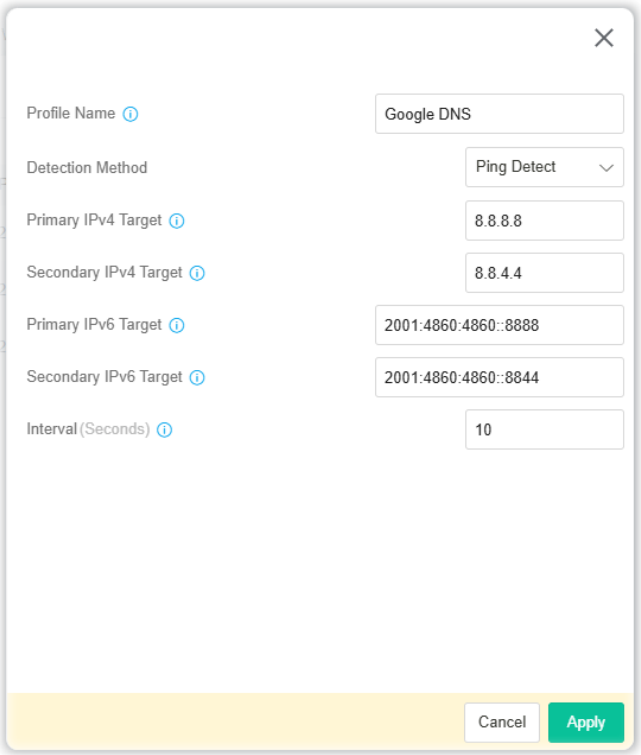
此頁面可讓您建立用於執行 WAN 介面鏈結健康狀況檢查的設定檔。

預設情況下，系統提供標準健康檢查選項，例如 Google DNS、CloudFlare DNS 和 Quad9 DNS。

以 Google DNS 為例。此設定檔指明主要/次要 IPv4 目標位址 (8.8.8.8/8.8.4.4) 用於檢查 IPv4 網路連接，而主要/次要 IPv6 目標位址 (2001:4860:4860::8888, 2001:4860:4860:::4864) 用於檢查 IPv6 連接。網路連線偵測每 10 秒執行一次。如果偵測到 IPv4 或 IPv6 位址連線失敗，則判定為網路連線偵測失敗。



欲新增/編輯設定檔，請按一下**+新增/編輯(+Add/Edit)**鏈結即可開啟如下頁面。



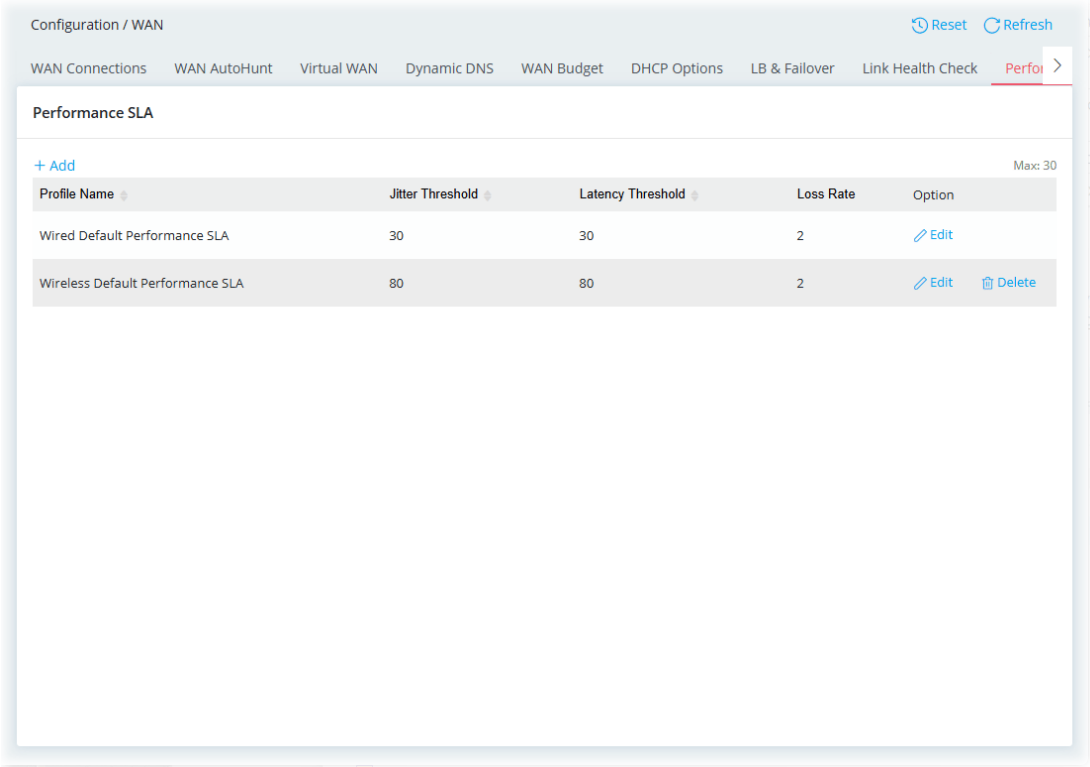
可用設定說明如下：

項目	**說明**
設定檔名稱(Profile Name)	輸入名稱作為鏈結健康檢查設定檔。
偵測方式(Detection	選擇 ping 偵測通訊協定。

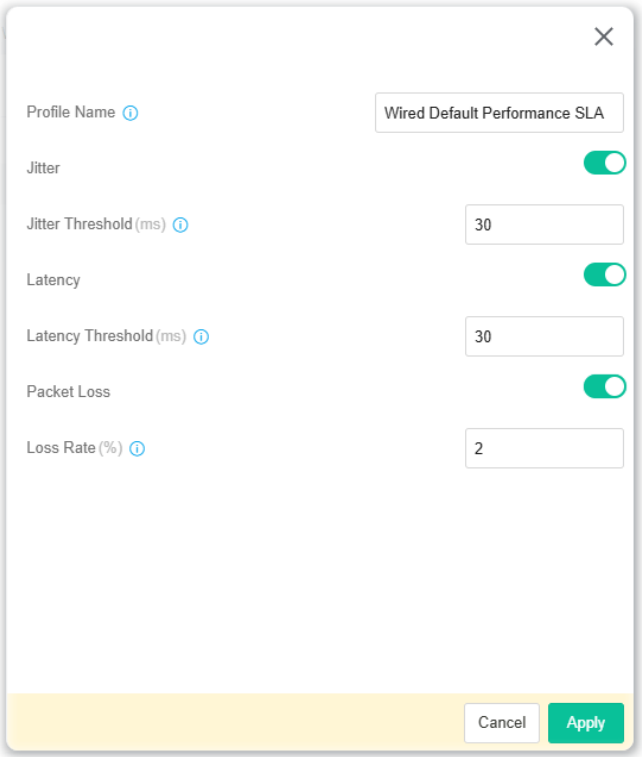
Method)	• HTTP Detect • Ping Detect
主要 IPv4 目標 (Primary IPv4 Target)	輸入第一個 IPv4 位址作為健康檢查的主要目標。
次要 IPv4 目標 (Secondary IPv4 Target)	輸入第二個 IPv4 位址作為健康檢查的次要目標。
主要 IPv6 目標 (Primary IPv6 Target)	輸入第一個 IPv6 位址作為健康檢查的主要目標。
次要 IPv6 目標 (Secondary IPv6 Target)	輸入第二個 IPv6 位址作為健康檢查的次要目標。
間隔(Interval)	設定網路偵測或檢查的時間間隔（單位為秒）。
取消(Cancel)	捨棄目前設定並回到前一頁面。
套用(Apply)	儲存目前設定並離開此頁面。

II-1-2-9 效能 SLA (Performance SLA)

此頁面可讓您設定效能 SLA(Service Level Agreement, 服務水準協議)的抖動、延遲和封包漏失門檻值，這些門檻值將用於偵測 WAN 連線的健康狀況。



欲新增/編輯設定檔，請按一下**+新增/編輯(+Add/Edit)**鏈結即可開啟如下頁面。



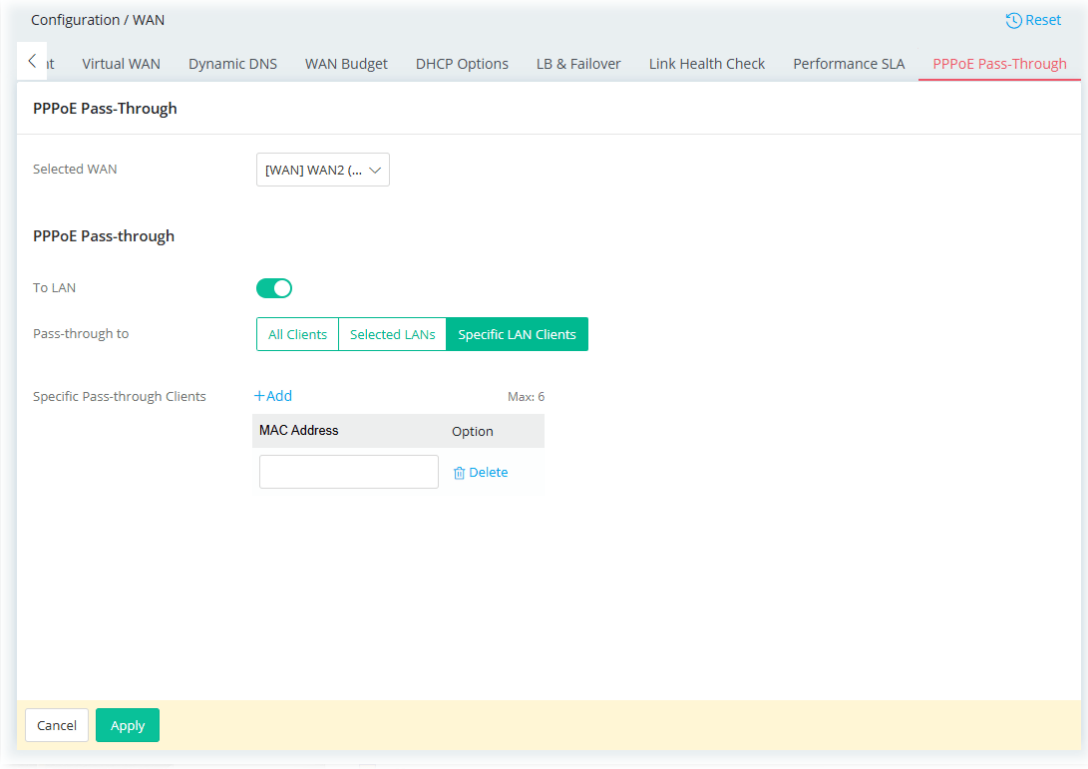
可用設定說明如下：

項目	說明
設定檔名稱(Profile Name)	輸入名稱作為效能 SLA 設定檔。
抖動(Jitter)	切換此開關即可啟用或停用抖動功能。 **抖動門檻值(Jitter Threshold)** - 定義延遲的變化率。對於穩定的連線數，抖動值越小越好。 當偵測到的值大於此處設定的值時，連線將被視為不穩定、連線失敗。
延遲(Latency)	切換此開關即可啟用或停用延遲功能。 **延遲門檻值(Latency Threshold)** - 定義 Vigor 路由器向鏈結狀態偵測中設定的 IP 位址發送封包所花費的時間。 當偵測到的值大於此處設定的值時，連線將被視為不穩定、連線失敗。
封包漏失(Packet Loss)	切換此開關以啟用或停用封包漏失偵測功能。 **漏失率(Loss Rate)** - 定義在到達鏈結狀態偵測中設定的 IP 位址之前將被丟棄的封包的比例。 當偵測到的值大於此處設定的值時，連線將被視為不穩定、連線失敗。
取消(Cancel)	捨棄目前設定並回到前一頁面。
套用(Apply)	儲存目前設定並離開此頁面。

II-1-2-10 PPPoE 通透(PPPoE Pass Through)

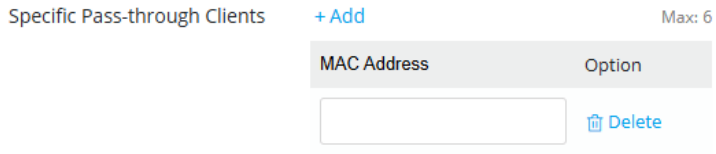
此路由器提供 PPPoE 撥號連線。此外，您也可以透過 Vigor 路由器直接從本機用戶端建立到 ISP 的 PPPoE 連線。根據 WAN 連線類型，此功能會將本機用戶端的 PPPoE 資料封包封裝並傳送至 WAN 伺服器。

因此，PC 可以透過這種方式存取網際網路。



可用設定說明如下：

項目	說明
選定的 WAN (Selected WAN)	選擇可應用於 PPPoE 通透的 WAN 介面。
至 LAN 端(To LAN)	切換開關即可啟用或停用此功能。 啟用後，有線區域網路用戶端可以向選定的廣域網路發起 PPPoE 撥接連線。
通透至(Pass-through to)	**全部的用戶端(All Clients)** – 所有有線 LAN 用戶端均可發起 PPPoE 撥號連線至選定的 WAN。 **選定的 LAN (Selected LANs)** – 一個或多個 LAN 用戶端可以向選定的 WAN 發起 PPPoE 撥號連線。 **指定 LAN 用戶端(Specific LAN Clients)** – 最多可設六個指定的通透 LAN 用戶端，可以發起 PPPoE 撥號連線到選定的 WAN。 ● **+新增(+Add)** – 按此新增用戶端。

	 - **MAC 位址(MAC Address)** – 輸入區域網路使用者的 MAC 位址。 - **選項(刪除) (Option (Delete))** – 按此以刪除選定條目。
取消(Cancel)	捨棄目前設定。
套用(Apply)	儲存目前設定。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-1-3 LAN

區域網路（LAN）由一組區域網路用戶端組成，這些用戶端是您場所內的連網裝置。區域網路用戶端可以是電腦、印表機、網路電話（VoIP）、手機、遊戲機、網路電視（IPTV）等，並且可以透過有線（使用乙太網路線）或無線（使用 Wi-Fi）網路連線。

同一區域網路內的用戶端通常可以直接相互通訊，因為它們彼此是對等的，除非採取了防火牆或虛擬區域網路（VLAN）等措施來限制這種存取。如今，最常見的區域網路防火牆都部署在客戶端本身。例如，自 Windows XP 起，Microsoft Windows 和 Apple OS X 都內建了防火牆，可以設定以限制進出電腦的流量。另一方面，VLAN 通常使用網路交換器或路由器進行設定。

若要與區域網路（LAN）外部的主機通訊，LAN 用戶端必須通過網路閘道，通常情況下，網路閘道是位於 LAN 和 ISP 網路（即廣域網，WAN）之間的路由器。路由器充當指揮中心角色，確保 LAN 和 WAN 之間的流量能夠到達其預期目的地。

IP 位址

在大多數寬頻網路中，網際網路服務供應商（ISP）會為每個使用者指派一個廣域網路（WAN）IP 位址。所有區域網路（LAN）用戶端在存取網際網路時都必須共用這個 WAN IP 位址。為達此目的，系統會使用網路位址轉換（NAT）技術。在 NAT 下，系統會為 LAN 用戶端指派一個私有的 IP 位址區塊，這些用戶端透過路由器（也稱為閘道器）與 WAN 主機通訊。

對於傳送至 WAN 的對外流量，路由器會注意到 LAN 用戶端嘗試連接 WAN 主機，並將請求轉送給預期的 WAN 接收者。

對於來自廣域網路主機並傳入區域網路的流量，路由器會檢查其記錄，查看是否存在來自區域網路用戶端對該廣域網路主機比對的未完成請求。如果存在，則將該流量轉送給區域網路用戶端；否則，該流量將被丟棄。

IPv4 位址中有 3 個不同的位址區塊被保留下來，用作區域網路上的私人 IP 位址。

名稱	IP 位址範圍	可用地址數量	最大子網路遮罩
24 位元區塊	10.0.0.0 至 10.255.255.255	16,777,216	255.0.0.0
20 位元區塊	172.16.0.0 至 172.31.255.255	1,048,576	255.240.0.0
16 位元區塊	192.168.0.0 至 192.168.255.255	65,536	255.255.0.0

LAN 1 的預設起始 IP 位址為 192.168.1.1，子網路遮罩為 255.255.255.0，總共可分配 254 個 IP 位址，範圍從 192.168.1.1 到 192.168.1.254。所選範圍的最後一個 IP 位址保留用於路由，不能指派給 LAN 用戶端。

大多數情況下，預設的 IP 位址區塊就能滿足需求。但是，有時您需要選擇不同的位址區塊，例如當您需要與其他已經使用相同位址區塊的區域網路通訊時。

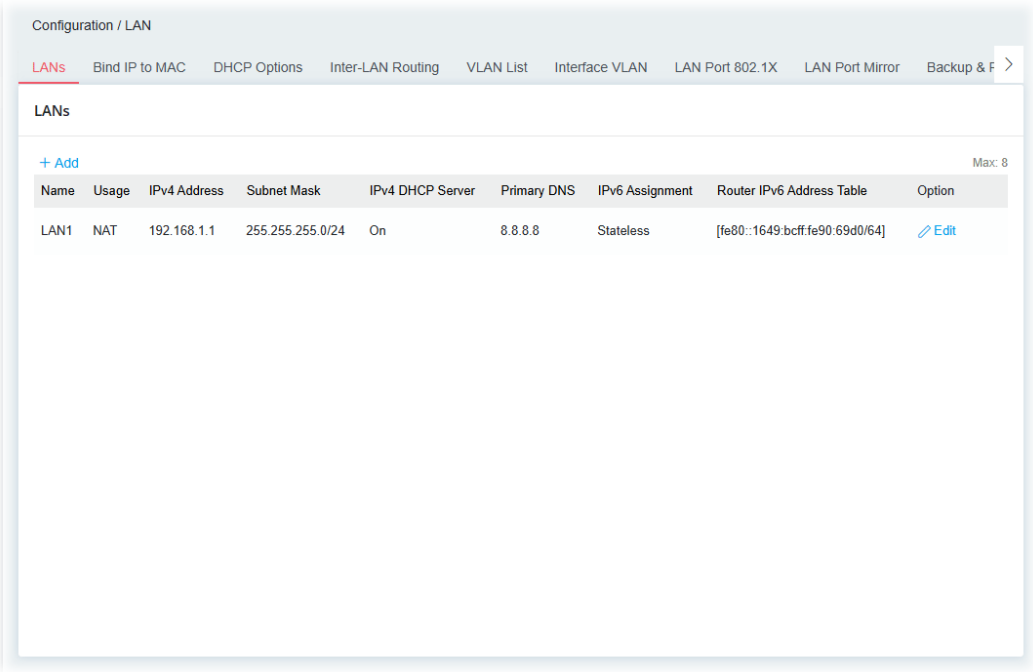
虛擬 IP 位址可以透過動態主機設定通訊協定 (DHCP) 自動指派給區域網路用戶端，也可以手動指派。DHCP 伺服器可以是路由器（最常見的情況），也可以是單獨的伺服器，負責分配 IP 位址到 DHCP 用戶端。

或者，也可以在區域網路用戶端的網路設定中手動設定靜態 IP 位址。無論採用何種 IP 位址配置方式，都必須確保沒有兩個裝置分配到相同的 IP 位址。如果網路中同時使用 DHCP 和靜態 IP 位址分配，則必須將靜態 IP 位址從 DHCP IP 位址儲備庫中排除。例如，如果您的區域網路使用 192.168.1.x 子網，並且有 20 個 DHCP 用戶端和 20 個靜態 IP 用戶端，則可以將起始 IP 位址設定為 192.168.1.10，IP 位址儲備庫數量設定為 50（足以滿足當下 DHCP 位址 192.168.1.100 的位址用於靜態 IP 位址分配)。

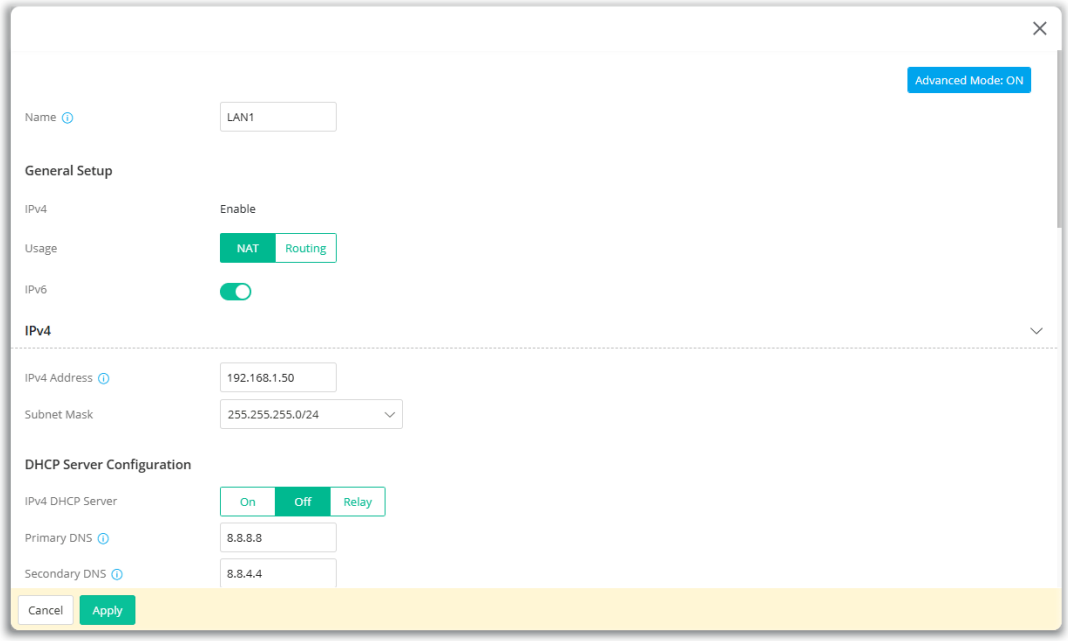
II-1-3-1 LANs 設定

本頁面提供區域網路的基本設定。

打開**設定>>區域網路(LAN) (Configuration>>LAN)**然後按下 **LANs** 標籤開啟下一頁。



欲新增/編輯設定檔，請按下**+新增/編輯(+Add/Edit)**鏈結即可開啟如下頁面。此處以 LAN1 為例。



可用設定說明如下：

項目	說明
進階模式:開啟/關閉 (Advanced Mode:ON/OFF)	按此顯示或隱藏 LAN 的進階設定
名稱(Name)	顯示名稱以便識別。如有需要，請更改名稱。
基本設定(General Setup)	
IPv4	顯示設定檔的狀態（啟用/停用）。
用法(Usage)	指定 IP 轉送方式。 • **NAT** • **路由(Routing)**
IPv6	切換此開關以設定/忽略 IPv6 設定。
IPv4	
IPv4 位址(IPv4 Address)	LAN 介面的 IP 位址(預設值：192.168.1.1)。
子網遮罩(Subnet Mask)	選擇 LAN 介面的子網路遮罩。
DHCP 伺服器設定(DHCP Server Configuration)	
IPv4 DHCP 伺服器(IPv4 DHCP Server)	LAN1 預設配置為 DHCP。 DHCP 代表動態主機設定協定。路由器出廠預設為充當網路中的 DHCP 伺服器，因此它會自動將相關的 IP 設定指派給任何配置為 DHCP 用戶端的本機使用者。如果您沒有為網路設定 DHCP 伺服器，強烈建議您保持路由器啟用 DHCP 伺服器功能。 如果您想在網路中使用 Vigor 路由器以外的其他 DHCP 伺服器，您可以讓 Relay Agent 協助您將 DHCP 請求重新導向到指定位置。 **開啟(On)** - 啟用路由器上的內建 DHCP 伺服器。

	關閉(Off) - 停用路由器上的內建 DHCP 伺服器。 **中繼(Relay)** - 選取後，所有 DHCP 請求都會轉送至 LAN 子網路以外的 DHCP 伺服器，其位址會在 DHCP 伺服器 IP 位址欄位中指定。
如果 DHCP 伺服器設定為開啟(On)	**起始 IP 位址(Start IP Address)** - 指派給 LAN DHCP 用戶端的起始 LAN IP 位址。 **IP 配置量計數(IP Pool Counts)** - DHCP 伺服器分配的 IP 位址的最大數量。預設值為 100。有效範圍為 1 到 253。 **閘道 IP 位址(Gateway IP Address)** - 閘道的 IP 位址，閘道是區域網路中負責轉送所有進出區域網路流量的主機。閘道通常是路由器。 **租約時間(Lease Time)** - DHCP 分配的 IP 位址在需要續約之前可以使用的最長時間。 **主要 DNS(Primary DNS)** - DNS 代表網域名稱系統。每個網路主機都必須有一個獨特的 IP 位址，它們還可以擁有一個易於記憶的域名，例如 www.yahoo.com。DNS 伺服器會將這個易於記憶的網域轉換為對應的 IP 位址。 **次要 DNS(Secondary DNS)** - 您可以在此指定次要 DNS 伺服器 IP 位址，因為您的 ISP 通常會為您提供多個 DNS 伺服器。
如果 DHCP 伺服器設定為中繼(Relay)	選取後，所有 DHCP 請求都會轉送至 LAN 子網路以外的 DHCP 伺服器，其位址會在 DHCP 伺服器 IP 位址欄位中指定。 **主要 DNS(Primary DNS)** - DNS 代表網域名稱系統。每個網路主機都必須有一個獨特的 IP 位址，它們還可以擁有一個易於記憶的域名，例如 www.yahoo.com。DNS 伺服器會將這個易於記憶的網域轉換為對應的 IP 位址。 您必須在此處指定 DNS 伺服器 IP 位址，因為您的 ISP 通常會為您提供多個 DNS 伺服器。 **次要 DNS(Secondary DNS)** - 您可以在此指定次要 DNS 伺服器 IP 位址，因為您的 ISP 通常會為您提供多個 DNS 伺服器。 **透過 WAN 之 DHCP 中繼(主要) (DHCP Relay over WAN (Primary))** – 切換此開關以啟用此功能。然後，為第一個 DHCP 伺服器指定一個 WAN 介面。 - **主要 DHCP 伺服器介面(Primary DHCP Server Interface)** – 使用下拉清單為第一個 DHCP 伺服器選擇 WAN 介面。 **主要 DHCP 伺服器位址(Primary DHCP Server IP Address)** - 輸入 DHCP 伺服器的 IP 位址，LAN 用戶端的 DHCP 請求將會轉送至該伺服器。 **透過 WAN 之 DHCP 中繼(次要) (DHCP Relay over WAN (Secondary))** - 次要 DHCP 伺服器是可選設定。如有需要，請為**次要** DHCP 伺服器指定一個 WAN 介面作為備援伺服器。 - **次要 DHCP 伺服器介面(Secondary DHCP Server Interface)** – 使用下拉清單為第二個 DHCP 伺服器選擇 WAN 介面。

	次要 DHCP 伺服器 IP 位址(Secondary DHCP Server IP Address) - 輸入 DHCP 伺服器的 IP 位址，LAN 用戶端的 DHCP 請求將會轉送至該伺服器。
遠端工作人員的 IP 分配 (IP Assignment for Teleworkers)	VPN 用戶端將從 DHCP 位址配置量或 IP 位址範圍（如下定義）接收遠端工作人員的 IP 位址。 **分派之起始 IP (Assignment Start IP)** – 輸入 IP 位址，該位址將作為 IP 位址範圍的起始點。 **分派之結束 IP (Assignment End IP)** – 輸入 IP 位址，該位址將作為 IP 位址範圍的終點。
	IPv6
IPv6 分派(IPv6 Assignment)	設定路由廣播中的受管理位址設定旗標(M-bit)。 **無狀態(Stateless)** – 未設定 M-bit。 **DHCPv6(Stateful)** – M 位元(M-bit)已設置，這表示 LAN 用戶端應從 DHCPv6 伺服器取得所有 IPv6 設定資訊。DHCPv6 伺服器可以是 Vigor 路由器內建的伺服器，也可以是獨立的 DHCPv6 伺服器。 **手動(Manual)** – 未傳送任何設定資訊。
路由器廣播組態(Router Advertisement Configuration)	當 IPv6 位址分配選擇為無狀態(Stateless)時，此功能可用。 路由器廣播常駐程式(daemon)會定期向本地乙太網路 LAN 發送路由器通告訊息（Router Advertisement messages），這些訊息遵循 RFC 2461 規範。當節點發送路由器請求訊息（Router Solicitation messages）時，也會傳送這些訊息。這些訊息是 IPv6 無狀態自動配置所必需的。 **產生前置碼的方式(Generate Prefix From)** – 選擇能夠產生 IPv6 位址前置碼的主要 WAN 介面。使用下拉清單指定用於 IPv6 的 WAN 介面。 
DNS 設定(DNS Configuration)	當 IPv6 位址分配選擇為無狀態(Stateless)時，可使用此功能。 **DNS 分派方式(DNS Assign Methods)** • **RA(RDNSS)** – 用於主機（例如 PC）的 DNS 伺服器將透過路由器廣播組態進行設定。 • **O-Bit(DHCPv6)** – 用於主機的 DNS 伺服器將透過 DHCPv6 伺服器進行設定。 • **手動(Manual)** – Vigor 路由器系統不會向主機發送 DNS 伺服器設定。 **主要 DNS 位址(Primary DNS Address)** - 輸入主要 IPv6 位址 DNS 伺服器。 **次要 DNS 位址(Secondary DNS Address)** - 如果需要，請輸入另一個 DNS 伺服器的 IPv6 位址。

DHCPv6 伺服器設定 (DHCPv6 Server Configuration)	當選擇 DHCPv6 (有狀態) 作為 **IPv6 分派(IPv6 Assignment)**時，可使用此功能。 **開啟(On)** - 啟用路由器上的內建 DHCPv6 伺服器。 ● **產生前置碼的方式(Generate Prefix From)** – 選擇能夠產生 IPv6 位址前置碼的主要 WAN 介面。使用下拉清單指定用於 IPv6 的 WAN 介面。 ● **自動 IPv6 位址範圍(Auto IPv6 Address Range)** - 啟用此功能後，路由器內建的 DHCPv6 伺服器將決定要使用的 LAN IPv6 位址範圍。取消選取此功能後，指派的 LAN IPv6 位址將位於**起始位址**和**結束地址**指定的範圍內。 ● **隨機 IPv6 位址分派(Random IPv6 Address Allocation)** - 啟用後，路由器將隨機分配 DHCPv6 IP 位址，以防止 IPv6 偵測技術攻擊。 **關閉(Off)** - 停用路由器上的內建 DHCPv6 伺服器。 **中繼(Relay)** - 選取後，所有 DHCP 請求都會轉送至 LAN 子網路以外的 DHCP 伺服器，其位址會在 DHCP 伺服器 IP 位址欄位中指定。 ● **DHCPv6 伺服器介面(DHCPv6 Server Interface)** – 使用下拉清單指定 IPv6 的 WAN 介面。 ● **DHCPv6 伺服器位址(DHCPv6 Server Address)** - 輸入 DHCPv6 伺服器的 IPv6 位址。
DNS 設定(DNS Configuration)	當 IPv6 位址分配選擇為 DHCPv6 (Stateful)時，可使用此功能。 **主要 DNS 位址(Primary DNS Address)** - 輸入主要 IPv6 位址 DNS 伺服器。 **次要 DNS 位址(Secondary DNS Address)** - 如果需要，請輸入另一個 DNS 伺服器的 IPv6 位址。
更多設定 – 強制執行 DNS 重導向 (Force DNS Redirection	**啟用(Enable)** – 切換開關即可啟用或停用此功能。 切換此開關即可啟用或停用此功能。此功能允許攔截所有傳出的 DNS 查詢並將其重導向到路由器內建的 DNS 伺服器，透過快取 DNS 查詢和結果來提高網域名稱尋找效能。
進階模式下的選項	
路由器 IPv6 位址表格 (Router IPv6 Address Table)	輸入要新增的 IPv6 位址和前置碼長度，或按一下下面的目前 IPv6 位址表中要刪除的現有 IPv6 位址，其值將自動複製過來。 **+新增(+Add)** – 按此處新增條目。最多可新增 5 個條目。 **靜態 IP 位址(Static IP Address)** – 輸入區域網路的靜態 IPv6 位址。 **Prefix Length** - Enter the IPv6 prefix length for the IPv6 address.
唯一區域位址(ULA)設定 (Unique Local Address Configuration)	**唯一區域位址(ULA)**是指派給 LAN 用戶端的虛擬 IPv6 位址。 **ULA 前置碼(ULA Prefix)** – LAN 用戶端將被指派根據手動輸入的前置碼所產生的 ULA。 ● **關閉(Off)** – ULA 已停用。 ● **自動(Auto)** – LAN 用戶端將使用自動決定的前置碼來分配 ULA。 ● **手動(Manual)** – 請輸入 IPv6 位址。
路由器廣播組態(Router Advertisement Configuration)	當 IPv6 位址分配選擇為無狀態(Stateless)時，可使用此功能。 進階設定頁面包含路由器通告和啟用多個 WAN 以進行 IPv6 流量的附加設定。 **RA 優先權(RA Priority)** – 選擇在路由通告訊息中傳送的路由器的預設首

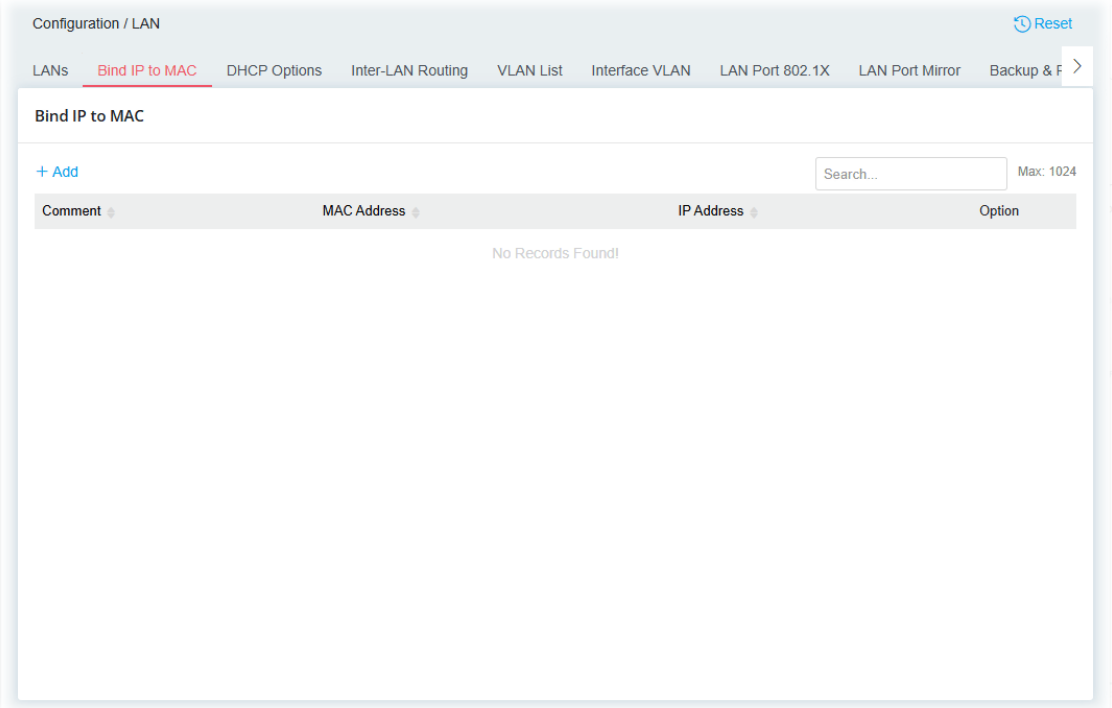
	選值（低、中、高）。 **最小/最大間隔時間(Min / Max Interval Time)** – RA 伺服器傳送未經請求的多重播送路由通告訊息之間的最短/最長時間間隔（以秒為單位）。 **有效時間(Valid Lifetime)** – 輸入一個數字(單位為秒)來指定 DHCPv6 伺服器的有效存活時間。本裝置（透過 LAN 介面連接）將用作預設路由器。 在有效期限內，該裝置（透過 LAN 介面連接）將被視為預設路由器。 **優選有效時間(Preferred Lifetime)** – 輸入一個數字（單位為秒）來指定 DHCPv6 伺服器的首選**有效時間**。該值必須小於或等於有效**時間**。在首選生存**時間**內，此設備（Vigor 路由器）將被視為預設路由器。當存在多個路由器時，需要設定優先權。通常，處於首選有效時間內的路由器優先權高於其他處於有效時間內的路由器。 **躍點限制(Hop Limit)** - 當使用 IPv6 時，路由器後面的裝置需要此值。路由通告訊息中跳數限製欄位的預設值。
DHCPv6 伺服器設定 (DHCPv6 Server Configuration)	當選擇 DHCPv6（Stateful）作為 **IPv6 分派(IPv6 Assignment)**時，可使用此功能。 **驗證通訊協定(Authentication Protocol)** – 此通訊協定用於用戶端在存取網際網路之前，系統透過 DHCPv6 伺服器對該用戶端進行身份驗證。可指定三種類型：**重新設定金鑰(Reconfigure Key)**、**延遲(Delayed)**和**無(None)**。通常，預設值為無。 ● **重新設定金鑰(Reconfigure Key)** – 在連線過程中，DHCPv6 伺服器將自動對用戶端進行身份驗證。 ● **延遲(Delayed)** - 在連線過程中，DHCPv6 伺服器將根據這些欄位中指定的金鑰 ID、領域和秘鑰資訊對用戶端進行身份驗證和識別。 **金鑰 ID (Key ID)** – 輸入一個值（範圍從 1 到 65535），該值將用於產生 HMAC-MD5 值。 **領域(Realm)** – 在此輸入的名稱（1 到 31 個字元）將標識產生 HMAC-MD5 值的密鑰。 **密鑰(Secret)** – 輸入一段文字（1 到 31 個字元）作為每個 DHCP 伺服器上每個用戶端的唯一識別碼。 ● **有效時間(Valid Lifetime)** – 輸入一個數字（單位為秒）來指定 DHCPv6 伺服器的有效存活時間。本裝置（透過 LAN 介面連接）將用作預設路由器。 在有效期限內，該裝置（透過 LAN 介面連接）將被視為預設路由器。 ● **優選有效時間(Preferred Lifetime)** – 輸入一個數字（單位為秒）來指定 DHCPv6 伺服器的首選**有效時間**。該值必須小於或等於有效**時間**。在首選生存**時間**內，此設備（Vigor 路由器）將被視為預設路由器。當存在多個路由器時，需要設定優先權。通常，處於首選有效時間內的路由器優先權高於其他處於有效時間內的路由器。 ● **前置碼授權(Prefix Delegation)** – 切換此開關啟用或停用此功能。若是啟用此功能，路由器可以將子前置碼從廣域網路分派往區域網路用戶端。
前置碼授權表(Prefix Delegation Table)	此功能在啟用**前置碼授權(Prefix Delegation)**後，即可使用。最多可設定 5 個設定檔。 **+新增(+Add)** – 按此可新增條目。 **前置碼(Prefix)** – 輸入 ISP 業者提供的 IPv6 位址之前置碼。 **前置碼長度(Prefix Length)** – 輸入 IPv6 位址的前置碼長度。 **用戶端鏈結本機位址(Client Link Local Address)** – 輸入遠端用戶端的 IPv6 位址。

	用戶端 DUID (Client DUID) – 輸入遠端用戶端的 DHCP Unique Identifier (DUID)識別碼。 **選項(Option)** – 按下刪除(Delete)以移除選定的項目。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前的設定並離開此頁面。

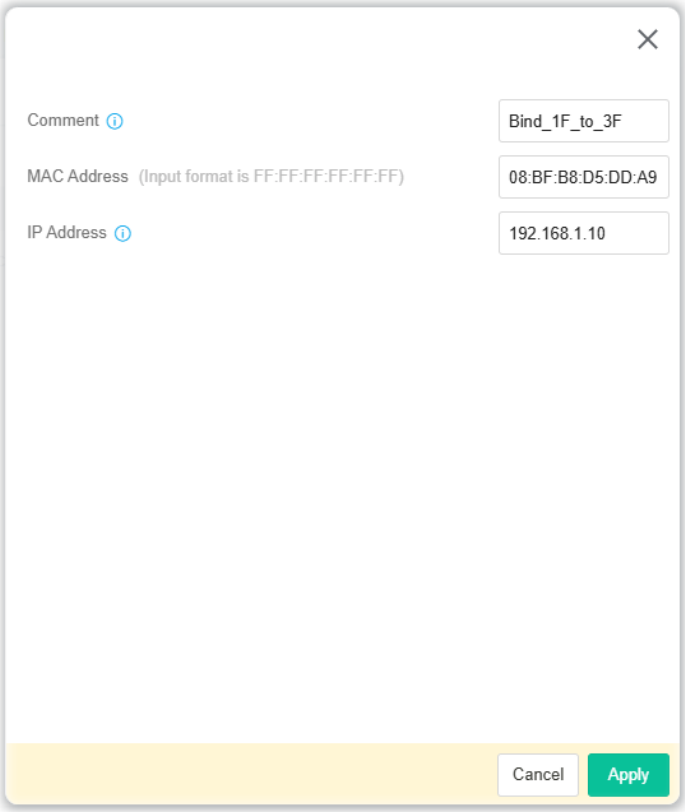
完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-1-3-2 綁定 IP 至 MAC (Bind IP to MAC)

此功能主要用在區域網路中綁定 IP 位址和 MAC 位址，以加強網路控制。透過綁定 IP 至 MAC 功能，您可以為區域網路用戶端預留 IP 位址。每個預留的 IP 位址都與一個媒體存取控制 (MAC) 位址相關。



欲新增/編輯設定檔，請按下**+新增/編輯(+Add/Edit)**鏈結即可開啟如下頁面。

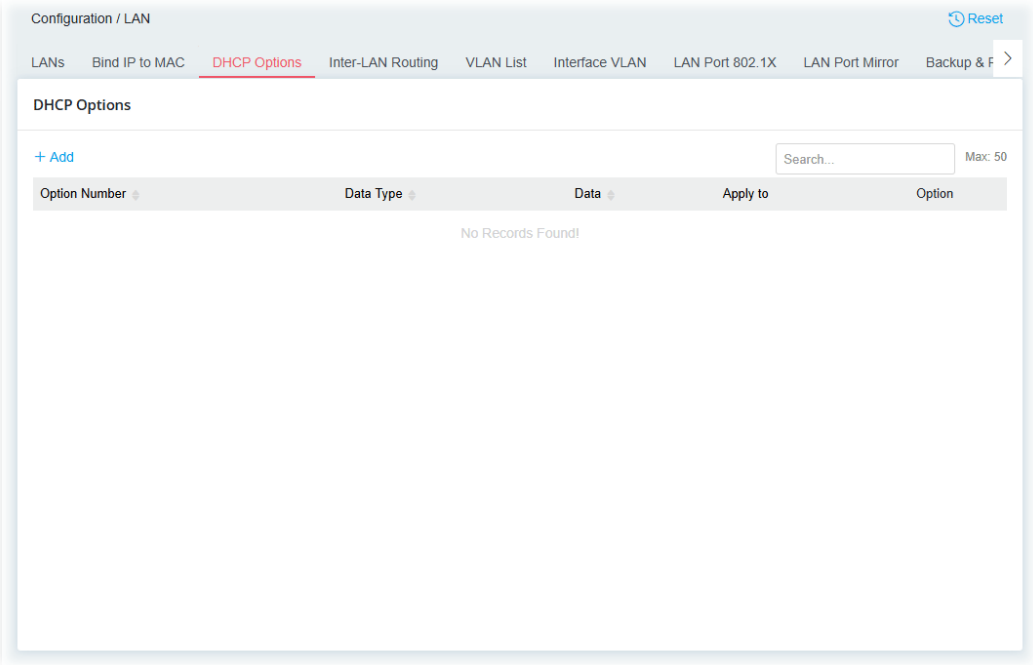


可用設定說明如下：

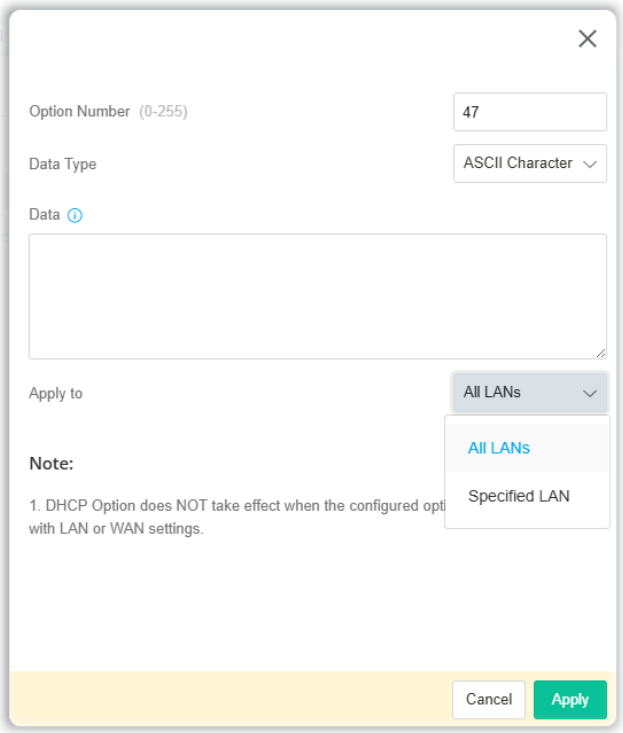
項目	說明
註解(Comments)	輸入簡短註釋以識別此組 IP 位址 - MAC 位址。
MAC 位址(MAC Address)	輸入區域網路用戶端網路介面的 MAC 位址。
IP 位址(IP Address)	輸入要與 MAC 位址關聯的 IP 位址。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

II-1-3-3 DHCP 選項(DHCP Options)

啟用並設定此功能後，可以透過新增選項編號(option number)和資料資訊來處理 DHCP 封包。



欲新增/編輯設定檔，請按下**+新增/編輯(+Add/Edit)**鏈結即可開啟如下頁面。



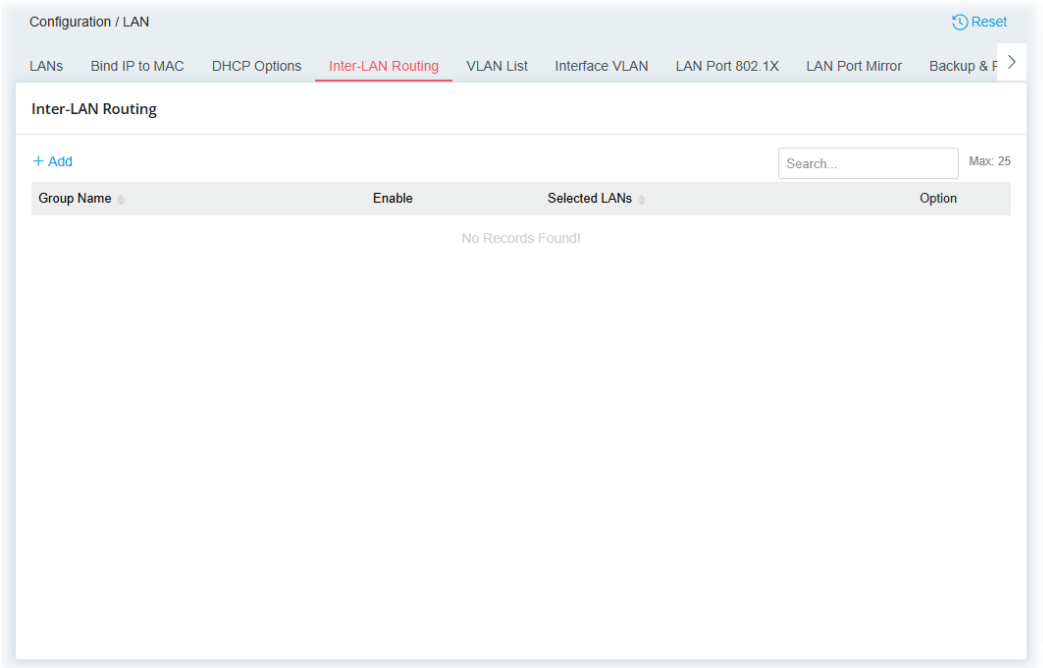
可用設定說明如下：

項目	說明
選項號碼(Option Number)	為此功能輸入 DHCP 選項編號。
資料類型(Data Type)	選擇要儲存的資料類型（ASCII、十六進位或位址清單）。
資料(Data)	依照所選資料類型，在資料欄位中輸入資料。 **ASCII 字元(ASCII Character)** - 一個文字字串。例如：/path。 **十六進位數字(Hexadecimal Digital)** - 十六進位字串。有效字元為 0 到

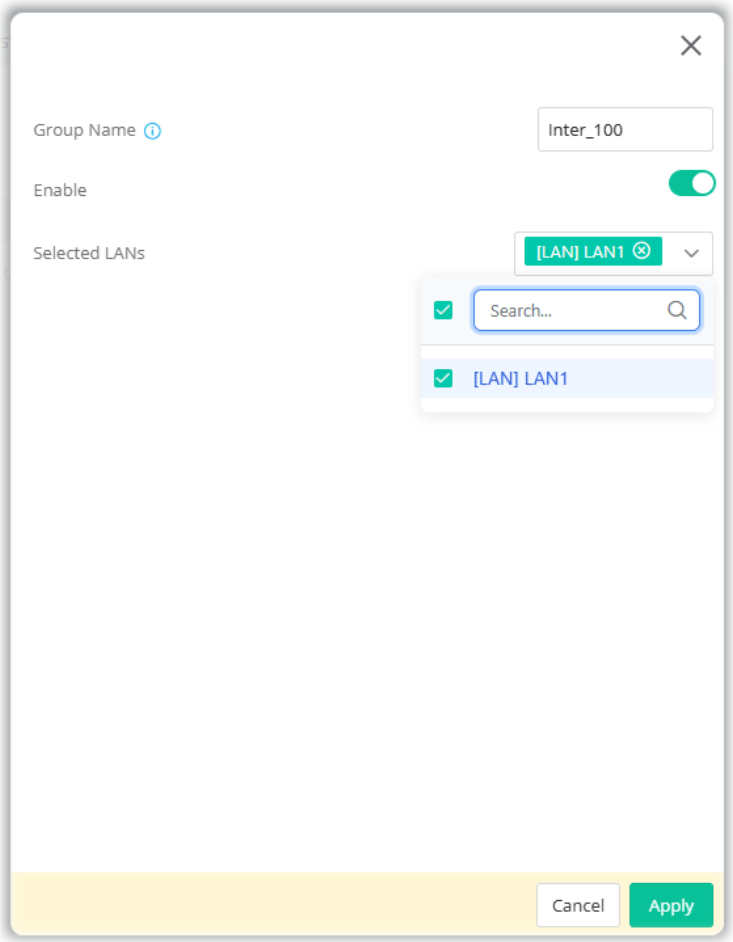
	9 和 a 到 f。例如：2f70617468。 **位址清單(Address List)** - 一個或多個 IPv4 位址，以逗號分隔。
套用(Apply) to	選擇此條目適用的 LAN 介面。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

II-1-3-4 跨 LAN 路由(Inter-LAN Routing)

路由器最多可提供 25 個路由設定檔，允許將使用者群組劃分到不同的子網路。此外，不同的子網路可以透過此跨 LAN 路由之設定來相互連接。



欲新增/編輯設定檔，請按下**+新增/編輯(+Add/Edit)**鏈結即可開啟如下頁面。



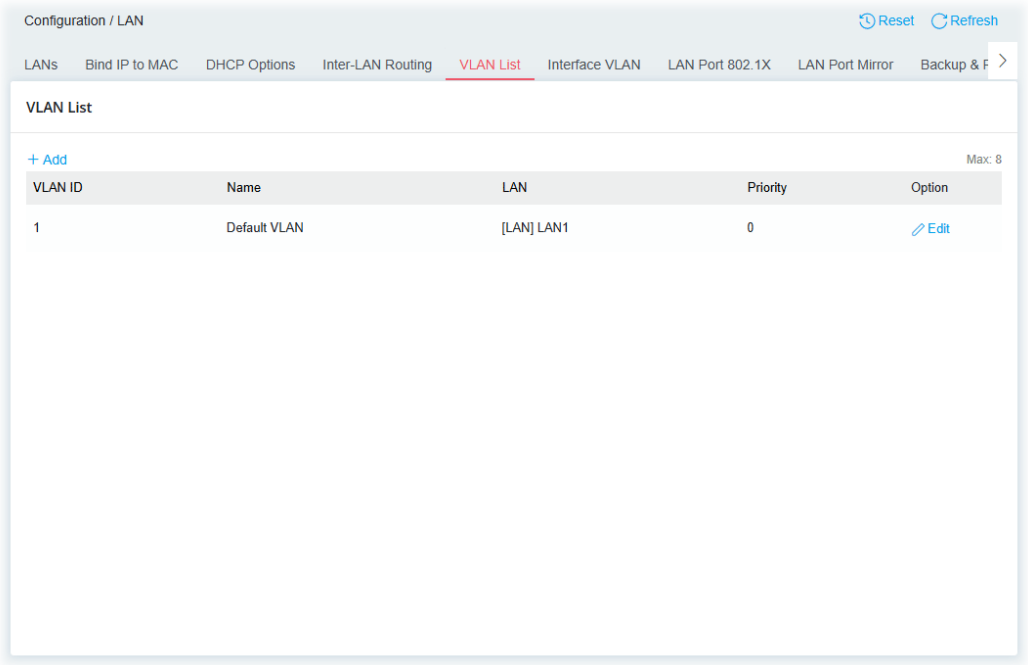
可用設定說明如下：

項目	說明
群組名稱(Group Name)	顯示名稱以便識別。如有需要，請更改名稱。
啟用(Enable)	切換此開關以啟用這些設定。
選定的 LAN (Selected LANs)	勾選此方塊可連接兩個或多個不同的子網路（LAN 和 LAN）。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

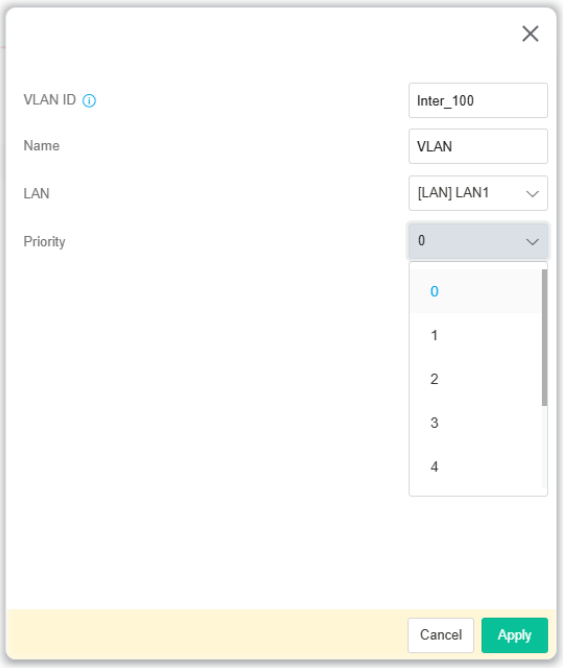
II-1-3-5 VLAN 清單(VLAN List)

虛擬區域網路（VLAN）可讓您將 LAN 細分，以便於管理或提高網路安全性。

此頁面可讓您建立最多 8 個 VLAN 設定檔。



欲新增/編輯設定檔，請按下**+新增/編輯(+Add/Edit)**鏈結即可開啟如下頁面。



可用設定說明如下：

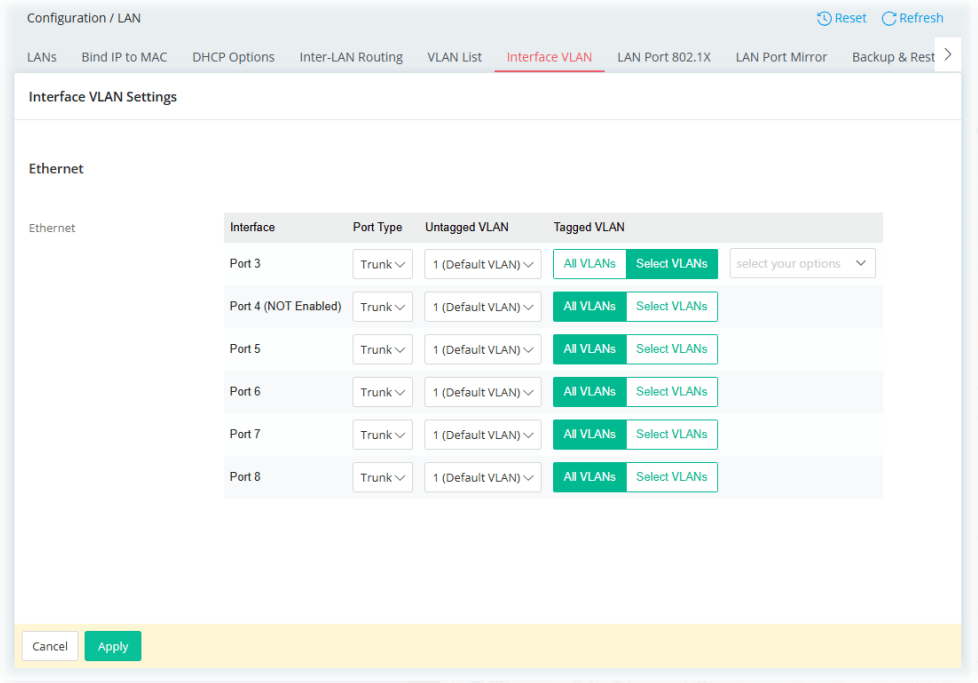
項目	說明
VLAN ID	請輸入數字作為 VLAN 識別碼。有效值為 1 至 4094。 VLAN 識別碼必須唯一的。

名稱(Name)	輸入 VLAN 設定檔的名稱。
LAN	顯示路由器上的實體區域網路子網路。選擇要綁定到所選 VLAN 下的區域網路子網路。
優先權(Priority)	選擇此區域網路設定檔的優先順序。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

II-1-3-6 介面 VLAN (Interface VLAN)

介面 VLAN 使用實體連接埠（P1 ~ P4）將客戶端分隔到不同的 VLAN 群組中。

虛擬區域網路功能提供了一種非常方便的主機管理方式，主要是依照實體連接埠來進行組別分類。多重子網路架構能夠為小型企業的多人共用環境用戶應用提供更好的隔離性。



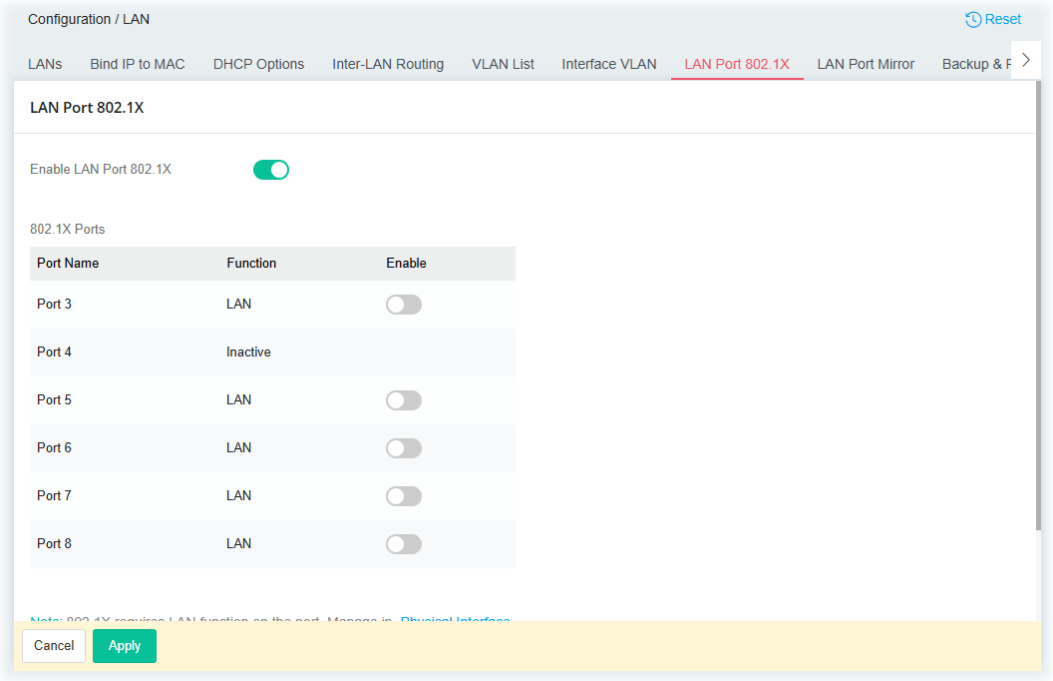
可用設定說明如下：

項目	說明
埠號類型(Port Type)	選擇介面(連接埠 1 至 4)將套用的 VLAN 類型。 **Trunk(幹道)** – 選定的乙太網路連接埠可用於或套用於多個 VLAN 設定檔。 **存取(Access)** – 選定的乙太網路連接埠可用於或套用於單一 VLAN 設定檔。
未標籤的 VLAN (Untagged VLAN)	選擇不會被標籤的 VLAN 設定檔。 至少保留一個未標籤的 VLAN，以防止因意外錯誤而無法連接到 Vigor 路由器。
已標籤的 VLAN (Tagged VLAN)	為選定的 VLAN 啟用 802.1Q 標記。 路由器在傳送封包給區域網路時，會將特定的 VLAN 編號加入所有封包中。

	全部的 VLAN (All VLANs) – 所有 VLAN 設定檔都將被加上標籤。 **選擇 VLAN (Select VLANs)** – 只有選定的 VLAN 設定檔才會被加上標籤。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

II-1-3-7 LAN 埠口 802.1X (LAN Port 802.1x)

有線 802.1X 為希望透過乙太網路連接到區域網路的用戶端提供身份驗證。每個區域網路連接埠只能對一個用戶端進行身份驗證。

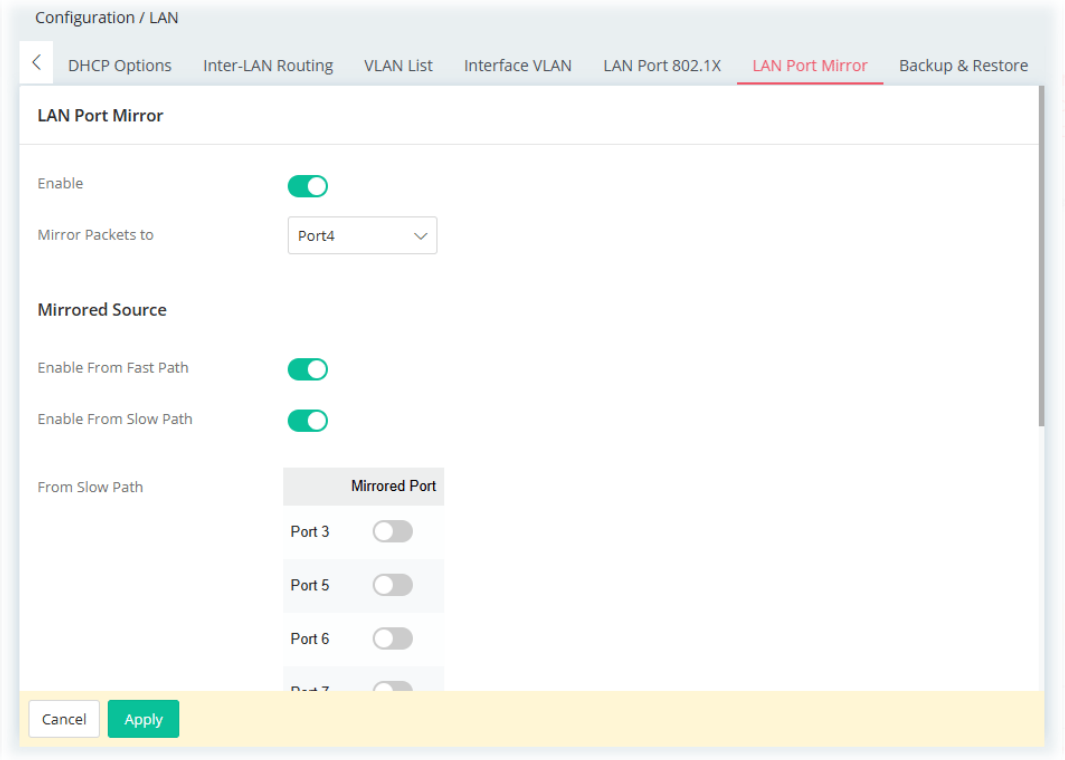


可用設定說明如下：

項目	說明
啟用 LAN 埠口 802.1X (Enable LAN 802.1X)	切換此開關以啟用或停用 LAN 802.1x 功能。
埠口名稱(Port Name)	顯示實體 LAN 連接埠的名稱。
啟用(Enable)	切換此開關即可啟用或停用此功能。 啟用後，所選 LAN 連接埠將支援 802.1X 身份驗證。
外接 RADIUS 伺服器設定檔(External RADIUS Server Profile)	選擇一個外部 RADIUS 伺服器設定檔，該設定檔將用於驗證來自已啟用 802.1 連接埠的使用者的身份。
取消(Cancel)	捨棄目前設定。
套用(Apply)	儲存目前設定。

II-1-3-8 LAN 埠口監控(LAN Port Mirror)

LAN 埠口監控功能可將指定 LAN 連接埠的網路流量鏡射至另一個 LAN 連接埠，以供分析。此功能有助於執行網路策略、偵測未經授權的存取、監控網路效能等。

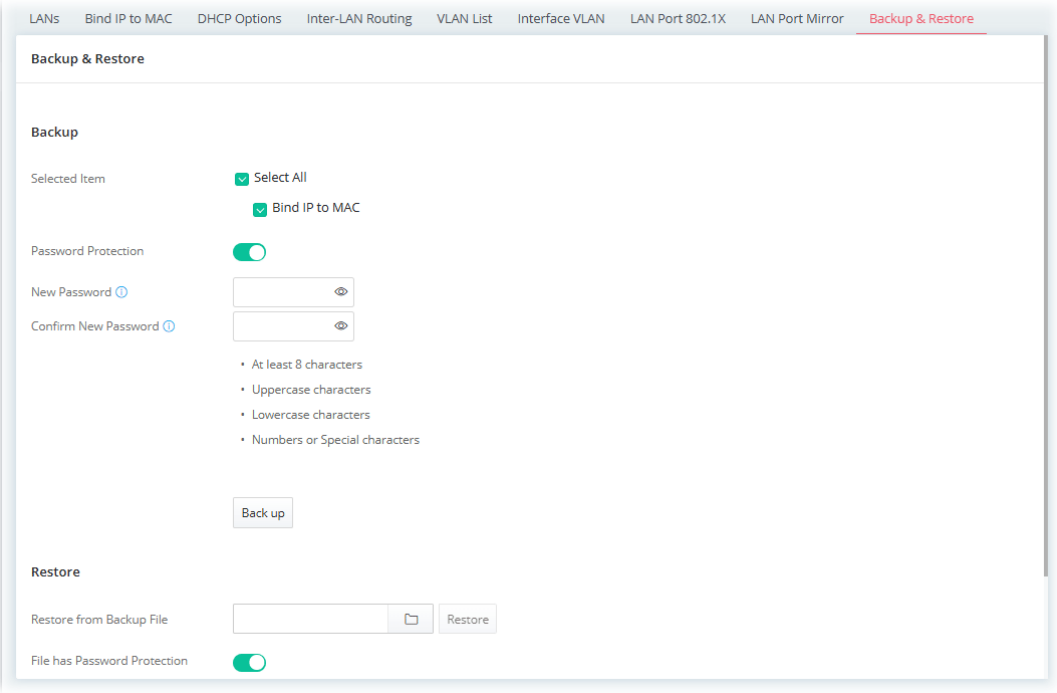


可用設定說明如下：

項目	說明
啟用(Enable)	切換開關即可啟用或停用 LAN 連接埠鏡像功能。
監控封包至(Mirror Packets to)	指定連接埠。 選擇一個且僅選擇一個埠口作為鏡像埠，網路流量將轉發到該埠口。
受監控之來源(Mirrored Source)	
啟用自快速路徑(Enable From Fast Path)	切換開關即可啟用或停用此功能。 啟用後，硬體加速器處理的全部已傳送 (TX) 和已接收 (RX)的封包都將被複製並傳送到鏡像連接埠。
啟用自慢速路徑(Enable From Slow Path)	切換開關即可啟用或停用此功能。 啟用後，所有經過所選鏡像連接埠的已傳送 (TX) 和已接收 (RX) 封包都將被複製並傳送到鏡像連接埠。
自慢速路徑(From Slow Path)	**受監控埠口(Mirrored Port)** – 切換開關，選擇此介面作為鏡像連接埠。
取消(Cancel)	捨棄目前設定。
套用(Apply)	儲存目前設定。

II-1-3-9 備份與還原(Backup & Restore)

LAN 設定可以備份為檔案。未來如果有需要，可以將備份檔案匯入此裝置以還原設定。



可用設定說明如下：

項目	說明
	備份(Backup)
選定項目 (Selected 項目)	選擇要備份設定的項目。
密碼保護 (Password Protection)	切換開關即可啟用或停用此功能。 如果啟用此功能，請設定密碼。 ● **新密碼(New Password)** – 輸入一個字串作為密碼。 ● **確認新密碼(Confirm New Password)** – E 再度輸入密碼。 **備份(Back up)** – 按此執行備份作業。
	還原(Restore)
還原自備份檔案 (Restore from Backup File)	選擇要還原的備份檔案。 – 按此尋找還原的檔案。 **還原(Restore)** – 按此可還原 LAN 設定。
檔案具有密碼保護 (File has Password Protection)	切換開關即可啟用或停用此功能。 如果啟用此功能，請設定密碼。 ● **密碼(Password)** – 請輸入一個字串作為還原設定的密碼。

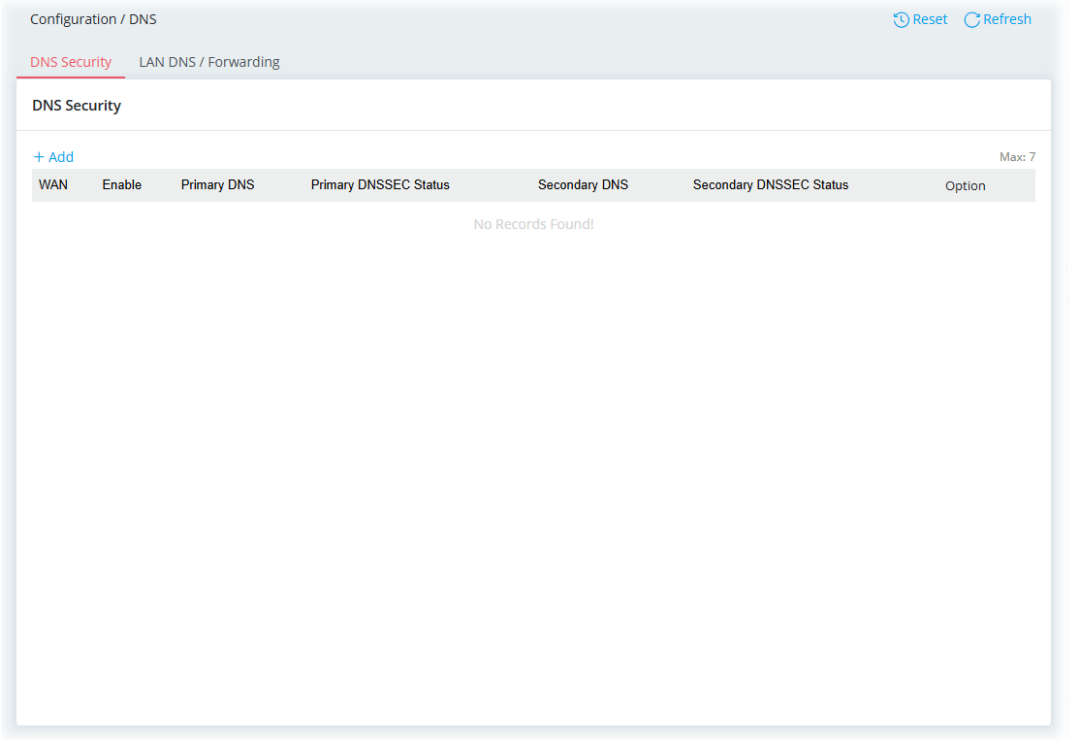
II-1-4 DNS

DNS 代表網域名稱系統。每個網路主機都必須有一個獨特的 IP 位址，它們還可以擁有一個易於記憶的域名，例如 www.yahoo.com。 DNS 伺服器會將這個易於記憶的網域轉換成對應的 IP 位址。

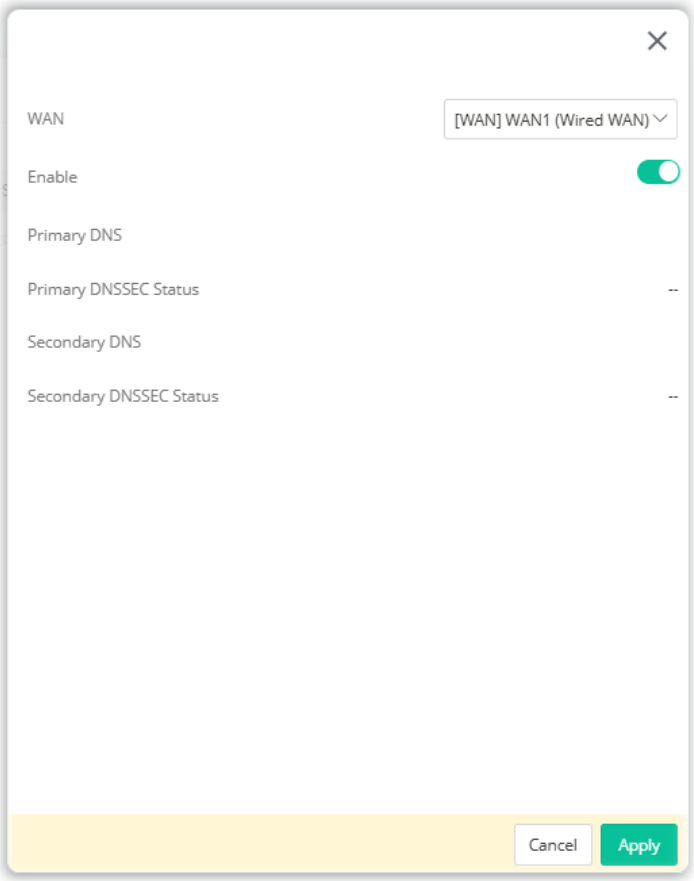
本節提供 DNS 安全性和 LAN DNS/轉送的設定。

II-1-4-1 DNS 安全性(DNS Security)

DNS 伺服器必須支援 DNS 安全性驗證，功能才能正常運作。



欲新增/編輯設定檔，請按下**+新增/編輯(+Add/Edit)**鏈結即可開啟如下頁面。



可用設定說明如下：

項目	說明
WAN	選擇要為其設定 DNS 安全性的 WAN 介面。
啟用(Enable)	切換此開關可啟用或停用此 WAN 介面的 DNS 安全性。啟用 DNS 安全性後，虛偽 DNS 回復(Bogus DNS Reply)將被丟棄。
主要 DNS (Primary DNS)	顯示此廣域網路使用的主要 DNS 伺服器。 如果出現 “--” ，則表示沒有廣域網路 WAN 或沒有設定 DNS 伺服器。
主要 DNSSEC 狀態 (Primary DNSSE Status)	顯示 DNS 伺服器是否支援 DNS 安全性的檢查結果。結果可能如下： ● [Supported] 表示 DNS 伺服器支援 DNS 安全性。 ● [Unsupported] 表示 DNS 伺服器不支援 DNS 安全性。 ● “--" 表示 WAN 介面未啟動或未偵測到 DNS 伺服器。 ● [Check Failed - WAN Issue] 表示由於沒有網路連線而導致檢查失敗。 ● [DNSSEC Disabled] 表示 DNS 安全功能已停用。 **注意:** 網域名稱系統安全擴充（DNSSEC）透過驗證 DNS 解析器的 DNS 回應來防止基於 DNS 的攻擊。
次要 DNS(Secondary DNS)	顯示此廣域網路使用的次要 DNS 伺服器。 如果出現 “--” ，則表示沒有廣域網路 WAN 或沒有設定 DNS 伺服器。
次要 DNSSEC 狀態 (Secondary DNSSE Status	顯示 DNS 伺服器是否支援 DNS 安全性的檢查結果。結果可能如下： ● [Supported] 表示 DNS 伺服器支援 DNS 安全性。 ● [Unsupported] 表示 DNS 伺服器不支援 DNS 安全性。 ● “--"表示 WAN 介面未啟動或未偵測到 DNS 伺服器。 ● [Check Failed - WAN Issue] 表示由於沒有網路連線而導致檢查失敗。

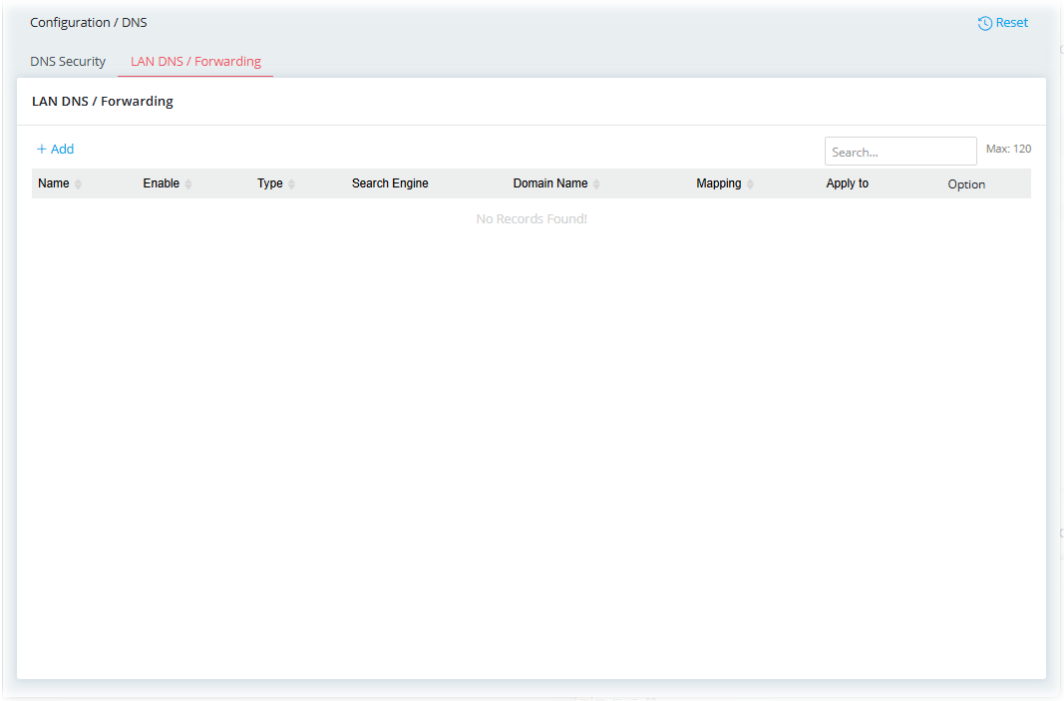
	• [DNSSEC Disabled] 表示 DNS 安全功能已停用。 **注意:** 網域名稱系統安全擴充（DNSSEC）透過驗證 DNS 解析器的 DNS 回應來防止基於 DNS 的攻擊。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

II-1-4-2 LAN DNS /轉發(LAN DNS/Forwarding)

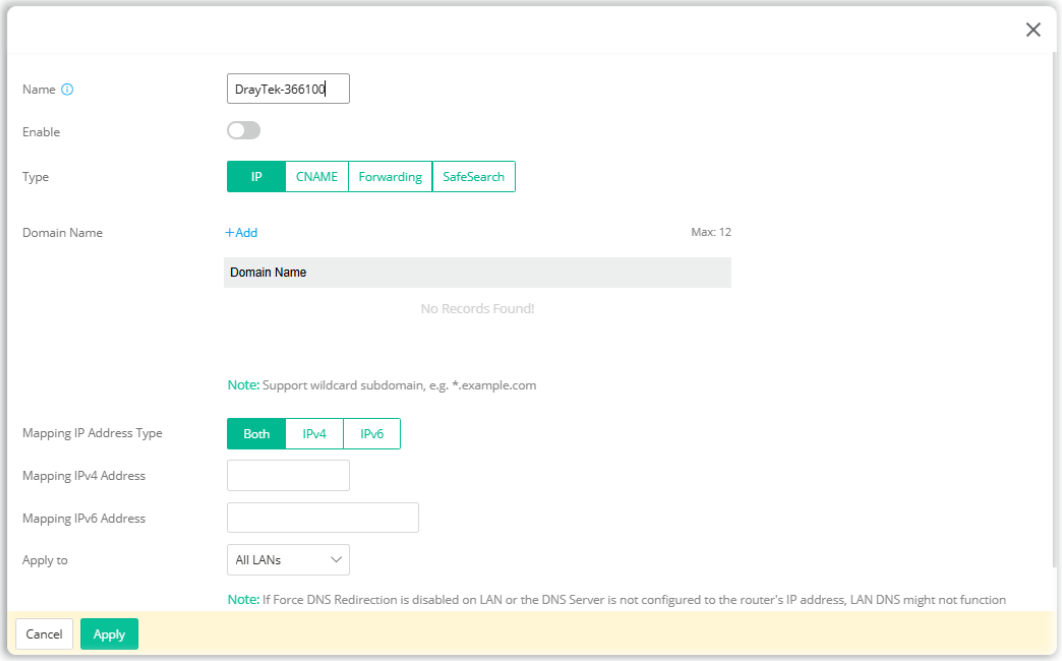
LAN DNS 是 DNS 伺服器的簡化版本。 LAN DNS 讓網路管理員覆蓋標準的 DNS 解析，從而選擇網域名稱位址。路由器會使用自訂 IP 位址回應符合網域名稱的查詢。使用者無需在區域網路中建置額外的 DNS 伺服器。借助此功能，使用者可以設定一些服務 (例如 FTP、網站或資料庫) ，並使用易於存取的網域名稱。

DNS 轉送讓網路管理員根據網域名稱將 DNS 查詢轉送到不同的 DNS 伺服器。

LAN DNS 和 DNS 轉送僅影響透過路由器傳送到 WAN 的 DNS 查詢。傳送到 LAN 上 DNS 伺服器的 DNS 查詢不會被路由器攔截。



欲新增/編輯設定檔(最多可達 120 個)，按下+新增/編輯(**+Add/Edit**)鏈結開啟如下頁面：



可用設定說明如下：

項目	說明
名稱(Name)	輸入字串作為設定檔名稱，以供識別。
啟用(Enable)	切換此開關以啟用/停用此設定檔。
類型(Type)	選擇 **IP, CNAME, 轉發(Forwarding)** 或是 **SafeSearch**。
網域名稱(Domain Name)	**+新增(+Add)** – 輸入路由器要在 DNS 查詢中尋找並攔截回覆的網域名稱。可以使用星號 (*) 作為萬用字元來比對網域名稱等級。例如，*.draytek.com 將比對 www.draytek.com 和 ftp.draytek.com 等網域。最多可以建立 12 個網域。
若類型選擇了 IP	此處列出的 IP 位址將用於與上面指定的網域名稱進行比對。 **對應 IP 位址類型(Mapping IP Address Type)** – 選擇兩者、IPv4 或是 IPv6 (Both, IPv4, IPv6)。 **對應 IPv4 位址(Mapping IPv4 Address)** – 若選擇了二者/IPv4(Both/IPv4)，請在此區輸入 IPv4 位址。 **對應 IPv6 位址(Mapping IPv6 Address)** – 若選擇了二者/IPv6(Both/IPv6)，請在此區輸入 IPv6 位址。 **套用至(Apply to)** – 選擇所有 LAN 或指定的 LAN 介面以套用此 DNS 伺服器設定檔。
若類型選擇了 CNAME	**CNAME** – 輸入網域名稱的別名。 **套用至(Apply to)** - 選擇所有 LAN 或指定的 LAN 介面以套用此 DNS 伺服器設定檔。
若類型選擇了轉發	**DNS 伺服器類型(DNS Server Type)** – 選擇兩者、IPv4 或是 IPv6 (Both, IPv4, IPv6)。 **主要 IPv4 DNS 伺服器(Primary IPv4 DNS Server)** – 輸入要用於 DNS 轉發的 DNS 伺服器的主要 IPv4 位址。 **次要 IPv4 DNS 伺服器(Secondary IPv4 DNS Server)** – 輸入要用於 DNS 轉發的 DNS 伺服器的次要 IPv4 位址。 **主要 IPv6 DNS 伺服器(Primary IPv6 DNS Server)** – 輸入要用於 DNS 轉發的 DNS 伺服器的主要 IPv6 位址。

	次要 IPv6 DNS 伺服器(Secondary IPv6 DNS Server) – 輸入要用於 DNS 轉發的 DNS 伺服器的次要 IPv6 位址。 **套用至(Apply to)** - 選擇所有 LAN 或指定的 LAN 介面以套用此 DNS 伺服器設定檔。
若類型選擇了 SafeSearch	一些搜尋引擎，例如 Bing、Google 和 Yandex，會採取安全措施過濾色情和可能令人反感的內容。這些搜尋引擎被歸類為安全搜尋(SafeSearch)類型。 **搜尋引擎(Search Engine)** – 選擇一個或多個常用的搜尋引擎。 **套用至(Apply to)** -選擇所有 LAN 或指定的 LAN 介面以套用此 DNS 伺服器設定檔。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

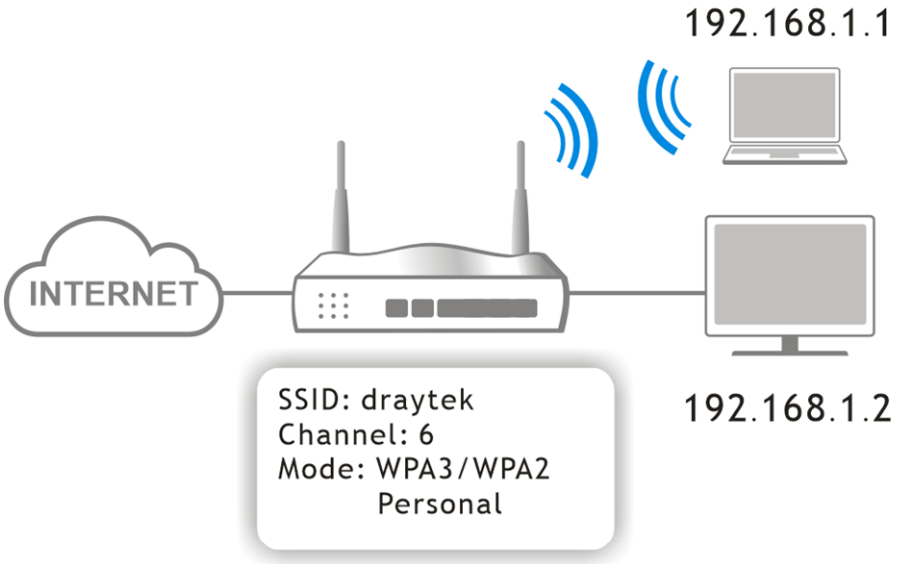
II-1-5 無線區域網路(Wireless LAN)

無線區域網路 (WLAN) 可實現高度移動性，因此 WLAN 使用者可以像在有線區域網路上一樣同時存取所有 LAN 設施以及網際網路。

近年來，無線通訊市場經歷了快速發展。無線技術如今幾乎覆蓋了地球上的每個角落。數十億人每天都在使用無線通訊產品交換資訊。 Vigor C410/C510 系列無線路由器 (型號名稱中帶有「ax」) 的設計充分考慮了靈活性和效率，是小型辦公室或家庭的理想之選。在商業環境中，任何授權人員都可以攜帶配備 WLAN 功能的平板電腦、PDA 或筆記型電腦進入會議室，無需在牆上鑽孔或拆除地板鋪設繁雜的 LAN 線纜即可連接到網路。無線網路實現了高度的移動性，因此 WLAN 使用者可以像在有線 LAN 上一樣存取所有 LAN 資源，而無需使用纜線。

實際資料總處理量會依據網路狀況和環境因素而變化，包括網路流量、網路開銷和建築材料等等

在無線網路的基礎架構模式下，Vigor 無線路由器可作為存取點 (AP)，連接多個無線用戶端或網站 (STA)。所有 STA 都將透過 Vigor 無線路由器共享相同網際網路連線。無線網路設定，例如 SSID、頻道和加密協議，都可以透過此章節進行。



多重 SSID

Vigor 無線路由器每個頻段最多支援四個 SSID (服務集識別碼) 用於無線連線。服務集是指一組具有相同網路參數的無線網路用戶端。每個服務集都可以配置為具有唯一的名稱 (SSID) 和特定的 VLAN 或 MAC 位址過濾列表，並可供不同類別的使用者使用。

即時硬體加密

Vigor 無線路由器配備了硬體 AES 加密引擎，可在不犧牲使用者體驗的前提下，提供最有效用、最高效率的無線流量保護。

完整的安全標準選擇

為了確保您的無線通訊的安全性和隱私性，我們提供市場上幾種主流標準。

有線等效加密（WEP, Wired Equivalent Privacy）是一種傳統的加密方法，它使用 64 位元或 128 位元金鑰對每個透過無線電傳輸的訊框進行加密。通常，無線基地台會預先設定一組四個金鑰，並僅使用其中一個金鑰與每個網站通訊。

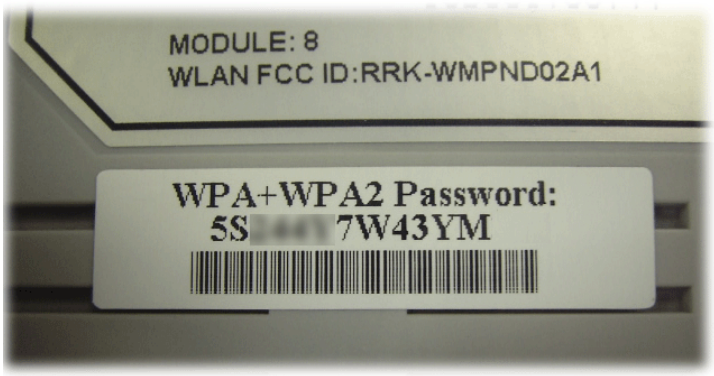
WPA（Wi-Fi Protected Access）是業界最主流的安全機制，分為兩類：WPA-個人版(WPA-Personal)或稱為 WPA 預先共享金鑰(WPA/PSK)，以及 WPA-企業版(WPA-Enterprise)或稱為 WPA/802.1x。

在 WPA-個人版中，預先定義金鑰 (PSK) 用於在資料傳輸期間加密流量。WPA 使用臨時金鑰完整性協定 (TKIP) 進行資料加密，而 WPA2/WPA3 則採用 AES（高級加密標準）。WPA-企業版的一個主要優勢在於它不僅支援加密，還支援身份驗證。

您應根據自身需求選擇合適的安全機制。由於 WEP 已被證實容易受到攻擊，為了獲得最安全的連接，建議您考慮使用 WPA。無論您選擇哪種安全方案，它們都能增強無線網路的無線資料保護和/或隱私保護。Vigor 無線路由器非常靈活，可以同時支援 WEP 和 WPA 的多個安全連線。

資訊

預設密碼（預先共用金鑰 PSK）印在路由器底部的標籤上。由於任何能夠接觸到路由器的人都可以找到預設密碼，因此強烈建議您更改密碼。

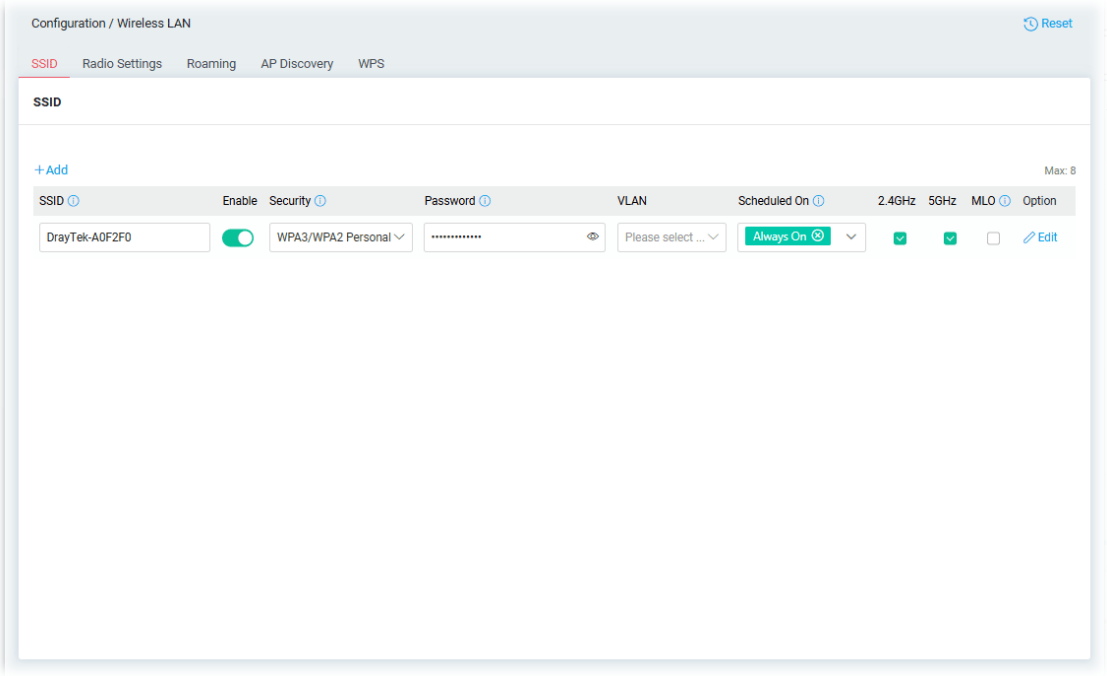


WPS

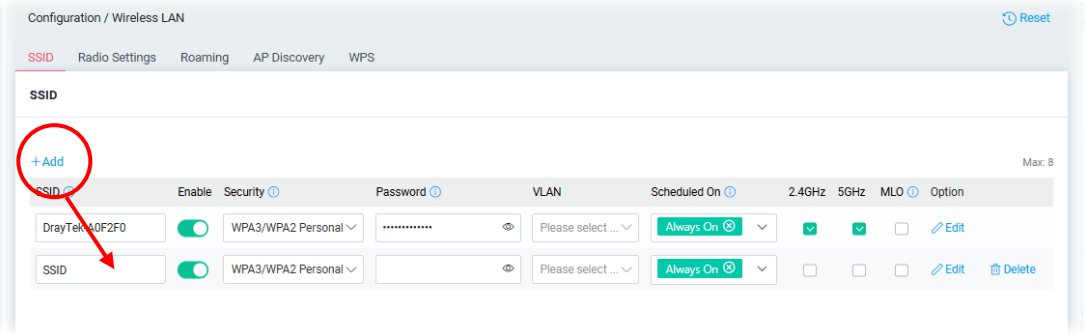
WPS（Wi-Fi 保護設定）讓無線用戶端與無線基地台和路由器的連線變得簡單。

II-1-5-1 SSID 設定

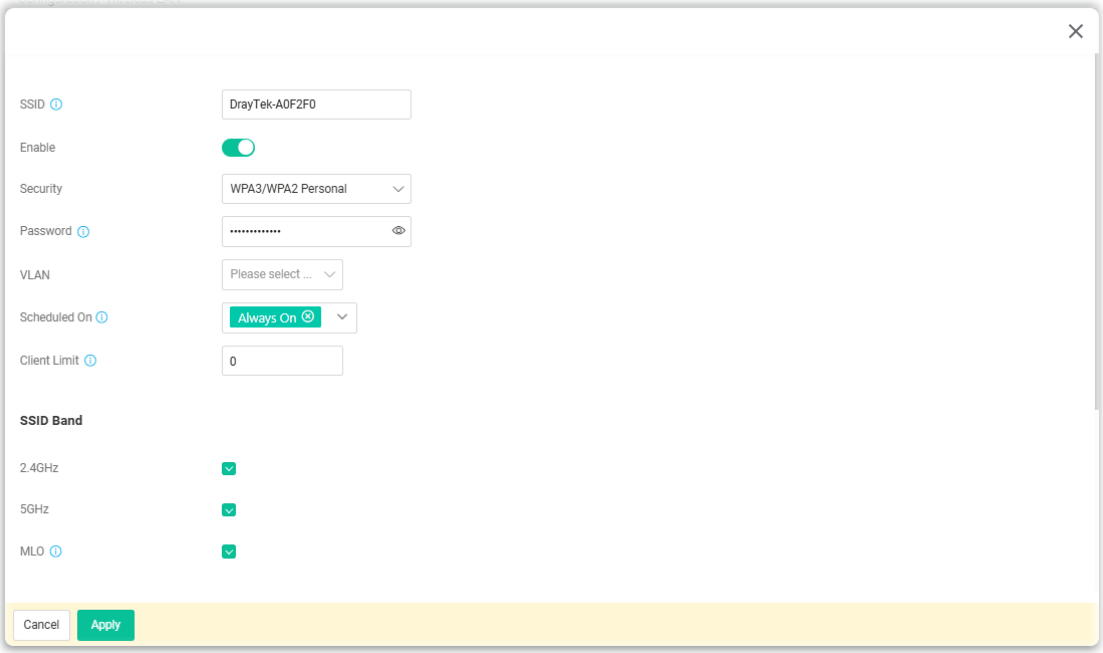
在配備 WiFi 的機型上，您可以設定 SSID 供內部使用者使用，讓他們可以存取 LAN 和 WAN (網際網路)。此頁面還可讓您設定訪客 SSID(僅限存取網際網路的無線用戶端，通常供訪客使用)，並設定 LAN VLAN。



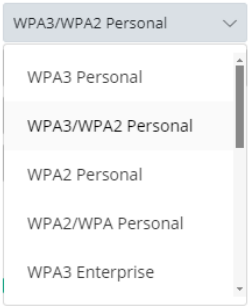
欲新增 SSID 設定檔，請按下**+新增(+Add)** 建立新的輸入框。

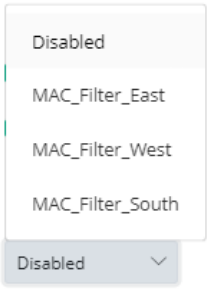


欲編輯設定檔，按下該設定檔最右邊的**編輯(Edit)**鏈結開啟如下頁面。



可用設定說明如下：

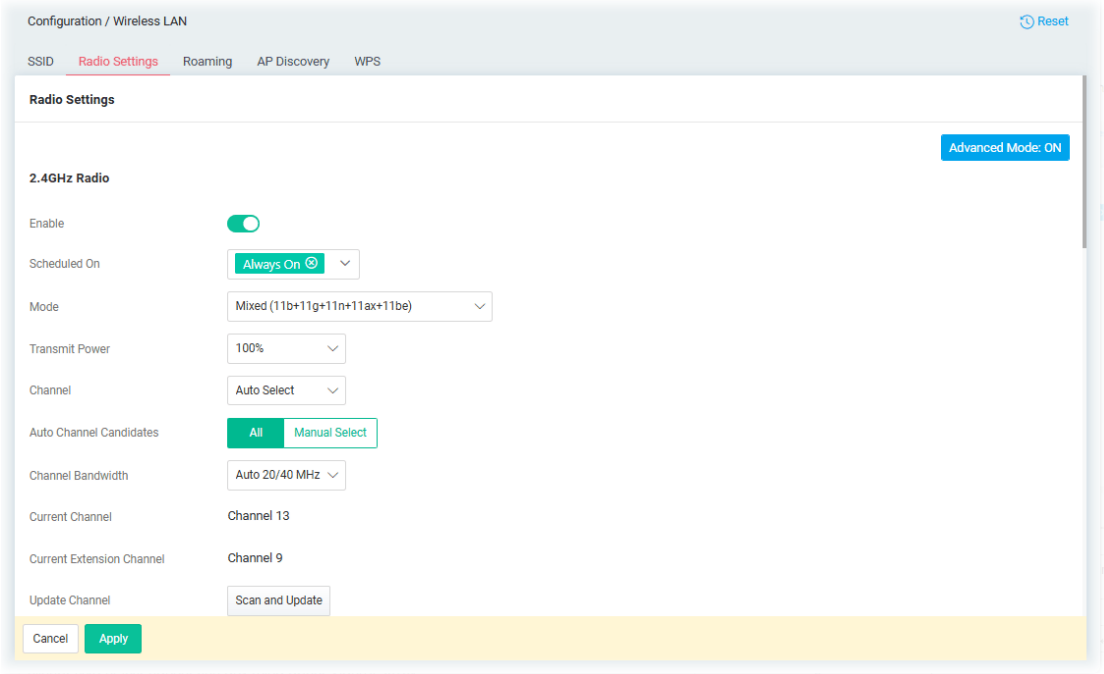
項目	說明
SSID	服務集識別碼 (SSID)，用以辨識基地台 AP 身分。最大長度為 32 個字元。 設定一個名稱，作為識別之用。
啟用(Enable)	切換開關以便啟用或停用該功能。
Security 	共有數個模式可以讓使用者選擇。 以下顯示具備高度安全性的模式; ● **WPA3 個人模式、WPA3/WPA2 個人模式、WPA2 個人模式、WPA2/WPA 個人模式(WPA3 Personal, WPA3/WPA2 Personal, WPA2 Personal, WPA2/WPA Personal)** – 僅接受 WPA 用戶端，加密金鑰應以 PSK 格式輸入。WPA 透過金鑰對無線網路發送的每個訊框進行加密，該金鑰是手動輸入到下方欄位中的密碼(Password)。 ● **WPA3 企業模式、WPA2 企業模式、WPA2/WPA 企業模式(WPA3 Enterprise, WPA2 Enterprise, WPA2/WPA Enterprise)** –僅接受 WPA 用戶端且驗證伺服器必須 在設定>>RADIUS/TACACS+>>外接 RADIUS(Configuration >> RADIUS/ TACACS+ >> External RADIUS)中設定妥當。WPA 使用金鑰對無線網路傳輸的每個訊框進行加密，該金鑰乃透過 802.1x 認證自動協商取得。 ● **OWE** – WPA3 還引入了一種新的開放且安全的連接模式：OWE。它允許客戶端無需密碼即可連接，非常適合熱點網路，但每個客戶端之間的連接在後台都經過獨特的加密來完成。 以下顯示具備基本安全性的模式; ● **WPA 個人模式(WPA Personal)** – 僅接受 WPA 用戶端，加密金鑰應以 PSK 格式輸入。WPA 透過金鑰對無線網路發送的每個訊框進行加密，該金鑰是手動輸入到下方欄位中的密碼(Password)。 ● **WPA 企業模式(WPA Enterprise)** – 僅接受 WPA 用戶端且驗證伺服器必須 在設定>>RADIUS/TACACS+>>外接 RADIUS(Configuration >> RADIUS/ TACACS+ >> External

	RADIUS)中設定妥當。WPA 使用金鑰對無線網路傳輸的每個訊框進行加密，該金鑰乃透過 802.1x 認證自動協商取得。 ● **WEP 個人模式(WEP Personal)** - 僅接受 WEP 用戶端，加密金鑰應輸入到 WEP 金鑰中。 ● **無(None)** - 關閉加密機制。
密碼(Password)	輸入 8~63 個 ASCII 字元，例如 "012345678"。此功能適用於 **WPA 個人模式(WPA Personal)** 或 **WPA2 個人模式(WPA2 Personal)** 或 **WPA2 / WPA 個人模式(WPA2 / WPA Personal)**、**WPA3 個人模式(WPA3 Personal)** 或 **WPA3/WPA2 個人模式(WPA3/WPA2 Personal)**。
RADIUS Server	此功能適用於 **WPA3 企業版(WPA3 Enterprise)**、**WPA2 企業版(WPA2 Enterprise)**、**WPA2/WPA 企業版(WPA2/WPA Enterprise)** 和 **WPA 企業版(WPA Enterprise)**模式。 使用下拉式清單選擇 RADIUS 伺服器設定。 **注意:**在設定 RADIUS 伺服器之前，請前往**設定>>RADIUS/TACACS+(Configuration>>RADIUS/TACACS+)**首先建立外部 RADIUS 設定檔 (至少一個) 。
VLAN	選擇此 SSID 歸屬的 VLAN。
排程啟用(Scheduled On)	選擇永遠或是其他的排程設定檔。 **永遠連線(Always On)** - 此 WLAN 設定檔將始終處於活動狀態。 或是，請使用下拉式清單選擇預設的排程設定檔。選擇之前，請先前往**設定>>物件(Configuration>>Object)**頁面設定幾組排程設定檔(至少要有一組)。
用戶端限制(Client Limit)	輸入透過此 SSID 連接到此裝置的用戶端數量限制(0 表示無限制) 。
SSID 頻(SSID Band)	
2.4GHz/5GHz	選擇此 SSID 需要的頻段。
MLO	Wi-Fi 7 用戶端可以同時在不同的頻段上傳送和接收資料。 啟用至少兩個主網路頻段，並將模式設定為 802.11be (在無線射頻設定頁面中) 。為此 SSID 選擇至少兩個頻段。
SSID 設定(SSID Settings)	
MAC 過濾清單(MAC Filtering List)	預設值是**停用(Disabled)**。 或是使用下拉式清單選擇預設的過濾設定檔。 選擇之前，請先前往**安全性>>MAC 過濾(Security>>MAC Filtering)**頁面建立至少一組的 MAC 過濾設定檔。 
隔離無線區域網路的用戶(Isolate Client from Wireless)	切換開關以啟用/停用此功能。 此功能可使具有相同 SSID 的無線用戶端(站點)彼此之間無法相互存取。

隱藏 SSID (Hide SSID)	切換開關以啟用/停用 SSID 顯示功能。 此功能可防止無線訊號嗅探，並使未經授權的用戶端或 STA 更難加入您的無線區域網路。依照無線工具運用的不同，使用者在現場勘測時可能只能看到除 SSID 之外的訊息，或者根本看不到任何關於 VigorAP 1062C 的訊息。該系統允許您設定四組 SSID 以因應不同的用途。
WPA 設定(WPA Settings)	
WPA 演算法(WPA Algorithm)	此功能僅適用與 WPA #相關之模式。 選擇 TKIP、AES 或 TKIP/AES 作為 WPA 的加密演算法。 請注意，並非所有 Vigor 路由器都支援 WPA3 模式。但是，如果 Vigor 路由器支援 WPA3 個人/企業安全模式，則 WPA 演算法將設定為 AES。
金鑰更新間隔(Key Renewal Interval)	此功能僅適用與 WPA #相關之模式。 使用分享密鑰作為網路驗證之用，不過，在正常的網路操作中，乃是使用隨機產生的不同加密密鑰，此隨機產生的密鑰會定期更換，請在此輸入更新間隔時間，間隔時間若較短，可獲得較高的安全性，預設值為 3600 秒，設定若是 0 則表示關閉輸入功能。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

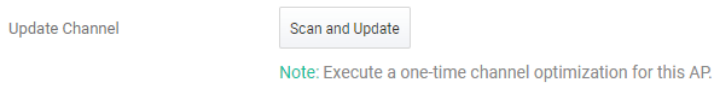
II-1-5-2 無線射頻設定(Radio Settings)

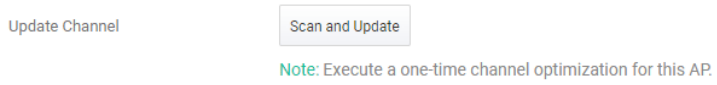
本頁面用於決定無線射頻的各項基本設定，例如模式、無線頻道及頻道頻寬等等。



可用設定說明如下：

項目	說明
進階模式:開啟/關閉 (Advanced Mode:ON/OFF)	按此顯示或隱藏無線射頻的進階設定
2.4GHz 的基本設定	
啟用(Enable)	切換開關以啟用/停用 RADIO 無線射頻設定。
排程啟用(Scheduled On)	選擇永遠連線或是其他的排程設定檔。 RADIUS 設定將根據所使用的排程設定檔(透過設定>>物件>>排程建立的設定檔) 生效進行。 預設值為**永遠連線(Always On)**。
模式(Mode)	選擇頻段上允許的 802.11 模式。 在 ax 機型的 2.4GHz 頻段上，可選擇以下無線模式： •限用 11b (11b Only) •限用 11g (11g Only) •限用 11n(2.4 GHz) (11n Only (2.4 GHz)) •綜合 (11b+11g) (Mixed (11b+11g)) •綜合 (11g+11n) (Mixed (11g+11n)) •綜合 (11b+11g+11n) (Mixed (11b+11g+11n)) •綜合 (11b+11g+11n+11ax) (Mixed (11b+11g+11n+11ax)) •綜合 (11b+11g+11n+11ax+11be) (Mixed (11b+11g+11n+11ax+11be))
傳輸功率(Transmit Power)	設定基地台發射訊號的功率百分比。 TX Power 值越大，訊號強度越高。

頻道(Channel)	允許您指定要使用的特定無線頻道，或透過選擇**自動選擇(Auto Select)**讓系統確定最佳頻道，可用頻道清單會根據路由器的目標地區而有所不同。
自動頻道候選(Auto Channel Candidates)	選擇自動選擇(Auto Select)，讓系統自動選擇最佳頻道。可用頻道清單會根據此處的設定而有所不同。 **全部 (All)** - Vigor 系統可以從所有頻道中選擇最佳頻道。 **手動選擇 (Manual Select)**– 選擇一個或多個頻道，Vigor 系統將選擇最佳頻道。
頻道頻寬(Channel Bandwidth)	**自動 20/40 MHz(Auto 20/40 MHz) –**本裝置會掃描相鄰區域的 AP 數量，使用 20 MHz(相鄰 AP 超過 10 個)或 40 MHz 作為基地台與無線用戶之間傳輸的資料速度，此選項可以增加資料傳輸的成效。 **20 MHz –** 本裝置使用 20 MHz 作為基地台與無線用戶之間傳輸的資料速度。 **40 MHz –** 本裝置使用 40 MHz 作為基地台與無線用戶之間傳輸的資料速度。
目前頻道(Current Channel)	顯示目前使用的頻道號碼。
目前擴充頻道(Current Extension Channel)	顯示目前使用的擴充頻道號碼。
更新頻道(Update Channel)	**掃描與更新(Scan and Update)** – 按一下即可再次選擇最佳頻道。
更新頻道結果(Updated Channel Result)	按下**掃描和更新(Scan and Update)**按鈕後，顯示最佳頻道。 
5GHz 射頻的基本設定	
啟用(Enable)	切換開關以啟用/停用 RADIO 無線射頻設定。
排程啟用(Scheduled On)	選擇永遠連線或是其他的排程設定檔。 RADIUS 設定將根據所使用的排程設定檔(透過設定>>物件>>排程建立的設定檔) 生效進行。 預設值為**永遠連線(Always On)**。
模式(Mode)	選擇頻段上允許的 802.11 模式。 在 ax 機型的 5GHz 頻段上，可選擇以下無線模式： •限用 11a (11a Only) •限用 11n(5 GHz) (11n Only (5GHz)) •綜合 (11a+11n) (Mixed ((11a+11n))) •綜合 (11a+11n+11ac) (Mixed (11a+11n+11ac)) •綜合 (11a+11n+11ac+11ax) (Mixed (11a+11n+11ac+11ax)) •綜合(11a+11n+11ac+11ax+11be))Mixed (11a+11n+11ac+11ax+11be))
傳輸功率(Transmit Power)	設定基地台發射訊號的功率百分比。 TX Power 值越大，訊號強度越高。
頻道(Channel)	允許您指定要使用的特定無線頻道，或透過選擇**自動選擇(Auto Select)**讓系統確定最佳頻道，可用頻道清單會根據路由器的目標地區而有所不同。
自動頻道候選(Auto Channel Candidates)	選擇自動選擇(Auto Select)，讓系統自動選擇最佳頻道。可用頻道清單會根據此處的設定而有所不同。 **全部 (All)** - Vigor 系統可以從所有頻道中選擇最佳頻道。 **排除 DFS 頻道(Exclude DFS Channels)** - Vigor 系統可以從 DFS 頻道以

	外的所有頻道中選擇最佳頻道。 **手動選擇 (Manual Select)** – 選擇一個或多個頻道，Vigor 系統將選擇最佳頻道。
頻道頻寬(Channel Bandwidth)	**20 MHz**–Vigor 路由器將使用 20 MHz 頻段在路由器和無線站點之間進行資料傳輸和接收。 **40 MHz**– Vigor 路由器將使用 40 MHz 頻段在路由器和無線站點之間進行資料傳輸和接收。 **80 MHz**–Vigor 路由器將使用 80 MHz 頻段在路由器和無線站點之間進行資料傳輸和接收。 **160 MHz**– Vigor 路由器將使用 160 MHz 頻段在路由器和無線站點之間進行資料傳輸和接收。
目前頻道(Current Channel)	顯示目前使用的頻道號碼。
更新頻道(Update Channel)	**掃描與更新(Scan and Update)** – 按一下即可再次選擇最佳頻道(**頻道**設定選擇自動選擇)。
更新頻道結果(Updated Channel Result)	按下**掃描和更新(Scan and Update)**按鈕後，顯示最佳頻道。 
頻段引導設定(Band Steering Settings)	
5Ghz 用戶端最小 RSSI (5Ghz Client Minimum RSSI)	如果啟用此功能，VigorAP 將在限定的時間內偵測無線用戶端是否支援雙頻。 此無線站點具備 5GHz 網路連線能力，但訊號效能可能不理想。因此，當無線站點連接到 VigorAP 時，如果訊號強度低於此處設定的值，VigorAP 將允許用戶端連接到 2.4GHz 網路。
進階模式下的選項	
TX/RX 串流(TX/RX Stream)	Vigor 路由器可以連接兩根天線以獲得良好的無線資料傳輸。但是，如果您只連接了一個天線，請選擇 1T1R 型號。
片段長度(Fragment Length)	設定無線射頻的片段門檻值。預設值為 2346。如果您不知道效果為何，請勿修改預設值。
RTS 門檻值(RTS Threshold)	縮減隱藏站點之間的衝突(單位為位元組)，以提高無線效能。 設定無線射頻的 RTS 門檻值。預設值為 2347。如果您不知道效果為何，請勿修改。
國家代碼(Country Code)	僅適用 2.4GHz。 VigorAP 遵循 802.11d 標準廣播國家/地區代碼。但部分無線站點會偵測/掃描國家代碼以避免衝突發生。如果偵測到了衝突，無線站點將收到警告，並且無法建立網路連線。因此，變更改國家/地區代碼以確保網路連線成功，對某些用戶來說就很有必要。
支援 WMM (WMM Capable)	WMM 為 Wi-Fi Multimedia 的縮寫，定義從 802.11e 衍生的四種存取類型錄的優先層級，這些類型都是針對流量、聲音、影像特別設計的，此四種類型分別是 - AC_VO, AC_VI, AC_BE 與 AC_BK。 在無線資料傳輸中應用 WMM 參數，切換此開關以啟用/停用此功能。
支援 APSD (APSD Capable)	自動省電模式(APSD, automatic power-save delivery)是 Wi-Fi 網路支援的強化省電機制，允許裝置花較多時間休眠，並透過縮小傳輸延遲時間，花費少許電力來改善成效。

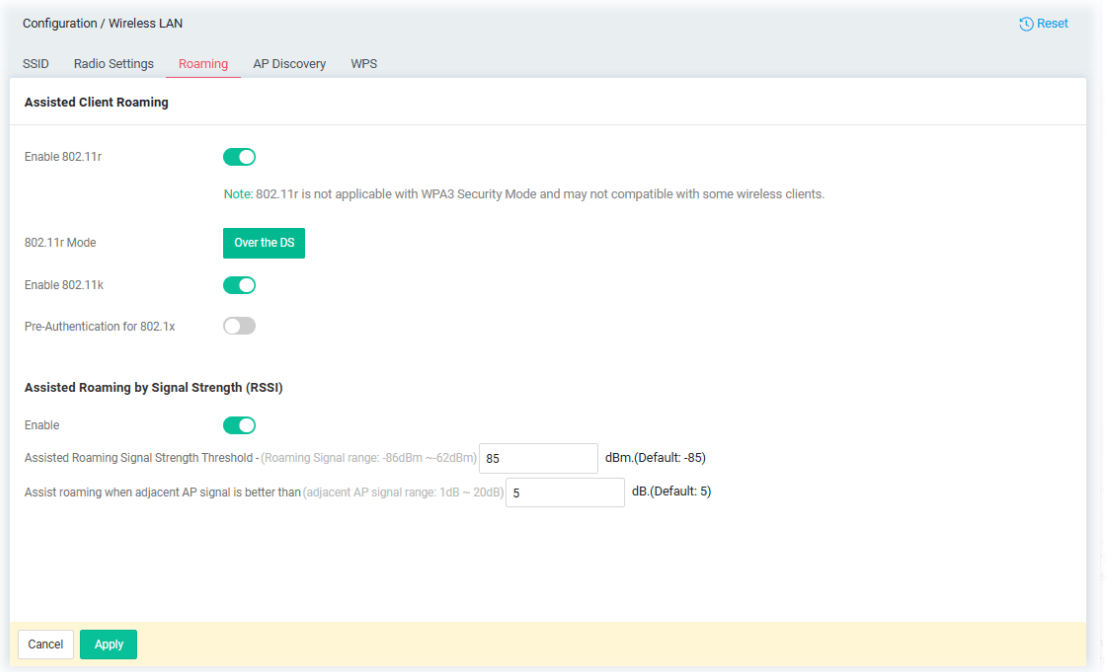
無線頻寬均化(Airtime Fairness)	切換此開關以啟用/停用此功能。 在服務品質層級一定的條件下，每個用戶端都享有同等的網路空中流通時間。因此在特定的環境中，此功能可以降低慢速無線裝置的不良影響，且可改善全面無線網路的成效。 適合環境： (1) 多個無線用戶 (2) 所有的無線用戶主要都是進行下載作業 (3) 成效的瓶頸主要在無線連線上
取消(Cancel)	捨棄目前設定。
套用(Apply)	儲存目前設定。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-1-5-3 漫遊(Roaming)

單一無線存取裝置的網路訊號往往受限於訊號的涵蓋範圍。因此，如果您想要在一個大型展場上延伸並擴充無線網路的覆蓋範圍，您可以安裝數台無線存取裝置於展場上，同時啟用每台裝置的漫遊功能，如此一來，就可以達成無縫連接無線網路，從而擴充無線訊號範圍。

本頁面允許您啟用並設定無線漫遊功能。



可用設定說明如下：

項目	說明
	輔助用戶端漫遊(Assisted Client Roaming)
啟用 802.11r(Enable 802.11r)	切換此開關以啟用/停用 802.11r 協定快速漫遊功能，讓無線用戶端在熱點之間能快速與安全地切換。
802.11r 模式(802.11r Mode)	**透過 DS (Over the DS)** - 因應訊號強度的變更，用戶端可以利用 Action Frames (FT 需求與 FT 回應) 透過原本的 AP 與其他的 AP 進行通訊。 **透過 OTA(Over The Air)** - 因應訊號強度的變更，用戶端可以利用漫遊驗

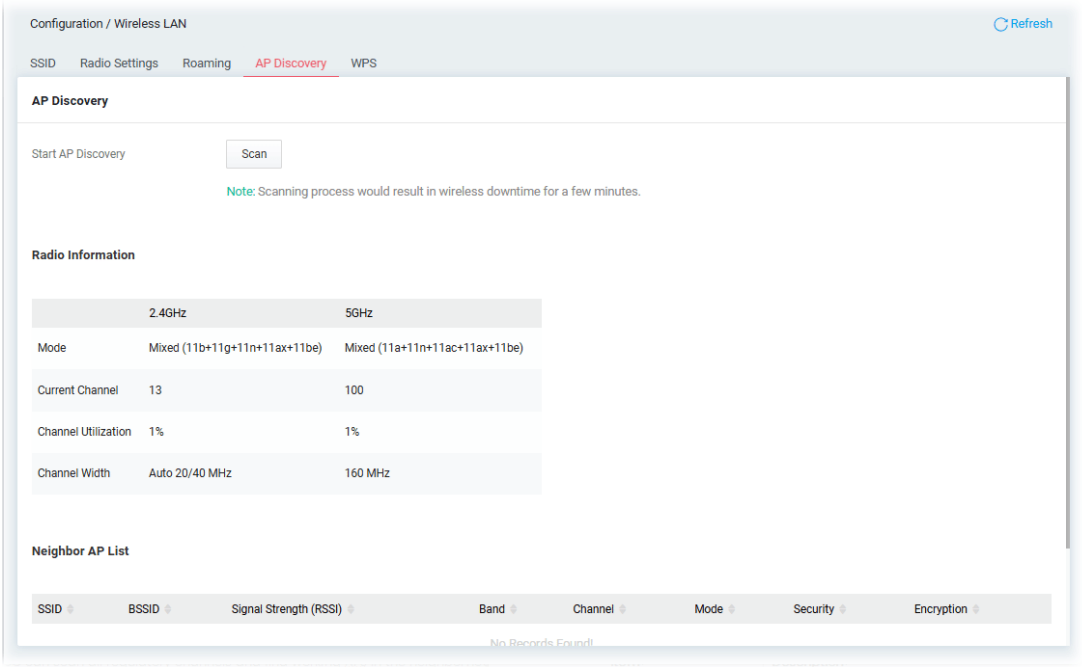
	證演算式直接與其他的 AP 通訊(無須在每一個 AP 中不斷的重新驗證)。 請注意雙邊的 AP 必須能夠透過 DS/WDS 彼此互相 ping 到對方。
啟用 802.11k (Enable 802.11k)	切換此開關以啟用/停用 802.11k 通訊協定(又名為無線資源管理（Radio Resource Management, RRM）啟用時，基地台/路由器會優化無線網路的效能。
802.1x 的預先身份驗證 (Pre-Authentication for 802.1x)	使網站能夠向多個存取點進行身份驗證，從而實現更安全、更快速的漫遊。透過 IEEE 802.11i 規範中定義的預認證流程，預先進行四向交握可縮短行動節點所感受到的切換延遲，使漫遊更快、更安全（僅在 WPA2 下有效）。 切換此開關以啟用/停用 802.11x 的預先身份驗證。 **啟用(Enable)** – 啟用 IEEE 802.11x 的預先身份驗證。 **停用(Disable)** – 停用 IEEE 802.11x 的預先身份驗證。 **暫存期間(Cache Period) -** 設定 WPA2 PMK（成對主金鑰）快取的過期時間。PMK 快取管理著已預先驗證過的關聯 SSID 中的 BSSID 清單。此功能適用於 WPA2 企業版模式。
利用訊號強度(RSSI)輔助漫遊(Assisted Roaming by Signal Strength (RSSI))	
啟用(Enable)	切換此開關以啟用/停用此功能。 當無線用戶端的連接速率過低，或無線用戶端接收到的訊號過差時，Vigor 路由器將會自動偵測(基於連接速率和 RSSI 要求)，並切斷該無線用戶端的網路連接，以幫助其連接到另一個無線基地台取得更好的訊號。
輔助漫遊訊號強度門檻值 (Assisted Roaming Signal Strength Threshold)	當無線用戶端的訊號強度低於此處設定的值(dBm)，且 Vigor 路由器偵測到相鄰 AP (必須是 DrayTek 路由器/AP，且也支援此功能)的訊號強度較高(該值在**輔助漫遊，當相鄰 AP 基地台訊號優於此門檻值時(Assist roaming when adjacent AP signal is better than)**欄位中定義)，Vigor 路由器將會中斷該無線用戶端的網路連線。之後，該無線用戶端可以連接到相鄰的 AP(具有更好的 RSSI 訊號強度)。
輔助漫遊，當相鄰 AP 基地台訊號優於此門檻值時 (Assist roaming when adjacent AP signal is better than)	指定一個數值作為門檻值。
取消(Cancel)	捨棄目前設定。
套用(Apply)	儲存目前設定。

完成設定之後，按下**套用(Apply)**按鈕儲存相關設定。

II-1-5-4 搜尋無線基地台(AP Discovery)

Vigor 路由器可以掃描所有受監管的頻道，並尋找附近可用的基地台（AP）依照掃描結果，使用者可以知道哪個頻道可以安全使用。此外，它還可以用於尋找 WDS 鏈結所需的基地台。請注意，在掃描過程中（約 5 秒），任何用戶端都無法連接到此 Vigor 路由器。

此頁面用於掃描周圍是否存在無線基地台。請按下**掃描(Scan)**尋找附近所有基地台。



可用設定說明如下：

項目	說明
開始搜尋無線基地台 (Start AP Discovery)	**掃描(Scan)** - 可用於搜尋附近所有基地台。結果將顯示在此按鈕下方的方塊中。
無線射頻資訊(Radio Information)	顯示 Vigor 路由器目前使用的 2.4GHz 和 5GHz 頻段資訊。
芳鄰 AP 清單(Neighbor AP List)	顯示 Vigor 路由器掃描到的所有附近 AP。

II-1-5-5 WPS 設定

Wi-Fi 保護設定(WPS, Wi-Fi Protected Setup) 提供了一種簡單的方法，可以將無線裝置連接到採用 WPA 或 WPA2 加密的無線基地台和路由器。

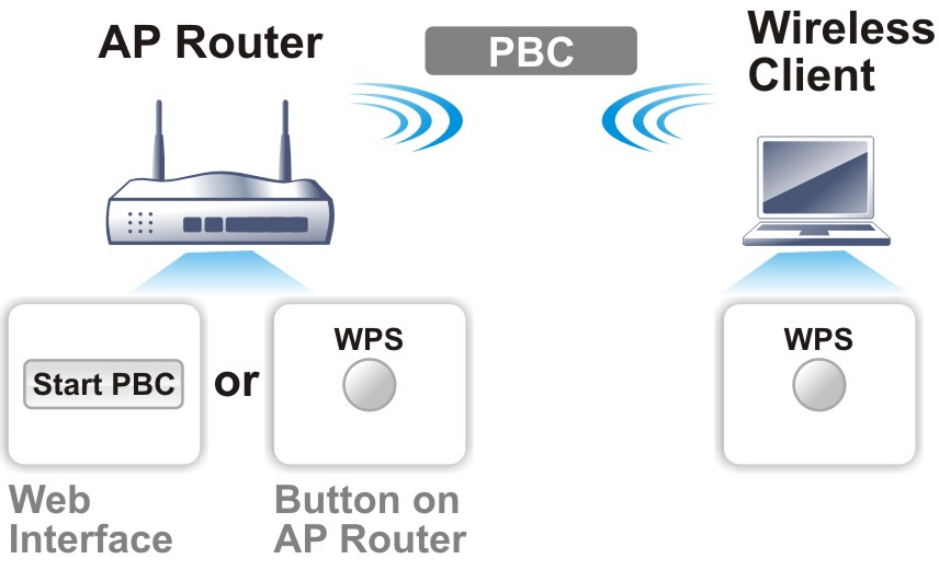
WPS 可與支援 WPA 或 WPA2 的無線網路搭配使用，但不支援 WEP。

這是在無線網路用戶端和 Vigor 路由器之間建立連線的最簡單方法。使用者無需每次都選擇加密模式或輸入冗長的加密密碼來設定無線用戶端。只需按下無線用戶端上的一個按鈕，WPS 即可自動連接用戶端和路由器。

透過 WPS 在 AP 和 Station 之間建立網路連線有兩種方法：按下***啟動 PBC(Start PBC)*** 按鈕或使用 ***PIN 碼 (PIN Code)***。

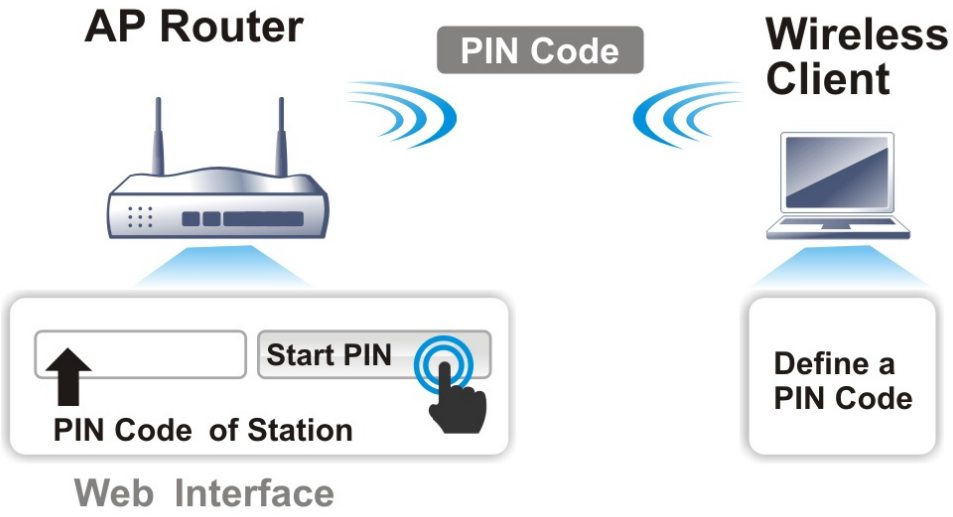
使用 PBC 按鈕

在 Vigor 路由器上，按住前面板上的 WPS 按鈕 2 秒鐘，或按一下在 Web 使用者介面中的**設定>>無線區域網路>>WPS(Configuration>>Wireless LAN>>WPS)** 的**啟動 PBC** 按鈕。在無線終端(例如筆記電腦)上，按下 **WPS/Start PBC** 網路卡上的按鈕。

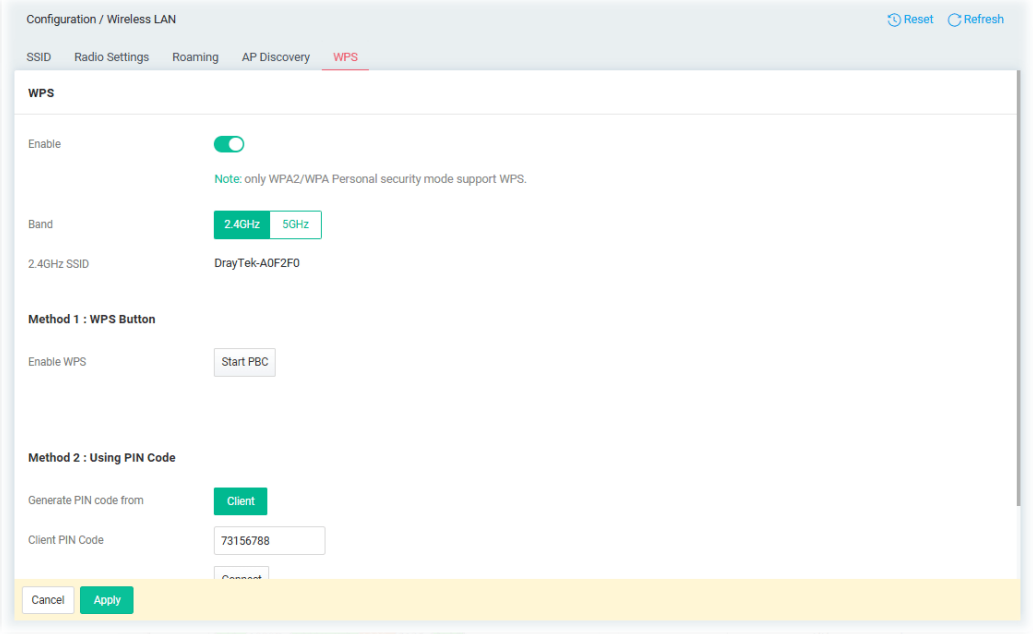


使用 PIN 碼

您可以透過輸入由支援 WPS 的無線用戶端產生的 PIN 碼來建立無線連線。



下圖為**設定>>無線區域網路>>WPS(Configuration>>Wireless LAN>>WPS)**設定頁面：



可用設定說明如下：

項目	說明
重置(Reset)	按此將 WPS 重置為預設值。
頁面更新(Refresh)	按此重新更新此頁面。
啟用(Enable)	切換此開關即可啟用/停用此功能。
頻段(Band)	選擇此功能的頻段(2.4GHz/5GHz)。
2.4GHz SSID / 5GHz SSID	顯示 2.4GHz/5GHz 頻段所使用的 SSID。
方式 1：WPS 按鈕 (Method 1: WPS Button)	**啟用 WPS(Enable WPS)** – 切換此開關以啟用/停用此功能。 **啟動 PBC(Start PBC)** – 按下此按鈕即可啟動按鍵式 WPS 設定程式。路由器將等待約 2 分鐘，以接收來自無線用戶端的 WPS 連線請求。WPS 設定過程中，路由器上的 ACT 指示燈和 WLAN 指示燈將同時快速閃爍，兩分鐘後恢復正常狀態。
方式 2：使用 PIN 碼 (Method 2: Using PIN Code)	輸入 PIN 碼，然後按下**連接(Connect)**按鈕。 **PIN 碼產生來自於(Generate PIN code from)** – 目前可用的選項僅有 Client。 **用戶端 PIN 碼(Client PIN Code)** – 輸入 PIN 碼。 **連線(Connect)** – 按此即可建立連線。WPS 連線進行時，路由器上的 ACT 指示燈和 WLAN 指示燈將同時快速閃爍，持續最多 2 分鐘，或直到無線用戶端成功建立 WPS 連線為止。
連線狀態(Connection Status)	顯示連線狀態**連線(Connect)**或者**啟動 PBC(Start PBC)**。
取消(Cancel)	捨棄目前設定。
套用(Apply)	儲存目前設定。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-1-6 路由(Routing)

透過 IP 位址和介面設定，可以使用路由策略來設定任何路由規則以適應實際需求。

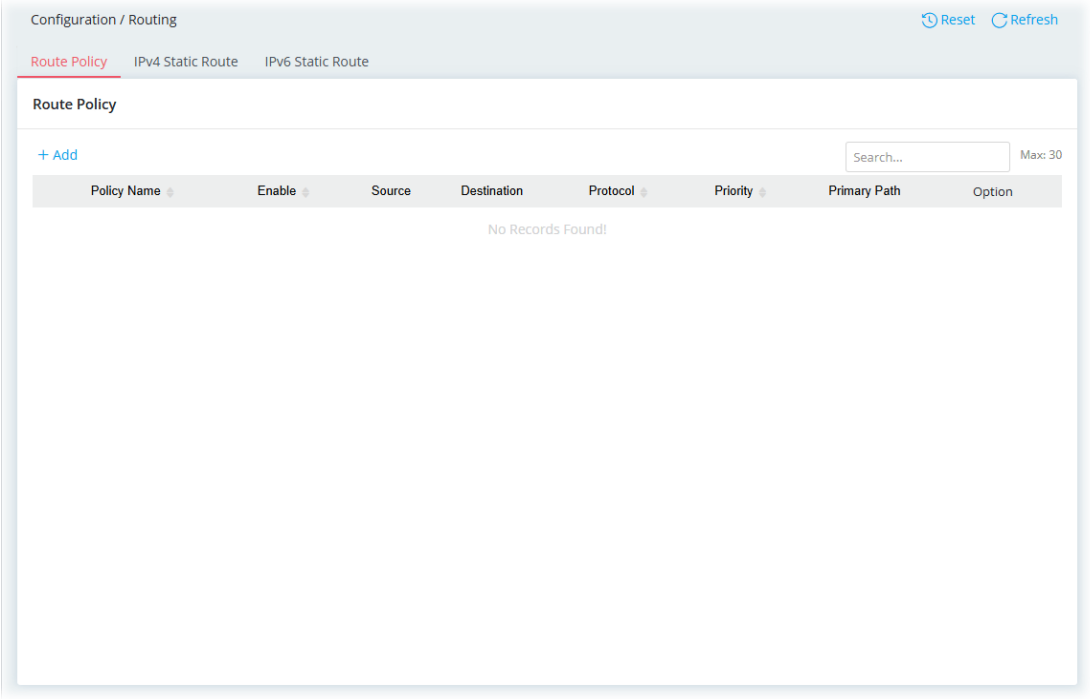
如果封包符合路由策略，則會被導引到指定的介面。

路由器提供 IPv4 和 IPv6 協定，供您設定靜態路由。這兩種協定指向不同的網頁。

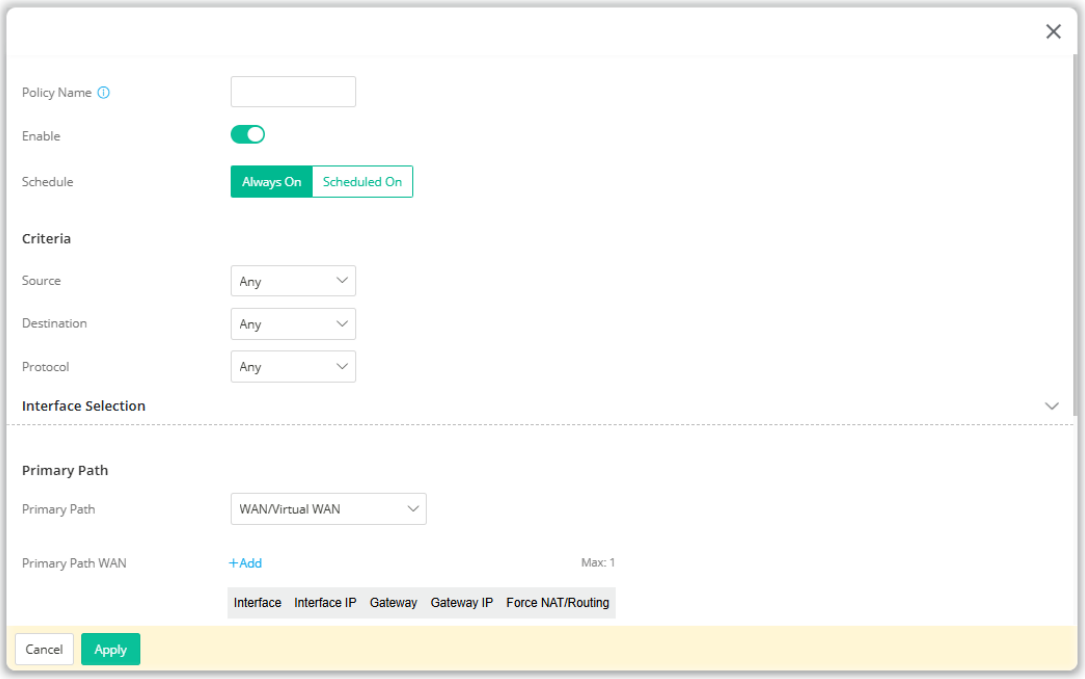
II-1-6-1 路由策略(Route Policy)

