DrayTek

Vigor2135 系列

寬頻防火牆路由器

使用手冊

V1.1

Vigor2135 系列
雙 WAN 口安全防護路由器

使用手冊

版本**: 1.1**

韌體版本**: V4.4.1**

(請造訪居易網站，隨時獲取更新資訊**)**

日期**: 2022** 年 **3** 月 **31** 日

版權資訊

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

安全說明和保障

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

成為一個註冊用戶

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

韌體及工具的更新

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

目錄

第一篇 安裝 i

I-1 簡介 1

I-1-1 指示燈與介面說明 2

I-1-1-1 Vigor2135 2

I-1-1-2 Vigor2135ac 3

I-2 硬體安裝 5

I-2-1 安裝 Vigor 路由器 5

I-2-2 壁掛安裝 6

I-3 進入設定網頁 7

I-4 變更密碼 9

I-5 儀表板簡介 10

I-5-1 虛擬面板 11

I-5-2 底線連結 11

I-5-3 常用功能的快速存取 12

I-5-4 圖形介面地圖(GUI 地圖) 13

I-5-5 網頁控制台 14

I-5-6 Config 設定備份 14

I-5-7 手冊下載 15

I-5-7 登出 15

I-5-8 連線狀態 16

I-5-8-1 實體連線 16

I-5-8-2 虛擬 WAN 18

I-6 快速設定精靈 19

I-6-1 對於 WAN1 介面(乙太網路) 20

I-6-2 對於 WAN3 (USB) 29

I-7 服務啟動精靈 31

I-8 註冊 Vigor 路由器 33

第二篇 連線設定 37

II-1 WAN 38

網頁使用者介面 40

II-1-1 基本設置 40

II-1-1-1 WAN1(乙太網路) 41

II-1-1-2 WAN3 (USB) 42

II-1-2 網際網路連線設定 43

II-1-2-1 WAN1 中的 PPPoE 模式細節設定(實體模式：乙太網路) 45

II-1-2-2 WAN1 中的靜態或是動態 IP 模式細節設定(實體模式：乙太網路) 48

II-1-2-3 WAN1 中的 PPTP/L2TP 模式細節設定(實體模式：乙太網路) 50

II-1-2-4 WAN3 中的 3G/4G USB 數據機模式細節設定(PPP 模式) 53

II-1-2-5 WAN3 中的 3G/4G USB 數據機模式細節設定(DHCP 模式) *55*
II-1-2-6 WAN1/WAN3 的離線模式細節設定(IPv6) *58*
II-1-2-7 WAN1 的 PPP 模式細節設定(IPv6) *58*
II-1-2-8 WAN1/WAN3 的 TSPC 模式細節設定(IPv6) *59*
II-1-2-9 WAN1/WAN3 的 AICCU 模式細節設定(IPv6) *61*
II-1-2-10 WAN1 的 DHCPv6 用戶端模式細節設定(IPv6) *62*
II-1-2-11 WAN1 的固定 IPv6 模式細節設定(IPv6) *64*
II-1-2-12 WAN1 的 6in4 固定通道模式細節設定(IPv6) *66*
II-1-2-13 WAN1 的 6rd 模式細節設定(IPv6) *67*

II-1-3 多重 VLAN 69

II-1-4 廣域網路連線額度 73

II-1-4-1 基本設定 *73*
II-1-4-2 狀態 *75*

II-2 LAN 77

網頁使用者介面 79

II-2-1 基本設置 79

II-2-1-1 LAN1–乙太網路 TCP/IP 與 DHCP 設定之細節設定 *81*
II-2-1-2 LAN2 ~ LAN4 之細節設定 *83*
II-2-1-3 IP 路由子網之細節設定 *85*
II-2-1-4 LAN IPv6 設定之細節設定 *86*
II-2-1-5 進階 DHCP 選項設定 *90*

II-2-2 VLAN(虛擬區域網路) 91

II-2-3 綁定 IP 與 MAC 位址 95

II-2-4 LAN 埠號監控 97

II-2-5 有線 802.1x 98

II-3 硬體加速 99

II-4 NAT 101

網頁使用者介面 102

II-4-1 通訊埠重導向 102

II-4-2 DMZ 主機 106

II-4-3 開放通訊埠 109

II-4-4 埠號觸發 111

II-4-5 ALG(應用層閘道) 112

II-5 其他應用 114

網頁使用者介面 115

II-5-1 動態 DNS 115

II-5-2 LAN DNS / DNS 轉發 119

II-5-3 DNS 安全性 123

II-5-3-1 基本設置 *123*
II-5-3-2 網域診斷 *124*

II-5-4 排程 125

II-5-5 RADIUS 128

II-5-6 UPnP 130

II-5-7 IGMP 131
II-5-7-1 基本設定 *131*
II-5-7-2 工作狀態 *132*
II-5-8 透過 LAN/WAN 喚醒電腦 133
II-5-9 簡訊/郵件警示服務 135
II-5-9-1 簡訊警示 *135*
II-5-10-2 郵件警示 *136*
II-5-11 Bonjour 137
應用說明 140
A-1 如何使用 DrayDDNS? *140*
II-6 路由 145
網頁使用者介面 146
II-6-1 靜態路由(固定路由) 146
II-6-2 路由策略 152
第三篇 無線區域網路設定 159
III-1 無線區域網路設定(2.4GHz/5GHz)) 160
網頁使用者介面 163
III-1-1 無線網路設定精靈 163
III-1-2 基本設置 166
III-1-3 安全性設定 167
III-1-4 存取控制 170
III-1-5 WPS 171
III-1-6 WDS 174
III-1-7 進階設定 177
III-1-8 無線用戶控制 180
III-1-9 頻寬管理 181
III-1-10 搜尋無線基地台 182
III-1-11 無線頻寬均化 183
III-1-12 頻段引導 185
III-1-13 漫遊 189
III-1-14 無線用戶端列表 190
III-2 無線網狀網路 191
III-2-1 無線網狀網路設定精靈 192
III-2-2 無線網狀網路設定 196
III-2-3 無線網狀網路狀態 198
III-2-4 無線網狀網路搜尋 199
III-2-5 基本 Config 設定同步 200
III-2-6 支援清單 202

第四篇 VPN 連線設定.....203

IV-1 VPN 與遠端存取.....204

網頁使用者介面.....205

IV-1-1 VPN 用戶端設定精靈.....205

IV-1-2 VPN 伺服器端精靈.....211

IV-1-3 遠端存取控制.....219

IV-1-4 PPP 基本設定.....220

IV-1-5 SSL 基本設定.....222

IV-1-6 IPSec IPSec 基本設定.....223

IV-1-7 IPSec 端點辨識.....224

IV-1-8 VPN Matcher 設定.....226

IV-1-9 OpenVPN.....227

IV-1-9-1 OpenVPN 伺服器設定.....227

IV-1-9-2 用戶端Config 設定.....229

IV-1-9-3 輸入憑證.....230

IV-1-10 遠端撥入使用者.....231

IV-1-11 LAN to LAN.....235

IV-1-12 連線管理.....243

IV-2 憑證管理.....244

網頁使用者介面.....245

IV-2-1 本機憑證.....245

IV-2-2 具公信力之 CA 憑證.....249

IV-2-3 憑證備份.....252

IV-2-4 自行簽核憑證.....253

IV-2-5 本機服務清單.....254

第五篇 安全性設定.....255

V-1 防火牆.....256

網頁使用者介面.....258

V-1-1 基本設定.....258

V-1-2 過濾器設定.....263

V-1-3 攻擊防禦功能設定.....273

V-1-3-1 防禦DoS 攻擊.....273

V-1-3-2 Spoofing 攻擊防禦.....275

V-1-4 診斷.....276

V-2 數位內容安全管理(CSM).....278

網頁使用者介面.....279

V-2-1 應用程式管控設定檔.....279

V-2-2 APPE 特徵碼更新.....281

V-2-3 URL 內容過濾器設定檔 283
V-2-4 網頁內容過濾器設定檔 287
V-2-5 DNS 過濾器設定檔 289
應用說明 292
A-1 如何建立一個 MyVigor 帳號 292
A-2 用網頁內容過濾器(WCF) / URL 內容過濾器來阻擋使用者存取 Facebook 服務 297

第六篇 管理設定 303

VI-1 系統維護 304
網頁使用者介面 305
VI-1-1 系統狀態 305
VI-1-2 TR-069 307
VI-1-2-1 ACS 和 CPE 設定 307
VI-1-2-2 報告設定 309
VI-1-2-3 輸出參數 309
VI-1-3 NetFlow 310
VI-1-4 管理員密碼 311
VI-1-5 使用者密碼 314
VI-1-6 登入頁面設定 317
VI-1-7 設定備份 319
VI-1-8 Webhook 322
VI-1-9 Syslog/郵件警示設定 323
VI-1-10 時間和日期 326
VI-1-11 SNMP 327
VI-1-12 管理 329
VI-1-13 面板控制 333
VI-1-14 自行簽核憑證 337
VI-1-15 重啟路由器 339
VI-1-16 韌體升級 340
VI-1-17 韌體備份 341
VI-1-18 儀表板控制 342
VI-2 頻寬管理 343
網頁使用者介面 344
VI-2-1 連線數限制 344
VI-2-2 頻寬限制 346
VI-2-3 服務品質 348
VI-2-4 APP QoS 355
VI-3 使用者管理 357
網頁使用者介面 358
VI-3-1 基本設置 358

VI-3-2 使用者設定檔 360
VI-3-3 使用者群組 364
VI-3-4 使用者線上狀態 365
VI-4 客製化入口網站設定 366
網頁使用者介面 366
VI-4-1 設定檔設定 366
VI-4-1-1 登入模式 367
VI-4-1-2 設定入口網站設定檔步驟 367
VI-4-2 額度管理 382
應用說明 384
A-1 如何建立臉書 APP ID 以利網頁入口驗證？ 384
A-2 如何建立 Google APP ID 以利網頁入口驗證? 390
VI-5 中央管理(無線基地台 AP) 392
網頁使用者介面 393
VI-5-1 狀態 393
VI-5-2 WLAN 設定檔 394
VI-5-3 AP 維護 400
VI-5-4 流量圖表 401
VI-5-5 負載平衡 402
VI-6 中央管理(外接裝置) 404
第七篇 其他設定 405
VII-1 物件設定 406
網頁使用者介面 407
VII-1-1 IP 物件 407
VII-1-2 IP 群組 410
VII-1-3 IPv6 物件 412
VII-1-4 IPv6 群組 414
VII-1-5 服務類型物件 415
VII-1-6 服務類型群組 418
VII-1-7 關鍵字物件 420
VII-1-8 關鍵字群組 422
VII-1-9 副檔名物件 423
VII-1-10 簡訊/郵件服務物件 425
VII-1-11 通知物件 430
VII-1-12 字串物件 432
VII-1-13 國家物件 433
VII-1-14 物件備份/還原 435
應用說明 436

A-1 當 WAN 斷線時如何使用 SMS 簡訊服務寄發通知至指定的電話號碼 *436*
VII-2 USB 應用 440
網頁使用者介面 441
VII-2-1 USB 基本設定 441
VII-2-2 USB 使用者管理 442
VII-2-3 檔案瀏覽器 445
VII-2-4 USB 裝置狀態 445
VII-2-5 溫度感應器 447
VII-2-6 數據機支援清單 449
VII-2-7 SMB 用戶端支援清單 449
應用說明 450
A-1 如何取得連接至 Vigor 路由器的 USB 裝置內的檔案? *450*

第八篇 故障排除 453
VIII-1 自我診斷工具 454
網頁使用者介面 455
VIII-1-1 撥號觸發 455
VIII-1-2 路由表 456
VIII-1-3 ARP 快取表 457
VIII-1-4 IPv6 芳鄰表格 458
VIII-1-5 DHCP 表格 459
VIII-1-6 NAT 連線數表格 460
VIII-1-7 DNS 快取表格 461
VIII-1-8 Ping 自我診斷 462
VIII-1-9 資料流量監控 463
VIII-1-10 流量圖表 465
VIII-1-11 VPN 圖表 466
VIII-1-12 追蹤路由 467
VIII-1-13 Syslog 瀏覽視窗 468
VIII-1-14 IPv6 TSPC 狀態 470
VIII-1-16 DoS Flood 表格 471
VIII-1-18 路由策略診斷 472
VIII-2 檢查路由器硬體狀態是否正常 474
VIII-3 檢查您電腦的網路連接設置是否正確 475
VIII-4 從電腦上 Ping 路由器 479
VIII-5 檢查 ISP 的設置是否正常 481
VIII-6 3G/4G 網路連線相關問題 482
VIII-7 還原路由器原廠預設值 483

VIII-8 聯絡居易 484

第一篇 安裝

本篇將介紹路由器並引導使用者進行硬體安裝及軟體的設定。

I-1 簡介

Vigor2135 系列為寬頻路由器，整合 IP 層級的 QoS、NAT 連線數/頻寬管理等功能，讓使用者能以較大的頻寬進行工作調配的需要。

藉由採用硬體 VPN 平臺及 AES/DES/3DS 硬體加密方式，Vigor2925 系列大大提昇了 VPN 的效用，並在 VPN 通道中提供數種協定(諸如 IPSec/PPTP/L2TP) 應用。

在 SPI (Stateful Packet Inspection)防火牆中提供的物件式設計，讓使用者能輕鬆的設定防火牆策略，數位內容安全管理(CSM, Content Security Management)讓使用者能更有效率的控制即時通訊軟體及點對點軟體，此外，URL/網頁內容過濾器及 DoS/DDoS 防止功能強化了路由器的外部安全性管理及內部的控制。

使用者管理功能可防止任一電腦，在沒有使用者名稱或是密碼的驗證下進行網際網路存取連線，這個功能還可讓雇主給辦公室的員工分別給予不同的時間額度。

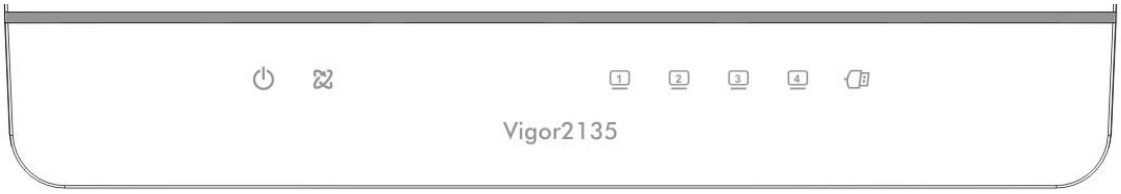
在具備無線功能的機種上(Vigor2135ac/Vac)，每個無線 SSID 皆可群組在 VLAN 上。

此外，Vigor2135 系列支援 USB 介面，可供連接 USB 印表機分享列印或是 USB 儲存裝置分享檔案。

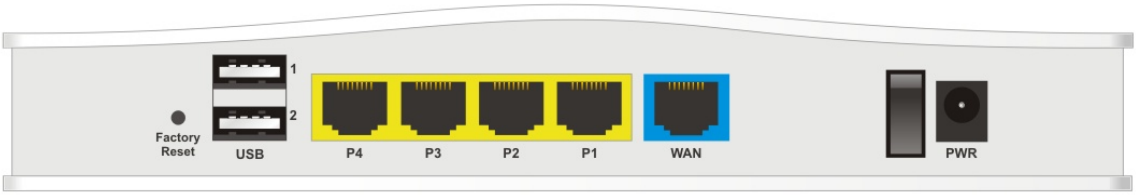
I-1-1 指示燈與介面說明

不同機種路由器之 LED 顯示面板以及背板連接介面有些許的差異，詳列如下：

I-1-1-1 Vigor2135

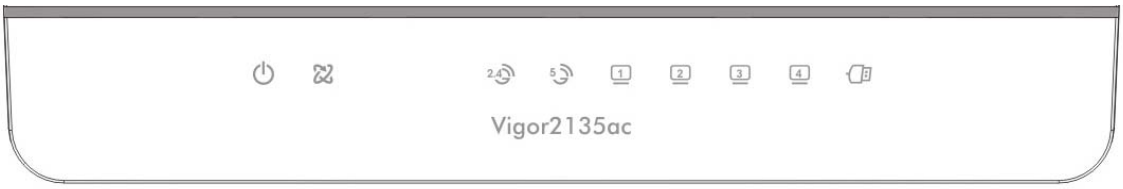


LED	狀態	說明
(Activity)	閃爍	路由器已開機並可正常運作。
	熄燈	路由器已關機。
WAN	亮燈	網際網路連線預備妥當可以使用。
	閃爍	正在傳輸資料中。
	熄燈	網際網路尚未預備妥當。
1 ~ 4 LAN1/2/3/4	亮燈	介面網路已連接。
	閃爍	正在傳輸資料中。
	熄燈	介面網路未連接。
USB	亮燈	USB 裝置已連接，等待使用中。
	閃爍	正在傳輸資料中。

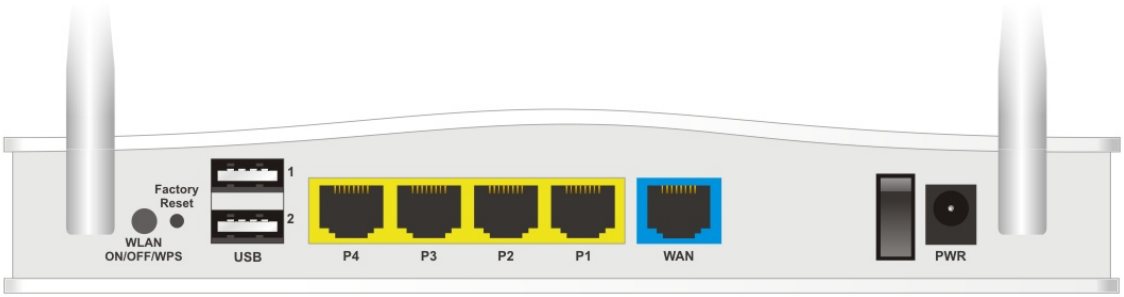


介面	說明
Factory Reset	還原成出廠預設值。 使用方法：開啟路由器（ACT LED 閃動）。用圓珠筆按下小孔內的按鈕，然後維持 5 秒左右。當您發現 ACT LED 快速閃動時，請鬆開按鈕。路由器隨後將重新啟動，並回復出廠預設值。
USB1~USB2	連接到 USB 3G/4G 數據機、印表機。
P4~P1	連接到電腦或網路設備。
WAN	連接到遠端網路裝置(透過乙太網路)。
ON/OFF	電源開關。
PWR	連接電源變壓器。

I-1-1-2 Vigor2135ac



LED	狀態	說明
(Activity)	閃爍	路由器已開機並可正常運作。
	熄燈	路由器已關機。
WAN	亮燈	網際網路連線預備妥當可以使用。
	閃爍	正在傳輸資料中。
	熄燈	網際網路尚未預備妥當。
2.4 ~ 5 WLAN	閃爍	系統收到來電。
	亮燈	無線基地台準備妥當。
	閃爍	透過無線區域網路傳送乙太網路封包。
	閃爍 (快速)	當 ACT 跟 WLAN 二個燈號快速閃爍時，表示 WPS 功能已經啟用且預備妥當，系統正等待無線用戶連線中。
	熄燈	無線區域網路未啟用。
1 ~ 4 LAN1/2/3/4	亮燈	介面網路已連接。
	閃爍	正在傳輸資料中。
	熄燈	介面網路未連接。
USB	亮燈	USB 裝置已連接，等待使用中。
	閃爍	正在傳輸資料中。



介面	說明
Wireless LAN ON/OFF/WPS	WLAN On - 按住此鈕並在 2 秒內放開，當無線功能預備妥當時，LED 將顯示綠燈。 WLAN Off - 按住此鈕並在 2 秒內放開，可關閉無線功能。 WPS - 若使用者介面已經啟用 WPS 功能，則按住 WPS 按鈕 2 秒鐘以上等待用戶裝置透過 WPS 執行網路連線。
Factory Reset	還原成出廠預設值。 使用方法：開啟路由器（ACT LED 閃動）。用圓珠筆按下小孔內的按鈕，然後維持 5 秒左右。當您發現 ACT LED 快速閃動時，請鬆開按鈕。路由器隨後將重新啟動，並回復出廠預設值。

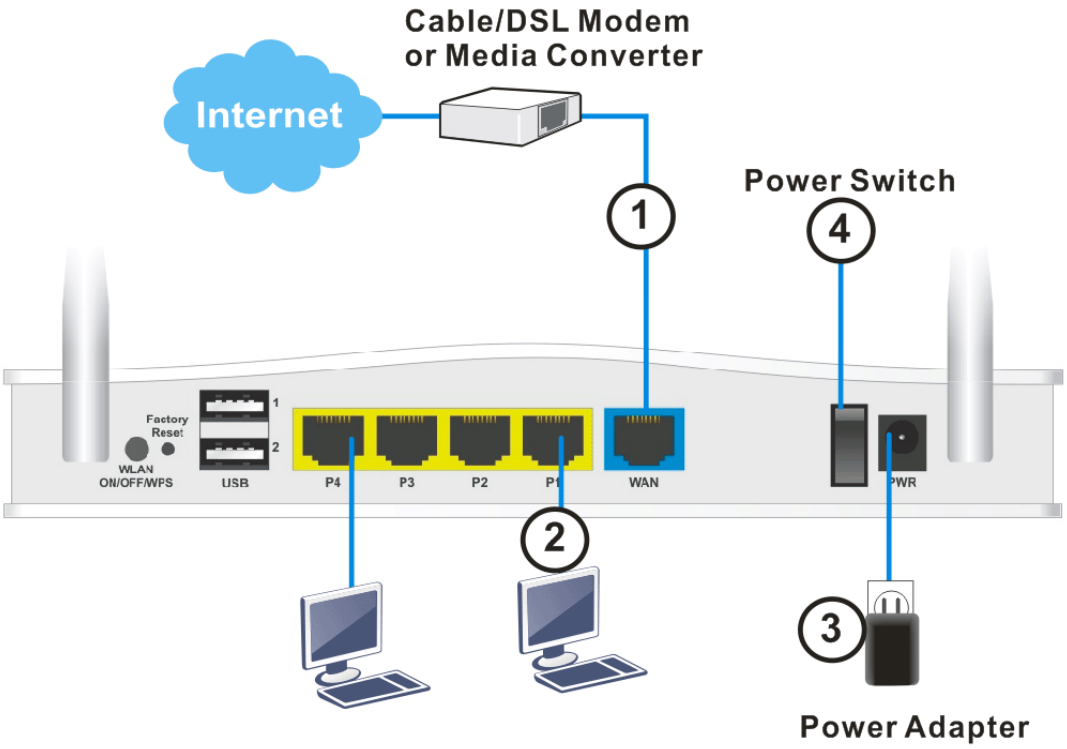
USB1~USB2	連接到 USB 3G/4G 數據機、印表機。
P4~P1	連接到電腦或網路設備。
WAN	連接到遠端網路裝置(透過乙太網路)
ON/OFF	電源開關。
PWR	連接電源變壓器。

I-2 硬體安裝

I-2-1 安裝 Vigor 路由器

本節引導您透過硬體連線安裝路由器。舉 Vigor2135ac 為例。

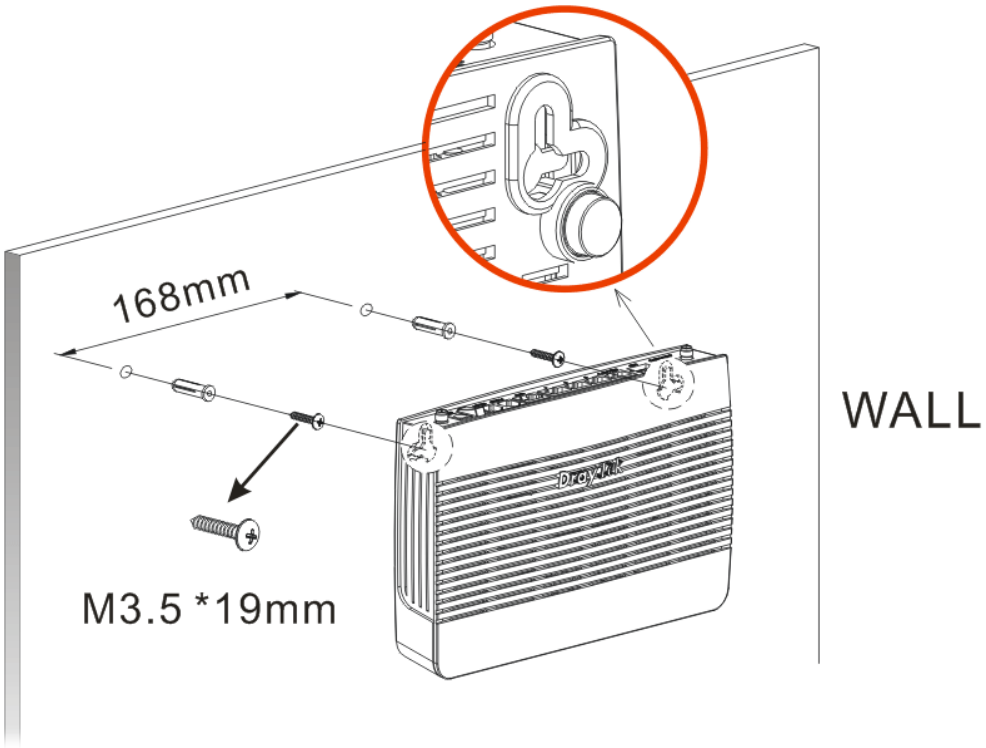
1. 利用乙太網路纜線(RJ-45)連接纜線數據機/DSL 數據機/媒體轉換器至路由器的 WAN 埠口。
2. 利用 RJ-45 纜線連接路由器(LAN 連接埠中選定其中一個)與您的電腦。
3. 將電源轉換器一端連接至路由器，另一端則連至牆上電源輸出孔。
4. 開啟路由器電源。
5. 系統開始初始化，完成測試後，檢查 **ACT** 與 **LAN** 燈號是否亮燈以確保連線無誤。



I-2-2 壁掛安裝

Vigor 路由器的背面有鎖孔式的安裝插槽，方便壁掛安裝使用。

1. 請在牆面上鑽鑿二個孔洞。距離間隔 168mm。
2. 用適當類型的螺絲套管將螺絲鎖進牆壁。



附註 建議的孔洞尺寸為 6.5釐米(1/4吋)。

3. 完成上述步驟後，路由器及可穩妥安置在牆壁上。

I-3 進入設定網頁

1. 確保您的電腦已經和路由器正確的連接。

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

2. 開啟網頁瀏覽器並輸入位址 http://192.168.1.1，登入視窗將會出現。

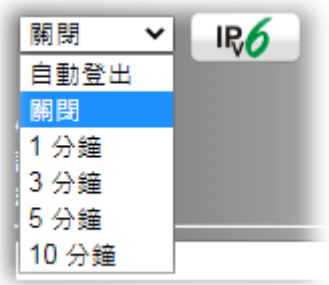
3. 請輸入“admin/admin”，再按下**登入**進入路由器網頁設定畫面。

注意	如果您無法進入網頁設定畫面，請參考“疑難排解”以解決您所面臨的問題。

4. 現在，設定介面的主選單會出現。舉 Vigor2135ac 為例：

注意 因為首頁會依照您的路由器的功能做些微改變，所以設定介面不一定都會如上圖所示。

5. 網頁將會依照您所選擇的條件開啟不同的頁面，預設值通常為自動登出，若操作者沒有進行任何動作時，網頁會在 5 分鐘後自動離開，您可以視需要改變登出的時間設定。



I-4 變更密碼

為了路由器的安全起見，建議您將先行變更密碼。

1. 開啟網頁瀏覽器並輸入位址 http://192.168.1.1。登入視窗將會出現並要求您輸入使用者名稱與密碼。
2. 請輸入 “admin/admin”進入管理者模式。
3. 進入**系統維護**頁面並選擇**管理員密碼**。

4. 輸入舊密碼 (預設值為空白)。 在**新密碼**及**確認密碼**輸入您想要設定的密碼，然後按**確定**儲存設定。
5. 現在密碼已經變更，下次登入時請使用新設定的密碼。

注意 即使密碼已經變更，登入使用者介面的使用者名稱仍然為“admin。

I-5 儀表板簡介

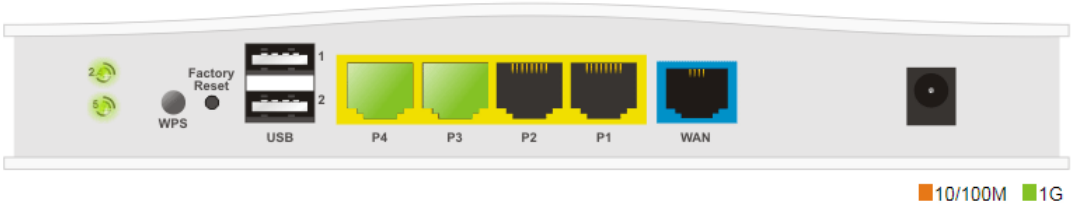
儀表板(Dashboard)顯示各種連線狀態，諸如系統資訊、IPv4 網際網路連線、IPv6 網際網路連線、介面(實體連線)、安全性設定與快速存取等等。

自左手邊的主選單上按下**儀表板**功能。

預設值網頁將會顯示在螢幕上，請參考下圖：

I-5-1 虛擬面板

在儀表板的正上方，您可以看到路由器的虛擬面板，顯示實體連線的狀態，每隔數秒，畫面會重新顯示一次。



項目	顏色顯示	說明
LED 燈號 (左邊)	黑色	表示該功能尚未運作。
	綠色	表示該功能正在運作當中。
USB	黑色	表示目前沒有連接 USB 裝置。
	綠色	表示已經連接上 USB 裝置。
乙太網路埠 (WAN/LAN)	黑色	表示該埠目前並未連接。
	綠色	表示該埠目前已經連接上路由器(傳輸速度達 Giga)。
	橘色	表示該埠目前已經連接上路由器。

有關燈號的詳細說明，請參考 **I-1-1 LED 指示燈與介面說明**一節。

I-5-2 底線連結

任何一個名稱下方含有底線者(如路由器名稱、目前時間、WAN1# 等等.)表示您可以按下該連結開啟設定頁面。

系統資訊

型號名稱	Vigor2135ac	系統上線時間	21:32:39
路由器名稱	DrayTek	目前時間	Sat Jan 01 2000 21:29:14
韌體版本	4.4.1_STD	建立日期/時間	Feb 14 2022 10:55:27
LAN MAC位址	14-49-BC-0A-8A-B8		

IPv4 LAN資訊

	IP 位址	DHCP		IP 位址	DHCP
區域網路(LAN)1	192.168.1.1/24	v	區域網路(LAN)2	192.168.2.1/24	v
區域網路(LAN)3	192.168.3.1/24	v	區域網路(LAN)4	192.168.4.1/24	v
IP路由子網	192.168.0.1/24	v			

IPv4 網際網路連線設定

	線路/模式	IP 位址	MAC位址	上線時間
廣域網路(WAN)1	乙太網路 / DHCP 用戶端	斷線	14-49-BC-0A-8A-B9	00:00:00
廣域網路(WAN)3	USB / ---	斷線	14-49-BC-0A-8A-BB	00:00:00

I-5-3 常用功能的快速存取

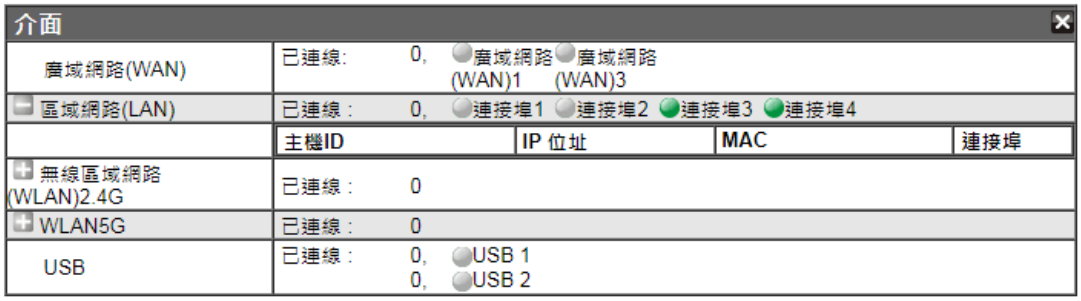
所有的項目都可以依照您的需要從左邊的主要功能區存取，不過針對一些較重要或是常用的項目，系統提供一個更為方便快速快速的方式來開啟。

請移動前往儀表板的右邊，您可以**在快速存取**一區中看到常用功能群。

本區將系統狀態、動態 DNS、TR-069、使用者管理、IM/P2P 阻擋、排程、Syslog/郵件警示、RADIUS、防火牆物件設定以及資料流量監控等常用連結歸納於此，移動您的滑鼠至任何一個連結再輕輕按下，相應頁面即可立刻開啟。

此外，VPN 安全設定的快速存取連結像是**遠端撥入使用者**以及 **LAN to LAN** 位於本頁的底端，請利用滑鼠在此頁面向下捲動即可見到相關內容。

請注意在 LAN/WLAN/VPN/MyVigor 的左邊有加號( ) 圖示，請按下該圖示檢視目前 LAN/WLAN/VPN/MyVigor 狀態。



介面				
廣域網路(WAN)	已連線: 0, 廣域網路(WAN)1 廣域網路(WAN)3			
區域網路(LAN)	已連線 : 0, 連接埠1 連接埠2 連接埠3 連接埠4			
	主機ID	IP 位址	MAC	連接埠
無線區域網路(WLAN)2.4G	已連線 : 0			
WLAN5G	已連線 : 0			
USB	已連線 : 0, USB 1 0, USB 2			

透過 LAN 埠口實體連接至路由器的主機會以綠色圓燈來呈現，表示目前該埠口是連接的。

所有列出主機 ID、IP 位址以及 MAC 位址的主機(包含無線用戶端)表示資料傳輸乃透過該 LAN 端及 WAN 端進出。這些清楚的標示目的在進行主機的流量監控作業。

I-5-4 圖形介面地圖(GUI 地圖)

路由器支援的全部功能可在此頁面下全部呈現出來，使用者可以按此功能連結進入相關頁面進行細部設定。機種不同，呈現的圖形介面地圖也會有所差異。

GUI 地圖

儀表板
設定精靈
- 快速設定精靈
- 服務啟動精靈
- VPN 用戶端設定精靈
- VPN 伺服器設定精靈
- 無線設定精靈
- 無線網狀網路設定精靈

線上狀態
- 實體連線
- 虛擬WAN介面

廣域網路(WAN)
- 基本設置
- 網際網路連線設定
- 多重VLAN
- 廣域網路連線額度

區域網路(LAN)
- 基本設置
- VLAN
- 綁定 IP 與 MAC 位址
- LAN 埠號監控
- 有線802.1X

客製化入口網站設定
- 設定檔設定
- 額度管理

憑證管理
- 本機憑證
- 具公信力之 CA 憑證
- 憑證備份
- 自行簽核憑證
- 本機服務清單

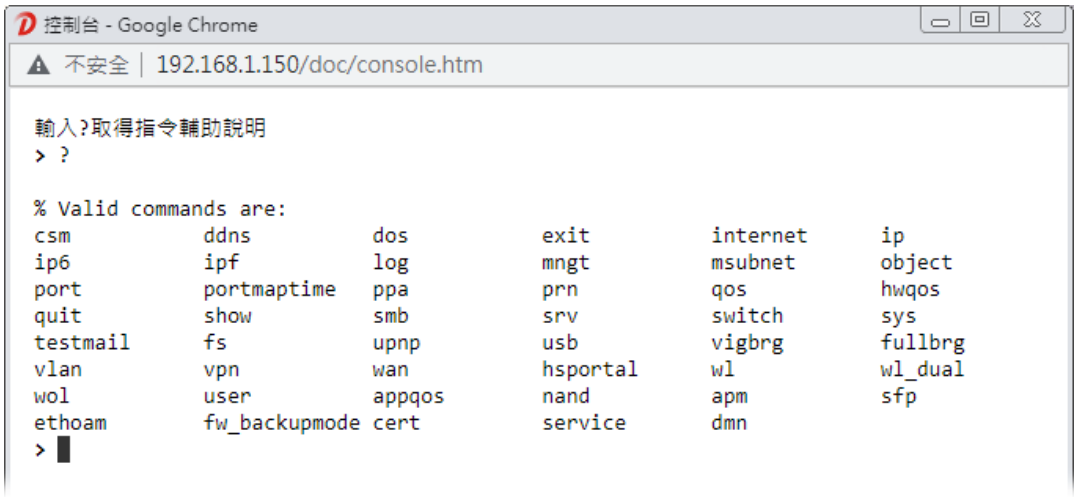
無線網狀網路
- 無線網狀網路設定
- 無線網狀網路狀態
- 無線網狀網路搜尋
- 基本Config設定同步
- 支援清單

無線區域網路 (2.4 GHz)
- 基本設置
- 安全性
- 存取控制
- WPS
- 進階設定
- 無線用戶控制
- 頻寬管理
- 搜尋無線基地台
- 無線頻寬均化
- 頻段引導
- 漫遊
- 無線用戶端列表

I-5-5 網頁控制台

透過這個功能可不必透過 DOS 提示頁面使用 Telnet 指令。使用網頁操作台所做的任何變更與透過網頁使用者介面所進行的改變是相同的。在此操作台下所玩的功能/設定修正可以同時在網頁使用者介面中呈現。

請按主頁面上方的網頁控制台圖示即可開啟如下視窗。

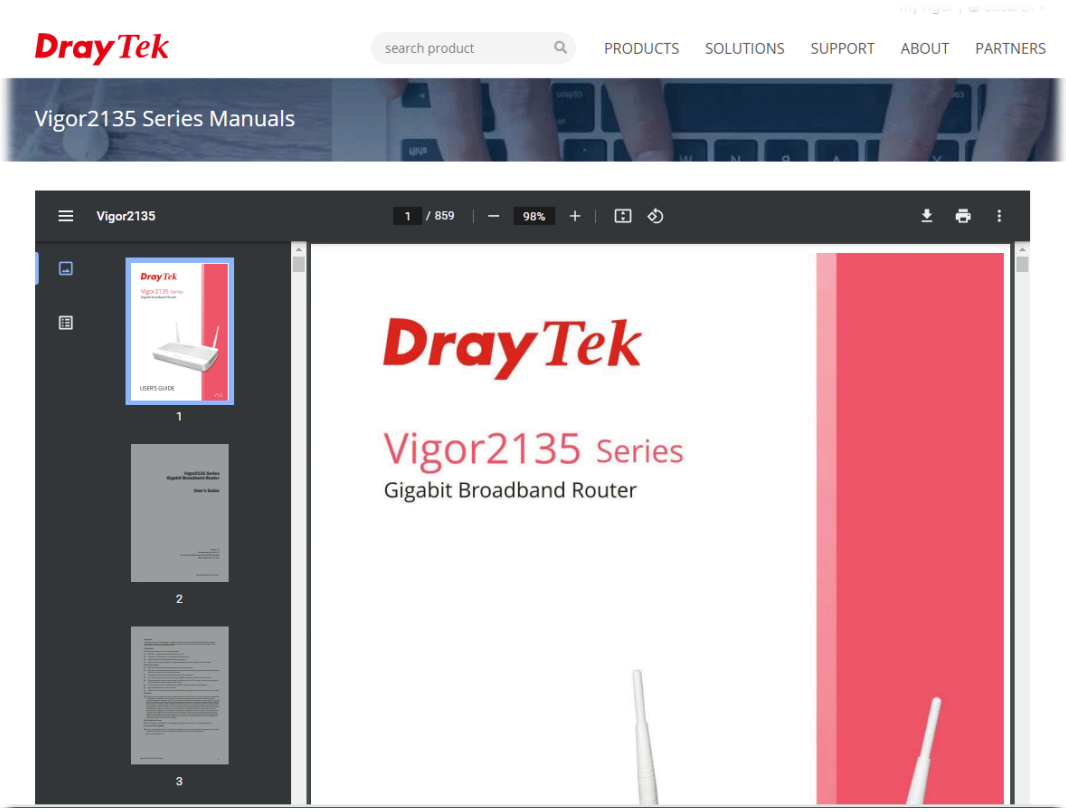


I-5-6 Config 設定備份

快速儲存目前使用中的設定可以透過 **Config 設定備份**圖示來完成，將目前的設定儲存為檔案，這個檔案後續還能利用**系統維護>>韌體備份**來還原。

I-5-7 手冊下載

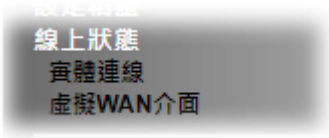
按此鈕可以開啟路由器手冊的線上閱讀器。



I-5-7 登出

按下登出按鈕即可離開此使用者設定介面。

I-5-8 連線狀態



I-5-8-1 實體連線

本頁顯示實體連線狀態，諸如 LAN 連線狀態、WAN 連線狀態、ADSL 連線狀態等等。

IPv4 協定的實體連線

線上狀態

實體連線　　系統上線時間: 7日 1:1:38

IPv4　IPv6

LAN 狀態

IP 位址	傳送封包	接收封包	路由器主要DNS:	路由器次要DNS:
192.168.1.150	449,142	699,876	8.8.8.8	8.8.4.4

廣域網路(WAN) 1 狀態　　>> 更新

啟用	線路	名稱	模式	上線時間	
是	乙太網路		DHCP 用戶端	00:00:00	
IP 位址	閘道器IP	傳送位元	傳送速率(bps)	接收位元	接收速率(bps)
---	---	0 (B)	0	0 (B)	0

廣域網路(WAN) 3 狀態

啟用	線路	名稱	模式	上線時間	訊號
是	USB		---	00:00:00	
IP 位址	閘道器IP	傳送位元	傳送速率(bps)	接收位元	接收速率(bps)
---	---	0 (B)	0	0 (B)	0

IPv6 協定的實體連線

詳細說明於後(IPv4):

項目	說明
LAN 狀態	**主要 DNS** - DNS.顯示主要 DNS 的 IP 位址。 **次要 DNS** - 顯示次要 DNS 的 IP 位址。 **IP 位址**- 顯示 LAN 介面的 IP 位址。 **傳送封包** - 顯示在區域網路全部的傳送封包量。。 **接收封包**- 顯示區域路網路中全部的接收封包量。
WAN #狀態	**啟用** – **是**(紅色字體) 表示此介面可以運用但尚未連接，**是**(藍色字體) 表示此介面已連接。 **線路** - 顯示此介面的實體連線類型。 **名稱** - 顯示 WAN1~WAN3 網頁上所顯示的名稱。 **模式** - 顯示 WAN 連線的模式類型(例如 PPPoE)。 **上線時間** - 顯示介面上全部的上傳時間。 **IP** - 顯示 WAN 介面的 IP 位址。 **閘道 IP** - 顯示預設閘道的 IP 位址。 **傳送位元** - 顯示 WAN 介面上全部傳送的封包數。 **傳送速率** - 顯示 WAN 介面上全部傳送速率位元數。 **接收位元** - 顯示 WAN 介面上全部接收的封包數。 **接收速率** - 顯示 WAN 介面上全部接收速率位元數。

詳細說明於後(IPv6):

項目	說明
LAN 狀態	**IP 位址** - 顯示 WAN 介面上的 IPv6 位址。 **傳送封包** - 顯示在區域網路中全部的傳送封包量。

項目	說明
	接收封包 - 顯示區域路網路中全部的接收封包量 **傳送位元** - 顯示區域網路上全部傳送的位元數。 **接收位元** - 顯示區域網路上全部接收的位元數。
WAN# IPv6 狀態	**啟用** – **是**(紅色字體) 表示此介面可以運用但尚未連接，**是**(藍色字體) 表示此介面已連接。 **模式** - 顯示 WAN 連線的模式類型(例如 TSPC)。 **上線時間** - 顯示介面上全部的上傳時間。 **IP** - 顯示 WAN 介面的 IP 位址。 **閘道 IP** - 顯示預設閘道的 IP 位址。

注意

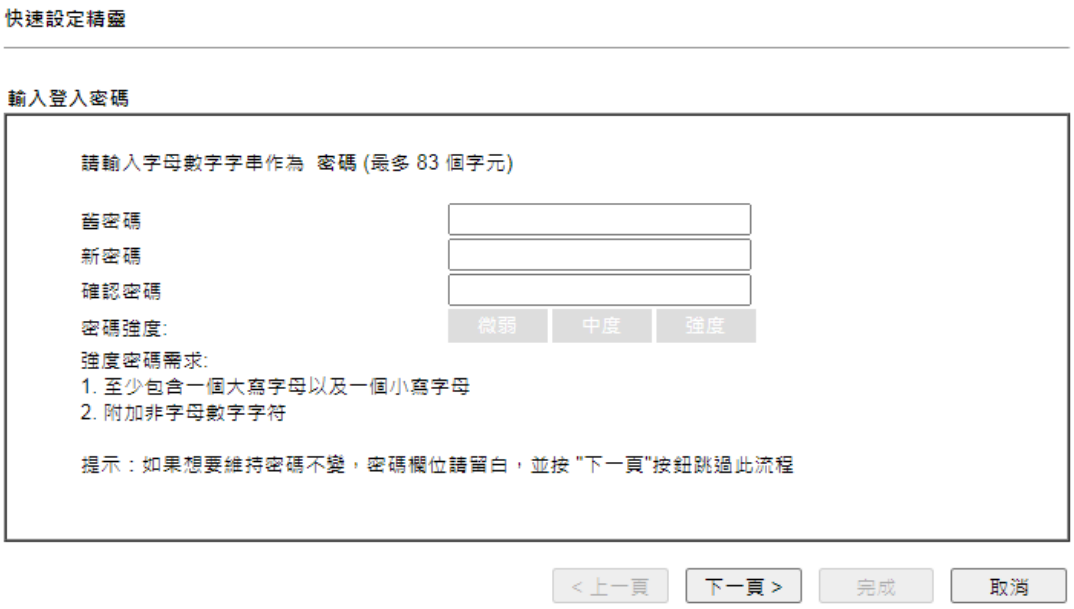
綠色字樣表示該WAN連接已預備妥當，隨時可以存取網際網路資料，紅色字樣則表示該WAN連接尚未預備妥當，也還無法透過路由器存取網際網路資料。

I-5-8-2 虛擬 WAN

本頁顯示虛擬 WAN 介面的資訊，虛擬 WAN 用於 TR-069 管理、VoIP 服務等方面，應用一欄可顯示此 WAN 連線的目地。

I-6 快速設定精靈

您可以依照下列的步驟**使用快速設定精靈**設定您的路由器。快速設定精靈的第一個畫面會要求您輸入密碼，輸入密碼之後，請按**下一頁**。



在下述頁面，請選擇使用的 WAN 介面，如果使用的是乙太網路介面，請選擇 WAN1，若使用的是 3G/4G USB 數據機，請選擇 WAN3。並選擇**自動協商**作為路由器的傳送資料模式，然後按**下一頁**。

WAN1 與 WAN3 帶來的設定頁面所不同，請參考下述細部說明。

I-6-1 對於 WAN1 介面(乙太網路)

WAN1 專用於乙太網路的實體連線模式。

可用設定說明如下：

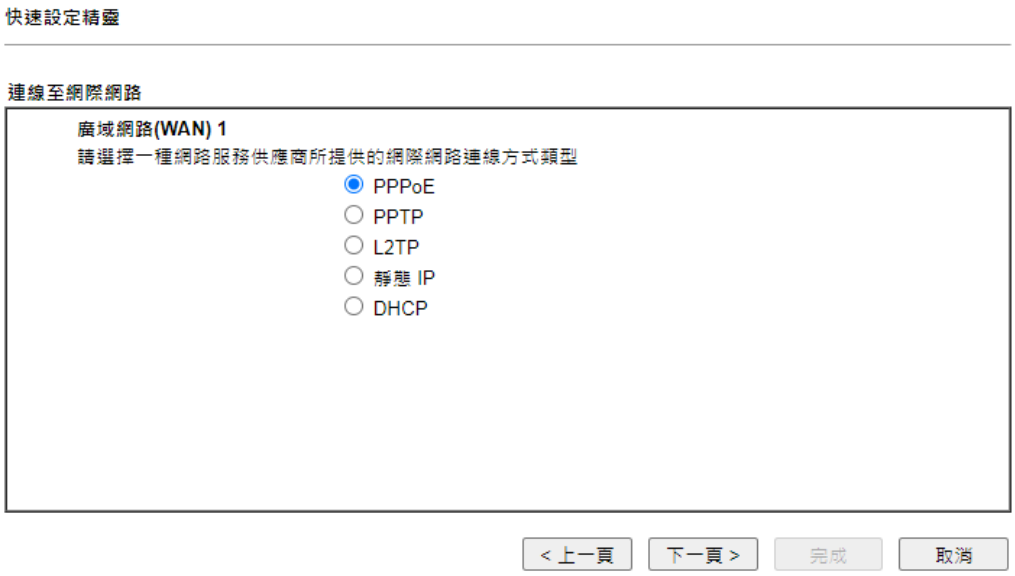
項目	說明
顯示名稱	請輸入路由器的名稱。
傳送資料模式	乙太網路鏈結參數。 **自動協商** – 自動設定速度與雙工模式。 **10M 半雙工** – 10 Mbit/s 乙太網路半雙工。 **10M 全雙工** – 10 Mbit/s 乙太網路全雙工。 **100M 半雙工**– 100 Mbit/s 快速乙太網路半雙工。 **100M 全雙工**– 100 Mbit/s 快速乙太網路全雙工。 **1000M 全雙工**– 1 Gbit/s Gigabit 乙太網路全雙工。

請依照 ISP 業者提供給您的資訊選擇適當的網際網路連線類型，舉例來說，如果 ISP 提供給您的是 PPPoE 介面，您應該選擇 PPPoE 模式，然後按**下一頁**繼續進行。

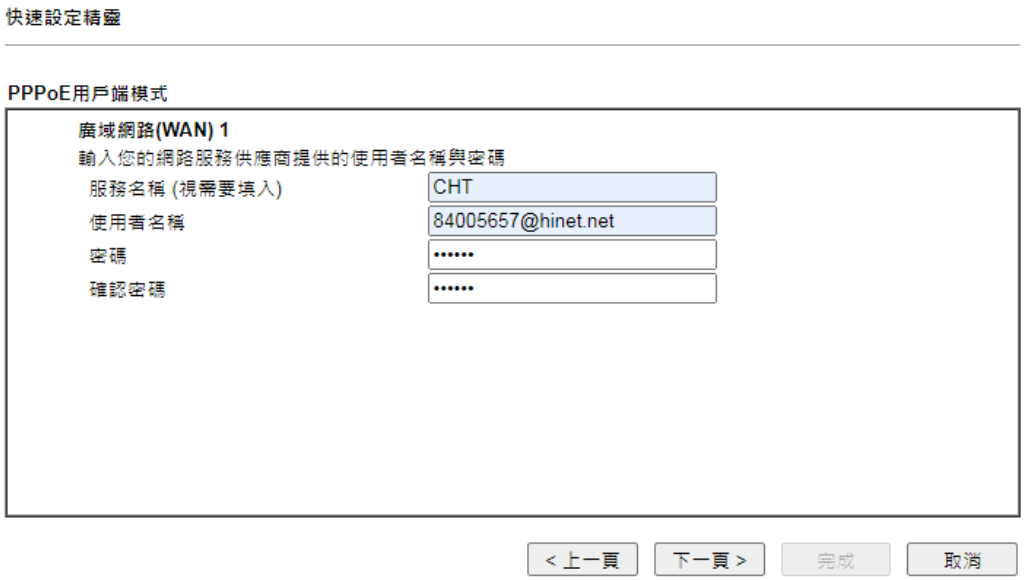
PPPoE

PPPoE 為 Point-to-Point Protocol over Ethernet 的縮寫，是一種利用個人電腦透過寬頻連接設備(如 xDSL、Cable、Wireless)連接至高速寬頻網路的技術，用戶僅需在個人的電腦上加裝乙太網路卡，然後向電信線路提供者(如：中華電信)與網際網路服務提供者(ISP，如：亞太線上)申請 ADSL 服務，就可以以類似傳統撥接的方式，透過一般的電話線連上網際網路。另外，PPPoE 也同時被用來在 ADSL 網路架構上進行用戶認證、紀錄用戶連線時間，以及取得動態 IP。

1. 選擇 **WAN1** 作為 WAN 介面，按**下一頁**按鈕後，下圖將會出現讓您指定網際網路連線類型。



2. 選擇 **PPPoE** 然後按**下一頁**開啟如下頁面。

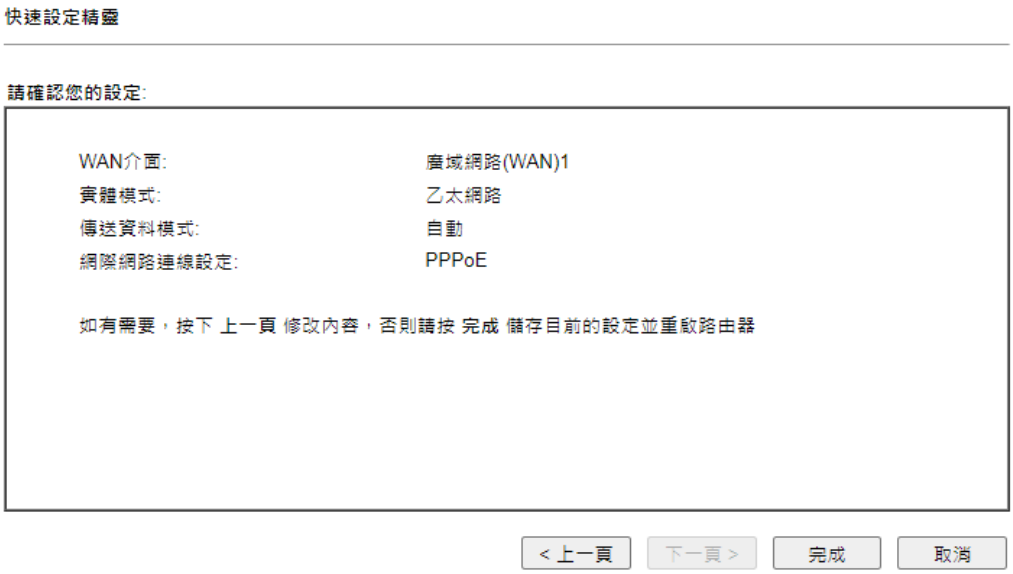


可用設定說明如下：

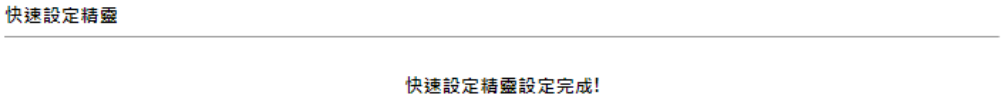
項目	說明
服務名稱(視需要填入)	輸入特定網路服務的說明。
使用者名稱	指定 ISP 提供之有效使用者名稱。
密碼	指定 ISP 提供之有效密碼。
確認密碼	重新輸入密碼以確認。

項目	說明
上一頁	按此鈕回到上一頁面。
下一頁	按此鈕進入下一頁面。
取消	按此鈕放棄快速設定精靈。

3. 請依照您的 ISP 業者提供的資料輸入使用者名稱與密碼。按**下一步**檢視連線的設定狀態。



4. 按完成，快速設定精靈設定完成頁面將會出現。

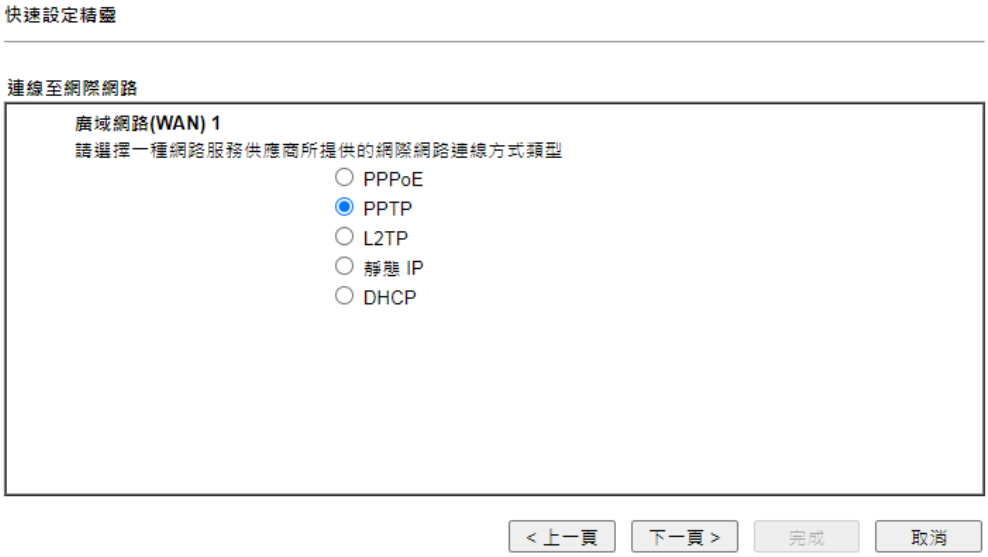


5. 現在您可以遨遊網際網路了。

PPTP/L2TP

PPTP 則是 Point-to-Point Tunneling Protocol 的簡稱。有些 DSL 服務提供者採用一種特別的 DSL 數據機(例如：阿爾卡特的 DSL 數據機)。這種數據機只支援 PPTP Tunnel 方法存取 Internet。在這種情形下，您建立一個到 DSL 數據機並且帶有 PPP Session 的 PPTP Tunnel。一但 Tunnel 建立後，這種 DSL 數據機會將 PPP Session 送往 ISP。當 PPP Session 建立後，當地的使用者共用這個 PPP Session 存取 Internet。如果您需要使用 PPPTP 連線，請先在視窗中選擇適當的模式，然後輸入相關資訊。

1. 選擇 **WAN1** 作為 WAN 介面，按**下一頁**按鈕後，下圖將會出現讓您指定網際網路連線類型。



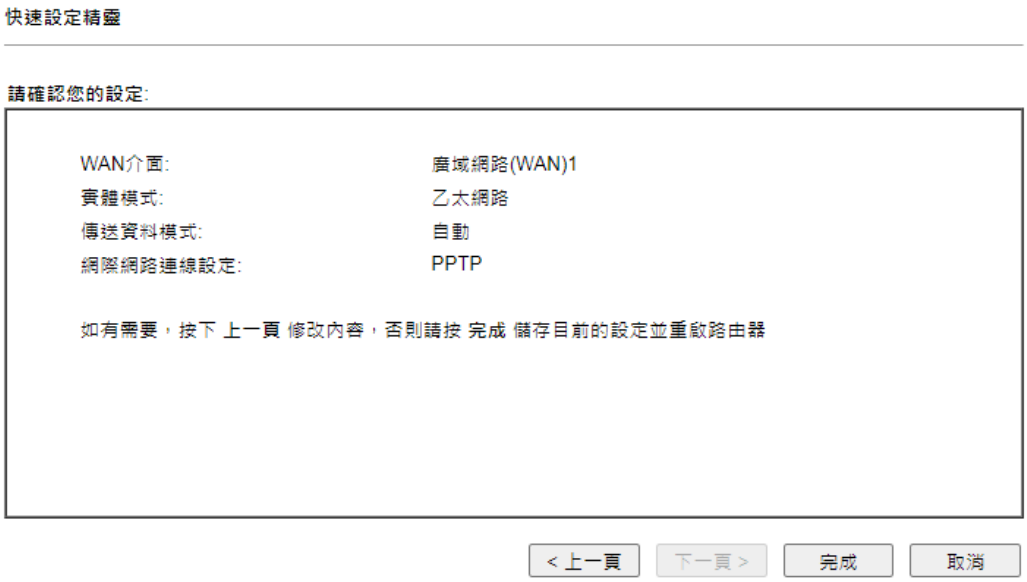
2. 選擇 **PPTP/L2TP** 然後按**下一頁**開啟如下頁面。

可用設定說明如下：

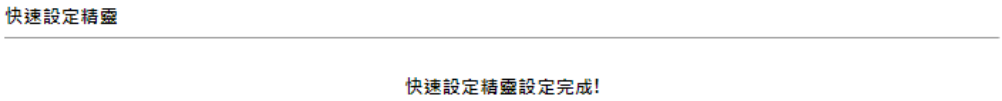
項目	說明
使用者名稱	指定 ISP 提供之有效使用者名稱。
密碼	指定 ISP 提供之有效密碼。

確認密碼	重新輸入密碼以確認。
WAN IP 設定	**自動取得 IP 位址** – 路由器可自 DHCP 伺服器自動取得 IP 位址。 **指定 IP 位址** – 使用者須手動輸入相關設定。 **IP 位址** – 輸入 IP 位址。 **子網遮罩**- 輸入子網路遮罩。 **閘道器** – 輸入閘道 IP 位址。 **主要 DNS** – 輸入路由器主要的 DNS IP 位址。 **次要 DNS** – 必要時輸入路由器次要的 DNS IP 位址。
PPTP 伺服器 / L2TP 伺服器	輸入伺服器的 IP 位址。
上一頁	按此鈕回到上一頁面。
下一頁	按此鈕進入下一頁面。
取消	按此鈕放棄快速設定精靈。

3. 請依照您的 ISP 業者提供的資料輸入相關資訊。按**下一頁**檢視連線的設定狀態。



4. 按完成，快速設定精靈設定完成頁面將會出現。

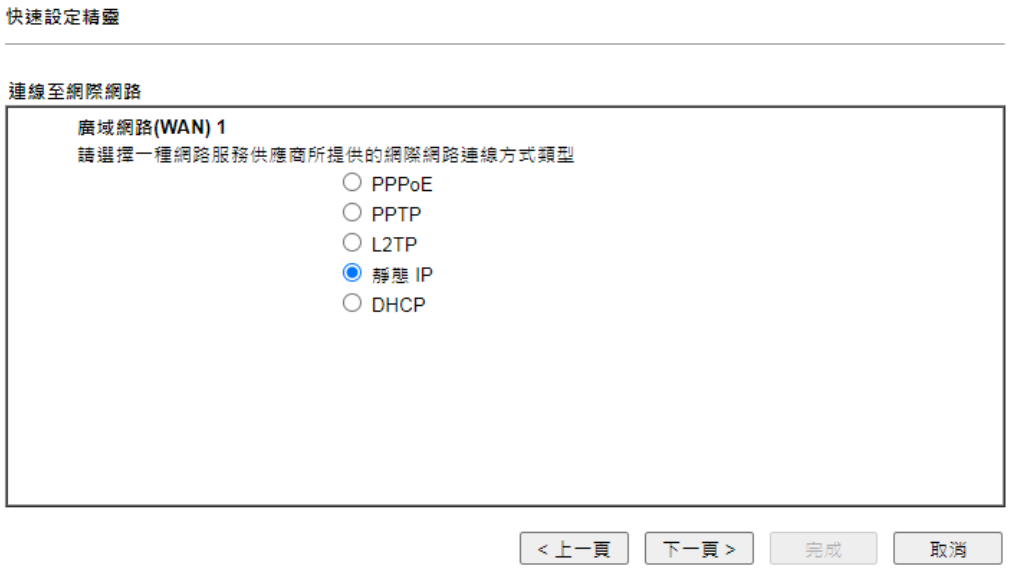


5. 現在您可以遨遊網際網路了。

靜態 IP(固定 IP)

在這種應用當中，您會從 ISP 取得一個固定真實 IP 位址或一個真實子網路(多個公開 IP 位址)。通常纜線(Cable) ISP 會提供一個固定的真實 IP，而 DSL ISP 則有可能會提供一個真實子網路。如果您擁有一個真實子網路，您可以選擇一個或多個 IP 位址設定在 WAN 介面。如果您需要使用固定 IP / 動態 IP，請先在視窗中選擇適當的模式，然後輸入相關資訊：

1. 選擇 **WAN1** 作為 WAN 介面，按**下一頁**按鈕後，下圖將會出現讓您指定網際網路連線類型。



2. 選擇**固定 IP(Static IP)**然後按**下一頁**開啟如下頁面。

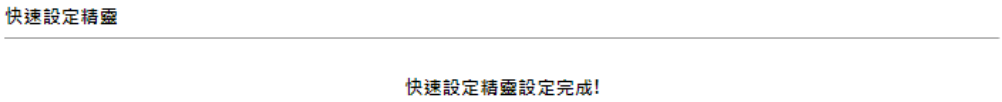
可用設定說明如下：

項目	說明
WAN IP	輸入 IP 位址。
子網遮罩	輸入子網路遮罩。

閘道器	輸入閘道 IP 位址。
主要 DNS	輸入路由器主要的 DNS IP 位址。
次要 DNS	必要時輸入路由器次要的 DNS IP 位址。
上一頁	按此鈕回到上一頁面。
下一頁	按此鈕進入下一頁面。
取消	按此鈕放棄快速設定精靈。

3. 請依照您的 ISP 業者提供的資料輸入使用者名稱與密碼。按**下一頁**檢視連線的設定狀態。

4. 按完成，快速設定精靈設定完成頁面將會出現。

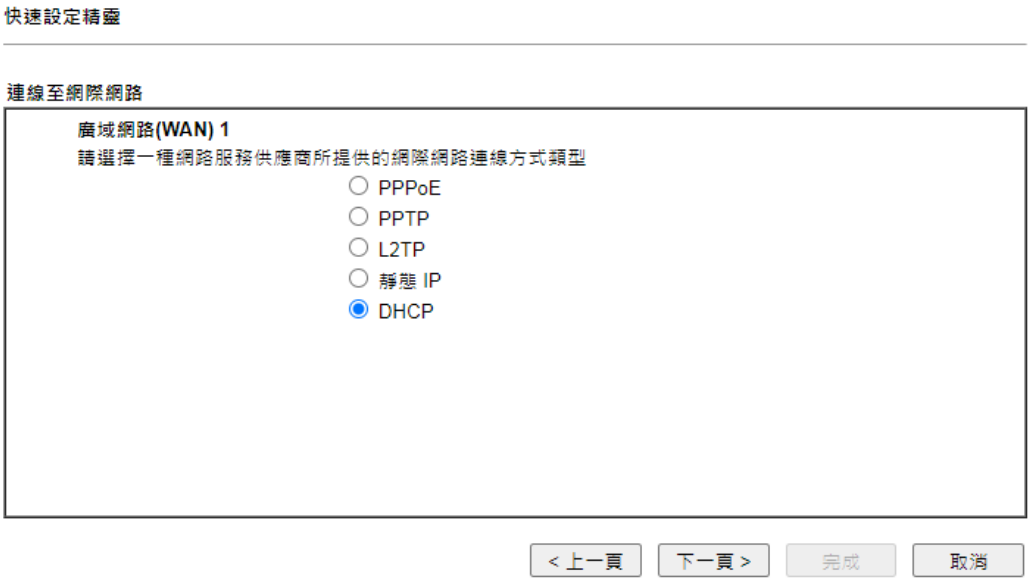


5. 現在您可以遨遊網際網路了。

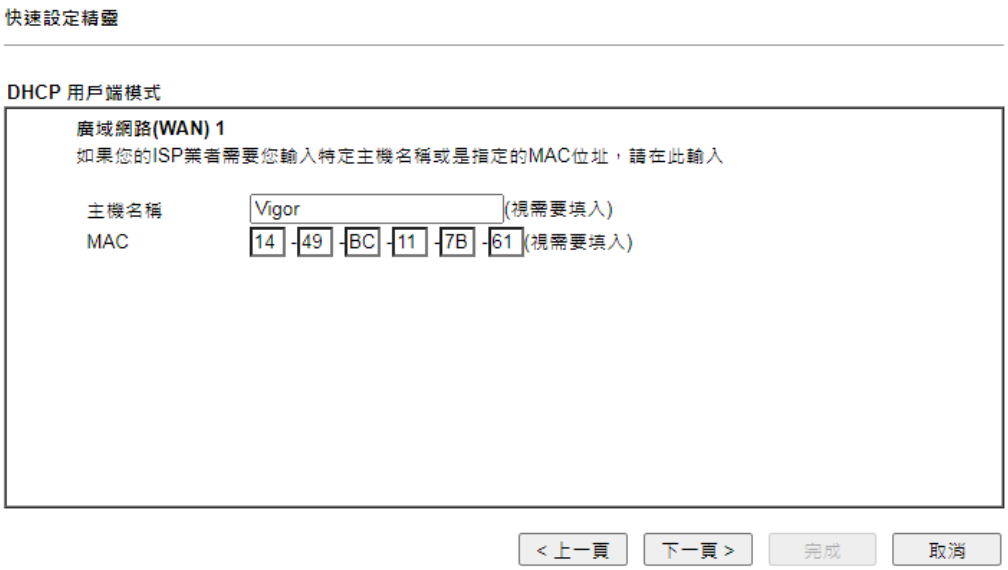
DHCP

選擇 **DHCP** 作為通訊協定，並在頁面上輸入 ISP 提供給您的全部訊息。

1. 選擇 **WAN1/WAN2** 作為 WAN 介面，按**下一頁**按鈕後，下圖將會出現讓您指定網際網路連線類型。



2. 選擇 **DHCP** 並按**下一頁**按鈕。



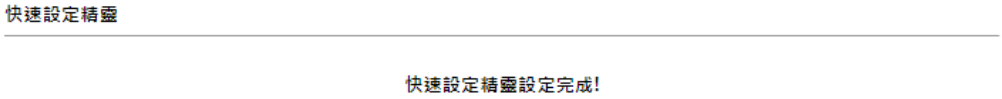
可用設定說明如下：

項目	說明
主機名稱	輸入主機名稱。
MAC	某些纜線服務供應商會要求提供 MAC 位址作為驗證，在此情況下，請於此欄位輸入 MAC 位址。

上一頁	按此鈕回到上一頁面。
下一頁	按此鈕進入下一頁面。
取消	按此鈕放棄快速設定精靈。

3. 完成上述設定之後，按**下一頁**檢視連線的設定狀態。

4. 按完成，快速設定精靈設定完成頁面將會出現。



5. 現在您可以遨遊網際網路了。

I-6-2 對於 WAN3 (USB)

如果要使用 3G /4G USB 數據機進行網路連線，請選擇 WAN3。

1. 選擇 **WAN3** 作為 WAN 介面。

可用設定說明如下：

項目	說明
顯示名稱	請輸入路由器的名稱。

2. 按**下一頁**，系統將會出現讓您指定網際網路連線類型。

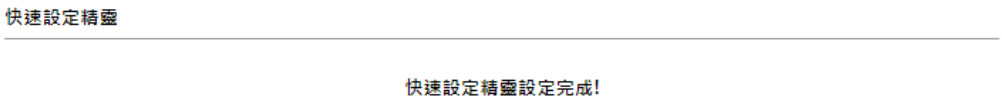
可用設定說明如下：

項目	說明
網際網路連線設定	選擇存取網際網路的連線模式。

3G/4G USB 數據機 (PPP 模式)	**SIM 卡 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。 **數據機初始化字串**– 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。 **APN 名稱**– 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，請輸入相關名稱並按下**套用**按鈕。
3G/4G USB 數據機 (DHCP 模式)	**SIM 卡 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**– 選擇適用的連線模式。 **APN 名稱**– 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。

3. 按**下一頁**檢視此連線的設定狀態。

4. 按完成，快速設定精靈設定完成頁面將會出現。



5. 現在您可以遨遊網際網路了。

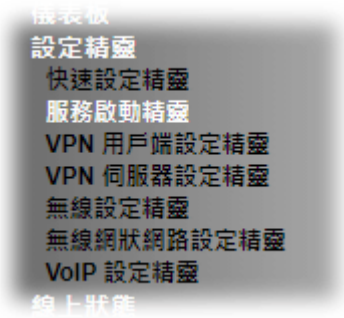
I-7 服務啟動精靈

服務啟用精靈可利用快速及簡便方式，幫助您啟用網頁內容過濾器服務機制(WCF)。服務啟用精靈是一個提供您使用試用版或是更新 WCF 授權憑證的工具，有了這項工具，您可不需要進入位於 http://myvigor.draytek.com 中的伺服器(***MyVigor***)。關於使用網頁內容過濾器的設定檔，請參考後續網頁內容過濾一節。

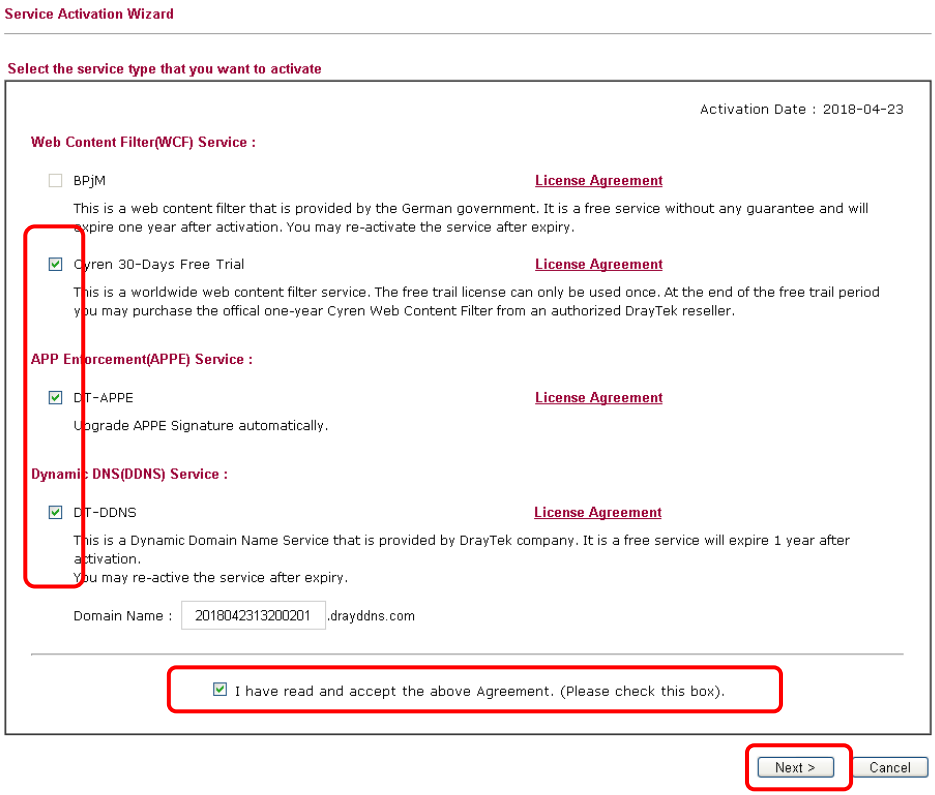
現在，請參考下述步驟進行啟用 WCF 功能作業。

資訊	此功能僅能於 Admin 模式下使用。

1. 開啟**設定精靈>>服務啟動精靈**。



2. 服務啟用精靈畫面顯示如下，您可以啟用 WCF 服務、APP 應用程式管控、DDNS 服務，勾選 “I have read....” 之後，按**下一頁**。



資訊

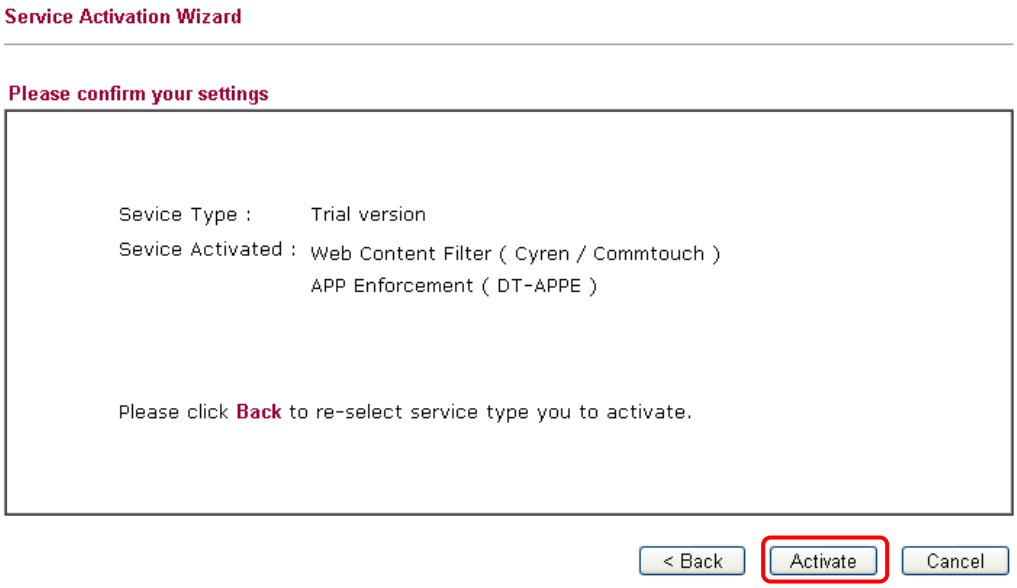
BPjM 是針對使用德語之用戶提供之服務，可為家庭與年輕人提供提供更安全的網際網路環境。

Cryan 提供30天試用版，之後您可以向Cryan GlobalView 採購正式版本。

DT-APPE是居易公司提供的免費服務，可自動更新APPE授權碼。

DT-DDNS是居易公司提供的免費動態DNS服務，供內部使用，為期一年。

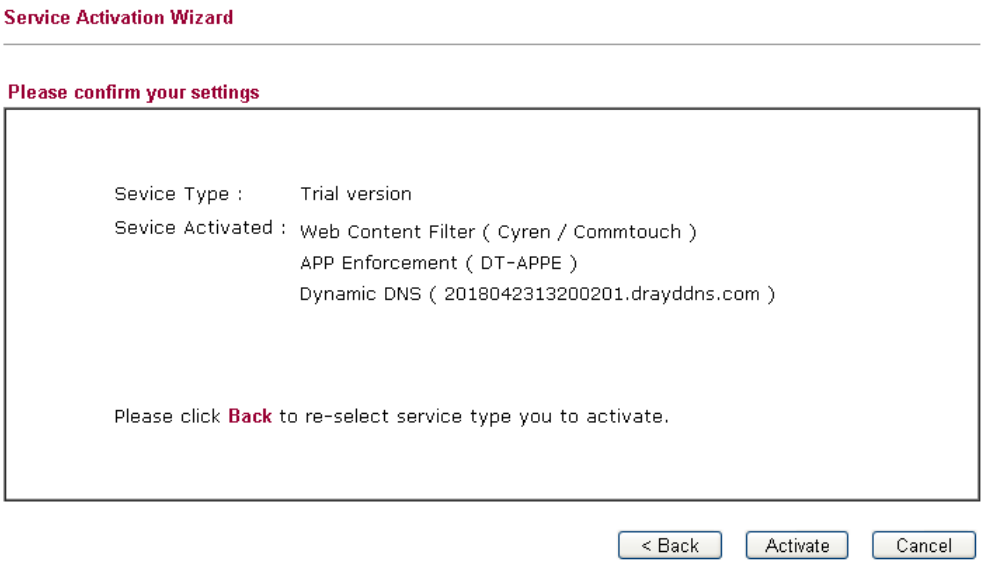
3. 設定確認頁面如下所示，請按下**啟動(Activate)**。



資訊

此項服務在**防火牆>>基本設定(Firewall>>General Setup)**中，可被視為預設規則啟用及套用

4. 現在，網頁將顯示您已經啟用的服務內容。

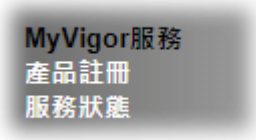


I-8 註冊 Vigor 路由器

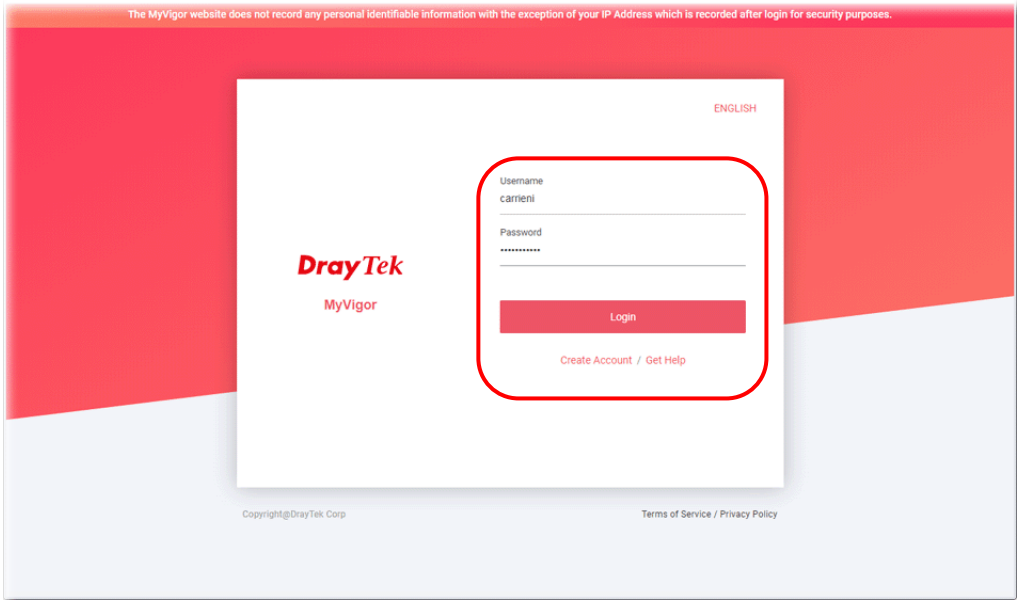
您已經完成快速安裝設定精靈，可隨時上網瀏覽您需要的資料與網站。現在您可以將 Vigor 路由器向 MyVigor 網站註冊登錄，以便取得更多的服務。請依下列步驟完成路由器註冊登錄作業。

1 請登錄路由器的網頁設定介面，並在使用者名稱與密碼欄位皆輸入 **admin**。

2 按下位於首頁上的 **MyVigor 服務>>產品註冊**。



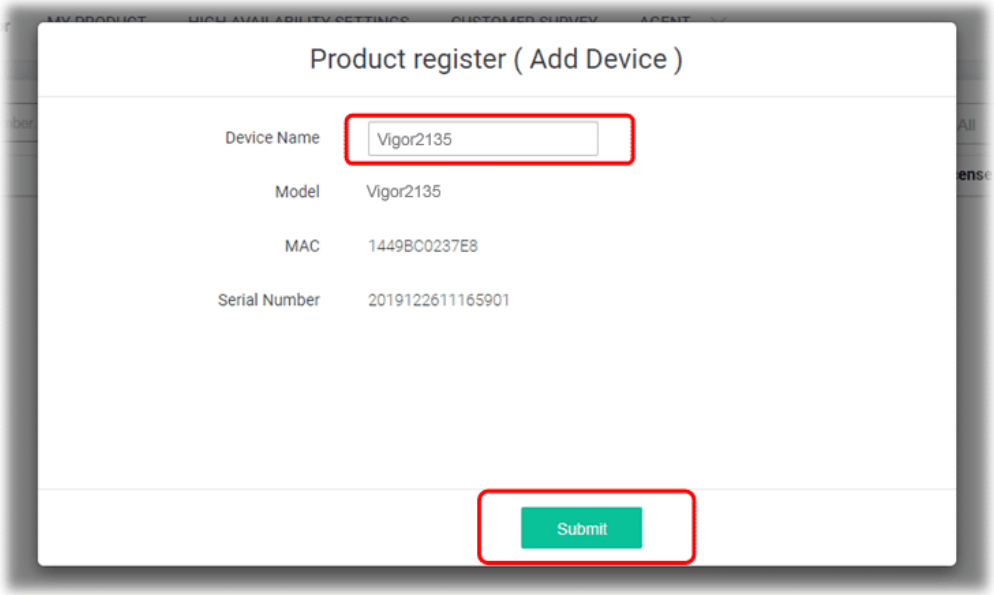
3 登入頁面出現如下圖，請輸入您先前即建立的帳號與密碼，然後按下**登入(Login)**。



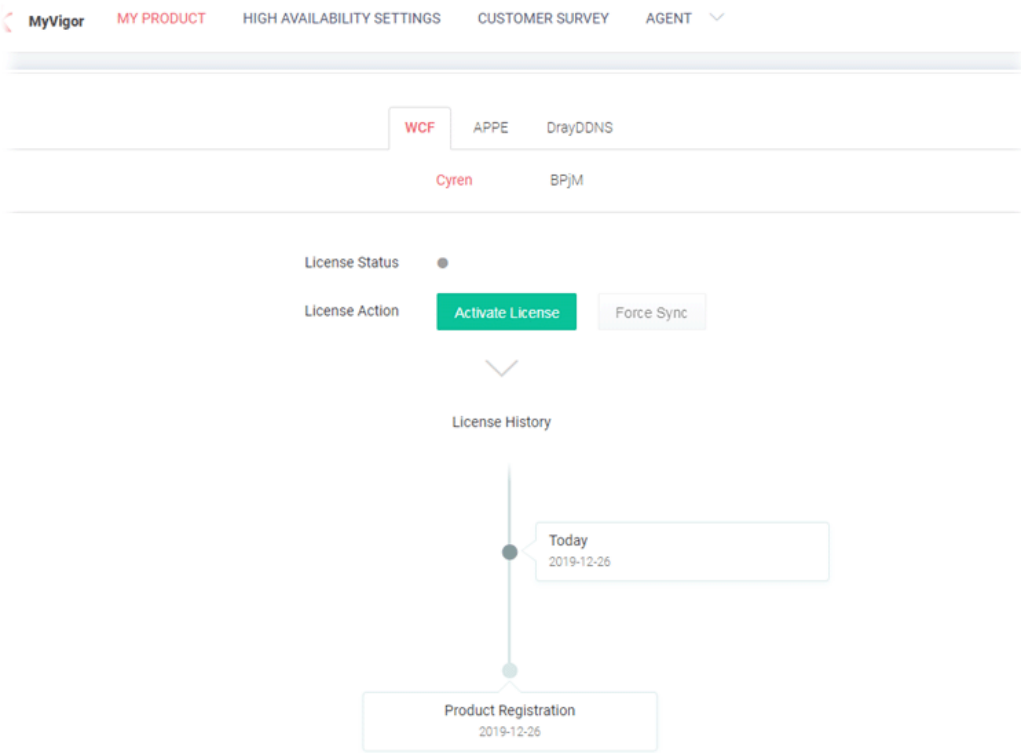
資訊

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。

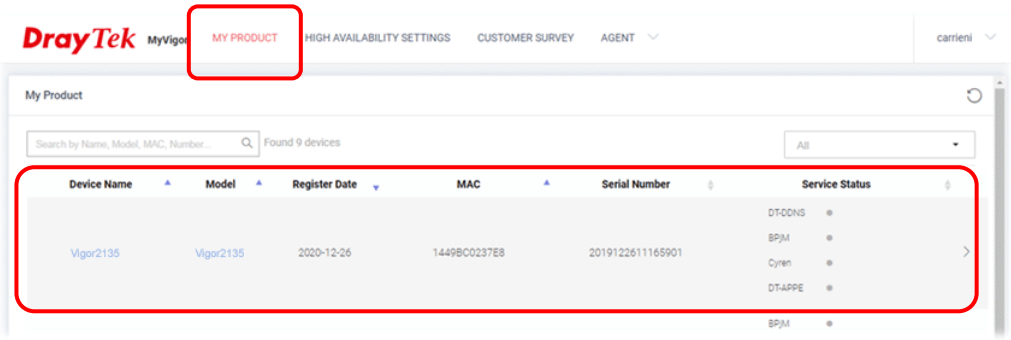
4 按下登入後，將會出現如下的畫面，輸入產品暱稱之後，按下**提交(Submit)**。



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。



6　按下 **MYPRODUCT**，查看註冊後的路由器基本資訊。



本頁留白

第二篇 連線設定

WAN

WAN表示寬頻網路，通常使用的是真實IP。

LAN

LAN代表區域網路，使用的是虛擬IP位址，基本上LAN是路由器規定且管理的子網群組，網路結構設計與取自ISP之真實IP位址類型有關聯。

NAT

當資料流量通過時，路由器的網路位址轉換(NAT)功能可以進行真實/虛擬IP位址轉換，封包可傳送至區域網路中正確的主機PC上。

Applications

應用的部份包含DDNS, LAN DNS, IGMP, LDAP, UPnP, WOL, RADIUS, SMS, Bonjour 等等

Routing

包含有固定路由、負載平衡/路由策略等等

II-1 WAN

可讓使用者登入網際網路。

網路的基本概念

IP 表示網際網路通訊協定，在以 IP 為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 位元址作為網路上身分辨識之用。為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，因為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，這些被稱之為虛擬 IP 位址，範圍條列如下：

From 10.0.0.0 to 10.255.255.255
From 172.16.0.0 to 172.31.255.255
From 192.168.0.0 to 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。

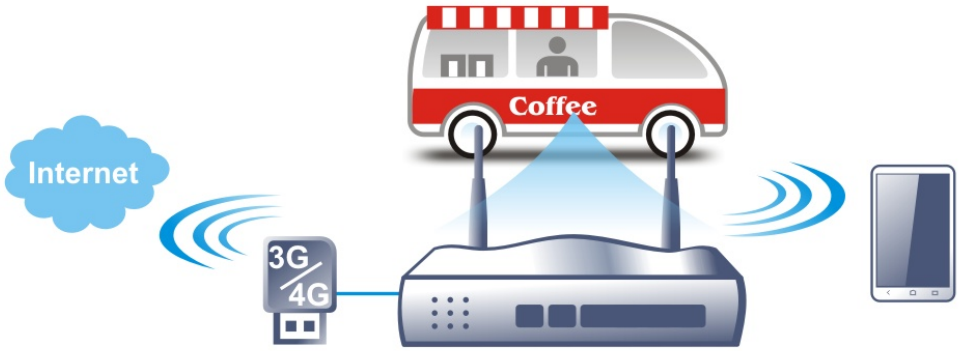
取得 ISP 提供的真實 IP 位址

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。

3G/4G USB Modem 網路連線

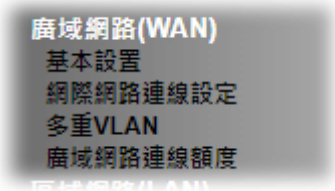
藉著連接 3G/4G USB 數據機至 Vigor2135 的 USB 埠，路由器可支援 HSDPA / UMTS / EDGE / GPRS / GSM / HSUPA 等標準，有了 USB 數據機的 Vigor2135ac 可讓您隨時隨地接收 3G/4G 信號，不論是在汽車上或是在戶外地區舉行活動時，都可讓多數人共用頻寬。



在連接上路由器後，3G/4G USB Modem 即被視為第二個 WAN 埠，雖然如此原本的乙太網路 WAN1 仍可作為負載平衡之用，此外 3G/4G USB Modem 也可被視為備存裝置。因此當 WAN1 無法使用時，路由器將自動改用 3G/4G USB Modem 以應需要。目前路由器支援哪些 3G/4G USB Modem，可在居易網站上取得，歡迎造訪 www.draytek.com。

網頁使用者介面

下圖為 WAN 的功能項目：



II-1-1 基本設置

本節介紹網際網路的一般設定，並詳細說明 WAN1, WAN3 介面。

可用設定說明如下：

項目	說明
索引	點選索引編號下的 WAN 介面連結，以登入 WAN 設定頁面。
啟用	勾選此框啟用此介面。
實體模式/類型	顯示此 WAN 介面的實體模式以及實體類型。
使用中的模式	顯示此 WAN 介面目前是主動裝置或是備援裝置。

完成上述設定之後，按下**確定**儲存設定內容。

II-1-1-1 WAN1(乙太網路)

WAN1 介面的實體模式固定為乙太網路。

可用設定說明如下：

項目	說明
啟用	選擇**是**啟動此 WAN 介面的設定，選擇**否**則關閉此介面的設定。
顯示名稱	輸入 WAN1 的說明內容。
實體模式	顯示此 WAN 介面的實體連線模式。
傳送資料模式	您可以改變 WAN 的傳送資料模式，或是選擇**自動協商**讓系統自行處理。
VLAN 標籤插入	此功能主要是提供給支援 IEEE_802.1ad 環境的用戶使用，其中服務(service)用在對外標籤(outer tag)；客戶(customer)用在對內標籤(inner tag)。 **啟用**- 啟動夾帶標籤的 VLAN 設定。 路由器將會加上特定的 VLAN 號碼於所有透過此 WAN 口傳出的封包上。 請輸入標籤值並指定由此 WAN 口傳送的封包的優先順序。 **停用**- 停止夾帶標籤的 VLAN 設定。 **標籤值**- 輸入準備作為 VLAN ID 編號的數值，可填範圍為 0 到 4095。 **優先權**- 輸入此 VLAN 設定的優先權限，可選範圍從 0 到 7。

完成上述設定之後，按下**確定**儲存設置內容。

II-1-1-2 WAN3 (USB)

如果要透過 3G/4G USB 數據機來使用 3G/4G 網路連線，請設定 WAN3 介面。

可用設定說明如下：

項目	說明
啟用	選擇**是**啟動此 WAN 介面的設定，選擇**否**則關閉此介面的設定。
顯示名稱	輸入 WAN1 的說明內容。
實體模式	顯示此 WAN 介面的實體連線模式。
使用中的模式	**永遠連線** – 讓 WAN 連線永遠啟用。 **失效切換** – 選擇此項讓目前的 WAN 連線成為備援連線。

完成上述設定之後，按下**確定**儲存設置內容。

II-1-2 網際網路連線設定

因為路由器支援多 WAN 口功能，使用者得以設定不同的 WAN 設定供網際網路存取之用，又因為 WAN1/ WAN3 的實體連線並不同，連線模式也會有些差異。

可用設定說明如下：

項目	說明
索引	顯示路由器支援的 WAN 介面。
顯示名稱	顯示 WAN 於一般設定中所輸入的名稱。
實體模式	按照實際網路連線狀況來顯示各個 WAN 實體連線。
連線模式	使用下拉式清單選擇適當的網際網路連線模式，接著按右邊的**細節頁面**以設定詳細內容。網頁提供數種網際網路連線模式。
細節頁面	此按鈕將依照您在 WAN 所選擇的連線模式展現不同的網頁內容。
IPv6	此按鈕將會開啟不同的網頁(以實體連線模式為基準)，針對 WAN 介面設定 IPv6 網際網路連線模式。 如果在 WAN 介面中 IPv6 已經啟動了，那麼您可以在網頁上看到綠色的 IPv6 字樣。
DHCP 用戶端選項	此按鈕可設定 DHCP 用戶端選項(DHCP client options)。 DHCP 封包可利用新增之選項號碼及資料資訊進行不同的處理。 **啟用**- 勾選此框啟用此 DHCP 選項功能。每個 DHCP 選項是由選項號碼與資料組合而成，例如

	Option number:100 Data: abcd 當功能啟用時，指定的 DHCP option 數值將可現於 DHCP 回覆封包中。 **介面** – 指定此功能可覆寫的 WAN 介面， WAN4 ~ WAN6 可透過 **WAN>>多重 VLAN** 中指定。 **選項號碼** – 請針對此功能輸入需求數字。 **附註:** 若您選擇設定 option 61，那麼 **WAN>>網際網路連線設定**中的的細節頁面內容將會被覆寫。 **資料類型** – 選擇要儲存的資料類型(ASCII 或是十六進位)。 **資料** – 輸入 DHCP option 功能準備處理的資料內容。

II-1-2-1 WAN1 中的 PPPoE 模式細節設定(實體模式：乙太網路)

如果想要使用 PPPoE 作為網際網路連線的通訊協定，請自 **WAN** 功能項目中選擇**網際網路連線設定**，接著在 WAN1 中選擇 PPPoE 模式，下面的細節設定網頁將會出現。

可用設定說明如下：

項目	說明
啟用/停用	按下**啟用**按鈕可啟動此功能，如果您選的是**停用**，此項功能將會關閉，全部調整過的設定也都將立即失效。
ISP 存取設定	輸入使用者名稱、密碼和驗證參數，按照 ISP 所提供給您的訊息。 **使用者名稱** – 在本區請輸入 ISP 提供的使用者名稱。 **密碼** – 在本區請輸入 ISP 提供的密碼。 **更多選項** - 按此顯示更多選項。 ● **服務名稱(選項)** - 輸入特定網路服務的相關說明。
PPPoE 通透	路由器提供 PPPoE 撥號連線，除此之外，您也可以直接建立 PPPoE 連線，連接本機用戶端與 ISP 業者。當選定 PPPoA 通訊協定時，PC 傳送的 PPPoE 封包將可轉換為 PPPoA 封包並傳送至 WAN 伺服器。如此一來，PC 可透過該傳輸方向存取網際網路。 **針對有線區域網路** – 若勾選此框，相同網路上的 PC 可以使用另一組 PPPoE 連線數(不同於主機 PC)以存取網際網路。 **針對無線區域網路** – 這個功能僅適用 *n/ax* 機種，若勾選此框，相同無線區域網路上的 PC 可以使用另一組 PPPoE 連線數(不同於主機 PC)以存取網際網路。

	附註: 欲使用 PPPoA 通透，請先選擇 PPPoA 通訊協定，在勾選此出的方框，路由器將表現有如數據機，僅提供 LAN 端的 PPPoE 用戶相關的服務，亦即路由器將提供 PPPoA 撥號連線。
WAN 連線偵測	這個功能讓您檢查目前網路是否還在連線中。可透過 PPP 偵測或是 Ping 偵測來完成。 **模式**– 選擇 **PPP 偵測**或 **Ping 偵測**執行 WAN 檢測動作。 ● **主要/次要 Ping IP** – 若您選擇了 **Ping 偵測**作為偵測模式，您必須在本區輸入主要或是次要 IP 位址。 ● **Ping 閘道 IP** – 若您選擇了 **Ping 偵測**作為偵測模式，您也可以啟用此設定，以便使用目前的 WAN 閘道做為 ping IP 位址。藉由 IP 位址 ping，路由器可以檢查該 WAN 連線是啟用的或是中斷的。 ● **TTL (Time to Live)** – 設定 ping 操作需要的 TTL 數值。 ● **Ping 間隔**- 輸入執行 Ping 操作系統所需要的時間間隔。 ● **Ping 重試次數** - 輸入判斷 WAN 連線中斷之前，系統執行 Ping 操作時容許的嘗試次數。
MTU	代表封包的最大傳輸單位。 **路徑 MTU 搜尋** – 用於偵測封包在特定傳輸路徑當中，不被分段的最大 MTU 尺寸。 按**偵測** 開啟如下頁面： ● **路徑 MTU 至** – 輸入 IPv4/IPv6 位址作為特定傳輸路徑。 ● **MTU 大小值起自** – 決定封包起始值，預設值為 1500。 ● **MTU 值之降低乃透過** – 決定 MTU 值的降低大小，例如此區指定數字為 8，最大的 MTU 大小為 1500，在您按下檢測按鈕之後，系統將會計算並取得適合的 MTU 值，像是 1500、1492、1484 等等。 ● **偵測** – 按此檢測出適合的 MTU 值。 ● **接受** – 選了此項之後，檢測得到的值會顯示在 MTU 欄位中。
PPP/MP 設定	**PPP 驗證** – 選擇**限用 PAP** 或是 **PAP / CHAP / MS-CHAP / MS-CHAPv2**。 **閒置逾時** – 設定網際網路在經過一段沒有任何動作的時間後自動斷線的時間。 **IP 位址指派方法(IPCP)** - 通常每次的連線，ISP 會隨機指派 IP 位址給您，在某些情況下，您的 ISP 可以提供給您相同的 IP 位址，不論您何時提出要求。您只要在固定 IP 位址欄位中輸入 IP 位址就可以達成上述的目的。詳情請聯絡您的 ISP 業者。 **WAN IP 別名** - 如果您有數個真實 IP 位址且想要在 WAN 介面上使用，請使用此功能。除了目前使用的這一組之外，您還可以設定多達 32 組的真實 IP 位址。

	固定 IP 位址 – 按**是**使用此功能並輸入一個固定的 IP 位址。
排程設定	您可以輸入四組時間排程，所有的排程皆可於**應用程式>>排程**頁面中事前設定，只要在此輸入該頁面設定的排成索引編號即可。
TTL	**變更 TTL 值** -啟用或是停用封包透過路由器傳輸時的 TTL 功能。 ● **啟用** – TTL 值會在通過路由器時降低(-1)，這會讓透過路由器存取網際網路的用戶端，在 TTL 的數值變為 0 的時候，直接被指定 ISP 封鎖住。 ● **停用** – TTL 值不會減少，之後當封包透過路由器傳送時，就不會被取消。也就是說，傳送此封包的用戶端並不會被 ISP 業者封鎖住。 **預設 MAC 位址** – 您可以在此使用**預設 MAC 位址**或是指定另一組 MAC 位址。 **使用下述 MAC 位址**- 手動輸入路由器需求之 MAC 位址。

完成上述設定之後，按下**確定**儲存設置內容。

II-1-2-2 WAN1 中的靜態或是動態 IP 模式細節設定(實體模式：乙太網路)

對固定 IP 模式來說，通常您會收到 DSL 或是 ISP 服務供應商提供給您的一個固定的真實 IP 位址或是真實子網路，在大多數的情形下，Cable 服務供應商將會提供一個固定的真實 IP，而 DSL 服務供應商提供的是真實子網路資料。如果您有一組真實的子網路，您可以指派一組或是多組 IP 位址至 WAN 介面。

若要使用**靜態或動態 IP** 為網際網路的連線協定，請自 **WAN** 中選擇**網際網路連線設定**，接著選擇**靜態或動態 IP**，即可出現下圖。

可用設定說明如下：

項目	說明
啟用/停用	按下**啟用**按鈕可啟動此功能，如果您選的是**停用**，此項功能將會關閉，全部調整過的設定也都將立即失效。
IP 網路設定	本區讓您自動取得 IP 位址或是手動輸入需求的 IP 位址。 **自動取得 IP 位址** – 如果您想要使用**動態 IP** 模式，按此鈕以自動取得 IP 位址。 **更多選項** - 按此顯示更多的選項。 ● **路由器名稱** – 輸入 ISP 的路由器名稱。 ● **網域名稱** – 輸入指定的網域功能變數名稱。 ● **DHCP 用戶端識別碼** – 勾選此框指定使用者名稱與密碼，做為某些 ISP 需求的 DHCP 用戶端辨識之用。

	● **使用者名稱** - 輸入任何名稱，最大長度不要超過 63 個字元。 ● **密碼** - 輸入任何密碼，最大長度不要超過 62 個字元。 **指定 IP 位址** – 按此鈕指定 IP 位址讓資料通過。 ● **IP 位址** - 輸入 IP 位址。 ● **子網遮罩** - 輸入子網路遮罩。 ● **閘道 IP 位址** - 輸入閘道 IP 位址。 **WAN IP 別名**- 如果您有多個真實 IP 位址，想要在 WAN 介面上利用這些 IP，請使用 WAN IP 別名。除了目前使用的 IP 外，您還可以另外設定 8 組真實 IP。
DNS 伺服器 IP 位址	若要使用固定 IP 模式，請輸入路由器的主要 IP 位址，如有必要，在將來，您也可以輸入次要 IP 位址以符合所需。
WAN 連線偵測	這個功能讓您檢查目前網路是否還在連線中。 **模式**– 選擇**嚴格 ARP 偵測**、**ARP 偵測**、**Ping 偵測**或是**永遠連線**執行 WAN 檢測動作。 ● **主要/次要 Ping IP** – 若您選擇了 **Ping 偵測**作為偵測模式，您必須在本區輸入主要或是次要 IP 位址。 ● **Ping 閘道 IP** – 若您選擇了 **Ping 偵測**作為偵測模式，您也可以啟用此設定，以便使用目前的 WAN 閘道做為 ping IP 位址。藉由 IP 位址 ping，路由器可以檢查該 WAN 連線是啟用的或是中斷的。 ● **TTL (Time to Live)** – 設定 ping 操作需要的 TTL 數值。 ● **Ping 間隔** – 輸入執行 Ping 操作系統所需要的時間間隔。 ● **Ping 重試次數** – 輸入判斷 WAN 連線中斷之前，系統執行 Ping 操作時容許的嘗試次數。
MTU	代表封包的最大傳輸單位。 **路徑 MTU 搜尋** – 用於偵測封包在特定傳輸路徑當中，不被分段的最大 MTU 尺寸。 按**偵測** 開啟如下頁面： 路徑MTU至: IPv4 主機 MTU 大小值起自 1500 (1000~1500) MTU值之降低乃透過 8 (1~100) 偵測 備註: 路徑 MTU 搜尋將會降低 MTU 大小3次 接受 取消 ● **路徑 MTU 至** – 輸入 IPv4/IPv6 位址作為特定傳輸路徑。 ● **MTU 大小值起自** – 決定封包起始值，預設值為 1500。 ● **MTU 值之降低乃透過** – 決定 MTU 值的降低大小，例如此區指定數字為 8，最大的 MTU 大小為 1500，在您按下檢測按鈕之後，系統將會計算並取得適合的 MTU 值，像是 1500、1492、1484 等等。 ● **偵測** – 按此檢測出適合的 MTU 值。 ● **接受** – 選了此項之後，檢測得到的值會顯示在 MTU 欄位中。

維持 WAN 連線	正常情況下，這個功能是設計用來符合動態 IP 環境，因為某些 ISP 會在一段時間沒有任何回應時中斷連線。請勾選**啟用 PING 以維持連線**。 ● **PING 至 IP** – 如果您啟用此功能，請指定 IP 位址讓系統可以 PING 到該 IP 以保持連線 ● **PING 間隔** - 輸入間隔時間讓系統得以執行 PING 動作。
TTL	**變更 TTL 值** -啟用或是停用封包透過路由器傳輸時的 TTL 功能。 ● **啟用** – TTL 值會在通過路由器時降低(-1)，這會讓透過路由器存取網際網路的用戶端，在 TTL 的數值變為 0 的時候，直接被指定 ISP 封鎖住。 ● **停用** – TTL 值不會減少，之後當封包透過路由器傳送時，就不會被取消。也就是說，傳送此封包的用戶端並不會被 ISP 業者封鎖住。
RIP 路由	指名路由器是如何變更路由表格資訊，勾選**啟用 RIP** 此項目以啟動此功能。
MAC 位址	**預設 MAC 位址** - 按此以使用路由器的預設 MAC 位址。 **指定一個 MAC 位址** - 某些纜線服務供應商會指定一個 MAC 位址以應存取驗證。在此情況下，您需要按此鈕並輸入 MAC 位址。

完成上述設定之後，按下**確定**儲存設置內容。

II-1-2-3 WAN1 中的 PPTP/L2TP 模式細節設定(實體模式：乙太網路)

若要使用 **PPTP/L2TP** 為網際網路的連線協定，請自 **WAN** 中選擇**網際網路連線設定**，接著選擇 **PPTP/L2TP**，即可出現下圖。

可用設定說明如下：

項目	說明
PPTP/L2TP	**啟用 PPTP** - 選擇此鈕已啟用 PPTP 用戶端建立通往 WAN 介面的 DSL 數據機之通道。 **啟用 L2TP** - 選擇此鈕已啟用 L2TP 用戶端建立通往 WAN 介面的 DSL 數據機之通道。 **停用** - 選擇此鈕停用 PPTP 或 L2TP 連線通道。 **伺服器位址** - 指定 PPTP/ L2TP 伺服器的 IP 位址。 **指定閘道 IP 位址** - 針對 PTP/L2TP 伺服器指定閘道 IP 位址。
ISP 存取設定	**使用者名稱** - 輸入 ISP 業者提供給您的使用者名稱。 **密碼** - 輸入 ISP 業者提供的密碼。 **排程設定檔** - 您可以輸入四組時間排程設定，所有的排程都是在時間**其他應用>>排程設定**網頁中事先設定完畢，您可直接輸入該時間排程的號碼即可。
MTU	代表封包的最大傳輸單位。 **路徑 MTU 搜尋** – 用於偵測封包在特定傳輸路徑當中，不被分段的最大 MTU 尺寸。 按**偵測**開啟如下頁面： ● **路徑 MTU 至** – 輸入 IPv4/IPv6 位址作為特定傳輸路徑。 ● **MTU 大小值起自** – 決定封包起始值，預設值為 1500。 ● **MTU 值之降低乃透過** – 決定 MTU 值的降低大小，例如此區指定數字為 8，最大的 MTU 大小為 1500，在您按下檢測按鈕之後，系統將會計算並取得適合的 MTU 值，像是 1500、1492、1484 等等。 ● **偵測** – 按此檢測出適合的 MTU 值。 ● **接受** – 選了此項之後，檢測得到的值會顯示在 MTU 欄位中。
PPP/MP 設定	**PPP 驗證** – 選擇**限用 PAP** 或是 **PAP / CHAP / MS-CHAP / MS-CHAPv2**。 **閒置逾時** – 設定網際網路在經過一段沒有任何動作的時間後自動斷線的時間。 **IP 位址指派方法(IPCP)** - 通常每次的連線，ISP 會隨機指派 IP 位址給您，在某些情況下，您的 ISP 可以提供給您相同的 IP 位址，不論您何時提出要求。您只要在固定 IP 位址欄位中輸入 IP 位址就可以達成上述的目的。詳情請聯絡您的 ISP 業者。 **WAN IP 別名** - 如果您有數個真實 IP 位址且想要在 WAN 介面上使用，請使用此功能。除了目前使用的這一組之外，您還可以設定多達 8 組的真實 IP 位址。 **固定 IP 位址** – 按**是**使用此功能並輸入一個固定的 IP 位址。
WAN IP 網路設定	**自動取得 IP 位址** – 按此鈕以自動取得 IP 位址。

	指定 IP 位址 – 按此鈕以指定 IP 位址。 ● **IP 位址** – 輸入 IP 位址。 ● **子網遮罩** – 輸入子網路遮罩。

完成上述設定之後，按下**確定**儲存設置內容。

II-1-2-4 WAN3 中的 3G/4G USB 數據機模式細節設定(PPP 模式)

如果要使用 3G/4G USB 數據機 (PPP 模式) (針對 3G/4G USB 數據機) 做為網際網路連線協定，請自 **WAN** 中選擇**網際網路連線設定**，接著在 WAN3 介面上選擇 **3G/4G USB 數據機(PPP 模式)**，即可出現下圖。

可用設定說明如下：

項目	說明
數據機支援清單	條列路由器支援的所有數據機。 192.168.1.150/doc/pppsuptlst.htm - Google Chrome 不安全 | 192.168.1.150/doc/pppsuptlst.htm 3G/4G 數據機支援清單(PPP 模式) 下述相容性測試列出在某些環境或是國家中Vigor路由器支援的 3.5G/LTE 數據機，如果您所擁有的LTE數據機在清單上但卻無法正常運作，請透過客服信箱 support@draytek.com 反應您的問題，或聯絡您的經銷商取得更多資訊。 品牌 / 型號 / LTE / 狀態 4G system / XSPlug P3 / ✗ / Y Aiko / Aiko 76E / ✗ / Y Alcatel / Alcatel X500 / ✗ / Y Alfa / ALFA Flyppp / ✗ / Y Amoi / Amoi H01 / ✗ / Y BandRich / Bandluxe C321 / ✗ / Y BandRich / Bandluxe C330 / ✗ / Y BandRich / Bandluxe C331 / ✗ / Y BandRich / Bandluxe C502 / ✗ / Y
3G/4G USB 數據機 (PPP 模式)	選擇**啟用**，開啟此功能。如果您選的是**停用**，此功能將不再運作，所有設定也都會失效。
SIM 卡 PIN 碼	輸入 SIM 卡 PIN 碼，以便連線網際網路。
數據機初始化字串	這個數值，用來初始化 USB 數據機，請使用預設值，如果您有

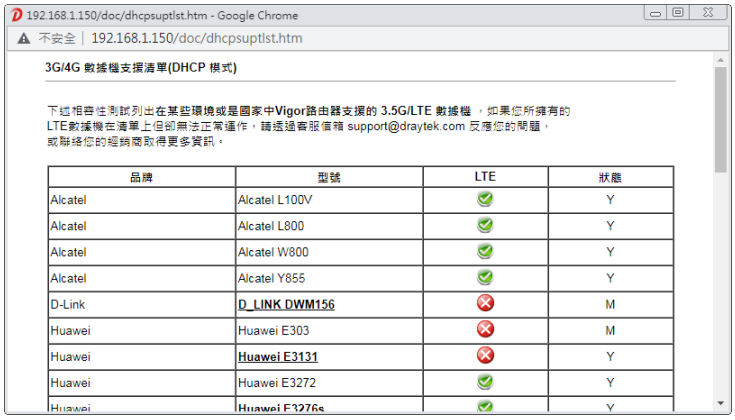
	任何疑問，請與當地 ISP 業者聯絡。
APN 名稱	APN 代表接入點名稱(Access Point Name)是由您的 ISP 所提供的，必要時請輸入 ISP 提供的資料，然後按下**套用**即可。
數據機初始化字串 **2**	初始化字串 1 是與 APN 搭配使用。 但在某些情況下，使用者可能會使用另外的初始化 AT 指令來限制 3G 頻寬或是其他特殊事宜。此時即可設定第二個數據機初始化字串。
數據機撥號字串	這個數值，目的是在 USB 模式下撥號使用，請使用預設值，如果您有任何疑問，請與當地 ISP 業者聯絡。
服務名稱	輸入指定網路服務的相關說明。
PPP 使用者名稱	輸入 PPP 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)。
PPP 驗證	選擇 **PAP** 或是 **PAP** 或 **CHAP**。
排程設定檔	可以輸入四組時間排程，全部的排程都是在**其他應用>>排程**網頁中事先設定完畢，您可在此輸入該排程的索引編號。
WAN 連線偵測	這個功能讓您檢查目前網路是否還在連線中。可透過 PPP 檢測或是 Ping Detect 來完成。 模式- 選擇 **PPP 偵測**或 **Ping 偵測**執行 WAN 檢測動作。 ● **主要/次要 Ping IP** – 若您選擇了 **Ping 偵測**作為偵測模式，您必須在本區輸入主要或是次要 IP 位址。 ● **TTL (Time to Live)** – 設定 ping 操作需要的 TTL 數值。 ● **Ping 間隔 -** 輸入執行 Ping 操作系統所需要的時間間隔。 ● **Ping 重試次數 -** 輸入判斷 WAN 連線中斷之前，系統執行 Ping 操作時容許的嘗試次數。

完成上述設定之後，按下**確定**儲存設置內容。

II-1-2-5 WAN3 中的 3G/4G USB 數據機模式細節設定(DHCP 模式)

欲使用 3G/4G USB 數據機(DHCP 模式)作為網際網路的存取協定，請開啟 **WAN>>網際網路連線設定**，然後自 WAN3 連線模式下拉式清單中選擇 **3G/4G USB 數據機(DHCP 模式)**。接著即可看見如下頁面：

可用設定說明如下：

項目	說明
數據機支援清單	條列路由器支援的所有數據機。 
啟用/停用	按**啟用**啟動此功能，如果您選擇**停用**，此功能將會關閉，所有本頁的設定也將立即失效。

192.168.1.150/doc/dhcpsuptlst.htm - Google Chrome
不安全 | 192.168.1.150/doc/dhcpsuptlst.htm

3G/4G 數據機支援清單(DHCP 模式)

下述相容性測試列出在某些環境或是國家中Vigor路由器支援的 3.5G/LTE 數據機，如果您所擁有的LTE數據機在清單上但卻無法正常運作，請透過電郵信箱 support@draytek.com 反應您的問題，或聯絡您的經銷商取得更多資訊。

品牌	型號	LTE	狀態
Alcatel	Alcatel L100V	✓	Y
Alcatel	Alcatel L800	✓	Y
Alcatel	Alcatel W800	✓	Y
Alcatel	Alcatel Y855	✓	Y
D-Link	D_LINK DWM156	✗	M
Huawei	Huawei E303	✗	M
Huawei	Huawei E3131	✗	Y
Huawei	Huawei E3272	✓	Y
Huawei	Huawei E3276s	✓	Y

SIM 卡 PIN 碼	輸入 SIM 卡 PIN 碼，以便連線網際網路。
網路模式	路由器將以此處所選擇的模式進行網路連線，如果您選擇 4G/3G/2G，路由器將依據實際的無線網路訊號自行挑選適合的模式。
APN 名稱	APN 代表基地台名稱(Access Point Name)是由您的 ISP 所提供的，必要時請輸入 ISP 提供的資料，然後按下**套用**即可。 **停用自動 APN** - 若條列之 APN 名稱與您的 ISP 業者提供的不同，請勾選此框並手動輸入正確的 APN。
WAN 連線偵測	這個功能讓您檢查目前網路是否還在連線中。可透過 ARP 檢測或是 Ping Detect 來完成。 **模式(Mode)** – 選擇 **ARP 偵測**、**嚴格 ARP 偵測**或 **Ping 偵測**執行 WAN 檢測動作。 ● **主要/次要 Ping IP** – 若您選擇了 **Ping 偵測** 作為偵測模式，您必須在本區輸入主要或是次要 IP 位址。 ● **Ping 閘道 IP** – 若您選擇了 **Ping 偵測**作為偵測模式，您也可以啟用此設定，以便使用目前的 WAN 閘道做為 ping IP 位址。藉由 IP 位址 ping，路由器可以檢查該 WAN 連線是啟用的或是中斷的。 ● **TTL (Time to Live)** – 設定 ping 操作需要的 TTL 數值。 ● **Ping 間隔** – 輸入執行 Ping 操作系統所需要的時間間隔。 ● **Ping 重試次數** – 輸入判斷 WAN 連線中斷之前，系統執行 Ping 操作時容許的嘗試次數。
排程設定檔	您可以選擇四組時間排程設定，所有的排程都是在時間**其他應用>>排程設定**網頁中事先設定完畢。
MTU	代表封包的最大傳輸單位。 **路徑 MTU 搜尋** – 用於偵測封包在特定傳輸路徑當中，不被分段的最大 MTU 尺寸。 按**偵測**開啟如下頁面： ● **路徑 MTU 至** – 輸入 IPv4/IPv6 位址作為特定傳輸路徑。 ● **MTU 大小值起自** – 決定封包起始值，預設值為 1500。 ● **MTU 值之降低乃透過** – 決定 MTU 值的降低大小，例如此區指定數字為 8，最大的 MTU 大小為 1500，在您按下檢測按鈕之後，系統將會計算並取得適合的 MTU 值，像是 1500、1492、1484 等等。 ● **偵測** – 按此檢測出適合的 MTU 值。 ● **接受** – 選了此項之後，檢測得到的值會顯示在 MTU 欄位中。
驗證	選擇 **PAP** 或是 **PAP 或 CHAP**。 **使用者名稱** – 輸入驗證需求之使用者名稱。

	密碼 – 輸入驗證需求之密碼。

完成上述設定之後，按下**確定**儲存設置內容。

II-1-2-6 WAN1/WAN3 的離線模式細節設定(IPv6)

當選擇**離線**類型時，IPv6 連線是中斷的。

II-1-2-7 WAN1 的 PPP 模式細節設定(IPv6)

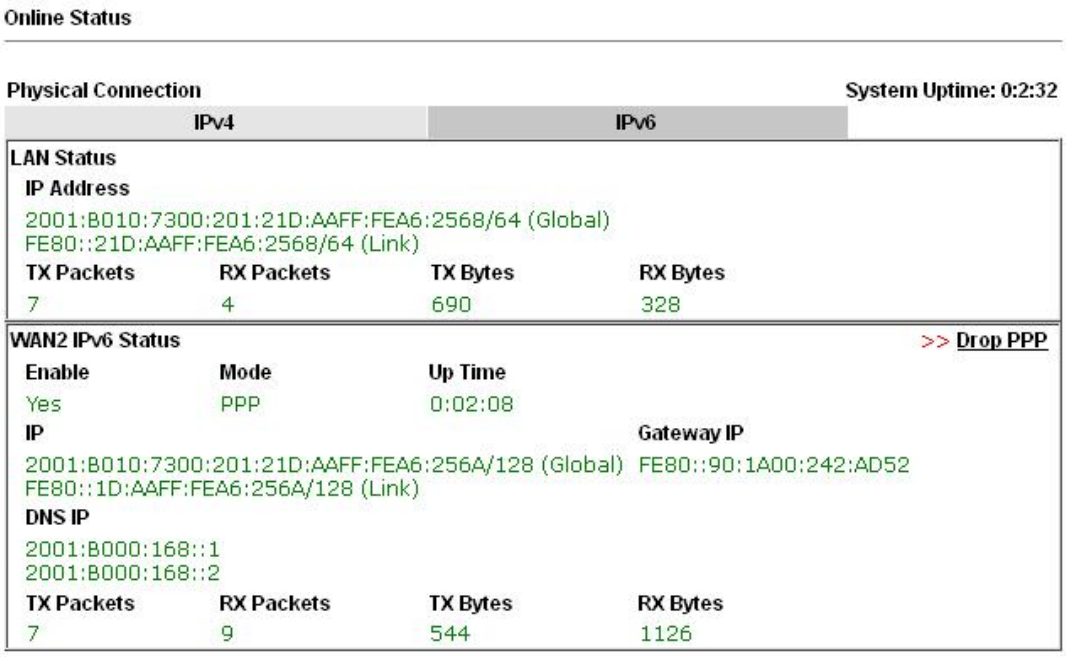
在 IPv4 PPPoE 連線中，我們可以在閘道器與 Vigor 路由器之間透過 IPv6CP 取得 IPv6 連線的本地位址。之後，使用 DHCPv6 或是接受 RA 來取得 IPv6 的前置碼位址(像是 2001:B010:7300:200::/64 等)，這些是由 ISP 所提供的。另外，在區域網路端的電腦也可以透過處理過的前置碼而擁有實際 IPv6 位址以便存取網際網路。

在 PPP 模式之下，不需進行任何設定。

可用設定說明如下：

項目	說明
WAN 連線偵測	這個功能讓您檢查目前網路是否還在連線中。 **模)** – 選擇**永遠連線或 Ping 偵測**執行 WAN 檢測動作。**永遠連線**表示無需進行任何檢測，網路永遠連線。 ● **Ping IP/主機** – 若您選擇了 **Ping 偵測**作為偵測模式，您必須在本區輸入 IP 位址或主機名稱。 ● **TTL (Time to Live)** – 設定 ping 操作需要的 TTL 數值。
RIPng 通訊協定	下一代 RIP(RIPng) 提供與 IPv4 RIP v2 相同的功用。

下圖顯示 PPP 模式下，成功的 IPv6 連線運作範例圖。



資訊

目前，IPv6前置碼可透過某些地區例如台灣(hinet)、荷蘭、澳洲及英國提供的PPP模式連線來取得。

II-1-2-8 WAN1/WAN3 的 TSPC 模式細節設定(IPv6)

TSPC(Tunnel setup protocol client)是一種應用，可幫助您輕鬆連至 IPv6 網路。

請先確認您的 IPv4 WAN 連線是可行的，並自 hexago (http://gogonet.gogo6.com/page/freenet6-account)此處先免費取得帳號，再來使用此連線。TSPC 可連接通道代理人(tunnel broker)並依照設定檔案內的規格來要求一條通道。這個模式可以自通道代理人處取得實際 IPv6 IP 位址以及前置碼，然後在背景處監督整個通道的資料運輸狀況。

在您取得 IPv6 前置碼並開始 RADVD 之後，路由器後方的電腦就可以直接連接到 IPv6 並登上網際網路。

可用設定說明如下：

項目	說明
使用者名稱	輸入您自通道代理人取得的名稱，建議您先進入此網站 http://gogonet.gogo6.com/page/freenet6-account 申請一個使用者名稱以及密碼。
密碼	請輸入搭配使用者名稱所分派的密碼。
通道代理伺服器	輸入通道代理人的的 IP 位址、FQDN 或是選項埠號。
WAN 連線偵測	這個功能讓您檢查目前網路是否還在連線中。 **模式**- 選擇**永遠連線**或 **Ping 偵測**執行 WAN 檢測動作。**永遠連線**表示無需進行任何檢測，網路永遠連線。 ● **Ping IP/主機名稱** – 若您選擇了 **Ping 偵測**作為偵測模式，您必須在本區輸入 IP 位址或主機名稱。 ● **TTL (Time to Live)** – 設定 ping 操作需要的 TTL 數值。

完成上述設定之後，按下**確定**儲存設置內容。

II-1-2-9 WAN1/WAN3 的 AICCU 模式細節設定(IPv6)

可用設定說明如下：

項目	說明
永遠連線	勾選此方塊讓系統隨時保持連線。
使用者名稱	輸入通道代理人提供的名稱，請先自此網站 http://www.sixxs.net/申請使用者名稱與密碼。
密碼	請輸入搭配使用者名稱所分派的密碼。
通道代理伺服器	輸入通道代理人的的 IP 位址、FQDN 或是選項埠號。
通道 ID	一個使用者帳號可以有數個通道，每個通道可擁有一個指定的 ID (例如 T115394)。
子網前置碼	輸入取自服務供應商的子網前置碼。
WAN 連線偵測	這個功能讓您檢查目前網路是否還在連線中。 **模式** – 選擇**永遠連線**或 **Ping 偵測**執行 WAN 檢測動作。**永遠連線**表示無需進行任何檢測，網路永遠連線。 ● **Ping IP/主機名稱** – 若您選擇了 **Ping 偵測**作為偵測模式，您必須在本區輸入 IP 位址或主機名稱。 ● **TTL (Time to Live)** – 設定 ping 操作需要的 TTL 數值。

完成上述設定之後，按下**確定**儲存設置內容。

II-1-2-10 WAN1 的 DHCPv6 用戶端模式細節設定(IPv6)

DHCPv6 用戶端模式可使用 DHCPv6 協定以便自伺服器取得 IPv6 位址。

可用設定說明如下：

項目	說明
DHCPv6 用戶端設定	**IAID** - 輸入號碼做為 IAID。 **DUID** – 顯示此 WAN 介面使用的 DHCP 唯一識別碼(DUID)。 **驗證通訊協定** – 用戶端登入網際網路之前，通過 DHCPv6 伺服器驗證時使用的協定。三種可選-**無**、**重新設定金鑰**與**延遲**。一般預設值為**無**。 ● **重新設定金鑰** – 連線過程中，DHCPv6 伺服器會自動驗證用戶端。 ● **延遲** - 連線過程中，DHCPv6 伺服器會以金鑰 ID 網域與密鑰資訊驗證用戶端。 **金鑰 ID** – 輸入數值 (範圍從 1 到 65535) 用來產生 HMAC-MD5 值。 **領域** – 此處輸入的名稱 (1 到 31 個字元) 用來識別產生 HMAC-MD5 值的金鑰。 **密鑰** – 輸入文字 (1 到 31 個字元) 做為每個 DHCP 伺服器上每個用戶端的身分識別符號。
WAN 連線偵測	這個功能讓您檢查目前網路是否還在連線中。 **模式**- 選擇**永遠連線)**或 **Ping 偵測**或 **NS 偵測**執行 WAN 檢測動作。透過 NS 檢測，系統將檢查網路連線是否已經建立，就像 IPv4 ARP 檢測一般。**永遠連線**表示無需進行任何檢測，網路永遠連線。 ● **Ping IP/主機名稱** – 若您選擇了 **Ping 偵測**作為偵測模式，

	您必須在本區輸入 IP 位址或主機名稱。 ● **TTL (Time to Live)** – 設定 ping 操作需要的 TTL 數值。
RIPng 通訊協定	下一代 RIP(RIPng) 提供與 IPv4 RIP v2 相同的功用。
橋接模式	**啟用橋接模式** – 若啟用此功能，路由器可以當成橋接數據機來運作。 **啟用防火牆** – 啟用橋接模式後，此功能亦可使用。當橋接模式與防火牆皆啟用時，在使用者管理下方的使用者設定檔內的設定將被忽略不計。而防火牆功能單中所定義並啟用的過濾器規則取而代之。 **橋接子網** – 在選定的 LAN 子網與此 WAN 介面之間建立橋接連線。

完成上述設定之後，按下**確定**儲存設置內容。

II-1-2-11 WAN1 的固定 IPv6 模式細節設定(IPv6)

這個類型可以您針對 WAN 介面設定固定的(靜態)IPv6 位址。

可用設定說明如下：

項目	說明
靜態 IPv6 位址設定	**IPv6 位址** - 輸入固定的 IPv6 位址。 **前置碼長度** - 輸入前置號碼長度固定值。 **新增** - 按下此鈕新增位址。 **更新** - 按下此鈕修改既有的設定內容。 **刪除** - 按下此鈕刪除現存的位址。
目前 IPv6 位址表格	顯示目前 IPv6 位址的介面。
靜態 IPv6 閘道設定	**IPv6 閘道設定** - 請在此輸入 IPv6 閘道的位址。
WAN 連線偵測	這個功能讓您檢查目前網路是否還在連線中。

	模式- 選擇**永遠連線**、**NS 偵測**或 **Ping 偵測**執行 WAN 檢測動作。**永遠連線**表示無需進行任何檢測，網路永遠連線。 ● **Ping IP/主機名稱** – 若您選擇了 **Ping 偵測**作為偵測模式，您必須在本區輸入 IP 位址或主機名稱。 ● **TTL (Time to Live)** – 設定 ping 操作需要的 TTL 數值。
橋接模式	**啟用橋接模式** – 若啟用此功能，路由器可以當成橋接數據機來運作。 **啟用防火牆** – 啟用橋接模式後，此功能亦可使用。當橋接模式與防火牆皆啟用時，在使用者管理下方的使用者設定檔內的設定將被忽略不計。而防火牆功能單中所定義並啟用的過濾器規則取而代之。 **橋接子網** – 在選定的 LAN 子網與此 WAN 介面之間建立橋接連線。

完成上述設定之後，按下**確定**儲存設置內容。

II-1-2-12 WAN1 的 6in4 固定通道模式細節設定(IPv6)

此模式可讓您針對 WAN 界面設定 6in4 固定通道模式。

路由器可透過 IPv4 網路登入以 IPv6 為基準的網路頁面。

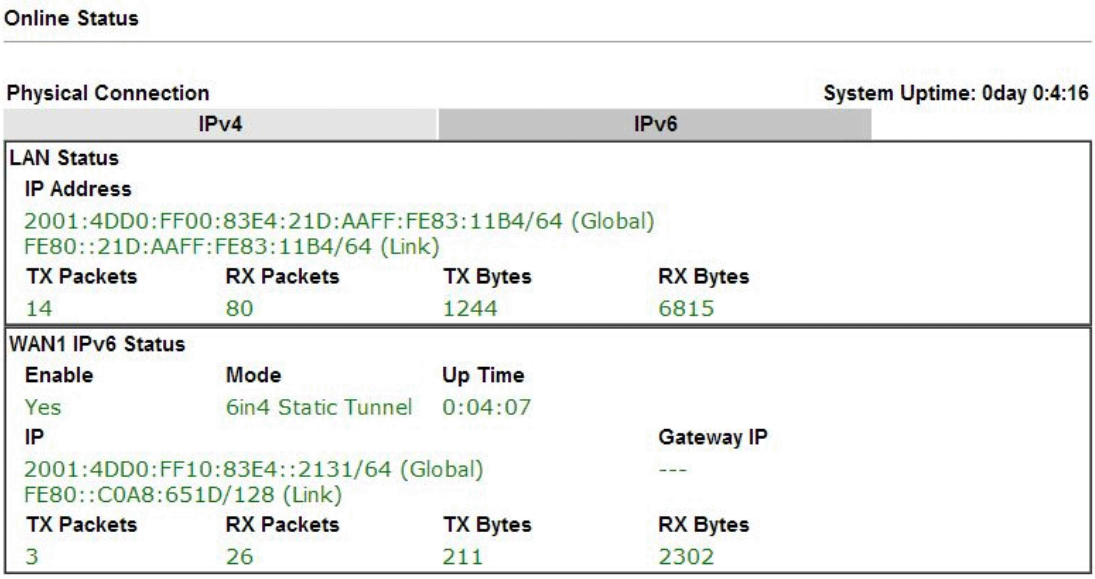
不過，6in4 提供除了 2002::0/16 格式以外的前置代碼，因此您可以使用事先固定的終點.值，不必理會，模式的可靠度也相當高。

可用設定說明如下：

項目	說明
遠端終點 IPv4 位址	輸入遠端伺服器的固定 IPv4 位址。
6in4 IPv6 位址	針對 IPv4 通道輸入含前置代碼長度的固定 IPv6 位址。
LAN 路由前置代碼	針對 LAN 路由輸入含前置代碼長度固定 IPv6 位址。
通道 TTL	輸入通道內資料保存期限。
WAN 連線偵測	這個功能讓您檢查目前網路是否還在連線中。 **模式**– 選擇**永遠連線**或 **Ping 偵測**執行 WAN 檢測動作。**永遠連線**表示無需進行任何檢測，網路永遠連線。 ● **Ping IP/主機名稱** – 若您選擇了 **Ping 偵測**作為偵測模式，您必須在本區輸入 IP 位址或主機名稱。 ● **TTL (Time to Live)** – 設定 ping 操作需要的 TTL 數值。

完成上述設定之後，按下**確定**儲存設置內容。

下圖顯示以此模式為基準，成功設定的 IPv6 連線範例。



II-1-2-13 WAN1 的 6rd 模式細節設定(IPv6)

本頁讓您針對 WAN 界面設定 6rd 模式。.

