

# DrayTek

## Vigor2925 系列 雙WAN安全防護路由器

DrayTek



Your reliable networking solutions partner

# 使用手冊

V3.1



# Vigor2925 系列

## 雙 WAN 安全防護路由器

### 使用手冊

版本: 3.1

韌體版本: V3.8.0

(請造訪居易網站，隨時獲取更新資訊)

日期: 2015 年 9 月 4 日

## 版權資訊

### 版權聲明

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

### 商標

本手冊內容使用以下商標：

- Microsoft 為微軟公司註冊商標
- Windows 視窗系列，包括 Windows 95, 98, Me, NT, 2000, XP, Vista, 7 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

### 安全說明

- 在設置前請先閱讀安裝說明。
- 由於路由器是複雜的電子產品，請勿自行拆除或是維修本產品。
- 請勿自行打開或修復路由器。
- 請勿把路由器置於潮濕的環境中，例如浴室。
- 請將本產品放置在足以遮風避雨之處，適合溫度在攝氏 5 度到 40 度之間。
- 請勿將本產品暴露在陽光或是其他熱源下，否則外殼以及零件可能遭到破壞。
- 請勿將 LAN 網線置於戶外，以防電擊危險。
- 請將本產品放置在小孩無法觸及之處。
- 若您想棄置本產品時，請遵守當地的保護環境的法律法規。

### 保固

自使用者購買日起二年內為保固期限(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。

### 成爲一個註冊用戶

建議在 Web 介面進行註冊。您可以到 <http://www.draytek.com.tw> 註冊您的 Vigor 路由器。

### 韌體及工具的更新

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

## 歐盟聲明

廠商: 居易科技股份有限公司  
地址: 臺灣新竹工業區湖口鄉復興路 26 號  
產品: Vigor2925 系列路由器

DrayTek 公司聲明 Vigor2925 服從以下基本要求以及其他 R&TTE 指令（1999/5/EEC）的相關規定。

產品根據 EN55022/Class B 以及 EN55024/Class B 規範，遵從電磁相容性（EMC）指令 2004/108/EEC。

產品根據 EN60951-0 規範，遵從低壓（LVD）2006/95/EC 的要求。

本產品針對 2.4 GHz/5GHz 無線網路而設計，適用範圍遍及歐洲共同體。

## 台灣 NCC 規定

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

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

## 法規資訊

### 聯邦通信委員會干擾聲明

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

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

此產品符合 FCC 規定的第 15 部分。其運作將有以下兩個情況：

- (1) 此產品不會造成有害的干擾，並且
- (2) 此產品可能會遭受其他接收到的干擾，包括那些可能造成不良運作的干擾。

此設備的安裝與操作要離使用者之最小距離為 20 公分。

電磁波曝露量 MPE 標準值  $1\text{mW}/\text{cm}^2$ ，送測產品實測值為： $0.0257\text{mW}/\text{cm}^2$ 。

請造訪 <http://www.draytek.com> 取得更多資訊





# 目錄

## 1

簡介.....	1
1.1 網頁設定按鈕說明 .....	2
1.2 LED 指示燈與介面說明.....	3
1.2.1 Vigor2925 .....	3
1.2.2 Vigor2925ac / Vigor2925n-plus / Vigor2925n.....	5
1.2.3 Vigor2925Vac/ Vigor2925Vn-plus .....	8
1.3 硬體安裝 .....	10
1.4 印表機安裝 .....	11
1.5 進入設定網頁.....	18
1.6 變更密碼.....	19
1.7 儀表板簡介 .....	20
1.7.1 虛擬面板.....	21
1.7.2 底線連結.....	22
1.7.3 常用功能的快速存取 .....	22
1.7.4 圖形介面地圖(GUI Map) .....	24
1.7.5 網頁操作台(Web Console).....	24
1.7.6 設定備份(Config Backup).....	25
1.8 連線狀態 .....	26
1.8.1 實體連線.....	26
1.8.2 虛擬 WAN.....	29
1.9 儲存設定 .....	29

## 2

快速設定 .....	31
2.1 快速設定精靈.....	32
2.1.1 對於 WAN1/WAN2 介面(乙太網路).....	33
2.1.2 對於 WAN3/WAN4 介面 (USB) .....	41
2.2 服務啟動精靈.....	44
2.3 VPN 用戶端設定精靈.....	47
2.4 VPN 伺服器端精靈 .....	53
2.5 無線設定精靈.....	58
2.6 VoIP 設定精靈 .....	62
2.7 註冊 Vigor 路由器 .....	64