路由策略(也稱為基於策略的路由，簡稱 PBR)是一種需要設定路由策略的功能。如果封包符合某個策略，則會被導引到指定的介面。您可以出於各種原因設定路由策略，例如負載平衡、安全性、路由決策等等。

透過協定、IP 位址、連接埠號碼和介面設定，路由策略可以用來設定任何路由規則以適應實際需求。

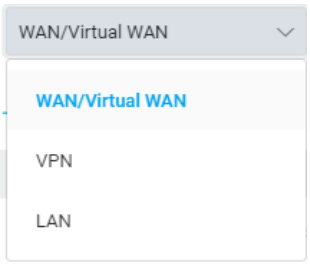


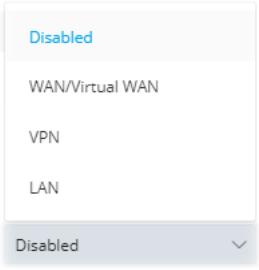
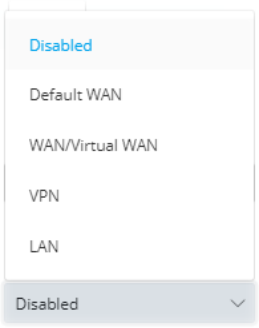
欲新增 IPv4 路由策略，請按一下**+新增(+Add)**鏈結即可開啟如下頁面。



可用設定說明如下：

項目	說明
策略名稱(Policy Name)	輸入路由設定檔名稱，以供識別。
啟用(Enable)	切換開關已啟用/停用此設定檔。
排程(Schedule)	制定路由設定檔的有效期間。 **永遠連線(Always On)** – 如果啟用，路由設定檔將始終運作有效。 **排程啟用(Scheduled On)** - 依照選定的排程檔案啟動路由設定檔。
標準(Criteria)	
來源/目的(Source / Destination)	選擇要套用此規則的 IP 位址類型。 ● **任一(Any)** - 此策略適用於所有來源/目的 IP 位址。 ● **IPv4 位址(IPv4 Address)** - 此策略適用於指定的來源 IP 位址範圍。 ● **IPv4 子網(IPv4 Subnet)** – 此策略適用於由指定的網路 IP 位址和子網路遮罩定義的來源 IP 位址。 ● **IP 物件(IP Object)** - 此策略適用於預先設定的 IP 物件。 ● **IP 群組(IP Group)** - 此策略適用於預先設定的 IP 群組。
來源/目的 IPv4 位址 (Source / Destination IPv4 Address)	當**來源/目地**設定為 **IPv4 位址**時，可使用此設定： **+新增(+Add)** –按此建立新條目。 **IPv4 位址起始/結束(IPv4 Address Start / End)** – 輸入兩組 IPv4 位址，一個當成起始位址，另一個當成結束位址。 **刪除(Delete)** – 按此移除目前條目。
來源/目的 IPv4 子網位址 (Source / Destination IPv4 Subnet Address)	當**來源/目地**設定為 **IPv4 子網位址**時，可使用此設定： **+新增(+Add)** – 按此建立新條目。 **IPv4 位址(IPv4 Address)** – 輸入 IP 位址。 **子網遮罩(Subnet Mask)** - 使用下拉式清單選擇適合的遮罩值。
來源/目的 IP 物件(Source / Destination IP Object)	當**來源/目地**設定為 **IP 物件**時，可使用此設定： **+新增(+Add)** – 按此新增物件(包含不同的 IP 位址)，最多可建立 12 個物件。

	選擇物件(Select Object) – 勾選後選擇一個物件或數個物件。
來源/目的 IP 群組(Source / Destination IP Group)	當**來源/目地**設定為 **IP 群組**時，可使用此設定： **+新增(+Add)** –按此新增群組(包含不同的 IP 物件)，最多可建立 12 個群組。 **選擇群組(Select Group)** - 勾選後選擇一個群組或數個群組。
通訊協定(Protocol)	為廣域網路 WAN 介面選擇合適的通訊協定。 **任一(Any)** – WAN 介面可以使用任何類型的通訊協定。 **服務物件(Service Object)** – 所使用的協定將由服務物件決定。 • **服務類型物件(Service Type Object)** – 按下+新增(+Add)建立一個新物件(包含不同的通訊協定)。最多可以建立 12 個物件。 **TCP/UDP** – 為 WAN 介面選擇 TCP/UDP。 • **指定來源埠號(Specify Source Port)** – 切換開關以啟用來源埠號設定。 • **來源埠號/目的埠號(Source Port / Destination Port)** – 設定範圍(1 到 65535)。 **TCP** – 與 TCP/UDP 相同。 **UDP** – 與 TCP/UDP 相同。 **ICMP** – 選擇 ICMP 作為 WAN 介面。
	介面選項(Interface Selection)
主要路徑(Primary Path)	指定此規則所描述的流量要導引前往的介面。 如果封包流量符合上述設定的標準，則會將其傳送到指定的介面和閘道。 **主要路徑(Primary Path)** – 資料封包將傳輸到此處選擇的介面。請從清單中選擇一個介面（WAN/LAN：廣域網路或區域網路介面；VPN：虛擬私人網路）。  **主要路徑 WAN (Primary Path WAN)** – 當選擇 WAN/虛擬 WAN 時，此功能可用。 **+新增(+Add)** – 按下**+新增(+Add)**建立主路徑。選擇 WAN 介面及其對應的 IP 位址。符合條件的封包將被轉送到此處選擇的介面。從清單中選擇一個介面。指定閘道(使用預設裝置或自訂閘道 IP)。然後確定路由器將使用哪種機制（強迫使用 NAT/路由）將封包轉送到 WAN。 **主要路徑 WAN (Primary Path WAN)** - 選擇 VPN 後即可使用。 **+新增(+Add)** – 按下**+新增(+Add)**建立新的 VPN 路徑。使用下拉清單選擇 VPN 設定檔。 **主要路徑 WAN (Primary Path WAN)** - 選擇區域網路 LAN 時可用。 **+新增(+Add)** – 按下**+新增(+Add)**建立新的 VPN 路徑。使用下拉清單選擇 VPN 設定檔。
次要路徑(Secondary Path)	**停用(Disabled)** – 停用次要路徑的功能設定。

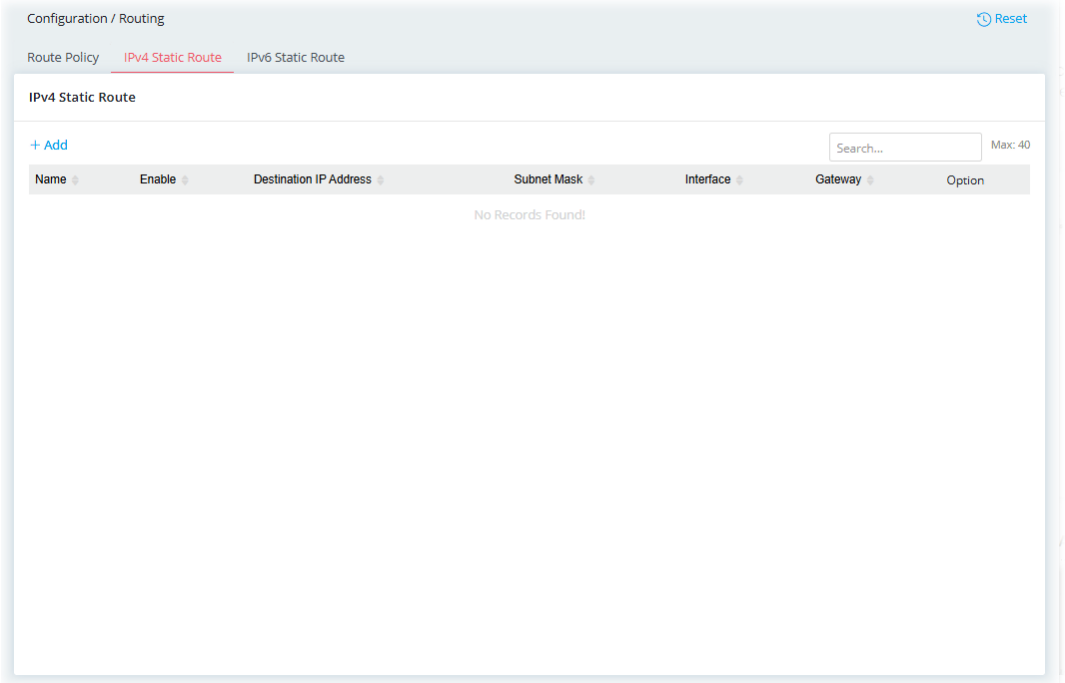
	 **次要路徑 WAN (Secondary Path WAN)** – 當 WAN/虛擬 WAN 設定為次要路徑時，此功能可用。 **+新增(+Add)** –按下**+新增(+Add)**透過指定 WAN 設定來建立次要路徑。 **次要路徑 LAN (Secondary Path LAN)** – 當 VPN 設定為次要路徑時，此功能可用。 **+新增(+Add)** –按下**+新增(+Add)**建立新的 VPN 路徑 **次要路徑 LAN (Secondary Path LAN)** – 當 LAN 設定為次要路徑時，此功能可用。 **+新增(+Add)** –按下**+新增(+Add)**建立新的 LAN 路徑。
最終採取路徑(Last Resort Path)	如果主要路徑或次要路徑無法用於引導流量，系統會採取最後的替代路徑（設定）。 **停用(Disabled)** – 停用**最終採取路徑**的功能設定。  任何符合上述標準(Criteria)中規定的規則（來源/目的/通訊協定）的資料封包，都會轉送到最終採取路徑上定義的介面。 **預設 WAN(Default WAN)** – 預設 WAN 介面將用作最後的採取路徑。 • **閘道器(Gateway)** – 選擇預設值(Default)或自訂(Customize)。 • **閘道器 IP 位址(Gateway IP Address)** – 如果選擇自訂，請輸入閘道的 IP 位址。 • **強迫使用 NAT/路由(Force NAT/Routing)** – 決定路由器將使用哪種機制（強迫使用 NAT/路由）將封包轉送到 WAN。 **WAN/虛擬 WAN(WAN/Virtual WAN)** – 為最後的採取路徑指定一個 WAN 介面或虛擬 WAN 介面。 • **最終採取路徑 WAN (Last Resort Path WAN)** – 按下+新增(+Add)。然後選擇 WAN 介面、IP 位址（WAN）、閘道 IP 位址（LAN）和封包轉發機制。 **VPN** – 為最後的採取路徑指定一個 VPN 設定檔。 • **最終採取路徑 VPN (Last Resort Path VPN)** – 按下+新增(+Add)。選擇一個 VPN 設定。 **LAN** – 為最後的採取路徑指定一個 LAN 介面。 • **最終採取路徑 LAN (Last Resort Path LAN)** – 按下+新增(+Add)然後選擇具有 IP 位址（閘道）和封包轉送機制的 LAN 介面。
更多設定	

啟用 Syslog (Enable Syslog)	切換開關以啟用/停用將相應日誌儲存到系統日誌的功能。
優先權(Priority)	指定該規則相對於其他規則的優先順序。 **正常模式(Normal)** – 此路由設定檔不會影響路由表中的其他路由。 **高(High)** – 此路由設定檔只會覆寫 VPN 路由，不會影響 LAN/靜態路由。 **頂(Top)** – 路由設定檔將覆蓋 VPN 和 LAN/靜態路由。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

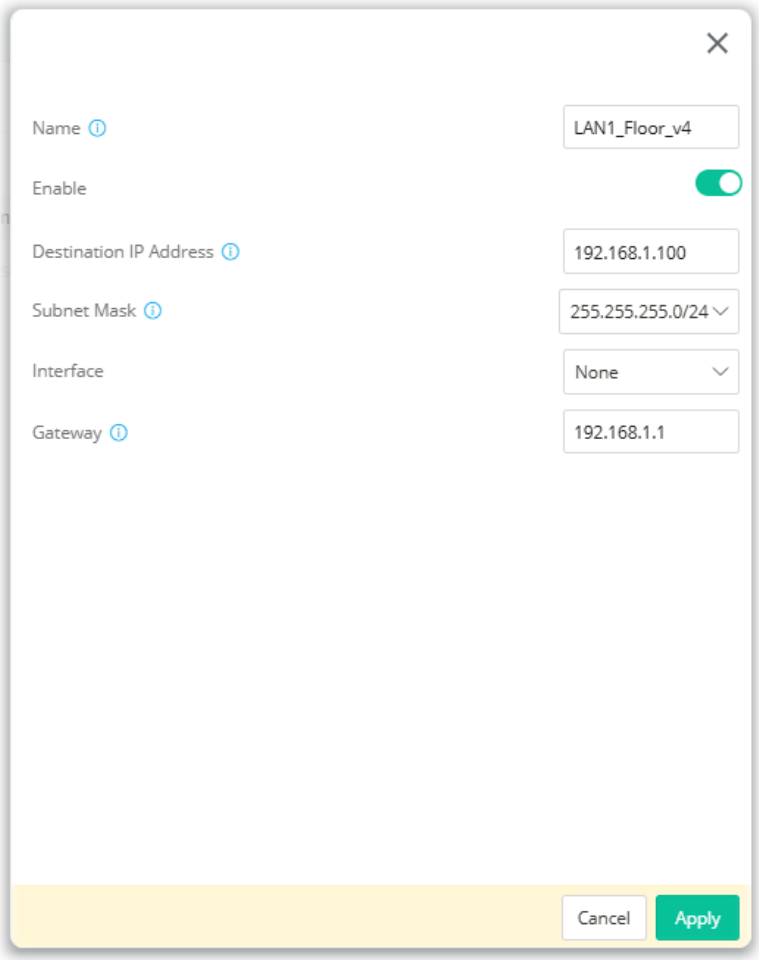
完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-1-6-2 IPv4 固定路由(IPv4 Static Route)

固定路由是動態路由的替代方案。它是指系統網路管理員設定網路路由器，使其具備資料封包轉送所需的所有資訊的過程。



欲新增 IPv4 路由策略，請按一下**+新增(+Add)**鏈結即可開啟如下頁面。



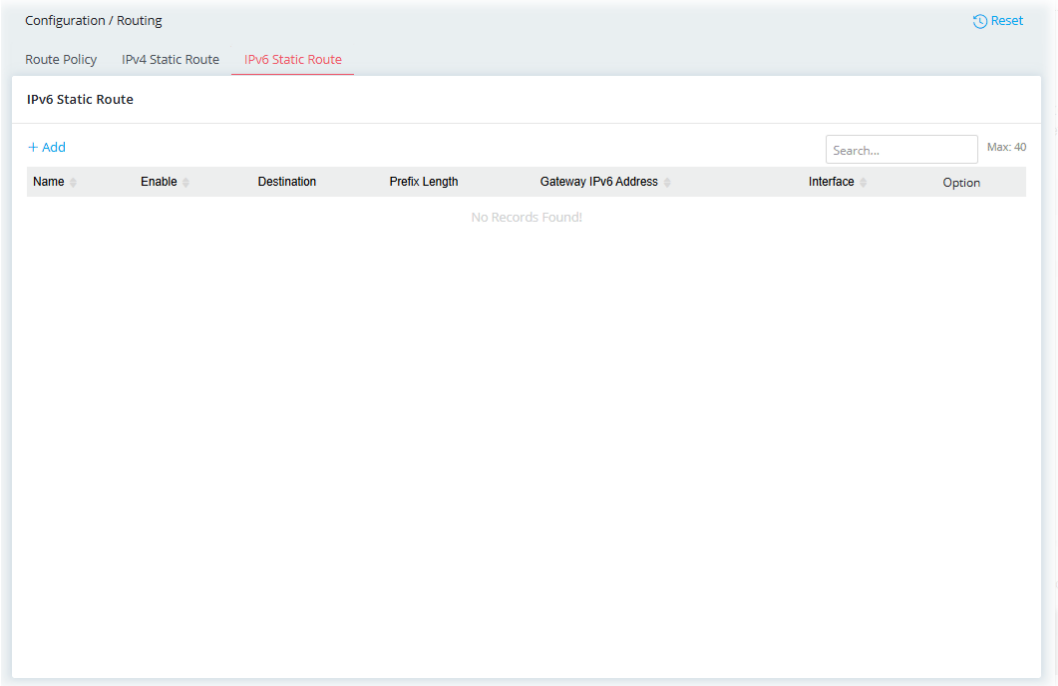
可用設定說明如下：

項目	說明
名稱(Name)	輸入字串作為名稱，以供識別。
啟用(Enable)	切換開關即可啟用或停用此功能。
目的 IP 位址(Destination IP Address)	輸入目的 IP 位址。
子網遮罩(Subnet Mask)	為該固定路由選擇一個子網路遮罩。
介面(Interface)	使用下拉清單為此固定路由指定介面。
閘道(Gateway)	輸入 IP 位址作為閘道。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

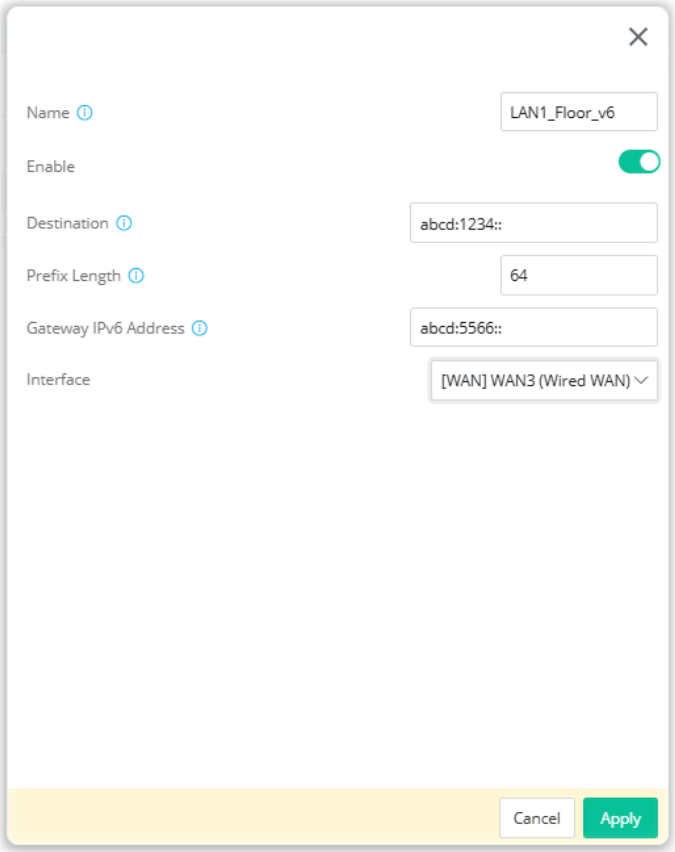
完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-1-6-3 IPv6 固定路由(IPv6 Static Route)

固定路由是動態路由的替代方案。它是指系統網路管理員設定網路路由器，使其具備資料封包轉送所需的所有資訊的過程。



欲新增 IPv6 路由策略，請按一下**+新增(+Add)**鏈結即可開啟如下頁面。



可用設定說明如下：

項目	說明
名稱(Name)	輸入字串作為設定檔名稱，以供識別。

啟用(Enable)	切換開關即可啟用或停用此功能。
目的(Destination)	輸入 IPv6 位址作為目的 IP 位址。
前置碼長度(Prefix Length)	輸入前置碼長度的固定值。
閘道 IPv6 位址(Gateway IPv6 Address)	輸入 IPv6 位址作為閘道。
介面(Interface)	使用下拉清單為此固定路由指定介面。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

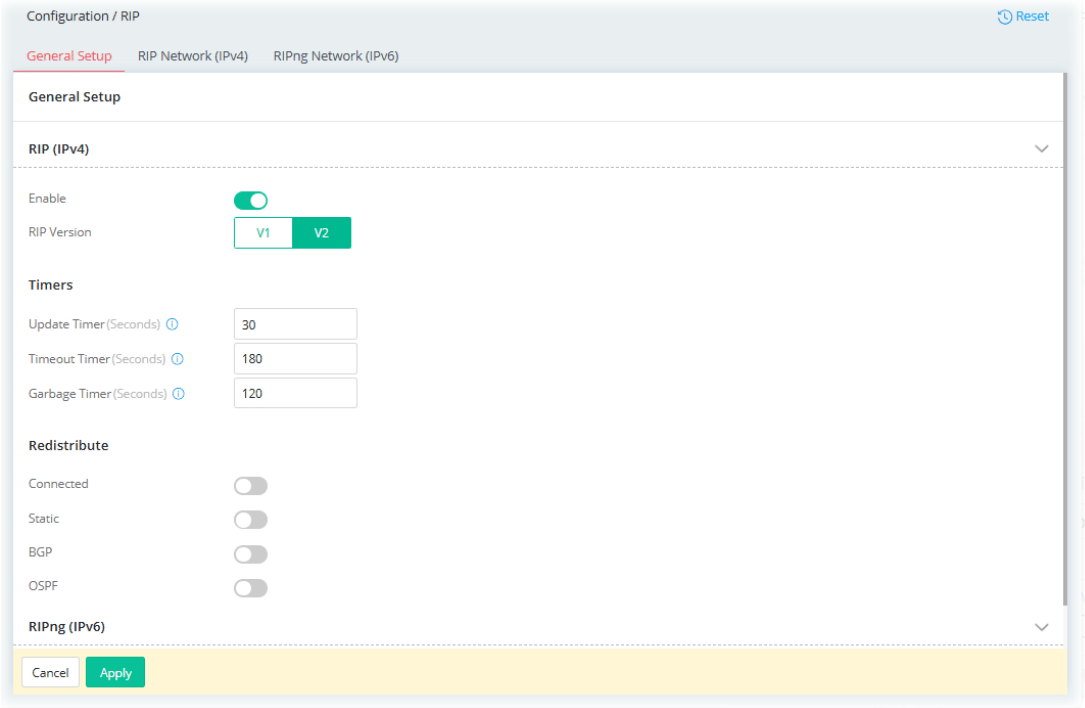
II-1-7 RIP 設定

路由資訊協定 (RIP) 和 RIPng (下一代 RIP) 是最受歡迎的內部路由協定。差別在於，RIPng (下一代 RIP) 是以 IPv6 位址為主，但提供的功能和優勢與 IPv4 RIP v2 相同。

如果啟用 RIP 功能，路由器將嘗試使用路由資訊協定與相鄰路由器交換路由資訊。

II-1-7-1 基本設定(General Setup)

RIP 有兩個版本可供選擇。本頁面提供了這兩個版本的詳細資訊設定。



可用設定說明如下：

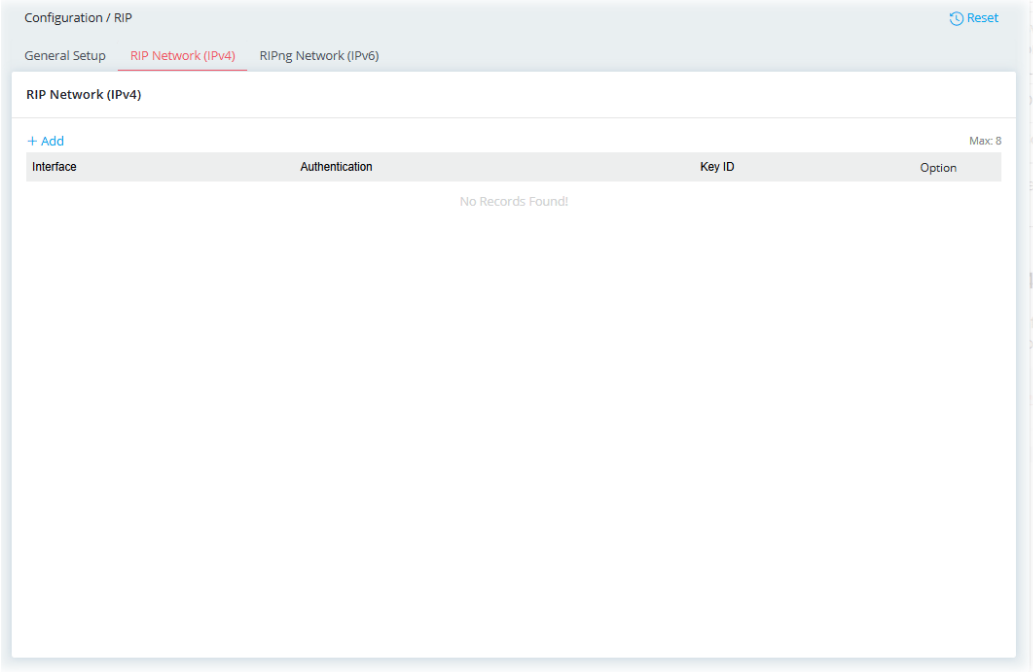
項目	**說明**

基本設定(General Setup)	
啟用(Enable)	啟用後，路由器將嘗試使用路由資訊協定與相鄰路由器交換路由資訊。
RIP 版本(RIP Version)	指定 RIP 協定的版本號（V1/V2）。
更新計時器 (Update Timer)	輸入更新計時器的設定值。 時間到後，Vigor 路由器會將包含完整路由表的訊息傳送給所有相鄰路由器，以便交換路由資訊。
逾時計時器 (Timeout Timer)	路由資訊將在該欄位中設定的逾時時間內有效（但不會被刪除）。 該資訊將暫時保留在路由表中。同時，鄰居伺服器將收到路由已失效的通知。
垃圾計時器 (Garbage Timer)	當垃圾定時器設定的過期時間到來時，該路由將從路由表中刪除。
已連線(Connected)	切換開關以啟用或停用該功能。 **全部的網路(All Networks)** – 將 RIP 設定檔套用到所有 LAN 介面。 **排除 NAT 網路(Exclude NAT Networks)** - 將 RIP 設定檔套用至 NAT 網路以外的所有 LAN 介面。
靜態(Static)	切換開關以啟用或停用該功能(將靜態路由套用到 RIP 設定檔)。
BGP	切換開關以啟用或停用該功能(允許依照從 BGP 協定中學習到的資訊動態地進行路由流量)。
OSPF	切換開關以啟用或停用該功能(允許依照從 OSPF 協定中學習到的資訊動態地進行路由流量)。
RIPng(Ipv6)	
啟用(Enable)	切換開關以啟用/停用下一代路由資訊協定 (RIPng) 功能。
更新計時器 (Update Timer)	輸入更新計時器的設定值。 時間到後，Vigor 路由器會將包含完整路由表的訊息傳送給所有相鄰路由器，以便交換路由資訊。
逾時計時器 (Timeout Timer)	路由資訊將在該欄位中設定的逾時時間內有效（但不會被刪除）。 該資訊將暫時保留在路由表中。同時，鄰居伺服器將收到路由已失效的通知。
垃圾計時器 (Garbage Timer)	當垃圾回收定時器設定的過期時間到來時，該路由將從路由表中刪除。
已連線(Connected)	切換開關以啟用(將 RIPng 設定套用至所有 LAN 介面)或停用此功能。
靜態(Static)	切換開關以啟用(將靜態路由套用至 RIP 設定檔)或停用該功能。
BGP	切換開關以啟用(允許依照從 BGP 協定學習到的資訊動態地進行流量路由。)或停用該功能。
OSPF	切換開關以啟用(允許依照從 OSPF 協定學習到的資訊動態地進行流量路由。)或停用該功能。
取消(Cancel)	捨棄目前設定。
套用(Apply)	儲存目前設定。

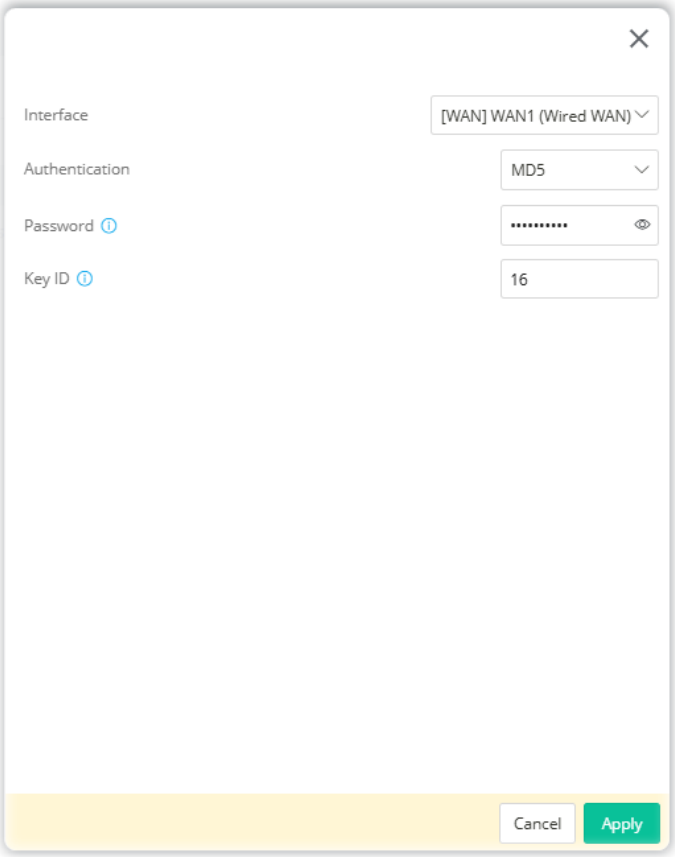
完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-1-7-2 RIP 網路(IPv4)(RIP Network (IPv4))

此頁面可讓您設定最多 8 個相鄰路由器，以便與本機路由器（Vigor C410/C510）交換路由資訊。



欲新增的 RIP 網路設定檔，請按一下**+新增(+Add)鏈結**即可開啟如下頁面。



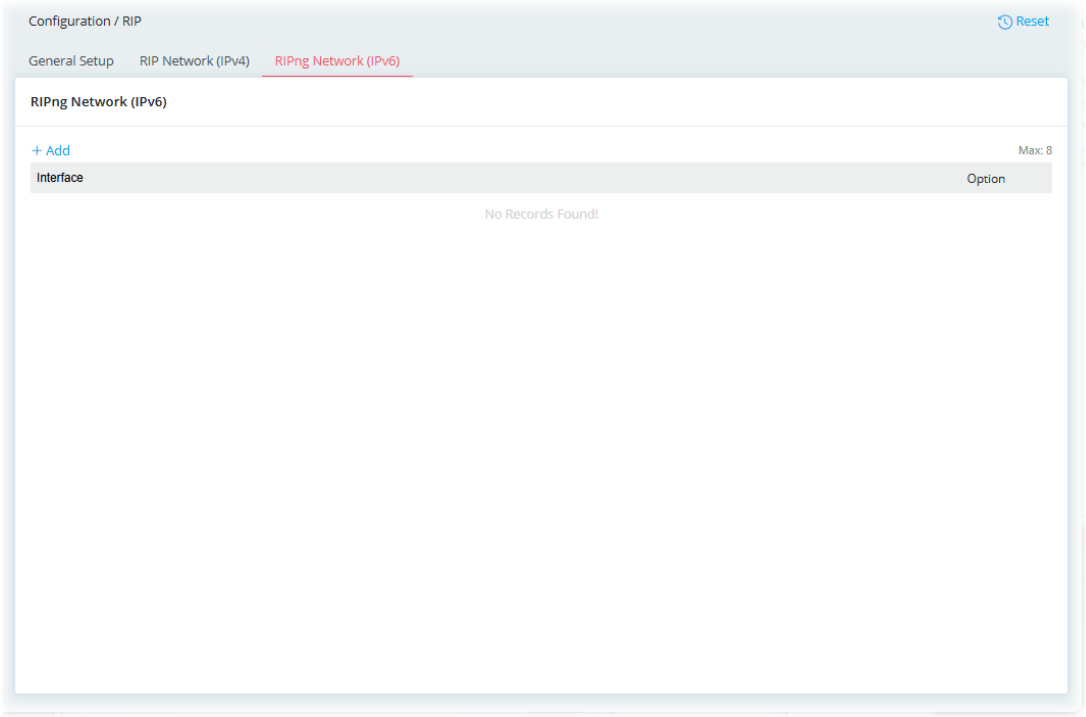
可用設定說明如下：

項目	說明
介面(Interface)	選擇 LAN / WAN 介面以套用為此設定檔的設定內容。
驗證(Authentication)	選擇此設定檔的身份驗證機制。 **停用(Disabled)** – 不會使用任何身份驗證機制。 **純文字(Plain-Text)** – 僅使用密碼進行身份驗證。 ● **密碼(Password)** – 輸入字元作為 MD5 驗證的密碼。 **MD5** – 使用 MD5 認證。 ● **密碼(Password)** – 輸入字元作為 MD5 驗證的密碼。 ● **金鑰 ID (Key ID)** – 輸入一個數字（0~255）。該 ID 將用於在自治系統中識別 Vigor 路由器。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

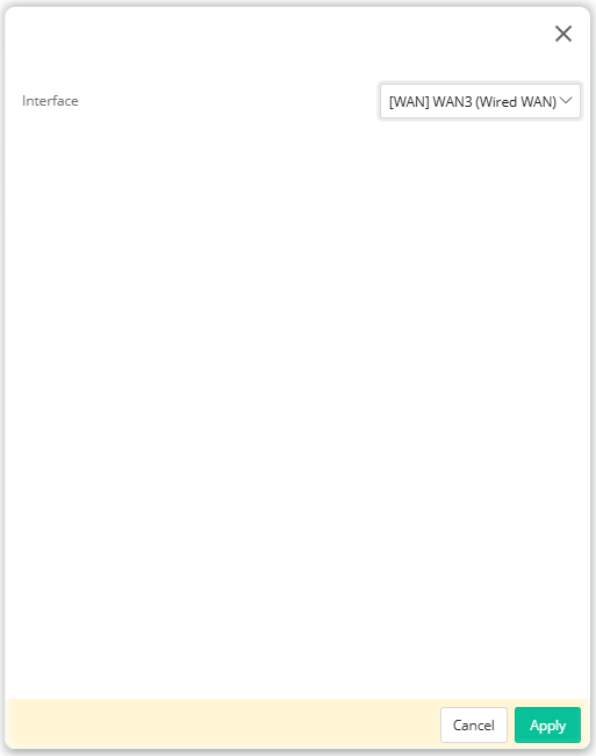
完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-1-7-3 RIPng 網路(IPv6)(RIPng Network (IPv6))

此頁面可讓您設定最多 8 個介面（WAN 或 LAN），以便基於 IPv6 位址與本機路由器（Vigor2928）交換路由資訊。



欲新增的 RIPng 網路設定檔，請按一下**+新增(+Add)鏈結**即可開啟如下頁面。



可用設定說明如下：

項目	說明
介面(Interface)	選擇 LAN / WAN 介面以套用為此設定檔的設定內容。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

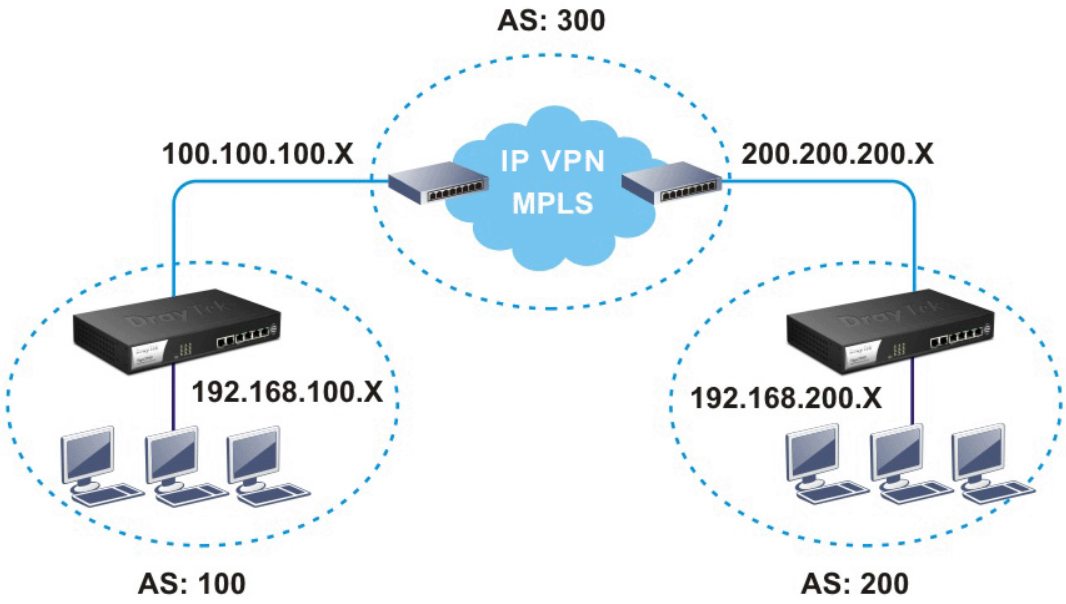
完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-1-8 BGP 設定

邊界閘道協定（BGP）是一種標準化通訊協定，旨在網際網路上的自治系統（AS）之間交換路由和可達性資訊。

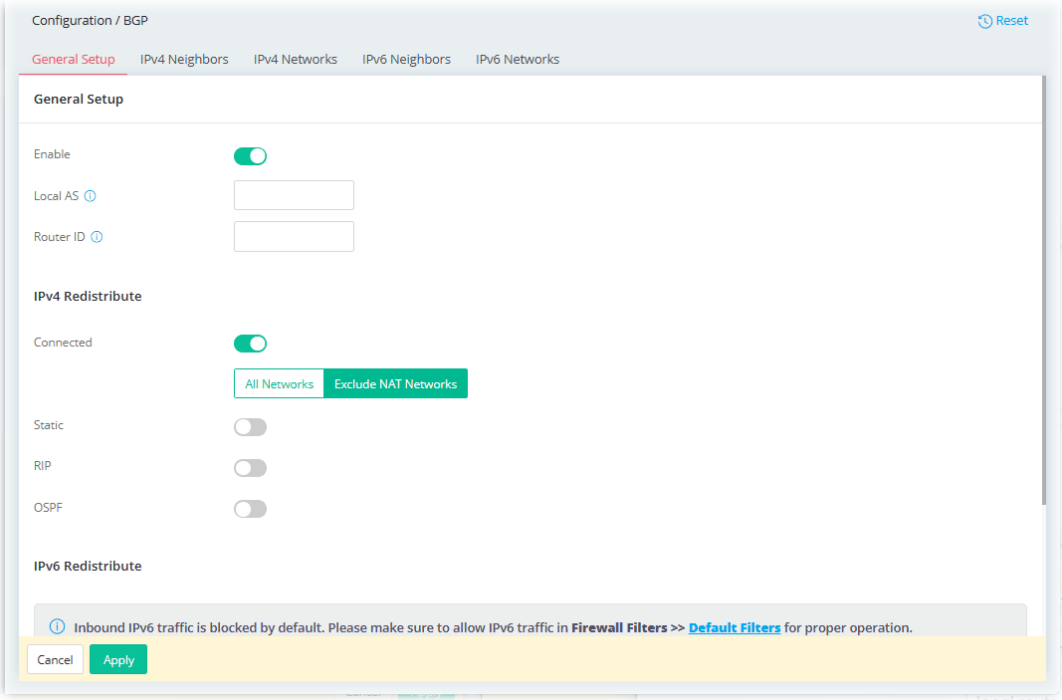
支援 BGP 的兩台路由器使用 TCP 協定進行資料傳輸。BGP 路由器之間互為「鄰居」，可以相互交換 BGP 路由資訊。路由器的 IPv4/IPv6 位址和 AS 號碼對於 BGP 路由資訊交換的 TCP 連線至關重要。

AS，即自治系統（Autonomous System）的縮寫，是指由多個 IPv4/IPv6 位址互連而成的網路群組。每個 AS 都會被指派一個 AS 編號（ASN）。 ASN 是 AS 的唯一標識符，用於區分整個網際網路中的每個網路群組。 AS 可以由一個或多個 ISP 經營，並遵循 ISP 制定的路由策略。



II-1-8-1 基本設定(General Setup)

設定本地路由器和相鄰路由器的基本設定。

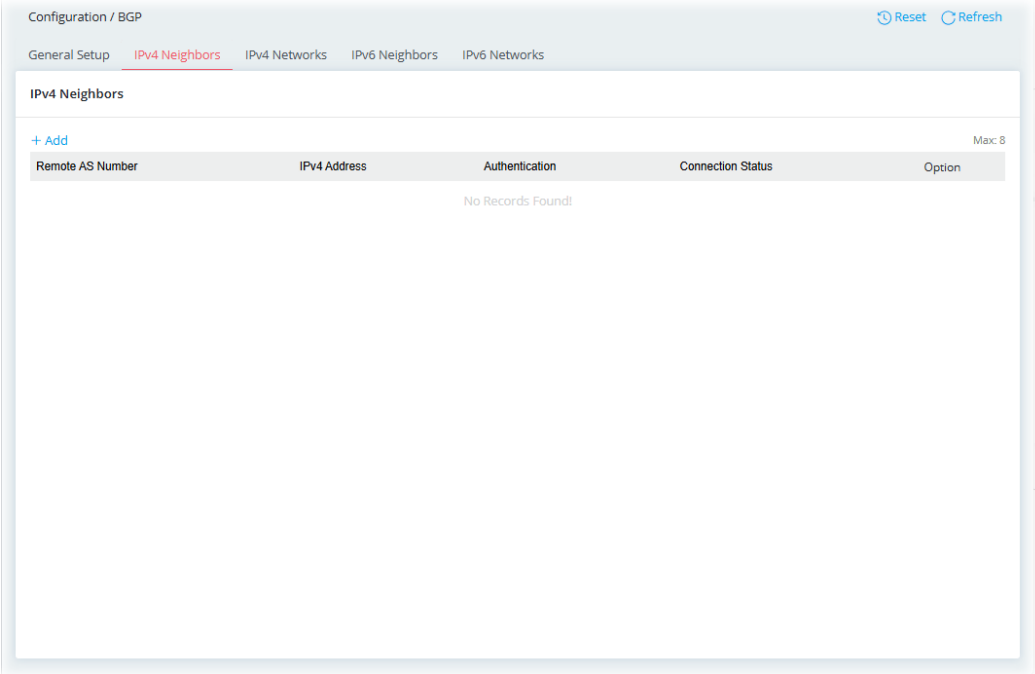


可用設定說明如下：

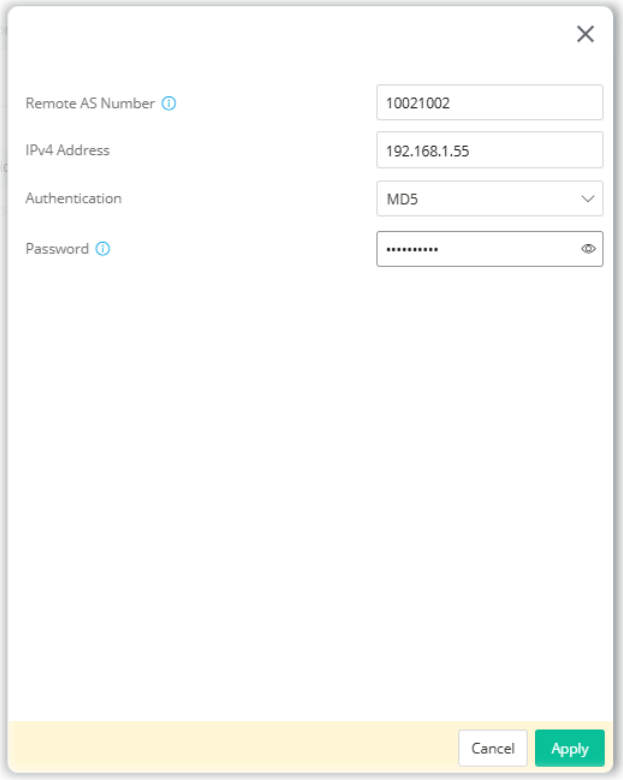
項目	說明
啟用(Enabled)	切換開關以啟用/停用本機路由器的基本 BGP 功能。
本機 AS (Local AS)	設定本機路由器的 AS 號。
路由器 ID(Router ID)	指定路由器的區域網路子網路。
IPv4 重新分配(IPv4 Redistribute)	
已連線(Connected)	**全部的網路(All Networks)** – 將 BGP 設定檔套用到所有 LAN 介面。 **排除 NAT 網路(Exclude NAT Networks)** - 將 BGP 設定檔套用至 NAT 網路以外的所有 LAN 介面。
靜態(Static)	切換開關以啟用或停用該功能(將靜態路由套用到 BGP 設定檔)。
RIP	切換開關以啟用或停用該功能(將 RIP 功能套用至 BGP 設定檔)。
OSPF	切換開關以啟用或停用該功能(將 OSPF 功能套用至 BGP 設定檔)。
IPv6 重新分配(IPv6 Redistribute)	
已連線(Connected)	切換開關以啟用(將 BGP 設定檔套用到所有 LAN 介面)或停用該功能。
靜態(Static)	切換開關以啟用或停用該功能(將靜態路由套用到 BGP 設定檔)。
RIP	切換開關以啟用或停用該功能(允許依照從 RIP 協定中學習到的資訊之動態路由流量)。
OSPF	切換開關以啟用或停用該功能(允許依照從 OSPF 協定中學習到的資訊之動態路由流量)。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

II-1-8-2 IPv4 芳鄰(IPv4 Neighbors)

設定相鄰路由器的基本設定(基於 IPv4 位址)。



欲新增新的 IPv4 芳鄰設定檔(最多 8 個)，請按一下**+新增(+Add)**鏈結即可開啟如下頁面。



可用設定說明如下：

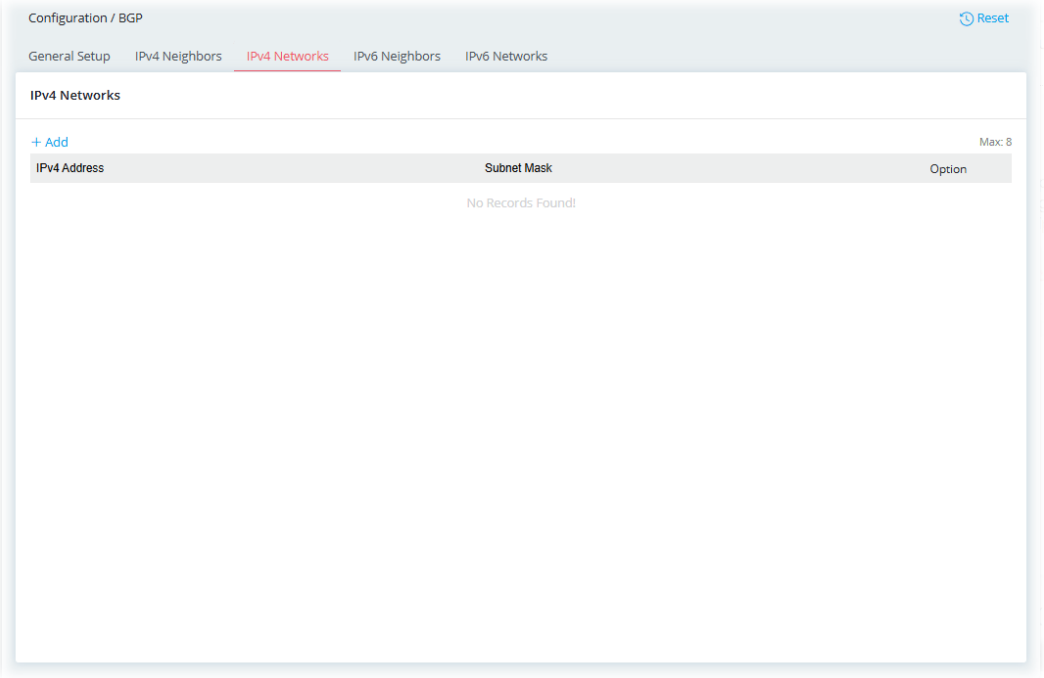
項目	說明
遠端 AS 號碼(Remote AS	指定相鄰路由器的 AS 號。

Number)	
IPv4 位址(IPv4 Address)	輸入相鄰設定檔的 IP 位址。
驗證(Authentication)	選擇此設定檔的身份驗證機制。 **停用(Disabled)** – 不會使用任何身份驗證機制。 **MD5** – 使用 MD5 認證。 ● **密碼(Password)** – 輸入字元作為 MD5 驗證的密碼。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

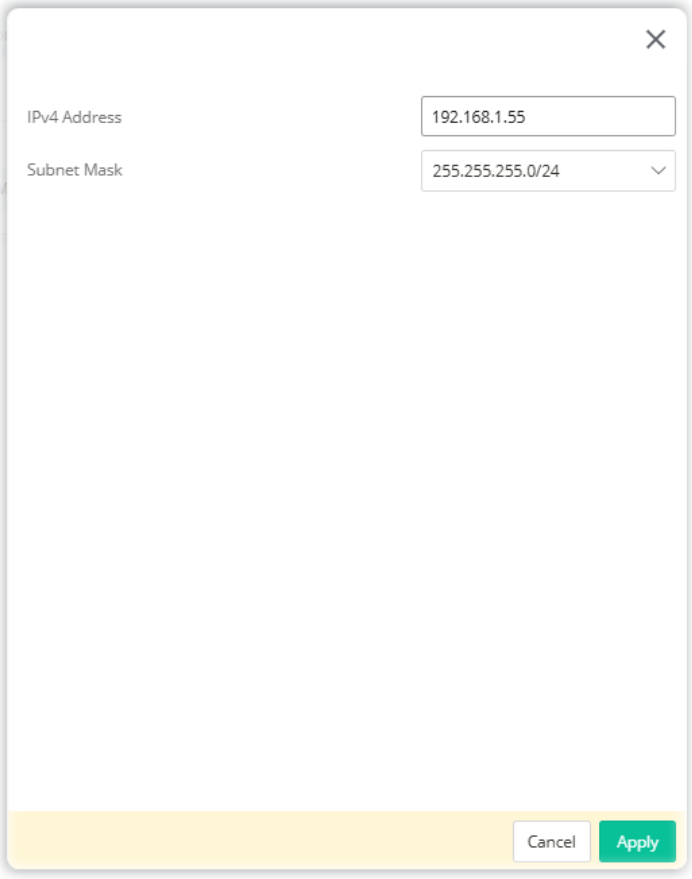
完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-1-8-3 IPv4 網路(IPv4 Networks)

此頁面允許您設定最多八個相鄰網路，以便與本機路由器(Vigor C410/C510)交換路由資訊。此頁面上定義的 IP 位址將用於聲明哪個網路將參與 RIP 協定。



欲新增 IPv4 網路設定檔(最多 8 個)，請按一下**+新增(+Add)**鏈結即可開啟如下頁面。



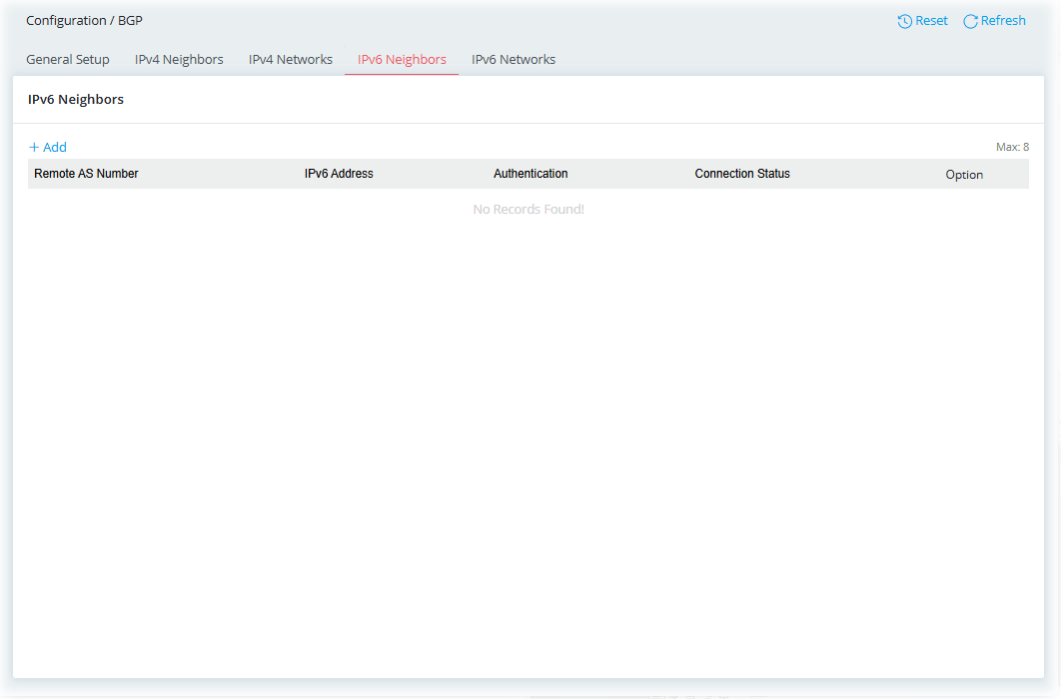
可用設定說明如下：

項目	說明
IPv4 位址(IPv4 Address)	輸入相鄰網路的 IPv4 位址(遵循 CIDR 格式)。 Vigor 路由器(例如 2928 系列)將與指定的網路交換路由資訊(RIP 資訊)。
子網遮罩(Subnet Mask)	選擇上面指定的 IPv4 位址的遮罩值。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

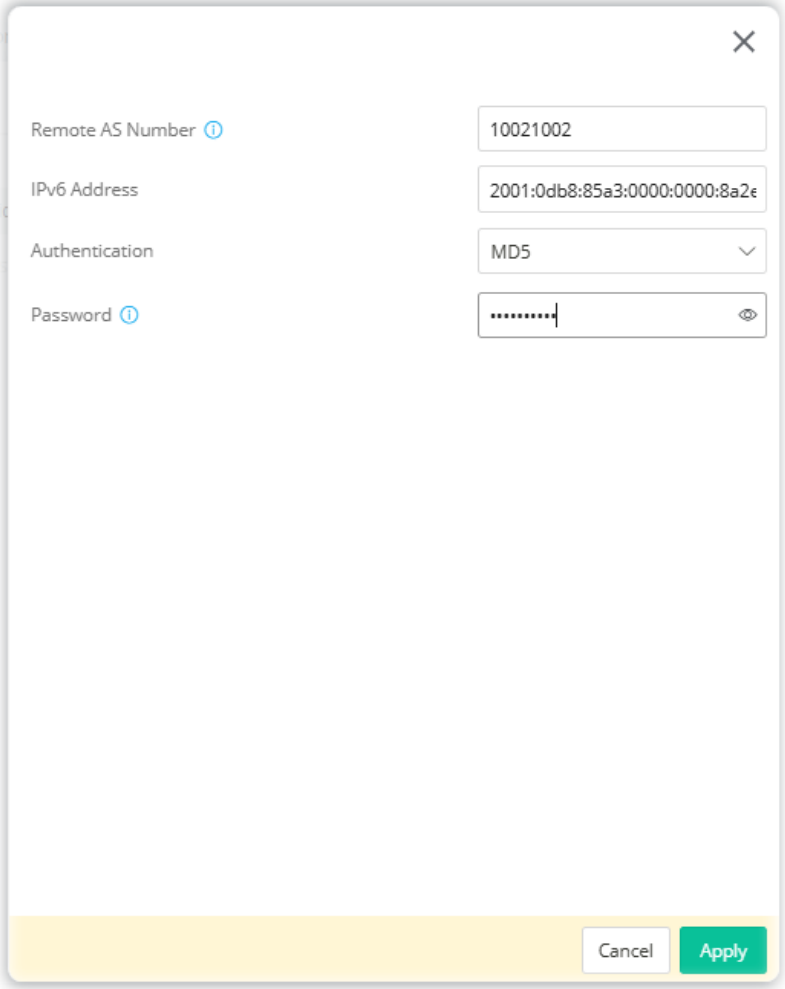
完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-1-8-4 IPv6 芳鄰(IPv6 Neighbors)

設定本機路由器和相鄰路由器的基本設定(基於 IPv6 位址)。



欲新增 IPv6 網路設定檔，請按一下**+新增(+Add)**鏈結即可開啟如下頁面。



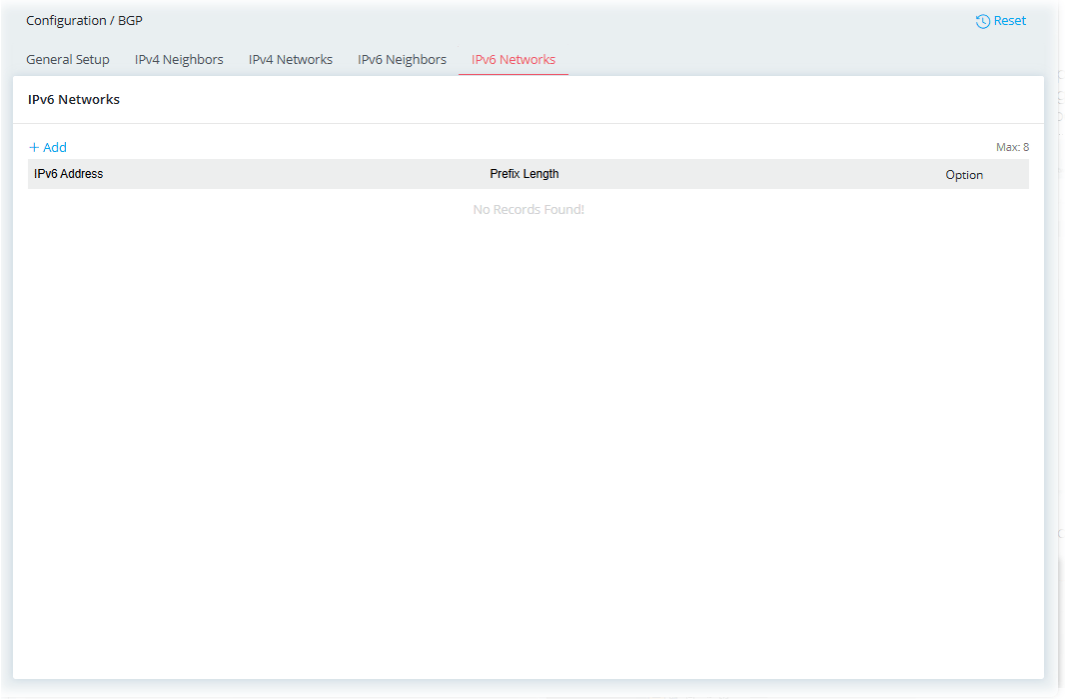
可用設定說明如下：

項目	說明
遠端 AS 號碼(Remote AS Number)	指定相鄰路由器的 AS 號。
IPv6 位址(IPv6 Address)	輸入相鄰設定檔的 IPv6 位址。
驗證(Authentication)	選擇此設定檔的身份驗證機制。 **停用(Disabled)** – 不會使用任何身份驗證機制。 **MD5** – 使用 MD5 認證。 ● **密碼(Password)** – 輸入字元作為 MD5 驗證的密碼。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

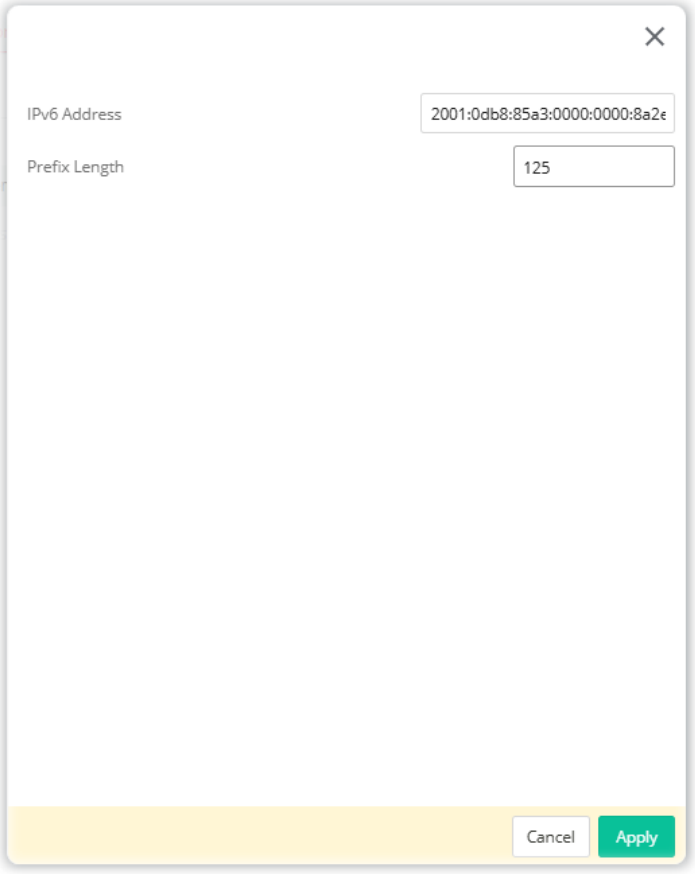
完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-1-8-5 IPv6 網路(IPv6 Networks)

此頁面允許您配置最多八個相鄰網路，以便與本地路由器(Vigor2928)交換路由資訊。此頁面上定義的 IPv6 位址將用於聲明哪個網路將參與 RIPng 協定。



欲新增 IPv6 網路設定檔，請按一下**+新增(+Add)**鏈結即可開啟如下頁面。



可用設定說明如下：

項目	說明
IPv6 位址(IPv6 Address)	輸入相鄰網路的 IPv6 位址（遵循 CIDR 格式）。 Vigor 路由器將與指定的網路交換路由資訊（RIPng 資訊）。
前置碼長度(Prefix Length)	請輸入 IPv6 位址的 IPv6 前綴長度。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-1-9 OSPF 設定

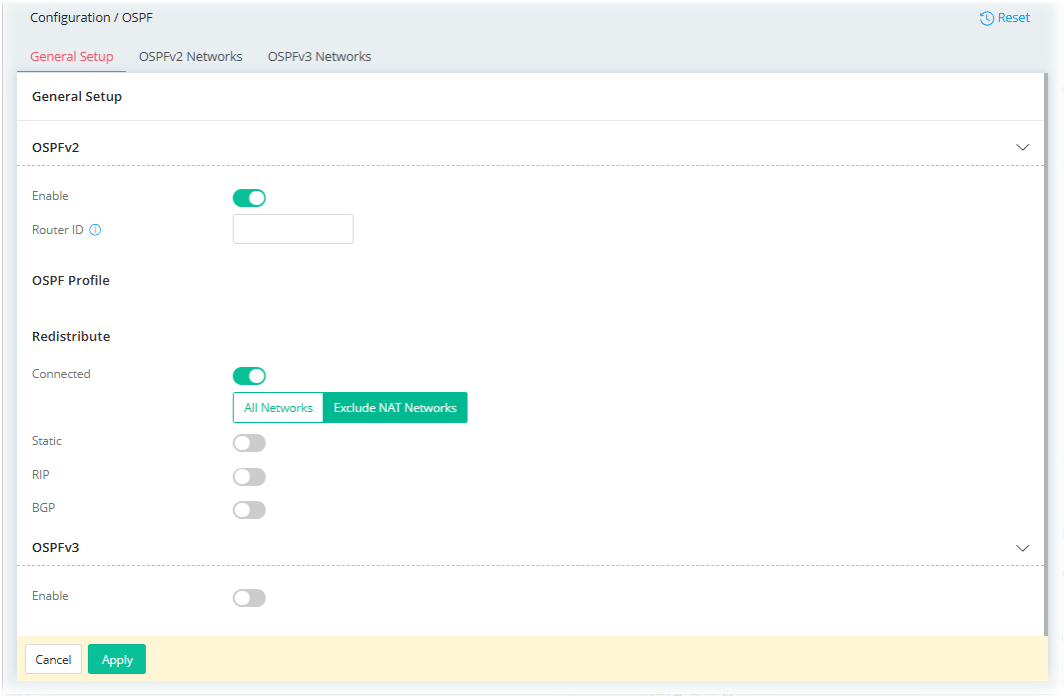
OSPF（開放式最短路徑優先，Open Shortest Path First）是一種基於 IP 協定的路由協議，運行於自治系統(AS)內。它使用 SPF(最短路徑優先)演算法計算路由度量值，適用於大型網路和複雜的資料交換。 Vigor 路由器支援 OSPF 版本 2（適用於 IPv4）和 OSPF 版本 3（適用於 IPv6）。

OSPF 中使用的自治系統（AS）可以分為幾個區域。通常，區域 0 將用作 OSPF 骨幹網，負責在各個區域之間分發路由資訊。

當您需要比距離向量路由更快的收斂速度、需要支援更大的網路或需要降低對錯誤路由資訊的敏感度時，可以啟用 OSPF 功能來滿足您的需求。請注意，要建立 OSPF 連接，兩個路由器必須同時支援 OSPF 功能。

II-1-9-1 基本設定(General Setup)

此頁面可讓您設定 OSPFv2 (IPv4) 與/或 OSPFv3 (Ipv6) 設定檔的基本設定。



可用設定說明如下：

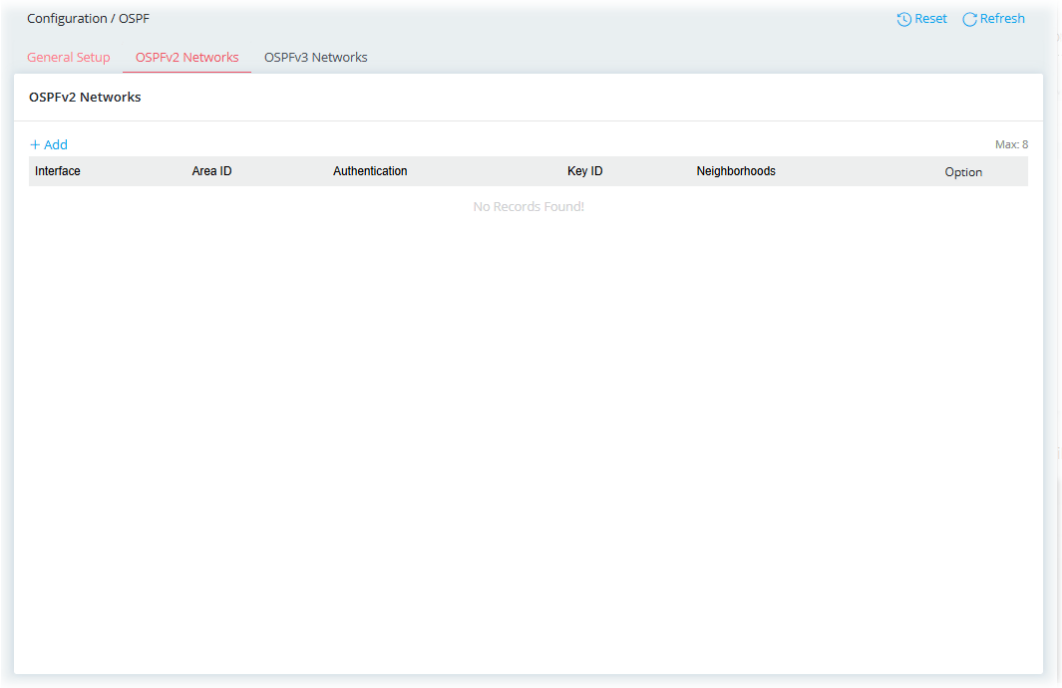
項目	說明
	OSPFv2
啟用(Enable)	切換開關以啟用/停用 OSPFv2 功能。
路由器 ID(Router ID)	指定 Vigor 路由器的 IPv4 位址，用於路由和鄰居搜尋。 這樣的 ID 有助於在自治系統中識別 Vigor 路由器。但是，如果沒有指定位址，系統將自動使用活動介面的 IP 位址。
已連線(Connected)	**所有網路(All Networks)** – 將 OSPF 設定檔套用到所有 LAN 介面。 **排除 NAT 網路(Exclude NAT Networks)** - 將 OSPF 設定檔套用至 NAT

	網路以外的所有 LAN 介面。
靜態(Static)	切換開關以將靜態路由套用到 OSPF 設定檔。
RIP	切換開關以啟用(允許依照 RIP 協定中學習到的資訊動態路由流量)或停用該功能。
BGP	切換開關以啟用(允許依照 BGP 協定中學習到的資訊動態路由流量)或停用該功能。
OSPFv3	
啟用(Enable)	切換開關以啟用/停用 OSPFv3 功能。
路由器 ID(Router ID)	指定 Vigor 路由器的 IPv6 位址，用於路由和鄰居搜尋。 這樣的 ID 有助於在自治系統中識別 Vigor 路由器。但是，如果沒有指定位址，系統將自動使用活動介面的 IP 位址。
已連線(Connected)	切換開關以啟用(將 OSPFv3 設定套用至所有 LAN 介面)或停用此功能。
靜態(Static)	切換開關以啟用(將靜態路由套用至 OSPFv3 設定檔)或停用此功能。
RIP	切換開關以啟用(允許依照從 RIP 協定中學習到的資訊動態路由流量)或停用該功能。
BGP	切換開關以啟用(允許依照從 BGP 協定中學習到的資訊動態路由流量)或停用該功能。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

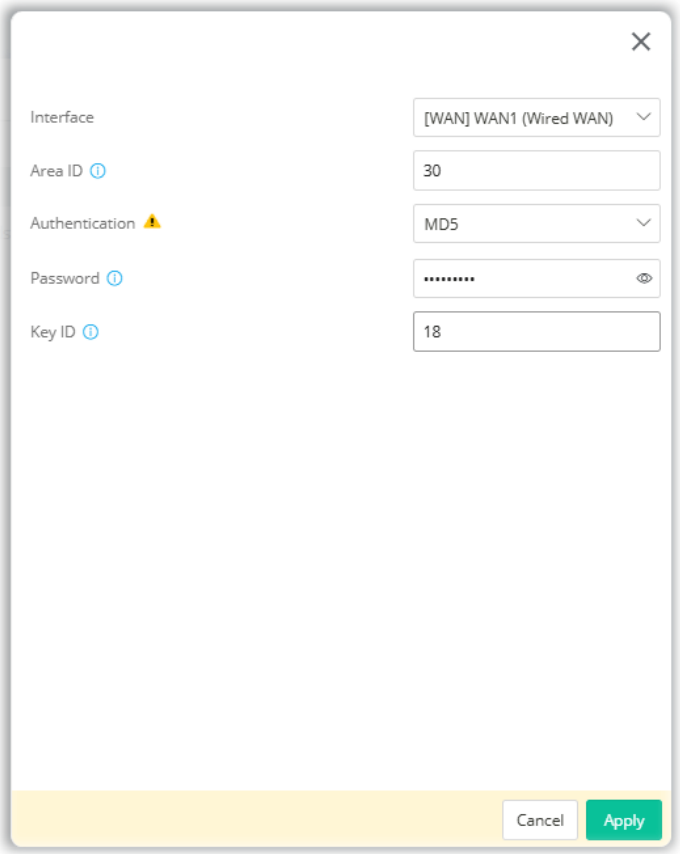
完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-1-9-2 OSPFv2 網路(OSPFv2 Networks)

此頁面可讓您為 OSPFv2 設定檔設定鄰居(按區域 ID)。



欲新增 OSPFv2 網路設定檔，請按一下**+新增(+Add)**鏈結即可開啟如下頁面。



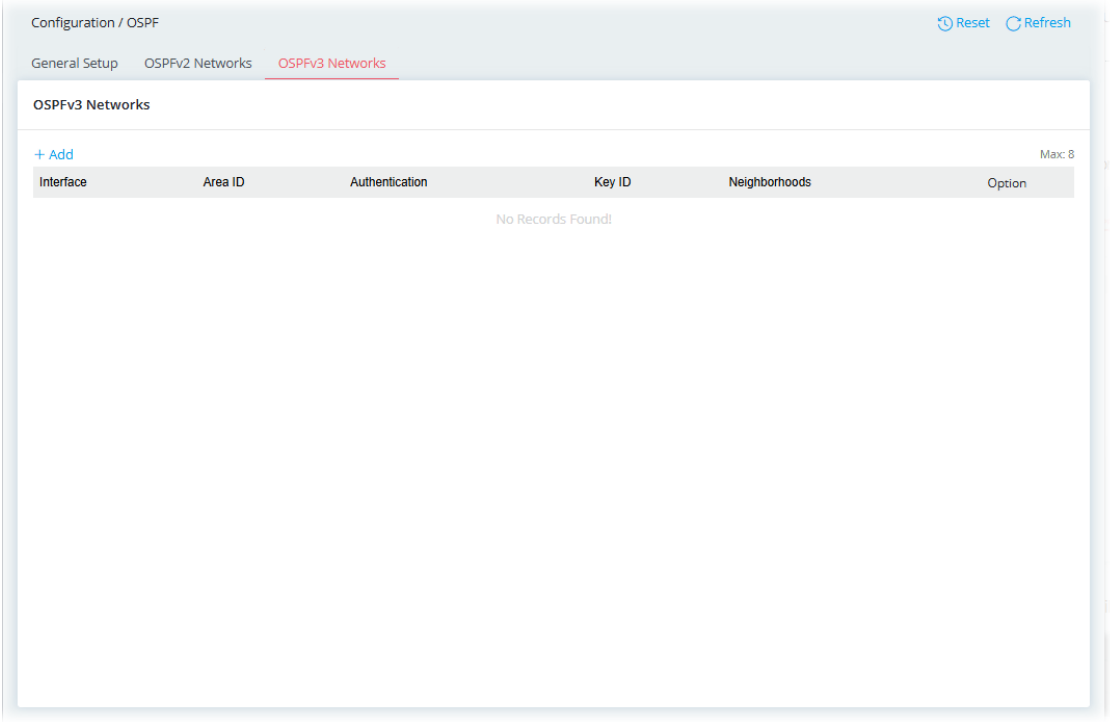
可用設定說明如下：

項目	說明
介面(Interface)	選擇 LAN / WAN 介面以套用為此設定檔的設定。
區域 ID(Area ID)	一個 AS（應用系統）將被劃分為若干區域。每個區域都必須分配一個專用編號。 請輸入數字或 IPv4 位址作為區域 ID。
驗證(Authentication)	選擇此設定檔的身份驗證機制。 **停用(Disabled)** – 不會使用任何身份驗證機制。 **純文字(Plain-Text)** – 僅使用密碼進行身份驗證。 ● **密碼(Password)** – 輸入字元作為 MD5 驗證的密碼。 **MD5** – 使用 MD5 認證。 ● **密碼(Password)** – 輸入字元作為 MD5 驗證的密碼。 ● **金鑰 ID (Key ID)** – 輸入一個數字(0~255)。該 ID 將用於在自治系統中識別 Vigor 路由器。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

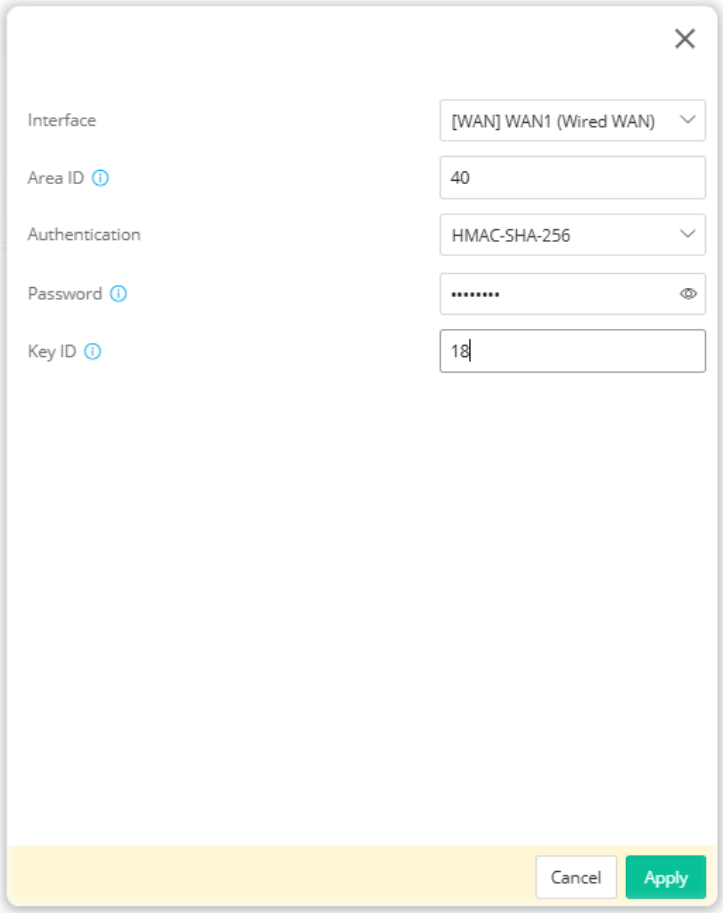
完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-1-9-3 OSPFv3 網路(OSPFv3 Networks)

此頁面可讓您為 OSPFv3 設定檔設定鄰居。



欲新增 OSPFv3 網路設定檔，請按一下**+新增(+Add)**鏈結即可開啟如下頁面。



可用設定說明如下：

項目	說明
介面(Interface)	選擇 LAN / WAN 介面以套用為此設定檔的設定。
區域 ID(Area ID)	一個 AS（應用系統）將被劃分為若干區域。每個區域都必須分配一個專用編號。 請輸入數字或 IPv4 位址作為區域 ID。
驗證(Authentication)	選擇此設定檔的身份驗證機制。 **停用(Disabled)** – 不會使用任何身份驗證機制。 **純文字(Plain-Text)** – 僅使用密碼進行身份驗證。 ● **密碼(Password)** – 輸入字元作為 MD5 驗證的密碼。 **MD5** – 使用 MD5 認證。 ● **密碼(Password)** – 輸入字元作為 MD5 驗證的密碼。 ● **金鑰 ID (Key ID)** – 輸入一個數字(0~255)。該 ID 將用於在自治系統中識別 Vigor 路由器。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

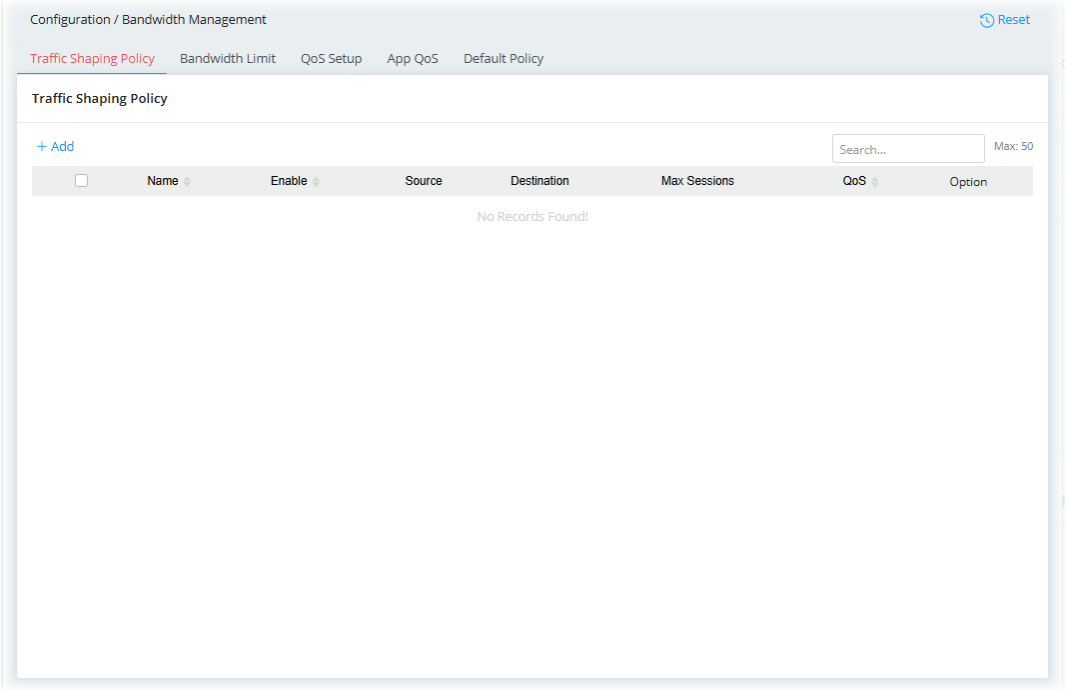
完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-1-10 頻寬管理(Bandwidth Management)

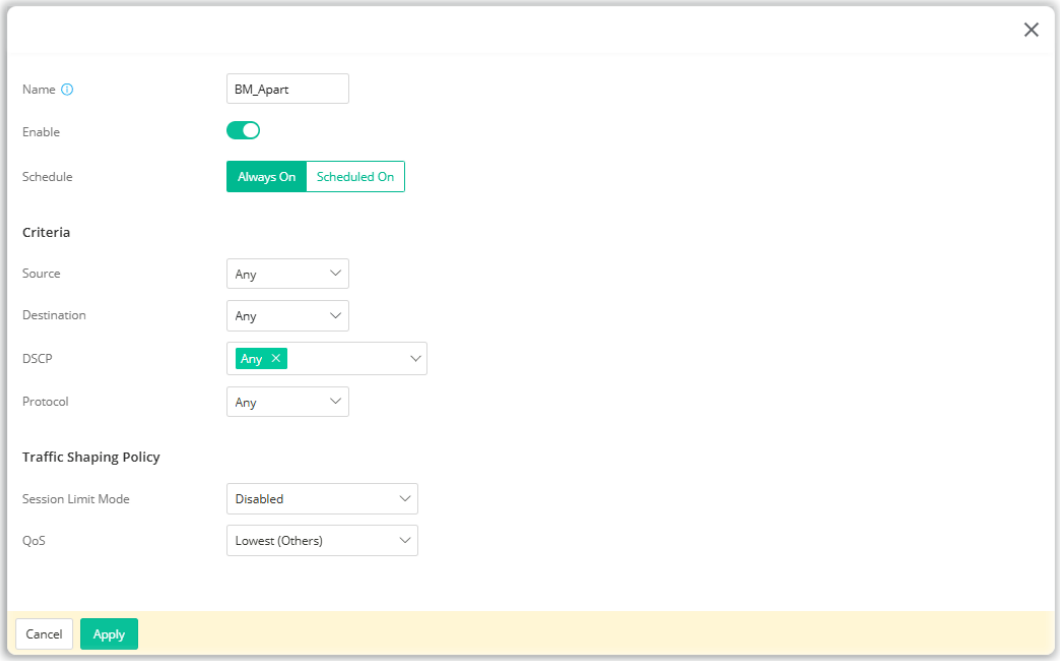
當局網域網路用戶端透過網路位址轉換 (NAT) 共用同一個真實 IP 位址時，路由器必須追蹤 NAT 連線數，以確保進出廣域網路的流量能夠到達預期目的地。路由器能夠追蹤的連線數數量有限，設定連線數限制可以防止路由器資源耗盡。這一點在使用 P2P 應用時尤其重要。P2P 應用（例如 BitTorrent）會嘗試同時與盡可能的跟廣域網路主機建立連線。

II-1-10-1 流量形成策略(Traffic Shaping Policy)

此頁面可讓您設定連線數限制和 QoS 設定。

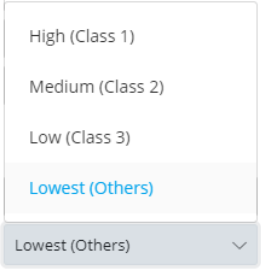


欲新增策略，請點選**+新增(+Add)**鏈結即可開啟如下頁面。



可用設定說明如下：

項目	說明
名稱(Name)	輸入設定檔名稱，以供辨識之用。
啟用(Enable)	切換此開關以啟用/停用流量形成策略(Traffic Shaping Policy)設定檔。
排程(Schedule)	Vigor 路由器可以一直執行流量形成策略設定檔，也可以在特定的日期和時間執行。 **永遠連線(Always On)** – 如果啟用，流量形成策略將一直處於運作狀態。 **排程啟用(Scheduled On)** - 依照選定的排程檔案啟動流量形成策略。
標準(Criteria)	
來源/目的(Source / Destination)	指定 IP 類型。 Vigor 路由器將依照預設策略限制 IP 的連線數。 ● 任一(Any) – 如果選擇此項，則此限制將適用於任何 IP 位址。 ● IPv4 位址(IPv4 Address) ● IPv4 子網(IPv4 Subnet) ● IPv6 位址(IPv6 Address) ● IPv6 子網(IPv6 Subnet) ● IP 物件(IP Object) ● IP 群組(IP Group)
來源/目的 IPv4 位址 (Source / Destination IPv4 Address)	當**來源/目地**設定為 **IPv4 位址**時，可使用此設定： **+新增(+Add)** – 按此建立新條目。 **IPv4 位址起始/結束(IPv4 Address Start / End)** - 輸入一個 IPv4 位址作為起始位址。然後，輸入另一個 IPv4 位址作為結束位址。
來源/目的子網位址 (Source / Destination IPv4 Subnet Address)	當**來源/目地**設定為 **IPv4 子網位址**時，可使用此設定： **+新增(+Add)** – 按此建立新條目。 **IPv4 位址(IPv4 Address)** – 輸入 IPv4 位址。 **子網遮罩(Subnet Mask)** – 指定 IPv4 位址的子網路遮罩。

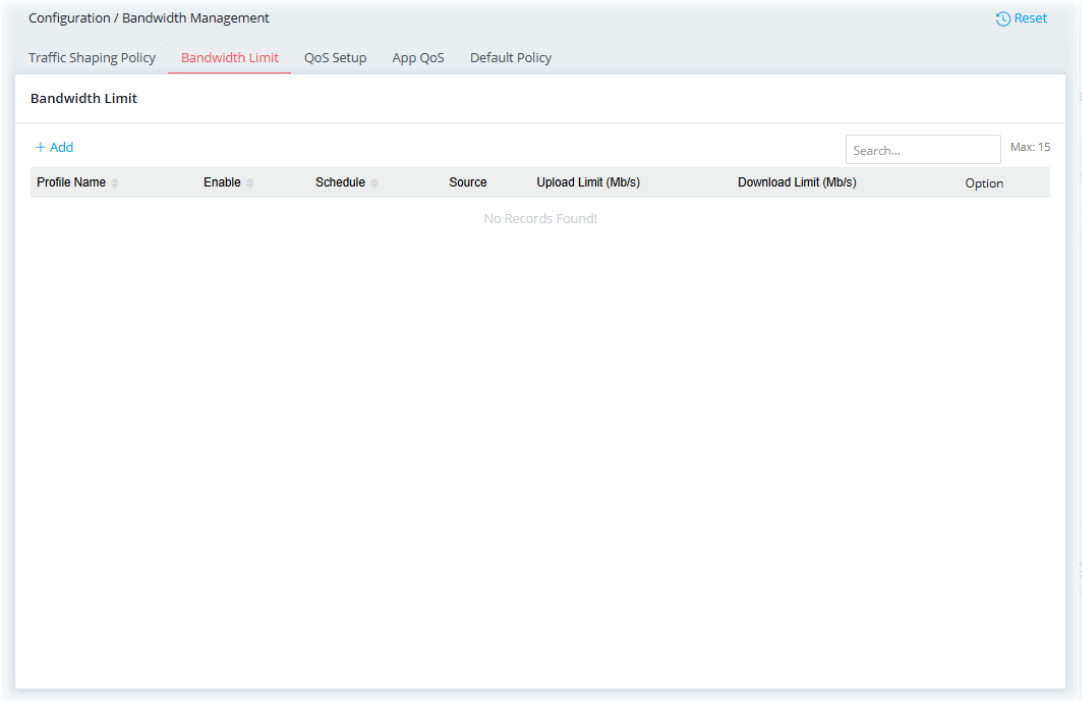
來源/目的 IPv6 位址 (Source / Destination IPv6 Address)	當**來源/目地**設定為 **IPv6 位址**時，可使用此設定： **+新增(+Add)** – 按此建立新條目。 **IPv6 位址起始/結束(IPv6 Address Start / End)** – 輸入一個 IPv6 位址作為起始位址。然後，輸入另一個 IPv6 位址作為結束位址。
來源/目的 IPv6 子網位址 (Source / Destination IPv6 Subnet Address)	當**來源/目地**設定為 **IPv6 子網位址**時，可使用此設定： **+新增(+Add)** – 按此建立新條目。 **IPv6 位址(IPv6 Address)** – 輸入 IPv6 位址。 **前置碼長度(Prefix Length)** – 設定 IPv6 位址的前置碼長度。
來源/目的物件(Source / Destination IP Object)	當**來源/目地**設定為 **IP 物件**時，可使用此設定： **+新增(+Add)** – 此處最多可指定 12 個物件。 **選擇物件(Select Object)** – 從右側的可用物件清單中選擇物件。
來源/目的 IP 群組(Source / Destination IP Group)	當**來源/目地**設定為 **IP 群組**時，可使用此設定： **+新增(+Add)** – 此處最多可指定 12 個群組。 **Select Group** – 從右側的可用群組清單中選擇物件。
DSCP	顯示套用 QoS 控制時的資料優先順序。 選擇此規則適用的封包的 DSCP 或 ToS 優先權。
通訊協定(Protocol)	只有通過所選通訊協定的流量才會受到限制。 從下拉式選單中選擇一種協定。 **任一(Any)** –所有流量都將受到限制 **服務類型物件(Service Type Object)** – Vigor 系統提供多種服務類型，並採用不同的協定。 ● **服務類型物件(Service Type Object)** – 按下+新增(+**Add**)建立一個新物件。最多可以建立 12 個物件。 **TCP/UDP** – 選擇 **TCP/UDP** 協定。 ● **指定來源埠號(Specify Source Port)** – 切換開關以啟用來源埠號設定。 ● **來源埠號/目的埠號 Source Port / Destination Port** – 設定連接埠範圍(1 到 65535)。 **TCP** – 傳輸控制通訊協定。設定方法與 TCP/UDP 相同。 **UDP** –使用者資料包通訊協定。設定方法與 TCP/UDP 相同。
流量形成策略(Traffic Shaping Policy)	
連線數限制模式 (Session Limit Mode)	**停用(Disabled)** – 選擇此項目可停用連線數限制功能。 **每一來源 IP 限制(Per Source IP Limit)** – 套用連線數限制至流量上。 ● **最大連線數(Max Sessions)** – 每個 LAN 用戶端允許的預設最大連線數數，除非在限制清單中指定不同的數字來覆寫此限制。
QoS	選擇將套用於此設定檔的頻寬等級 (類別 1、類別 2 、類別 3 及其他) 。 
取消(Cancel)	捨棄目前設定並離開此頁面。

套用(Apply)	儲存目前設定並離開此頁面。

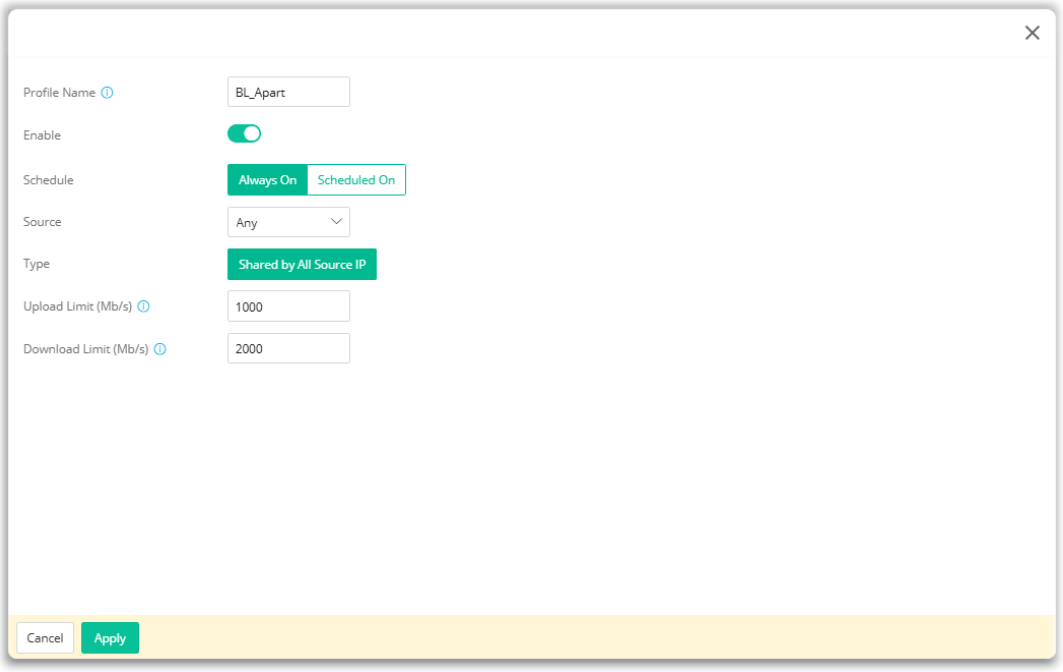
完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-1-10-2 頻寬限制(Bandwidth Limit)

頻寬限制功能透過限制上行與下行網路速度，確保 LAN 用戶端能公平分配網路頻寬。



欲新增頻寬限制策略檔案，請按下**+新增(+Add)**鏈結即可開啟如下頁面。



可用設定說明如下：

項目	說明
設定檔名稱(Profile Name)	輸入字串作為設定檔名稱，以供識別。

啟用(Enable)	切換此開關以啟用/停用此設定檔。
排程(Schedule)	Vigor 路由器可以一直執行頻寬限制，也可以在特定的日期和時間執行。 **永遠連線(Always On)** – 如果啟用，頻寬限制將一直處於運作狀態。 **排程啟用(Scheduled On)** - 依照選定的排程檔案啟動頻寬限制。
來源(Source)	確定頻寬限制將應用於哪個物件。 ● **任一(Any)** – 在定義的範圍內的所有 IP 位址都將受到 TX 限制和 RX 限制定義的頻寬限制。 ● **IPv4 位址(IPv4 Address)** ● **IPv4 子網(IPv4 Subnet)** ● **IP 物件(IP Object)** ● **IP 群組(IP Group)**
來源 IPv4 位址(Source IPv4 Address)	當來源設定為 IPv4 Address 時，可使用此設定： 按下**+新增(+Add)**新增條目。 ● **IPv4 位址起始(IPv4 Address Start)** – 輸入限制條目的起始 IP 位址。 ● **IPv4 位址結束(IPv4 Address End)** – 輸入限制條目的結束 IP 位址。
來源 IPv4 子網位址 (Source IPv4 Subnet Address)	當來源設定為 IPv4 子網時，可使用此設定： 按下**+新增(+Add)**新增條目。 ● **IPv4 位址(IPv4 Address)** – 指定起始 IP 位址。 ● **子網遮罩(Subnet Mask)** – 選擇一個子網遮罩。
來源 IP 物件 (Source IP Object)	當來源設定為 IP 物件時，可使用此設定： 所選 IP 物件中所有 IP 位址都將受到以下 TX 限制和 RX 限制定義的頻寬限制。 按下**+新增(+Add)**開啟 IP 物件表格。選擇 IP 物件，然後按一下關閉(Close)。新條目將立即新增。
來源 IP 群組 (Source IP Group)	當來源設定為 IP 群組時，可使用此設定： 所選 IP 群組中所有 IP 位址都將受到以下 TX 限制和 RX 限制定義的頻寬限制。 按下**+新增(+Add)**開啟 IP 群組表格。選擇 IP 群組，然後按一下關閉(Close)。新條目將立即新增。
上傳限制 (Upload Limit)	設定每個區域網路用戶端的上行速度限制。該值必須介於 1 和 3999 (Mbps) 之間。
下載限制 (Download Limit)	設定每個區域網路用戶端的下行速度限制。該值必須介於 1 和 3999 (Mbps) 之間。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

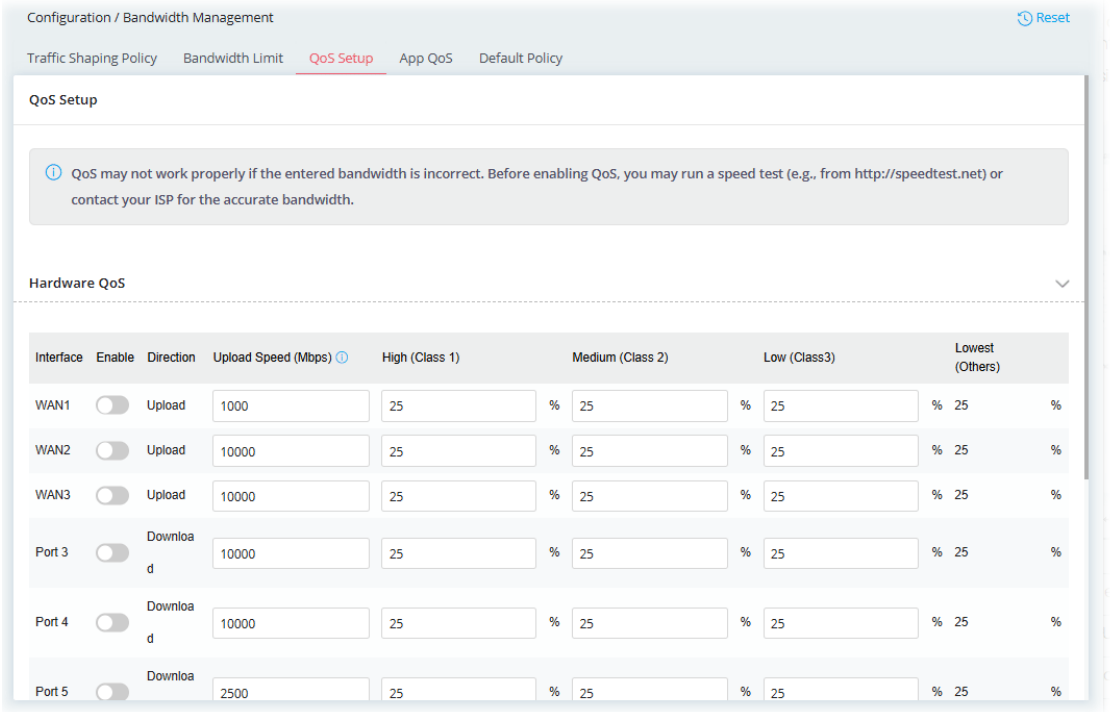
II-1-10-3 QoS 設定(QoS Setup)

服務品質(QoS)確保所有區域網路用戶端都能獲得讓應用程式正常、有效運作所需的公平分配網路頻寬。

如果沒有服務品質 (QoS)，某些應用程式可能會消耗過多的網路資源，從而降低更重要應用程式的效能，尤其是那些對抖動（延遲變化）或丟包/延遲容忍度較低的應用程式。此外，在網路擁塞時，QoS 能夠根據預先定義的優先順序對不同類型的流量進行優先排序，從而確保更重要的流量優先處理。

典型的 QoS 部署包含兩個元件：

- 分類：識別低延遲或關鍵應用程式，並將它們標記為在整個網路中執行高優先級服務等級。
- 調度：依照服務級別，將資料封包分派到不同的佇列和服務類型，從而確定資料封包的優先順序。



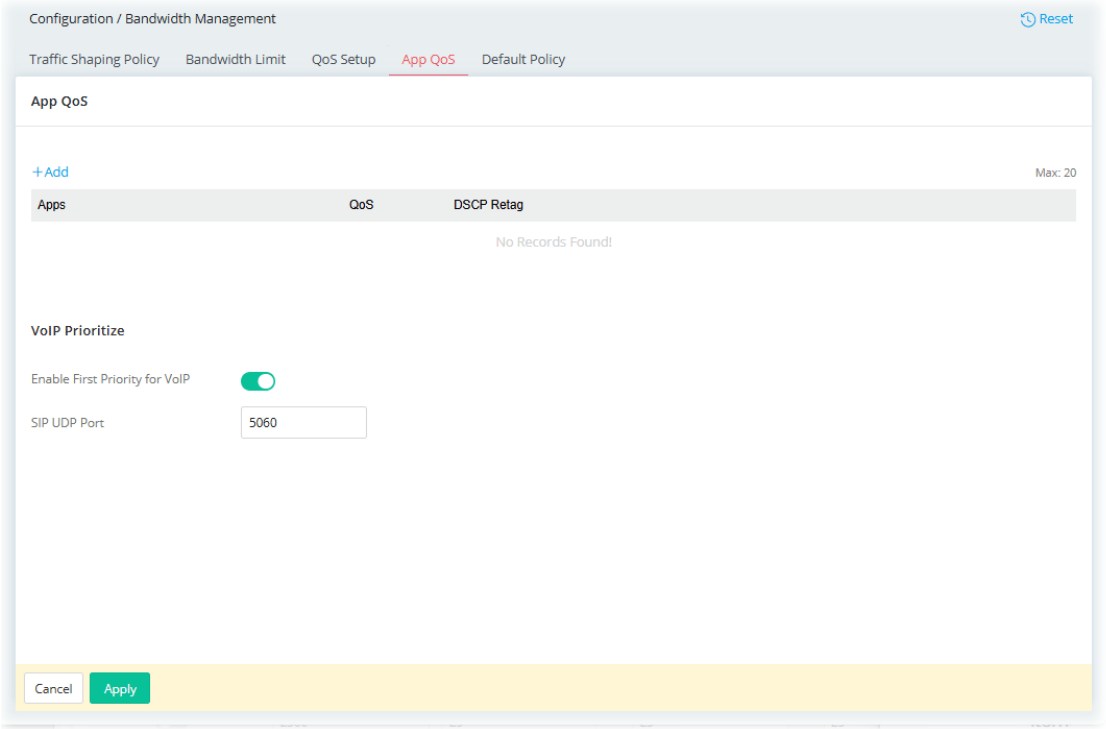
可用設定說明如下：

項目	說明
啟用(Enable)	切換開關以啟用/停用 WAN 介面設定。
方向(Direction)	目前僅支援上傳(用於對外流量)。
速度(Speed(Mbps))	設定 WAN/LAN 的對外頻寬(預設值為 1000)。
高(類別 1) (High(Class 1))	設定分配給類別 1 的頻寬(上傳速度)百分比。
中(類別 2) (Medium(Class 2))	設定分配給類別 2 的頻寬(上傳速度)百分比。
低(類別 3) (Low(Class 3))	設定分配給類別 3 的頻寬(上傳速度)百分比。
Lowest(Others)	設定分配給其他使用者的頻寬(上傳速度)百分比。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-1-10-4 APP QoS 設定

APP QoS 允許將 QoS 應用於選定的協定和應用程式。



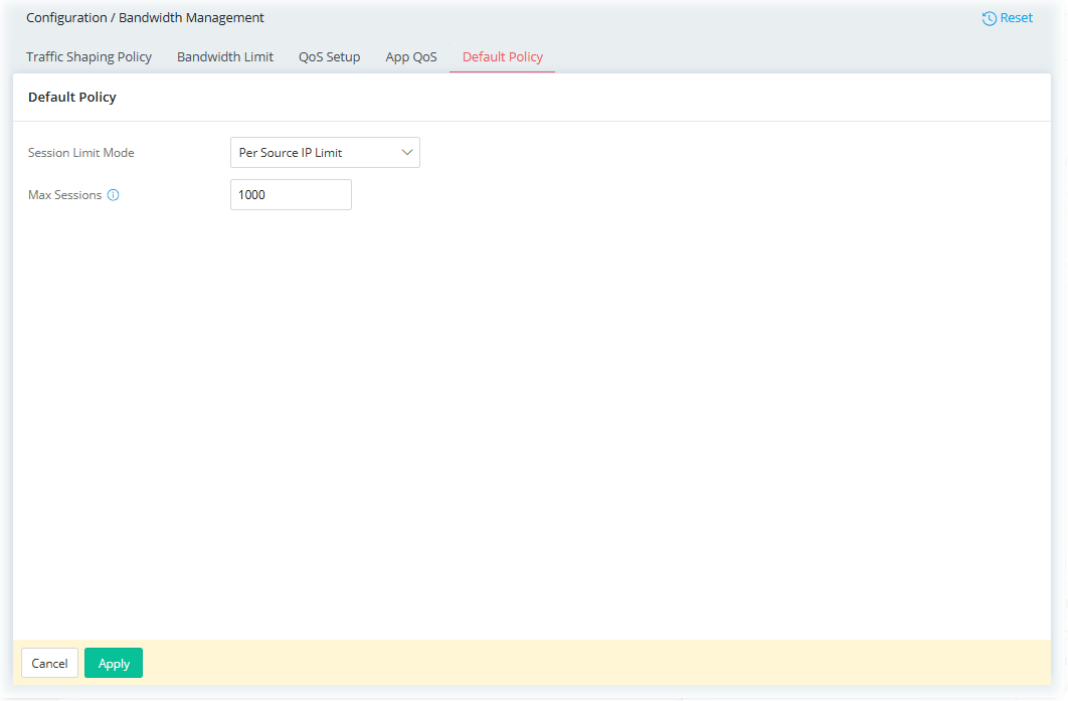
可用設定說明如下：

項目	說明
+新增(+Add)	**Apps** – 下拉式選單顯示了各種應用程式(APPE)。請選擇您需要的那一個。 **QoS** – 選擇為應用程式預留的頻寬等級(類別 1、類別 2、類別 3 及其他)。 **DSCP 重新標記(DSCP Retag)** – 選擇要使用 QoS 控制進行處理的資料等級。 **刪除(Delete)** – 按此刪除選定條目。
VoIP 優先化(VoIP Prioritize)	
啟用 VoIP 最高優先權功能(Enable First Priority for VoIP)	切換開關即可啟用/停用此功能。 啟用後，VoIP 流量將獲得最高優先權。
SIP UDP 埠號 (SIP UDP Port)	輸入要監控 SIP 流量的連接埠號碼。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-1-10-5 預設策略(Default Policy)

預設策略定義了所有流量的頻寬限制和連線數限制。



可用設定說明如下：

項目	說明
連線數限制模式(Session Limit Mode)	**停用(Disabled)** – 選此可停用連線數限制功能。 **每一來源 IP 限制(Per Source IP Limit)** – 套用連線數限制至流量上。 • **最大連線數(Max Sessions)** - 設定每個 LAN 用戶端預設可建立的最大連線數。若在限制清單(Limitation List)中已指定不同的限制值，則會套用該設定。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-1-11 NAT 設定

大多數網際網路服務供應商 (ISP) 會為每個使用者指派一個廣域網路 (WAN) IP 位址。為了同時將多個裝置連接到網際網路，需要採用一種稱為網路位址轉換 (NAT) 的技術。

通常，路由器會扮演 NAT（網路位址轉換）路由器的角色。NAT 是一種將一個或多個私有 IP 位址對應到單一公用 IP 位址的機制。公用 IP 位址通常由您的網路服務供應商（ISP）分配，您可能需要為此付費。私有 IP 位址僅在內部主機之間有效。

當發送到網際網路上某個公共伺服器的對外輸出資料封包到達 NAT 路由器時，路由器會將封包的來源位址變更為自身的公用 IP 位址，並選擇可用的公網連接埠進行轉送。同時，路由器會在路由表中記錄此位址/連接埠對映關係。當公用伺服器回應時，對內傳入流量自然會指向路由器的真實 IP 位址，路由器會根據路由表進行反向轉換。因此，內部主機可以與外部主機順暢通訊。

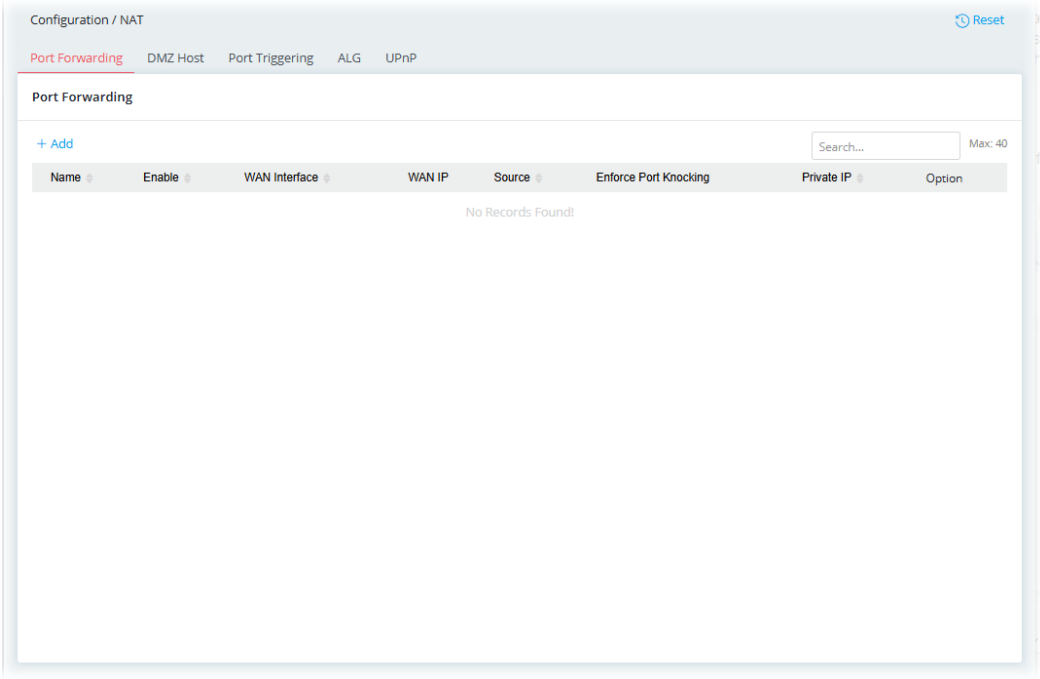
NAT 的優勢包括：

- **節省申請公網 IP 位址的成本，並實現 IP 位址的高效利用。**NAT 允許將本機的內部 IP 位址轉換為一個公用 IP 位址，因此您可以只使用一個 IP 位址來代表所有內部主機。
- **透過隱藏 IP 位址來增強內部網路的安全性。**許多攻擊都以 IP 位址為目標。由於攻擊者無法獲知任何私有 IP 位址，NAT 功能可以保護內部網路。

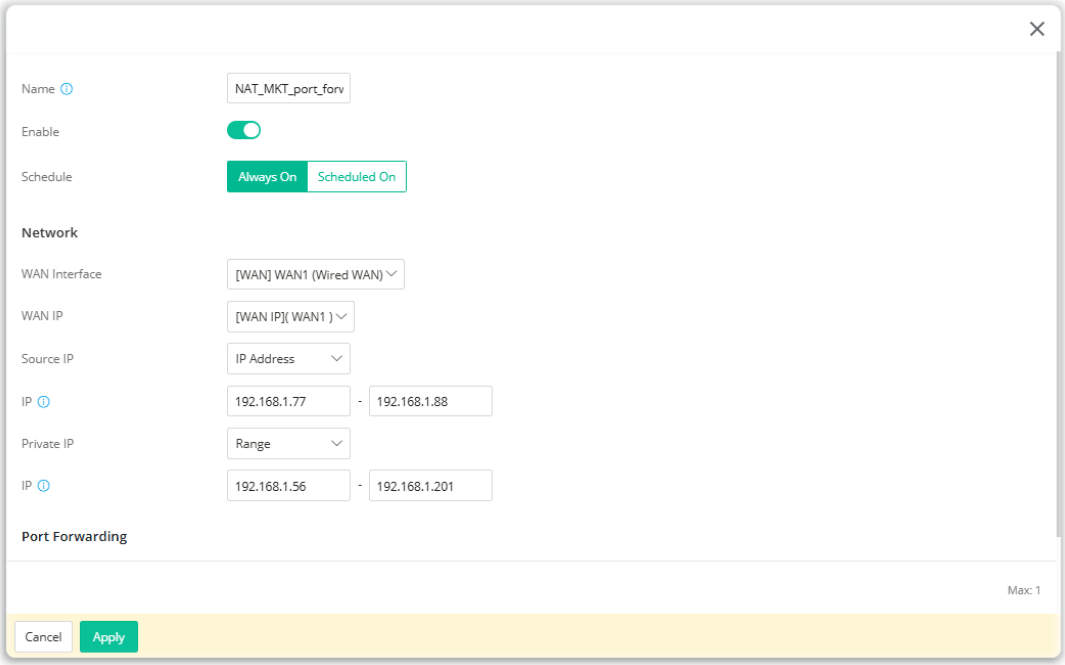
II-1-11-1 埠號轉發(Port Forwarding)

此功能允許將來自 WAN 介面上特定連接埠的傳入流量轉送至 LAN 用戶端。

可為特定應用程式開放一段連接埠範圍，讓其網路連線正常運作。

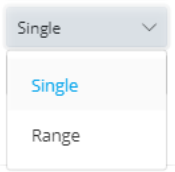


若要新增新的轉發策略，請按下**+新增(+Add)**鏈結開啟以下頁面。

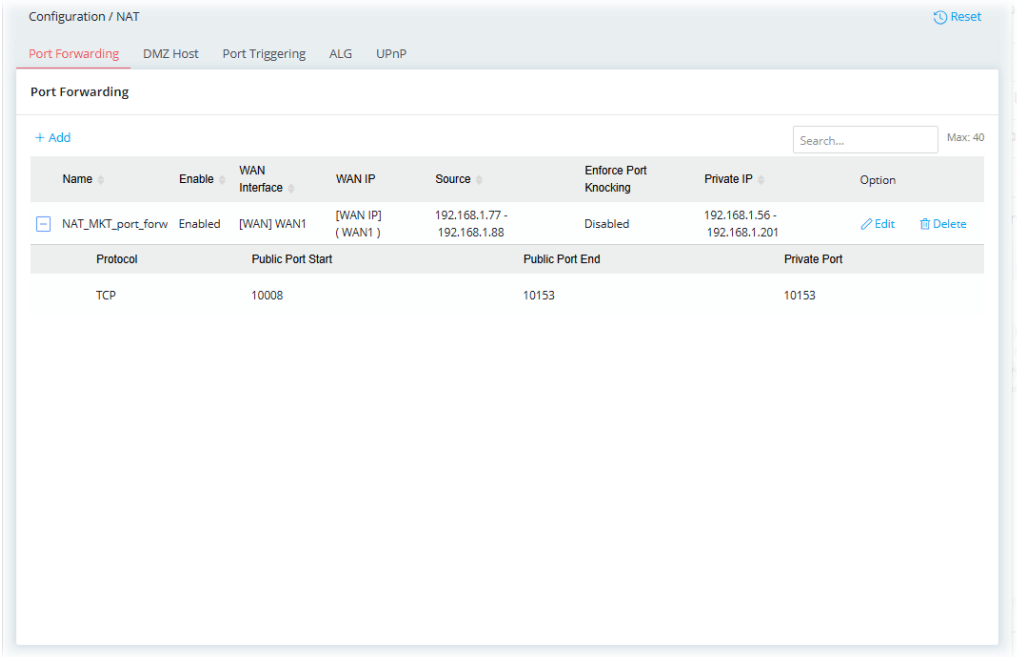


可用設定說明如下：

項目	說明
名稱(Name)	輸入名稱以供辨識用。
啟用(Enable)	切換開關即可啟用或停用此功能。
排程(Schedule)	**永遠連線(Always On)** – 如果啟用，埠號轉發功能將始終有效。 **排程啟用(Scheduled On)** - 選擇排程索引編號，允許埠號轉發在特定時間啟用。
網路(Network)	
WAN 介面(WAN Interface)	若要將傳入流量轉送至 LAN 用戶端的 WAN 連接埠。從特定的 WAN 介面 WAN# 中選擇，以將規則套用至該 WAN 介面。
WAN IP	選擇與 WAN 介面相符的 WAN IP 位址。
來源 IP(Source IP)	**任一(Any)** – 來自來源 IP 的任何資料流量都會被轉送到 LAN。 • **強制執行 Port Knocking (Enforce Port Knocking)** - 切換開關以啟用/停用此功能。 **IP 位址(IP Address)** – 設定一個 IP 位址範圍。來自該範圍內 IP 位址的任何資料流量都將被轉送到區域網路。 **IP 物件(IP Object)** – 來自 IP 物件內 IP 位址的資料流量將會轉送至 LAN 用戶端。 • **+新增(+Add)** – 按一下以指定 IP 物件設定檔。 **IP 群組(IP Group)** – 來自 IP 群組內 IP 物件的資料流量將會轉送至 LAN 用戶端。 • **+新增(+Add)** – 指定 IP 群組設定檔。
虛擬 IP(Private IP)	指定一個區域網路 IP 位址或一個區域網路 IP 位址範圍，流量將轉送至該位址。

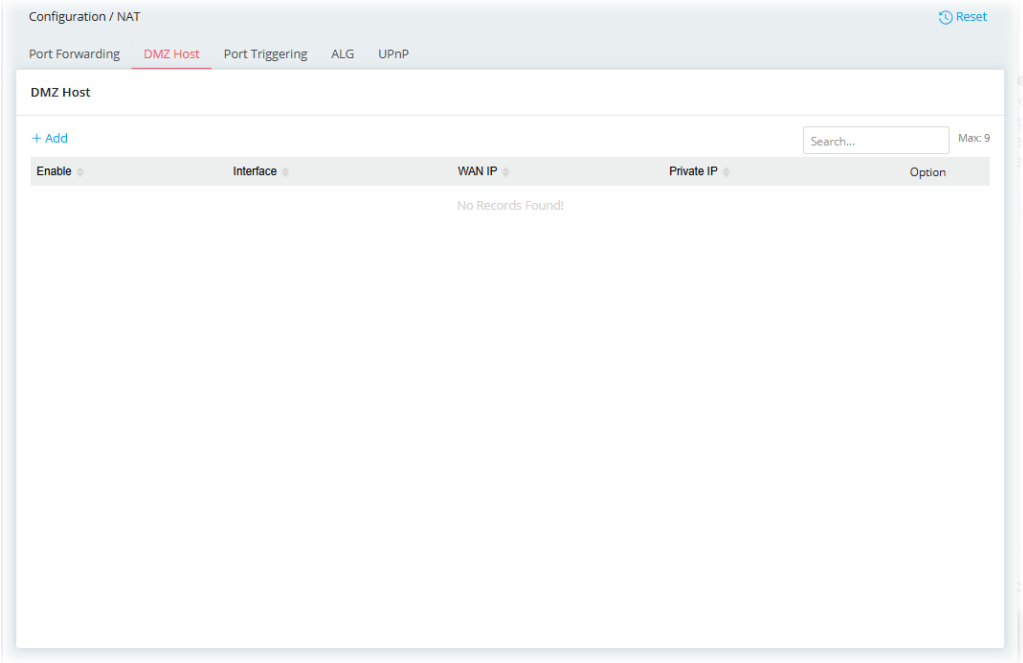
	 **單一(Single)** – 指定接收轉送流量的目的 LAN IP 位址。 **範圍(Range)** – 指定將接收轉送流量的目的 LAN IP 位址範圍。
埠號轉發(Port Forwarding)	
+新增(+Add)	按一下以設定連接埠轉發設定檔指定的通訊協定（TCP、UDP 或 TCP/UDP）的連接埠號碼。
通訊協定(Protocol)	本規則適用的協定為 TCP、UDP 或 TCP/UDP。
公用埠號起始 **(Public Port Start)**	指定一個埠號，此埠號用以重定向到內部主機中指定的虛擬 IP 和埠號。 請輸入所需的號碼作為起始埠號。
公用埠號結束 **(Public Port End)**	請輸入所需的號碼作為結束埠號。
虛擬埠號起始 **(Private Port Start)**	設定每個區域網路用戶端上流量將被導往之埠號。 請輸入所需的號碼作為起始埠號。
虛擬埠號結束 **(Private Port End)**	請輸入所需的號碼作為結束埠號。
選項(Option)	按下**刪除(Delete)**以移除選定的條目。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

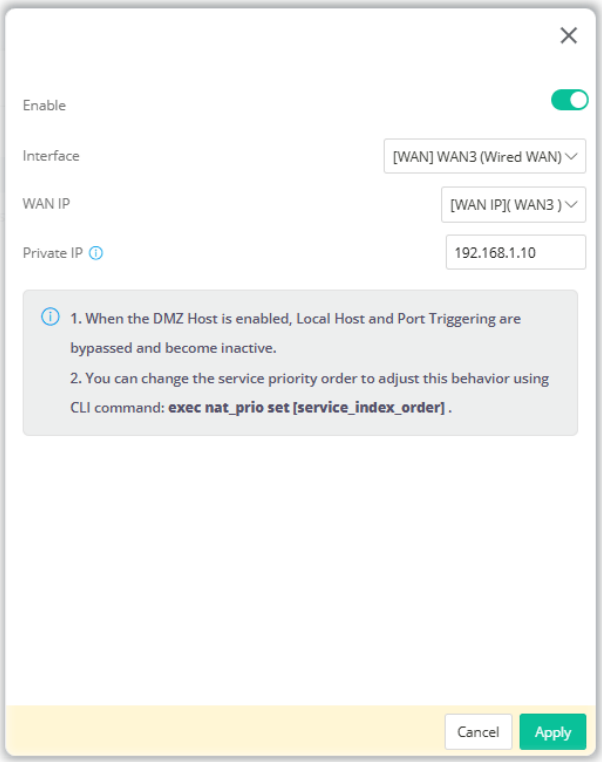


II-1-11-2 DMZ 主機(DMZ Host)

Vigor 路由器提供的功能 - **DMZ 主機** - 它會將任何協定上的所有未經請求的資料對應到區域網路中的單一主機。其他客戶端的正常網頁瀏覽和其他網路活動將繼續正常運行，不會受到不必要的干擾。**DMZ 主機**允許指定的內部用戶完全暴露於網際網路，通常對某些特殊應用，例如網路會議或網路遊戲等會很有幫助。



欲新增新的 DMZ 主機設定檔，請按一下**+新增(+Add)**連結即可造訪以下頁面。



可用設定說明如下：

項目	說明
啟用(Enable)	切換開關即可啟用或停用此功能。
介面(Interface)	允許將廣域網路(WAN)流量傳送到特定的區域網路(LAN)IP 位址。
WAN IP	啟用套用 WAN 別名 IP 的功能。然後，從設定 >> WAN >> WAN 連線(Configuration >> WAN >> WAN Connections)中設定的可用 IPv4 別名設定中選擇一個 WAN 別名 IP。
虛擬 IP(Private IP)	請輸入要作為 DMZ 主機的 IP 位址。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-1-11-3 埠號觸發(Port Triggering)

如果您執行的程式是作為伺服器應用程式執行，並且期望從 WAN 接收未經請求的流量，則可以在埠號觸發頁面中設定規則，以偵測這些程式發起的 LAN 到 WAN 流量，並自動開啟 WAN 連接埠以接受傳入流量並將其轉送到執行伺服器應用程式的 LAN 用戶端。

這些連接埠的開放持續時間取決於所使用的協定類型。 預設值如下所示，這些持續時間值可以透過 telnet 指令進行修改。

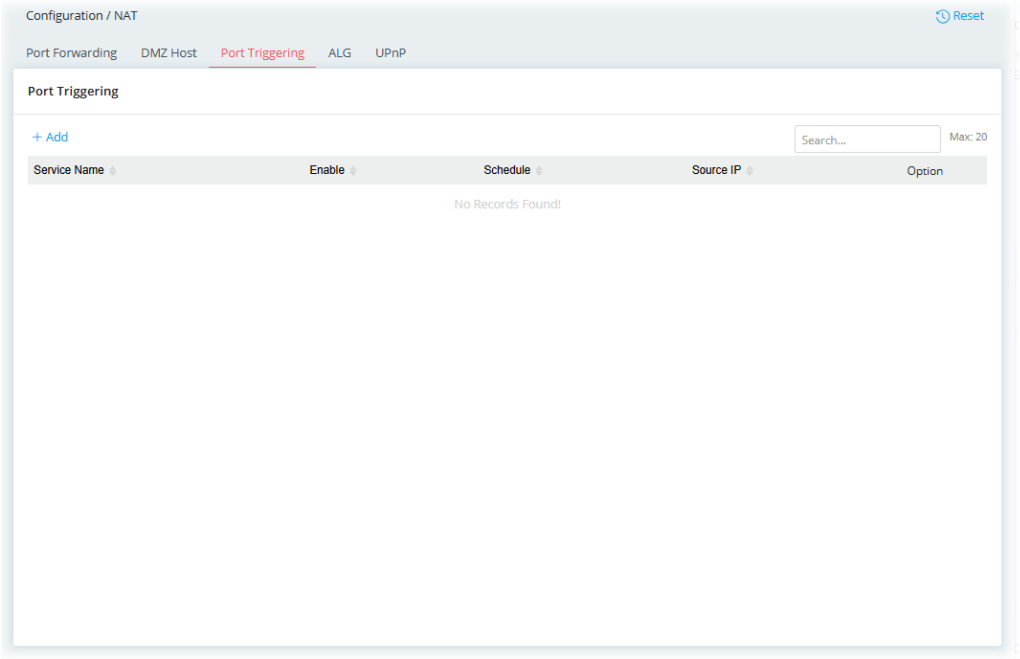
TCP: 86400 秒

UDP: 180 秒

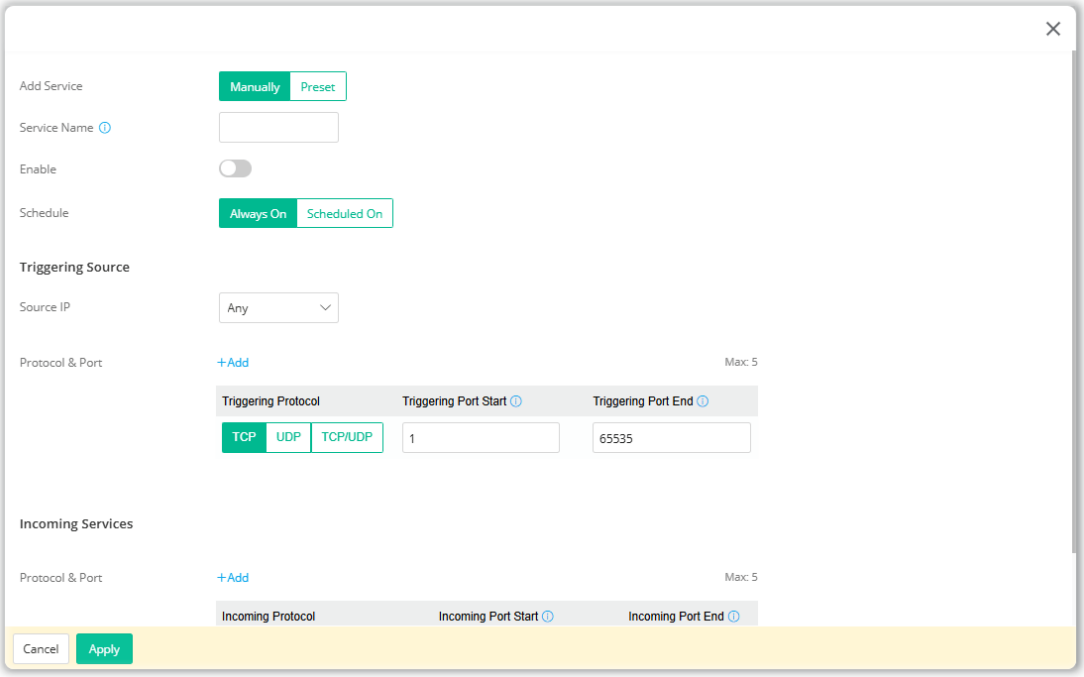
IGMP: 10 秒

TCP WWW: 60 秒

TCP SYN: 60 秒



欲新增新的埠號觸發設定檔，請按一下**+新增(+Add)**連結即可造訪以下頁面。



可用設定說明如下：

項目	說明
新增服務(Add Service)	從預定義的服務清單中選擇，或手動設定觸發、傳入協定及連接埠號。 **手動(Manually) -** 如果選擇此項，請自行定義服務名稱。 ● **服務名稱(Service Name)** – 輸入服務的名稱。 **預設(Preset) -** 如果選擇此項，系統將提供多種服務供您選擇作為服務名稱。 ● **服務名稱(Service Name)** – 使用下拉式清單指定一個服務。
啟用(Enable)	切換此開關以啟用/停用此功能。
排程(Schedule)	Vigor 路由器可讓連接埠觸發功能持續啟用，或設定只在特定日期與時間啟用。 **永遠連線(Always On)** – 如果啟用，埠號觸發將始終有效。 **排程啟用(Scheduled On)** - 埠號觸發是否有效依照選定的排程檔案而定。
觸發來源(Triggering Source)	
來源 IP(Source IP)	**任一(Any) -** 任何來源 IP 位址都將被轉送到區域網路。 **IP 位址(IP Address) -** 設定轉送至區域網路的 IP 位址範圍。 ● **IP 位址(IP Address)** – 請輸入 IP 位址和子網路遮罩。 **IP 物件(IP Object)** – 按此**+新增(+Add)**指定 IP 物件設定檔(最多 12 個設定檔)。 **IP 群組(IP Group) -** 按此**+新增(+Add)**指定 IP 群組設定檔(最多 12 個設定檔)。
通訊協定及埠號 (Protocol & Port)	**+新增(+Add) -** 按一下以設定指定協定(TCP、UDP 或 TCP/UDP)的傳出資料(此規則監視的資料)的埠號(開始和結束)。 **觸發協定(Triggering Protocol) -** 輸出流量的協定。 ● **TCP** - 開啟 TCP 流量埠號。 ● **UDP** - 開啟 UDP 流量埠號。 ● **TCP/UDP** - 開啟 TCP 與 UDP 流量埠號。 選擇此觸發設定檔的傳出資料協定(TCP、UDP 或 TCP/UDP)。

	觸發埠號起點/觸發埠號終點(Triggering Port Start / Triggering Port End) – 將發送至這些連接埠號碼的 WAN 輸出流量轉送至觸發該規則的 LAN 用戶端。 請輸入對外輸出資料封包的埠號或埠號範圍。
傳入服務(Incoming Services)	
通訊協定及埠號 (Protocol & Port)	**+新增(+Add) –** 按此以設定指定協定(TCP、UDP 或 TCP/UDP)的傳入資料的埠號(埠號起點和埠號終點)。 **傳入通訊協定(Incoming Protocol) –** 傳入流量的通訊協定。 ● **TCP** – 開啟 TCP 流量埠號。 ● **UDP** – 開啟 UDP 流量埠號。 ● **TCP/UDP** – 開啟 TCP 與 UDP 流量埠號。 選擇觸發設定檔的傳入資料的通訊協定(TCP、UDP 或 TCP/UDP)。 **輸入埠號起點/輸入埠號終點(Incoming Port Start / Incoming Port End)** – 來自 WAN 的網路流量，只要目的連接埠符合這些連接埠號碼，就會轉送至觸發此規則的 LAN 用戶端。 請輸入由外輸入資料封包的埠號或埠號範圍。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

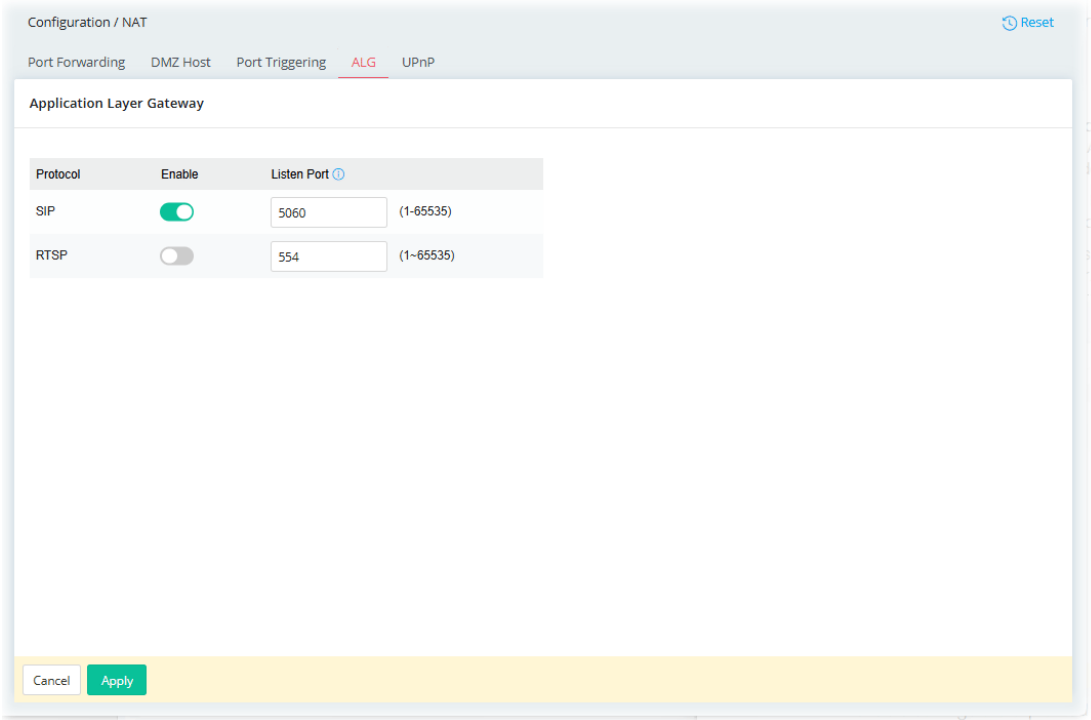
完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-1-11-4 ALG 設定

ALG 指應用層閘道(Application Layer Gateway)，Vigor 路由器提供了兩種處理語音和視訊資料封包的方法，即 RTSP(即時串流通訊協定) ALG 和 SIP(連線數啟動協定)ALG。

其中，RTSP ALG 使 Vigor 路由器能夠透過 NAT 正確地傳輸和接收 RTSP 訊息、RTCP 訊息以及語音和視訊的 RTP 封包。

而 SIP ALG 使 SIP 訊息和語音 RTP 封包能夠透過 Vigor 路由器經 NAT 正確傳輸和接收。



可用設定說明如下：

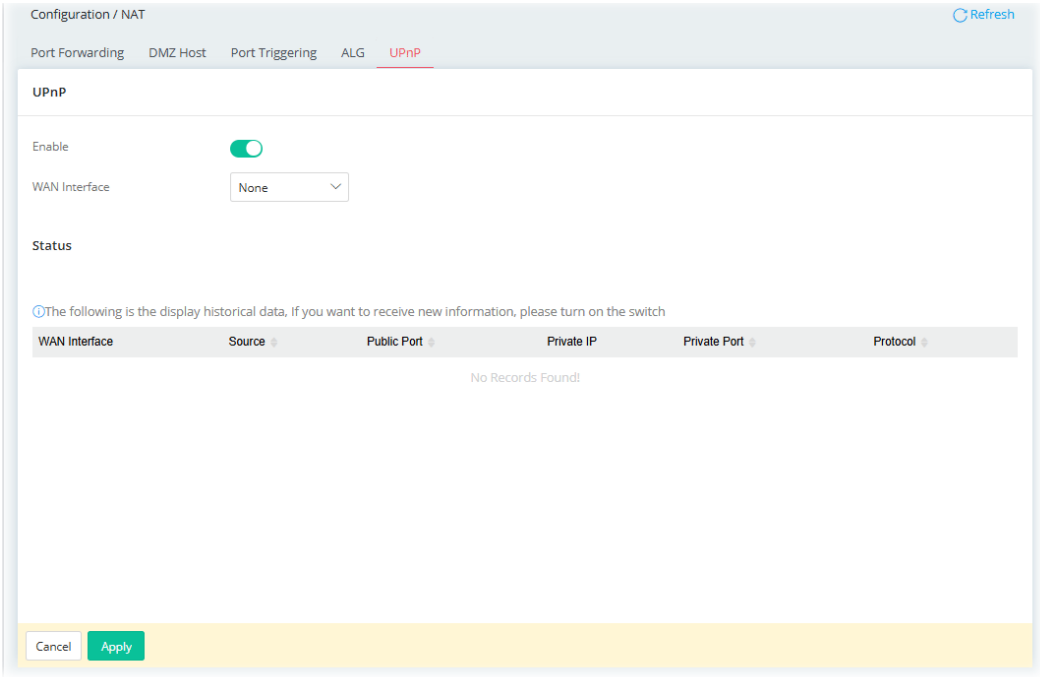
項目	說明
啟用(Enabled)	切換開關即可啟用或停用此功能。
監聽通訊埠(Listen Port)	輸入 SIP 或 RTSP 通訊協定的埠號。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-1-11-5 UPnP 設定

Vigor 路由器支援通用即插即用（Universal Plug and Play, UPnP），這是一套簡化網路設定的網路協定。支援 UPnP 的區域網路(LAN)應用程式和網路設備可以請求路由器修改其設定以允許 NAT 穿透，從而使廣域網路(WAN)主機能夠直接連接到它們。

