DrayTek

Vigor2960 系列

雙WAN口安全防火牆路由器

Your reliable networking solutions partner

使 用 手 冊

V2.1

Vigor2960
雙 WAN 口安全防火牆路由器
使用手冊

版本: **2.1**

韌體版本: **V1.2.1**

(請造訪居易網站，隨時獲取更新資訊**)**

日期: **2016** 年 **8** 月 **23** 日

版權資訊

版權聲明

©版權所有，翻印必究。此出版物所包含資訊受版權保護。未經版權所有人書面許可，不得對其進行拷貝、傳播、轉錄、摘錄、儲存到檢索系統或轉譯成其他語言。交貨以及其他詳細資料的範圍若有變化，恕不預先通知。

商標

本手冊內容使用以下商標:

- Microsoft 爲微軟公司註冊商標
- Windows 視窗系列，包括 Windows 95, 98, Me, NT, 2000, XP, Vista, 7, 10 以及其 Internet 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
- 其他產品則爲各自生產廠商之註冊商標

安全說明和保障

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。
- 請勿自行打開或修復路由器。
- 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 5 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。
- 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爲保固期限(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，因爲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。

成爲一個註冊用戶

建議在 Web 介面進行註冊。您可以到 http://www.draytek.com.tw 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。
http://www.draytek.com.tw

名稱：Vigor2960
額定電壓/頻率：100~240V/50_60Hz
總額定消耗電功率：19 瓦
生產國別：台灣
警語：無
功能規格：符合電信管制認證標準，台灣 NCC 規定
使用方法/注意事項：請參照使用手冊說明
製造商：居易股份有限公司
地址：臺灣新竹工業區湖口鄉復興路 26 號

歐盟聲明

廠商:　　居易科技股份有限公司
地址:　　臺灣新竹工業區湖口鄉復興路 26 號
產品:　　Vigor2960 系列
居易科技聲明 Vigor2690 系列服從以下基本要求以及其他 R&TTE 指令（1999/5/EEC）的相關規定。
產品根據 EN55022/Class A 以及 EN55024/Class A 規範，遵從電磁相容性（EMC）指令 2004/108/EEC。
產品根據 EN60950-1 規範，遵從低壓（LVD）2006/95/EC 的要求。

台灣 NCC 規定

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

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

前項合法通信，指一電信規定，作業之無線電通信功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

法規資訊

聯邦通信委員會干擾聲明

此設備經測試，依照 FCC 規定第 15 章，符合 A 級數位器件的限制標準。這些限制是為居住環境不受有害的干擾，而提供合理的保護。若沒有按指導進行安裝和使用，此器件生成、使用以及發射出的無線電能量可能會對無線電通訊有害的干擾。然而，我們並不保證在特殊安裝下，不會產生干擾。如果此產品確實對無線電或電視接受造成了有害的干擾（可以透過開關路由器來判定），我們建議用戶按照以下的幾種方法之一來解決干擾：

- 重新調整或定位接收天線。
- 增加設備和接受器之間的間隔。
- 將設備接到一個與接受者不同的回路的出口。
- 請代理商或是有經驗的無線電/電視技師協助處理。

此產品符合 FCC 規定的第 15 部分。其運作將有以下兩個情況：

(1) 此產品不會造成有害的干擾，並且

(2) 此產品可能會遭受其他接收到的干擾，包括那些可能造成不良運作的干擾。

更多資訊，請造訪 http://www.draytek.com.

目錄

第一章: 簡介 1

1.1 網頁設定按鈕說明 1

1.2 LED 指示燈與介面說明 2

1.3 硬體安裝 4

1.3.1 網路連線 4
1.3.2 壁掛安裝 5

第二章: 初始設定 7

2.1 變更密碼 7

2.2 快速設定精靈 9

2.2.1 步驟 1 – 指定 WAN 設定檔 9
2.2.2 步驟 2 – 設定協定 9

2.3 註冊 Vigor 路由器 16

第三章: 應用解說 19

3.1 如何透過登入路由器的 HTTPS 伺服器建立具備 RDP 服務的 SSL VPN 通道? 19

3.2 如何設定 OSPF? 24

3.3 如何在 Vigor2960 與其他路由器之間建立 LAN to LAN IPSec 通道 (Main Mode) 30

3.4 CVM 應用 – 如何透過 Vigor2960 管理 CPE (路由器)? 33

3.5 CVM 應用 – 如何在 Vigor2960 與遠端設備之間建立 VPN? 38

3.6 CVM 應用 – 如何透過 Vigor2960 更新遠端 CPE 韌體? 41

3.7 如何運用 Vigor2960 的高可靠度(High Availability)功能? 45

3.8 如何設定 Vigor2960 中 DNS Inbound 負載平衡? 50

第四章: 進階設定 55

4.1 WAN 設定 55

4.1.1 基本設定 56
4.1.2 Inbound 負載平衡 76
4.1.3 交換器 81

4.2 區域網路(LAN) 85

4.2.1 基本設定 86
4.2.2 PPPoE 伺服器 98
4.2.3 交換器 102
4.2.4 綁定 IP 到 MAC 107
4.2.5 LAN DNS 111

4.3 路由設定 114

4.3.1 負載平衡配置量 114

4.3.2 固定路由.....118
4.3.3 策略路由.....124
4.3.4 預設路由.....140
4.3.5 RIP 設定.....141
4.3.6 OSPF 設定.....143
4.3.7 BGP 設定.....145

4.4 NAT..... 149

4.4.1 通訊埠重導向.....149
4.4.2 DMZ 主機.....152
4.4.3 ALG.....155
4.4.4 連線逾時.....156

4.5 防火牆..... 157

4.5.1 過濾器設定.....157
4.5.2 DoS 防禦.....180
4.5.3 封鎖 MAC.....184
4.5.4 過濾器封包計數.....187

4.6 物件設定..... 188

4.6.1 IP 物件.....188
4.6.2 IP 群組.....190
4.6.3 IPv6 物件.....192
4.6.4 MAC/製造商物件.....194
4.6.5 國家物件.....195
4.6.6 服務類型物件.....197
4.6.7 服務類型群組.....199
4.6.8 關鍵字/DNS 物件.....200
4.6.9 副檔名物件.....204
4.6.10 APP 物件.....206
4.6.11 網頁分類物件.....210
4.6.12 QQ 物件.....213
4.6.13 QQ 群組.....215
4.6.14 時間物件.....217
4.6.15 時間群組.....219
4.6.16 簡訊 SMS 服務物件.....220
4.6.17 郵件服務物件.....222
4.6.18 通知物件.....224

4.7 使用者管理..... 228

4.7.1 入口網站.....228
4.7.2 使用者設定檔.....234
4.7.3 使用者群組.....245
4.7.4 訪客設定檔.....247
4.7.5 RADIUS 伺服器.....252
4.7.6 單一帳號/活動目錄管理(LDAP/Active Directory).....253

4.8 其他應用..... 257

4.8.1 動態 DNS.....257
4.8.2 GVRP.....263
4.8.3 IGMP 代理.....264
4.8.4 UPnP.....265
4.8.5 高可靠度.....266
4.8.6 網路喚醒.....274

4.8.7 簡訊/郵件警示服務 277

4.9 VPN 以及遠端存取 281

4.9.1 VPN 用戶端設定精靈 281
4.9.2 VPN 伺服器設定精靈 288
4.9.3 遠端存取控制 292
4.9.4 PPP 基本設定 294
4.9.5 IPsec 基本設定 299
4.9.6 VPN 設定 300
4.9.7 VPN Trunk 管理 311
4.9.8 連線管理....316

4.10 憑證管理 318

4.10.1 本機憑證 319
4.10.2 具公信力之 CA 憑證....324
4.10.3 遠端憑證 325

4.11 SSL 代理.... 326

4.11.1 SSL 網頁代理....326
4.11.2 SSL 應用....328
4.11.3 線上使用者狀態....332

4.12 VPN 中央管理.... 333

4.12.1 基本設定 334
4.12.2 CPE 管理 336
4.12.3 日誌/警告....344

4.13 頻寬管理 345

4.13.1 服務品質 345
4.13.2 QoS 規則 349
4.13.3 連線數限制....355
4.13.4 頻寬限制 357

4.14 USB 應用.... 361

4.14.1 磁碟狀態 361
4.14.2 FTP 伺服器 362
4.14.3 SAMBA 伺服器 363
4.14.4 印表機....366
4.14.3 溫度計....366
4.14.4 數據機支援列表....369

4.15 系統維護 370

4.15.1 TR-069....370
4.15.2 管理員密碼....372
4.15.3 設定備份 373
4.15.4 系統日誌/郵件警告....376
4.15.5 時間與日期....379
4.15.6 連線控制 380
4.15.7 SNMP 設定 384
4.15.8 重啓路由器....385
4.15.9 韌體更新 387
4.15.10 APP 特徵碼更新....391
4.15.11 APP 支援列表 393

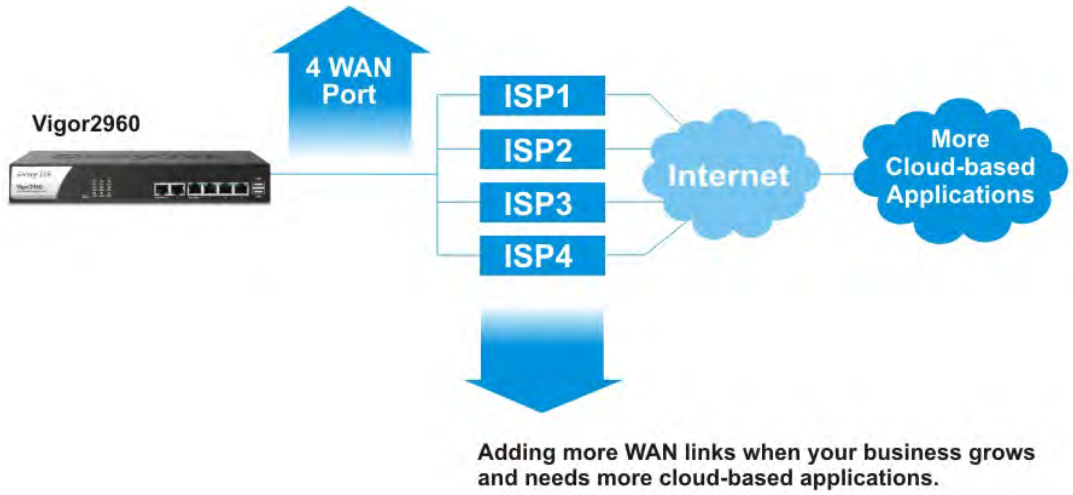
4.16 自我診斷 394
4.16.1 路由列表 394
4.16.2 ARP 緩存列表 397
4.16.3 DHCP 列表 399
4.16.4 NAT 連線數列表 401
4.16.5 MAC 位址列表 402
4.16.6 流量統計 402
4.16.7 流量圖 404
4.16.8 Web 終端機 405
4.16.9 Ping/路由追蹤 406
4.16.10 資料流量監控 407
4.16.11 使用者狀態 409
4.17 外部裝置 410
4.18 產品註冊 411

第五章: 疑難排解 413
5.1 檢查路由器硬體狀態是否正常 413
5.2 檢查您電腦的網路連接設置是否正確 414
5.3 從電腦上 Ping 路由器 417
5.4 檢查 ISP 的設置是否正常 418
5.5 還原路由器原廠預設組態 419
5.6 聯絡居易 420

第一章: 簡介

居易科技 Vigor2960 系列 - 雙 WAN 口安全防火牆路由器是特別爲中型企業設計的最新產品，網路連線速度可達 1G，並整合完善的防火牆，同時提供小型企業使用者安全且可靠的遠端存取方式-VPN 連線通道，使用者可從任何地方容易且安全的存取電子郵件、檔案、內部網路、更新軟體，大大降低了維護及支援費用。Vigor2960 擁有快速且強大的系統，可身兼數職同時處理多種程式，公司連線不間斷並延續企業的生命力，公司的資產也更有保障。

虛擬私有網路(簡稱 VPN)乃是虛擬網路的延伸，經由共享或是公用網路如網際網路來連結。VPN 讓您透過共享公用網路，以模擬點對點專屬連結的方式，在二台電腦之間傳送資料，居易 Vigor3900 支援網際網路標準技術以提供客戶開放且可交互運作的 VPN 解決方案，像是 X.509, DHCP over Internet Protocol Security (IPSec)與點對點通道協定(PPTP)。



1.1 網頁設定按鈕說明

在路由器的網頁設定中，有數種常見的按鈕，其定義如下所示：

Apply	儲存並套用目前的設定。
Cancel	取消目前設定並回復先前的設定值。
Next	進入下一頁。
Previous	回到上一頁。
Finish	完成設定。
	移除您不滿意的設定。
	移除選定的輸入內容。

附註:有關網頁上所出現的其他按鈕，請參考第四章。

1.2 LED 指示燈與介面說明

在您使用路由器之前，請先熟悉 LED 指示燈與各個連接口。

LED 燈號說明

LED		狀態	說明
ACT		閃爍	路由器已開機並可正常運作。
		暗	路由器已關機。
CSM		亮	關於 IM/P2P、URL/網頁內容過濾器的 CSM (數位內容安全設定)之設定檔，啓動機制在**防火牆>>基本設定**中，(此類設定檔的建立必須在**數位內容安全設定**功能表單下。)
VPN		亮	VPN 通道已建立。
		暗	VPN 通道未建立。
DoS		亮	DoS/DDoS 功能已啓動。
		閃爍	檢測到正受到外部攻擊。
WAN1/2		亮	WAN1 或 WAN2 介面已連接。
		閃爍	資料封包傳輸中。
QoS		亮	QoS 功能已開啓。
		暗	QoS 功能已關閉。
USB1/2		亮	USB 裝置已安裝且預備妥當。
		閃爍	正在傳輸資料中。
LED on Connector			
GigaWAN 1/2	Left LED (Green)	亮	乙太網路已連接。
		暗	乙太網路未連接。
		閃爍	正在傳輸資料中。
	Right LED (Green)	亮	介面的連接速度爲 1000Mbps。
		暗	介面的連接速度爲 10/100Mbps。
GigaLAN 1/2/3/4	Left LED (Green)	亮	乙太網路已連接。
		暗	乙太網路未連接。
		閃爍	正在傳輸資料中。
	Right LED (Green)	亮	介面的連接速度爲 1000Mbps。
		暗	介面的連接速度爲 10/100Mbps。

連接介面

介面	說明
Factory Reset	還原成出廠預設值。 用法：當路由器正在運作時（ACT LED 燈號閃爍），利用尖銳的物品（例如：原子筆）壓住 Factory Reset 超過 5 秒；當 ACT LED 燈號開始迅速閃爍時，鬆開此動作，路由器將會還原成出廠預設值。
GigaWAN 1/2	遠端網路裝置連接介面。
GigaLAN 1/2/3/4	本機網路之裝置連接介面。
USB1/2	連接到行動硬碟、3G 數據機或是印表機。
	連接電源變壓器。 ON/OFF -電源開關，“1” 爲開，“0” 爲關。

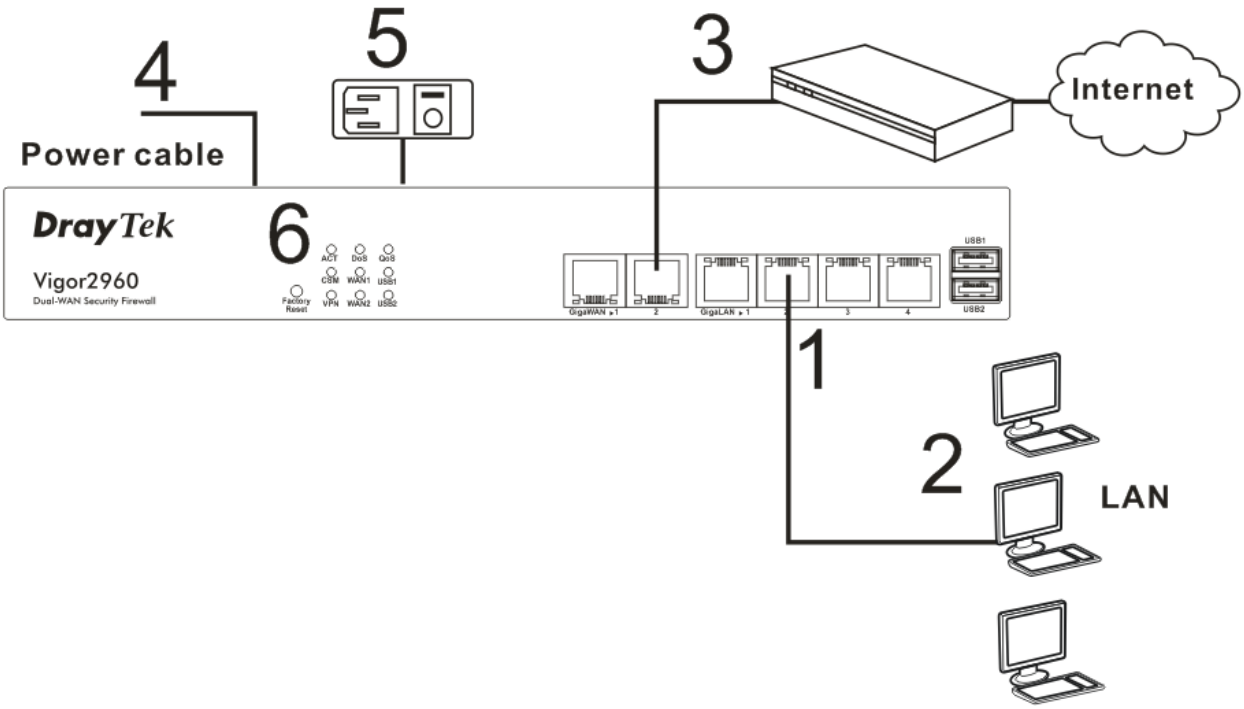
1.3 硬體安裝

1.3.1 網路連線

設定路由器前，請參考以下步驟，先將裝置確實連接。

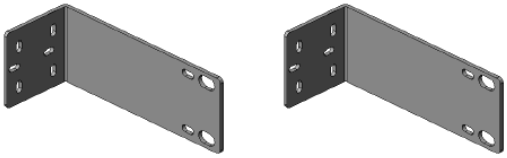
1. 將乙太網路纜線(RJ-45)之一端連接到本裝置任一 LAN 連接埠。
2. 乙太網路纜線(RJ-45)的另一端連接至電腦(可連接至其他電腦形成小型的區域網路)的乙太網路連接埠，面板的 **LAN** LED 燈號將會亮起。。
3. 利用乙太網路纜線(RJ-45) 連接纜線數據機/DSL 數據機/媒體格式轉換器至本裝置任一 WAN 連接埠。面板的 **WAN** LED 燈號將會亮起。
4. 將電源線一端連接到本裝置，另一端連接到牆上電源輸出孔。
5. 按下本裝置背面的電源開關，前面的 **ACT** LED 燈號將會亮起。
6. 系統開始初始化，完成之後，**ACT** LED 燈號將會亮燈並持續閃爍。

下圖顯示硬體安裝示意圖供您參考：

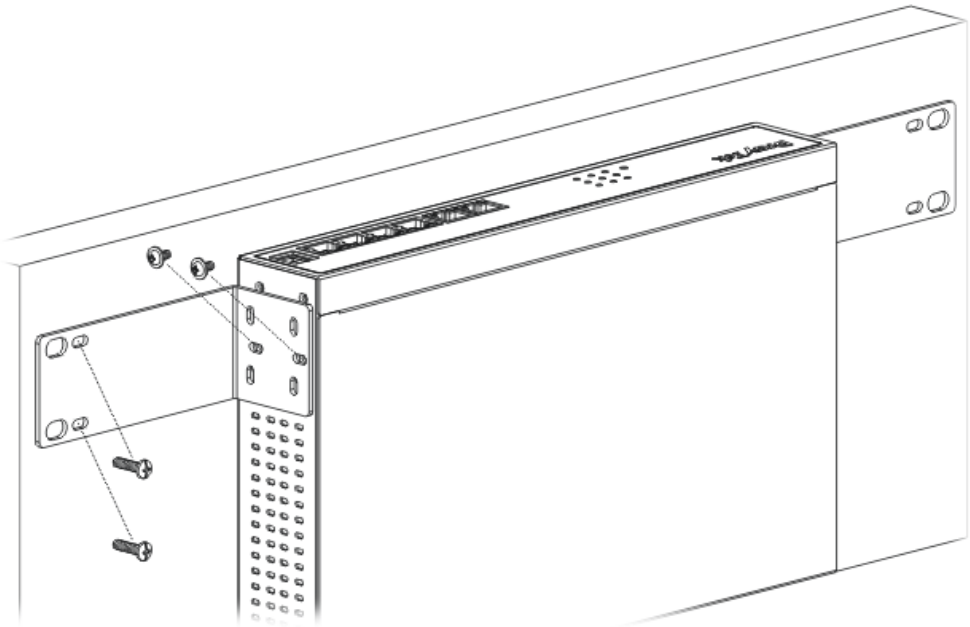


1.3.2 壁掛安裝

利用下圖所示的標準固定架(需要 2 個)，可以將路由器安裝在牆壁上。



選擇一個適合安置路由器的平滑的表面(牆壁上)，將固定架上短邊的螺絲孔洞對準路由器上預留的螺絲孔洞，然後使用螺絲鎖緊固定架(路由器左右雙邊都要鎖上)，接著使用另外的螺絲鎖緊牆壁與支架。請參考下圖：



完成上述動作後，路由器即可穩穩的固定在牆壁上。

本頁留白

第二章: 初始設定

在開始使用路由器時，基於安全的考量，我們強烈建議你在路由器上設定一組管理者密碼。

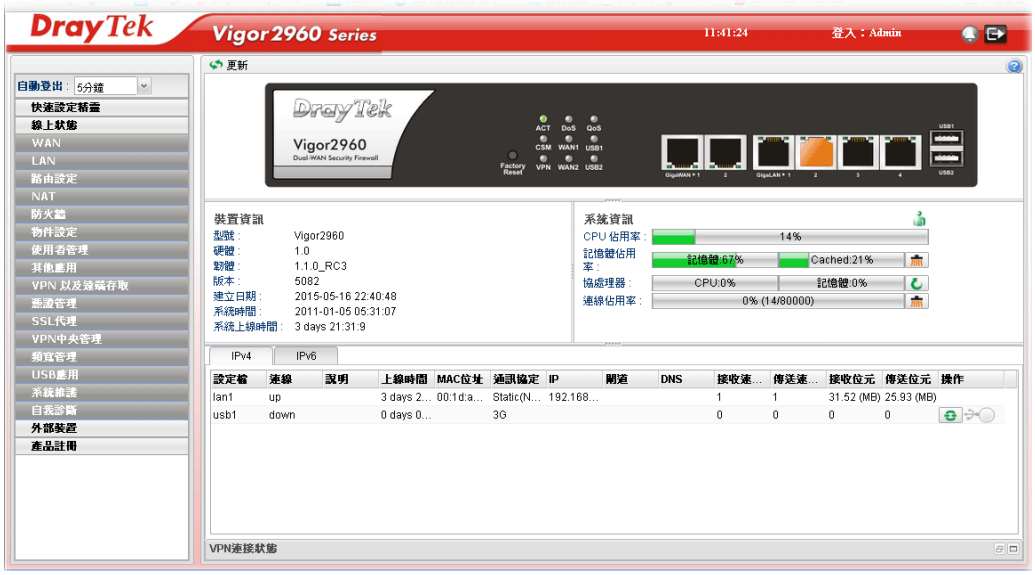
2.1 變更密碼

1. 確認您的 PC 已正確的連接到路由。

> **注意**：您可以讓您的電腦自動從路由器獲取 IP 位址，也可以手動為電腦設定路由器預設之 IP 位址 **192.168.1.1** 的相同子網路地址。詳細的資訊請參考最後章節—疑難排解。

2. 打開網頁瀏覽器，然後輸入 **http://192.168.1.1**。視窗將會彈出並要求您輸入使用者名稱、密碼以及選擇語系(請選繁體中文)。選擇完畢後，按下**登入**。

3. 設定介面的主選單出現如下。



4. 進入**系統維護**頁面並選擇**管理員密碼**。

5. 在**原始密碼**欄位中輸入登入的舊密碼，在**新的密碼**欄位中輸入您準備使用的新密碼，接著在**確認密碼**欄位中在次輸入此新密碼。輸入完畢後請下**套用**儲存。

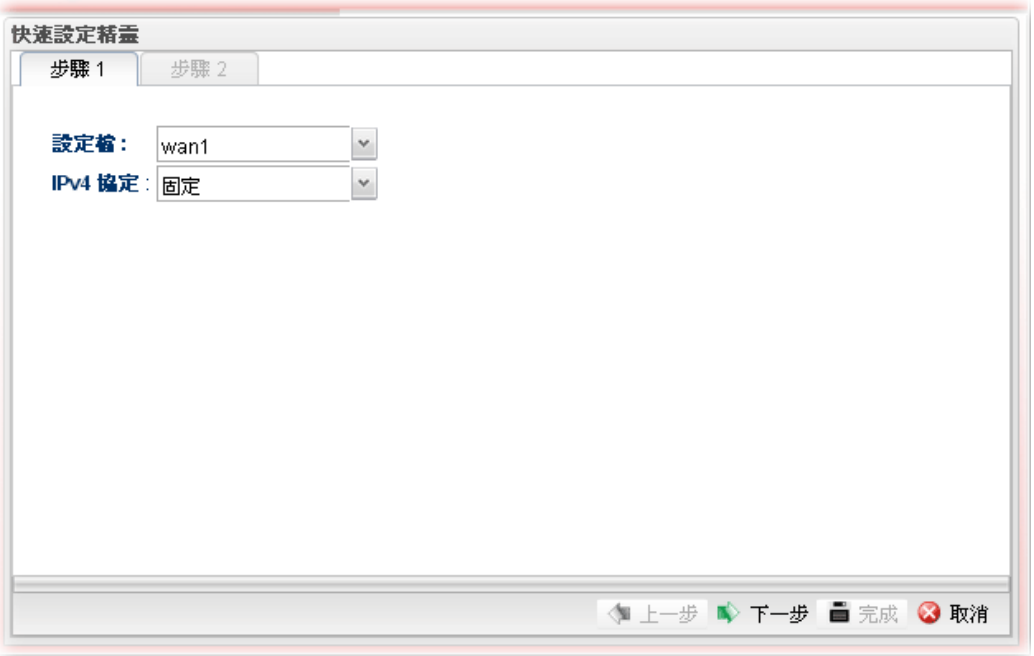
6. 現在新密碼已經變更，下一次，請使用新密碼登入此路由器的網頁設定介面。

2.2 快速設定精靈

快速設定精靈是爲了方便您設置路由器的網際網路連線而設計的。

2.2.1 步驟 1 – 指定 WAN 設定檔

在快速設定精靈首頁上，請先建立一個 WAN 設定檔。



可用參數詳列如下：

項目	說明
設定檔	使用下拉式清單選擇一個 WAN 設定檔。 wan1 wan1 wan2 usb1 usb2
IPv4 協定	使用下拉式清單挑選一個連線模式。 固定 固定 DHCP PPPoE PPTP

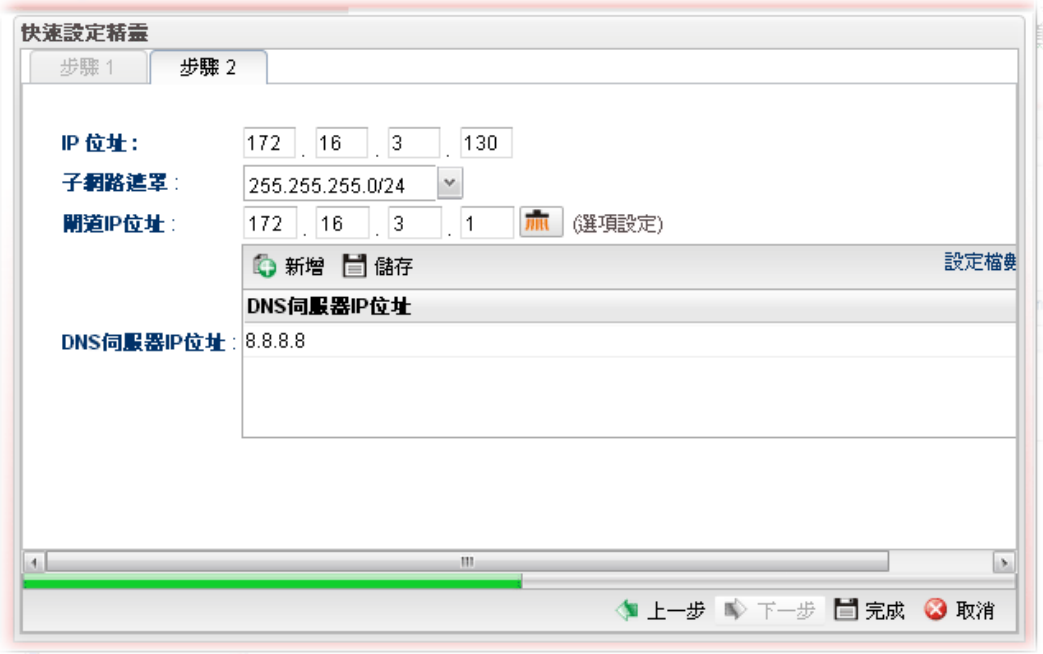
完成上述設定後，按**下一步**繼續進行。

2.2.2 步驟 2 – 設定協定

這個頁面將依照選擇的 **IPv4 協定類型**顯示相關設定頁面。

如果選擇 Static 協定類型

如果選擇了**固定(Static)**模式，您需要手動指定一個固定位址給予 WAN 介面，套用此設定及重新啟動路由器。請輸入您的 ISP 提供給您的 IP 位址、子網遮罩、閘道位址與 DNS 伺服器 IP 位址，再按下**完成**。路由器將重新啟動。



可用參數詳列如下：

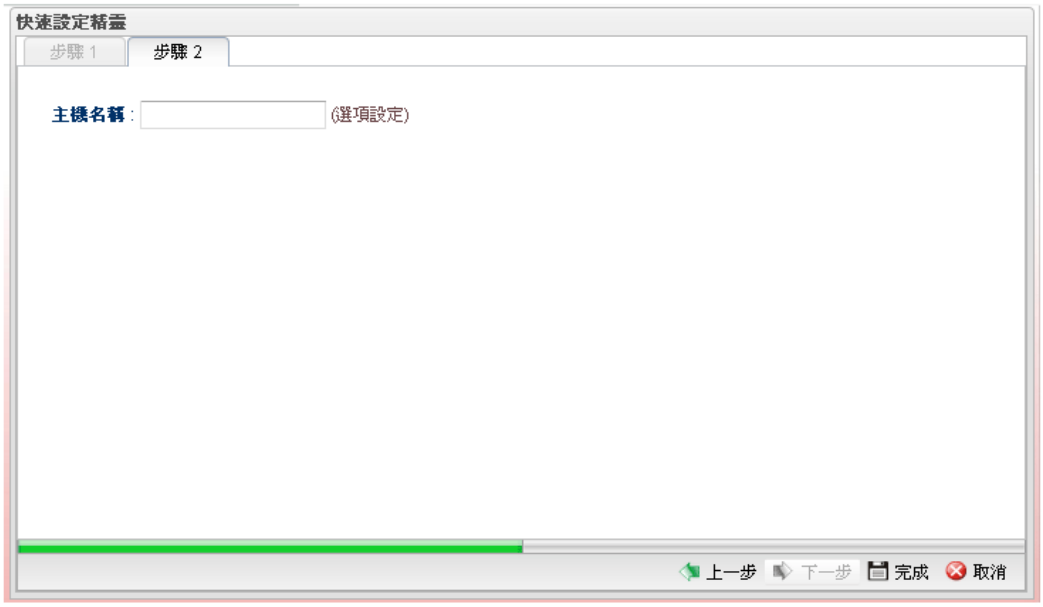
項目	說明
IP 位址	輸入此 WAN 設定檔所需的真實 IP 位址。
子網路遮罩	自下拉式清單選擇網路遮罩。
閘道 IP 位址	輸入真實閘道位址。
DNS 伺服器 IP 位址	輸入 DNS (Domain Name Server) 伺服器所需的真實 IP 位址。按下**新增**可以增加新的 IP 位址，畫面上將會出現四個小方塊，您可在上面輸入 IP 位址，當您完成設定後，按下**儲存**。 **新增** – 按此以新增 IP 位址。 **儲存** – 按此儲存設定。
上一步	按此回到前一個設定頁面。
完成	按此儲存本頁設定並離開此頁面。

取消	按此捨棄本頁設定。

完成上述設定後，按**完成**結束連線上網設定。

如果選擇 DHCP 協定類型

這個類型可以讓使用者自動從 DHCP 伺服器取得一組 IP 位址，如果選擇了此模式，您的 ISP 業者的 DHCP 伺服器將會自動分派一組 IP 位址給予路由器。(某些 ISP 業者可能還會提供主機名稱與網域名稱，視情況而定)。



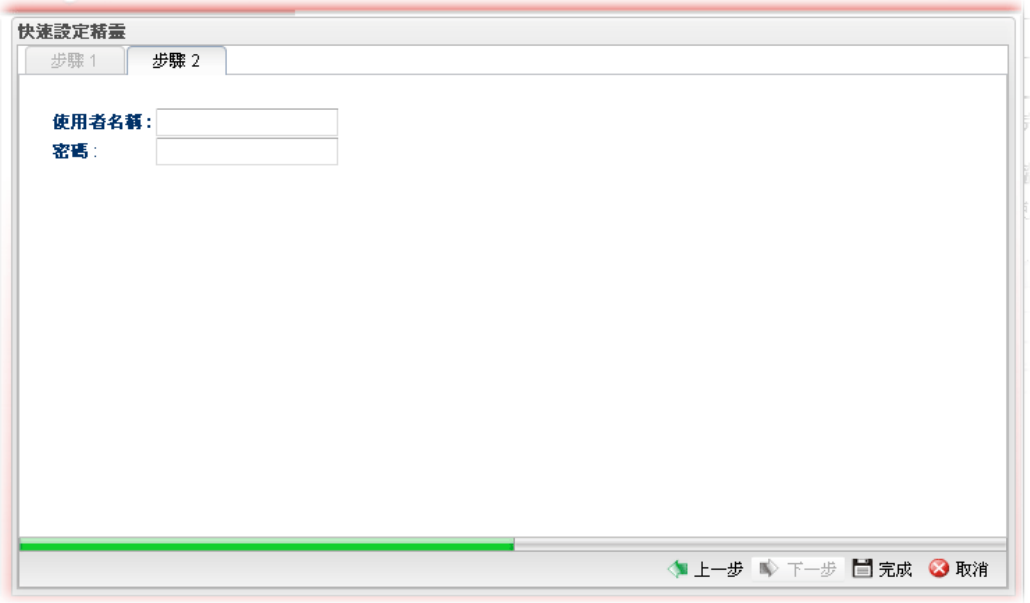
可用參數詳列如下：

項目	說明
主機名稱 (選項設定)	輸入辨識專用的主機名稱(此為選項設定)。
上一步	按此回到前一個設定頁面。
完成	按此儲存本頁設定並離開此頁面。
取消	按此捨棄本頁設定。

完成上述設定後，按**完成**結束連線上網設定。

如果選擇 PPPoE 協定類型

大多數 DSL 數據機使用此模式，當您選擇此模式時，請輸入業者提供給您的帳號及密碼等資訊。



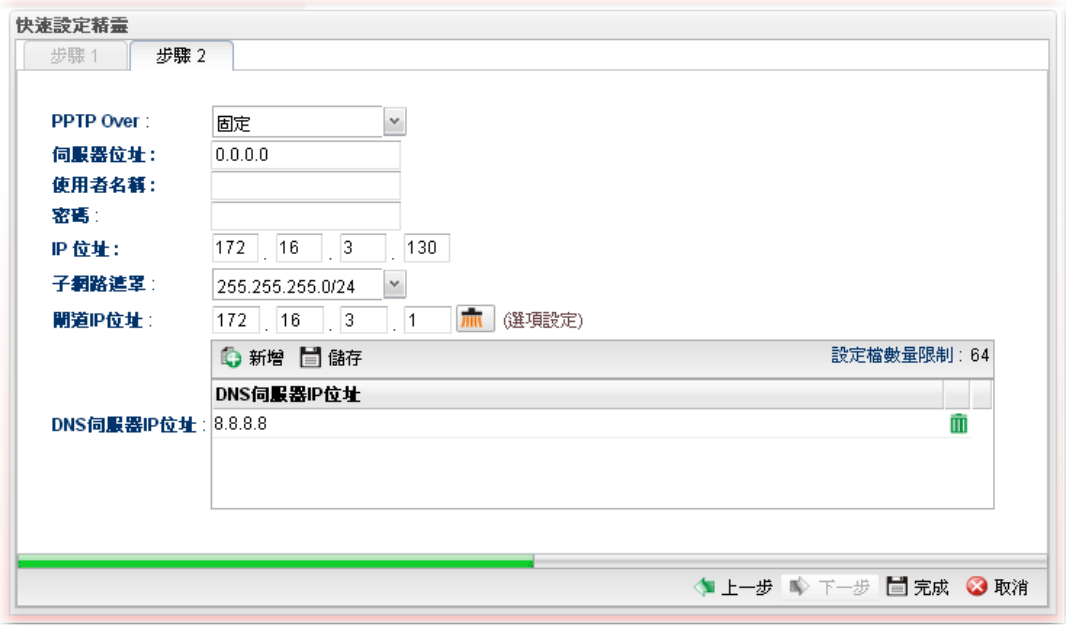
可用參數詳列如下：

項目	說明
使用者名稱	輸入 ISP 業者所提供的使用者名稱。
密碼	輸入 ISP 業者所提供的密碼。
上一步	按此回到前一個設定頁面。
完成	按此儲存本頁設定並離開此頁面。
取消	按此捨棄本頁設定。

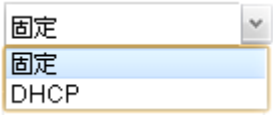
完成上述設定後，按**完成**結束連線上網設定。

如果選擇 PPTP 協定類型

這個模式讓使用者透過具 PPTP 服務的 DSL 數據機向 ISP 業者取得 IP 群組資訊，您的服務供應商將給您使用者名稱、密碼與驗證模式，請於此頁面輸入所有 ISP 業者提供給您的資訊。

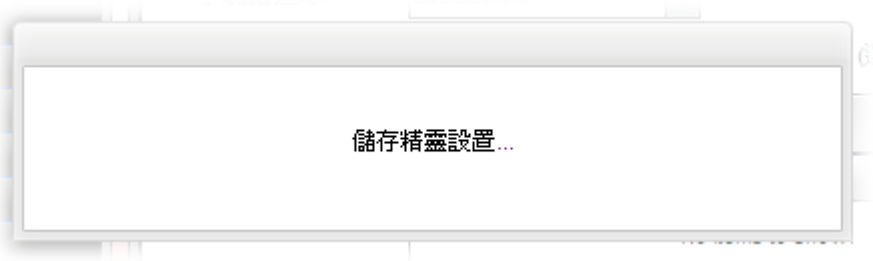


可用參數詳列如下：

項目	說明
PPTP Over	每當您連嘗試連線時，一般來說 ISP 會隨機指派 IP 位址給您，在某些情況下，ISP 業者會視您的要求，指派給您相同的 IP 位址，因此您只要在固定 IP 區域中輸入該 IP 位址，即可每次使用相同的 IP。**在您使用此設定功能之前，請先與您的 ISP 連絡，提出您的要求。**  **固定** – 指定 IP 位址。 **DHCP** – 自動取得 IP 位址。

伺服器位址	輸入 PPTP 伺服器的遠端 IP 位址。
使用者名稱	輸入 ISP 業者所提供的使用者名稱。
密碼	輸入 ISP 業者所提供的密碼。
IP 位址	輸入此 WAN 設定檔所需的真實 IP 位址。
子網路遮罩	自下拉式清單選擇網路遮罩。
閘道 IP 位址	輸入真實閘道位址。
DNS 伺服器 IP 位址	輸入 DNS (Domain Name Server) 伺服器所需的真實 IP 位址。按下**新增**可以增加新的 IP 位址，畫面上將會出現四個小方塊，您可在上面輸入 IP 位址，當您完成設定後，按下**儲存**。 **新增** – 按此以新增 IP 位址。 **儲存** – 按此儲存設定。
上一步	按此回到前一個設定頁面。
完成	按此儲存本頁設定並離開此頁面。
取消	按此捨棄本頁設定。

完成上述設定後，按**完成**結束連線上網設定。



當下列視窗出現時，即表示您已經完成快速安裝設定。

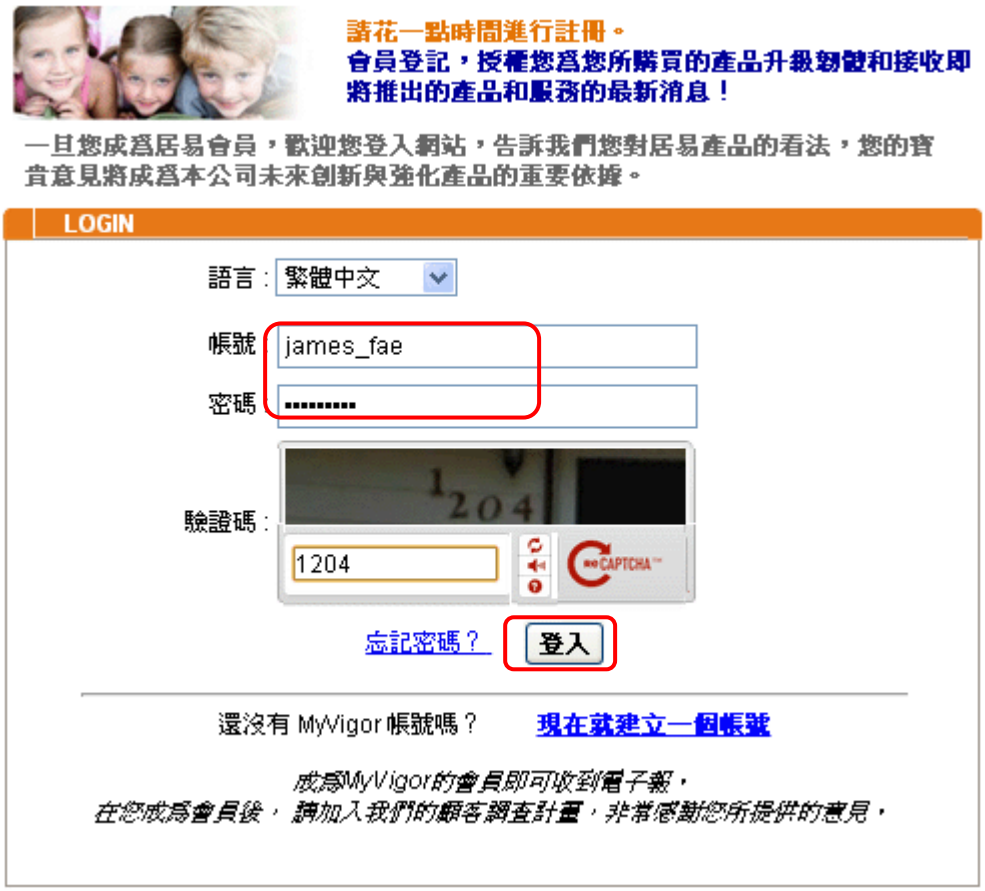
稍後，您可以隨時隨地瀏覽網頁，享受上網的樂趣。

2.3 註冊 Vigor 路由器

您已經完成快速安裝精靈的設定，接著您即可隨時上網。現在可以註冊路由器至 MyVigor 網站，取得更多的服務，請依照下列步驟完成註冊作業。

1 請登入路由器的網頁設定介面，輸入使用者名稱與密碼 (**"admin/admin"**)。然後自左邊的功能選單中選擇**產品註冊**。

2 登入頁面出現如下圖，請輸入您先前即建立的帳號與密碼，然後按下**登入**。如果您尚未申請過帳號與密碼，您可以按此頁下方"**現在就建立一個帳號**" 連結先建立個人的帳密，再回來本頁繼續進行。

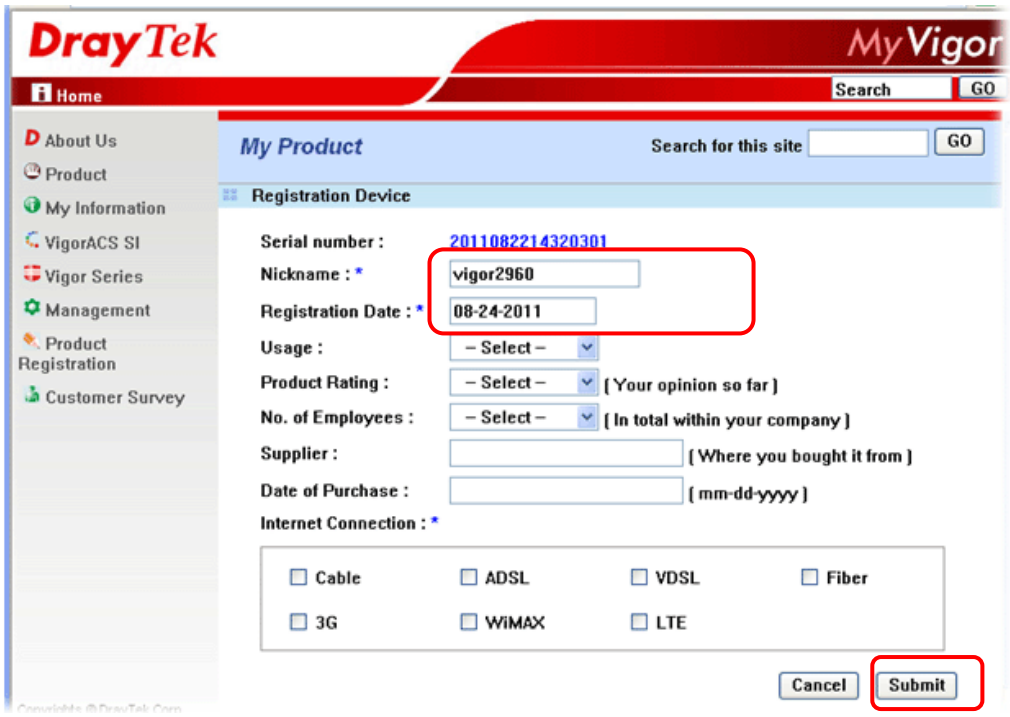


注意: 如果您尚未擁有登入帳號，請先申請建立一個帳號，並仔細閱讀與會員權利相關的各式條文。

3　按下登入後，將會出現如下的畫面，請按下**新增(Add)**。

> **注意:** 在 **Your Device List** 區域下方，所有已經在 MyVigor 網站註冊的路由器都會按照順序詳列出來。

4　當下述頁面出現時，請輸入路由器暱稱(Nickname)並選擇註冊日期(滑鼠移動至註冊日期方塊時會自動出現日曆供您選擇)，接著輸入路由器的基本訊息，最後按下**提交(Submit)**按鈕。

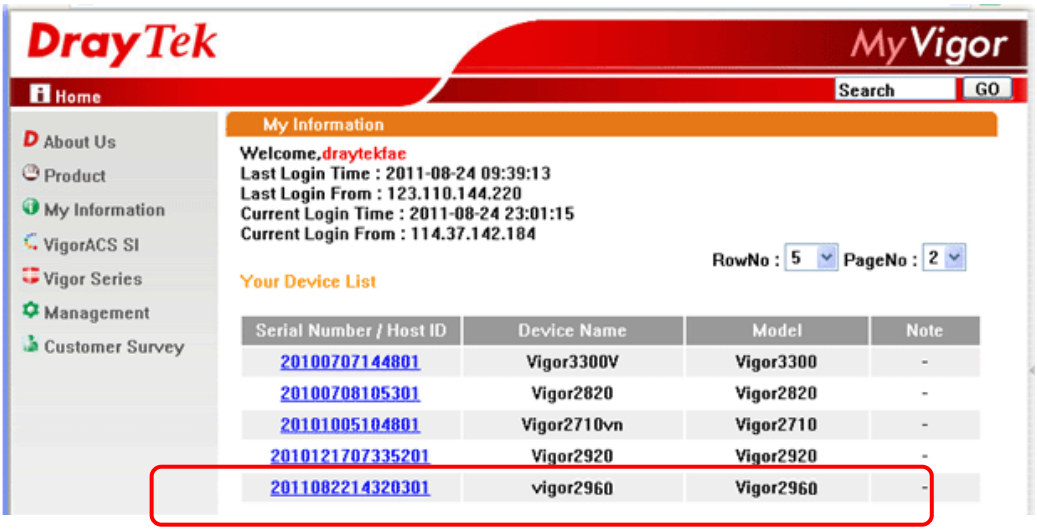


5 下述頁面出現後，您的路由器資訊已經加入 MyVigor 的資料庫中。按下確定(**OK**)，回到 **My Information** 網頁。

Your device has been successfully added to the database.

OK

6 看看 **My Information** 網頁，新增的路由器將會列在 **Your Device List** 清單中，現在您已經完成產品註冊。

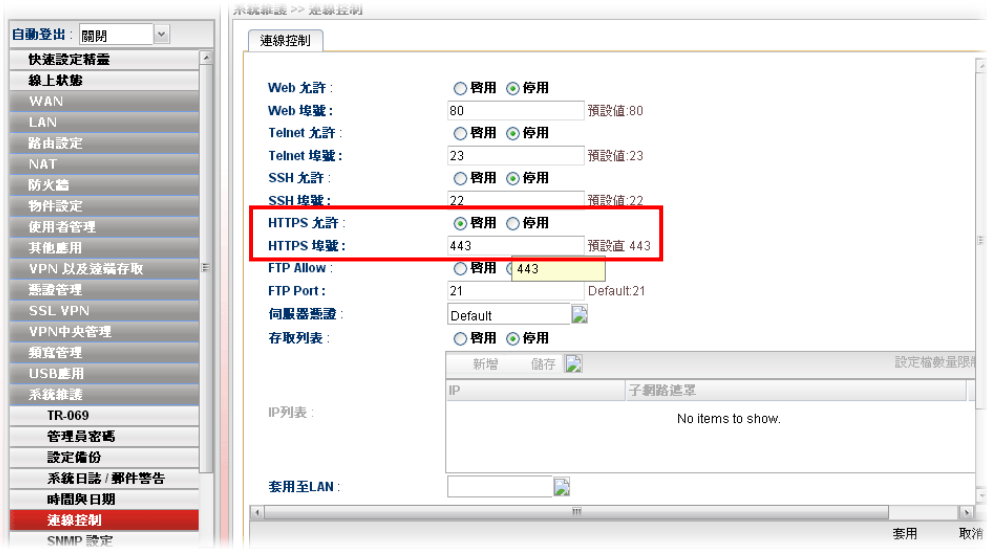


第三章: 應用解說

3.1 如何透過登入路由器的 HTTPS 伺服器建立具備 RDP 服務的 SSL VPN 通道?

Remote Desktop Protocol (RDP)協定是爲了在網路中能利用 Microsoft Terminal Services 達成安全通訊目的而產生，以下提供一個簡易的例子，說明利用瀏覽器在路由器與 RDP 伺服器之間建立連線。

1. 開啓 Vigor2960 的網頁設定介面。
2. 開啓**系統維護>>連線控制**，按下 **HTTPS 允許**的**啓用**鈕，輸入埠號值 443。



3. 開啓 **SSL VPN>>SSL 應用**並按下 **RDP** 標籤以便建立設定檔(命名爲 Win7)，輸入實際 RDP 伺服器的 IP 位址、埠號、螢幕大小等資訊，然後按下**套用**儲存。

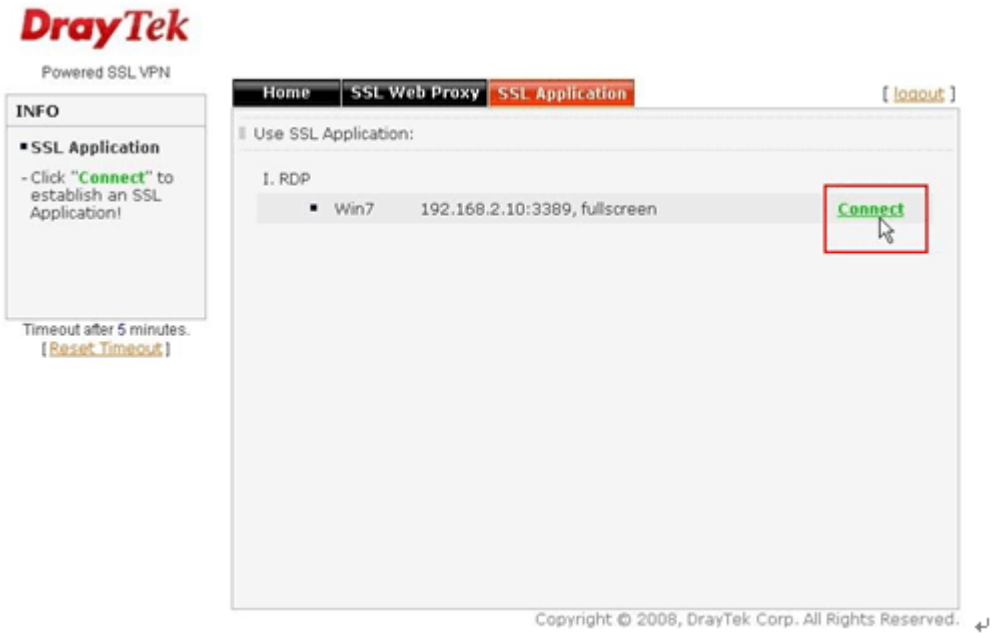
4. 開啓**使用者管理>>使用者設定檔**以便建立新的設定檔(命名爲 7788)，將**密碼**也設定爲 7788 並選擇 Win7 作爲 **SSL 應用(RDP)** ，然後按下**套用**儲存。

5. 登出 Vigor2960 網頁設定介面。

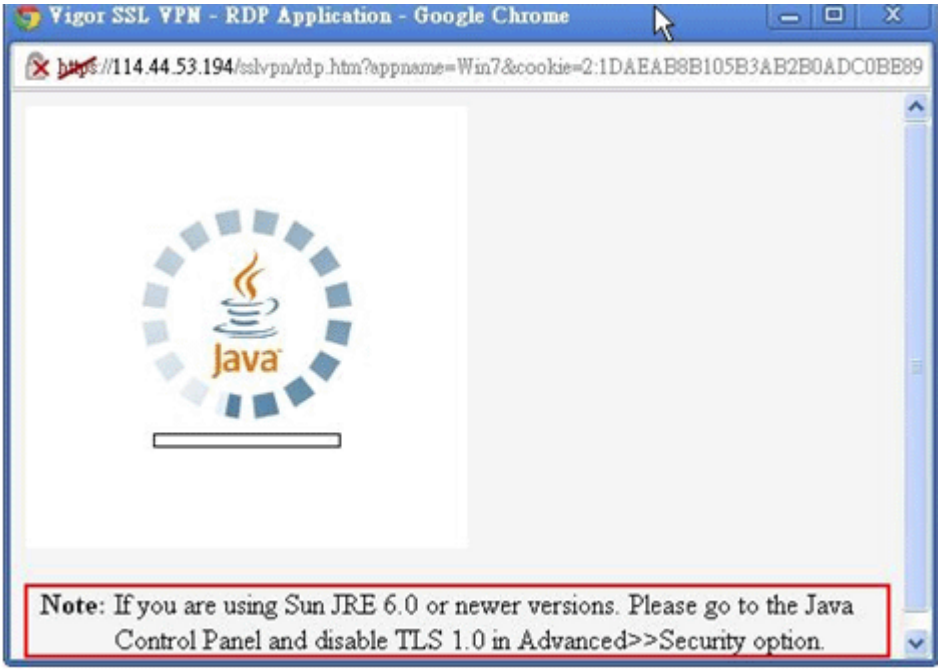
6. 以使用者名稱及密碼皆爲 7788 登入 Vigor2960 HTTPS 伺服器。

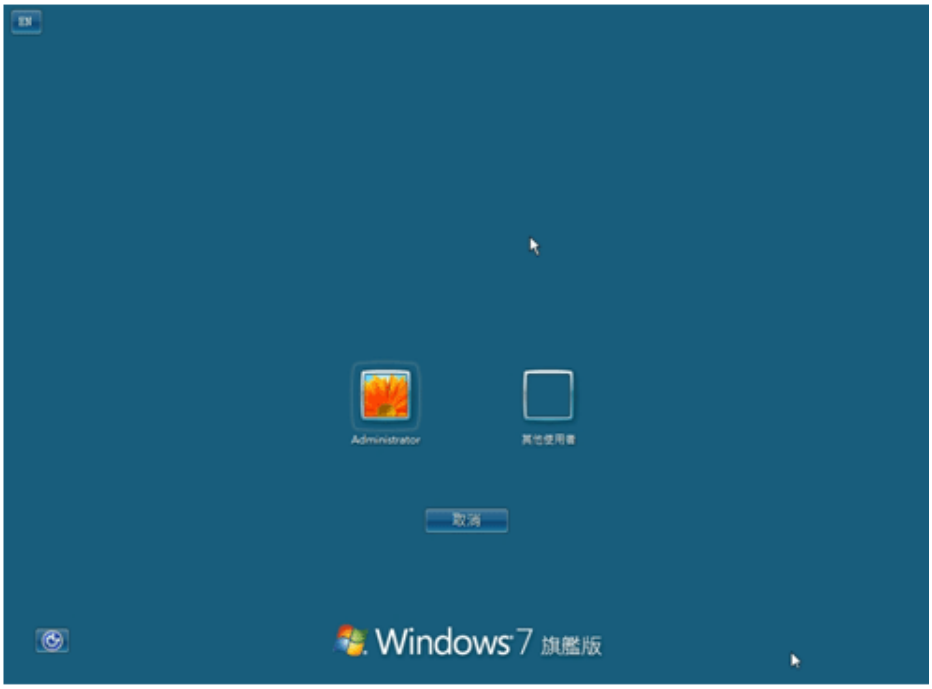
7. 類同如下的頁面將會出現，請按下 **SSL 應用**連結。

8. 在如下頁面當中，按下**連結**以便連接至 Win7 --- RDP 伺服器。



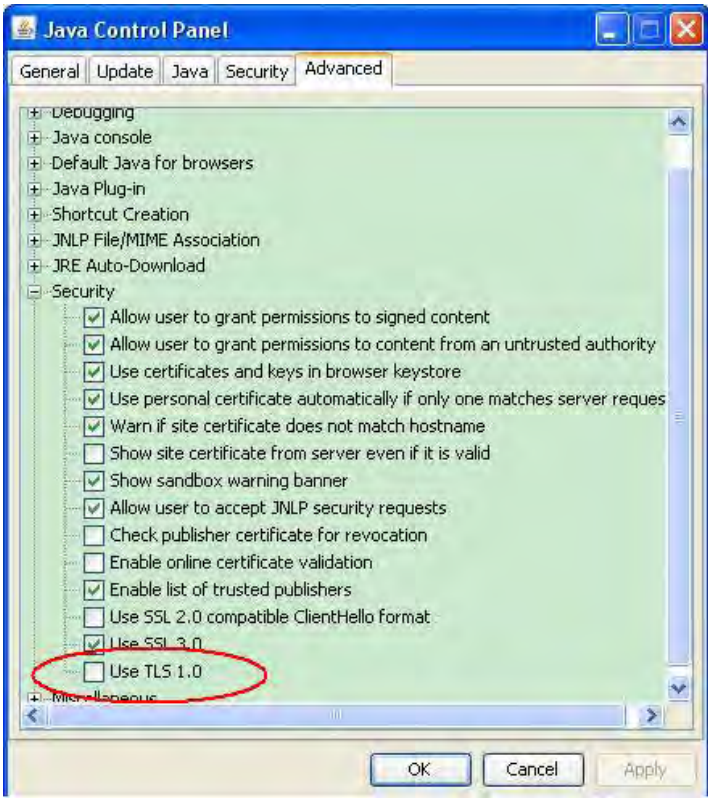
9. 之後，您可以透過流覽器登入 Windows 7，注意視窗下方的訊息，TLS 為 Transport Layer Security 之縮寫。





疑難排除

如果您已經安裝 Java Runtime Environment edition 6 但仍無法建立連線，請先確認 **Java Control Panel** 中“**Use TLS 1.0**”已被停用，如下圖所示，接著，再次嘗試連線。



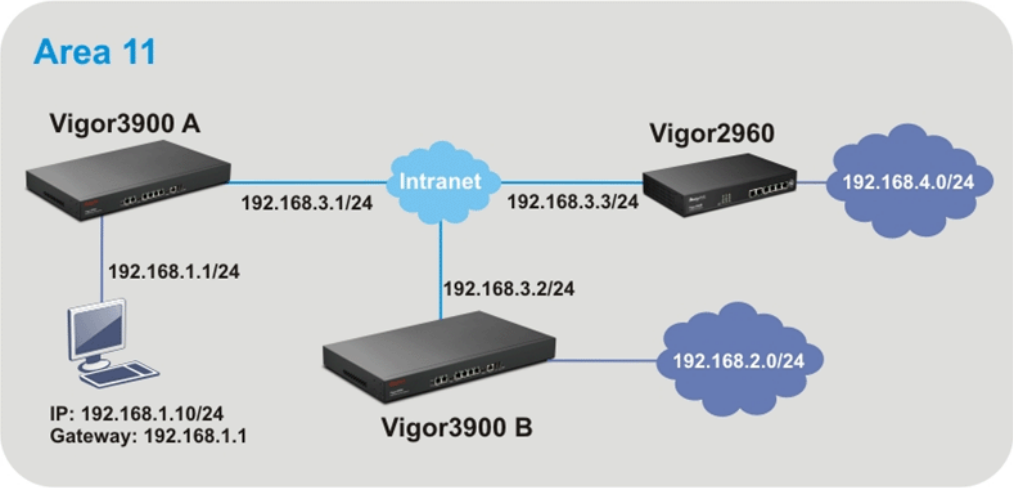
3.2 如何設定 OSPF?

OSPF (Open Shortest Path First) 使用 SPF (Shortest Path First) 演算方式來計算路由度量，適合大型網路與複雜的資料交換，Vigor3900 與 Vigor2960 皆支援 OSPF 版本 2(僅適於 IPv4)。

用於 OSPF 中的自主系統(AS)表示大型實體可以分割成數區，通常區域 0(Area 0)爲 OSPF 的主幹，可分配路由資訊予其他區域。

當您想要支援大型網路或想要較少破壞的路由資訊，您可以啓用 OSPF 功能來滿足您的需求，請注意雙端的路由器皆必須同時支援 OSPF 功能以便建立 OSPF 連線。

下圖範例中，無須設定任何固定路由，電腦可前往 192.168.2.0/24 與 192.168.4.0/24。

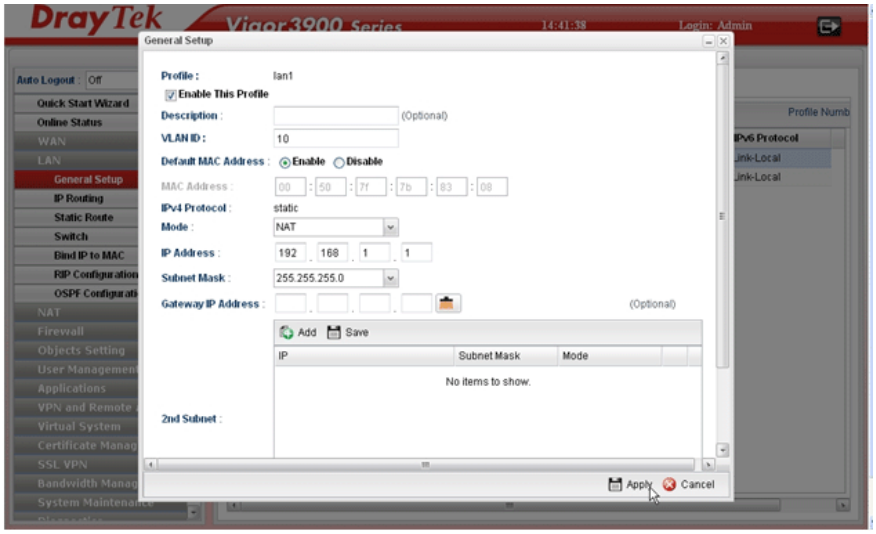


OSPF 可將每台路由器(例如上圖的 Vigor3900A, Vigor3900B 與 Vigor2960)，放在結構上端，依照累計費用來計算每個目標 OSPF 至每個目的地的最短距離。

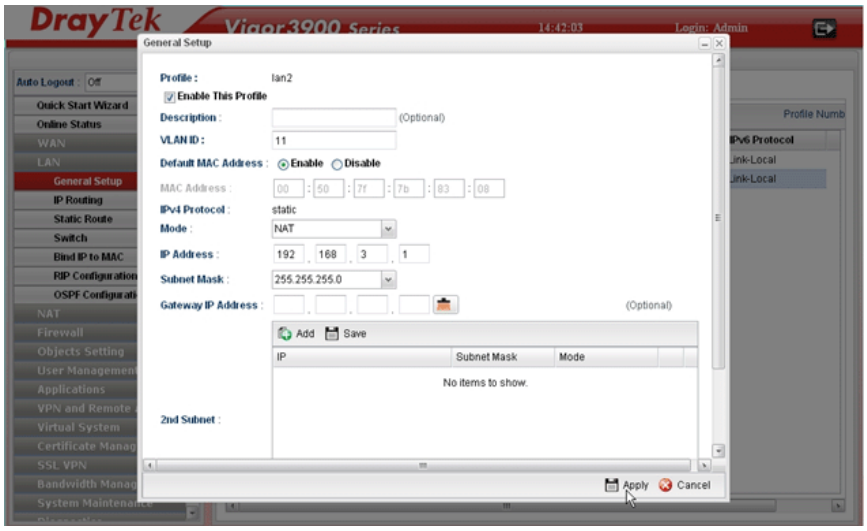
即使所有的路由器都使用相同的連結狀態資料庫，來建立最短路徑，每個路由器都有自身的拓璞以及計算其 SPF 結構樹。

Vigor3900 A 的設定

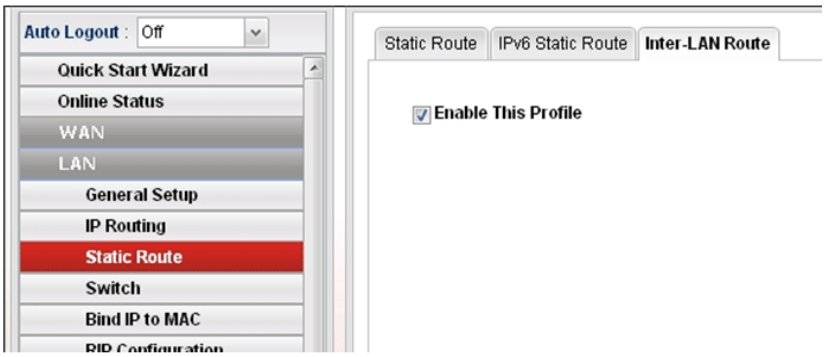
1. 開啓 **Routing >> General Setup** 建立一個 LAN (192.168.1.1/24) 設定檔，檔名爲 lan1，設定內容如下圖所示。



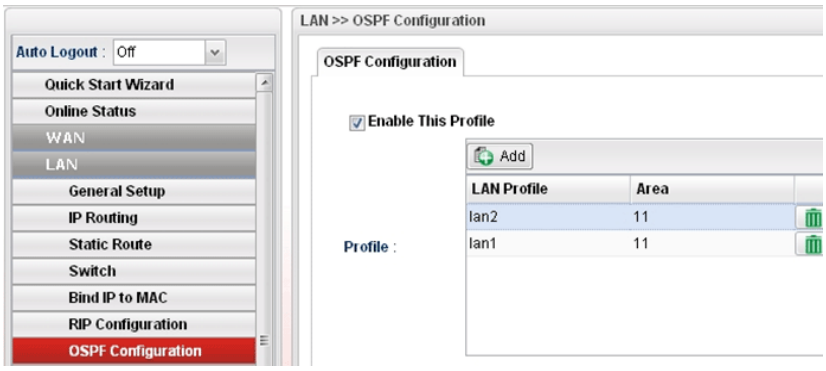
2. 接著，繼續建立 LAN (192.168.3.1/24)設定檔，檔名爲 lan2，其餘設定內容如下所示。



3. 開啓 **LAN >> Static Route Setup** 並按下 **Inter-LAN Route** 標籤，勾選**啓用此設定檔**。

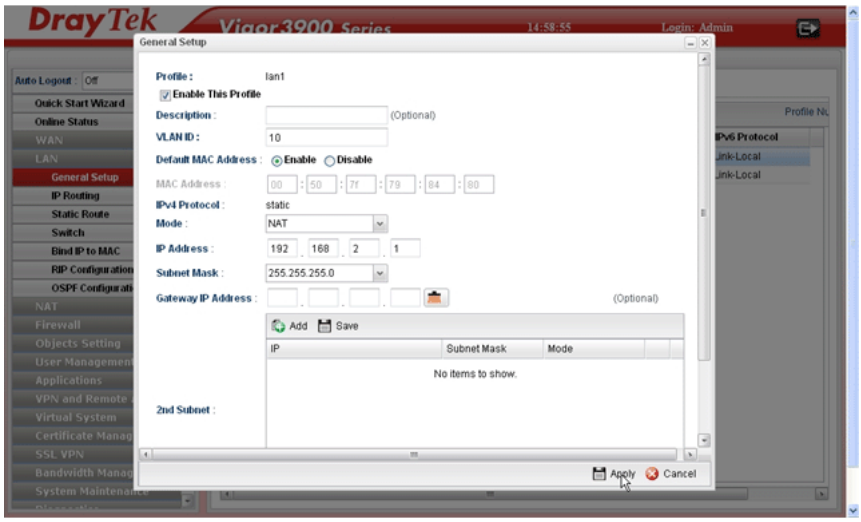


4. 開啓 **LAN >> OSPF Configuration** 並啓用此設定檔，接著按下新增將 LAN 設定檔 lan2 的區域設定設成 11 而 lan1 區域設定設爲 11 (如前述拓墣圖所示)。

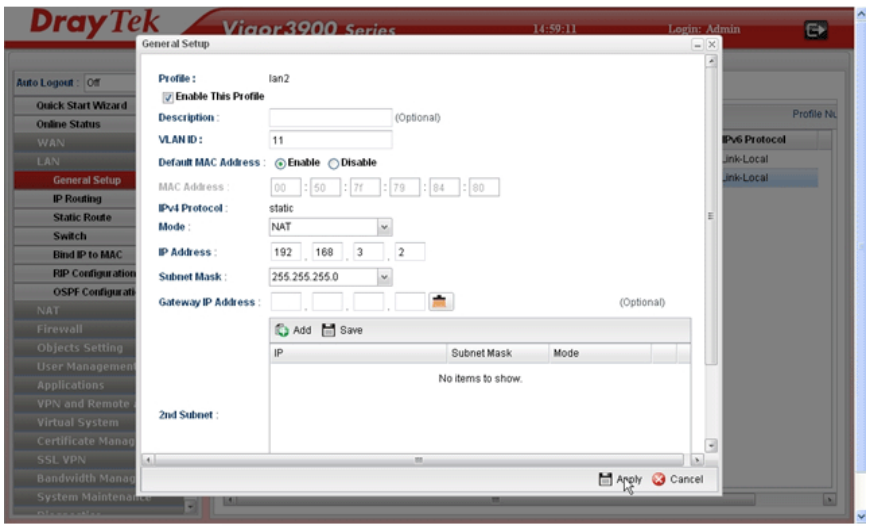


Vigor3900 B 的設定,

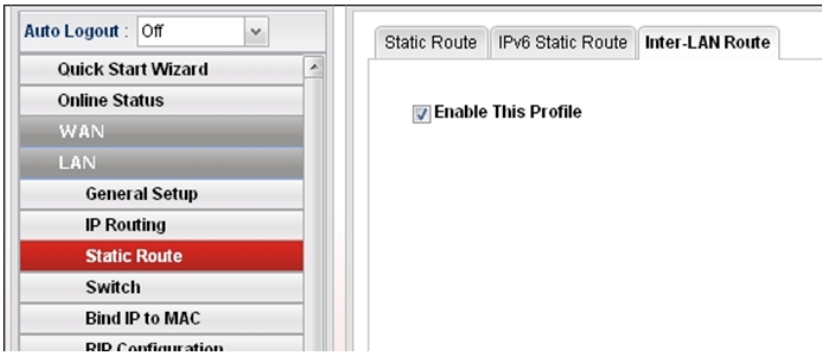
1. 開啓 **Routing >> General Setup** 建立一個 LAN (192.168.2.1/24) 設定檔，檔名爲 lan1，設定內容如下圖所示。



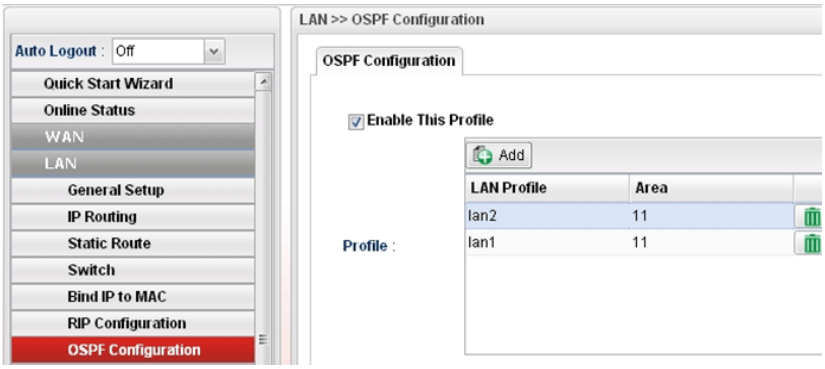
2. 接著，繼續建立 LAN (192.168.3.2/24)設定檔，檔名爲 lan2，其餘設定內容如下所示。



3. 開啓 **LAN >> Static Route Setup** 並按下 **Inter-LAN Route** 標籤，勾選**啓用此設定檔**。



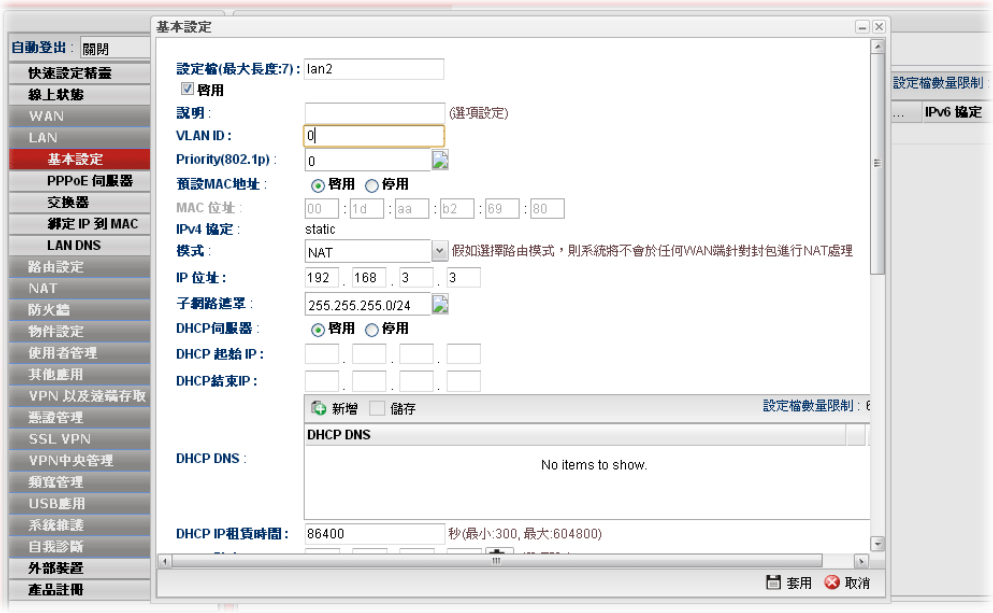
4. 開啓 **LAN >> OSPF Configuration** 並啓用此設定檔，接著按下**新增**將 LAN 設定檔 lan2 的區域設定設成 11 而 lan1 區域設定設爲 11 (如前述拓墣圖所示)。



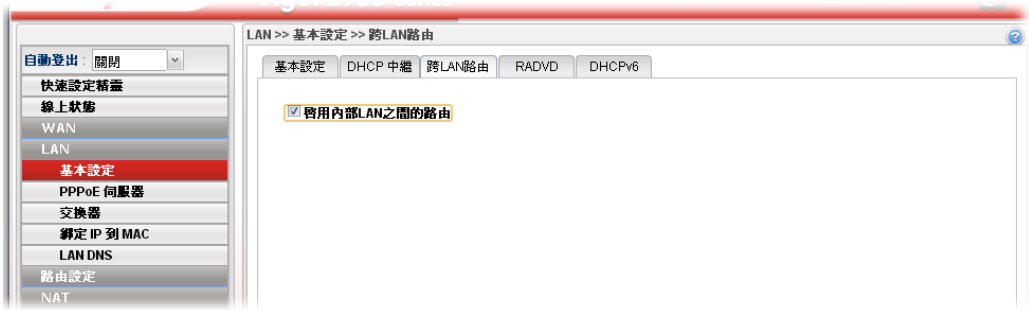
Vigor2960 的設定,

1. 開啓 **LAN>> 基本設定**建立一個 LAN (192.168.4.1/24) 設定檔，檔名爲 lan1，設定內容如下圖所示。

2. 接著，繼續建立 LAN (192.168.3.3/24)設定檔，檔名為 lan2，其餘設定內容如下所示。



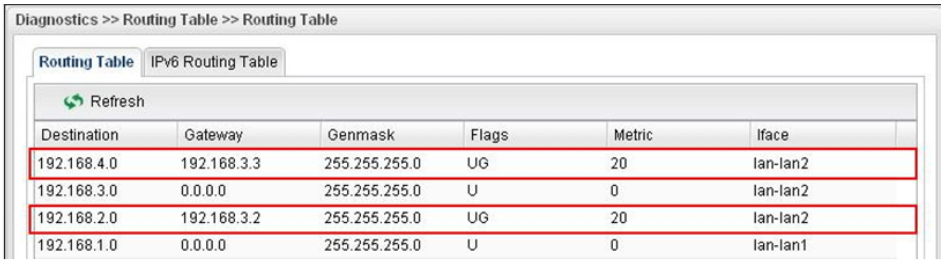
3. 開啓 **LAN >> 基本設定**並按下**跨 LAN 路由**標籤，勾選**啓用內部 LAN 之間的路由**。



4. 開啓**路由設定 >> OSPF 設定**並啓用此功能，再按下**新增**將 LAN 設定檔 lan2 的區域設定設成 11 而 lan1 區域設定設為 11 (如前述拓撲圖所示)。

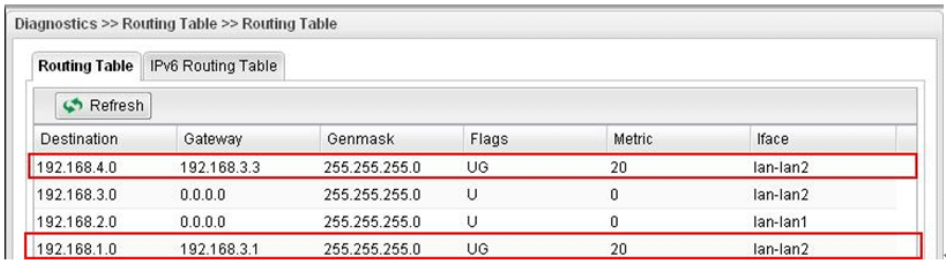
5. 設定完畢之後，檢查 OSPF 所產生的路由資訊(紅框部份)。

Vigor3900 A 的路由資訊



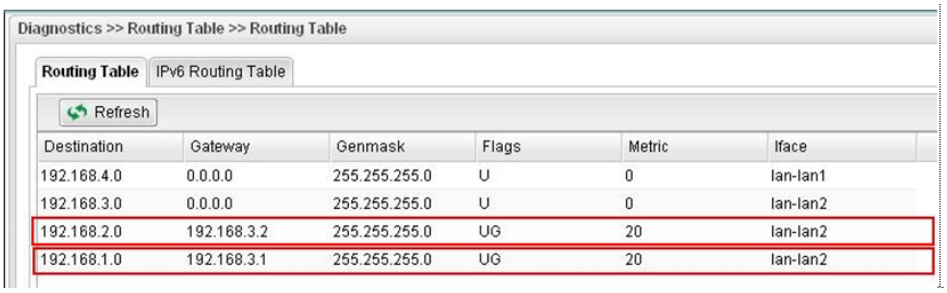
Destination	Gateway	Genmask	Flags	Metric	Iface
192.168.4.0	192.168.3.3	255.255.255.0	UG	20	lan-lan2
192.168.3.0	0.0.0.0	255.255.255.0	U	0	lan-lan2
192.168.2.0	192.168.3.2	255.255.255.0	UG	20	lan-lan2
192.168.1.0	0.0.0.0	255.255.255.0	U	0	lan-lan1

Vigor3900 B 的路由資訊



Destination	Gateway	Genmask	Flags	Metric	Iface
192.168.4.0	192.168.3.3	255.255.255.0	UG	20	lan-lan2
192.168.3.0	0.0.0.0	255.255.255.0	U	0	lan-lan2
192.168.2.0	0.0.0.0	255.255.255.0	U	0	lan-lan1
192.168.1.0	192.168.3.1	255.255.255.0	UG	20	lan-lan2

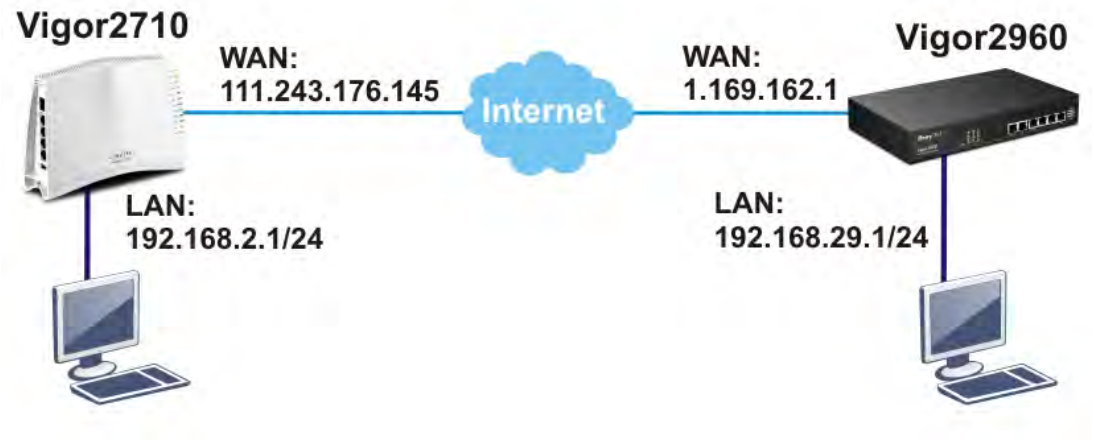
Vigor2960 的路由資訊



Destination	Gateway	Genmask	Flags	Metric	Iface
192.168.4.0	0.0.0.0	255.255.255.0	U	0	lan-lan1
192.168.3.0	0.0.0.0	255.255.255.0	U	0	lan-lan2
192.168.2.0	192.168.3.2	255.255.255.0	UG	20	lan-lan2
192.168.1.0	192.168.3.1	255.255.255.0	UG	20	lan-lan2

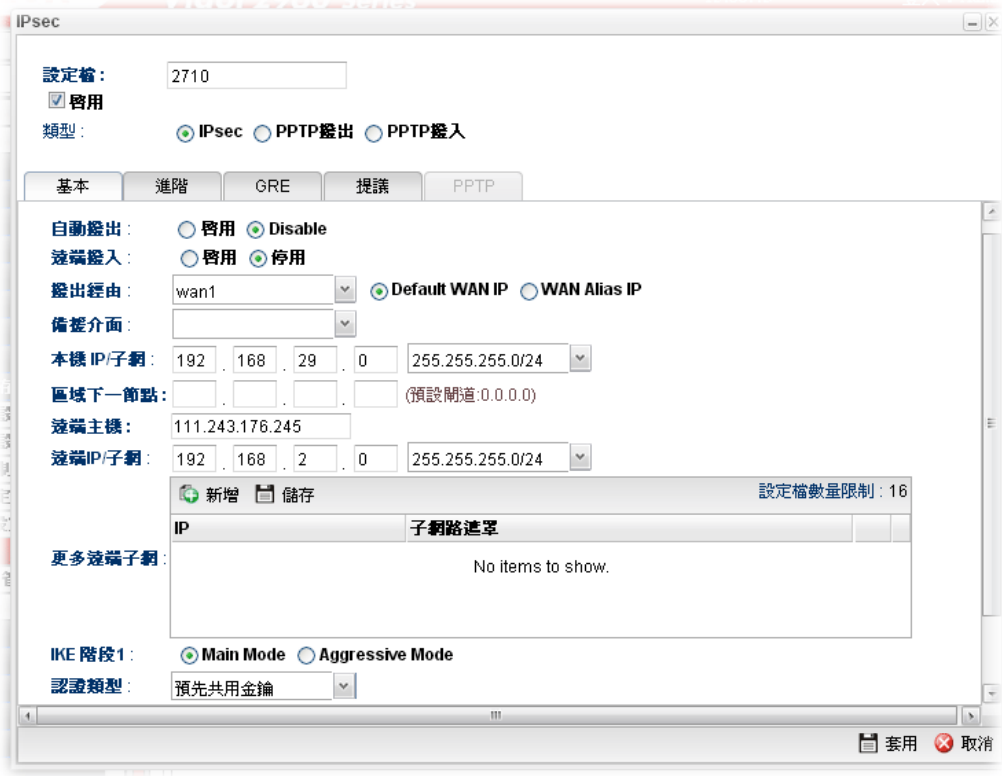
3.3 如何在 Vigor2960 與其他路由器之間建立 LAN to LAN IPSec 通道 (Main Mode)

本文以 Vigor2960 與 Vigor2710 爲例，說明 LAN to LAN IPSec 通道的設定方式。



設定 Vigor2960

1. 登入 Vigor2960 的網頁設定介面，開啓 **VPN 以及遠端存取 >> VPN 設定**以便建立新的 VPN 通道設定檔。按下**新增**開啓如下頁面。

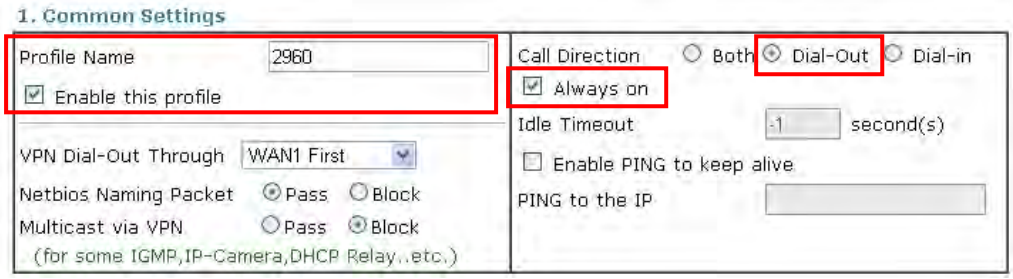


如上圖所示，輸入預先共用金鑰然後選擇一個 WAN 設定檔(例如 wan1)，指定本機 IP/子網 (例如 192.168.29.0/24)，遠端主機位址設定爲 Vigor 2710 的 WAN IP 位址，遠端 IP/子網則設定爲 192.168.2.0/24。

2. 按下**套用**儲存設定並回到上一頁。

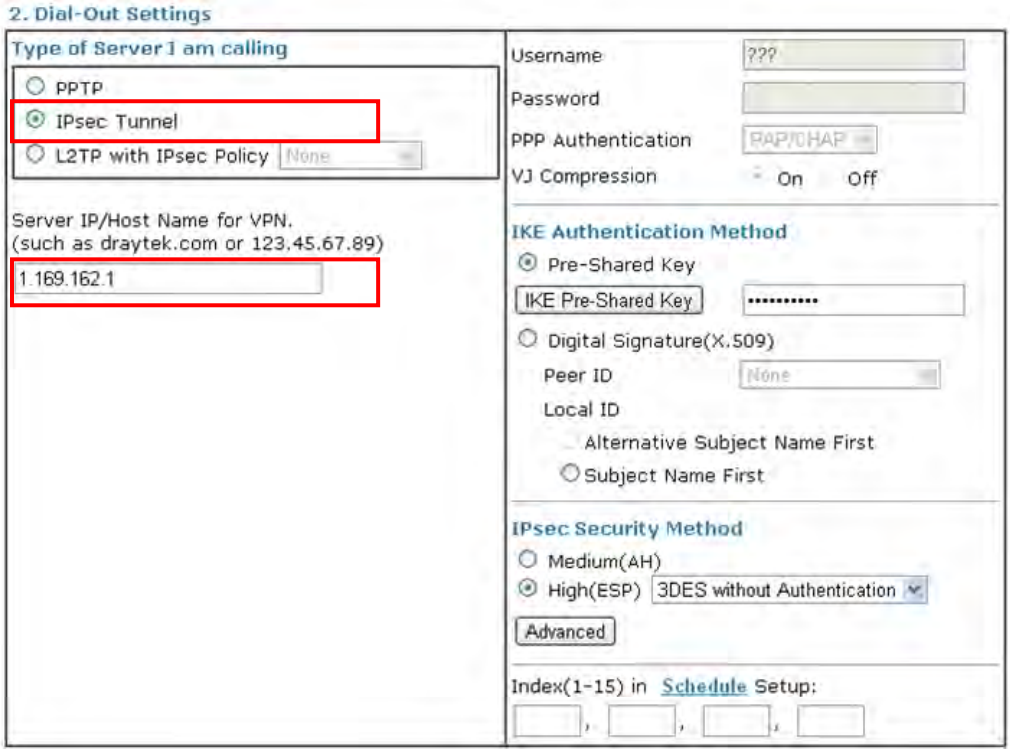
設定 Vigor2710

1. 在 Vigor2710 中，需建立 VPN 通道連接到 Vigor2960，登入 Vigor2710 網頁設定介面並開啓 **VPN and Remote Access >> LAN to LAN**。

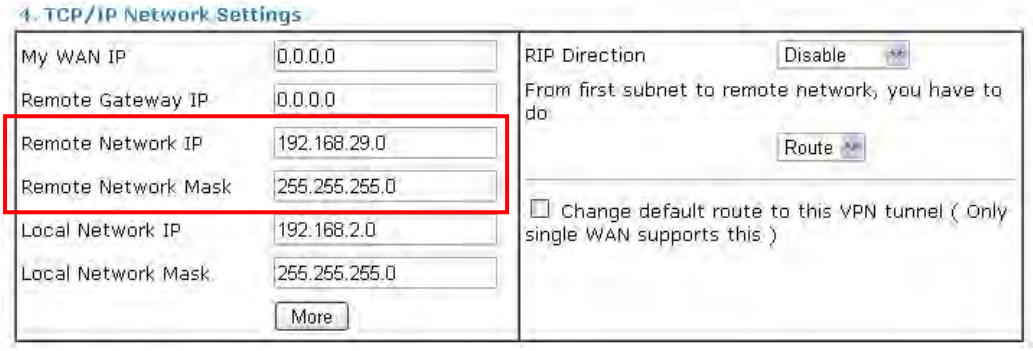


- 請在 Profile Name 欄位中輸入此 VPN 連線的設定檔名稱(例如 2960)。
- 勾選 **Enable this profile** 方塊。
- 選擇 **Dial-Out** 作爲 **Call Direction** 然後勾選 **Always on** 方塊。

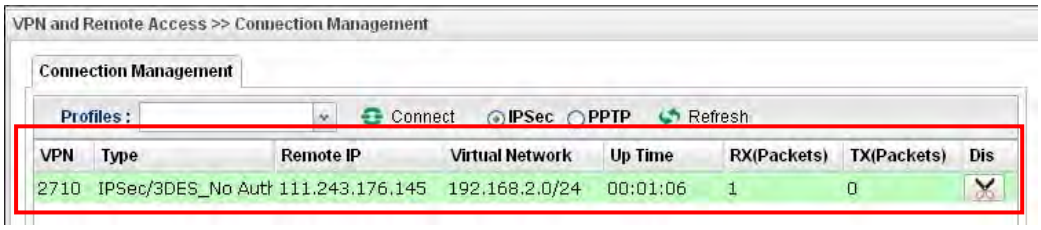
2. 針對 **Dial-Out Settings** 部分，請選擇 **IPSec Tunnel** 並在 **Server IP/Host Name for VPN** 欄位中輸入 Vigor2960 的 WAN IP 位址(例如 1.169.162.1)，輸入您在 Vigor2960 中所設定的 IKE Pre-Shared Key 金鑰值。



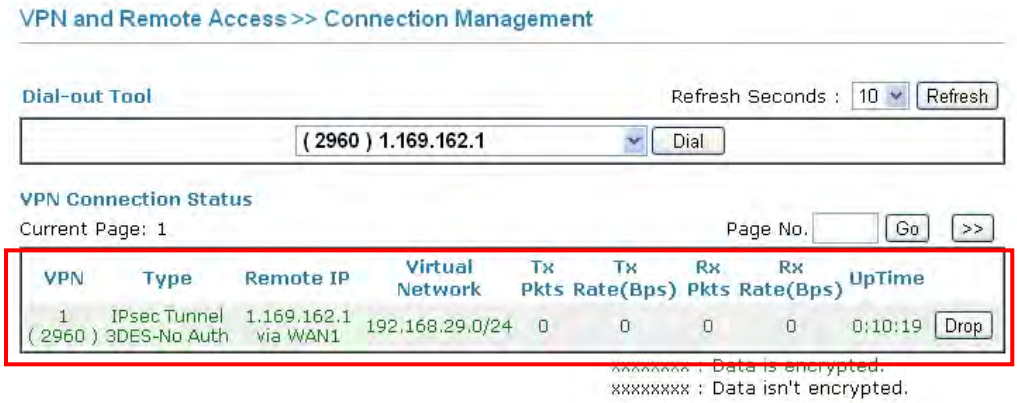
3. 由於 Vigor2710 的角色乃作爲撥出端(dialing-out)，請跳過 Dial-In 設定部份，在 **Remote Network IP** 與 **Remote Network Mask** 欄位設定中輸入 Vigor2960 的遠端位置設定，最後按下確定 **OK** 按鈕儲存設定。



4. 接著分別檢查二端的 VPN 連線是否成功，關於 Vigor2960 部份，可開啓 **VPN and Remote Access>>IPSec>>Status** 檢查設定的結果。



至於 Vigor2710 部份，則開啓 **VPN and Remote Access>>Connection Management** 頁面來確認連線是否成功。



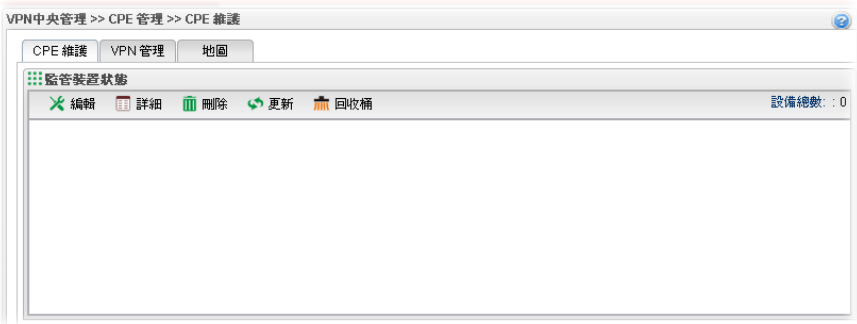
3.4 CVM 應用 – 如何透過 Vigor2960 管理 CPE (路由器)?

欲透過 Vigor29600 管理 CPE，您必須先設定 CPE 的 ACS URL 再設定 Vigor2960 的使用者名稱與密碼，這個範例中，我們使用 Vigor2830 系列來說明。

3.4.1 設定 Vigor2960

1. 登入 Vigor2960 的網頁使用者設定介面。
2. 開啓**系統維護>>連線控制**，**Web 允許**項目勾選**啓用**，輸入 **Web 埠號**所需的數值，然後按下**套用**儲存設定。

3. 開啓 **VPN 中央管理>>CPE 管理**，在 **CPE 維護**的頁面上，尚無任何 CPE 在 Vigor2960 的管理之下。



4. 開啓 **VPN 中央管理>>基本設定**。
5. 按下**基本設定**標籤，勾選**啓用**方塊，自 WAN 設定檔下拉式清單中選擇 WAN 介面，輸入埠號、使用者名稱與密碼，牢記本頁的設定。

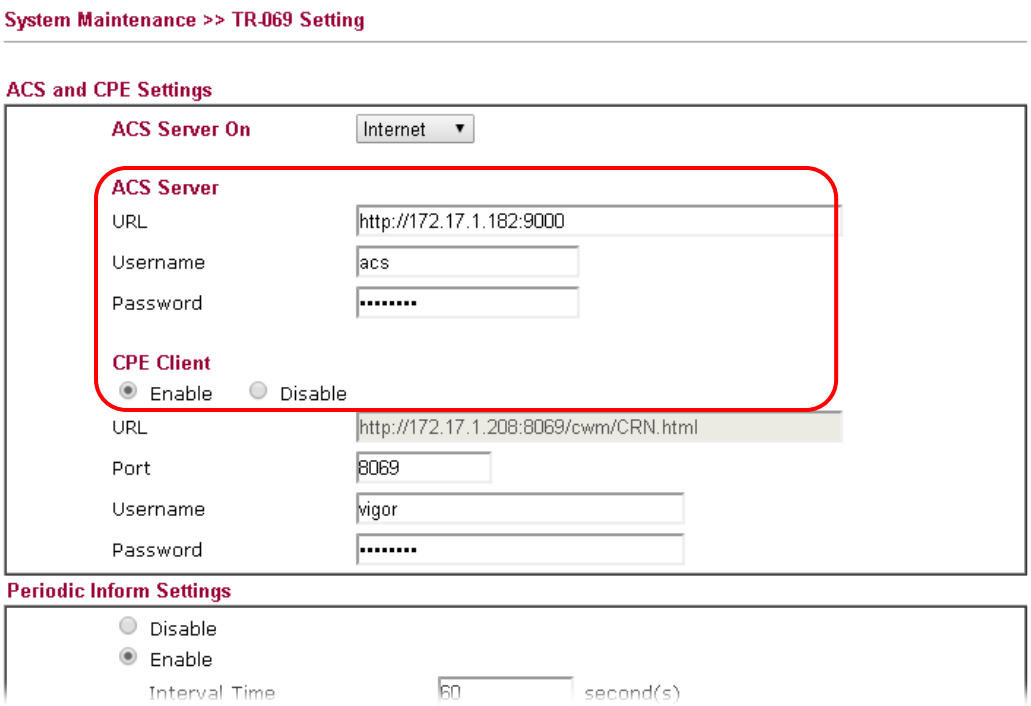
6. 按下**套用**儲存設定。

3.4.2 設定 CPE

如果要讓 Vigor2960 管理 CPE，那麼必須先在 CPE 端設定好 ACS URL，以及 Vigor2960 使用的使用者名稱與密碼。

1. 連接一台 CPE(例如 Vigor2830 系列)，準備進入該 CPE 的網頁使用者設定介面。
2. 在連接 CPE 的電腦端，開啟任一網頁瀏覽器(例如 IE, Mozilla Firefox 或 Netscape)，網址欄處輸入 **http://192.168.1.1**。
3. 請輸入使用者名稱及密碼，如果不知道正確的名稱及密碼，請先與經銷商聯絡取得正確資料。
4. 開啟 **System Maintenance >> TR-069**。

5. 在 ACS Server 欄位中，請輸入 Vigor3900 的 URL (格式為 http://{IP address of Vigor2960}:{CVM port}/ACSServer/services/ACSServlet)並在 Vigor2960 的 **Central VPN Management>>General Setup** 頁面中輸入與此相同的使用者名稱及密碼資訊，接著，CPE Client 項目按下 **Enable**，再按下 **OK** 儲存設定。

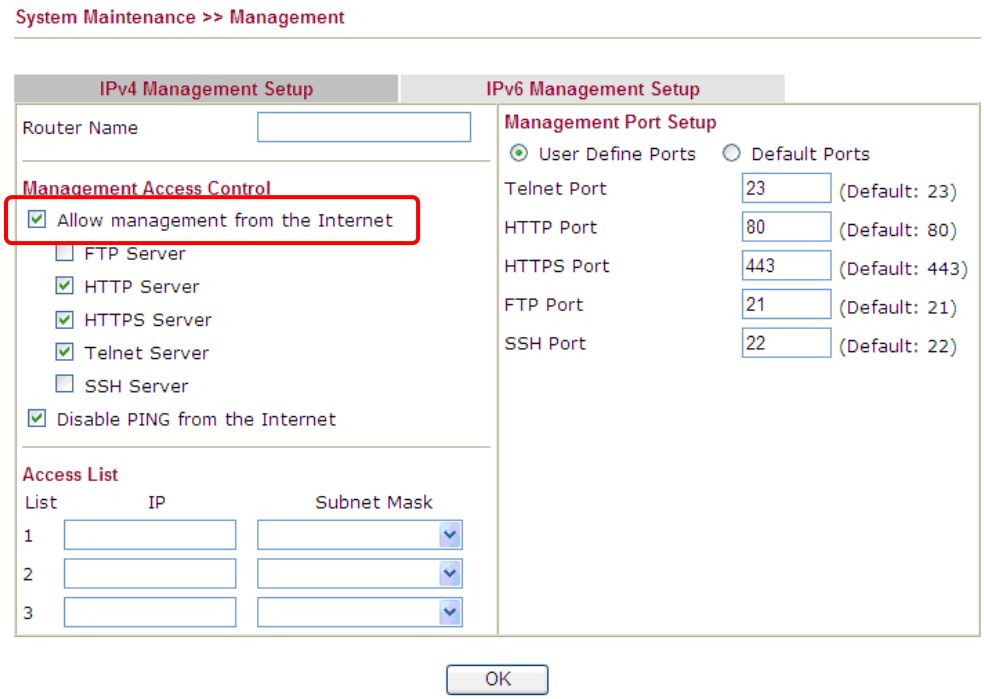


3.4.3 啟用 CPE 的遠端管理功能

1. 登入 CPE 的網頁使用者設定介面。

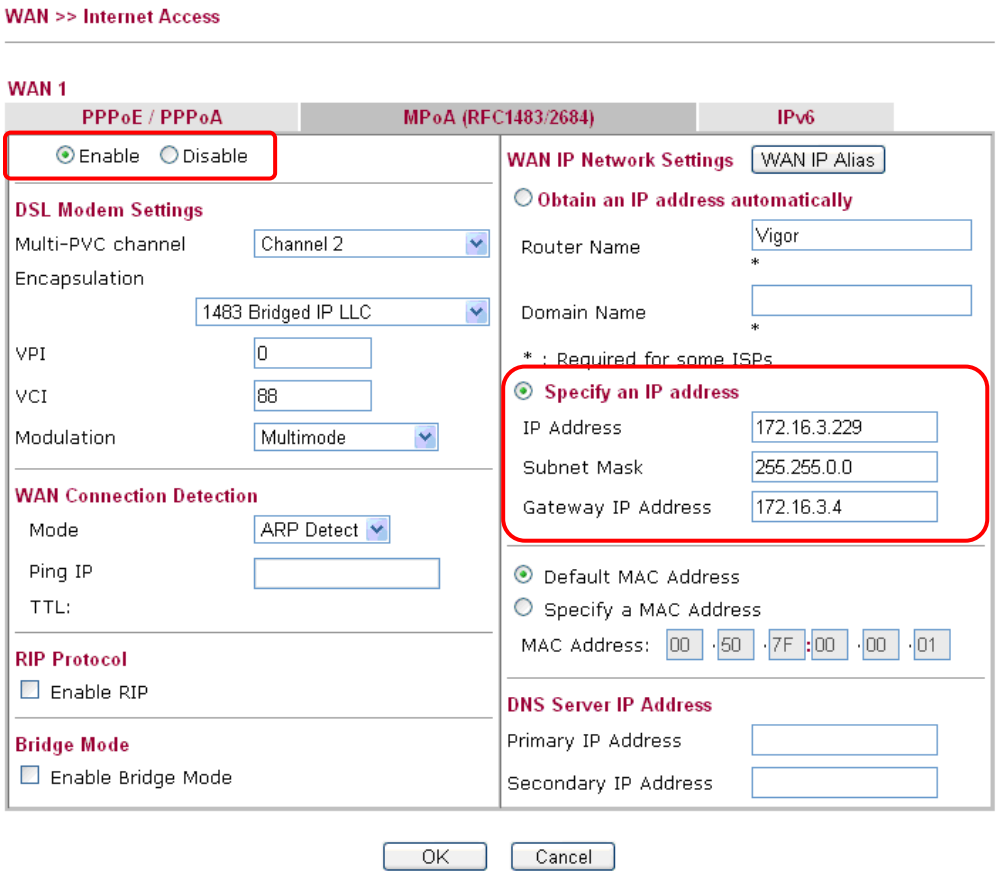
2. 開啓 **System Maintenance>>Management Setup**。

3. 勾選 **Allow management from the Internet** 以設定管理存取控制。



3.4.4 啓用 CPE 的 WAN 連線

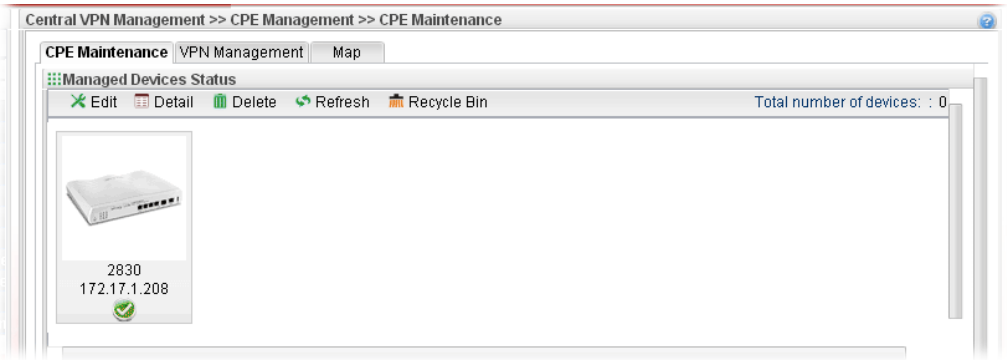
1. 登入 CPE 的網頁使用者設定介面。
2. 開啓 **WAN>>Internet Access**，在 WAN1 項目下使用 **Access Mode** 下拉式清單，選擇 **MPoA** (RFC1483/2684)模式，接著按下 **Details Page**。
3. 按下 **Specify an IP address**，輸入有關 CPE 正確的 WAN IP 位址，子網遮罩以及閘道 IP 位址，再按下 **OK** 儲存。



注意 ： 啓動 CPE 並重新登入 Vigor2960，已經登錄至 Vigor2960 的 CPE 將立刻由系統擷取相關資料並會顯示在 Vigor2960 網頁使用者設定介面之 **Central VPN Management>>CPE Management** 頁面中。

3.4.5 檢查 CPE 管理頁面

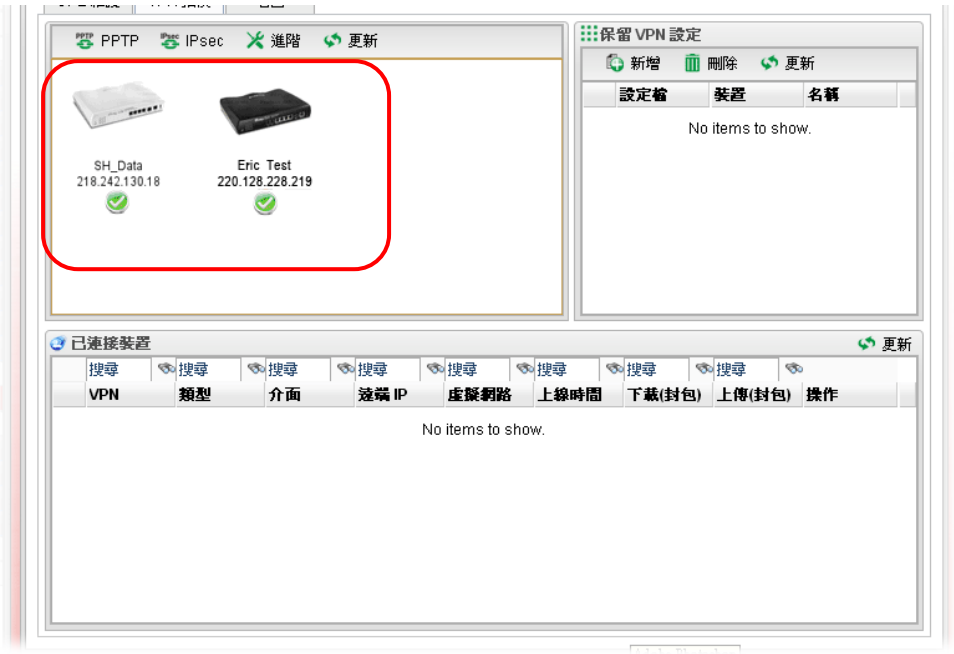
1. 回到 Vigor2960 的網頁使用者設定介面。
2. 開啓 **VPN 中央管理>>CPE 管理**。
3. 現在已經有一台 CPE (Vigor2830)在 Vigor2960 的管理下。



3.5 CVM 應用 – 如何在 Vigor2960 與遠端設備之間建立 VPN?

當遠端設備已被納入 Vigor2960 管理之下，我們可以很輕易的在這二者之間建立一條 VPN 連線。

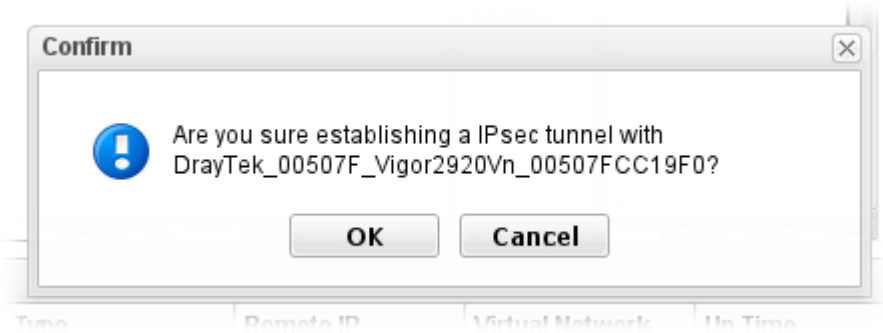
1. 登入 Vigor2960 系列的網頁使用者設定介面。
2. 開啓 **VPN 中央管理>>CPE 管理**之 **VPN 管理**，螢幕上顯示出來的圖示，即表示該遠端設備已準備妥當，可以和 Vigor2960 建立 VPN 連線。



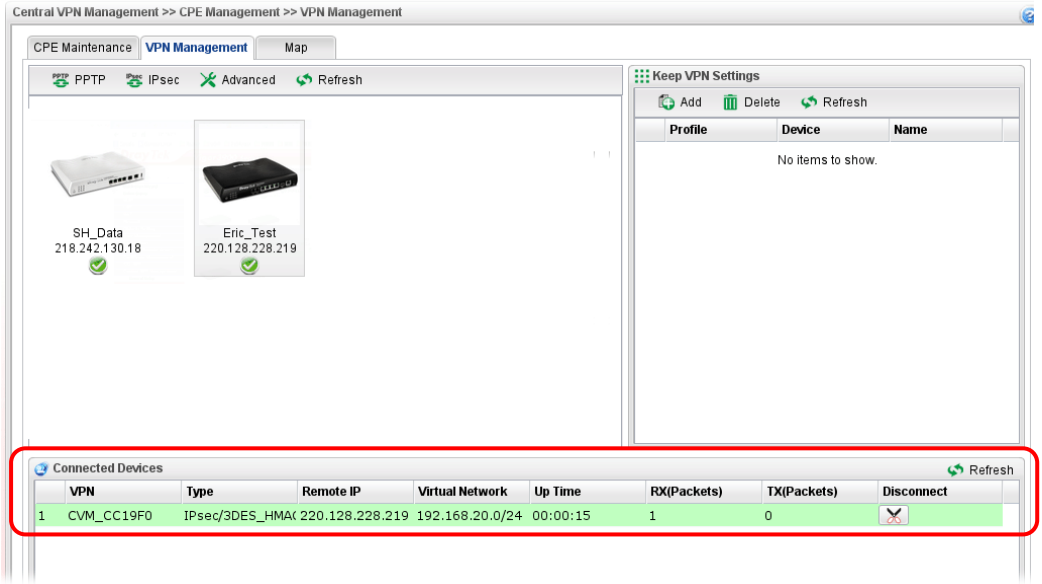
3. 按下遠端設備圖示(標示)並按下 **PPTP** 或是 **IPsec** 按鈕。

或者按下**進階**開啓如下頁面，指定您想要的 CPE 設定內容，再按**連接**完成設定。

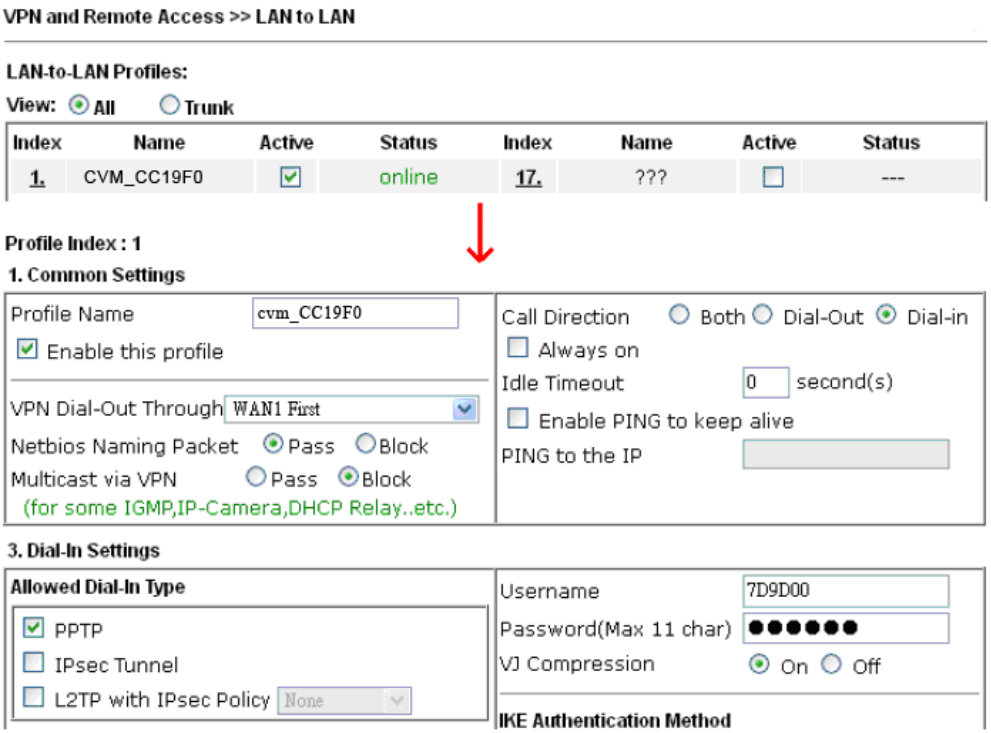
4. 確認對話框將會出現，請按下 **OK** 並耐心等候。



5. 如果 VPN 連線建立成功，相關資訊將會顯示在畫面下方的**已連接裝置**區域。



6. 現在針對此 VPN，系統已經自動產生一組 LAN to LAN 設定檔，您可以進入遠端設備的 **VPN and Remote Access>>LAN to LAN** 頁面檢視詳細的內容。



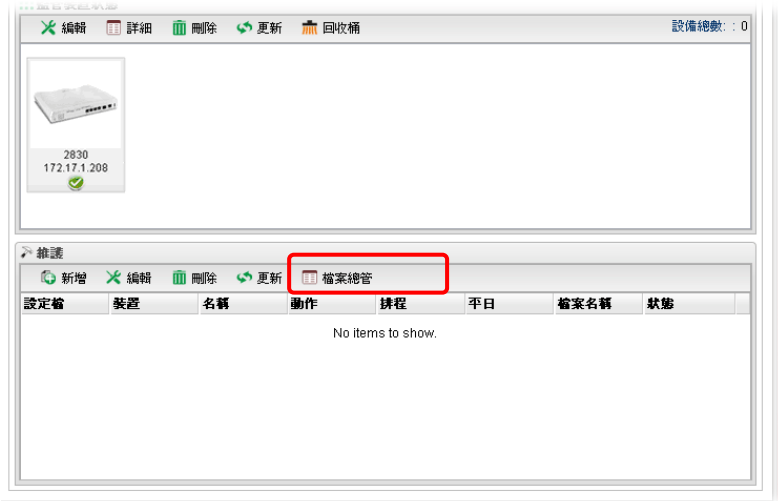
注意：設定檔是由系統自動產生，請勿任意修正內容以免造成 VPN 連線錯誤。

3.6 CVM 應用 – 如何透過 Vigor2960 更新遠端 CPE 韌體?

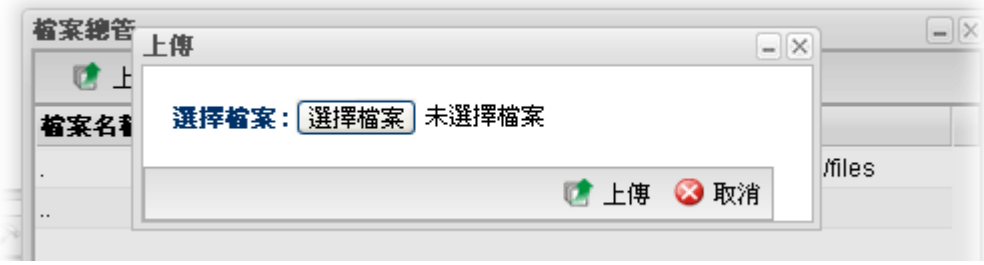
3.6.1 韌體檔案自電腦輸入至 Vigor2960 中

1. 假設最新的韌體檔案已經存放在電腦中，您可以將其上傳至 Vigor2960 上。
2. 登入 Vigor2960 的網頁使用者設定介面。
3. 開啓**系統維護>>連線控制**，**Web 允許**項目點選**啓用**並輸入 **Web 埠號**所需的埠號值，接著按下**套用**儲存設定。

4. 開啓 **VPN 中央管理>>CPE 管理**，按下 **VPN 管理**。在**維護**區域中，按下**檔案總管**。



5. 在**檔案總管**對話盒中，按下**上傳**。
6. 在 Upload 對話盒中，按下**選擇檔案**按鈕並找到您想要從電腦上傳到 Vigor2960 的韌體(例如本範例選擇的是 2830_0508)，然候按下**上傳**。

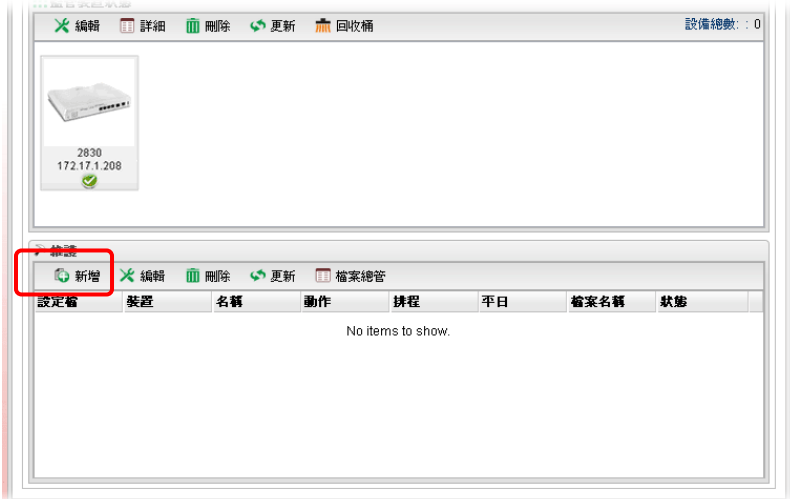


7. 當檔案上傳成功，不久，您就可以在**檔案總管**對話盒中看見該檔案。

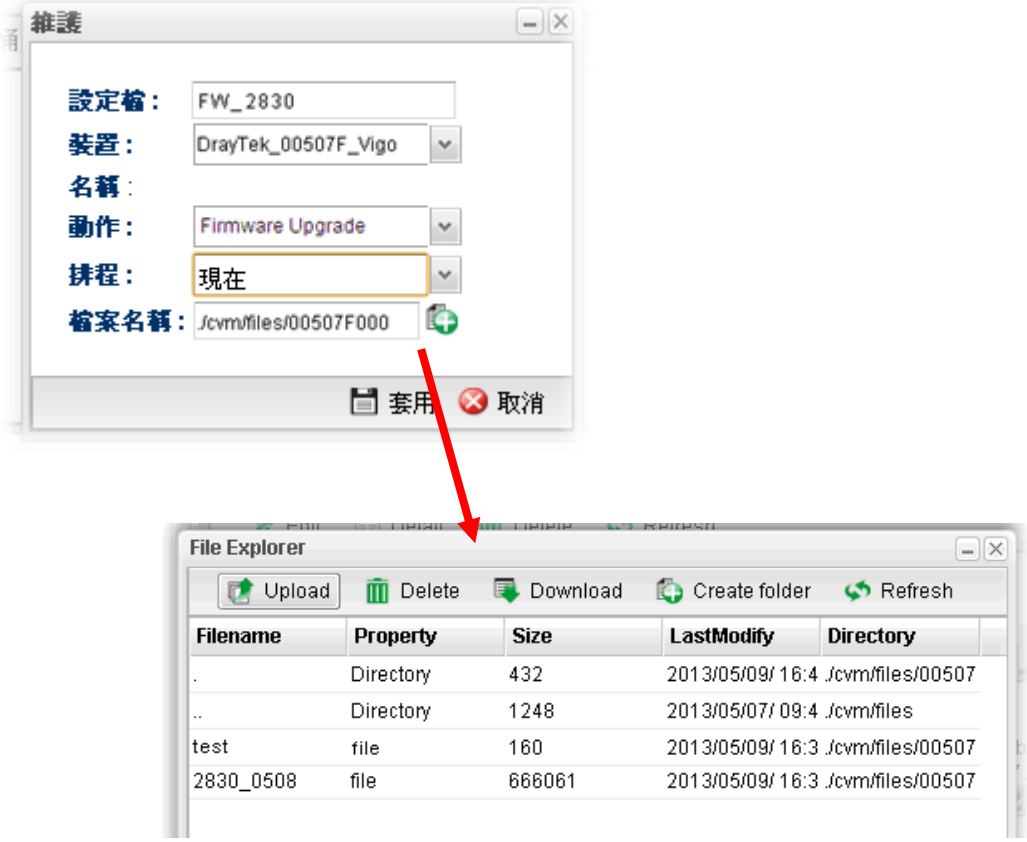
3.6.2 建立一組新的韌體更新設定檔

建立一組新的韌體更新設定檔，至少要有一台 CPE(例如本例的 Vigor2830)在 Vigor2960 的管理下，否則您無法成功建立韌體更新設定檔。

1. 開啓 **VPN 中央管理>>CPE 管理**，按下 **VPN 管理**，在**維護**區域中，按下**新增**。



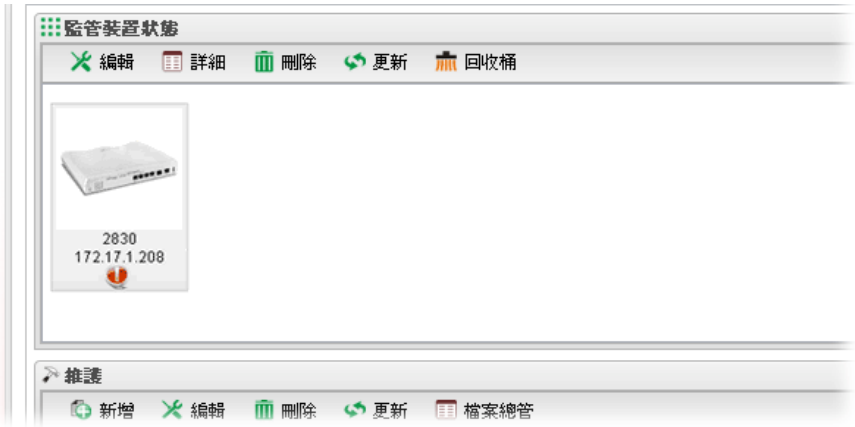
2. 在下述的對話盒中，輸入新設定檔的檔名；指定檔案預備套用的 Vigor 路由器；**動作**項目選擇 **Firmware Upgrade**；**排程**項目選擇**現在**(表示韌體更新將在按下套用按鈕後立刻進行)；輸入韌體檔名字串或是按下 選擇正確的檔名。



3. 當您完成上述設定後，按下**套用**儲存設定。新維修設定檔已經成功建立並顯示在維護區域中。

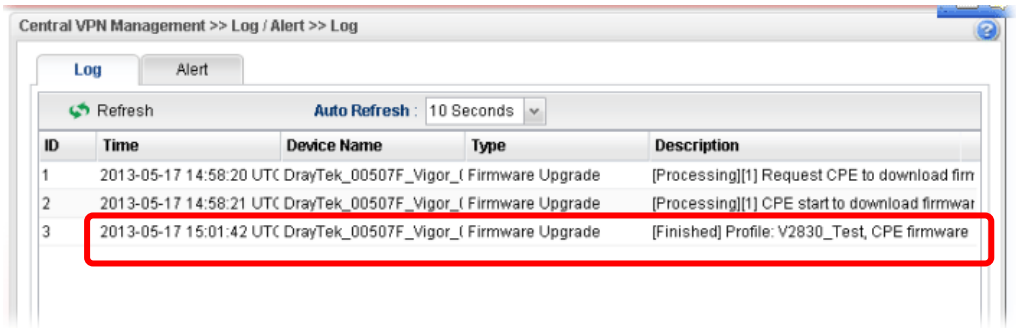
4. 現在新韌體將會立刻載入 CPE(基於剛剛的排程設定選項→現在)。

請注意在韌體更新期間，紅色圖示 將會出現在畫面上。



在 CPE 端的網頁設定介面上，系統將會顯示出韌體更新進行中的訊息。

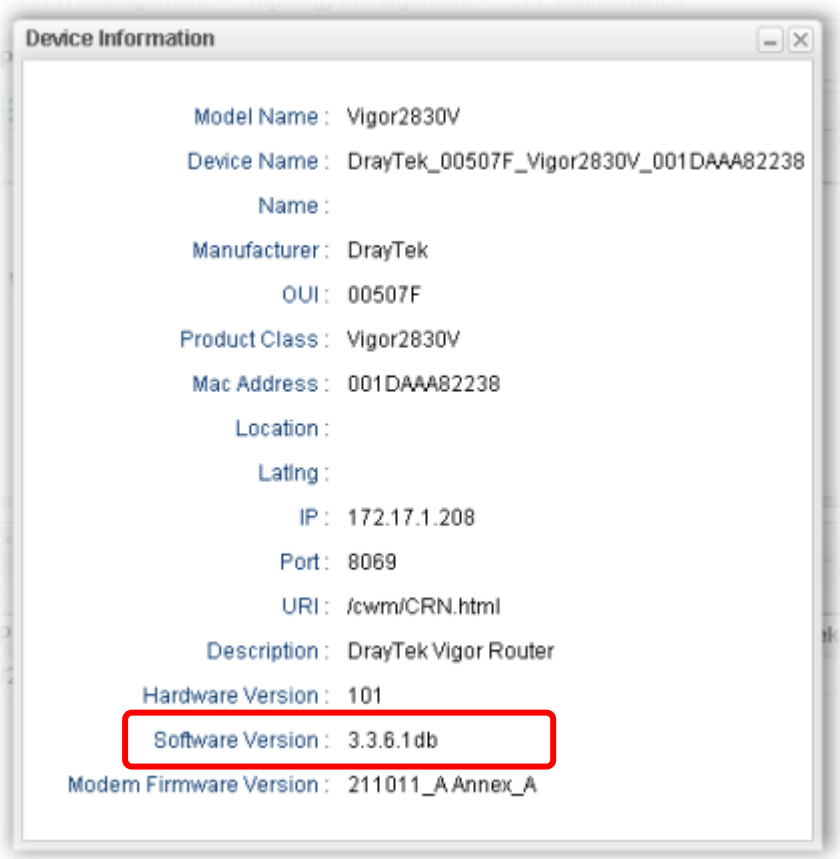
5. 請耐心等待。之後，開啓 **VPN 中央管理>>日誌/警告**中的**日誌**頁面檢查更新結果，如果畫面顯示[Finished]即表示指定的 CPE 韌體更新已經完成。



3.6.3 檢查裝置設備資訊

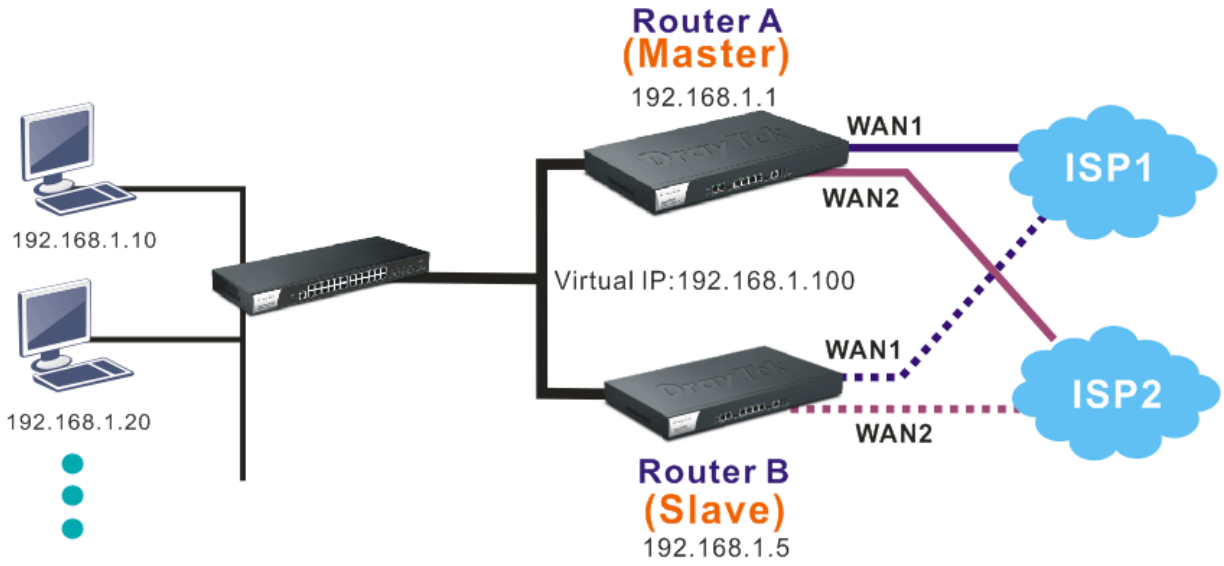
1. 開啓 **VPN 中央管理>>拓墣管理**，在**監管裝置狀態**區域中，選擇表示 Vigor2830 的路由器圖示並按下**詳細**。

2. 檢查軟體版本。


Device Information
Model Name : Vigor2830V
Device Name : DrayTek_00507F_Vigor2830V_001DAAA82238
Name :
Manufacturer : DrayTek
OUI : 00507F
Product Class : Vigor2830V
Mac Address : 001DAAA82238
Location :
Lating :
IP : 172.17.1.208
Port : 8069
URI : /cwm/CRN.html
Description : DrayTek Vigor Router
Hardware Version : 101
Software Version : 3.3.6.1db
Modem Firmware Version : 211011_A Annex_A

3.7 如何運用 Vigor2960 的高可靠度(High Availability)功能?