# 3

<b>應用與練習</b> .....	<b>69</b>
3.1 如何設定 IPv6 服務.....	69
3.2 如何取得連接至 Vigor 路由器的 USB 裝置內的檔案? .....	80
3.3 如何在總公司與遠端分公司建立 LAN-to-LAN VPN 連線通道(透過 Main 模式).....	83
3.4 QoS 設定範例.....	88
3.5 如何利用 QoS 來最佳化頻寬管理.....	91
3.6 如何客製化登入頁面.....	95
3.7 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.....	98
3.8 如何建立一個 MyVigor 帳號 .....	102
3.8.1 透過 Vigor 路由器來建立.....	102
3.8.2 透過 MyVigor 網站來建立.....	106
3.9 如何限定特定電腦存取網際網路.....	109
3.10 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.....	114
3.11 如何讓內部電腦對應到某個 WAN IP.....	120
3.12 如何設定封包負載平衡? .....	124
3.13 如何透過使用者管理驗證用戶端.....	127
3.14 如何使用 DNS 過濾器.....	136
3.15 CVM 應用 – 如何透過 Vigor2925 管理 CPE (路由器)?.....	139
3.16 CVM 應用 – 如何於 Vigor2925 與遠端設備之間建立 VPN 連線? .....	143
3.17 CVM 應用 – 如何透過 Vigor2925 更新遠端 CPE 韌體?.....	145
3.18 如何在 Vigor2925 系列中搭配使用 SmartMonitor .....	147

# 4

<b>進階設定</b> .....	<b>149</b>
4.1 WAN .....	149
4.1.1 IP 網路的基本概念 .....	149
4.1.2 基本設定.....	151
4.1.3 網際網路連線控制 .....	155
4.1.4 多重 VLAN .....	174
4.1.5 WAN 計量收費 .....	177
4.2 區域網路(LAN).....	180
4.2.1 區域網路基本概念 .....	180
4.2.2 基本設定.....	182
4.2.3 固定路由.....	191
4.2.4 VLAN (虛擬區域網路) .....	196
4.2.5 綁定 IP 與 MAC 位址.....	200
4.2.6 埠口監控.....	201



4.2.7 有線 802.1x .....	202
4.2.8 客製化入口網站設定 .....	203
4.3 負載平衡/策略路由 .....	205
4.4 NAT .....	207
4.4.1 通訊埠重導向 .....	208
4.4.2 DMZ 主機設定 .....	211
4.4.3 開放通訊埠 .....	214
4.4.4 埠號觸發 .....	215
4.5 硬體加速 .....	219
4.5.1 設定 .....	219
4.6 防火牆 .....	220
4.6.1 防火牆基本常識 .....	220
4.6.2 基本設定 .....	223
4.6.3 過濾器設定 .....	228
4.6.4 DoS 攻擊防禦功能設定 .....	235
4.7 使用者管理 .....	238
4.7.1 基本設定 .....	239
4.7.2 使用者設定檔 .....	241
4.7.3 使用者群組 .....	245
4.7.4 使用者線上狀態 .....	246
4.8 物件設定 .....	247
4.8.1 IP 物件設定檔 .....	247
4.8.2 IP 群組 .....	250
4.8.3 IPv6 物件 .....	252
4.8.4 IPv6 群組 .....	254
4.8.5 服務類型物件 .....	255
4.8.6 服務類型群組 .....	257
4.8.7 關鍵字物件 .....	258
4.8.8 關鍵字群組 .....	260
4.8.9 副檔名物件 .....	261
4.8.10 簡訊(SMS)/郵件服務物件 .....	263
4.8.11 通知物件 .....	268
4.9 數位內容安全管理(CSM)設定檔 .....	270
4.9.1 應用程式管控設定檔 .....	271
4.9.2 APPE 特徵碼更新 .....	275
4.9.3 URL 內容過濾器設定檔 .....	276
4.9.4 網頁內容過濾器設定檔 .....	280
4.9.5 DNS 過濾器設定檔 .....	283
4.10 頻寬管理 .....	285
4.10.1 NAT 連線數限制 .....	285
4.10.2 頻寬限制 .....	287
4.10.3 服務品質(QoS) .....	289
4.11 其他應用 .....	298
4.11.1 動態 DNS .....	298
4.11.2 LAN DNS / DNS 轉送 .....	301