支援 UPnP 的應用程式和裝置範例包括：uTorrent、Vuze 和 eMule 等檔案共享應用程式；Sony PlayStation 3 和 4、Xbox 360 和 Xbox One 等遊戲主機；Plex 和 XBMC 等媒體串流應用；以及 Skype 等即時通訊和通話應用程式。若要了解特定應用程式或網路設備是否支援或需要 UPnP，請查閱其使用手冊或諮詢供應商。



可用設定說明如下：

項目	說明
	UPnP
啟用(Enable)	切換開關即可啟用或停用此功能。 UPnP 是某些應用程式(例如 PPS、Skype、eMule 等)所必需的。如果您不熟悉 UPnP，基於安全考量建議關閉此功能。
WAN 介面(WAN Interface)	選擇 WAN 連接埠以回應 UPnP 指令。
狀態(Status)	顯示歷史資料。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

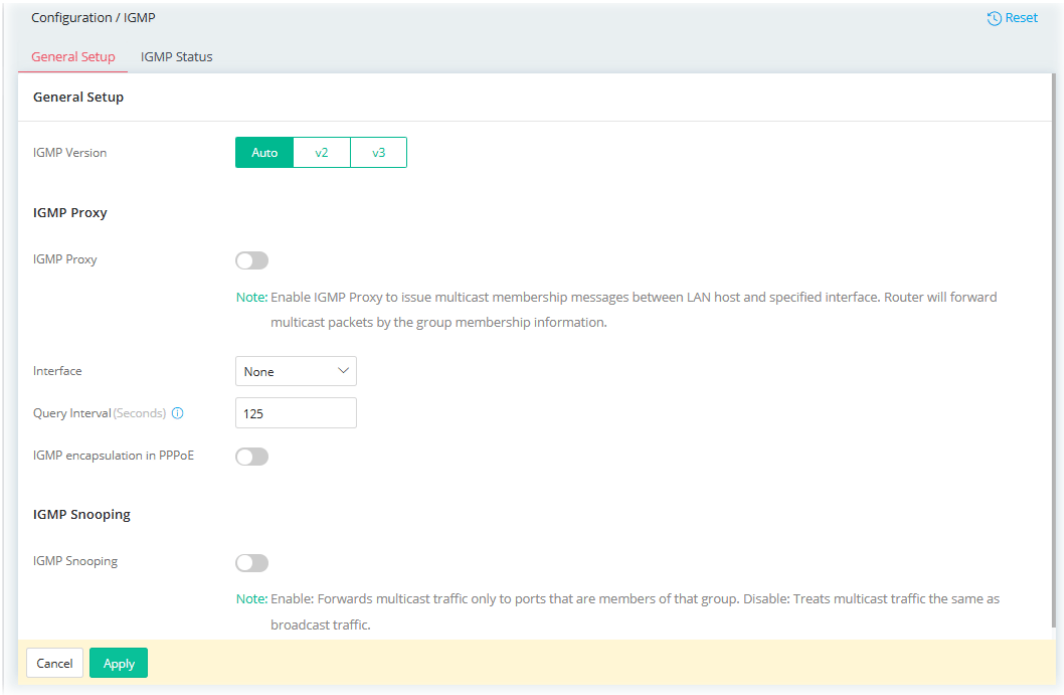
完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-1-12 IGMP 設定

網際網路群組管理協定(IGMP)是一種用於建立多播群組成員關係的 IPv4 通訊協定。

II-1-12-1 基本設定(General Setup)

本頁面提供 IGMP 功能的一般設定。



可用設定說明如下：

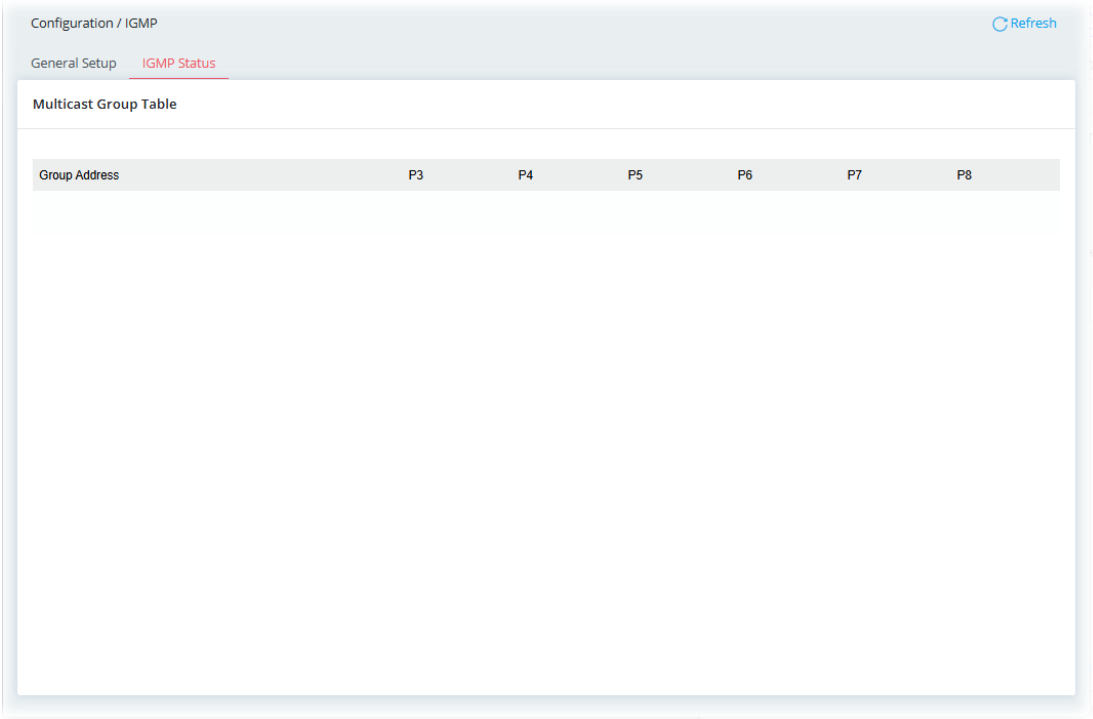
項目	說明
IGMP 版本(IGMP Version)	請選擇 v2、v3 或自動模式(Auto)。目前，Vigor 路由器支援 v2 和 v3 兩個版本。請根據您訂閱的 IPTV 服務選擇正確的版本。
IGMP 代理伺服器(IGMP Proxy)	
IGMP 代理伺服器(IGMP Proxy)	切換開關即可啟用或停用此功能。 多播功能將透過 WAN/PVC/VLAN 連接埠執行。此外，NAT 模式下也支援此功能。
介面(Interface)	指定封包通過的介面。
查詢間隔(Query Interval)	Vigor 路由器會定期發送查詢，檢查哪個 IP 位址正在取得 IPTV 服務。這可能會給客戶端帶來不便。因此，請設定適當的查詢間隔(單位：秒)，以限制 Vigor 路由器發送查詢的頻率。
在 PPPoE 上的 IGMP 封裝(IGMP encapsulation in PPPoE)	取決於各網路服務提供者的具體規定。如果您不知道如何啟用或停用，請聯絡您的網路服務供應商。
IGMP Snooping	
IGMP Snooping	選擇啟用 IGMP Snooping，以便將組播流量轉送至已加入多播群組的 IGMP 用戶端。
IGMP 快速切換(IGMP	僅當啟用 IGMP Snooping 時才會顯示此選項。選取此選項可啟用 IGMP

Fast Leave)	快速切換。 通常情況下，當路由器收到來自 IGMP 主機的"離開"訊息時，它會發送最後成員查詢訊息，以查看多播群組中是否還有成員。啟用快速切換後，當多播群組中的最後一個主機發送離開訊息時，該群組的多播將立即終止。
IGMP 接受清單(IGMP Accept List)	只有具有此處指定的 IP 位址的裝置才能透過 IGMP 代理伺服器處理多播流量。 **任一(Any)** – 所有 IP 位址均可使用 IGMP 代理伺服器。 **IP 物件(IP Object)** – 選擇 IP 物件。利用物件內 IP 位址傳輸的資料流量將透過 IGMP 代理伺服器進行處理。 **IP 群組(IP Group)** - 選擇 IP 群組。群組內物件的流量將透過 IGMP 代理進行處理。利用群組內 IP 物件傳輸的資料流量將透過 IGMP 代理伺服器進行處理。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-1-12-2 IGMP 狀態(IGMP Status)

此頁面顯示活動多播群組清單。



可用設定說明如下：

項目	說明
群組位址(Group Address)	多播群組的位址，位於 IGMP 保留的 IP 位址範圍，從 224.0.0.0 到 239.255.255.254 內。
P1 到 P5 (C410 系列) P1 到 P4 (C510 系列)	已將 IGMP 主機加入此多播群組的 LAN 連接埠。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-1-13 物件(Objects)

Vigor 路由器系統提供物件功能。

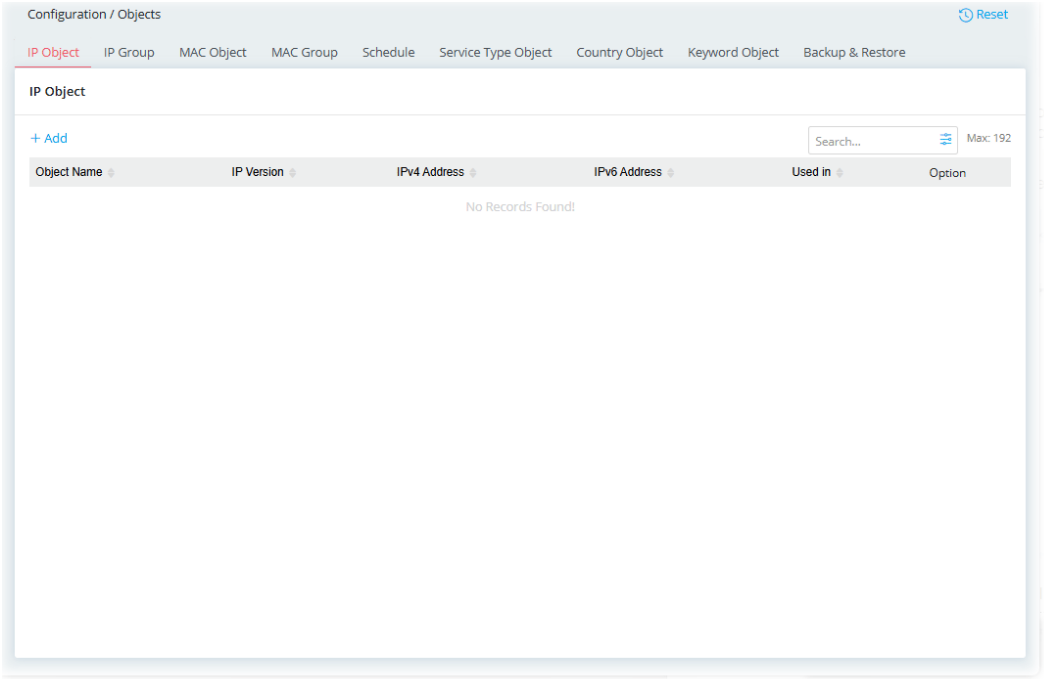
使用者可以定義各種類型的物件和群組，然後將其應用於各種場景，例如設定>>NAT>>埠號轉發(Configuration>>NAT>> Port Forwarding)、安全性>>防火牆過濾器(Security>>Firewall Filters)。

其優點在於使用者無需重複設定，從而可提高效率。目前可預設的物件包括 IP、MAC、排程、服務類型、關鍵字，以及包含 IP、MAC 群組等等。

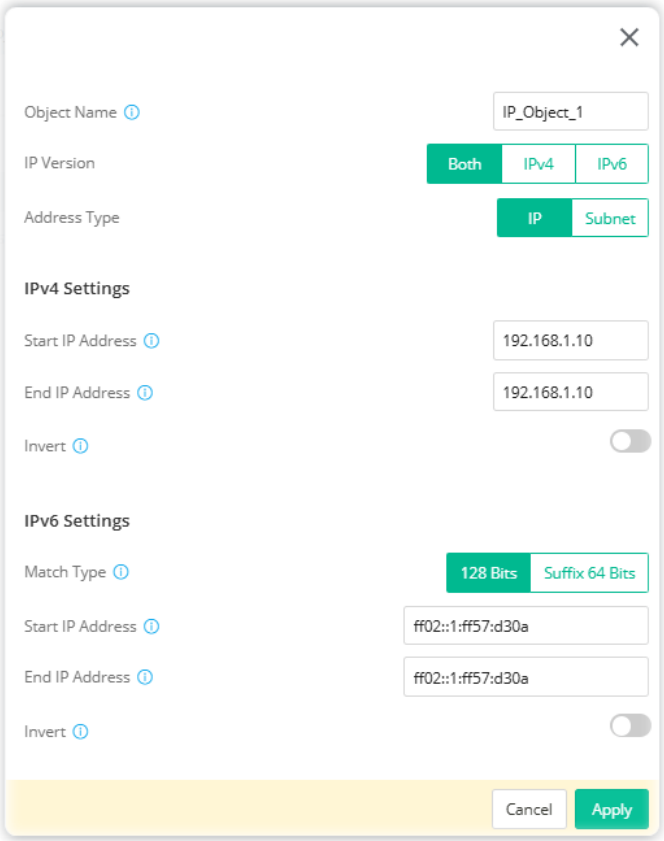
II-1-13-1 IP 物件(IP Object)

通常情況下，路由器設定中會套用一定範圍內的 IP 位址和服務埠號，因此我們可以用物件以及將物件綁定在群組內，方便後續使用。之後，我們可以選擇該物件/群組來套用到不同的情境。

例如，可以使用 IP 物件定義同一部門內的 IP 位址範圍。



欲新增 IP 物件設定檔，請按下**+新增(+Add)**鏈結即可開啟如下頁面。



可用設定說明如下：

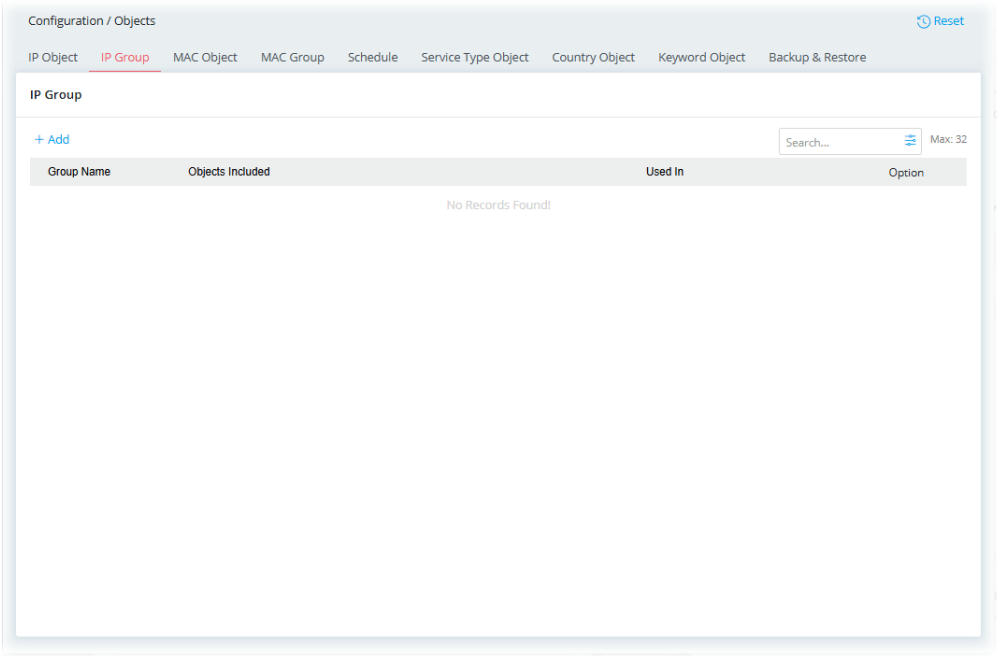
項目	說明
物件名稱(Object Name)	輸入一個用於識別此物件的名稱。
IP 版本(IP Version)	選擇 IP 版本(IPv4、IPv6 或二者)以輸入正確的 IP 位址。
位址類型(Address Type)	選擇位址類型 IP(IP)或子網(Subnet)位址。
IPv4 設定(IPv4 Settings)	
起始 IP 位址(Start IP Address)	如果位址類型為 IP，請輸入起始 IP 位址。 若要設定 IP 位址範圍，請在起始 IP 位址和結束 IP 位址欄位分別輸入不同的 IP 位址。
結束 IP 位址(End IP Address)	如果位址類型為 IP，請輸入結束 IP 位址。
IP 位址(IP Address)	如果位址類型為子網，請輸入 IP 位址。
子網遮罩(Subnet Mask)	如果位址類型為子網，請輸入子網路遮罩。
反向(Invert)	如果啟用此功能，將使用除上面輸入的位址之外的所有位址。
IPv6 設定(IPv6 Settings)	
符合類型(Match Type)	指定 IPv6 位址的符合類型（128 位元或字尾 64 位元）。
起始 IP 位址(Start IP Address)	如果位址類型為 IP，請輸入起始 IPv6 位址。 若要設定 IP 位址範圍，請在起始 IP 位址和結束 IP 位址欄位分別輸入不同的 IPv6 位址。
結束 IP 位址(End IP Address)	如果位址類型為 IP，請輸入結束 IPv6 位址。

IP 位址(IP Address)	如果位址類型為子網，請輸入 IPv6 位址。
前置碼長度(Prefix Length)	如果位址類型為子網，請輸入 IPv6 前置碼長度。
反向(Invert)	啟用此功能後，系統將使用所有位址，但不包含上述輸入的位址。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

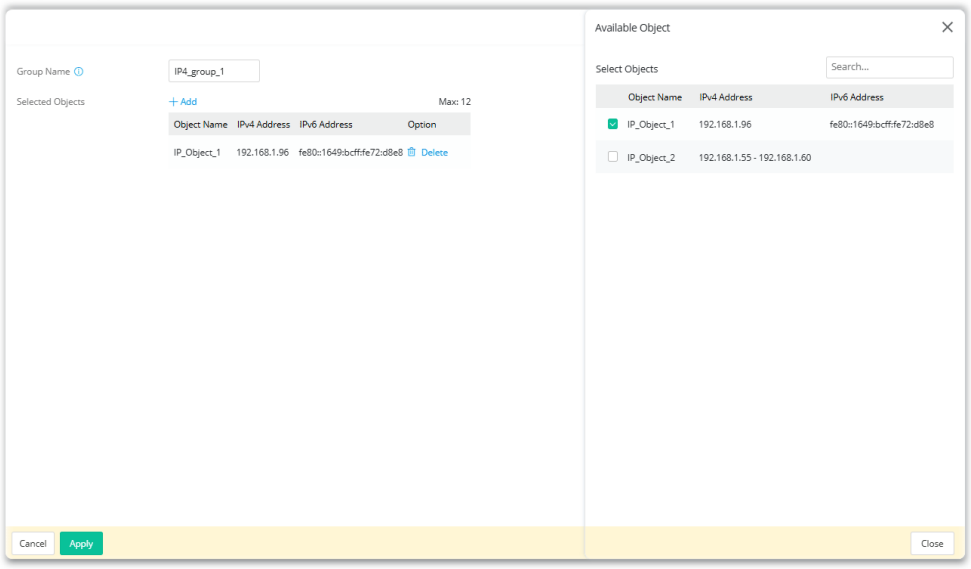
完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-1-13-2 IP 群組(IP Group)

本頁允許將數個 IPv4 物件/IPv6 物件納入一個 IPv4 群組 / IPv6 群組中。



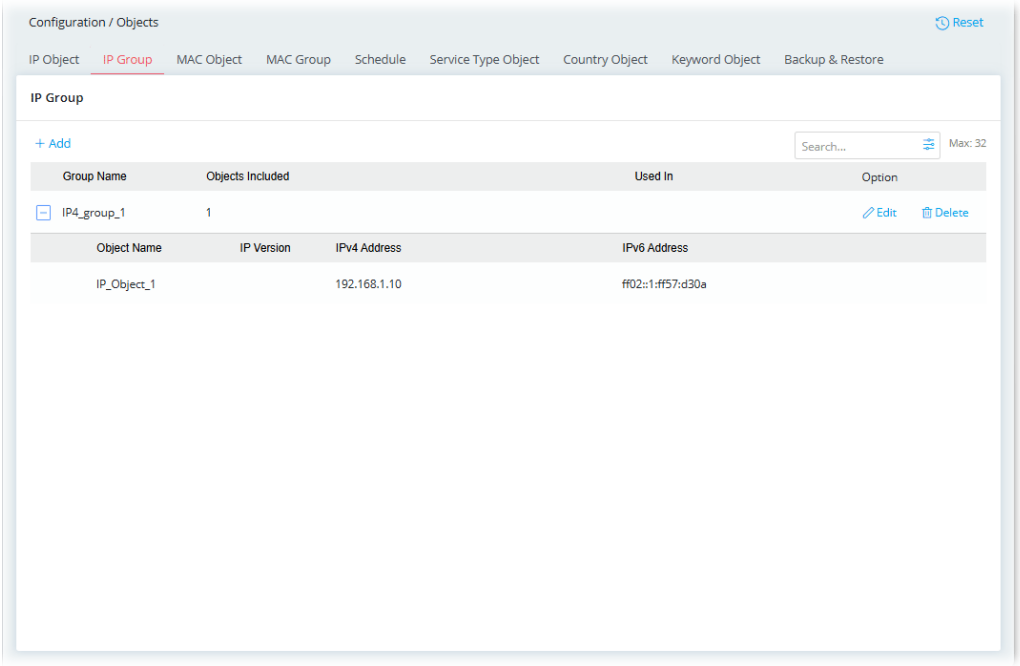
欲新增 IP 群組設定檔，請按下**+新增(+Add)**鏈結即可開啟如下頁面。



可用設定說明如下：

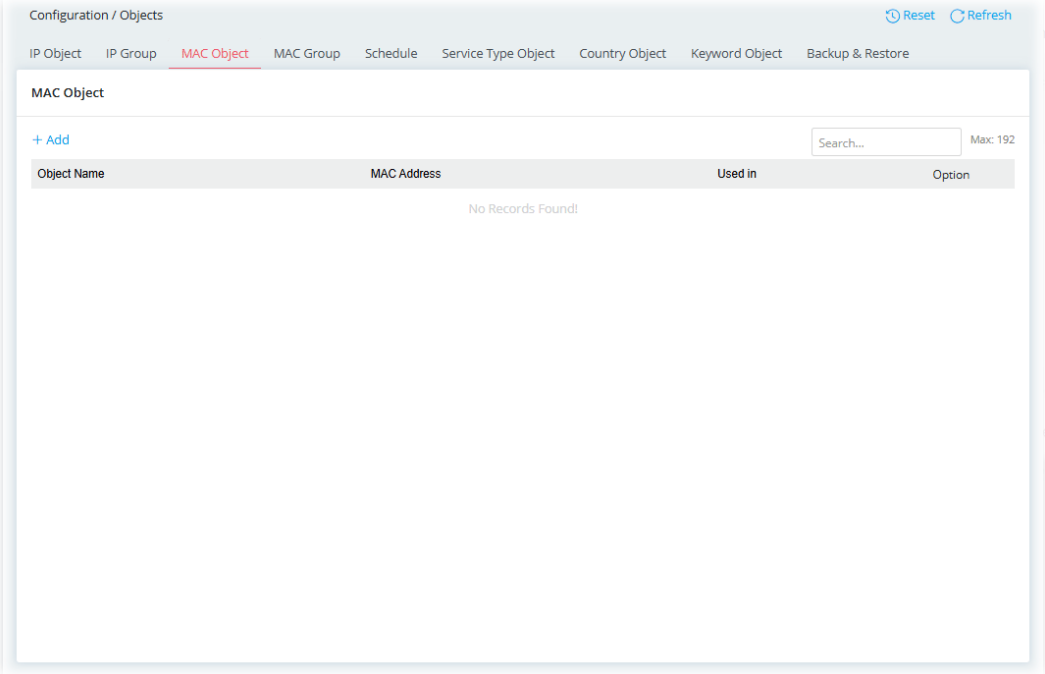
項目	說明
群組名稱(Group Name)	輸入一個用於識別此設定檔名稱。
選定物件(Selected Objects)	+新增(+Add) – 按此開啟包含可用物件的頁面。
可用物件(Available Object)	
搜尋(Search)	輸入 IP 物件名稱或 IPv4/IPv6 位址以搜尋相關 IP 物件。
選擇物件(Select Objects)	此處將顯示可用於分組的物件。選擇一個或多個物件，將其分組到目前 IP 群組下。
物件名稱(Object Name)	顯示目前存在的 IPv4/IPv6 物件。 若要將 IP 物件新增至目前 IP 群組，只需選擇所需的物件即可。選取的物件將顯示在左側的選定物件下方。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

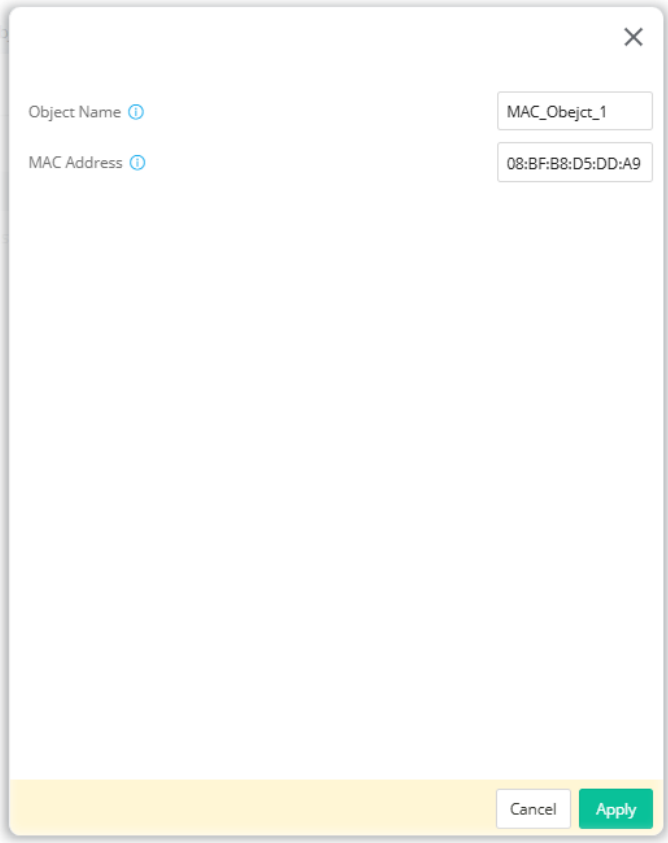


II-1-13-3 MAC 物件(MAC Object)

可以在 MAC 物件頁面中指定本機或遠端用戶端的 MAC 位址。



欲新增 MAC 物件設定檔，請按下**+新增(+Add)**鏈結即可開啟如下頁面。



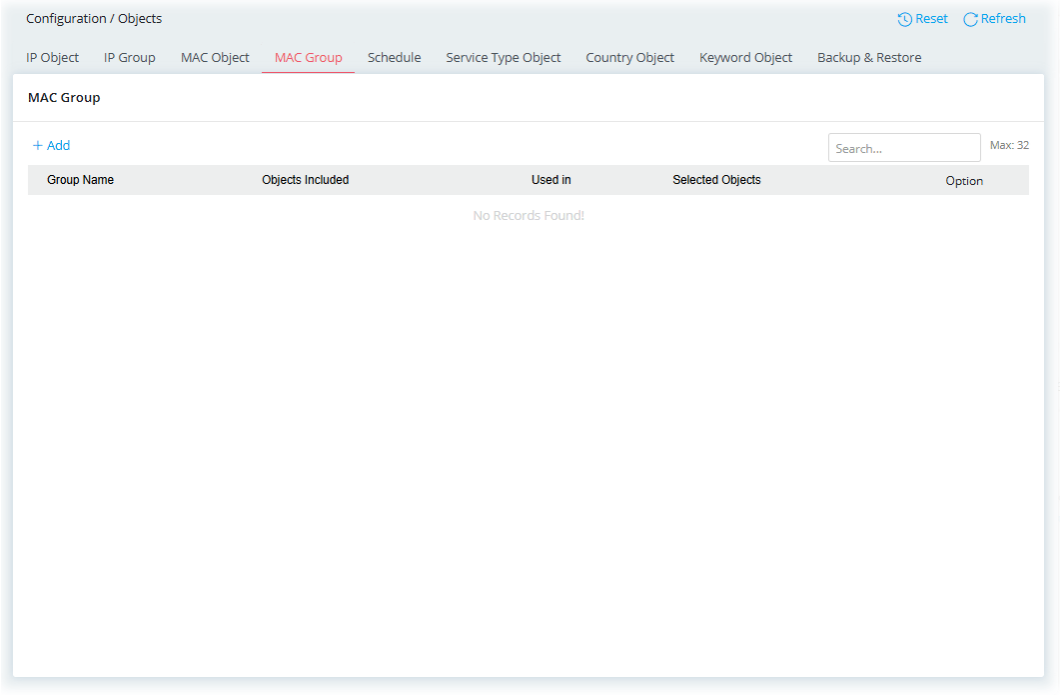
可用設定說明如下：

項目	說明
物件名稱(Object Name)	輸入一個用於識別此物件的名稱。
MAC 位址(MAC Address)	輸入用戶端的 MAC 位址。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

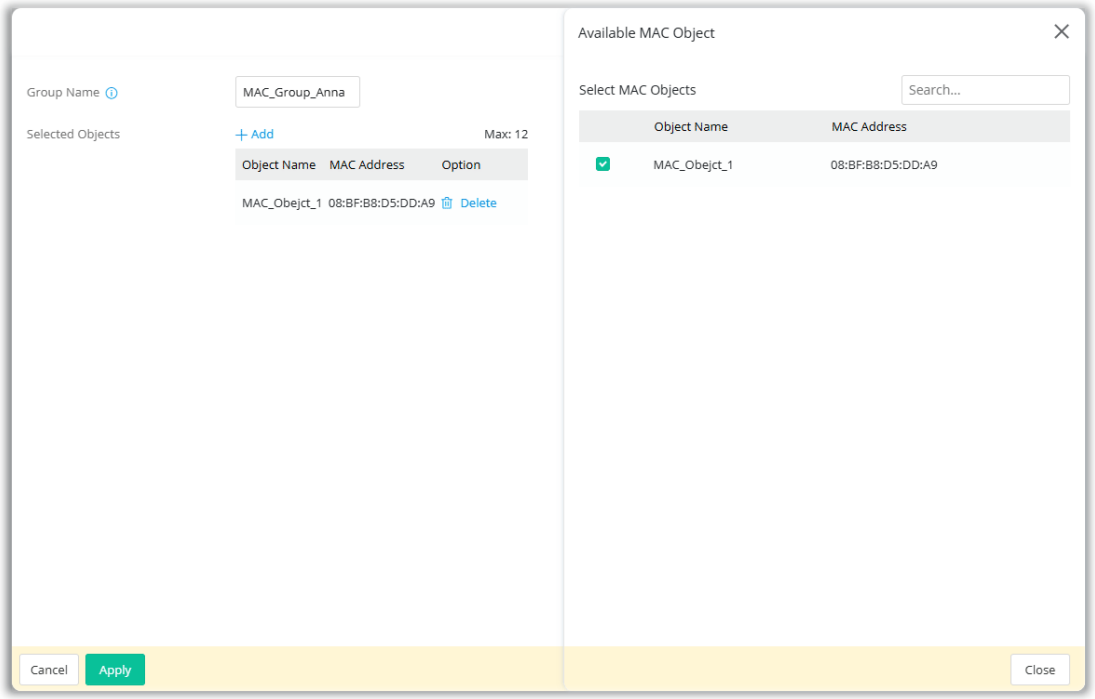
完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-1-13-4 MAC 群組(MAC Group)

本頁允許將數個 MAC 物件納入一個 MAC 群組中。



欲新增 MAC 群組設定檔，請按下**+新增(+Add)**鏈結即可開啟如下頁面。



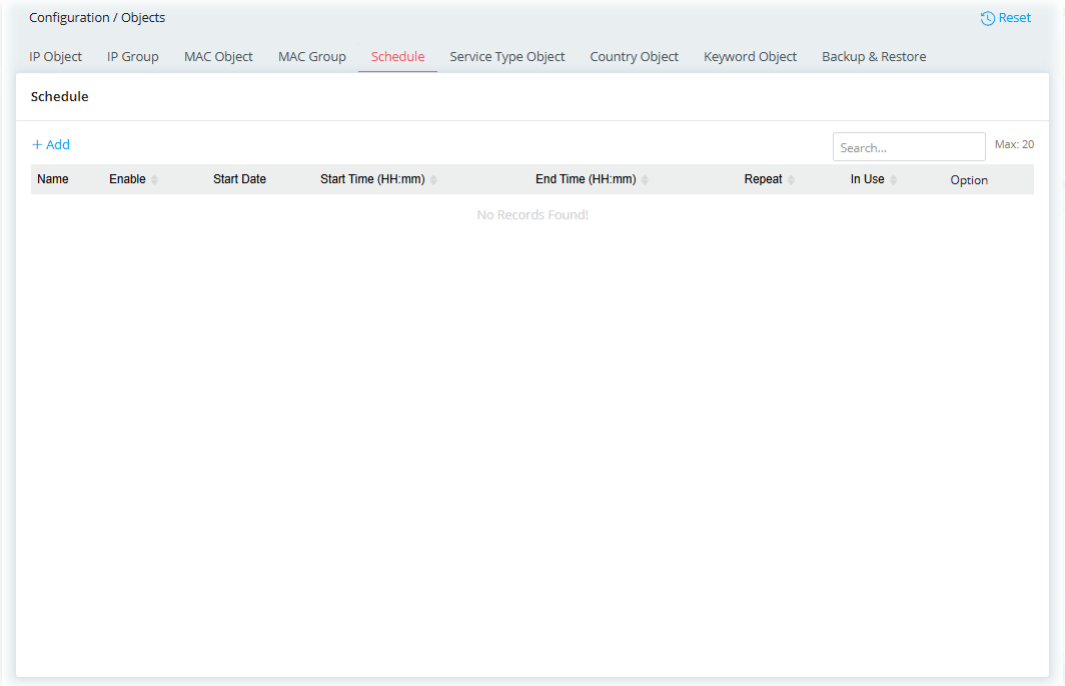
可用設定說明如下：

項目	說明
群組名稱(Group Name)	輸入一個用於識別此設定檔名稱。
選定物件(Selected Objects)	+新增(+Add) – 按此開啟包含可用物件的頁面。
可用的 MAC 物件(Available MAC Object)	
選擇 MAC 物件(Select MAC Objects)	搜尋(Search) - 輸入 MAC 物件名稱以顯示已存在的 MAC 物件。
物件名稱(Object Name)	選擇要納入目前 MAC 群組的物件。 選取的物件將顯示在左側的選定物件下方。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

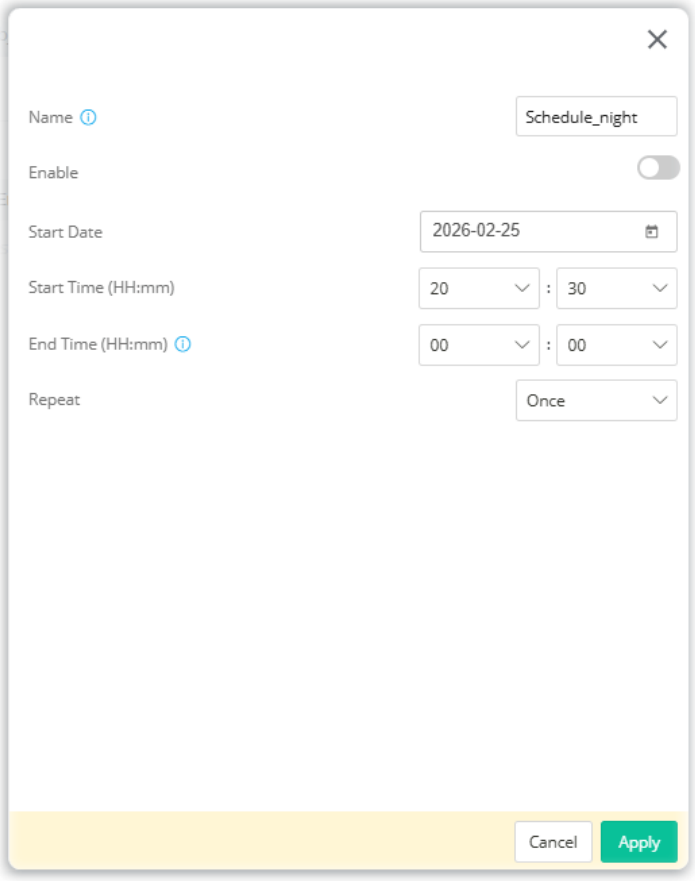
完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-1-13-5 排程(Schedule)

本頁可以建立時間排程表，可與支援排程功能的路由器一起使用，以便讓這些功能可以在預先設定的時間自動開啟和關閉。



欲新增排程設定檔，請按下**+新增(+Add)**鏈結即可開啟如下頁面。



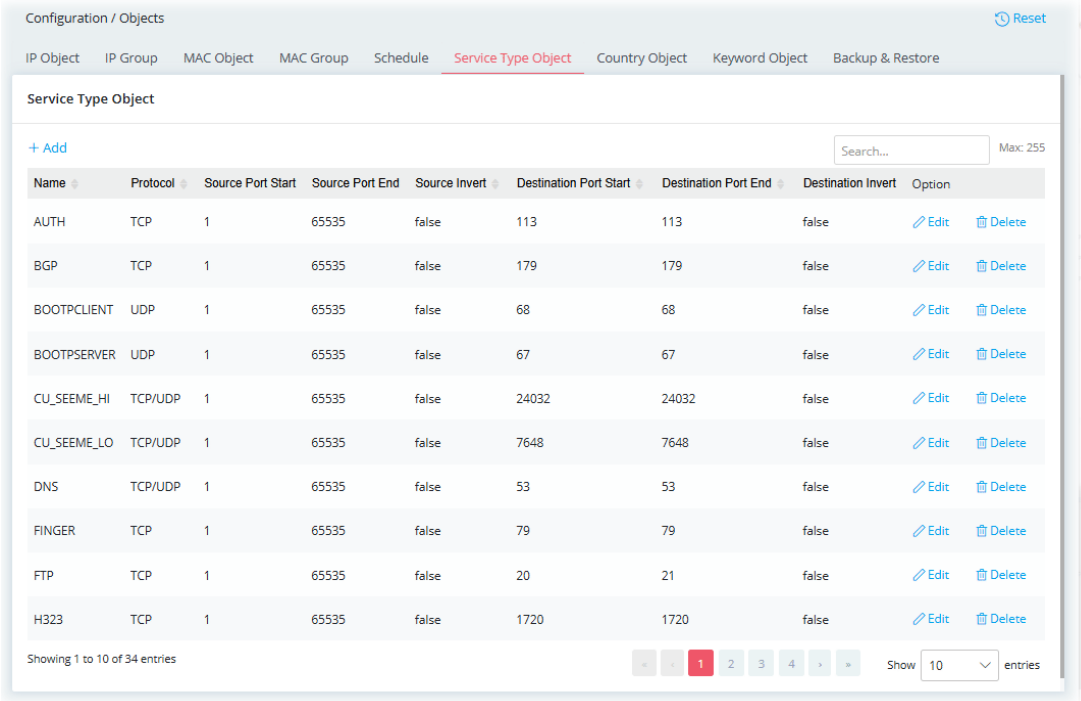
可用設定說明如下：

項目	說明
名稱(Name)	輸入排程設定檔的名稱。
啟用(Enable)	切換開關即可啟用或停用此日程安排設定檔。
起始日期(Start Date)	選擇此設定檔生效的日期。
起始時間(Start Time)	計劃觸發的時間。
結束時間(End Time)	設定行程結束時間。
重覆(Repeat)	**一次(Once)** - 此排程會根據以下條件觸發一次：日期、起始時間和結束時間。 **每天(Daily)** - 此排程每天都會根據起始時間和結束時間觸發。 ● **結束重複(End Repeat)** - 如果啟用此功能，則排程將每天觸發，直到結束重複日期中定義的日期為止。 ● **結束重複日期(End Repeat Date)** - 排程將於指定日期結束。 **每週(Weekly)** - 此排程將於所選星期的指定起始時間觸發，並持續至結束時間。 ● **每(Every)** - 選擇觸發排程的日期。 ● **結束重複(End Repeat)** - 如果啟用此功能，則排程將每周觸發，直到結束重複日期中定義的日期為止。 ● **結束重複日期(End Repeat Date)** - 排程將於指定日期結束。 **每月(Monthly)** - 此排程將根據日期設定按月觸發。例如，選擇 2022 年 4 月 27 日作為日期設定。之後，此計劃將在每月 27 日觸發。 ● **結束重複(End Repeat)** - 如果啟用此功能，則排程將每月觸發，直到結束重複日期中定義的日期為止。 ● **結束重複日期(End Repeat Date)** - 排程將於指定日期結束。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

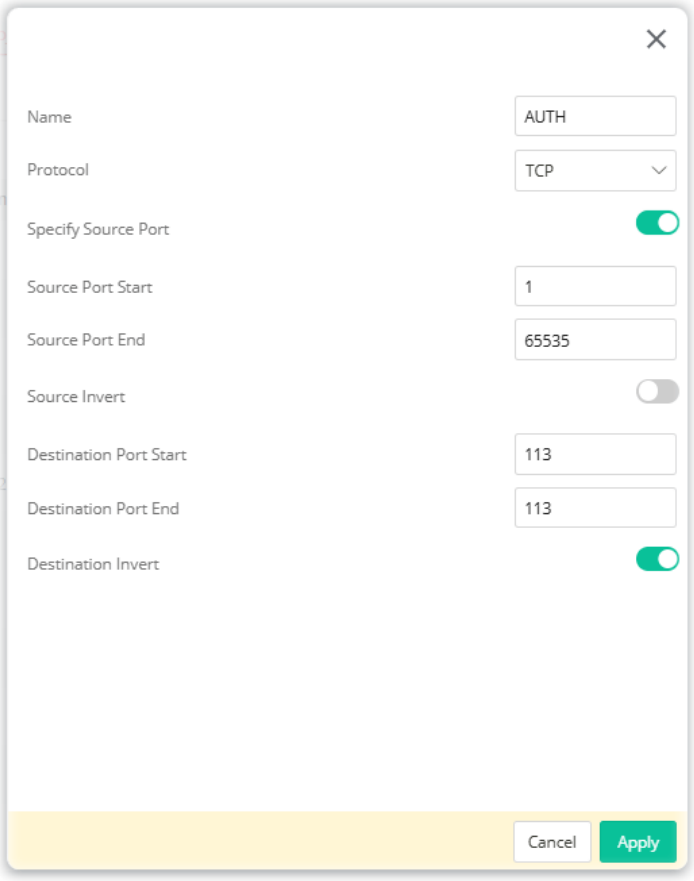
完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-1-13-6 服務類型物件(Service Type Object)

最多可以建立 255 個服務類型物件。



欲新增/編輯服務類型物件設定檔，請按下**+新增(+Add)/編輯(Edit)**鏈結即可開啟如下頁面。



可用設定說明如下：

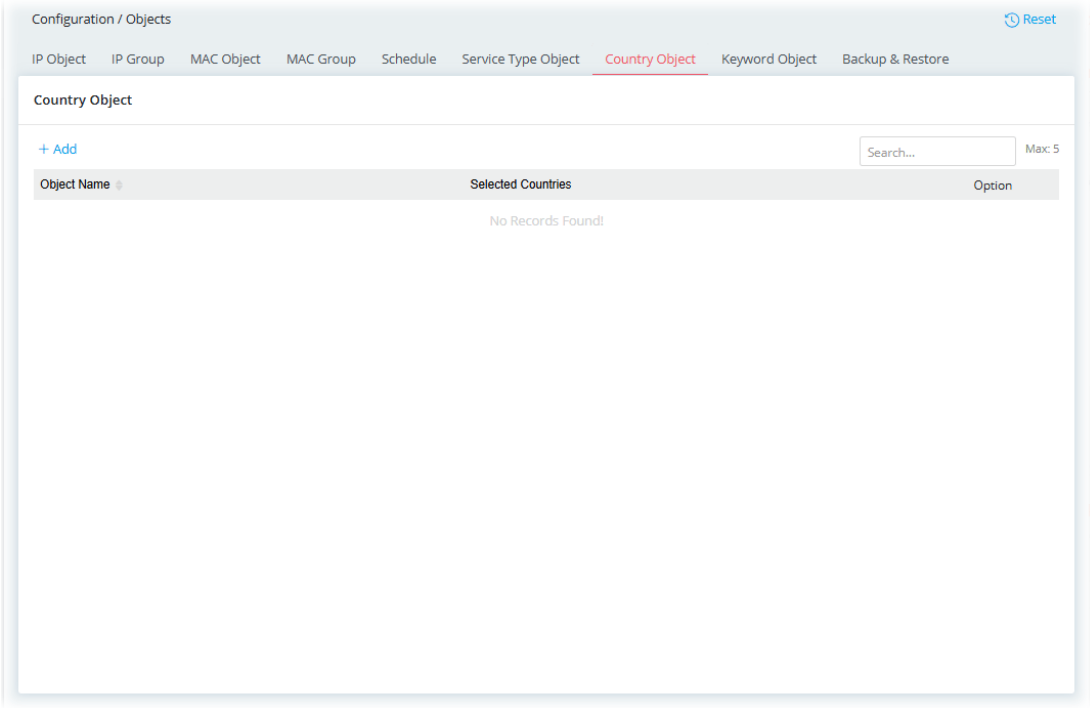
項目	說明
名稱(Name)	輸入辨識用的設定檔名稱。最多可包含 15 個字元。
通訊協定(Protocol)	選擇適合此設定檔的通訊協定。 **任一(Any)** – 所有的通訊協定。 **ICMP / ICMPv6** – 網際網路控制訊息協定。 **IGMP** – 網際網路群組管理協定。 **TCP** – 傳輸控制協定。 **UDP** – 使用者資料包協定。 **TCP/UDP** – 傳輸控制協定與使用者資料包協定。 **其他(Other)** – 其他未列出的通訊協定。請在文字方塊中輸入通訊協定編號。
指定來源埠號(Specify Source Port)	當選擇的通訊協定包含 TCP 或 UDP 時，可以指定來源連接埠和目的連接埠。 切換開關以啟用/停用來源連接埠號設定。 **起始來源埠號/結束來源埠號(Source Port Start / Source Port End)** – 輸入此二值來定義來源連接埠的連接埠範圍。 **來源反向(Source Invert)** - 如果啟用此功能，則將使用除上面輸入的連接埠值(來源連接埠起始/結束)以外的所有連接埠值。
起始目的埠號/結束目的埠號（Destination Port Start / Destination Port End)	當選擇的通訊協定包含 TCP 或 UDP 時，可以指定來源連接埠和目的連接埠。
目的反向(Destination Invert)	如果啟用此功能，則將使用除上面輸入的連接埠值(目的連接埠起始/結束)之外的所有連接埠值。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

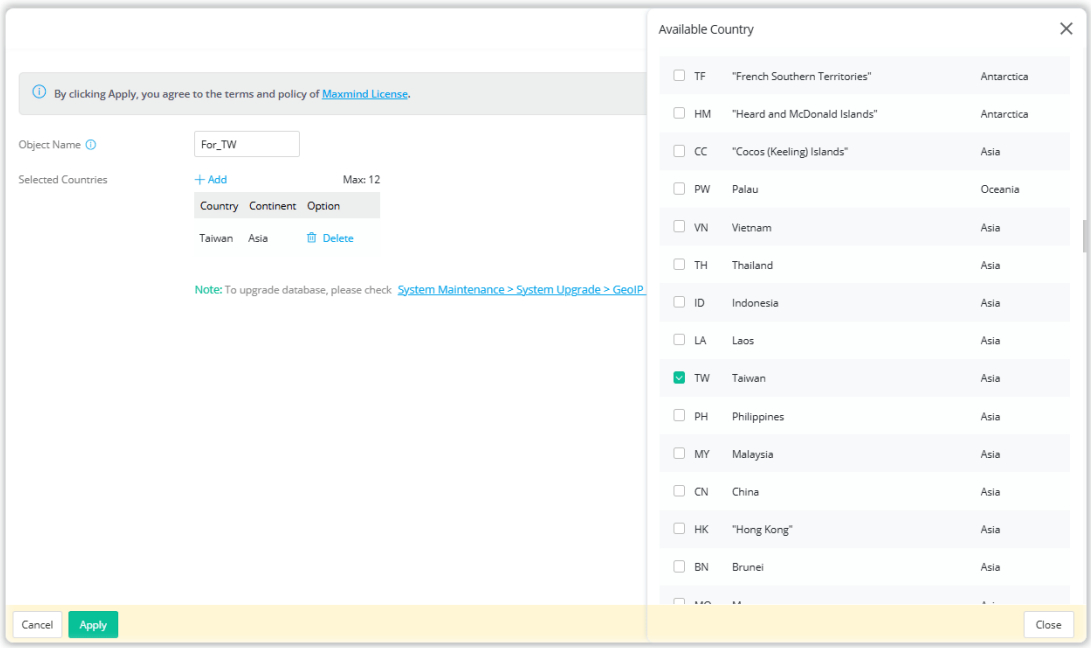
II-1-13-7 國家物件(Country Object)

國家物件設定檔可以確定 Vigor 路由器的防火牆應阻止哪些國家。

最多可建立 5 個國家物件設定檔文件，作為黑名單或白名單之用。



欲新增國家物件設定檔，請按下**+新增(+Add)鏈結**即可開啟如下頁面。



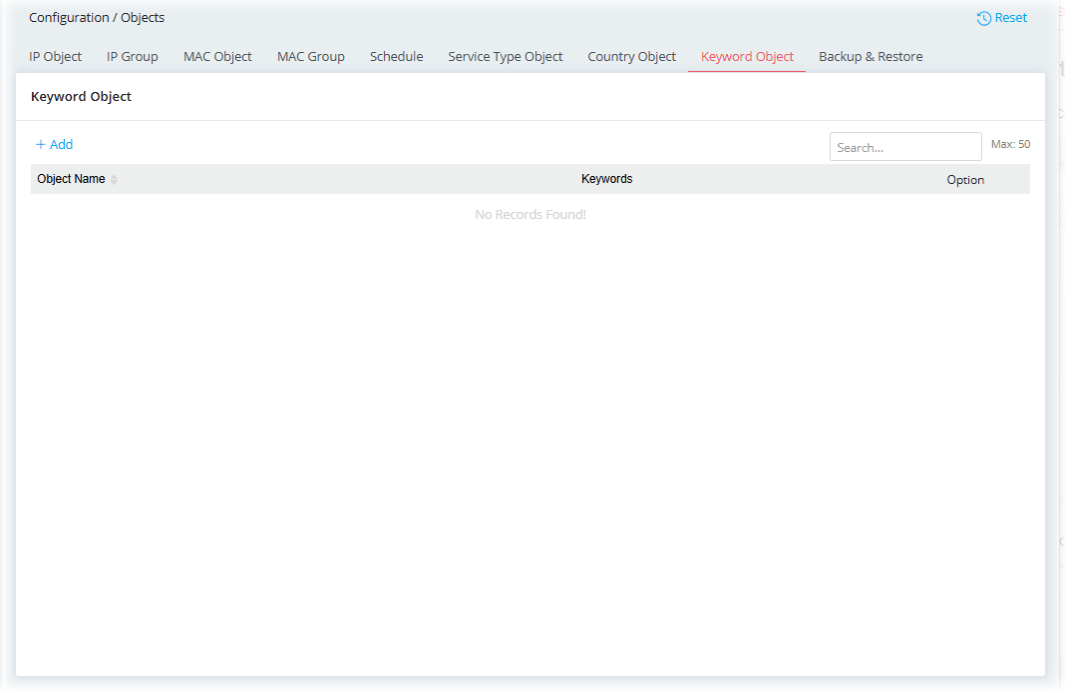
可用設定說明如下：

項目	說明
物件名稱(Object Name)	作為辨別用之設定檔名稱。長度最多為 63 個字元。
選定國家 (Selected Countries)	**+新增(+Add)** - 按此選擇可用的國家物件。右側將顯示國家/地區代碼清單。最多可選擇 12 個代碼。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

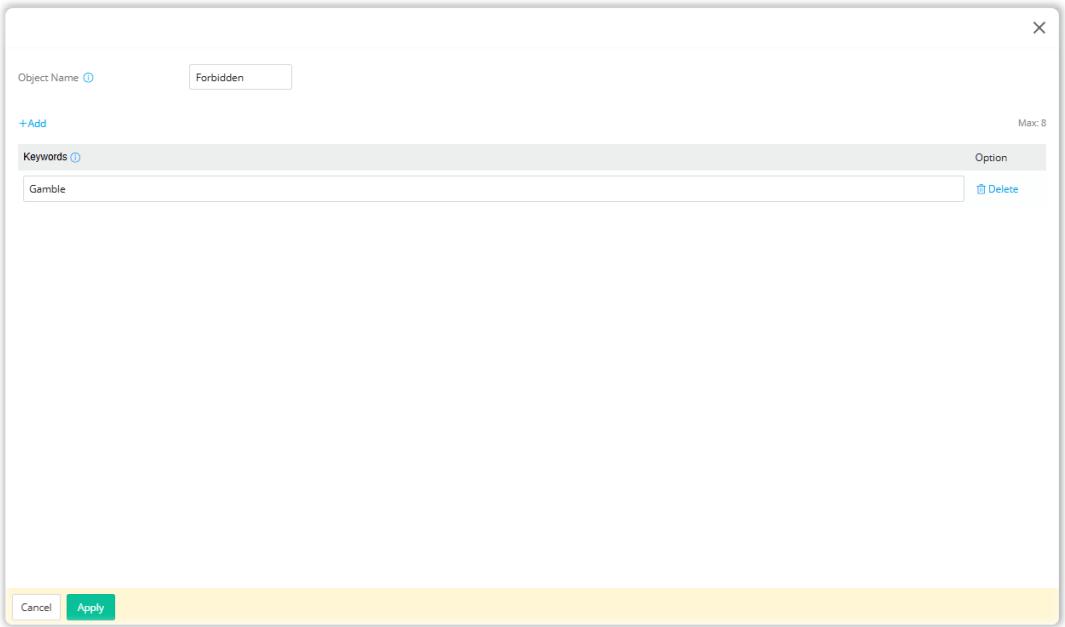
完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-1-13-8 關鍵字物件(Keyword Object)

本頁允許建立 50 個關鍵字物件設定檔，用作黑名單或白名單。



欲新增關鍵字設定檔，請按下**+新增(+Add)鏈結**即可開啟如下頁面。



可用設定說明如下：

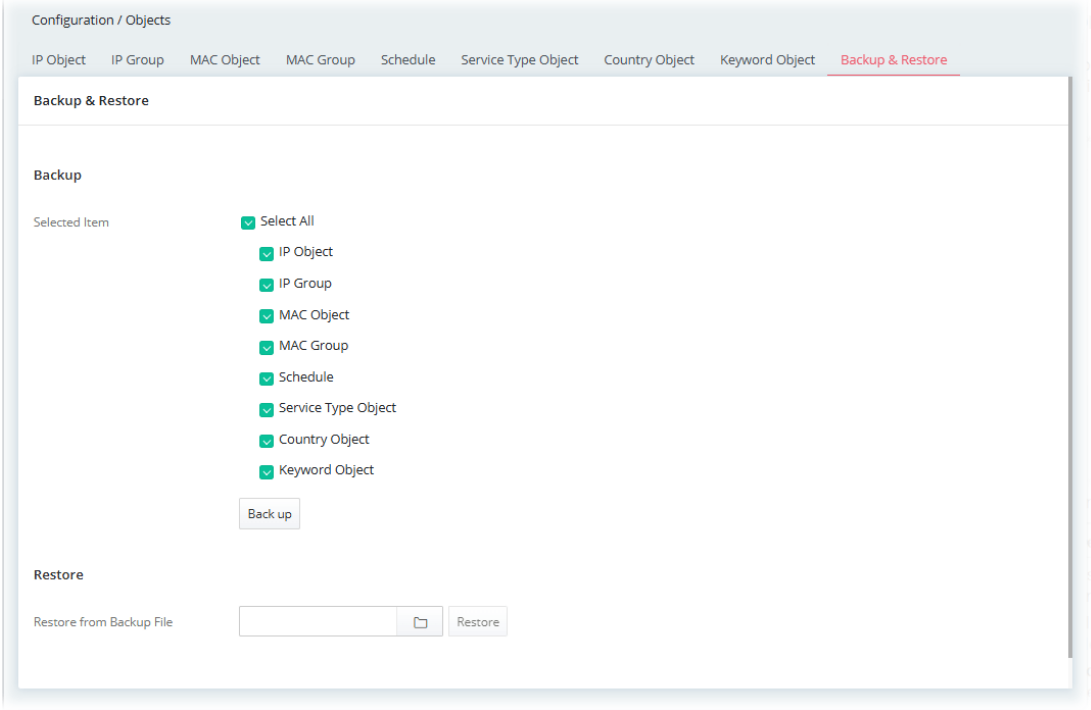
項目	說明
物件名稱(Object Name)	輸入此設定檔名稱。最多可包含 16 個字元。
關鍵字(Keywords)	定義用來匹配的關鍵字。 輸入此設定檔的內容。例如，內容中輸入 *gambling*。當您瀏覽網頁時，包含賭博資訊(gambling)的頁面將被監視，並依照防火牆設定進行攔截或是放行。

	此外，最多可以輸入 3 個關鍵字詞組，短語之間以空格分隔，總長度不超過 63 個字元。如果關鍵字短語中包含空格，請將空格替換為 %20。例如，“keep out” 應輸入為 “keep%20out” 。
刪除(Delete)	按此可移除選定的輸入項目。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-1-13-9 備份與還原(Backup & Restore)

物件設定可以備份為檔案。未來如果有需要，可以將備份檔案匯入此裝置以還原設定。



可用設定說明如下：

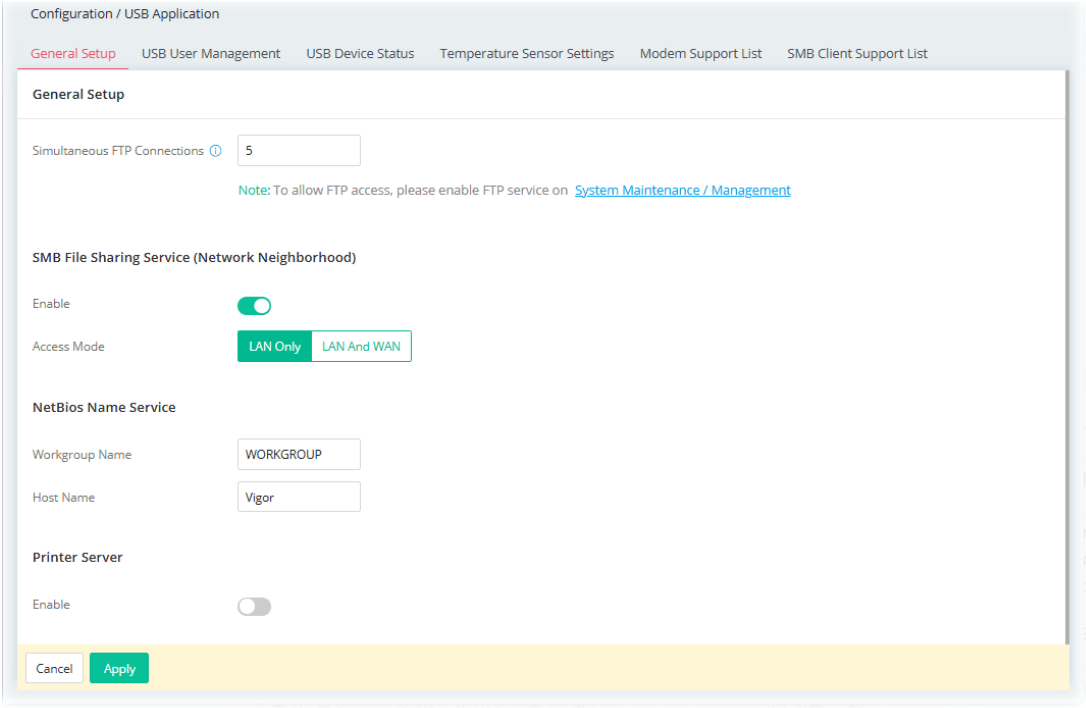
項目	說明
備份(Backup)	一般來說，使用者可以透過網頁上的物件選項來建立物件。 按下載按鈕，即可將所有物件(或範本)儲存並匯出為檔案。 **備份(Back up)** – 按此可將目前物件備份到檔案上。此檔案將來可用於還原。
還原(Restore)	**還原自備份檔案(Restore from Backup File)** – 按此以指定先前備份的檔案。 **還原(Restore)** – 按此執行復原操作。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-1-14 USB 應用

II-1-14-1 基本設定(General Settings)

此頁面可讓您設定 Vigor 路由器的檔案共用功能，讓 USB 大容量儲存裝置（例如隨身碟和硬碟等）可供 LAN 用戶端存取。



可用設定說明如下：

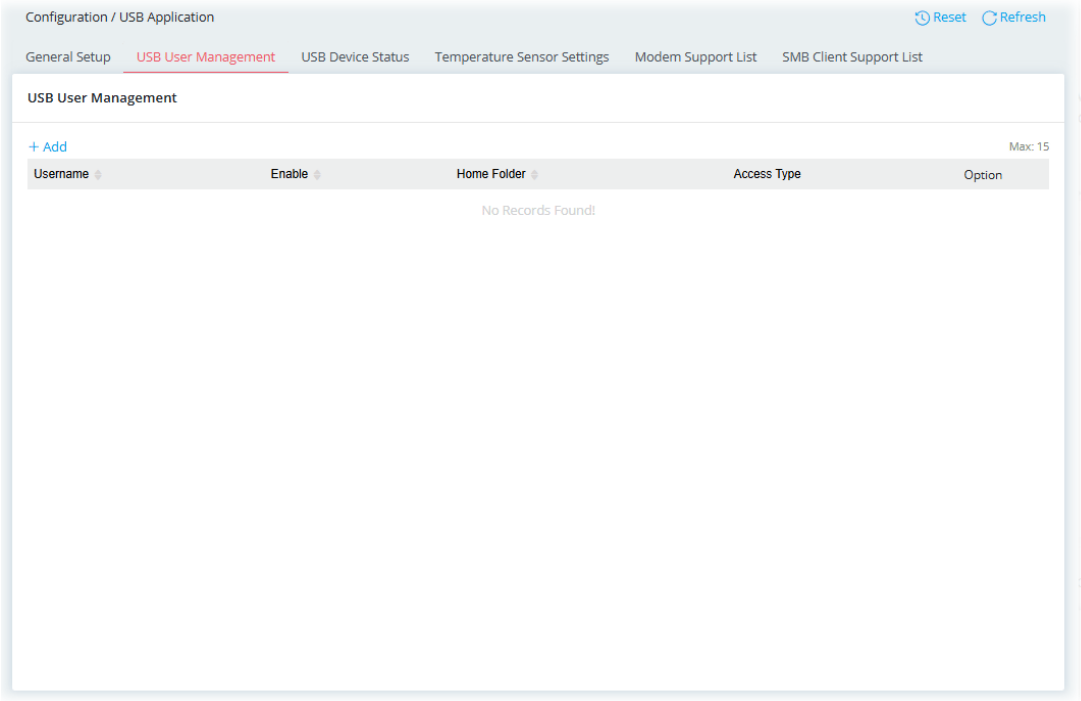
項目	說明
同步 FTP 連線 (Simultaneous FTP Connections)	輸入允許的最大同步 FTP 連線數。路由器最多允許 6 個同步連線數。
SMB 檔案分享服務(網路芳鄰) (SMB File Sharing Service (Network Neighborhood))	按下**啟用(Enabled)**以透過路由器啟動 SMB 檔案共享服務。 **存取模式(Access Mode) –** 選擇檔案分享服務的存取模式。 ● **限用 LAN(LAN Only) –** 來自網際網路端的使用者無法連接至路由器的 SMB 伺服器。 ● **LAN 與 WAN (LAN And WAN) -** LAN 和 WAN 使用者都可以存取路由器的 SMB 伺服器。
NetBios 名稱服務 (NetBios Name Service)	對於 USB 儲存磁碟的 NetBIOS 服務，您必須指定工作群組名稱和主機名稱。工作群組名稱不能與主機名稱相同。工作組名稱最多可包含 15 個字元，主機名稱最多可包含 23 個字元。兩者都不能包含以下任何一個字元：; : " < > * + = \ | ?。 **工作群組名稱(Workgroup Name) –** 輸入工作群組的名稱。 **主機名稱(Host Name) –** 輸入路由器的主機名稱。
印表機伺服器(Printer Server)	切換此開關以啟用/停用印表機伺服器功能。 若啟用此功能，路由器將充當透過 USB 連接之印表機的列印伺服器。
取消(Cancel)	捨棄目前設定。

套用(Apply)	儲存目前設定。

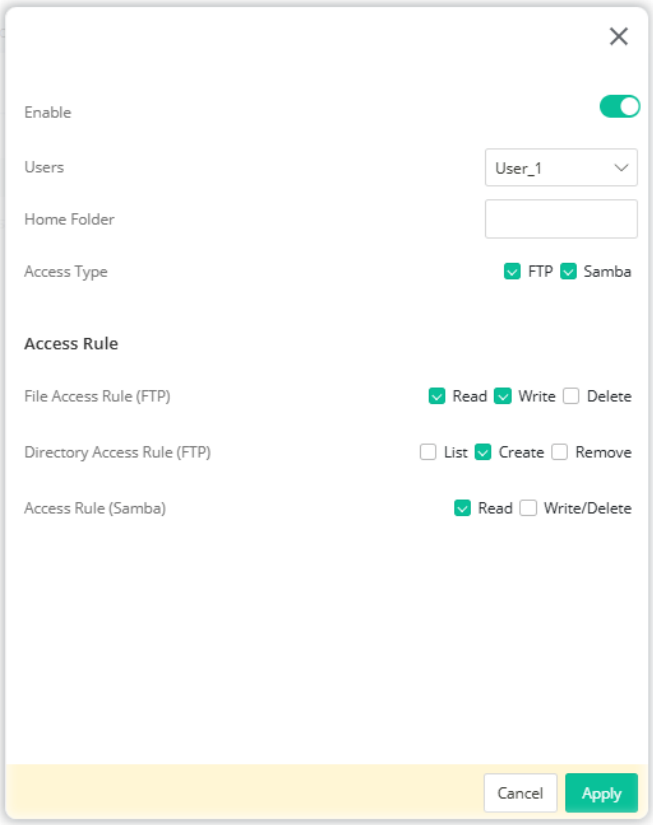
完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-1-14-2 USB 使用者管理(USB User Management)

此頁面可讓您為 FTP/SMB 使用者設定設定檔。任何想要存取 USB 儲存磁碟的使用者都必須使用在此頁面上設定的使用者名稱和密碼進行身份驗證。



欲新增設定檔，按下**+新增(+Add)**開啟如下頁面：



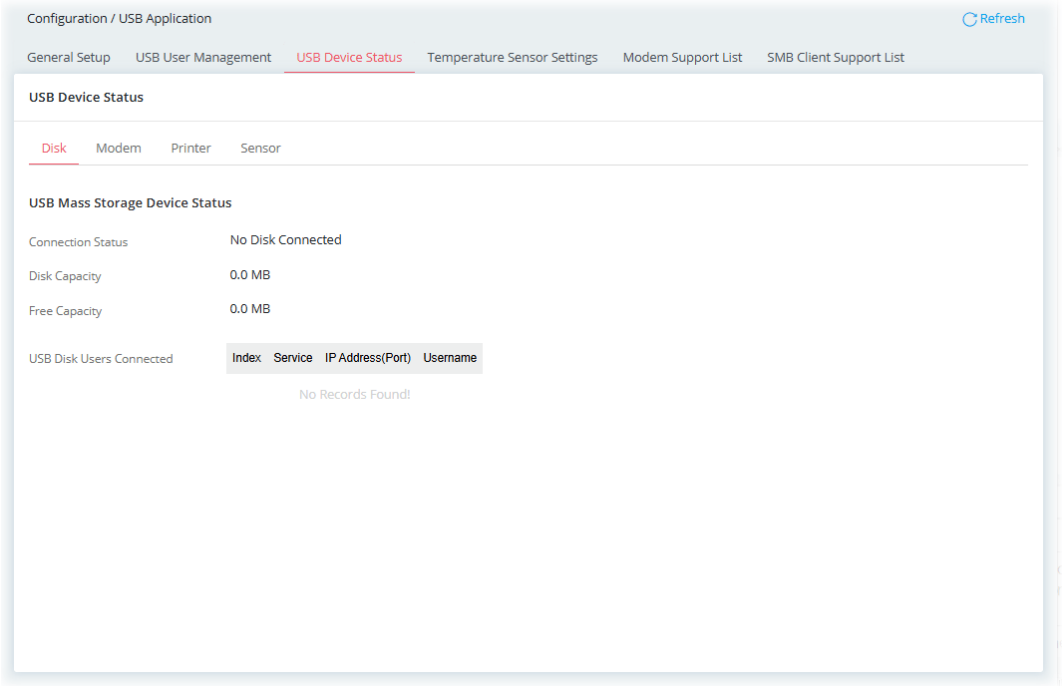
可用設定說明如下：

項目	說明
啟用(Enable)	切換此開關以啟用/停用此設定檔。
使用者(Users)	使用下拉清單選擇既有使用者帳戶（於 IAM>>使用者和群組>>使用者(IAM>>Users & Groups>>Users)中建立）。
Home 資料夾 (Home Folder)	輸入資料夾名稱，該資料夾將作為使用此使用者設定檔憑證建立的 FTP 和 SMB 連線數之根資料夾。使用者只能存取此根資料夾內的資料夾和檔案。
連線方式類型 (Access Type)	**FTP** - 允許您透過 FTP 服務存取和控制遠端 PC。 **Samba** - 允許您透過 Samba 服務存取和控制遠端 PC。
存取規則(Access Rule)	決定設定檔的權限。任何使用該設定檔存取 USB 儲存磁碟的使用者都必須遵守此處設定的規則。 **檔案存取規則(FTP) (File Access Rule (FTP))** – 勾選設定檔的權限（讀取、書寫和刪除）。 **目錄存取規則 (FTP)(Directory Access Rule (FTP))** – 勾選設定檔的選項（清單、建立和移除）。 **存取規則(Samba)(Access Rule (Samba))** – Check the items (Read, Write/Delete) for such profile. 勾選設定檔的選項(讀取、書寫和刪除）。
取消(Cancel)	捨棄目前設定並回到前一頁。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-1-14-3 USB 裝置狀態(USB Device Status)

此頁面允許監測連接到 Vigor 路由器的 USB 裝置（磁碟、數據機、印表機和感應器）的狀態。



可用設定說明如下：

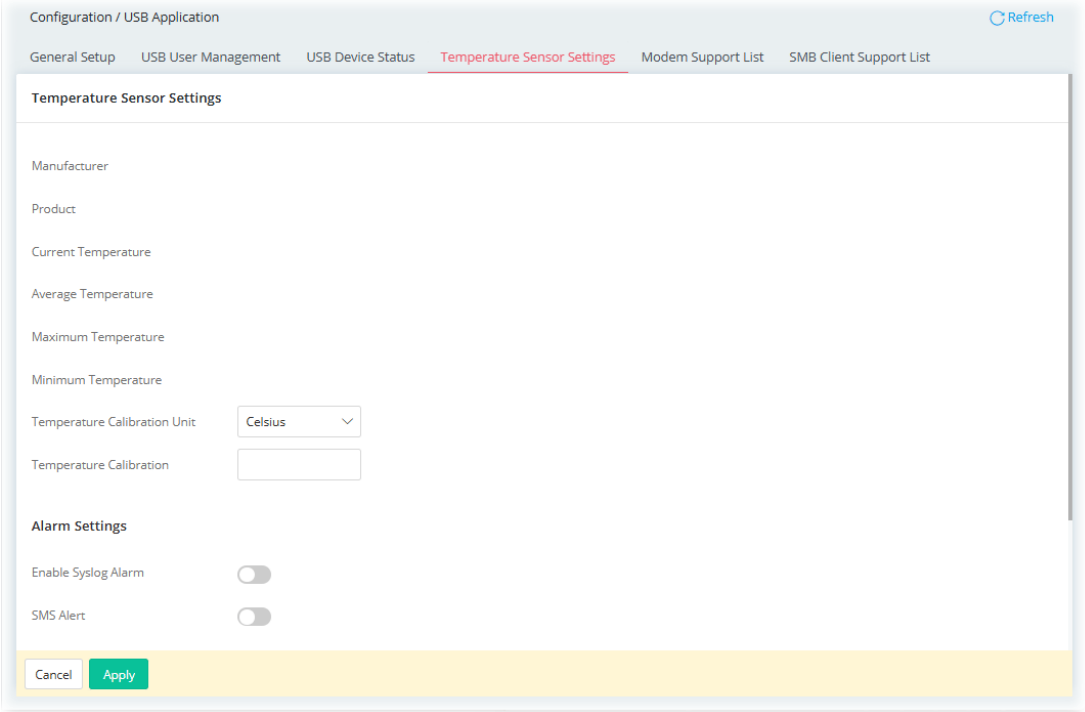
項目	說明
連線狀態(Connection Status)	顯示是否連接了 USB 磁碟。如果 Vigor 路由器上沒有連接任何 USB 裝置，則會顯示無連接任何磁碟。。
磁碟容量(Disk Capacity)	顯示 USB 磁碟的全部容量。
剩餘容量(Free Capacity)	顯示 USB 磁碟的可用空間。隨時按下**頁面更新(Refresh)**按鈕即可取得最新可用空間。
USB 磁碟使用者已連線(USB Disk Users Connected)	顯示已連線至 SMB/FTP 伺服器的用戶端資訊。 **索引(Index)** – 用戶端用於建立連線的設定檔索引。 **服務(Service)** – 顯示連線使用的是 FTP 還是 SMB。 **IP 位址(IP Address)** – 顯示用戶端的 IP 位址。 **使用者名稱(Username)** – 顯示用於建立連線的使用者名稱。

II-1-14-4 溫度感應器設定(Temperature Sensor Settings)

USB 溫度計可與您已安裝的 DrayTek 路由器搭配使用，協助您監視伺服器或資料通訊機房的環境，並在機房過熱時發出通知。

尤其是在夏季時，可確保您的伺服器或數據通訊設備不會因冷卻系統故障而過熱。

與 Vigor 路由器相容的 USB 溫度計將持續監視環境溫度。當溫度達到預設門檻值時，您將收到電子郵件或簡訊通知，以便採取相應措施。



可用設定說明如下：

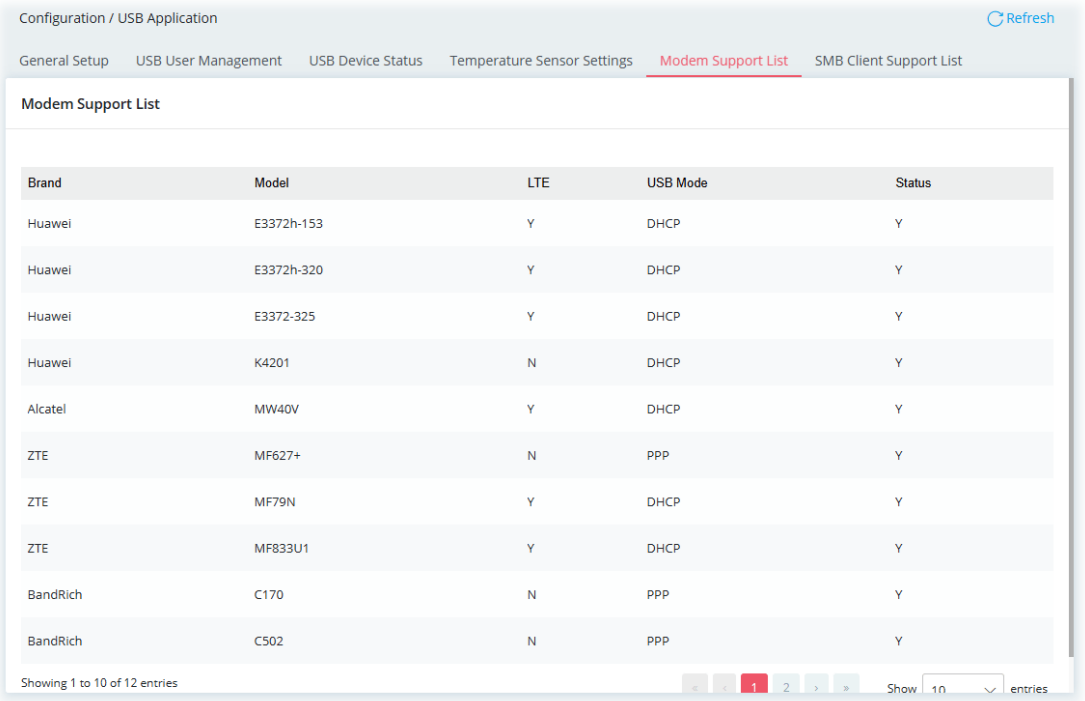
項目	說明
溫度感應器設定(Temperature Sensor Settings)	顯示與製造商、產品、目前溫度、平均溫度、最高溫度和最低溫度相關的資訊。 **溫度校正單位(Temperature Calibration Unit)** -選擇要使用的溫度單位。 **溫度校正(Temperature Calibration)** – 輸入實際溫度與溫度計讀數之間的差值。
警報設定(Alarm Settings)	**啟用 Syslog 警報功能(Enable Syslog Alarm)** – 選此可啟用在系統日誌中記錄溫度。 **簡訊警示(SMS Alert)** – 切換開關即可啟用/停用簡訊警示。 ● **傳送警示簡訊至(Send Alert SMS to)** – 選擇簡訊發送者設定檔（在 IAM>>使用者和群組>>使用者(IAM>>Users & Groups>>Users)、系統維護>>帳號與許可>>本機管理帳號(System Maintenance>>Account & Permission>>Local Admin Account) 中建立）。 **電子郵件警示(Email Alert)** – 切換開關即可啟用/停用電子郵件警示。 ● **傳送警示郵件至(Send Alert Email to)** – 選擇郵件發送者設定檔（在 IAM>>使用者和群組>>使用者(IAM>>Users & Groups>>Users)、系統維護>>帳號與許可>>本機管理帳號(System Maintenance>>Account & Permission>>Local Admin Account) 中建立）。 **溫度下限/溫度上限(Lower temperature limit / Upper temperature**

	limit)– 輸入溫度上限和下限。如果溫度超出此範圍，系統將發出警報。
取消(Cancel)	捨棄目前設定。
套用(Apply)	儲存目前設定。

II-1-14-5 數據機支援清單(Modem Support List)

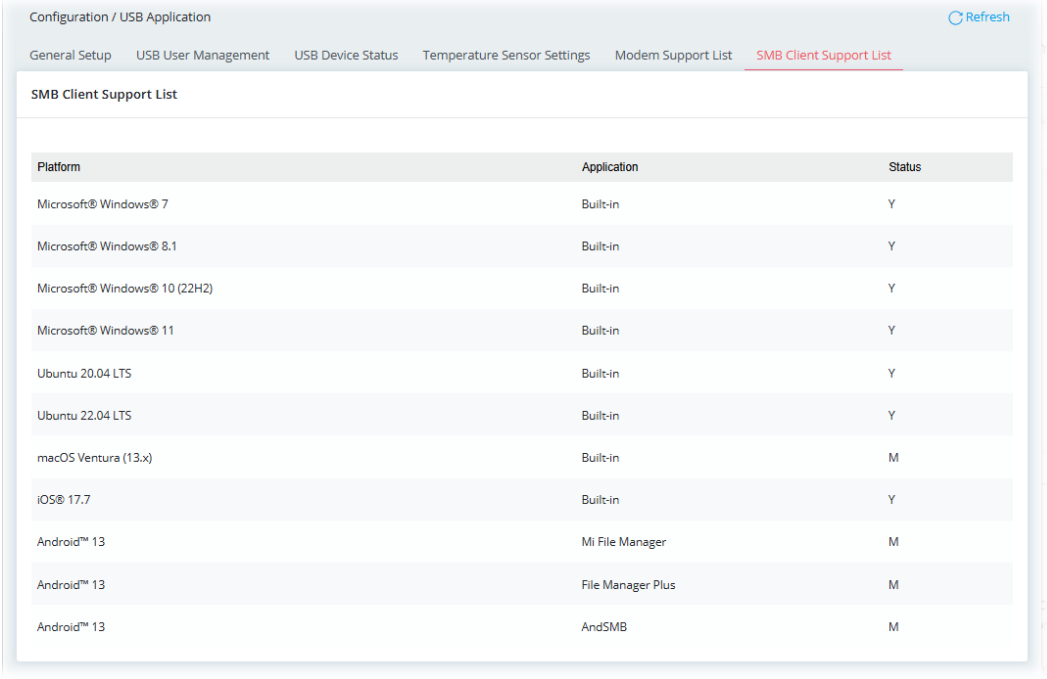
本頁面列出了 Vigor 路由器支援的 USB 數據機品牌和型號。

隨著韌體版本更新而新增支援之新型數據機，此列表可能會有所變化。



II-1-14-6 SMB 用戶端支援清單(SMB Client Support List)

SMB 用戶端支援清單提供在不同平台上執行的檔案共用應用程式的測試狀態資訊。

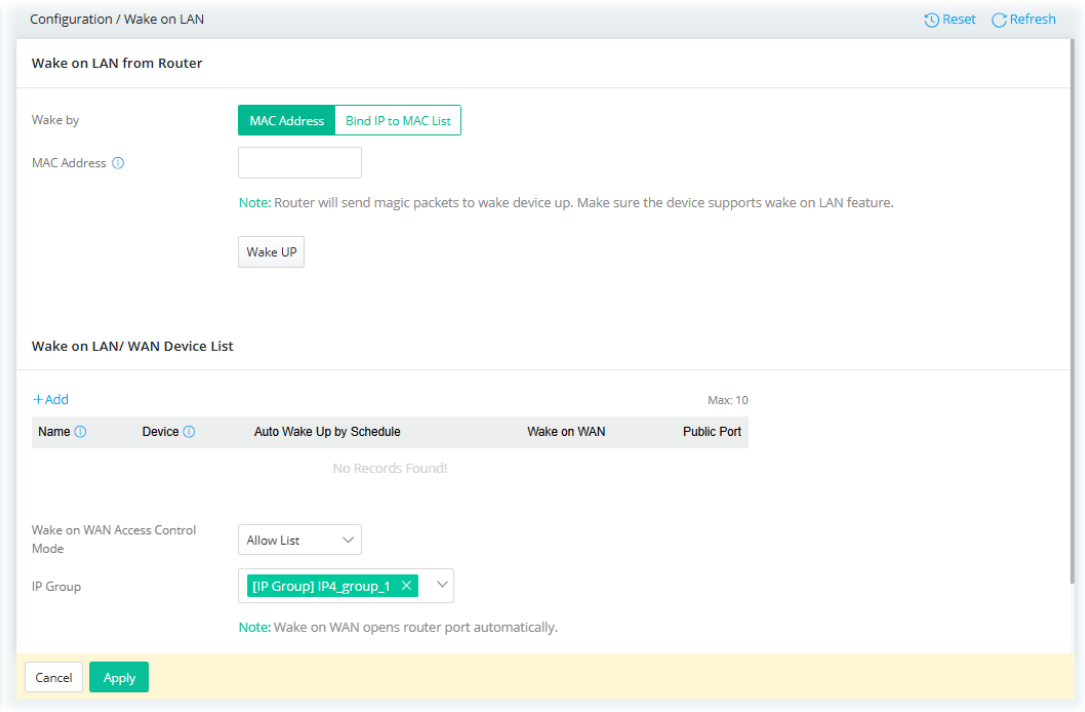


II-1-15 網路喚醒(Wake on LAN)

使用網路喚醒（WoL）功能，支援 WoL 的 LAN 用戶端可以透過網路開啟或從睡眠狀態恢復，而無需實體存取裝置。

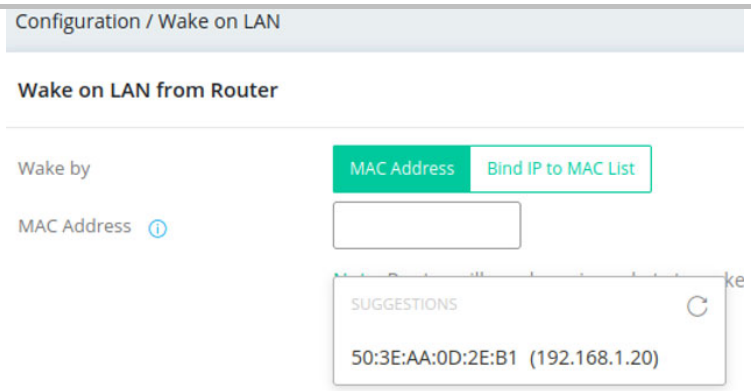
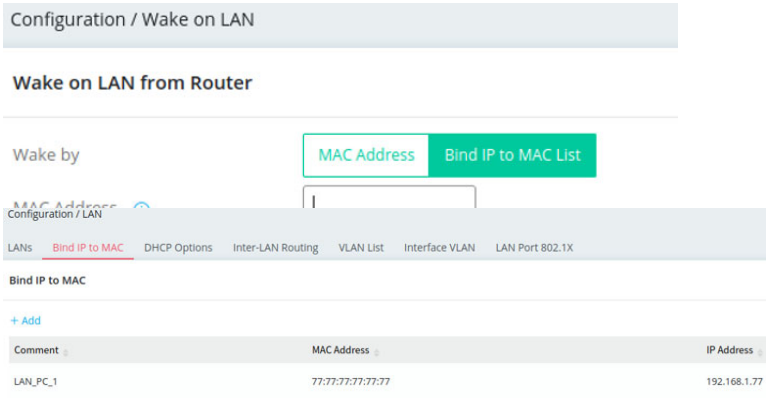
為了使區域網路用戶端能夠從睡眠或關機狀態喚醒，必須將網路卡設定為監聽網路喚醒（Wake-on-LAN）訊息。有關如何設定網路介面以啟用網路喚醒（Wake-on-LAN）的詳細訊息，請參閱區域網路用戶端的文件。

如果您希望能夠選擇 Wake-on-LAN 用戶端的 IP 位址，則必須先使用將 IP 綁定到 MAC 功能將其 MAC 位址綁定到固定 IP 位址。



可用設定說明如下：

項目	說明
從路由器透過 LAN 喚醒電腦(Wake on LAN from Router)	
喚醒方式 **(Wake by)**	要喚醒的區域網路用戶端的位址類型。 ● **MAC 位址(MAC Address)** ● **綁定 IP 至 MAC 清單(Bind IP to MAC List)**
MAC 位址(MAC Address)	此處提供的 MAC 位址將是 Vigor 路由器將喚醒的裝置位址。 如果在喚醒方式中選擇 MAC 位址，則在 ARP 列表中會顯示內容供您選擇。

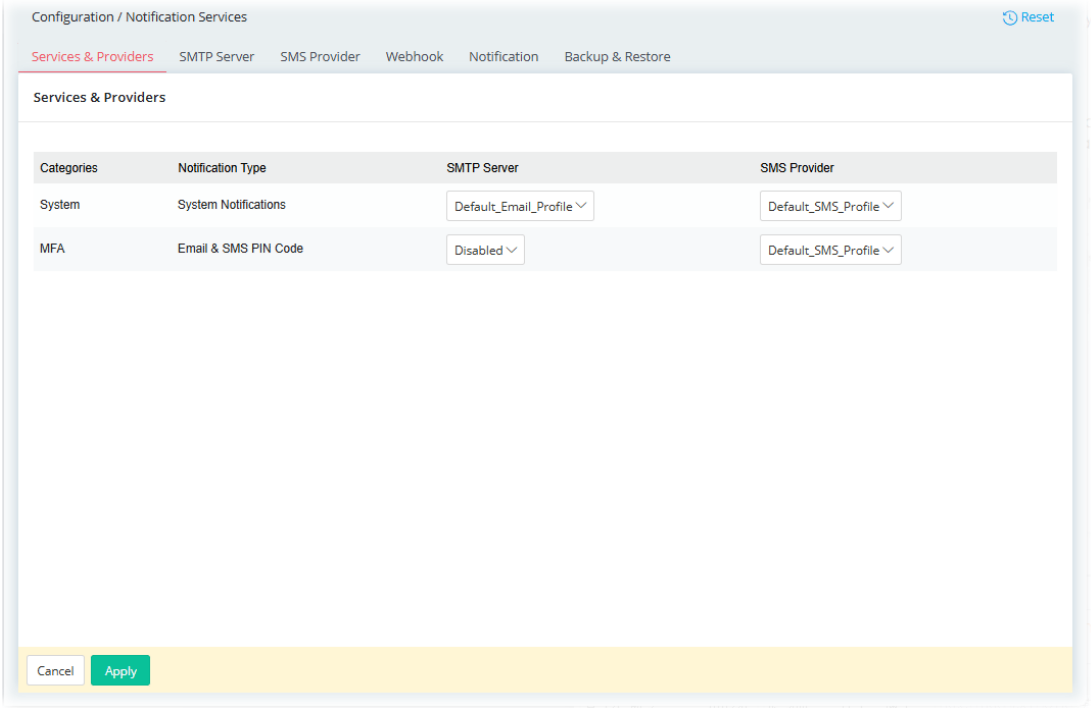
	 如果在 Wake by 中選擇**綁定 IP 至 MAC 清單(Bind IP to MAC List)**，於設定>>區域網路>>將 IP 位址綁定到 MAC 位址中的設定檔內容列將顯示選項供您選擇。 
喚醒(Wake Up)	按此以傳送網路喚醒訊息至指定的區域網路用戶端。
網路喚醒(Wake on LAN/ WAN)裝置清單(Wake on LAN/WAN Device List)	
+新增(+Add)	按此指定要喚醒的新裝置。 **名稱(Name)** –請輸入裝置名稱。 **裝置(Device)** –輸入裝置的 MAC 位址。 **透過排程自動喚醒(Auto Wake Up by Schedule)** – 本裝置可依設定的時間表自動喚醒。 **網路喚醒(Wake on WAN)** – 切換開關以啟用/停用此功能。此裝置可透過白清單中選定的 IP 位址喚醒。 **公用埠號(Public Port)** – 輸入連接埠號碼。 **選項(刪除)(Option (Delete))** – 移除選定的裝置。
網路喚醒(Wake on WAN)存取控制模式 (Wake on WAN Access Control Mode)	設定啟動資料封包(由手機傳送)傳送到遠端裝置的路徑。 **白名單(Allow List)** – 啟動封包將透過任意 WAN IP 位址或 IP 群組中列出的 IP 位址傳輸到遠端設備。 **IP 群組(IP Group)** – 選擇 IP 群組
取消(Cancel)	捨棄目前設定。
套用(Apply)	儲存目前設定。

II-1-16 通知服務(Notification Services)

通常，通知服務指的是透過電子郵件或簡訊通知使用者。

II-1-16-1 服務與供應商(Services & Providers)

在通知客戶端之前，路由器系統管理員需要設定用於發送信件或簡訊的伺服器和服務供應商。



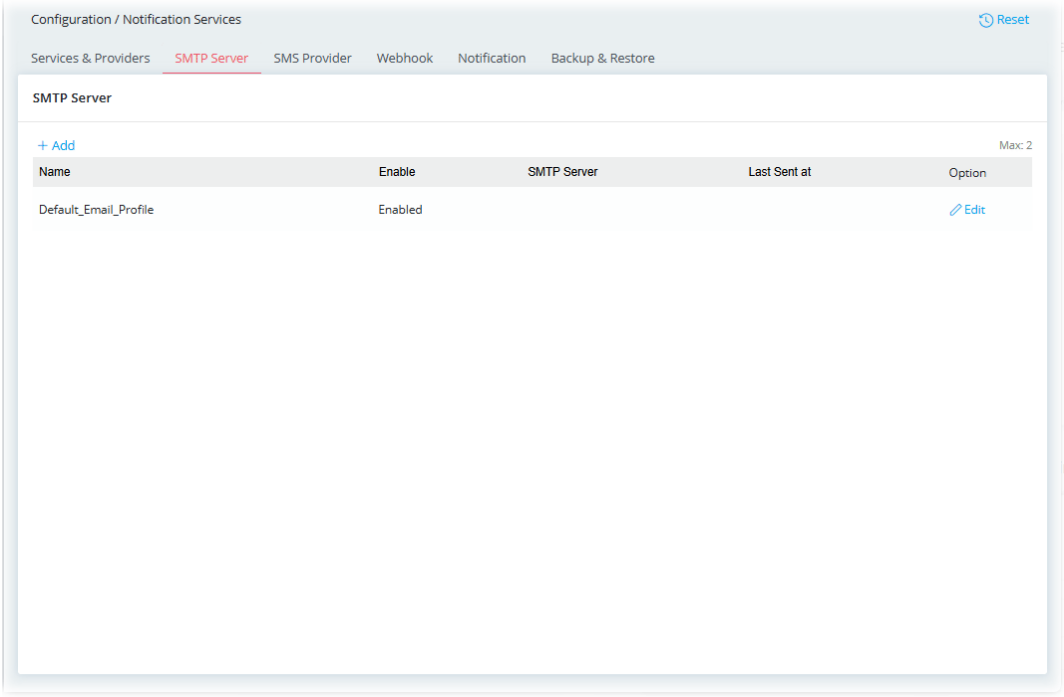
可用設定說明如下：

項目	說明
SMTP 伺服器(SMTP Server)	使用下拉式選單選擇用於傳送電子郵件的 SMTP 伺服器。
SMS Provider	使用下拉式選單選擇用於發送簡訊的簡訊服務供應商。
取消(Cancel)	捨棄目前設定。
套用(Apply)	儲存目前設定。

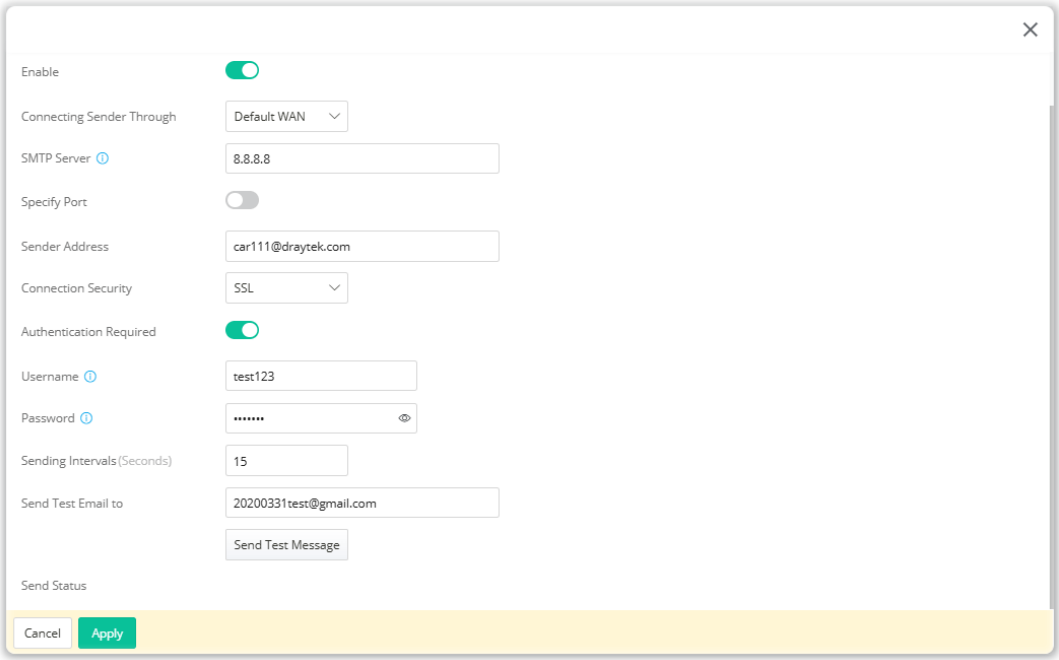
完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-1-16-2 SMTP 伺服器(SMTP Server)

最多可以設定 2 個 SMTP 伺服器設定檔供服務和供應商選擇。



欲新增設定檔，請按下**+新增(+Add)鏈結**即可開啟如下頁面。



可用設定說明如下：

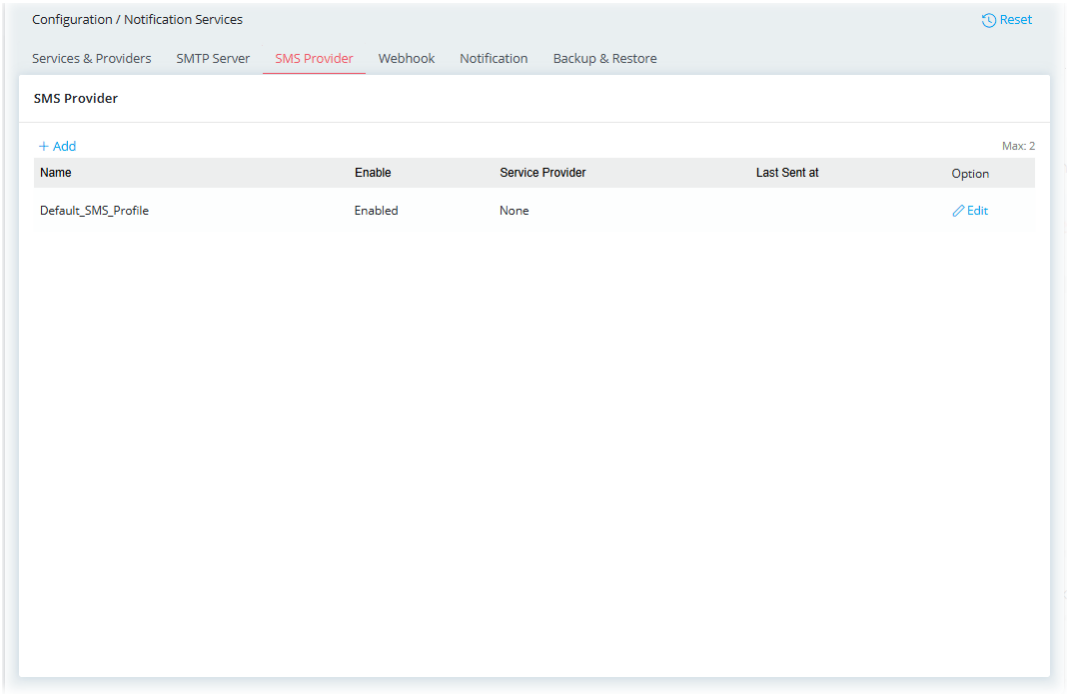
項目	說明
名稱(Name)	輸入設定檔名稱。
啟用(Enable)	切換開關即可啟用/停用此設定檔。
連接寄件人方式	指定用於連接寄件人的 WAN 介面。

(Connecting Sender Through)	
SMTP 伺服器(SMTP Server)	輸入 SMTP 伺服器的 IP 位址。
指定埠號 (Specify Port)	切換開關以啟用連接埠號設定。 **指定 SMTP 埠號(Specify SMTP Port)** – 輸入 SMTP 伺服器的連接埠號碼。
寄件人地址 (Sender Address)	輸入寄件者的電子郵件地址。
連線安全性 (Connection Security)	有三種方法可以增強 SMTP 伺服器的連線安全性。 **無(None)** - 不使用 SSL。封包將以未加密的方式傳輸。 **SSL** - 封包將透過加密連線傳輸。請選擇使用 SMTPS(基於 SSL 的 SMTP)與 SMTP 伺服器通訊。請注意，SMTPS 伺服器使用的連接埠號碼為 465。 **StartTLS** - 此為通訊協定，用於啟動從不安全通道到安全通道間的傳輸轉換。
驗證需要 (Authentication Required)	選擇此項目可將使用者名稱和密碼傳送至 SMTP 伺服器進行身份驗證。 **使用者名稱(Username)** – 用於身份驗證的使用者名稱。最大長度為 31 個字元。 **密碼(Password)** – 用於身份驗證的密碼。最大長度為 31 個字元。
傳送間隔 (Sending Intervals)	發送電子郵件之間最短等待時間(以秒為單位)。
傳送測試郵件至 (Send Test Email to)	指定一個電子郵件地址。 **傳送測試訊息(Send Test Message)** - 按此可依照上述設定發送測試電子郵件。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

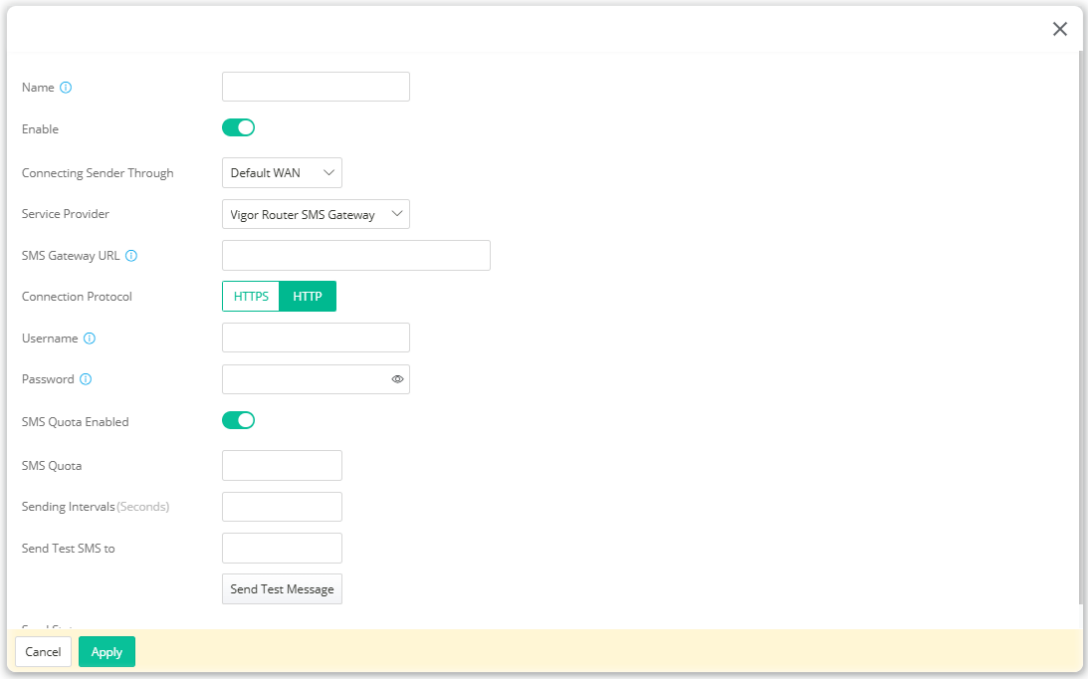
完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-1-16-3 簡訊服務供應商(SMS Provider)

最多可設定 2 個簡訊服務供應商。



欲新增設定檔，請按下**+新增(+Add)鏈結**即可開啟如下頁面。



可用設定說明如下：

項目	說明
名稱(Name)	輸入設定檔名稱。
啟用(Enable)	切換開關即可啟用/停用此設定檔。

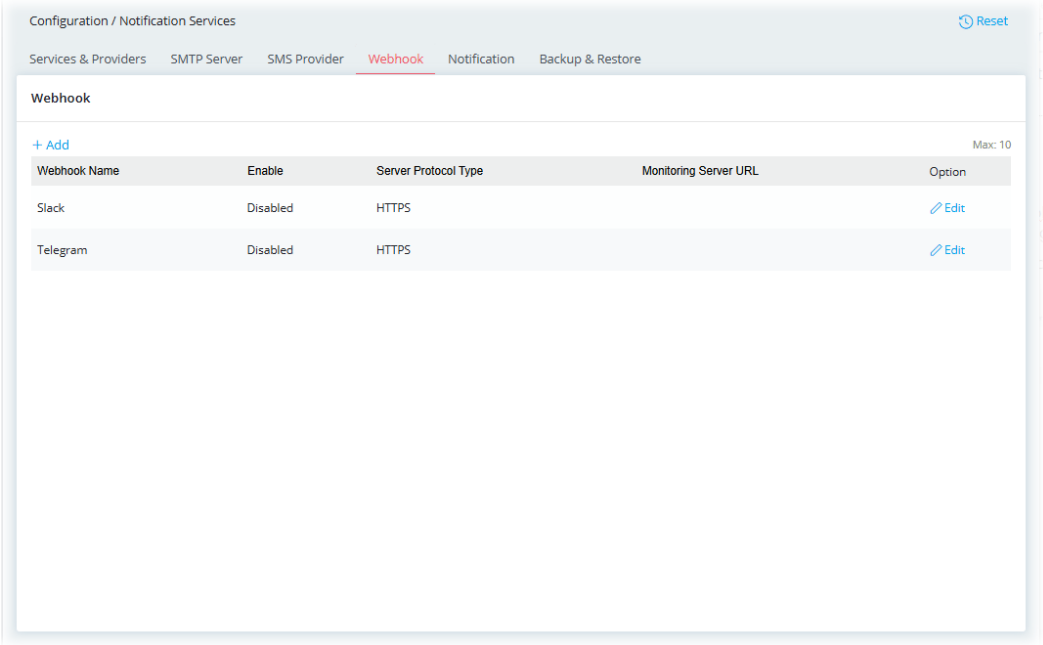
連接寄件人方式 (Connecting Sender Through)	指定用於連接寄件人的 WAN 介面。
服務供應商(Service Provider)	**Vigor 路由器簡訊閘道(Vigor Router SMS Gateway)** – 並非所有 Vigor 路由器都支援簡訊功能。此選項可讓您設定路由器的 IP 位址，該位址可用作簡訊閘道。 **客製化(Customized)** – 設定簡訊服務供應商提供的 IP 位址或 URL。
當選擇 Vigor 路由器簡訊閘道(Vigor Router SMS Gateway)作為服務供應商時	**簡訊閘道 URL (SMS Gateway URL)** – 輸入服務供應商的識別碼(網域名稱或 IP 位址)。 **連線通訊協定(Connection Protocol)** – 指定 HTTP 或是 HTTPS。 **使用者名稱(Username)** - 用於服務供應商進行身份驗證。最大長度為 31 個字元。 **密碼(Password)** - 用於服務供應商進行身份驗證。最大長度為 31 個字元。
當選擇客製化(Customized) 作為服務供應商時	**簡訊服務供應商 API URL (SMS Provider API URL)** – 輸入簡訊服務的網址。網址長度最多為 255 個字元。請聯絡服務供應商以取得正確的網址。 **簡訊 API 參數(SMS API Parameter)** - 對於每個具有獨立簡訊和收件人號碼(發送至)的 API(應用程式介面)，請輸入每個 API 所代表的字串。 **HTTP 方式(HTTP Method)** – 提供兩種請求方式。 • **取得(GET)** - 用於從指定資源請求資料。 • **POST** - 用於向伺服器發送資料以建立/更新資源。
簡訊額度啟用 (SMS Quota Enabled)	切換開關即可啟用/停用額度設定
簡訊額度(SMS Quota)	剩餘允許發送的簡訊數量。路由器每次發送短信，額度值就會減 1。當額度值降至 0 時，將無法發送任何短信，直到額度值重置為大於 0 為止。
傳送間隔 (Sending Intervals)	發送簡訊之間最短等待時間(以秒為單位)。
傳送測試簡訊至 (Send Test SMS to)	指定一個電子郵件地址。 **傳送測試訊息(Send Test Message)** - 按此可根據上述設定發送測試電子郵件。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

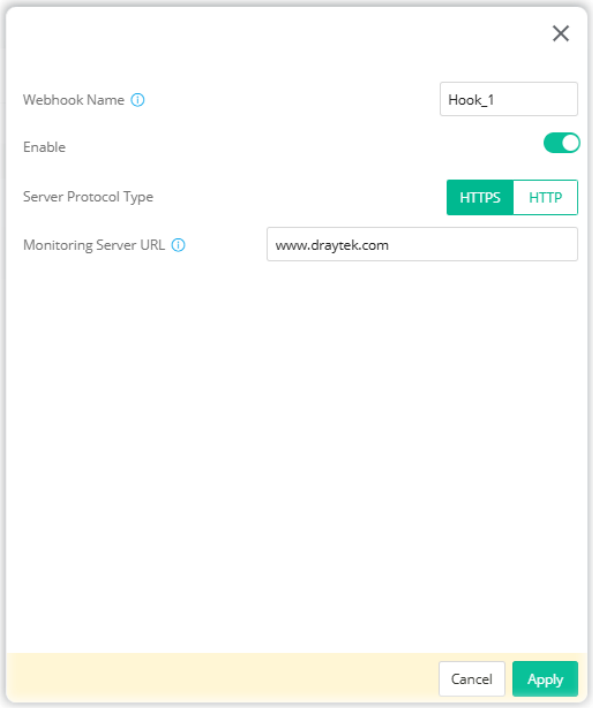
II-1-16-4 Webhook 設定

Vigor 路由器會定期向監控伺服器發送報告(webhook 訊息)，其中包括 WAN 連線狀態(上線、下線)、CPU 使用率、記憶體使用率等資訊。

最多可設定 10 個 webhook 設定檔。



欲新增設定檔，請按下**+新增(+Add)鏈結**即可開啟如下頁面。



可用設定說明如下：

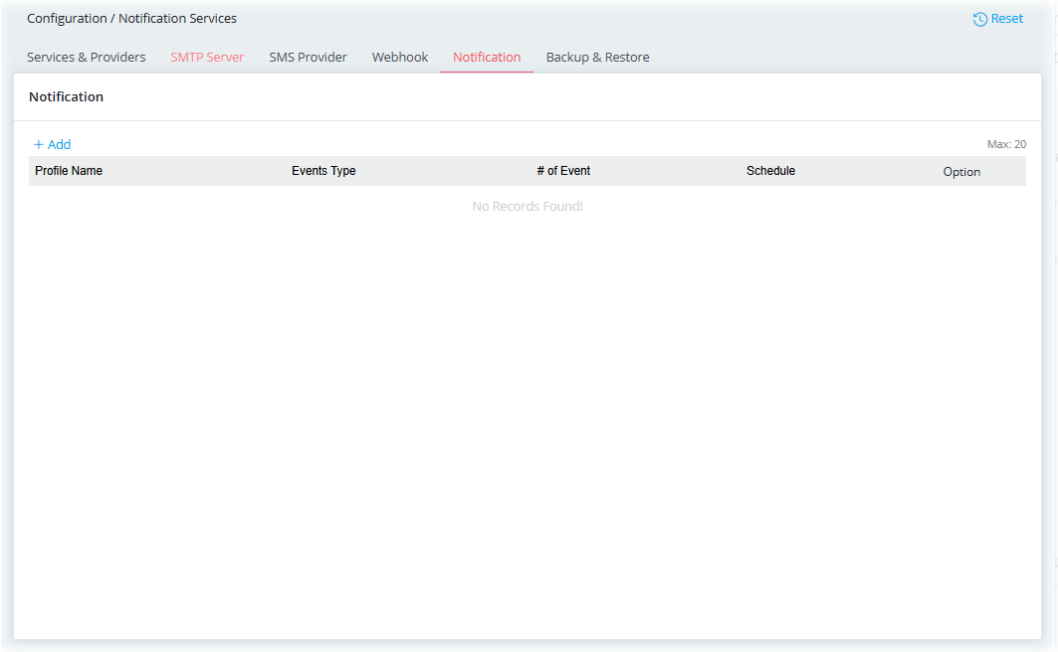
項目	說明
Webhook 名稱	輸入設定檔名稱。

(Webhook Name)	
啟用(Enable)	切換開關即可啟用/停用此設定檔。
伺服器通訊協定類型 (Server Protocol Type)	選擇伺服器使用的通訊協定(HTTPS 或 HTTP)。
監控伺服器 URL (Monitoring Server URL)	輸入伺服器的 URL。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

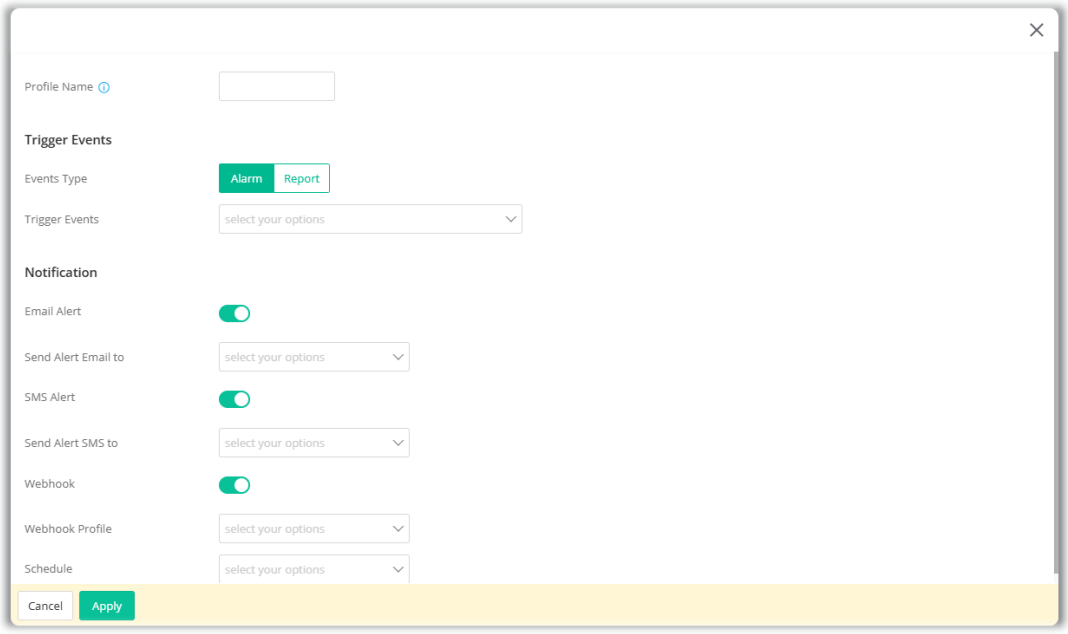
完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-1-16-5 通知(Notification)設定

最多可以建立 20 個通知設定文件，並將其應用於服務供應商之通知服務。



欲新增設定檔，請按下**+新增(+Add)鏈結**即可開啟如下頁面。



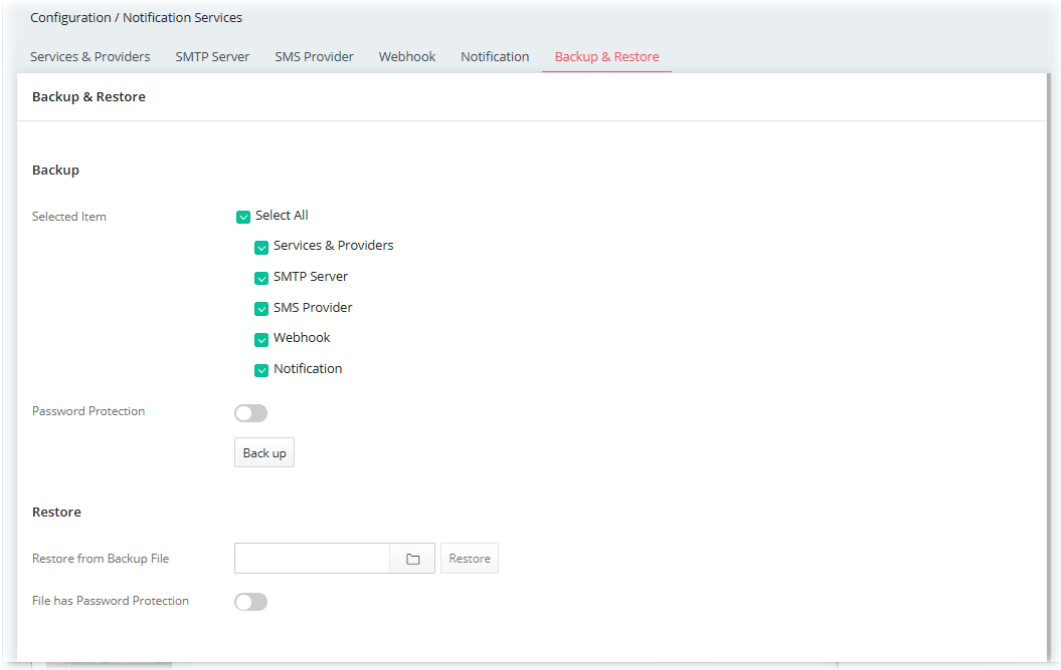
可用設定說明如下：

項目	說明
設定檔名稱(Profile Name)	輸入服務設定檔的名稱。
觸發事件(Trigger Events)	
事件類型 (Events Type)	**警報(Alarm)** – 如果發生警報事件，Vigor 系統將向收件者發送警報訊息。 **報告(Report)** – Vigor 系統會在發生警報事件時定期向收件者發送報告。 • **報告期間(Report Period)** – 設定 Vigor 系統透過電子郵件、簡訊等方式發送報告的週期（60-360 分鐘）。
觸發事件 (Trigger Events)	使用下拉清單選擇允許 Vigor 系統透過電子郵件、簡訊等方式發送報告或警報的事件。
通知(Notification)	
電子郵件警示 (Email Alert)	切換開關即可啟用/停用電子郵件提醒功能。 **傳送警示郵件至(Send Alert Email to)** - 選擇要透過電子郵件傳送通知的電子郵件設定檔。
簡訊警示 (SMS Alert)	切換開關即可啟用/停用簡訊警示功能。 **傳送警示簡訊至(Send Alert SMS to)** - 選擇用於透過簡訊發送通知的簡訊設定檔。
Webhook	切換開關即可啟用/停用 webhook 通知。 **Webhook 設定檔(Webhook Profile)** - 選擇用於傳送通知的 webhook 設定檔。
排程(Schedule)	選擇要發送通知(簡訊、電子郵件)的排程設定檔。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-1-16-6 備份與還原(Backup & Restore)

備份和還原通知服務的設定。



可用設定說明如下：

項目	說明
選定項目 (Selected 項目)	選擇要備份或還原設定的項目。
密碼保護 (Password Protection)	切換開關即可啟用或停用此功能。 如果啟用此功能，請設定密碼。 **新密碼(New Password)** – 輸入一個字串作為密碼。 **確認新密碼(Confirm New Password)** – E 再度輸入密碼。 **備份(Back up)** – 按此執行備份作業。
還原自備份檔案 (Restore from Backup File)	選擇要還原的備份檔案。
檔案具有密碼保護 (File has Password Protection)	切換開關即可啟用或停用此功能。 如果啟用此功能，請設定密碼。 **密碼(Password)** – 請輸入一個字串作為還原設定的密碼。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-1-17 RADIUS/TACACS+設定

遠端使用者撥入驗證服務(RADIUS)是一種用戶端/伺服器端安全性驗證之通訊協定，支援驗證、授權和計費等功用，通常為網際網路服務供應商所廣泛應用，是用來作為驗證和授權撥接網路使用者最常見的一種方法。

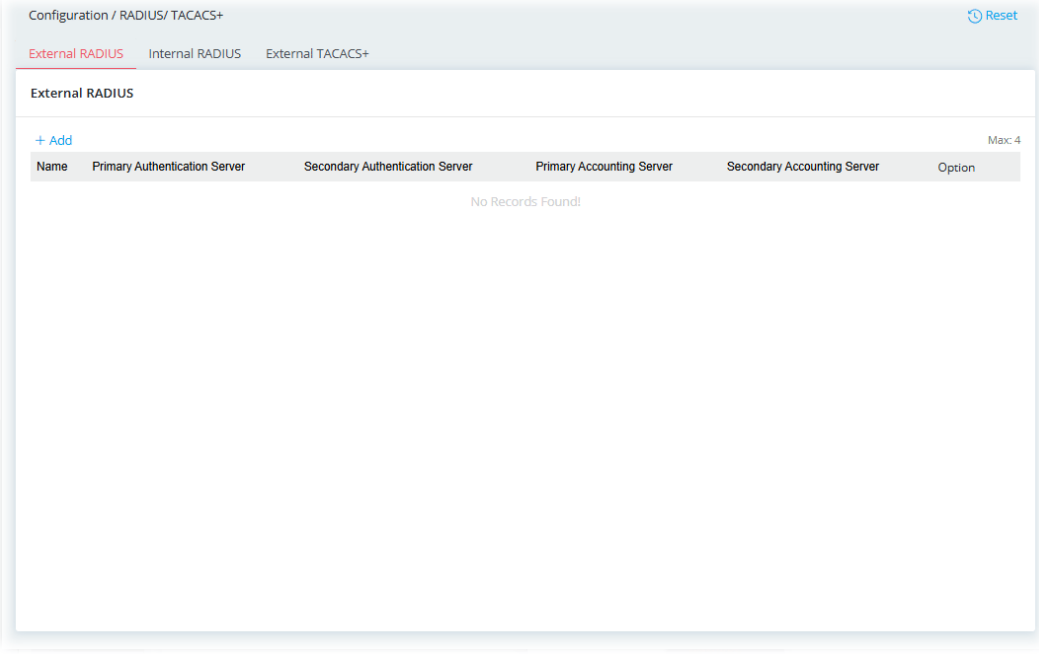
此路由器支援外部 TACACS+ 以及內部和外部 RADIUS 伺服器進行使用者身份驗證。需要使用者驗證的服務包括 WLAN 和 VPN。

II-1-17-1 外接 RADIUS (External RADIUS)

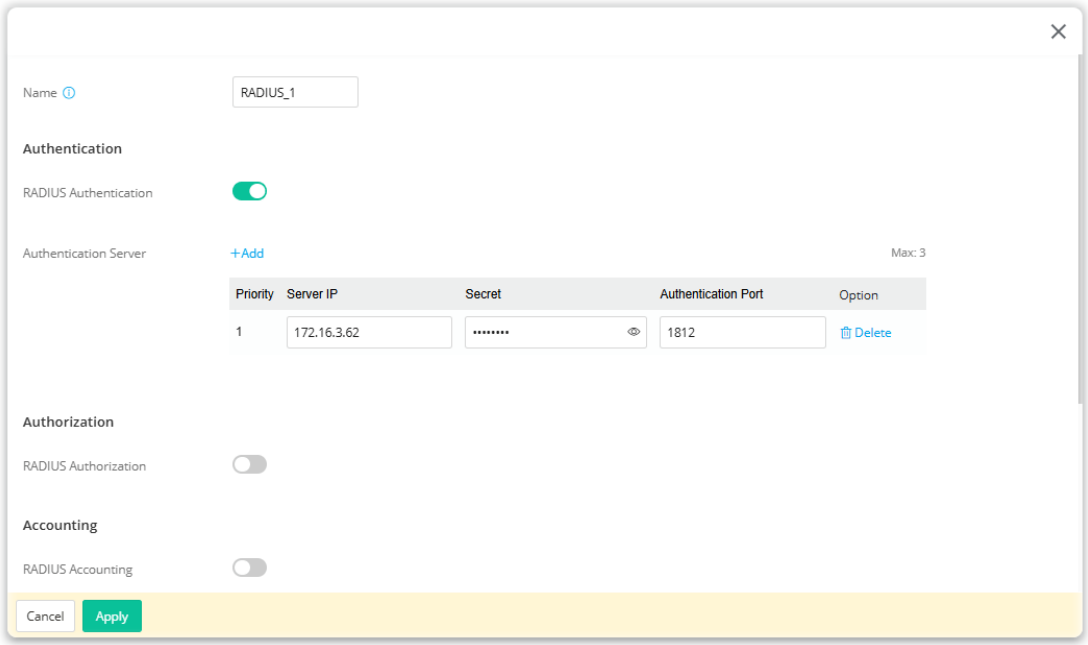
內建的 RADIUS 用戶端功能可讓路由器協助遠端撥入使用者或無線站點與 RADIUS 伺服器進行相互認證。它支援集中式遠端存取認證，便於網路管理。

Vigor 路由器可以作為 RADIUS 用戶端運作。此網頁用於設定外部 RADIUS 伺服器的設定。之後，Vigor 路由器的區域網路使用者將透過該伺服器進行身份驗證和帳戶管理，以便存取網路應用程式。

選擇外部 RADIUS 以設定路由器使用外部 RADIUS 伺服器進行使用者驗證。



若要新增(最多 4 個)設定檔，請按下**+新增(+Add)**連結以獲取以下頁面。



可用設定說明如下：

項目	說明
名稱(Name)	輸入設定檔名稱。
驗證(Authentication)	
RADIUS 驗證 (RADIUS Authentication)	切換開關即可啟用/停用此設定檔。
驗證伺服器 (Authentication Server)	**+新增(+Add)** – 按此新增伺服器(最多可設立三個)。 **伺服器 IP(Server IP)** – 輸入 RADIUS 伺服器的 IP 位址。 **密鑰(Secret)** – RADIUS 伺服器和用戶端共用一個金鑰，用於驗證它們之間發送的訊息。雙方必須設定為使用相同的共享密鑰。共享密鑰的最大長度為 36 個字元。 **驗證埠口(Authentication Port)** – 輸入 RADIUS 伺服器的連接埠號。預設值為 1812 (基於 RFC 2138)。 **選項(刪除)(Option (Delete))** - 按此移除選定的設定檔。
授權(Authorization)	
RADIUS 授權 (RADIUS Authorization)	切換開關即可啟用/停用此設定檔。 **中斷訊息埠口(Disconnect Message Port)** -設定一個 UDP 連接埠號碼（預設為 3799），用於接收來自 AAA 伺服器的中斷連接請求封包。請注意，這些封包在被 AAA 伺服器斷開連接之前，已被 RADIUS 伺服器接收。
計費(Accounting)	
RADIUS 計費 (RADIUS Accounting)	RADIUS 計費是 RADIUS 伺服器的網路客戶計費機制。 如果啟用，Vigor 路由器將定期向指定的 RADIUS 伺服器發送計費請求(例如，IP 位址、來自用戶端的流量）。 切換開關即可啟用/停用此設定檔。
計費伺服器 (Accounting Server)	**+新增(+Add)** – 按此新增伺服器（最多可設定 3 個)。 **伺服器 IP(Server IP)** - 輸入 RADIUS 伺服器的 IP 位址。 **密鑰(Secret)** - RADIUS 伺服器和用戶端共用一個金鑰，用於驗證它們之間發送的訊息。雙方必須配置為使用相同的共享密鑰。共享密鑰的最大長度為

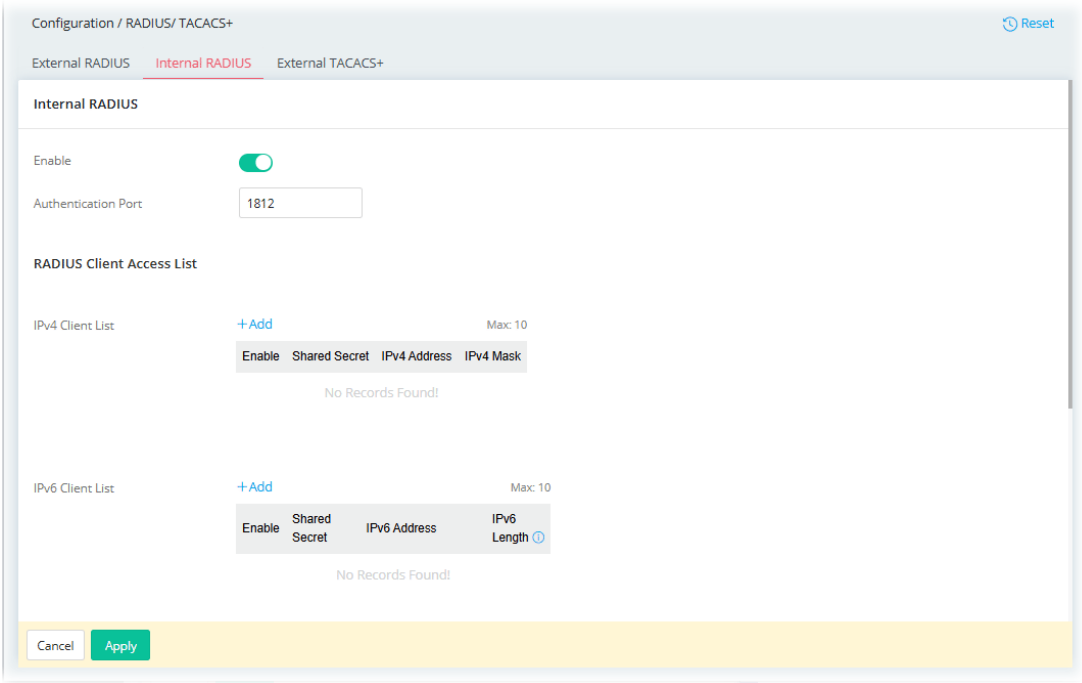
	36 個字元。 **驗證埠號(Authentication Port)** -輸入 RADIUS 伺服器的連接埠號。預設值為 1812 (基於 RFC 2138)。 **選項(刪除)(Option (Delete))** - 按此移除選定的設定檔。
臨時更新間隔 (Interim Update Interval)	設定路由器向 RADIUS 伺服器發送計費請求的時間間隔，範圍從 10 分鐘到 1440 分鐘(1 天)。
RADIUS 伺服器備援策略(RADIUS Server Failover Policy)	
重試(Retry)	設定與 RADIUS 伺服器重新連線的嘗試次數。如果與主伺服器的連線仍然失敗，則停止連線嘗試並開始與備用伺服器建立連線。
逾時(Timeout)	設定路由器等待 RADIUS 伺服器回應的逾時值。如果未收到回應，Vigor 路由器將再次發送身份驗證請求。
連線測試(Connection Test)	
連線測試 (Connection Test)	**使用狀態伺服器進行測試(Test with Status Server)** – 按此進行身份驗證伺服器和計費伺服器的測試。
伺服器狀態 (Server Status)	顯示連線測試結果。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-1-17-2 內部 RADIUS (Internal RADIUS)

除了內建 RADIUS 用戶端外，Vigor 路由器還可以作為 RADIUS 伺服器運行，自行執行安全認證。此頁面用於設定內部 RADIUS 伺服器的設定。設定完成後，Vigor 路由器的區域網路使用者將直接透過 Vigor 路由器進行身份驗證。

選擇內部 RADIUS 以設定路由器的內建 RADIUS 伺服器。



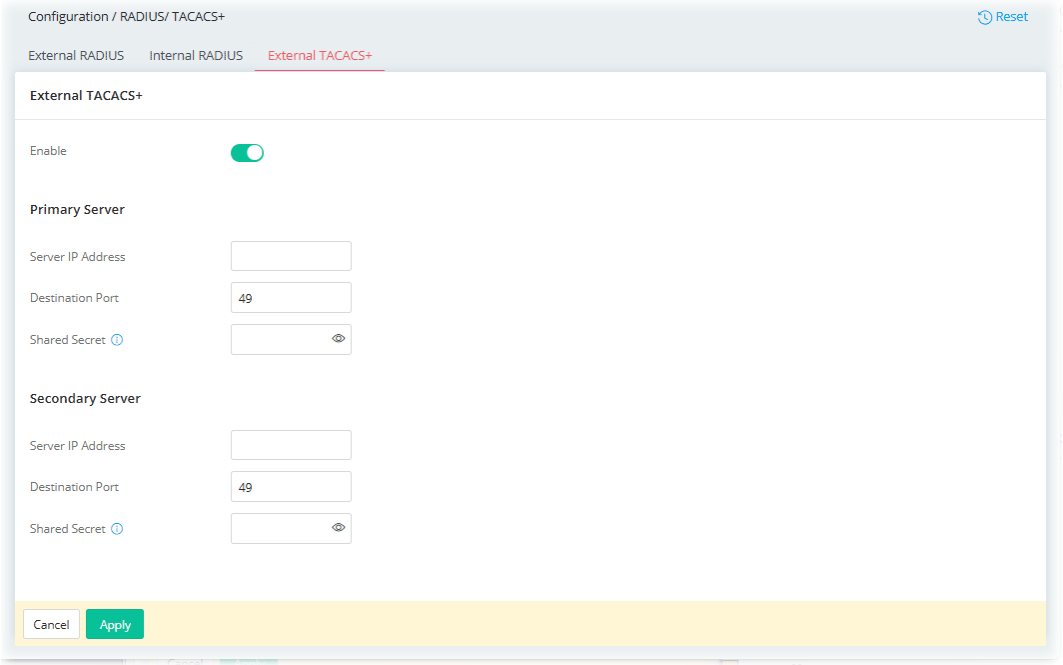
可用設定說明如下：

項目	說明
啟用(Enable)	切換開關以啟用/停用此 RADIUS 伺服器的設定。
驗證埠號 (Authentication Port)	輸入 RADIUS 伺服器的 UDP 連接埠號。預設值為 1812 (基於 RFC 2138)。
RADIUS 用戶端存取清單(RADIUS Client Access List)	
IPv4 用戶端清單 (IPv4 Client List)	只有符合存取清單中設定條件的用戶端才能存取 RADIUS 伺服器。 **+新增(+Add)** – 按此新增用戶端(最多可設立 10 個)。 **啟用(Enabled)** – 切換開關以啟用/停用此條目。 **共享密鑰(Shared Secret)** –一組路由器的 RADIUS 伺服器和 RADIUS 用戶端都知悉的文字字串，用於驗證彼此之間發送的訊息。最大長度為 36 個字元。 **IPv4 位址(IPv4 Address)** –輸入用戶端的 IPv4 位址。 **IPv4 遮罩(IPv4 Mask)** – 選擇 IP 遮罩以設定 IP 區塊的大小。 **選項(刪除)(Option (Delete))** - 按此移除選定的用戶端。
IPv6 用戶端清單 (IPv6 Client List)	只有符合存取清單中設定條件的用戶端才能存取 RADIUS 伺服器。 **+新增(+Add)** – 按此新增用戶端(最多可設立 10 個)。 **啟用(Enabled)** – 切換開關以啟用/停用此條目。 **共享密鑰(Shared Secret)** –一組路由器的 RADIUS 伺服器和 RADIUS 用戶端都知悉的文字字串，用於驗證彼此之間發送的訊息。最大長度為 36 個字元。 **IPv6 位址(IPv6 Address)** – 輸入用戶端的 IPv6 位址。 **IPv6 長度(IPv6 Length)** – 輸入 IPv6 區塊的前置碼長度。 **選項(刪除)(Option (Delete))** - 按此移除選定的用戶端。
驗證(Authentication)	
方式(Method)	指定無線客戶端的身份驗證方式。 **限用 PAP (PAP Only)** – 僅使用密碼驗證協定來驗證使用者身分。 **PAP/CHAP/MS-CHAP/MS-CHAP2** - PAP/CHAP/MS-CHAP/MS-CHAP2-PAP、CHAP (Challenge-Handshake Authentication Protocol)和 Microsoft 版本的 CHAP 可用於驗證使用者。
802.1X 方式 (802.1X Method)	**支援 802.1X 方式(Support 802.1X Method)** – Vigor 路由器內建的 RADIUS 伺服器可以作為 AAA 伺服器。選擇以啟用 802.1X 支援。
憑證(Certificate)	選擇要套用於內部 RADIUS 伺服器的憑證(於設定>>憑證>>本機憑證(Configuration>>Certificates>>Local Certificates)中建立)。
使用者設定檔(User Profile)	
使用者(User)	在安全認證過程中，需要使用者帳號和密碼進行身份驗證。在設定此類頁面之前，請至少於 **IAM>>使用者和群組**(**IAM>>Users & Groups**)中先建立一個使用者設定檔。 **所有使用者(All Users)** – 按此建立所有使用者設定檔以進行安全認證。 **選擇使用者(Select Users)** – 按此選選擇用於安全認證的使用者設定檔。
使用者群組 (User Groups)	**所有群組(All Groups)** – 按此建立所有使用者群組以進行安全認證。 **選擇群組(Select Groups)** –按此選選擇用於安全認證的使用者群組。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-1-17-3 外接 TACACS+(External TACACS+)

指的是終端存取控制器存取控制系統增強版(簡稱 TACACS+)。它的工作原理類似於 RADIUS。點選外部的 TACACS+開啟以下頁面：



可用設定說明如下：

項目	說明
啟用(Enable)	切換開關即可啟用/停用此設定檔。
驗證埠號 (Authentication Port)	輸入 RADIUS 伺服器的 UDP 連接埠號。預設值為 1812 (基於 RFC 2138)。
主要/次要伺服器(Primary Server/Secondary Server)	
伺服器 IP 位址 (Server IP Address)	輸入 TACACS+伺服器的 IP 位址。 本頁面允許設定兩個外部 TACACS+ 伺服器。 當主要 TACACS+ 伺服器發生故障時，次要 TACACS+ 伺服器將用作備份伺服器。
目的埠號 (Destination Port)	請輸入 TACACS+伺服器使用的連接埠號。最常用的數值是 49。
共享密鑰 (Shared Secret)	TACACS+ 伺服器和用戶端 (路由器) 都知道的文字字串，用於驗證它們之間發送的訊息。最大長度為 36 個字元。 一組路由器的 RADIUS 伺服器和 RADIUS 用戶端都知悉的文字字串，用於驗證彼此之間發送的訊息。最大長度為 36 個字元。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