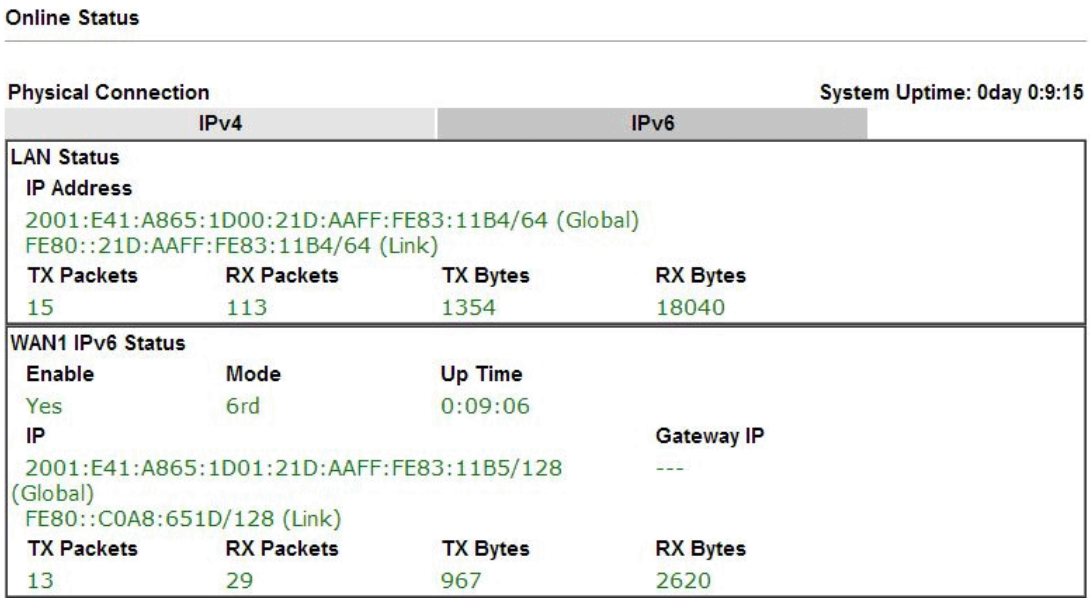
可用設定說明如下：

項目	說明
6rd 模式	**自動 6rd -** 自 6rd 服務供應商自動取回 6rd 前置代碼資料。搭配的 IPv4 WAN 介面必須設定為 DHCP 模式。 **靜態 6rd -** 手動設定 6rd 選項。
IPv4 邊界中繼	選擇**靜態 6rd** 模式之後，針對 6rd 網域提供 IPv4 位址作為 6rd Border 的中繼。
IPv4 遮罩長度	選擇**靜態 6rd** 模式之後，在 6rd 的網域中，輸入所有 CE 的 IPv4 位址需求的遮罩長度值。

6rd 前置代碼	選擇**靜態 6rd** 模式之後，輸入 6rd IPv6 位址。
6rd 前置代碼長度	選擇**靜態 6rd** 模式之後，輸入 6rd IPv6 前置代碼需求的長度數字。
WAN 連線偵測	這個功能讓您檢查目前網路是否還在連線中。 **模式** – 選擇**永遠連線**或 **Ping 偵測**執行 WAN 檢測動作。**永遠連線**表示無需進行任何檢測，網路永遠連線。 ● **Ping IP/主機名稱** – 若您選擇了 **Ping 偵測**作為偵測模式，您必須在本區輸入 IP 位址或主機名稱。 ● **TTL (Time to Live)** – 設定 ping 操作需要的 TTL 數值。

完成上述設定之後，按下**確定**儲存設置內容。

下圖顯示以此模式為基準，成功設定的 IPv6 連線範例。



II-1-3 多重 VLAN

多重 VLAN 可讓用戶針對 WAN 介面建立設定檔與橋接連線，以便用於需要高度網路流量的應用上。

頻道 1 到 3 分別具有固定的用途：

- 頻道 1: WAN1 (乙太網路)
- 頻道 3: USB1 (WAN3)

頻道 4 到**頻道 10** 可橋接至 1 到 3 個以上的 LAN 埠口(P2 至 P5)，此外，**頻道 4** 至**頻道 6** 則可設定為虛擬 WAN 介面(從 WAN4 到 WAN6)。

基本

本頁顯示每個頻道的基本設定值。

可用設定說明如下：

項目	說明
頻道	顯示每個頻道的編號。 頻道 1 專屬於網際網路使用者介面，因此在此處是不可以變更的。 頻道 4 ~ 10 是可以設定調整的。
啟用	顯示此頻道的設定是啟用(是)還是停用(否)。
WAN 類型	顯示頻道使用的實體介面類型。
VLAN 標籤	顯示用於此頻道封包傳輸攜帶的 VLAN 標籤值。

埠號式橋接	系統可透過個別 VLAN 標籤值來辨識每個頻道網路流量，不同頻道即使利用相同 WAN 介面，也不可採用相同的 VLAN 標籤值。 **啟用** - 勾選此方塊以便啟用該頻道的埠號橋接功能。 **P1 ~ P4** – 選需要的埠號以便建立區域網路端的橋接連線。

預設定一個 PVC 頻道，請按下頻道號碼連結。

頻道 4~6 的 WAN 連結主要用於路由器的應用，例如 **TR-069**。這邊的設定值必須取自 ISP 業者，且只能套用在該 ISP 業者。如果有特殊需要，請與您的 ISP 業者聯絡，然後再至此設定此三個頻道。

可用設定說明如下：

項目	說明
啟用頻道 4/5/6	勾選此框啟用此頻道。
基本設定	**VLAN 標籤-** 輸入 VLAN ID 號碼，可設定範圍自 1 到 4095，系統可透過 VLAN 標籤來辨識每個頻道，使用相同 WAN 類型的頻道不可設定相同的 VLAN 標籤值。

	優先權- 選擇一個號碼來決定此 VLAN 封包的優先權為何，可設定範圍自 0 到 7。
針對此頻道開啟埠號式橋接連線	此處設定將會在 LAN 埠口間與 WAN 口建立橋接連線，橋接連線建立在選定的 WAN 介面並使用 VLAN 標籤值。 **實體成員 -** 勾選您想要群組的埠號，使其套用橋接模式連線。 請注意，LAN 埠口 1 保留作為 NAT 轉址之用，不可以選其做為橋接介面。
針對此頻道開啟 WAN 介面	勾選選框啟用相關功能。 **WAN 應用 -** ● **管理**可指定為一般管理之用(網頁設定/telnet/TR069)，如果您選擇此項，此 VLAN 設定將僅對網頁設定/telnet/TR069 產生作用。 ● **IPTV** - 允許 WAN 介面傳送 IGMP 封包到 IPTV 伺服器。 **WAN 設定** – 選擇 PPPoE/PPPoA 或是靜態固定或動態 IP 設定，以便決定哪個 WAN 介面需要設定。
ISP 存取設定	依照 ISP 提供的資訊，輸入使用者名稱、密碼與驗證參數。 **ISP 名稱** – 指明 PPP 服務名稱，若您的 ISP 需要此設定值，請輸入名稱，否則此區可留空白。 **使用者名稱** –ISP 提供 PPPoE/PPPoA 驗證的名稱，最大長度為 62 個字元。 **密碼** –ISP 提供 PPPoE/PPPoA 驗證的密碼，最大長度為 62 個字元。 **PPP 驗證** – 指定 PPP 驗證需求的通訊協定。 ● **限用 PAP** - 僅能使用 PAP (Password Authentication Protocol)。 ● **PAP 或 CHAP** - PAP 與 CHAP (Challenge-Handshake Authentication Protocol)二種協定皆可用於 PPP 驗證。路由器與PPTP或是L2TP伺服器協商以決定要使用哪種協定。 **永遠連線** – 勾選此項後，路由器將維持 PPPoE/PPPoA 連線且不斷線。 **閒置逾時** – 指定連線斷線之前等待的時間(沒有流量)長度，單位為秒。 **來自 ISP 的 IP 位址** – 指定頻道之 WAN IP 位址的設定方式。 ● **固定 IP** **是**– 在固定 IP 位址欄位中輸入的 IP 位址將做為虛擬 WAN 的 IP 位址。 **否** – 虛擬 WAN IP 位址由 ISP 的 PPPoE/PPPoA 伺服器來分派。
WAN IP 網路設定	**自動取得 IP 位址** – 按此鈕以自動取得 IP 位址。 ● **路由器名稱** – 設定 DHCP Option 12 的名稱，某些 ISP 需要此設定內容。 ● **網域名稱** – 設定 DHCP Option 15 的名稱，某些 ISP 需要此設定內容。 **指定 IP 位址** – 按此鈕以指定 IP 位址。 ● **IP 位址** – 輸入 IP 位址。 ● **子網遮罩**– 輸入子網路遮罩。

	● **閘道 IP 位址** – 輸入閘道 IP 位址。 **DNS 伺服器 IP 位址** - 如果要使用固定 IP 模式，請在此輸入路由器的主要 IP 位址；如有必要，亦可輸入次要 IP 位址以備將來之需。

在您完成上述的設定之後，請按**確定**按鈕回到上一頁。

按下索引編號(7~10)可以看到如下頁面：

可用設定說明如下：

項目	說明
啟用頻道 7~10	勾選此框啟用此頻道。
基本設定	**VLAN 標籤** - 輸入 VLAN ID 號碼，可設定範圍自 1 到 4095，系統可透過 VLAN 標籤來辨識每個頻道，使用相同 WAN 類型的頻道不可設定相同的 VLAN 標籤值。 **優先權** - 選擇一個號碼來決定此 VLAN 封包的優先權為何，可設定範圍自 0 到 7。
橋接模式	**啟用** - 選擇此項啟用此頻道設定的橋接模式。 **實體成員** - 勾選您想要群組的埠號，使其套用橋接模式連線。 請注意，LAN 埠口 1 保留作為 NAT 轉址之用，不可以選其做為橋接介面。

完成上述設定之後，按下**確定**儲存設置內容。

II-1-4 廣域網路連線額度

本功能可用來分別測定每個 WAN 介面的資料流量，避免自 ISP 收到過多的數據傳輸。請注意額度限制與每月的 Billing cycle day 皆應設定正確，才能正確執行相關的計算。

II-1-4-1 基本設定

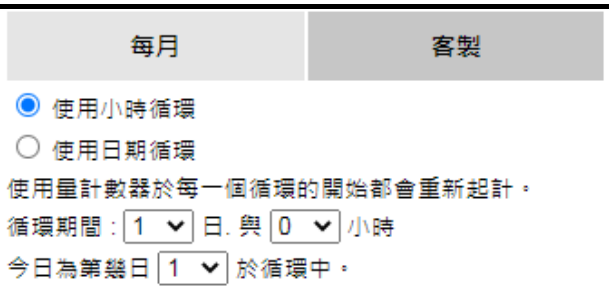
可用設定說明如下：

項目	說明
索引	代表 WAN 埠口。 按編號設定 WAN 計量。
啟用	選擇方框啟用此 WAN 介面的 WAN 計量收費功能。
額度	目前網際網路周期用量已 x/y 來表示，其中 x 為累計用量而 y 為上限值。例如 100MB/200MB 表示循環值是 100MB 上限值為 200MB。
當超過額度時	一旦達到額度值時，系統會採取的行動。 **關閉** – WAN 介面停用。 **郵件警示** – 警示郵件將會寄給管理者。
時間循環	顯示重置資料用量的頻率。
持續時間	顯示目前周期的開始與結束時間。

按下 WAN# 連結以便開啟如下頁面。

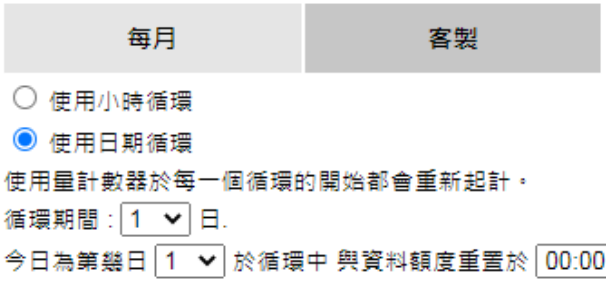
可用設定說明如下：

項目	說明
啟用	勾選此框啟用此功能。
額度限制	請輸入此 WAN 介面最大的網路流量限制(單位是百萬位元或是 GB)。
當超過額度時	當超過額度限制時，系統可以依據選擇的方式來執行流量傳送。 **關閉 WAN 介面**- 所有透過此 WAN 介面的對外流量都將中止。 ● **使用通知物件** – 系統將依照通知物件的內容發送通知訊息。 ● **設定郵件警示** – 當額度快要用完時，系統將發送警告訊息予管理者，不過連線費用仍然持續計算。 ● **設定簡訊訊息** – 當額度快要用完時，系統將發送警告訊息予管理者。
每月	某些 ISP 業者可能想以每月流量限制來運用網路限制，這項設定可提供每月重新設定流量紀錄的機制以供 ISP 運用。 每月 客製 請選擇每月(格狀系統)數據重設的日期 資料額度每隔數日重置 1 於 00:00 **資料額度每隔數日重置** – 結算週期大約是一個月，您可以決定一個月當中的某日某時作為結算週期的起始日。
客製	此設定可讓 ISP 業者依照實際的需要定義所需的結算週期。 WAN 計量收費可以經過一個週期間隔之後重新起算。 預設值是每個月，如果您需要一個更長或是更短的週期，請改設定**使用者定義**，結算週期介於 1 到 60 天，您可以指定日數與時數來決定週期的長短，此外您也可以指定目前週期內的天數為幾天。 **使用小時循環** –



- **循環期間** – 指定重設流量紀錄的期間(日、時)。例如數字 7 表示整個週期有 7 天；20 就表示有 20 天。當時間已到，路由器就會自動重置流量紀錄。
- **今日為第幾日** – 指定循環期間中哪一天作為結算的起始日，例如數字 3 就表示整個循環期間的第 3 日為起始日。

使用日期循環 -

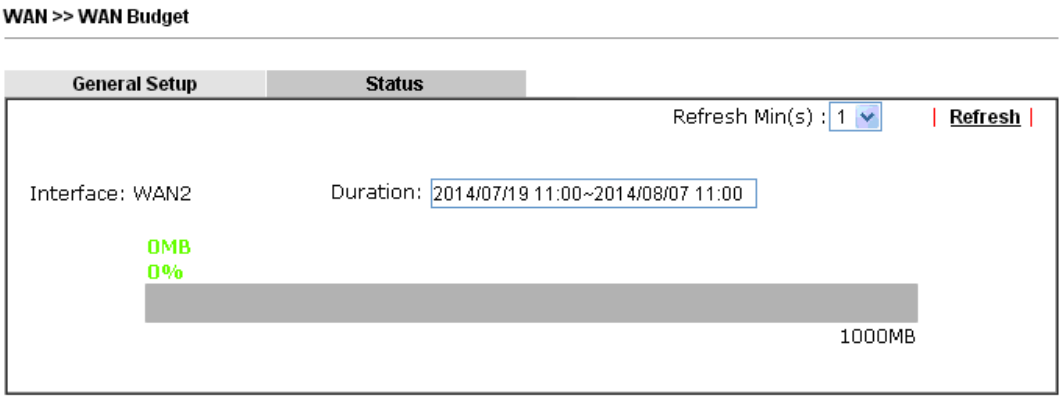


- **循環期間** – 指定重設流量紀錄的期間(日)。例如數字 7 表示整個週期有 7 天；20 就表示有 20 天。當時間已到，路由器就會自動重置流量紀錄。
- **今日為第幾日** – 指定結算週期內中的哪一天作為結算的起始日，例如數字 3 就表示整個結算週期的第 3 日為起始日。

完成上述設定之後，按下**確定**儲存設置內容。

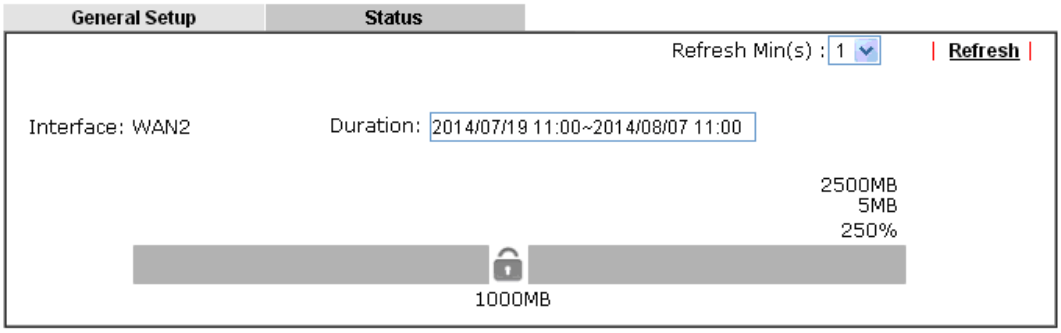
II-1-4-2 狀態

狀態頁面顯示 WAN 計量收費的目前狀態，包含持續時間與用量。



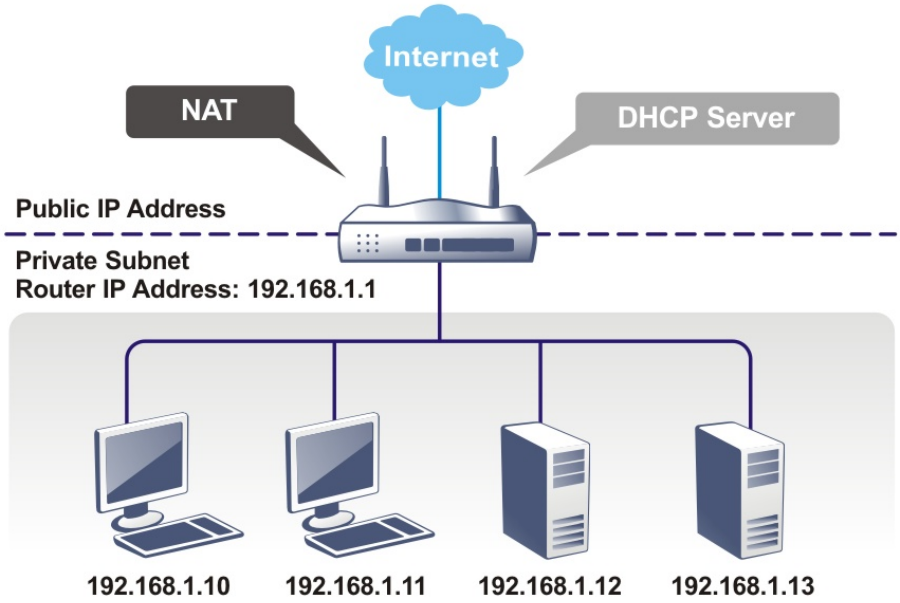
若 WAN 計量已耗盡且**關閉 WAN 介面**功能也被啟動，本頁會呈現一把鎖來表示，代表系統不會再處理任何資料傳輸。此外，若有指定郵件警示功能設定檔，系統也會發出警告訊息給予管理者；若有指定簡訊功能設定檔，則系統會傳送簡訊給予管理者。

WAN >> WAN Budget

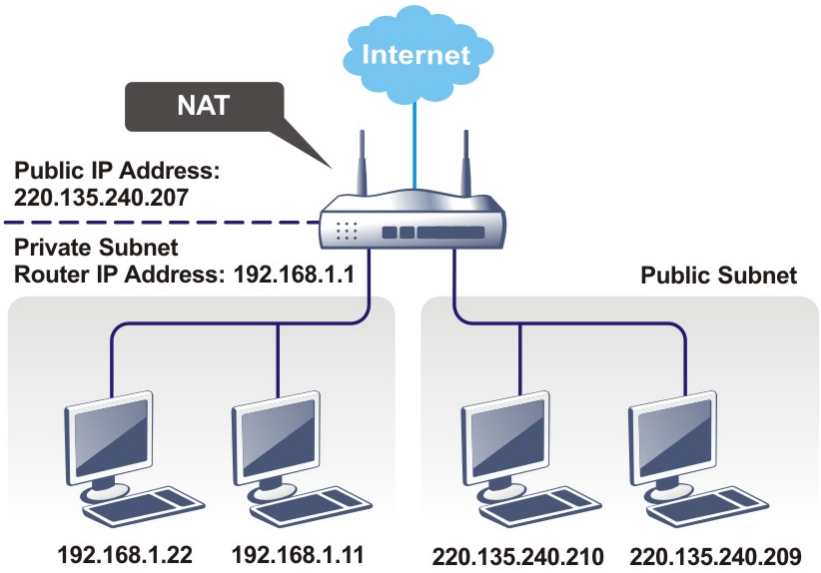


II-2 LAN

Vigor 路由器最基本的功能為 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，請參考下麵的範例圖，即可獲得大略的瞭解。



在某些特殊的情形當中，您可能會有 ISP 提供給您的真實 IP 子網路像是 220.135.240.0/24，這表示您可以設定一個真實子網路，或是使用配備有真實 IP位址之主機的第二組子網路，作為真實子網路的一部份，Vigor 路由器將會提供 IP 路由服務，幫助真實地區子網路上的主機能與其他真實主機/外部伺服器溝通連繫，因此路由器必須設定為真實主機的通訊閘道才行。



什麼是 RIP(Routing Information Protocol)

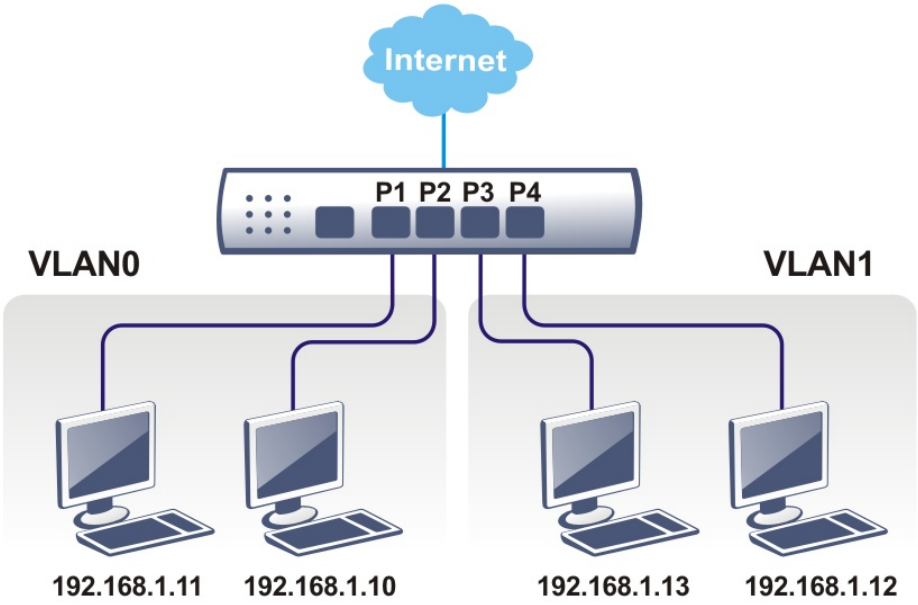
Vigor 路由器可利用 RIP 與鄰近路由器交換路由資訊，達到 IP 路由的目的。這樣可讓使用者變更路由器的資訊，例如 IP 地址，且路由器還會自動通知雙方此類訊息。

什麼是固定路由

當您的區域網路上有數個子網路時，比起其他的方法有時候對連線來說最有效也是最快速的方式就是固定路由功能，您可設定一些規則來傳送指定子網路上的資料到另一個指定的子網路上而不需要透過 RIP。

什麼是虛擬區域網路(VLAN)

您可以利用實體的連接埠將群組區域網路上的主機，然後建立虛擬區域網路，最多可達 4 個。為了要管理不同群組間的通訊狀況，請再虛擬區域網路功能上設定一些規則，以及每個網路的傳送速率。

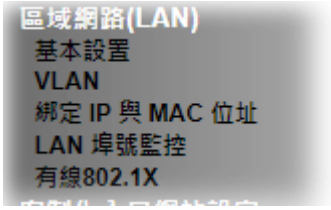


網頁使用者介面

區域網路(LAN)是由一群 LAN 用戶端亦即所在位置所有的網路裝置組合而成，LAN 用戶端可以是電腦、印表機、VoIP 電話、行動電話、遊戲機、IPTV 等等，可透過有線(使用乙太網路纜線)或是無線(使用 Wi-Fi)網路連線。

在相同區域網路下的用戶端一般可以直接與另一個設備溝通，只要他們是彼此的另一端即可。除非是透過某些方法如防火牆或是 VLAN 等功能限制了彼此的存取，例如，從 Windows XP 開始的微軟系統與 Apple OS X 系統都有內建的防火牆可以設定限制進出資料流量，另一方面，使用網路交換器或是路由器(例如本 Vigor 路由器)設定 VLAN 功能。

為了能跟區域網路外部的主機溝通，區域網路用戶端必須通過網路閘道，在大部分的例子中，此閘道多半是位於區域網路與 ISP 網路(指的是 WAN 廣域網路)之間的路由器。路由器就像是一個指引器，可確保區域網路(LAN)與廣域網路(WAN)之間的流量達到預期的目的地。



II-2-1 基本設置

本頁提供您區域網路的基本設定。按**區域網路(LAN)**開啟區域網路設定並選擇**基本設置**。

路由器提供數個子網，讓使用者來區隔，此外，不同子網可透過 Inter-LAN 路由讓彼此互通。目前 LAN1 設定固定為 NAT 模式專用，LAN2 至 LAN4 可用於 NAT 或是路由模式。IP 路由子網則可於路由模式下操作。

可用設定說明如下：

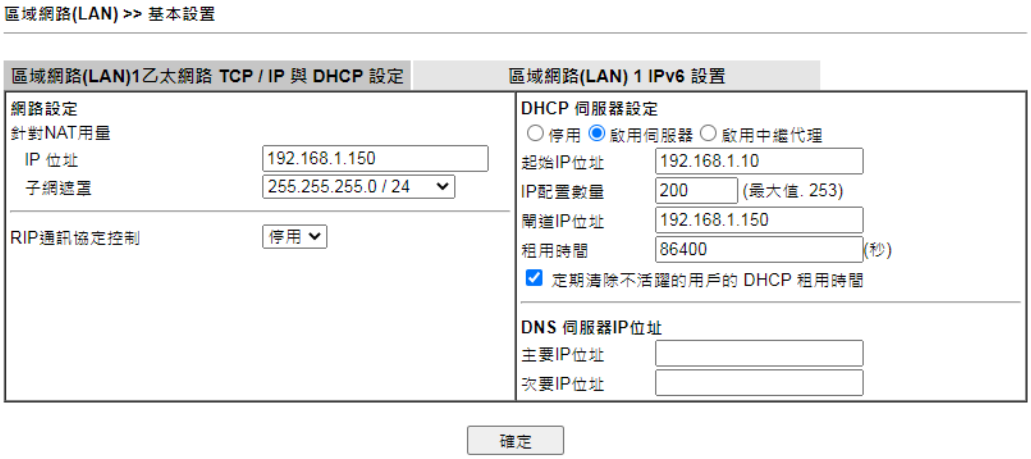
項目	說明
基本設置	允許針對個別子網設定不同內容。 **索引-** 顯示全部的 LAN 項目。 **啟用 -** 基本上 LAN1 狀態於預設時是啟用的，LAN2 之後與 IP 路由子網只有在**啟用**欄位已勾選時，始可查閱。 **DHCP/DHCPv6-** 預設狀態下，LAN1 設定為 DHCP/DHCPv6 模式，如果有必要，請針對每個 LAN 勾選此方塊。 **IP 位址 -** 顯示每個 LAN 的 IP 位址。 **細節頁面-** 按下此鈕可進入設定頁面，每條 LAN 都可以有不同的設定內容，也勾可以設定在不同的子網下。 **IPv6 -** 按下此鈕進入 IPv6 設定頁面。
DHCP 伺服器選項	DHCP 封包可以藉由新增 option 號碼以及資料資訊來處理。 詳情請參考後續章節說明。
強迫路由器使用...	強迫路由器使用 LAN1 / LAN2 / LAN3 / LAN4 中設定的 DNS 伺服器而非網際網路存取伺服器((PPPoE, PPTP, L2TP 或 DHCP 伺服器)指定的 DNS 伺服器。
LAN 與 LAN 間之路由	勾選方塊來連結二個或是多個不同的子網(LAN 與 LAN 間)。 這個功能允許不同的 LAN 子網彼此之間相連或是隔離。這個功能僅在 VLAN 功能已被啟用時可用。 在 **LAN 與 LAN 間之路由**表格中，選定的核取方框表示這二個互相交叉之區域網路可以彼此溝通。

當您完成上述設定之後，請按下**確定**儲存。

資訊	如欲設定子網，請選擇細節設定頁面，開啟設定頁面。

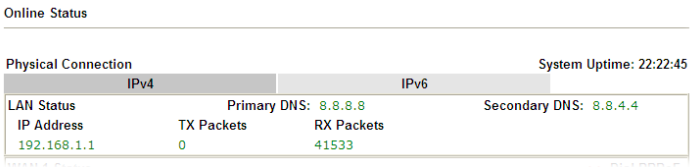
II-2-1-1 LAN1–乙太網路 TCP/IP 與 DHCP 設定之細節設定

LAN1 中有二種設定頁面，一個是乙太網路 TCP/IP 與 DHCP 設定(以 IPv4 為基準)，另一個是 IPv6 設定。按下每個類型的標籤，並參考下述說明：



可用設定說明如下：

項目	說明
網路設定	**針對 NAT 用量,** **IP 位址-** 請輸入虛擬 IP 位址以便連接區域虛擬網路(預設值為 192.168.1.1)。 **子網遮罩-** 請輸入決定網路大小的位址代碼(預設值為 255.255.255.0/ 24)。 **RIP 通訊協定控制,** **停用 -** 關閉 RIP 協定，可讓不同路由器之間資訊交換暫停 (此為預設值)。 **啟用 -** 啟動此協定。
DHCP 伺服器設定	DHCP 是 Dynamic Host Configuration Protocol 的縮寫，路由器的出廠預設值可以作為您的網路的 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，將該使用者設定成為 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。 如果您想要使用網路上另外的 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。 **停用-** 讓您手動指定 IP 地址到區域網路上的每個主機上。 **啟用伺服器-** 讓路由器指定 IP 地址到區域網路上的每個主機上。 ● **起始 IP 位址 -** 輸入 DHCP 伺服器的 IP 位址配置的數值作為指定 IP 位址的起始點。 ● **IP 配置數量 -** 輸入您想要 DHCP 伺服器指定 IP 地址的最大數量，預設值為 200，最大值為 1021。

	● **閘道 IP 位址** -輸入 DHCP 伺服器所需的閘道 IP 位址，這項數值通常與路由器的第一組 IP 位址相同，表示路由器為預設的閘道。 ● **租用時間**- 輸入 DHCP 伺服器可以使用來分派 IP 位址的時間長度。 ● **定期清除不活躍的用戶的 DHCP 租用時間** - 選擇此項後，路由器將發送 ARP 請求，以便回收早先分配給未活動 DHCP 客戶端的 IP 位址，防止 IP 位置耗竭殆盡。 **注意**: 當啟用此功能時，路由器將會執行如下作業： ■ 當可用的 DHCP IP 配置數量低於 30 個的時候，透過每分鐘 ARP 請求，檢查 DHCP 用戶的活動狀況 ■ 當用戶端不回應 ARP 請求時，清除 DHCP 分派位址 **啟用中繼代理**- 選擇此項後，所有的 DHCP 請求都會被轉發至 LAN 子網外的 DHCP 伺服器上，需求的 IP 位址就從 DHCP 伺服器 IP 位址欄位中指定。 ● **第一個/第二個 DHCP 伺服器 IP 位址**- 當您勾選了**啟用中繼代理**之後，即可見到此項目，設定您準備使用的伺服器 IP 位址讓中繼代理幫忙轉送 DHCP 需求至 DHCP 伺服器上。
DNS 伺服器設定	DNS 是 Domain Name System 的縮寫，每個網際網路的主機都必須擁有獨特的 IP 位址，也必須有人性化且容易記住的名稱諸如 www.yahoo.com 一般，DNS 伺服器可轉換此名稱至相對應的 IP 地址上。 **主要 IP 位址** -您必須在此指定 DNS 伺服器的 IP 位址，因為通常您的 ISP 應該會提供一個以上的 DNS 伺服器，如果您的 ISP 並未提供，路由器會自動採用預設的 DNS 伺服器 IP 地址 194.109.6.66，放在此區域。 **次要 IP 位址**- 您可以在此指定第二組 DNS 伺服器 IP 位址，因為 ISP 業者會提供一個以上的 DNS 伺服器。如果您的 ISP 並未提供，路由器會自動採用預設的第二組 DNS 伺服器，其 IP 位址為 194.98.0.1，放在此區域。 預設 DNS 伺服器 IP 位址可在線上狀態上查看:  如果主要和次要 IP 地址區都是空白的，路由器將會指定其本身的 IP 位址給予本地使用者作為 DNS 代理伺服器並且仍保有 DNS 快速緩衝貯存區。 如果網域名稱的 IP 位址已經在 DNS 快速緩衝貯存區內，路由器將立即解析網域名稱。否則路由器會藉著建立 WAN (例如 DSL/Cable)連線時，傳送 DNS 疑問封包至外部 DNS 伺服器。

當您完成上述設定之後，請按下**確定**儲存。

系統可以透過 DHCP 自動分派虛擬 IP 位址給 LAN 端的用戶或是手動輸入給予。向 DHCP 客戶端分派 IP 位址的 DHCP 伺服器可以是路由器(最常見的例子)或是另一個伺服器。

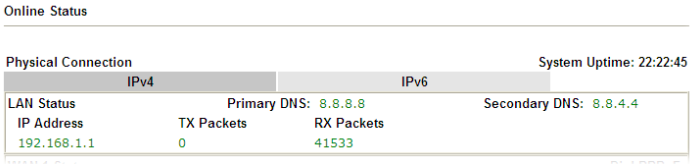
或者，可以手動輸入固定 IP 予 LAN 用戶，無論如何設定 IP 位址，沒有二個裝置會設定成相同的 IP 位址。若要在網路中同時使用 DHCP 與固定 IP 位址，請自 DHCP IP 配置中排除該固定 IP。例如，您的 LAN 使用 192.168.1.x 網段而您有 20 個 DHCP 用戶端以及 20 個固定 IP 用戶，您可以

將 192.168.1.10 設定成起始 IP 位址，IP 配置數量設定為 50，使用大於 192.168.1.100 的位址作為固定 IP 分派用。

II-2-1-2 LAN2 ~ LAN4 之細節設定

可用設定說明如下：

項目	說明
網路設定	**啟用/停用** - 選擇**啟用**來啟動此設定，按下**停用**則關閉此設定。 **針對 NAT 用量** - 選擇此鈕讓設定資料供 NAT 使用。 **針對路由用量** - 選擇此鈕讓設定資料套用於路由。 **IP 位**- 請輸入虛擬 IP 位址以便連接區域虛擬網路(預設值為 192.168.1.1)。 **子網遮罩** - 請輸入決定網路大小的位址代碼(預設值為 255.255.255.0/ 24)。
DHCP 伺服器設定	**停用** - 讓您手動指定 IP 地址到區域網路上的每個主機上。 **啟用伺服器** - 讓路由器指定 IP 地址到區域網路上的每個主機上。 ● **起始 IP 位址** - 輸入 DHCP 伺服器的 IP 位址配置的數值作為指定 IP 位址的起始點。 ● **IP 配置數量** - 輸入您想要 DHCP 伺服器指定 IP 地址的最大數量，預設值為 100，最大值為 1021。 ● **閘道 IP 位址** - 輸入 DHCP 伺服器所需的閘道 IP 位址，這項數值通常與路由器的第一組 IP 位址相同，表示路由器為預設的閘道。 ● **租用時間** - 輸入 DHCP 伺服器可以使用來分派 IP 位址的時間長度。 ● **定期清除不活躍的用戶的 DHCP 租用時間** - 選擇此項後，路由器將發送 ARP 請求，以便回收早先分配給未活動 DHCP 客戶端的 IP 位址，防止 IP 位置耗竭殆盡。 **注意**: 當啟用此功能時，路由器將會執行如下作業： ■ 當可用的 DHCP IP 配置數量低於 30 個的時候，透過每分鐘 ARP 請求，檢查 DHCP 用戶的活動狀況 ■ 當用戶端不回應 ARP 請求時，清除 DHCP 分派位址

	啟動中繼代理 – 選擇此項後，所有的 DHCP 請求都會被轉發至 LAN 子網外的 DHCP 伺服器上，需求的 IP 位址就從 DHCP 伺服器 IP 位址欄位中指定。 ● **第一個/第二個 DHCP 伺服器 IP 位址** – 當您勾選了**啟動中繼代理**之後，即可見到此項目，設定您準備使用的伺服器 IP 位址讓中繼代理幫忙轉送 DHCP 需求至 DHCP 伺服器上。
DNS 伺服器 IP 位址	DNS 是 Domain Name System 的縮寫，每個網際網路的主機都必須擁有獨特的 IP 位址，也必須有人性化且容易記住的名稱諸如 www.yahoo.com 一般，DNS 伺服器可轉換此名稱至相對應的 IP 地址上。 **主要 IP 位址** - 您必須在此指定 DNS 伺服器的 IP 位址，因為通常您的 ISP 應該會提供一個以上的 DNS 伺服器，如果您的 ISP 並未提供，路由器會自動採用預設的 DNS 伺服器 IP 地址 194.109.6.66，放在此區域。 **次要 IP 位址** - 您可以在此指定第二組 DNS 伺服器 IP 位址，因為 ISP 業者會提供一個以上的 DNS 伺服器。如果您的 ISP 並未提供，路由器會自動採用預設的第二組 DNS 伺服器，其 IP 位址為 194.98.0.1，放在此區域。 預設 DNS 伺服器 IP 位址可在線上狀態上查看:  如果主要和次要 IP 地址區都是空白的，路由器將會指定其本身的 IP 位址給予本地使用者作為 DNS 代理伺服器並且仍保有 DNS 快速緩衝貯存區。 如果網域名稱的 IP 位址已經在 DNS 快速緩衝貯存區內，路由器將立即解析網域名稱。否則路由器會藉著建立 WAN (例如 DSL/Cable)連線時，傳送 DNS 疑問封包至外部 DNS 伺服器。

當您完成上述設定之後，請按下**確定**儲存。

II-2-1-3 IP 路由子網之細節設定

可用設定說明如下：

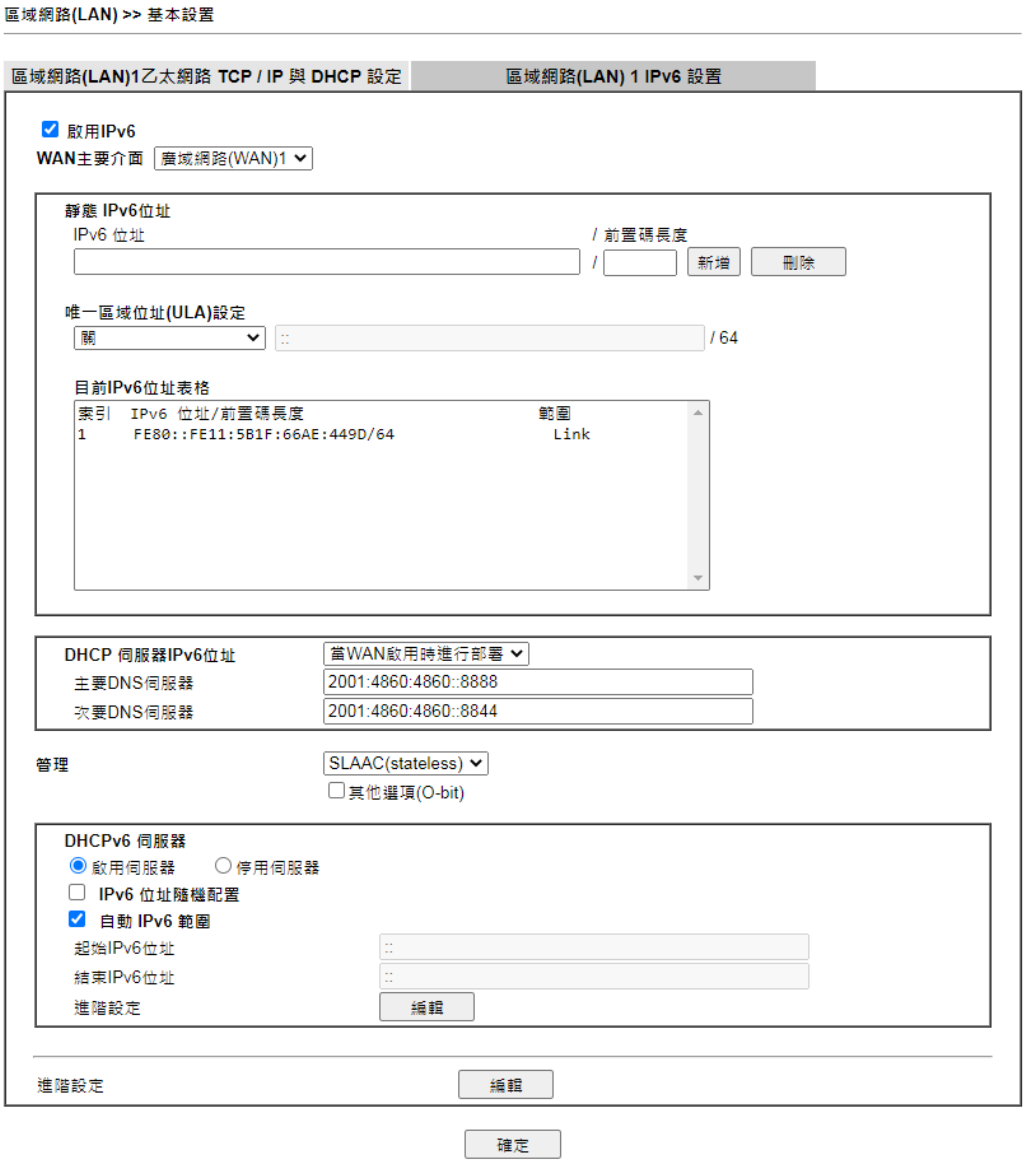
項目	說明
網路設定	**啟用/停用** - 選擇**啟用**來啟動此設定，按下**停用**則關閉此設定。 **針對路由用途,** **IP 位址** - 請輸入虛擬 IP 位址以便連接區域虛擬網路(預設值為 192.168.1.1)。 **子網遮罩** - 請輸入決定網路大小的位址代碼(預設值為 255.255.255.0/ 24)。 **RIP 協定控制,** **停用** - 關閉 RIP 協定，可讓不同路由器之間資訊交換暫停 (此為預設值)。 **啟用** - 啟動此協定。路由器將會嘗試以相鄰路由器透過 RIP 協定進行路由資訊交換。
DHCP 伺服器設定	DHCP 是 Dynamic Host Configuration Protocol 的縮寫，路由器的出廠預設值可以作為您的網路的 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，將該使用者設定成為 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。 如果您想要使用網路上另外的 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。 **起始 IP 位址** - 輸入 DHCP 伺服器的 IP 位址配置的數值作為指定 IP 位址的起始點。 **IP 配置數量** - 輸入您想要 DHCP 伺服器指定 IP 地址的最大數量。

	租用時間 - 輸入 DHCP 伺服器可以使用來分派 IP 位址的時間長度。 **使用 LAN 埠口 -** 指定一個 IP 位址供 IP 路由子網使用，如果啟用此埠，DHCP 伺服器將會自動指派一個 IP 位址給予 P1 與/或 P2 的用戶。請勾選準備使用的 LAN 埠口(P1 與/或 P2)。 **使用 MAC 位址** - 勾選此方框可指定 MAC 位址。 ● **MAC 位址** - 輸入輸入主機的 MAC 位址然後按下方的**新增**按鈕，建立伺服器分派位址的主機清單，也可以刪除或編輯清單內容。設定一群 MAC 位址以因應第二個 DHCP 伺服器使用可以幫助路由器分派給主機正確網段，正確的 IP 位址。如此一來再第二個網段下的主機就不會從第一個網段中取得任何 IP 位址。 **新增 -** 在上方 MAC 位址框中輸入位址內容，按下此鈕之後即可新增。 **刪除** – 刪除上方選定的 MAC 位址。 **編輯** – 編輯上方選定的 MAC 位址。 **取消** – 取消新增、編輯以及刪除等運作。

當您完成上述設定之後，請按下**確定**儲存。

II-2-1-4 LAN IPv6 設定之細節設定

LAN1~LAN8/DMZ 埠口有二種設定頁面，一個是乙太網路 TCP/IP 與 DHCP 設定頁面(基於 IPv4)，另一個是 IPv6 設定頁面。按下每種類型的標籤並參考本節如下的說明。下圖為 IPv6 設定頁面。



可用設定說明如下：

項目	說明
啟用 IPv6	勾選此框啟用 LAN 1 IPv6 設定。
WAN 主要介面	使用下拉式清單指定一個 WAN 介面。
靜態(固定)IPv6 位址設定	**IPv6 位址** – 輸入固定 IPv6 位址。 **前置碼長度** - 輸入一個固定值作為前置碼長度。 **新增** - 按此新增一條新的位址。 **刪除** - 按此移除現有的位址。
唯一區域位址(ULA)設定	ULA 是分派給 LAN 用戶端的虛擬 IPv6 位址。 **關閉** - 停用 ULA。 **手動輸入 ULA 前置碼** - LAN 用戶端取得之 ULA 將依照手動輸入的前置碼產生。 **自動取得 ULA 前置碼**- LAN 用戶端取得之 ULA 將依照系統自動決定的前置碼產生。
目前 IPv6 位址表格	顯示目前使用的 IPv6 位址。

DNS 伺服器 IPv6 位址	**當 WAN 啟用時進行佈署 –** 含 DNS 伺服器資訊的 RA (router advertisement) 封包僅在任何一個 WAN 介面連上網路時傳送至 LAN PC。 **啟用** – 含 DNS 伺服器資訊的 RA (router advertisement) 封包將傳送至 LAN PC，不論 WAN 有無連線。 ● **主要 DNS 伺服器** – 輸入主要 DNS 伺服器的 IPv6 位址。 ● **次要 DNS 伺服器** – 輸入次要 DNS 伺服器的 IPv6 位址。 **停用** – 不再使用 DNS 伺服器。
管理	設定在路由廣播下的 Managed Address Configuration flag (M-bit) 。 ● **關閉**- 無任何設定資訊會透過 RA 傳送出去。 ● **SLAAC(stateless) -** M-bit 未設定。 ● **DHCPv6(stateful)** - M-bit 已設定，表示 LAN 用戶端應該自 DHCPv6 伺服器獲得所有的 IPv6 設定資訊。DHCPv6 伺服器可以是路由器內建伺服器或是另外的 DHCPv6 伺服器。 **其他選項(O-bit)** – 勾選此框啟用 O-bit 以便從 DHCPv6 獲取額外的資訊(例如 DNS)。 選定此項時，其他設定旗標已設定完畢，表示除了 LAN IPv6 位址外的 IPv6 設定資訊皆可從 DHCPv6 伺服器取得。 設定 M-bit (參考上方的**管理**)亦有同樣的效果，如同 O-bit 的 DHCPv6 提供所有的 IPv6 設定資訊。
DHCPv6 伺服器	**啟用伺服器**- 啟動 DHCPv6 伺服器，DHCPv6 伺服器可以依照起始/結束 IP 位址設定來分派 IPv6 位址至電腦上。 **停用伺服器**- 停用 DHCPv6 伺服器的運作。 **自動 IPv6 範圍-** 勾選此框後，路由器將會自動指定 IPv6 範圍以分派位址。 **起始 IPv6 位址 / 結束 IPv6 位址**- 分別輸入起始以及結束的 IP 位址。 **進階設定**- 按下**編輯**按鈕以便設定 DHCPv6 伺服器進階的內容。
進階設定	進階設定頁面具有額外的路由器廣播功能設定，並可啟用多重 WAN 介面供 IPv6 流量使用。

路由器廣播設定- 按下**啟用**以使用路由器廣播伺服器。當某個節點提出需求傳送路由器蒐集(Router Solicitation)訊息時，路由器廣播伺服器將定期傳送 RFC 2461 所指定的路由器廣播訊息至本機乙太網路 LAN 上。IPv6 stateless 自動配置需要這些訊息。

停用- 按此停用路由器的 RA 伺服器。

躍點限制- 使用 IPv6 時，需要輸入此數值予位於路由器後方的裝置使用。

最小/最大間隔時間- 定義傳送 RA 封包的間隔(最小時間與最大時間二者之間)。

預設有效時間- 在此期間，路由器可被視之為預設的閘道器。

預設喜好設定 - 當 RA 封包傳送時，決定路由器後方主機的優先權。

MTU - 封包的最大傳輸單位，若選擇**自動**，路由器將自行決定 LAN 端的 MTU 數值。

RIPng 通訊協定-下一代 RIP(RIPng) 提供與 IPv4 RIP v2 相同的功用。

延伸 WAN - 除了在 LAN IPv6 設定頁面中於 WAN 主要介面，指定處理 IPv6 流量之預設 WAN 外，可以在延伸 WAN 處選擇其他的 WAN 介面來處理 IPv6 流量。

可用 WAN- 其他可用但目前尚未被選定做為處理 IPv6 流量的 WAN 介面。

選定的 WAN- 用來處理 IPv6 流量的 WAN 介面。

完成進階頁面的設定變更之後，按**確定**按鈕儲存變更並回到 LAN IPv6 設定頁面。

II-2-1-5 進階 DHCP 選項設定

按下 LAN 基本設定中的 **DHCP 伺服器選項**按鈕可以設定 DHCP options。

可用設定說明如下：

項目	說明
客製化清單	顯示系統設定的所有 DHCP 選項設定。
啟用	勾選此項啟用此頁設定。
介面	指定套用此設定的 LAN 介面。
下一個伺服器 P 位址/SIAddr	覆蓋 DHCP 伺服器所提供的 DHCP 下一個伺服器 IP 位址(DHCP Option 66)。
選項號碼	DHCP 選項號碼(例如 100)。
資料類型	資料欄位中的資料類型。 **ASCII 字元** – 文字字串，範例: /path。 **十六進位數字** - 十六進位的字串，有效字元從 0 到 9，從 a 到 f，範例: 2f70617468。 **位址清單** - 一個或多個 IPv4 位址，用逗號分隔。
資料	此 DHCP 選項的資料內容。

欲重頭開始新增 DHCP option，請先按下**重置**按鈕清除資料欄位內所有的資訊，之後填入需求資訊(如啟用、介面、選項號碼、資料類型與資料內容等等)再按下**新增**，即可增加新的內容。

如要修改現有 DHCP 選項條目，請在**客製化清單**中按該條目，資料欄位將會以目前的數值顯示出來，完成必要的變更之後，按下**更新**儲存。

如要刪除某個 DHCP 選項條目，請在**客製化清單**中按該條目，然後按下**刪除**即可。

II-2-2 VLAN(虛擬區域網路)

虛擬區域網路(VLAN)讓您細分區域網路以便管理或是改善網路的安全性。

選擇**區域網路>>VLAN** 開啟 VLAN 設定頁面。

以標籤為主的 VLAN(Tagged VLAN)

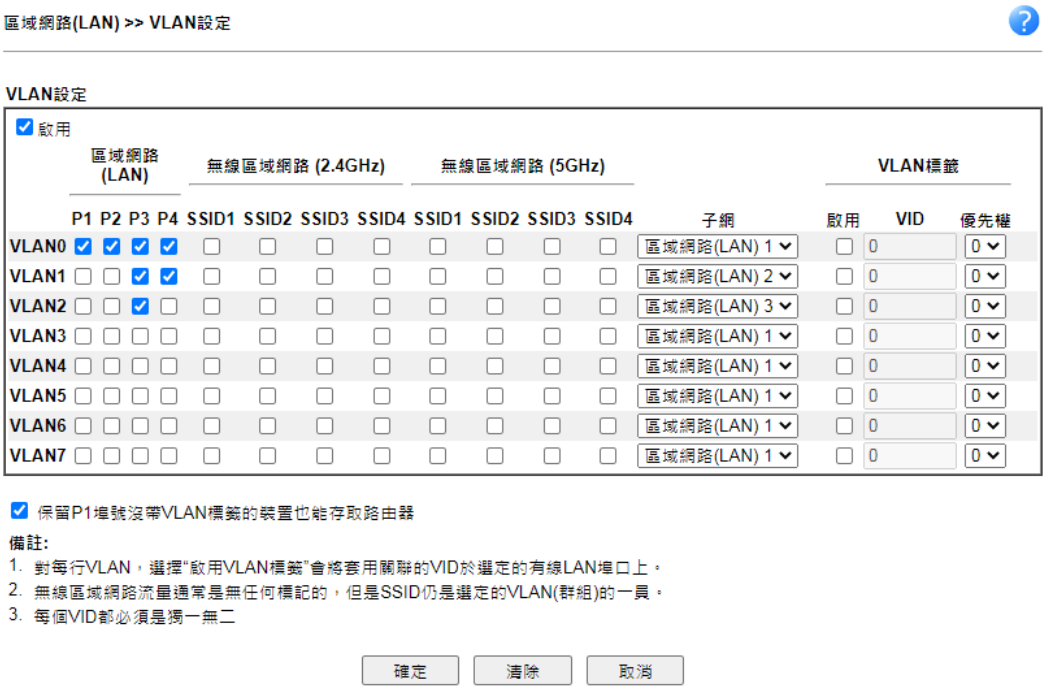
含標籤的 VLANs (802.1q)可將每筆資料標示 VLAN 識別碼，此一識別碼透過乙太網路交換器運送至指定的埠口，當資料傳送到區域網路時，指定的 VLAN 用戶即可以取得此識別碼。您可以設定 LAN 端 QoS 的優先權屬性，分派每個 VLAN 至不同的 IP 子網，讓路由器能操作提供更多不同的服務，這類的功能稱之為含標籤的多重子網。

以埠口為主的 VLAN(Port-Based VLAN)

相對於以標籤為主的 VLAN 以標籤來群組用戶，以埠口為主的 VLAN 使用的是實體的 LAN 埠口來區分用戶端至不同的 VLAN 群組上。

VLAN(虛擬區域網路)的功能提供您一個方便的方式，藉由群組實體通訊埠上的連結主機達到管理的目的。請開啟**區域網路>>VLAN**，可出現如下頁面，勾選**啟用**方塊啟動 VLAN 功能。

網頁顯示如下:



資訊	本頁設定僅能套用於 LAN 埠口而非 WAN 埠口。

可用設定說明如下：

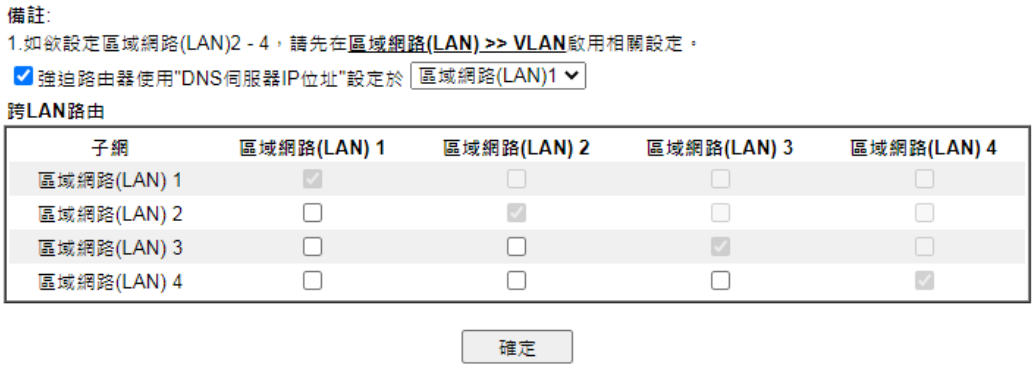
項目	說明
啟用	勾選此框啟用 VLAN 設定。
LAN	**P1 - P4**–勾選準備納入此 VALN 群組下的 LAN 埠口。
無線區域網路(2.4GHz)	**SSID1 - SSID4 -**勾選準備納入此 VLAN 群組下的 SSID 方框。
無線區域網路(5GHz)	**SSID1 - SSID4 -**勾選準備納入此 VLAN 群組下的 SSID 方框。 這個選項限用於 Vigor2135ac / Vigor2135Vac 等型號。
子網	選擇其中一個埠口讓選定的 VLAN 僅對應至此。例如，LAN1 指定為 VLAN0，就表示在 VLAN0 底下的電腦可透過此子網來取得 IP 位址。
VLAN 標籤	**啟用** – 勾選此框啟用 VLAN 標籤功能。 區域網路中向外傳送的封包，路由器將指定 VLAN 號碼至全部封包上。 請輸入標籤值並指定其優先權。 **VID** – 輸入 VLAN ID 號碼值，範圍是 0 到 4095。 **優先權** – 選擇此 VLAN 的優先權，範圍是 0 到 7。
允許在 P1 的未加標籤裝置存取路由器	可讓使用者在設定了錯誤的 VLAN 標籤設定情形下，還能與路由器溝通。由於路由器僅有一個 LAN 實體埠口，建議啟用管理埠口(LAN1)以確保資料傳輸保持暢通。

資訊	至少保留一處未加標籤的 VLAN 以便在發生不預期錯誤時，還能連上路由器。

跨 LAN 路由

路由器支援最多可達 7 組 VLAN，每條 VLAN 可以設定成一個或多個乙太網路埠口與無線區域網路服務組別辨識符(SSID)，在 VLAN(水平行)與 LAN 介面(垂直欄)中，

- 相同 VLAN(水平行)下所有主機彼此可見
- 相同 LAN 或是 WLAN 介面(垂直欄)下所有主機彼此可見，假若
  - 他們皆屬於相同的 VLAN，或是
  - 他們屬於不同的 VLAN，但是有啟用跨 LAN 路由功能，參考下圖

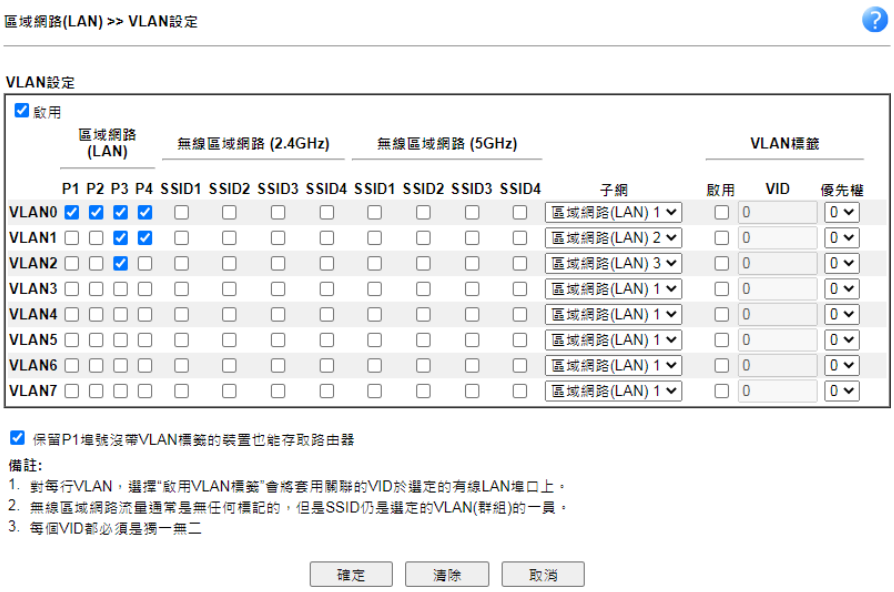


跨 LAN 路由可讓不同的 LAN 網段能彼此相連或是彼此隔離，這個功能僅在 VLAN 功能也啟用的狀況下才可使用。在跨 LAN 路由中，選定的核取方框表示上、左方這二個 LAN 可以互相溝通。

Vigor2135 系列具有靈活的 VLAN 系統，在最簡單的形式中，每個 Gigabit LAN 埠口可以彼此隔離，例如提供不同的資訊給予不同的公司或部門，但與本機流量完全區隔開來。

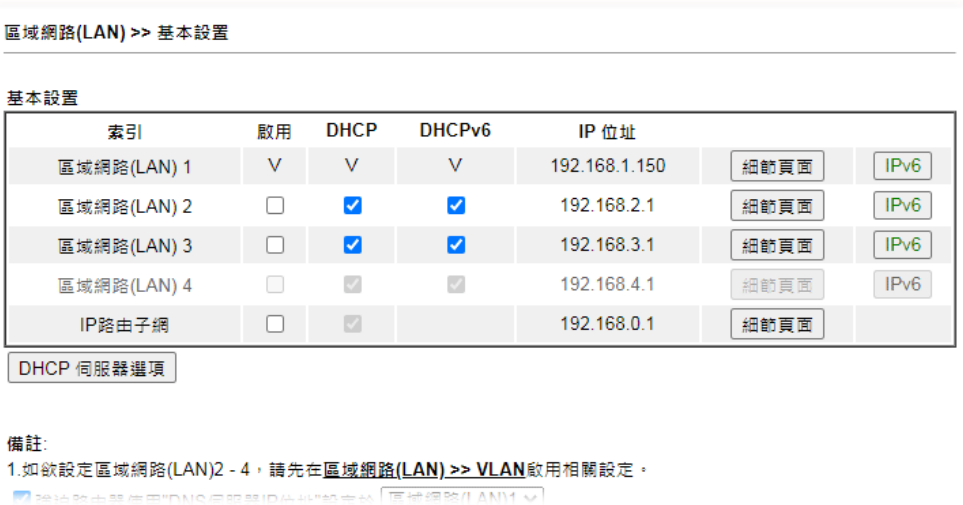
設定埠號式 VLAN 予無線與非無線用戶端

1. 所有的有線網路用戶端分類至群組 VLAN0，網段為 192.168.1.0/24(LAN1)之下。
2. 所有無線網路用戶端分類至群組 VLAN1，網段為 192.168.2.0/24 (LAN2)之下。
3. 開啟 **LAN>>VLAN 設定**，依照步驟 1 及 2 的說明勾選核取方框。



4. 按下**確定**。

5. 開啟**LAN>>基本設置**，如果您想要讓二個群組間的用戶能彼此溝通，可以勾選**LAN1**與**LAN2**間的方框。



路由器在 LAN 端最多可支援 4 組 IP 子網，每組子網都可以是獨立的或是彼此互連，對於部門或是需要多用途應用而言，是很理想的選擇。

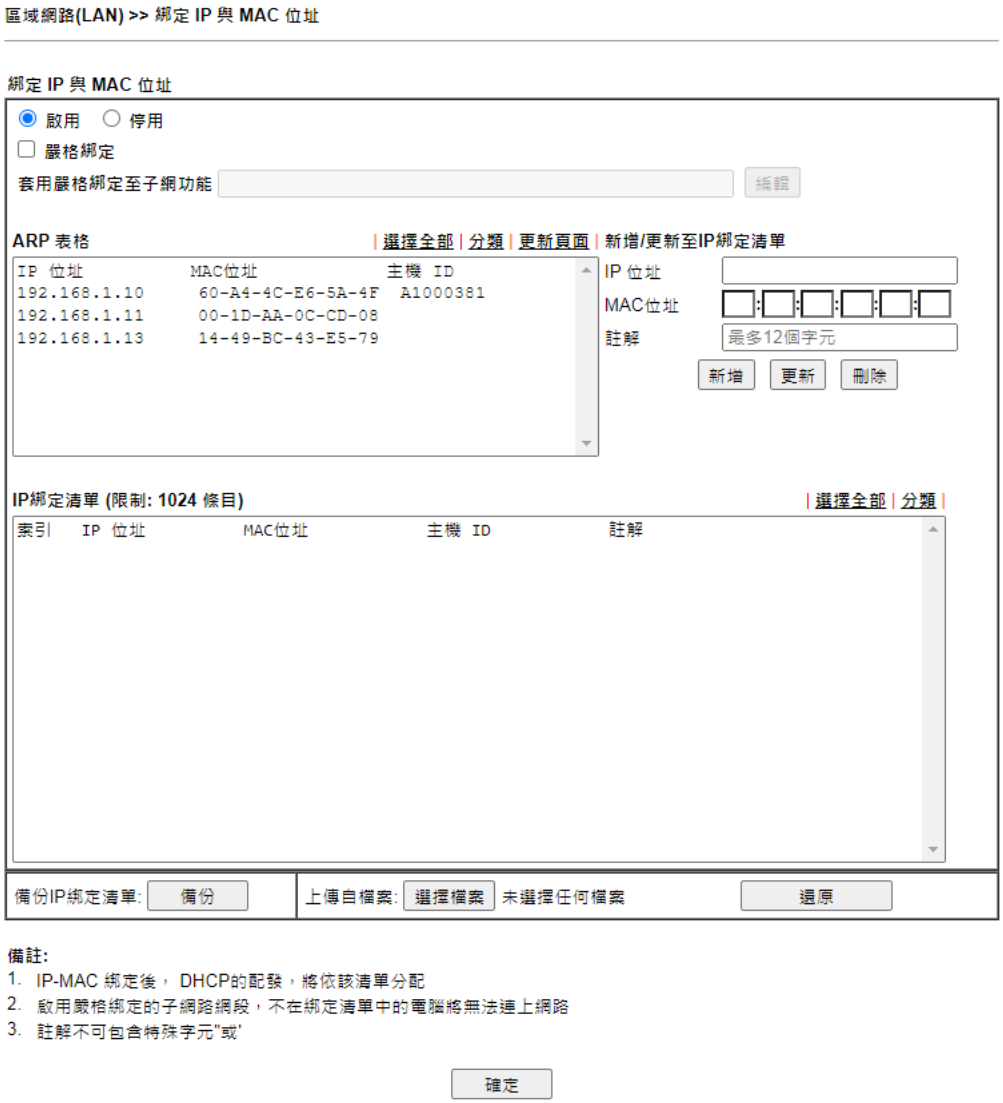
資訊

有關 VLAN 應用部分，請參考"附錄 I: 於 Vigor 路由器上的 VLAN 應用"取得更多細節資訊。

II-2-3 綁定 IP 與 MAC 位址

此功能用來綁定區域網路中的電腦之 IP 與 MAC 位址，如此一來可在網路上達到更有效的控制。當此一功能啟用時，所有被綁定的 IP 與 MAC 位址的電腦都不能在變更，如果您修改了綁定 IP 或 MAC 位址，可能會造成無法存取網際網路的窘態。

按**區域網路(LAN)**並選擇**綁定 IP 與 MAC 位址(Bind IP to MAC)**開啟設定網頁。



可用設定說明如下：

項目	說明
啟用	按此鈕啟用此功能，不過未列在 IP 綁定清單中的 IP/MAC 位址以可以連上網際網路。
停用	按此鈕關閉此功能，頁面上全部的設定都將會失效。
嚴格綁定	勾選此框以封鎖未列入 IP 綁定清單中的 IP/MAC 連線。 LAN 用戶端將依照 MAC 至 IP 位址組合由系統分派 IP 位址，MAC 位址尚未綁定 IP 位址者的 LAN 用戶端將無法進行網際網路連線。 **附註**: 在選擇**嚴格綁定**之前，確保至少有一個有效的 MAC 位址

	有綁定一個 IP 位址，否則將會發生沒有任何一個 LAN 用戶端得以存取網際網路，也無法連上路由器進行設定變更。 **套用嚴格綁定至子網功能** – 選擇子網以便套用綁定 IP 至 MAC 的規則。
ARP 表格	此表格為路由器的區域網路 ARP 表，IP 和 MAC 資訊將顯示於本區。列於 ARP 表中的每組 IP 和 MAC 位址都可以為使用者挑選並透過**新增**按鈕加到 IP 綁定清單上。
選擇全部	按此連結選擇表格內全部內容。
分類	按此連結將表格內容按照 IP 位元址重新排序。
更新頁面	用來更新 ARP 表格，當新的電腦增加到區域網路上時，您可以按此連結取得最新的 ARP 表格資訊。
新增/更新至 IP 綁定清單	**IP 位址** – 輸入 IP 位址以作為指定 MAC 位址之用。 **MAC 位址** – 輸入 MAC 位址以便與指定的 IP 位址綁在一起。 **註解** – 輸入簡易說明。
新增	允許您將 ARP 表格中所挑選的或是在新增和編輯上所輸入的 IP/MAC 位址新增至 **IP 綁定清單(IP Bind List)**上。
更新	允許您編輯或修正先前所建立的 IP 位址和 MAC 位址。
刪除	您可以刪除 **IP 綁定清單**上任何一個項目，選擇您想刪除的項目然後按**刪除**按鈕，選定的項目將自 **IP 綁定清單**上刪除。
IP 綁定清單	顯示綁定 IP 至 MAC 資訊清單。
備份 IP 綁定清單	按**備份**將設定檔儲存成檔案。
上傳自檔案	按**選擇檔案**挑選一個備份檔案，之後按**還原**將備份檔案取回覆蓋目前使用的清單。

資訊

在您選擇**嚴格綁定**前，您必須為一台電腦設定一組 IP/MAC 位址，若無設定的話，沒有一台電腦可以連上網際網路，路由器的網頁組態設定也無法進入了。

當您完成上述設定時，請按下**確定**按鈕儲存設定。

II-2-4 LAN 埠號監控

LAN 埠口監控可以套用於區域網路上的所有使用者，此功能可從一個或是多個指定的埠口複製傳輸流量至目標埠口。這項機制可幫助追蹤網路錯誤或是不正常封包傳輸，但卻不會影響一般網路資料存取。也就是說，使用者可以套用此功能來監控需要監督之使用者所有的傳輸資料。

這項功能還有一些優點，首先對於沒有其他偵測設備的人來說，它是相當經濟實用的；其次，它可以同時檢視 VLAN 群組中一個以上埠口的資料傳輸；第三它可將監控的資料到監控埠口端的分析人員處；最後是它很方便也很容易設定。

可用設定說明如下：

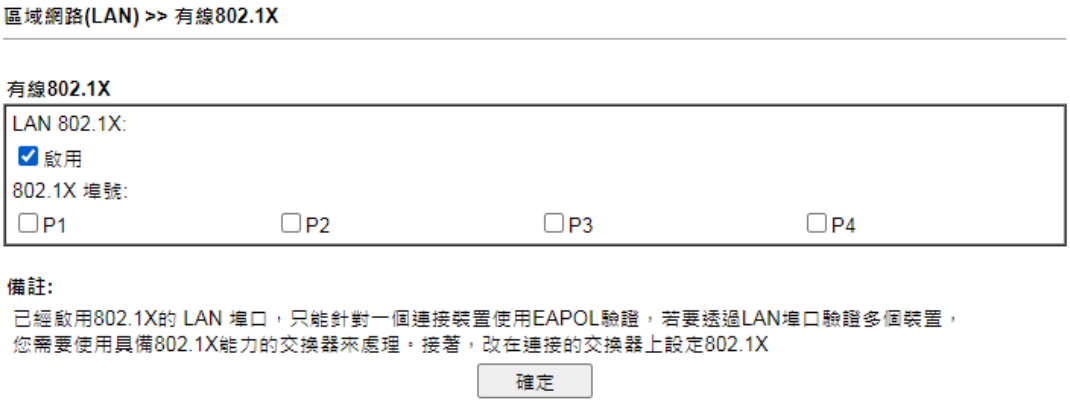
項目	說明
埠號監控	按下**啟用**可啟動此功能，或是按下**停用**停止此功能。
監控埠口	選擇任一埠口來檢視來自受控埠口的流量。
被監控傳送埠口	選擇埠口作為傳輸資訊用，須受到監控，可多選。
被監控接收埠口	選擇埠口作為接收資訊用，須受到監控，可多選。

完成設定之後，按下**確定**按鈕儲存相關設定。

II-2-5 有線 802.1x

IEEE 802.1x 是以 port-based Network Access Control (PNAC)為基準的 IEEE 標準，提供驗證機制以便驗證 LAN 或是 WLAN 端的連接裝置。

有線 802.1x 可針對每個 LAN 埠口上的網路裝置進行驗證作業，RADIUS 伺服器設定必區在啟用此功能之前事先設定完畢，因為 EAP (Extensible Authentication Protocol) 驗證機制仰賴 RADIUS 伺服器來進行，每個設定了有線 802.1x 的 LAN 埠口將僅轉送 802.1x 封包並阻擋其他的封包進入，直到驗證作業完成為止。



可用設定說明如下：

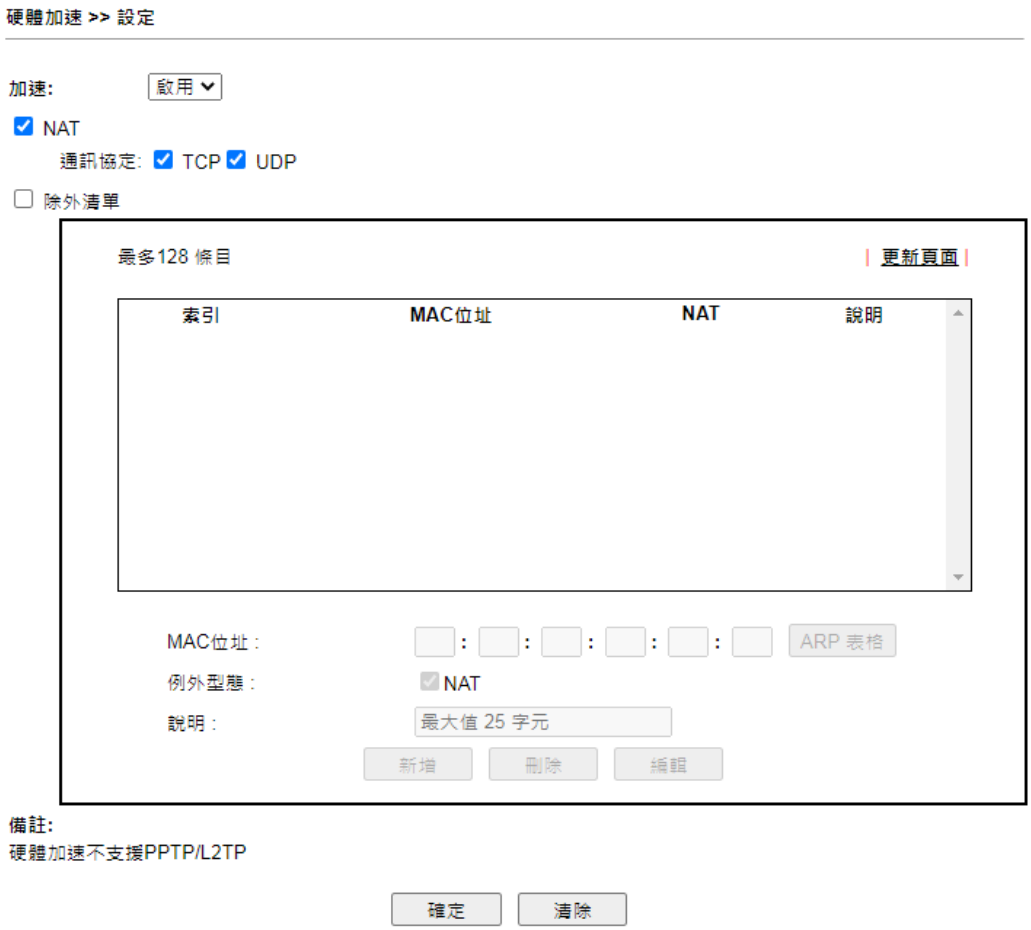
項目	說明
啟用	勾選此框啟用 LAN 802.1x 功能。
802.1x 埠號	啟用 LAN 802.1x 功能之後，請指定套用此功能的實體 LAN 埠口。

完成設定之後，按下**確定**按鈕儲存相關設定。

II-3 硬體加速

硬體加速在居易又稱為 PPA，因為是以 Infinion 的 PPE 為基準設計的，此項功能支援 4096 條連線數的網路流量(進與出)。

當您發現資料的流量過大且傳輸速度開始變得緩慢時，您可設定本頁透過硬體本身來加速資料流量。開啟**硬體加速**，可見如下的設定頁面。



可用設定說明如下：

項目	說明
加速	**停用** - 預設值。 **啟用** - 選擇此項啟用硬體加速功能設定。
NAT	硬體加速可以套用在 NAT 轉址的用戶上。 勾選 TCP 與/或 UDP 通訊協定。
除外清單	如果要限制一些透過路由器傳輸資料的用戶不得套用硬體加速功能，可以在此設立除外清單。 **MAC 位址** - 輸入用戶端的 MAC 位址。最多可以設定 128 條。 **ARP 表格** - 可以按此鈕開啟 ARP 表格，挑選需要的用戶裝置，以便使該裝置的 MAC 位址顯示在 MAC 位址欄位上。 **例外型態** - 勾選 NAT 與/或 IPsec。

	說明 - 針對此選定裝置輸入簡易說明。

檢查 PPA 狀態

如果要檢查 PPA 是否運作中，使用者可以利用 telnet 指令檢視傳輸中的連線數有多少，請使用指令“**ppa –v**，參考下圖。

```
> ppa -v
% PPA mode is Auto
% PPA mode is Manual (traffic)
%PPA time  is 10
%PPA range is 255
 ***************************************************************************
 WAN Acceleration session
 Session - Src_ip:Src_port ------- Dest_ip:Dest_port --- Nat_ip:Nat_port
 ***************************************************************************
 ***************************************************************************
 LAN Acceleration session
 Session - Src_ip:Src_port ------- Dest_ip:Dest_port --- Nat_ip:Nat_port
 ***************************************************************************
      0 - 192.168.  1. 10: 2938 - 119.236.154.122: 5590 - 192.168.  3. 10:52524
        Src_mac:00:22:15:8f:85:59 ---- Dest_mac:00:50:7f:37:c8:4c
      1 - 192.168.  1. 10: 2952 - 193. 88.  6. 13:33033 - 192.168.  3. 10:52538
        Src_mac:00:22:15:8f:85:59 ---- Dest_mac:00:50:7f:37:c8:4c
```

II-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。

NAT 的好處如下：

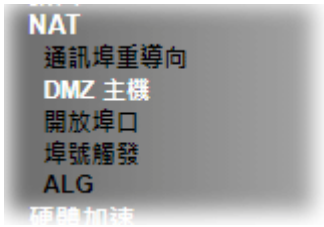
- **於應用真實 IP 位址上節省花費以及有效利用 IP 位址** NAT 允許本機中的 IP 位址轉成真實 IP 位址，如此一來您可以一個 IP 位址來代表本機。
- **利用隱匿的 IP 位址強化內部網路的安全性** 有很多種攻擊行動都是基於 IP 位址而對受害者發動的，既然駭客並不知曉任何虛擬 IP 位址，那麼 NAT 功能就可以保護內部網路不受此類攻擊。

資訊

在 NAT 頁面中，您將可看見以 RFC-1918 定義的虛擬 IP 位址，通常我們會使用 192.168.1.0/24 子網路給予路由器使用。就如前所提及的一般，NAT 功能可以對應一或多個 IP 位址和/或服務通訊埠到不同的服務上，換句話說，NAT 功能可以利用通訊埠對應方式來達成。

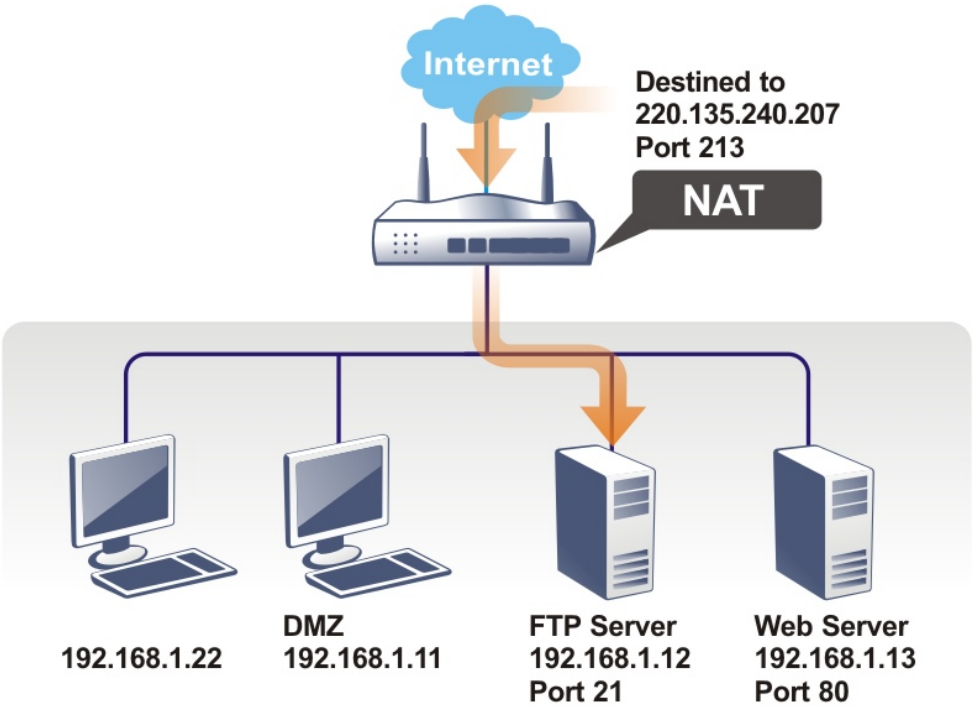
網頁使用者介面

下圖為 NAT 功能項目：



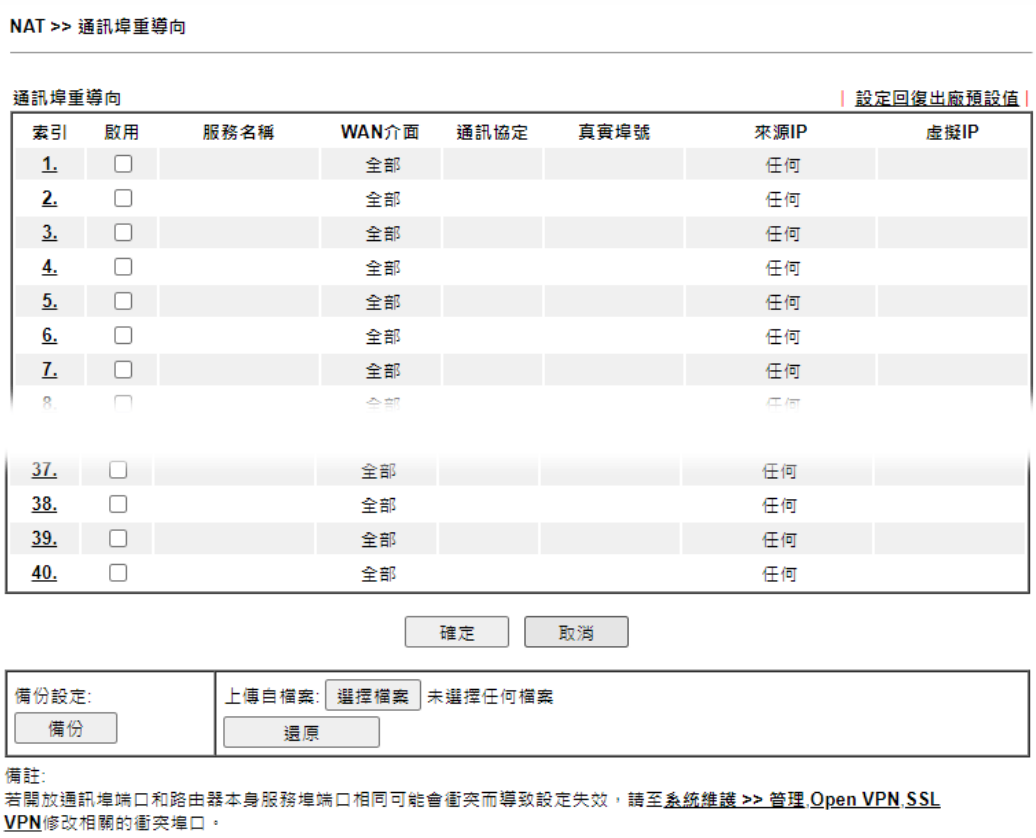
II-4-1 通訊埠重導向

通訊埠重導向通常是爲了本地區域網路中的網頁伺服器、FTP 伺服器、E-mail 伺服器等相關服務而設定，大部分的情形是您需要給每個伺服器一個真實 IP 位址，此一真實 IP 位址/網域名稱可以為所有使用者所辨識。既然此伺服器實際坐落於區域網路內，因此網路可以受到路由器之 NAT 的詳密保護，且可由虛擬 IP 位址/通訊埠來辨認。通訊埠重導向表的功能是傳送所有來自外部使用者對真實 IP 位址之存取需求，以對應至伺服器的虛擬 IP 位址/通訊埠。



通訊埠重導向只能應用在流入的資料量上。

欲使用此項功能，請開啟 **NAT** 頁面然後選擇**通訊埠重導向**。**通訊埠重導向**提供 40 組通訊埠對應入口給予內部主機對應使用。



可用設定說明如下：

項目	說明
索引	顯示設定檔的編號。
啟用	勾選此框啟用此設定檔。
服務名稱	顯示網路服務的說明。
WAN 介面	顯示設定檔使用的 WAN IP 位址。
通訊協定	顯示使用的協定類別（TCP 或是 UDP）。
真實埠號	顯示將被導引至指定的內部主機的虛擬 IP 及埠口的埠號。
來源 IP	顯示來源 IP 的 IP 物件名稱。
虛擬 IP	顯示提供此服務之內部主機的 IP 位址。

按下索引編號下的號碼連結，進入次層之設定頁面。

可用設定說明如下：

項目	說明
啟用	勾選此方塊啟用此通訊埠重導向設定。
模式	有二種模式可以供使用者選擇，如欲設定範圍給予指定服務，請選擇**範圍**。在"範圍" 模式下，若 IP 位元址與第一個對外通訊埠號皆填入之後，系統將自動計算並顯示第二個對外通訊埠值。
服務名稱	輸入特定網路服務的名稱。
通訊協定	選擇傳送層級的通訊協定(TCP 或 UDP)。
WAN 介面	選擇通訊埠重導向的 WAN IP 位址，有 8 組 WAN IP 別名可以選擇。 預設值是**全部(All)**，表示從任何一個通訊埠進入的資料都會重新導引至指定的 IP 位址及通訊埠。
真實埠號	指定哪一個通訊埠可以重新導向至內部主機特定的虛擬 IP 通訊埠上。如果您選擇**範圍**作為重導向模式，您將會在此看見二個方塊，請在第一個方塊輸入需要的數值，系統將會自動指定數值予第二個方塊。
來源 IP	使用下拉式清單指定 IP 物件，或是按下 IP 物件連結建立另一個新的物件來使用。
虛擬 IP	指定提供服務的主機之 IP 位址，如果您選擇**範圍(Range)**作為重導向模式，您將會在此看見二個方塊，請在第一個方塊輸入完整的 IP 位址 (作為起點)，在第二個方塊輸入四位數字(作為終點)。
虛擬埠號	指定內部主機提供服務之虛擬通訊埠號。

完成設定之後，按下**確定**按鈕儲存相關設定。

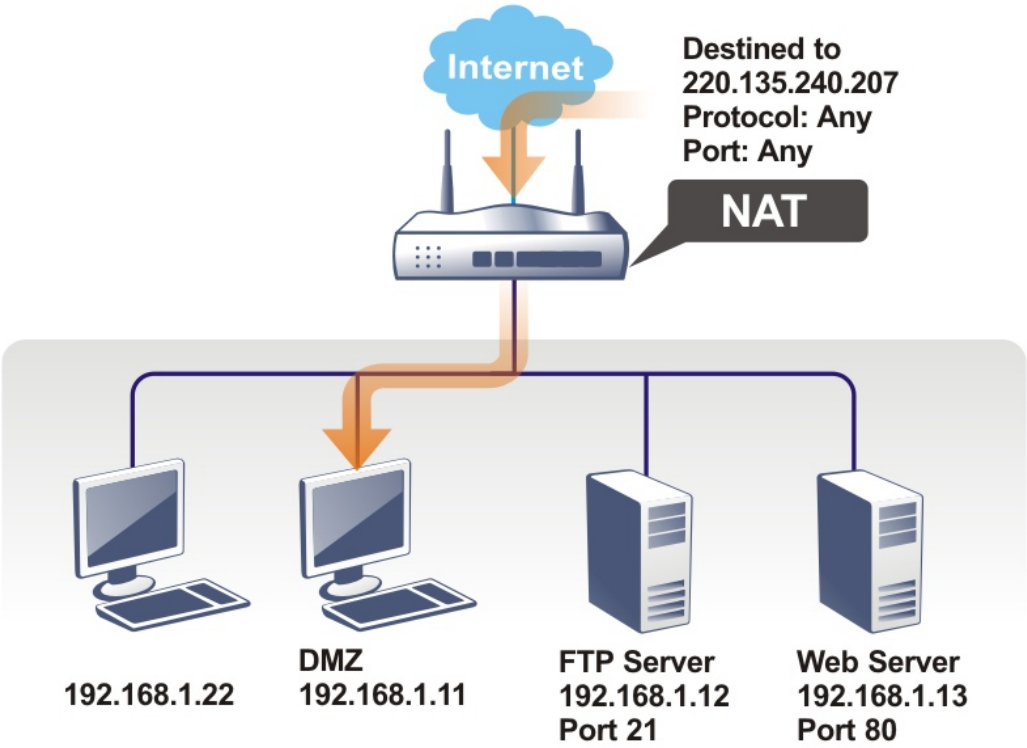
注意路由器有其內建服務(伺服器)諸如 Telnet、HTTP 和 FTP，因為這些服務(伺服器)的通訊埠號幾乎都相同，因此您可能需要重新啟動路由器以避免衝突發生。

例如，路由器的內建網頁設定給予的設定值是埠號 80，它可能造成與本地網路中網頁伺服器 http://192.168.1.13:80 產生衝突，因此您需要改變路由器的 **http** 通訊埠號，除了 80 以外任何一種都可以（例如 8080），來防止衝突發生。請改登入管理者模式並在系統維護群中的管理設定

做調整，接著您可在 IP 位址尾端加入 8080 (如 http://192.168.1.1:8080 而非僅只通訊埠號 80) 來進入管理畫面。

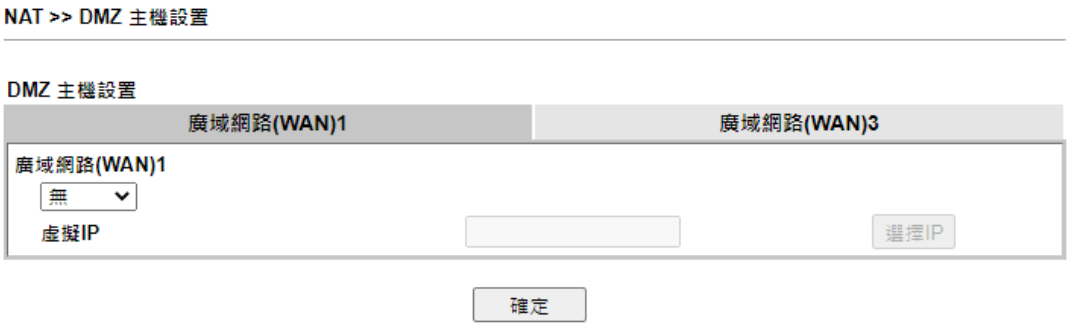
II-4-2 DMZ 主機

如同上面所提及的內容，通訊埠重導向可以將流入的 TCP/UDP 或是特定通訊埠中其他的流量，重新導向區域網路中特定主機之 IP 位址/通訊埠。不過其他的 IP 協定例如協定 50 (ESP)和 51(AH)是不會在固定通訊埠上行動的，Vigor 路由器提供一個很有效的工具 DMZ 主機，可以將任何協定上的需求資料對應到區域網路的單一主機上。來自用戶端的正常網頁搜尋和其他網際網路上的活動將可繼續進行，而不受到任何打擾。DMZ 主機允許內部被定義規範的使用者完全暴露在網際網路上，通常可促進某些特定應用程式如 Netmeeting 或是網路遊戲等等的進行。

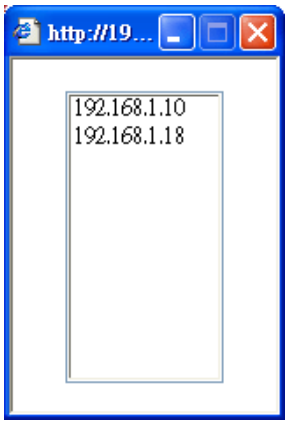
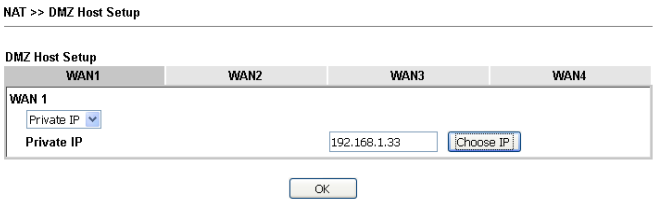


NAT 固有的安全性屬性在您設定 DMZ 主機時稍微被忽略了，建議您另外新增額外的過濾器規則或是第二組防火牆。

請按 **DMZ 主機**開啟下述頁面， WAN.您可以針對每個 WAN 界面設定不同的 DMZ 主機，按下 WAN 標籤即可切換到各個不同 WAN 設定頁面。

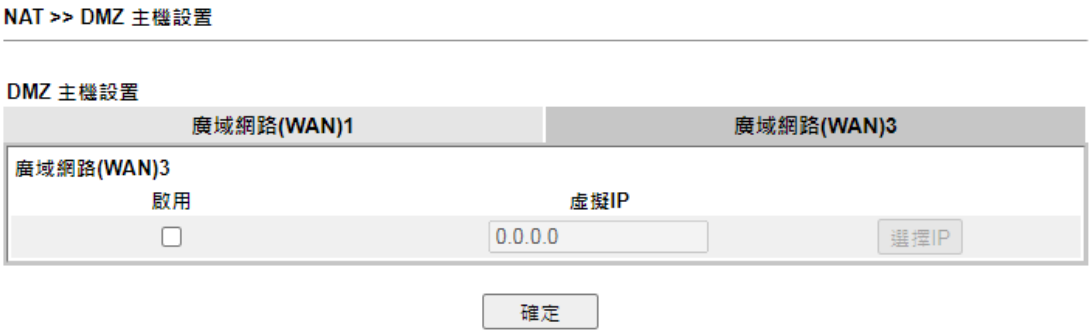


可用設定說明如下：

項目	說明
廣域網路(WAN1)	請先選擇**虛擬 IP** 或是**無**。
虛擬 IP	輸入 DMZ 主機的虛擬 IP 位址，或是按**選擇 IP(Choose IP)**開啟另一頁面來選擇。
選擇 IP	按下此鈕後，如下視窗立即跳出。此視窗包含您的區域網路中全部主機的虛擬 IP 位址清單，請自清單中選擇一個虛擬 IP 位址作為 DMZ 主機。  當您已經從上面的視窗選好了虛擬 IP 位址時，該 IP 位址將會顯示在下面的螢幕上，請按**確定**儲存這些設定。 

當您已經從上面的視窗選好了虛擬 IP 位址時，該 IP 位址將會顯示在下面的螢幕上，請按**確定**儲存這些設定。

其他 WAN 介面的 DMZ 主機設定畫面與 WAN1 有些微不同，參考下圖：



如果您在 WAN2 介面的**網際網路連線設定**選擇 **PPPoE/靜態(固定)IP/PPTP**，並且設定 **WAN 別名**，您將可在此頁面發現**輔助 WAN IP** 項目。

NAT >> DMZ 主機設置

DMZ 主機設置

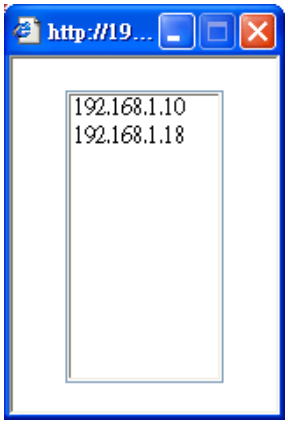
廣域網路(WAN)1	廣域網路(WAN)3

廣域網路(WAN)1

索引	啟用	輔助WAN IP	虛擬IP	
1.	☐	---	0.0.0.0	選擇IP
2.	☐	192.168.1.203	0.0.0.0	選擇IP

確定 清除

可用設定說明如下：

項目	說明
啟用	勾選此項以啟動 DMZ 主機功能。
虛擬 IP	輸入 DMZ 主機的虛擬 IP 位址，或是按**選擇 IP** 開啟另一頁面來選擇。
選擇 IP	按下此鈕後，如下視窗立即跳出。此視窗包含您的區域網路中全部主機的虛擬 IP 位址清單，請自清單中選擇一個虛擬 IP 位址作為 DMZ 主機。  當您已經從上面的視窗選好了虛擬 IP 位址時，該 IP 位址將會顯示在下面的螢幕上，請按**確定**儲存這些設定。

完成設定之後，按下**確定**按鈕儲存相關設定。

II-4-3 開放通訊埠

開放通訊埠允許您開啟一段範圍內的通訊埠，供特定應用程式使用。

常見的應用程式包含有 P2P 應用程式(如 BT、KaZaA、Gnutella、WinMX、eMule 和其他)、Internet Camera 等等，您需要先確定應用程式包含最新的資料，以免成為安全事件的受害者。

按**開放通訊埠**開啟下面的網頁。

可用設定說明如下：

項目	說明
索引	表示本地主機中您想要提供之服務，其特定內容網頁之相關號碼，您應該選擇適當的索引號碼以編輯或是清除相關的內容。
啟用	勾選此框啟用此設定檔。
註解	指定特定網路服務的名稱。
WAN 介面	顯示此設定檔使用的 WAN 介面。
輔助 WAN IP	顯示此設定檔使用的 IP 別名設定，若無任何別名存在，此區將不會顯示出來。
來源 IP	顯示來源 IP 的 IP 物件名稱。
本機 IP 位址	顯示提供此項服務之本地主機的 IP 位址。
備份	按下**備份**儲存開放通訊埠設定。

還原	按下**選擇檔案**挑選設定檔，接著按下**還原**按鈕套用檔案。

如果要新增或是編輯通訊埠設定，請按索引下方的號碼按鈕。該索引號碼入口設定頁面隨即出現，在每個輸入頁面中，您可以指定 10 組通訊埠範圍給予不同的服務。

可用設定說明如下：

項目	說明
啟用開放通訊埠	勾選此項以啟動此功能。
註解	請爲所定義的網路應用/服務命名。
WAN 介面	指定該項設定之 WAN 介面。
來源 IP	使用下拉式清單選擇 IP 物件/IP 群組。
WAN IP	如果您在**網際網路連線設定**選擇 **PPPoE/靜態(固定)IP/PPTP**，並且設定 **WAN 別名**，您將可在此頁面發現 **WAN IP** 項目。請自下拉式選項中選擇需要的 IP 位址。
虛擬 IP	輸入本機的虛擬 IP 位址或是按**選擇 IP** 挑選另外一個。
通訊協定	指定傳送層級的通訊協定，有 **TCP**、**UDP** 和 **----- (none)**等幾種選擇。
起始埠號	指定本機所提供之服務的開始通訊埠號。
結束埠號	指定本機所提供之服務的結束通訊埠號。

完成設定之後，按下**確定**按鈕儲存相關設定。

II-4-4 埠號觸發

埠號觸發式開放通訊埠的變更版。二者最主要的差異是：

- 一旦按下確定按鈕，設定檔即開始生效，開放通訊埠下的埠口永遠呈現開啟狀態。
- 一旦按下確定按鈕，設定檔即開始生效，埠號觸發會在觸發條件符合時嘗試開啟相關埠口。
- 所有埠口的持續開放的時間端賴使用的通訊協定而定，預設時間顯示如下，相關數據可以利用 telnet 指令進行變更。

  TCP: 86400 sec.

  UDP: 180 sec.

  IGMP: 10 sec.

  TCP WWW: 60 sec.

  TCP SYN: 60 sec.