Vigor2960 的高可靠度(High Availability 簡稱 HA)功能可保障組織業務的持續性，IT 人員可以使用 HA 作爲災難恢復的簡易解決方案。Vigor2960 利用 Common Address Redundancy Protocol (CARP)來避免系統因停止運作造成整個公司組織相當可觀的損失。



當 HA 功能啓用時，網路管理者可以設定其他的 Vigor2960 做爲備援裝置，如此一來在主要裝置 Vigor2960 停止運作期間，由備援裝置傳送完整的路由服務。網路管理者可以在主要與備援裝置使用相同的虛擬 IP(例如 192.168.1.100)，在系統上線的時候，主要裝置(例如 192.168.1.1)可透過虛擬 IP 來提供服務，一旦主要裝置暫時無法使用時，備援裝置(例如 192.168.1.5)立即接管虛擬 IP 所提供的服務並供應所有的路由功能。

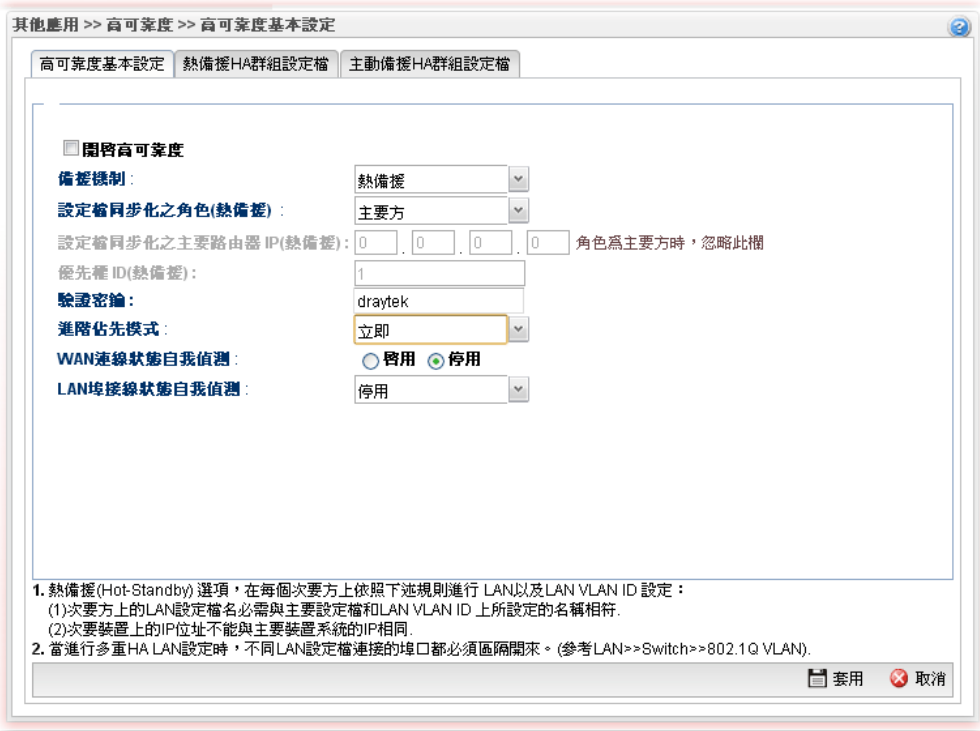
注意 ： 務必確認路由器 A 與路由器 B 的 WAN 介面已經連接妥當，二台路由器都必須能夠登入網際網路。

注意 ： 有關更多應用資訊，請造訪居易網站 www.draytek.com 參考 FAQ/Application Notes 相關內容。

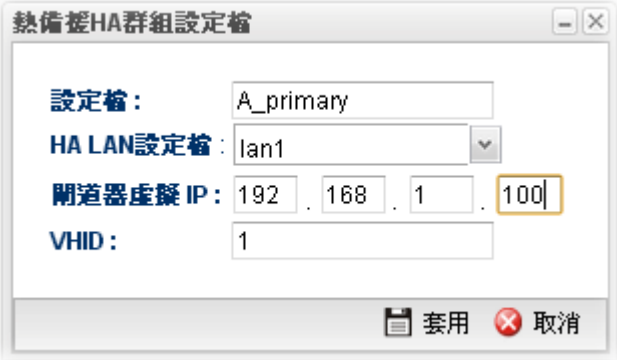
路由器 A 部分

1. 登入 Vigor2960 的網頁使用者設定介面。
2. 開啓**其他應用**>>**高可靠度**。

3. 在**高可靠度基本設定**標籤中，選擇**熱備援(Hot-Standby)**作爲備援機制，選擇**主要方**作爲**設定檔同步化之角色**；輸入 **draytek** 作爲驗證密鑰；選擇**立即**作爲**進階佔先模式**。然後按下**套用**儲存設定。



4. 按下**熱備援 HA 群組設定檔**標籤建立 HA 設定檔，接著按下**新增**。
5. 參考下述內容建立一個 HA 設定檔。按下**套用**儲存。

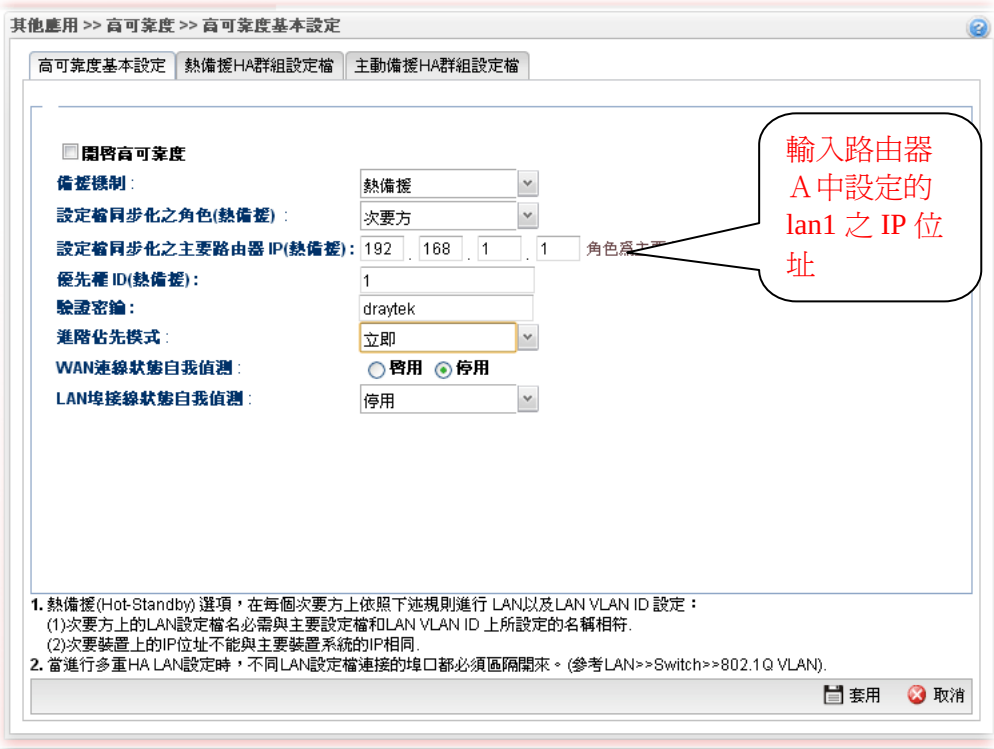


6. 現在路由器 A 的相關設定已經完成。

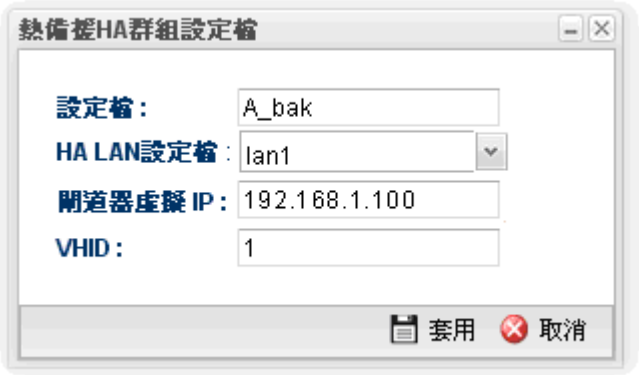
路由器 B 部分

1. 登入 Vigor2960 的網頁使用者設定介面。
2. 開啓**其他應用**>>**高可靠度**。

3. 在**高可靠度基本設定**標籤中，選擇**熱備援(Hot-Standby)**作爲備援機制，選擇**次要方**作爲**設定檔同步化之角色**；輸入路由器 A 中 lan1 的 IP 位址；輸入 **draytek** 作爲驗證密鑰；選擇**立即**作爲**進階佔先模式**。然後按下**套用**儲存設定。



4. 按下**熱備援 HA 群組設定檔**標籤建立 HA 設定檔，接著按下**新增**。
5. 參考下述內容建立一個 HA 設定檔。按下**套用**儲存。



6. 現在路由器 B 的相關設定已經完成。

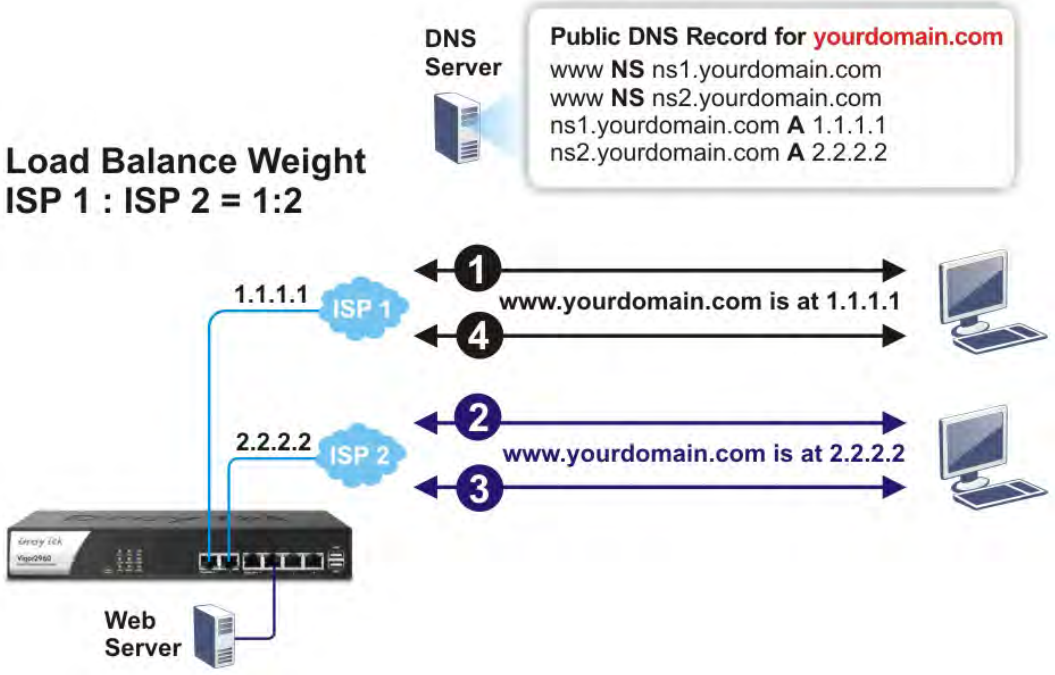
完成上述設定之後，即可啓用路由器 A 與路由器 B 的 HA 功能。**建議您先啓用路由器 A(主要)的 HA 功能，再啓用路由器 B(次要)的 HA 功能。**

- 開啓**其他應用>>高可靠度**並按下**高可靠度基本設定**標籤，勾選**開啓高可靠度**接著按下**套用**儲存設定。

在這樣的結構之下，當路由器 A(定義爲主要裝置) 斷電時，路由器 B (定義爲備援裝置) 將立即上線並接管路由器 A 的所有作業，之後一旦路由器 A 再次上線，所有的工作也將轉回路由器 A。

3.8 如何設定 Vigor2960 中 DNS Inbound 負載平衡?

Vigor2960 可提供對應的 IP 位址以回應來自遠端透過指定網域的 DNS 查詢，減少網路流量負載。



上圖中

WAN1 IP 位址: 1.1.1.1

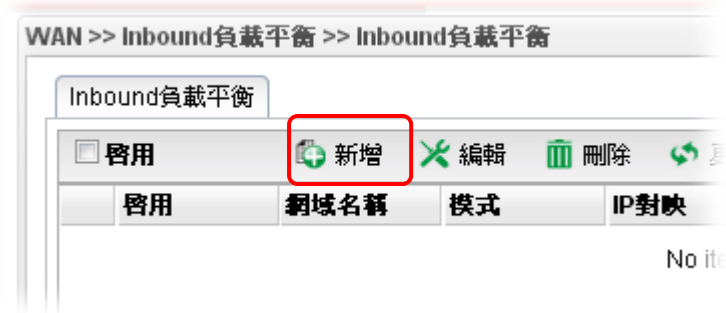
WAN2 IP 位址: 2.2.2.2

Inbound Load Balance 負載平衡讓 Vigor2960 有如 DNS 伺服器運作，將每個 WAN 介面的流量依照 DNS 查詢次數分隔開來，請依照下述步驟進行 DNS Inbound 負載平衡設定。

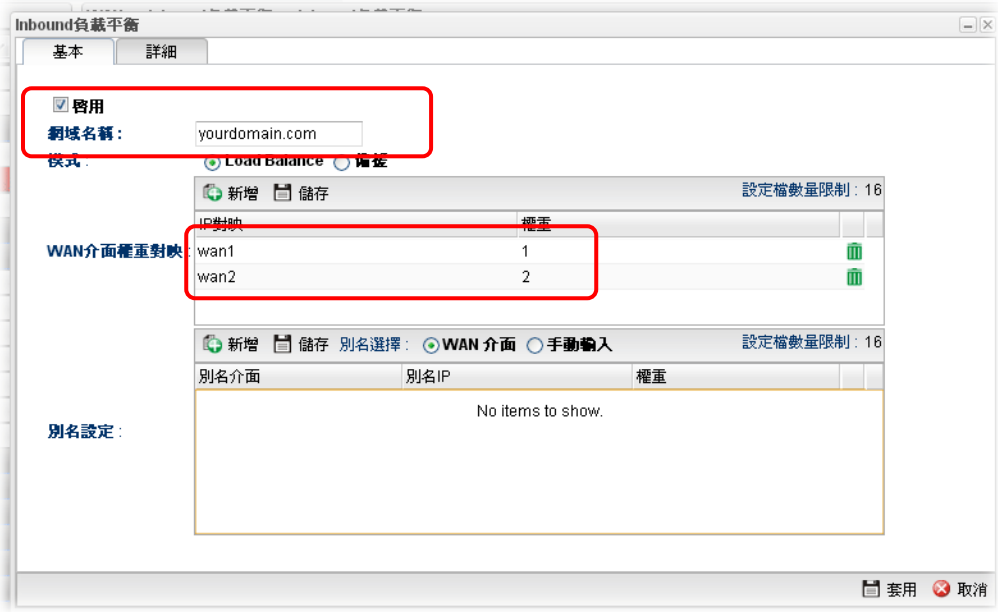
啓用路由器的網頁服務功能

1. 開啓 **NAT >> 通訊埠重導向**頁面，依照下述內容設定網頁伺服器所需的通訊埠重導向規則，再按下**套用**儲存設定。

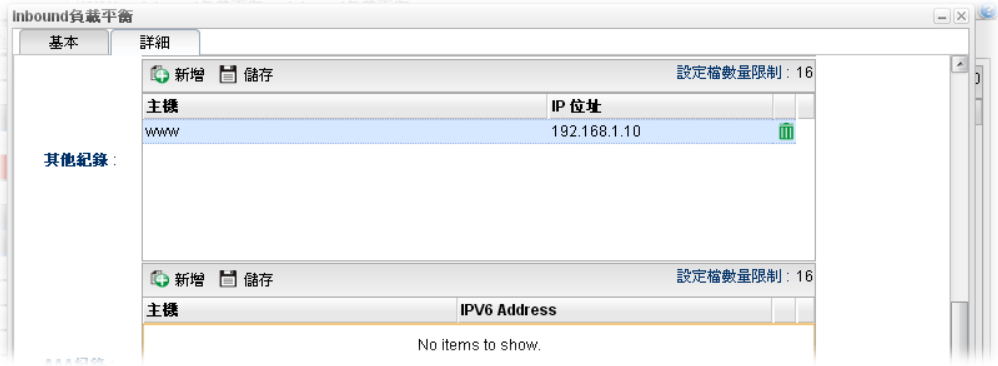
2. 開啓 **WAN >> Inbound 負載平衡**，再按下**新增**。



3. 新增一個設定檔，命名爲“yourdomain.com”，分別定義 WAN1 權重爲 1 與 WAN2 權重爲 2，此表示全部的 DNS 查詢次數爲三次，其中 1 次查訊透過 WAN1 進行，2 次查詢透過 WAN2 進行。



4. 按下**詳細**標籤並在**其他記錄**項目中，**主機**欄位輸入“www”，**IP 位址**欄位輸入“192.168.1.10”。



5. 按下**套用**儲存設定。

現在，先進行一個簡單的 inbound 負載平衡測試：

按下 **Start>> Run** 並輸入 **cmd**，執行 nslookup 命令進行 DNS 查詢測試。

第一個 DNS 查詢，畫面顯示如下

```
>www.yourdomain.com
Server: [google-public-dns-a.google.com]
Address: 8.8.8.8
Name: www. yourdomain.com
Address: 1.1.1.1
```

第二個 DNS 查詢，畫面顯示如下

```
> www.yourdomain.com
Server: [google-public-dns-a.google.com]
Address: 8.8.8.8
```

Name: www.yourdomain.com
Address: 2.2.2.2

第三個 DNS 查詢，畫面顯示如下

> www.yourdomain.com
Server: [google-public-dns-a.google.com]
Address: 8.8.8.8
Name: www.yourdomain.com
Address: 2.2.2.2

注意：建議您再執行“nslookup” DNS 查詢前，先將快取(cache)資料清除乾淨。

本頁留白

第四章: 進階設定

完成路由器基本設定之後，您可以輕鬆瀏覽網際網路。對於需要設定更進階的功能的使用者，可參考本章取得更多資訊。特殊應用與練習，可參考第三章。

4.1 WAN 設定

快速安裝精靈提供使用者一個簡單的方法，以便能快速設定路由器的連線模式。如果您想要針對不同廣域網路模式調整更多的設定，請開啓 **WAN** 群組然後選擇**基本設定**。

IP 網路的基本概念

IP 表示網際網路通訊協定，在以 IP 爲主的網路像是路由器、列印伺服器和主機電腦的每一種裝置，都需要一組 IP 位元址作爲網路上身分辨識之用。爲了避免位址產生衝突，IP 位址都必須於網路資訊中心(NIC) 公開註冊，擁有個別 IP 位址對那些於真實網路分享的裝置是非常必要的，但在虛擬網路上像是路由器所掌管下的主機電腦就不是如此，因爲它們不需要讓外人從真實地區進入存取資料。因此 NIC 保留一些永遠不被註冊的特定位址，這些被稱之爲虛擬 IP 位址，範圍條列如下：

從 10.0.0.0 到 10.255.255.255
從 172.16.0.0 到 172.31.255.255
從 192.168.0.0 到 192.168.255.255

什麼是真實 IP 位址和虛擬 IP 位址

由於路由器扮演著管理及保護其區域網路的角色，因此它可讓主機群間互相聯繫。每台主機都有虛擬 IP 位址，是由路由器的 DHCP 伺服器所指派，路由器本身也會使用預設之虛擬 IP 位址 192.168.1.1 與本地主機達成聯繫目的，同時，Vigor 路由器可藉由真實 IP 位址與其他的網路裝置溝通連接。當資料經過時，路由器的網路位址轉換(NAT)功能將會在真實與虛擬位址間執行轉換動作，封包將可傳送至本地網路中正確的主機電腦上，如此一來，所有的主機電腦就都可以共用一個共同的網際網路連線。

取得 ISP 提供的真實 IP 位址

在 ADSL 之部署中，PPP (Point to Point)型態之驗證和授權是橋接用戶前端設備所需要的。PPPoE (Point to Point Protocol over Ethernet)透過一台存取裝置連接網路主機至遠端存取集中器，此種應用讓使用者覺得操作路由器是很簡單的，同時也可依照使用者的需要提供存取控制及服務類型。

當路由器開始連接至 ISP 時，路由器將執行一系列過程以尋求連線，然後即可產生一個連線數，您的使用者辨識名稱和密碼由 **RADIUS** 驗證系統的 **PAP** 或 **CHAP** 來驗證，通常您的 IP 位址、DNS 伺服器和其他相關資訊都是由 ISP 指派的。

下圖爲 WAN 的功能項目：

4.1.1 基本設定

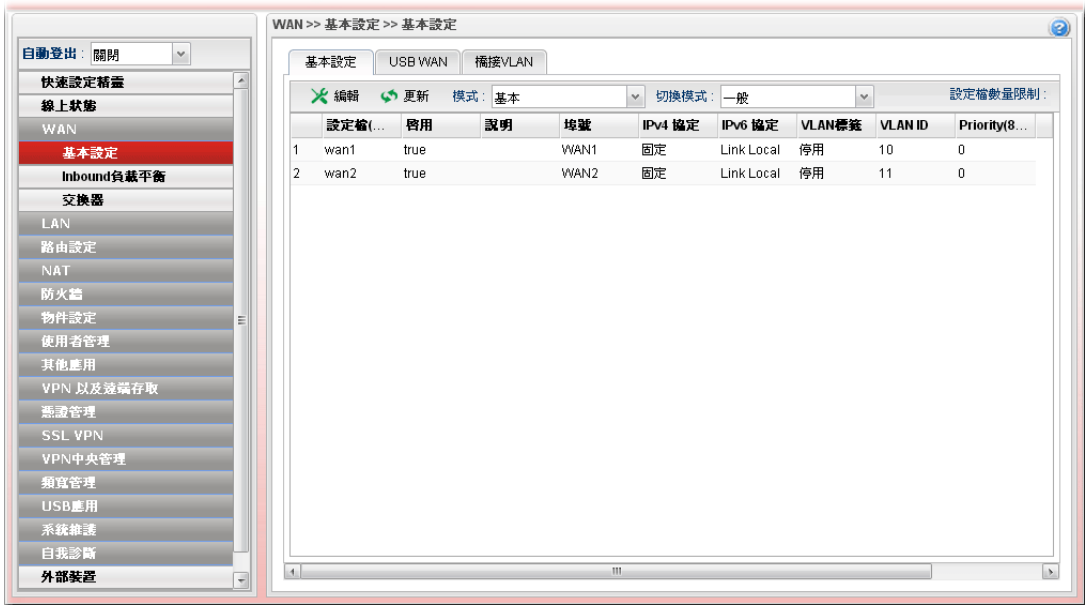
本節介紹數種網際網路的一般設定，並詳細說明各個 WAN 介面。

路由器支援多 WAN 口功能，可讓使用者存取網際網路並整合 WAN 口頻寬以加速網路資料傳輸。每個 WAN 連接埠可以連接到不同的 ISP，即使 ISP 使用不同的技術提供不同的電信服務(如 DSL, Cable 數據機等等)也都沒有問題。如果任何一個 ISP 連線出了問題，全部的傳輸動作都將引導並切換至正常的 WAN 口連接埠並繼續運行。

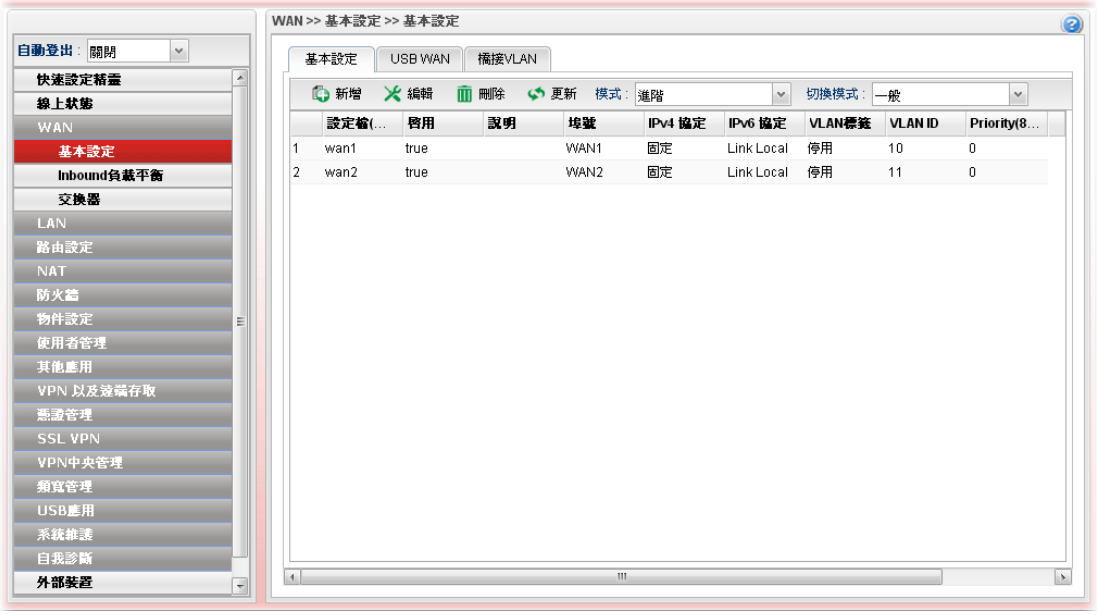
系統提供您二種模式設定 WAN 設定檔，**基本**模式讓您檢視並編輯現有的 WAN 設定檔，而**進階**模式可讓您定義(新增)新的 WAN 設定檔。

當您從**進階**切換到**基本**或是由**基本**切換到**進階**，系統都會要求您重新登入使用者網頁設定介面，以便讓參數生效。

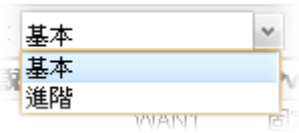
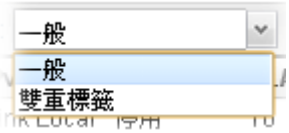
基本模式下的頁面



進階模式下的頁面



每個項目說明如下：

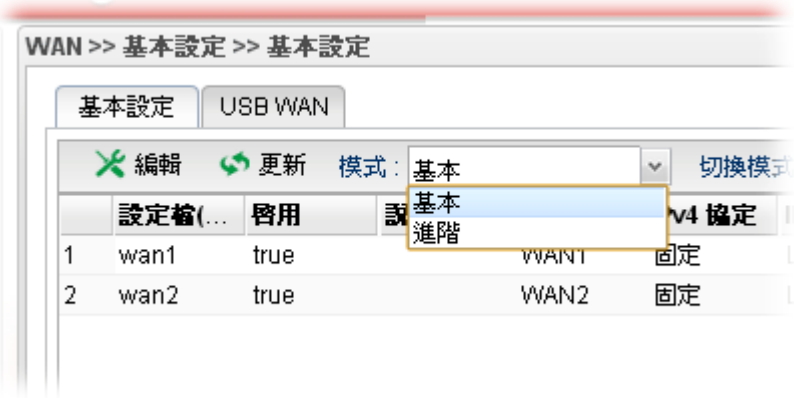
項目	說明
新增	新增一個 WAN 設定檔，這個功能只有在 Advance 模式下可用。
編輯	修改選定的 WAN 設定檔。 先選擇您想要修改的設定檔，再按下**編輯**按鈕，編輯視窗隨即出現讓您修改與該規則設定檔有關的各式設定。
刪除	移除選定的 WAN 設定檔，這個功能只有在 Advance 模式下可用。 先選擇您想刪除的設定檔，再按下刪除按鈕即可刪除。
頁面更新	重新更新本頁面。
模式	指定模式以便新增(選**進階**)WAN 設定檔或是編輯(選**基本**)既有的 WAN 設定檔。 
切換模式	這個模式決定 WAN 介面具有單一或是雙重 VLAN ID 值。  **一般** – 表示此 WAN 界面設定檔可以設定一組 VLAN ID 值。 **雙重標籤** – 表示此 WAN 界面設定檔可以設定二組 VLAN ID 值(802.1q in q)。

設定檔數量限制	顯示可以建立的設定檔的最高數目(50)。
設定檔(最大長度限制:7)	顯示設定檔名。
啓用	顯示設定檔狀態，False 表示停用；True 表示啓用。
說明	顯示該設定檔的簡易說明。
VLAN 標籤	顯示標籤功能是否啓用。 如果資料傳輸帶有標籤，本區會顯示**啓用**，若未帶標籤則顯示**停用**。
VLAN ID	顯示設定檔的 VLAN ID 。
優先權	顯示設定檔的優先權等級。
埠口	顯示設定檔的實體 WAN 介面。
IPv4 協定類型	顯示設定檔使用的 IPv4 協定。
IPv6 協定類型	顯示設定檔使用的 IPv6 協定。

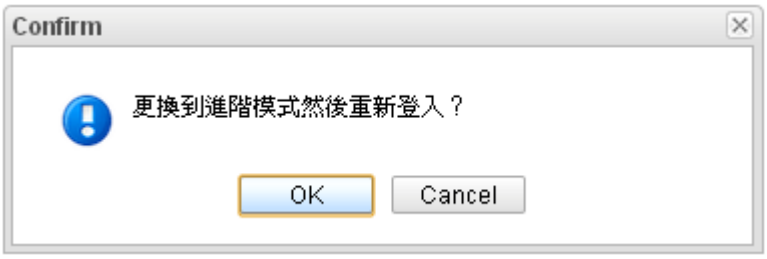
4.1.1.1 乙太網路 WAN 設定檔

如何新增一個 WAN 設定檔：

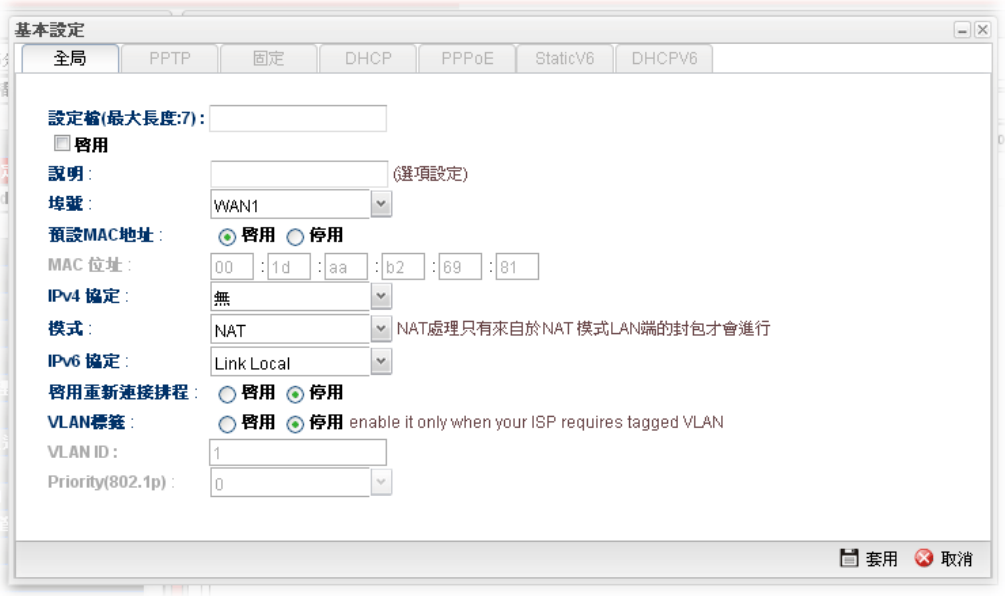
1. 如果路由器在 **Basic** 模式下，您必須先切換到**進階**模式，如果已經在**進階**模式，可忽略此步驟直接進到步驟 4。



2. 確認對話盒將會出現，請按下 **OK** 儲存套用新設定，系統會要求重新登入。

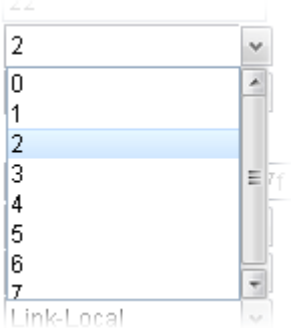


3. 重新登入網頁設定介面。
4. 開啓 **WAN>>基本設定**，按下**新增**按鈕開啓如下對話盒，不同協定類型會帶出不同的設定頁面。



可用參數詳列如下：

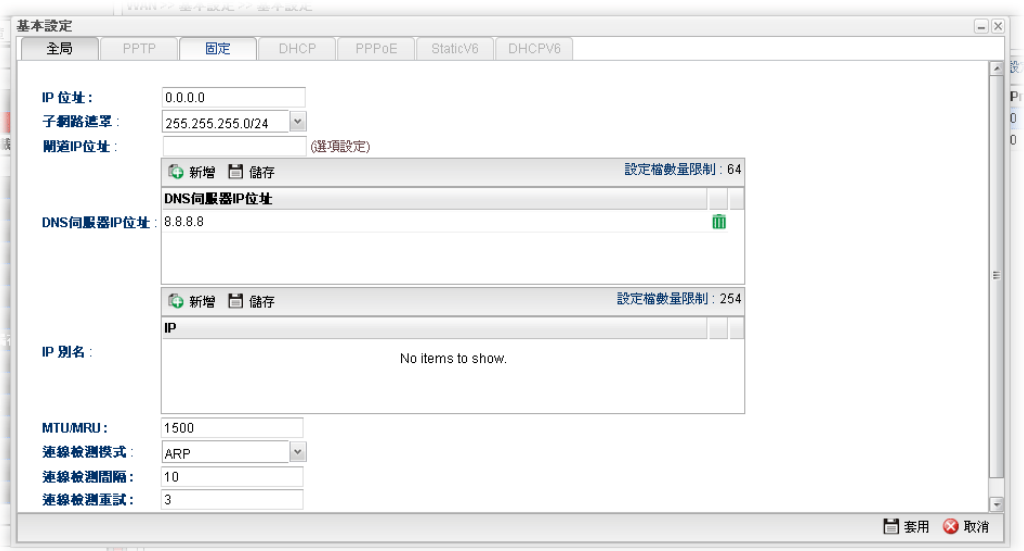
項目	說明
設定檔(最大長度:7)	輸入設定檔的檔名(勿超過 7 個字元)。
啓用	勾選此方框啓用此設定檔。
說明	輸入與此設定檔相關的簡易說明。
埠號	選擇此設定檔所需的實體 WAN 介面。 WAN1 WAN1 WAN2
預設 MAC 位址	**啓用** – 按此可以啓用預設的 MAC 位址。 **停用** – 按此之後須手動輸入 MAC 位址。 **MAC 位址** – 您若選擇停用，則須在此欄位輸入 MAC 位址。系統的預設值是啓用的。
IPv4 協定	有數種連線模式提供給您，每種模式的頁面設定皆有所不同。 無 固定 DHCP PPPoE PPTP
模式	決定此設定檔採用 NAT 或是路由模式來進行。 ROUTING NAT ROUTING
IPv6 協定	有數種模式可供您選擇，每種模式皆有不同的設定頁面。

啓用重新連接排程	啓用– 按此啓用自動重新連線功能。 ● **選擇時間物件設定檔** – 選擇時間物件套用於此 WAN 設定。 停用 – 按此停止排程重新連線功能。
VLAN 標籤	選擇**啓用**即可針對通過此介面的封包加入標籤號碼。 選擇**停用**則不需給封包加入任何標籤。
VLAN ID	輸入 VLAN ID 號碼，凡是通過套用此設定檔的 WAN 介面之封包都會被帶入此標籤。
優先權(802.1p)	指定此 VLAN 的封包優先權，範圍從 0 到 7。 
套用	按此儲存設定並離開對話盒。
取消	按此離開對話盒，不儲存任何設定。

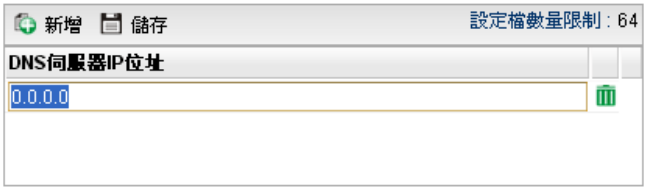
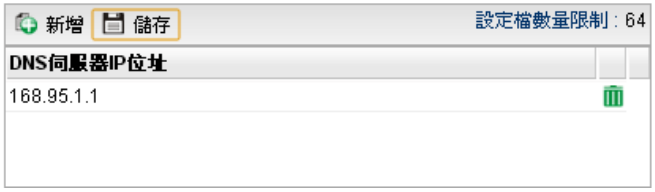
全域設定讓您啓用設定檔，提供簡易說明，指定 VLAN ID，指定 MAC 位址，選擇 IPv4 與 IPv6 協定，並指定資料傳輸的模式(**NAT** 或是**路由**)。

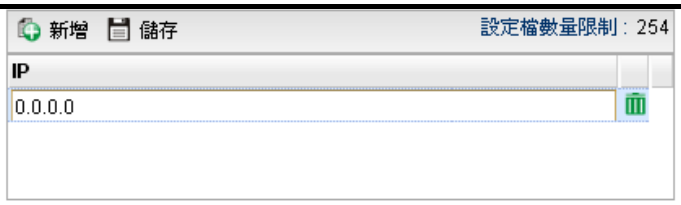
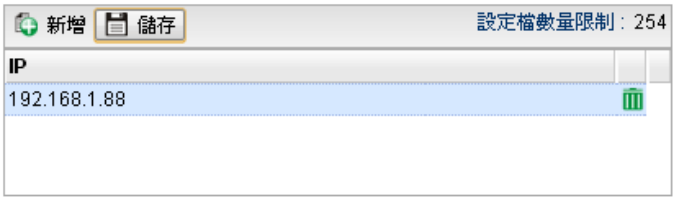
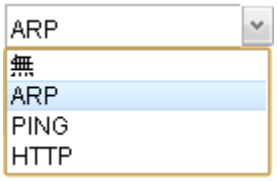
不同的 IPv4 與 IPv6 協定會帶來不同的網頁設定。

- ***如果您選擇固定爲 IPv4 協定類型，請按下固定標籤開啓如下頁面：***

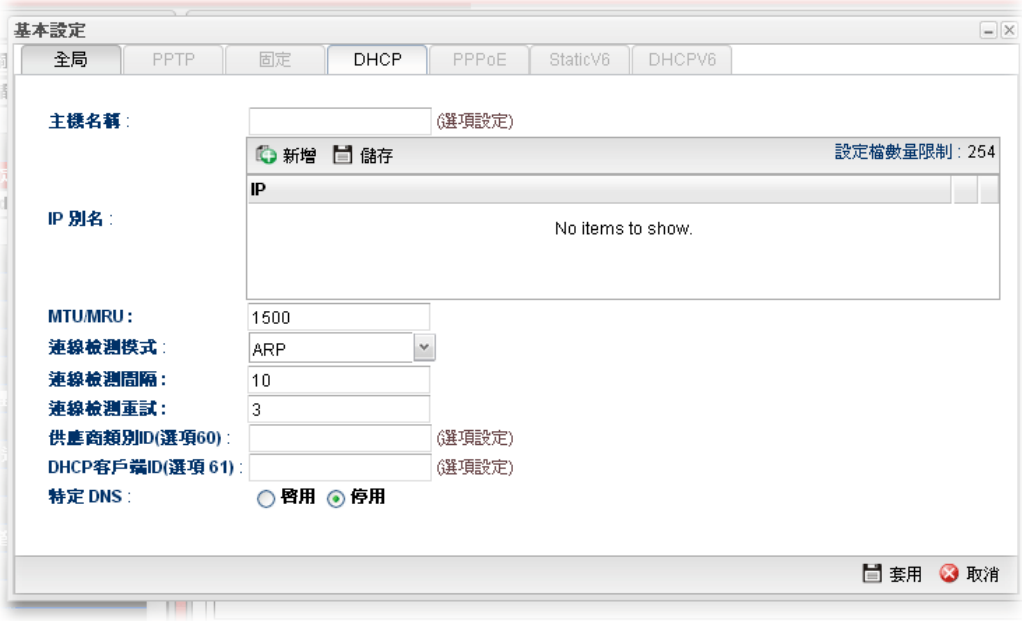


可用參數詳列如下：

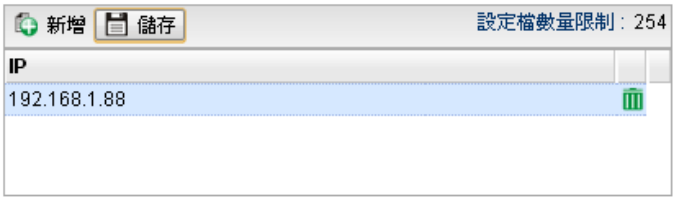
項目	說明
IP 位址	輸入此設定檔所需的 IP 位址(例如 192.168.1.x)。
子網路遮罩	使用下拉式清單選擇適當的子網路遮罩。
閘道 IP 位址	輸入閘道 IP 位址。
DNS 伺服器 IP 位址	輸入真實 IP 位址作爲主要的 DNS(Domain Name Server)伺服器。  **新增** – 按此顯示 IP 位址區域以便輸入新的 IP 位址。 **儲存** – 按此儲存 IP 位址設定。 
IP 別名	輸入其他的 IP 位址綁定在此介面上，這項設定是選擇性的，如果您在此輸入位址，您在稍後其他的設定頁面也能見到並能選擇使用（例如 **NAT>>Port Redirection/DMZ Host**）。 **新增** – 按此顯示 IP 位址新增方塊，請分別輸入內容。

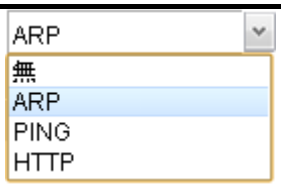
	 **新增** – 按此顯示 IP 位址新增方塊，請分別輸入內容。 **儲存** – 按此儲存設定。 
MTU/MRU	輸入 MTU/MRU 值，預設值為 1500。
連線檢測模式	選擇此 WAN 介面需要的偵測模式，有三種方式 **ARP, PING** 與 **HTTP** 可以挑選。 
連線檢測主機	指定 IP 位址或是網域名稱以檢測主機(傳送回應給路由器)是否仍運作，如果不再運作，WAN 介面連線就會被視為斷線，這個功能僅在連線檢測模式設定為 PING 或是 HTTP 時才有作用。 **新增** – 按下此鈕顯示新增 IP 位址方塊，以便輸入您需要設定的 IP 位址。 **儲存** – 按下此鈕儲存設定。
連線檢測間隔	指定每次偵測的時間間間隔。
連線檢測重試	指定檢測次數，經過您所設定的時間之後，WAN 連線介面將被自動斷線。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕取消設定值並離開此對話盒。

- *如果您選擇 DHCP 作爲 IPv4 協定，可按 DHCP 標籤開啓下述頁面：*



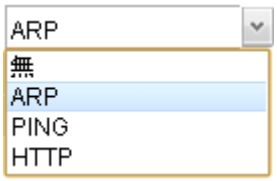
可用參數詳列如下：

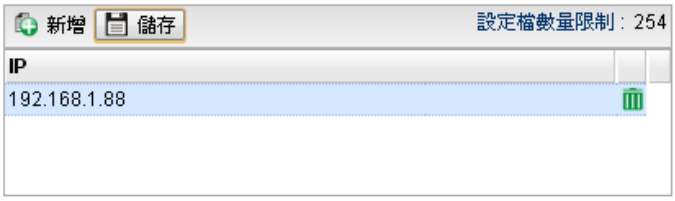
項目	說明
主機名稱 (選項設定)	輸入辨識用的名稱做爲主機名稱。
IP 別名	輸入與此介面綁定的 IP 位址，此設定是選項設定，如果您在此輸入位址，您可以看見並在稍後的頁面設定(例如 **NAT>>埠號重新導向/DMZ 主機**)中選擇這裡所設定的內容。 如欲新增 IP 位址，按下**新增**，輸入 IP 位址並使用選項清單指定子網遮罩，接著按下**儲存**，新 IP 位址即可加入並顯示在方塊下方的區域中。  **新增** – 按此鈕以便輸入新的位址。 **儲存** – 按此鈕儲存設定。
MTU/MRU	表示封包的最大傳輸單元，預設值爲 1500。
連線檢測模式	選擇一種檢測模式，系統提供三種方法 ARP、PING 以及 HTTP 讓您選擇外送需要的資料。

	
連線檢測主機	指定 IP 位址或是網域名稱以檢測主機(傳送回應給路由器)是否仍運作，如果不再運作，WAN 介面連線就會被視爲斷線，這個功能僅在連線檢測模式設定爲 PING 或是 HTTP 時才有作用。 **新增** – 按此鈕以便輸入新的位址。 **儲存** – 按下此鈕儲存設定。
連線檢測間隔	指定每次檢測需要的時間間隔。
連線檢測次數	指定檢測時間確保 WAN 介面的連線狀態，經過您在此所設定的檢測次數之後，路由器並未收到任何回應，WAN 介面連線將被視爲連線中斷。
供應商類別 ID (選項 60)	用於辨識供應商的類型以及 DHCP 用戶端設定。
DHCP 用戶端 ID (選項 61)	用於指定 DHCP 用戶端辨識器，讓 DHCP 得以找出主機。 某些 ISP 需要指定使用者名稱與密碼。
特定 DNS	**啓用** - 按此鈕啓動指定 DNS 功能，此功能適用於本機服務(如 NTP、ping 診斷)或適用於轉送風暴至 LAN/VPN 的電腦上。 **停用** –.按此鈕關閉指定 DNS 功能。
DNS	**新增** – 按此鈕以便輸入新的位址。 **儲存** – 按下此鈕儲存設定。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

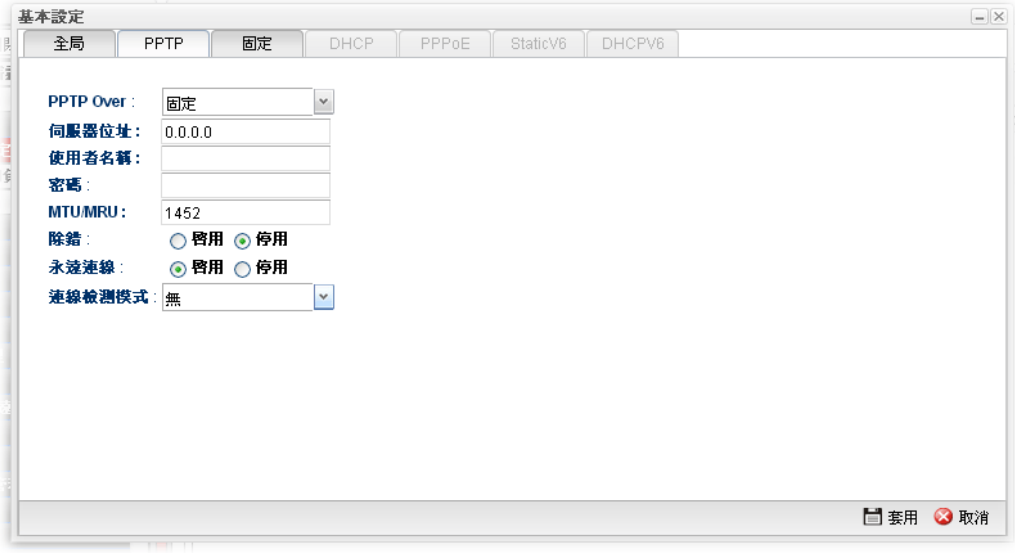
- *如果您選擇 **PPPoE** 作爲 **IPv4** 協定，可按 **PPPoE** 標籤開啓下述頁面：*

可用參數詳列如下：

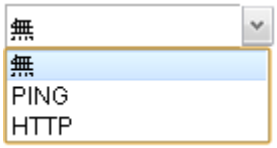
項目	說明
使用者名稱	輸入 ISP 提供的使用者名稱。
密碼	輸入 ISP 提供的密碼。
MTU/MRU	表示封包的最大傳輸單元，預設值爲 1492。
服務名稱	此爲選項設定，某些 ISP 業者會提供此類資訊並要求您在此輸入相關內容。
除錯	按下**啓用**顯示 Syslog 中的 PPPoE 除錯訊息，預設值爲**停用**。
永遠連線	按**啓用**啓動永選連線功能，路由器將一直保持網路連線。 按**停用**關閉永遠連線功能。
固定 IP	按**啓用**啓動使用固定 IP 功能。 按**停用**關閉固定 IP 使用功能。
固定 IP 位址	如果啓用了**固定 IP**，請在此輸入一組 IP 位址。
連線檢測模式	選擇一種檢測模式，系統提供三種方法 ARP、PING 以及 HTTP 讓您選擇外送需要的資料。 
連線檢測主機	指定 IP 位址或是網域名稱以檢測主機(傳送回應給路由器)是否仍運作，如果不再運作，WAN 介面連線就會被視爲斷線，這個功能僅在連線檢測模式設定爲 PING 或是 HTTP 時才有作用。

	 新增 – 按此鈕以便輸入新的位址。 **儲存** – 按下此鈕儲存設定。
連線檢測間隔	指定每次檢測需要的時間間隔。
連線檢測次數	指定檢測時間確保 WAN 介面的連線狀態，經過您在此所設定的檢測次數之後，路由器並未收到任何回應，WAN 介面連線將被視爲連線中斷。
IP 別名	輸入與此介面綁定的 IP 位址，此設定是選項設定，如果您在此輸入位址，您可以看見並在稍後的頁面設定(例如 **NAT>>埠號重新導向/DMZ 主機**)中選擇這裡所設定的內容。 如欲新增 IP 位址，按下**新增**，輸入 IP 位址並使用選項清單指定子網遮罩，接著按下**儲存**，新 IP 位址即可加入並顯示在方塊下方的區域中。  **新增** – 按此鈕以便輸入新的位址。 **儲存** – 按此鈕儲存設定。
特定 DNS	**啓用** - 按此鈕啓動指定 DNS 功能，此功能適用於本機服務(如 NTP、ping 診斷)或適用於轉送風暴至 LAN/VPN 的電腦上。 **停用** –.按此鈕關閉指定 DNS 功能。
DNS	**新增** – 按此鈕以便輸入新的位址。 **儲存** – 按下此鈕儲存設定。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

- *如果您選擇 PPTP 作爲 IPv4 協定，可按 PPTP 標籤開啓下述頁面：*



可用參數詳列如下：

項目	說明
PPTP Over	每次連線時，通常 ISP 會隨機分配 IP 位址給您， 某些情況下，ISP 業者會提供給您相同的 IP 位址以符合您的特殊需求，這時候，您必須提供固定的 IP 位址。使用此功能前，可先與 ISP 業者聯絡取得更多資訊。 選擇適當的協定**固定**或 **DHCP**。完成設定後，還需要開啓 Static 或是 DHCP 頁面進行更詳盡的設定。
伺服器位址	輸入 ISP 提供的 PPTP 之 IP 位址。
使用者名稱	輸入 ISP 提供的使用者名稱。
密碼	輸入 ISP 提供的密碼。
MTU/MRU	輸入 MTU/MRU 值，預設值爲 1452。
除錯	按下**啓用**顯示 Syslog 中的 PPPTP 除錯訊息，預設值爲**停用**。
永遠連線	按**啓用**啓動永選連線功能，路由器將一直保持網路連線。 按**停用**關閉永遠連線功能。
連線檢測模式	選擇一種檢測模式，系統提供二種方法 PING 以及 HTTP 讓您選擇外送需要的資料。 
連線檢測主機	指定 IP 位址或是網域名稱以檢測主機(傳送回應給路由器)是否仍運作，如果不再運作，WAN 介面連線就會被視爲斷線，這個功能僅在連線檢測模式設定爲 PING 或是

	HTTP 時才有作用。 **新增** – 按此鈕以便輸入新的位址。 **儲存** – 按此鈕儲存設定。
連線檢測間隔	指定每次檢測需要的時間間隔。
連線檢測重試	指定檢測時間確保 WAN 介面的連線狀態，經過您在此所設定的檢測次數之後，路由器並未收到任何回應，WAN 介面連線將被視爲連線中斷。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

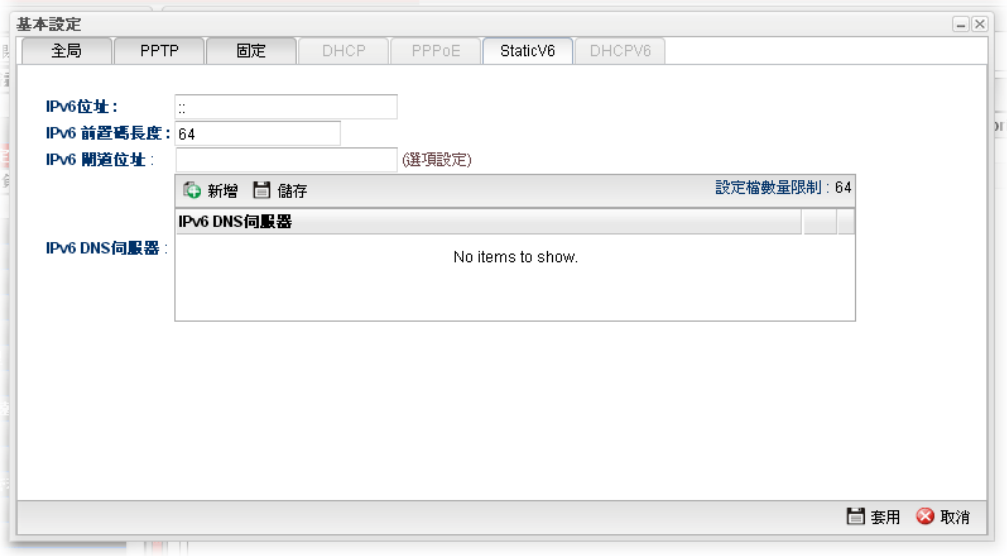
- ***如果您選擇 Link-Local 作爲 IPv6 協定***

  Link-Local 位址用於溝通相同連結下的其他鄰近節點，定義方式通常前端以 **fe80::/64** 開頭，您不需要手動設定 Link-Local 位址，因爲系統會依據您的 MAC 位址自動幫您計算並產生。

- ***如果您選擇 PPP 作爲 IPv6 協定***

  設定部份請參考*如果您選擇 PPPoE 作爲 IPv4 協定，可按 PPPoE 標籤開啓下述頁面*一節。

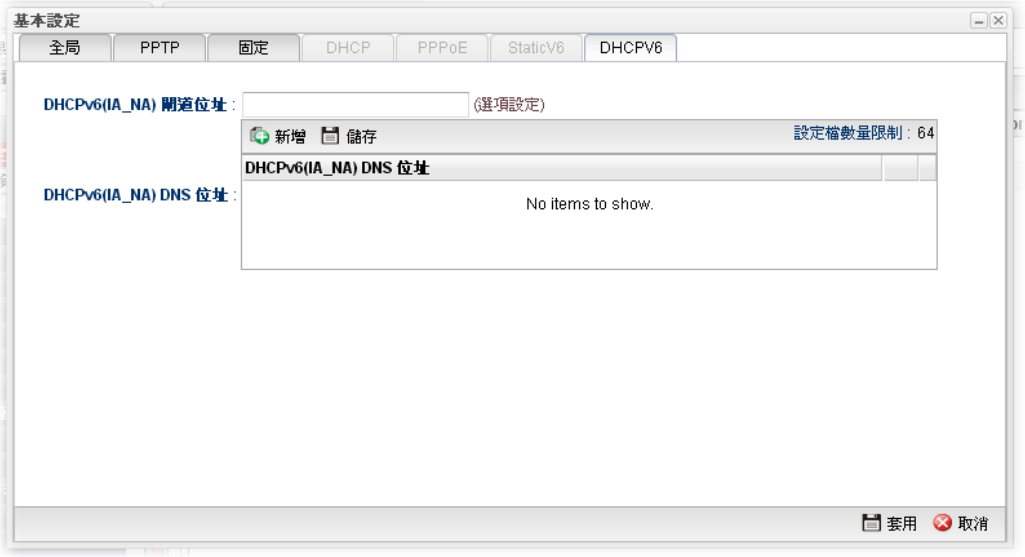
- *如果您選擇 Static 作爲 IPv6 協定，可按 StaticV6 標籤開啓下述頁面：*



可用參數詳列如下：

項目	說明
IPv6 位址	輸入此協定的 IP 位址。
IPv6 前置碼長度	輸入 IPv6 位址的前置碼長度，建議使用預設值。
IPv6 閘道位址	輸入 IPv6 閘道位址。
IPv6 DNS 伺服器	輸入 IPv6 主要 DNS 伺服器位址。 **新增** – 按此鈕以便輸入新的位址。 **儲存** – 按此鈕儲存設定。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

- *如果您選擇DHCP-IA_NA 作爲IPv6 協定，可按DHCP-IA_NA 標籤開啓下述頁面：*



可用參數詳列如下：

項目	說明
DHCP (IA_NA) 閘道位址	輸入 IPv6 DHCP IA_NA 模式所需的閘道 IP 位址。
DHCP (IA_NA) DNS 位址	**新增** – 按下此鈕輸入主要 IPv6 DNS 伺服器位址。 **儲存** – 按下此鈕儲存設定。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

- *如果您選擇 DHCP-IA_PD 作爲 IPv6 協定*

  您不需要設定任何頁面。

5. 輸入所有設定值，接著按下**套用**儲存設定。

4.1.1.2 USB WAN 設定檔

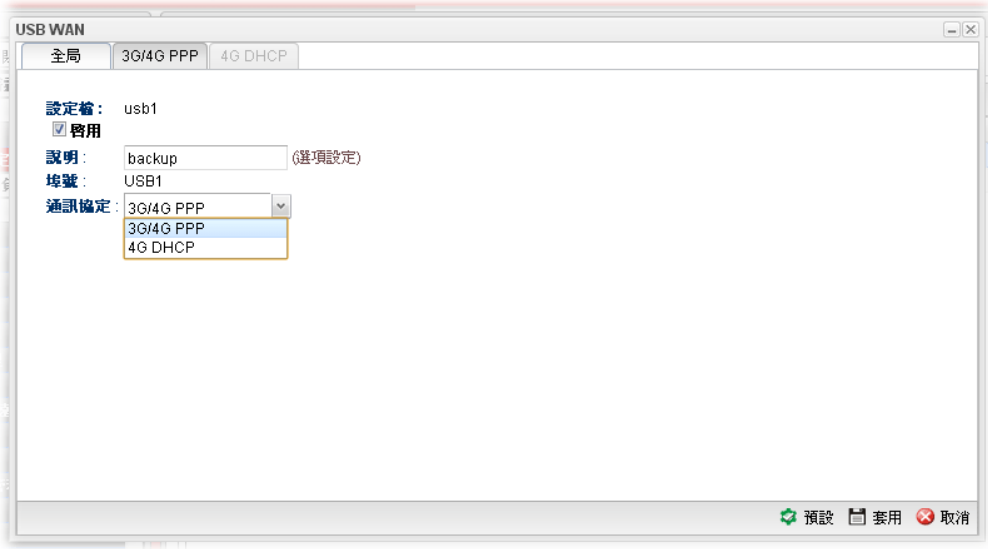
開啓 **WAN>>基本設定**再按下 **USB WAN** 標籤。

每個項目說明如下：

項目	說明
編輯	修改選定的 USB WAN 設定檔。 選擇您想要編輯的設定檔，然後按下**編輯**按鈕，編輯視窗將會出現讓您修改相應的設定。
更新	重新更新本頁面。
設定檔	顯示設定檔名稱。
啓用	顯示設定檔狀態，False 表示停用，True 表示啓用。
說明	顯示設定檔的簡易說明。
埠號	顯示設定檔的實體 WAN 介面。
通訊協定	顯示設定檔選用的協定。

如何編輯 USB WAN 設定檔

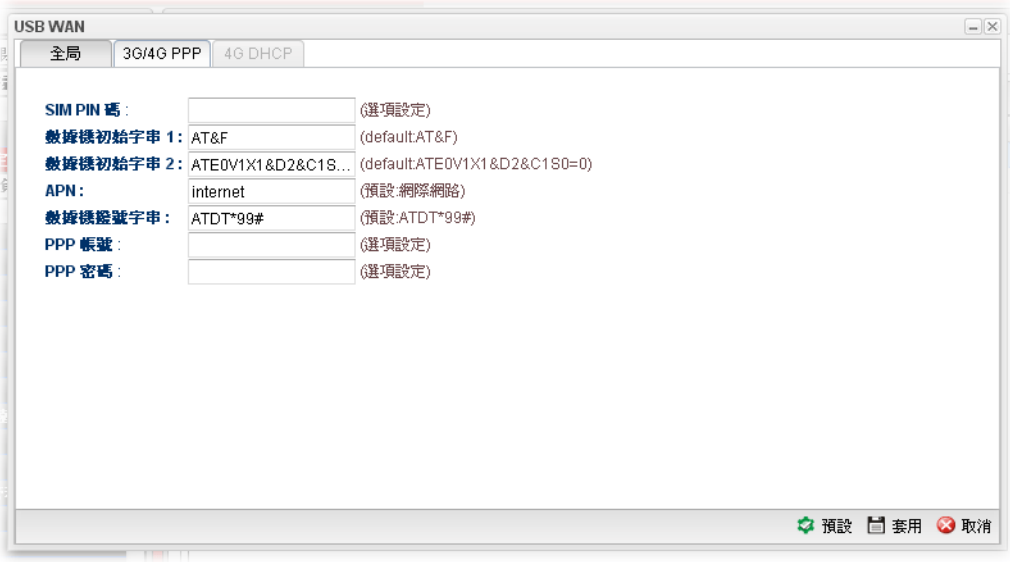
1. 請從頁面中選擇一個 USB WAN 設定檔，然後按下**編輯**按鈕。
2. **全局(Global)**標籤下方的設定顯示如下：



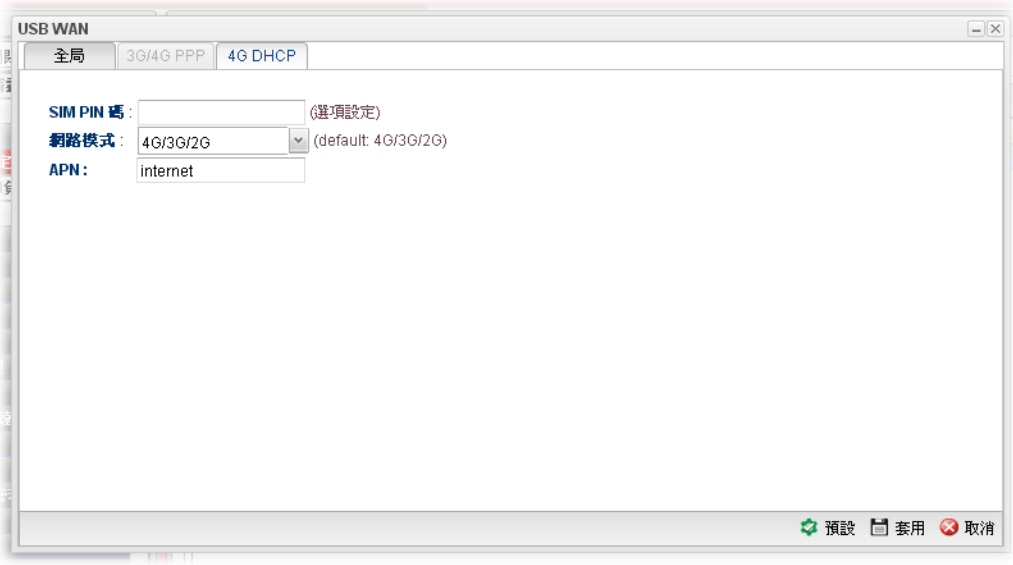
可用參數詳列如下：

項目	說明
設定檔	顯示 USB WAN 設定檔名稱。
啓用	勾選此框啓用 USB WAN 設定檔。
說明	輸入與此設定檔有關的簡易說明。
埠號	顯示設定檔的實體 WAN 介面。
通訊協定	選擇連線模式。 3G/4G PPP 3G/4G PPP 4G DHCP
預設	勾選此框還原預設值。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

3. 完成上述設定之後，按下 3G/4G PPP 或是 4G DHCP 標籤(依照電信業者提供服務內容而定) 顯示如下頁面。

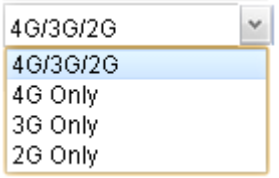


或是，



可用參數詳列如下：

項目	說明
3G/4G PPP	**SIM PIN 碼**-輸入用來登入網際網路之 SIM 卡的 PIN 代碼，最大長度爲 15 個字元。 **數據機初始字串 1**- 這個數值，用來初始化 USB 數據機，請使用預設值，如果您有任何疑問，請與當地 ISP 業者聯絡。 **數據機初始字串 2**- 初始化字串 1 是與 APN 搭配使用。但在某些情況下，使用者可能會使用另外的初始化 AT 指令來限制 3G 頻寬或是其他特殊事宜。此時即可設定第二個數據機初始化字串。 **APN**-APN 表示基地台的名稱，通常是由 ISP 業者提供並

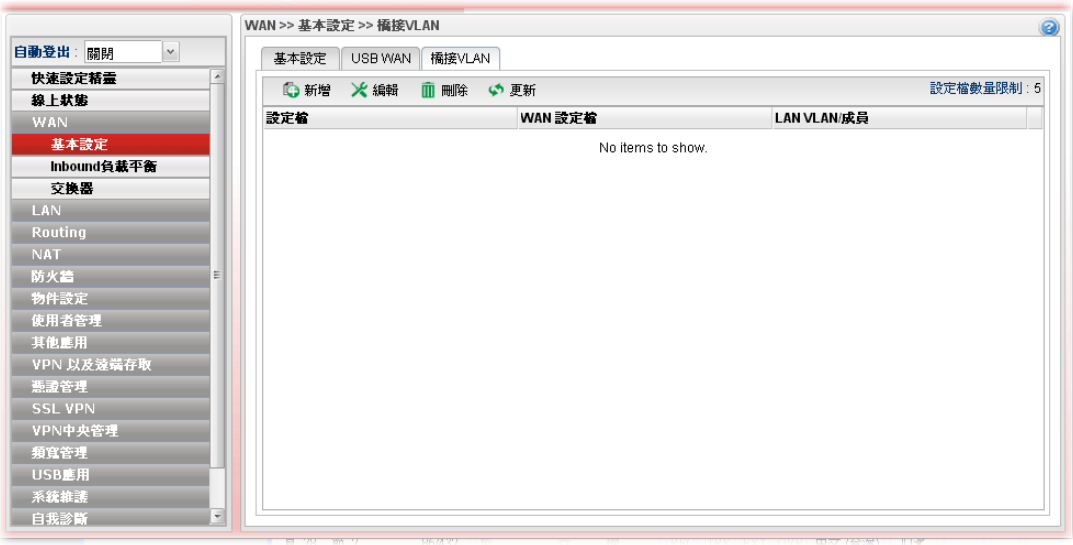
	要求您在此輸入，請輸入相關名稱。 **數據機撥號字串**- 這個數值，目的是在 USB 模式下撥號使用，請使用預設值，如果您有任何疑問，請與當地 ISP 業者聯絡。 **PPP 帳號**-輸入 PPP 使用者名稱 (視您實際需要而設定)。 **PPP 密碼**- 輸入 PPP 密碼 (視您實際需要而設定)。
4G DHCP	**SIM PIN 碼**-輸入用來登入網際網路之 SIM 卡的 PIN 代碼，最大長度為 15 個字元。 **網路模式** – 強迫路由器透過此處指定的模式進行網際網路連線，如果您選擇 4G/3G/2G，路由器將自動依據無線訊號選擇最適當的連線類型。  **APN**-APN 表示基地台的名稱，通常是由 ISP 業者提供並要求您在此輸入，請輸入相關名稱。
預設	勾選此框還原預設值。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

4. 在您完成上述的設定之後，請按**確定**按鈕來啓動設定。

4.1.1.3 橋接 VLAN 設定檔

開啓 **WAN>>基本設定**並按下**橋接 VLAN** 標籤。

橋接 VLAN 設定檔可以指定 WAN 埠口的 VLAN ID 值，並透過 WAN 與 LAN 埠口的橋接技術，提供使用者更進階的環境應用。

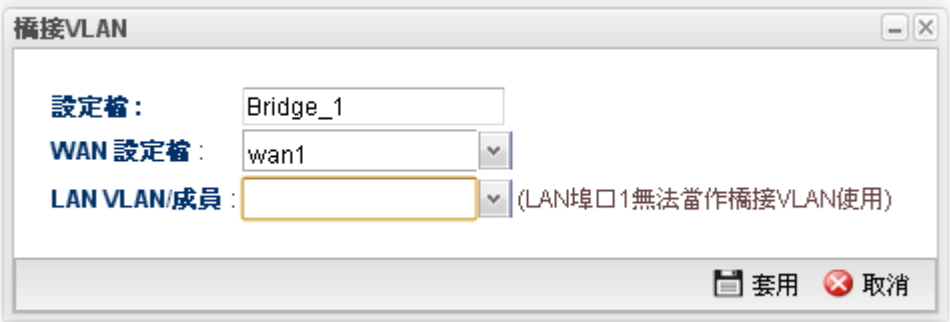


每個項目說明如下：

項目	說明
新增	按此建立新的設定檔。
編輯	修改選定的 USB WAN 設定檔。 選擇您想要編輯的設定檔，然後按下**編輯**按鈕，編輯視窗將會出現讓您修改相應的設定。
刪除	移除選定的 WAN 設定檔。 選擇您要刪除的設定檔，再按下刪除按鈕即可刪除該檔。
更新	重新更新本頁面。
設定檔數量限制	顯示可以建立的設定檔的最高數目。
設定檔	顯示 USB WAN 設定檔名稱。
WAN 設定檔	顯示選定的 WAN 設定檔名稱。
LAN VLAN/成員	顯示選定 LAN 埠口的 VLAN ID 號碼。

如何新增橋接 VLAN 設定檔

1. 按下**新增**。
2. 設定顯示如下：



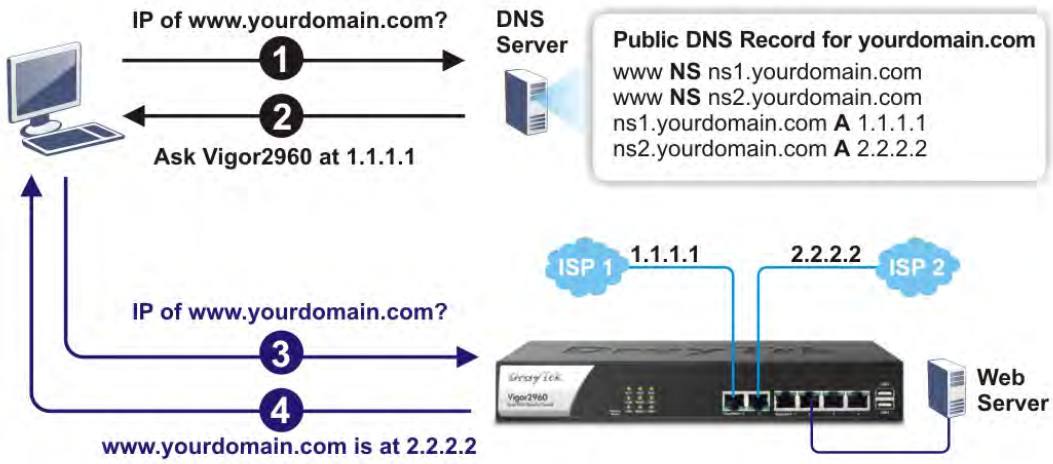
可用參數詳列如下：

項目	說明
設定檔	輸入設定檔的名稱。
WAN 設定檔	使用下拉式清單選擇適合此 VLAN 的 WAN 設定檔。
LAN VLAN/成員	自下拉式清單中選擇 VLAN 設定檔。 您必須先開啓 **LAN>>交換器**頁面並按下 **802.1Q** VLAN 以便建立與 LAN 埠口(802.1Q VLAN 設定檔)綁定的 VLAN ID 號碼，否則這個欄位將無任何選項可以挑選。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

3. 完成上述的設定之後，請按**套用**按鈕儲存設定，新增設定檔顯示如下：

4.1.2 Inbound 負載平衡

Vigor2960 提供對應的 IP 位址來回應遠端透過指定的網域發出的 DNS 詢問，藉此降低網路流量負擔。



開啓 **WAN>>負載平衡**並按下 **Inbound 負載平衡**標籤。

每個項目說明如下：

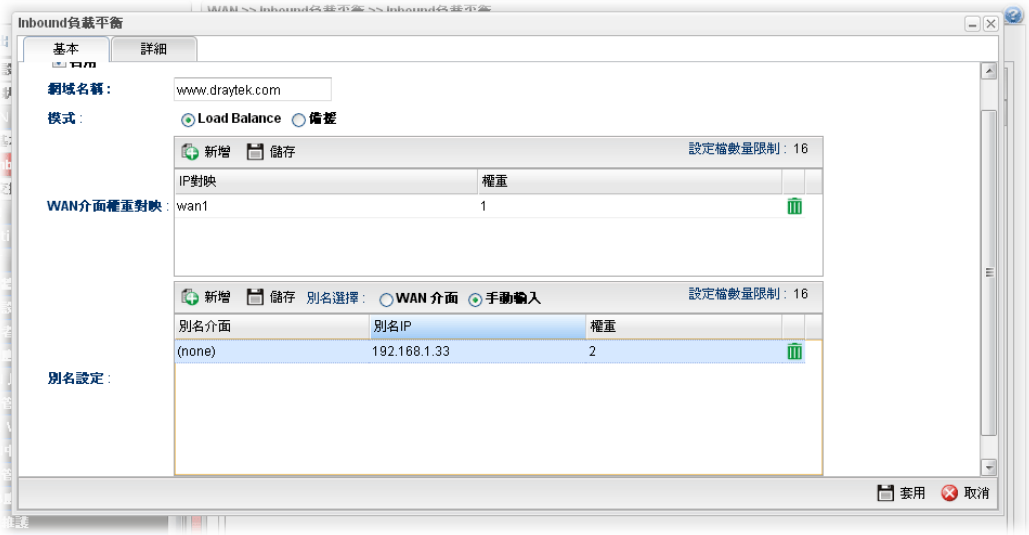
項目	說明

啓用	勾選此方塊啓用負載平衡功能。
新增	增加新的設定檔。
編輯	修改選定的 WAN 設定檔。 如欲編輯設定檔，請選擇您想要修正的項目，按下**編輯**按鈕，編輯視窗將會開啓讓您得以修改選定規則的細部內容。
刪除	移除選定的 WAN 設定檔。 如欲刪除設定檔，請選擇您要要移除的項目，按下**刪除**按鈕即可。
更新	重新更新本頁面。
設定檔數量限制	顯示可以建立的設定檔的最高數目。
啓用	顯示設定檔狀態，False 表示停用；True 表示啓用。
網域名稱	顯示設定檔使用的網域名稱。
模式	顯示設定檔套用的模式(備援或是負載平衡)。
IP 對映	顯示設定檔使用的 WAN 介面。
權重	顯示 WAN 介面的權重值。
別名介面	顯示 IP 別名使用的 WAN 介面。
IP	顯示設定檔使用的 IP 別名位址設定。
別名權重	顯示上述 IP 別名位址使用的權重值。

如何建立新的 Inbound 負載平衡設定檔

本頁讓您針對 inbound 負載平衡建立新的 WAN 設定檔。

1. 開啓 **WAN>>負載平衡**並按下 **Inbound 負載平衡**標籤。
2. 按下**新增**按鈕開啓如下頁面。



可用參數詳列如下：

項目	說明
啓用	勾選此框啓用此設定檔。
網域名稱	輸入可用的網域名稱提供 inbound 負載平衡服務。
模式	指定 WAN 設定檔套用的模式(備援或是負載平衡)。
優先權設定	這個選項僅在**模式**選擇備援式可用。 有五種等級可以選擇(Top, 2, 3, 4 與 5)套用於 WAN 設定檔(包含預設值與使用者自定值)。
WAN 介面權重對映	網域名稱將提供一組 IP 位址以回應遠端提出的 DNS 詢問事宜。 自 IP 對應中指定的 WAN 介面而來的詢問，系統將會依照權重值來處理。 **新增** – 按此選擇 WAN 介面以及權重。 **儲存** – 按此儲存設定。 **IP 對映** – 使用下拉式清單選擇給網域使用的 WAN 介面。 **權重** – 使用下拉式清單選擇權重值。
別名設定	此設定的目的是要從 WAN 界面指定一組 WAN IP 位址或是手動輸入 IP 位址以便回應遠端的 DNS 詢問。 **新增** – 按此以便輸入新的 IP 位址。 **儲存** – 按此以便儲存設定值。 **別名選擇** – 別名 IP 設定可以從現有的 WAN IP 別名中選取。 **WAN IP**-從現有的 WAN IP 別名中選取。 **手動輸入** –別名 IP 設定可以手動輸入，此種方法不需選擇別名介面。 **別名介面** – 使用下拉式清單選擇 WAN 介面設定檔。 **別名 IP** – 使用下拉式清單選擇別名 IP 設定或是手動輸入 IP 位址。 **權重** – 使用下拉式清單選擇您想要的權重值。

3. 完成**基本**頁面的設定之後，按下**詳細**標籤開啓如下對話盒：

可用參數詳列如下：

項目	說明
DNS 參數	設定 Vigor 路由器爲 DNS 伺服器時，請輸入相關資訊以套用 DNS 功能。 **TTL** – 代表 DNS 回應的有效時間，可用的設定範圍從 0 到 2147483647。 **更新** – 設定時間讓 LAN 端的電腦更新資料。 **重試** – 設定在更新時間到期前，電腦與 Vigor 路由器聯繫失敗時的重試次數。 **過期** – 當這邊設定的時間值已屆，電腦即停止回應路由器的詢問。 **Nagative Cache TTL** – 設定負緩存時間(名稱錯誤)。 **電子信箱** – 輸入管理者的郵件信箱。
NS 紀錄	本頁用來指定可作爲 DNS 伺服器的名稱伺服器。 **新增** – 按此新增新的伺服器。 **儲存** – 按此儲存設定。 **主機** – 輸入伺服器的網域名稱，這是選項設定，如果沒有在此輸入任何資訊，路由器會使用基本標籤中的網域名稱所設定的 DNS 伺服器來運作。 **名稱伺服器** – 輸入名稱伺服器的URL，將用於接收由主機轉過來的DNS詢問事宜。 **IP 位址** – 這是選項設定，如有必要請輸入 NS 紀錄伺服器的 IP 位址。
MX 紀錄	這項功能用來指定郵件伺服器。 **新增** – 按此新增新的伺服器。 **儲存** – 按此儲存設定。 **主機** –輸入伺服器的網域名稱。

	郵件伺服器 –輸入郵件伺服器的 URL。 **IP 位址** – 輸入郵件伺服器的 IP 位址。 **偏好**- 輸入什麼數字決定優先級別。
其他紀錄	以 IPv4 位址記錄 DNS 詢問。 **新增** – 按此新增新的主機。 **儲存** – 按此儲存設定。 **主機** – 設定網域名稱。 **IP 位址** – 輸入伺服器的 IP 位址。
AAA 紀錄	以 IPv6 位址記錄 DNS 詢問。 **新增** – 按此新增新的主機。 **儲存** – 按此儲存設定。 **主機** – 設定網域名稱。 **IPv6位址** – 輸入伺服器的IPv6位址。 任何詢問關於主機的問題都會被轉往參考區選定的伺服器上，以便進行下一個流程。
CNAME 紀錄	用來記錄關於 CNAME 的 DNS 詢問。 **新增** – 按此新增新的主機。 **儲存** – 按此儲存設定。 **主機** – 設定網域名稱。 **參考** – 自下拉式清單選擇網域名稱。 任何詢問關於主機的問題都會被轉往參考項目選定的伺服器上，以便進行下一個流程。

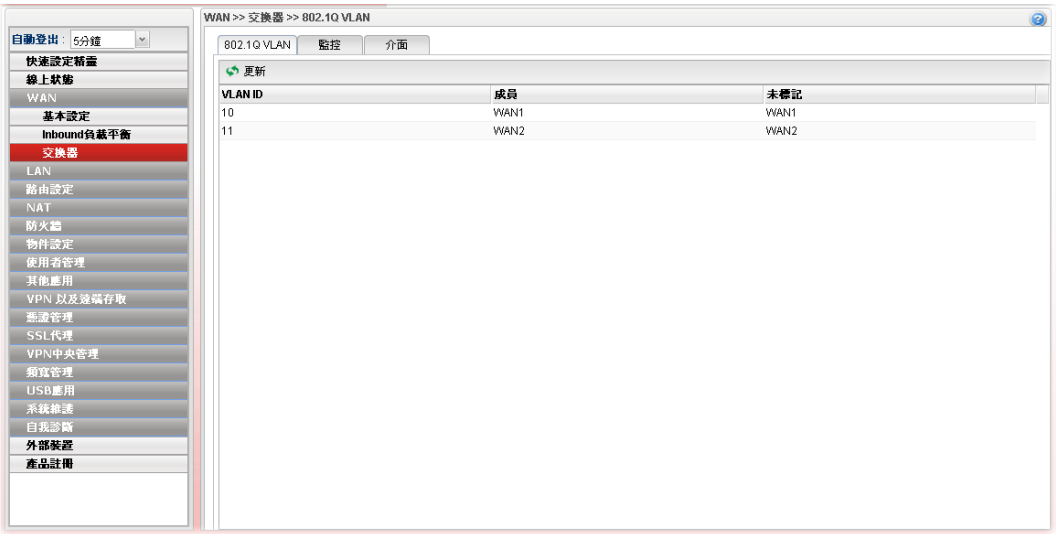
4. 按下**套用**，新設定檔將會顯示在頁面上。

在選定的負載平衡設定檔中，您可以按下左邊的 ▶ 建立子網域，如下的**子網域設定**頁面將顯示出來讓您增加新的設定檔。

注意，此處的設定方式與上述步驟說明的內容是相同的。

4.1.3 交換器

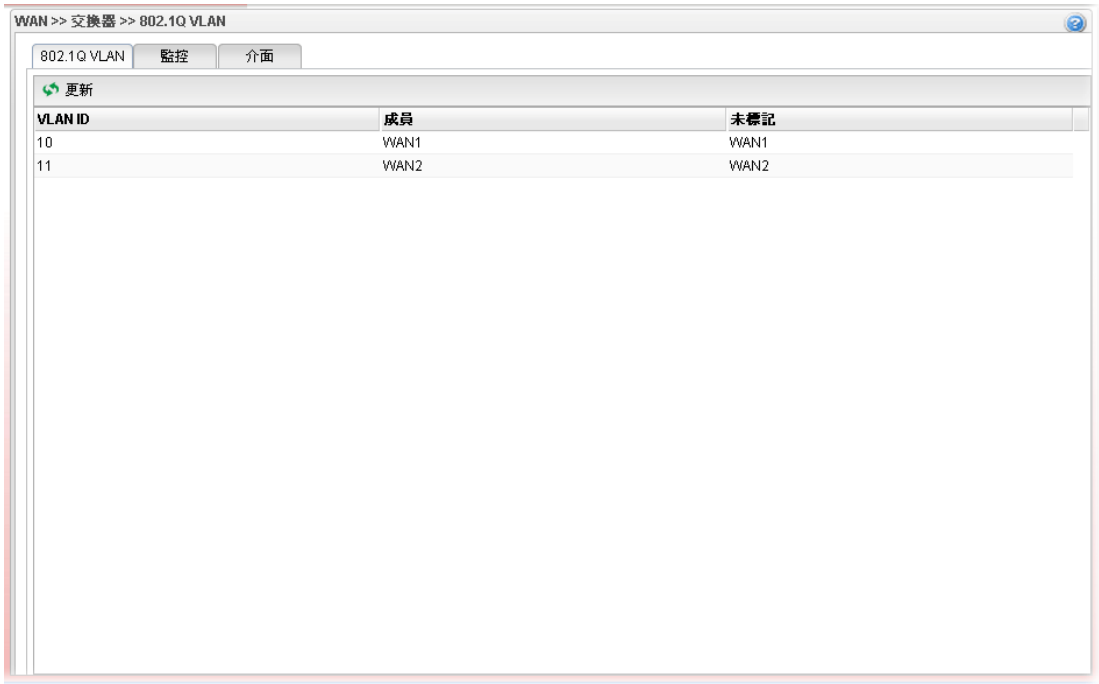
本頁讓您設定監控口(Mirroring Port)、被監控口(Mirrored Port)、啓用/停用 WAN 介面並設定 802.1Q VLAN ID 以應不同 WAN 介面之需。



4.1.3.1 802.1Q VLAN

透過 WAN 介面傳送的封包可以貼上 VLAN ID 編號標籤或是不加上任何標籤，這須視 **WAN>>基本設定>>設定檔**中的 VLAN ID 配置內容而定。

本頁簡單呈現出目前 802.1Q VALN 的設定檔內容。

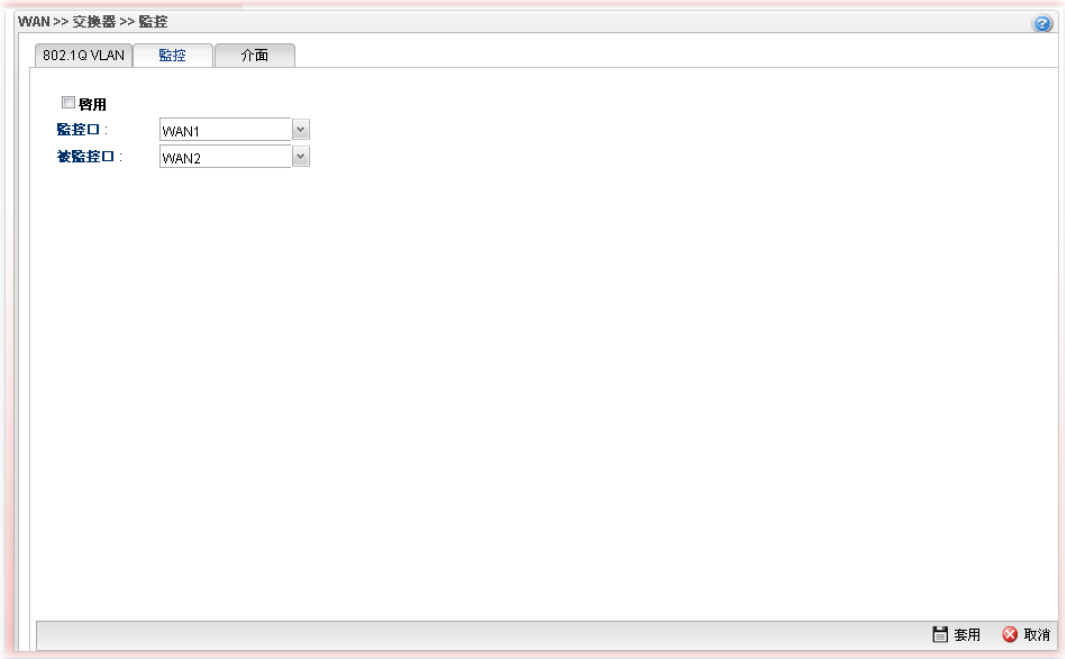


每個項目說明如下：

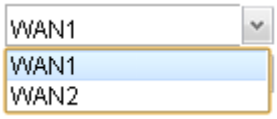
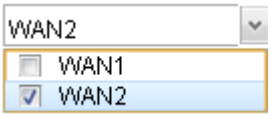
項目	說明
更新	重新更新本頁面。
VLAN ID	顯示 VLAN ID 編號。
成員	顯示標示 VLAN ID 編號的封包所通過的 WAN 介面口為何。
未標記	顯示未加標籤的封包所通過的 WAN 介面口為何。

4.1.3.2 監控設定

管理者可以利用監控口來監看所有從被監控口出入的的封包，這個功能對管理者想要分析網路故障發生原因來說相當有助益。

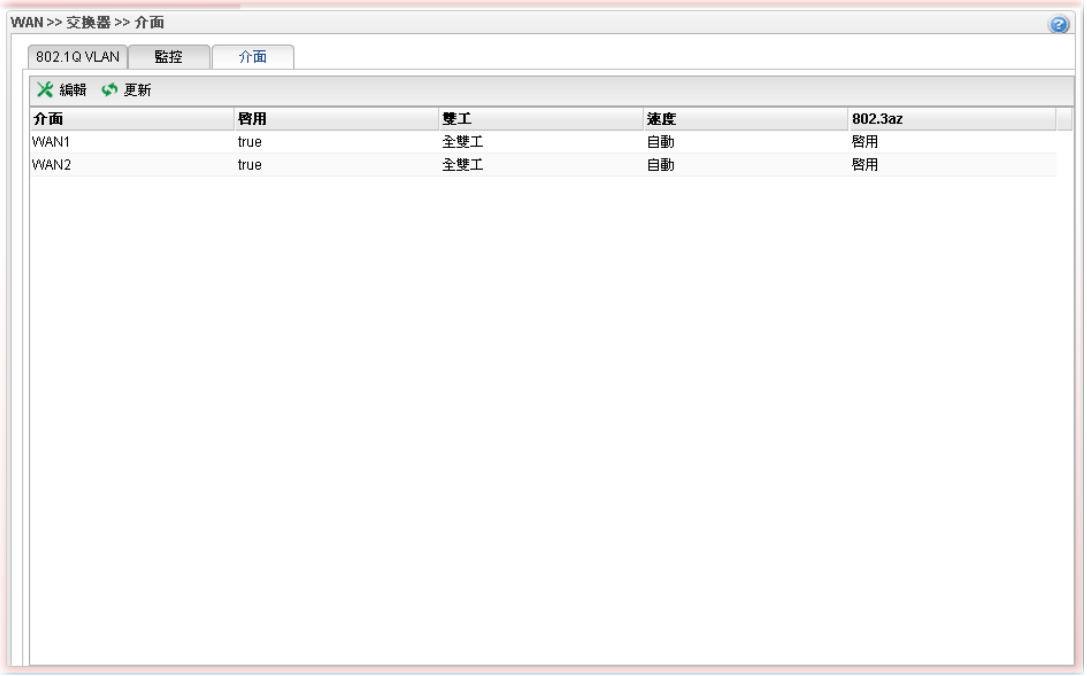


可用參數詳列如下：

項目	說明
啓用	勾選此方框啓用監控功能。
監控口	選擇一個管理者可以用來檢視被監控口的網路流量之介面。 
被監控口	選擇一個埠口，讓封包能透過該埠口出入並受到管理者的監控。 
套用	按此鈕儲存設定。
取消	按此鈕捨棄頁面設定。

4.1.3.3 介面

本頁可讓您分別修正 WAN 口的狀態(啓用/停用)、雙工(半/全)、速度及 802.3az。



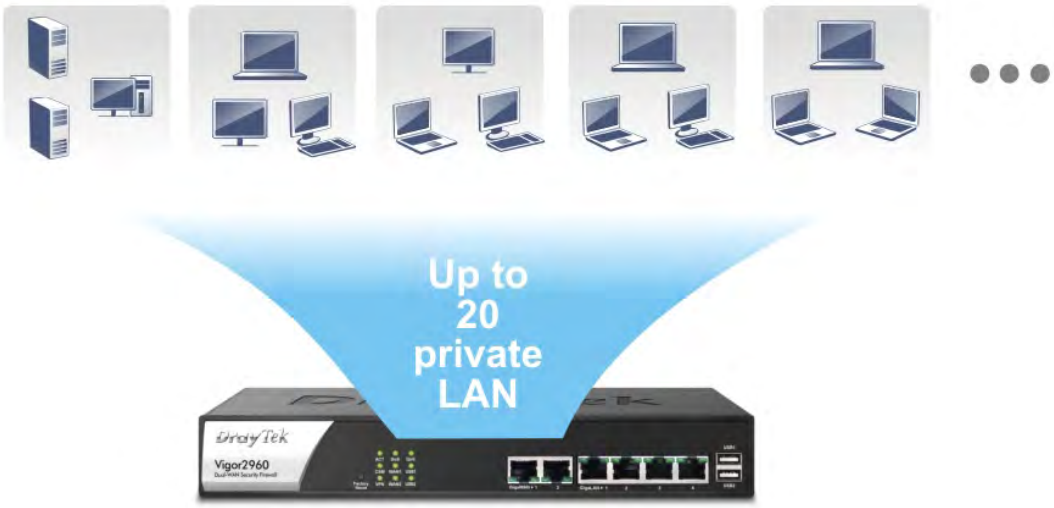
每個項目說明如下：

項目	說明
編輯	選擇下面列出的介面並按下**編輯**按鈕進行設定修正，畫面將會跳出另一個視窗讓您變更設定。 **介面** – 顯示 WAN 介面的名稱。 **啓用** – 勾選此框啓用此設定。 **速度** – 使用下拉式清單指定傳輸速度(**自動**、**10M**、**100M**、**1000M**、**1000M-停用自動偵側**、**100M-停用自動偵側**)。 **802.3az –** 乙太網路節能特色。能自動偵測網路流量以調整電源輸出，讓 Vigor2960 在使用量較低的時段內節省能源，避免浪費。選擇**啓用**以啓動此功能。

	套用 – 按此儲存設定並離開此視窗。 取消 – 按此捨棄設定並離開畫面。
更新	重新更新本頁面。
介面	顯示路由器 WAN 埠口的名稱。
啓用	顯示設定檔狀態，False 表示停用；True 表示啓用。
雙工	顯示設定檔的雙工值(全或半) 。
速度	顯示設定檔的傳輸速率(例如 1000M)。
802.3az	顯示此功能是否爲啓用。

4.2 區域網路(LAN)

區域網路(LAN)是由路由器所管理的一群子網路，網路結構設計和您自 ISP 所取得之真實 IP 位址有關。



Vigor 路由器最基本的功能爲 NAT，可用來建立虛擬的子網路，如前所述，路由器利用真實 IP 位址與網際網路上其他的真實主機互相通訊，或是使用虛擬 IP 位址與區域網路上的主機連繫。NAT 要完成的事情就是轉換來自真實 IP 位址的封包到私有 IP 地址，以便將正確的封包傳送至正確的主機上，反之亦然。此外 Vigor 路由器還有內建的 DHCP 伺服器，可指定虛擬 IP 地址至每個區域主機上。

4.2.1 基本設定

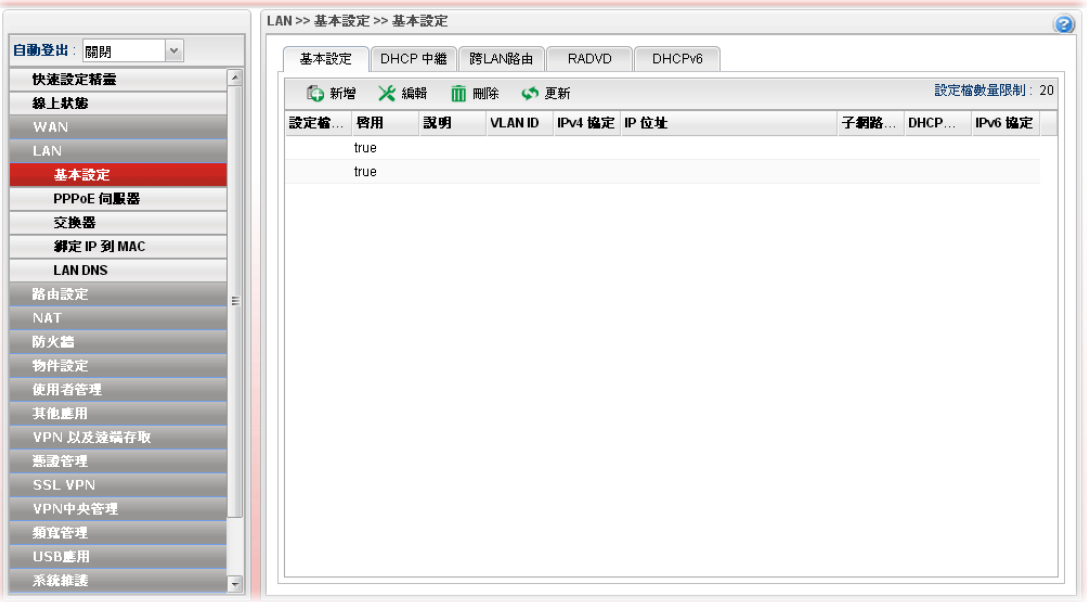
本頁讓您設定區域網路中所有電腦皆適用的基本設定檔。

當 LAN 設定檔建立時，系統會自動產生預設值，您可以編輯這些數值變更設定。

注意：至少要啓動一個 LAN 設定檔以維持正常的操作，預設的 LAN 設定檔名稱爲 lan1，這個檔案絕不可以刪除，否則路由器系統可能會毀損，如果您不小心刪除了此檔案，請立即重新啓動路由器回復出廠預設值。

4.2.1.1 基本設定

本頁讓您啓用設定檔，定義簡單的說明，指定 VLAN ID，指定 MAC 位址並選擇適合的協定類型。



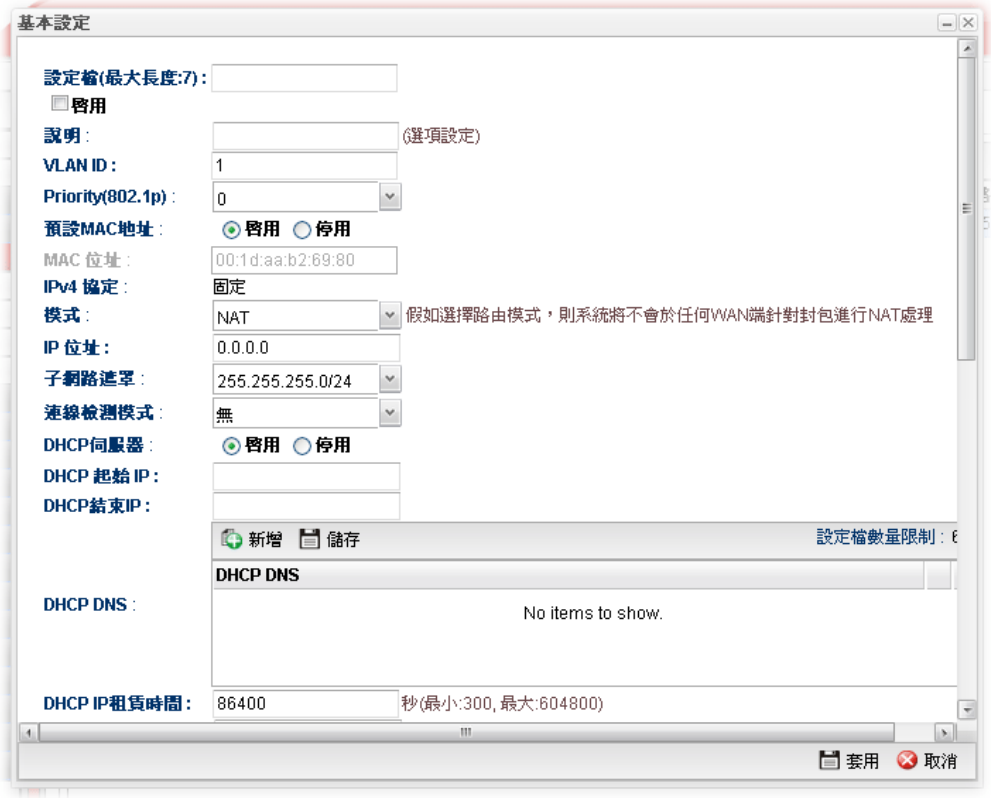
每個項目說明如下：

項目	說明
新增	新增 LAN 設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
刪除	移除選定的設定檔。 請選擇您想要刪除的既有設定檔，然後按下刪除按鈕，該設定檔即可被移除。
更新	重新更新本頁面。
設定檔數量限制	顯示允許建立的設定檔總數。
設定檔(最大長度限制:7)	顯示設定檔名。
啓用	顯示設定檔狀態，False 表示停用；True 表示啓用。
說明	顯示該設定檔的簡易說明。

VLAN ID	顯示設定檔的 VLAN ID 。
IPv4 協定	顯示設定檔使用的 IPv4 協定。
IP 位址	顯示設定檔的 IP 位址。
子網路遮罩	顯示設定檔的子網路遮罩。
DHCP 伺服器	顯示 DHCP 伺服器的狀態(啓用/停用) 。
IPv6 協定	顯示設定檔的 IPv6 位址。

如何新增 LAN 設定檔

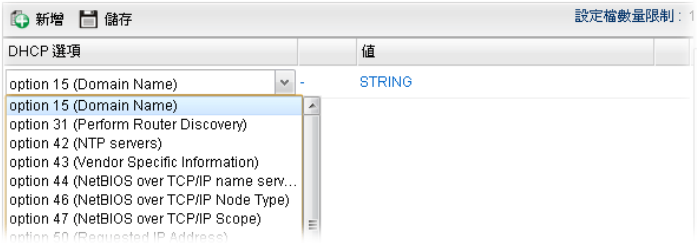
1. 開啓 **LAN>>基本設定**並按下**基本設定**標籤。
2. 按下**新增**按鈕開啓如下畫面，不同的協定類型，設定的頁面也會有些差異。



可用參數詳列如下：

項目	說明
設定檔(最大長度限制:7)	輸入設定檔名。
啓用	勾選核取框啓用此設定檔。
說明	輸入設定檔的簡易說明。
VLAN ID	輸入設定檔的 VLAN ID，以便執行資料傳輸時用來辨認相關資料。
Priority (802.1q)	指定此 VLAN 的封包優先權，範圍從 0 到 7。

預設 MAC 位址	**啓用** – 按此可以啓用預設的 MAC 位址。 **停用** – 按此之後須手動輸入 MAC 位址。 **MAC 位址** – 您若選擇停用，則須在此欄位輸入 MAC 位址。系統的預設值是啓用的。輸入格式如 “00:1d:aa:b2:69:80”。
IPv4 協定	顯示此設定檔使用的協定類型。
模式	決定此設定檔採用 NAT 或是路由模式來進行。
IP 位址	輸入此設定檔所需的 IP 位址(輸入格式如 192.168.1.25 等)。
子網路遮罩	使用下拉式清單選擇適當的子網路遮罩。
連線檢測模式	選擇此 LAN 介面需要的偵測模式，有 **ARP** 與**無**可以挑選。 當您選擇**無**時，系統將不會進行連線檢測。 這項功能主要是爲了搭配**策略路由**使用。系統透過連線檢測，可以讓路由器採用適合的路由規則。
閘道 IP 位址	此功能僅在 ARP 選爲連線檢測模式時才有作用。 輸入閘道 IP 位址。系統將偵測此處設定的目標 IP 位址，若偵測不到，即顯示爲斷線。
連線檢測間隔	此功能僅在 ARP 選爲連線檢測模式時才有作用。 指定每次偵測的時間間隔。.
連線檢測重試	此功能僅在 ARP 選爲連線檢測模式時才有作用。 指定檢測次數，經過您所設定的時間之後，LAN 連線介面將被自動斷線。
DHCP 伺服器	啓用 – 按此啓用 DHCP 伺服器，DHCP 伺服器將會隨機分派 IP 位址給予 LAN 端的用戶，可分派的 IP 位址範圍定義在 DHCP 起始 IP 與結束 IP 欄位。 停用 – 按此停止使用 DHCP 伺服器。
DHCP 起始 IP	輸入 DHCP 伺服器所需的起始 IP 位址點。
DHCP 結束 IP	輸入 DHCP 伺服器所需的結束 IP 位址點。
DHCP DNS	設定 DNS 伺服器的 IP 位址，如果本區空白，LAN 端的使用者將視 Vigor2960 爲 DNS 伺服器。 DHCP DNS : 新增 儲存 DHCP DNS 168.95.1.1 **新增** – 按此加入一組作爲 DNS 伺服器的 IP 位址。 **儲存** – 按此儲存設定。

DHCP IP 租賃時間	設定 DHCP 伺服器的租約時間，時間單位爲分鐘。
DHCP 路由	一般來說，此區是空白的，它表示 Vigor2960 被視爲使用者的閘道器。 然而，如果您想使用其他的閘道，請在本區指定一組位址。
DHCP Next Server	輸入次要 DHCP 伺服器的 IP 位址。
DHCP 選項	當此區啓用時，DHCP 封包可藉由加入 option 編號與資料相關資訊進行處理。 每個 DHCP option 都是由一個 option 號碼加上資料而成，例如： Option number:100 Data: abcd 當此功能啓用的時候，DHCP option 指定值在 DHCP 回傳封包中即可見到。  **新增** –按此鈕以便建立 DHCP option。 **儲存** – 按下此鈕儲存設定。 **DHCP Option** –使用下拉式清單選擇您需要的 option 內容。 **值** – 輸入 DHCP 選項需處理的資料內容。
指定遠端撥入 IP	**啓用** – 勾選此框啓用此功能，下述指定範圍內的遠端用戶都可以存取 Vigor2960。
閘道 IP 位址	輸入閘道 IP 位址。
更多子網	指定未來可能有所需求的其他子網。 **新增** – 按此鈕以便輸入新的子網遮罩與 IP 位址並指定需用模式。 **儲存** – 按此鈕儲存設定。 **IP** – 輸入 IP 位址。 **子網遮罩** – 使用下拉式清單選擇需要的遮罩。 **模式**– 指定 NAT 或是路由做爲需求模式。 **DHCP** – 選擇**啓用**讓 DHCP 功能生效，您必須指定 IP 範圍讓 DHCP 伺服器針對此子網分派 IP 位址。

	起始 IP – 輸入 IP 位址作爲起點。 **結束 IP** – 輸入 IP 位址作爲結束點。
DNS 重導向	**啓用**–可重新導向 DNS 查詢至路由器的 DNS 伺服器上，這個功能必須與 LAN DNS 功能搭配運作。
IPv6 協定	定義 LAN 介面的 IPv6 連線類型，可用的類型包含 Link-Local, Static and DHCP-SLA，除了 Link-Local 以外，其他的類型都需更進一步的參數設定。 **Link-Local**-這個協定的位址用來與位於相同連結中的相鄰節點彼此互相通訊之用，其位址定義格式爲 **fe80::/10**，您不需要手動輸入 Link-Local 的位址，因爲系統會依照您的 MAC 位址自動給與位址設定。 **固定** – 這個類型讓您設定固定的 IPv6 位址。 **DHCP-SLA**- DHCPv6 用戶端模式將使用 IA_NA option of DHCPv6 協定以便從伺服器處取得 IPv6 位址。
IPv6 位址	如果 IPv6 協定選擇**固定**，請您在此輸入指定的 IPv6 位址。
IPv6 前置碼長度	定義 IPv6 前置碼的長度。
DHCPv6 SLA WAN 介面	I 如果 IPv6 協定選擇 **DHCP-SLA**，請在本區選擇一個 WAN 設定檔。
DHCPv6 SLA ID	這裡設定的 ID 用於個人組織以便產生專屬的本地位址並可用以辨識子網。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

3. 當您完成上述設定之後，請按下**套用**儲存設定內容並離開對話盒。

4.2.1.2 DHCP 中繼

DHCP 是 Dynamic Host Configuration Protocol 的縮寫，路由器的出廠預設值可以作爲您的網路的 DHCP 伺服器，所以它可自動分派相關的 IP 設定給區域的使用者，將該使用者設定成爲 DHCP 的用戶端。如果您的網路上並沒有任何的 DHCP 伺服器存在，建議您讓路由器以 DHCP 伺服器的型態來運作。

如果您想要使用已存在或其它的 DHCP 伺服器，而非路由器的伺服器，您可以利用中繼代理來幫您重新引導 DHCP 需求到指定的位置上。

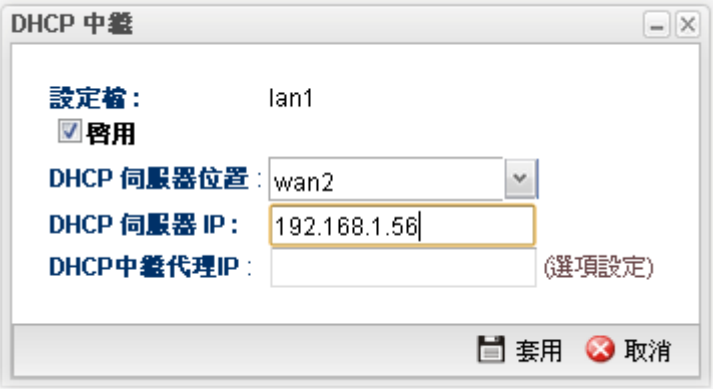
本頁可讓使用者指定 DHCP 伺服器所在的子網位置，讓中繼代理能將 DHCP 要求重新導向至該區。

每個項目說明如下：

項目	說明
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
更新	重新更新本頁面。
設定檔	顯示設定檔名稱。
啓用	顯示設定檔的狀態，False 表示停用；True 表示啓用。
DHCP 伺服器位置	顯示 DHCP 伺服器的 LAN 或是 WAN 設定檔。
DHCP 伺服器 IP	顯示 DHCP 伺服器的 IP 位址。
DHCP Relay Agent IP	顯示 DHCP 中繼代理伺服器的 IP 位址。

如何編輯 DHCP 中繼的 LAN 設定檔

1. 開啓 **LAN>>基本設定**並按下 **DHCP 中繼**標籤。
2. 選擇一個 LAN 設定檔，點選之後按下**編輯**按鈕開啓如下對話盒：



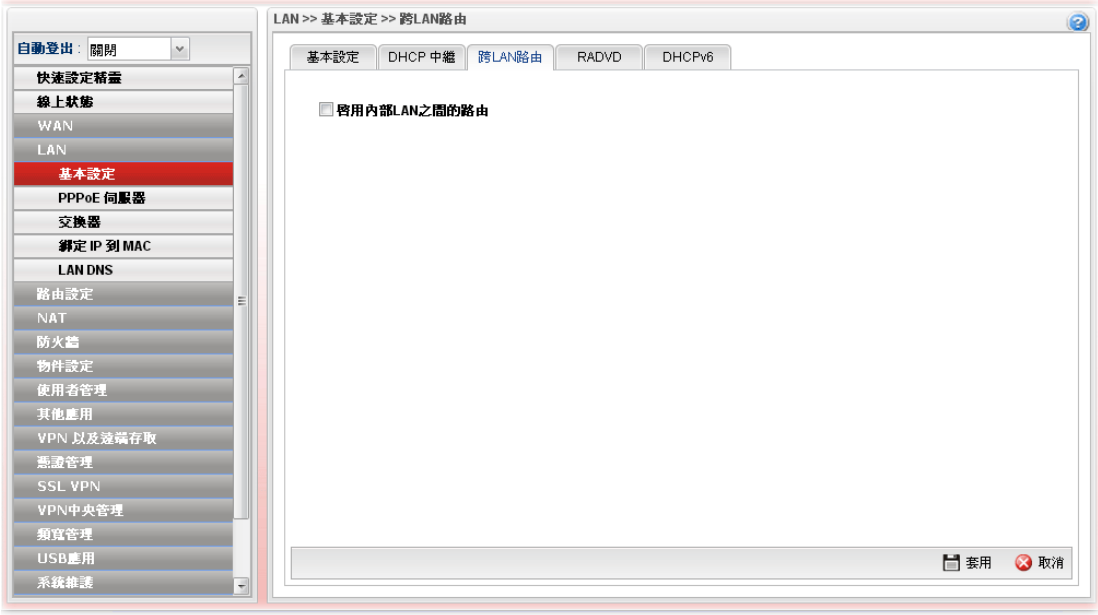
可用參數詳列如下：

項目	說明
設定檔	顯示 LAN 設定檔的檔名。
啓用	勾選此框啓用此設定檔。
DHCP 伺服器位置	選擇 DHCP 伺服器的介面。
DHCP 伺服器 IP	輸入 DHCP 伺服器的 IP 位址。
DHCP 中繼代理 IP	輸入 DHCP 中繼代理伺服器的 IP 位址。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

3. 當您完成上述設定之後，請按下**套用**儲存設定並離開對話盒。
4. LAN 設定檔已經編輯完成。

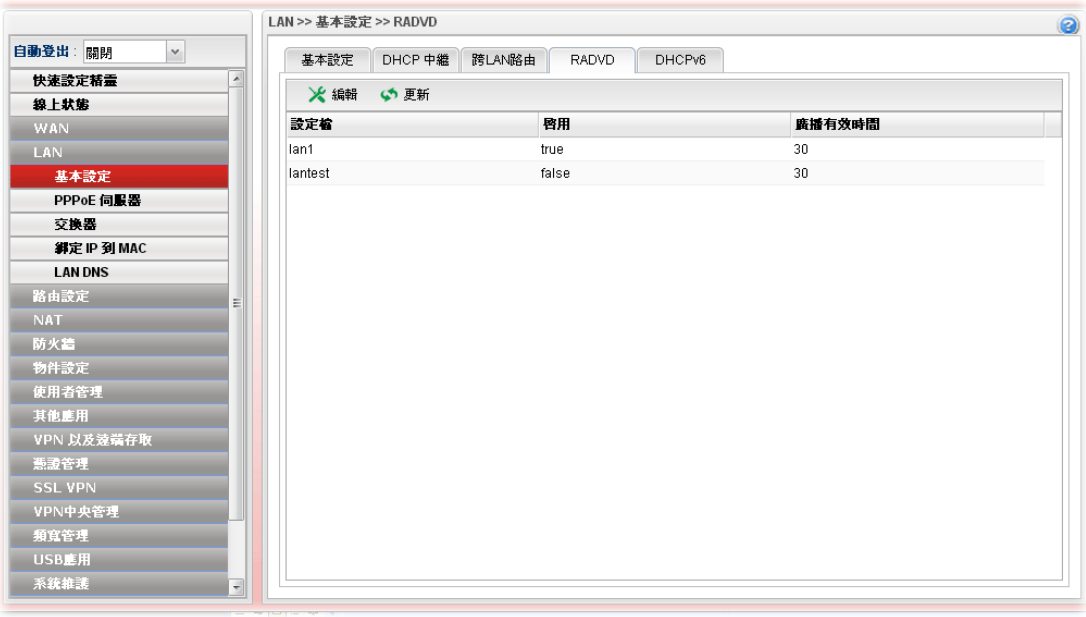
4.2.1.3 跨 LAN 路由

不同 LAN 的使用者若要彼此相通，請勾選**啓用內部 LAN 之間的路由**框啓用該功能。



4.2.1.4 RADVD

當節點傳送路由需求訊息時，路由器的 RADVD 定期傳送由 RFC 2461 指定的路由廣告訊息至本地乙太網路 LAN，這些訊息皆爲 IPv6 無狀態自動組態設定(IPv6 stateless auto-configuration)



每個項目說明如下：

項目	說明
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
更新	重新更新本頁面。
設定檔	顯示設定檔名稱。
啓用	顯示設定檔狀態，False 表示停用；True 表示啓用。
廣播有效時間	顯示有效時間值。 與預設路由器有關的有效時間單位爲分鐘，範圍從 10 到 150 爲止，若設定爲 0 則表示路由器並非爲預設的路由器，在預設的路由器清單上也不該出現該台路由器。

如何編輯 RADVD 的 LAN 設定檔

1. 開啓 **LAN>>基本設定**，按下 **RADVD** 標籤。
2. 移動滑鼠至任何一個 LAN 設定檔，按下去選定該檔，接著再按**編輯**按鈕開啓如下對話盒：

可用參數詳列如下：

項目	說明
設定檔	顯示 LAN 設定檔名。
啓用	勾選此框啓用此設定檔。
廣播有效時間	顯示有效時間值。 與預設路由器有關的有效時間單位爲分鐘，範圍從 10 到 150 爲止，若設定爲 0 則表示路由器並非爲預設的路由器，在預設的路由器清單上也不該出現該台路由器。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

3. 當您完成上述設定之後，按下**套用**儲存設定並離開對話盒。
4. LAN 設定檔已經完成編輯。

4.2.1.5 DHCP6

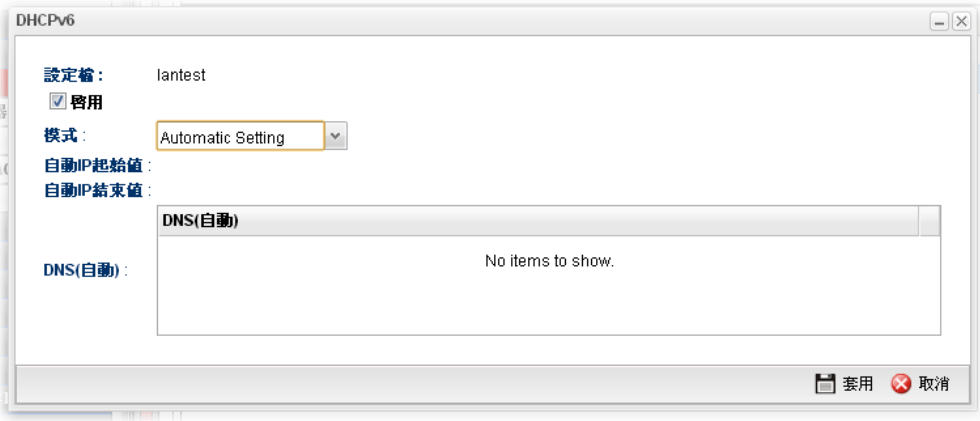
DHCP6 伺服器可依照 IPv6 位址設定指派 IPv6 位址至電腦上。

每個項目說明如下：

項目	說明
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
更新	重新更新本頁面。
設定檔	顯示設定檔名稱。
啓用	顯示設定檔狀態，False 表示停用；True 表示啓用。
模式	顯示此設定檔指定的模式選項(自動設定或是手動設定)。
起始 IP	顯示 DHCP 伺服器 IP 位址配置量的起始 IP 位址)。
結束 IP	顯示 DHCP 伺服器 IP 位址配置量的結束 P 位址。
DNS	顯示 DNS 伺服器的虛擬 IP 位址。

如何編輯 DHCPv6 的 LAN 設定檔

1. 開啓 **LAN>>基本設定**，按下 **DHCPv6** 標籤。
2. 移動滑鼠至任何一個 LAN 設定檔，按下去選定該檔，接著再按**編輯**按鈕開啓如下對話盒：



可用參數詳列如下：

項目	說明
設定檔	顯示 LAN 設定檔名。
啓用	勾選此框啓用此設定檔。
模式	選擇**自動設定**或是**手動設定**。 **Automatic Setting(自動設定)** – 選擇此模式時，系統將會自動提供適當的位址值。 **Manual Setting(手動設定)** – 您必須自行輸入起始 IP 位址以及結束 IP 位址。
起始 IP	設定 DHCP 伺服器的 IP 位址配置量的起始 IP 位址，輸入格式如同下列範例： 2000:0000:0000:0000:0000:0000:0000:10 或是 2000::10。
結束 IP	設定 DHCP 伺服器的 IP 位址配置量的結束 IP 位址，輸入格式如同下列範例： 2000:0000:0000:0000:0000:0000:0000:10 或是 2000::10。
DNS	這個選項在手動設定選擇爲模式時才可使用。請設定 DNS 伺服器的虛擬 IP 位址，如果此區空白，LAN 端的使用者將視 Vigor2960 爲 DNS 伺服器。

	DNS : **新增** – 按此加入新的 IP 位址以應 DNS 伺服器之需。 **儲存** – 按此儲存設定。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

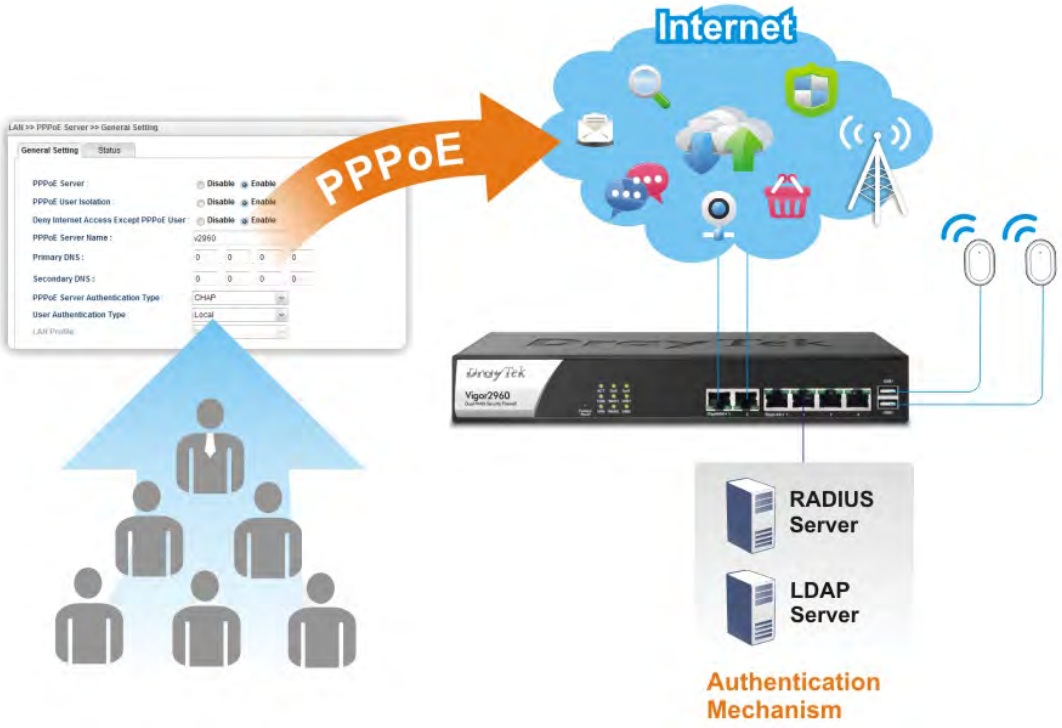
3. 當您完成上述設定時，請按下**套用**儲存設定並離開對話盒。

4. LAN 設定檔已經完成編輯。

4.2.2 PPPoE 伺服器

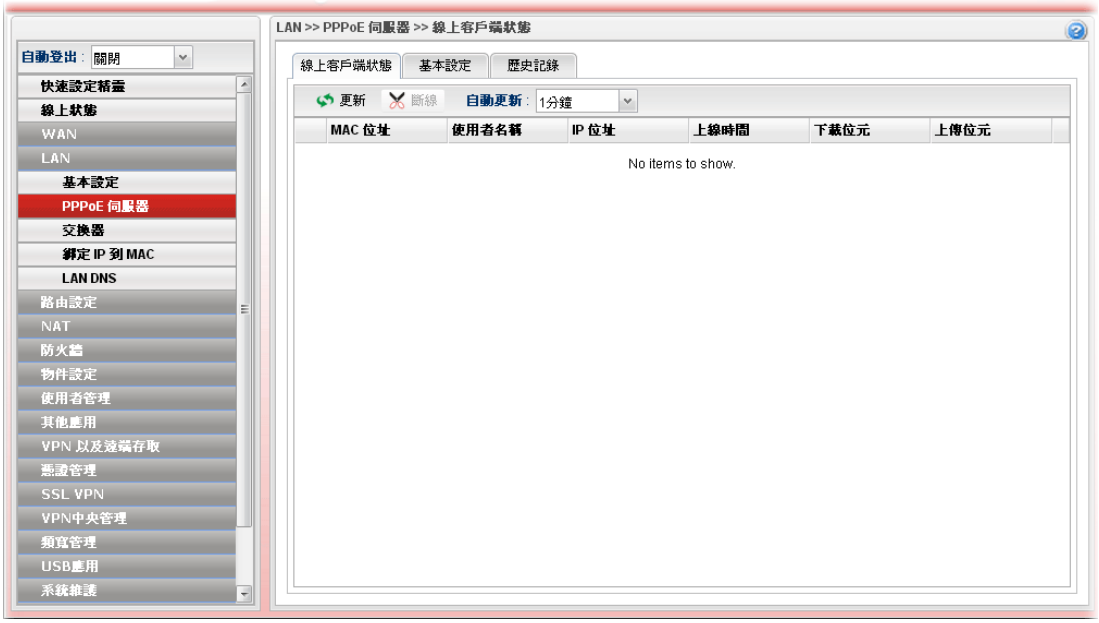
這個功能讓路由器有如 ISP 般運作，提供 PPPoE 連線給予 LAN 端的電腦。唯一差異是本地電腦不需要一個 ADSL 數據機。