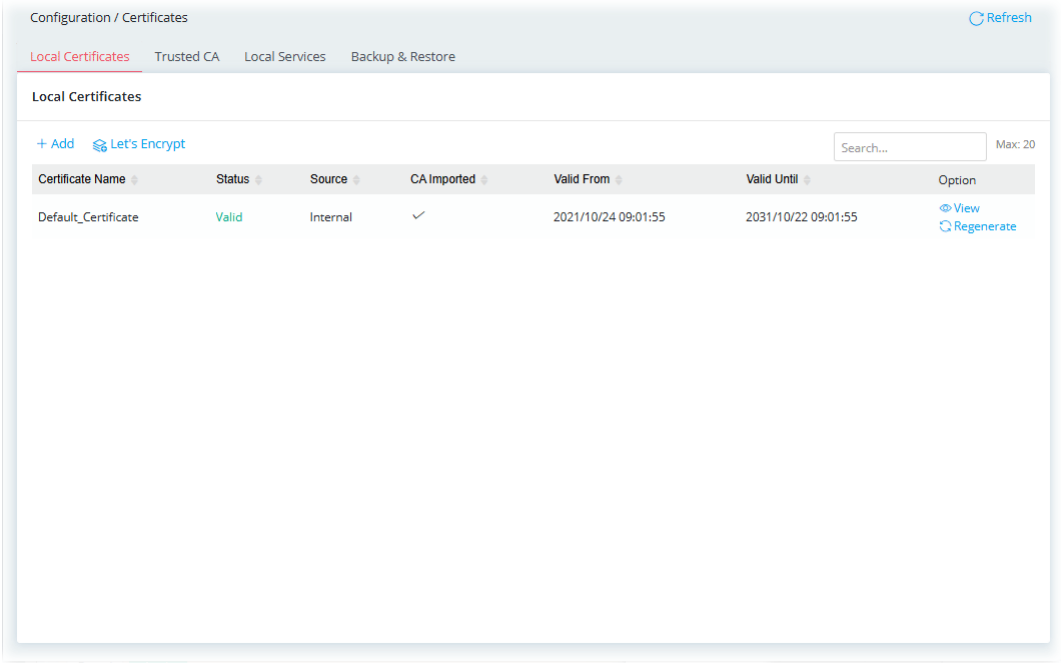
II-1-18 憑證(Certificates)

數位憑證是由特定實體向授權單位(CA)申請核發電子文檔，以證明該實體具有該公鑰之所有權。內容包含了身分識別訊息，例如憑證授權者的名稱、序號、到期日期等，以及憑證授權單位的數位簽名，以便接收方可以驗證憑證的真實性。Vigor 路由器支援符合 X.509 標準的數位憑證。

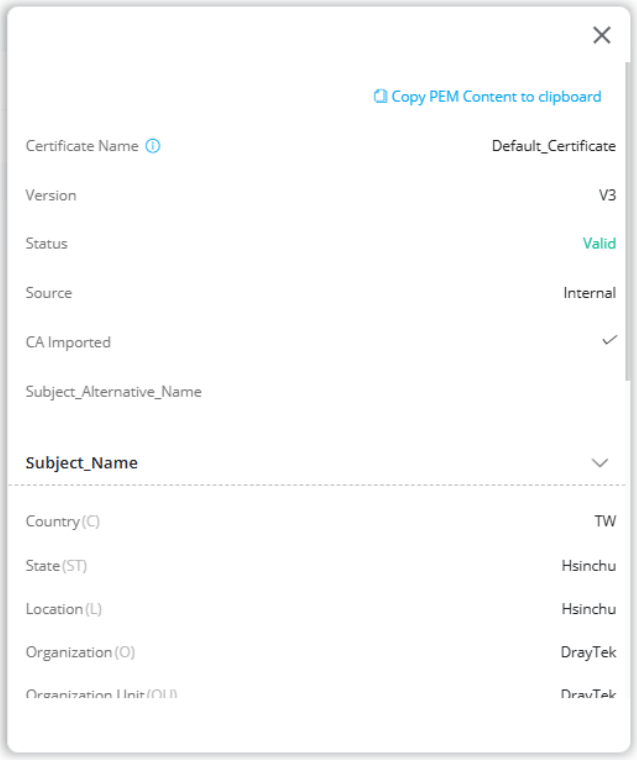
在本節中，您可以產生和管理本機數位憑證，並匯入受信任的 CA 證書。請確保基地台上的時間設定是正確的，以免因系統時間不正確(超出憑證的有效期限)而導致憑證被錯誤地判定為無效。最簡單的方法是定期同步化系統時間與網路時間協定(NTP)伺服器。

II-1-18-1 本機憑證(Local Certificates)

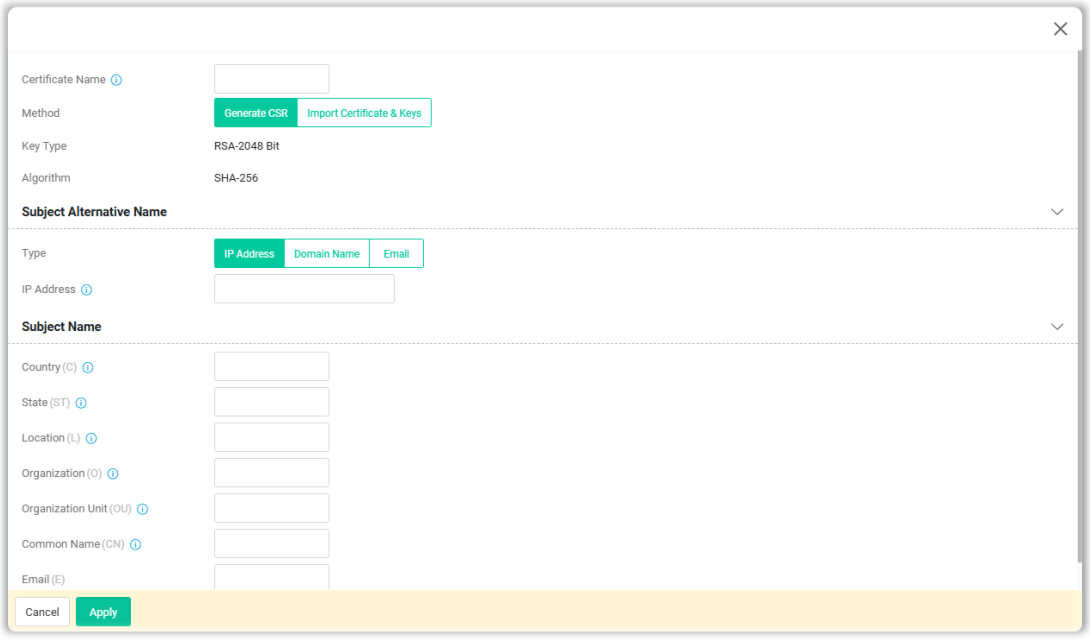
您可以在本頁產生、匯入或是檢視本機憑證。



欲檢查選定憑證的細部內容，請按下**檢視(View)**：



欲新增本機憑證，按下**新增(+Add)**連結開啟如下頁面。



可用設定說明如下：

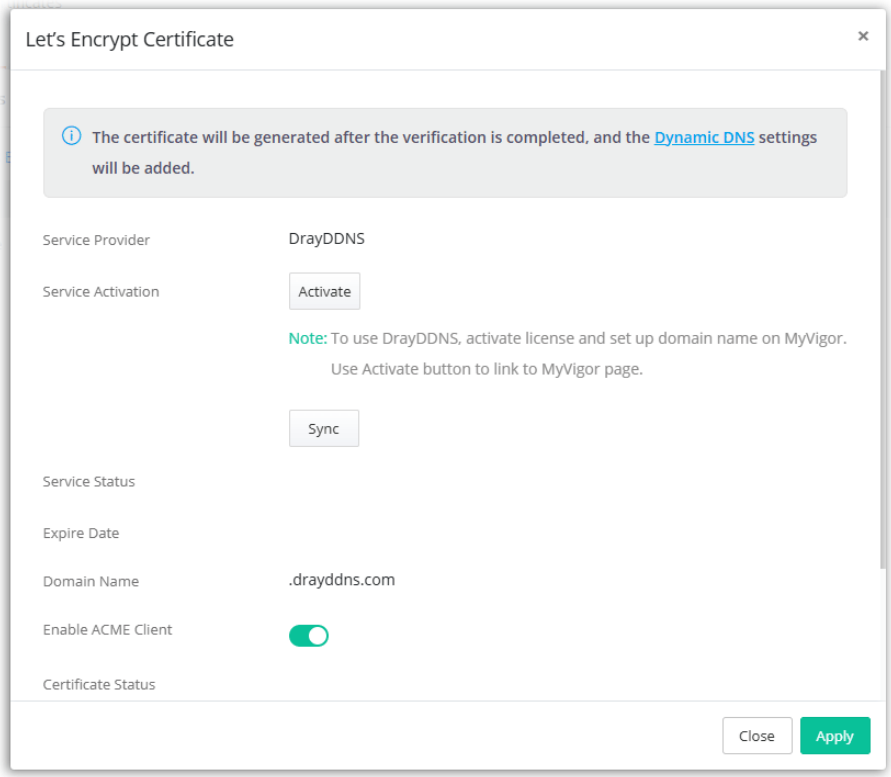
項目	說明
憑證名稱(Certificate Name)	輸入用以識別此憑證的名稱。
方式(Method)	**產生 CSR (Generate CSR) -** 產生新的本機憑證。 **匯入憑證與密鑰(Import Certificate & Keys) -** Vigor 路由器可讓您產生憑證需求並提交至 CA 伺服器，後續讓您匯入作為本機憑證。如果您已經從第三方取得了憑證，您也可以直接採用。支援的類型為 PKCS12 憑證以及含有密鑰的憑證。

方法 - 產生 CSR (Generate CSR)	
金鑰類型(Key Type)	顯示憑證使用的金鑰類型。
演算法(Algorithm)	顯示產生憑證的演算方法。
類型(Type)	選擇主體替代名稱(Subject Alternative Name)並輸入相應的數值。 ● **IP 位址(IP Address)** ● **網域名稱(Domain Name)** ● **電子郵件(Email)**
國家(Country (C))	輸入實體組織所在的國家名稱(代碼)。
州(State (ST))	輸入實體組織所在的州或省。
位置(Location (L))	輸入實體組織所在的城市。
組織(Organization (O))	輸入實體組織的合法名稱。
組織單位 (Organization Unit (OU))	輸入您希望將此憑證與組織內哪個部門有所關聯的部門名稱。
常見名稱 (Common Name (CN))	輸入用於存取伺服器的完整網域名稱/WAN IP 位址。
電子郵件(Email (E))	輸入實體組織的電子郵件位址。
取消(Cancel)	捨棄目前的設定並離開此頁面。
套用(Apply)	儲存目前的設定並離開此頁面。
方法 - 匯入憑證與密鑰(Import Certificate & Keys)	
檔案類型 (File Type)	Vigor 路由器可讓您產生憑證請求並將其提交給 CA 伺服器，然後將其匯入為**本機憑證**。如果您已從第三方獲得證書，則可以直接匯入。支援的憑證類型包括 PKCS12 憑證和帶有私鑰的憑證。 **限用憑證(Certificate Only)** -本機憑證。 ● **上傳憑證(Upload Certificate)** - 按下**選擇檔案(Choose a file)**挑選一個本機憑證。 **PKCS12** - 使用者可以輸入副檔名為.pfx 或 .p12 的憑證，這些憑證通常需要密碼驗證。PKCS12 為安全儲存虛擬密鑰與憑證的一種標準，主要用於 Netscape 與微軟 IE 上。 ● **上傳 PKCS12 檔案(Upload PKCS12 File)** -按下**選擇檔案(Choose a file)**挑選一個 PKCS12 憑證檔案。 ● **密碼(Password)** - 輸入與憑證、金鑰檔案相關聯的密碼。 **憑證與金鑰(Certificate & Keys)** - 當用戶擁有獨立的憑證和私鑰時，此功能非常有用。如果私鑰已加密，則需要密碼。 ● **上傳檔案(Upload File)** - 按下**選擇檔案(Choose a file)**挑選一個本機憑證。 ● **上傳金鑰(Upload Key)** - 按下**選擇檔案(Choose a file)**挑選一個金鑰。 ● **密碼(Password)** - 輸入與憑證、金鑰檔案相關聯的密碼。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下**套用(Apply)**按鈕儲存相關設定。

除了手動建立本機憑證外，您還可以使用 Let's Encrypt 產生憑證。按下設定>>憑證>>本機憑證 (Configuration>>Certificates>>Local Certificates)中的 Let's Encrypt 鏈接，即可進入以下頁面。在此

處，您可以使用 DrayDDNS 服務產生 Let's Encrypt 憑證。您也可以在設定>>WAN>>動態 DNS(Configuration>>WAN>>Dynamic DNS)中查看其他選項。



可用設定說明如下：

項目	說明
服務供應商(Service Provider)	顯示 Let's Encrypt 憑證的服務供應商。
服務啟動 (Service Activation)	啟動(Activate) – 按下鏈結前往 MyVigor 網站以啟動 Let's Encrypt 證書。 同步(Sync) - 的網域名稱已在 MyVigor 伺服器上設定。按此按鈕加載並取得網域名稱(如果可用)。
啟用 ACME 用戶端 (Enable ACME Client)	切換開關以產生由 Let's Encrypt 頒發的憑證，以便套用至此類 DDNS 帳戶。
更多設定(More Settings)	
使用以下方式更新 DDNS (DDNS Update DDNS with)	如果 Vigor 路由器安裝於任何 NAT 路由器後方，您可以啟用此功能，以取得實際的 WAN IP 位址。 當 Vigor 路由器使用的 WAN IP 為私人 IP 時，此功能可以偵測 NAT 路由器使用的公用 IP，並使用偵測到的 IP 位址進行 DDNS 更新。 有兩種方法供您選擇： 網際網路 IP (Internet IP) – 網際網路 IP 將使用真實的公網 IP 位址。如果指派給路由器 WAN 介面的 IP 位址不是實際的外部 IP 位址，請選擇此選項。 WAN IP – 使用路由器 WAN 介面的 IP 位址。
更新 WAN IP 模式 (Update WAN IP Mode)	更新所有選定的 WAN IP (Update All Selected WAN IPs) – Vigor 路由器系統將根據下表取得多個 WAN IP 位址並上傳至服務供應商。 依序更新單一 WAN IP (Update Single WAN IP by Sequence) – Vigor

	系統將使用下表中選定的第一個 WAN IP 並上傳到服務供應商。 **+新增(+Add)** – 按下可建立新的綁定介面和介面 IP 之群組。最多可建立 6 組。 **綁定介面(Binding Interface)** – 選擇與 DDNS 設定檔有關聯的 WAN 介面。 **介面 IP (Interface IP)** – 請選擇一個 WAN IP 位址。若未選擇，系統將使用預設的 WAN IP 位址。
自動更新間隔 (Auto Update Interval)	路由器連接到 DDNS 伺服器以更新 IP 位址資訊的頻率 (以分鐘為單位)。預設值為 14400。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

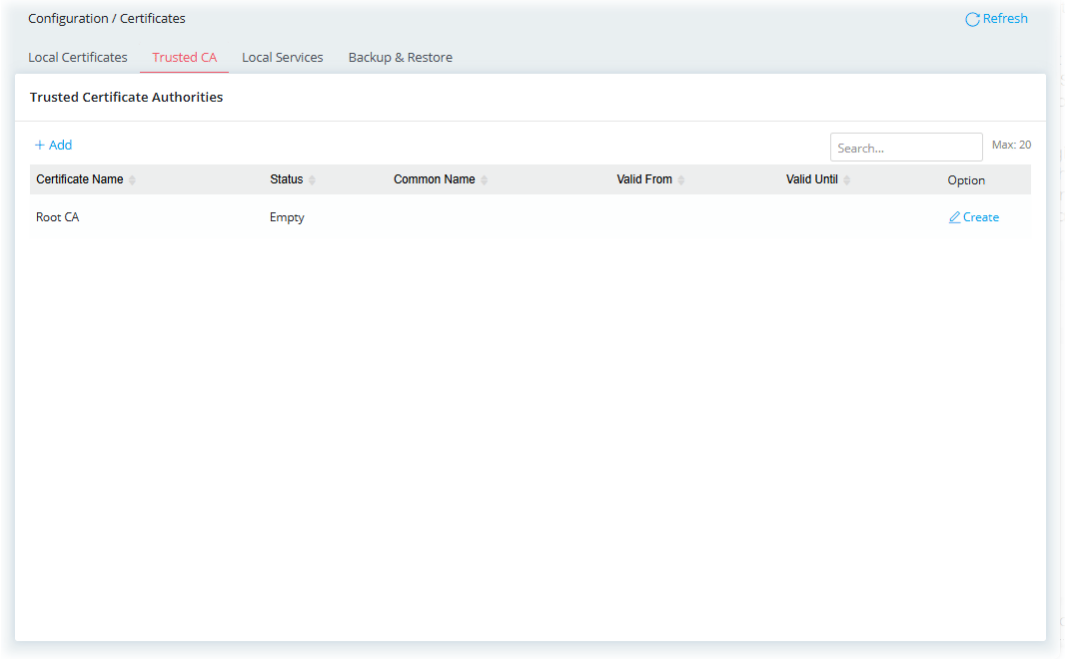
II-1-18-2 受信任的 CA (Trusted CA)

若有必要，您可以在此頁面建立一個 RootCA 憑證。

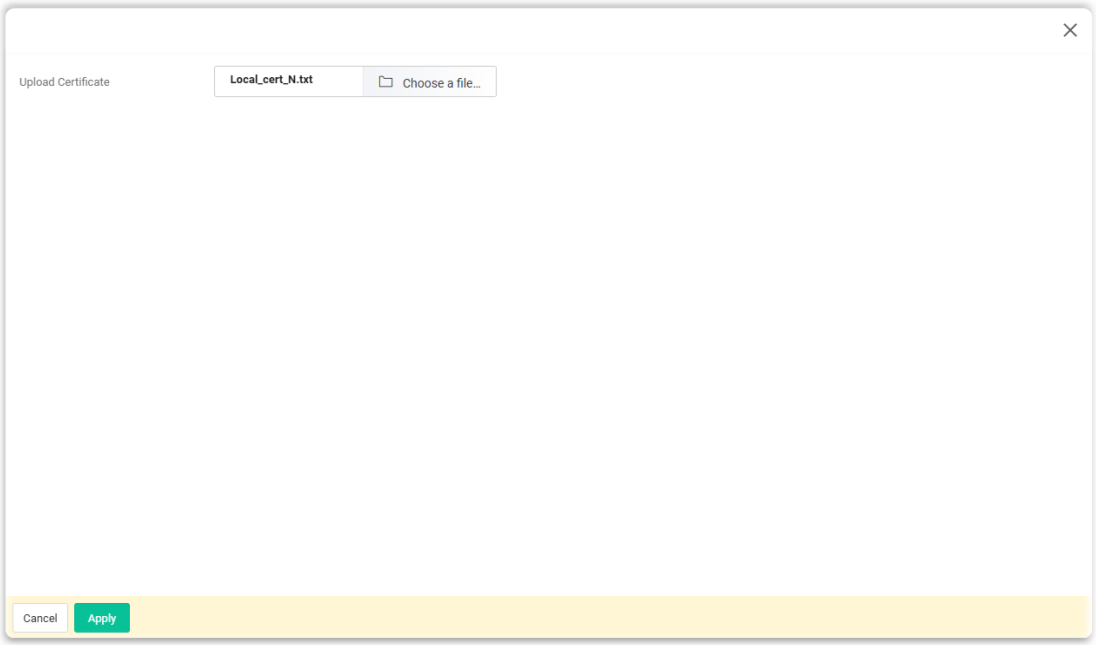
當本機用戶與遠端用戶都需要進行憑證驗證(例如 IPsec X.509)以便讓資料通過 SSL 通道並且防止來自 MITM 攻擊時，可使用根憑證授權機構(Root CA)來驗證雙邊提供的數位憑證。

然而，套用來自受信任的憑證機構的數位憑證是相當複雜且花時間的過程，因此基地台提供一個簡易機制讓您可以產生 Root CA 節省時間並提供一般使用者更多的便利性。之後此 Root CA 可以進行本機憑證之發行事宜。

根憑證授權機構(Root CA)可以刪除，但不能編輯。若要修改根憑證授權單位的設定，請先刪除舊有的，然後按下建立(Create)按鈕建立新的 Root CA。



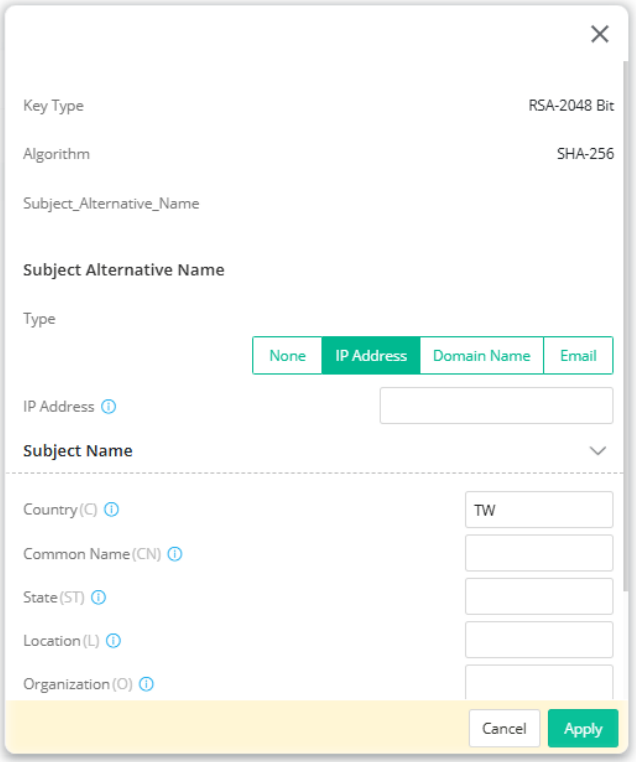
欲匯入根憑證授權機構(Root CA)至 Vigor 路由器上，請按下**新增(+Add)**開啟如下頁面。



可用設定說明如下：

項目	說明
上傳憑證 (Upload Certificate)	**選擇檔案(Choose a file)** - 選擇一個憑證。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	按此將選定的憑證檔案匯入到路由器中。

欲建立新的根憑證授權機構(Root CA)，按下**建立(Create)**開啟如下頁面。



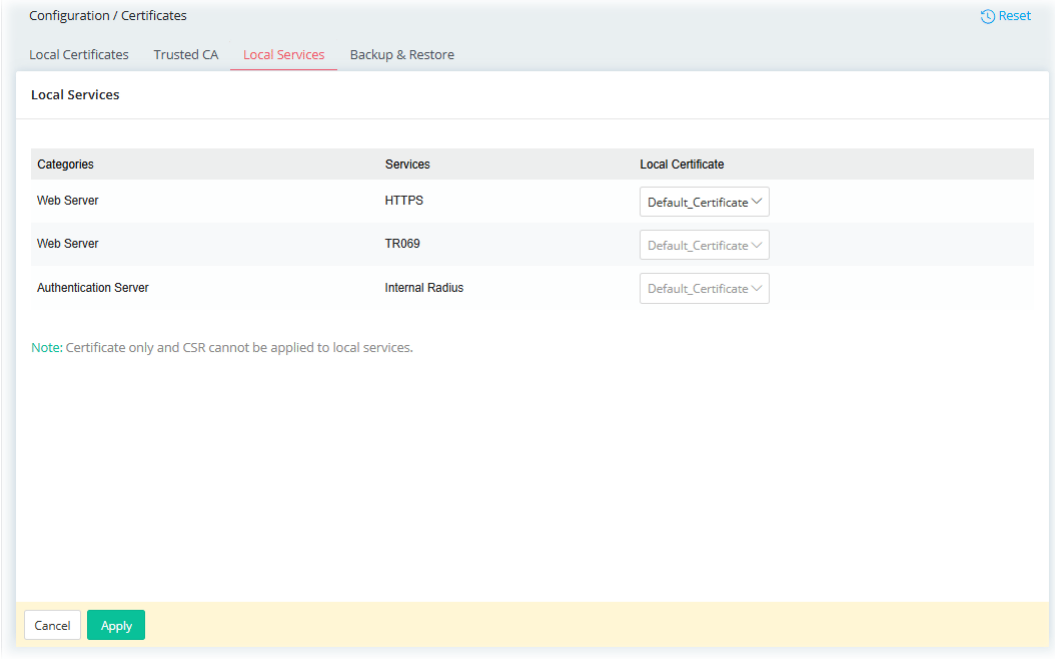
可用設定說明如下：

項目	說明
金鑰類型(Key Type)	顯示金鑰類型(目前設定為 RSA)。
演算法(Algorithm)	顯示演算法。
主體替代名稱(Subject Alternative Name)	
類型(Type)	選擇主體替代名稱(Subject Alternative Name)並輸入相應的數值。
主體名稱(Subject Name)	
國家(Country (C))	輸入實體組織所在的國家名稱(代碼)。
常見名稱 (Common Name (CN))	輸入用於存取伺服器的完整網域名稱/WAN IP 位址。
州(State (ST))	輸入實體組織所在的州或省。
位置(Location (L))	輸入實體組織所在的城市。
組織(Organization (O))	輸入實體組織的合法名稱。
組織單位 (Organization Unit (OU))	輸入您希望將此憑證與組織內哪個部門有所關聯的部門名稱。
電子郵件(Email (E))	輸入實體組織的電子郵件位址。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前的設定並離開此頁面。

完成設定之後，按下**套用(Apply)**按鈕儲存相關設定。

II-1-18-3 本機服務(Local Services)

此頁面可讓您針對本機憑證設定不同的類別和服務，以防止因使用不同的瀏覽器而彈出安全警告訊息。



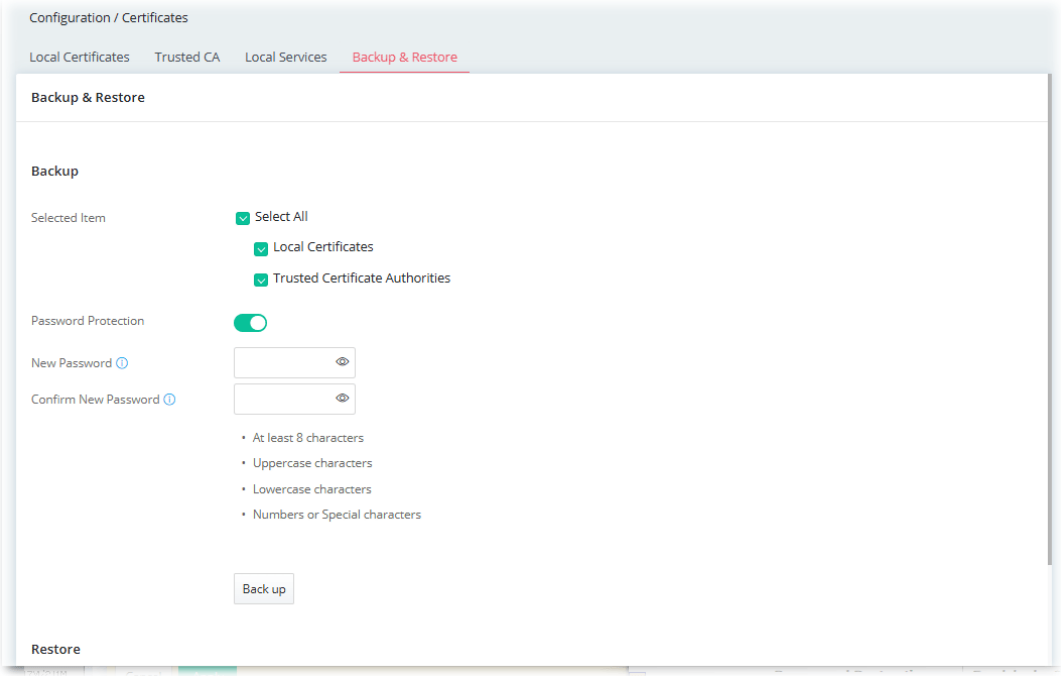
可用設定說明如下：

項目	說明
本機憑證 **(Local Certificate)**	請選擇已匯入至 Vigor 裝置的本機證書，該證書必須包含完整的金鑰和認證資訊。 缺少金鑰或證書籤署請求(CSR)檔案的憑證無法被選擇成為本機憑證。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-1-18-4 備份與還原(Backup & Restore)

您可以將路由器上的本機憑證和受信任的 CA 憑證備份至或還原到某檔案中。



可用設定說明如下：

項目	說明
	Backup
選定項目(Selected Item)	選擇憑證類型(本機、受信任的或是全部憑證)。
密碼保護(Password Protection)	**啟用(Enabled)** - 切換開關即可啟用或停用此功能。 ● **新的密碼(New Password)** -輸入您想要加密憑證所需的密碼內容。 ● **確認新密碼(Confirm New Password)** - 再度輸入密碼。. **備份(Backup)** - 按此下載憑證檔案。
	還原(Restore)
還原自備份檔案(Restore from Backup File)	選擇您想要執行還原作業的備份檔案。 **還原(Restore)** - 按此進行憑證還原。
檔案具有密碼保護(File has Password Protection)	切換開關即可啟用或停用此功能。 若啟用了此功能，須設定一組密碼。 ● **密碼(Password)** - 輸入您想要加密憑證所需的密碼內容。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-2 安全性(Security)

II-2-1 防火牆過濾器(Firewall Filters)

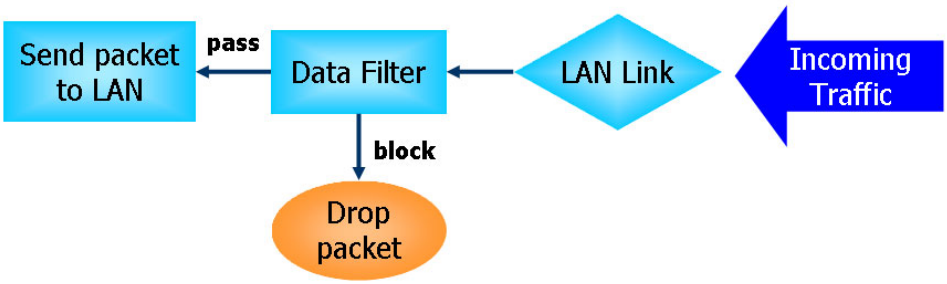
當寬頻使用者需要更多的頻寬以便用於多媒體、應用程式或是遠程學習時，安全性總是最受到重視的一環。Vigor 路由器的防火牆可以協助保護您本地網路免受外在人物的攻擊，同時它可限制本地網路的使用者存取網際網路。此外它還可以過濾一些由觸發路由器所建立的連線特定封包。

區域網路使用者可透過以下防火牆功能獲得安全保護：

- 使用者可設定的 IP 過濾器（資料過濾器）。
- 狀態包偵測（SPI）：追蹤資料包並拒絕未經請求的傳入資料
- 可選擇的拒絕服務（DoS）/ 分散式阻斷服務（DDoS）攻擊防護

資料過濾器

網際網路正處於連線狀態時，資料過濾器可應用在流入與流出的資料傳輸上，系統會按照過濾器規則檢查封包，如果是合法的，該封包即可通過。



封包狀態檢測(SPI)

在網路層級上，封包狀態檢測是一種防火牆結構，它會建立一個封包狀態機器來追蹤防火牆於所有介面的連線狀況，並確保這些連線都是有效的。此類型防火牆並不只是檢查封包標頭資訊，它同時也監視著連線的狀態。

DoS 攻擊防禦（DoS Defense）

DoS 攻擊防禦功能協助用戶檢測並減輕 DoS 攻擊，這類攻擊通常可分成二大類 – flood 類型攻擊和弱點攻擊。flood 類型攻擊嘗試耗盡您的系統資源，而弱點攻擊則是利用通訊協定或是操作系統的弱點嘗試癱瘓系統。

DoS 攻擊防禦功能的引發是以 Vigor 路由器的攻擊特徵值資料庫為基礎，執行每一個封包的檢查，任何可能重複產生以癱瘓主機之惡意封包，在安全的區域網路中都將嚴格阻擋，如果您有設定系統紀錄伺服器，那麼系統紀錄訊息也會傳送警告資訊給您。

Vigor 路由器也可以監視資料流量，任何違反事先定義的參數的不正常資料流(例如臨界值的數字)，都會被視為是一種攻擊行為，Vigor 路由器將啟動防衛機制，及時阻擋減輕災害。

下列表格顯示出 DoS 攻擊防禦功能所能檢測出的攻擊類型。

1. SYN flood attack
2. UDP flood attack
9. SYN fragment
10. Fraggle attack

3. ICMP flood attack
4. Port Scan attack
5. IP options
6. Land attack
7. Smurf attack
8. Trace route
11. TCP flag scan
12. Tear drop attack
13. Ping of Death attack
14. ICMP fragment
15. Unassigned Numbers

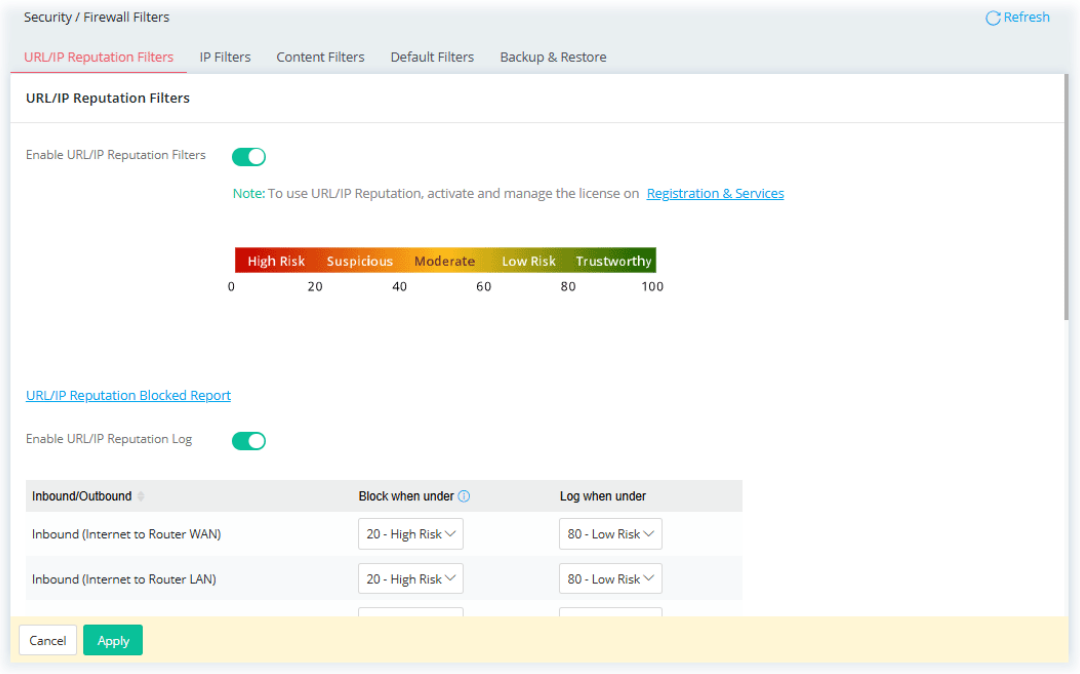
II-2-1-1 IP 信譽過濾器(IP Reputation Filters)

IP 信譽過濾器是一種安全工具，它根據 IP 位址的歷史行為和各種因素來評估其可信度。此過濾器有助於偵測和阻止惡意活動，例如垃圾郵件、駭客攻擊和其他形式的網路攻擊。

Vigor 路由器使用的 IP 信譽過濾器旨在過濾和阻止危險的 IP 位址。為了有效實現此過濾，需要考慮以下三個方向作為過濾條件：

1. 輸入流量(從網際網路到路由器的 WAN 端)
2. 輸入流量(從網際網路到路由器的 LAN 端)
3. 輸出流量(從 LAN 到網際網路)

這種方法可以確保全面抵禦有害 IP 位址。



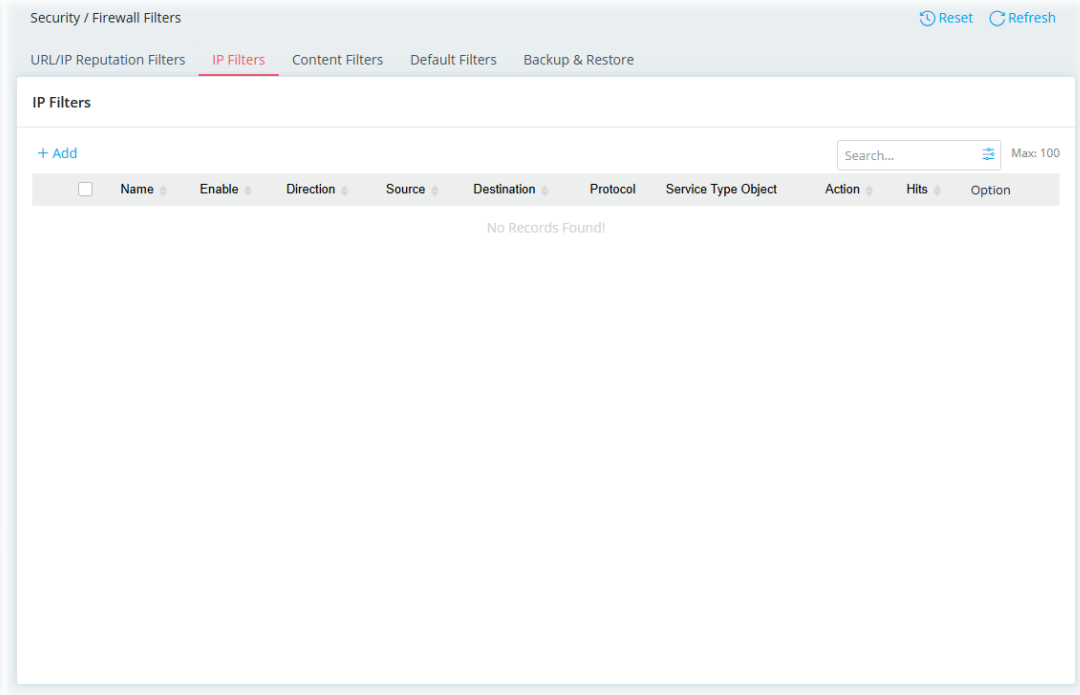
可用設定說明如下：

項目	說明
IP 信譽過濾器(IP Reputation Filters)	
啟用 IP 信譽過濾器 (Enable IP Reputation Filters)	切換開關即可啟用/停用此功能。
IP 信譽封鎖報告 (IP Reputation Blocked Report)	按此顯示 IP 信譽封鎖報告。
啟用 IP 信譽日誌 (Enable IP Reputation Log)	切換開關即可啟用或停用日誌記錄功能。

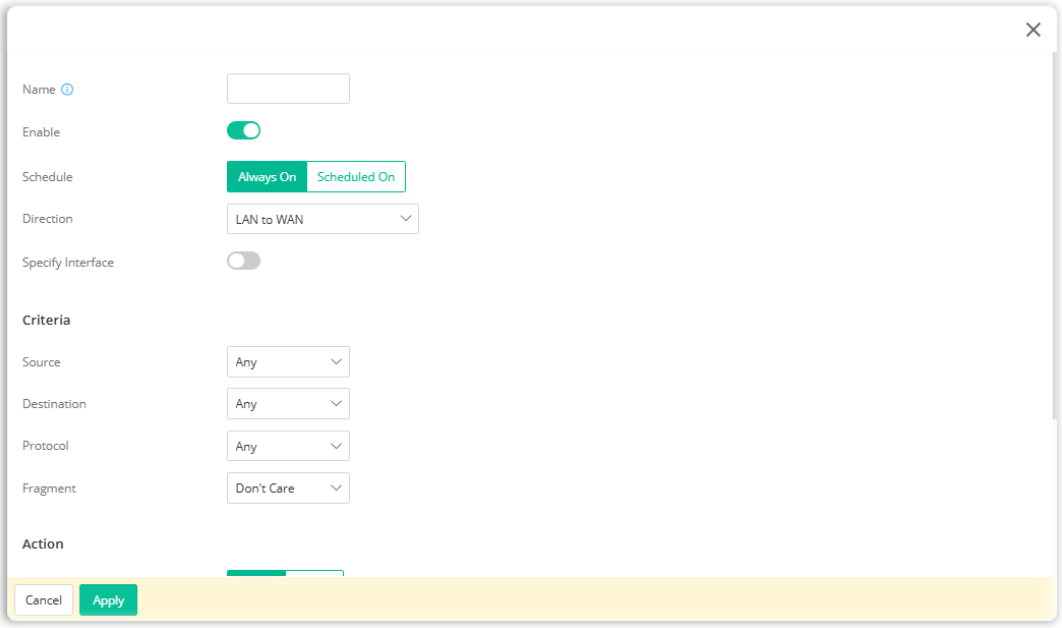
如下情況即封鎖 (Block when under)	選擇風險等級。一旦資料封包(輸入/輸出)的風險達到此處定義的門檻值（20/40/60/80），Vigor 系統將立即封鎖該 IP 位址。預設為 “停用” ，亦即不會執行任何過濾操作。
如下情況即記錄 (Log when under)	選擇風險等級。一旦資料封包(輸入/輸出)風險達到此處定義的百分比，Vigor 系統會將對應資訊記錄到 SysLog 伺服器。預設為 “停用” 。
白名單(Allow List)	
輸入(網際網路至路由器 WAN 端)/ **輸入(網際網路至 LAN 端)/** **輸出(LAN 端至網際網路)** Inbound (Internet to Router WAN) / Inbound (Internet to LAN) / Outbound (LAN to Internet)	允許清單(白名單)中的用戶端 IP 位址將不會透過 IP 信譽過濾器進行過濾。 資料封包傳輸方向包括： ● **輸入(網際網路至路由器 WAN 端))(Inbound (Internet to Router WAN))** ● **輸入(網際網路至 LAN 端)(Inbound (Internet to LAN))** ● **輸出(LAN 端至網際網路) (Outbound (LAN to Internet))** 按每個標籤頁分別建立允許清單(白名單)。 **+新增(+Add)** – 此以新增新的 IP 位址到允許清單(白名單)中。 ● **IP 位址(IP Address)** –輸入 IP 位址。 **+新增(+Add)** – 按此以將新物件/群組新增為允許清單(白名單)中的成員。 ● **物件和群組(Object & Group)** – 使用下拉清單指定物件和群組設定檔。 **+新增(+Add)** – 按此選擇新的服務類型。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定。

II-2-1-2 IP 過濾器(IP Filters)

使用者可以建立存取控制策略並設定黑白名單。



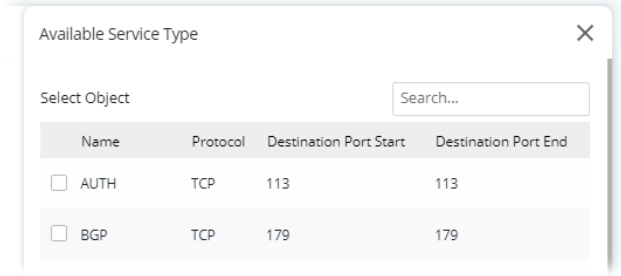
若要新增 IP 過濾器設定檔，請按下**+新增(+Add)**連結以獲取以下頁面。



可用設定說明如下：

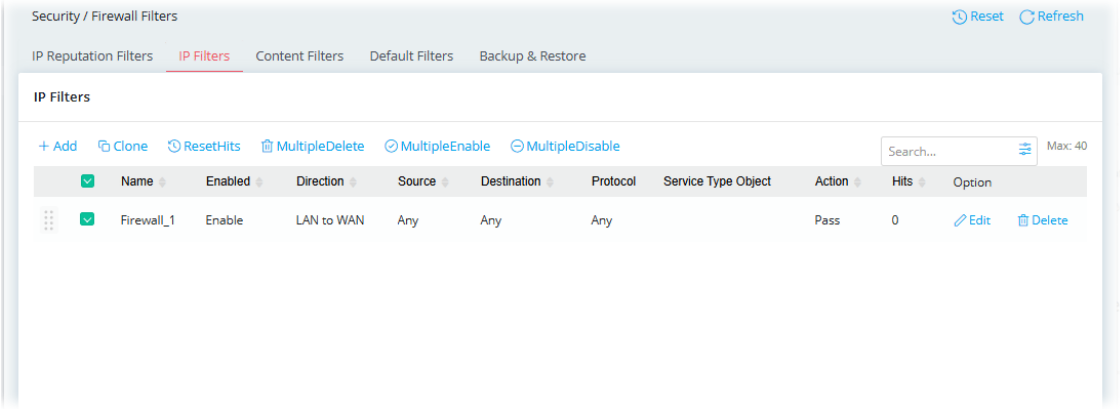
項目	說明
名稱(Name)	輸入用以識別此規則的名稱。
啟用(Enable)	切換開關即可啟用/停用此設定檔。
排程(Schedule)	**永遠連線(Always On)** – 如果啟用，規則將始終有效。 **排程啟用(Scheduled On)** - 選擇排程索引編號，允許規則在特定時間啟

	用。您可以在設定>>物件>>排程(Configurations>>Objects>>Schedule)15 個排程中選擇排程，最多可選 4 個。如果未選擇任何索引，則規則始終啟用狀態。 ● **當排程啟用時，清除連線數(Clear Session when Schedule is On)** - 如果排程任務設定檔啟用了規則更改，請選擇此選項以清除現有會話。所有連線都將被重置。
方向(Direction)	指定此過濾規則適用的流量流向。 ● LAN 至 WAN (LAN to WAN) ● WAN 至 LAN (WAN to LAN) ● LAN/VPN 至 LAN/VPN (LAN/VPN to LAN/VPN)
指定介面 **(Specify Interface)**	切換開關即可啟用/停用此功能。 如果啟用，請指定流量介面。 **來源介面(Source Interface)** – 選擇 LAN/VPN 介面。 **目的介面(Destination Interface)** –選擇 WAN 介面。
標準(Criteria)	
來源 **(Source)**	設定來源 IP 位址。 若要手動設定 IP 位址，請選擇任一 / IPv4 位址 / IPv4 子網 / IPv6 位址 / IPv6 子網 / IP 物件 / IP 群組/ MAC 物件 / MAC 群組作為資訊來源並輸入所需資訊。 **任一(Any)** –所有 IP 位址。 **IPv4 位址(IPv4 Address)** – 輸入 IP 位址。 ● 來源 IPv4 位址(Source IPv4 Address) – 按下+新增(+Add)輸入 IP 位址。 **IPv4 子網(IPv4 Subnet)**–輸入 IP 位址和子網路遮罩。 ● 來源 IPv4 子網位址(Source IPv4 Subnet Address) -按下+新增(+Add)輸入帶有子網路遮罩的 IPv4 位址。 **IPv6 位址(IPv6 Address)**-輸入 IPv6 位址。 ● 來源 IPv6 位址(Source IPv6 Address) – 按下+新增(+Add)輸入 IPv6 位址。 **IPv6 子網(IPv6 Subnet)** – 輸入 IPv6 位址和前置碼長度。 ● 來源 IPv6 子網位址(Source IPv6 Subnet Address) -按下+新增(+Add)輸入帶有子網路遮罩的 IPv6 位址。 **IP 物件(IP Object)** – 允許選擇事先定義的 IP 物件。 ● 來源 IP 物件(Source IP Object) – 按下+新增(+Add)選擇 IP 物件。 **IP 群組(IP Group)**–允許選擇事先定義的 IP 群組。 ● 來源 IP 群組(Source IP Group) -按下+新增(+Add)選擇 IP 群組。 **MAC 物件(MAC Object)** –允許選擇事先定義的 MAC 物件。 ● 來源 MAC 物件(Source MAC Object) – 按下+新增(+Add)以選擇 MAC 物件。 **MAC 群組(MAC Group)** – 允許選擇事先定義的 MAC 群組。 來源 MAC 群組(Source MAC Group) - 按下+新增(+Add)選擇 MAC 群組。
目的 **(Destination)**	設定目標 IP 位址。 若要手動設定 IP 位址，請選擇任一 / IPv4 位址 / IPv4 子網 / IPv6 位址 / IPv6 子網 / IP 物件 / IP 群組/國家物件作為目的位址並輸入所需資訊。 **任一(Any)** –所有 IP 位址。 **IPv4 位址(IPv4 Address)** – 輸入 IP 位址。 ● 目的 IPv4 位址(Destination IPv4 Address) – 按下+新增(+Add)輸

	入 IP 位址。 **IPv4 子網(IPv4 Subnet)**–輸入 IP 位址和子網路遮罩。 • 目的 IPv4 子網位址(Destination IPv4 Subnet Address) -按下+新增(+Add)輸入帶有子網路遮罩的 IPv4 位址。 **IPv6 位址(IPv6 Address)**-輸入 IPv6 位址。 • 目的 IPv6 位址(Destination IPv6 Address) – 按下+新增(+Add)輸入 IPv6 位址。 **IPv6 子網(IPv6 Subnet)** – 輸入 IPv6 位址和前置碼長度。 • 目的 IPv6 子網位址(Destination IPv6 Subnet Address) - 按下+新增(+Add)輸入帶有子網路遮罩的 IPv6 位址。 **IP 物件(IP Object)** – 允許選擇事先定義的 IP 物件。 • 目的 IP 物件(Destination IP Object) – 按下+新增(+Add)選擇 IP 物件。 **IP 群組(IP Group)** – 允許選擇事先定義的 IP 群組。 • 目的 IP 群組(Destination IP Group) - 按下+新增(+Add)選擇 IP 群組。 **國家物件(Country Object)** – 允許選擇事先定義的國家物件。 • 目的國家物件(Destination Country Object) – 選擇物件。
通訊協定 **(Protocol)**	指定此過濾規則將套用於哪些協定。 • 任一(Any) • 服務物件(Service Object) • TCP/UDP • TCP • UDP • ICMP • ICMPv6 • IGMP • Others
服務類型物件 **(Service Type Object)**	當服務物件設定為通訊協定時，可用此功能。 按下+新增(+Add)選擇您想要的服務類型物件（最多 12 個）。 
指定來源埠號 **(Specify Source Port)**	當協定設定為 TCP、UDP 或 TCP/UDP 時，可用此功能。 切換開關以啟用/停用連接埠設定。 **來源連接埠(Source Port)** – 如果啟用此功能，請提供起始連接埠和結束連接埠值。
目的埠號 **(Destination Port)**	當通訊協定設定為 TCP、UDP 時或是，此功能可用。 預定義埠號範圍，請提供起始與結束埠號值。
通訊協定數值 **(Protocol Number)**	當通訊協定設定為 “其他” 時，此功能可用。 輸入數值。
分段	針對分段資料封包應採取的措施。

(Fragment)	● **不在乎(Don't care)** – 對於碎片化的資料封包，將不採取任何措施。 ● **未分段(Unfragmented)** – 將規則套用於未分段的套件。 ● **分段(Fragmented)** – 將此規則套用至分段封包。 ● **太短(Too Short)** – 僅對太短而無法包含完整頭部的資料封包套用此規則。
動作(Action)	
動作 **(Action)**	當封包符合規則時要採取的動作。 **通過(Pass)** - 符合規則的資料封包將立即通過。 **封鎖(Block)** - 符合規則的資料封包將立即丟棄。
繞過內容過濾器 **(Bypass Content Filter)**	可按下切換開關以啟用此功能。 如果啟用此功能，Vigor 路由器將繞過內容過濾規則進行資料傳輸。
啟用 Syslog **(Enable Syslog)**	切換開關以啟用將過濾器日誌記錄到 SysLog 的功能。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。



選擇現有的 IP 過濾設定檔之一，將會出現更多選項。

可用設定說明如下：

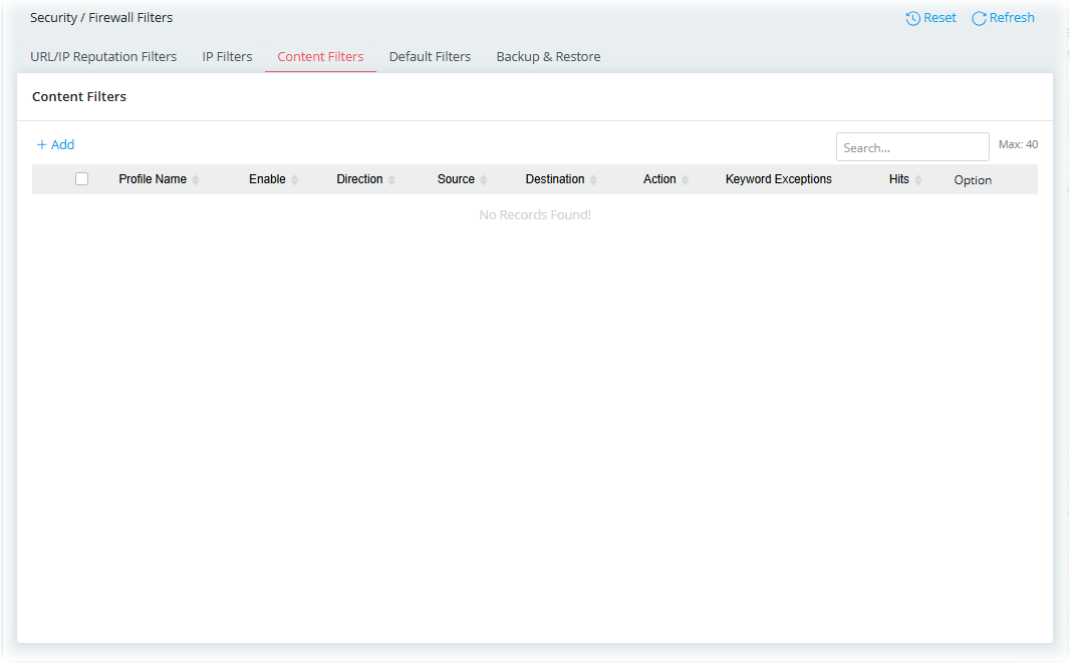
項目	說明
仿製(Clone)	複製選定的 IP 過濾器設定文件，並賦予其新名稱。
ResetHits	將每個 IP 規則在封包比對時的匹配次數重設為預設值。
刪除多數 **(MultipleDelete)**	如果選擇了多個 IP 過濾設定文件，請按一下即可一次刪除這些項目。
啟用多數 **(MultipleEnable)**	如果選擇了多個 IP 過濾設定文件，請按一下即可一次啟用這些設定檔。
停用多數 **(MultipleDisable)**	如果選擇了多個 IP 過濾設定文件，請按一下即可一次停用這些設定檔。
編輯(Edit)	修改選定的 IP 過濾設定檔。
刪除(Delete)	移除選定的 IP 過濾設定檔。

II-2-1-3 內容過濾器(Content Filters)

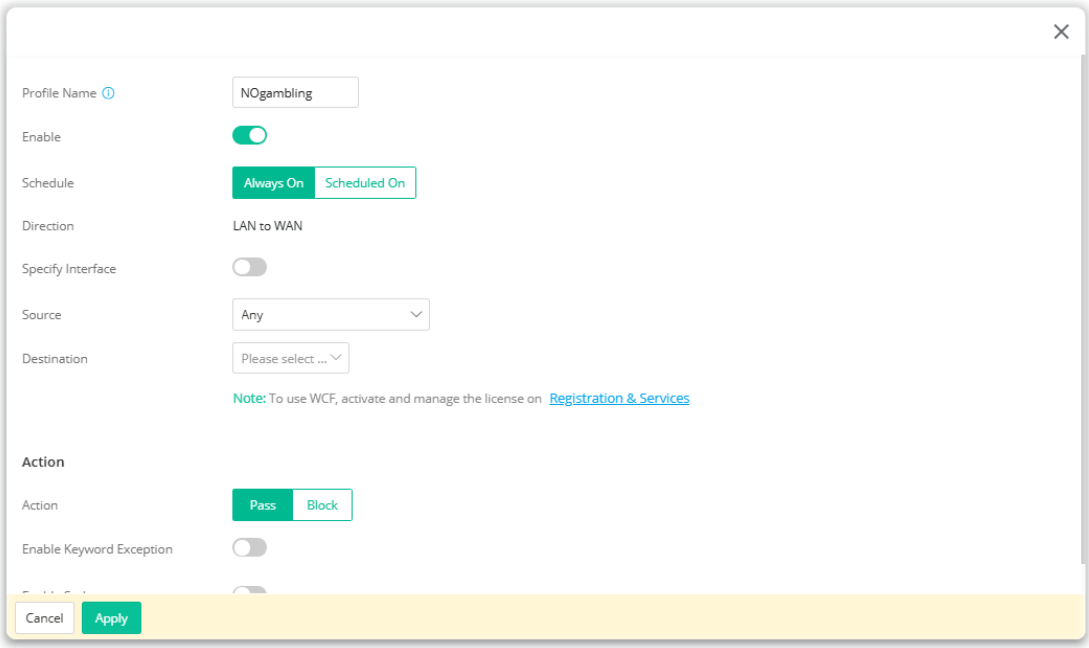
內容過濾器包括 APPE、URL 過濾器和 WCF 服務。 APPE 根據預先定義的模式進行篩選。 URL 過濾器和 WCF 過濾器透過檢查 DNS 請求封包或 TLS 用戶端 Hello 封包中的伺服器名稱來過濾要連接的伺服器。

此頁面可讓您設定最多 40 個內容過濾器設定檔(包括 APPE、URL 和 WCF)。

Vigor 路由器將根據本頁定義的過濾器設定文件，對每個連線數(LAN 到 WAN)中的封包執行有效載荷(內容)分析，直到找出哪個內容過濾器滿足流量要求。



若要新增內容過濾器設定檔，請按下**+新增(+Add)**連結以獲取以下頁面。



可用設定說明如下：

項目	說明

設定檔名稱(Profile Name)	輸入用以識別此過濾器規則的名稱。
啟用(Enable)	切換開關即可啟用/停用此設定檔。
排程(Schedule)	**永遠連線(Always On)** – 如果啟用，規則將始終有效。 **排程啟用(Scheduled On)** - 選擇排程索引編號，允許規則在特定時間啟用。您可以在設定>>物件>>排程(Configurations>>Objects>>Schedule) 15 個排程中選擇排程，最多可選 4 個。如果未選擇任何索引，則規則始終啟用狀態。 ● **當排程啟用時，清除連線數(Clear Session when Schedule is On)** - 如果排程任務設定檔啟用了規則更改，請選擇此選項以清除現有會話。所有連線都將被重置。
方向(Direction)	指定此過濾規則適用的流量流向。
指定介面 **(Specify Interface)**	切換開關即可啟用/停用此功能。 如果啟用，請指定流量介面。 **指定 LAN (Specified LAN)** – 選擇 LAN 介面。
來源 **(Source)**	設定來源 IP 位址。 若要手動設定 IP 位址，請選擇任一 / IPv4 位址 / IPv4 子網 / IPv6 位址 / IPv6 子網 / IP 物件 / IP 群組/ MAC 物件 / MAC 群組作為資訊來源並輸入所需資訊。 **任一(Any)** –所有 IP 位址。 **IPv4 位址(IPv4 Address)** – 輸入 IP 位址。 ● 來源 IPv4 位址(Source IPv4 Address) – 按下+新增(+Add)輸入 IP 位址。 **IPv4 子網(IPv4 Subnet)**–輸入 IP 位址和子網路遮罩。 ● 來源 IPv4 子網位址(Source IPv4 Subnet Address) -按下+新增(+Add)輸入帶有子網路遮罩的 IPv4 位址。 **IPv6 位址(IPv6 Address)**-輸入 IPv6 位址。 ● 來源 IPv6 位址(Source IPv6 Address) – 按下+新增(+Add)輸入 IPv6 位址。 **IPv6 子網(IPv6 Subnet)** – 輸入 IPv6 位址和前置碼長度。 ● 來源 IPv6 子網位址(Source IPv6 Subnet Address) -按下+新增(+Add)輸入帶有子網路遮罩的 IPv6 位址。 **IP 物件(IP Object)** – 允許選擇事先定義的 IP 物件。 ● 來源 IP 物件(Source IP Object) – 按下+新增(+Add)選擇 IP 物件。 **IP 群組(IP Group)**–允許選擇事先定義的 IP 群組。 ● 來源 IP 群組(Source IP Group) -按下+新增(+Add)選擇 IP 群組。 **MAC 物件(MAC Object)** –允許選擇事先定義的 MAC 物件。 ● 來源 MAC 物件(Source MAC Object) – 按下+新增(+Add)以選擇 MAC 物件。 **MAC 群組(MAC Group)** – 允許選擇事先定義的 MAC 群組。 ● 來源 MAC 群組(Source MAC Group) - 按下+新增(+Add)選擇 MAC 群組。
目的 **(Destination)**	選擇要包含在過濾器中的特定 WCF 和/或 APPE 和/或 UCF (關鍵字物件) 設定檔。
動作(Action)	
動作 **(Action)**	當封包符合規則時要採取的動作。 **通過(Pass)** - 符合規則的資料封包將立即通過。

	封鎖(Block) – 符合規則的資料封包將立即丟棄。
啟用關鍵字例外 (Enable Keyword Exception)	切換開關即可啟用/停用此功能。 **關鍵字例外(Keyword Exceptions)** – 顯示選定的關鍵字物件。 系統也會使用選定的關鍵字設定檔檢查連線數。如果連線數符合關鍵字篩選條件，系統將執行相反的操作。
啟用(Enable) Syslog	切換開關以啟用將過濾器日誌記錄到系統日誌的功能。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

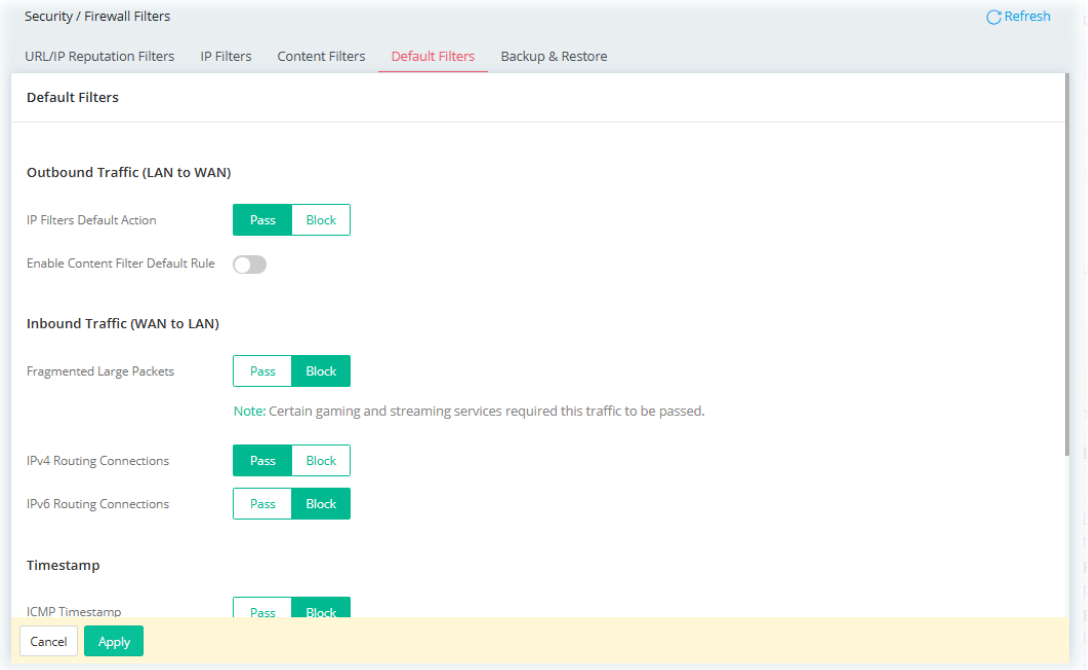
II-2-1-4 預設過濾器(Default Filters)

防火牆會依照以下順序過濾流量：

1. 資料過濾器組和規則
2. 封鎖來自廣域網路的連線
3. 預設規則

此頁面可讓您選擇過濾設定文件，包括 QoS、負載平衡策略、WCF、APP 強制執行、URL 內容過濾器，用於透過 Vigor 路由器進行資料傳輸。

預設規則適用於所有未受其他過濾器或規則限制的流量。



可用設定說明如下：

項目	說明
輸出流量(LAN 至 WAN)(Outbound Traffic (LAN to WAN))	
IP 過濾器預設動作 (IP Filters Default Action)	設定未符合任何 IP 過濾規則之封包(對外輸出)的預設動作。 **通過(Pass)** - 不符合任何 IP 過濾規則的封包將被放行，然後等待內容過濾。 **封鎖(Block)** – 不符合任何 IP 過濾規則的封包將被 Vigor 系統封鎖。

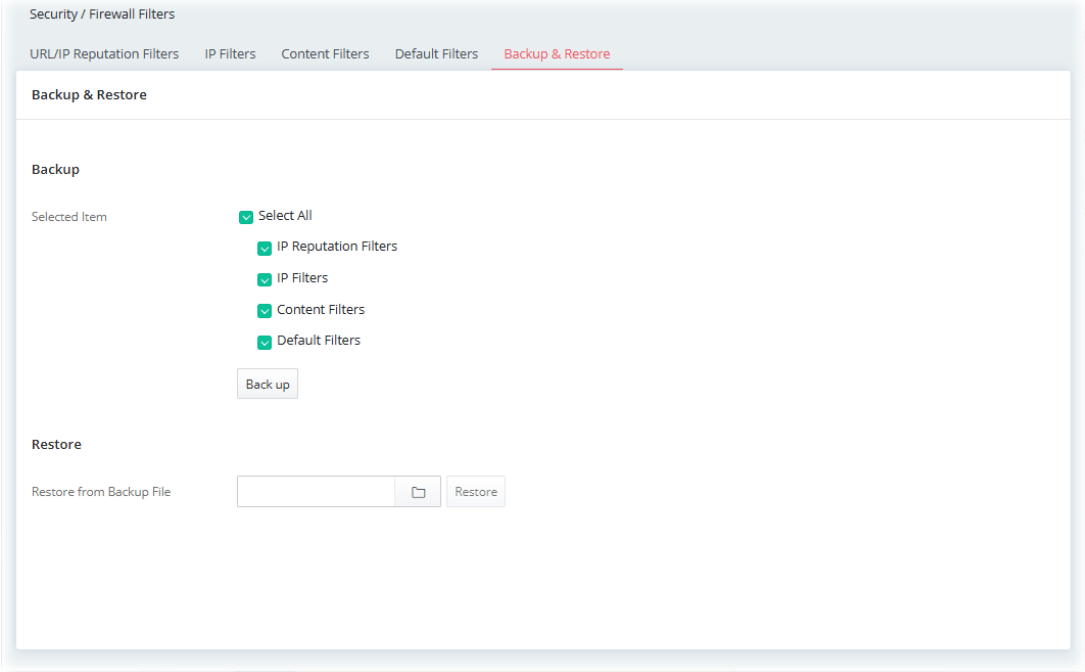
啟用內容過濾器預設規則 (Enable Content Filters Default Rule)	切換開關即可啟用或停用此功能。
內容過濾器預設規則 (Content Filters Default Rule)	定義符合下列內容目標規則的對外輸出流量的預設操作。 如果輸出流量不符合任何 IP/內容過濾規則，且 **IP 過濾器預設操作**如果為 PASS，則也會根據此規則進行額外檢查。 如果對外輸出流量符合上述條件，但仍不符合下列內容目標規則，系統將執行相反的操作。 **通過(Pass)** –符合以下內容目標規則的輸出流量將被允許通過；否則，將被阻止。 **封鎖(Block)** – 符合下列內容目標規則的輸出流量將被阻止。否則，將允許其通過。
內容目的 (Content Destination)	選擇要包含在過濾器中的特定 WCF 和/或 APPE 和/或 UCF（關鍵字物件）設定檔。
輸入流量(WAN 至 LAN)(Inbound Traffic (WAN to LAN))	
分段的大型封包 (Fragmented Large Packets)	某些遊戲和視訊串流服務使用分段式 UDP 資料封包來傳輸資料。 **通過(Pass)**- 無論資料封包大小如何，路由器始終將分片資料封包直接傳遞，而不進行重組。 **封鎖(Block)** - 路由器會嘗試重新組裝長度不超過一定值（例如 15xx~2102 千位元組）的碎片化資料封包。大於該值的資料封包將被丟棄。
IPv4 路由連線 (IPv4 Routing Connections)	**通過(Pass)** – 對於使用 IP 路由子網路接收 WAN IPv4 位址的 LAN 主機，選擇此選項可阻止 WAN 主機連線至 LAN 主機。此選項對私有 LAN 子網路上的 LAN 主機無效。 **封鎖(Block)** - 阻止 LAN 主機使用 IPv4 連線到 WAN 主機。
IPv6 路由連線 (IPv6 Routing Connections)	**通過(Pass)** –IPv6 不使用網路位址轉換 (NAT)，因此所有 LAN 主機都會取得暴露給 WAN 的真實 IPv6 IP 位址。 **封鎖(Block)** - 阻止 WAN 主機使用 IPv6 連線到 LAN 主機。
Syslog	**啟用 Syslog (Enable Syslog)** – 如果啟用，與預設過濾器相關的日誌將記錄到系統日誌中。
取消(Cancel)	捨棄目前設定。
套用(Apply)	儲存目前設定。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-2-1-5 備份與還原(Backup & Restore)

此頁面允許備份和還原路由器設定。

除了還原 Vigor2928 本身的設定備份外，還可以從某些 DrayTek 路由器還原 Vigor2928 上的備份。



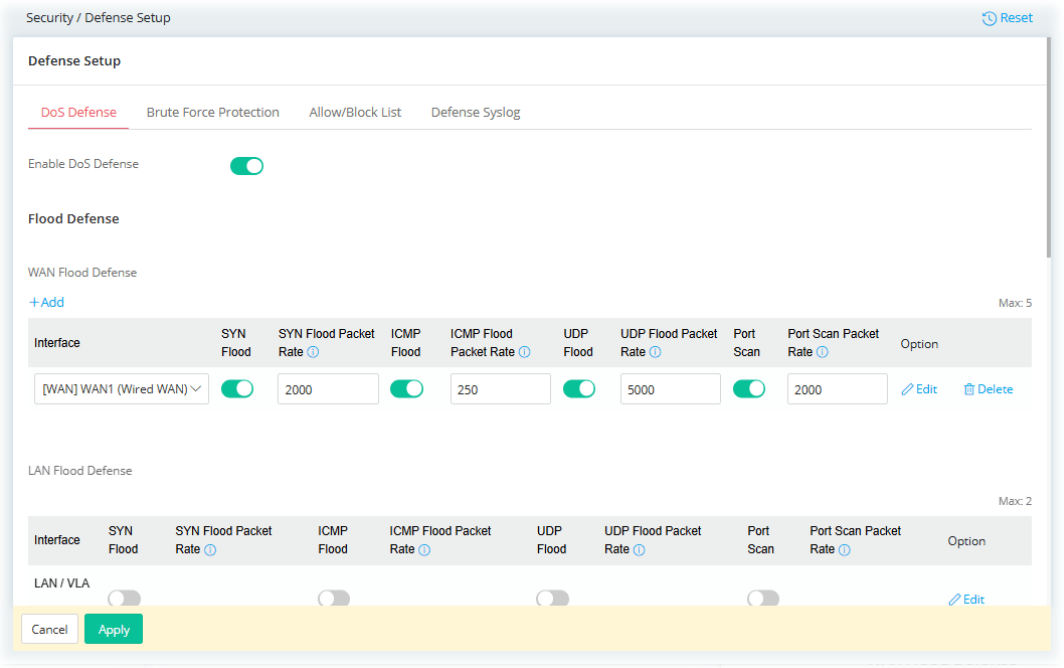
可用設定說明如下：

項目	說明
備份(Backup)	**選定項目(Selected Items)** – 選擇項目。 **備份(Back up)** – 根據上面選擇的項目(選擇全部、IP 過濾器、內容過濾器和預設過濾器）執行此路由器的設定備份。
還原(Restore)	**還原自備份檔案(Restore from Backup File)** – 按此以指定要用來還原的檔案。 **還原(Restore)** – 按此開始還原作業。如果備份檔案已加密，系統會提示您輸入密碼。

II-2-2 攻擊防禦設定(Defense Setup)

II-2-2-1 防禦 DoS 攻擊(DoS Defense)

作為 IP 過濾/防火牆的子功能，**防禦 DoS 攻擊(DoS Defense)**設定中，包含幾種類型的偵測/防禦功能。預設情況下，DoS 防禦功能處於停用狀態。



可用設定說明如下：

項目	說明
啟用防禦 DoS 攻擊功能 (Enable DoS Defense)	切換開關以啟用/停用防禦 DoS 攻擊功能。
	Flood 攻擊防禦(Flood Defense)
WAN Flood 攻擊防禦 (WAN Flood Defense)	**+新增(+Add)** – 按此設定 Flood 攻擊防禦設定檔，最多可建立 6 個設定檔 **介面(Interface)** – 選擇一個 WAN 介面。設定廣域網路的封包速率值以滿足您的需求。 **SYN Flood** – 切換此開關可啟用/停用 SYN flood 攻擊、防禦。當 SYN 封包的到達率超過門檻值時，路由器將開始隨機丟棄 TCP SYN 封包，丟棄時間由逾時設定決定。這樣做是為了防止 TCP SYN 封包耗盡路由器資源。 ● **SYN Flood 封包速率(SYN Flood Packet Rate)** –門檻值和逾時的預設值分別為每秒 2000 個資料封包和 10 秒。 **ICMP Flood** – 切換此開關可啟用/停用 ICMP flood 攻擊防禦。當 ICMP 封包的到達率超過門檻值時，路由器將開始隨機丟棄 TCP SYN 封包，丟棄時間由逾時設定決定。 ● **ICMP Flood 封包速率(ICMP Flood Packet Rate)** –門檻值和逾時的預設值分別為每秒 250 個資料封包和 10 秒。 **UDP Flood** – 切換此開關可啟用/停用 UDP Flood 攻擊防禦。當 UDP 封包的到達率超過門檻值時，路由器將開始隨機丟棄 TCP SYN 封包，丟棄時間由逾時時間設定。 ● **UDP Flood 封包速率(UDP Flood Packet Rate)** –門檻值和逾時的

	預設值分別為每秒 5000 個資料封包和 10 秒。 **Port Scan** –切換此開關可啟用/停用連接埠掃描偵測。連接埠掃描會向一系列連接埠發送封包，試圖找到回應的服務，從而攻擊您的網路。啟用連接埠掃描偵測後，當路由器偵測到連接埠掃描活動超過門檻值時，會發送警告訊息。 ● **Port Scan 封包速率(Port Scan Packet Rate)** – 預設門檻值為每秒 2000 個資料封包。 **選項(編輯/刪除(Edit/Delete))** - 點擊**編輯**點擊開啟設定頁面進行詳細修改（資料封包速率和突發速率）。**刪除**刪除選定的條目。
LAN Flood 攻擊防禦 (LAN Flood Defense)	**介面(Interface)** – 它包含 LAN/VLAN 和 VPN 設定。其中，LAN/VLAN 的預設封包速率值與 WAN flood 防禦相同，並將對 VLAN 內的所有 LAN 介面生效。 VPN 的封包速率值將對用於 VPN 的 LAN 介面生效。請根據需要設定 LAN/VLAN 和 VPN 的封包速率值。 **SYN Flood** – 切換此開關可啟用/停用 SYN flood 防禦。當 SYN 封包的到達率超過門檻值時，路由器將開始隨機丟棄 TCP SYN 封包，丟棄時間由逾時設定決定。這樣做是為了防止 TCP SYN 封包耗盡路由器資源。 ● **SYN Flood 封包速率(SYN Flood Packet Rate)** – 門檻值和逾時的預設值分別為每秒 2000 個資料封包和 10 秒。 **ICMP Flood** – 切換此開關可啟用/停用 ICMP flood 攻擊防禦。當 ICMP 封包的到達率超過門檻值時，路由器將開始隨機丟棄 TCP SYN 封包，丟棄時間由逾時設定決定。 ● **ICMP Flood 封包速率(ICMP Flood Packet Rate)** –門檻值和逾時的預設值分別為每秒 250 個資料封包和 10 秒。 **UDP Flood** – 切換此開關可啟用/停用 UDP flood 攻擊防禦。當 UDP 封包的到達率超過門檻值時，路由器將開始隨機丟棄 TCP SYN 封包，丟棄時間由逾時時間設定。 ● **UDP Flood 封包速率(UDP Flood Packet Rate)**–門檻值和逾時的預設值分別為每秒 5000 個資料封包和 10 秒。 **Port Scan** –切換此開關可啟用/停用連接埠掃描偵測。連接埠掃描會向一系列連接埠發送封包，試圖找到回應的服務，從而攻擊您的網路。啟用連接埠掃描偵測後，當路由器偵測到連接埠掃描活動超過門檻值時，會發送警告訊息。 ● **Port Scan 封包速率(Port Scan Packet Rate)** –預設門檻值為每秒 2000 個資料封包。 **選項(編輯/刪除(Edit/Delete))** – 按下**編輯(Edit)**開啟設定頁面進行詳細修改(資料封包速率和突發速率)。**刪除**刪除選定的條目。
基本(General)	切換開關以啟用/停用以下列出的功能。 **阻擋 IP 選項(Block IP Options)** – 如果啟用此功能，Vigor 路由器將忽略資料標頭中設定了 IP 選項欄位的 IP 封包。 IP 選項很少使用，但攻擊者可能會濫用它們，因為它們攜帶有關私有網路的訊息，例如安全設定、TCC（封閉用戶群組）參數、一系列網際網路位址、路由訊息等，這些資訊通常無法從外部網路獲取。外部竊聽者可以利用這些資訊來發現私人網路的詳細資訊。 **阻擋 Land 攻擊(Block Land)** – 啟用此功能可阻止 LAND 攻擊。LAND 攻擊是指攻擊者發送偽造的 SYN 封包，將來源位址和目標位址都設定為目標系統的位址，從而導致目標系統不斷回復自身。 **阻擋 Smurf 攻擊(Block SMURF)** – 啟用此功能可阻止 Smurf 攻擊。路由器將忽略任何廣播的 ICMP echo 請求。 **阻擋追蹤路由(Block Trace Route)** – 啟用此選項可封鎖路由追蹤。路由器將不會轉送路由追蹤封包。 **阻擋 SYN Fragment 封包(Block SYN Fragment)** – 啟用此選項可封鎖 SYN 封包分段。路由器將丟棄任何同時設定了 SYN 位元和更多分段位元的套件。

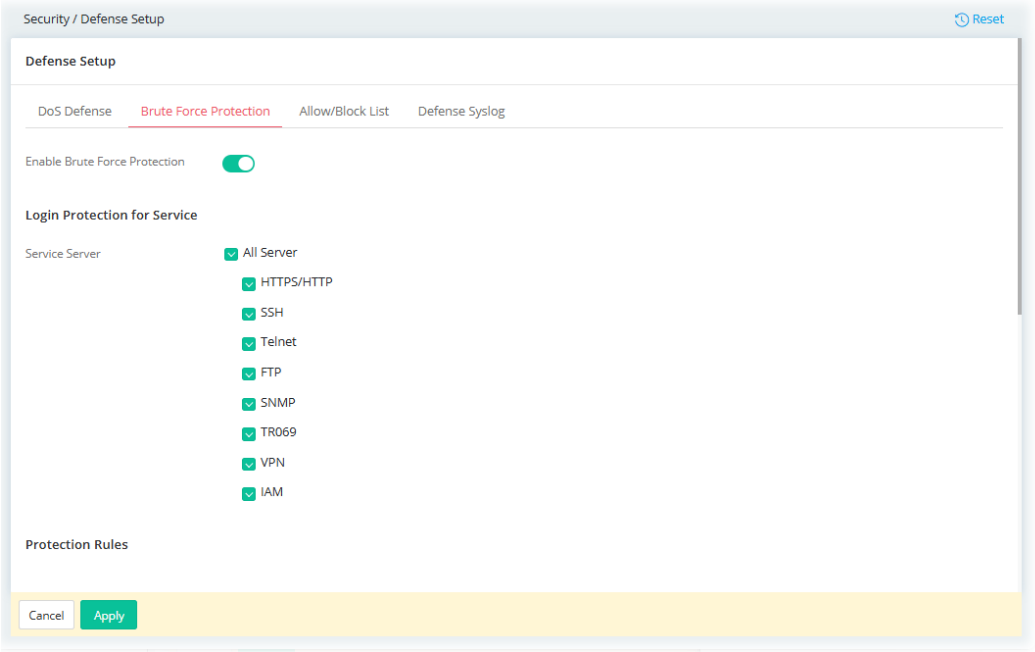
	阻擋 Fraggle (Block Fraggle) – 啟用此功能可阻止 Fraggle 攻擊。將阻止從網際網路接收的廣播 UDP 封包。 啟用此功能可能會攔截一些合法的資料封包。由於所有來自網路的廣播 UDP 封包都會被攔截，因此來自網路的 RIP 封包也可能會遺失。 **阻擋 Tear Drop 攻擊(Block Tear Drop)** – 啟用此功能可阻止 Tear Drop 攻擊。某些用戶端在接收長度超過最大限制的 ICMP 資料封包（封包）時可能會崩潰。路由器會丟棄任何長度超過 1024 位元組的分段 ICMP 封包。 **阻擋 Ping of Death 攻擊(Block Ping of Death)** – 啟用此功能可阻止 Ping of Death 攻擊，該攻擊會將碎片化的 ping 封包傳送到目標主機，導致這些主機在重新組裝格式錯誤的 ping 封包時崩潰。 **阻擋 ICMP 封包片段攻擊(Block ICMP Fragment)** – 啟用此功能可阻止 ICMP 封包片段。設定了更多片段位元的 ICMP 封包將被丟棄。 **阻擋未知協定(Block Unknown Protocol)** – 啟用此功能後，路由器將阻止協定號未指派的資料封包。每個 IP 封包的資料標頭中都有一個協定字段，用於指示上層網路運行的協定類型。然而，目前大於 100 的協定類型是保留起來的，尚未定義。因此，路由器應具備偵測並拒絕此類資料封包的能力。
ARP Spoofing 攻擊防禦(ARP Spoofing Defense)	
阻擋 ARP 回應(Block ARP replies with)	此功能可保護網路免受 ARP(位址解析協定)欺騙攻擊。 **來源 MAC 位址不一致(Inconsistent Source MAC addresses)** – 如果 ARP 封包中的傳送者 MAC 位址與 ARP 封包乙太網路標頭中的來源 MAC 位址不匹配，Vigor 系統將立即阻止該封包。 **目的 MAC 位址不一致(Inconsistent Destination MAC addresses)** – 如果 ARP 封包中的目標 MAC 位址與 ARP 封包乙太網路標頭中的目標 MAC 位址不匹配，Vigor 系統將立即阻止該封包。
在 ARP 表格中的虛擬 MAC 位址 (VRRP)	**接受(Accept)** – 虛擬 MAC 位址可以記錄在 ARP 表中。 **降低(Decline)** – 虛擬 MAC 位址無法記錄在 ARP 表中。
IP Spoofing 攻擊防禦(IP Spoofing Defense)	
阻擋 IP 封包(Block IP Packets with)	IP 欺騙防禦可防止未經授權的訪問，從而保護資料完整性，確保網路安全。 **來自 WAN 端來源 IP 位址不一致(Inconsistent Source IP addresses from WAN)** – 封鎖來自廣域網路的虛假 IP 位址。例如，如果來自廣域網路介面的來源 IP 位址是區域網路子網路的 IP 封包，Vigor 系統將立即封鎖這些封包。 **來自 LAN 端來源 IP 位址不一致(Inconsistent Source IP addresses from LAN)** – 攔截來自區域網路的虛假 IP 位址。例如，如果來自區域網路介面的來源 IP 位址是廣域網路子網路的 IP 封包，Vigor 系統將立即攔截這些封包。
取消(Cancel)	捨棄目前設定。
套用(Apply)	儲存目前設定。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-2-2-2 BFP 設定(BFP Settings)

BFP 是 Brute Force Protection 的縮寫。

任何嘗試透過 Vigor 路由器存取網際網路的用戶端都會被要求進行使用者身份驗證。此功能可以防止駭客嘗試所有可能的字母、數字和符號組合，直到找到正確的密碼，從而保護 Vigor 路由器免受攻擊。



可用設定說明如下：

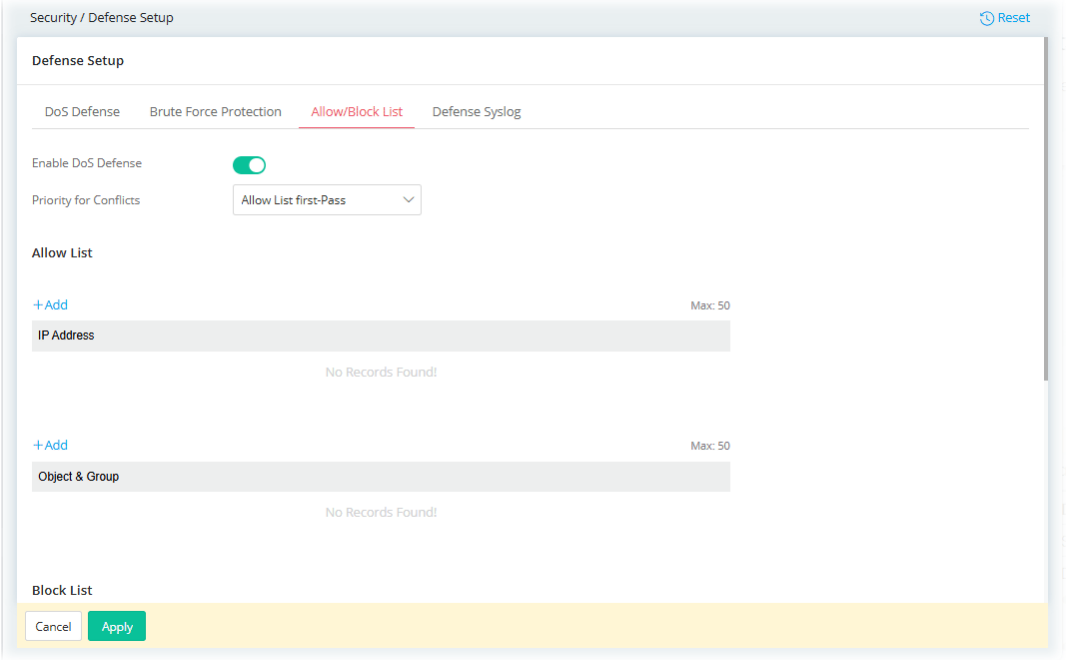
項目	說明
啟用啟用暴力攻擊防護(Enable Brute Force Protection)	切換開關以啟用或停用暴力破解登入嘗試的偵測。
	服務登入防護(Login Protection for Service)
服務伺服器(Service Server)	BFP 可以保護 Vigor 路由器的登入功能免受駭客攻擊，防止駭客透過 HTTPS/HTTP、SSH、Telnet、FTP、SNMP、TR-069、VPN、IAM 等協定破解帳戶和密碼。 預設為**所有伺服器(All Server)**。
	防護規則(Protection Rules)
IAM 使用者(IAM Users)	定義 IAM 使用者的保護規則(例如使用 FTP 和 IAM 服務)。 **啟用(Enable)** – 切換開關以啟用或停用 IAM 使用者的防禦設定設定。 **最多登入嘗試次數(Maximum Login Attempts)** – 指定封鎖進一步登入前允許的最大登入失敗次數。 多次登入失敗(達到最大登入嘗試次數)的使用者將被處罰一段時間，不得登入 Vigor 系統(例如使用 FTP 和 IAM 服務)。 **罰期(Penalty Period)** – 設定滯納金期限。 在此期間，用戶將無法登入。此設定旨在防止外部自動化攻擊透過反覆嘗試來猜測密碼、驗證碼或其他憑證。 **啟用使用者帳戶鎖定(Enable User Account Lockout)** – 切換開關以啟用

	或停用 IAM 使用者帳戶鎖定功能。 **登入嘗試(Login Attempts)** – 為所有使用者帳號設定最大登入失敗次數。達到此限制後，如果登入失敗 (例如透過 FTP 或 IAM 服務) ，IAM 使用者帳戶將被鎖定。 **在下述條件後，解鎖使用者帳戶(Unlock User Account After)** – 設定解鎖特定 IAM 使用者帳號的時間段。 **郵件通知(Email Notification)** – 當使用者發生帳戶鎖定事件時，透過電子郵件向該帳戶發送通知。
VPN	定義 VPN 連線的保護規則。 **啟用(Enable)** – 切換開關以啟用或停用 VPN 連線的防禦設定。 **最多登入嘗試次數(Maximum Login Attempts)** – 指定封鎖進一步登入前允許的最大登入失敗次數。 多次登入失敗(達到最大登入嘗試次數)的使用者將被處罰一段時間，不得登入 Vigor 系統。 **罰期(Penalty Period)** – 設定滯納金期限。 在此期間，用戶將無法登入或存取 Vigor 系統。此設定旨在防止外部自動化攻擊透過反覆嘗試來猜測密碼、驗證碼或其他憑證。 **郵件通知(Email Notification)** - 當使用者發生帳戶鎖定事件時，透過電子郵件向該帳戶發送通知。
System Account	定義系統帳戶(使用者和管理員)的保護規則。 **啟用(Enable)** – 切換開關以啟用或停用系統帳號的防禦設定設定。 **最多登入嘗試次數(Maximum Login Attempts)** – 系統帳號如果多次登入失敗，達到最大登入嘗試次數，將被處罰一段時間，不得登入 Vigor 系統(例如，使用 HTTPS/HTTP、SSH、Telnet、SNMP 和 TR069 服務)。 **罰期(Penalty Period)**– 設定滯納金期限。 在此期間，用戶將無法登入或存取 Vigor 系統。此設定旨在防止外部自動化攻擊透過反覆嘗試來猜測密碼、驗證碼或其他憑證。 **啟用使用者帳戶鎖定(Enable User Account Lockout)** – 切換開關以啟用或停用系統帳號鎖定功能。 **登入嘗試(Login Attempts)** – 指定所有系統帳戶的最大登入失敗次數。超過此次數後，如果登入失敗 (例如，登入 HTTPS/HTTP、SSH、Telnet、SNMP 和 TR-069 服務) ，系統帳戶將被鎖定。 **在下述條件後，解鎖使用者帳戶(Unlock User Account After)** – 指定解鎖特定系統帳戶的時間段。 **郵件通知(Email Notification)** - 當使用者發生帳戶鎖定事件時，透過電子郵件向該帳戶發送通知。
取消(Cancel)	捨棄目前設定。
套用(Apply)	儲存目前設定。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-2-2-3 白/黑名單(Allow/Block List)

為用戶端定義白名單和黑名單。



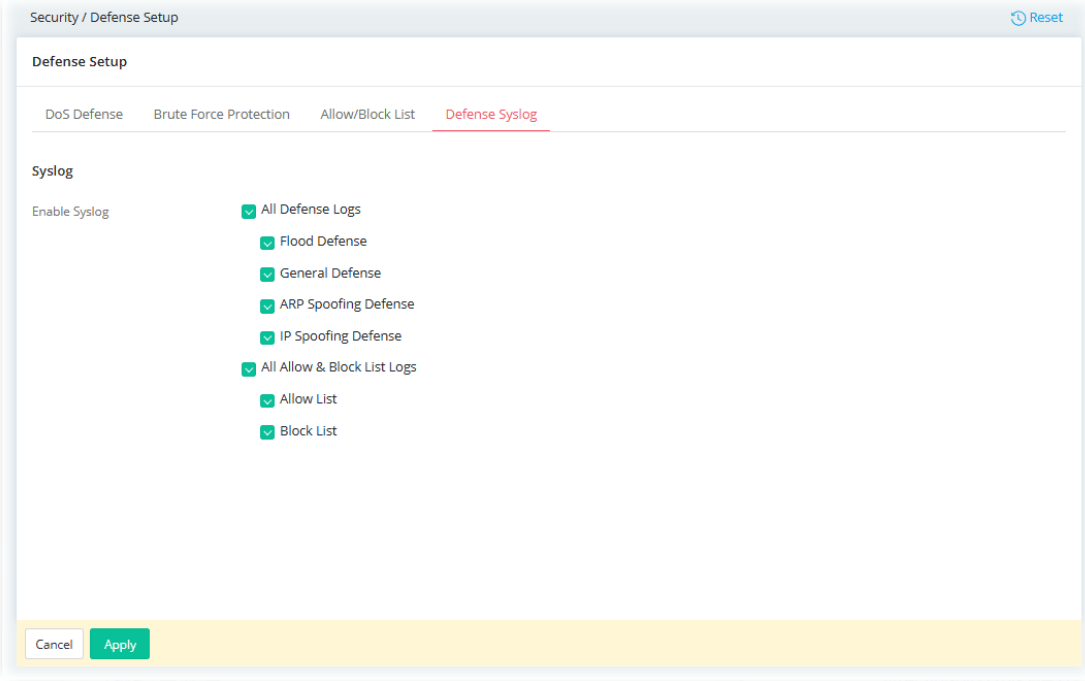
可用設定說明如下：

項目	說明
啟用防禦 DoS 攻擊功能(Enable DoS Defense)	切換開關以啟用或停用 DoS 防禦功能。
衝突優先等級(Priority for Conflicts)	決定衝突的處理順序/優先順序。 ● **白名單優先通過(Allow List first-Pass)** – 允許白清單中列出的 IP 位址通過。 ● **黑名單優先封鎖(Block List first-Block)** – 封鎖黑名單上的 IP 位址通過。
白名單(Allow List)	定義可透過 Vigor 路由器接收/傳送封包的用戶端 IP 位址。 **+新增(+Add)** – 按此新增 IP 位址到白清單中。 ● **IP 位址(IP Address)** – 輸入 IP 位址。 **+新增(+Add)** – 按此新增物件/群組為白名單中的成員。 ● **物件與群組(Object & Group)** – 使用下拉式清單指定物件和群組設定檔。
黑名單(Block List)	定義 Vigor 路由器將阻止的客戶端 IP 位址。 **+新增(+Add)** – 按此新增 IP 位址到黑清單中。 ● **IP 位址(IP Address)** – 輸入 IP 位址。 **+新增(+Add)** –按此新增物件/群組為黑名單中的成員。 ● **物件與群組(Object & Group)** – 使用下拉式清單指定物件和群組設定檔。
套用(Apply)	儲存目前設定。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-2-2-4 攻擊防禦 Syslog (Defense Syslog)

顯示 Vigor 路由器提供的系統日誌類型。與 Vigor 路由器的運作、狀態和防禦相關的資訊將被記錄到系統日誌伺服器。



可用設定說明如下：

項目	說明
啟用 Syslog (Enable Syslog)	選擇功能項目。操作步驟、結果或與該功能相關的任何資訊都將記錄到系統日誌伺服器中。
取消(Cancel)	捨棄目前設定。
套用(Apply)	儲存目前設定。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

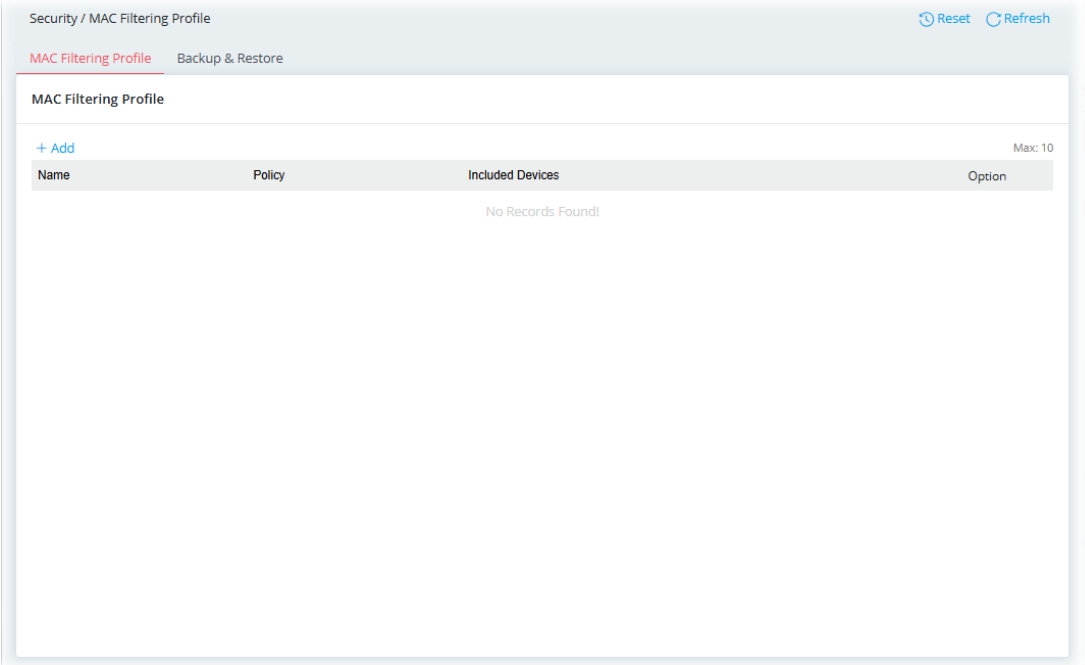
II-2-3 MAC 過濾設定檔(MAC Filtering Profile)

Vigor 路由器可以透過參考 MAC 位址黑名單/白名單來限制無線用戶端的存取。

系統管理員可以透過將無線用戶端的 MAC 位址新增至黑名單來封鎖無線用戶端連線；也可以透過將無線用戶端 MAC 位址新增至白名單來允許部分無線用戶端連線。

II-2-3-1 MAC 過濾設定檔(MAC Filtering Profile)

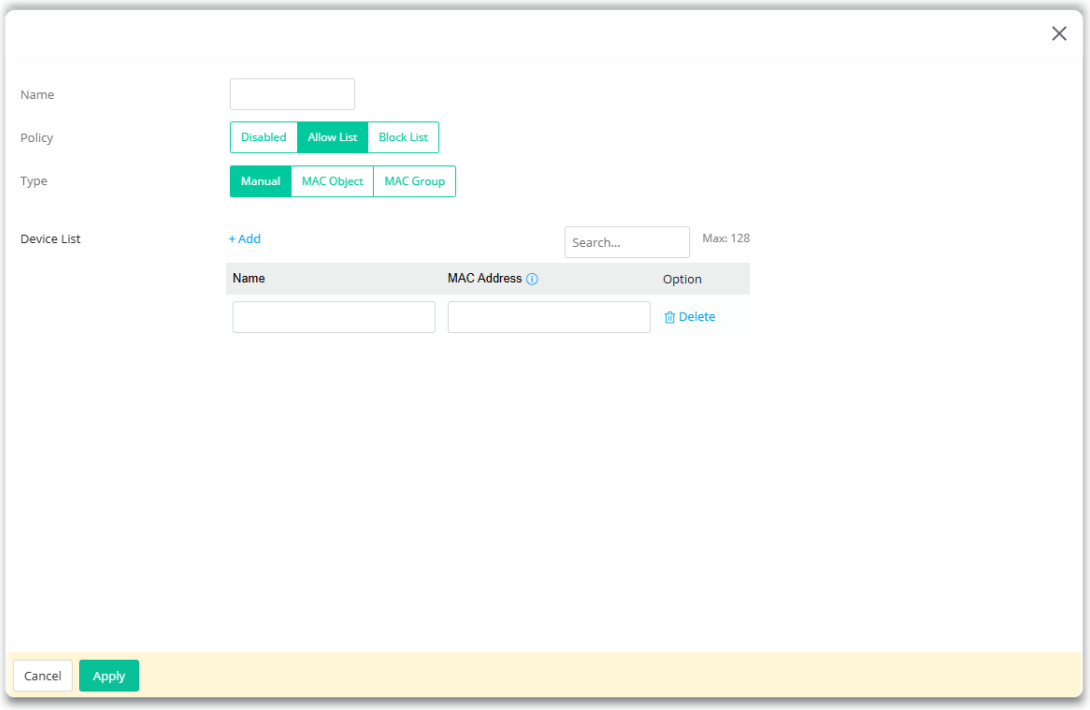
此頁面可讓您設定最多 10 個 MAC 位址過濾設定檔案(將套用於**設定>>無線區域網路>>SSID(Configuration>>Wireless LAN>>SSID** 中之 SSID 項目))，以滿足不同需求。



可用的設定說明如下：

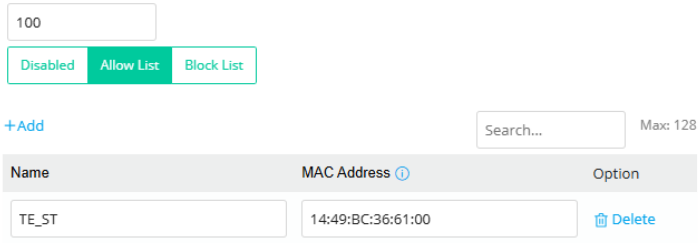
項目	說明
新增(+Add)	按此建立新的設定檔。
編輯(Edit)	按此修正選定的設定檔。
刪除(Delete)	按此移除選定的設定檔。

欲新增一組新的 MAC 過濾設定檔，按下**新增(+Add)**開啟如下頁面。



可用設定說明如下：

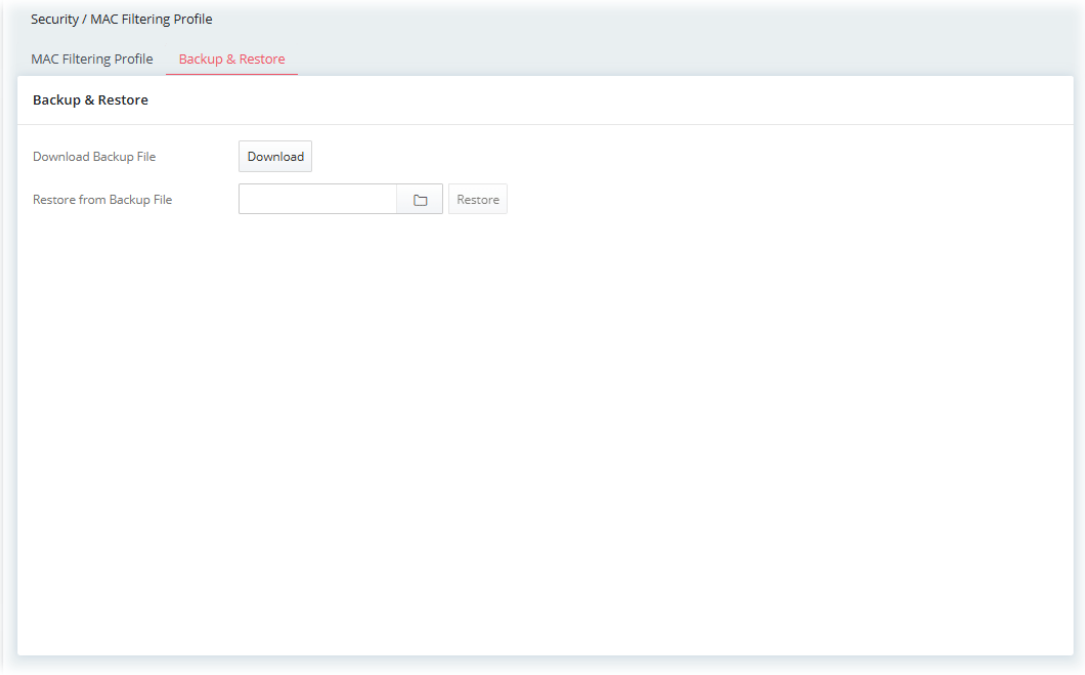
項目	說明

名稱(Name)	輸入設定檔的名稱。
策略(Policy)	**停用(Disabled)** - 停用此設定檔。 如果啟用了此設定檔，繼續設定黑白名單。 **白名單(Allow List)** - 指定名稱。只有 MAC 位址與清單中定義的裝置名稱相符的使用者才能存取此路由器。 **黑名單(Block List)** - 指定名稱。只有 MAC 位址與清單中定義的裝置名稱相符的使用者不得存取存取此路由器。
類型(Type)	決定哪些無線客戶端可以套用至 SSID。 **手動(Manual) –** 輸入特定裝置的 MAC 位址。 **MAC 物件(MAC Object) –** 選擇 MAC 物件。在 MAC 物件下的所有 MAC 位址都可以納入白名單(可通過)或黑名單(不可通過)。 **MAC 群組(MAC Group) –** 選擇 MAC 群組。在 MAC 群組下的所有 MAC 物件都可以納入白名單(可通過)或黑名單(不可通過)。
裝置清單(Device List)	此功能於白名單/黑名單被選為策略時即可使用。 **新增(+Add)** – 按下後出現新的輸入框，即可設定檔名與輸入 MAC 位址。 
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前的設定並離開此頁面。

完成設定之後，按下**套用(Apply)**按鈕儲存相關設定。

II-2-3-2 備份與還原(Backup & Restore)

本頁可讓您將備份及還原 MAC 過濾設定檔。

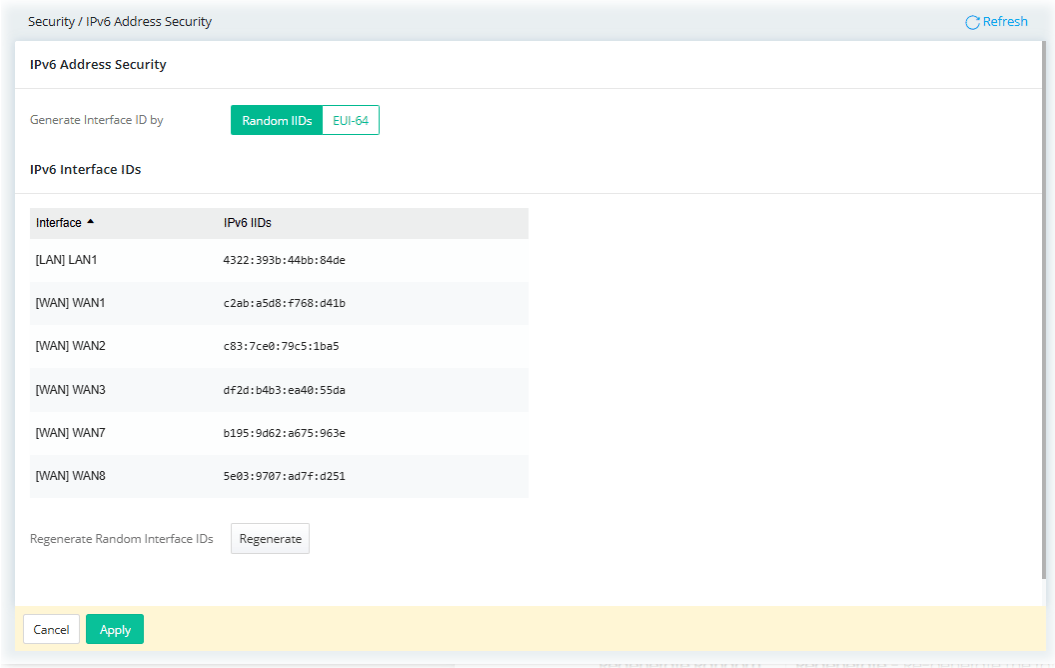


可用設定說明如下：

項目	說明
下載備份檔案 (Download Backup File)	**下載(Download)** - 按此儲存 MAC 過濾設定檔。
還原自備份檔案(Restore from Backup File)	選擇您準備要使用的備份檔案(MAC 過濾設定檔) **還原(Restore)** - 按此還原 MAC 過濾設定檔的內容。

II-2-4 IPv6 位址安全性(IPv6 Address Security)

此頁面可讓您設定 IPv6 介面 ID。



可用設定說明如下：

項目	說明
產生介面 ID 方式 (Generate Interface ID by)	選擇使用隨機 IID 或 EUI-64 IID 作為介面 ID。 • **Random IIDs** • **EUI-64**
IPv6 介面 ID (IPv6 Interface IDs)	顯示介面及其對應的 IPv6 IID。
重新產生隨機介面 ID (Regenerate Random Interface IDs)	**重新產生(Regenerate)** - 為所有介面重新產生隨機 IID。
取消(Cancel)	捨棄目前設定。
套用(Apply)	儲存目前設定。

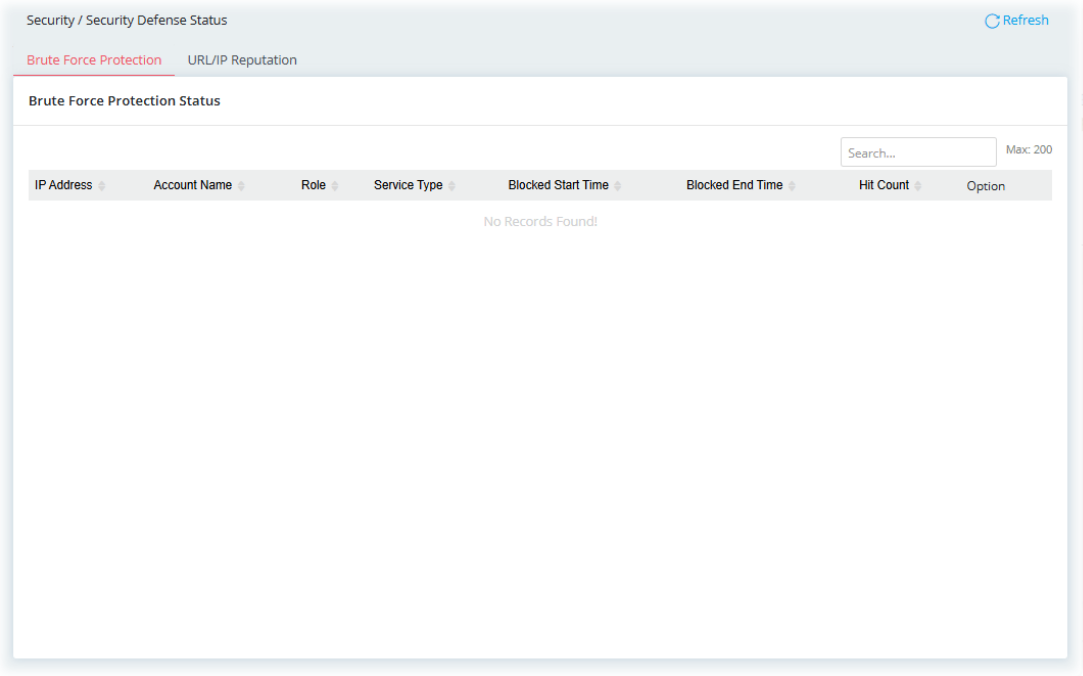
完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-2-5 安全性防禦狀態(Security Defense Status)

路由器目前的安全保護機制包括暴力攻擊防護(BFP)和 IP 信譽保護。本頁面提供有關這些保護機制狀態的詳細資訊。

II-2-5-1 BFP 狀態(BFP Status)

此頁面顯示暴力攻擊防護(BFP)的狀態。

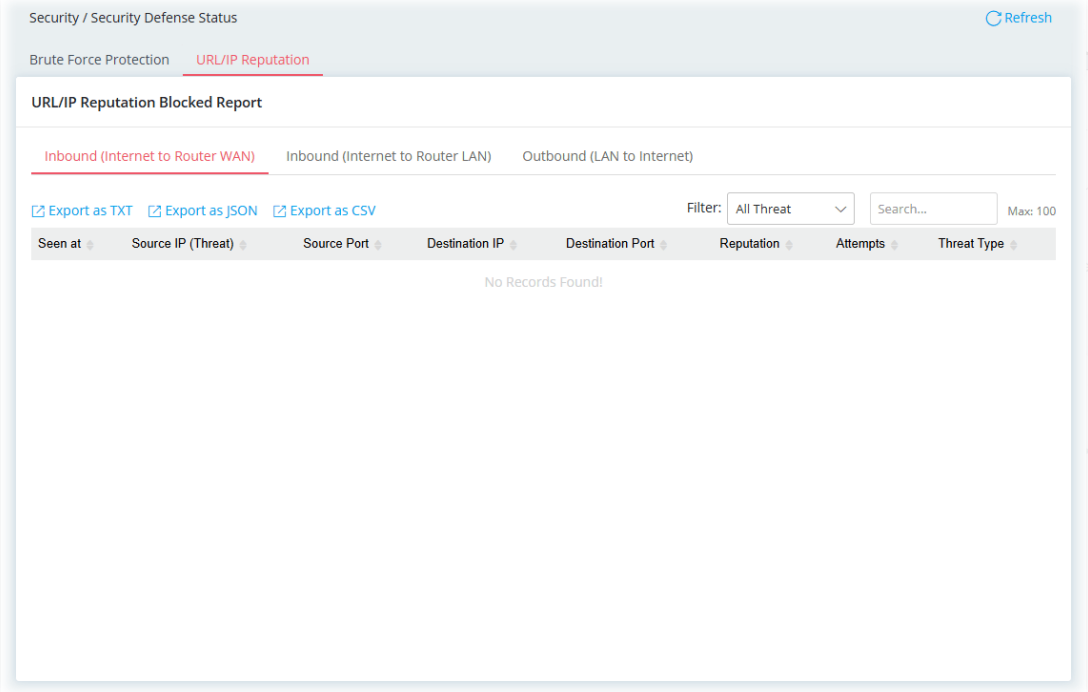


可用設定說明如下：

項目	說明
IP 位址(IP Address)	顯示因使用系統帳戶(例如，登入 HTTPS/HTTP、SSH、Telnet、SNMP 和 TR-069 服務) 而觸發處罰或使用者帳戶鎖定功能而被封鎖的 IP 位址。
帳戶名稱(Account Name)	顯示因使用系統帳戶(例如，登入 HTTPS/HTTP、SSH、Telnet、SNMP 和 TR-069 服務) 而觸發處罰或使用者帳戶鎖定功能而被封鎖的帳戶名稱。
角色(Role)	顯示帳戶的角色。
服務類型(Service Type)	顯示使用者帳戶的服務類型。
阻擋起始時間/阻擋結束時間(Blocked Start Time / Blocked End Time)	顯示阻擋 IP 位址的開始時間和結束時間。
命中次數(Hit Count)	顯示系統帳戶觸發處罰或使用者帳戶鎖定的次數。
選項(Option)	**解除封鎖(Unblock)** – 移除被封鎖的 IP 位址。 **新增至黑名單(Add to Block List)** - 將 IP 位址新增至防禦設定的白/黑名單。

II-2-5-2 IP 信譽(IP Reputation)

此頁面顯示 Vigor 路由器的 IP 信譽狀態，包括流量輸入和輸出。

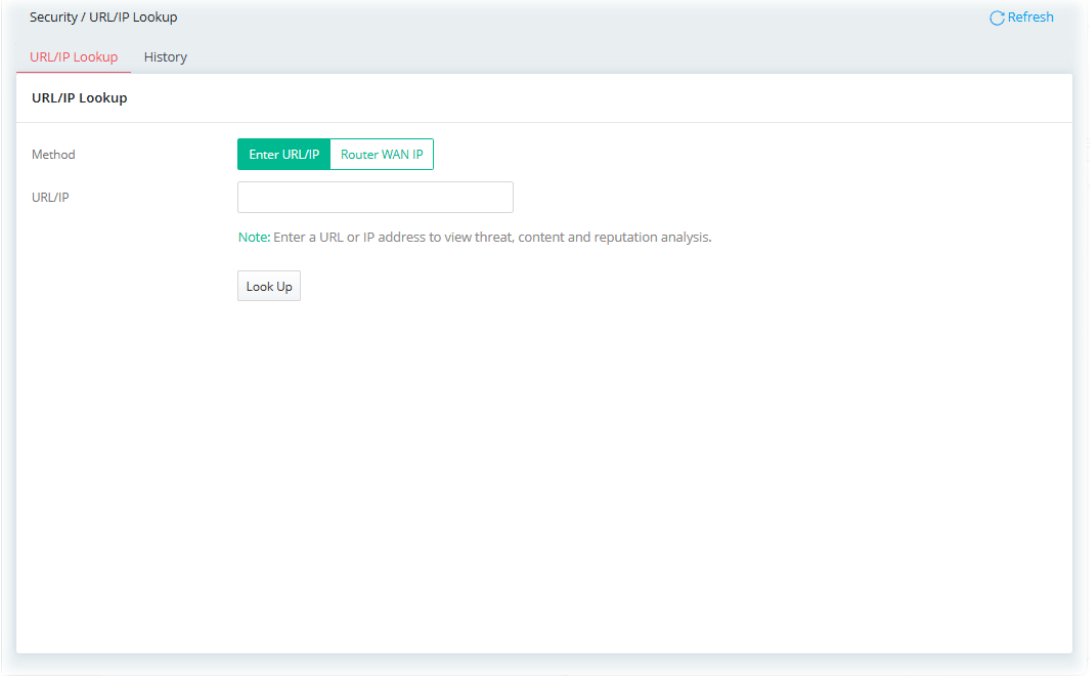


可用設定說明如下：

項目	說明
匯出為 TXT/JSON/CSV 文件(Export as TXT/JSON/CSV)	以 TXT、JSON 或 CSV 檔案格式匯出 IP 信譽設定。
見於(Seen at)	顯示資料封包符合指定規則的時間。.
來源 IP (Source IP(Threat))	顯示威脅來源的 IP 位址。
目的 IP (Destination IP)	顯示威脅所針對的目的 IP 位址。
目的埠號 (Destination Port)	顯示威脅所針對的目的 IP 位址埠號。
信譽(Reputation)	顯示該 IP 位址的得分。
嘗試次數(Attempts)	顯示威脅對目的地點發動攻擊的次數。
威脅類型(Threat Type)	顯示威脅類型。

II-2-6 URL/IP 查詢(URL/IP Lookup)

此頁面可讓您查看指定 IP 或 URL 的各種評分，按**查詢(Look Up)**按鈕即可查看相關資訊。分析完成後，Vigor 系統將提供有關 IP/URL 的相關訊息，包括風險等級、信譽評分、類別等。

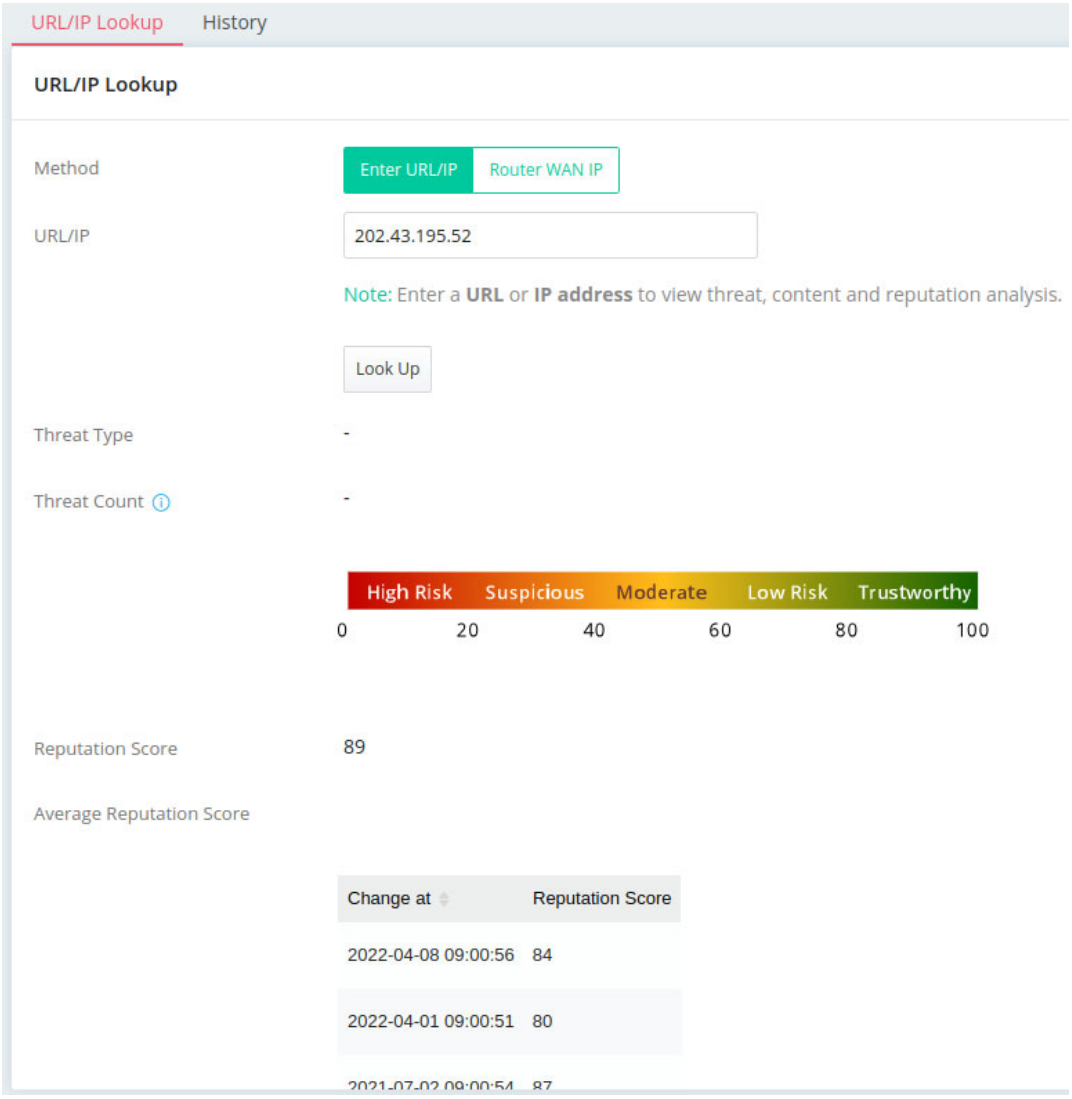


可用設定說明如下：

項目	說明
方式(Method)	**輸入 URL/IP (Enter URL/IP) –** 選擇此方法可使用 URL 或 IP 位址進行搜尋。 ● **URL/IP –** 輸入您要尋找的主題的網址或 IP 位址。 **路由器 WAN IP (Router WAN IP)** – 選擇此方法透過 WAN 介面進行查詢。
查詢(Look Up)	按此顯示與查詢 IP/URL 相關的資訊。 其中，與 IP 位址關聯的相關資訊（見下文）將顯示在頁面上。 ● 威脅類型(Threat Type) ● 威脅計數(Threat Count) ● 信譽評分(Reputation Score) ● 平均信譽評分(Average Reputation Score) ● 組織(Organization) ● 位置(Location) ● 緯度(Latitude) ● 經度(Longitude) 或者，輸入網址名稱。頁面上將顯示與該網址關聯的相關資訊。 ● 信譽評分(Reputation Score) ● 類別(Category) ● 類別信心(Category Confidence)

	• 受歡迎程度(Popularity) • 名稱伺服器(Name Servers) • 註冊名稱(Registrar Name) • 建立日期(Created Date) • 到期日(Expired Date) • 組織(Organization) • 位置(Location)

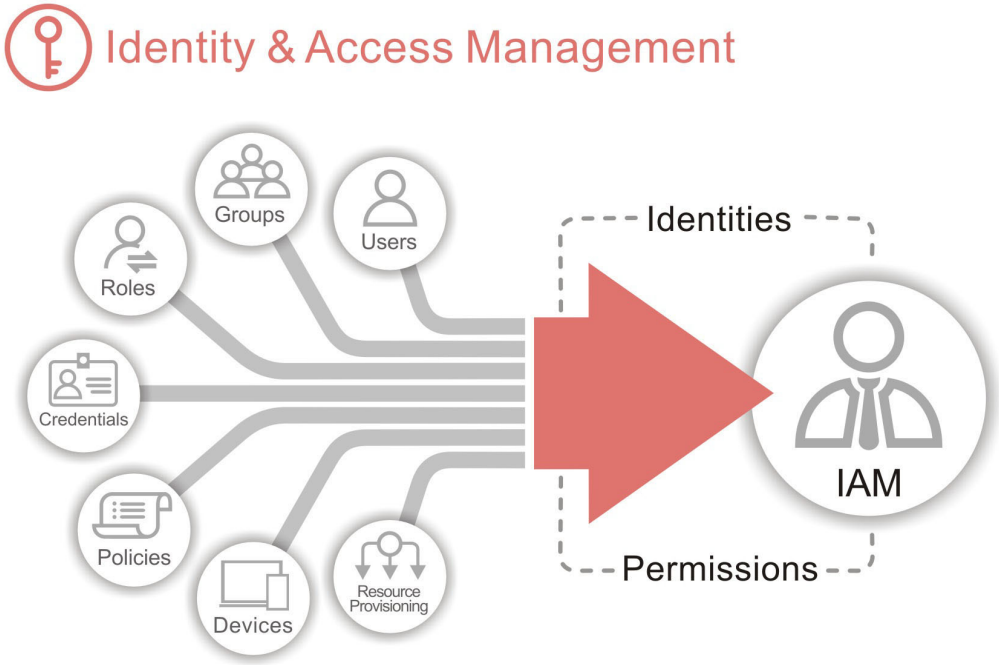
下圖顯示查詢 IP/URL 的範例：



II-3 IAM

身分識別和存取管理 (IAM) 允許網路管理員在使用者層級管理網路存取權限。使用者透過使用者名稱和密碼驗證身分後，即可取得網際網路存取權限，此外，還可以套用可選的防火牆規則和區域網路存取原則。

除了用於識別(透過使用者帳戶/VLAN)之外，IAM 還可以設定存取策略來控制使用者存取網路，並且可以透過群組原則用作防火牆來執行網路管理。

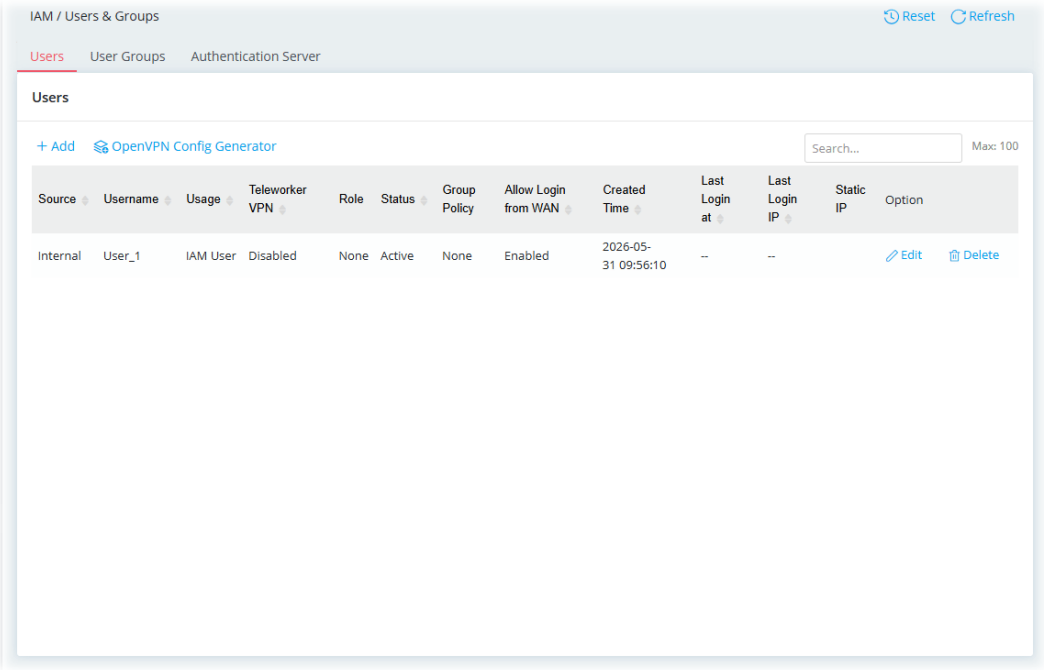


II-3-1 使用者與群組(Users & Groups)

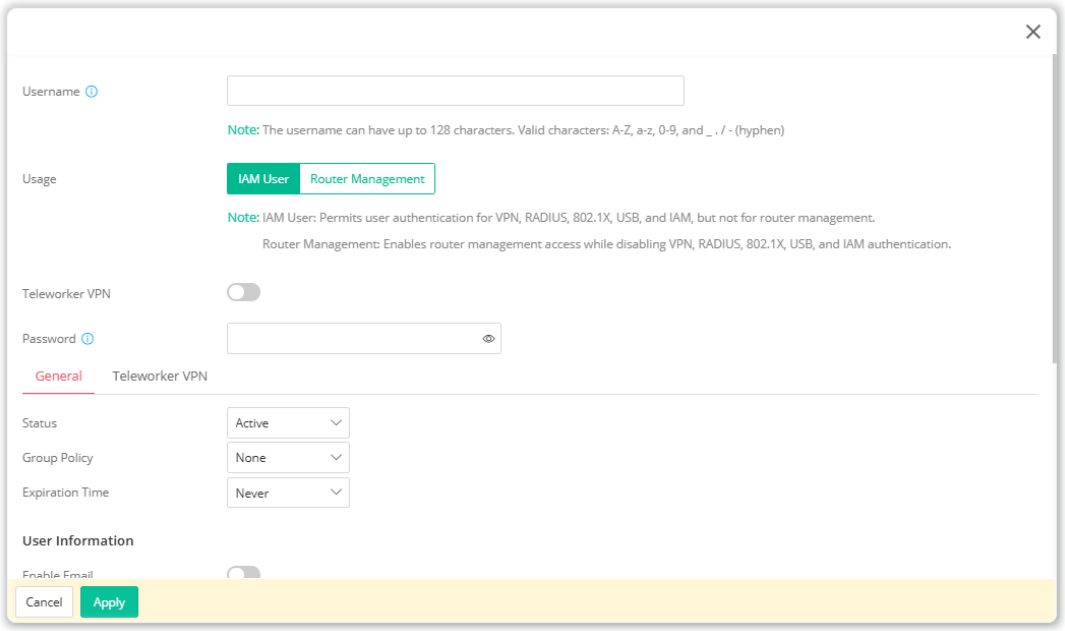
在透過裝置存取網路之前，任何使用者都必須經過 Vigor 系統進行身份驗證，以確保系統安全。本節幫助系統管理員建立不同的使用者和群組設定檔作為驗證依據。

II-3-1-1 使用者(Users)

此部分最多可設定 100 個使用者設定檔。



欲新增設定檔，請按下**+新增(+Add)鏈結**即可開啟如下頁面。



可用設定說明如下：

項目	說明
使用者名稱(Username)	輸入登入名稱（例如，*LAN_User_Group_1*、*WLAN_User_Group_A*、*WLAN_User_Group_B* 等等）針對此使用者設定檔。
用法(Usage)	定義此使用者設定檔的類型。 **IAM 使用者(IAM User)**–此設定檔可用於 VPN、RADIUS、802.1X、USB 和 IAM（身分和存取管理）驗證。 **路由器管理(Router Management)**–此設定檔僅用於路由器管存取，不能用於 VPN、RADIUS、802.1X、USB 和 IAM 驗證。
遠端工作者 VPN (Teleworker VPN)	如果用法選擇了 IAM 使用者，則可用此功能。 切換開關即可啟用或停用遠端工作者 VPN 功能。

密碼(Password)	如果用法選擇了 IAM 使用者，則可用此功能。 針對此使用者設定檔設定密碼 (例如，*lug123*、*wug123*、*wug456* 等等)。 當使用者嘗試存取網際網路時，必須提供有效的使用者名稱和密碼組合進行身份驗證。系統會將符合的使用者名稱和密碼對應的設定檔套用至本次連線數。
密碼/新的密碼/確認新密碼(Password New Password/ Confirm New Password)	如果用法選擇了路由器管理，則可用此功能。 針對此使用者設定檔設定密碼 (例如，*lug123*、*wug123*、*wug456* 等等)。 當使用者嘗試存取網際網路時，必須提供有效的使用者名稱和密碼組合進行身份驗證。系統會將符合的使用者名稱和密碼對應的設定檔套用至本次連線數。
基本(General) **(如果用法選的是 IAM 使用者)**	
狀態(Status)	**使用中(Active)** – 啟用此頁面中的一般設定。 **未啟用(Inactive)** – 停用此頁面上的一般設定。
群組策略(Group Policy)	如果用法選擇了 IAM 使用者，則可用此功能。 選擇要套用到此使用者設定檔的群組策略設定檔。
到期日(Expiration Time)	如果用法選擇了 IAM 使用者，則可用此功能。 設定網路連線僅在特定時間間隔內運作。預設情況下，所有使用者帳戶將自動套用此時間設定。 **永不(Never)** – 網路連線始終保持開啟狀態。 **剩餘時間(Expire in)** – 網路連線建立後，將在指定的分鐘、小時、天或周後過期並終止連線。 **到期時間(Expire at)** – 網路連線建立後，將在以下指定的日期和時間到期並終止連線。 • 日期(Date) • 時間(Time) • 到期日(Expiration Time)
使用者資訊(User Information)	**啟用電子郵件(Enable Email)**– 切換開關以啟用或停用電子郵件設定。 • **電子郵件(Email)**–輸入用於接收 MFA PIN 碼的電子郵件地址。 • **傳送電子郵件通知至新建立的使用者(Send Email Notification to the newly created User)**– 向此使用者帳號發送通知郵件。 **啟用簡訊(Enable SMS)** –切換開關以啟用或停用簡訊設定。 • **簡訊(SMS)** – 輸入接收 MFA PIN 碼的簡訊接收號碼。
MFA 與 Port Knocking (MFA & Port Knocking)	多因驗證 (MFA) 可以提供更安全的網路連線。 **啟用 MFA(Enable MFA)** – 切換開關以啟用/停用 MFA 功能。 • **允許的 MFA 方式(Allowed MFA Method)** – 選擇從 WAN 登入時是否需要 TOTP、簡訊或電子郵件驗證。 **TOTP** – 對於基於時間的一次性密碼 (TOTP) 機制，請確保您的路由器時區設定正確。然後，在您的手機上安裝 Google Authenticator 應用程式。開啟該應用程式掃描此頁面上的 QR 碼(QR Code)。您的手機上將顯示一次性密碼。選擇 TOTP 並按下套用(Apply)，即可彈出如下對話框：

	 在驗證碼(Validation Code)欄位中，輸入一次性密碼，然後按一下驗證(Verify)。 現在設定已完成。在通過使用者名稱和密碼驗證後，您將被要求輸入雙因認證碼。 **簡訊/電子郵件(SMS/Email)** – 密碼將根據您在上方使用者資訊中選擇的方式透過簡訊或電子郵件發送。 • **強制執行 Port Knocking (Enforce Port Knocking)** – 切換開關以啟用/停用 Port Knocking 功能。 **第一個 Knock 埠口(1st Knock Port)** – 請輸入數值（3001~59999）。按下感嘆號（！）以查看更多資訊。 **TOTP 密鑰(TOTP Secret)** – 顯示用於 TOTP 的金鑰。
帳號資訊(Account Info)	顯示使用者帳戶的一般資訊（建立時間、上次登入時間和上次登入 IP）。
	遠端工作者 VPN (Teleworker VPN) **(如果用法選的是 IAM 使用者)**
基本(General)	**閒置逾時(Idle Timeout)** – 如果使用者空閒時間超過設定的逾時時間，則該使用者的網路連線將會中斷。預設情況下，閒置逾時時間為 300 秒。 **VPN 排程(VPN Schedule)** – 選擇**永遠連線(Always On)**（遠距辦公 VPN 始終運作）。或選擇**排程啟用(Scheduled On)**根據排程建立 VPN 連線。 在設定 VPN 排程之前，請在設定>>物件>>排程 (Configuration>>Objects >>Schedule) 中新增所需的時間間隔。 **下載 SmartVPN Client (Download SmartVPN Client)** – 按此下載用於建立 VPN 連線的 DrayTeck SmartVPN 用戶端工具。
允許的 VPN 通訊協定 (Allowed VPN Protocols)	選擇 IPsec、WireGuard、L2TP 或 OpenVPN 作為遠端工作者 VPN 連線的通訊協定。 **IPsec** – 切換開關以啟用 IPsec 協定。 如果啟用，請選擇 IKEv1/v2、EAP 和/或 XAuth 作為 IPsec 協定。 **OpenVPN** – 切換開關以啟用 OpenVPN 協定。 **WireGuard** – 切換開關以啟用 WireGuard 協定。 **L2TP** – 切換開關以啟用 L2TP 協定。
WireGuard 設定 (WireGuard Settings)	如果**允許的 VPN 通訊協定**選擇了 **WireGuard**，則可用此功能。 **產生金鑰模式(Generate Key Mode)** – 選擇自動(Auto)或客製化(Customized)。 **產生金鑰組(Generate Key Pair)** – 按此即可自動產生用戶端虛擬金鑰和用戶端公開金鑰。 **用戶端公開金鑰(Client Public Key)** – 輸入遠端 WireGuard VPN 用戶端提供的字串。