可用設定說明如下：

項目	說明
索引	表示埠號觸發設定檔的相應號碼，選擇適當的索引號碼以編輯或是清除相關的內容。
啟用	勾選此框啟用此設定檔。
註解	顯示與此規則相關的說明內容。
觸發協定	顯示觸發封包使用的協定。
觸發埠號	顯示觸發封包使用的埠號。
來源 IP	顯示 IP 物件的名稱。
輸入協定	顯示觸發設定檔輸入資料使用的協定。
輸入埠號	顯示觸發設定檔輸入資料使用的埠號。

按下任一索引連結開啟設定頁面：

可用設定說明如下：

項目	說明
啟用	勾選方框啟用此設定檔。
服務	您可以選擇事先定義的服務套用到此觸發設定檔。
註解	輸入此設定檔需要特別說明的內容。
來源 IP	使用下拉式清單選擇 IP 物件/IP 群組類型，接著自旁邊的清單終選擇物件來使用。
觸發協定	針對此觸發設定檔選擇適當的協定（如 TCP, UDP 或 TCP/UDP)。
觸發埠號	輸入觸發設定檔的埠號或是埠號範圍。
輸入協定	當收到觸發封包時，輸入封包將會利用此處所選擇的協定來處理。
輸入埠號	輸入封包的埠號或是埠號範圍。

完成設定之後，按下**確定**按鈕儲存相關設定。

II-4-5 ALG(應用層閘道)

ALG 代表應用層閘道(**Application Layer Gateway)**，路由器提供二種方式 RTSP (Real Time Streaming Protocol) ALG 以及 SIP (Session Initiation Protocol) ALG 來處理聲音與影音封包。RTSP ALG 可透過路由器的 NAT 傳送並接收 RTSP 訊息、RTCP 訊息與 RTP 的聲音與影音封包。而 SIP ALG 可透過路由器的 NAT 傳送並接收 SIP 訊息與 RTP 聲音封包。

可用設定說明如下：

項目	說明
啟用 ALG	勾選此框啟用此功能。
監聽埠口	輸入 SIP 或是 RTSP 通訊協定需求之埠號。
TCP	勾選此框以便透過 NAT 從 TCP 傳輸與接收相應協定訊息封包。
UDP	勾選此框以便透過 NAT 從 UDP 傳輸與接收相應協定訊息封包。

II-5 其他應用

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。

LAN DNS / DNS 轉發

LAN DNS 讓網路管理者得以掌管具隱私與安全性的伺服器，當網管理者於 LAN 內端設定 FTP、郵件或是網頁伺服器，您可以指定特殊的虛擬 IP 予相應的伺服器上。如此一來，即使遠端 PC 採用真實 DNS 作為 DNS 伺服器，路由器的 LAN DNS 解決方案將回應指定的虛擬 IP 位址。

排程

路由器具有內建時鐘，可以讓您手動或是透過網路時間協定(NTP)自動更新時間，因此您不只可以規劃路由器在特定時間撥號至網際網路，也能限制於特定時間內存取網際網路資料，如此一來使用者只能在限定時間(或說上班時間)上網，時間排程也可以和其他功能搭配使用。

RADIUS

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。

內建 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。

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。

透過 WAN/LAN 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，也可以透過遠端來喚醒。

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 設定中開啟 WOL 功能。

網頁使用者介面

II-5-1 動態 DNS

啟動此功能並增加一個動態 DNS 帳戶

1. 假設您已經從 DDNS 供應商註冊了一個網域名稱(例如 hostname.dyndns.org)，且獲得一個帳號，其使用者名稱為 *test*；密碼為: *test*。
2. 開啟**其他應用>>動態 DNS**。
3. 勾選**啟用動態 DNS 設定**。

可用設定說明如下：

項目	說明
啟用動態 DNS 設定	勾選此方塊啟用此功能。
設定回復出廠預設值	清除全部設定資料並回復到出廠的設定。
檢視日誌	可開啟另一個對話盒並顯示 DDNS 資訊紀錄。
強迫更新	按此按鈕強迫路由器取得最新的 DNS 資訊。

自動更新間隔	輸入動態 DNS 伺服器的自動更新的間隔時間。
索引	按下方的號碼連結進入 DDNS 設定頁面，以設定帳戶。
啟用	勾選此框啟用此帳戶。
WAN 介面	顯示使用的 WAN 介面。
網域名稱	顯示您在 DDNS 設定頁面上所設定的網域名稱。

4. 選擇索引號碼 1，為您的路由器新增一個帳號。勾選**啟用動態 DNS 帳號**，然後選擇正確的服務供應商(例 dyndns.org)，輸入註冊的主機名稱(例 hostname)，並於網域名稱區塊中輸入網域的字尾名稱(例 dyndns.org)；接著輸入您的帳號登入名稱(例 dray)和密碼(例 test)。

若您選擇**使用者自訂**作為服務供應商設定，網頁將會有些許不同：

可用設定說明如下：

項目	說明
啟用動態 **DNS** 帳號	勾選此方塊以啟用目前帳號，如果您勾選此方塊，您可在步驟 2 中的網頁上看到啟動欄位出現勾選標示。
WAN 介面	**WAN#**優先- 連線時，路由器將會優先使用 WAN#作為首選頻道，如果 WAN#連線失敗，路由器才會另外的 WAN 介面連線。 限用 **WAN#** - 連線時，路由器僅會使用 WAN#作為此帳號的唯一連線介面。
服務供應商	為此 DDNS 帳號選擇適當的服務供應商。若無找到需要的服務供應商，請選擇使用者自訂。 供應商主機 - 輸入提供關服務的主機 IP 位址或是網域名稱。 請注意這個選項僅在您選擇使用者自定作為服務供應商設定時，始可使用。 服務 **API** - 輸入字 DDNS 伺服器取得之 API 資訊。 請注意這個選項僅在您選擇使用者自定作為服務供應商設定時，始可使用。 (e.g: /dynamic/dns/update.asp?u=jo***&p=jo********&hostname=j****.changeip.org&ip=###IP### &cmd=update&offline=0) 驗證類型 - 有二種方式可以用來驗證。 ● 基本 – 定義的使用者名稱與密碼，之後可以從擷取的封包上顯示出來。 ● **URL** -定義的使用者名稱與密碼，之後可以從 URL 上顯示出來。(例如 http://ns1.vigorddns.com/ddns.php?username=xxxx&password=xxxx&domain=xxxx.vigorddns.com) 請注意這個選項僅在您選擇使用者自定作為服務供應商設定時，始可使用。 連線類型 - 有二種(HTTP 與 HTTPs)連線類型可以指定，請注意這個選項僅在您選擇使用者自定作為服務供應商設定時，始可使用。 伺服器回應 - 輸入您想要從 DDNS 伺服器接收的文字。 請注意這個選項僅在您選擇使用者自定作為服務供應商設定時，始可使用。
服務類型	選擇服務類型(動態、自訂、固定)。如果您選擇的是自訂，您可以修正網域名稱區域中所選定的網域資料。
網域名稱	輸入您所申請的網域名稱。請使用下拉式選項選擇想要使用的一個名稱。 請注意當您選擇使用者自定作為服務供應商設定時，這個選項將無法使用。
登入名稱	輸入您在申請網域名稱時所設定之登入名稱。
密碼	輸入您在申請網域名稱時所設定之密碼。
萬用字元及備份 **MX**	並非所有的動態 DNS 供應商都支援萬用字元與備份 MX(郵件交換)功能，您可以從其官網取的相關資訊。
郵件延伸程式	某些 DDNS 伺服器可能會要求提供額外的資訊，如電子郵件地址，請您在此輸入必要的電子郵件位址，以配合該 DDNS 伺服器之需要。

決定 **WAN IP**	如果路由器安裝在 NAT 路由器的後端，您可以啟用此功能來定位真實的 WAN IP 位址。 當 Vigor 路由器使用的真實 IP 其實為虛擬 IP 時，此功能可以偵測出 NAT 路由器使用的真實 IP 並且利用偵測出來的 IP 位址來更新 DDNS。 有二種方法可以選擇: ● **WAN IP** - 如果選擇此項且路由器的 WAN IP 為虛擬 IP，那麼 DDNS 更新時就會以偵測到的真實 IP 來替代。 ● **Internet IP** – 如果選擇此項且路由器的 WAN IP 為虛擬 IP，在 DDNS 更新之前，它就會被轉換為真實 IP。

5. 按**確定**按鈕啟動此設定，您將會看到所做的設定已被儲存。

DrayDDNS 設定

DrayDDNS 是居易科技自行研發提供的 DDNS 服務，它可以記錄單一網域名稱內多個 WAN IP (IPv4) 位址。對使用者來說，方便使用且容易設定，每個 Vigor 路由器皆可註冊一個網域名稱。

選擇 **DrayDDNS (Global)** 作為服務供應商，網頁將顯示如下：

可用設定說明如下：

項目	說明
啟用動態 DNS 帳號	勾選此框啟用目前的帳號。
服務供應商	選擇 **DrayDDNS (Global)**作為服務供應商。 **設定精靈**– 此鈕僅在選定 **DrayTek Global** 為服務供應商時可用，欲啟用居易科技的 DDNS 服務，按此進入**設定精靈>>服務啟用設定精靈**網頁以啟用授權書。 可參考章節 **A-1 如何使用 DrayDDNS?** 查看詳細內容。
狀態	顯示授權書是否啟用。
決定 WANIP	如果路由器安裝在 NAT 路由器的後端，您可以啟用此功能來定位真實的 WAN IP 位址。 當 Vigor 路由器使用的真實 IP 其實為虛擬 IP 時，此功能可以偵測出 NAT 路由器使用的真實 IP 並且利用偵測出來的 IP 位址來更新 DDNS。

	有二種方法可以選擇: ● **WAN IP** - 如果選擇此項且路由器的 WAN IP 為虛擬 IP，那麼 DDNS 更新時就會以偵測到的真實 IP 來替代。 ● **網際網路 IP** – 如果選擇此項且路由器的 WAN IP 為虛擬 IP，在 DDNS 更新之前，它就會被轉換為真實 IP。
WAN 介面	**WAN#優先** - 連線時，路由器將會優先使用 WAN#作為首選頻道，如果 WAN#或 LTE /WAN4 連線失敗，路由器才會另外的 WAN 介面連線。 **限用 WAN#** - 連線時，路由器僅會使用 WAN#作為此帳號的唯一連線介面。
Let's Encrypt 憑證	**建立** – 按此鈕可已產生一組由 Let's Encrypt 所發行的憑證。 **自動更新** – 勾選此框讓系統自動更新憑證資訊。

停用此功能並清除全部動態 DNS 帳號

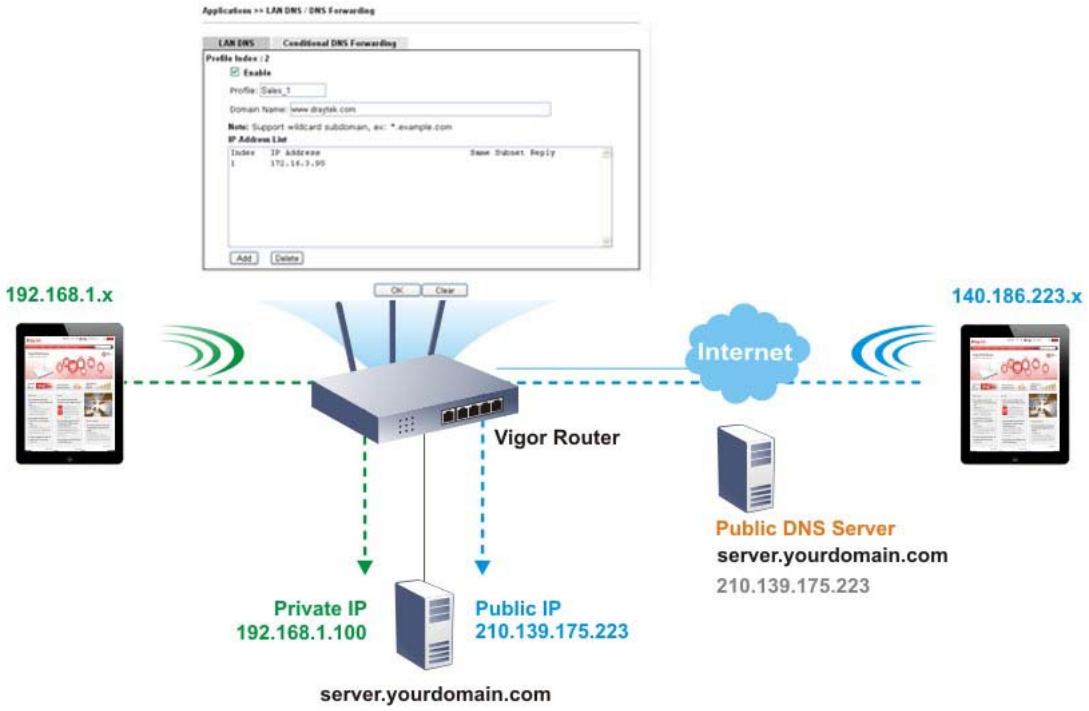
取消勾選**啟用動態 DNS 設定**，然後按下**清除全部**按鈕即可停用此功能並刪除所有的帳號。

刪除動態 DNS 帳號

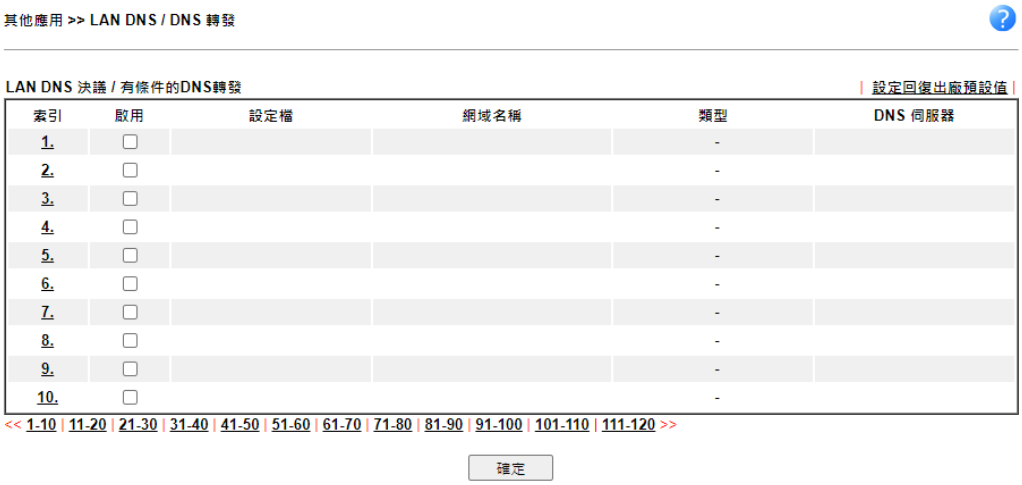
按下您想要刪除項目的索引編號連結，然後然後按下**清除全部**按鈕刪除所有的帳號。

II-5-2 LAN DNS / DNS 轉發

LAN DNS 讓網路管理者得以掌管具隱私與安全性的伺服器，當網管理者於 LAN 內端設定 FTP、郵件或是網頁伺服器，您可以指定特殊的虛擬 IP 予相應的伺服器上。如此一來，即使遠端 PC 採用真實 DNS 作為 DNS 伺服器，路由器的 LAN DNS 解決方案將回應指定的虛擬 IP 位址。



點選**其它應用>>LAN DNS / DNS 轉發**開啟如下頁面：

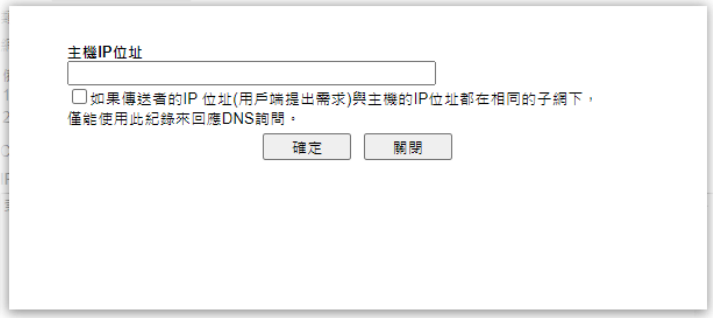


每個項目說明如下：

項目	說明
設定回復出廠預設值	清除所有的設定檔內容並回復出廠的預設值。
索引	按下索引編號下方的號碼連結可進入設定頁面。
啟用	勾選此方框啟用選定的設定檔。
設定檔	顯示 LAN DNS 設定檔的名稱。
網域名稱	顯示 LAN DNS 設定檔的網域名稱。
類型	顯示此設定檔的類型(LAN DNS 或是 DNS 轉發)。
DNS 伺服器	顯示 DNS 伺服器的 IP 位址。

建立 LAN DNS 設定檔，請按下任何一個索引編號，開啟如下頁面。

可用設定說明如下：

項目	說明
啟用	勾選此方框啟用此功能。
設定檔	輸入設定檔名。 **附註:** 若在此 LAN DNS 設定檔名，且按下**確定**儲存配置，相關名稱也會自動套用到條件式 DNS 轉送頁面。
類型	請選擇 LAN DNS 或是 DNS 轉發。
如果選擇的是 LAN DNS	**網域名稱** - 輸入此設定檔的網域名稱。 **CNAME** - 按下**新增**可為目前的網域名稱另加一個網域名稱別名。後續若不需要，可案**刪除**按鈕來移除。 **IP 位址清單** - IP 位址清單用來對照上述指定的網域名稱，一般來說，一個網域名稱對應一組 IP 位址，如有必要，您可以設定二組 IP 位址給予相同的網域名稱。 **新增** – 按下此按鈕後會出現如下對話方塊讓您輸入主機的 IP 位址。 

	● **主機 IP 位址** - 輸入回送之 IP 位址，用來回應 DNS 詢問網域名稱與別名時之用。 ● **如果傳送者的 IP 位址....** – 不同區域網路端的電腦以共享相同的網域名稱，但是您必須勾選此方框讓路由器辨認並回應 IP 位址以因應來自區域網路端不同電腦 DNS 詢問要求。 **刪除** – 按下此鈕刪除清單中選定的 IP 位址。
如果選擇的是 DNS 轉發	**網域名稱** - 輸入此設定檔的網域名稱。 **DNS 伺服器 IP 位址** - 輸入 DNS 伺服器的 IP 位址，以便作為 DNS 轉發之 DNS 伺服器。

按下**確定**按鈕儲存設定。

II-5-3 DNS 安全性

DSN 安全性能確保輸入的資料不是偽造的，且資料來源安全正確，防止受到外力發動的 DNS 攻擊。

II-5-3-1 基本設置

路由器所有的 WAN 介面都可以個別地啟用 DNS 安全性設定。

可用設定說明如下：

項目	說明
介面	路由器的 WAN 介面都可以設定成啟用 DNS 安全性功能。
啟用	勾選此框啟用 DNS 安全性管理。
主要 DNS	顯示自 DHCP 伺服器取得或是由固定 WAN 所指定的主要 DNS 的 IP 位址。
次要 DNS	顯示自 DHCP 伺服器取得或是由固定 WAN 所指定的次要 DNS 的 IP 位址。
偽造 DNS 回覆	有時路由器可能會遇到偽造 DNS 查詢的封包，以下有二種方式可以回應這類的查詢： **捨棄**- 直接丟棄該封包。 **通過** – 接受該封包並讓其通過路由器。

II-5-3-2 網域診斷

本頁可利用手動設定來診斷特定網域是否安全。

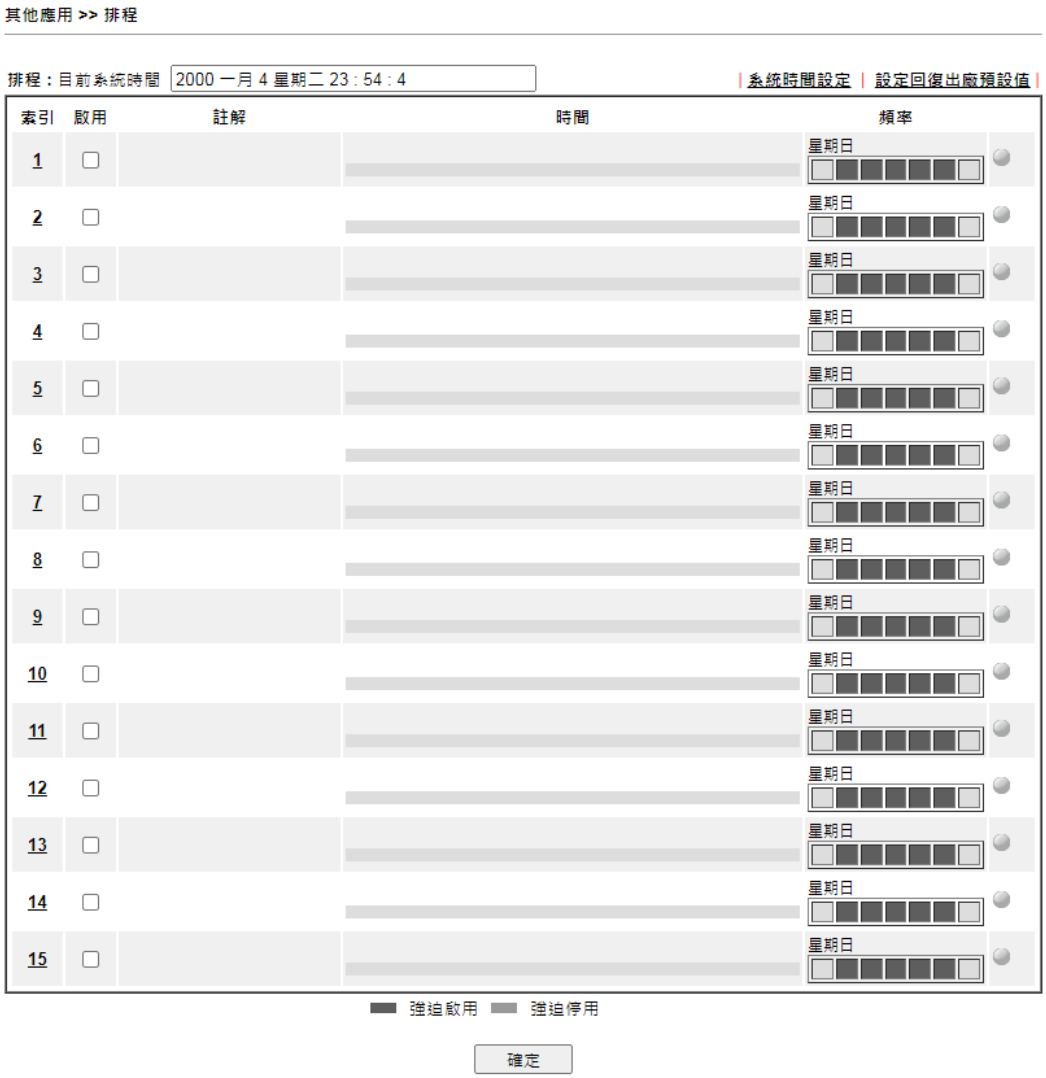
可用設定說明如下：

項目	說明
網域	輸入您想要查詢的網域名稱或是 IP 位址(IPv4/IPv6)。
介面	指定需要執行診斷的介面。
DNS 伺服器	輸入用來診斷上述指定的網域名稱之 DNS 伺服器 IP 位址。
診斷	按此執行網域診斷。
結果	診斷資訊將會顯示在本區。

II-5-4 排程

Vigor 路由器可允許您手動更新，或利用網路時間協定(NTP)更新時間，因此您不只可以規劃路由器在特定時間撥號至網際網路，也能限制於特定時間內存取網際網路資料，如此一來使用者只能在限定時間(或說上班時間)上網，時間排程也可以和其他功能搭配使用。

您必須在設定排程前先設定好時間，在**系統維護**群組中，選擇**時間和日期**以開啟時間設定頁面，按**取得時間**按鈕取得與電腦(或網際網路)一致的時間，一旦您關閉或是重新啟動路由器，時鐘的時間也會重新啟動。還有另一種方法可以設定時間，您可以在網際網路上請求 NTP 伺服器(這是一個時間伺服器)以同步化路由器的時鐘，這個方法只能在廣域網路連線建立時才能使用。



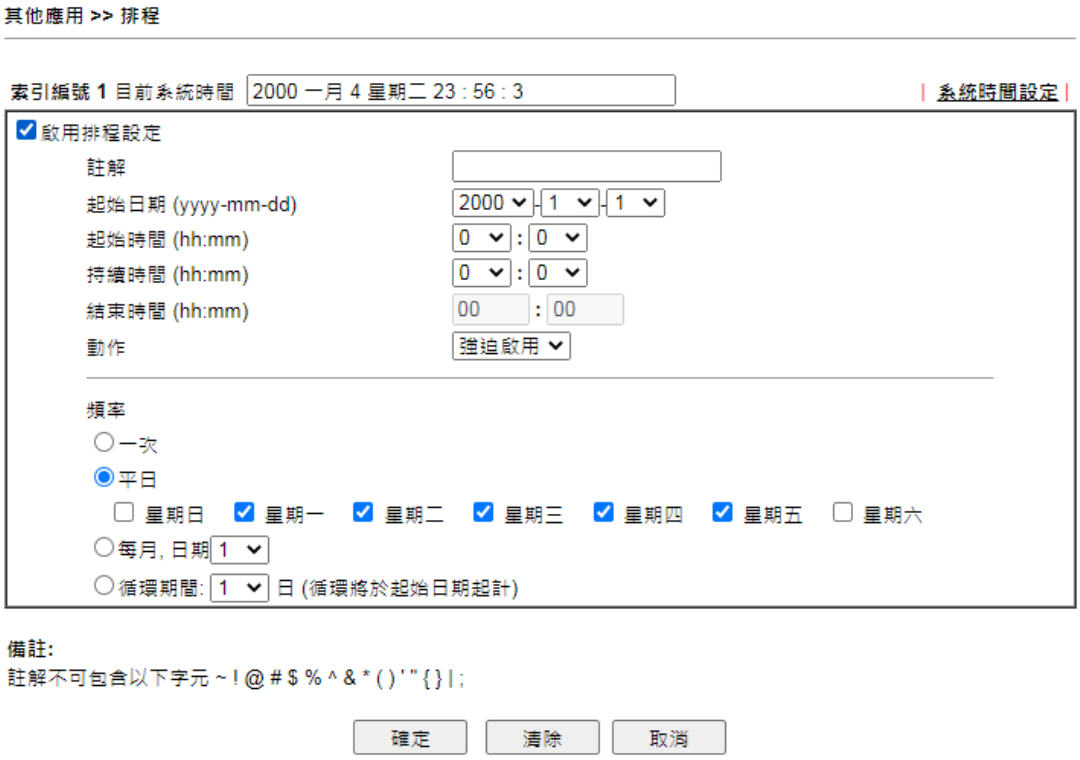
可用設定說明如下：

項目	說明
目前系統時間	顯示路由器使用的時間。
系統時間設定	按此連結開啟時間設定頁面(系統維護>>時間與日期)。
設定回復出廠預設值	清除全部設定資料並回復到出廠的設定。
索引	按下方的號碼進入排程設定頁面。
啟用	點選此框啟用此排程設定檔。

註解	顯示時間排程的名稱。
時間	顯示有效的時程。
頻率	以色塊顯示排程設定檔內何日永遠連線，何日永遠下線。 ● - 如顯示綠燈，表示路由器正使用該排程中。

您最多可以設定 15 個排程，然後可以應用於**網際網路連線控制**或是 **VPN 與遠端存取控制 >>LAN-to-LAN** 設定上。

欲新增一個排程，請按任何一個索引號碼，開啟排程的細部設定。



可用設定說明如下：

項目	說明
啟用排程設定	勾選此項目以啟動此排程。
註解	輸入此設定檔的簡短說明。
起始日期	指定排程的開始日期。
起始時間	指定排程的開始時間。
持續時間	指定排程的持續時間。
結束時間	當開始時間與持續時間皆設定完畢之後，系統會自動計算結束時間。
動作	指定排程套用的方式： **強迫啟用** - 強迫連線永遠存在。 **強迫停用** - 強迫連線永遠停止。

頻率	指定套用的排程頻率。 ● **一次 -** 此計劃的頻率只會應用一次。 ● **平日 -** 指定一週當中哪些日子需要執行此項排程作業。 ● **每月,日期 -** 路由器在每個月特定的日期(1 到 28 號)執行此排程做業。 ● **循環期間-** 輸入日期。套用此排程的任何動作即可在每隔數日執行。例如輸入 3 做為循環期間，套用此排程的任何動作將每隔 3 天執行一次，日期就從起始日期開始。

按**確定**按鈕以儲存設定。

範例

假設您想要控制 PPPoE 網際網路存取連線能夠在每天的 9:00 到 18:00 都能保持開啟狀態(強迫啟用)，其他時間則中斷連線(強迫停用)。

Office Hour:

(Force On)

Mon - Sun **9:00 am** **to** **6:00 pm**

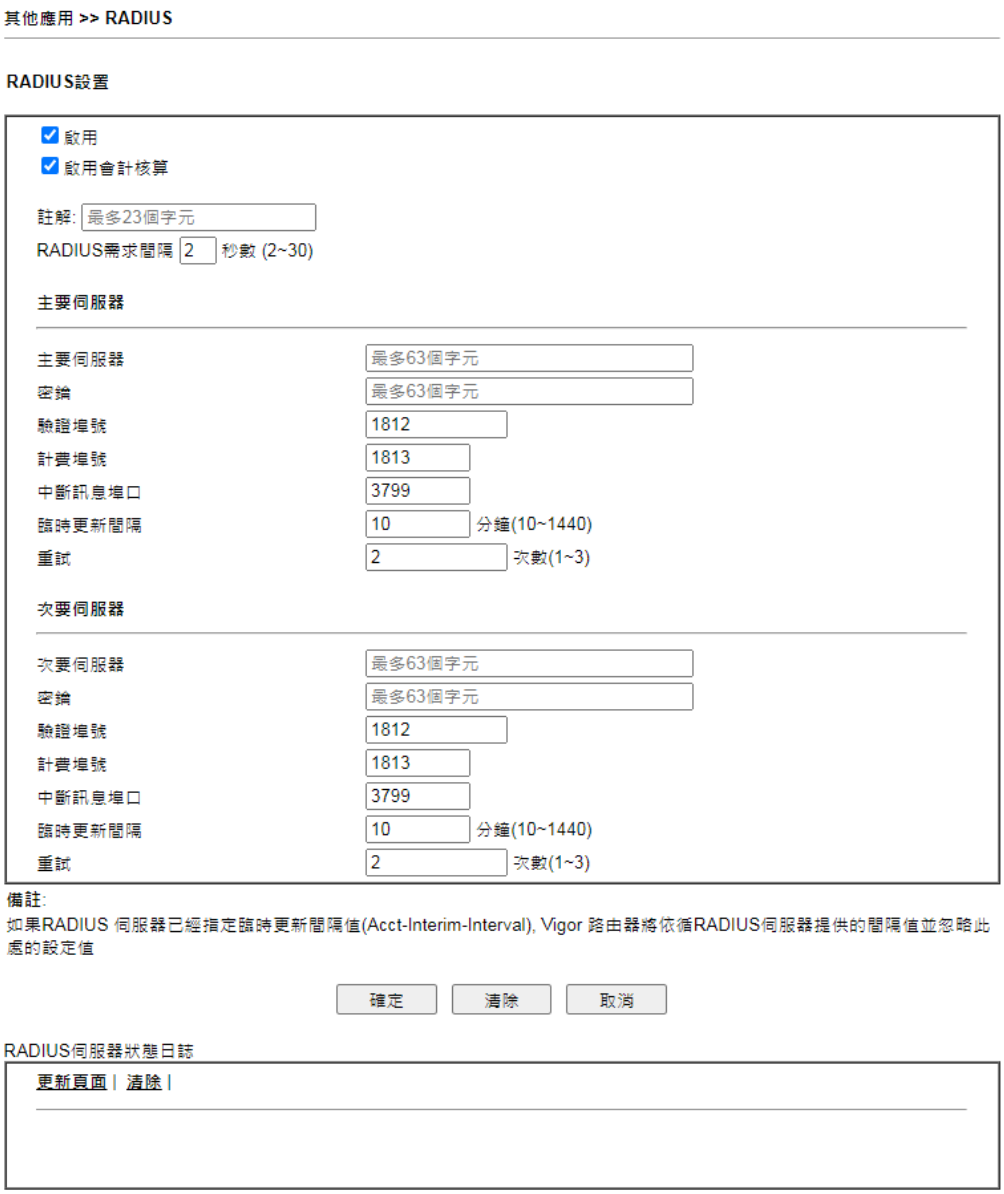
1. 確定 PPPoE 連線和**時間設定**都能正常運作。
2. 設定 PPPoE 每天早上 9:00 到下午 18:00 都保持連線狀態。
3. 設定每天晚上 18:00 到第二天早上 9:00 都是強迫停用狀態。
4. 在PPPoE網際網路存取設定檔中，指定此二個設定檔，現在PPPoE會依照時間排程，**強迫啟用**與**強迫停用**來計畫其網際網路連線。

II-5-5 RADIUS

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。

內建 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。

Vigor 路由器可以當成 RADIUS 用戶端使用，因此本頁可用來調整外接 RADIUS 伺服器的相關設定，之後路由器的 LAN 使用者將由此伺服器進行網路應用驗證。



可用設定說明如下：

項目	說明
啟用	勾選此項以啟動 RADIUS 設定。 **註解** - 輸入此設定檔的簡易說明。

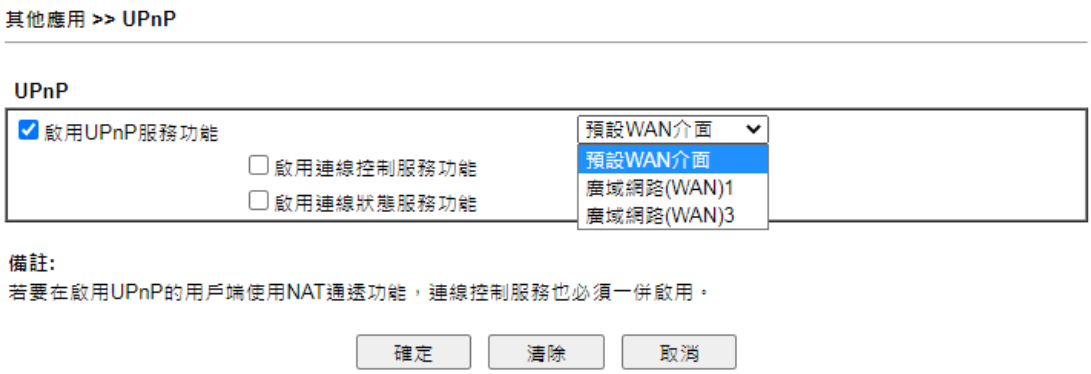
	RADIUS 需求間隔 - 設定路由器等待 RADIUS 伺服器回應的時間，若無收到任何回應，路由器將會再度傳送驗證需求。 **啟用會計核算** - RADIUS 會計是RADIUS伺服器的網路客戶計費機制。 若啟用此功能，路由器將定期傳送計費請求(例如 IP 位址、用戶流量)至指定的 RADIUS 伺服器。 ● **計費埠號** - 設定 UDP 埠號(預設值為 1813) 。 ● **中斷訊息埠號** - 設定 UDP 埠號(預設值為 3799)以便接收 AAA 伺服器傳過來的中斷請求封包。要注意的是這些封包在被 AAA 伺服器中斷連線之前，已為 RADIUS 伺服器接受。 ● **臨時更新間隔** - 設定數值(預設值為 10 分鐘)，表明特定連線數每次傳輸的臨時更新間隔時間。
主要伺服器	**主要伺服器**- 輸入 RADIUS 伺服器的 IP 位址。 **密鑰** - RADIUS 伺服器與用戶共享一個密鑰，用來驗證彼此之間訊息傳送。 **驗證埠號** - RADIUS 伺服器使用的 UDP 埠號，預設值為 1812 以 RFC 2138 標準為基準。 **重試** - 設定嘗試執行與 RADIUS 伺服器連線的次數，如果此連線(主要伺服器)仍然失敗，則停止連接嘗試，並開始改連接次要伺服器。
主要伺服器	**次要伺服器**- 輸入 RADIUS 伺服器的 IP 位址。 **密鑰** - RADIUS 伺服器與用戶共享一個密鑰，用來驗證彼此之間訊息傳送。 **驗證埠號** - RADIUS 伺服器使用的 UDP 埠號，預設值為 1812 以 RFC 2138 標準為基準。 **重試** - 設定嘗試執行與 RADIUS 伺服器連線的次數，如果此連線(主要伺服器)仍然失敗，則停止連接嘗試，並開始改連接次要伺服器。
RADIUS 伺服器狀態日誌	顯示 RADIUS 伺服器目前狀態之紀錄。

完成上述設定之後，請按下**確定**儲存。

II-5-6 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。對於 NAT 路由器來說，最主要的功能在於“NAT Traversal”，它可讓防火牆內的應用程式得以自動開放通過路由器的埠口。

資訊 某些應用程式需要 UPnP 來運作，像是 PPS, Skype, eMule…等等，如果您對 UPnP 不熟悉，建議您關閉此功能以確保安全。



可用設定說明如下：

項目	說明
啟用 UPnP 服務功能	您可以視情況勾選**啟用連線控制服務**或是**啟用連線狀態服務**。
WAN 介面清單	用來指定套用此功能的 WAN 介面。

有關防火牆與 UPnP 功能之提示:

無法與防火牆軟體配合

在您的電腦上啟用防火牆有可能造成 UPnP 不正常運作，這是因為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

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

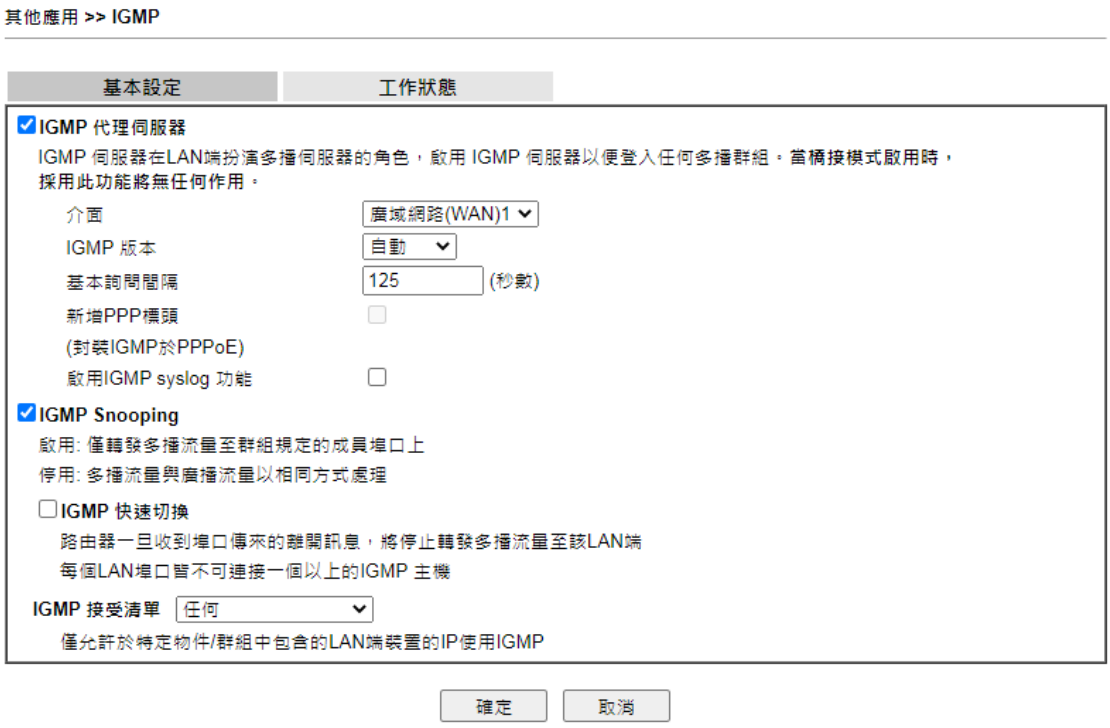
- 某些微軟操作系統已發現到 UPnP 的缺點，因此您需要確定已經應用最新的服務封包。
- 未享有特權的使用者可以控制某些路由器的功能，像是移除和新增通訊埠對應等。

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。

II-5-7 IGMP

IGMP 為 *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。

II-5-7-1 基本設定



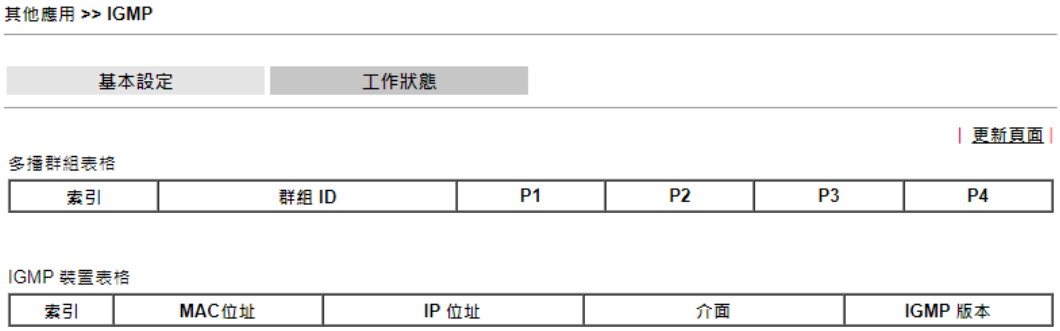
可用設定說明如下：

項目	說明
IGMP 伺服器	勾選此框啟用此功能。多重播送將透過 WAN/PVC/VLAN 埠口來執行。此外，此功能僅在 NAT 模式下可用。 **介面**- 指定封包傳輸的介面。 **IGMP 版本**- 目前路由器支援二個版本(v2 與 v3)，請依照您所訂購的 IPTV 服務選擇適合的版本。 **基本詢問間隔**- 透過發送詢問的方式，路由器會定期檢查從 IPTV 服務中獲取哪個 IP 位址，對用戶來說可能會造成些許不便，因此設定適合的時間(單位：秒)作為詢問的間隔，以限制路由器發送詢問的頻率。 **新增 PPP 標題** - 如果選擇的介面是 PVC/VLAN，請勾選此框。取決於各個 ISP 的規格而定。如果您不知道該如何設定可以連絡您的 ISP 業者取得進一步協助。
IGMP Snooping	勾選此方塊啟用此功能，多重播送流量將會轉送往具有該會員的群組之連接埠中。關閉此功能將會使多重播送流量被視為一般的廣播播送流量。
IGMP 快速切換	勾選此框讓路由器一旦接收切換訊息時，即停止轉送多重播送流量至 LAN 埠口。每個 LAN 埠口都應連上一個 IGMP 主機。

IGMP 接受清單	選擇 IP 物件或是 IP 群組。 只有在 IP 物件或是 IP 群組上列明的 LAN 裝置之 IP 位只允許使用 IGMP。

完成設定之後，按下**確定**鈕儲存相關設定。

II-5-7-2 工作狀態



可用設定說明如下：

項目	說明
頁面更新	按下此連結更新多重播送群組狀態。
索引	多播群組的索引編號。
群組 ID	此區顯示多重播送群組的 ID 連接埠，可用範圍為 224.0.0.0 至 239.255.255.254。
P1 到 P4	多重播送群組中所使用的 LAN 連接埠。

II-5-8 透過 LAN/WAN 喚醒電腦

II-5-8-1 透過 LAN 網路喚醒(Wake on LAN)

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。

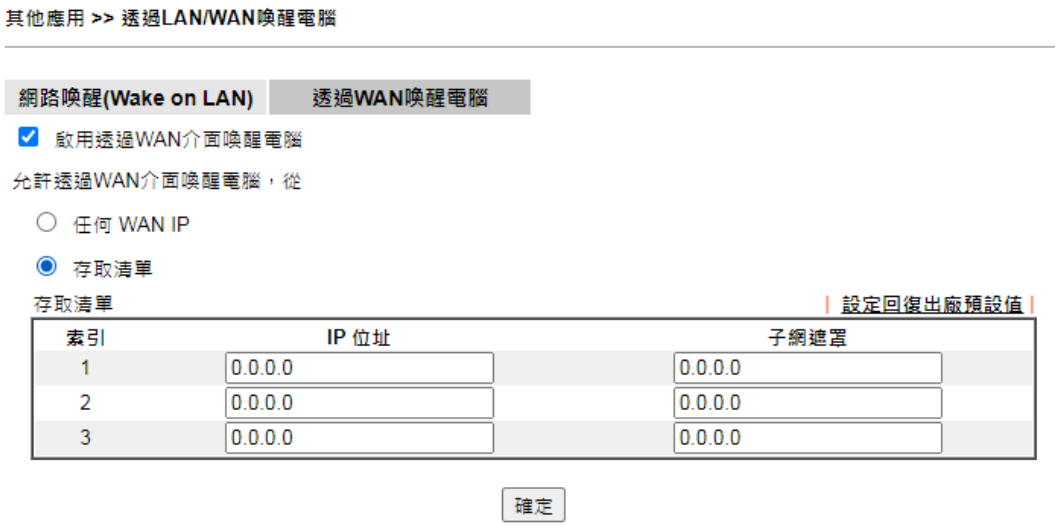
此外，此台電腦必須安裝有支援 WOL 功能的網卡，並在 BIOS 設定中開啟 WOL 功能。

可用設定說明如下：

項目	說明
喚醒方式	有二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。
IP 位址	已在**防火牆>>綁定 IP 至 MAC(Firewall>>Bind IP to 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。
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。

II-5-8-2 透過 WAN 網路喚醒(Wake on WAN)

設定透過 WAN 網路喚醒(Wake on WAN)，請開啟**其他應用 >> 透過 LAN/WAN 喚醒電腦** 並選擇透過 WAN 喚醒電腦。



可用設定說明如下：

項目	說明
啟用透過 WAN 介面喚醒電腦	勾選此框啟用此功能。
允許透過 WAN 介面喚醒電腦，從	設定開機封包(透過遠端裝置)傳送致遠端裝置的路徑。 **任何 WAN IP** -任何 WAN IP 可以做為喚醒遠端裝置的路徑。 **存取清單** - APP 傳送開機封包)已便連接至 Vigor 路由器網路。開機封包將會透過 WAN IP 或是存取清單上的 IP 位址傳送到遠端裝置。

II-5-9 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。

II-5-9-1 簡訊警示

本頁讓您指定簡訊服務供應商、收信人為何以及收信內容。

可用設定說明如下：

項目	說明
啟用	勾選此方框啟用設定檔。
簡訊服務供應商	使用下拉式清單選則簡訊服務供應商。 您可以點**簡訊服務供應商**連結來定義 SMS 簡訊伺服器。
接收者號碼	輸入收信人的電話號碼。
通知設定檔	使用下拉式清單選擇訊息設定檔。收信人將會收到通知設定檔內的訊息。 您可以點**通知設定檔**連結來定義簡訊的內容。
排程 (1-15)	輸入簡訊發出的時間排程編號。 您可點**排程(1-15)**連結來定義排程內容。

完成設定之後，按下**確定**按鈕儲存相關設定。

II-5-10-2 郵件警示

本頁讓您指定郵件伺服器設定檔，收信人為何以及收信內容。

可用設定說明如下：

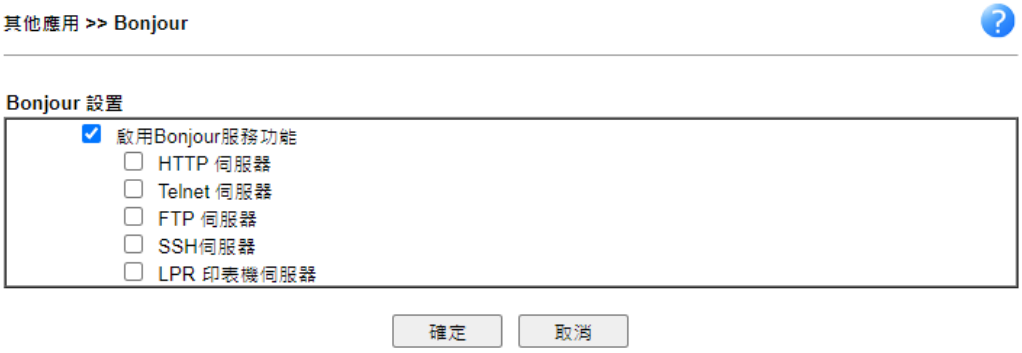
項目	說明
啟用	勾選此方框啟用設定檔。
郵件服務	使用下拉式清單選擇郵件服務物件。所有可用的物件皆可在**物件設定>>簡訊/郵件服務物件**建立。 您可以點**郵件服務**連結來定義郵件伺服器。
郵件位址	輸入收信人的電子郵件信箱。
通知設定檔	使用下拉式清單選擇訊息設定檔。收信人將會收到通知設定檔內的訊息。 您可以點**通知設定檔**連結來定義簡訊的內容。
排程(1-15)	輸入簡訊發出的時間排程編號。 您可點**排程(1-15)**連結來定義排程內容。

完成設定之後，按下**確定**按鈕儲存相關設定。

II-5-11 Bonjour

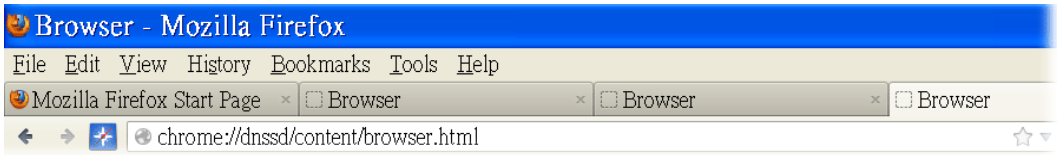
通常，使用者必須設定路由器或是個人電腦來使用各式各樣的服務，但有時候，設定很繁雜(出如 IP 設定、埠號設定等等)也不容易完成。這個功能的目的就是在降低設定的配置程度，如果主機與使用者的電腦安裝了 Bonjour 外掛驅動程式，它們就可透過點選路由器名稱圖示的方式來使用路由器提供的服務。簡單來說，用戶/使用者只要知道路由器的名稱就夠了。

要啟用 Bonjour 服務，請開啟**其他應用>>Bonjour**，勾選您想要分享區域網路用戶的服務項目。

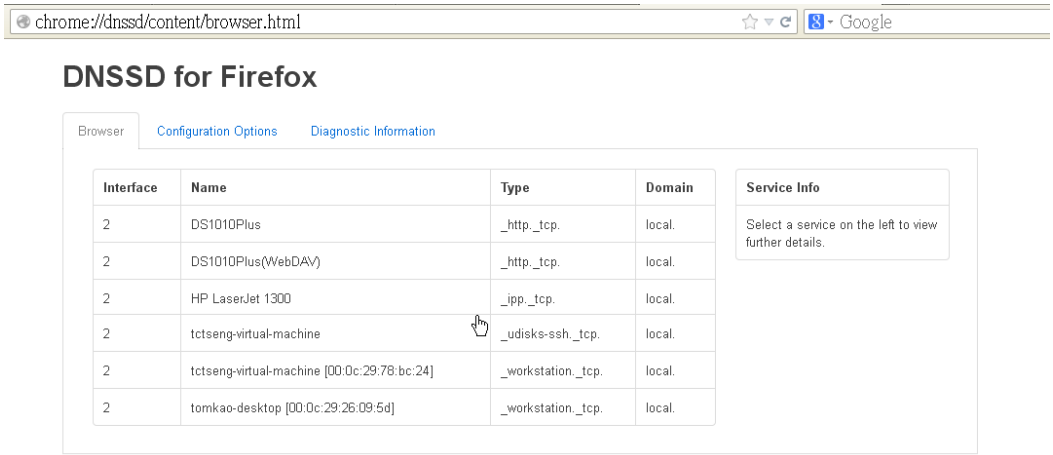


下面提供一個簡單的範例來應用 bonjour 功能：

1. 此處我們使用 Firefox 與 DNSSD 來說明，請先確認 Bonjour 用戶端程式與 Firefox 的 DNSSD 已經安裝在電腦上。



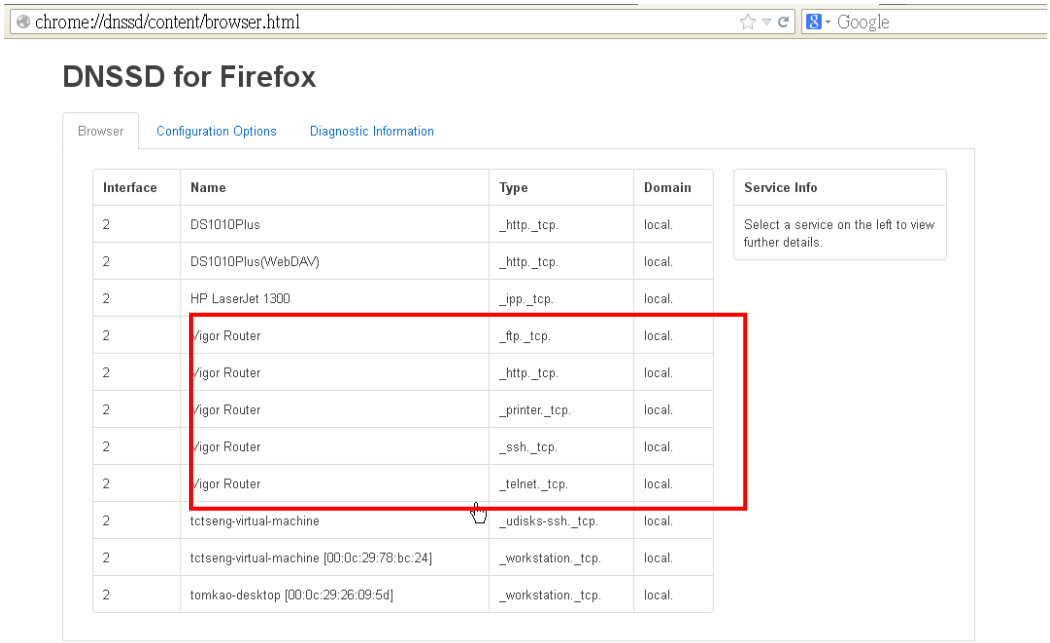
2. 在 Firefox 網頁瀏覽器上，如果 Bonjour 與 DNSSD 已經安裝完畢，您可以開啟相關網頁並看到如下的結果：



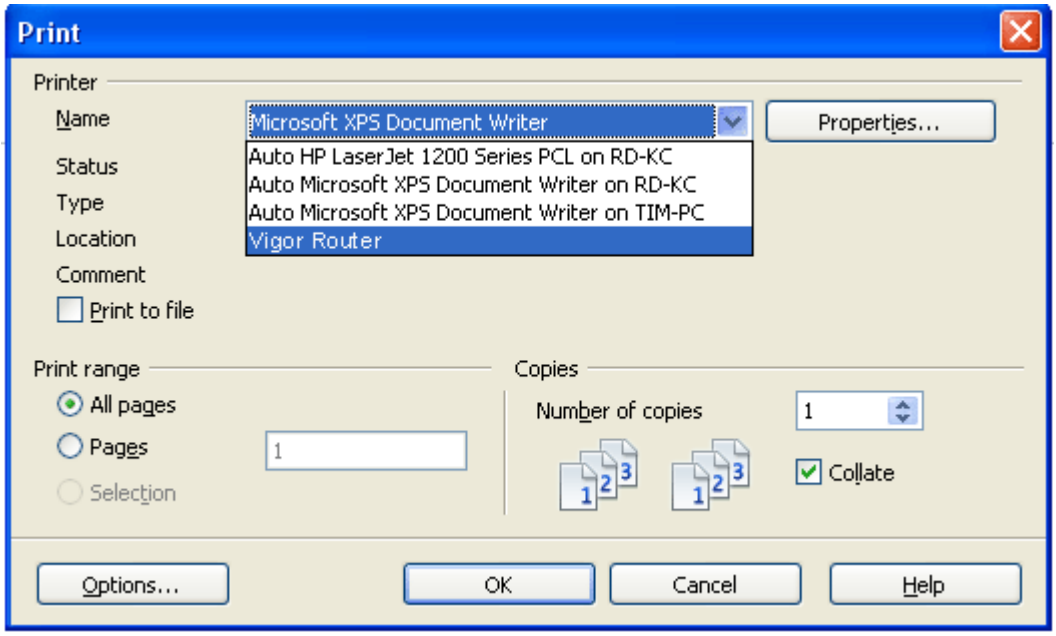
3. 開啟**系統維護>>管理**，輸入**路由器名稱**(例如 DrayTek)，然後按下**確定**儲存。

4. 接著，開啟**其他應用>>Bonjour**，勾選您想要透過 Bonjour 分享的服務。

5. 再次打開 DNSSD 頁面，可用的項目變更如下，表示 Vigor 路由器(以 Bonjour 協定為基準)已經準備妥當可以作為印表機伺服器、FTP 伺服器、SSH 伺服器、Telnet 伺服器以及 HTTP 伺服器。



6. 現在，任何頁面或是文件都可以透過 Vigor 路由器(配備有印表機)來列印輸出。



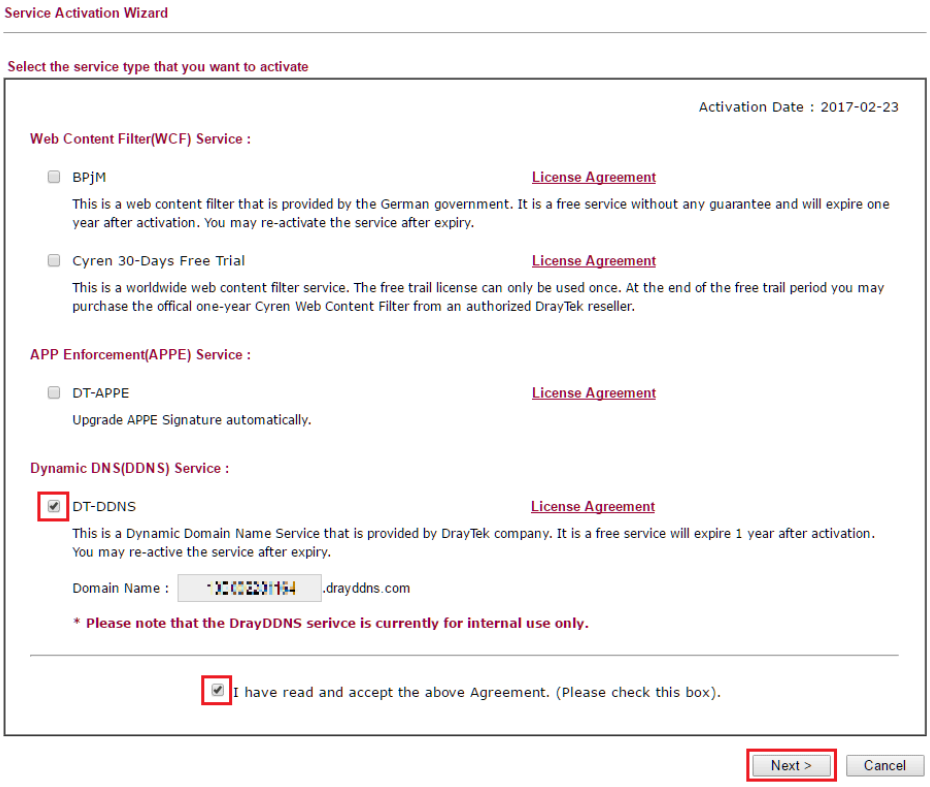
應用說明

A-1 如何使用 DrayDDNS?

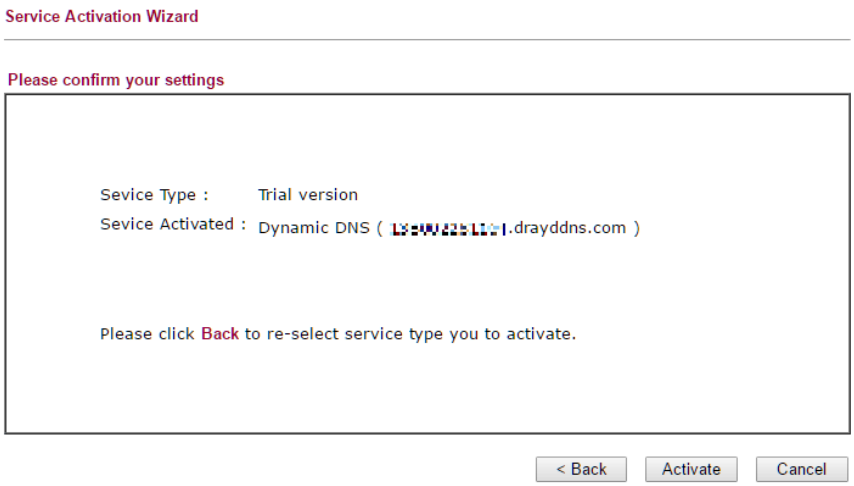
路由器支援不同的 DDNS 服務供應商，使用者可以設定使用者定義之設定檔來更新 DDNS，甚至該服務供應商不在清單上亦可處理。目前，居易開始支援自提的 DDNS 服務，稱為 DrayDDNS，我們將針對每個居易路由器提供網域名稱，此個別的網域名稱可以記錄所有 WAN 介面的 IP 位址。

啟動 DrayDDNS 授權書

1. 開啟**設定精靈>>服務啟用設定精靈**，等待路由器連線到 MyVigor 伺服器，然後勾選 **DT-DDNS** 與 **I have read and accept the above Agreement** 選框，接著按**下一頁**。



2. 確認資訊，按下**啟動(Activate)**。



3. MyVigor 伺服器將回覆服務啟用資訊。

DrayTek Service Activation

Service Name	Start Date	Expire Date	Status
Web Content filter	---	---	Not Activated
APP Enforcement	---	---	Not Activated
DDNS	2017-02-23	2018-02-23	DT-DDNS

Please check if the license fits with the service provider of your signature. To ensure normal operation for your router, update your signature again is recommended.

設定 DDNS 設定檔

1. 開啟**其他應用>>動態 DNS 設定**，

   a. 勾選**啟用動態 DNS 設定**

   b. 選擇可用的設定檔索引編號

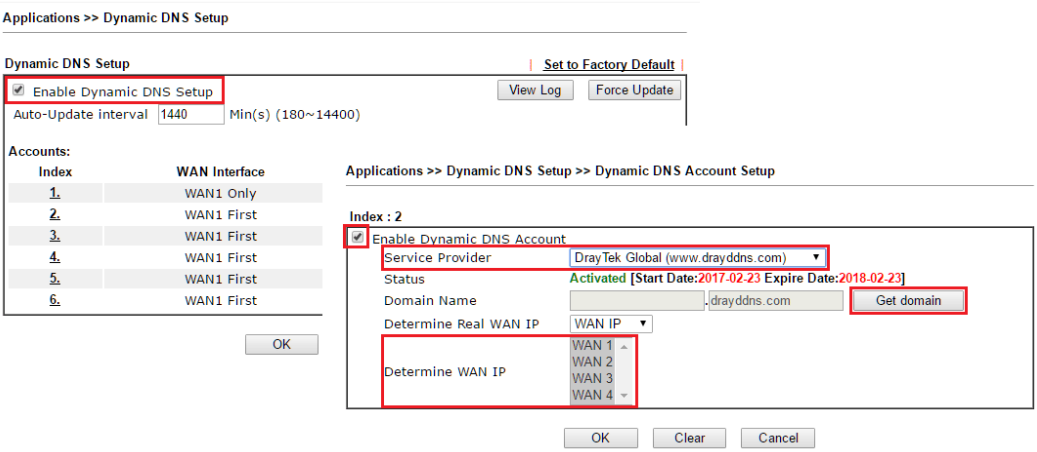
   c. 勾選**啟用動態 DNS 帳號**

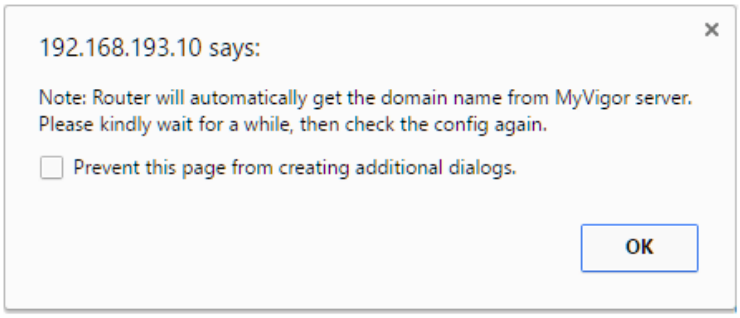
   d. 選擇 **DrayDDNS Global** 作為**服務供應商**

   e. 選擇想要的 WAN 介面以便上傳 IP 至 DDNS 伺服器

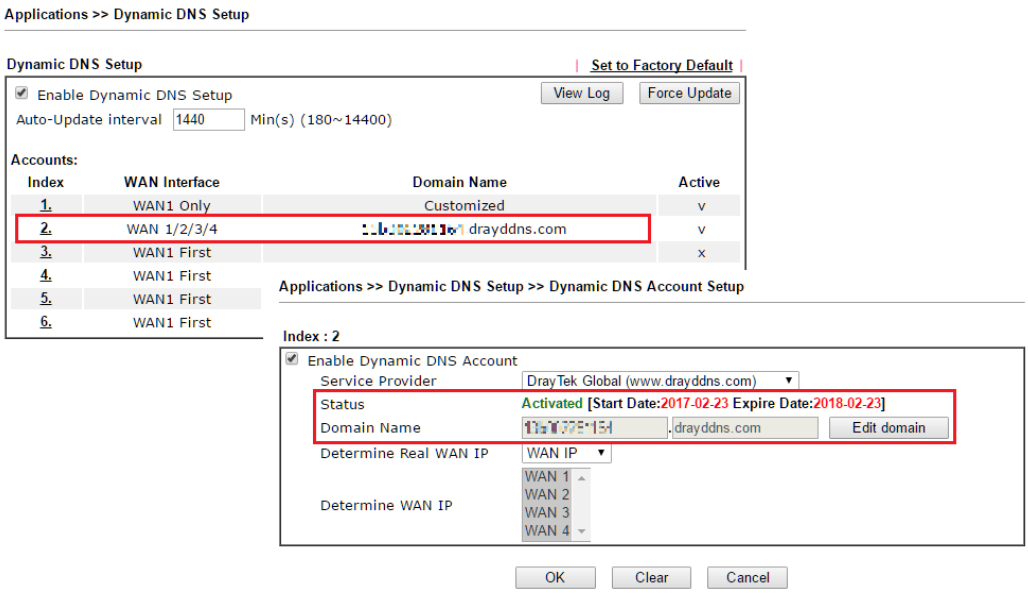
   f. 按下**取得網域**

   g. 在跳出的通知視窗上，按下**確定**





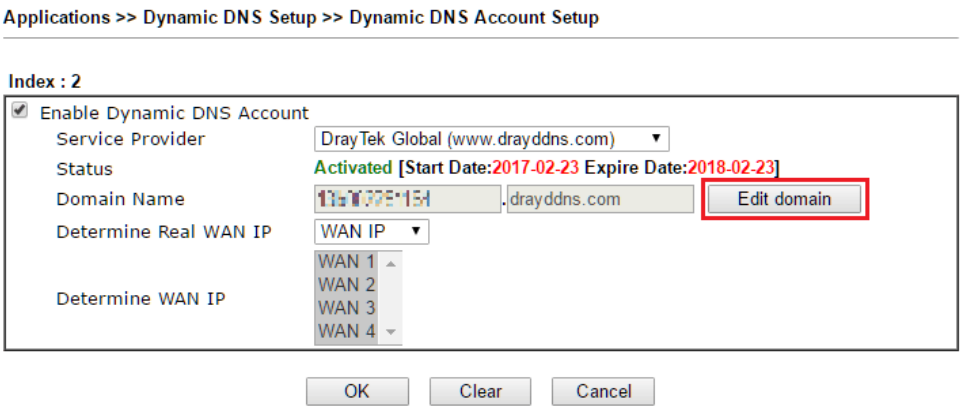
2. 等待數秒讓路由器取得網域名稱，接著我們可以選擇設定檔以便檢查授權書資訊以及網域名稱



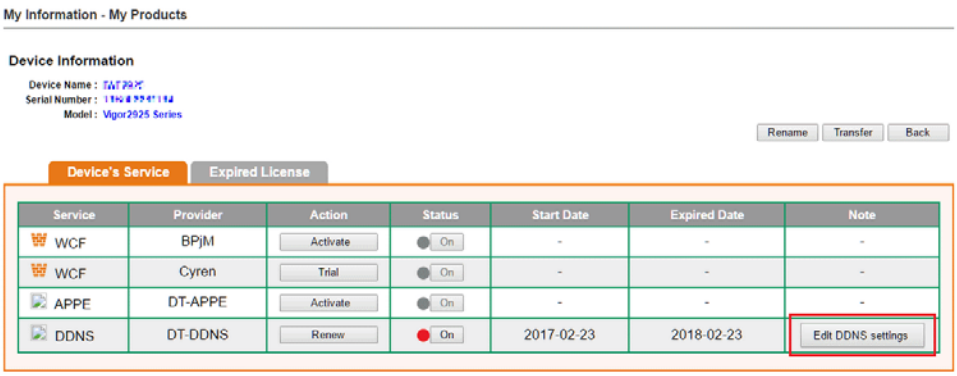
修改網域名稱

目前，只有網域名稱可以修改 MyVigor 網站，我們需要註冊路由器至 MyVigor 伺服器並且登入 MyVigor 網站修改名稱。

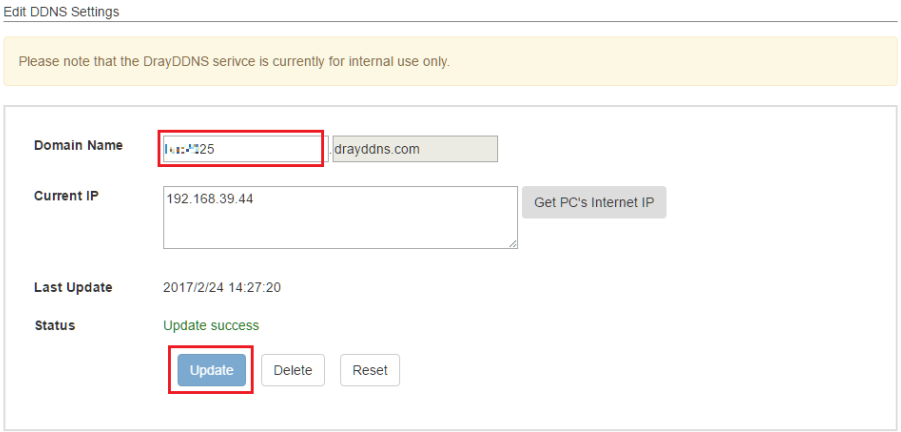
1. 請造訪 https://myvigor.draytek.com/ 或是開啟**其他應用>>動態 DNS 設置>>DrayDDNS 設定檔**，再按下**編輯網域**。



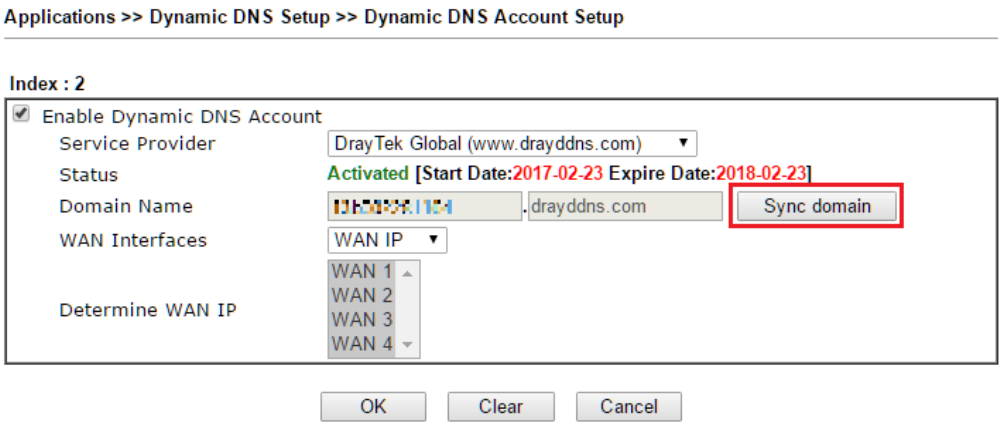
2. 登入 MyVigor 網站，選擇設定檔然後按下**編輯 DDNS 設定(Edit DDNS settings)**。



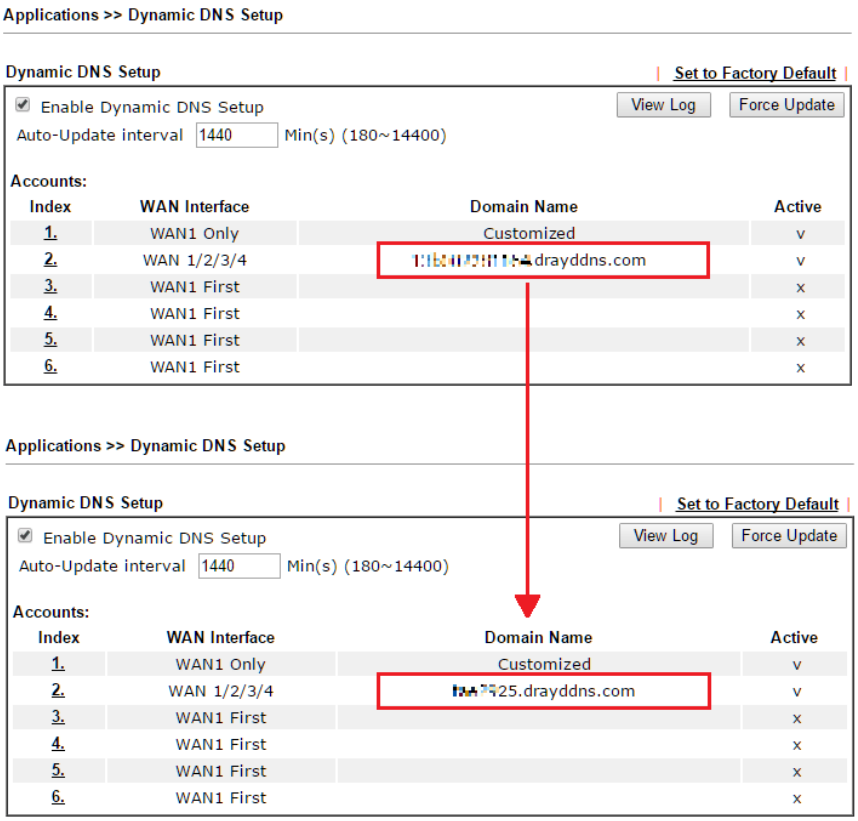
3. 輸入需要的網域名稱(例如 XXXX25)然後按下更新(**Update**)。



4. 當 Vigor 路由器執行下一個 DDNS 更新時，可以取得修正後的網域名稱，我們可以按下**同步網域(Sync domain)**加速處理流程。



數秒後，路由器將取得網域名稱並可顯示在設定檔清單上。


Applications >> Dynamic DNS Setup
Dynamic DNS Setup
Set to Factory Default
Enable Dynamic DNS Setup
View Log
Force Update
Auto-Update interval 1440 Min(s) (180~14400)
Accounts:
Index WAN Interface Domain Name Active
1. WAN1 Only Customized v
2. WAN 1/2/3/4 drayddns.com v
3. WAN1 First x
4. WAN1 First x
5. WAN1 First x
6. WAN1 First x
Applications >> Dynamic DNS Setup
Dynamic DNS Setup
Set to Factory Default
Enable Dynamic DNS Setup
View Log
Force Update
Auto-Update interval 1440 Min(s) (180~14400)
Accounts:
Index WAN Interface Domain Name Active
1. WAN1 Only Customized v
2. WAN 1/2/3/4 25.drayddns.com v
3. WAN1 First x
4. WAN1 First x
5. WAN1 First x
6. WAN1 First x

II-6 路由

策略路由(又稱為 PBR，策略式路由) 功能允許您設定事先規則或是策略供後續使用，如果有某個封包符合任何一條策略的定義，該封包將會被導入指定的介面中。您可以為了因應負載平衡、網路安全性、路由方針等各種不同的理由來設定策略。

透過通訊協定、IP 位址、埠號與介面設定，策略路由可以用來配置任何路由規則來符合實際的需要。一般來說，策略路由可以輕易達到如下的目的：

負載平衡

您可以手動建立各種策略來平衡通過網路介面上的資訊流量。

指定介面

透過指定介面(WAN/LAN/VPN)，資料可以從來源 IP 傳送到目的 IP。

位址對應

允許您針對內部虛擬 IP 位址或是一定範圍的虛擬 IP 位址，指定對外 WAN IP 位址。

優先權

依據固定路由與策略路由的優先權設定，路由器可決定採用哪種策略來傳輸封包。

故障轉移/故障恢復

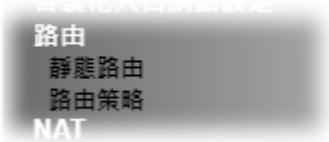
當原始介面斷線時(故障)，封包將透過其他介面或是依循策略規則傳送出去。一旦原始介面恢復運作(故障恢復)了，封包也會立刻回到原始介面傳輸。

其他路由

指定路由策略來決定資料傳輸的方向。

資訊	有關策略路由的詳細資訊，可以參考居易官網 www.draytek.com 的技術支援部份。

網頁使用者介面



II-6-1 靜態路由(固定路由)

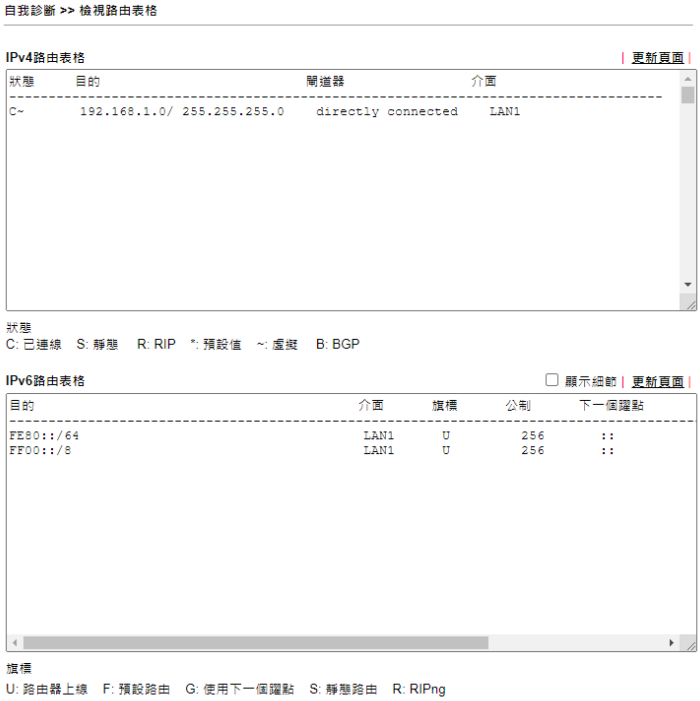
固定路由是動態路由的另一種選擇，它是系統網路管理者透過設定路由器的必要資訊以利封包轉送的一種過程，

開啟**路由>>靜態路由**，路由器提供 IPv4 與 IPv6 頁面設定固定路由，二種協定會帶來不同的網頁設定內容。

靜態路由(IPv4)

可用設定說明如下：

項目	說明
索引編號	索引編號下的號碼(1 到 40)可讓您開啟次頁面設定固定路由。
啟用	勾選此框啟用此固定路由設定檔。
目的位址	顯示固定路由的目的位址。
遮罩	顯示遮罩位址。
閘道器	顯示閘道 IP 位址。

介面	顯示路由經由介面。
設定回復出廠預設值	清除所有設定並回到出廠的設定狀態。
檢視路由表	開啟畫面檢視目前的路由狀況。 
備份	按此備份靜態(固定)路由設定內容。
還原	按此還原靜態(固定)路由設定。執行之前，請務必先上傳設定檔至路由器上。

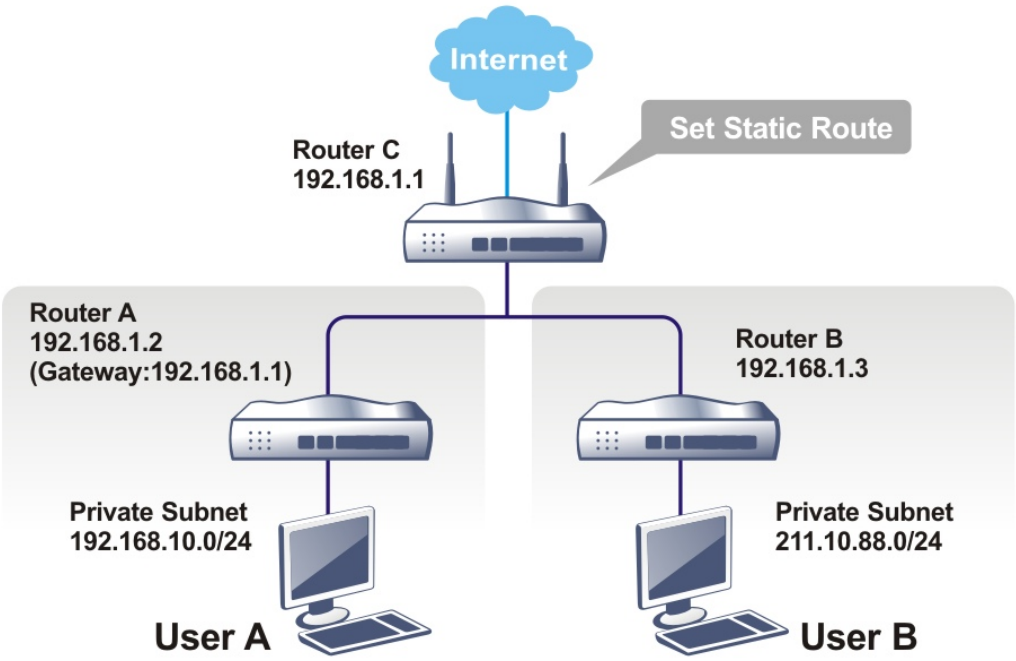
當您完成上述的設定之後，請按**確定**按鈕來啟動設定。

增加固定路由至虛擬或真實網路上(以 IPv4 為基準)

此處為固定路由的範例，不同子網路上的使用者 A 與 B 可以透過路由器彼此溝通。假定網際網路的存取已設定完畢，路由器可以適當的運作。

- 使用主要路由器進入網際網路
- 利用內部的路由器 A(192.168.1.2)，建立虛擬子網路 192.168.10.0
- 透過內部的路由器 B(192.168.1.3)，建立真實子網路 211.100.88.0
- 已設定主要路由器 192.168.1.1 爲路由器 A (192.168.1.2) 的預設閘道

在設定固定路由之前，使用者 A 無法與使用者 B 溝通，因為路由器 A 只會傳送辨認出的封包至主要路由器的預設閘道。



1. 在**區域網路(LAN)**群組中，選擇**一般設定(General Setup)**。再選擇第一子網路作為 **RIP 協定控制**，然後點選**確定(OK)**按鈕。

資訊	有二個理由讓我們一定要在第一子網路上應用 RIP 通訊協定。第一個理由是區域網路介面可以透過第一子網路(192.168.1.0/24)與鄰近路由器作 RIP 封包交換，第二個，理由是網際網路虛擬子網路上(例如 192.168.10.0/24)的主機群可以藉此路由器存取網際網路資訊，並和不同子網路持續進行 IP 路由資訊交換。

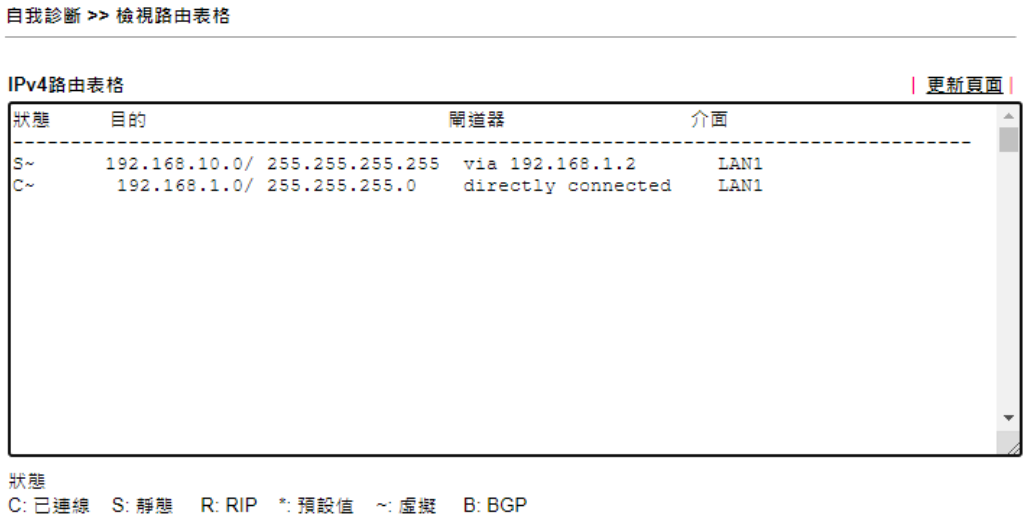
2. 在**路由>>靜態路由**，按索引編號 1 勾選**啟用**方塊， 請以下列數字新增一個固定路由，讓所有應前往 192.168.10.0 的封包都能透過 192.168.1.2 來轉送，接著按**確定**。

可用設定說明如下：

項目	說明
啟用	勾選此框啟用此設定檔。
目的 IP 位址	輸入 IP 位址做為固定路由的目的地。
子網遮罩	輸入此固定路由的子網遮罩。
網路介面	使用下拉式清單指定此固定路由的介面。

3. 回到**固定路由設定**頁面，按另一個索引編號增加另一個固定路由，設定如下圖。它可將所有指定前往 211.100.88.0 的封包轉送至 192.168.1.3，然後按**確定**。

4. 按**自我診斷**中的**路由表**檢查目前的路由表格。



靜態路由(IPv6)

可以設定 40 組 IPv6 固定路由，按下 IPv6 標籤開啟設定頁面。

路由 >> 靜態路由設定

IPv4 | IPv6 | 設定回復出廠預設值 | 檢視 IPv6 路由表格 |

索引	啟用	目的位址	閘道器	介面
1.	☐			
2.	☐			
3.	☐			
4.	☐			
5.	☐			
6.	☐			
7.	☐			
8.	☐			
9.	☐			
10.	☐			
11.	☐			
12.	☐			
13.	☐			
14.	☐			
15.	☐			
16.	☐			
17.	☐			
18.	☐			
19.	☐			
20.	☐			
21.	☐			

可用設定說明如下：

項目	說明
索引編號	索引編號下的號碼(1 到 40)可讓您開啟次頁面設定靜態(固定)路由。
啟用	勾選此框啟用此固定路由設定檔。
目的位址	顯示靜態(固定)路由的目的位址。
閘道器	顯示閘道 IP 位址。
介面	顯示路由經由介面。
設定回復出廠預設值	清除所有設定並回到出廠的設定狀態。
檢視 IPv6 路由表	開啟畫面檢視目前的路由狀況。
備份	按此備份靜態(固定)路由設定內容。
還原	按此還原靜態(固定)路由設定。執行之前，請務必先上傳設定檔至路由器上。

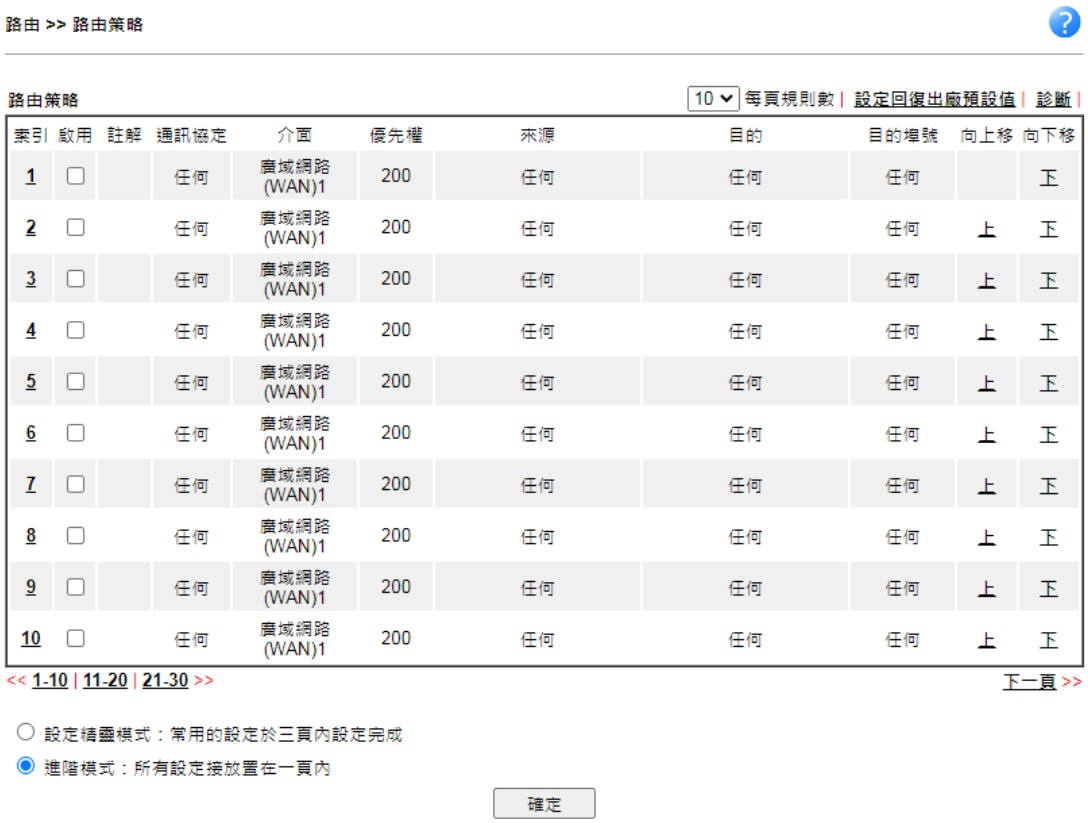
按下任一索引編號連結開啟如下頁面。

可用設定說明如下：

項目	說明
啟用	按此啟用此設定檔。
目的 IPv6 位址/前置碼長度	輸入此設定檔的 IPv6 位址以及前置碼長度。
閘道 IPv6 位址	輸入此設定檔的閘道位址。
網路介面	使用下拉式清單指定此固定路由的介面。

當您完成上述的設定之後，請按**確定**按鈕來啟動設定。

II-6-2 路由策略

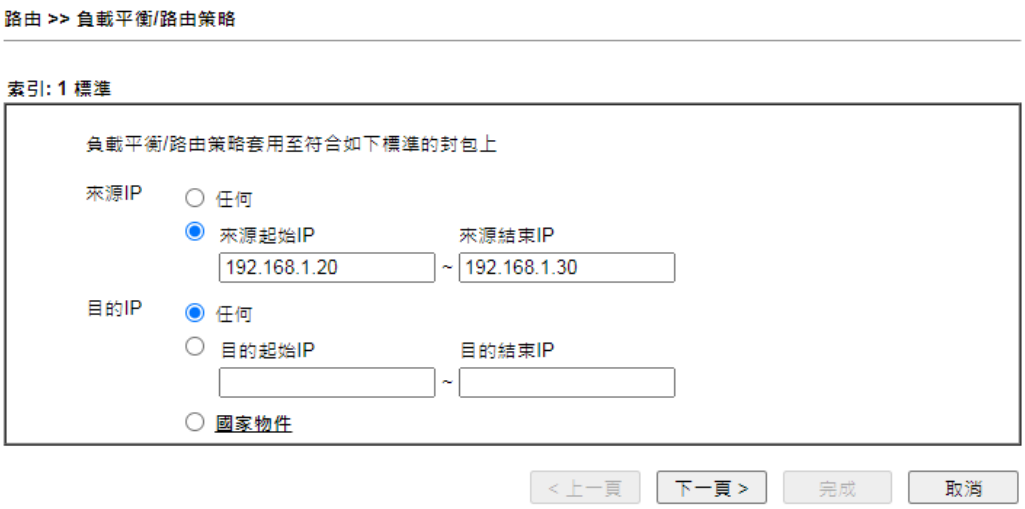


可用設定說明如下：

項目	說明
索引	點下號碼連結即可進入設定頁面。
啟用	勾選此方框啟用此策略設定檔。
通訊協定	顯示用於此路由策略設定檔的協定內容。
介面	顯示此路由策略設定檔指定的封包傳送的介面。
優先權	顯示此路由策略設定檔的優先權數值。
來源	顯示來源 IP、子網、物件或群組內容。
目的	顯示目的 IP、子網、物件或群組內容。
目的埠號	顯示目標埠號的內容。
上/下	使用上移下移連結來移動策略路由的順序。
設定精靈模式	允許透過三個頁面進行策略路由的常用設定。
進階模式	允許設定策略路由的細部設定。

欲使用設定精靈模式，參考如下的設定步驟：

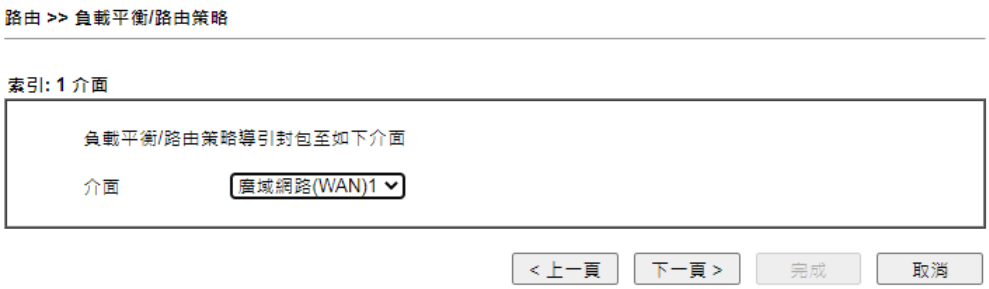
1. 按下**設定精靈模式**按鈕。
2. 點選**索引 1** 連結，開啟如下頁面。



可用設定說明如下：

項目	說明
來源 IP	**任何**- 任何一個 IP 位址皆可視為來源 IP。 **來源啟始 IP** - 輸入指定 WAN 介面的來源 IP 起始位址。 **來源結束 IP** - 輸入指定 WAN 介面的來源 IP 結束位址，如果此區留白，即表示所有區域網路內的來源 IP 皆可通過此 WAN 介面。
目的 IP	**任何**- 任何一個 IP 位址皆可視為目標 IP。 **目的啟始 IP** - 輸入指定 WAN 介面的目標 IP 起始位址。 **目的結束 IP** - 輸入指定 WAN 介面的目標 IP 結束位址，如果此區留白，即表示所有區域網路內的來源 IP 皆可通過此 WAN 介面。 **國家物件** – 指定一個國家物件，所有來自該國家的 IP 都可通過此 WAN 介面。

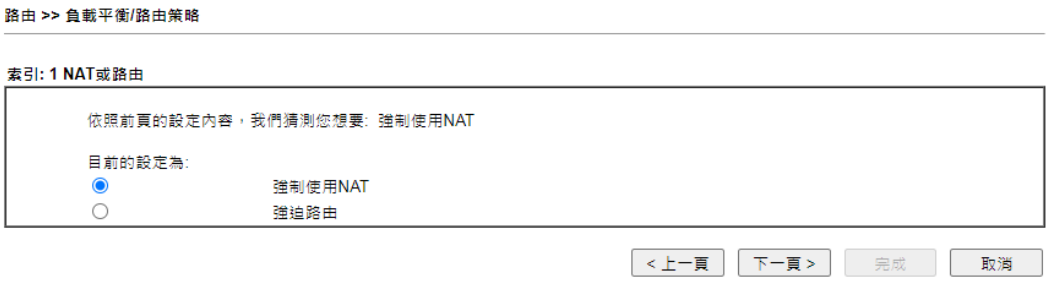
3. 按**下一頁** 開啟下述頁面。



可用設定說明如下：

項目	說明
介面	使用下拉式清單選擇一個 WAN 或是 LAN 介面或是 VPN 設定檔，符合此規定的封包就會透過此介面進行傳輸。

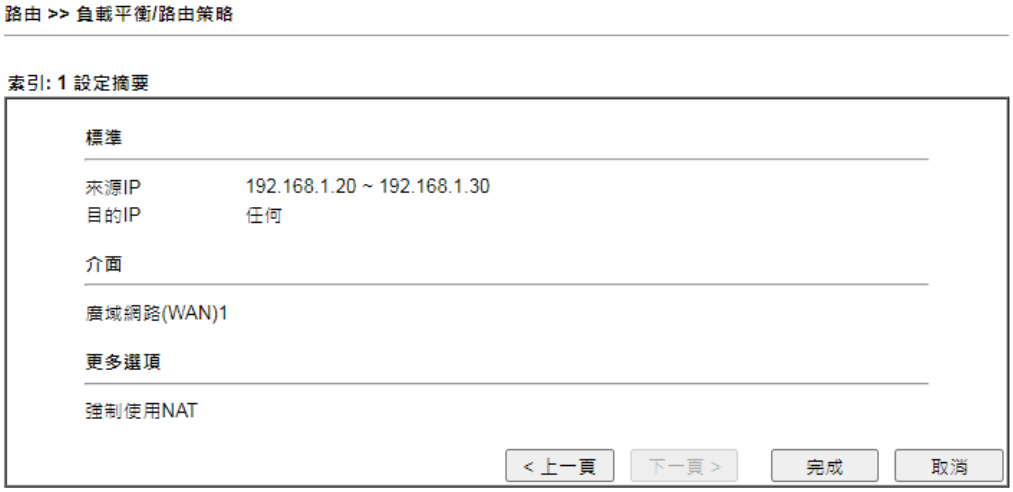
4. 指定完介面後，按**下一頁** 進入次一個設定頁面。



可用設定說明如下：

項目	說明
強制使用 NAT/強迫路由	決定路由器可以使用的機制來轉送 WAN 端的封包。

5. 機制選擇完畢之後，按**下一頁** 查看設定總結內容。



6. 若無任何錯誤，請按**完成**結束設定精靈。

使用進階模式，參考如下的設定步驟：

1. 按下**進階模式**按鈕。
2. 點選**索引**|編號 **1** 連結，開啟如下頁面。

可用設定說明如下：

項目	說明
啟用	勾選此框啟用此策略設定檔。
註解	輸入與此設定檔有關的簡易說明。
通訊協定	使用下拉式清單選擇一個 WAN 或是 LAN 介面或是 VPN 設定檔，符合此規定的封包就會透過此介面進行傳輸。
來源	**任何**- 任何一個 IP 位址皆可視為來源 IP 位址。 **IP 範圍**- 定義一段 IP 範圍作為來源 IP 位址。 ● **起始** - 輸入一個 IP 位址作為此設定檔的來源 IP 的起始位址。 ● **結束**- 輸入一個 IP 位址作為此設定檔的來源 IP 的結束位址。

	IP 子網- 定義子網，包含 IP 位址與遮罩位址。 ● **網路**– 輸入 IP 位址。 ● **遮罩** – 使用下拉式清單選擇適當的網路遮罩。 **IP 物件/IP 群組**- 使用下拉式清單選擇事先設定的 IP 物件/群組。
目的	**任何**- 任何一個 IP 位址皆可視為目標 IP 位址。 **IP 範圍** – 定義一段 IP 範圍作為目標 IP 位址。 ● **起始** - 輸入一個 IP 位址作為此設定檔的目標 IP 的起始位址。 ● **結束** - 輸入一個 IP 位址作為此設定檔的目標 IP 的結束位址。 **IP 子網** – 定義子網，包含 IP 位址與遮罩位址。 ● **網路** – 輸入 IP 位址。 ● **遮罩** – 使用下拉式清單選擇適當的網路遮罩。 **網域名稱** – 指定目標網域名稱。 ● **選擇** – 按此選擇**物件設定>>字串物件**中已經設定好的既有網域名稱。 ● **刪除** – 移除目前使用的網域名稱。 ● **新增** – 建立新的網域名稱作為目的地。 **IP 物件/IP 群組**- 使用下拉式清單選擇事先設定的 IP 物件/群組。 **國家物件**– 使用下拉式清單選擇事先設定的物件，之後該國家內的所有 IP 全都會被視為目標 IP。
目的埠號	**任何** – 任何一個埠號皆可視之為目標埠號。 **目標埠號範圍-** ● **起始 -** 輸入一個埠號為此設定檔的目標 IP 的起始埠號。 ● **結束 -** 輸入一個埠號作為此設定檔的目標 IP 之結束埠號。如果此區留白，即表示所有區域網路內的目標埠號可通過此 WAN 介面。
若符合下述標準則轉發	**介面** – 使用下拉式清單選擇 WAN 或是 LAN 介面或是 VPN 設定檔。符合上述原則的封包就會透過這裡所選的介面來傳輸。 **閘道器**-當您想轉送封包至需要的閘道上，請輸入指定閘道位址。通常預設閘道為系統預設值。 **封包轉發至 WAN/LAN** – 當您選擇 WAN 介面以應封包傳輸，您必須指定轉送的方式為何，請選擇**強制使用 NAT** 或是**強迫路由**。 **失效切換** – 勾選此框可在選擇的 WAN 介面中斷連線時，將資料自動利用其它介面((WAN / LAN / VPN / 路由策略)來傳送。 ● **WAN/LAN -** 使用下拉式清單選擇自動備援介面。 ● **VPN -** 使用下拉式清單選擇 VPN 通道做為備援通道。 ● **路由策略 -** 使用下拉式清單選擇既有的路由策略設定檔。 ● **閘道器** – 當您想要轉送封包至指定閘道時可在此輸入指定位址，通常系統會指定預設閘道位址。
優先權	以全部路由或是路由策略為基準傳送封包，路由器將依據固定

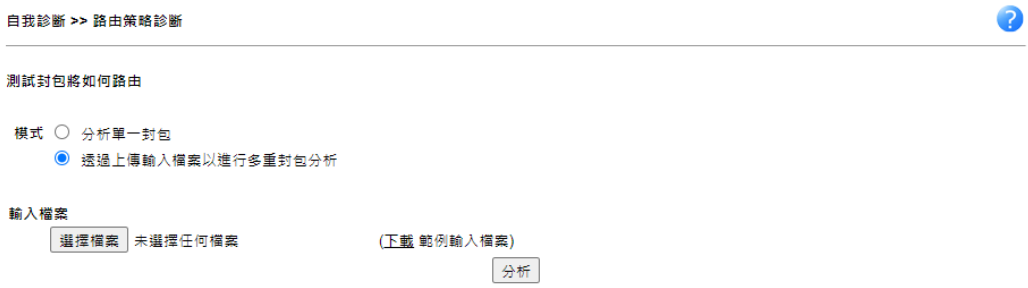
	路由或是路由策略的優先順序，決定採用哪種規則來傳送封包。 數值越大，優先權越低。預設值為 200 代表具有比預設路由還高的優先權。

3. 當您結束設定後，請按下**確定**儲存並離開此頁面。

自我診斷

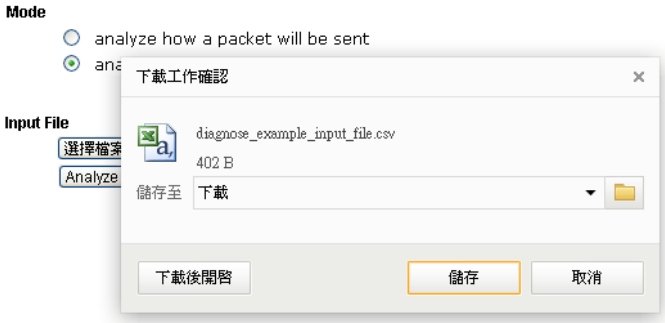
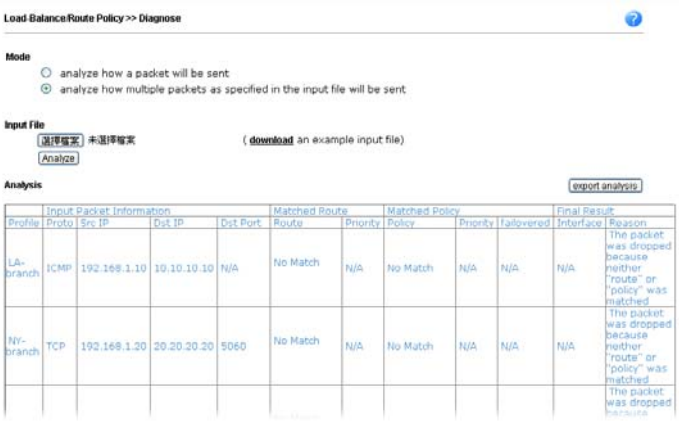
透過觀察此頁面完成的分析作業，管理人員可以追蹤封包傳輸的可能路徑(固定路由、路由表格或是策略路由等等)。

或是



可用設定說明如下：

項目	說明
模式	**分析單一封包-** 選擇此模式以便路由器能針對單一封包進行分析，該封包會如何透過路由策略傳送出去。 **透過上傳輸入檔案以進行多重封包分析 -** 選擇此模式以便路由器能針對指定檔案中的多重封包進行分析，這些封包會如何透過路由策略傳送出去。

封包資訊	指定由路由器分析的封包性質。 **通訊協定 -** 指定一種協定(**ICMP/UDP/TCP/ANY**)以應診斷之需。 **來源 IP** – 輸入一個 IP 位址作為來源 IP。 **目的 IP** – 輸入一個 IP 位址作為目標 IP。 **目的埠號** – 使用下拉式清單指定一個目標埠號。 **分析** – 按此鈕執行分析工作。分析的結果將會顯示在本頁上，如有必要，可以按下輸出分析按鈕將結果以檔案的方式儲存起來。
輸入檔案	**選擇檔案** – 按下載連結取得空白範例檔案，接著按此鈕選擇該空白“.csv” 檔案以儲存分析的結果。  **分析** – 按此執行分析作業，分析的結果將會顯示在頁面上，如有必要可以按書出分析按鈕將結果以檔案輸出。  注意分析是以目前的負載平衡/策略路由設定為基準，我們並不擔保能夠與真實例子百分百相同。

第三篇 無線區域網路設定

Wireless

無線區域網路可提供高移動性，因此無線區域網路的用戶能夠同時存取所有區域網路設備，如同有線區域網路以及網際網路一般。

III-1 無線區域網路設定(2.4GHz/5GHz))

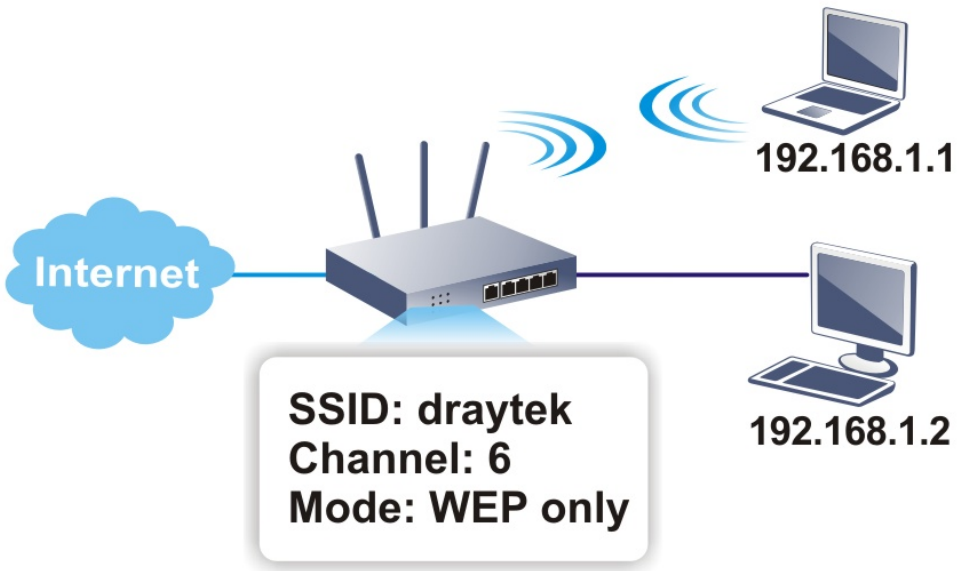
本節所提供的資訊僅針對 *ax* 及 *ac* 系列機型。

在最近幾年無線通訊的市場有了極大的成長，無線技術線在到達了或說是有能力到達地球表面上的每一個點，數以百萬的人們每天透過無線通訊產品彼此交換資訊，Vigor G 系列路由器，又稱為 Vigor 無線路由器，被設計成為一個適合小型辦公室/家庭需要的路由器，擁有最大的彈性與效率，任何一個被授權的人，都可以攜帶內建的無線區域網路用戶端 PDA 或是筆記型電腦，進入會議室開會，因而不需擺放一堆亂七八糟的纜線或是到處鑽孔以便連線。無線區域網路機動性高，因此無線區域網路使用者可以同時存取所有區域網路中的工具，以及遨遊網際網路，好比是以有線網路連接的一樣。

Vigor 無線路由器皆配有與標準 802.11n draft 2 通訊協定相容之無線區域網路介面，爲了進一步提高其效能，Vigor 路由器也承載了進階無線技術以便將速率提升至 300 Mbps*，因此在最後您可以非常順利的享受流暢的音樂與影像。

資訊 資料的實際總處理能力會依照網路條件和環境因素而改變，如網路流量、網路費用以及建造材料。

在無線網路的基礎建設模式(Infrastructure Mode)中，Vigor 無線路由器扮演著無線網路基地台(AP)的角色，可連接很多的無線用戶端或是無線用戶站(STA)，所有的用戶站透過路由器，都可分享相同的網際網路連線。**基本設定**可讓您針對無線網路所需的訊息包含 SSID、頻道等項目做基本的配置。



多重 SSID

Vigor 路由器支援四組無線連線 SSID 設定，每個 SSID 都可以定義不同的名稱及上下載速率，方便遠端用戶於尋求無線連線時挑選使用。

即時硬體加密

Vigor 路由器配有 AES 加密引擎，因此可以採用最高級的保護措施，在不影響使用者的習慣之下，對資料達成保護效果。

完整的安全性標準選項

為了確保無線通訊的安全性與私密性，提供數種市場上常見的無線安全標準。

有線對應隱私權(Wired Equivalent Privacy, WEP)是一種傳統的方法，使用 64-bit 或是 128-bit 金鑰透過無線收發裝置來加密每個資料訊框。通常無線基地台會事先配置一組含四個金鑰的設定，然後使用其中一個金鑰與每個無線用戶端通訊聯絡。

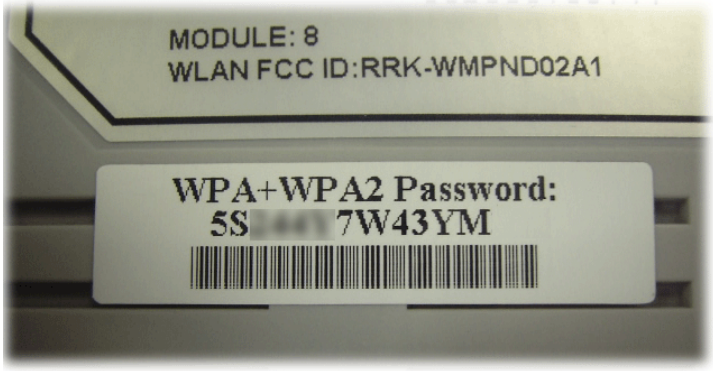
Wi-Fi 保護存取協定(Wi-Fi Protected Access, WPA)是工業上最佔優勢的安全機制，可分成二大類：WPA-personal 或稱為 WPA Pre-Share Key (WPA/PSK)以及 WPA-Enterprise 又稱為 WPA/802.1x。

在 WPA-Personal 機制中，會應用一個事先定義的金鑰來加密傳輸中的資料，WPA 採用 Temporal Key Integrity Protocol (TKIP) 加密資料而 WPA2 則是採用 AES，WPA-Enterprise 不只結合加密也還涵括驗證功能。

由於 WEP 已被證明是有弱點的，您可以考慮使用 WPA 作為安全連線之用。您應該按照所需來選擇適當的安全機制，不論您選擇哪一種安全防護措施，它們都可以全方位的加強您無線網路上之資料保護以及/或是機密性。Vigor 無線路由器是相當具有彈性的，且能同時以 WEP 和 WPA 支援多種安全連線。

資訊

路由器提供預設安全性模式的密碼，在路由器底部的標籤中條列出來。對於想要透過此路由器登入網際網路的無線用戶，請於連線時記得輸入此預設的 PSK 號碼。



分隔無線與有線區域網路

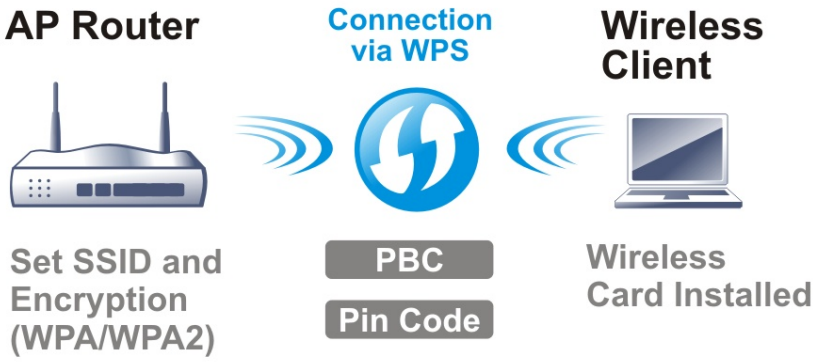
可使您自有線區域網路中，分隔出無線區域網路以便隔離或是限制存取。隔離代表著雙方彼此都無法存取對方的資料，欲詳細說明商業用途之範例，您可以為訪客設定一個無線區域網路，讓他們只能連接到網際網路而不必擔心洩露機密資訊。更彈性的作法是，您可以新增 MAC 位址的過濾器來區隔有線網路之單一使用者的存取行為。

無線區域網路 - 無線用戶端列表

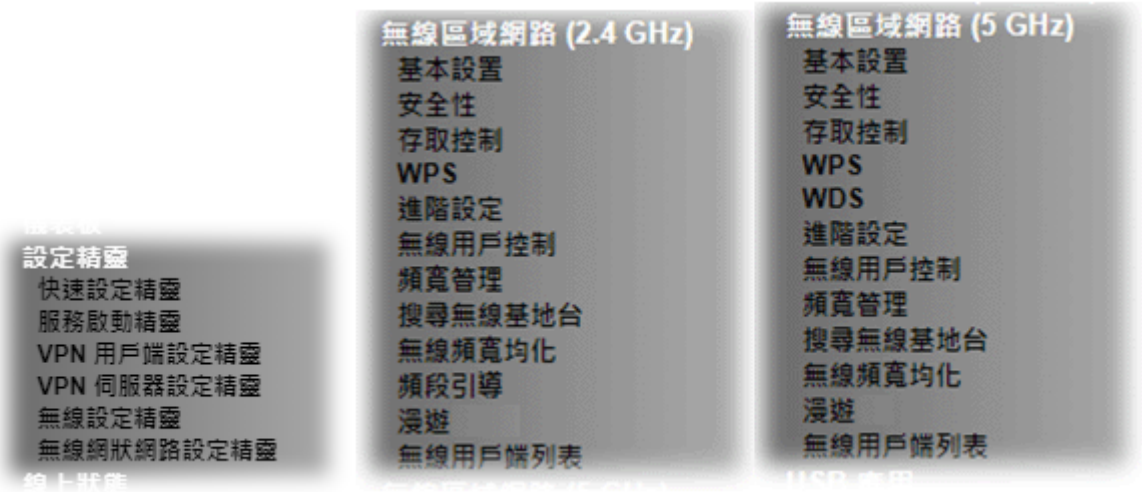
顯示無線網路中全部的無線用戶端以及連接狀態。

WPS

WPS (Wi-Fi Protected Setup) 提供簡易操作流程，讓無線用戶與無線基地台之間以 WPA 和 WPA2 之加密方式，成功完成網路連線。


AP Router
Connection via WPS
Wireless Client
Set SSID and Encryption (WPA/WPA2)
PBC
Pin Code
Wireless Card Installed

網頁使用者介面



III-1-1 無線網路設定精靈

無線網路設定精靈允許您設定主機 AP(針對家庭用途或是公司內部運作)，以及指定客戶 AP(針對任何存取網際網路的無線用戶)之相關設定。

依照下列步驟進行：

1. 開啟**設定精靈>>無線設定精靈**。
2. 設定精靈頁面呈現如下，本頁針對公司或是家庭內部使用者而設定。此外細部設定內容會依照您所使用的路由器機種略有差異。本例是以 Vigor2135ac 系列為範本。

可用設定說明如下：

項目	說明

無線網路 2.4G 設定	
名稱	輸入路由器的 SSID 名稱(SSID1)。預設名稱為 DrayTek。
模式	目前路由器提供的模式包含如圖各項，請選用綜合(11b+11g+11n)模式。
頻道	代表無線區域網路的頻率頻道，預設值為 6，如果選定的頻道受到嚴重的干擾，您可以切換其他頻道，如果對於頻道選擇沒有特定的顧慮，請選擇自動即可。
安全性金鑰	此精靈提供的無線網路密碼模式為 WPA2/PSK。 WPA 利用密鑰針對傳輸的每個訊框進行加密作用，可利用手動輸入 PSK 或是透過 802.1x 驗證進行自動協商。 請輸入 8 至 63 個 ASCII 字元例如 012345678(或是 64 個十六進位數字且開頭為 0x 的內容，如“0x321253abcde...”。
無線網路 5G 設定 - 這個部份是當路由器支援無線網路 5GHz 時可用。	
使用與上述相同的 SSID 與安全性密鑰	勾選此方塊以使用上述相同之設定。
名稱	輸入路由器無線 5GHz 的 SSID 名稱(SSID2)。
模式	目前路由器可以連接的模式。
頻道	代表無線區域網路的頻率頻道，預設值為 36，如果選定的頻道受到嚴重的干擾，您可以切換其他頻道，如果對於頻道選擇沒有特定的顧慮，請選擇自動即可。
安全性金鑰	此精靈提供的無線網路密碼模式為 WPA2/PSK。 WPA 利用密鑰針對傳輸的每個訊框進行加密作用，可利用手動輸入 PSK 或是透過 802.1x 驗證進行自動協商。 請輸入 8 至 63 個 ASCII 字元例如 012345678(或是 64 個十六進位數字且開頭為 0x 的內容，如“0x321253abcde...”。
下一頁	按此進入下一個設定頁面。
取消	按此離開設定精靈，任何設定變更將無法儲存。

3. 輸入完畢必要資訊之後，按**下一頁**。本頁的內容限制無線站台(即客戶端)登入網際網路，但無法分享區域網路(LAN)以及虛擬網路(VPN)的連線。

可用設定說明如下：

項目	說明
無線網路 2.4G 設定	
啟用/停用	啟用或是停用本頁的設定。
SSID	輸入路由器的 SSID 名稱(SSID1) 。
安全性金鑰	此精靈提供的無線網路密碼模式為 WPA2/PSK。 WPA 利用密鑰針對傳輸的每個訊框進行加密作用，可利用手動輸入 PSK 或是透過 802.1x 驗證進行自動協商。 請輸入 8 至 63 個 ASCII 字元例如 012345678(或是 64 個十六進位數字且開頭為 0x 的內容，如“0x321253abcde...”。
頻寬限制	**啟用** – 勾選此框以進行頻寬限制設定。控制透過無線連線的資料傳輸速度。 **總計上傳** – 勾選啟用方塊之後，接著輸入資料上傳的速度，預設值為 30,000 kbps。 **總計下載** – 勾選啟用方塊之後，接著輸入資料下載的速度，預設值為 30,000 kbps。
無線網路 5G 設定	
啟用/停用	啟用或是停用本頁的設定。
使用與上述相同的 SSID 與安全性密鑰	勾選此方框使用上述相同的設定。
SSID	輸入路由器的 SSID 名稱(SSID2) 。
安全性金鑰	此精靈提供的無線網路密碼模式為 WPA2/PSK。 WPA 利用密鑰針對傳輸的每個訊框進行加密作用，可利用手動輸入 PSK 或是透過 802.1x 驗證進行自動協商。 請輸入 8 至 63 個 ASCII 字元例如 012345678(或是 64 個十六進位數字且開頭為 0x 的內容，如“0x321253abcde...”。
下一頁	按此進入下一個設定頁面。
取消	按此離開設定精靈，任何設定變更將無法儲存。

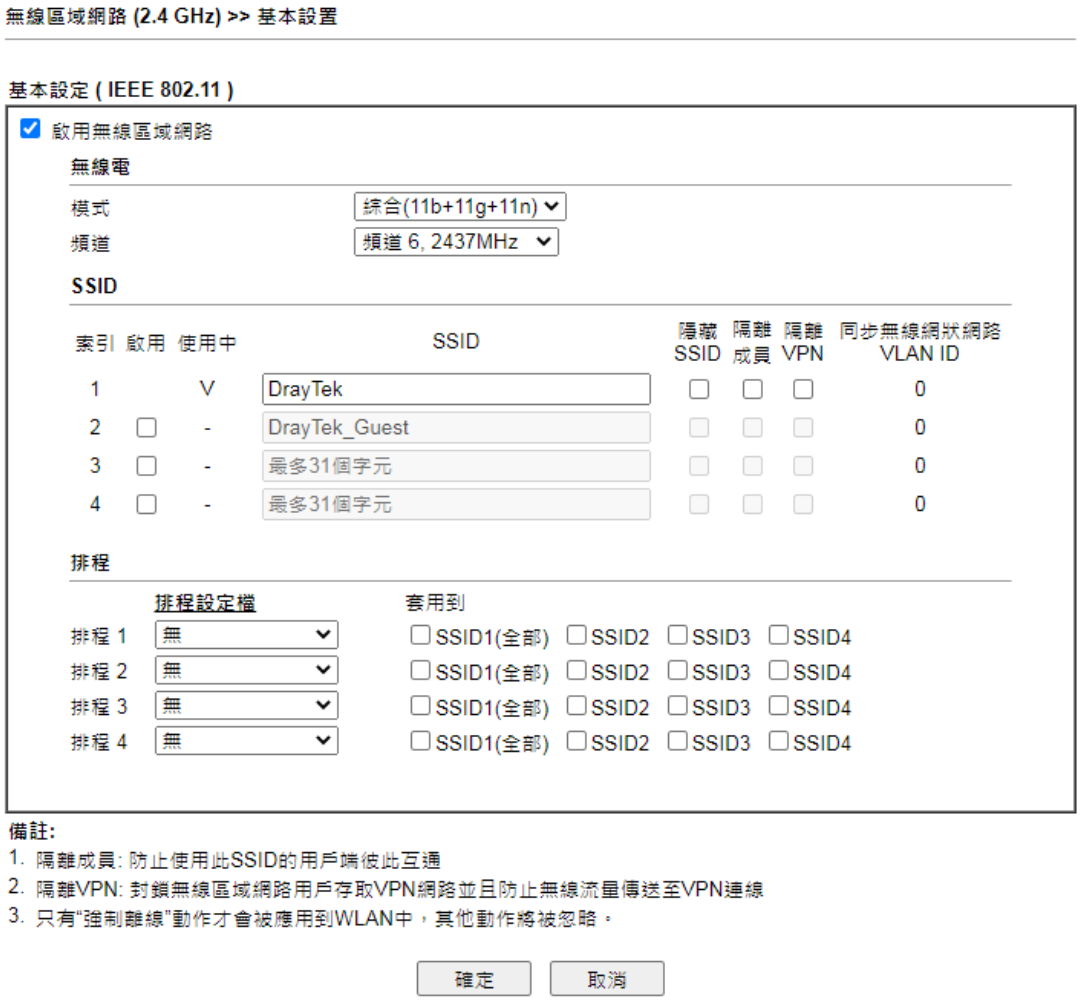
4. 輸入完上述資訊之後，按**下一頁**。

5. 接著螢幕會顯示無線設定的摘要內容。

6. 若無任何疑問，按下**完成**按鈕來結束設定。

III-1-2 基本設置

按下**無線區域網路>>基本設置**，新的網頁即會開啟，您可以設定 SSID 和無線頻道資訊，請參考下圖：



可用設定說明如下：

項目	說明
啟用無線區域網路	勾選此方塊啟動無線功能。
無線電	
模式(Mode)	請選擇一個適當的無線模式。可選之無線模式依照所安裝之路由器機種而定。 **注意**: 802.11b/g 用於 2.4G 頻；802.11a 用於 5G 頻；802.11n 用於 2.4G 或是 5G 頻；802.11ac 用於 5G 頻
頻道(Channel)	無線區域網路的通道頻率，802.11n 與 802.11ac 的預設頻道是不同的，如果選定的頻道受到嚴重的干擾的話，您可自行切換為其他頻道。
SSID	
SSID	預設的 SSID 值為 **DrayTek**，建議您變更為另一個特殊名稱。它

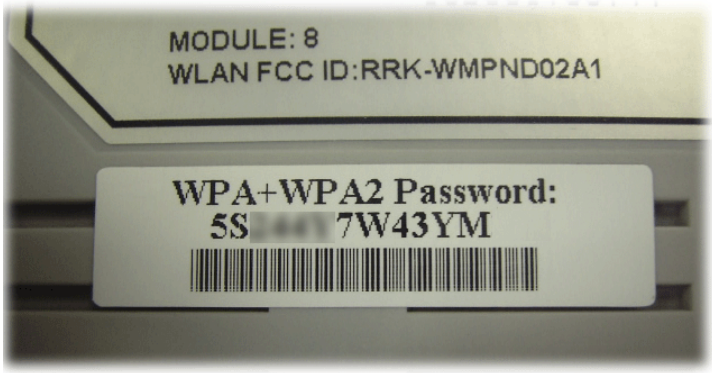
	是無線區域網路的身分辨識碼，SSID 可以是任何文字、數字或是各種特殊字元。
隱藏 SSID	勾選此方塊，防止他人得知 SSID 值，未知此路由器的 SSID 之無線用戶在搜尋網路時，看不到 Vigor 無線路由器的訊息。
隔離(Isolate)	**VPN** – 勾選此方塊讓使用相同 VPN 的無線用戶無法存取彼此的電腦資料。 **成員(Member)**– 勾選此方塊讓使用相同 SSID 的無線用戶彼此無法存取對方資料。
同步無線網狀網路 VLAN ID	顯示 VLAN ID，此 ID 將同步複製到使用相同 SSID 的網狀節點上。
排程	
排程設定檔	設定無線區域網路在特定的時間間隔中運作。您可以從**應用**的**排程設定(Applications >> Schedule)**頁面上，自 15 個排程中選擇 4 個，本區預設值是空白的，表示無線功能是永遠可以運作的狀態。
套用到	選定的 SSID (2 /3 /4) 將在使用的排程設定檔安排下，強行上線/下線。