LAN 中使用 PPPoE 連線有數種好處，PPPoE 伺服器透過帳號/密碼驗證的方式，提供 LAN 端電腦安全防護；其次它可以避免 ARP 攻擊；第三，系統管理者可以對每個使用者設定不同的時間/流量定額，就像是 ISP 業者所做的事情一樣。



4.2.2.1 線上用戶端狀態

本頁顯示 PPPoE 伺服器的一般資訊，也可讓您中斷與 PPPoE 伺服器相連的網路連線。

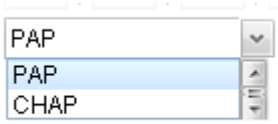


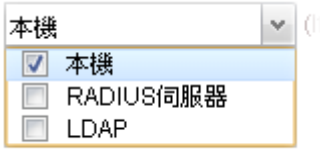
每個項目說明如下：

項目	說明
更新	重新更新本頁面。
斷線	按此中斷設定檔連線。
自動更新	指定更新時間的間隔以便獲得最新的狀態資訊。 當您按下頁面更新按鈕時，可立即取得更新後的訊息。
MAC 位址	顯示用戶主機的 MAC 位址。
使用者名稱	顯示用來登入 PPPoE 伺服器的使用者名稱。
IP 位址	顯示用戶主機的 IP 位址。
上線時間	顯示 PPPoE 連線建立的時間。
下載位元	顯示接收封包的總量。
上傳位元	顯示傳送封包的總量。

4.2.2.2 基本設定

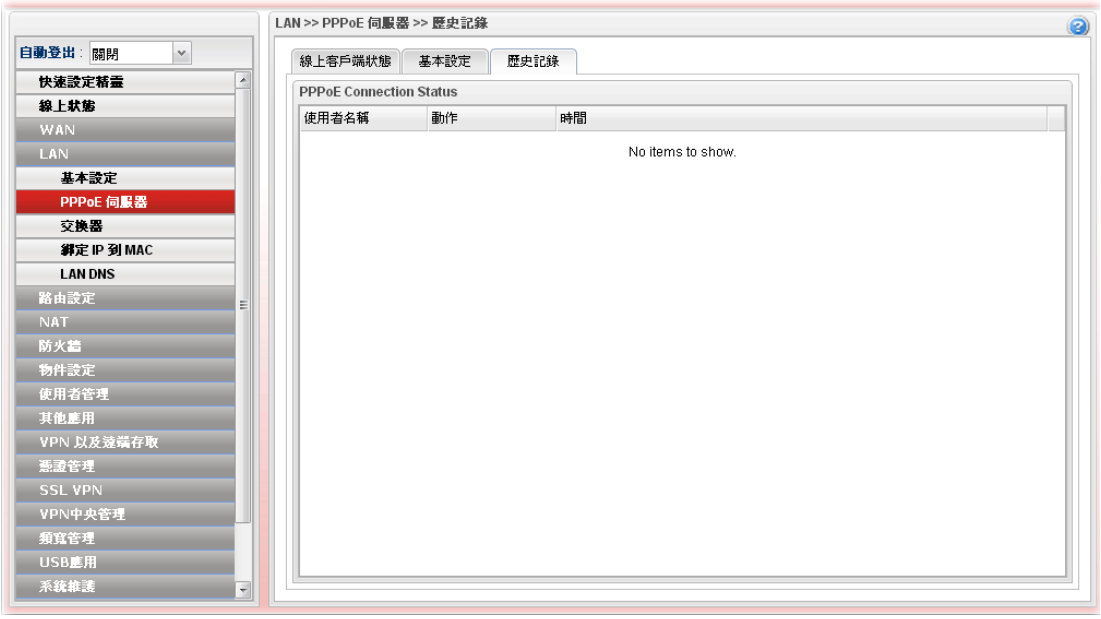
可用參數詳列如下：

項目	說明
PPPoE 伺服器	**停用** – 按此停用此功能。 **啓用** – 按此啓用此功能。
PPPoE 使用者隔離	**停用** – 按此停用此功能。 **啓用** – 按此隔離透過 Vigor 路由器登入網際網路的 PPPoE 用戶 。
拒絕非 PPPoE 使用者上網	**停用** – 按此停用此功能。 **啓用** – 按此限定僅有 PPPoE 用戶可以登入網際網路。
存取集訊器名稱	輸入可做爲存取集訊器(AC)名稱的內容。
服務名稱	輸入驗證專屬字串。
主要 DNS	輸入 IP 位址作爲主要 DNS。
次要 DNS	輸入 IP 位址作爲次要 DNS。
PPPoE 伺服器驗證類型	選擇 PPPoE 伺服器的驗證類型。  任何 PPPoE 使用者皆可通過 PPPoE 伺服器的驗證並登入網際網路。
用戶驗證類型	區域網路上的使用者可以藉由 RADIUS、LDAP 或是驗證

	等方式透過路由器登入網際網路。 
LDAP 設定	這個選項僅在 LDAP 被選擇爲使用者驗證類型時可用。 請使用下拉式清單指定需要的 LDAP 設定檔。
DHCP 來自於	這個選項僅在 RADIUS 被選擇爲使用者驗證類型時可用。
DHCP 中繼	**啓用** - 如果您想要在網路上使用另一個 DHCP 伺服器，您必須讓中繼代理協助，將 DHCP 需求重新導向指定的位置。 **DHCP 伺服器位置** – 選擇其中一個介面作爲 DHCP 伺服器介面。 **DHCP 伺服器 IP 位址** - 設定您想要使用的 DHCP 伺服器 IP 位址，讓 DHCP 中繼可以幫忙轉送 DHCP 需求至 DHCP 伺服器上。
套用	按此鈕儲存設定。
取消	按此鈕捨棄頁面設定。

4.2.2.3 歷史記錄

本頁顯示連線狀態的歷史紀錄資料(上線或是斷線)以及連線時間與登入此路由器的 PPPoE 伺服器的使用者名稱。



每個項目說明如下：

項目	說明
使用者名稱	顯示用來登入 PPPoE 伺服器的使用者名稱。

動作	顯示使用者帳號的連線狀態(上線或是斷線)。
時間	顯示連線的時間。 如果動作爲 “Down”，本區將會顯示全部的連線時間。 如果動作爲“up”，本區將會顯示使用者帳號登入 PPPoE 伺服器的時間點。

4.2.3 交換器

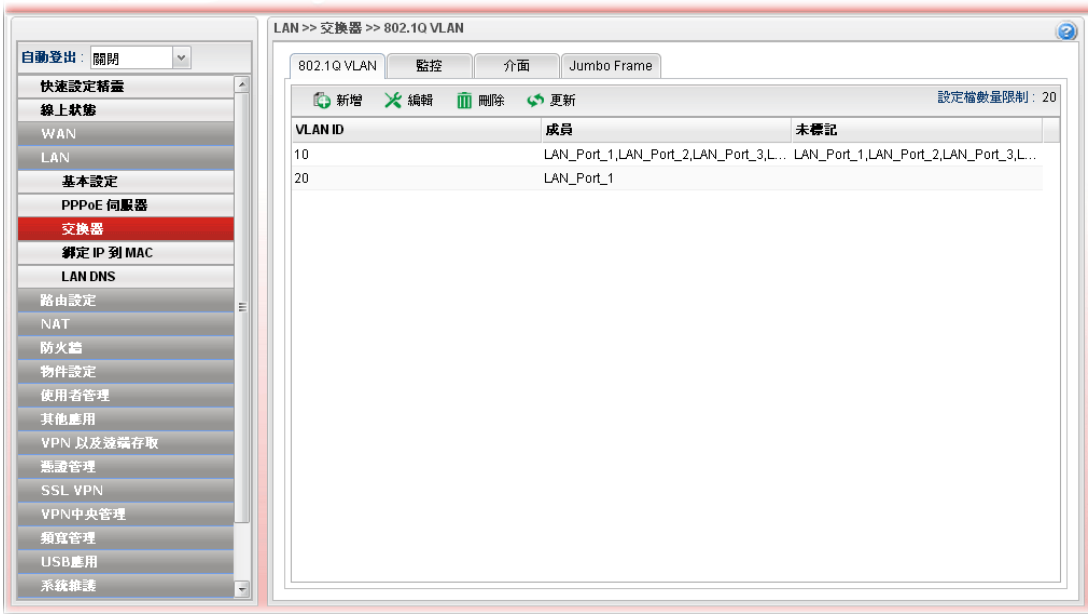
本頁讓您設定監控埠、被監控埠、啓用/停用 LAN 介面，以及針對不同 LAN 界面設定 802.1Q VLAN ID 等內容。

4.2.3.1 802.1Q VLAN

Virtual LANs (VLANs) 爲網路中符合邏輯且個別獨立的群組，這些群組彼此之間能夠有如實體網路連線般的互相溝通。不過 VLAN 並不受限於實際連接到網路中的傳統 LAN 區段等硬體限制，因此 VLAN 允許網路管理者將網路區分成符合邏輯思考但卻很有層次的結構。VLAN 可以透過應用程式或是部門別定義網路，例如在企業當中，公司可以針對多媒體使用者建立一個 VLAN；針對電子郵件使用者，公司可以針對工程部門另外建立一組 VLAN，針對來訪客戶則建立另一個群組，讓他們可以登入網際網路而非公司網路。VLANs 也可以依照公司的組織結構來設定，例如：公司董事長可能擁有專屬的 VLAN，其執行團隊可能擁有不同的 VLAN，而其餘同仁則歸屬於另外的 VLAN，即使是在相同的建築物下，這些 VLAN 可以依照不同公司而分別給予不同設定，節省金錢費用並減少設備的架設。

使用者可以選擇依些埠口來加入 VLAN 群組，在 VLAN 群組中，埠口數可以是單獨一個也可以設定多個。

VLAN 的目的是在隔離不同用戶之間的網路流量，可以提供更加的安全應用。



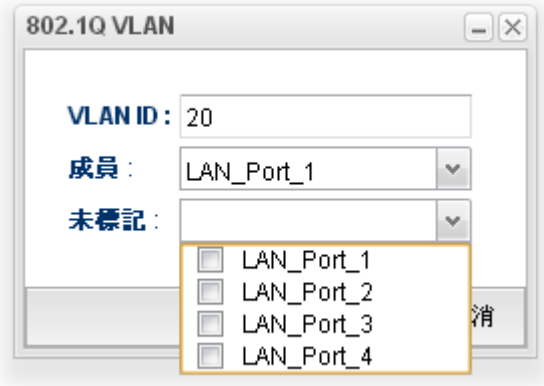
每個項目說明如下：

項目	說明
新增	新增新的 VLAN ID 設定檔。

編輯	修改選定的 VLAN ID 設定檔。 自既有的 VLAN ID 設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
刪除	移除選定的 VLAN ID 設定檔。 請選擇您想要刪除的既有 VLAN ID 設定檔，然後按下刪除按鈕，該設定檔即可被移除。
更新	重新更新本頁面。
設定檔數量限制	顯示可以建立的設定檔總數。
VLAN ID	顯示 VLAN ID 號碼。
成員	顯示含 VLAN ID 編號的 LAN 設定檔，其用來登入網際網路的 LAN 介面。
未標記	顯示不含標籤的 LAN 設定檔。

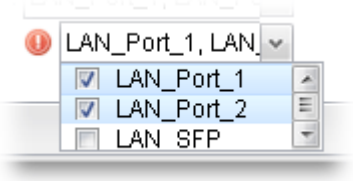
如何新增 802.1Q VLAN 設定檔

1. 開啓 **LAN>>交換器**並按下 **802.1Q VLAN** 標籤。
2. 按下**新增**按鈕。
3. 下述對話盒將出現在螢幕上。



可用參數詳列如下：

項目	說明
VLAN ID	輸入編號作爲 VLAN ID，這個編號乃是在 VLAN 中用以辨識身分的號碼，之後您還必須在準備納入相同 VLAN 群組的每台電腦上都輸入相同的號碼。
成員	決定此一含有 VLAN ID 編號的 LAN 設定檔所使用的 LAN 介面，用來登入網際網路。 如果 出現在下拉式清單的前端，即表示該選項已經被其他設定檔選定了，您已無法再次選擇該選項，如果您想要指定該項目，請離開此對話盒，自原始 VLAN 設定檔中釋放該選定的項目，然後到本頁重新選擇。

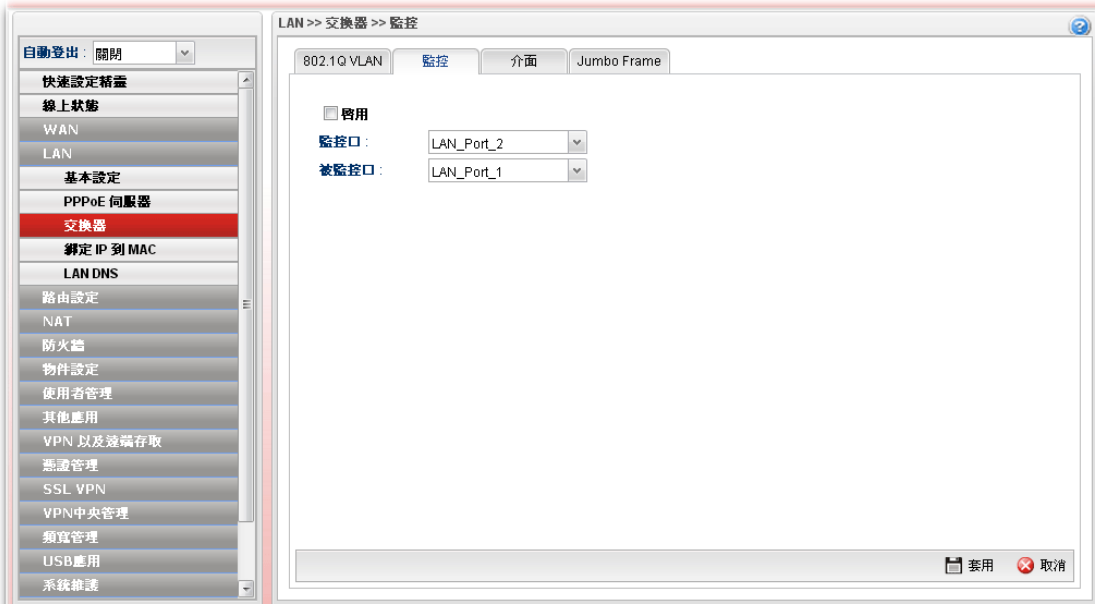
	
未標記	決定經由此 LAN 設定檔且含 VLAN ID 編號傳輸至網際網路的封包是否加上標籤。 如果 出現在下拉式清單的前端，即表示該選項已經被其他設定檔選定了，您已無法再次選擇該選項，如果您想要指定該項目，請離開此對話盒，自原始 VLAN 設定檔中釋放該選定的項目，然後到本頁重新選擇。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

4. 輸入所有設定之後，按下**套用**儲存，新增設定檔將立即顯示在螢幕上。

4.2.3.2 監控

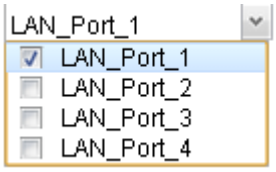
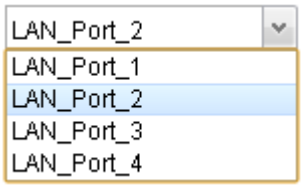
Vigor2960 支援 LAN 介面的埠號監控功能，此機制幫助管理者追蹤網路謬誤或是不正常的封包傳輸，但卻不會阻礙資料在網路上的運行，另外，使用者可以套用此功能來監控使用者想檢視的所有流量。

此功能包含數項特徵優勢，首先功能相當經濟實惠不需要加裝其他的偵測設備，其次可以同時檢視 VLAN 中一個以上監控埠內的資料，第三可以用來傳送受監控的資料至監控埠口的分析儀上，最後使用者介面很方便也很容易設定。



可用參數詳列如下：

項目	說明
啓用	勾選此框啓用監控功能。

監控口	選擇埠口用來檢視受監控埠口傳送過來的流量。 
被監控口	選擇被監控的埠口。 
套用	按此鈕儲存設定。
取消	按此鈕捨棄任何設定。

4.2.3.3 介面

本頁讓您分別修正 LAN 埠口的狀態(啓用/停用)、雙工(半/全)、速度以及 802.3az (啓用/停用)。

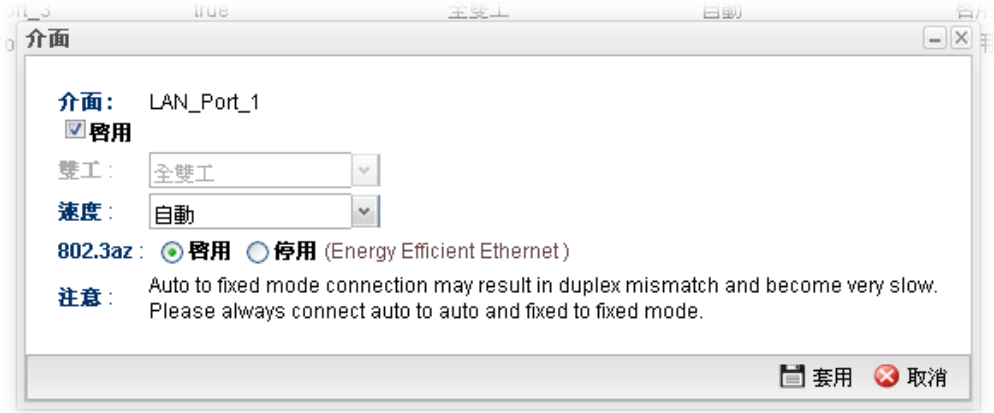
每個項目說明如下：

項目	說明
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
更新	重新更新本頁面。
介面	顯示介面名稱。
啓用	顯示設定檔狀態，False 表示停用；True 表示啓用。

雙工	顯示此設定檔使用的雙工爲全雙工或是半雙工。
速度	顯示設定檔的資料傳輸率(例如自動)。
802.3az	顯示此功能是否爲啓用。
注意	顯示此介面的附加資訊。

如何編輯介面設定檔

1. 開啓 **LAN>>交換器**並按下**介面**標籤。
2. 選擇想要編輯的設定檔，再按下**編輯**按鈕。
3. 出現如下畫面。



可用參數詳列如下：

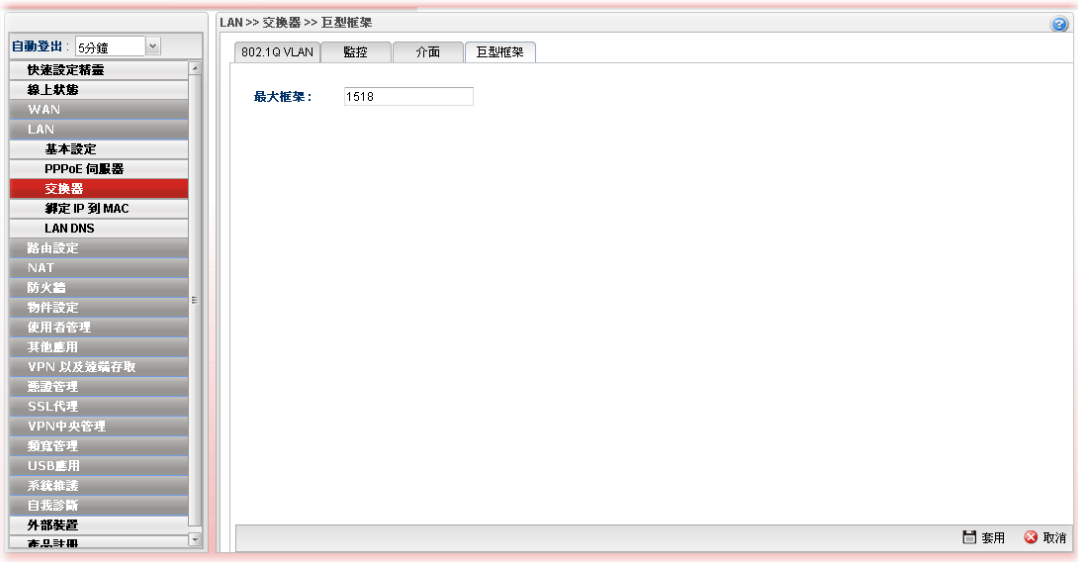
項目	說明
介面	顯示 LAN 界面設定檔名稱。
啓用	勾選此框啓用此功能。
雙工	選擇**全**或**半**。
速度	使用下拉式清單指定設定檔的傳輸率。 如果選擇**自動**，就不需要指定雙工設定。
802.3az	乙太網路節能特色。 能自動偵測網路流量以調整電源輸出，讓 Vigor2960 在使用量較低的時段內節省能源，避免浪費。
注意	顯示此介面的附加資訊。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

4. 輸入所有設定並按下**套用**儲存，完成設定檔編輯。

4.2.3.4 巨型框架(Jumbo Frame)

巨型框架的目的是透過加大資料的方式，加快來自 LAN 端的封包傳輸速率。

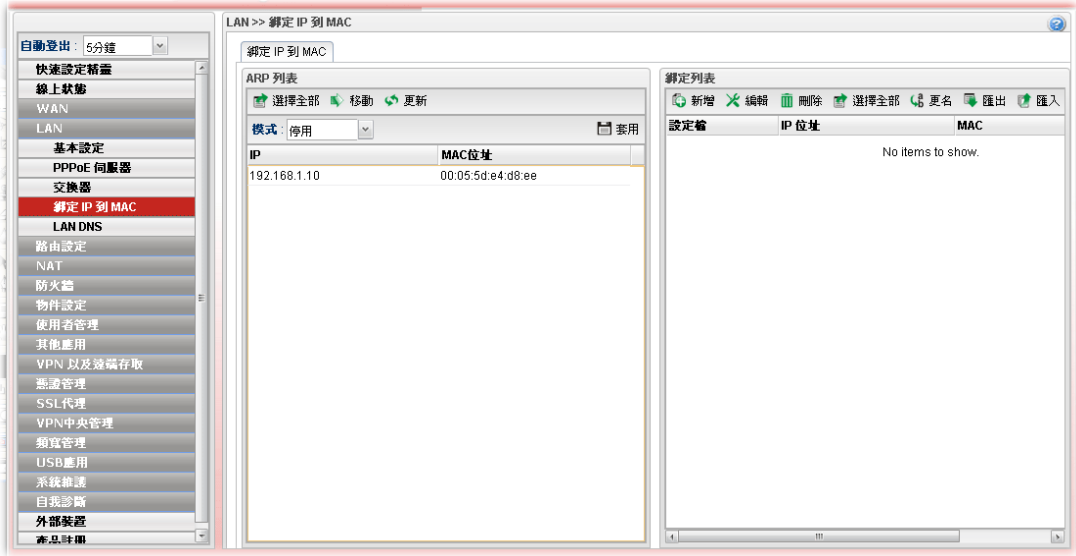
MTU (Max Transmit Unit) 決定了封包最大的尺寸大小，當大型封包透過 Vigor 路由器傳輸時，路由器會將其切割成數的區段以便易於傳送，但這往往會花費較多的時間，爲了減低傳送的次數、減少頻寬浪費並降低傳送的時間，可以使用巨型框架功能來加大資料的尺寸，加速來自 LAN 端封包的傳輸速率。



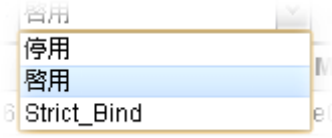
4.2.4 綁定 IP 到 MAC

此功能用於綁定 LAN 中 IP 與 MAC 位址以便在網路中取得有力控制。當此功能啓用時，所有分派的 IP 與 MAC 位址綁定者皆不會被變更，如果您修改綁定的 IP 或 MAC 位址，可能會造成無法登入網際網路。

本頁讓您設定與綁定 IP 到 MAC 功能有關的各式設定。

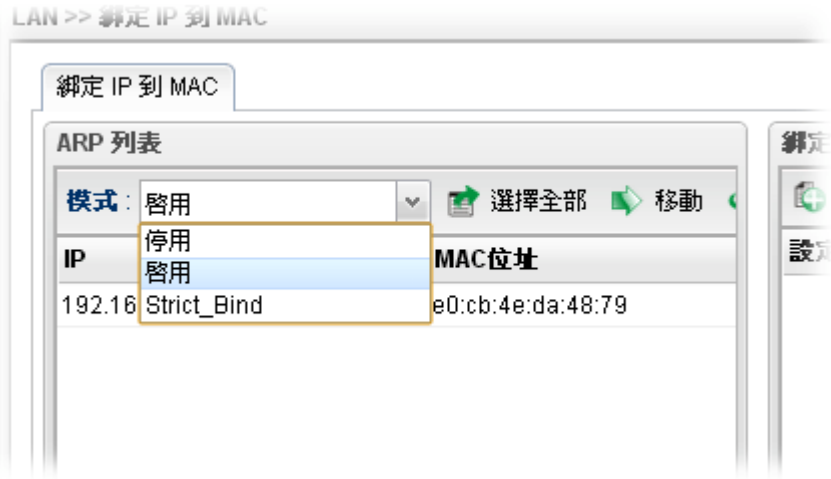


每個項目說明如下：

項目	說明
ARP 表格	此表格為路由器的 LAN 端 ARP 表格資料，IP 與 MAC 資訊將顯示在本區中，列於 ARP 表格中的每組 IP 與 MAC 位址，都可以藉由**移動**按鈕選擇加入**綁定表格**。 **選擇全部** - 讓您選擇列入 ARP 表格中的所有項目。 **移動** - 移動選定項目至**綁定表格**中。 **更新** - 用於更新 ARP 表格，當新 PC 加入 LAN 中時，您可以按此取得最新的 ARP 表格資訊。 **模式** -  ● **啓用** – 選此啓用此功能。不過未列入**綁定表格**中的 IP/MAC 無法登入網際網路。 ● **停用** – 選此停用此功能，本頁所有的設定將失效。 ● **Strict_Bind(嚴格綁定)** – 選擇此項可鎖住未列入**綁定表格**的 IP/MAC 連線。 **介面** – 若選擇嚴格綁定，請指定一個介面，預設值為 “lan1”。 **Syslog** - 若選擇嚴格綁定，您可勾選此方塊將相關紀錄儲存在 Syslog 中。 **套用** – 按此儲存設定。 **IP –** 顯示裝置的 IP 位址。 **MAC 位址 –** 顯示裝置的 MAC 位址。
綁定表格	顯示 IP 綁定 MAC 資訊清單。 **新增** - 讓您新增一組 IP/MAC 位址並顯示在**綁定表格**上。 **編輯** - 讓您編輯並修正先前建立的 IP 位址與 MAC 位址。 **刪除** - 您可以移除任何**綁定表格**上的項目，只要選擇該項目並按下**刪除**按鈕即可。 **選擇全部** - 一次選擇所有的項目。 **更名** -按此鈕後將會跳出視窗，讓您修改選定設定檔的檔名。在使用此功能之前，至少要有一個設定檔存在始可運作。 **匯出/匯入** – 匯出匯入綁定清單資料。 **設定檔 –** 顯示設定檔檔名。 **IP 位址 –** 顯示設定檔的 IP 位址。 **MAC –** 顯示設定檔的 MAC 位址。 **註解** – 顯示此設定檔的簡單說明。

如何設定綁定 IP 到 MAC

1. 開啓 **LAN>>綁定 IP 到 MAC**。
2. 使用**模式**下拉式清單指定適當的模式。



有三種模式可以選擇：

- **停用** – 選擇此項即停止綁定 IP 到 MAC 功能。
- **啓用** – 綁定表格中的特定 IP 位址將保留給綁定 MAC 位址的裝置使用，其他未列入榜定表格的裝置**仍可**自 DHCP 伺服器取得 IP 位址。
- **Strict_Bind** – 僅有指定 IP 位址將會分派予綁定 MAC 位址的裝置，其他未列入榜定表格的裝置**無法**自 DHCP 伺服器取得 IP 位址。

3. 按下**新增**。

4. 出現如下畫面。

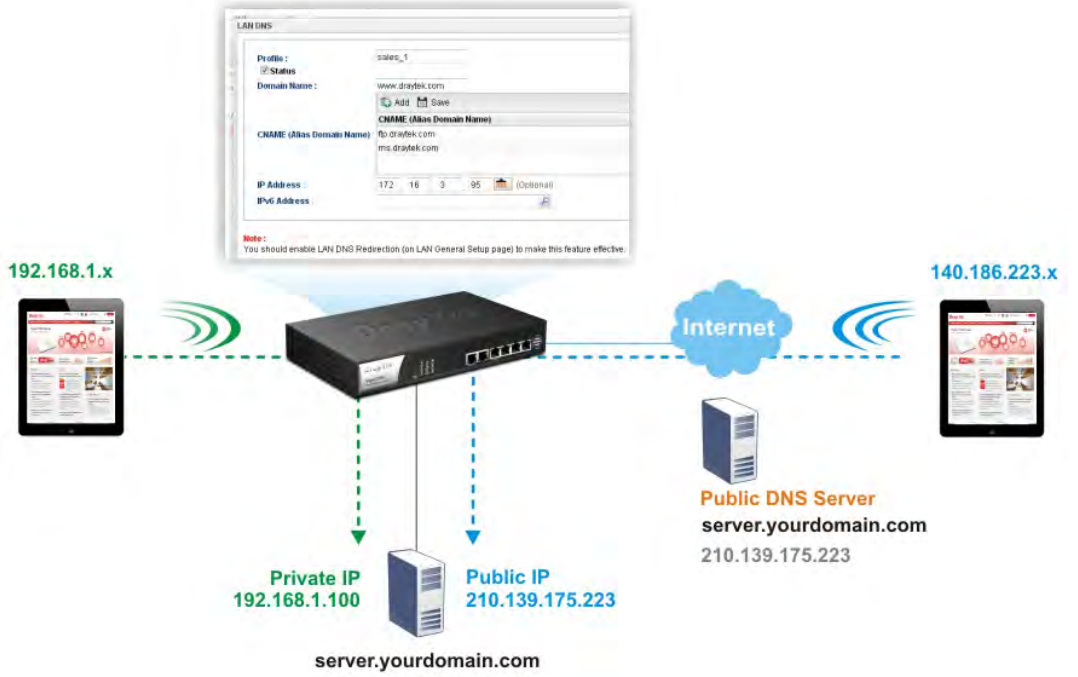
可用參數詳列如下：

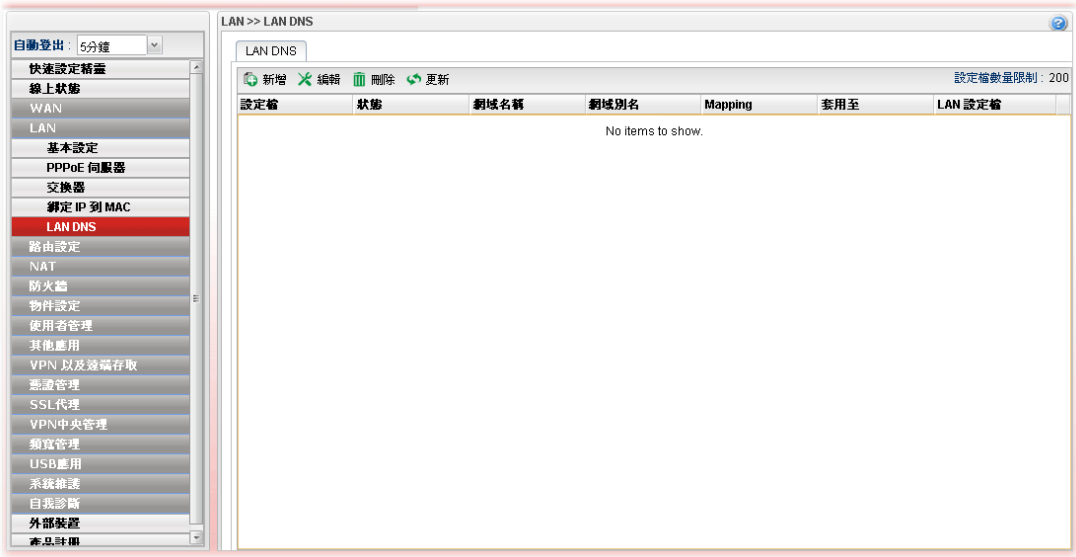
項目	說明
設定檔	輸入設定檔的檔名。
IP 位址	輸入用於搭配指定 MAC 位址的 IP 位址。
MAC	輸入 MAC 位址用來綁定分派得來的 IP 位址。
註解	輸入設定檔的簡易說明。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

5. 輸入所有設定並按下**套用**儲存。
6. 新的設定檔將會出現在**綁定表格**上。

4.2.5 LAN DNS

LAN DNS 是簡易版的 DNS 伺服器，使用者不需要在 LAN 端建立另一個 DNS 伺服器，透過此功能，使用者可以設定某些以網域名稱即可容易登入的服務(像是 FTP、WWW 或是資料庫等等)。





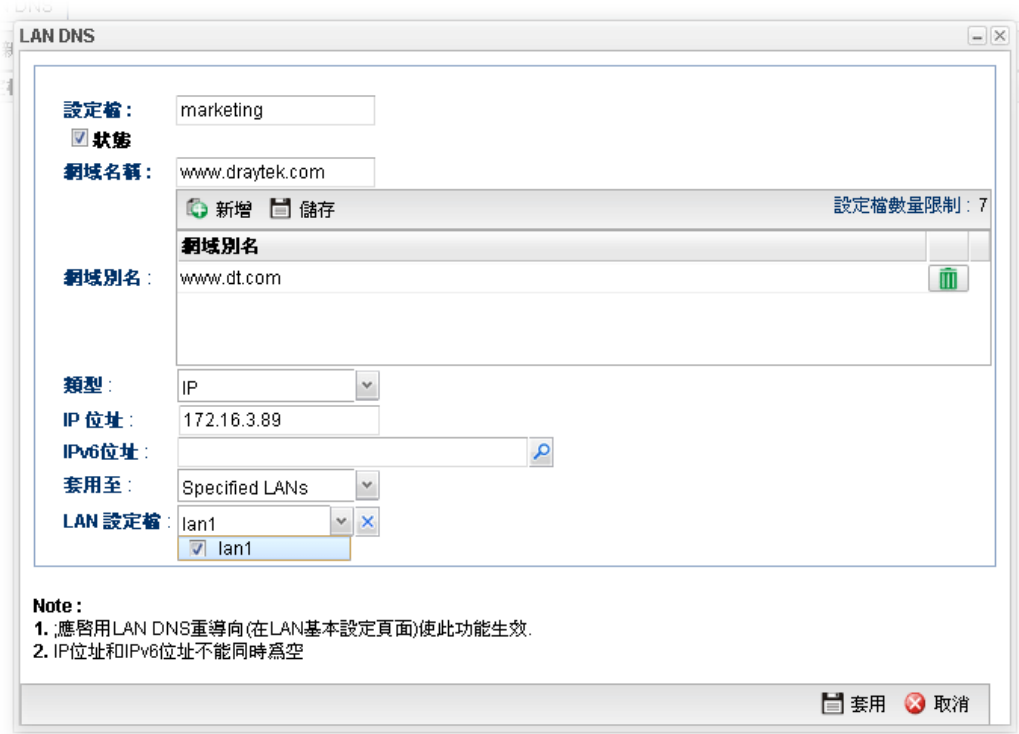
每個項目說明如下：

項目	說明
新增	新增新的設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。

刪除	移除選定的設定檔。 請選擇您想要刪除的既有設定檔，然後按下刪除按鈕，該設定檔即可被移除。
更新	重新更新本頁面。
設定檔數量限制	顯示可以建立的設定檔總數。
設定檔	顯示設定檔名稱。
狀態	顯示設定檔爲啓用(true)或是停用(false)。
網域名稱	顯示設定檔的網域名稱。
網域別名	顯示設定檔的別名網域名稱。
Mapping	顯示 LAN DNS 所指定的 IP 位址。
套用至	顯示 LAN DNS 所套用的 LAN 設定檔爲何。
LAN 設定檔	顯示網域名稱的 IP 位址。

如何新增 LAN DNS 設定檔

1. 開啓 **LAN>>LAN DNS**。
2. 按下**新增**按鈕。
3. 出現如下畫面。



可用參數詳列如下：

項目	說明
設定檔	輸入設定檔的檔名。

狀態	勾選此框啓用設定檔。
網域名稱	輸入設定檔所需的網域名稱。
網域別名	在本區中可以輸入數個網域名稱，LAN DNS 將重新導引網域名稱與網域別名至分派的 IP。 例如，網域名設定爲 www.draytek.com 且別名設定爲 www.dray.com，如果 IP 位址設定爲 192.168.1.123，那麼這二個設定 www.draytek.com 與 www.dray.com 都會被導引至 192.168.1.123。
類型	當您選擇 IP，您需要輸入 IP 位址與/或 IPv6 位址作爲對應目標。 當您選擇 CNAME，您需要輸入 CNAME 的內容作爲對應目標。 選擇類型以便決定是要對應至 IP 還是對應至 CNAME。
IP 位址	輸入 IP 位址，如此一來上述的網域名稱以及網域別名都會對應至此指定 IP 位址。
IPv6 位址	輸入 IPv6 位址，如此一來上述的網域名稱以及網域別名都會對應至此指定 IPv6 位址。
CNAME	輸入另外一組網域名稱，如此一來上述的網域名稱以及網域別名都會對應至此指定網域。
套用至	可選擇將此設定檔套往所有的 LAN 設定檔，或是指定某個 LAN 設定檔使用。 **LAN 設定檔-** 當您選擇 **Specified LANs** 時，需要再此指定至少一個 LAN 設定檔，來套用 LAN DNS。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

4. 輸入所有設定並按下**套用**儲存，新的設定檔將顯示在螢幕上。

4.3 路由設定

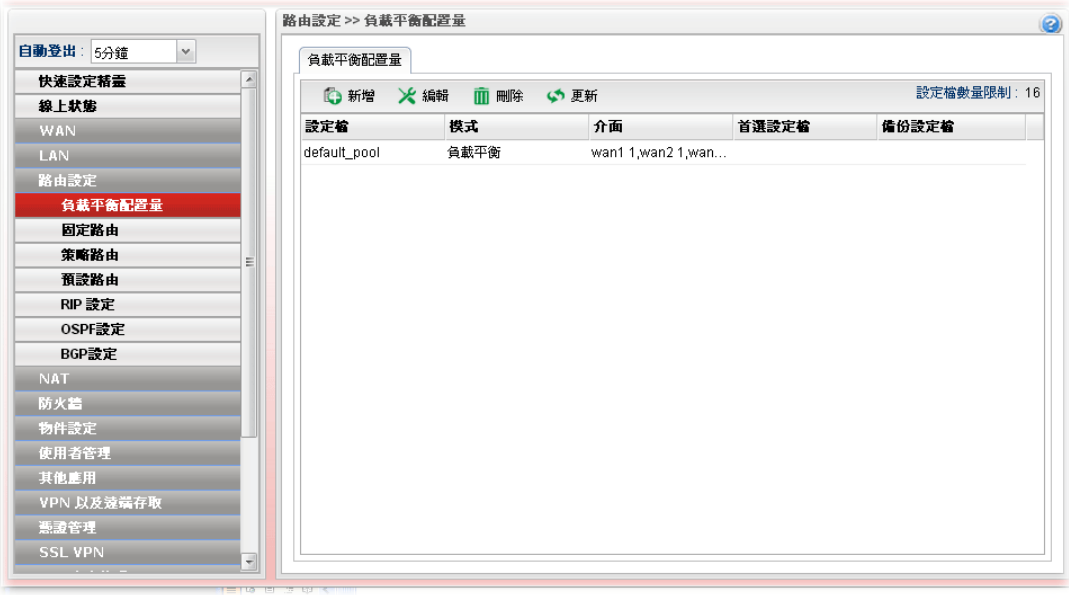
路由功能項目包含負載平衡配置量、固定路由、策略路由、預設路由、RIP 設定、OSPF 設定與 BGP 設定。

4.3.1 負載平衡配置量

Vigor2960 支援負載平衡功能，可透過協定類型、指定主機的 IP 位址、子網路的主機以及 WAN 介面的埠號範圍進行流量分派作業，基於負載平衡網頁的設定，使用者可以指定流量種類並強迫至指定的網路介面。

在**路由設定**選單中，請選擇**負載平衡配置量**功能選項。

本頁可讓使用者整合數個 WAN 設定檔，作爲負載平衡或是備援功能所需的配置量設定檔。此處所設定的檔案將應用在**路由設定>>預設路由**頁面中。



每個項目說明如下：

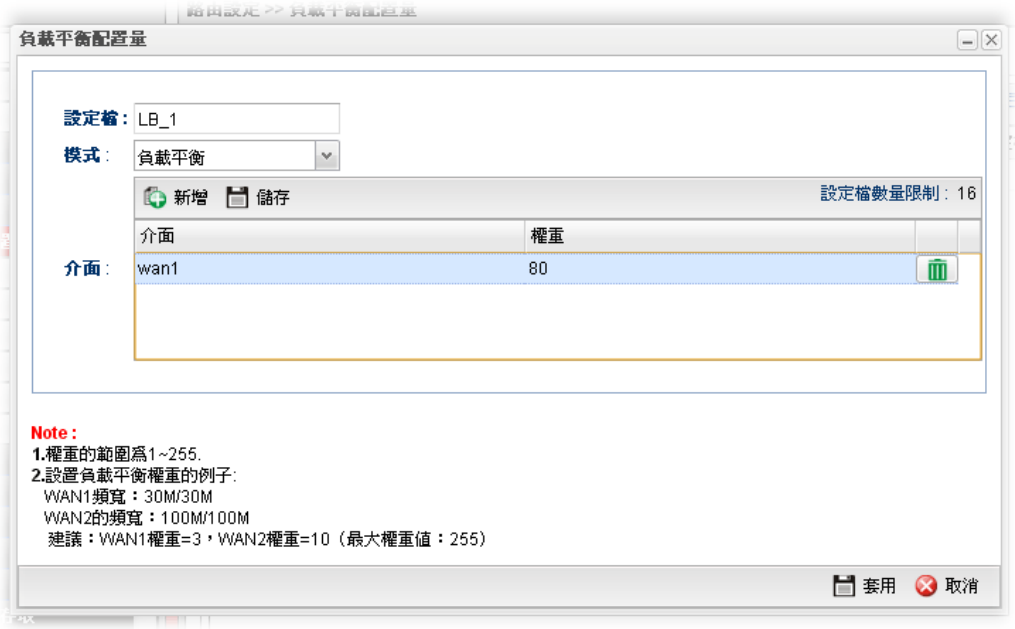
項目	說明
新增	新增新的配置量設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編

	輯按鈕，編輯視窗將會出現讓您修改內容。
刪除	移除選定的設定檔。 請選擇您想要刪除的既有設定檔，然後按下刪除按鈕，該設定檔即可被移除。
更新	重新更新本頁面。
設定檔	顯示設定檔名稱。
模式	顯示配置量設定檔使用的模式(備援或是負載平衡)。
介面	顯示負載平衡設定檔所搭配的 WAN 設定檔名稱。
首選設定檔	顯示備援設定檔選定的主要設定檔名稱。
備份設定檔	顯示備援設定檔選定的備份設定檔名稱。

有二種模式，**負載平衡**與**備援**，供您選擇作爲**配置量**設定檔模式，如果您選擇的是負載平衡，那麼**負載平衡**標籤將會顯示出來讓您針對不同的 WAN 介面進行不同的設定；如果您選擇的是備援，**備援**標籤將會顯示出來讓您指定首選設定檔以及備份設定檔。

如何新增配置量 - 負載平衡模式之設定檔

1. 開啓**路由設定>>負載平衡配置量**。
2. 按下**新增**按鈕開啓如下頁面，輸入設定檔名稱(例如 LB_1)並選擇**負載平衡**模式。



可用參數詳列如下：

項目	說明
設定檔	輸入設定檔的名稱。
模式	選擇**負載平衡**做爲**模式**選項。
介面	按下**新增**，新的輸入行將出現，供您輸入資料。 **介面**選項部分使用下拉式清單選擇 WAN 設定檔。接著輸入**權重**所需的數值。

3. 按下**套用**儲存設定，新的設定檔已建立完成。

如何新增配置量 - 備援模式之設定檔

此頁面讓您設定備援設定檔，此設定檔會在首選設定檔失效時自動啓用。

1. 開啓**路由設定>>負載平衡配置量**。
2. 按下**新增**按鈕開啓如下頁面，輸入設定檔名稱(例如 FL_1)並選擇**備援**模式。

可用參數詳列如下：

項目	說明
設定檔	輸入設定檔的名稱。
模式	選擇**備援**做爲**模式**選項。
首選設定檔	系統的預設值會直接套用首選設定檔，如果首選設定檔無法使用，備份設定檔將會取而代之。 使用下拉式清單選擇您需要的設定檔作爲首選設定檔。
備份設定檔	使用下拉式清單選擇您需要的設定檔作爲備份設定檔。

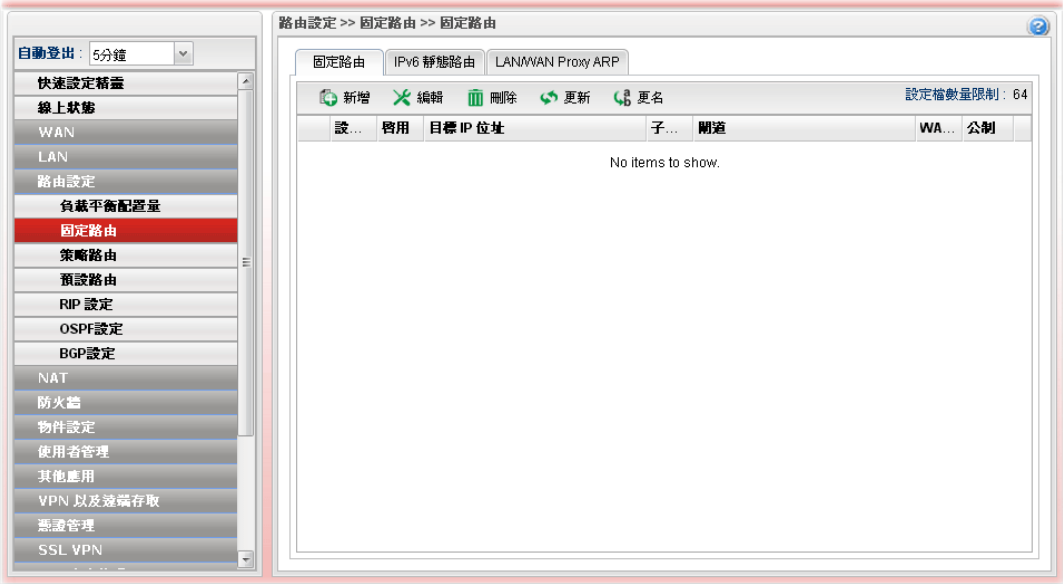
3. 按下**套用**儲存設定，新的設定檔已建立完成。

4.3.2 固定路由

當區域網路中有數個子網時，固定路由會比其他方法要來的有效率及快速。您只要簡單設定某個子網轉發資料至另一個指定子網的相關規則即可達成。

4.3.2.1 固定路由

路由器提供 IPv4 與 IPv6 協定讓您設定固定路由，這二種協定的設定頁面有些不同，請參考下述。



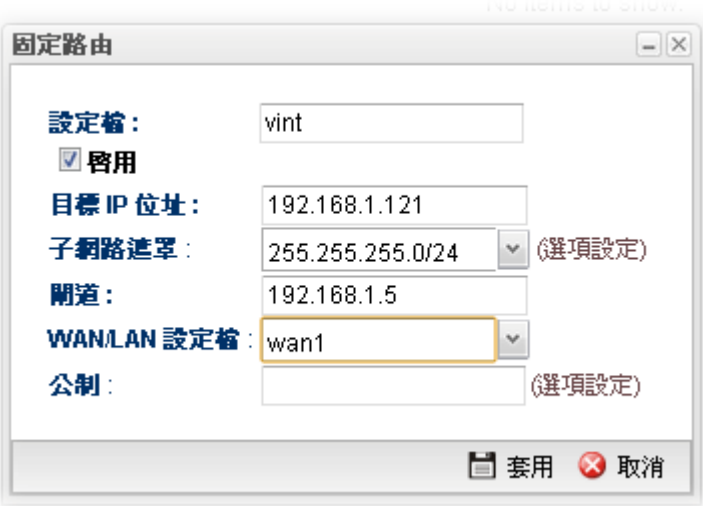
每個項目說明如下：

項目	說明
新增	新增新的設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
刪除	移除選定的設定檔。 請選擇您想要刪除的既有設定檔，然後按下刪除按鈕，該設定檔即可被移除。
更新	重新更新本頁面。
更名	按此鈕後將會跳出視窗，讓您修改選定設定檔的檔名。 在使用此功能之前，至少要有一個設定檔存在始可運作。
設定檔數量限制	顯示可以建立的設定檔的最高數目。
設定檔	顯示固定路由的名稱。
啓用	顯示設定檔狀態，False 表示停用；True 表示啓用。
目標 IP 位址	顯示設定檔的目標 WAN IP 位址。
子網遮罩	顯示固定路由設定檔的子網遮罩。

閘道	顯示固定路由設定檔的閘道位址。
WAN/LAN 設定檔	顯示閘道的子網 / LAN 或是 WAN 設定檔。
公制	顯示至目的的距離。

如何新增固定路由設定檔

1. 開啓**路由>>固定路由**並按下**固定路由**標籤。
2. 按下**新增按**鈕。
3. 下述頁面將會出現。



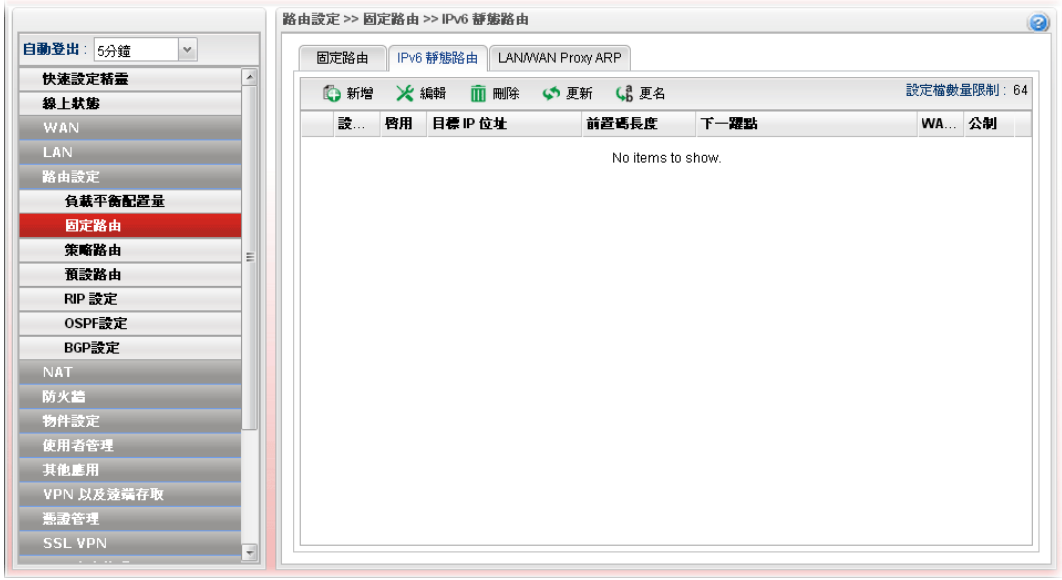
可用參數詳列如下：

項目	說明
設定檔	輸入固定路由設定檔的檔名。
啓用	勾選此框啓用此設定檔。
目標 IP 位址	輸入設定檔所需的 IP 位址。
子網路遮罩	使用下拉式清單選擇此固定路由設定檔所需的子網遮罩。
閘道	輸入此固定路由所需的閘道位址。
WAN/LAN 設定檔	選擇一個套用至此固定路由的 LAN/WAN 設定檔。
公制	輸入到目的的距離(通常以站-躍點來計算)。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

5. 輸入所有的設定然後按下**套用**儲存，新的設定檔將會呈現在螢幕上。

4.3.2.2 I IPv6 靜態路由

針對 IPv6 協定，請按 **IPv6 靜態路由**標籤設定細部的內容。



每個項目說明如下：

項目	說明
新增	新增新的設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
刪除	移除選定的設定檔。 請選擇您想要刪除的既有設定檔，然後按下刪除按鈕，該設定檔即可被移除。
更新	重新更新本頁面。
更名	按此鈕後將會跳出視窗，讓您修改選定設定檔的檔名。 在使用此功能之前，至少要有一個設定檔存在始可運作。
設定檔數量限制	顯示可以建立的設定檔的最高數目。
設定檔	顯示固定路由的名稱。
啓用	顯示設定檔狀態，False 表示停用；True 表示啓用。
目標 IP 位址	顯示設定檔的目標 WAN IP 位址。
前置碼長度	顯示設定檔的前置碼長度。
下一躍點	顯示此固定路由設定檔躍點位址。
WAN/LAN 設定檔	選擇一個套用至此固定路由的 LAN/WAN 設定檔。
公制	輸入到目的的距離。

如何新增 IPv6 固定路由設定檔

1. 開啓**路由>>靜態路由**並按下 **IPv6 靜態路由**標籤。
2. 按下**新增按**鈕。
3. 下述頁面將會出現。

可用參數詳列如下：

項目	說明
設定檔	輸入固定路由設定檔的檔名。
啓用	勾選此框啓用此設定檔。
目標 IP 位址	輸入設定檔所需的 IP 位址。
前置碼長度	輸入設定檔的前置碼長度。
下一躍點	輸入此固定路由設定檔下一個躍點位址。
WAN/LAN 設定檔	選擇一個套用至此固定路由的 LAN/WAN 設定檔。
公制	輸入到目的的距離(通常以站-躍點來計算)。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

4. 輸入所有的設定然後按下**套用**儲存，新的設定檔將會呈現在螢幕上。

4.3.2.3 LAN/WAN Proxy ARP

如果要讓區域網路端的裝置不透過 NAT 機制進入外部網路，或是讓遠端裝置登入區域網路裝置而不需透過路由器的 NAT 機制，可使用 IP 路由功能來達成您的要求。

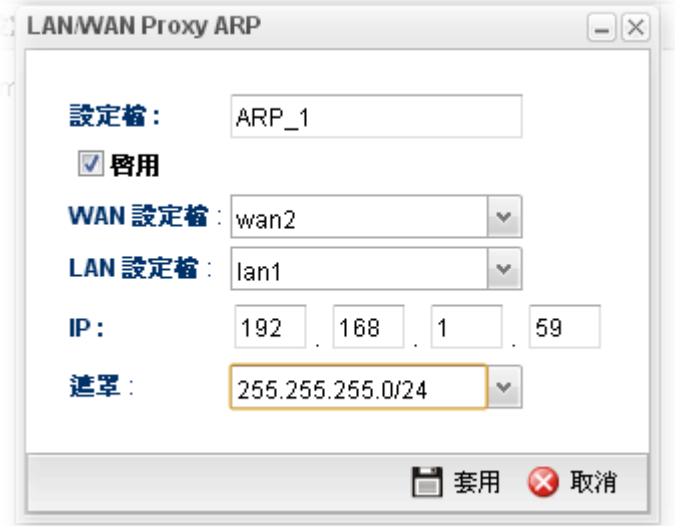
通常區域網路端的裝置會被分派一組公用 IP 位址或是一組跟指定 WAN 相同子網的 IP 位址。當區域網路裝置嘗試傳送資料封包出去的時候，路由器將會透過該特定 WAN 界面來進行傳送，無須經過 NAT 機制的處理，同時遠端裝置也可以直接登入區域網路裝置，不會有任何的問題。

每個項目說明如下：

項目	說明
新增	新增新的設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
刪除	移除選定的設定檔。 請選擇您想要刪除的既有設定檔，然後按下刪除按鈕，該設定檔即可被移除。
更新	重新更新本頁面。
更名	按此鈕後將會跳出視窗，讓您修改選定設定檔的檔名。 在使用此功能之前，至少要有一個設定檔存在始可運作。
設定檔數量限制	顯示可以建立的設定檔的最高數目。
設定檔	顯示設定檔的名稱。
啓用	顯示設定檔狀態，False 表示停用；True 表示啓用。
WAN 設定檔	顯示此 ARP 設定檔所用的 WAN 設定檔。
LAN 設定檔	顯示此 ARP 設定檔所用的 LAN 設定檔。
IP	顯示此 ARP 設定檔所用的 IP 位址。
遮罩	顯示此 ARP 設定檔所用的遮罩位址。

如何新增伺服器 ARP 設定檔

1. 開啓**路由>>固定路由**並按下 **LAN/WAN Proxy ARP** 標籤。
2. 按下**新增按**鈕。
3. 下述頁面將會出現。



可用參數詳列如下：

項目	說明
設定檔	輸入設定檔的檔名。
啓用	勾選此框啓用此設定檔。
WAN 設定檔	選擇所需的 WAN/USB 設定檔。
LAN 設定檔	選擇所需的 LAN 設定檔。
IP	輸入此設定檔的 IP 位址。T
遮罩	使用下拉式選單指定遮罩位址。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

4. 輸入所有的設定然後按下**套用**儲存，新的設定檔將會呈現在螢幕上。

4.3.3 策略路由

策略路由(又稱爲 PBR - policy-based routing)功能意指您可能需要針對路由設定一系列的策略，之後傳送的封包若符合策略定義中的任何一條規則，即可透過路由器導往指定的介面。您可以依照各種理由條件進行路由設定，像是負載平衡、安全性傳輸、路由方向的決定等等。

透過協定、模式、IP 位址、埠號與介面設定，策略路由可用於設定各種路由規則以因應實際的需要。一般來說可達成如下的目的：

- 自動負載平衡以降低網路流量的負擔

  您必須手動建立路由規則以便強迫流量轉至特定的網路介面。

- 嚴格綁定效果

  透過指定介面(如 WAN/LAN)，資料可以從來源 IP 傳送至目的 IP。

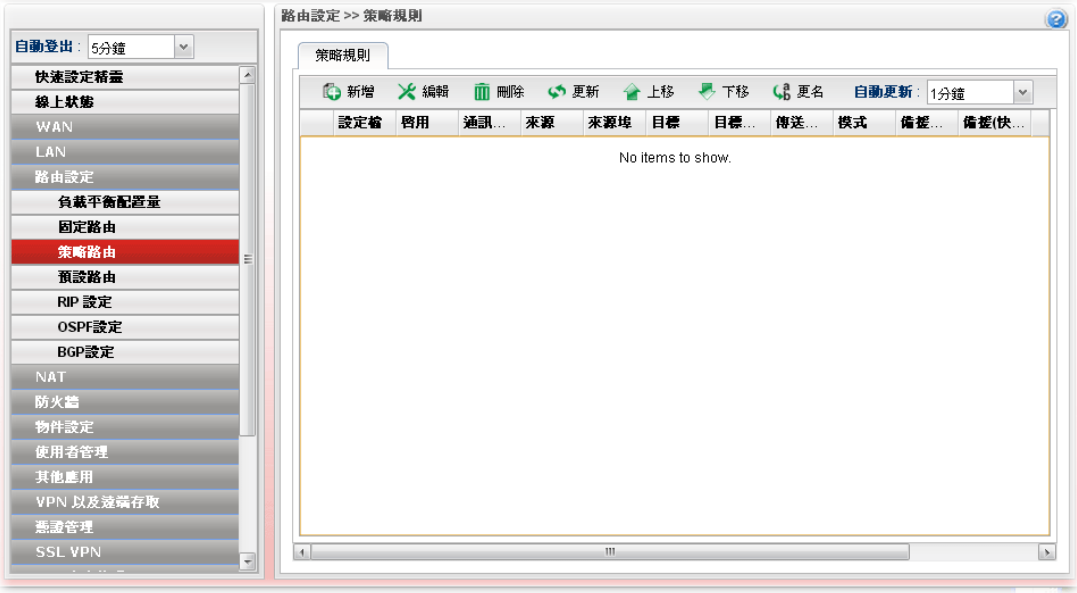
- 位址對映

  讓您針對內部虛擬 IP 或是 IP 群組指定對外的 WAN IP 位址。

- 其他路由目的

  指定路由規則以便決定資料傳送的方向等等。

附註：有關使用策略路由的詳細資訊，可以造訪居易網站 www.draytek.com，有關技術支援/應用說明等內容。



可用參數詳列如下：

項目	說明
新增	新增新的設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。

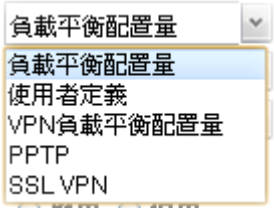
刪除	移除選定的設定檔。 請選擇您想要刪除的既有設定檔，然後按下刪除按鈕，該設定檔即可被移除。
更新	重新更新本頁面。
上移	將設定檔往上移動改變選定設定檔的順序。
下移	將設定檔往下移動改變選定設定檔的順序。
更名	按此鈕後將會跳出視窗，讓您修改選定設定檔的檔名。 在使用此功能之前，至少要有一個設定檔存在始可運作。
自動更新	指定更新時間間隔以取得最新的狀態，若您按下**更新**按鈕，系統將立即更新資訊並呈現出來。
設定檔	顯示設定檔的名稱。
啓用	顯示設定檔狀態，False 表示停用；True 表示啓用。
通訊協定	顯示此規則的通訊協定。
來源	顯示來源子網/IP 物件/IP 群組的名稱。
來源埠	顯示來源埠號範圍。
目標	顯示子網/IP 物件/ IP 群組/DNS 物件的名稱。
目標埠	顯示目標埠號範圍。
傳送規則	顯示選擇的路由方式(流量轉發送)。
模式	顯示此策略路由使用的路由模式(NAT 或是路由)。
備援至下一個規則	顯示此功能的狀態(啓用或是停用)。
備援(快速回復)	顯示此功能的狀態(啓用或是停用)。

如何新增策略路由

1. 開啓**路由>>策略路由**。
2. 按下**新增**按鈕。
3. 對話盒出現如下：

可用參數詳列如下：

項目	說明
設定檔	輸入規則設定檔名稱。
啓用	勾選此框啓用此設定檔。
優先順序	選擇適合此設定檔的優先順序(頂端、高、一般)
通訊協定	選擇任一協定 (全部、TCP、UDP、TCP/UDP、ICMP) 以便套用，**全部**爲預設值。
Source	**來源類型** - 選擇一種來源類型(所有、子網或是物件)

	每種類型都會帶出不同的設定功能介面。
	當來源類型爲子網時
	● **IP 位址** - 輸入一組 IP 位址作爲來源 IP 位址。 ● **子網遮罩**- 使用下拉式清單選擇來源 IP 需求的子網路遮罩。
	當來源類型爲物件時
	● **IP 物件** – 使用下拉式清單選擇來源 IP 物件。 ● **IP 群組** – 使用下拉式清單選擇來源 IP 群組。
Destination	**目標類型** - 選擇一種來源類型(所有、子網、物件或是國家) 每種類型都會帶出不同的設定功能介面。
	當目標類型爲子網時
	● **IP 位址** - 輸入一組 IP 位址作爲目標 IP 位址。 ● **子網遮罩**- 使用下拉式清單選擇目標 IP 需求的子網路遮罩。
	當目標類型爲物件時
	● **IP 物件** – 使用下拉式清單選擇目標 IP 物件。 ● **IP 群組** – 使用下拉式清單選擇目標 IP 群組。 ● **DNS 物件** – 使用下拉式清單選擇 DNS 物件。
	當目標類型爲國家時
	● **國家物件** – 使用下拉式清單選擇目標**國家**物件。
Route Rule	**傳送規則**-決定接收的流量轉往他處的方式。  **負載平衡配置量** –接收之流量將會轉到指定 WAN 介面或是負載平衡配置量處。 **使用者定義** – 接收之流量將會轉到指定 WAN 或 LAN 介面以及閘道位址。 **VPN 負載平衡配置量**– 接收之流量將會轉到指定的 VPN trunk 設定檔。 **PPTP** – 接收之流量將會轉到指定的 PPTP VPN 設定檔。 **SSL VPN** – 接收之流量將會轉到指定的 SSL VPN 設定檔。
	當傳送規則爲負載平衡配置量時

- **負載平衡規則** - 選擇任何一個設定檔套用此規則，其中 wan1 到 wan2 設定檔爲系統預設，另外您在 **路由>>負載平衡 配置量**所設定的設定檔也會在此顯示出來。
- **模式** – 指定此規則使用的模式 (NAT 或是路由) 。
- **使用 IP 別名** – 按**啓用**來啓用此功能，或是按**停用**關閉此功能。當啓用了此功能之後，請選擇一組 WAN IP 別名以取代預設的 WAN IP 位址。
- **備援至下一個規則**- 當指定的介面因爲某些原因中斷了連線，路由器將會自動使用下一個符合策略路由的規則來進行資料轉送。按下**啓用**開啓此**規則**，或是按**停用**關閉此功能。
  - **When interface down** – 若指定介面(傳送規則選定的介面)連線中斷，路由器即利用下一個符合策略的規則進行資料傳送。
  - **When target …..**- 當某個指定的 IP 或是網域連線成功/失敗並經過數秒時，路由器將視此指定介面(傳送規則選定的介面)連線中斷。例如您設定內容爲

    傳送規則 = 使用者自訂

    傳送介面 = wan1

    備援至下一個規則 = 啓用

    when target [8.8.8.8] ping [Fail] for [5] seconds

    即表示即使 wan1 一直保持連線狀態，只要 wan1 有 5 秒 ping 不到[8.8.8.8]，那麼路由器系統就會立刻執行備援至下一個符合策略的規則。
- **備援(快速回復)** – 當指定介面重新連線了，透過其他介面的網路流量將會立即受到干擾，路由器會再次使用原先指定的介面進行資料轉送。按下**啓用**開啓此**規則**，或是按**停用**關閉此功能。

當傳送規則爲使用者定義時

- **傳送介面** - 選擇一組設定檔套用此規則，其中 wan1 到 wan2 設定檔爲系統預設。
- **傳送(閘道)** – 輸入 IP 位址作爲閘道，注意 LAN 介面沒有預設閘道值，您必須在選擇 LAN 作爲傳送介面之前，先指定閘道位址才能使用。
- **模式** – 指定此規則使用的模式 (NAT 或是路由) 。
- **使用 IP 別名** – 按**啓用**來啓用此功能，或是按

	停用關閉此功能。當啓用了此功能之後，請選擇一組 WAN IP 別名以取代預設的 WAN IP 位址。 ● 備援至下一個規則- 當指定的介面因爲某些原因中斷了連線，路由器將會自動使用下一個符合策略路由的規則來進行資料轉送。按下**啓用**開啓此**規則**，或是按**停用**關閉此功能。 ◆ **When interface down** – 若指定介面(傳送規則選定的介面)連線中斷，路由器即利用下一個符合策略的規則進行資料傳送。 ◆ **When target …..**- 當某個指定的 IP 或是網域連線成功/失敗並經過數秒時，路由器將視此指定介面(傳送規則選定的介面)連線中斷。例如您設定內容爲 **傳送規則 = 使用者自訂** **傳送介面 = wan1** **備援至下一個規則 = 啓用** **when target [8.8.8.8] ping [Fail] for [5] seconds** 即表示即使 wan1 一直保持連線狀態，只要 wan1 有 5 秒 ping 不到[8.8.8.8]，那麼路由器系統就會立刻執行備援至下一個符合策略的規則。 ● 備援(快速回復) – 當指定介面重新連線了，透過其他介面的網路流量將會立即受到干擾，路由器會再次使用原先指定的介面進行資料轉送。按下**啓用**開啓此**規則**，或是按**停用**關閉此功能。
	當傳送規則爲 **VPN** 負載平衡配置量時
	● 負載平衡配置量 – IPsec VPN trunk 設定檔可以用於策略路由，使用之前，請先在 **VPN 與遠端存取>>VPN TRUNK 管理>>負載平衡配置量**頁面設定好 VPN TRUNK 設定檔。 ● 模式 – 指定此規則使用的模式 (NAT 或是路由) 。 ● 備援至下一個規則- 當指定的介面因爲某些原因中斷了連線，路由器將會自動使用下一個符合策略路由的規則來進行資料轉送。按下**啓用**開啓此**規則**，或是按**停用**關閉此功能。 ◆ **When interface down** – 若指定介面(傳送規則選定的介面)連線中斷，路由器即利用下一個符合策略的規則進行資料傳送。 ◆ **When target …..**- 當某個指定的 IP 或是網域連線成功/失敗並經過數秒時，路由器將視此指定介面(傳送規則選定的介面)連線

中斷。例如您設定內容為

傳送規則 = 使用者自訂

傳送介面 = wan1

備援至下一個規則 = 啓用

when target [8.8.8.8] ping [Fail] for [5] seconds

即表示即使 wan1 一直保持連線狀態，只要 wan1 有 5 秒 ping 不到[8.8.8.8]，那麼路由器系統就會立刻執行備援至下一個符合策略的規則。

- **備援(快速回復) –** 當指定介面重新連線了，透過其他介面的網路流量將會立即受到干擾，路由器會再次使用原先指定的介面進行資料轉送。按下**啓用**開啓此**規則**，或是按**停用**關閉此功能。

當傳送規則為 PPTP 時

- **PPTP 設定檔 – VPN PPTP 撥出與 VPN PPTP 撥入**設定檔可以用於策略路由。
- **模式** – 指定此規則使用的模式 (NAT 或是路由) 。
- **備援至下一個規則**- 當指定的介面因為某些原因中斷了連線，路由器將會自動使用下一個符合策略路由的規則來進行資料轉送。按下**啓用**開啓此**規則**，或是按**停用**關閉此功能。
  - **When interface down** – 若指定介面(傳送規則選定的介面)連線中斷，路由器即利用下一個符合策略的規則進行資料傳送。
  - **When target …..**- 當某個指定的 IP 或是網域連線成功/失敗並經過數秒時，路由器將視此指定介面(傳送規則選定的介面)連線中斷。例如您設定內容為

    傳送規則 = 使用者自訂

    傳送介面 = wan1

    備援至下一個規則 = 啓用

    when target [8.8.8.8] ping [Fail] for [5] seconds

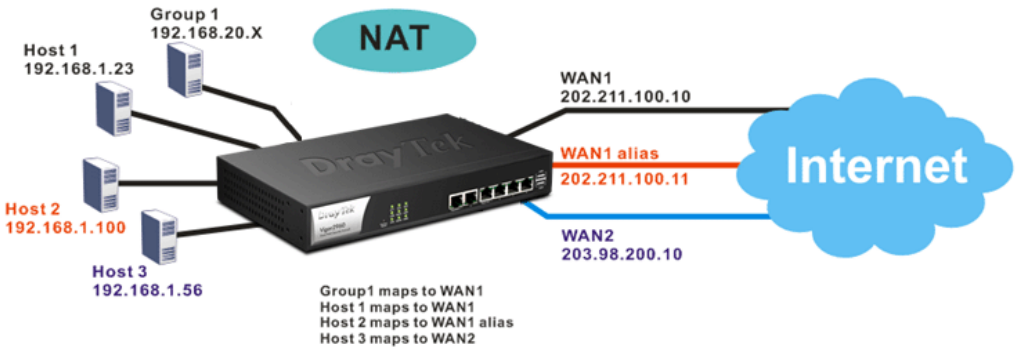
    即表示即使 wan1 一直保持連線狀態，只要 wan1 有 5 秒 ping 不到[8.8.8.8]，那麼路由器系統就會立刻執行備援至下一個符合策略的規則。
- **備援(快速回復) –** 當指定介面重新連線了，透過其他介面的網路流量將會立即受到干擾，路由器會再次使用原先指定的介面進行資料轉送。按下**啓用**開啓此**規則**，或是按**停用**關閉此

	功能。
	當傳送規則爲 SSL VPN 時
	● **SSL Profile – VPN SSL** 設定檔可以用於策略路由。 ● **模式** – 指定此規則使用的模式 (NAT 或是路由) 。 ● **備援至下一個規則**- 當指定的介面因爲某些原因中斷了連線，路由器將會自動使用下一個符合策略路由的規則來進行資料轉送。按下**啓用**開啓此**規則**，或是按**停用**關閉此功能。 ◆ **When interface down** – 若指定介面(傳送規則選定的介面)連線中斷，路由器即利用下一個符合策略的規則進行資料傳送。 ◆ **When target …..**- 當某個指定的 IP 或是網域連線成功/失敗並經過數秒時，路由器將視此指定介面(傳送規則選定的介面)連線中斷。例如您設定內容爲 **傳送規則 = 使用者自訂** **傳送介面 = wan1** **備援至下一個規則 = 啓用** **when target [8.8.8.8] ping [Fail] for [5] seconds** 即表示即使 wan1 一直保持連線狀態，只要 wan1 有 5 秒 ping 不到[8.8.8.8]，那麼路由器系統就會立刻執行備援至下一個符合策略的規則。 ● **備援(快速回復)** – 當指定介面重新連線了，透過其他介面的網路流量將會立即受到干擾，路由器會再次使用原先指定的介面進行資料轉送。按下**啓用**開啓此**規則**，或是按**停用**關閉此功能。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

4. 輸入所有必要設定然後按下**套用**，新規則設定檔將會出現在畫面上。

範例 1: 如何使用策略路由設定位址對映

址對映可用來將 NAT 子網中指定的虛擬 IP 或是某個範圍內的虛擬 IP，對映到某個指定的 WAN IP(或是 WAN IP 別名)，參考下圖：



假設路由器的 WAN 端設定如下：

WAN1: 202.211.100.10, WAN1 別名: 202.211.100.11

WAN2: 203.98.200.10

在沒有對映功能的情況下，IP 位址爲"192.168.1.10" 的 NAT 主機傳送封包到 WAN 端(或是網際網路)時，NAT 主機的來源位址不是對映到 202.211.100.10 就是對映到 203.98.200.10(使用哪個 IP 或是如何對映由內部負載平衡演算機制來決定)。

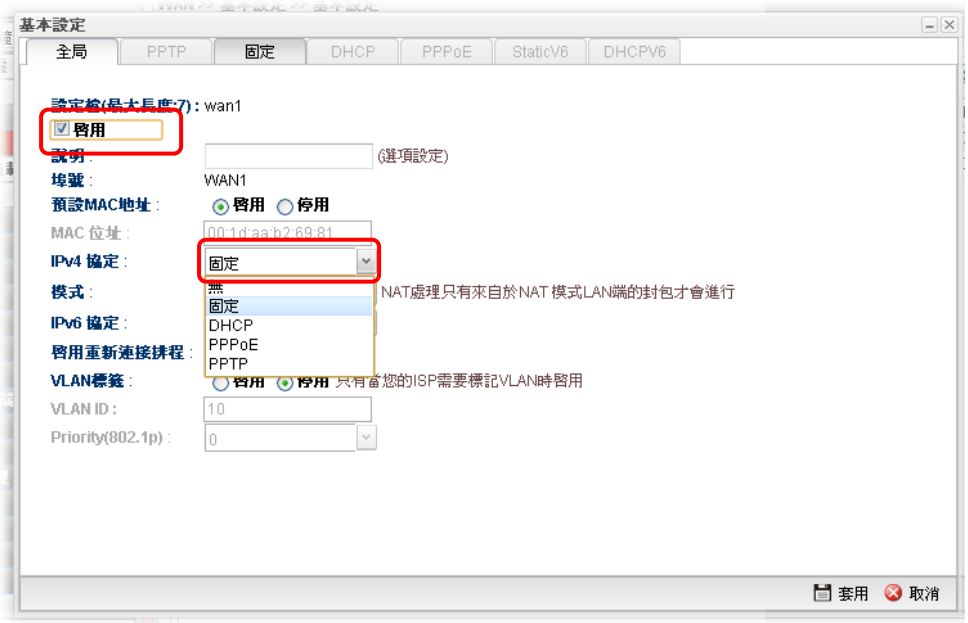
透過位址對映功能，您可以手動設定任何主機對映到任何的 WAN 界面，以便因應實際的需要。在上面的示意圖當中，您可以將 NAT Host 1 設定爲永遠對映到 202.211.100.10 (WAN1)；Host 2 則永遠對映到 202.211.100.11 (WAN1 別名)；Host 3 則永遠對映到 203.98.200.10 (WAN2)；Group 1 則永遠對映到 202.211.100.10 (WAN1)。

NAT 位址對映功能可讓您針對一組或是一群對內 IP 位址指定一組對外 IP 位址。

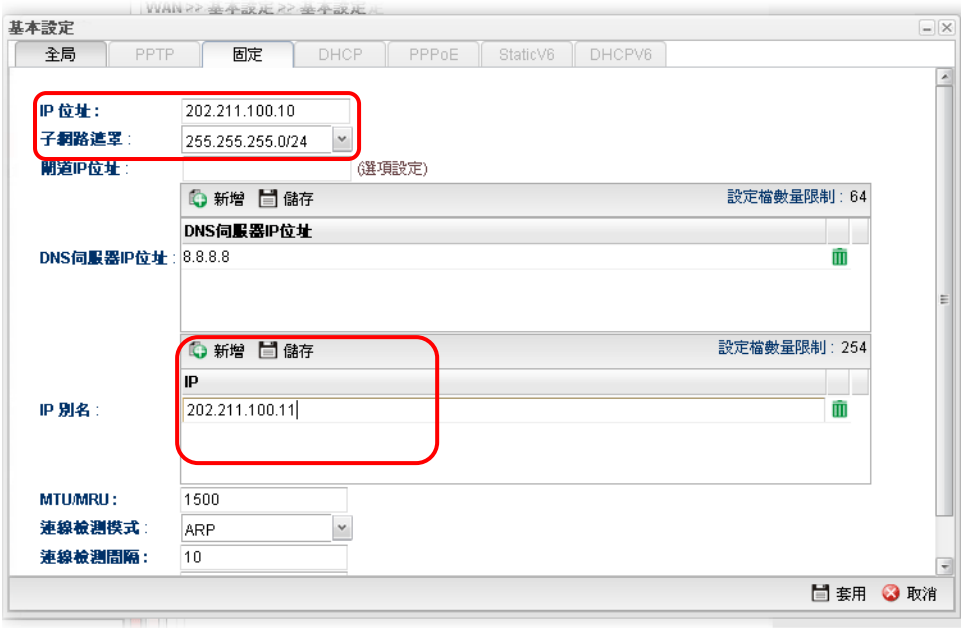
下列步驟將說明如何使用此功能。

1. 登入 Vigor2960 的使用者設定介面。

2. 開啓 **WAN>>基本設定**，針對 WAN1 請選擇 wan1 項目然後按下**編輯**，接著選擇**固定**作爲 **IPv4 協定**。

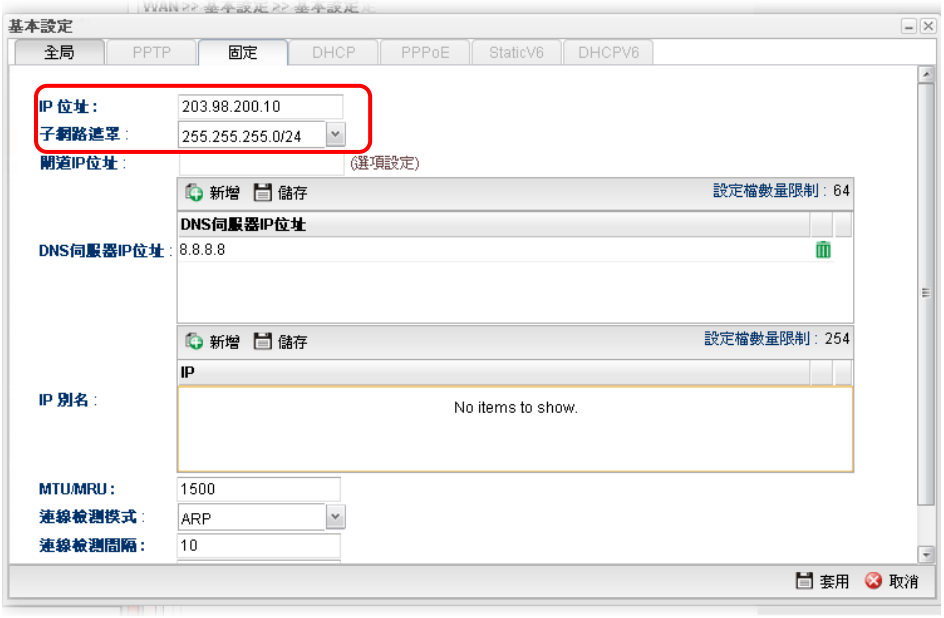


3. 在下列設定頁面中，請將主要 WAN IP 位址設定爲 *202.211.100.10.*。



在 IP 別名區域中按下新增，設定另外的 IP 位址(如 *202.211.100.11*)。

4. 完成 WAN1 設定之後，繼續設定 WAN2 的內容，此時 IP 位址應設定為 *“203.98.200.10”*。



5. 開啓**物件設定>>IP 物件**並按下**新增**建立一個新的 IP 物件設定檔。如下圖所示請輸入必要的內容，按下**套用**儲存剛剛的設定。

6. 開啓**路由>>策略路由**，按下**新增**建立新的設定檔。

7. 在如下頁面中，勾選**啓用**方塊，選擇**物件**作爲**來源類型**，選擇 IP_range 作爲 **IP 物件**，接著按下**套用**儲存設定。

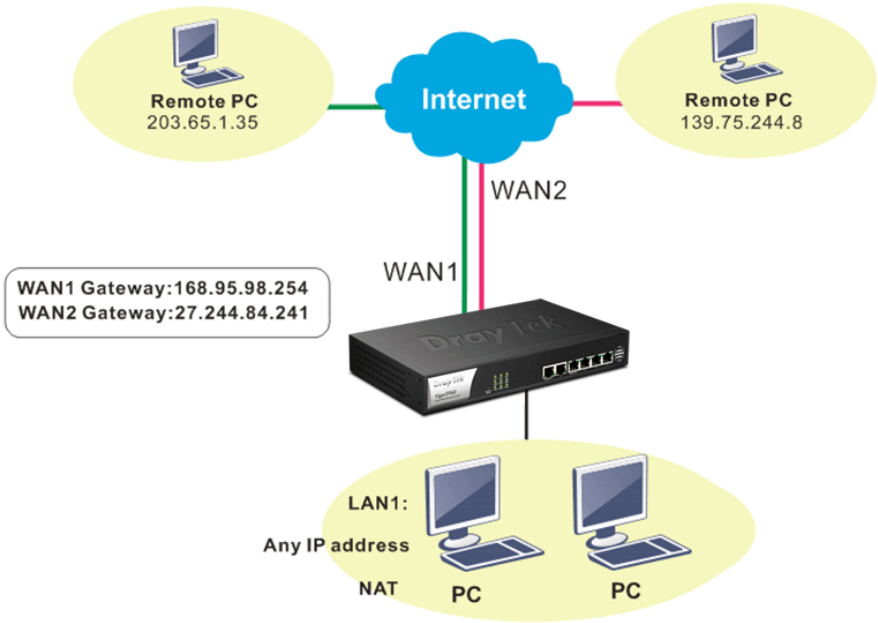
再設定另一個設定檔：

8. 完成了上述設定之後，您已經對某些電腦設定資料輸出的 IP 位址。

現在，特定電腦已經與某些 WAN IP 位址綁定，以利資料對外傳送。

範例 2：如何使用策略路由設定負載平衡

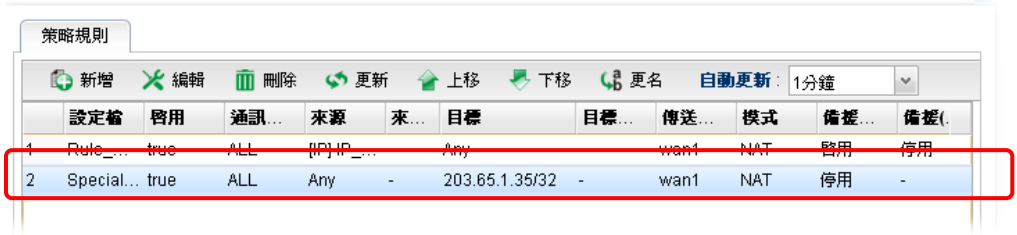
下圖顯示簡易的負載平衡運用，WAN1 和 WAN2 可以用來登入網際網路，在 LAN1 端的電腦可以透過 WAN1 傳送資料到遠端電腦上。



1. 登入 Vigor2960 的使用者設定介面。
2. 開啓**路由>>策略路由**，按下**新增**建立新的設定檔。

3. 在如下頁面中，輸入此設定檔的檔名，勾選**啓用**，選擇**子網**作爲**目標類型**，IP 位址則輸入 203.65.1.35，選擇**負載平衡配置量**作爲**傳送規則**，選擇 WAN1 作爲負載平衡規則，**備援至下一個規則項目**則按下**停用**。

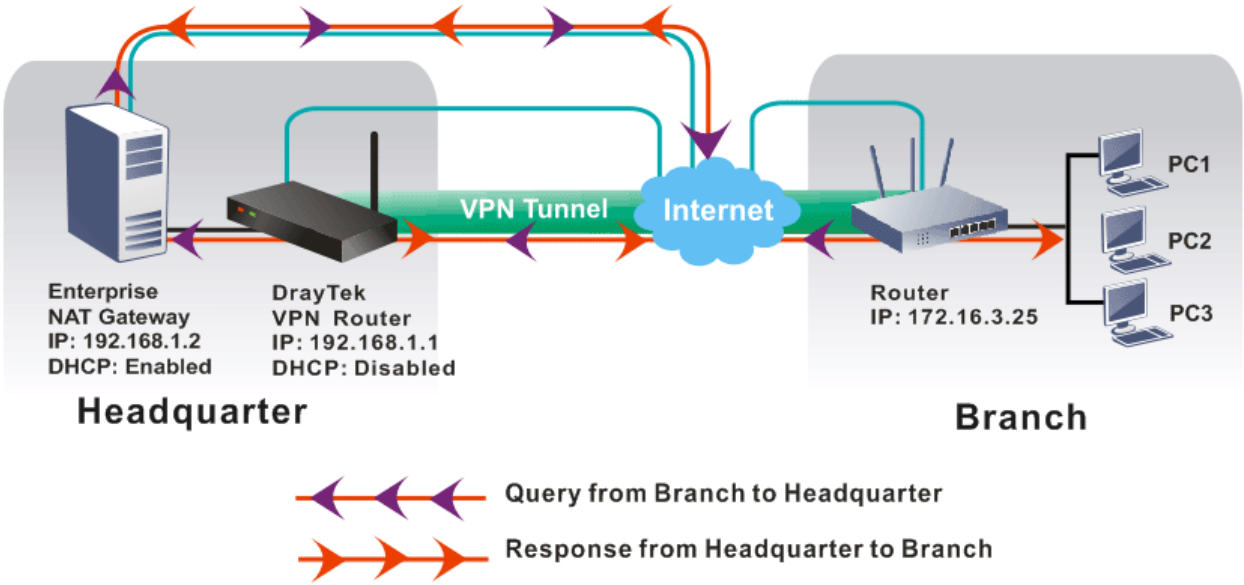
4. 完成了上述設定之後，按下**套用**儲存設定。



現在任何自 LAN1 傳送至遠端 PC(IP 位址 203.65.1.35)的封包都會被強制通過 WAN1 介面。

範例 3：如何使用策略路由在總公司與分公司建立安全路由

居易 VPN 路由器(例如 Vigor2960)與遠端路由器之間已經建立一條 LAN to LAN 的 VPN 通道，企業級防火牆路由器(架設於總公司)可以控制所有來自遠端電腦(位於分公司)登入網際網路的流量。



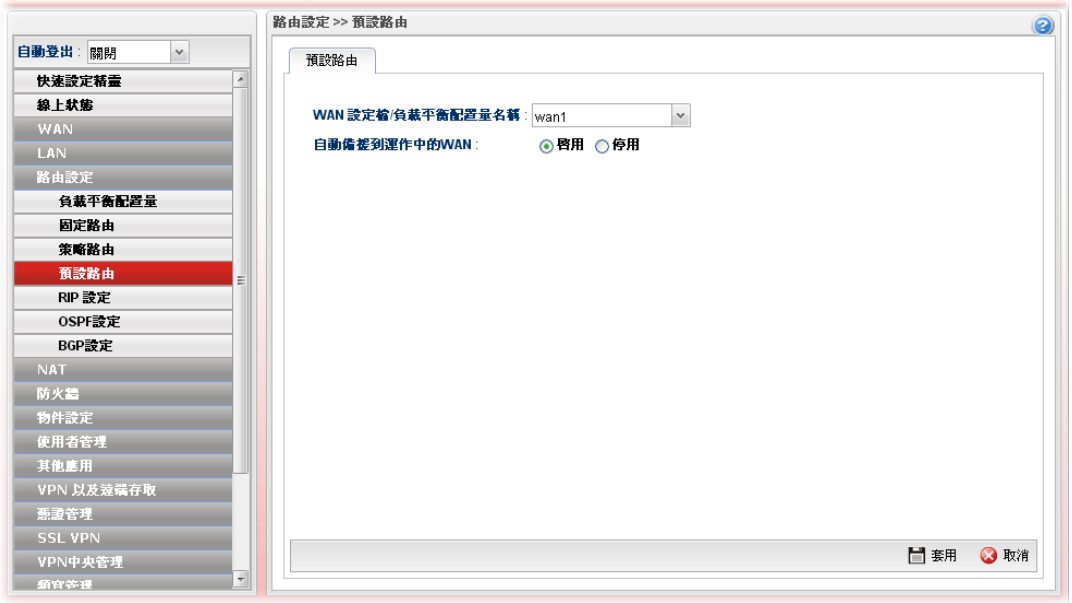
1. 登入 Vigor2960 網頁設定介面。
2. 開啓**路由>>策略路由**並按下**新增**以建立新的設定檔。

3. 在下述頁面中，輸入設定檔的名稱(本例使用 Secure_route)；**來源類型**選擇**子網**；輸入來源 IP 位址 172.16.3.25；傳送規則部分選擇使用者定義；選擇 **lan1** 作爲傳送介面；輸入 192.168.1.2 作爲**傳送(閘道)**；**備援至下一個規則**部分，則選擇**停用**。

4. 完成上述設定之後，按下**套用**儲存設定。

4.3.4 預設路由

本頁用於指定 WAN 設定檔或是負載平衡設定檔爲預設路由。



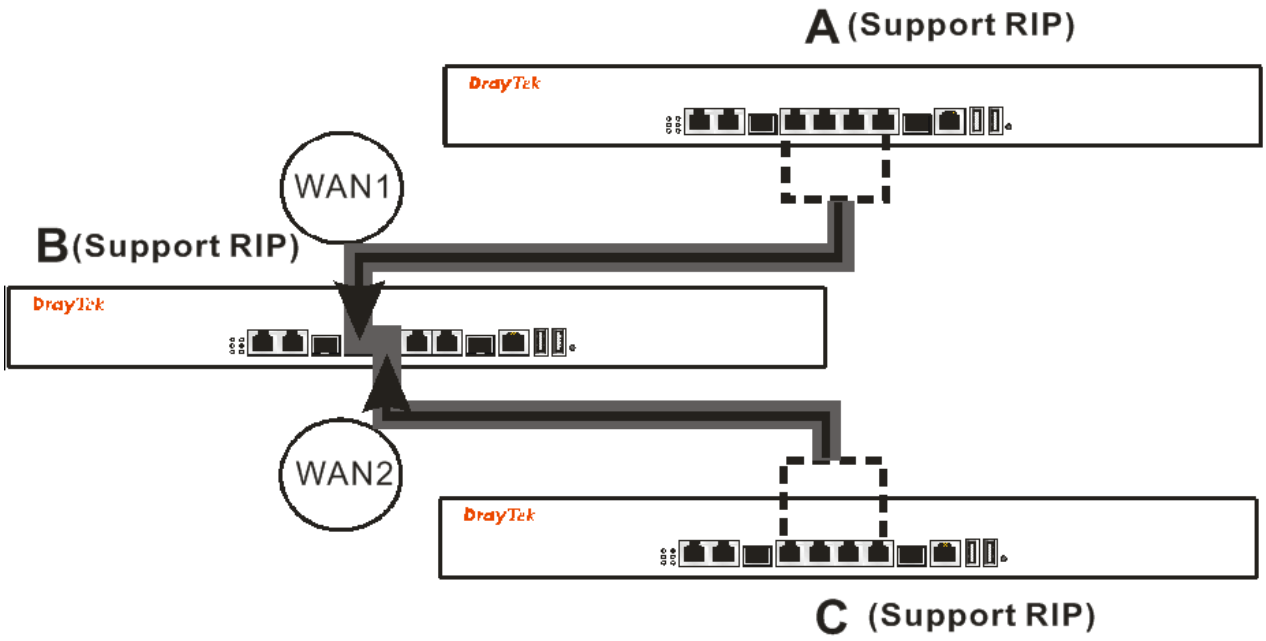
可用參數詳列如下：

項目	說明
WAN 設定檔 /負載平衡配置量名稱	可自下拉式清單中選擇一組設定檔作爲預設路由。
自動備援至運作中的 WAN	**啓用** – 選擇此項已利用任何活動中的 WAN 介面進行網路連線。 **停用** –選擇此項關閉此功能。
套用	按此鈕儲存設定。
取消	按此鈕捨棄頁面設定。

4.3.5 RIP 設定

RIP (Routing Information Protocol) 是動態路由協定，用於區域或是廣域網路上。路由資訊封包將定期透過網頁伺服器或是路由器發送出去，並可用來和其他路由器通訊。它會計算路由中網路節點的數目，以確保網路線路中沒有任何的阻礙，此外，它將基於 Distance Vector Routing 方法選擇正確的路由，並使用 Bellman-Ford 演算方式來計算路由表格。

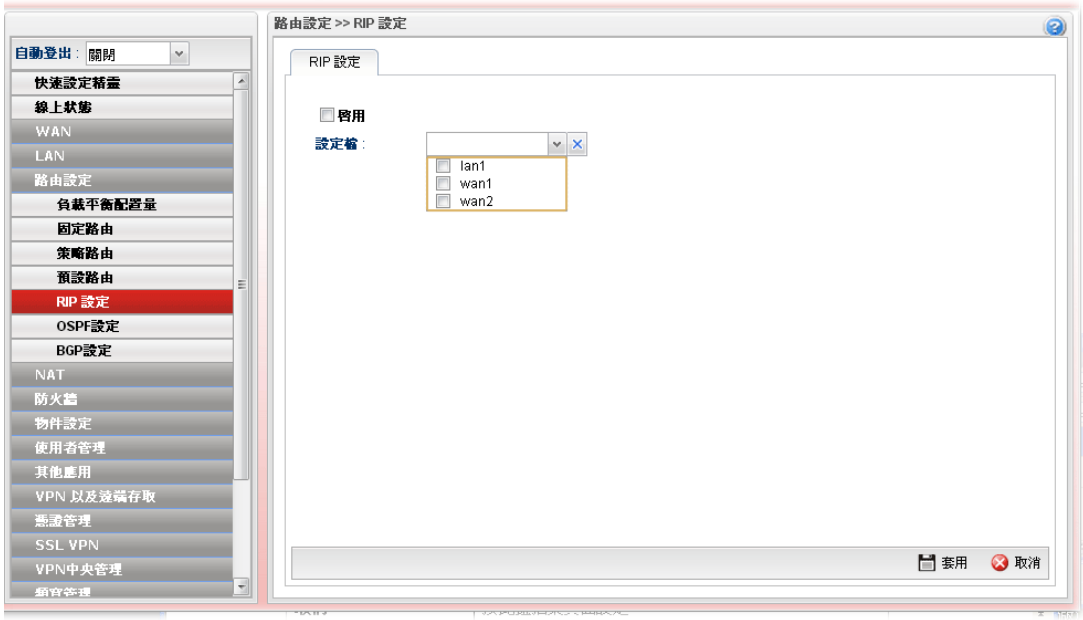
RIP 可自動更新路由表格，並找到一條路由發送封包，請參考下述範例圖：



假設路由器 A 的 WAN1/WAN2/WAN3/WAN4 介面支援 RIP，路由器 B 的 WAN1/WAN2 介面支援 RIP，而路由器 C 的 WAN1/WAN2/WAN3/WAN4 介面支援 RIP。

路由器 B 會告知路由器 A "如果您想要傳送封包至路由器 C，請先傳給我"，然後路由器 A 建立一個路由規則以轉發目的地在路由器 C 的封包先至路由器 B。

反過來看，路由器 C 也會做相同的事情。



可用參數詳列如下：

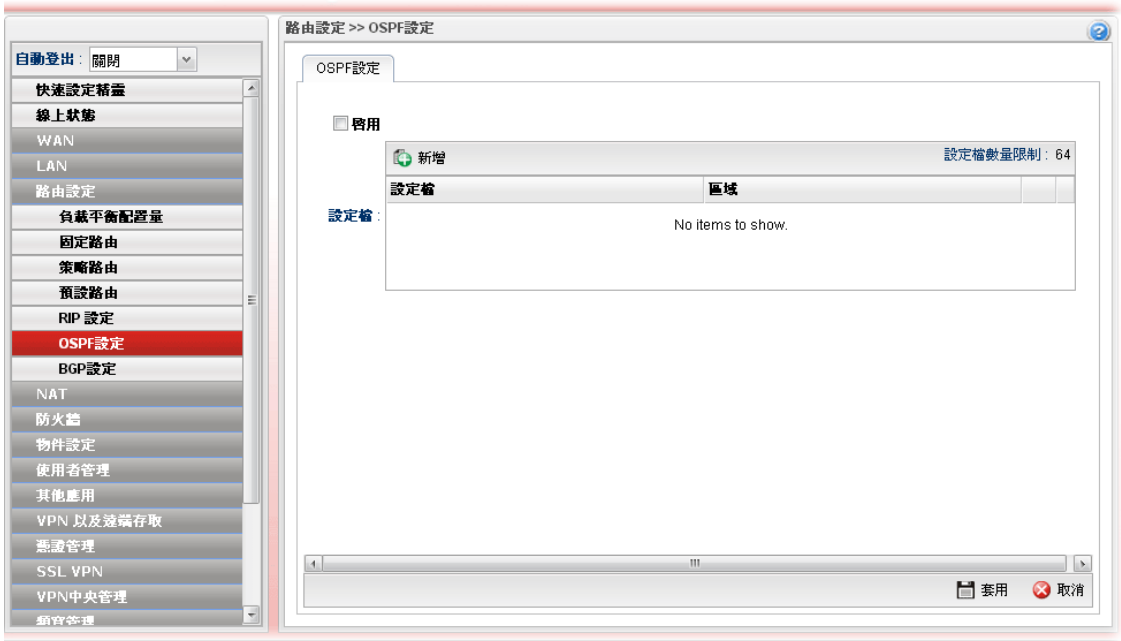
項目	說明
啓用	勾選此框啓用此功能。
設定檔	選擇 LAN/WAN 介面設定檔。
套用	按此鈕儲存設定。
取消	按此鈕捨棄頁面設定。

完成設定之後，按下**套用**儲存。

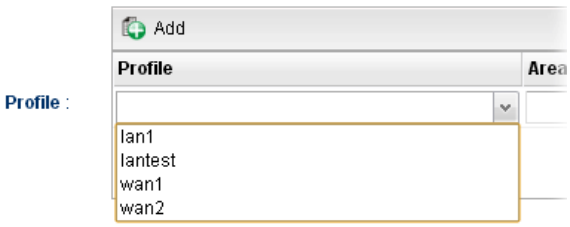
4.3.6 OSPF 設定

OSPF 開放最短路徑協定(Open Shortest Path First)使用 SPF (Shortest Path First)演算方式來計算路由 metric，這個功能非常適合用於大型網路與複雜的資料交換上。

當您想要支援更大型的網路或是想要擁有不易毀損的路由訊息時，您可以啓用 OSPF 功能來達成您的需要。請注意二端的路由器必須同時支援 OSPF 功能才能建立 OSPF 連線。



可用參數詳列如下：

項目	說明
啓用	勾選此框啓用此功能。
設定檔	**新增** – 按此鈕以便建立新的設定檔。  **設定檔** – 選擇 LAN/WAN 介面設定檔。 **區域** – AS 可區分成數個地區，每個地區都必須指定一個專屬號碼。 **注意**：有關詳細的說明，可參考 3.2 如何設定 OSPF 一節。
套用	按此鈕儲存設定。
取消	按此鈕捨棄頁面設定。

如何新增設定檔

1. 開啓**路由設定>> OSPF 設定**。
2. 勾選**啓用**。
3. 在設定檔空白處按下滑鼠鍵，設定畫面出現如下，按下**新增**。
4. 使用下拉式清單選擇需要的設定檔介面，接著指定區域值(可以設定爲 0.0.0.0 ~ 255.255.255.255 或是設定爲 0 ~ 4294967295)。

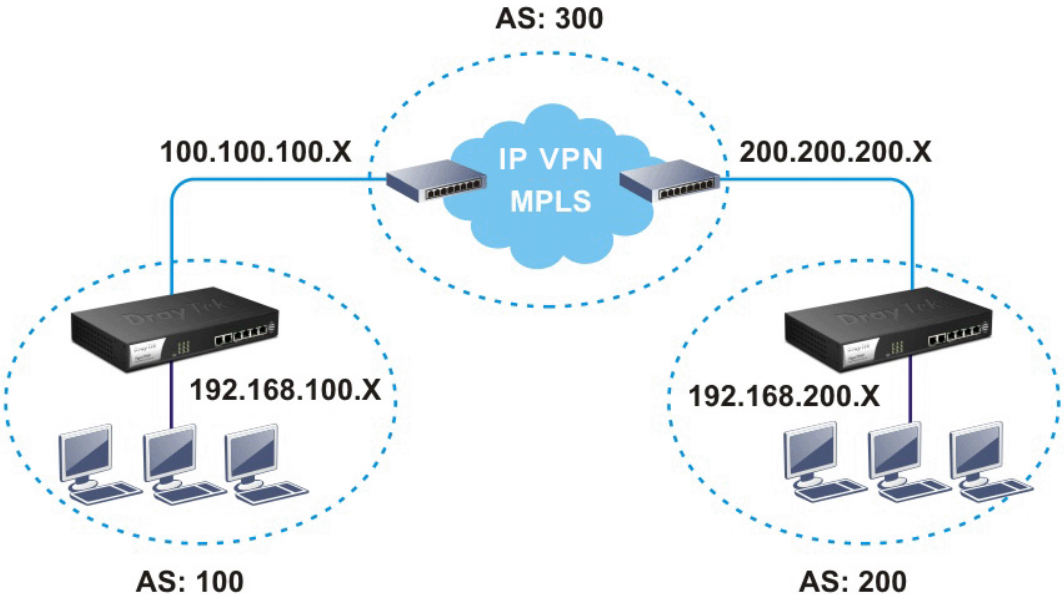
5. 按下**套用**儲存設定，新的設定檔已經產生並顯示在畫面上。

4.3.7 BGP 設定

BGP 是邊界網關協議(Border Gateway Protocol)的縮寫，是標準化外部閘道協定，用於網際網路上不同 AS 系統之間交換路由與可及性資訊。

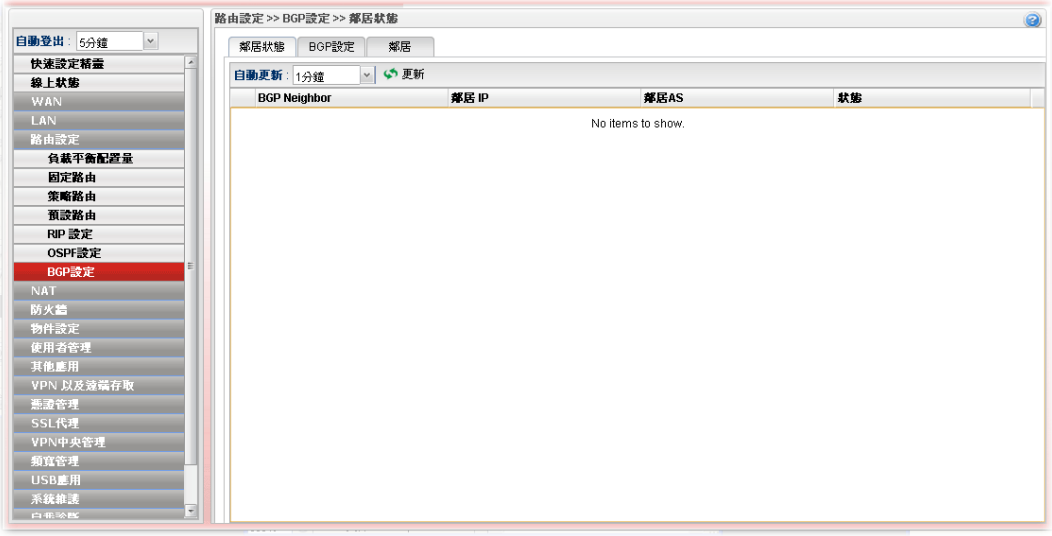
TCP 協定用於二台支援支援 BGP 功能的路由器以便進行資料傳送作業，他們彼此交換著 BGP 路由訊息，一個 BGP 路由器是其他 BGP 路由器的”鄰居”(neighbor)，對透過 TCP 連線來進行 BGP 路由資訊交換來說，有必要針對路由器定義 IP 位址與 AS 編號。

AS 是自主系統(Autonomous System)的縮寫，是以數個 IP 位址相互連接的群組，AS 號碼指出將採用的路由資訊之完整路徑，可以由一個或是數個 ISP 操作，並遵守 ISP 所制定的路由策略。



4.3.7.1 鄰居狀態

本頁顯示目前在 BGP 路由環境中鄰居的狀態為何。



可用參數詳列如下：

項目	說明
自動更新	指定取得最新狀態的間隔時間，當按下**更新**按鈕時，系統將會立刻更新資訊並呈現在頁面上。
更新	重新更新本頁面。
BGP Neighbor (BGP 鄰居)	顯示在**路由>>BGP 設定**的**鄰居**標籤中，成功設定的鄰居設定檔名稱。
鄰居 IP	顯示在**路由>>BGP 設定**的**鄰居**標籤中，成功設定的鄰居 IP 位址。
鄰居 AS	顯示在**路由>>BGP 設定**的**鄰居**標籤中，成功設定的鄰居自主系統(AS)號碼。
狀態	顯示鄰居設定檔的狀態，如果成功建立，本區應該會出現”建立(時間)”等字樣。

4.3.7.2 BGP 設定

本頁用於設定準備應用 BGP 功能的主機其相關的基本設定。

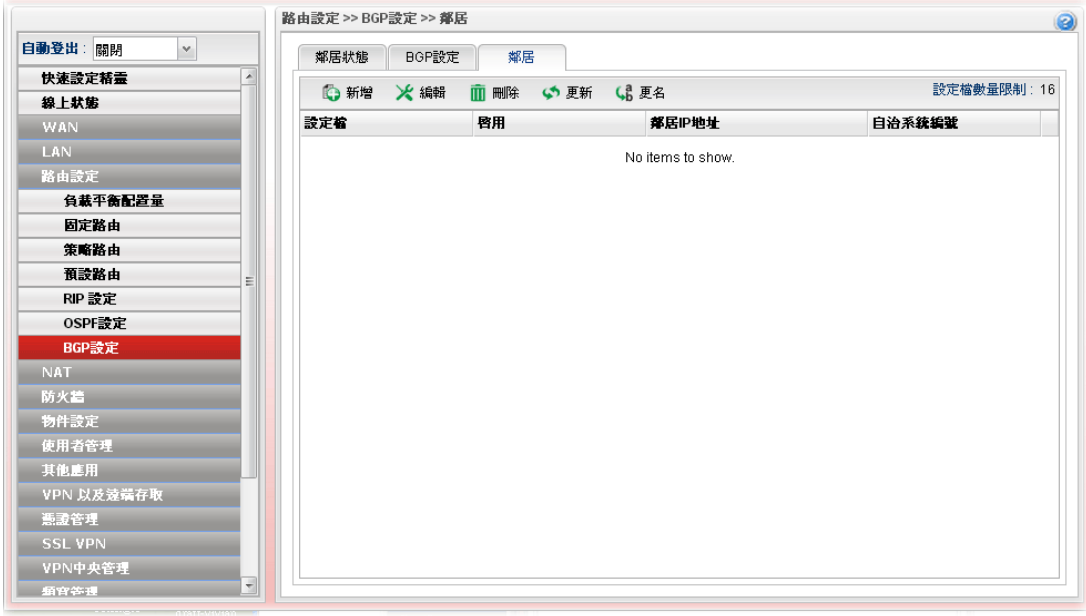
可用參數詳列如下：

項目	說明
啓用	勾選此框啓用此功能。
自主系統編號	輸入 BGP 應用中主機所需的自主系統號碼。
靜態網路	定義允許其他用戶透過固定路遊來連線的 IP 位址 (形成網路範圍)。 **新增** – 按此新增指定的 IP 位址與網路遮罩。 **設定檔數量限制** -顯示可建立的設定檔總數。 **IP** – 輸入 IP 位址。 **子網路遮罩**– 自動顯示搭配 IP 位址的子網遮罩。

完成上述設定之後，按**套用**儲存檔案。

4.3.7.3 鄰居

本頁用於設定交換 BGP 路由資訊的鄰居 IP 位址與自主系統編號(AS)。



可用參數詳列如下：

項目	說明
新增	新增新的配置量設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
刪除	移除選定的設定檔。 請選擇您想要刪除的既有設定檔，然後按下刪除按鈕，該設定檔即可被移除。
更新	重新更新本頁面。
更名	按此鈕後將會跳出視窗，讓您修改選定設定檔的檔名。 在使用此功能之前，至少要有一個設定檔存在始可運作。
設定檔	顯示設定檔名稱。
啓用	顯示設定檔狀態，False 表示停用；True 表示啓用。
鄰居 IP 位址	顯示鄰居的 IP 位址。
自主系統編號	顯示 BGP 應用中，鄰居使用的自主系統號碼。

如何新增 BGP 設定檔

1. 開啓**路由設定>> BGP 設定**並按下**鄰居**標籤。
2. 按下**新增**按鈕。

3. 下述頁面將會出現。

可用參數詳列如下：

項目	說明
設定檔	輸入設定檔名稱。
啓用	勾選此框啓用此功能。
鄰居 IP 位址	輸入此設定檔所需的 IP 位址。
自主系統編號	輸入 BGP 應用中相鄰者的自主系統編號。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

4. 輸入所有設定並按下**套用**儲存。
5. 新設定檔已經建立並顯示在頁面上。

4.4 NAT

通常，路由器可以 NAT 路由器提供其相關服務，NAT 是一種機制，一個或多個虛擬 IP 位址可以對應到某個單一的真實 IP 位址。真實 IP 位址習慣上是由您的 ISP 所指定的，因此您必須為此負擔費用，虛擬 IP 位址則只能在內部主機內辨識出來。

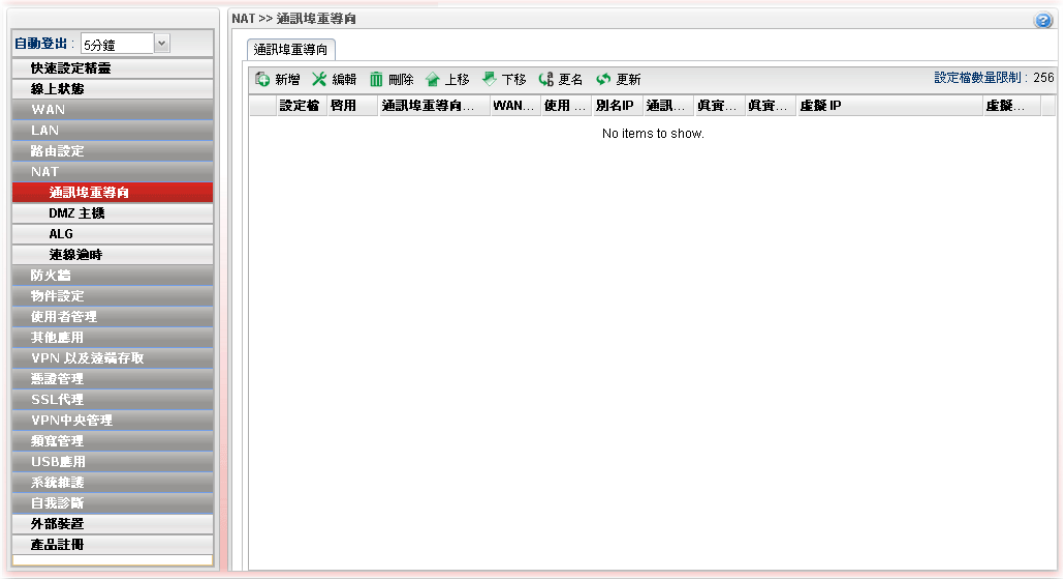
當封包之目的地位址為網路上某個伺服器時，會先送到路由器，路由器即改變其來源位址，成為真實 IP 位址，並透過真實通訊埠傳送出去。同時，路由器在連線數表格中列出清單，以記錄位址與通訊埠對應的相關資訊，當伺服器回應時，資料將直接傳回路由器的真實 IP 位址。

Vigor2960 的 NAT 機制於預設值中是開啓的，透過固定、PPPoE、DHCP 模式自 ISP 取得可全球路由的 IP 位址。Vigor2960 依照 RFC-1918 協定指派虛擬網路 IP 位址並轉換虛擬網路位址為可全球路由的 IP 位址，讓本地主機可以和路由器溝通並存取網際網路。

NAT 提供數種功能，包含如下：

4.4.1 通訊埠重導向

通訊埠重導向指的是通訊埠重導向。可用來公開內部伺服器至公用網域或是開啓指定埠號給予內部主機。網際網路主機可以使用 WAN IP 位址存取網際網路服務，像是 FTP、WWW 等等，例如內部 FTP 伺服器在本地主機中運作，位址為 192.168.1.2，當其他使用者將此類型需求透過網際網路傳送至您的網路，路由器將會引導此類需求至適當的主機上。使用者也可以透過設定的方式轉換此埠號為另外的埠號，比方說埠號 1024 可以轉移給 LAN 端 IP 位址為 192.168.1.100 的裝置上，如果埠號符合表格內的定義，那麼封包就會被轉發至指定主機上。

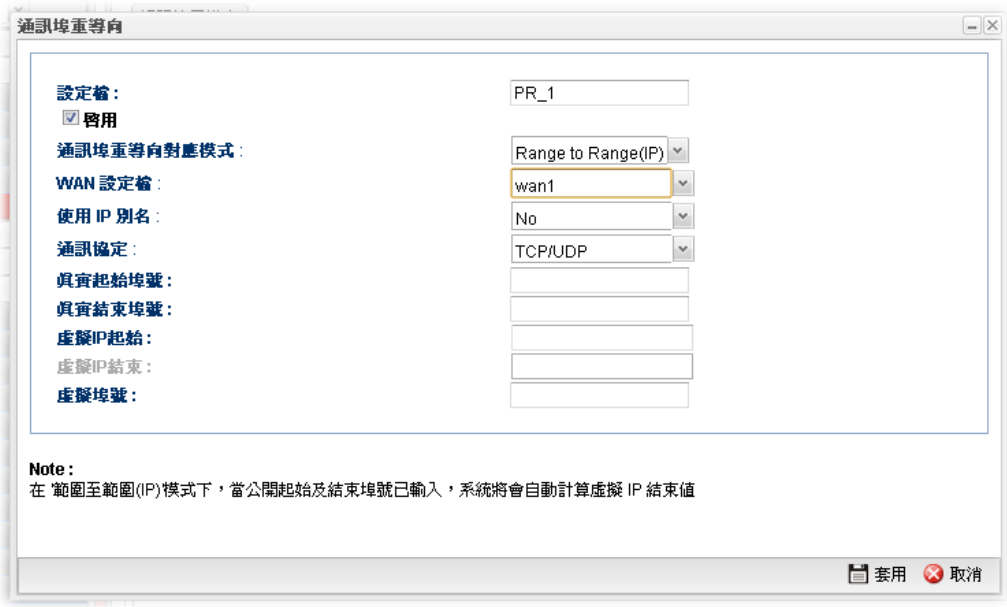


每個項目說明如下：

項目	說明
新增	新增新的設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
刪除	移除選定的設定檔。 請選擇您想要刪除的既有設定檔，然後按下刪除按鈕，該設定檔即可被移除。
更新	重新更新本頁面。
上移	將設定檔往上移動改變選定設定檔的順序。
下移	將設定檔往下移動改變選定設定檔的順序。
更名	按此鈕後將會跳出視窗，讓您修改選定設定檔的檔名。 在使用此功能之前，至少要有一個設定檔存在始可運作。
設定檔	顯示設定檔名稱。
啓用	顯示設定檔狀態，False 表示停用；True 表示啓用。
通訊埠重導向對應模式	顯示埠號被轉發的方向。
WAN 設定檔	顯示設定檔的 WAN 介面。
使用 **IP** 別名	顯示 IP 別名使用的類型(no, Single_Alias, All)。
別名	顯示選定的 WAN IP 別名。
通訊協定	顯示此設定檔使用的協定。
真實起始埠號	顯示真實埠號的起始號碼。
真實結束埠號	顯示真實埠號的結束號碼。
虛擬 **IP**	顯示此設定檔的虛擬 IP 位址。
虛擬埠號	顯示虛擬埠號值

如何新增通訊埠重導向設定檔

1. 開啓 **NAT>>通訊埠重導向**。
2. 按下**新增**按鈕。
3. 下述頁面將會出現。



可用參數詳列如下：

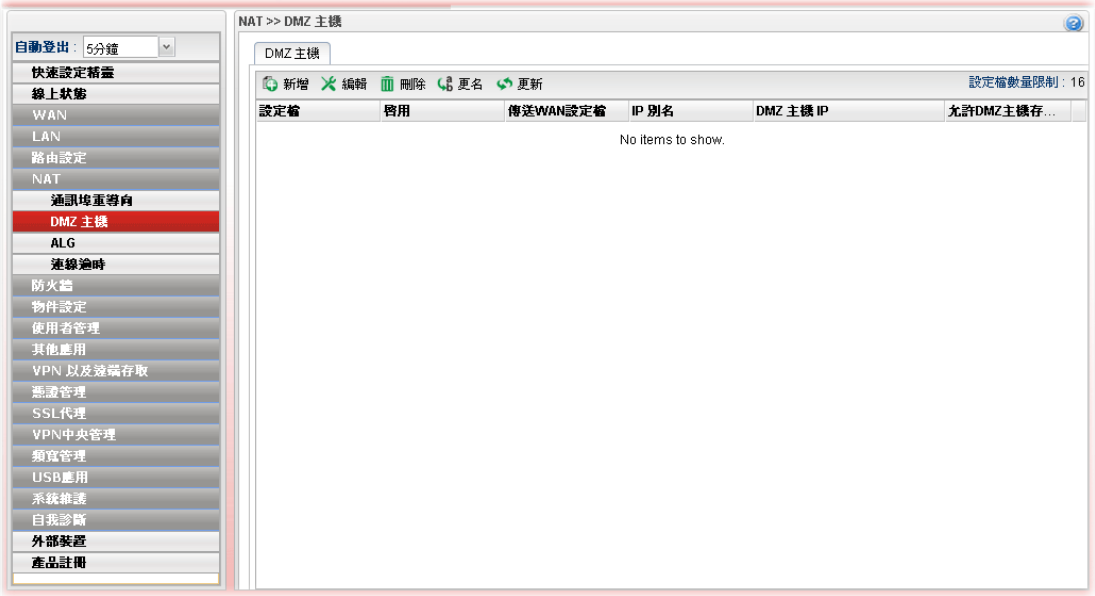
項目	說明
設定檔	輸入設定檔名稱。
啓用	勾選此框啓用此功能。
通訊埠重導向對應模式	指定通訊埠重導向的模式。 One to One Range to One Range to Range(p... Range to Range(IP)
WAN 設定檔	指定需要的 WAN 介面設定檔。
使用 IP 別名	當 WAN 設定檔選擇 All 時，這個功能會暫時關閉。 使用下拉式清單選擇適當的模式。 **Single Alias** –您必須手動輸入一個 IP 位址作爲 IP 別名。 **所有** – 所有的 IP 位址都被視爲 IP 別名。
別名 IP	WAN IP 別名可以選擇並用於通訊埠重導向，在使用之前，請先至 **WAN>>基本設定**啓用 wan1 設定檔，在 wan1 的**固定**模式下新增數個 IP 位址。
通訊協定	選擇用於此設定檔的協定內容。
眞實起始埠號 / 眞實結束埠號	當 **Range to One** 或 **Range to Range (port)** 或 **Range to Range (IP)**被選定爲通訊埠重導向對映模式時，即需要輸

	入此處的資訊。 輸入真實埠號的起點與終點埠號值。 對於 Range-to-One，將起點與終點值皆設定爲相同值。
虛擬 IP	指定提供服務的內部主機之虛擬 IP 位址，只要輸入 IP 位址即可。
虛擬 IP 起始 / 虛擬 IP 結束	當 **Range to Range (IP)**被選定爲通訊埠重導向模式時，即需要輸入此處的資訊。 指定內部主機提供的服務之 IP 位址。
虛擬埠號	輸入設定檔需求的埠號值。
更多埠號設定	可輸入其他的埠號。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

4. 輸入所有設定並按下**套用**儲存。
5. 新增設定檔將呈現在畫面上。

4.4.2 DMZ 主機

電腦網路中，DMZ (De-Militarized Zone)是電腦主機或是小型網路介入公司虛擬網路與對外真實網路之間中立地帶。它可以避免使用者直接進入公司網路，對防火牆來說 DMZ 是一種可以選擇且更爲安全的方式，作爲代理伺服器也相當有效率。小型公司的典型 DMZ 設定中，分隔的電腦（或是網路中的主機）接收來自虛擬網路的使用者，提出登入網際網路的需求，或是來自其他公司要求存取公司網路的需求。DMZ 主機接著針對此類需求在真實網路上初始化連線，然而 DMZ 主機無法初始化連線回送至虛擬網路，只能轉發被特別註明要求的封包，公司外部的真實網路上的使用者僅能存取 DMZ 主機。DMZ 主機可具備一些公司能提供給外部世界相關服務的網頁，如果外部使用者甚破壞 DMZ 主機的安全性，毀損的只是看到的網頁，其他公司資訊網頁不會被透露出去。



每個項目說明如下：

項目	說明
新增	新增新的設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
刪除	移除選定的設定檔。 請選擇您想要刪除的既有設定檔，然後按下刪除按鈕，該設定檔即可被移除。
更新	重新更新本頁面。
更名	按此鈕後將會跳出視窗，讓您修改選定設定檔的檔名。 在使用此功能之前，至少要有一個設定檔存在始可運作。
設定檔	顯示設定檔名稱。
啓用	顯示設定檔狀態，False 表示停用；True 表示啓用。
傳送 **WAN** 設定檔	顯示 DMZ 主機設定檔將要套用的 WAN 介面設定檔。
IP 別名	顯示選定 WAN IP 位址別名,前提是使用 IP 別名已啓動。
DMZ 主機 **IP**	顯示 DMZ 主機的 IP 位址。
允許 **DMZ** 主機存取網路	顯示此功能爲啓用或是停用。

如何新增 DMZ 主機設定檔

1. 開啓 **NAT>> DMZ** 主機。
2. 按下**新增**按鈕。
3. 下述頁面將會出現。

可用參數詳列如下：

項目	說明
設定檔	輸入設定檔名稱。
啓用	勾選此框啓用此功能。
傳送 WAN 設定檔	選擇 WAN 介面設定檔。
使用 IP 別名	選擇**啓用**開啓此功能。
IP 別名	WAN IP 別名可以選擇並用於 DMZ 主機，在使用之前，請先至 **WAN>>基本設定**啓用 wan1 設定檔，在 wan1 的**固定**模式下新增數個 IP 位址。
DMZ 主機 IP	輸入 DMZ 主機的 IP 位址。
允許 DMZ 主機存取網路	選擇**啓用**讓 DMZ 主機存取網際網路。
允許 IP 物件	這是選項設定。 使用下拉式清單選擇 IP 物件設定檔套用至此設定檔。
允許 IP 群組	這是選項設定。 使用下拉式清單選擇 IP 群組設定檔套用至此設定檔。
允許服務類型	這是選項設定。 使用下拉式清單選擇服務類型套用至此設定檔。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