	預先共享金鑰(Pre-Shared Key) – 顯示按下產生預先共享金鑰(PSK)按鈕所產生的虛擬金鑰。 **產生預先共享金鑰(PSK) (Generate PSK)** – 按下產生預先共享金鑰(PSK)按鈕產生預共用金鑰。 **持續維持連線(Persistent Keepalive)** – 預設值為 60 秒。如果對方位於 NAT 或防火牆之後，請使用預設設定。
安全性(Security)	**指定對方 VPN (Specify VPN Peer)** – 切換開關以啟用/停用遠端客戶端的安全機制。 ● **遠端用戶端 IP (Remote Client IP)** – 如果啟用了指定對方 VPN 功能，請輸入遠端對等體的 IP 位址。 ● **預先共享金鑰(Pre-Shared Key)** – 當選擇 IPsec 作為允許的 VPN 協定時，則可用此功能。**指定對方 VPN** 可以限制 IPsec 只能由指定的對方 IP 位址或網域名稱發起，並可指定要使用的虛擬金鑰。 **X509 數位簽章(X.509 Digital Signature)** - 當選擇 IPsec 作為允許的 VPN 協定時，則可用此功能。接受憑證身份驗證。若要使用 X.509 數位簽章，請選擇一種身份驗證方法，並為每種方法輸入所需資訊。 ● **停用(Disabled)** –選擇此項目可停用 VPN 連線的憑證應用。 ● **接受主體替代名稱(Accept Subject Alternative Name)** – 以下三種對方 ID 格式均可接受，包括 IP 位址、網域名稱和電子郵件。 ● **從現有憑證中選擇(Select from Existing Certificates)** –選擇已預先取得並儲存在設定>>憑證>>本機憑證 (Configuration>>Certificates>> Local Certificate)中的對等憑證。 ● **接受主體名稱(Accept Subject Name)** – 請輸入完整的憑證主體名稱。 ● **接受任一(Accept Any)** – 任何由設定>>憑證>>受信任的 CA(Configuration>>Certificates>> Trusted CA)中受信任的 CA 簽署的憑證都將被視為有效。
本機 IP 分派(Local IP Assignment)	**分派 IP 藉由(Assign IP By) –** 選擇 **LAN DHCP** 或者**固定 IP 位址**。如果啟用了 WireGuard VPN 通訊協定，則此選項將無法使用。 **分派 IP 來自(Assign IP from)** – 選擇一個 LAN 介面進行 IP 分配。 ● **固定 IP(Static IP)** –指定 IPv4 位址。 **DNS 分派方式(Assign DNS By)** – 選擇 **LAN DHCP**（DNS IP 位址將由 Vigor 路由器自動分配）或是**固定 DNS**，如果選擇固定 DNS，請設定主要 DNS 和次要 DNS。 ● **主要 DNS (Primary DNS)** – 輸入主要 DNS 伺服器的 IPv4 位址。 ● **次要 DNS (Secondary DNS)** – 如果需要，請輸入另一個 DNS 伺服器的 IPv4 位址。 若選擇**固定 IP(Static IP)**， ● **固定 IP(Static IP)** –指定 IPv4 位址。
用戶端 Config 設定產生器(Client Config Generator)	如果啟用了 WireGuard VPN 通訊協定，則此選項將無法使用。 **VPN 伺服器(VPN Server) –** 請輸入此路由器的 WAN IP 位址或網域名稱。 **設定 VPN 做為預設閘道(Set VPN as Default Gateway) –** 切換開關即可啟用/停用此功能。 ● **啟用(Enable)** - Vigor 路由器將被視為 WireGuard VPN 用戶端的預設閘道。 WireGuard VPN 用戶端會將所有流量透過 WireGuard VPN 通道重新導向至 Vigor 路由器。 ● **停用(Disable)** - 停用此功能。 ● **取代預設路由(Replace the Default Route)** –切換開關以啟用/停用此功能。按下套用(Apply)用戶端的預設路由將被 VPN 路由取代。 **設定(config) –** 此欄位中的預設文字會自動顯示，並會根據 QR 碼的不同

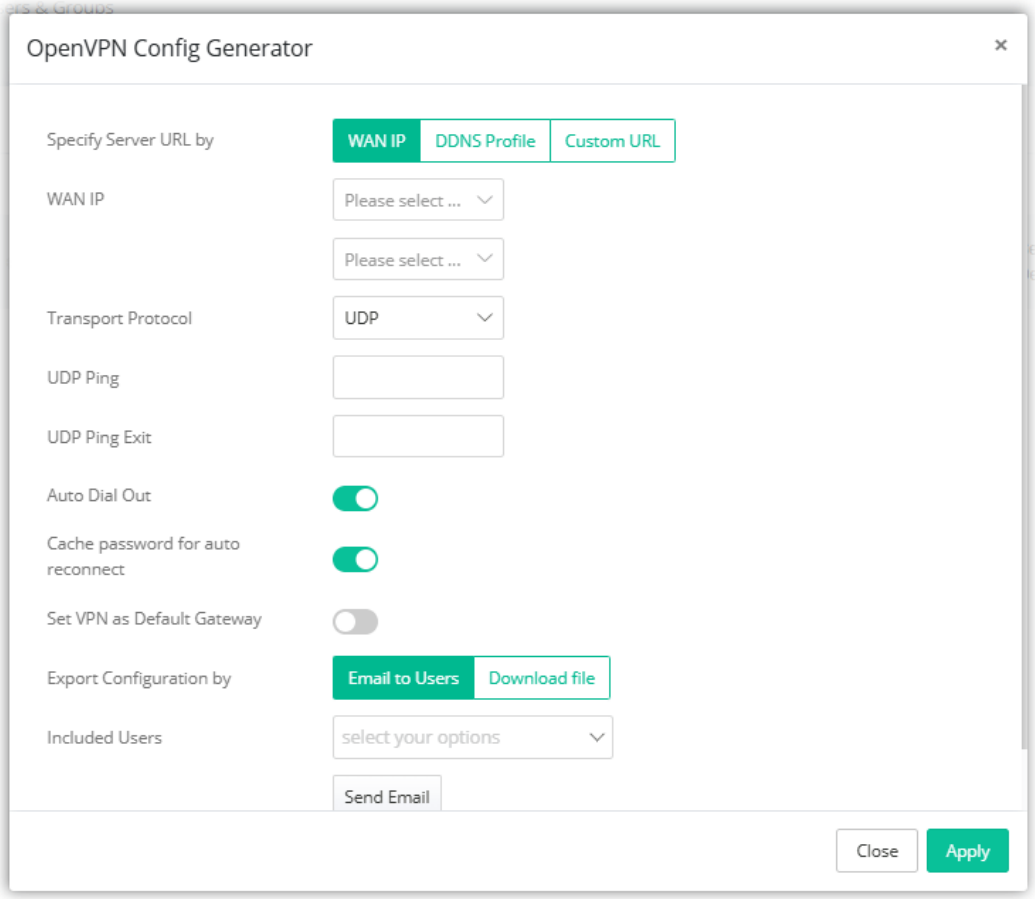
	而變化。如有需要，請修改文字。 **下載設定(Download Configuration) -** 按此鈕將此頁面上的設定下載為文件，該文件可以匯入到 VPN 用戶端中以建立 WireGuard VPN 連線。
基本(General) (如果用法選的是路由器管理者)	
角色(Role)	如果用法選擇了路由器管理，則可用此功能。 ● **管理者(Administrator)** ● **訪客(Guest)** ● **使用者(Users)**
狀態(Status)	**使用中(Active)** – 啟用此頁面中的一般設定。 **未啟用(Inactive)** – 停用此頁面上的一般設定。
允許透過 WAN 登入 (Allow Login from WAN)	如果用法選擇了路由器管理，則可用此功能。 若啟用，使用者可以從 WAN 端登入。
使用者資訊(User Information)	**啟用電子郵件(Enable Email)**– 切換開關以啟用或停用電子郵件設定。 ● **電子郵件(Email)**–輸入用於接收 MFA PIN 碼的電子郵件地址。 ● **傳送電子郵件通知至新建立的使用者(Send Email Notification to the newly created User)**– 向此使用者帳號發送通知郵件。 **啟用簡訊(Enable SMS)** –切換開關以啟用或停用簡訊設定。 ● **簡訊(SMS)** - 輸入接收 MFA PIN 碼的簡訊接收號碼。
MFA 與 Port Knocking (MFA & Port Knocking)	多因驗證（MFA）可以提供更安全的網路連線。 **啟用 MFA(Enable MFA)** – 切換開關以啟用/停用 MFA 功能。 ● **允許的 MFA 方式(Allowed MFA Method)** - 選擇從 WAN 登入時是否需要 TOTP、簡訊或電子郵件驗證。 **TOTP** – 對於基於時間的一次性密碼 (TOTP) 機制，請確保您的路由器時區設定正確。然後，在您的手機上安裝 Google Authenticator 應用程式。開啟該應用程式掃描此頁面上的 QR 碼(QR Code)。您的手機上將顯示一次性密碼。選擇 TOTP 並按下套用(Apply)，即可彈出如下對話框：  在驗證碼(Validation Code)欄位中，輸入一次性密碼，然後按一下驗證(Verify)。 現在設定已完成。在通過使用者名稱和密碼驗證後，您將被要求輸入雙因認證碼。 **簡訊/電子郵件(SMS/Email)** – 密碼將根據您在上方使用者資訊中選擇的方式透過簡訊或電子郵件發送。

	• **強制執行 Port Knocking (Enforce Port Knocking)** – 切換開關以啟用/停用 Port Knocking 功能。 **第一個 Knock 埠口(1st Knock Port)** – 請輸入數值（3001~59999）。按下感嘆號(!)以查看更多資訊。 **TOTP 密鑰(TOTP Secret)** – 顯示用於 TOTP 的金鑰。
帳號資訊(Account Info)	顯示使用者帳戶的一般資訊（建立時間、上次登入時間和上次登入 IP）。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

若要新增新的 OpenVPN 設定文件，請按下 **OpenVPN 設定產生器(OpenVPN Config Generator)**。

在本頁中，您可以建立遠端 OpenVPN 用戶端連接到路由器所需的設定，然後直接下載或透過電子郵件傳送給使用者。



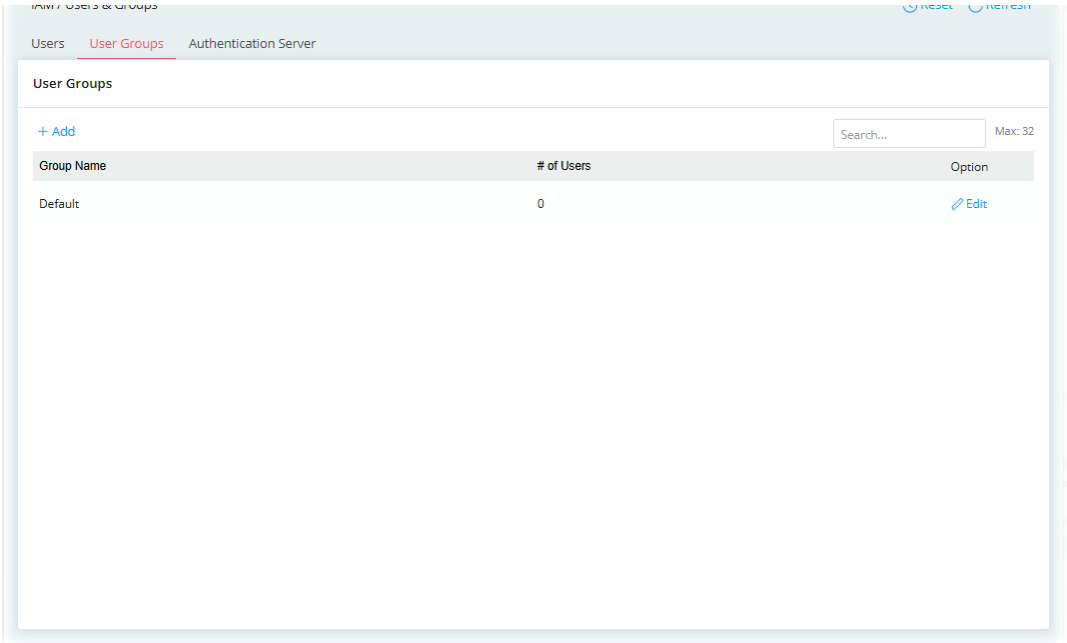
可用設定說明如下：

項目	說明
指定伺服器 URL 方式 (Specify Server URL by)	OpenVPN 用戶端將使用 IP 位址或網域名稱連接到路由器。 **WAN IP** – OpenVPN 設定檔將使用數字型式的 IP 位址作為伺服器位址。 • **WAN IP** – 選擇 WAN 介面。 **DDNS 設定檔(DDNS Profile)** – OpenVPN 設定檔將使用 DDNS 設定檔中的網域名稱。 • **DDNS 設定檔(DDNS Profile)** – 選擇一個 DDNS 設定檔。

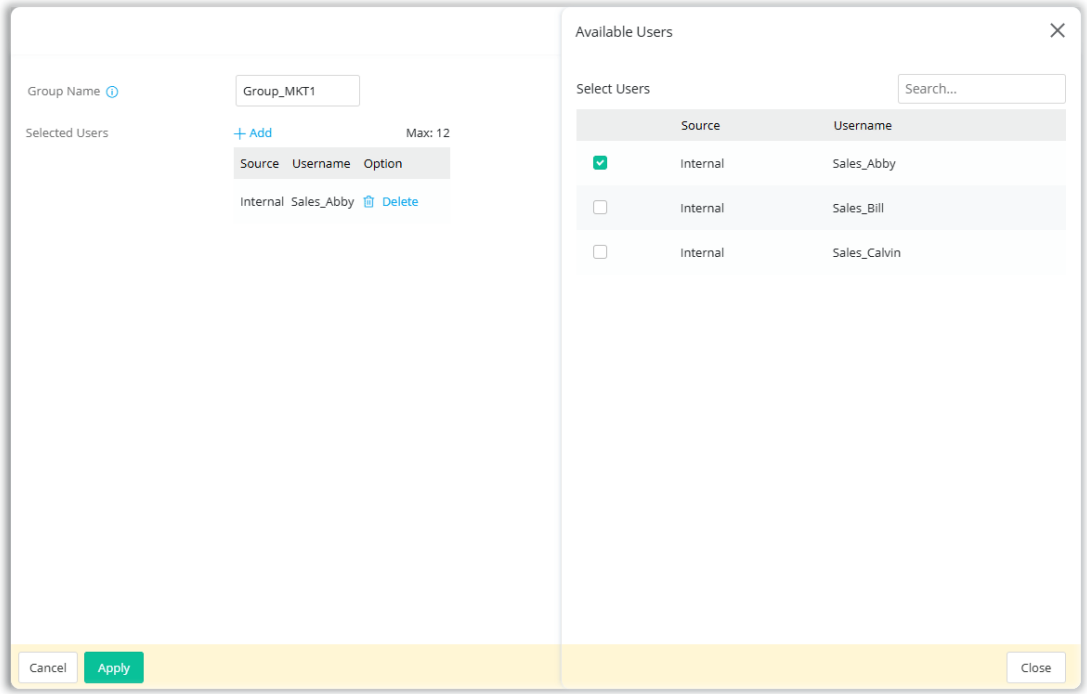
	客製 URL (Custom URL) – OpenVPN 設定檔將使用使用者定義的伺服器 IP 或網域名稱。 ● **客製 URL (Custom URL)**– 指定使用者設定中的 URL。
傳輸通訊協定(Transport Protocol)	**TCP/UDP** – 選擇 UDP 或 TCP 作為 OpenVPN 用戶端連線到路由器時所使用的協定。
UDP Ping	如果在設定的秒數內沒有發送任何資料封包，則透過 UDP 控制通道 ping 遠端設備。
UDP Ping 離開(UDP Ping Exit)	如果未收到來自遠端裝置的 ping 或其他封包，則讓 OpenVPN 在此處設定的秒數後退出。
自動撥出(Auto Dial Out)	切換開關即可啟用/停用此功能。 **啟用(Enable)** – 遠端用戶端可以自動撥號連接到這台 Vigor 路由器，以建立 OpenVPN 通道。 **停用(Disable)** – 停用此功能。
自動重新連線之暫存密碼 (Cache password for auto reconnect)	切換開關即可啟用/停用此功能。 **啟用(Enable)** – OpenVPN 將每小時自動重新連線一次。重新連線時需要輸入密碼。如果啟用此功能，Vigor 系統將保存 OpenVPN 連線的密碼，並在每次重新連線時使用。 **停用(Disable)** –停用此功能。
設定 VPN 做為預設閘道 (Set VPN as Default Gateway)	切換開關即可啟用/停用此功能。 **啟用(Enable)** – Vigor 路由器將被視為 OpenVPN 用戶端的預設閘道。OpenVPN 用戶端會將所有流量透過 OpenVPN 通道重新導向至 Vigor 路由器。 **停用(Disable)** – 停用此功能。
匯出設定檔方式(Export Configuration by)	**郵件至使用者(Email to Users)** – 若選擇此功能，下方將顯示包含使用者欄位。OpenVPN 設定檔將傳送給包含使用者清單中的使用者。 ● **包含使用者(Included Users)** – 選擇將從 Vigor 路由器接收設定的遠端工作者(辦公用戶)。 ● **傳送電子郵件(Send Email)** – 按此即可將此頁面上的設定以檔案的形式透過電子郵件傳送，該檔案可以匯入到 VPN 用戶端中，以便與遠端辦公使用者建立 OpenVPN 連線。 **下載 zip 檔案(Download zip file)** – OpenVPN 的設定檔將儲存在資料庫中。若選擇此項，下方將顯示下載設定按鈕。 ● **下載設定(Download Configuration)** – 按下此按鈕，將此頁面上的設定下載為檔案，該檔案可以匯入到 VPN 用戶端以建立 OpenVPN 連線。
關閉(Close)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

II-3-1-2 使用者群組(User Groups)

此頁面允許您將多個使用者設定檔放入群組中。



欲新增設定檔，請按下**+新增(+Add)鏈結**即可開啟如下頁面。

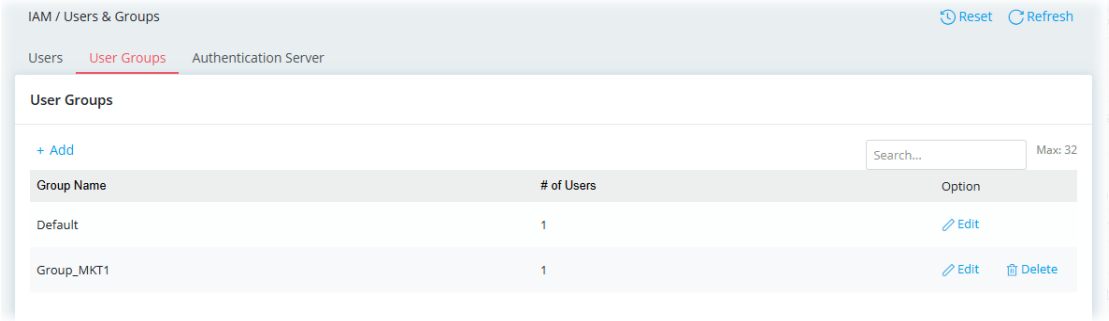


可用設定說明如下：

項目	說明
群組名稱(Group Name)	輸入辨識用的名稱。
選定的使用者(Selected Users)	**+新增(+Add)** – 按此選擇要分組到目前群組設定檔下的使用者設定檔。

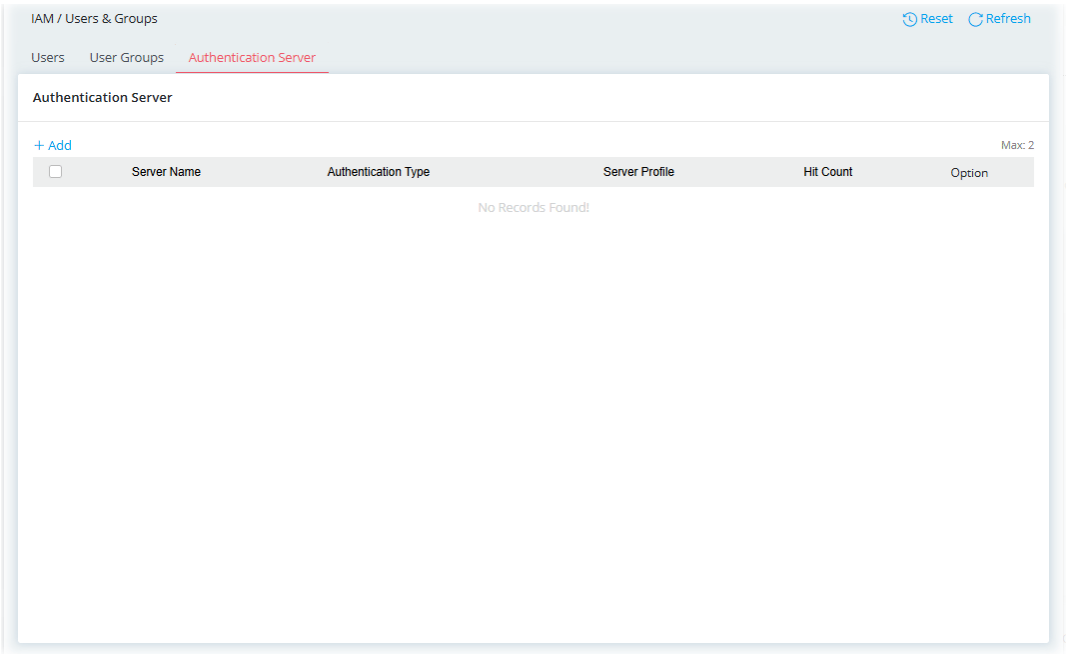
可用使用者(Available Users)	按下**+新增**後可出現此選項。 **選定的使用者(Selected Users)** – 從可用的使用者資設定檔中選擇成員。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

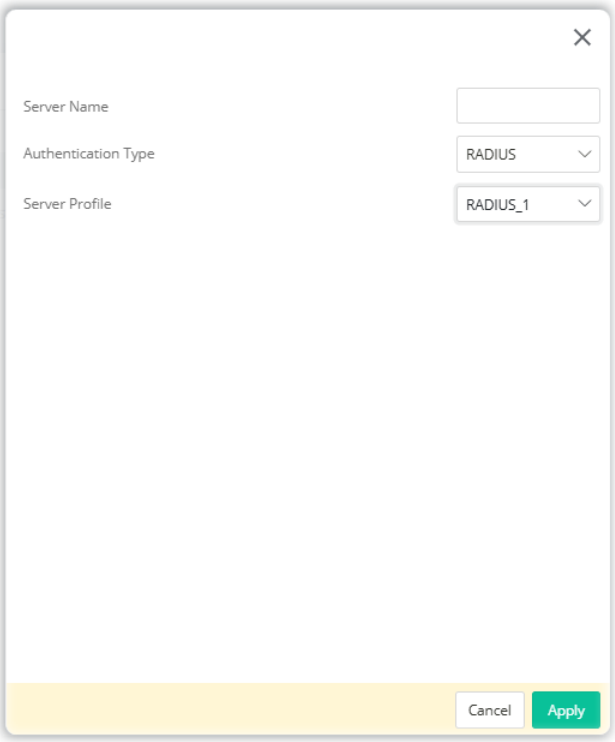


II-3-1-3 驗證伺服器(Authentication Server)

Vigor 路由器可以使用內建（無）或外接（Radius 或 TACACS+）服務伺服器對使用者進行身份驗證。



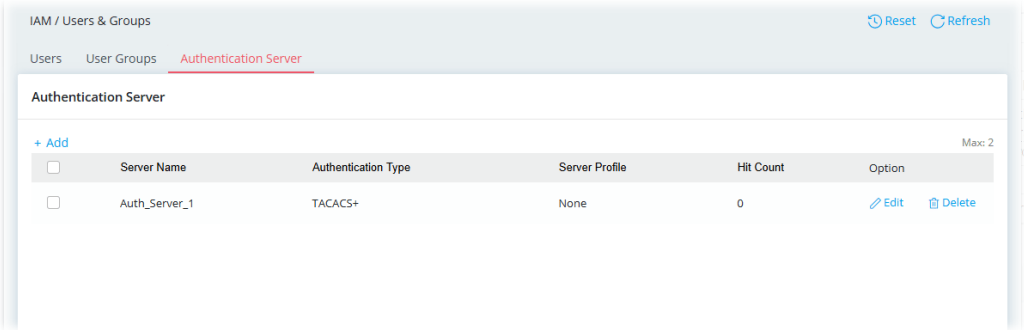
欲建立新的驗證伺服器檔案，請按**+新增(+Add)** 。



可用設定說明如下：

項目	說明
伺服器名稱(Server Name)	輸入作為辨識用的名稱。
驗證類型 (Authentication Type)	選擇驗證的類型(RADIUS 或是 TACACS+)。
伺服器設定檔(Server Profile)	如果選擇 RADIUS 作為驗證類型，則此區域將顯示可用的 RADIUS 伺服器設定檔（在設定>>RADIUS/TACACS+ (Configuration>>RADIUS/TACACS+)中建立）。請選擇所需的設定檔。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

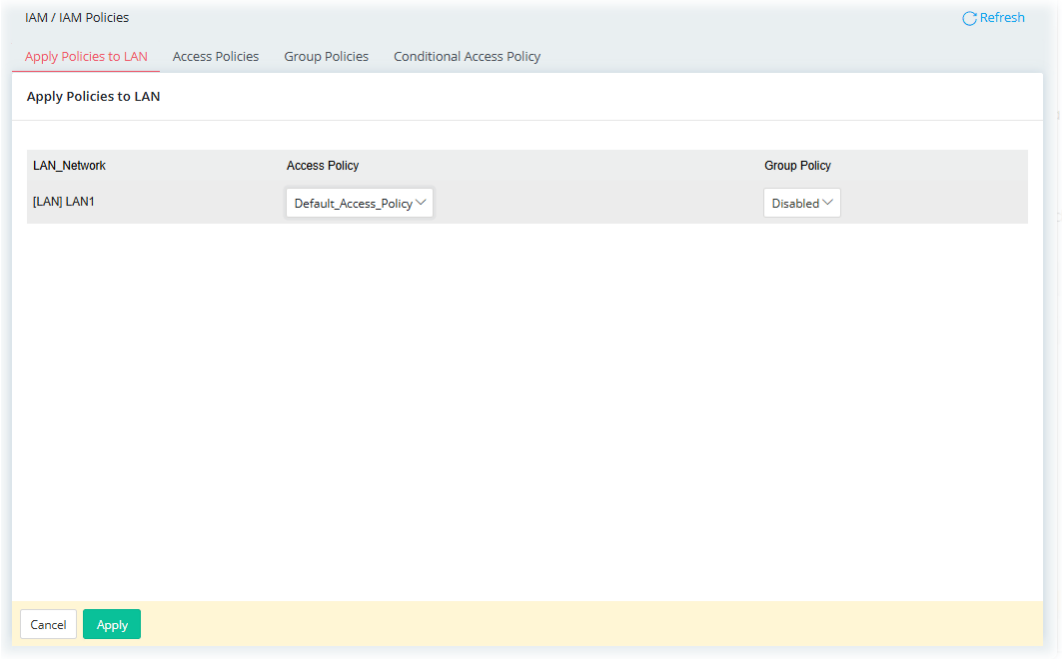


II-3-2 IAM 策略(IAM Policies)

IAM 策略包含存取策略、群組策略和條件式存取策略。

II-3-2-1 套用策略至 LAN (Apply Policies to LAN)

此頁面用於選擇將套用於 LAN 設定檔的存取策略和群組策略。



可用設定說明如下：

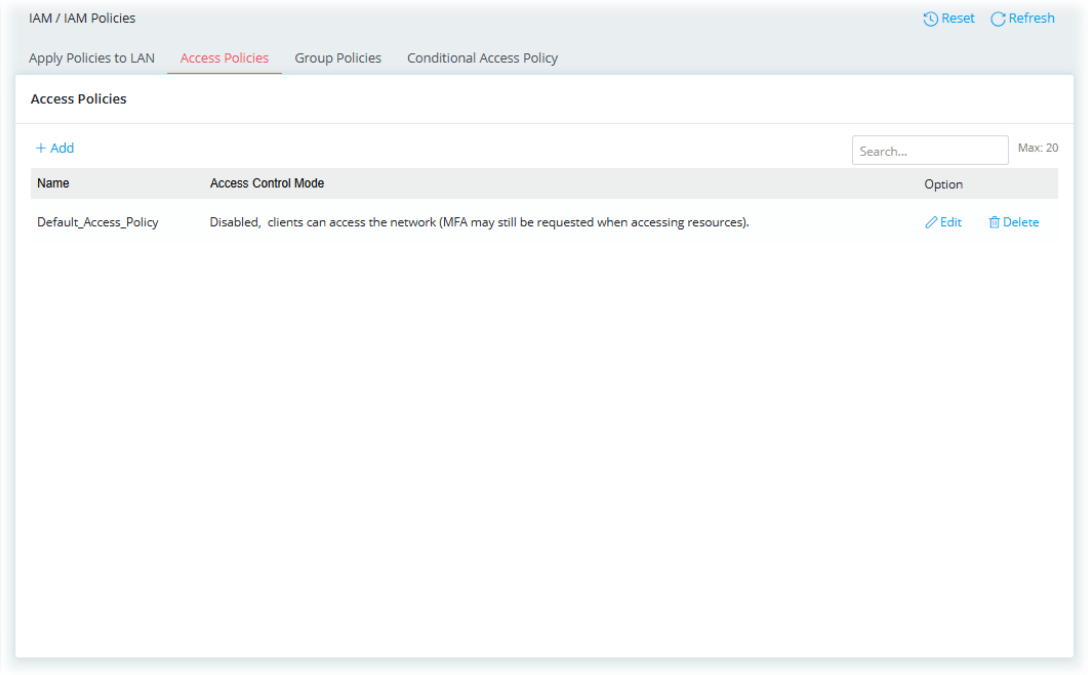
項目	說明
LAN 網路(LAN Network)	顯示將套用到介面的 IAM 策略。
存取策略(Access Policy)	請為此介面選擇存取策略。或選擇 “停用” 忽略此設定。
群組策略(Group Policy)	為此介面選擇群組策略。或選擇 “已停用” 忽略此設定。
取消(Cancel)	捨棄目前設定。
套用(Apply)	儲存目前設定。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

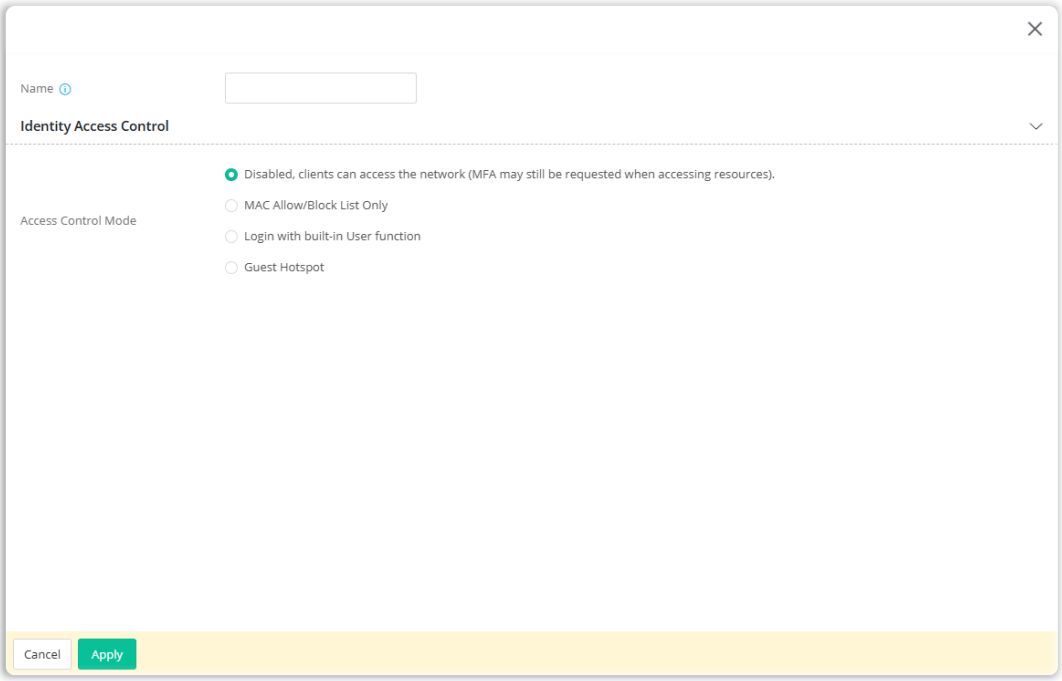
II-3-2-2 存取策略(Access Policies)

存取策略可以應用於 LAN 介面以確定使用者/用戶端如何透過身份驗證存取網際網路。

此頁面用於定義 IAM 應用的不同存取策略。



欲新增新的設定檔，按下**+新增(+Add)** 。



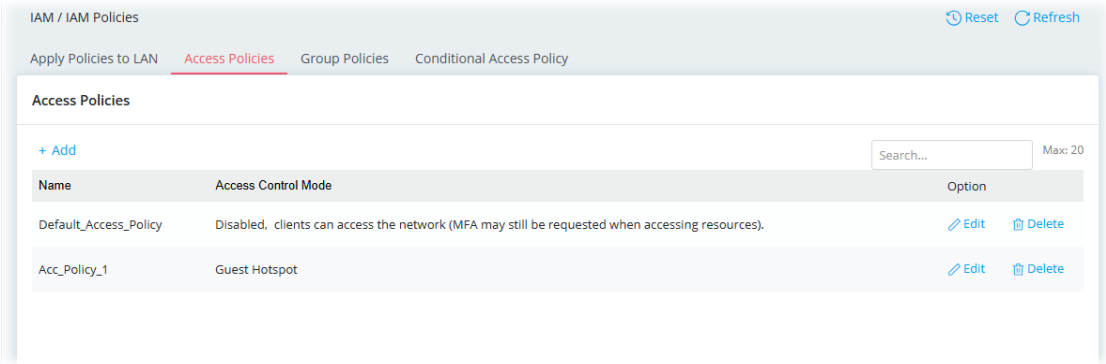
可用設定說明如下：

項目	說明
名稱(Name)	輸入辨識用的名稱。
	身分識別存取控制(Identity Access Control)

存取控制模式(Access Control Mode)	**已停用(Disabled)** – 所有用戶端/使用者帳戶均可存取網路。 **限用 MAC 黑/白名單(MAC Allow/Block List Only)** – 透過 MAC 位址過濾設定檔允許或拒絕用戶端/使用者帳戶存取網路。 **使用內建使用者功能登入(Login with built-in User function)** – 用戶端在存取網路之前需要進行身份驗證。 **訪客熱點(Guest Hotspot)** - 根據所選熱點設定檔，允許或拒絕客戶端/使用者帳戶存取網路。
如果**存取控制模式**選擇了**限用 MAC 黑/白名單(MAC Allow/Block List Only)**	
MAC 位址過濾器(MAC Address Filter)	
設定 MAC 位址過濾器方式(Set up MAC Address Filter by)	**自設定檔中選取(Selecting from Profile)** – 使用預先定義的 MAC 位址過濾設定檔作為過濾基礎。 • **MAC 過濾設定檔(MAC Filtering Profile)** - 選擇其中一個 MAC 位址過濾設定檔（安全性>>MAC 位址過濾設定檔）作為過濾基礎。 **手動(Manually)** – 定義 MAC 位址並將其分為白名單和黑名單。 • **MAC 位址過濾器模式(MAC Address Filter Mode)** – 選擇白名單(允許客戶端存取)或黑名單(拒絕客戶端存取)。然後，將客戶端的 MAC 位址分別輸入到 MAC 位址過濾表中。 • **MAC 位址過濾器表格(MAC Address Filter Table)** – 點擊**+新增(+Add)**輸入客戶端的 MAC 位址。
如果**存取控制模式**選擇了**限用使用內建使用者功能登入(Login with built-in User function)**	
驗證模式(Authentication Mode)	**單一因素(Single-Factor)** - 僅需進行身份認證。 **多因素(Multi-Factor)** - 多因素身份驗證增加了一層額外的安全保障，確保只有應用指定群組原則的使用者或 VLAN 中的使用者或裝置才能存取指定的資源。
MAC 位址過濾器(MAC Address Filter)	
設定 MAC 位址過濾器方式(Set up MAC Address Filter by)	**自設定檔中選取(Selecting from Profile)** – 使用預先定義的 MAC 位址過濾設定檔作為過濾基礎。 • **MAC 過濾設定檔(MAC Filtering Profile)** - 選擇其中一個 MAC 位址過濾設定檔（安全性>>MAC 位址過濾設定檔）作為過濾基礎。 **手動(Manually)** – 定義 MAC 位址並將其分為白名單和黑名單。 • **MAC 位址過濾器模式(MAC Address Filter Mode)** – 選擇白名單(允許客戶端存取)或黑名單(拒絕客戶端存取)。然後，將客戶端的 MAC 位址分別輸入到 MAC 位址過濾表中。 • **MAC 位址過濾器表格(MAC Address Filter Table)** – 點擊**+新增(+Add)**輸入客戶端的 MAC 位址。
允許使用者清單(Allowed User List)	
使用者(User)	設定白名單。使用者可以傳送和接收符合白名單設定的流量。 **所有使用者(All Users)** – 所有使用者用戶帳號都將被列入白名單。 **選定的使用者(Selected Users)** – 白名單只考慮已選取的使用者帳號。 **無(None)** - 不套用任何使用者帳戶。
使用者群組(User Groups)	設定白名單。允許群組傳送和接收滿足白名單設定的流量。 **所有群組(All Groups)** – 所有使用者群組都將納入白名單。 **選定的群組(Selected Groups)** – 白名單只考慮已選定的使用者群組。 **無(None)** – 不套用任何使用者群組。
登入連線數生存期(Login Session Lifetime)	
登入連線數生存期(Login Session Lifetime)	控制使用者/客戶端的連線數時間。連線數結束後，使用者/用戶端必須重新

	登入才能存取網路。 請具體說明天數、小時數和分鐘數。
如果**存取控制模式**選擇了**訪客熱點(Guest Hotspot)**	
熱點設定檔(Hotspot Profile)	選擇一個熱點設定檔。
登入連線數生存期(Login Session Lifetime)	
登入連線數生存期(Login Session Lifetime)	控制使用者/客戶端的連線數時間。連線數結束後，使用者/用戶端必須重新登入才能存取網路。 請具體說明天數、小時數和分鐘數。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

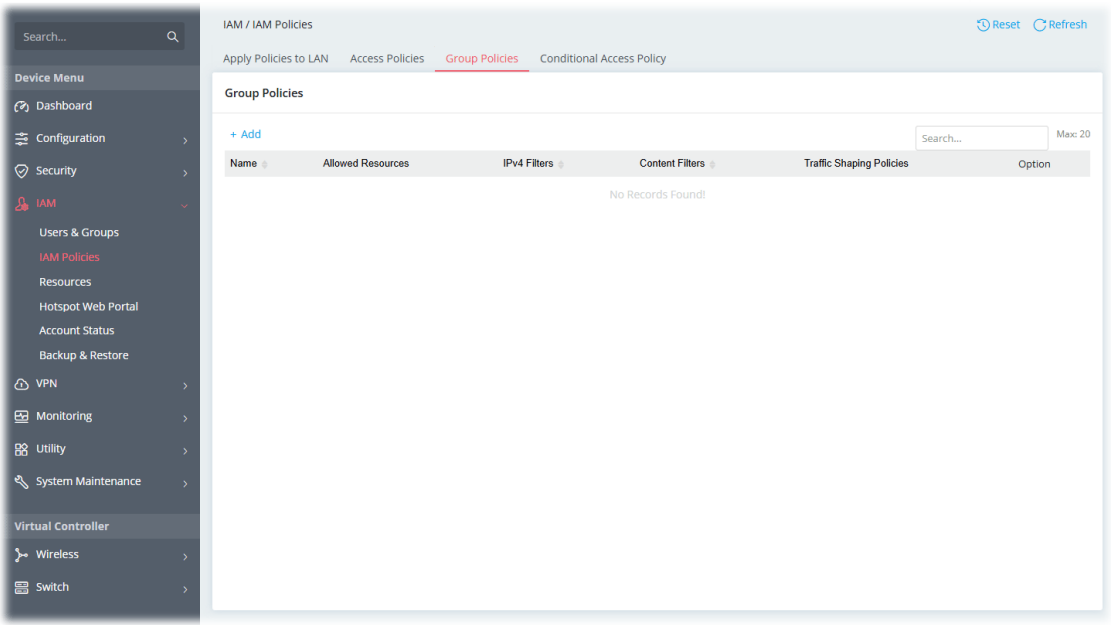
完成設定之後，按下套用(Apply)按鈕儲存相關設定。



II-3-2-3 群組策略(Group Policies)

傳統防火牆通常提供一種封鎖阻擋機制，該機制主要基於 IP 的規則來阻止指定連接埠上的流量。為了更安全地管理存取權限，群組策略提供了一種更好的方法，幫助管理員為特定使用者設定權限，基於角色行為定義限制和設定，以授予相應的限制，例如時間和日期限制、資源限制、防火牆策略和流量形成策略。

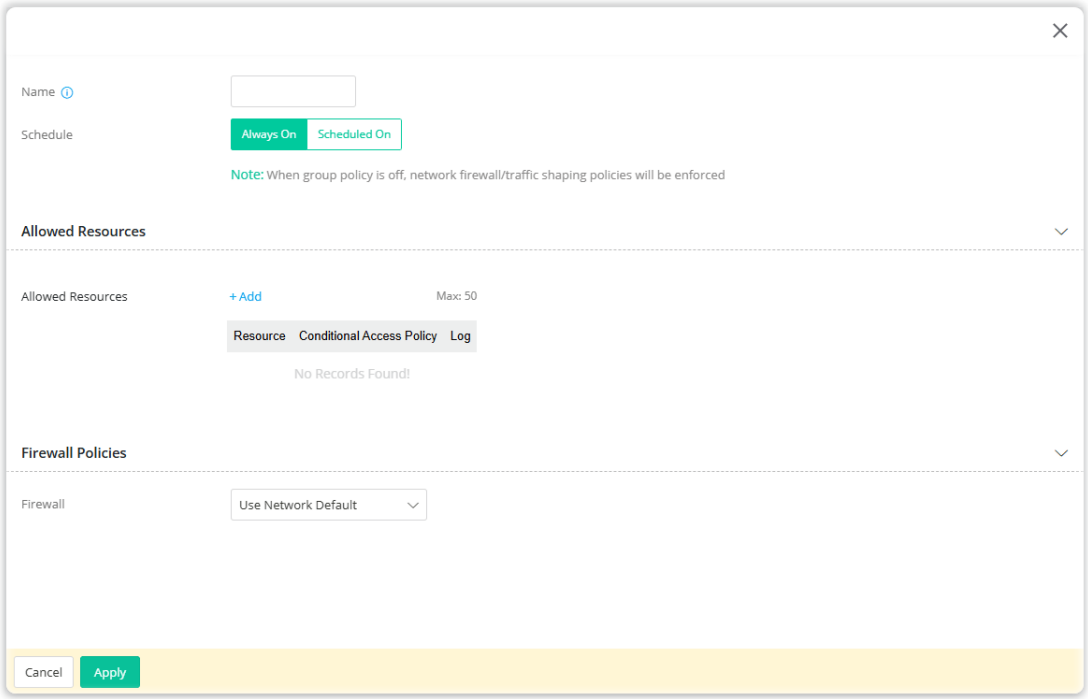
此頁面用於設定 IAM 應用程式的群組原則。



注意:

一旦將群組策略套用至使用者帳戶/VLAN 設定文件，即使已設定防火牆過濾器，群組策略也會覆寫防火牆過濾器中設定的規則。

欲新增群組策略設定檔，請按一下**+新增(+Add)**。



可用設定說明如下：

項目	說明
名稱(Name)	輸入辨識用的名稱。
排程(Schedule)	**永遠連線(Always On)** – 如果啟用，群組策略將始終有效。 **排程啟用(Scheduled On)** - 群組策略是否有效依照選定的排程檔案而定。
允許資源(Allowed Resources)	
允許資源(Allowed Resources)	選擇資源設定檔並將其套用至此策略設定檔。 **+新增(+Add)** – 按此新增新的資源設定檔。 **資源(Resource)** – 使用下拉式選單選擇 IP 或 MAC 資源設定檔。 **條件式存取策略(Conditional Access Policy)** – 使用下拉式選單選擇存取條件設定檔。 **日誌(Log)** – 選擇「放行」、「封鎖」或「兩者皆行」。相應的記錄（與通過或阻止資料封包相關的記錄）將儲存為日誌。 **選項(刪除)(Option (Delete))** – 按此刪除該條目。

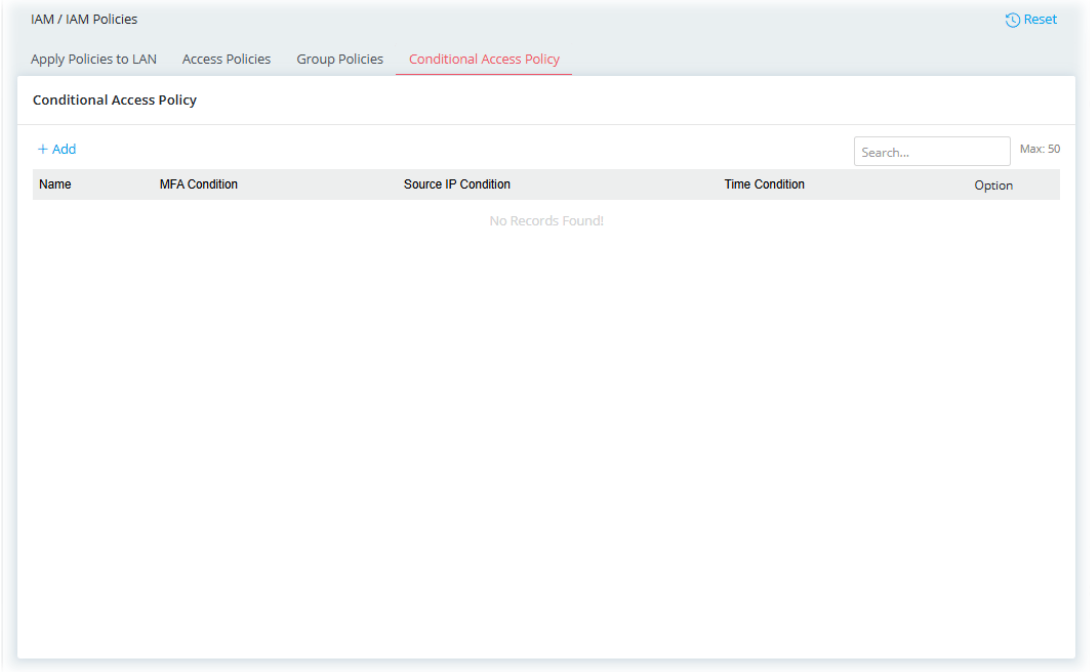
防火牆策略(Firewall Policies)	
防火牆(Firewall)	**使用網路預設值(Use Network Default)** – 選擇此項目可使用預設群組防火牆篩選器設定。 **客製化群組防火牆過濾器(Customize Group firewall filters)** – 選擇此項目可自訂群組防火牆篩選器設定。防火牆策略將應用於上面定義的允許資源。
如果**防火牆**選擇了**客製化群組防火牆過濾器(Customize Group firewall filters)**	
輸出流量 IPv4 過濾器 (Outbound IPv4 Filters)	**+新增(+Add)** – 點選新增新的 IPv4 過濾設定檔（最多 10 個），用於對外流量。 **名稱(Name)** – 設定用於標識 IP 過濾設定檔的名稱。設定檔名稱的最大長度為 15 個字元。 **目的 IP 起始(Destination IP Start)** – 輸入起始 IP 位址。 **目的 IP 結束(Destination IP End)** – 輸入一個 IP 位址作為結束 IP 位址。如果此設定檔僅過濾一個固定 IP 位址，則輸入與「目標 IP 起始位址」相同的 IP 位址。 **通訊協定(Protocol)** – 指定此過濾規則將套用於哪些協定。 **起始目的埠號(Dest Port Start)** – 如果協定是 TCP 或 UDP，請指定目的連接埠範圍（起始連接埠）。 **結束目的埠號(Dest Port End)** – 如果協定是 TCP 或 UDP，請指定目的連接埠範圍（結束點）。 **動作(Action)** – 選擇「允許」以允許存取該 IP 位址；選擇「封鎖」以禁止存取該 IP 位址。 **選項(刪除)(Option(Delete))** - 刪除所選條目。
內容過濾器(Content Filters)	系統也會使用選定的內容過濾器設定檔檢查傳出的連線數。 **+新增(+Add)** – 新增新的內容篩選設定檔（最多 10 個）。 **設定檔名稱(Profile Name)** – 設定一個用於標識內容過濾器設定檔的名稱。設定檔名稱的最大長度為 15 個字元。 **排程啟用(Scheduled On)** - 此過濾器設定檔將根據此處指定的時間排程生效。 **目的(Destination)** – 選擇要包含在過濾器中的特定 WCF 和/或 APPE 和/或 UCF（關鍵字物件）設定檔。 **動作(Action)** – 選擇放行(Pass)以允許存取目標位置；選擇封鎖(Block)以禁止存取目標位置。 **啟用關鍵字例外(Enable Keyword Exception)** – 切換開關以啟用/停用此功能。 **關鍵字例外(Keyword Exceptions)** - 顯示選定的關鍵字物件。 系統也會使用選定的關鍵字設定檔檢查連線數。如果連線數符合關鍵字篩選條件，系統將執行相反的操作。 **選項(刪除)(Option(Delete))** - 刪除所選條目。
IP 過濾器預設動作(IP Filters Default Action）	任何不符合對外流量 IPv4 過濾器和內容過濾器中設定的規則的封包都將按照預設操作進行處理。 • **放行(Pass)** - 允許存取該 IP 位址。 • **封鎖(Block)** - 禁止存取該 IP 位址。
啟用內容過濾器預設規則 (Enable Content Filter Default Rule)	如果啟用， **內容過濾器預設動作(Content Filters Default Action)** - 任何不符合上述防火牆過濾規則但符合內容目標規則的連線數將依照預設動作處理。 • 放行(Pass) - 允許符合內容目標規則的連線數通過。符合以下內容目標規則的對外流量將被允許通過；否則，將被阻止。

	• 封鎖(Block) - 禁止符合內容目的規則的連線數通過。符合以下內容目的規則的對外流量將被阻止。否則，流量將被允許通過。 **內容目的(Content Destination)** – 選擇要包含在過濾器中的 WCF、APPE 和/或 UCF（關鍵字物件）設定檔。它將作為一條附加的內容過濾規則，用於確定資料封包/連線數是被允許放行還是被阻止通過。
啟用 Syslog (Enable Syslog)	可以依照 Syslog 設定來記錄過濾結果。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

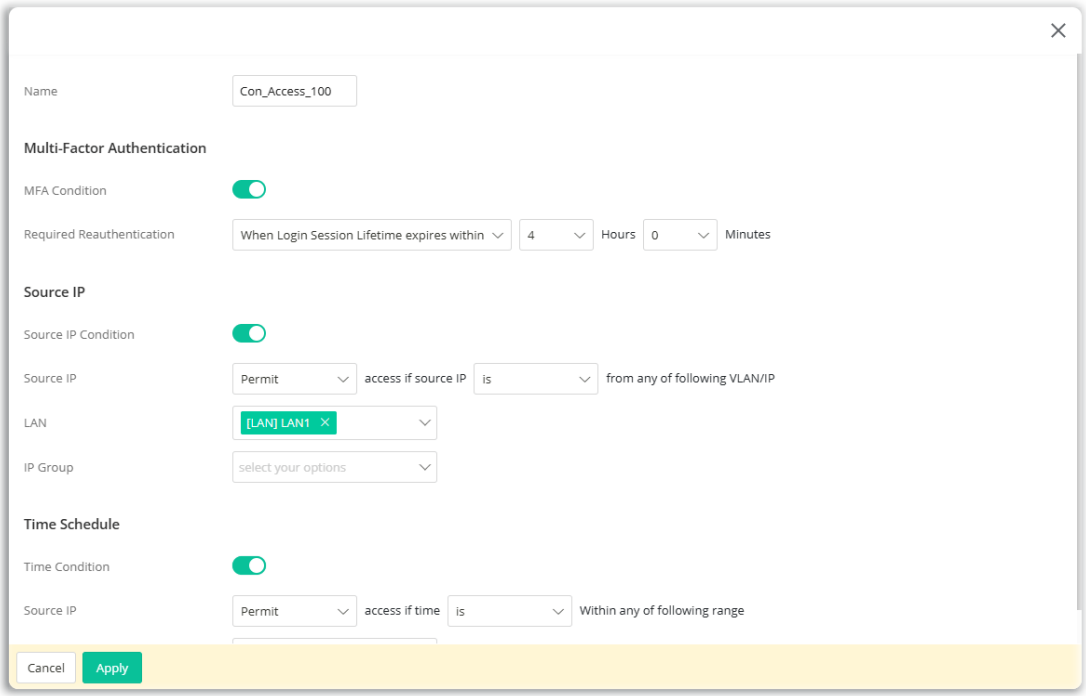
完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-3-2-4 條件式存取策略(Conditional Access Policy)

與用於設定存取控制模式的存取策略不同，此頁面提供了一種結合了時間安排、來源 IP 和多因素身份驗證 (MFA) 的策略。它可以與資源一起使用。



欲新增條件式存取策略，按下**+新增(+Add)** 。



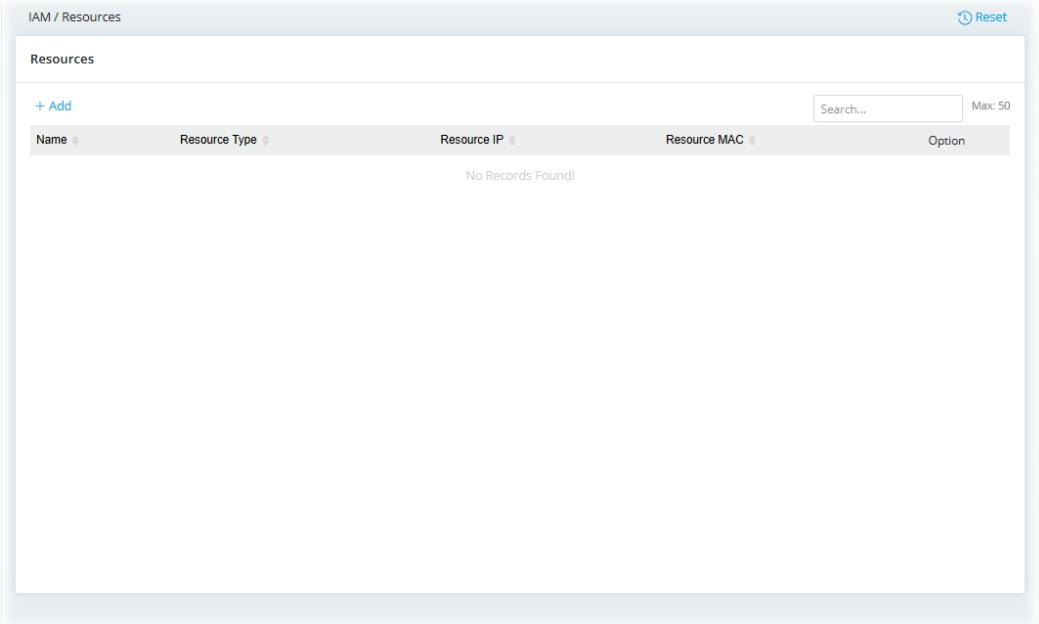
可用設定說明如下：

項目	說明
名稱(Name)	輸入辨識用的名稱。
多因驗證(Multi-Factor Authentication)。	
MFA 條件(MFA Condition)	切換開關即可啟用/停用此功能。
需要重新驗證(Required Reauthentication)	選擇每次(Everytime)或是當登入連線數有效期限在一段時間內過期時(When Login Session Lifetime expires within)。 Vigor 系統將對使用者（用戶端）執行重新驗證工作。
來源 IP(Source IP)	
來源 IP 條件(Source IP Condition)	如果來源 IP 位址來自指定的 VLAN/IP，則允許或拒絕存取。
來源 IP(Source IP)	指定來源 IP 的動作(允許或拒絕)。
LAN	選擇一個介面。
IP 群組(IP Group)	選擇要包含在此策略中的一個或多個適當的 IP 群組。
時間排程(Time Schedule)	
時間條件(Time Condition)	切換開關即可啟用/停用時間表。
來源 IP(Source IP)	確定是否允許或拒絕來源 IP 位址。
排程物件(Schedule Object)	選擇一個或多個合適的排程設定檔，以便應用於此策略。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

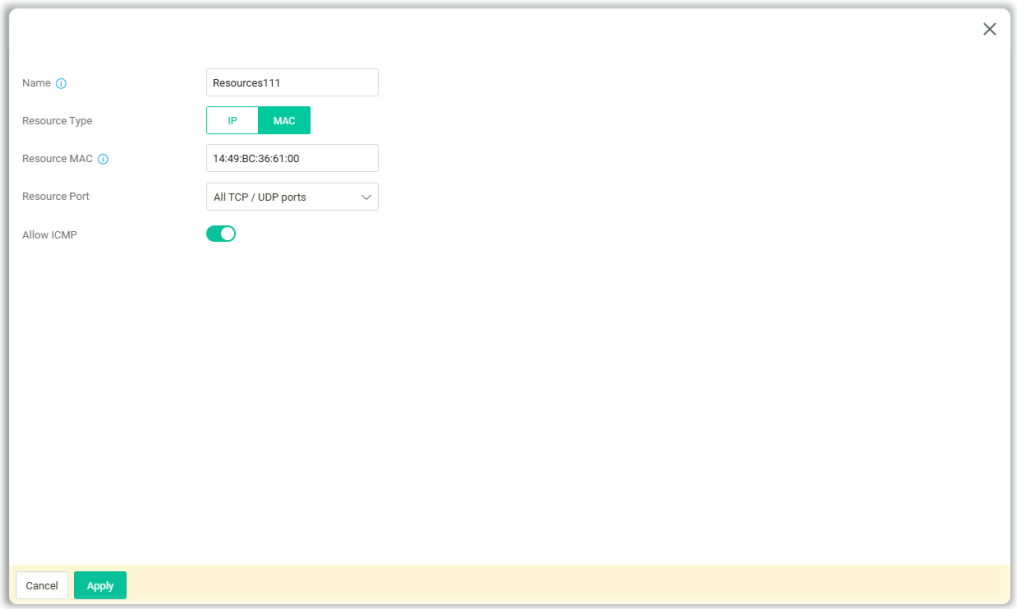
完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-3-3 資源(Resources)

此頁面透過指定來源物件的 **IP**、相應的 **MAC** 位址和連接埠類型，協助封鎖 IAM 控制下的來源物件。

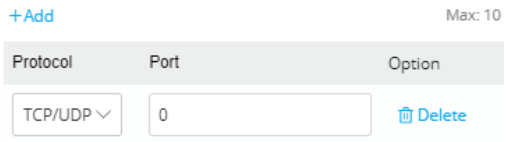
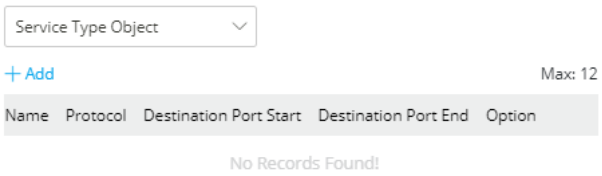


欲新增資源設定檔(最多可設定 50 個)，按下**+新增(+Add)**。



可用設定說明如下：

項目	說明
名稱(Name)	輸入辨識用的名稱。
資源類型(Resource Type)	選擇 **IP** 或者 **MAC** 作為資源類型。
資源 IP /MAC (Resource IP / MAC)	根據為此設定檔選擇的資源類型，輸入 IP 位址或 MAC 位址。
資源埠號(Resource	選擇資源連接埠類型。

Port)	• **全部的 TCP / UDP 埠號(All TCP/UDP ports)** - 傳輸控制協定(TCP)和使用者資料包協定(UDP)。 • **全部的 TCP 埠號(All TCP ports)** - 傳輸控制協定(TCP)。 • **全部的 UDP 埠號(All UDP ports)** - 使用者資料包協定(UDP)。 • **指定埠號(Specify ports)** – 選擇此連接埠類型，並分別設定 TCP/UDP、TCP 或 UDP 的連接埠號碼。  • **服務類型物件(Service Type Object)** –此欄位最多可設定 12 個服務類型物件設定檔。  按下**+新增(+Add)**在右側顯示可用服務類型清單。選擇您需要的服務類型。
允許 ICMP (Allow ICMP)	用於診斷和控制目的，發送有關 IP 操作的錯誤訊息、有關請求服務的訊息或有關主機或路由器可及性的訊息。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

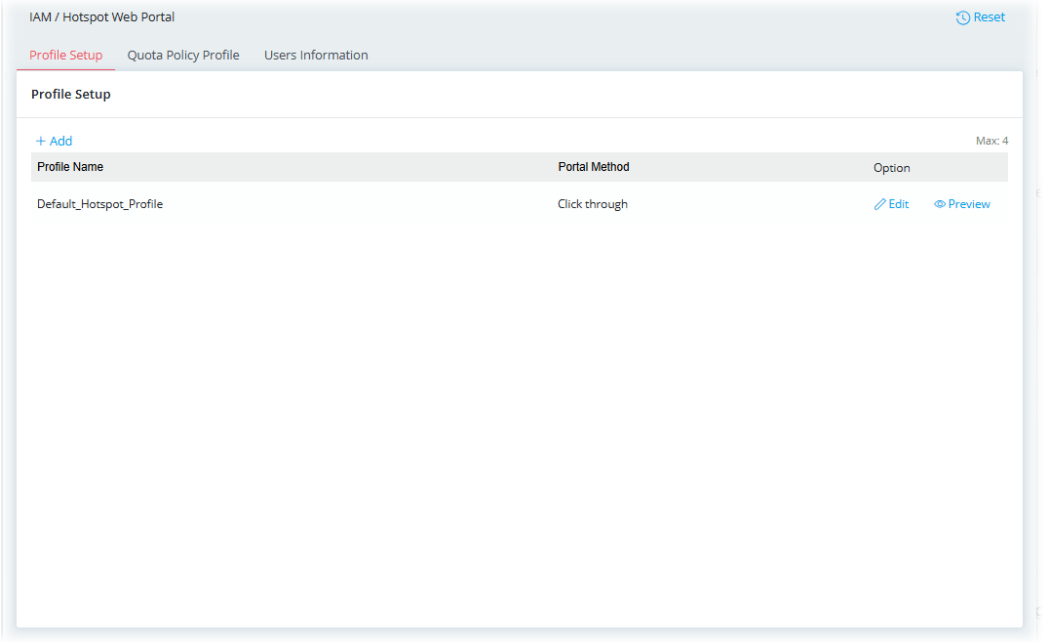
完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-3-4 客製化入口網站設定(Hotspot Web Portal)

客製化入口網站設定可讓您控制和管理來自區域網路使用者的存取。

II-3-4-1 設定檔設定(Profile Setup)

是身分識別和存取管理 (IAM) 的一種方式，用於識別、驗證和授權來自 LAN 端的任何訪問，或將使用者重新導向到您指定的登入頁面。

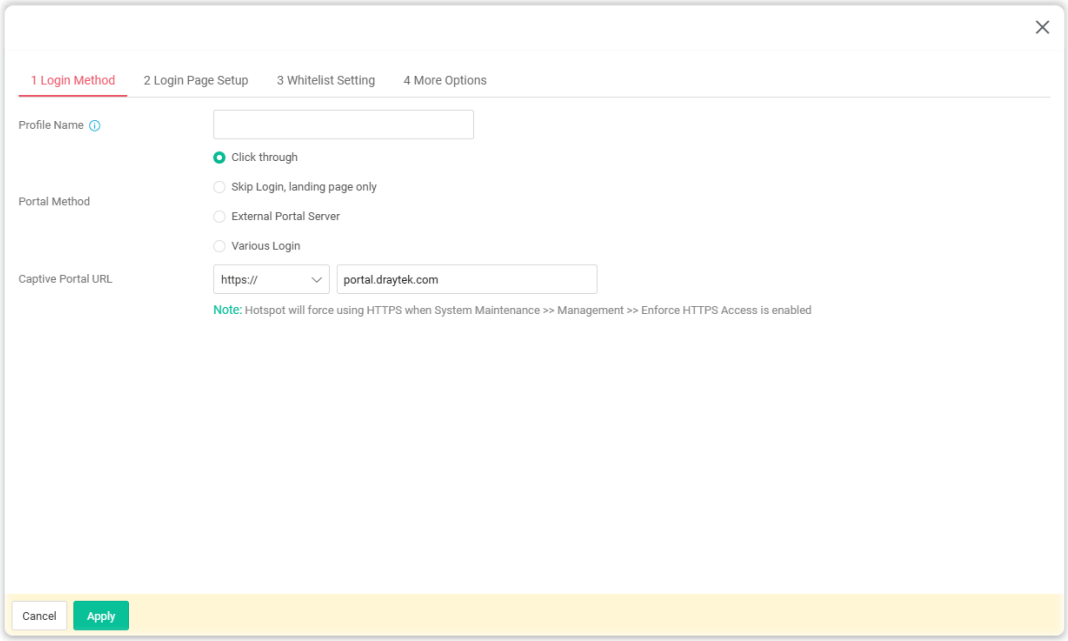


欲新增設定檔，按下**+新增(+Add)**。

按下登入方式(Login Method)、登入頁面設定(Login Page Setup)、白名單設定(Whitelist Setting)和/或更多選項(More Options)進行詳細配置。

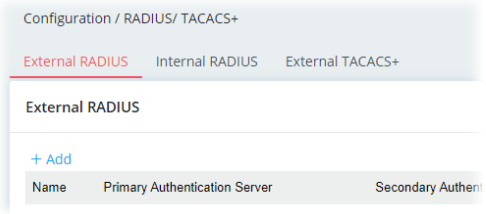
1 登入方式(Login Method)

目前，網路用戶端身份驗證有數種登入方式可供選擇：**透過點擊(Click Through)**、**跳過登入，僅指定首頁(Skip Login, landing page only)**、**外接入口網站伺服器(External Portal Server)**和**各種登入(Various Login)**，每種登入方式都會在使用者連接到網路時顯示不同的網頁。



可用設定說明如下：

項目	說明
設定檔名稱(Profile Name)	輸入辨識用的名稱。
入口網站方式(Portal Method)	**透過點擊(Click Through)**– 使用者將被重新導向至登入頁面（在強制登入 URL 中定義），並被授予存取網際網路的權限。 **跳過登入，僅指定首頁(Skip Login, landing page only)** – 此模式不執行任何身份驗證。用戶將被重新導向到登入頁面。之後，使用者可以離開登入頁面造訪其他網站。 **外接入口網站伺服器(External Portal Server)** - 當使用者首次嘗試透過路由器存取網際網路時，外部 RADIUS 伺服器將對使用者進行身份驗證。 **各種登入(Various Login)** - 當使用者第一次嘗試透過路由器存取網際網路時，會出現一個身份驗證頁面。用戶使用 Facebook 帳戶、Google 帳戶、PIN 碼或 RADIUS 伺服器密碼進行身份驗證後，將被重導向到登入頁面並獲得網路存取權限。
強制登入 URL (Captive Portal URL)	輸入強制登入 URL 網址。
重導向 URL (Redirection URL)	此功能在選擇**外接入口網站伺服器(External Portal Server)**為入口網站方式時可用。 請輸入用戶端將被重新導向到的 URL。
RADIUS	此功能在選擇**外接入口網站伺服器(External Portal Server)**為入口網站方式時可用。 如果啟用此功能，請設定以下設定： **外接 RADIUS 伺服器設定檔(External RADIUS Server Profile)** - 若要設定 RADIUS 伺服器，請按一下外接 RADIUS 鏈接，即可進入設定頁面。

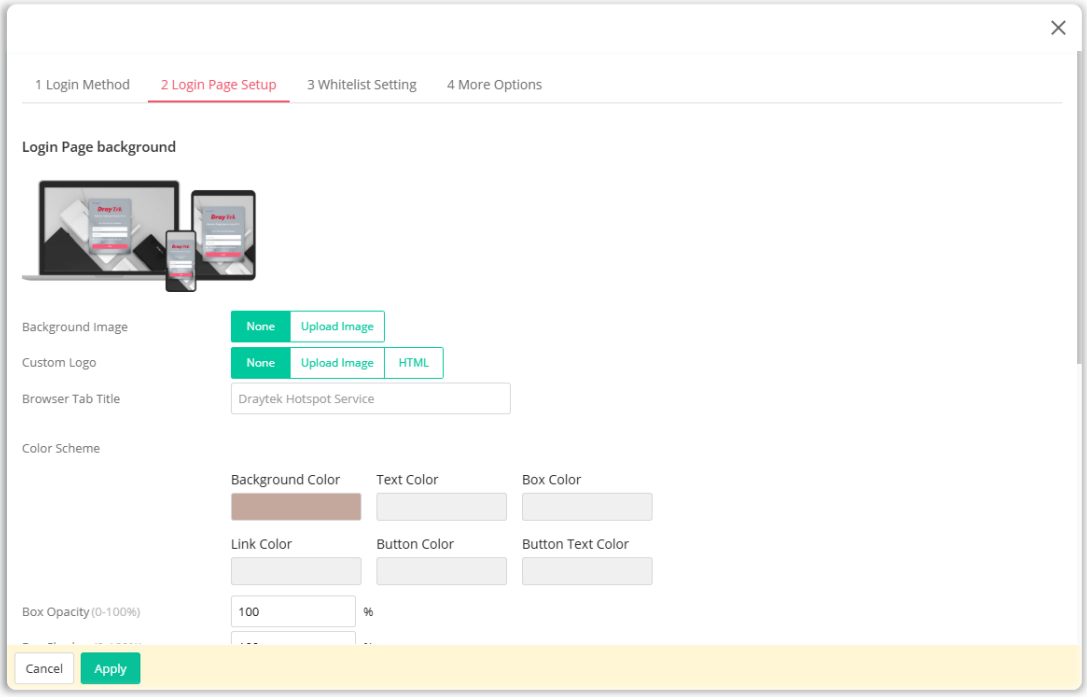
	 **RADIUS MAC 驗證(RADIUS MAC Authentication)** – 換開關以啟用/停用此功能。如果 RADIUS 伺服器支援透過 MAC 位址進行身份驗證，請啟用此功能。**RADIUS MAC 驗證**並選擇 RADIUS 伺服器使用的 MAC 位址格式。 **MAC 位址格式(MAC Address Format)** - 選擇 MAC 位址格式。 **RADIUS NAS-識別碼(RADIUS NAS-Identifier)** - 輸入 ID。
登入方式(Login Method)	此設定在以下情況下，可選擇**各種登入(Various Login)**作為門戶方法。 選擇一種或多種所需的登入方式。切換開關以啟用所需選項。 • **Facebook** • **Google** • **透過簡訊輸入 PIN 碼(PIN via SMS)** • **透過郵件輸入 PIN 碼(PIN via Mail)** • **RADIUS** • **切換資訊(Leave Info)** **臉書(Facebook) -** 選擇 **Facebook** 為登入方式時可設定如下內容。 • **臉書 APP ID (Facebook APP ID)** -輸入有效的 Facebook 開發者應用程式 ID。 • **臉書 APP 密鑰(Facebook APP Secret)** - 輸入為上方輸入的 APP ID 設定的金鑰。 **Google -** 選擇 **Google** 為登入方式時可設定如下內容。 • **Google App ID** – 輸入有效的 Google 應用程式 ID。 • **Google APP 密碼(Google App Secret)** - 輸入為上方輸入的 APP ID 設定的金鑰。 **PIN 碼透過簡訊(PIN via SMS) -** 選擇 **PIN 碼透過簡訊**為登入方式時可設定如下內容。 • **簡訊服務供應商(SMS Provider)** - 選擇用於發送 PIN 碼通知的簡訊服務提供者。 • **簡訊內容(SMS Content)** – 輸入訊息。 **PIN 碼透過郵件(PIN via Mail) -** 選擇 **PIN 碼透過郵件**為登入方式時可設定如下內容。 • **郵件伺服器(Mail Server)** -選擇用於發送 PIN 碼通知的郵件伺服器。 • **郵件內容(Mail Content)** – 輸入訊息。 **RADIUS -** 選擇 **RADIUS** 為登入方式時可設定如下內容。 • **外接 RADIUS 伺服器設定檔(External RADIUS Server Profile)** - 選擇 RADIUS 伺服器設定檔。 • **RADIUS MAC 驗證(RADIUS MAC Authentication)** – 切換開關以啟用/停用此功能。如果 RADIUS 伺服器支援透過 MAC 位址進行身份驗證，請啟用此功能。**RADIUS MAC 認證**並選擇 RADIUS 伺服器使用的 MAC 位址格式。 • **MAC 位址格式(MAC Address Format) –** 選擇 MAC 位址格式。 • **RADIUS NAS-識別碼(RADIUS NAS-Identifier) -** 輸入 ID。 **表格(因應切換資訊) –** 選擇**切換資訊(Leave Info)**為登入方式時可設定如下內容。

	• **+新增(+Add)** – 新增新的切換資訊條目（最多 10 個）。 • **資訊類型(Info Type)** – 選擇客戶需要提供的資訊（例如，一般資訊、電話、電子郵件或核取方塊）以建立連線。 • **必需(Required)** –若啟用，登入頁面上將要求輸入進一步連接所需的資訊。 • **標題(Title)** –輸入切換資料的標題。 • **內容(Content)** – 輸入切換資料替代文字。 • **選項(刪除)(Option (Delete))** – 按此移除選定的項目。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

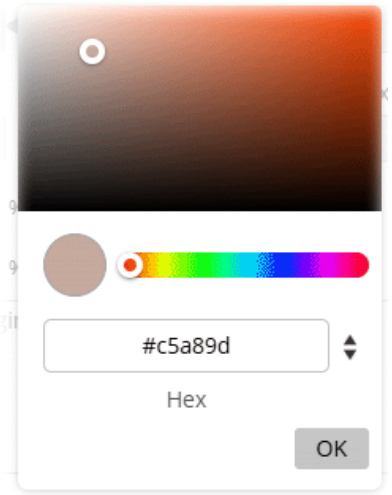
2 登入頁面設定(Login Page Setup)

如果您選擇的登入模式需要身份驗證，請點選**登入頁面設定(Login Page Setup)**選擇登入頁面的背景。



可用設定說明如下：

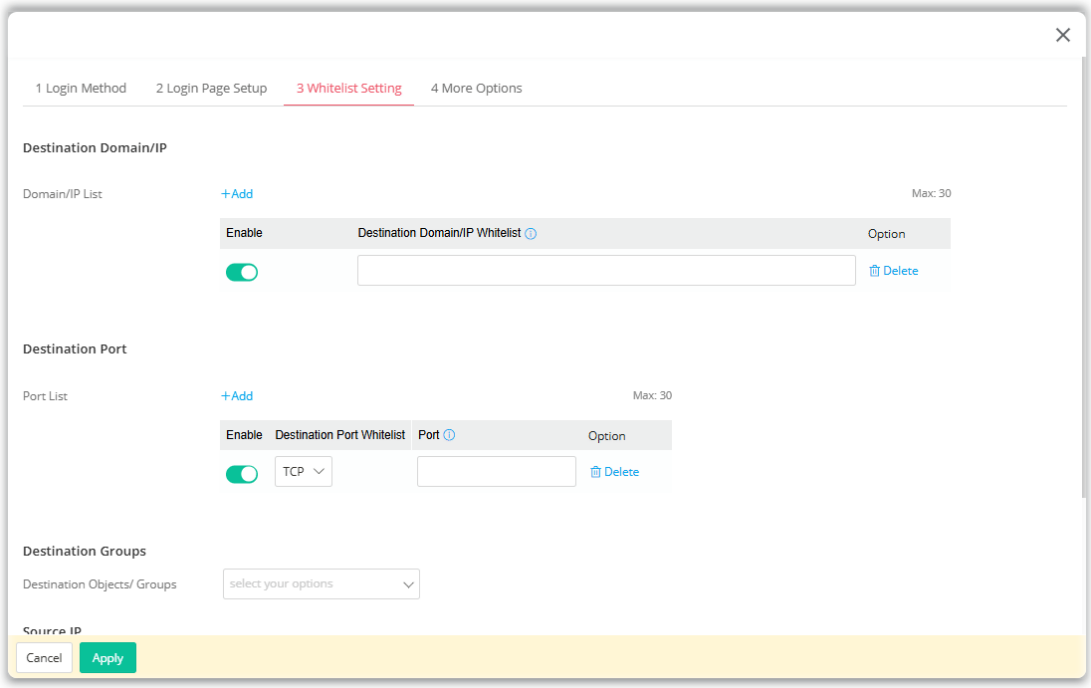
項目	說明
	登入頁面背景(Login Page background)
背景影像(Background Image)	設定登入頁面背景方案。 **無(None)** – 不會使用任何圖片。 **上傳影像(Upload Image)** – 選擇圖片檔案（.JPG 或 .PNG 格式）作為背景圖片。檔案大小必須小於 5MB。 ● **目前背景影像(Current Background Image)** – 按下**上傳(Upload)**將選定的檔案上傳到 Vigor 路由器系統。
客製化標誌(Custom Logo)	設定入口網站上顯示的標誌。 **無(None)** –將使用 DrayTek 的預設標誌。 **上傳影像(Upload Image)** – 按此以使用其他圖片作為標誌。檔案大小必須小於 1MB。 ● **目前標誌影像(Current Logo Image)** – 按下**上傳(Upload)** 將選定的檔案儲存到 Vigor 路由器系統。 **HTML** – 輸入影像的 HTML (e.g., < <img src="https://www.example.com/logo.png" style="display: block;" width="220" height="80">)。
瀏覽器標籤標題(Browser Tab Title)	輸入要在瀏覽器中顯示為網頁標題的文字。
顏色方案(Color Scheme)	設定背景、文字、方框、連結、按鈕和按鈕文字的顏色。此時會彈出一個顏色框，您可以拖曳滑鼠游標選擇所需的顏色。

	
方框不透明度(Box Opacity)	設定背景影像的不透明度（0-100%）。
方框陰影(Box Shadow)	設定登入欄位的透明度（0-100%）。
歡迎訊息(Welcome Message)	輸入要顯示的歡迎訊息文字。
條款和條件(Terms and Conditions)	切換開關以啟用此功能。 **使用者必須勾選以取得網際網路存取權限(User must tick to get the internet access)** – 如果選取此項，任何希望存取網路的使用者都必須勾選此方塊以同意相關條款和條件。否則，Vigor 系統將拒絕其網路存取權限。
相關條款與條件內容(Terms and Conditions Content)	選擇**內部內容** 或者**外部內容**。 **內部內容(Internal Content)** - 輸入要在條款與條件彈出視窗中顯示的文字。 **外部內容(External Content)** - 輸入網址。點擊熱點登入頁面上的條款與條件連結後，用戶端將被重新導向到此處指定的網址存取網頁。
用於行銷的資料蒐集(Data Collection for Marketing)	切換開關以啟用此功能。 **使用者必須勾選以取得網際網路存取權限(User must tick to get the internet access)** – 如果選取此項，任何希望存取網路的使用者都必須勾選此方塊以同意相關條款和條件。否則，Vigor 系統將拒絕其網路存取權限。 **行銷內容(Marketing Content) -** 輸入要告知使用者的文字。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

3 白名單設定(Whitelist Setting)

在此頁面，您可以設定白名單設定。使用者可以傳送和接收符合白名單設定的資料流量。



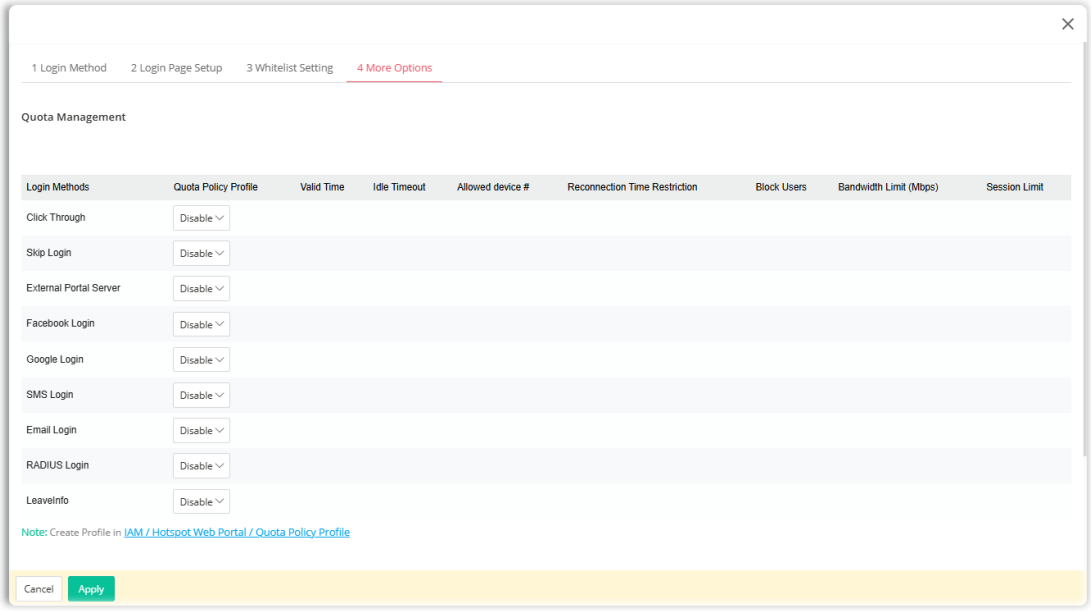
可用設定說明如下：

項目	說明
目的網域/IP (Destination Domain/IP)	
網域/IP 清單(Domain/IP List)	**+新增(+Add) –** 按此新增條目。 **啟用(Enable)** – 切換開關以啟用/停用該設定。 **目的網域/IP 白名單(Destination Domain/IP Whitelist)** – 請輸入 IP 位址或域名，無需新增「http://」或「https://」等前置文字。 **選項(刪除)(Option (Delete))** – 刪除目前的條目。
目的埠號(Destination Port)	
埠號清單(Port List)	**+新增(+Add) –** 按此新增條目。 **啟用(Enable)** – 切換開關以啟用/停用該設定。 **目的埠號白名單(Destination Port Whitelist)** – 選擇 TCP、UDP 或 TCP/UDP。然後，輸入連接埠號。 **埠號(Port)** – 輸入數字。 **選項(刪除)(Option (Delete))** – 刪除目前的條目。
目的群組(Destination Groups)	
目的物件/群組 (Destination Objects/ Groups)	選擇一個或多個 IP 物件/群組作為目的。 允許存取選定的群組。
來源 IP(Source IP)	
來源 IP 清單(Source IP List)	選定的 IP 位址已獲准通過路由器。 **+新增(+Add) –** 按此新增條目。 **啟用(Enable)** – 切換開關以啟用/停用該設定。 **來源 IP 白名單(Source IP Whitelist)** – 輸入 IP 位址。 **選項(刪除) (Option (Delete))** – 刪除目前的條目。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

4 更多選項(More Options)

在此步驟中，您可以進行設定進階的客製化入口網站設定選項。



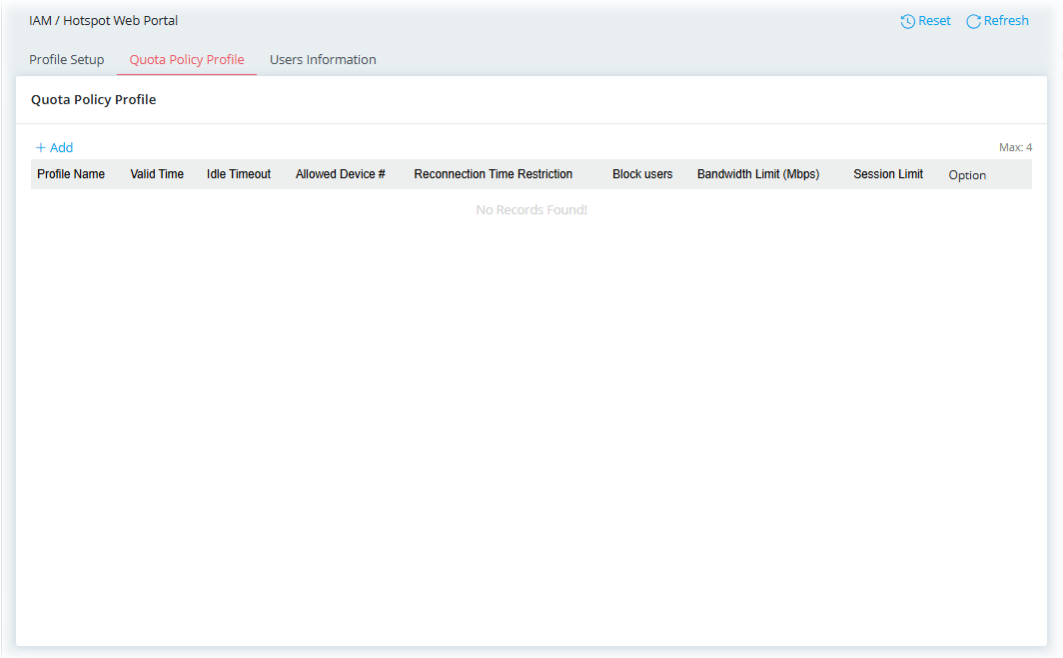
可用設定說明如下：

項目	說明
額度管理(Quota Management)	
登入方式 (Login Methods)	顯示不同的登入方式。每種方式皆可單獨設定額度策略設定檔。
額度策略設定檔 (Quota Policy Profile)	為每種登入方式指定額度策略設定檔。 預設值為**停用**。 如有需要，可前往 **IAM>>客製化入口網站>>額度策略設定檔** **(IAM>>Hotspot Web Portal>>Quota Policy Profile)**設定多個設定檔。
驗證後登入指定首頁(Landing Page After Authentication)	
驗證後登入指定首頁 (Landing Page After Auth)	**固定 URL (Fixed URL)** – 指定使用者成功通過驗證後將顯示的網頁。 使用者將被重新導向到指定的 URL。可用於向使用者顯示特定的廣告，例如在飯店內向要求無線網路存取的客人顯示廣告。 **使用者請求的 URL (User Requested URL)** – 使用者將被重導向到他們最初請求的網址。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

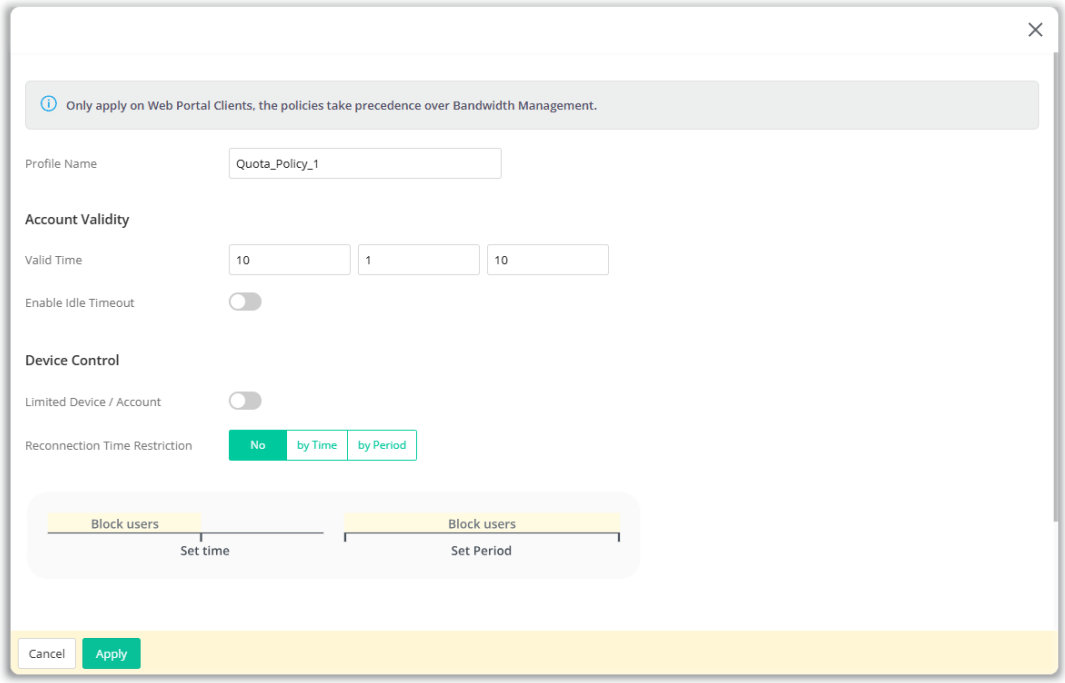
完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-3-4-2 額度策略設定檔(Quota Policy Profile)

系統管理員可以設定僅適用於入口網站用戶端的有效時間、空閒時間、重新連線時間、頻寬和連線數配額的限制。



欲新增額度策略設定檔，請按下+**新增(+Add)**。



可用設定說明如下：

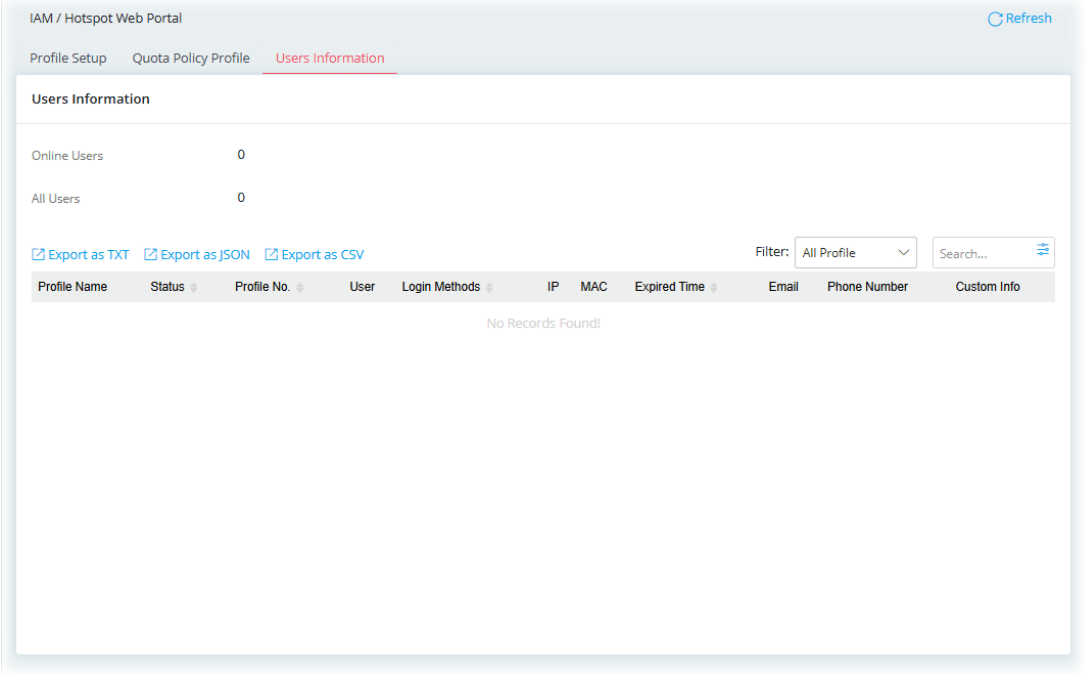
項目	說明
設定檔名稱(Profile Name)	輸入辨識用的名稱。

帳戶效期(Account Validity)	
有效時間(Valid Time)	透過設定天數（0-180）、小時數（0-23）和分鐘數（0-59）來設定登入的有效期限。 登入期限到期後，Vigor 路由器將中斷客戶端與網路或網際網路的連線。如果用戶端希望再次登錄，則需要透過 Vigor 路由器進行驗證或認證。
啟用閒置逾時(Enable Idle Timeout)	啟用此選項後，如果在指定的空閒時間過後使用者沒有任何活動，Vigor 路由器將終止網路連線。 **閒置逾時(Idle Timeout)** – 輸入一個數字（1-480，分鐘）。
裝置控制(Device Control)	
限制的裝置/帳戶 (Limited Device / Account)	設定每個帳戶可連線的最大裝置數，以及用戶端透過網路入口網站存取網際網路的時間限制。 切換開關即可啟用或停用該功能。 如果啟用，請設定允許的設備數量。 **允許的裝置 # (Allowed device #)** – 設定每個帳戶可連線的最大裝置數，以及用戶端透過網頁入口網站存取網際網路的時間限制。最大值為 100。
重新連接時間限制 (Reconnection Time Restriction)	透過以下數種方式之一阻止該帳戶用於將裝置連接到網路： **不(No)** – 不封鎖不封鎖阻檔。 **透過時間(by Time)** – 登入過期後，該帳戶將無法用於將裝置連接到網絡，直到設定的時間為止。 • **封鎖使用者前(Block users before)** – 從下拉式選單中選擇截止時間(小時和分鐘)。時間到期後，使用者的存取權限將被中斷並封鎖。 **透過期限(by Period)** – 登入過期後，該帳戶在一段時間內無法用於將裝置連接到網路。 • **封鎖使用者以(Block users for)** – 輸入小時數和分鐘數，以指定使用者封鎖期間。
頻寬與連線數限制(Bandwidth & Session Limit)	
頻寬限制(Bandwidth Limit)	設定最大上傳和下載速度。 切換開關即可啟用或停用此功能。 如果啟用此功能，請設定以下限制： **上傳限制/下載限制 (Upload Limit / Download Limit)** – 輸入一個數字(1 到 9999)。
連線數限制(Session Limit)	設定入口網站用戶端的最大連線數限制。 切換開關即可啟用或停用此功能。 如果啟用此功能，請設定以下內容： **連線數(Sessions)** –輸入一個數字(1 到 50000)。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-3-4-3 使用者資訊(User Information)

此頁面提供有關連接到此路由器的使用者（網頁入口網站用戶端）的詳細資訊。

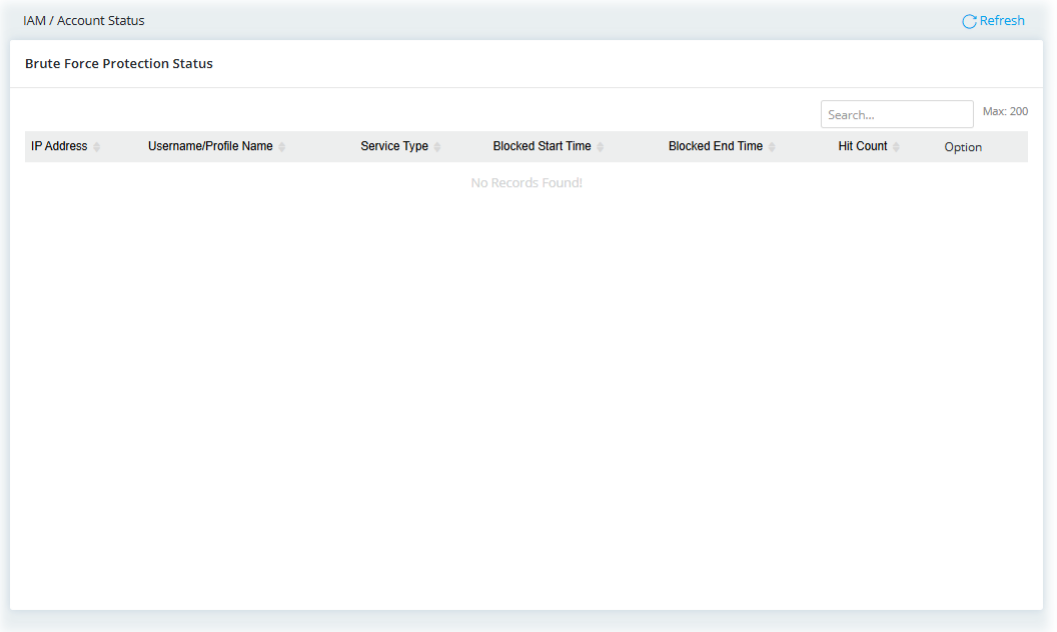


可用設定說明如下：

項目	說明
線上使用者(Online Users)	顯示透過 Vigor 路由器連接到網路的線上使用者數量。
所有使用者(All Users)	顯示透過 Vigor 路由器連接到網際網路的使用者總數（包括線上使用者和離線使用者）。
匯出為 TXT 文件(Export as TXT)	按此可匯出用戶資訊為 TXT 檔。
匯出為 JSON 文件(Export as JSON)	按此可將使用者資訊匯出為 JSON 檔案。
匯出為 CSV 文件(Export as CSV)	按此可將使用者資訊匯出為 CSV 檔案。
過濾器(Filter)	顯示客製化入口網站設定的個人資料。

II-3-5 帳號狀態(Account Status)

此頁面顯示 IAM 使用者帳戶（例如使用 FTP 和 IAM 服務）的暴力攻擊防護狀態。

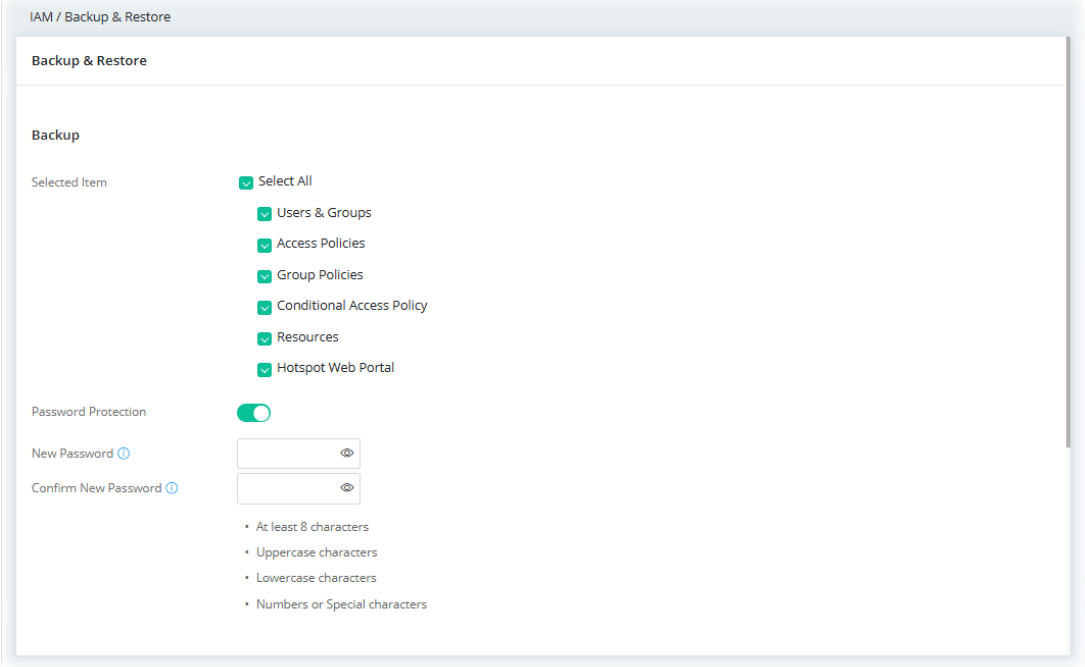


可用設定說明如下：

項目	說明
命中次數(Hit Count)	顯示 IAM 使用者觸發處罰或使用者帳戶鎖定的次數。
選項(Option)	**解除封鎖(Unblock)** – 移除被封鎖的 IP 位址。 **新增至黑名單(Add to Block List)** - 將 IP 位址新增至防禦設定的白/黑名單。

II-3-6 備份與還原(Backup & Restore)

此頁面可用於備份/還原 IAM 設定。



可用設定說明如下：

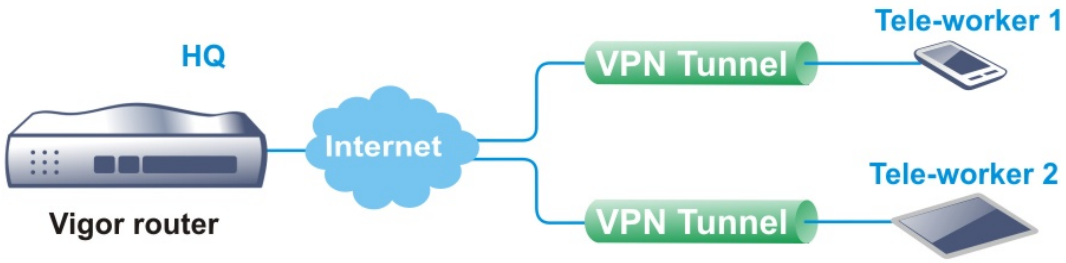
項目	說明
	備份(Backup)
選定項目(Selected Items)	選擇用於設定備份的項目類型。
密碼保護(Password Protection)	為了安全起見，可以對此裝置的設定檔進行加密。 切換開關即可啟用或停用此功能。 **新的密碼(New Password)** – 輸入字元作為加密設定檔的密碼。 **確認新密碼(Confirm New Password)** – 再次輸入字元確認。 **備份(Back up)** – 按此即可備份設定檔。
	還原(Restore)
還原自備份檔案(Restore from Backup File)	– 按此找到要還原的檔案。 **還原(Restore)** – 按此執行還原操作。
檔案具有密碼保護(File has Password Protection)	切換開關即可啟用或停用此功能。 如果啟用，則還原設定時需要密碼。 **密碼(Password)** – 輸入用於還原設定的密碼。

II-4 VPN 連線設定

虛擬私人網路 (VPN) 是專用網路的擴展，它涵蓋了跨越共享或公共網路 (例如網際網路) 的連接。簡而言之，借助 VPN 技術，您可以透過共享或公共網路在兩台電腦之間傳輸數據，其方式模擬了點對點專用鏈路的特性。

以下是 VPN 的一些用途：

- 總部與客戶之間的溝通。
- 遠距辦公人員、出差員工和總部之間建立安全連線。
- 遠端辦公室與總部之間交換資料。
- 連鎖店與總部之間的 POS 系統。
- 繞過網路審查，即繞過對網站或內容的過濾。
- 規避服務提供者或供應商為阻止或限制使用者服務而採用的地理位置定位技術。
- 透過公共基地台進行安全通信

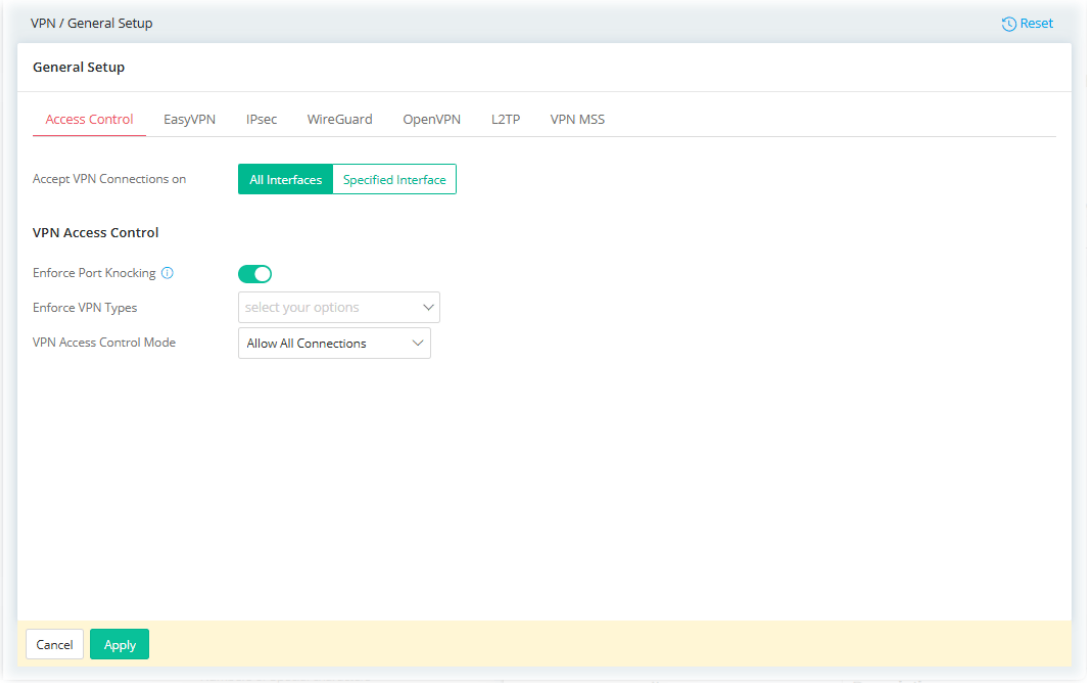


II-4-1 基本設定

本節提供不同類型（例如 IPsec、WireGuard 和 OpenVPN）VPN 伺服器的基本設定。

II-4-1-1 存取控制(Access Control)

管理員可以透過設定允許 VPN 撥入的介面，並將其與 VPN 來源 IP 位址的白名單或黑名單配對，來建立安全的 VPN 連線。



可用設定說明如下：

項目	說明
接受 VPN 連線於(Accept VPN Connections on)	透過設定 IP 物件/群組白名單或黑名單來過濾受信任的 VPN 連線。 選擇要接受 VPN 連線的 WAN 介面。 **全部的介面(All Interfaces)** – 在所有 WAN 介面上接受 VPN 連線。 **指定介面(Specified Interface)** – 自訂 WAN 介面、IP 位址和 VPN 通訊協定，以允許 VPN 連線。 **+新增(+Add)** – 按此新增條目，最多可設定 8 個。 • **WAN** – 選擇 WAN 介面。 • **IPv4 位址(IPv4 Address)** – 選擇 WAN IP 位址(預設 WAN IP)或停用此選項。 • **允許的 VPN 通訊協定(Allowed VPN Protocols)** – 共有四種協定（IPsec、WireGuard、OpenVPN 和 EasyVPN）。請選擇允許用於 VPN 連線的協定。 • **選項(Option)** – 按此移除選取的介面。
VPN Access Control	
Enforce Port Knocking	切換開關以啟用/停用 Port Knocking 功能。. **強制執行服務類型(Enforce Service Types)** – 選擇通訊協定。只有成功完

	成 Port Knocking 的來源 IP 位址才能存取這些選定的服務（從 WAN 介面）；其他 IP 位址都會被拒絕。
VPN 存取控制模式(VPN Access Control Mode)	透過設定 IP 物件/群組白名單或黑名單來過濾受信任的 VPN 連線。 **允許全部連線(Allow All Connections)** – 接受所有用戶端的 VPN 連線。 **白名單(Allow List)** – 接受以下所選 IP 物件/群組設定中的使用者的 VPN 連線。 • **+新增(+Add)** - 按此進行新的條目設定。 **黑名單(Block List)** – 拒絕來自下列選定的 IP 物件/群組設定中的使用者的 VPN 連線。 • **+新增(+Add)** -按此進行新的條目設定。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

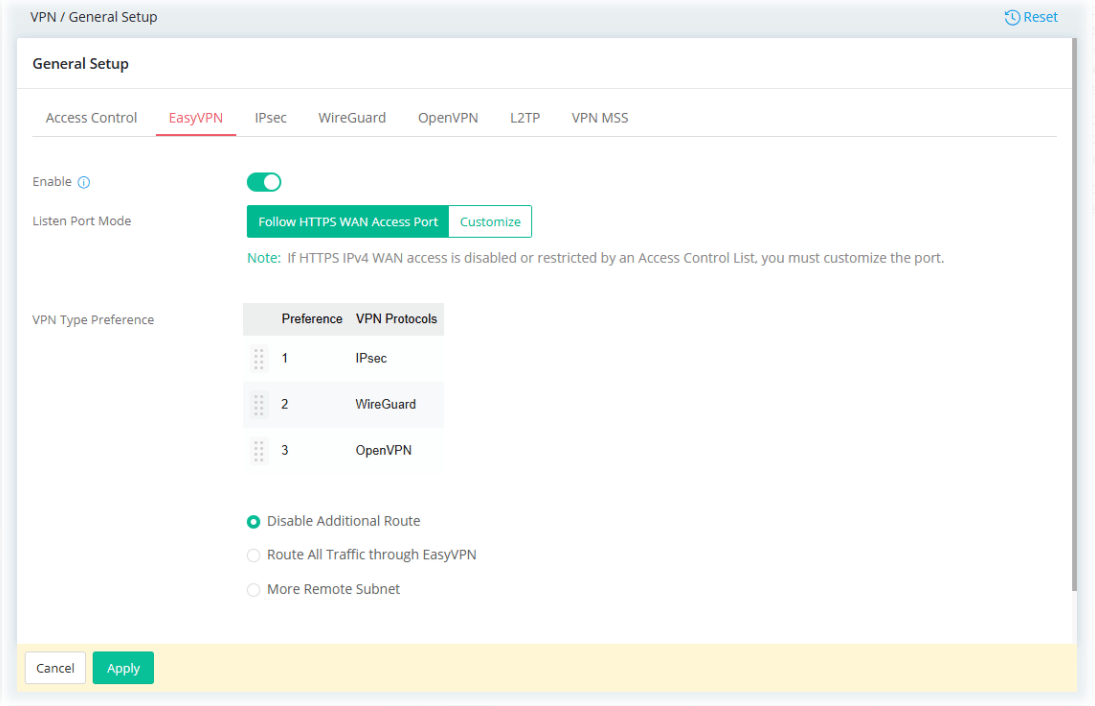
完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-4-1-2 EasyVPN 設定

Vigor 路由器支援多種 VPN 協議，包括 IPsec、WireGuard 和 OpenVPN。然而，一般用戶可能難以選擇合適的通訊協定，或在 VPN 設定過程中遇到困難。此外，環境因素有時也會影響 VPN 連線是否成功。為了解決這些問題，Vigor 路由器引入了一種名為 EasyVPN 的新通訊協定，簡化 VPN 設定流程。

使用 EasyVPN，使用者無需再為 WireGuard 產生金鑰、導入 OpenVPN 設定檔或上傳憑證。欲成功建立 VPN 連接，使用者只需輸入使用者名稱和密碼，或透過電子郵件獲取一次性密碼 (OTP)。

此外，如果無法建立 VPN 連線，不論是何種原因，Vigor 系統都會自動將 EasyVPN 連線切換到下一個可用協定並嘗試重新連接。



可用設定說明如下：

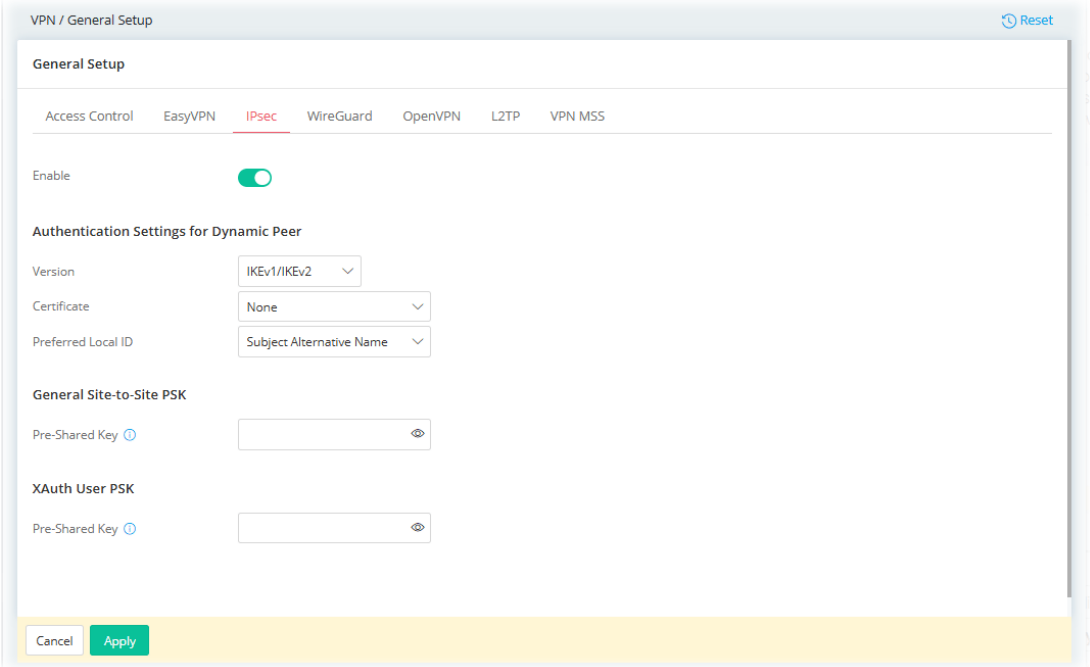
項目	說明
啟用(Enable)	切換開關以啟用/停用此服務。
監聽通訊埠模式(Listen Port Mode)	設定 EasyVPN 服務監聽的埠號。 **依循 HTTPS WAN 存取埠號(Follow HTTPS WAN Access Port) –** 對於 EasyVPN 服務，請使用與 HTTPS 管理連接埠相同的埠號。確保已啟用來自 WAN 的 HTTPS 管理，以允許 EasyVPN 用戶端和 EasyVPN 伺服器之間進行通訊。 **客製化(Customize) –** 選擇此項可手動定義監聽埠值。 ● **監聽埠(Listen Port) –** 輸入埠值(1-65535)。
VPN 類型喜好設定(VPN Type Preference)	此功能允許使用者自訂撥號 VPN 連線的優先權。預設情況下，優先順序是基於 VPN 效能，排列如下：IPsec VPN > WireGuard VPN > OpenVPN。 欲更改順序，只需在提供的介面中拖曳並重新排列項目即可。 **喜好設定(Preference) –** 顯示 VPN 協定的順序。 **VPN 通訊協定(VPN Protocols) –** 顯示 VPN 協定名稱。
停用附加路由(Disable Additional Route)	如果選取（啟用）此功能，則其他路由（在更多遠端子網(More Remote Subnet)中建立的）將不會用於 VPN 連線。

透過 EasyVPN 路由所有流量(Route All Traffic through EasyVPN)	如果選取（啟用）此功能，則所有流量都將透過 EasyVPN 路由。
更多遠端子網(More Remote Subnet)	選擇此功能可為 Vigor 路由器建立更多子網，從而為遠端用戶端提供 VPN 服務。 **+新增(+Add)** – 按此即可建立新的 VPN 連線設定。最多可建立 8 個 VPN 連線設定檔。 **遠端網路(Remote Network)** – 輸入遠端客戶端的 IPv4 位址。 **子網遮罩(Subnet Mask)** – 使用下拉式清單指定遠端客戶端的子網路遮罩。 **選項(Option)** – 按此刪除按鈕以移除所選介面。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-4-1-3 IPsec 設定

IPsec（網際網路協定安全）對網路流量進行加密和驗證，確保透過 VPN 進行安全資料傳輸。它可以防止未經授權的存取、資料篡改和竊聽，使其成為遠端辦公、站點間連接和遠端辦公人員連接的理想選擇，同時還能保護在不受信任的網路上傳輸的敏感資訊。



可用設定說明如下：

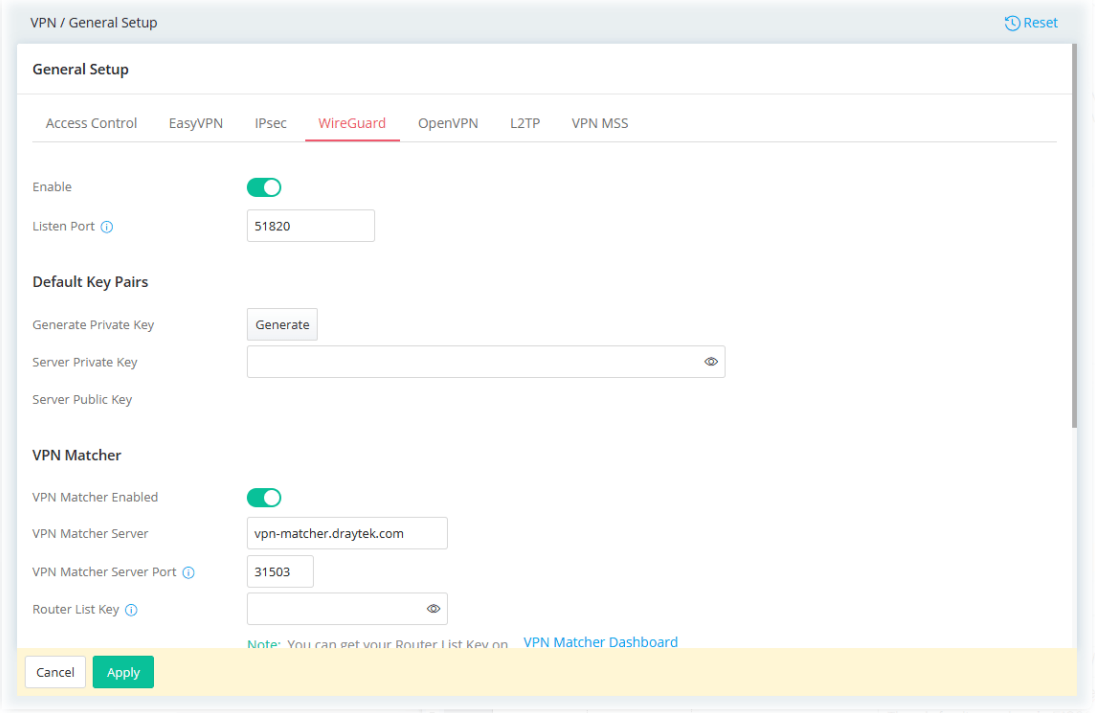
項目	說明
啟用(Enable)	切換開關以啟用/停用此設定。
動態對端驗證設定(Authentication Settings for Dynamic Peer)	
版本(Version)	選擇 IPsec VPN 的安全協定版本(IKEv1/IKEv2，IKEv1 或 IKEv2)。
憑證(Certificate)	選擇路由器 VPN 伺服器憑證。它將用於 IPsec 連線中的 X.509 身份驗

	證。 若要在路由器上設定憑證，請前往設定>>憑證 (Configuration>>Certificates) 部分。
優選本機 ID (Preferred Local ID)	選擇**主體替代名稱(Alternative Subject Name)**或是**主體名稱(Subject Name)**。 指定 IPsec 驗證的首選本機 ID 資訊(主體替代名稱或主體名稱)。
一般點對點預先共享金鑰 (PSK) (General Site-to-Site PSK)	**預先共享金鑰(Pre-Shared key)** - 定義用於一般身份驗證的 PSK 金鑰。
XAuth 使用者預先共享金鑰(PSK) (XAuth User PSK)	**預先共享金鑰(Pre-Shared key)** - 定義 IPsec XAuth 驗證的 PSK 金鑰。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-4-1-4 WireGuard 設定

WireGuard 是一種安全、快速且現代的開源 VPN 通訊協定。此 VPN 連線可以透過在 VPN 伺服器(例如 Vigor 路由器)和 VPN 用戶端(例如 WireGuard VPN 用戶端)之間交換虛擬金鑰和公開金鑰來建立 VPN 連線。



可用設定說明如下：

項目	說明
啟用(Enable)	切換開關以啟用/停用此設定。
監聽埠(Listen Port)	請輸入 WireGuard VPN 伺服器的埠號。 預設值為 51820。
預設金鑰組(Default Key Pairs)	
產生虛擬金鑰(Generate Private Key)	**產生(Generate)** – 產生 VPN 伺服器的金鑰(虛擬和公開)。
伺服器虛擬金鑰(Server Private Key)	顯示產生的虛擬金鑰。
伺服器公開金鑰(Server Public Key)	需要在 WireGuard VPN 用戶端路由器中進行設定。 按下**產生(Generate)**按鈕後，公開金鑰將顯示在此頁面上。
VPN 比對機制(VPN Matcher)	
VPN 比對機制已啟用(VPN Matcher Enabled)	此 VPN 比對技術基於標準的 WireGuard VPN 協定。 通常，要建立 VPN 連接，至少一方必須擁有真實 IP 位址。 VPN 比對伺服器可以幫助位於 NAT 後面的兩台 Draytek 路由器建立安全的 VPN 隧道，用於彼此之間的資料傳輸。 切換此開關即可啟用/停用 VPN 比對功能。 請注意，只有支援 WireGuard 的 drayos4 型號才能透過比對與

	Vigor2928 建立 VPN 連線。
VPN 比對機制伺服器(VPN Matcher Server)	DrayTek VPN 比對伺服器的 IP 位址定義為 vpn-matcher.draytek.com。
VPN 比對機制伺服器埠號(VPN Matcher Server Port)	DrayTek VPN 比對伺服器的 IP 位址定義為 vpn-matcher.draytek.com，連接埠號碼為 “31503” 。
路由器清單金鑰 (Router List Key)	輸入身份驗證金鑰，用於從 VPN 比對伺服器尋找與該裝置屬於同一組的 Vigor 路由器。然後透過 VPN 設定精靈在兩端 Vigor 路由器之間設定 VPN 連結。
STUN 伺服器 (STUN Server)	**偵測(Detect)** - 按此查看 Vigor 路由器使用的 NAT 類型是否為核心 NAT。如果不是，則無法建立任何的 VPN 連線。
偵測狀態 (Detect Status)	**取得裝置清單(Get Device List) -** 輸入上面的授權金鑰後，按此取得與本裝置屬於同一組的可用 Vigor 路由器。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-4-1-5 OpenVPN 設定

OpenVPN 協定利用公開金鑰、憑證以及使用者名稱和密碼來驗證客戶端身分。流量會透過採用業界標準 SSL/TLS 加密通訊協定建立的安全通道傳輸。

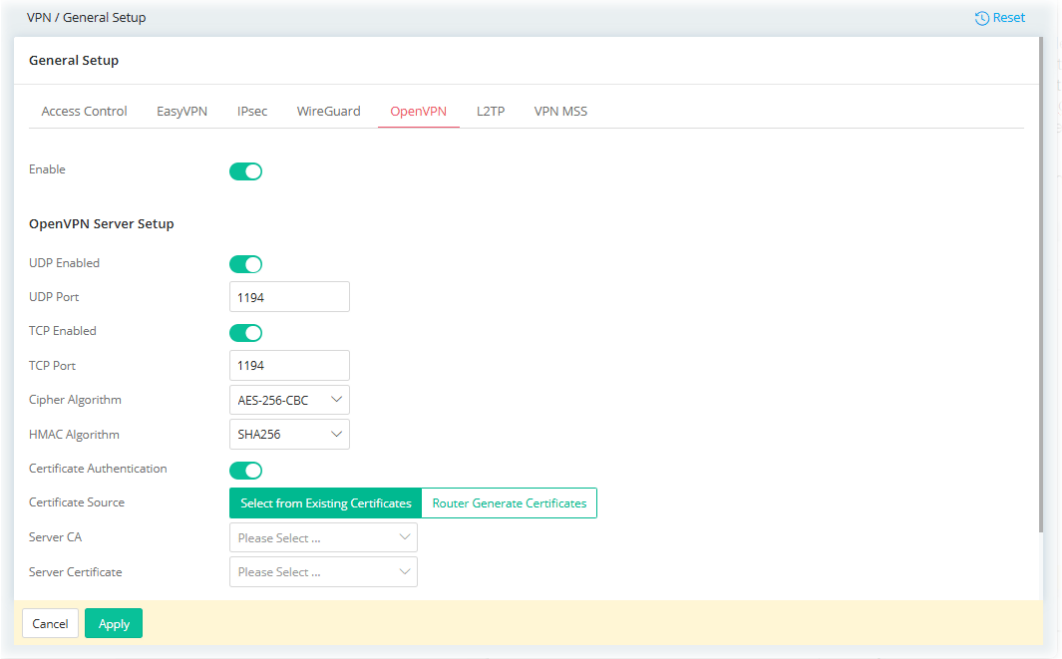
透過整合 OpenVPN，Vigor 路由器可以幫助使用者實現更強大、更可靠、更安全的私有連線，以滿足企業需求。

OpenVPN 為使用者提供了一種便捷的方式來建立本地端和遠端之間的 VPN 連線。 OpenVPN 有兩個優點：

- 它可以運行在不同的系統上，例如 Windows、Linux 和 MacOS。
- 基於 SSL 加密的標準協議，OpenVPN 可以為您提供可擴展的用戶端/伺服器模式，允許多個用戶端透過單一 TCP 或 UDP 連接埠連接到單一 OpenVPN 伺服器進程。

在憑證方面，管理員可以選擇讓路由器產生憑證，或匯入第三方憑證頒發機構 (CA) 頒發的憑證。如果路由器產生憑證，它將作為 Root CA 頒發具公信力之憑證。但是，如果使用第三方 CA 所發出的憑證，則需要將該 CA 的憑證和路由器產生的憑證分別匯入路由器的具公信力之憑證和本機憑證部分。

OpenVPN 需要使用憑證。建立 OpenVPN 連線之前，應先設定 OpenVPN 服務的基本設定。



可用設定說明如下：

項目	說明
啟用(Enable)	切換開關以啟用/停用此設定。
OpenVPN 伺服器設置(OpenVPN Server Setup)	
啟用 UDP (UDP Enabled)	切換開關以啟用/停用 OpenVPN 連線的 UDP 協定。 **UDP 埠號(UDP Port)** - 輸入 UDP 連接埠號碼。
啟用 TCP (TCP Enabled)	切換開關以啟用/停用 OpenVPN 連線的 TCP 協定。 **TCP 埠號(TCP Port)** -輸入 TCP 連接埠號碼。
密碼演算法(Cipher Algorithm)	選擇所需的加密演算法。 AES256 比 AES128 更安全，但計算開銷更高，效能可能更低。
HMAC 演算法(HMAC	HMAC 代表基於雜湊的訊息認證碼，用於驗證 VPN 資料的完整性和真實

Algorithm)	性。 選擇所需的 HMAC 哈希演算法。支援三種雜湊演算法：SHA1、SHA256 和 SHA512。建議使用 SHA512，因為它比 SHA1 更強大、更可靠。
憑證驗證(Certificate Authentication)	如果您想驗證用戶端憑證是否由受信任的 CA 頒發，請將此開關切換為啟用狀態。
憑證來源(Certificate Source)	選擇用於 OpenVPN 的憑證來源。 **從現有憑證中選擇(Select from Existing Certificates)** – OpenVPN 將使用第三方憑證。 **路由器產生憑證(Router Generate Certificates)** – 用於 OpenVPN 的路由器產生的憑證。
伺服器 CA (Server CA)	使用下拉清單選擇已上傳至路由器的信任 CA 憑證。 若要將更多受信任的 CA 憑證上傳到路由器，請前往憑證設定>>憑證(Certificate Configuration>>Certificates)頁面，然後按一下受信任的 CA 標籤以取得更多憑證。
伺服器驗證(Server Certificate)	使用下拉清單選擇已上傳到路由器的伺服器憑證。 若要上傳更多本機證書，請前往設定>>憑證(Configuration>>Certificates)頁面，然後按一下本機憑證標籤以取得更多憑證。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-4-1-6 L2TP

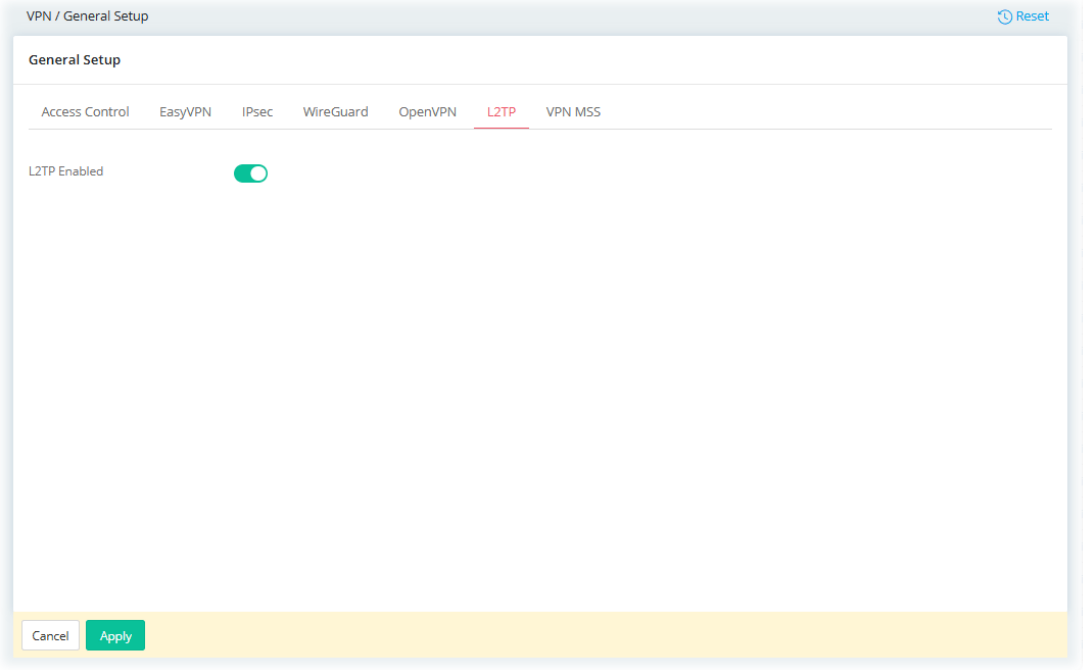
為了建立安全加密的資料傳輸通道，此選項將結合使用 L2TP 和 IPsec 加密。

When this option is enabled, the device supports:

當啟用此選項時，本裝置即支援：

- 使用 L2TP over IPsec 的 VPN 站點撥入連線
- 使用 L2TP over IPsec 的遠端工作者 VPN 連線

允許遠端使用者或分公司使用標準的 L2TP/IPsec 連線安全地連接到 VPN 閘道。

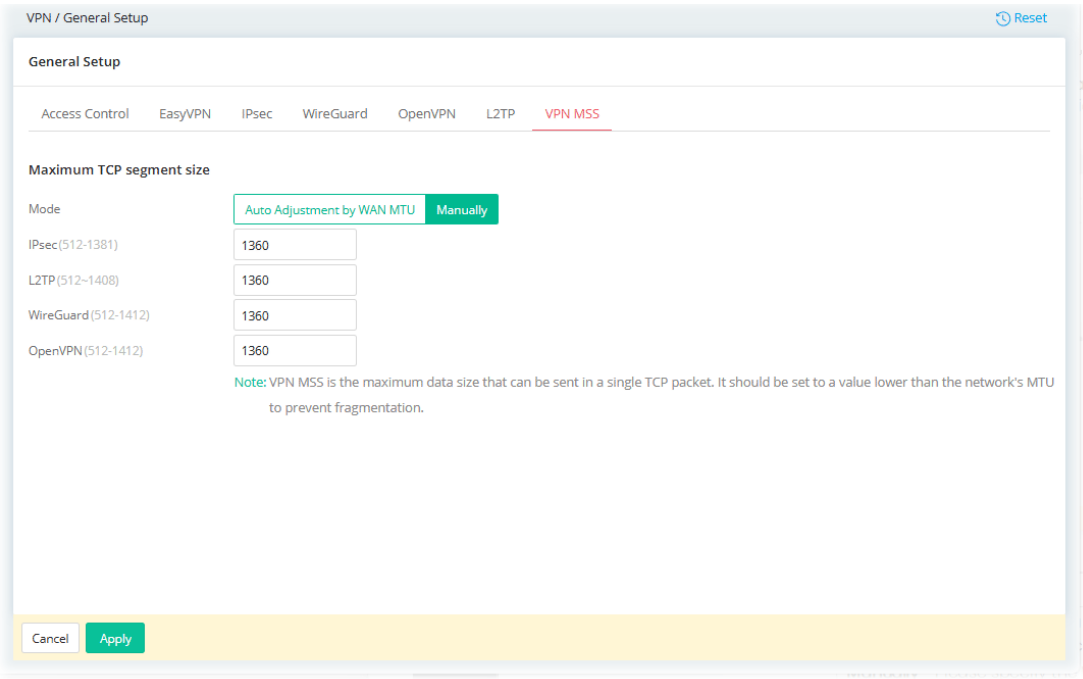


切換開關以啟用/停用 L2TP VPN 連線。按下**套用(Apply)**可儲存設定。

II-4-1-7 VPN MSS 設定

MSS 是 Maximum TCP segment size（最大 TCP 段大小）的縮寫。

此頁面用於自動調整 VPN 通道內的 TCP MSS 值。它優化資料封包大小，防止資料封包分片，並確保網路資料傳輸有效率地進行。



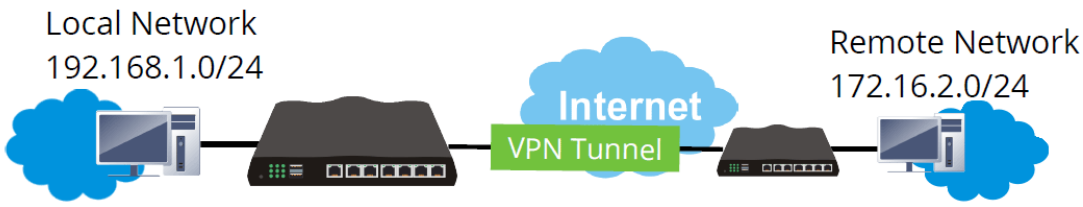
可用設定說明如下：

項目	說明
模式(Mode)	**透過 WAN MTU 自動調整(Auto Adjustment by WAN MTU)** – 根據 WAN MTU 自動調整 MSS 值，可獲得 MSS 值。 **手動(Manually)** - 為每種類型指定 MSS 值，以避免在透過 VPN 連線進行資料傳輸期間資料封包被 MTU 截斷。 • **IPsec** • **WireGuard** • **OpenVPN**
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

II-4-2 站點對站點 VPN (Site-to-Site VPN)

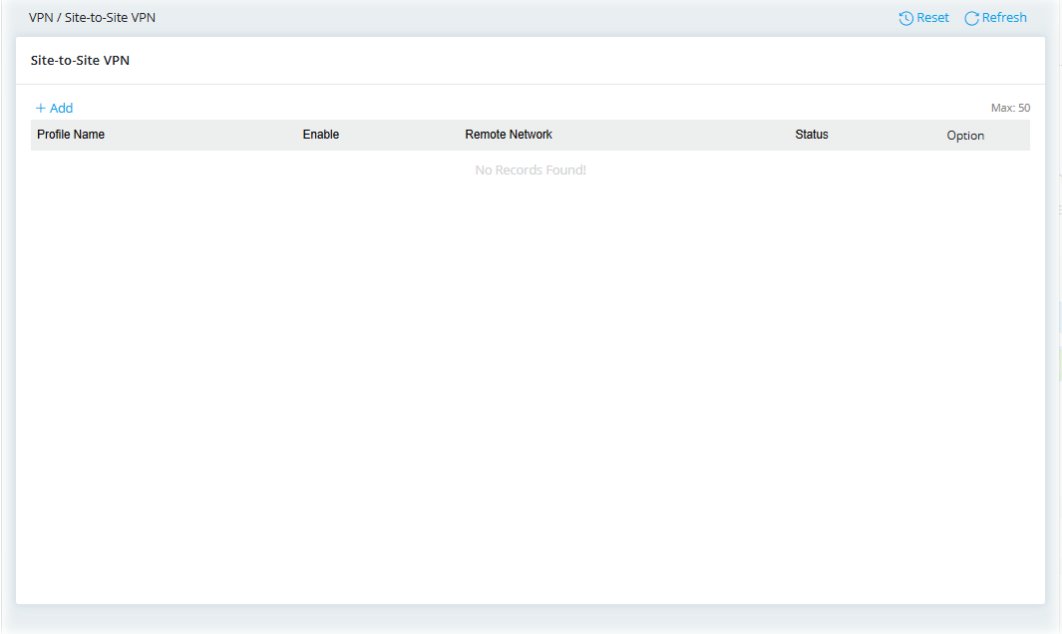
VPN 指的是兩個路由器區域網路之間的連線。

- 允許分公司和總部員工共享相同的網路資源。



- 設定 VPN 伺服器以接收來自其他路由器的傳入連線。

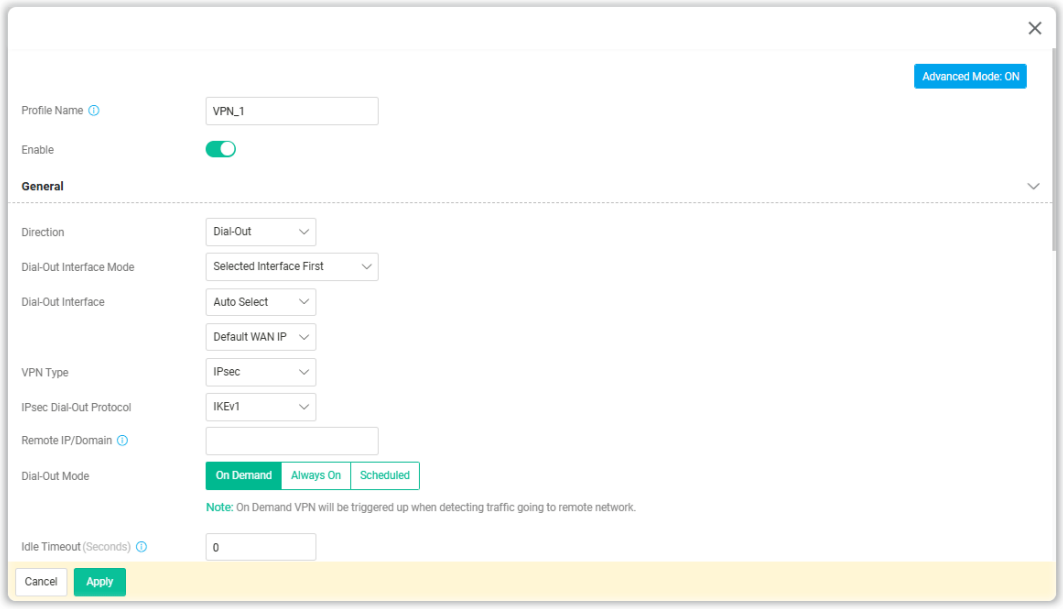
站點對站點 VPN 頁面允許設定 VPN 伺服器，以接收來自其他路由器的傳入連線。