完成設定之後，按下**確定**按鈕儲存相關設定。

III-1-3 安全性設定

本頁讓使用者對 SSID 1,2,3 及 4 設定不同模式的安全性規則，設定完後，請按下**確定**按鈕儲存所有的變更。

路由器提供預設安全性模式的密碼，在路由器底部的標籤中條列出來。對於想要透過此路由器登入網際網路的無線用戶，請於連線時記得輸入此預設的 PSK 號碼。



選擇**無線區域網路>>安全性**後，新的網頁將會出現，您可以在此頁面上調整 WEP 和 WPA 設定。

可用設定說明如下：

項目	說明
模式	此一設定有數種模式可供您選擇。 **資訊** 若有選擇了 802.1x 模式，那麼您還需要同時設定**其它應用>>RADIUS**。 **停用** - 關閉加密機制。 **WEP** - 只接受 WEP 用戶以及僅接受以 WEP 金鑰輸入的加密鑰匙。 **限用 WEP/802.1x** - 僅接受 WEP 用戶端以及得自 RADIUS 伺服器(含 802.1X 協定)動態分配之密鑰。 **限用 WPA/802.1x** - 僅接受 WPA 用戶端以及得自 RADIUS 伺服器(含 802.1X 協定)動態分配之密鑰。 **限用 WPA2/802.1x** - 僅接受 WPA2 用戶端以及得自 RADIUS 伺服器(含 802.1X 協定)動態分配之密鑰。 **綜合(WPA+WPA2)/限用 802.1x** - 同時接受 WPA 與 WPA2 用戶端以及得自 RADIUS 伺服器(含 802.1X 協定)動態分配之密鑰。 **WPA/PSK** - 接受 WPA 用戶，請在 PSK 中輸入加密金鑰。 **WPA2/PSK** - 接受 WPA2 用戶，請在 PSK 中輸入加密金鑰。 **綜合(WPA+ WPA2)/PSK** - 同時接受 WPA 與 WPA2 用戶，請在 PSK 中輸入加密金鑰。

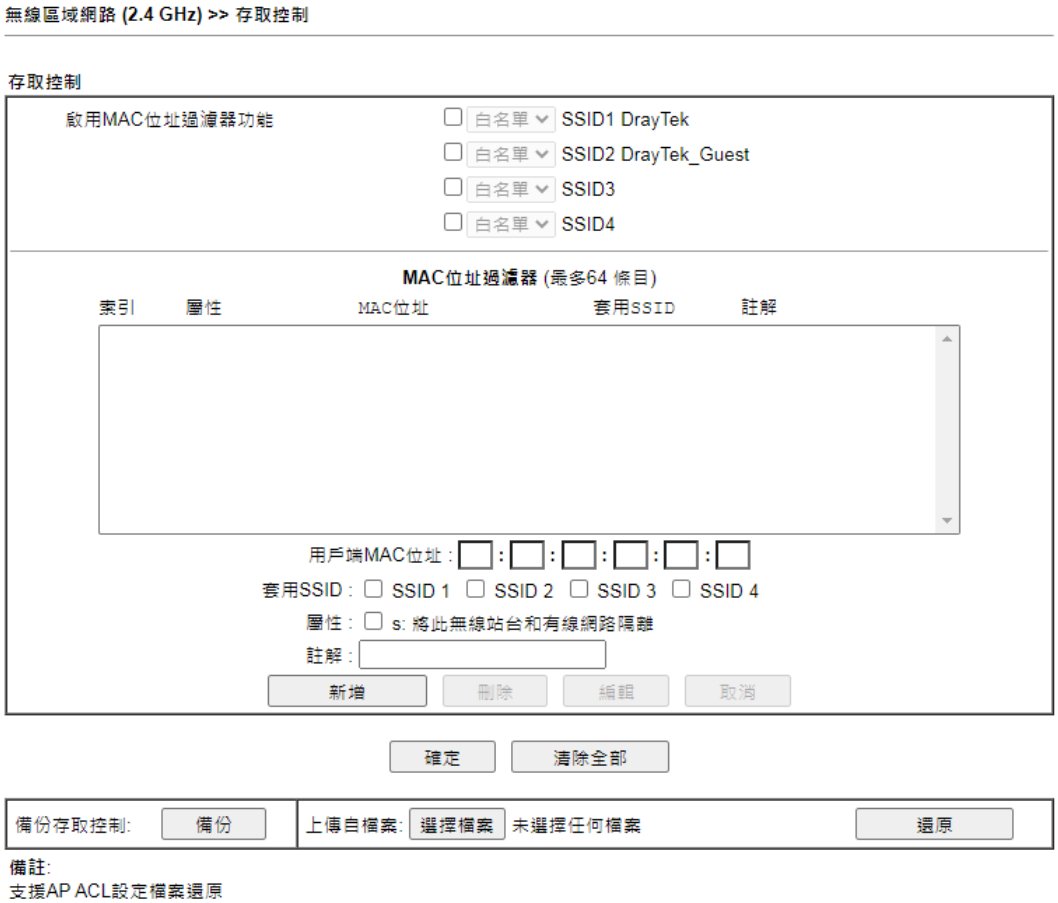
	WPA3/SAE - 接受 WPA3 用戶，請在 PSK 中輸入加密金鑰。 **綜合(WPA2+ WPA3)/SAE** - 同時接受 WPA2 與 WPA3 用戶，請在 PSK 中輸入加密金鑰。 **OWE** - WPA3 也同時採用新的開放且安全的連線模式 "Opportunistic Wireless Encryption" (OWE)。允許用戶端進行無密碼連線，適合用於入口網站等網路登入，但是個別用戶端彼此之間的連線都是分別加密的。
WPA	WPA 可藉由金鑰加密每個來自無線網路的訊框，可在本區手動輸入 PSK，或是藉由 802.1x 驗證方式來自動加密。 **預先共享金鑰** - 輸入 **8~63** 個 ASCII 字元，像是 012345678(或是 64 個 16 進位數字，以 0x 開頭，如 0x321253abcde…等)。 **密碼強度**-系統將會顯示密碼強度(以極弱、中度、極強等文字來表示)。 **EAPOL 密鑰重試** - 預設值為**啟用**，可確保密鑰安裝並只使用一次，以防止遭受金鑰重新安裝之攻擊行動。
WEP	**64-Bit** - 針對 64 位元的 WEP 金鑰，請輸入 5 個 ASCII 字元，像是 12345（或是 10 個 16 進位數字，以 0x 開頭，如 0x4142434445）。 **128-Bit** - 針對 128 位元的 WEP 金鑰，請輸入 13 個 ASCII 字元，像是 ABCDEFGHIJKLM（或是 16 個 16 進位數字，以 0x 開頭，如 0x4142434445）。 所有的無線裝置都必須支援相同的 WEP 加密位元大小，並擁有相同的金鑰。這裡可以輸入四組金鑰，但一次只能選擇一組號碼來使用，這些金鑰可以 ASCII 文字或是 16 進位元字元來輸入。請點選您想使用的金鑰組別。

完成設定之後，按下**確定**按鈕儲存相關設定。

III-1-4 存取控制

為了增加額外的無線存取安全性，連線控制頁面可讓您透過無線區域網路的用戶 MAC 位址來限制網路存取動作。

在連線控制頁面上，路由器可透過黑白名單的方式，進行封鎖 MAC 位址來限制無線用戶端存取無線網路。對於想封鎖的無線用戶，使用者可將其 MAC 位址放入黑名單中；或是讓用戶的 MAC 位址放入白名單，使無線用戶得以通行。



可用設定說明如下：

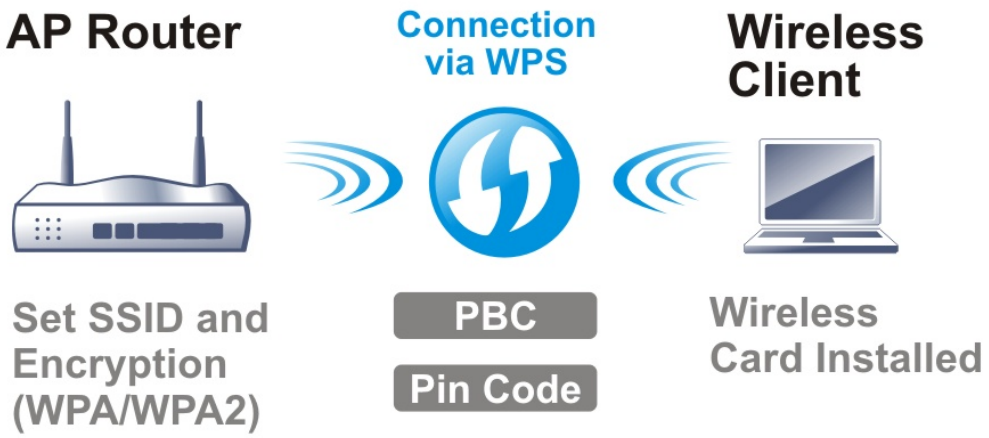
項目	說明
啟用 MAC 位址過濾器功能	請勾選任一 SSID 1 到 4 中以啟動無線 LAN 的 MAC 位址過濾器。下述方框中所有的無線用戶(以 MAC 位址表示)都可分別群組在不同的無線區域網路中，比方說假設您同時勾選了 SSID 1 及 SSID 2，那麼無線用戶將在 SSID 1 與 SSID 2 下群組起來。
MAC 位址過濾器	顯示之前編輯的全部 MAC 位元址。
用戶端 MAC 位址	請手動輸入無線用戶端的 MAC 位址。
套用 SSID	輸入用戶的 MAC 位址之後，勾選 SSID 的方框即可將其與 MAC 位址同時套入連線控制。
屬性	**s -**勾選此項以便隔離無線用戶端之無線連線。
註解	針對用戶端 MAC 位址輸入簡單的說明。
新增	新增新的 MAC 位址於清單上。

刪除	刪除清單中選定的 MAC 位址。
編輯	編輯清單中選定的 MAC 位址。
取消	放棄連線控制設定。
確定	按此鈕儲存連線控制清單。
清除全部	按此鈕儲存連線控制清單。
備份存取控制	此頁面的設定可以儲存成一個檔案，後續可在此裝置還原使用或是套用至其他裝置使用。
上傳自檔案	還原無線存取控制設定並套用到此裝置上。

完成設定之後，按下**確定**按鈕儲存相關設定。

III-1-5 WPS

WPS (Wi-Fi Protected Setup) 提供簡易操作流程，讓無線用戶與無線基地台之間以 WPA 和 WPA2 之加密方式，成功完成網路連線。

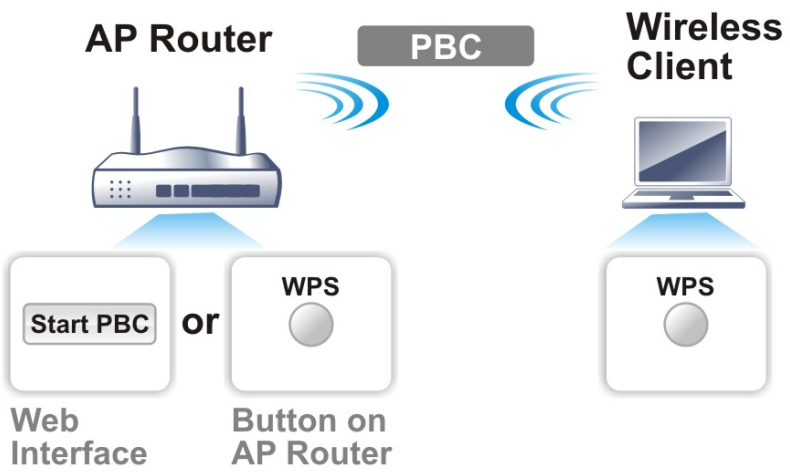


資訊 此功能僅在無線用戶端也支援 WPS 功能時可用。

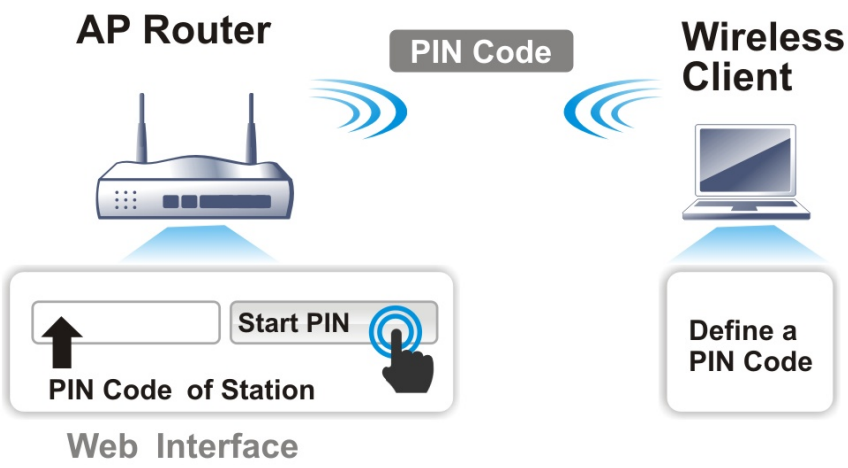
建立無線網路用戶與Vigor路由器之間的連線有個快速及簡單的方式，使用者不需要每次都必須選擇加密模式，或輸入任何長篇的資料以建立無線連線。使用者只要按下無線用戶端中的一個小小按鈕，WPS功能就會替他/她自動建立一個無線連線。

透過基地台與無線用戶之間的WPS來達成無線連線，有二個方式可以進行，一個是壓下*啟動 PBC* 按鈕，一個是利用*PIN Code*來進行。

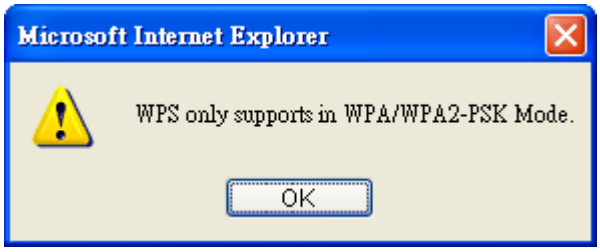
- Vigor2135系列這一端，角色如同無線基地台，可按下路由器面板上的 **WPS** 按鈕一次或是按網頁設定頁面上的 **啟動 PBC** 按鈕一次即可。而在無線用戶那一端，(確保網路卡已經安裝完畢)，則按下網路卡網頁畫面所提供的**啟動PBC** 按鈕。



- 保網路卡已經安裝完畢，則按下網路卡網頁畫面所提供的**啟動 PBC** 按鈕。



因為 WPS 僅在 WPA-PSK 或 WPA2-PSK 模式下可用，如果您沒有在**無線區域網路>>安全性**選擇此模式，您會看到如下的訊息。



請按下**確定**鈕，然後回到**無線區域網路>>安全性**頁面，選擇 WPA-PSK 或 WPA2-PSK 模式，再進入 WPS 頁面。

下圖為**無線區域網路>>WPS** 網頁畫面。

無線區域網路 (2.4 GHz) >> WPS (Wi-Fi安全防護設定)

☑ 啟用WPS功能

Wi-Fi 保護設定資訊

WPS狀態	已設定完成
SSID	DrayTek
驗證模式	WPA2/PSK

裝置設定

經由 Push 按鈕設定	啟動 PBC
經由用戶端 PinCode設定	啟動 PIN

狀態: 準備就緒

備註:
WPS可幫助您的無線網路用戶自動連接至AP基地台
: WPS已停用
: WPS已啟用
: 等待來自無線用戶端的WPS請求。

可用設定說明如下：

項目	說明
啟用 WPS 功能	勾選此方塊啟動 WPS 設定。
WPS 狀態	顯示 WPS 相關的系統訊息，如果無線安全性(加密)功能已設定，您可以在此看到”設定完畢”等訊息。
SSID	顯示路由器的 SSID1 名稱，WPS 僅在 SSID1 中可用。
驗證模式	顯示路由器目前的驗證模式，請注意僅有 WPA2/PSK 和 WPA/PSK 支援 WPS。
經由 Push 按鈕設定	請按**啟動 PBC** 啟用 Push-Button 式的 WPS 設定程式，路由器將會等待 2 分鐘取得無線用戶傳送過來的 WPS 需求，當 WPS 運作時，WLAN 燈號將會快速閃爍，2 分鐘後，路由器會回復一般的運作(您必須在 2 分鐘內設定 WPS)。
經由用戶端 PinCode 設定	請輸入您想要連接的無線用戶所指定的 PIN 碼，在按**啟動 PIN** 按鈕。當 WPS 運作時，WLAN 燈號將會快速閃爍，2 分鐘後，路由器會回復一般的運作(您必須在 2 分鐘內設定 WPS)。

III-1-6 WDS

WDS 表示無線分派系統，是一個連結二個無線基地台的通訊協定，通常可以下列二種方式來應用。

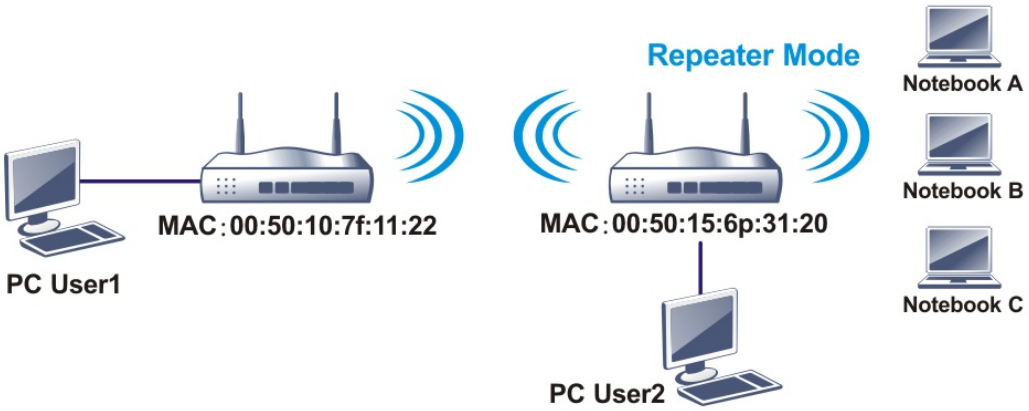
- 提供二個區域網路間空中交流的橋樑
- 延長無線區域網路的涵蓋範圍

參考如下表格：

WDS 模式	無線訊號	差異比較
橋接 (Bridge)	受限	● 在無線訊號有效範圍內的無線站台(用戶端)可以透過路由器/AP 存取網際網路 ● 超出無線訊號有效範圍內的無線站台(用戶端)**無法**透過路由器/AP 的橋接(Bridge)模式存取網際網路 ● 來自 WDS 連結的封包僅能被轉發至本地有線或是無線主機
中繼 (Repeater)	延伸	● 在無線訊號有效範圍內的無線站台(用戶端)可以透過路由器/AP 存取網際網路 ● 超出無線訊號有效範圍內的無線站台(用戶端)**可以**透過路由器/AP 的中繼(Repeater)模式存取網際網路 ● 來自路由器的封包可以藉由 WDS 連結 repeat 到另一台 AP(遠端)上 ● 僅有中繼(Repeater)模式可以進行 WDS-to-WDS 封包轉發

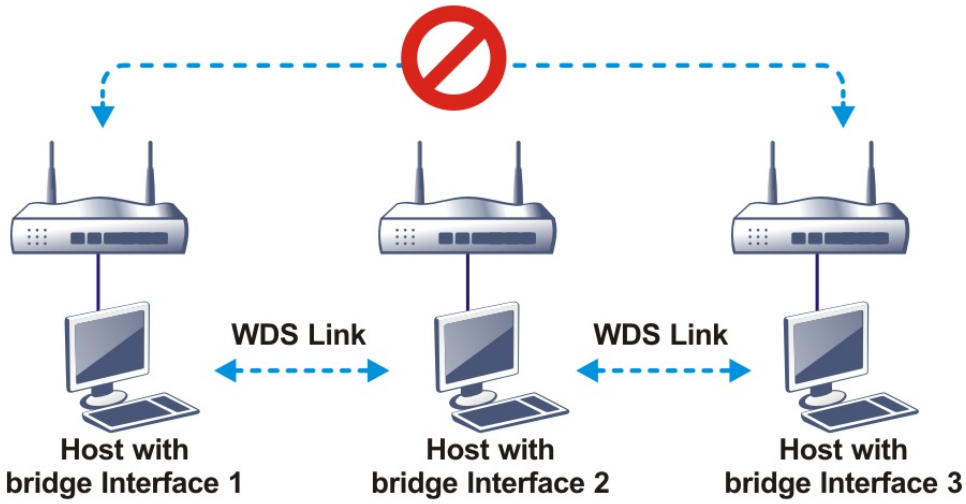
迎合以上的需要，路由器可應用二種 WDS 模式，一為**橋接(Bridge)**一為**中繼(Repeater)**，下圖顯示 WDS 橋接介面的功能：

WDS-中繼模式的應用則描繪如下：

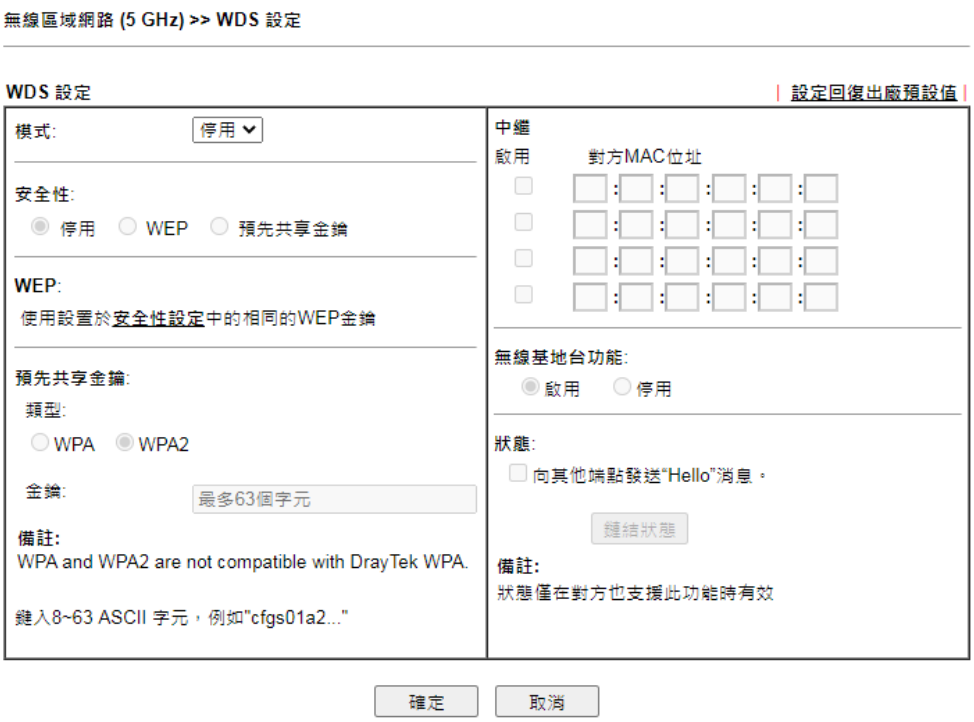


二種模式的主要不同點在於：**中繼(Repeater)**模式下，從一端 AP 過來的封包可以透過 WDS 連結再另一個 AP 上重複產生，WDS 連結傳送過來的封包只能轉送至本機有線或無線的主機。-而橋接(Bridge)模式，來自 WDS 連結的封包僅能轉發至本機有線或無線主機上。換言之，只有中繼模式能完成 WDS 到 WDS 封包轉送的工作

在下面這個例子當中，連接至橋接介面 1 或 3 的主機可以透過 WDS 連結與橋接介面 2 相連。不過連接至橋接 1 的主機無法透過橋接介面 2 與橋接介面 3 的主機相通。



按**無線區域網路**中的 **WDS** 功能以出現如下畫面：



可用設定說明如下：

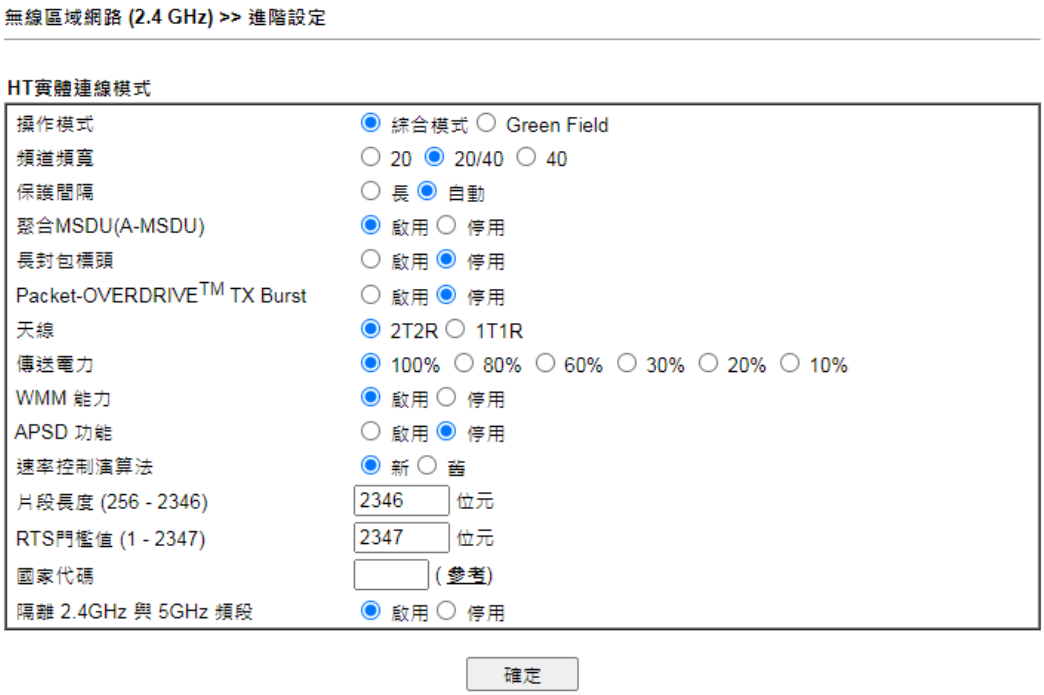
項目	說明
模式	選擇 WDS 設定模式，**停用**將無法啟用任何 WDS 設定；**中繼**模式則是設計用來符合第二種實際之應用。
安全性	有三種安全性類型可選擇，**停用**、**WEP** 和**預設共享金鑰**。您在此處所選擇的設定將會使得 WEP 或是預設共享金鑰有效或是無效。請自三種中挑選出一種。
WEP	當選擇 **WEP** 為安全性模式時，路由器將會使用於**無限區域網路>>安全性**頁面中設定的 WEP 金鑰內容。 請務必確認 WEP 模式與 WEP 金鑰設定都已經在**無限區域網路>>安全性**頁面中設定完畢。 **附註:** 若在**無限區域網路>>安全性**頁面中設定的安全性模式與此處設定的模式不同，系統會發出警告訊息，提醒您並要求您務必確保雙邊的設定一致。
預設共享金鑰	當選擇**預設共享金鑰**為安全性模式時，視需要設定如下項目： **類型-** 有數種類型可以選擇，您可以設定 WPA 或是 WPA2 為加密模式，建立 AP 與路由器之間的 WDS 系統。 **金鑰 -** 請在此區設定加密金鑰，輸入開頭為“0x”之 8 ~ 63 個 ASCII 字元或是 64 的 16 進位的數字。
中繼	如果您選擇**中繼**做為通訊模式，請在此區輸入對方的 MAC 位址，本頁可讓您一次輸入二個對方 MAC 位址。同樣的，如果您想要啟動對方的 MAC 位址，記得輸入完成後勾選**啟用**方塊。
無線基地台功能	當選擇中繼作為 WDS 模式時，按**啟用**讓路由器提供無線基地台的服務；若是選擇橋接作為 WDS 模式，則請按**停用**取消此功能。
狀態	允許使用者傳送招呼訊息給對方，然而則此功能僅在對方也支援時才有效用。

完成設定之後，按下**確定**按鈕儲存相關設定。

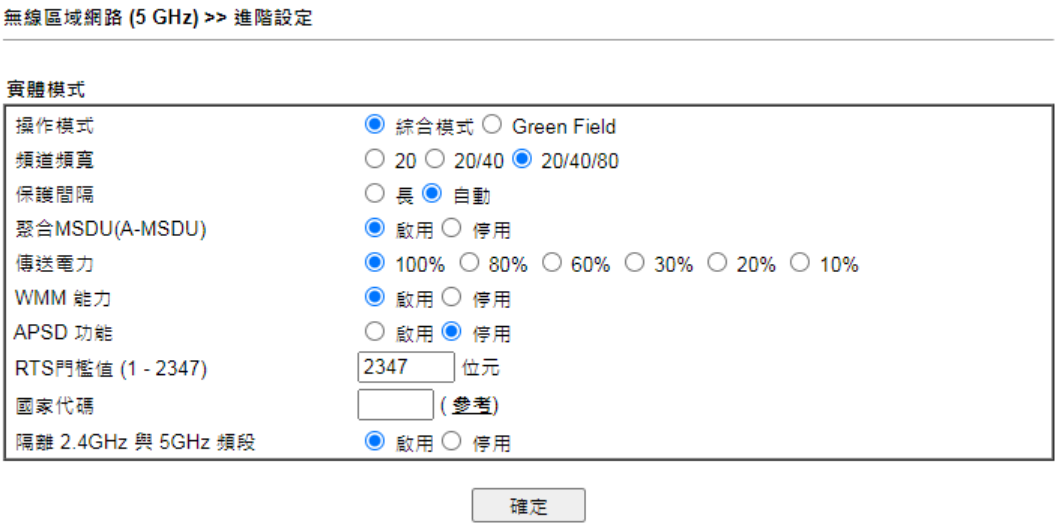
III-1-7 進階設定

本頁允許用戶設定進階項目，例如操作模式、頻道頻寬、防護間隔以及 aggregation MSDU 等無線資料傳輸設定。

2.4 GHz 頁面



5 GHz 頁面



可用設定說明如下：

項目	說明
操作模式	**綜合模式**- 路由器可以 802.11a/b/g 和 802.11n 標準所支援的方式來傳送資料，但是若 802.11g 或 802.11b 無線用戶連接上此路由器的話，整個網路傳輸速率將會降低。 **Green Field** – 為了取得較高的處理能力，請選擇此項模式。此

	模式僅讓資料在 11n 系統中傳輸。另外，此模式也沒有防護機制好避免與相鄰採用 802.11a/b/g 的裝置產生衝突。
頻道頻寬	**20-** 路由器使用 20Mhz 作為基地台與無線用戶之間傳輸的資料速度。 **40-** 路由器使用 40Mhz 作為基地台與無線用戶之間傳輸的資料速度。 **20/40 -** 路由器使用 20Mhz 或 40Mhz 作為基地台與無線用戶之間傳輸的資料速度。此選項可以增加資料傳輸的成效。
保護間隔	確保宣傳延遲的安全性以及敏感數位資訊的反映，如果您選擇**自動**的話，基地台路由器將依照無線用戶的能力，選擇較短的間隔(增加無線性能)或是較長的間隔來傳輸資料。
聚合 MSDU(A-MSDU)	Aggregation MSDU 可整合不同大小的選框，用來改善某些品牌用戶的 MAC 層級成效，預設值為**啟用**。
長封包標頭	此選項用來定義 802.11 封包中同步區塊的長度，最新的無線網路以 56 bit 同步區來使用短封包標頭，而不是以 128 bit 同步區來使用長封包標頭。不過，一些原始 11b 無線網路裝置只有支援長封包標頭而已，因此如果您需要和此種裝置通訊溝通的話，請勾選此方塊。
傳送電力	設定裝置的傳輸訊號的電力百分比，數值越大，訊號密度越高。
WMM 能力	WMM 為 Wi-Fi Multimedia 的縮寫，定義從 802.1d 衍生的四種存取類型錄的優先層級，這些類型都是針對流量、聲音、影像特別設計的，此四種類型分別是 - AC_BE , AC_BK, AC_VI and AC_VO。 在無線資料傳輸中應用 WMM 參數，請按**啟用**鈕。
APSD 功能	自動省電模式(APSD, automatic power-save delivery)是 Wi-Fi 網路支援的強化省電機制，允許裝置花較多時間休眠，並透過縮小傳輸延遲時間，花費少許電力來改善成效。 預設值為**停用**。
速率控制演算法	系統採取動態的無線傳輸速率，通常使用**新的**演算法會優於使用**舊的**演算法。
訊框長度(256 - 2346)	設定無線信號的訊框門檻值，如果不清楚此功能作用，則毋須變更預設值，預設值為 2346。
RTS 門檻值(1 - 2347)	縮減隱藏用戶端間的碰撞數以改善無線的成效。 設定無線訊號的 RTS 門檻值，如果不清楚此功能作用，則毋須變更預設值，預設值為 2347。
國家代碼	Vigor 路由器依循 802.11d 標準廣播國家代碼，然而某些無線站台會偵測/掃描國家代碼以避免衝突的發生，若是偵測到衝突，無線站台將會收到警告且無法進行網路連線，因此改變國碼可以確保特定用戶時刻皆擁有成功的網路連線。
隔離 2.4GHz 與 5GHz 頻段	預設值為啟用，表示使用 2.4GHz 頻段無線用戶端無法連接至使用 5GHz 頻段的無線用戶端，反之亦然。 對於 2.4GHz 與 5GHz 皆設定使用相同的 SSID 名稱: ● 如果**無線區域網路>>基本設置**上的**隔離成員**未啟用，那麼無論此功能是啟用或停用狀態，使用 2.4GHz 與 5GHz 的用戶皆可彼此溝通。

	● 不過，如果此 SSID 在**無線區域網路>>基本設置**上的**隔離成員**是啟用的，那麼使用 2.4GHz 與 5GHz 的無線用戶彼此之間是不可能溝通的。

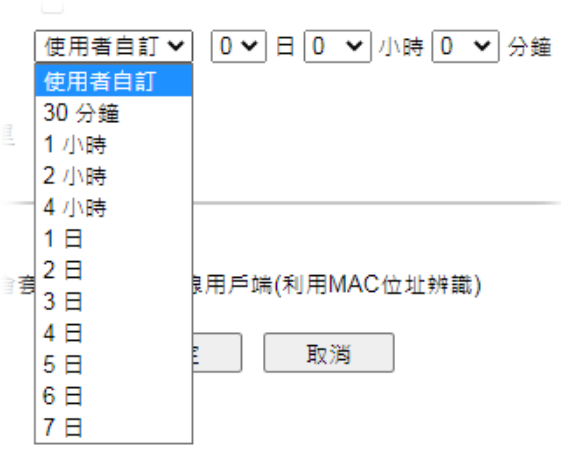
完成設定之後，按下**確定**按鈕儲存相關設定。

III-1-8 無線用戶控制

無線用戶控制用於指定無線用戶連接與重新連接 Vigor 路由器的時間，如果沒有啟用此功能，無線用戶可以一直連線路由器，直到路由器關機為止。

對免費 Wi-Fi 服務而言，此功能相當有用，比方說咖啡車每日提供免費一小時無線服務給予顧客，那麼連線時間可以設定為 1 小時，重新連線可以設定為 1 日，如此顧客可以在一小時內完成工作，不會長期佔據無線網路。

可用設定說明如下：

項目	說明
SSID	顯示無線用戶連接 Vigor 路由器使用的 SSID。
啟用	勾選此框啟用此功能。
連線時間/重新連線時間	使用下拉式清單選擇連線/重新連線 Vigor 路由器的時間，如果選擇**使用者自定**，請手動輸入連線時間。 
顯示全部無線用戶控制清單	顯示所有透過此 SSID 連線至 Vigor 路由器的無線用戶清單。
客製化入口網站設定	按此連結可開啟**客製化入口網站設定**頁面進行修改。

完成設定之後，按下**確定**按鈕儲存相關設定。

III-1-9 頻寬管理

來自 FTP, HTTP 或是某些 P2P 應用程式的上傳或是下載都會佔據大量的頻寬，且影響其他應用程式的運作。請使用頻寬管理功能讓頻寬的運用更有效率。

可用設定說明如下：

項目	說明
SSID	顯示 SSID 名稱。
啟用	勾選此框以啟用用戶端的頻寬管理機制。
頻寬限制類型	**自動調整** - 系統自動決定頻寬限制。 **每個無線站台限制** – 依照無線用戶決定頻寬的限制。
總計上傳限制(kbps)	當選擇**自動調整**為頻寬限制類型，可設定此項目。 輸入用來限制全部無線用戶連接至路由器的最大資料流量(上傳)之數值。
總計下載限制(kbps)	當選擇**自動調整**為頻寬限制類型，可設定此項目。 輸入用來限制全部無線用戶連接至路由器的最大資料流量(下載)之數值。
上傳限制(kbps)	當選擇每個無線站台限制為頻寬限制類型，可設定此項目。 輸入用來限制單一無線用戶連接至路由器的最大資料流量(上傳)之數值。
下載限制(kbps)	當選擇每個無線站台限制為頻寬限制類型，可設定此項目。 輸入用來限制單一無線用戶連接至路由器的最大資料流量(下載)之數值。

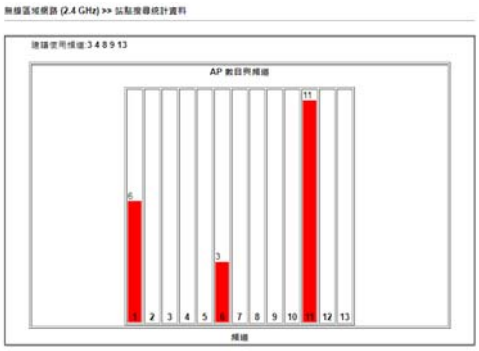
完成設定之後，按下**確定**按鈕儲存相關設定。

III-1-10 搜尋無線基地台

路由器可以掃描全部的頻道以及發現鄰近地區運作中的無線基地台，基於掃描的結果，使用者將會知道哪個頻道是可用的，此外它也可以用來發現 WDS 連結中的無線基地台，注意在掃描過程中(約 5 秒)，任何一台無線用戶都不可以連接上路由器。

本頁可用來掃描無線區域網路中的無線基地台的存在，不過只有與路由器相同頻道的無線基地台可以被發現，請按**掃描**按鈕尋找所有相連的無線基地台。

可用設定說明如下：

項目	說明
掃描	用來尋找所有相連的無線基地台，搜尋結果將會顯示在按鈕上方的方框中。
統計資訊	顯示基地台所使用的頻道統計資料。 
新增至 WDS 設定	本區適用無線區域網路(5GHz)。
新增至	您想要找到套用 WDS 設定的無線基地台，請在本頁底部輸入該 AP 的 MAC 位址，並點選**中繼**模式，然後按**新增至**，稍後該 MAC 位址即會加入 WDS 設定頁面中。

III-1-11 無線頻寬均化

無線頻寬均化在那些必須支援關鍵企業應用程式的無線網路運用中是相當重要的。

大部分的應用不是同步進行就是須要更多的下載連結能力(非上傳能力)，電話與電子郵件在每個方向都會傳送相同數額的資料，而比起其他方式，影音串流和網頁瀏覽涉及到更多來自基地台的流量。這個功能可確保預測的成效與服務品質，允許使用 802.11n 及後續無線用戶都能同時共存在相同的網路下。若無無線頻寬均化，使用綜合模式的辦公室就會冒著讓傳統客戶拖慢整個網路的風險，或是讓速度較快的用戶排擠到其他用戶。

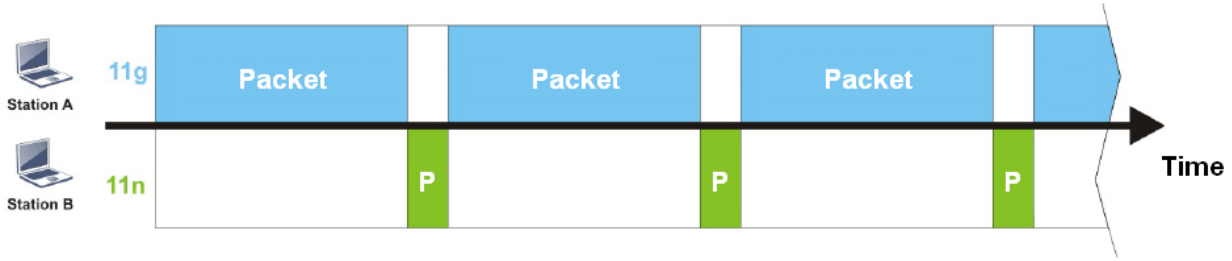
透過此功能，每個用戶在給定的 QoS 層級下能擁有平等機會存取空中無線網路。

同一時間僅容許一個無線站台存取特定無線頻道。

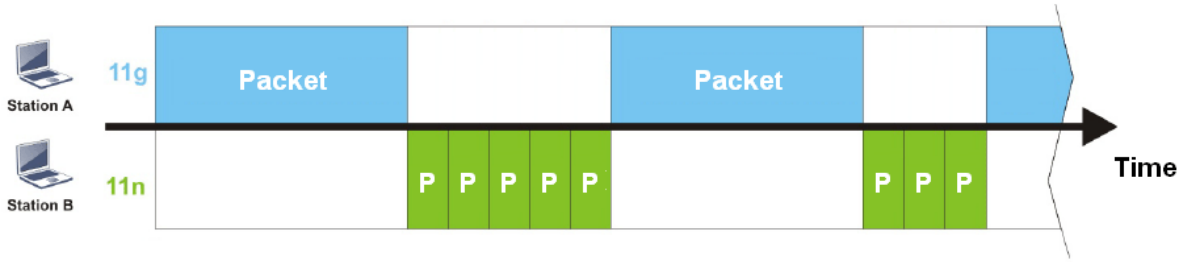
IEEE802.11 頻道存取機制的原理在於每個站台都具有同等的概率使用無線頻道。當無線站台們都有相同的資料傳輸速率時，這個原理可引導一個較為公平的結果，在這種情況下，無線站台們都可以取得相同的頻道存取時間。

不過，當無線站台具有不同的傳輸速率時(例如 11g, 11n)，使用結果將會不大公平。慢速的站台(11g)以緩慢的資料傳輸運行，佔據太多的傳輸時間，相對來看，快速的站台(11n)就變得慢了許多。

以下圖為例，站台 A(11g)和 B(11n)皆透過路由器傳輸資料封包，雖然他們都有同等的概率存取無線頻道，站台 B(11n)僅能用到一點點時間，卻得等待很久讓站台 A(11g)花很長的時間傳輸一個封包。換言之，站台 B 被站台 A 給阻塞了。



為改善這樣的現象，使用此功能可透過控制傳輸流量的方式讓站台 A/B 使用相同的存取時間，藉由這種方式站台 B(速度快)具有較高的可能性傳送比站台 A(速度慢)更多的資料封包出去。



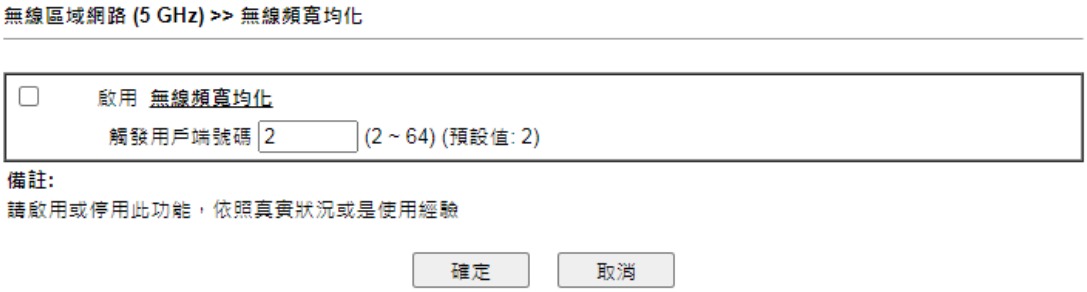
這有點類似自動頻寬限制，每個無線站台的動態的頻寬限制，乃視即時活動的無線站台數目與頻寬均化分派結果而定。請注意 2.4GHz 和 5GHz 的無線頻寬均化是獨立的。但是具有不同 SSID 功能的無線站台會一起運作，因為他們都是使用相同的無線頻道，在特定的環境中，此功能可以減少慢速的無線設備造成的不良影響，且改善整體的無線成效。

適合的環境如下：

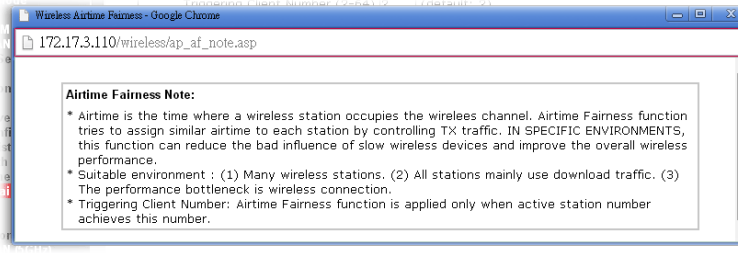
(1) 多個無線站台

(2) 所有的無線站台主要用途在下載

(3) 成效瓶頸在無線連線上



可用設定說明如下：

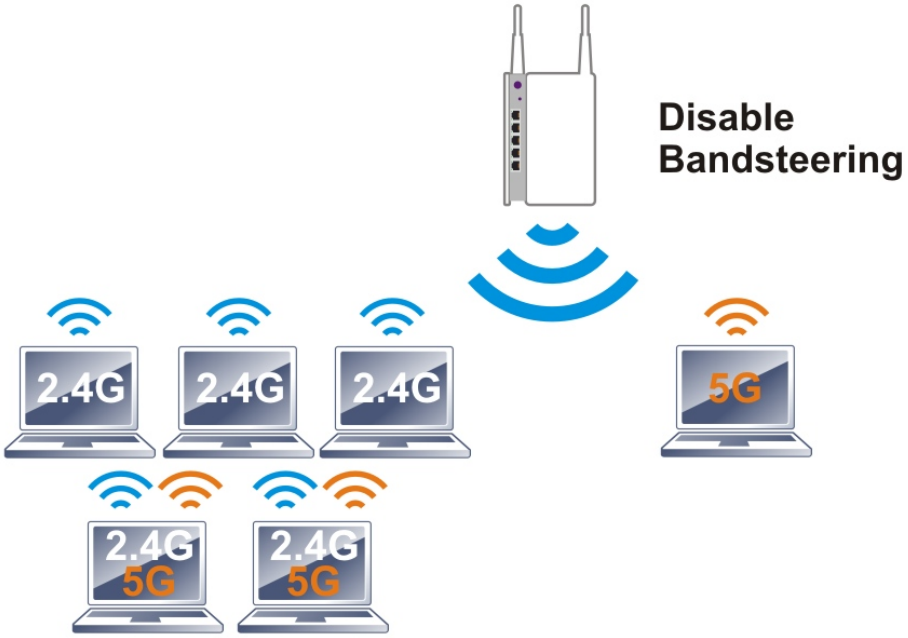
項目	說明
啟用無線頻寬均化	藉由控制傳輸流量，分派相同的無線頻寬給予每一個無線站台。 **無線頻寬均化-** 按此連結可以開啟視窗顯示無線頻寬均化的注意事項。  **觸發用戶數目-**無線頻寬均化功能僅在運作的無線站台達到此設定數目時才套用。

完成設定之後，按下**確定**按鈕儲存相關設定。

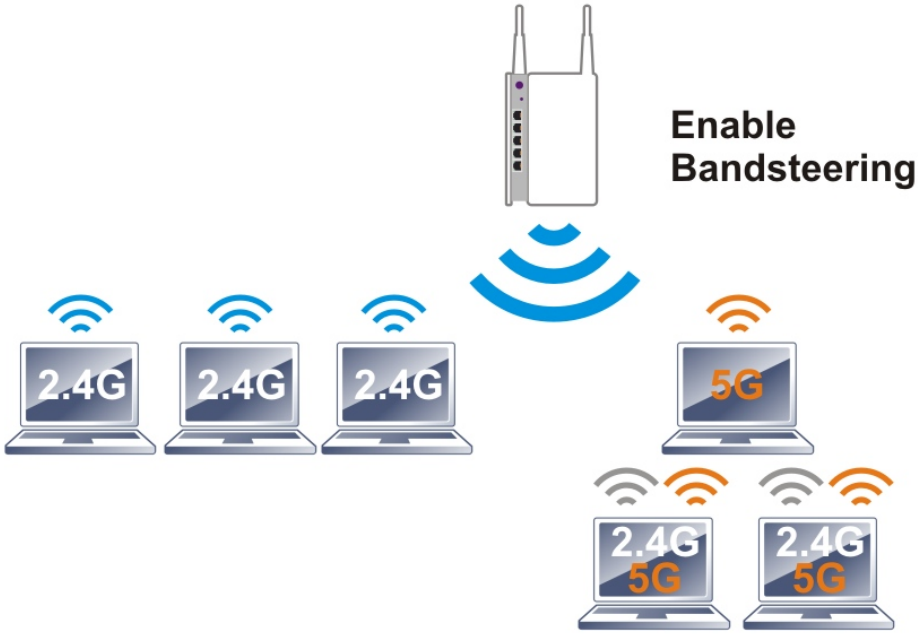
資訊	無線頻寬均化功能與頻寬限制功能是互斥的，因此其個別網頁上皆有額外的動作確保二個功能不會同時啟用。

III-1-12 頻段引導

頻段引導偵測無線用戶是否具有 5GHz 操作能力，並可引導用戶使用該頻率，這個功能可以協助傳統用戶離開 2.4GHz 頻，降低頻道利用率以改善用戶使用經驗。

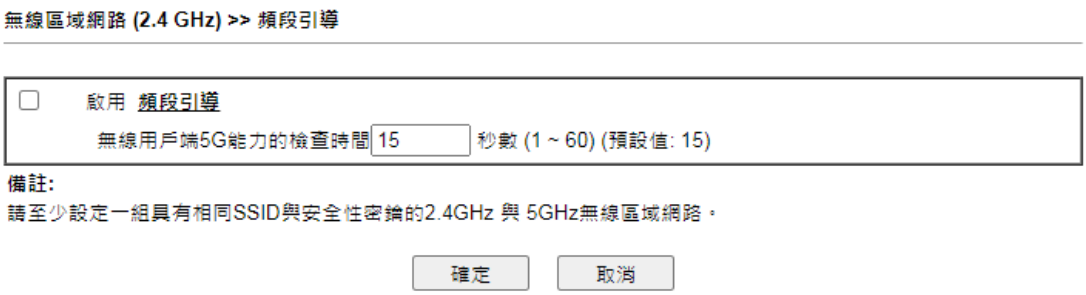


若是偵測出雙頻功能，基地台將讓無線用戶連接到較不擁擠的無線區域網路，諸如 5GHz 等以避免網路塞車。



資訊	欲成功運作頻段引導，於 2.4GHz 上的 SSID 與安全性也必須同時廣播至 5GHz。

開啟**無線區域網路>>頻段引導**：

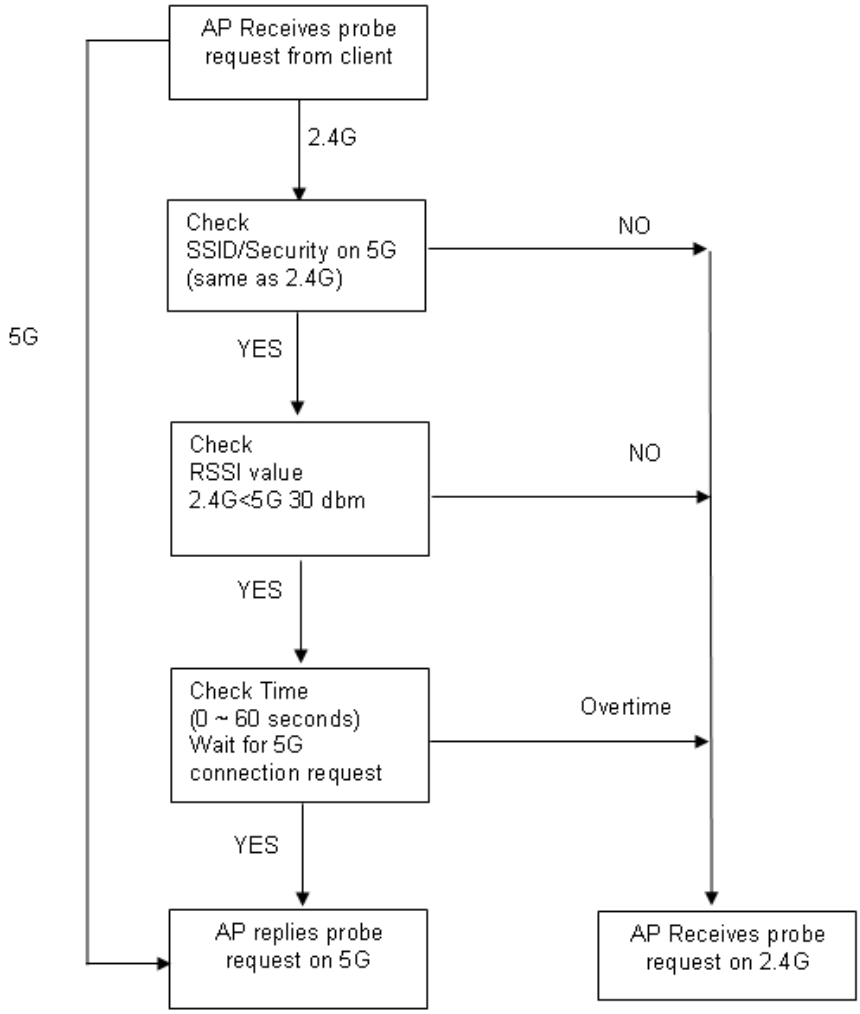


可用設定說明如下：

項目	說明
啟用頻段引導	若啟用了此功能，路由器將會在限定時間內偵測無線用戶是否具有雙頻能力。 **檢查時間...**– 如果無線站台不具備 5GHz 網路連線能力，系統得等待並檢查數秒(預設值等 15 秒)以進行 2.4GHz 網路連線。請設定時間限制秒數以利路由器偵測無線用戶。

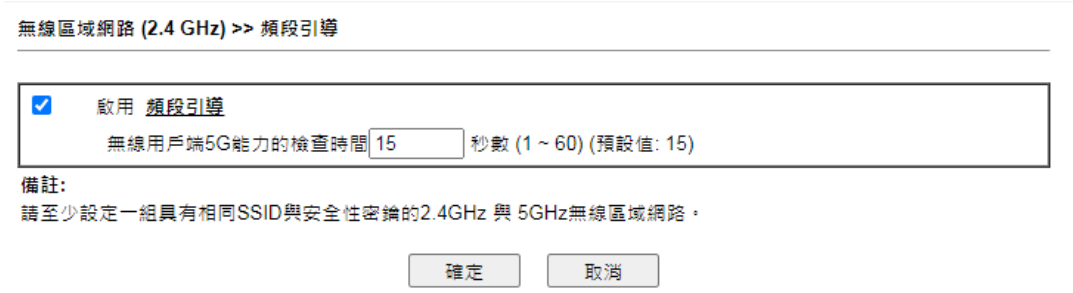
完成設定之後，按下**確定**按鈕儲存相關設定。

下圖顯示頻段引導的運作方式。



如何使用頻段引導?

1. 開啟**無線區與網路(2.4GHz)>>頻段引導**。
2. 勾選**啟用頻段引導**並使用預設值(15)作為檢查時間之設定。



3. 按下**確定**儲存設定。
4. 開啟**無線區與網路(2.4GHz)>>基本設置**以及**無線區與網路(5GHz)>>基本設置**，二邊的頁面皆設定 SSID 為 *DrayTek2135_BandSteering*。按下**確定**儲存設定。

設定為相同的 SSID

5. 開啟**無線區與網路(2.4GHz)>>安全性設定**以及**無線區與網路(5GHz)>> 安全性設定**，二邊的頁面皆將安全性設定為 *12345678*。按下**確定**儲存設定。

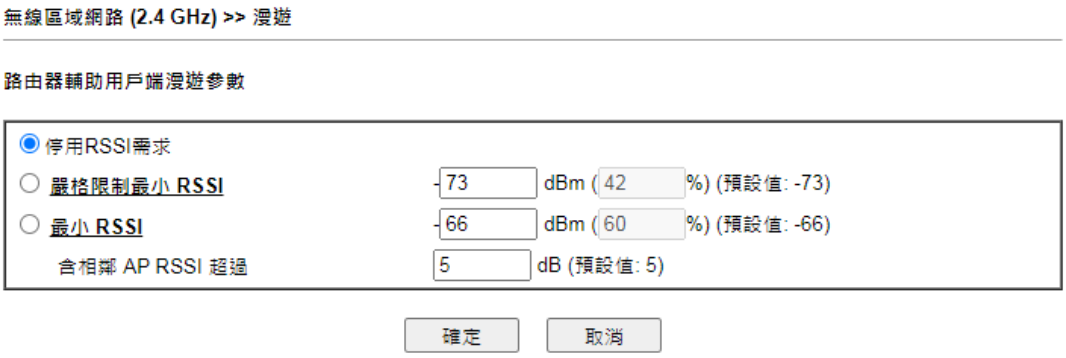
設定為相同的數值

6. 現在，路由器將可讓無線用戶連接至較不擁擠的無線區域網路像是 5GHz 好避免網路壅塞的情形。

III-1-13 漫遊

單一無線網路基地台的網路訊號會受到其涵蓋範圍的限制，因此若您想要以快速的方式在大型的展示區域擴展無線網路，您可以安裝多個基地台，啟用每台基地台的漫遊功能，就可以達成無縫擴展無線訊號的目的了。

這些彼此相連的基地台可以利用預先認證的方式來驗證，本頁面可讓您啟用漫遊以及預先認證功能。



可用設定說明如下：

項目	說明
停用 RSSI 需求	當無線站台的連結速率過慢或是接收的訊號太差，路由器將會自動偵測（依照連線速率以及 RSSI 需求）並切斷網路連線，幫助該站台連線至其他無線基地台取得更好的無線訊號。 此選項可停止漫遊機制。
嚴格限制最小 RSSI	路由器使用 RSSI（接收訊號強度指示器）來決定中止無線站台的網路連線。 當訊號強度低於此處的設定值時，路由器將立刻中止網路連線。
最小 RSSI	**最小 RSSI -**當訊號強度低於此處的設定值時，而路由器偵測出的相鄰基地台(必須是居易 AP 且也支援此功能)具有較高的訊號強度(數值定義在此)，那麼 Vigor 路由器將中止該無線站台的網路連線，稍後該無線站台即可連線至相鄰的無線基地台(訊號較佳)。 ● **相鄰 AP 的 RSSI 值超過 -** S 指定一個數值作為門檻。

完成設定之後，按下**確定**按鈕儲存相關設定。

III-1-14 無線用戶端列表

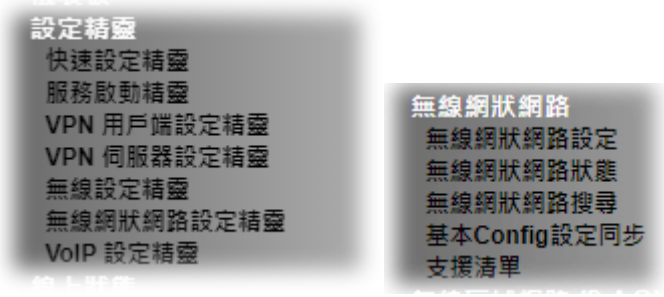
無線用戶端列表提供您目前相連之無線用戶的狀態碼，下圖針對狀態碼提供了詳盡的解說，爲了能有更方便的連線控制，您可以選擇一台 WLAN 用戶站然後選擇**新增至存取控制**，這樣就可以了。

可用設定說明如下：

項目	說明
更新頁面	按此鈕更新用戶端的 MAC 位址列表。
新增	按此鈕新增選定之 MAC 位址至**存取控制**。

III-2 無線網狀網路

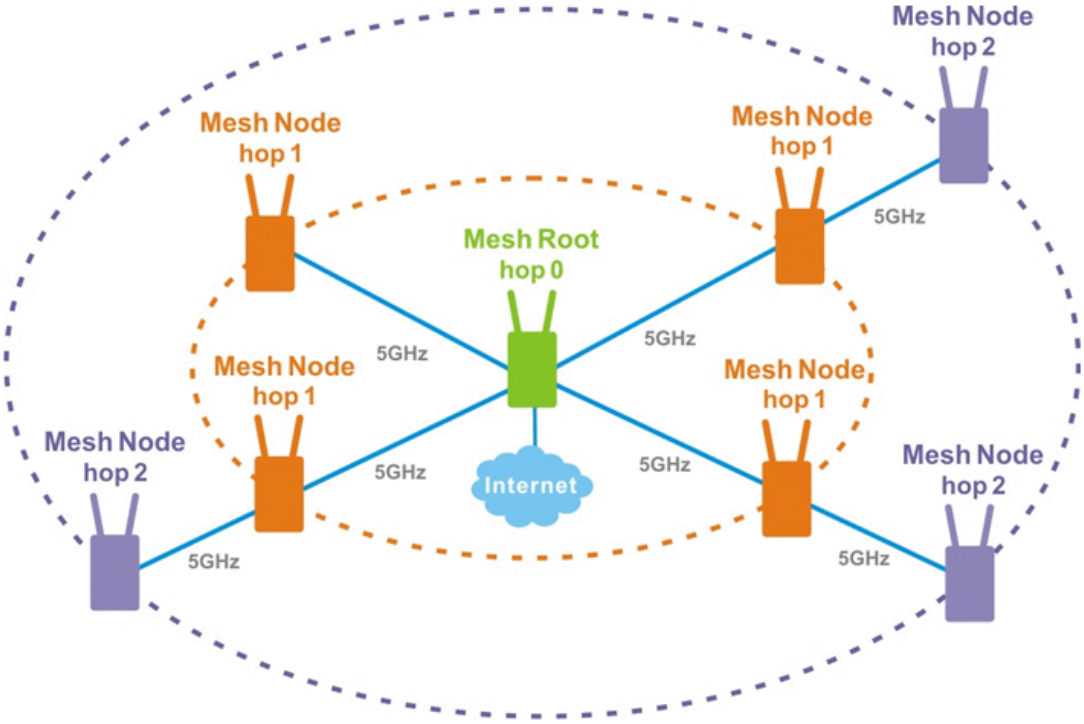
在 Vigor 無線網狀網路中，Vigor 路由器扮演著無線主點的角色。設定無線網狀網路時，請使用無線網狀網路設定精靈或是開啟無線網狀網路選單來進行。



請注意在 VigorMesh 無線網狀網路中，

- 最多支援 8 個無線網狀網路支點(包含無線主點)
- 最多支援 3 個躍點

請參考下圖：



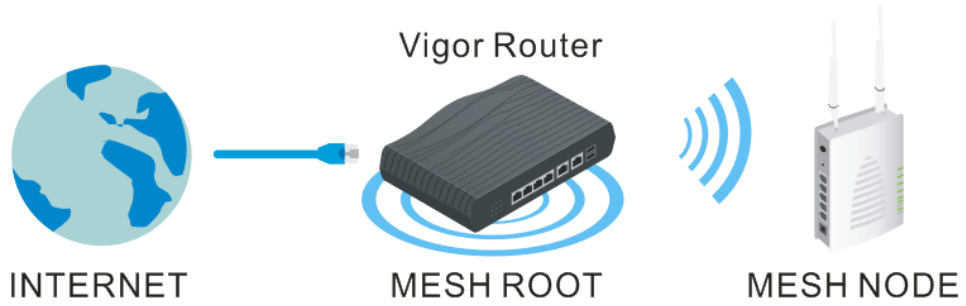
關於在 VigorMesh 無線網狀網路上的群組，

- 必須是由一個無線主點跟 “0~7” 個無線支點組成
- (漫遊)一般來說在無線網狀網路群組中的成員都使用相同的無線 SSID/安全性金鑰
- (新增)只有無線主點可以新增一個無線支點至網狀網路群組中
- (回復)中斷的無線支點可自動嘗試連接至相同群組中另一個無線支點

無線網狀網路主點

網路主點指的是 Vigor 路由器為別的基地台的上行鏈路連線，做為無線主點，路由器必須透過 WAN 介面連接至網際網路。

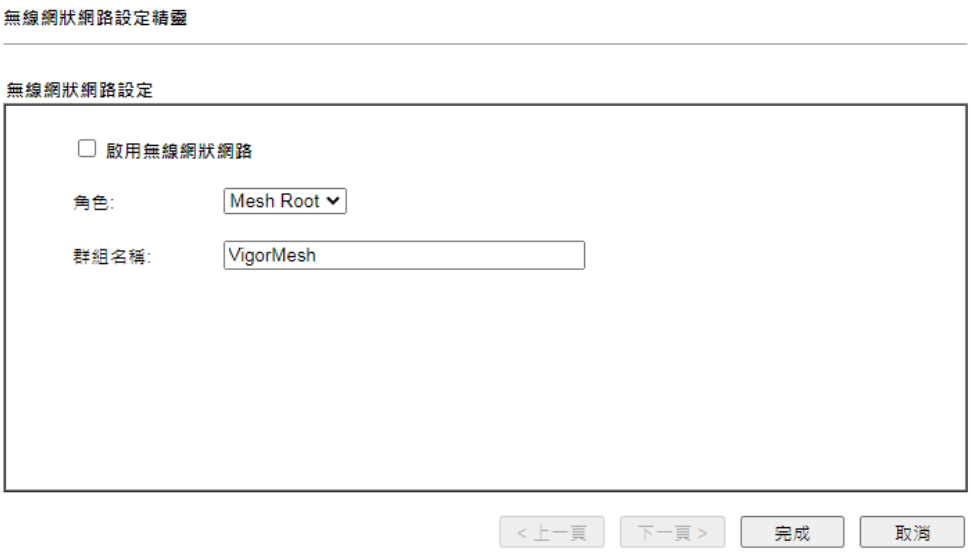
下圖顯示路由器以無線網狀網路主點運行的態樣：



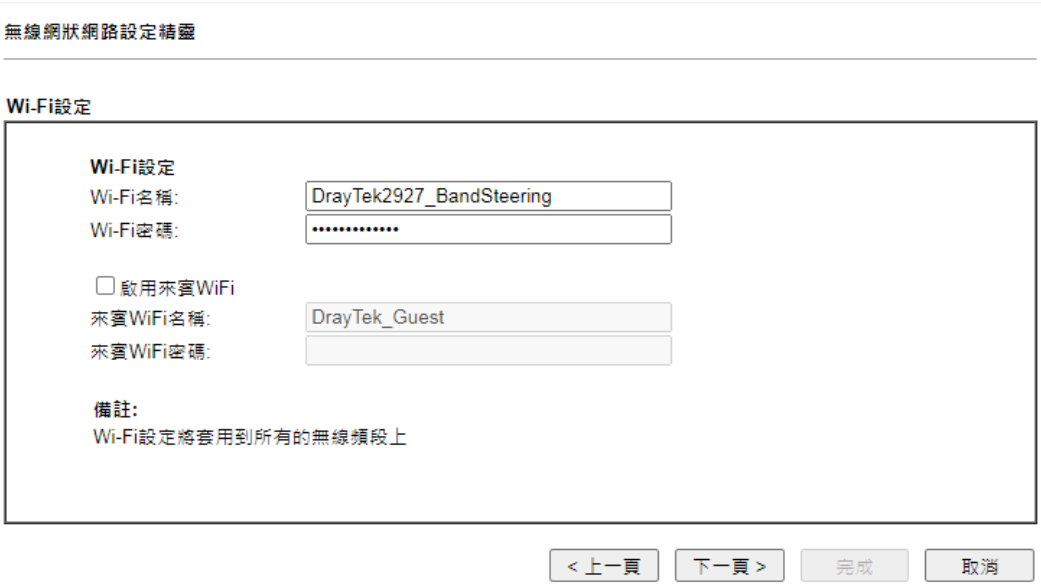
III-2-1 無線網狀網路設定精靈

無線網狀網路設定精靈提供一個簡易快速的方式讓您設定無線網狀網路。

1. 開啟**設定精靈>>無線網狀網路設定精靈**。

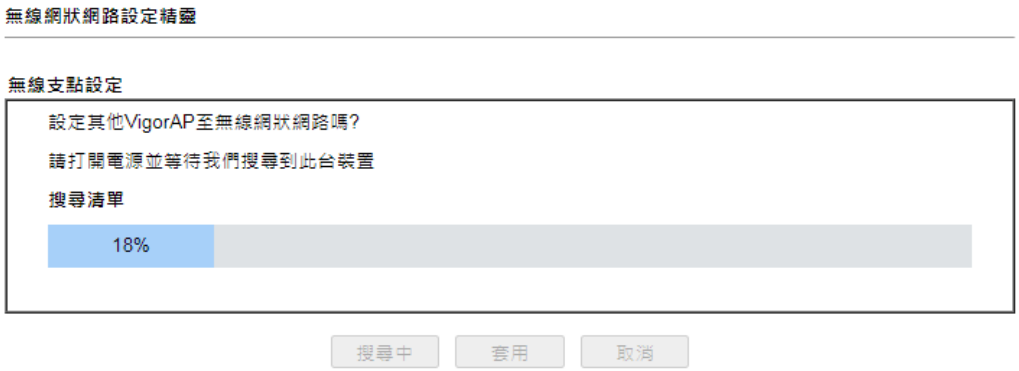


2. 勾選**啟用無線網狀網路**方框之後，**按下一頁**開啟如下頁面。



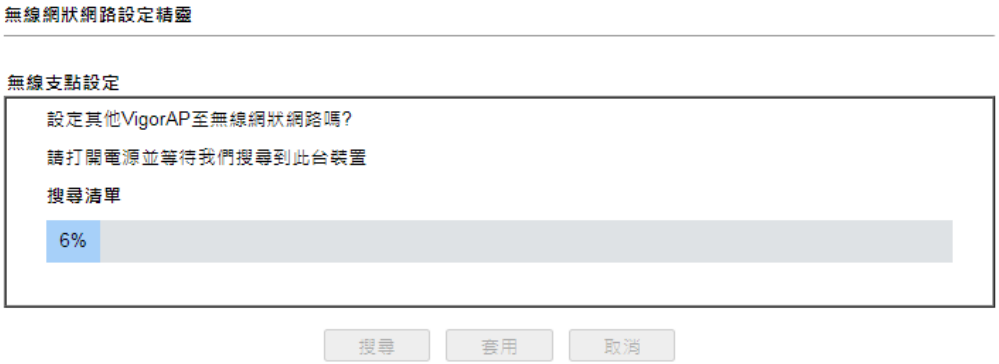
3. 設定 Wi-Fi 名稱與密碼，按**下一頁**開啟如下頁面。

4. 如有需要可設定密碼。之後按**完成**，系統開始進行搜尋。

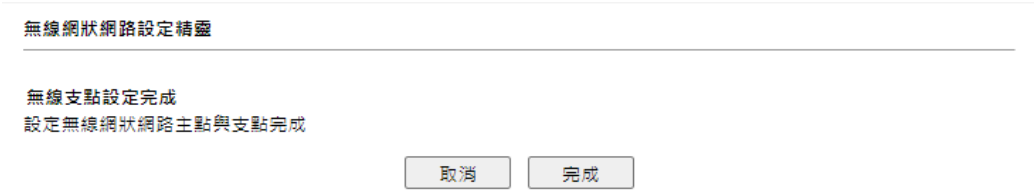


5. 等待數分鐘，之後路由器附近的基地台將會顯示在頁面上。

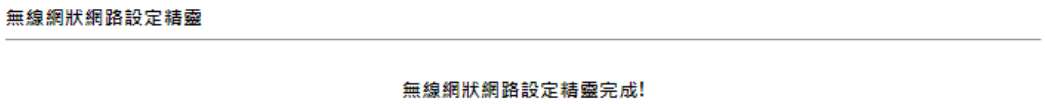
6. 勾選需要納入目前路由器群組中的基地台(例如本例的 VigorAP960C)，按下**套用**。



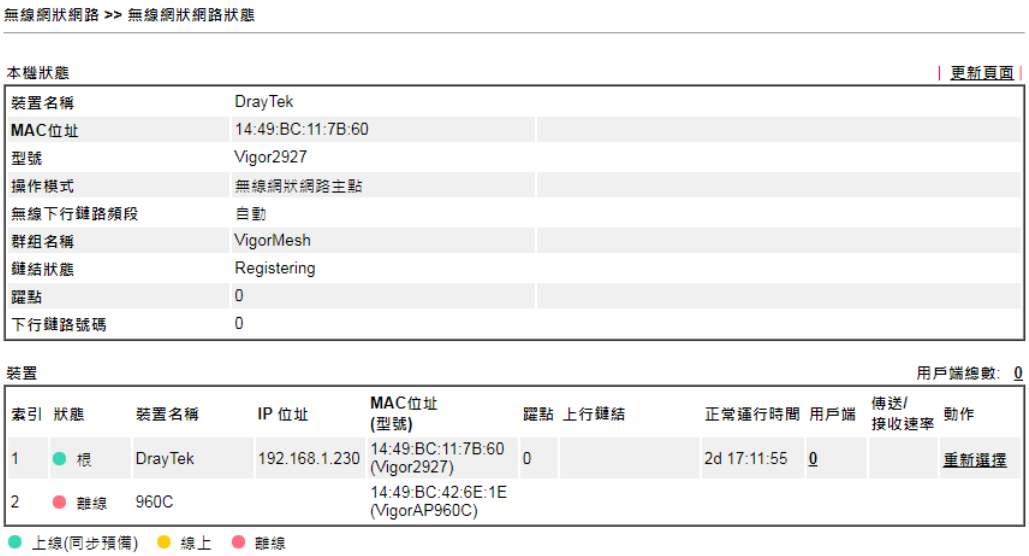
7. 完成無線支點設定之後，請按下**完成**。



8. 接著系統會出現"設定完成"。



請前往**無線網狀網路>>無線網狀網路狀態**。無線網狀網路支點(AP960C)已經納入 Vigor 路由器群組下。

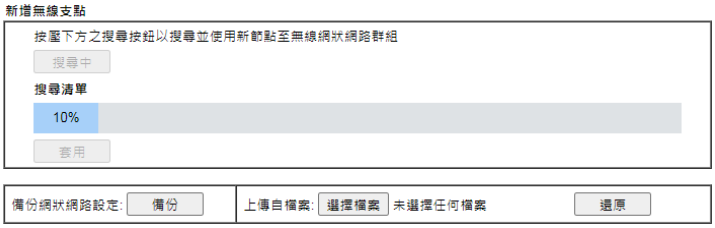


III-2-2 無線網狀網路設定

本頁用以修改無線網狀網路相關設定，使用者可以搜尋並指定無線網狀網路支點做為此無線網狀網路群組的一員。

可用設定說明如下：

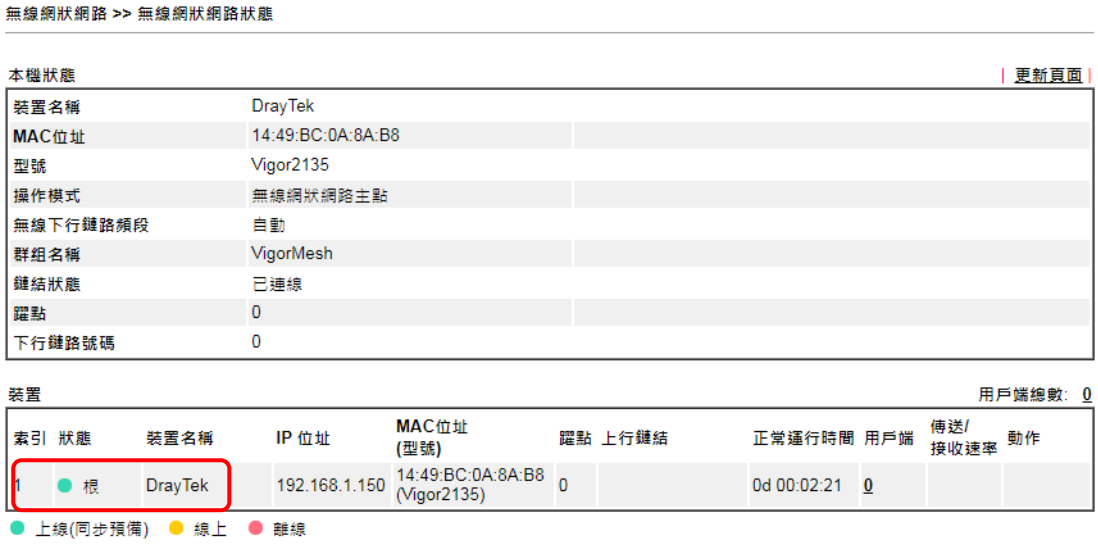
項目	說明
基本設置	
啟用無線網狀網路	勾選以啟用此功能。
角色	顯示目前路由器的角色。 Vigor 路由器在整個無線網狀網路中扮演的角色為無線網狀網路主點，提供網際網路瀏覽的服務。
無線下行鏈路頻段	目前只有 5GHz 被指定為下行鏈路頻段，以連接上行鏈路之無線網狀網路支點。
群祖名稱	顯示目前無線網狀網路群組的名稱。

自動重新選擇	預設值這個功能是啟用的。 欲執行此功能，請先確認無線支點的設定同步與設定檢查已成功完成。若啟用了此功能，在改變了無線網狀網路的環境(例如離線或是中斷連線)後，無線網狀網路主點裝置將會進行自動重新選擇，重新建構整個無線網狀網路。.
日誌等級	可選擇**基本**或是**細節內容**，相關資訊會顯示在**自我診斷 >>Syslog 瀏覽視窗**頁面上。
無線網狀網路群組	基本資訊包含角色、MAC 位址、型號(最多可以有 8 的條目，1 個主點加上 7 個支點)。 **重置** - 按此清除無線網狀網路資訊。 **刪除** - 按此移除選擇的項目。
橋接 VLAN 至網狀網路	選擇此項啟用此功能。
新增無線支點 - 僅在無線網狀網路功能啟用時才出現。	
搜尋	按此掃描路由器附近可用的基地台。  系統偵測出的基地台將顯示在搜尋清單中。
套用	選擇您需要的無線支點再按下此鈕。新的網狀網路支點將會顯示在無線網狀網路群組中。
備份網狀網路設定	**備份** – 按此儲存目前的設定檔。
選擇檔案/還原	按**選擇檔案**以指定設定檔，之後再按**還原**鈕套用相關設定。 注意，當 Vigor 路由器的 MAC 位址不是無線網狀網路群組中的網狀網路主點位址，將無法成功執行還原操作。

III-2-3 無線網狀網路狀態

本頁顯示無線網狀網路狀態。

一個無線網狀網路群組可包含 8 個裝置，在下圖中，躍點值為 0 的裝置為特殊的乙太網路回程，意即當其他支點都使用無線鏈結時，該支點卻是使用乙太網路纜線加入此無線網狀網路群組。



可用設定說明如下：

項目	說明
本機狀態	顯示本裝置的基本資訊。
裝置	顯示群組中本裝置(做為無線主點)與無線支點的細部資訊。 **索引** – 顯示在無線網狀網路群組中裝置的順序編號。 **狀態** – 顯示該裝置的連線狀態與扮演角色。 **裝置名稱** – 顯示裝置的名稱(辨識用)。 **IP 位址** – 顯示裝置的 IP 位址。 **MAC 位址** – 顯示裝置的 MAC 位址。 **躍點** – 顯示該裝置在無線網狀網路中的層級。 "0" 表示該裝置連接至網際網路是透過乙太網路纜線(有線連線) 。 "1" 到 "3" 表示該裝置必須經過幾個無線鏈結才能到達躍點 0 裝置。 **上行鏈結** – 顯示基地台想連接過去的裝置之 MAC 位址。
用戶端總數	顯示全部無線網狀網路裝置清單。

Station List of All Devices

Index	MAC Address	Hostname	Vendor	SSID	Channel	RSSI	TxRate(Kbps)	RxRate(Kbps)
1	00:50:7F:F0:C9:72	TA001029	DrayTek	staffs_4F	6	68%(-63dBm)	0	0
2	00:50:7F:F0:D1:1D	ta002171	DrayTek	staffs_4F	6	41%(-73dBm)	0	0
3	5C:97:F3:D3:D5:F7	Tze-Pingde...	Apple	staffs_4F	6	100% (-49dBm)	0	0
4	40:98:AD:5B:F2:52	Tyronetkii...	Apple	staffs	6	55%(-68dBm)	0	0
5	00:50:7F:37:6D:E5	N/A	DrayTek	staffs_4F	6	52%(-69dBm)	0	0
6	00:50:7F:37:67:BE	N/A	DrayTek	staffs_4F	6	55%(-68dBm)	0	0
7	30:F7:C5:1D:3D:11	N/A	Apple	guests	6	83%(-57dBm)	30	12
8	40:F0:2F:22:EB:A0	N/A	LiteonTe	staffs	6	34%(-76dBm)	22	4
9	18:65:90:DE:D4:E5	N/A	Apple	staffs_4F	6	100% (-44dBm)	0	0
10	60:45:CB:57:1F:36	N/A	N/A	staffs_4F	6	15%(-84dBm)	0	0
11	AC:5F:3E:62:E6:0D	N/A	Samsung	staffs_4F	6	81%(-58dBm)	0	0
12	50:BC:96:E0:00:11	N/A	Apple	staffs	6	71%(-62dBm)	0	0
13	04:B1:67:52:48:90	Redmi5-my5...	N/A	staffs_4F	6	45%(-72dBm)	0	0
14	04:C2:3E:3F:CB:F8	android-ac...	HTC	staffs_4F	6	55%(-68dBm)	0	0
15	0C:8B:FD:31:0B:78	N/A	Intel	staffs_4F	6	89%(-55dBm)	2	2
16	58:48:22:EB:F8:62	android-5f...	Sony	staffs	6	55%(-68dBm)	0	0
17	CC:9F:7A:63:11:27	N/A	N/A	staffs_4F5...	36	52%(-69dBm)	0	0
18	20:47:DA:58:17:79	RedmiNote5...	N/A	staffs_4F5...	36	50%(-70dBm)	0	0
19	70:81:EB:65:80:E5	cheng	Apple	staffs_4F5...	36	87%(-56dBm)	0	0
20	8C:85:90:64:FE:A4	N/A	Apple	staffs_4F5...	36	36%(-75dBm)	0	0

III-2-4 無線網狀網路搜尋

在連接無線網狀網路支點之前，無法從無線網狀主點端檢查裝置的狀態。本頁可以幫助用戶搜尋周圍全部的無線網狀網路裝置，並提供每個裝置的鏈結狀態與操作模式。

欲取得最新的裝置清單，請按下掃描按鈕，之後，周圍的無線網狀網路裝置都會顯示在頁面上。

無線網狀網路 >> 無線網狀網路搜尋

裝置清單

索引	MAC位址	型號	操作模式	鏈結狀態	RSSI

掃描

備註:
在搜尋過程中(少於10秒)，無線站台將無法和路由器連線且網狀網路也可能中斷連線。

無線網狀網路 >> 無線網狀網路搜尋

裝置清單

索引	MAC位址	型號	操作模式	鏈結狀態	RSSI
1	00:50:7F:F1:7F:1D	VigorAP903	無線網狀網路支點(無線)	已連線	-59dBm(良好)
2	00:1D:AA:04:F0:6C	VigorAP1000C	RangeExtender	已連線	-81dBm(公平)
3	00:1D:AA:7C:F5:A4	VigorAP1060C	無線基地台(AP)	已連線	-53dBm(極佳)
4	00:1D:AA:80:FE:D4	VigorAP1060C	無線基地台(AP)	已連線	-77dBm(公平)
5	14:49:BC:42:7D:B6	VigorAP960C	無線基地台(AP)	已連線	-82dBm(公平)
6	14:49:BC:42:4B:B0	VigorAP920C	無線基地台(AP)	已連線	-60dBm(良好)
7	00:1D:AA:62:0F:A8	Vigor2862	無線網狀網路主點	已連線	-71dBm(良好)
8	00:1D:AA:80:FE:B8	VigorAP1060C	無線基地台(AP)	已連線	-86dBm(極差)
9	00:1D:AA:3F:74:64	VigorAP912C	無線基地台(AP)	已連線	-73dBm(公平)
10	00:1D:AA:67:D6:40	VigorAP1000C	無線網狀網路支點(無線)	斷線	-89dBm(極差)
11	14:49:BC:05:F1:A8	Vigor2865ax	無線網狀網路主點	已連線	-78dBm(公平)

掃描

備註:
在搜尋過程中(少於10秒)，無線站台將無法和路由器連線且網狀網路也可能中斷連線。

值得注意的是，只有鏈結狀態標示為"新"的裝置，可以被此路由器選定並納入無線網狀網路群組中。

III-2-5 基本 Config 設定同步

如果您在無線網狀網路群組中新增一個網狀網路支點，網狀網路主點將會傳送基本設定至該裝置上。本頁可協助您變更無線網狀網路主點設定，並傳送新的設定至所有相連的無線網狀網路支點上。

無線網狀網路 >> 基本設定同步

☐ 系統維護

索引	名稱	值
1	X_00507F_System.Management.SkipQuickStartWizard	Enable
2	X_00507F_System.TR069Setting.CPEEnable	0
3	ManagementServer.URL	
4	ManagementServer.Username	
5	ManagementServer.Password	*****
6	ManagementServer.ConnectionRequestUsername	vigor
7	ManagementServer.ConnectionRequestPassword	*****
8	X_00507F_System.AdminmodePassword.Admin	admin
9	X_00507F_System.AdminmodePassword.Password	*****
10	X_00507F_System.SyslogMail.SysLogAccess.SysLogEnable	0
11	X_00507F_System.SyslogMail.SysLogAccess.LogServerIP	
12	X_00507F_System.SyslogMail.SysLogAccess.LogServerPort	514
13	X_00507F_System.SyslogMail.MailAlert.MailAlertEnable	0
14	X_00507F_System.SyslogMail.MailAlert.SMTPServer	
15	X_00507F_System.SyslogMail.MailAlert.MailTo	
16	X_00507F_System.SyslogMail.MailAlert.Username	
17	X_00507F_System.SyslogMail.MailAlert.Password	*****
18	X_00507F_System.SyslogMail.MailAlert.UseTLS	0
19	X_00507F_System.SyslogMail.MailAlert.SMTPServerPort	25
20	X_00507F_System.PasswordEncryption.AdminPassword	*****
21	X_00507F_System.PasswordEncryption.AdminSalt	*****

☐ 無線區域網路 (2.4GHz)

索引	名稱	值
1	X_00507F_WirelessLAN_AP.General.EnableWLAN	1
2	X_00507F_WirelessLAN_AP.General.SSID.1.ESSID	DrayTek2927_BandSteering
3	X_00507F_WirelessLAN_AP.General.SSID.1.Enable	1
4	X_00507F_WirelessLAN_AP.General.SSID.1.Hide	0

可用設定說明如下：

項目	說明
系統維護 / **無線區域網路 (2.4Hz) /** **無線區域網路(5GHz)**	勾選您想要進行設定同步的項目。 **套用** – 按下此鈕套用所有的設定至全部的無線網狀網路支點上。

關於無線網狀網路設定的小撇步

- 設定二個無線網狀網路裝置，上行鏈路 RSSI 值大於-65dBm
- 透過網狀網路鏈結更新無線網狀網路裝置的韌體版本，從躍點數值較少的開始，例如從主點更新韌體，接著躍點 1 網狀網路支點，再來是躍點 2 網狀網路支點，依此類推

- VigorMesh 網路支援最多可達 3 個無線網狀網路躍點，雖然如此，建議連接至無線網狀網路群組的躍點能少於或等於 2 就好

  我們做一個實際的網狀網路環境測試，取得如下的紀錄(使用 VigorAP APP 針對不同躍點值的網狀網路支點，進行網際網路速度測試

  網際網路下載速度(主點與躍點值 1 ~ 3):

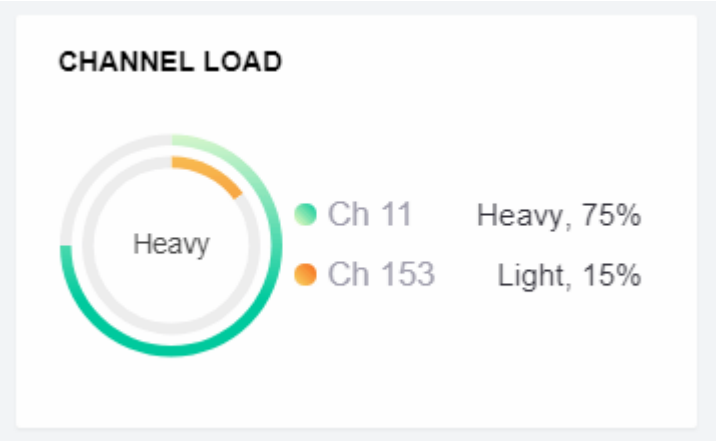
  iPad 連接至主點 ：80Mbps

  iPad 連接至躍點 1 支點：49Mbps (上行鏈路 RSSI 值: -55dBm)

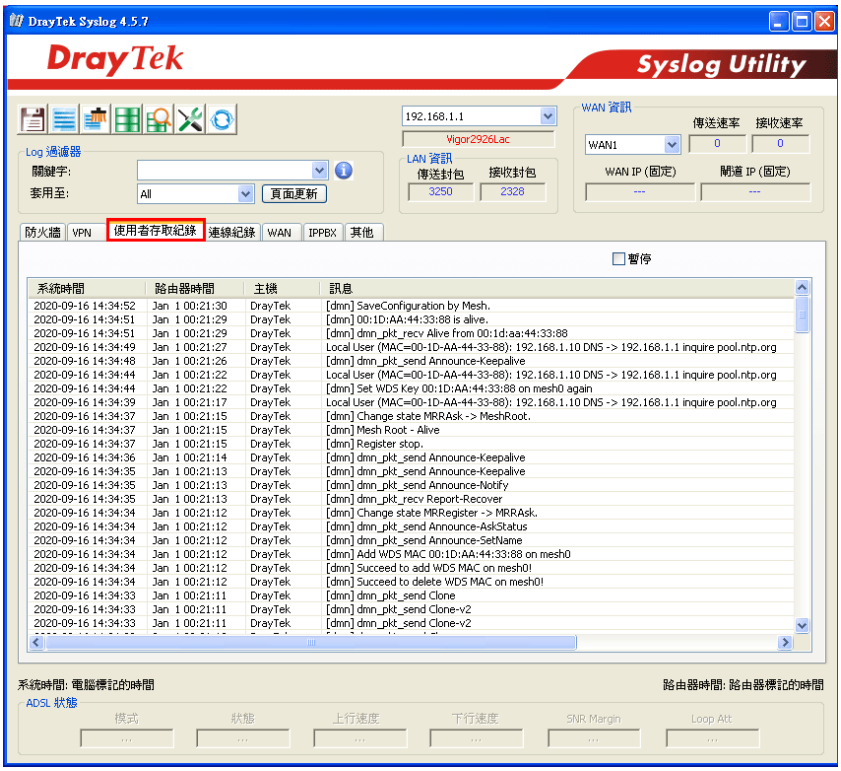
  iPad 連接至躍點 2 支點：41Mbps (上行鏈路 RSSI 值: 躍點 2 -64dBm / 躍點 1 -55dBm)

  iPad 連接至躍點 3 支點：26Mbps (上行鏈路 RSSI 值: 躍點 3 -62dBm / 躍點 2 -68dBm / 躍點 1 -55dBm)

- 不建議使用乙太網路纜線連接無線網狀網路支點至無線網狀網路主點上
- 如果重新設定無線網狀網路主點
  - 所有"已連接"無線網狀支點將被通知重新設定
  - 群組清單與群組金鑰都將重新設定
  - 對那些無法重新設定的無線網狀網路支點，請手動重新設定。透過網頁來重新設定或是回復出廠預設值
- 如果重新設定無線網狀網路支點
  - 群組清單與群組金鑰都將被清除
  - 連接狀態將改變成為"新"的狀態
- 如果無線網狀網路搜尋 / 套用 / 掃描運作過於快速或是沒有得到任何結果，您的需求可能會被拒絕，請重新再試
- 故障排除
  - 檢查韌體版本，請先確認無線網狀網路群組內的基地台都使用最新的韌體版本
  - 檢查操作模式，確認新的無線網狀網路支點沒有取得 DHCP IP 且變成 AP 模式
  - 檢查國碼與頻道，例如想使用歐洲國碼連接 5G 頻道 VigorAP 912C 網狀網路主點與 VigorAP920R 網狀網路支點，這是不可能的
  - 檢查頻道負載，確保沒有超過 70%



  - 蒐集無線網狀網路日誌，並將結果傳送給居易進行分析



III-2-6 支援清單

無線網狀網路 >> 支援清單

下述相容測試清單列出Vigor路由器無線網狀網路支援的DrayTek AP 型號。

型號	狀態	韌體版本
VigorAP 802	Y	1.3.6
VigorAP 903	Y	1.3.8
VigorAP 912C	Y	1.3.6
VigorAP 1000C	Y	1.3.5
VigorAP 960C	Y	1.4.0
VigorAP 1060C	Y	1.4.2

Y:已經測試並且支援
N:未支援

第四篇 VPN 連線設定

VPN

VPN是虛擬網路的延伸，包含共享或公共網路(如網際網路)，簡而言之，透過VPN技術，您可以透過模擬點對點虛擬連結的方式，在二台電腦之間傳送資料。

SSL VPN

為一種可用於標準的網頁瀏覽器的VPN形式。

Certificate Management

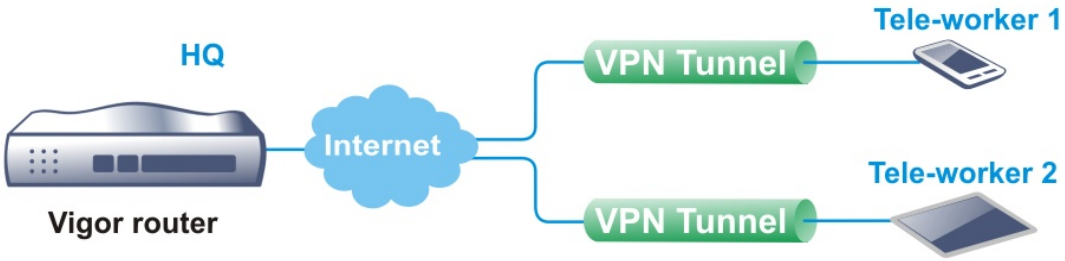
數位憑證的作用就像是電子ID，是由憑證中心(CA)所發行的，包含的內容資訊有名稱、序號、到期日期以及憑證單位發行的數位簽章，讓收取者可以驗證憑證是否真實，Vigor路由器支援符合標準X.509的數位憑證。

IV-1 VPN 與遠端存取

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。

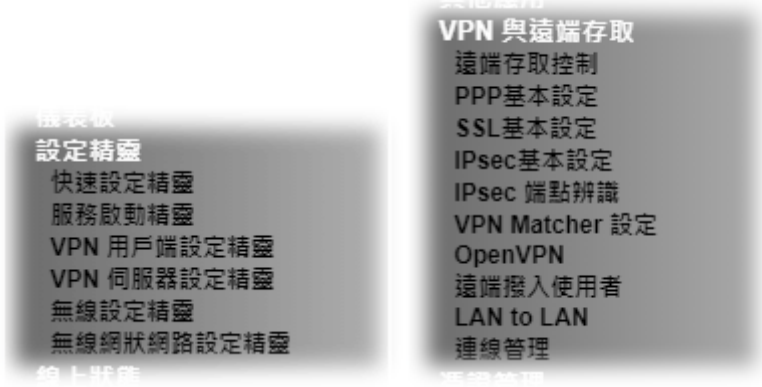
VPN 建構適合用於：

- 家用辦公室與客戶間的聯繫
- 遠距工作人員、出差人員與主辦公室之間的安全連線
- 遠端辦公室與主辦公室之間交換資料
- 分公司與總公司間的 POS 銷售情報系統



網頁使用者介面

下圖為 VPN 與遠端存取的主要功能項目：



IV-1-1 VPN 用戶端設定精靈

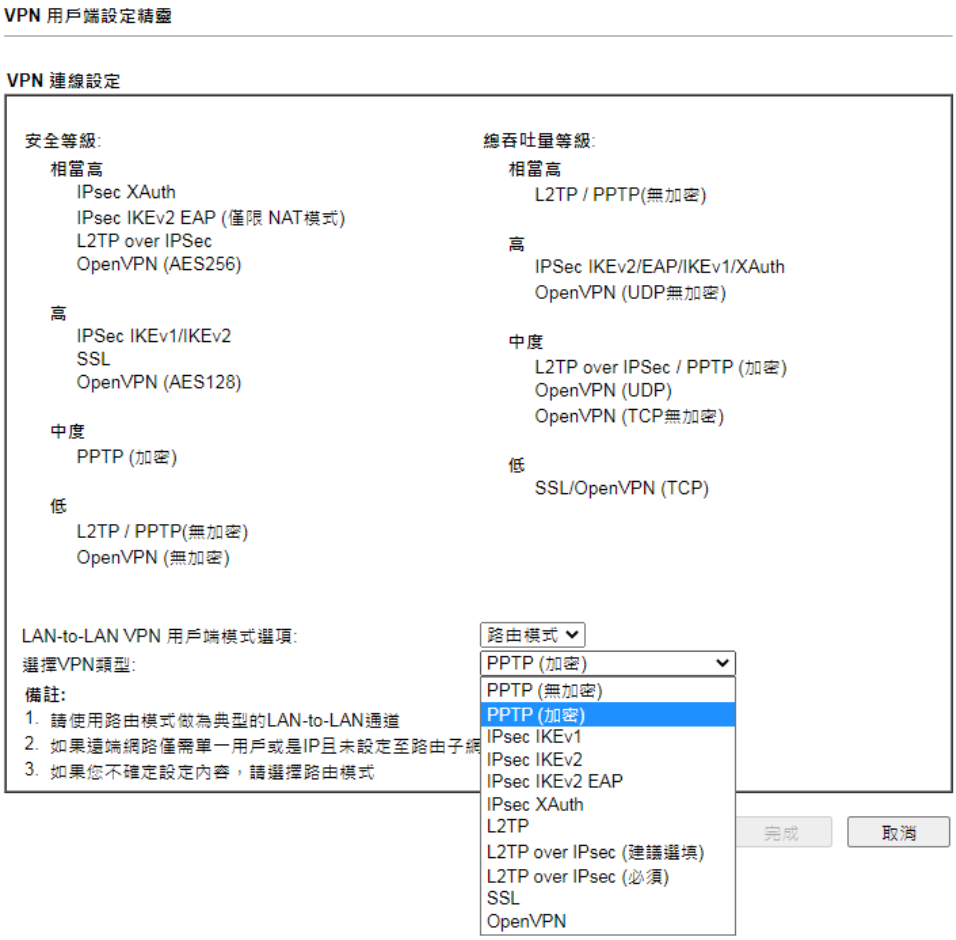
此精靈用來設定 VPN 用戶端所需的 VPN 設定，精靈將引導您一步步建立 VPN 撥出方向的 LAN-to-LAN 設定檔(從伺服器到用戶端)。

1. 開啟**設定精靈>VPN 用戶端設定精靈**，設定頁面如下所示：

可用設定說明如下：

項目	說明
請選擇一個 LAN-to-LAN 設定檔	共有 64 個 VPN 設定檔可以供使用者選擇來設定。

2. 選擇好模式與設定檔選項之後，請按**下一頁**開啟下一個頁面。



可用設定說明如下：

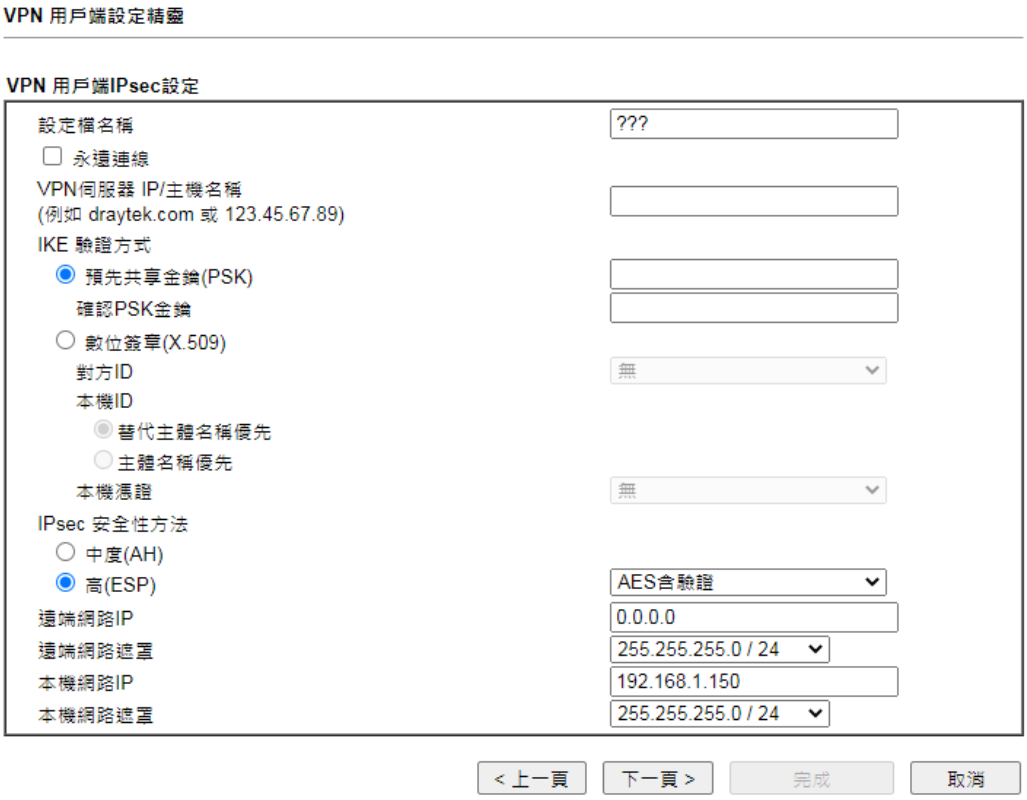
項目	說明
LAN-to-LAN 用戶端模式選項	選擇用戶端模式。 **路由模式/NAT 模式** – 如果遠端網路只允許您以單一 IP 撥入，請選擇此一模式，否則請選擇路由模式。
選擇 VPN 類型	針對 VPN 用戶設定檔選擇適當的 VPN 類型，總共有 6 個類型可以選擇，不同的類型會導引出不同的配置頁面。

在本頁中，您必須，在選擇完畢後，請按**下一頁(Next)**，根據您所選擇的條件，您將會看到不同的配置畫面：

資訊	以下提供的 VPN 類型說明以**路由模式**為基準。

當您選擇 **PPTP (無加密)** 或 **PPTP (加密)**時，您會看到如下頁面：

當您選擇 **IPSec** 您看到的頁面如下：



當您選擇 **SSL** 您看到的頁面如下：

當您選擇 **L2TP over IPSec (建議選填)** 或是 **L2TP over IPSec (必須)**，您看到的頁面如下：

當您選擇 **OpenVPN**，您看到的頁面如下：

可用設定說明如下：

項目	說明
設定檔名稱 (Profile Name)	請輸入設定檔的檔名，檔案的長度限制在 10 的字元間。
永遠連線	勾選此方塊讓路由器永遠保持 VPN 連線。
VPN 伺服器 IP/主機名稱	輸入伺服器的 IP 位址或是輸入此 VPN 設定檔的主機名稱。
IKE 驗證方式	IKE 驗證方式通常套用在使用動態 IP 位址與 IPsec 相關的 VPN 連線如 L2TP over IPsec 與 IPsec 通道之遠端撥入使用者或是節點(LAN to LAN)。 **預先共享金鑰-** 勾選此方塊啟用此功能並按 **IKE 預先共享金鑰** 按鈕輸入金鑰及確認金鑰。 **確認 PSK 金鑰-** 再度輸入金鑰內容。
數位簽章 (X.509)	點選**數位簽章**啟用此功能。 **對方 ID**-自下拉式清單中選擇對方的 ID。 **本機 ID** – 選擇**替代主體名稱優先**或是**主體名稱優先**。 **本機憑證**-自下拉式清單中選擇一種憑證，您必須事先在**憑證管理>>本機憑證**中設定至少一組的憑證，否則無憑證可以使用。
IPSec 安全性方法	對 IPSec 通道和 L2TP 含 IPSec 原則來說，本區為必要設定。 **中度 (AH)** 表示資料將被驗證，但未被加密，此選項的預設時是勾選狀態。 **高 (ESP-Encapsulating Security Payload)** 表示資料將被加密及驗證，請自下拉式清單中選取適合項目： *DES 不含驗證* - 使用 DES 加密演算式，但不採用任何驗證計畫。 *DES 含驗證* - 使用 DES 加密演算式，且採用 MD5 或 SHA-1 驗證計畫。 *3DES 不含驗證* - 使用三重 DES 加密演算式，但不採用任何驗

	證計畫。 *3DES 含驗證* -使用三重 DES 加密演算式，且採用 MD5 或 SHA-1 驗證計畫。 *AES 不含驗證* - 使用 AES 加密演算式，但不採用任何驗證計畫。 *AES 含驗證* -使用 AES 加密演算式，且採用 MD5 或 SHA-1 驗證計畫。
使用者名稱	輸入字元作為使用者名稱。當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區資料可用來驗證連線。
密碼	輸入密碼資料。當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區資料可用來驗證連線。
遠端網路 IP	請輸入區域網路 IP 位址（依照遠端主機實際位置）建立 VPN 連線。
遠端網路遮罩	請輸入區域網路遮罩（依照遠端主機實際位置）建立 VPN 連線。
本機網路 IP	請輸入本機區域網路 IP 位址。
本機網路遮罩	請輸入本機區域網路遮罩。

3. 完成配置後，請按**下一頁**，確定頁面將顯示如下，如果沒有任何問題的話，您可以按下面可至不同設定頁面的按鈕，然後按**完成**進行另一個 VPN 設定。

可用設定說明如下：

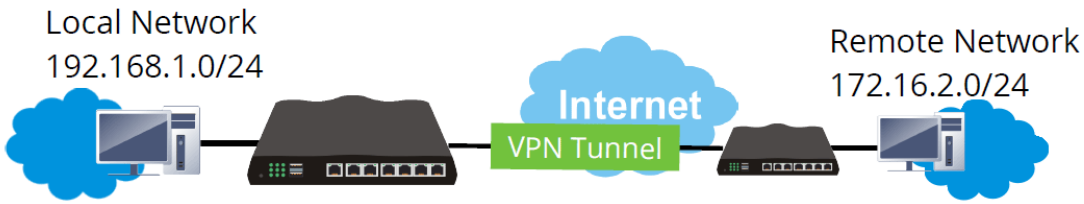
項目	說明
前往 VPN 連線管理	按此鈕進入 **VPN 及遠端存取>>連線管理**頁面檢視 VPN 連線狀態。
進行另一個 VPN 用戶端設定精靈設置	按此鈕以便利用 VPN 伺服器設定精靈設定另一個 VPN 伺服器設定檔。
檢視更詳細的設定內容	按此鈕進入 **VPN 及遠端存取>> LAN to LAN** 以檢視細節內容。

IV-1-2 VPN 伺服器端精靈

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)。

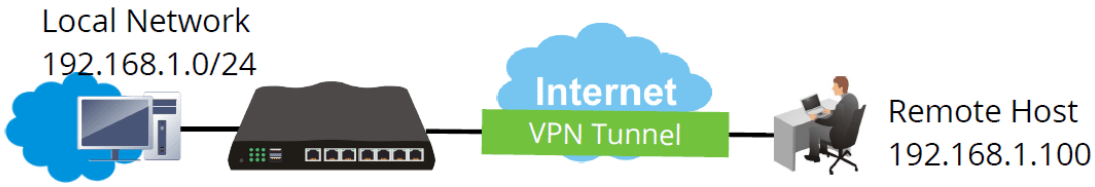
站對站(LAN-to-LAN)

- 二台路由器 LAN 網路間的連線
- 允許分支機構雇員和總公司分享相同的網路資源

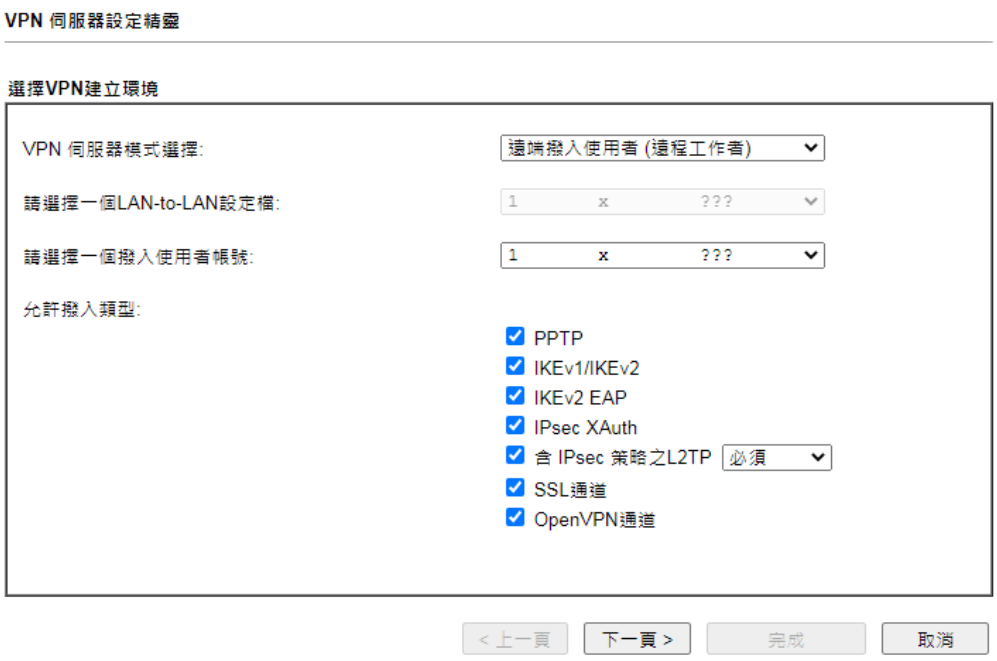


遠端存取(遠端撥入)

- 遠端主機與路由器 LAN 網路之間的連線，主機將使用本機子網中的 IP 位址
- 允許雇員在外商旅時存取公司內部資源



1. 開啟**設定精靈>VPN 伺服器設定精靈**，設定頁面如下所示：



可用設定說明如下：

項目	說明
VPN 伺服器模式選項	請選擇 VPN 伺服器的方向。 **站點至站點 VPN** – 想要自動設定 LAN-to-LAN 設定檔，請選擇**站點至站點 VPN**。 **遠端撥入使用者(遠程工作者)**– 管理遠端使用者設定檔表格來管理遠端用戶的存取狀態，使用者透過 VPN 連線存取網路時，必須接受驗證過程。 **注意**: VPN 伺服器設定精靈畫面會依據所選擇的 VPN 伺服器模式而有所不同。
請選擇一個 LAN-to-LAN 設定檔	當您選擇的是點對點 VPN**(**LAN-to-LAN**)**作為 VPN 伺服器模式時，即可使用此設定檔，共有 64 個 VPN 設定檔可以供使用者選擇並設定。
請選擇一個撥入使用者帳號	當您選擇了遠端撥入使用者作為 VPN 伺服器模式時，即可使用此項目，總共有 64 個不同的 VPN 通道供用戶設定使用。
允許的撥入類型	當您選擇了任何一個撥入使用者帳號設定檔，即可使用此類型設定，您必須針對 VPN 伺服器設定檔選擇適當的撥入類型，此處提供數種可以選擇的項目（類似 VPN 用戶端精靈）。 ☑ PPTP ☑ IKEv1/IKEv2 ☑ IKEv2 EAP ☑ IPsec XAuth ☑ 含 IPsec 策略之L2TP 必須 ☑ SSL通道 ☑ OpenVPN通道

	不同的撥入類型所帶出的設定頁面也會有些許的差異。此外，依照選擇的 VPN 伺服器模式，每種撥入類型的設定項目也會隨之改變。

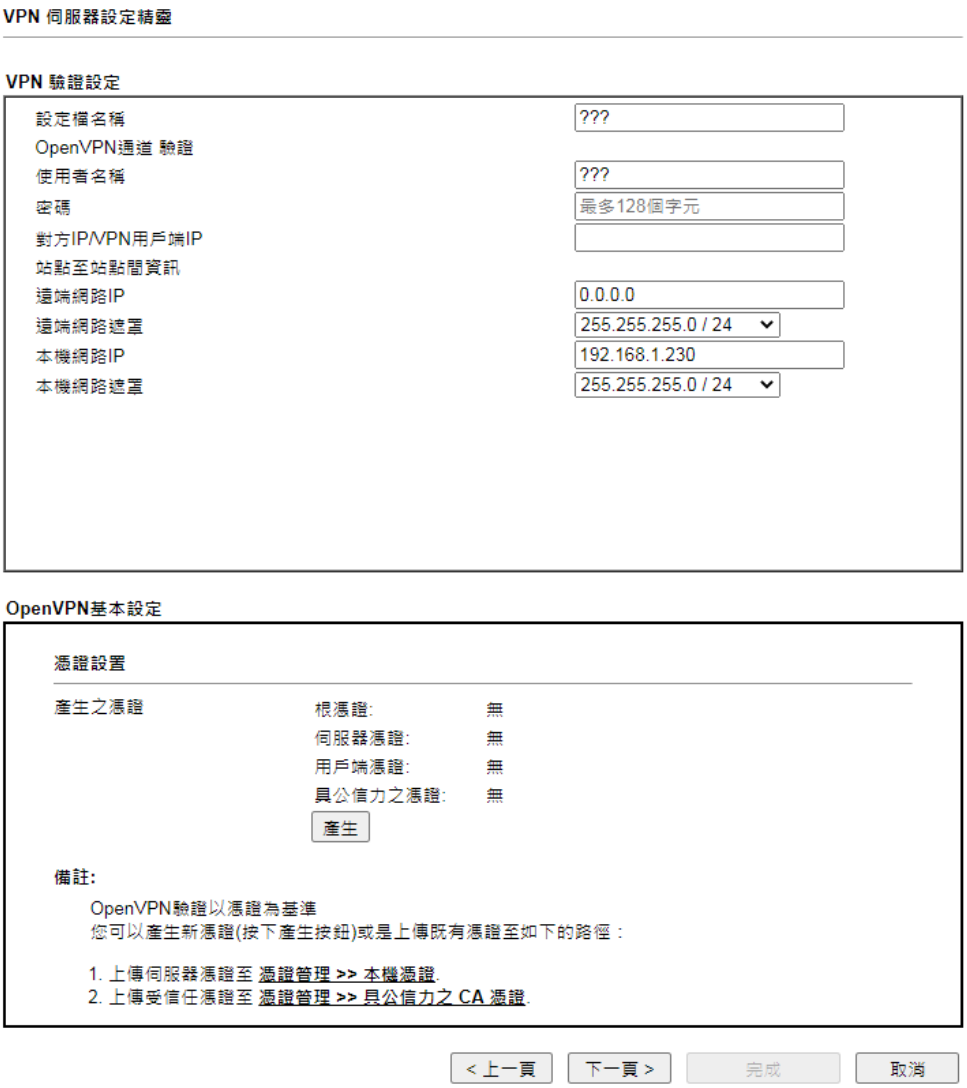
2. 在選擇完畢後，請按**下一頁**，根據您所選擇的條件，您將會看到不同的配置畫面。此處所舉的範例是以**站點至站點 VPN** 作為 **VPN 伺服器模式選項**。

當您勾選了 **PPTP/SSL** 之後，您會看到如下頁面：

當您選擇 **PPTP, IPSec, L2TP** 或 **PPTP, IPSec** 或含 **IPsec 策略之 L2TP (建議選填/必須)**，您會看到如下頁面：

當您選擇 **IPSec**，您看到的頁面如下：

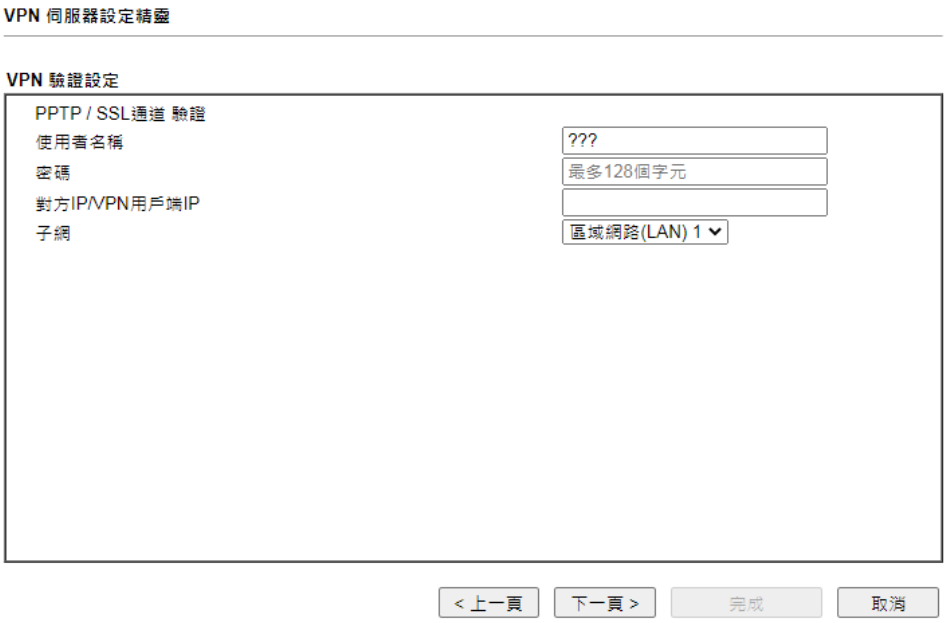
當您選擇 **OpenVPN**，您看到的頁面如下：



可用設定說明如下：

項目	說明
設定檔名稱	請輸入設定檔的檔名，檔案的長度限制在 10 的字元間。
使用者名稱	當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區資料可用來驗證連線。
密碼	當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區資料可用來驗證連線。
IPsec / IPsec XAuth / 含 IPsec 策略之 L2TP / SSL 通道驗證	
預先共享金鑰	為了驗證 IPSec/L2TP IPSec，請輸入金鑰內容。
確認 PSK 金鑰	再輸入一次金鑰內容確認。
數位簽章 (X.509)	勾選此方塊啟用此功能並選擇一組事先定義的簽章內容 (在 **VPN 和遠端存取>>IPSec 端點辨識**中設定)。 **對方 ID** – 自下拉式清單中選擇一組對方 ID。 **本機 ID** – 選擇**替代主體名稱優先**或是**主體名稱優先**
對方 IP/VPN 用戶端 IP	請輸入遠端用戶的 WAN IP 位址或是 VPN 用戶端 IP 位址。
對方 ID	請輸入遠端用戶的 ID 名稱。
站點對站點資訊	
遠端網路 IP	請輸入區域網路 IP 位址(依照遠端主機實際位置)建立 VPN 連線。
遠端網路遮罩	請輸入區域網路遮罩(依照遠端主機實際位置)建立 VPN 連線。
本機網路 IP	請輸入本機區域網路 IP 位址。
本機網路遮罩	請輸入本機區域網路遮罩。
OpenVPN 基本設定	**產生** - 按此產生憑證以因應 OpenVPN 驗證。或是上傳取自本機之憑證或是受信任的 CA 憑證。

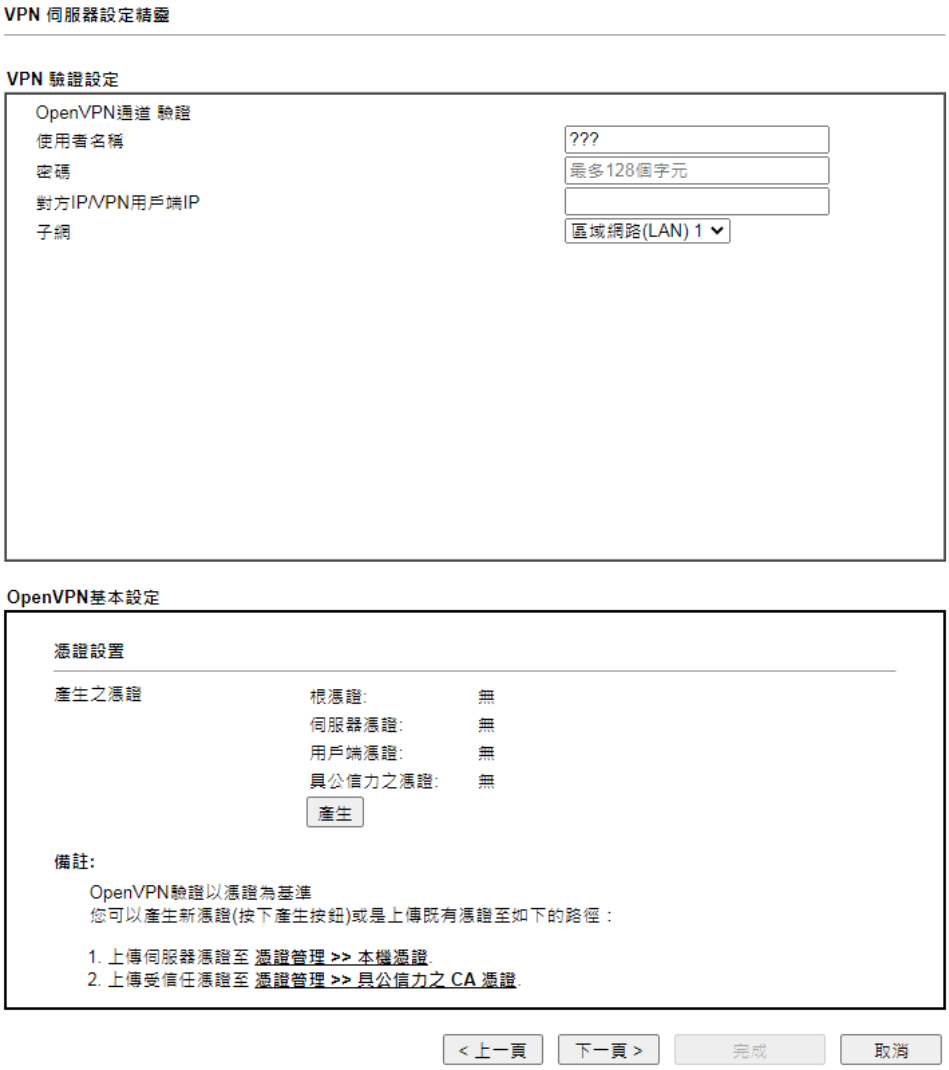
3. 若選擇**遠端撥入使用者(遠程工作者)**作為 **VPN 伺服器模式選項**並勾選 **PPTP/SSL** 作為撥入類型。當您勾選了 **PPTP/SSL** 之後，您會看到如下頁面：



當您勾選了 **IPsec XAuth/含 IPsec 策略之 L2TP (無)**，您會看到如下頁面：

當您勾選了 **IPsec XAuth/含 IPsec 策略之 L2TP (建議選填)/ 含 IPsec 策略之 L2TP (必須)**，您會看到如下頁面：

當您選擇 **OpenVPN**，您看到的頁面如下：



可用設定說明如下：

項目	說明
使用者名稱	遠端區域網路用來建立 VPN 連線的使用者名稱。
密碼	遠端區域網路用來建立 VPN 連線的密碼。
IPsec / IPsec XAuth / 含 IPsec 策略之 L2TP / SSL 通道驗證	
預先共享金鑰	針對 IKEv1/IKEv2 / IPsec / IPsec XAuth / L2TP with IPsec / SSL 通道驗證，您必須設定**預先共享金鑰**與/或**數位簽章**。 請注意，如果遠端用戶具有動態 IP 位址，請勿啟用本頁面上任何設定(PSK /**數位簽章**)，改至 **VPN 與遠端存取>>IPsec 基本設定**頁面處理。 **預先共享金鑰** - 選擇此項後輸入金鑰。 **確認 PSK 金鑰** - 再次輸入金鑰以確認。
數位簽章 (X.509)	**Digital Signature (X.509)** - 選擇此項以啟用此功能。 **對方 ID** – 選擇事前已經定義的數位簽章作為對方 ID。
對方 IP/VPN 用戶端 IP	請輸入遠端用戶的 WAN IP 位址或是 VPN 用戶端 IP 位址。
對方 ID	輸入遠端用戶端的 ID 名稱。
子網	選擇一個介面。
OpenVPN 基本設定	**產生** - 按此產生憑證以因應 OpenVPN 驗證。或是上傳取自本機之憑證或是受信任的 CA 憑證。

4. 完成配置後，請按**下一頁**，確定頁面將顯示如下，如果沒有任何問題的話，您可以按下面可至不同設定頁面的按鈕，然後按**完成**進行另一個 VPN 設定。

可用設定說明如下：

項目	說明
前往 VPN 連線管理	按此鈕進入 **VPN 及遠端存取>>連線管理**頁面檢視 VPN 連線狀態。
進行另一個 VPN 用戶端設定精靈設置	按此鈕以便利用 VPN 伺服器設定精靈設定另一個 VPN 伺服器設定檔。
檢視更詳細的設定內容	按此鈕進入 **VPN 及遠端存取>> LAN to LAN** 以檢視細節內容。

IV-1-3 遠端存取控制

這個設定可以啟動必要的 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。

開啟 **VPN 與遠端存取>>遠端存取控制**。

可用設定說明如下：

項目	說明
啟用 PPTP VPN 服務功能	勾選此方塊啟動經由 PPTP 通訊協定之 VPN 服務。
啟用 IPSec VPN 服務功能	勾選此方塊啟動經由 IPSec 通訊協定之 VPN 服務。
啟用 L2TP VPN 服務功能	勾選此方塊啟動經由 L2TP 通訊協定之 VPN 服務。
啟用 SSL VPN 服務功能	勾選此方塊啟動經由 SSL 通訊協定之 VPN 服務。
啟用 OpenVPN 服務功能	勾選此方塊啟動經由 OpenVPN 通訊協定之 VPN 服務。

完成設定之後，按下**確定**按鈕儲存相關設定。

IV-1-4 PPP 基本設定

這項功能可以應用在 PPP 相關的 VPN 連線中，諸如 PPTP、L2TP、L2TP over IPSec 等。

可用設定說明如下：

項目	說明
撥入 PPP 驗證	**限用 PAP -** 選擇此項目強迫路由器以 PAP 協定來驗證撥入使用者。 **PAP/CHAP/MS-CHAP/MS-CHAPv2 -** 選擇此項目表示路由器會嘗試先以 CHAP 協定驗證撥入使用者，如果撥入使用者沒有支援此項協定，系統會改用 PAP 協定來驗證使用者。
撥入 PPP 加密(MPPE)	**選用 MPPE -** 此選項代表 MPPE 加密方式是由路由器針對遠端撥入使用者選擇性採用的方法，如果遠端撥入使用者沒有支援 MPPE 加密演算式，路由器將會傳送無 MPPE 加密封包出去，否則 MPPE 加密將直接用於資料加密處理。 ● **需求 MPPE (40/128 位元) -**選擇此項目可以強迫路由器利用 MPPE 加密演算式加密資料封包，此外遠端撥入使用者在使用 128-bit 之前可先使用 40-bit 執行加密動作，換言之，如果沒有支援 128-bit 加密法，系統將會自動使用 40-bit 加密方式於資料加密上。 ● **最大 MPPE 值(128 位元)-**此選項指出路由器將會使用 MPPE 最大值(128 位元)來加密資料。
雙方共同驗證 (PAP)	共同驗證功能主要應用於和其他路由器或是需要雙向驗證的用戶連絡，以便取得更佳安全性能，因此當您的對點路由器需要共同驗證時，您就應該啟動此功能，並進一步指定使用者名稱和密碼。
撥入使用者的 IP 位址指派 (當 DHCP 停用時)	輸入撥入 PPP 連線的 IP 位址(LAN1) 。 LAN2 ~ LAN8 若有啟用則亦可設定 IP 位址，可前往 **LAN>>基本**

	設置開啟需要的 LAN 介面。
PPP 驗證方式	勾選您想要用來進行 PPP 連線驗證的方式。
當使用 RADIUS 驗證時	如果 PPP 連線將透過 RADIUS 伺服器進行驗證，您有必要指定一個 LAN 設定檔給予撥入使用者，以取得 IP 位址。

完成上述設定之後，請按下**確定**儲存。

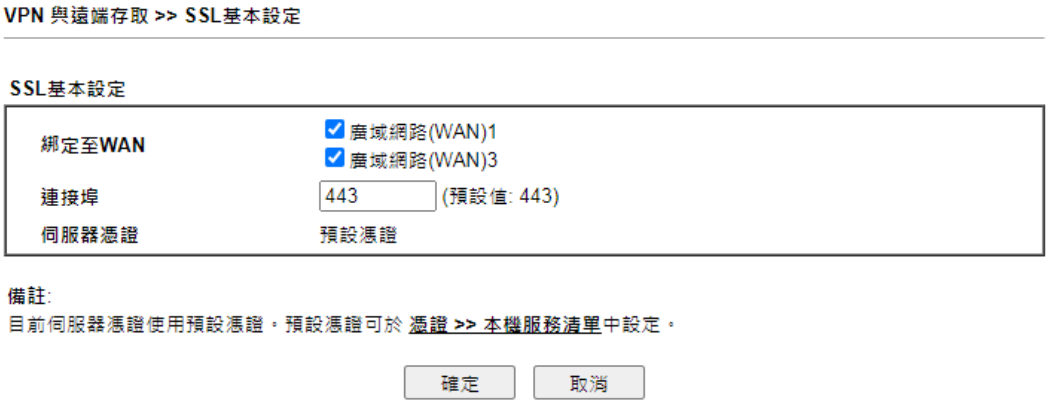
IV-1-5 SSL 基本設定

SSL VPN 是一種可以使用 SSL 來加密資料流量的 VPN 型式，與一些安全網站使用的技術是相同的。由於在網際網路加密協定上 SSL 的地位相當突出，因此大多數的網路對 SSL 的資訊流量幾乎沒有甚麼限制，結果就是當其他 VPN 技術因遭遇防火牆與 NAT 等障礙而停滯不前時，SSL VPN 更有機會能發揮作用。

簡而言之，

- 使用者不需要事先安裝 VPN 用戶端軟體進行 SSL VPN 連線
- 與傳統的其他 VPN 相比，透過 SSL VPN 加密的資料限制最少

本頁用來設定 SSL VPN 伺服器與 SSL 通道的基本設定值。



可用設定說明如下：

項目	說明
綁定至 WAN	選擇一個 WAN 介面，接收 SSL VPN 連線的封包流量輸入。
連接埠	用於 SSL VPN 伺服器的通訊埠號，此數值與系統維護>>管理頁面設定的管理埠口(HTTPS)值必須不同。預設值為 443。
伺服器憑證	指定用於 SSL 連線的憑證。可以選擇由路由器輸入或是路由器自行產生的憑證，或是選擇自行簽核，然後使用路由器內建的預設憑證。選定的憑證可同時用於 SSL VPN 伺服器與 HTTPS 網頁代理伺服器上。

完成上述設定之後，請按下**確定**儲存。

IV-1-6 IPSec IPSec 基本設定

在 **IPSec 基本設定**中，有二種主要的配置方式。

- 第一階段：IKE 參數的協商作業包含加密、重述、Diffie-Hellman 參數值和壽命，以保護後續 IKE 交換、使用預先共同金鑰或是數位簽章(x.509)之對等驗證。協商程式起始方提出所有的原則給遠端的另一方，遠端一方嘗試尋找符合其政策之最高優先權，最後建立一個 IKE 階段 2 的安全通道。
- 第二階段：IPSec 安全協商包含驗證封包頭(AH)或是 ESP，供後續 IKE 交換和雙邊安全通道設立之檢測之用。

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。

可用設定說明如下：

項目	說明
IKE 驗證方式	通常應用在遠端撥入使用者或是使用動態 IP 位址的節點(LAN-to-LAN)以及 IPSec 相關之 VPN 連線上，像是 L2TP over IPSec 和 IPSec 通道。有二種方式可用來驗證來自遠端撥入用戶的資料 - **憑證**以及**預先共享金鑰**。 **憑證** – X.509 憑證可用於 IKE 驗證。要設定路由器上使用的憑

	證，請前往憑證管理頁面。 **優選本機 ID** - 指定優選本機 ID 資訊(如替代主體名稱或是主體名稱)，當使用者使用一般設定的時候，這部分資訊可用於 IPsec 驗證(無須在 VPN 設定檔中指定對方 IP 或是 ID 身份)。 **一般預先共享金鑰** - 請指定一個金鑰作為一般驗證之用。 **確認一般共享金鑰(PSK)**- 再次輸入確認您所輸入的共用金鑰。 **XAuth 使用者 PSK 密鑰**-請指定一個金鑰作為 IPsec XAuth 驗證之用。 **確認 XAuth 使用者 PSK 密鑰**-再次輸入確認您所輸入的 IPsec XAuth 驗證需求之共用金鑰。 **注意：**來自遠端撥入使用者的任何一個封包，若不符合 **VPN 與遠端存取>>遠端撥入使用者**定義的規則，即會套用此處選擇的方式。
IPSec 安全防護方式	有三種方式 **基本 -** 表示資料將被驗證，但是並未加密。在預設值設定中，這個方式是啟用的。 **中度**-選擇此項時，AH 協定可用來驗證 IPsec 資料流量。 **高** - 選擇此項時，ESP 協定可用來驗證及加密 IPsec 資料流量，有三種加密標準，按照安全排序分別為 DES, 3DES 與 AES。

完成設定之後，按下**確定**按鈕儲存相關設定。

IV-1-7 IPSec 端點辨識

如果在 LAN-to-LAN 連線或是遠端撥入使用者連線上，想要使用數位認證作為遠端驗證工具，您可以編輯對方認證表格供後續選擇使用。路由器提供 32 種 IPSec 端點辨識設定檔：

索引	啟用	名稱	索引	啟用	名稱
1.	☐	???	17.	☐	???
2.	☐	???	18.	☐	???
3.	☐	???	19.	☐	???
4.	☐	???	20.	☐	???
5.	☐	???	21.	☐	???
6.	☐	???	22.	☐	???
7.	☐	???	23.	☐	???
8.	☐	???	24.	☐	???
9.	☐	???	25.	☐	???
10.	☐	???	26.	☐	???
11.	☐	???	27.	☐	???
12.	☐	???	28.	☐	???
13.	☐	???	29.	☐	???
14.	☐	???	30.	☐	???
15.	☐	???	31.	☐	???
16.	☐	???	32.	☐	???