4. 輸入所有設定並按下**套用**儲存。

5. 新設定檔新增完成並顯示在 **DMZ 主機**表格上。

4.4.3 ALG

4.4.3.1 SIP ALG

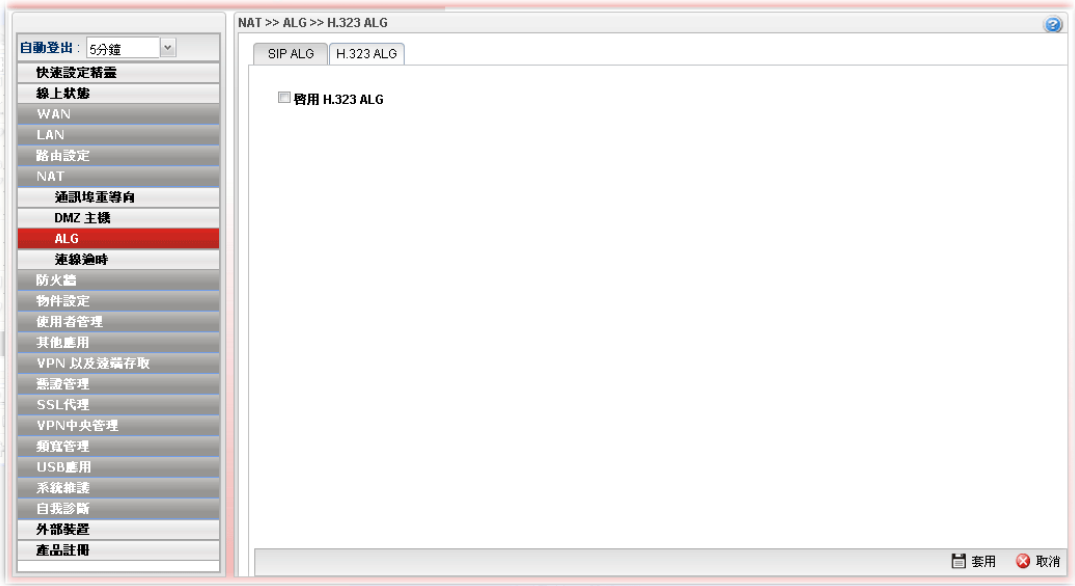
SIP ALG 表示 **Session Initiation Protocol, Application Layer Gateway**，這個頁面讓您透過 NAT 正確傳輸及接收 SIP 訊息與 RTP 聲音封包。

可用參數詳列如下：

項目	說明
啓用 **SIP ALG**	勾選此框啓用此功能。
套用	按此鈕儲存設定。

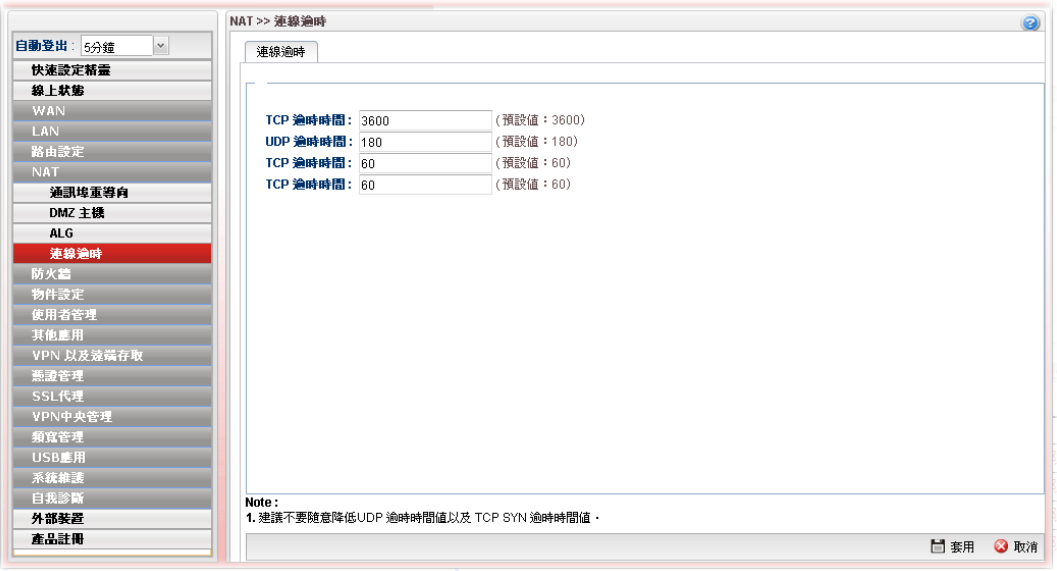
4.4.3.2 H.323 ALG

讓進入及撥出的 VoIP 電話透過 NAT 來傳送，如有必要，請勾選**啓用**方框，再按下**套用**儲存設定。



4.4.4 連線逾時

設定連線數(session)逾時的設定，意指一條連線在時間設定內若無何動作，則關閉此連線。建議不要隨意降低 UDP 逾時時間值以及 TCP SYN 逾時時間值。



可用參數詳列如下：

項目	說明
TCP 逾時時間	針對 TCP 連線類型的連線數設定逾時限制(不包含埠號 80 與埠號 443)。
UDP 逾時時間	針對 UDP 類型的連線數設定逾時限制。
TCP WWW 逾時時間	針對埠號 80、埠號 443 之 TCP 連線的連線數設定逾時限

	制。
TCP SYN 逾時時間	針對 TCP SYN 類型的連線數設定逾時限制。
套用	按此鈕儲存設定。
取消	按此鈕離開對話盒，且不儲存任何設定。

4.5 防火牆

防火牆掌控著允許與拒絕封包進出路由器，**防火牆設定**主要包含封包過濾、DoS 以及 URL 過濾工具之設定。這些防火牆規則幫助您保護區域網路免受外來攻擊，同時也提供方法限制區域網路使用者無法隨意存取網際網路內容，並過濾可能觸發不預期之對外連線像是木馬程式等特定封包的進出。

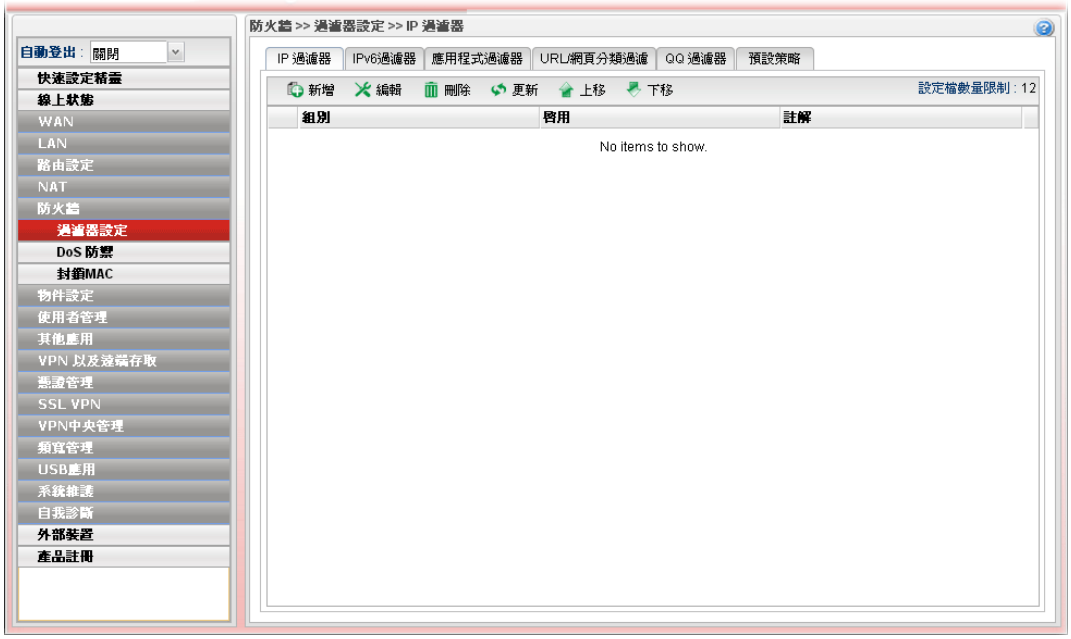
下述章節將說明如何設定路由器的防火牆，使用者可以從選單中挑選 **IP 過濾器**、**DoS 攻擊設定**、**MAC 封鎖**與**埠號封鎖**項目，其中 **DoS 攻擊設定**工具可以偵測並減緩 DoS 攻擊。

4.5.1 過濾器設定

路由器將基於此設定進行封包過濾，包含 IP 過濾器、應用程式過濾器、URL/網頁過濾器與 QQ 過濾器設定，這些過濾器將群組特定的物件(例如 IP 物件、服務物件、關鍵字物件、副檔名物件、IM 物件、P2P 物件、協定物件、網頁內容物件、QQ 物件、QQ 群組、時間物件等等)並形成強而有力的防火牆進行電腦防護作業。

4.5.1.1 IP 過濾器

本頁讓您建立新的 IP 過濾器，以便後續其他頁面設定套用。



每個項目說明如下：

項目	說明
新增	新增新的設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
刪除	移除選定的設定檔。 請選擇您想要刪除的既有設定檔，然後按下刪除按鈕，該設定檔即可被移除。
更新	重新更新本頁面。
上移	將設定檔往上移動改變選定設定檔的順序。
下移	將設定檔往下移動改變選定設定檔的順序。
設定檔數量限制	顯示可建立設定檔的總數。
組別	顯示 IP 過濾器群組設定檔的檔名。
啓用	顯示設定檔狀態，False 表示停用；True 表示啓用。
註解	顯示關於此設定檔的簡易說明。

如何建立新的 IP 過濾器群組

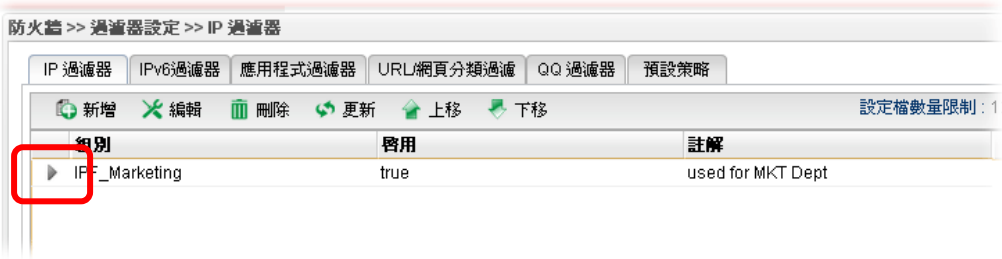
建立一個包含 IP 過濾器規則的 IP 群組，請依照下列步驟進行：

1. 開啓**防火牆>>過濾器設定**並按下 **IP 過濾器**標籤。
2. 按下**新增**按鈕。
3. 下述頁面將會出現。

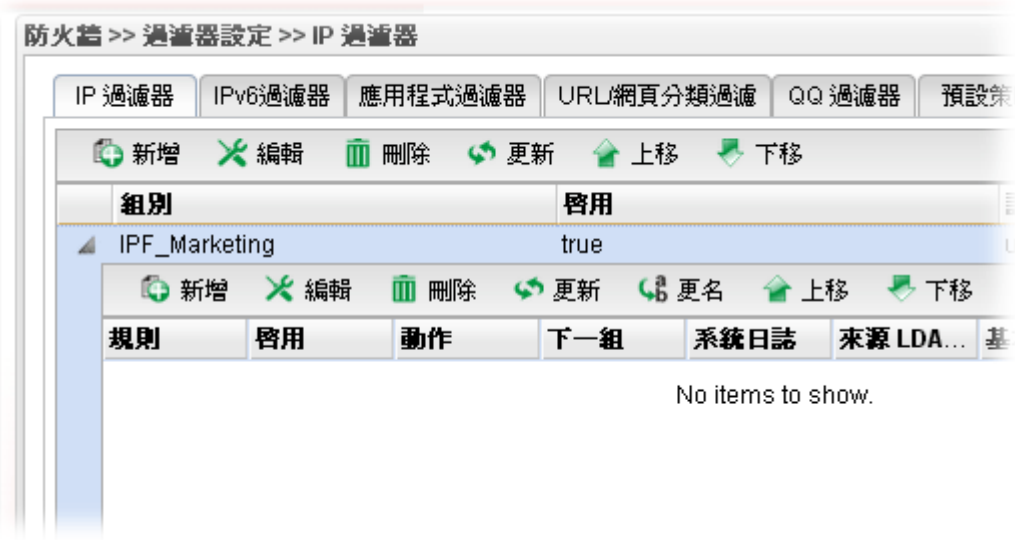
可用參數詳列如下：

項目	說明
群組	輸入 IP 過濾器群組名稱。
啓用	勾選此框啓用此設定檔。
說明	針對此設定檔提供簡易的說明。 針對此設定檔提供簡易的說明。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

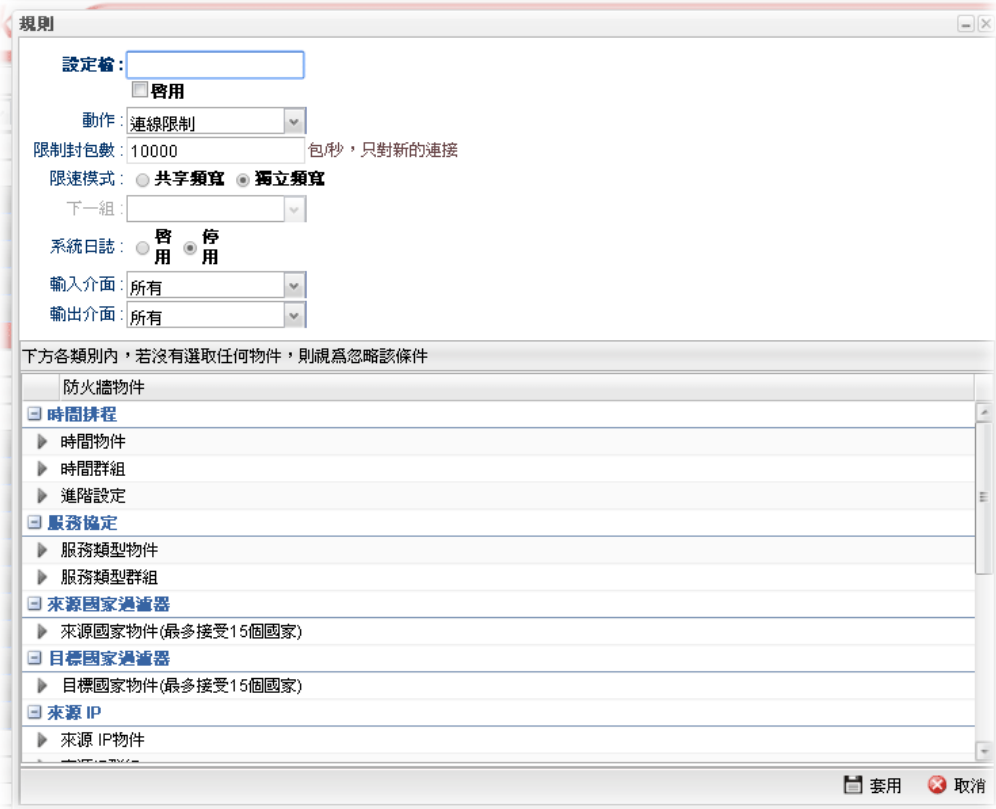
4. 輸入所有設定並按下**套用**儲存。
5. 新的過濾器群組顯示如下。



6. 您可以按下選定 IP 過濾器群組左邊的 ▶ 圖示來建立新的過濾器規則，設定頁面將出現如下讓您加入新的 IP 過濾器規則設定檔。

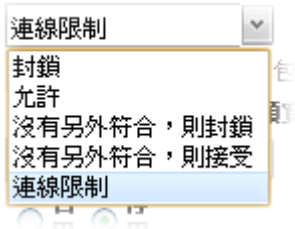


7. 移動滑鼠並按下**新增**。
8. 設定頁面出現如下。



可用參數詳列如下：

項目	說明
設定檔	輸入 IP 過濾器規則之設定檔名稱。
啓用	勾選此框啓用此設定檔。
動作	指定封包符合此規則時所應採取的動作。 **封鎖** – 符合此規則的封包立即捨棄。

	允許 – 符合此規則的封包立即放行。 **沒有另外符合，則封鎖** – 封包符合規則，但不符合下個階段的規則將會被捨棄。 **沒有另外符合，則接受** – 封包符合規則，但不符合下個階段的規則將可立即放行。 **連線限制** –限制每秒連線的數量以避免受到他人攻擊。針對每次連線，封包數若小於限制封包數設定者則立即放行該封包；但若封包數大於限制封包數設定，則封鎖該封包。亦即，封包的放行或捨棄是由當時連線速率(新連線數)的大小來決定。 
限制封包數	當您選擇**連線限制**作爲採取的**動作**時，您必須輸入封包限制數目來決定每秒究竟有多少數量的封包可以放行。
限速模式	當您選擇**連線限制**作爲採取的**動作**時，除了設定限制封包數之外，您還必須則一選擇： **共享頻寬** – 表示區段內所有的 IP 共享系統所限制的封包數量。 **獨立頻寬** – 表示每個 IP 享有個別限制的封包數量。
下一組	當您選擇**沒有另外符合，則封鎖**或是時**沒有另外符合，則接受**，您必須指定下一個 IP 過濾器群組供進一步符合條件。
系統日誌	按下啓用讓防火牆動作的歷程紀錄可以呈現在系統維護**系統日誌檔**頁面中。
輸入介面	選擇 LAN 或是 WAN 設定檔作爲輸入資料介面。
輸出介面	選擇 LAN 或是 WAN 設定檔作爲資料傳送介面。
時間排程	**時間物件** – 按下三角圖示 ▶ 以顯示設定檔選擇框，選擇適當的排程套用至此規則。 您可以按下圖示 來建立另一個時間物件設定檔。 **時間群組** - 按下三角圖示 ▶ 以顯示設定檔選擇框，選擇適當的時間群組設定檔套用至此規則。 按下圖示 可建立其他的時間物件群組設定檔。 **進階設定** – 當套用上述排程設定檔時，勾選**排程啓用時清除連線數**方塊。
服務協定	**服務類型物件** – 按下三角圖示 ▶ 以顯示設定檔選擇框，自下拉式清單中選擇一個或是多個服務類型物件設定檔，選定的設定檔將可視爲服務類型，您可以按下圖示

	建立其他的服務類型物件設定檔。 **服務類型群組** – 按下三角圖示 ▶ 以顯示設定檔選擇框，自下拉式清單中選擇一個或是多個服務類型物件設定檔，選定的設定檔將可視爲服務類型，您可以按下圖示 建立其他的服務協定物件設定檔。
來源國家過濾器	**來源國家物件 (至多 15 個國家)** -按下三角圖示 ▶ 以顯示設定檔選擇框，自下拉式清單中選擇一個或是多個國家物件設定檔，選定的設定檔將可視爲輸入國家過濾器，您可以按下圖示 建立其他的過濾器設定檔。
目標國家過濾器	**目的國家物件 (至多 15 個國家)** -按下三角圖示 ▶ 以顯示設定檔選擇框，自下拉式清單中選擇一個或是多個國家物件設定檔，選定的設定檔將可視爲輸出國家過濾器，您可以按下圖示 建立其他的過濾器設定檔。
來源 IP	**來源 IP 物件** - 按下三角圖示 ▶ 以顯示設定檔選擇框，自下拉式清單中選擇一個或是多個 IP 物件設定檔，選定的設定檔被視爲來源目標，您可以按下圖示 建立其他的 IP 物件設定檔。 **來源 IP 群組** - 按下三角圖示 ▶ 以顯示設定檔選擇框，自下拉式清單中選擇一個或是多個 IP 群組設定檔，選定的設定檔被視爲來源目標，您可以按下圖示 建立其他的 IP 群組設定檔。 **來源使用者設定檔** – 按下三角圖示 ▶ 以顯示設定檔選擇框，自下拉式清單中選擇一個或是多個使用者設定檔，選定的設定檔被視爲來源目標，您可以按下圖示 建立其他的使用者物件設定檔。 **來源使用者群組** – 按下三角圖示 ▶ 以顯示設定檔選擇框，自下拉式清單中選擇一個或是多個使用者群組，選定的設定檔被視爲來源目標，您可以按下圖示 建立其他的使用者群組設定檔。 **來源 LDAP 群組** – 按下三角圖示 ▶ 以顯示設定檔選擇框，自下拉式清單中選擇一個或是多個 LDAP 群組設定檔，選定的設定檔被視爲來源目標，您可以按下圖示 建立其他的 LDAP 群組設定檔。
目標 IP	**目標 IP 物件** - 按下三角圖示 ▶ 以顯示設定檔選擇框，自下拉式清單中選擇一個或是多個 IP 物件設定檔，選定的設定檔被視爲目的目標，您可以按下圖示 建立其他的 IP 物件設定檔。 **目的地 IP 群組** - 按下三角圖示 ▶ 以顯示設定檔選擇框，自下拉式清單中選擇一個或是多個 IP 群組設定檔，選定的設定檔被視爲目的目標，您可以按下圖示 建立其他的 IP 群組設定檔。 **目標 DNS 物件** - 按下三角圖示 ▶ 以顯示設定檔選擇

	框，自下拉式清單中選擇一個或是多個 DNS 物件設定檔，選定的設定檔被視爲目的目標，您可以按下圖示 建立其他的 DNS 物件設定檔。 **目標使用者設定檔** – 按下三角圖示 ▶ 以顯示設定檔選擇框，自下拉式清單中選擇一個或是多個使用者設定檔，選定的設定檔被視爲目的目標，您可以按下圖示 建立其他的使用者物件設定檔。 **目標使用者群組** – 按下三角圖示 ▶ 以顯示設定檔選擇框，自下拉式清單中選擇一個或是多個使用者群組設定檔，選定的設定檔被視爲目的目標，您可以按下圖示 建立其他的使用者群組設定檔。 **目標 LDAP 群組** – 按下三角圖示 ▶ 以顯示設定檔選擇框，自下拉式清單中選擇一個或是多個 LDAP 群組設定檔，選定的設定檔被視爲目的目標，您可以按下圖示 建立其他的 LDAP 群組設定檔。
來源 MAC 過濾器	**來源 MAC 物件** - 按下三角圖示 ▶ 以顯示設定檔選擇框，自下拉式清單中選擇一個或是多個使用者群組設定檔，選定的設定檔被視爲目的目標，您可以按下圖示 建立其他的使用者群組設定檔。
目標 MAC 過濾器	**目標 MAC 物件** - 按下三角圖示 ▶ 以顯示設定檔選擇框，自下拉式清單中選擇一個或是多個使用者群組設定檔，選定的設定檔被視爲目的目標，您可以按下圖示 建立其他的使用者群組設定檔。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

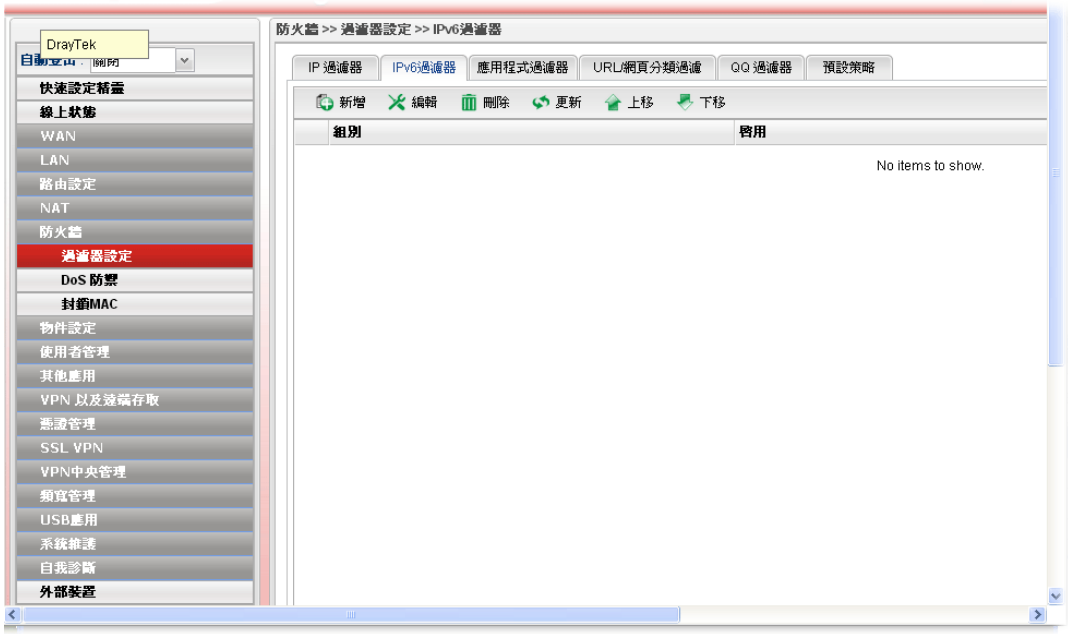
9. 輸入所有設定並按下套用儲存。

10. 新的 IP 過濾器規則已經建立在 IP 過濾器群組下(本例中名爲 IPF_Market)。

注意：在特定的 IP 過濾器群組下可以建立多個 IP 過濾器規則。

4.5.1.2 IPv6 過濾器

本頁讓您建立新的 IPv6 過濾器，以便後續其他頁面設定套用。



每個項目說明如下：

項目	說明
新增	新增新的設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
刪除	移除選定的設定檔。 請選擇您想要刪除的既有設定檔，然後按下刪除按鈕，該設定檔即可被移除。
更新	重新更新本頁面。
上移	將設定檔往上移動改變選定設定檔的順序。
下移	將設定檔往下移動改變選定設定檔的順序。
設定檔數量限制	顯示可建立設定檔的總數。
組別	顯示 IP 過濾器群組設定檔的檔名。
啓用	顯示設定檔狀態，False 表示停用；True 表示啓用。
註解	顯示關於此設定檔的簡易說明。

如何建立 IPv6 過濾器群組

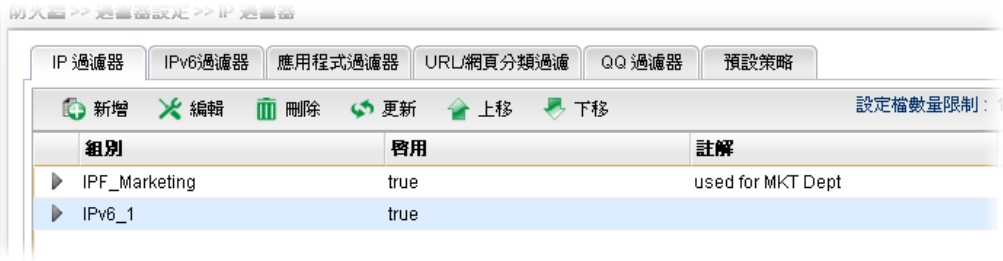
建立一個包含 IP 過濾器規則的 IP 群組，請依照下列步驟進行：

1. 開啓**防火牆>>過濾器設定**並按下 **IPv6 過濾器**標籤。
2. 按下**新增**按鈕。
3. 下述頁面將會出現。

可用參數詳列如下：

項目	說明
組別	輸入 IPv6 過濾器群組名稱。
啓用	勾選此框啓用此設定檔。
註解	針對此設定檔提供簡易的說明。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

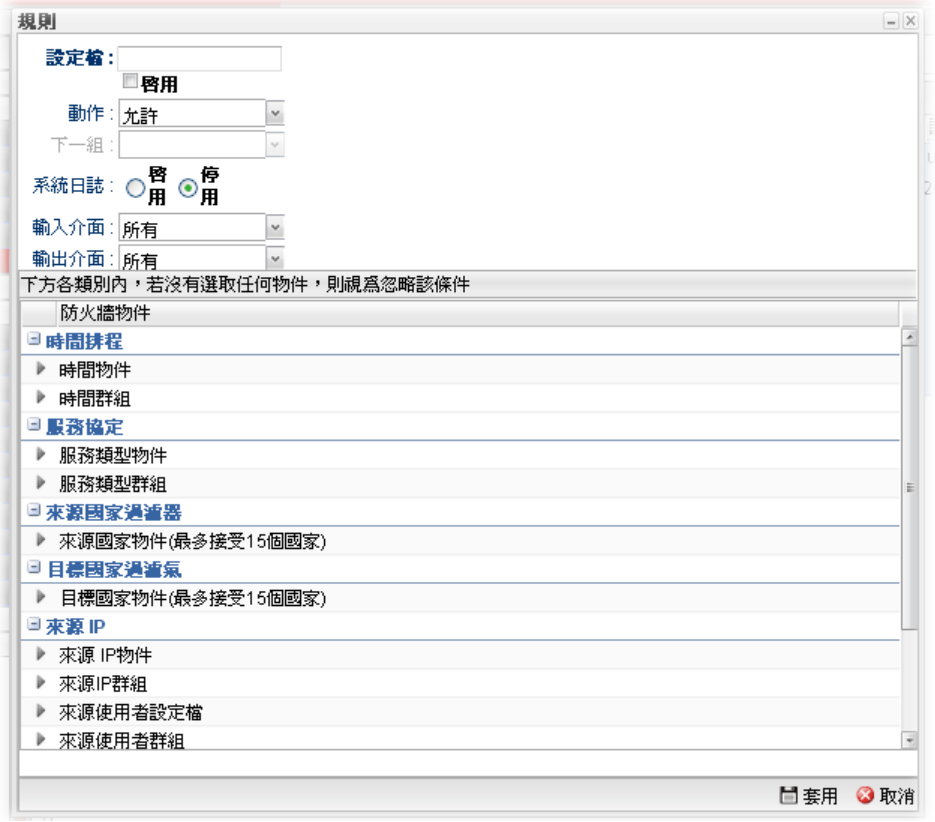
4. 輸入所有設定並按下套用儲存。
5. 新的過濾器群組顯示如下。



6. 您可以按下選定 IP 過濾器群組左邊的 ▶ 圖示來建立新的過濾器規則，設定頁面將出現如下讓您加入新的 IP 過濾器規則設定檔。

7. 移動滑鼠並按下**新增**。

8. 設定頁面出現如下。



可用參數詳列如下：

項目	說明
設定檔	輸入 IPv6 過濾器規則之設定檔名稱。
啓用	勾選此框啓用此設定檔。

動作	指定封包符合此規則時所應採取的動作。 **封鎖** - 符合此規則的封包立即捨棄。 **允許** – 符合此規則的封包立即放行。 **沒有另外符合，則封鎖**–封包符合規則，但不符合下個階段的規則將會被捨棄。 **沒有另外符合，則通過**- 封包符合規則，但不符合下個階段的規則將可立即放行。
下一組	當您選擇**沒有另外符合，則封鎖**或是時**若沒有另外符合，則通過**，您必須指定下一個 IP 過濾器群組供進一步符合條件。
系統日誌	按下啓用讓防火牆動作的歷程紀錄可以呈現在系統維護**系統日誌檔**頁面中。
輸入介面	選擇 LAN 或是 WAN 設定檔作爲輸入資料介面。
輸出介面	選擇 LAN 或是 WAN 設定檔作爲資料傳送介面。
時間排程	**時間物件** – 按下三角圖示 ▶ 以顯示設定檔選擇框，選擇適當的排程套用至此規則。 您可以按下圖示 來建立另一個時間物件設定檔。 **時間群組** - 按下三角圖示 ▶ 以顯示設定檔選擇框，選擇適當的時間群組設定檔套用至此規則。 按下圖示 可建立其他的時間物件群組設定檔。
服務協定	**服務類型物件** – 按下三角圖示 ▶ 以顯示設定檔選擇框，自下拉式清單中選擇一個或是多個服務類型物件設定檔，選定的設定檔將可視爲服務類型，您可以按下圖示 建立其他的服務類型物件設定檔。 **服務類型群組** – 按下三角圖示 ▶ 以顯示設定檔選擇框，自下拉式清單中選擇一個或是多個服務類型物件設定檔，選定的設定檔將可視爲服務類型，您可以按下圖示 建立其他的服務協定物件設定檔。
來源國家過濾器	**來源國家物件 (至多 15 個國家)** -按下三角圖示 ▶ 以顯示設定檔選擇框，自下拉式清單中選擇一個或是多個國家物件設定檔，選定的設定檔將可視爲輸入國家過濾器，您可以按下圖示 建立其他的過濾器設定檔。
目標國家過濾器	**目的國家物件 (至多 15 個國家)** -按下三角圖示 ▶ 以顯示設定檔選擇框，自下拉式清單中選擇一個或是多個國家物件設定檔，選定的設定檔將可視爲輸出國家過濾器，您可以按下圖示 建立其他的過濾器設定檔。
來源 IP	**來源 IPv6 物件** - 按下三角圖示 ▶ 以顯示設定檔選擇框，自下拉式清單中選擇一個或是多個 IP 物件設定檔，選定的設定檔被視爲來源目標，您可以按下圖示 建立其他的 IPv6 物件設定檔。

目標 IP	**目的 IPv6 物件-** 按下三角圖示 ▶ 以顯示設定檔選擇框，自下拉式清單中選擇一個或是多個 IP 物件設定檔，選定的設定檔被視爲目的目標，您可以按下圖示 建立其他的 IPv6 物件設定檔。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

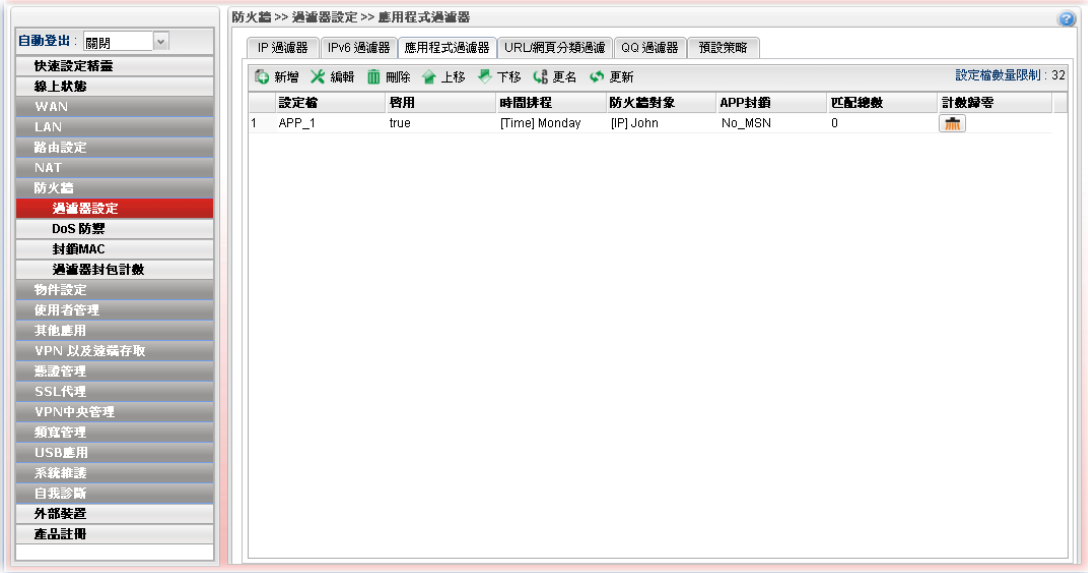
9. 輸入所有設定並按下**套用**儲存。

10. 新的 IPv6 過濾器規則已經建立在 IPv6 過濾器群組下(本例中名爲 For_IPv61)。

注意：在特定的 IPv6 過濾器群組下可以建立多個 IPv6 過濾器規則。

4.5.1.3 應用程式過濾器

應用程式過濾器可以整合數種應用程式物件在一個設定檔下，以限制應用程式的運用。例如，這個功能可以封鎖 IP 物件設定檔中指定的使用者無法使用即時通訊軟體，無法使用點對點檔案分享且無法透過特定協定下載任何檔案。



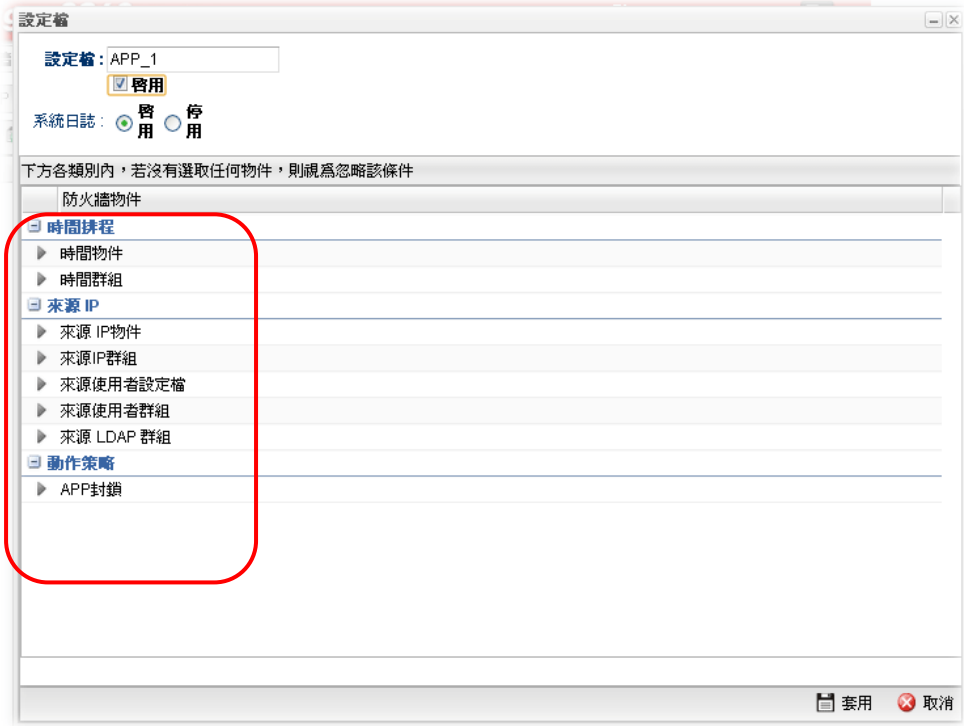
每個項目說明如下：

項目	說明
新增	新增新的設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
刪除	移除選定的設定檔。 請選擇您想要刪除的既有設定檔，然後按下刪除按鈕，該設定檔即可被移除。
上移	將設定檔往上移動改變選定設定檔的順序。
下移	將設定檔往下移動改變選定設定檔的順序。
更名	按此鈕後將會跳出視窗，讓您修改選定設定檔的檔名。 在使用此功能之前，至少要有一個設定檔存在始可運作。
更新	重新更新本頁面。
設定檔	顯示應用程式過濾器設定檔的檔名。
啓用	顯示設定檔狀態，False 表示停用；True 表示啓用。
時間排程	如果尚未設定任何時間物件，本區只會呈現”無”這個項目。
防火牆對象	顯示此應用程式設定檔套用之 IP 物件設定檔名。
APP 封鎖	顯示此應用程式設定檔選擇的 APP 物件設定檔的檔名。

項目	說明
計數歸零	按下此圖示可刪除選定的設定檔。

如何建立應用程式過濾器設定檔

1. 開啓**防火牆>>過濾器設定**並按下**應用程式過濾器**標籤。
2. 按下**新增**按鈕。
3. 下述頁面將會出現。按下圖示▶顯示設定檔選擇框(紅框處)。



可用參數詳列如下：

項目	說明
設定檔	輸入應用程式過濾器規則之設定檔名稱。
啓用	勾選此框啓用此設定檔。
系統日誌	按下啓用以便記錄**系統維護>>系統日誌/郵件警示>>系統日誌檔案**中防火牆採取之動作的歷程。
時間排程	**時間物件** – 按下三角圖示 ▶ 以顯示設定檔選擇框，選擇適當的排程套用至此應用程式過濾器規則。 您可以按下圖示 來建立另一個時間物件設定檔，或是您可以按下編輯圖示 修改現有的物件設定檔。 **時間群組** - 按下三角圖示 ▶ 以顯示設定檔選擇框，選擇適當的時間群組設定檔套用至此應用程式過濾器規則。按下圖示 可建立其他的時間群組設定檔，或是您可以按下編輯圖示 修改現有的群組設定檔。

來源 IP	**來源 IP 物件** - 按下三角圖示 ▶ 以顯示設定檔選擇框，自下拉式清單中選擇一個或是多個 IP 物件設定檔，當此應用程式過濾器設定檔被套用的時候，路由器將據此過濾選定的 IP 物件，您可以按下圖示 建立其他的 IP 物件設定檔，或是按下編輯圖示 修改現有的物件設定檔。 **來源 IP 群組** - 按下三角圖示 ▶ 以顯示設定檔選擇框，自下拉式清單中選擇一個或是多個 IP 群組設定檔，當此應用程式過濾器設定檔被套用的時候，路由器將據此過濾選定的 IP 群組，您可以按下圖示 建立其他的 IP 群組設定檔，或是按下編輯圖示 修改現有的群組設定檔。 **來源使用者設定檔** – 按下三角圖示 ▶ 以顯示設定檔選擇框，自下拉式清單中選擇一個或是多個使用者設定檔，選定的設定檔被視爲來源目標，當此應用程式過濾器設定檔被套用的時候，路由器將據此過濾選定的使用者，您可以按下圖示 建立其他的使用者物件設定檔，或是按下編輯圖示 修改現有的使用者設定檔。 **來源使用者群組** – 按下三角圖示 ▶ 以顯示設定檔選擇框，自下拉式清單中選擇一個或是多個使用者群組，選定的設定檔被視爲來源目標，當此應用程式過濾器設定檔被套用的時候，路由器將據此過濾選定的使用者，您可以按下圖示 建立其他的使用者群組設定檔，或是按下編輯圖示 修改現有的使用者群組設定檔。 **來源 LDAP 群組** – 按下三角圖示 ▶ 以顯示設定檔選擇框，自下拉式清單中選擇一個或是多個 LDAP 群組設定檔，選定的設定檔被視爲來源目標，當此應用程式過濾器設定檔被套用的時候，路由器將據此過濾選定的使用者，您可以按下圖示 建立其他的 LDAP 群組設定檔，或是按下編輯圖示 修改現有的 LDAP 群組設定檔。
動作策略)	**APP 封鎖** - 按下三角圖示 ▶ 以顯示設定檔選擇框，自下拉式清單中選擇一個或是多個 APP 物件設定檔，當此應用程式過濾器設定檔被套用的時候，路由器將據此過濾 APP 物件，您可以按下圖示 建立其他的 APP 物件設定檔，或是按下編輯圖示 修改現有的 APP 物件設定檔。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

4. 輸入所有設定並按下套用儲存。
5. 新的應用程式過濾器設定檔已建立完成並呈現在畫面上。

4.5.1.4 URL/網頁分類過濾器

URL 過濾器可以整合 URL、關鍵字、副檔名與 WCF 物件設定檔於一個設定檔內，以便限制特定使用者存取網際網路。

每個項目說明如下：

項目	說明
新增	新增新的設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
刪除	移除選定的設定檔。 請選擇您想要刪除的既有設定檔，然後按下刪除按鈕，該設定檔即可被移除。
更新	重新更新本頁面。
上移	將設定檔往上移動改變選定設定檔的順序。
下移	將設定檔往下移動改變選定設定檔的順序。

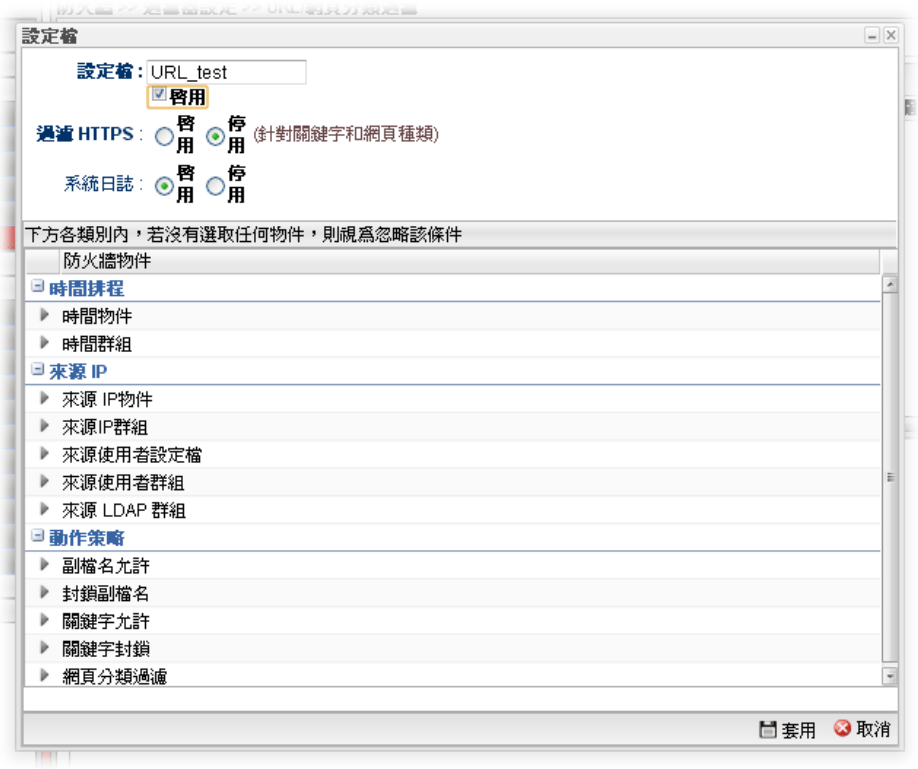
項目	說明
更名	按此鈕後將會跳出視窗，讓您修改選定設定檔的檔名。 在使用此功能之前，至少要有一個設定檔存在始可運作。
設定檔數量限制	顯示可以建立的設定檔的總數。
設定檔	顯示分類過濾器設定檔的檔名。
啓用	顯示設定檔狀態，False 表示停用；True 表示啓用。
過濾器 **Https**	顯示 HTTPs 過濾器是啓動的或是關閉的。
時間排程	如果尚未設定任何時間物件，本區只會呈現”無”這個項目。
防火牆對象	顯示此應用程式設定檔套用之 IP 物件設定檔名。
允許	顯示此過濾器規則允許路由器接受的關鍵字/副檔名物件設定檔。
封鎖	顯示此過濾器規則拒絕路由器接受的關鍵字/副檔名物件設定檔
封鎖網頁	顯示此過濾器規則拒絕路由器接受的網頁目錄物件設定檔。
計數歸零	按下此圖示可刪除選定的設定檔。
設定檔	顯示此過濾器規則選擇的使用者物件設定檔的檔名。
使用者群組	顯示此過濾器規則選擇的使用者群組設定檔的檔名。
使用預設訊息	**啓用** – 在使用者嘗試登入封鎖的網頁時，預設的訊息會顯示在頁面上。 **停用** – 在使用者嘗試登入封鎖的網頁時，手動輸入的訊息會顯示在頁面上。
預設網頁目錄管理訊息	本區僅在使用預設訊息失效時始有作用。 使用者嘗試登入封鎖的網頁時，訊息將顯示於使用者的瀏覽器上。
使用 **HTTPs** 過濾器預設訊息	**啓用** – 在使用者嘗試透過 HTTPs 登入封鎖的網頁時，預設的訊息會顯示在頁面上。 **停用** – 在使用者嘗試透過 HTTPs 登入封鎖的網頁時，手動輸入的訊息會顯示在頁面上。
使用 **HTTPs** 網頁過濾訊息	使用者嘗試透過 HTTPs 登入封鎖的網頁時，訊息將顯示於使用者的瀏覽器上。
套用	按此鈕儲存設定。
取消	按此鈕捨棄本頁任何設定。

如何建立 URL 過濾器設定檔

1. 開啓**防火牆>>過濾器設定**並按下 **URL/網頁目錄過濾器**標籤。

2. 按下**新增**按鈕。

3. 下述頁面將會出現。



可用參數詳列如下：

項目	說明
設定檔	輸入設定檔的名稱。
啓用	勾選此框啓用此設定檔。
過濾器 Https (Filter https)	**啓用** – 選擇此項啓用 HTTPS 過濾功能。 **停用** – 如果此規則只針對關鍵字和網頁目錄，請選擇**停用**。
系統日誌	按下啓用以便記錄**系統維護>>系統日誌/郵件警示>>系統日誌檔案**中防火牆採取之動作的歷程。
時間排程	**時間物件** – 按下三角圖示 ▶ 以顯示設定檔選擇框，選擇適當的排程套用至此規則。 您可以按下圖示 來建立另一個時間物件設定檔，或是您可以按下編輯圖示 修改現有的物件設定檔。 **時間群組** - 按下三角圖示 ▶ 以顯示設定檔選擇框，選擇適當的時間群組設定檔套用至此過濾器規則。 按下圖示 可建立其他的時間群組設定檔，或是您可以按下編輯圖示 修改現有的群組設定檔。
來源 I	**來源 IP 物件** - 按下三角圖示 ▶ 以顯示設定檔選擇框，自下拉式清單中選擇一個或是多個 IP 物件設定檔，當此 URL 過濾器設定檔被套用的時候，路由器將據此過濾選

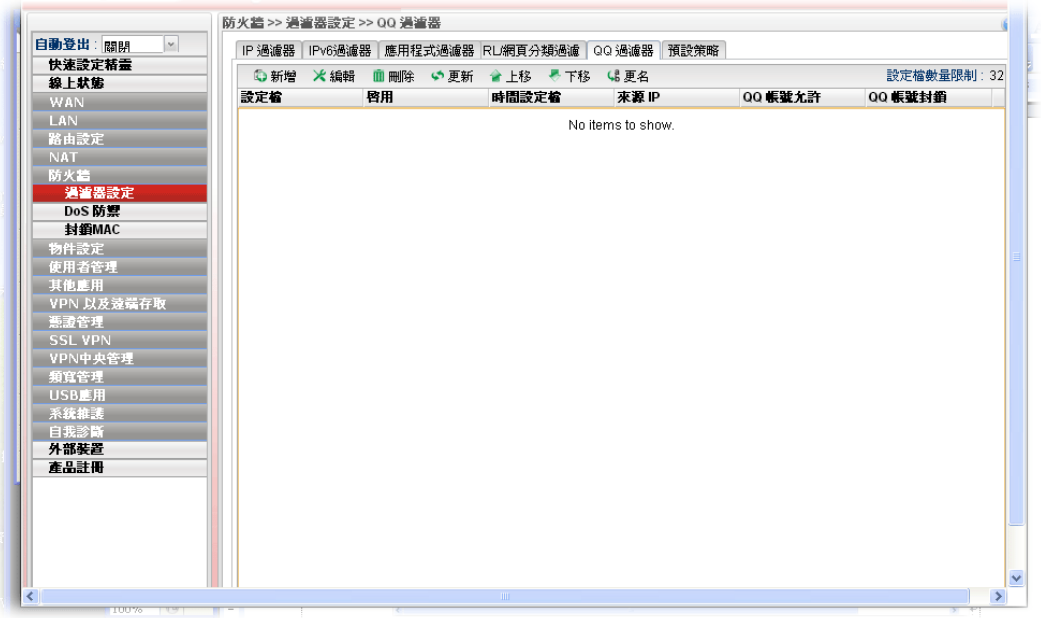
	定的 IP 物件，您可以按下圖示 建立其他的 IP 物件設定檔，或是按下編輯圖示 修改現有的物件設定檔。 **來源 IP 群組** - 按下三角圖示 ▶ 以顯示設定檔選擇框，自下拉式清單中選擇一個或是多個 IP 群組設定檔，當此 URL 過濾器設定檔被套用的時候，路由器將據此過濾選定的 IP 群組，您可以按下圖示 建立其他的 IP 群組設定檔，或是按下編輯圖示 修改現有的群組設定檔。 **來源使用者設定檔** – 按下三角圖示 ▶ 以顯示設定檔選擇框，自下拉式清單中選擇一個或是多個使用者設定檔，選定的設定檔被視爲來源目標，當此 URL 過濾器設定檔被套用的時候，路由器將據此過濾選定的使用者，您可以按下圖示 建立其他的使用者物件設定檔，或是按下編輯圖示 修改現有的使用者設定檔。 **來源使用者群組** – 按下三角圖示 ▶ 以顯示設定檔選擇框，自下拉式清單中選擇一個或是多個使用者群組，選定的設定檔被視爲來源目標，當此 URL 過濾器設定檔被套用的時候，路由器將據此過濾選定的使用者，您可以按下圖示 建立其他的使用者群組設定檔，或是按下編輯圖示 修改現有的使用者群組設定檔。 **來源 LDAP 群組** – 按下三角圖示 ▶ 以顯示設定檔選擇框，自下拉式清單中選擇一個或是多個 LDAP 群組設定檔，選定的設定檔被視爲來源目標，當此 URL 過濾器設定檔被套用的時候，路由器將據此過濾選定的使用者，您可以按下圖示 建立其他的 LDAP 群組設定檔，或是按下編輯圖示 修改現有的 LDAP 群組設定檔。
動作策略	**副檔名允許/封鎖副檔名**- 按下三角圖示 ▶ 以顯示設定檔選擇框，自下拉式清單中選擇一個或是多個副檔名物件設定檔，當此 URL 過濾器設定檔被套用的時候，路由器將據此過濾接受或拒絕選定的副檔名，您可以按下圖示 建立其他的物件設定檔，或是按下編輯圖示 修改現有的物件設定檔。 **關鍵字允許/封鎖關鍵字** - 按下三角圖示 ▶ 以顯示設定檔選擇框，自下拉式清單中選擇一個或是多個關鍵字物件設定檔，當此 URL 過濾器設定檔被套用的時候，路由器將據此過濾接受或拒絕選定的關鍵字，您可以按下圖示 建立其他的關鍵字物件設定檔，或是按下編輯圖示 修改現有的物件設定檔。 **網頁分類過濾** - 按下三角圖示 ▶ 以顯示設定檔選擇框，自下拉式清單中選擇一個或是多個網頁分類物件設定檔，當此 URL 過濾器設定檔被套用的時候，路由器將據

	此過濾以拒絕選定的網頁分類的內容，您可以按下圖示 建立其他的網頁分類物件設定檔，或是按下編輯圖示 修改現有的物件設定檔。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

4. 輸入所有設定並按下**套用**儲存。
5. 新增 URL 過濾器設定檔已經建立完成。

4.5.1.5 QQ 過濾器

本頁僅適用中國使用者，居住於中國以外地區的用戶，可跳過此節。



每個項目說明如下：

項目	說明
新增	新增新的 QQ 過濾器設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
刪除	移除選定的設定檔。 請選擇您想要刪除的既有設定檔，然後按下刪除按鈕，該設定檔即可被移除。
更新	重新更新本頁面。
上移	將設定檔往上移動改變選定設定檔的順序。
下移	將設定檔往下移動改變選定設定檔的順序。
更名	按此鈕後將會跳出視窗，讓您修改選定設定檔的檔名。 在使用此功能之前，至少要有一個設定檔存在始可運作。
設定檔數量限制	顯示可以建立的設定檔的總數。
設定檔	顯示設定檔的檔名。
啓用	顯示設定檔狀態，False 表示停用；True 表示啓用。
時間設定檔	如果尚未設定任何時間排程，本區只會呈現”無”這個項目。
來源 IP	顯示每個規則套用的 IP 物件設定檔。

項目	說明
QQ 帳戶允許	在選定 QQ 設定檔已經啟用的情況下，顯示允許通過的帳戶名稱。
QQ 帳戶封鎖	在選定 QQ 設定檔已經啟用的情況下，顯示拒絕通過的帳戶名稱。

如何建立 QQ 過慮器設定檔

1. 開啟**防火牆>>過濾器設**並按下 **QQ 過濾器**標籤。
2. 按下**新增**按鈕。
3. 下述頁面將會出現。

可用參數詳列如下：

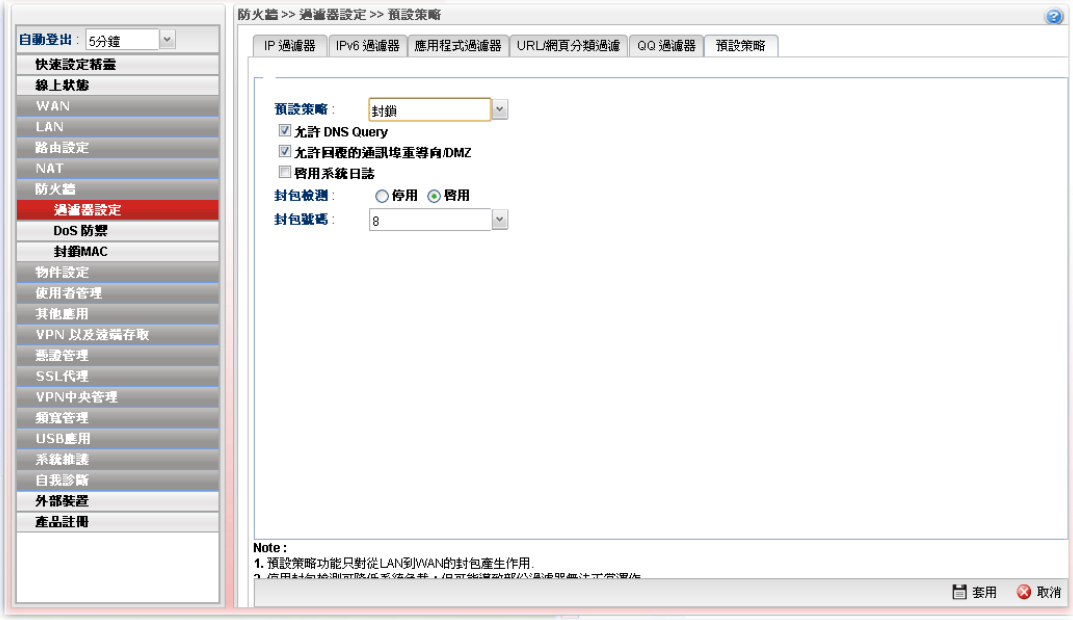
項目	說明
設定檔	輸入 QQ 過濾器設定檔之檔名。
啟用	勾選此框啟用此設定檔。
時間設定檔	使用下拉式清單定設定檔的時間排程。 您可以按下 建立另一個新的時間物件排程以便加以利用。
來源 IP	指定此設定檔需求的使用者設定，當此設定檔被啟用時，在來源 IP 範圍中的使用者皆由 Vigor 路由器進行過濾。
QQ 帳戶允許	使用下拉式清單指定 QQ 帳戶設定檔，選定的設定檔不會受到 Vigor 路由器的封鎖對待。 您可以按下 建立另一個新的 QQ 帳戶以便加以利用。

項目	說明
QQ 帳戶封鎖	使用下拉式清單指定 QQ 帳戶設定檔，選定的設定檔將受到 Vigor 路由器的封鎖對待。 您可以按下 建立另一個新的 QQ 帳戶以便加以利用。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

4. 輸入所有設定並按下套用儲存。
5. 的 QQ 設定檔已經建立完成。

4.5.1.6 預設策略

如果 IP 過濾器、應用程式過濾器、URL/網頁目錄過濾器以及 QQ 過濾器皆不適合輸入封包時，預設策略將套用至所有輸入的封包上。



可用參數詳列如下：

項目	說明
預設策略	**允許** – 所有的輸入封包都可通過 Vigor 路由器，不會有任何的阻礙。 **封鎖** – 所有的輸入封包皆無法通過，除了下述例外： ● **允許 DNS Query** – 勾選此框讓 DNS 詢問能通過 Vigor 路由器的防火牆。 ● **允許回覆的通訊埠重導向/DMZ** – 勾選此框讓埠號重導向/DMZ 處理的輸出封包能通過 Vigor 路由器的防火牆。 ● **啓用系統日誌** – 勾選此框讓封鎖的封包其相關資訊能記錄在系統日誌中。

項目	說明
	上述三種策略在**防火牆>>過濾器設定>>IP 過濾器/應用程式過濾器**頁面中都可以進行設定。
封包檢測	**停用** – 不執行任何檢測。 **啓用** – 執行封包檢測。
封包號碼	如果啓用了**封包檢測**，可在此區選擇受檢的封包數。可選的範圍從 4 到 16。例如您選擇了“8”，即表示只有前 8 個封包需要經過防火牆的規則檢測，其餘的封包則直接放行。
套用	按此鈕儲存設定。
取消	按此鈕捨棄頁面設定。

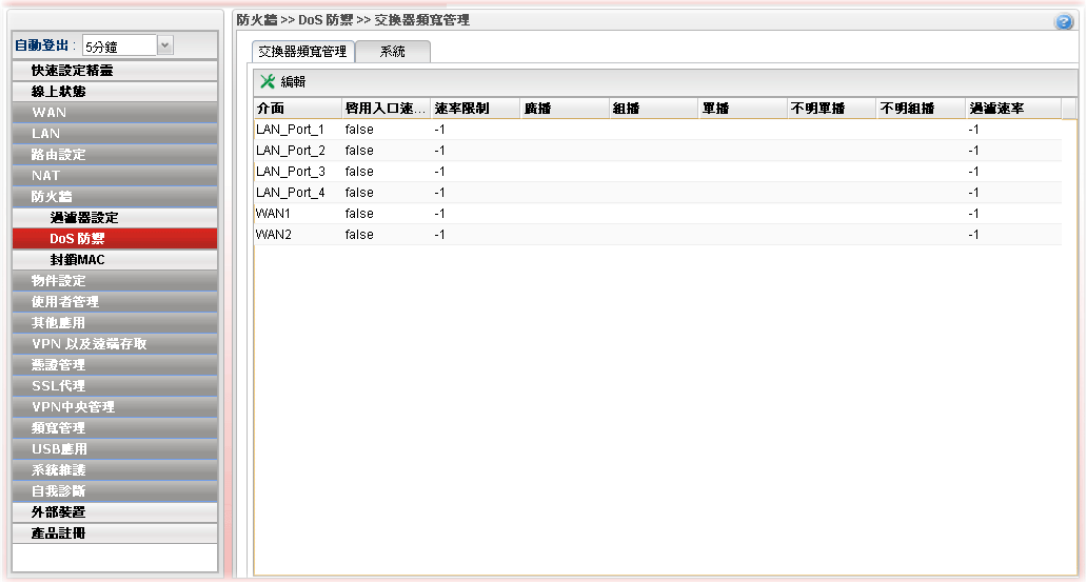
完成設定後，按下**套用**儲存設定。

4.5.2 DoS 防禦

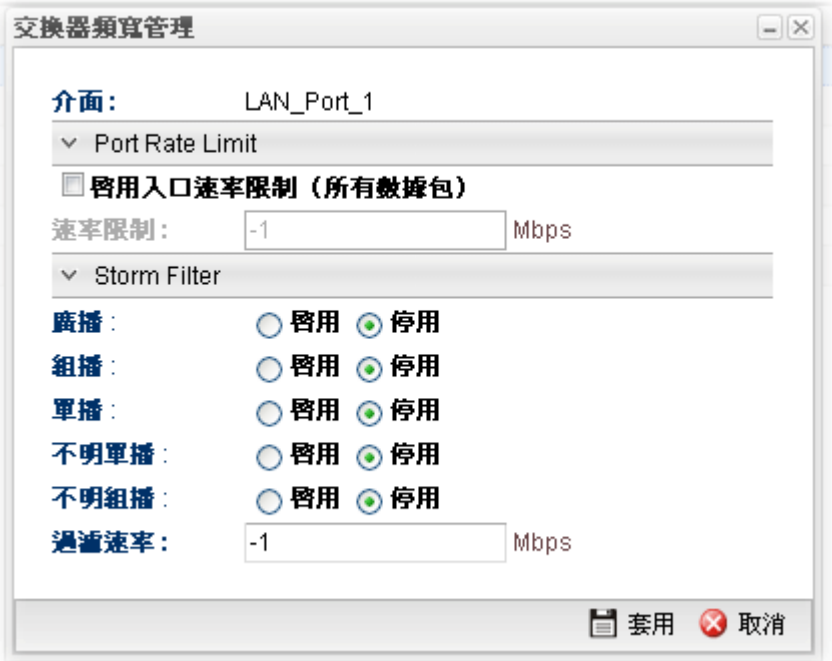
DoS 功能可偵測並降低 DoS 的攻擊。

4.5.2.1 交換器速率限制

預設介面設定檔顯示於頁面上。



您可以針對每個介面設定檔手動修改速率限制。請選擇任一設定檔再按下**編輯**。



可用參數詳列如下：

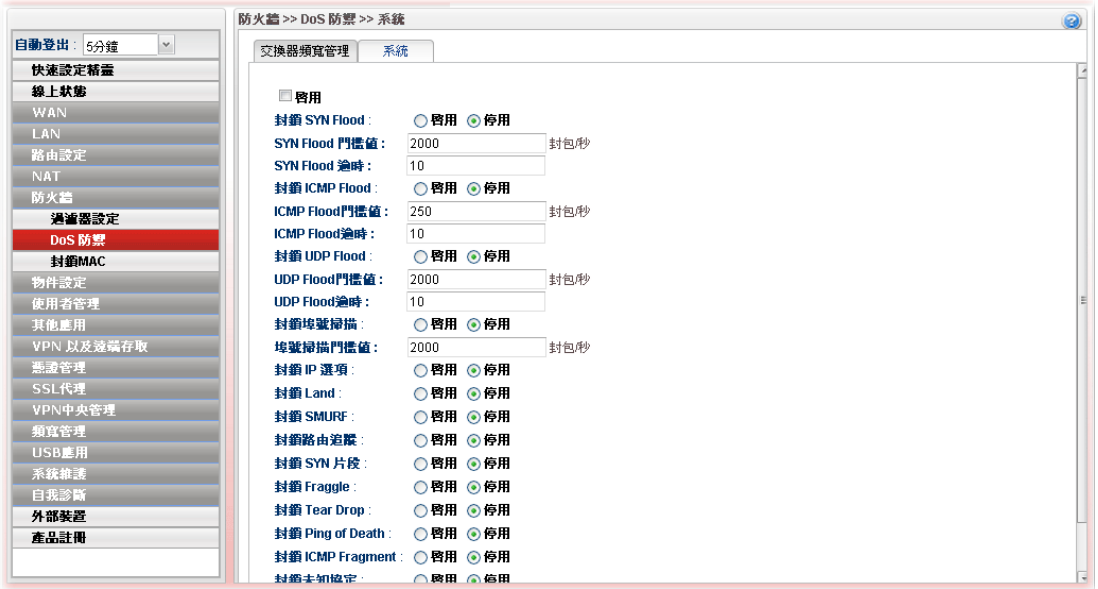
項目	說明
介面	顯示選定的介面名稱。
Port Rate Limit	**啓用入口速率限制(所有數據包)** – 勾選此框讓所有的封包都受到入口速率限制。 **速率限制** – 預設值爲-1，表示沒有限制。如有限制需求，請在此輸入需求的速率值。
Storm Filter	**廣播** - 按下**啓用**以封鎖來自廣播風暴(broadcast Storm)的封包攻擊。 **組播** - 按下**啓用**以封鎖來自組播風暴(Multicast Storm)的封包攻擊。 **單播** – 按下**啓用**以封鎖來自單播風暴(Unicast Storm)的封包攻擊。 **不明單播** - 按下**啓用**以封鎖來自未知單播風暴(Unknown Unicast Storm)的封包攻擊。 **未知組播** - 按下**啓用**以封鎖來自未知組播風暴(Unknown Multicast Storm)的封包攻擊。 **過濾速率** - 輸入過濾速度所需的數值(1~4096，單位爲64Kpbs)。
套用	按此鈕儲存設定。

完成設定後，按下套用儲存設定。

4.5.2.2 系統

在**防火牆**群組中，按下 **DoS 防禦**並按下**系統**標籤，您將看到如下設定頁面。DoS 攻擊引擎檢測每個流入封包並對照攻擊特徵資料庫，任何可能癱瘓安全區域主機的封包都

會被系統封鎖在外。DoS 攻擊防禦引擎也監控流量行爲，任何違反 DoS 攻擊防禦設定的異常狀況都會提報給系統以緩解攻擊。



可用參數詳列如下：

項目	說明
啓用	勾選此框啓用此設定檔。
封鎖 SYN flood	勾選此項以啓動 SYN 攻擊防禦功能，一旦檢查到 TCP SYN 封包的門檻值超過定義數值，Vigor 路由器在所設定之逾時期間即開始捨棄其後之 TCP SYN 封包，這項功能的目的是防止 TCP SYN 封包嚐試耗盡路由器有限的資源。
SYN Flood 門檻值	門檻值的預設值爲每秒 2000 個封包。
SYN Flood 逾時	逾時的預設值 10 秒。
封鎖 ICMP Flood	勾選**啓用**以啓動 ICMP 攻擊防禦功能。 如果 ICMP 回應網際網路之需求超過使用者定義的門檻值，路由器在逾時的範圍內將捨棄隨後的回應請求。
CMP Flood 門檻值	門檻值的預設值爲每秒 250 個封包。
CMP Flood 逾時	逾時的預設值 10 秒。
封鎖 UDP Flood	勾選**啓用**以啓動 UDP 攻擊防禦功能，一旦檢查到 UDP 封包門檻值超過定義數值，Vigor 路由器在所設定之逾時期間即開始捨棄其後之 UDP 封包。 **注意**：勾選此項之後，若有大量流量進出，機制啓動時，設備會無法上網，但內網仍可順利連到管理介面。
UDP Flood 門檻值	門檻值的預設值爲每秒 2000 個封包。
UDP Flood 逾時	逾時的預設值 10 秒。
封鎖埠號掃描	勾選**啓用**以啓動通訊埠掃瞄檢測功能，當利用通訊埠掃瞄

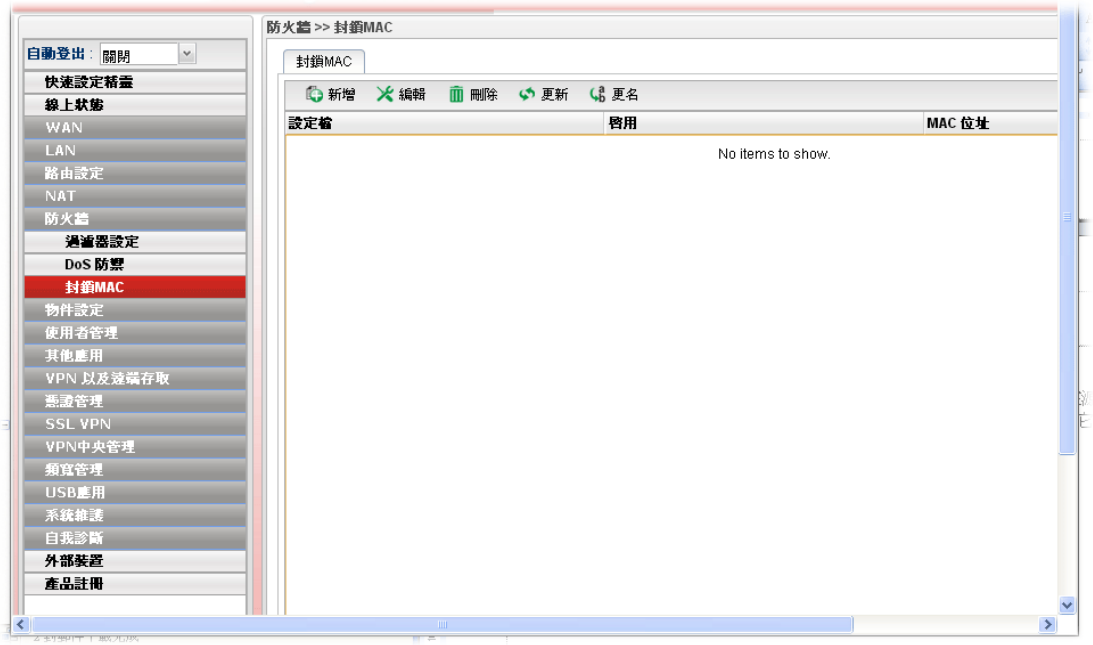
項目	說明
	門檻值速率而檢測出惡意探測之行爲時，Vigor 路由器將傳送警告訊息出去
埠號掃描門檻值	門檻值的預設值爲每秒 2000 個封包。
封鎖 IP 選項	勾選**啓用**以啓動阻攔 IP options 功能，Vigor 路由器將會忽略資料封包頭中(含 IP 選項區)的 IP 封包。限制的原因是 IP option 的出現是區域網路安全性中的弱點，因爲它攜帶令人注意的資訊像是安全性、TCC (封閉使用者群組)參數、網際網路位址、路由訊息等等，讓外部的竊聽者有機會取得您虛擬網路的細節內容。
封鎖 Land	勾選**啓用**以強迫 Vigor 路由器防護 Land 攻擊，Land 攻擊結合含 IP spoofing 的 SYN 攻擊技術，當駭客傳送 spoofed SYN 封包(連同相同來源和目的位址)，以及通訊埠號至受害一方時，Land 攻擊即由此發生。
封鎖 SMURF	勾選**啓用**以啓動封鎖 SMURF 攻擊功能，Vigor 路由器將忽略任何一次的播送 ICMP 回應需求。
封鎖路由追蹤	勾選**啓用**以強迫 Vigor 路由器不轉送任何路由封包的行蹤。
封鎖 SYN Fragment 片段	勾選**啓用**以啓動封鎖 SYN Fragment 的封包功能。Vigor 路由器將會停止任何具有 SYN 旗標及更多的區段設定之封包傳送作業。
封鎖 Fraggle	勾選此項以啓動封鎖 Fraggle 攻擊功能，任何播送來自網際網路的 UDP 封包都會被封鎖起來。 啓動 DoS/DDoS 防禦功能可能會阻擋一些合法的封包，例如當您啓動 fraggle 攻擊防禦時，所有來自網際網路的 UDP 封包播送都會被阻擋在外，因此得自網際網路的 RIP 封包全都會被阻擋掉。
封鎖 Tear Drop	勾選**啓用**以啓動封鎖 Tear Drop 攻擊功能，很多機器在接收到超過最大值得 ICMP 資料段(封包)時，系統就會當機。爲了避免這類型的攻擊行爲，Vigor 路由器便被設計成具有捨棄片段 ICMP (超過 1024 位元組)封包的能力。
封鎖 Ping of Death	勾選**啓用**以啓動封鎖 Ping of Death 攻擊功能，這項攻擊意味著犯罪者傳送重疊封包至目的主機，這些目的主機一旦重新建構封包時就會造成當機現象，Vigor 路由器將會阻擋此種攻擊活動的封包進入。
封鎖 ICMP Fragment	勾選**啓用**以啓動封鎖 ICMP 封包片段功能，任何含有多個片段的 ICMP 封包都會被捨棄阻擋。
封鎖未知協定	勾選**啓用**以啓動封鎖不明封包協定封包功能，個別 IP 封包在資料段封包頭中都擁有一個協定區域，指名該協定於上層運作的類型。
套用	按此鈕儲存設定。

項目	說明
取消	按此鈕捨棄頁面設定。

完成設定後，按下**套用**儲存設定。

4.5.3 封鎖 MAC

封鎖 MAC 允許您設定大量 MAC 位址，如果封包的來源或目標 MAC 位址符合指定 MAC 位址，該封包將會被捨棄。MAC 封鎖的優點再於它可以過濾一些不必要的封包或是來自區域網路端攻擊封包。



每個項目說明如下：

項目	說明
新增	新增新的設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
刪除	移除選定的設定檔。 請選擇您想要刪除的既有設定檔，然後按下刪除按鈕，該設定檔即可被移除。
更新	重新更新本頁面。
更名	按此鈕後將會跳出視窗，讓您修改選定設定檔的檔名。 在使用此功能之前，至少要有一個設定檔存在始可運作。
設定檔數量限制	顯示可以建立的設定檔的總數。
設定檔	顯示設定檔的檔名。
啓用	顯示設定檔狀態，False 表示停用；True 表示啓用。

項目	說明
MAC 位址	顯示此設定檔的 MAC 位址。

如何建立 MAC 封鎖設定檔

1. 開啓**防火牆>>封鎖 MAC**。
2. 按下**新增**按鈕。
3. 下述頁面將會出現。

可用參數詳列如下：

項目	說明
設定檔	輸入此設定檔的檔名。
啓用	勾選此框啓用此設定檔。
MAC 位址	路由器將封鎖此處設定檔指定的MAC位址，請輸入位址。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

4. 輸入所有設定並按下**套用**儲存。
5. 新的 MAC 封鎖設定檔已建立完成。

4.5.4 過濾器封包計數

本頁顯示防火牆群組、規則資訊、IPv6 過濾器、應用程式過濾器與 URL/網頁過濾器的紀錄或是狀態。

按下 IP 過濾器、IPv6 過濾器、應用程式過濾器與 URL/網頁過濾器標籤即可取得每種過濾器的狀態資訊。

若本頁沒有顯示特定規則之相關資料(計數爲”0”)即表示該規則可能設定錯誤或是被其他規格封鎖住。管理者或是使用者可以據此調整其過濾器的規則以符合實際需求。

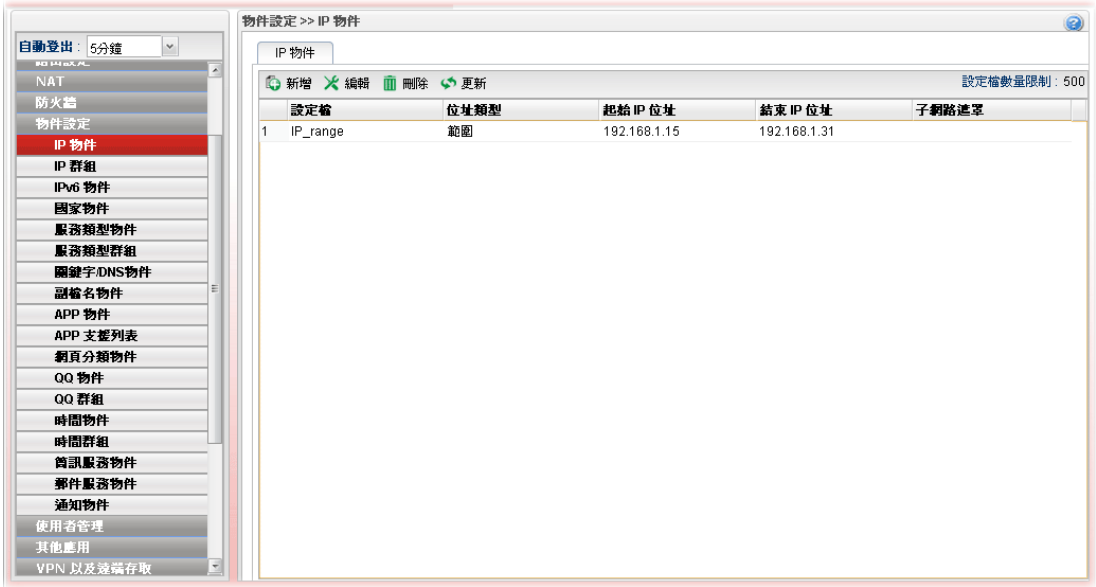
4.6 物件設定

Vigor2960 允許使用者建立各種不同且以 IP 位址、服務類型、關鍵字、副檔名、即時通訊、P2P、協定、網頁分類、QQ 應用、時間設定、簡訊服務、郵件服務與通知應用爲基準的過濾器設定檔，這些物件檔皆可運用於防火牆中。

4.6.1 IP 物件

通常，在路由器的配置中會將某些 IP 位址設定於限制範圍內，這種情況我們可先將他們定義爲物件並整合數個物件形成一個群組，如此即可方便運用，之後，在不同的網頁選擇該物件/群組加以套用，例如同一棟公寓中所有的 IP 可以定義在一個 IP 物件(以 IP 範圍來限定)當中。

本頁讓您指定 IP 位址，IP 位址範圍或是子網遮罩，將其設定爲一個物件以便之後套用於**防火牆**設定中。



每個項目說明如下：

項目	說明
新增	新增新的設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
刪除	移除選定的設定檔。 請選擇您想要刪除的既有設定檔，然後按下刪除按鈕，該設定檔即可被移除。
更新	重新更新本頁面。
設定檔數量限制	顯示可以建立的設定檔總數。
設定檔	顯示設定檔的檔名。
位址類型	顯示此設定檔的位址類型(如單一、範圍或是子網)。

項目	說明
起始 IP 位址	顯示此設定檔 IP 位址範圍的起始點。
結束 IP 位址	顯示此設定檔 IP 位址範圍的結束點。 當您選擇**範圍**爲**位址類型**時，這個選項與起始 IP 位址搭配運用。
子網路遮罩	顯示此設定檔的子網遮罩。

如何新增 IP 物件設定檔

1. 開啓**物件設定>>IP 物件**。
2. 按下**新增**按鈕。
3. 下述頁面將會出現。

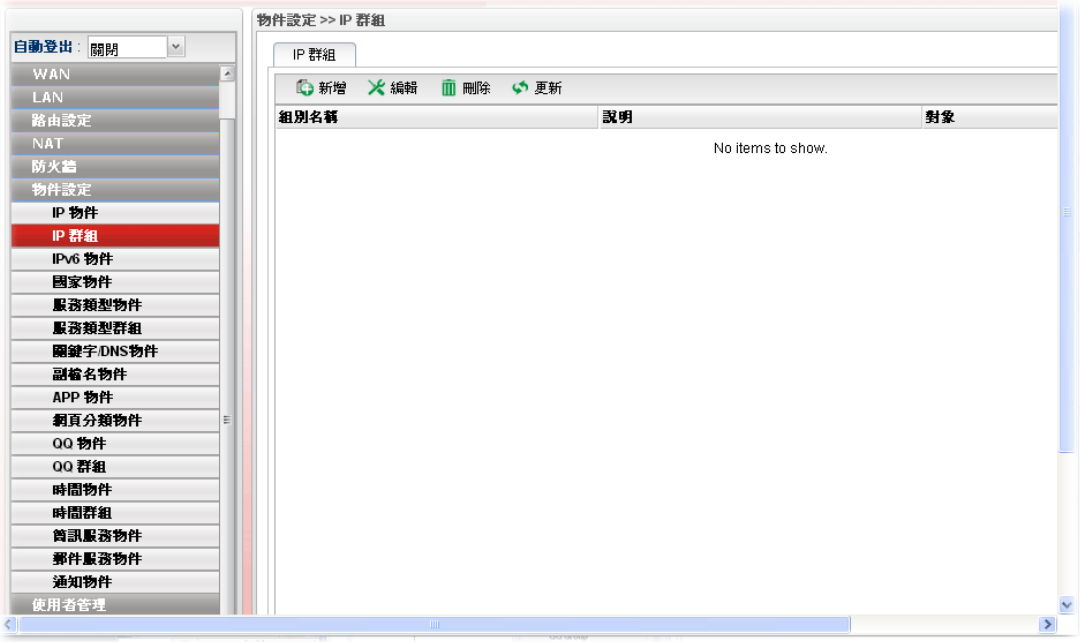
可用參數詳列如下：

項目	說明
設定檔	輸入設定檔的檔名。
位址類型	選擇此設定檔的位址類型(包含 Single、範圍與子網)。
起始 IP 位址	輸入此設定檔的起始 IP 位址。
結束 IP 位址	輸入此設定檔的結束 IP 位址。 當您選擇**範圍**爲**位址類型**時，這個選項與起始 IP 位址搭配運用。
子網路遮罩	當您選擇**子網路遮罩**爲**位址類型**時，請使用下拉式清單選則需求之子網路遮罩。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

4. 輸入所有設定並按下**套用**儲存。
5. 新 IP 物件設定檔已經建立完成。

4.6.2 IP 群組

爲了更加方便管理，數個 IP 物件可以組合成一個群組，不同的 IP 群組可包含不同的 IP 物件設定檔。



每個項目說明如下：

項目	說明
新增	新增新的設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
刪除	移除選定的設定檔。 請選擇您想要刪除的既有設定檔，然後按下刪除按鈕，該設定檔即可被移除。
更新	重新更新本頁面。
設定檔數量限制	顯示可以建立的設定檔總數。
組別名稱	顯示物件群組的檔名。
說明	顯示關於此設定檔的簡易說明。
對象	顯示納入此群組下的物件有哪些。

如何新增 IP 群組設定檔

1. 開啓**物件設定>>IP 群組**。
2. 按下**新增**按鈕。
3. 下述頁面將會出現。

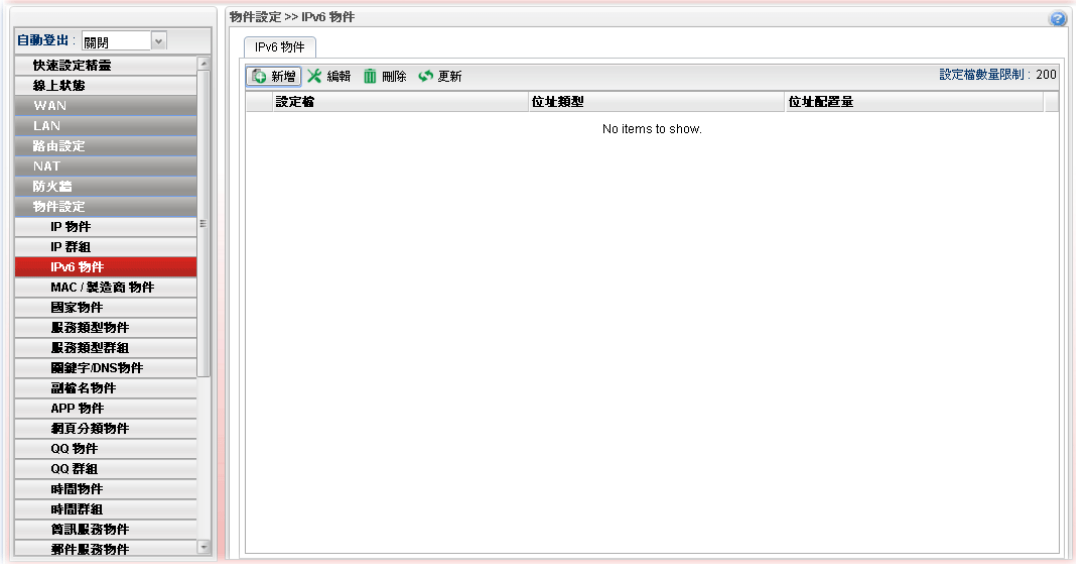
可用參數詳列如下：

項目	說明
組別名稱	輸入物件群組的設定檔名。
說明	如果設定檔名不夠清晰，可在此針對此設定檔提供簡易說明。
對象	使用下拉式清單勾選那入此群組中的 IP 物件設定檔。 所有在**物件設定>>IP 物件**選單中建立且可用的 IP 物件都可在此呈現供您選取。 如欲刪除選定的設定檔，可按 ✕ 將該物件項目移除。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

4. 輸入所有設定並按下**套用**儲存。
5. 新 IP 群組設定檔已經建立完成。

4.6.3 IPv6 物件

您可以設定高達 200 組，各含不同條件的 IPv6 物件。

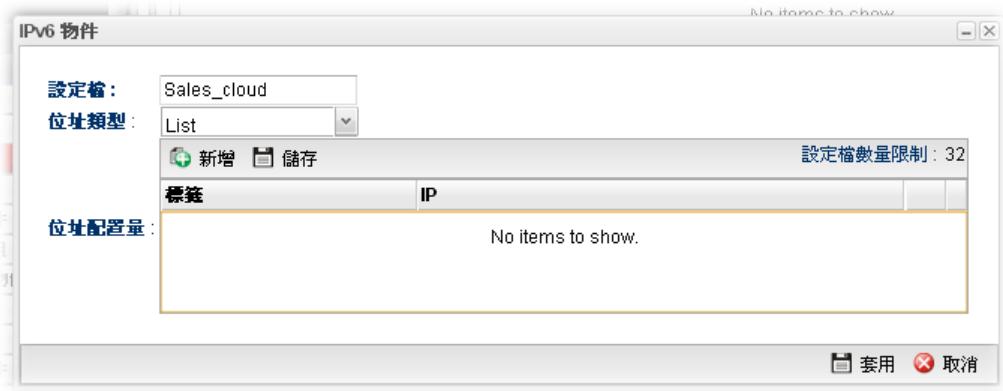


每個項目說明如下：

項目	說明
新增	新增新的設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
刪除	移除選定的設定檔。 請選擇您想要刪除的既有設定檔，然後按下刪除按鈕，該設定檔即可被移除。
更新	重新更新本頁面。
設定檔數量限制	顯示可以建立的設定檔總數。
設定檔	顯示設定檔的檔名。
位址類型	顯示此設定檔的位址類型。
位址配置量	顯示物件的 IP 位址/IP 範圍/子網遮罩內容。

如何新增 IPv6 物件設定檔

1. 開啓**物件設定>>IPv6 物件**。
2. 按下**新增**按鈕。
3. 下述頁面將會出現。



可用參數詳列如下：

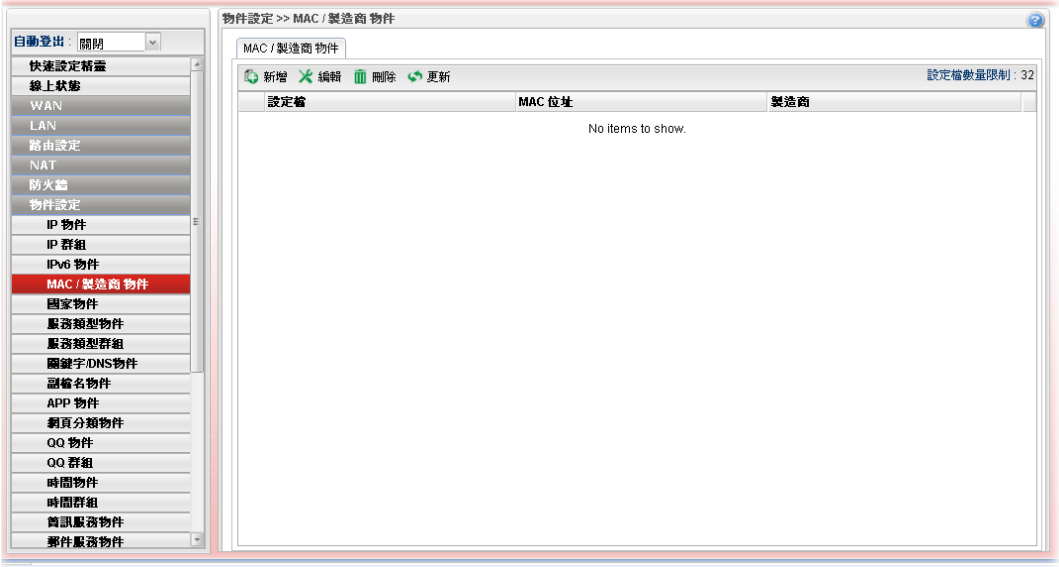
項目	說明
設定檔	輸入設定檔的檔名。
位址類型	有三種類型可以選擇： **List** – 用來指定 IP 位址。 **範圍**– 用來指定一定範圍的 IP 位址。 **Prefix** –用來指定 IPv6 IP 位址字首。 **Suffix** –用來指定 IPv6 IP 位址的字尾。
位址配置量	本區讓您指定 IP 位址、標籤號碼或是子網遮罩，端賴位址類型的選項結果而定。 標籤爲選項區域，僅用於辨別定義位址的名稱/用途。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

4. 輸入所有設定並按下**套用**儲存。

5. 新 IPv6 物件設定檔已經建立完成。

4.6.4 MAC/製造商物件

MAC/製造商物件設定檔可以決定路由器的防火牆該封鎖哪個製造商的 MAC 位址。



每個項目說明如下：

項目	說明
新增	新增新的設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
刪除	移除選定的設定檔。 請選擇您想要刪除的既有設定檔，然後按下刪除按鈕，該設定檔即可被移除。
更新	重新更新本頁面。

如何新增 MAC /製造商物件設定檔

1. 開啓物件設定>>MAC/製造商物件。
2. 按下新增按鈕。
3. 下述頁面將會出現。

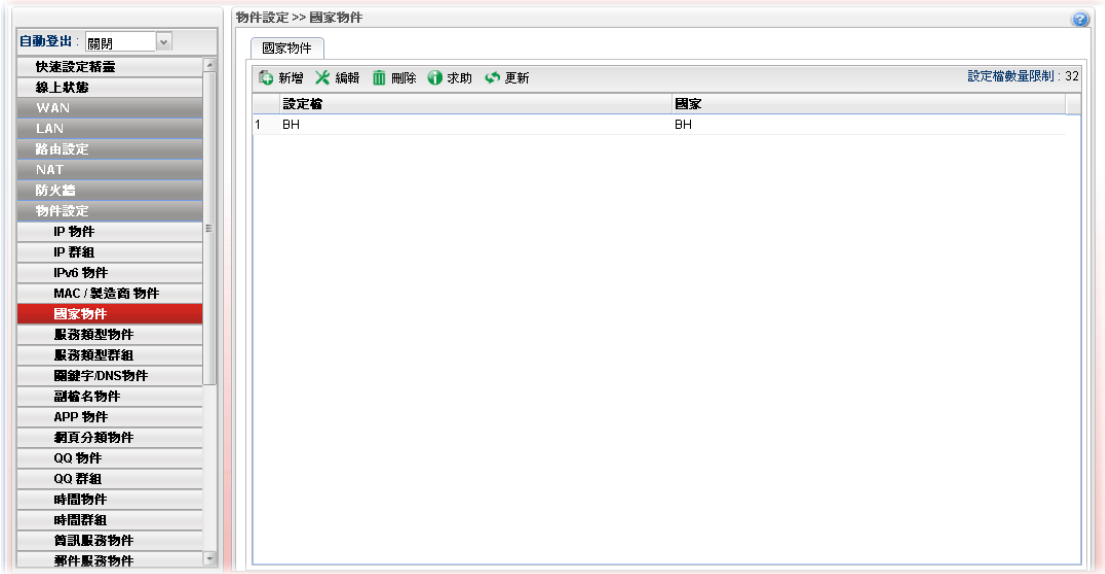
可用參數詳列如下：

項目	說明
設定檔	輸入設定檔的檔名。
MAC 位址	按下新增按鈕，並以正確的格式輸入位址與遮罩值，可移動滑鼠至輸入欄位，參考格式將會顯示在畫面上。
套用	按此鈕儲存設定並離開本頁。
製造商	**編輯** – 按此開啓製造商清單，選擇並勾選您想要的製造商之後離開編輯盒，選定製造商的名稱隨後即會顯示出來。
取消	按此鈕離開對話盒，且不儲存任何設定。

4. 輸入所有設定並按下**套用**儲存。
5. 新 MAC/製造商物件設定檔已經建立完成。

4.6.5 國家物件

國家物件可以決定防火牆可以封鎖住哪個國家或是哪些國家。

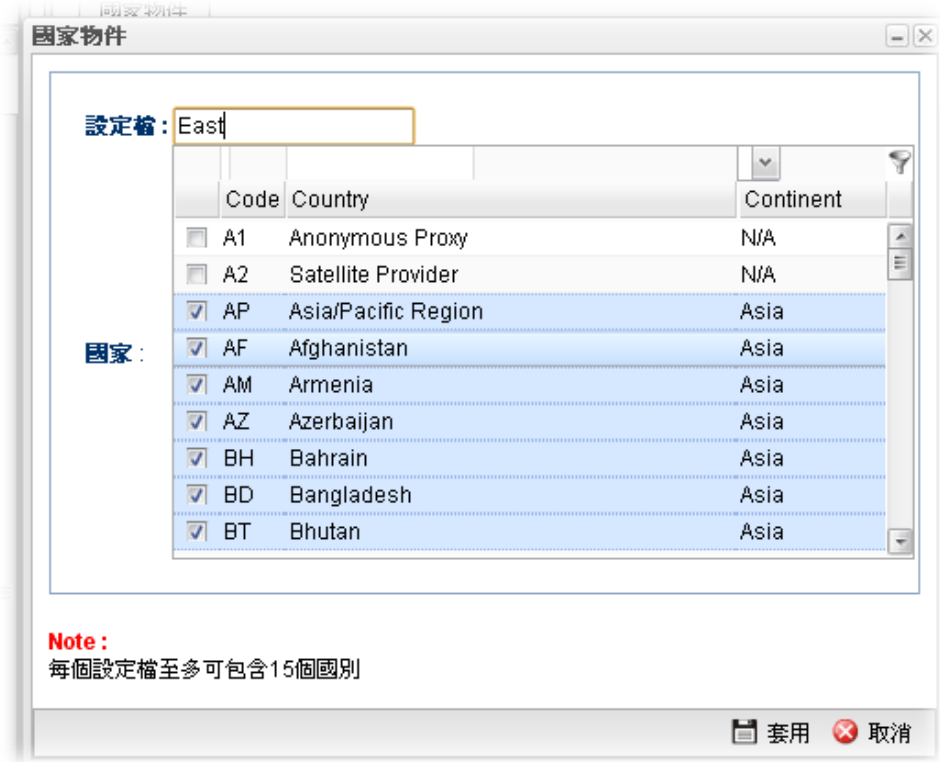


每個項目說明如下：

項目	說明
新增	新增新的配置量設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
刪除	移除選定的設定檔。 請選擇您想要刪除的既有設定檔，然後按下刪除按鈕，該設定檔即可被移除。
更新	重新更新本頁面。
設定檔	顯示設定檔的檔名。
國家	顯示此設定檔影響所及的國家名稱。

如何新增國家物件設定檔

6. 開啟**物件設定>>國家物件**。
7. 按下**新增**按鈕。
8. 下述頁面將會出現。



可用參數詳列如下：

項目	說明
設定檔	輸入設定檔的檔名。
國家	勾選防火牆將會封鎖的國家別。

項目	說明
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

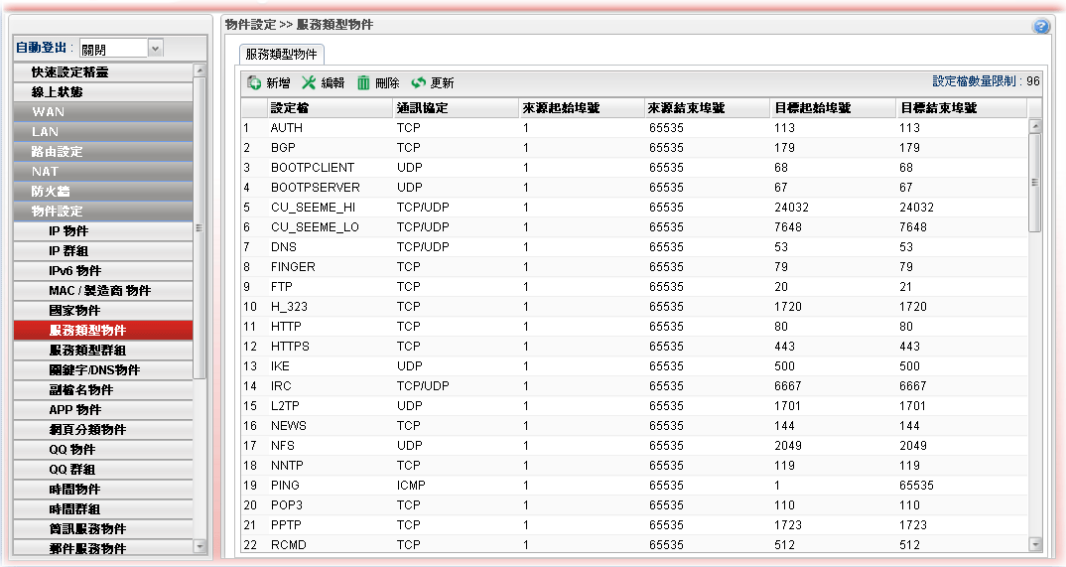
9. 輸入所有設定並按下**套用**儲存。

10. 新國家物件設定檔已經建立完成。

4.6.6 服務類型物件

含埠號範圍的 TCP 與 UDP 服務可以不同的服務類型物件設定檔方式來儲存，之後可以過濾器規則套用在防火牆上。

本頁列出預設且常用的服務類型設定檔。您可以編輯該檔，也可以另外建立新的服務類型設定檔。



	設定檔	通訊協定	來源起始埠號	來源結束埠號	目標起始埠號	目標結束埠號
1	AUTH	TCP	1	65535	113	113
2	BGP	TCP	1	65535	179	179
3	BOOTPCLIENT	UDP	1	65535	68	68
4	BOOTPSERVER	UDP	1	65535	67	67
5	CU_SEEME_HI	TCP/UDP	1	65535	24032	24032
6	CU_SEEME_LO	TCP/UDP	1	65535	7648	7648
7	DNS	TCP/UDP	1	65535	53	53
8	FINGER	TCP	1	65535	79	79
9	FTP	TCP	1	65535	20	21
10	H_323	TCP	1	65535	1720	1720
11	HTTP	TCP	1	65535	80	80
12	HTTPS	TCP	1	65535	443	443
13	IKE	UDP	1	65535	500	500
14	IRC	TCP/UDP	1	65535	6667	6667
15	L2TP	UDP	1	65535	1701	1701
16	NEWS	TCP	1	65535	144	144
17	NFS	UDP	1	65535	2049	2049
18	NNTP	TCP	1	65535	119	119
19	PING	ICMP	1	65535	1	65535
20	POP3	TCP	1	65535	110	110
21	PPTP	TCP	1	65535	1723	1723
22	RCMD	TCP	1	65535	512	512

每個項目說明如下：

項目	說明
新增	新增新的設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
刪除	移除選定的設定檔。 請選擇您想要刪除的既有設定檔，然後按下刪除按鈕，該設定檔即可被移除。
更新	重新更新本頁面。
設定檔數量限制	顯示可以建立的設定檔總數。
設定檔	顯示設定檔的檔名。
通訊協定	顯示此設定檔使用的協定。

項目	說明
來源起始埠號	顯示此設定檔的來源起始埠號。
來源結束埠號	顯示此設定檔的來源結束埠號。
目標起始埠號	顯示此設定檔的目的起始埠號。
目標結束埠號	顯示此設定檔的目的結束埠號。

如何新增服務類型物件設定檔

1. 開啓物件設定>>服務類型物件。
2. 按下新增按鈕。
3. 下述頁面將會出現。

可用參數詳列如下：

項目	說明
設定檔	輸入設定檔的檔名。
通訊協定	指定此設定檔的使用協定。
來源起始埠號	此設定僅對 TCP/UDP 協定產生作用，對於 ICMP 協定，可以直接忽略。 請輸入埠號數值(0 – 65535)當成起始來源埠號。
來源結束埠號	此設定僅對 TCP/UDP 協定產生作用，對於 ICMP 協定，可以直接忽略。 請輸入埠號數值(0 – 65535)當成結束來源埠號。
目標起始埠號	此設定僅對 TCP/UDP 協定產生作用，對於 ICMP 協定，可以直接忽略。 請輸入埠號數值(0 – 65535)當成起始目標埠號。
目標結束埠號	此設定僅對 TCP/UDP 協定產生作用，對於 ICMP 協定，可以直接忽略。 請輸入埠號數值(0 – 65535)當成結束目標埠號。

項目	說明
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

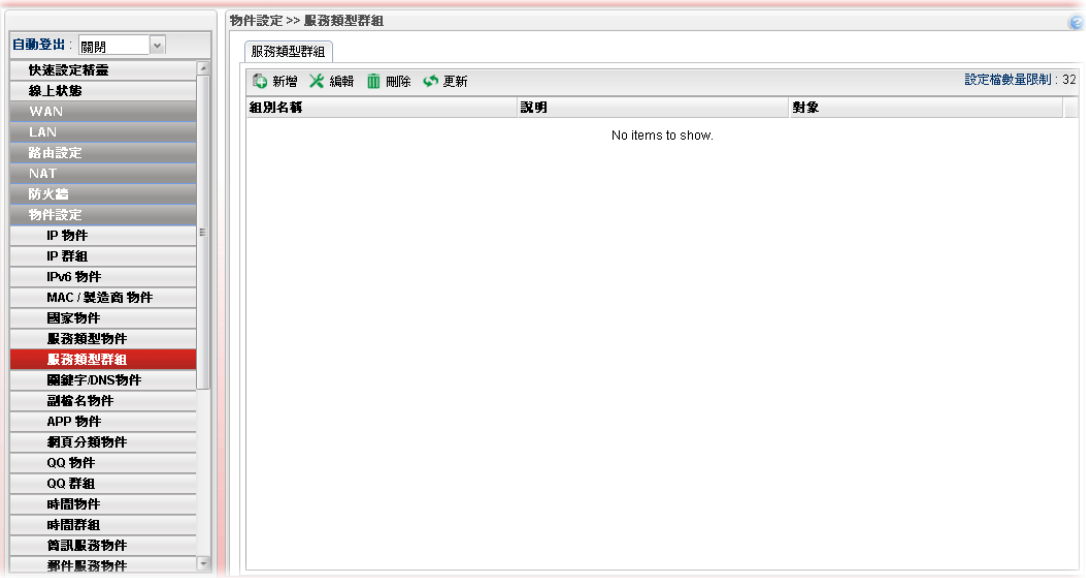
4. 輸入所有設定並按下**套用**儲存。

5. 新服務類型物件設定檔已經建立完成。

4.6.7 服務類型群組

本頁讓您整合數個服務類型成爲一個服務類型群組。

爲了方便管理，可將數種服務類型設定檔納入一個群組當中，不同的服務類型群組可包含各種不同的服務類型設定檔。



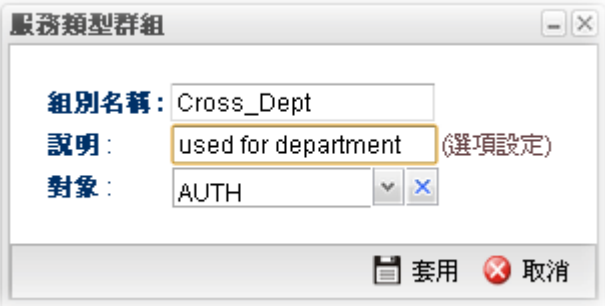
每個項目說明如下：

項目	說明
新增	新增新的設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
刪除	移除選定的設定檔。 請選擇您想要刪除的既有設定檔，然後按下刪除按鈕，該設定檔即可被移除。
更新	重新更新本頁面。
設定檔數量限制	顯示可以建立的設定檔總數。
組別名稱	顯示服務類型群組的名稱。

項目	說明
說明	顯示關於此設定檔的簡易說明。
對象	顯示在此群組下選定的服務類型物件設定檔為何。

如何新增服務類型群組設定檔

1. 開啟**物件設定>>服務類型群組**。
2. 按下**新增**按鈕。
3. 下述頁面將會出現。



可用參數詳列如下：

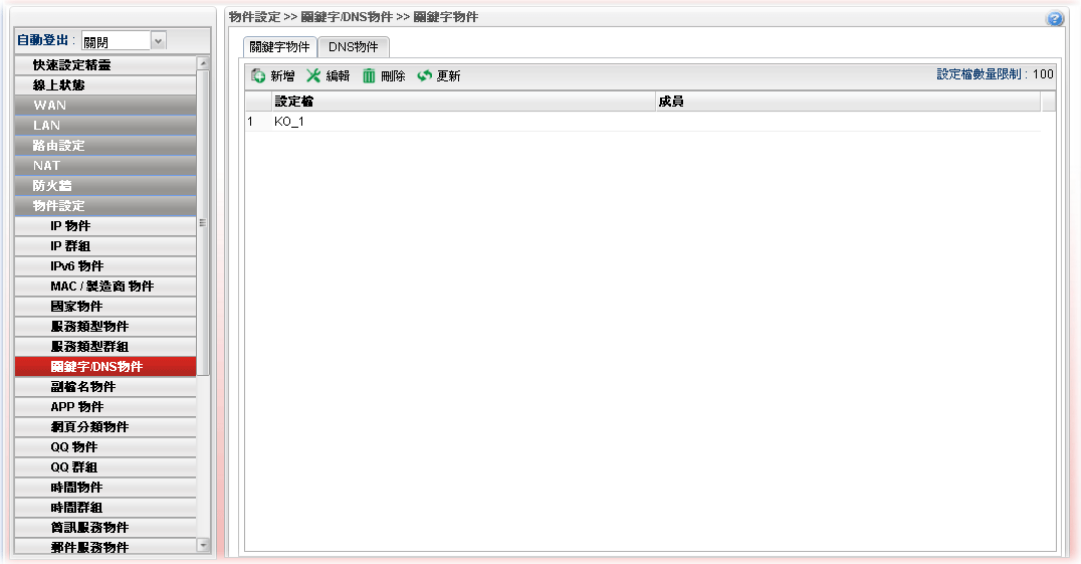
項目	說明
組別名稱	輸入服務類型物件群組的檔名。
說明	針對此群組輸入簡易說明。
對象	使用下拉式清單勾選那入此群組中的 IP 物件設定檔。 所有在**物件設定>>IP 物件**選單中建立且可用的 IP 物件都可在此呈現供您選取。 如欲刪除選定的設定檔，可按 ✕ 將該物件項目移除。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

4. 輸入所有設定並按下**套用**儲存。
5. 新服務類型群組設定檔已經建立完成。

4.6.8 關鍵字/DNS 物件

4.6.8.1 關鍵字物件

關鍵字可以設定為過濾器規則，套用在防火牆上。Vigor2960 允許使用者設定數個關鍵字形成一個關鍵字設定檔，甚至可允許使用者群組數個關鍵字設定檔成為關鍵字群組，方便應用於防火牆上。

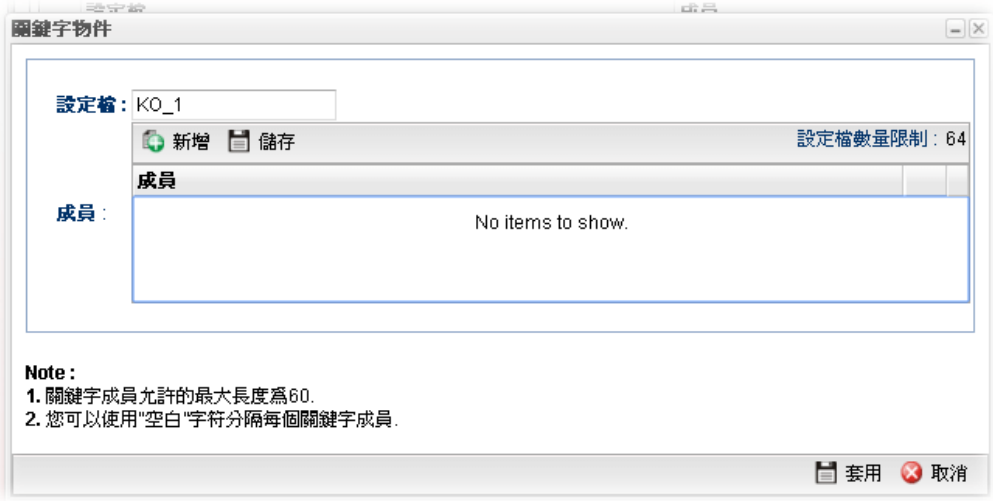


每個項目說明如下：

項目	說明
新增	新增新的設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
刪除	移除選定的設定檔。 請選擇您想要刪除的既有設定檔，然後按下刪除按鈕，該設定檔即可被移除。
更新	重新更新本頁面。
設定檔數量限制	顯示可以建立的設定檔總數。
設定檔	顯示關鍵字物件設定檔的檔名。
成員	顯示此設定檔指定的文字內容。

如何新增關鍵字物件設定檔

1. 開啓**物件設定>>關鍵字物件/DNS 物件**，按**關鍵字**標籤。
2. 按下**新增**按鈕。
3. 下述頁面將會出現。



可用參數詳列如下：

項目	說明
設定檔	輸入關鍵字物件設定檔名。
成員	輸入此設定檔的內文，例如您在此輸入 *gambling*，當您瀏覽到某個網頁含有 *gambling* 資訊時，將會依照防火牆設定的內容放行或是封鎖該網頁。 **新增**– 按此鈕以便輸入新的關鍵字物件。 **儲存**– 按下儲存設定。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

4. 輸入所有設定並按下**套用**儲存。
5. 新關鍵字物件設定檔已經建立完成。

4.6.8.2 DNS 物件

DNS 也可以設定爲過濾器規則並套用在防火牆上。

每個項目說明如下：

項目	說明
新增	新增新的設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
刪除	移除選定的設定檔。 請選擇您想要刪除的既有設定檔，然後按下刪除按鈕，該設定檔即可被移除。
更新	重新更新本頁面。
設定檔數量限制	顯示可以建立的設定檔總數。
設定檔	顯示物件設定檔的檔名。
成員表	顯示此設定檔指定的文字內容。

如何新增 DNS 物件設定檔

1. 開啓**物件設定>>關鍵字物件/DNS 物件**，按 **DNS 物件**標籤。
2. 按下**新增**按鈕。
3. 下述頁面將會出現。

可用參數詳列如下：

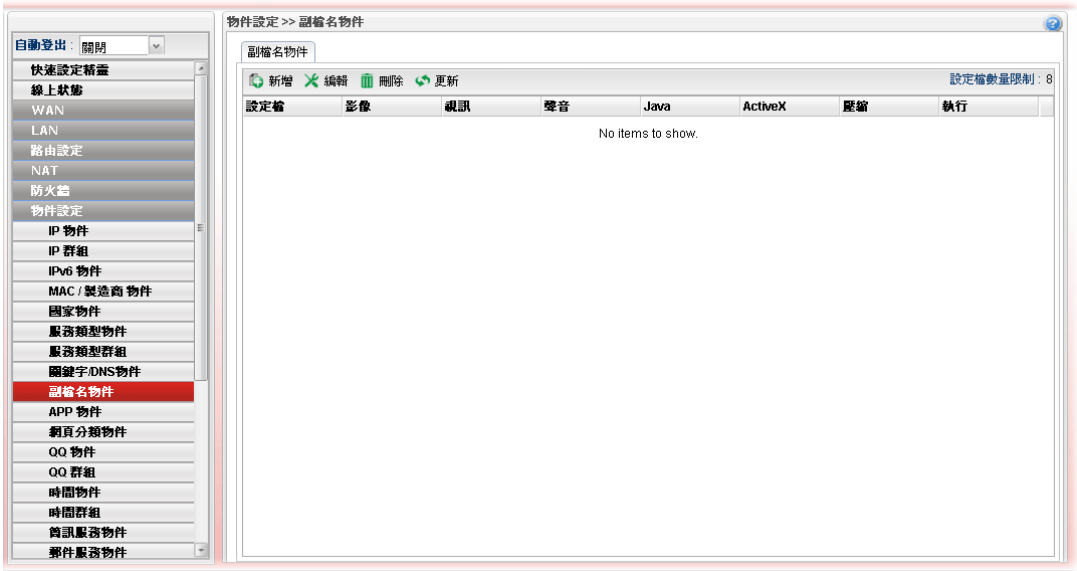
項目	說明
設定檔	輸入關鍵字物件設定檔名。
成員表	輸入您想要過濾的 DNS 網域名稱。 **新增** – 按此鈕以便輸入新的 DNS 物件。 **儲存**– 按下儲存設定。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

4. 輸入所有設定並按下**套用**儲存。

5. 新 DNS 物件設定檔已經建立完成。

4.6.9 副檔名物件

本頁允許您設定可套用在防火牆的副檔名物件，所有含有此副檔名的檔案都將依照選定的動作(通過/封鎖)來處理。



每個項目說明如下：

項目	說明
新增	新增新的設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
刪除	移除選定的設定檔。 請選擇您想要刪除的既有設定檔，然後按下刪除按鈕，該設定檔即可被移除。
更新	重新更新本頁面。
設定檔數量限制	顯示可以建立的設定檔總數。
設定檔	顯示設定檔的檔名。
影像	顯示選定圖像的副檔名。
視音	顯示選定影音的副檔名。
聲音	顯示選定聲音的副檔名。
Java	顯示選定 java 副檔名。
ActiveX	顯示選定 activeA 的副檔名。
壓縮	顯示選定壓縮的副檔名。
執行	顯示選定執行的副檔名。

如何新增副檔名物件設定檔

1. 開啟**物件設定>>副檔名物件**。
2. 按下**新增**按鈕。
3. 下述頁面將會出現。

可用參數詳列如下：

項目	說明
設定檔	輸入副檔名物件設定檔名。
影像	系統提供數個與圖像相關的副檔名供您選取，請使用下拉式清單勾選需求的項目。
視音	系統提供數個聲音與影像相關的副檔名供您選取，請使用下拉式清單勾選需求的項目。
聲音	系統提供數個與聲音相關的副檔名供您選取，請使用下拉式清單勾選需求的項目。
Java	系統提供數個與 Java 相關的副檔名供您選取，請使用下拉式清單勾選需求的項目。
ActiveX	系統提供數個與 ActiveX 相關的副檔名供您選取，請使用下拉式清單勾選需求的項目。
壓縮	系統提供數個與壓縮相關的副檔名供您選取，請使用下拉式清單勾選需求的項目。
執行	系統提供數個與執行相關的副檔名供您選取，請使用下拉式清單勾選需求的項目。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

4. 輸入所有設定並按下**套用**儲存。

5. 新副檔名物件設定檔已經建立完成。

4.6.10 APP 物件

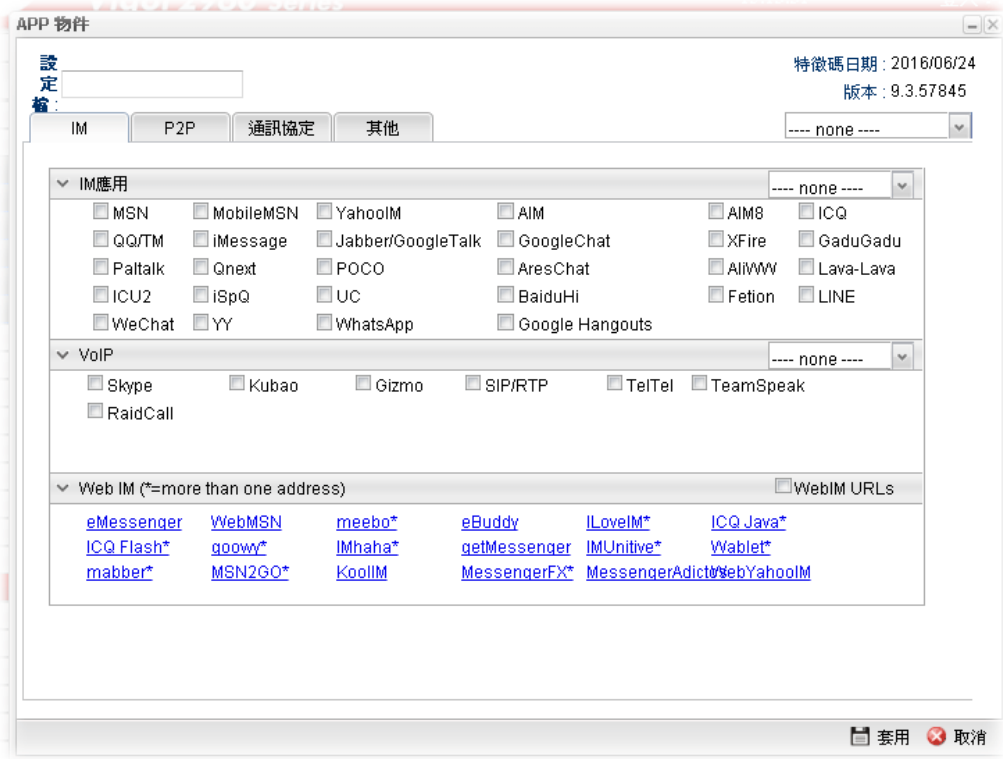
即時通訊、點對點、協定與其他類型都可整合為 APP 物件，然後套用在防火牆設定中，以便封鎖特定的應用程式。

每個項目說明如下：

項目	說明
APP 特徵碼更新	按此連結開啓**系統維護>>APP 特徵碼更新**設定頁面。
APP 支援列表	APP 支援列表可顯示 Vigor 路由器支援的 APP 應用程式的版本爲何。所有的 APP 都分別歸類於 IM、P2P、通訊協定與其他項目底下。 以下範例圖顯示在 IM 標籤下路由器支援的 APP 資料。
新增	新增新的設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
刪除	移除選定的設定檔。 請選擇您想要刪除的既有設定檔，然後按下刪除按鈕，該設定檔即可被移除。
更新	重新更新本頁面。
設定檔數量限制	顯示可以建立的設定檔總數。
設定檔	顯示設定檔的檔名。
IM	顯示此設定檔指定的即時通訊應用程式。
P2P	顯示此設定檔指定的點對點應用程式。
通訊協定	顯示此設定檔指定的協定內容。
其他	顯示此設定檔指定的其他類型。

如何新增 APP 物件設定檔

1. 開啓**物件設定>>APP 物件**。
2. 按下**新增**按鈕。
3. 下述頁面將會出現。 按下 **IM** 標籤取得如下頁面。因爲好玩或是容易且方便之故，人們通常喜歡利用即時通訊和他人線上交談，但是，這麼做可能會降低員工的生產力，因此提供可以封鎖或是限制即時通訊應用的工具對公司來說顯得相當的重要。IM 物件設定列出所有常見的即時通訊應用程式讓您選取加以封鎖，請勾選想要封鎖的項目，將其儲存爲 IM 物件設定檔，之後，此設定檔可以做爲過濾器的規則套用在**防火牆**上，如此即可達成封鎖的目的。

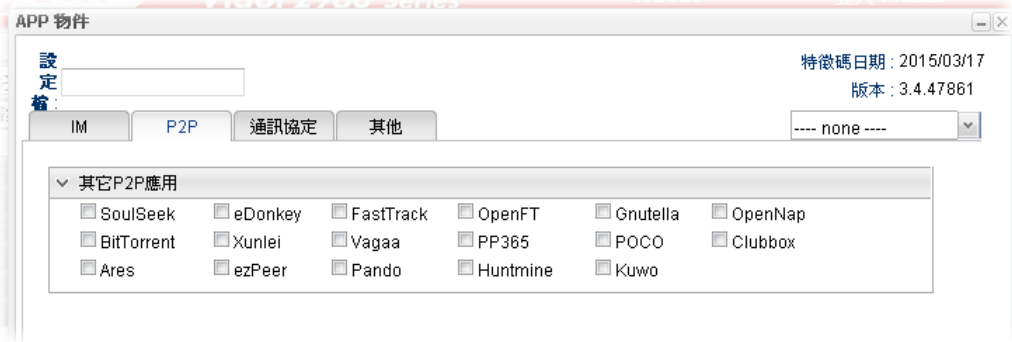


可用參數詳列如下：

項目	說明
設定檔	輸入物件設定檔的檔名。
IM 應用	系統提供數種應用程式供您選取，請勾選您想要的項目。
VoIP	系統提供數種應用程式供您選取，請勾選您想要的項目。
WebIM	列出以網頁爲基礎的 IM 應用，請勾選您想要的項目。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

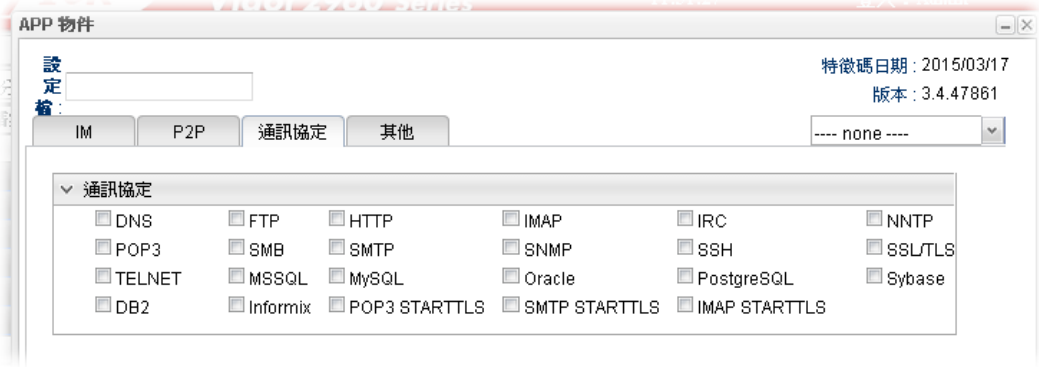
按下 **P2P** 開啓如下頁面，Vigor2960 可封鎖點對點應用程式，尤其是封鎖那些經常上傳或是下載不適宜檔案至網際網路上的用戶。

P2P 物件設定列出所有點對點的應用方便您勾選以便加以封鎖，請選擇您想要封鎖的項目，然後儲存爲 P2P 物件設定檔，此設定檔可以做爲過濾器的規則套用在**防火牆**上，如此即可達成封鎖的目的。



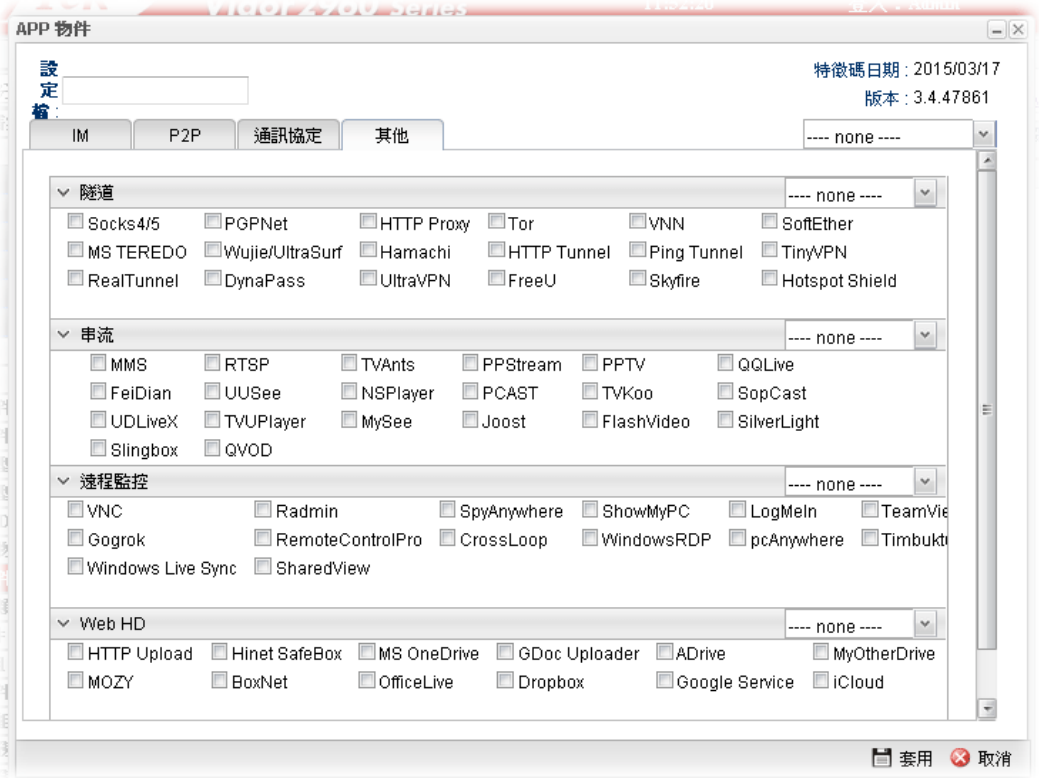
項目	說明
其他 P2P 應用	有數種 P2P 應用程式可以選擇，請勾選該項目加以選擇。

按下**通訊協定**開啓如下頁面，針對區域網路用戶的網路服務諸如 DNS, FTP, HTTP, POP3 都可透過 Vigor2960 加以封鎖，您可以勾選列於此區內常見的服務，讓路由器封鎖其運作。



項目	說明
通訊協定	有數種協定可以選擇，請勾選該項目加以選擇。

按下**其他**取得如下頁面：



項目	說明
隧道/串流/遠程監控 (Tunneling/Streaming/Remote	有數種協定可以選擇，請勾選該項目加以選擇。

項目	說明
Control/Web HD)	