II-4-2-1 VPN 類型 - IPsec

IPsec(網際網路協定安全)對網路流量進行加密和驗證，確保透過 VPN 進行安全資料傳輸。它可以防止未經授權的存取、資料篡改和竊聽，使其成為遠端辦公、站點間連接和遠端辦公人員連接的理想選擇，同時還能保護在不受信任的網路上傳輸的敏感資訊。

若要新增新的資源設定檔(IPsec VPN 類型)，請開啟 VPN >>站點對站點 VPN(VPN>>Site-to-Site VPN)並按一下**+新增**。



可用設定說明如下：

項目	說明
進階模式:開啟/關閉 (Advanced Mode:ON/OFF)	按此顯示或隱藏站點對站點 VPN(site-to-site VPN)的進階設定
設定檔名稱(Profile Name)	輸入設定檔名稱，以供辨識。
啟用(Enable)	切換開關以啟用/停用此設定。
基本(General)	
方向(Direction)	指定此 VPN 設定檔的允許撥號方向。 **二者(Both)** – 此設定檔用於發起（撥出）或接受（撥入）連線。 **撥出(Dial-Out)** – 設定檔用於發起對外連線。 **撥入(Dial-In)** – 此設定檔用於接受傳入連線。 **VPN 比對機制(VPN Matcher)**– 此 VPN 比對機制技術基於標準的 WireGuard VPN 協定。 VPN 比對伺服器可以幫助位於 NAT 後面的兩台 Draytek 路由器建立安全的 VPN 通道道，用於彼此之間的資料傳輸。請注意，只有支援 WireGuard 的 drayos4 型號才能透過比對與 Vigor2928 建立 VPN 連線。
VPN 類型(VPN Type)	選擇用於建立 VPN 連線的 VPN 類型。 **方向設定為撥出時** – 可用選項包含： • IPsec • OpenVPN • WireGuard **方向設定為撥入時** – 可用選項包含： • IPsec • OpenVPN • WireGuard • L2TP **方向設定為二者時** – 可用選項包含： • IPsec

	• OpenVPN **方向設定為 VPN 比對機制**– 可用選項包含： • WireGuard 與 IPsec VPN 類型相關的其他選項將根據所使用的方向而變更。 **IPsec (方向設定為二者/撥入時)** -可用選項包含： • **IPsec 撥入通訊協定(IPsec Dial-In Protocol)** • **撥入允許排程(Dial-in Allowed Schedule)** **IPsec (方向設定為二者/撥出時)** -可用選項包含： • **IPsec 撥出通訊協定(IPsec Dial-Out Protocol)** • **遠端 IP/網域(Remote IP/ Domain)** • **撥出模式(Dial-Out Mode)**
IPsec 撥入通訊協定 (IPsec Dial-In Protocol)	選擇通訊協定以透過網際網路觸發 IPsec VPN 連線。 • IKEv1/v2 • XAuth.
IPsec 撥出通訊協定 (IPsec Dial-Out Protocol)	選擇通訊協定以透過網際網路觸發 IPsec VPN 連線。 • IKEv1 • IKEv2 • IKEv2 EAP • XAuth
遠端 IP/網域 (Remote IP/ Domain)	輸入遠端 VPN 伺服器之 IPv4 位址或是主機名稱。
撥出模式(Dial-Out Mode)	**需要時(On Demand)** – 當偵測到發送到遠端網路的流量時，將觸發 VPN 連線。 **永遠連線(Always On)** – 選擇此項可使撥號連線始終維持連線。 **排程(Scheduled)** – 選擇此選項可依照排程建立 VPN 連線。 • **當排程為強迫時，中斷目前的通道(Drop the Active Tunnel when Schedule is Enforced)** – 切換開關以啟用/停用此功能。 • **VPN 排程(VPN Schedule)** – 用下拉式選單指定一個 VPN 設定檔。在設定 VPN 排程之前，請先在設定>>物件>>排程(Configuration>> Objects>> Schedule)中新增所需的時間間隔。
撥入允許排程(Dial-In Allowed Schedule)	依照預設的時程安排進行連接和中斷連接。 **永遠允許(Always Allow)** – 選擇此選項可保持始終連線。 **排程(Scheduled)** – 選擇此選項可依照排程建立 VPN 連線。 • **當排程為強迫時，中斷目前的通道(Drop the Active Tunnel when Schedule is Enforced)** –切換開關以啟用/停用此功能。 • **VPN 排程(VPN Schedule)** – 用下拉式選單指定一個 VPN 設定檔。在設定 VPN 排程之前，請先在設定>>物件>>排程(Configuration>> Objects>> Schedule)中新增所需的時間間隔。
使用者名稱與密碼(Username and Password)	
使用者名稱(Username)	當選擇 XAuth 作為 IPsec 撥入/撥出協定時，即可用此功能。 用於遠端區域網路建立 VPN 連線。
密碼(Password)	當選擇 XAuth 作為 IPsec 撥入/撥出協定時，即可用此功能。 用於遠端區域網路建立 VPN 連線。
撥出/二者之 IKE 驗證(IKE Authentication for Dial-Out/Both)	
撥出設定(Dial-Out	當方向選擇撥出(Dial-Out)且 VPN 類型選擇了 **IPsec** 時，可用此功能。

Settings)	
協商(Negotiation)	當 IPsec 撥出通訊協定(IPsec Dial-Out Protocol)選擇了 IKEv1 時，可用此功能。 選擇**主要(Main)**模式或**積極(Aggressive)**模式。最終目標是交換安全方案以建立受保護的安全通道。Vigor 路由器的預設值為主要模式。 **主要模式(Main Mode) / 積極模式(Aggressive Mode) – 主要的**模式比**積極**模式安全，因為有更多的資料交換是在安全通道中進行，以建立 IPsec 連線數。然而，**積極**模式速度更快。 ● **預先共享金鑰(Pre-Shared Key)** – 輸入預先共享金鑰中的字元。
驗證(Authentication)	當選擇了 **IKEv1 (在主要模式下)**或是 **IKEv2** 時，可用此功能。 **預先共享金鑰(Pre-Shared Key)** – 選擇作為身份驗證方法。 ● **預先共享金鑰(Pre-Shared Key)** – 輸入預先共享金鑰中的字元。 **憑證(Certificate)** – 選擇作為身份驗證方法。 ● **本機憑證(Local Certificate)** – 選擇設定>>憑證>>本機憑證(Configuration>>Certificates>> Local Certificates)中的設定檔其中之一。 ● **本機 ID (Local ID)** – 選擇主體名稱或主體替代名稱。 ● **對方 ID (Peer ID)** – 輸入下述需要的資訊。 **選擇接受主體替代名稱(Select Accept Subject Alternative Name)** -下述三種對方 ID 格式均可接受，包括 IP 位址、網域名稱和電子郵件。 **對方憑證(Peer Certificate)** - 選擇已預先取得並儲存於設定>>憑證>>本機憑證(Configuration >> Certificates >> Local Certificates)中的對方憑證。 **接受主體名稱(Accept Subject Name)** – 請輸入完整的憑證主體名稱。 **接受任一(Accept Any)** -設定>>憑證>>受信任的 CA(Configuration >> Certificates >> Trusted CA)中，由受信任的 CA 簽署的任何憑證都將被視為有效。
IKE 識別碼(IKE Identifier)	設定用於識別的本機 ID 和對等方 ID。 對於某些需要指定 ID 的連接，例如使用積極模式(Aggressive)的 IKEv1 和 IKEv2(選項功能)，會提供本地 ID 和對方 ID。
本機 ID (Local ID)	指定使用 IPsec VPN 類型建立 VPN 連線時要使用的本機 ID。
對方 ID(Peer ID)	請輸入遠端客戶端的 ID 名稱。 如果指定了相關數值，則系統只會接受來自指定 IP 位址和/或具有指定對等 ID 的連線。
撥入/二者之 IKE 驗證(IKE Authentication for Dial-In/Both)	
撥入設定(Dial-In Settings)	當方向選擇撥入(**Dial-In**)且 VPN 類型選擇了 **IPsec** 時，可用此功能。
協商(Negotiation)	選擇**主要(Main)**模式或**積極(Aggressive)**模式。最終目標是交換安全方案以建立受保護的安全通道。Vigor 路由器的預設值為主要模式。 **主要模式(Main Mode) / 積極模式(Aggressive Mode)–主要的**模式比**積極**模式安全，因為有更多的資料交換是在安全通道中進行，以建立 IPsec 連線數。然而，**積極**模式速度更快。
指定對方 VPN (Specify VPN Peer)	當 IPsec 撥號協定選擇 IKEv1/v2 時，可用此功能。 此功能可以限制 IPsec 只能由指定的對方 IP 位址或網域名稱發起，並指定要使用的虛擬金鑰。 如果啟用了，則設定 **遠端 IP/網域(Remote IP/Domain)** – 輸入遠端對等方的 IP 位址。

	預先共享金鑰(Pre-Shared Key) – 輸入字元以預先共用金鑰進行身份驗證。
X509 數位簽章(X.509 Digital Signature)	當 IPsec 撥號協定選擇了 IKEv1/v2 時，可使用此功能。 若要使用 X.509 數位簽章，請選擇一種身份驗證方法，並輸入該方法所需的資訊。 **選擇接受主體替代名稱(Select Accept Subject Alternative Name)** - 下述三種對方 ID 格式均可接受，包括 IP 位址、網域名稱和電子郵件。 **對方憑證(Peer Certificate)** - 選擇已預先取得並儲存於設定>>憑證>>本機憑證(Configuration >> Certificates >> Local Certificates)中的對方憑證。 **接受主體名稱(Accept Subject Name)** – 請輸入完整的憑證主體名稱。 **接受任一(Accept Any)** - 設定>>憑證>>受信任的 CA(Configuration >> Certificates >> Trusted CA)中，由受信任的 CA 簽署的任何憑證都將被視為有效。
IKE 識別碼(IKE Identifier)	設定用於識別的本機 ID 和對等方 ID。 對於某些需要指定 ID 的連接，例如使用積極模式(Aggressive)的 IKEv1 和 IKEv2(選項功能)，會提供本地 ID 和對方 ID。
本機 ID (Local ID)	指定使用 IPsec VPN 類型建立 VPN 連線時要使用的本機 ID。
對方 ID(Peer ID)	請輸入遠端客戶端的 ID 名稱。 如果指定了相關數值，則系統只會接受來自指定 IP 位址和/或具有指定對等 ID 的連線。
更多 IKE 驗證(IKE Authentication)設定	
IKE Phase 1	**加密(Encryption)** – 使用自動/AES/3DES/DES 加密演算法，並套用 MD5 或 SHA-1 認證演算法。 **群組(Group)** – 指定一個密鑰交換方案。 **驗證(Authentication)** – 選擇 SHA256 或 SHA1 進行資料封包認證。 **有效時間(Lifetime)** - 基於安全考量，密鑰的有效期限必須定義清楚。預設值為 28800 秒。您可設定的秒數範圍為 900 秒到 86400 秒。
強迫 UDP 封裝(Force UDP Encapsulation)	切換開關即可啟用/停用此功能。 如果啟用，所有 IPsec 封包都將封裝 UDP 封包標頭。
強制重新驗證(Force Reauthentication)	切換開關即可啟用/停用此功能。 如果啟用此選項，則在更新 IPsec 連線數時，將重新驗證雙方的身分。
IKE Phase 2	指定安全通訊協定、提案加密和提案認證方式。 **安全性通訊協定(Security Protocol)** – AH(中)表示資料將進行身份驗證，但不會被加密。預設情況下，此選項處於啟用狀態。 ESP(高)表示有效載荷(資料)將被進行加密和身份驗證。 **加密(Encryption)** – 使用 AES/3DES/DES 加密演算法。 **驗證(Authentication)** – 選擇全部、SHA256 或 SHA1 進行資料封包認證。 **有效時間(Lifetime)** – 基於安全考量，密鑰的有效期限必須定義清楚。預設值為 3600 秒。您可設定的秒數範圍為 600 秒到 28800 秒。 **完美前向保密 PFS (Perfect Forward Secret)** – 切換開關以啟用/停用此功能。 PFS 會在第二階段週期性換鍵期間強制執行金鑰交換。
階段 2 網路 ID (Phase 2 Network ID)	將 VPN 流量的來源 IP 位址變更為在網路欄位中所選的 NAT 模式之指定 IP 位址。
Dead Peer Detection	DPD 是偵測 IPsec 連線的方法。 **DPD 延遲(DPD Delay)** – 這是一個保持連線定時器。當通道處於空閒狀態時，系統會定期發送 Hello 訊息。當數值設定為 0 時，可停用此功能。如

	果啟用，建議值設定為 30 秒。 **DPD 逾時(DPD Timeout)** - 這是逾時計時器。如果在逾時時間後仍未收到確認訊息，則對等方將被判定為失效。當數值設定為 0 時，可停用此功能。如果啟用此功能，建議值設定為 120 秒。
網路(Network)	
網路(Network)	指定允許本地子網和遠端子網的流量透過 VPN 連線。 **本機網路(Local Network)** – 預設值為 0.0.0.0，這表示 Vigor 路由器將在 IPCP 協商階段從遠端路由器取得 PPP IP 位址。如果遠端的 PPP IP 位址是固定的，請在此指定該固定 IP 位址。如果您不選擇 PPTP 或 L2TP，那麼請勿變更預設值。 **子網遮罩(Subnet Mask)** – 顯示本機網路的 TCP/IP 設定 IP 位址和子網路遮罩。請選擇符合本機網路要求的選項。 **遠端網路(Remote Network)** – 預設值為 0.0.0.0，這表示 Vigor 路由器將在 IPCP 協商階段從遠端路由器取得遠端閘道 PPP IP 位址。如果遠端的 PPP IP 位址是固定的，請在此指定該固定 IP 位址。如果您不選擇 PPTP 或 L2TP，那麼請勿變更預設值。 **子網遮罩(Subnet Mask)** - 選擇符合本機網路要求的選項。此功能用來新增一條固定路由，將所有發送到此遠端網路 IP 位址/遠端網路遮罩的流量皆透過 VPN 連線進行。針對 IPsec 而言，這是第二階段快速模式的目地用戶端 ID。
路由/NAT 模式 (Routing/NAT Mode)	**路由模式(Routing Mode)** – 支援標準的站點到站點 VPN，流量可以直接在兩個網路之間路由，而無需更改來源 IP 位址。 **NAT 模式(NAT Mode)** – 修改發送到遠端站台的 VPN 流量，將來源 IP 位址轉換為虛擬 IP 位址，然後再將其傳送至目地位置。
更多遠端子網(More Remote Subnets)	新增更多固定路由，因應發送到遠端網路的子網路之用。 **停用(Disabled)** – 停用此功能。 **多重 SA (Multiple SAs)** – 多重安全關聯 (SA) 將基於本機網路和遠端網路建立不同的第二階段安全關聯，以提供額外的資料傳輸安全性。選擇此項以便新增路由。 • **+新增(+Add)** – 按此新增固定路由。輸入本機網路、子網路遮罩、遠端網路和子網路遮罩等必要資訊。
進階模式下更多的選項	
撥出介面模式(Dial-Out Interface Mode)	選擇使用此設定檔建立連線的 WAN 連線。此設定僅適用於撥出連線。 **優先選擇介面(Selected Interface First)** – 連線時，路由器會先使用選定的 WAN 介面進行 VPN 連線。如果選定的 WAN 介面連線失敗，路由器會嘗試使用其他 WAN 介面。 **限用選定介面(Selected Interface Only)** – 連線時，路由器將使用選定的 WAN 作為 VPN 連線的唯一介面。 **手動(Manual)** – 自行定義 VPN 設定。指定哪些 WAN 可用作對外連線介面。
撥出介面(Dial-Out Interface)	當此 VPN 設定檔的撥號方向設定為撥出時，可用此功能。 **自動選擇(Auto Select)** – 依照預設路由決定要撥出的介面。 **預設 WAN IP/IP 位址(Default WAN IP / IP Address)** – 用下拉清單為此 VPN 設定檔指定一個 WAN IP 位址。
閒置逾時(Idle Timeout)	如果在空閒逾時時間內未偵測到任何流量，隧道將斷開連線。將值設為 0 可停用此功能。
GRE Over IPsec	切換開關即可啟用/停用此功能。 設定好 IPsec 撥號輸出設定後，此功能將先驗證資料並透過 GRE over IPsec 加密資料封包後傳輸。通訊雙方必須設定相同的虛擬 IP 位址才能確

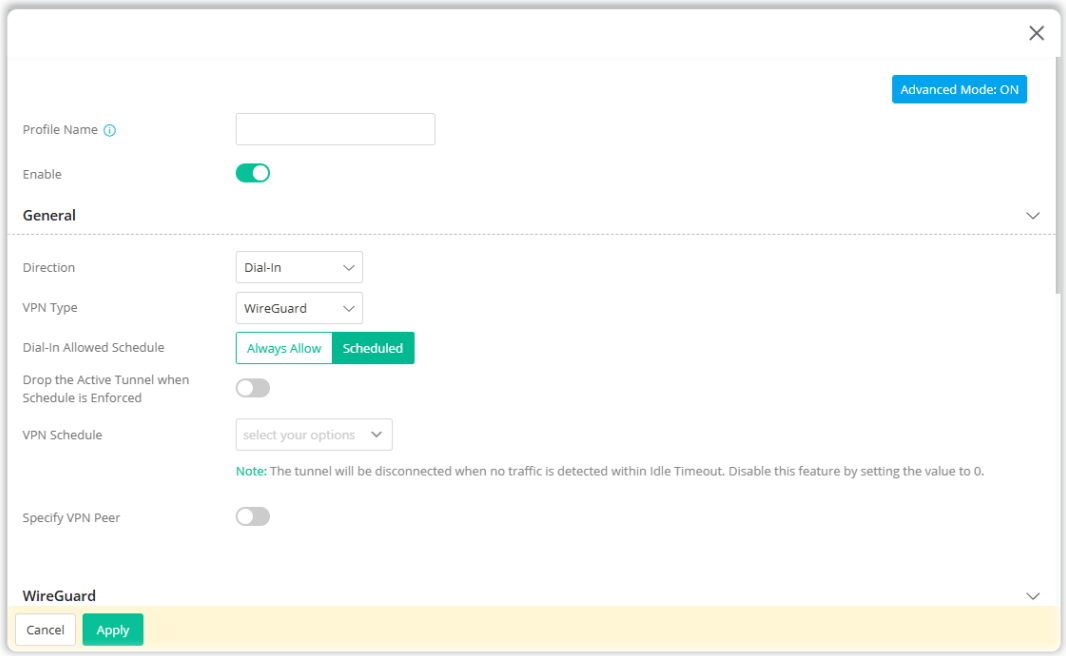
	保通訊的一致性。 **GRE 本機 IP (GRE Local IP)** – 輸入路由器本身的虛擬 IP 位址，以便對等方進行驗證。 **GRE 遠端 IP(GRE Remote IP)** - 輸入待路由器驗證的對等主機的虛擬 IP 位址。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-4-2-2 VPN 類型 - WireGuard

WireGuard 是一種安全、快速且現代的開源 VPN 協定。此 VPN 連線可以透過在 VPN 伺服器（例如 Vigor 路由器）和 VPN 用戶端（例如 WireGuard VPN 用戶端）之間交換虛擬金鑰和公開金鑰來建立 VPN 連線。

若要新增新的資源設定檔（WireGuard VPN 類型），請開啟 VPN >> 網站到網站 VPN 並按一下**+新增(+Add)**。



可用設定說明如下：

項目	說明
進階模式:開啟/關閉(Advanced Mode:ON/OFF)	按此顯示或隱藏站點對站點 VPN(site-to-site VPN)的進階設定。
設定檔名稱(Profile Name)	輸入設定檔名稱，以供識別。
啟用(Enable)	切換開關以啟用/停用此設定。
基本(General)	
方向(Direction)	指定此 WireGuard VPN 設定檔的允許撥號方向。 **撥出(Dial-Out)** – 設定檔用於發起對外連線。 **撥入(Dial-In)** – 此設定檔用於接受傳入連線。 **VPN 比對機制(VPN Matcher)**– 此 VPN 比對機制技術基於標準的 WireGuard VPN 協定。 VPN 比對伺服器可以幫助位於 NAT 後面的兩台 Draytek 路由器建立安全的 VPN 通道道，用於彼此之間的資料傳輸。請注意，只有支援 WireGuard 的 drayos4 型號才能透過比對與 Vigor2928 建立 VPN 連線。
VPN 類型(VPN Type)	選擇用於建立 WireGuard VPN 連線的 VPN 類型。 **WireGuard (方向設定為撥入時)** -可用選項包含： ● **撥入允許排程(Dial-in Allowed Schedule)** ● **指定對方 VPN(Specify VPN Peer)** **WireGuard (方向設定為撥出時)** -可用選項包含：

	• **遠端 IP/網域(Remote IP/ Domain)** • **伺服器埠號(Server Port)** • **撥出模式(Dial-Out Mode)** **WireGuard (方向設定為 VPN Matcher)** –可用選項包含： • **裝置(Device**) • **遠端 IP/網域(Remote IP/ Domain)** • **伺服器埠號(Server Port)** • **撥出模式(Dial-Out Mode)**
撥入允許排程(Dial-In Allowed Schedule)	依照預設的時程安排進行連接和中斷連接。 **永遠允許(Always Allow)** – 選擇此選項可保持始終連線。 **排程(Scheduled)** – 選擇此選項可依照排程建立 VPN 連線。 • **當排程為強迫時，中斷目前的通道(Drop the Active Tunnel when Schedule is Enforced)** –切換開關以啟用/停用此功能。 • **VPN 排程(VPN Schedule)** – 用下拉式選單指定一個 VPN 設定檔。在設定 VPN 排程之前，請先在設定>>物件>>排程(Configuration>> Objects>> Schedule)中新增所需的時間間隔。
指定對方 VPN(Specify VPN Peer)	切換開關以啟用/停用遠端客戶端的安全機制。 • **遠端 IP/網域(Remote IP/ Domain)** – 如果啟用了**指定對方 VPN(Specify VPN Peer)**，請輸入遠端對方的 IP 位址/網域名稱。
伺服器埠號(Server Port)	設定 VPN 伺服器的連接埠號碼。
撥出模式(Dial-Out Mode)	**需要時(On Demand)** – 當偵測到發送到遠端網路的流量時，將觸發 VPN 連線。 **永遠連線(Always On)** – 選擇此項可使撥號連線始終維持連線。 **排程(Scheduled)** – 選擇此選項可依照排程建立 VPN 連線。 • **當排程為強迫時，中斷目前的通道(Drop the Active Tunnel when Schedule is Enforced)** – 切換開關以啟用/停用此功能。 • **VPN 排程(VPN Schedule)** – 用下拉式選單指定一個 VPN 設定檔。在設定 VPN 排程之前，請先在設定>>物件>>排程(Configuration>> Objects>> Schedule)中新增所需的時間間隔。
裝置(Device)	DrayTek VPN 路由器註冊到同一個 DrayTek VPN 比對機制帳戶後，可以相互定位，在兩台路由器之間建立安全的端對端加密 VPN 通道。 此欄位僅顯示已註冊至 DrayTek 比對機制伺服器的裝置。請選擇要與此 Vigor 路由器建立 VPN 連線的裝置。
	WireGuard
介面(Interface)	在以下情況下使用：方向選擇**撥出**和 VPN 類型選擇 **Wireguard**。 **虛擬金鑰(Private Key)** – 顯示按下**產生(Generate)**按鈕所製作的虛擬金鑰。 **產生虛擬金鑰(Generate Private Key)** – 按下**產生(Generate)**按鈕產生金鑰組(包括虛擬金鑰和公開金鑰)。 **公開金鑰(Public Key)** - 顯示按下**產生(Generate)**按鈕所製作的公開金鑰。
對方(Peer)	設定對等方。 在以下情況下使用：方向選擇**撥出/撥入**和 VPN 類型選擇 **Wireguard**。 **公開金鑰(Public Key)** - 輸入對等 VPN 伺服器的公開金鑰。 **預先共享金鑰(Pre-Shared Key)** - 顯示按下**產生預先共享金鑰(Generate PSK)**按鈕後產生的虛擬金鑰內容。 **產生預先共享金鑰(Generate PSK)** - 按下此鈕以產生金鑰。 **針對 NAT 用戶端位址(For NAT Client Address (選項功能))** – 僅限撥入。輸入遠端對等方的 IP 位址。

	維持連線(Keepalive) - 預設值為 60 秒。
	網路(Network)
網路(Network)	指定允許本地子網和遠端子網的流量透過 **WireGuard** VPN 連線。 **本機網路(Local Network)** – 定義屬於本機網路的 IP 位址範圍，此範圍用於透過 VPN 路由流量。 **子網遮罩(Subnet Mask)** – 子網路遮罩有助於定義本地網路的大小，並告訴 VPN 如何解釋 IP 位址中的網路部分。子網路遮罩為 255.255.255.0(或 CIDR 表示法中的 /24)表示 IP 位址的前 24 位元用於路，其餘 8 位元用於本地網路中的主機(裝置)。 **遠端網路(Remote Network)** – 定義您要連接的遠端網路的 IP 位址範圍。例如，如果遠端網路是 10.0.0.0/24，則您是在告訴 VPN 遠端網路的 IP 位址範圍是 10.0.0.1 到 10.0.0.254。 **子網遮罩(Subnet Mask)** – 與本機網路類似，遠端網路的子網路遮罩決定了遠端網路 IP 位址範圍的劃分方式。若遠端網路的子網路遮罩為 255.255.255.0（或 /24），則表示遠端網路有 254 個可供裝置使用的位址。
路由/NAT 模式 (Routing/NAT Mode)	當方向選擇**撥入(Dial-In)**時，只能選擇路由模式。遠端網路僅允許本機網路使用一個 IP 位址。 當方向選擇**撥出/二者/VPN 比對機制(Dial-Out/Both/VPN Matcher)**： 如果遠端網路只允許本機網路使用一個 IP 位址，請選擇 NAT；否則，請選擇路由。 **路由(Routing)** – 支援標準的站點到站點 VPN，流量可以直接在兩個網路之間路由，而無需更改來源 IP 位址。 • **內部網路位址轉換(Translate Local Network)** – 要建立雙邊 VPN 連接，本機子網路和遠端子網路不能相同。如果碰巧相同，則需要進行 IP 位址轉換（例如，如果雙方都使用 192.168.1.10，則需要將其中一個轉換為 192.168.2.10 才能啟用雙邊 VPN 連線）。 • **已轉換之網路(Translated Network)** – 指定 IPv4 位址。 **NAT** – 修改發送到遠端站點的 VPN 流量，將來源 IP 位址轉換為虛擬 IP 位址，然後再將其傳送到目地位置。
更多子網(More Subnets)	新增更多固定路由，可用於發送到遠端網路的子網路上。 **停用(Disabled)** – 停用此功能。 • **新增(+Add)** – 按此新增新的固定路由。輸入遠端網路和子網路遮罩所需的資訊。
進階模式下的選項	
撥出介面模式(Dial-Out Interface Mode)	選擇使用此設定檔建立連線的 WAN 連線。此設定僅適用於撥出連線。 **優先選擇介面(Selected Interface First)** – 連線時，路由器會先使用選定的 WAN 介面進行 VPN 連線。如果選定的 WAN 介面連線失敗，路由器會嘗試使用其他 WAN 介面。 **限用選定介面(Selected Interface Only)** – 連線時，路由器將使用選定的 WAN 作為 VPN 連線的唯一介面。 **手動(Manual)** – 自行定義 VPN 設定。指定哪些 WAN 可用作對外連線介面。
撥出介面(Dial-Out Interface)	當此 VPN 設定檔的撥號方向設定為撥出時，可用此功能。 **自動選擇(Auto Select)** – 依照預設路由決定要撥出的介面。 **預設 WAN IP/IP 位址(Default WAN IP / IP Address)** – 用下拉清單為此 VPN 設定檔指定一個 WAN IP 位址。
閒置逾時(Idle Timeout)	如果在空閒逾時時間內未偵測到任何流量，隧道將斷開連線。將值設為 0 可停用此功能。

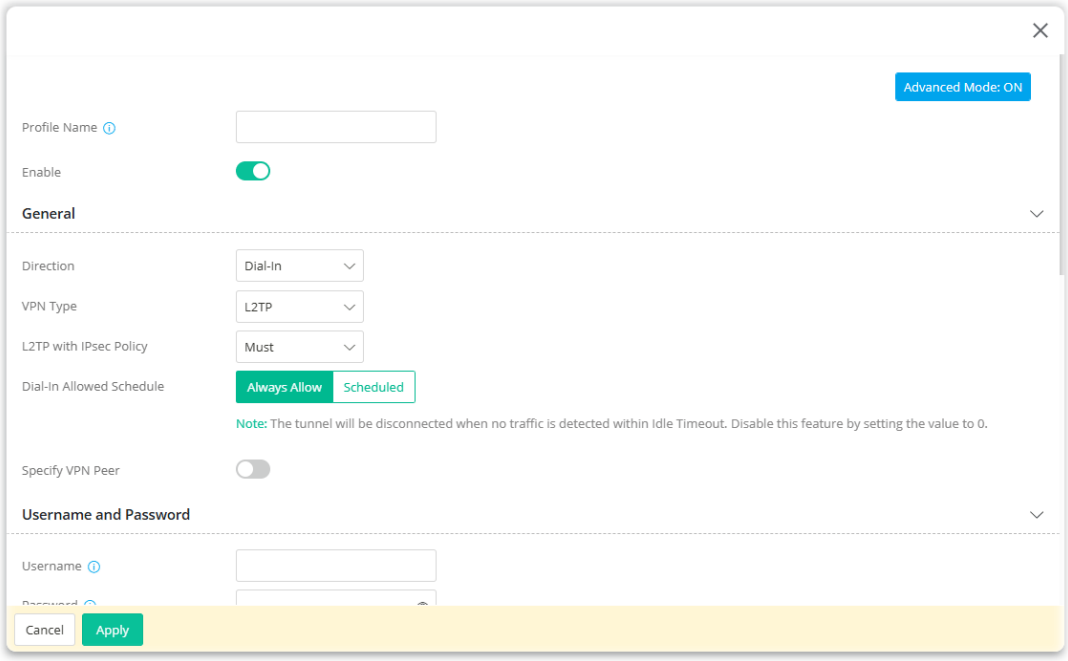
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-4-2-3 VPN 類型 – L2TP

L2TP 使用強制性的 IPsec 加密來建立安全的 VPN 通道。為確保資料完整性和機密性，此連線類型不支援 IPsec 加密的 L2TP。

若要新增新的資源設定檔（L2TP VPN 類型），請開啟 VPN>>站點對站點 VPN (VPN>>Site-to-Site VPN)，然後按一下**+新增(+Add)**。



可用設定說明如下：

項目	說明
進階模式:開啟/關閉 (Advanced Mode:ON/OFF)	按此顯示或隱藏站點對站點 VPN(site-to-site VPN)的進階設定。
設定檔名稱(Profile Name)	輸入設定檔名稱，以供識別。
啟用(Enable)	切換開關以啟用/停用此設定。
基本(General)	
方向(Direction)	指定此 L2TP 設定檔的允許撥號方向。 **撥入(Dial-In)** – 此設定檔用於接受傳入連線。
VPN 類型(VPN Type)	選擇 **L2TP**。
含 IPsec 策略之 L2TP (L2TP with IPsec Policy)	對於這種連線類型，必須使用 L2TP 和 IPsec 加密，以確保資料完整性和機密性。 **必須(Must)** - 指定要對 L2TP 連線套用的 IPsec 策略。
撥入允許排程(Dial-In Allowed Schedule)	依照預設的時程安排進行連接和中斷連接。

	永遠允許(Always Allow) – 選擇此選項可保持始終連線。 **排程(Scheduled)** – 選擇此選項可依照排程建立 VPN 連線。 ● **當排程為強迫時，中斷目前的通道(Drop the Active Tunnel when Schedule is Enforced)** –切換開關以啟用/停用此功能。 ● **VPN 排程(VPN Schedule)** – 用下拉式選單指定一個 VPN 設定檔。在設定 VPN 排程之前，請先在設定>>物件>>排程(Configuration>> Objects>> Schedule)中新增所需的時間間隔。
指定對方 VPN(Specify VPN Peer)	切換開關以啟用/停用遠端客戶端的安全機制。 ● **遠端 IP/網域(Remote IP/ Domain)** – 如果啟用了**指定對方 VPN(Specify VPN Peer)**，請輸入遠端對方的 IP 位址/網域名稱。
使用者名稱與密碼(Username and Password)	
使用者名稱(Username) **密碼(Password)**	**使用者名稱(Username)** – 用於遠端區域網路建立 VPN 連線。 **密碼(Password)** – 用於遠端區域網路建立 VPN 連線。
IKE 驗證(IKE Authentication)	
協商(Negotiation)	選擇**主要(Main)**或**積極(Aggressive)**模式。最終目標是交換安全方案，以建立受保護的安全通道。 Vigor 路由器的預設值為**要(Main)**模式。 選擇**主要(Main)**模式或**積極(Aggressive)**模式。最終目標是交換安全方案以建立受保護的安全通道。Vigor 路由器的預設值為主要模式。 **主要模式(Main Mode) / 積極模式(Aggressive Mode)** – **主要的**模式比**積極**模式安全，因為有更多的資料交換是在安全通道中進行，以建立 IPsec 連線數。然而，**積極**模式速度更快。
指定對方 VPN (Specify VPN Peer)	當 IPsec 撥號協定選擇 IKEv1/v2 時，可用此功能。 此功能可以限制 IPsec 只能由指定的對方 IP 位址或網域名稱發起，並指定要使用的虛擬金鑰。 如果啟用了，則設定 **遠端 IP/網域(Remote IP/Domain)** – 輸入遠端對等方的 IP 位址。 **預先共享金鑰(Pre-Shared Key)** – 輸入字元以預先共用金鑰進行身份驗證。
X509 數位簽章(X.509 Digital Signature)	當 IPsec 撥號協定選擇了 IKEv1/v2 時，可使用此功能。 若要使用 X.509 數位簽章，請選擇一種身份驗證方法，並輸入該方法所需的資訊。 **選擇接受主體替代名稱(Select Accept Subject Alternative Name)** - 下述三種對方 ID 格式均可接受，包括 IP 位址、網域名稱和電子郵件。 **對方憑證(Peer Certificate)** - 選擇已預先取得並儲存於設定>>憑證>>本機憑證(Configuration >> Certificates >> Local Certificates)中的對方憑證。 **接受主體名稱(Accept Subject Name)** – 請輸入完整的憑證主體名稱。 **接受任一(Accept Any)** - 設定>>憑證>>受信任的 CA(Configuration >> Certificates >> Trusted CA)中，由受信任的 CA 簽署的任何憑證都將被視為有效。
IKE 識別碼(IKE Identifier)	設定用於識別的本機 ID 和對等方 ID。 對於某些需要指定 ID 的連接，例如使用積極模式(Aggressive)的 IKEv1 和 IKEv2(選項功能)，會提供本地 ID 和對方 ID。
本機 ID (Local ID)	指定使用 IPsec VPN 類型建立 VPN 連線時要使用的本機 ID。
對方 ID(Peer ID)	請輸入遠端客戶端的 ID 名稱。 如果指定了相關數值，則系統只會接受來自指定 IP 位址和/或具有指定對等 ID 的連線。
更多設定	

IKE Phase 1	**加密(Encryption)** – 使用自動/AES/3DES/DES 加密演算法，並套用 MD5 或 SHA-1 認證演算法。 **群組(Group)** – 指定一個密鑰交換方案。 **驗證(Authentication)** – 選擇 SHA256 或 SHA1 進行資料封包認證。 **有效時間(Lifetime)** - 基於安全考量，密鑰的有效期限必須定義清楚。預設值為 28800 秒。您可設定的秒數範圍為 900 秒到 86400 秒。
IKE Phase 2	指定安全通訊協定、提案加密和提案認證方式。 **安全性通訊協定(Security Protocol)** – ESP（高）表示有效載荷（資料）將被進行加密和身份驗證。 **加密(Encryption)** – 使用 AES/3DES/DES 加密演算法。 **驗證(Authentication)** – 選擇全部、SHA256 或 SHA1 進行資料封包認證。 **有效時間(Lifetime)** – 基於安全考量，密鑰的有效期限必須定義清楚。預設值為 3600 秒。您可設定的秒數範圍為 600 秒到 28800 秒。 **完美前向保密 PFS (Perfect Forward Secret)** – 切換開關以啟用/停用此功能。 PFS 會在第二階段週期性換鍵期間強制執行金鑰交換。
Dead Peer Detection	DPD 是偵測 IPsec 連線的方法。 **DPD 延遲(DPD Delay)** – 這是一個保持連線定時器。當通道處於空閒狀態時，系統會定期發送 Hello 訊息。當數值設定為 0 時，可停用此功能。如果啟用，建議值設定為 30 秒。 **DPD 逾時(DPD Timeout)** - 這是逾時計時器。如果在逾時時間後仍未收到確認訊息，則對等方將被判定為失效。當數值設定為 0 時，可停用此功能。如果啟用此功能，建議值設定為 120 秒。
	網路(Network)
網路(Network)	指定允許本地子網和遠端子網的流量透過 VPN 連線。 **本機網路(Local Network)** – 預設值為 0.0.0.0，這表示 Vigor 路由器將在 IPCP 協商階段從遠端路由器取得 PPP IP 位址。如果遠端的 PPP IP 位址是固定的，請在此指定該固定 IP 位址。如果您不選擇 PPTP 或 L2TP，那麼請勿變更預設值。 **子網遮罩(Subnet Mask)** – 顯示本機網路的 TCP/IP 設定 IP 位址和子網路遮罩。請選擇符合本機網路要求的選項。 **遠端網路(Remote Network)** – 預設值為 0.0.0.0，這表示 Vigor 路由器將在 IPCP 協商階段從遠端路由器取得遠端閘道 PPP IP 位址。如果遠端的 PPP IP 位址是固定的，請在此指定該固定 IP 位址。如果您不選擇 PPTP 或 L2TP，那麼請勿變更預設值。 **子網遮罩(Subnet Mask)** - 選擇符合本機網路要求的選項。此功能用來新增一條固定路由，將所有發送到此遠端網路 IP 位址/遠端網路遮罩的流量皆透過 VPN 連線進行。針對 IPsec 而言，這是第二階段快速模式的目地用戶端 ID。
路由/NAT 模式 (Routing/NAT Mode)	如果選擇**撥入(Dial-In)**作為方向，則僅使用**路由(Routing)**。遠端網路僅允許本機網路使用一個 IP 位址。
內部網路位址轉換 (Translate Local Network)	要建立雙邊 VPN 連接，本機子網路和遠端子網路不能相同。如果碰巧相同，則需要進行 IP 位址轉換（例如，如果雙方都使用 192.168.1.10，則需要將其中一個轉換為 192.168.2.10 才能啟用雙邊 VPN 連線）。 切換開關以啟用/停用此功能。 **已轉換之網路(Translated Network)** – 指定 IPv4 位址。
更多子網(More Subnets)	切換此開關以啟用/停用此功能。 新增更多固定路由，可用於發送到遠端網路的子網路上。 **停用(Disabled)** – 停用此功能。 ● **新增(+Add)** – 按此新增新的固定路由。輸入遠端網路和子網路遮罩所

	需的資訊。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

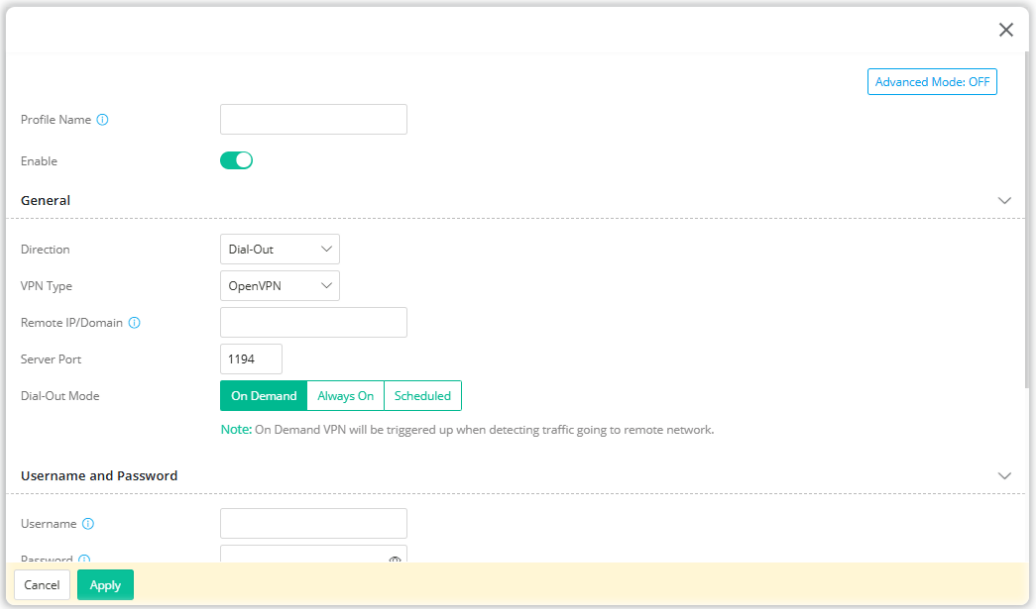
完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-4-2-4 VPN 類型 - OpenVPN

OpenVPN 協定利用公開金鑰、憑證以及使用者名稱和密碼來驗證客戶端身分。流量透過基於業界標準 SSL/TLS 加密協定建構的安全通道傳輸。

OpenVPN 需要使用憑證。建立 OpenVPN 連線之前，應先設定 OpenVPN 服務的基本設定。

若要新增新的資源設定檔（OpenVPNVPN 類型），開啟 VPN>>站點對站點 VPN (VPN>>Site-to-Site VPN) 並按下**+新增(+Add)**。



可用設定說明如下：

項目	說明
進階模式:開啟/關閉 (Advanced Mode:ON/OFF)	按此顯示或隱藏站點對站點 VPN(site-to-site VPN)的進階設定。
設定檔名稱(Profile Name)	輸入設定檔名稱，以供識別。
啟用(Enable)	切換開關以啟用/停用此設定。
基本(General)	
方向(Direction)	指定此 VPN 設定檔的允許撥號方向。 **撥出(Dial-Out)** – 設定檔用於發起對外連線。 **撥入(Dial-In)** – 此設定檔用於接受傳入連線。 **二者(Both)** - 設定檔用於發起（撥出）或接受（撥入）連線。
VPN 類型(VPN Type)	選擇用於建立 OpenVPN 連線的 VPN 類型。與 OpenVPN 類型相關的其他選項將根據所使用的方向而變更。 **OpenVPN (方向設定為二者/撥入時)** -可用選項包含： • **撥入允許排程(Dial-in Allowed Schedule)** **OpenVPN (方向設定為二者/撥出時)** -可用選項包含： • **遠端 IP/網域(Remote IP/ Domain)** • **伺服器埠號(Server Port)** • **撥出模式(Dial-Out Mode)**

撥入允許排程(Dial-In Allowed Schedule)	依照預設的時程安排進行連接和中斷連接。 **永遠允許(Always Allow)** – 選擇此選項可保持始終連線。 **排程(Scheduled)** – 選擇此選項可依照排程建立 VPN 連線。 ● **當排程為強迫時，中斷目前的通道(Drop the Active Tunnel when Schedule is Enforced)** –切換開關以啟用/停用此功能。 ● **VPN 排程(VPN Schedule)** – 用下拉式選單指定一個 VPN 設定檔。在設定 VPN 排程之前，請先在設定>>物件>>排程(Configuration>> Objects>> Schedule)中新增所需的時間間隔。
遠端 IP/網域(Remote IP/ Domain)	輸入遠端 VPN 伺服器的 IPv4 位址或主機名稱。
伺服器埠號(Server Port)	設定 VPN 伺服器的連接埠號碼。
撥出模式(Dial-Out Mode)	**需要時(On Demand)** – 當偵測到發送到遠端網路的流量時，將觸發 VPN 連線。 **永遠連線(Always On)** – 選擇此項可使撥號連線始終維持連線。 **排程(Scheduled)** – 選擇此選項可依照排程建立 VPN 連線。 ● **當排程為強迫時，中斷目前的通道(Drop the Active Tunnel when Schedule is Enforced)** – 切換開關以啟用/停用此功能。 ● **VPN 排程(VPN Schedule)** – 用下拉式選單指定一個 VPN 設定檔。在設定 VPN 排程之前，請先在設定>>物件>>排程(Configuration>> Objects>> Schedule)中新增所需的時間間隔。
指定對方 VPN (Specify VPN Peer)	當方向選擇二者(Both) 時，可用此功能。 切換此開關啟用/停用此功能。 **遠端 IP/網域(Remote IP/Domain)** – 輸入遠端對等方的 IP 位址。
使用者名稱與密碼(Username and Password)	
使用者名稱與密碼 (Username and Password)	**使用者名稱(Username)** - 用於遠端區域網路建立 VPN 連線。 **密碼(Password)** - 用於遠端區域網路建立 VPN 連線。
OpenVPN 設定 (OpenVPN Settings)	在以下情況下使用：方向選擇**撥出(Dial-Out)/二者(Both)**和 VPN 類型選擇 **OpenVPN**。 **撥出通訊協定(Dial-Out Protocol)** – 選擇 TCP 或 UDP 作為 VPN 伺服器協定。 **匯入 OpenVPN 設定(Import OpenVPN Config)** - 可以將其他 Vigor 路由器的 OpenVPN 設定檔匯入並套用到此路由器。 選擇將 OpenVPN 設定檔從指定的 OpenVPN 伺服器(例如 Vigor 路由器、PC、其他 VPN 提供者等) 匯入到 Vigor 路由器。之後，該路由器可以作為 VPN 用戶端，透過使用者名稱和密碼存取 VPN 伺服器。如果設定檔包含憑證，則會自動匯入。
網路(Network)	
網路(Network)	指定允許本地子網和遠端子網的流量透過 **OpenVPN** 連線。 **本機網路(Local Network)** – 定義屬於本機網路的 IP 位址範圍，此範圍用於透過 VPN 路由流量。 **子網遮罩(Subnet Mask)** – 子網路遮罩有助於定義本地網路的大小，並告訴 VPN 如何解釋 IP 位址中的網路部分。子網路遮罩為 255.255.255.0(或 CIDR 表示法中的 /24)表示 IP 位址的前 24 位元用於路，其餘 8 位元用於本地網路中的主機(裝置)。 **遠端網路(Remote Network)** – 定義您要連接的遠端網路的 IP 位址範圍。例如，如果遠端網路是 10.0.0.0/24，則您是在告訴 VPN 遠端網路的 IP 位址範圍是 10.0.0.1 到 10.0.0.254。 **子網遮罩(Subnet Mask)** – 與本機網路類似，遠端網路的子網路遮罩決定

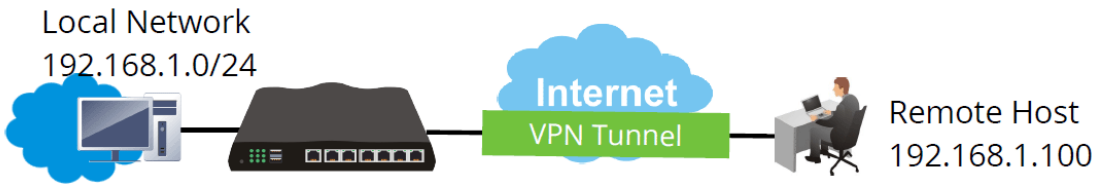
	了遠端網路 IP 位址範圍的劃分方式。若遠端網路的子網路遮罩為 255.255.255.0（或 /24），則表示遠端網路有 254 個可供裝置使用的位址。
路由/NAT 模式 (Routing/NAT Mode)	當方向選擇**撥入(Dial-In)**時，只能選擇路由模式。遠端網路僅允許本機網路使用一個 IP 位址。 當方向選擇**撥出/二者 (Dial-Out/Both)**： 如果遠端網路只允許本機網路使用一個 IP 位址，請選擇 NAT；否則，請選擇路由。 **路由(Routing)** – 支援標準的站點到站點 VPN，流量可以直接在兩個網路之間路由，而無需更改來源 IP 位址。 • **內部網路位址轉換(Translate Local Network)** – 要建立雙邊 VPN 連接，本機子網路和遠端子網路不能相同。如果碰巧相同，則需要進行 IP 位址轉換（例如，如果雙方都使用 192.168.1.10，則需要將其中一個轉換為 192.168.2.10 才能啟用雙邊 VPN 連線）。 • **已轉換之網路(Translated Network)** – 指定 IPv4 位址。 **NAT** – 修改發送到遠端站點的 VPN 流量，將來源 IP 位址轉換為虛擬 IP 位址，然後再將其傳送到目地位置。
更多子網(More Subnets)	新增更多固定路由，可用於發送到遠端網路的子網路上。 切換此開關以啟用/停用此功能。 • **新增(+Add)** – 按此新增新的固定路由。輸入遠端網路和子網路遮罩所需的資訊。
進階模式下的選項	
撥出介面模式(Dial-Out Interface Mode)	選擇使用此設定檔建立連線的 WAN 連線。此設定僅適用於撥出連線。 **優先選擇介面(Selected Interface First)** – 連線時，路由器會先使用選定的 WAN 介面進行 VPN 連線。如果選定的 WAN 介面連線失敗，路由器會嘗試使用其他 WAN 介面。 **限用選定介面(Selected Interface Only)** – 連線時，路由器將使用選定的 WAN 作為 VPN 連線的唯一介面。 **手動(Manual)** – 自行定義 VPN 設定。指定哪些 WAN 可用作對外連線介面。
撥出介面(Dial-Out Interface)	**自動選擇(Auto Select)** – 依照預設路由決定要撥出的介面。 **預設 WAN IP/IP 位址(Default WAN IP / IP Address)** – 用下拉清單為此 VPN 設定檔指定一個 WAN IP 位址。
撥出進階設定(Dial Out Advanced Settings)	**密碼演算法(Cipher Algorithm)** – 選擇所需的加密演算法。目前有幾種加密演算法：AES128、AES192 和 AES256。AES256 比 AES128 更安全，但由於其計算開銷更高，可能導致性能變低。 **HMAC 演算法(HMAC Algorithm)** – HMAC 代表基於雜湊的訊息認證碼。用於驗證 VPN 資料的完整性和真實性。 選擇所需的 HMAC 哈希演算法。支援兩種雜湊演算方式：SHA1 和 SHA256。建議使用 SHA256，因為它比 SHA1 更穩健可靠。 **用戶端憑證(Client Certificate)** – 使用下拉式清單選擇已上傳至路由器的用戶端憑證。匯入 OpenVPN 設定檔後，系統會自動選擇預設選項(亦即使用 OpenVPN 設定中的憑證)。 **受信任的 CA (Trusted CA)** – 用下拉清單選擇已上傳至路由器的受信任 CA 憑證。匯入 OpenVPN 設定檔後，系統會自動選擇預設選項(亦即使用 OpenVPN 設定中的 CA)。 **壓縮(Compress)** – 選擇一種方法來壓縮資料封包，以減少傳輸壓縮資料封包時的頻寬使用量。 **TLS 驗證(TLS Auth)** – 切換此開關以啟用/停用 TLS 驗證方法。如果

	OpenVPN 設定檔包含 TLS 金鑰，則會自動匯入。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

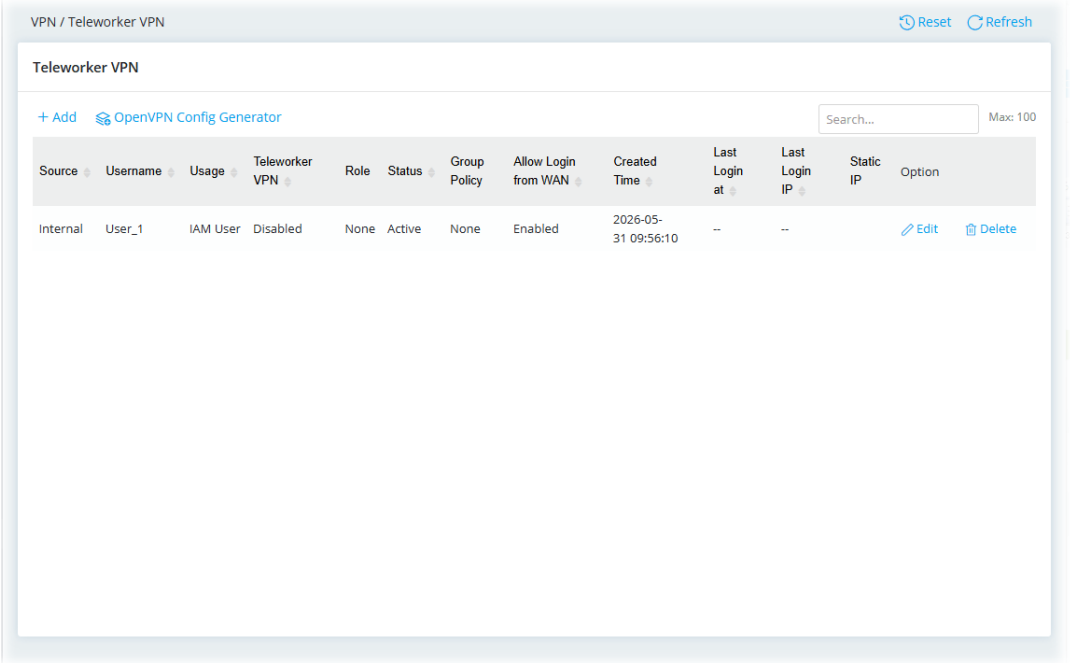
完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-4-3 遠端工作者 VPN(Teleworker VPN)

VPN 指的是遠端主機與路由器區域網路之間的連線。主機使用的是本機子網路中的 IP 位址。它允許員工在出差時存取公司的內部資源。

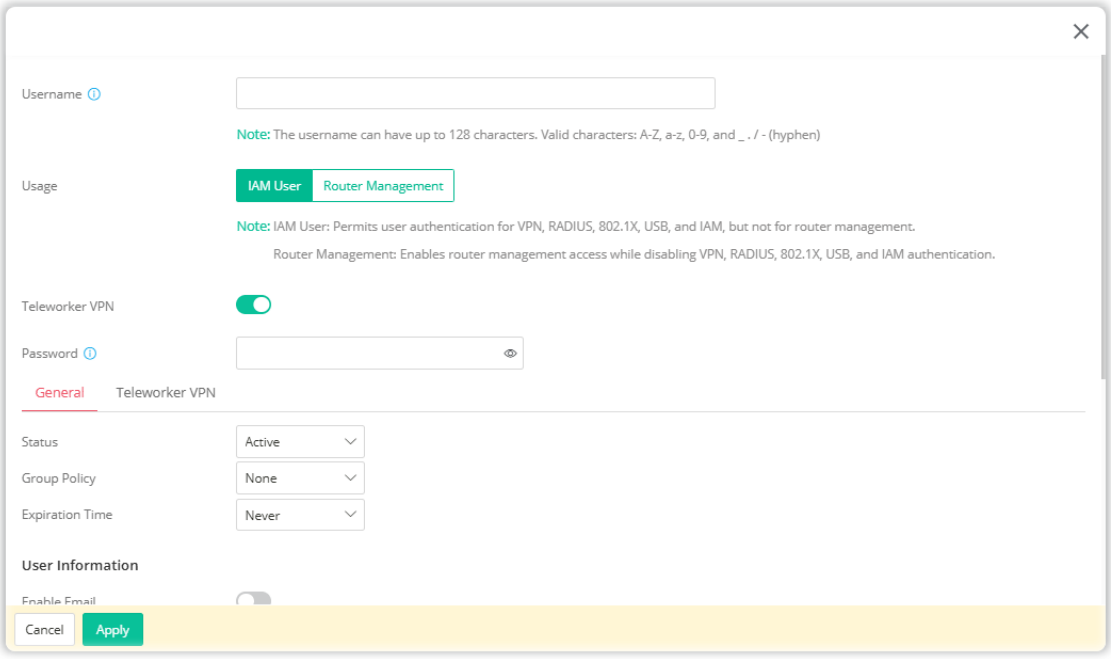


開啟 VPN>>遠端工作者 VPN，即可進入以下頁面。



若要新增 VPN 設定檔，請按**+新增(+Add)**。

請注意，此處對使用者設定檔進行的設定修改 (無論是新增還是編輯) 都會同步改寫 IAM>>使用者和群組>>使用者中的設定內容，反之亦然。



可用設定說明如下：

項目	說明
使用者名稱(Username)	輸入登入名稱（例如，*LAN_User_Group_1*、*WLAN_User_Group_A*、*WLAN_User_Group_B* 等等）針對此使用者設定檔。
用法(Usage)	定義此使用者設定檔的類型。 **IAM 使用者(IAM User)**–此設定檔可用於 VPN、RADIUS、802.1X、USB 和 IAM（身分和存取管理）驗證。 **路由器管理(Router Management)**–此設定檔僅用於路由器管存取，不能用於 VPN、RADIUS、802.1X、USB 和 IAM 驗證。
遠端工作者 VPN (Teleworker VPN)	如果用法選擇了 IAM 使用者，則可用此功能。 切換開關即可啟用或停用遠端工作者 VPN 功能。
密碼(Password)	如果用法選擇了 IAM 使用者，則可用此功能。 針對此使用者設定檔設定密碼（例如，*lug123*、*wug123*、*wug456* 等等）。 當使用者嘗試存取網際網路時，必須提供有效的使用者名稱和密碼組合進行身份驗證。系統會將符合的使用者名稱和密碼對應的設定檔套用至本次連線數。
密碼/新的密碼/確認新密碼(Password New Password/ Confirm New Password)	如果用法選擇了路由器管理，則可用此功能。 針對此使用者設定檔設定密碼（例如，*lug123*、*wug123*、*wug456* 等等）。 當使用者嘗試存取網際網路時，必須提供有效的使用者名稱和密碼組合進行身份驗證。系統會將符合的使用者名稱和密碼對應的設定檔套用至本次連線數。
基本(General) (如果用法選的是 IAM 使用者)	
狀態(Status)	**使用中(Active)** – 啟用此頁面中的一般設定。 **未啟用(Inactive)** – 停用此頁面上的一般設定。
群組策略(Group Policy)	如果用法選擇了 IAM 使用者，則可用此功能。 選擇要套用到此使用者設定檔的群組策略設定檔。
到期日(Expiration Time)	如果用法選擇了 IAM 使用者，則可用此功能。

	設定網路連線僅在特定時間間隔內運作。預設情況下，所有使用者帳戶將自動套用此時間設定。 **永不(Never)** – 網路連線始終保持開啟狀態。 **剩餘時間(Expire in)** – 網路連線建立後，將在指定的分鐘、小時、天或周後過期並終止連線。 **到期時間(Expire at)** – 網路連線建立後，將在以下指定的日期和時間到期並終止連線。 • 日期(Date) • 時間(Time)
使用者資訊(User Information)	**啟用電子郵件(Enable Email)**– 切換開關以啟用或停用電子郵件設定。 • **電子郵件(Email)**–輸入用於接收 MFA PIN 碼的電子郵件地址。 • **傳送電子郵件通知至新建立的使用者(Send Email Notification to the newly created User)**– 向此使用者帳號發送通知郵件。 **啟用簡訊(Enable SMS)** –切換開關以啟用或停用簡訊設定。 • **簡訊(SMS)** – 輸入接收 MFA PIN 碼的簡訊接收號碼。
MFA 與 Port Knocking (MFA & Port Knocking)	多因驗證（MFA）可以提供更安全的網路連線。 **啟用 MFA(Enable MFA)** – 切換開關以啟用/停用 MFA 功能。 • **允許的 MFA 方式(Allowed MFA Method)** – 選擇從 WAN 登入時是否需要 TOTP、簡訊或電子郵件驗證。 **TOTP** – 對於基於時間的一次性密碼 (TOTP) 機制，請確保您的路由器時區設定正確。然後，在您的手機上安裝 Google Authenticator 應用程式。開啟該應用程式掃描此頁面上的 QR 碼(QR Code)。您的手機上將顯示一次性密碼。選擇 TOTP 並按下套用(Apply)，即可彈出如下對話框：  在驗證碼(Validation Code)欄位中，輸入一次性密碼，然後按一下驗證(Verify)。 現在設定已完成。在通過使用者名稱和密碼驗證後，您將被要求輸入雙因認證碼。 **簡訊/電子郵件(SMS/Email)** – 密碼將根據您在上方使用者資訊中選擇的方式透過簡訊或電子郵件發送。 • **強制執行 Port Knocking (Enforce Port Knocking)** – 切換開關以啟用/停用 Port Knocking 功能。 **第一個 Knock 埠口(1st Knock Port)** – 請輸入數值（3001~59999）。按下感嘆號（！）以查看更多資訊。 **TOTP 密鑰(TOTP Secret)** – 顯示用於 TOTP 的金鑰。
帳號資訊(Account Info)	顯示使用者帳戶的一般資訊（建立時間、上次登入時間和上次登入 IP）。

遠端工作者 VPN (Teleworker VPN) (如果用法選的是 IAM 使用者)	
基本(General)	**閒置逾時(Idle Timeout)** – 如果使用者空閒時間超過設定的逾時時間，則該使用者的網路連線將會中斷。預設情況下，閒置逾時時間為 300 秒。 **VPN 排程(VPN Schedule)** – 選擇**永遠連線(Always On)**（遠距辦公 VPN 始終運作）。或選擇**排程啟用(Scheduled On)**根據排程建立 VPN 連線。 在設定 VPN 排程之前，請在設定>>物件>>排程 (Configuration>>Objects >>Schedule) 中新增所需的時間間隔。 **透過 VPN 進行 Netbios 命名(Netbios Naming over VPN)** – 切換開關以允許/拒絕 NetBIOS 命名封包透過 VPN 通道傳輸。 **VPN 多播(Multicast over VPN)** - 切換開關以允許/拒絕多播封包穿過 VPN 通道。 **透過 VPN 傳送 mDNS (mDNS over VPN)** - 切換開關以允許/拒絕 mDNS 封包透過 VPN 通道傳輸。 **下載 SmartVPN Client (Download SmartVPN Client)** - 按此下載用於建立 VPN 連線的 DrayTeck SmartVPN 用戶端工具。
允許的 VPN 通訊協定 (Allowed VPN Protocols)	選擇 IPsec、WireGuard 或 OpenVPN 作為遠端工作者 VPN 連線的通訊協定。 **IPsec** – 切換開關以啟用 IPsec 協定。 如果啟用，請選擇 IKEv1/v2、EAP 和/或 XAuth 作為 IPsec 協定。 **OpenVPN** – 切換開關以啟用 OpenVPN 協定。 **WireGuard** – 切換開關以啟用 WireGuard 協定。 • **產生金鑰模式(Generate Key Mode)** – 選擇自動(Auto)或客製化(Customized)。 選擇自動(Auto)並按下**產生金鑰組(Generate Key Pair)** 以自動產生用戶端虛擬金鑰和用戶端公開金鑰。 選擇客製化(Customized)輸入對方的公開金鑰。 • **用戶端公開金鑰(Client Public Key)** – 輸入遠端 WireGuard VPN 用戶端提供的字串。 • **預先共享金鑰(Pre-Shared Key)** – 顯示按下產生預先共享金鑰(PSK)按鈕所產生的虛擬金鑰。 • **產生預先共享金鑰(PSK) (Generate PSK)** – 按下產生預先共享金鑰(PSK)按鈕產生預共用金鑰。 • **持續維持連線(Persistent Keepalive)** – 預設值為 60 秒。如果對方位於 NAT 或防火牆之後，請使用預設設定。 **L2TP** –切換開關以啟用 L2TP 協定。啟用後，請設定： • **含 IPsec 策略之 L2TP (L2TP with IPsec Policy)** - 對於這種連線類型，必須使用 L2TP 和 IPsec 加密，以確保資料完整性和機密性。 **必須(Must)** - 指定要對 L2TP 連線套用的 IPsec 策略。
WireGuard 設定 (WireGuard Settings)	如果**允許的 VPN 通訊協定**選擇了 **WireGuard**，則可用此功能。 **產生金鑰模式(Generate Key Mode)** – 選擇自動(Auto)或客製化(Customized)。 **產生金鑰組(Generate Key Pair)** – 按此即可自動產生用戶端虛擬金鑰和用戶端公開金鑰。 **用戶端公開金鑰(Client Public Key)** – 輸入遠端 WireGuard VPN 用戶端提供的字串。 **預先共享金鑰(Pre-Shared Key)** – 顯示按下產生預先共享金鑰(PSK)按鈕所產生的虛擬金鑰。 **產生預先共享金鑰(PSK) (Generate PSK)** – 按下產生預先共享金鑰(PSK)按鈕產生預共用金鑰。 **持續維持連線(Persistent Keepalive)** – 預設值為 60 秒。如果對方位於

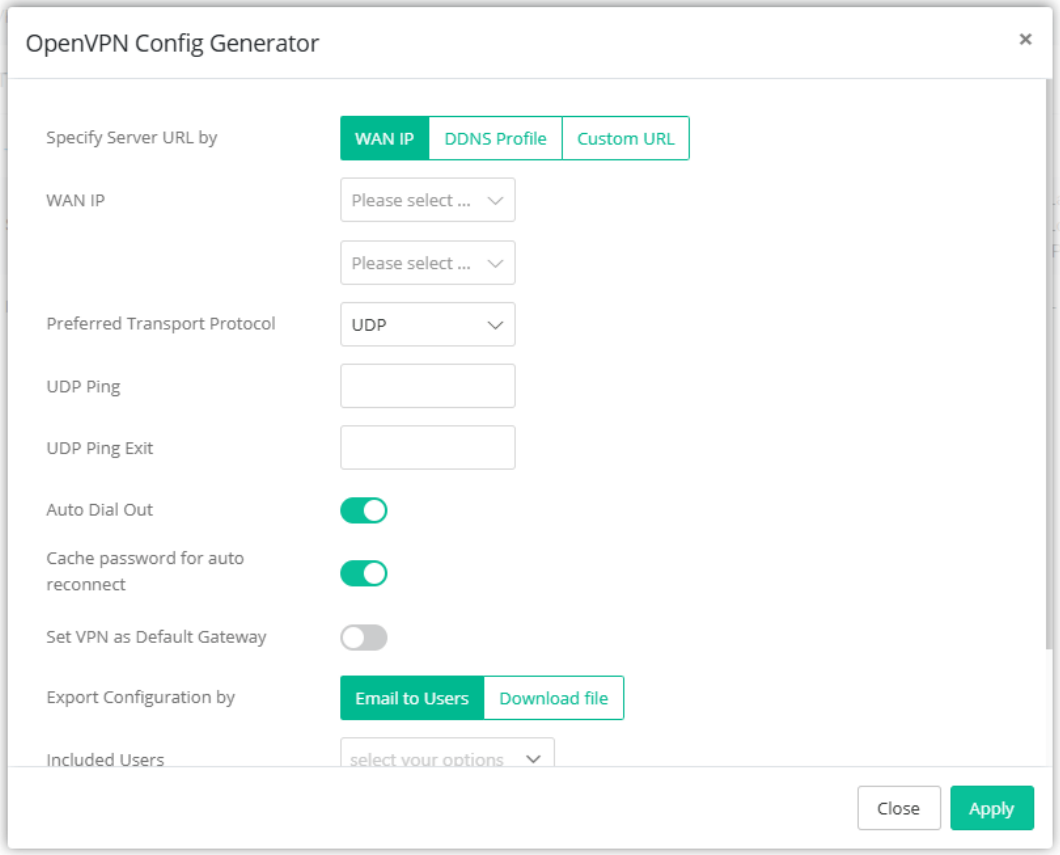
	NAT 或防火牆之後，請使用預設設定。
安全性(Security)	**指定對方 VPN (Specify VPN Peer)** – 切換開關以啟用/停用遠端客戶端的安全機制。 ● **遠端用戶端 IP (Remote Client IP)** – 如果啟用了指定對方 VPN 功能，請輸入遠端對等體的 IP 位址。 ● **預先共享金鑰(Pre-Shared Key)** – 當選擇 IPsec 作為允許的 VPN 協定時，則可用此功能。**指定對方 VPN** 可以限制 IPsec 只能由指定的對方 IP 位址或網域名稱發起，並可指定要使用的虛擬金鑰。 **X509 數位簽章(X.509 Digital Signature)** - 當選擇 IPsec 作為允許的 VPN 協定時，則可用此功能。接受憑證身份驗證。若要使用 X.509 數位簽章，請選擇一種身份驗證方法，並為每種方法輸入所需資訊。 ● **停用(Disabled)** –選擇此項目可停用 VPN 連線的憑證應用。 ● **接受主體替代名稱(Accept Subject Alternative Name)** – 以下三種對方 ID 格式均可接受，包括 IP 位址、網域名稱和電子郵件。 ● **從現有憑證中選擇(Select from Existing Certificates)** –選擇已預先取得並儲存在設定>>憑證>>本機憑證 (Configuration>>Certificates>> Local Certificate)中的對等憑證。 ● **接受主體名稱(Accept Subject Name)** – 請輸入完整的憑證主體名稱。 ● **接受任一(Accept Any)** – 任何由設定>>憑證>>受信任的 CA(Configuration>>Certificates>> Trusted CA)中受信任的 CA 簽署的憑證都將被視為有效。
本機 IP 分派(Local IP Assignment)	**分派 IP 藉由(Assign IP By) –** 選擇 **LAN DHCP** 或者**固定 IP 位址**。如果啟用了 WireGuard VPN 通訊協定，則此選項將無法使用。 若選擇**固定 IP(Static IP)**， ● **固定 IP(Static IP)** –指定 IPv4 位址。 **分派 IP 來自(Assign IP from)** – 選擇一個 LAN 介面進行 IP 分配。 **DNS 分派方式(Assign DNS By)** – 選擇 **LAN DHCP**（DNS IP 位址將由 Vigor 路由器自動分配）或是**固定 DNS**，如果選擇固定 DNS，請設定主要 DNS 和次要 DNS。 ● **主要 DNS (Primary DNS)** – 輸入主要 DNS 伺服器的 IPv4 位址。 ● **次要 DNS (Secondary DNS)** – 如果需要，請輸入另一個 DNS 伺服器的 IPv4 位址。
	基本(General) **(如果用法選的是路由器管理者)**
角色(Role)	如果用法選擇了路由器管理，則可用此功能。 ● **管理者(Administrator)** ● **訪客(Guest)** ● **使用者(Users)**
狀態(Status)	**使用中(Active)** – 啟用此頁面中的一般設定。 **未啟用(Inactive)** – 停用此頁面上的一般設定。
允許透過 WAN 登入 (Allow Login from WAN)	如果用法選擇了路由器管理，則可用此功能。 若啟用，使用者可以從 WAN 端登入。
使用者資訊(User Information)	**啟用電子郵件(Enable Email)**– 切換開關以啟用或停用電子郵件設定。 ● **電子郵件(Email)**–輸入用於接收 MFA PIN 碼的電子郵件地址。 ● **傳送電子郵件通知至新建立的使用者(Send Email Notification to the newly created User)**– 向此使用者帳號發送通知郵件。 **啟用簡訊(Enable SMS)** –切換開關以啟用或停用簡訊設定。

	• **簡訊(SMS)** - 輸入接收 MFA PIN 碼的簡訊接收號碼。
MFA 與 Port Knocking (MFA & Port Knocking)	多因驗證（MFA）可以提供更安全的網路連線。 **啟用 MFA(Enable MFA)** – 切換開關以啟用/停用 MFA 功能。 • **允許的 MFA 方式(Allowed MFA Method)** - 選擇從 WAN 登入時是否需要 TOTP、簡訊或電子郵件驗證。 **TOTP** – 對於基於時間的一次性密碼 (TOTP) 機制，請確保您的路由器時區設定正確。然後，在您的手機上安裝 Google Authenticator 應用程式。開啟該應用程式掃描此頁面上的 QR 碼(QR Code)。您的手機上將顯示一次性密碼。選擇 TOTP 並按下套用(Apply)，即可彈出如下對話框：  在驗證碼(Validation Code)欄位中，輸入一次性密碼，然後按一下驗證(Verify)。 現在設定已完成。在通過使用者名稱和密碼驗證後，您將被要求輸入雙因認證碼。 **簡訊/電子郵件(SMS/Email)** – 密碼將根據您在上方使用者資訊中選擇的方式透過簡訊或電子郵件發送。 • **強制執行 Port Knocking (Enforce Port Knocking)** – 切換開關以啟用/停用 Port Knocking 功能。 **第一個 Knock 埠口(1st Knock Port) -** 請輸入數值（3001~59999）。按下感嘆號(!)以查看更多資訊。 **TOTP 密鑰(TOTP Secret) –** 顯示用於 TOTP 的金鑰。
	遠端工作者 VPN (Teleworker VPN) **(如果用法選的是路由器管理者)**
透過 VPN 進行 Netbios 命名(Netbios Naming over VPN)	切換開關以允許/拒絕 NetBIOS 命名封包透過 VPN 通道傳輸。
VPN 多播(Multicast over VPN)	切換開關以允許/拒絕多播封包穿過 VPN 通道。
帳號資訊(Account Info)	顯示使用者帳戶的一般資訊（建立時間、上次登入時間和上次登入 IP）。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

OpenVPN 設定產生器(OpenVPN Config Generator)

在本頁中，您可以建立遠端 OpenVPN 用戶端連接到路由器所需的設定，然後直接下載或透過電子郵件傳送給使用者。



可用設定說明如下：

項目	說明
指定伺服器 URL 方式 (Specify Server URL by)	OpenVPN 用戶端將使用 IP 位址或網域名稱連接到路由器。 **WAN IP** – OpenVPN 設定檔將使用數字型式的 IP 位址作為伺服器位址。 ● **WAN IP** – 選擇 WAN 介面。 **DDNS 設定檔(DDNS Profile)** – OpenVPN 設定檔將使用 DDNS 設定檔中的網域名稱。 ● **DDNS 設定檔(DDNS Profile)** – 選擇一個 DDNS 設定檔。 **客製 URL (Custom URL)** – T OpenVPN 設定檔將使用使用者定義的伺服器 IP 或網域名稱。 ● **客製 URL (Custom URL)**– 指定使用者設定中的 URL。
傳輸通訊協定(Transport Protocol)	**TCP/UDP** – 選擇 UDP 或 TCP 作為 OpenVPN 用戶端連線到路由器時所使用的協定。
UDP Ping	如果在設定的秒數內沒有發送任何資料封包，則透過 UDP 控制通道 ping 遠端設備。
UDP Ping 離開(UDP Ping Exit)	如果未收到來自遠端裝置的 ping 或其他封包，則讓 OpenVPN 在此處設定的秒數後退出。
自動撥出(Auto Dial Out)	切換開關即可啟用/停用此功能。 **啟用(Enable)** – 遠端用戶端可以自動撥號連接到這台 Vigor 路由器，以建立 OpenVPN 通道。 **停用(Disable)** – 停用此功能。

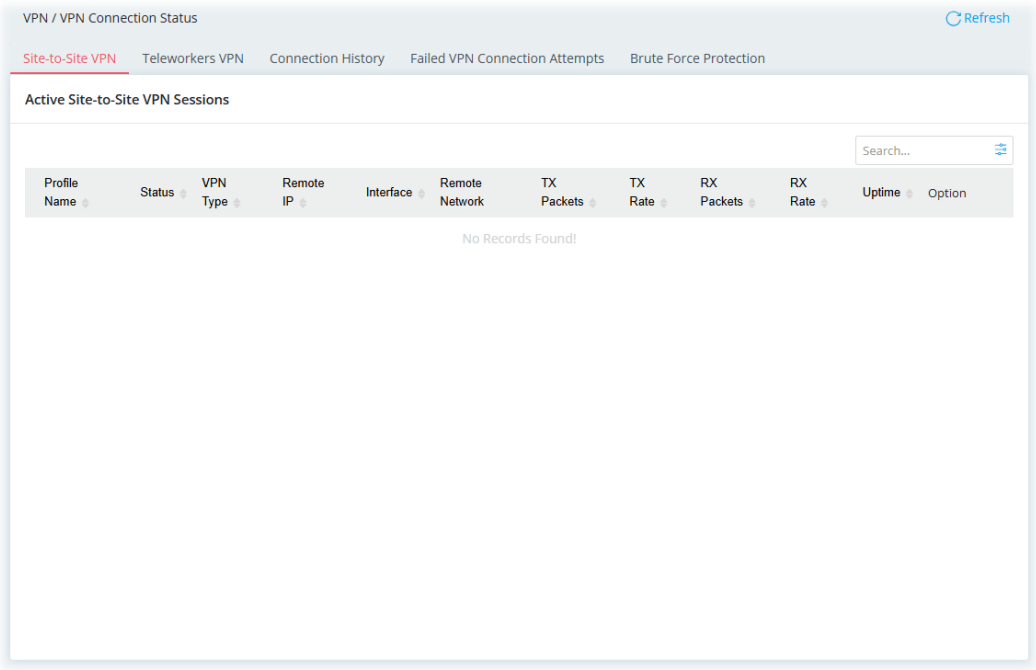
自動重新連線之暫存密碼 (Cache password for auto reconnect)	切換開關即可啟用/停用此功能。 **啟用(Enable)** - OpenVPN 將每小時自動重新連線一次。重新連線時需要輸入密碼。如果啟用此功能，Vigor 系統將保存 OpenVPN 連線的密碼，並在每次重新連線時使用。 **停用(Disable)** -停用此功能。
設定 VPN 做為預設閘道 (Set VPN as Default Gateway)	切換開關即可啟用/停用此功能。 **啟用(Enable)** - Vigor 路由器將被視為 OpenVPN 用戶端的預設閘道。OpenVPN 用戶端會將所有流量透過 OpenVPN 通道重新導向至 Vigor 路由器。 **停用(Disable)** - 停用此功能。
匯出設定檔方式(Export Configuration by)	**郵件至使用者(Email to Users)** – 若選擇此功能，下方將顯示包含使用者欄位。OpenVPN 設定檔將傳送給包含使用者清單中的使用者。 ● **包含使用者(Included Users)** – 選擇將從 Vigor 路由器接收設定的遠端工作者(辦公用戶)。 ● **傳送電子郵件(Send Email)** – 按此即可將此頁面上的設定以檔案的形式透過電子郵件傳送，該檔案可以匯入到 VPN 用戶端中，以便與遠端辦公使用者建立 OpenVPN 連線。 **下載檔案(Download file)** – OpenVPN 的設定檔將儲存在資料庫中。若選擇此項，下方將顯示下載設定按鈕。 ● **下載設定(Download Configuration)** - 按下此按鈕，將此頁面上的設定下載為檔案，該檔案可以匯入到 VPN 用戶端以建立 OpenVPN 連線。
Close	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-4-4 VPN 連線設定

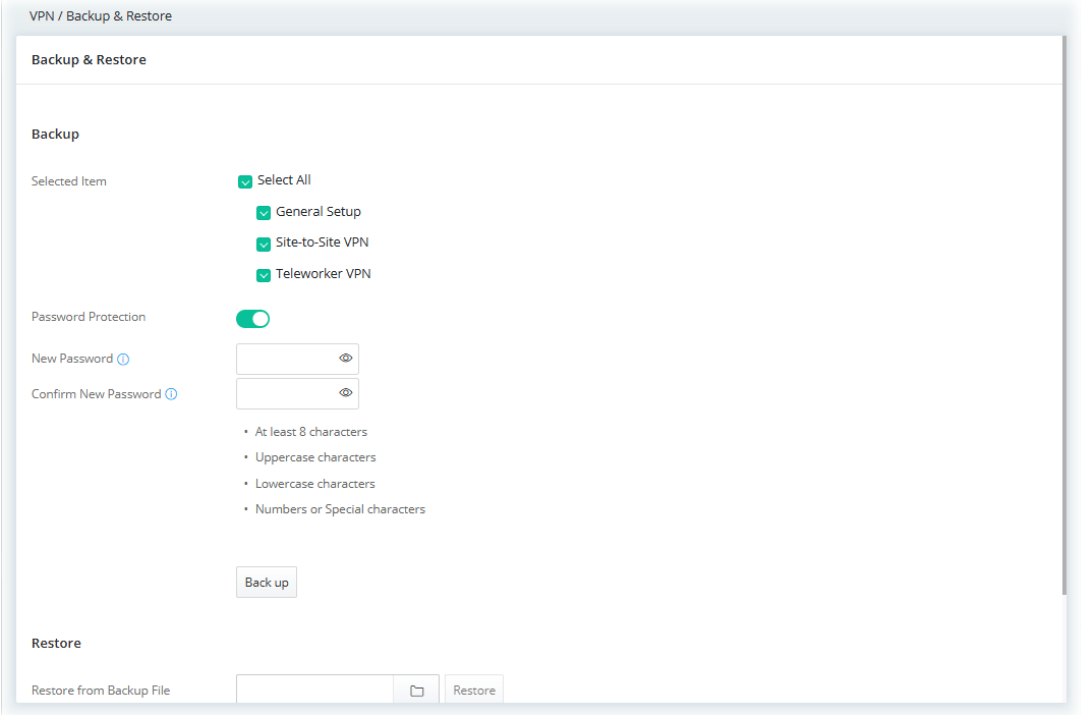
本頁顯示各種 VPN 連線狀態，包括

- 站點對站點 VPN(Site-to-Site VPN)
- 遠端工作者 VPN(Teleworker VPN)
- 連線歷史(Connection History)
- 失敗的 VPN 連線嘗試(Failed VPN Connection Attempts)
- 暴力攻擊防護(Brute Force Protection)



II-4-5 備份與還原(Backup & Restore)

此頁面可用於備份/還原 VPN 設定。



可用設定說明如下：

項目	說明
	備份(Backup)
選定項目(Selected Items)	選擇用於設定備份的 VPN 類型。
密碼保護(Password Protection)	為了安全起見，可以對此裝置的設定檔進行加密。 切換開關即可啟用或停用此功能。
新的密碼/確認新密碼(New Password/ Confirm New Password)	輸入字元作為加密設定檔的密碼。
備份(Back up)	按此即可備份設定檔。
	還原(Restore)
還原自備份檔案(Restore from Backup File)	- 按此找到要還原的檔案。 **還原(Restore)** - 按此執行還原操作。
檔案具有密碼保護(File has Password Protection)	切換開關即可啟用或停用此功能。 如果啟用，則還原設定時需要密碼。
密碼(Password)	輸入用於還原設定的密碼。

II-5 虛擬控制器 – 無線網路(Virtual Controller - Wireless)

此功能可讓使用者建立和管理由無線或有線鏈結連接的 DrayTek 裝置組成的網路。

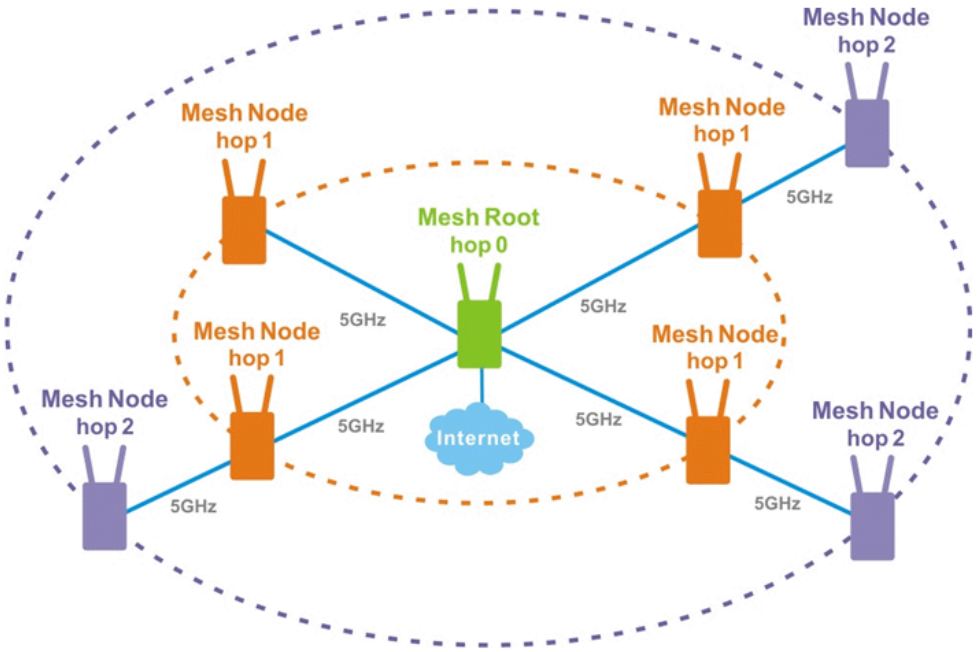
此網路由一個根節點(Root)及多個子節點(Nodes)組成。根節點控制整個網路並將設定內容同步到所有子節點。通常，根節點和子節點使用相同的無線 SSID/安全性設定，無線用戶端可以連接到其中任何一個。

對於無線網狀網路，根節點也是通往網際網路的入口。網路中的所有裝置都位於同一個群組中。根節點可以增加節點至群組中或從群組中刪除任一成員。使用者可以選擇 VigorMesh 或 EasyMesh 來建立無線網狀(Mesh)網路。如果停用無線網狀網路，只要啟用了 AP 管理，仍可僅透過有線連結建立網路。

VigorMesh 是 DrayTek 專屬的無線網狀網路功能。請注意，在 VigorMesh 網路中

- 群組成員總數允許為 8 個(包括網路主點)
- 最大躍點數為 3

參考下圖：



對於 VigorMesh 網路中的無線網狀網路群組

- 必須由 “1” 無線網狀網路主點和 “0~7” 無線網狀網路節點組成。
- (漫遊)通常情況下，網狀網路中的成員使用相同的無線 SSID/安全設定。
- (新增)只有無線網狀網路主點才能在無線網狀網路群組中新增一個無線網狀網路節點。
- (恢復)斷開連接的網狀網路節點將自動嘗試連接到同一組中另一個已連接的網狀節點。

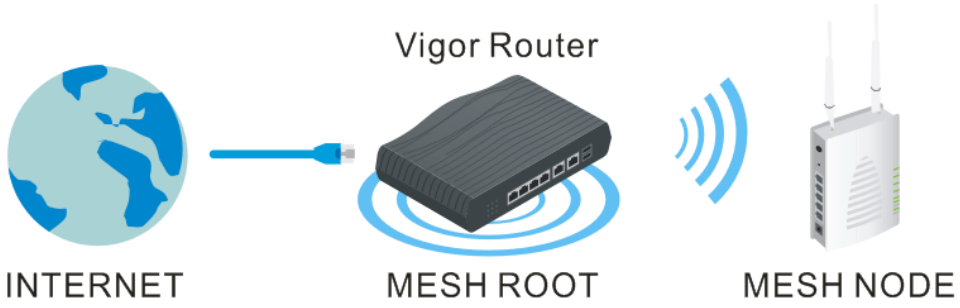
無線網狀網路主點(Mesh Root)與無線網狀網路節點(Mesh Node)

無線網狀網路主點(Mesh Root)表示該裝置將是另一台裝置的上行鏈路連線。

作為網路主點，該裝置必須先透過乙太網路線連接到一台閘道器，才能連接到網際網路。

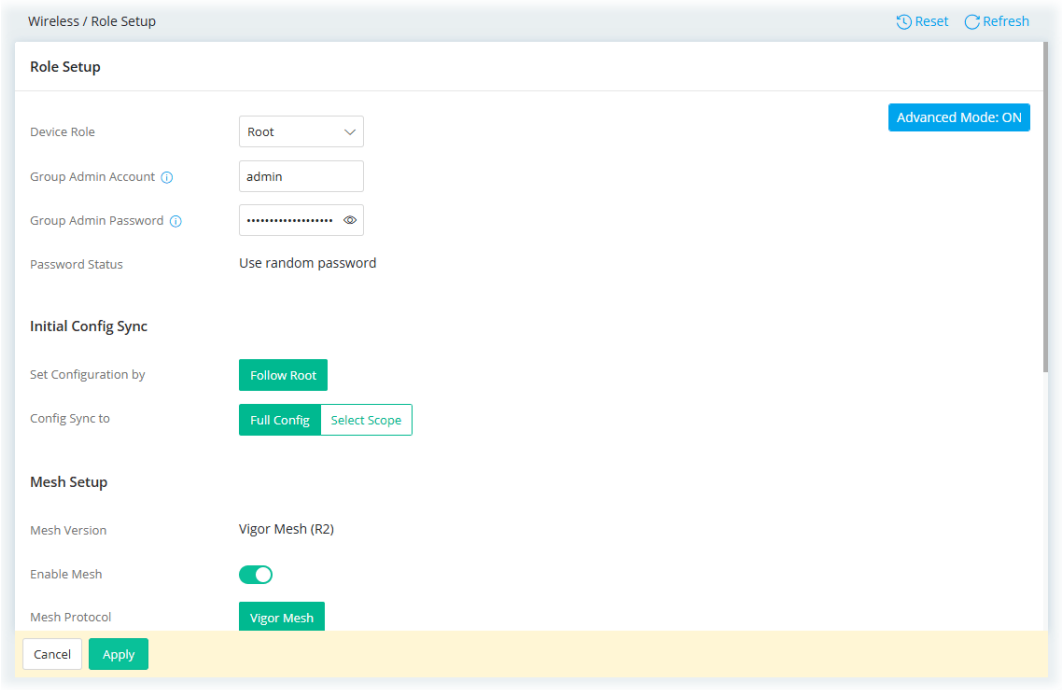
作為網路節點，該裝置可以透過無線或有線鏈路連接到同一無線網狀網路群組內的網路主點或網路節點。

下圖展示了 Vigor 路由器如何作為 MESH ROOT 運作：



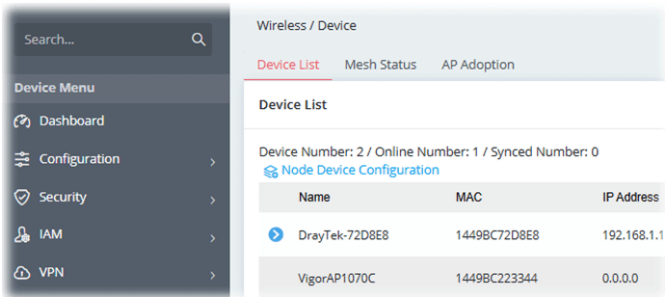
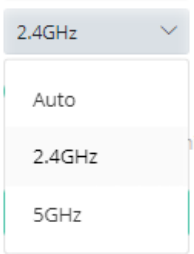
II-5-1 角色設定(Role Setup)

本頁面可以決定與電腦實體連接的 Vigor 路由器的角色，並設定其無線網狀網路(Mesh)功能和 AP 管理功能。



可用設定說明如下：

項目	說明
進階模式:開啟/關閉 (Advanced Mode:ON/OFF)	按此顯示或隱藏進階設定(如**無線下行鏈路頻帶**、**自動無線上行鏈路最佳化**與**日誌等級**)。
裝置角色(Device Role)	**網路主點(Root)** – 本裝置是網路主點。可控制網路並將設定同步到其所屬群組的各個節點上。
群組管理帳號(Group Admin Account)	設定一組帳號，供系統管理者用管理無線網狀網路節點。 此處設定的帳號將取代每個節點各自的帳號名稱，以確保無線網狀網路節點帳號的安全性。

群組管理密碼(Group Admin Password)	為系統管理者設定管理無線網狀網路節點的密碼。 此處所設定的密碼將取代每個節點的現有密碼，以確保無線網狀網路節點帳號的安全性。
密碼狀態(Password Status)	**使用者隨機密碼(User random password)** – 此為預設顯示狀態。在預設情況下，網狀網路組密碼將由 Vigor 系統隨機產生。 **準備(Ready)** – 如果密碼是手動設定或變更的，設定完成後，將顯示準備就緒 Ready 字樣。
初始設定同步(Initial Config Sync)	
設定配置方式(Set Configuration by)	**依網路主點(Follow Root)** - 依照主點設定內容套用至設定上 - **完整設定(Full Config)**或**選擇範圍(Select Scope)**。
設定同步至(Config Sync to)	**完整設定(Full Config)** – 將完整設定同步到所有節點。 **選擇範圍(Select Scope)** - 將選定的設定同步到所有節點。
無線網狀網路設置(Mesh Setup)	
啟用無線網狀網路(Enable Mesh)	切換此開關以啟用/停用無線網狀網路功能。
無線網狀網路通訊協定(Mesh Protocol)	選擇網狀網路協定，以管理無線網狀網路。 ● **Vigor Mesh** - DrayTek 開發的協定。
群組名稱(Group Name)	顯示目前無線網狀網路群組的名稱。如有需要，請更改名稱。
自動有線納管模式(Auto Wired Adoption)	允許使用者跳過在 Web AP 納管過程中的搜尋/選擇步驟，只需將 AP 連接到根設備的 LAN 連接埠即可建立 VigorMesh 群組。 啟用此功能後，在 VigorMesh 透過乙太網路封包偵測到新的有線基地台(AP)時，網狀網路主點(例如 VigorC410)會將其新增至**裝置>>裝置清單(Device>>Device List)**並開始註冊。然後，該節點將自動被納管入網路。 注意兩方(主點與節點)都必須支援並啟用**自動有線納管模式(Auto Wired Adoption)**功能。 
無線下行鏈路頻帶(Wireless Downlink Band)	此功能僅在進階設定啟用時(ON)才可使用。 選擇無線上行鏈路時，請將選擇網狀網路成員作為首要考慮因素。 選擇無線頻段(自動、2.4GHz 或 5GHz)以連接到下行網狀網路主點或下行網狀網路節點。 
自動無線上行鏈路最佳化(Auto Wireless Uplinks	此功能僅在進階設定啟用時(ON)才可使用。 預設已啟用此功能。若要執行自動重選，請確保網狀網路節點(成員)的 CFG

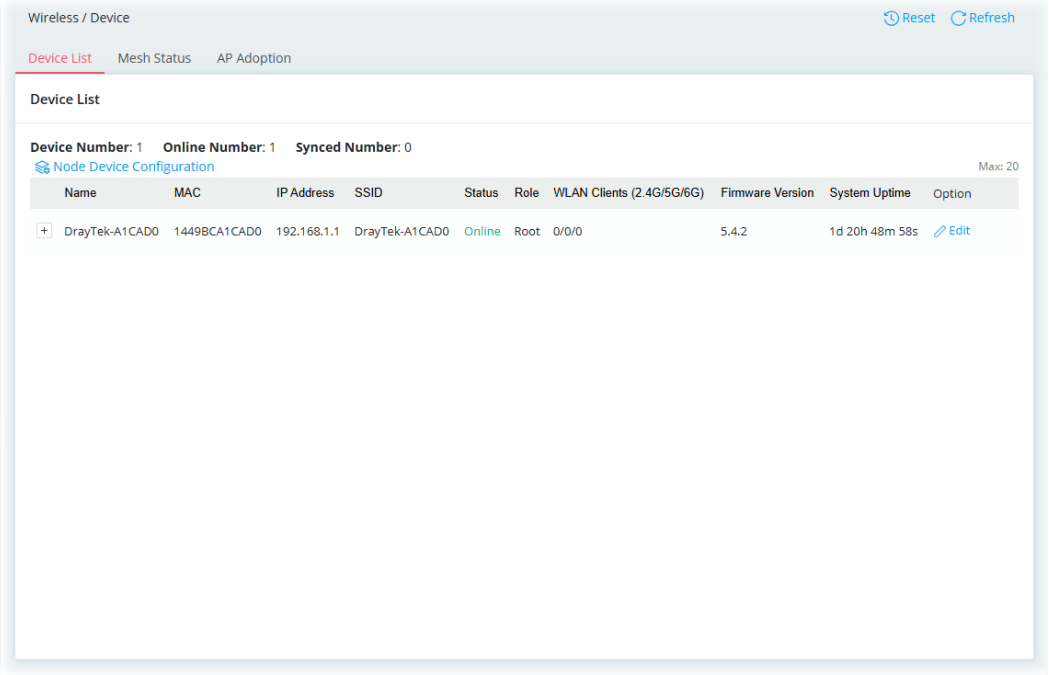
Optimization)	Sync 和 CFG Check 流程已成功完成。如果啟用此功能，在網狀網路環境發生變化（例如離線、斷開連接）後，主設備將執行自動重選以重建無線網狀網路。
日誌等級(Log Level)	此功能僅在進階設定啟用時(ON)才可使用。 選擇基本(Basic)或是詳細的(Detailed)。相關資訊將會顯示在 Syslog 中。
AP 管理設定(AP Management Setup)	
啟用(Enable) AP Management	切換此開關以啟用/停用 AP 管理功能。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

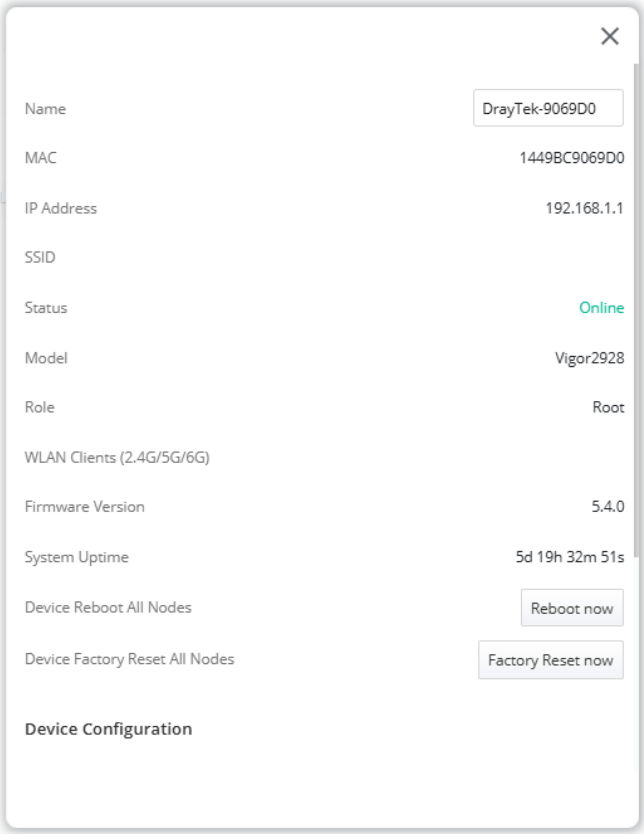
II-5-2 裝置(Device)

II-5-2-1 裝置清單(Device List)

本頁面將顯示有關此路由器偵測到的或由 Vigor 路由器的 AP 管理系統管理的 Vigor AP 裝置的一般資訊。



按下**編輯(Edit)**修改所選裝置的設定。根據網路值點根主點和節點的角色，AP 的設定略有不同。



可用設定說明如下：

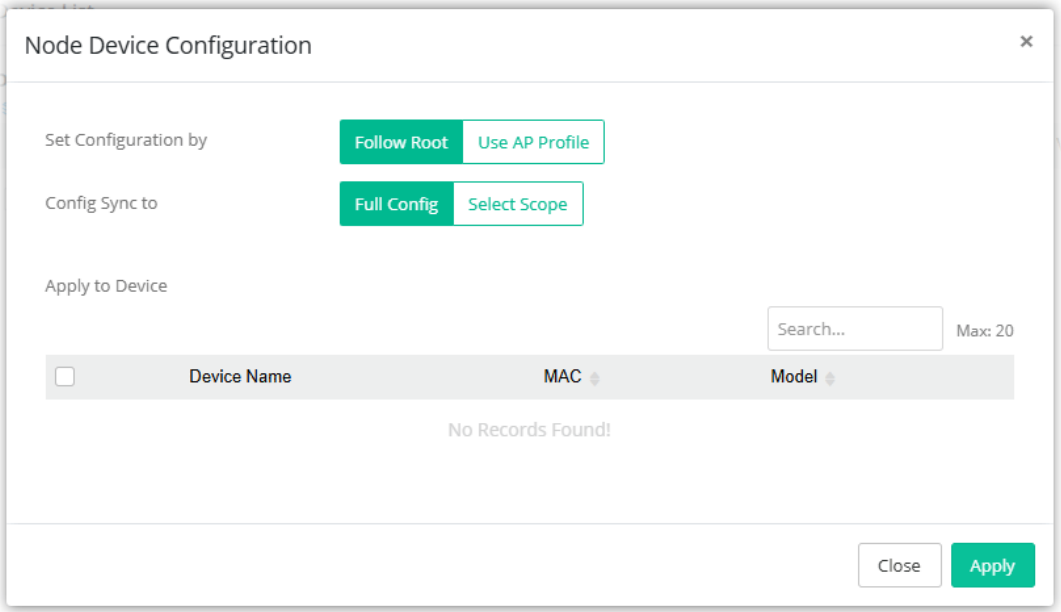
項目	說明
裝置重新啟動所有節點(Device Reboot All Nodes)	**立即重新啟動(Reboot Now)** – 按此立即重啟所有節點。
裝置回復所有節點之出廠預設值(Device Factory Reset All Nodes)	**立即回復出廠預設(Factory Reset No)** - 按此即可立即將所有節點重設為原廠之出廠設定值。
全部節點之設定同步(Config Sync to All Nodes)	**完整設定(Full Config)** – 將完整設定同步到所有節點。 **選擇範圍(Select Scope)** - 將選定的設定同步到所有節點。
同步設定(Sync Config)	**立即同步(Sync now)** – 按一下以執行同步配置。
裝置維護(Device Maintenance) – 適用 AP 節點	
管理帳號(Admin Account)	主節點使用這些設定來管理其 AP 節點。 選擇您需要的類型。 **預設值(Default) –** 使用**無線網路>>角色設定**(Wireless>>Role Setup)中設定的**群組管理帳號/群組管理密碼**(Group Admin Account / Group Admin Password)存取 AP 節點。 **客製化(Customize) –** 使用本頁面設定的**節點帳號/節點密碼**(Node Account / Node Password)存取 AP 節點。 在透過網路主點管理之前，如果節點的帳號和密碼已變更(非預設值)，請確保在此處將節點的帳號和密碼設定成與 AP 節點相同的值。否則，網路主點將沒有權限管理所選的 AP 節點。
節點帳號 **(Node Account)**	如果管理帳號已設定為**客製化(Customize)**，請輸入所選裝置的特定使用者帳號名稱。

	按下**套用(Apply)** 後，下次登入此裝置時，請輸入新的帳號名稱。
節點密碼 **(Node Password)**	如果管理帳號已設定為**客製化(Customize)**，請輸入所選裝置的特定使用者密碼。 按下**套用(Apply)**後，下次登入此裝置時，請輸入新的密碼。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下**套用(Apply)**按鈕儲存相關設定。

節點裝置設定(Node Device Configuration)

Vigor 路由器作為網狀網路主點，可同時管理多達 49 個網狀網路節點。這些節點可使用 Vigor 路由器定義的設定內容進行配置。透過節點裝置設定(Node Device Configuration)功能，可以方便地將預設配置套用到所有基地台。



可用設定說明如下：

項目	**說明**
設定配置方式(Set Configuration by)	有兩種模式可以套用到設定中： **依網路主點(Follow Root) –** 遵循網路主點的設定內容來套用。 ● **完整設定(Full Config) –** 將完整設定同步化到所有的節點中。 ● **選擇範圍(Select Scope) -** 將選擇的設定同步化到所有的節點中。 **使用 AP 設定檔(Use AP Profile) –** 選擇特定 AP 設定檔來套用其中的設定。 ● **AP 設定檔(AP Profile) -** 自下拉式清單中選擇一個 AP 設定檔。
套用至裝置(Apply to Device)	顯示可與此基地台的設定配合運用的 AP 裝置清單。
裝置名稱(Device Name)	顯示 AP 節點的裝置名稱。
MAC	顯示 AP 節點的 MAC 位址。
型號(Model)	顯示 AP 節點的型號名稱。
關閉(Close)	捨棄目前設定並離開此頁面。

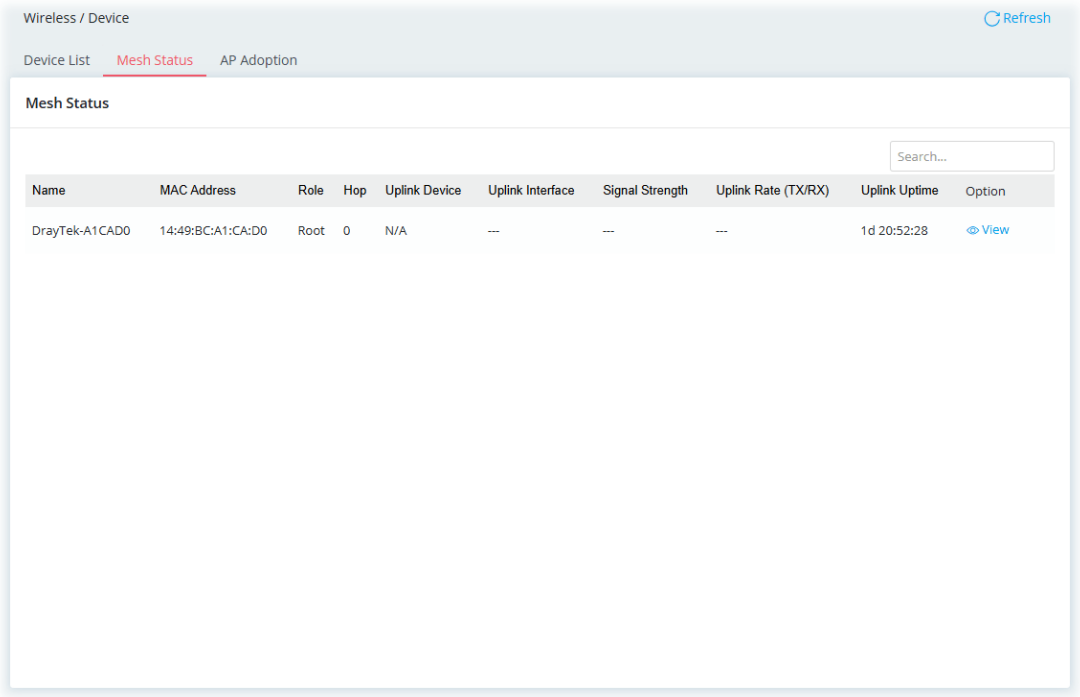
套用(Apply)	儲存目前的設定並離開此頁面。

完成設定之後，按下**套用(Apply)**按鈕儲存相關設定。

II-5-2-2 無線網狀網路狀態(Mesh Status)

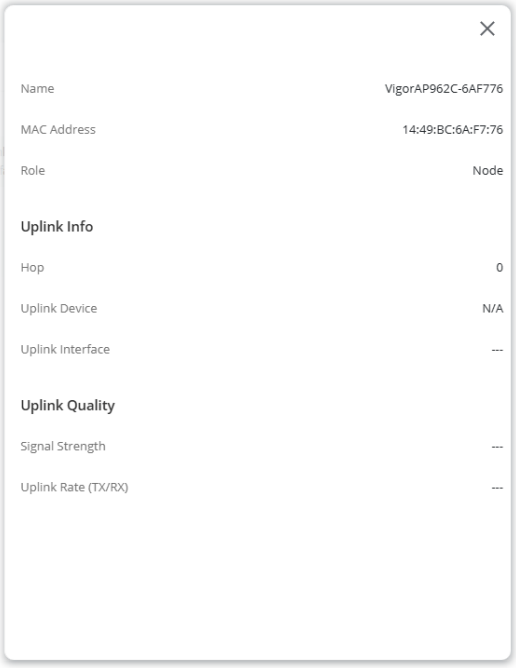
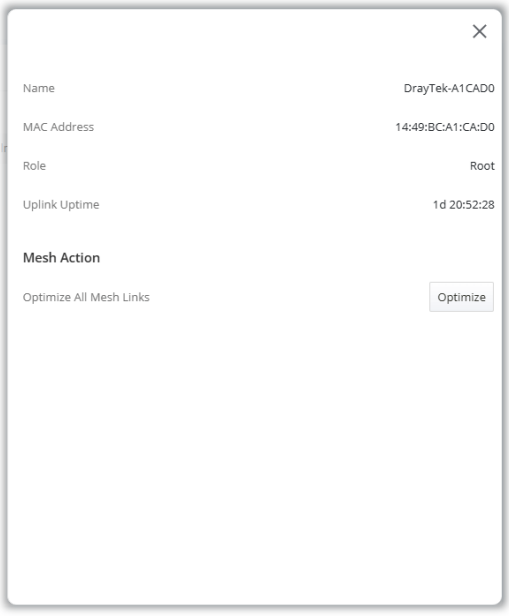
顯示無線網狀網路的一般訊息，包括網狀網路主點和網狀網路節點。

本頁僅在**啟用無線網狀網路(Enable Mesh**，在**虛擬控制器>>無線網路>>角色設定(Virtual Controller>>Wireless>>Role Setup))**為啟用狀態時可用。



可用設定說明如下：

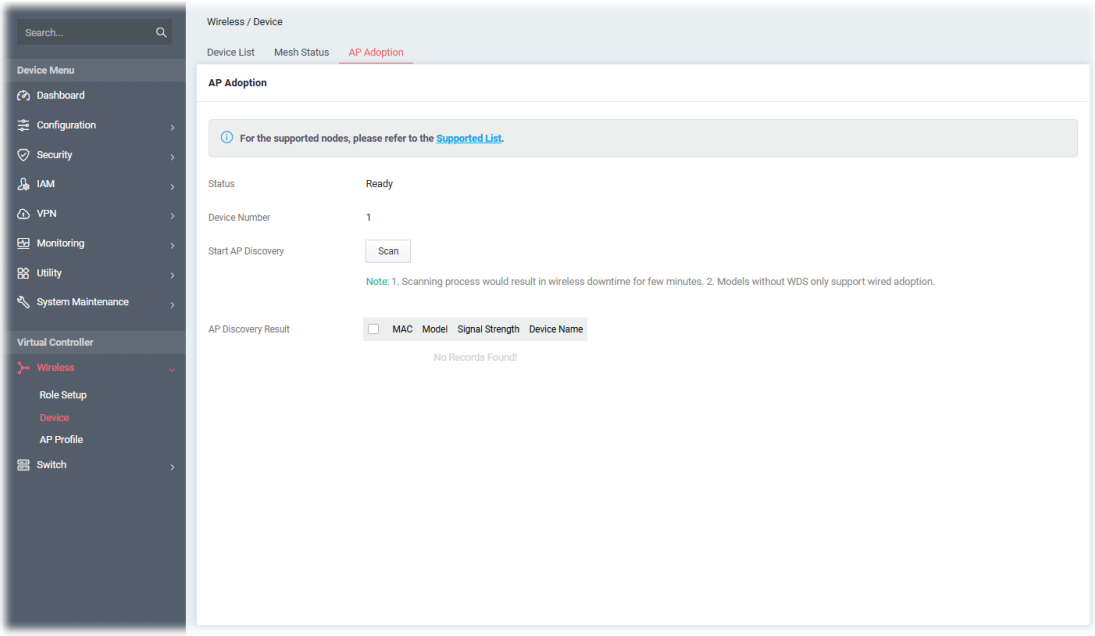
項目	說明
名稱(Name)	顯示此裝置的名稱(辨識之用)。
MAC 位址(MAC Address)	顯示此裝置的 MAC 位址。
角色(Role)	顯示此裝置的角色。
躍點(Hop)	顯示此裝置到無線主點的無線鏈結的數字。0 表示此裝置目前使用的是有線上行鏈路。
上行鏈路裝置(Uplink Device)	顯示此裝置連接的另一台裝置的 MAC 位址。
上行鏈路介面(Uplink Interface)	顯示此裝置用於連接上行鏈路的介面。
訊號強度(Signal Strength)	顯示此裝置與上行鏈路之間的訊號強度。
上行鏈路速率(傳送/接收)(Uplink Rate(Tx/RX))	只有當 VigorMesh 被選擇作為**無線網狀網路通訊協定(Mesh Protocol)**時，此功能才可使用。 顯示此裝置與其上行鏈路的連接速率。

上行鏈路運作時間(Uplink Uptime)	只有當 VigorMesh 被選擇作為**無線網狀網路通訊協定(Mesh Protocol)**時，此功能才可使用。 顯示此裝置在線上的時間。
選項(Option)	按下**檢視(View)** 可修改選定無線網狀網路裝置內容。   **優化全部的網狀網路鏈結(Optimize All Mesh Links)** - 只有當 VigorMesh 被選擇作為**無線網狀網路通訊協定(Mesh Protocol)**且此裝置的身分為無線網狀網路主點時，此功能才可使用。 按下**優化(Optimize)** 按鈕，執行重新選擇以重建網狀網路。

II-5-2-3 AP 納管(AP Adoption)

搜尋並在裝置群組中新增節點。

此頁面僅當目前設備角色(Current Device Role)為主點(Root)時可用。



可用設定說明如下：

項目	說明
狀態(Status)	顯示目前的掃描按鈕是否為可用狀態。
開始搜尋無線基地台(Start AP Discovery)	按下掃描按鈕可搜尋有無新的網路節點。
搜尋無線基地台結果(AP Discovery Result)	顯示掃描的結果。 **□** - 如果您想要新增某裝置到群組內，勾選裝置前面的核取方塊。 **MAC** - 顯示裝置的 MAC 位址。 **型號(Model)** - 顯示裝置的型號。 **訊號強度(Signal Strength)** - 顯示透過無線網路找到的裝置的訊號強度。 **裝置名稱(Device Name)** – 輸入裝置名稱以供識別。
取消 (Cancel)	捨棄目前設定。
套用 (Apply)	儲存目前的設定。

VigorMesh 網路設定提示

- VigorMesh 支援自動上行鏈路。如果裝置無法存取其閘道器，那麼該裝置會自動成為無線節點。.

  無線網狀網路主點(Mesh Root)或有線網狀網路節點(Mesh Node)應該能夠透過乙太網路 ping 其閘道器。

- VigorMesh 可以透過無線和有線方式為網狀網路群組增加新的網狀網路節點。但是，我們建議先使用乙太網路纜線將新節點連接到網路主點，然後再將其新增至網狀網路群組。

  等待設定同步完成，然後將節點移動到目標位置。

- VigorMesh 最多支援 3 個躍點。但是，還是建議連接 Mesh 網路時躍點數不超過 2 個。
- 建議使所有無線網狀網路節點的上行鏈路訊號強度大於 -65 dBm。
- 透過乙太網路線連接的無線網狀網路節點不應與其他節點形成環路。
- 如果網路主點消失，並且有設備角色為「自動」的線上有線網狀節點，則其中一個有線網狀節點將自動成為網路主點。
- VigorMesh 群組可透過**虛擬控制器>>無線網路>>裝置>>裝置清單**(**Virtual Controller >> Wireless >> Device >> Device List**)上的重設(Reset)按鈕重新設定。

  如果重新設定無線網狀網路主點(Mesh Root)
  - 所有的線上節點都會被重新設定
  - 無法主動被重新設定的節點，可以透過手動的方式重新設定

  如果重新設定無線網狀網路節點(Mesh Node)
  - 裝置會再度成為新的節點
  - 裝置的無線 SSID 設定也會被重新設定

故障排除：

- 檢查國碼以及無線頻道
- 檢查韌體版本，請務必確認所有的無線網狀網路成員皆使用最新的韌體版本
- 檢查裝置目前的裝置角色與目前的上行鏈結
- 確認裝置目前並未處於 DFS CAS 偵測階段
- 檢查頻道負載，確保不要超過 70%

EasyMesh 網路設定技巧

- 設定多個網狀網路設備，其上行鏈路 RSSI 值大於-65dBm
- 建議使用有線連接和設備清單進行設置，以便新增設備
- EasyMesh 網狀網路支援 3 個裝置躍點，但是建議躍點數少於或是等於 2 個即可
- 建議不要將 EasyMesh 加入現有的 VigorMesh 環境
- 裝置數量最大為 (ssid_num * device_num <= 56) -> 其中 device_num 指的是裝置數目

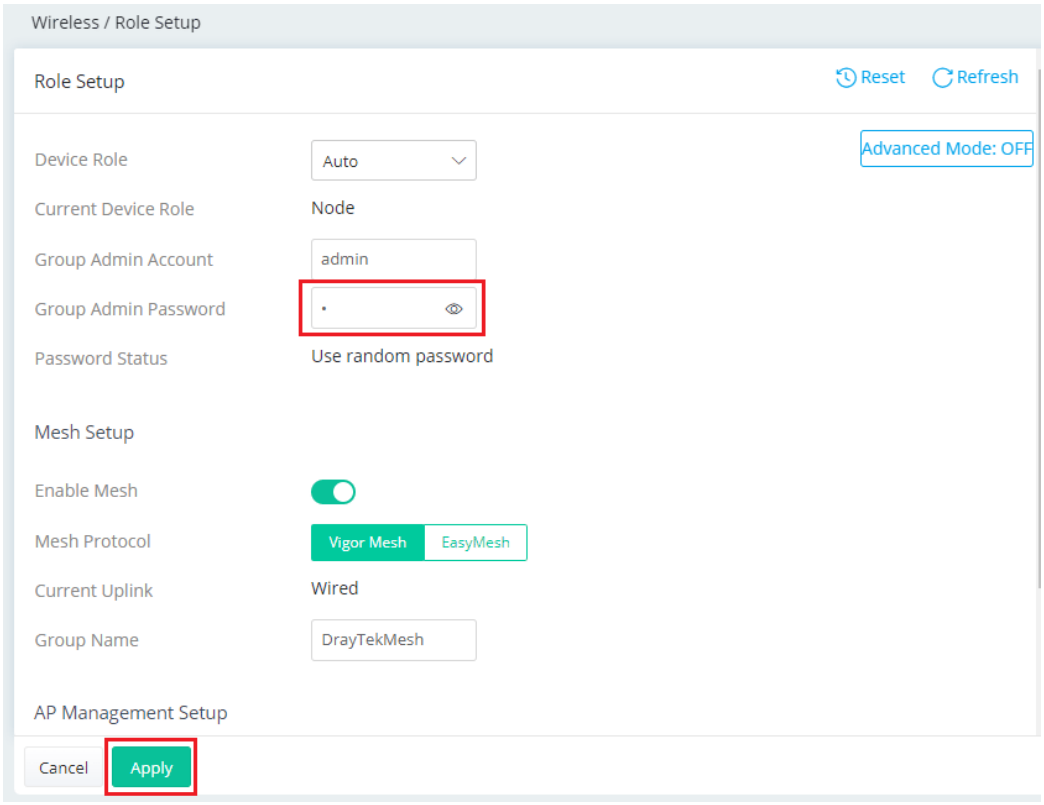
如何設定 VigorMesh 群組?