可用設定說明如下：

項目	說明
設定回復出廠預設值	按此鈕清除全部設定。
索引	請按索引下方的號碼以進入設定頁面。
啟用	勾選此框啟用該設定檔。
名稱	顯示 LAN-to-LAN 設定檔案中特定撥入使用者的使用者名稱，符號**???**代表該設定檔是空的，未做任何設定。

點選每個索引號碼以便編輯遠端使用者設定檔，每個撥入類型需要您在右邊填入不同資訊，如果該區域是灰色的，即表示您無法在該項目做任何設定，下面的說明可以引導您於各個設定區填入相關資訊。

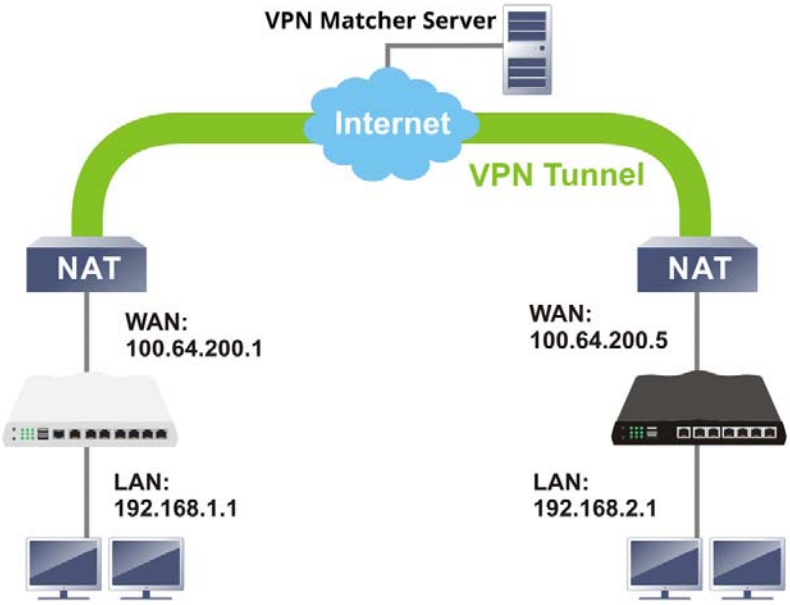
可用設定說明如下：

項目	說明
啟動此帳號	勾選方框啟用帳號設定檔。
設定檔名稱	請輸入此設定檔的檔名。
接受任何對方 ID	按此鈕可以接受任何一個電腦的連線而不理會它是誰。
接受主體替代名稱	按此鈕以決定特定之數位簽章接受符合要求的對手，本區可以是 IP 位址、網域或是電子郵件，類型下方區域方塊依據您所選的類型而有所不同，請按照實際需要填入必要資訊。
接受主體名稱	按此鈕讓特定區域的數位簽章能接受符合要求的對手，本區包含有國家、狀態、居住地區、組織、單位、常用名稱及電子郵件等等。

完成設定之後，按下**確定**按鈕儲存相關設定。

IV-1-8 VPN Matcher 設定

一般來說要建立 VPN 連線，至少要有一方具備真實 IP 位址，VPN Matcher 伺服器可幫助讓二台在 NAT 後方的居易路由器建立安全的 VPN 通道，方便雙邊進行資料傳輸。請先參考下圖



還有一個 VPN 連線上小小的限制，雙邊路由器必須都在錐形 NAT 後方，而不是對稱型 NAT。

開啟 **VPN 與端存取>>VPN Matcher 設定**頁面。

可用設定說明如下：

項目	說明
啟用 / 停用	按此可啟用/停用 VPN Matcher 設定的功能。
VPN Matcher 伺服器	居易 VPN Matcher 伺服器的 IP 位址定義為 "vpn-matcher.draytek.com"，埠號為"31503"
路由器清單金鑰	輸入驗證金鑰，在 VPN Matcher 伺服器上尋找跟這台裝置相同群組的 Vigor 路由器。接著在二台路由器之間設立一個 VPN 鏈結，可透過 VPN 設定精靈來處理。

確定	按此儲存設定。
STUN 伺服器	**偵測** - 按此可檢查路由使用的 NAT 是否為錐形 NAT，因為如果不是，那麼將無法建立 VPN 連線。
群組裝置清單	**取得清單** - 輸入驗證金鑰之後，可按此鈕取得跟這台裝置相同群組且可用的 Vigor 路由器。

IV-1-9 OpenVPN

OpenVPN 通訊協定使用公開金鑰、憑證、使用者名稱及密碼來驗證用戶。資料流量可透過符合工業標準的 SSL/TLS 加密協定等安全頻道來攜帶傳輸。

藉由整合 OpenVPN，Vigor 路由器可幫助用戶實現更可靠、穩定且安全的私人連線，滿足商業要求。

OpenVPN 提供方便的方式給本機及遠端用戶雙邊建立 VPN 連線，主要有二種優點:

- 可在不同的平台諸如 Windows, Linux, 及 MacOS 上操作
- 基於 SSL 加密的標準協議，OpenVPN 可提供擴展的用戶端/伺服器模式，允許多用戶透過單一 TCP 或 UDP 埠號連接到單一 OpenVPN 伺服器。

IV-1-9-1 OpenVPN 伺服器設定

OpenVPN 需要使用到憑證，在建立連線之前，必須先設定好 OpenVPN 服務的基本設定。

可用設定說明如下：

項目	說明

基本設置	
UDP	**啟用 -** 勾選此框啟用 UDP 通訊協定。 **UDP 埠號** – 輸入 UDP 埠號。
TCP	**啟用-**勾選此框啟用 TCP 通訊協定。 **TCP 埠號**–輸入 TCP 埠號。
密碼演算法	請選擇適當的演算方式，共有二種加密方式: AES128 以及 AES256。因為計算量更高的緣故，AES256 比 AES128 更為安全，但是性能較低。
HMAC 演算法	HMAC 為 Hash-based Message Authentication Code 的縮寫，用於驗證 VPN 資料的完整性與真實性。 請選擇適當的 HMAC 演算方式，有二種可以選擇: SHA1 以及 SHA256。建議使用 SHA256。
憑證驗證	如果您想驗證客戶憑證是否由具公信力且受信賴的 CA 所發行，請勾選此框。
憑證設置	
憑證來源	請選擇用於 OpenVPN 的憑證來源。 **路由器產生憑證** - 用於 OpenVPN 的憑證是由路由器產生的 ● **產生** - 按此鈕產生憑證。 ● **刪除所有的憑證** - 按此可移除所有路由器所產生的憑證。 **上傳憑證至路由器** - 用於 OpenVPN 的憑證是由第三方機構所產生 ● **具公信力之 CA** - 使用下拉式清單選擇已經事先上傳到路由器具公信力的 CA 憑證。如果要在多加幾個且先上傳至路由器，請按**具公信力之 CA** 連結，系統將會自動導引並開啟**憑證管理>>具公信力之 CA 憑證**頁面。 ● **伺服器憑證** - 使用下拉式清單選擇已經事先上傳到路由器的伺服器憑證。如果要在多加幾個且先上傳至路由器，請按**伺服器憑證**連結，系統將會自動導引並開啟**憑證管理>>本機憑證**頁面。

完成設定之後，按下**確定**按鈕儲存相關設定。

IV-1-9-2 用戶端 Config 設定

在此頁面您可以建立並輸出設定內容，方便遠端 OpenVPN 用戶端得以連接至此路由器。

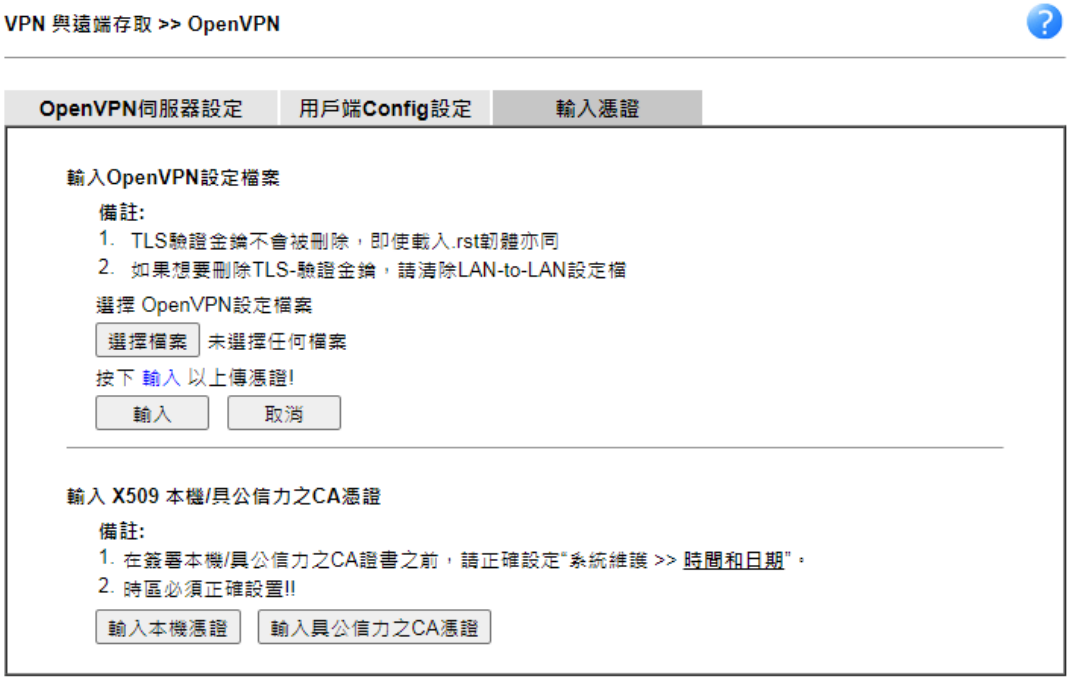
可用設定說明如下：

項目	說明
遠端伺服器	OpenVPN 用戶可使用 IP 位址或是網域名稱連接至路由器。請選擇 IP 位址或是網域名稱選項。 **IP 位址** – OpenVPN 設定檔案將使用 IP 位址作為伺服器之位址。 **網域** – OpenVPN 設定檔案將使用網域作為伺服器之位址。. **VPN matcher** - OpenVPN 設定檔案將使用 VPN matcher 作為伺服器之位址。
傳輸通訊協定	選擇 UDP 或是 TCP 作為 OpenVPN 用戶連接至路由器的通訊協定。
自動撥出	**啟用** - 選擇此項讓遠端用戶能自動撥打給這台路由器，建立 OpenVPN 通道。 **停用** - 選擇此項，停用此功能。
設定 VPN 作為預設閘道	**啟用** - 選擇此項讓路由器可被當成 OpenVPN 用戶的預設閘道。OpenVPN 用戶將透過 OpenVPN 通道重新導向所有的資料流量到 Vigor 路由器。 **停用** - 選擇此項，停用此功能。

自動重新連線之暫存密碼	**啟用** - OpenVPN 每小時都會重新連線，當重新連線時，需要重新輸入密碼。啟用此功能後，該密碼將會被系統紀錄著，且在每次更新的時候自動使用密碼進行連線。 **停用** - 選擇此項，停用此功能。
UDP Ping	若是沒有任何封包在此指定的時間內傳輸，那麼可使用此功能，透過 UDP 控制頻道來查看遠端裝置。
UDP Ping 離開	若在經過一段時間（此處所設定）之後，沒有從遠端裝置獲得封包或是收到 ping 需求，中斷 OpenVPN。
檔案名稱	輸入設定檔的檔案名稱，以便從路由器下載下來。
用戶端憑證	輸入由第三方取得之用戶端憑證的檔案名稱。
用戶端金鑰	輸入由第三方取得之虛擬金鑰檔案名稱。
郵件設定檔	使用下拉式清單指定一個郵件設定檔。 **郵件位址** - 輸入郵件位址以便接收通知郵件。 **傳送電子郵件** - 按此傳送 OpenVPN Config。
輸出	按此鈕下載本頁設定為一個檔案，此檔案可以由 VPN 用戶端輸入使用並建立一個 OpenVPN 連線。

IV-1-9-3 輸入憑證

在此頁面上，您可從其他地方輸入憑證，供遠端 OpenVPN 用戶與路由器連線使用。



可用設定說明如下：

項目	說明
輸入 OpenVPN 設定檔案	
選擇 OpenVPN 設定檔案	**選擇檔案** - 按此以選擇檔案。 **輸入** - 按此上傳選擇的設定檔案。

輸入 X509 本機/具公信力之 CA 憑證	
輸入本機憑證	按此進入本機憑證頁面以利輸入憑證。
輸入具公信力之 CA 憑證	按此進入具公信力之 CA 憑證頁面以利輸入憑證。

IV-1-10 遠端撥入使用者

藉由維護遠端使用者設定檔表格，您可以管理遠端存取狀況，這樣使用者可以經由驗證得以撥入或是建立 VPN 連線。您可以設定包含指定連線對點 ID、連線 ID (PPTP、IPSec Tunnel 以及 L2TP 和 L2TP over IPSec)等參數，和相關安全防護方式。

路由器提供 32 種存取使用者號碼予撥入用戶，此外經由內建 RADIUS 用戶端功能，您可以將帳號延伸至 RADIUS 伺服器。下圖顯示帳號總表格：

索引	啟用	使用者	狀態	索引	啟用	使用者	狀態
1.	☐	???	---	17.	☐	???	---
2.	☐	???	---	18.	☐	???	---
3.	☐	???	---	19.	☐	???	---
4.	☐	???	---	20.	☐	???	---
5.	☐	???	---	21.	☐	???	---
6.	☐	???	---	22.	☐	???	---
7.	☐	???	---	23.	☐	???	---
8.	☐	???	---	24.	☐	???	---
9.	☐	???	---	25.	☐	???	---
10.	☐	???	---	26.	☐	???	---
11.	☐	???	---	27.	☐	???	---
12.	☐	???	---	28.	☐	???	---
13.	☐	???	---	29.	☐	???	---
14.	☐	???	---	30.	☐	???	---
15.	☐	???	---	31.	☐	???	---
16.	☐	???	---	32.	☐	???	---

可用設定說明如下：

項目	說明
設定回復出廠預設值	按此鈕清除全部設定。
檢視	全部 - 按此顯示全部使用者帳號。

	上線 – 按此顯示上線使用者帳號。 **離線**– 按此顯示下線使用者帳號。
索引	請按索引下方的號碼以進入遠端撥入使用者之設定頁面。
使用者	顯示 LAN-to-LAN 設定檔案中特定撥入使用者的使用者名稱，符號**???**代表該設定檔是空的，未做任何設定。
狀態	顯示特定撥入使用者的存取狀態，符號 V 和 X 分別代表活動中與不活動的檔案。
備份	按下**備份**儲存設定。
還原	按下**選擇檔案**挑選設定檔，接著按下**還原**按鈕套用檔案。

點選每個索引號碼以便編輯遠端使用者設定檔，每個撥入類型需要您在右邊填入不同資訊，如果該區域是灰色的，即表示您無法在該項目做任何設定，下面的說明可以引導您於各個設定區填入相關資訊。

可用設定說明如下：

項目	說明

使用者帳號與驗證	**啟用此帳號** - 勾選此方塊以啟用此功能。 **允許多重同時連線** -勾選此方塊後，系統允許多位 VPN 用戶使用相同的帳號密碼與 Vigor 裝置連線。 **閒置逾時** - 如果撥入使用者閒置超過所設定的時間，路由器將會自動中斷連線，預設閒置逾時為 300 秒。
允許撥入類型	**PPTP-**爲伺服器建立一個透過網際網路的 PPTP VPN 連線，您必須設定連線類型和身分辨識像是使用者名稱與密碼等，以便驗證遠端伺服器。 **IPSec 通道 -** 允許遠端撥入使用者透過網際網路觸發 IPSec VPN 連線。 **含 IPSec 策略之 L2TP** - 爲伺服器建立一個透過網際網路的 L2TP VPN 連線。您可以選擇使用單獨 L2TP 或是含有 IPSec 的 L2TP，請自下拉式選項選取： ● **無** - 此選項完全不會應用 IPSec 原則，VPN 連線採用不帶有 IPSec 原則的 L2TP，可以在完全 L2TP 連線中檢視內容。 ● **建議選填** - 如果在整個連線過程中完全可以運用，此選項會先應用 IPSec 原則。否則撥入 VPN 連線會成為一種完全的 L2TP 連線。 ● **必須** - 此選項可在 L2TP 連線中明確指定所要運用的 IPSec 原則。 **SSL 通道 –** 允許遠端撥入用戶透過網際網路進行 SSL VPN 連線。 **指定遠端節點** - 您可以指定遠端撥入使用者或是對方 ID (應用於 IKE 主動模式中)的 IP 位址。若您不勾選此項，即表示您所選擇的連線類型，將會應用**基本設定**中所設定的驗證方式和安全防護方式。 **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。 ● **阻擋** – 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。 **經由 VPN 執行多重播送(Multicast 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。 ● **阻擋** – 此為預設值。點選此鈕之後，路由器將會封鎖多重播送封包。 **使用者名稱** – 當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區是可應用的。 **密碼** – 當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區是可應用的。 **啟用 mOTP 功能** - 勾選此框以便利用 mOTP 功能進行驗證。 **PIN 碼** – 輸入驗證專用碼(例如 1234)。 **密鑰** – 使用行動電話中由 mOTP 產生的 32 個數字密碼(例如 e759bb6f0e94c7ab4fe6)。
子網	選擇此 VPN 設定檔所需的子網。 **分派靜態 IP 位址** – 請輸入固定 IP 位址。
IKE 驗證方式	當您指定遠端節點的 IP 位址時，本區僅適用於 **IPsec 通道**與**具**

	有 **IPSec** 原則的 **L2TP** 類型，唯一例外的是當您選擇 **IPsec 通道**時，不論有無指定 IP 位址，您還可以設定數位簽章(X.509)。 **預先共享金鑰**–勾選此方塊啟用此功能並輸入 1-63 文字做為預先共同金鑰。 **數位簽章 (X.509)** –勾選此方塊啟用此功能並選擇一組事先定義的簽章內容 (在 **VPN 與遠端存取>>IPSec 端點辨識**中設定)。
IPSec 安全性方法	對 IPSec 通道和 L2TP 含 IPSec 原則來說，本區為必要設定。請勾選中級或是高級設定作為安全防護方式。 **中度 -Authentication Header (AH)**表示資料將被驗證，但未被加密，此選項的預設時是勾選狀態。 **高 -Encapsulating Security Payload (ESP)**表示資料將被加密及驗證，請自下拉式清單中選取適合項目。 **本機 ID(視需要填入) -**指定一個本地 ID 以便作為 LAN-to-LAN 的撥入設定，此項是選擇項目且只能應用在 IKE 主動模式上。
排程設定檔	最多可指定四組排程。

完成設定之後，按下**確定**按鈕儲存相關設定。

IV-1-11 LAN to LAN

您可以透過維護連線檔案的表格來管理 LAN-to-LAN 連線，您可設定包含指定連線方向(撥進或是撥出)的參數、連線對方的 ID、連線型態(VPN 含 PPTP, IPSec Tunnel 和 L2TP 或是其他)以及相關的安全防護方法等等。

路由器提供 32 個設定檔，下圖顯示設定檔案的簡易清單。

可用設定說明如下：

項目	說明
設定回復出廠預設值	按此鈕清除全部設定。
索引	請按索引下方的號碼以進入設定頁面。
啟用	勾選此框啟用此設定檔。
永遠連線	勾選此框讓此設定檔一旦被使用，其連線可保持連線。
名稱	意即 LAN-to-LAN 檔案名稱，**???**符號代表該檔案目前是空的。
遠端網路	顯示遠端網路的名稱。
狀態	**線上**- 表示此 LAN to LAN 設定檔目前運作中。

	離線– 表示此 LAN to LAN 設定檔目前並未運作，即使已經啟動。
變更預設路由至…	變更預設路由至選定的 VPN 通道上。
允許路由模式的 LAN 介面傳送封包至 VPN 通道	若勾選此項，來自 LAN 路由之封包可以透過 VPN 通道來傳送。
當 VPN 中斷時，將封包傳送到 WAN 端	若勾選此項，當 VPN 斷線時，封包可以透過 WAN 介面來傳送。
備份	按下**備份**儲存設定。
還原	按下**選擇檔案**挑選設定檔，接著按下**還原**按鈕套用檔案。

如欲編輯設定檔，請：

1. 請按索引編號連結以編輯個別設定檔，按下後可看到如下的頁面，每個 LAN-to-LAN 檔案包含有四個子群組，如果該區域是灰色的，即表示您無法在該項目做任何設定，下面的說明可以引導您於各個設定區填入相關資訊。由於網頁太長，我們將之切成數個段落來說明。

可用設定說明如下：

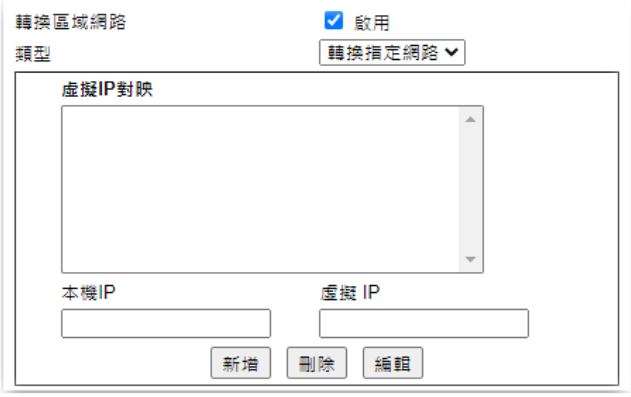
項目	說明
常見設定	
啟用此設定檔	按此方塊啟用此設定檔。 **設定檔名稱** - 針對此 LAN-to-LAN 連線，請指定一個設定檔案名稱。 **撥號方向**–針對此 LAN-to-LAN 連線，請指定允許的撥號方向。 ● **雙向** – 發話方/接話方 ● **撥出** – 發話方 ● **撥入** – 接話方 **撥出經由**-使用下拉式選項選擇適合的 WAN 介面，此設定僅適合撥出時使用。 ● **WAN#優先** - 連線時，路由器會將 WAN1#視為 VPN 連線的首要選擇，如果 WAN#連線失敗，路由器將使用其他 WAN 介面來取代。 ● **限用 WAN#** - 連線時，路由器會將 WAN1#視為 VPN 連線的唯一選擇。 **永遠連線**–勾選此方塊讓路由器永遠保持 VPN 連線。 **閒置逾時**–預設值為 300 秒，若連線閒置時間超過此數值，路由器將自動中斷連線。 **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。 ● **阻擋**– 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。 **經由 VPN 執行多重播送-**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。 ● **阻擋** – 此為預設值。點選此鈕之後，路由器將會封鎖多重播送封包。
撥出設定	
VPN 伺服器類型	選擇一個類型。每種類型都會帶出不同的細部設定。 ● **PPTP-**為伺服器建立一個透過網際網路的 PPTP VPN 連線，您必須設定連線類型和身分辨識像是使用者名稱與密碼等，以便驗證遠端伺服器。 ● **IPSec 通道-**為伺服器建立一個透過網際網路的 IPSec VPN 連線。 ● **含 IPsec 策略之 L2TP** -為伺服器建立一個透過網際網路的 L2TP VPN 連線。您可以選擇使用單獨 L2TP 或是含有 IPSec 的 L2TP，請自下拉式選項選取： **無-** 此選項完全不會應用 IPSec 原則，VPN 連線採用不帶有 IPSec 原則的 L2TP，可以在完全 L2TP 連線中檢視內容。 **建議選填-**如果在整個連線過程中是可以運用的情形下，此選項會先應用 IPSec 原則。否則撥出 VPN 連線會成為一種完全的 L2TP 連線。 **必須-** 此選項可在 L2TP 連線中明確指定所要運用的 IPSec

	原則。 ● **SSL 通道** - 透過網際網路建立 SSL VPN 連線。 ● **OpenVPN 通道**- 透過網際網路建立 OpenVPN 連線。
伺服器 **IP/**主機名稱	輸入遠端 VPN 主機的 IP 位址或是 DNS 主機名稱。
排程設定檔	可以輸入四組時間排程，全部的排程都是在**其他應用>>排程**網頁中事先設定完畢，您可在此輸入該排程的索引編號。
使用者名稱	當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區是可應用的。
密碼	當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區是可應用的。
當 **PPTP/** 含 **IPsec** 策略之 **L2TP/** **SSL** 通道選擇為 **VPN** 伺服器類型	**PPP 進階設定** - 按此展開 PPP 進階設定。 ● **PPP 驗證-**當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區是可應用的。PAP/CHAP 是最平常的選項。 ● **VJ 壓縮-**當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區是可應用的。VJ 壓縮可作為 TCP/IP 協定標頭壓縮之用，通常設定選擇**開啟**以改善頻寬利用的狀況。 ● **請求 IP 位址-**輸入 IP 位址。
當 **IPsec** 通道/含 **IPsec** 策略之 **L2TP** 選擇為 **VPN** 伺服器類型	**IKE Phase 1 設定 -** 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，因為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。路由器的預設值為**主要模式**。 ● **驗證- 數位簽章(X.509)** - **對方 ID -**自下拉式清單中(設定於 **VPN 與遠端存取>>IPsec 端點辨識**)選擇對方的 ID。 - **本機 ID -** 指定一個本機 ID(**替代主體名稱**或是**主體名稱**，用於撥入設定，這個項目是選填項目。 - **本機憑證-** 自下拉式清單中選擇一種憑證，您必須事先在**憑證管理>>本機憑證**中設定至少一組的憑證，否則無憑證正可以使用。 ● **驗證-預先共享金鑰(PSK)** - **預先共享金鑰(PSK) -** 輸入 1-128 字元作為 **IKE 預先共享金鑰**。 - **本機 ID -** 輸入本機 IKE 辨識碼已便於建立 IPsec 連線時能做為資訊交換用。 ● **提案加密** - 使用自動/ AES/ 3DES/ DES 加密演算法。 ● **提案 ECDH 群組 -** 指定一個群組選項。若提案加密選擇的不是自動，請在此挑選一個群組項目。 ● **提案驗證**- 可選 SHA256、SHA1 以驗證封包。 ● **強迫使用 UDP 封裝 -** 選擇此項強迫封裝 UDP。所有的封裝的 IPsec 封包都會加上 UDP 標頭。 **IKE Phase 2 設定 -** 指定安全性通訊協定、提案加密與提案驗證等資訊。 ● **安全性通訊協定** - AH (中等) 表示資料會被驗證但未被加密，此為預設選項。ESP (高) 表示資料會加密且被驗證。 ● **提案加密** - 使用 AES/3DES 加密演算法並套用 MD5 或 SHA-1 驗證演算法。

	● **提案驗證-** 可選擇全部、SHA256 或是無。 **IKE 進階設定-**指定模式、建議和 IKE 階段金鑰有效時間等設定，可按**進階**按鈕進入進階設定。 ● **階段 1 金鑰有效時間(IKE phase 1 key lifetime)-** 考慮到安全之故，使用者必須訂定有效時間，預設值為 28800 秒，您可以在 900 與 86400 秒之間指定所需的時間值。 ● **階段 2 金鑰有效時間(IKE phase 2 key lifetime)-** 考慮到安全之故，使用者必須訂定有效時間，預設值為 3600 秒，您可以在 600 與 86400 秒之間指定所需的時間值。 ● **階段 2 網路 ID -** 這是選填設定，當在 TCP/IP 網路設定區域中選擇了 NAT 模式，請變更 VPN 流量的來源 IP 位址為此處指定的 IP 位址。 ● **啟用完美前向保密 PFS -** IKE Phase 1 密鑰可再次使用以便防止 phase 2 產生計算複雜的問題。預設狀況是不啟用此功能。 **PING 以維持連線狀態 -** 勾選此項啟用此功能。 **PING 目標 IP -** 輸入目標 IP 位址以便維持連線。
當 OpenVPN 通道選擇為 VPN 伺服器類型	**OpenVPN 進階設定 -** 按此可展開進階設定。 ● **密碼演算法 -** 選擇一種加密方式來處理透過 OpenVPN 傳送的封包。 ● **HMAC 演算法 -**選擇一種驗證式來處理透過 OpenVPN 傳送的封包。 ● **用戶端憑證 -** 指定一個用戶端憑證或是自行簽署一個新的憑證或是使用 DrayDDNS 憑證。 ● **具公信力之 CA -** 指定一個具公信力的 CA 憑證。 ● **壓縮 -** 選擇壓縮方式將封包進行壓縮，如此即可在傳輸封包時減少頻寬用量。 ● **TLS 驗證 -** 選擇開啟使用此驗證方式，相關金鑰可以按**檢視**來查看。 **輸入 OpenVPN 設定檔案 -** 來自其他機種的 OpenVPN 設定檔可以套用到此機種上。 ● **選擇檔案 -** 自硬碟選擇需要的設定檔。 ● **輸入 -** 按此上傳選擇的設定檔案至此 Vigor 路由器。
撥入設定	
允許 VPN 類型	以不同類型來決定撥入連線。 ● **PPTP-**允許遠端撥入用戶透過網際網路達成 PPTP VPN 連線，請設定遠端撥入用戶的使用者名稱和密碼。 ● **IPSec 通道(IKEv1/IKEv2)-**允許遠端撥入用戶透過網際網觸發 IPSec VPN 連線。 ● **IPsec XAuth** ● **含 IPSec 策略之 L2TP-**允許遠端撥入用戶透過網際網路製造 L2TP VPN 連線，您可以選擇使用單獨 L2TP 或是含有 IPSec 的 L2TP，請自下拉式選項選取： ■ **無-** 此選項完全不會應用 IPSec 原則，VPN 連線採用不帶有 IPSec 原則的 L2TP 可以在完全 L2TP 連線中檢視內容。 ■ **建議選填-**如果在整個連線過程中是可以運用的情形

	下，此選項會先應用 IPSec 原則。否則撥出 VPN 連線會成為一種完全的 L2TP 連線。 ■ **必須 -** 此選項可在 L2TP 連線中明確指定所要運用的 IPSec 原則。 ● **SSL 通道-** 讓遠端撥入使用者透過網際網路觸發 SSL VPN 連線。 ● **OpenVPN 通道**
指定遠端 VPN 閘道	您可勾選此項，並指定遠端撥入用戶的真實 IP 位址或 ID (必須與撥入類型中所設定的 ID 相同)。此外針對 VPN 功能，您應該進一步指定右邊相關安全設定。 如果您不勾選此方框，您上述選定的連線類型將會套用基本設定中所選用的驗證方式及安全性方法。 **使用者名稱-**當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區是可應用的。 **密碼-**當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區是可應用的。
PPP 進階設定	按此開展 PPP 進階設定。 **VJ 壓縮(VJ Compression)-**當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區是可應用的。VJ 壓縮可作為 TCP/IP 協定標頭壓縮之用。 **分派對方 IP 位址-**輸入 IP 位址。
OpenVPN 進階設定	按此展開進階設定。 **密碼演算法 -** 選擇一種加密方式來處理透過 OpenVPN 傳送的封包。 **HMAC 演算法 -**選擇一種驗證式來處理透過 OpenVPN 傳送的封包。
允許 IKE 驗證方式	當您指定遠端節點的 IP 位址時，IKE 驗證可套用在 IPSec 通道和含 IPSec 原則之 L2TP 上。不過，不管有沒有指定遠端節點的 IP 位址予 IPSec 通道使用，您仍然可以設定數位簽章(X.509)。 **預先共享金鑰-** 勾選此方塊啟用此功能並按 **IKE 預先共享金鑰** 按鈕輸入金鑰及確認金鑰。 **X509 數位簽章-**勾選此方塊啟用此功能並自下拉式清單中選擇 **VPN 遠端存取控制>>IPSec 端點辨識**中所預先定義的設定檔。 ● **優選本機 ID**–指定先檢測下方哪一種類型。 **- 替代主體名稱**– 先檢測替代主體名稱(於**憑證管理>>本機憑證**中定義)。 **- 主體名稱**–先檢測主體名稱(於**憑證管理>>本機憑證**中定義)。
允許 IPSec 安全性方式	當您指定遠端模式時，對 IPSec 通道和 L2TP 含 IPSec 原則來說，本區為必要設定。 ● **AH -**表示資料將被驗證，但未被加密，此選項的預設時是勾選狀態。 ● **ESP-DES/ESP-3DES/ESP-AES -** 表示資料將被加密及驗證，請選取適合項目。
TCP/IP 網路設定	
本機網路	**IP 位址/遮罩-** 顯示 TCP / IP 設定中的本機網路 IP 位址與遮

	罩，如有必要，您可以修改設定。
遠端網路	**IP 位址/遠遮罩-** 新增一個靜態路由以便透過網際網路，引導遠端網路 IP 位址/遠端網路遮罩預定之全部傳輸流量。對 IPSec 而言，這項設定是第二階段快速模式的目的用戶端之身分。
更多遠端子網	新增一個靜態路由，並藉由網際網路引導更多的遠端網路 IP 位址/遠端網路遮罩預定之全部傳輸流量。通常在您發現遠端 VPN 路由器有數個子網路存在時，您會使用此按鈕設定更多的路由。
模式	如果遠端網路只允許您以單一 IP 撥號，請選擇 **NAT** 否則請選擇**路由**。
透過 VPN 進行 RIP	此選項指定 RIP (路由資訊協定) 封包的方向，您可以啟用也可以停用 RIP 方向，於此，我們提供您四種選擇：傳送/接收、限用傳送、限用接收以及停用。
當模式設定為路由時	當選擇**路由**時，可用的選項設定如下： **轉換區域網路** - 勾選此框啟用此功能。增加靜態固定路由，透過 VPN 連線，導引全部流量至遠端網路 IP 位址/遠端網路遮罩。這個功能通常在您發現遠端 VPN 路由器後方有數個子網時使用。 **類型** - 共有 2 種(**轉換整個子網**與**轉換指定 IP**)可以選擇 選擇**轉換整個子網**時，可設定的項目如下 - **本機子網** - 選擇內含之 IP 位址準備被轉譯的區域網路。 - **轉換的 IP** - 指定一個位址。 - **更多本機子網** - 按此新增更多的子網。 當選擇**轉換指定 IP** 時，可設定的項目如下

	 - **虛擬 IP 對映 –** 系統跳出視窗讓您指定本機 IP 位址以及對映的虛擬 IP 位址。
當模式設定為 NAT 時	當選擇 **NAT** 時，可用的選項設定如下： **透過 VPN 進行 RIP-**此選項指定 RIP (路由資訊協定) 封包的方向，您可以啟用也可以停用 RIP 方向，於此，我們提供您四種選擇：傳送/接收、限用傳送、限用接收以及停用。 ● 傳送/接收- 可傳送或接收 RIP 封包 ● 限用傳送 – 僅傳送但未接收 RIP 封包 ● 限用接收 – 僅接收但未傳送 RIP 封包 ● 停用 – 停用 RIP **變更預設路由此 VPN 通道-**勾選此方塊變更此 VPN 通道的預設路由。

2. 完成設定之後，按下**確定**按鈕儲存相關設定。

IV-1-12 連線管理

您可以查看全部 VPN 連線的總結清單，您可中斷任何一個 VPN 連線，只要輕輕按下**中斷**按鈕即可。您也可以使用撥出工具並按**撥號**按鈕主動撥出任何的電話。

可用設定說明如下：

項目	說明
撥出工具	**撥號** - 按此鈕執行撥號功能。 **更新頁面-**按此鈕以重新顯示整個連線狀態。

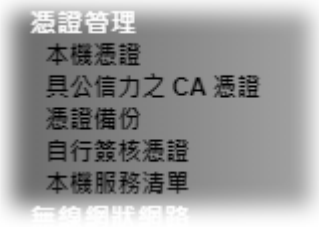
IV-2 憑證管理

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。

網頁使用者介面



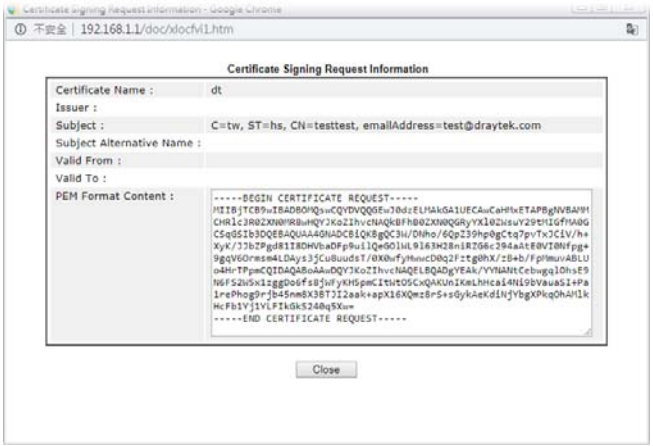
IV-2-1 本機憑證

尚無憑證的頁面：

請求簽署憑證的頁面：

可用設定說明如下：

項目	說明

名稱	顯示憑證的名稱。
主體	顯示憑證的主體名稱。
狀態	顯示憑證目前的狀態。
修正	**檢視**–按此鈕以檢視憑證詳細的設定。  **刪除**–按此鈕刪除選定的憑證及其相關資訊。
產生	按此鈕以開啟**產生憑證簽署需求**視窗。 輸入全部的資訊，然後再按一次**產生**按鈕。
輸入	按此鈕以匯入儲存的檔案作為憑證資訊。
憑證存放	顯示儲存用量(以百分比呈現)。
頁面更新	按此鈕以更新資訊。

產生

按下此鈕開啟**產生憑證簽署需求**視窗，輸入所有必要資訊，例如檔名(用來分辨憑證)、主體替代名稱類型以及相關的設定內容，然後按最下方的**產生**按鈕。

憑證管理 >> 本機憑證

產生憑證簽署需求

憑證名稱

主體替代名稱
類型 IP 位址
IP 位址

主體名稱
國家
州(ST)
位置
組織(O)
組織單位(OU)
常見名稱 (CN)
電子郵件(E)

金鑰種類 RSA
金鑰大小 2048 位元
演算法 SHA-256

產生

資訊 請注意常用名稱必須設定為路由器的 WAN IP 位址或是網址。

輸入

路由器可讓您產生憑證需求並提交至 CA 伺服器，後續讓您匯入作為本機憑證。如果您已經從第三方取得了憑證，您也可以直接採用。支援的類型為 PKCS12 憑證以及含有密鑰的憑證。

按下此鈕後可以匯入檔案作為憑證資訊，有三種本機憑證類型可以運用。

憑證管理 >> 本機憑證

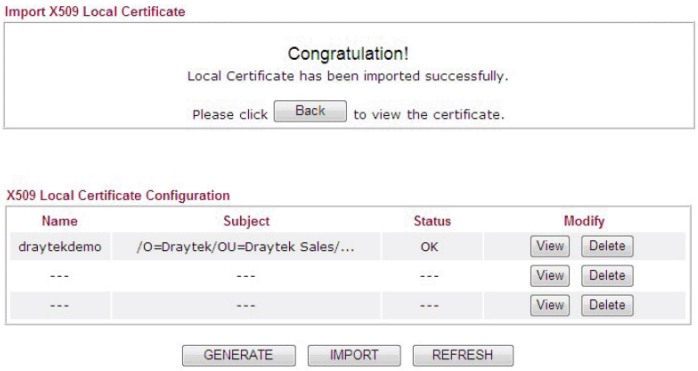
輸入 X509本機憑證

上傳本機憑證
選擇本機憑證檔案
憑證檔案: 選擇檔案 未選擇任何檔案
按下 匯入 以上傳至本機憑證
輸入 取消

上傳PKCS12憑證
選擇PKCS12檔案
PKCS12檔案: 選擇檔案 未選擇任何檔案
密碼:
按下 輸入 以上傳 PKCS12 檔案
輸入 取消

上傳憑證與虛擬金鑰
選擇憑證檔案以及與其匹配之虛擬金鑰
憑證檔案: 選擇檔案 未選擇任何檔案
金鑰檔案: 選擇檔案 未選擇任何檔案
按下 輸入 以上傳本機憑證與虛擬密鑰
輸入 取消

可用設定說明如下：

項目	說明
上傳本機憑證	可讓使用者輸入路由器產生的且由 CA 伺服器簽署之憑證。 如果您已完成憑證產生作業，憑證的狀態欄會顯示**確定**。 
上傳 **PKCS12** 憑證	可讓使用者輸入副檔名為.pfx 或 .p122 的憑證，這些憑證通常需要密碼驗證。 請注意 PKCS12 為安全儲存虛擬密鑰與憑證的一種標準，主要用於 Netscape 與微軟 IE 上。
上傳憑證與虛擬金鑰	這個功能在使用者有不同的憑證與虛擬密鑰時特別有用，若金鑰本身需要加密，那麼請輸入密碼內容。

IV-2-2 具公信力之 CA 憑證

具公信力 CA 憑證列出三組憑證，若有必要，您也可以建立一個 RootCA 憑證。

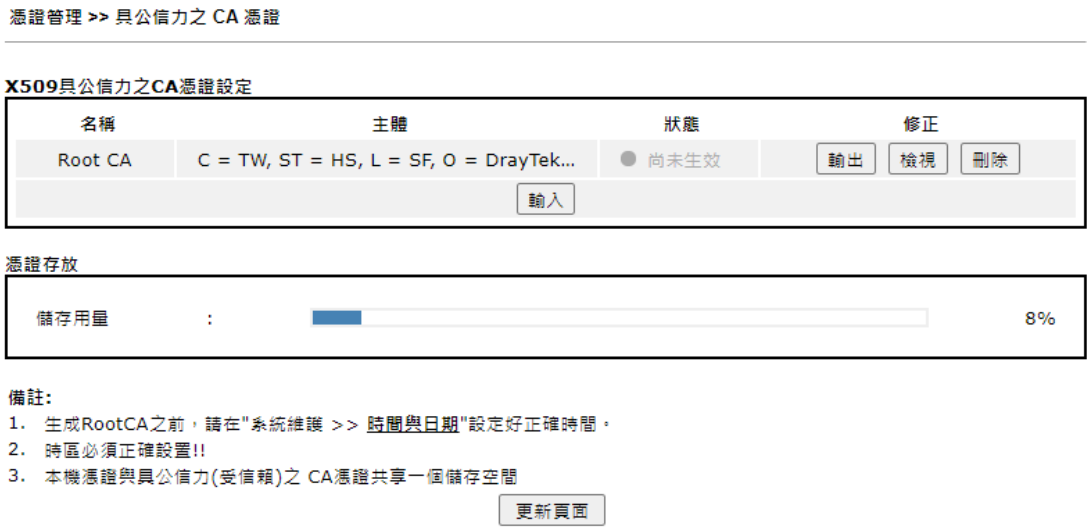
當本機用戶與遠端用戶都需要進行憑證驗證(例如 IPsec X.509)以便讓資料通過 SSL 通道並且防止來自 MITM 攻擊時，可使用具公信力之憑證(Root CA)可用來驗證雙邊提供的數位憑證。

然而，套用來自具公信力數位憑證的數位憑證是相當複雜且花時間，因此路由器提供一種機制讓您可以產生根 CA 節省時間並提供一般使用者更多的便利性。之後此根 CA 可以進行本機憑證之發行事宜。

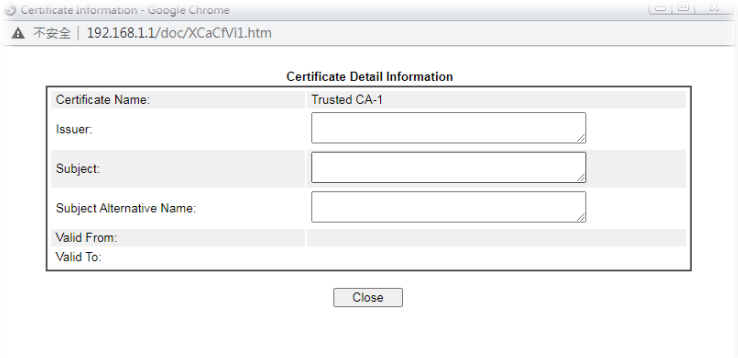
資訊 根 CA(Root CA)可以刪除但無法編輯改寫，如果您想要修改根 CA 設定，請刪除該憑證，重新再建立一個。

尚無 CA 憑證的頁面：

已有 Root CA 憑證的頁面：



可用設定說明如下：

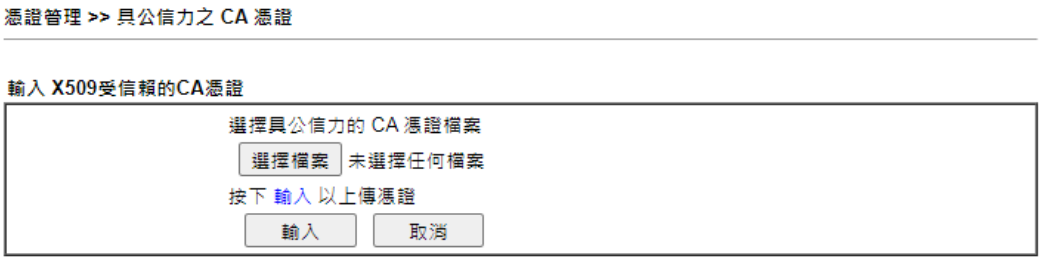
項目	說明
建立 Root CA	按此建立新的 root CA。
名稱	顯示憑證的名稱。
主體	顯示憑證的主體內容。
狀態	顯示憑證目前的狀態。
修正	當無任何 root CA 憑證時 ● **建立 Root CA -** 按此填入與憑證相關之細節內容，啟動產生憑證的程序。 當已有任何 root CA 憑證時 ● **輸出 -** 按此可以輸出憑證並儲存成檔案。 ● **檢視 -** 按此檢視憑證的細節內容。  ● **刪除 -** 按此可以刪除憑證。
輸入	按下此鈕輸入任何一個既有的憑證。
更新頁面	按此更新本頁，顯示最新的憑證資訊。

建立 Root CA

按下**建立**開啟如下頁面。輸入頁面要求的所有資訊，例如憑證名稱(用於辨識不同的憑證用)、主體替代名稱類型與其他相關的設定，接著再按下**產生**。

輸入具公信力的 CA 憑證

若要輸入事先儲存的具公信力之 CA 憑證，請按**輸入**鈕開啟如下的視窗，並使用**選擇檔案**找到儲存的文字檔案，接著按下**輸入**鈕，您所要匯入的檔案將會列在視窗上。



如要檢視每個具公信力之 CA 憑證，請按**檢視**按鈕開啟憑證的詳細資訊視窗，如果您想要刪除 CA 憑證，選擇該憑證並按下**刪除**按鈕，所有相關的憑證資訊即可刪除。

IV-2-3 憑證備份

路由器的本機憑證與具公信力之 CA 憑證可以儲存為一個檔案，請按下述畫面的備份按鈕來儲存，如果您想要設定加密的密碼，請在**加密密碼**與**確認密碼**二欄中輸入所需的字元。

同時，您也可以隨時使用**還原**功能取回設定內容。

憑證管理 >> 憑證備份

憑證備份/還原

備份

加密密碼: 最多23個字元

確認密碼:

按下 備份 以下載憑證檔案至本機電腦上

還原

選擇備份檔案以還原

選擇檔案 未選擇任何檔案

解密密碼:

按下 還原 以上傳檔案

IV-2-4 自行簽核憑證

自行簽核憑證是裝置設備(例如 Vigor 路由器)自身的獨特標識，裝置會自己產生憑證以確保路由器的安全性。這種自行簽核憑主要是使用自己的虛擬金鑰來簽署的。

自行簽核憑可套用於 SSL VPN、HTTPS 等等。此外，它可以透過各種工具免費建立。

憑證管理 >> 自行簽核憑證

自行簽核憑證資訊

憑證名稱：	self-signed
發行人：	C=TW, ST=HsinChu, L=HuKou, O=DrayTek Corp., OU=DrayTek Support, CN=Vigor Router
主體：	C=TW, ST=HsinChu, L=HuKou, O=DrayTek Corp., OU=DrayTek Support, CN=Vigor Router
主體替代名稱：	DNS:www.draytek.com
效期自：	Aug 11 15:25:24 2021 GMT
有效至：	Sep 10 15:25:24 2022 GMT
PEM 格式內容：	-----BEGIN CERTIFICATE----- MIIDpjCCAo6gAwIBAgIJAJnOuRT3dPm8MA0GCSqGSIb3DQEBCwUAMHgxCzAJBgNV BAYTAlRXMRAwDgYDVQQIDAdIc2luQ2h1MQ4wDAYDVQQHDAVIdUtvdTEWMBQGA1UE CgwNRHJheVRlayBDb3JwLjEYMBYGA1UECwwPRHJheVRlayBTdXBwb3J0MRUwEwYD VQQDDAxWaWdvciBSb3V0ZXIwHhcNMjEwODExMTUyNTI0WhcNMjIwOTEwMTUyNTI0 WjB4MQswCQYDVQQGEwJUVzEQMA4GA1UECAwHSHNpbkNodTEOMAwGA1UEBwwFSHVL b3UxFjAUBgNVBAoMDURyYXlUZWsgQ29ycC4xGDAWBgNVBAsMD0RyYXlUZWsgU3Vw cG9ydDEVMBMGA1UEAwwMVmlnb3IgUm91dGVyMIIBIjANBgkqhkiG9w0BAQEFAAOC AQ8AMIIBCgKCAQEAzRPQIBezQp4PdiUpQ8ZDJiF3tTiJmfLRTVOcmZWYWr6KDX1C CD5Qv0zko56k7bGYjp2Vk/caj4TO5DDh2galmQHEA5/v3iHB6mDCY9nF0LnTsnW6 0fOj6F//HY5zRyAHjBVkjJLGmjr7YEL1PXF6sF4PaB3Ax1dDQQwMH8WQY98DdTSN cVCngKFkJF/Tm/wF0OoR1YZuknujhJ1RfP8MIWqOQg5xBSGMAnOLXEj3APJVcLnJ v+v444WLIMQVx1LzpVKfW+S5arQbQ6qQDcEuguL5VP3FB1J0IwVXZw4Y+eA7HtHL qRkXKPbPuAigaW1aLfaZ4EeF1/26N6tr2+/OUQIDAQABozMwMTATBgNVHSUEDDAK BggrBgEFBQcDATAaBgNVHREEEzARgg93d3cuZHJheXRlay5jb20wDQYJKoZIhvcN AQELBQADggEBAEm0YlSEJd7pf+O1iUxqwt64CgV3WEnlslNIBuCvjzjFBWbdwJ+B RkkebsGbyrk+HTVgGgDC8i3CHKYpA85X0MLPOxFtwhJ50YC84EIss63yzV8P5FKk c+ZJqtJD0dJ4AnbFPCumJH0r1iIvQ4myhS1ATS1IW8VoeFirqYovUR347hAeDNL1 gnzWWw2VPdo/epKASaIrRCqzCZYFWsqbf6ucr0jWHbj73xA88NxxOeywowI0TxGB RqQlX8J5XGT+abCKE7GUUmeyKu23zge8Xe8872BpY80n+Fu8sFJp2fRP5tz/1iot sec6daBUUScM5P4VMiVeDU7EY0Uaqe+Ad9M= -----END CERTIFICATE-----

備註:

1. 在嘗試重新生成自行簽核憑證之前，請在系統維護 >> 時間和日期設定好正確時間！！
2. 時區必須正確設置!!

重新產生

按下**重新產生**以打開重新產生自行簽核憑證的窗口。輸入所有請求的訊息包括憑證名稱(用於區分不同的憑證)、主體替代名稱類型和主題名稱的相關設定，然後按下**產生**。

IV-2-5 本機服務清單

本頁顯示本機服務所使用的各種憑證，使用者可以按連結建立新憑證。

憑證管理 >> 本機服務清單

預設憑證 自行簽核

憑證名稱	本機服務
預設憑證	路由器管理 -- 透過LAN或WAN端對網站進行存取
	路由器管理 -- SSH
	VPN 與遠端存取 >> LAN to LAN -- SSL VPN
	VPN 與遠端存取 >> 遠端撥入使用者 -- SSL VPN
	VPN 與遠端存取 >> LAN to LAN -- OpenVPN
	VPN 與遠端存取 >> 遠端撥入使用者 -- OpenVPN
	客製化入口網站設定
	數位內容安全管理(CSM) >> DNS 過濾器 -- 空白頁面
	USB 應用 >> USB 使用者管理
無	VPN 與遠端存取 >> IPsec基本設定

確定

第五篇 安全性設定

Firewall

當使用者需要更多的頻寬以便用於多媒體、交互運用或是遠距學習時，最關心的莫過於網路安全性議題。路由器的防火牆功能可保護您的區域網路，免受未經授權之外來者的攻擊，同時也可限制區域網路中的使用者登入網際網路。

CSM

CSM是中央安全性管理的簡稱，用來控制IM/P2P運用，過濾網頁內容以及URL內容，已達成安全性管理的目標。

V-1 防火牆

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

防火牆工具

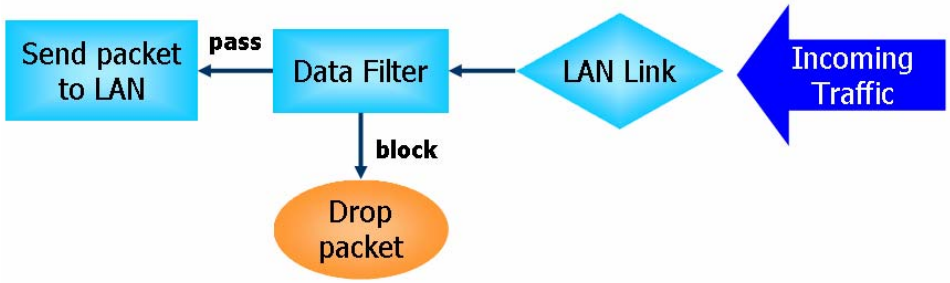
區域網路上的使用者可以下述的防火牆工具，接受良好的安全防護：

- 用戶設定 IP 過濾器(呼叫過濾器/資料過濾器)
- Stateful Packet Inspection (SPI): 追蹤封包並阻擋未經要求而流入的資料
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS)攻擊防禦

資料過濾器

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

以下圖表解釋流入(傳入)與流出(對外)之資料傳輸程式。



封包狀態檢測(SPI)

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

DoS 攻擊防禦 (DoS Defense)

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

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

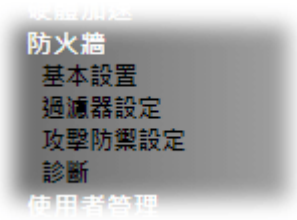
Vigor 路由器也可以監視資料流量，任何違反事先定義的參數的不正常資料流(例如臨界值的數字)，都會被視為是一種攻擊行為，Vigor 路由器將啟動防衛機制，及時阻擋減輕災害。

下列表格顯示出 DoS 攻擊防禦功能所能檢測出的攻擊類型。

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

網頁使用者介面

下圖為防火牆的功能項目：



V-1-1 基本設定

基本設置允許您調整 IP 過濾器和一般選項的設定內容，在此頁面您可以啟動或是關閉**資料過濾器**。

基本設定頁面

此頁面可讓您啟用/停用資料過濾器，決定過濾進出資料的一般規則。

可用設定說明如下：

項目	說明
資料過濾器	選擇**啟用**以啟動資料過濾器功能，並指定開始過濾器組別。

允許分段的大型封包流量輸入(因應某些遊戲或是媒體流量之需要)	一些線上遊戲都會使用很多的片段 UDP 封包來傳送遊戲資料，出於安全防火牆的本能直覺，Vigor 路由器會將這些片段封包給退回，以避免攻擊發生，除非您啟動**允許分段的大型封包流量輸入**功能。勾選此方塊後，您就可以在這些線上遊戲上悠遊。如果安全利害關係具有較高的重要性，您就不要啟動此功能。
啟用嚴格安全防火牆策略	為了安全起見，路由器將會執行嚴格的資料傳輸安全性檢驗動作。 此功能在預設狀態下是啟用的，所有透過路由器傳送的封包都會經過防火牆過濾一番。如果防火牆系統（例如內容過濾伺服器）並未有任何回應(通過或是封鎖)，那麼路由器防火牆會直接封鎖所有的封包。
阻擋從 WAN 端主動發起的路由連線	通常，由 WAN 至 LAN 的 IPv6 網路連線數/流量是允許。 **IPv6** - 勾選此方塊讓路由器得以封鎖透過 IPv6 傳送過來的封包(自 WAN 到 LAN)，這個功能對於封鎖路由封包有效用，但是對於 NAT 過來的封包就沒有作用。 **IPv4** - 勾選此方塊讓路由器得以封鎖透過 IPv4 傳送過來的封包(自 WAN 到 LAN)，這個功能對於封鎖路由封包有效用，但是對於 NAT 過來的封包就沒有作用。
備份防火牆	按此按鈕儲存防火牆設定。
還原防火牆	按下**選擇**按鈕挑選防火牆設定檔案，接著按下**還原**按鈕套用此檔案。

如預儲存頁面設定，請按下**確定**。若要捨器變更，請按**取消**。

防火牆過濾流量依照如下的順序進行：

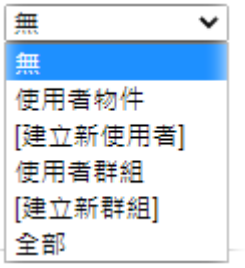
1. 資料過濾器組別與規則
2. 阻擋從 WAN 端主動發起的路由連線
3. 預設規則

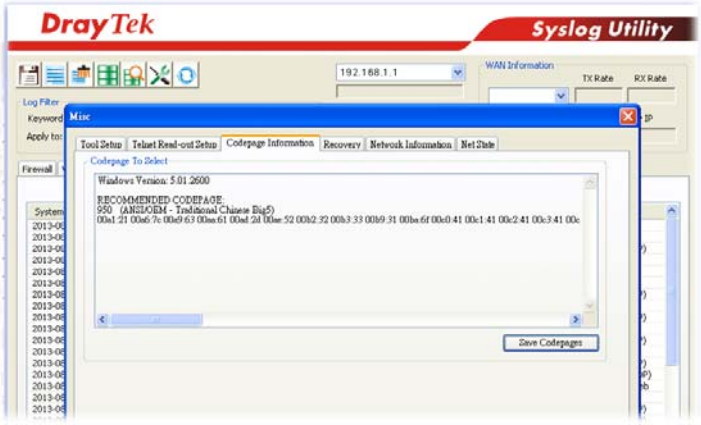
預設規則頁面

本頁讓您選擇過濾設定檔包含 QoS、負載平衡策略、WCF、應用程式管控、URL 內容過濾、網頁內容過濾、DNS 過濾等等以便透過路由器進行資料傳輸。

可用設定說明如下：

項目	說明
過濾器	**通過-** 所有的封包都可通過路由器，不需考慮**防火牆>>過濾器**的設定內容。 **阻擋** - 所有的封包都不許通過路由器，且不需考慮**防火牆>>過濾器**的設定內容。
連線數控制	此處輸入的值為全部的封包連線數，預設值為 50000。
服務品質	選擇一組 QoS 規則作為防火牆規則，設定 QoS 細節資訊部分，請參考稍後的相關章節。
使用者管理	本項目僅在**使用者管理>>基本設置**中選擇**基於規則**時可用，一

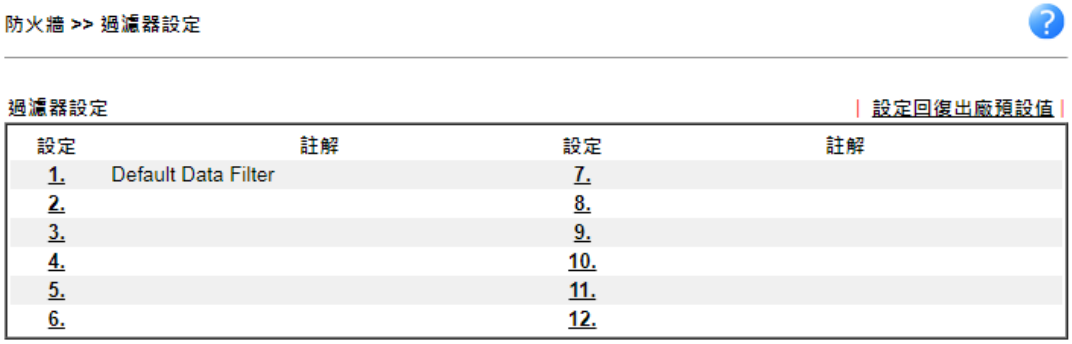
	般防火牆規則將套用在使用者/使用者群組/全部使用者上。  **注意:** 當沒有任何使用者設定檔或是使用者群組可供選擇時，系統會出現**建立新使用者**或是**建立新群組**選項供您建立新的設定檔。
APP 應用程式管控	選擇應用程式管控設定檔來封鎖 IM/P2P 之類的應用，如果沒有任何設定檔可供選擇時，請從下拉式清單中選擇**建立新檔**來建立一個新的設定檔。所有區域網路中的主機必須依循應用程式管控設定檔內的標準。有關詳細資訊，請參考**數位內容安全管理>>應用程式管控設定檔**章節。 因應疑難排解的需要，您可勾選 IM/P2P 紀錄方塊以便將資訊記錄起來，這些紀錄會傳送到 Syslog 伺服器，詳情請參考 **Syslog/郵件警告**章節。
URL 內容過濾器	選擇一個 **URL 內容過濾器**設定檔**(**在**數位內容安全管理(CSM)>> URL 內容過濾器**中所建立)，請務必先在**數位內容安全管理(CSM)> URL 內容過濾器**中設定一個設定檔，或是從下拉式選單中選擇[建立新檔]產生新的設定檔。因應疑難排解的需要，您可勾選紀錄方塊以便將資訊記錄起來，這些紀錄會傳送到 Syslog 伺服器，詳情請參考 **Syslog/郵件警告(Syslog/Mail Alert)**章節。
網頁內容過濾器	選擇一個**網頁內容過濾器**設定檔（在**數位內容安全管理(CSM)>> 網頁內容過濾器**中所建立)，請務必先在**數位內容安全管理(CSM)>> 網頁內容過濾器**中設定一個設定檔，或是從下拉式選單中選擇[建立新檔]產生新的設定檔。因應疑難排解的需要，您可勾選紀錄方塊以便將資訊記錄起來，這些紀錄會傳送到 Syslog 伺服器，詳情請參考 **Syslog/郵件警告(Syslog/Mail Alert)**章節
DNS 過濾器	選擇一組 DNS 過濾器設定檔(於**數位內容安全管理>>DNS 過濾器**頁面中建立)，在**數位內容安全管理>>網頁內容過濾器設定檔**頁面中至少要先建立一個設定檔案以供選擇，或是從下拉式清單中選擇 DNS 過濾器連結以重新建立新的設定檔。
進階設定	按**編輯**按鈕開啟下述視窗，不過，在此強烈建議您使用預設值為佳。 **編碼語系-** 此功能用來比較不同語言之間的字元數，選擇正確的 codepage 可以幫助系統從 URL 解碼資料後能取得正確的

	ASCII 碼，並強化 URL 內容過濾器的正確性。預設值為 ANSI 1252 Latin，如果您未選擇任何的 codepage，URL 解碼動作也不會執行，請自下拉式清單中選擇一個 codepage。 如果您不知道要如何選擇適宜的**編碼語系**，請開啟 Syslog。從 Setup 對話盒中的**編碼語系**(codepage)資訊，您將會看到系統建議的 codepage 內容。  **視窗大小** – 決定 TCP 協定的大小(0~65535)，數值越大，成效越佳，不過網路會較為不穩定，小的數值比較適合穩定網路。 **連線數逾時** – 設定連線數逾時時間可讓網路資源獲得較佳的運用，但是連續暫停僅適用於 TCP 協定，連線數逾時主要是針對符合防火強規則的資料流量而設定。
備份防火牆	按**備份**儲存防火牆頁面設定。
還原防火牆	按**選擇檔案**挑選一個防火牆設定檔案。按**還原**套用選擇的檔案。

完成設定之後，按下**確定**按鈕儲存相關設定。

V-1-2 過濾器設定

按**防火牆**並選擇**過濾器設定**以開啟如下的設定網頁。



如果要新增一個過濾器，請按組別下方的數字按鈕以便編輯個別設定。如下的頁面將立即出現，每一個過濾器都含有 7 組規則，請按規則按鈕編輯每個規則，勾選**啟用**則可啟動該項規則。

可用設定說明如下：

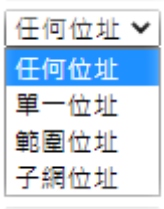
項目	說明
規則	請按號碼按鈕(1 ~ 7)編輯過濾器的規則，按下此鈕可以開啟過濾器規則網頁，有關詳細的資訊，請參考稍後的說明。
啟用	啟動或是關閉此項過濾規則。
註解	輸入過濾規則註解說明，最大長度可以達到 23 個字元。
方向	顯示封包的方向。
來源 IP/目的 IP	顯示來源/目的 IP 位址。
服務類型	顯示封包的類型與埠號。

動作	顯示處理的封包是通過還是封鎖。
數位內容安全管理(CSM)	顯示 CSM 是否啟用。
移動上/下	使用**上/下**連結來移動過濾器規則的順序。
下一個過濾器組別	設定前往下一個執行的過濾器連結，請勿讓多個過濾器設定形成一個迴路。
設定精靈模式	允許利用數個設定頁面，配置經常使用的過濾器規則設定。
進階模式	允許設定過濾器規則細節內容。

欲使用**設定精靈模式**，請依下述步驟進行：

1. 按下**設定精靈模式**。
2. 按下索引編號 1，設定頁面出現如下：

可用設定說明如下：

項目	說明
註解	輸入過濾器設定註解說明，最大長度為 14 個字元。
方向	設定封包流向的方向，此項設定僅適用**資料過濾器**。 **注意:** RT 表示第二個子網的路由網域或是其他 LAN。
來源/目的 IP	手動設定 IP 位址時，請選擇**任何位址/單一位址/範圍位址/子網位址**作為位址類型，並在其後的方框中輸入相應內容。 
通訊協定	指定此過濾器規則將套用的通訊協定。

來源埠號/目的埠號	*(=)* – 當起始埠號與結束埠號與的數值相同時，此符號表示一個通訊埠。當起始埠號與結束埠號的數值不同時，即表示設定檔所適用的通訊埠範圍。 *(!=)* –當起始埠號與結束的數值相同時，此符號表示除了這裡所指明的通訊埠以外，全都適用於此設定檔。當起始埠號與結束埠號數值不同時，即除了此處所設定的範圍以外，所有的通訊埠都適用於此設定檔。 *(>)* – 大於此數值的通訊埠號皆可使用。 *(<)* – 小於此數值的通訊埠號皆可使用。

3. 按**下一頁** 進入如下頁面：

可用設定說明如下：

項目	說明
立刻通過	符合規則之封包可立即通過。 **APP 應用程式管控 -** 選擇應用程式管控設定檔來封鎖 IM/P2P 之類的應用，如果沒有任何設定檔可供選擇時，請從下拉式清單中選擇**建立新設定[Create New]**來建立一個新的設定檔。所有區域網路中的主機必須依循應用程式管控設定檔內的標準。有關詳細資訊，請參考**數位內容安全管理>>應用程式管控設定檔**章節。 因應疑難排解的需要，您可勾選 IM/P2P 紀錄方塊以便將資訊記錄起來，這些紀錄會傳送到 Syslog 伺服器，詳情請參考 Syslog/郵件警告章節。 **URL 內容過濾器 -** 選擇一個 **URL 內容過濾器**設定檔(在**數位內容安全管理(CSM)>> URL 內容過濾器**中所建立)，請務必先在**數位內容安全管理(CSM)> URL 內容過濾器**中設定一個設定檔，或是從下拉式選單中選擇**[建立新檔]**產生新的設定檔。因應疑難排解的需要，您可勾選紀錄方塊以便將資訊記錄起來，這些紀錄會傳送到 Syslog 伺服器，詳情請參考 Syslog/郵件警告章節。 **網頁內容過濾器 -** 選擇一個**網頁內容過濾器**設定檔(在**數位內容安全管理(CSM)>> 網頁內容過濾器**中所建立)，請務必先在**數位內容安全管理(CSM)>> 網頁內容過濾器**中設定一個設定檔，或是從下拉式選單中選擇**[建立新檔]**產生新的設定檔。因應疑難排解的需要，您可勾選紀錄方塊以便將資訊記錄起來，這些紀錄會傳送到 Syslog 伺服器，詳情請參考 Syslog/郵件警告章節

	DNS 過濾器 - 選擇一組 DNS 過濾器設定檔(於**數位內容安全管理>>DNS 過濾器**頁面中建立)，在**數位內容安全管理>>網頁內容過濾器設定檔**頁面中至少要先建立一個設定檔案以供選擇，或是從下拉式清單中選擇 DNS 過濾器連結以重新建立新的設定檔。
立刻阻擋	系統封鎖符合規則之封包。

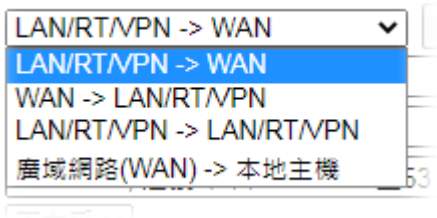
4. 指定相關項目之後，按**下一頁** 進入總結頁面。

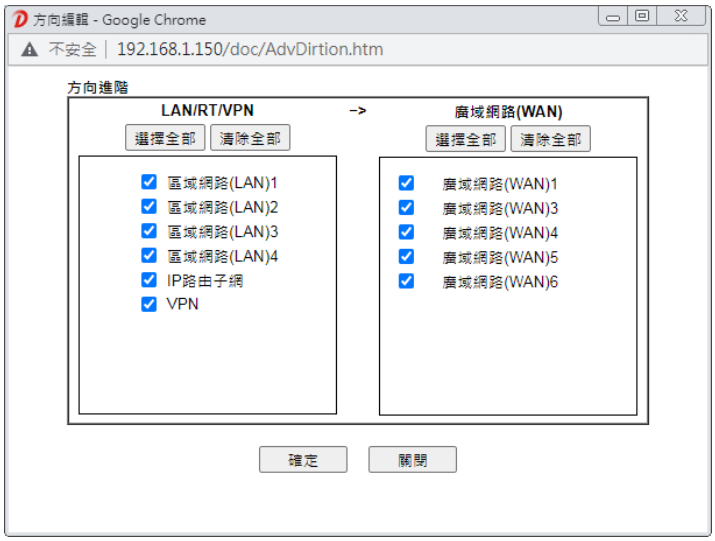
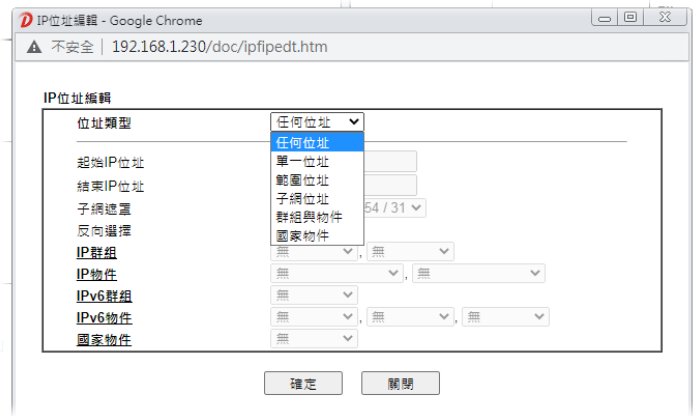
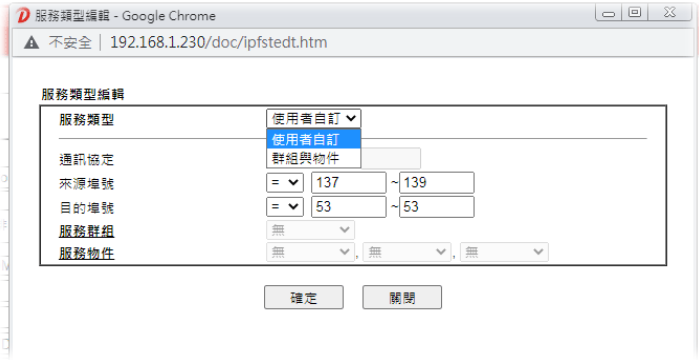
5. 若顯示頁面內容無誤，請按**完成**結束精靈設定。

欲使用**進階模式**，請依下述步驟進行：

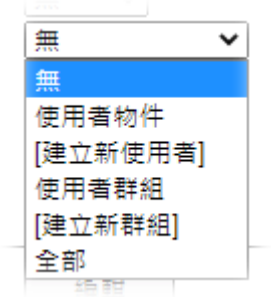
1. 按下**進階模式**。
2. 按下索引編號 **1**，設定頁面出現如下：

可用設定說明如下：

項目	說明
啟用	勾選此項目以啟動過濾規則。
註解	輸入過濾器設定註解說明，最大長度為 14 個字元。
排程設定檔	設定區域網路上的電腦工作的時間間隔，您可以輸入四組時間排程，所有的排程都可在**其他應用>>排程**網頁上事先設定完畢，然後在此輸入該排程的對應索引號碼即可。
當排程啟用時，清除連線數	勾選此方框可依據上述排程設定期間清除連線數資料。
方向	設定封包流向的方向，此項設定僅適用**資料過濾器**，對於呼叫過濾器而言，這項設定是不適用的。  **注意:** RT 表示第二個子網的路由網域或是其他 LAN。

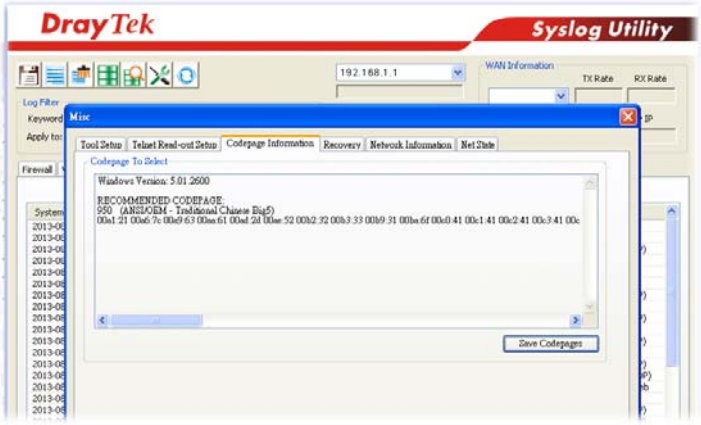
	進階 - 選擇方向之後，按此鈕指定封包流量之通過介面。 
來源 IP /國別 以及 **目的 IP/國別**	按下**編輯**進入如下的畫面，選擇來源/國家/目的 IP 或是 IP 範圍。  欲手動設定 IP 位址，請選擇**任何位址/單一位址/範圍位址/子網位址**作為位址類型，並在此對話方塊輸入相關內容。此外，如果您想要在定義的群組或物件上使用 IP 範圍，請勾選**群組與物件**或是**國家物件**。 從 **IP 群組**下拉式清單中，選擇您需要應用的群組，或是使用 **IP 物件**下拉式清單，選擇您所需要的物件。
服務類型	按**編輯**進入如下的畫面，以選擇適合之服務類型。  欲手動設定服務類型，請選擇使用者自訂做為服務類型，並輸入相關的設定資料，此外如果您想要使用群組或是物件中所定義的服務類型，請選擇**群組與物件(Group and Objects)**作為

	服務類型。 **通訊協定 -** 指定本過濾器規則套用的協定。 **來源/目的埠號 -** *(=)* – 當起始埠號與結束埠號與的數值相同時，此符號表示一個通訊埠。當起始埠號與結束埠號的數值不同時，即表示設定檔所適用的通訊埠範圍。 *(!=)* –當起始埠號與結束的數值相同時，此符號表示除了這裡所指明的通訊埠以外，全都適用於此設定檔。當起始埠號與結束埠號數值不同時，即除了此處所設定的範圍以外，所有的通訊埠都適用於此設定檔。 *(>)* – 大於此數值的通訊埠號皆可使用。 *(<)* – 小於此數值的通訊埠號皆可使用。 **服務群組/物件-** 使用下拉式選項選擇所需的項目。
片段	指定片段封包的執行動作，這個項目也是僅針對**資料過濾器**。 **忽略-** 不論是怎樣的片端封包，系統皆不採取行動。 **無片段-** 應用規則至無片段之封包上。 **片段-** 應用規則至片段之封包上。 **太短-** 只有過短無法包含完整封包頭之封包，可應用此規則。
過濾器	指定系統針對符合規則之封包所採取的行動。 **立刻通過 -** 符合規則之封包可立即通過。 **立刻阻擋 -** 系統封鎖符合規則之封包。 **若無符合其餘規則即通過 -** 符合限定規則且並未符合其他規則之封包可立即通過。 **若無符合其餘規則即阻擋-** 系統封鎖符合限定規則且並未符合其他規則之封包。 基於疑難排除的需要，您可指定記錄過濾器資訊，只要勾選 **Syslog** 方框即可。
連接至其他過濾器組別	封包符合過濾器規則，下一個過濾器規則將分至指定之過濾器設定。請自下拉式選項中選擇下一個過濾器規則以便做分支動作，要注意路由器將會採用指定之過濾器規則，且絕對不會回到先前所設定之過濾器規則。
連線數控制	此處輸入的值為全部的封包連線數，預設值為 50000。
MAC 綁定 IP	**嚴格的** – 讓 IP 物件中設定來源 IP 與目標 IP 中的 MAC 位址與 IP 位址設定完全綁定，並用於此過濾器規則。 **不嚴格的 -** 此指完全沒有限制。
服務品質	選擇一組 QoS 規則作為防火牆規則，設定 QoS 細節資訊部分，請參考稍後的相關章節。
使用者管理	本項目僅在**使用者管理>>基本設置**中選擇**基於規則**時可用，一般防火牆規則將套用在使用者/使用者群組/全部使用者上。

	 **注意:** 當沒有任何使用者設定檔或是使用者群組可供選擇時，系統會出現**建立新使用者**或是**建立新群組**選項供您建立新的設定檔。
APP 應用程式管控	選擇應用程式管控設定檔來封鎖 IM/P2P 之類的應用，如果沒有任何設定檔可供選擇時，請從下拉式清單中選擇**建立新設定**來建立一個新的設定檔。所有區域網路中的主機必須依循應用程式管控設定檔內的標準。有關詳細資訊，請參考**數位內容安全管理>>應用程式管控設定檔**章節。 因應疑難排解的需要，您可勾選 IM/P2P 紀錄方塊以便將資訊記錄起來，這些紀錄會傳送到 Syslog 伺服器，詳情請參考 Syslog/郵件警告章節。
URL 內容過濾器	選擇一個 **URL 內容過濾器**設定檔（在**數位內容安全管理(CSM)>> URL 內容過濾器**中所建立），請務必先在**數位內容安全管理(CSM)> URL 內容過濾器**中設定一個設定檔，或是從下拉式選單中選擇[建立新檔](**[Create New]**)產生新的設定檔。 因應疑難排解的需要，您可勾選紀錄方塊以便將資訊記錄起來，這些紀錄會傳送到 Syslog 伺服器，詳情請參考 Syslog/郵件警告章節。
網頁內容過濾器	選擇一個**網頁內容過濾器**設定檔(在**數位內容安全管理(CSM)>> 網頁內容過濾器**中所建立)，請務必先在**數位內容安全管理(CSM)>> 網頁內容過濾器**中設定一個設定檔，或是從下拉式選單中選擇[建立新檔]產生新的設定檔。 因應疑難排解的需要，您可勾選紀錄方塊以便將資訊記錄起來，這些紀錄會傳送到 Syslog 伺服器，詳情請參考 Syslog/郵件警告章節。
DNS 過濾器	選擇一組 DNS 過濾器設定檔(於**數位內容安全管理>>DNS 過濾器**頁面中建立)，在**數位內容安全管理>>網頁內容過濾器設定檔**頁面中至少要先建立一個設定檔案以供選擇，或是從下拉式清單中選擇 DNS 過濾器連結以重新建立新的設定檔。
進階設定	按**編輯**按鈕開啟下述視窗，不過，在此強烈建議您使用預設值為佳。

編碼語系 - 此功能用來比較不同語言之間的字元數，選擇正確的codepage可以幫助系統從URL解碼資料後能取得正確的ASCII 碼，並強化 URL 內容過濾器的正確性。預設值為 ANSI 1252 Latin，如果您未選擇任何的 codepage，URL 解碼動作也不會執行，請自下拉式清單中選擇一個 codepage。

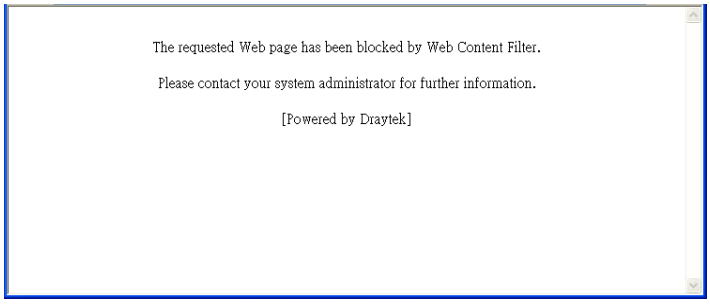
如果您不知道要如何選擇適宜的**編碼語系**，請開啟 Syslog。從 Setup 對話盒中的**編碼語系**資訊，您將會看到系統建議的 codepage 內容。



視窗大小 – 決定 TCP 協定的大小(0~65535)，數值越大，成效越佳，不過網路會較為不穩定，小的數值比較適合穩定網路。

連線數逾時 – 設定連線數逾時時間可讓網路資源獲得較佳的運用，但是連續暫停僅適用於 TCP 協定，連線數逾時主要是針對符合防火強規則的資料流量而設定。

DrayTek 橫幅 – 請勿勾選此方框，下述畫面就不會出現在無法取用的網頁上，預設值是勾選的。



嚴格安全性檢測- 為安全起見，您可能會想讓路由器針對資料傳輸進行較為嚴格的安全性檢測，不過您若進行此項檢測有可能對路由器的成效造成一定的影響。

3. 當您完成上述設定之後，請按**確定**按鈕儲存並離開頁面。

V-1-3 攻擊防禦功能設定

這是 **IP 過濾程式/防火牆**的次功能選項，有 15 種檢測/防禦功能類型，DoS 攻擊防禦功能的預設值是關閉的。

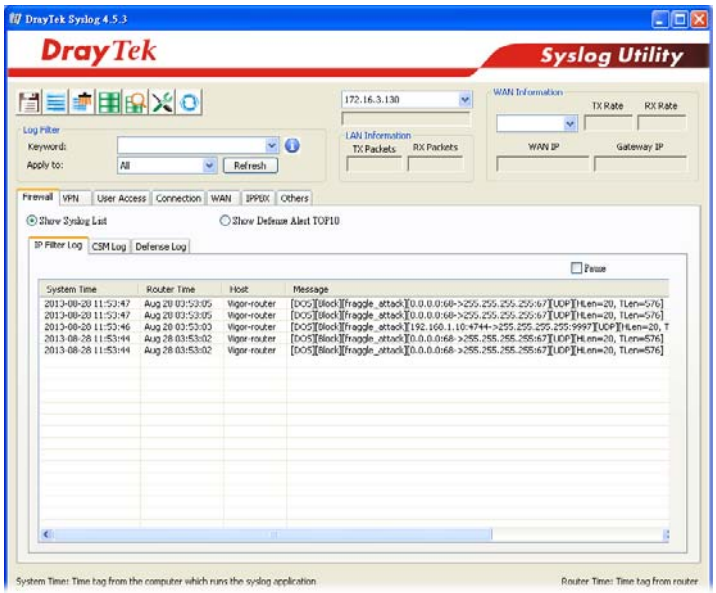
V-1-3-1 防禦 DoS 攻擊

按**防火牆**並選擇**攻擊防禦設定**開啟設定網頁。

可用設定說明如下：

項目	說明
啟用防禦 DoS 攻擊功能	勾選此項以啟動 DoS 攻擊防禦功能。
選擇全部	按下此鈕選擇下列全部項目。
啟用 SYN flood 攻擊防禦	勾選此項以啟動 SYN 攻擊防禦功能，一旦檢查到 TCP SYN 封包的臨界值超過定義數值，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。臨界值和逾時的預設值分別為每秒 2000 個封包和 10 秒。
啟用 UDP flood 攻擊防禦功能	勾選此項以啟動 UDP 攻擊防禦功能， 一旦檢查到 UDP 封包臨界值超過定義數值，Vigor 路由器在所設定之逾時期間即開始捨棄其後之 UDP 封包。臨界值和逾時的預設值分別為每秒 2000 個封包和 10 秒。 **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。

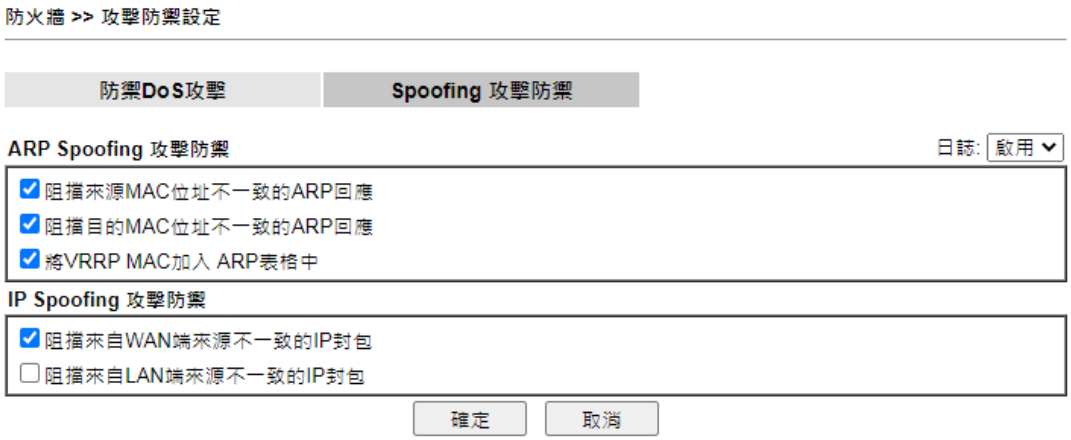
啟用 ICMP flood 攻擊防禦功能	勾選此項以啟動 ICMP Fragment 封包，與 UDP 攻擊防禦功能相同的是，一旦檢查到 ICMP 封包臨界值超過定義數值，路由器便會於所設定之逾時期間，不再回應來自網際網路的 ICMP 需求。臨界值和逾時的預設值分別為每秒 250 個封包和 10 秒。
啟用防禦通訊埠掃瞄偵測功能	通訊埠掃瞄藉由傳送大量封包到數個通訊埠，以嘗試找出未知服務所回應之內容來攻擊 Vigor 路由器。勾選此方塊啟動通訊埠掃瞄檢測功能，當利用通訊埠掃瞄臨界值速率而檢測出惡意探測之行為時，Vigor 路由器將傳送警告訊息出去。臨界值的預設值為每秒 2000 個封包。
阻擋 IP 選項	勾選此項以啟動阻攔 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，因為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。
阻擋 Land 攻擊	勾選此項以強迫 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元址)，以及通訊埠號至受害一方時，Land 攻擊即由此發生。
阻擋 Smurf 攻擊	勾選此項以啟動封鎖 Smurf 攻擊功能，Vigor 路由器將忽略任何一次的播送 ICMP 回應需求。
阻擋路由追蹤	勾選此項以強迫 Vigor 路由器不轉送任何路由封包的行蹤。
阻擋 SYN Fragment 封包	勾選此項以啟動封鎖 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。
阻擋 Fraggle 攻擊	勾選此項以啟動封鎖 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。 啟動 DoS/DDoS 防禦功能可能會阻擋一些合法的封包，例如當您啟動 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。
阻擋 TCP Flags 掃描	勾選此項以啟動阻攔 TCP Flags 掃描功能，任何具有異常 TCP 封包的設定都會被捨棄掉，這些掃描行動包含有 *no flag scan*, *FIN without ACK scan*, *SYN FINscan*, *Xmas scan* 以及 *full Xmas scan* 等等。
阻擋 Tear Drop 攻擊	勾選此項以啟動封鎖 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。為了避免這類型的攻擊行為，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。
阻擋 Ping of Death 攻擊	勾選此項以啟動封鎖 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。
阻擋 ICMP 封包片段攻擊	勾選此項以啟動封鎖 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。
阻擋不明封包	勾選此項以啟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。
警告訊息	我們提供使用者系統記錄功能以便檢視路由器發出的訊息。作為系統紀錄伺服器，使用者可接收來自路由器(系統紀錄用戶端)傳送之報告。 所有與 DoS 攻擊有關的警告訊息都將傳送與使用者，使用者可以重新檢查其內容，在訊息中尋找關鍵字，所遭受的攻擊之名稱即可立即檢測出來。 

在您完成上述的設定之後，請按**確定**按鈕來儲存設定。

V-1-3-2 Spoofing 攻擊防禦

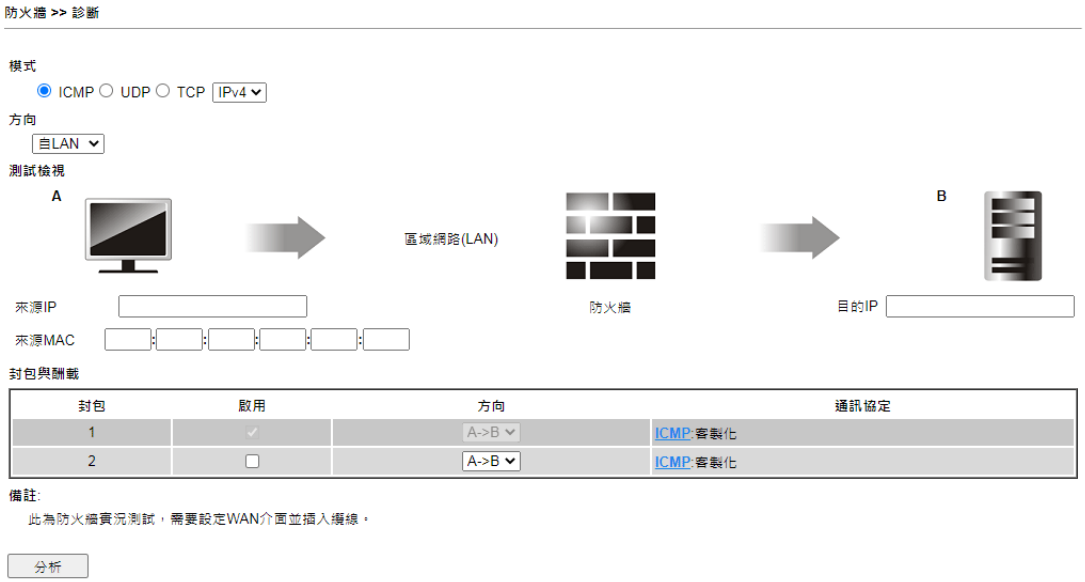
按 **Spoofing 攻擊防禦**標籤開啟如下頁面。



V-1-4 診斷

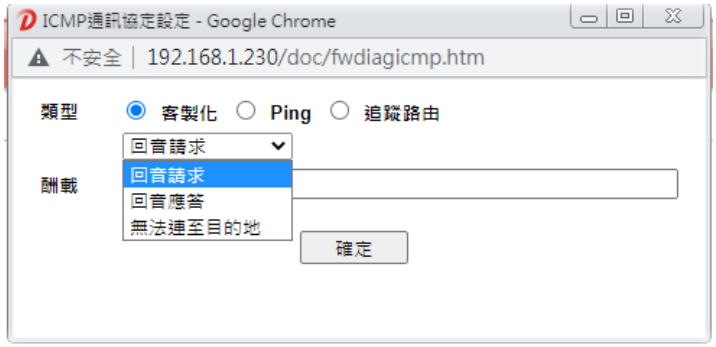
診斷的目的是為了測試當路由器接收封包，套用的是哪條防火牆規則。測試的結果包含防火牆規則設定檔、封包傳輸時的 IP 位址轉換、防火牆功能狀態等等，同時也會顯示在此頁面上。

資訊 使用診斷工具的測試結果可作為研發人員除錯之用，依照實際網路連線設定之不同，結果也會不同。

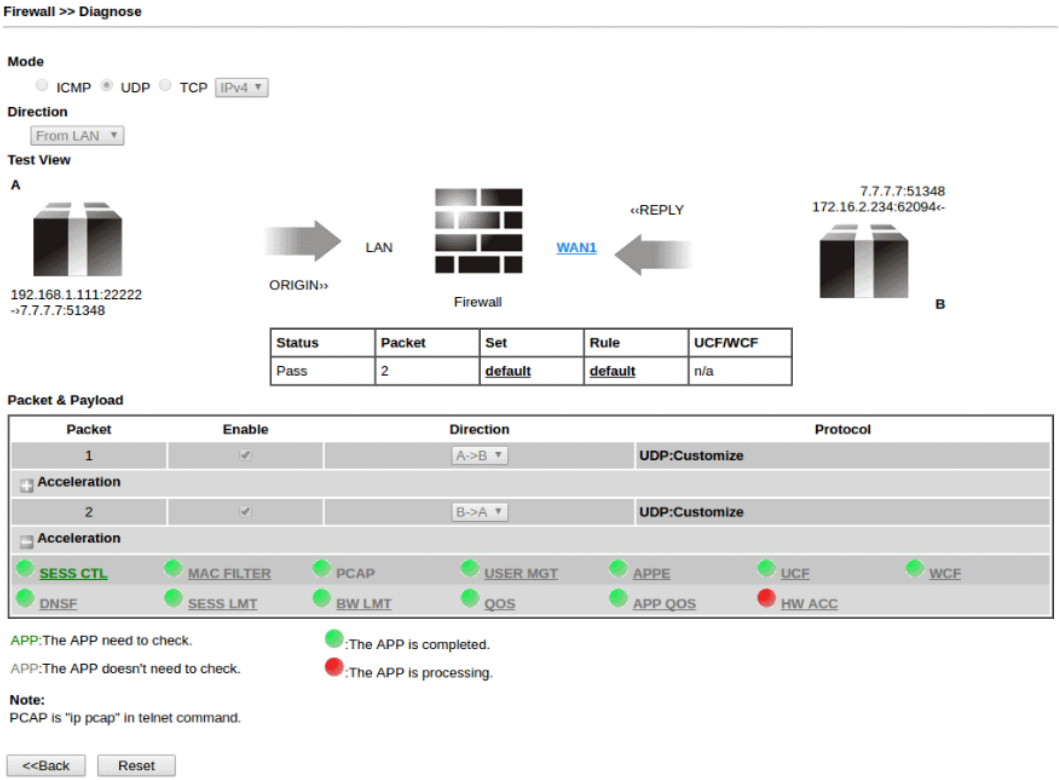


可用設定說明如下：

項目	說明
模式	欲執行防火牆測試，請指定服務類型(如 ICMP、UDP、TCP)然後輸入 IP 位址(IPv4/IPv6)。
方向	設定路由器接收第一個封包的方向來源以進行測試(來自 WAN 或來自 LAN)。
測試檢視	這是動態顯示頁面。 依照指定的方向，測試顯示畫面會呈現圖表引導您輸入 IP 位置、埠號與 MAC 位址。 之後，按下分析按鈕，防火牆規則設定檔的資訊與位址轉換資訊就會呈現在頁面上。
來源 IP	輸入封包來源的 IPv4/IPv6 位址。
來源埠號	輸入封包來源的埠號。
來源 MAC	輸入封包來源的 MAC 位址。
目的 IP	輸入封包目的的 IPv4/IPv6 位址。
目的埠號	輸入封包目的的埠號。
封包與有效承載	在防火牆的診斷中，二個封包屬於一次連線。一般來說，路由器只需要二個封包就可以進行這項測試了。 **啟用**- 勾選此框以傳送測試封包。

	方向- 防火牆測試中第一個封包會依循上述指定的方向送出，然而第二個封包的方向有可能不同。請在此選擇第二個封包的傳送方向(自電腦 A 至 B 或是自電腦 B 至 A)。 **通訊協定-** 顯示選擇的模式與狀態，如要必要，可按模式連結設定進階內容。.  ● **類型** – 可選客製化、Ping 以及追蹤路由。 ● **有效承載-** 選擇客製化為類型時可以設定此項。請輸入代表特定封包(如 DNS 封包)之 16 進位的字元數字 16 個即可。
分析	執行測試並分析結果。

下圖顯示按下**分析**按鈕之後的測試結果，與防火牆有關的功能(如 MAC 過濾器、QoS、使用者管理等等)之狀態也會以綠燈或紅燈呈現在網頁上。



V-2 數位內容安全管理(CSM)

數位內容安全管理(CSM, Content Security Management)主要是用來控制即時通訊、點對點應用、過濾網頁內容以及過濾 URL 內容，以便達成安全管理的效果。

應用程式管控設定檔

由於即時通訊應用程式蓬勃的發展，人與人間的通訊變得越來越容易。然而一些企業利用此種程式作為與客戶通訊的有力工具時，部分公司對此可能還是抱持保留態度，這是因為他們想要減少員工在上班時間誤用此程式或是防止未知的安全漏洞發生。對於準備應用點對點程式的公司來說，情況也是相同的，因為檔案分享可以很方便但是同時也很危險。為了應付這些需求，我們提供了 CSM 阻擋功能。

URL 內容過濾器

爲了提供一個適當的網路空間給予使用者，Vigor 路由器配有 URL 內容過濾器，可限制一些不合法的資料於網站上進出，同時也禁止隱藏惡意碼的網路特徵於路由器內出入。

一旦使用者輸入關鍵字連結，URL 關鍵字阻擋工具將會拒絕該網頁之 HTTP 需求，如此一來使用者即無法存取該網站。您可以這樣想像一下，URL 內容過濾器為一個訓練有素的便利商店櫃員，絕對不販售成人雜誌給予未成年的小孩子。在辦公室內，URL 內容過濾器也可以提供與工作相關的環境，由此來增加員工的工作效率。URL 內容過濾器為什麼可以比傳統防火牆在過濾方面提供更好的服務呢？那是因為它能夠檢查 URL 字串或是一些隱藏在 TCP 封包負載的 HTTP 資料，而一般防火牆僅能以 TCP/IP 封包標頭來檢測封包。

換言之，Vigor 路由器可以防止使用者意外自網頁下載惡意的程式碼。惡意碼隱藏在執行物件當中是一件很普遍的事情，像是 ActiveX、Java Applet、壓縮檔和其他執行檔案。一旦用戶下載這些類型的檔案，用戶便會有這些可能爲系統帶來威脅的風險，例如一個 ActiveX 控制物件通常用於提供網頁人機通信交換功能，萬一裡面隱藏惡意的程式碼的話，該程式碼就可能會佔據使用者的系統。

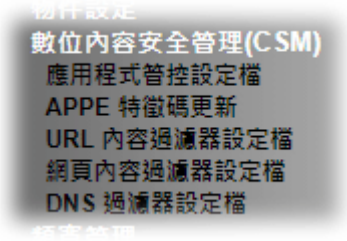
網頁內容過濾器

我們都知道網際網路上的內容，有時候可能並不太合宜，作為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。

一旦您啟動了網頁內容過濾服務，也選擇一些您想要限制存取的網站目錄，每個 URL 位址需求(例 www.bbc.co.uk) 將在由 SurfControl 所運作的伺服器資料庫中先接受檢測。資料庫涵蓋 70 種語言和 200 個國家，超過 1 億個網頁，區分成 40 種容易瞭解的目錄。此資料庫每一天都由網際網路的國際研究團隊不斷更新，伺服器將查閱 URL 然後傳回其類別給路由器，您的 Vigor 路由器即可按照您所選擇的分類項目來決定是否允許用戶存取該網站，因為每一個多路負載平衡資料庫伺服器一次可以管理數百萬的分類需求。

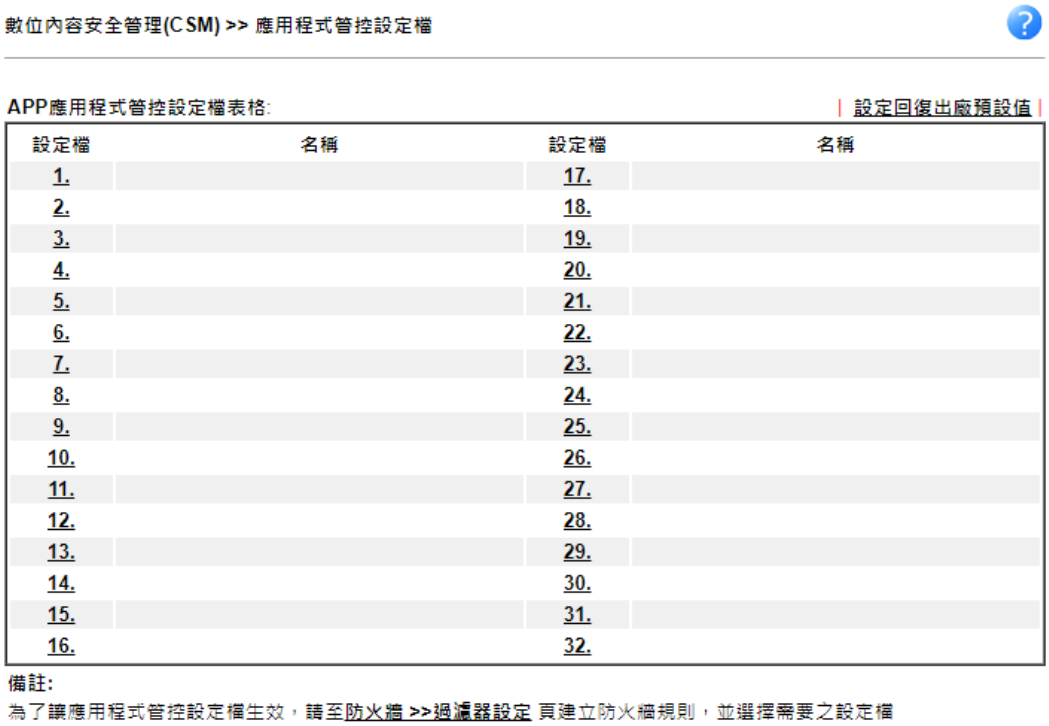
資訊	URL 內容過濾器的優先權高於網頁內容過濾器。

網頁使用者介面



V-2-1 應用程式管控設定檔

您可針對即時通訊/點對點/通訊協定/其他應用定義不同的策略檔案，以通訊及應用之需要，此處所建立的設定檔可以運用在**防火牆>>基本設置**的**預設規則**中，做為主機依循的標準。



可用設定說明如下：

Item	Description
設定回復出廠預設值	清除全部的設定資料。
設定檔	顯示索引編號連結讓您點選進入設定頁面。
名稱	顯示應用程式管控的設定檔名稱。

按索引下方的號碼連結開啟如下視窗進行細節設定。

頁面中呈現四種不同的標籤，IM、P2P、協定與其他。下圖顯示協定標籤下的設定內容與支援的版本內容，您可核取方框選擇該項目阻擋用戶使用：

可用設定說明如下：

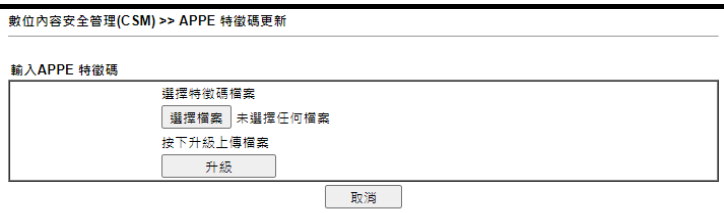
項目	說明
設定檔名稱	請輸入此設定檔名稱。
選擇全部	按此選擇本頁中全部的設定項目。
清除全部	按此捨棄選擇的項目。
☐	勾選此方框讓路由器封鎖選定的 APP。

V-2-2 APPE 特徵碼更新

路由器採用的 APP 物件設定檔被視為 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。

可用設定說明如下：

項目	說明
升級設定	**APPE 模組版本**– 顯示 APP 特徵碼目前的版本。 **自網際網路取得之新版本** – **下載**按鈕僅在 Vigor 路由器偵測出新的 APPE 版本之後才會有作用，按下該按鈕之後，畫面將會出現含有新版資訊的對話盒，按下**確定**按鈕離開該對話盒並開始更新特徵碼。 **透過介面升級** – 選擇一個 WAN 介面作為 APP 特徵碼更新的通道。
設定下載伺服器	輸入下載伺服器所在的 URL 以便進行下載作業，您也可以按更多連結來搜尋需要的下載伺服器。 **特徵碼驗證/下載訊息**–顯示 APPE 特徵碼更新時的狀態。
手動升級	**輸入** – 按下此鈕開啟如下頁面，按**選擇檔案**尋找先前自居易官網下載取得之特徵碼檔案，然後再按**升級**按鈕，等待系統完成更新作業。