4. 輸入所有設定並按下**套用**儲存。
5. 新 APP 物件設定檔已經建立完成。

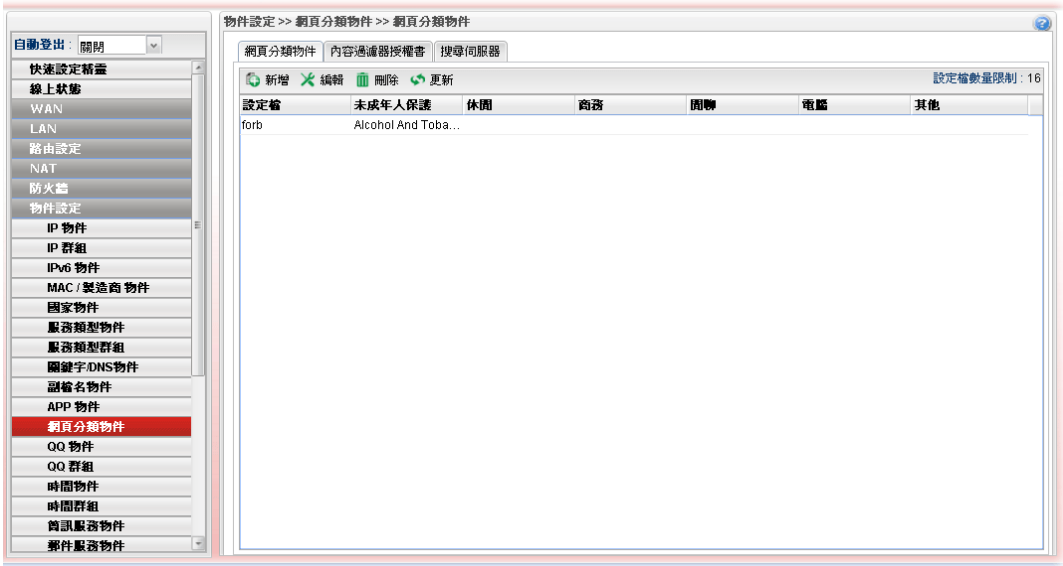
4.6.11 網頁分類物件

我們都知道網際網路上的內容，有時候可能並不太合宜，作爲一個負責任的父母或是雇主，您應該保護那些您信賴的人免受危險的侵擾。藉由 Vigor 路由器的網頁過濾服務，您可以保護您的商業機密不受一般常見威脅；對於父母來說，您可以保護您的孩童不致誤闖成人網站或是成人聊天室。

WCF(網頁內容過濾器)採用特定服務供應商研發供應的機制。而不論是啓動 WCF 功能或是自網頁內容過濾器取得全新之授權，您都必須按下**啓用連結**，才能達成您的要求。需注意的是目前搭配 Vigor 路由器的服務供應商，提供短期免費試用版讓使用者體驗，如果您想要購買正式的版本，可洽詢居易客服或是經銷商，取得更多資訊。

注意 1: WCF 並非 Vigor 路由器的內建機制，該服務是由 Commtouch 公司所提供，如果您想要使用此類服務(試用版或是正式版)，您必須先進行啓用的程序。若您想要使用正式版，請先與經銷商聯絡，獲取更多更詳細的 WCF 資訊。
注意 2: Commtouch 已經併入 Cyren，其 GlobalView 服務仍將持續提供強大且以雲端爲基準的安全性解決方案相關資訊。請參考：
http://www.prnewswire.com/news-releases/commtouch-is-now-cyren-239025151.html

4.6.11.1 網頁分類物件



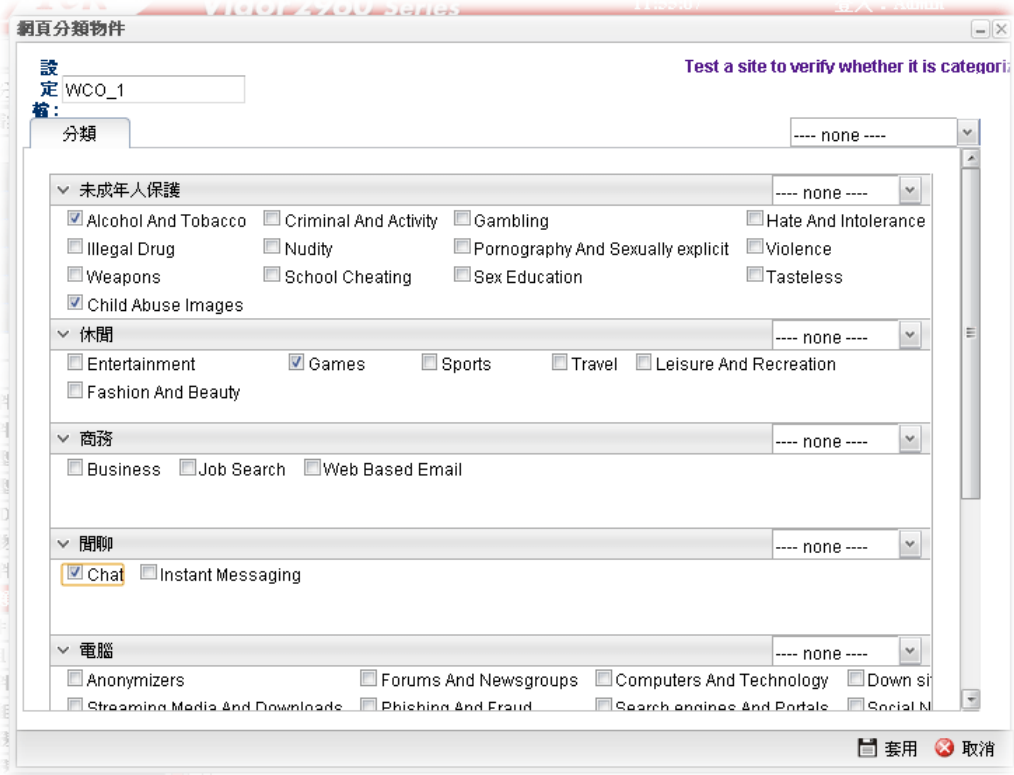
每個項目說明如下：

項目	說明
新增	新增新的設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編

項目	說明
	輯按鈕，編輯視窗將會出現讓您修改內容。
刪除	移除選定的設定檔。 請選擇您想要刪除的既有設定檔，然後按下刪除按鈕，該設定檔即可被移除。
更新	重新更新本頁面。
設定檔數量限制	顯示可以建立的設定檔總數。
設定檔	顯示設定檔的檔名。
未成年人保護	顯示此分類下的項目，您可以視需要勾選相關項目已達保護兒童之目的。
休閒	顯示此分類下的項目，您可以視需要勾選相關項目讓系統封鎖相關的網頁內容。
商務	顯示此分類下的項目，您可以視需要勾選相關項目讓系統封鎖相關的網頁內容。
閒聊	顯示此分類下的項目，您可以視需要勾選相關項目讓系統封鎖相關的網頁內容。
電腦	顯示此分類下的項目，您可以視需要勾選相關項目讓系統封鎖相關的網頁內容。
其他	顯示此分類下的項目，您可以視需要勾選相關項目讓系統封鎖相關的網頁內容。

如何新增網頁分類物件設定檔

1. 開啟**物件設定>>網頁分類物件**。
2. 按下**新增**按鈕。
3. 下述頁面將會出現。



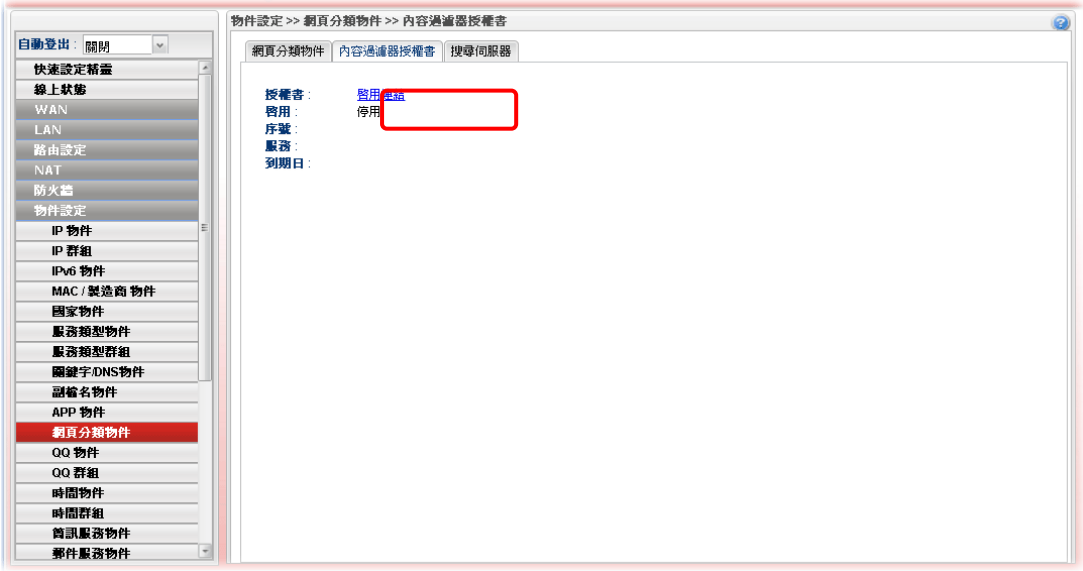
可用參數詳列如下：

項目	說明
設定檔	輸入物件設定檔的檔名。
未成年人保護	不適合兒童觀看的網頁將分別歸類於不同的類別，選擇您不希望兒童造訪的項目並勾選該項目。
休閒	勾選您不希望使用者造訪的類型。
商務	勾選您不希望使用者造訪的類型。
閒聊	勾選您不希望使用者用來與遠端用戶聊天的類型。
電腦	勾選您不希望使用者造訪的類型。
其他	勾選您不希望使用者造訪的類型。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

4. 輸入所有設定並按下**套用**儲存。
5. 新網頁分類物件設定檔已經建立完成。

4.6.11.2 內容過濾器授權書

移動滑鼠至**啓動 URL** 然後按下該連結，系統將導引您登入 MyVigor 網站。

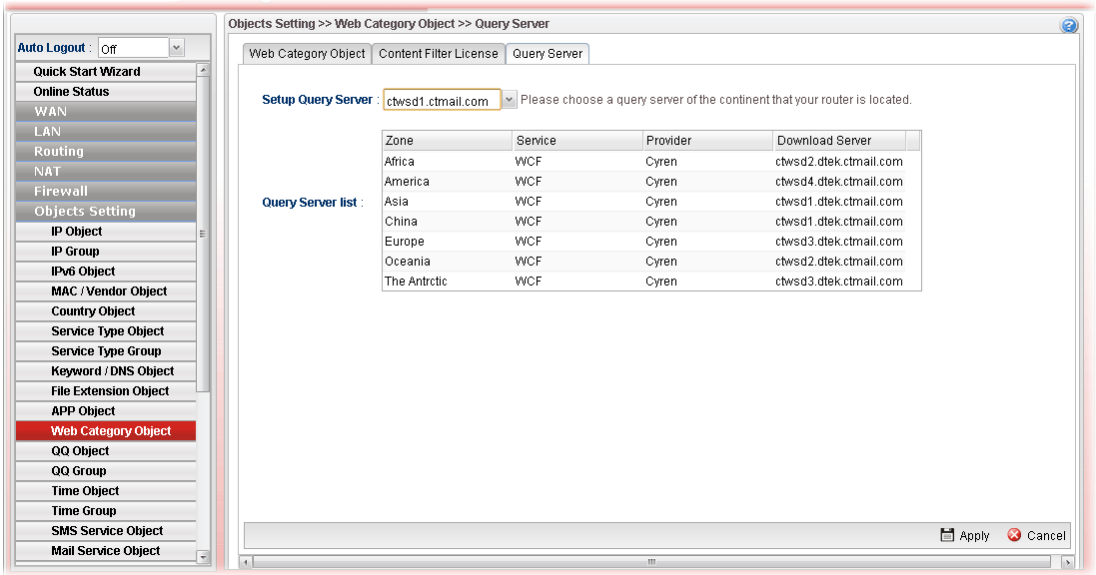


完成 WCF 試用版的啓動之後，記得向居易經銷商購買 WCF 服務的銀卡。

4.6.11.3 搜尋伺服器

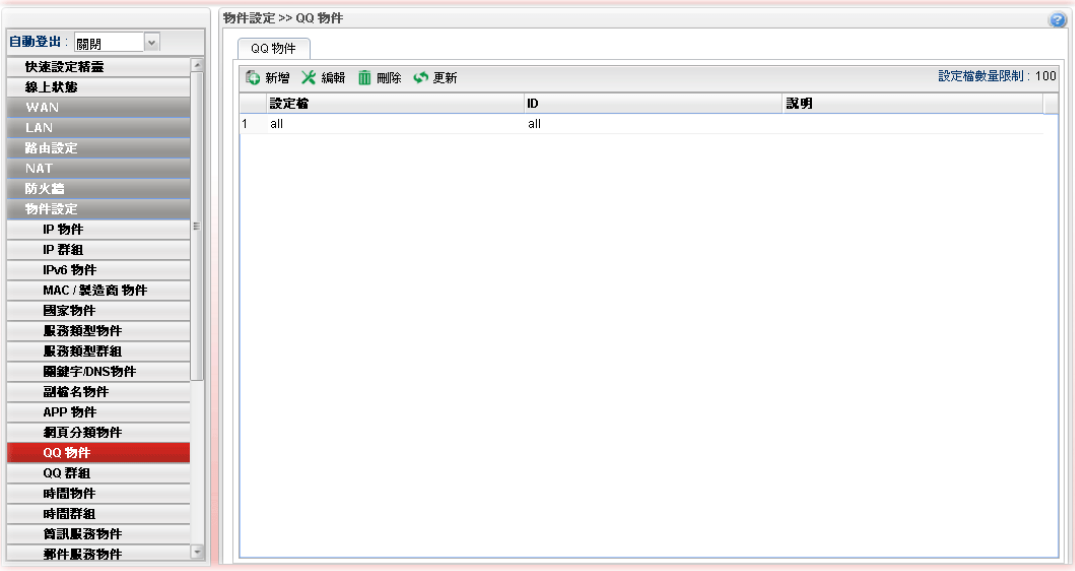
在您於瀏覽器輸入 URL 之前，您必須先指定分類搜尋需用的伺服器。建議您使用預設值。

> **附註：**由於地點的差異之故，每種搜尋伺服器的回應時間也會有所不同，因此也影響了 WCF 的效用。



4.6.12 QQ 物件

> **注意:** 本頁主要是針對中國即時通訊"Tencent QQ" 用戶而設計，對於未使用 QQ 的使用者來說，可以跳過此節。



每個項目說明如下：

項目	說明
新增	新增新的設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
刪除	移除選定的設定檔。 請選擇您想要刪除的既有設定檔，然後按下刪除按鈕，該設定檔即可被移除。
更新	重新更新本頁面。
設定檔數量限制	顯示可以建立的設定檔總數。
設定檔	顯示設定檔的檔名。
ID	顯示 QQ 物件設定檔的帳戶名稱。
說明	顯示 QQ 物件設定檔的簡易說明。

如何新增 QQ 物件設定檔

1. 開啓**物件設定>>QQ 物件**。
2. 按下**新增**按鈕。
3. 下述頁面將會出現。

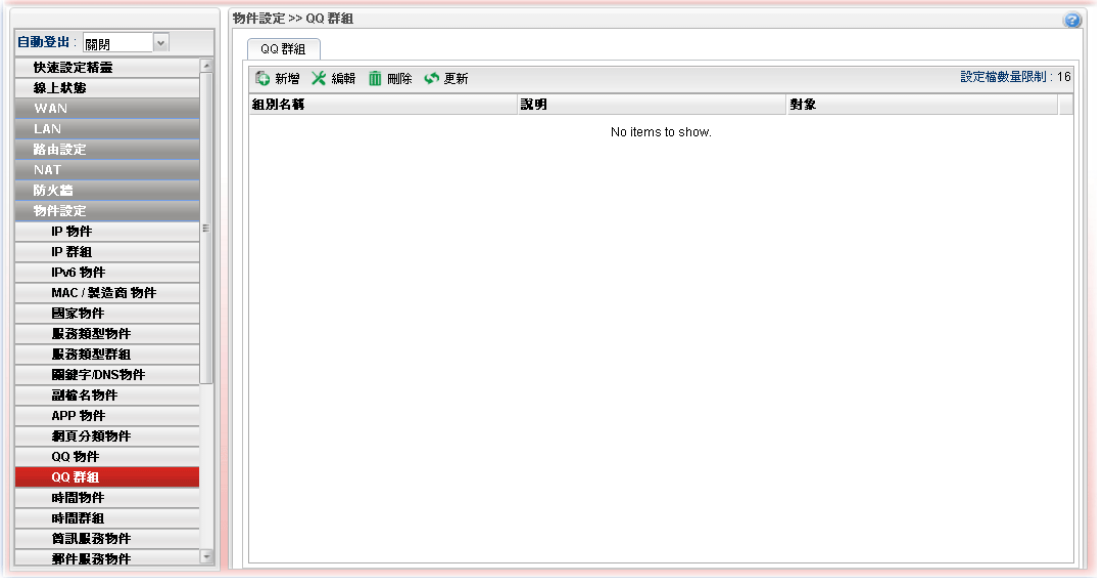
可用參數詳列如下：

項目	說明
設定檔	輸入物件設定檔的檔名。
ID	針對此 QQ 物件設定檔，建立一組帳號。 **新增** – 按此鈕以便建立新的帳號。 **儲存** – 按此鈕儲存新帳號。
說明	輸入與 QQ 物件設定檔有關的說明。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

4. 輸入所有設定並按下**套用**儲存。
5. 新 QQ 物件設定檔已經建立完成。

4.6.13 QQ 群組

本頁讓您將數個 QQ 物件設定檔納入一個群組當中。

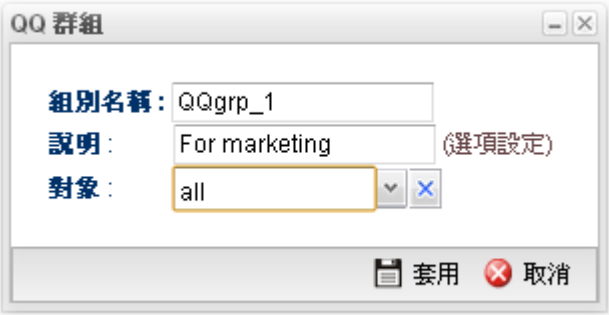


每個項目說明如下：

項目	說明
新增	新增新的設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
刪除	移除選定的設定檔。 請選擇您想要刪除的既有設定檔，然後按下刪除按鈕，該設定檔即可被移除。
更新	重新更新本頁面。
設定檔數量限制	顯示可以建立的設定檔總數。
組別名稱	顯示群組設定檔的檔名。
說明	顯示此群組的簡易說明。
對象	顯示此群組包含的物件名稱。

如何新增 QQ 群組設定檔

1. 開啟**物件設定>>QQ 群組**。
2. 按下**新增**按鈕。
3. 下述頁面將會出現。



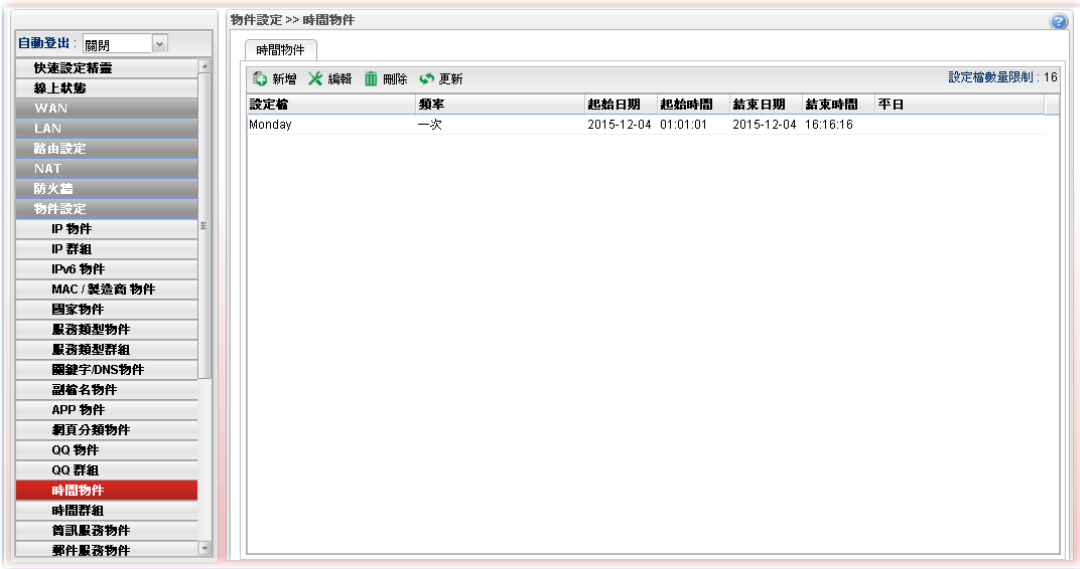
可用參數詳列如下：

項目	說明
設定檔	輸入物件設定檔的檔名。
說明	輸入與 QQ 群組設定檔有關的說明。
對象	使用下拉式清單選則準備納入此群組當中的物件設定檔。 所有您在物件**設定>>QQ 物件**頁面中設定的可用的物件都可在此呈現。 如欲清除選定的物件，請按 ✕ 以移除目前的物件選擇。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

4. 輸入所有設定並按下**套用**儲存。
5. 新 QQ 群組設定檔已經建立完成。

4.6.14 時間物件

限制使用者於特定時間登入網際網路，並限制存取時數，此物件對其他功能例如防火牆也很實用。



每個項目說明如下：

項目	說明
新增	新增新的設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
刪除	移除選定的設定檔。 請選擇您想要刪除的既有設定檔，然後按下刪除按鈕，該設定檔即可被移除。
更新	重新更新本頁面。
設定檔數量限制	顯示可以建立的設定檔總數。
設定檔	顯示時間物件設定檔的檔名。
頻率	顯示時間物件設定檔的持續時間。
起始日期	顯示時間物件設定檔的起始日期。
起始時間	顯示時間物件設定檔的起始時間。
結束日期	顯示時間物件設定檔的結束日期。
結束時間	顯示時間物件設定檔的結束時間。
平日	顯示時間物件設定檔的使用天數。

如何新增時間物件設定檔

1. 開啟**物件設定>>時間物件**。
2. 按下**新增**按鈕。
3. 下述頁面將會出現。

可用參數詳列如下：

項目	說明
設定檔	輸入物件設定檔的檔名。
頻率	指定排程套用的頻率為何(平日或是一次)。
起始日期	指定時間物件設定檔的起始日期。
起始時間	指定時間物件設定檔的起始時間。
結束日期	指定時間物件設定檔的結束日期。
結束時間	指定時間物件設定檔的結束時間。
平日	指定一週當中哪些天數執行此排程。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

4. 輸入所有設定並按下**套用**儲存。

5. 新時間物件設定檔已經建立完成。

4.6.15 時間群組

本頁允許您群組數個時間物件設定檔。

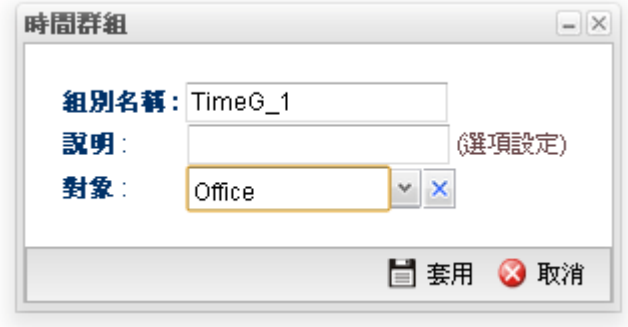
每個項目說明如下：

項目	說明
新增	新增新的設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
刪除	移除選定的設定檔。 請選擇您想要刪除的既有設定檔，然後按下刪除按鈕，該

項目	說明
	設定檔即可被移除。
更新	重新更新本頁面。
設定檔數量限制	顯示可以建立的設定檔總數。
組別名稱	顯示群組的名稱。
說明	顯示關於此群組的簡易說明。
對象	顯示此群組選定的時間物件。

如何新增時間群組設定檔

1. 開啟**物件設定>>時間群組**。
2. 按下**新增**按鈕。
3. 下述頁面將會出現。



可用參數詳列如下：

項目	說明
設定檔	輸入物件設定檔的檔名。
說明	如果群組設定檔名稱不夠清晰，請在此輸入補充說明。
對象	使用下拉式清單選則準備納入此群組當中的物件設定檔。所有您在物件**設定>>時間物件**頁面中設定的可用的物件都可在此呈現。 如欲清除選定的物件，請按 ✕ 以移除目前的物件選擇。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

4. 輸入所有設定並按下**套用**儲存。
5. 新時間群組設定檔已經建立完成。

4.6.16 簡訊 SMS 服務物件

本頁讓您設定可套用於**其他應用>>簡訊/郵件警示服務**網頁中的設定檔。

每個項目說明如下：

項目	說明
新增	新增新的設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
刪除	移除選定的設定檔。 請選擇您想要刪除的既有設定檔，然後按下刪除按鈕，該設定檔即可被移除。
更新	重新更新本頁面。
設定檔數量限制	顯示可以建立的設定檔總數。
設定檔	顯示設定檔的檔名。
啓用	顯示設定檔狀態，False 表示停用；True 表示啓用。
簡訊服務供應商	顯示提供簡訊服務的供應商爲何。
使用者名稱	顯示寄信者用來登入簡訊服務供應商系統時所使用的帳號名稱。
配額	顯示您自服務供應上購買取得的簡訊則數。
間隔(秒)	顯示傳送簡訊的時間間隔。

如何新增簡訊服務設定檔

1. 開啓**物件設定>>簡訊服務物件**。
2. 按下**新增**按鈕。
3. 下述頁面將會出現。

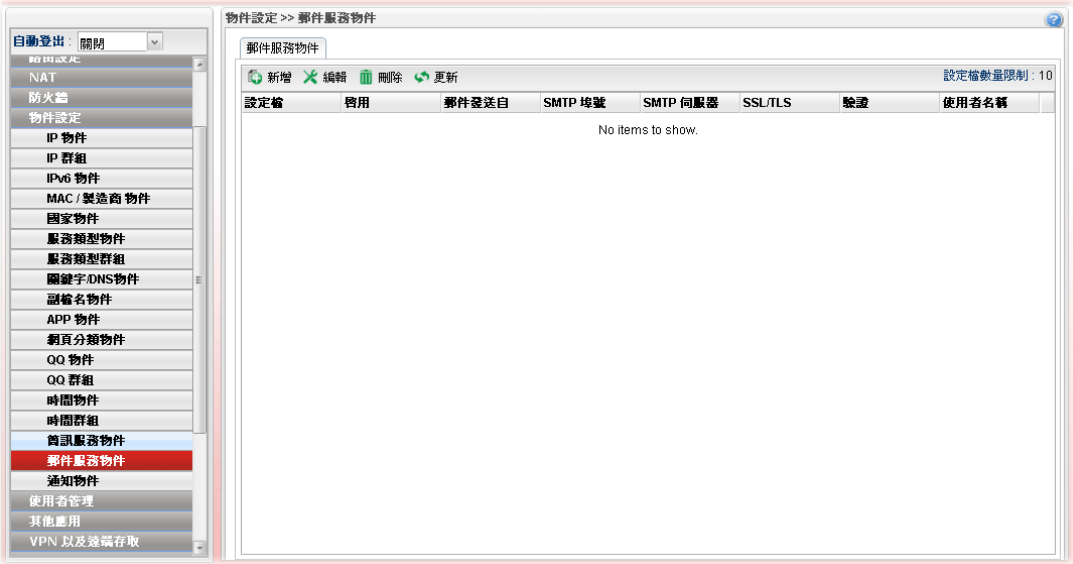
可用參數詳列如下：

項目	說明
設定檔	輸入物件設定檔的檔名。
啓用	勾選此方塊啓用此設定檔。
簡訊服務供應商	使用下拉式清單指定提供簡訊服務的供應商。
使用者名稱	輸入寄信者用來登入選定的服務供應商之使用者名稱。
密碼	輸入寄信者用來登入選定的服務供應商之密碼。
配額	輸入您自上述選定的服務供應商處購買的簡訊則數。 請注意額度一等於在標準路由中，一則簡訊文字。
間隔(秒)	爲了避免額度過早被用罄，請輸入發出簡訊的時間間隔。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

4. 輸入所有設定並按下**套用**儲存。
5. 新 SMS 簡訊物件設定檔已經建立完成。

4.6.17 郵件服務物件

本頁讓您設定可套用於**其他應用>>簡訊/郵件警示服務**網頁中的設定檔。



每個項目說明如下：

項目	說明
新增	新增新的設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
刪除	移除選定的設定檔。 請選擇您想要刪除的既有設定檔，然後按下刪除按鈕，該設定檔即可被移除。
更新	重新更新本頁面。
設定檔數量限制	顯示可以建立的設定檔總數。
設定檔	顯示設定檔的檔名。
啓用	顯示設定檔狀態，False 表示停用；True 表示啓用。
郵寄發送自	顯示寄件者郵件地址。
SMTP 埠號	顯示 SMTP 服務使用的埠號。
SMTP 伺服器	顯示 SMTP 伺服器的 IP 位址。
SSL/TLS	顯示 SS:/TLS 伺服器的 IP 位址。
驗證	啓用表示此設定檔必須經過伺服器驗證。 停用表示此設定檔不必經過伺服器驗證。
使用者名稱	顯示用於驗證的使用者名稱。

如何新增郵件服務設定檔

1. 開啓**物件設定>>郵件服務物件**。
2. 按下**新增**按鈕。

3. 下述頁面將會出現。

可用參數詳列如下：

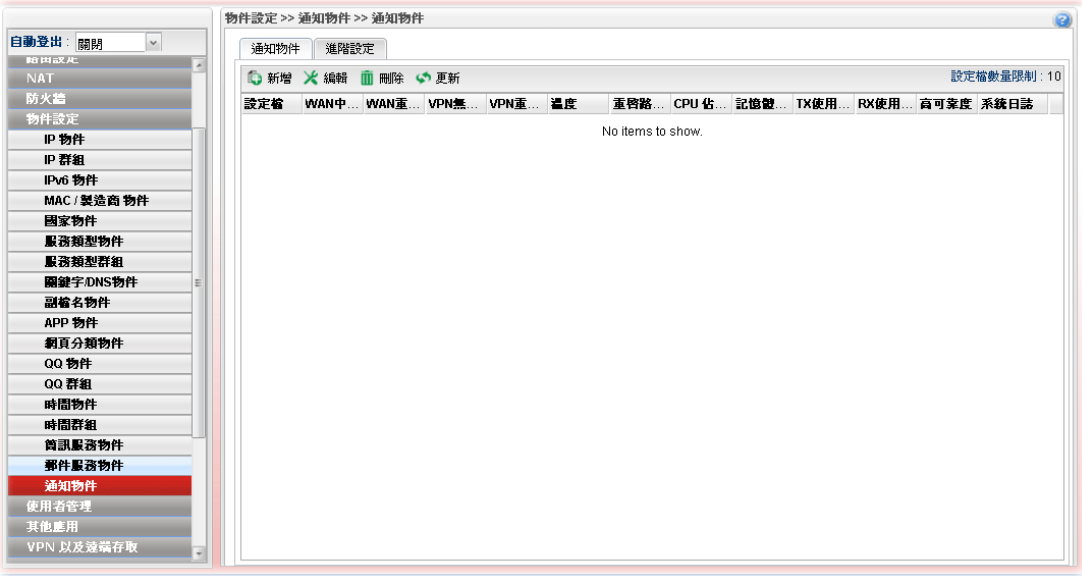
項目	說明
設定檔	輸入物件設定檔的檔名。
啓用	勾選此方塊啓用此設定檔。
郵寄發送自	輸入寄件者郵件地址。
SMTP 埠號	輸入 SMTP 服務使用的埠號。
SMTP 伺服器	輸入 SMTP 伺服器的 IP 位址。
SSL/TLS	選擇**啓用**框啓用此功能。
驗證	郵件伺服器必須利用使用者名稱與密碼進行驗證，才得授權發送訊息出去。勾選此框啓用此功能。 **使用者名稱** – 輸入驗證所需的使用者名稱。 **使用者密碼** – 輸入驗證所需的密碼。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

4. 輸入所有設定並按下**套用**儲存。
5. 新郵件服務物件設定檔已經建立完成。

4.6.18 通知物件

本頁讓您設定可套用於**其他應用>>簡訊/郵件警示服務**網頁中的設定檔。

4.6.18.1 通知物件



每個項目說明如下：

項目	說明
新增	新增新的設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
刪除	移除選定的設定檔。 請選擇您想要刪除的既有設定檔，然後按下刪除按鈕，該設定檔即可被移除。
更新	重新更新本頁面。
設定檔數量限制	顯示可以建立的設定檔總數。
設定檔	顯示設定檔的檔名。
WAN 中斷連線	顯示此功能爲啓用或是停用。
WAN 重新連線	顯示此功能爲啓用或是停用。
VPN 無法連線	顯示此功能爲啓用或是停用。
VPN 重新連線	顯示此功能爲啓用或是停用。
溫度	顯示此功能爲啓用或是停用。
重啓路由器	顯示此功能爲啓用或是停用。
系統日誌	顯示此功能爲啓用或是停用。

如何新增通知設定檔

1. 開啓**物件設定>>通知物件**。
2. 按下**新增**按鈕。

3. 下述頁面將會出現。

可用參數詳列如下：

項目	說明
設定檔	輸入物件設定檔的檔名。
WAN 中斷連線	啓用 – 當 WAN 介面發生中斷連線，路由器系統將會傳送警告訊息給予收信人。
WAN 重新連線	啓用 – 當 WAN 介面重新連線後，路由器系統將會傳送警告訊息給予收信人。
VPN 無法連線	啓用 – 當 VPN 通道發生中斷連線，路由器系統將會傳送警告訊息給予收信人。
VPN 重新連線	啓用 – 當 VPN 通道重新連線後，路由器系統將會傳送警告訊息給予收信人。
溫度	啓用 – 當溫度超出設定範圍後，路由器系統將會傳送警告訊息給予收信人。
重啓路由器	啓用 – 當路由器重新啓動後，路由器系統將會傳送警告訊息給予收信人。
CPU 佔用率	啓用 – 當 CPU 使用達到一定量後，路由器系統將會傳送警告訊息給予收信人。
記憶體佔用率	啓用 – 當記憶體使用達到一定量後，路由器系統將會傳送警告訊息給予收信人。

TX/RX 使用情況	**啓用** – 當 TX/RX 傳送接收使用達到一定量後，路由器系統將會傳送警告訊息給予收信人。
高可靠度	**啓用** – 當路由器成爲 HA 應用中的主要裝置時，路由器系統將會傳送警告訊息給予收信人。
系統日誌	**啓用** – 此通知訊息將會記錄於 Syslog 中。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

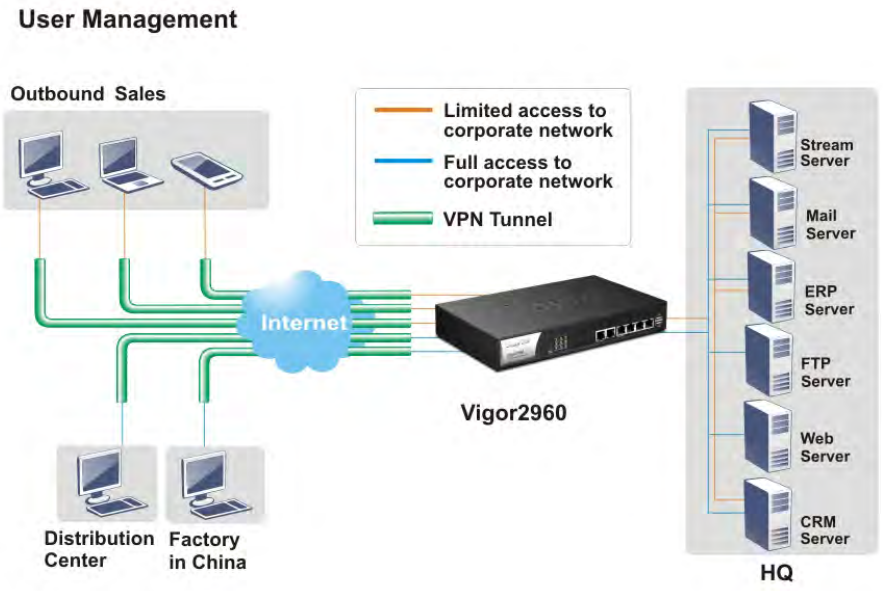
4. 輸入所有設定並按下**套用**儲存。
5. 新通知物件設定檔已經建立完成。

4.6.18.2 進階設定

本頁用來設定的 CPU、記憶體、TX/RX 等使用限制值，當 CPU、記憶體、TX/RX 達到設定的門檻之後，路由器系統將會傳送警告訊息給予特定收信人。

4.7 使用者管理

使用者管理可以透過不同的協定控制所有的帳戶(使用者設定檔)存取網際網路。



以下為使用者管理的功能選單：

4.7.1 入口網站

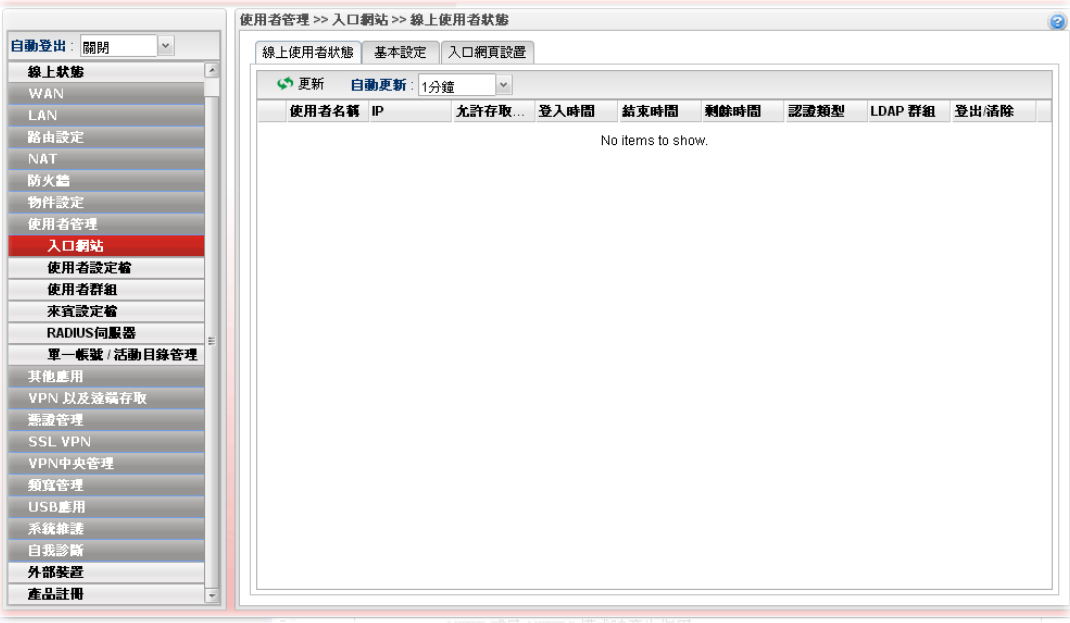
入口網站是一個能夠管理 LAN 端主機存取網路的出入口，LAN 端主機的身分可由入口機制來辨識，之後再接受某些功能的管理，像是防火牆、負載平衡等等。

本頁用來設定使用者管理機制控制所有用戶的基本規則，這裡選擇的模式會對套用到每個用戶的過濾器規則產生直接的影響。

4.7.1.1 線上使用者狀態

線上使用者狀態為一種監督工具，僅在您於**基本設定**頁面中選擇 HTTP 或是 HTTPS 模式時產生作用。

請參考 4.7.1.2 基本設定一節，取得設定網頁入口的詳細資訊。

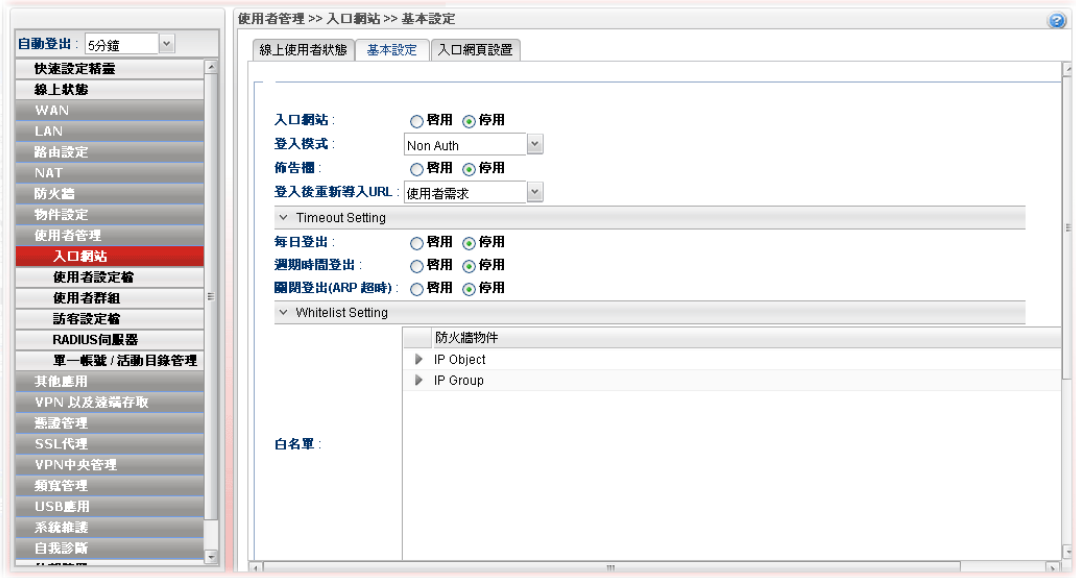


可用參數詳列如下：

項目	說明
更新	更新目前頁面。
自動更新	指定更新時間的間隔，取得最新的狀態。當按下頁面更新按鈕時，畫面上的資訊將會立即更新。
使用者名稱	顯示登入 Vigor2960 使用者設定介面的用戶名稱資訊。
IP	顯示登入 Vigor2960 使用者設定介面的用戶 IP 位址。
允許存取時間	顯示允許用戶登入網路連線的全部時間。
登入時間	顯示網路連線的起始時間。
結束時間	顯示網路連線的終止時間。
剩餘時間	顯示網路連線的剩餘時間。
認證類型	顯示此用戶使用的驗證類型(local, RADIUS, LDAP, Login Disable, Guest)。
LDAP 群組	顯示此用戶使用的 LDAP 群組。
登出/清除	此按鈕用來手動中斷連線。

4.7.1.2 基本設定

本頁可配置入口網站功能的主要設定內容。



可用參數詳列如下：

項目	說明
入口網站	選擇**啓用**按鈕以啓用此功能。
登入模式	有數種模式可以選擇： **不驗證** – 無任何驗證需求。 **HTTP/HTTPS-** 如果您選擇此模式，使用者就可以透過 HTTP 或是 HTTPS 登入 Vigor 路由器。
驗證類型	這個選項僅在您選擇 HTTP 或是 HTTPS 模式時可用，要注意的是系統採用的驗證序爲先**本機**，其次是**來賓**，**RAIUS 伺服器**爲第三，第四 **LDAP**，最後是 SMS。不過如果您勾選了 SMS，路由器將會同時以 SMS 規則及其他類型同時驗證使用者。 **LDAP 設定檔** – 當選定 LDAP 爲驗證類型時，這個選項即可使用，請自下拉式清單中指定一個設定檔(於**使用者管理>> 單一帳號/活動目錄管理**頁面中先行定義)。
佈告欄	**停用** – 關閉佈告欄功能。 **啓用** – 啓用佈告欄功能。當使用者登入 Vigor 路由器的使用者介面時，佈告欄上的訊息將會先顯示在登入螢幕上。 ● **顯示公告在強制網路登入頁面** - 這個功能在**佈告欄**啓用且 **HTTP/HTTPS** 選定爲**登入模式**時才會出現，用來決定是否在入口網站登入頁面上顯示佈告欄的內容。 ● **在未經過 Portal 認證前允許非 HTTP 協定封包** – 這個功能在**佈告欄**啓用且 **HTTP/HTTPS** 選定爲**登入模式**時才會出現，啓用此功能後，在入口網站出現之前，只有非 HTTP 的流量可允許通過。
封鎖移動裝置	**啓用** – Vigor 路由器偵測有無行動裝置嘗試透過路由器

	登入網際網路，若有發現隨即封鎖該裝置的存取行動。 **警報訊息** – 若偵測到行動裝置，本區輸入的警告訊息會顯示在行動裝置的螢幕上，預設的內容為偵測到”行動裝置”。
登入後重新導入 URL	**使用者需求** – 通過路由器的驗證之後，使用者將被導入需求的網頁。 **佈告欄** – 如果選擇此項，使用者在通過入口網站時將被強制閱讀顯示於布告欄內的訊息。 **自定義 URL** -任何一個想要透過此路由器登入網際網路的用戶都會被重新導向到此處指定的 URL 網頁。這個功能對希望達成廣告效果而言非常有效，例如，可以強迫飯店內的無線用戶進入該飯店希望他/她造訪的網頁。 ● **自定義 URL** – 請輸入準備導向的網頁。
簡訊設定 – 當 **SMS** 被選定為**驗證類型**時，即可使用本設定項目。使用者如果想要登入網際網路，系統會要求使用驗證碼進行驗證。	
簡訊供應商	使用下拉式清單指定提供簡訊服務的供應商。
簡訊按鈕名稱	用來告訴使用者此按鈕可以用來取得使用者名稱及密碼以便登入網際網路。
簡訊重發間隔	在此區輸入簡訊發送的間隔時間，此功能的優點在於可避免系統在極短的時間內經常發送簡訊因而造成成本增加與浪費。
簡訊內容	輸入簡訊的內容，預設的編碼格式為“UTF-8” 。 在輸入內文之前，請先確認服務供應商提供之編碼格式，如果供應商不支援“UTF-8”，轉碼就必須先行完成，如果您有任何的問題，請聯絡簡訊服務供應商。
Customized Field 1/2/3	管理者可以蒐集詢問驗證碼以便登入網際網路之使用者的資訊(如名字、電子郵件、地址、年齡、工作等等)，自行動裝置用戶取得資訊主要有三方面，每個區域都可以分別啓用或是停用。 **啓用** – 於 Customized Field 1/2/3 定義之標題可以在行動裝置上清晰可見，當這些區域啓用時，行動用戶必須提供這些標籤所指定標題的相關資料，之後才會給予驗證碼。 **停用** – 於 Customized Field 1/2/3 定義之標題不會顯示在行動裝置上，行動裝置用戶可以在輸入電話號碼並按下確認按鈕(簡訊按鈕名稱定義的按鈕)之後，取得驗證碼資訊。 **啓用且必填** – 行動裝置用戶必須輸入電話號碼以及填畢螢幕上所有必要的資訊，之後按下確認按鈕(簡訊按鈕名稱定義的按鈕)之後，取得驗證碼資訊。
Customized Field 1/2/3 Label	定義上述客製化區域的標籤內容。
日誌檔案限制	自行動用戶(透過驗證法之需求)蒐集而得之資訊將以日

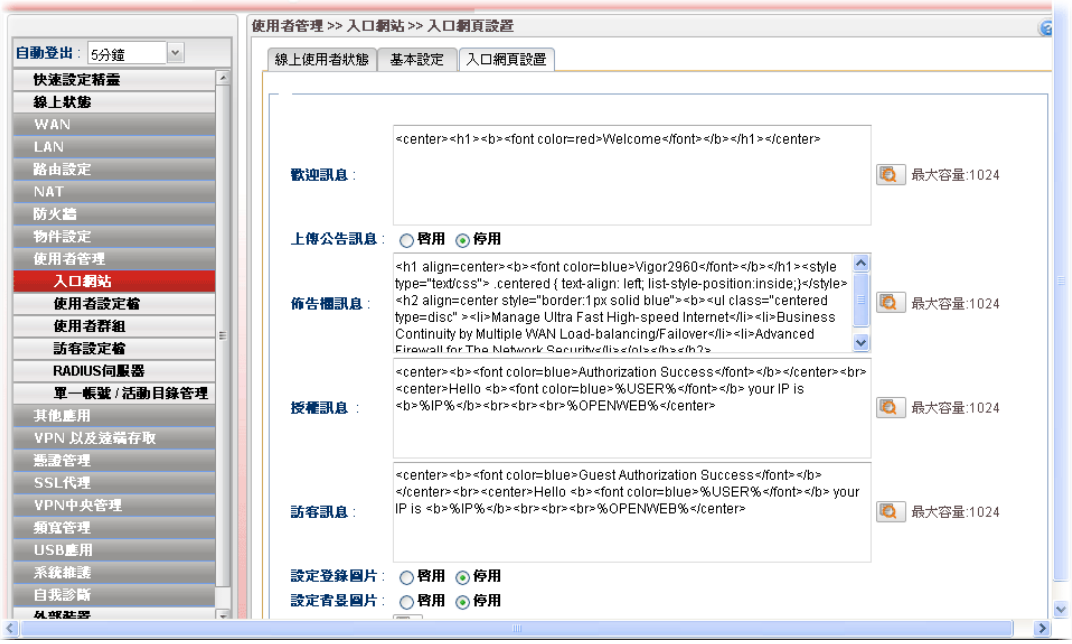
	誌檔案儲存起來，本設定用來限制日誌檔案的大小。
匯出日誌檔案	簡訊日誌可以輸出成格式為“.csv”的檔案。
逾時設定	
每日登出	**啓用** - 強迫線上使用者每日皆須登出 Vigor 路由器的使用者介面。 ● **每日登出時間** -這個功能僅在**每日登出**啓用時可用。輸入時間設定(時：分)讓路由器強迫線上使用者離開路由器的設定頁面。 ● **每日登出後自動補足時間配額** -這個功能僅在**每日登出**啓用時可用。當**每日登出**功能被執行後，所有本機用戶的時間額度會重新回復。
週期時間登出	**啓用** - 強迫線上使用者經過一段時間後登出 Vigor 路由器的使用者介面。 ● **週期登出時間** - 這個功能僅在**週期時間登出**啓用時可用。
閒置登出	**啓用** - 在路由器閒置的狀態下，強迫線上使用者登出路由器的網頁設定介面。 ● **閒置時間(分鐘)** – 設定一段時間，當時間到達時，路由器將會中斷線上使用者的網路連線。
白名單設定	
白名單	選擇入口網站功能可以忽略的來源 IP 物件/群組。
IPv6 白名單	選擇入口網站功能可以忽略的來源 IP 物件/群組。
套用	按此鈕儲存設定。
取消	按此鈕捨棄頁面設定。

注意：如果要關閉入口網站的功能，請同時停用**登入模式**與**佈告欄**。

4.7.1.3 入口網頁設置

本頁讓您設定入口頁面中準備出現的訊息(支援 HTML-格式)，如此一來，當使用者透過入口網站登入網際網路時即可見到該訊息。

不論無線網路用戶/區域網路用戶的目的為何，只要使用者透過此路由器嘗試進入網際網路或是想要造訪的網頁時，都會被直接帶往此頁指定的網頁，也就是說，公司行號如果想要打產品廣告時，可以在此指定相關頁面就可以達成其目的。



可用參數詳列如下：

項目	說明
歡迎訊息	在此輸入文字語句，此處資訊會顯示在登入頁面的頂端。
上傳公告訊息	**上傳選擇的檔案** – 這個功能在您**啓**用**上傳公告訊息**後始可使用，請選擇特定檔案上傳至 Vigor2960。
佈告欄訊息	這個功能在您**停**用**上傳公告信息**後始可使用， 此處輸入的文字將會顯示在登入頁面或是授權頁面的底部。在登入頁面上，可取消勾選”在登入頁面顯示佈告欄”選項關閉此訊息。
授權訊息	此處輸入的內容將顯示在使用者成功通過驗證之後系統呈現的授權頁面上。
訪客訊息	在來賓成功通過驗證之後，歡迎來賓訊息內容將會顯示在螢幕上。
設定登錄圖片	指定使用者或是來賓嘗試登入網際網路時，可直接在登入頁面上看到的影像。 **上傳登錄圖片** – 選擇一個檔案上傳至路由器，這個功能適合用於打廣告。
設定背景圖片	指定影像檔案，使其在登入頁面上以背景方式來呈現。 **上傳背景圖片** – 選擇檔案上傳至路由器。

項目	說明
登入頁面預覽	按此鈕可預覽登入頁面的內容(包含歡迎資訊與公佈欄訊息)。
重置爲出廠預設值	重新回復上述所有的訊息爲預設內容，勾選此方塊並按**套用**即可。
套用	按此鈕儲存設定。
取消	按此鈕捨棄頁面設定。

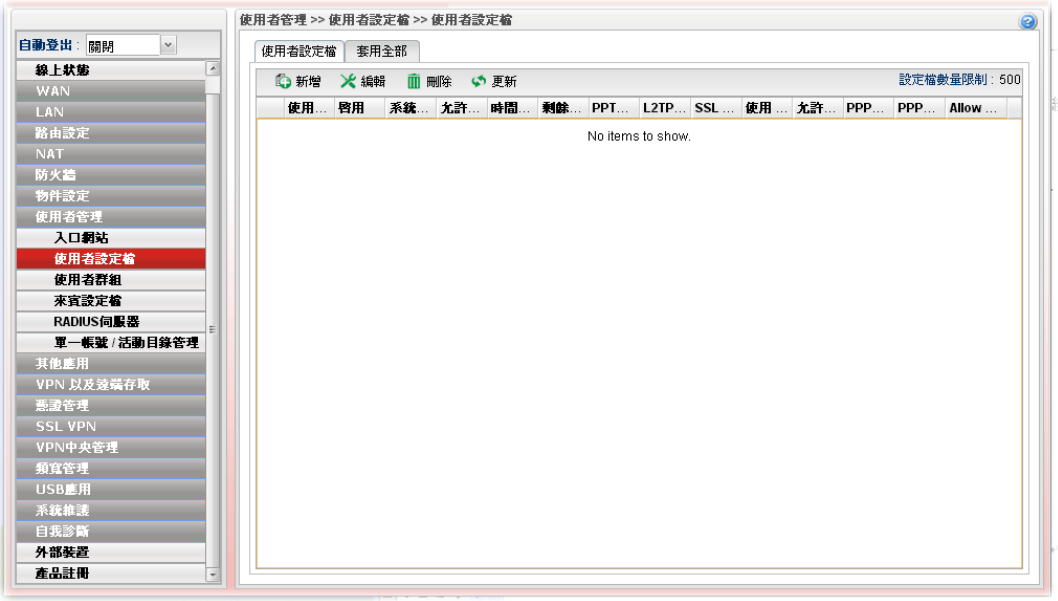
完成設定後，按下**套用**儲存設定。

4.7.2 使用者設定檔

此功能允許您設定 Vigor2960 管理的所有帳戶(使用者設定檔)，包含 PPTP/L2TP、系統使用者等等。

4.7.2.1 使用者設定檔

使用者設定檔可針對 Vigor2960 管理的用戶，提供不同的授權內容，包含入口網站、VPN 撥入、PPPoE 伺服器、系統管理等等。



每個項目說明如下：

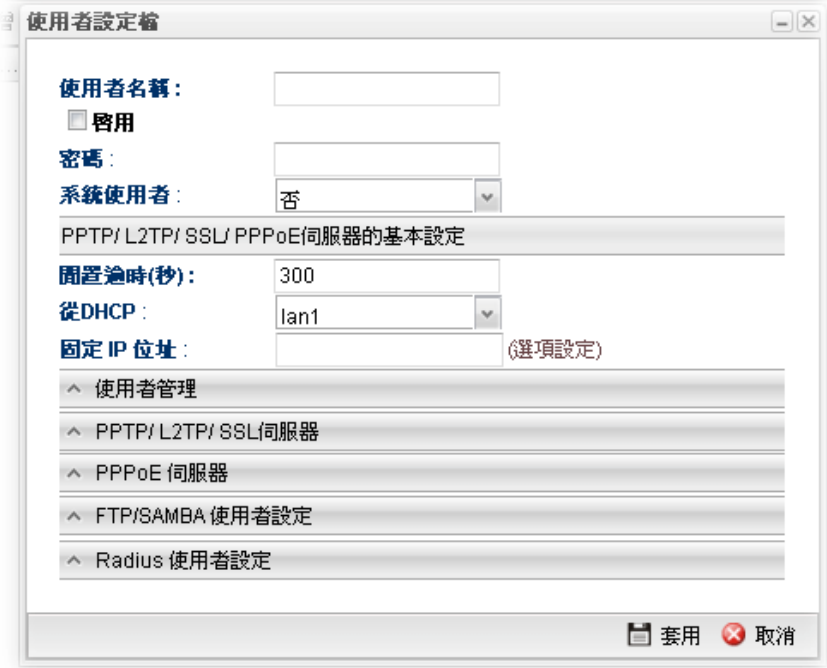
項目	說明
新增	新增新的設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
刪除	移除選定的設定檔。 請選擇您想要刪除的既有設定檔，然後按下刪除按鈕，該設定檔即可被移除。

項目	說明
更新	重新更新本頁面。
設定檔數量限制	顯示可以建立的設定檔總數。
使用者名稱	顯示使用者的帳戶名稱。
啓用	顯示設定檔狀態，False 表示停用；True 表示啓用。
系統使用者	顯示系統使用者狀態，False 表示停用；True 表示啓用。
允許入口網站登入	顯示登入入口網站的帳戶狀態(啓用/停用)。
時間配置	顯示入口網站運用機制時間額度的狀態(啓用/停用)。
剩餘時間	顯示此使用者設定檔的剩餘時間。 **補足時間配額** – 可及時將剩餘時間回復到使用者剛登入時擁有的時間額度(線上使用者不會被登出)。
PPTP 撥入	顯示此使用者設定檔的 PPTP 連線狀態。
L2TP 撥入	顯示此使用者設定檔的 L2TP 連線狀態。
SSL 通道	顯示 SSL 通道是否已被啓動(啓用或是停用)。
使用 **mOTP**	顯示 mOTP 是否已被啓動(啓用或是停用)。
允許 **PPPoE** 伺服器登入	顯示使用者設定檔的 PPPoE 連線狀態(啓用或是停用)。
PPPoE 時間配額(分)	顯示此使用者設定檔目前的 PPPoE 時間額度爲何。
PPPoE 流量配額(百萬位元組)	顯示此使用者設定檔目前的 PPPoE 網路流量額度的運用情形。
允許 **FTP** 伺服器登入	顯示 FTP 伺服器登入是否已經啓動(啓用或是停用)。
允許 **SMABA** 伺服器登入	顯示 SAMBA 伺服器登入是否已經啓動(啓用或是停用)。
允許 **Radius** 伺服器登入	顯示 Radius 伺服器登入是否已經啓動(啓用或是停用)。

如何新增使用者設定檔

1. 開啓**使用者管理>>使用者設定檔**。
2. 按下**新增**按鈕。

3. 下述頁面將會出現。



可用參數詳列如下：

項目	說明
使用者名稱	請輸入此使用者設定檔的名稱(例如 *LAN_User_Group_1, WLAN_User_Group_A, WLAN_User_Group_B* 等等)，當使用者嘗試利用本路由器登入網際網路時，必須先通過驗證步驟。使用者必須輸入此處所設定的使用者名稱才能通過驗證，一旦通過驗證，使用者即可利用此路由器享受網際網路。不過，在操作網際網路時會受到此設定檔所做的限制。
啓用	勾選此方塊啓用此設定檔。
密碼	請輸入此使用者設定檔的密碼(例如 *lug123, wug123,wug456* 等等)，當使用者嘗試利用本路由器登入網際網路時，必須先通過驗證步驟。使用者必須輸入此處所設定的密碼才能通過驗證，一旦通過驗證，使用者即可利用此路由器享受網際網路。不過，在操作網際網路時會受到此設定檔所做的限制。

系統使用者	具備優先權限的使用者，可以決定以管理者身份來操作路由器功能 否 – 選此停用系統使用者功能，則此使用者設定檔即不具備操作路由器功能的權利。 是 –.選此啓用系統使用者功能。 特權等級– 如果系統使用者選擇啓用，您必須爲此設定檔指定權限等級(使用者/操作員/管理員)。 管理員具有最高路由器操作權限，使用者具有最低路由器操作權限。
PPTP/L2TP/SSL/PPPoE 伺服器的基本設定	
閒置逾時(秒)	如果使用者有一段時間沒有任何動作，網路連線將會自動中斷，預設值爲 300 秒。
從 DHCP	選擇一個 LAN 設定檔以應 DHCP 伺服器 IP 調度。 使用此設定檔進行 PPTP/L2TP 撥入連線的遠端用戶，可依照 DHCP 位址配置量取得 IP 位址。
固定 IP 位址	輸入準備以 PPTP/L2TP 連線登入網際網路的使用者設定檔之 IP 位址。
使用者管理	
允許入口網站登入	啓用 – 選擇此項即可使用此設定檔進行入口網站登入功能。 停用 – 選擇此項關閉功能。
時間配置	啓用 – 選擇此項開啓功能。 停用 – 選擇此項關閉功能。 設定時間配額(分)– 輸入時間值。 剩餘時間 – 顯示此使用者設定檔的剩餘時間。 注意：時間配額的設定值範圍在 1~14400 之間。
同時登入限制	此設定檔可以讓很多使用者使用，您可以設定最多登入網際網路的使用者總數。 設定範圍爲 1 到 255，-1 表示沒有限制；0 則表示無法存取。
PPTP/L2TP/SSL 伺服器	
PPTP/L2TP 撥入/SSL 通道	按下啓用可讓準備透過此設定檔登入網際網路的使用者，透過 PPTP/L2TP/SSL 通道協定進行網路連線。
使用 mOTP	選啓用以便使用 mOTP 功能驗證。 mOTP PIN 碼 - 輸入驗證所需的代碼(例如 1234)。 mOTP 密碼 – 使用行動電話中 mOTP 產生的 32 位數密碼 (如 e759bb6f0e94c7ab4fe6)。

SSL 代理	這個功能僅在**系統使用者**設定爲**否**時可用。SSL 網頁代理伺服器將可套用至 VPN。 欲清除選定項目，按下 ✕ 即可移除目前的選項。
SSL 應用(VNC)	這個功能僅在**系統使用者**設定爲**否**時可用。選擇任一個 SSL 應用設定檔(VNC)以套用至此設定檔上。 欲清除選定項目，按下 ✕ 即可移除目前的選項。
SSL 應用(RDP)	這個功能僅在**系統使用者**設定爲**否**時可用。選擇任一個 SSL 應用設定檔(RDP)以套用至此設定檔上。 欲清除選定項目，按下 ✕ 即可移除目前的選項。
PPPoE 伺服器	
允許 PPPoE 伺服器登錄	按**啓用**來啓動相關的 PPPoE 設定。
配額重新設定頻率	這個功能用來設定 PPPoE 連線額度的週期，請注意每次額度重新設定時，目前已用時間/目前已用流量的額度都會被重新回復成初始狀態(0)。 **每日**– PPPoE 連線額度爲每日重新計算。 **每月**–PPPoE 連線額度爲每月重新計算。
時間配額(分)	輸入 PPPoE 連線的時間額度值。 **注意**：時間配額的設定值範圍在 1~14400 之間。
目前已用時間配額(分)	顯示使用者已經使用的累計時間值。 **重新設定** – 按此回復設定爲出廠預設值(0)。
流量配額(MB)	用來設定此使用者設定檔的最大允許流量(MB)。
目前已用流量配額(MB)	顯示使用者已經使用的累計流量值。 **重新設定** – 按此回復設定爲出廠預設值(0)。
綁定 MAC 位址	指定一組 MAC 位址，限制只能給目前的 PPPoE 帳號使用。 **啓用** – 按此啓用此功能。 **MAC 位址** – 如果啓用了 MAC 綁定，只要在此區輸入路由器的 MAC 位址即可。
FTP/SAMBA 使用者設定)	
允許 FTP 伺服器登入	按**啓用**讓遠端使用者得以透過 FTP 伺服器登入網際網路。
Radius 使用者設定	
允許 Radius 伺服器登入	按**啓用**讓遠端使用者得以透過 **Radius** 伺服器登入網際網路。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

4. 輸入所有設定並按下**套用**儲存。

5. 新使用者設定檔已經建立完成。

4.7.2.2 套用全部

本頁允許您修正一些功能並套用到所有的使用者設定檔上，由於管理者無須一個個開啓使用者設定檔進行設定編輯與修正事宜，因爲對於管理者來說這個功能相當的方便。

您可以按下**套用**儲存修改後設定，之後此處所做的改變都將全部套用到所有的使用者設定檔。

可用參數詳列如下：

項目	說明
修改入口網站登入狀態	勾選此框以便進行其他設定。 **啓用** – 選擇此項可以爲遠端用戶啓動入口網站登入功能。
修改時間配額狀態	勾選此框以便進行其他設定。 **啓用** – 選擇此項可以爲所有的使用者設定檔啓動時間額度功能。
修改時間配額值	勾選此框以便進行其他設定。 **時間配額(分)** - 您需勾選此項並在其後的方框中輸入時間額度資訊。
修改使用者登入最大數	勾選此框以便進行其他設定。 **最大用戶登入數量** - -1 表示沒有限制; 0 表示不可存取。
修改閒置逾時	勾選此框以便進行其他設定。 **閒置逾時**- 如果使用者有一段時間沒有任何動作，網路連線將會自動中斷，預設值爲 300 秒。

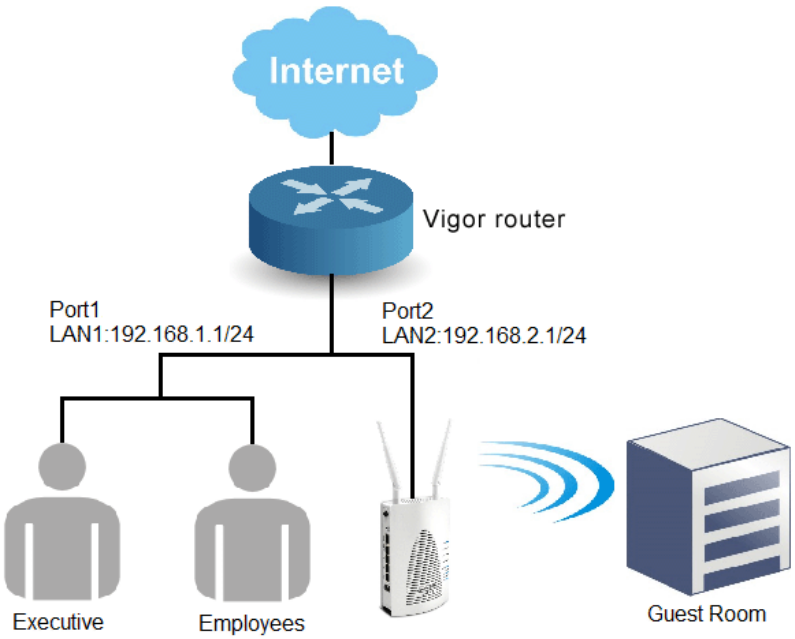
修改 PPTP/ **修改 L2TP 狀態/** **修改 SSL 通道狀態**	勾選此框以便進行其他設定。 **啓用** – 選此項可讓所有的使用者設定檔皆透過 PPTP/L2TP/SSL 通道連線網際網路。
修改 mOTP 狀態	勾選此框以便進行其他設定。 **mOTP –** 選**啓用**可讓所有的使用者設定檔都啓用 mOTP 功能。
修改 PPPoE/FTP/Radius/ SAMBA 伺服器登入狀態	勾選此框以便進行其他設定。 **PPPoE/FTP/Radius/SAMBA 伺服器登入–** 選**啓用**可對所有的使用者進行 **PPPoE/FTP/Radius/SAMBA** 驗證。
套用至	**所有** – 所有的修改內容套用至全部的使用者設定檔。 **部分** – 所有的修改內容套用至指定的使用者設定檔。
套用	按此鈕儲存設定。
取消	按此鈕捨棄頁面設定。

完成設定後，按下**套用**儲存設定。

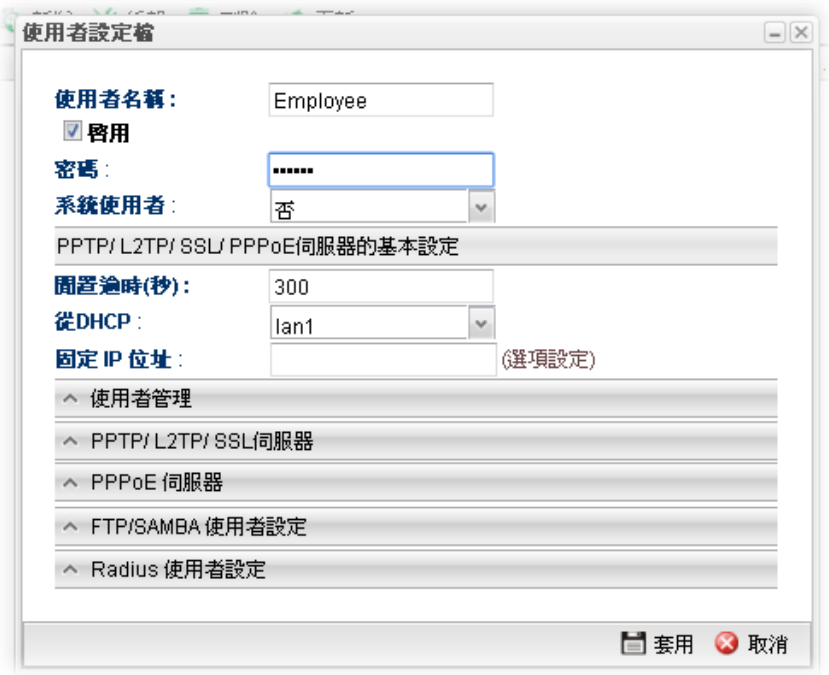
範例：如何利用使用者管理產生大量的 LAN 用戶

下列表格顯示使用者設定檔與訪客設定檔(透過大量來賓帳號產生器產生)二者之間的差異：

	使用者設定檔	大量來賓帳號產生器
帳號數量	一次最多可建立 500 組帳號	一次最多產生 250 組帳號
帳號	手動操作	自動規律產生
密碼	由管理員分別建立不同的密碼	隨機產生，密碼長度可由管理員指定
每組帳號同時允許上線的使用者數量	1~255 個或是不限制(設定值爲-1)	不支援
權限	網際網路、VPN、PPPOE 連線	僅限網際網路存取
使用限制/期滿時間	時間配額 (1~14400 分)	時間配額 (1~14400 分) 有效期限 (天數)
驗證	是	是
綁定 IP 位址	是	否



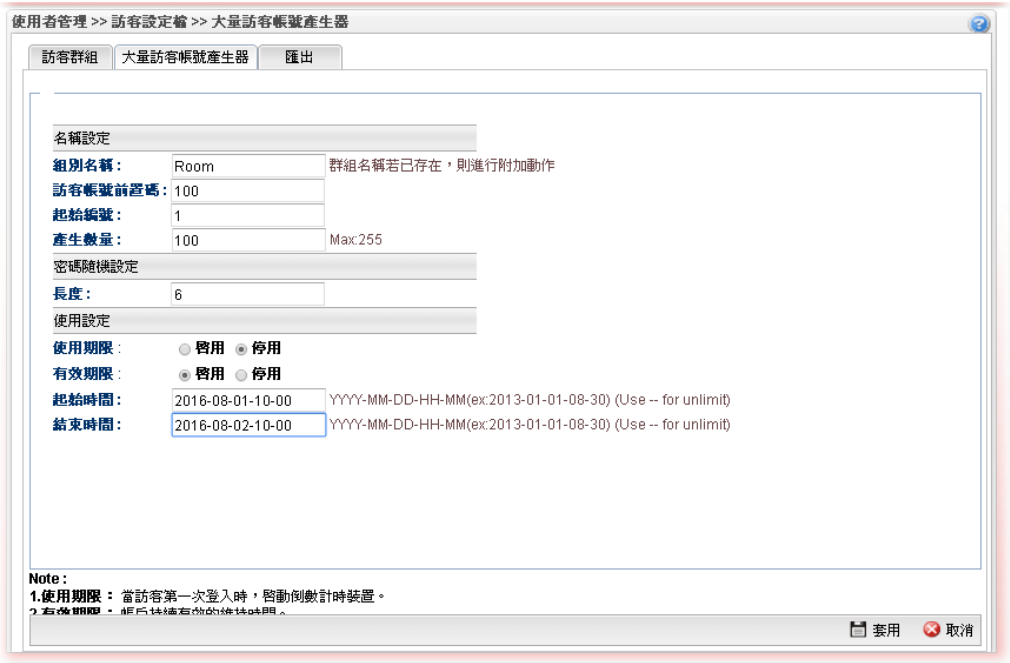
1. 開啓**使用者管理** >> **使用者設定檔**，按下**新增**。
2. 參考下圖設定使用者設定檔，輸入**使用者名稱**、按下**啓用**並輸入**密碼**，接著輸入**同時登入限制**數量，按下**套用**儲存設定。.



3. 開啓**物件設定>>IP 物件**並按下**新增**。

4. 設定 Executive 的 IP 物件，輸入設定檔的名稱(例如 boss)，選擇 Single 作爲位址類型，接著輸入 IP 位址 192.168.1.11。按下**套用**儲存設定。

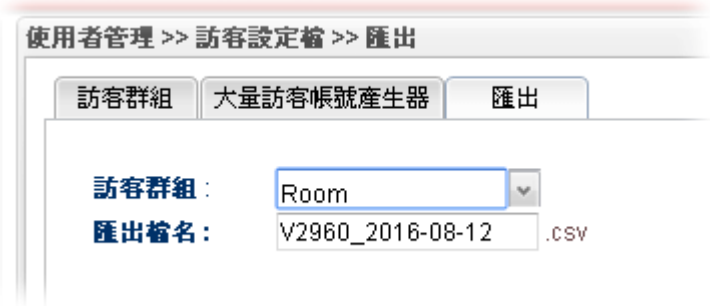
5. 開啓**使用者管理>>訪客設定檔**，按下**大量訪客帳號產生器**標籤開啓如下頁面，輸入**組別名稱**(本例爲 Room)；**訪客帳號前置碼**；**產生數量**(本例爲 100)，**有效期間**選擇**啓用**，輸入**起始時間**與**結束時間**，按下**套用**儲存設定。

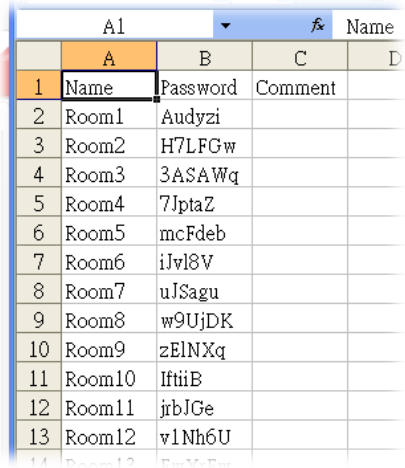


6. 開啓**使用者管理>>訪客設定檔**，按下**訪客群組**檢查大量使用者帳號群組內容。

透過按下每個帳號(例如選擇 1001 然後按下**編輯**)，我們可以檢查該帳號的相關資訊，同時也可以手動進行帳號名稱與密碼修正。

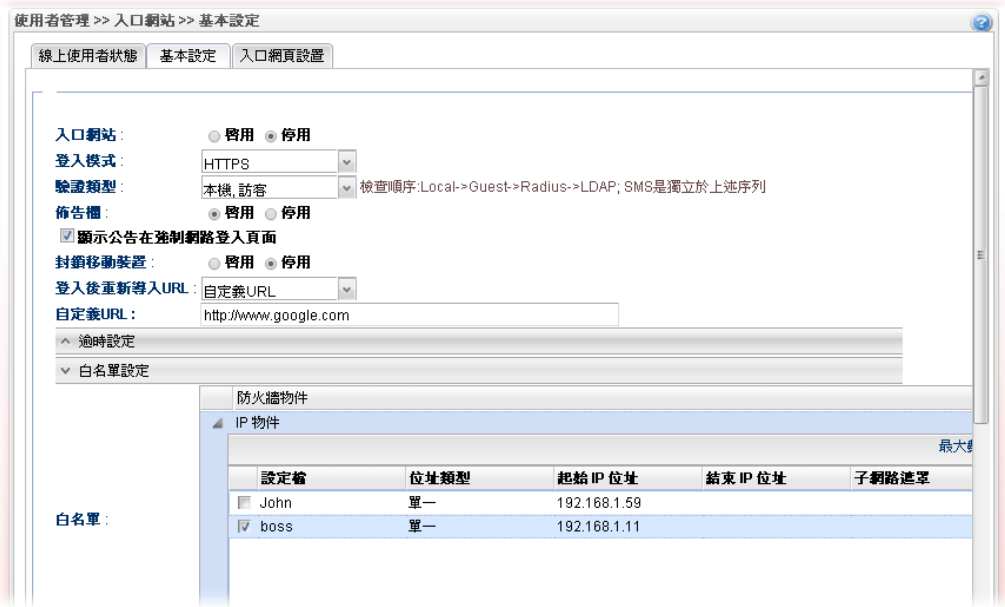
注意，管理員(Administrator)可以輸出整個群組資訊並儲存爲.*csv* 檔案，方便將帳號與密碼組合重新分派給予不同的使用者。





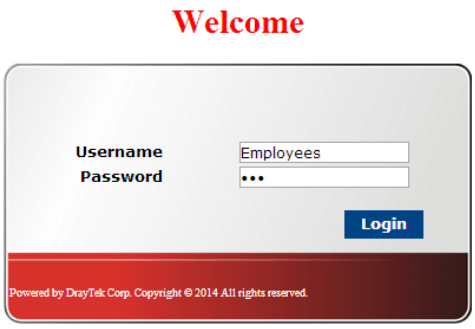
	A	B	C
1	Name	Password	Comment
2	Room1	Audyzi	
3	Room2	H7LFGw	
4	Room3	3ASAWq	
5	Room4	7JptaZ	
6	Room5	mcFdeb	
7	Room6	iJvl8V	
8	Room7	uJSagu	
9	Room8	w9UjDK	
10	Room9	zElNXq	
11	Room10	IftiiB	
12	Room11	jrbJGe	
13	Room12	v1Nh6U	

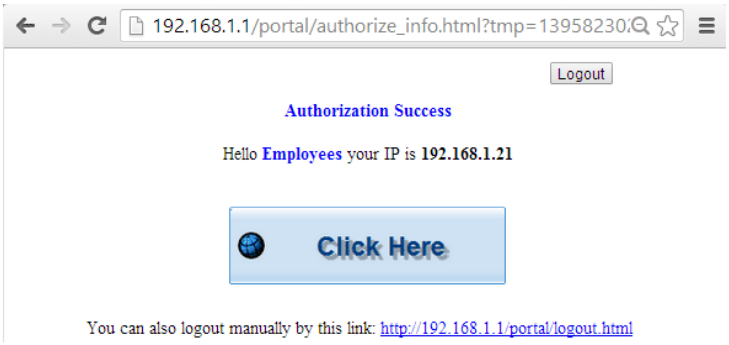
7. 開啓**使用者管理>>入口網站**並按**基本設定**開啓如下頁面，**登入模式**選擇 HTTP/HTTPS，選擇**本機**與**訪客**作爲**驗證類型**，白名單部分選擇名爲 **Boss** 的 IP 物件設定檔，讓設定檔內的 IP 位址能在無須驗證的情況下登入網際網路。



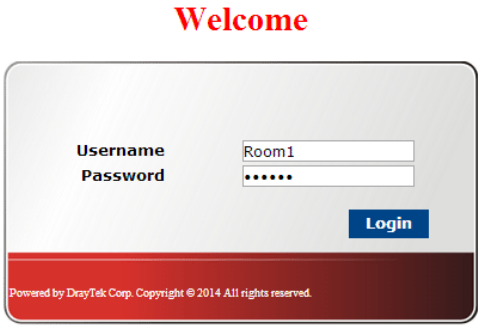
8. 完成設定後，Vigor2960 將在使用者登入網際網路時，重新導入使用者進入驗證頁面。

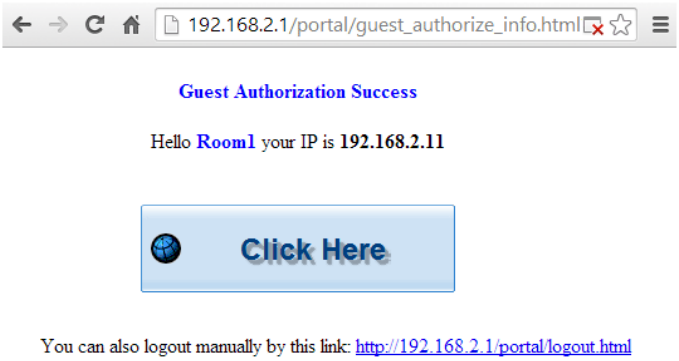
系統對員工嘗試登入網際網路時呈現的頁面：





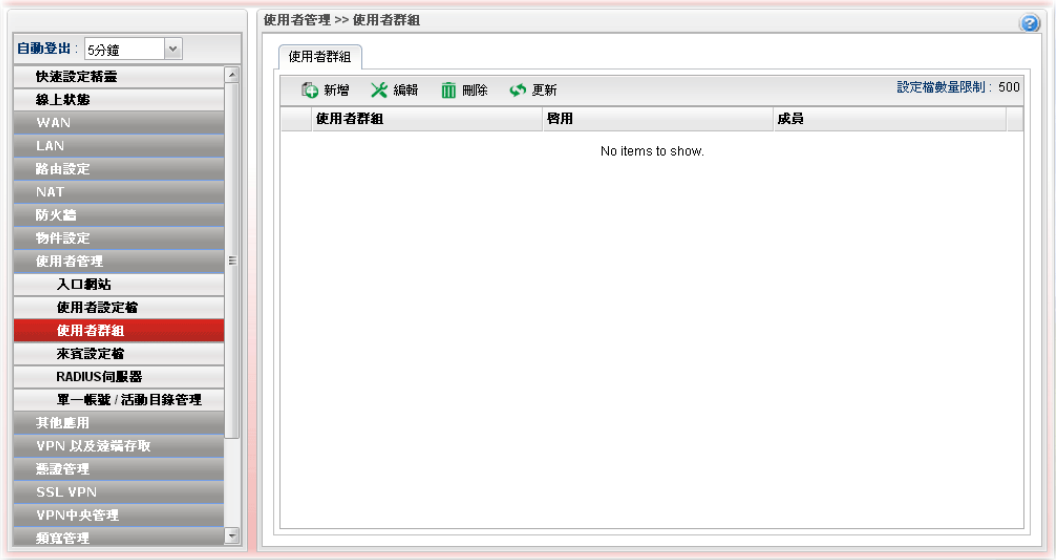
系統對飯店來賓嘗試登入網際網路時呈現的頁面：





4.7.3 使用者群組

使用者群組包含數個使用者設定檔，方便管理者管理大量的用戶。



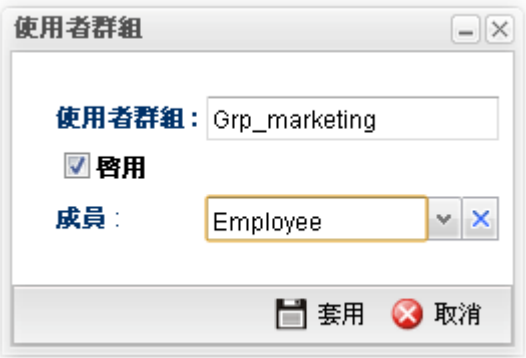
每個項目說明如下：

項目	說明
新增	新增新的設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編

項目	說明
	輯按鈕，編輯視窗將會出現讓您修改內容。
刪除	移除選定的設定檔。 請選擇您想要刪除的既有設定檔，然後按下刪除按鈕，該設定檔即可被移除。
更新	重新更新本頁面。
設定檔數量限制	顯示可以建立的設定檔總數。
使用者群組	顯示使用者群組的名稱。
啓用	顯示設定檔狀態，False 表示停用；True 表示啓用。
成員	顯示此群組下的使用者設定檔爲何。

如何新增使用者群組設定檔

1. 開啓**使用者管理>>使用者群組**。
2. 按下**新增**按鈕。
3. 下述頁面將會出現。



可用參數詳列如下：

項目	說明
使用者群組	輸入此設定檔名稱。
啓用	勾選此框啓用設定檔。
成員	使用下拉式清單選擇使用者設定檔。 如欲刪除選定的項目，按下 ✕ 即可刪除該項。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

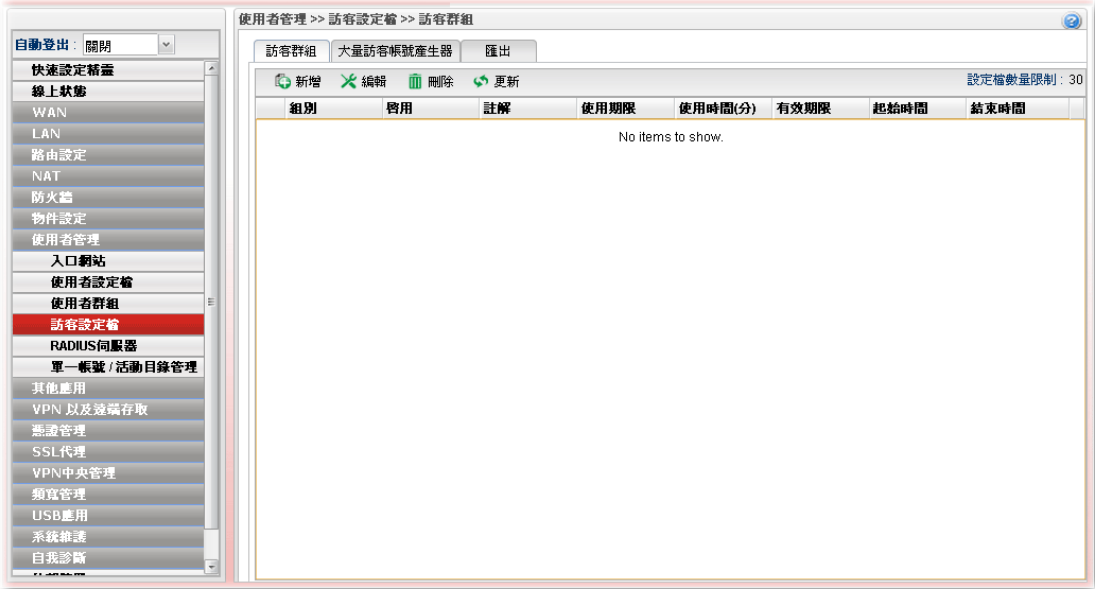
4. 輸入所有設定並按下**套用**儲存。

5. 新使用者群組設定檔已經建立完成。

4.7.4 訪客設定檔

訪客設定檔允許使用者在一定的期間登入網際網路並限制使用者僅能登入入口網站指定的網頁。

4.7.4.1 訪客群組



可用參數詳列如下：

項目	說明
新增	新增新的設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
刪除	移除選定的設定檔。 請選擇您想要刪除的既有設定檔，然後按下刪除按鈕，該設定檔即可被移除。
更新	重新更新本頁面。
設定檔數量限制	顯示可以建立的設定檔總數。
組別	顯示來賓群組名稱。
啓用	顯示設定檔狀態，False 表示停用；True 表示啓用。
註解	顯示與此設定檔有關的簡易說明。
使用期限	顯示使用時間功能的狀態(啓用/停用)。
使用時間(分)	顯示提供給來賓每次登入網際網路的使用時間。
有效期限	顯示來賓登入網際網路的有效期間。

項目	說明
起始時間/結束時間	顯示細部時間設定。

如何新增訪客群組設定檔

1. 開啓使用者管理>>訪客設定檔，按下訪客群組標籤。
2. 按下新增按鈕。
3. 下述頁面將會出現。

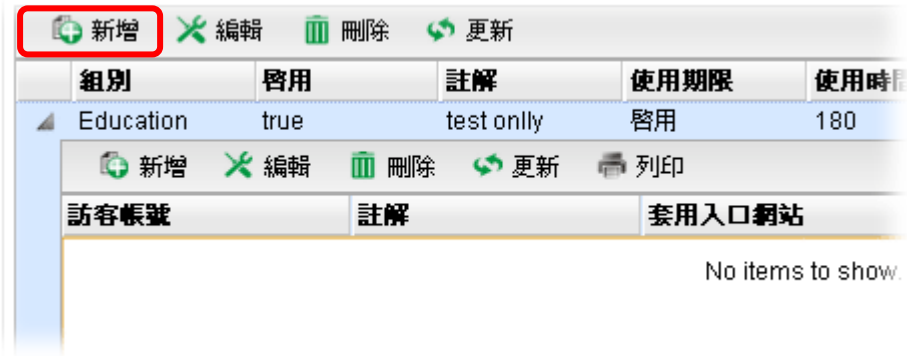
可用參數詳列如下：

項目	說明
組別	輸入此設定檔名稱。
啓用	勾選此框啓用設定檔。
註解	針對此設定檔提供簡易的說明。
使用期限	這個選項決定來賓每次登入網際網路的使用時間，按下啓用啓動此功能。 使用時間(分) - 這個選項決定每次給予登入網際網路的持續時間，預設值爲 180 分鐘，當時間已屆，使用者將被迫離開網際網路。
有效期限	有效期間選項決定使用者帳戶/來賓的網路使用有效期限，在有效期間內，使用者/來賓可以隨時進出網際網路。 起始時間/結束時間 – 指定有效期間的起點與終點，輸入格式爲年-月-日-時-分(YYYY-MM-DD-HH-MM)。 當設定爲“--“時，表示時間設定爲沒有限制。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

4. 輸入所有設定並按下套用儲存。
5. 新訪客群組設定檔已經建立完成。

6. 按下選定訪客群組設定檔左邊的 ▶ 圖示，您可以建立多個訪客名稱，設定頁面將出現在畫面上讓您新增訪客名單。

7. 移動滑鼠以按下**新增**按鈕。



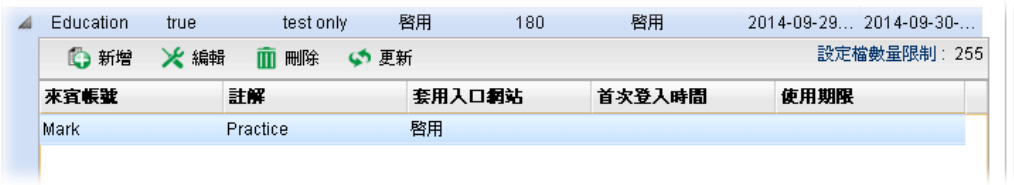
8. 設定頁面出現如下。

可用參數詳列如下：

項目	說明
訪客帳號	顯示納入訪客群組下的訪客名稱。
註解	針對訪客提供簡易說明。
套用入口網站	啓用 – 按此讓此設定檔得以套用至入口網站頁面。 停用 – 按此停用此功能。
清除使用期限	解除封鎖訪客設定檔讓該檔可由其他使用者運用。

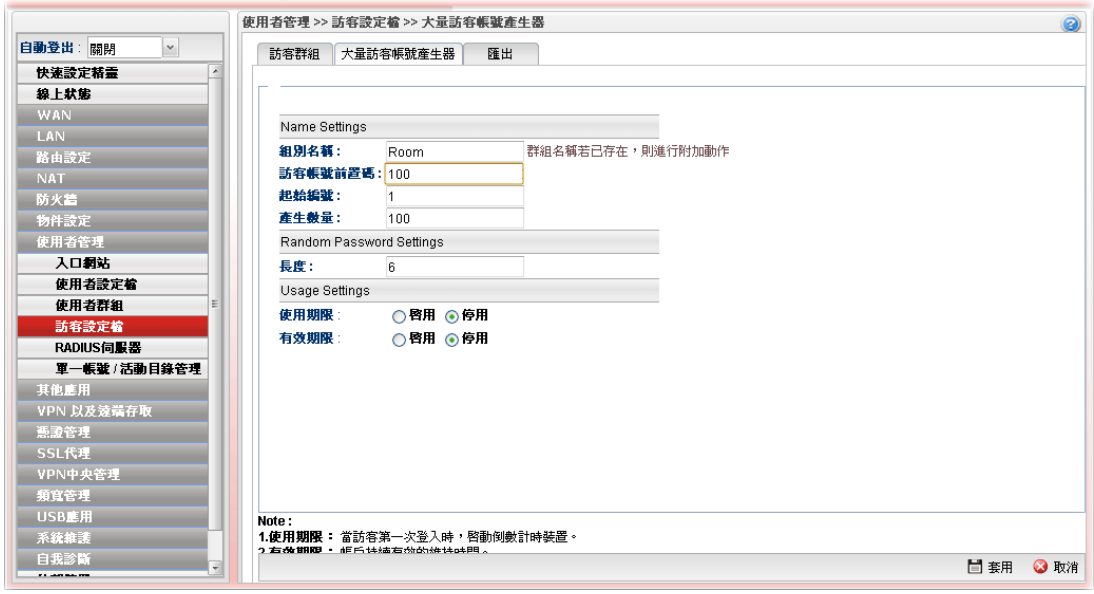
9. 輸入所有設定並按下**套用**儲存。

10. 新訪客(例如本例使用的 Mark)已加入訪客群組設定檔(例如本例使用的 Education)已經建立完成。



4.7.4.2 大量訪客帳號產生器

這個頁面可以最迅速的方式建立大量的訪客設定檔。



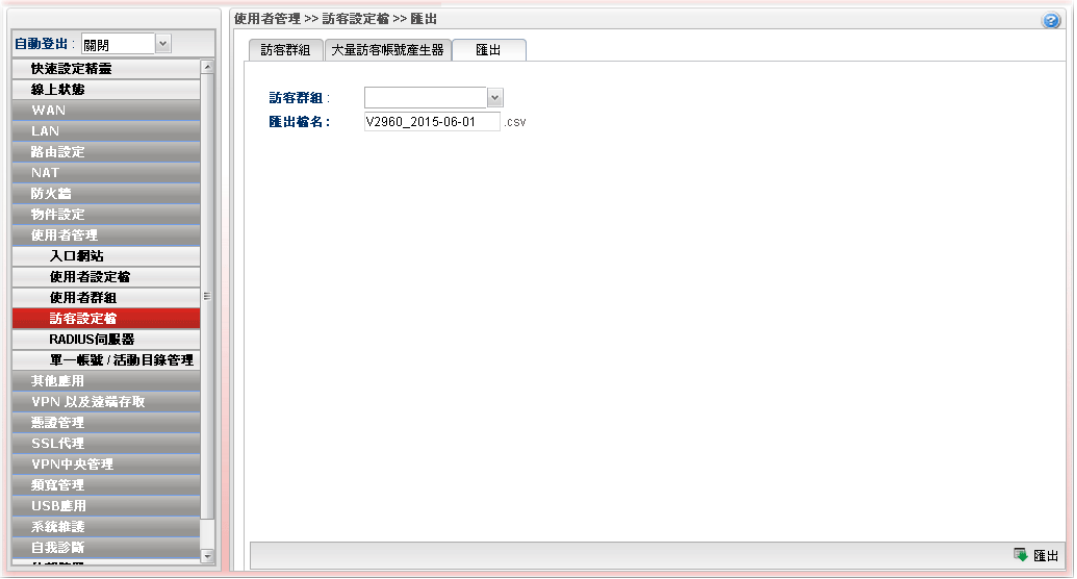
可用參數詳列如下：

項目	說明
Name Settings (命名設定)	**組別名稱** – 輸入來賓群組的名稱。 **訪客帳號前置詞** – 以此方式來命名的訪客名稱需要前置詞，當成命名輸入的基礎。 **注意:** 來賓帳號前置詞不允許下述字元"^?$%.&"。 **起始編號** – 輸入一個號碼，這個號碼可被視爲大量訪客設定檔的起始編號。 **注意:** 起始編號範圍爲 1~10000。 **產生數量** – 輸入一次產生的來賓總數。例如想要產生 10 筆，就請輸入 10。 訪客帳號的命名方式爲” 訪客帳號前置詞”+”起始編號”，例如： 來賓前置詞爲(Guest Name Prefix) => teashop_ 起始索引爲(Start Index) => 100 產生的數目爲(Number to Generate) => 50 那麼，系統將會將訪客命名爲:

項目	說明
	teashop_100 (開始) teashop_101 teashop_102 ... teashop_150 (結束)
Random Password Settings (隨機密碼設定)	**長度** – 輸入決定隨機密碼的長度值，此密碼在系統產生大量訪客設定檔時會自動分派。密碼長度範圍爲 6~12。
Usage Settings (使用設定)	**使用期限** –這個項目決定訪客每次登入網際網路的使用期限，按下**啓用**以便啓動此選項。. ● **使用時間(分)**-預設值爲 180 分鐘。 **有效期限** – 這個項目決定訪客登入網際網路的有效期間，也就是一旦過了有效期間，訪客就再也無法登入網際網路。按下**啓用**以便啓動此選項。 ● **起始時間/結束時間(Start Time/End Time)** – 指定有效期間，輸入格式爲年-月-日-分 (YYYY-MM-DD-MM)。
套用	按此鈕儲存設定。
取消	按此鈕捨棄頁面設定。

4.7.4.3 匯出

本頁用來匯出訪客設定檔名稱與隨機密碼。



可用參數詳列如下：

項目	說明
訪客群組	選擇一個您想要輸出設定內容包含訪客設定檔與隨機密碼的群組，輸出內容可供您參考。
匯出檔名	按此鈕立刻執行輸出作業。

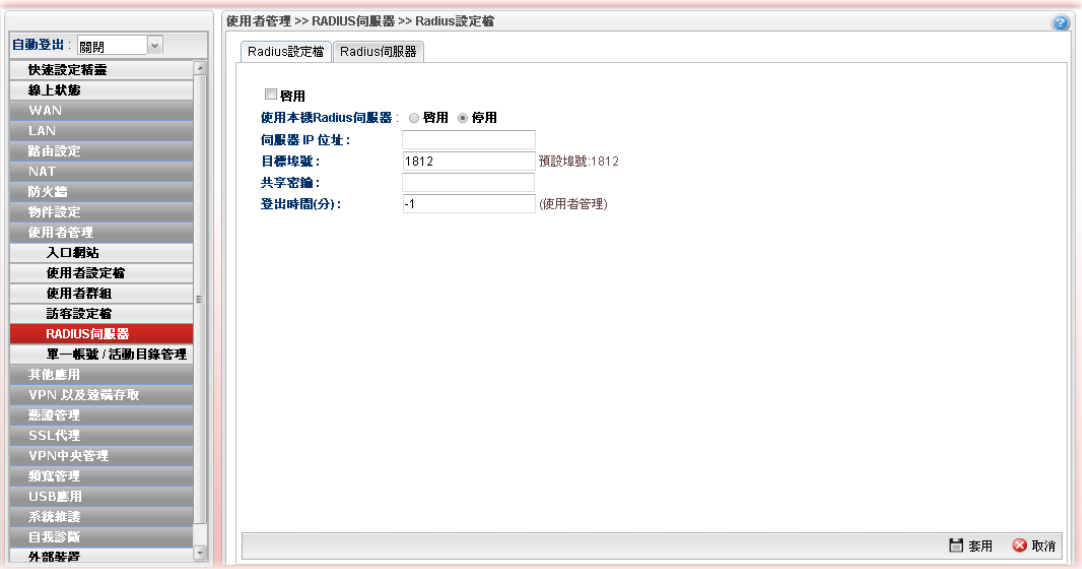
4.7.5 RADIUS 伺服器

撥接使用者遠端認證服務(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、授權和說明，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。

建立一個 RADIUS 用戶特徵設定，可以讓路由器協助遠端撥入用戶、無線工作站以及 RADIUS 伺服器能夠共同執行驗證的動作，它可集中遠端存取驗證工作以達成網路管理。

4.7.5.1 Radius 設定檔

Vigor 路由器可以指定一個外部的 RADIUS 伺服器執行安全性驗證的作業需求。



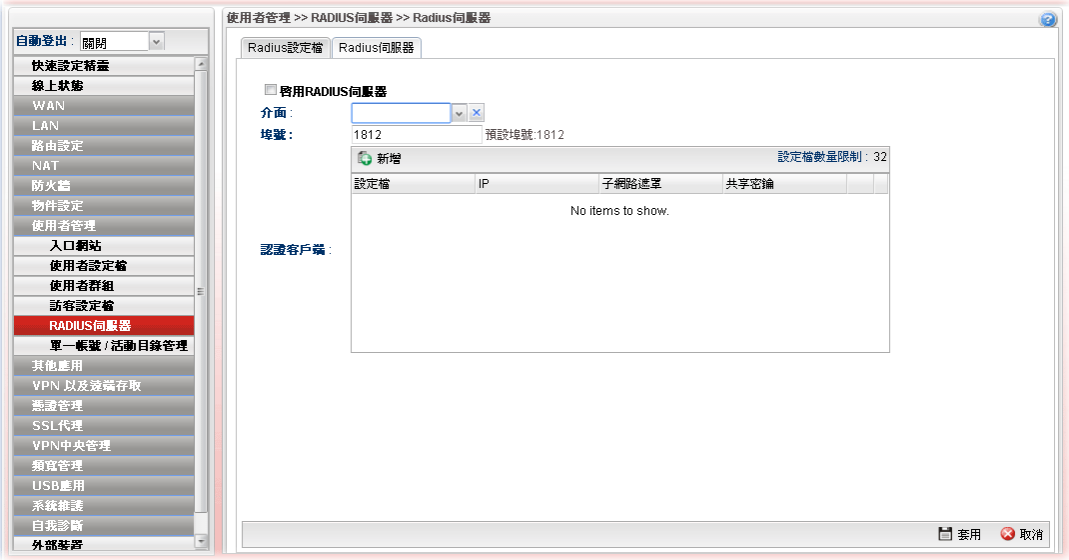
可用參數詳列如下：

項目	說明
啓用	勾選此框啓用此設定。
使用本機 Radius 伺服器	按**啓用**鈕以便啓用本機的 Radius 伺服器作為驗證伺服器。
伺服器 IP 位址	輸入 RADIUS 伺服器的 IP 位址。
目標埠號	輸入 RADIUS 伺服器所使用的 UDP 通訊埠號，基於 RFC 2138，預設值為 1812。
共用密鑰	RADIUS 伺服器和用戶共用一個用來驗證二者之間傳遞訊息的密鑰，雙方都必須設定相同的共用密鑰。
登出時間(分)	表示 RADIUS 驗證的最大使用期間。
套用	按此鈕儲存設定。
取消	按此鈕捨棄頁面設定。

完成設定後，按下**套用**儲存設定。

4.7.5.2 Radius 伺服器

.除了指定外部 RADIUS 伺服器進行安全性驗證之外，Vigor 路由器本身也可以被視爲 RADIUS 伺服器，提供 RADIUS 服務以對指定的用戶進行安全驗證。



可用參數詳列如下：

項目	說明
啓用 RADIUS 伺服器	勾選此框啓讓 Vigor 路由器可作爲內部 RADIUS 伺服器。
介面	只有透過此介面進出的用戶可以透過 Vigor 路由器內部的 RADIUS 伺服器進行驗證。
埠號	用戶可以使用指定的埠號進行 RADIUS 資訊交換。
認證客戶端	只有此區所指定的用戶可以透過 Vigor 路由器內部的 RADIUS 伺服器進行驗證。
套用	按此鈕儲存設定。
取消	按此鈕捨棄頁面設定。

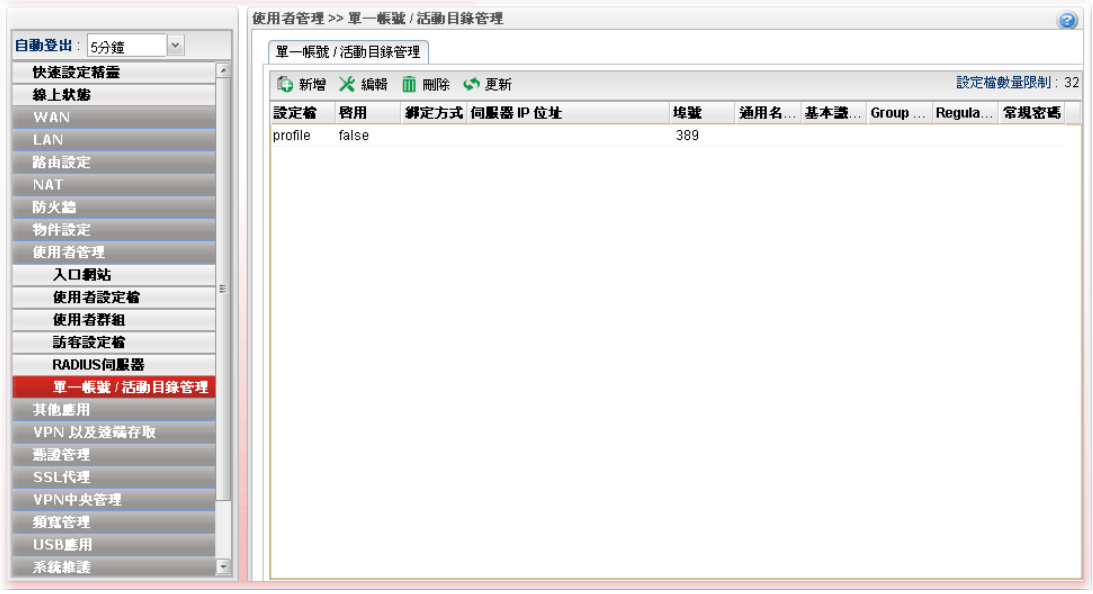
完成設定後，按下**套用**儲存設定。

附註：在**使用者管理>>使用者設定檔**的設定頁面中，提供啓用“**允許 Radius 伺服器登入**”的功能，讓使用者透過 Vigor 路由器自身的 RADIUS 伺服器進行帳號密碼認證。

4.7.6 單一帳號/活動目錄管理(LDAP/Active Directory)

LDAP (Lightweight Directory Access Protocol)是運用 TCP/IP 網路的共用協定，它可定義用戶端存取分享目錄伺服器的方法，在目錄上工作以及共享目錄內的資訊。LDAP 標準是由國際網路工程研究團隊(IETF)所建立。

LDAP 的設計就是成爲一個存取目錄伺服器最有效的方式，而無其他目錄伺服器協定複雜特性。因爲 LDAP 被定義爲可在目錄內安全地執行、查詢及修改資訊，因此使用者可套用 LDAP 來搜尋或是條列目錄物件，查詢或是管理運作中的目錄。



可用參數詳列如下：

項目	說明
新增	新增新的設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
刪除	移除選定的設定檔。 請選擇您想要刪除的既有設定檔，然後按下刪除按鈕，該設定檔即可被移除。
更新	重新更新本頁面。
設定檔數量限制	顯示可以建立的設定檔總數。
設定檔	顯示設定檔的檔名。
啓用	顯示設定檔狀態，False 表示停用；True 表示啓用。
綁定方式	顯示此設定檔的綁定類型爲何。
伺服器 IP 位址	顯示 LDAP 伺服器的 IP 位址。
埠號	顯示此設定檔使用的通訊埠號。
通用名稱標示符 (Common Name Identifier)	顯示辨識用的名稱。
基本識別名稱(Base DN)	顯示當綁定類型選擇簡易模式時所設定的 Base DN 值。
Group DN	顯示當綁定類型選擇簡易模式時所設定的群組 DN 值。
Regular DN	顯示當綁定模式選擇 Regular 模式時所設定的 Regular DN 值。

項目	說明
常規密碼(Regular Password)	顯示當綁定模式選擇 Regular 模式時所設定的 Regular 密碼。

如何新增設定檔

1. 開啓**使用者管理>>單一帳號/活動目錄管理**。
2. 按下**新增**按鈕。
3. 下述頁面將會出現。

可用參數詳列如下：

項目	說明
設定檔	輸入設定檔名稱。
啓用	勾選此框啓用此設定檔。
綁定方式	系統支援如下類型： **簡易模式** – 不用進行任何搜尋動作，直接綁定驗證。 **匿名模式** – 先以匿名帳號執行搜尋動作，再進行綁定驗證。 **正規模式** – 大部分皆與匿名模式相同，不同之處再於伺服器將會先檢查是否具備搜尋權限。 在 Regular 模式下，您還必須輸入 **Regular DN** 與**常規密碼**等資料。
伺服器 IP 位址	輸入 LDAP 伺服器的 IP 位址。
埠號	輸入埠號值作爲 LDAP 伺服器的目標埠號。

通用名稱標示符 (Common Name Identifier)	輸入或是編輯 LDAP 伺服器的名稱識別碼，通用名稱爲 cn。
基本識別名稱(Base DN)	爲“**Base Distinguished Name**”的縮寫，請在此輸入易於分辨的名稱，以便在 LDAP 伺服器上便於搜尋。
Group DN	爲“**Group Distinguished Name**” 的縮寫，. 請在此輸入易於分辨的名稱，以便在 LDAP 伺服器上便於搜尋。
Regular DN	如果**正規模式**被選爲綁定類型，請在此輸入相關資訊。
常規密碼	如果**正規模式**被選爲綁定類型，請指定一個密碼。
登出時間(分)	表示驗證的最大使用期間。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

4. 輸入所有設定並按下**套用**儲存。
5. 新 LADP/Active Directory 設定檔已經建立完成。

4.8 其他應用

下圖顯示**其他應用**的功能項目：

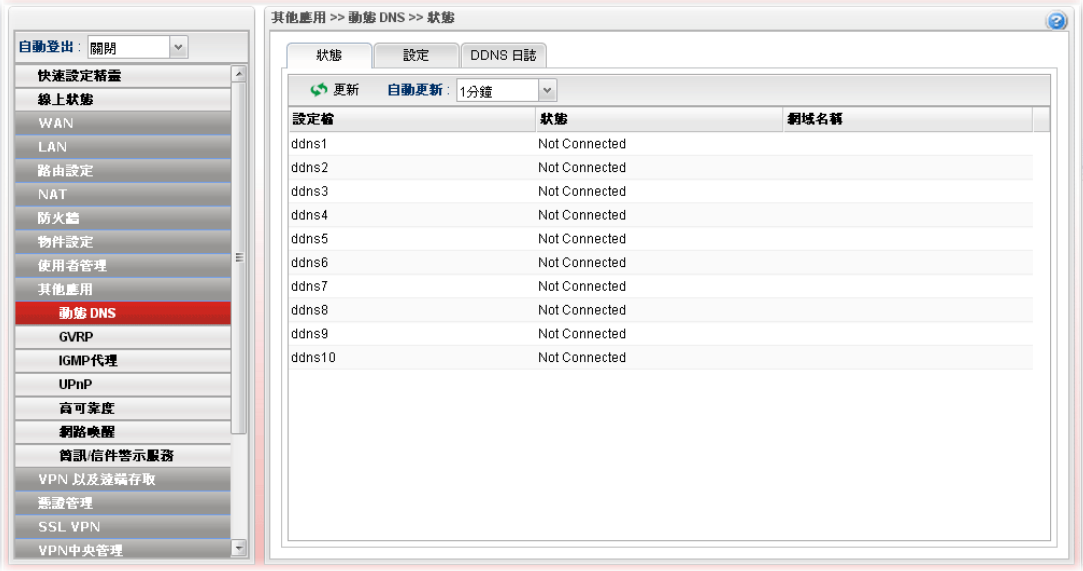
4.8.1 動態 DNS

當您透過 ISP 業者嘗試連接到網際網路時，ISP 業者提供的經常是一個浮動 IP 位址，這表示指派給您的路由器使用之真實 IP 位址每次都會有所不同，DDNS 可讓您指派一個網域名稱給予浮動廣域網路 IP 位址。它允許路由器線上更新廣域網路 IP 位址，以便對應至特定的 DDNS 伺服器上。一旦路由器連上網路，您將能夠使用註冊的網域名稱，並利用網際網路存取路由器或是內部虛擬的伺服器資料。如果您的主機擁有網路伺服器、FTP 伺服器或是其他路由器後方提供的伺服器，這項設定就特別有幫助也有意義。

在您使用 DDNS 時，您必須先向 DDNS 服務供應商要求免費的 DDNS 服務，路由器提供分別來自不同DDNS服務供應商的三種帳號。基本上，Vigor路由器和大多數的DDNS服務供應商 **www.dyndns.org, www.no-ip.com**、**www.dtdns.com**、**www.changeip.com**、**www.dynamic-nameserver.com** 像是都能相容，您應該先造訪其網站爲您的路由器註冊自己的網域名稱。

4.8.1.1 狀態

本頁顯示所有可用的 DDNS 設定檔的使用狀態。

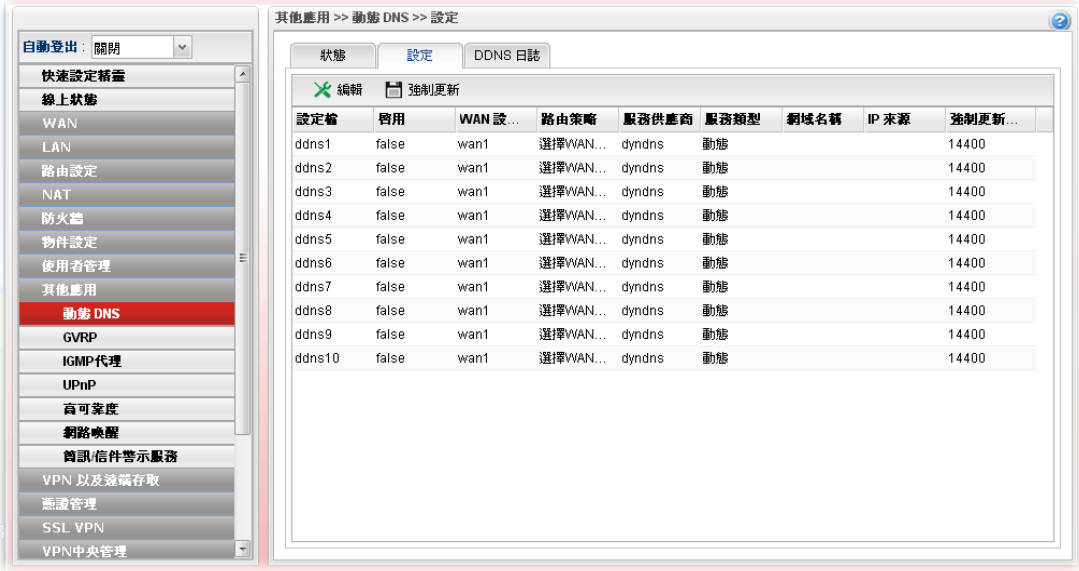


每個項目說明如下：

項目	說明
更新	重新更新本頁面。
自動更新	指定更新時間間隔以取得最新的狀態，若您按下**頁面更新**按鈕，系統將立即更新資訊並呈現出來。
設定檔	顯示 DDNS 設定檔名稱。
狀態	顯示 DDNS 伺服器的連線狀態。
網域名稱	顯示 DDNS 伺服器的網域名稱。

4.8.1.2 設定

本頁允許您設定符合您需求的 DDNS 設定檔。



每個項目說明如下：

項目	說明
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
強制更新	強迫路由器立即更新 DDNS 伺服器的最新資訊。
設定檔	顯示設定檔的檔名。
啓用	顯示設定檔狀態，False 表示停用；True 表示啓用。
WAN 設定檔	顯示 DDNS 設定檔目前使用的 WAN 介面設定檔。
路由策略	顯示 DDNS 設定檔目前使用的路由策略爲何。
服務供應商	顯示此設定檔使用的服務供應商名稱。
服務類型	顯示此設定檔的類型。
網域名稱	顯示此設定檔的網域名稱。
IP 來源	顯示此 DDNS 設定檔選擇的介面(My WAN IP 或是 My Internet IP)。
強制更新間隔	顯示此設定檔資料更新的間隔設定內容。

如何新增 DDNS 設定檔

有 10 組 DDNS 伺服器設定檔提供給您修改及設定，請選擇任一設定檔並按下**編輯**，即可開啓如下頁面進行修正：

1. 開啓**其他應用>>動態 DNS** 並按下**設定**標籤。

2. 選擇任何一個 DDNS 設定檔後，按下**編輯**按鈕。

可用參數詳列如下：

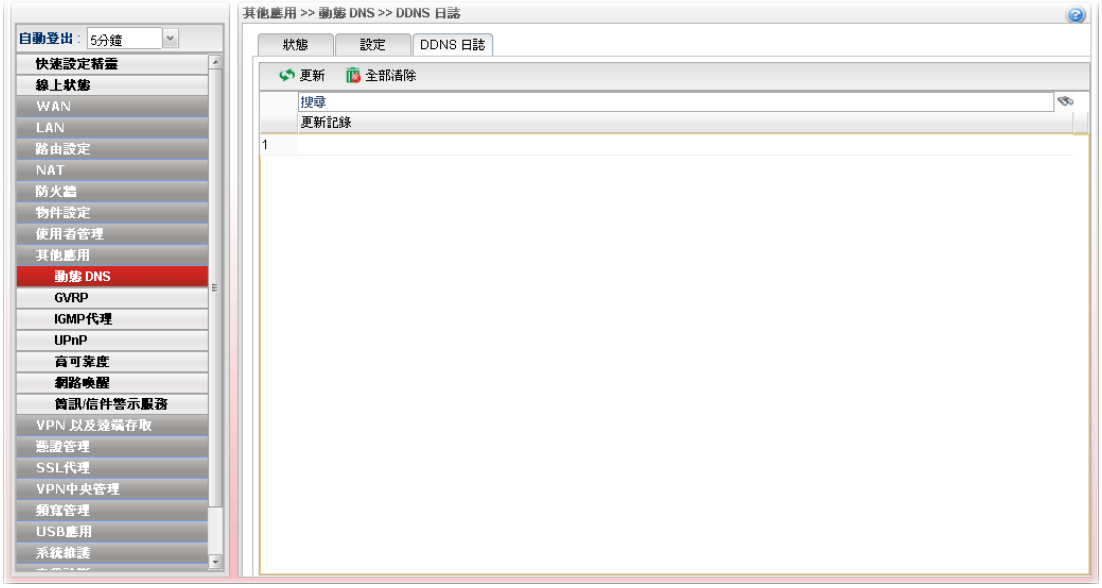
項目	說明
設定檔	顯示設定檔的檔名。
啓用	勾選此框啓用此設定檔。
WAN 設定檔	選擇 WAN 介面以便套用此設定檔。
路由策略	選擇套用至 DDNS 設定檔的路由策略： **選擇 WAN 優先** – DDNS 設定檔將先透過 WAN 介面進行資料傳輸，然後才以其他的介面來傳輸資料。 **僅選擇 WAN** –DDNS 設定檔僅透過 WAN 介面進行資料傳輸，不再透過其他介面運作。
服務供應商	選擇適當的服務供應商。
服務類型	選擇一種服務類型(動態、固定或是客製化)，如果您選的是客製，您可以修改網域內容。
網域名稱	輸入您先前套用的網域名稱。
使用者登錄名稱	輸入用來套用網域所需的登入名稱。

密碼	輸入用來套用網域所需的密碼。
IP 來源	選擇我的 WAN IP 或是 My Internet IP 作爲 DDNS 設定檔的來源 IP。
萬用字元與備份 MX	通用字符與備份 MX 功能並未所有的 DDNS 供應商都有支援，您可自供應商的相關網站取得更多的資訊。
郵件延伸程式	輸入郵件伺服器的 IP 位址/網域名稱。
強制更新間隔	設定一段時間讓路由器自動更新 DDNS 服務。
清除	還原爲預設值。
強制更新	強迫更新此設定檔。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

3. 輸入所有設定並按下**套用**儲存。
4. 新 DDNS 定檔已經建立完成。

4.8.1.3 DDNS 日誌

本頁顯示有關 DDNS 的資訊。



4.8.2 GVRP

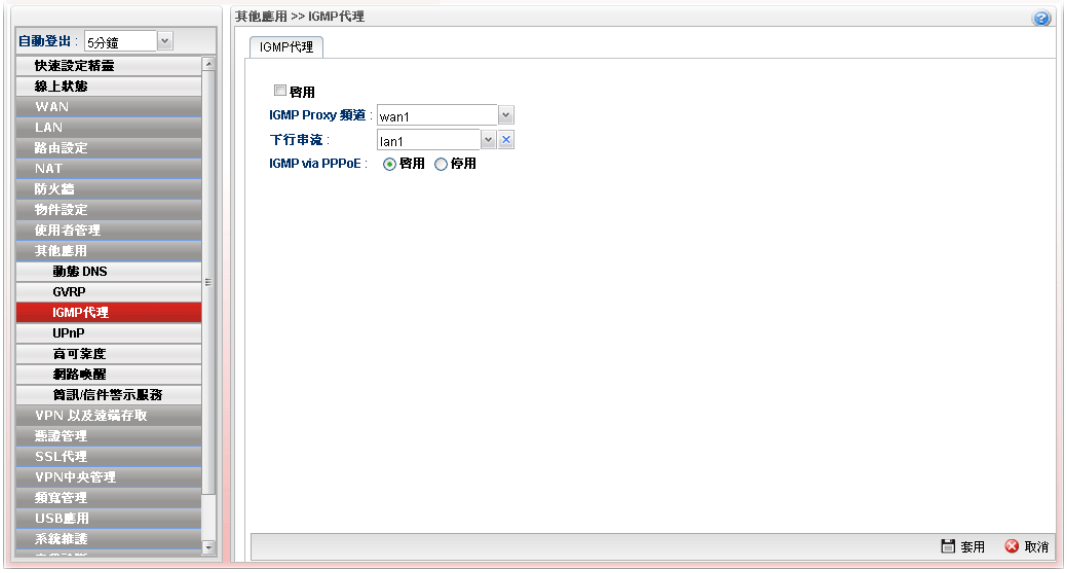
這項功能可以定義變更裝置間 VLAN 等資訊的方法，有了 GVRP，路由器可以接收來自其他裝置的 VLAN 資訊。

可用參數詳列如下：

項目	說明
啓用	勾選此框啓用此功能。
介面	選擇 LAN 與/或 WAN 設定檔。 如欲清除選定的項目，請按 ✕ 即可移除選定內容。t
加入時間	定義系統傳送 GVRP 封包到其他裝置的時間，單位是秒。
套用	按此鈕儲存設定。
取消	按此鈕捨棄頁面設定。

4.8.3 IGMP 代理

IGMP 爲 *Internet Group Management Protocol* 的縮寫，主要是用來管理網際網路協定多重播送群組會員數目的一種協定。

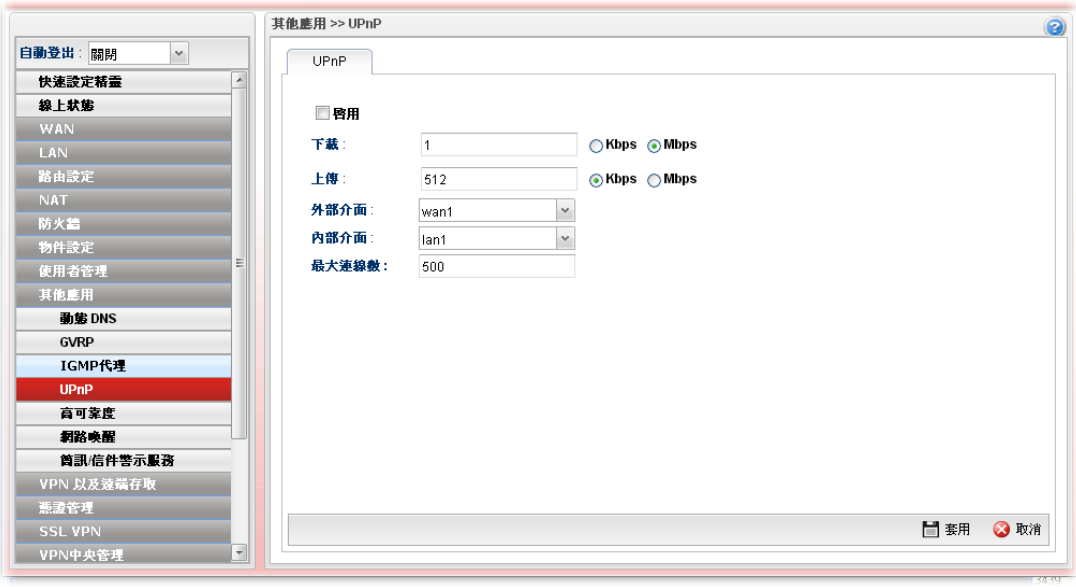


可用參數詳列如下：

項目	說明
啓用	勾選此框啓用此功能。
IGMP Proxy 頻道	多重播送的應用透過 WAN 埠來執行，另外，此功能在 NAT 模式下始可作用。
下行串流	使用下拉式清單選擇 LAN 設定檔作爲資料由 WAN 介面流往的目的地。
IGMP via PPPoE	啓用 – 在 LAN 端，使用 PPPoE 撥入路由器的電腦可收到 IGMP Proxy 的封包。 停用 – 在 LAN 端，使用 PPPoE 撥入路由器的電腦無法收到 IGMP Proxy 的封包。 ● **IGMP Interface IP** – 輸入 IGMP 伺服器 IP 位址。
套用	按此鈕儲存設定。
取消	按此鈕捨棄頁面設定。

4.8.4 UPnP

UPnP 協定爲網路連線裝置提供一個簡易安裝和設定介面，爲 Windows 隨插即用系統上的電腦週邊設備提供一個直接連線的方式。使用者不需要手動設定**通訊埠對應**或是 **DMZ**，**UPnP** 只在 Windows XP 系統下可以運作，路由器提供相關的支援服務給 MSN Messenger，允許完整使用聲音、影像和訊息特徵。



可用參數詳列如下：

項目	說明
啓用	勾選此框啓用此功能。
下載	輸入最大的 WAN 持續下載速度，此項資訊某些 UPnP 用戶會要求提供。
上傳	輸入最大的 WAN 持續上傳速度，此項資訊某些 UPnP 用戶會要求提供。
外部介面	選擇 UPnP 協定所需的 WAN 設定檔。
內部介面	選擇 UPnP 協定所需的 LAN 設定檔。
最大連線數	決定 UPnP 功能需求的最大連線數。
套用	按此鈕儲存設定。
取消	按此鈕捨棄頁面設定。

有關防火牆與 UPnP 功能之提示–

無法與防火牆軟體配合

在您的電腦上啓用防火牆有可能造成 UPnP 不正常運作，這是因爲這些應用程式會擋掉某些網路通訊埠的存取能力。

安全考量

在您的網路上啓用 UPnP 功能可能會招致安全威脅，在您啓用 UPnP 功能之前您應該要小心考慮這些風險。

- 某些微軟操作系統已發現到 UPnP 的缺點，因此您需要確定已經應用最新的服務封包。
- 未享有特權的使用者可以控制某些路由器的功能，像是移除和新增通訊埠對應等。

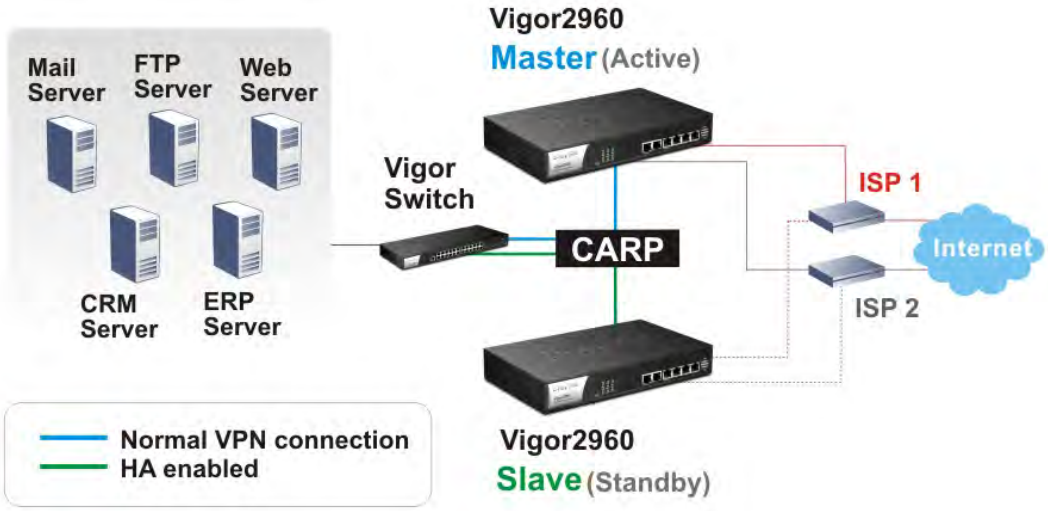
UPnP 功能可不斷變化的新增通訊埠對應來表示一些察覺 UPnP 的應用程式，當這些應用程式不正常的運作中止時，這些對應可能無法移除。

4.8.5 高可靠度

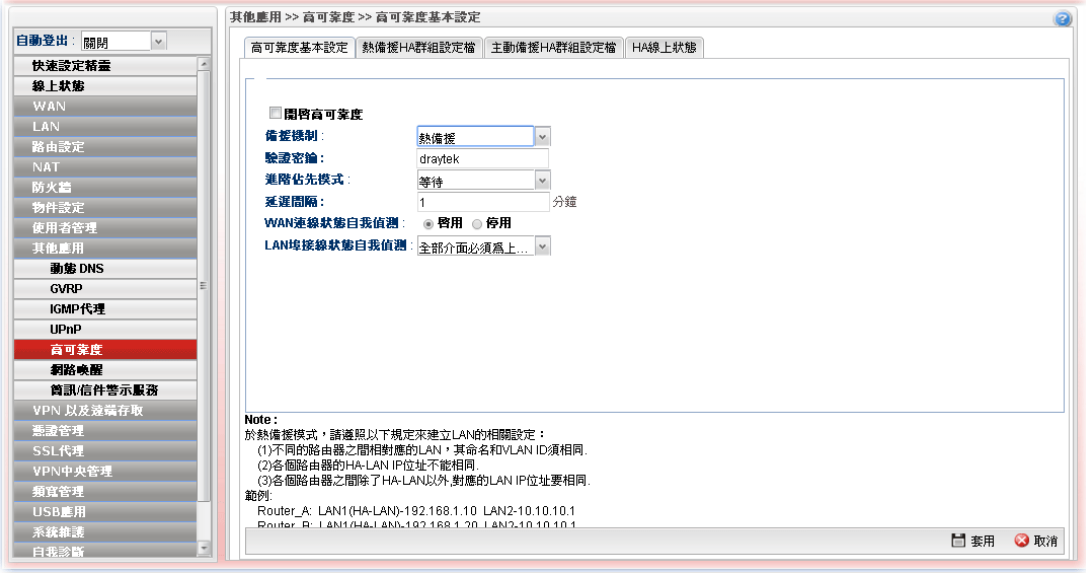
高可靠度(HA)與察覺組件故障與備份資源可用性有關，HA 的複雜度由可用性需求和系統中斷的容忍度來決定，通常，提供全時可靠度的系統，都具有即使系統失敗也還能運作的軟硬體。

Vigor2960 高可靠度功能其設計主要是用來避免單點故障，當故障發生時，失效元件(主裝置)所執行的處理過程將會移轉到備援元件(備援裝置)，這個過程可維持系統資源，恢復部分失效的處置，並在短暫的時間內將系統還原至正常狀態。

以下圖為例，左邊 Vigor2960 被視為主裝置，右邊的 Vigor2960 被視為次裝置。當主裝置發生故障，次裝置可以取代主裝置的角色，儘速接管所有的網路作業。但是一旦原本主裝置可以再次運作，次裝置就會變更回其原來的角色，維持在待機狀態。



4.8.5.1 高可靠度基本設定



可用參數詳列如下：

項目	說明
開啓高可靠度	勾選此框啓用 HA 功能。
備援機制	有二種方式可以選擇。 **熱備援**– 熱備援具有數個次要服務的節點，這些節點以另一個具有相同主要服務節點的備援角色存在運轉著，若主要節點發生故障，系統會立即從中挑選一個節點來接管所有的網路服務，在待機狀態下，次要節點即時複製主要節點的設定，如此一來整個系統就能確保以相同的設定來運行。 **主動備援** – 主備份也是一個冗餘方式，其下的 AP 分別設定不同的內容，以各自的 LAN 介面參與 HA 連線應用，由於爲一個主動閘道 LAN，在其他路由器處於等待的狀態時，會將使用者的資料以路由的方式傳輸出去。
熱備援下的設定	**驗證密鑰(** 輸入一字串作爲驗證密鑰，此密鑰用於加密 HA 連線數通訊以避免來自外部的惡意攻擊。 **進階佔先模式**– 指定模式以變更設定同步化角色(Config Synchronization Role)。 ● **立即** – 一旦服務還原，路由器將立刻回復主要路由器的位置。 ● **等待** – 當服務還原時，路由器必須等候一些時間才能回復其主要路由器的位置。 **延遲間隔** – 指定等待的時間。 ● **手動** – 依照**手動搶占存取**模式啓用或停用進行還原動作。 **手動搶占存取** – 選擇啓用或是停用。 **手動模式臨界點** – 設定一段時間，讓系統在偵測不出任何主裝置路由器存在時，能夠決定由哪個裝置替代

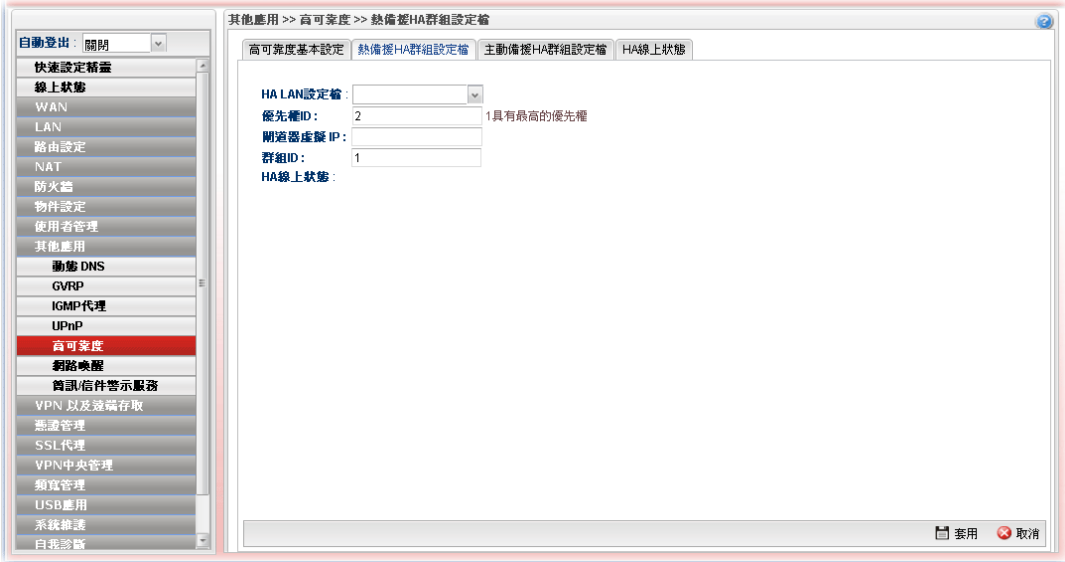
項目	說明
	成爲主裝置路由器。 如果路由器設定爲主要路由器，您又將手動先發狀態從啓用改成停用，一旦路由器偵測到停用狀態時，就會採取先發的模式，但如果沒有次要路由器可以接管此類服務，所有的資料傳送都將被迫中止。 爲了解決這個問題，可以採用二種方法來處理： 1. 重新設定**手動搶占存取**爲**啓用**，然後按**套用**儲存設定。 2. 設定**手動模式臨界點**，在經過該段設定的時間之後，如果系統仍偵測不出主裝置的存在，那麼**手動搶占存取**將會重新設定爲**啓用**以便找出主裝置路由器。 **WAN 連線狀態自我偵測** – 按下**啓用**讓路由器自動偵測 WAN 連線狀態，這個功能類似 LAN 埠口偵測模式，但是主要是偵測所有啓用的 WAN 設定檔的連線狀況，如果所有的連線狀態爲斷線，那麼主要裝置路由器將會退場。 **LAN 埠接線狀態自我偵測** – 如果 LAN 端有發生任何故障時，路由器(角色爲主要裝置)將會自動進行偵測事宜，這個功能將強迫主裝置路由器於偵測到 LAN 端故障時，轉由其他備援裝置進行，有二種方法用來決定 LAN 埠口的失敗狀況： ● **至少有一個介面爲上線狀態** – 只要有一個 LAN 埠連線時，主裝置路由器即可擁有其地位。 ● **全部介面必須爲上線狀態** – 主裝置路由器僅在所有的 LAN 埠都連線時，始可擁有其地位。
主動備援下的設定	**驗證密鑰**– 輸入一字串作爲驗證密鑰，此密鑰用於加密 HA 連線數通訊以避免來自外部的惡意攻擊。 **手動搶占存取** – 選擇啓用或是停用。 **手動模式臨界值** – 設定一段時間，讓系統在偵測不出任何主裝置路由器存在時，能夠決定由哪個裝置替代成爲主裝置路由器。 **WAN 連線狀態自我偵測**– 按下**啓用**讓路由器自動偵測 WAN 連線狀態，這個功能類似 LAN 埠口偵測模式，但是主要是偵測所有啓用的 WAN 設定檔的連線狀況，如果所有的連線狀態爲斷線，那麼主要裝置路由器將會退場。.