以下步驟引導您設定一個 VigorMesh 群組：

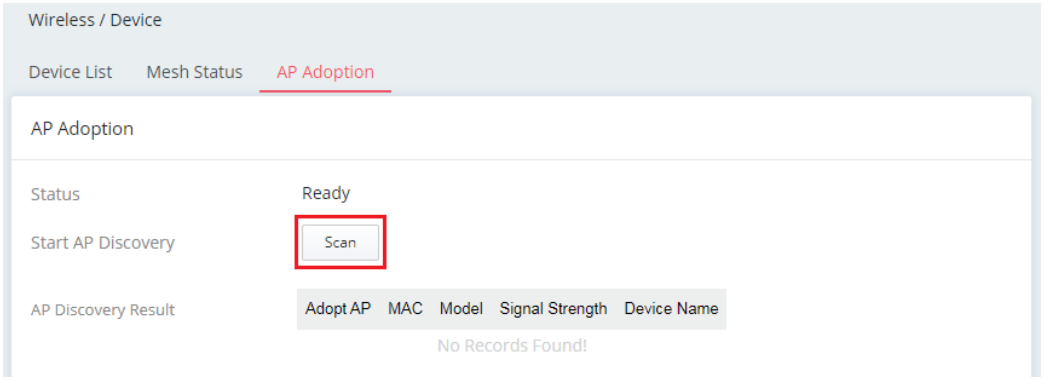
決定哪個裝置為網路主點後，登入該裝置的設定頁面。

1. (選項設定) 開**啟虛擬控制器>>無線網路>>角色設定(Virtual Controller>>Wireless>>Role Setup)**。

   設定**群組管理密碼(Group Admin Password)**。此設定值為節點加入網狀群組並完成設定同步後的管理者密碼。



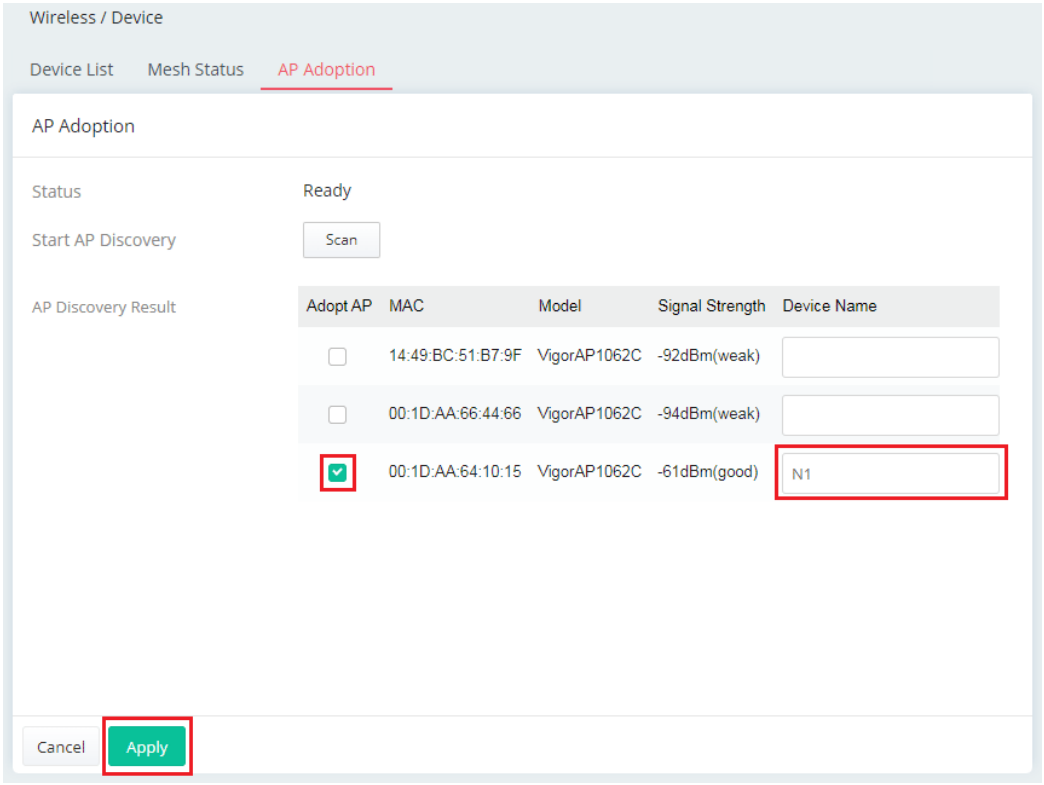
2. 開啟**虛擬控制器>>無線網路>>裝置>>AP 納管(Virtual Controller>>Wireless>>Device>>AP Adoption)**頁面，按下**掃描(Scan)**按鈕。



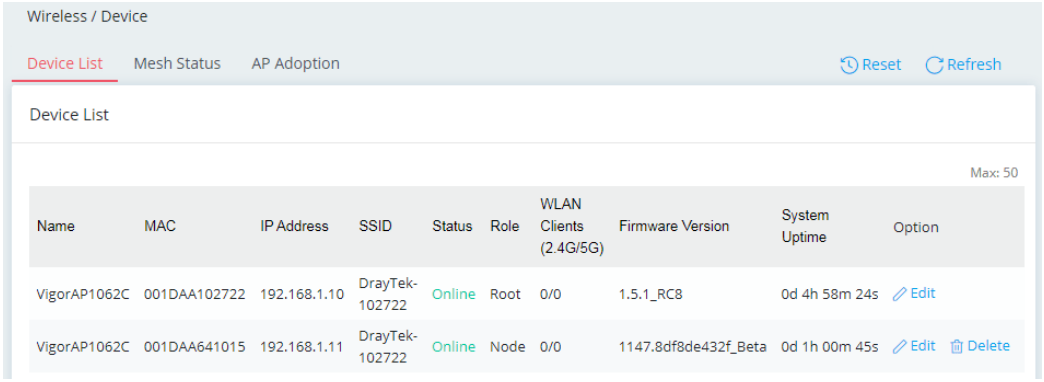
3. 稍待，直到掃描結果出現。

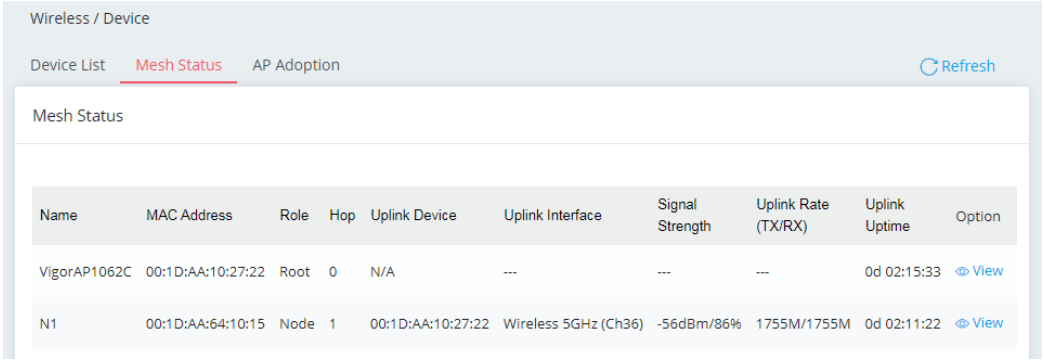
選擇您想要加入群組中的裝置，並輸入可供辨識的名稱。

按下**套用(Apply)**按鈕，等待系統完成加入流程。



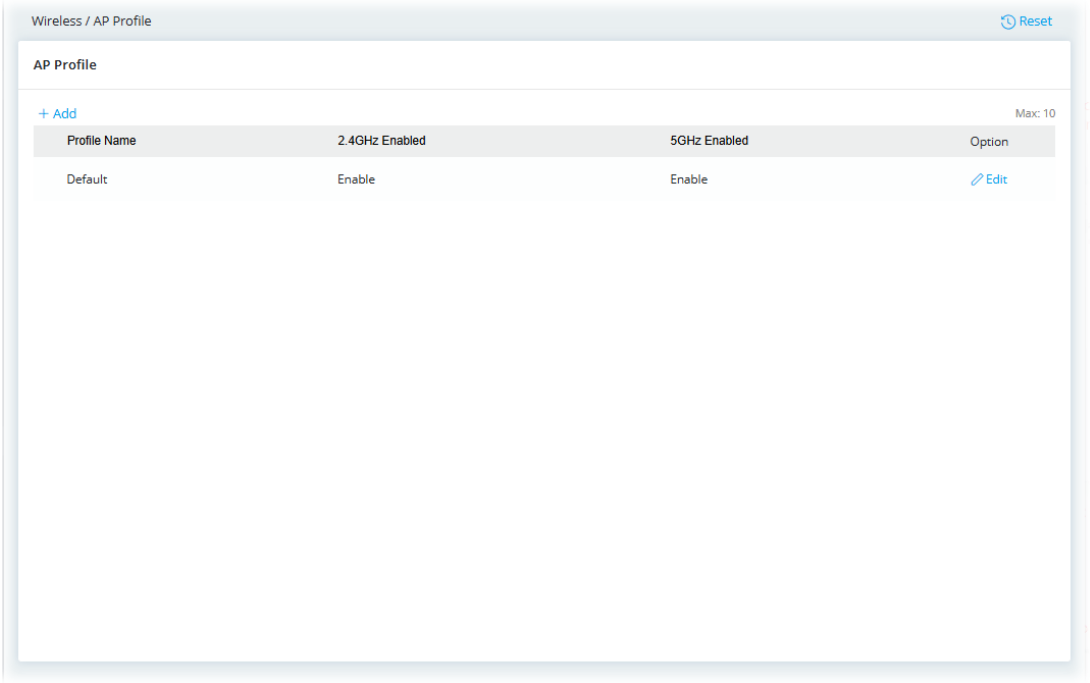
4. 參考**虛擬控制器>>無線網路>>裝置>>裝置清單(Virtual Controller>>Wireless>>Device>>Device List)** 以及**虛擬控制器>>無線網路>>裝置>>無線網狀網路狀態(Virtual Controller >> Wireless >> Device >>Mesh Status)**檢視結果。





II-5-3 AP 設定檔(AP Profile)

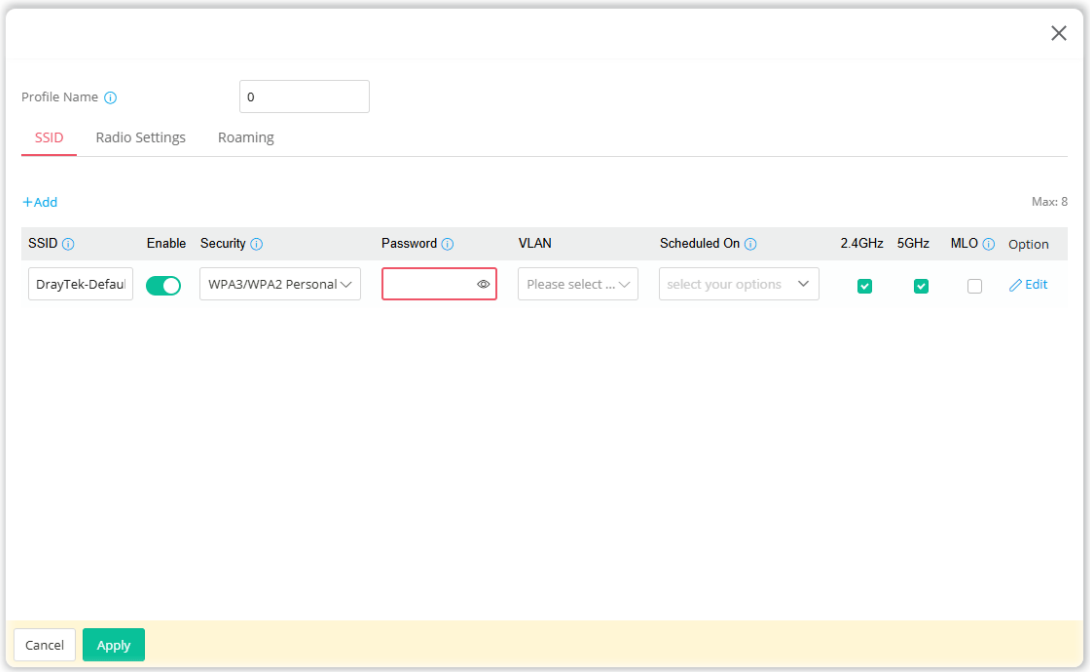
AP 設定檔主要是運用於選定的基地台。管理人員無需開啟基地台的網頁使用者介面，即可輕鬆設定基地台的相關網頁設定。



欲新增設定文件，請按**新增(+Add)**以建立具有各種 SSID、無線射頻設定和漫遊設定的 AP 設定檔。

II-5-3-1 SSID 設定

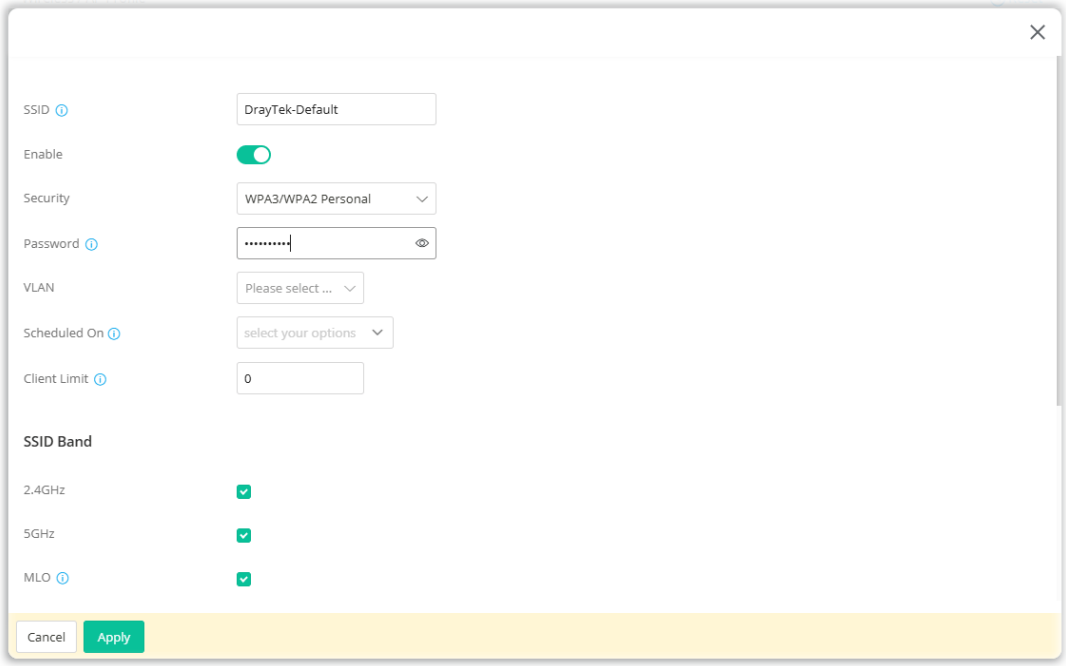
一個 AP 設定檔最多可以支援 8 個 SSID。



可用設定說明如下：

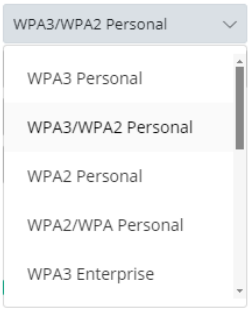
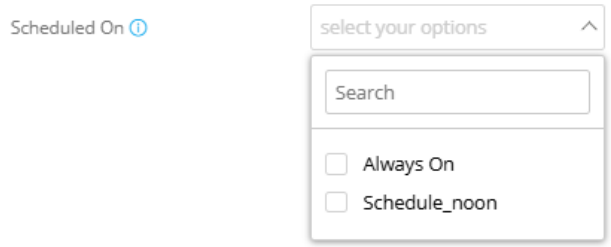
項目	說明
SSID	輸入名稱作為辨識 AP 之用。
啟用(Enable)	切換開關以啟用/停用此 SSID 設定。
安全性(Security)	選擇安全模式。
密碼(Password)	輸入 8~64 個 ASCII 字元。
VLAN	選擇此 SSID 歸屬的 VLAN。
排程啟用(Scheduled On)	此 SSID 設定檔將依照所選的排程設定強制啟用/停用。
2.4GHz/5GHz	選擇此 SSID 需要的頻段。
MLO	Wi-Fi 7 用戶端可以同時在不同的頻段上傳送和接收資料。 啟用至少兩個主網路頻段，並將模式設定為 802.11be（在無線射頻設定頁面中）。為此 SSID 選擇至少兩個頻段。
選項(Option)	**編輯(Edit)** – 按此可設定此 SSID 更細部的內容。

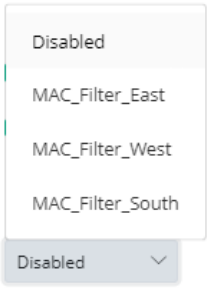
按下**編輯(Edit)**進行設定 SSID 細部的內容。



可用設定說明如下：

項目	說明
SSID	服務集識別碼（SSID），用以辨識基地台 AP 身分。最大長度為 32 個字元。 設定一個名稱，作為識別之用。
啟用(Enable)	切換開關以便啟用或停用該功能。
安全性(Security)	共有數個模式可以讓使用者選擇。 以下顯示具備高度安全性的模式; ● **WPA3 個人模式、WPA3/WPA2 個人模式、WPA2 個人模式、WPA2/WPA 個人模式(WPA3 Personal, WPA3/WPA2 Personal, WPA2 Personal, WPA2/WPA Personal)** – 僅接受 WPA 用戶端，加密金鑰應以 PSK 格式輸入。WPA 透過金鑰對無線網路發送的每個訊框進行加密，該金鑰是手動輸入到下方欄位中的密碼(Password)。 ● **WPA3 企業模式、WPA2 企業模式、WPA2/WPA 企業模式(WPA3**

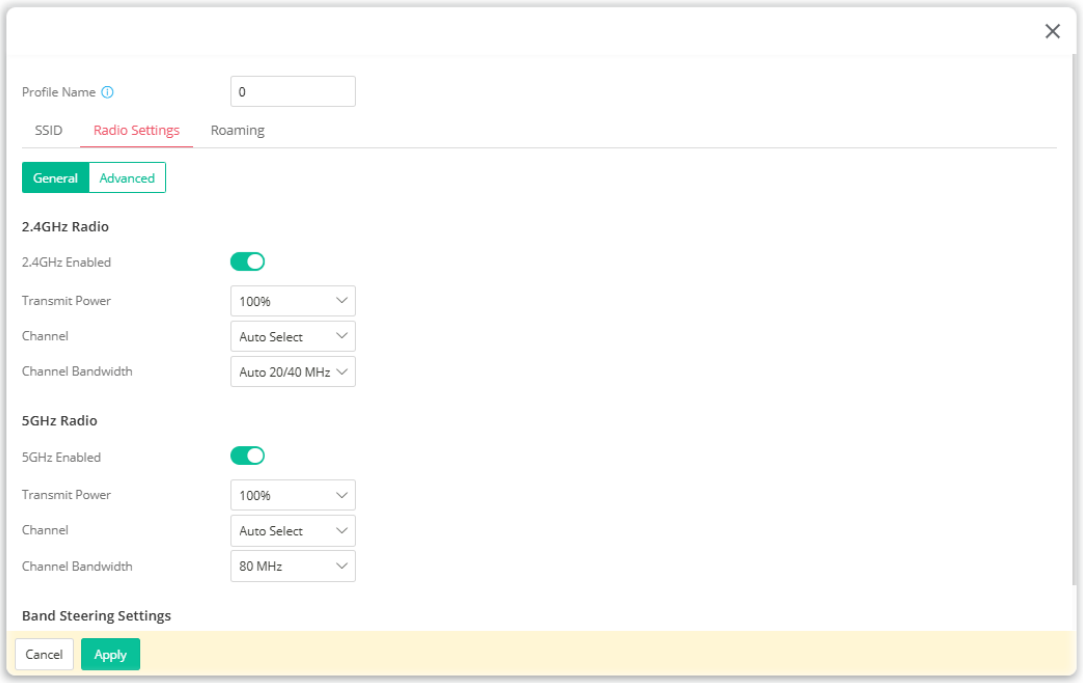
	**Enterprise, WPA2 Enterprise, WPA2/WPA Enterprise)** -僅接受 WPA 用戶端且驗證伺服器必須 在設定>>RADIUS/TACACS+>>外接 RADIUS(Configuration >> RADIUS/ TACACS+ >> External RADIUS)中設定妥當。WPA 使用金鑰對無線網路傳輸的每個訊框進行加密，該金鑰乃透過 802.1x 認證自動協商取得。 ● **OWE** - WPA3 還引入了一種新的開放且安全的連接模式：OWE。它允許客戶端無需密碼即可連接，非常適合熱點網路，但每個客戶端之間的連接在後台都經過獨特的加密來完成。 以下顯示具備基本安全性的模式; ● **WPA 個人模式(WPA Personal)** - 僅接受 WPA 用戶端，加密金鑰應以 PSK 格式輸入。WPA 透過金鑰對無線網路發送的每個訊框進行加密，該金鑰是手動輸入到下方欄位中的密碼(Password)。 ● **WPA 企業模式(WPA Enterprise)** - 僅接受 WPA 用戶端且驗證伺服器必須 在設定>>RADIUS/TACACS+>>外接 RADIUS(Configuration >> RADIUS/ TACACS+ >> External RADIUS)中設定妥當。WPA 使用金鑰對無線網路傳輸的每個訊框進行加密，該金鑰乃透過 802.1x 認證自動協商取得。 ● **無(None)** -關閉加密機制。
密碼(Password)	輸入 8~64 個 ASCII 字元，例如 "012345678"。此功能適用於 **WPA 個人模式(WPA Personal)** 或 **WPA2 個人模式(WPA2 Personal)** 或 **WPA2 / WPA 個人模式(WPA2 / WPA Personal)**、**WPA3 個人模式(WPA3 Personal)** 或 **WPA3/WPA2 個人模式(WPA3/WPA2 Personal)**。
VLAN	選擇此 SSID 歸屬的 VLAN。
排程啟用(Scheduled On)	 選擇永遠或是其他的排程設定檔。 **永遠連線(Always On)** - 此 WLAN 設定檔將始終處於活動狀態。 或是，請使用下拉式清單選擇預設的排程設定檔。選擇之前，請先前往**設定>>物件(Configuration>>Object)**頁面設定幾組排程設定檔(至少要有一組)。
用戶端限制(Client Limit)	設定允許透過此 SSID 設定檔連接到網際網路的用戶端數量。
SSID 頻(SSID Band)	
2.4GHz/5GHz	選擇此 SSID 需要的頻段。
MLO	Wi-Fi 7 用戶端可以同時在不同的頻段上傳送和接收資料。 啟用至少兩個主網路頻段，並將模式設定為 802.11be (在無線射頻設定頁面中) 。為此 SSID 選擇至少兩個頻段。
SSID 設定(SSID Settings)	
MAC 過濾清單(MAC Filtering List)	預設值是**停用(Disabled)**。 或是使用下拉式清單選擇預設的過濾設定檔。 選擇之前，請先前往**安全性>>MAC 過濾(Security>>MAC Filtering)**頁面建

	立至少一組的 MAC 過濾設定檔。 
隔離無線區域網路的用戶 (Isolate Client from Wireless)	切換開關以啟用/停用此功能。 此功能可使具有相同 SSID 的無線用戶端(站點)彼此之間無法相互存取。
隱藏 SSID (Hide SSID)	切換開關以啟用/停用 SSID 顯示功能。 此功能可防止無線訊號嗅探，並使未經授權的用戶端或 STA 更難加入您的無線區域網路。依照無線工具運用的不同，使用者在現場勘測時可能只能看到除 SSID 之外的訊息，或者根本看不到任何關於 VigorAP 1062C 的訊息。該系統允許您設定四組 SSID 以因應不同的用途。
WPA 設定(WPA Settings)	
金鑰更新間隔(Key Renewal Interval)	此功能僅適用與 WPA #相關之模式。 使用分享密鑰作為網路驗證之用，不過，在正常的網路操作中，乃是使用隨機產生的不同加密密鑰，此隨機產生的密鑰會定期更換，請在此輸入更新間隔時間，間隔時間若較短，可獲得較高的安全性，預設值為 3600 秒，設定若是 0 則表示關閉輸入功能。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下**套用(Apply)**按鈕儲存相關設定。

II-5-3-2 無線射頻設定(Radio Settings)

本頁面用於決定無線射頻的各項基本設定，例如模式、無線頻道及頻道頻寬等等。



可用設定說明如下：

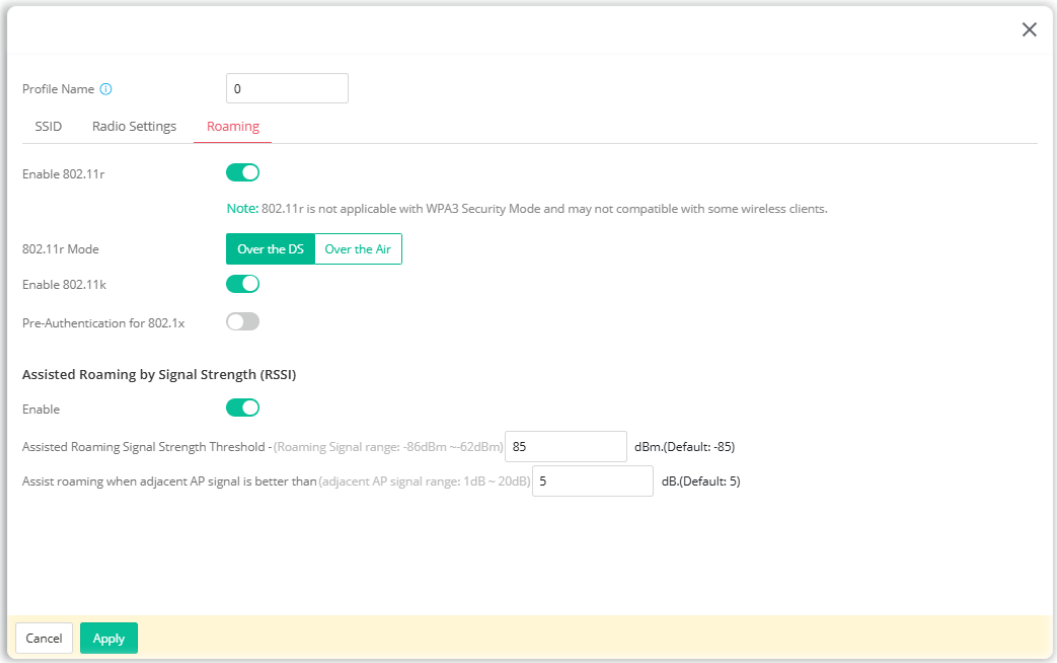
項目	說明
	2.4GHz 的基本設定
2.4GHz 啟用(2.4GHz Enabled)	切換開關以啟用/停用 2.4GHz 無線射頻設定。
傳輸功率(Transmit Power)	預設值為 100%。 降低數值可能會降低無線網路的覆蓋範圍和總處理量。
頻道(Channel)	無線區域網路的頻率頻道。 如果所選頻道受到嚴重干擾，您可以切換頻道。若您不知道如何選擇頻率，請選擇**自動選擇(Auto Select)**，讓系統自動為您選擇。
頻道頻寬(Channel Bandwidth)	**自動 20/40 MHz(Auto 20/40 MHz)** –本裝置會掃描相鄰區域的 AP 數量，使用 20 MHz(相鄰 AP 超過 10 個)或 40 MHz 作為基地台與無線用戶之間傳輸的資料速度，此選項可以增加資料傳輸的成效。 **20 MHz** - 本裝置使用 20 MHz 作為基地台與無線用戶之間傳輸的資料速度。 **40 MHz** - 本裝置使用 40 MHz 作為基地台與無線用戶之間傳輸的資料速度。
	5GHz 的基本設定
5GHz 啟用(5GHz Enabled)	切換開關以啟用/停用 5GHz 無線射頻設定。
傳輸功率(Transmit Power)	設定基地台傳輸訊號的百分比，預設值為 100%。 降低數值可能會降低無線網路的覆蓋範圍和總處理量。
頻道(Channel)	無線區域網路的頻率頻道。 如果所選頻道受到嚴重干擾，您可以切換頻道。若您不知道如何選擇頻率，

	請選擇**自動選擇(Auto Select)**，讓系統自動為您選擇。
頻道頻寬(Channel Bandwidth)	**20 MHz** -本裝置使用 20 MHz 作為基地台與無線用戶之間傳輸的資料速度。 **40 MHz** -本裝置使用 40 MHz 作為基地台與無線用戶之間傳輸的資料速度。 **80 MHz** -本裝置使用 80 MHz 作為基地台與無線用戶之間傳輸的資料速度。 **160 MHz** -本裝置使用 160 MHz 作為基地台與無線用戶之間傳輸的資料速度。
頻段引導設定(Band Steering Settings)	
5Ghz 用戶端最小 RSSI (5Ghz Client Minimum RSSI)	如果啟用此功能，VigorAP 將在限定的時間內偵測無線用戶端是否支援雙頻。 此無線站點具備 5GHz 網路連線能力，但訊號效能可能不理想。因此，當無線站點連接到 VigorAP 時，如果訊號強度低於此處設定的值，VigorAP 將允許用戶端連接到 2.4GHz 網路。
進階(Advanced)	
片段長度(Fragment Length)	設定無線射頻的片段門檻值。預設值為 2346。如果您不知道效果為何，請勿修改預設值。
RTS 門檻值(RTS Threshold)	縮減隱藏站點之間的衝突(單位為位元組)，以提高無線效能。 設定無線射頻的 RTS 門檻值。預設值為 2347。如果您不知道效果為何，請勿修改。
國家代碼(Country Code)	僅適用 2.4GHz。 VigorAP 遵循 802.11d 標準廣播國家/地區代碼。但部分無線站點會偵測/掃描國家代碼以避免衝突發生。如果偵測到了衝突，無線站點將收到警告，並且無法建立網路連線。因此，變更改國家/地區代碼以確保網路連線成功，對某些用戶來說就很有必要。
支援 WMM (WMM Capable)	WMM 為 Wi-Fi Multimedia 的縮寫，定義從 802.1e 衍生的四種存取類型錄的優先層級，這些類型都是針對流量、聲音、影像特別設計的，此四種類型分別是 - AC_VO, AC_VI, AC_BE 與 AC_BK。 在無線資料傳輸中應用 WMM 參數，切換此開關以啟用/停用此功能。
支援 APSD (APSD Capable)	自動省電模式(APSD, automatic power-save delivery)是 Wi-Fi 網路支援的強化省電機制，允許裝置花較多時間休眠，並透過縮小傳輸延遲時間，花費少許電力來改善成效。
無線頻寬均化(Airtime Fairness)	切換此開關以啟用/停用此功能。 在服務品質層級一定的條件下，每個用戶端都享有同等的網路空中流通時間。因此在特定的環境中，此功能可以降低慢速無線裝置的不良影響，且可改善全面無線網路的成效。 適合環境： (1) 多個無線用戶 (2) 所有的無線用戶主要都是進行下載作業 (3) 成效的瓶頸主要在無線連線上
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下**套用(Apply)**按鈕儲存相關設定。

II-5-3-3 漫遊(Roaming)

單一無線存取裝置的網路訊號往往受限於訊號的涵蓋範圍。因此，如果您想要在一個大型展場上延伸並擴充無線網路的覆蓋範圍，您可以安裝數台無線存取裝置於展場上，同時啟用每台裝置的漫遊功能，如此一來，就可以達成無縫連接無線網路，從而擴充無線訊號範圍。



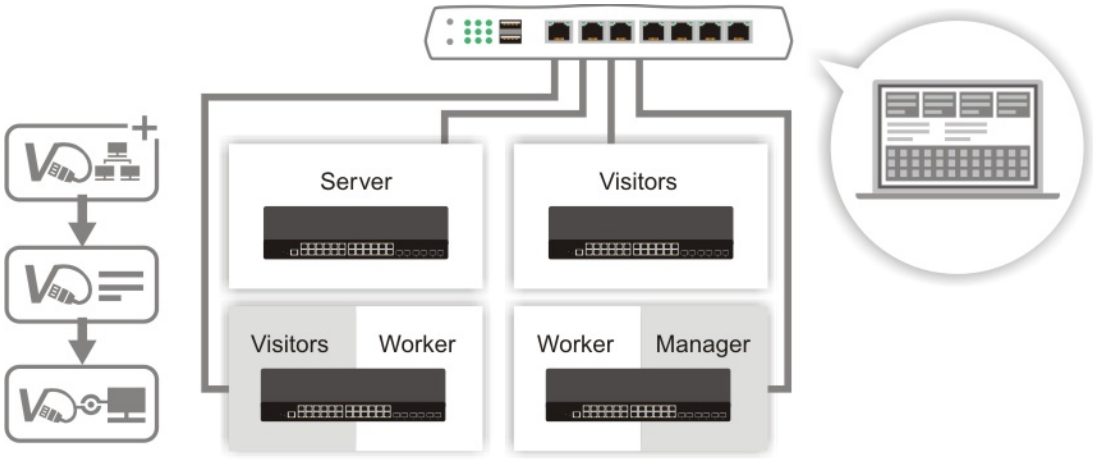
可用設定說明如下：

項目	說明
啟用 802.11r (Enable 802.11r)	切換此開關以啟用/停用 802.11r 協定快速漫遊功能，讓無線用戶端在熱點之間能快速與安全地切換。
802.11r 模式 (802.11r Mode)	**透過 DS (Over the DS)** - 因應訊號強度的變更，用戶端可以利用 Action Frames (FT 需求與 FT 回應) 透過原本的 AP 與其他的 AP 進行通訊。 **透過 OTA(Over The Air)** - 因應訊號強度的變更，用戶端可以利用漫遊驗證演算式直接與其他的 AP 通訊(無須在每一個 AP 中不斷的重新驗證)。
啟用 802.11k (Enabled 802.11k)	切換開關以啟用 802.11k 協定 (也稱為無線資源管理 (RRM))。啟用後，基地台將優化無線網路的效能。
利用訊號強度(RSSI)輔助漫遊(Assisted Roaming by Signal Strength (RSSI))	
啟用(Enable)	切換此開關以啟用/停用此功能。 當無線用戶端的連接速率過低，或無線用戶端接收到的訊號過差時，Vigor 路由器將會自動偵測(基於連接速率和 RSSI 要求)，並切斷該無線用戶端的網路連接，以幫助其連接到另一個無線基地台取得更好的訊號。
輔助漫遊訊號強度門檻值 (Assisted Roaming Signal Strength Threshold)	當無線用戶端的訊號強度低於此處設定的值(dBm)，且 Vigor 路由器偵測到相鄰 AP (必須是 DrayTek 路由器/AP，且也支援此功能)的訊號強度較高(該值在**輔助漫遊，當相鄰 AP 基地台訊號優於此門檻值時**(Assist roaming when adjacent AP signal is better than)欄位中定義)時，Vigor 路由器將會中斷該無線用戶端的網路連線。之後，該無線用戶端即可連接到相鄰的 AP(具有更好的 RSSI)。
輔助漫遊，當相鄰 AP 基地台訊號優於此門檻值時 (Assist roaming when adjacent AP signal is better than)	指定一個數值作為門檻值。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前的設定並離開此頁面。

完成設定之後，按下**套用(Apply)**按鈕儲存相關設定。

II-6 虛擬控制器 – 交換器(Virtual Controller – Switch)

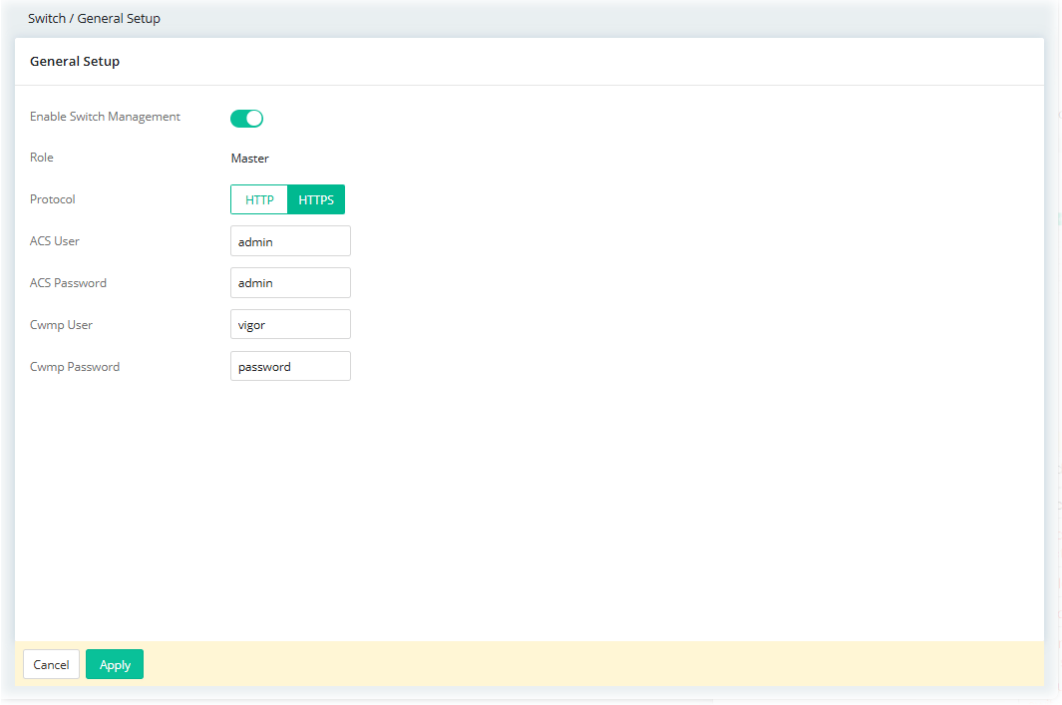
Vigor 路由器可以管理與其連接的大量 VigorSwitch 設備。管理員可以透過設定檔和群組設定，一次執行 VigorSwitch 設備的韌體/設定備份、還原、重新啟動設備或恢復出廠設定等操作。



此功能可讓使用者建立和管理透過無線或有線連接的 DrayTek 裝置。

II-6-1 基本設定(General Setup)

在此頁面中，切換開關以啟用/停用交換器管理功能。



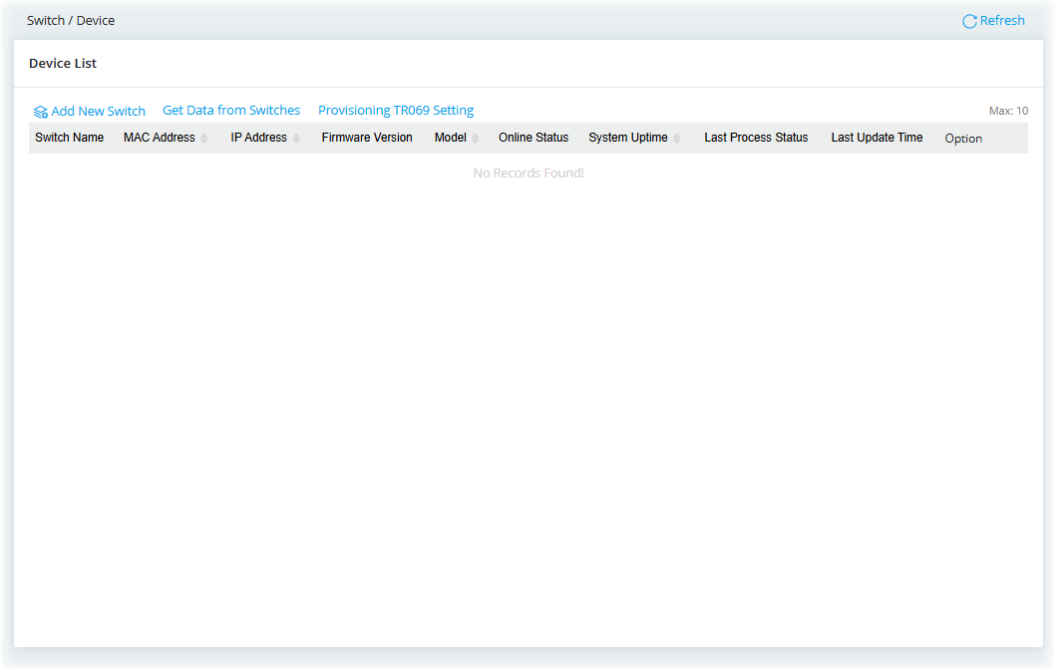
可用設定說明如下：

項目	說明

啟用交換器管理(Enable Switch Management)	切換開關以啟用或停用交換器管理功能。
角色(Role)	顯示裝置的角色。
通訊協定(Protocol)	選擇 HTTP 或 HTTPS 作為連接到此路由器之通訊協定。
ACS 使用者(ACS User)	輸入 Vigor 交換器連接到 ACS 伺服器所需的使用者名稱。 此處設定的使用者名稱將與此路由器管理的交換器同步。(此使用者名稱應與 VigorSwitch 交換器的 ACS 伺服器在系統維護>>存取管理>>TR-069(System Maintenance >> Access Management >> TR-069)下設定的使用者名稱一致)。
ACS 密碼（ACS Password)	輸入 Vigor 交換器連接到 ACS 伺服器所需的密碼。 此處設定的密碼將與此路由器管理的交換器同步。(此密碼應與 VigorSwitch 交換器的 ACS 伺服器在系統維護>>存取管理>>TR-069(System Maintenance >> Access Management >> TR-069)下設定的密碼一致)。
Cwmp 使用者(Cwmp User)	請輸入 Vigor 路由器連接到此交換器所需的使用者名稱。(此使用者名稱應與 VigorSwitch 交換器的 ACS 伺服器在系統維護>>存取管理>>TR-069(System Maintenance >> Access Management >> TR-069) 下的 CPE 設定中的使用者名稱一致。)
Cwmp 密碼(Cwmp Password)	請輸入 Vigor 路由器連接到此交換器所需的密碼。 (該密碼應與 Vigor 交換器的系統維護>>存取管理>>TR-069(System Maintenance >> Access Management >> TR-069)下的 CPE 設定中之密碼一致。)
取消(Cancel)	捨棄目前設定。
套用(Apply)	儲存目前設定。

II-6-2 裝置(Device)

此頁面顯示連接到 Vigor 路由器的 VigorSwitch 的訊息，包括交換器名稱、MAC 位址、IP 位址、韌體版本、型號、線上狀態、系統運行時間、連接埠使用情況、用戶端、最後處理狀態和選項等等。

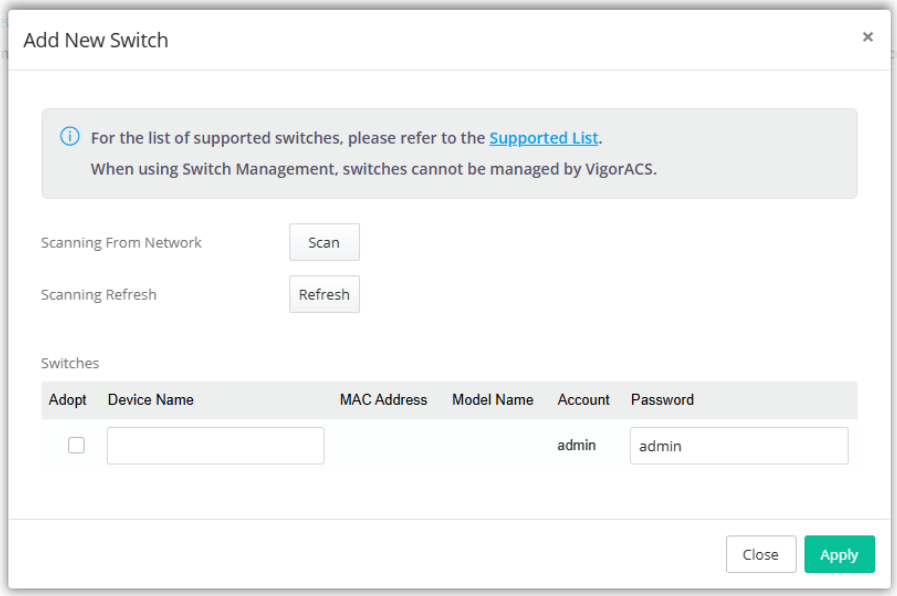


可用設定說明如下：

項目	說明
新增交換器(Add New Switch)	按此新增一台新的交換機，由 Vigor 路由器進行管理。
自交換器取得資料(Get Data from Switches)	按此以取得與 Vigor 路由器管理的所有交換器相關的新資訊(例如：交換器名稱、MAC 位址、IP 位址等) 。
佈建 TR069 設定(Provisioning TR069 Setting)	按此將 TR-069 設定檔內的設定(包括協定類型、ACS 使用者名稱、ACS 密碼、CPE 使用者名稱和 CPE 密碼)傳送至 Vigor 路由器管理的所有交換器上。
選項(Option)	**編輯(Edit)** –修改所選 Vigor 交換器的設定。 **刪除(Delete)** – 按此以移除選定的 Vigor 交換器。 **取得(Get)** – 按此以將 IP 位址指派給選定的 Vigor 交換器。

新增交換器

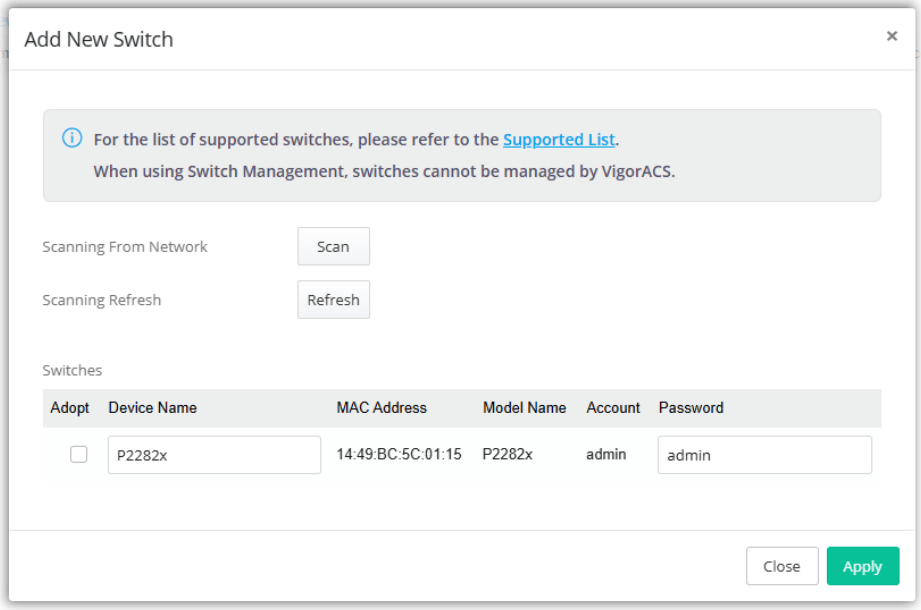
1. 若要新增交換器，請按一下**新增交換器(Add New Switch)**鏈結以開啟如下頁面。



可用設定說明如下：

項目	說明
掃描(Scan)	在 Vigor 路由器附近尋找交換器。找到的交換器將顯示在交換器表格清單中。
頁面更新(Refresh)	重新顯示交換器表格。
納管(Adopt)	選擇要由 Vigor 路由器管理的 Vigor 交換器。
裝置名稱(Device Name)	顯示 Vigor 交換器的名稱。
密碼(Password)	顯示此 Vigor 交換器的登入密碼。
關閉(Close)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定。

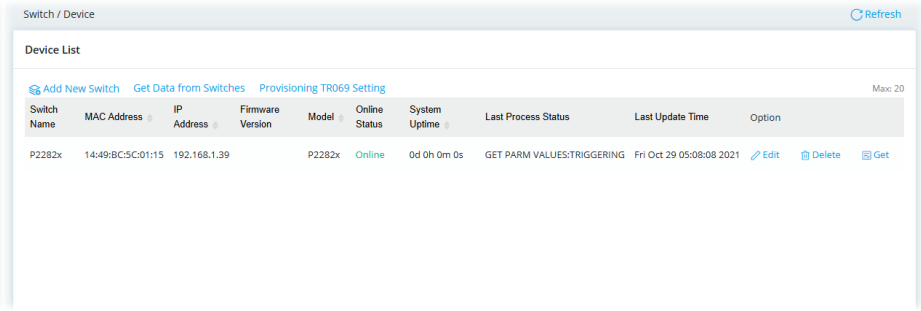
2. 按一下**掃描(Scan)**並稍等片刻，Vigor 路由器將掃描並列出連接到 Vigor 路由器的交換器。



3. 請勾選**納管(Adopt)**下方的方框。選擇所需的裝置並按下**套用(Apply)**。

   注意：如果此處顯示的密碼與 VigorSwitch 登入密碼不同，請將其修改為與 VigorSwitch 中使用的密碼一致。

   選定的交換器將顯示在裝置清單中，如下所示。

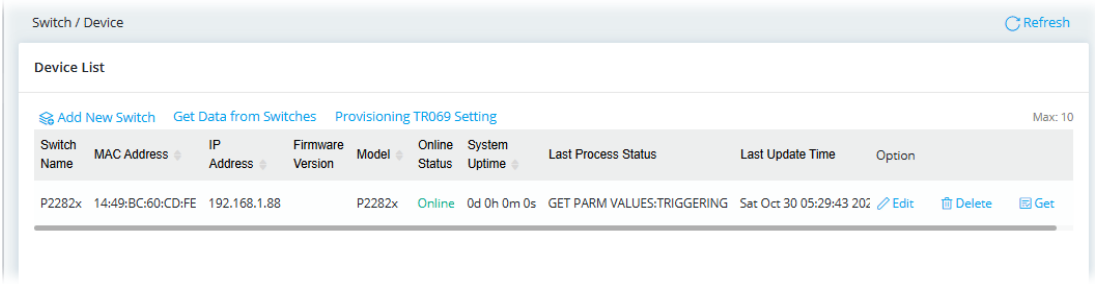


   注意：如果**線上狀態(Online Status)**顯示為斷線(Offline)，請按**取得(Get)**以獲取 Vigor 路由器指派的 IP 位址。

4. 當**線上狀態(Online Status)**顯示為線上(Online)。選定之交換器即由 Vigor 路由器管理。

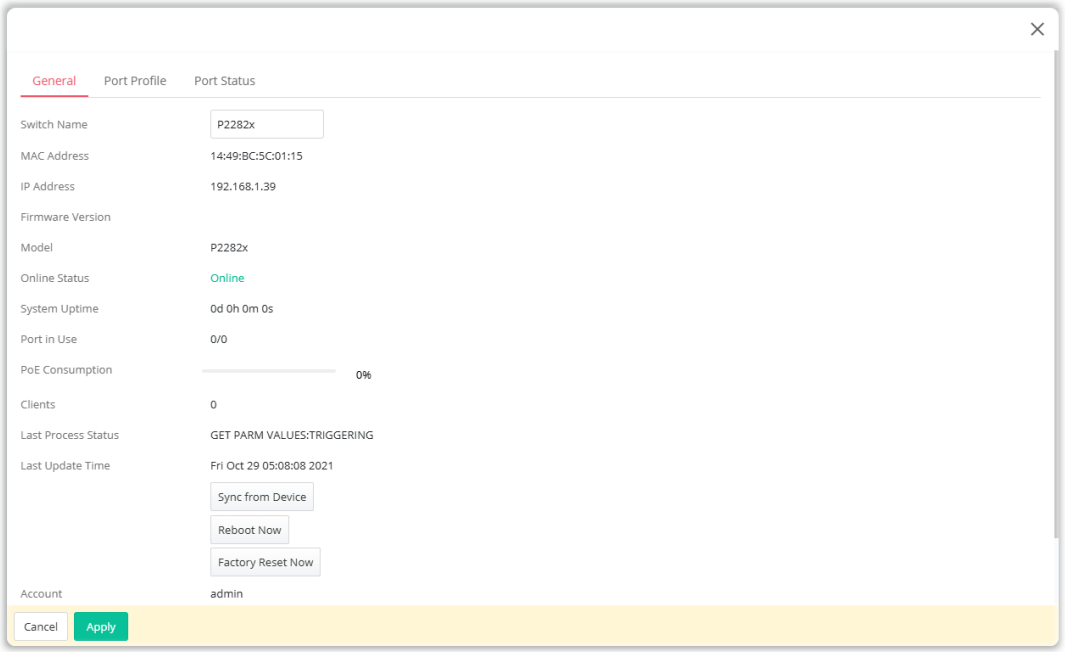
編輯交換器設定

若要編輯裝置資訊、設定連接埠設定檔或查看交換器的連接埠狀態，請按一下**編輯(Edit)**。



基本(General)

此頁面顯示有關 VigorSwitch 的摘要資訊。此外，它還提供立即重新啟動(Reboot Now)和立即回復出廠預設(Factory Reset Now)按鈕，以幫助用戶更新交換器。



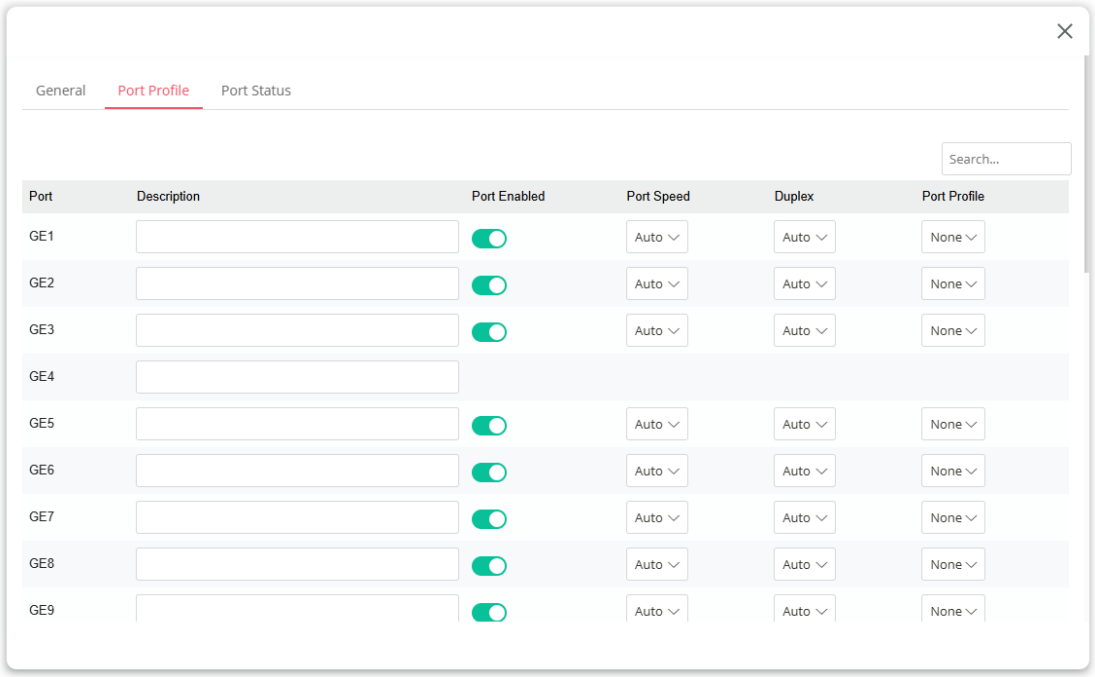
可用設定說明如下：

項目	說明
交換器名稱(Switch Name)	顯示交換器的名稱。如有需要，可變更名稱。
從設備同步(Sync from Device)	按此取得與此交換器相關的新資訊 (例如，交換器名稱、MAC 位址、IP 位址等) 。
立即重新啟動(Reboot Now)	按一下即可使用目前設定立即重新啟動交換器。
立即回復出廠預設(Factory Reset Now)	按此即可將交換器恢復出廠預設值。
密碼(Password)	此處顯示的密碼必須與 Vigor 交換器的登入密碼一致。否則，Vigor 路由器將無法管理所選定之交換機，且連接埠設定檔和連接埠狀態亦可能無法準確顯示。 **佈建 CWMP 設定(Provisioning CWMP Conf)** – 按一下可將 TR-069 設定從 Vigor 路由器傳送到交換器上 (請確保交換器由 Vigor 路由器管理) 。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

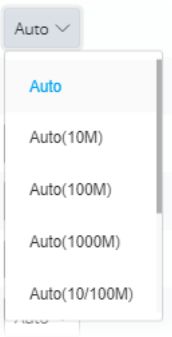
完成設定之後，按下套用(Apply)按鈕儲存相關設定。

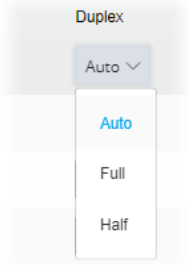
埠口設定檔(Port Profile)

此頁面可設定 VigorSwitch 的每個 GE 連接埠的速度、雙工模式和連接埠設定檔。



可用設定說明如下：

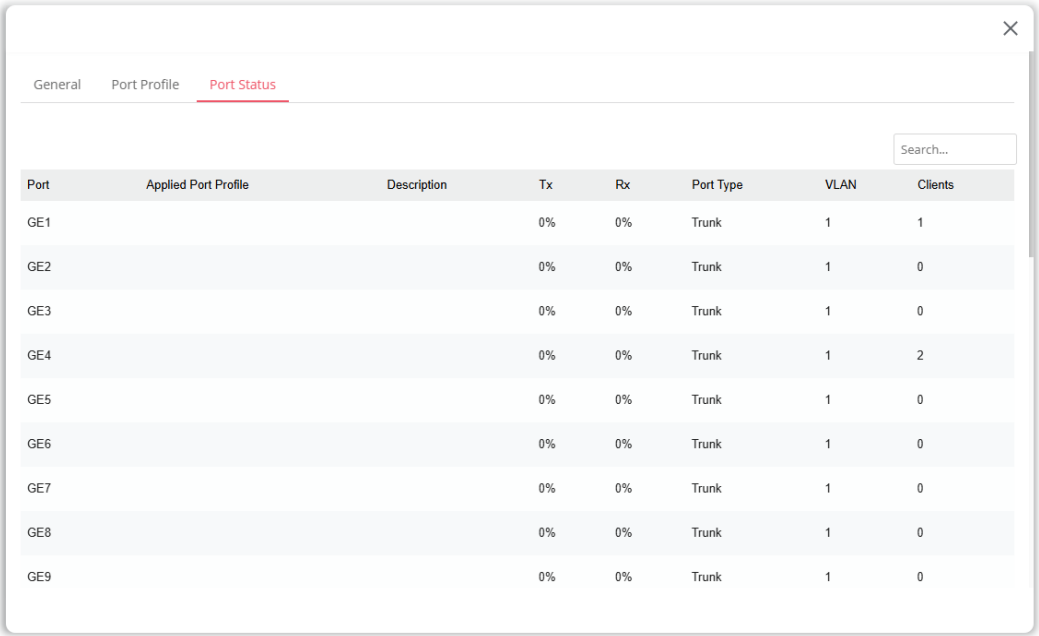
項目	說明
埠口(Port)	顯示 GE 連接埠號碼。
說明(Description)	如有需要，請輸入簡要說明，解釋透過 LAN 連接埠連接到 VigorSwitch 的裝置。
埠口啟用(Port Enabled)	用於連接 VigorSwitch 和 Vigor 路由器的連接埠口(例如，本例中的 GE2) 不會被 Vigor 路由器關閉。 VigorSwitch 的其他 LAN 連接埠允許連接到任何 LAN 裝置上。勾選該部口後，按下套用(Apply)後。該裝置與 VigorSwitch 之間的網路連線將被終止。
埠口速度(Port Speed)	乙太網路速度由路由器系統自動設置，也可以手動設定為 10M/100M/1000M 位元/秒。  連接埠速度能力： • **自動(Auto):** 自動速度，具備所有功能。 • **Auto(10M):** 僅限具備 10M 能力的自動速度。 • **Auto(100M):** 僅限具備 100M 能力的自動速度。 • **Auto(1000M):** 僅限具備 1000M 能力的自動速度。

	• **Auto(10/100M):** 僅限具備 10/100M 能力的自動速度。 • **10M:** 強制使用 10 M 連線速度。 • **100M:** 強制使用 100 M 連線速度。 • **1000M:** 強制使用 1000 M 連線速度。 選擇自動(自動協商)模式後，交換器上的連接埠將自動與對端連接埠協商，以獲得雙方都支援的連線速度和雙工模式。啟用自動協商後，交換器上的連接埠將自動與對端連接埠協商，以決定連線速度和雙工模式。如果對端連接埠不支援自動協商或已關閉此功能，交換器將透過偵測網路線訊號並使用半雙工模式來確定連線速度。如果交換器的自動協商功能已關閉，則連接埠在建立連線時將使用預設的速度和雙工模式，因此需要確保對端連接埠的設定與交換器相同才能成功連線。 對於 SFP 光纖模組，您可能需要手動配置速度以符合光纖模組的速度。
雙工(Duplex)	選擇 LAN 連接埠的雙工模式。 **自動(Auto)** – 自動雙工模式，具備所有功能。 **全(Full)** – 僅限具備 10/100/1000M 能力的自動速度。所有數據傳送皆可雙向資料傳輸。 **半(Half)** - 僅限具備 10/100M 能力的自動速度。所有數據傳送皆可雙向資料傳輸。但是，一次僅有一台裝置(路由器本身或是對方裝置)允許進行資料傳輸。 
埠口設定檔(Port Profile)	選擇一個 VigorSwitch LAN 埠口可套用的埠口設定檔。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

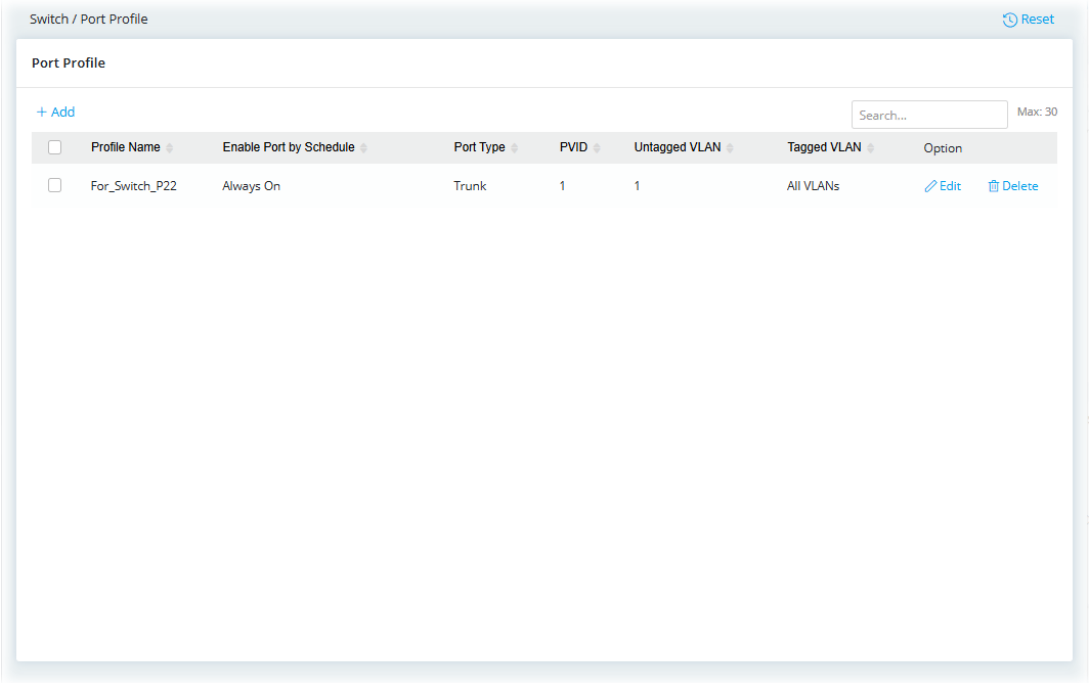
埠口狀態(Port Status)

此頁面將顯示 Vigor 交換器的每個 GE 連接埠的目前狀態，例如傳輸速率(TX/RX)、連接埠類型、VLAN ID、應用程式的連接埠設定檔等。


General
Port Profile
Port Status
Search...
Port
Applied Port Profile
Description
Tx
Rx
Port Type
VLAN
Clients
GE1 0% 0% Trunk 1 1
GE2 0% 0% Trunk 1 0
GE3 0% 0% Trunk 1 0
GE4 0% 0% Trunk 1 2
GE5 0% 0% Trunk 1 0
GE6 0% 0% Trunk 1 0
GE7 0% 0% Trunk 1 0
GE8 0% 0% Trunk 1 0
GE9 0% 0% Trunk 1 0

II-6-3 埠口設定檔(Port Profile)

此頁面可讓您設定埠口設定檔，包含 VigorSwitch 連接到此 Vigor 路由器時所需的基本設定，例如名稱、群組、IP 位址、MAC 位址、型號和密碼。

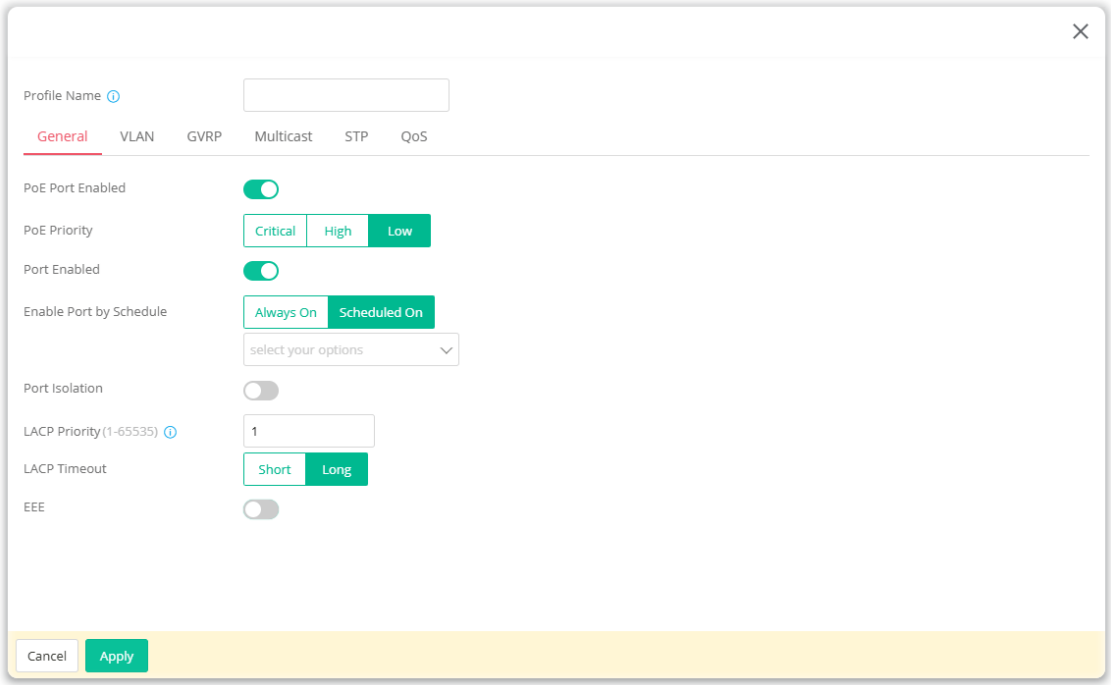


若要新增個人資料，請按下**+新增(+Add)**。若要修改現有設定文件，請選擇該設定檔並按一下**+編輯(+Edit)**鏈結開啟設定頁面。

按下**+新增(+Add)**後，下方顯示的是設定頁面。

基本(General)

此處顯示的可用設定會因 Vigor 路由器管理的 VigorSwitch 而有所不同。



可用設定說明如下：

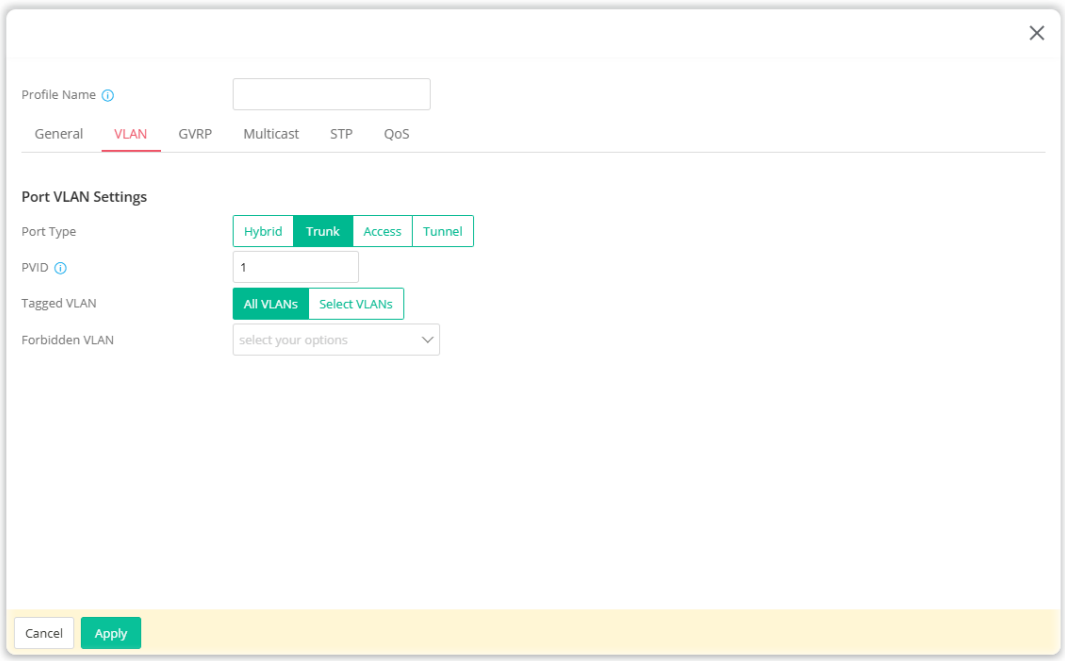
項目	說明
設定檔名稱(Profile Name)	請為交換器輸入名稱。設定名稱目的是用於識別交換器。 當許多 VigorSwitch(相同模式)裝置連接到 Vigor 路由器時，此功能非常有用。
PoE 埠口啟用(PoE Port Enabled)	啟用/停用所選連接埠的 PoE 功能。啟用後，此連接埠可用於連接 PoE 裝置。
PoE 優先權(PoE Priority)	選擇 PoE 裝置的優先順序。 **重要的(Critical)** - 將 PoE 裝置設定為最高優先權連線。 **高(High)** – 將 PoE 設備設定為高優先權連線。 **低(Low)** – 將 PoE 設備設定為低優先權連線。
埠口啟用(Port Enabled)	切換此開關以啟用/停用**透過排程啟用埠號(Enable Port by Schedule)**功能。
透過排程啟用埠號(Enable Port by Schedule)	設定連接埠設定檔套用於特定 GE 連接埠時的有效時間。 **永遠連線(Always On)** – 如果啟用，連接埠設定檔將始終有效。 **排程啟用(Scheduled On)** – 連接埠設定檔將根據此處指定的時間排程生效。
埠口隔離(Port Isolation)	允許網路管理員設定受保護連接埠之設定，以防止選定的連接埠相互通訊。埠口隔離僅允許與未受保護的連接埠通訊。 例如，在連接埠清單中選擇 GE1 和 GE3，並按一下啟用(Enable)以進行連接埠隔離，則位於 GE1 和 GE3 後方的使用者將被隔離，無法彼此相互通訊。 切換此開關即可啟用/停用此功能。
LACP 優先權(LACP Priority)	請輸入連接埠優先權編號(1 至 65535)。
LACP 逾時(LACP Timeout)	逾時選項決定了本機 LAG 連線交換器如何判斷連線是否已中斷。交換器也會將此設定值通知遠端交換器，以便遠端交換器能夠準時發送 LACP PDU。 **短(Short) -** LACP PDU 每秒發送一次。如果超過 3 秒未偵測到連接埠成員，則會導致連接埠成員逾時。 **長(Long) -** LACP PDU 每 30 秒發送一次。如果 90 秒內未偵測到連接埠

	成員，則會導致連接埠成員逾時。
EEE	切換開關以啟用或停用所選連接埠的 EEE(高能效乙太網路)功能。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

VLAN

此頁面允許使用者設定與 VLAN 相關的介面(GE)設定內容。



可用設定說明如下：

項目	**說明**
設定檔名稱 **(Profile Name)**	請為交換器輸入名稱。設定名稱目的是用於識別交換器。 當許多 VigorSwitch(相同模式)裝置連接到 Vigor 路由器時，此功能非常有用。
埠號類型 **(Port Type)**	選擇介面的 VLAN 模式。 **混合模式(Hybrid)** - 支援 IEEE 802.1Q 規範所定義的所有 VLAN 功能。 **幹道模式(Trunk)** - 最多可作為一個 VLAN 的未標籤(Untagged)成員，並可同時作為零個或多個 VLAN 的已標籤(Tagged)成員。 **存取模式(Access)** - 僅接受未標籤(Untagged)的資料框（Frame），並加入一個未標籤(Untagged)VLAN。 **通道模式(Tunnel)** - 僅接受未標籤(Untagged)的資料框(Frame)，並加入一個未標籤(Untagged)VLAN。
PVID	PVID(埠口 VLAN ID)是一個標籤，它會加入到連接埠接收到的未標籤之訊框中，以便將這些封包轉送到該標籤定義的 VLAN 群組。 對於存取模式/通道模式下的連接埠，以 PVID 形式提供的 VLAN ID 將自動被選擇為未標籤之 VLAN。
接受類型 **(Accepted Type)**	當選擇混合模式(Hybrid)時，此功能可用。 指定所選介面可接受的資料框類型。此功能僅在混合模式下可用。 **全部(All)** - 無論幀是否帶有 802.1q 標籤，都接受它。

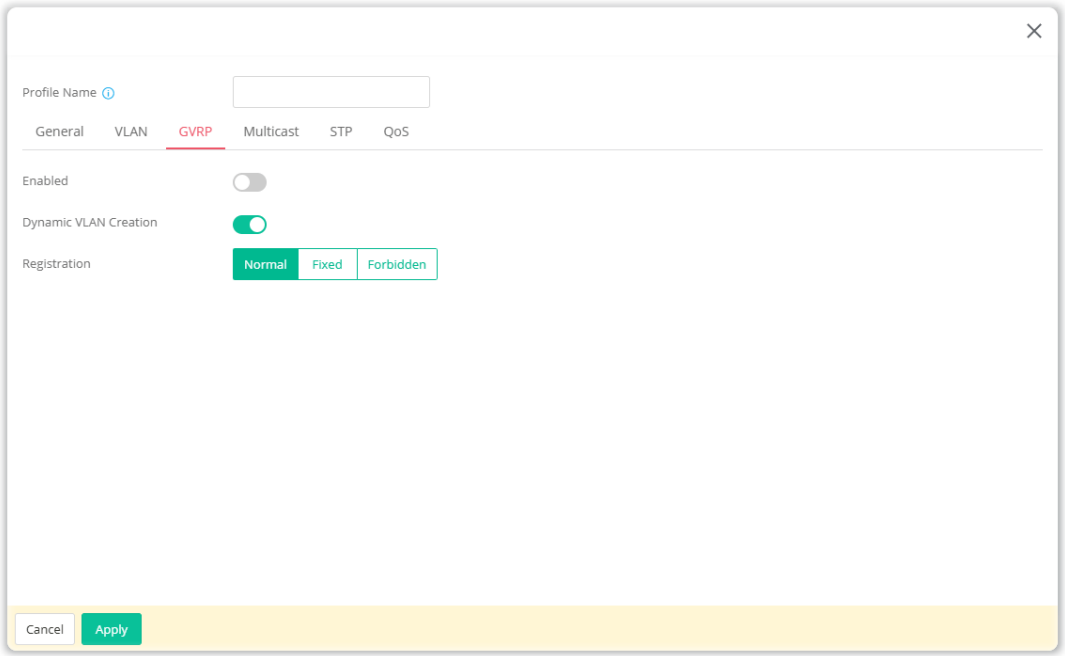
	限用標籤(Tag Only) - 只接受 802.1q 標籤的訊框。 **限用未標籤(Untag Only)** - 接受未標籤的訊框。
未標籤的 VLAN (Untagged VLAN)	當選擇**混合模式(Hybrid)**埠號類型時，此功能可用。 請指定要在 VLAN 中取消標籤的 VLAN 設定檔。
已標籤的 VLAN (Tagged VLAN)	選擇在 VLAN 中的要貼上標籤的所有 VLAN 設定檔或個別的 VLAN 設定檔。
禁止 VLAN (Forbidden VLAN)	VLAN 設定檔中設定的 GE 連接埠允許預設 VLAN 封包通過。 請選擇 VLAN 設定檔作為禁止 VLAN。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

GVRP

此頁面允許網路管理員為每個 GE 連接埠設定 GVRP(GARP VLAN 登錄通訊協定)的註冊模式(如正常、固定或禁止)。

此功能可消除不必要的網路流量，並防止任何向未註冊用戶傳輸資訊的企圖。



可用設定說明如下：

項目	說明
設定檔名稱(Profile Name)	請為交換器輸入名稱。此名稱主要用於身分識別。 此功能在許多 VigorSwitch(相同模式)裝置連接到 Vigor 路由器時，將會非常有用。
啟用(Enabled)	切換此開關已啟用/停用 GVRP 埠號設定。
動態 VLAN 建立 (Dynamic VLAN Creation)	切換此開關已啟用/停用 VLAN 建立功能。
註冊(Registration)	有三種模式可以指定。 **正常模式(Normal)** – 此為預設設定。所有資料封包均可通過選定的 GE 連接埠。

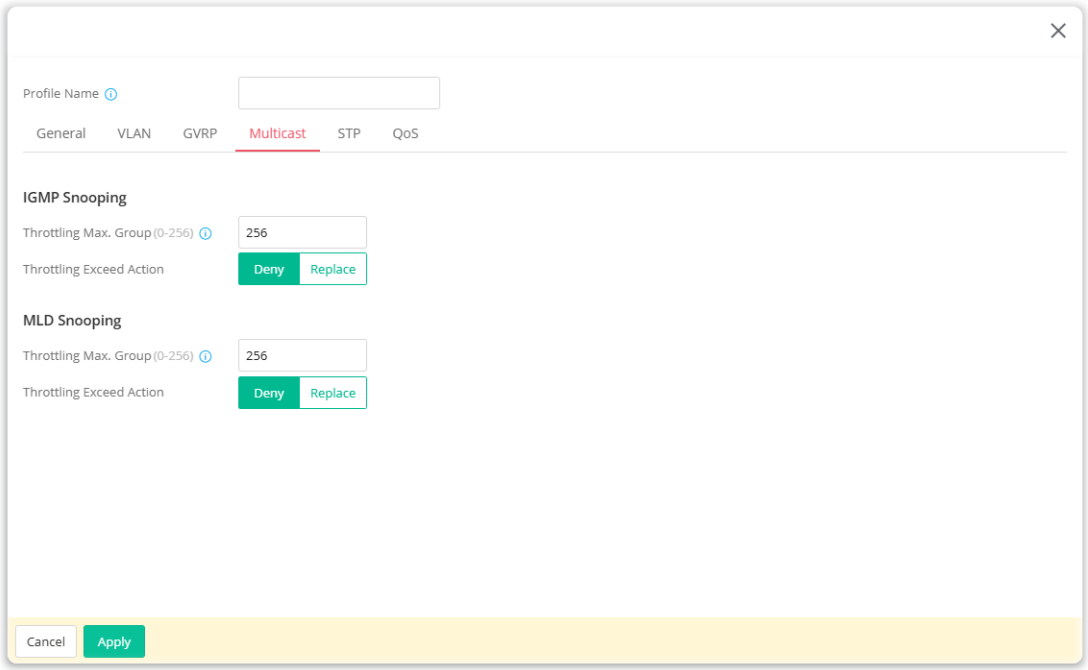
	固定模式(Fixed) – 選定的 GE 連接埠僅向相鄰設備發送固定 VLAN 訊息，並允許固定 VLAN 封包通過。 **禁止模式(Forbidden)** – 選定的 GE 連接埠僅允許預設 VLAN 封包通過。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

多播(Multicast)

IGMP snooping 是指監聽網際網路群組管理協定 (IGMP) 網路流量的過程。此功能允許網路交換器監聽主機和路由器之間的 IGMP 對話。透過監聽這些會話，交換器可以維護一張表格，記錄哪些鏈結需要哪些 IP 群播流。交換器可以對不需要多點傳播的連結進行群播過濾，從而控制哪些連接埠接收特定的群播流量。

MLD snooping 與 **IGMP snooping** 的功能相同。差別在於 IGMP snooping 作用於 IPv4 封包，而 MLD snooping 作用於 IPv6 封包。MLD snooping 是指監聽多重播放監聽器發現網路流量的過程。它可以檢查 IPv6 封包，並透過 VLAN 連接埠成員將這些封包轉送到指定位置。



可用設定說明如下：

項目	說明
設定檔名稱(Profile Name)	請為交換器輸入名稱。此名稱主要用於身分識別。 此功能在許多 VigorSwitch(相同模式)裝置連接到 Vigor 路由器時，將會非常有用。
	IGMP Snooping
流量限制最大群組數(Throttling Max. Group)	定義交換器上使用者可以加入的最大 IGMP 群組設定檔數量。如果選擇 “0” ，則該介面(連接埠)可以加入所有 IGMP 群組設定檔(在過濾設定檔中定義)。
流量限制超過時的動作(Throttling Exceed Action)	當指定介面的 IGMP 加入報告數量超過最大群組中定義的數值時，VigorSwitch 將執行以下定義的操作。 **拒絕(Deny)** – 此為預設值。透過此類介面收到的 IGMP 加入報告(用於多播

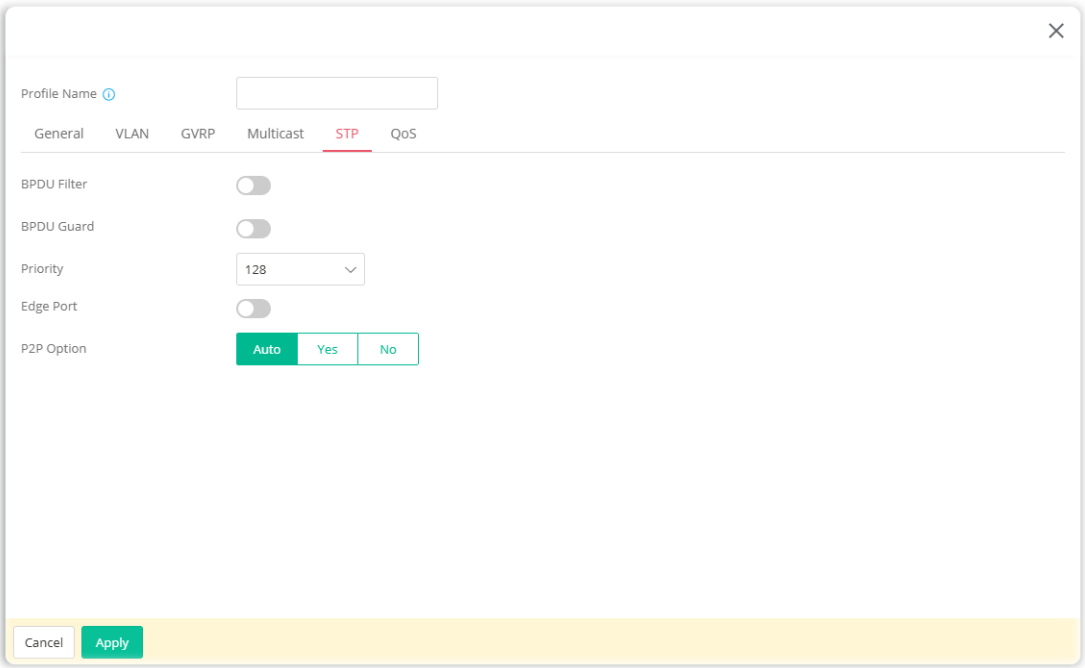
	服務)將被丟棄。 **取代(Replace) –** 選定後，收到 IGMP 報告的新群組將取代現有群組。
	MLD Snooping
流量限制最大群組數 (Throttling Max. Group)	定義交換器上使用者可以加入的最大 MLD 群組設定檔數量。如果選擇 “0” ，則該介面(連接埠)可以加入所有 MLD 群組設定檔(在過濾設定檔中定義)。
流量限制超過時的動作 (Throttling Exceed Action)	當指定介面的 MLD 加入報告數量超過最大群組中定義的數值時，VigorSwitch 將執行以下定義的操作。 **拒絕(Deny) –** 此為預設值。透過此類介面收到的 MLD 加入報告(用於多播服務)將被丟棄。 **取代(Replace) –** 選定後，收到 MLD 報告的新群組將取代現有群組。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

STP

STP(生成樹協定)是一種網路協定，能確保任何橋接乙太網路區域網路的無迴路拓撲結構。

BPDU(橋接協定資料單元)為一種訊框，包含生成樹協定(STP)相關資訊。交換器使用其來源連接埠的唯一 MAC 位址和多播位址作為目的 MAC 位址來發送 BPDU (對每個 VLAN 產生樹來說，可以是 01:80:C2:00:00:00 或 01:00:0C:CC:CC:CD) 。



可用設定說明如下：

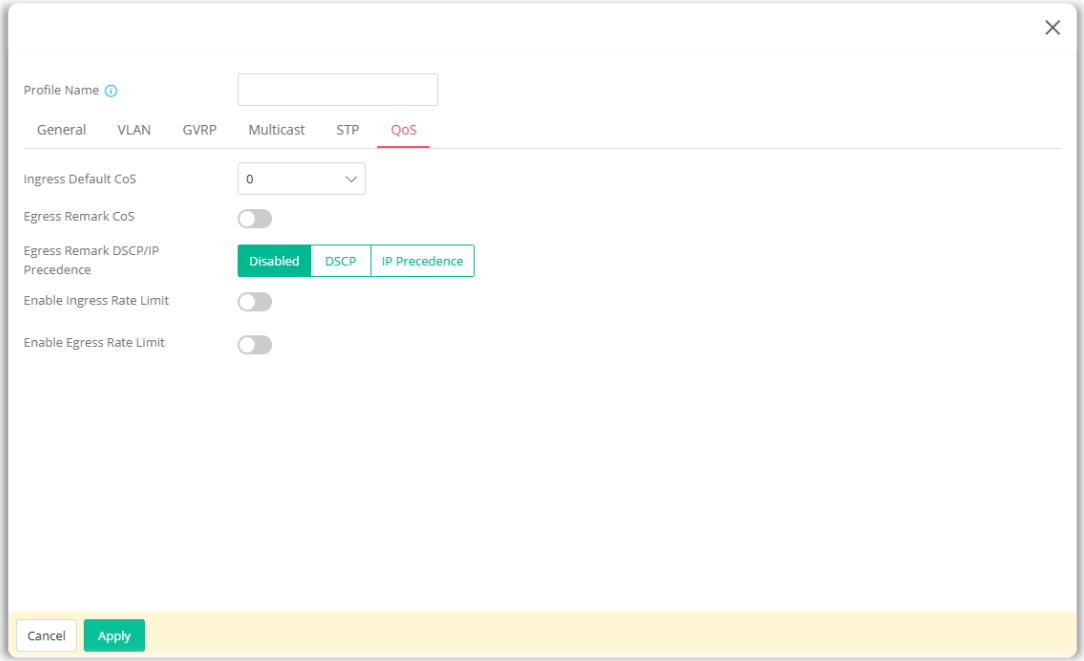
項目	說明
設定檔名稱 (Profile Name)	請為交換器輸入名稱。此名稱主要用於身分識別。 此功能在許多 VigorSwitch(相同模式)裝置連接到 Vigor 路由器時，將會非常有用。
BPDU 過濾器 (BPDU Filter)	切換開關以啟用/停用捨棄所有 BPDU 封包的功能，啟用後將不會傳送任何 BPDU。
BPDU 防護	BPDU 防護功能會在收到來自該連接埠的任何 BPDU 時，將該連接埠置於

(BPDU Guard)	錯誤狀態並關閉，從而進一步保護您的交換器。請勾選此選項以啟用此功能。 切換開關以啟用/停用 BPDU 防護功能。
優先權(Priority)	為交換器指定優先權值。優先權值越小，優先權越高，成為主交換器的機會就越大。
Edge 埠口(Edge Port)	在 **Edge 埠口(Edge Port)**模式下，連結建立後介面會立即進入轉發狀態。如果介面啟用了 **Edge 埠口(Edge Port)**模式，且介面上收到了 BPDU，則在 STP 狀態改變前，可能會在短時間內發生環路。 切換開關即可啟用/停用此功能。
P2P 選項(P2P Option)	**自動(Auto)** – VigorSwitch 自動決定此連接埠的 STP 鏈結類型。 **是(Yes)** – 表示此連接埠上的鏈結類型為全雙工，可直接連接到另一台交換器或主機。 **否(No)** – 表示此連接埠上的 STP 鏈結類型不是全雙工，且不直接連接到另一個交換器或主機。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

QoS

此頁面用於設定服務品質(QoS)的連接埠設定。每個連接埠的設定結果將顯示在本頁下方的表格中。



可用設定說明如下：

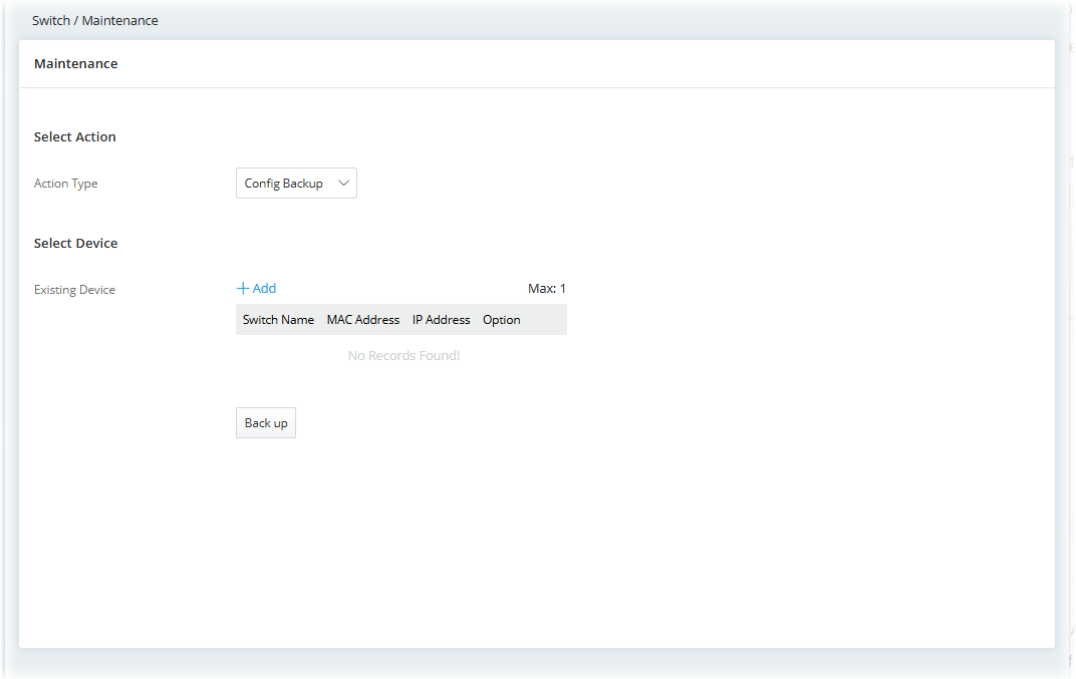
項目	**說明**
設定檔名稱 **(Profile Name)**	請為交換器輸入名稱。此名稱主要用於身分識別。 此功能在許多 VigorSwitch(相同模式)裝置連接到 Vigor 路由器時，將會非常有用。
對內預設 CoS **(Ingress Default CoS)**	針對那些沒有給予信任 QoS 標籤(802.1q/DSCP/IP 優先權，依照設定情況而定)的對內訊框指定預設 CoS 優先值。
對外 Remark CoS	切換開關即可啟用/停用此功能。

(Egress Remark CoS)	
對外 Remark DSCP/IP 優先(Egress Remark DSCP/IP Precedence)	**停用(Disabled)** - 選擇此項目可停用此功能。 **DSCP** - 根據 DSCP 對應表佇列順序，對外流量將被標記 DSCP 值。 **IP 優先(IP Precedence)** - 根據 DSCP 對應表佇列順序，對外流量將被標記 IP 優先權值。
啟用對內速率限制 (Enable Ingress Rate Limit)	此頁面用於設定服務品質(QoS)的連接埠值。每個連接埠的設定結果將顯示在本頁下方的表格中。 切換開關即可啟用/停用此功能。 **對內速率限制(Ingress Rate Limit)** - 輸入速率值(16-1000000)，單位：16 Kbps。
啟用對外速率限制 (Enable Egress Rate Limit)	此頁面用於設定服務品質(QoS)的連接埠值。每個連接埠的設定結果將顯示在本頁下方的表格中。 切換開關即可啟用/停用此功能。 **對外速率限制(Egress Rate Limit)** - 輸入速率值(16-1000000)，單位：16 Kbps。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

完成設定之後，按下套用(Apply)按鈕儲存相關設定。

II-6-4 維護(Maintenance)

Vigor 路由器可以備份、還原、重新啟動或重置轄下管理的 Vigor 交換器裝置。



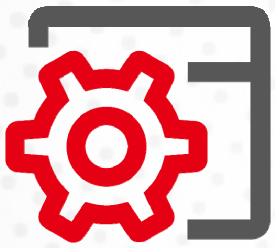
可用設定說明如下：

項目	說明
選項動作(Selection Action)	
動作類型(Action Type)	Vigor 路由器可以對 Vigor 交換器執行四種類型的操作。 **設定備份(Config Backup)** – 備份 Vigor 交換器的目前設定。 **設定還原(Config Restore)** – 使用備份檔案還原 Vigor 交換器的設定。 **遠端重啟(Remote Reboot)** – 透過 Vigor 路由器遠端重新啟動 Vigor 交換器。 **回復出廠預設值(Factory Reset)** – 透過 Vigor 路由器遠端重設 Vigor 交換器。
選擇裝置(Select Device)	
現有裝置(Existing Device)	**+新增(+Add)** – 按此新增新的裝置，該裝置將套用上述的設定。 目前，本區只能新增一個裝置。 選擇**設定備份**為**動作類型**時： ● **備份(Backup)** – 按此以備份所選裝置(列在現有裝置清單中)的目前設定。 選擇**設定還原**為**動作類型**時： ●  – 按此尋出用於還原的備份檔案。 ● **還原(Restore)** – 按此以使用備份檔案還原所選裝置(列在現有裝置清單中)的設定。 選擇**遠端重啟**為**動作類型**時： ● **重新啟動(Reboot)** – 按此以使用目前設定重新啟動遠端交換器(由 Vigor 路由器管理)。

	選擇**回復出廠預設值**為**動作類型**時： • **重置(Reset)** – 按此將選取的裝置(列在現有裝置清單中)重設為出廠預設值設定。

本頁留白

第三章 管理



III-1 系統維護(System Maintenance)

對於系統設置，您需要了解以下幾種設定：裝置設定、管理、韌體、備份與還原、帳號和重啟路由器以及韌體升級。

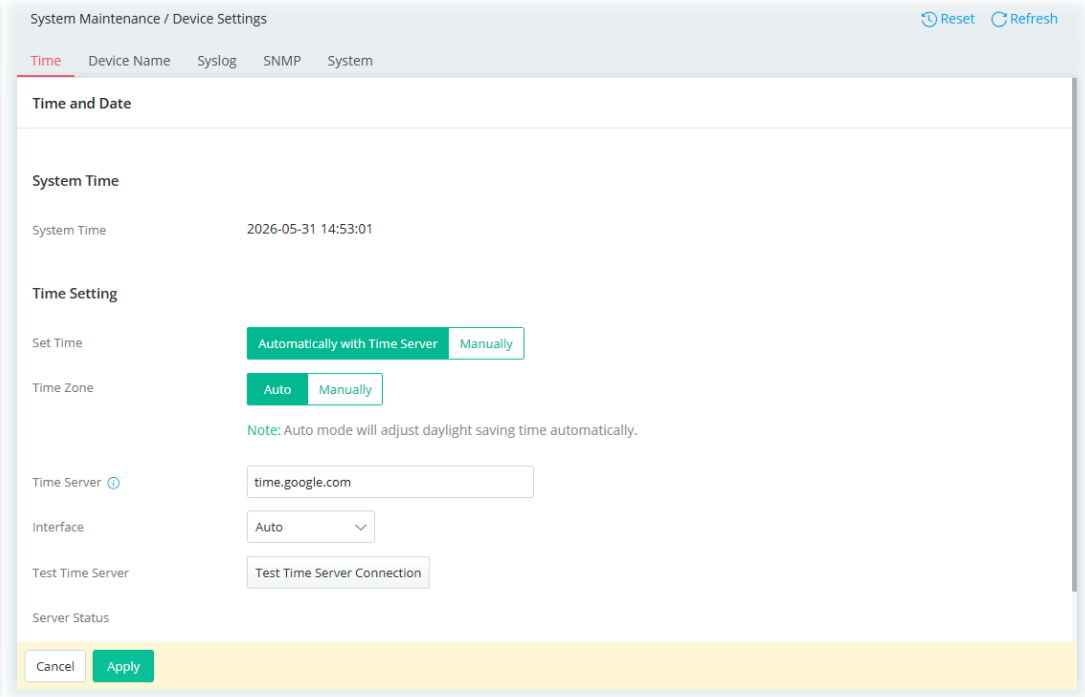
III-1-1 裝置設定(Device Settings)

使用者可以修改裝置的時間、名稱和系統日誌。

III-1-1-1 時間(Time)

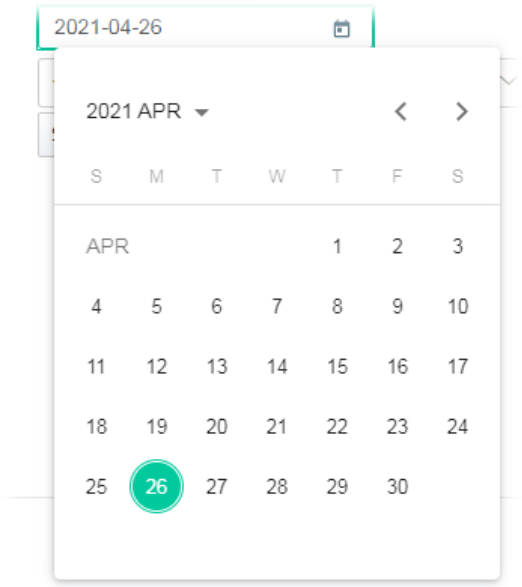
打開**系統維護>>裝置設定(System Maintenance>>Device Settings)**然後按下**時間(Time)**標籤。

本頁可讓您指定從何查詢 Vigor 裝置的時間。



可用設定說明如下：

項目	說明
	系統時間(System Time)
系統時間(System Time)	顯示目前時間。
	時間設定(Time Setting)
設定時間(Set Time)	選擇設定時間的方法(自動或手動)。 **自動使用時間伺服器(Automatically with Time Server)** - 使用網路時間協定(NTP)從指定的網路時間伺服器取得時間資訊。 **手動(Manually)** -使用網頁瀏覽器顯示的時間取得系統時間。
當設定時間選擇了自動使	**時區(Time Zone)** - 選擇路由器所在的時區。

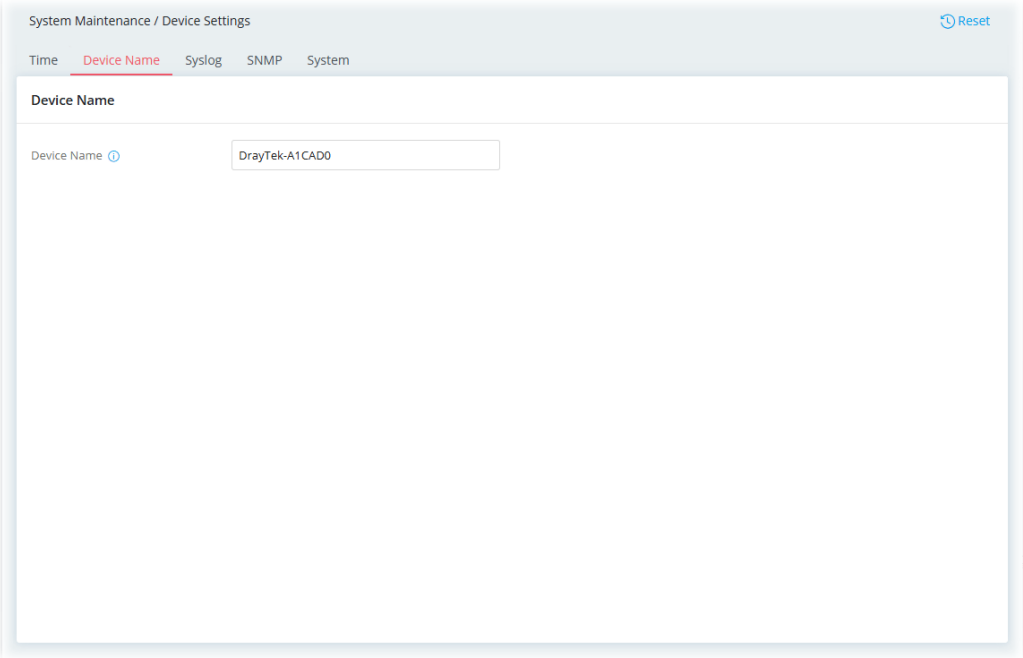
用時間伺服器 (Automatically with Time Server)	**時間伺服器(Time Server)** - 輸入主要時間伺服器的網站位址。 **介面(Interface)** - 透過選定的 WAN/LAN 介面更新時間。如果選擇自動(Auto)，Vigor 系統將透過 WAN 或 LAN 更新時間。 **測試時間伺服器(Test Time Server)** – 按下**測試時間伺服器連線(Test Time Server Connection)** 按鈕以測試時間伺服器是否正常運作。 **伺服器狀態(Server Status)** - 顯示上次更新時間狀態。 **更多設定(More Settings)** - 按此以開啟時間伺服器的進階設定。 ● **自動更新間隔(Auto Update Interval)** - 選擇路由器定期更新系統時間的時間間隔(30 分鐘或 60 分鐘)。 ● **次要伺服器(Secondary Server)** - 如需備份時間伺服器，請在此輸入 URL/IP 位址。 ● **次要介面(Secondary Interface)** - 透過選定的 WAN/LAN 介面更新時間。如果選擇自動(Auto)，Vigor 系統將透過 WAN 或 LAN 更新時間。此為選項設定，作位備份時間伺服器的使用介面。如果主要時間伺服器更新時間失敗，Vigor 系統將改用次要時間伺服器來進行。 ● **日光節約(Daylight Saving)** - 當時區選擇手動(Manually)時，切換開關即可啟用或停用此功能。如果您的地區適用**日光節約**時區(DST)時，請啟用此功能。 ● **日光節約期間(Daylight Saving Period)** - 此功能僅在啟用日光節約時可用。選擇依周(by Week)或依日期(by Date)，並指定開始時間和結束時間。
當設定時間選擇了手動 (Manually)	**日期(Date) -** 請使用下拉式日曆以指定正確的日期。  **時間(Time) -** 透過指定時、分和秒來設定時間。 **與瀏覽器同步(Synchronize with Browser)** – 按下**立即同步(Sync now)**將時間設定與瀏覽器同步。
套用(Apply)	儲存目前設定並更新系統時間。
取消(Cancel)	捨棄目前設定並離開此頁面。

完成網頁設定之後，按下**套用(Apply)**更新系統時間。

III-1-1-2 裝置名稱(Device Name)

顯示路由器名稱。如果需要，可以變更名稱。

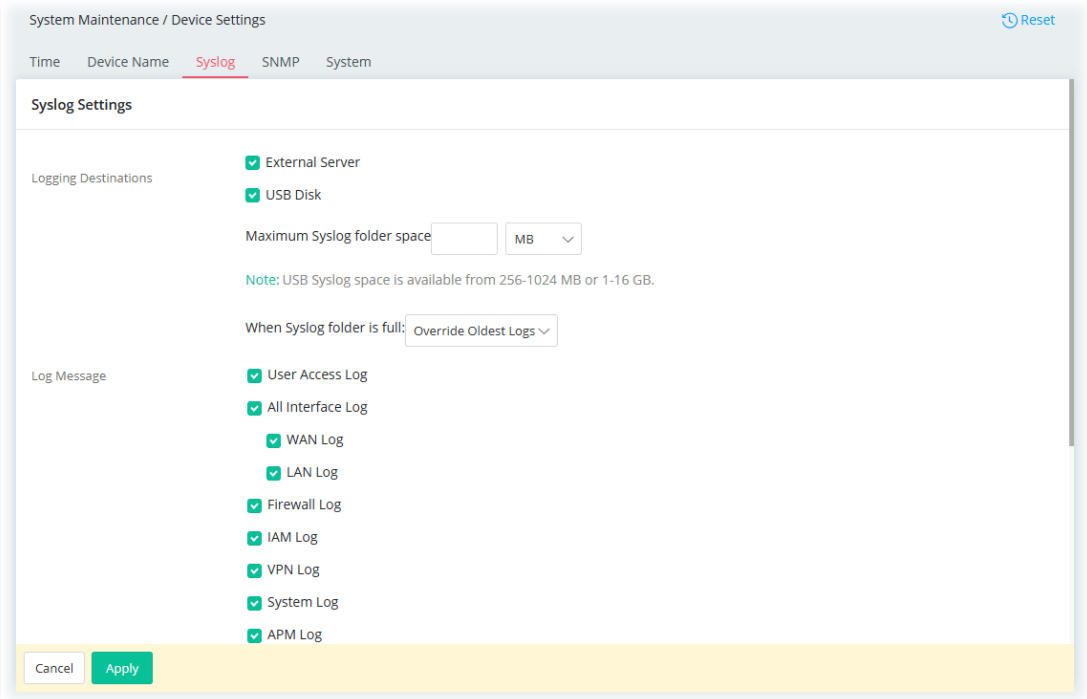
打開**系統維護>>裝置設定(System Maintenance>>Device Settings)**然後按下**裝置名稱(Device Name)**標籤。



III-1-1-3 Syslog

SysLog 功能供使用者監控路由器。

打開**系統維護>>裝置設定(System Maintenance>>Device Settings)**然後按下 **Syslog** 標籤。



可用設定說明如下：

項目	說明
Syslog 設定(Syslog Settings)	
記錄目的(Logging Destinations)	**外接伺服器(External Server)** - 選擇以設定日誌訊息項目並設定系統日誌伺服器。 **USB 磁碟(USB Disk)** - 選擇此項可設定與 USB 相關的設定內容。 **最大 Syslog 資料夾空間(Maximum Syslog folder space)** - 請輸入資料夾空間大小。 其中，MB 格式的值範圍為 256 – 1024 MB，GB 格式的值範圍為 1 – 16 GB。 **當 Syslog 資料夾已滿(When Syslog folder is full)** -選擇系統日誌資料夾已滿時要執行的操作。 • 覆寫最舊之日誌(Override Oldest Logs) • **滿碟時停止紀錄(Stop when Full)**
日誌訊息(Log Message)	選擇傳送相應的使用者存取資訊、介面和系統資訊到 Syslog 上。
Syslog 伺服器(Syslog Servers)	
新增(+Add)	按一下以顯示用於建立新 Syslog 伺服器設定檔的新輸入框。 新增的 Syslog 伺服器的最多可設定 3 個。
伺服器 IP(Server IP)	輸入 Syslog 伺服器的 IP 位址。
埠號(Port)	輸入 Syslog 伺服器的連接埠號碼。
選項(Option)	**刪除(Delete)** - 按此可刪除選定的伺服器設定檔。
套用(Apply)	儲存目前設定。
取消(Cancel)	捨棄目前設定並離開此頁面。

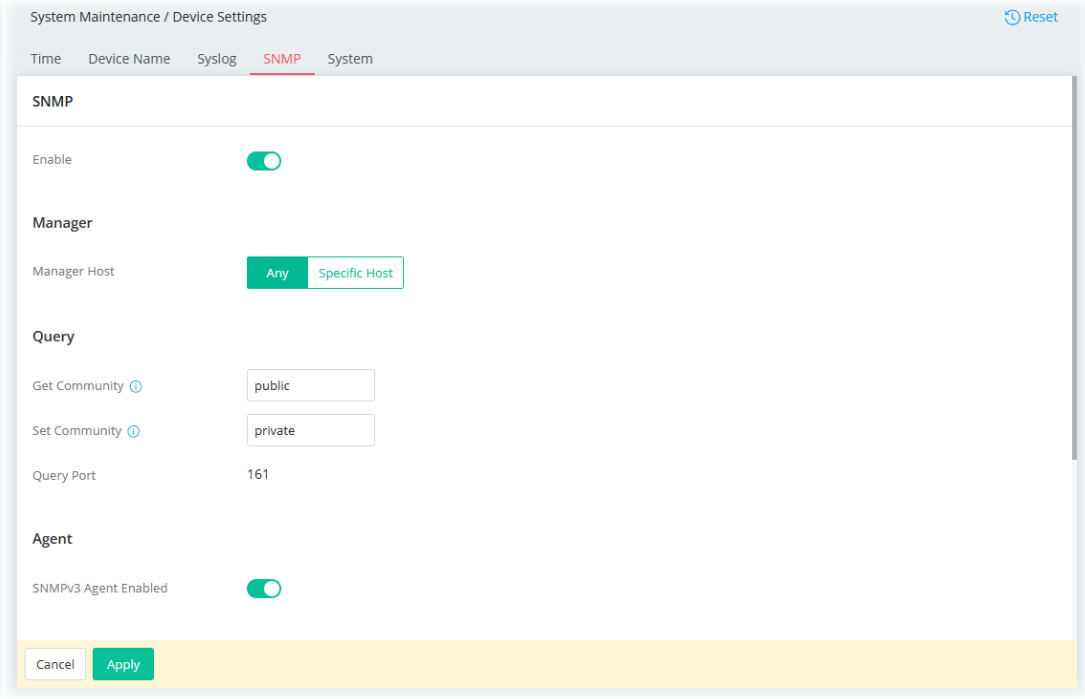
完成設定之後，按下**套用(Apply)**按鈕儲存相關設定。

III-1-1-4 SNMP

本節可讓您設定 SNMP 服務設定。

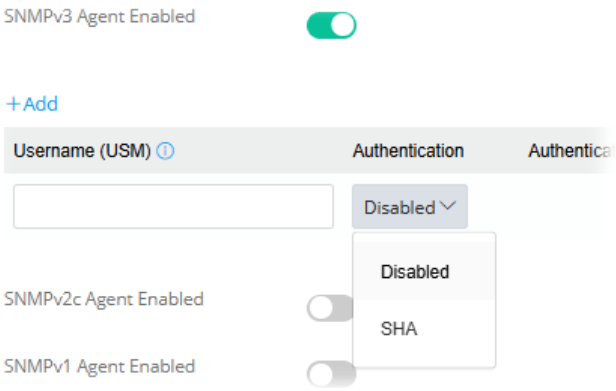
比起 SNMP，SNMPv3 透過使用加密(支援 AES 和 DES)和身份驗證(支援 MD5 和 SHA)來滿足管理需求，因此更安全。

打開**系統維護>>裝置設定(System Maintenance>>Device Settings)**，按下 SNMP 標籤。



可用設定說明如下：

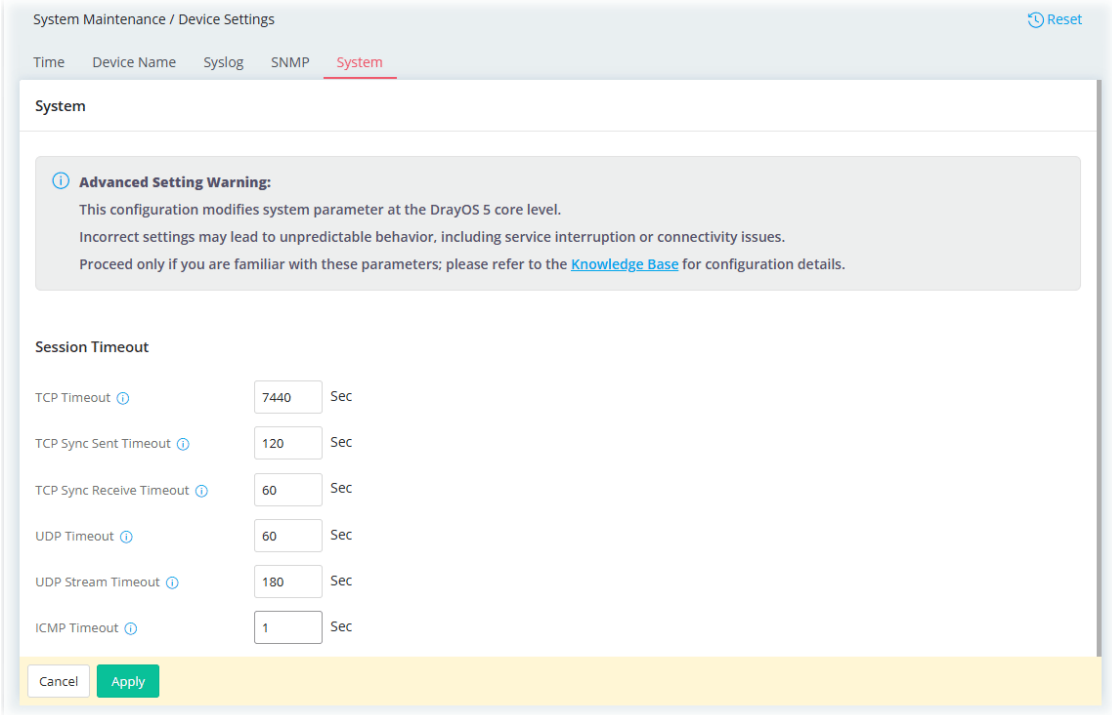
項目	說明
	SNMP
啟用(Enable)	切換開關以啟用/停用 SNMP 功能。 如果啟用，您可以設定管理員、查詢、代理和陷阱設定。
	管理者(Manager)
管理者主機(Manager Host)	**任一(Any)** - 任何 IP 位址都可以設定為管理主機。 **指定主機(Specific Host)** - 指定一個主機(IPv4 或 IPv6)或多個主機(IPv4 和 IPv6)。 ● **IP 類型(IP Type)** –選擇 IPv4 或 IPv6 或二者。 **指定管理者主機(Specific Manager Host (IPv4/IPv6))** - 當選擇 IPv4/IPv6 作為 IP 類型時可用。點選**+新增(Add)**新增條目。 輸入允許發出 SNMP 指令的主機 IPv4 位址(含子網路遮罩)/ IPv6 位址(含指定前置代碼)。如果這些欄位是空白的，即表示允許任何 IPv4/IPv6 區域網路主機發出 SNMP 指令。
	查詢(Query)
取得 Community (Get Community)	輸入取得 Community 字串。預設為 public，使用 get 命令傳送請求以查詢資訊的裝置必須傳遞正確的 Get Community 字串。
設定 Community (Set Community)	輸入設定 Community 字串。預設為 private，使用 set 指令傳送變更設定要求之裝置必須傳遞正確的 Set Community 字串。

查詢埠(Query Port)	顯示查詢伺服器所使用的連接埠號碼。
代理(Agent)	
啟用 SNMPv3 代理功能 (SNMPv3 Agent Enabled)	切換開關以啟用/停用 SNMPv3 功能。 如果啟用此功能，請指定相應的設定內容。按下**+新增(Add)**新增條目。  **使用者名稱(Username(USM))** - USM 指的是以使用者為基礎的安全模式。請輸入用於身份驗證的使用者名稱。 **驗證(Authentication)** - 選擇一種與身份驗證演算法一併使用的雜湊方法(hashing methods)。 **驗證密碼(Authentication Password)** - 請輸入密碼進行身份驗證。 **隱私(Privacy)** - 選擇一種加密方法作為隱私演算法。 **隱私密碼(Privacy Password)** - 請輸入密碼以保護隱私。
啟用 SNMPv2c 代理功能 (SNMPv2c Agent Enabled)	切換開關以啟用/停用 SNMPv2 功能。
啟用 SNMPv1 代理功能 (SNMPv1 Agent Enabled)	切換開關以啟用/停用 SNMPv1 功能。
陷阱(Trap)	
啟用(Enabled)	切換開關以啟用/停用 Trap 功能。
陷阱版本(Trap Version)	選擇陷阱版本。 - **V1** - **V2c** - **V3**
陷阱 Community (Trap Community)	輸入陷阱 Community 字串。預設為 public。向 SNMP 控制台傳送未經請求的訊息之裝置，必須傳遞正確的陷阱團體字串。 文字長度上限為 23 個字元。
陷阱埠(Trap Port)	輸入 Trap 伺服器使用的連接埠號碼。
通知主機 IP 類型 (Notification Host IP Type)	選擇通知主機的類型： - **二者(Both)** - **IPv4** - **IPv6**
通知主機(IPv4) (Notification Host(IPv4))	**+新增(+Add)** - 輸入允許接收 SNMP trap 的主機的 IPv4 位址。
通知主機(IPv6) Notification Host(IPv6))	**+新增(+Add)** - 輸入允許接收 SNMP trap 的主機的 IPv6 位址。

陷阱事件(Trap Events)	選擇要套用此頁面中設定的事件。
套用(Apply)	儲存目前設定並離開此頁面。

III-1-1-5 系統(System)

本節可讓您設定與連線數逾時相關的設定。



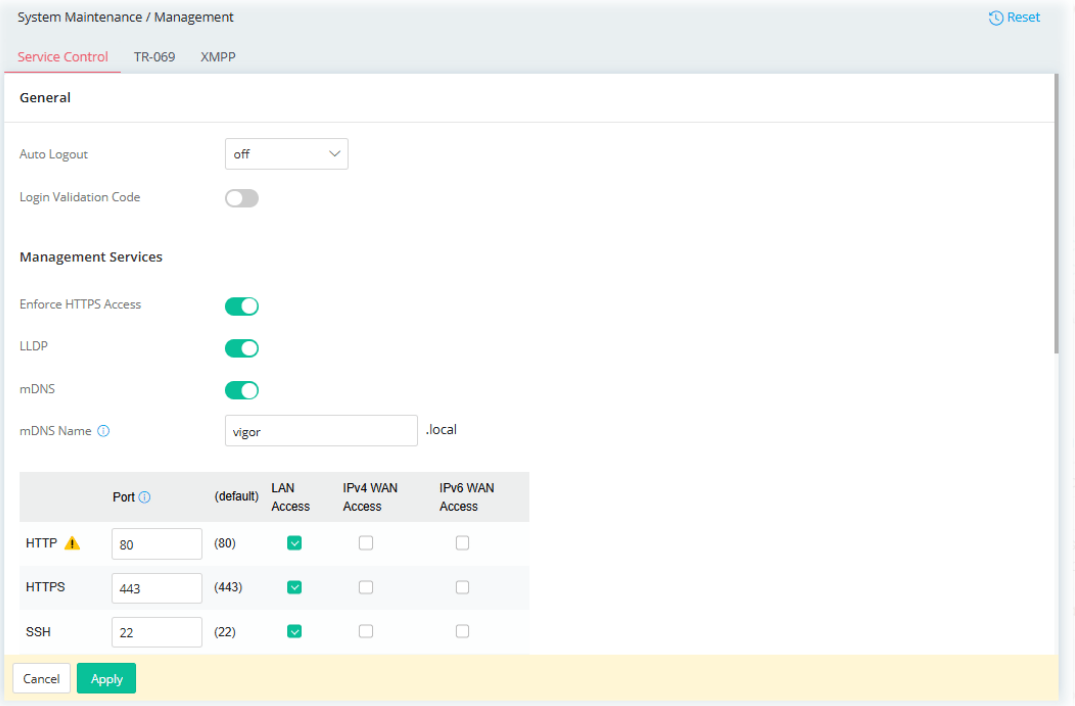
可用設定說明如下：

項目	**說明**
TCP 逾時 **(TCP Timeout)**	設定連線數保持時間。 TCP 完成三向交握(Three-way Handshake)和雙向資料傳輸後，如果沒有新的資料封包傳入或傳出，則當時間到期時，連線將會終止。
TCP 同步傳送逾時(TCP Sync Sent Timeout)	設定 TCP SYN 發送逾時時間。 指定客戶端在發送 SYN 請求後等待 SYN/ACK 回應的時間。
TCP 同步接收逾時(TCP Sync Receive Timeout)	設定 TCP SYN 接收逾時時間。 指定路由器在回覆 SYN/ACK 後等待客戶端 ACK 的時間。
UDP 逾時 **(UDP Timeout)**	設定 UDP 逾時時間。 指定在等待對端回應期間，UDP 封包保持有效的時長。
UDP 串流逾時(UDP Stream Timeout)	指定在偵測到雙向流量後應用於 UDP 串流的逾時時間。
ICMP 逾時 **(ICMP Timeout)**	設定 ICMP 逾時時間。 指定 ICMP 封包 (例如 ping 和 traceroute) 的連線數逾時時間。
套用(Apply)	儲存目前設定。
取消(Cancel)	捨棄目前設定並離開此頁面。

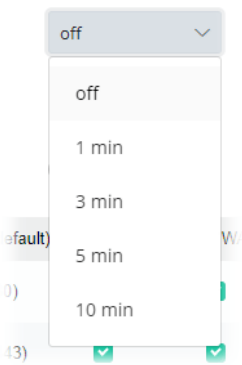
III-1-2 管理(Management)

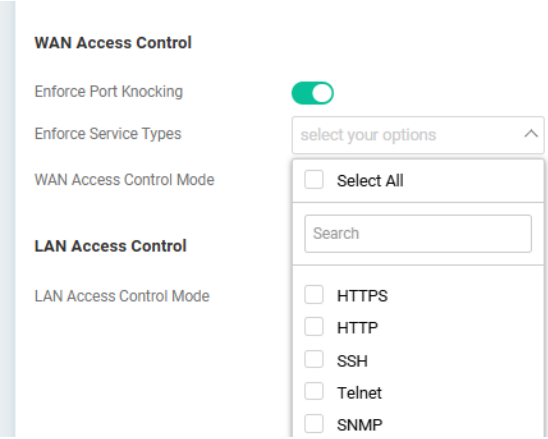
III-1-2-1 服務控制(Service Control)

此頁面可讓您管理一般基本設定、管理服務以及 TLS/SSL 加密設定。使用者透過使用者名稱和密碼驗證身分後，即可取得網際網路存取權限，並可套用選項配備的防火牆規則和 WAN 網路存取策略。



可用設定說明如下：

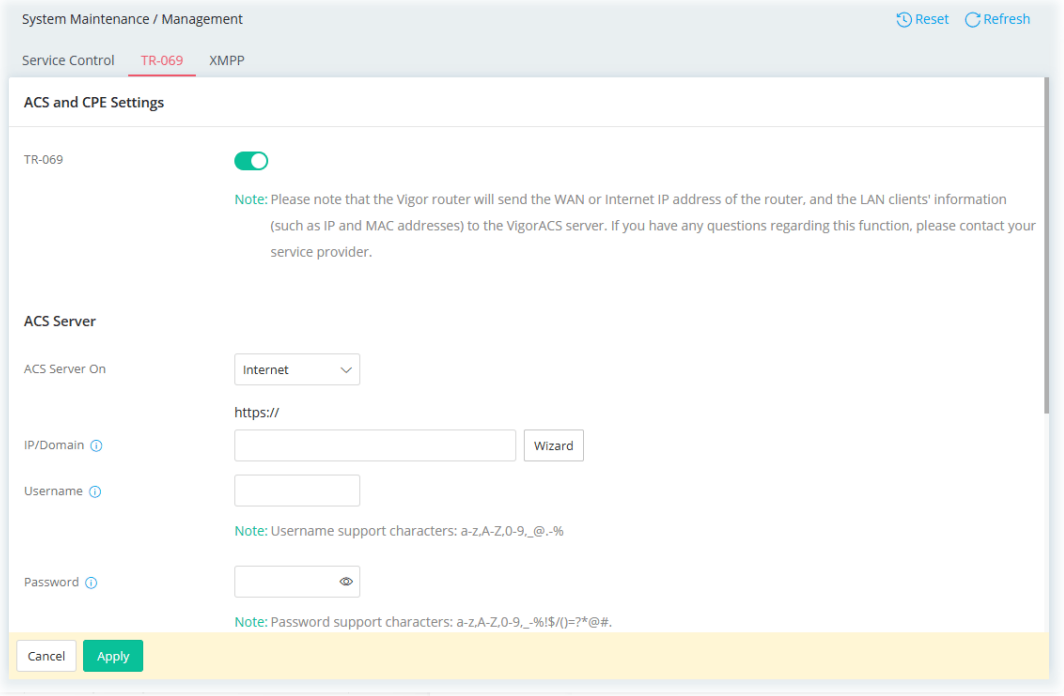
項目	說明
	基本(General)
自動登出(Auto Logout)	如果選擇 “關閉” ，則網頁使用者介面的自動登出功能將被停用。 因此直到您手動按下登出圖示前，網頁使用者介面將保持開啟狀態。  根據所選時間設定條件，可以登出網頁。預設值為關閉。請依照需要更改設定。
登入驗證碼(Login Validation Code)	如果啟用此功能，Vigor 路由器會在使用者登入時要求使用者輸入驗證碼。
	管理服務(Management Services)
強制以 HTTPS 存取登入	切換開關以啟用/停用允許系統管理員透過 HTTPS 登入 Vigor 路由器的

(Enforce HTTPS Access)	功能。
LLDP	切換開關以啟用/停用 LLDP 服務。
mDNS	切換開關以啟用/停用多播網域名稱系統(mDNS, Multicast Domain Name System, mDNS)服務。
mDNS 名稱 (mDNS Name)	輸入名稱作為本機網路中的身分標識，以便與其他裝置通訊。
埠號(Port)	針對 HTTP、HTTPS、SSH、Telnet 和 SNMP 伺服器指定使用者自訂連接埠號碼。
LAN 存取(LAN Access)	勾選此核取方塊以允許系統管理員從 LAN 介面登入。稍後，設定下方之 **LAN 存取控制**以決定(客戶端)誰能存取 LAN 管理服務(HTTP、HTTPS、SSH、Telnet 和 SNMP)。
IPv4/IPv6 WAN 存取 (IPv4/IPv6 WAN Access)	勾選此核取方塊以允許系統管理員透過 IPv4/IPv6 WAN 介面登入。稍後，進行配置。設定下方之 WAN 存取控制以決定(客戶端)誰能存取 IPv4 WAN 管理服務(HTTP、HTTPS、SSH、Telnet 和 SNMP)。
TLS 加密(TLS Encryption)	
TLS 1.3/TLS 1.2	切換開關即可啟用或停用此功能。
存取控制清單(Access Control List)	
WAN 存取控制(WAN Access Control)	一般來說，所有透過 WAN 介面的用戶端都可以存取 IPv4 WAN 管理服務(依照選擇的 HTTP、HTTPS、SSH、Telnet 和 SNMP 等核取方塊而定）。 **強制執行 Port Knocking (Enforce Port Knocking)** -切換開關以啟用/停用 Port Knocking 功能。 **強制執行服務類型(Enforce Service Types) –** 選擇通訊協定。只有成功完成 **Port Knocking** 的來源 IP 位址才能存取這些選定的服務（從 WAN 介面）；其他 IP 位址都會被拒絕。  **TOTP 密鑰(TOTP Secret) –** 顯示用於 TOTP 的金鑰。 **WAN 存取控制模式(WAN Access Control Mode) –** 選擇允許全部連線或白名單。只有選定 IP 群組物件中的指定 IP 物件才能透過 WAN 介面存取此頁面上列出的服務。 • **允許全部連線(Allow All Connections)** - 此為預設值。 • **白名單(Allow List)** – 按下+新增(+Add)新增一筆資料，最多可以建立 6 筆。
LAN 存取控制(LAN Access Control)	一般來說，所有透過 LAN 介面的用戶端都可以存取 LAN 管理服務(依照選擇的 HTTP、HTTPS、SSH、Telnet 和 SNMP 等核取方塊而定）。 **LAN 存取控制模式(LAN Access Control Mode)** -選擇允許全部連線或白名單。只有選定 IP 群組物件中的指定 IP 物件才能透過 LAN 介面存取此頁面上列出的服務。 • **允許全部連線(Allow All Connection)** -此為預設值。 • **白名單(Allow List)** -按下+新增(+Add)新增一筆資料，最多可以建立 6 筆。

取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

III-1-2-2 TR-069

Vigor 裝置支援 TR-069 標準，可透過自動設定伺服器（例如 VigorACS）遠端管理用戶終端設備(Customer-Premises Equipment，CPE)。



可用設定說明如下：

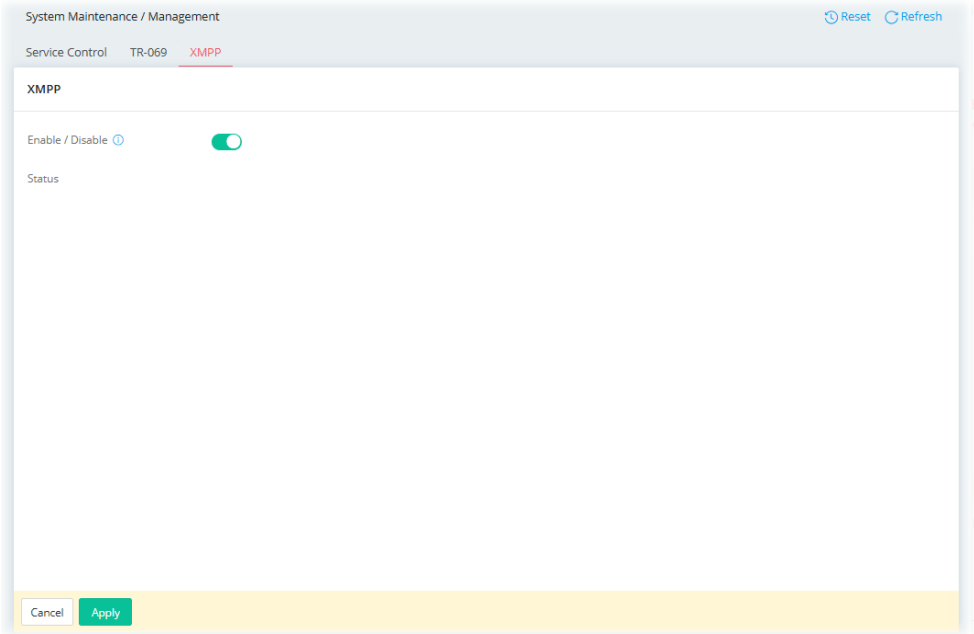
項目	說明
TR-069	切換開關即可啟用或停用此功能。
ACS 伺服器(ACS Server)	
ACS 伺服器開啟(ACS Server On)	選擇路由器與自動設定伺服器(ACS)的連接介面。
URL	輸入用於連接 ACS 的 IP 位址/網域名稱。 **設定精靈(Wizard)** -按下以輸入 VigorACS 伺服器的 IP 位址、連接埠號碼和處理程序。
使用者名稱/密碼(Username/Password)	輸入連接 ACS 伺服器所需的憑證。
連線測試(Test Connection)	
事件代碼(Event Code)	使用下拉式選單指定要執行測試的事件。 **測試通知(Test With Inform)** - 按一下即可根據事件代碼選擇發送訊息，以測試此類 CPE 是否能夠與 VigorACS 伺服器通訊。
更多設定(More settings)	
CPE 用戶端(CPE Client)	規定 CPE 客戶端的設定。 **通訊協定(Protocol)** - 如果連線已加密，請選擇 HTTPS；否則請選擇 HTTP。 **埠號(Port)** - 如果發生連接埠衝突，請變更 CPE 的連接埠號碼。

	密碼(Password) - 輸入 VigorACS 將用於連接到 CPE 的密碼。
定期通知設定(Periodic Inform Settings)	**啟用(Enable) / Disable** - 切換開關即可啟用或停用此功能。預設為 “啟用” ，這表示 CPE 用戶端將定期連接到 ACS 伺服器，並按照 “間隔時間” 欄位中指定的時間間隔更新其連線參數。 **時間間隔(Time Interval)** - 設定路由器向 CPE 發送通知的間隔時間或排程時間。(1-65535)
STUN 設定(STUN Settings)	**模式(Mode)** - 預設值為自動(Auto)。如果選擇已啟用(**Enabled**)，請輸入以下相關設定： ● **伺服器位址(Server Address)** - 輸入 STUN 伺服器的 IP 位址。 ● **伺服器 STUN 埠號(Server STUN Port)** - 輸入 STUN 伺服器的連接埠號碼(1-65535)。 ● **最小維持連線時間(Minimum Keep Alive Period)** -如果啟用了 STUN，CPE 必須向伺服器傳送綁定請求，以維持閘道中的綁定關係。請輸入最小間隔時間。預設為 “60 秒” 。 ● **最大維持連線時間(Maximum Keep Alive Period)** - 如果啟用了 STUN，CPE 必須向伺服器傳送綁定請求，以維持閘道中的綁定關係。請輸入一個數字作為最大維持連線時間。 “-1” 表示未指定最大期限。
套用(Apply)	儲存目前設定並離開此頁面。
取消(Cancel)	捨棄目前設定並離開此頁面。

完成設定之後，按下**套用(Apply)**按鈕儲存相關設定。

III-1-2-3 XMPP

XMPP 是可延伸訊息和存在協定（Extensible Messaging and Presence Protocol）的縮寫。如果您的裝置已在 XMPP 伺服器上註冊，VigorACS 可以隨時無阻礙地管理 NAT 下的 AP 基地台。



切換啟用/停用開關，即可啟用或停用 XMPP 功能。

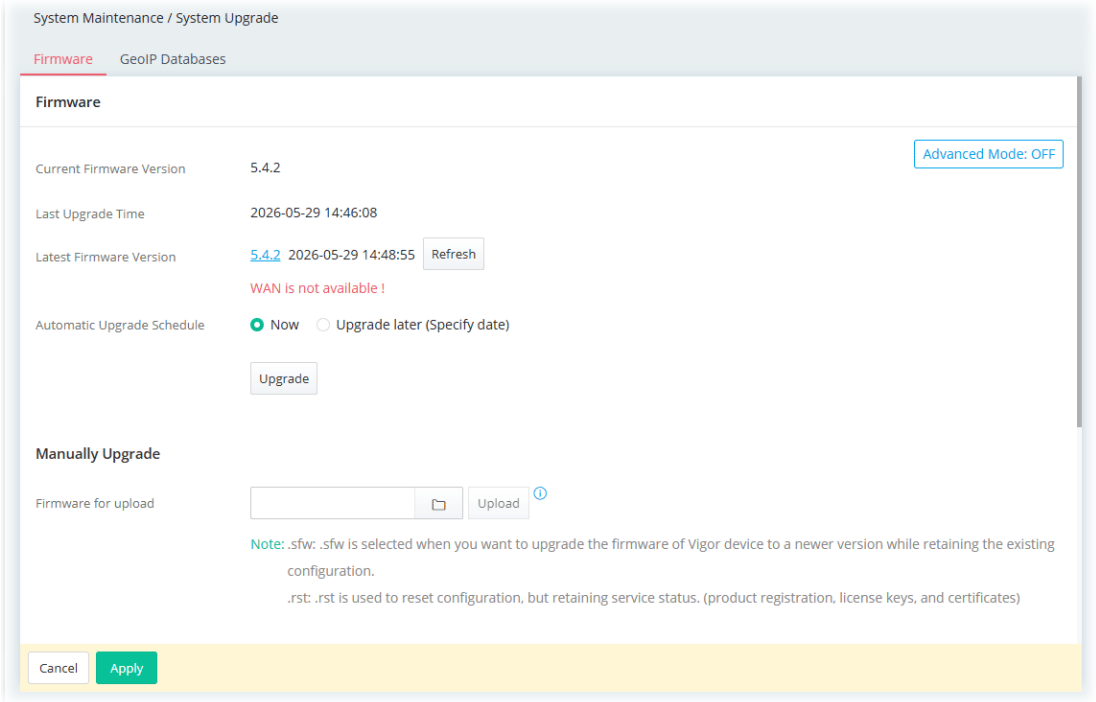
III-1-3 系統升級(System Upgrade)

III-1-3-1 韌體(Firmware)

開啟**系統維護>>系統升級(System Maintenance>> System Upgrade.)**。此網頁將透過範例引導您升級韌體。請注意，此範例以 Windows 作業系統為主。

有兩種方法可以進行韌體升級：

- **手動升級(Manual Upgrade)** – 韌體升級前，**請先從** DrayTek 網站或 FTP 網站下載最新韌體。DrayTek 網址是 www.draytek.com（或本地 DrayTek 網站），FTP 網站為 ftp.draytek.com。
- **自動升級(Automatic Upgrade)** – Vigor 路由器系統現已提供自動韌體升級功能(選項設定，預設為關閉)，方便用戶隨時了解重要的韌體變更、安全問題以及需要立即更新的重大漏洞。啟用此功能後，用戶無需手動下載最新韌體版本。 Vigor 系統會自動偵測最新版本，下載並升級路由器。此一方法對於解決關鍵安全問題和修復重大漏洞尤其重要。



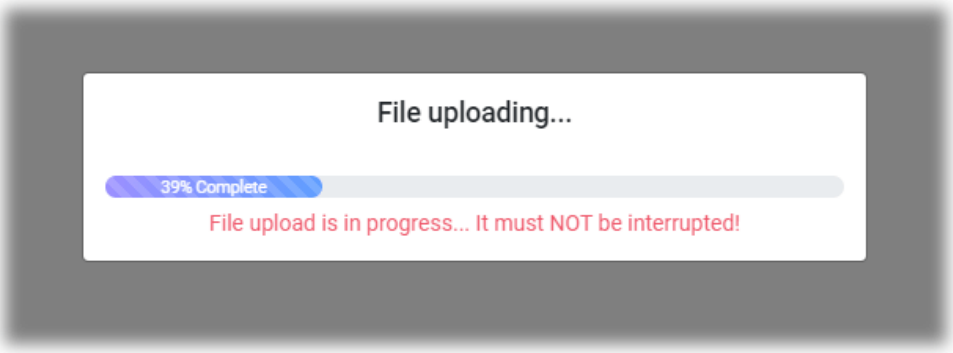
可用設定說明如下：

項目	說明
進階模式:開啟/關閉 (Advanced Mode:ON/OFF)	按此顯示或隱藏進階設定。
目前韌體版本(Current Firmware Version)	顯示目前使用的韌體之版本。
最新韌體版本(Latest Firmware Version)	**頁面更新(Refresh)** – 按下查看 DrayTek 網站上是否有最新韌體版本。
輸出流量介面 (Outbound Interface)	選擇用於從 DrayTek 網站下載韌體以進行自動升級的 WAN 介面。然後針對此所選的 WAN 介面選擇一個 IP 位址或 IP 別名。 預設值為**自動選定(Auto Select)**。
狀態(Status)	**立即升級(Upgrade Now)** – 按此立即更新韌體。

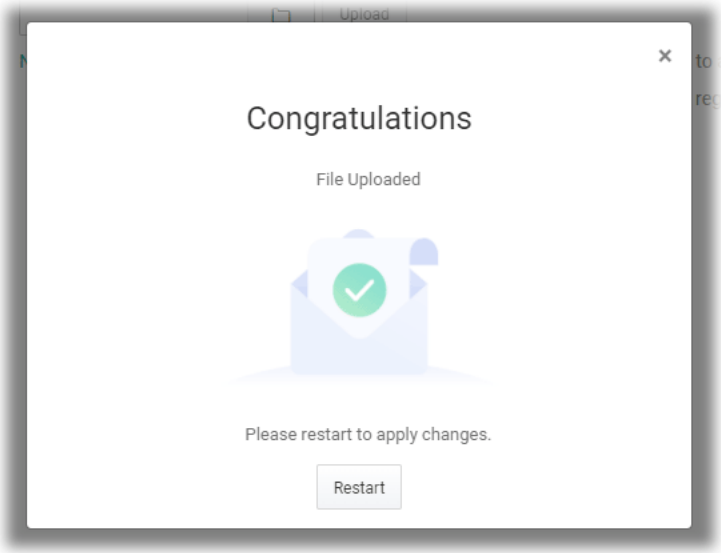
排程升級(Scheduled Upgrade)	在指定的時間與日期升級韌體。 **立即(Now)** – 選擇並按下升級按鈕立刻進行韌體更新。 **指定日期(Specify date)** – 指定日期升級韌體。
手動升級(Manually Upgrade)	
上傳用之韌體(Firmware for upload)	– 按此尋找用於升級的韌體檔案。 **上傳(Upload)** – 按此上傳選定的檔案至 Vigor 系統。
一般更新的自動升級(Automatic Upgrade for General Updates)	
啟用自動升級(Enabled Automatically Upgrade)	預設值為停用。 切換開關以便啟用或停用指定時間內的自動韌體升級。
升級時機(Upgrade Timing)	設定韌體升級時間。 **在午夜時(In the middle of the night)** – 韌體升級將於午夜進行。 **排程更新(Schedule Update)** - 韌體升級將在每週特定一天和時間進行。
重要更新的自動升級(Automatic Upgrade for Critical Updates)	
啟用重要安全性修復/重大錯誤修復(Enabled Critical Security and Major Bug Fixes)	一旦 Vigor 路由器收到包含重要安全性修復/重大錯誤修復的新韌體後，將自動執行系統升級。 此功能預設值為停用。切換開關即可啟用/停用此功能。
升級時機(Upgrade Timing)	設定韌體升級時間。 **在午夜時(In the middle of the night)**– 韌體升級將於午夜進行。 **排程更新(Schedule Update)** - 韌體升級將在每週特定一天和時間進行。
通知(Notifications)	
允許通知(Allow Notifications)	切換開關以便啟用或停用通知機制功能。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

按此 自主機中尋找最新韌體。

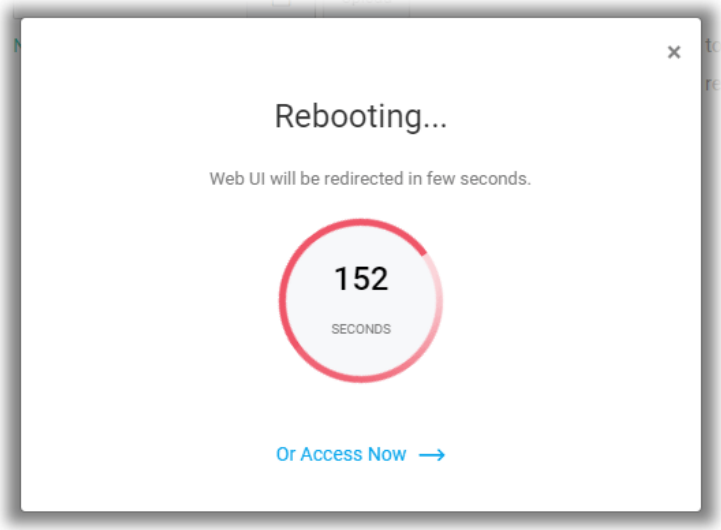
接著，按下**上傳(Upload)**並稍待一會。



上傳完成後，請按下**重新啟動(Restart)**按鈕。



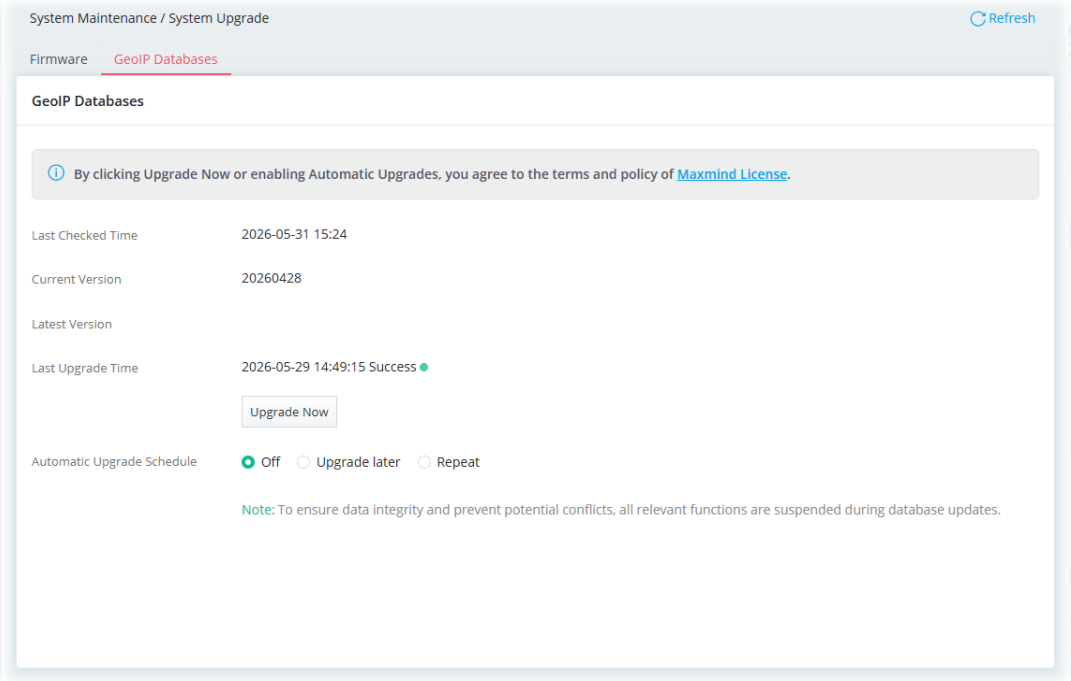
請稍等片刻，直到系統完成重新啟動。



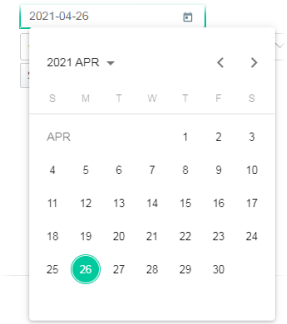
III-1-3-2 GeoIP 資料庫(GeoIP Database)

GeoIP 資料庫提供無類別域間路由 (CIDR) 和位置資訊。 Vigor 路由器採用基於 MaxMind 提供的 GeoIP 資料庫的地理分佈資訊。

如有需要，更新 GeoIP 資料庫。

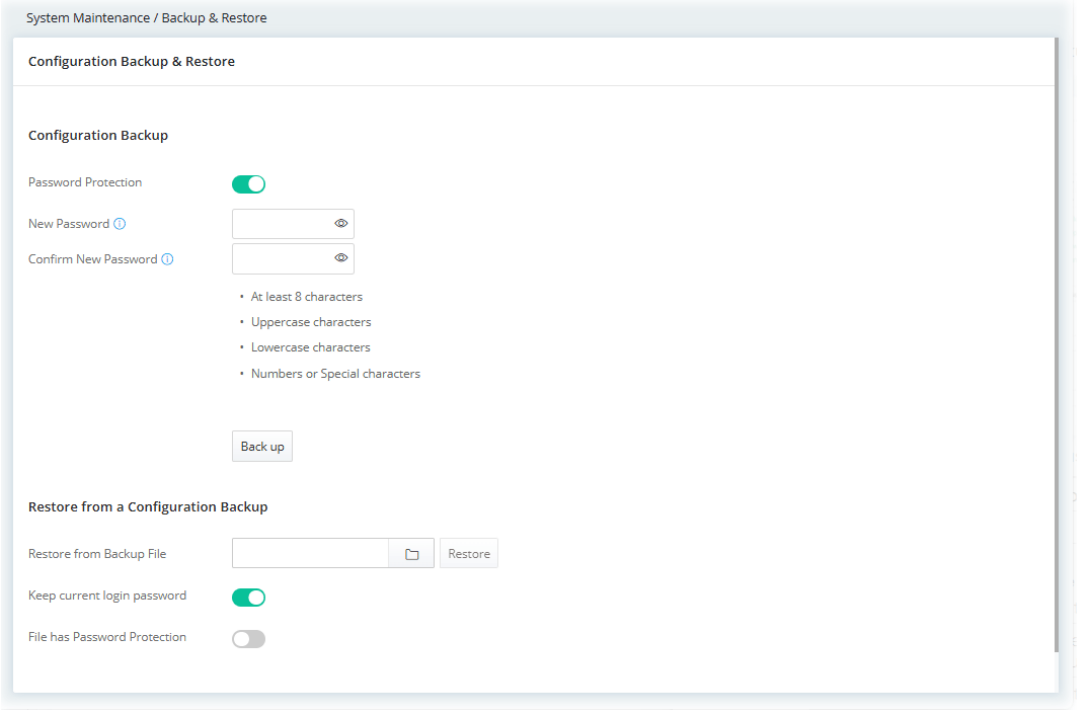


可用設定說明如下：

項目	說明
立即升級 (Upgrade Now)	按此升級 GeoIP 資料庫。
自動升級排程 (Automatic Upgrade Schedule)	**關閉(Off) –** 即使有新版本可用，也無需升級資料庫。 **稍後升級(Upgrade Later) –** 允許指定資料庫升級時間。 ● **起始日期(Start Date) –** 使用下拉式日曆指定正確的日期。  ● **起始時間(Start Time) -** 使用下拉式清單選擇時間。 **重覆(Repeat) –** 系統將在每月的第一天檢查是否有新的版本更新。 ● **每個月第一天，在(1st of each month at) -** 使用下拉式清單選擇時間。

III-1-4 備份與還原(Backup & Restore)

此功能可用於備份/還原 Vigor 路由器設定。



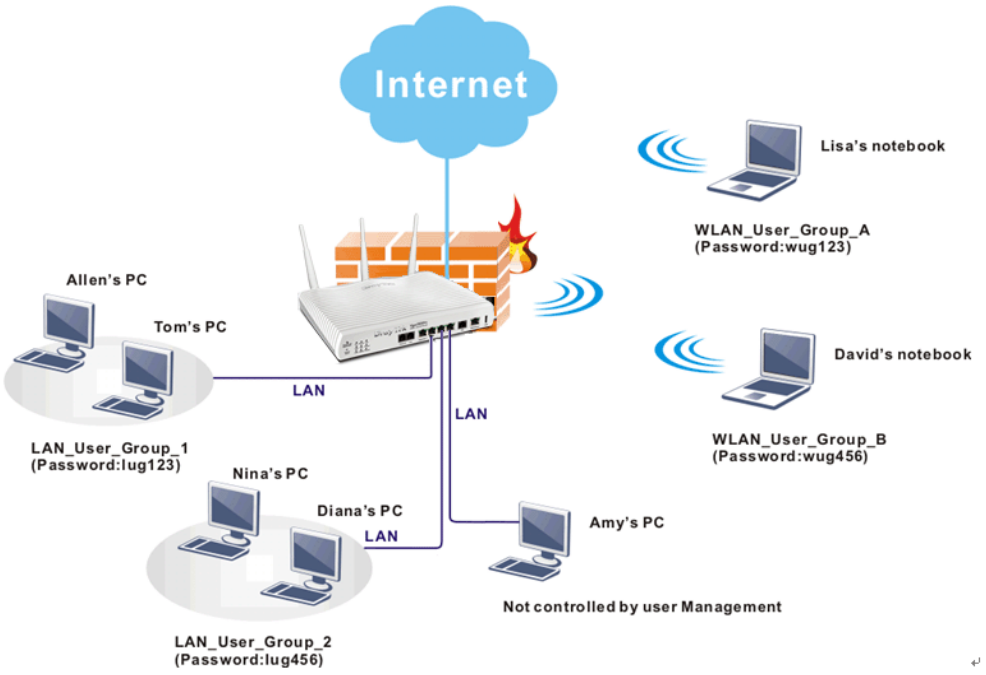
可用設定說明如下：

項目	說明
Configuration Backup	
密碼保護(Password Protection)	因應安全性之故，路由器的設定檔是可以加密處理的。 切換開關以便啟用或停用該功能。
新的密碼/確認新密碼(New Password/ Confirm New Password)	輸入幾個字元作為加密設定檔的密碼。
備份(Back up)	按此即可備份設定檔。
從設定備份還原(Restore from a Configuration Backup)	
還原自備份檔案(Restore from Backup File)	- 按此尋找用於升級的韌體檔案。 還原(Restore) - 按此執行還原作業。
保留目前登入密碼(Keep current login password)	切換開關即可啟用或停用此功能。
檔案具有密碼保護(File has Password Protection)	切換開關即可啟用或停用此功能。如果啟用，則還原設定時需要密碼。 還原密碼(Restore Password) -輸入用於還原設定的密碼。

III-1-5 帳號與許可(Account & Permission)

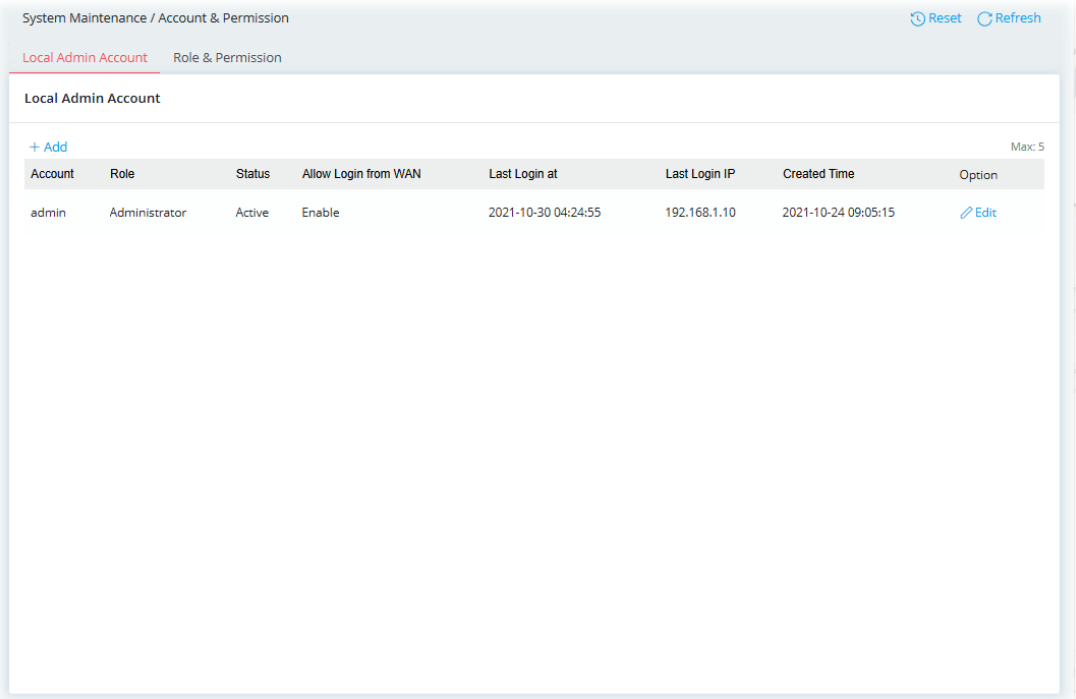
此頁面可讓您修改目前管理員帳號及密碼。

允許網路管理員在用戶層級管理網路存取。



III-1-5-1 本機管理帳號(Local Admin Account)