	
自動升級	**排程更新 -** 勾選此框讓路由器能在指定的時間內進行 APPE 特徵碼更新。

完成設定之後，按下**確定**按鈕儲存相關設定。

V-2-3 URL 內容過濾器設定檔

爲了提供一個適當的網路空間給予使用者，Vigor 路由器配有 URL 內容過濾器，可限制一些不合法的資料於網站上進出，同時也禁止隱藏惡意碼的網路特徵於路由器內出入。

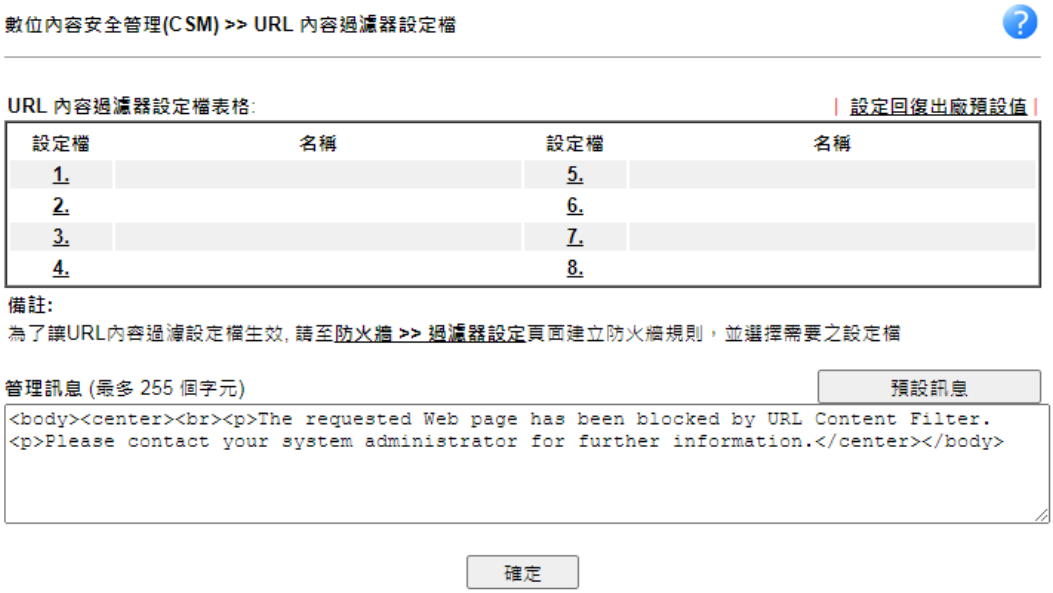
一旦使用者輸入關鍵字連結，URL 關鍵字阻擋工具將會拒絕該網頁之 HTTP 需求，如此一來使用者即無法存取該網站。您可以這樣想像一下，URL 內容過濾器為一個訓練有素的便利商店櫃員，絕對不販售成人雜誌給予未成年的小孩子。在辦公室內，URL 內容過濾器也可以提供與工作相關的環境，由此來增加員工的工作效率。URL 內容過濾器為什麼可以比傳統防火牆在過濾方面提供更好的服務呢？那是因為它能夠檢查 URL 字串或是一些隱藏在 TCP 封包負載的 HTTP 資料，而一般防火牆僅能以 TCP/IP 封包標頭來檢測封包。

換言之，Vigor 路由器可以防止使用者意外自網頁下載惡意的程式碼。惡意碼隱藏在執行物件當中是一件很普遍的事情，像是 ActiveX、Java Applet、壓縮檔和其他執行檔案。一旦用戶下載這些類型的檔案，用戶便會有這些可能爲系統帶來威脅的風險，例如一個 ActiveX 控制物件通常用於提供網頁人機通信交換功能，萬一裡面隱藏惡意的程式碼的話，該程式碼就可能會佔據使用者的系統。

例如，假設您新增關鍵字是“sex(性)” ，路由器即會限制進入某些網頁或是網站存取的功能，比方 www.sex.com、www.backdoor.net/images/sex/p_386.html，或者您也可以指定 URL 全名或部分的名稱如 www.sex.com 或是 sex.com 來加以限制。

此外，Vigor 路由器也會捨棄任何嘗試取回這些惡意程式碼的需求。

請至**數位內容安全管理(CSM)>> URL 內容過濾器設定檔**，下圖將會出現在螢幕上。



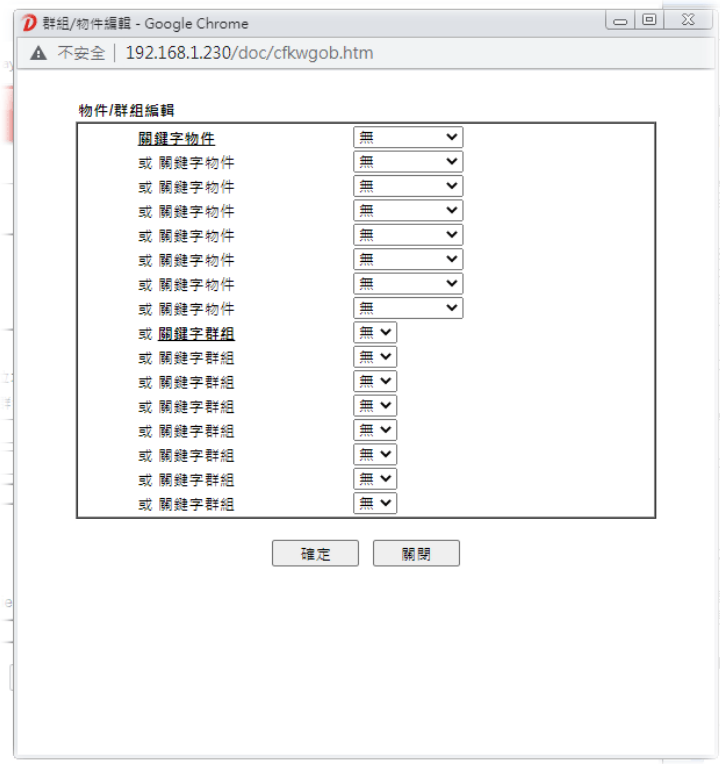
可用設定說明如下：

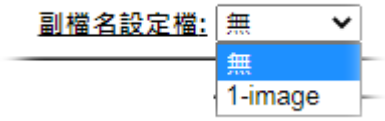
項目	說明
設定回復出廠預設值	清除全部的設定資料。
設定檔	顯示索引編號連結讓您點選進入設定頁面。
名稱	顯示設定檔名稱。
管理訊息	您可以視您的需要輸入所需的訊息。 **預設訊息-** 您可以手動輸入訊息或是按下此按鈕取得預設的訊息，並顯示在**管理訊息**方框內。

您可設定 8 組 URL 內容過濾器設定檔，請按索引編號連結，開啟如下頁面。

可用設定說明如下：

項目	說明
設定檔名稱	請輸入此設定檔名稱。
優先權	決定路由器採用的動作順序。 **二者:通過** – 路由器讓符合 URL 存取控制與網頁特徵所指定條件的封包放行通過，當您選擇此項設定時，本頁針對 URL 存取控制與網頁特徵所設定的限制都將暫停作用。 **二者:阻擋**- 路由器封鎖住任何符合 URL 存取控制與網頁特徵所指定條件的封包，當您選擇此項設定時，本頁針對 URL 存取控制與網頁特徵所設定的限制都將暫停作用。 **二者選一: URL 存取控制優先** – 當所有封包皆符合 URL 存取控制與網頁特徵之設定條件時，此功能可以決定先執行的動作為何。針對此項，路由器將先處理符合 URL 存取控制設定條件下的封包，然後再處理符合網頁特徵條件的封包。 **二者選一: 網頁特徵優先**- 當所有封包皆符合 URL 存取控制與網頁內容之設定條件時，此功能可以決定先執行的動作為何。針對此項，路由器將先處理符合網頁特徵條件下的封包，然後再處理符合 URL 存取控制設定條件的封包。
日誌	**通過**- 只有通過動作會記錄在 Syslog 中。 **阻擋**- 只有封鎖動作會記錄在 Syslog 中。 **全部**- 所有的動作(包含通過與封鎖)都會記錄在 Syslog 中。
URL 存取控制	**啟用 URL 存取控制功能** - 勾選此方塊啟動 URL 存取控制設定，請注意 **URL 存取控制**優先權原本就高於**網頁特徵(Restrict Web Feature)**，如果網頁內容符合 URL 存取控制中的設定，路由器將先執行此區所指定的動作，而忽略網頁特徵中所指定的動作。 **防止透過 IP 位址對網站進行存取**- 勾選此方塊拒絕任何使用 IP

	位址例如 http://202.6.3.2 來要求存取資料的活動，這個項目可以防止他人躲避 URL 存取控制的監控，您必須先清除瀏覽器的快取資料，讓 URL 內容過濾器工具能夠在您所造訪的網頁上適當的操作。 **動作** – 此功能僅在您選擇了**二者選一: URL 存取控制優先**或**二者選一: 網頁特徵優先**時才能使用。 ● **通過** - 允許進入含有關鍵字清單中之關鍵字的網頁。 ● **阻擋** - 不允許進入含有關鍵字清單中之關鍵字的網頁。若網頁並不符合此處所設定的關鍵字清單設定，該網頁將以相反動作來處理。 **除外清單** – 指定物件設定檔，以便採取與上述指定的動作相反的行為。 **群組/物件選擇** – Vigor 路由器提供數種方框讓您定義關鍵字，每個方框都支援數個關鍵字。關鍵字可以是一個名詞、數字、部分名稱或是完整的 URL 字串，方框內多數關鍵字可以空白、逗號或是分號來區隔。另外，每個方框最大的長度為 32 個字元。指定完關鍵字後，Vigor 路由器將婉拒符合任何使用者定義的關鍵字之網頁的 URL 連線需求。注意，封鎖的關鍵字寫得越簡化，Vigor 路由器執行起來也會更加有效率。 
網頁特徵	**啟用限制網頁特徵-** 勾選此方塊讓關鍵字被封鎖或是放行。 **動作** - 此功能僅在您選擇了**二者選一: URL 存取控制優先**或**二者選一: 網頁特徵優先**時才能使用。 **通過** - 允許進入含有關鍵字清單中之關鍵字的網頁。 **阻擋** - 不允許進入含有關鍵字清單中之關鍵字的網頁。若網頁並不符合此處所設定的關鍵字清單設定，該網頁將以相反動作來處理。 **副檔名設定檔** - 請自**物件設定>>副檔名物件**中選擇一個事先設定完成的設定檔，並決定其對檔案下載採取封鎖或是放行的動作。

	 **Cookie** - 勾選此方塊從內部到外部過濾 cookie 傳輸資料以保護本地用戶的隱私。 **代理伺服器** - 勾選此方塊退回任何的伺服器傳輸要求。想要有效控制頻寬，讓封鎖機制過濾從網站下載的多媒體檔案是最有價值的事情。 **上傳**- 勾選此方框以封鎖檔案透過網頁上傳。

完成設定之後，按下**確定**按鈕儲存相關設定。

V-2-4 網頁內容過濾器設定檔

服務啟動精靈讓您使用試用版或是直接更新 WCF 授權碼，無需登入 http://myvigor.draytek.com 的伺服器(***MyVigor***)。

按下**數位內容安全管理**(CSM)然後選擇**網頁內容過濾器設定檔**開啟設定頁面，其中，設定搜尋伺服器/設定測試伺服器都是自動選定的，您可以按下**更多**連結開啟另一視窗然後選擇需要的伺服器。

資訊 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)，您必須先進行啟用的程序。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。
資訊 2	Commtouch 已經併入 Cyren，其 GlobalView 服務仍將持續提供強大且以雲端為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

可用設定說明如下：

項目	說明
啟動	按下此鈕登入 MyVigor 以便啟動 WCF 服務。
設定詢問伺服器	建議您使用預設的設定，當您以 WCF 設定檔為基準，在瀏覽器

	上輸入 URL 時，您需要指定伺服器來歸類搜尋的內容。
設定測試伺服器	建議您使用預設的設定。
搜尋更多	按下此鈕開啟畫面選擇另外的伺服器。
快取	**無**– 路由器將會透過 WCF 機制檢查使用者想要登入的 URL，處理的速度為一般，這個選項可提供最準確的 URL 過濾作業。 **L1** – 路由器將會透過 WCF 機制檢查使用者想要登入的 URL，如果該 URL 早先已經存取過，系統會將此資料在路由器內儲存非常短暫的時間(大約 1 秒)，讓必要時可以快速登入。此選項可以提供速度較快的 URL 過濾作業。 **L2** – 路由器將會透過 WCF 機制檢查使用者想要登入的 URL，如果該 URL 早先已經存取過，系統會將其 IP 位址在路由器內儲存非常短暫的時間(大約 1 秒)，當使用者想要再次登入相同的 IP 時，路由器會將其與儲存的內容做比對，如果符合，該頁面就會迅速取回並呈現出來。此選項可以提供速度最快的 URL 過濾作業。 **L1+L2 快取** – 路由器將會以 L1 加上 L2 的功能快速檢查 URL。
設定回復出廠預設值	按下此連結回復出廠預設值。
設定檔	設定檔索引編號。
名稱	設定檔之檔名。
管理訊息	您可以手動輸入訊息或是按下**預設訊息**按鈕取得預設的訊息，並顯示在**管理訊息**方框內。

您可設定 8 組網頁內容過濾器設定檔，請按索引編號連結，開啟如下頁面。分類中的項目依照不同的服務供應商而有所改變，如果您已經且啟動了另一個網頁內容過濾器授權碼，相關的分類項目也會隨之變更。所有 WCF 所做的設定都會被刪除，因此在您變更網頁內容過濾器授權碼之前，請先備份資料。

可用設定說明如下：

項目	說明
設定檔名稱	輸入網頁內容過濾器設定檔的名稱。
日誌	**通過**- 只有通過動作會記錄在 Syslog 中。 **封鎖**- 只有封鎖動作會記錄在 Syslog 中。 **阻擋**- 所有的動作(包含通過與封鎖)都會記錄在 Syslog 中。
黑/白名單	**啟用-** 勾選此方塊啟用過濾機制，利用黑白名單的內文來決定。 ● **動作，通過** – 網頁內文符合本區所選定的關鍵字物件/群組內容，於經過路由器時可通行無阻。 ● **動作，阻擋** - 網頁內文符合本區所選定的關鍵字物件/群組內容，於經過路由器時會被阻擋下來。 **URL 關鍵字-**請按**編輯(Edit)**按鈕開啟視窗，並自其中選擇一個您需要的項目，然後針對此項目再選擇要執行的動作為何。
群組與種類	選擇設定檔包含的種類。 **動作** - 當 URL 符合關鍵字群組與物件的設定條件內容時可以採取如下的動作。 ● **通過** – 允許進入勾選的方塊等相關類型頁面。 ● **阻擋** – 限制進入勾選的方塊等相關類型頁面。如果網頁未符合此處所設定的內容，系統將以反向做為處理該網頁。 **選擇全部** - 按此選擇各群組的全部類別。 **清除全部** - 按此清除各群組的全部類別。

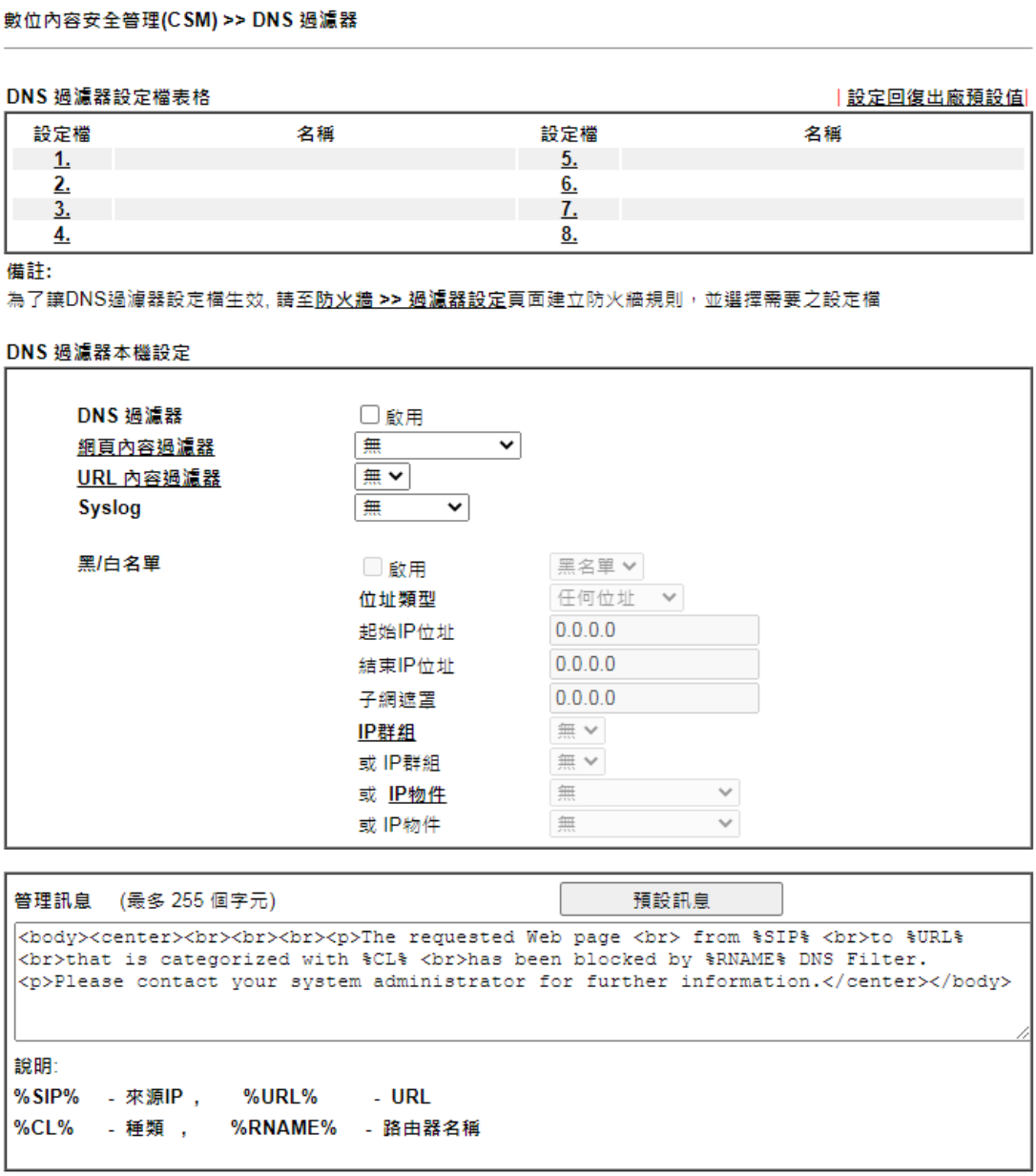
完成設定之後，按下**確定**按鈕儲存相關設定。

V-2-5 DNS 過濾器設定檔

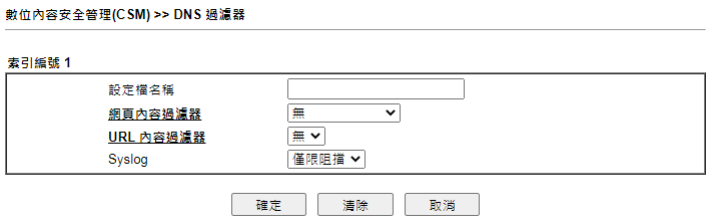
DNS 過濾器監控 DNS 的諮詢，並將相關資訊傳送至 WCF，以便歸類 HTTPS URL。

DNS 可利用路由器伺服器(例如 168.95.1.1)或是外部 DNS 伺服器(例如 8.8.8.8)於 **LAN>>基本設定**中指定，如果使用路由器伺服器，**DNS 過濾器基本設定(DNS Filter General Setting)**將套用到 LAN 端用戶的 DNS 詢問中。不過如果使用的是外接 DNS 伺服器，**DNS 過濾器設定檔(DNS Filter Profile)**將套用到 LAN 端用戶的 DNS 詢問中。

資訊	因為 DNS 過濾器必須使用 WCF 服務來過濾封包，因此 WCF 授權碼必須事先啟動才行。否則，DNS 過濾器無法對封包產生任何效用。



可用設定說明如下：

項目	說明
DNS 過濾器設定檔表格	顯示不同的 DNS 過濾器設定檔清單資料。 按下索引編號連結開啟如下頁面，然後輸入設定檔名稱並依照您的需要指定網頁內容過濾器(WCF)/URL 內容過濾器(UCF)等過濾器設定檔以資套用。 
DNS 過濾器本機設定	若尚未設定好任何 DNS 設定檔，此處的基本設定將會套用至 DNS 過濾器。

	DNS 過濾器) - 勾選**啟用**以便啟用此功能。 **網頁內容過濾器-** 設定網頁內容過濾器的過濾條件。 **URL 內容過濾器-** 設定 URL 內容過濾器的過濾條件。 **Syslog -** 過濾結果將依照 Syslog 設定來記錄。 ● **無** –此設定沒有任何內容會被記錄下來。 ● **僅限通過** –只有封包通過的記錄會被轉往 Syslog。 ● **僅限阻擋** –只有封包被封鎖的記錄會被轉往 Syslog。 ● **二者**–所有的動作(通過與阻擋)記錄都會被轉往 Syslog。 **黑/白名單 -** 可指定 IP 位址、子網遮罩、IP 物件或是 IP 群組作為黑名單或是白名單，讓路由器可以放行 DNS 封包或是阻擋封包。
管理訊息	輸入文字或是完整句子，當 Vigor 路由器封鎖頁面時將會呈現此管理訊息。

完成設定之後，按下**確定**按鈕儲存相關設定。

應用說明

A-1 如何建立一個 MyVigor 帳號

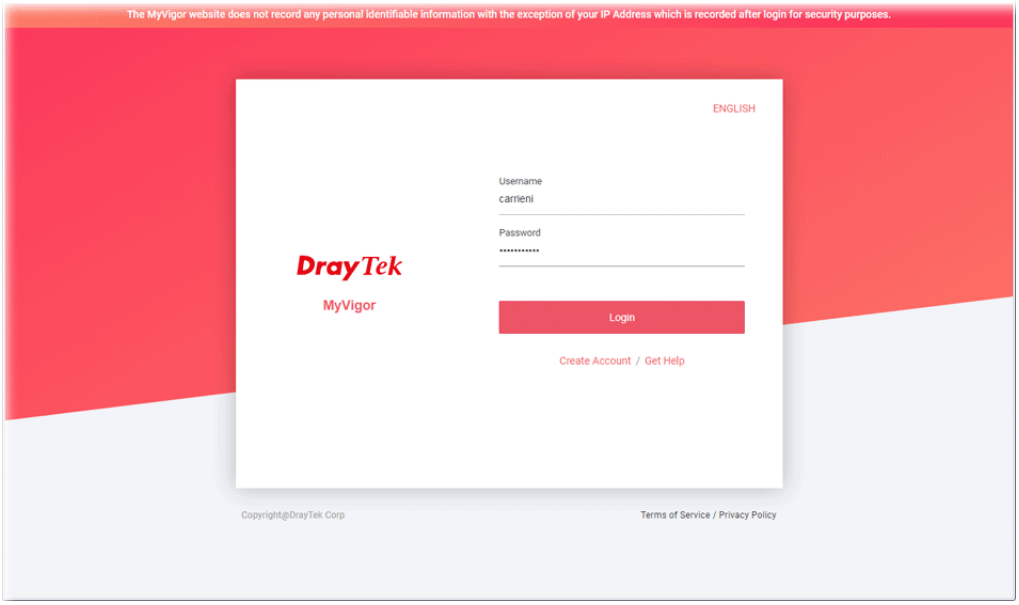
MyVigor 網站(http://myvigor.draytek.com)提供數種有用的服務(諸如防垃圾信、網頁內容過濾、防入侵等等)來過濾網頁，以便保障您的系統的安全。

如要進入 MyVigor 取得更多的資訊，請先建立一個 MyVigor 帳號。

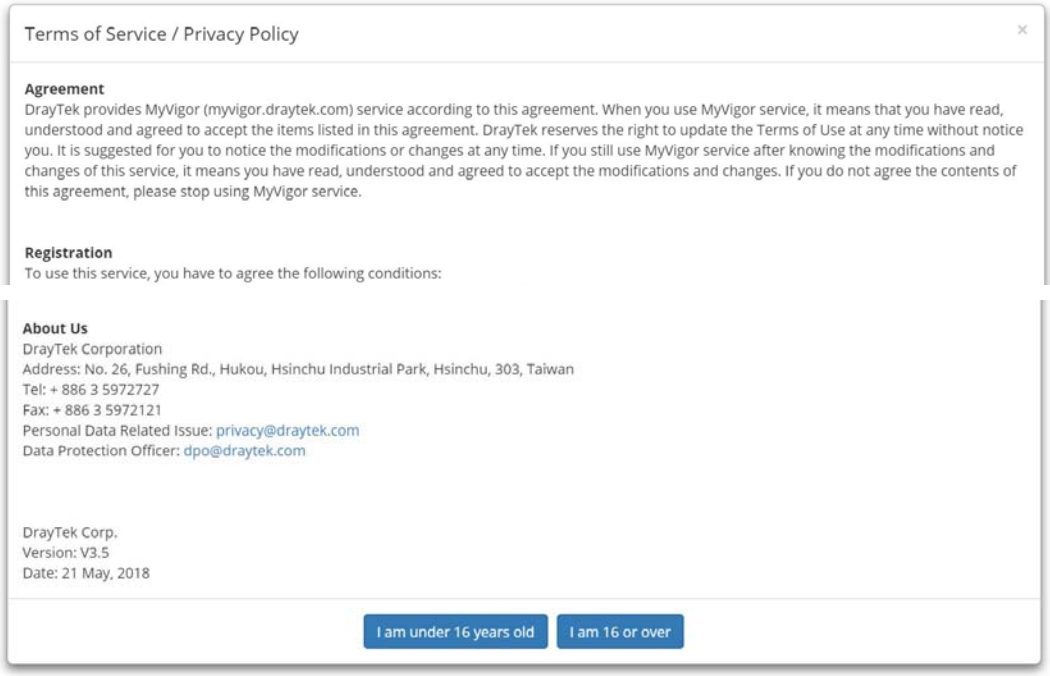
透過 Vigor 路由器來建立

1. 開啟**數位內容安全管理(CSM)>>網頁內容過濾器設定檔**，您可見到如下頁面：

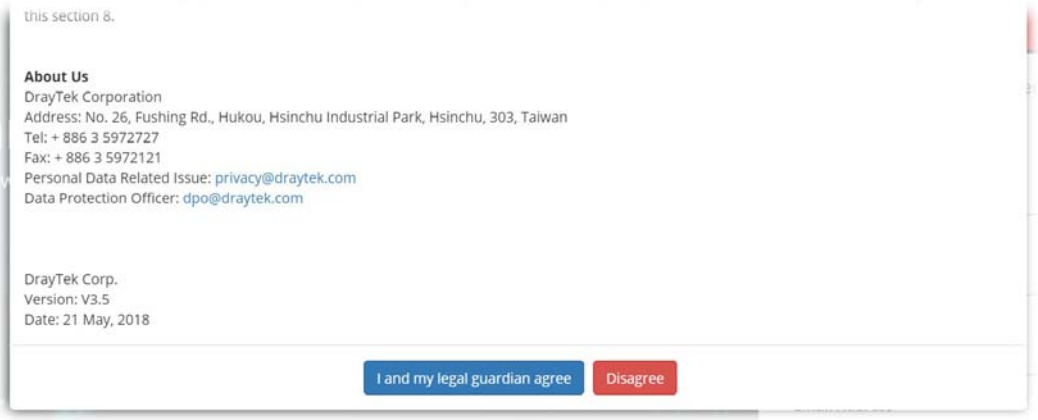
2. 按下**啟動**連結，MyVigor 登入視窗將會自動跳出。



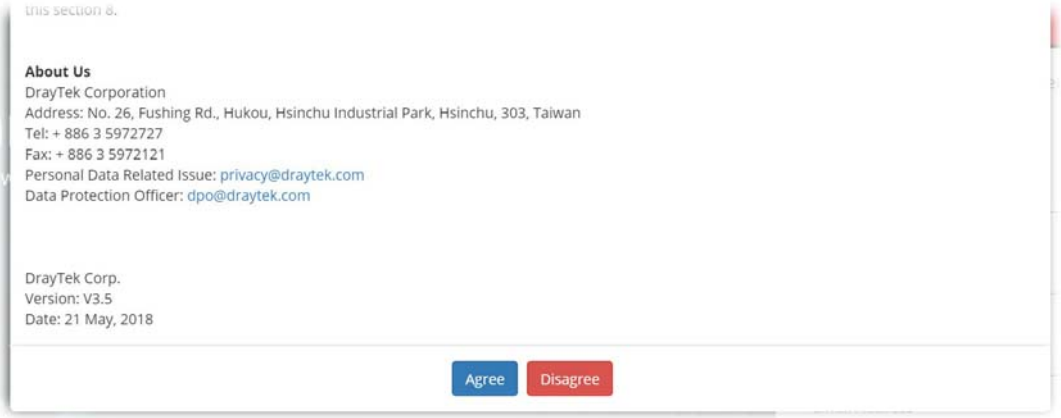
3. 按下 **Create Account** 連結。
4. 系統將會詢問你是否已滿 16 歲。
   - 如果是，請按下 **I am 16 or over**。



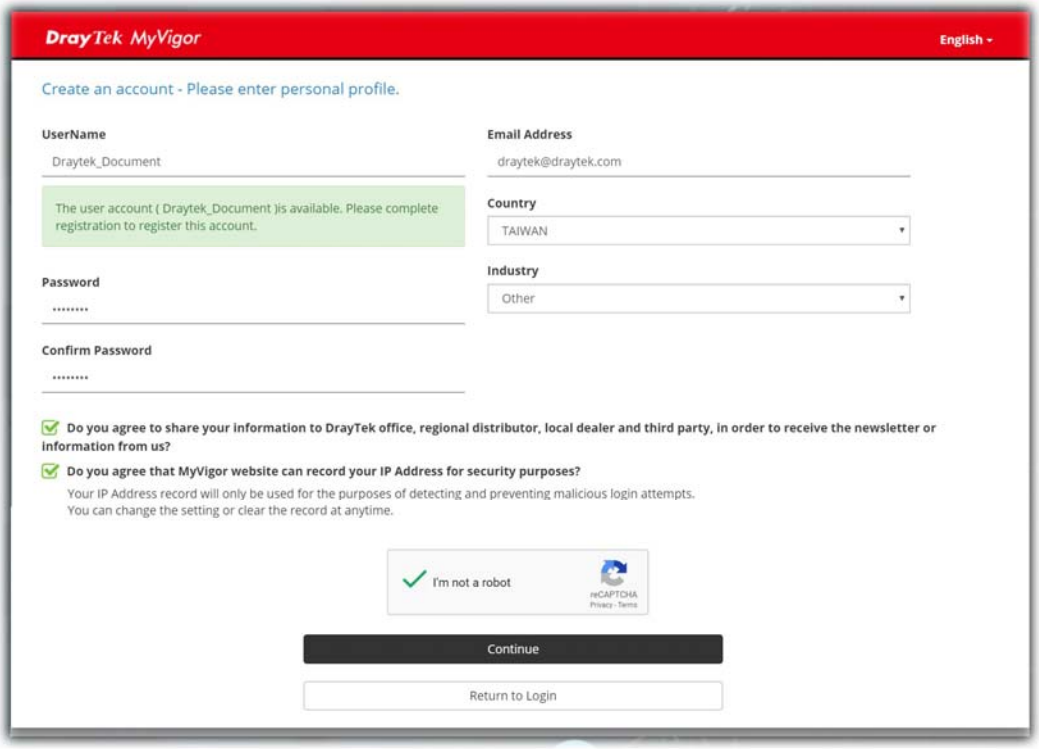
   - 如果不是，請按 **I am under 16 years old** 進入以下頁面，接著按下 **I and my legal guardian agree**。



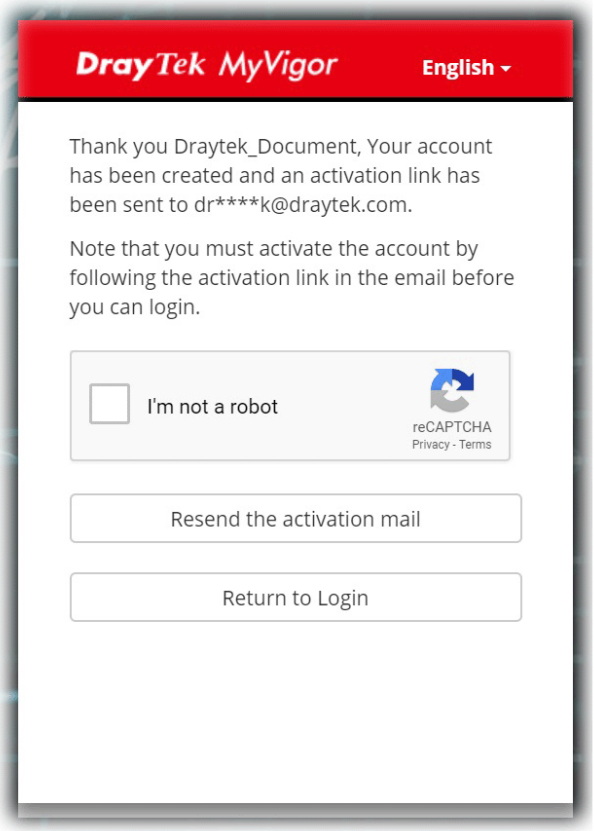
5. 閱讀上面的說明之後，接著請按下 **Agree**。



6. 輸入個人資訊並按下 **Continue**。



7. 選擇適合您的電腦的選項，再按下 **Continue**。


DrayTek MyVigor
English
Thank you Draytek_Document, Your account has been created and an activation link has been sent to dr****k@draytek.com.
Note that you must activate the account by following the activation link in the email before you can login.
I'm not a robot
reCAPTCHA
Privacy - Terms
Resend the activation mail
Return to Login

8. 現在您已經成功建立一個帳號了。
9. 請先去信箱查看郵件，是否收到標題為 **New Account Confirmation Letter from myvigor.draytek.com** 的信件。

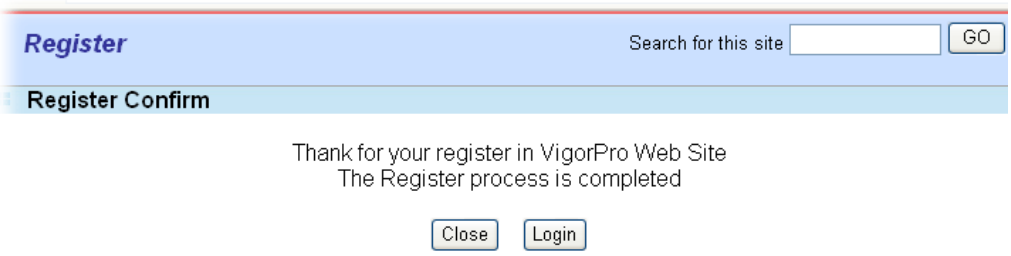
****** This is an automated message from myvigor.draytek.com. ******

Thank you (**Mary**) for creating an account.

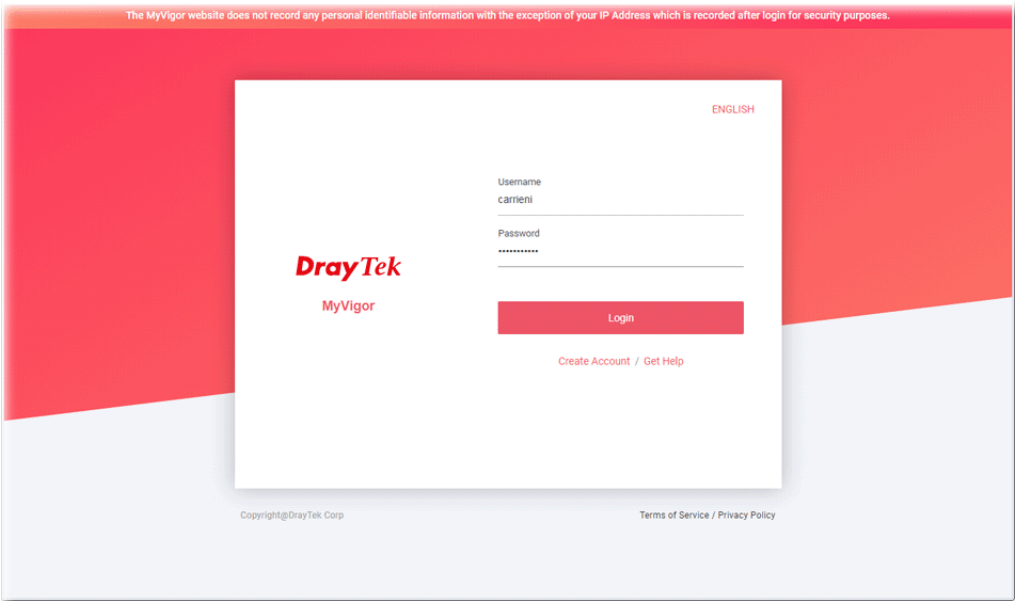
Please click on the activation link below to activate your account

Link : Activate my Account

10. 若已收到，請按下 **Activate my Accoun** 連結啟動帳號，下圖將會顯示出來，表示註冊過程已經完成，請按 **Login**。



11. 當您看看如下頁面時，請輸入帳號與密碼(您剛剛在前述步驟中建立)。



12. 按下 Login。系統將帶您進入 MyVigor 伺服器。

A-2 用網頁內容過濾器(WCF) /URL 內容過濾器來阻擋使用者存取 Facebook 服務

阻擋使用者存取 Facebook 網頁有二種方式，網頁內容過濾器(WCF)與 URL 內容過濾器。

網頁內容過濾器(WCF),

優點：簡單迅速套用至您想要阻擋的類別/網站

附註：需搭配授權碼

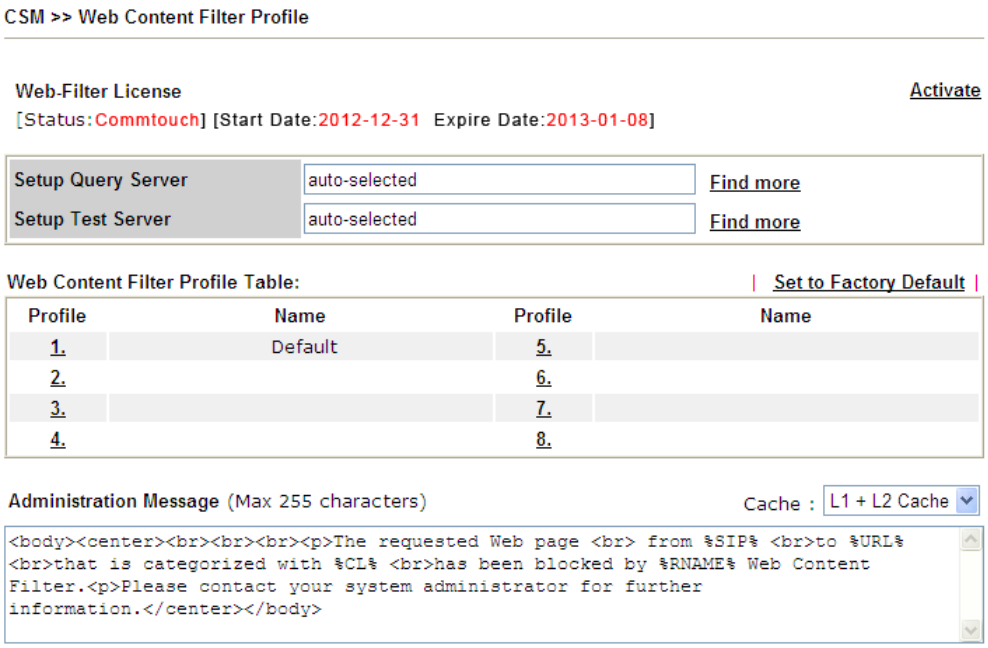
URL 內容過濾器,

優點：免費，對於客製化網頁具有彈性

附註：須手動調整設定 (例如一個網站設定一個關鍵字等)

I. 透過網頁內容過濾器(WCF)

1. 請確認網頁內容過濾器(WCF) (由 Commtouch 提供服務)授權碼仍在有效期內。



2. 開啟**數位內容安全管理(CSM) >> 網頁內容過濾器設定檔**建立新的 WCF 設定檔，請勾選**社群網路**，**動作**請選擇**阻擋**。

3. 在**防火牆>>基本設定>>預設規則**這個頁面當中，請用剛剛設定的設定檔。

4. 下次，當用戶嘗試透過路由器進入 Facebook 時，網頁將被封鎖起來，系統並傳送及顯示如下訊息給您。

The requested Web page
from 192.168.2.114
to www.facebook.com/
that is categorized with [Social Networking]
has been blocked by Web Content Filter.

Please contact your system administrator for further information.

[Powered by DrayTek]

II. 透過 URL 內容過濾器

A. 阻擋存取 Facebook 字眼的網頁

1. 開啟**物件設定>>關鍵字物件**，按下任一索引連結以進入設定頁面。
2. 在**內容**區域中，輸入 *facebook*，參考下圖所示。按下**確定**儲存。

3. 開啟**數位內容安全管理>>URL 內容過濾器設定檔**，按下任一索引連結開啟設定頁面。
4. 請按下圖所示輸入內容。

5. 完成上述設定之後，按下**確定**儲存。接著開啟**防火牆>>基本設置**。

6. 選擇**預設規則**標籤，在開啟的頁面上，於 **URL 內容過濾器**選項中選擇剛剛設定的設定檔。按下**確定**儲存。

B. 阻擋使用者使用 **Facebook** 的小遊戲

1. 開啟**物件設定>>關鍵字物件**，按下任一索引連結以進入設定頁面。

2. 在**內容**區域中，輸入 *apps.facebook*，參考下圖所示。按下**確定**儲存。

3. 開啟**數位內容安全管理(CSM)>>URL 內容過濾器設定檔**，按下任一索引連結開啟設定頁面。
4. 請按下圖所示輸入內容。

5. 完成上述設定之後，按下**確定**儲存。接著開啟**防火牆>>基本設置**。
6. 選擇**預設規則**標籤，在開啟的頁面上，於 **URL 內容過濾器**選項中選擇剛剛設定的設定檔。按下**確定**儲存，才能阻擋 apps.facebook 字眼的網址。

防火牆 >> 基本設置

基本設置

基本設置 | 預設規則

預設規則之動作:

其他應用	動作/設定檔	Syslog
過濾器	通過	☐
連線數控制	0 / 60000	☐
服務品質	無	☐
使用者管理	無	☐
APP應用程式管控	無	☐
URL 內容過濾器	1-facebook.apps	☐
網頁內容過濾器	無	☐
DNS 過濾器	無	☐

進階設定 [編輯]

[確定] [取消]

備份防火牆: [備份] | 還原防火牆: [選擇檔案] 未選擇任何檔案 [還原]

備註:
這並不會備份服務品質(QoS)與排程的細節設定

第六篇 管理設定

System Maintenance

路由器系統安裝包含數種項目：系統狀態、TR-069、管理者密碼、使用者密碼、登入頁面歡迎詞、設定備份、Syslog/郵件警告、時間與日期、管理、重新啟動系統、韌體更新與啟動等等。

Bandwidth Management

用於控制資料傳輸之頻寬，主要是透過連線數限制、頻寬限制以及服務品質(QoS) TR-069等等。

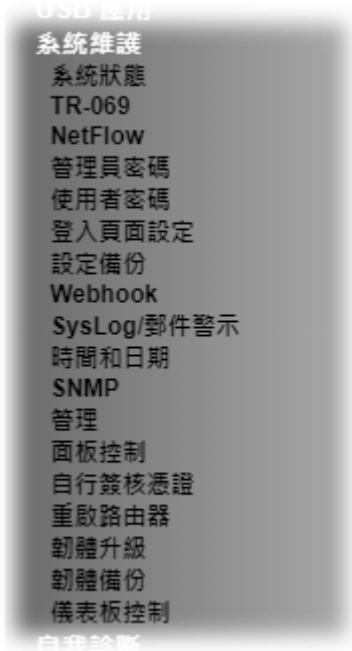
User Management

此功能不允許來自特定主機的任何IP流量(除了DHCP相關的封包外)，除非該主機能提供正確的使用者名稱與密碼。

VI-1 系統維護

系統設定方面，有數種項目是使用者需要瞭解的：系統狀態、TR-069、NetFlow、系統管理員密碼、使用者密碼、登入頁面設定、Webhook、SysLog/郵件警示、時間和日期、SNMP、管理、面板控制、自行簽核憑證、重啟路由器、韌體升級、韌體備份及儀表板控制等等。

下圖為系統維護的主要設定功能。



網頁使用者介面

VI-1-1 系統狀態

系統狀態提供基本的網路設定，包含區域網路和 WAN 介面等資訊，同時您也可以獲得目前執行中的韌體版本或是韌體其他的相關資訊。

系統狀態

型號名稱 : Vigor2135ac
韌體版本 : 4.4.1_STD
建立日期/時間 : Feb 14 2022 10:55:27

區域網路(LAN)					
	MAC位址	IP 位址	子網遮罩	DHCP 伺服器	DNS
區域網路(LAN)1	14-49-BC-0A-8A-B8	192.168.1.1	255.255.255.0	關閉	8.8.8.8
區域網路(LAN)2	14-49-BC-0A-8A-B8	192.168.2.1	255.255.255.0	關閉	8.8.8.8
區域網路(LAN)3	14-49-BC-0A-8A-B8	192.168.3.1	255.255.255.0	關閉	8.8.8.8
區域網路(LAN)4	14-49-BC-0A-8A-B8	192.168.4.1	255.255.255.0	關閉	8.8.8.8
IP路由子網	14-49-BC-0A-8A-B8	192.168.0.1	255.255.255.0	關閉	8.8.8.8

無線區域網路 (2.4GHz)			
MAC位址	頻率網域	韌體版本	SSID
16-49-BC-4A-8A-B8	歐洲	5.0.4.0	DrayTek

無線區域網路 (5GHz)			
MAC位址	頻率網域	韌體版本	SSID
14-49-BC-0A-8A-B8	歐洲	5.0.4.0	DrayTek_5G

廣域網路(WAN)					
	鏈結狀態	MAC位址	連線	IP 位址	預設閘道
廣域網路(WAN)1	斷線	14-49-BC-0A-8A-B9	DHCP 用戶端	---	---
廣域網路(WAN)3	斷線	14-49-BC-0A-8A-BB	---	---	---

IPv6			
	位址	範圍	網際網路連線模式
區域網路(LAN)	FE80::1649:BCFF:FE0A:8AB8/64	Link	---

使用者模式 現已 關閉

可用設定說明如下：

項目	說明
型號名稱	顯示路由器的型號名稱。
韌體版本	顯示路由器的韌體版本。
建立日期/時間	顯示目前韌體建立的日期與時間。
LAN	**MAC 位址** - 顯示區域網路介面的 MAC 位址。 **IP 位址** - 顯示區域網路介面的 IP 位址。 **子網遮罩** - 顯示區域網路介面的子網路遮罩位址。 **DHCP 伺服器**

	- 顯示區域網路介面的 DHCP 伺服器目前的狀態。 **DNS** - 顯示主要 DNS 的 IP 位址。
無線網路	**MAC 位址** - 顯示無線區域網路的 MAC 位址。 **頻率網域** - 網域可以是歐洲(13 個可用頻道)，美國(11 個可用頻道)，無線產品所支援之可用頻道在不同的國家下是不相同的。 **韌體版本** - 表示配備 WLAN miniPCi 卡的詳細資訊，同時可以提供該卡相關的特徵訊息。 **SSID** - 顯示路由器的 SSID。
WAN	**鏈結狀態** - 顯示目前實體連線的狀態。 **MAC 位址** - 顯示 WAN 介面的 MAC 位址。 **連線** - 顯示目前連線的類型。 **IP 位址** - 顯示 WAN 介面的 IP 位址。 **預設閘道** - 顯示預設閘道指定的 IP 位址。

VI-1-2 TR-069

此路由器支援 TR-069 標準，對管理人員來說透過 ACS (例如 VigorACS) 來管理 TR-069 裝置是相當方便的。

VI-1-2-1 ACS 和 CPE 設定

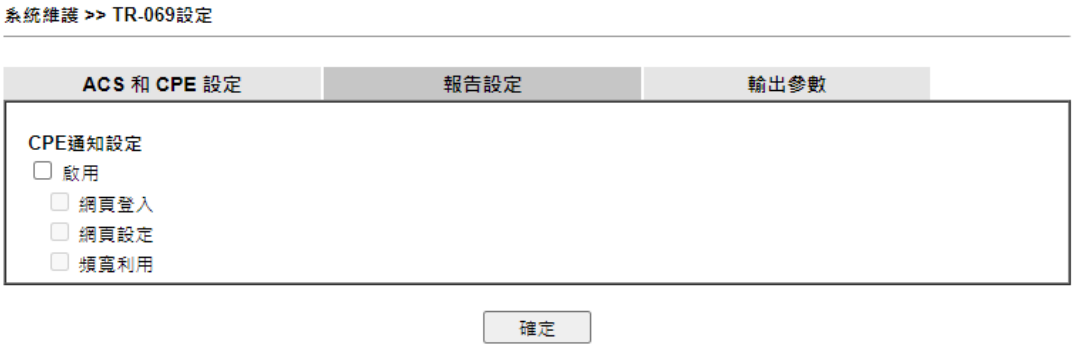
可用設定說明如下：

項目	說明
TR-069	啟用或停用 TR-069 供能。
ACS 伺服器開啟	選擇路由器連往 ACS 伺服器的介面。
啟用系統維護 >> 管理 >> 網際網路連線設定控制的 TR069 伺服器	當啟用 TR-069 功能時，為了讓 VigorACS 與路由器能雙邊連絡，可以勾選此框，讓系統自動啟用位於系統維護 >> 管理 >> 網際網路連線設定控制的 TR-069 伺服器。若該 TR-069 伺服器未被勾選，VigorACS 將無法順利操作進行或遠端控制此路由器。
ACS 伺服器	**URL/使用者名稱/密碼-** 此資料必須依照您想要連結的 ACS 內容來輸入，請參考 ACS 使用者取得詳細的資訊。 **測試通知** – 如果 CPE 能與 VigorACS SI 伺服器溝通，按此傳送以事件代碼選項為基準的訊息進行測試。 **事件代碼** – 使用下拉式清單指定事件以應測試之需。 **上次通知回應時間**– 顯示 VigorACS 伺服器上次接收 CPE 通知訊息並做出回應的時間。
CPE 用戶端	基本上您不需要在此輸入任何資料，因為這邊的資料主要是提供給 ACS 伺服器參考使用的。 **通訊協定** – 如果連線要加密請選 Https；否則可選 Http。 **連接埠** – 有時候，埠號衝突是可能發生的，為了解決這樣的困境，您可以替 CPE 變更不同的埠號值。 **使用者名稱與密碼**– 輸入 VigorACS 用來登入此 CPE 所需之使用者名稱與密碼。
定期通知設定	預設值為**啟用**，請設定間隔時間或是排程時間，讓路由器傳送通知訊息給 CPE 端，或是選**停用**關閉通知機制。
STUN 設定	預設值是**停用**，如果您選擇了**啟用**，請輸入下述相關資料： **伺服器位址 -** 輸入 STUN 伺服器的 IP 位址。 **伺服器 STUN 埠號 -** 輸入 STUN 伺服器的埠號。 **最小維持連線時間-** 如果啟用了 STUN，CPE 必須傳送綁定需求至伺服器，以便維持與閘道綁定的需要。請輸入數字作為最小的維持時間，預設值為 60 秒。 **最大維持連線時間-** 如果啟用了 STUN，CPE 必須傳送綁定需求至伺服器，以便維持與閘道綁定的需要。請輸入數字作為最大的維持時間，數值-1 表示未指定最大維持時間。
套用設定至 AP	啟用此項可讓 TR-069 設定同時套用到路由器管理下的全部 AP 上。 **停用**– 相關設定不會套用到 AP 上。 **啟用**– 上述 STUN 設定在按下**確定**之後會套用到 AP 上，啟用此功能之後，請輸入密碼以利後續登入 AP。 ● **AP 密碼**– 輸入您想套用路由器 TR-069 設定之 VigorAP 的登入密碼。 **指定 AP/交換器需求之 STUN 設定** – 選擇**啟用**後，若您僅想要套用 STUN 設定至 VigorAP 上以符合特殊需要，請勾選此框。接著分別輸入伺服器 IP 位址、伺服器埠號、最小維持連線時間與最大維持連線時間。

完成設定之後，按下**確定**按鈕儲存相關設定。

VI-1-2-2 報告設定

與路由器建康有關的資訊區分成數種並且分別條列於本區中。檢查完相關項目之後，路由器將會整理並傳送資訊至 VigorACS 伺服器，提供予系統管理員參考。



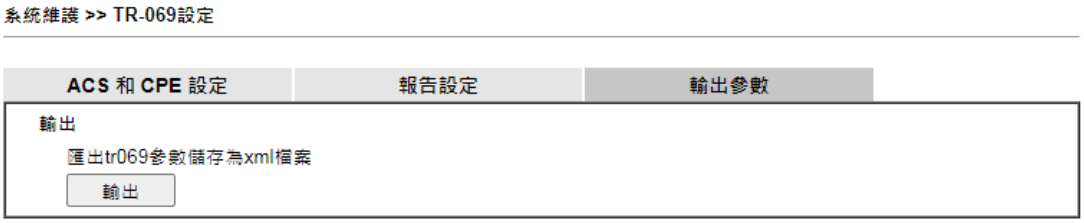
可用設定說明如下：

項目	說明
CPE 通知設定	**啟用** - 勾選此框選擇通知項目。 Vigor 路由器將傳送使用狀態給予 VigorACS。

按**確定**儲存頁面變更。

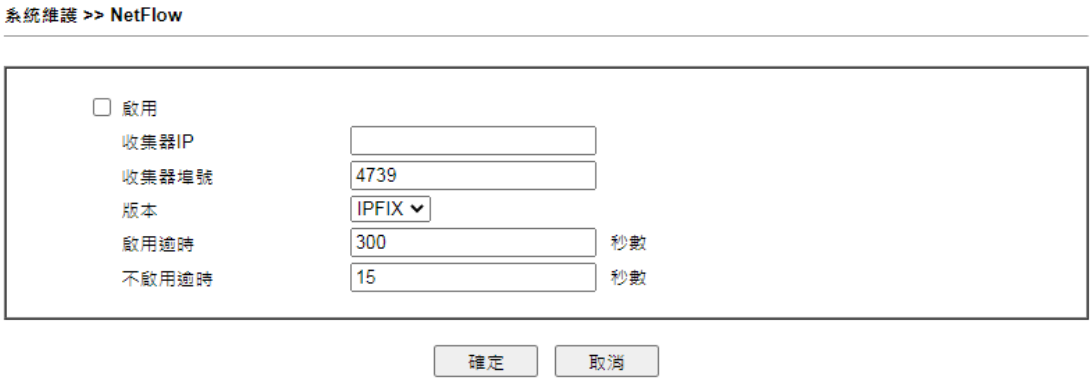
VI-1-2-3 輸出參數

按下**輸出**將 TR-069 參數設定儲存為".xml"檔案。



VI-1-3 NetFlow

本頁可讓您設定透過 NetFlow 功能監控封包資訊的伺服器 IP 位址、埠號、版本與逾時秒數。



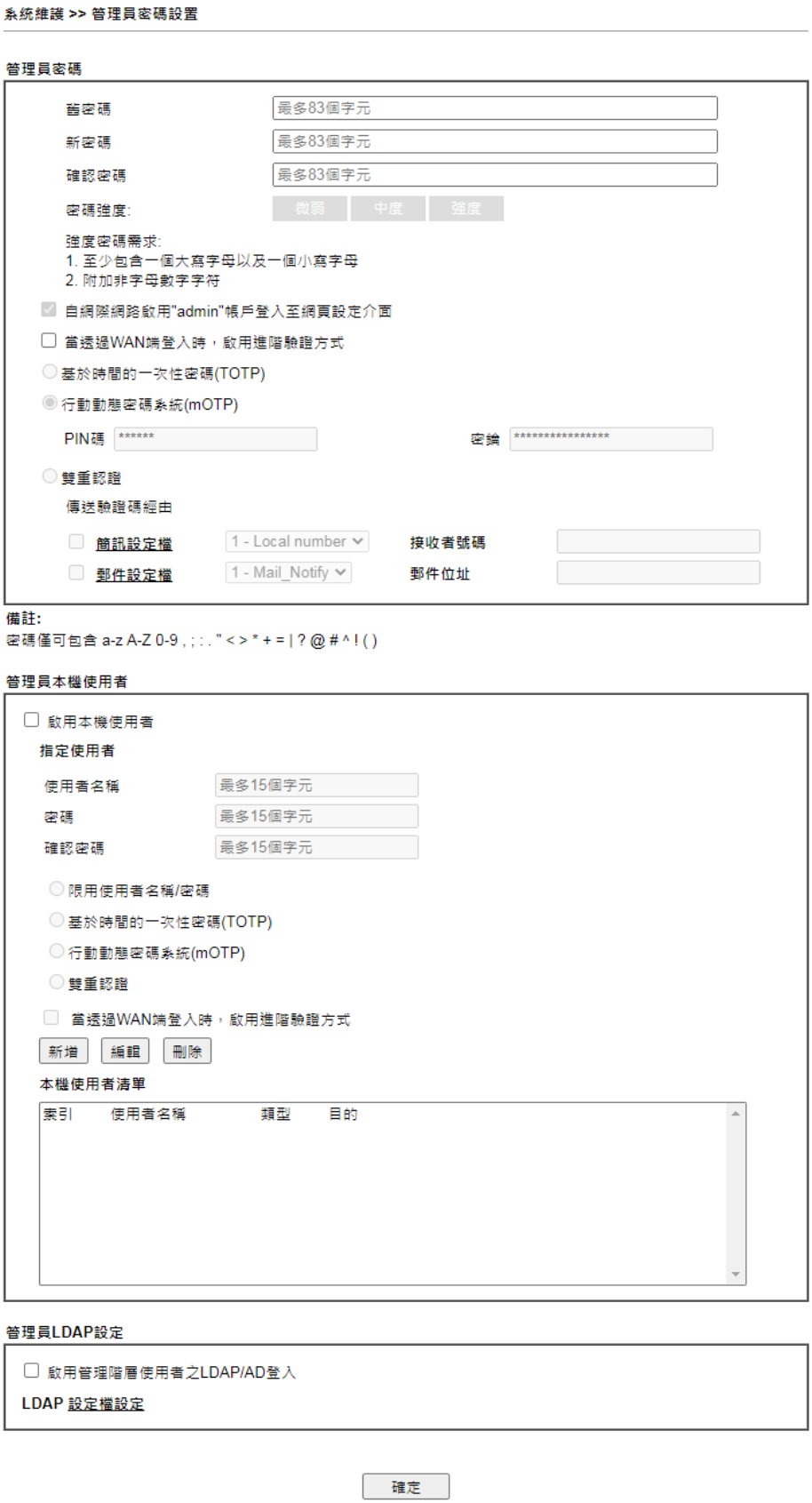
可用設定說明如下：

項目	說明
啟用	**啟用** - 勾選此框啟用此功能。
收集器 IP	輸入作為資料流收集器之伺服器(例如 VigorConnect)的 IP 位址。
收集器埠號	輸入伺服器埠號值。
版本	路由器支援三種版本(v5, v9 與 IPFIX) 。
活動逾時	可設定範圍自 60 到 1800 秒，預設值為 300 秒。 設定標記資料流活動的時間間隔，伺服器將不斷的收集資料流資訊直到設定停止之時間為止。
不活動逾時	可設定範圍自 15 到 1800 秒。 設定標記資料流不再活動的時間間隔，在到達不活動逾時之設定時間後，收集的資料流資訊將立即被輸出。

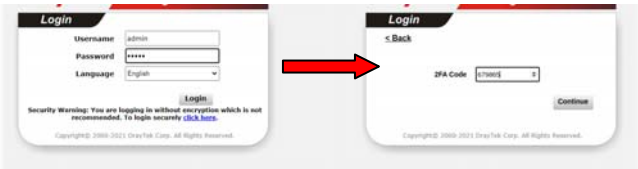
按**確定**儲存頁面變更。

VI-1-4 管理員密碼

本頁允許您設定新的密碼。



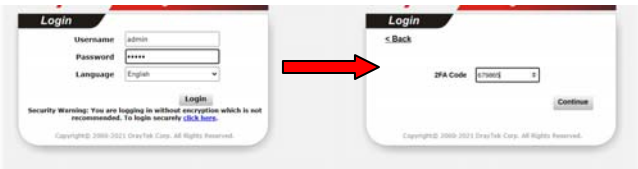
可用設定說明如下：

項目	說明
管理員密碼	管理員可以登入網頁使用者介面，進行設定修改以便符合實際需求。 **舊密碼** – 輸入舊的密碼，出廠預設值為**“admin”**。 **新密碼** – 在本區輸入新的密碼。 **確認密碼** – 再次輸入新的密碼。 **密碼強度** - 顯示上述設定之密碼之安全性強度。 **自網際網路啟用‘admin’帳戶登入至網頁設定介面**– 選擇此項讓管理員能從網際網路端登入此網頁設定介面，這個選項在管理員本機使用者為啟用狀態時，也是啟用的。 **當透過 WAN 端登入時，啟用進階驗證方式** – 進階驗證方法提供一個更加安全的網路連線，從 WAN 端登入時，可選擇基於時間的一次性密碼(TOTP) 或是行動動態密碼系統(mOTP)或是雙重認證。 ● **基於時間的一次性密碼(TOTP) -** 請確認路由器的時區是否正確，接著在手機或行動裝置上安裝 Google 驗證 APP，開啟 APP 掃描本頁上的 QR code，您的手機將會顯示出一次性的密碼資訊。 在**驗證碼**中，請輸入密碼並按下**驗證**。 現在，已完成設定。系統將會要求您在輸入使用者名稱及密碼後，另外輸入二階段密碼進行驗證。  ● **行動動態密碼系統(mOTP)** –選擇此項可以使用 mOTP 密碼來登入。輸入 PIN 碼及密鑰設定，以取得一次性密碼。 ● **雙重認證，透過簡訊設定檔 與/或 郵件設定檔** –選擇簡訊與/或郵件設定檔，接收者號碼以及/或電子郵件，以便傳輸密碼。
管理員本機使用者	管理者可以登入 Vigor 路由器的使用者介面，以修改設定符合實際的需要。此項功能讓 LAN 端其他的用戶具有管理者相同的權限，藉以登入路由器的使用者介面。 **啟用本機使用者**– 勾選此框啟用本地使用者設定。 **指定使用者** – 建立新的使用者名稱做為本機使用者，然後再指定驗證方法(區分為基本與進階)。 ● **使用者名稱**– 給予本地用戶之使用者名稱。 ● **密碼**– 輸入本地用戶的密碼。

- **確認密碼**– 再次輸入本地用戶的密碼以確認。
- **限用使用者名稱及密碼**–若選定此項，您需要輸入使用者的名稱與密碼。
- **基於時間的一次性密碼(TOTP) -** 請確認路由器的時區是否正確，接著在手機或行動裝置上安裝 Google 驗證 APP，開啟 APP 掃描本頁上的 QR code，您的手機將會顯示出一次性的密碼資訊。

在**驗證碼**中，請輸入密碼並按下**驗證**。

現在，已完成設定。系統將會要求您在輸入使用者名稱及密碼後，另外輸入二階段密碼進行驗證。

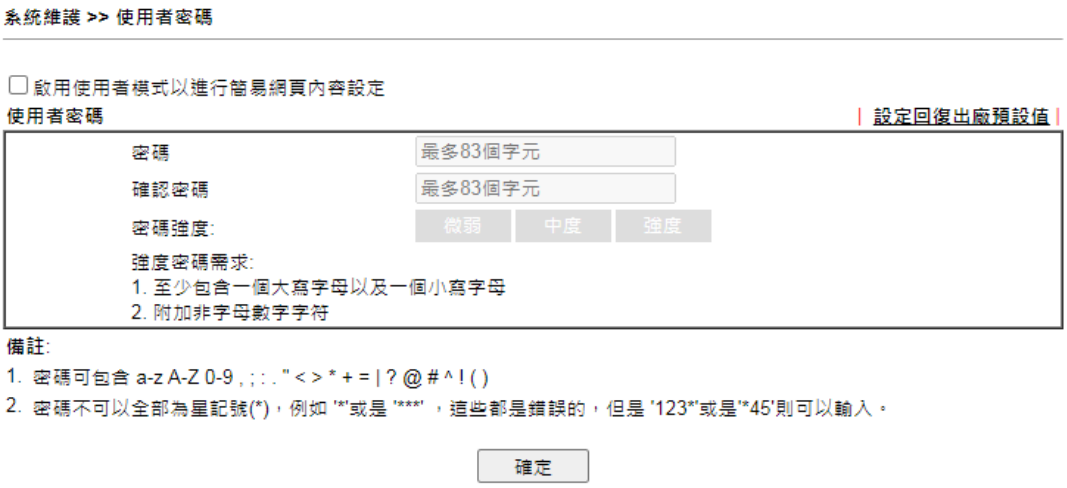


- **行動動態密碼系統(mOTP)** –選擇此項可以使用 mOTP 密碼來登入。輸入 PIN 碼及密鑰設定，以取得一次性密碼。
- **雙重認證，透過簡訊設定檔 與/或 郵件設定檔** –選擇簡訊與/或郵件設定檔，接收者號碼以及/或電子郵件，以便傳輸密碼。
- **當透過 WAN 端登入時，啟用進階驗證方式** – 進階驗證方法提供一個更加安全的網路連線，從 WAN 端登入時，可選擇基於時間的一次性密碼(TOTP) 或是行動動態密碼系統(mOTP)或是雙重認證。
- **新增**– 輸入上述使用者名稱與密碼後，按下此鈕建立新的本地用戶，新的用戶名稱會立即顯示在本地使用者清單上。
- **編輯**– 如果不滿意上述清單內的某個使用者設定，選擇該名稱，進行修正然後按下此**編輯**按鈕即可更新相關設定資訊。
- **刪除**– 如果不滿意上述清單內的某個使用者設定，選擇該名稱，按下此**刪除**按鈕即可移除該使用者名稱。
- **本機使用者清單** – 顯示可管理路由器的使用者清單。

完成設定之後，按下**確定**按鈕儲存相關設定。後續若是離開了網頁設定介面，當您再度登入時，請使用新的密碼。

VI-1-5 使用者密碼

本頁允許您設定新的密碼。



可用設定說明如下：

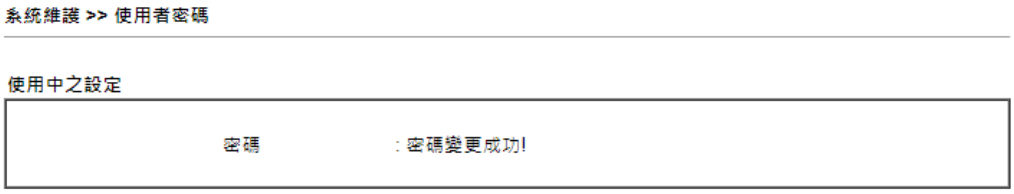
項目	說明
啟用使用者模式進行簡易網頁內容設定	勾選此框之後，您可以透過此處輸入的密碼登入網頁使用者介面，進行簡易設定。 簡易網頁使用者介面的設定項目，與透過管理者密碼登入的完整使用者介面有些不同。
密碼	請在本區輸入新密碼。
確認密碼	再次輸入新密碼以確認。
密碼強度	顯示上述指定的密碼其強度等級為何。
設定回復出廠預設值	按此連結回復出廠預設值。

當您按下**確定**鍵後，登入視窗將會出現，請使用新的密碼以便再次存取網頁設定頁面。

1. 開啟**系統維護>>使用者密碼**。

2. 勾選**啟用使用者模式進行簡易網頁設定**以便啟用使用者模式操作。在**密碼**與**確認密碼**欄位中輸入新的密碼，然後按下**確定**。

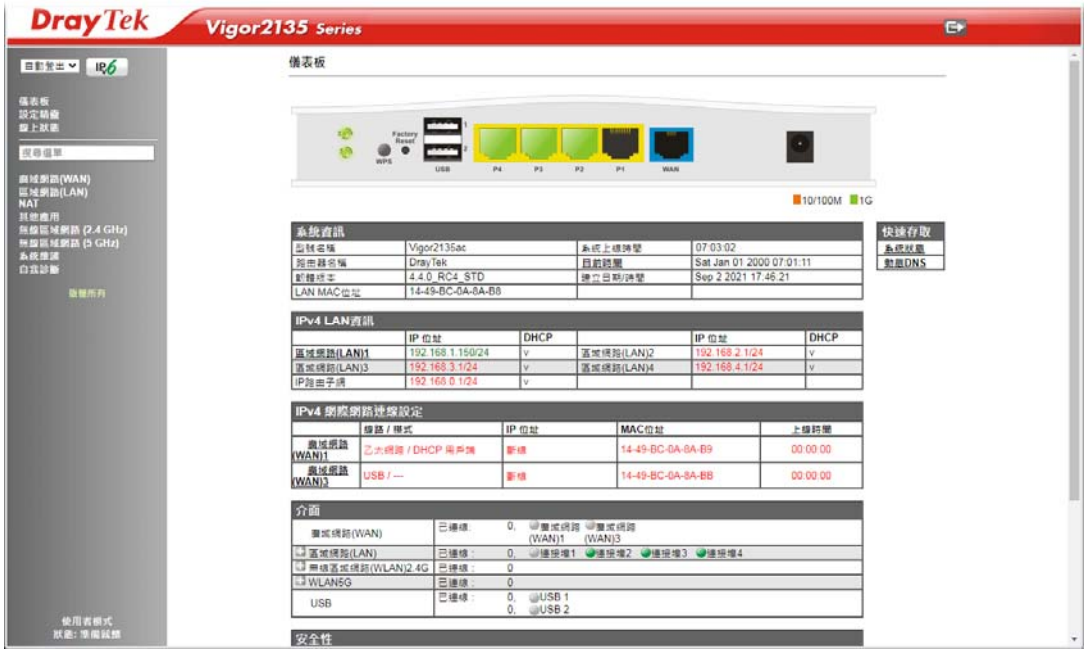
3. 下述畫面顯示出來後，按下**確定**。



4. 按**登出**按鈕離開 Vigor 路由器網頁使用者介面。

5. 接著如下視窗將會開啟要求輸入使用者名稱與密碼，請輸入新的密碼然後按下**登入**。

6. 使用者模式的主要畫面顯示如下：



使用者模式中的設定少於管理者模式，只包含基本設定。

資訊	使用者模式中的設定方式如同管理者模式。

VI-1-6 登入頁面設定

當您想要登入路由器的網頁使用者介面，系統將詢問您提供使用者名稱與密碼，登入視窗網頁的背景是空白且沒有標題在其上，如有需求本頁可讓您在登入視窗中指定登入 URL 以及標題。

可用設定說明如下：

項目	說明
登入頁面標誌	設定登入頁面上方的影像。 **預設值** - **啟用歡迎功能**可讓您設定登入頁面標題。 **空白** - 無影像也無歡迎詞。 **上傳一個檔案** - 選擇一個影像檔案然後按上傳按鈕，之候選定的影像就會顯示在登入頁面的上方。
啟用歡迎功能	勾選此框以便輸入頁面標題。
登入頁面標題	輸入簡短說明(例如 Welcome to DrayTek)使其顯示在登入對話盒的標題上。
歡迎訊息與佈告欄	輸入文字或文句，這些文字將會出現在佈告訊息欄中，此外，也可以顯示登入對話盒的下方。 注意您不可在此輸入 URL 重導向連結。
預覽	按下此連結顯示以本頁設定為基準的登入視窗的預覽畫面。
設定回復出廠預設值	按下此連結回到出廠預設值。

下圖顯示登入頁面範例：

歡迎訊息

This welcome message is displayed in the Login page of the router. Replace this text with your own message.

1. The welcome message can be written in HTML so lists such as this one can be created
2. Other markup tags such as p, font or img can be used

VI-1-7 設定備份

此功能可以將 Vigor2135 上的路由器設定套用至此裝置。

設定備份

請依照下列步驟備份您的路由器設定。

1. 在**系統維護**群組中按**設定備份**，您將可看見如下視窗。

可用設定說明如下：

項目	說明
還原	**選擇檔案/USB 儲存**– 點選此項以指定檔案還原。 **還原設定檔案，但登入密碼除外-** 若是密碼設定不得還原並套用至此裝置，請選擇此項已排除密碼設定。 按下**還原**按鈕還原設定至此裝置，若檔案有加密，系統會詢問您輸入密碼以便解密該設定檔。
備份	按下此按鈕進行設定備份。 **以密碼保護-** 路由器的設定檔可以加密以因應安全性需要。

	備份目前內容至設定檔案 ☑ 以密碼保護 密碼 [最多23個字元] 確認密碼 [最多23個字元] 備註: Only 1-9, A-Z, a-z, and ,;:<>+=|?@#^!() are allowed. [備份] ● **密碼**– 輸入字元以便作為解密設定檔之密碼。 ● **確認密碼**– 再次輸入密碼確認。
自動備份至 USB 磁碟	設定檔可以儲存連接至此裝置的 USB 磁碟上，做為備份設定。 **備份檔案夾**– 設定下載的路徑。 **定期備份**– 設定備份的循環期間。 **變更設定後備份**– 當設定檔一有變更，立刻採取備份動作。
支援的型號清單	來自其他 Vigor 路由器(目前只有 Vigor2135)的網頁設定檔案可以套用到此裝置。 本區顯示此裝置能夠接受的路由器網頁設定檔的型號與韌體等資訊。

2. 按**備份**按鈕進入下一個對話盒，按**儲存**以儲存設定。設定檔將會以檔名**config.cfg**自動下載至電腦上。

上述範例是以 Windows 平臺來完成，對於 **Mac** 或是 **Linux** 平臺的用戶，螢幕上將會出現不一樣的視窗，但是備份的功能仍是有效的。

資訊	憑證備份須以另一種方式來儲存，備份設定並不包含憑證資訊。

還原設定

1. 在**系統維護**群組中按**設定備份**，您將可看見如下視窗。

2. 按**選擇檔案**按鈕選擇正確的設定檔案，以便上傳至路由器。
3. 按**還原**按鈕並等待數秒鐘。

VI-1-8 Webhook

Vigor 路由器會定期向監控服務器寄送包括 WAN 上線、斷線、CPU 使用率、記憶體使用率等報告 (訊息)。

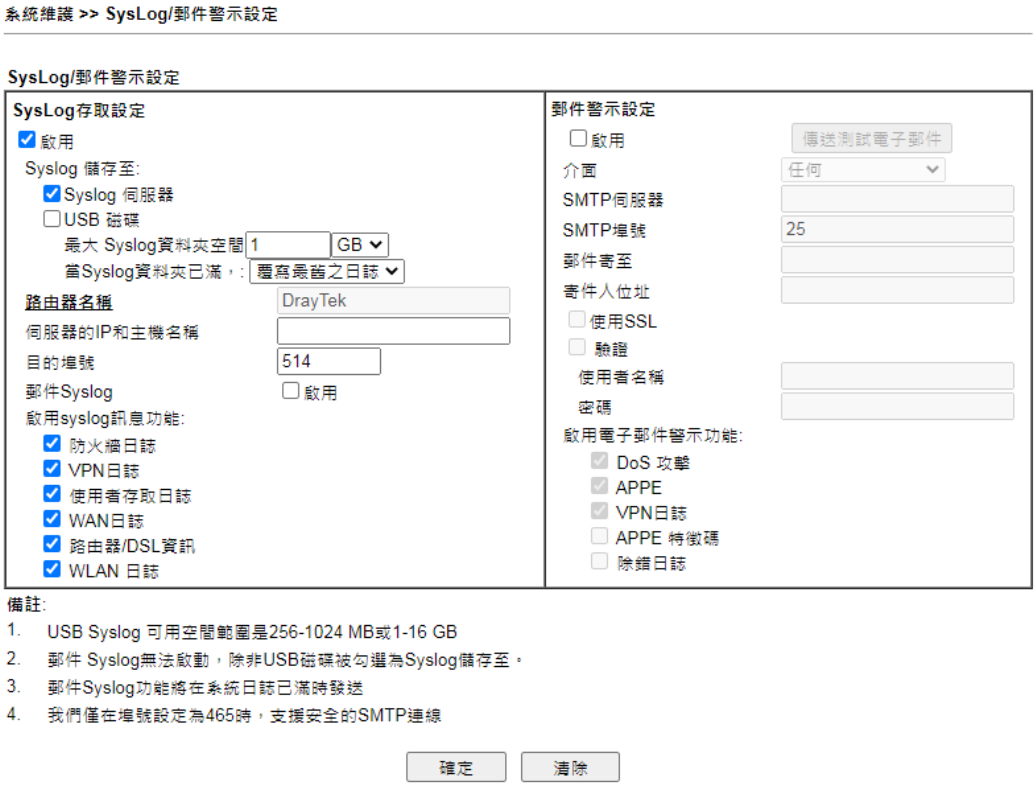
可用設定說明如下：

項目	說明
啟用	勾選此框啟用此功能。
監控伺服器 URL	輸入 URL 做為監控伺服器。
報告期間	定義每份報告傳送的間隔時間。

完成設定之後，按下**確定**按鈕儲存相關設定。

VI-1-9 Syslog/郵件警示設定

如果要監視路由器的運作狀態，您可以執行 SysLog 程式擷取路由器上所有的活動。此程式可以在本機電腦或是網際網路上任一遠端電腦上執行，此外 Vigor 路由器提供郵件警示功能，這樣 SysLog 訊息可以郵件方式打包寄給資訊管理人員。



可用設定說明如下：

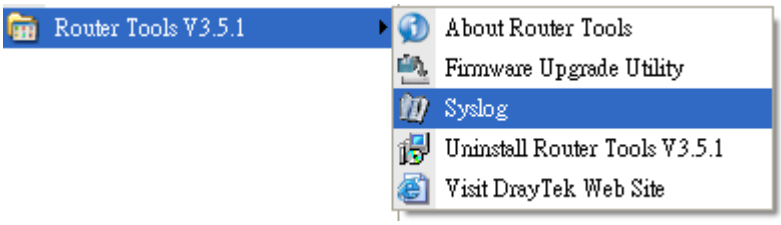
項目	說明
SysLog 存取設定	**啟用-** 勾選**啟用**以啟動系統記錄服務功能/啟動郵件警示功能。 **Syslog 儲存至-** 勾選此框可儲存紀錄至 Syslog 伺服器中。 **USB 磁碟-** 勾選此框可儲存紀錄至 USB 儲存碟中。
路由器名稱	顯示此路由器於**系統維護>>管理**頁面中設定的名稱。 若此處沒有名稱，請至**系統維護>>管理**設定路由器名稱。 **伺服器的 IP 位址和主機名稱-**指定全部系統紀錄訊息傳送前往目的地之 IP 位址。 **目的埠號-**指定全部系統紀錄訊息傳送前往目的地之通訊埠。 **郵件 Syslog-** 勾選**啟用**以便紀錄郵件事件至 Syslog 上。 **啟用 syslog 訊息功能-**勾選此頁面上所列的小方塊，傳送防火牆、VPN、使用者存取、撥號、WAN、路由器/DSL 等資訊紀錄至 Syslog 上。
郵件警示設定	勾選**啟用**以便啟動郵件警示功能。 **傳送測試電子郵件-**執行一個簡單的電子郵件測試，請於下方先指定郵件地址，然後在按此測試鈕，以檢查此電子郵件地址是

	否可用。 **介面** - 指定郵件發送使用的介面。 **SMTP 伺服器/SMTP 埠號** -指定 SMTP 伺服器的 IP 位址，直接傳送來自 Vigor 路由器的郵件至收信人的信箱。 **郵件寄至-**指定收信人信箱的郵件位址，全部的系統紀錄訊息將會自動傳送至此處。收信人可以是想要檢視或是分析系統紀錄訊息的管理人員。 **寄件人位址** - 輸入傳送者的電子郵件位址。 **使用 SSL** - 勾選此框使用埠號 445 確保連線安全性，因為某些伺服器需使用 HTTPS 作為傳輸方法。 **驗證**-當使用電子郵件應用程式，勾選此方塊可啟動驗證的功能。 ● **使用者名稱**-輸入驗證所需的使用者名稱。 ● **密碼**-輸入驗證所需的密碼。 **啟用電子郵件警示功能**-勾選此方塊以便在路由器檢測到相關項目時，自動傳送警告訊息至郵件信箱。

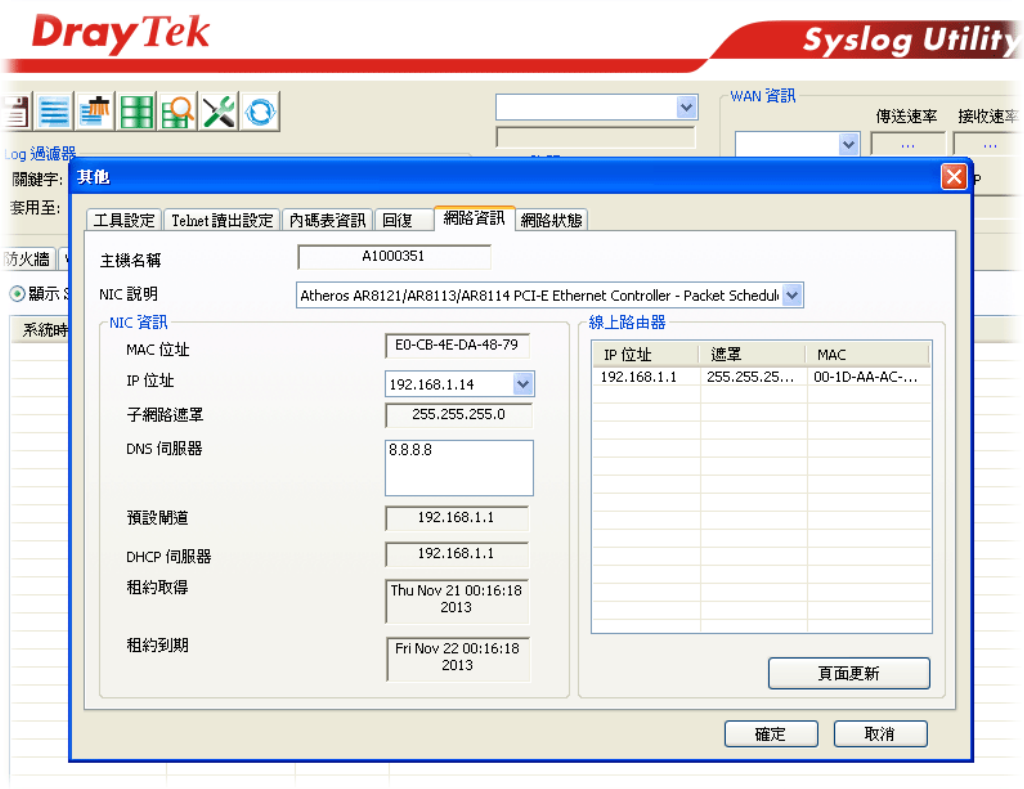
按**確定**儲存所有的設定。

如欲檢視系統紀錄，請依照下述步驟進行：

1. 請在伺服器 IP 地址中設定監視電腦的 IP 地址。
2. 安裝光碟片中 **Utility** 下的路由器工具，安裝完畢後，請自程式集選取 **Router Tools>>Syslog**。

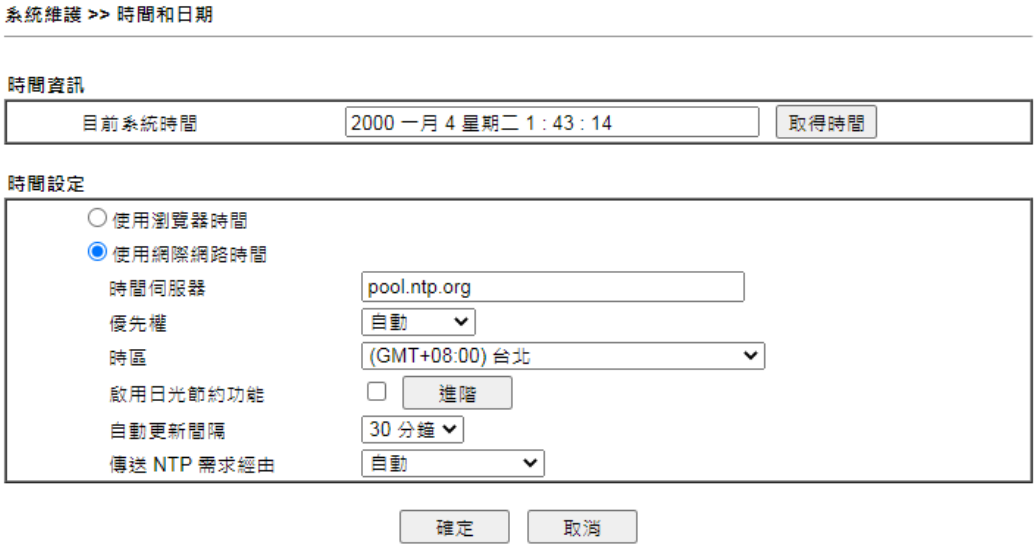


3. 自 Syslog 畫面上，選擇您想要監視的路由器。請記住在網路資訊中，選擇用來連接路由器的網路交換器，否則您無法成功檢索來自路由器的資訊。



VI-1-10 時間和日期

允許您指定自何處取得路由器時間。



可用設定說明如下：

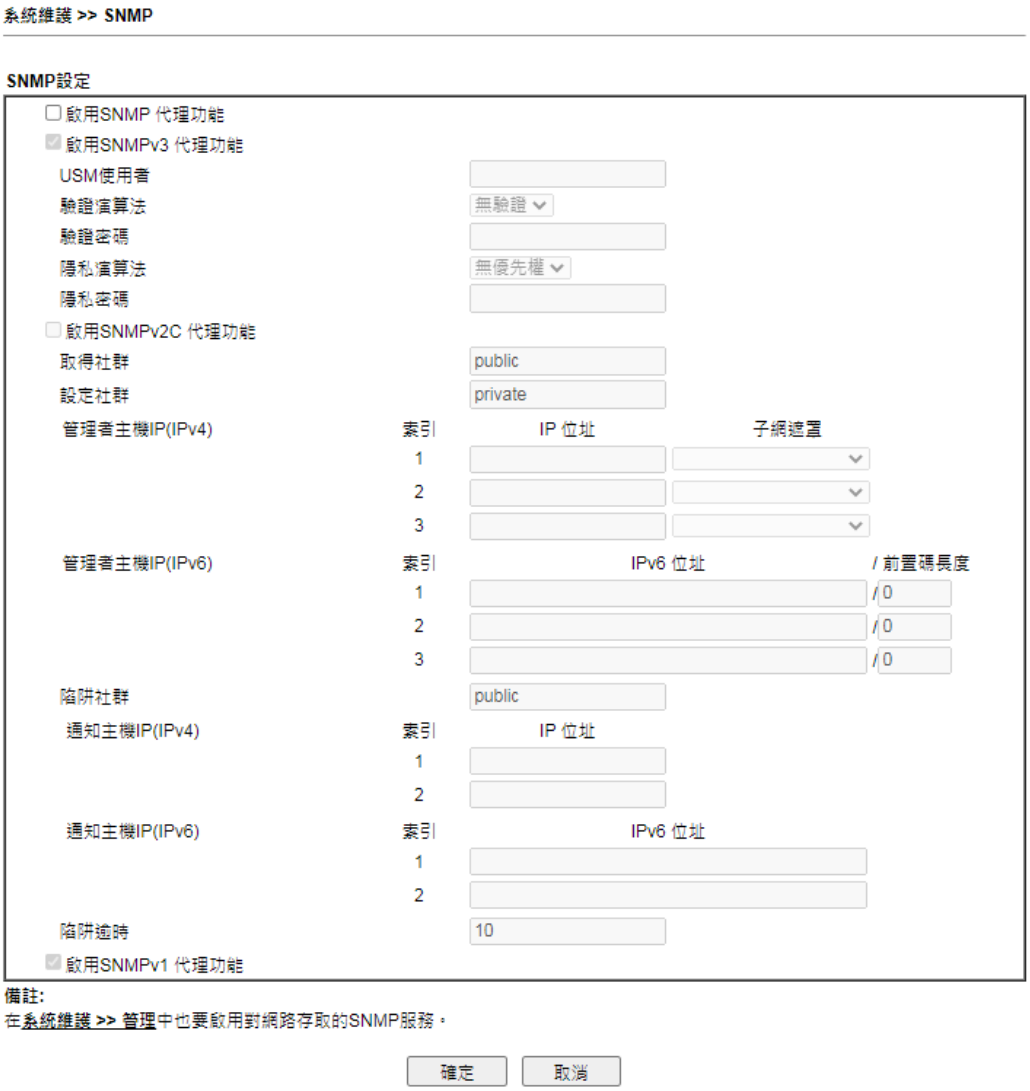
項目	說明
目前系統時間)	按**取得時間**按鈕取得目前時間。
使用瀏覽器時間	選擇此項以便採用遠端管理者電腦上的瀏覽器時間。
使用網際網路時間	選擇此項以便自網際網路上的時間伺服器選擇所需的時間資訊。
時間伺服器	輸入時間伺服器所需的 IP 位址或網址。
優先權	選擇**自動**或是 **IPv6 優先**作為優先選項。
時區	選擇路由器所在的時區。
啟用日光節約功能	勾選此方塊啟動日光節約時間，在某些地區，這個項目是很有用處的。 **進階-** 按此鈕開起如下對話盒。 依照需要使用預設時間設定或是設定使用者定義時間。
自動更新間隔	選定時間間隔以供 NTP 伺服器更新之用。
傳送 NTP 需求經由	指定 WAN 介面已傳送 NTP 需求進行時間同步化。

按**確定**儲存所有的設定。

VI-1-11 SNMP

本頁讓您設定 SNMP 與 SNMP3 服務的相關設定。

因應管理之需，利用加密(AES 與 DES)與驗證(MD5 與 SHA)二種方法，SNMPv3 比 SNMP 提供更安全的服務。



可用設定說明如下：

項目	說明
啟用 SNMP 代理功能	勾選此項以啟動 SNMP 功能，之後再接著啟用 **SNMPv1 代理功能 / SNMPv2C 代理功能 / SNMPv3C 代理功能**。
啟用 SNMPV3 代理功能	勾選此框啟用此功能。 **USM 使用者** - USM 代表使用者為主的安全模式。 輸入做為驗證之用的使用者名稱。 **驗證演算法** - 選擇任一種方式作為驗證演算法。 **驗證密碼** - 輸入驗證需求的密碼。 **隱私演算法** - 選擇下列任一種方式作為隱私演算法。

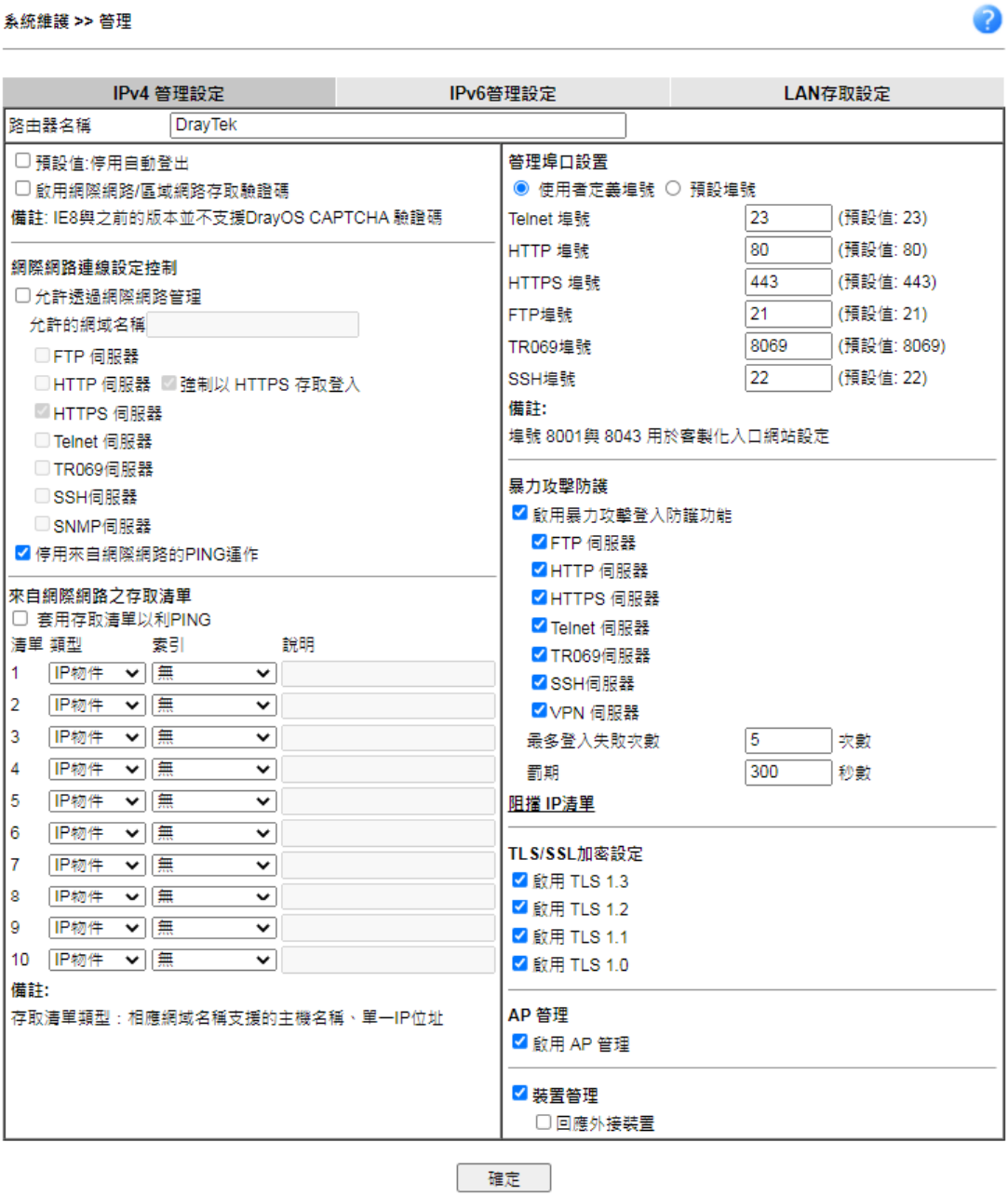
	隱私密碼 - 輸入隱私需求的密碼。
取得社群	請輸入適當的文字以設定取得社群名稱，預設名稱為 **public。**
設定社群	請輸入適當的名稱以設定社群，預設名稱為 **private**。
管理者主機 IP (IPv4)	設定一台主機做為管理者以便執行 SNMP 功能，請輸入 IP 位址(IPv4)指定特定主機。
管理者主機 IP(IPv6)	設定一台主機做為管理者以便執行 SNMP 功能，請輸入 IP 位址(IPv6)指定特定主機。
陷阱社群	輸入適當名稱設定陷阱社群，預設名稱為 **public**。
通知主機 IP(IPv4)	設定主機的 IP 位址(IPv4)接收封鎖社群的資料。
通知主機 IP (IPv6)	設定主機的 IP 位址(IPv6)接收封鎖社群的資料。
陷阱逾時	預設值為 10 秒。

按**確定**儲存所有的設定。

VI-1-12 管理

本頁讓您管理存取控制、存取清單以及通訊埠設定。例如管理存取控制時，埠號用來傳送/接收 SIP 訊息以便建立連線。

針對 IPv4



可用設定說明如下：

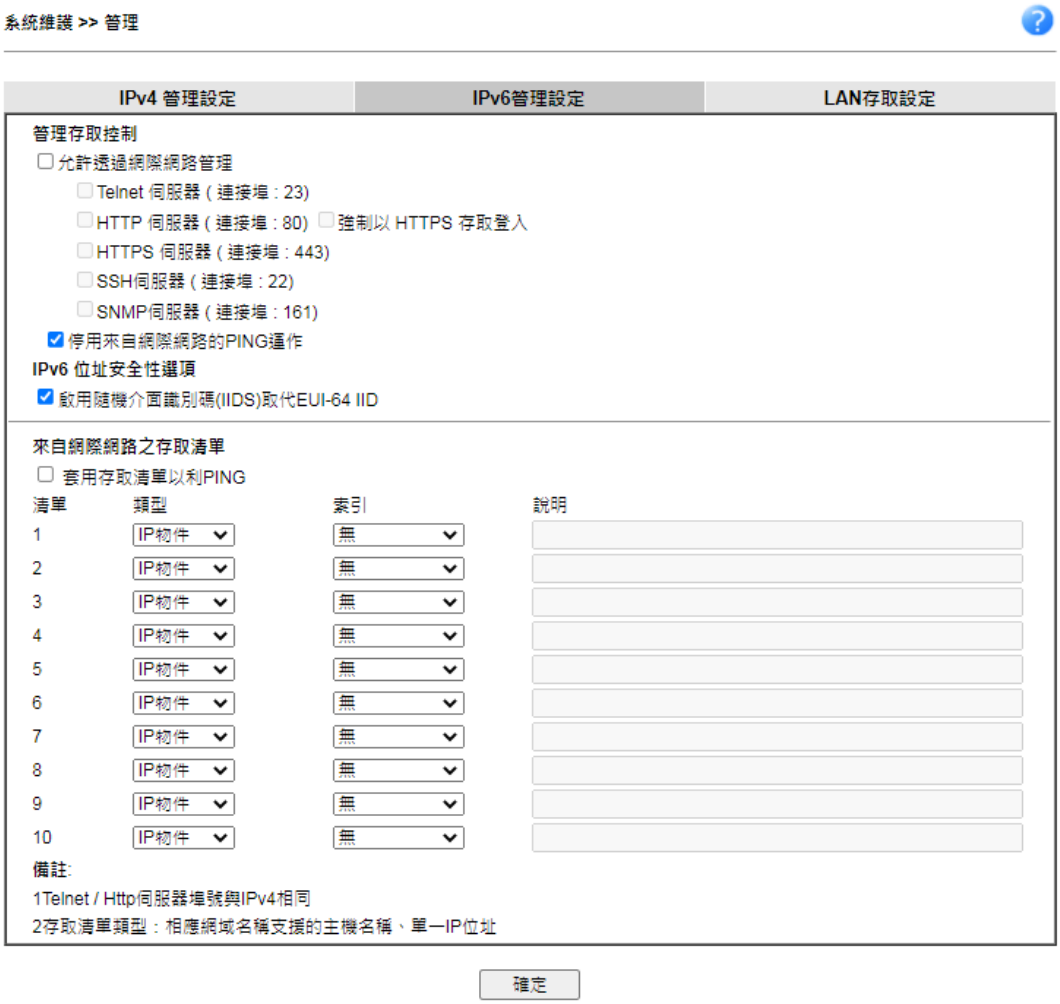
項目	說明
路由器名稱	輸入路由器的名稱。
預設值：停用自動登出	若勾選此框，自動登出功能將被停止使用。

	 網頁使用者介面將會持續開啟直到按下手動登出為止。
啟用網際網路/區域網路存取驗證碼	若啟用此功能，路由器將會提供驗證代碼。用戶必須輸入此代碼才能獲准登入網際網路或是路由器的網頁使用者介面。
網際網路連線設定控制	**允許透過網際網路管理**-勾選此方塊允許系統管理者自網際網路登入。系統提供數種不同的伺服器供您選擇作為網路管理介面，請勾選所需的項目。 **停用來自網際網路的 PING 運作** -勾選此方塊以退回所有來自網際網路的 PING 封包，考量到安全性問題，這項功能的預設值是啟動的。
來自網際網路之存取清單	系統管理者登入路由器的網頁設定介面最多可限制 10 個特定主機或網路。 **套用存取清單以利 PING** – 當**停用來自網際網路的 PING 運作**未勾選，但勾選了此功能時，只要 IP 位址或是子網遮罩如下所設定，系統就會接受來自網際網路端的 PING 動作。不過當勾選了**停用來自網際網路的 PING 運作**項目時，這個選項功能就不會有任何做效用，所有的 PING 運作都會被阻擋在外。 **類型** -請選擇 **IP 物件**。 **索引** - 自下拉式清單中選擇預先設定的 IP 物件。 **說明** - 顯示選定物件的註解內容。
管理埠口設置	**使用者定義埠號-**勾選此項以指定使用者定義的埠號作為各個伺服器之用。 **預設埠號-**勾選此項讓各個通訊協定使用標準埠號。
暴力攻擊防護	任何一個嘗試利用 Vigor 路由器登入網際網路使用者都會被要求必須通過使用者驗證程序。此功能可以讓路由器不會受到駭客使用各種字元直到發現正確的密碼組合而發動的網路攻擊。 **啟用暴力攻擊登入防護功能** – 勾選此框啟用此功能。 **最多登入失敗次數** – 用戶使用密碼登入，系統所能容忍的最多錯誤次數。 **罰期** – 設定一段時期以便封鎖不斷嘗試通過使用者驗證但卻一再失敗的 IP 位址。當到達指定時間，路由器系統將會解所該 IP 並讓人重新使用該 IP 登入 Vigor 路由器。 **阻擋 IP 清單** – 開啟另一個網頁顯示目前被封鎖的 IP 清單。
TLS/SSL 加密設定	**啟用 TLS 1.0/1.1/1.2/1.3 -** 勾選此框啟用 **TLS 1.0/1.1/1.2/1.3** 功能。 鑒於安全考量，路由器內建 HTTPS 伺服器已經更新至 TLS1.x 協定。

AP 管理	**啟用 AP 管理** – 勾選此框啟用**中央管理>>無線基地台(AP)**功能，若未勾選，**中央管理>>無線基地台(AP)**相關的設定選單將會隱藏起來。
裝置管理	勾選此框啟用裝置管理功能。 **回應外接裝置-** 若勾選此項，路由器將被視為次要(slave)裝置，當外接裝置(主要裝置)傳送需求封包至路由器的時候，路由器將回傳資訊以回應外接裝置(可管理路由器)的詢問。

全部設定完成之後，請按**確定**儲存目前的設定。

針對 IPv6



可用設定說明如下：

項目	說明
管理存取控制	**允許透過網際網路管理-** 勾選下述方框可讓系統管理者自網際網路登入此路由器設定介面，有數種伺服器可以選擇讓您來管理。 **停用來自外部網際網路的 PING 運作-** 勾選此方框可讓系統停止接受來自外部網際網路的封包檢測。
IPv6 位址安全性選項	**啟用隨機介面識別碼(IIDs)取代 EUI64 ID -** IPv6 位址將會隨機產生但是並未使用 LAN/WAN MAC，以防止駭客的攻擊。

來自網際網路之存取清單	系統管理者登入路由器的網頁設定介面最多可限制 10 個特定主機或網路。 **套用存取清單以利 PING** – 當**停用來自網際網路的 PING 運作**未勾選，但勾選了此功能時，只要 IPv6 位址或是子網遮罩如下所設定，系統就會接受來自網際網路端的 PING 動作。不過當勾選了**停用來自網際網路的 PING 運作**項目時，這個選項功能就不會有任何做效用，所有的 PING 運作都會被阻擋在外。 **類型** - 請選擇 **IPv6 物件**。 **索引** - 自下拉式清單中選擇預先設定的 IP 物件。 **說明** - 顯示選定物件的註解內容。

全部設定完成之後，請按**確定**儲存目前的設定。

針對 LAN

可用設定說明如下：

項目	說明
允許透過 LAN 端管理	勾選下述方框可讓系統管理者自 LAN 端登入此路由器設定介面，有數種伺服器可以選擇讓您來管理。
套用至子網	您可以指定系統管理者可以使用的 LAN 介面以便登入網頁使用者介面。 **於 IP 物件的索引編號** - 勾選前面的方框，然後於長條欄位中輸入 IP 物件的索引編號，要注意該物件所選擇的 IP 位址類型不可以是任何位址。

全部設定完成之後，請按**確定**儲存目前的設定。

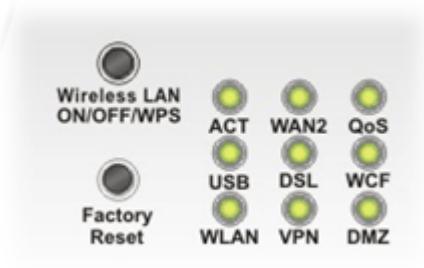
VI-1-13 面板控制

路由器前面板的 LED、按鈕、USB 埠口以及 LAN 埠口的行為可以視實際需要調整開與關。

對於 LED

所有的 LED 在預設的情況下都是開啟的，也會持續的閃爍來顯示路由器各種功能的運作狀態。不過，這些 LED 燈號可以設定為關閉狀態，直到按壓某個按鈕來喚醒燈號。

可用設定說明如下：

項目	說明
更新頁面	按此連結更新此頁面以顯示最新的訊息。
啟用 **LED** 功能	請勾選此項以便啟用前面板的 LED 燈號。 ● **啟用睡眠模式/在經過__分鐘後，關閉 LED** – 當勾選了啟用 LED 後，請選擇此項目並且設定需要的時間以便關閉 LED 燈號。 ● 當睡眠模式啟用時，可以利用按壓 **Wireless LAN ON/OFF/WPS** 按鈕，或前面板的 **Factory Reset** 按鈕，或是此頁面的**喚醒 LED** 按鈕來喚醒燈號。而當 LED 燈號亮起時，只要按下 **Factory Reset** 按鈕或是此頁面的 **LED 立即睡眠**按鈕，就可以再度關閉 LED 燈號顯示。 
狀態	顯示 LED 燈號狀態。

	狀態：睡眠 喚醒LED – LED 全都處於睡眠模式下，如果要喚醒燈號，可採取如下方式： ● 按下本頁面上的**喚醒 LED** 按鈕 ● 按下路由器前面板的 **Wireless On/Off/WPS** 按鈕 ● 按下路由器前面板的 **Factory Reset** 按鈕 狀態：喚醒，睡眠在 1 分鐘 LED立即睡眠 – LED 已被喚醒，如果要熄燈號，可採取如下方式： ● 按下本頁面上的 **LED 立即睡眠**按鈕 ● 按下路由器前面板的 **Factory Reset** 按鈕 1 秒鐘

全部設定完成之後，請按**確定**儲存目前的設定。

對於按鈕

路由器前面板的 **Factory Reset** 與 **Wireless ON/OFF/WPS** 按鈕，預設值皆是啟用的，且若有需要可以將其停用。停用出廠預設值(Factory Reset)按鈕可防止被未授權的人竄改，或是防止按鈕用來喚醒 LED 時意外觸發路由器系統重啟。停用無線按鈕可在 LED 睡眠模式啟用時，防止變動到無線網路設定，這二個按鈕基本上都可以用來喚醒/熄滅 LED 燈號。

按下**按鈕**標籤開啟如下頁面。

可用設定說明如下：

項目	說明
更新頁面	按此連結更新此頁面以顯示最新的訊息。
啟用出廠預設值按鈕	預設值是啟用的(勾選)。 取消勾選可以停用出廠預設值的系統重啟功能。 停用此按鈕僅可防止其被用來重新啟動路由器，按鈕仍然可以用來喚醒前面板的 LED 燈號(當 LED 睡眠模式啟用時)。
啟用無線網路按鈕	預設值是啟用的(勾選)。 取消勾選可以停用無線網路按鈕控制 WLAN 與 WPS 功能的能

	力。 停用此按鈕僅可防止其被用來控制 WLAN 功能，按鈕仍然可以用來喚醒前面板的 LED 燈號(當 LED 睡眠模式啟用時) 。

全部設定完成之後，請按**確定**儲存目前的設定。

對於 USB

USB 埠口可以個別啟用或是停用，當停用 USB 埠口的時候，路由器將無法辨認其上接的裝置。

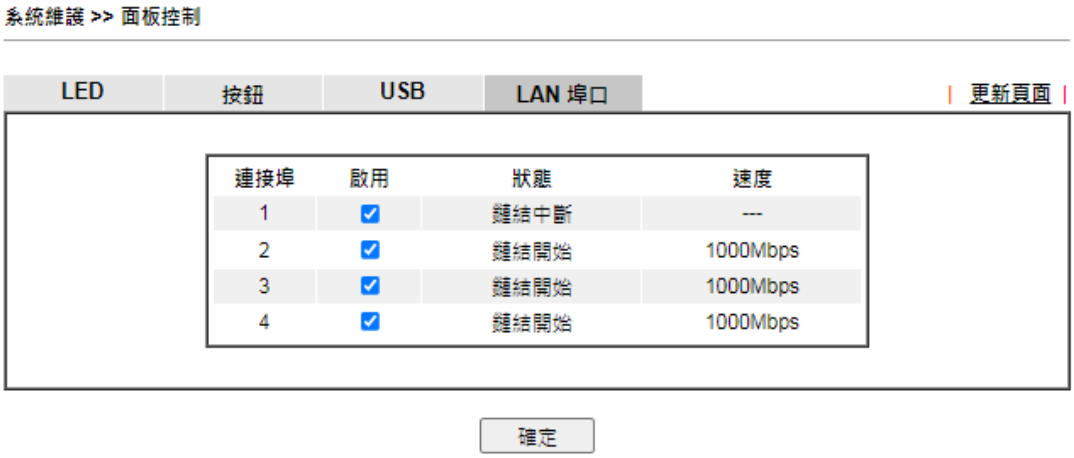
可用設定說明如下：

項目	說明
更新頁面	按此連結更新此頁面以顯示最新的訊息。
連接埠	代表前面板顯示的 USB 埠口(1/2)。
啟用	取消勾選可以停用 USB 埠口，預設值是啟用的。
狀態	顯示 USB 埠口的狀態。 **無裝置** – 沒有 USB 裝置插入該埠口。 **已連接** – 有 USB 裝置插入該埠口。 **---** – USB 埠口已停用。

全部設定完成之後，請按**確定**儲存目前的設定。

對於 LAN 埠口

LAN 埠口可以個別啟用或是停用，當停用 LAN 埠口的時候，路由器將無法辨認其上接的裝置。



可用設定說明如下：

項目	說明
更新頁面	按此連結更新此頁面以顯示最新的訊息。
連接埠	代表前面板顯示的 LAN 埠口(1/2/3/4)。
啟用	取消勾選可以停用 LAN 埠口，預設值是啟用的。
狀態	顯示 LAN 埠口的狀態。 **鏈結開始** – 表示目前有乙太網路裝置連接至該埠口。 **鏈結中斷** – 表示目前尚未偵測到乙太網路裝置。 **---** – 顯示 USB 埠口的狀態。
速度	顯示 LAN 埠口的協商速度。 **1000Mbps** – LAN 埠口的協商速度為 1000 Mbps。 **100Mbps** – LAN 埠口的協商速度為 100 Mbps。 **10Mpbs** – LAN 埠口的協商速度為 10 Mbps。 **---** – LAN 埠口已停用或是沒有任何裝置連接上。

全部設定完成之後，請按**確定**儲存目前的設定。

VI-1-14 自行簽核憑證

自行簽核憑證是裝置(如 Vigor 路由器)的獨特身分辨識，是由裝置自行產生的憑證以確保路由器的安全性，此自行簽核憑證是以路由器擁有的私鑰來自行簽署。

自行簽核憑證可套用在 SSL VPN, HTTPS 等等，此外，此憑證可以透過各種工具免費產生。

系統維護 >> 自行簽核憑證

自行簽核憑證資訊

憑證名稱：	self-signed
發行人：	C=TW, ST=HsinChu, L=HuKou, O=DrayTek Corp., OU=DrayTek Support, CN=Vigor Router
主體：	C=TW, ST=HsinChu, L=HuKou, O=DrayTek Corp., OU=DrayTek Support, CN=Vigor Router
主體替代名稱：	DNS:www.draytek.com
效期自：	Aug 11 15:25:24 2021 GMT
有效至：	Sep 10 15:25:24 2022 GMT
PEM 格式內容：	-----BEGIN CERTIFICATE----- MIIDpjCCAo6gAwIBAgIJAJnOuRT3dPm8MA0GCSqGSIb3DQEBCwUAMHgxCzAJBgNV BAYTAlRXMRAwDgYDVQQIDAdIc2luQ2h1MQ4wDAYDVQQHDAVIdUtvdTEWMBQGA1UE CgwNRHJheVRlayBDb3JwLjEYMBYGA1UECwwPRHJheVRlayBTdXBwb3J0MRUwEwYD VQQDDAxWaWdvciBSb3V0ZXIwHhcNMjEwODExMTUyNTI0WhcNMjIwOTEwMTUyNTI0 WjB4MQswCQYDVQQGEwJUVzEQMA4GA1UECAwHSHNpbkNodTEOMAwGA1UEBwwFSHVL b3UxFjAUBgNVBAoMDURyYXlUZWsgQ29ycC4xGDAWBgNVBAsMD0RyYXlUZWsgU3Vw cG9ydDEVMBMGA1UEAwwMVmlnb3IgUm91dGVyMIIBIjANBgkqhkiG9w0BAQEFAAOC AQ8AMIIBCgKCAQEAzRPQIBezQp4PdiUpQ8ZDJiF3tTiJmfLRTVOcmZWYWr6KDX1C CD5Qv0zko56k7bGYjp2Vk/caj4TO5DDh2galmQHEA5/v3iHB6mDCY9nF0LnTsnW6 0fOj6F//HY5zRyAHjBVkjJLGmjr7YEL1PXF6sF4PaB3Ax1dDQQwMH8WQY98DdTSN cVCngKFkJF/Tm/wF0OoRlYZuknujhJlRfP8MIWqOQg5xBSGMAnOLXEj3APJVcLnJ v+v444WLIMQVx1LzpVKfW+S5arQbQ6qQDcEuguL5VP3FBlJ0IwVXZw4Y+eA7HtHL qRkXKPbPuAigaW1aLfaZ4EeF1/26N6tr2+/OUQIDAQABozMwMTATBgNVHSUEDDAK BggrBgEFBQcDATAaBgNVHREEEzARgg93d3cuZHJheXRlay5jb20wDQYJKoZIhvcN AQELBQADggEBAEm0Y1SEJd7pf+O1iUxqwt64CgV3WEnlslNIBuCvjzjFBWbdwJ+B RkkebsGbyrk+HTVgGgDC8i3CHKYpA85X0MLPOxFtwhJ50YC84EIss63yzV8P5FKk c+ZJqtJD0dJ4AnbFPCumJH0r1iIvQ4myhS1ATS1IW8VoeFirqYovUR347hAeDNL1 gnzWWw2VPdo/epKASaIrRCqzCZYFWsqbf6ucr0jWHbj73xA88NxxOeywowI0TxGB RqQ1X8J5XGT+abCKE7GUUmeyKu23zge8Xe8872BpY80n+Fu8sFJp2fRP5tz/1iot sec6daBUUScM5P4VMiVeDU7EY0Uaqe+Ad9M= -----END CERTIFICATE-----

備註:

1. 在嘗試重新生成自行簽核憑證之前，請在系統維護 >> 時間和日期設定好正確時間！！
2. 時區必須正確設置!!