4.8.5.2 熱備援 HA 群組設定檔

熱備份(Hot-Standby)機制是指每個次要 AP 都可以是主要 AP(路由器)的備援裝置，當主要裝置失效的時候，其中一個次要裝置將被系統挑選成爲新的主要裝置。

當主裝置失效時，次要裝置中的其中一個會被系統挑選爲主裝置，以提供網路服務給予線上所有的電腦。

下述頁面用於建立熱備援設定檔。

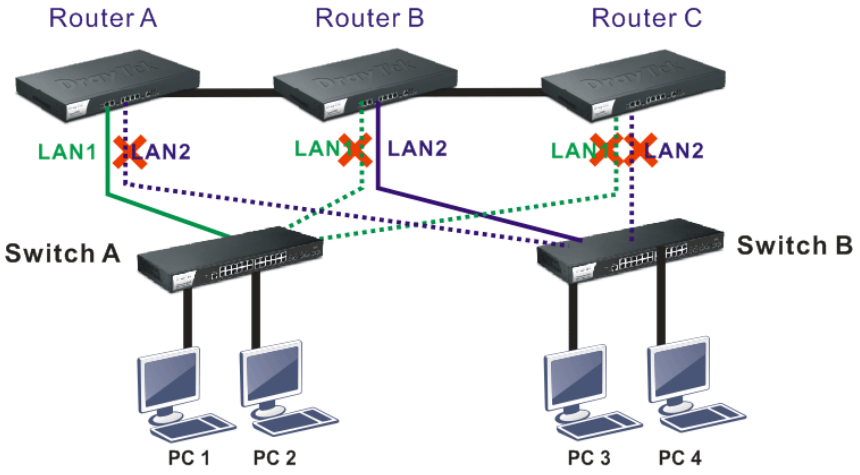


可用參數詳列如下：

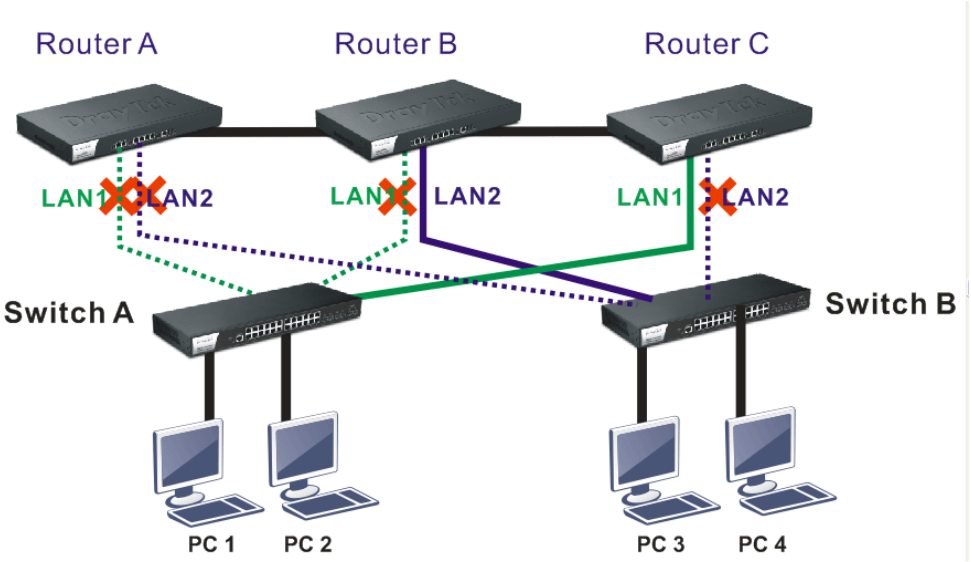
項目	說明
HA LAN 設定檔	選擇一個 LAN 設定檔以便在 HA 應用中溝通使用。
優先權 ID	“1” 具有最高權限，例如具有 1 之優先權的路由器在 HA 運用中被視爲主裝置。
閘道器虛擬 IP	指定任何一組 IP 位址做爲虛擬 IP。
群組 ID	輸入任一數值以便在 HA 運用中辨識。 在特定 HA 運用下所有的路由器都必須設定成相同的群組 ID 值，不同的 HA 運用擁有不同的群組 ID 值。
HA 線上狀態	顯示此路由器在 HA 運用中的狀態身分(主要或備援)。
套用	按此鈕儲存設定。
取消	按此鈕捨棄本頁設定。

4.8.5.3 主動備援機制

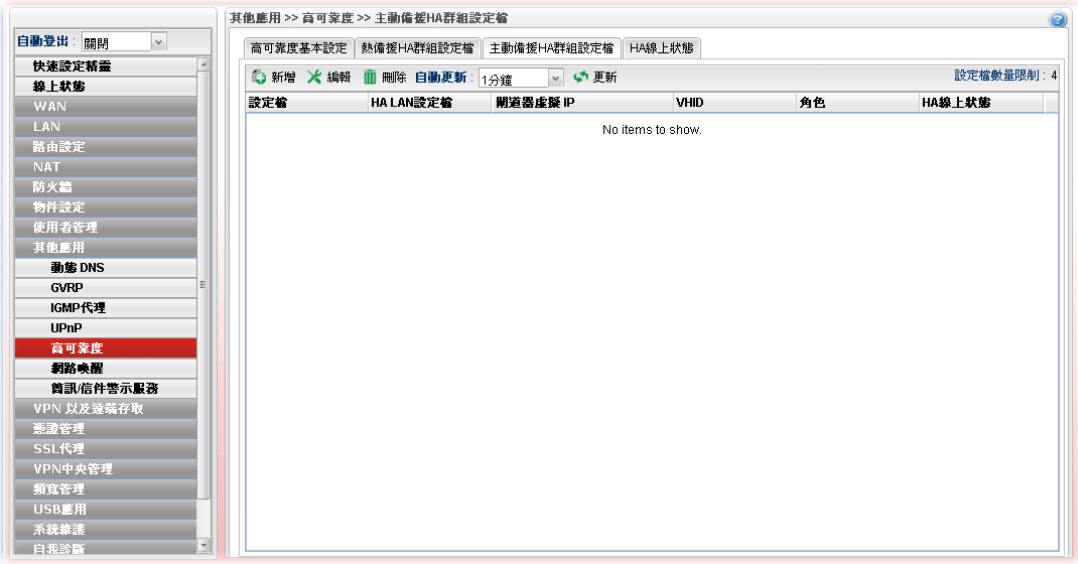
主動備援機制是指 LAN 中每個 AP 皆以不同的高可靠度連線數參與網路連線，所以的 WAN 介面都可以是主動的，提供更具彈性的網路服務應用。



當路由器 A 中的 LAN 1 失效時，任何一個有效的連線(例如路由器 C 中的 LAN 1)將被系統選擇以提供網路服務給予線上所有的電腦。



下述頁面用於建立主動備援備份設定檔。



可用參數詳列如下：

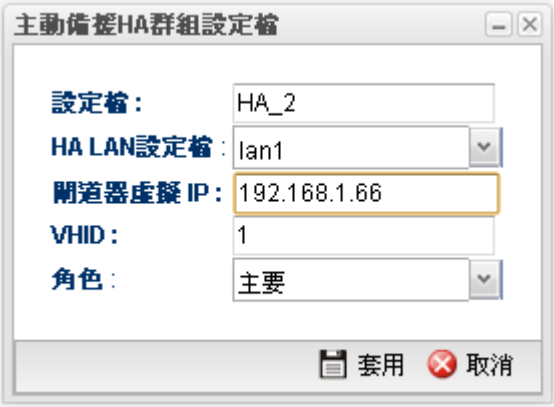
項目	說明
新增	新增新的配置量設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
刪除	移除選定的設定檔。 請選擇您想要刪除的既有設定檔，然後按下刪除按鈕，該設定檔即可被移除。
自動更新	指定更新時間間隔以取得最新的狀態，若您按下**頁面更新**按鈕，系統將立即更新資訊並呈現出來。
更新	重新更新本頁面。
設定檔數量限制	顯示可以建立的設定檔總數。
設定檔	顯示 HA 設定檔的名稱。
HA LAN 設定檔	顯示此 HA 使用的 LAN 設定檔。
閘道器虛擬 IP	顯示閘道的 IP 位址。
VHID	顯示設定檔的虛擬主機 ID 號碼。
角色	顯示此設定檔在 HA 群組當中的角色是什麼。
HA 線上狀態	顯示此 HA 設定檔的線上狀態(主要、備援、LAN_failed、WAN_Failed 等等)。

如何新增主動備援備份設定檔

1. 開啓**其他應用>>高可靠度**並按下**主動備援 HA 群組設定檔**標籤。

2. 按下**新增**按鈕。

3. 下述頁面將會出現。



可用參數詳列如下：

項目	說明
設定檔	顯示設定檔的檔名。
HA LAN 設定檔	選擇準備套用此功能的 LAN 設定檔。
閘道器虛擬 IP	指定虛擬 IP 位址。
VHID	表示虛擬主機 ID，請輸入一個數值，VHID 用於備援路由器，以辨認出哪一個主要裝置需要備援。
角色	針對 HA 配置的 LAN 設定檔可獨立設定，且彼此之間不會互相干擾，因此路由器 A 的 LAN1(備份)可以是路由器 B(主要)LAN1 的備援；路由器 B 的 LAN2(備份)可以是路由器 A(主要)LAN2 的備援。 同一個路由器下設定的每個 HA LAN 設定檔，必須指定其角色爲主裝置或是備份裝置。
套用	按此鈕儲存設定。
取消	按此鈕捨棄頁面設定。

4. 輸入所有設定並按下**套用**儲存。

4.8.5.4 HA 線上狀態

可用參數詳列如下：

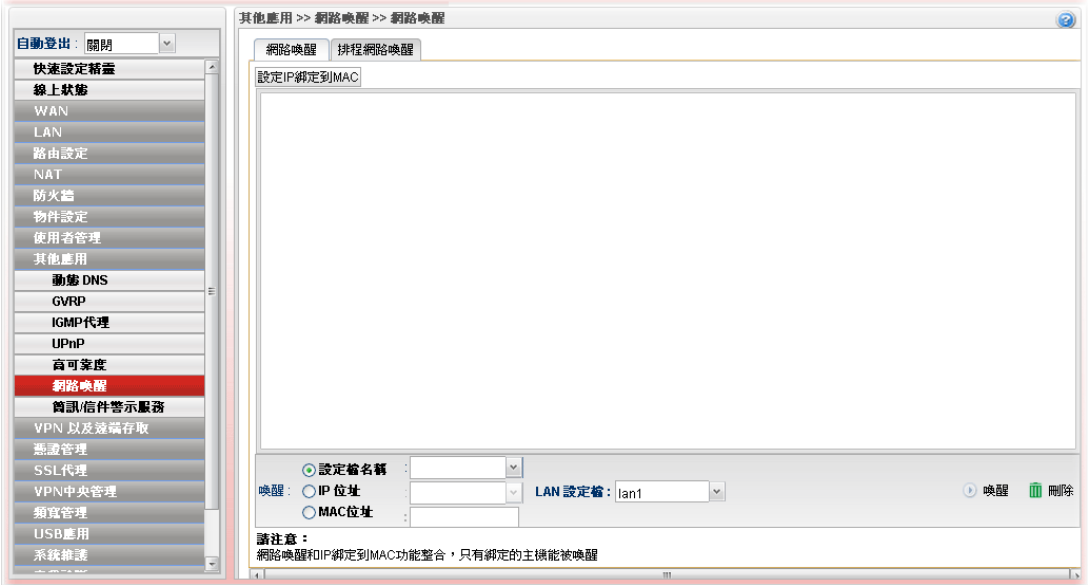
項目	說明
自動更新	指定更新時間間隔以取得最新的狀態，若您按下**頁面更新**按鈕，系統將立即更新資訊並呈現出來。
更新	重新更新本頁面。
群組 ID	顯示路由器的群組 ID 號碼。
優先權 ID	顯示 HA 運用中路由器的優先權限編號，號碼越低，優先權限越高，路由器若是具有最高的優先權，在 HA 運用中就會被視爲主裝置。
IP	顯示路由器的 IP 位址。
路由器名稱	顯示路由器的名稱。
備援機制	顯示 HA 運用中使用的方法(熱備援或是主動備援) 。
HA 線上狀態	顯示 HA 設定檔的線上使用狀態(主、備援、LAN_failed 與 WAN_Failed)。
詳細	此處若顯示圖示，即可用來開啓 HA 設定中的細節設定內容頁面。

4.8.6 網路喚醒

區域網路上的電腦可以透過所連結的路由器來喚醒，當使用者想要從路由器喚醒指定的電腦時，使用者必須在此頁面上輸入該電腦正確的 MAC 位址。

此外，此台電腦必須安裝有支援 WOL 功能的網卡，並在 BIOS 設定中開啓 WOL 功能。

4.8.6.1 網路喚醒



可用參數詳列如下：

項目	說明
設定綁定 IP 到 MAC	按此開啓綁定 IP 到 MAC 頁面。
喚醒方式	有三種方式提供給使用者喚醒綁定 IP 的電腦，如果您選擇由 MAC 位址來喚醒的話，您必須輸入該主機正確的 MAC 位址；如果您選擇的是由 IP 位址來喚醒的話，您必須選擇正確的 IP 位址。 **設定檔名稱** – 自下拉式清單中選擇一個設定檔(於 **LAN>>綁定 IP 到 MAC** 建立)。 **IP 位址** - 已在**防火牆>>綁定 IP 至 MAC** 中設定完成的 IP 位址，將會出現在下拉式清單中，請自清單中選取您想要喚醒的電腦 IP。 **MAC 位址** - 輸入被綁定之電腦的 MAC 位址。 **LAN 設定檔** – 使用下拉式清單選擇一個 LAN 設定檔。
喚醒	按此鈕可以喚醒選定的電腦，喚醒結果將會顯示在方框內。
刪除	按此鈕移除所有的設定。

4.8.6.1 排程網路喚醒

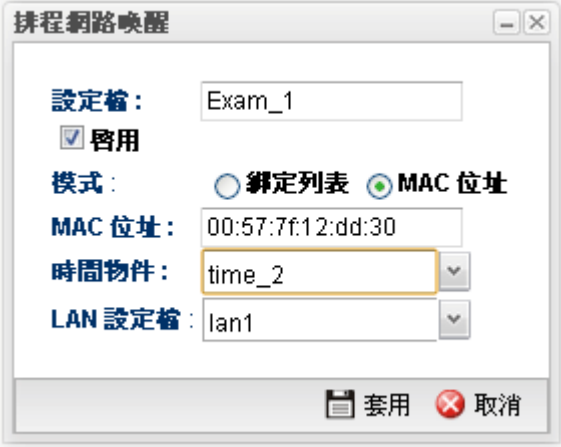
本頁可配置用來執行網路喚醒的設定檔，依照綁定列表、MAC 位址、LAN 設定檔以及時間物件等條件來進行。

可用參數詳列如下：

項目	說明
新增	新增設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
刪除	移除選定的設定檔。
更新	重新更新本頁面。
設定檔	顯示設定檔的名稱。
啓用	顯示設定檔的狀態(true 表示啓用/false 表示用)。
綁定列表	顯示自綁定列表選擇之設定檔名稱。
MAC 位址	顯示準備喚醒的電腦之 MAC 位址。
時間物件	顯示用於網路喚醒的時間物件。
LAN 設定檔	顯示 LAN 設定檔名。

如何新增網路喚醒需求之排程設定檔

1. 開啓**其他應用>>網路喚醒**並按下**排程網路喚醒**標籤。
2. 按下**新增**按鈕。
3. 下述頁面將會出現。



可用參數詳列如下：

項目	說明
設定檔	輸入此設定檔的名稱。
啓用	勾選此方塊啓用此設定檔。
模式	選擇輸入模式，**綁定列表**或是 **MAC 位址**。
綁定列表	自綁定列表中選擇一組設定檔。
MAC 位址	若選擇 **MAC 位址**爲模式設定，您必須在此欄位中輸入相關的 MAC 位址，之後即可透過遠端喚醒具此 MAC 位址的電腦。
時間物件	選擇時間物件，以便在指定的時間內喚醒電腦。時間物件設定檔可於**物件設定>>時間設定**中事先設定。
LAN 設定檔	選擇 LAN 設定檔，之後即可透過遠端喚醒此設定檔內的電腦。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

4. 輸入所有設定並按下**套用**儲存。

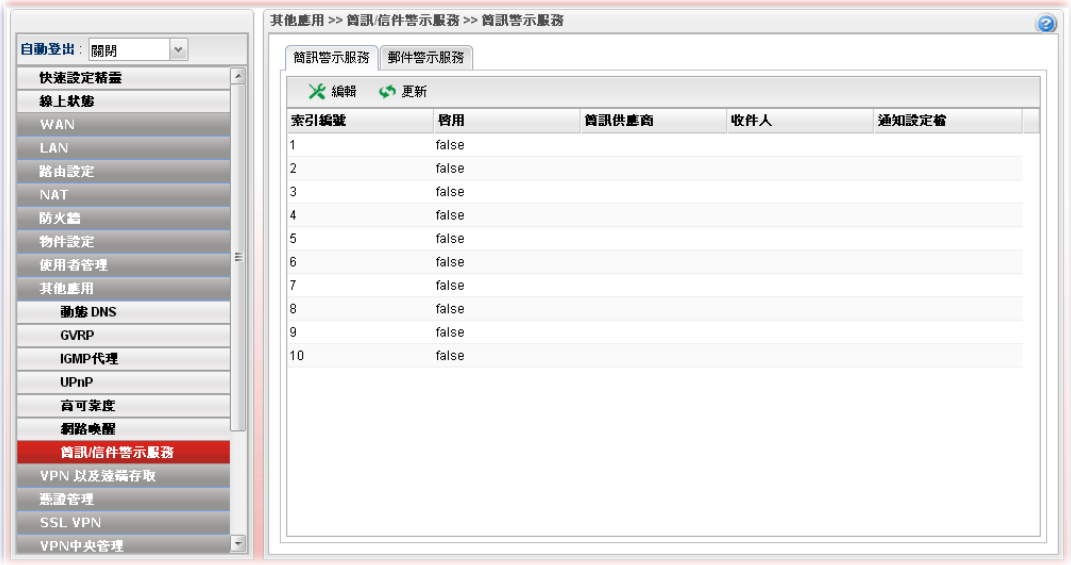
4.8.7 簡訊/郵件警示服務

簡訊/郵件警示功能是路由器透過指定的服務供應商，傳送訊息至使用者行動電話或是電子郵件信箱，幫助使用者即時了解異常現象。

Vigor 路由器可讓您設定 10 組簡訊設定檔，可依據不同條件發送出去。

4.8.7.1 簡訊服務供應商

本頁讓您指定簡訊服務供應商、收信人為何以及收信內容。



每個項目說明如下：

項目	說明
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
更新	重新更新本頁面。
索引編號	顯示設定檔的順序編號。
啓用	顯示設定檔狀態，False 表示停用；True 表示啓用。
簡訊供應商	顯示簡訊服務供應商名稱。
收件人	顯示誰會收到此封簡訊。
通知設定檔	顯示通知設定檔的檔名。

如何新增簡訊警示服務設定檔

1. 開啓**其他應用>>簡訊/郵件警示服務**再按下**簡訊警示服務**標籤。
2. 選擇任一個索引編號，按下**編輯**按鈕。
3. 下述頁面將會出現。

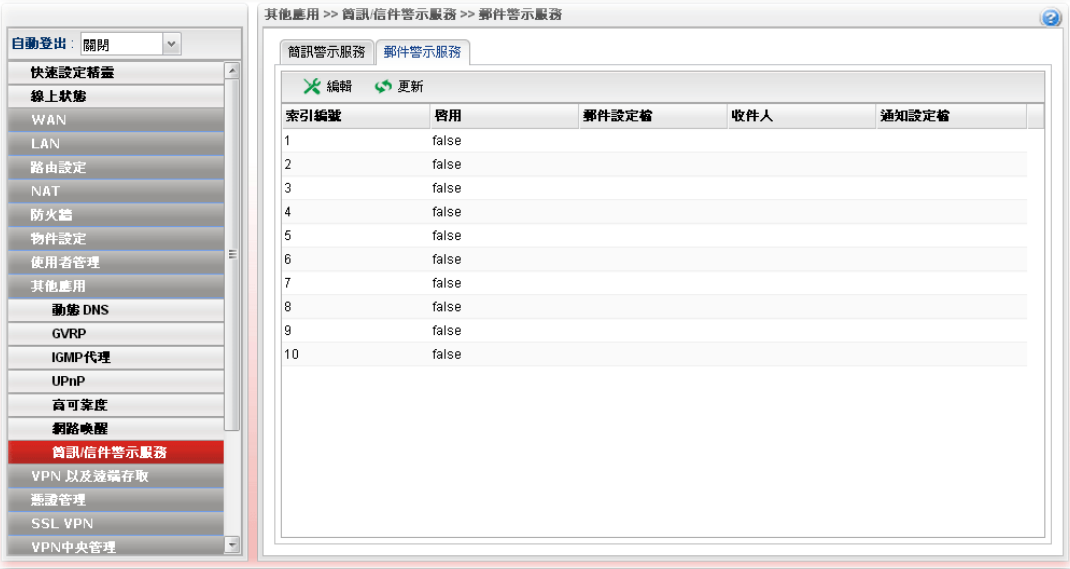
可用參數詳列如下：

項目	說明
啓用	勾選此框啓用此設定檔。
簡訊供應商	自下拉式清單中選擇您需要的簡訊服務供應商。 相關設定檔可在**物件設定>>簡訊服務物件**頁面中事先建立。
收件人	輸入接收此簡訊的電話號碼。
通知設定檔	自下拉式清單中選擇一個設定檔(指定發送簡訊的時機)。 相關設定檔可在**物件設定>>通知物件**頁面中事先建立。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

4. 輸入所有設定並按下**套用**儲存。
5. 新簡訊警示服務設定檔已經建立完成。

4.8.7.2 郵件警示服務

本頁允許您設定郵件伺服器，指明誰會獲得通知郵件，通知內容為何以及何時傳送訊息出去。

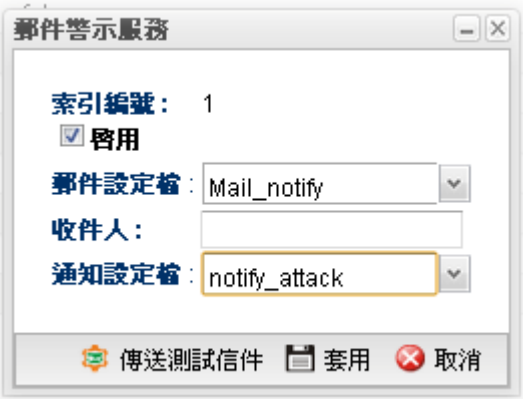


每個項目說明如下：

項目	說明
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
更新	重新更新本頁面。
索引編號	顯示設定檔的編號順序。
啓用	顯示設定檔狀態，False 表示停用；True 表示啓用。
郵件設定檔	顯示郵件設定檔的檔名。
收件人	顯示接收郵件警示的人員為何。
通知設定檔	顯示通知設定檔的名稱。

如何新增郵件警告服務設定檔

1. 開啓**其他應用>>簡訊/郵件警示服務**再按下**郵件警示服務**標籤。.
2. 選擇任一個索引編號，按下**編輯**按鈕。
3. 下述頁面將會出現。



可用參數詳列如下：

項目	說明
啓用	勾選此框啓用此設定檔。
郵件設定檔	自下拉式清單中選擇郵件服務物件設定檔。 相關設定檔可在**物件設定>>郵件服務物件**頁面中事先建立。
收件人	輸入接收此郵件的電子郵件地址。
通知設定檔	自下拉式清單中選擇一個設定檔(指定發送郵件的時機)。 相關設定檔可在**物件設定>>通知物件**頁面中事先建立。
傳送測試信件	按此鈕可以進行簡易的信件測試。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

4. 輸入所有設定並按下**套用**儲存。
5. 新郵件警示服務設定檔已經建立完成。

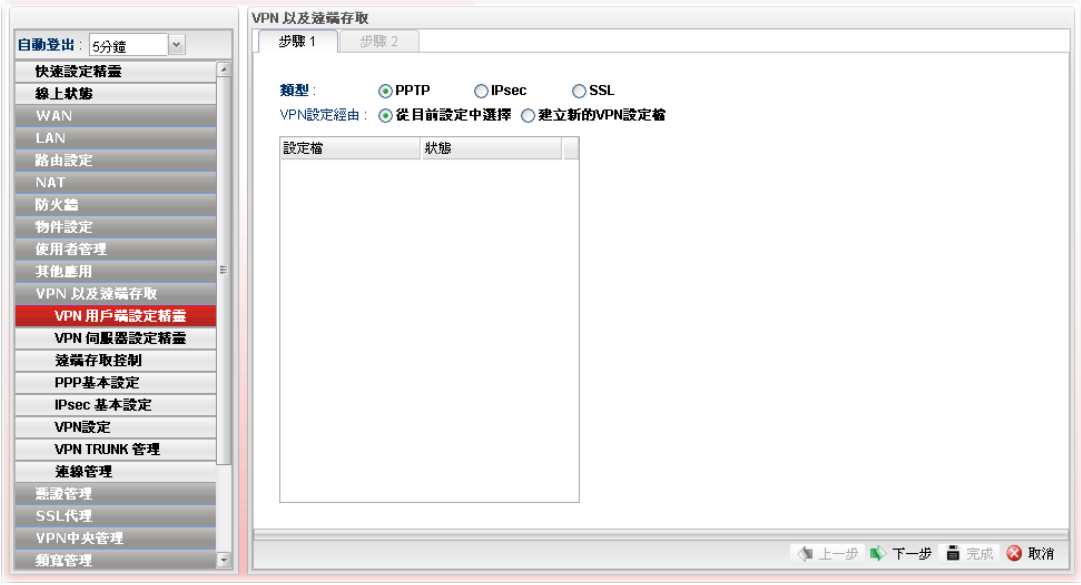
4.9 VPN 以及遠端存取

VPN 是 Virtual Private Network (虛擬私有網路) 的縮寫，是一種利用公眾網路建立一個虛擬的、安全的、方便的通道。企業可透過這個安全通道讓兩個不同地方的辦公室互通內部資料或讓出差在外的辦公人員可以遠端撥入 VPN 通道擷取公司內部的資料。

下圖為 VPN 與遠端存取的主要功能項目：

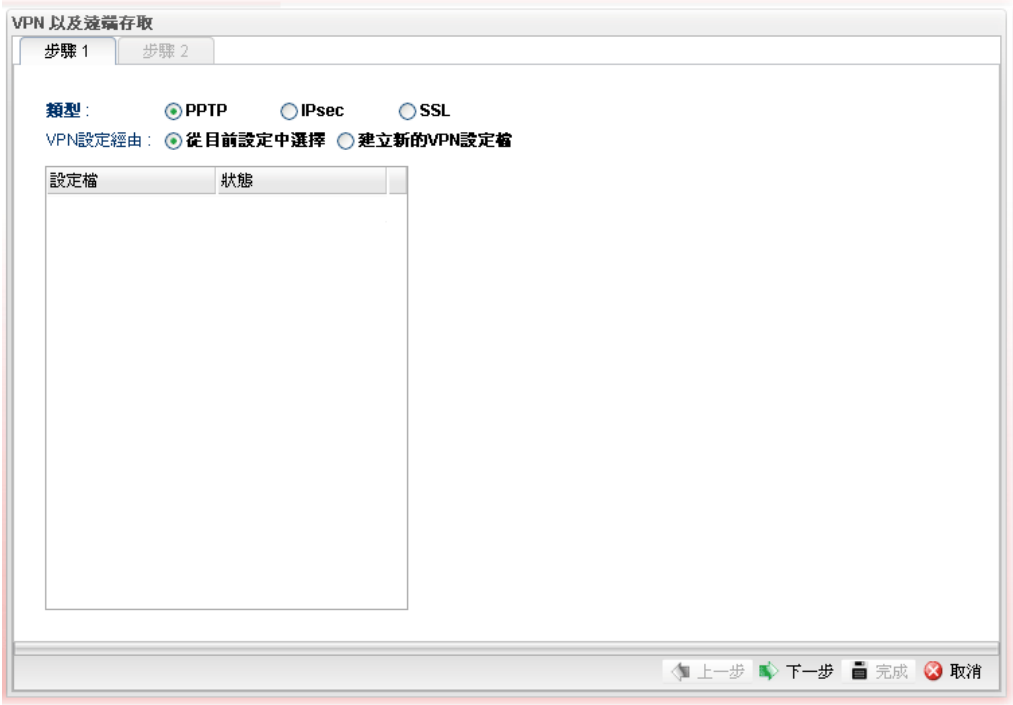
4.9.1 VPN 用戶端設定精靈

此精靈用來設定 VPN 用戶端所需的 VPN 設定，精靈將引導您一步步建立 VPN 撥出方向的 LAN-to-LAN 設定檔(從伺服器到用戶端)。



如何為 VPN 用戶端的建立 LAN-to-LAN(撥出)設定檔

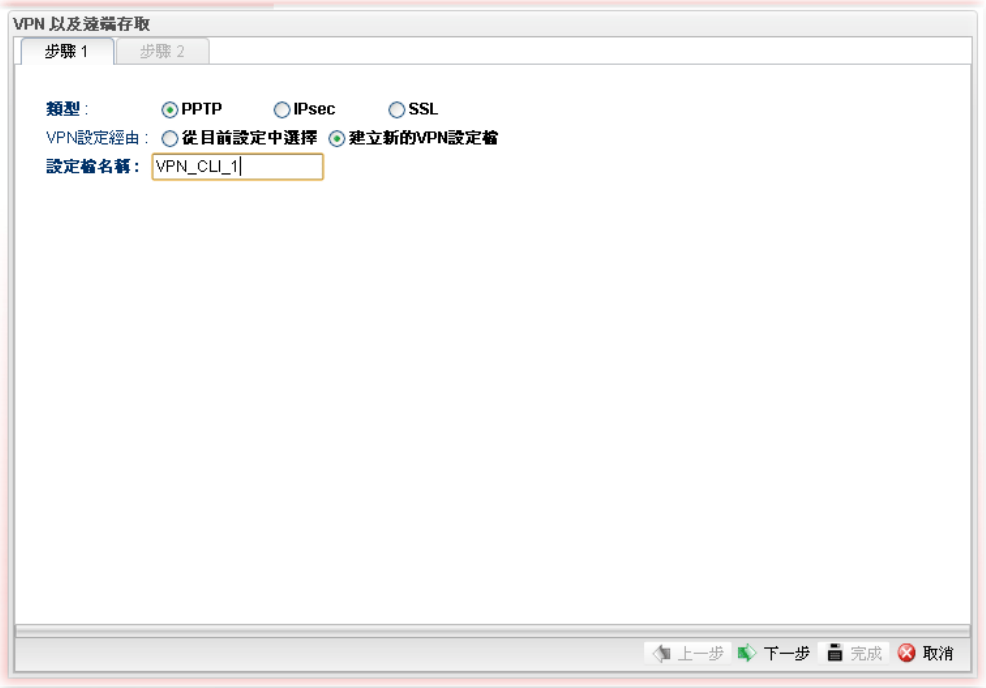
1. 開啓 **VPN 與遠端存取>>VPN 用戶端設定精靈**。
2. 下述頁面將會出現。



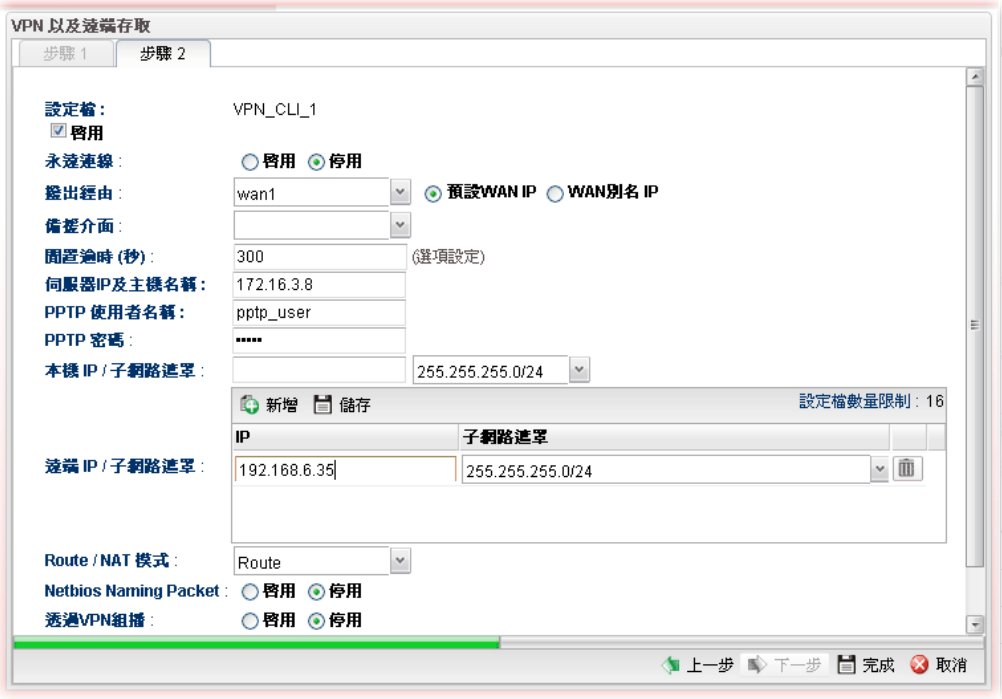
可用參數詳列如下：

項目	說明
類型	指定用於此 VPN 設定檔所需的協定類型(**PPTP / IPSec / SSL**)。
VPN 設定經由	**從目前設定中選擇** – 若您已經事先建立好 LAN to LAN 設定檔，那麼已建立的 VPN LAN to LAN 設定檔會詳列於下方，選擇您需要的設定檔。 **建立新的 VPN 設定檔** – 這個選項可讓您建立一個全新的 LAN to LAN 設定檔，可在設定檔名稱欄位中輸入檔名。

3. 選擇需求類型，按下**建立新的 VPN 設定檔**，然後輸入設定檔的檔名，接著按下**一步**。



4. 如果您選擇的是 **PPTP**，您將可看到如下頁面：

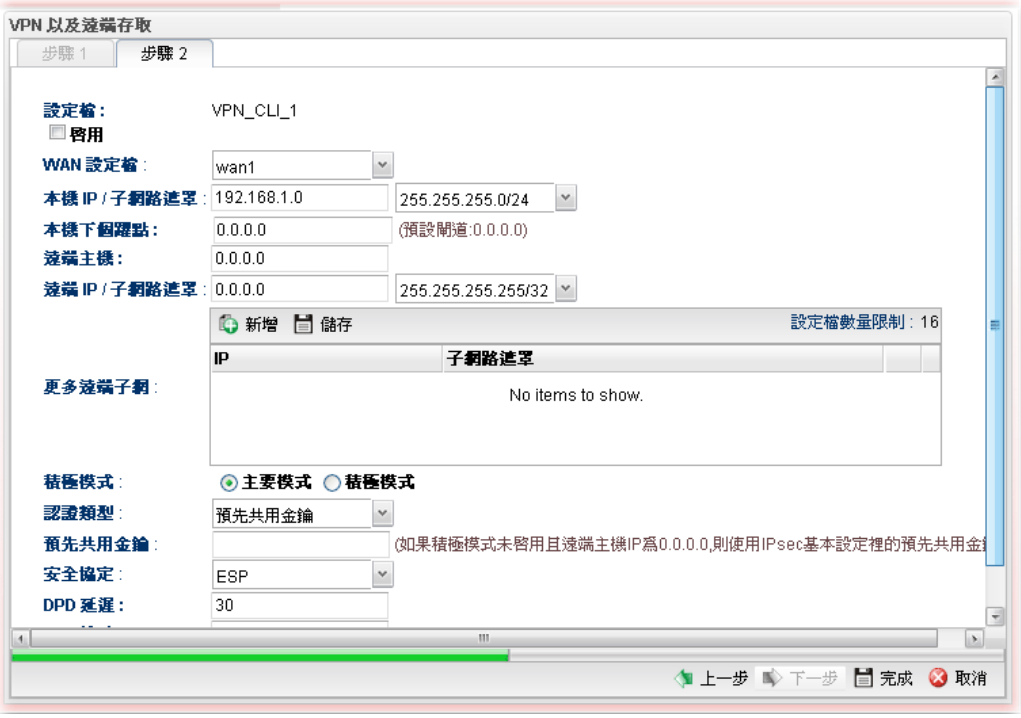


可用參數詳列如下：

項目	說明
設定檔	顯示 VPN 設定檔的檔名。
啓用	勾選此框啓用此設定檔。

永遠連線	選擇啓用讓路由器永遠保持連線狀態。
撥出經由	選擇 WAN 設定檔介面。選擇 WAN 設定檔介面。然後選擇預設 WAN IP (default WAN IP)或是指定 WAN 別名 IP (WAN Alias IP)用於 VPN 通道。
備援介面	選擇 WAN 設定檔，當選定的 WAN 介面發生故障時，系統能自動引導資料由其他 WAN 進出。
閒置逾時	當永遠連線停用時，您必須在此輸入終止網路連線的等待時間。
伺服器 IP/主機名稱	輸入 PPTP 伺服器的 IP 位址或是主機名稱。
PPTP 使用者名稱	輸入用以驗證 PPTP 連線的使用者名稱。
PPTP 密碼	輸入用以驗證 PPTP 連線的密碼。
本機 **IP**/子網路遮罩	輸入本機的 IP 位址與子網遮罩。
遠端 **IP**/子網路遮罩	輸入遠端主機的 IP 位址與子網遮罩。
Route/NAT 模式	指定此設定檔的目的。
Netbios Naming Packet (Netbios 命名封包**)**	啓用 – 按下此鈕可在連線時於 VPN 通道二端的主機之間提出資料傳送之要求。 停用 – 當連線時 VPN 通道二端的主機之間發生衝突，此功能將可阻擋通道內的 Netbios 命名封包的傳送作業。
透過 **VPN** 組播	某些程式可透過 VPN 連線進行多重播送封包。 ● 通過 –點選此鈕讓多重播送封包通過路由器。 ● 封鎖 – 此爲預設值。點選此鈕之後，路由器將會封鎖多重播送封包。
RIP via VPN	啓用 – 選此項以便透過 VPN 連線交換 RIP 封包。 停用 – 關閉此功能。停用爲預設值。

如果您選擇的是 **IPSec**，您將可看到如下頁面：

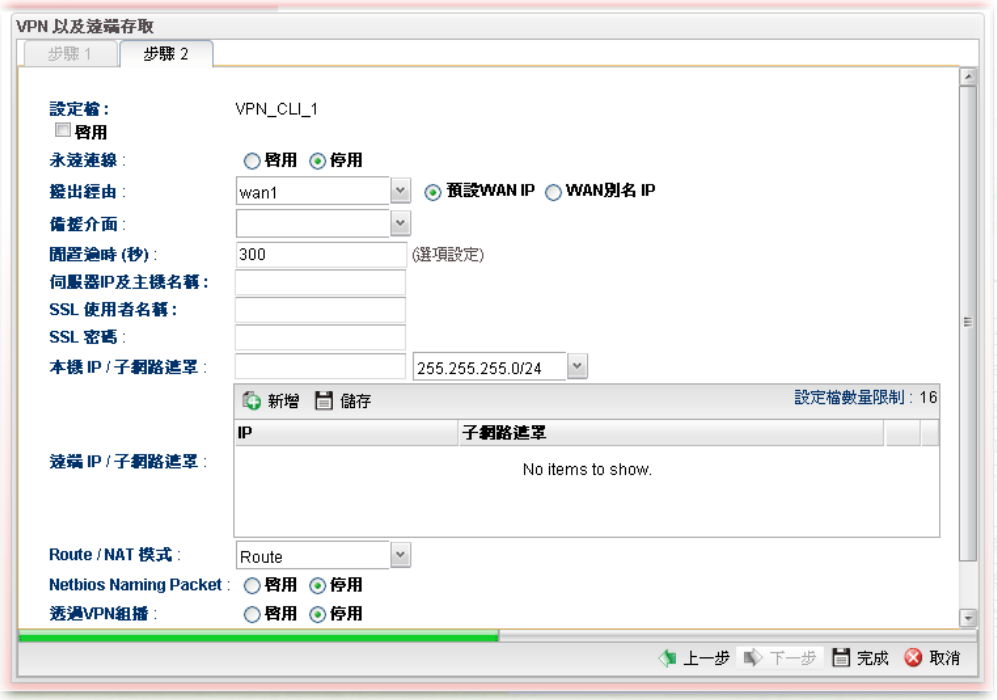


可用參數詳列如下：

項目	說明
設定檔	顯示 VPN 設定檔的檔名。
啓用	勾選此框啓用此設定檔。
WAN 設定檔	選擇用於此設定檔的 WAN 介面設定檔。
本機 **IP/**子網路遮罩	輸入本機的 IP 位址與子網遮罩。
區域下一節點	指定 WAN 介面的閘道，建議使用預設值即可 (維持空白)。
遠端主機	輸入遠端主機的 WAN IP 位址。
遠端 **IP/**子網路遮罩	輸入遠端主機的 IP 位址與子網遮罩。
更多遠端子網	如有必要可在本區增加更多的遠端子網。
認證類型	選擇用於 Pre-Shared Key 或是 RSA Signature 的驗證類型，可選 **PSK** 或是 **RSA**。
憑證	如果 RSA 被選定爲驗證類型，請再此利用下拉式清單選擇一個本機憑證。
預先共用金鑰	如果 PSK 被選定爲驗證類型，請在此輸入共享密鑰值。
安全協定	選擇 **ESP** 以便指定 IPsec 協定，所有的資料將被加密且須受到驗證。若要驗證表頭，則選擇 **AH** 以指定 IPsec 協定，資料將會受到驗證但不會被加密。
DPD 延遲	DPD 爲 dead peer detection 的縮寫，指的是對點狀態偵測，看看 VPN 另一端是否正常。因爲這是一個維持連線

	的計時裝置，因此當某條通道閒置時，系統會定期發出招呼訊息以維持連線運作，輸入 0 可關閉此功能，如果要啓用此功能，建議設定值爲 30 秒。
DPD 逾時	此爲逾時計時器，一旦逾時之後系統沒有收到任何來自 VPN 對方的應答訊息，則該方將被宣告已廢。輸入 0 可關閉此功能，如果要啓用此功能，建議設定值爲 120 秒。

如果您選擇的是 **SSL**，您將可看到如下頁面：



可用參數詳列如下：

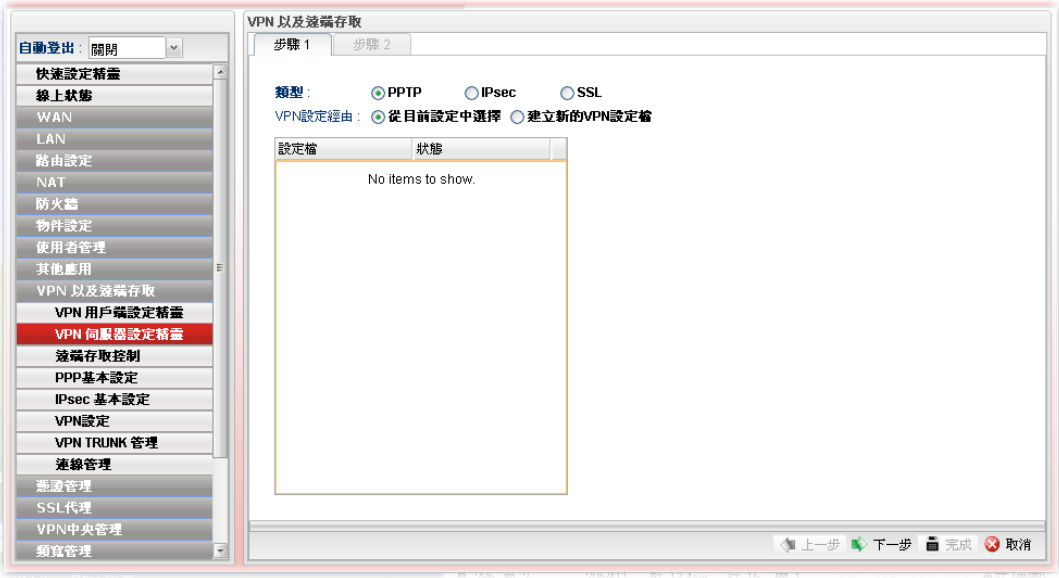
項目	說明
設定檔	顯示 VPN 設定檔的檔名。
啓用	勾選此框啓用此設定檔。
永遠連線	選擇**啓用**讓路由器永遠保持連線狀態。
撥出經由	選擇 WAN 設定檔介面。選擇 WAN 設定檔介面。然後選擇預設 WAN IP (default WAN IP)或是指定 WAN 別名 IP (WAN Alias IP)用於 VPN 通道。
備援介面	選擇 WAN 設定檔，當選定的 WAN 介面發生故障時，系統能自動引導資料由其他 WAN 進出。
閒置逾時	當永遠連線停用時，您必須在此輸入終止網路連線的等待時間。
伺服器 IP/主機名稱	輸入 SSL 伺服器的 IP 位址或是主機名稱。
SSL 使用者名稱	輸入用以驗證 SSL 連線的使用者名稱。

SSL 密碼	輸入用以驗證 SSL 連線的密碼。
本機 IP/子網路遮罩	輸入本機的 IP 位址與子網遮罩。
遠端 IP/子網路遮罩	輸入遠端主機的 IP 位址與子網遮罩。
Route/NAT 模式	指定此設定檔的目的。
Netbios Naming Packet (Netbios 命名封包)	**啓用** – 按下此鈕可在連線時於 VPN 通道二端的主機之間提出資料傳送之要求。 **停用** – 當連線時 VPN 通道二端的主機之間發生衝突，此功能將可阻擋通道內的 Netbios 命名封包的傳送作業。
透過 VPN 組播	某些程式可透過 VPN 連線進行多重播送封包。 ● **通過** –點選此鈕讓多重播送封包通過路由器。 ● **封鎖** – 此爲預設值。點選此鈕之後，路由器將會封鎖多重播送封包。
RIP via VPN	**啓用** – 選此項以便透過 VPN 連線交換 RIP 封包。 **停用** – 關閉此功能。停用爲預設值。

5. 輸入上述設定之後，按下**完成**，新的設定檔已經建立完成。

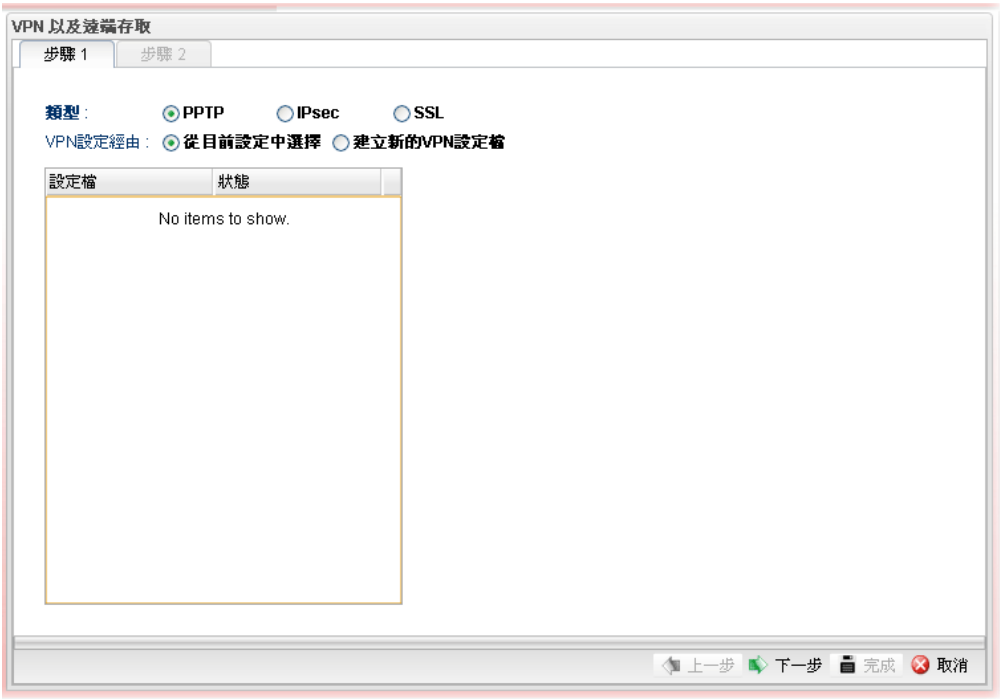
4.9.2 VPN 伺服器設定精靈

此精靈用來設定 VPN 伺服器端所需的 VPN 設定，精靈將引導您一步步建立 VPN 撥入方向的 LAN-to-LAN 設定檔(從用戶端到伺服器)。



如何為 VPN 伺服器端的建立 LAN-to-LAN 設定檔

1. 開啓 **VPN 與遠端存取>>VPN 伺服器設定精靈**。
2. 下述頁面將會出現。

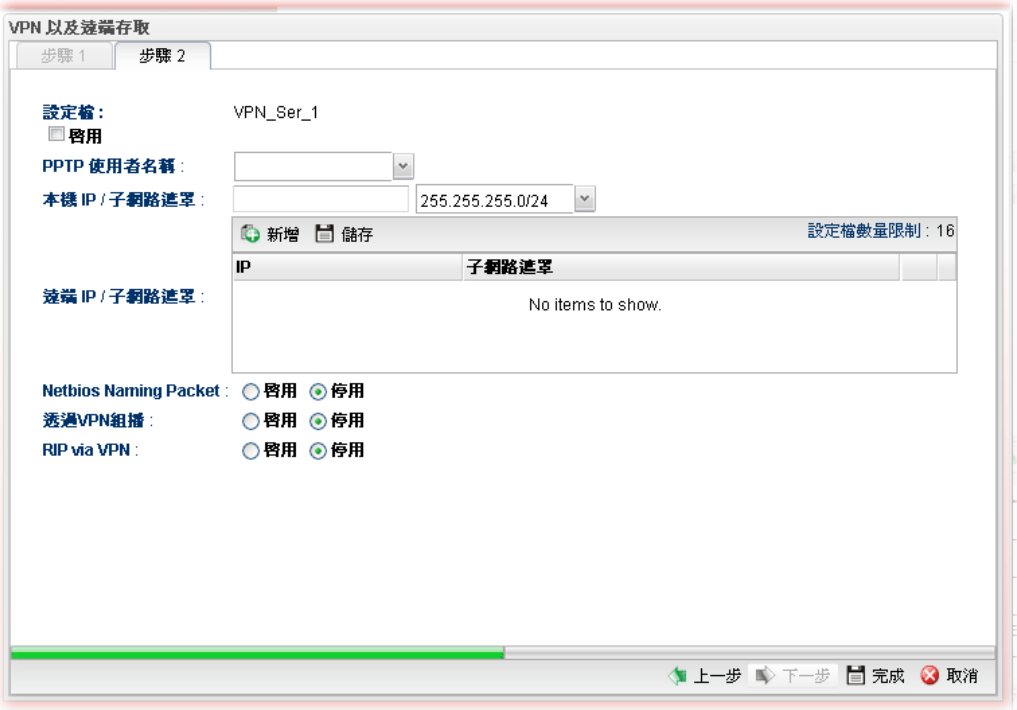


可用參數詳列如下：

項目	說明
類型	指定用於此 VPN 設定檔所需的協定類型 (**PPTP** 或是

	IPSec)。
VPN 設定經由	**從目前設定中選擇** – 若您已經事先建立好 LAN to LAN 設定檔，那麼已建立的 VPN LAN to LAN 設定檔會詳列於下方，選擇您需要的設定檔。 **建立新的 VPN 設定檔** – 這個選項可讓您建立一個全新的 LAN to LAN 設定檔，可在設定檔名稱欄位中輸入檔名。
設定檔名稱	輸入設定檔的名稱。
下一頁	進入下一頁。
取消	按此鈕捨棄頁面設定。

3. 選擇需求類型(PPTP/IPsec/SSL)，按下**建立新的 VPN 設定檔**，然後輸入設定檔的檔名，接著按**下一步**。若您選擇 **PPTP** 爲需求類型，您可見到如下頁面：

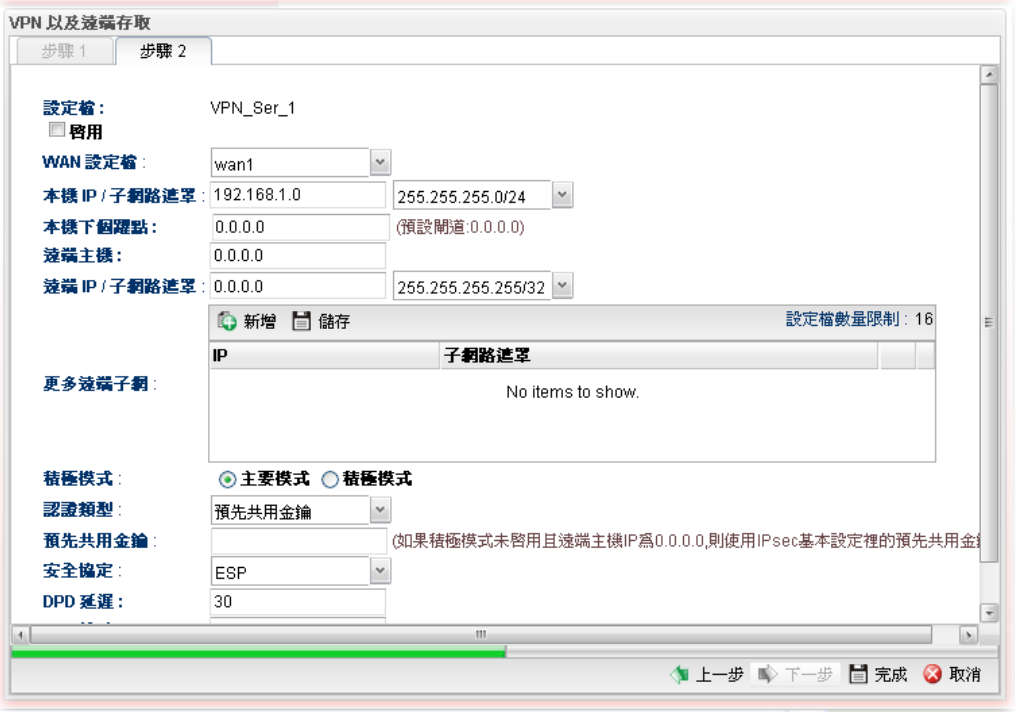


可用參數詳列如下：

項目	說明
設定檔	顯示設定檔名稱。
啓用	勾選此框啓用此設定檔。
PPTP 使用者名稱	輸入用以驗證 PPTP 連線的使用者名稱。 這裡的設定檔可透過**使用者管理>>使用者設定檔**來建立，若未事先建立，這區將無任何選項可以選取。
本機 IP/子網路遮罩	輸入本機的 IP 位址與子網遮罩。
遠端 IP/子網路遮罩	輸入遠端主機的 IP 位址與子網遮罩。

Netbios Naming Packet	啓用 – 按下此鈕可在連線時於 VPN 通道二端的主機之間提出資料傳送之要求。 停用 – 當連線時 VPN 通道二端的主機之間發生衝突，此功能將可阻擋通道內的 Netbios 命名封包的傳送作業。
透過 VPN 組播	某些程式可透過 VPN 連線進行多重播送封包。 ● **通過** –點選此鈕讓多重播送封包通過路由器。 ● **封鎖** – 此爲預設值。點選此鈕之後，路由器將會封鎖多重播送封包。
RIP via VPN	啓用 – 選此項以便透過 VPN 連線交換 RIP 封包。 停用 – 關閉此功能。停用爲預設值。

如果您選擇的是 **IPSec**，您將可看到如下頁面：

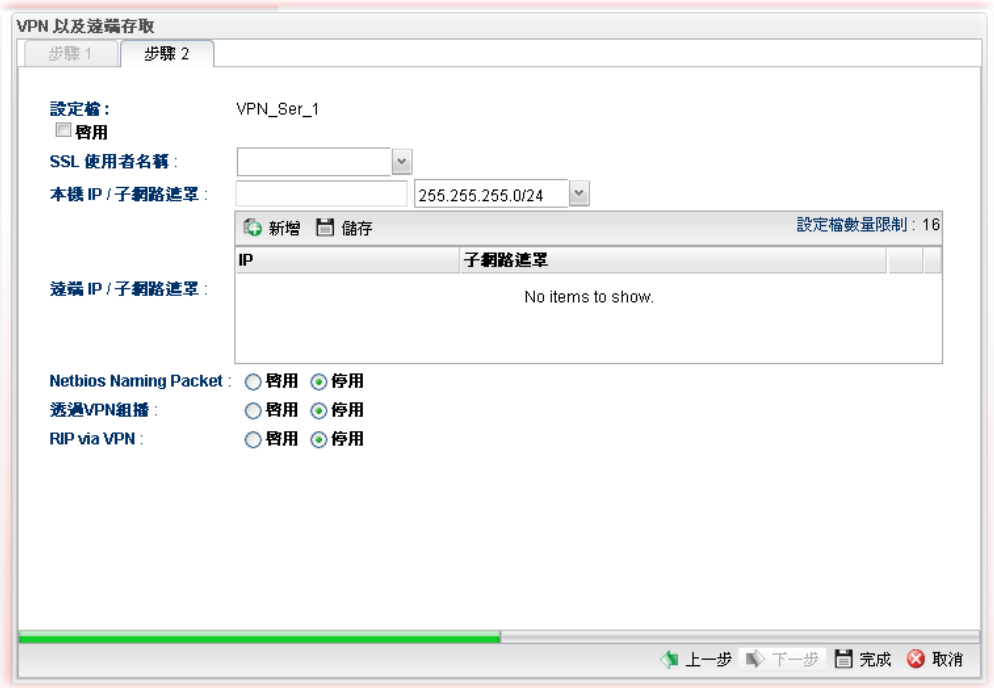


可用參數詳列如下：

項目	說明
設定檔	顯示 VPN 設定檔的檔名。
啓用	勾選此框啓用此設定檔。
WAN 設定檔	選擇用於此設定檔的 WAN 介面設定檔。
本機 **IP/**子網路遮罩	輸入本機的 IP 位址與子網遮罩。
本機下個躍點	指定 WAN 介面的閘道，建議使用預設值即可。
遠端主機	輸入遠端主機的 WAN IP 位址。
遠端 **IP/**子網路遮罩	輸入遠端主機的 IP 位址與子網遮罩。

更多遠端子網	如有必要可在本區增加更多的遠端子網。
積極模式	選擇主要模式或是積極模式。比起積極模式，主要模式顯得更加安全，因爲在安全通道中有更多的交換動作於此完成，不過，積極模式是比較快速的模式。路由器的預設值爲主要模式。 **Local ID –** 僅在積極模式中可運作，輸入可由遠端用戶設定的 Vigor 路由器的身分 ID。 **Remote ID –** 僅在積極模式中可運作，當鑑定遠端 VPN 伺服器身分時，遠端 ID 代表 IP 位址，ID 長度限制於 47 個字元。
認證類型	選擇用於 Pre-Shared Key 或是 RSA Signature 的驗證類型，可選 **PSK** 或是 **RSA**。
預先共用金鑰	如果 PSK 被選定爲驗證類型，請在此輸入共享密鑰值。
安全協定	選擇 **ESP** 以便指定 IPsec 協定，所有的資料將被加密且須受到驗證。若要驗證表頭，則選擇 **AH** 以指定 IPsec 協定，資料將會受到驗證但不會被加密。
DPD 延遲	DPD 爲 dead peer detection 的縮寫，指的是對點狀態偵測，看看 VPN 另一端是否正常。因爲這是一個維持連線的計時裝置，因此當某條通道閒置時，系統會定期發出招呼訊息以維持連線運作，輸入 0 可關閉此功能，如果要啓用此功能，建議設定值爲 30 秒。
DPD 逾時	此爲逾時計時器，一旦逾時之後系統沒有收到任何來自 VPN 對方的應答訊息，則該方將被宣告已廢。輸入 0 可關閉此功能，如果要啓用此功能，建議設定值爲 120 秒。

如果您選擇的是 **SSL**，您將可看到如下頁面：



可用參數詳列如下：

項目	說明
設定檔	顯示設定檔名稱。
啓用	勾選此框啓用此設定檔。
SSL 使用者名稱	輸入用以驗證 SSL 連線的使用者名稱。 這裡的設定檔可透過**使用者管理>>使用者設定檔**來建立，若未事先建立，這區將無任何選項可以選取。
本機 IP/子網路遮罩	輸入本機的 IP 位址與子網遮罩。
遠端 IP/子網路遮罩	輸入遠端主機的 IP 位址與子網遮罩。
Netbios Naming Packet	**啓用** – 按下此鈕可在連線時於 VPN 通道二端的主機之間提出資料傳送之要求。 **停用** – 當連線時 VPN 通道二端的主機之間發生衝突，此功能將可阻擋通道內的 Netbios 命名封包的傳送作業。
透過 VPN 組播	某些程式可透過 VPN 連線進行多重播送封包。 ● **通過** –點選此鈕讓多重播送封包通過路由器。 ● **封鎖** – 此爲預設值。點選此鈕之後，路由器將會封鎖多重播送封包。
RIP via VPN	**啓用** – 選此項以便透過 VPN 連線交換 RIP 封包。 **停用** – 關閉此功能。停用爲預設值。

4. 輸入上述設定之後，按下**完成**，新的設定檔已經建立完成。

4.9.3 遠端存取控制

這個設定可以啓動必要的 VPN 服務，如果您想要在區域網路中執行 VPN 伺服器功能，您一定要適度關閉路由器的 VPN 服務，讓 VPN 通道暢通，並關閉類似 DMZ 或是開放埠等 NAT 設定。

可用參數詳列如下：

項目	說明
啓用 PPTP VPN / L2TP VPN / SSL 通道 /IPsec 服務	勾選個別方框啓用個別功能。
IPSec 遠端撥入服務	按下任一服務按鈕以選擇該項服務。
套用	按此鈕儲存設定。
取消	按此鈕捨棄頁面設定。

選擇完畢之後，按下**套用**儲存設定。

4.9.4 PPP 基本設定

遠端用戶可以透過路由器與使用者之間建立的 VPN 連線，經過驗證之後，連接至網站、主機或是伺服器等處。

4.9.4.1 PPTP

本頁顯示基於 PPTP 協定建立的 VPN 通道目前的狀態。

可用參數詳列如下：

項目	說明
驗證協定	路由器將會透過此處選擇的協定驗證撥入用戶。 MS-CHAP-v2 PAP CHAP MS-CHAP MS-CHAP-v2 **PAP -** 選擇此項目強迫路由器以 PAP 協定來驗證撥入使用者。 **CHAP** – 表示路由器將嘗試以 CHAP 協定驗證撥入用戶。
MPPE 加密	指定此伺服器需要的加密方式，這個選項僅在 MS-CHAP 或是 MS-CHAP_v2 被選為**驗證協定**時有作用。 128-bit 40/128-bit 128-bit Disable
用戶驗證類型	可設定的類型包含 **Local**、**RADIUS**、**LDAP** 伺服器。 Local Local RADIUS LDAP

LDAP 設定	如果使用者驗證類型選擇的是 **LDAP**，請於此挑選 PPTP 伺服器需求的 LDAP 設定檔。 如欲清除選定的設定檔，按下 ✕ 即可移除該選定物件。
DHCP 來自於	如果使用者驗證類型選擇的是 **RADIUS**，請於此挑選 L2TP 伺服器需求的 LAN 設定檔。
DHCP 中繼	**啓用** – 讓路由器分派 IP 位址到 LAN 端的每個主機上。 **停用** – 讓您手動指派 IP 位址到 LAN 端的每個主機上。
PPTP MSS	輸入用於 PPTP VPN 通道的 MSS 值(最大分段大小)。
NetBIOS 命名封包	**通過** – 按此鈕讓資料能在二台主機之間所建立的 VPN 通道上傳輸。 **封鎖** –當雙方所建立的 VPN 通道連線產生衝突時，此功能可以封鎖此通道。
Multicast Packet via VPN	某些程式可透過 VPN 連線進行多重播送封包。 ● **通過** –點選此鈕讓多重播送封包通過路由器。 ● **封鎖** – 此爲預設值。點選此鈕之後，路由器將會封鎖多重播送封包。
PPTP 加速	**啓用** – 選擇此項以便讓在 VPN 通道中執行 PPTP 加速功能。
套用	按此鈕儲存設定。
取消	按此鈕捨棄頁面設定。

輸入所有的設定並按下**套用**儲存。

4.9.4.2 L2TP

本頁顯示基於 L2TP 協定建立的 VPN 通道目前的狀態。

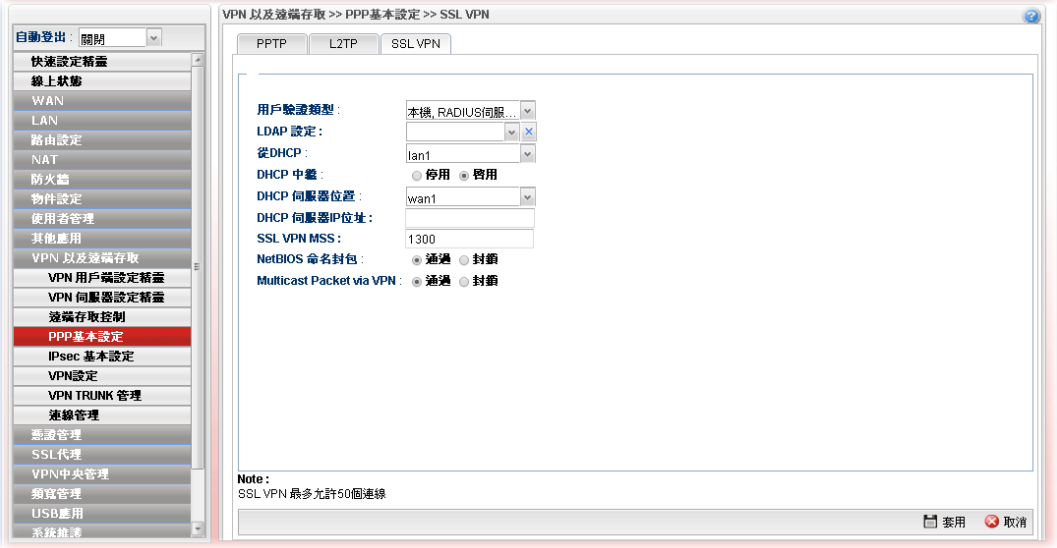
可用參數詳列如下：

項目	說明
驗證協定	路由器將會透過此處選擇的協定驗證撥入用戶。 MS-CHAP-v2 PAP CHAP MS-CHAP MS-CHAP-v2 **PAP -** 選擇此項目強迫路由器以 PAP 協定來驗證撥入使用者。 **CHAP** – 表示路由器將嘗試以 CHAP 協定驗證撥入用戶。
用戶驗證類型	可設定的類型包含 **Local**、**RADIUS**、**LDAP** 伺服器。 LDAP Local RADIUS LDAP
LDAP 設定	如果使用者驗證類型選擇的是 **LDAP**，請於此挑選 PPTP 伺服器需求的 LDAP 設定檔。 如欲清除選定的設定檔，按下 按鈕即可移除。
DHCP 來自於	如果使用者驗證類型選擇的是 **RADIUS**，請於此挑選 L2TP 伺服器需求的 LAN 設定檔。
DHCP 中繼	啓用 – 讓路由器分派 IP 位址到 LAN 端的每個主機上。 停用 – 讓您手動指派 IP 位址到 LAN 端的每個主機上。
DHCP 伺服器位置	針對 DHCP 伺服器選擇適當的 WAN/LAN 介面。
DHCP 伺服器 **IP** 位址	這個選項僅在 **DHCP Relay** 選項開啓時才有作用，輸入您準備使用的 DHCP 伺服器的 IP 位址，讓延遲代理伺服器可以幫忙轉發 DHCP 需求至該處。
強制 **L2TP with IPsec** 策略	如果勾選此項，路由器將會使用 L2TP with IPsec policy 進行 VPN 連線。
套用	按此鈕儲存設定。
取消	按此鈕捨棄頁面設定。

輸入所有設定並按下**套用**儲存。

4.9.4.3 SSL VPN

本頁顯示基於 SSL 協定建立的 VPN 通道目前的狀態。



可用參數詳列如下：

項目	說明
用戶驗證類型	可設定的類型包含**本機**、**RADIUS**、**LDAP** 伺服器。
LDAP 設定	如果使用者驗證類型選擇的是 **LDAP**，請於此挑選 PPTP 伺服器需求的 LDAP 設定檔。 如欲清除選定的設定檔，按下 ✕ 按鈕即可移除。
從 DHCP	如果使用者驗證類型選擇的是 **RADIUS**，請於此挑選 L2TP 伺服器需求的 LAN 設定檔。
DHCP 中繼	**啓用** – 讓路由器分派 IP 位址到 LAN 端的每個主機上。 **停用** – 讓您手動指派 IP 位址到 LAN 端的每個主機上。
DHCP 伺服器位置	針對 DHCP 伺服器選擇適當的 WAN/LAN 介面。
DHCP 伺服器 IP 位址	這個選項僅在 **DHCP Relay** 選項開啓時才有作用，輸入您準備使用的 DHCP 伺服器的 IP 位址，讓延遲代理伺服器可以幫忙轉發 DHCP 需求至該處。
SSL VPN MSS	輸入用於 SSL VPN 通道的 MSS 值(最大分段大小)。
NetBIOS 命名封包	**通過** – 按此鈕讓資料能在二台主機之間所建立的 VPN 通道上傳輸。 **封鎖** –當雙方所建立的 VPN 通道連線產生衝突時，此功能可以封鎖此通道。
Multicast Packet via VPN	某些程式可透過 VPN 連線進行多重播送封包。 ● **通過** –點選此鈕讓多重播送封包通過路由器。 ● **封鎖** – 此爲預設值。點選此鈕之後，路由器將會封鎖多重播送封包。

套用	按此鈕儲存設定。
取消	按此鈕捨棄頁面設定。

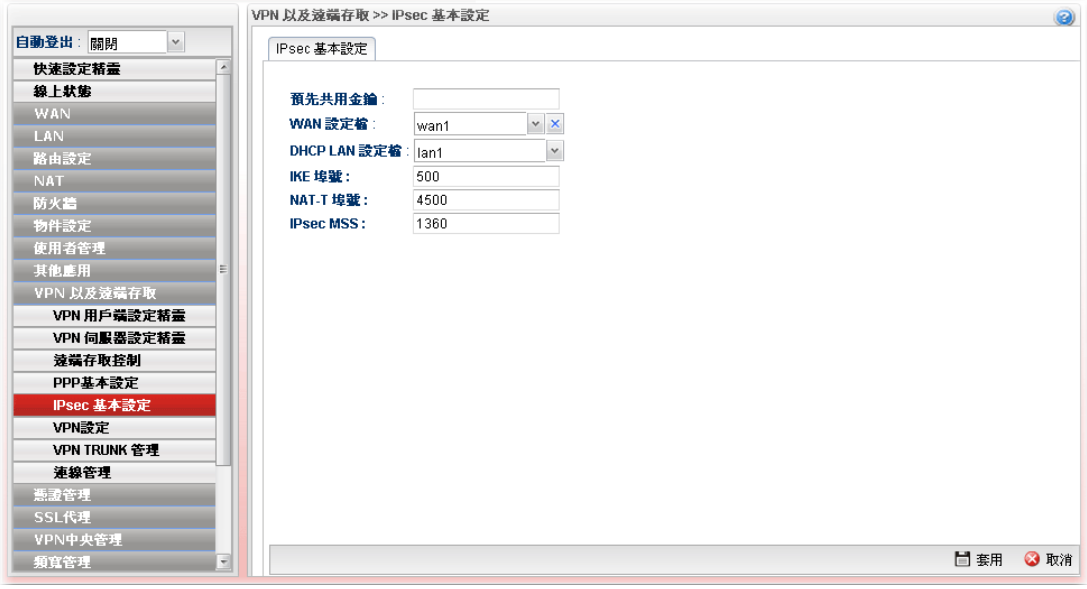
輸入所有設定並按下**套用**儲存。

4.9.5 IPsec 基本設定

在 IPSec 中有二種加密方式 – 傳送與通道，傳送模式將會增加 AH/ESP 承載量並使用原始 IP 標頭來加密承載的資料，此模式只應用於本地封包上如 L2TP over IPSec，通道模式不只增加 AH/ESP 承載量也會使用新的 IP 封包頭來加密整個原始 IP 封包。

驗證封包頭(AH) 提供 VPN 雙方的 IP 封包資料驗證和整合，可以單方重述功能來達成建立訊息摘要的動作，這些摘要隨著封包傳送將放置於封包頭。接收方將會在封包上執行同樣的動作，並與所接收到的數值比較。

封裝式安全酬載(ESP)提供選擇性驗證方法，對資料機密化和防護的安全協定，可重新進行檢測。



可用參數詳列如下：

項目	說明
事先共用金鑰	指定用於 IKE 驗證需求的密鑰。 **確認事先共用金鑰(Confirm Pre-Shared Key)-** 再次輸入以確認您所輸入的共用金鑰。
WAN 設定檔	選擇一組 WAN 設定檔。 如欲刪除選定的設定檔，請按下 ✕ 即可移除。
DHCP LAN 設定檔	選擇一組 LAN 設定檔。
IKE 埠號	輸入 IKE 流向 VPN 伺服器所需的 UDP 埠號。
NAT-T 埠號	輸入 IPsec NAT-T 流量所需的 UDP 埠號。
IPSec MSS	輸入 IPsec VPN 通道需求之 MSS 值。
套用	按此鈕儲存設定。
取消	按此鈕捨棄頁面設定。

輸入所有設定並按下**套用**儲存。

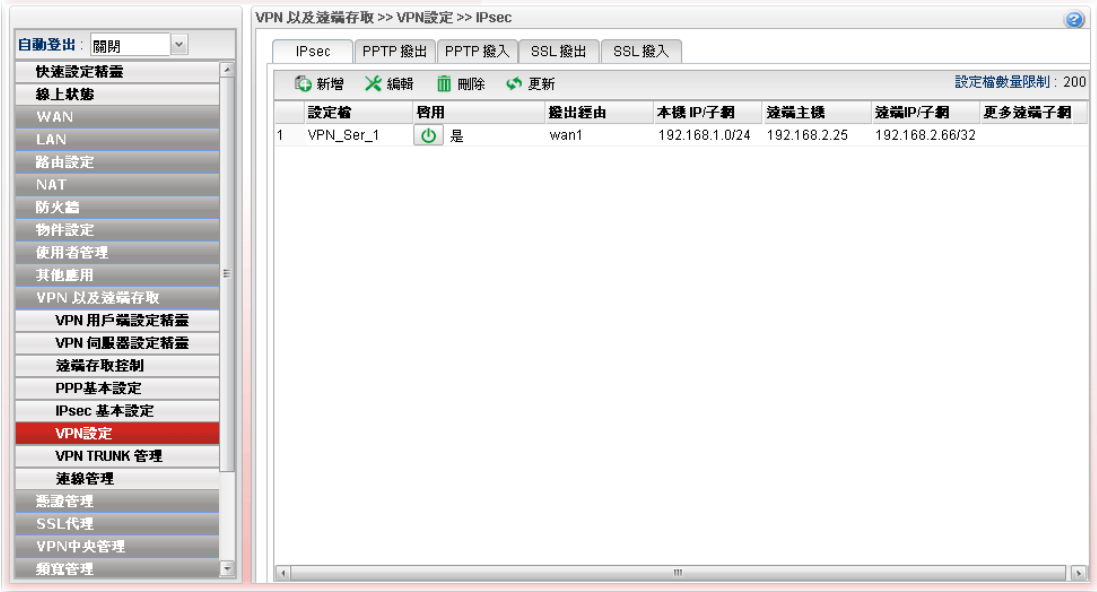
4.9.6 VPN 設定

本頁允許您透過 IPsec 或是 PPTP 協定(撥入或是撥出)建立 VPN 設定檔。

所有 VPN 設定檔都將顯示在本頁面。

4.9.6.1 IPsec 通道

顯示以 IPsec 策略爲主的 LAN to LAN 設定檔。



每個項目說明如下：

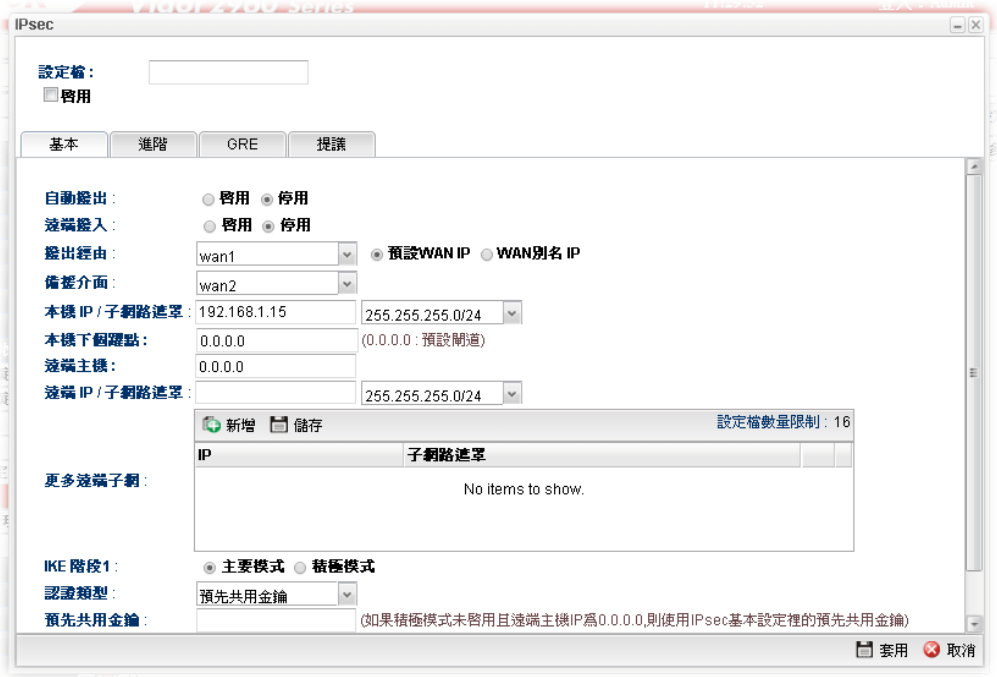
項目	說明
新增	新增新的設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
刪除	移除選定的設定檔。 請選擇您想要刪除的既有設定檔，然後按下刪除按鈕，該設定檔即可被移除。
更新	重新更新本頁面。
設定檔數量限制	顯示可以建立的設定檔總數。
設定檔	顯示設定檔的檔名。
啓用	顯示設定檔狀態，False 表示停用；True 表示啓用。
撥出經由	顯示此設定檔選定的 WAN 介面。
本機 IP/子網	顯示此設定檔的 LAN IP 位址與子網遮罩。
遠端主機	顯示此設定檔遠端主機的名稱。
遠端 IP/子網	顯示此設定檔的 WAN IP 位址與子網遮罩。

更多遠端子網	顯示其他可供此設定檔使用的 LAN IP 位址與子網遮罩。

如何新增 IPsec VPN 設定檔

IPSec 服務可提供存取控制、資料原始驗證、拒絕重播封包及透過加密來保密。這些物件都是透過二種方式，驗證封包頭(AH)與封裝式安全酬載(ESP)，加上密鑰管理程序和協議來完成。

1. 開啓 **VPN 與遠端存取>> VPN 設定**。
2. 按下**新增**按鈕。
3. 下述頁面將會出現。按下**基本**標籤以進行設定配置。

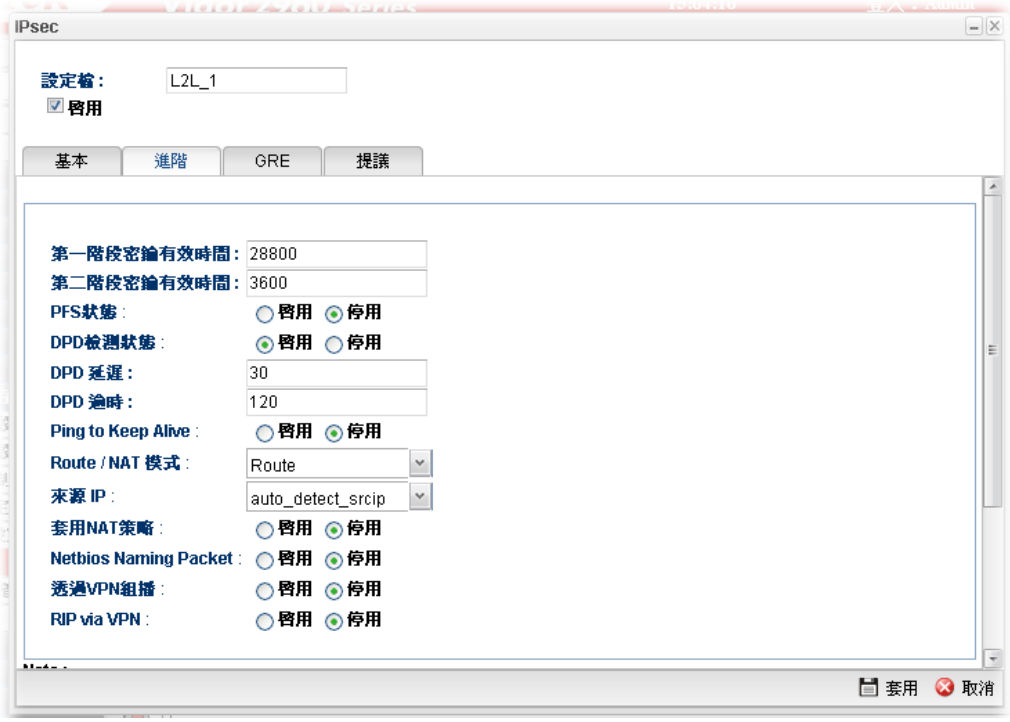


可用參數詳列如下：

項目	說明
設定檔	輸入設定檔的檔名。
啓用	勾選此框啓用此設定檔。
基本	**自動撥出** – 選擇**啓用**讓路由器選擇建立 VPN 連線的時機(例如永遠撥出、如果 WAN1/WAN2 斷線、如果 USB1/USB2 斷線等等)。 **遠端撥入**- 選擇**啓用**允許透過 IPsec 遠端撥入主機進行連線。 **撥出經由** - 選擇 WAN 設定檔介面。然後選擇預設 WAN IP (default WAN IP)或是指定 WAN 別名 IP (WAN Alias IP)用於 VPN 通道。 **備援介面** – 選擇 WAN 設定檔，當選定的 WAN 介面發生故障時，系統能自動引導資料由其他 WAN 進出。

	本機 IP/子網路遮罩 - 輸入本機的 IP 位址與子網遮罩。 **本機下個躍點** – 指定 WAN 介面的閘道，通常使用預設值(空白)。 **遠端主機**– 輸入遠端主機的 WAN IP 位址。 **遠端 IP/子網路遮罩**– 輸入遠端主機的 LAN IP 位址與子網遮罩。 **更多遠端子網** – 如有必要，可按此設定更多的遠端子網。 **IKE 階段 1** - 選擇 **Main 模式**或是 **Aggressive 模式**。比起 **Aggressive 模式**，**Main 模式**顯得更加安全，因爲在安全通道中有更多的交換動作於此完成，不過，**Aggressive 模式**是比較快速的模式。路由器的預設值爲 **Main 模式**。 **認證類型**– **選擇用於 PSK 或是 RSA** Signatureg 的驗證類型。 **預先共用金鑰**– 當 PSK 被選定爲驗證類型時，請在此輸入金鑰以因應 IKE 驗證。 **本機憑證**– 若是驗證類型選擇 **RSA**，請自下拉式清單中選擇本機憑證。 **Local ID** – 輸入代表此裝置的 ID 內容，讓遠端也能依此設定的 ID，這個選項僅在 Aggressive 模式啓用時可用。 **Remote ID –** 此處輸入的內容主要是讓遠端 VPN 伺服器驗證之用，ID 長度限於 47 個字元內，這個選項僅在 Aggressive 模式啓用時可用。 **安全協定**– 選擇 **ESP** 以便指定 IPsec 協定，所有的資料將被加密且須受到驗證。若要驗證表頭，則選擇 **AH** 以指定 IPsec 協定，資料將會受到驗證但不會被加密。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

4. 填完**基本**標籤內的資訊之後，按下**進階**標籤開啓如下頁面。

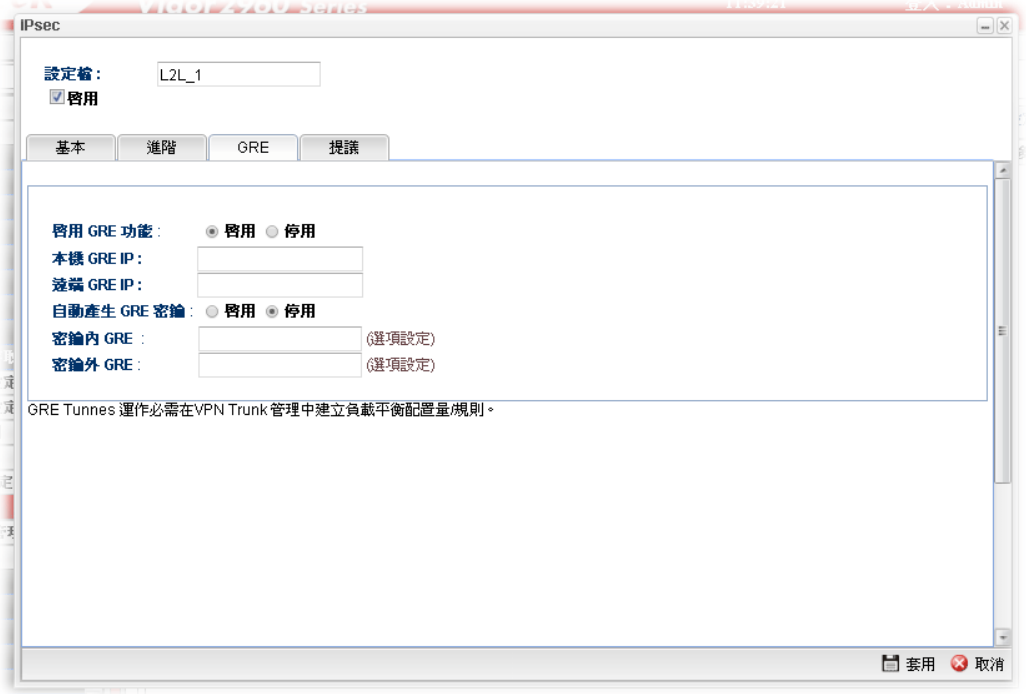


可用參數詳列如下：

項目	說明
第一階段密鑰有效時間	第一階段密鑰(IKE)之連線密鑰更新後，重新談判的時期，可接受的範圍從 5 到 480 分鐘（約莫 8 小時)。
第二階段密鑰有效時間	第二階段密鑰(IKE)之連線密鑰更新後，重新談判的時期，可接受的範圍從 5 到 480 分鐘（約莫 8 小時)。
PFS 狀態	啓用 PFS 功能，每次 PFS 計算加密與/或驗證密鑰，都會包含新的 Diffie-Hellman 密鑰交換值。
DPD 檢測狀態	**啓用** – 選擇此項啓用 DPD 功能。當系統偵測到 IPsec 通道中沒有任何流量時，伺服器與用戶雙方都將傳送 DPD 封包給對方，確保該通道仍持續有效。 **停用** – 選此項停用 DPD 功能。
DPD 延遲	DPD 爲 dead peer detection 的縮寫，指的是對點狀態偵測，看看 VPN 另一端是否正常。因爲這是一個維持連線的計時裝置，因此當某條通道閒置時，系統會定期發出招呼訊息以維持連線運作，輸入 0 可關閉此功能，如果要啓用此功能，建議設定值爲 30 秒。
DPD 逾時	此爲逾時計時器，一旦逾時之後系統沒有收到任何來自 VPN 對方的應答訊息，則該方將被宣告已廢。輸入 0 可關閉此功能，如果要啓用此功能，建議設定值爲 120 秒。
Ping to Keep Alive	**啓用**–選擇此項啓用此功能。 **Ping to the IP -** 如果啓用了此功能，請先指定 IP 位址讓系統能採取相關的動作以便維持運作。

Route/NAT 模式	如果遠端網路僅允許您以單一 IP 撥入，請選擇 NAT 模式，否則請選擇路由模式。
來源 IP	選擇一組 LAN 設定檔成爲來源 IP。
套用 NAT 策略	**啓用** – 此選項允許對所有透過 VPN 傳輸的流量執行一對一 NAT。 **傳輸至本機網路**– 指定網路的 IP 位址與子網遮罩，所有的資訊都將流入該處。
Netbios Naming Packet	**啓用** – 按下此鈕可在連線時於 VPN 通道二端的主機之間提出資料傳送之要求。 **停用** – 當連線時 VPN 通道二端的主機之間發生衝突，此功能將可阻擋通道內的 Netbios 命名封包的傳送作業。
透過 VPN 組播	某些程式可透過 VPN 連線進行多重播送封包。 ● **通過** –點選此鈕讓多重播送封包通過路由器。 ● **封鎖** – 此爲預設值。點選此鈕之後，路由器將會封鎖多重播送封包。
RIP via VPN	**啓用** – 選此項以便透過 VPN 連線交換 RIP 封包。 **停用** – 關閉此功能。停用爲預設值。
套用	按此鈕儲存設定。
取消	按此鈕捨棄頁面設定。

5. 完成進階設定之後，按下 **GRE** 開啓如下頁面：

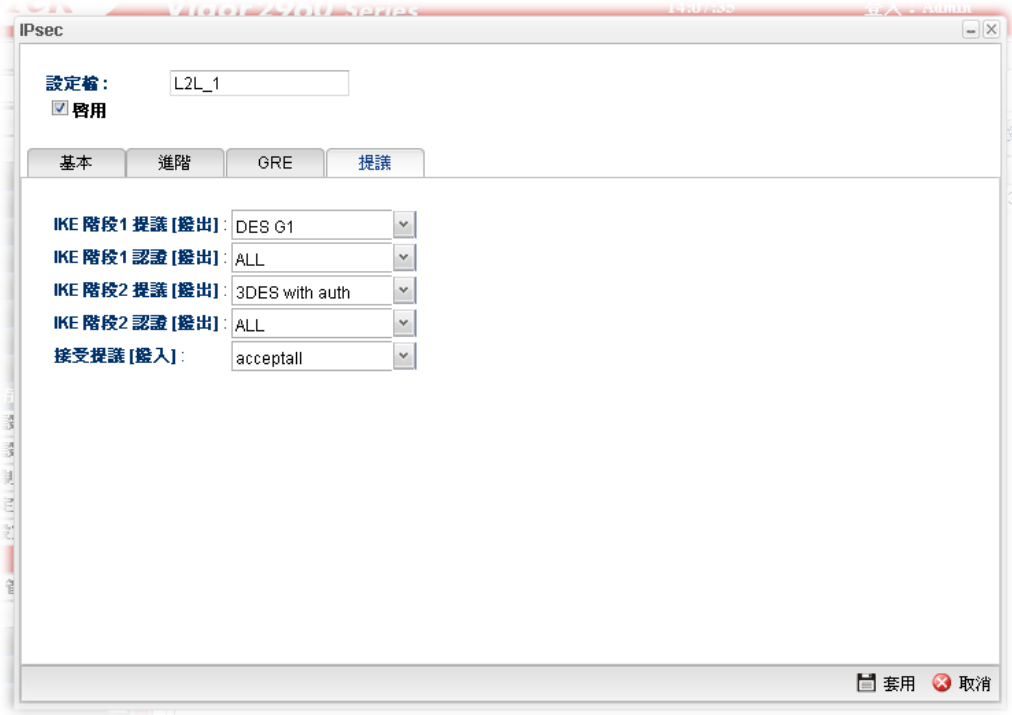


可用參數詳列如下：

項目	說明

啓用 GRE 功能	勾選此項啓用此功能。
本機 GRE IP	路由器的虛擬 IP 位址。
遠端 GRE IP	遠端用戶的虛擬 IP 位址。
自動產生 GRE 密鑰 (Auto Generate GRE Key)	選擇**啓用**讓系統自動產生 GRE 密鑰。 如果您選擇**停用**，您必須手動輸入該密鑰。
密鑰內 GRE	輸入 16 進位數字作爲 GRE In Key，這是路由器用來驗證封包來源的密鑰，長度爲 4 位元。
密鑰外 GRE	輸入 16 進位數字作爲 GRE Out Key，這是遠端用戶用來驗證封包來源的密鑰，長度爲 4 位元。
套用	按此鈕儲存設定。
取消	按此鈕捨棄頁面設定。

6. 在填完 **GRE** 相關資訊後，按下**提議**標籤開啓如下頁面：



可用參數詳列如下：

項目	說明
IKE 階段 1 提議(撥出)	建議本機對 VPN 用戶可用的驗證法與加密演算方法，並獲取回饋以尋找有無符合的內容。
IKE 階段 1 認證(撥出)	建議本機對 VPN 用戶可用的演算方式，並獲取回饋以尋找有無符合的內容。
IKE 階段 2 提議(撥出)	建議本機對 VPN 用戶可用的驗證法與加密演算方法，並獲取回饋以尋找有無符合的內容。
IKE 階段 2 認證(撥	建議本機對 VPN 用戶可用的演算方式，並獲取回饋以尋

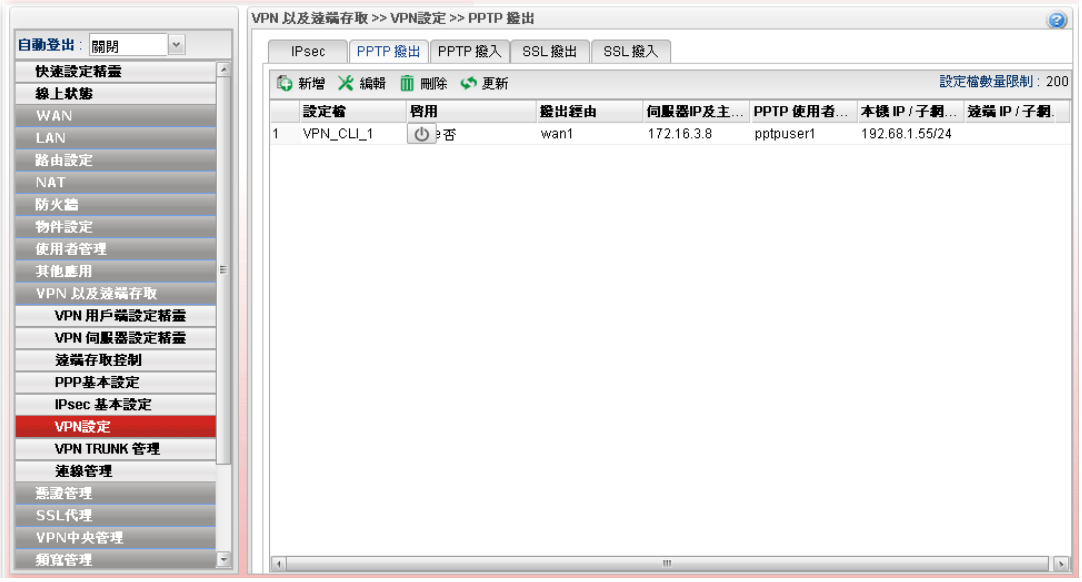
出)	找有無符合的內容。
接受提議(撥入)	對於撥入的 VPN 用戶，請指定建議事項： **接受所有的建議 (acceptall)** - 當 VPN 通道建立後，此裝置支援的所有建議都可被套用。 **僅接受上述列出的建議(acceptabove)** - 當 VPN 通道建立後，只有被選擇的建議會被路由器系統接受及套用。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

7. 輸入所有設定並按下**套用**儲存。

8. 新 IPSec LAN-to-LAN 設定檔已經建立完成。

4.9.6.2 PPTP/SSL 撥出設定檔

顯示以 PPTP/SSL 撥出策略為主的 LAN to LAN 設定檔。



每個項目說明如下：

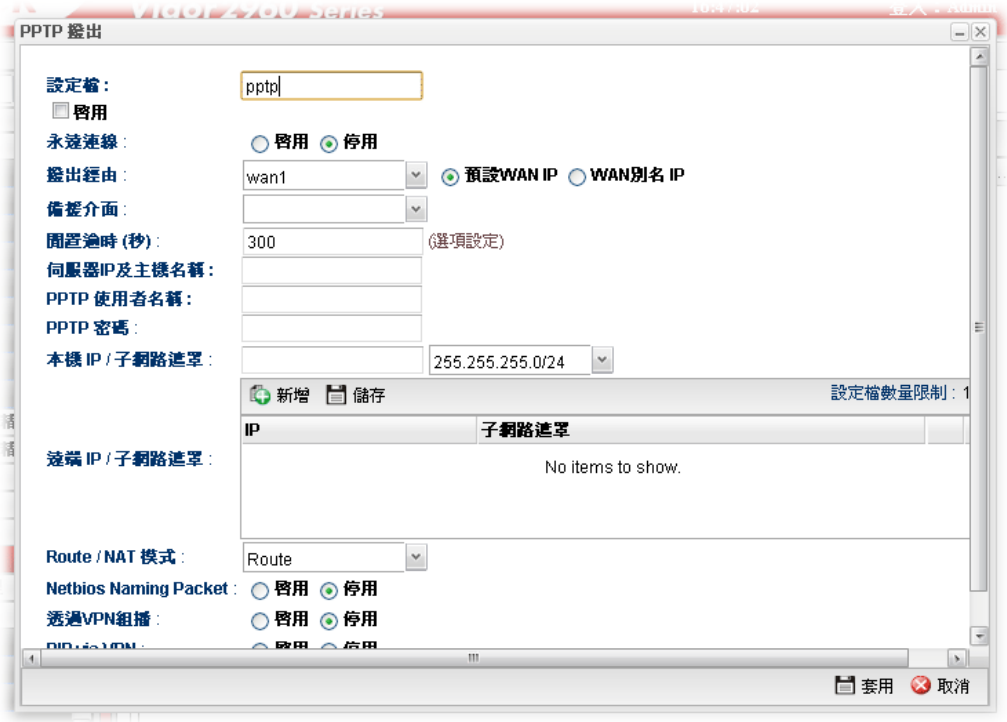
項目	說明
新增	新增新的設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
刪除	移除選定的設定檔。 請選擇您想要刪除的既有設定檔，然後按下刪除按鈕，該設定檔即可被移除。
更新	重新更新本頁面。
設定檔數量限制	顯示可以建立的設定檔總數。

設定檔	顯示設定檔的檔名。
啓用	顯示設定檔狀態，False 表示停用；True 表示啓用。
PPTP/SSL 使用者名稱	輸入 PPTP/SSL 連線需求的使用者名稱。
本機 IP/子網路遮罩	顯示此設定檔的 LAN IP 位址與子網遮罩。
遠端主機	顯示此設定檔遠端主機的名稱。
遠端 IP/子網路遮罩	顯示此設定檔的 WAN IP 位址與子網遮罩。

如何新增 PPTP/SSL 撥出設定檔

以下將告訴您如何針對 VPN 連線建立以 PPTP/SSL 撥出爲基準的設定檔。

1. 開啓 **VPN 與遠端存取>>VPN 設定**。
2. 切換至 PPTP/SSL 撥出標籤，按下**新增**按鈕。
3. 下述頁面將會出現。



可用參數詳列如下：

項目	說明
設定檔	輸入設定檔的檔名。
啓用	勾選此框啓用此設定檔。
永遠連線	選擇**啓用**讓設定檔保持連線狀態。
撥出經由	選擇 WAN 設定檔介面。選擇 WAN 設定檔介面。然後選擇預設 WAN IP (default WAN IP)或是指定 WAN 別名 IP (WAN Alias IP)用於 VPN 通道。

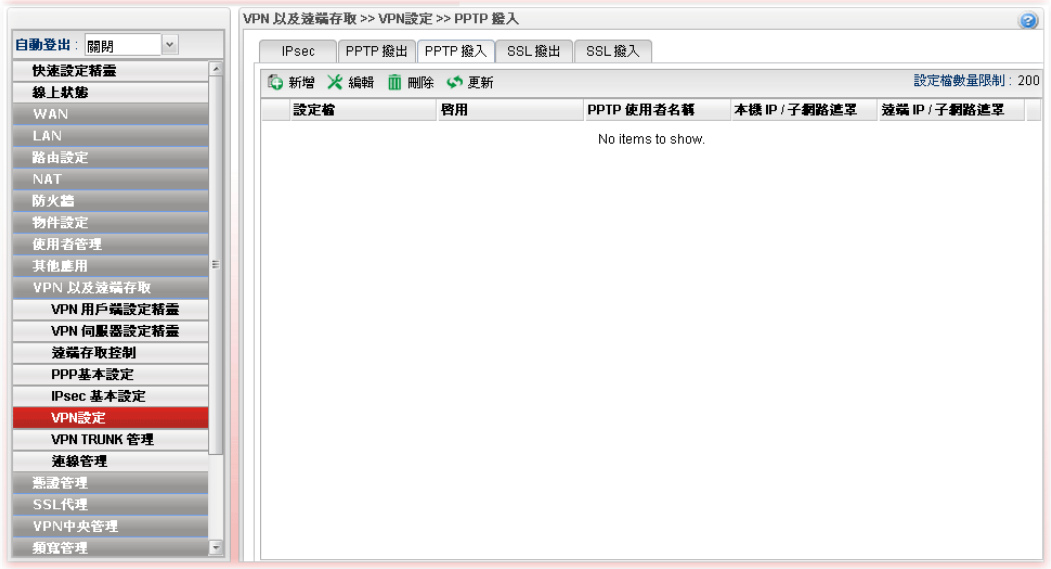
備援介面	選擇 WAN 設定檔，當選定的 WAN 介面發生故障時，系統能自動引導資料由其他 WAN 進出。
閒置逾時	當永遠連線停用時，您必須在此輸入終止網路連線的等待時間。
伺服器 IP/主機名稱	輸入 PPTP/SSL 伺服器的 IP 位址或是主機名稱。
PPTP 使用者名稱/ SSL 使用者名稱	輸入 PPTP/SSL 連線需求的使用者名稱。
PPTP/SSL 密碼	輸入 PPTP/SSL 連線需求的密碼。
本機 IP/子網路遮罩	輸入本機的 IP 位址與子網遮罩。
遠端 IP/子網路遮罩	輸入遠端主機的 IP 位址與遮罩。
Route / NAT 模式	指定此設定檔的使用目的。
Netbios Naming Packet	**啓用** – 按下此鈕可在連線時於 VPN 通道二端的主機之間提出資料傳送之要求。 **停用** – 當連線時 VPN 通道二端的主機之間發生衝突，此功能將可阻擋通道內的 Netbios 命名封包的傳送作業。
透過 VPN 組播	某些程式可透過 VPN 連線進行多重播送封包。 ● **通過** –點選此鈕讓多重播送封包通過路由器。 ● **封鎖** – 此爲預設值。點選此鈕之後，路由器將會封鎖多重播送封包。
RIP via VPN	**啓用** – 選此項以便透過 VPN 連線交換 RIP 封包。 **停用** – 關閉此功能。停用爲預設值。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

4. 輸入所有設定並按下**套用**儲存。

5. 新 PPTP/SSL 撥出設定檔已經建立完成。

4.9.6.3 PPTP/SSL 撥入通道

顯示 PTP/SSL 撥入 LAN to LAN 設定檔。



每個項目說明如下：

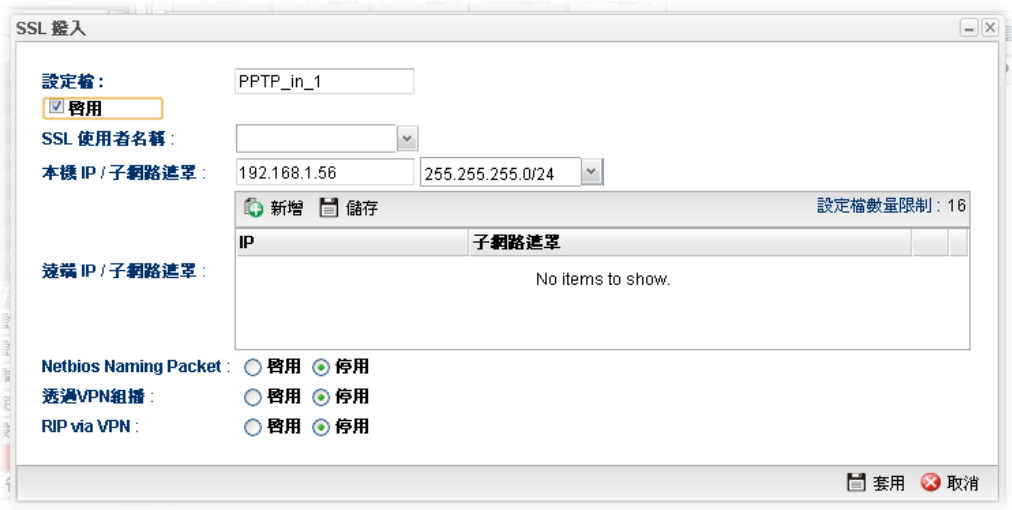
項目	說明
新增	新增新的設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
刪除	移除選定的設定檔。 請選擇您想要刪除的既有設定檔，然後按下刪除按鈕，該設定檔即可被移除。
更新	重新更新本頁面。
設定檔數量限制	顯示可以建立的設定檔總數。
設定檔	顯示設定檔的檔名。
啓用	顯示設定檔狀態，False 表示停用；True 表示啓用。
PPTP/SSL 使用者名稱	輸入 PPTP/SSL 連線需求的使用者名稱。
本機 IP/子網	顯示此設定檔的 LAN IP 位址與子網遮罩。
遠端主機	顯示此設定檔遠端主機的名稱。
遠端 IP/子網	顯示此設定檔的 WAN IP 位址與子網遮罩。

如何新增 PPTP/SSL 撥入設定檔

以下將告訴您如何針對 VPN 連線建立以 PPTP/SSL 撥入爲基準的設定檔。

1. 開啓 **VPN 以及遠端存取>>VPN 設定檔**。
2. 切換至 PPTP/SSL 撥入標籤，按下**新增**按鈕。

3. 下述頁面將會出現。



可用參數詳列如下：

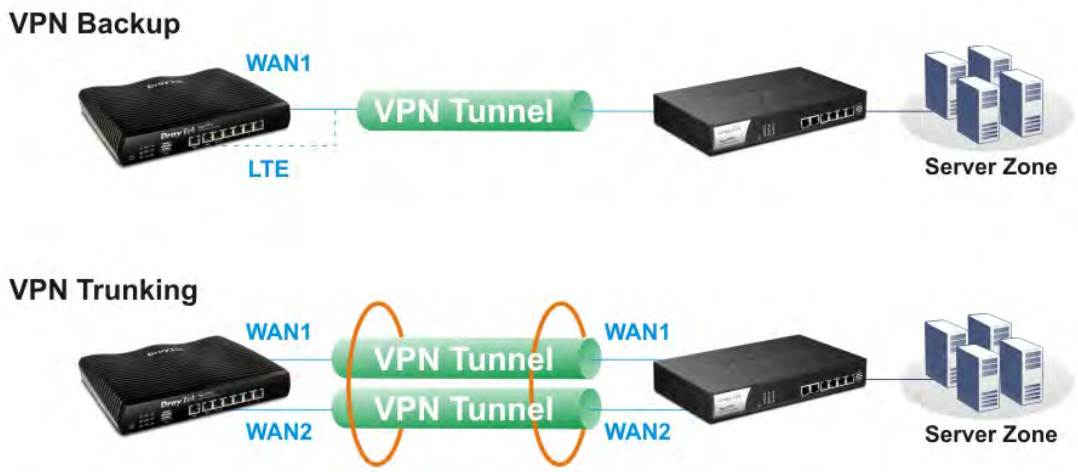
項目	說明
設定檔	輸入設定檔的檔名。
啓用	勾選此框啓用此設定檔。
PPTP/SSL 使用者名稱	選擇於 PPTP/SSL 連線中用來驗證的 PPTP/SSL 使用者設定檔。 此處的設定檔乃是在**使用者管理>>使用者設定檔**中建立，如果您尚未建立任何設定檔，在本區將無法看到任何下拉式選項。
本機 IP/子網路遮罩	輸入本機的 IP 位址與子網遮罩。
遠端 IP/子網路遮罩	輸入遠端主機的 IP 位址與子網遮罩。
Netbios Naming Packet	啓用 – 按下此鈕可在連線時於 VPN 通道二端的主機之間提出資料傳送之要求。 停用 – 當連線時 VPN 通道二端的主機之間發生衝突，此功能將可阻擋通道內的 Netbios 命名封包的傳送作業。
透過 VPN 組播	某些程式可透過 VPN 連線進行多重播送封包。 ● 通過 –點選此鈕讓多重播送封包通過路由器。 ● 封鎖 – 此爲預設值。點選此鈕之後，路由器將會封鎖多重播送封包。
RIP via VPN	啓用 – 選此項以便透過 VPN 連線交換 RIP 封包。 停用 – 關閉此功能。停用爲預設值。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

4. 輸入所有設定並按下**套用**儲存。

5. 新 PPTP/SSL 撥入設定檔已經建立完成。

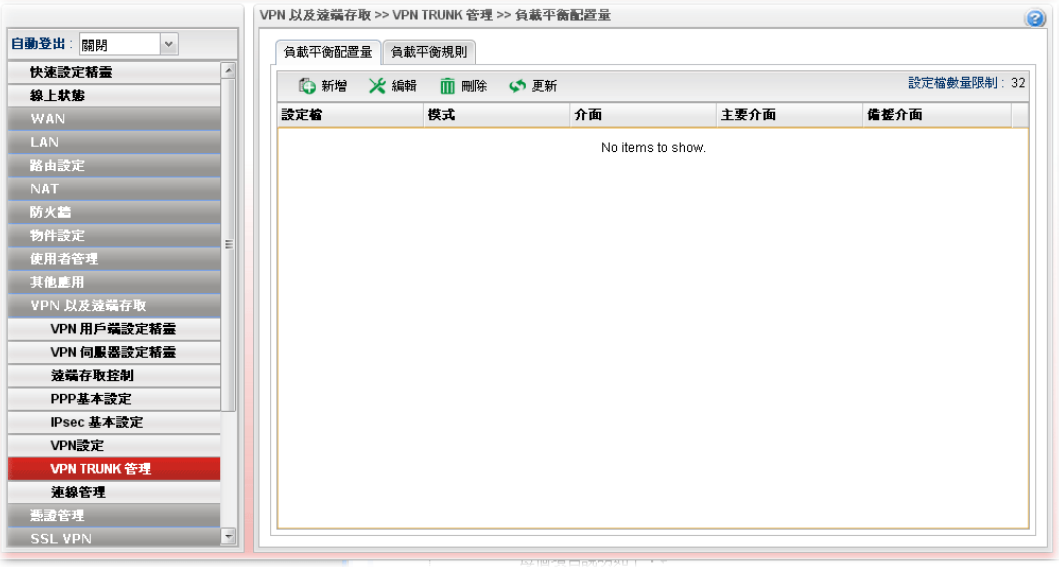
4.9.7 VPN Trunk 管理

VPN 負載平衡機制可以設定多重 VPN 通道，作爲流量負載平衡通道之用。它可依照實際的頻寬，幫助使用者確保多重 VPN 通道可以進行有效率的負載分享。另外，它還可提供三種不同的演算方式來運作負載平衡以及綁定通道策略機制，讓管理者管理網路更有彈性。



4.9.7.1 負載平衡配置量(Load Balance Pool)

本頁允許使用者整合數個 WAN 設定檔成爲一個配置設定檔，內含負載平衡或是備援應用等功能。

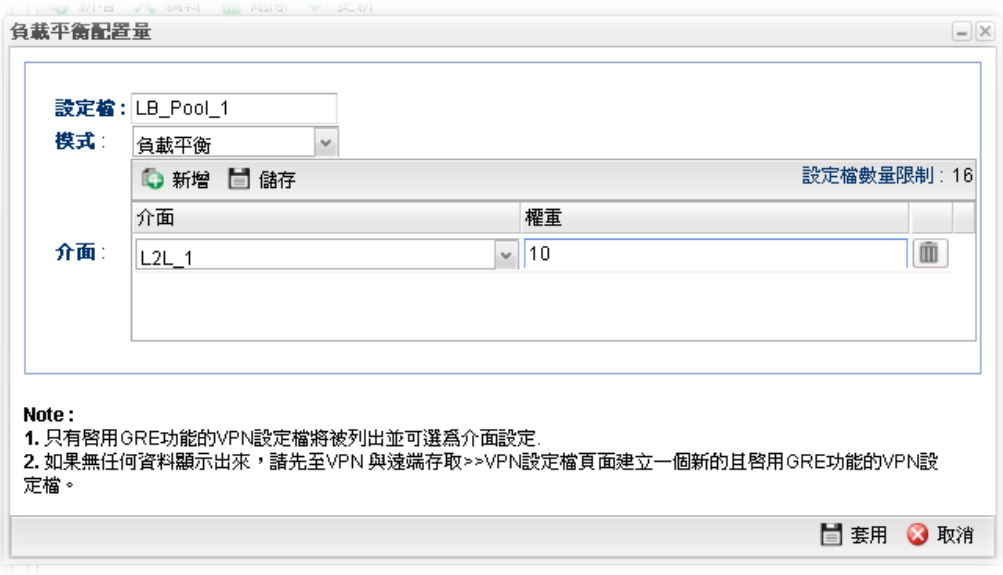


每個項目說明如下：

項目	說明
新增	新增新的設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
刪除	移除選定的設定檔。 請選擇您想要刪除的既有設定檔，然後按下刪除按鈕，該設定檔即可被移除。
更新	重新更新本頁面。
設定檔數量限制	顯示可以建立的設定檔總數。
設定檔	顯示設定檔的檔名。
模式	顯示選定的模式爲何(負載平衡或是備援)。
介面	顯示被群組在此配置量設定檔下的負載平衡設定檔名稱。
主要介面	顯示備援的主要介面。
備援介面	顯示用來備援的介面。

如何新增負載平衡配置量設定檔

1. 開啓 **VPN 與遠端存取>>VPN TRUNK 管理**並按下**負載平衡配置量**標籤。
2. 按下**新增**按鈕。
3. 下述頁面將會出現。



可用參數詳列如下：

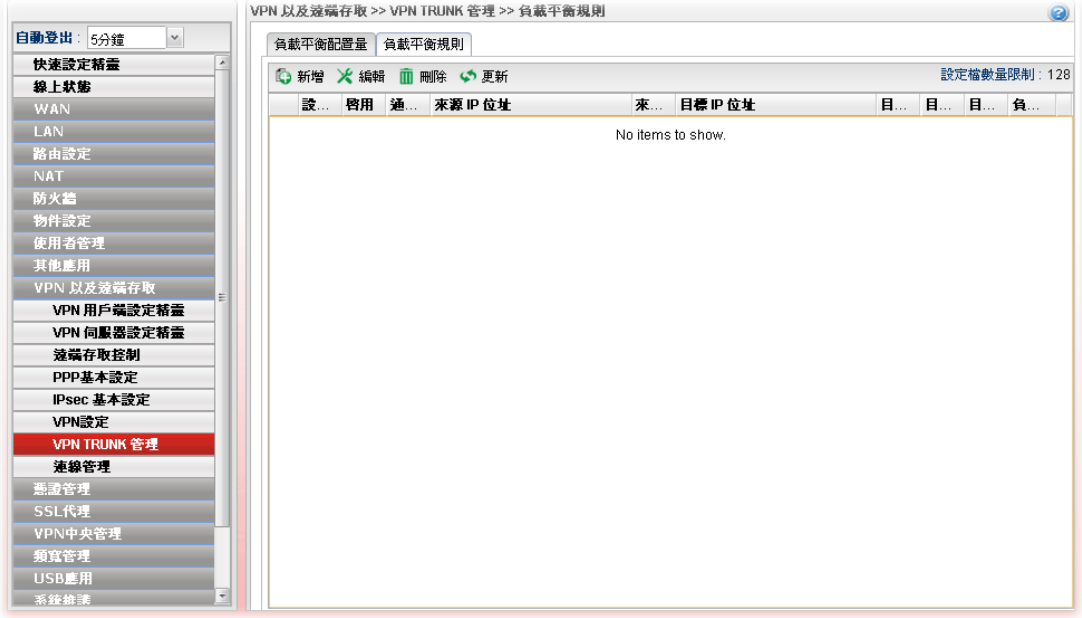
項目	說明
設定檔	輸入設定檔名稱(例如本例使用 LB_Pool_1)。
模式	選擇負載平衡或是備援模式。 **若選負載平衡** ● **介面**– 請選擇 VPN 設定檔作爲介面。 **注意**：只有含 GRE 功能的 VPN 設定檔且已被啓用，才會在此列出供您選取。如果此處沒有任何設定檔可供選擇，請至 **VPN 與遠端存取 >>VPN 設定檔**頁面先建立 VPN 設定檔，GRE 功能也務必要啓用。 ● **權重**– 在本區輸入全種植。 **若選備援** ● **主要介面/備援介面**– 使用下拉式清單分別指定 VPN 設定檔作爲主要與備援介面。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