此頁面可讓您建立最多五個本機管理員帳戶設定檔。

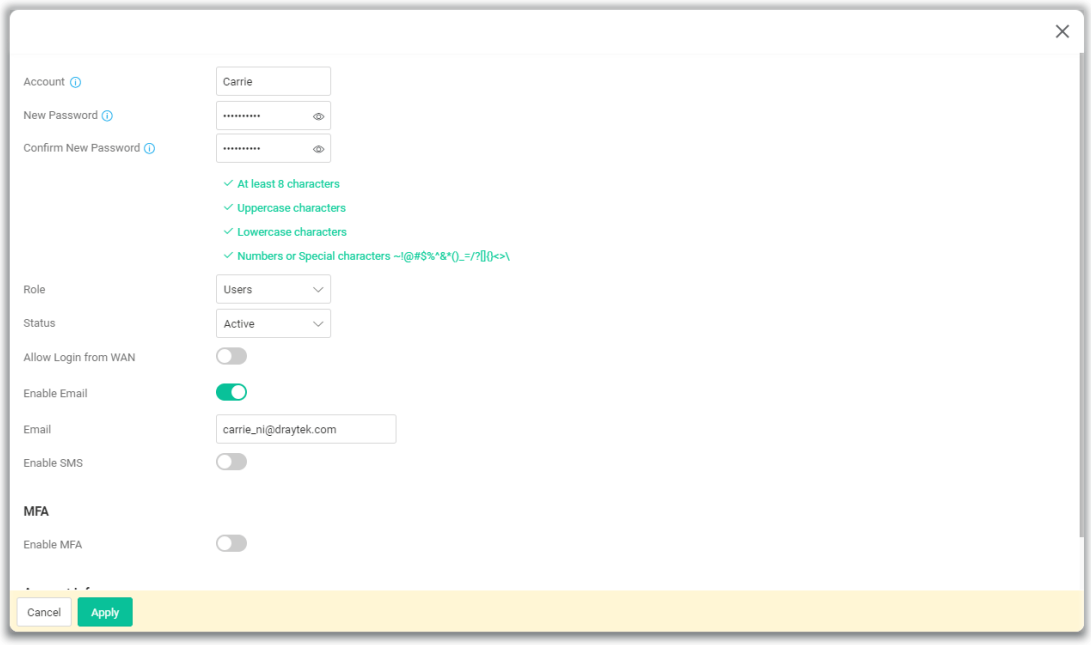


可用設定說明如下：

項目	說明
新增(+Add)	建立一個新的帳號設定檔。
編輯(Edit)	修改選定的設定檔。
刪除(Delete)	移除選定的設定檔。

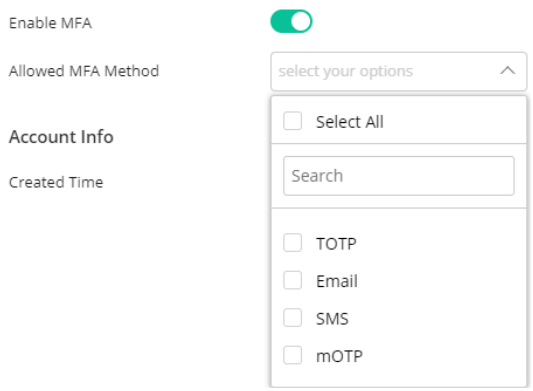
欲修改現有設定檔案，請選擇該設定檔，然後按一下**+編輯(+Edit)**連結以開啟設定頁面。

欲新增全新的設定檔，請按一下**新增(+Add)**。



可用設定說明如下：

項目	說明
本機管理帳號(Local Admin Account)	
帳號(Account)	顯示帳號的名稱。
新的密碼(New Password)	於此區輸入密碼。
確認新的密碼(Confirm New Password)	再次輸入密碼。
角色(Role)	指定帳號的角色。 • **管理者(Administrator)** • **訪客(Guest)** • **使用者定義角色(於 Role & Permission 頁面建立)**
狀態(Status)	**使用中(Active)** - 啟用選定的帳號設定檔。 **未啟用(Inactive)** – 停用選定的帳號設定檔。
允許透過 WAN 登入 (Allow Login from WAN)	如果啟用此功能，使用者可以透過此使用者帳號從 WAN 端登入。
啟用(Enable) Email	切換此開關即可啟用或停用電子郵件設定。 **電子郵件(Email)** – 輸入用於接收 MFA PIN 碼的電子郵件地址。

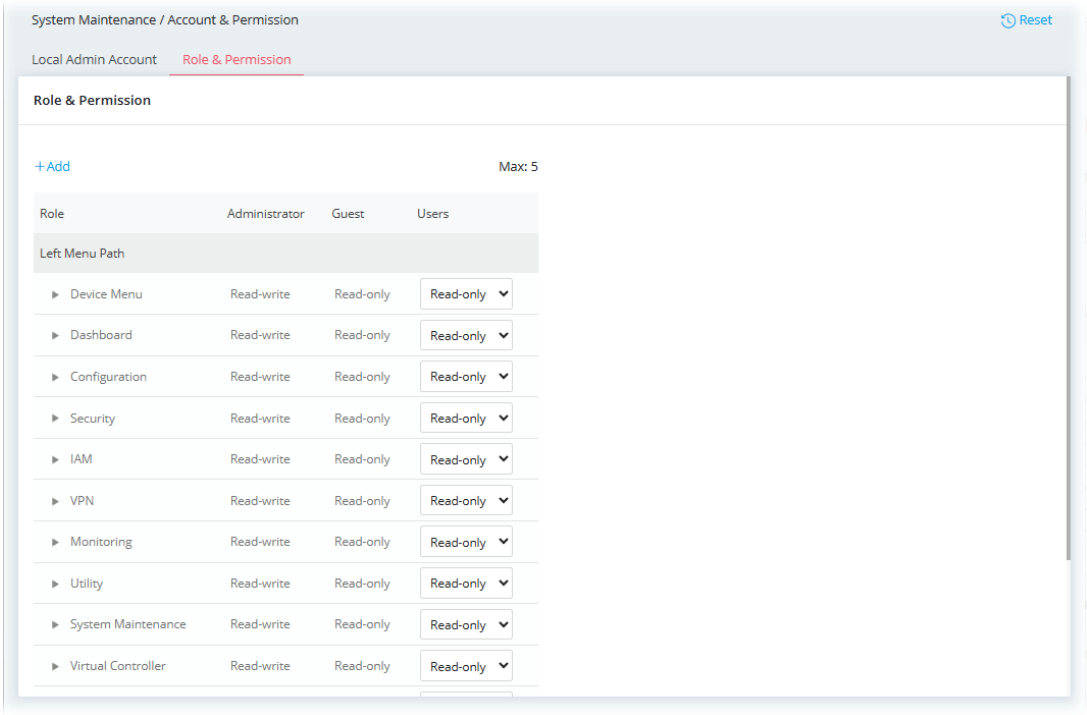
啟用(Enable) SMS	切換此開關即可啟用或停用簡訊(SMS)設定。 **簡訊** - 輸入接收 MFA PIN 碼的簡訊接收號碼。
MFA	
啟用(Enable) MFA	切換此開關以啟用/停用多因身份驗證 (MFA) 功能。 **允許的 MFA 方式(Allowed MFA Method)**- 選擇登入 Vigor 路由器時是否需要 TOTP、電子郵件或簡訊身份驗證。  **TOTP** – 對於基於時間的一次性密碼 (TOTP) 機制，請確保您的路由器時區設定正確。然後，在您的手機上安裝 Google Authenticator 應用程式。開啟應用程式並掃描此頁面上的二維碼(QR code)。一次性密碼將顯示在您的手機上。  在驗證碼(Validation Code)欄位中，輸入一次性密碼，然後按一下驗證(Verify)。 現在設定已完成。在通過使用者名稱和密碼驗證後，系統將要求您輸入雙因認證碼。 **簡訊/電子郵件(SMS/Email)** –系統將透過您在上述使用者資訊中選擇的簡訊和/或郵件方式發送密碼。
帳號資訊(Account Info)	
建立時間(Created Time)	顯示使用者帳號的建立時間。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

按下套用(Apply)以儲存設定。

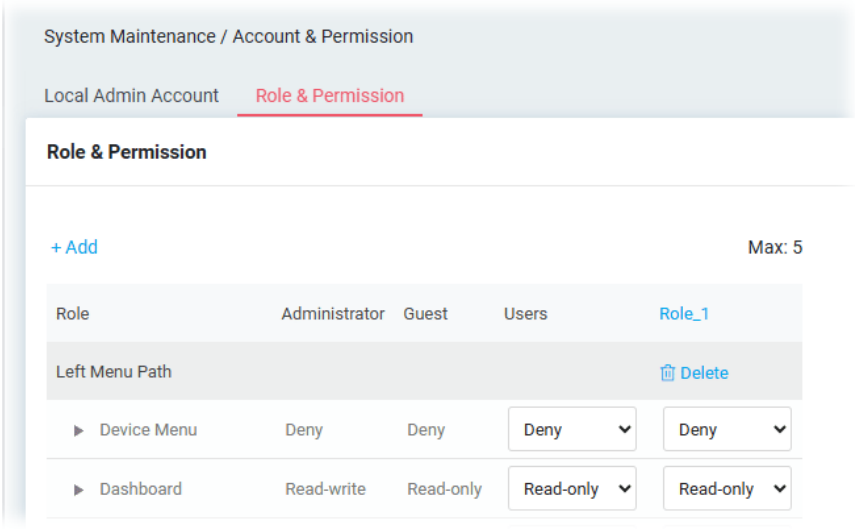
III-1-5-2 角色與權限(Role & Permission)

此頁面允許建立最多五個角色，這些角色可以應用於本機管理帳號。

預設角色包括管理者、訪客和使用者。

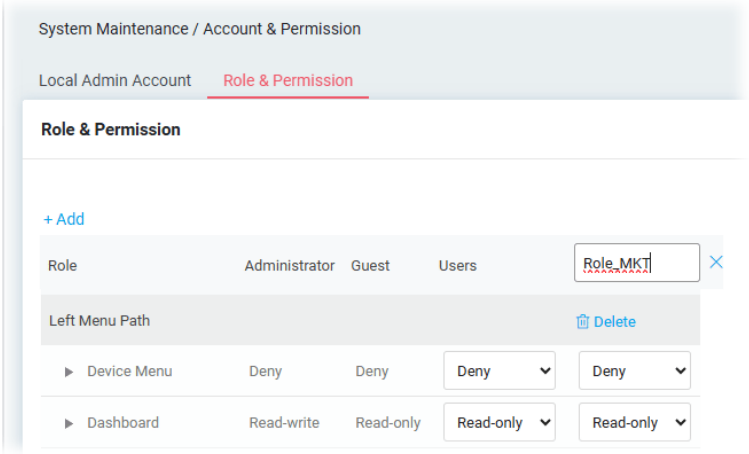
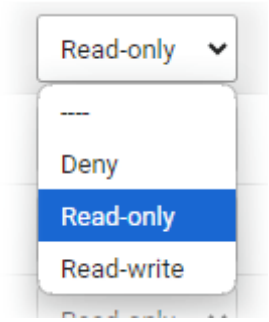


若要建立新的角色設定檔，請按下**+新增(Add)**，頁面上將會新增一個新角色。

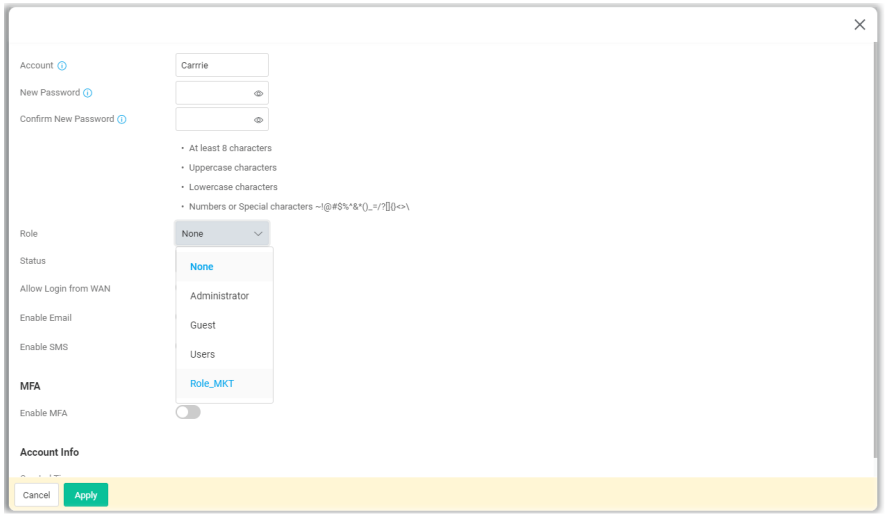


可用設定說明如下：

項目	說明
+新增(Add)	建立新的角色設定檔。
Role_1	設定檔名稱欄位。新增的設定檔將命名為 Role_#。要修改名稱，只需按下該名稱並輸入新字串（例如，Role_MKT）即可。

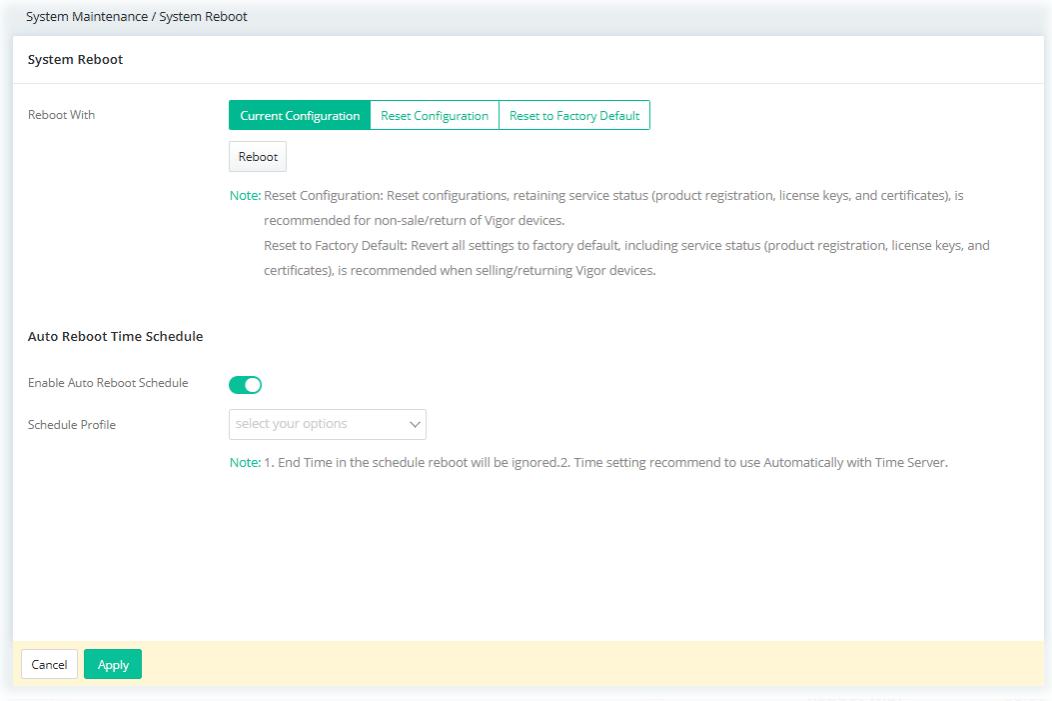
	
左側選單路徑 **(Left Menu Path)**	**管理者**擁有存取 Vigor 路由器的最高權限。 **訪客/使用者**對存取 Vigor 路由器擁有最低權限。 使用者自訂角色的權限是基於對每個選單路徑 (例如儀表板、配置、裝置選單等) 單獨授予的唯讀或讀寫存取權限。
刪除(Delete)	移除選定的使用者自訂角色設定檔。
	為使用者定義的角色指定每個選單項目的權限。 **拒絕(Deny)**- 使用者自訂角色設定檔無權存取左側選單項目。 **僅限閱讀(Read-only)**- 左側選單項目的權限允許使用者自訂角色設定檔為僅限閱讀。 **讀寫(Read-write)**- 左側選單項目的權限允許使用者定義的角色設定檔既可以閱讀亦可以寫入。
套用(Apply)	儲存目前設定並離開此頁面。

設定完成後，按下**套用(Apply)**。新角色可以在以下位置查看和選擇：**系統維護>>帳戶和權限>>本機管理帳號(System Maintenance>>Account & Permission>>Local Admin Account)**。



III-1-6 系統重新啟動(System Reboot)

網頁使用者介面可以用來重新啟動路由器。打開**系統維護>>系統重新啟動(System Maintenance >> System Reboot)**取得以下頁面。

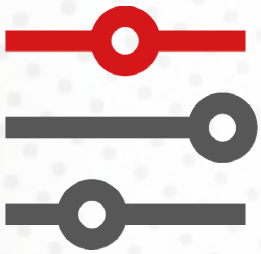


可用設定說明如下：

項目	說明
重新啟動的方式(Reboot With)	選擇下述選項其中之一種，然後按**重新啟動(Reboot)**按下按鈕重新啟動路由器。 **目前設定(Current Configuration)** – 選擇此選項可使用目前設定，重新啟動路由器。 **重置設定(Reset Configuration)** – 選擇此選項可將某些服務狀態(產品註冊、許可證金鑰和憑證)保留的情況下重設路由器。 **回復到出廠預設值(Reset to Factory Default)** – 選擇此選項可在重新啟動前將路由器的設定值重設為出廠預設值。
自動重啟時間排程(Auto Reboot Time Schedule)	**啟用自動重啟排程(Enable Auto Reboot Schedule)** – 切換此開關即可啟用或停用此功能。 啟用時，路由器將會依照選擇的排程自動地重新啟動。 **排程設定檔(Schedule Profile)** – 使用下拉是清單選擇設定檔。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

本頁留白

第四章 其他

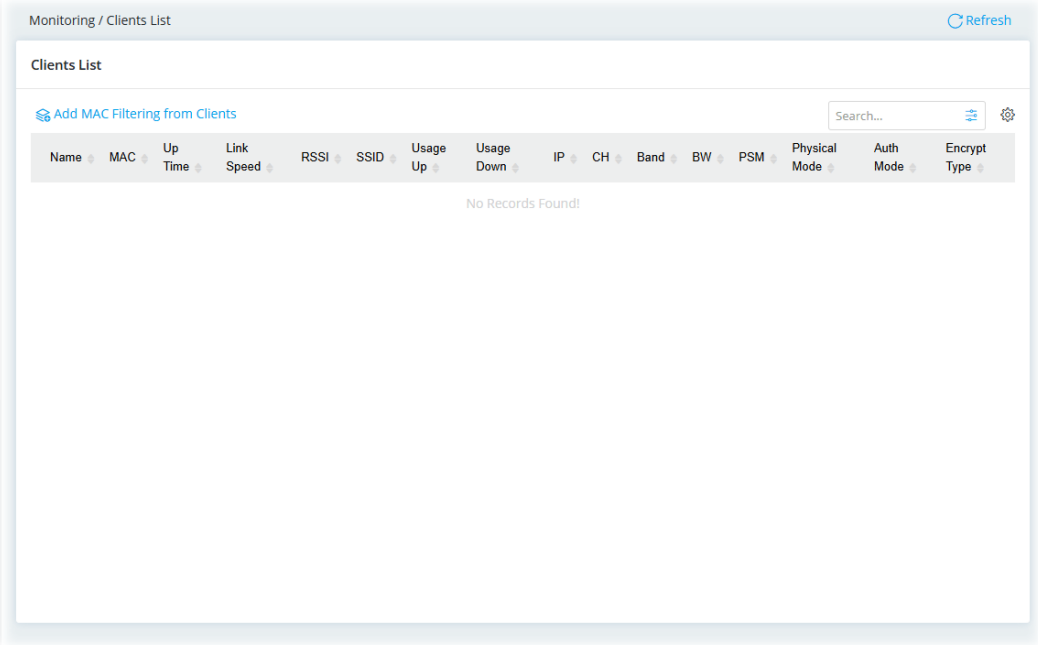


IV-1 監控(Monitoring)

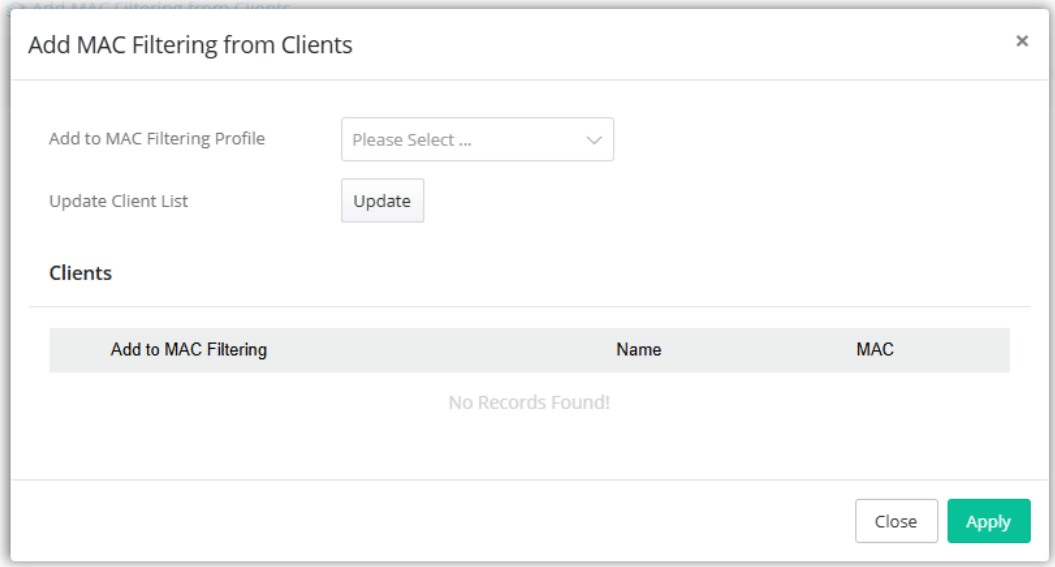
IV-1-1 用戶端清單(Clients List)

用戶端清單顯示透過 Wi-Fi 連線連接到 Vigor 路由器的無線用戶端的設定狀態。

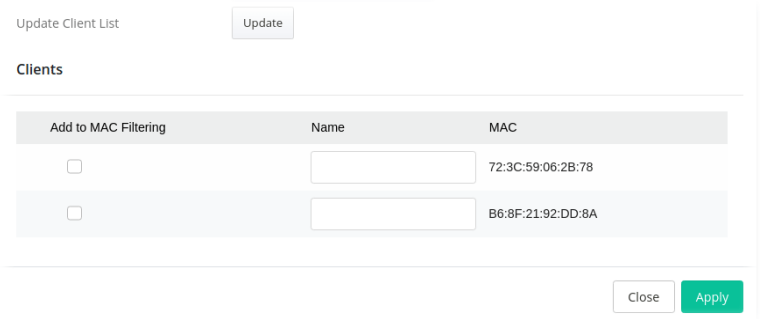
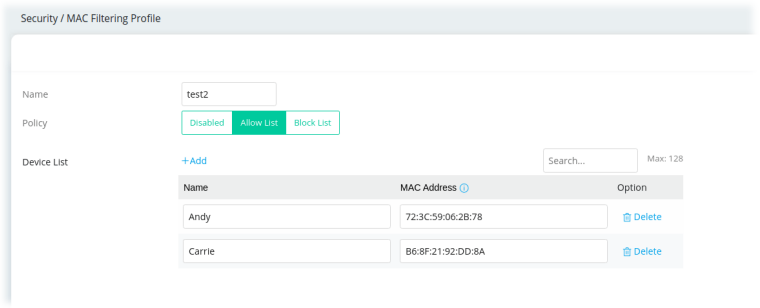
此外，本頁面還提供了一種快速方法，可將無線用戶端新增至任何現有的 MAC 位址過濾設定檔中。



若要將無線用戶端新增至現有的 MAC 位址過濾設定檔中，請按一下**新增客戶端 MAC 位址過濾功能(Add MAC Filtering from Clients)** 開啟下一頁。



可用設定說明如下：

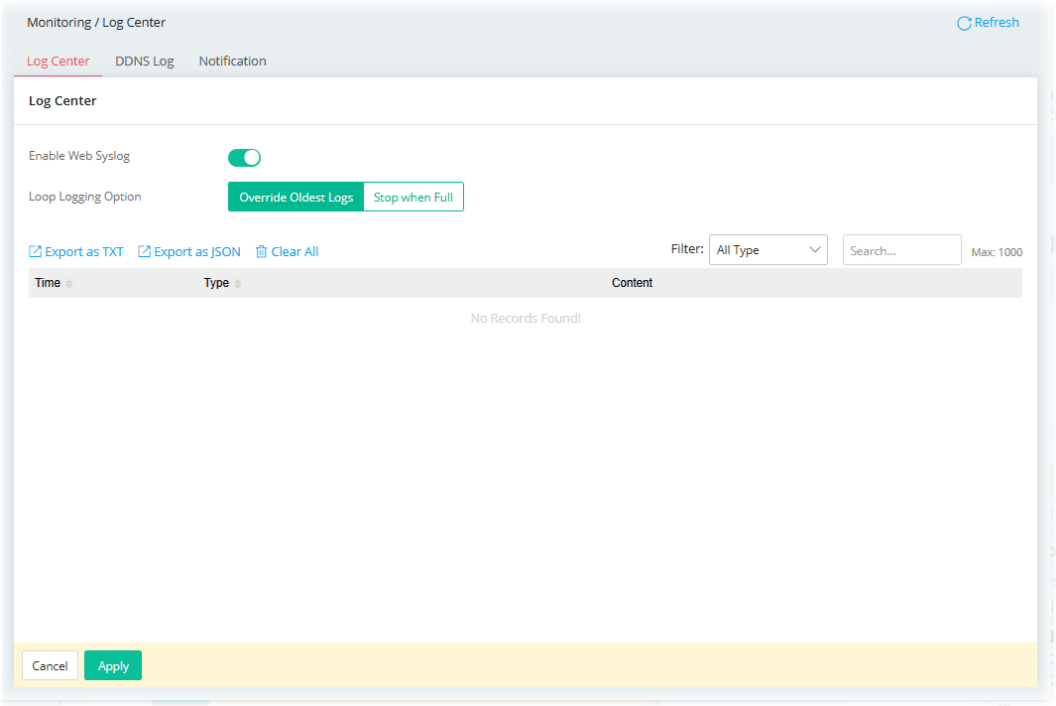
項目	說明
新增至 MAC 位址過濾設定檔 **(Add to MAC Filtering Profile)**	自下拉式清單選擇其中一個 MAC 位址過濾設定檔(安全性>>MAC 位址過濾設定檔)作為過濾基礎。
更新用戶端清單 **(Update Client List)**	**更新(Update)** –按下此鈕以便根據實際無線連線更新用戶端清單。 
用戶端(Clients)	顯示無線用戶端的 SSID 名稱、MAC 位址和 IP 位址。 **新增至 MAC 位址過濾(Add to MAC Filtering)**–選擇此項目可使無線用戶端加入上面設定的 MAC 過濾設定檔。 **名稱(Name)** - 請輸入用於識別的名稱。
關閉(Close)	放棄目前設定並返回上一頁。
套用(Apply)	儲存目前設定並離開此頁面。 若要檢查新新增的無線用戶端是否已新增至 MAC 位址過濾設定檔中，請參閱**安全性>>MAC 位址過濾設定檔(Security>>MAC Filtering Profile)**。 

按下**套用(Apply)**以儲存設定。

IV-1-2 日誌中心(Log Center)

IV-1-2-1 日誌中心(Log Center)

與此設備的設定與/或執行操作的相關日誌，可以儲存在 Web Syslog 系統日誌中。按下更新頁面(Refresh)重新加載此頁面以獲取最新資訊。



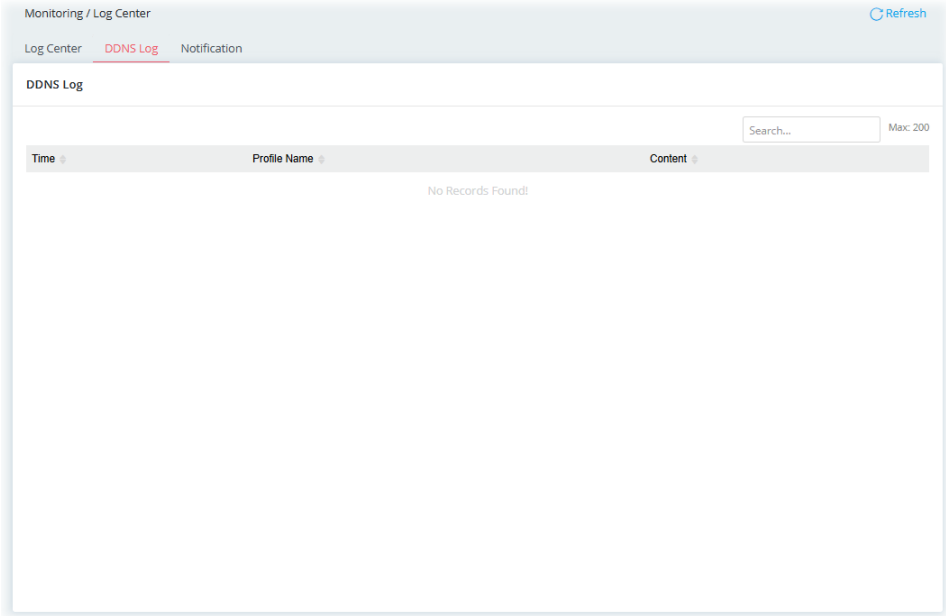
可用設定說明如下：

項目	說明
啟用網頁 Syslog (Enabled Web Syslog)	切換開關即可啟用或停用此功能。 如果啟用此功能，循環日誌記錄選項(**Loop Logging Option**)將顯示於後。
循環日誌記錄選項 (Loop Logging Option)	**覆寫最舊之日誌(Override Oldest Logs)** - Vigor 路由器系統會將快閃記憶體中所有現有資訊備份到主機，並清除快閃記憶體中的資訊。之後，開始新的記錄。 **滿碟時停止紀錄(Stop when Full)** - Vigor 路由器系統將停止向快閃記憶體記錄使用者資訊。
匯出 TXT 檔案(Export as TXT) **匯出 JSON 檔案(Export as JSON)**	按此即可將日誌記錄匯出為檔案(.txt, .json)。
清除全部(Clear All)	按此即可清除此頁面上的所有日誌記錄。
過濾器(Filter)	選擇要在此頁面顯示的日誌類型。
取消(Cancel)	捨棄目前設定並離開此頁面。
套用(Apply)	儲存目前設定並離開此頁面。

按下**套用(Apply)**以儲存設定。

IV-1-2-2 DDNS 日誌(DDNS Log)

此頁面可顯示與此裝置執行的動態 DNS 操作相關的日誌(時間、設定檔名稱和內容)。

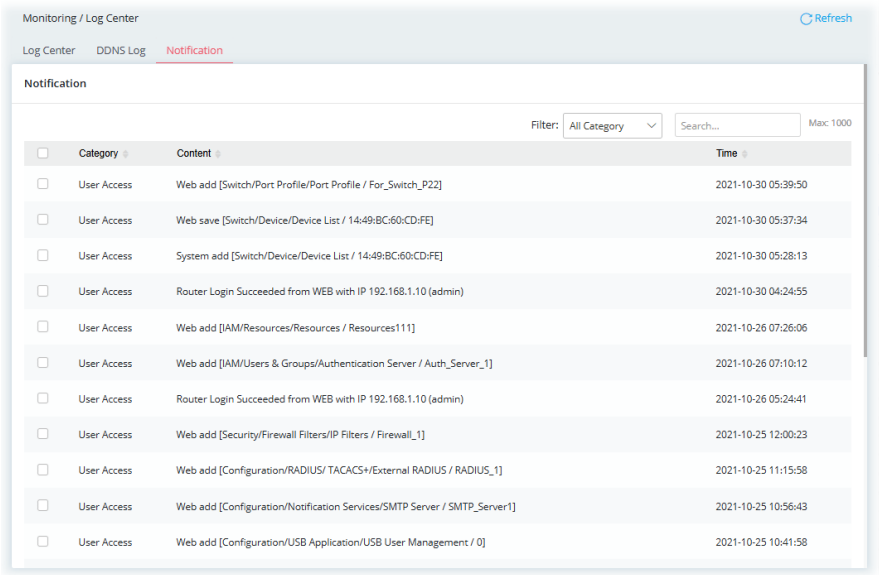


按下**更新頁面(Refresh)**重新載入此頁面以獲取最新資訊。

IV-1-2-3 通知(Notification)

此頁面顯示重要的日誌訊息，包含：

- 重要訊息
- SSH/Telnet 登入以及 Web 登入通知
- 韌體升級狀態通知
- 組態設定轉換(還原或更新)通知

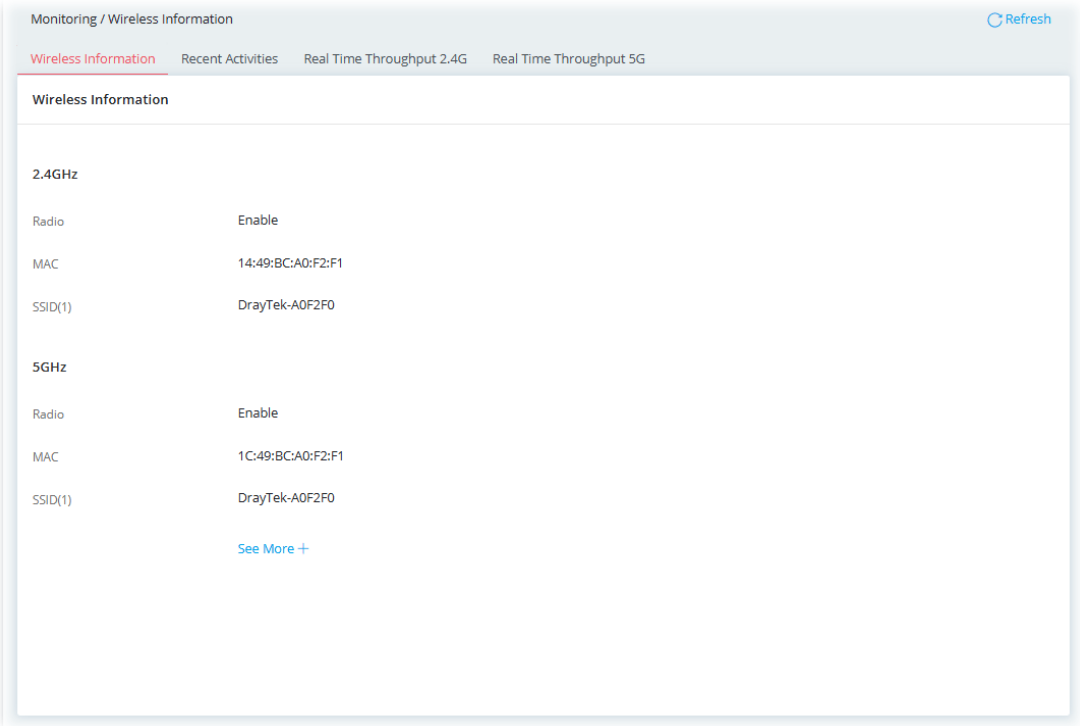


IV-1-3 無線資訊(Wireless Information)

如欲查看 2.4GHz/5GHz 所使用的 SSID 或 2.4GHz/5GHz 的即時總處理量，請開啟監控>>無線資訊(Monitoring>>Wireless Information)以查看詳細資訊。

IV-1-3-1 無線資訊(Wireless Information)

此頁面顯示無線連線的一般資訊（例如，有無啟用 2.4GHz/5GHz、MAC 位址、SSID 名稱等）。

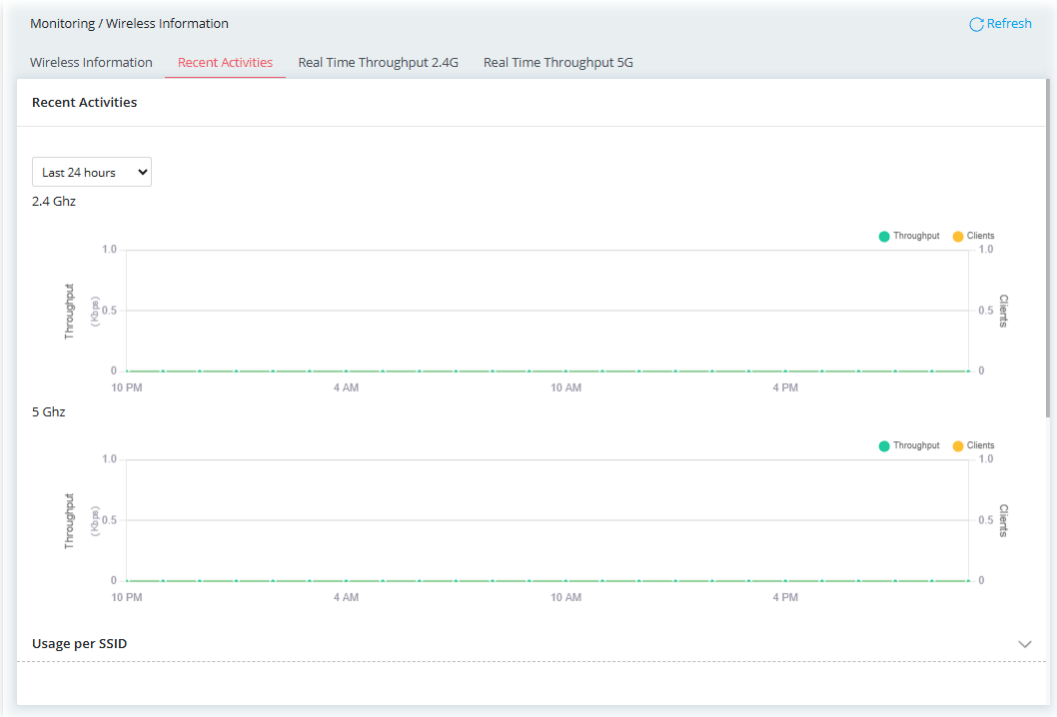


按下**更新頁面(Refresh)**重新載入此頁面以獲取最新資訊。

按下**查看更多詳情(See More+)**檢視更多資訊。.

IV-1-3-2 近期活動(Recent Activities)

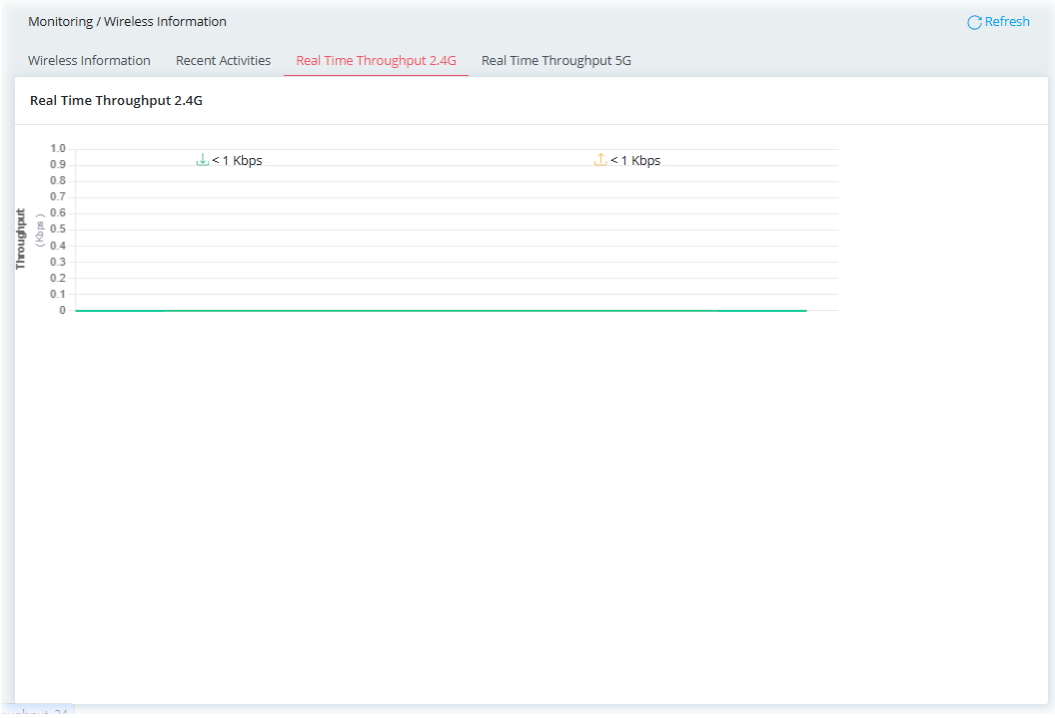
無線網路相關的活動可以用折線圖表示。



按下**更新頁面(Refresh)**重新載入此頁面以獲取最新資訊。

IV-1-3-3 即時總處理量 2.4G(Real Time Throughput 2.4G)

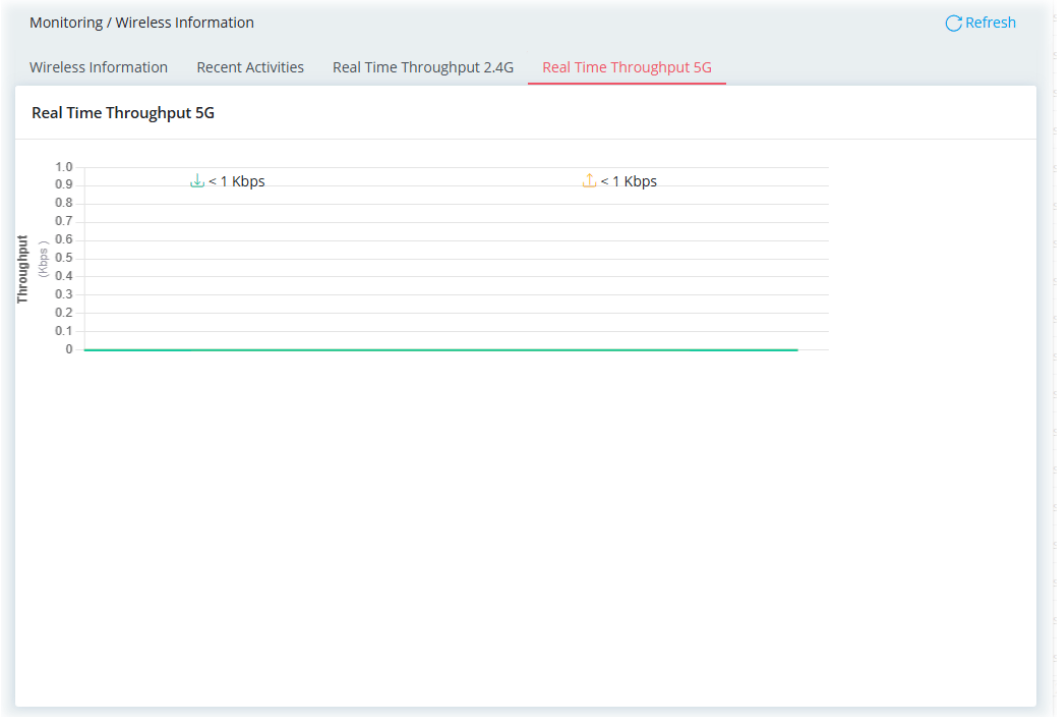
即時總處理量(2.4G)可以用折線圖表示。



按下**更新頁面(Refresh)**重新載入此頁面以獲取最新資訊。

IV-1-3-4 即時總處理量 5G(Real Time Throughput 5G)

即時總處理量(5G)可以用折線圖表示。



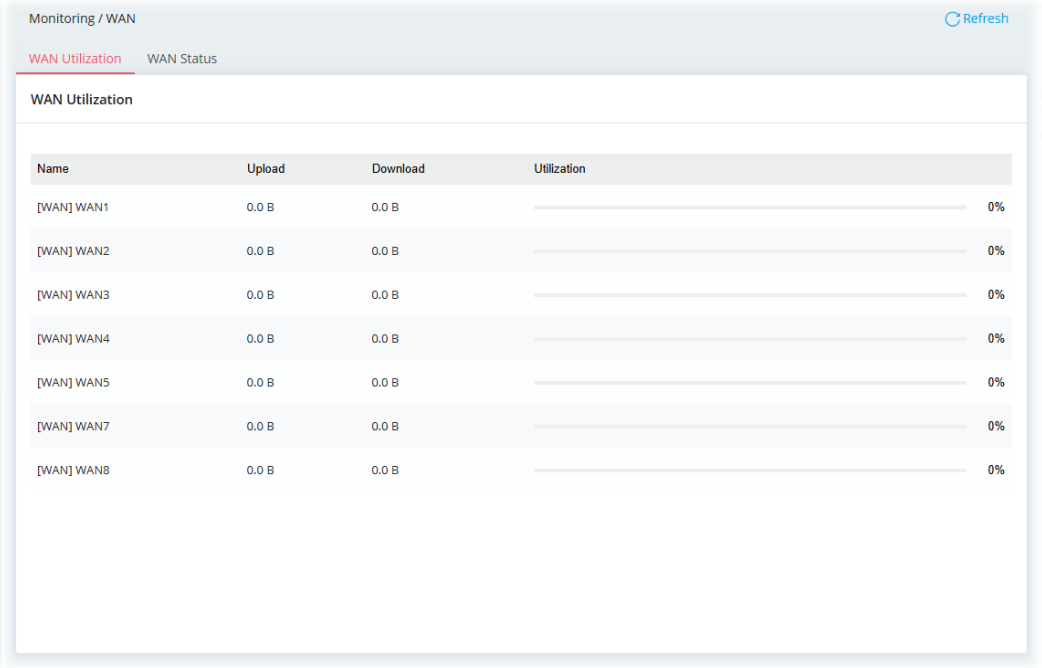
按下**更新頁面(Refresh)**重新載入此頁面以獲取最新資訊。

IV-1-4 WAN

此頁面可以顯示 WAN 連線狀態，包括連線介面、MAC 位址、連線類型、連線 IP 位址、連線閘道、主要與次要 DNS 伺服器位址、上線時間等等。

IV-1-4-1 WAN 運用(WAN Utilization)

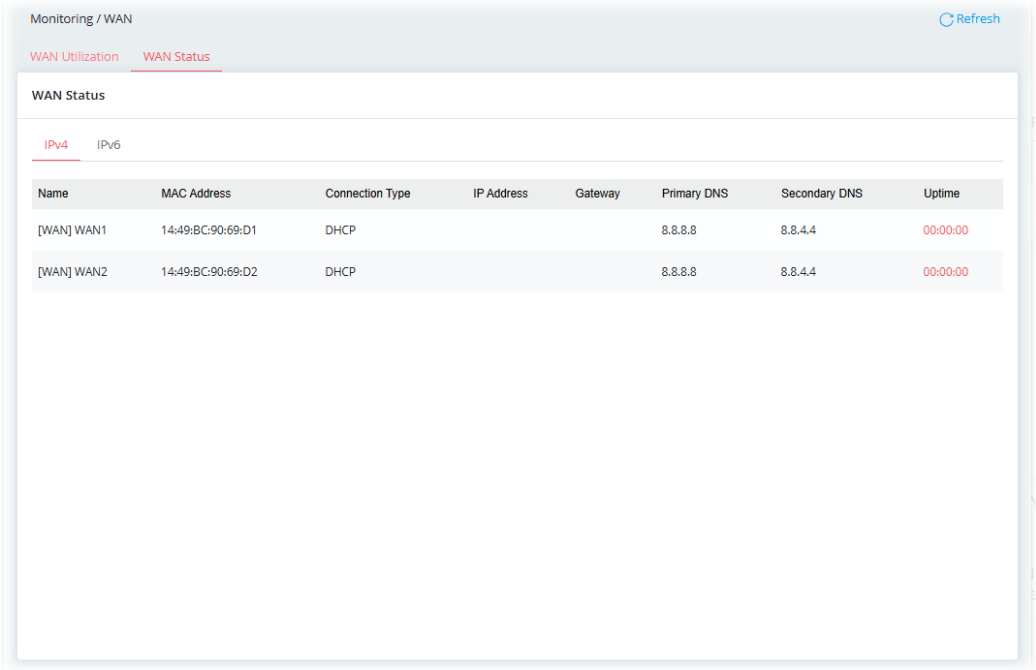
此頁面顯示各個 WAN 介面的使用率，包括上傳、下載和資料傳輸百分比等等。



IV-1-4-2 WAN 狀態(WAN Status)

IPv4

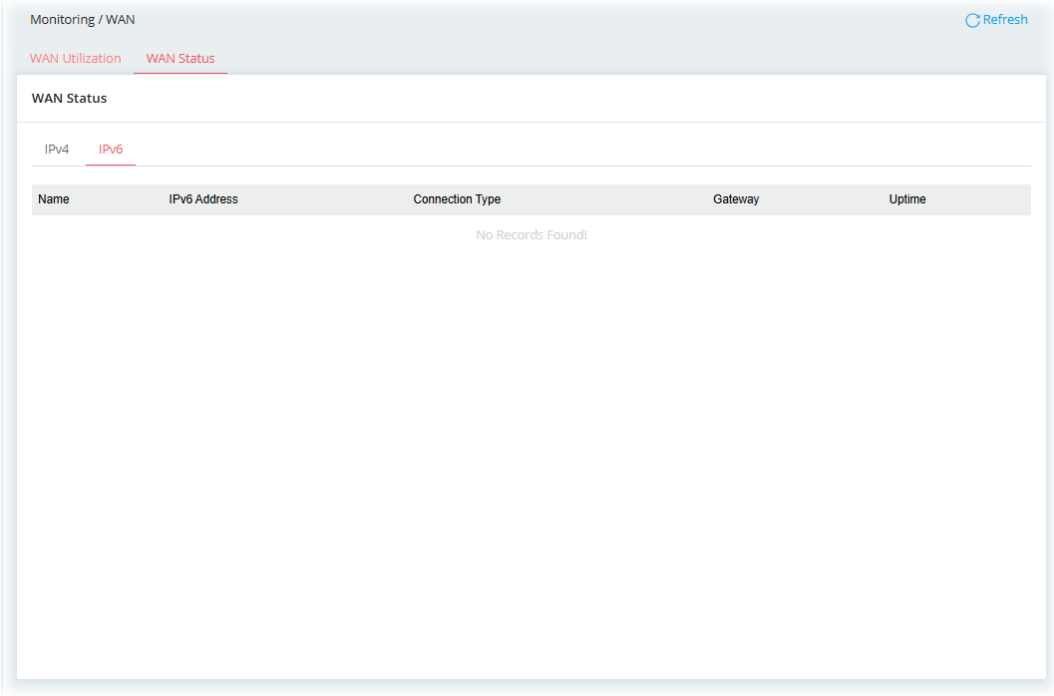
選擇 IPv4 標籤以顯示 IPv4 WAN 連線狀態。



按下**更新頁面(Refresh)**重新載入此頁面以獲取最新資訊。

IPv6

選擇 IPv6 標籤以取得 WAN 連線資訊(例如，名稱、IPv6 位址、連線類型、閘道和運行時間)。



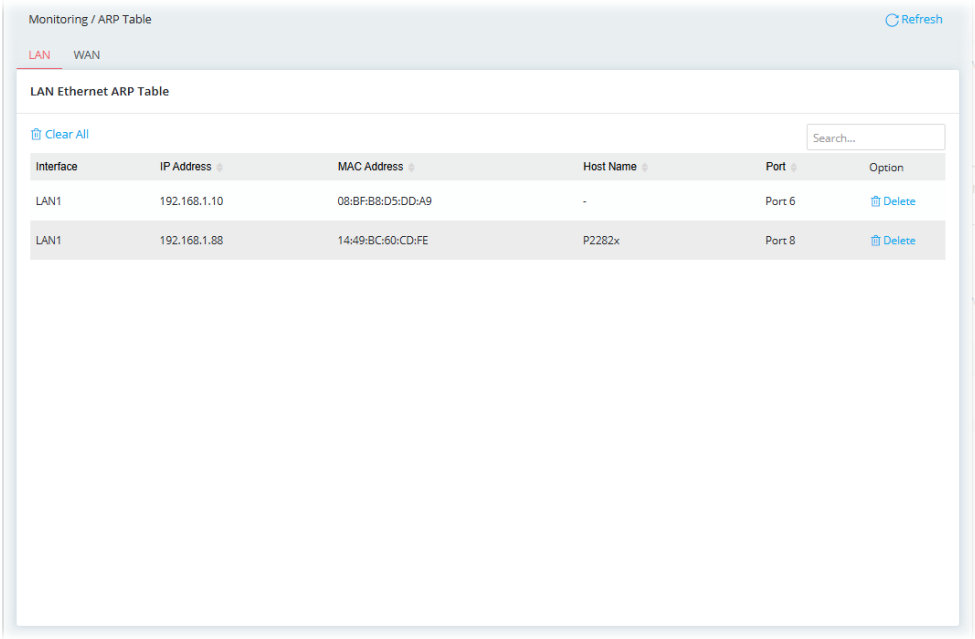
按下**更新頁面(Refresh)**重新載入此頁面以獲取最新資訊。

IV-1-5 ARP 表格(ARP Table)

此表格顯示路由器中保存的 ARP(位址解析協定)快取的內容，並顯示了乙太網路硬體位址(MAC 位址)和 IP 位址之間的對應關係。

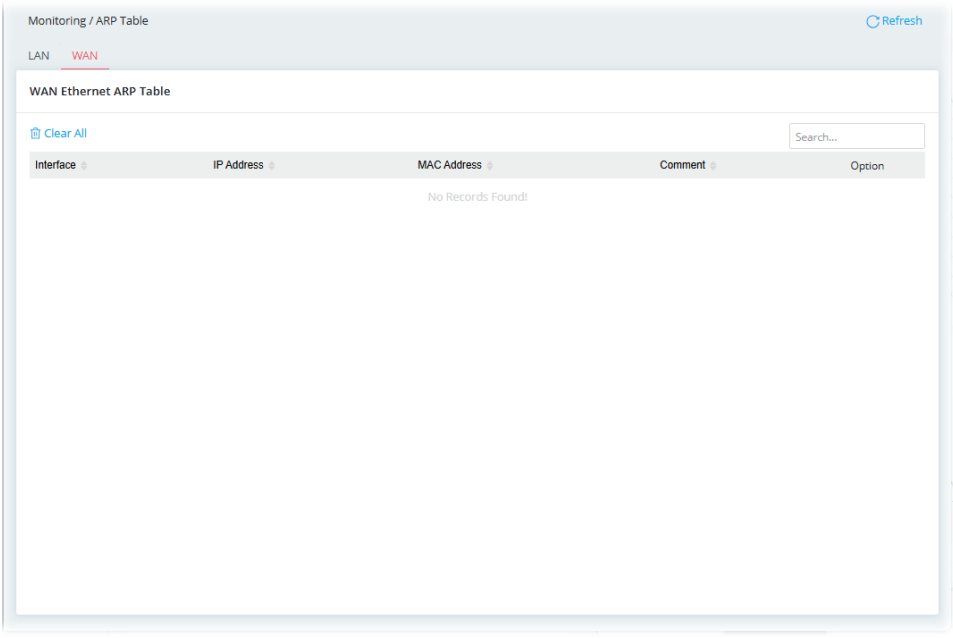
IV-1-5-1 LAN

按下**更新頁面(Refresh)** 重新載入此頁面以取得最新的 LAN 乙太網路 ARP 表格資訊。



IV-1-5-2 WAN

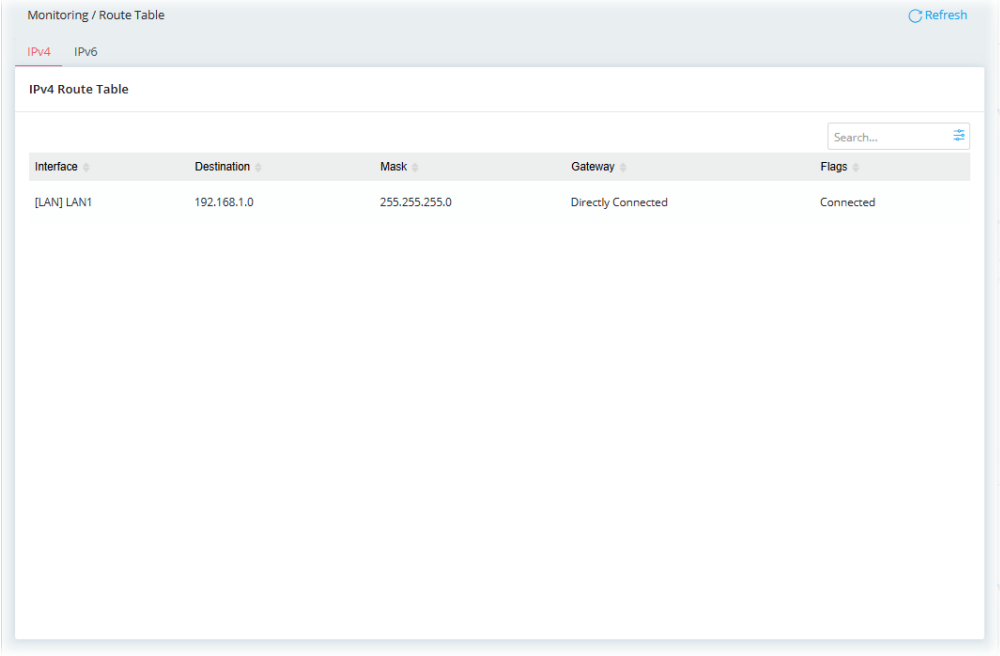
按下**更新頁面(Refresh)** 重新載入此頁面以取得最新的 WAN 乙太網路 ARP 表格資訊。



IV-1-6 路由表格(Route Table)

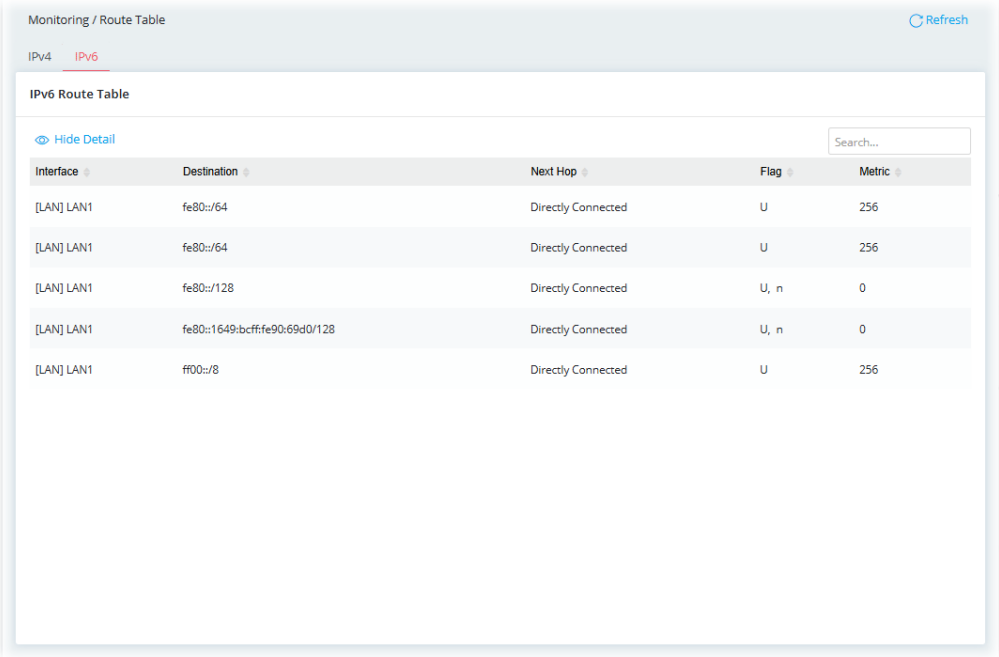
IV-1-6-1 IPv4

按下**更新頁面(Refresh)** 重新載入此頁面以取得最新的 IPv4 路由資訊。



IV-1-6-2 IPv6

按下**更新頁面(Refresh)** 重新載入此頁面以取得最新的 IPv6 路由資訊。



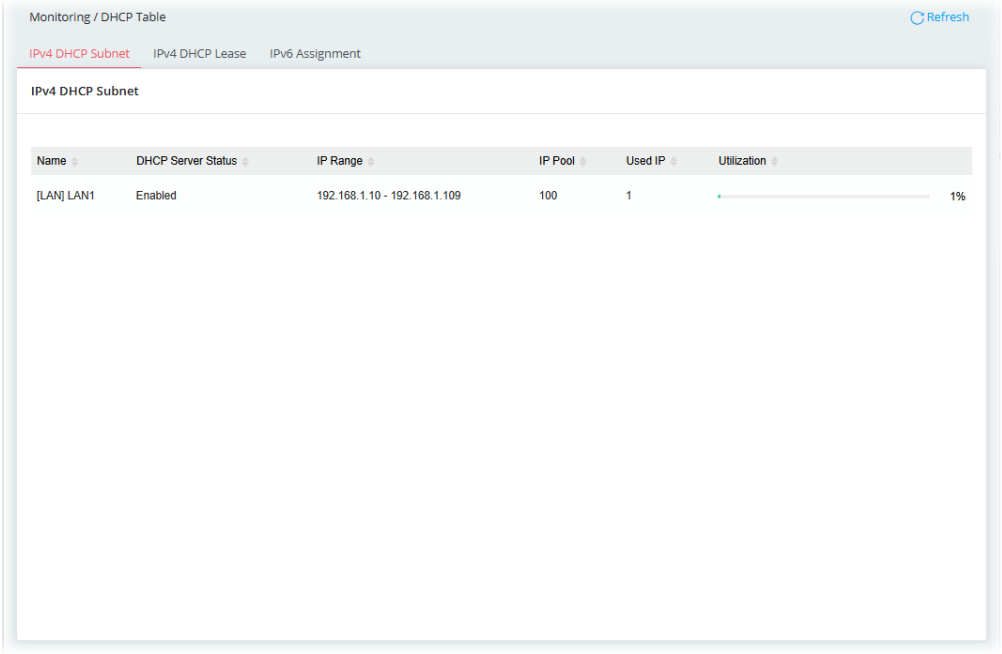
IV-1-7 DHCP 表格(DHCP Table)

本頁面提供有關 IP 位址分配的資訊。這些資訊有助於診斷網路問題，例如 IP 位址衝突等等。

按下**更新頁面(Refresh)**重新載入此頁面以獲取最新資訊。

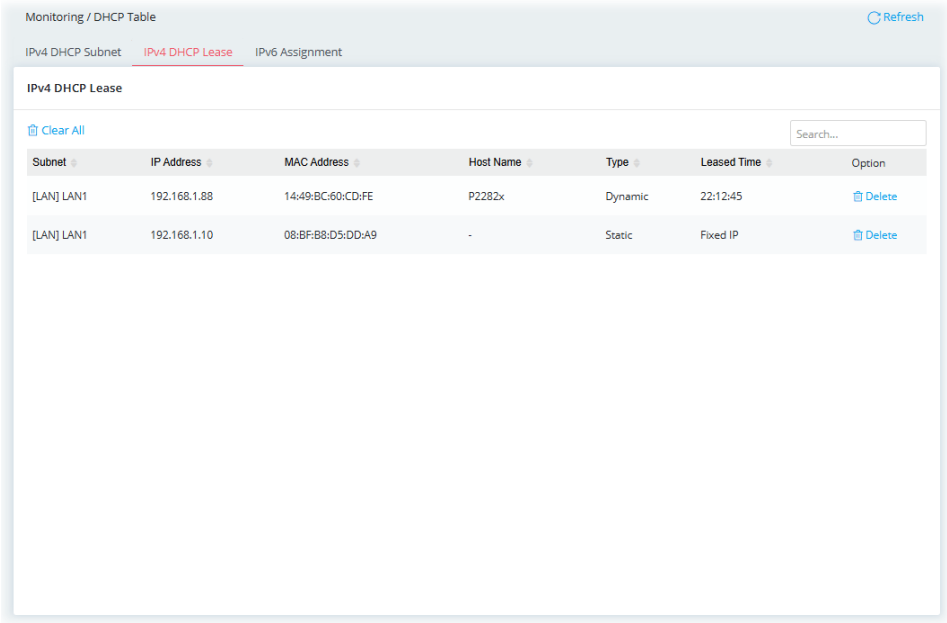
IV-1-7-1 IPv4 DHCP 子網(IPv4 DHCP Subnet)

此頁面顯示每個 LAN 介面的 DHCP 伺服器狀態、IP 位址範圍、IP 配置數量、已使用之 IP 位址和使用率百分比。



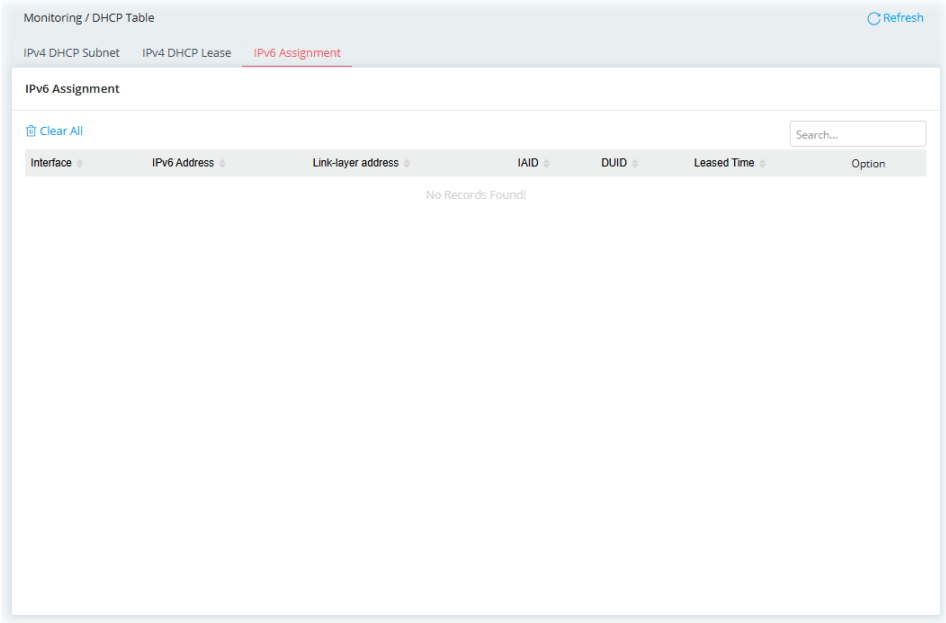
IV-1-7-2 IPv4 DHCP 租用時間(IPv4 DHCP Lease)

此頁面顯示設備的 IPv4 DHCP 租約剩餘時間。


Monitoring / DHCP Table
Refresh
IPv4 DHCP Subnet
IPv4 DHCP Lease
IPv6 Assignment
IPv4 DHCP Lease
Clear All
Search...
Subnet
IP Address
MAC Address
Host Name
Type
Leased Time
Option
[LAN] LAN1
192.168.1.88
14:49:BC:60:CD:FE
P2282x
Dynamic
22:12:45
Delete
[LAN] LAN1
192.168.1.10
08:BF:B8:D5:DD:A9
-
Static
Fixed IP
Delete

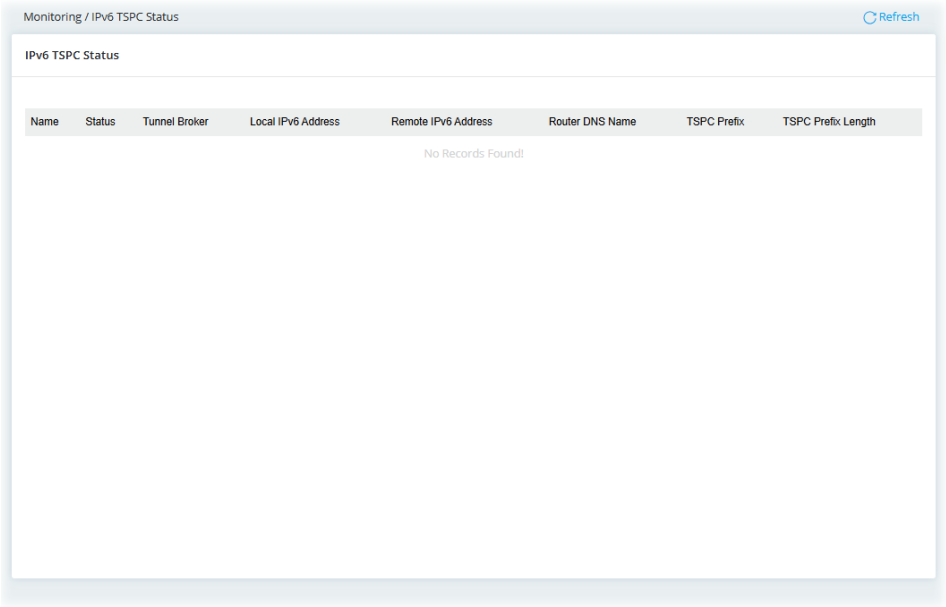
IV-1-7-3 IPv6 分派(IPv6 Assignment)

此頁面顯示設備的 IPv6 DHCP 租約剩餘時間。



IV-1-8 IPv6 TSPC 狀態(IPv6 TSPC Status)

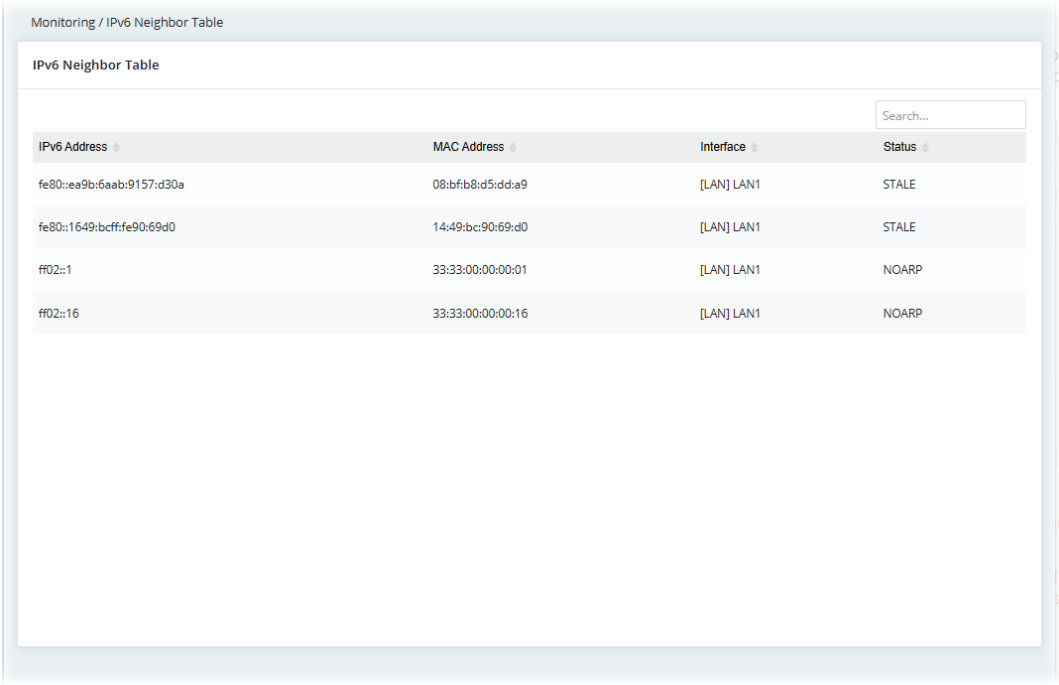
IPv6 通道建立協定用戶端(TSPC)狀態頁面可以協助您診斷使用 TSP 的 IPv6 連線的問題。如果 TSPC 設定正確，當路由器成功連接到通道代理伺服器時，路由器將可顯示以下內容。



按下**更新頁面(Refresh)**重新載入此頁面以獲取最新資訊。

IV-1-9 IPv6 相鄰表格(IPv6 Neighbor Table)

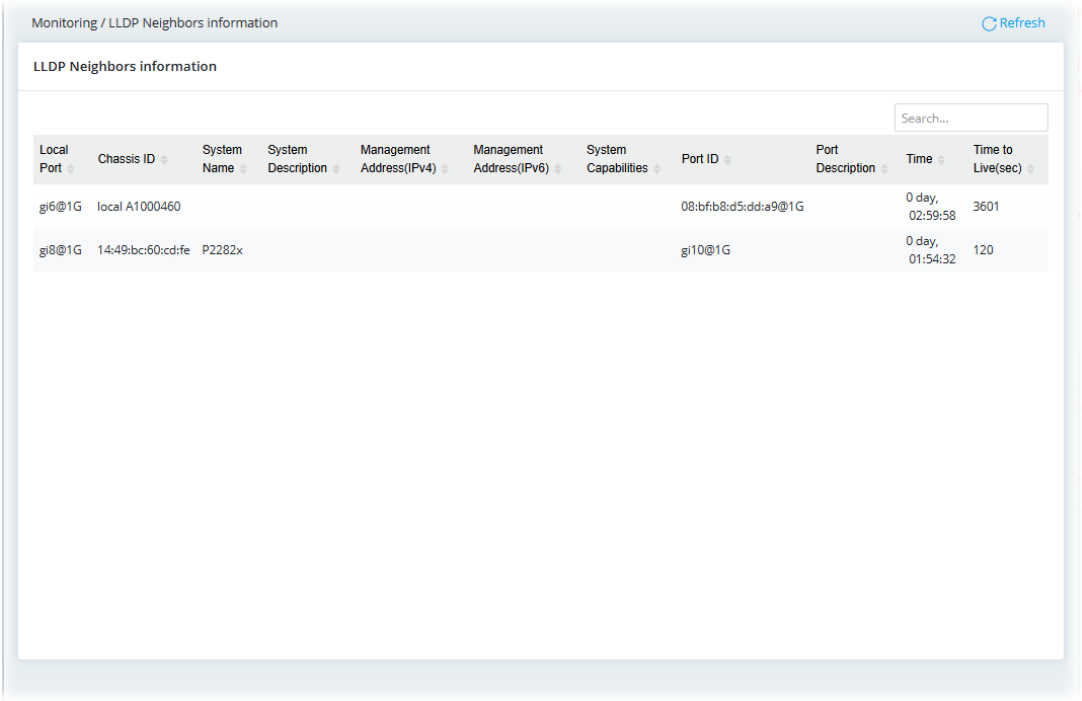
此頁面顯示乙太網路硬體位址(MAC 位址)與 IPv6 位址之間的對應關係。此資訊有助於診斷網路問題，例如 IP 位址衝突。



IV-1-10 LLDP 鄰居(LLDP Neighbors)

此頁面可讓系統管理員了解網路設備的拓撲結構以及設備之間的關係。通常資訊包含：

- 系統名稱
- 系統說明
- IPv4/IPv6 位址(可選)
- 系統功能
- 連接埠 ID
- 連接埠說明
- 時間
- 存活時間

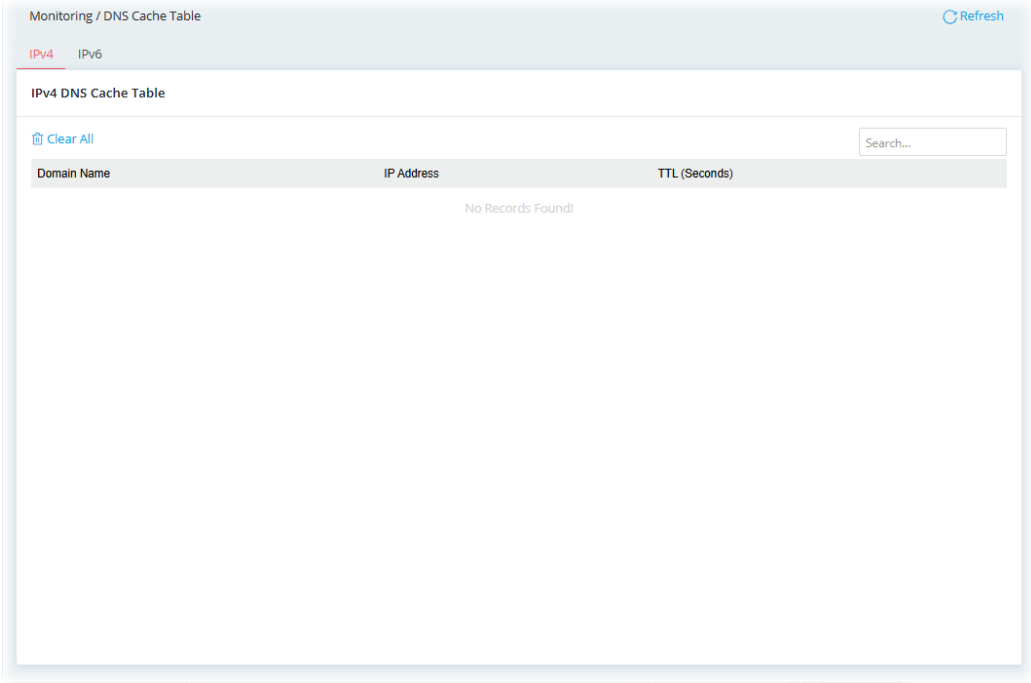


IV-1-11 DNS 快取表格(DNS Cache Table)

路由器可以做為 DNS 伺服器，允許區域網路用戶端透過向路由器發送 DNS 請求來查詢 DNS 資訊。透過此頁面可以查看暫存於路由器的 DNS 相關資訊。

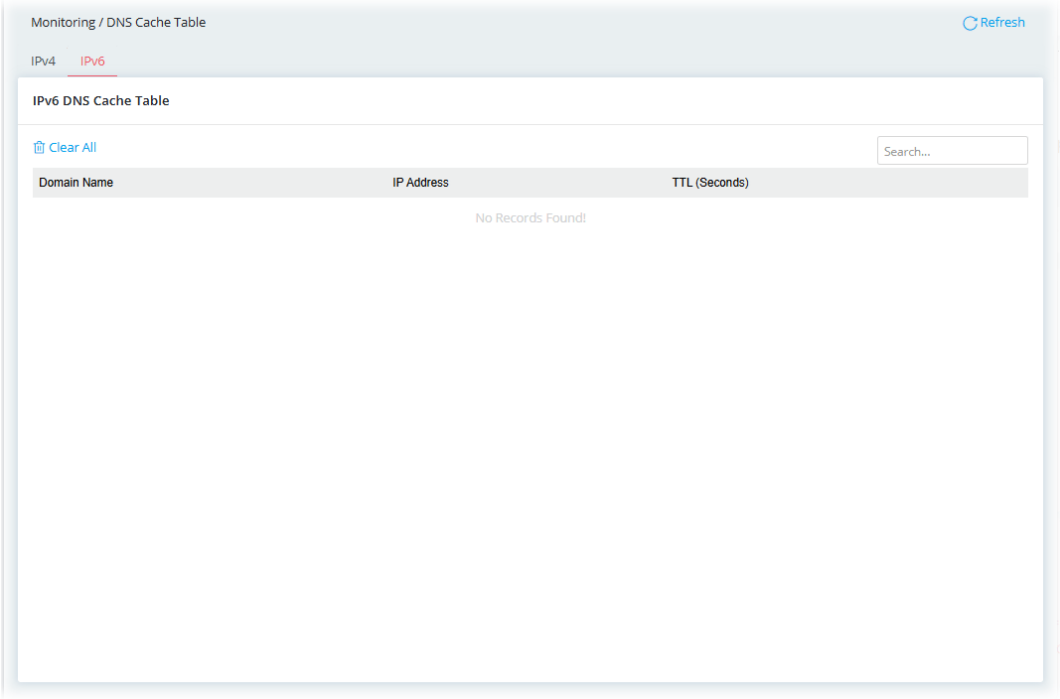
IV-1-11-1 IPv4

按下**更新頁面(Refresh)**重新載入此頁面以獲取最新 IPv4 DNS 快取資料。



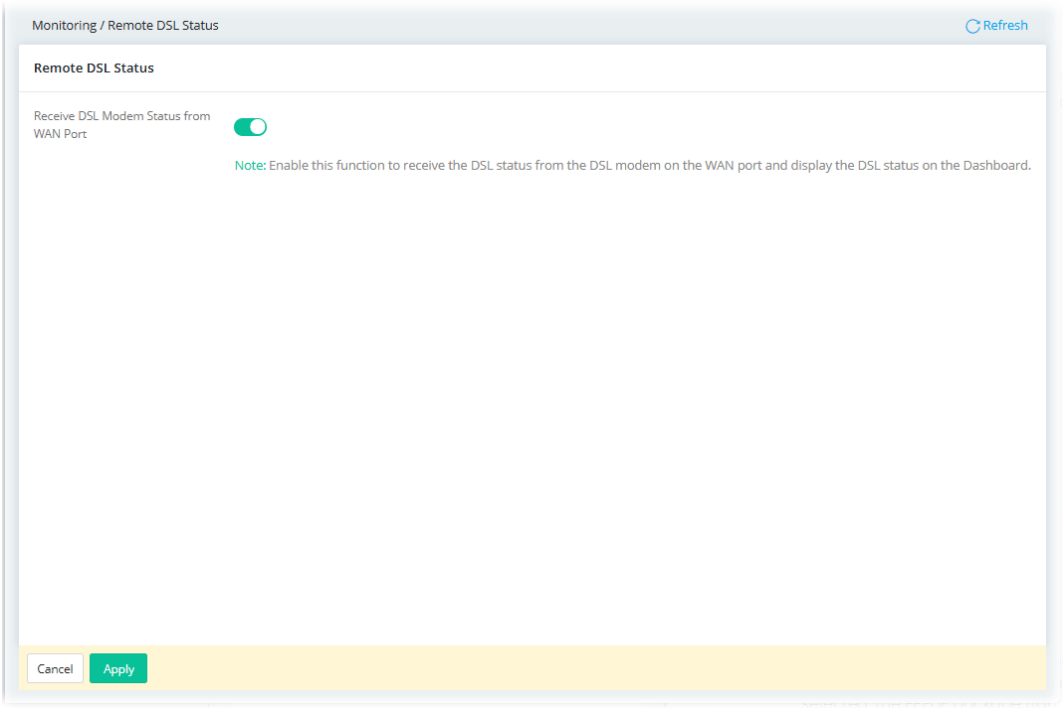
IV-1-11-2 IPv6

按下**更新頁面(Refresh)**重新載入此頁面以獲取最新 IPv6 DNS 快取資料。



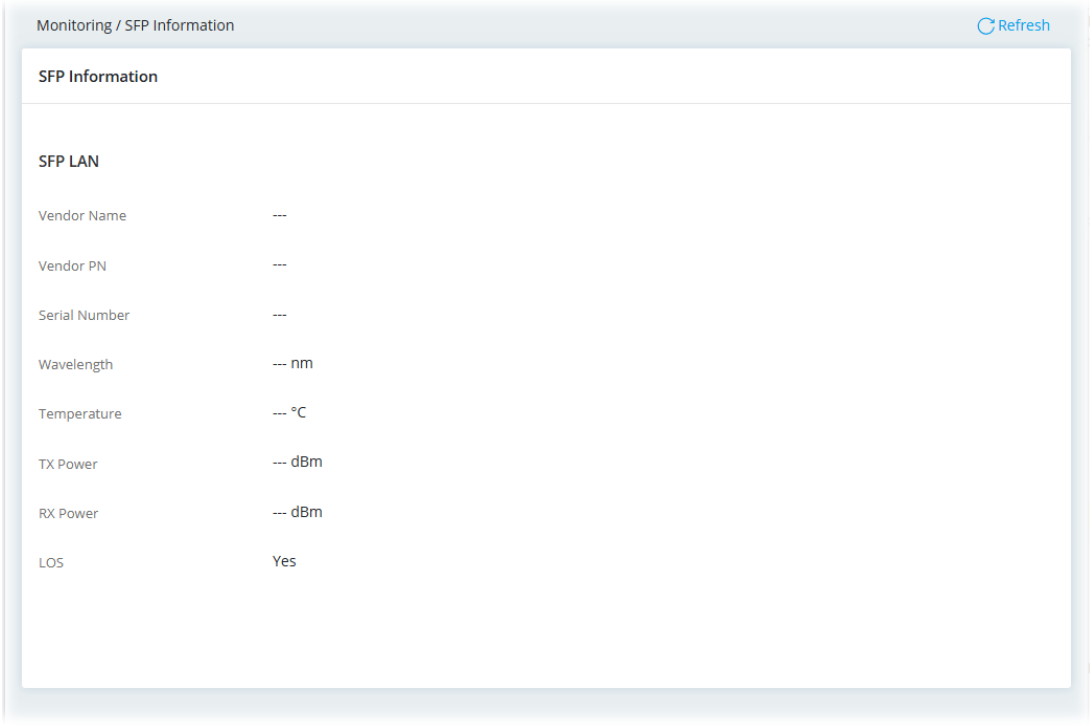
IV-1-12 遠端 DSL 狀態(Remote DSL Status)

此頁面允許您啟用或停用從 WAN 連接埠上的 DSL 數據機接收 DSL 狀態，並在儀表板上顯示 DSL 狀態的功能。



IV-1-13 SFP 資訊(SFP Information)

顯示 SFP WAN 和 SFP LAN 的資訊。

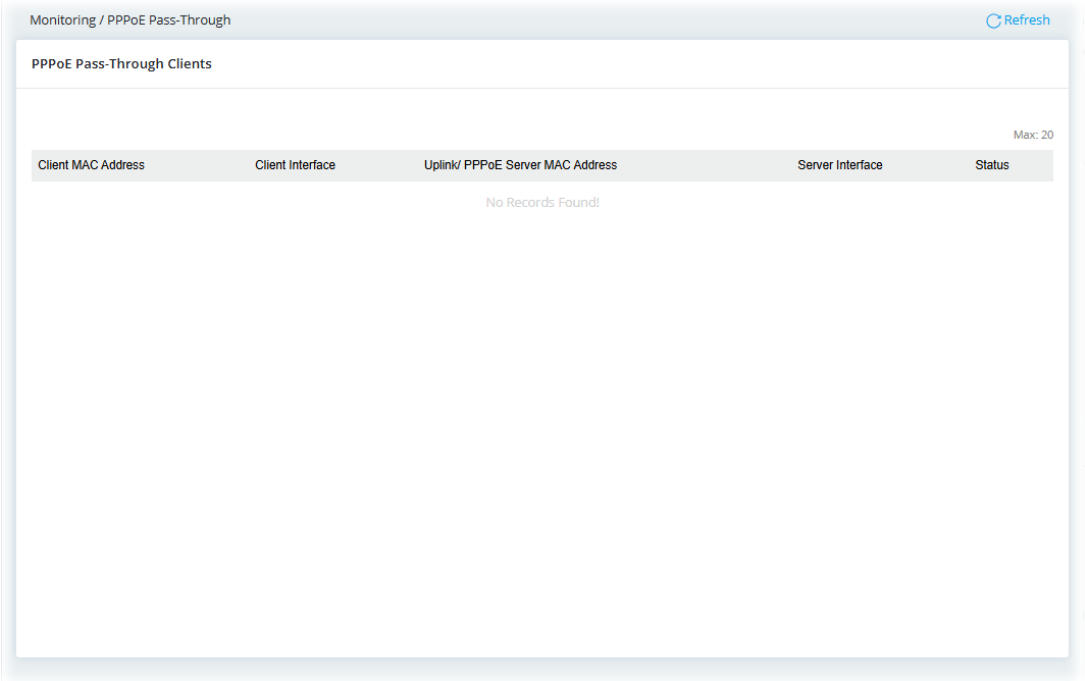


IV-1-14 PPPoE 通透(PPPoE Pass-Through)

路由器提供 PPPoE 撥號連線。此外，您還可以透過 Vigor 路由器，直接建立本機用戶端與 ISP 的 PPPoE 連線。當選擇 PPPoA 協定時，透過 PC 傳送的 PPPoE 封包將轉換為 PPPoA 封包並傳送至 WAN 伺服器。如此一來，PC 即可透過這種方式存取網際網路。

此頁面顯示執行 PPPoE 通透的結果。

按下更新頁面(Refresh)重新載入此頁面以獲取最新資訊。

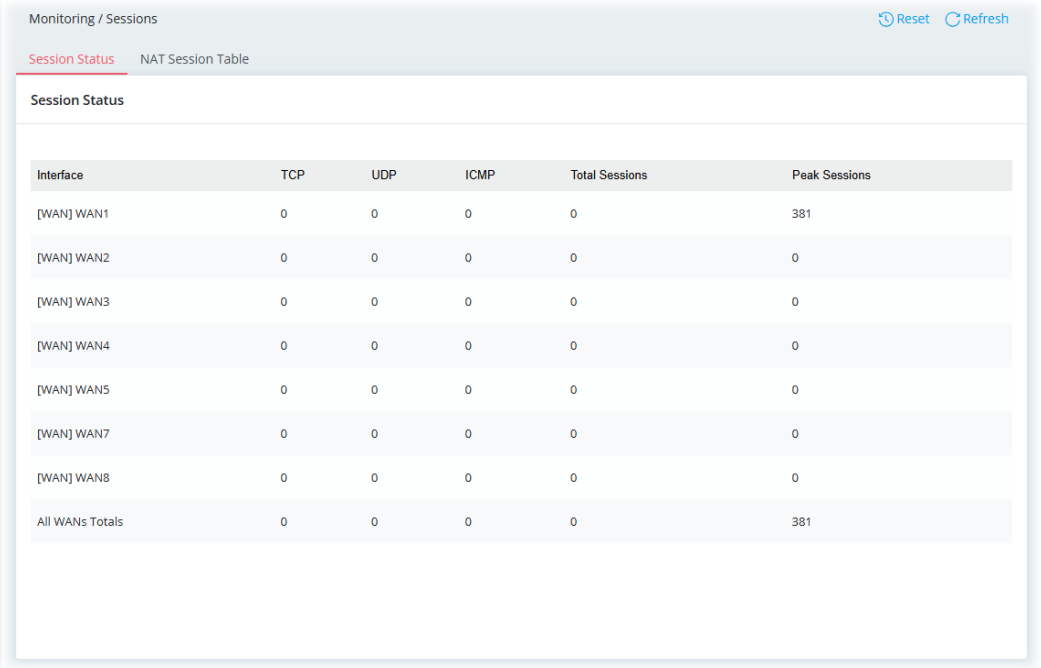


IV-1-15 連線數表(Session Table)

IV-1-15-1 連線數狀態(Session Status)

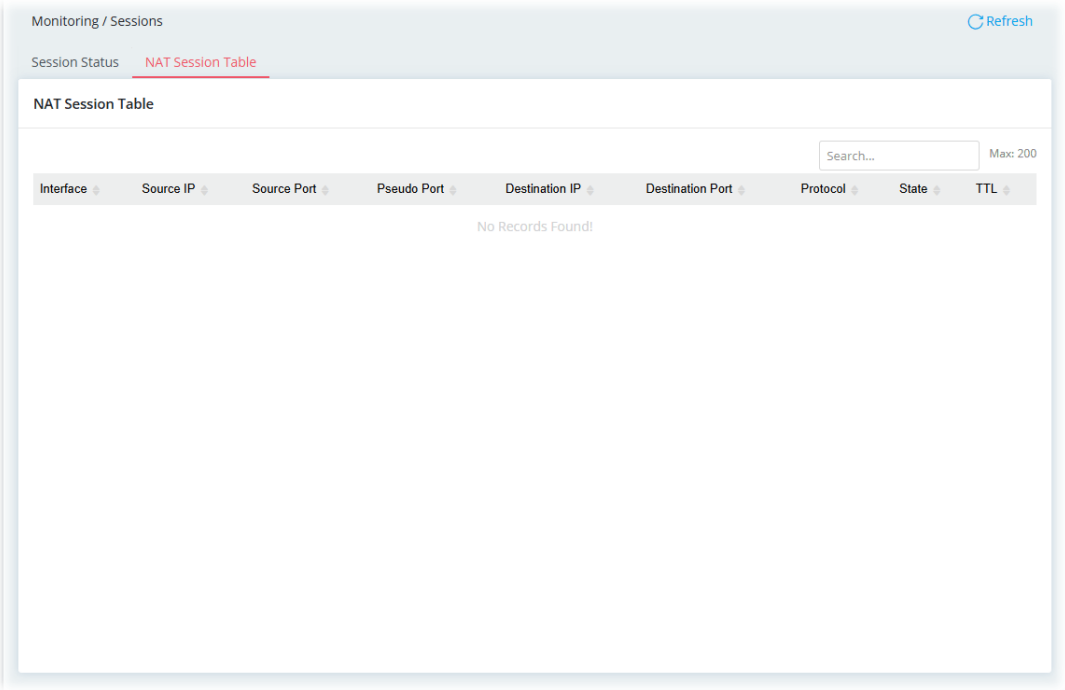
此頁面顯示每個 WAN 介面的連線數 (TCP/UDP/ICMP/總數/峰值)。按下**更新頁面(Refresh)**重新載入此頁面以獲取最新資訊。

最後一欄位的峰值連線數(Peak Sessions)表示路由器啟動以來的最高連線數。



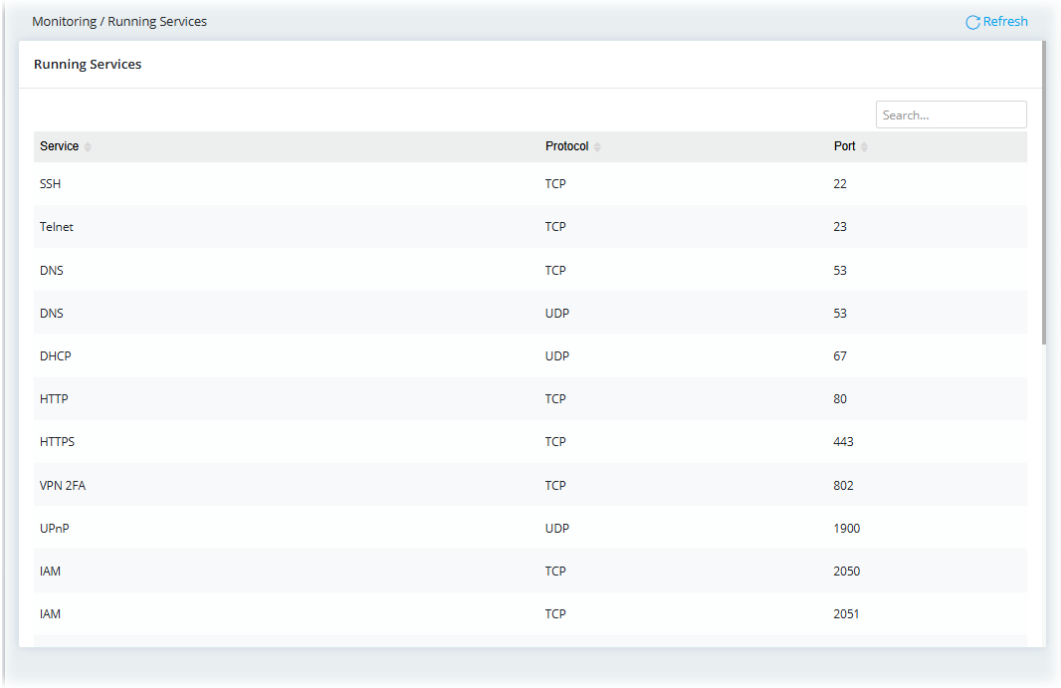
IV-1-15-2 NAT 連線數表(NAT Session Table)

此畫面可顯示 NAT 連線數表中最新的記錄。按下**更新頁面(Refresh)**重新載入此頁面以獲取最新資訊。



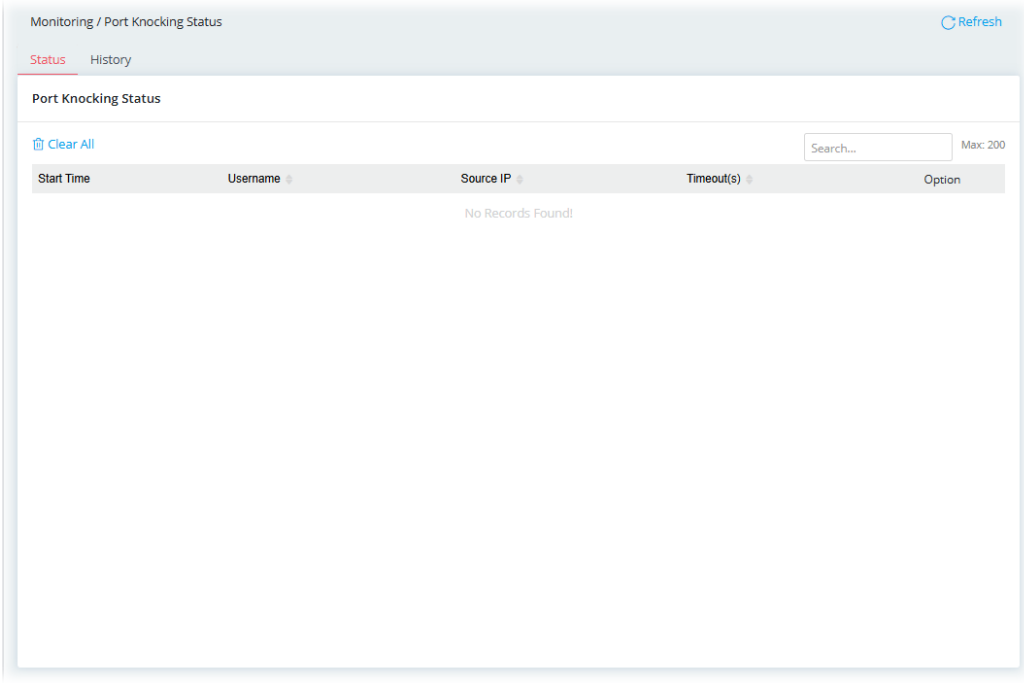
IV-1-16 執行中的服務(Running Services)

此畫面顯示 Vigor 路由器目前正在執行的服務(包含服務名稱、協定與連接埠號碼)。



IV-1-17 Port Knocking 狀態(Port Knocking Status)

此頁面顯示已成功透過連接埠敲擊(Port Knocking)認證的使用者與 IP 位址。



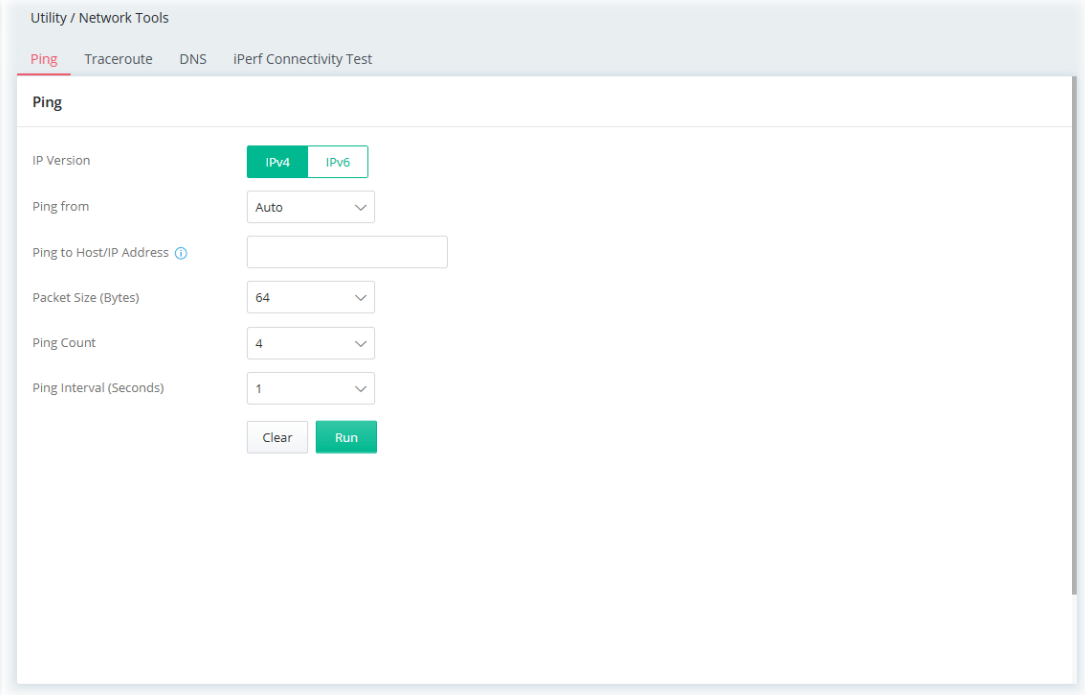
IV-2 工具(Utility)

本節包含一些實用工具(例如 ping 工具、traceroute、DNS 等等)，可協助您分析路由器設定和運作過程中出現的故障和問題。

IV-2-1 網路工具(Network Tools)

IV-2-1-1 Ping 工具(Ping Tool)

使用者可以對指定的 IP(主機)執行 ping 操作，以便診斷資料傳輸是否正常。



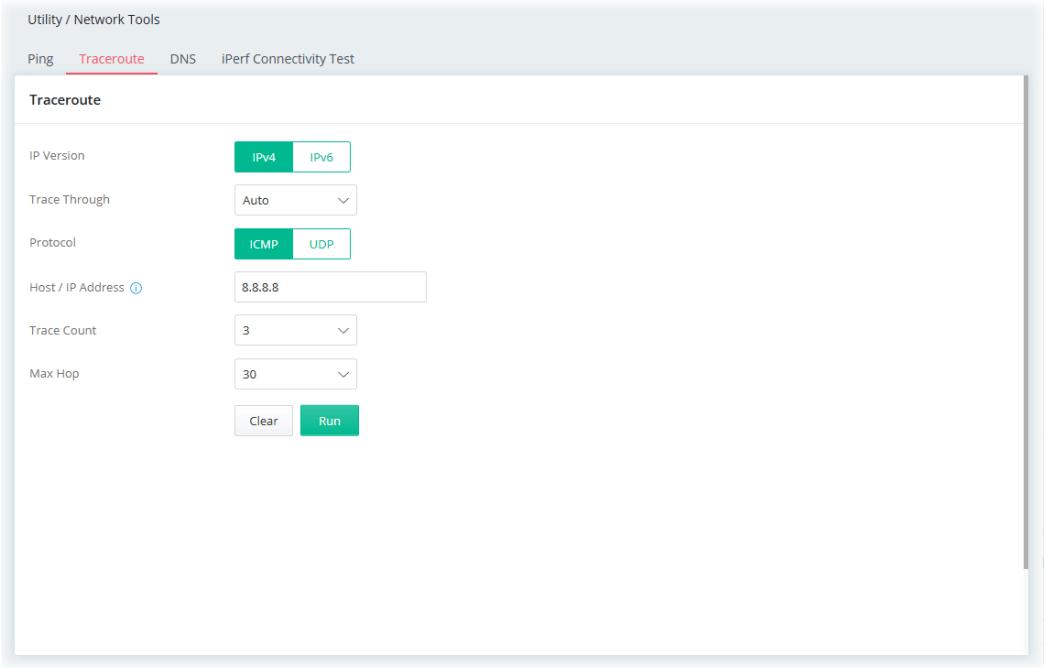
可用設定說明如下：

項目	說明
IP 版本(IP Version)	請選擇 IP 版本以便輸入正確的 IP 位址。
PING 運作來自 (Ping from)	請自下拉式清單中選擇要執行 ping 操作的介面(LAN 或 WAN)，或選擇自動(Auto)讓路由器選擇 WAN 介面。
Ping 至主機/IP 位址 (Ping to Host/IP Address)	輸入準備要 ping 的主機/IP 位址。
封包大小(位元) (Packet Size (byte))	指定 ping 任務的封包大小。
Ping 計數 (Ping Count)	指定被 ping 的封包數量。
Ping 間隔(秒)	設定系統 ping 上述 IP 位址的時間間隔(單位：秒)。

(Ping Interval (sec.))	
清除(Clear)	移除設定並恢復原廠設定。
執行(Run)	執行 ping 任務。

IV-2-1-2 追蹤路由(Traceroute)

使用者可以對指定的 IP 位址(主機)執行路由追蹤任務，以診斷透過 Vigor 系統的資料傳輸是否正常。

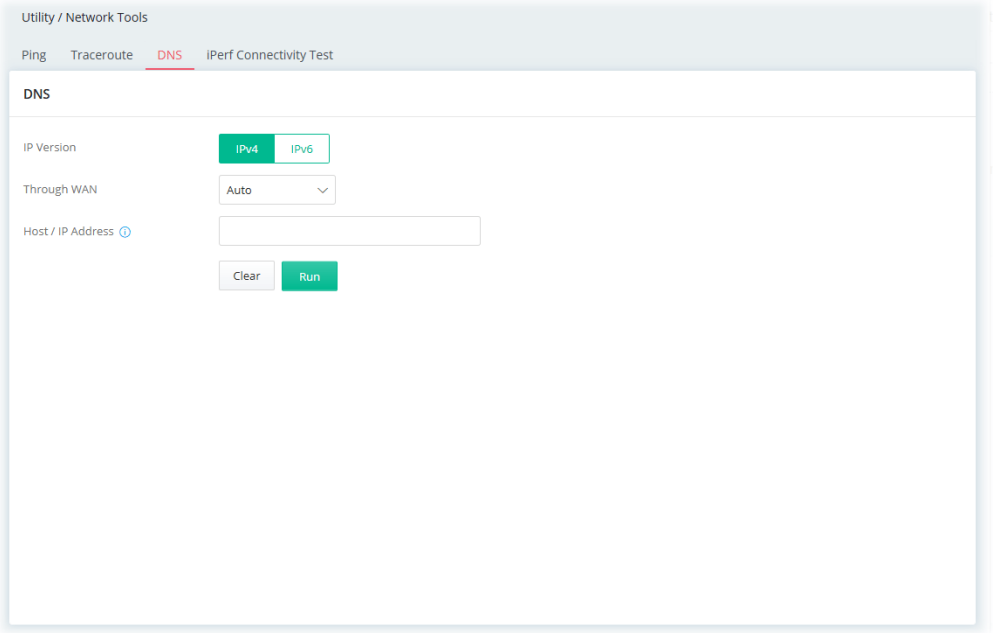


可用設定說明如下：

項目	**說明**
IP 版本(IP Version)	請選擇 IP 版本以便輸入正確的 IP 位址。
追蹤經由(Trace Through)	透過特定介面進行追蹤。目前僅提供**自動(Auto)**選項。
通訊協定(Protocol)	選擇 ICMP 或 UDP 協定。
主機/IP 位址(Host/IP Address)	輸入要追蹤路由的主機/IP 位址。
追蹤計數(Trace Count)	選擇追蹤路由的最大躍點數，選擇無(None)則表示無限制。
最大躍點(Max Hop)	設定搜尋目標的最大躍點數。
清除(Clear)	移除設定並恢復原廠設定。
執行(Run)	執行工作。

IV-2-1-3 DNS

使用者可以透過查詢網域名稱系統(DNS)伺服器來取得網域名稱或 IP 位址訊息，進而診斷路由器的狀態。

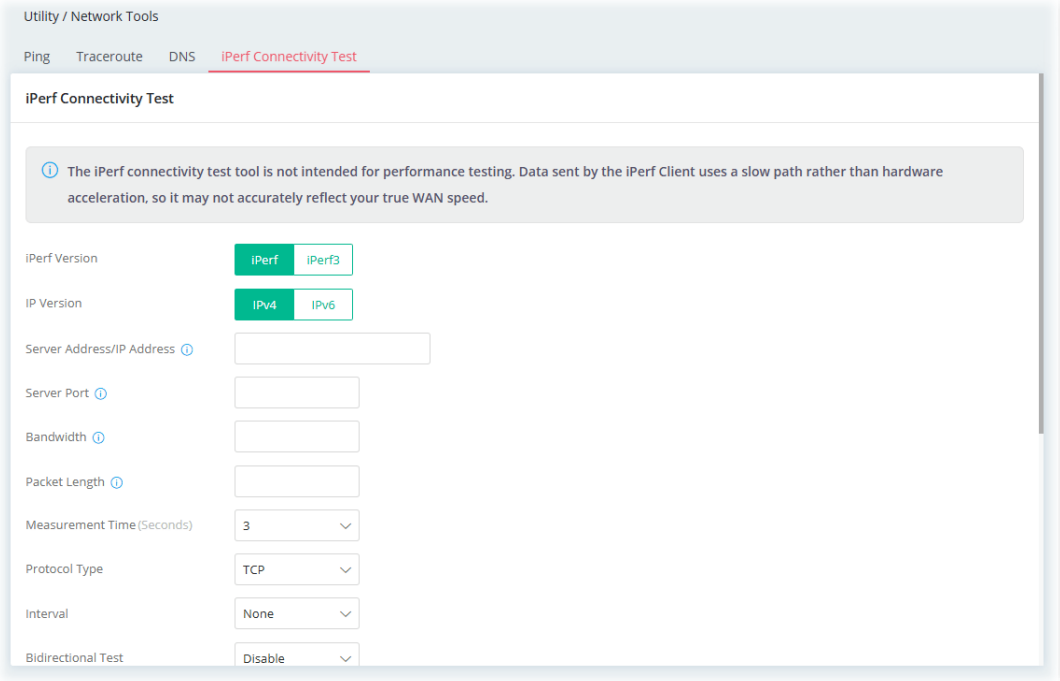


可用設定說明如下：

項目	說明
IP 版本(IP Version)	請選擇 IP 版本以便輸入正確的 IP 位址。
透過 WAN(Through WAN)	選擇 DNS 查詢介面。
主機/IP 位址(Host/IP Address)	輸入網域名稱或 IP 位址進行 DNS 查詢，以取得相應資訊。
清除(Clear)	移除設定並恢復原廠設定。
執行(Run)	執行工作。

IV-2-1-4 iPerf 連接性測試(iPerf Connectivity Test)

iPerf 是一款用於測試 Vigor 路由器與其他裝置(例如筆記型電腦或手機)之間網路連線的工具。



可用設定說明如下：

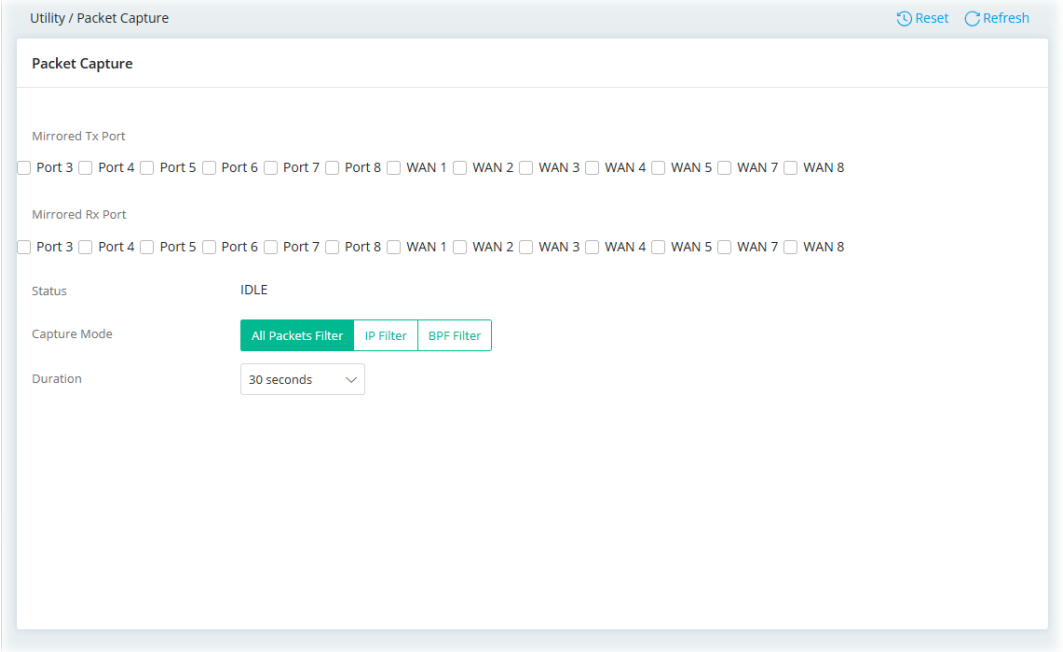
項目	說明
iPerf 版本(iPerf Version)	依據所使用的 iPerf 伺服器選擇 iPerf 版本。
IP 版本(IP Version)	請選擇 IP 版本以便輸入正確的 IP 位址。
伺服器位址/IP 位址 (Server Address/IP Address)	輸入 iPerf 伺服器的 IPv4/IPv6 位址或主機名稱。
伺服器埠號(Server Port)	請輸入 iPerf 伺服器的連接埠號碼。
頻寬(Bandwidth)	設定每次效能測試之頻寬(1-1000MB)。
封包長度(Packet Length)	指定測試之封包長度(8-64000 位元組 s)。
測量時間(Measurement Time)	選擇每次效能測試的持續時間(3、5、10、20 和 50)。 單位為秒數。
通訊協定類型(Protocol Type)	選擇 TCP 或 UDP 作為 iPerf 伺服器的傳輸品質測試協定。 針對雙向測試，請選擇 UDP。
間隔(Interval)	指定測試的時間間隔(1、2、3、5、10 和無)。 單位為秒數。
雙向測試(Bidirectional Test)	每次測試都包含上傳(TX)和下載(RX)封包。注意，測試可能會導致 CPU 之使用率顯著提高。 **停用(Disable)** – 停用測試。 **權衡(Tradeoff)** – 先測試上傳流量，再測試下載流量。 **雙測試(Dualtest)** – 同時測試上傳和下載流量。

清除(Clear)	移除設定並恢復原廠設定。
執行(Run)	執行工作。

IV-2-2 封包擷取(Packet Capture)

封包擷取技術能夠完整記錄通過網路介面的封包，隨後可以使用各種工具（例如 Wireshark 和 tcpdump）檢視和分析這些封包。

該技術主要用於除錯、協定分析、故障排除和網路安全調查。



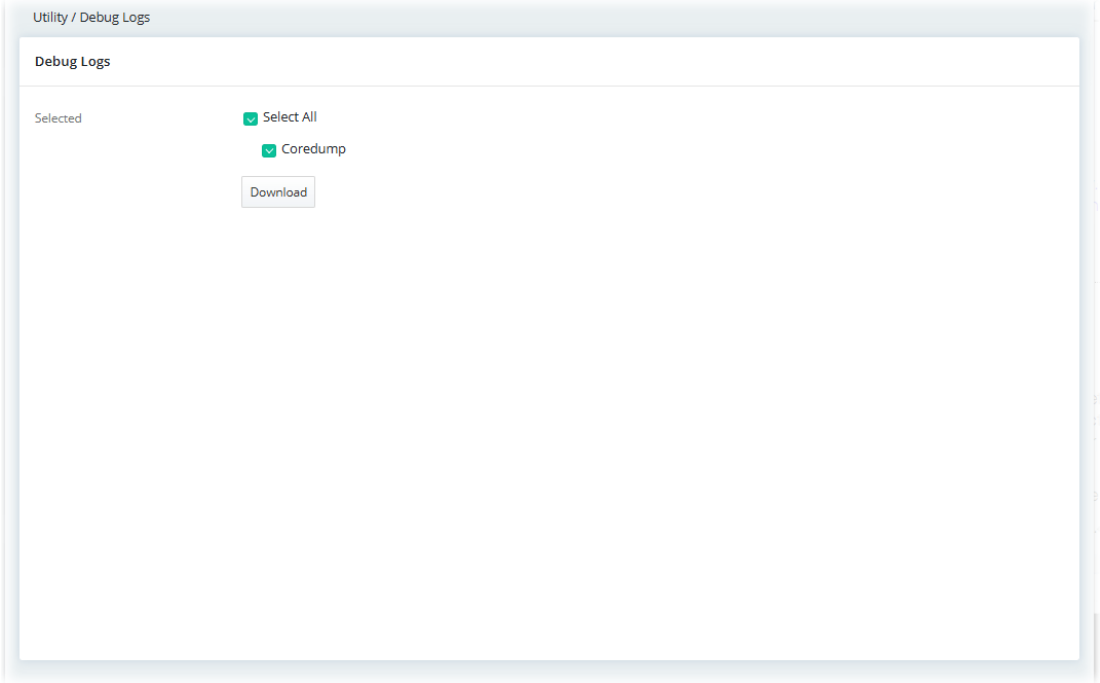
可用設定說明如下：

項目	說明
受監控傳送埠口 (Mirrored Tx Port)	選擇要擷取通過的資料封包的介面。
受監控接收埠口 (Mirrored Rx Port)	選擇作為資料封包之接收介面。
狀態(Status)	顯示資料封包擷取的目前狀態。
擷取模式 (Capture Mode)	選擇一種擷取資料封包的方法。 **全部的封包過濾器(All Packets Filter)** – 擷取所有的資料封包。 ● **持續時間(Duration)** - 到了規定之時間後，系統將自動停止擷取資料封包。 **IP 過濾器(IP Filter)** – 只會擷取經過指定 IP 位址的封包。 ● **通訊協定(Protocol)** – 選擇一通訊協定（任一、ICMP、TCP、UDP 或是 TCP/UDP). ● **IP 位址(IP Address)** – 選擇 “任一” 或選擇自訂 IP(Customize IP) 以輸入指定的 IP 位址。 ● **埠號(Port)** – 選擇 TCP、UDP 或 TCP/UDP 作為協定時，請指定連接埠號碼。您可以選擇任意數字，也可以選擇自訂連接埠 (Customized Port)選項輸入特定連接埠號碼。

	• **持續時間(Duration) -**到了規定之時間後，系統將自動停止擷取資料封包。 **BPF 過濾器(BPF Filter) -** 將會擷取符合 BPF 過濾器（使用標準 tcpdump/libpcap BPF 語法，libpcap 1.9.1）的封包。 • **持續時間(Duration) -** 到了規定之時間後，系統將自動停止擷取資料封包。
開始擷取 (Start Capture)	指定受監控的傳輸連接埠或接收連接埠後，即可使用。 執行資料封包擷取。
停止(Stop)	指定受監控的傳輸連接埠或接收連接埠後，即可使用。 按一下停止資料封包擷取。
下載(Download)	指定受監控的傳輸連接埠或接收連接埠後，即可使用。 將記錄儲存為文件，以便使用指定的工具進行分析。

IV-2-3 除錯日誌(Debug Logs)

此頁面僅供技術人員使用。

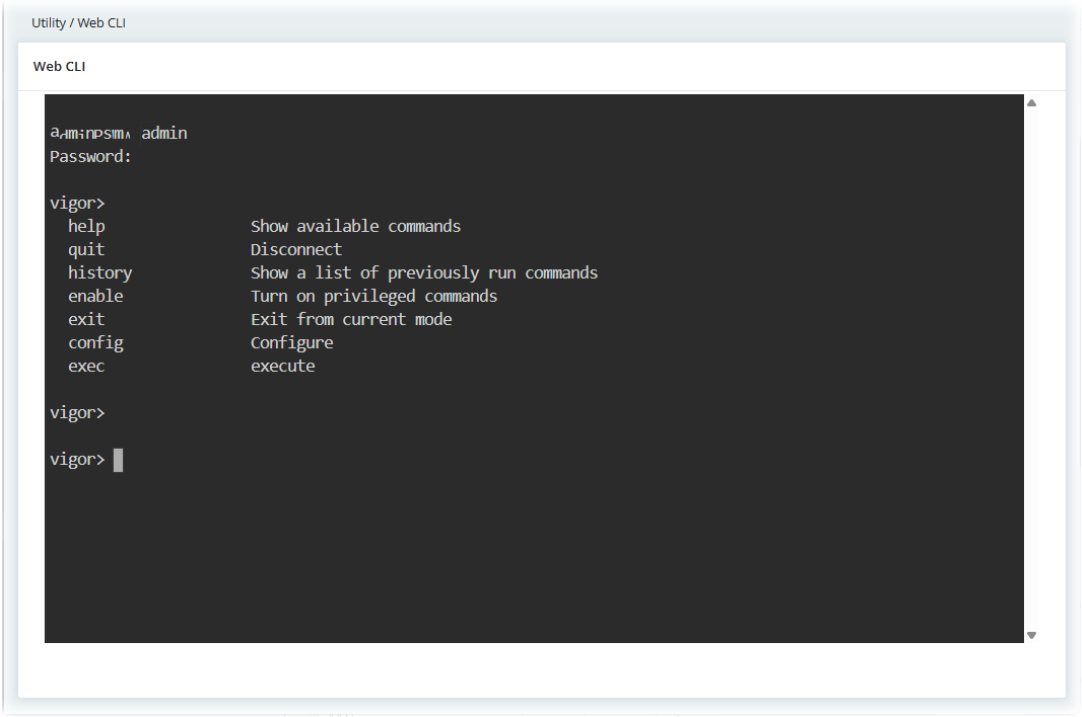


IV-2-4 網頁命令列介面(Web CLI)

本頁可讓使用者無需透過 DOS 命令提示字元即可使用 telnet 指令。透過網頁控制台進行的變更與利用網路使用者介面進行的變更具有相同的效果。在網頁控制台下修改的功能/設定也可以透過網頁使用者介面查看。

按下位於主畫面頂部的圖標**網頁控制台**(Web Console)，開啟如下頁面。

開啟頁面**工具>>網頁命令列介面**(Utility>>Web CLI.)。


Utility / Web CLI
Web CLI
admin
Password:
vigor>
help Show available commands
quit Disconnect
history Show a list of previously run commands
enable Turn on privileged commands
exit Exit from current mode
config Configure
exec execute
vigor>
vigor>

本頁留白

第五章 故障排除

V-1 檢查路由器硬體狀態是否正常

檢查路由器硬體狀態是否正常：

1. 檢查電源線以及纜線連接。詳細資訊請參考“**I-2 硬體安裝**”。
2. 開啟路由器，確認 **WAN**、 **ACT** 與 **LAN** 指示燈是否亮燈。
3. 如果沒有，意味著路由器的硬體有問題。那麼請回到“**I-2 硬體安裝**”，再重新執行一次硬體安裝，然後再試試。

V-2 檢查您電腦的網路連接設置是否正確

有些時候無法上網是因為網路連接設置錯誤所造成的，若在嘗試過上面的方法，依然無法連接成功，請按以下步驟確認網路連接是否正常。

V-2-1 對於 Windows 系統

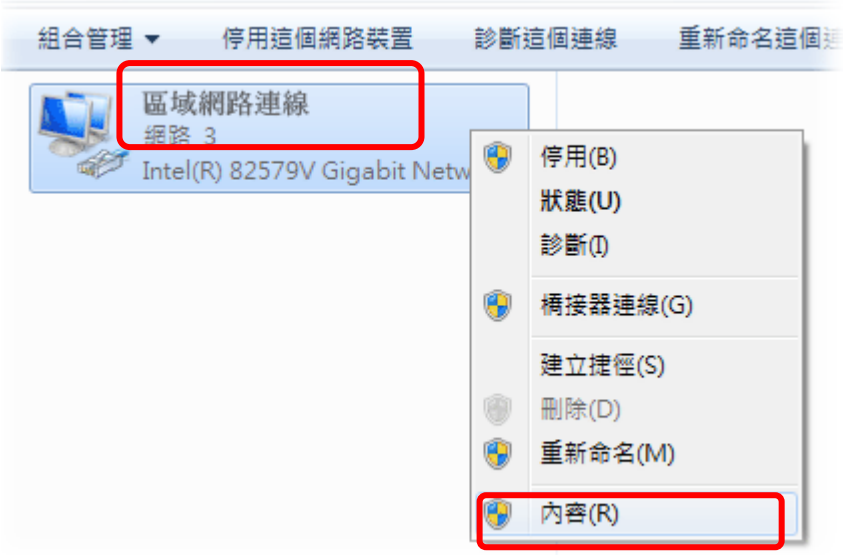
注意:

下列的範例是以 Windows 7 作業系統為基礎而提供。若您的電腦採用其他的作業系統，請參照相似的步驟或至 www.draytek.com.tw 查閱相關的技術文件說明。

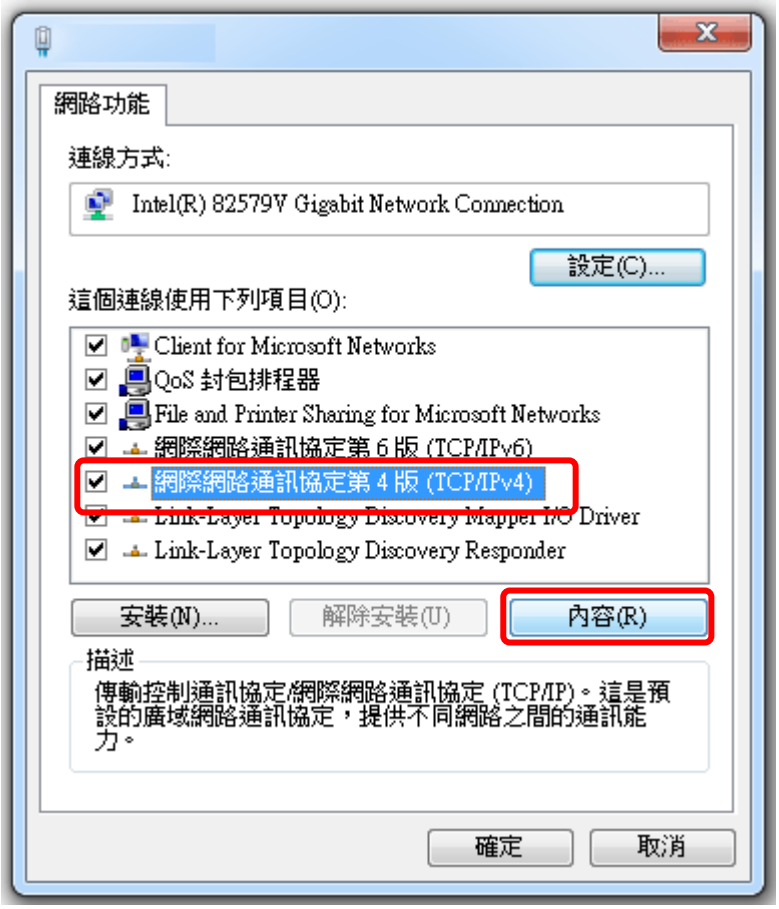
1. 開啟**程式集>>控制台**(All Programs>>Getting Started>>Control Panel)，**按網路和共用中心**(Network and Sharing Center)。

2. 在開啟的畫面上，按下**變更介面卡設定**連結。

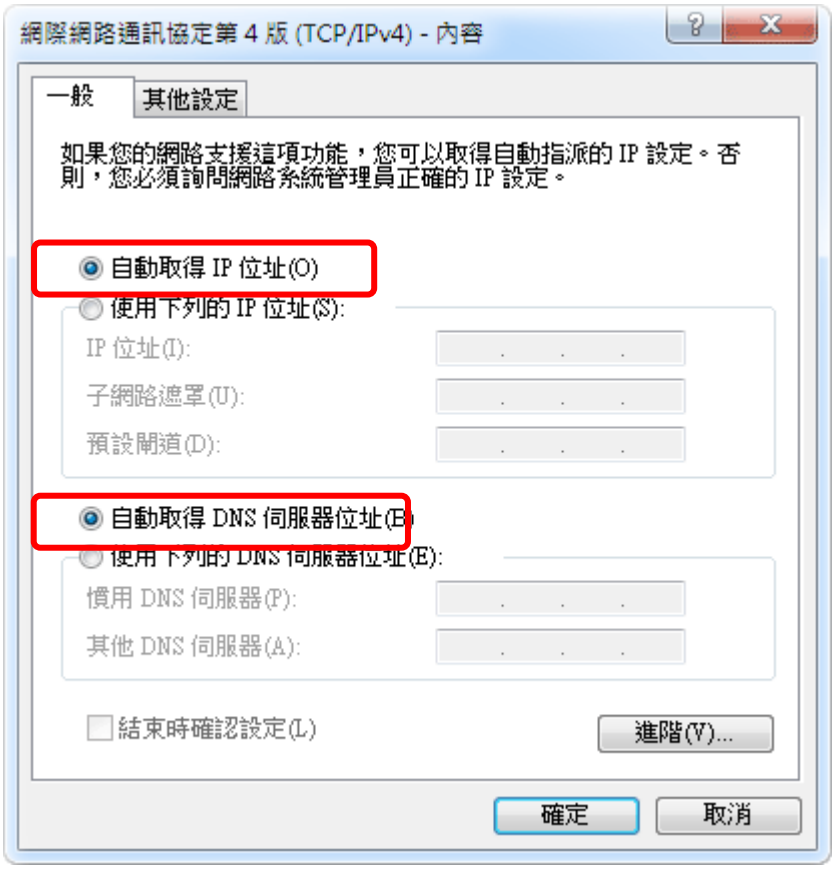
3. 網路連線圖示將會顯示在螢幕上，請在**區域網路連線**圖示上按下右鍵，然後向下移動點選**內容**。



4. 進入區域連線內容畫面後，選擇**網際網路通訊協定第四版(TCP/IPv4)**，再按下**內容**鍵。



5. 進入網際網路通訊協定第四版的內容畫面後，選擇**自動取得 IP 位址**及**自動取得 DNS 伺服器位址**，按下**確定**鍵後完成設定。


網際網路通訊協定第 4 版 (TCP/IPv4) - 內容
一般
其他設定
如果您的網路支援這項功能，您可以取得自動指派的 IP 設定。否則，您必須詢問網路系統管理員正確的 IP 設定。
自動取得 IP 位址(O)
使用下列的 IP 位址(S):
IP 位址(I):
子網路遮罩(U):
預設閘道(D):
自動取得 DNS 伺服器位址(B)
使用下列的 DNS 伺服器位址(E):
慣用 DNS 伺服器(P):
其他 DNS 伺服器(A):
結束時確認設定(L)
進階(V)...
確定
取消

V-2-2 對於 Mac 系統

1. 在桌面上選擇目前所使用的 MacOS 磁碟機按滑鼠二下。
2. 選擇**應用**檔案夾中的**網路**檔案夾。
3. 進入**網路**畫面，在**設定**選項中，選擇**使用 DHCP**。

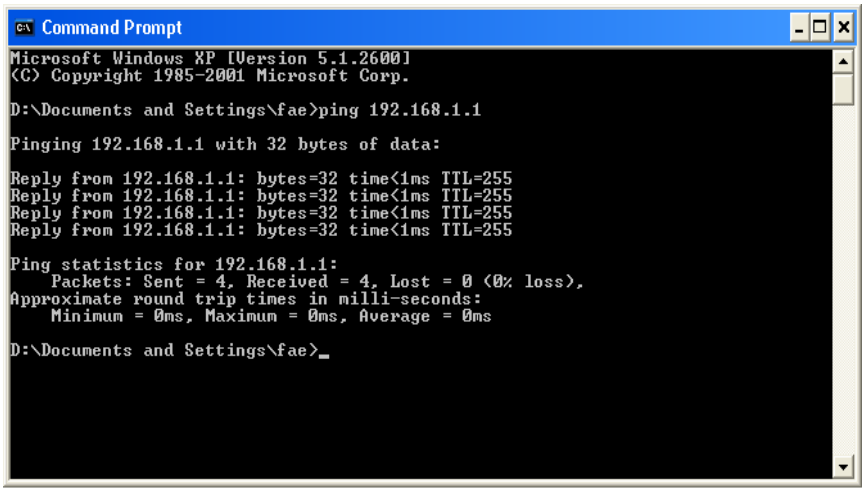
V-3 從電腦上 Ping 路由器

路由器的預設閘道為 192.168.1.1. 因為某些理由，你可能需要使用 " ping " 指令檢查路由器的連結狀態。比較重要的是電腦是否收到來自 192.168.1.1 的回應，如果沒有，請檢查個人電腦上的 IP 位址。我們建議您將網際網路連線設定為自動取得 IP 位址。(請參照 V-2 檢查您個人電腦內的網路連線設定是否正確)，請依照以下的步驟正確地 ping 路由器。

Please follow the steps below to ping the router correctly.

V-3-1 對於 Windows 系統

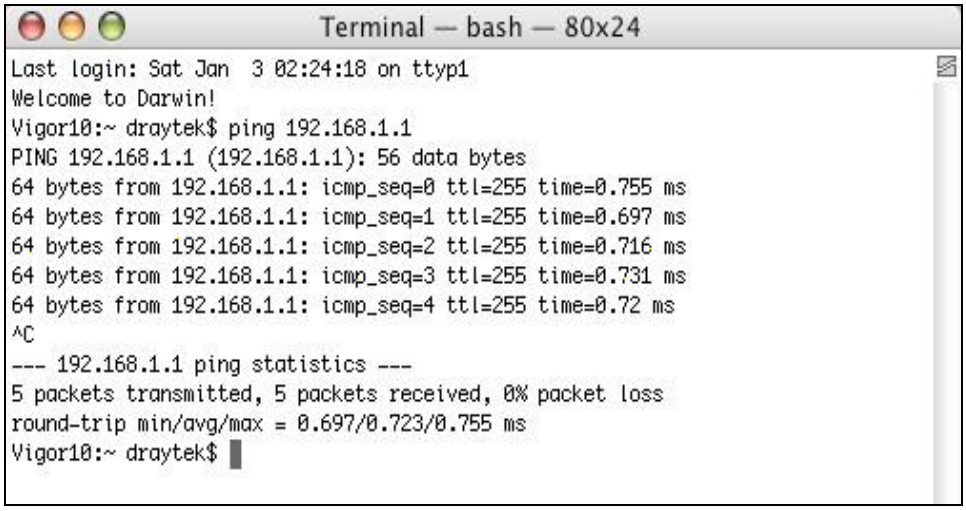
1. 開啟**命令提示字元視窗**(功能表選單**開始>>執行**)。
2. 輸入 **cmd** (適用於 Windows 7 及以上)。DOS 命令提示字元視窗將會出現。



3. 輸入 **ping 192.168.1.1** 並按下 **Enter**，如果連結成功，電腦會收到來自 192.168.1.1 的回應 "**Reply from 192.168.1.1: bytes=32 time<1ms TTL=255**"。
4. 如果連結失敗，請確認個人電腦的 IP 位址設定是否有誤。

V-3-2 對於 MacOs (終端機)系統

1. 在桌面上選擇目前所使用的 Mac OS 磁碟機，並在上面按滑鼠二下。
2. 選擇 **Applications** 檔案夾中的 **Utilities** 檔案夾。
3. 滑鼠按二下 **Terminal**；終端機的視窗將會跳出並顯現在螢幕上。.
4. 輸入 **ping 192.168.1.1** 並且按下 **Enter** 鍵。如果連結正常，終端機視窗會出現"**64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=xxxx ms**" 的訊息。


Terminal — bash — 80x24
Last login: Sat Jan 3 02:24:18 on ttyp1
Welcome to Darwin!
Vigor10:~ draytek$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=0.755 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.697 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.716 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=0.731 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=0.72 ms
^C
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.697/0.723/0.755 ms
Vigor10:~ draytek$

V-4 還原路由器原廠預設值

有時，錯誤的連線設定可以藉由還原廠預設組態來重新設定，您可以利用**重啟路由器**或硬體重新設定的方法還原路由器的設定值。此供能僅在**管理者模式**下可以運作。

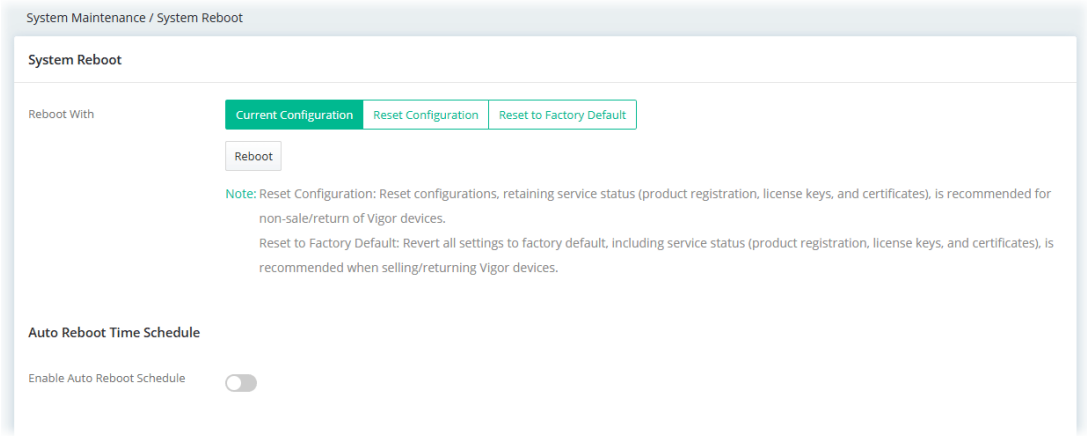
警告:

在使用原廠預設值後，您之前針對分享器所調整的設定都將恢復成預設值。請確實記錄之前路由器所有的設定。

V-4-1 軟體重新設定

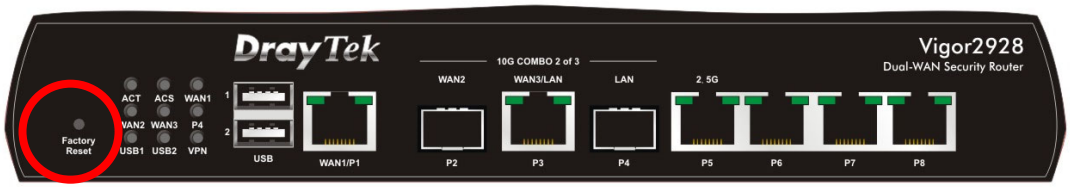
您可以重置路由器，並回復到出廠預設值。

請進入管理者模式，再到網頁介面上的**系統維護>>重啟路由器(System Maintenance>> System Reboot)**，可見下圖。選擇**回復到出廠預設值(Reset to Factory Default)**，並按下**重新啟動(Reboot)**。幾秒鐘後，路由器就會恢復至出廠預設設定。



V-4-2 硬體重新設定

當路由器正在運作時(ACT 燈號閃爍)，如果您壓住 **Factory Reset** 按鈕超過 5 秒以上，且看到 ACT 燈號開始快速閃爍時，請鬆開 **Factory Reset** 按鈕，此時，路由器將會還原成出廠預設值狀態。



恢復至出廠預設值後，您就可以按個人需要，重新設定路由器。

V-5 聯絡居易

假如經過多次嘗試設定後，路由器仍舊無法正常運作，請立即與經銷商聯絡或與居易科技技術服務部聯絡 support@draytek.com.tw。