重新產生

按下**重新產生**按鈕開啟**重新產生自我簽核憑證**視窗，接著輸入所有相關的資訊，後續按下**產生**即可。

系統維護 >> 重新產生自行簽核憑證

重新產生自行簽核憑證

憑證名稱	自行簽核
主體替代名稱	
類型	IP 位址
IP 位址	
主體名稱	
國家	
州(ST)	
位置	
組織(O)	
組織單位(OU)	
常見名稱 (CN)	
電子郵件(E)	
金鑰種類	RSA
金鑰大小	2048 位元

產生

VI-1-15 重啟路由器

此頁面可用來重新啟動路由器，請自**系統維護**中按**重啟路由器**開啟如下頁面。

排程設定檔 - 您可以輸入四組排程設定檔進行系統重啟作業，所有的排程都可以在**其他應用>>排程**頁面中先行設定。

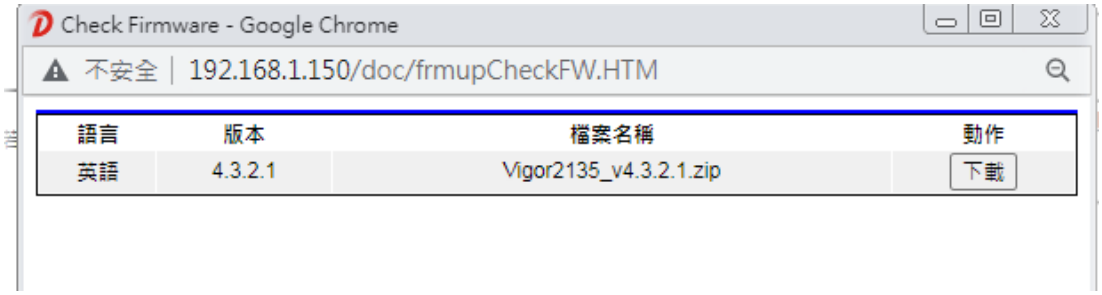
如果您想要使用目前的設定來重新啟動路由器，請勾選**使用目前設定內容**，然後按**立刻重啟**；如果要重設路由器設定回復成為預設值，請勾選**使用出廠預設值**，然後按**立刻重啟**，路由器將會花 5 秒重新啟動系統。

資訊	當系統在您完成網頁設定並跳出**重啟路由器**網頁後，請務必按下**立刻重啟**以重新啟動路由器，這個動作可以確保系統的操作正常，且可避免未來發生不預期的錯誤。

VI-1-16 韌體升級

請自**系統維護**選擇**韌體升級**以便啟動韌體更新工具。

按下**最新韌體細節內容**按鈕，系統會跳出視窗顯示此路由器目前最新的韌體版本為何。



按**下載**將檔案儲存至硬碟中。之後在網頁韌體升級區域中，按下**選擇檔案**挑選您剛下載的檔案，接著按**升級**，系統將會自動更新路由器韌體。

VI-1-17 韌體備份

路由器韌體可以儲存在電腦主機做為備份韌體，之後若路由器因韌體錯誤而造成毀損，就可套用此備份韌體讓路由器恢復正常運作。

可用設定說明如下：

項目	說明
自動韌體還原	**啟用自動韌體還原功能-** 若勾選了此項，當路由器意外的重新啟動達三次時，路由器將以最新備份的韌體檔案直接還原。
備份設定	備份的方式有： ● **重新啟動後備份 -** 路由器在重新啟動之後，會立刻將目前使用的韌體製作備份。 ● **系統上線… -** 路由器在重新啟動後經過一段時間，會立刻將目前使用的韌體製作備份。 ● **手動備份 -** 路由器不會自動將目前使用的韌體製作備份。按下此項並按下**確定**之後，系統才會進行韌體備份。 **備份韌體 -** 顯示目前備份韌體版本。 **上次備份 -** 顯示最近一次備份韌體時間。

請指定備份條件運作韌體備份，然後按下**確定**按鈕儲存設定。

VI-1-18 儀表板控制

儀表板上可以顯示九組設定資訊供管理員/使用者參考。除前面板和系統資訊外，如有必要，可以隱藏本頁列出之群組有關的設定訊息。

VI-2 頻寬管理

頻寬管理

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。為瞭解決這種問題，您可以使用連線數限制來限制指定主機的連線數。

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。

服務品質(QoS)

QoS (Quality of Service)管理部署可確保所有應用程式能夠接收到所需的服務以及足夠的頻寬，符合用戶所期待的效果，此項控制對現代企業網路來說是相當重要的觀點。

使用 QoS 的理由之一是很多 TCP 為主的應用程式嘗試不斷增加其傳輸速率，導致消耗掉全部的頻寬，我們稱之為 TCP 慢速啟動。如果其他的應用程式未受 QoS 的保護，那麼他們在擁擠的網路中將會降低效能，對那些無法忍受任何損失、延遲的功能像是 VoIP、視訊會議以及流動影像來說，這項控制尤其必要。

另一個理由是由於網路的擁擠狀況，內部連線迴路速度不符合或是傳輸流量過份聚集，資料封包排隊等候傳送，整個傳輸慢了下來。如果沒有定義後先後順序，以指定在滿檔的隊伍中哪個封包必須丟棄，上述提及的應用程式封包就可能成為被捨棄掉的一個，這樣的話對應用程式的成效會造成令人無法想像的後果。

在基本設定中有二個元件要注意：

- 分類: 可辨識低潛在因素或是重要的應用程式，並標示這些程式為高優先權服務等級，以便在網路中能夠強迫執行。
- 排定計畫: 以服務等級分類為基礎來指定封包排列順序以及整合的服務型態。

基本 QoS 應用是以 IP 封包頭中之服務類型資訊為基礎來分類及規劃封包，例如爲了確保封包頭之連線，電信工作人員在執行大量運作時，可能會強迫一個 QoS 控制索引保留頻寬予 HTTP 連線。

Vigor 路由器作為 DS 管理之終端路由器，應該檢查通過流量之 IP 封包頭中標記 DSCP 之數值，這樣才可分配特定資源數量來執行適當政策、分類或是排程。網路骨幹之核心路由器在執行動作前也會做同樣的檢查，以確保整個 QoS 啟動之網路中服務等級保持一致性。

APP QoS

APP QoS 允許在通訊協定和程式應用中運用 QoS。

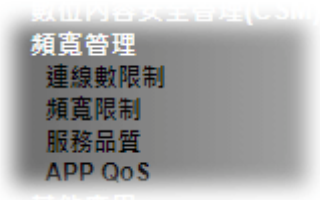
通訊協定與應用程式可分成二大類：可追蹤的與無法追蹤的。

可追蹤的應用程式代表 100%的流量都可被路由器追蹤，所以可各別分配至特定的 QoS 類別。

而無法追蹤的應用程式可能只能在和遠端主機建立連線時被偵測出來，所以和本機之間的全部流量都只能使用相同的 QoS 類別。

網頁使用者介面

下圖是頻寬管理的設定項目:



VI-2-1 連線數限制

在**頻寬管理**群組中，按**連線數限制**開啟如下的網頁。

如果要啟動限制連線數的功能，只要在此頁面上按**啟用**鈕，並設定預設的連線數限制即可。

可用設定說明如下：

項目	說明
連線數限制	**啟用** - 按此鈕啟動連線數限制功能。 **停用** - 按此鈕關閉連線數限制功能。 **預設最大連線數** - 定義區域網路中每台電腦的預設連線數。
限制清單	顯示網頁中所設定的指定限制之電腦清單資料。

指定限制	**起始 IP** - 定義限制連線數的起始 IP 位址。 **結束 IP** - 定義限制連線數的結束 IP 位址。 **最大連線數** - 定義指定 IP 位址的範圍中可用的連線數，如果您沒有在此區設定連線數，系統將會使用此機種所支援之預設連線數。 **新增** - 新增指定連線數限制並顯示在上面的框框中。 **編輯** - 允許您編輯選定的連線數設定。 **刪除** - 刪除限制清單上任何一個您所選定的設定。
管理訊息	請輸入系統允許的網路連線數屆滿時，顯示在螢幕上的文字。 **預設訊息** - 按下此鈕可以直接使用路由器預設的訊息並顯示在管理訊息框內。
時間排程	您可以選擇四組時間排程，所有的排程都可在**其他應用-排程**網頁上事先設定完畢，然後在此輸入該排程的對應索引號碼即可。

完成設定之後，按下**確定**按鈕儲存相關設定。

VI-2-2 頻寬限制

在**頻寬管理**群組中，按**頻寬限制**開啟如下的網頁。

如果要啟動限制頻寬的功能，只要在此頁面上按**啟用**鈕，並設定預設的上下行資料傳送限制即可。

可用設定說明如下：

項目	說明
啟用/停用	**啟用** - 按此鈕啟動限制頻寬功能。 **停用** - 按此鈕關閉限制頻寬功能。 **IP 路由子網** – 勾選此方塊套用頻寬限制至**區域網路>>基本設置定**中所指定的 IP 路由子網。 **預設限制值(每個使用者)** ● **傳送限制** - 定義區域網路中每台電腦預設的上行速度。 ● **接收限制** - 定義區域網路中每台電腦預設的下行速度。
限制清單	顯示網頁中所設定的指定限制之電腦清單資料。
新增項目	**IP 範圍** – 範圍內所有的 IP 都會受限於下方定義的傳送限制與接收限制。 ● **起始 IP** - 定義限制頻寬的起始 IP 位址。

	● **結束 IP** - 定義限制頻寬的結束 IP 位址。 **IP 物件** – 選定 IP 物件或是 IP 群組設定檔內的全部 IP 都會受限於下方定義的傳送限制與接收限制。 ● **IP 群組** - 使用下拉式清單指定一個 IP 群組。 ● **IP 物件** - 使用下拉式清單指定一個 IP 物件。 **每一個/共享 -** 選擇 Each 讓起始 IP 與結束 IP 範圍內的每個 IP 都能享有傳送限制與接收限制中所定義的速度；選擇 **Shared** 則讓範圍內的 IP 共用傳送限制與接收限制的全部頻寬。 ● **傳輸限制** - 定義上行傳送的速度限制，如果您未在此區設定限制的話，系統將使用您在每個索引內容中索引中所預設的限制速度。 ● **接收限制** - 定義下行傳送的速度限制，如果您未在此區設定限制的話，系統將使用您在每個索引內容中索引中所預設的限制速度。 **新增** - 新增指定速度限制並顯示在上面的框框中。 **編輯** - 允許您編輯選定的限制設定。 **刪除** - 刪除限制清單上任何一個您所選定的設定。
自動調整	**當出現可用的頻寬時，允許使用者利用更多頻寬-**路由器將會檢查是否保留足夠的頻寬，依照使用者所設定的頻寬限制而定。如果足夠的話，路由器將會調整可用的頻寬給予使用者使用，以便提升整體的效能。
聰明頻寬限制	勾選此框即可由系統自動控制頻寬。 **套用下述限制至未列入限制清單中的使用者，當使用者超過連線數 ...** - 運用聰明頻寬限制前，允許區域網路用戶所能使用的連線數限制。 **傳送限制** - 定義上傳速度限制，如果沒有設定限制值，系統將會使用預設的速度。 **接收限制** - 定義下載速度限制，如果沒有設定限制值，系統將會使用預設的速度。
時間排程	您可以設定四組時間排程，所有的排程都可在**其他應用-排程**網頁上事先設定完畢，然後在此輸入該排程的對應索引號碼即可。

完成設定之後，按下**確定**按鈕儲存相關設定。

VI-2-3 服務品質

在**頻寬管理**群組中，選擇**服務品質**開啟如下的網頁。

可用設定說明如下：

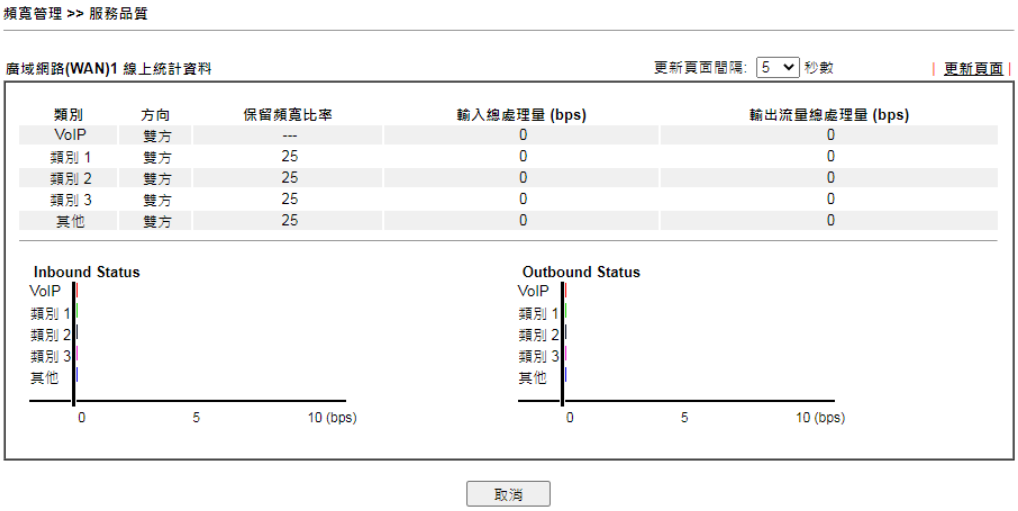
項目	說明
硬體 QoS 基本設置	使用硬體 QoS 之前，請先啟用**硬體加速**功能。 **索引**－顯示 WAN/LAN 介面的編號。 **啟用** － 勾選方框啟用 WAN/LAN 介面之 QoS 功能，如果啟用此功能，您可以針對每個介面設定基本 QoS 設定。 ● **方向** － 僅套用 QoS 至傳出封包流量。 ● **對外頻寬** －WAN/LAN 介面的傳出頻寬設定值。 ● **類別 1/類別 2/類別 3/其他**–每個類別的所佔的頻寬比例。 ● **狀態**－按此開啟線上統計頁面，顯示 WAN/LAN 介面的統計數據。

項目	說明
軟體 QoS 基本設置	**索引** – 顯示 WAN 介面的編號。 **啟用** – 勾選此框啟用 WAN/LTE 介面的 QoS 功能。若啟用，您可設定每個 WAN/LTE 介面的基本 QoS 設定。 ● **方向** – 設定 QoS 套用的流量方向 - **輸入** - 套用 QoS 至傳入封包流量。 - **輸出** - 套用 QoS 至傳出封包流量。 - **雙向** - 套用 QoS 至傳入及傳出封包流量。 ● **對內/對外頻寬**–該 WAN 介面的傳入傳出頻寬設定值。 ● **類別 1/類別 2/類別 3/其他**–每個類別的所佔的頻寬比例。 **狀態** – 按此開啟線上統計頁面，顯示 WAN 介面的統計數據。
類別規則	定義及列出類別規則。 **索引** – 顯示您可以編輯的類別編號。 **啟用** - 顯示此類別規則之狀態。 **QoS 類別** - 顯示 QoS 類別等級。 **本機位址** - 顯示此規則之本機 IP 位址。 **遠端位址** - 顯示此規則之遠端 IP 位址。 **DSCP** - 顯示要使用 QoS 控制來處理的資料級別。 **服務類型** – 顯示此**服務類型**的細部設定內容。 **新增** - 按此建立新的類別規則。
啟用 VoIP SIP/RTP 具有最高優先權功能	當此功能啟用的時候，VoIP SIP/UDP 封包會以最高優先傳送出去。 **SIP UDP 埠號** – 設定 SIP 使用的埠號。 - 按此圖示顯示 VoIP QoS 狀態。
標示輸出流量	以 DSCP 或是優先級值標示輸出之流量。 **新增 DSCP 或是優先級值**-勾選類別 1, 2, 3 方框以便套用 DSCP 或是優先級值於類別上。

完成設定之後，按下**確定**按鈕儲存相關設定。

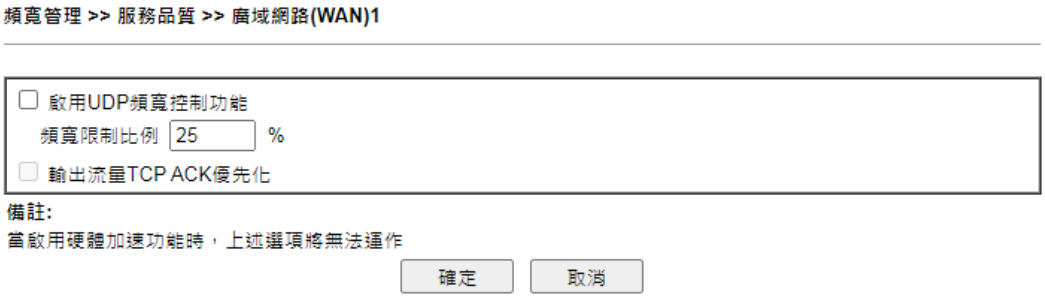
連線狀態統計

按下**狀態**鏈結可顯示服務品質的連線狀態統計圖供使用者參考。此功能僅在 QoS 的 WAN 介面已經啟用的狀態下始有作用。


頻寬管理 >> 服務品質
廣域網路(WAN)1 線上統計資料
更新頁面間隔: 5 秒數
| 更新頁面 |
類別 方向 保留頻寬比率 輸入總處理量 (bps) 輸出流量總處理量 (bps)
VoIP 雙方 --- 0 0
類別 1 雙方 25 0 0
類別 2 雙方 25 0 0
類別 3 雙方 25 0 0
其他 雙方 25 0 0
Inbound Status
VoIP
類別 1
類別 2
類別 3
其他
0
5
10 (bps)
Outbound Status
VoIP
類別 1
類別 2
類別 3
其他
0
5
10 (bps)
取消

WAN 介面之基本設置(軟體 QoS)

按 WAN 介面索引鏈結，設定介面的 QoS 頻寬限制。



可用設定說明如下：

項目	說明
啟用 UDP 頻寬控制功能	選擇限制 UDP 流量的頻寬值，**頻寬限制比例**值為 UDP 流量的最大頻寬百分比值。 ● **頻寬限制比例** - 輸入百分比值。
輸出流量 TCP ACK 優先化	下載速度可能會受到上傳 TCP ACK 封包的影響，您可以勾選此方塊讓 ACK 上傳得快一點，以便讓網路流通的更順暢。

資訊

WAN 下載頻寬/上傳頻寬速率必須小於真實的頻寬，以確保 QoS 計算能夠正確執行。建議將下載頻寬/上傳頻寬頻寬值設定為 ISP 業者所提供的實體網路速度的 80% - 85%，以便達到最佳的 QoS 成效。

新增/編輯 QoS 的類別規則

1. 按**類別規則**中的**新增**按鈕。若是要修改已經存在的類別規則，則按下該規則之**編輯**按鈕。

2. 在您按下**新增**或**編輯**之後，您可以看到如下的頁面。

可用設定說明如下：

項目	說明
啟用	勾選此方塊啟用本頁的設定。
IP 版本	選擇 IPv4 或是 IPv6。
本機 IP 位址	按**編輯**按鈕以設定規則的來源位址。

遠端 IP 位址	按**編輯**按鈕以設定規則的目標位址。 **位址類型-** 決定來源位址的位址類型。 關於**任何位址**，您無須填入起始 IP 位址，由系統決定。 關於**單一位址**，您可以填入起始 IP 位址。 關於**範圍位址**，您必須填入起始和終點 IP 位址。 關於**子網位址**，您必須填入起始 IP 位址和子網路遮罩。
DiffServ CodePoint	所有的資料封包將會被切割成不同等級，並且依照系統的等級層別來處理資料封包。請指定資料所需的層級作為 DoS 控制之用。
服務類型	決定 QoS 控制處理時資料的服務類型，這項類型可以視情況編輯改變，您可以從下拉式選項中選擇事先定義的服務類型，這些類型都是出廠時即設定好的類型，請自行挑選一種想要使用的類型。
QoS 類別	指定 QoS 類別 (1, 2 或 3)。

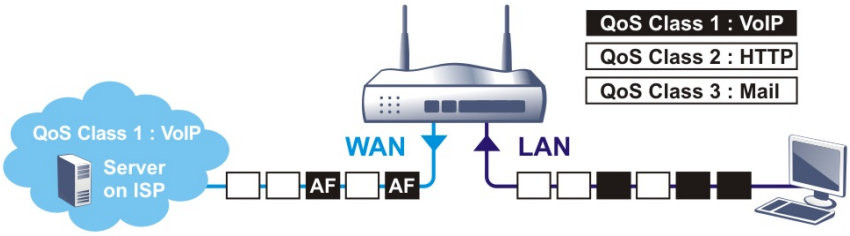
3. 完成設定之後，按下**確定**按鈕儲存相關設定。

4. 完成設定之後，按下**確定**按鈕儲存相關設定。

封包重新標籤以供辨識

來自於區域網路 IP 的封包可以透過 QoS 設定封包重新標籤，當該封包透過 WAN 界面傳送出去時，所有的封包都會標示特定的標頭讓 ISP 上的伺服器容易辨識出來。

例如，在下述範例圖當中，區域網路端的 VoIP 封包進入路由器時並沒有任何標頭，但是當它們透過路由器轉往 ISP 的伺服器時，所有的封包就都被標示上 AF 標頭(可在頻寬管理>>服務品質(QoS)類別中設定)。



類別規則

索引	啟用	QoS類別	本機位址	遠端位址	DSCP	服務類型
1	☑	類別1	任何	任何	任何	SIP(UDP:5060)
2	☑	類別1	任何	任何	任何	HTTP(TCP:80)
3	☑	類別1	任何	任何	任何	SMTP(TCP:25)

新增

備註:
1. 不符任何類別規則的封包將被分類至"其他"項目
2. 前往 使用者定義服務 以編輯/刪除使用者定義服務類型設定檔
3. 當啟用硬體加速(NAT)時，QoS性能對輸出封包也會同步提高，不過當類別1~3的保留頻寬未完全使用時，只有"其他"類別可以使用多出的頻寬比率

VoIP 優先順序

☑ 啟用VoIP SIP/RTP具有最高優先權功能:
SIP UDP 埠號: 5060 (預設值:5060)

標示輸出流量

類別 1	☑	新增 DSCP 或優先級值	AF 類別1 (中度捨棄)
類別 2	☑	新增 DSCP 或優先級值	AF 類別2 (低度捨棄)
類別 3	☑	新增 DSCP 或優先級值	AF 類別3 (中度捨棄)

VI-2-4 APP QoS

QoS 功能用於管理特定 IP 或是埠號等服務所需使用的頻寬。然而，對於無固定 IP 或是埠號的 VNC 或是 PPTV 的頻寬管理是完全沒有作用的。

APP QoS 使用應用程式管控功能進行軟體類型偵測，藉由結合 QoS 的功能，路由器可以對通訊協定、串流、遠端管理、網頁硬碟等等進行頻寬管理。

選擇**頻寬管理>>APP QoS** 開啟如下頁面：

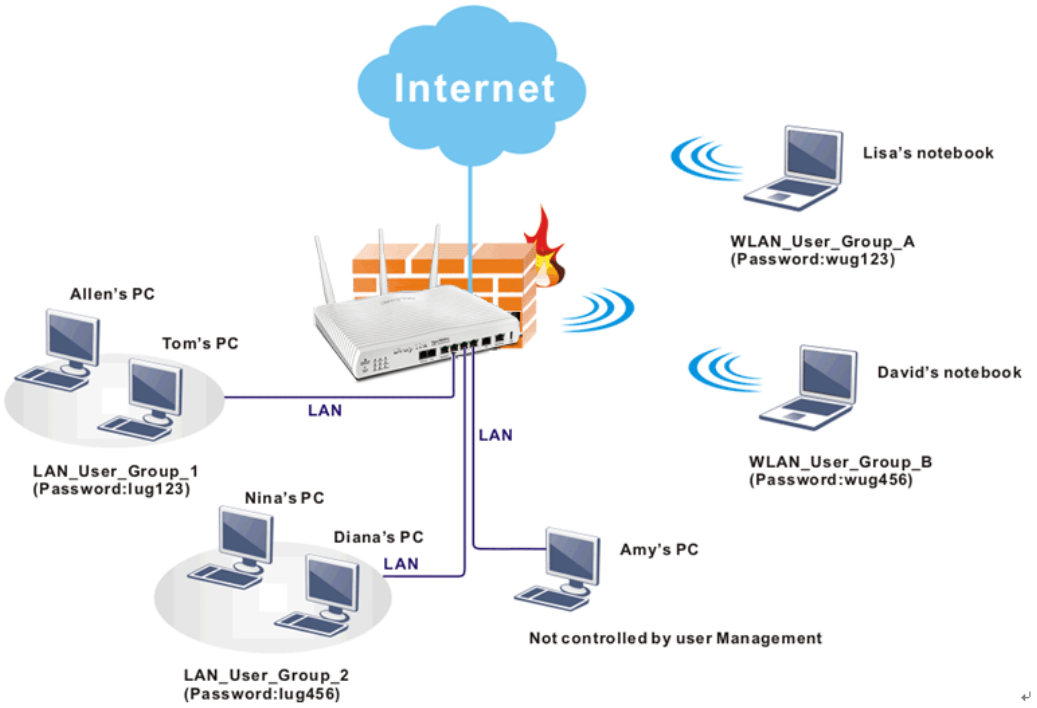
可用設定說明如下：

項目	說明
啟用/停用	選**啟用**可啟用 APP QoS 功能。 選**停用**停止 APP QoS 功能。
可追蹤的	表列的通訊協定可由路由器追蹤。每種標籤提供不同的協定類型。
無法追蹤	表列的通訊協定無法由路由器追蹤。每種標籤提供不同的協定類型。
選擇全部	選擇此頁面上全部的通訊協定。
清除全部	取消選擇此頁面上全部的通訊協定。
套用至全部	選擇一種動作便於套用至所有的通訊協定上。 **套用-** 按此可讓選定的動作立刻套用到選定的通訊協定上。
動作	通訊協定可以分別套用不同的 QoS 等級。

	動作 QoS類別 1 (高) QoS類別 2 (中度) QoS類別 3 (低) QoS其他 (最低) QoS類別 1 (高)

VI-3 使用者管理

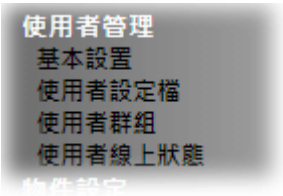
使用者管理這項功能具有安全性檢測的效果，除非特定主機提供正確使用者名稱以及密碼，否則它不允許來自該主機任何資料流量(除了 DHCP 相關封包以外)。使用者管理功能可以透過使用者帳號，而非利用 IP 位址/MAC 位址來管理主機。網路管理者可以針對不同主機透過不同使用者管理帳號，提供不同的防火牆策略或是規則。不只提供基本網際網路存取檢測，還能提供額外的防火牆規則諸如數位內容安全管理來保護管理下的各式主機。



資訊

防火牆中過濾器規則通常只會套用再主機上(亦即路由器安裝的那台)，有了使用者管理功能之後，設定的規則就可以套用在連結上該台路由器的每一個使用者電腦上。

網頁使用者介面



VI-3-1 基本設置

基本設定可以決定使用者管理準備運用在使用者上的標準為**基於規則模式**還是**基於使用者模式**，此處所選擇的模式將會影響套用於每個使用者上的過濾器規則內涵。

可用設定說明如下：

項目	說明
模式選擇	有二種模式可供您選擇，每種模式都會對受影響的使用者帶來不同的過濾效果。 **基於使用者** - 如果您選擇此模式，路由器將會套用您在**使用者管理>>使用者設定檔**中的過濾規則至使用者上。 **基於規則**- 如果您選擇此模式，路由器將會套用您在**防火牆>>基本設定**中的過濾規則至使用者上。
驗證頁面	**網頁驗證** - 選擇網頁驗證使用的協定(HTTPS/HTTP)。 **登入頁面設定**- 此連結讓您開啟登入頁面設定網頁，詳細資訊請參考**系統維護>>登入頁面設定**一節。 **顯示出成功登入後.....** - 勾選此框以顯示追蹤視窗中用戶端的

	IP 位址。
指定首頁	用戶透過本台路由器登入存取網際網路時，將會先開啓此處所輸入的網站。

完成設定之後，按下**確定**按鈕儲存相關設定。

VI-3-2 使用者設定檔

本功能可讓您設定客製化使用者設定檔(最多可設定 200 個)，這些設定檔將會套用於使用者管理之下的使用者帳號。開啟**使用者管理>>使用者設定檔**即可見到如下頁面。

使用者管理 >> 使用者設定檔

使用者設定檔表格 | 設定回復出廠預設值 |

選擇全部 清除全部 搜尋

設定檔	啟用	名稱	設定檔	啟用	名稱
1.	☑	admin	17.	☐	
2.	☑	Dial-In User	18.	☐	
3.	☐		19.	☐	
4.	☐		20.	☐	
5.	☐		21.	☐	
6.	☐		22.	☐	
7.	☐		23.	☐	
8.	☐		24.	☐	
9.	☐		25.	☐	
10.	☐		26.	☐	
11.	☐		27.	☐	
12.	☐		28.	☐	
13.	☐		29.	☐	
14.	☐		30.	☐	
15.	☐		31.	☐	
16.	☐		32.	☐	

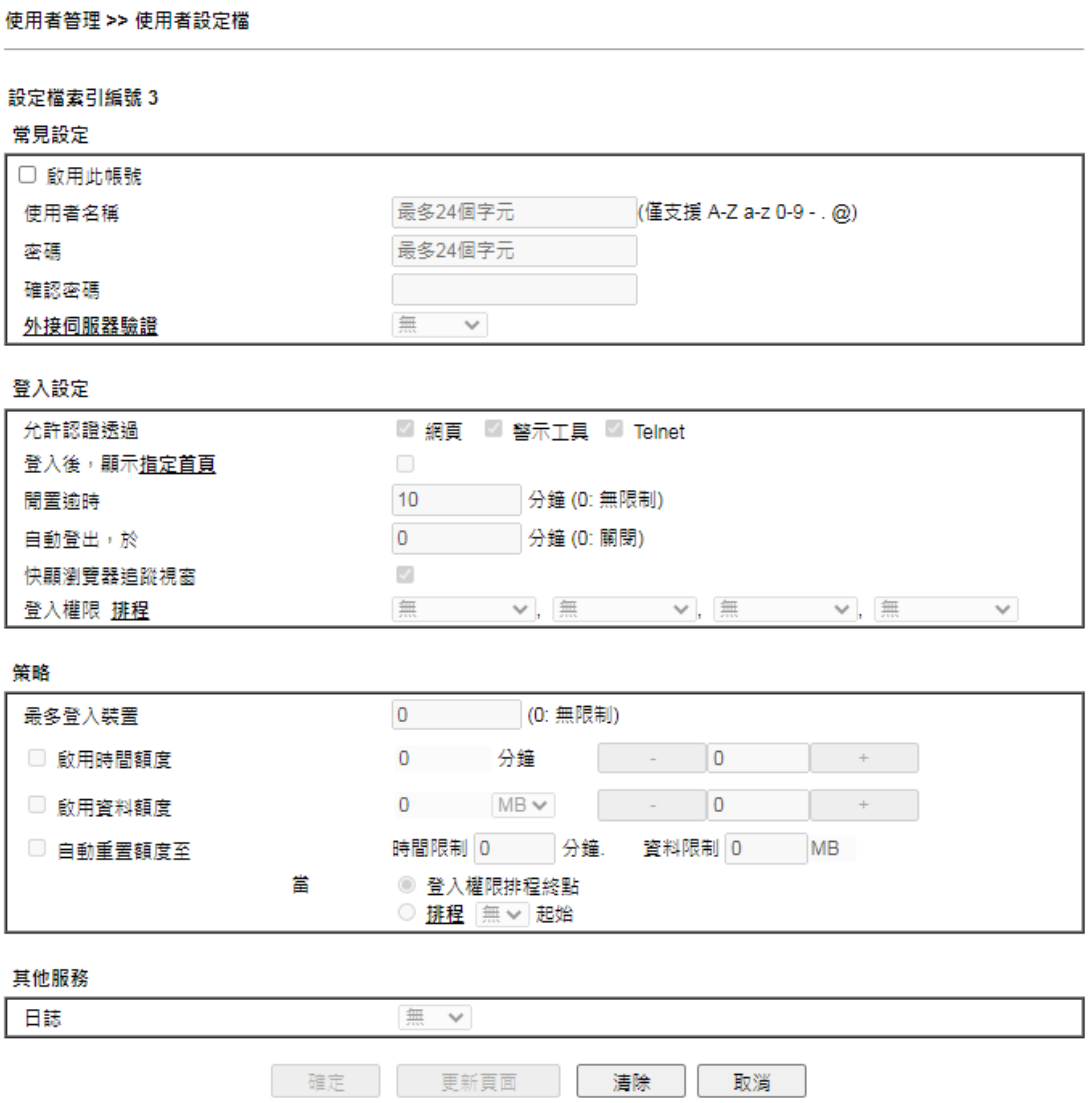
<< 1-32 | 33-64 | 65-96 | 97-128 | 129-160 | 161-192 | 193-200 >> 下一頁 >>

備註:

1. 管理：欲變更管理者密碼，請前往系統維護>>管理者密碼。
2. 撤入使用者設定檔：撤入使用者設定檔保留用於VPN驗證
3. 驗證期間，路由器將先檢查所有本機使用者設定檔，然後是外接伺服器的設定檔。

確定 取消

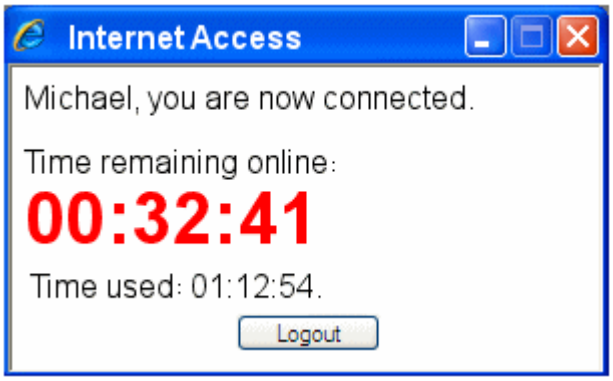
欲設定使用者設定檔，請點選任何一的設定檔編號連結，不過要注意的是連結 1(admin) 與連結 2(Dial-In User)這二個都是預設值。請按連結 3。



可用設定說明如下：

項目	說明
常見設定	
啟用此帳號	勾選此方塊啟用此設定檔。
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。
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。
確認密碼	再次輸入密碼以確認。
外接伺服器驗證	路由器將透過外部服務例如 LDAP 伺服器或是 RADIUS 伺服器或是自身對撥入使用者進行驗證。如果您在此選擇了 LDAP 伺服器

	或是 RADIUS 伺服器，上述的密碼設定都可以省略不必設定。
登入設定	
允許認證透過	任何使用者(不管是 LAN 端或是 WAN 端)嘗試透過路由器連結網際網路，都必須通過路由器的驗證，有三種方式可讓使用者挑選使用： **網頁**- 如果選擇此項，使用者可在任何瀏覽器上輸入路由器的 URL，登入視窗將會跳出並要求使用者輸入使用者名稱與密碼。如果通過驗證了，歡迎訊息視窗(可於使**用者管理>>基本設定**中設定)會顯示在螢幕上，驗證之後，路由器也會自動導引至目的 URL(若使用者有需要的話)。 **警告工具** – 如果選擇此項，使用者必須打開警告工具(Alert Tool)並輸入使用者名稱及密碼進行驗證，通過驗證後，系統會出現小視窗告知使用者剩餘多少時間可以使用網路，接著，使用者可利用任何一個瀏覽器登入網際網路。 **Telnet** – 如果選擇此項，使用者可透過 Telnet 指令來進行驗證作業。
登入後，顯示指定首頁	當使用者利用帳號及密碼登入路由器的使用者介面時，將會被引導至**使用者管理>>基本設定**中所設定的指定首頁。 勾選此方塊可開啟此項功能。
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，預設值為 10 分鐘。
自動登出，於	在特定的時間過後，此帳號將會被強迫登出。
快顯瀏覽器追蹤視窗	如果啟用此功能，且設定了閒置逾時的功能，那麼含有倒數計時的視窗即會跳出告訴您還剩下多少時間，不過系統會定期更新時間讓連線維持不斷，如此依來，閒置逾時就不會中斷網路連線了。
登入權限排程	您可以在此輸入四組時間排程，所有的排程都可在**其他應用>>排程**頁面事先設定，在本頁您只要將排程的索引編號輸入即可。
策略	
最多登入裝置	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。預設值為 0，這表示沒有人數上的限制。
啟用時間額度	時間額度表示路由器針對本設定檔的使用者所允許的全部連線時間，勾選此方塊啟用此功能。 [+] – 按下此方塊可增加此設定檔的時間額度，單位是分鐘，請在後方空格輸入數值。 [-] – 按下此方塊可減少此設定檔的時間額度，單位是分鐘，請在後方空格輸入數值。 **注意:** 當使用者成功透過路由器登入網際網路之後，下述對話盒會跳出通知使用者還有多少時間可以使用網路。

	 時間一旦到達，所有連線工作包括網路、IM、社交媒體、臉書等等都會暫停。
啟用資料額度	資料額度表示給予使用者的全部資料傳輸量。 + – 按下此方塊可增加此設定檔的資料額度，單位是 MB，請在後方空格輸入數值。 - –按下此方塊可減少此設定檔的資料額度，單位是 MB，請在後方空格輸入數值。
自動重置額度至	勾選此方框使用預設的時間與資料額度值。 設定此檔的預設時間額度與資料額度。當排程時間已到，路由器將會自動使用預設的額度設定。 **時間限制** – 輸入時間額度數值 **資料限制** – 輸入資料額度數值。 **登入權限排程終點** - 當到達排程時間限制點時，路由器即以使用者設定的時間與資料限制重新設定相關額度。 **排程** - 指定排程設定檔。
其他服務	
日誌	登入登出的時間，封鎖/放行使用者等內容都可傳送並且顯示在 Syslog 上，請選擇任何一個項目以便紀錄與該使用者相關的內容。

完成設定之後，按下**確定**按鈕儲存相關設定。

VI-3-3 使用者群組

本頁可讓您將數個使用者設定檔歸類成一個使用者群組，這裡所設定的群組也會在**防火牆>>基本設定**中當成過濾器規則來應用。

使用者管理 >> 使用者群組

使用者群組表格: | 設定回復出廠預設值 |

索引	名稱	索引	名稱
1.		17.	
2.		18.	
3.		19.	
4.		20.	
5.		21.	
6.		22.	
7.		23.	
8.		24.	
9.		25.	
10.		26.	
11.		27.	
12.		28.	
13.		29.	
14.		30.	
15.		31.	
16.		32.	

按下任何一個索引編號連結開啟如下頁面：

使用者管理 >> 使用者群組

群組索引編號：1

名稱:

可用使用者物件

1-admin
2-Dial-In User
3-marketing

選定的使用者物件 (最多 32)

確定 清除 取消

可用設定說明如下：

項目	說明
名稱	輸入使用者群組的名稱。
可用使用者物件	您可以將數個使用者設定檔(物件)組合為一個群組，所有可用的使用者物件都會顯示在此區域內，特別注意的是使用者物件 Admin 以及 Dial-In User 乃是預設的物件，可以供您自由設定的物件檔則是編號為 3, 4, 5 及之後物件連結。

選定的使用者物件	按下 » 按鈕將選定的使用者物件移至本區。

完成設定之後，按下**確定**按鈕儲存相關設定。

VI-3-4 使用者線上狀態

本頁呈現連接至路由器的使用者，且在固定的間隔時間會自動更新頁面。

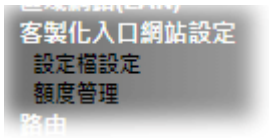
可用設定說明如下：

項目	說明
更新頁面秒數	使用下拉式清單選擇時間間隔，讓系統於固定時間更新本頁內容。
更新頁面	按下此鈕立即更新頁面。
索引	顯示線上使用者的順序編號。
使用者	顯示目前連結至路由器的使用者，您可按下檔名稱下方連結開啟該使用者設定檔頁面。
IP 位址	顯示裝置的 IP 位址。
設定檔	顯示使用者的權限。
上次登入時間	顯示使用者上次登入路由器的時間。
到期時間	顯示使用者使用網路的到期時間。
資料額度	顯示資料傳送的額度。
閒置時間	顯示設定檔的閒置時間設定。
動作	**阻擋** - 封鎖使用者使用網路。 **解鎖** - 解除使用者使用網路。 **登出** - 強迫使用者登出。 **刪除** - 移除選定之使用者。

VI-4 客製化入口網站設定

客製化入口網站設定可讓您設定數個設定檔，利用指定 URL 的方式，讓無線用戶/LAN 用戶在登入網際網路時連結至指定的頁面。亦即不論該用戶的目的為何，都會先被強制導入此頁所指定的網頁。換句話說，若公司行號想要為其產品對用戶進行廣告宣傳，就可利用此頁面達到不錯的效果。

網頁使用者介面



VI-4-1 設定檔設定

選擇**設定檔設定**建立或是修改入口網站設定檔，依照 LAN 子網、WLAN SSID、原始與目的 IP 位址等，最多可以設定 4 個設定檔以因應不同的需要。

可用設定說明如下：

項目	說明
索引	按下索引編號連結可以檢視或是更新設定檔內容。
啟用	勾選此框以便啟動此設定檔。
註解	顯示此設定檔的說明。
登入模式	顯示設定檔使用的登入模式。
套用介面	顯示設定檔套用的介面。
預覽	按此鈕預覽即將顯示給使用者觀看的入口網站頁面。

備份	**設定檔清單** - 請選擇一個來源設定檔。 **備份** - 按此儲存以來源設定檔為基準的 config 設定檔案。
還原 ...	**選擇檔案** - 按此選擇一個設定檔。 至.. - 選擇目地檔案。此檔可被選定的設定檔來還原。 **還原** - 按此鈕執行還原工作。 **還原額度管理設定**- 若勾選此項，額度管理設定也會跟著還原至目地檔案內。

VI-4-1-1 登入模式

有 5 種登入模式可以用來驗證網路用戶：**跳過登入**、**透過點擊**、**各種不同的入口網站登入**、**外接入口伺服器**，每種模式都會帶出不同的網頁。

(A)跳過登入

這個模式不會執行任何驗證，系統將直接導引使用者至指定首頁，之後使用者可以離開該頁面前網希望造訪的網站。

(B)透過點擊

當使用者第一次嘗試登入網際網路時，系統會呈現如下頁面。再按下頁面上的**接受(Accept)**按鈕後，使用者將被導引至指定首頁，然後許可登入網際網路。

(C) 各種不同的入口網站登入

當使用者第一次嘗試登入網際網路時，系統會出現驗證頁面。再透過使用臉書帳號、Google 帳號、PIN 碼、RADIUS 伺服器密碼驗證之後，用者將被導引至指定首頁，然後許可登入網際網路。

(D) 外接入口伺服器

當使用者透過此路由器第一次嘗試登入網際網路時，外接 RADIUS 伺服器將驗證使用者。

VI-4-1-2 設定入口網站設定檔步驟

1 **登入方式**

按下選定設定檔的索引編號連結(例如 #1)顯示如下頁面。

客製化入口網站設定 >> 設定檔設定

啟用此設定檔

註解:

入口網站伺服器

入口網站方式

- 跳過登入，僅指定首頁
- 透過點擊
- 各種不同的入口網站登入
- 外接入口伺服器

強制登入URL http:// portal.draytek.com

儲存與下一頁 取消

可用設定說明如下：

項目	說明
啟用此設定檔	勾選此框啟用此設定檔。
註解	輸入可以辨識此設定檔的說明內容。
入口網站伺服器	
入口網站方式	選擇想要的登入模式。 ◉ 跳過登入，僅指定首頁 ○ 透過點擊 ○ 各種不同的入口網站登入 ○ 外接入口伺服器
*當選擇**跳過登入**或是**透過點擊**為入口網站方式時*	
強制登入 URL	輸入強制登入的網站 URL。
*當選擇**各種不同的入口網站登入**為入口網站方式時*	
強制登入 URL	輸入強制登入的網站 URL。
登入方式	選擇一種或多種想要的登入方式。 ● 以臉書登入 ● 以 Google 登入 ● 透過簡訊接收 PIN ● 透過郵件接收 PIN ● 以 RADIUS 登入
Facebook (以臉書登入)	當選擇**以臉書登入**時，系統會出現如下的設定： **臉書 APP ID** - 輸入有效的臉書開發商 app ID。 若您尚未具有 APP ID，可參考節 A-1 如何建立臉書 APP ID 以利網頁

	入口驗證。 **臉書 APP 密鑰** - 輸入上述 APP ID 所使用的密鑰。
Google (以 Google 登入)	當選擇**以 Google 登入**時，系統會出現如下的設定： **Google App ID** - 輸入有效的 Google 開發商 app ID。 若您尚未具有 APP ID，可參考 A-2 節取得 APP ID。 **Google App 密鑰** -入上述 APP ID 所使用的密鑰。
簡訊服務供應商 (透過簡訊接收 PIN)	當選擇**透過簡訊接收 PIN** 時，系統會出現如下的設定： **透過簡訊服務供應商接收 PIN** - 選擇簡訊服務供應商以便傳送 PIN 通知。簡訊服務供應商乃透過**物件設定>>簡訊/郵件服務物件**來設定。
郵件伺服器 (透過簡訊接收 PIN)	當選擇**透過郵件接收 PIN** 時，系統會出現如下的設定： **透過郵件伺服器接收 PIN** - 選擇郵件伺服器以便傳送 PIN 通知。郵件伺服器乃透過**物件設定>>簡訊/郵件服務物件**來設定。
RADIUS 伺服器 (以 RADIUS 登入)	當選擇**以 RADIUS 登入**時，系統會出現如下的設定： **驗證方式** – 按此鏈結設定外接 RADIUS 伺服器以驗證用戶。 **RADIUS MAC 驗證** – 勾選**啟用**讓系統能透過 MAC 位址進行使用者驗證。 **MAC 位址格式** – 選擇一種 MAC 位址格式做為 RADIUS 伺服器輸入 MAC 位址之用。 **RADIUS NAS-識別碼** - 請輸入識別碼。
*當選擇**外接入口伺服器**為入口網站方式時*	
強制登入 URL	輸入強制登入的網站 URL。
重導向 URL	輸入 URL 讓用戶皆可被導往該網站。
RADIUS 伺服器 (以 RADIUS 登入)	當選擇**以 RADIUS 登入**時，系統會出現如下的設定： **驗證方式** – 按此鏈結設定外接 RADIUS 伺服器以驗證用戶。 **RADIUS MAC 驗證** – 勾選**啟用**讓系統能透過 MAC 位址進行使用者驗證。 **MAC 位址格式** – 選擇一種 MAC 位址格式做為 RADIUS 伺服器輸入 MAC 位址之用。 **RADIUS NAS-識別碼** - 請輸入識別碼。
儲存與下一頁	按此儲存本頁的設定並進入下一頁。
取消	按此捨棄本頁設定並回到前一頁。

若您選擇**跳過登入**作為登入模式，請直接跳至步驟 4 *白名單*。

其他模式請繼續依循步驟 2 與 3 進行。

2 背景

若您選擇需要驗證的登入模式，請選擇登入頁面的背景圖樣。

可用設定說明如下：

項目	說明

選擇登入背景	選擇**顏色背景**或是**影像背景**作為登入頁面的背景方案。
瀏覽器標籤標題	輸入顯示在瀏覽器網頁的標題文字。
標誌影像	預設狀態下會顯示居易商標，您可以輸入 HTML 文字或是上傳影像取代預設商標影像。
標誌背景顏色	從事先定義的顏色清單中選擇商標的背景顏色，或是選擇**客製化顏色**並輸入 RGB 值，按**預覽**可以檢視選定的顏色。
登入方式背景顏色	從事先定義的顏色清單中選擇登入面板的背景顏色，或是選擇**客製化顏色**並輸入 RGB 值，按**預覽**可以檢視選定的顏色。
不透明度(10 ~ 100)	當選擇**影像背景**時，可以設定背景影像的不透明度。
背景影像	當選擇影像背景時，可以按**選擇檔案**按鈕挑選影像檔案(格式為.JPG 或.PNG)之後按**上傳**將檔案上傳至路由器。
儲存與下一頁	按此儲存本頁的設定並進入下一頁。
取消	按此捨棄本頁設定並回到前一頁。

若您已經選擇**跳過登入**作為登入模式，請直接跳至步驟 4 *白名單(Whitelisting)*。

其他模式請繼續依循步驟 3 進行。

3 登入頁面設定

在此步驟，您可以設定登入頁面的內容。

透過點擊

本節說明透過點擊登入模式的頁面設定。

客製化入口網站設定 >> 設定檔設定

1 登入方式 — 2 背景 — 3 登入頁面設定 — 4 白名單設定 — 5 更多選項

設定登入方式與細節內容

Welcome!
We are pleased to provide free Wi-Fi to you!
By clicking the button below you agree to the Terms and Conditions
Accept

隱私政策及條款和條件

接受按鈕說明與顏色

歡迎訊息

Welcome!
Please log in to enjoy Wi-Fi.

(最多 1360 個字元) 預設值

隱私政策及條款和條件

條款和條件

☑ 啟用

☑ 使用者必須勾選以便進訪網際網路

說明

By clicking the button below you agree to the Terms and Conditions.

(最多 170 個字元) 預設值

內容

◉ 內部內容：將會直接開啟條件與條款內容

(最多 1360 個字元)

○ 外部內容：將鏈結至包含書面條款和條件的網頁

外部內容URL

用於行銷的資料蒐集

☐ 啟用

☐ 使用者必須勾選以便進訪網際網路

說明

I would like to receive emails about the latest events, products, and services from you.

(最多 170 個字元) 預設值

當使用者未勾選時出現之錯誤訊息

Please check this box if you want to proceed.

(最多 170 個字元) 預設值

接受按鈕說明

Submit

(最多 170 個字元) 預設值

接受按鈕顏色

客製化顏色

A2A2A2 (格式：FFFFFF) 預覽 預設值

可用設定說明如下：

項目	說明
登入對話框顯示如下: 設定登入方式與細節內容 	
不過，如果選擇的是**含憑證之 PIN**，那麼登入對話框顯示如下: 設定登入方式與細節內容 	
歡迎訊息	輸入顯示於歡迎訊息中的文字。
隱私政策及條款和條件	
條款和條件	**啟用** - 勾選此框啟用此選項。 **使用者必須勾選以便造訪網際網路** - 如果啟用了**條款和條件**，那麼使用者還必須勾選此框以便造訪網際網路。 **說明** - 輸入顯示在條款與條件跳出視窗上的文字。 **內容** - 分成內部內容與外部內容。選擇內部內容並輸入相關文字做為條款與條件超連結內容。或是選擇外部內容並輸入網站 URL 以便顯示條款與條件細則。
用於行銷的資料蒐集	**啟用** - 勾選此框啟用此選項。 **使用者必須勾選以便造訪網際網路** -勾選此框啟用此選項。 **說明** - 輸入相關文字告知使用者。
當使用者未勾選時出現之錯誤訊息	輸入相關文字通知使用者。
接受按鈕說明	輸入顯示在接受按鈕上的文字。
接受按鈕顏色	自事先定義的顏色清單中選擇接受按鈕的顏色，或是選擇**客製化顏色**並輸入 RGB 值。按下**預覽**按鈕檢視選定的顏色。
儲存與下一頁	按此儲存本頁的設定並進入下一頁。
取消	按此捨棄本頁設定並回到前一頁。

當選擇**含憑證之 PIN** 時,	
PIN 需求之提示訊息	輸入訊息提醒輸入 PIN 碼。
輸入 PIN 說明	輸入已存之 PIN 碼。
提交按鈕說明	輸入顯示在提交按鈕上的文字。
提交按鈕顏色	自事先定義的顏色清單中選擇提交按鈕的顏色，或是選擇**客製化顏色**並輸入 RGB 值。按下**預覽**按鈕檢視選定的顏色。
儲存與下一頁	按此儲存本頁的設定並進入下一頁。
取消	按此捨棄本頁設定並回到前一頁。

各種不同的入口網站登入

本節說明各種不同的入口網站登入模式的頁面設定。

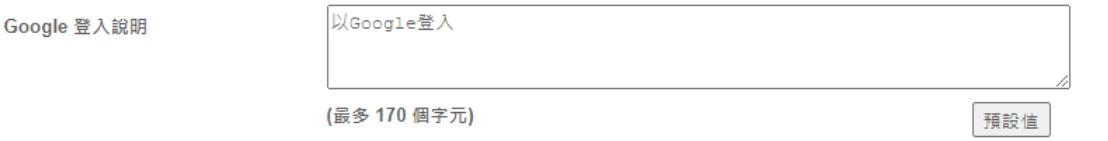
相關設定於臉書、Google、PIN、RADIUS 驗證的共用設定為：

項目	說明
歡迎訊息	輸入顯示於歡迎訊息中的文字。
條款和條件	**啟用** - 勾選此框啟用此選項。 **使用者必須勾選以便造訪網際網路** - 如果啟用了**條款和條件**，那麼使用者還必須勾選此框以便造訪網際網路。 **說明** - 輸入顯示在條款與條件跳出視窗上的文字。 **內容** - 分成內部內容與外部內容。選擇內部內容並輸入相關文字做為條款與條件超連結內容。或是選擇外部內容並輸入網站 URL 以便顯示條款與條件細則。
用於行銷的資料蒐集	**啟用** - 勾選此框啟用此選項。 **使用者必須勾選以便造訪網際網路** -勾選此框啟用此選項。 **說明** - 輸入相關文字告知使用者。
當使用者未勾選時出現之錯誤訊息	輸入相關文字通知使用者。

若您選擇了**以臉書登入**，設定頁面如下：

項目	說明
臉書登入說明	輸入顯示於臉書登入按鈕上的文字。 **預設值** - 按此使用預設文字。

若您選擇了**以 Google 登入**，設定頁面如下：



項目	說明
Google 登入說明 (Google Login	輸入顯示於 Google 登入按鈕上的文字。 **預設值** - 按此使用預設文字。

若您選擇了**透過簡訊接收 PIN** 或**透過郵件接收 PIN**，設定頁面如下：

項目	說明
PIN 需求之提示訊息	輸入用來建議使用者選擇簡訊驗證方式的訊息。
接收 PIN 說明	輸入使用者點選以接收簡訊 PIN 碼的按鈕上文字。
透過簡訊內容接收 PIN	輸入簡訊發送的文字，以便通知使用者 PIN 碼。
透過郵件主題接收 PIN	輸入郵件主題，以便通知使用者 PIN 碼。
透過郵件內容接收 PIN	輸入郵件內容，以便通知使用者 PIN 碼。
輸入 PIN 說明	輸入顯示在 PIN 文字方塊內的訊息，促使用戶輸入 PIN 碼。

提交按鈕說明	輸入顯示在提交 PIN 按鈕內的文字。
提交按鈕顏色	自事先定義的顏色清單中選擇提交按鈕的顏色，或是選擇**客製化顏色**並輸入 RGB 值。按下**預覽**按鈕檢視選定的顏色。

若您選擇了**以 RADIUS 登入**，設定頁面如下：

項目	說明
RADIUS 需求之提示訊息	輸入提醒使用這需要登入的提示說明。
RADIUS 帳號說明	輸入提醒使用者需輸入使用者帳號的提示說明。
RADIUS 密碼說明	輸入提醒使用者需輸入密碼的提示說明。
登入按鈕說明	輸入顯示在登入按鈕內的文字。
登入按鈕顏色	自事先定義的顏色清單中選擇登入按鈕的顏色，或是選擇**客製化顏色**並輸入 RGB 值。按下**預覽**按鈕檢視選定的顏色。

最後是，每頁都存在的按鈕：

項目	說明
儲存與下一頁	按此儲存本頁的設定並進入下一頁。
取消	按此捨棄本頁設定並回到前一頁。

透過簡訊接收 PIN/ 透過郵件接收 PIN 的第二階段設定頁面

如果您已選擇了**透過簡訊接收 PIN/ 透過郵件接收 PIN** 作為登入模式，您還需要另外設定 PIN 碼相關的設定頁面。

客製化入口網站設定 >> 設定檔設定

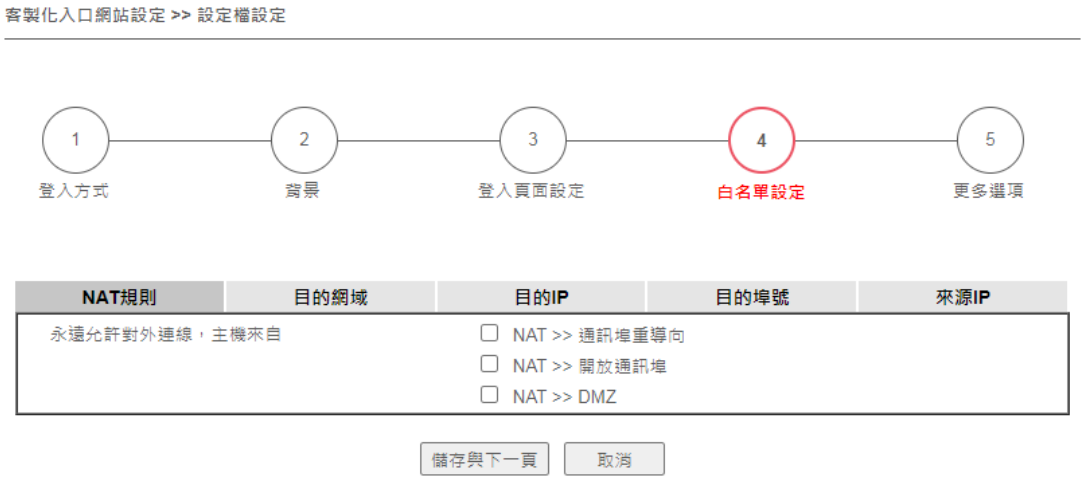
可用設定說明如下：

項目	說明
上一頁按鈕說明	輸入回到前一個頁面的超連結標籤內文。
PIN 碼訊息	輸入顯示在頁面主體內文的文字。
預設國家	選擇顯示在下拉式選單中的預設國碼。
輸入行動號碼說明	輸入於行動電話文字框中，提醒用戶輸入行動電話號碼的訊息。
傳送按鈕說明	輸入傳送按鈕的標籤內文。
傳送按鈕顏色	自事先定義的顏色清單中選擇傳送按鈕的顏色，或是選擇**客製化顏色**

	並輸入 RGB 值。按下**預覽**按鈕檢視選定的顏色。
傳送成功的訊息	輸入於 PIN 碼傳送成功之後，通知用戶成功的訊息。
儲存與下一頁	按此儲存本頁的設定並進入下一頁。
取消	按此捨棄本頁設定並回到前一頁。

4.白名單設定

在此步驟中，您可以配置白名單設定，允許使用者傳送並接收滿足白名單設定的資料流量。



可用設定說明如下：

項目	說明
NAT 規則)	避免入口網站設定與 NAT 規則產生衝突，導致不預期的錯誤，選擇允許繞過入口網站設定的 NAT 規則，選定 NAT 規則中條列的主機得以允許登入網際網路，不會被入口網站攔截。
目的網域	輸入允許通過路由器的目標網域，最多可以設定 30 個。
目的 IP	輸入允許通過路由器的目標 IP 位址，最多可以設定 30 個。
目的埠號	輸入允許通過路由器的目標通訊協定，最多可以設定 30 個。
來源 IP	輸入允許通過路由器的來源 IP 位址，最多可以設定 30 個。
儲存與下一頁	按此儲存本頁的設定並進入下一頁。
取消	按此捨棄本頁設定並回到前一頁。

5. 更多選項

在此步驟中，您可以針對客製化入口網站設定進階選項。

客製化入口網站設定 >> 設定檔設定

1 登入方式 — 2 背景 — 3.1 — 3.2 登入頁面設定 — 4 白名單設定 — 5 更多選項

額度管理

登入方式	額度策略設定檔	有效時間	允許的裝置	頻寬限制	連線數限制
電子郵件登入	1.Default	0d 5h 0m	無限制	無限制	無限制
省略	1.Default	0d 5h 0m	無限制	無限制	無限制

備註:
欲修改額度設定，請至**客製化入口網站設定 >> 額度管理**。

JSON API

☐ 啟用JSON API
伺服器URL
取得JSON並更新使用者狀態 0 小時 5 分鐘
更新資訊
☐ NAS 辨識碼 ☐ MAC位址 ☐ 所有使用者編號 ☐ Wi-Fi使用者名稱

客製化入口網站選項

HTTPS重新導向 ☑ 啟用
當未受驗證用戶端開啟HTTPS頁面時，重導向仍能運做但會顯示出憑證錯誤
停用此功能，重新導引至 HTTP 頁面，若無重新導向且無憑證錯誤，系統會停止
HTTPS 瀏覽功能

強制登入驗證 ☐ 啟用
觸發未經驗證用戶端於連接上Wi-Fi時，系統自動跳出入口網站頁面
此功能在使用**社交登入** 時是不可用的，因為受到OS內建的強制登錄驗證網頁偵測
限制之故，頁面無法正常顯示

可用設定說明如下：

項目	說明
額度管理	
額度管理策略設定檔	選擇一個策略設定檔，套用至使用入口網站的用戶。
JSON API	
啟用 JSON API	勾選此框啟用此功能。使用者可以修改入口網站設定並取得使用者相關資訊，無需登入 Vigor 裝置之網頁設定介面。 **伺服器 URL** - 啟用功能後，輸入遠端伺服器的的 IP 位址或是網域名稱。伺服器將透過 JSON API 格式編輯入口網站設定。 **取得 JSON 並更新使用者狀態** - 設定路由器取得 JSON 及使用者資訊的間隔時間(時與分)。 **更新資訊** - 選擇要讓遠端伺服器更新的資訊類別。
客制化入口網站選項	
HTTPS 重新導向	若選定了此項，嘗試登入 HTTPS 網站未被驗證的使用者會被系統導引至登入頁面，瀏覽器則警告用戶憑證有誤。如果沒有勾選此項，任何 TTPS 網站登入嘗試都會逾時也無重新導向。
強制登入驗證	若選定了此項，當一個未驗證用戶嘗試登入網際網路時，系統會自動觸發入口網站頁面。當登入模式為社群登入時，這個功能基本上是不

	可用的，因為入口網站頁面會因操作系統內建的強制登入驗證網頁針測之限制，無法正確顯示頁面。
省略	勾選此框後，如果 HTTPS 連線數超過預設值限制，入口網站暫時跳過而不進行身份驗證。 這些用戶將被重導向到入口網站，且稍後才進行身份驗證。
驗證後進入指定首頁	
固定 URL	驗證後進入指定首頁可指定使用者成功驗證之後系統顯示的網頁。 使用者將被重新導引至指定的 URL 頁面。這個部份可用於顯示廣告讓用戶參考，例如飯店客人想要使用無線網際網路時先看廣告。
使用者需求 URL	使用者將被重新導引至其原本想要登入的 URL
公告訊息	此處設定的訊息會顯示給用戶檢視數秒。 **預設訊息 -** 當選定了公告訊息之後，此按鈕即可啟用，點選此鈕載入預設文字做為公告欄顯示的訊息。
套用介面	
子網	目前的客製化入口網站設定檔可對選定子網生效。 **WLAN –** 目前的客製化入口網站設定檔可對選定的 WLAN SSID 生效。
WLAN	目前的入口網站設定對選定的無線區域網路 SSID 皆有效。
完成	按此儲存本頁的設定。
取消	按此捨棄本頁設定並回到前一頁。

VI-4-2 額度管理

系統管理員可以指定頻寬與連線數額度，套用在使用入口網站登入的用戶。

在此所進行的設定都會直接改寫**頻寬管理>>頻寬限制**與**頻寬管理>>連線數限制**上原本的設定值。

客製化入口網站設定 >> 額度管理

客製化入口網站頻寬與連線數限制

此處的設定僅套用在入口網站用戶，且會覆蓋頻寬管理中設定的策略內容

☐ 頻寬限制

☐ 連線數限制

額度策略設定檔

索引	名稱	首次登入後的到期時間	每個帳戶允許的裝置	重新連接時間限制	頻寬限制	連線數限制
1	Default	0日 5時 0分	無限制	無限制	無限制	無限制

新增 (最多 20)

取消 確定

可用設定說明如下：

項目	說明
頻寬限制	勾選此框直接改寫**頻寬管理>>頻寬限制**上所設定的內容。
連線數限制	勾選此框直接改寫**頻寬管理>>連線數限制**上所設定的內容。
額度策略設定檔	**新增** - 建立新的策略設定檔，最多可以設定 20 個。

欲建立新的額度策略設定檔，請按下**新增**按鈕開啟如下頁面：

客製化入口網站設定 >> 管理 >> 額度策略設定檔 2

設定檔名稱 level 2

帳戶效期

首次登入後到期時間 0 日 5 小時 0 分鐘

閒置逾時 0 分鐘

裝置控制

每個帳戶允許的裝置 無限制

重新連接時間限制 於 0 : 0 每日

阻擋同一使用者於設定時間前再度連線

0 小時 0 分鐘

阻擋同一使用者於設定期間再度連線

頻寬與連線數限制

頻寬限制

下載速度限制 0 Kbps Mbps

上傳限制 0 Kbps Mbps

連線數限制 0 連線數

取消 確定

可用設定說明如下：

項目	說明
設定檔名稱	輸入設定檔之檔名。
帳戶效期	設定登入有效的時間。 **首次登入後到期時間**-設定日、時與分。在登入到期的時候，路由器就會封鎖用戶不再讓用戶存取網際網路。 **閒置逾時** – 勾選此框後，如果用戶在指定的一段時間內都無動作的話，路由器會中斷網路連線。
裝置控制	設定一個帳戶可以連接的最多裝置數，及每個透過入口網站登入網路的用戶之時間限制。 **每個帳戶允許的裝置** – 使用下拉式清單選擇最多的連線裝置數目。 **重新連接時間限制** – 阻擋帳戶重新連接網路的方式： ● **於 .... 每日** -登入時間到期後，在每日的設定時間到達之前，都無法使用帳戶連接裝置。 ● **小時.. 分鐘** – 登入時間到期後，在此設定時間到達之前，都無法使用帳戶連接裝置。
頻寬與連線數限制	**頻寬限制** – 勾選此框設定入口網站用戶的頻寬限制。 ● **下載限制/上傳限制** – 設定最大的下載跟上傳的速度值。 **連線數限制** - 勾選此框設定入口網站用戶的連線數限制。

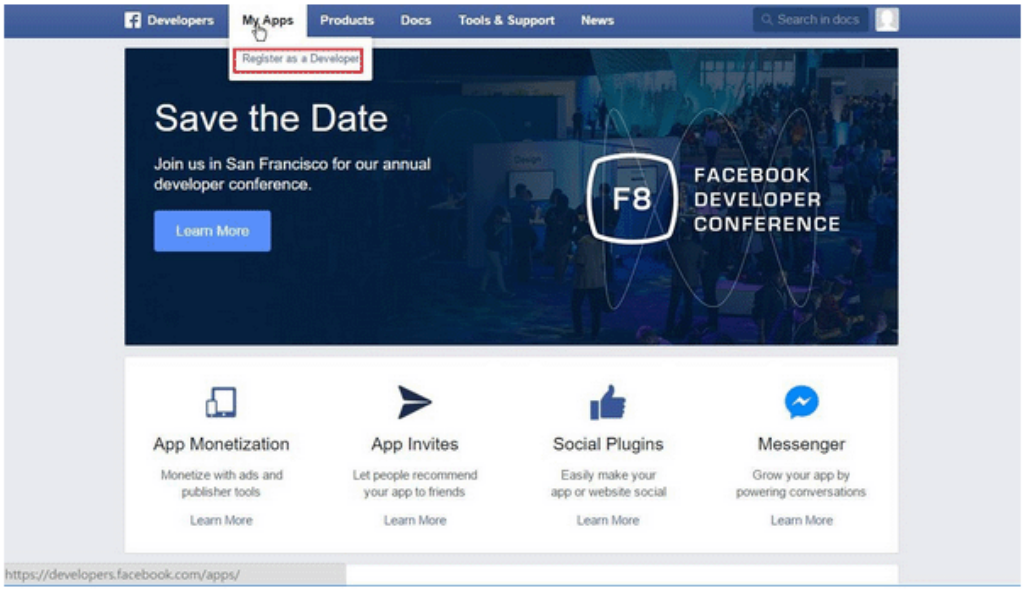
完成設定之後，按下**確定**按鈕儲存相關設定。

應用說明

A-1 如何建立臉書 APP ID 以利網頁入口驗證？

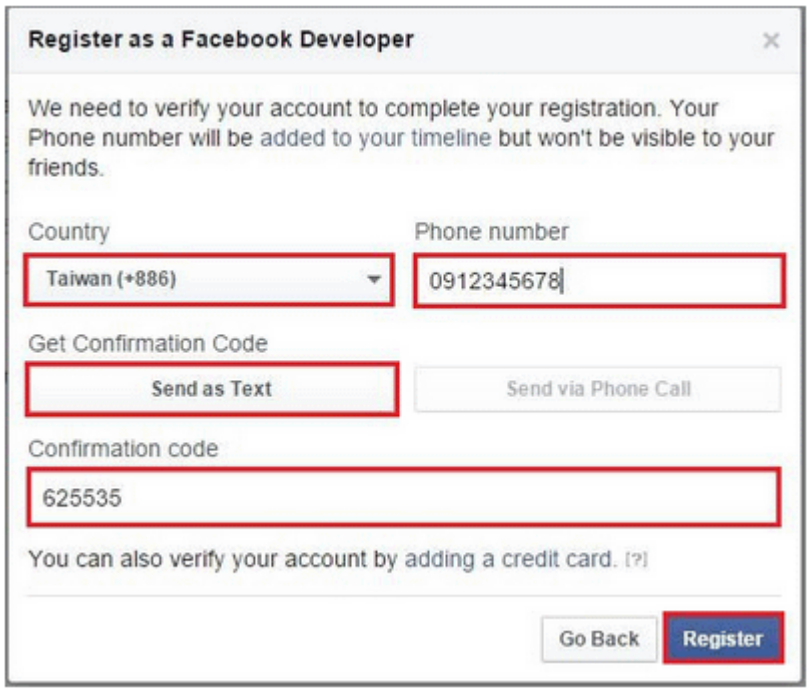
入口網站的新功能支援社群登入作為驗證的方式，並允許網路管理者透過 Google 或臉書帳號來驗證 LAN 端用戶，本文將告訴您如何在入口網站設定頁面中建立臉書 APP 並產生 APP ID 以及 APP 密鑰。

1. 請註冊為 FB 開發人員，請前往 https://developers.facebook.com/ 並登入臉書帳號。
2. 以臉書帳號註冊為開發人員(若帳號先前已經查證過，本步驟可以省略)。
3. 按下 **My Apps** 接著選擇 **Register as Developer**。

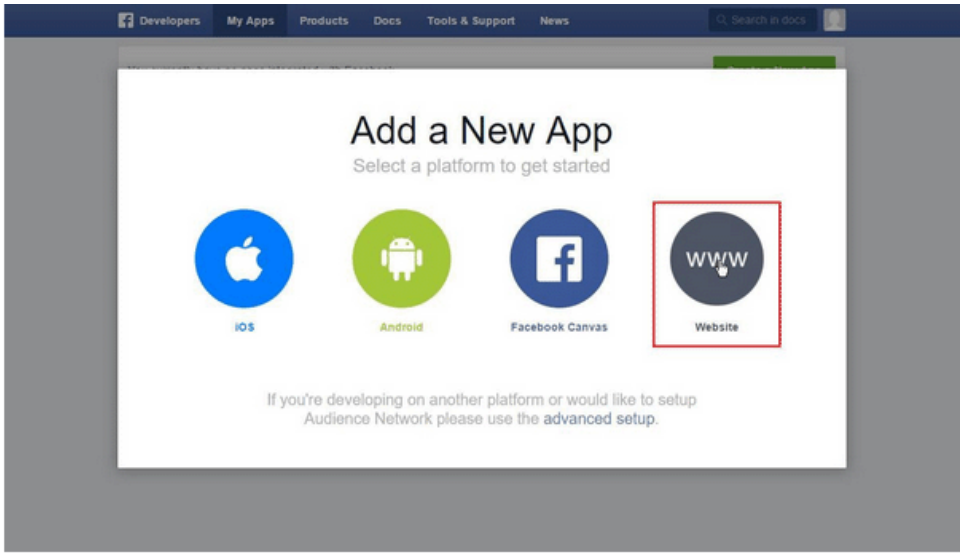


4. 切換到 **YES** 然後於跳出視窗上點選下一頁 **Next**。

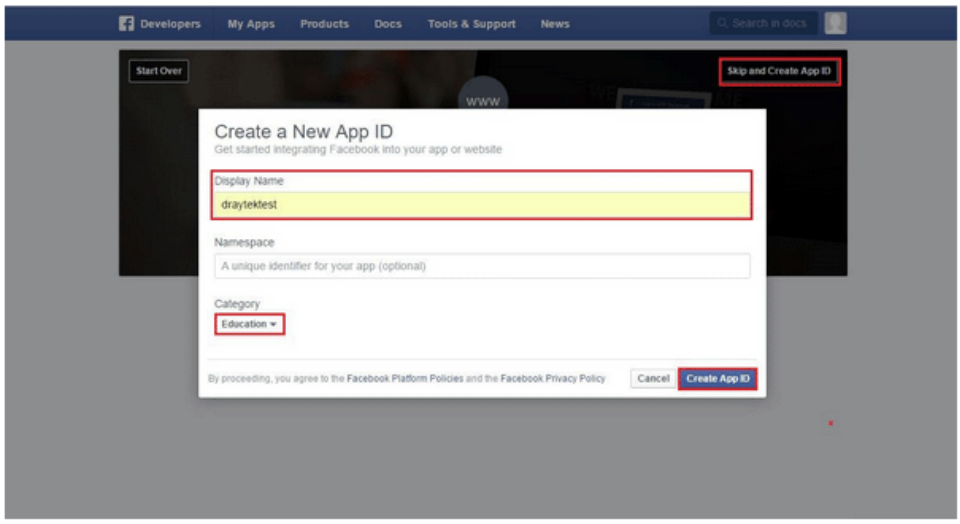
5. 選擇國別 **country** 再輸入電話號碼 **Phone number**，於取得確認碼欄位中按 **Send as Text**，等收到確認碼訊息後，輸入該確認碼。按下 **Register** 已完成註冊過程。



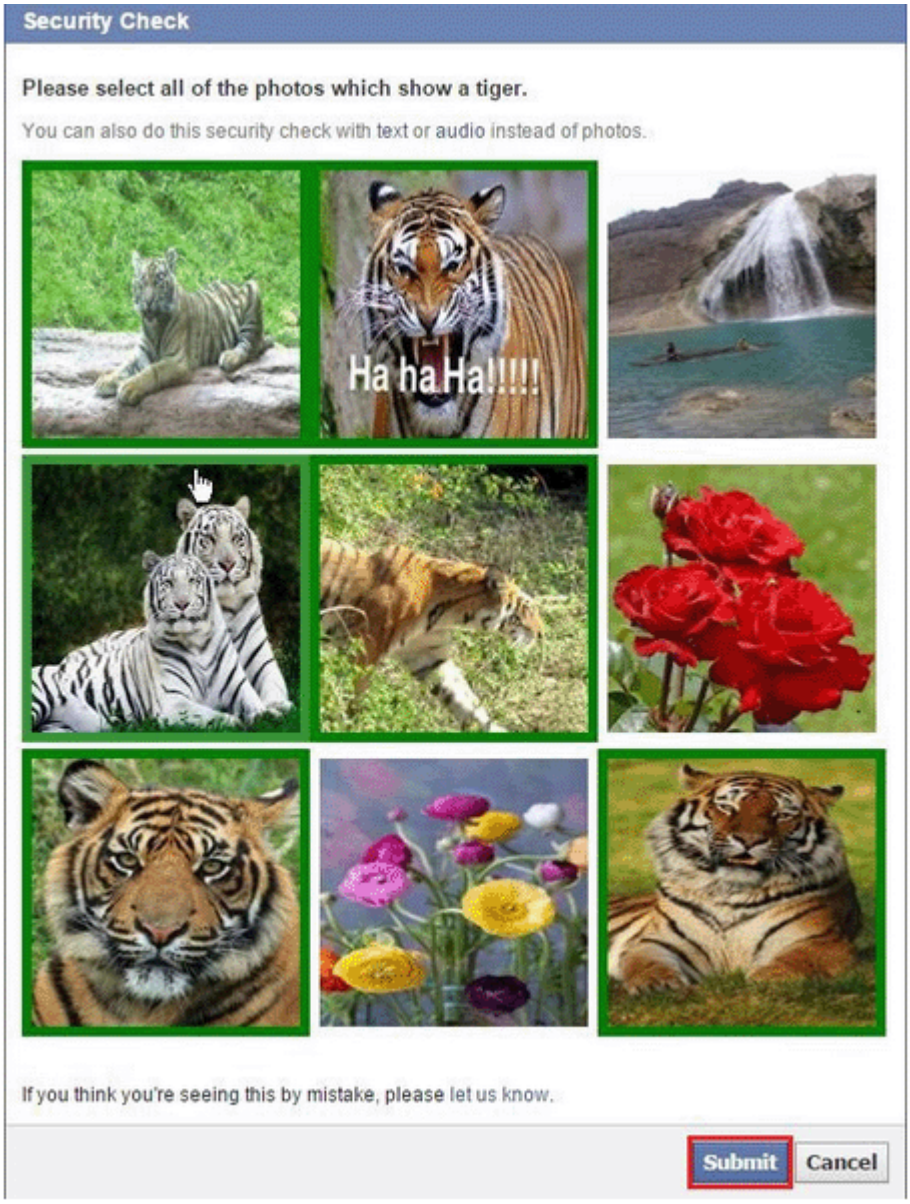
6. 新增一個 App，點選 **My Apps > Add a New App**，選擇 **Website** 平台。



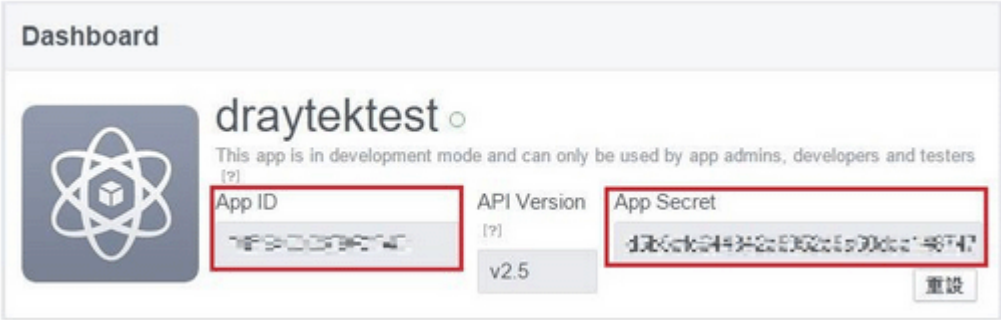
7. 若是第一次使用，請點選 **Skip and Create App ID**，輸入 **Display Name** 再選擇 **Category**。點選 **Create App ID**。



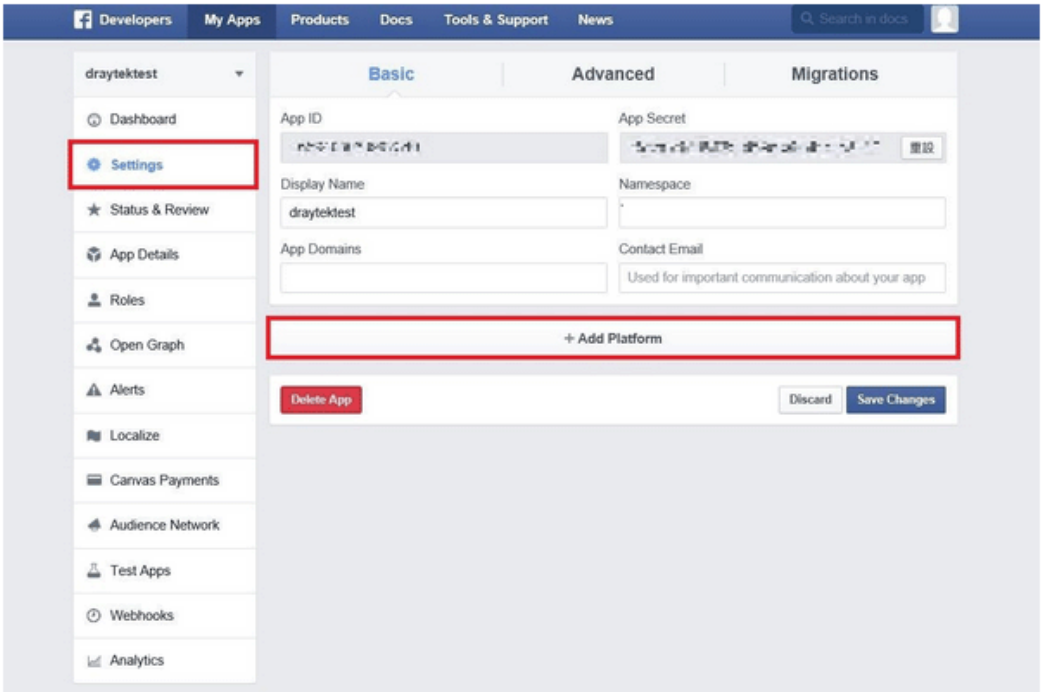
8. 安全性檢查視窗接著跳出，請依文意選擇，然後按 **Submit** 按鈕完成整個過程。



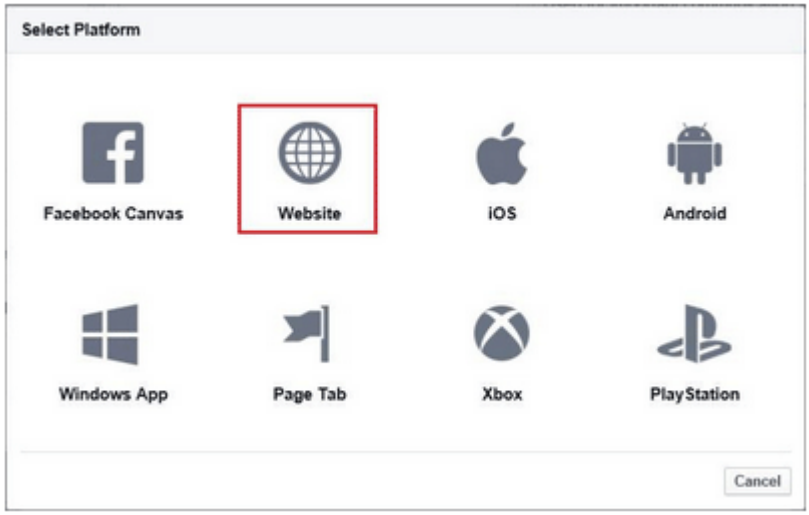
9. 在儀表板上，使用者可以取得 **App ID** 與 **App Secret**，這些資訊將被運用在路由器的入口網站設定上。



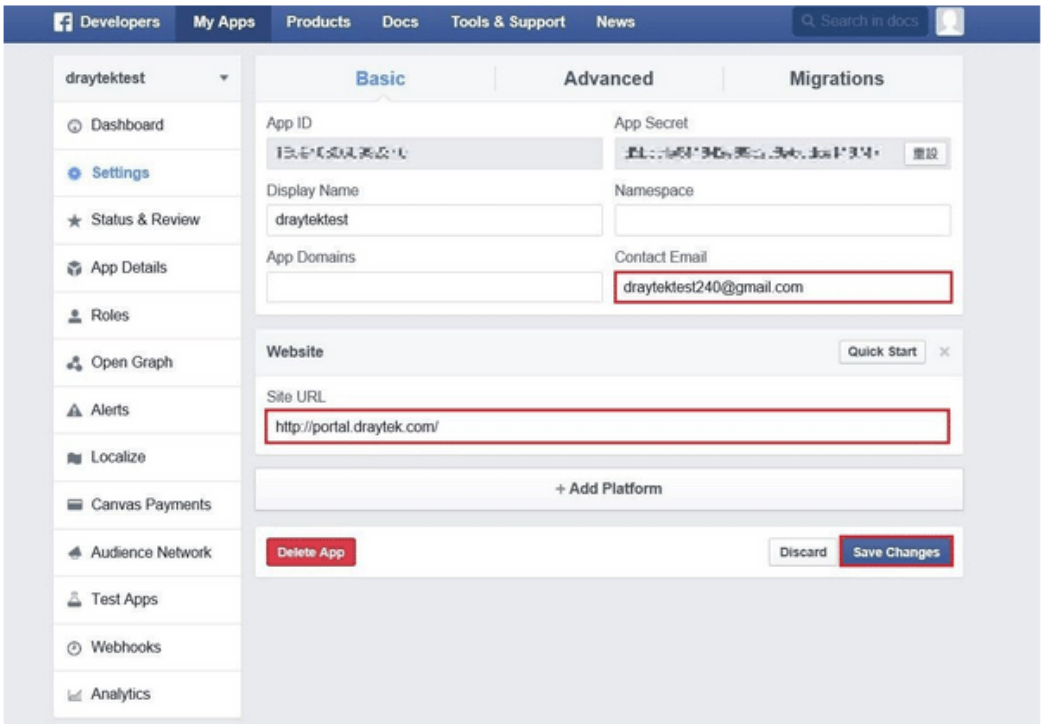
10. 在 My Apps 上新增平台，前往 **Settings** 並選擇 **Add Platform**。



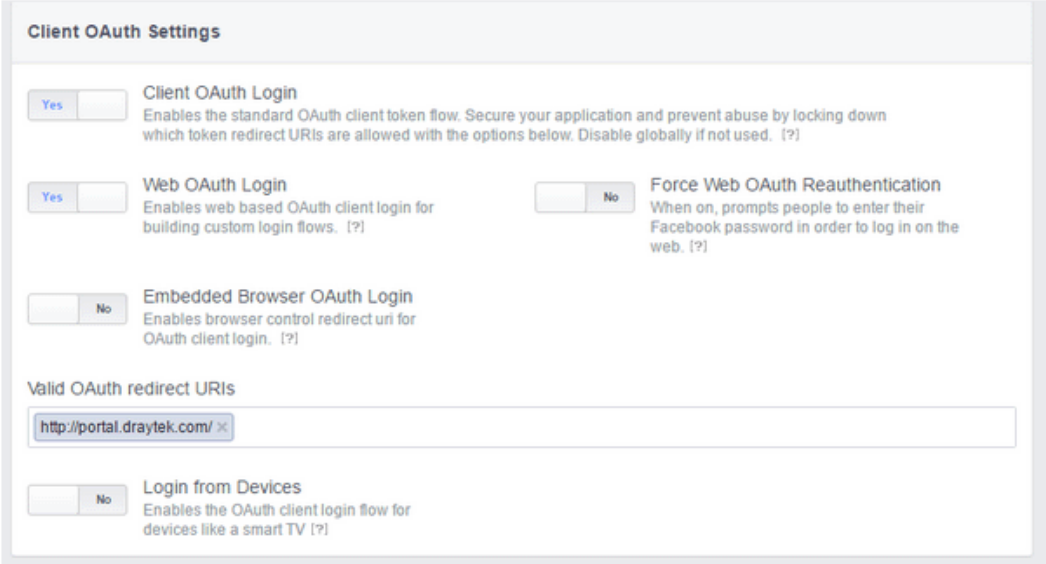
11. 選擇 **Website**。



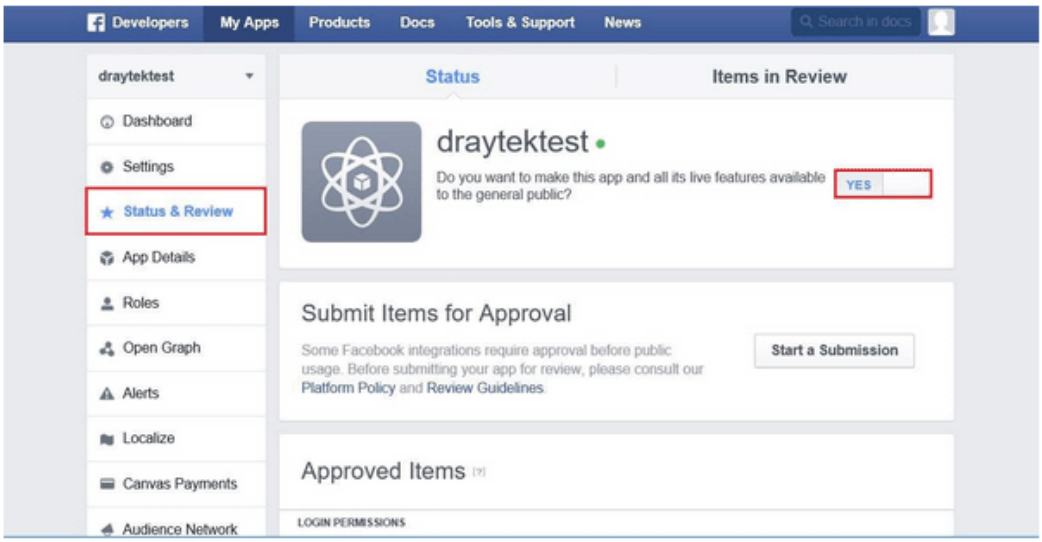
12. 輸入網站 **Site URL:** http://portal.draytek.com. (附註: 如果您改變了 http 埠號，請在 URL 中新增 http 埠號。例如我們使用 8080 做為 http 埠號，URL 連結為 http://portal.draytek.com:8080)，輸入連絡電子郵件 **Contact Email**，然後點選儲存變更 **Save Change**。



13. 設定用戶的 Client OAuth，請前往 **Settings** >> **Advanced** >>**Client OAuth Settings**，並在。**Valid OAuth redirect URI** 中輸入 "http://portal.draytek.com"。



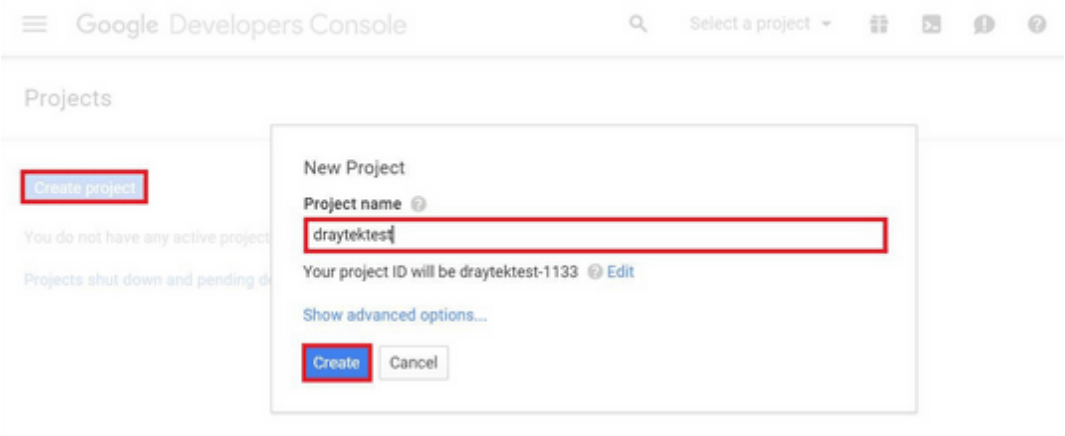
14. 前往 **My Apps>>Status & Review**，切換可用狀態為 **YES** 以便啟動 APP。


Developers
My Apps
Products
Docs
Tools & Support
News
Search in docs
draytektest
Dashboard
Settings
Status & Review
App Details
Roles
Open Graph
Alerts
Localize
Canvas Payments
Audience Network
Status
Items in Review
draytektest
Do you want to make this app and all its live features available to the general public?
YES
Submit Items for Approval
Some Facebook integrations require approval before public usage. Before submitting your app for review, please consult our Platform Policy and Review Guidelines.
Start a Submission
Approved Items
LOGIN PERMISSIONS

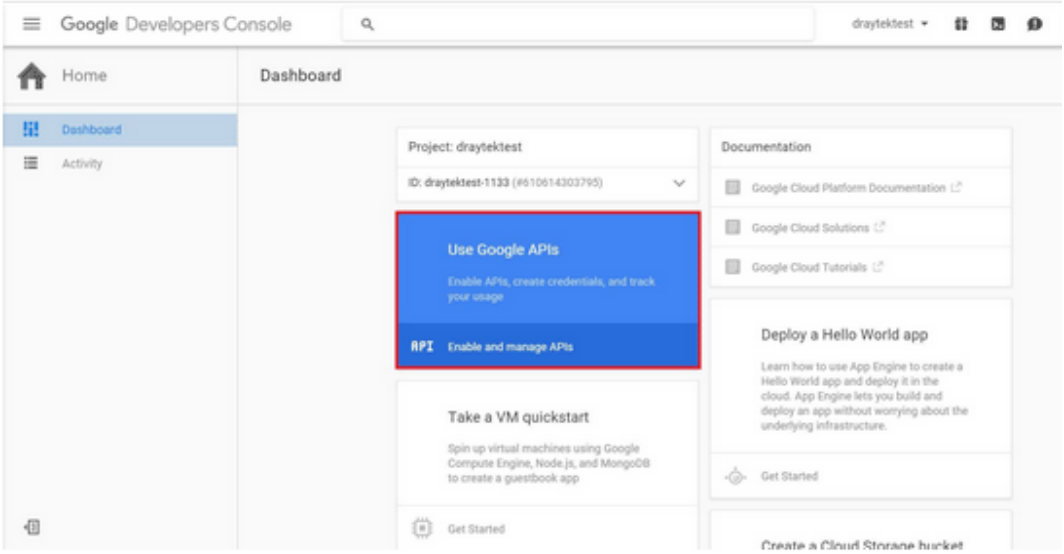
A-2 如何建立 Google APP ID 以利網頁入口驗證?

入口網站的新功能支援社群登入作為驗證的方式，並允許網路管理者透過 Google 或臉書帳號來驗證 LAN 端用戶，本文將告訴您如何在入口網站設定頁面中建立臉書 APP 並產生 APP ID 以及 APP 密鑰。

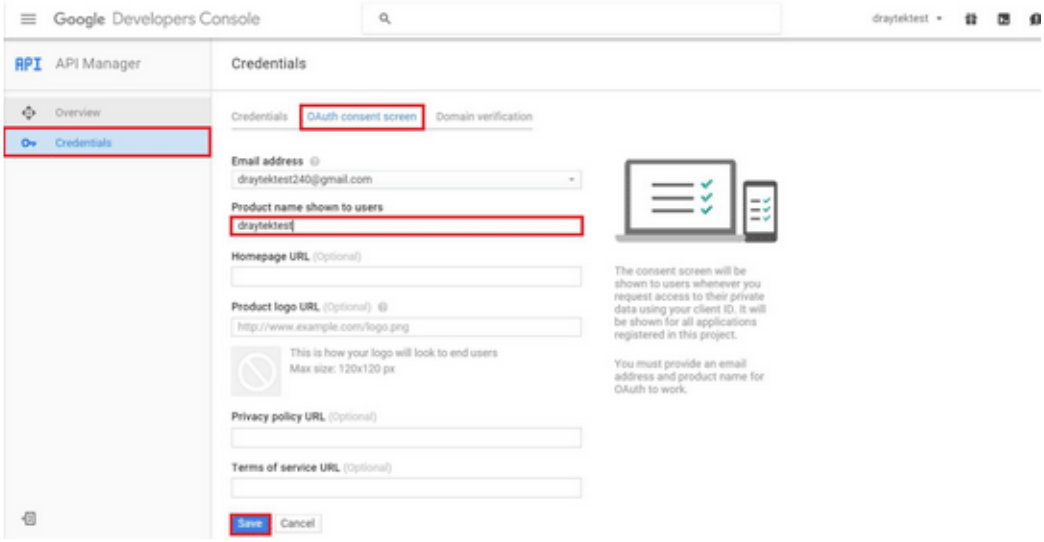
1. 建立開發商項目，前往 https://code.google.com/apis/console，以 Google 帳號登入然後按下建立項目 **Create project**，輸入項目名稱 **project name** 然後按建立 **Create**。



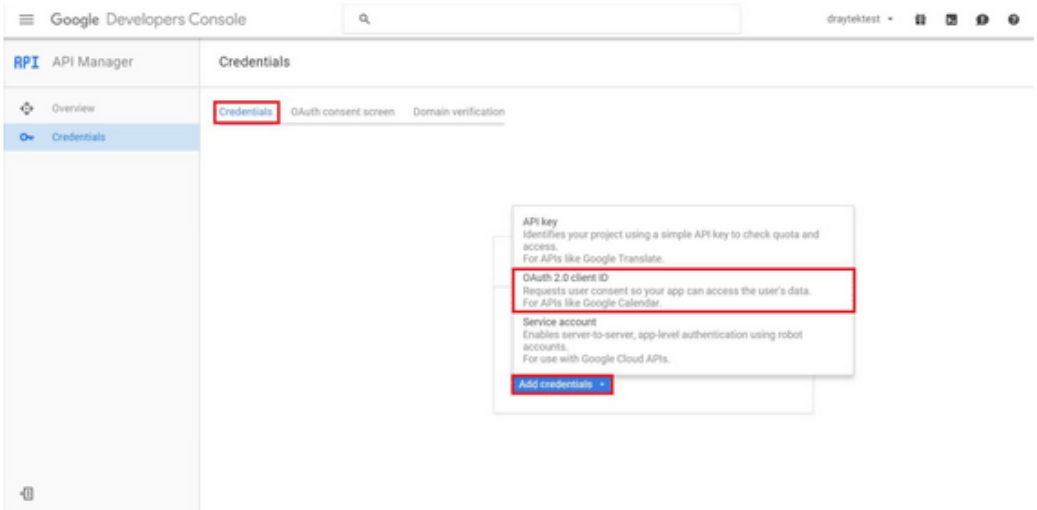
2. 在儀表板 Dashboard 上，選擇 **Use Google APIs**。



3. 編輯驗證同意頁面，前往 **Credentials > Auth consent screen**，輸入電郵 **email**、產品名稱 **product name** 和其他選擇項目，然後按 **Save**。



4. 建立用戶端 Client ID，按 **Credentials** 並選擇 **Add credentials > OAuth2.0 client ID**。



5. 選擇 **Web application** 做為驗證類型，然後輸入名稱 **name**，設定 **Authorized JavaScript origins** 以及設定 **Authorized redirect URLs** 為 http://portal.draytek.com 並按 **Create**。(附註：如果您變更路由器的 http 埠號，請在 URL 中加入 http 埠號，例如我們使用 8080 做為 http 埠號，如 http://portal.draytek.com:8080)。

6. 取得用戶端 **client ID** 與用戶密碼 **client secret**，相關資訊之後可用於路由器的入口網站設定中。

VI-5 中央管理(無線基地台 AP)

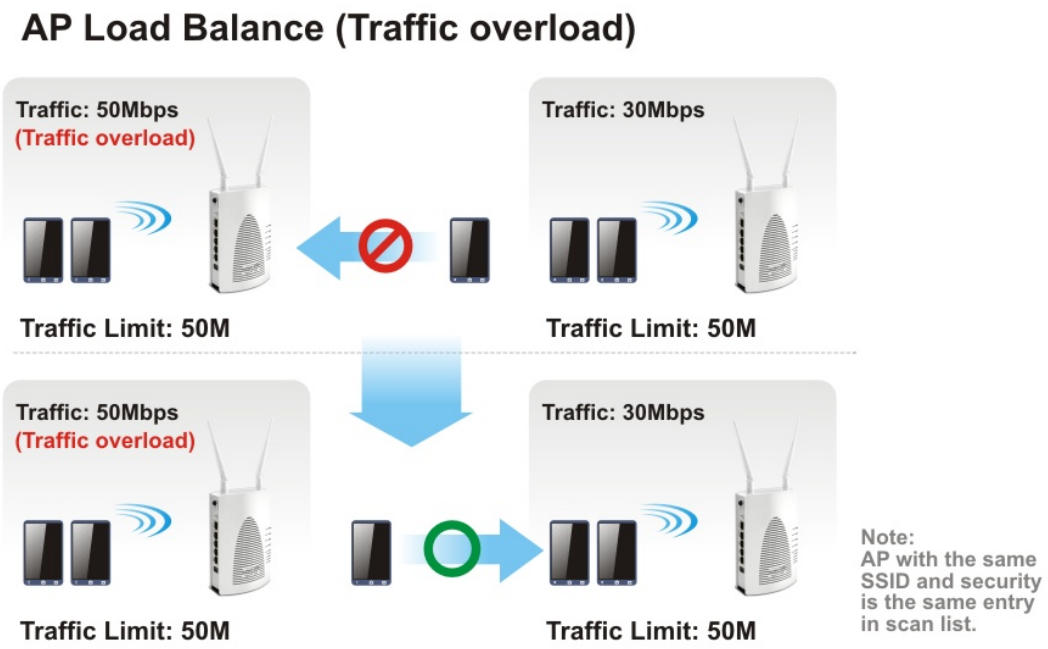
透過中央管理功能，Vigor2135 能管理支援 AP 管理特性的 VigorAP 基地台。

AP 維護

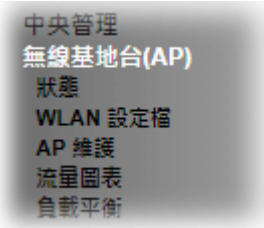
針對受管理的 AP，Vigor 路由器可執行設定備份、設定配置還原、韌體更新與遠端重啟等作業，無需登入基地台的網頁設定介面即可進行相關維護作業，對管理者而言，非常方便。

負載平衡

負載平衡的設定參數可以幫忙分配所有註冊至 Vigor 路由器的 AP 基地台的網路流量，這樣頻寬就不會被特定的基地台佔據過久。



網頁使用者介面



VI-5-1 狀態

頁顯示 Vigor 路由器所管理的基地台目前的狀態(包含連線、斷線或是隱藏 SSID、IP 位址、加密、頻道、版本、密碼等等資訊)。

可用設定說明如下：

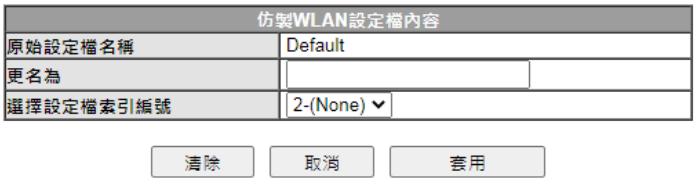
項目	說明
索引	按下索引編號連結以檢視 AP 基地台的設定總結。
裝置名稱	顯示 Vigor 路由器所管理的 AP 裝置名稱。
IP 位址	顯示 AP 基地台的 IP 位址。
SSID	顯示連接至路由器的 AP 基地台其使用的 SSID 內容。
頻道	顯示 AP 基地台使用的頻道。
正常運行時間(Uptime)	顯示 AP 啟用後持續的時間。
版本	顯示此 AP 基地台目前使用的韌體版本。
密碼	顯示路由器得以進入 AP 基地台取得所需的設定資訊的密碼。 此按鈕主要是用來修改登入連結之基地台的密碼。
細節內容	按此開啟另一個視窗，包含與這個項目的 AP 有關的詳細資訊。

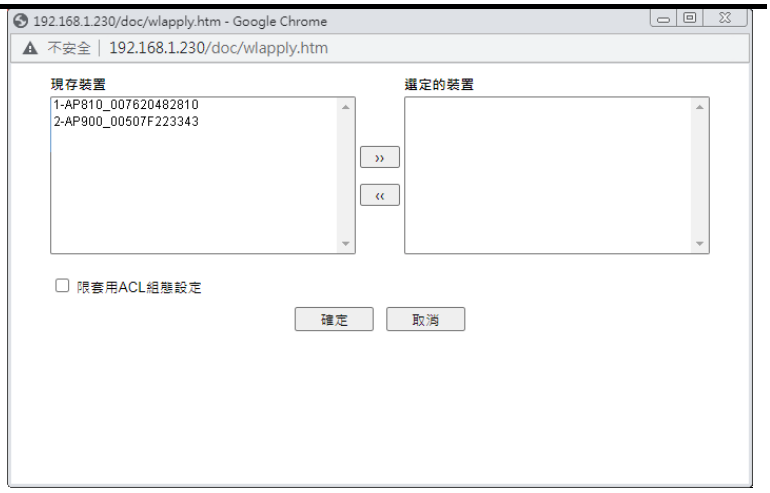
VI-5-2 WLAN 設定檔

無線網路(WLAN)設定檔可套用至選定的 AP 基地台，無需開啟基地台使用者介面即可變更基地台的設定，對於管理者而言，非常便利。

點選左邊的連結，可修改該設定檔的內容。

可用設定說明如下：

項目	說明
設定檔	顯示設定檔的連結。
名稱	顯示設定檔的名稱。 預設的設定檔名稱(Default)無法更改名稱。
主要 SSID	顯示此無線設定檔使用的 SSID 名稱。
安全性	顯示此無線設定檔選定的安全性模式。
多重 SSID	啟用表示多重 SSID 為活動狀態。 停用表示僅有 SSID1 為活動狀態。
WLAN ACL	顯示無線控制清單的名稱。
速率控制	顯示上傳與/或下載的傳輸速率。
仿製	用以自現有的 WLAN 設定檔複製相同的設定內容至另一個 WLAN 設定檔內。 請先勾選現有的 WLAN 設定檔作為原始設定檔，接著按下**仿製**按鈕，下面的對話盒將會出現：  然後，選擇準備套用的設定檔之索引編號，於**更名為**欄位中再輸入一個新的名稱，最後按下**套用**即可儲存相同的設定。 新的設定檔(含有原始設定檔的設定)即可完成建立。
至 AP	按此鈕可套用選定的無線設定檔至指定的 AP 基地台。

	 自**現存裝置**區域中選擇您想要的裝置，然後按**>>按**鈕將該選定裝置移往右邊的**選定的裝置**欄位，然後按下**確定**按鈕。 選定的無線區域網路設定檔將會立即套用至選定的基地台，之後該基地台會自行重新啟動。
至本機	本頁設定的設定檔主要是提供給連接至路由器的 VigorAP。 如有必要，這些設定也可以運用於路由器上。選擇並勾選無線設定檔，並按下此按鈕以便套用本頁設定至路由器的無線網路設定上。

如何編輯無線區域網路設定檔?

1. 選擇要編輯的設定檔(1 或 2)，按下其索引連結。
2. 相關頁面顯示如下。

中央管理 >> 無線基地台(AP) >> WLAN 設定檔

WLAN 設定檔編輯

裝置設定	
設定檔名稱	Default ☐ 自動規定
系統管理員	admin
密碼	•••••
第二子網	◉ 啟用 ○ 停用
管理VLAN	☐ 啟用管理VLAN功能: 區域網路(LAN)-A VLAN ID 0 (0 ~ 4095) 區域網路(LAN)-B VLAN ID 0 (0 ~ 4095)

WLAN 基本設定

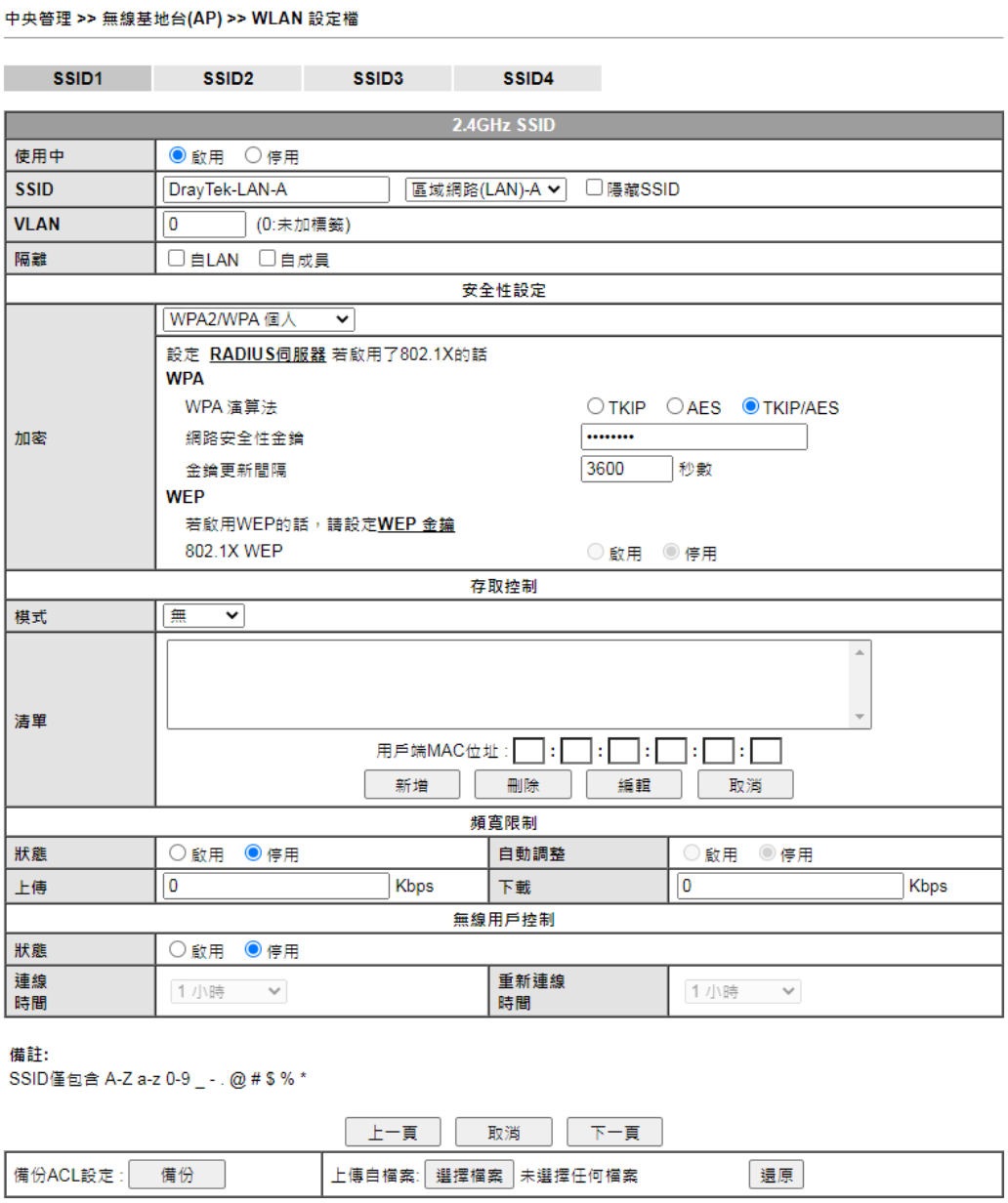
2.4GHz	5GHz	5GHz-2
無線區域網路	◉ 啟用 ○ 停用	
限制用戶端	☐ 啟用 64 (3 ~ 128, 預設值: 64)	
操作模式	無線基地台(AP)	
2.4G 模式	綜合 (11b+11g+11n)	
2.4G 頻道	2462MHz (頻道 11)	
無線頻寬均化	☐ 啟用無線頻寬均化功能: 觸發用戶端號碼 2 (2 ~ 128, 預設值: 2)	
頻段引導	☐ 啟用頻段引導功能: 無線用戶端5G能力的檢查時間 15 秒數 (1 ~ 60, 預設值: 15)	
漫遊中	☐ 最小基本速率 1 Mbps ◉ 停用RSSI需求 ○ 嚴格限制最小 RSSI - 73 dbm (42 %) (預設值: -73) ○ 最小 RSSI - 66 dbm (60 %) (預設值: -66) 含相鄰 AP RSSI 超過 5 dB (預設值: 5) ☐ 啟用快速漫遊(WPA2/802.1x): PMK 暫存期間 10 分鐘 (10 ~ 600, 預設值: 10)	
WMM	○ 啟用 ◉ 停用	
傳送電力	100%	
頻道寬度	自動 20/40 MHz	

備註:
1. 管理員僅可以包含 a-z A-Z 0-9 ,.;<>+=|?@~`$%_-*[]{}^!()
2. 密碼僅可包含a-z A-Z 0-9 ,.;<>+=\|?@#~`$%/_-*[]{}^!()
3. 5GHz-2頻之設定僅對三頻機種有效用
4. 如果因國別和型號之差異，套用了未支援之頻道，AP將會忽略此項變更

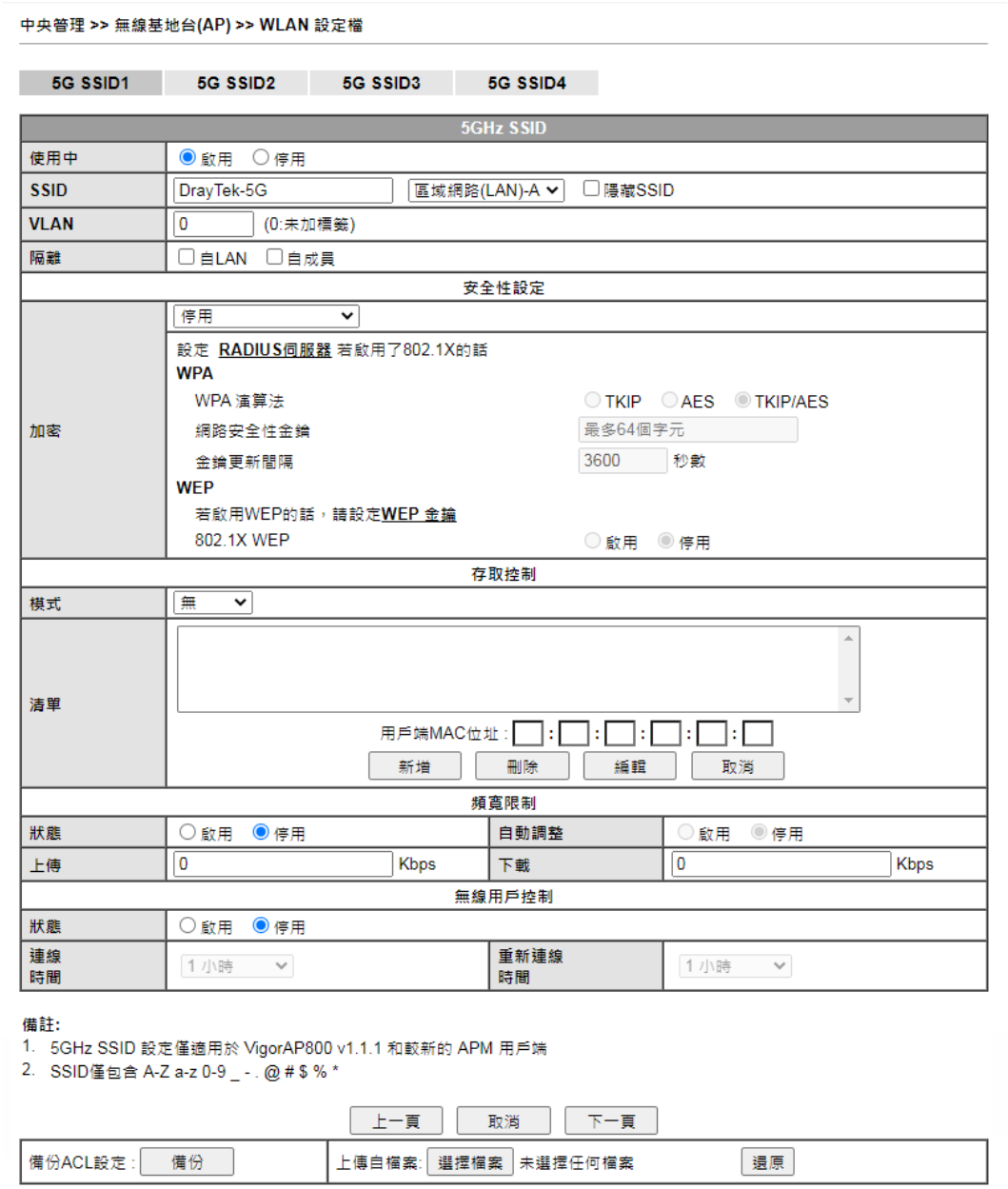
取消 下一頁

資訊 自動規定僅在 WLAN 的預設設定檔中可以使用。

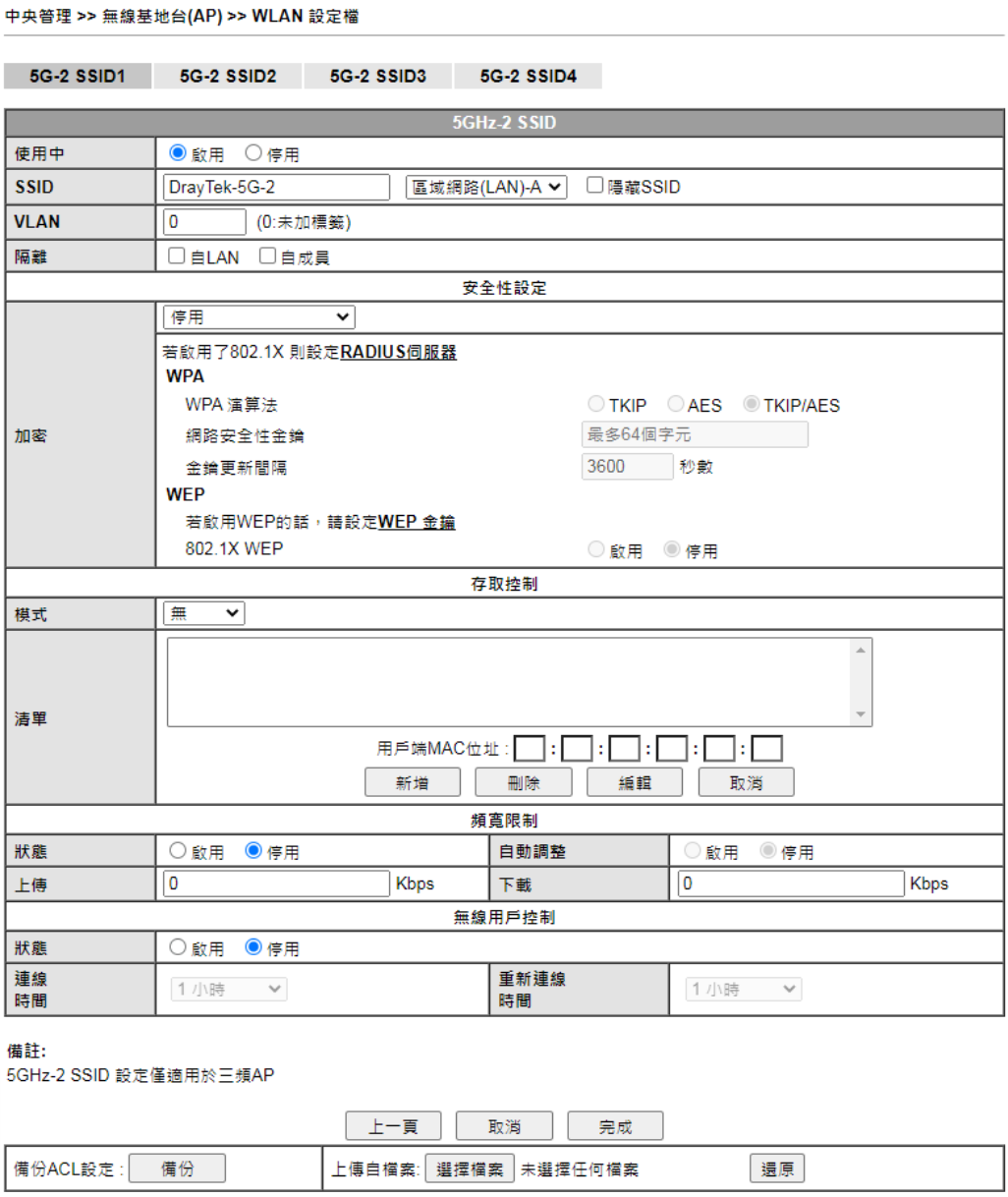
3. 完成基本設定之後，按**下一頁**開啟如下頁面進行 2.4GHz 無線安全性設定。



4. 完成上述的頁面設定之後，按**下一頁**開啟如下頁面進行 5GHz 無線安全性設定。



及 5GHz-2 無線安全性設定。



5. 完成 5G 無線安全性設定，請按**完成**結束頁面設定。修正後的無線設定檔將會顯示在網頁上。

VI-5-3 AP 維護

針對受管理的 AP，Vigor 路由器可執行設定備份、設定配置還原、韌體更新與遠端重啟等作業，無需登入基地台的網頁設定介面即可進行相關維護作業，對管理者而言，非常方便。

資訊	透過路由器進行 AP 設定備份一次只能針對一台 AP 進行，其他的功能(如設定還原、韌體更新與遠端重啟則可一次針對數台 AP 進行)。

可用設定說明如下：

項目	說明
動作類型	有四種動作可以進行，分別是 Config 設定備份、Config 設定還原、韌體升級與遠端重啟以及出廠預設。 路由器可以備份選定 AP 的設定，還原選定 AP 的設定，執行選定 AP 的韌體更新，遠端重新啟動選定 AP，以及回復選定 AP 的出廠預設值。
檔案/路徑	指定 **Config 設定還原**以及**韌體升級**作業需求之檔案與路徑。
現存裝置	顯示路由器管理下的現有的 AP 基地台，按下<<或是>>按鈕讓選定的 AP 於左邊現存裝置區域或右邊選定裝置區域之間移動。
選定的裝置	顯示按下確定按鈕後，將套用此功能的基地台名稱。

完成上述設定之後，按下**確定**儲存並執行相關作業。

VI-5-4 流量圖表

選擇流量圖表可開啟如下頁面，選擇一台受管理的 AP 基地台(LAN-A 或是 LAN-B)，每日或是每週，以便檢視資料傳輸圖表。按下**更新頁面**可以隨時重新整理顯示的頁面。

水平軸代表時間；垂直軸代表傳輸速率(單位 kbps)。

資訊	啟用/停用此功能將會啟用/停用外接裝置功能。

VI-5-5 負載平衡

負載平衡的設定參數可以幫忙分配所有註冊至 Vigor 路由器的 AP 基地台的網路流量，這樣頻寬就不會被特定的基地台佔據過久。

可用設定說明如下：

項目	說明
AP 負載平衡(	此選項用來決定系統用來偵測過載已啟用負載平衡的模式。 **依無線用戶數(**- 負載平衡乃依照本頁設定的無線用戶數目為基準來執行，此項設定可用來限制連接至基地台的無線用戶總數，目的是要避免同時段過多的無線用戶連接至AP基地台造成網路塞車不平衡。 **依流量** – 依照本頁的流量設定執行負載平衡的運作。 **依無線用戶數或流量**-負載平衡的操作依照無線用戶數或是網路流量限制而定。
無線用戶數門檻	設定無線用戶數目，作為啟用 AP 負載平衡功能的門檻值。
流量門檻	**上傳限制** – 使用下拉式清單指定上傳的網路流量限制。 **下載限制** – 使用下拉式清單指定下載的網路流量限制。
當超過門檻限制時採取的措施動作	**停止接受新的連線** – 當無線站台數或是流量達到了設定的門檻值時，路由器將會停止接受任何其他基地台的連線要求。 **分離閒置時間最長之現有無線用戶**- 當 AP 過載時(例如達到無線

	站台數或是流量的門檻值)，將會中止長期閒置未連線的無線用戶站台。 **分離訊號強度最差之現有無線用戶-** 當 AP 過載時(例如達到無線站台數或是流量的門檻值)，將會中止訊號強度最弱的無線站台之網路連線。
選擇以套用	決定哪個 AP 應該套用負載平衡。 **全部 AP** – 全部的基地台 AP 都將套用負載平衡。 **指定 AP** – 負載平衡功能套用到指定的 AP 上。

完成設定之後，按下**確定**按鈕儲存相關設定。

VI-6 中央管理(外接裝置)

Vigor 路由器可以用來連結不同類型的外接裝置，為了方便管理這些外接裝置，請開啟**外接裝置**以便進行細部設定。

可用設定說明如下：

項目	說明
外接裝置 Syslog	勾選此方塊以便在 Syslog 上顯示被偵測裝置的相關資訊。
外接裝置自動搜尋	勾選此方塊可以讓系統自動偵測外接裝置並顯示在本頁面上。

從這個網頁當中，勾選外接裝置自動搜尋方塊，稍後，所有可用的裝置都將會呈現在螢幕上，並以小圖示顯示。

完成上述設定之後，按**確定**儲存設定。

資訊 路由器透過此功能所偵測出來的裝置僅包含居易的產品。

第七篇 其他設定

Objects Settings

定義物件如 IP 位址、服務類型、關鍵字、檔案副檔名及其他等等，這些事先預定的物件可以套用在 CSM 中。

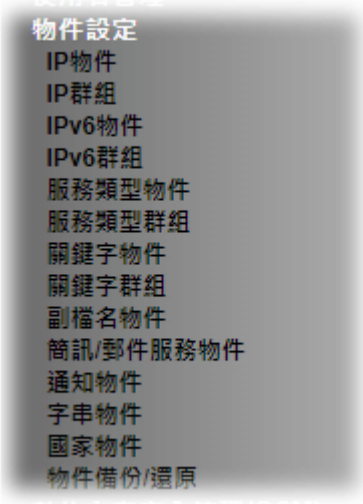
USB

連接至路由器的 USB 裝置可以視之為伺服器或是 WAN 介面，藉由路由器，LAN 端的用戶可以存取、寫入以及讀取儲存在 USB 磁碟內的資料。

VII-1 物件設定

定義物件如 IP 位址、服務類型、關鍵字、檔案副檔名及其他等等，這些事先預定的物件可以套用在 CSM 中。

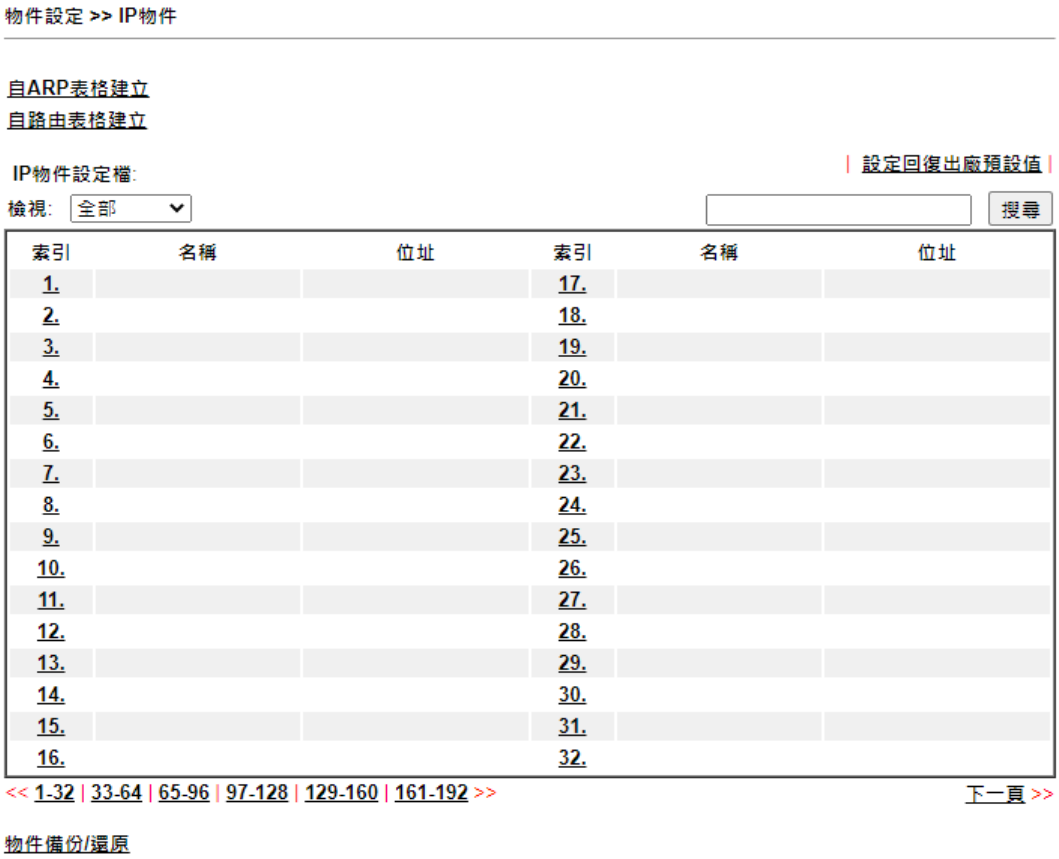
網頁使用者介面



VII-1-1 IP 物件

對某些範圍內的 IP 和侷限於特定區域的服務通訊埠，通常可以套用於路由器網頁設定中。因此我們可以將他們定義成為物件，並結合成群組以便後續能方便的應用。之後，我們可以選擇該物件/群組來套用，比方說，相同部門內所有的 IP 可定義成為一個 IP 物件(意即 IP 位址範圍)。

您可設定 192 組不同條件的 IP 物件。



可用設定說明如下：

項目	說明
檢視	使用下拉式清單選擇類型(單一位址、範圍位址、子網位址、MAC 位址或是全部)。與該類型相關的 IP 物件將顯示在頁面上。
設定回復出廠預設值	清除全部的設定資料。
搜尋	輸入您想要搜尋之 IP 物件的代表字串。
索引	顯示您可以設定的設定檔索引編號。
名稱	顯示物件設定檔的檔名。
位址	顯示物件設定檔中設定的 IP 位址。
物件備份/還原	按此備份或是還原 IP 物件。

如欲建立新的設定檔，請依下述步驟進行：

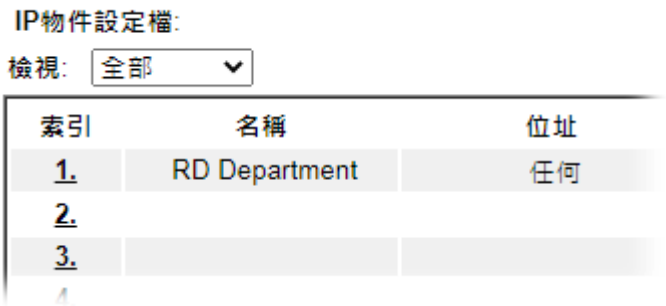
1. 在索引編號欄位中選擇一個號碼(例如 #1)以便設定細節內容。
2. 設定頁面顯示如下：

可用設定說明如下：

項目	說明
名稱	請輸入本設定檔的名稱，最多可以輸入 15 個字元。
介面	請選擇適當的介面。 例如，**防火牆>>編輯過濾器組別>>編輯過濾器規則**中的**方向**設定會要求您針對 WAN 或 LAN/RT/VPN 介面或是任何 IP 位址，指定一個 IP 或是 IP 範圍，或是任何的 IP 位址，如果您選擇 LAN/RT/VPN 作為介面，並選擇 LAN/RT/VPN 作為**編輯過濾器規則**中的**方向**設定，那麼所有的 LAN/RT/VPN 介面的 IP 位址通通都會開放予您在**編輯過濾器規則**頁面上選擇。
位址類型	決定 IP 位址的位址類型。 如果物件僅包含 IP 位址的話，請選擇**單一位址**。 如果物件包含某個範圍內數個 IP 位址的話，請選擇**範圍位址**。 如果物件包含 IP 位址的子網路的話，請選擇**子網位址**。 如果物件包含任何一種 IP 位址的話請選擇**任何位址**。 如果物件包含任何一種 MAC 位址的話請選擇 **MAC 位址**。

MAC 位址	如果選擇的是 **MAC 位址**類型，請輸入網卡的 MAC 位址。
起始 IP 位址	輸入單一位址類型所需的起始 IP 位址。
結束 IP 位址	如果選擇的是範圍位址類型，請輸入結束 IP 位址。
子網遮罩	如果選擇的是子網位址類型，請輸入子網路遮罩位址。
反向選擇	如果勾選此項的話，除了上面所提及的以外，其他的 IP 位址將會在被選擇之後全部套用上設定內容。

4. 完成設定之後，按下**確定**按鈕儲存相關設定。下表為 IP 物件設定的範例之一。



VII-1-2 IP 群組

本頁可讓您綁定數個 IP 物件成為一個 IP 群組。

物件設定 >> IP群組

IP群組表格: | 設定回復出廠預設值 |

索引	名稱	索引	名稱
1.		17.	
2.		18.	
3.		19.	
4.		20.	
5.		21.	
6.		22.	
7.		23.	
8.		24.	
9.		25.	
10.		26.	
11.		27.	
12.		28.	
13.		29.	
14.		30.	
15.		31.	
16.		32.	