重要！！如果介面選單中沒有任何選項出現，請務必回到 **VPN 以及遠端存取 >>VPN 設定檔**頁面先建立 VPN 設定檔，GRE 功能也務必要啓用。再回到此頁面繼續設定。

4. 輸入所有設定並按下**套用**儲存。
5. 新設定檔已經建立完成。

4.9.7.2 負載平衡規則(Load Balance Rule)

如要建立負載平衡規則以便與其他路由器進行 VPN 負載平衡連線，您可以在本頁面定義相關的設定。



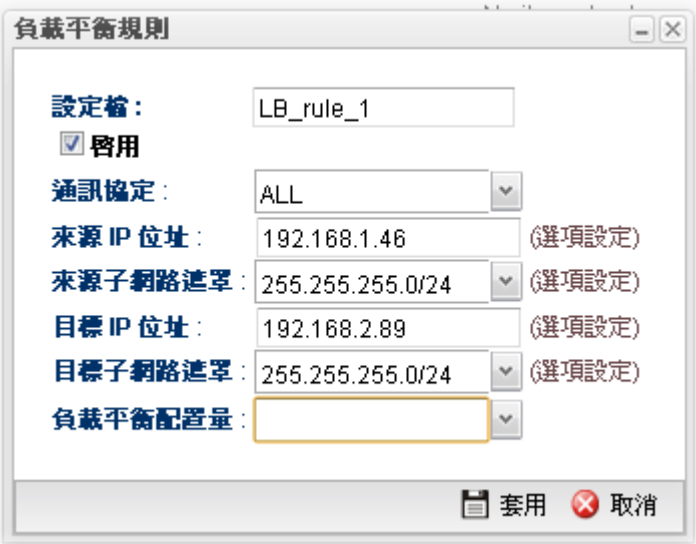
每個項目說明如下：

項目	說明
新增	新增新的設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
刪除	移除選定的設定檔。 請選擇您想要刪除的既有設定檔，然後按下刪除按鈕，該設定檔即可被移除。
更新	重新更新本頁面。
設定檔數量限制	顯示可以建立的設定檔總數。
設定檔	顯示設定檔的檔名。
啓用	顯示設定檔狀態，False 表示停用；True 表示啓用。
通訊協定	顯示設定檔使用的協定。
來源 IP 位址	顯示設定檔指定來源 IP 位址。
來源子網路遮罩	顯示設定檔指定來源遮罩位址。
目標 IP 位址	顯示設定檔指定目標 IP 位址。
目標子網路遮罩	顯示設定檔指定目標遮罩位址。
目標起始埠號	顯示設定檔之目標通訊埠起點值。

目標結束埠號	顯示設定檔目標通訊埠終點值。
負載平衡配置量	顯示負載平衡配置量選擇之設定檔。

如何新增負載平衡規則設定檔

1. 開啓 **VPN 與遠端存取>>VPN TRUNK 管理**並按下**負載平衡規則**標籤。
2. 按下**新增**按鈕。
3. 下述頁面將會出現。



可用參數詳列如下：

項目	說明
設定檔	輸入設定檔名稱(例如本例使用 LB_rule_1)。
啓用	勾選此框啓用此設定檔。
協定	選擇適當的協定。
來源 IP 位址	輸入此設定檔指定的來源 IP 位址。
來源子網路遮罩	選擇來源 IP 所需的遮罩位址。
目標 IP 位址	輸入此設定檔指定的目標 IP 位址。
目標子網路遮罩	選擇目標 IP 所需的遮罩位址。
目標起始埠號	輸入此設定檔的目標通訊埠起點值。
目標結束埠號	輸入此設定檔的目標通訊埠終點值。
負載平衡配置量	使用下拉式清單選擇負載平衡配置量所需之設定檔，其規則將套用到此配置量設定檔中。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

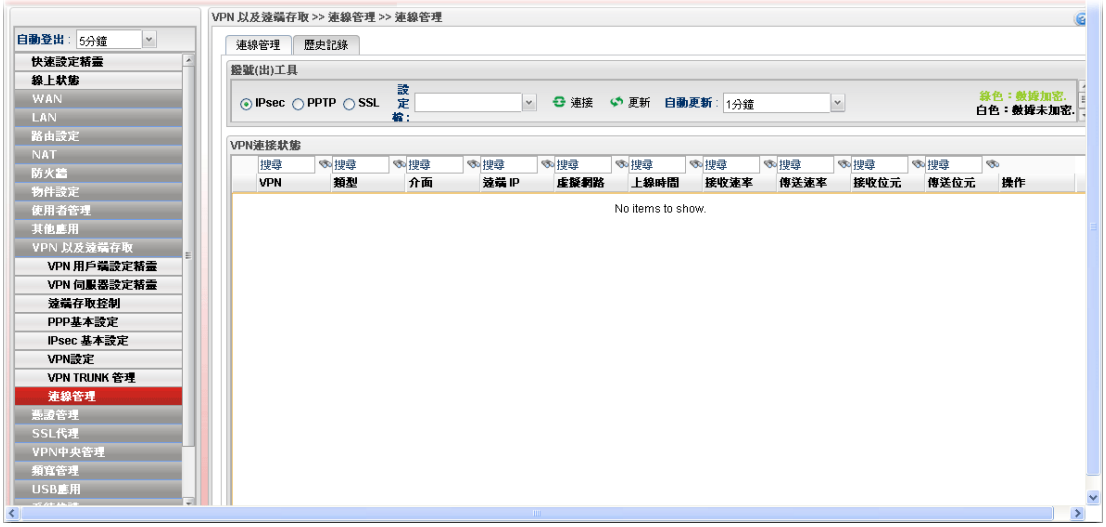
4. 輸入所有設定並按下**套用**儲存。

5. 新設定檔已經建立完成。

4.9.8 連線管理

4.9.8.1 連線管理

您可以在此查詢所有 VPN 連線的相關資訊，也能利用**中斷**按鈕切斷任何一條 VPN 連線。



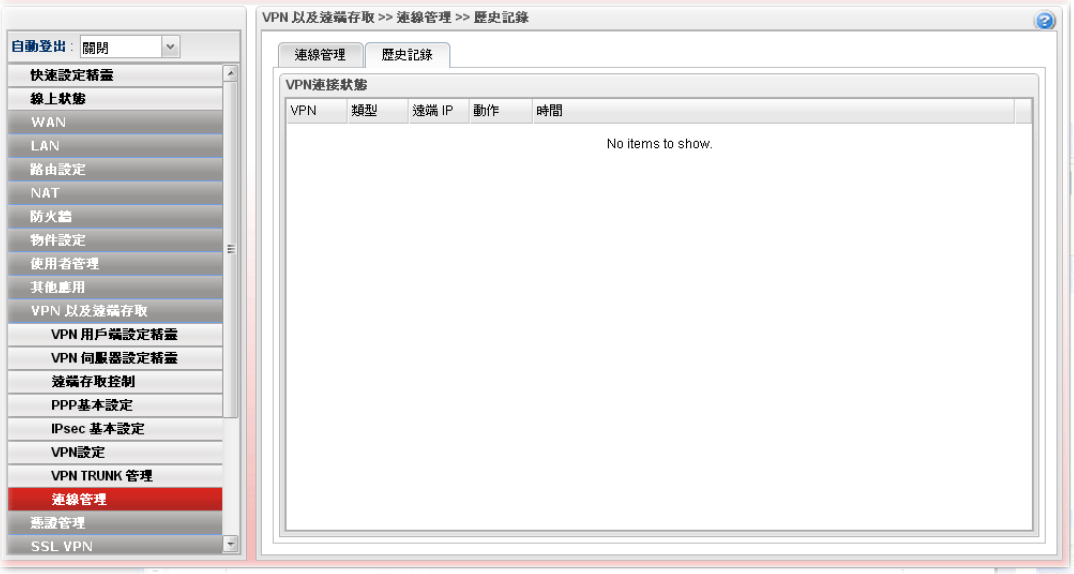
每個項目說明如下：

項目	說明
IPSec/PPTP/SSL	按此選擇 IPsec/**PPTP/SSL** VPN 連線。
設定檔	本區顯示在 LAN-to-LAN 中所配置的設定檔，由**基本模式**所建立的 VPN 連線不支援 VPN 備援功能。
連線	按此鈕執行撥出連線功能。
更新	按此更新本頁面。
自動更新	指定更新時間間隔以取得最新的狀態，若您按下**更新**按鈕，系統將立即更新資訊並呈現出來。
VPN	顯示 VPN 設定檔的名稱。
類型	顯示此 VPN 設定檔的連線類型(PPTP 或是 IPsec)。
介面	顯示此 VPN 設定檔的 WAN 介面。
遠端 **IP**	顯示此 VPN 設定檔的遠端 IP 設定。
虛擬網路	顯示此 VPN 設定檔建立的虛擬網路。
上線時間	顯示此 VPN 通道的連線時間。
接收速率/位元	顯示透過此 VPN 連線全部接收速度/封包數。
傳送速率/位元	顯示透過此 VPN 連線全部傳送速度/封包數。

操作	顯示此 VPN 設定檔的終止/檢視圖示。

4.9.8.2 歷史紀錄

本頁顯示 VPN 連線的歷程紀錄。



每個項目說明如下：

項目	說明
VPN	顯示 VPN 設定檔的檔名。
類型	顯示 VPN 連線的類型。
遠端	顯示 VPN 連線遠端 IP 位址。
動作	顯示 VPN 設定檔的連線狀態(上線或是下線)。
時間	顯示 VPN 連線/斷線的時間。

4.10 憑證管理

數位憑證就像是一個電子 ID，此 ID 可以由憑證授權中心註冊取得。它包含有您的名字、序號、到期日、憑證授權的數位簽章，這樣一來，接收者可以確認該憑證是否是真實的。本路由器支援遵守標準 X.509 的數位憑證。

任何想要使用數位憑證的人都應該先有 CA 伺服器註冊的憑證，此憑證也可從其他具公信力的 CA 伺服器取得，如此還可以驗證其他從公信力的 CA 伺服器取得憑證的另一方。

此處您可以管理產生本機的數位憑證，並設定具公信力之 CA 憑證，使用憑證前，請記得調整路由器的時間，這樣才可取得正確的憑證有效期。

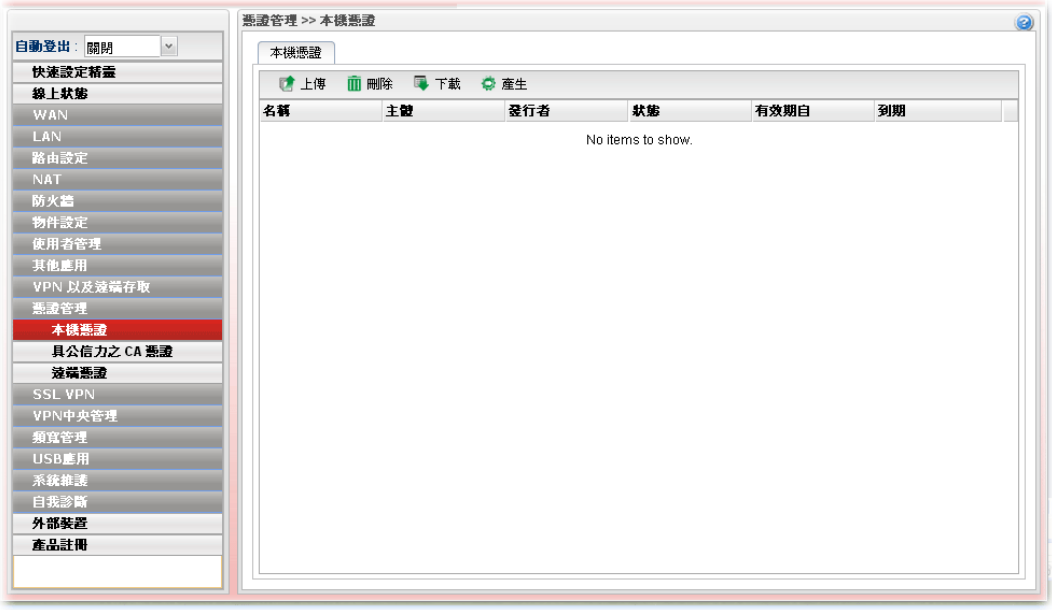
下圖顯示憑證管理選單內容：

L 本機憑證由使用者建立產生，且必須通過具公信力之 CA 憑證中心核可。Vigor2960 可以提供相似的服務，作爲具公信力之 CA 伺服器稱之爲“Root CA”，因此任何一個使用者都可以要求 Vigor2960 簽核申請的憑證。

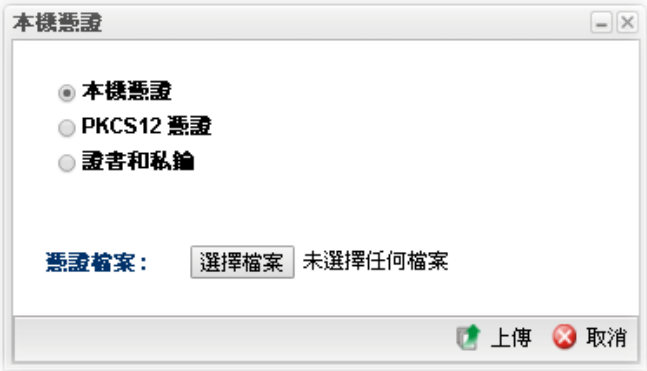
當 Vigor2960 提供“Root CA”服務時，它可以簽署來自使用者的憑證申請，首先按下具公信力之 CA 憑證已建立一個 Root CA，之後，來自其他使用者的憑證申請可以上傳到 Root CA(Vigor2960)上，然後由 Vigor2960 核可並簽署該憑證要求。

4.10.1 本機憑證

本頁讓使用者基於不同需求產生相關的憑證，本機憑證可自行簽署或是透過 root CA 伺服器(例如 Vigor2960 上的 root CA 伺服器)簽署憑證。



每個項目說明如下：

項目	說明
上傳	按下此鈕開啟如下對話盒以便上傳選定的憑證至路由器上。  在您選擇了憑證檔案類型之後，輸入必要資訊並選擇需求檔案(例如 Key Passphrase, Key File, PKCS12 密碼與 PKCS12 檔案)。 之後，按下**上傳**即可。
刪除	移除下方列表中選定的憑證項目。
下載	允許下載現有的本機憑證至路由器上。
產生	開啟另一個網頁以建立本機憑證。
名稱	顯示本機憑證名稱。

主題	顯示本機憑證的主題內容。
發行者	顯示本機憑證的發行者。
狀態	顯示本機憑證建立的狀態。
有效期自	顯示本機憑證有效期的起始點。
到期	顯示本機憑證有效其的截止點。

如何建立本機憑證

1. 開啓憑證管理>>本機憑證。
2. 按下產生按鈕。
3. 下述頁面將會出現。

可用參數詳列如下：

項目	說明
憑證名稱	輸入本機憑證的名稱。
ID 類型	此憑證的 ID 類型，共有數種可以設定： **Domain Name(網域名稱)**: 以網域來指定憑證。 **IP**: 以 IP 位址來指定憑證。 **電子信箱**: 以郵件信箱來指定憑證。 **無**: 不輸入任何 ID 值。
ID 值	ID 值依據上述選定的 ID 類型而定。 例如，您選擇的 ID 類型爲**網域名稱**，那麼請在此區域輸入網域名稱。

組織單位	輸入組織單位的簡易說明。
組織	輸入組織名稱。
位置 (城市)	輸入城市名稱。
洲/省	輸入洲/省的名稱。
常用名稱	輸入常用的名稱。
電子郵件位址	輸入郵件位址。
國家	輸入國家名稱。
密鑰大小	選擇密鑰所需的大小。
自簽名	**啓用** – 選此即可使用內建預設的憑證，該預設憑證主要用於 SSL VPN 伺服器與 HTTPS 網頁代理伺服器上。
CA 密鑰密碼	輸入文字做爲加密密碼。
套用	按此鈕建立新的本機憑證，以此處的設定爲基準。
取消	按此鈕離開對話盒，且不儲存任何設定。

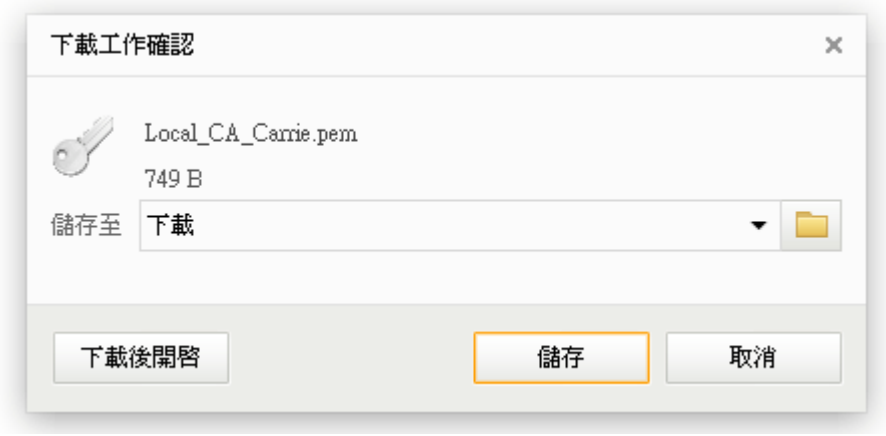
4. 輸入所有設定並按下**套用**儲存。
5. 新的本機憑證已建立完畢。

如何下載本機憑證至指定位置

路由器允許您產生憑證需求並提交至 CA 伺服器，在產生本機憑證之後，您可以將其下載至任何您想要儲存的地方。

如果您已經從第三方獲得了憑證，您也可以直接輸入該憑證至路由器上，支援的類型有 PKCS12 憑證以及加上私人密鑰的憑證。

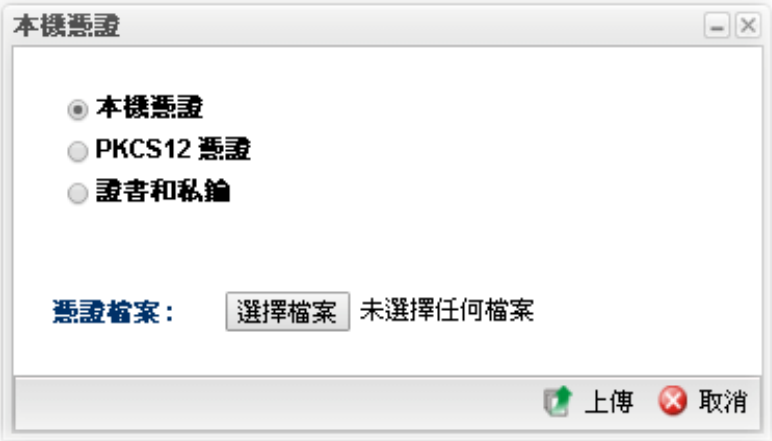
1. 開啓**憑證管理>>本機憑證**。
2. 指定憑證後按**下載**按鈕開啓如下視窗。



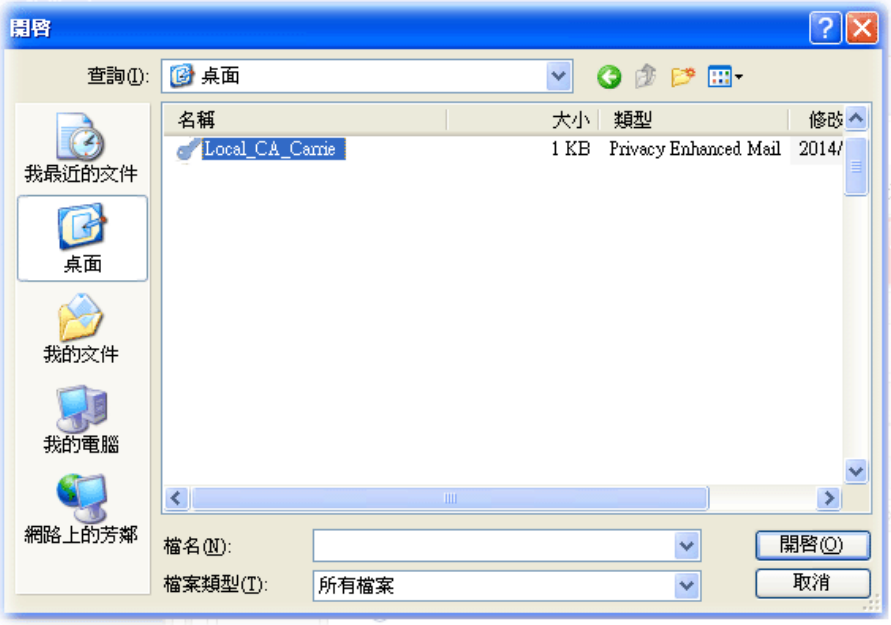
3. 接著按**儲存**，檔案將存放在指定的檔案夾中。

如何上傳本機憑證

1. 開啓**憑證管理>>本機憑證**。
2. 按**上傳**按鈕，開啓如下視窗。

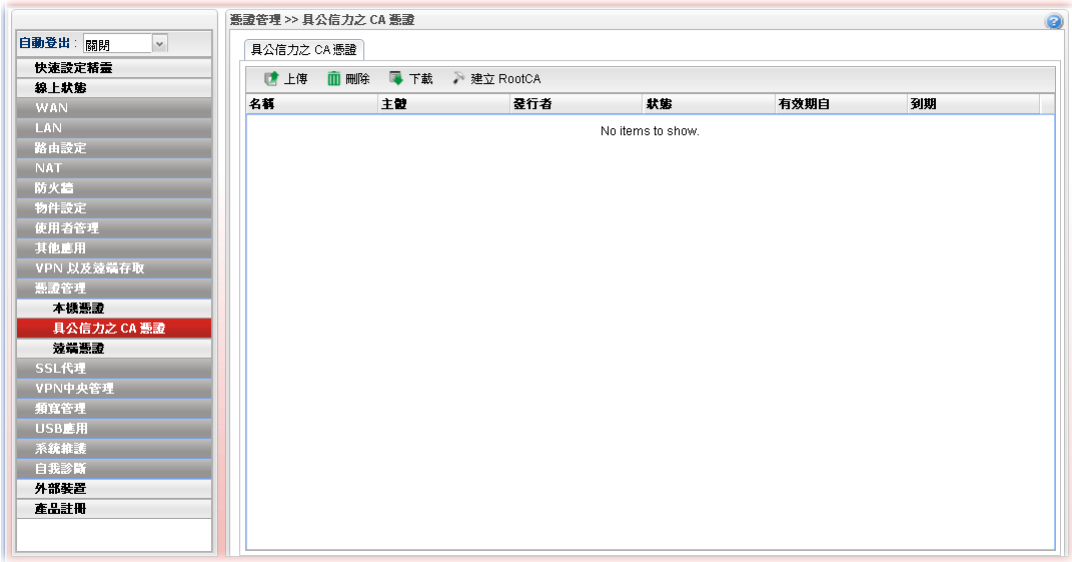


3. 按下**開啓**。選擇**本機憑證**並按下**選擇檔案**按鈕開啓如下對話盒。



4. 自上述對話盒中，選擇您要的憑證並按下**開啓**。
5. 按**上傳**，系統開始上傳選定的檔案。

4.10.2 具公信力之 CA 憑證



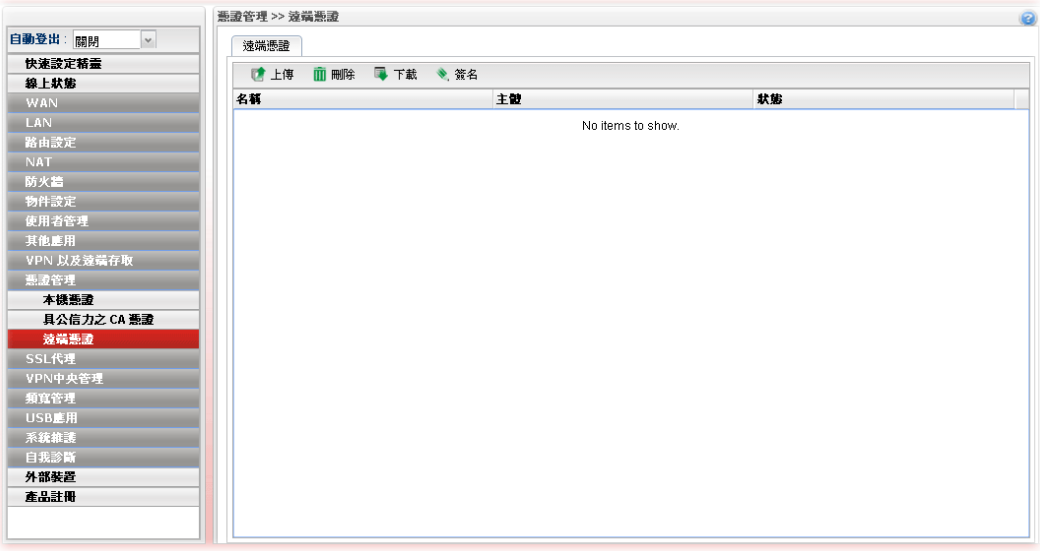
每個項目說明如下：

項目	說明
上傳	按下此鈕開啟如下對話盒以便上傳選定的憑證至路由器上。 在您選擇了憑證檔案類型之後，輸入必要資訊並選擇需求檔案(例如 Key Passphrase, Key File, PKCS12 密碼與 PKCS12 檔案)。 之後，按**上傳**即可。
刪除	移除下方列表中選定的憑證項目。
下載	下載既有具公信力的 CA 憑證至路由器上。
建立 RootCA	開啟另一個網頁以產生 CA 憑證。
名稱	顯示具公信力的 CA 憑證名稱。

主題	顯示具公信力的 CA 憑證的主題內容。
發行者	顯示具公信力的 CA 憑證的發行者。
狀態	顯示具公信力的 CA 憑證建立的狀態。
有效期自	顯示具公信力的 CA 憑證有效期的起始點。
到期	顯示具公信力的 CA 憑證有效其的截止點。

4.10.3 遠端憑證

本頁讓使用者上傳憑證至遠端用戶。



每個項目說明如下：

項目	說明
上傳	按下此鈕開啟如下對話盒以便上傳選定的憑證至路由器上。 在您選擇了憑證檔案類型之後，輸入必要資訊並選擇需求檔案(例如 Key Passphrase, Key File, PKCS12 密碼與 PKCS12 檔案)。 之後，按下**上傳**即可。

刪除	移除下方列表中選定的憑證項目。
選擇檔案	使用**選擇檔案**按鈕定某個檔案，作爲遠端憑證之用。
下載	下載既有具公信力的 CA 憑證至路由器上。
簽名	按此讓選定之檔案得以作爲憑證。
名稱	顯示遠端憑證名稱。
主題	顯示遠端憑證的主題內容。
狀態	顯示遠端憑證建立的狀態。

4.11 SSL 代理

SSL VPN (Secure Sockets Layer virtual private network) 是 VPN 形式的一種，它可與標準的網頁瀏覽器搭配使用。

SSL VPN 提供的好處有二：

- 使用者不需事先安裝 VPN 用戶端軟體以便進行 SSL VPN 連線
- 比起傳統 VPN，透過 SSL VPN 的資料加密限制較少

4.11.1 SSL 網頁代理

SSL 網頁代理伺服器可使遠端使用者透過 SSL 登入內部的網站。

每個項目說明如下：

項目	說明

新增	新增新的設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
刪除	移除選定的設定檔。 請選擇您想要刪除的既有設定檔，然後按下刪除按鈕，該設定檔即可被移除。
更新	重新更新本頁面。
設定檔數量限制	顯示可以建立的設定檔總數。
設定檔	顯示設定檔名稱。
URL	顯示設定檔的 URL。
主機 IP 位址	顯示主機的 IP 位址。

如何建立 SSL 網頁代理伺服器設定檔

1. 開啟 **SSL 代理>>SSL 網頁代理**。
2. 按下**新增**按鈕。
3. 下述頁面將會出現。

可用參數詳列如下：

項目	說明
設定檔	輸入設定檔的檔名。
URL	輸入代理伺服器的位址或是路徑。
主機 IP 位址	如果您輸入功能為 URL，您必須在本區輸入相應的 IP 位址，此區必須符合 URL 設定。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

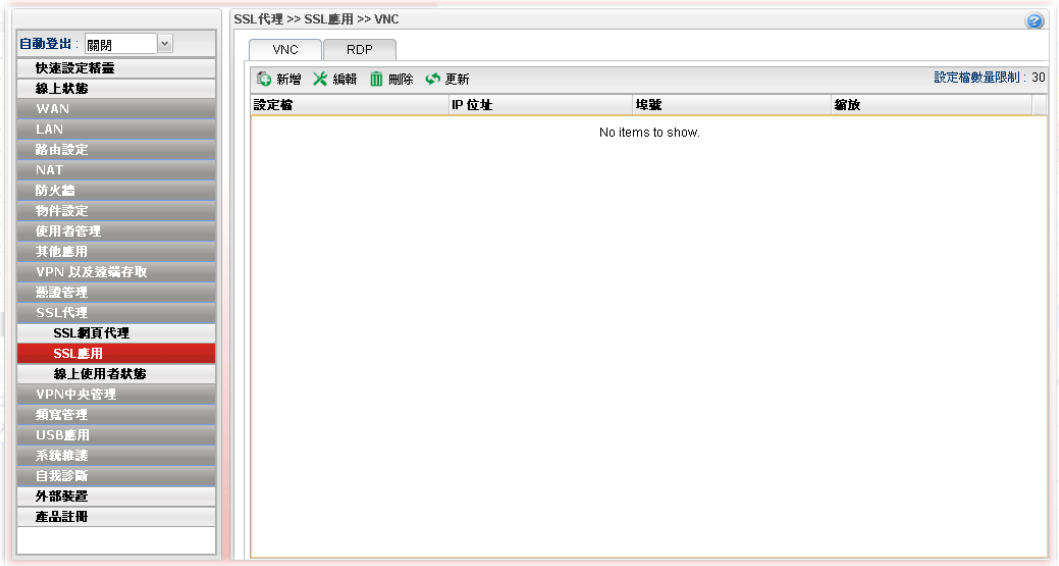
4. 輸入所有設定並按下**套用**儲存。
5. 新的設定檔已完成。

4.11.2 SSL 應用

對於遠端使用者，系統提供一個安全且彈性的網路資源使用方案，給予任何一個利用網際網路與網頁瀏覽器登入的遠端使用者，包含 VNC(虛擬網路計算)/RDP(遠端桌面協定)。

4.11.2.1 VNC

VNC(Virtual Network Computing) 表示虛擬網路計算，可讓您透過 VNC 協定存取並控制遠端電腦。



每個項目說明如下：

項目	說明
新增	新增新的設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
刪除	移除選定的設定檔。 請選擇您想要刪除的既有設定檔，然後按下刪除按鈕，該設定檔即可被移除。
更新	重新更新本頁面。
設定檔數量限制	顯示可建立的設定檔總數。
設定檔	顯示設定檔名稱。
IP 位址	顯示此協定的 IP 位址。
埠號	顯示協定的埠號值。
縮放	顯示此應用的百分比。

如何建立以 VNC 協定爲主的 SSL 應用設定檔

1. 開啓 **SSL 代理>>SSL 應用**並按下 **VNC** 標籤。
2. 按下**新增**按鈕。
3. 下述頁面將會出現。

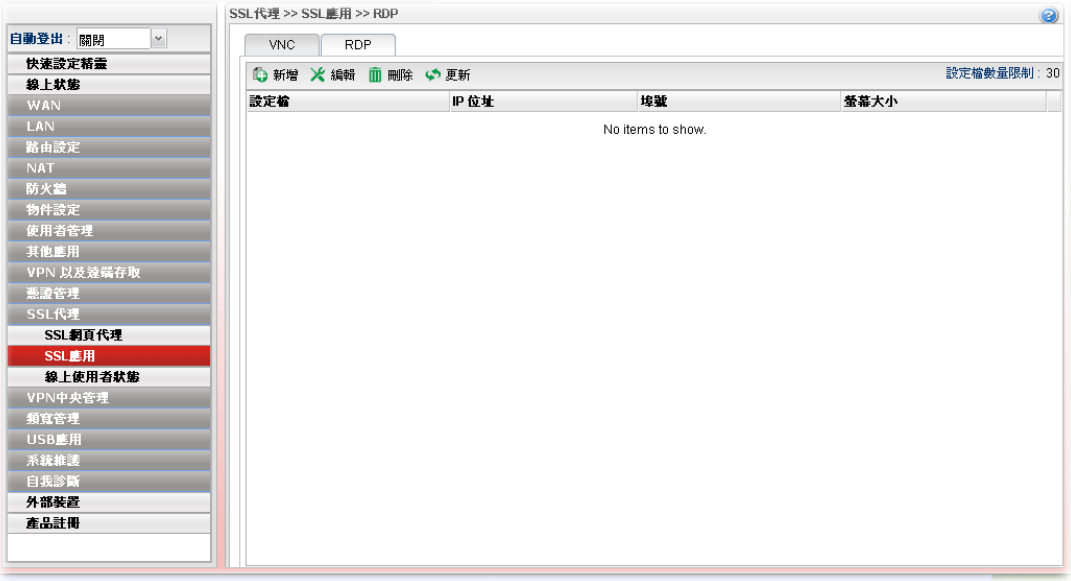
可用參數詳列如下：

項目	說明
設定檔	輸入此協定的的設定檔名。
IP 位址	輸入此協定的 IP 位址。
埠號	輸入此協定的埠號值，預設值爲 5900。
縮放	選擇百分比選項 100%, 80%, 60%。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

4. 輸入所有設定並按下**套用**儲存。
5. 新的 SSL 應用程式設定檔已建立。

4.11.2.2 RDP

RDP(Remote Desktop Protocol) 表示遠端桌面通訊協定，可讓您透過 RDP 協定存取並控制遠端電腦。



每個項目說明如下：

項目	說明
新增	新增新的設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
刪除	移除選定的設定檔。 請選擇您想要刪除的既有設定檔，然後按下刪除按鈕，該設定檔即可被移除。
更新	重新更新本頁面。
設定檔數量限制	顯示可建立的設定檔總數。
設定檔	顯示設定檔名稱。
IP 位址	顯示此協定的 IP 位址。
埠號	顯示協定的埠號值。
螢幕大小	顯示設定檔的螢幕尺寸。

如何建立以 RDP 協定爲主的 SSL 應用設定檔

1. 開啓 **SSL 代理>>SSL 應用**並按下 **RDP** 標籤。
2. 按下**新增**按鈕。
3. 下述頁面將會出現。

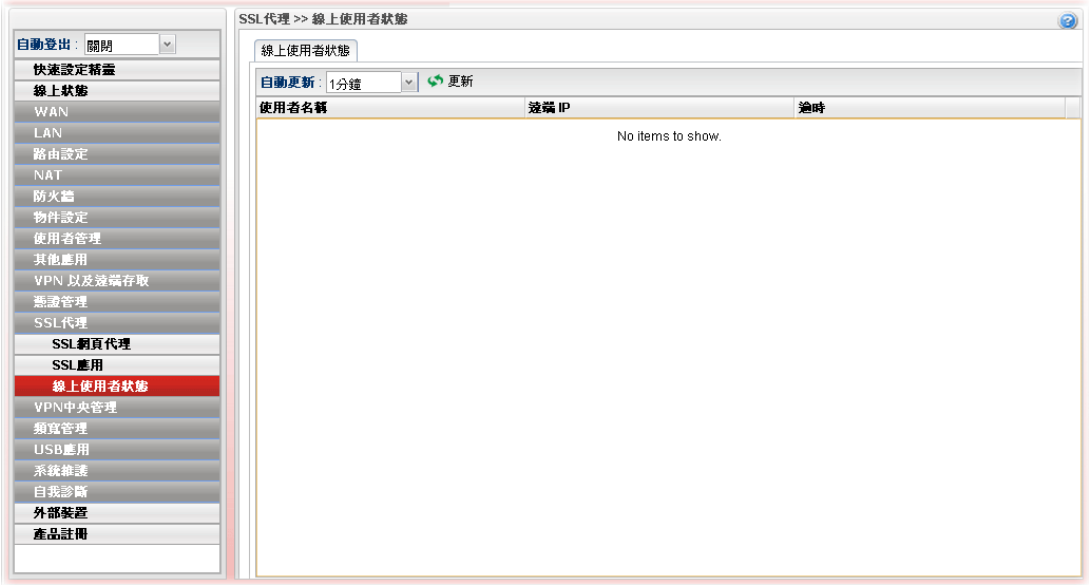
可用參數詳列如下：

項目	說明
設定檔	輸入此協定的的設定檔名。
IP 位址	輸入此協定的 IP 位址。
埠號	輸入此協定的埠號值。
螢幕大小	選擇適合的尺寸大小。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

4. 輸入所有設定並按下**套用**儲存。
5. 新的 SSL 應用程式設定檔已建立。

4.11.3 線上使用者狀態

如果您已經完成 SSL 網頁代理伺服器的設定，當使用者登入居易 SSL 代理介面時，將可以看到相應的設定內容。



每個項目說明如下：

項目	說明
自動更新	指定更新本頁狀態的時間間隔。
更新	重新更新本頁面。
使用者名稱	顯示目前造訪 SSL VPN 伺服器的用戶。
遠端 IP	顯示主機的 IP 位址。
逾時	顯示登出的剩餘時間。

4.12 VPN 中央管理

Vigor2960 能夠在自身與其他遵循 TR-069 標準的 CPE 之間，透過中央 VPN 連線管理功能建立虛擬私人網路(VPN)。此外，Vigor2960 還可以被視爲伺服器(稱爲 CVM 伺服器)，管理多重 TR-069 CPE 並定期執行韌體更新、設定備存與設定還原等作業。

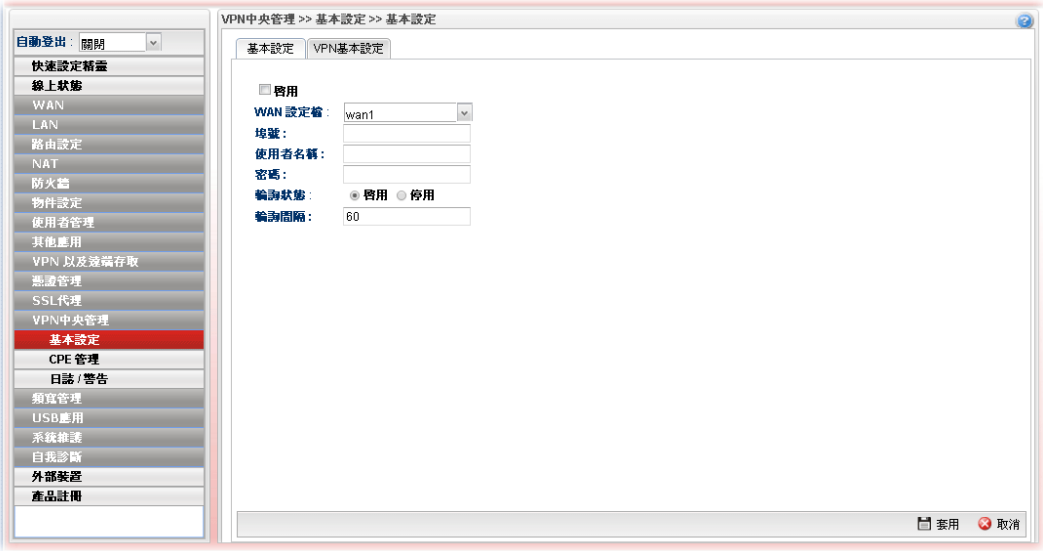
下圖爲可設定的選單內容：

注意：	1. 此選單僅能管理透過 WAN 介面連接的 CPE。 2. 最多可達 12 台 CPE 裝置可以同時納入管理。

4.12.1 基本設定

4.12.1.1 基本設定

本頁用來設定用戶向 Vigor 路由器登錄註冊所需的相關內容。

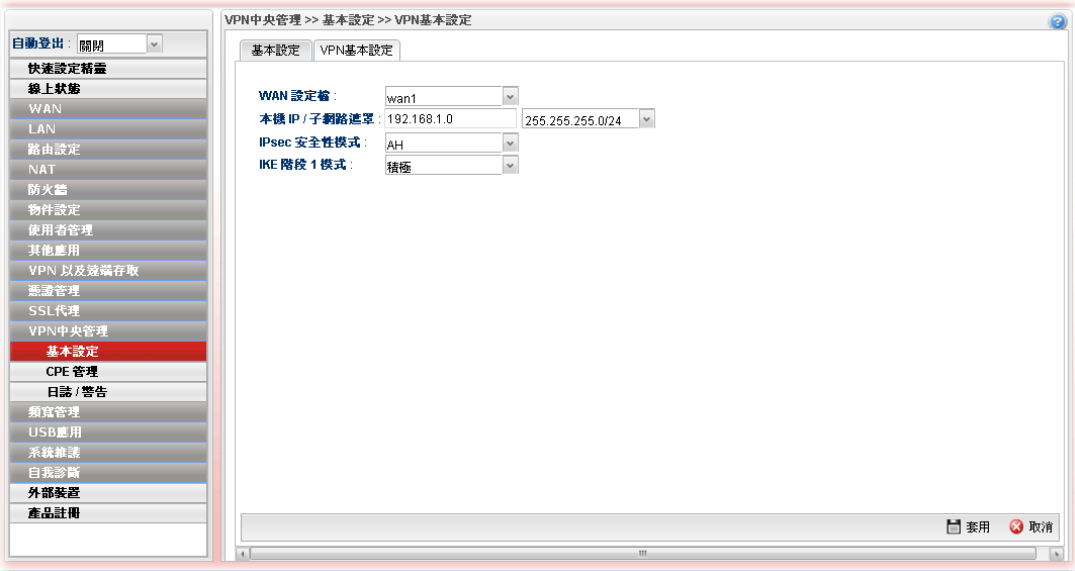


可用參數詳列如下：

項目	說明
啓用	勾選此框啓用此設定。
WAN 設定檔	指定 VPN 管理需求的 WAN 介面設定檔。
埠號	輸入 Vigor2960 需求埠號。
使用者名稱	輸入任何一台 CPE 嘗試連接至 Vigor 路由器時需要鍵入的使用者名稱。
密碼	輸入任何一台 CPE 嘗試連接至 Vigor 路由器時需要鍵入的密碼。
輪詢狀態	啓用 – 選擇此項啓用此功能。 停用 – 選擇此項停用此功能。
輪詢間隔	輸入時間值(單位爲秒)，可調範圍在 60 ~ 86400 之間。
套用	按此鈕儲存設定。
取消	按此鈕捨棄頁面設定。

4.12.1.2 VPN 基本設定

本頁可設定 Vigor2960 的 VPN 基本參數值。



可用參數詳列如下：

項目	說明
WAN 設定檔	選擇 WAN 介面設定檔以應 VPN 連線之需。
本機 IP/子網路遮罩	輸入本機主機的 IP 位址與子網遮罩。
IPsec 安全性模式	有關資料傳輸安全性部份，自下拉式清單中選擇一種方法來防護，例如選擇 AH 以便指定 AH 協定中所需的 IPsec 協定，資料會受到驗證防護而非加密保護。
IKE 階段 1 模式	可選擇**積極(Aggressive)** 或是**主要(Main)**。
套用	按此鈕儲存設定。
取消	按此鈕捨棄頁面設定。

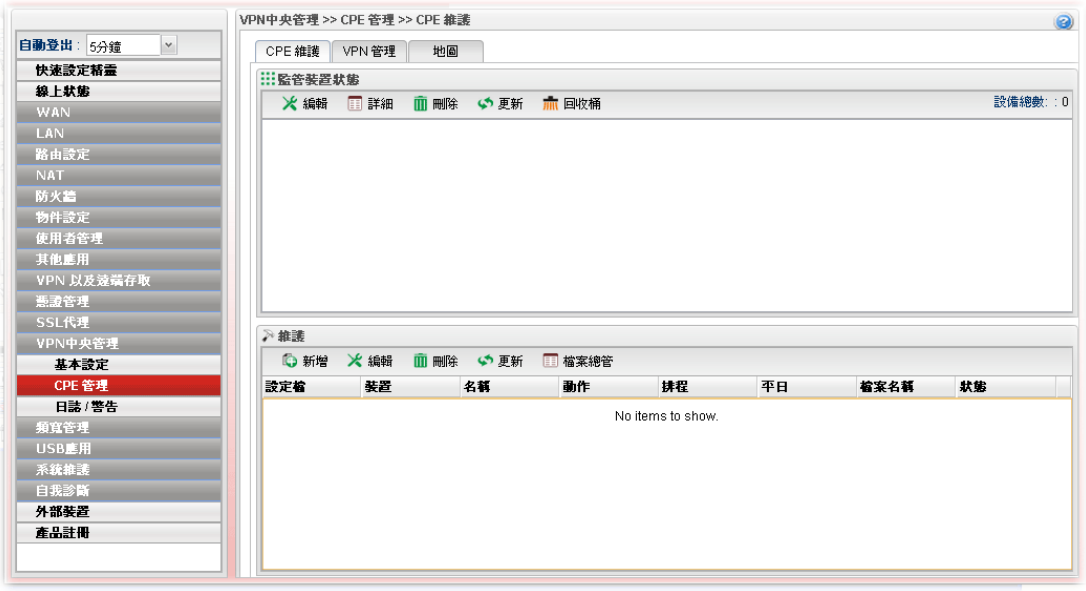
4.12.2 CPE 管理

所有 Vigor2960 管理下的 CPE 都會在本頁中以小圖示的方式呈現出來。

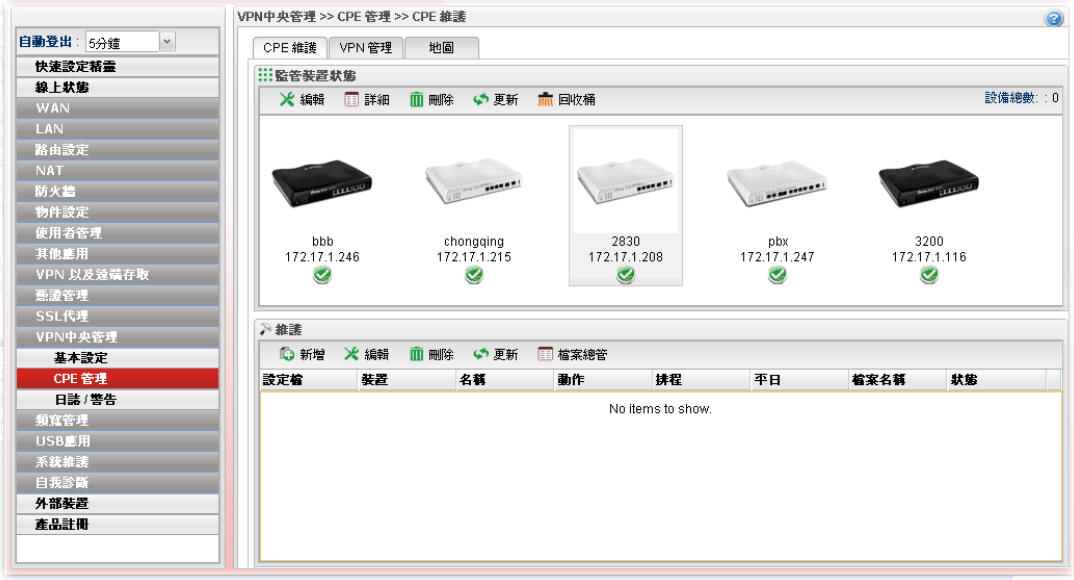
4.12.2.1 CPE 維護

本頁可讓您管理連接至 Vigor2960 的 CPE。

- CPE 尚未連接至路由器的頁面

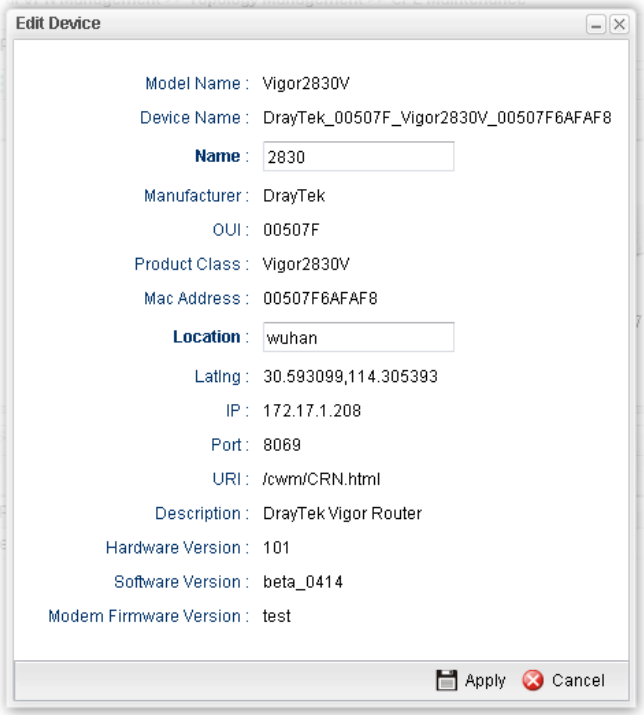


- CPE 已經連接至路由器的頁面



可用參數詳列如下：

項目	說明
監管裝置狀態	本區顯示 Vigor2960 管理之下的所有 CPE，以小圖示呈現。 **編輯** – 欲修改某 CPE 名稱與位置，選擇您準備修改的 CPE 圖示，然後按下此**編輯**按鈕，可彈跳出相關視窗，

	只要手動直接修改名稱(辨識用)與位置，最後按下**套用**即可完成編輯。  **細節** – 顯示出與編輯按鈕相同的資訊，不過無法進行任何變動。 **刪除** – 如要中斷任何 CPE 與 Vigor2960 之間的連結，按下該 CPE 圖示然後按此**刪除**按鈕即可。 **頁面** – 按此重新整理此頁面。 **回收桶** – 所有刪除的 CPE 都會先暫存某處等候管理者重新取回，這對不小心誤刪的情況來說是相當有用的補救方式。 如果您想要取回某一個 CPE，按下其圖示開啓另一個視窗，刪除的 CPE 連帶相關訊息都將會呈現在螢幕上，選擇您想要取回的機種然後按下還原(Restore)，稍後，選定的圖示將再次出現在**監管裝置狀態**區。
維護	本區顯示所有建立用來套用至管理裝置的設定檔。 **新增** – 欲新增設定檔，按下此鈕開啓另一視窗。 **編輯** – 欲修改現有的設定檔，選擇您想要變更的檔案再按下此鈕，開啓編輯視窗。 **刪除** – 欲捨棄任何現有的設定檔，選擇您想要刪除的檔案再按下此鈕。 **更新** – 按此鈕更新頁面。 **檔案總管** – 按此開啓檔案瀏覽畫面，可用的韌體將呈現在頁面上。 **設定檔** – 顯示設定檔的檔名。 **裝置** – 顯示此設定檔選定的名稱(由 Vigor3900 命名)。

	名稱 – 顯示裝置的名稱(可讓管理者自由更改)。 **動作** – 顯示此設定檔所執行的動作爲何。 **排程** – 顯示此設定檔爲 Vigor 路由器執行的頻率。 **平日** – 顯示此設定檔被實施的平常日有哪些。 **檔案名稱** – 顯示韌體的檔案名稱。 **狀態** – 顯示設定檔的目前的執行狀態爲完成或是未完成。

參考章節**"3.4 如何透過 Vigor2960 管理 CPE (路由器)?"** 以及 **"3.6 如何透過 Vigor2960 更新遠端 CPE 韌體?"** 取得更多資訊。

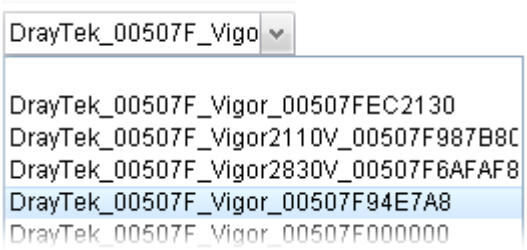
如何新增維護設定檔

依照下述步驟建立新的維護設定檔。

1. 按下**維護**區域中的**新增**按鈕。
2. 維護對話盒如下：

可用參數詳列如下：

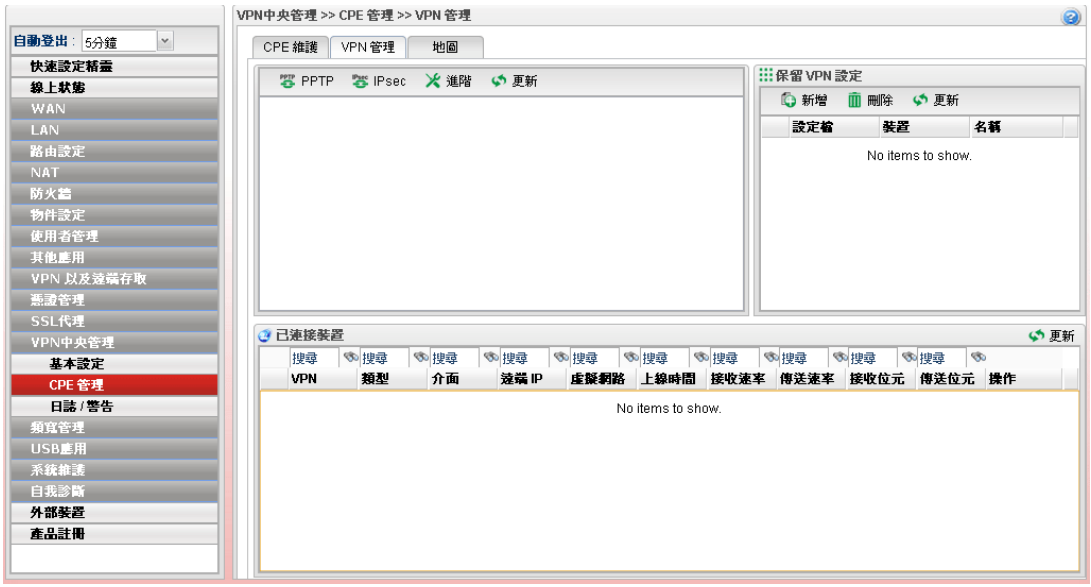
項目	說明
設定檔	輸入設定檔的檔名。
裝置	下拉式清單將呈現所有受到 Vigor2960 管理的裝置，選擇您想套用新的設定檔的裝置。

	 通常，裝置名稱都是 Vigor2960 自動命名，如果您想要給予簡單好記的名稱，可參考 4.11.2.1 CPE 維護章節以指定其他名稱。
名稱	顯示裝置的名稱(管理者可以變更)。
動作	有三種動作可以選擇： **韌體更新(Firmware Upgrade)** – 選擇此項即表示此設定檔將用於韌體更新。 **設定備份(Configuration Backup)** – 選此項即表示此設定檔將用於 CPE 的設定備份上。 **設定還原(Configuration Restore)** – 選此即表示此設定檔將用於 CPE 的設定還原上。
排程	新建立的設定檔可以套用到選擇的 CPE，依照此處排程設定的時間進行。 **現在** – 此動作立即更新 CPE。 **一次** – 此動作可對選定的 CPE 於指定的期間內執行動作一次。 **平日** – 此動作可對選定的 CPE 於每週固定時段(平日)執行更新。
起始日期/結束日期	這個選項僅在**排程**選擇**一次**時可用。 指定起始與結束日期，輸入格式為(西元年月日 YYYY-MM-DD)。
起始時間/結束時間	這個選項僅在**排程**選擇**一次**時可用。 指定起始與結束時間，輸入格式為時-分-秒。
平日	這個選項僅在**排程**選擇**平日**時可用。挑選您要的項目即可。
檔案名稱	輸入準備用於檔案更新、設定備份與設定還原的檔案完整名稱。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

3. 輸入所有設定並按下套用儲存。
4. 新的維護設定檔已完成建立。

4.12.2.2 VPN 管理

Vigor2960 提供一個簡易的方式，用於建立 Vigor2960(視爲 VPN 伺服器) 與其他 Vigor 路由器(視爲 CPE 裝置) 之間的 VPN 通道。



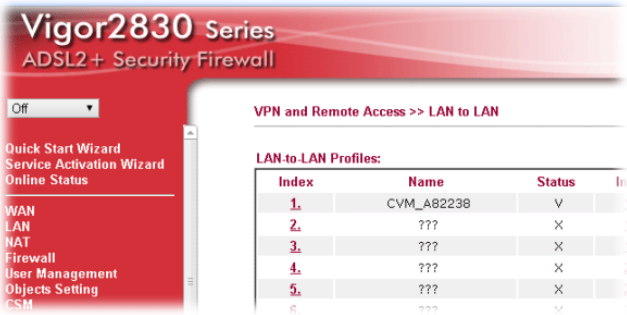
可用參數詳列如下：

項目	說明
顯示螢幕	一旦某裝置納入 Vigor2960 的管理下，它會自動呈現在顯示螢幕上，如果沒有任何圖示的話，請參考”**3.4 CVM 應用 – 如何透過 Vigor2960 管理 CPE (路由器)?**”取得進一步的訊息。 如果 VPN 無法成功建立，螢幕就會出現紅線來表示聯線失敗。
PPTP	建立快速的 **IPsec** VPN 連線，請先按遠端 CPE 圖示(請等候圖示稍微變大)再按下此按鈕，如果連線成功，畫面上會出現綠色的線條。
IPsec	建立快速的 **IPsec** VPN 連線，請先按遠端 CPE 圖示(請等候圖示稍微變大)再按下此按鈕，如果連線成功，畫面上會出現藍色的線條。
進階	建立含細部資訊(例如 PPP 驗證與 VJ 壓縮等) 的 VPN 連

線，請按**進階**按鈕。

自**裝置**一欄中選擇您要的 CPE 裝置，接著選擇**撥號類型**(會帶出不同的相關設定)。

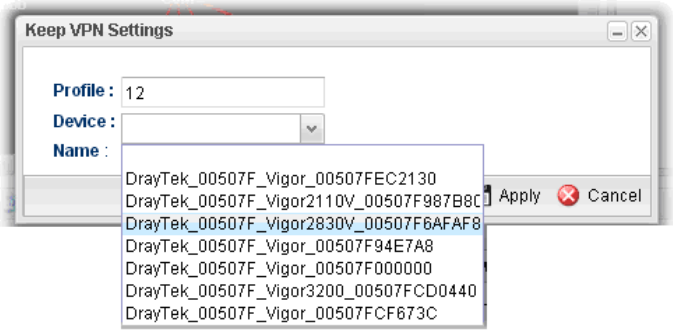
注意: 如果 VPN 連線已經成功建立，新的 LAN to LAN 設定檔將會自動於 CPE 端產生，請參考下圖：



保留 VPN 設定

爲了避免因爲用戶端設定變更而造成 VPN 斷線，可於此區進行維持 VPN 連線的狀態的相關設定。

新增 – 按下此鈕開啓如下對話盒，輸入設定檔名稱，選擇 CPE 裝置，然後按套用儲存。此設定檔後續將可用在以 VPN 連線方式和 Vigor2960 相連的 CPE 裝置。



刪除 – 按此紐刪除設定檔，路由器與用戶端之間的 VPN 連線將不保證仍能繼續維持

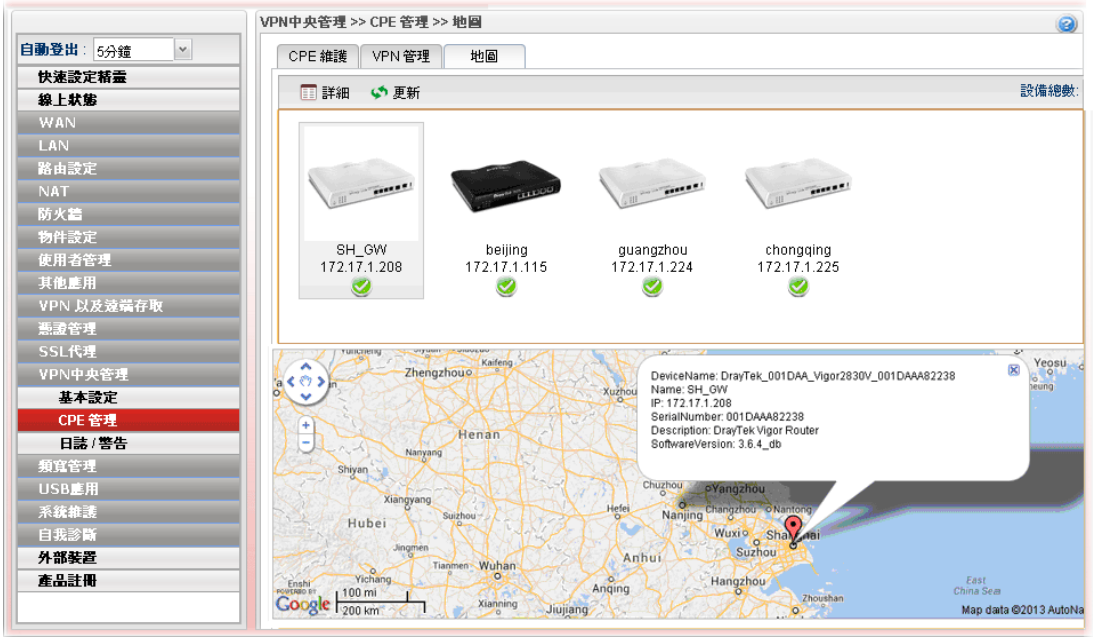
更新 – 按此更新目前頁面資訊。

設定檔 – 顯示目前使用的設定檔的檔名。

	裝置 –VPN.顯示透過 VPN 與路由器連接的 CPE 身分。 **名稱**– .顯示裝置的名稱(管理者可以手動變更此名稱)，詳細資訊請參考第 4.11.2.1 節 。
已連接裝置	VPN 一旦建立成功，基本資訊就會顯示在本區中。 **更新** – 按此鈕更新目前頁面。 **VPN –** 顯示 VPN 的名稱。 **類型** – 顯示連線模式。 **介面** – 顯示 WAN 介面。 **遠端 IP –** 顯示遠端用戶的 IP 位址。 **虛擬網路** – 顯示 Vigor2960 的 IP 位址。 **上線時間**– 顯示 VPN 目前連線的時間。 **傳送速率/位元**以及**接收速率/位元** – 顯示此 VPN 所交換的封包資訊。 **操作** – 按下此區的按鈕進行字面顯示的動作(例如中斷連線)。

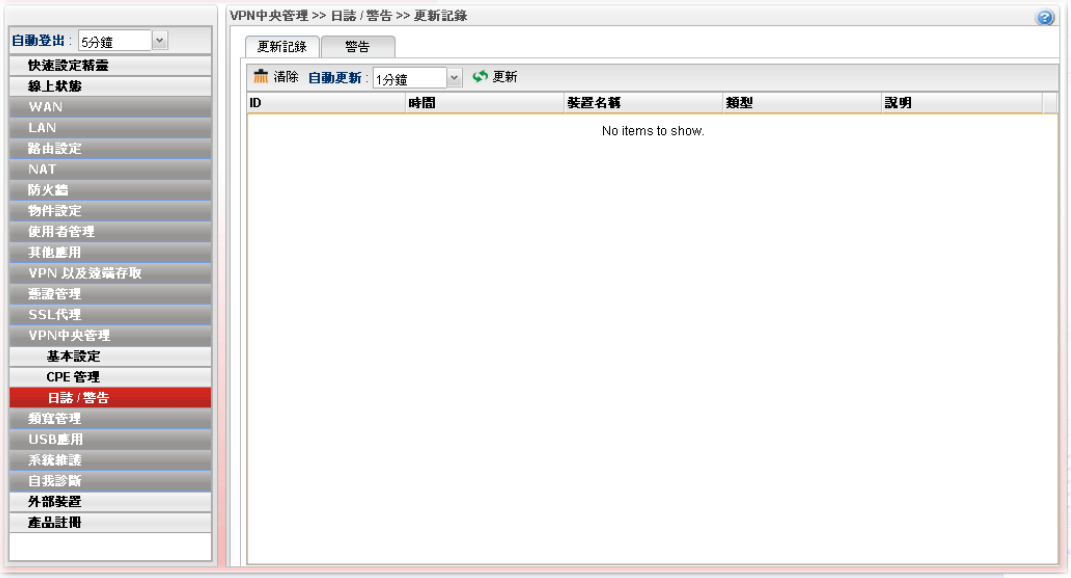
4.12.2.3 地圖

欲以鳥瞰的方式顯示出選定 CPE 的位置，請開啓 **VPN 中央管理>>CPE 管理**然後按**地圖**標籤。

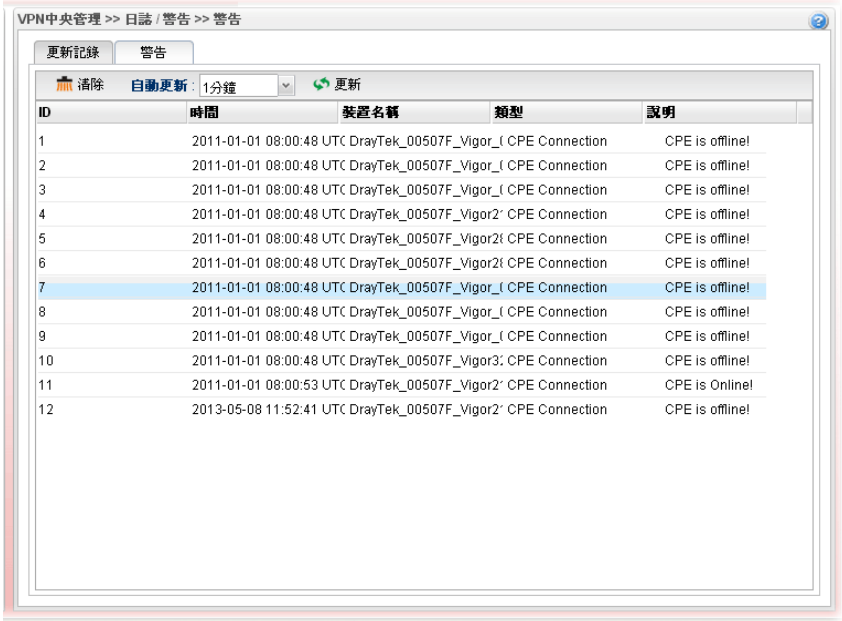


4.12.3 日誌/警告

本頁提供簡易資訊以辨識連接至 Vigor2960 的 CPE 為何。



下圖為警告頁面。



4.13 頻寬管理

下面是頻寬管理的設定項目：

Vigor 路由器中的 QoS (Quality of Service) 技術可讓網路管理者即時監控、分析並分派頻寬以因應不同網路流量與/或關鍵業務的流量。因此，不會因為受到網頁或是其他較不重要的應用諸如檔案傳輸等瞬間爆量，從而破壞了那些容易受到時機敏感影響之應用。在沒有 QoS 擔保控制下，幾乎沒有什麼辦法可以讓某些用戶/服務得到優先處理的機會，也無法擔保具有時機敏感和關鍵任務之網路應用像是 VoIP 與線上遊戲等，在有限的頻寬下能取得網路或服務頻寬分配。

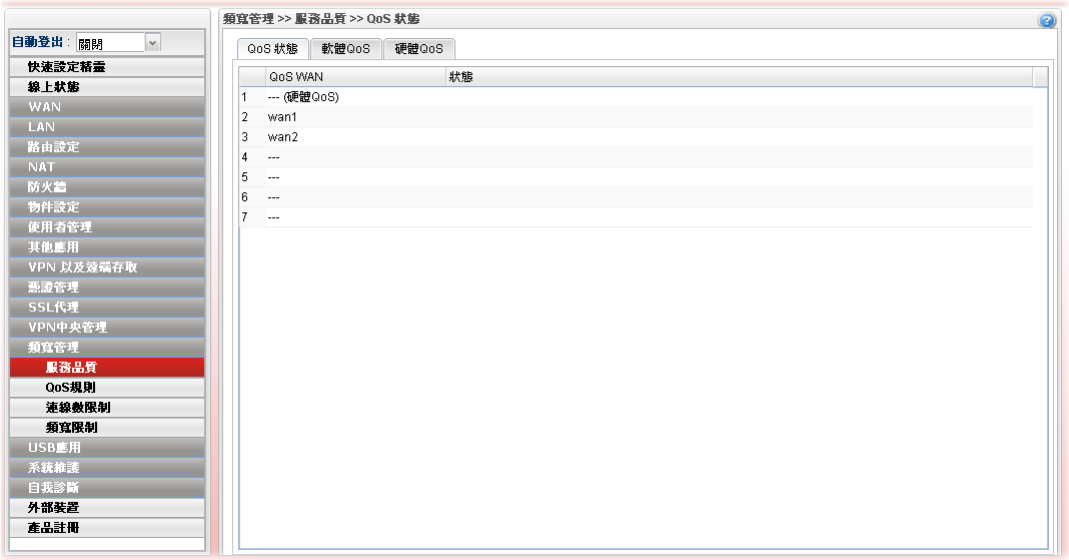
因此差異化的服務品質是網際網路基礎建設中最重要的議題當中的其中一個，在 QoS 控制模組的設計當中，也同時需要考量納入 DSCP (Differentiated Service Code Point)支援。

4.13.1 服務品質

QoS 功能分別掌控著輸入與輸出等級，使用者可以個別設定輸入或是輸出內容，而無須擔憂其彼此互相牽制影響。

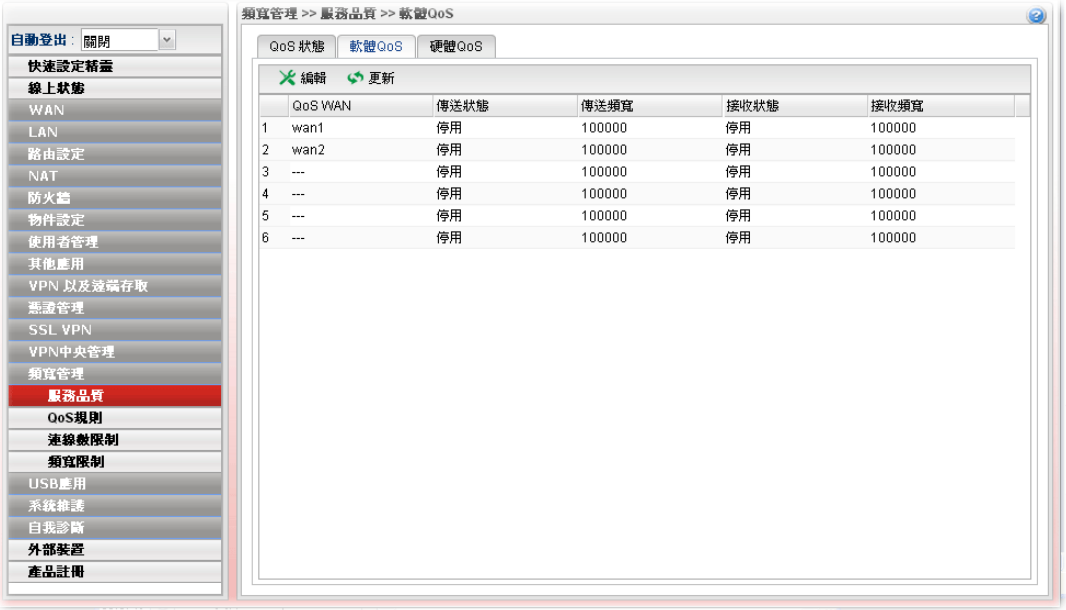
4.12.1.1 QoS 狀態

本頁顯示 QoS 狀態內容。



4.13.1.2 軟體 QoS

本頁顯示目前軟體 QoS 狀態以及讓您編輯每個 QoS WAN 的相關的設定，像是頻寬、順序(高、中與低) 等等。



可用參數詳列如下：

項目	說明
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
更新	重新更新本頁面。
QoS WAN	顯示 QoS 使用的 WAN 介面。
傳送狀態	顯示傳送資料的頻寬為啓用或是停用。
傳送頻寬	顯示資料傳送的傳輸速率的總額。
接收狀態	顯示資料接收的傳輸速率的總額。
接收頻寬	顯示接收資料的頻寬為啓用或是停用。

如何編輯 QoS 設定檔

依照下述步驟編輯維護設定檔。

1. 點選任何一個 QoS WAN 設定檔。
2. 按下**編輯**。

3. QoS 設定頁面顯示如下：

可用參數詳列如下：

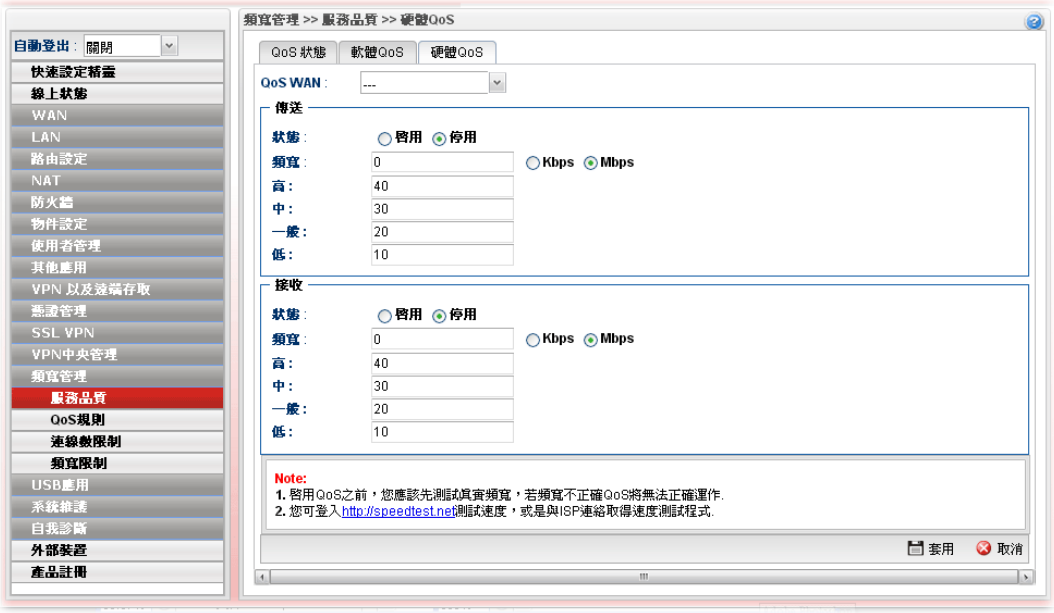
項目	說明
QoS WAN	使用下拉式清單選擇 WAN 介面。
狀態	啓用 – 按此啓用此 QoS 設定檔。 停用 – 按此停用此 QoS 設定檔。
頻寬	指定輸入/輸出資料的總傳輸速率，範圍由 64000 到 10000000。按 Kbps 或 Mbps 指定傳輸速率單位。
高/中/一般/低	有數種輸出順序可供選擇，資料群組中的佇列可以權重值 0 進行初始化。 輸入佇列的權重值，單位爲位元。範圍由 0 到 1000000。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

4. 輸入所有設定並按下**套用**儲存。

4.13.1.3 硬體 QoS

本頁讓您設定透過硬體介面執行資料傳送與接收(資訊與聲音訊號)的傳輸頻寬。

注意：硬體 QoS 與軟體 QoS 的差別在於硬體 QoS 僅支援一個 WAN 介面，但軟體介面卻支援六個 WAN 介面。



可用參數詳列如下：

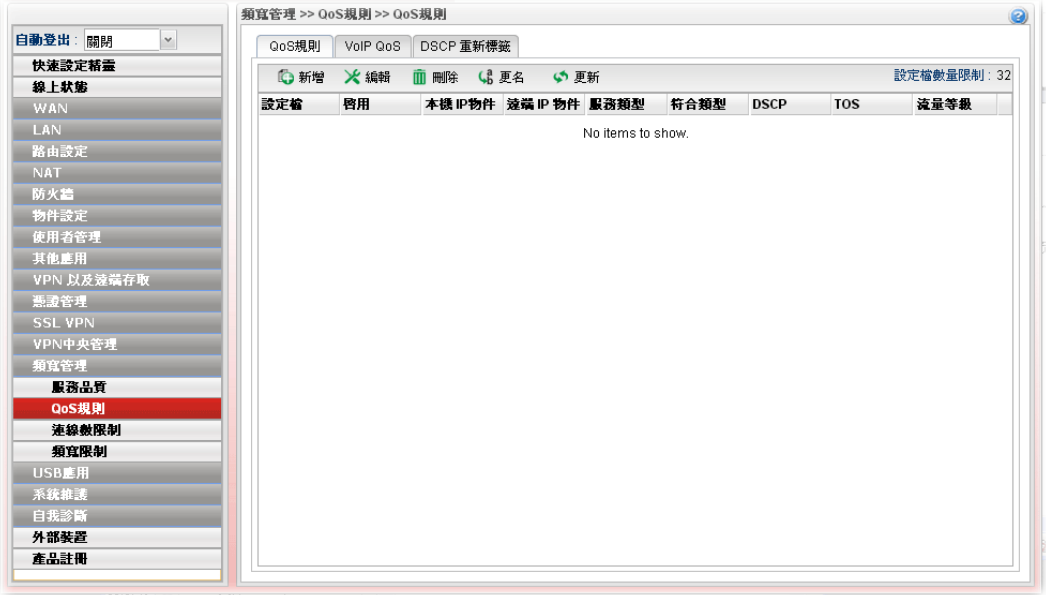
項目	說明
QoS WAN	使用下拉式清單選擇 WAN 介面。
狀態	**啓用** – 按此啓用此 QoS 設定檔。 **停用** – 按此停用此 QoS 設定檔。
頻寬(	指定輸入/輸出資料的總傳輸速率，範圍由 64 到 10000000。 按 Kbps 或 Mbps 指定傳輸速率單位。
高/中/一般/低	有數種輸出順序可供選擇，資料群組中的佇列可以權重值 0 進行初始化。 輸入佇列的權重值，單位爲位元。範圍由 0 到 1000000。
套用	按此鈕儲存設定。
取消	按此鈕捨棄頁面設定。

輸入所有設定並按下**套用**儲存。

4.13.2 QoS 規則

有 32 條過濾器規則可以針對資料輸入與輸出進行不同的設定。

4.12.2.1 QoS 規則



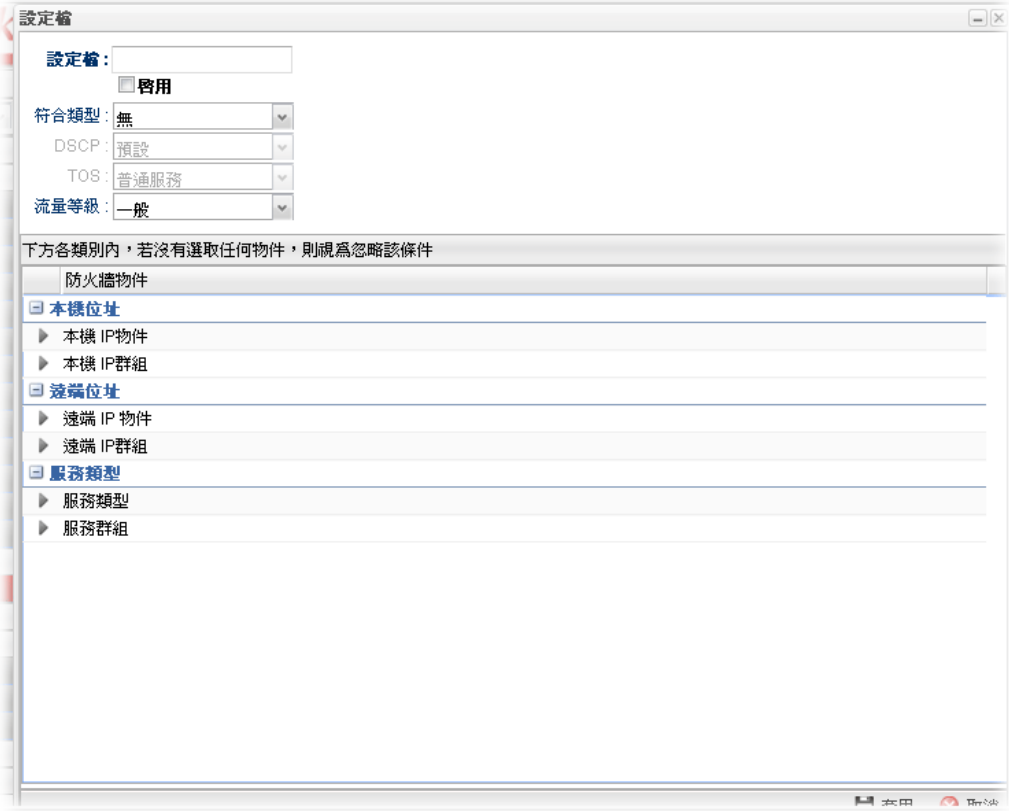
可用參數詳列如下：

項目	說明
新增	新增新的設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
刪除	移除選定的設定檔。 請選擇您想要刪除的既有設定檔，然後按下刪除按鈕，該設定檔即可被移除。
更名	按此鈕後將會跳出視窗，讓您修改選定設定檔的檔名。 在使用此功能之前，至少要有一個設定檔存在始可運作。
更新	重新更新本頁面。
設定檔數量限制	顯示設定檔可建立的總數。
設定檔	顯示設定檔名稱。
啓用	顯示設定檔狀態，False 表示停用；True 表示啓用。
本機 IP 物件	顯示過濾器的來源 IP 位址。
遠端 IP 物件	顯示過濾器的目標 IP 位址。
服務類型	顯示過濾器的服務類型(例如 IKE, HTTP, AUTH 等等)。
符合類型	顯示過濾器的符合類型(例如 TOS 或是 DSCP)。

DSCP	顯示 DSCP 設定內容。
TOS	顯示 TOC 設定內容。
流量等級	顯示分類的過濾器的隊列號碼序。

如何新增 QoS 規則設定檔

1. 開啓**頻寬管理>>QoS 規則**。
2. 按下**新增**按鈕。
3. 下述頁面將會出現。



可用參數詳列如下：

項目	說明
設定檔	輸入設定檔的檔名。
啓用	勾選此框啓用此設定檔。
符合類型	使用下拉式清單選擇適當的類型。
DSCP	當符合類型選擇 DSCP 時，此選項始可作用。
TOS	當符合類型選擇 TOS 時，此選項始可作用。
流量等級	選擇隊列號碼以分類符合上述條件的封包，**高**指的是最高等級，**正常**則爲最低等級。
本機位址	按下設定檔左方的三角按鈕 ▶ ， 勾選物件設定檔作爲

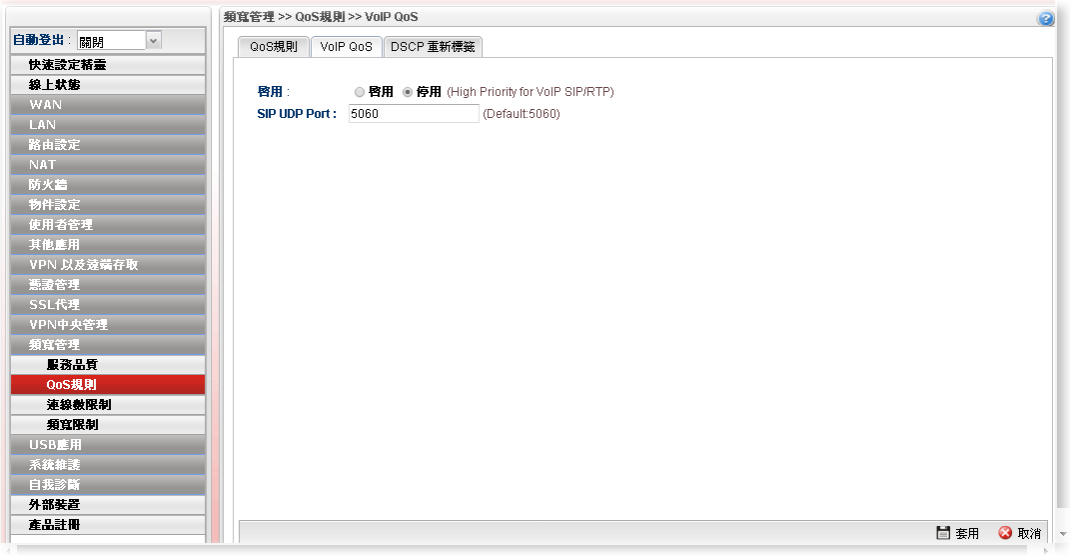
	來源目標。 **本機 IP 物件–** 使用下拉式清單選擇一個 IP 物件。 **本機 IP 群組–** 使用下拉式清單選擇一個 IP 群組。 如果您想要在新增其他的 IP 物件，請按 開啓如下對話框，即可建立新的物件。 ● **設定檔–** 針對此 IP 物件輸入檔名。 ● **位址類型–** 選擇位址類型(單一、範圍、子網)，每個類型的設定項目皆有所差異。 ● **起始 IP 位址-** 輸入一組 IP 位址當成此設定檔所需的起始 IP 位址。 ● **結束 IP 位址-** 若您選擇**範圍**爲**位址類型**，請多輸入一組 IP 位址當成此設定檔所需的結束 IP 位址。 ● **子網路遮罩** – 您選擇**子網路遮罩**爲**位址類型**，請再佀自下拉式清單中選擇一組子網遮罩。
遠端位址	按下**遠端 IP 物件/遠端 IP 群組**設定檔左方的三角按鈕 ，勾選物件設定檔作爲目的目標。 **遠端 IP 物件–** 使用下拉式清單選擇一個 IP 物件。 **遠端 IP 群組–** 使用下拉式清單選擇一個 IP 群組。 如果您想要在新增其他的 IP 物件，請按 開啓如下對話框，即可建立新的物件。 ● **設定檔–** 針對此 IP 物件輸入檔名。 ● **位址類型–** 選擇位址類型(單一、範圍、子網)，每個類型的設定項目皆有所差異。 ● **起始 IP 位址) -** 輸入一組 IP 位址當成此設定檔所需的起始 IP 位址。

	● **結束 IP 位址-** 若您選擇**範圍**爲**位址類型**，請多輸入一組 IP 位址當成此設定檔所需的結束 IP 位址。 ● **子網路遮罩–** 您選擇**子網路遮罩**爲**位址類型**，請再佀自下拉式清單中選擇一組子網遮罩。
服務類型	**服務類型–** 自下拉式清單中選擇一組服務類型。 如果您想要在新增其他的服務類型物件，請按 開啓如下對話框，即可建立新的物件。 ● **設定檔–** 針對此服務類型輸入檔名。 ● **通訊協定–** 有 **TCP**、**UDP** 與 **TCP/UDP** 數種選項，請選擇適當的一個選項。 ● **來源起始/結束埠號** - 輸入此設定檔所需的來源埠號範圍，包含起點與終點埠號值。 ● **目標起始/結束埠號-** 輸入此設定檔所需的目標埠號範圍，包含起點與終點埠號值。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

4. 輸入所有設定並按下**套用**儲存。
5. 新的 QoS 規則設定檔已建立。

4.13.2.2 VoIP QoS

啓用此功能時，VoIP SIP/UDP 封包於資料傳輸過程當中將優先傳送出去。



每個項目說明如下：

項目	說明
啓用	按啓用可以啓動 VoIP QoS 功能。
SIP UDP Port	設定 SIP 需求的埠值。
套用	按此鈕儲存設定。
取消	按此鈕捨棄頁面設定。

4.13.2.3 DSCP 重新標籤

來自於 LAN IP 的封包可以經由 QoS 設定重新加上標籤，當封包透過 WAN 介面傳送出去時，所有的封包都會以帶上指定的標頭，如此一來在 ISP 端的伺服器就可以輕易的將其辨識出來。

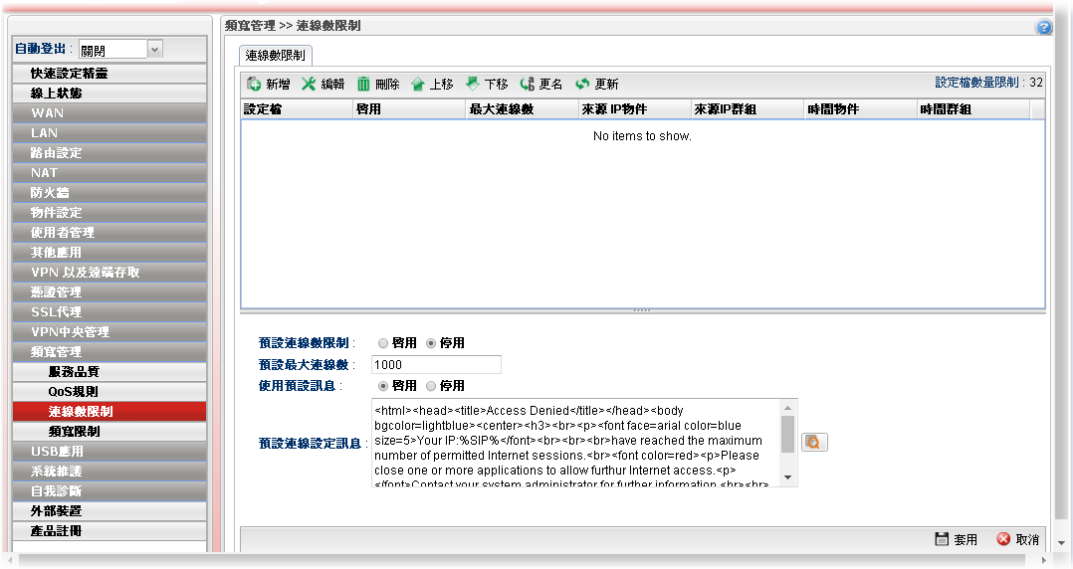
每個項目說明如下：

項目	說明
啓用	啓用 – 選此項以啓用 DSCP Re-Tag 功能。 停用 – 選此項已停止使用此功能。
高/中/一般/低	QoS 控制有數種排列方式，使用下拉式清單指定每個列的標頭，後續將可套用至含標籤的封包上。
套用	按此鈕儲存設定。
取消	按此鈕捨棄頁面設定。

4.13.3 連線數限制

擁有虛擬 IP 的電腦可以透過 NAT 路由器存取網際網路，針對此連線需求路由器將會產生 NAT 連線數的紀錄，P2P (Peer to Peer)應用程式(如 BitTorren)經常需要很大的連線數來處理，同時也會佔據很大的資源空間，造成重要的資料存取動作受到嚴重的影響。爲瞭解決這種問題，您可以使用連線數限制來限制指定主機的連線數。

在**頻寬管理**群組中，按**連線數限制**開啓如下的網頁。



每個項目說明如下：

項目	說明
新增	新增新的設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
刪除	移除選定的設定檔。 請選擇您想要刪除的既有設定檔，然後按下刪除按鈕，該設定檔即可被移除。
上移	將設定檔往上移動改變選定設定檔的順序。
下移	將設定檔往下移動改變選定設定檔的順序。
更名	允按此鈕後將會跳出視窗，讓您修改選定設定檔的檔名。 在使用此功能之前，至少要有一個設定檔存在始可運作。
更新	重新更新本頁面。
設定檔	顯示設定檔名稱。
啓用	顯示設定檔狀態，False 表示停用；True 表示啓用。
Limit(限制)	顯示此設定檔最大可用連線數爲何。
來源 IP 物件	顯示來源 IP 物件設定檔名。

來源 IP 群組	顯示來源 IP 群組設定檔名。
時間物件	如果尚未設定任何時間排程，本區只會呈現”無”這個項目。
時間群組	顯示此設定檔套用的時間群組檔。
預設連線數限制	顯示區域網路中每部電腦的預設連線數為何。
預設最大連線數	顯示區域網路中每部電腦的預設的最大連線數為何。
使用預設訊息	**啓用** – 使用預設訊息，將在使用者嘗試登入封鎖的網頁時顯示出來。 **停用** – 手動輸入訊息內容，將在使用者嘗試登入封鎖的網頁時顯示出來。
預設連線設定訊息	此區僅在停用**使用預設訊息**時始有作用。 將在使用者嘗試登入封鎖的網頁時顯示出來。
套用	按此鈕儲存設定。
取消	按此鈕捨棄頁面設定。

如何新增連線數限制設定檔

1. 開啓**頻寬管理>>狀連線數限制**。
2. 按下**新增**按鈕。
3. 下述頁面將會出現。

可用參數詳列如下：

項目	說明
設定檔	輸入設定檔名稱。
啓用	勾選此框啓用此設定檔。

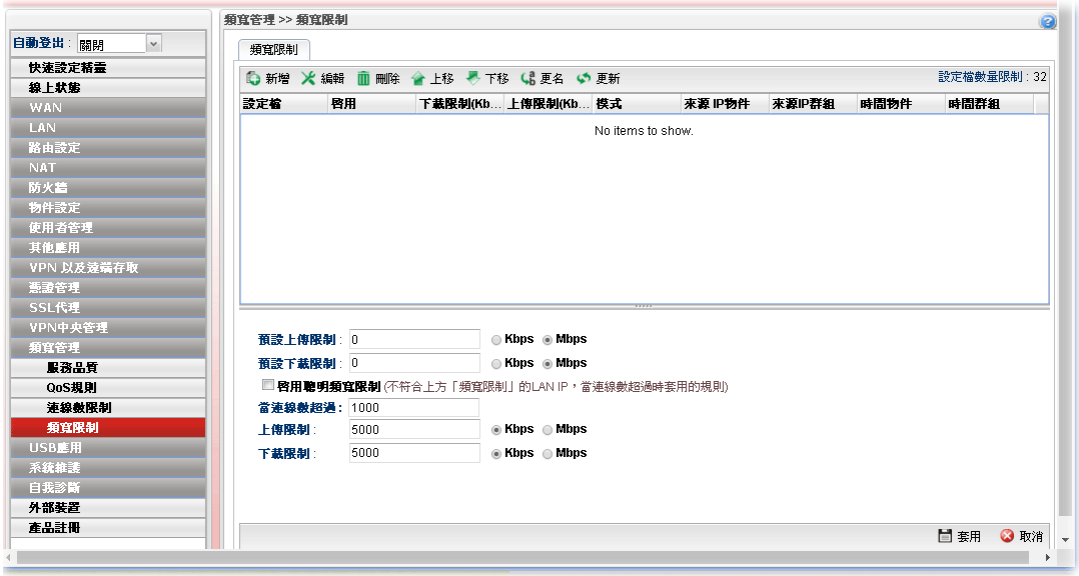
最大連線數	定義指定 IP 位址範圍中每台主機可用的連線數為何，如果您未在此區制定連線數，系統將套用預設限制值於每個設定檔上，本區不可輸入 0，否則設定檔將無法儲存。
基本目標	**時間物件** – 按下選項左方的三角按鈕 ▶ 顯示設定檔選框，以勾選方式選擇排程物件套用至此設定檔，您可以按 以建立新的時間物件。 **時間群組**- 按下選項左方的三角按鈕 ▶ 顯示設定檔選框，以勾選方式選擇排程群組套用至此設定檔，您可以按 以建立新的時間群組。
來源目標	**來源 IP 物件** - 按下選項左方的三角按鈕 ▶ 顯示設定檔選框，自下拉式清單中選擇一個或多個 IP 物件，選定的物件檔將被視為來源目標，您可以按 以建立新的 IP 物件設定檔。 **來源 IP 群組** - 按下選項左方的三角按鈕 ▶ 顯示設定檔選框，自下拉式清單中選擇一個或多個 IP 群組，定的物件群組將被視為來源目標，您可以按 以建立新的 IP 群組設定檔。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

4. 輸入所有設定並按下**套用**儲存。
5. 新的連線數設定檔已建立。

4.13.4 頻寬限制

從 FTP,HTTP 或是某些 P2P 應用程式的下行或上行資料會佔據很大的頻寬，並影響其他程式的運作。請使用限制頻寬讓頻寬的應用更有效率。

在**頻寬管理**群組中，按**頻寬限制**開啟如下的網頁。



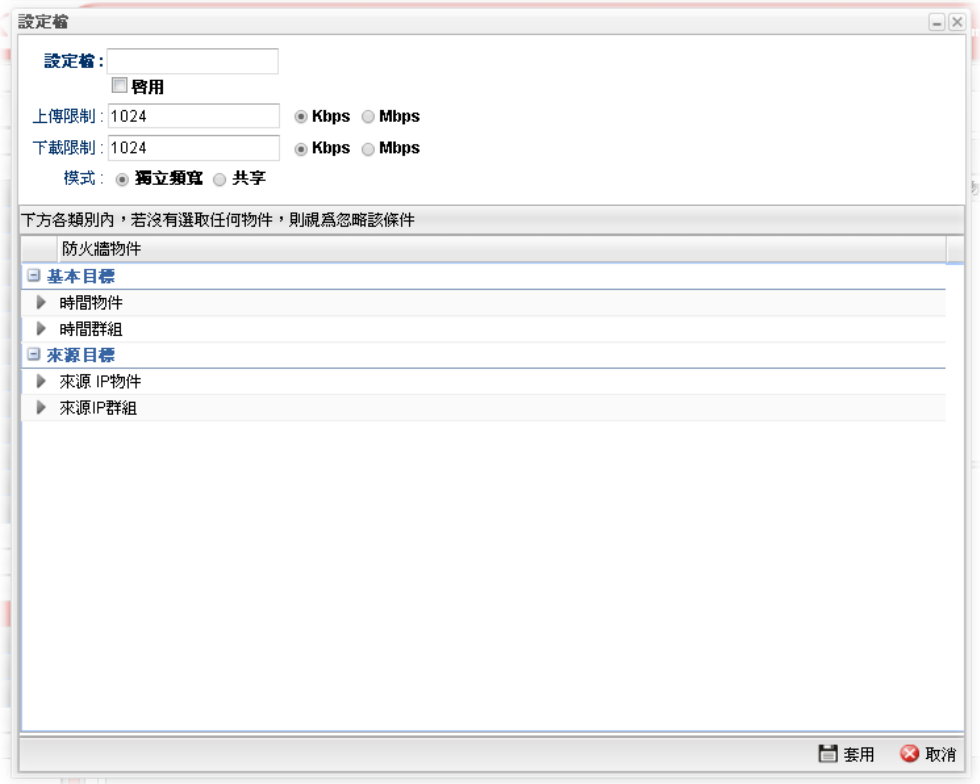
每個項目說明如下：

項目	說明
新增	新增新的設定檔。
編輯	修改選定的設定檔。 自既有的設定檔中，選擇您想要修正的設定檔，再按下編輯按鈕，編輯視窗將會出現讓您修改內容。
刪除	移除選定的設定檔。 請選擇您想要刪除的既有設定檔，然後按下刪除按鈕，該設定檔即可被移除。
上移	將設定檔往上移動改變選定設定檔的順序。
下移	將設定檔往下移動改變選定設定檔的順序。
更名	按此鈕後將會跳出視窗，讓您修改選定設定檔的檔名。 在使用此功能之前，至少要有一個設定檔存在始可運作。
更新	重新更新本頁面。
設定檔	顯示設定檔名稱。
啓用	顯示設定檔狀態，False 表示停用；True 表示啓用。
下載限制	顯示資料下行速度之限制。
上傳限制	顯示資料上行速度之限制。
模式	顯示設定檔的模式選項(**Each/Shared**)。
來源 IP 物件	顯示來源 IP 物件設定檔名。
來源 IP 群組	顯示來源 IP 群組設定檔名。
時間物件	如果尚未設定任何時間排程，本區只會呈現”無”這個項目。

時間群組	顯示此設定檔選定的時間群組。
預設上傳/下載限制	此處設定的預設值將會套用在不適合上述設定的 LAN IP 上。 **預設上傳限制(Default TX Limit)** – 定義上行速度限制。 **預設下載限制(Default RX Limit)** –定義下行速度限制。
啓用聰明頻寬限制	選此項目以設定未列入限制清單中，任何 LAN IP 的頻寬限制預設值。
當連線數超過	當連線數超過門檻設定值之後，聰明頻寬限制就會立即啓動運作。
上傳限制	定義聰明頻寬的上行速度，如果您未設定此限制，系統將會使用預設速度套用在資料傳輸上。
下載限制	定義聰明頻寬的下行速度，如果您未設定此限制，系統將會使用預設速度套用在資料傳輸上。
套用	按此鈕儲存設定。
取消	按此鈕捨棄頁面設定。

如何新增頻寬限制設定檔

1. 開啓**頻寬管理>>頻寬限制**。
2. 按下**新增**按鈕。
3. 下述頁面將會出現。



可用參數詳列如下：

項目	說明
設定檔	輸入設定檔名稱。
啓用	勾選此框啓用此設定檔。
上傳限制	定義上行速度限制，如果您未在此區設定限制值，系統將依據您對每個索引設定檔所指定的限制值，分別套用於每個設定檔上，本區不可輸入 0，否則設定檔將無法儲存。
下載限制	定義下行速度限制，如果您未在此區設定限制值，系統將依據您對每個索引設定檔所指定的限制值，分別套用於每個設定檔上，本區不可輸入 0，否則設定檔將無法儲存。
模式	選擇 **Each** 可讓起始 IP 與結束 IP 範圍中的每個 IP 都同樣具有傳輸限制與接收限制區域定義的速率；選擇**共享**則可讓範圍內的所有 IP 共同分享傳輸限制與接收限制區域定義的速率。
基本目標	**時間物件**– 按下選項左方的三角按鈕 ▶ 顯示設定檔選框，以勾選方式選擇排程物件套用至此設定檔，您可以按 以建立新的時間物件。 **時間群組**- 按下選項左方的三角按鈕 ▶ 顯示設定檔選框，以勾選方式選擇排程群組套用至此設定檔，您可以按 以建立新的時間群組。
來源目標	**來源 IP 物件** - 按下選項左方的三角按鈕 ▶ 顯示設定檔選框，自下拉式清單中選擇一個或多個 IP 物件，選定的物件檔將被視爲來源目標，您可以按 以建立新的 IP 物件設定檔。 **來源 IP 群組** - 按下選項左方的三角按鈕 ▶ 顯示設定檔選框，自下拉式清單中選擇一個或多個 IP 群組，定的物件群組將被視爲來源目標，您可以按 以建立新的 IP 群組設定檔。
套用	按此鈕儲存設定並離開本頁。
取消	按此鈕離開對話盒，且不儲存任何設定。

4. 輸入所有設定並按下套用儲存。
5. 新的頻寬限制設定檔已建立。

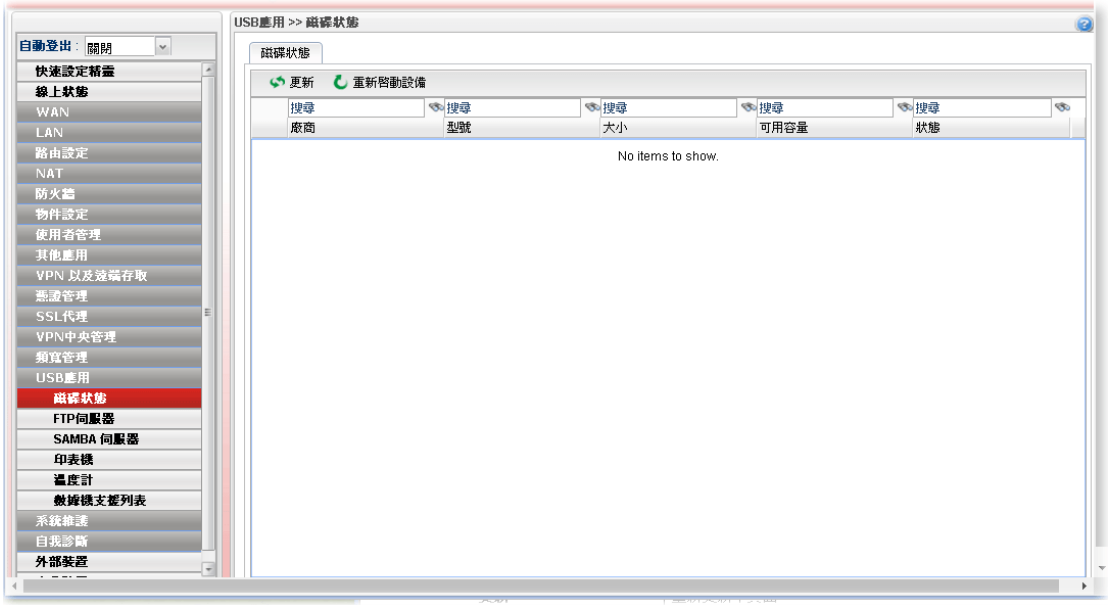
4.14 USB 應用

連接至路由器的 USB 存取磁碟可以被視爲伺服器的一種。透過 Vigor 路由器，區域網路端的用戶可以透過不同的應用程式登入、寫入並讀取儲存在 USB 儲存碟內的資料。在完成 USB 應用設定之後，您可以在用戶端軟體上輸入路由器的 IP 位址，以及在 **USB 應用>>FTP 使用者管理**頁面所建立的帳號以及密碼，然後，用戶端就可以使用 FTP(USB 儲存碟)服務。

注意：Vigor 路由器的 USB 埠口可以連接 USB 數據機，支援的型號請參見 **USB 應用>>數據機支援列表**，有關透過 USB 數據機進行的網路連線，參考 **WAN>>基本設**定以便取得詳細資訊。

4.14.1 磁碟狀態

本頁用來監督透過 Vigor 路由器來存取 FTP 或是 USB 磁碟資料的使用者狀態，另外 USB 數據機或是 USB 印表機的連線狀態也可自此頁面檢視。



可用參數詳列如下：

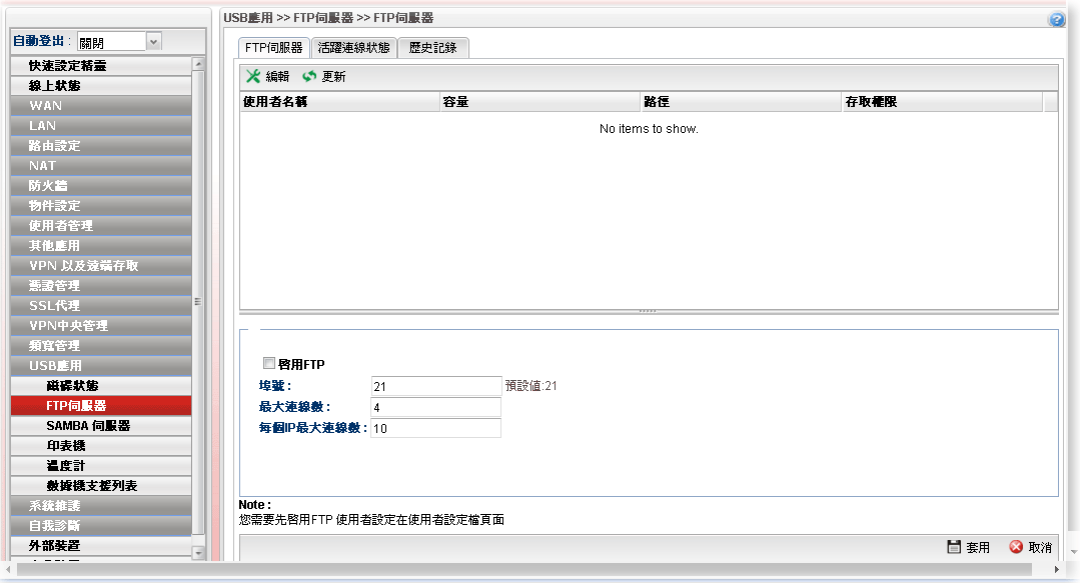
項目	說明
更新	重新更新本頁面。
重新啓動設備	按此重新啓動 USB 裝置。
廠商	顯示 USB 裝置的製造商資料。

型號	顯示 USB 裝置的型號。
大小	顯示 USB 裝置的全部容量。
可用容量	顯示 USB 裝置目前可用的容量。
狀態	顯示 USB 裝置的使用狀態。
(移除圖示)	目前路由器系統只有支援 FAT、EXT2、EXT3 等 USB 格式， 如果將此類 USB 插入路由器的 USB 插槽，狀態欄位將會顯示"使用中"，移除圖示也會顯示在螢幕上。當您想要移除 USB 磁碟時，按下該圖示即可。

4.14.2 FTP 伺服器

本頁讓您編輯 FTP 用戶的 FTP 使用者設定，任何想要存取此 USB 磁碟的使用者，必須輸入與設定相同的使用者名稱及密碼，在編輯本頁設定之前，請先將 USB 磁碟插入路由器的 USB 插槽中。

所有在此顯示的設定檔皆可在**使用者管理>>使用者設定檔**頁面中建立，並在**允許 FTP 伺服器登錄**項目中記得按下**啓用**。



可用參數詳列如下：

項目	說明
編輯	按此編輯選定的 USB 裝置。
更新	按此更新目前頁面。
使用者名稱	顯示登入 FTP 伺服器的用戶所使用的帳號名稱，如果本區未顯示任何資訊，即表示尚未建立任何 FTP 使用者設定檔，請開啓**使用者管理>>使用者設定檔**，先建立一組啓用 **Allow FTP Server Login** 的設定檔。
容量	顯示連接的 USB 磁碟內的儲存空間容量。
路徑	顯示連接的 USB 磁碟內的目錄名稱。

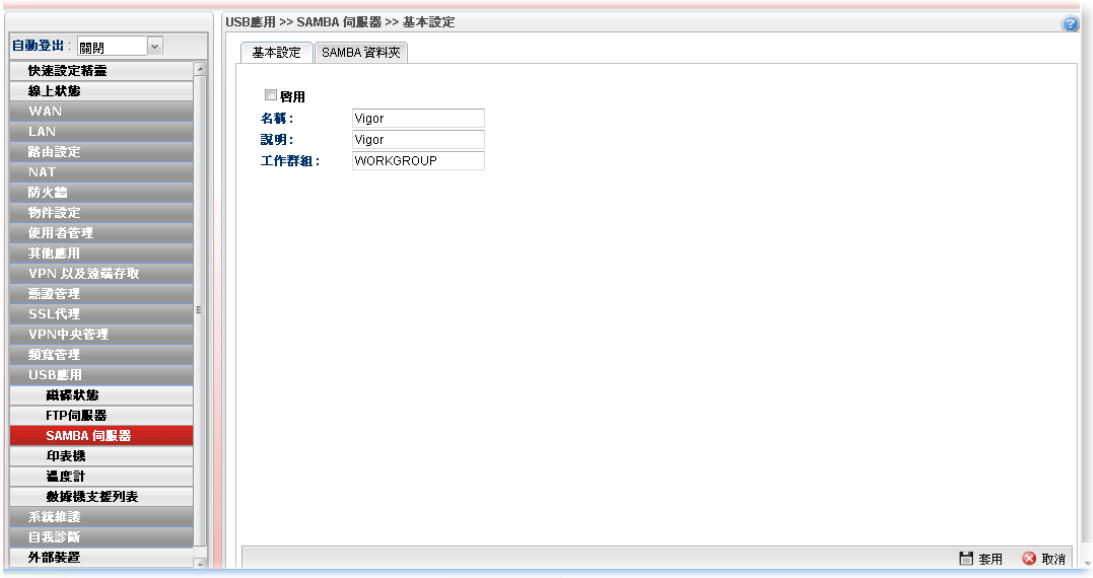
存取權限	顯示連接的 USB 磁碟的存取權限。
啓用 FTP	勾選此框啓用 FTP 伺服器。
埠號	輸入 FTP 伺服器需求的埠號，或是直接套用預設值。
最大連線數	表示 FTP 伺服器的連線數最大值，預設值爲 4。
每個 IP 最大連線數	表示 FTP 伺服器中每個 IP 位址的連線數限制，例如 2 個 FTP 使用者使用一組 IP 位址連線網路，即表示 2 個連線數分別用於 IP 與 FTP 伺服器。
套用	按此鈕儲存設定。
取消	按此鈕不儲存任何設定。

4.14.3 SAMBA 伺服器

SAMBA 伺服器透過指定的檔案夾提供檔案分享服務，任何一個想要登入 USB 儲存碟的使用者必須輸入相同的名稱並使用相同的工作群組。在新增或是修改本頁的設定之前，請先將 USB 儲存碟插入路由器。

4.14.3.1 基本設定

本頁用來配置 SAMBA 伺服器的相關設定。

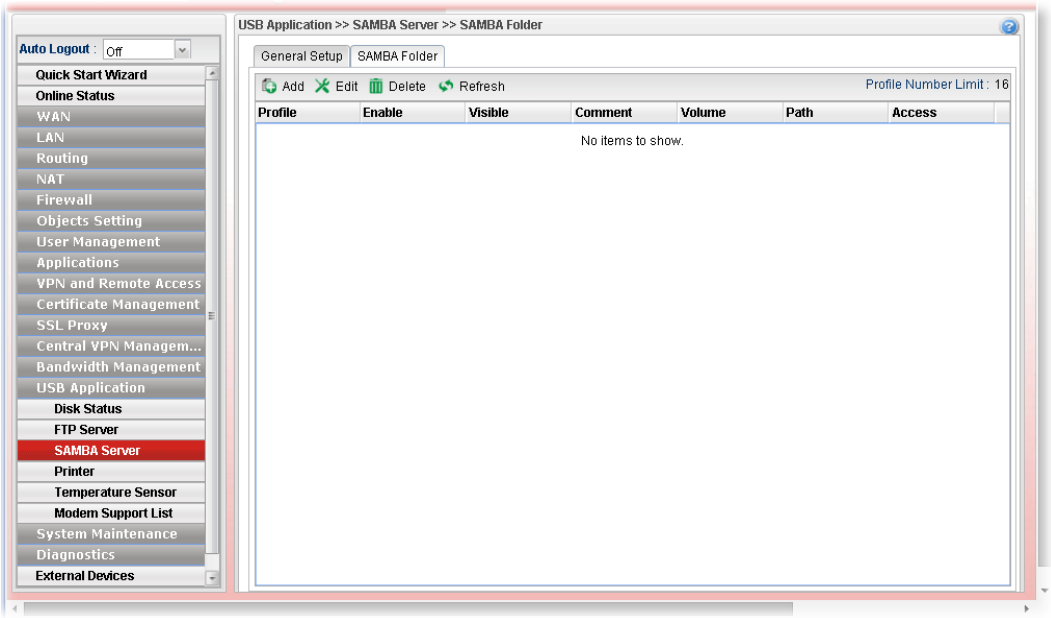


可用參數詳列如下：

項目	說明
啓用	勾選此方塊啓用 SAMBA 伺服器。
名稱	輸入 SAMBA 伺服器的名稱。
說明	輸入與 SMABA 伺服器有關的文字說明。
工作群組	輸入 SMABA 伺服器於 Windows 系統中的工作群組名稱。Windows 系統會提供預設名稱。

4.14.3.2 SAMBA 資料夾

鑒於 SAMBA 伺服器檔案分享特徵之故，本頁可讓您建立網路上用戶得以分享檔案的設定檔。



如何新增/編輯 SMABA 資料夾設定檔

1. 開啓 **USB 應用>>SMABA 伺服器**並按下 **SAMBA 資料夾**標籤。
2. 按下**新增**按鈕開啓畫面。對於已經存在的設定檔，只要選擇該檔案然後按下**編輯**按鈕即可開啓設定畫面。
3. 下圖爲資料夾設定畫面。

可用參數詳列如下：

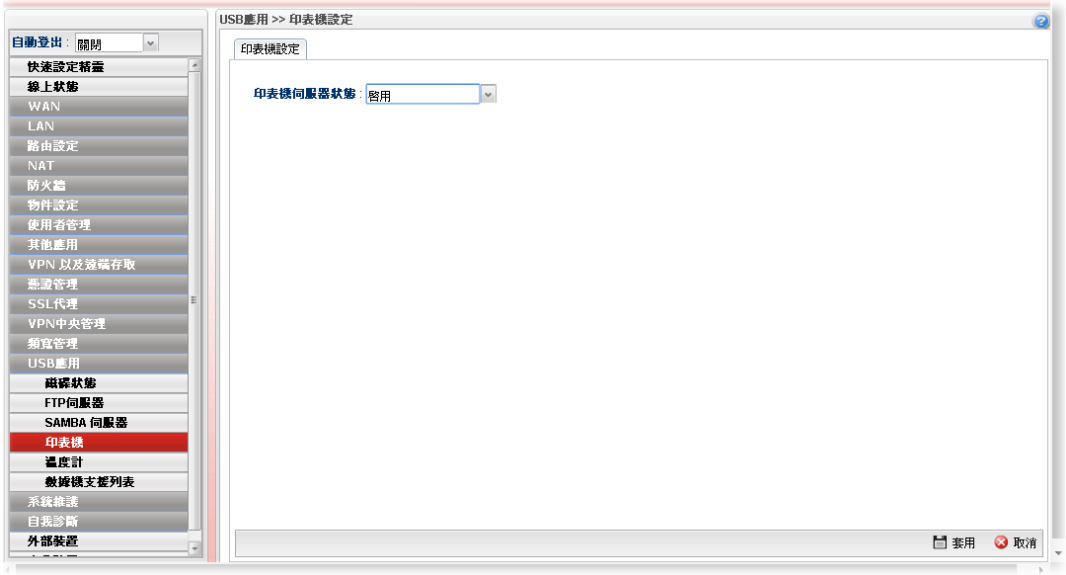
項目	說明
設定檔	輸入得以分享之檔案資料夾名稱。

啓用	勾選此框啓用此設定檔。
可見	勾選此框讓使用者能看見此設定檔，若未勾選，使用者必須知悉並且手動輸入檔案資料夾的名稱及路徑才能登入該資料夾。
註解	如有必要，可輸入與此設定檔相關的文字說明。
容量	使用下拉式清單指定適當的資料夾空間容量。
路徑	指出連接至 USB 磁碟的目錄名稱。 預設值爲“/”。
存取	有三個選項可以指定。 **所有用戶唯讀** – 此選項可讓所有的用戶分享 SAMBA 服務以便讀取分享資料夾內的檔案。 **所有用戶讀寫** – 此選項可讓所有的用戶分享 SAMBA 服務以便讀取並寫入資料夾內的檔案。 若選定**特定用戶**，您必須另外指定唯讀用戶與讀寫用戶。 ● **唯讀用戶** – **使用者管理>>使用者設定檔**下建立的使用者設定檔(啓用了**允許 SAMBA 伺服器**登入選項)會顯示於此，請從中選取一個設定檔，使其具有讀取 SAMBA 資料夾檔案的權限。 ● **讀寫用戶** – **使用者管理>>使用者設定檔**下建立的使用者設定檔(啓用了**允許 SAMBA 伺服器**登入選項)會顯示於此，請從中選取一個設定檔，使其具有寫入與讀取 SAMBA 資料夾檔案的權限。
套用	按此鈕儲存設定。
取消	按此鈕不儲存任何設定。

4. 輸入設定並按下**套用**。
5. 新的資料夾立即建立。

4.14.4 印表機

當印表機透過 USB 埠連接至路由器時，可利用本頁啓動印表機伺服器。



可用參數詳列如下：

項目	說明
印表機伺服器狀態	**自動** – 此爲預設值，路由器將會偵測連接的裝置是否爲印表機，如果是印表機，伺服器會自動啓動以便使用印表機。 **啓用** – 啓用印表機伺服器 **停用** – 停用印表機伺服器。
套用	按此鈕儲存設定。
取消	按此鈕不儲存任何設定。

4.14.3 溫度計

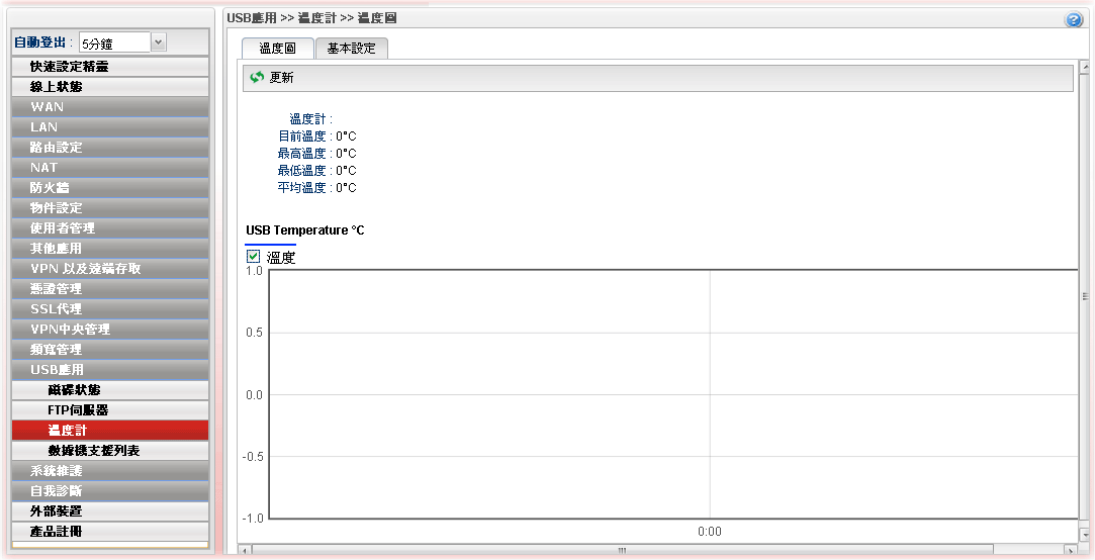
目前 USB 溫度計可以與您安裝的居易路由器搭配使用，幫助您監控伺服器或是機房環境，並在伺服器機房或是資料通訊機房過熱時立即通知您。

尤其是在夏天，確保伺服器機房或是資料通訊機房設備不因冷卻系統失效而造成過熱線現象，是很重要的一件事。

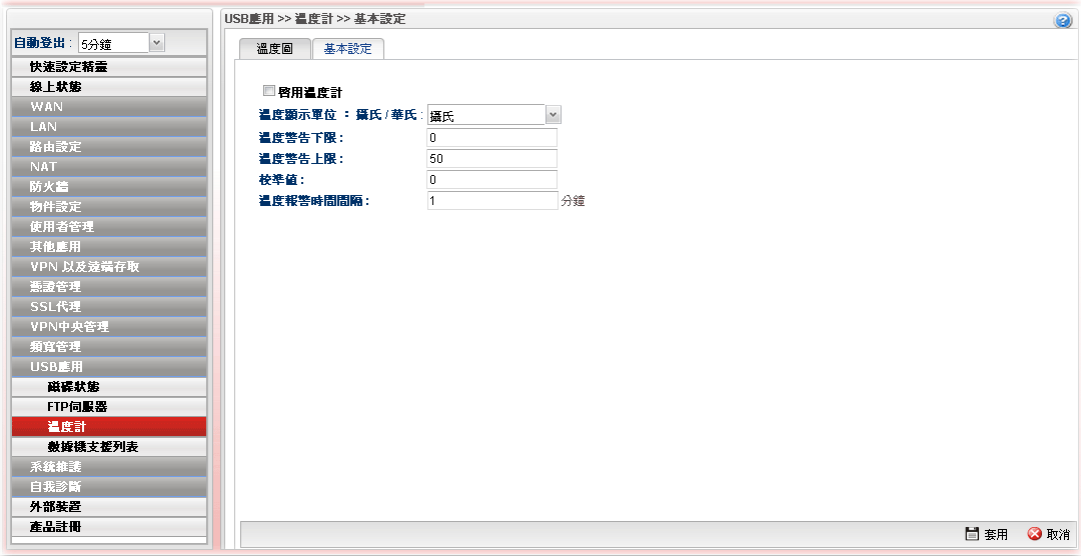
USB 溫度計與 Vigor 路由器相容，將持續不斷監控週遭環境的溫度變化，當達到事先設定的門檻值時，系統將透過電子郵件或是簡訊通知，讓您能採取適當的行動。

4.14.3.1 溫度圖

下圖顯示溫度圖表範例。



4.14.1.2 基本設定



可用參數詳列如下：

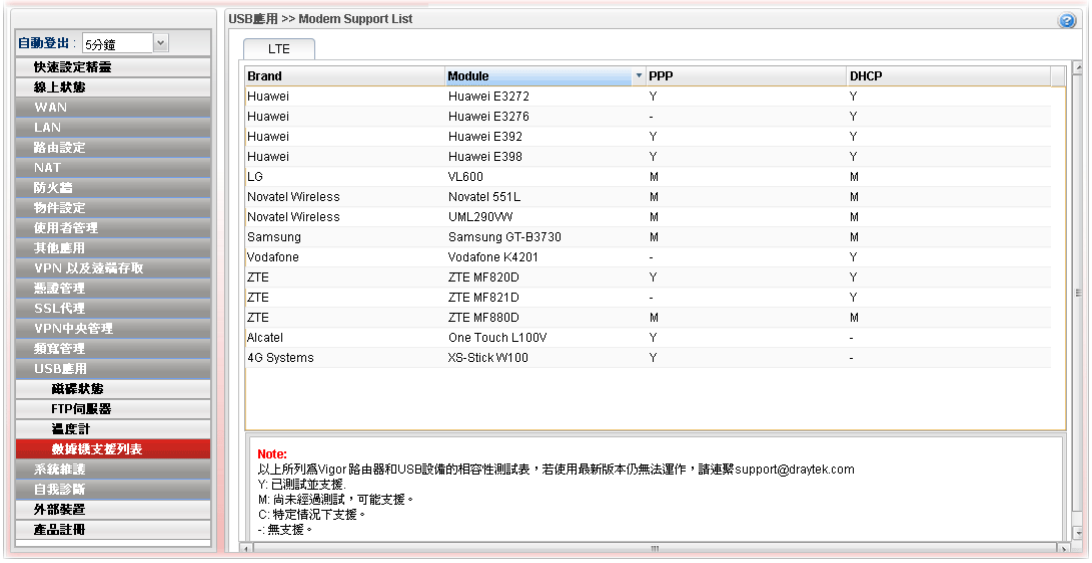
項目	說明
啓用溫度計	勾選此框啓用此功能。
溫度顯示單位	選擇攝氏或是華氏。
溫度警告下限	輸入溫度的上下限值，以便讓系統寄出溫度警示通知。

溫度警告上限	
校準值	輸入修正溫度錯誤的校正值。
溫度報警時間間隔	預設值為 1 分鐘，亦即溫度警告將會每分鐘發佈一次。
套用	按此鈕儲存設定。
取消	按此鈕捨棄頁面設定。