物件備份/還原

可用設定說明如下：

項目	說明
設定回復出廠預設值	清除全部的設定資料。
索引	顯示您可以設定的設定檔索引編號。
名稱	顯示物件設定檔的檔名。
物件備份/還原	按此備份或是還原 IP 群組物件。

如欲建立新的設定檔，請依下述步驟進行：

1. 在索引編號欄位中選擇一個號碼(例如 #1)以便設定細節內容。

2. 設定頁面顯示如下：

可用設定說明如下：

項目	說明
名稱	請輸入本設定檔的名稱，最多可以輸入 15 個字元。
介面	請選擇適當的介面(WAN, LAN 或是任何一種)以顯示所有指定介面內的 IP 物件。
可用 IP 物件	所有選定之指定介面中可用的 IP 物件全都會顯示在此方塊中。
選定的 IP 物件	按下 **>>** 按鈕來新增選定 IP 物件並呈現在此方塊內。

3. 完成設定之後，按下**確定**按鈕儲存相關設定。

VII-1-3 IPv6 物件

您可設定 64 組不同條件的 IPv6 物件。

物件設定 >> IPv6物件

IPv6物件設定檔: | 設定回復出廠預設值 |

索引	名稱	索引	名稱
1.		17.	
2.		18.	
3.		19.	
4.		20.	
5.		21.	
6.		22.	
7.		23.	
8.		24.	
9.		25.	
10.		26.	
11.		27.	
12.		28.	
13.		29.	
14.		30.	
15.		31.	
16.		32.	

<< 1-32 | 33-64 >> 下一頁 >>

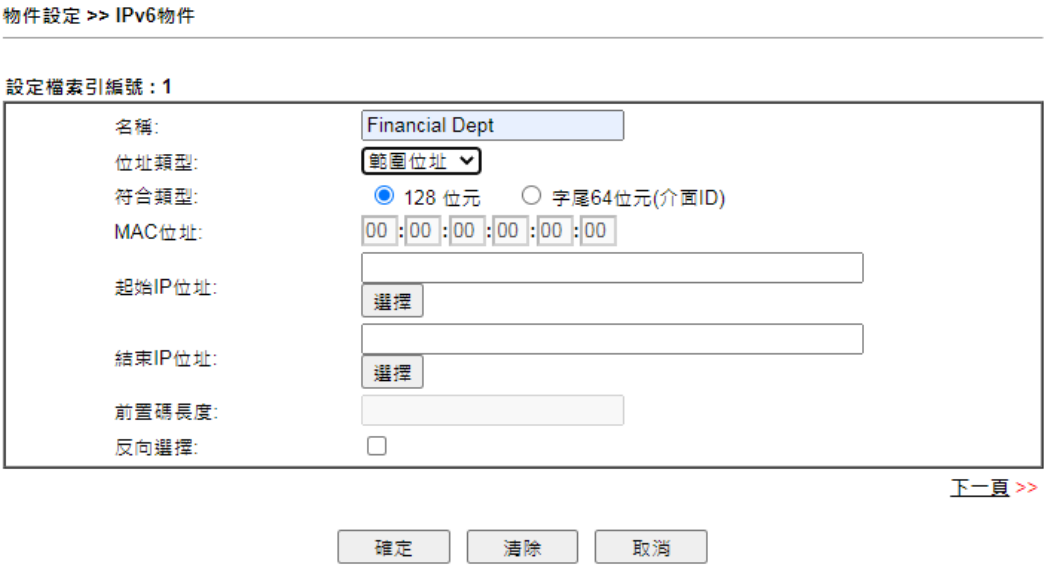
物件備份/還原

可用設定說明如下：

項目	說明
設定回復出廠預設值	清除全部的設定資料。
索引	顯示您可以設定的設定檔索引編號。
名稱	顯示物件設定檔的檔名。
物件備份/還原	按此備份或是還原 IPv6 物件。

如欲建立新的設定檔，請依下述步驟進行：

1. 在索引編號欄位中選擇一個號碼(例如 #1)以便設定細節內容。
2. 設定頁面顯示如下：



可用設定說明如下：

項目	說明
名稱	輸入設定檔名稱。
位址類型	決定 IPv6 的位址類型。 如果此物件僅含一組 IPv6 位址，請選擇**單一位址**。 如果此物件包含數個 IPv6 位址，請選擇**範圍位址**。 如果此物件包含一個 IPv6 子網路位址，請選擇**子網位址**。 如果此物件包含任何一個 IPv6 位址，，請選擇**任何位址**。 如果此物件包含 MAC 位址，請選擇 **MAC 位址**。
MAC 位址	輸入網卡的 MAC 位址。
起始 IP 位址	輸入單一位址/範圍位址的起始 IP 位址。
結束 IP 位址	如果選擇範圍位址，請在此輸入結束 IP 位址。
前置號碼長度	輸入 IPv6 位址的前置號碼長度值(例如 64)。
反向選擇	若勾選此項，除了上述以外，全部的 IPv6 位址都將套用此物件規則。

3. 完成設定之後，按下**確定**按鈕儲存相關設定。

VII-1-4 IPv6 群組

本頁可讓您綁定數個 IPv6 物件成為一個 IPv6 群組。

物件設定 >> IPv6群組

IPv6群組表格: | 設定回復出廠預設值 |

索引	名稱	索引	名稱
1.		17.	
2.		18.	
3.		19.	
4.		20.	
5.		21.	
6.		22.	
7.		23.	
8.		24.	
9.		25.	
10.		26.	
11.		27.	
12.		28.	
13.		29.	
14.		30.	
15.		31.	
16.		32.	

物件備份/還原

可用設定說明如下：

項目	說明
設定回復出廠預設值	清除全部的設定資料。
索引	顯示您可以設定的設定檔索引編號。
名稱	顯示物件設定檔的檔名。
物件備份/還原	按此備份或是還原 IPv6 群組物件。

如欲建立新的設定檔，請依下述步驟進行：

1. 在索引編號欄位中選擇一個號碼(例如 #1)以便設定細節內容。
2. 設定頁面顯示如下：

物件設定 >> IPv6群組

設定檔索引編號：1

名稱:

可用IPv6物件

選定的IPv6物件 (最多 8)

確定 清除 取消

可用設定說明如下：

項目	說明
名稱	請輸入本設定檔的名稱，最多可以輸入 15 個字元。
可用 IPv6 物件	所有可用的 IPv6 物件全都會顯示在此方塊中。
選定的 IPv6 物件	按下 **>>** 按鈕來新增選定 IP IPv6 物件並呈現在此方塊內。

3. 完成設定之後，按下**確定**按鈕儲存相關設定。

VII-1-5 服務類型物件

您可設定 96 組不同條件的服務類型物件。

物件設定 >> 服務類型物件

服務類型物件設定檔: | 設定回復出廠預設值 |

索引	名稱	索引	名稱
1.		17.	
2.		18.	
3.		19.	
4.		20.	
5.		21.	
6.		22.	
7.		23.	
8.		24.	
9.		25.	
10.		26.	
11.		27.	
12.		28.	
13.		29.	
14.		30.	
15.		31.	
16.		32.	

<< 1-32 | 33-64 | 65-96 >> 下一頁 >>

物件備份/還原

可用設定說明如下：

項目	說明
設定回復出廠預設值	清除全部的設定資料。
索引	顯示您可以設定的設定檔索引編號。
名稱	顯示物件設定檔的檔名。
物件備份/還原	按此備份或是還原服務類型物件。

如欲建立新的設定檔，請依下述步驟進行：

1. 在索引編號欄位中選擇一個號碼(例如 #1)以便設定細節內容。
2. 設定頁面顯示如下：

可用設定說明如下：

項目	說明
名稱	輸入此設定檔的名稱。
通訊協定	此設定檔準備套用的通訊協定。 **任何** – 全部的通訊協定。 **ICMP** – 為網際網路控制訊息協定(Internet Control Message Protocol) 的縮寫。 **IGMP** – 為網際網路群組管理協定(Internet Group Management Protocol) 的縮寫。 **TCP** – 為傳輸控制協定(Transmission Control Protocol) 的縮寫。 **UDP** –為用戶資料報協定(User Datagram Protocol) 的縮寫。 **TCP/UDP** –為 Transmission Control Protocol and User Datagram Protocol 的縮寫。 **其他** – 其他未列入上表清單中的協定，請在文字區輸入協定編號。
來源/目的埠號	**來源通訊埠**與**目標通訊埠**欄位皆為 TCP/UDP 可用之通訊埠，如果是其他的通訊協定，這些欄位即可省略，過濾器規則將可過濾任何一種通訊埠號。 *(=)* – 當第一與最後的數值相同時，此符號表示一個通訊埠。當第一與最後的數值不同時，此符號表示此設定檔所適用的通訊埠號範圍。 *(!=)* –當第一與最後的數值相同時，此符號表示除了這裡所指明的通訊埠以外，全都適用於此設定檔。當第一與最後的數值不同時，此符號表示所有的通訊埠除了此處所設定的範圍以外，全都適用於此設定檔。 *(>)* – 大於此數值的通訊埠號皆可使用。 *(<)* – 小於此數值的通訊埠號皆可使用。

3. 完成設定之後，按下**確定**按鈕儲存相關設定。

物件設定 >> 服務類型物件

服務類型物件設定檔:

索引	名稱
1.	www
2.	
3.	
4	

VII-1-6 服務類型群組

本頁可讓您綁定數個服務類型物件成為一個群組。

物件設定 >> 服務類型群組

服務類型群組表格: | 設定回復出廠預設值 |

群組	名稱	群組	名稱
1.		17.	
2.		18.	
3.		19.	
4.		20.	
5.		21.	
6.		22.	
7.		23.	
8.		24.	
9.		25.	
10.		26.	
11.		27.	
12.		28.	
13.		29.	
14.		30.	
15.		31.	
16.		32.	

物件備份/還原

可用設定說明如下：

項目	說明
設定回復出廠預設值	清除全部的設定資料。
索引	顯示您可以設定的設定檔索引編號。
名稱	顯示物件設定檔的檔名。
物件備份/還原	按此備份或是還原服務類型群組物件。

如欲建立新的設定檔，請依下述步驟進行：

1. 按下索引欄位下方的任一編號連結(例如 #1) 進入設定頁面。
2. 設定頁面顯示如下：

可用設定說明如下：

項目	說明
名稱	輸入此設定檔的名稱。
可用服務類型物件	您可以從 IP 物件頁面中先新增一些服務類型，所有可用的服務類型將會顯示在此區域中。
選定的服務類型物件	按下 **>>** 按鈕來新增選定服務類型並呈現在此方塊內。

3. 完成設定之後，按下**確定**按鈕儲存相關設定。

VII-1-7 關鍵字物件

您有 200 組關鍵字物件設定可供您在**數位內容安全管理(CSM)>>URL 網頁內容過濾器設定檔**中選擇作為黑白名單之用。

物件設定 >> 關鍵字物件

關鍵字物件設定檔: | 設定回復出廠預設值 |

索引	名稱	索引	名稱
1.		17.	
2.		18.	
3.		19.	
4.		20.	
5.		21.	
6.		22.	
7.		23.	
8.		24.	
9.		25.	
10.		26.	
11.		27.	
12.		28.	
13.		29.	
14.		30.	
15.		31.	
16.		32.	

<< 1-32 | 33-64 | 65-96 | 97-128 | 129-160 | 161-192 | 193-200 >> 下一頁 >>

物件備份/還原

可用設定說明如下：

項目	說明
設定回復出廠預設值	清除全部的設定資料。
索引	顯示您可以設定的設定檔索引編號。
名稱	顯示物件設定檔的檔名。
物件備份/還原	按此備份或是還原關鍵字物件。

如欲建立新的設定檔，請依下述步驟進行：

1. 在索引編號欄位中選擇一個號碼(例如 #1)以便設定細節內容。
2. 設定頁面顯示如下：

可用設定說明如下：

項目	說明
名稱	輸入此設定檔的名稱。
內容	輸入此設定檔的實際內容，例如可輸入 gambling。當您瀏覽網頁時，含有 gambling (賭博)等訊息之頁面就會被砍掉，並依照防火牆對此的設定放行/封鎖。

3. 完成設定之後，按下**確定**按鈕儲存相關設定。

VII-1-8 關鍵字群組

您可以將數個關鍵字物件組合成一個群組，此關鍵字群組可供您在**數位內容安全管理(CSM)>>URL 網頁內容過濾器設定檔**中選擇作為黑白名單之用。

物件設定 >> 關鍵字群組

關鍵字群組表格: | 設定回復出廠預設值 |

索引	名稱	物件	索引	名稱	物件
1.			17.		
2.			18.		
3.			19.		
4.			20.		
5.			21.		
6.			22.		
7.			23.		
8.			24.		
9.			25.		
10.			26.		
11.			27.		
12.			28.		
13.			29.		
14.			30.		
15.			31.		
16.			32.		

物件備份/還原

可用設定說明如下：

項目	說明
回復出廠預設值	清除全部的設定資料。
索引	顯示您可以設定的設定檔索引編號。
名稱	顯示物件設定檔的檔名。
物件	顯示此群組所包含的關鍵字物件檔案。
物件備份/還原	按此備份或是還原關鍵字群組。

如欲建立新的設定檔，請依下述步驟進行：

1. 在索引編號欄位中選擇一個號碼(例如 #1)以便設定細節內容。
2. 設定頁面顯示如下：

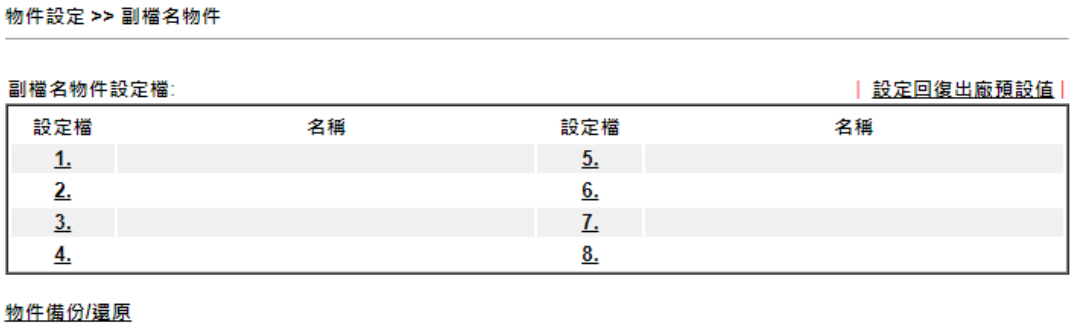
可用設定說明如下：

項目	說明
名稱	輸入此設定檔的名稱。
可用關鍵字物件	您可組合關鍵字物件成為一個關鍵字群組，所有可用的關鍵字物件都會顯示在本方塊區中。
選定的關鍵字物件	按 » 按鈕增加選定之關鍵字物件於本方塊區中。

3. 完成設定之後，按下**確定**按鈕儲存相關設定。

VII-1-9 副檔名物件

本頁允許您設定 8 組設定檔，這些設定檔將應用在**數位內容安全管理(CSM)>>URL 內容過濾器設定檔**中。設定檔中指定之所有含附檔名稱的檔案都可按照所選擇的動作來處理。



可用設定說明如下：

項目	說明
設定回復出廠預設值	清除全部的設定資料。
索引	顯示您可以設定的設定檔索引編號。
名稱	顯示物件設定檔的檔名。
物件備份/還原	按此備份或是還原副檔名物件。

如欲建立新的設定檔，請依下述步驟進行：

1. 按下索引欄位下方的任一編號連結(例如 #1) 進入設定頁面。

2. 設定頁面顯示如下：

可用設定說明如下：

項目	說明
設定檔名稱	請輸入此設定檔名稱。

3. 輸入設定檔名稱並勾選路由器會處理的副檔名項目，然後按**確定**儲存本頁的設定。

VII-1-10 簡訊/郵件服務物件

簡訊服務供應商

本頁讓您設定 10 組設定檔，後續將運用在**其他應用>>簡訊/郵件警示服務**中。

物件設定 >> 簡訊 / 郵件服務物件

簡訊服務供應商 | 郵件伺服器 | 設定回復出廠預設值 |

索引	設定檔名稱	簡訊服務供應商
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.	客製 1	
10.	客製 2	

物件備份/還原

每個項目說明如下：

項目	說明
設定回復出廠預設值	清除全部的設定資料。
索引	顯示您可以設定的設定檔索引編號。
設定檔名稱	顯示物件設定檔的檔名。
簡訊服務供應商	顯示提供簡訊服務的供應商名稱。
物件備份/還原	按此備份或是還原物件。

如欲建立新的設定檔，請依下述步驟進行：

1. 選擇簡訊供應商標籤欄，然後按下索引欄位下方的任一編號連結(例如 #1) 進入設定頁面。

簡訊服務供應商 | 郵件伺服器

索引	設定檔名稱
1.	
2.	
3.	
4.	

2. 設定頁面顯示如下：

可用設定說明如下：

項目	說明
設定檔名稱	請輸入此設定檔名稱。
服務供應商	使用下拉式清單選擇提供簡訊服務的服務供應商。
連線通訊協定	請指定 HTTP 或是 HTTPS。
使用者名稱	輸入發簡訊人員用來註冊選擇簡訊服務供應商所需的名稱。 使用者名稱長度不可超過 31 個字元。
密碼	輸入發簡訊人員用來註冊選擇簡訊服務供應商所需的密碼。密碼長度不可超過 31 個字元。
簡訊則數	輸入您自服務供應商所購得的簡訊則數。
傳送間隔	為了防止發信額度太早用罄，請輸入傳送簡訊所需的間隔時間。
傳送測試訊息	按此可依照上數設定傳送測試電子郵件。

3. 完成設定之後，按下**確定**按鈕儲存相關設定。

客製化簡訊服務(Customized SMS Service)

路由器提供數種簡訊服務供應商的名稱來供應簡訊服務，然而，如果您的服務供應商不在清單上，您可以透過索引編號 9 與 10 自行設定簡訊服務供應商的相關資料。編號 9 與 10 的設定檔名稱是固定無法改變的。

物件設定 >> 簡訊 / 郵件服務物件

簡訊服務供應商 | 郵件伺服器 | 設定回復出廠預設值

索引	設定檔名稱	簡訊服務供應商
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.	客製 1	
10.	客製 2	

物件備份/還原

按下索引編號 9 與 10 開啟設定頁面：

物件設定 >> 簡訊 / 郵件服務物件

設定檔索引編號: 9

設定檔名稱 Custom 1

服務供應商

最多255個字元

請聯絡您的簡訊服務供應商取得正確的URL字串

eg:bulksms.vsms.net:5567/eapi/submission/send_sms/2/2.0?username=###txtUser###&password=###txtPwd###&msisdn=###txtDest###&message=###txtMsg###

伺服器回應 最多31個字元

使用者名稱 最多31個字元

密碼 最多31個字元

額度 10

傳送間隔 3 (秒數)

備註:

1. 在"發送間隔"時間內只能發送一條消息。
2. 如果"發送間隔"設定為0，則沒有限制。

確定 清除 取消 傳送測試訊息

可用設定說明如下：

項目	說明
設定檔名稱	顯示設定檔名稱。
服務供應商	輸入服務供應商的網址。 在此項目的下方區塊中輸入 URL，您必須先與簡訊服務供應商聯絡以便獲得正確的 URL 字串。

伺服器回應	輸入簡訊服務供應商提供的 API 內容，可讓 Vigor 路由器認知已收到供應商所提的需求。
使用者名稱	輸入發簡訊人員用來註冊選擇簡訊服務供應商所需的名稱。 使用者名稱長度不可超過 31 個字元。
密碼	輸入發簡訊人員用來註冊選擇簡訊服務供應商所需的密碼。 密碼長度不可超過 31 個字元。
簡訊則數	輸入您自服務供應商所購得的簡訊則數。 注意，每則簡訊等於標準路由中所註記的簡訊文字訊息。
傳送間隔	為了防止發信額度太早用罄，請輸入傳送簡訊所需的間隔時間。
傳送測試訊息	按此可依照上數設定傳送測試電子郵件。

完成設定之後，按下**確定**按鈕儲存相關設定。

郵件伺服器

本頁讓您設定 10 組設定檔，後續將運用在**其他應用>>簡訊/郵件警示服務**中。

物件設定 >> 簡訊 / 郵件服務物件

簡訊服務供應商 | 郵件伺服器 | 設定回復出廠預設值 |

索引	設定檔名稱
1.	
2.	
3.	
4.	
5.	
6.	
7.	
8.	
9.	
10.	

物件備份/還原

可用設定說明如下：

項目	說明
設定回復出廠預設值	清除全部的設定資料。
索引	顯示您可以設定的設定檔索引編號。
設定檔名稱	顯示物件設定檔的檔名。
物件備份/還原	按此備份或是還原設定檔。

如欲建立新的設定檔，請依下述步驟進行：

1. 選擇郵件伺服器標籤欄，然後按下索引欄位下方的任一編號連結(例如 #1) 進入設定頁面。

2. 設定頁面顯示如下：

可用設定說明如下：

項目	說明
設定檔名稱	請輸入此設定檔名稱。
介面	選擇郵件傳送經由介面。
SMTP 伺服器	輸入郵件伺服器的 IP 位址。
SMTP 埠號	輸入 SMTP 伺服器需要的埠號。
傳送者位址	輸入寄件人的電子郵件位址。
使用 SSL	勾選使用 SSL 確保連線安全性。
驗證	郵件伺服器必須透過正確的使用者名稱與密碼來進行驗證，才有權利傳送訊息，請勾選方框啟用此功能。 **使用者名稱** – 請自訂驗證所需的使用者名稱。 **密碼** –請自訂驗證所需的密碼。
傳送間隔	請輸入傳送簡訊所需的間隔時間。

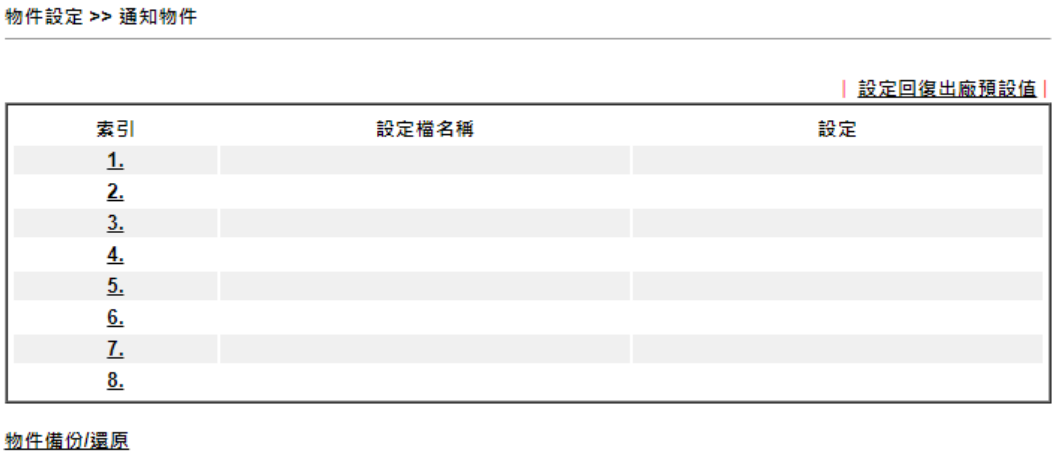
傳送測試電子郵件	按此可依照上數設定傳送測試電子郵件。

3. 完成設定之後，按下**確定**按鈕儲存相關設定。

VII-1-11 通知物件

本頁讓您設定 8 組設定檔，後續將運用在**其他應用>>簡訊/郵件警示服務**中。

每個物件可以設定不同的監控條件。



可用設定說明如下：

項目	說明
設定回復出廠預設值	清除全部的設定資料。
索引	顯示您可以設定的設定檔索引編號。
設定檔名稱	顯示物件設定檔的檔名。
設定	顯示物件設定檔的內容。
物件備份/還原	按此備份或是還原設定檔。

如欲建立新的設定檔，請依下述步驟進行：

1. 開啟**物件設定>>通知物件**，然後按下索引欄位下方的任一編號連結(例如 #1) 進入設定頁面。

2. 設定頁面顯示如下：

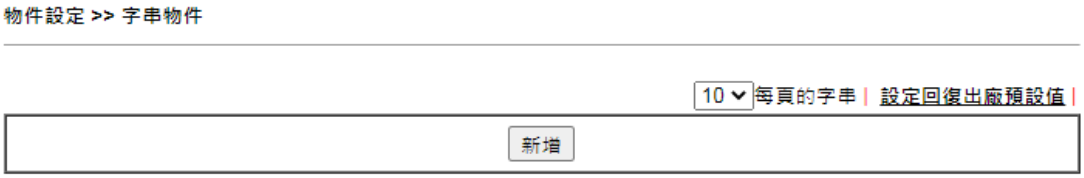
可用設定說明如下：

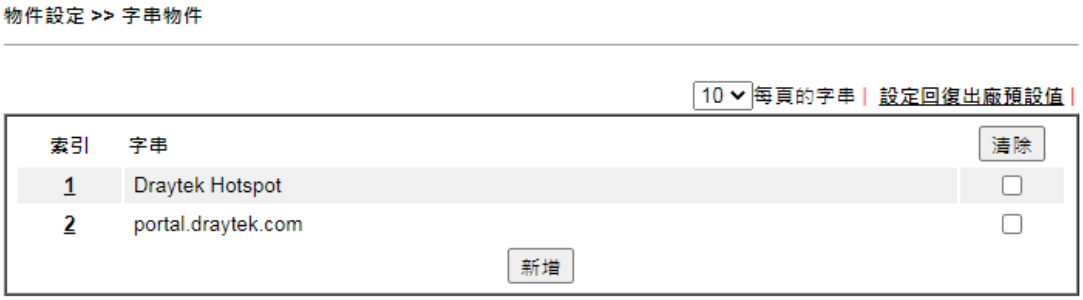
項目	說明
設定檔名稱	請輸入此設定檔名稱。
種類	顯示被監控的類型。
狀態	顯示類型的狀態，您可以勾選想要監控的類型狀態方塊。

3. 完成設定之後，按下**確定**按鈕儲存相關設定。

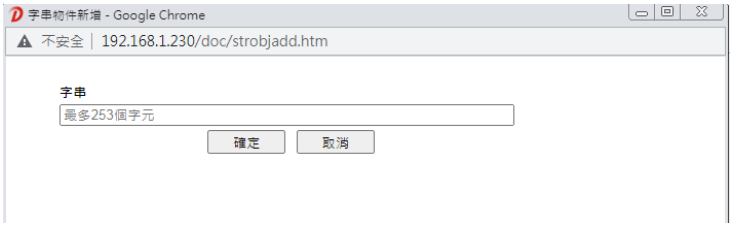
VII-1-12 字串物件

本頁讓您設定字串物件設定檔，可套用在路由策略中(網域名稱選項)、客製化入口網站等等。

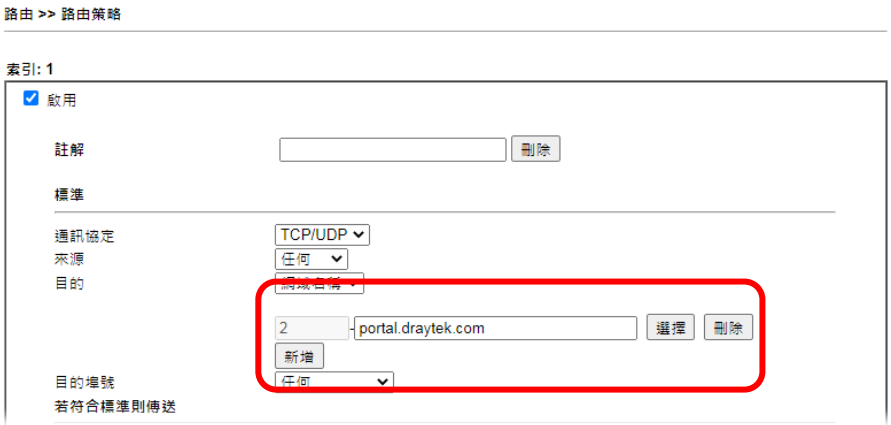




可用設定說明如下：

項目	說明
新增	按此開啟下述頁面以新增字串物件。 
設定回復出廠預設值	按此清除本頁所有設定。
索引	顯示您可以設定的設定檔索引編號。
字串	顯示定義的字串內容。
清除	選擇您想要移除的字串，接著按下此鈕刪除選擇的字串。

下列顯示套用字串物件的範例(在路由策略):



VII-1-13 國家物件

國家物件可以決定路由器防火牆應該封鎖哪個/些國家。

物件設定 >> 國家物件

國家物件表格: | 設定回復出廠預設值 |

索引	名稱	索引	名稱
1.		17.	
2.		18.	
3.		19.	
4.		20.	
5.		21.	
6.		22.	
7.		23.	
8.		24.	
9.		25.	
10.		26.	
11.		27.	
12.		28.	
13.		29.	
14.		30.	
15.		31.	
16.		32.	

物件備份/還原

國家物件，藉由群組多個國家多組 IP 位址，可被其他功能如路由器策略目標使用。請參考以下範例圖：

路由 >> 路由策略

索引: 1

☑ 啟用

註解 [ ] 刪除

標準

通訊協定 TCP/UDP

來源 任何

目的 國家物件

1-Taiwan

目的埠號 任何

若符合標準則傳送

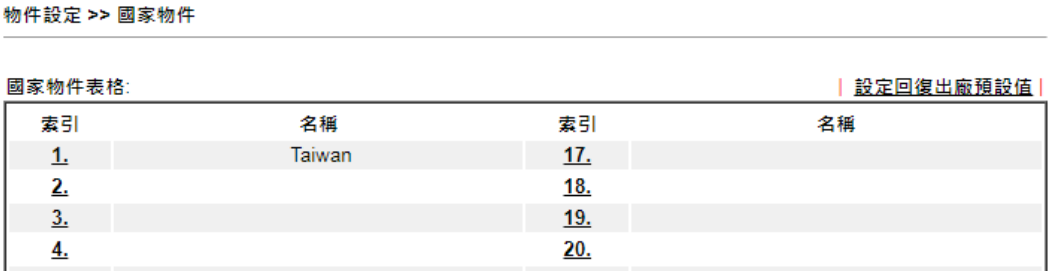
如欲建立新的設定檔，請依下述步驟進行：

1. 開啟**物件設定>>國家物件**，按下任一索引編號(如#1)。
2. 設定頁面顯示如下：

可用設定說明如下：

項目	說明
名稱	輸入設定檔名稱。
國家	請自左方選擇需要被封鎖的國家，按下>>將其移至選定國家區域中。 注意，每一個國家設定檔可包含 1 到 16 個國家。

3. 完成設定之後，按下**確定**按鈕儲存相關設定。



VII-1-14 物件備份/還原

物件設定可以備份成檔案，在必要時，此檔可以輸入別的裝置好還原在此裝置上的設定內容。

可用設定說明如下：

項目	說明
備份	通常，物件可以透過物件設定選單一個一個建立，對於想要節省時間去建立物件的用戶來說，Vigor 路由器提供了一種快速方法，可以使用單一文件(CSV 檔案)來修改物件。 所有的物件或是範本都可以輸出成檔案，之後使用者可以用 Microsoft Excel 開啟 CSV 檔案，同時也可修改 IP 物件的內容。 **備份目前 IP 物件，儲存為 CSV 檔案** – 選擇此項以便將目前 IP 物件儲存為 CSV 檔案，此檔案可以在將來還原使用。 **下載預設 CSV 範本以利編輯** – 選擇此項後，按下載按鈕儲存預設的 CSV 範本(空白表格無任何資料) 並將其儲存在硬碟中。 **下載** – 自路由器下載 CSV 檔案並將其儲存在硬碟中。
還原	**選擇檔案** – 按此以指定事前定義的 CSV 檔案。 **還原** – 輸入選定的 CSV 檔案至 Vigor 路由器。

應用說明

A-1 當 WAN 斷線時如何使用 SMS 簡訊服務寄發通知至指定的電話號碼

請參考下列步驟：

1. 登入路由器的網頁設定介面。
2. 首先開啟**物件設定>>簡訊/郵件服務物件**頁面。

物件設定 >> 簡訊 / 郵件服務物件

簡訊服務供應商 | 郵件伺服器 | 設定回復出廠預設值

索引	設定檔名稱	簡訊服務供應商
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.	客製 1	
10.	客製 2	

物件備份/還原

索引編號 1~8 可以讓使用者選取內建的 SMS 簡訊服務供應商，若您所使用的簡訊服務供應商不在內建的清單中，即可使用索引編號 9 與 10 來新增您的 SMS 簡訊服務供應商（請參考備註）。

3. 選擇任何一個索引編號(例如本例使用編號 1)進行簡訊服務供應商設定，在下列開啟的頁面中，請填入您的帳號密碼，並設定此路由器可發送的簡訊則數。

物件設定 >> 簡訊 / 郵件服務物件

設定檔索引編號: 1

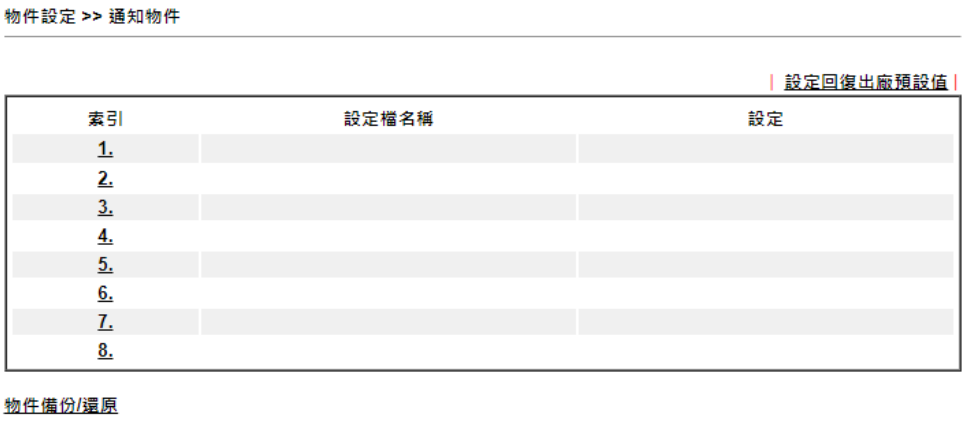
設定檔名稱	Local number
服務供應商	kotsms.com.tw (TW)
連線通訊協定	HTTP HTTPS
使用者名稱	abc5026
密碼	••••••
額度	10
傳送間隔	3 (秒數)

備註:
1. 在"發送間隔"時間內只能發送一條消息。
2. 如果"發送間隔"設定為0，則沒有限制。

確定 清除 取消 傳送測試訊息

4. 設定完畢之後，按下**確定**回到上頁，便完成簡訊服務供應商的設定。

5. 接著開啟**物件設定>>通知物件**，設定通知的事件內容。



6. 選擇任何一個索引編號(例如本例使用編號 1)進行通知發送的條件設定，在下列開啟的頁面中，輸入設定檔名稱，再勾選 WAN 類別中的**斷線**與**重新連線**來呼應本文的主題。

7. 設定完畢之後，按下**確定**回到上頁，便完成通知設定檔的設定。

8. 開啟**其他應用>>簡訊/郵件警告服務**頁面。分別自下拉式清單中選擇您需要的簡訊服務供應商與通知設定檔(設定使用簡[訊發送通知的事件)等設定，然後在**接收者號碼**欄位中填入您要接收簡訊通知的號碼。

9. 按**確定**儲存相關設定，之後若路由器有某條 WAN 斷線，系統將會寄出簡訊給指定的人。如果路由器僅有一個 WAN 介面，那麼系統也會重新連接 WAN 介面成功之後，寄送簡訊給指定的人。

備註：如何自訂簡訊服務供應商

開啟**物件設定>>簡訊/郵件服務物件**，選取任一可自訂的索引連結(例如索引編號 9 或 10)，在開啟的頁面中填入您的簡訊服務供應商的 URL 字串並填入您的帳號密碼，即可新增您所使用的簡訊服務供應商來寄發簡訊 SMS 通知。

VII-2 USB 應用

連接至路由器的 USB 存取磁碟可以被視為伺服器的一種。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>>USB 使用者管理**頁面所建立的帳號與密碼，然後，用戶端就可以使用 FTP(USB 儲存碟)或是分享檔案服務。

資訊	Vigor 路由器的 USB 埠口可用來連接 USB 數據機，Vigor 路由器支援哪些數據機可從 **USB 應用>>數據機支援清單**中取得相關資訊，有關透過 USB 數據機建構的網路連線，請參考 **WAN>>網際網路連線設定**與 **WAN>>基本設定**。

網頁使用者介面

VII-2-1 USB 基本設定

本頁決定同步 FTP 連線的數目、預設字集伺服器以及啟用 Samba 服務，目前，Vigor 路由器可支援格式為 FAT16 與 FAT32 的 USB 儲存碟，因此在連接 USB 儲存碟之前，請務必確認記憶格式是 FAT16 還是 FAT32。建議您使用 FAT32 來檢視檔案名稱(FAT16 不支援長檔名) 。

可用設定說明如下：

項目	說明
基本設定	**同步 FTP 連線** - 此區用來指定 FTP 連線數總量，路由器允許一次連接 USB 儲存碟數量，最多可達 6 個 FTP 連線數。 **預設字符集** - 目前，Vigor 路由器支援四種語文字集，預設字集為英文。
SMB 檔案分享服務	按下**啟用**以便透過路由器使用 SMB 服務(檔案分享)。
連線模式	**限用 LAN** – 網際網路使用者不可連接至路由器的 samba 伺服

	器。 **LAN 與 WAN** - LAN 與 WAN 端使用者皆可登入路由器的 samba 伺服器。
NetBios 名稱服務	針對 USB 儲存碟的 NetBios 服務，您必須指定工作群組名稱以及主機名稱。工作群組名稱不可與主機名稱相同，工作群組名稱最多可有 15 個字元而主機名稱最多可有 23 個字元。二者皆不可包含下述字元; : " < > * + = \\| ?。 **工作群組名稱** - 輸入工作群組的名稱。 **主機名稱** - 輸入路由器的主機名稱。
印表機伺服器	**啟用** - 按此可讓路由器作為印表機伺服器(但需外接一台 USB 印表機)。

完成設定之後，按下**確定**按鈕儲存相關設定。

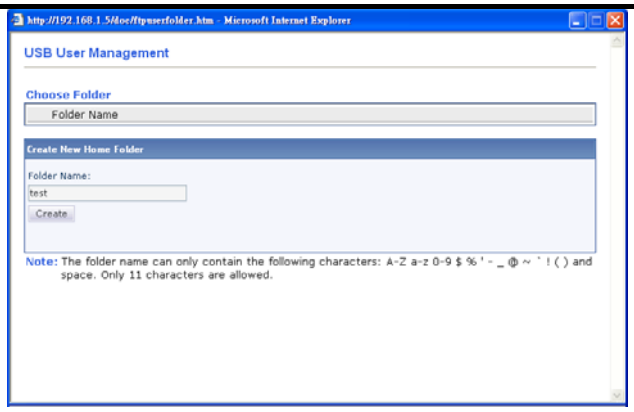
VII-2-2 USB 使用者管理

本頁讓您針對 FTP/SMB 使用者設定數個設定檔，任何想要登入 USB 儲存碟的使用者，必須鍵入與本頁設定相同的使用者名稱與密碼。在新增或是修正本頁設定之前，請先插入 USB 儲存碟，否則系統會出現錯誤訊息。

按任一索引號碼連結登入設定頁面。

可用設定說明如下：

項目	說明
啟用	勾選此框以啟動此設定檔，之後，使用者可使用本頁指定的名稱來登入 FTP 伺服器。
使用者名稱	輸入 FTP/SMB 使用者的使用者名稱以登入 FTP 伺服器(USB 儲存碟)，注意，使用者不可以匿名方式登入 USB 儲存碟，之後您可以打開 FTP 用戶軟體再輸入此處指定的使用者名稱，即可登入 USB 儲存碟。 **注意:** 此處的使用者名稱不可輸入“Admin” ，因為該名稱是用來登入路由器的使用者介面，同時，該名稱也供 FTP 韌體更新時使用。 **注意:** 路由器不支援 FTP Passive 模式。請在 FTP 用戶端停用此模式。
密碼	輸入 FTP/SMB 使用者的密碼以登入 FTP 伺服器(USB 儲存碟)，之後您可以打開 FTP 用戶軟體再輸入此處指定的密碼，即可登入 USB 儲存碟。
確認密碼	再次輸入密碼確認。
Home 檔案夾	此功能決定用戶登入的檔案夾。 使用者可以在本區輸入目錄名稱，接著按下**確定**，路由器將會在 USB 儲存碟中建立特定/新的檔案夾，此外，如果使用者輸入“/”，就能進入 USB 儲存碟中所有的檔案夾觀看檔案。 **注意:** 當 USB 儲存碟的防寫狀態開啟時，您就無法在此輸入新檔案夾名稱，在此情況下只有“/”可以運用。 您可以點 以開啟下述對話盒新增檔案夾作為預設檔案夾。

	
存取規則	此功能決定設定檔的權限，任何使用此設定檔以便登入 USB 儲存碟的使用者必須遵循此處設定的規則。 **檔案** – 勾選允許開放的項目(讀取、寫入、刪除)。 **目錄** – 勾選允許開放的項目(清單、建立、移除)。

在您按下**確定**之後，您必須在路由器的 USB 介面插入 USB 儲存碟，否則您無法儲存設定。

VII-2-3 檔案瀏覽器

檔案瀏覽提供一個很簡易的方式讓使用者檢視及管理 USB 儲存碟(連接至 Vigor 路由器)的內容。

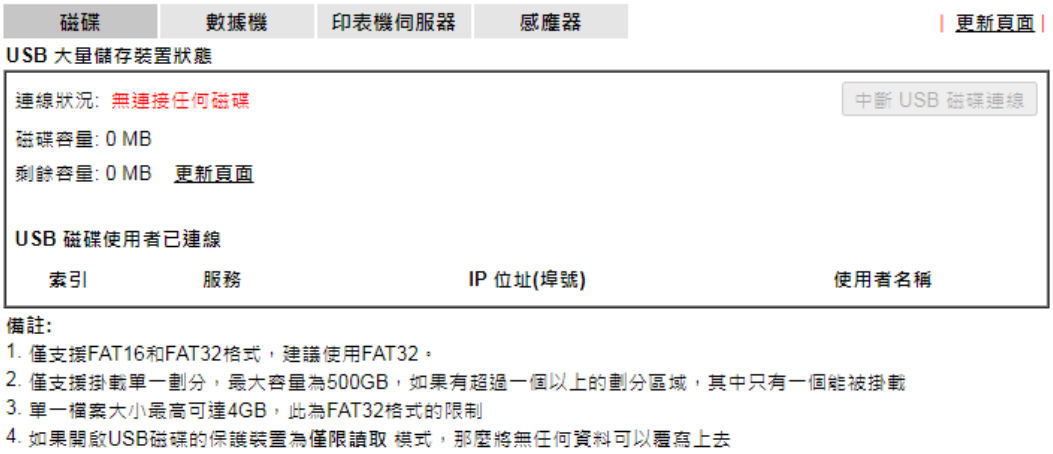
可用設定說明如下：

項目	說明
更新	按此圖示更新檔案清單。
上層	按此圖示回到上一層目錄。
建立	按此圖示新增檔案夾。
目前路徑	顯示目前檔案夾的位址。
上傳	按此鈕上傳選定檔案至 USB 儲存碟，在碟內要上傳的檔案可以給其他 FTP 使用者分享。

VII-2-4 USB 裝置狀態

本頁用來監督透過 Vigor 路由器來存取 FTP 或是 Samba 伺服器的使用者狀態，如果您想要從路由器移除 USB 隨身碟，請先按下**中斷 USB 磁碟連線**，然後移除隨身碟。

USB 應用 >> USB 裝置狀態

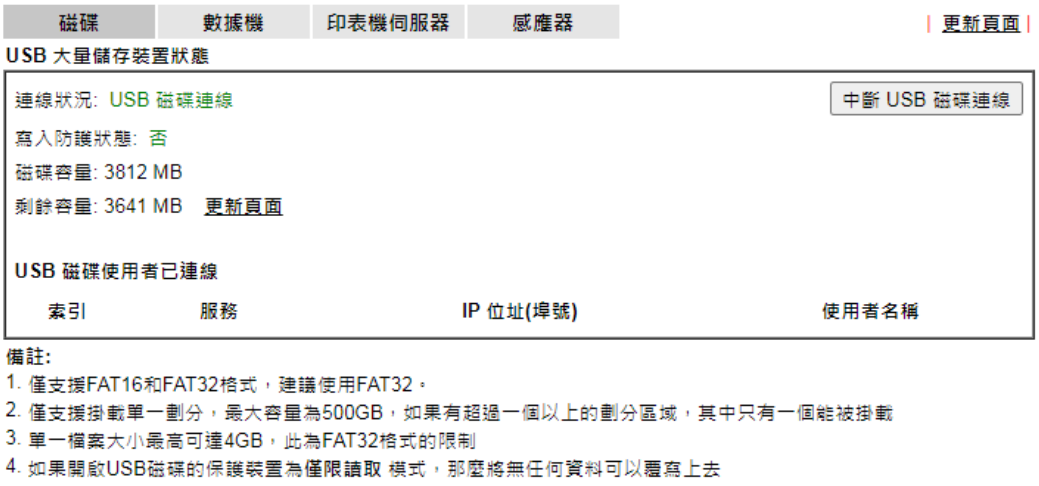


可用設定說明如下：

項目	說明
連線狀況	如果路由器沒有連接任何 USB 儲存碟，此處會顯示"**無連接任何磁碟**"。
磁碟容量	顯示 USB 儲存碟的總容量。
剩餘容量	顯示 USB 儲存碟的目前剩餘的容量。按下**更新頁面**可取得最新的容量資訊。
USB 磁碟使用者已連線	**索引** - 顯示使用 USB 儲存碟服務的用戶編號。 **IP 位址** - 顯示使用 USB 儲存碟服務的用戶的 IP 位址。 **使用者名稱** - 顯示使用 USB 儲存碟服務的用戶登入時使用的名稱。
中斷 USB 磁碟連線	將 USB 磁碟自路由器拔除之前，請務必確定先按此鈕，確保所有的資料皆已覆寫到磁碟。

當您將 USB 儲存碟插入 Vigor 路由器時，系統將會在數秒鐘內尋找此裝置。

USB 應用 >> USB 裝置狀態



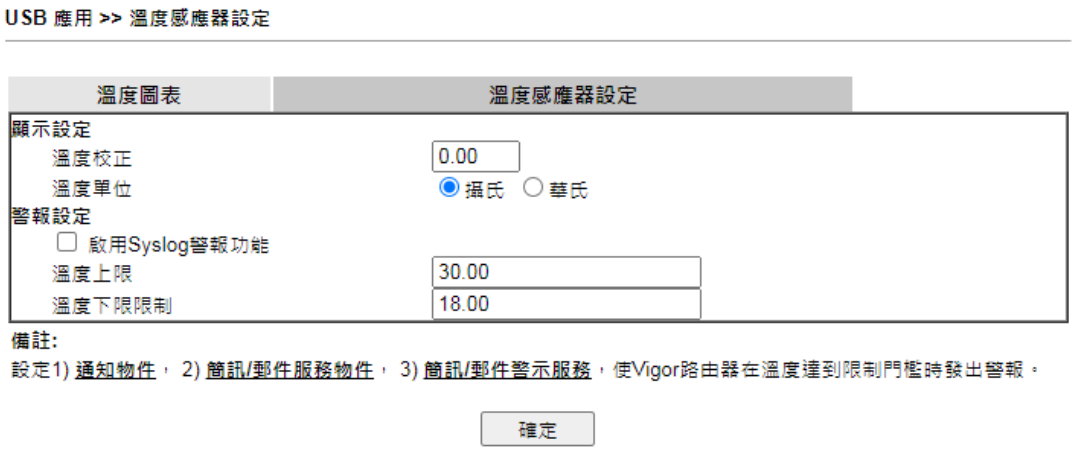
VII-2-5 溫度感應器

Vigor 路由器允許插入 USB 溫度感應器以便監控環境溫度，如果溫度高於上限或是低於下限時，警示訊息將會發送出去。

尤其是在夏天，確保伺服器或是資料通訊設備有無因冷卻系統失效導致過熱發生，是相當重要的事情。

與 Vigor 路由器相容的溫度計可持續監控周圍環境的溫度，當偵測到已達預先設定的門檻溫度時，系統會透過電子郵件或是簡訊發出警告通知，讓使用者能採取適當的行動。

溫度感應器設定



可用設定說明如下：

項目	說明
顯示設定	**溫度校正** - 輸入校正溫度錯誤的數值。 **溫度單位**- 選擇溫度的顯示單位，有二種類型可以選擇。
警報設定	**啟用 Syslog 警報功能**- 勾選此框啟用此功能。 **溫度上限/溫度下限** - 輸入系統傳送溫度警示的上下限溫度。

完成設定之後，請按下**確定**按鈕儲存。

溫度圖表

下圖為溫度圖表的範例：

VII-2-6 數據機支援清單

本頁提供 Vigor 路由器支援的 USB 數據機的品牌與型號等相關資訊。

USB 應用 >> 數據機支援清單

下述相容性測試列出在某些環境或是國家中**Vigor路由器支援的 3.5G/LTE 數據機**，如果您所擁有的LTE數據機在清單上但卻無法正常運作，請透過客服信箱 support@draytek.com 反應您的問題，或聯絡您的經銷商取得更多資訊。

品牌	型號	LTE	存取模式	狀態
4G system	XSPlug P3		PPP	Y
Aiko	Aiko 76E		PPP	Y
Alcatel	Alcatel L100V	✓	DHCP	Y
	Alcatel L800	✓	DHCP	Y
	Alcatel W800	✓	DHCP	Y
	Alcatel X500		PPP	Y
	Alcatel Y855	✓	DHCP	Y
Alfa	ALFA Flyppp		PPP	Y
Amoi	Amoi H01		PPP	Y

VII-2-7 SMB 用戶端支援清單

此清單提供在不同平台下，檔案分享操作等應用之測試狀態資訊。

USB 應用 >> SMB用戶端支援清單

下述相容測試清單列出Vigor路由器支援的SMB用戶。

平台	其他應用	狀態
Microsoft® Windows® XP	Built in	I
Microsoft® Windows Vista™	Built in	Y
Microsoft® Windows® 7	Built in	Y
Microsoft® Windows® 8	Built in	M
Microsoft® Windows® 10	Built in	Y
OS X® 10.7.5	Built in	Y
OS X® 10.10	Built in	Y
Ubuntu 14.04	Built in	Y
Android™	AndSMB	Y
Android™	ES File Explorer	Y
Android™	File Expert	Y
Android™	File Manager	Y
Android™	Solid Explorer	Y
Android™	SharesFinder	Y
iOS	eXPlayer	Y
iOS	nPlayer	Y

Y: 已經測試並且支援
I: 支援但仍有些疑問
M: 尚未測試，但可能支援

應用說明

A-1 如何取得連接至 Vigor 路由器的 USB 裝置內的檔案?

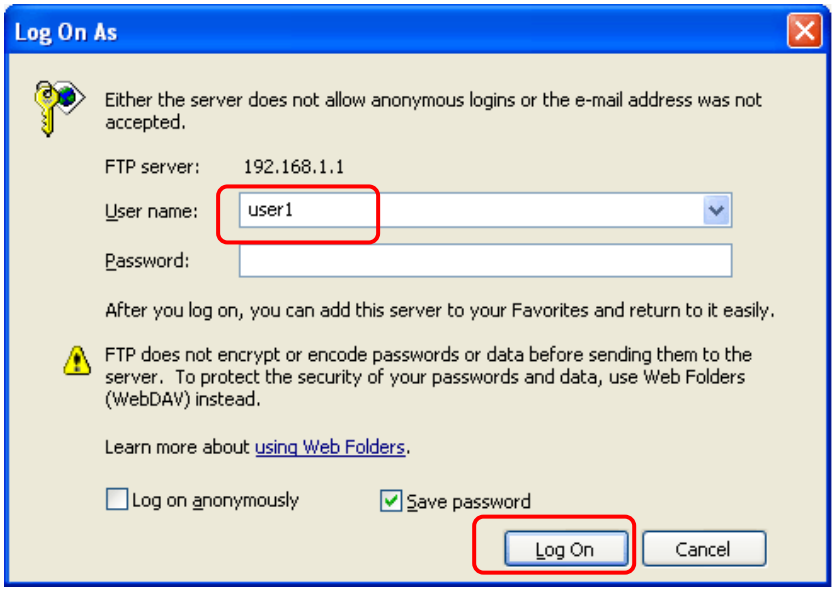
1. 將 USB 裝置連接至路由器的 USB 埠口，務必確認連線狀態欄位中出現 USB **磁碟連線**的訊息，如下所示：

2. 開啟 **USB 應用>>USB 基本設定**以啟用 SMB 服務，按下**確定**。

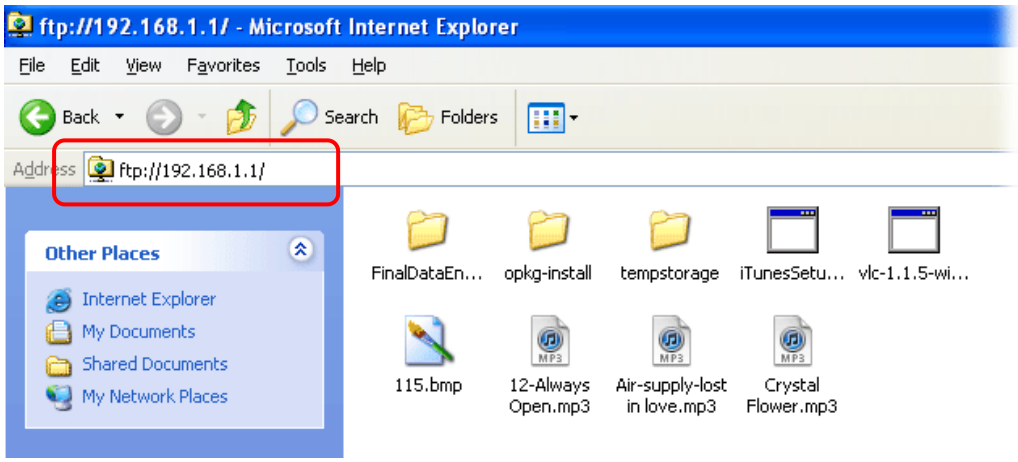
3. **USB 應用>>USB 使用者管理**設定一組使用 FTP 服務的使用者帳號，按下**啟用**以便啟動此 FTP/SMB 使用者帳號，此例我們新增一個名為 user1 的帳號，給予讀取、覆寫、清單的權限。

4. 按下**確定**按鈕儲存設定。

5. 確認 FTP 服務可以順利運作，請開啟任一瀏覽器並鍵入 *ftp://192.168.1.1*。使用帳號 **user1** 來登入。



6. 當下列視窗出現時，即表示 FTP 服務可正常運作。



7. 回到 **USB 應用>>USB 磁碟狀態**，FTP 伺服器資訊將會顯示如下圖：

現在，路由器 LAN 端的使用者可以存取 USB 裝置內容，只要在瀏覽器輸入 ftp://192.168.1.1 即可，使用者可以新增或移除檔案/目錄，相關權限視 **USB 應用>>USB 使用者管理**中對於 FTP 帳戶設定所做的存取規則而定。

第八篇 故障排除

如果安裝並完成路由器設定之後，您無法存取網際網路，本篇可以引導您解決一些異常狀況。

VIII-1 自我診斷工具

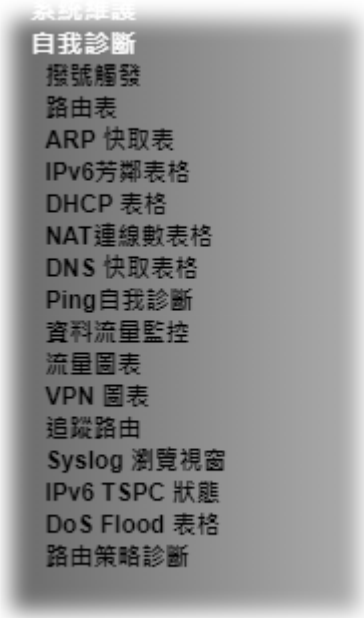
這個章節將會指導您，如何解決在完成安裝和設置路由器後依然無法上網的問題。請按以下方法一步一步地進行檢查。

- 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。

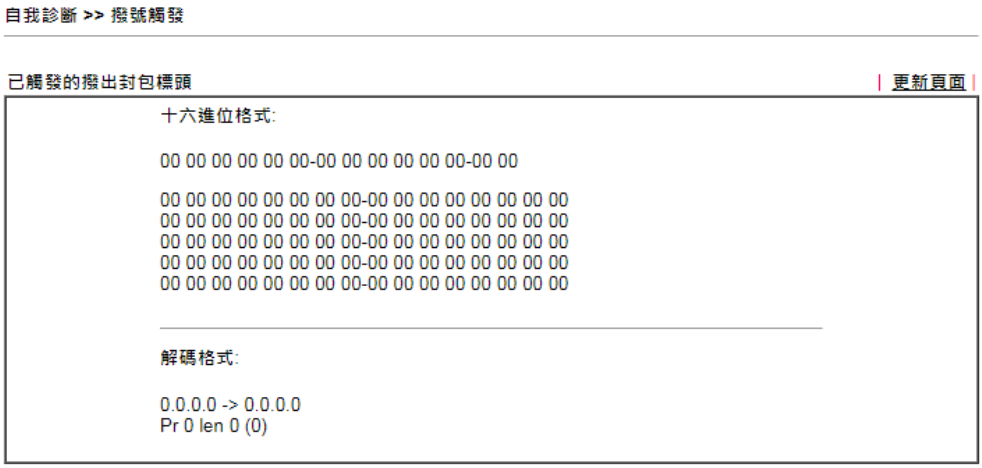
網頁使用者介面

自我診斷工具提供一個非常有效的方式，讓使用者能夠檢視或是診斷路由器的現況。以下為自我診斷的選單項目：



VIII-1-1 撥號觸發

按**自我診斷**的**撥號觸發**開啟網頁，網際網路連線(如 PPPoE)可由來源 IP 位址封包來觸發。

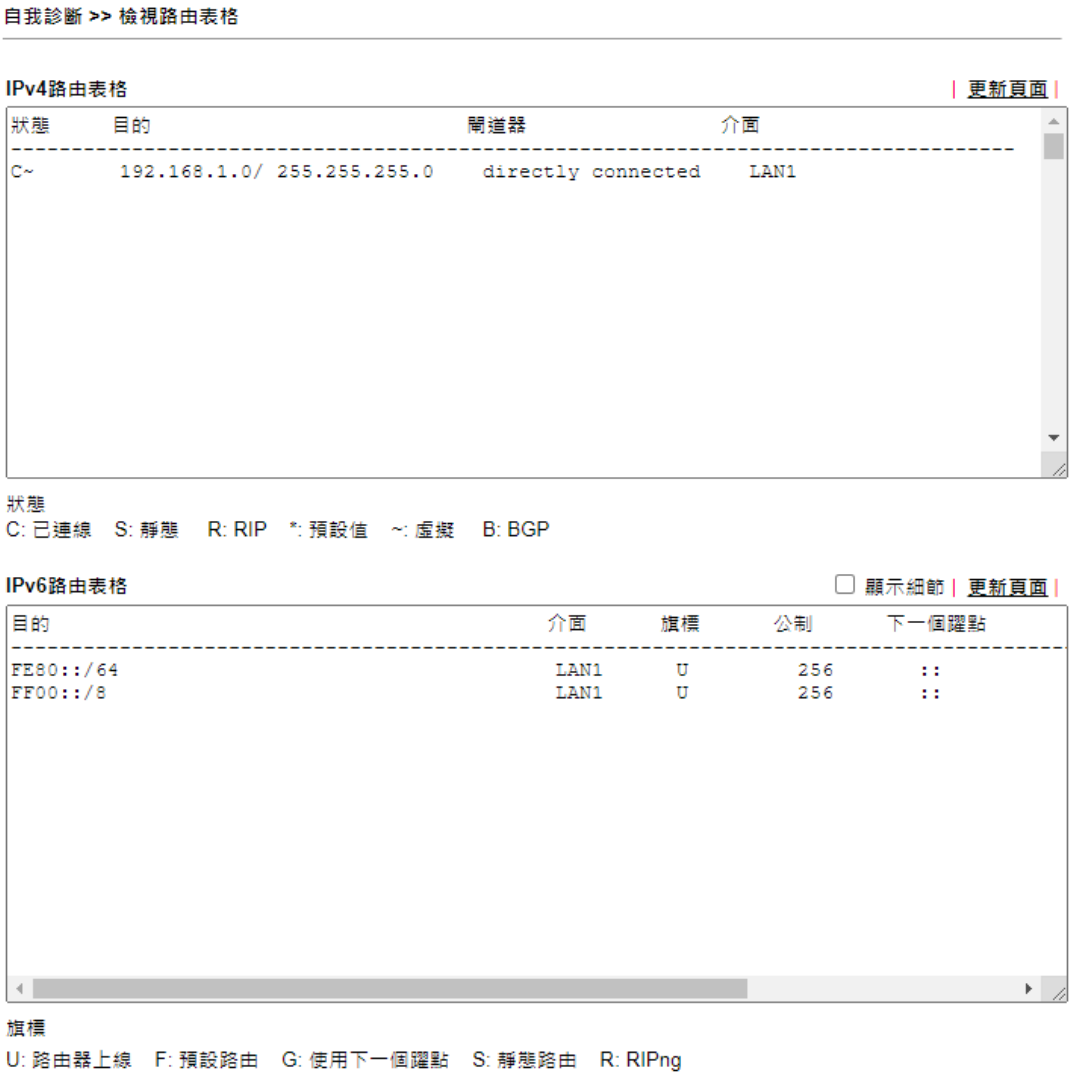


可用設定說明如下：

項目	說明
解碼格式	顯示來源 IP 位址、目標 IP 位址、通訊協定和封包的長度。
更新頁面	按此重新載入本頁。

VIII-1-2 路由表

按**自我診斷**的**路由表**檢視路由器的路由表格，此表格可提供目前的 IP 路由資訊。



可用設定說明如下：

項目	說明
更新頁面	按此重新載入本頁。

VIII-1-3 ARP 快取表

按**自我診斷工具**的 **ARP 快取表**檢視路由器中 ARP(Address Resolution Protocol)快取的內容，此表格顯示乙太網路硬體位址(MAC 位址)和 IP 位址間的對應狀況。

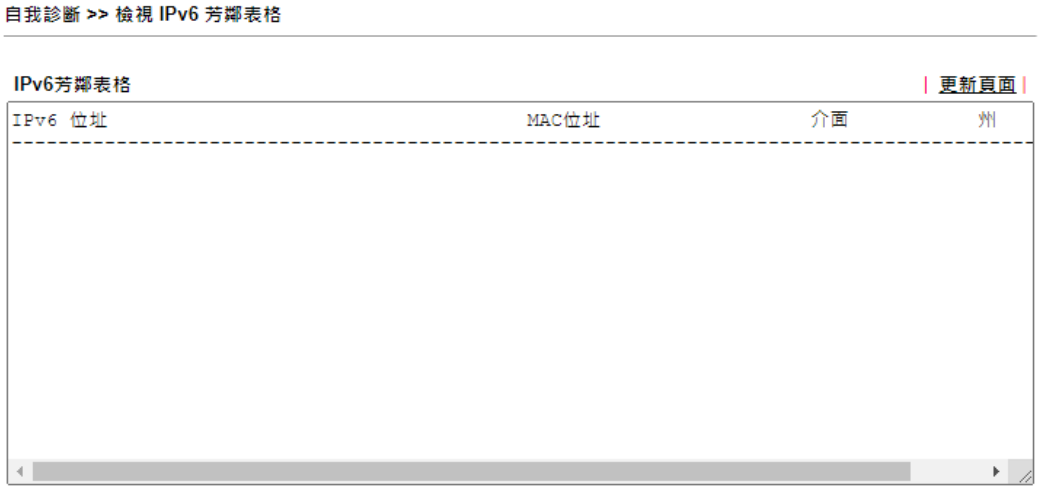
可用設定說明如下：

項目	說明
顯示	指定 LAN 與 VLAN 顯示相關資訊。 本頁在預設的狀態下將會顯示 LAN 與 VLAN 所有的資訊。
更新頁面	按此鈕重新載入本頁。

VIII-1-4 IPv6 芳鄰表格

表格顯示乙太網路硬體位址(MAC 位址)與 IPv6 位址之間的對應關係，此項資訊對於診斷網路問題諸如 IP 位址衝突等方面很有幫助。

按**自我診斷工具>> IPv6 芳鄰表格**開啟如下頁面。



可用設定說明如下：

項目	說明
更新頁面	按此重新載入本頁。

VIII-1-5 DHCP 表格

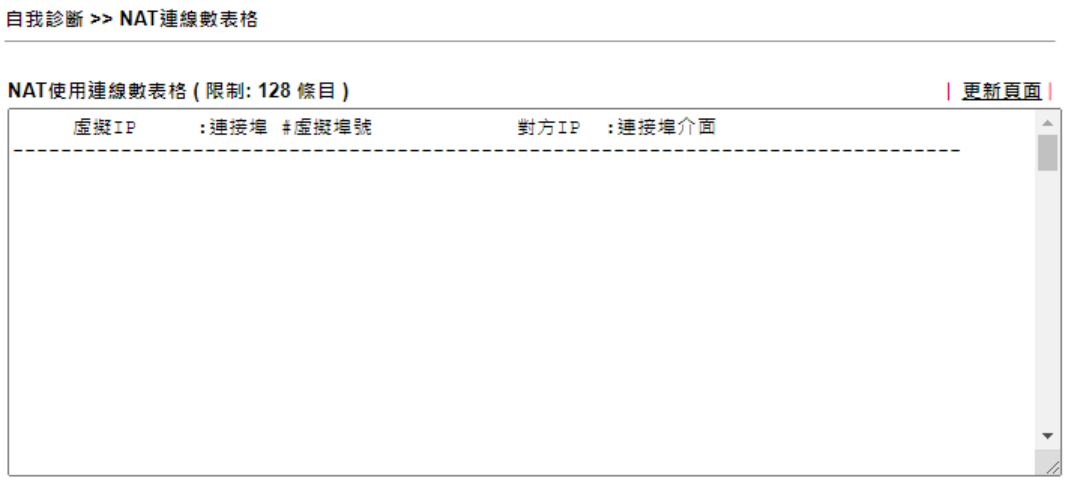
此工具提供指派 IP 位址的相關資訊，這項資訊對於診斷網路問題像是 IP 位址衝突等是很有幫助的。按**自我診斷**，選擇 **DHCP 表格**開啟相關網頁。

可用設定說明如下：

項目	說明
索引	顯示連線項目編號。
IP 位址	顯示路由器指派給特定電腦的 IP 位址。
MAC 位址	顯示 DHCP 指派給特定電腦的 MAC 位址。
租用時間	顯示指定電腦的租用時間。
主機 **ID**	顯示指定電腦的主機 ID 名稱。
更新頁面	按此重新載入本頁。

VIII-1-6 NAT 連線數表格

按**自我診斷**，選擇 **NAT 連線數表格**開啟相關網頁。



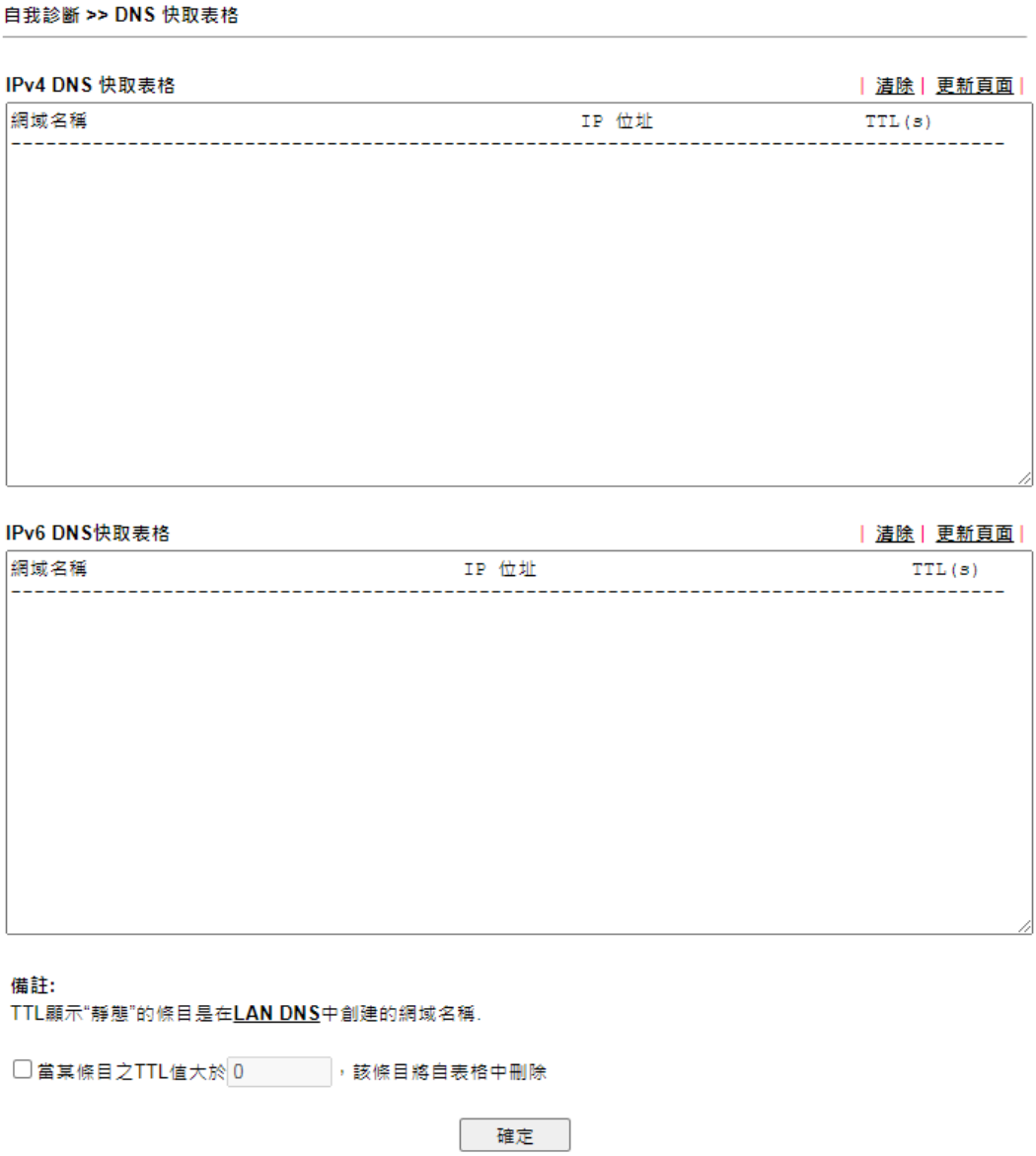
可用設定說明如下：

項目	說明
虛擬 IP:連接埠	本機電腦的 IP 位址和埠號。
#虛擬埠號	路由器為了執行 NAT 所使用的暫時通訊埠。
對方 IP: 連接埠	遠端主機的目標 IP 位址與埠號。
介面	顯示 WAN 連線的介面。
更新頁面	按此重新載入本頁。

VIII-1-7 DNS 快取表格

按下**自我診斷>>DNS 快取表格**開啟設定網頁。

回應 LAN 端的 DNS 詢問的網域名稱與對應 IP 位址記錄，將會儲存在 Vigor 路由器暫存器並顯示於本頁面。



可用設定說明如下：

項目	說明
清除	按此連結移除畫面上全部的結果。
頁面更新	按此重新載入本頁。
當某條目之 TTL 值大於..	勾選此框並輸入 TTL 值，按下確定(OK)按鈕之後，即可啟用此功能。 此數值表示當每個 DNS query 達到 TTL 值，相應的紀錄將自路由器的暫存器中自動刪除。

VIII-1-8 Ping 自我診斷

按**自我診斷工具**，選擇 **Ping 自我診斷**開啟相關網頁。

或是

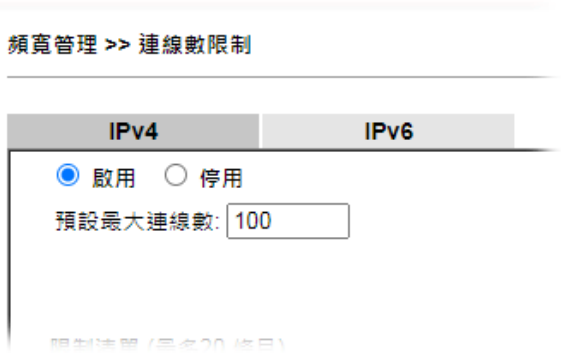
可用設定說明如下：

項目	說明
IPV4 /IPV6	選擇其中一項以便顯示相應的資訊內容。
Ping 經由	使用下拉式清單選擇您想要 Ping 經由的 WAN/LTE 介面。
Ping 至	使用下拉式清單選擇您想要 Ping 的目標。
IP 位址	輸入您想要 Ping 的主機/IP 上的 IP 位址。
Ping IPv6 位址	輸入您想要 Ping 的主機/IP 上的 IPv6 位址。
執行/運作	按此鈕啟動 Ping 作業，結果將會顯示在螢幕上。

清除	按此連結清除視窗上的結果。

VIII-1-9 資料流量監控

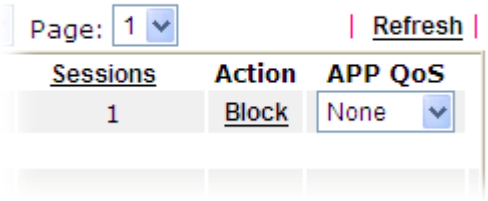
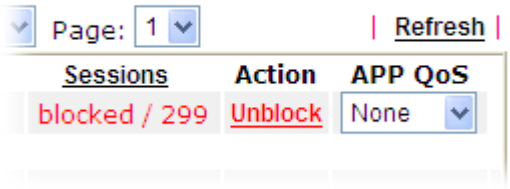
本頁顯示所監視的 IP 位址執行的過程，並在數秒的間隔後重新更新頁面，此處所列出的 IP 位址是在頻寬管理中設定完成的，在啟動資料流量監控之前，您必須啟動 IP 頻寬限制以及 IP 連線數限制。若沒有這麼做的話，系統會出現知會畫面提醒您先啟動相關設定。



按**自我診斷**，選擇**資料流量監控**開啟相關網頁。您可按下 **IP 位址**、**傳送速率**、**接收速率**或是 **NAT 連線數(IP Address, TX rate, RX rate 或 Session)**來排列資料。

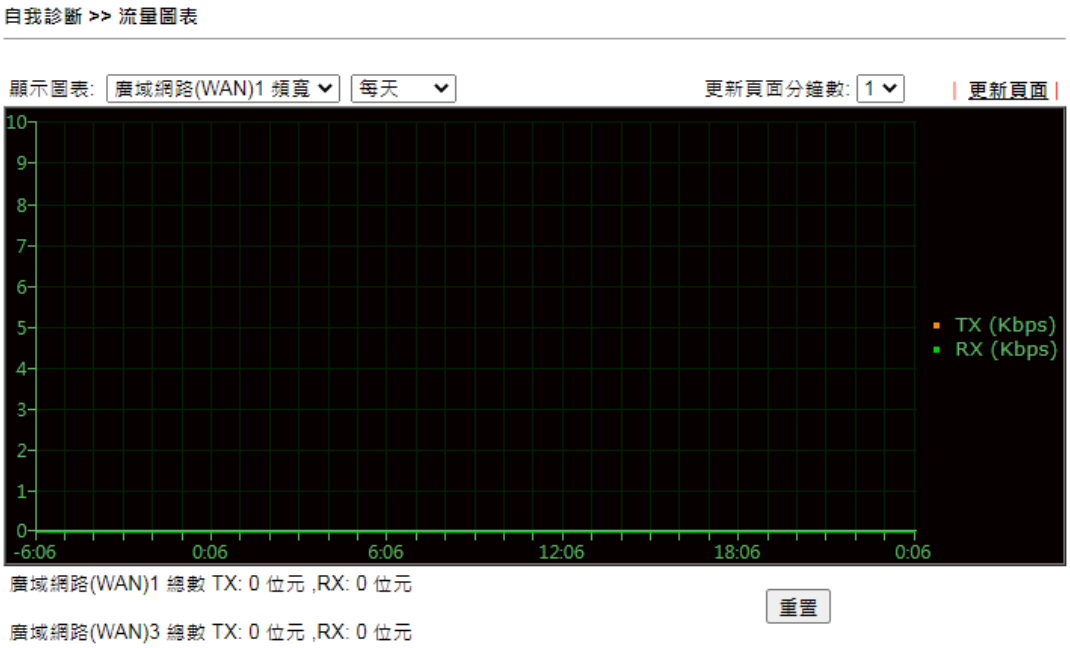
可用設定說明如下：

項目	說明
啟用資料流量監控功能	勾選此方塊以啟動此功能。
更新頁面秒數	使用下拉式選項選擇系統自動更新資料的間隔時間。
更新頁面	按此連結更新本頁。

索引	顯示資料流量的項目筆數。
IP 位址	顯示被監視裝置的 IP 位址。
傳送速率	顯示被監視裝置的傳送速率。
接收速率	顯示被監視裝置的接收速率。
連線數	顯示您在連線數限制網頁中所設定的連線數。
動作	**封鎖**- 可以避免指定電腦在 5 分鐘內存取網際網路。  **解除**- 指定 IP 位址的裝置將在五分鐘內封鎖起來，剩餘時間將顯示在 NAT 連線數欄位中。按下此鈕可以取消封鎖 IP 位址。 
APP QoS	使用下拉式清單選擇指定 IP 位址的資料傳輸的優先順序。
現值/峰值/速度	**現值**表示目前 WAN 介面的傳輸速率與接收速率。 **峰值**表示路由器在資料傳輸上所檢測到的最高數值。 **速度**表示 **WAN>>基本設定**中所指定的線路速度，如果您未指定任何速率，這邊將顯示自動，以說明速率由系統自行指定。

VIII-1-10 流量圖表

按**自我診斷**，選擇**流量圖表**開啟相關網頁。可以選擇 **WAN#頻寬**、**連線數**、**每日**、**每週**來檢視流量圖表。按下**重置/重新設定**可以將累計的傳送/接收資料全部歸零。您可隨時按**更新頁面**重新顯示圖表內容。



水平軸代表時間；而垂直軸代表的意義就很不同了。對 WAN#/ LTE 頻寬圖表而言，垂直軸代表的是過去所傳送與接收封包的數量。

但對連線數圖表來說，垂直軸代表的是過去一段時間之內的 NAT 連線數。

VIII-1-11 VPN 圖表

按**自我診斷**，選擇 **VPN 圖表**開啟相關網頁。

VIII-1-12 追蹤路由

從**自我診斷工具**，選擇**追蹤路由**開啟相關網頁。本頁允許您追蹤路由器至主機之間的路由情況，只要簡單的輸入主機的 IP 位址並按下**運作/執行**按鈕，整個路由狀況都將顯示在螢幕上。

或是

可用設定說明如下：

項目	說明
IPv4 / IPv6	選擇其中一項以便顯示相應的資訊內容。

追蹤經由	使用下拉式清單選擇您想要經由其處來追蹤的 WAN 介面，或使用**不指定**讓路由器自動決定選擇哪一種介面。
通訊協定	使用下拉式清單選擇您想要通訊協定。
主機/IP 位址	指明主機的 IP 位址。
追蹤主機/IP 位址	指明主機的 IPv6 位址。
運作/執行	按此鈕開始路由追蹤動作。
清除	按此連結刪除視窗上的結果。

VIII-1-13 Syslog 瀏覽視窗

本頁提供即時的 Syslog 並且在頁面上顯示相關資訊。

針對網頁 Syslog

本頁顯示使用者/防火牆/電話/WAN/VPN 等設定的時間與訊息，您可以勾選啟用網頁 Syslog 方塊，指定 Syslog 的類型，並選擇顯示的模式。之後，特定類型事件的 Syslog 資料將會顯示於頁面上。

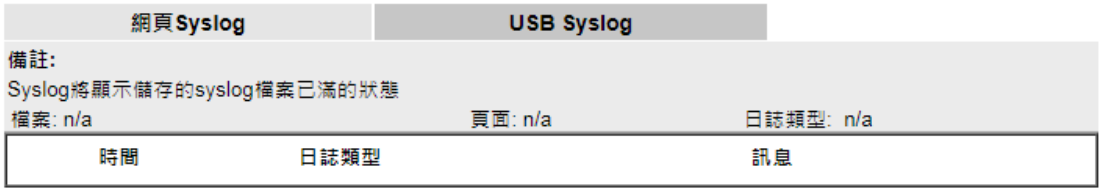
可用設定說明如下：

項目	說明
啟用網頁 Syslog	勾選此方塊可啟動網頁 Syslog 記錄功能。
Syslog 類型	使用下拉式清單指定準備顯示出來的 Syslog 的類型。
輸出	按下此連結可以將本頁紀錄的內容儲存成檔案。
更新頁面	按下此連結可以手動更新本頁紀錄的內容。
清除	按下此連結可以清除本頁紀錄的內容。
顯示模式	有二種模式可以選擇： **滿碟時停止紀錄-** 當 syslog 的容量已滿，系統將停止紀錄。 **永遠紀錄最新事件-** 系統只紀錄最新的事件。
時間	顯示事件發生的時間。
訊息	顯示事件發生的相關資訊。

針對 USB Syslog

本頁顯示暫存在 USB 儲存碟內的 Syslog 紀錄。

自我診斷 >> Syslog 瀏覽視窗



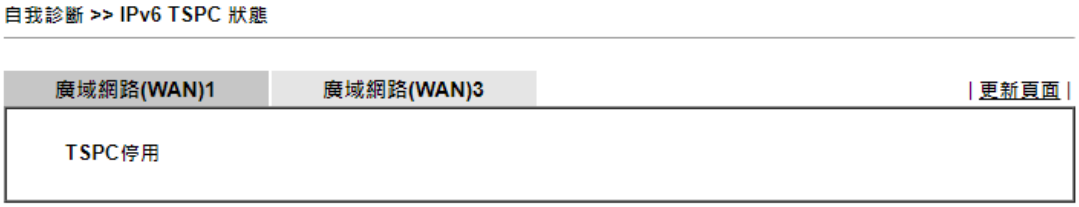
可用設定說明如下：

項目	說明
時間	顯示事件發生的時間。
日誌類型	顯示紀錄的類型。
訊息	顯示事件發生的相關資訊。

VIII-1-14 IPv6 TSPC 狀態

IPv6 TSPC 狀態頁面可以幫助您診斷 TSPC 的連線狀態是否正常。

如果 TSPC 設定無誤，當使用者成功連上通道的時候，路由器將會顯示如下頁面：



可用設定說明如下：

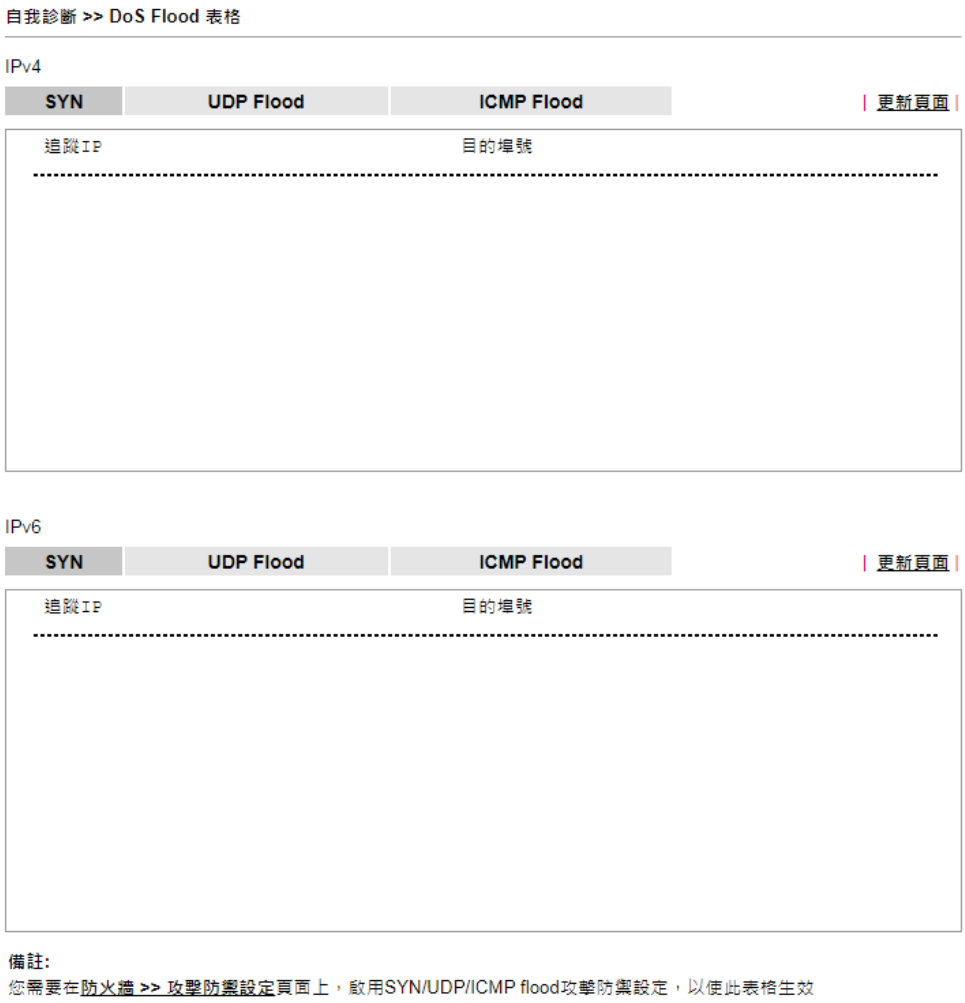
項目	說明
更新頁面	按下此連結可以手動更新本頁紀錄的內容。

VIII-1-16 DoS Flood 表格

本頁顯示 DoS Flooding Defense 機制偵測出的 IP 連線內容，對於網路工程師來說，這項工具有助於檢驗網路環境以期發現有無異常連線

系統可檢測並分別呈現用於 SYN Flood、UDP Flood 與 ICMP Flood 攻擊的 IP 追蹤與目的埠號資訊於不同的頁面上。

此外，被偵測出可能攻擊網路系統的 IP 位址可以透過 SYN Flood, UDP Flood 與 ICMP Flood 標籤頁面的 Block 按鈕暫時封鎖。



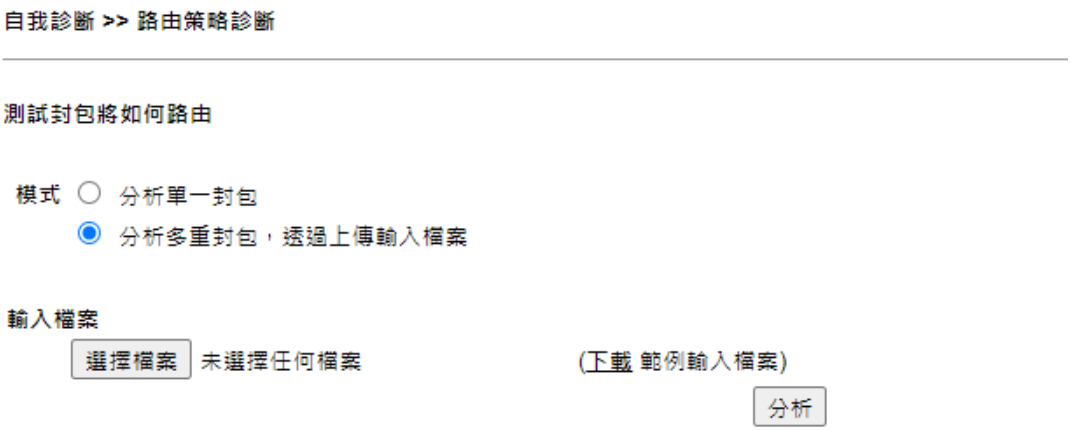
資訊

圖示 - ( )- 表示該 IP 位址出了些問題 (例如攻擊系統等)。

VIII-1-18 路由策略診斷

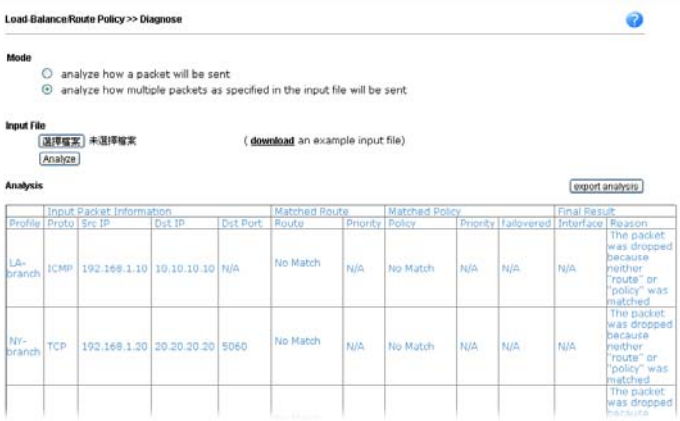
透過本頁所做的分析內容，可以輕易追蹤傳送至路由器的封包可能的路徑(固定路由、路由表格或是策略路由)。

或是



可用設定說明如下：

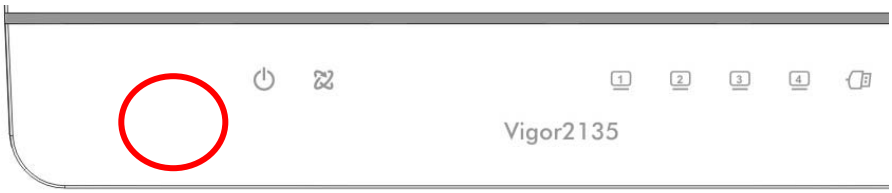
項目	說明
模式	**分析單一封包-** 路由器可利用路由策略分析被傳送之單一封包。 **分析多重封包…-** 路由器可利用路由策略分析特定檔案中被傳送的多重封包。
封包資訊	指定由路由器進行分析的封包本質。 **ICMP/UDP/TCP/ANY-** 指定診斷的通訊協定。 **來源 IP** – 輸入 IP 位址作為來源 IP。 **目的 IP** – 輸入 IP 位址作為目標 IP。 **目的埠號** – 使用下拉式清單指定目標埠號。 **分析** – 按此鈕執行分析任務，分析結果會顯示在頁面上。

輸入檔案	這個功能只有在選擇**分析多重封包...** 為模式時可用。 **選擇檔案** – 按下下載連結以便取得空白範例檔案，接著按此按鈕選擇 CSV 檔案以儲存分析結果。 **分析** – 按此執行分析任務，分析結果將會顯示在頁面上，如有需要，可按**輸出分析**按鈕將結果以檔案方式輸出。 

VIII-2 檢查路由器硬體狀態是否正常

檢查路由器硬體狀態是否正常

1. 檢查電源線以及 LAN 的連接。詳細資訊請參考“**I-2 硬體安裝**”。
2. 開啟路由器，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，意味著路由器的硬體有問題。那麼請回到“**I-2 硬體安裝**”，再重新執行一次硬體安裝，然後再試試。

VIII-3 檢查您電腦的網路連接設置是否正確

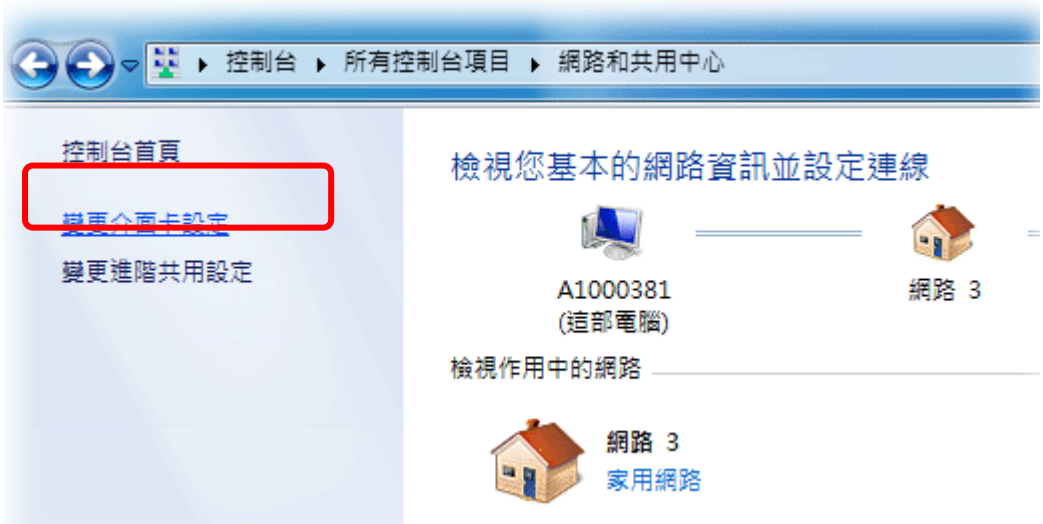
有些時候無法上網是因為網路連接設置錯誤所造成的，若在嘗試過上面的方法，依然無法連接成功，請按以下步驟確認網路連接是否正常。

對於 Windows 系統

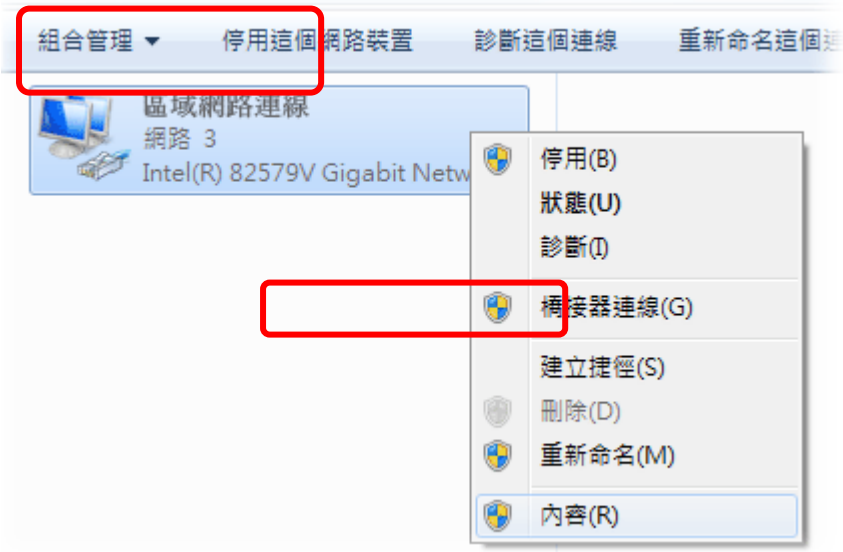
資訊	下列的範例是以 Windows 7 作業系統為基礎而提供。若您的電腦採用其他的作業系統，請參照相似的步驟或至 www.draytek.com.tw 查閱相關的技術文件說明。

1. 開啟程式集>>控制台，按網路和共用中心。

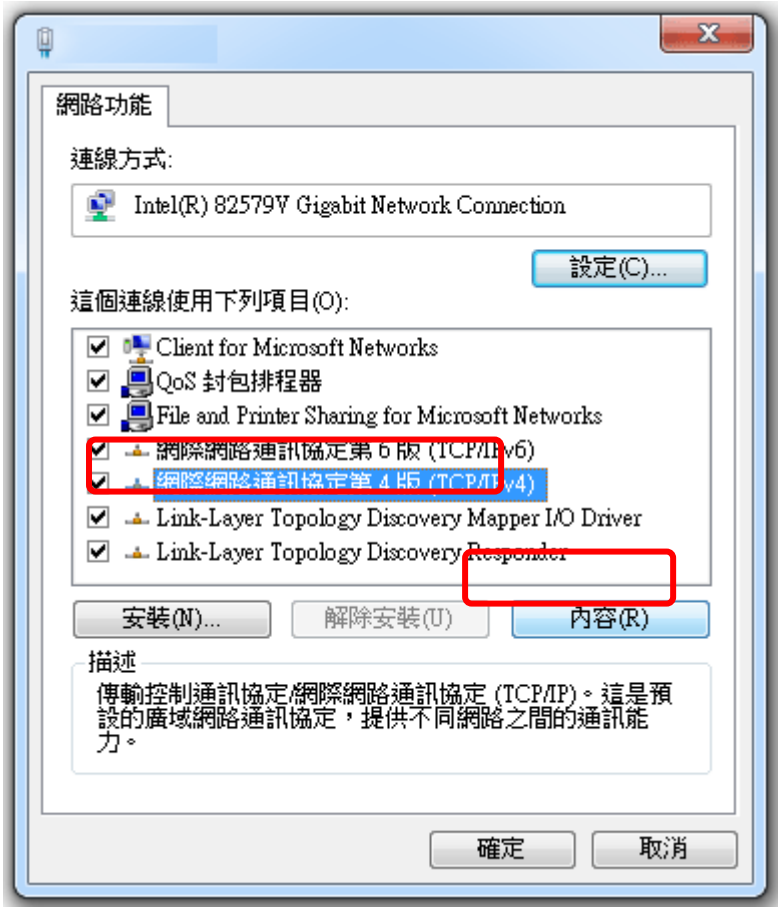
2. 在開啟的畫面上，按下變更介面卡設定連結。



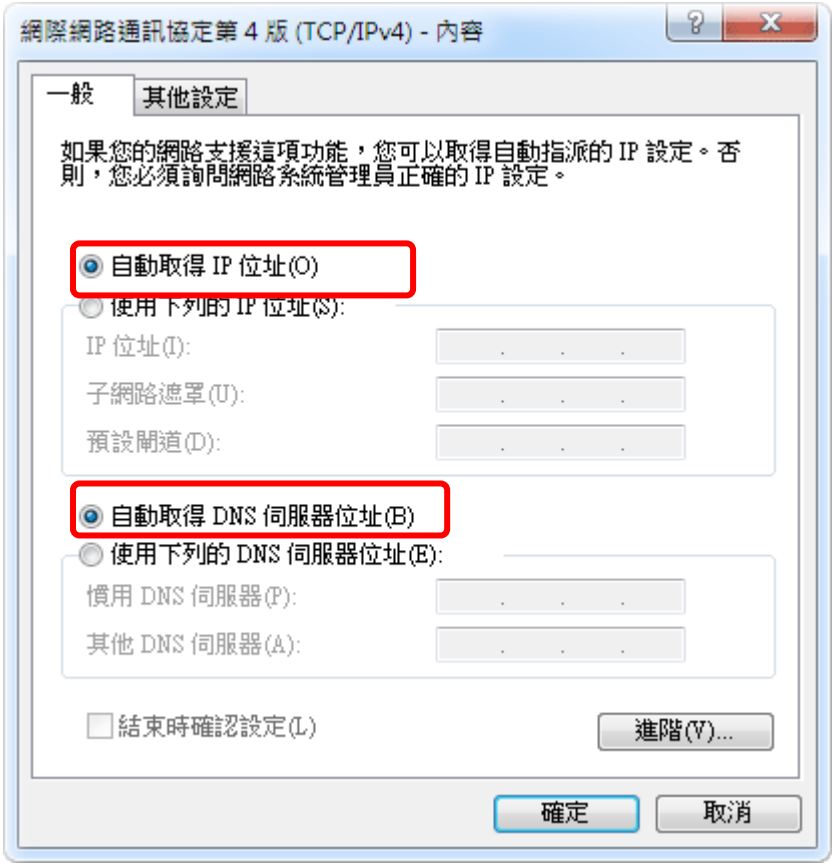
3. 網路連線圖示將會顯示在螢幕上，請在區域網路連線圖示上按下右鍵，然後向下移動點選內容。



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



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


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

對於 Mac 系統

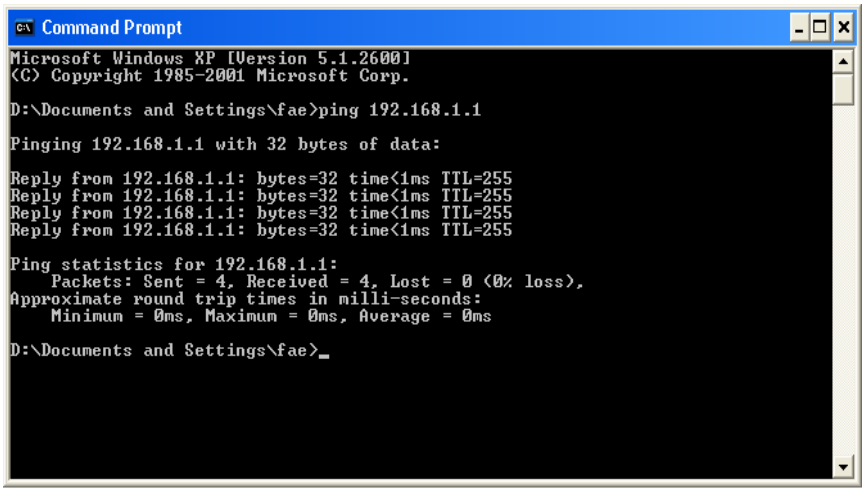
1. 在桌面上選擇目前所使用的 MacOS 磁碟機按滑鼠二下。
2. 選擇**應用**檔案夾中的**網路**檔案夾。
3. 進入**網路**畫面，在**設定**選項中，選擇**使用 DHCP**。

VIII-4 從電腦上 Ping 路由器

路由器的預設閘道為 192.168.1.1. 因為某些理由，你可能需要使用 " ping " 指令檢查路由器的連結狀態。比較重要的是電腦是否收到來自 192.168.1.1 的回應，如果沒有，請檢查個人電腦上的 IP 位址。我們建議您將網際網路連線設定為自動取得 IP 位址。(請參照 IX-3 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

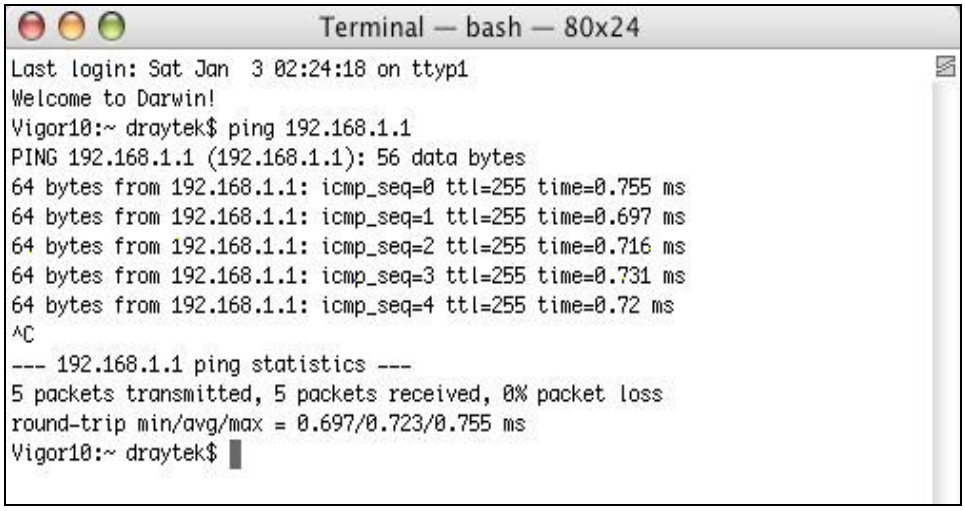
1. 開啟**命令提示字元視窗** (功能表選單**開始>>執行**) 。
2. 輸入 **cmd** (適用於 Windows 7 及以上)。DOS 命令提示字元視窗將會出現。



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

對於 MacOs (終端機)系統

1. 在桌面上選擇目前所使用的 Mac OS 磁碟機，並在上面按滑鼠二下。
2. 選擇 **Applications** 檔案夾中的 **Utilities** 檔案夾。
3. 滑鼠按二下 **Terminal**；終端機的視窗將會跳出並顯現在螢幕上。
4. 輸入 **ping 192.168.1.1** 並且按下 **Enter** 鍵。如果連結正常，終端機視窗會出現"6**4 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=xxxx ms**" 的訊息。


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

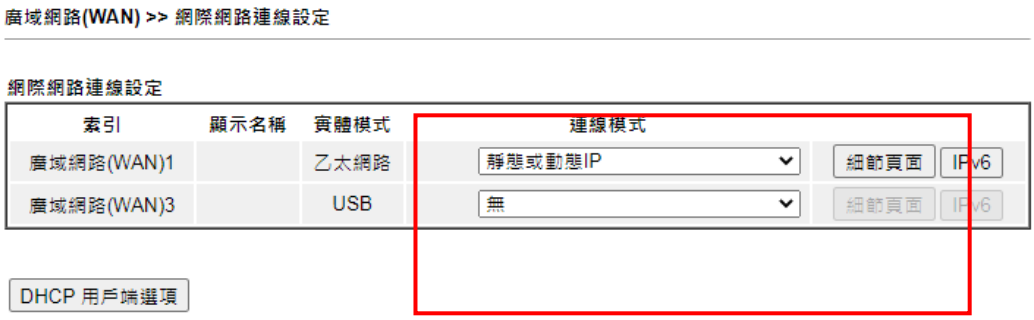
VIII-5 檢查 ISP 的設置是否正常

如果 WAN 連不起來，檢查燈號是否正確(依照前述 LED 說明檢查)，或是開啟**廣域網路(WAN)>>網際網路連線設定**頁面，檢查存取設定模式是否正確，按**細節頁面**檢視先前所設定的內容。

- 將實體連線改為其他的數值(例如 100M 全雙工)等。
- 下一步，將數據機(例如 DSL/FTTX(GPON)/Cable modem)的實體連線類型設定成 ISP 業者提供的類型，檢查路由器的 LED 燈號是否顯示亮燈。
- 如果沒亮燈，請另安裝交換器連接路由器與數據，接著再次檢查路由器的 LED 燈號是否顯示亮燈。
- 如果上述步驟還是無法解決 LED 燈號的問題，請與最近的經銷商聯絡，或是寄郵件予居易客服尋求進一步的技術援助。
- 檢查 ISP 提供的設定是否配置完成。

LED 燈號正確但是 WAN 連線還是無法成功，則：

- 開啟**廣域網路(WAN)>>網際網路連線設定**，檢查 ISP 設定是否正確，按下**細節頁面**檢視之前的內容。



VIII-6 3G/4G 網路連線相關問題

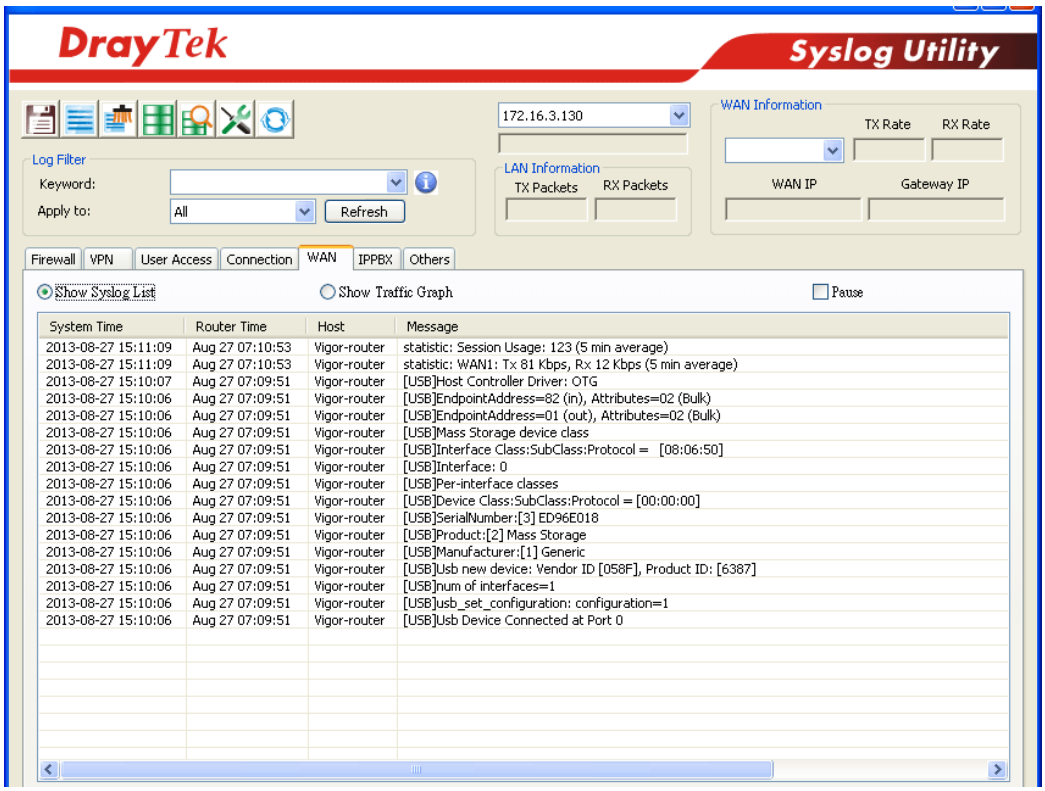
當您使用 3G/4G 網路傳輸發現問題時，請先檢查下列各項：

檢查 USB LED 燈號

在插入 3G/4G USB Modem 至 Vigor2135 後，您必須等待 15 秒左右，稍後 USB LED 會亮燈，表示 3G/4G USB Modem 安裝成功。如果 USB LED 燈號未亮，請將 3G/4G USB Modem 移除再重新插入，如果仍然失敗，請重新啟動路由器。

USB LED 亮燈但是網路連線依然失敗

檢查 SIM 卡上的 PIN 碼是否是關閉的，請使用 3G/4G USB Modem 的工具關閉 PIN 碼然後再試一次。如果還是不行，那就可能是系統的相容性問題，麻煩開啟 DrayTek Syslog 工具擷取連線資訊(WAN Log) 並將此頁面(類似下述畫面)傳送至居易的服務中心尋求解答。



傳輸速率不夠快

利用筆記型電腦連接 3G/4G USB Modem 來測試連線速度，檢查是否這個問題是 Vigor2135 所造成的，此外，請參考 3G/4G USB Modem 手冊中燈號意義，確保數據機是透過 HSDPA 模式連接網際網路。如果您想要在室內使用 3G/4G USB Modem，請放置在靠窗位置以取得較佳的接收信號。

VIII-7 還原路由器原廠預設值

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

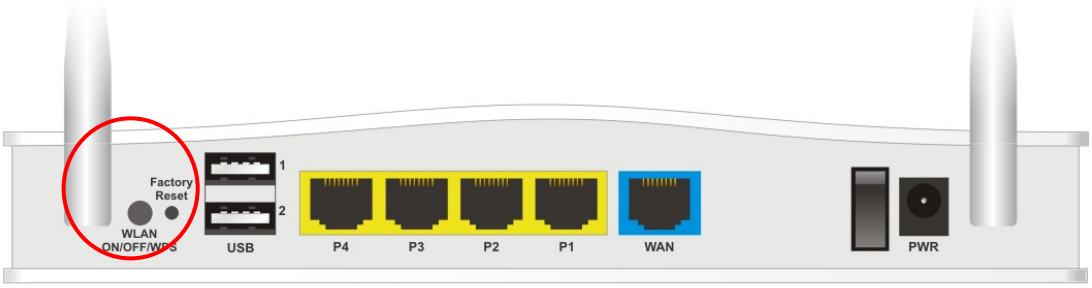
資訊	在使用原廠預設值後，您之前針對分享器所調整的設定都將恢復成預設值。請確實記錄之前路由器所有的設定。

軟體重新設定

請進入管理者模式，再到網頁介面上的**系統維護>>重啟路由器**，可見下圖。選擇**使用出廠預設值**，並按下**立刻重啟**。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。

VIII-8 聯絡居易

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