輸入所有設定並按下**套用**儲存。

4.14.4 數據機支援列表

本頁提供關於 Vigor 路由器支援的 USB 數據機品牌名稱與型號資訊。

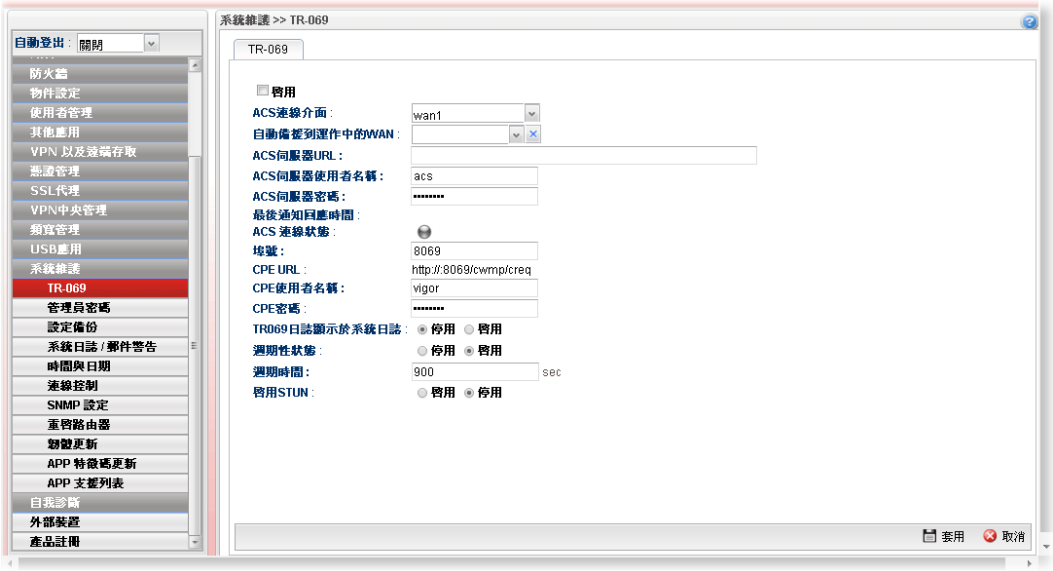


4.15 系統維護

下圖顯示系統維護的功能項目：

4.15.1 TR-069

本路由器支援 TR-069 標準，方便管理人員透過 Auto Configuration Server(例如 VigorACS)來管理 TR-069 裝置(Vigor 路由器、AP 及其他)。



每個項目說明如下：

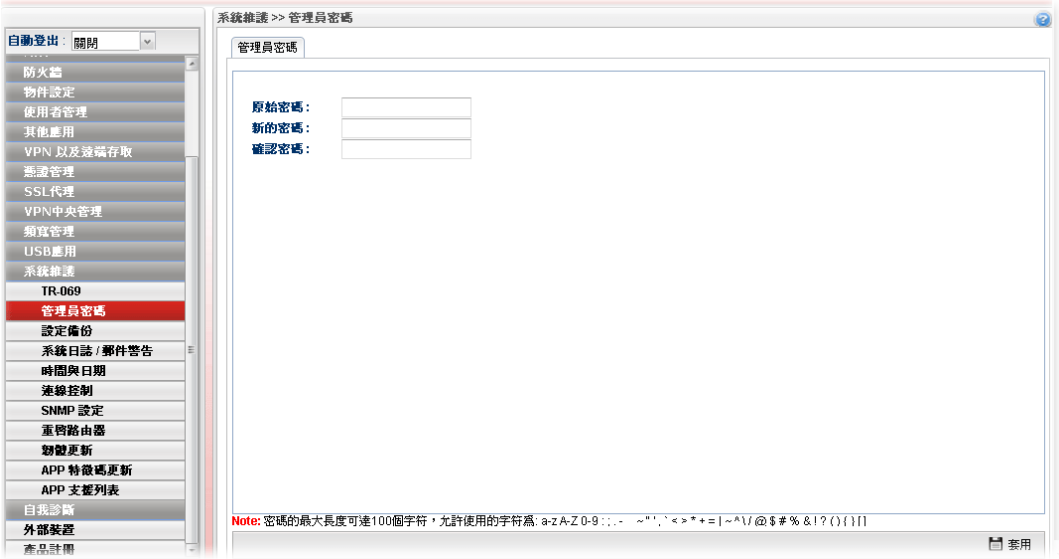
項目	說明
啓用	勾選此框啓用此設定檔。
ACS 連線介面	選擇 VigorACS 能夠辨認的 WAN 或 LAN 設定檔。
自動備援到運作中的 WAN	指定 WAN 介面以便在原始 WAN 介面失效時能夠接管網路連線作業。
ACS 伺服器 URL/	此區域必須依照您想要連接的 ACS (Auto Configuration

ACS 伺服使用者名稱 / ACS 伺服密碼	Server)的實際資訊來填寫，請參考 Auto Configuration Server 使用手冊取得細部資訊。
最後通知回應時間	顯示 VigorACS 知會的回應時間。
ACS 連線狀態	當綠燈亮起，即表示路由器已經通過偵測，可由 VigorACS 來管理。
埠號	輸入此台裝置的埠號方便 VigorACS 辨別。
CPE URL	顯示此台路由器的 URL。.
CPE 使用者名稱	輸入 CPE 的使用者名稱，這個名稱將由 VigorACS 管理者用來登入本台裝置之用。
CPE 密碼	輸入 CPE 的密碼，這個密碼將由 VigorACS 管理者用來登入本台裝置之用。
TR069 日誌顯示於系統日誌	預設值為**停用**，如果要讓 log 訊息由 Syslog 來記錄，請按下**啓用**。
週期性狀態	預設值是**啓用**的，請設定 VigorACS 定期傳送通知給 CPE 的時間，或是按下**停用**，關閉此功能。
週期時間	輸入 VigorACS 定期傳送通知給 CPE 的時間。
啓用 STUN	**啓用/停用** – 預設值為停用，如果您啓用此功能，請輸入下列必要的資訊。 **伺服器位址–** 輸入 STUN 伺服器的 IP 位址。 **伺服器埠號–** 輸入 STUN 伺服器所需的埠號。 **發送訊號的最短時間–** 如果啓用了 STUN，CPE 必須傳送綁定需求至伺服器以繼續綁定閘道。請輸入最小時間數值，預設值為 60 秒。 **最大保持活動週期** – 如果啓用了 STUN，CPE 必須傳送綁定需求至伺服器以繼續綁定閘道。請輸入最大時間數值，若此區輸入-1 即表示最大連線時間為沒有限制。
套用	按此鈕儲存設定。
取消	按此鈕捨棄頁面設定。

輸入所有設定並按下**套用**儲存。

4.15.2 管理員密碼

本頁可讓您設定新的密碼以便登入路由器的網頁設定介面。



每個項目說明如下：

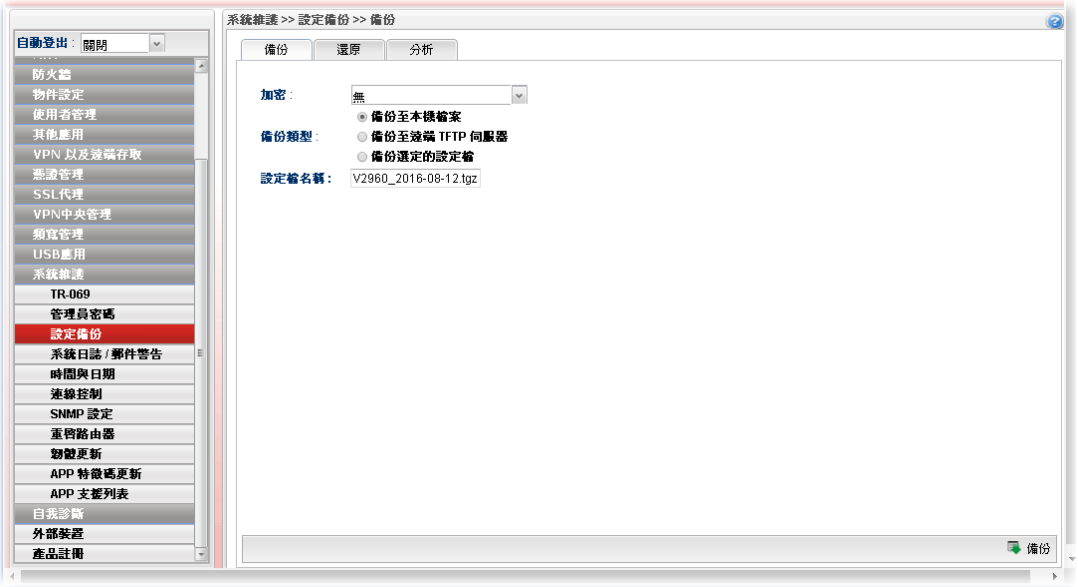
項目	說明
原始密碼	輸入舊密碼。
新的密碼	輸入新密碼。
確認密碼	再次輸入新密碼確認。

輸入所有設定並按下**套用**儲存。

4.15.3 設定備份

大多數的設定都可以設定檔的格式儲存起來，且可套用在其他的同款的路由器上。路由器支援還原與備份功能。

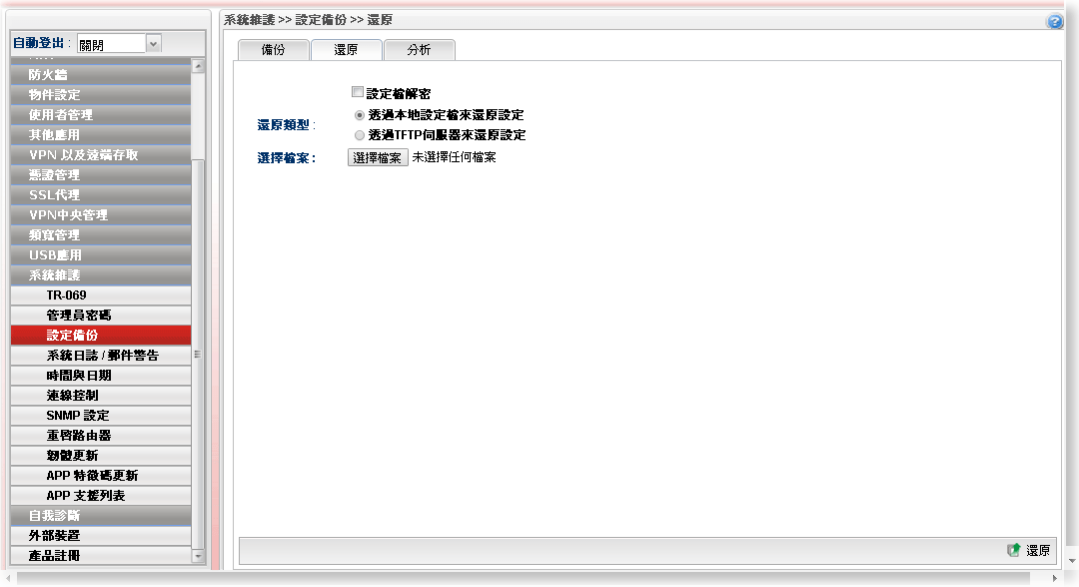
4.15.3.1 備份



每個項目說明如下：

項目	說明
加密	**無** – 不使用任何加密。 **加密設定檔**– 選擇此項可加密整個設定檔案。 ● **密碼** – 輸入加密檔案所需的密碼。 ● **確認密碼** – 再次輸入密碼。 **密碼編碼設定** – 選擇此項針對設定中的密碼資訊再次加密。
備份類型	選擇其中依種類型決定檔案將儲存的樣式。 **備份至本機檔案** – 設定檔案儲存在本機主機上。 **備份至遠端 TFTP 伺服器** – 設定檔案將將儲存在遠端的 TFTP 伺服器上。 **備份選定的設定檔** – 設定檔案將以選定的檔名儲存在本機電腦上，您必須先選擇想要儲存的檔案名稱。
設定檔案名稱	顯示預設的設定檔案名稱，如有必要，您可以更改名稱。
備份	執行檔案下載至電腦的工作。

4.15.3.2 還原

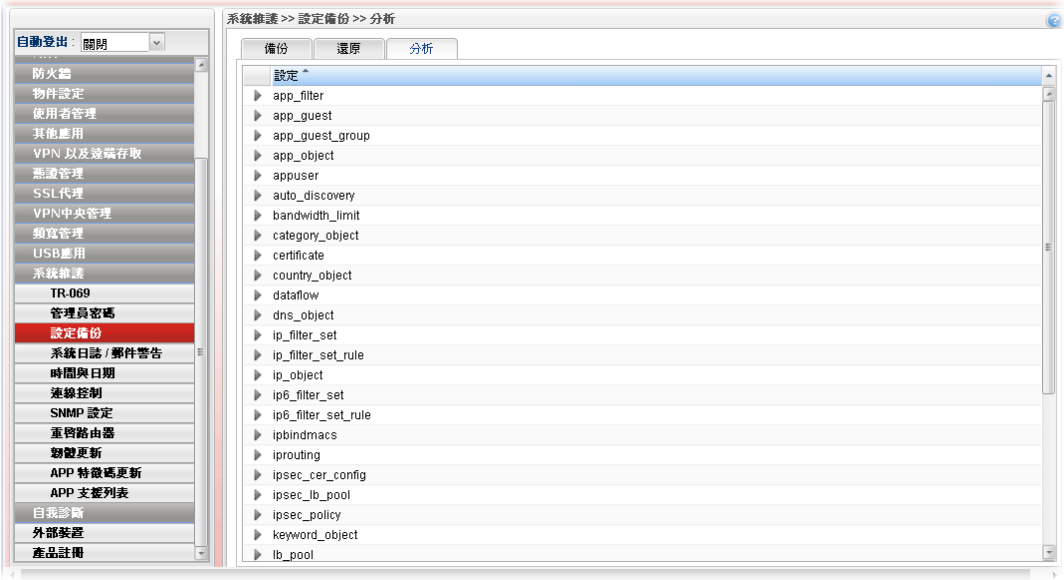


每個項目說明如下：

項目	說明
設定檔解密	勾選此框解密被加密的設定檔，您可以指定一組密碼作爲下次還原設定檔時用以解密。 **密碼** – 輸入用來解密檔案的密碼。 **確認密碼** – 再次輸入密碼確認。
還原類型	選擇任一類型來決定從何處下載檔案。 **透過本地設定檔來還原設定**– 按此透過儲存於本機的檔案來還原設定檔。 **透過 TFTP 伺服器來還原設定**– 按此透過 TFTP 伺服器還原設定。
選擇檔案	使用**選擇檔案**按鈕，找到上傳至路由器的檔案。
還原	按此上傳選定的檔案置路由器，在完成還原後，系統將要求您重新啓動路由器。

4.15.3.3 分析

分析頁面可以顯示使用者定義的設定結果，透過比較本頁所顯示的預設值資訊，管理者、使用者或是 RD 工程人員可以藉此清除可能的錯誤。

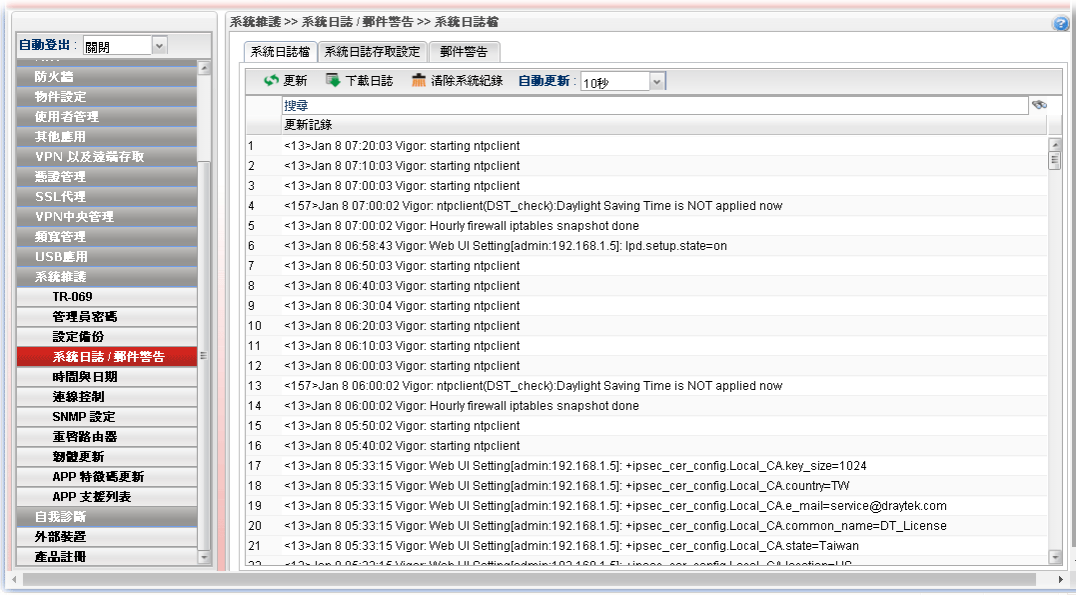

系統維護 >> 設定備份 >> 分析
自動登出：關閉
防火牆
物件設定
使用者管理
其他應用
VPN 以及遠端存取
憑證管理
SSL代理
VPN中央管理
頻寬管理
USB應用
系統維護
TR-069
管理員密碼
設定備份
系統日誌 / 郵件警告
時間與日期
連線控制
SNMP 設定
重啓路由器
韌體更新
APP 特徵碼更新
APP 支援列表
自我診斷
外部裝置
產品註冊
備份
還原
分析
設定
app_filter
app_guest
app_guest_group
app_object
appuser
auto_discovery
bandwidth_limit
category_object
certificate
country_object
dataflow
dns_object
ip_filter_set
ip_filter_set_rule
ip_object
ip6_filter_set
ip6_filter_set_rule
ipbindmacs
iprouting
ipsec_cer_config
ipsec_lb_pool
ipsec_policy
keyword_object
lb_pool

4.15.4 系統日誌/郵件警告

系統日誌功能主要是提供使用者一個監控路由器的機制。

4.15.4.1 系統日誌檔

本頁顯示路由器的所有操作紀錄。

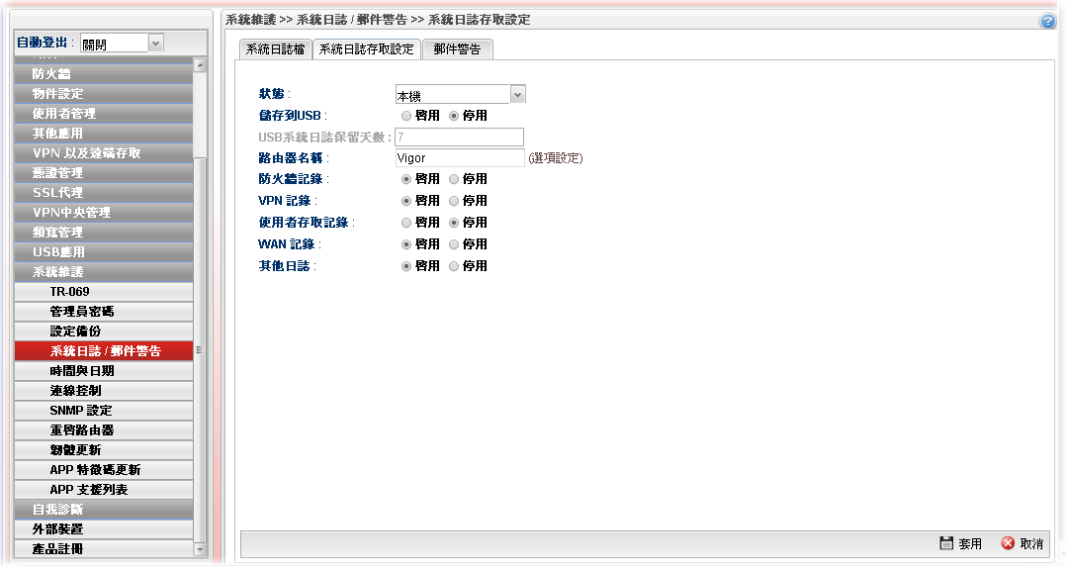


可用參數詳列如下：

項目	說明
更新	重新更新本頁面。
下載日誌	儲存或是開啓系統日誌檔案。
清除系統紀錄	移除全部紀錄。
自動更新	指定更新時間間隔以取得最新的狀態，若您按下**更新**按鈕，系統將立即更新資訊並呈現出來。

4.15.4.2 系統日誌存取設定

開啓**系統維護>>系統日誌/郵件警告**頁面，按下**系統日誌存取設定**標籤。



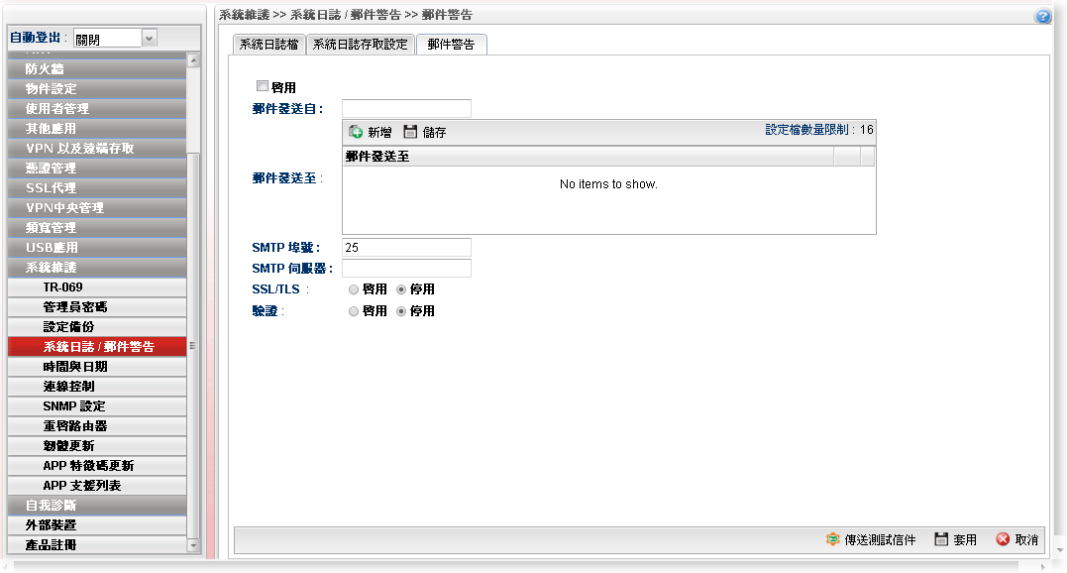
可用參數詳列如下：

項目	說明
狀態	選擇決定目前系統日誌存取狀態的選項，如果您選的是本機，您不需要輸入任何伺服器 IP 與埠號，只要定一個路由器名稱即可。
儲存到 USB	**啓用** – 按此儲存紀錄至 USB 磁碟。 **停用** – 按此關閉紀錄至 USB 的功能。 **USB 系統日誌保留天數**– 輸入 USB 磁碟保留紀錄的天數。
伺服器 IP	輸入系統日誌伺服器的 IP 位址。 僅在**遠端**或是**雙方**選項被選取時可用。
伺服器埠號	輸入系統日誌伺服器的埠號。 僅在**遠端**或是**雙方**選項被選取時可用。
路由器名稱	輸入路由器的辨識名稱，預設名稱爲 ***Vigor***。
防火牆紀錄	按下**啓用**讓防火牆紀錄能確實記載在系統日誌。
VPN 紀錄	按下**啓用**讓 VPN 紀錄能確實記載在系統日誌。
使用者存取紀錄	按下**啓用**讓使用者存取紀錄能確實記載在系統日誌。
WAN 紀錄	按下**啓用**讓 WAN 紀錄能確實記載在系統日誌。
其他日誌	按下**啓用**讓其他紀錄能確實記載在系統日誌。
套用	按此鈕儲存設定。
取消	按此鈕捨棄頁面設定。

輸入所有設定並按下**套用**儲存。

4.15.4.3 郵件警告

開啓**系統維護>> 系統日誌/郵件警告**頁面，按下**郵件警告**標籤。



可用參數詳列如下：

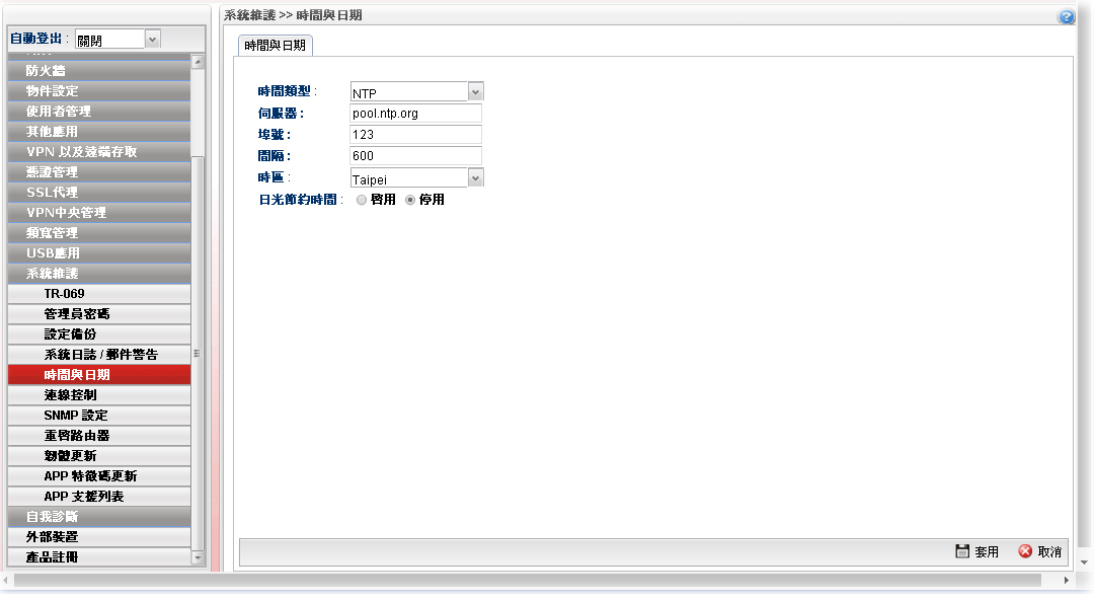
項目	說明
啓用	勾選此框啓用設定檔。
郵寄發送自	輸入郵件寄送者的郵件地址。
郵寄發送至	指定郵件接收人的郵件信箱。 **新增** – 按此鈕顯示可新增電郵位址的區域。 **儲存** – 完成位址設定之後，請按下儲存將所有變動都記錄起來。
SMTP 埠號	輸入 SMTP 伺服器的埠號。。
SMTP 伺服器	輸入 SMTP 伺服器的 IP 位址。
SSL/TLS	按下啓用以啓動 SSL/TLS 伺服器。
驗證	按下**啓用**讓任何使用者都能登入郵件伺服器，若您選擇**啓用**，您必須輸入使用者名稱及密碼。
使用者名稱	輸入驗證用的使用者名稱。
使用者密碼	輸入驗證用的密碼。
傳送測試信件	按此以傳送測試郵件至指定的位址。
套用	按此鈕儲存設定。
取消	按此鈕捨棄頁面設定。

輸入所有設定並按下**套用**儲存。

4.15.5 時間與日期

本頁讓您指定路由器時間應自何處取得。

作爲一個 NTP(Network Time Protocol)用戶端，路由器自時間伺服器取得標準時間，若系統時間功能無法成功運作，那麼一些以時間爲基準的功能可能無法正確的運行，一般來說透過多重伺服器與不同的網路路徑可讓 NTP 達成高準確性與可靠性。



可用參數詳列如下：

項目	說明
時間類型	**NTP** – 選擇此項以便自網際網路的時間伺服器取得時間。 **瀏覽器** – 選擇此項以便使用遠端管理者主機提供的瀏覽器時間作爲路由器的系統時間。S
伺服器	輸入伺服器的網域名稱。
埠號	輸入伺服器的埠號。
間隔	選擇自 NTP 伺服器更新的時間間隔。
時區	選擇路由器所在地區的時區。
日光節約時間	選擇**啓用**以啓動日光節約時間，此功能僅在某些地區有作用。
套用	按此鈕儲存設定。
取消	按此鈕捨棄頁面設定。

輸入所有設定並按下**套用**儲存。

4.15.6 連線控制

4.15.6.1 連線控制

本頁讓您能透過 Telnet、SSH、HTTP、HTTPS 等等來開啓或是關閉路由器的網頁使用者設定介面。

可用參數詳列如下：

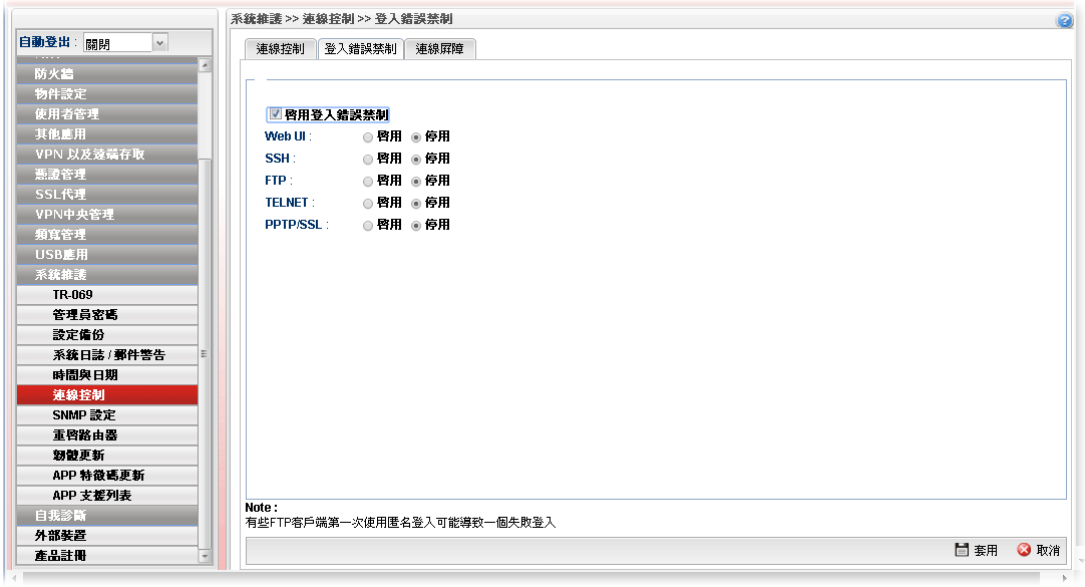
項目	說明
預設:停用自動登出	啓用 – 開啓網頁設定介面的自動登出功能，亦即系統將依照您所選擇的時間設定(如 1、3、5、10 分鐘)登出。 停用 – Vigor2960 網頁設定介面的自動登出功能將會關閉。
使用驗證碼	啓用 – 登入網頁設定介面時，系統將出現驗證畫面，以便驗證登入之使用者。 停用 – 登入網頁設定介面時，無須通過任何驗證。
自定義登錄圖片	啓用– 按此鈕可挑選圖片作爲登入畫面的背景影像。 ● 上傳登入圖片 – 按下**選擇檔案**按鈕指定需要的影像檔案。 停用– 按此鈕關閉自定圖片之功能，系統將自動使用預設之圖片。
網路存取控制	
套用到 WAN 介面	選擇套用的介面。
Web 允許/Telnet 允許/ SSH 允許/ HTTPS 允許 /FTP 允許/SAMBA 允許	按下**啓用**讓系統管理者可以從網際網路/telnet/SSH 伺服器/HTTPS 伺服器/FTP 伺服器/SAMBA 伺服器登入並管理路由器設定。
伺服器憑證	使用預設值。
存取列表	按下**啓用**讓系統管理者可以從使用者定義的 IP 位址登入

	並管理路由器的使用者設定介面。如果您啓用此功能，透過 WAN 介面，系統將由此處所輸入的 IP 位址來管理。
IP 列表	輸入 IP 位址讓系統管理者登入。 前面的方框指出允許登入路由器的 IP 位址，後面的方框指出允許登入路由器需設定的子網遮罩。
允許從 WAN Ping	按下**啓用**讓系統管理者可從 WAN 介面 ping 此台路由器。
LAN 存取控制	
允許由 LAN 端管理	按下**啓用**讓系統管理者可從 LAN 端管理此台路由器。
套用至 LAN 子網	選擇受此設定檔控制的 LAN 設定檔(含 IP 設定)，以便登入路由器的使用者設定介面。
Web 允許/Telnet 允許/ SSH 允許/ HTTPS 允許 /FTP 允許/SAMBA 允許	按下**啓用**讓系統管理者可以從網際網路/telnet/SSH 伺服器/HTTPS 伺服器/FTP 伺服器/SAMBA 伺服器登入並管理路由器設定。
允許從 LAN Ping	按下**啓用**讓系統管理者可從 LAN 介面 ping 此台路由器。
管理端口設定	
Web 埠號	輸入可以透過網頁進行管理所需的埠號值。
Telnet 埠號	輸入可以透過 telnet 進行管理所需的埠號值。
SSH 埠號	輸入可以透過 SSH 伺服器進行管理所需的埠號值。
HTTPS 埠號	輸入可以透過 HPPTS 伺服器進行管理所需的埠號值。
FTP 埠號	輸入可以透過 FTP 進行管理所需的埠號值。
套用	按此鈕儲存設定。
取消	按此鈕捨棄頁面設定。

輸入所有設定並按下**套用**儲存。

4.15.6.2 登入錯誤禁制

當有人嘗試數次但始終無法登入路由器時，Vigor 路由器系統將會暫時封鎖此網路連線以保護系統的安全性，目前共有五種協定 (Web User Interface, SSH, FTP, Telnet, PPTP/SSL) 可供設定，防止惡意攻擊。

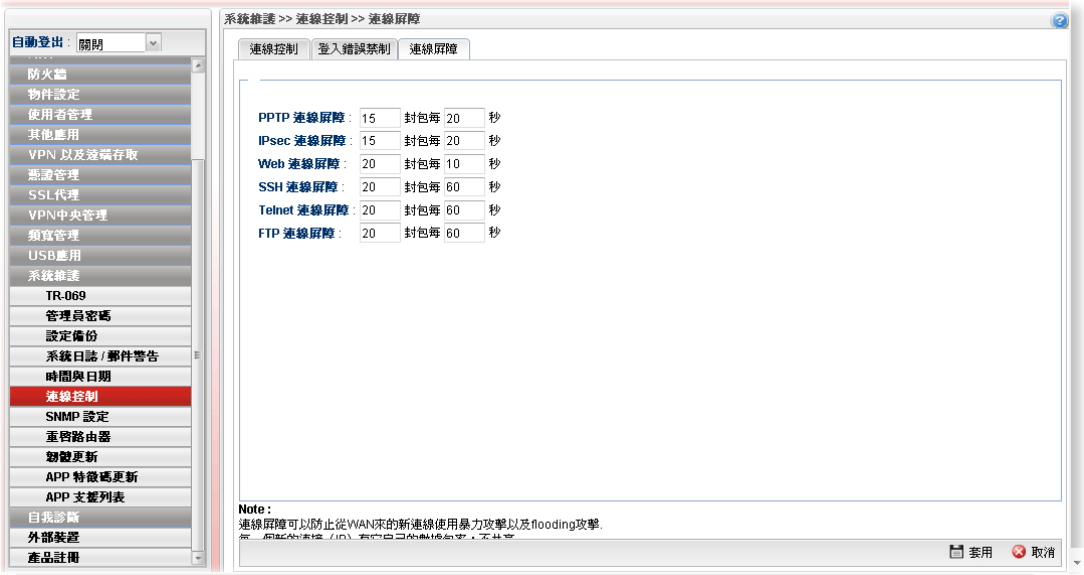


可用參數詳列如下：

項目	說明
啓用登入錯誤禁制	啓用防止惡意嘗試帳號密碼的功能。
Web UI/SSH/FTP/ TELNET/PPTP/SSL	啓用 – 啓用登入錯誤禁制功能(透過 Web UI/SSH/FTP/TELNET/PPTP/SSL 等不同協定)。 ● 登入最大錯誤次數 – 此處輸入的數字代表系統允許帳號密碼登入的最大錯誤嘗試次數。 ● 登入錯誤懲罰時間 – 設定使用者帳號密碼登入超出容忍限制後的封鎖時間。預設值爲 60 秒，亦即當使用者錯誤登入 Vigor 路由器數次(於登入最大錯誤次數定義)後，會封鎖此連線 60 秒，當時間限制已至，Vigor 路由器才會允許使用者繼續嘗試登入。 停用 – 停用登入錯誤禁制功能(透過 Web UI/SSH/FTP/TELNET/PPTP/SSL 等不同協定)。
套用	按此鈕儲存設定。
取消	按此鈕捨棄頁面設定。

4.15.6.3 連線屏障

本頁用於設定防止暴力攻擊以及 flooding 攻擊，確保表列之協定得以正常運作。



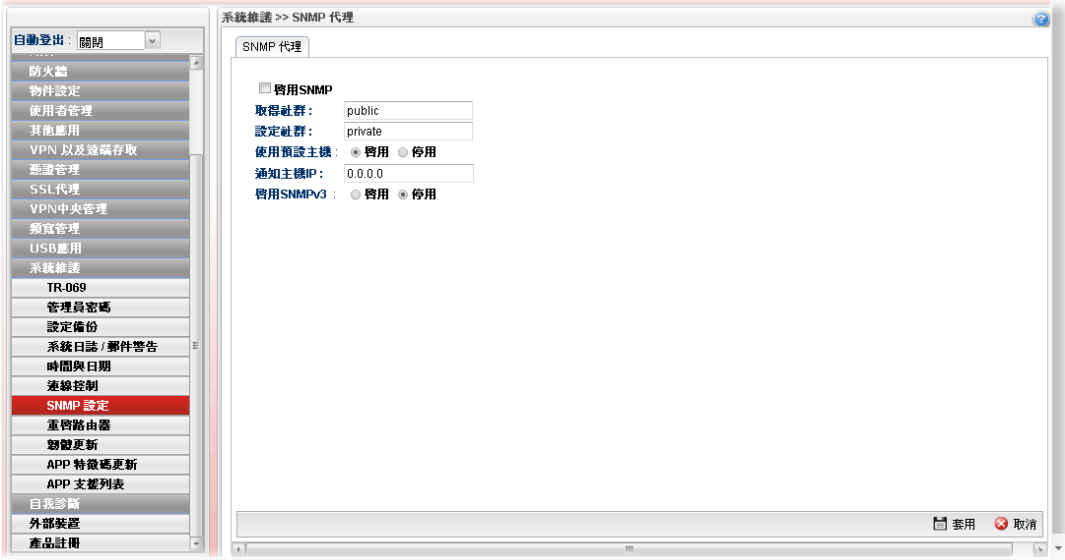
可用參數詳列如下：

項目	說明
PPTP/IPsec/Web/ SSH/Telnet/FTP 連線屏障	由於各項協定所使用的埠號，經常成爲攻擊的標的，因此限制 Vigor 路由器這些埠號的封包接收速率，可以避免來自外部的攻擊。
套用	按此鈕儲存設定。
取消	按此鈕捨棄頁面設定。

4.15.7 SNMP 設定

本頁讓您管理 SNMP 功能的相關設定。

在管理上，比起 SNMP，SNMPv3 是更爲安全的加密方式(支援 AES 與 DES)與驗證方法(支援 MD5 與 SHA)。



可用參數詳列如下：

項目	說明
啓用	勾選此框啓用此功能。
取得社群	輸入適當字元爲取得社群之名稱，預設值爲 **public**。
設定設群	輸入適當字元爲設定社群之名稱，預設值爲 **private**。
使用預設主機	按下**啓用**，使用主機預設的 IP 與遮罩爲 SNMP 代理者。 若您按下**停用**，您需手動輸入 IP 位址並選擇適當的遮罩。
通知主機 IP	輸入做爲通知用的主機之 IP 位址。
啓用 SNMPv3	按下**啓用**以啓動此功能。
USM 使用者	USM 表示以使用者爲基準的安全模式。 輸入驗證所需的使用者名稱。
驗證演算法	自下拉式清單中選擇一種驗算方式作爲驗證演算法。
驗證密碼(最小長度:8)	輸入驗證所需的密碼。
保密演算法	自下拉式清單中選擇一種驗算方式作爲保密演算法。
隱私密碼(最小長度:8)	輸入驗證所需的密碼。
隱私保護演算法	選擇下列一種方法作爲隱私保護演算法。
套用	按此鈕儲存設定。
取消	按此鈕捨棄頁面設定。

輸入所有設定並按下**套用**儲存。

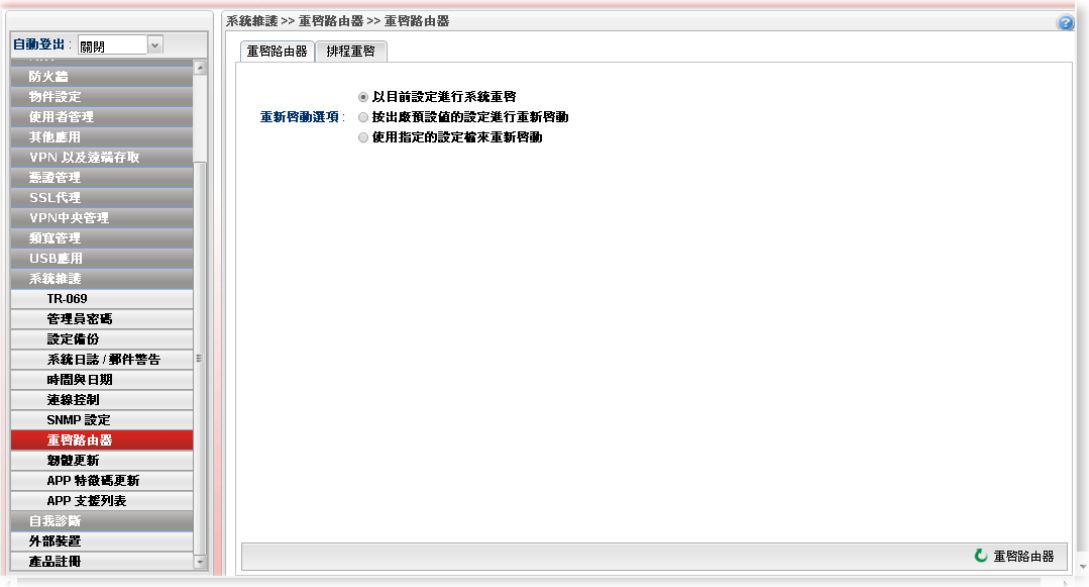
4.15.8 重啓路由器

Vigor 路由器系統可以從網頁瀏覽器執行系統重新啓動，每次網頁設定變更之後須重新啓動系統使可讓新設定生效。

如果您想要利用目前的設定來重新啓動路由器，請選擇”**以目前設定進行系統重啓**”並按下**重新啓動**按鈕；如果要讓路由器設定回復出廠預設值，請選擇”**按出廠預設值的設定進行重新啓動**”，再按下**重啓路由器**按鈕，路由器將需要一些時間進行啓動作業。

4.15.8.1 重啓路由器

開啓**系統維護>>重啓路由器**。

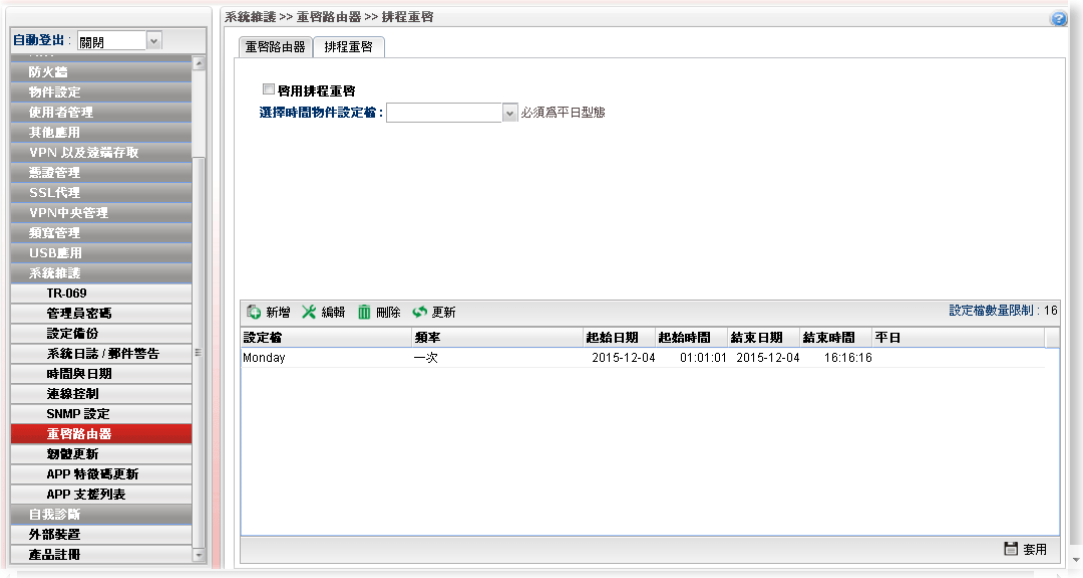


可用參數詳列如下：

項目	說明
以目前設定進行系統重啓	按此以便讓路由器採用目前的設定來重新啓動。
按出廠預設值的設定進行重新啓動	按此以便讓路由器採用出廠預設值來重新啓動。 **清除所有憑證檔案** – 一般來說出廠預設值並不包含憑證檔案，因此即使路由器以預設值重新啓動，憑證檔案還是會被保留下來，除非點選此項目。
使用指定的設定檔來重新啓動	按此以便讓路由器採用預先設定檔案來重新啓動，如果您選擇此項，畫面上將會出現**選擇設定檔**供您選擇套用的設定檔。
重啓路由器	按此鈕執行重新啓動作業。

4.15.8.2 排程重啓

Vigor 路由器可以在預定的時間重新啓動，勾選**啓用排程重啓**方塊，並從下拉式清單中選擇時間物件設定檔，按下**套用**之後，Vigor 路由器會在指定的時間重新啓動。



通常您必須先開啓**物件設定>>時間物件**設定必要的時間物件，如果未事先建立任何時間物件，您也可以直接自本頁設定需要的時間物件，按網頁下方的**新增**按鈕開啓設定對話盒，設定方式可以參考物件設定>>時間物件。

4.15.9 韌體更新

本頁將引導您如何透過本頁設定進行韌體更新。

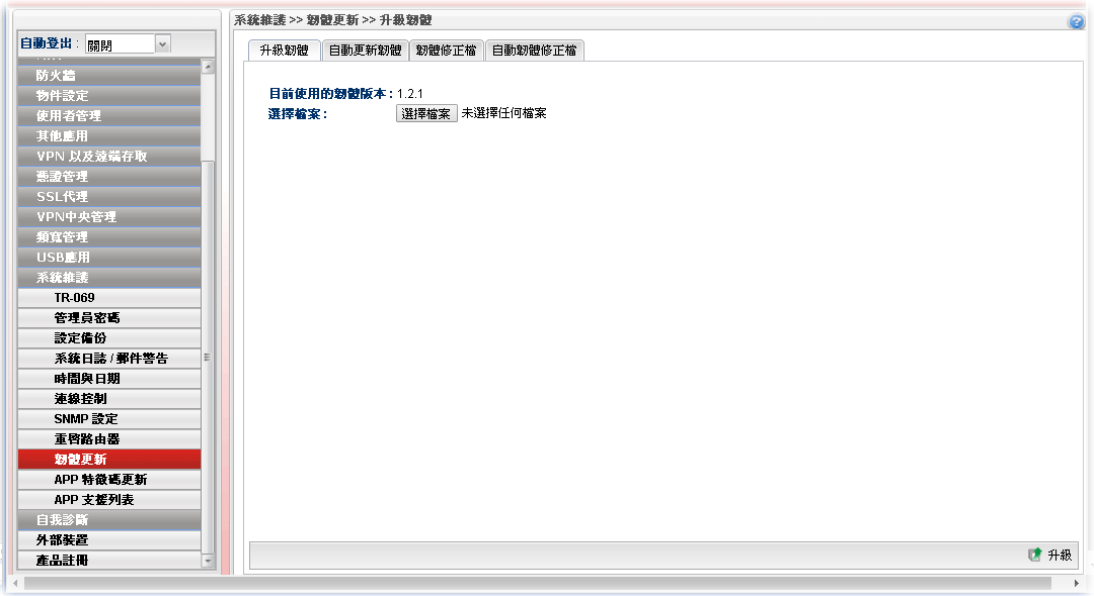
請先自居易網站(www.DrayTek.com) 或是 FTP 站點(ftp.DrayTek.com)下載最新的韌體。

開啓**系統維護>>韌體更新**。

4.15.9.1 升級韌體

本頁顯示目前使用的韌體版本，並允許您選擇最新的韌體並立刻更新至此路由器上。

使用者需事先連線到居易官網新韌體發佈之網址 (http://www.draytek.com.tw/ftp)下載韌體並存放於電腦上。

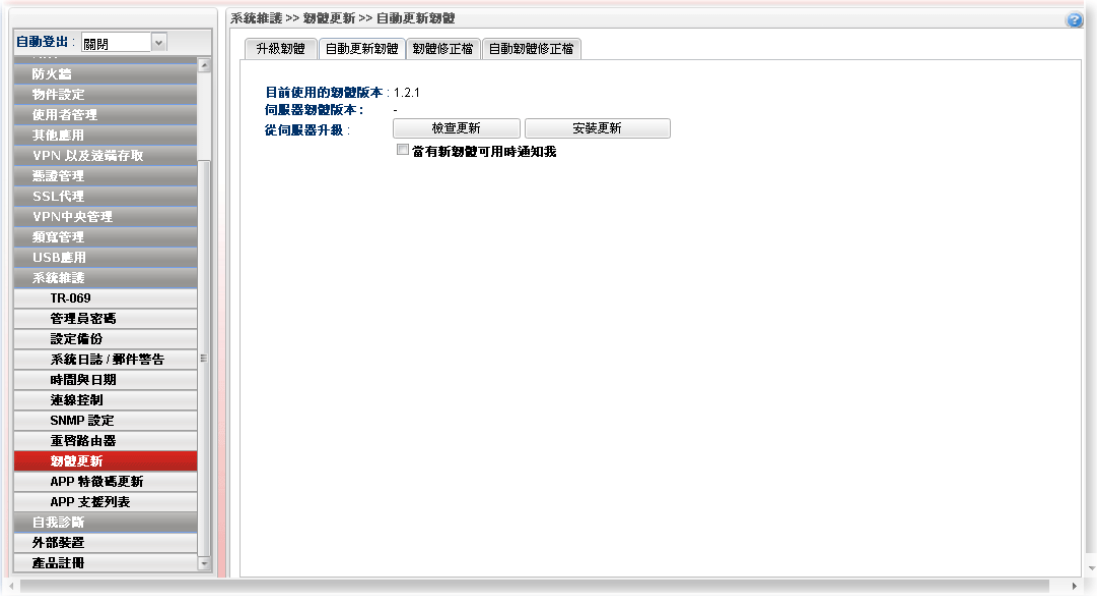


可用參數詳列如下：

項目	說明
目前使用的韌體版本	顯示目前使用中的韌體版本。
選擇檔案	按下**選擇檔案**按鈕挑選最新的韌體檔案。
升級	按此鈕執行韌體更新。

4.15.9.2 自動更新韌體

Vigor 路由器可自動連線到居易官網新韌體發佈之網址 (http://www.draytek.com.tw/ftp)下載/更新韌體，並於此一頁點選**檢查更新/安裝更新**及可完成新版韌體的安裝作業。

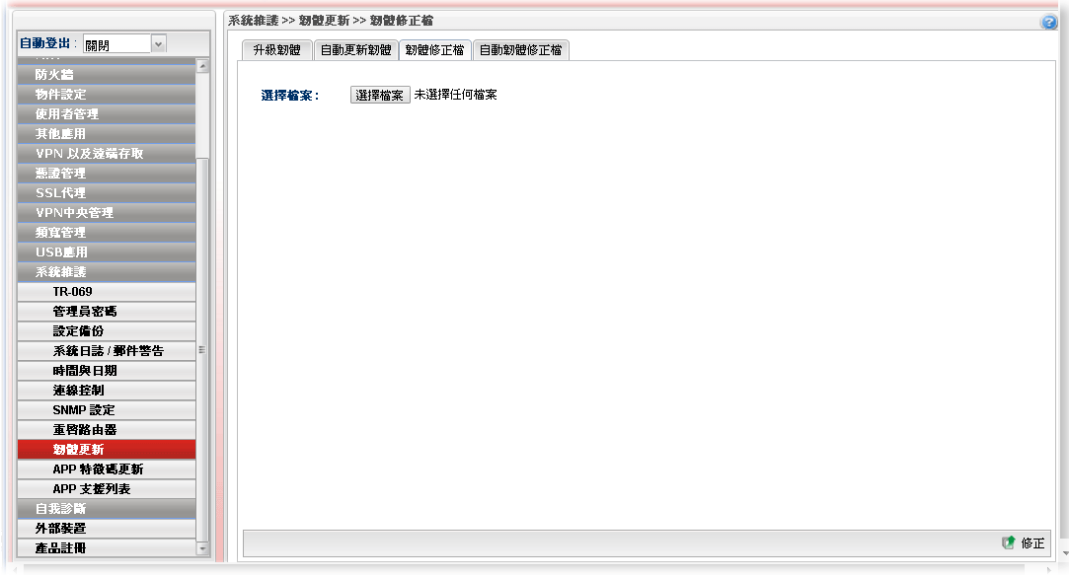


可用參數詳列如下：

項目	說明
伺服器韌體版本	顯示居易官網韌體發佈伺服器中的韌體版本。
從伺服器升級	**檢查更新** – 向居易官網韌體發佈伺服器詢問有無更新之韌體可用，若已有新韌體，路由器將自動下載最新的韌體至路由器上。 **安裝更新** – 若韌體發佈伺服器中韌体版本比存放於本機(路由器)中的版本新穎，則自動安裝新版韌體。 **當有新韌體可用時通知我** – 若勾選此方框，系統在偵測到新韌體之後，將會自動下載(但不會自動安裝) 並在使用者登入網頁設定介面時通知提示使用者。

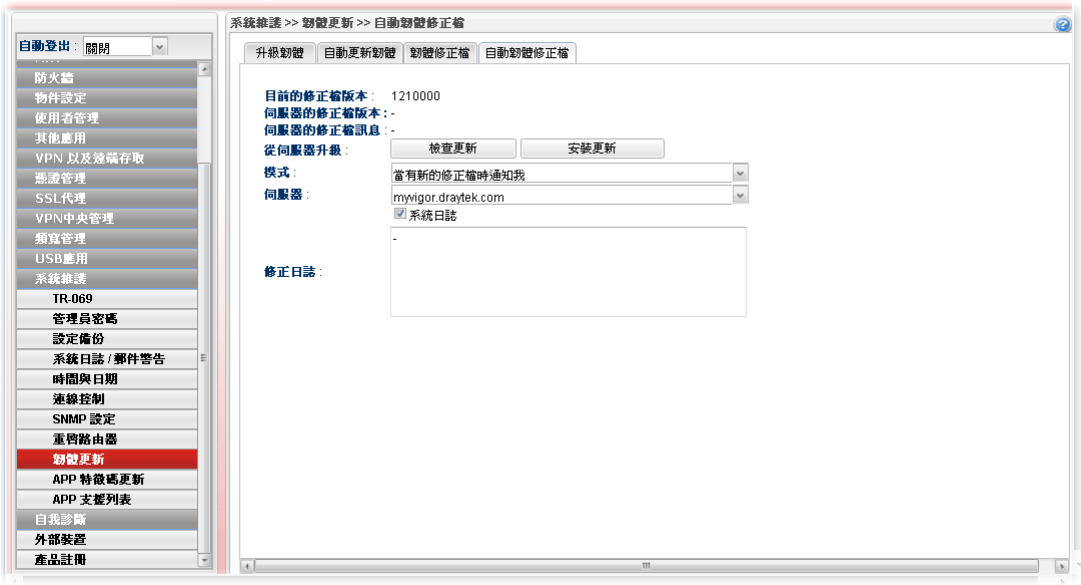
4.15.9.3 韌體修正檔

路由器管理者/使用者可以手動選擇檔案(.pat)以便修復/修正目前韌體發生之錯誤。通常此類含有立即修正之韌體可以從 DrayTek MyVigor 修正伺服器中取得。



4.15.9.4 自動韌體修正檔

路由器系統會自動下載最新含有修正內容的韌體，以便修復/修正目前韌體發生之錯誤。



可用參數詳列如下：

項目	說明
目前的修正檔版本	顯示目前系統上安裝的修正檔版本。
伺服器的修正檔版本	顯示居易 MyVigor 伺服器上最新的修正檔版本。
伺服器的修正檔訊息	顯示修正檔詳細資訊。
從伺服器升級	**檢查更新** – 按此鈕讓系統檢查並取得伺服器修正版本。 **安裝更新** – 按此鈕安裝伺服器修正版本至路由器中。
模式	有三種模式可以選擇： **手動更新** – 若選擇此模式，則只有在按下**檢查更新/安裝更新**之後系統才會進行檢查與安裝修正檔。

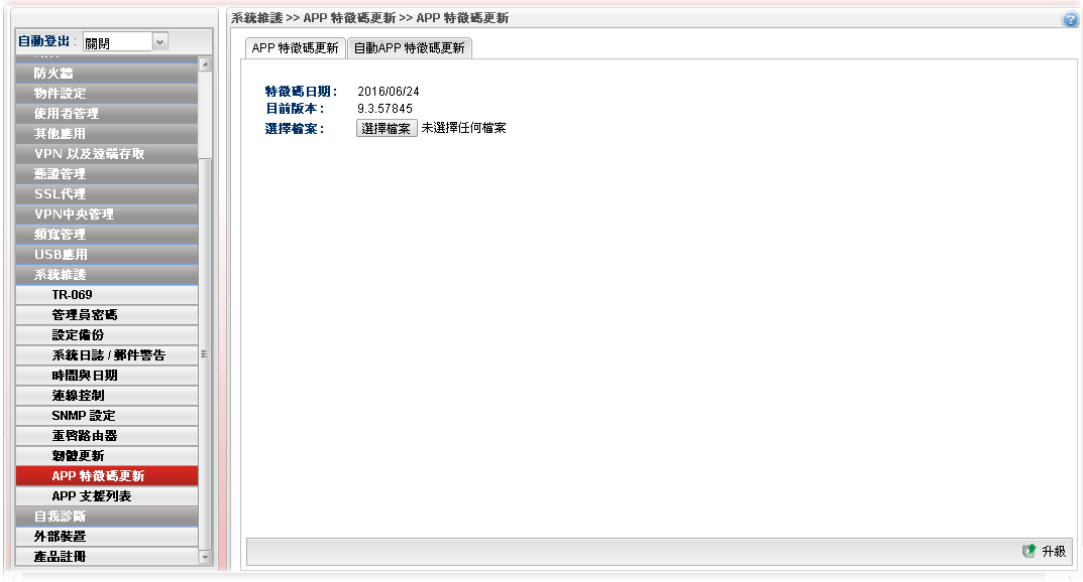
	當有新的修正檔時通知我 - 若選擇此模式，在偵測出最新的修正檔之後，路由器系統將會自動下載修正檔資訊並儲存在主機上。之後，當使用者登入路由器使用者設定介面時，系統會在登入視窗給予提示通知使用者。 **當新的修正檔可用時自動更新-** 若是修正資訊儲存在 MyVigor 伺服器比儲存在主機內的資訊還要新穎，路由器將會自動下載並更新爲最新的韌體修正資訊。
伺服器	使用下拉式清單指定適合的伺服器。
Syslog	勾選此框將修正日誌儲存在 Syslog 上。
修正日誌	韌體修正若被執行，本區會顯示與有修正相關的日誌內容。

4.15.10 APP 特徵碼更新

路由器採用的 APP 物件設定檔被視爲 APP 特徵碼。居易將定期更新所支援的特徵碼的版本資訊。然而，若由使用者一個接一個來更新 APP 特徵碼，顯得有些不便，本功能乃特別設計用於提供快速執行 APP 版本資訊更新事宜，使用者可手動執行 APP 特徵碼更新或是設定本頁內容讓 Vigor 路由器自動執行 APP 特徵碼更新。

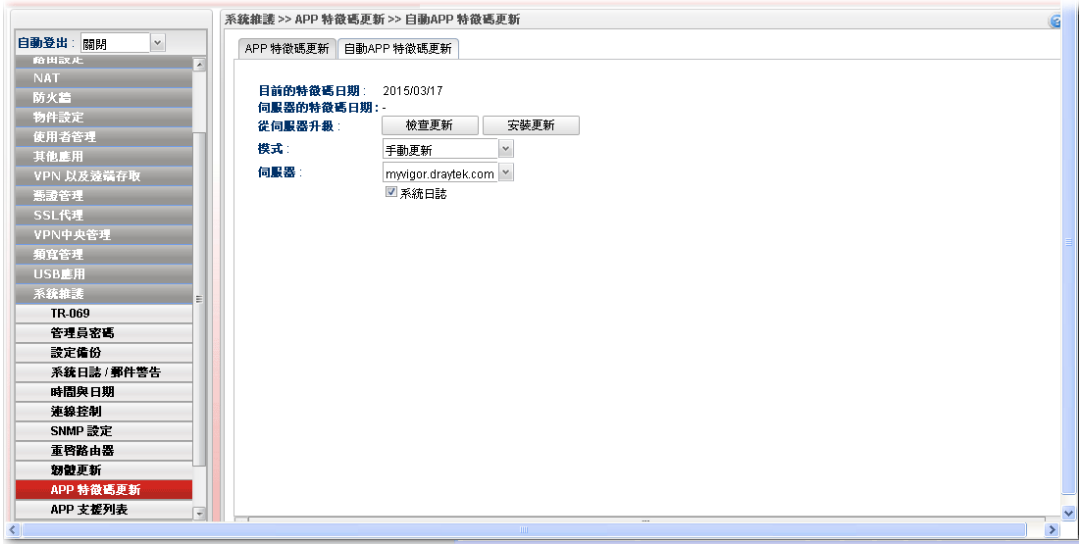
4.15.10.1 APP 特徵碼更新

更新 APP 特徵碼之前，請先按下本頁的**選擇**按鈕，稍後，再按下**更新**執行特徵碼更新事宜。



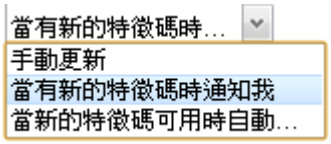
4.15.10.2 自動 APP 特徵碼更新

本頁讓路由器執行特徵碼自動更新事宜。



可用參數詳列如下：

項目	說明

目前的特徵碼日期	顯示目前安裝於路由器中特徵碼**安裝日期**。
伺服器的特徵碼日期	顯示記錄於伺服器(myvigor.draytek.com 或是 myvigoreu.draytek.com)中最新的特徵碼版本。
從伺服器升級	自 MyVigo 伺服器(myvigor.draytek.com 或是 myvigoreu.draytek.com)取得最新的特徵碼資訊。 **檢查更新** – 向 MyVigor 伺服器詢問有無更新之特徵碼資訊，若已有之，路由器將自動下載最新的特徵碼資訊至路由器上。 **安裝更新** – 若 MyVigo 伺服器(myvigor.draytek.com 或是 myvigoreu.draytek.com)中特徵碼資訊比存放於本機(路由器)中的資訊新穎，則自動下載特徵碼資訊。
模式	選擇執行 APP 特徵碼更新條件或是傳送通知訊息。  **手動更新** – 若選擇此模式，則檢查與安裝特徵碼資訊僅在手動按下**檢查更新/安裝更新**時才會執行。 **當有新的特徵碼時通知我** - 若選擇此模式，當系統偵測到 MyVigor 伺服器已有最新的特徵碼資訊，Vigor 路由器系統將自動下載特徵碼資訊並儲存在主機中，之後當使用者再度登入路由器設定介面時，系統將於登入視窗中給予提示通知使用者相關資訊。 **當有新的特徵碼可用時自動…**- 若選擇此模式，若 MyVigor 伺服器中的特徵碼資訊比主機(Vigor 路由器)中的資料還要新穎，路由器將會自動下載並更新最新的特徵碼資訊。
伺服器	自下拉式清單中選擇適當的特徵碼伺服器。目前有二種伺服器(myvigor.draytek.com 或是 myvigoreu.draytek.com)可供選擇。
系統日誌	勾選此方框紀錄相關資訊於 Syslog 中。

4.15.11 APP 支援列表

APP 支援列表可顯示 Vigor 路由器支援的 APP 應用程式的版本為何。所有的 APP 都分別歸類於 IM、P2P、通訊協定與其他項目底下。

4.16 自我診斷

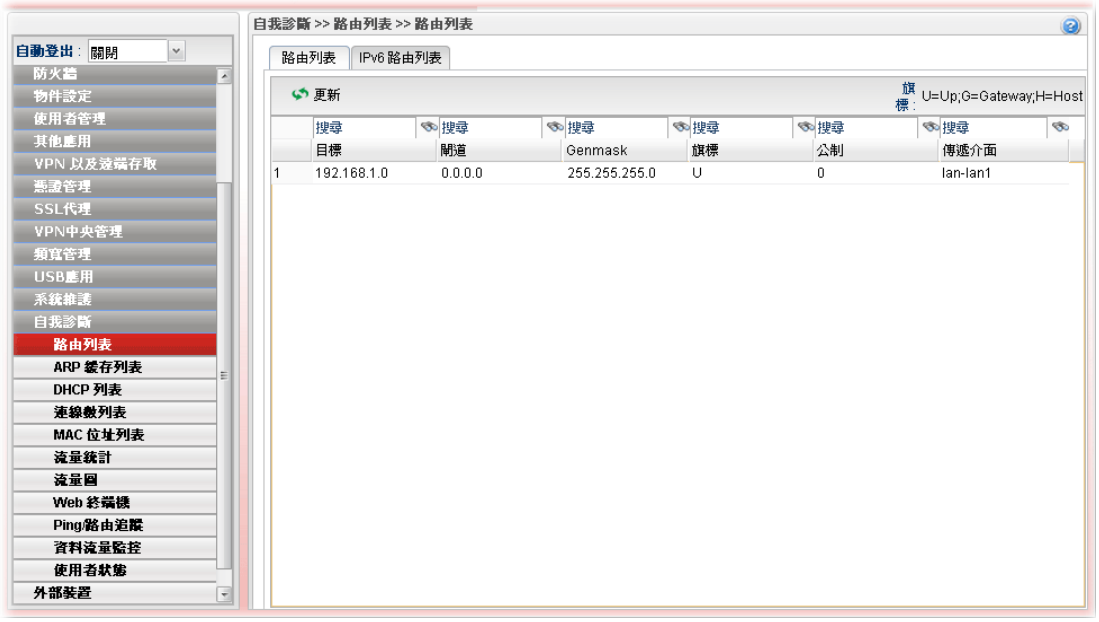
在某些情況下，使用者可能會需要知道與路由器有關的資訊，像是固定或動態資料庫或其他的路由資料。Vigor2960 提供數種功能如路由列表、ARP 暫存列表、DHCP 列表、NAT 連線數列表、流量圖、Web 終端機、Ping/路由追蹤、資料流量控制等等，讓使用者得以輕鬆的檢視有關資訊。

4.16.1 路由列表

從**自我診斷**選單中選擇**路由列表**，開啓如下頁面：

4.16.1.1 路由列表

顯示每條路由的細部內容。



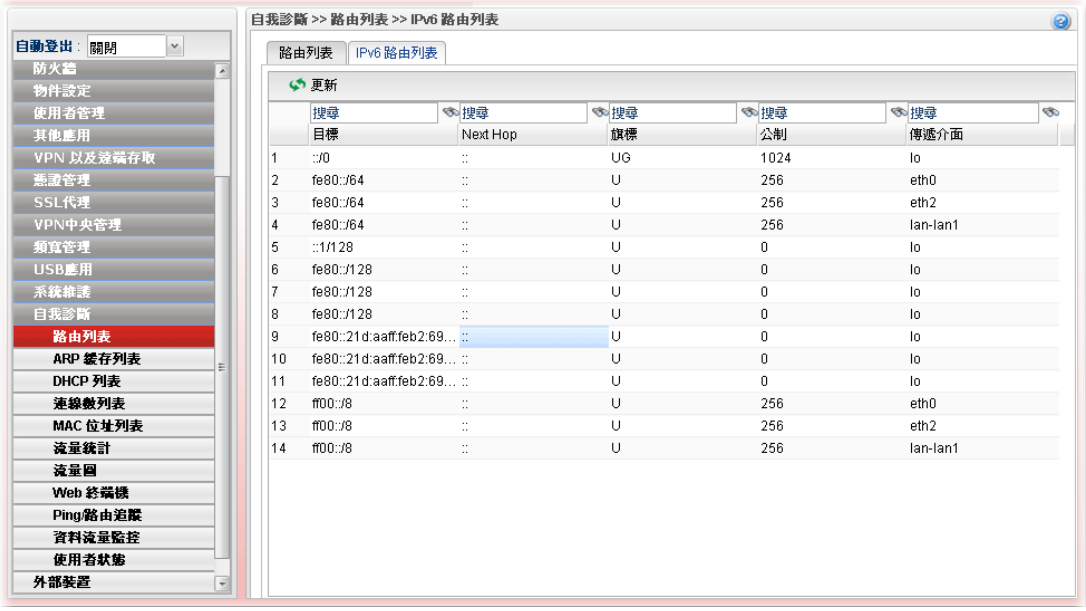
每個項目說明如下：

項目	說明
更新	重新更新本頁面。

搜尋	移動滑鼠至搜尋方框，按下滑鼠鍵並輸入關鍵字，系統將顯示與此關鍵字相關的紀錄。
目標	顯示不同路由的目標 IP 位址為何。
閘道	顯示預設的閘道 IP 位址。
Genmask	顯示不同路由的子網遮罩位址。
旗標	顯示每條路由的旗標內容，可能的旗標條列如下： U (表示路由已開啓並使用中) H (目標區是台主機) G (使用閘道) R (針對動態路由重新恢復路徑) D (透過過程或是重新引導方式來安裝) M (自路由過程修正或是重新引導) A (透過 *addrconf* 安裝) C (每條路由) **! (**路由被拒**)**
公制	顯示至目標的距離(通常以跳躍來計算)，某些路由過程需要此項資訊。
傳遞介面	此路由方向以 LAN/WAN 設定檔來顯示(從 LAN/WAN 設定檔開始到 LAN/WAN 設定檔結束)。

4.16.1.2 IPv6 路由列表

顯示每條透過 IPv6 協定來路由的細部內容。



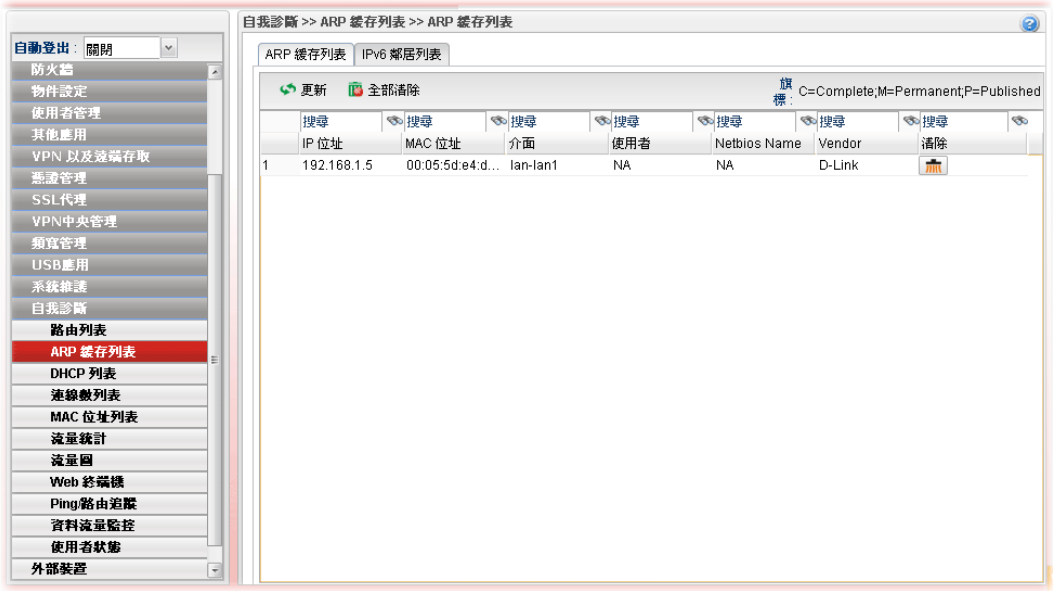
每個項目說明如下：

項目	說明
更新	重新更新本頁面。
搜尋	移動滑鼠至搜尋方框，按下滑鼠鍵並輸入關鍵字，系統將顯示與此關鍵字相關的紀錄。
目標	顯示不同路由的目標 IP 位址為何。
Next Hop	顯示此路由的下一跳 IP 位址。
旗標	顯示每條路由的旗標內容，可能的旗標條列如下： U (表示路由已開啓並使用中) H (目標區是台主機) G (使用閘道) R (針對動態路由重新恢復路徑) D (透過過程或是重新引導方式來安裝) M (自路由過程修正或是重新引導) A (透過 *addrconf* 安裝) C (每條路由) **! (**路由被拒**)**
公制	顯示至目標的距離(通常以跳躍來計算)，某些路由過程需要此項資訊。
傳遞介面	此路由方向以 LAN/WAN 設定檔來顯示(自 LAN/WAN 設定檔開始到 LAN/WAN 設定檔結束)。

4.16.2 ARP 緩存列表

從**自我診斷**選單中選擇 **ARP 緩存列表**檢視路由器中 ARP 緩存的內容，表格顯示乙太網路硬體位址(MAC 位址)與 IP 位址的對應關係：

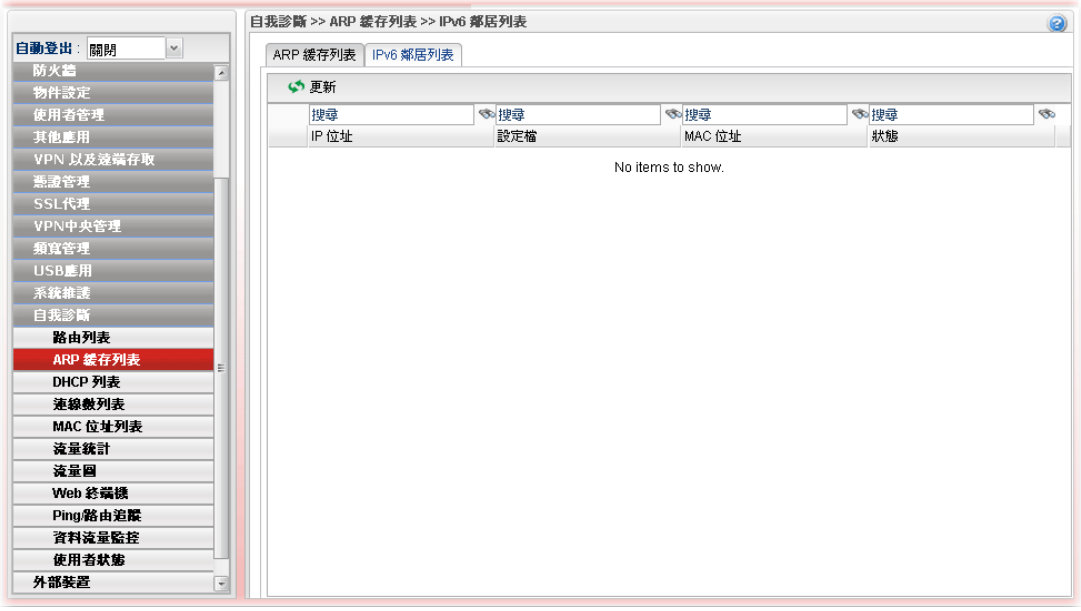
4.16.2.1 ARP 緩存列表



每個項目說明如下：

項目	說明
更新	重新更新本頁面。
全部清除	清除本頁中全部的資訊。
搜尋	移動滑鼠至搜尋方框，按下滑鼠鍵並輸入關鍵字，系統將顯示與此關鍵字相關的紀錄。
IP 位址	顯示不同 ARP 緩存內容的 IP 位址。
MAC 位址	顯示不同 ARP 緩存的 MAC 位址。
介面	顯示 ARP 緩存的介面資訊。
使用者	顯示使用者的身分/名稱。
Netbios Name	顯示 **Netbios Name** 的名稱。
Vendor	顯示什麼裝置供應商名稱.
清除	刪除選定的設定檔。

4.16.2.2 IPv6 鄰居列表



每個項目說明如下：

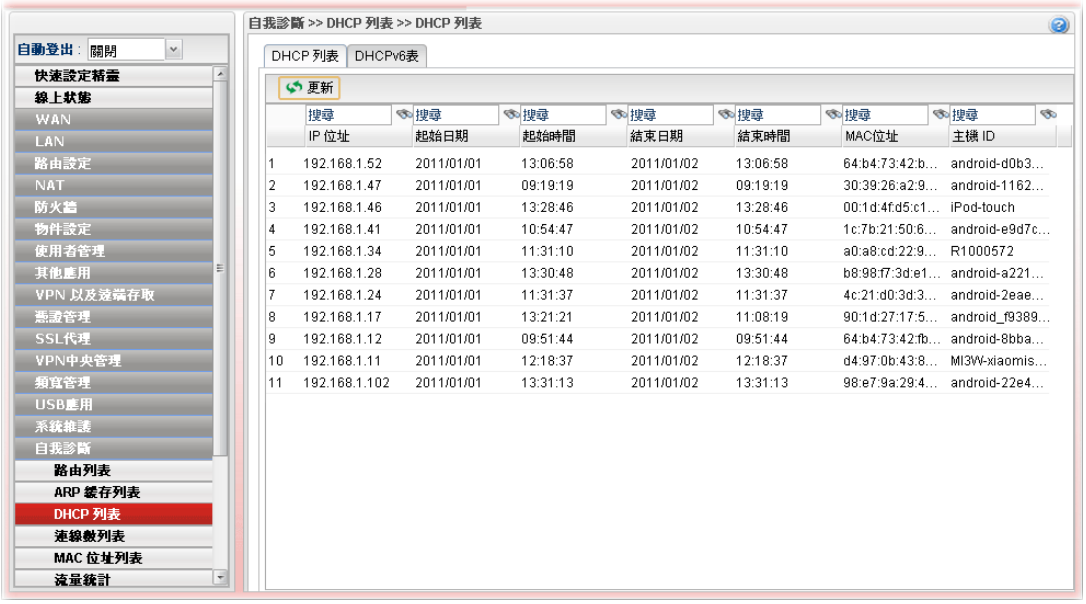
項目	說明
更新	重新更新本頁面。
搜尋	移動滑鼠至搜尋方框，按下滑鼠鍵並輸入關鍵字，系統將顯示與此關鍵字相關的紀錄。
IP 位址	顯示相鄰裝置的 IPv6 位址。
設定檔	顯示相鄰裝置的介面。
MAC 位址	顯示相鄰裝置的 MAC 位址。
狀態	顯示相鄰裝置的狀態： **INCOMPLETE** -位址搜尋中，尚未找到該裝置的位址。 **REACHABLE** - 最近可達相鄰裝置位址(10 秒內)。 **STALE**- 無法到達相鄰裝置，不過資料仍可傳輸到相鄰裝置，但不再嘗試驗證其可達性。 **DELAY** - 無法到達相鄰裝置，且最近有傳輸資料至該相鄰裝置。 不利及探測相鄰裝置，延遲傳送探測訊息以便讓上層協定有機會提供可達確認訊息。 **PROBE** - 無法到達相鄰裝置，單播送的相鄰裝置請求會被傳送出去以便驗證可達性。

4.16.3 DHCP 列表

這個頁面提供 IP 位址分派的相關資訊，對診對網路問題來說，這類資訊相當有用。

4.16.3.1 DHCP 列表

從**自我診斷**選單中選擇 **DHCP 列表**，開啓如下頁面：

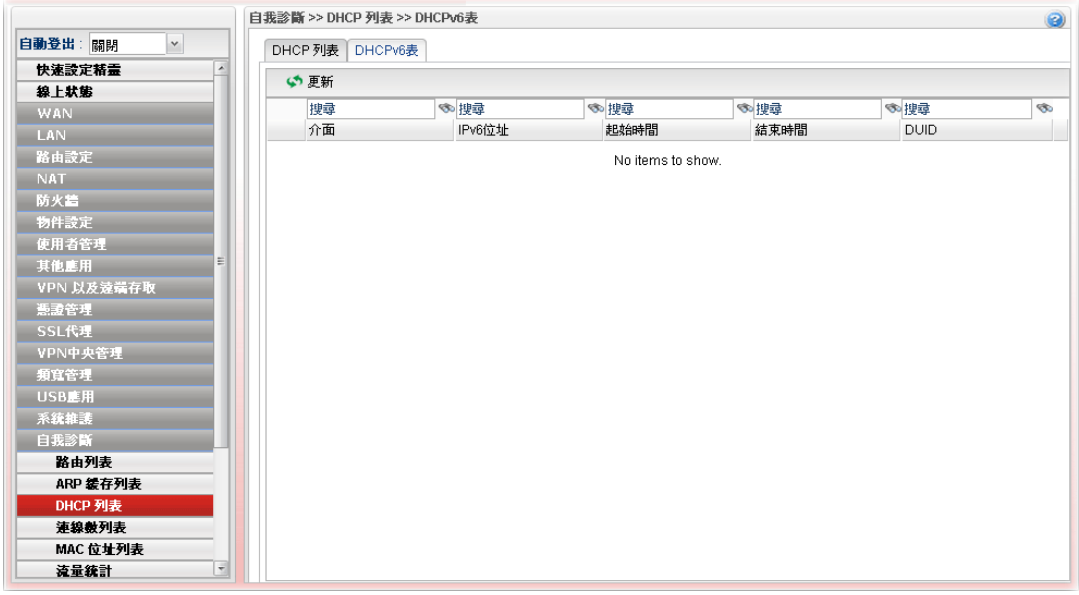


每個項目說明如下：

項目	說明
更新	重新更新本頁面。
搜尋	移動滑鼠至搜尋方框，按下滑鼠鍵並輸入關鍵字，系統將顯示與此關鍵字相關的紀錄。
IP 地址	顯示 DHCP 伺服器的 IP 位址。
起始日期	顯示 DHCP 伺服器啓動的起始日期。
起始時間	顯示 DHCP 伺服器啓動的起始時間。
結束日期	顯示 DHCP 伺服器關閉的結束日期。
結束時間	顯示 DHCP 伺服器關閉的結束時間。
MAC 位址	顯示 DHCP 伺服器的 MAC 位址。
主機 **ID**	顯示主機的 IP 位址。

4.16.3.2 DHCPv6 列表

按下 **DHCPv6** 列表標籤開啓此頁面。

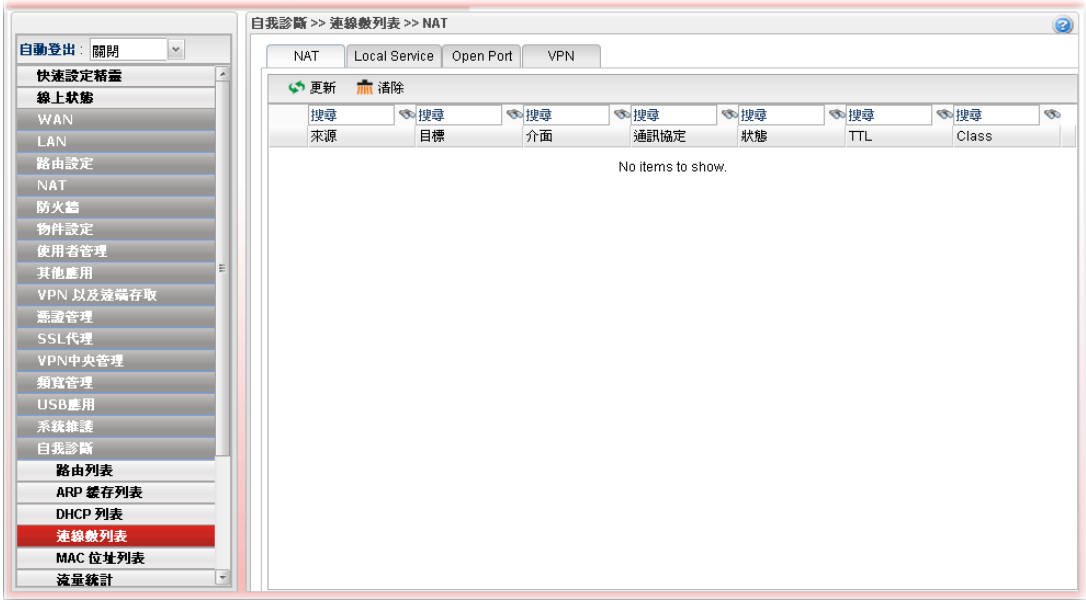


每個項目說明如下：

項目	說明
更新	重新更新本頁面。
搜尋	移動滑鼠至搜尋方框，按下滑鼠鍵並輸入關鍵字，系統將顯示與此關鍵字相關的紀錄。
介面	顯示 DHCP 伺服器使用的介面。
IPv6 位址	顯示 DHCP 伺服器的 IPv6 位址。
起始時間	顯示 DHCP 伺服器啓動的起始時間。
結束時間	顯示 DHCP 伺服器關閉的結束時間。
DUID	顯示 DUID 細部資訊。

4.16.4 NAT 連線數列表

這個列表清單可以顯示 20 頁 30000 筆左右的連線數資料。按下 NAT、Local Service、Open Port 或是 VPN 檢查細部的內容。



每個項目說明如下：

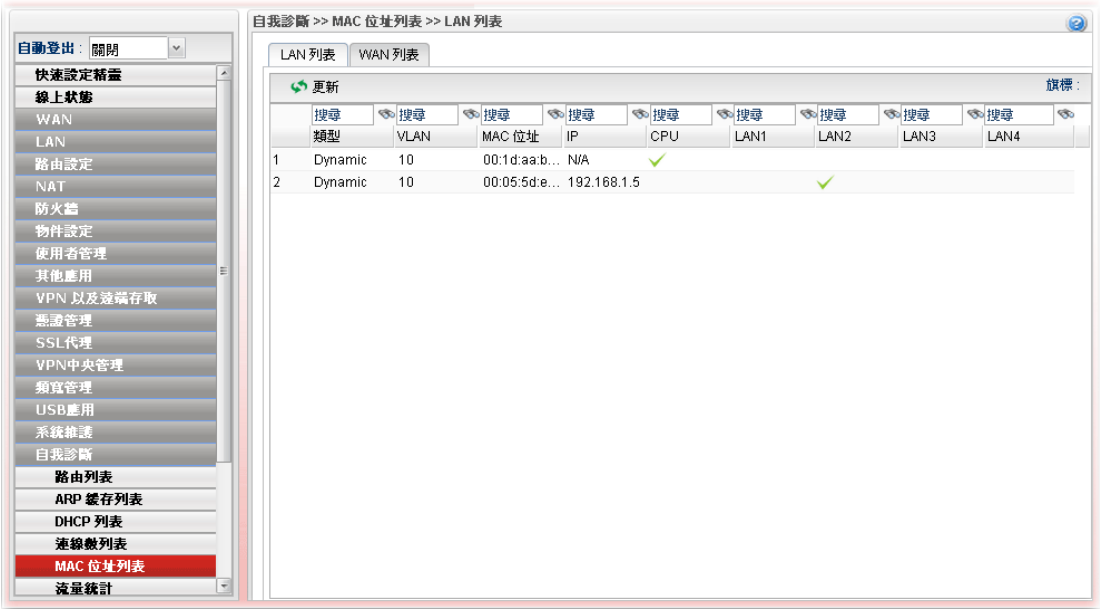
項目	說明
更新	重新更新本頁面。
清除	清除本頁資料。
搜尋	移動滑鼠至搜尋方框，按下滑鼠鍵並輸入關鍵字，系統將顯示與此關鍵字相關的紀錄。
來源	顯示來源 IP 位址與本地 PC 的連接埠號。
目標	顯示目的 IP 位址與遠端主機的連接埠號。
介面	顯示使用的 WAN 介面。
通訊協定	顯示此 NAT 連線數使用的協定。
狀態	顯示 TCP 連線的實際狀態。
TTL	顯示連結跟蹤存活的時間。

4.16.5 MAC 位址列表

MAC 位址表格最多可條列 8192 條內容，可以先利用 VLAN ID，然後再以 MAC 位址來排序。

每頁可以展示 999 條 MAC 位址的內容，預設值是 20 條，當第一次造訪本頁時，網頁會顯示首 20 條內容，VLAN ID 號碼最低以及 MAC 位址較小的內容會由上而下顯示出來。

按下**更新**按鈕則可更新目前的表格內容。



4.16.6 流量統計

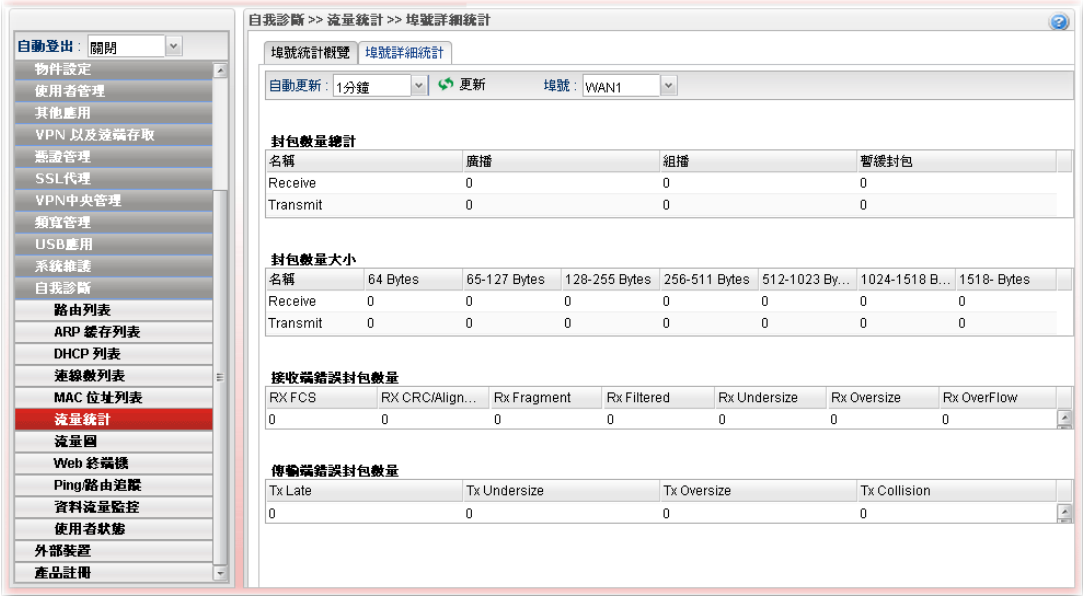
埠號統計概覽本頁提供所有連接埠一般資料傳送流量統計概況。

每個項目說明如下：

項目	說明

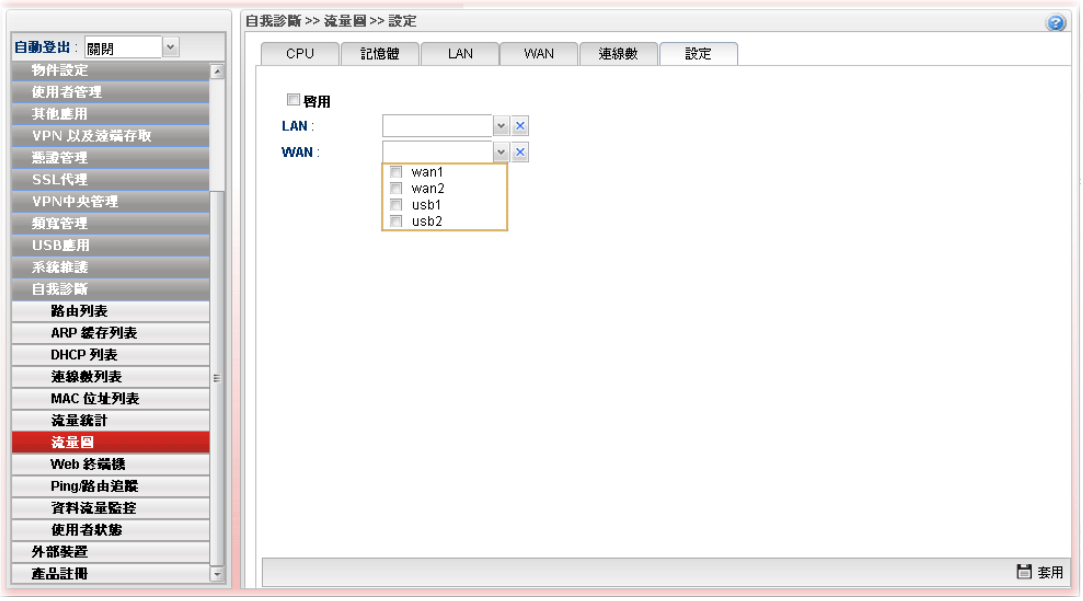
更新	重新更新本頁面。
清除	按此鈕清除全部埠號的計數資料。
埠號	顯示資料傳輸需透過的介面。
接收端/傳輸端(封包)	顯示在接收與傳送中資料封包的大小。
接收端/傳輸端(Bytes)	顯示每個埠號接收與傳送的位元數。
接收端/傳輸端(錯誤)	顯示資料在接收與傳送中產生的錯誤數。
過濾接收	顯示轉送過程中被過濾的接收訊框數。

埠號詳細統計頁顯示 WAN/LAN 介面的細部統計資料。



4.16.7 流量圖

從**自我診斷**選單中選擇**流量圖**，開啓如下頁面，指定 LAN 與 WAN 設定檔來顯示 CPU、記憶體、LAN、WAN 與連線數設定的相應圖面。



每個項目說明如下：

項目	說明
設定	在本頁，可指定需套用的 LAN 設定檔與 WAN 設定檔，系統將以此爲基準呈現出流量圖。 **啓用**–.勾選此方塊啓用此設定檔。 **LAN** –使用下拉式選項選擇 LAN 設定檔。 **WAN** –使用下拉式選項選擇 WAN 設定檔。 **套用**-按下此鈕儲存設定標籤下的內容。
CPU	按下 CPU 標籤。 有數種選項供您使用來呈現圖面。 **最近 24 小時**–顯示 CPU 操作在最近 24 小時中的相關資訊。 **最近 7 天**–顯示 CPU 操作在最近 7 天中的相關資訊。 **最近 4 周**–顯示 CPU 操作在最近 4 個星期中的相關資訊。
記憶體	按下記憶體標籤。 有數種選項供您使用來呈現圖面。 **最近 24 小時**–顯示記憶體操作在最近 24 小時中的相關資訊。 **最近 7 天**–顯示記憶體操作在最近 7 天中的相關資訊。 **最近 4 周**–顯示記憶體操作在最近 4 個星期中的相關資訊。
LAN	按下 LAN 標籤。 有數種選項供您使用來呈現圖面。

項目	說明
	網路介面 –顯示 LAN 操作的相關資訊。 **最近 24 小時**–顯示 LAN 操作在最近 24 小時中的相關資訊。 **最近 7 天**–顯示 LAN 操作在最近 7 天中的相關資訊。 **最近 4 周**–顯示 LAN 操作在最近 4 個星期中的相關資訊。
WAN	按下 WAN 標籤。 有數種選項供您使用來呈現圖面。 **網路介面** – 顯示 WAN 或是 WAN 操作的相關資訊。 **最近 24 小時** – 顯示 WAN 操作在最近 24 小時中的相關資訊。 **最近 7 天**–顯示 WAN 操作在最近 7 天中的相關資訊。 **最近 4 周**–顯示 WAN 操作在最近 4 個星期中的相關資訊。

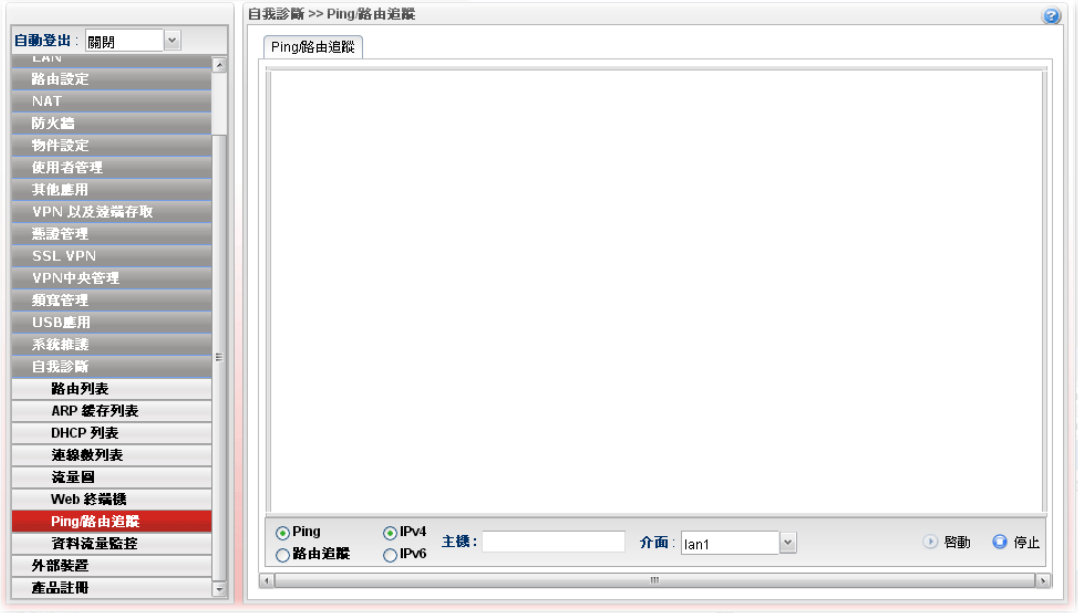
下圖顯示 CPU 的流量圖面：

4.16.8 Web 終端機

從**自我診斷**選單中選擇 **Web 終端機**，開啓如下頁面，您可以在此頁面上輸入終端機常用指令，遠端使用者可透過此網頁來操作 Vigor2960 而無須安裝、開啓連線工具。

4.16.9 Ping/路由追蹤

本頁讓您追蹤路由器至主機的路由，只要輸入主機的 IP 位址並按下**啓動**按鈕即可，路由結果隨即顯示在螢幕上。



每個項目說明如下：

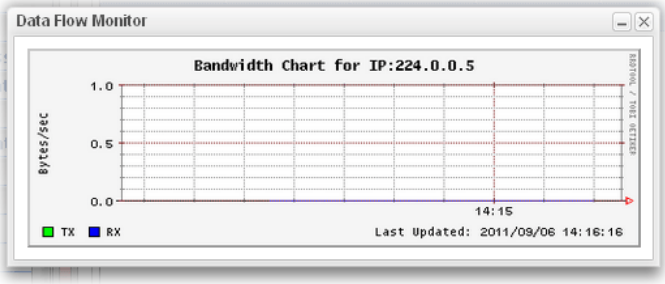
項目	說明
Ping /路由追蹤	選擇 **Ping** 以便執行動作。 選擇**路由追蹤**以便啓動此功能。
IPv4 / IPv6	選擇 IPv4 /IPv6 決定您要輸入的 IP 位址格式。
主機	輸入主機的 IP 位址。
介面	選擇 LAN 或是 WAN 設定檔套用至此功能。
啓動	啓動 Ping 或是路由追蹤動作。
停止	停止 Ping 或是路由追蹤動作。

4.16.10 資料流量監控

本頁顯示受到監控的 IP 位址的運作過程，並且每間隔數秒便更新一次網頁。

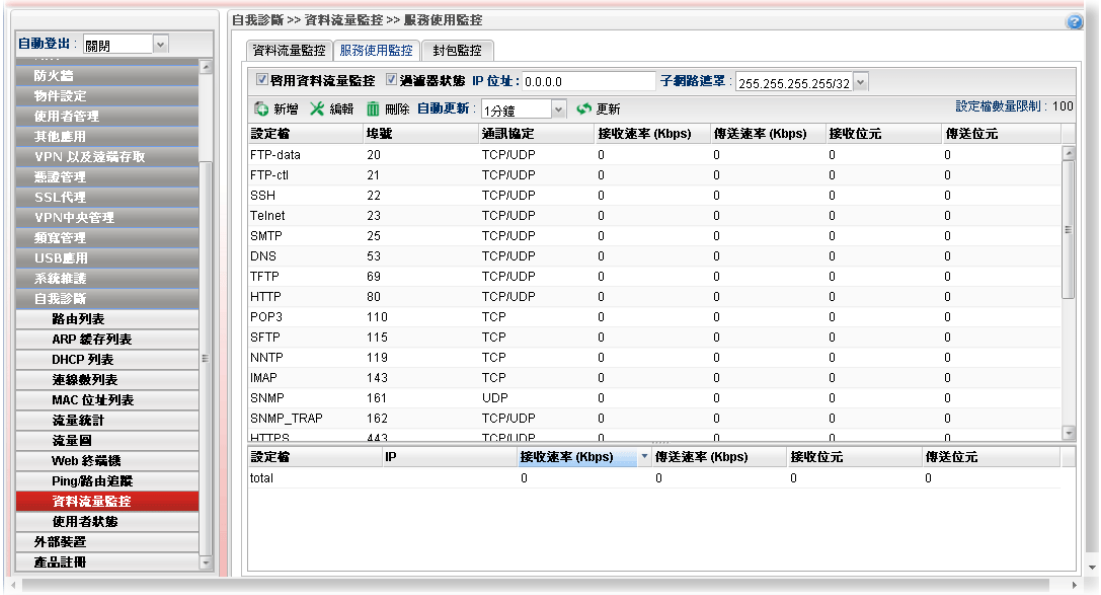
4.16.10.1 資料流量監控

每個項目說明如下：

項目	說明
啓用資料流量監控	勾選此方塊啓用此功能。
封鎖	避免指定的 PC 在 5 分鐘內存取網際網路。
解鎖	允許指定的 PC 在 5 分鐘內存取網際網路。
圖表	按下此鈕可以描繪圖表出來，可參考下圖。 
最近 1 小時/ 最近 24 小時/最近 7 天	顯示 1 小時/24 小時/7 天內的紀錄。
自動更新	可指定更新資料的時間間隔。
更新	按下此鈕，讓系統直接更新頁面資料。
IP 地址	顯示監控裝置的 IP 位址。
RX rate (Kbps)	顯示監控裝置的接收速度。
上傳速率(Kbps)	顯示監控裝置的傳送速度。

下載位元	顯示資料的接收大小。
上傳位元	顯示資料的傳輸大小。
連線數	顯示限制連線數網頁中所指定的連線數。
封鎖時間	顯示封鎖期間有多長。
設定檔	顯示 WAN 介面設定檔。
IP	顯示 WAN 介面設定檔的 IP 位址。
接收/傳送速率	顯示接收/傳送的資料速率。
接收/傳送位元	顯示接收/傳送的資料量。

4.16.10.2 服務使用監控

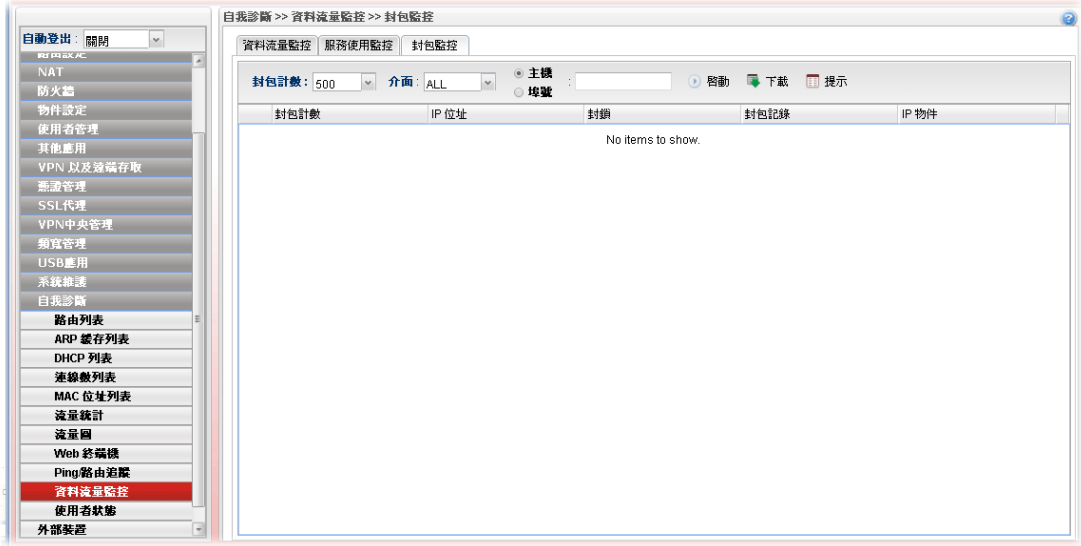


每個項目說明如下：

項目	說明
啓用資料流量監控	勾選此框啓用此功能。

4.16.10.3 封包監控

本頁目的用於擷取封包並進行初步分析。

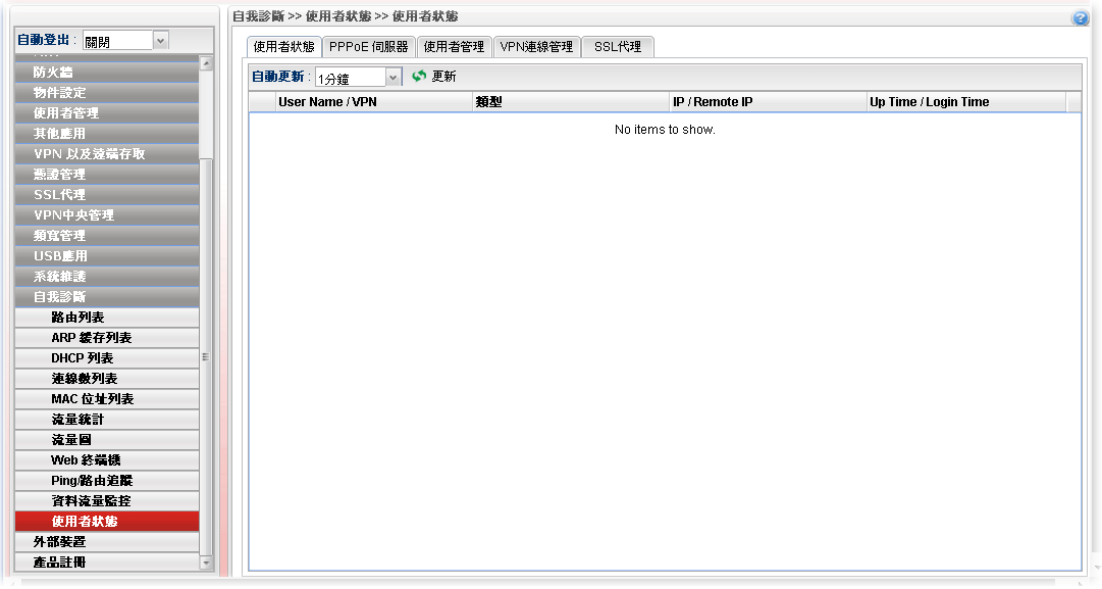


每個項目說明如下：

項目	說明
封包計數	設定封包擷取的數量最高值。若達到此門檻值，系統將停止封包擷取。
介面	指定用以擷取封包的介面。預設值爲全部(All) 。
主機 / 埠號	輸入您想要監控的主機其相關的 IP 位址或是監控的埠號。
啓動	選此鈕以擷取封包並顯示結果在頁面上。
下載	路由器擷取的封包會以“packetmonitor.pcap”檔名儲存在路由器內，請按此鈕下載此檔並儲存在主機上。
提示	跳出之視窗會顯示與此功能有關的特殊說明。

4.16.11 使用者狀態

本頁顯示使用者、PPPoE 伺服器、使用者管理、VPN 連線管理與 SSL 代理等相關參考資料。



4.17 外部裝置

Vigor 路由器可用來連接多種外接裝置類型，爲了方便控制及管理外接裝置，可開啓這個網頁進行細部的設定。

每個項目說明如下：

項目	說明
自動搜尋外部裝置	勾選此方塊可以偵測連接到路由器 Vigor2960 的外接裝置。
更新	重新更新本頁面。
狀態	顯示外接裝置目前的開啓狀態。
型號	顯示外接裝置的型號。
MAC 位址	顯示外接裝置的 MAC 位址。

IP 位址	顯示外接裝置的 IP 位址。
連線時間	顯示外接裝置連接到路由器的連線時間。
清除	當外接裝置斷線時可移除與該裝置相關的紀錄。

勾選啓用外部裝置核取方塊，稍後，與路由器相連接的所有可用的外接裝置及相關資訊都會顯示在本頁上。

注意:此功能只能偵測出居易的產品。

4.18 產品註冊

請參考第 2.3 節註冊 Vigor 路由器取得更多資訊。

本頁留白

第五章: 疑難排解

這個章節將會指導您，如何解決在完成安裝和設置路由器後依然無法上網的問題。請按以下方法一步一步地進行檢查。

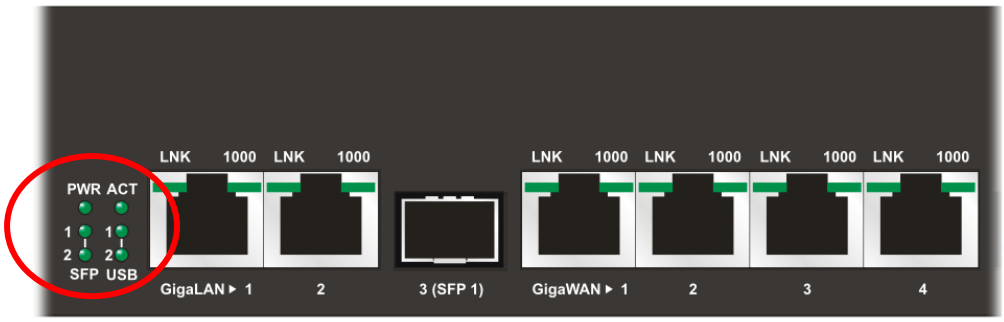
- 檢查路由器硬體狀態是否正常
- 檢查您電腦的網路連接設置是否正確
- 試試看能否從電腦 ping 到路由器
- 檢查 ISP 的設置是否正常
- 必要的話將路由器恢復至預設出廠設置

如果以上步驟仍無法解決您的問題，您需要聯絡代理商取得進一步的協助。

5.1 檢查路由器硬體狀態是否正常

按以下步驟檢查硬體狀態：

1. 檢查電源線以及 LAN 的連接。詳細資訊請參考“**1.3 硬體安裝**”。
2. 開啓路由器，確認 **ACT** 指示燈差不多每秒閃爍一次，以及相對應的 **LAN** 指示燈是否亮燈。



3. 如果沒有亮燈，意味著路由器的硬體有問題。那麼請回到“1.3 硬體安裝”，再重新執行一次硬體安裝，然後再試試。

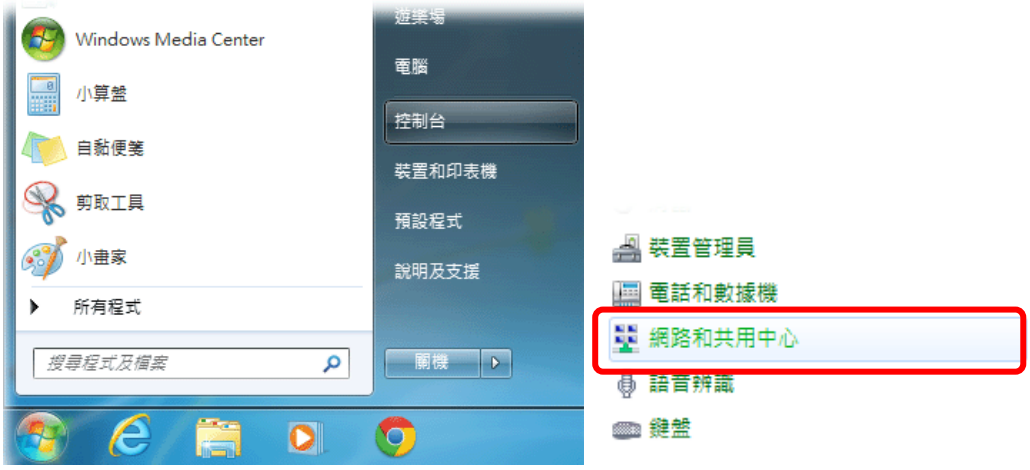
5.2 檢查您電腦的網路連接設置是否正確

有些時候無法上網是因爲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。

對於 Windows 系統

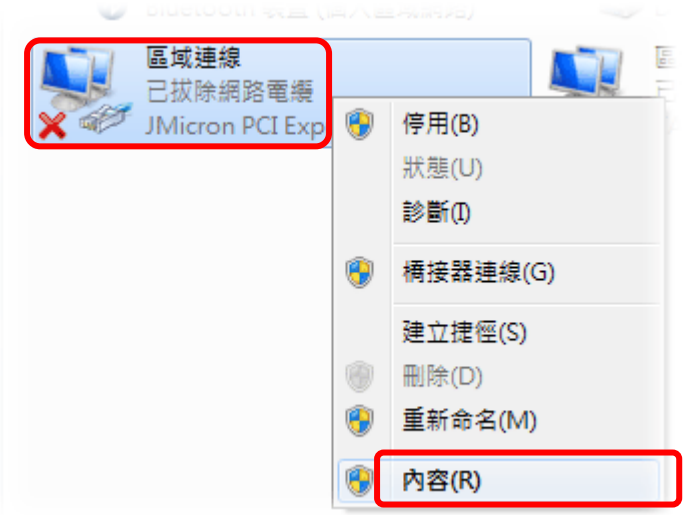
> 下列的範例是以 Windows 7 作業系統爲基礎而提供。若您的電腦採用其他的作業系統，請參照相似的步驟或至 www.draytek.com.tw 查閱相關的技術文件說明。

1. 開啓**所有程式**，選擇**控制台**，選擇**網路和共用中心**。

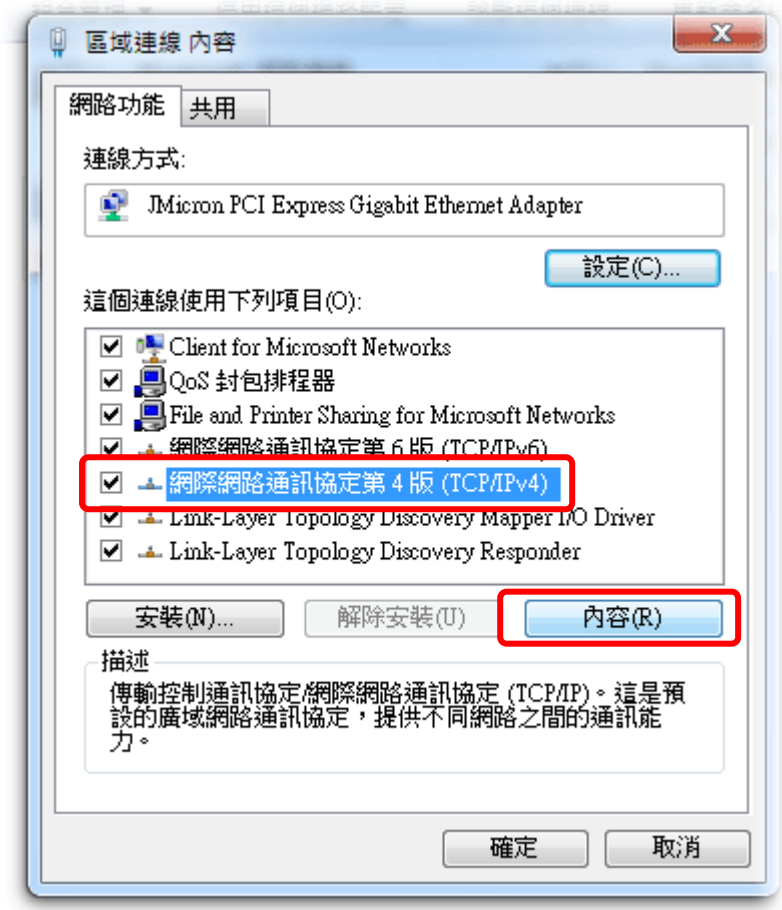


2. 選擇**變更介面卡設定**。

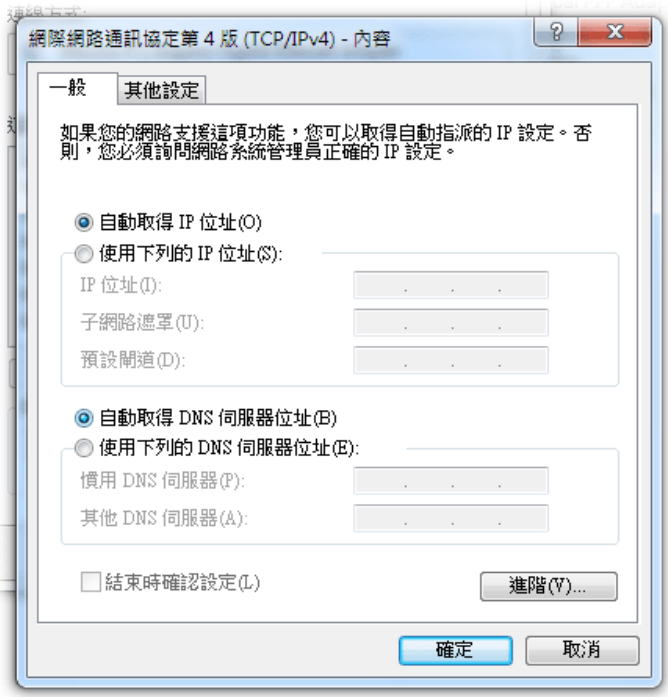
3. 區域連線圖示顯示於視窗上，請在**區域連線**上按滑鼠右鍵並選擇**內容**。



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/IP)**，按下**內容**鍵。



5. 進入**網際網路通訊協定第四版 (TCP/IP)**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。



對於 Mac 系統

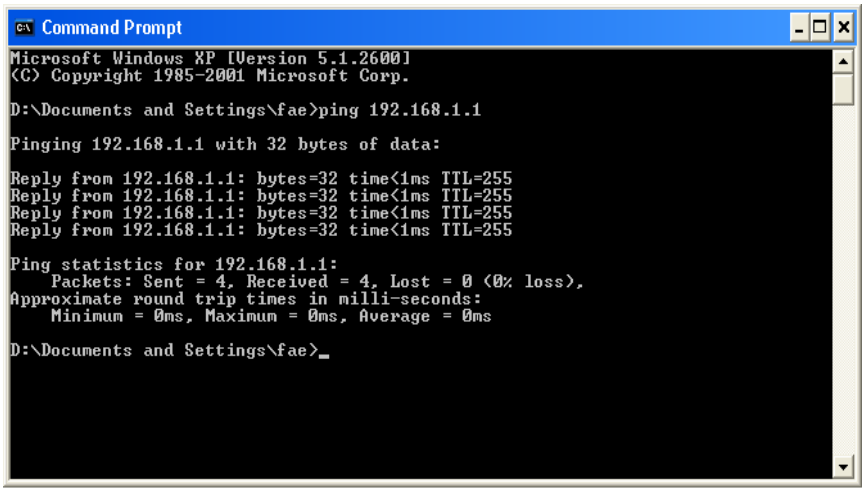
1. 在桌面上選擇目前所使用的 MacOS 磁碟機按滑鼠二下。
2. 選擇**應用**檔案夾中的**網路**檔案夾。
3. 進入**網路**畫面，在**設定**選項中，選擇**使用 DHCP**。

5.3 從電腦上 Ping 路由器

路由器的預設閘道爲 192.168.1.1. 因爲某些理由，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爲自動取得 IP 位址。(請參照 5.2 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。

對於 Windows 系統

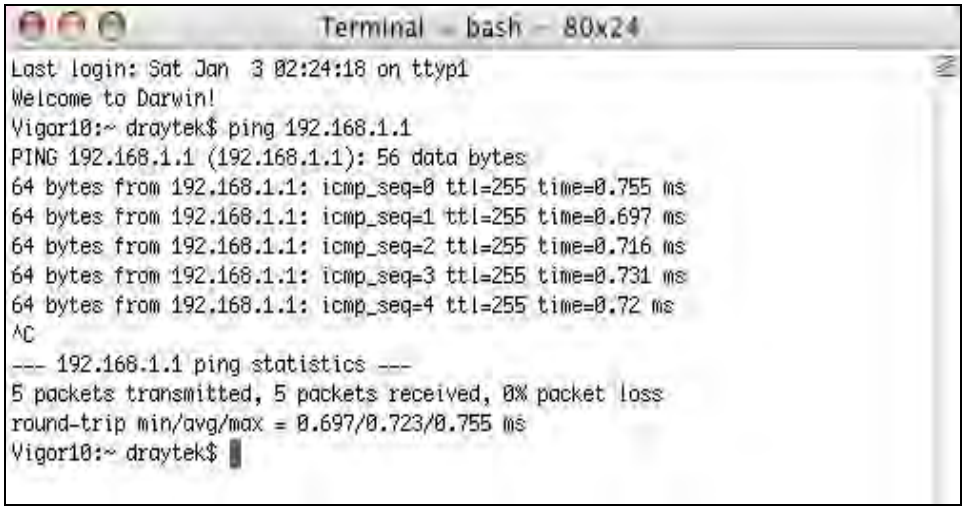
1. 開啓**命令提示字元視窗** (功能表選單**開始**>>**執行**) 。
2. 輸入 **command** (適用於 Windows 95/98/ME)或 **cmd** (適用於 Windows NT/ 2000/XP/Vista/7)。DOS 命令提示字元視窗將會出現。



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。

對於 Mac OS (終端機)系統

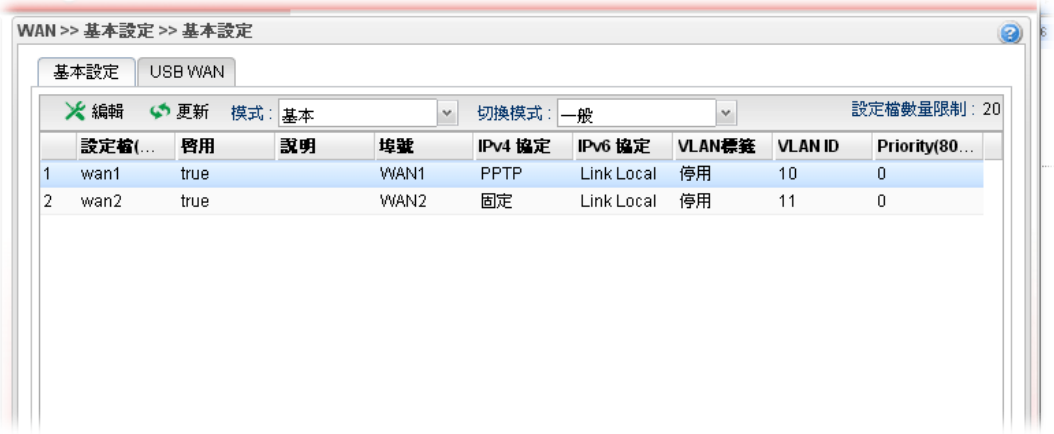
1. 在桌面上選擇目前所使用的 Mac OS 磁碟機，並在上面按滑鼠二下。
2. 選擇 **Applications** 檔案夾中的 **Utilities** 檔案夾。
3. 滑鼠按二下 **Terminal**；終端機的視窗將會跳出並顯現在螢幕上。
4. 輸入 **ping 192.168.1.1** 並且按下 **Enter** 鍵。如果連結正常，終端機視窗會出現**"64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=xxxx ms"** 的訊息。



5.4 檢查 ISP 的設置是否正常

開啓狀態頁面，檢查網路連線設定模式及內容是否正確。

如果設定上發現了任何錯誤，請再次回到**WAN>>基本設定**頁面修改相關的WAN設定。



5.5 還原路由器原廠預設組態

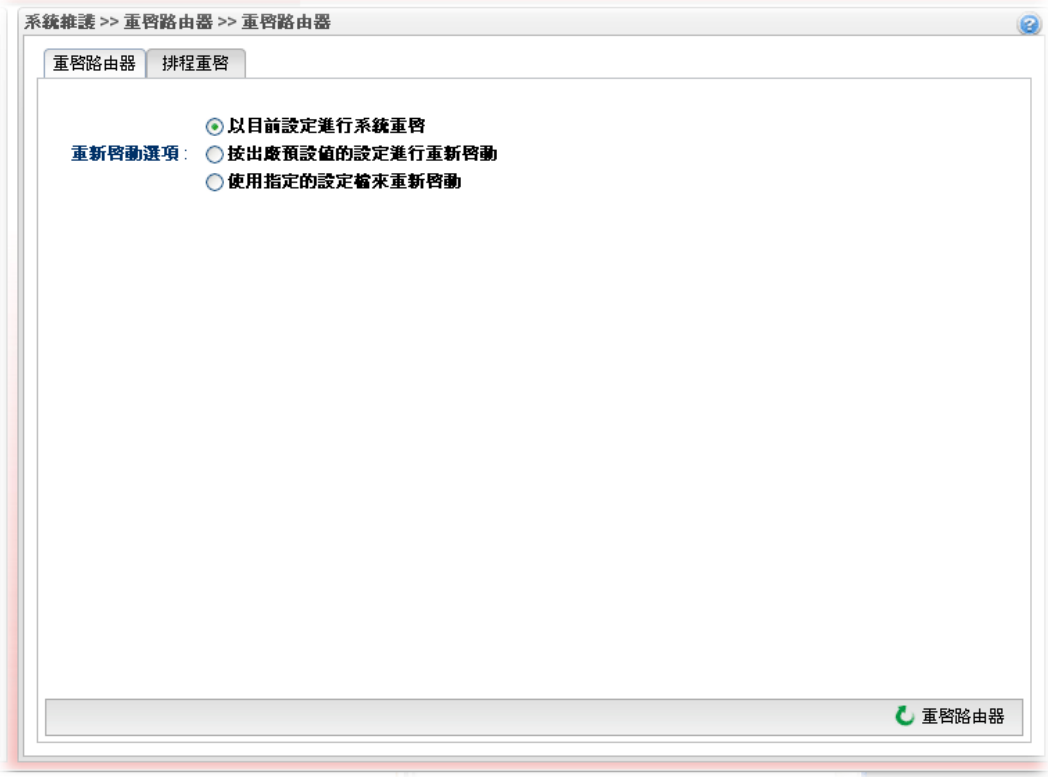
有時，錯誤的連線設定可以藉由還原廠預設組態來重新設定，您可以利用**重啓路由器**或硬體重新設定的方法還原路由器的設定值。

警告： 在使用原廠預設組態後，您之前針對分享器所調整的設定都將恢復成預設值。請確實記錄之前分享器所有的設定。

軟體重新設定

您可以在路由器的網頁介面上，直接將它回復至出廠預設值。

開啓網頁介面上的**系統維護>>重啓路由器**，可見下圖。選擇**按出廠預設值的設定重新啓動**，並按下**重啓路由器**。幾秒鐘後，路由器就會恢復至出廠預設設定。



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。

5.6 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，請立即與居易科技技術服務部聯絡 support@draytek.com.tw。