4.11.3 排程.....	304
4.11.4 RADIUS/TACACS+ .....	306
4.11.5 Active Directory/ LDAP .....	307
4.11.6 UPnP.....	310
4.11.7 IGMP.....	312
4.11.8 網路喚醒(WOL).....	313
4.11.9 簡訊(SMS) / 郵件警示服務.....	314
4.11.10 Bonjour .....	316
4.12 VPN 與遠端存取.....	319
4.12.1 遠端存取控制 .....	319
4.12.2 PPP 基本設定 .....	320
4.12.3 IPSec IPsec 基本設定 .....	321
4.12.4 IPSec 端點辨識.....	323
4.12.5 遠端撥入使用者.....	325
4.12.6 設定 LAN to LAN.....	329
4.12.7 VPN TRUNK 管理.....	339
4.12.8 連線管理.....	349
4.13 憑證管理 .....	350
4.13.1 本機憑證.....	350
4.13.2 具公信力之 CA 憑證.....	354
4.13.3 憑證備份.....	355
4.14 VPN 中央管理.....	355
4.14.1 基本設定.....	356
4.14.2 CPE 管理 .....	358
4.14.3 VPN 管理 .....	364
4.14.4 紀錄與警示 .....	366
4.15 AP 中央管理 .....	367
4.15.1 狀態.....	367
4.15.2 WLAN 設定檔.....	368
4.15.3 AP 維護.....	373
4.15.4 流量圖表.....	374
4.15.5 非法 AP 偵測(Rogue).....	374
4.15.6 負載平衡.....	378
4.15.7 功能支援列表 .....	379
4.16 無線區域網路設定 .....	380
4.16.1 基本觀念.....	380
4.16.2 基本設定.....	382
4.16.3 安全性設定.....	385
4.16.4 連線控制.....	388
4.16.5 WPS.....	390
4.16.6 WDS.....	393
4.16.7 進階設定.....	396
4.16.8 WMM 設定 .....	397
4.16.9 搜尋無線基地台.....	399
4.16.10 無線用戶端列表.....	400
4.17 SSL VPN .....	401
4.17.1 基本設定.....	401
4.17.2 SSL 網頁代理伺服器.....	402
4.17.3 SSL 應用設定.....	403

4.17.4 使用者帳號.....	406
4.17.5 使用者群組.....	410
4.17.6 線上使用者狀態.....	412
4.18 USB 應用.....	413
4.18.1 USB 基本設定.....	413
4.18.2 USB 使用者管理.....	414
4.18.3 檔案瀏覽.....	417
4.18.4 USB 磁碟狀態.....	417
4.18.5 Syslog 系統資源管理.....	418
4.18.6 溫度感應器.....	420
4.18.7 數據機支援清單.....	421
4.19 系統維護.....	422
4.19.1 系統狀態.....	422
4.19.2 TR-069.....	424
4.19.3 系統管理員密碼.....	425
4.19.4 使用者密碼.....	426
4.19.5 登入頁面設定.....	428
4.19.6 設定備份.....	430
4.19.7 Syslog/郵件警示設定.....	432
4.19.8 時間和日期.....	434
4.19.9 SNMP.....	436
4.19.10 管理.....	438
4.19.11 重啓路由器.....	440
4.19.12 韌體升級.....	441
4.19.13 開啓授權碼.....	442
4.20 自我診斷工具.....	443
4.20.1 撥號觸發器.....	443
4.20.2 路由表.....	444
4.20.3 ARP 快取表.....	445
4.20.4 IPv6 芳鄰表.....	445
4.20.5 DHCP 表.....	446
4.20.6 NAT 連線數狀態表.....	447
4.20.7 Ping 自我診斷.....	448
4.20.8 資料流量監控.....	449
4.20.9 流量圖表.....	451
4.20.10 追蹤路由.....	452
4.20.11 網頁防火牆 Syslog.....	453
4.20.12 IPv6 TSPC 狀態.....	455
4.21 外接裝置.....	455

## 5

### 疑難排解..... 457

5.1 檢查路由器硬體狀態是否正常.....	457
5.2 檢查您電腦的網路連接設置是否正確.....	458
5.3 從電腦上 Ping 路由器.....	461
5.4 檢查 ISP 的設置是否正常.....	462

5.5 3G 網路連線相關問題.....	462
5.6 還原路由器原廠預設組態.....	463
5.7 聯絡居易.....	464

# 1 簡介

Vigor2925 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。

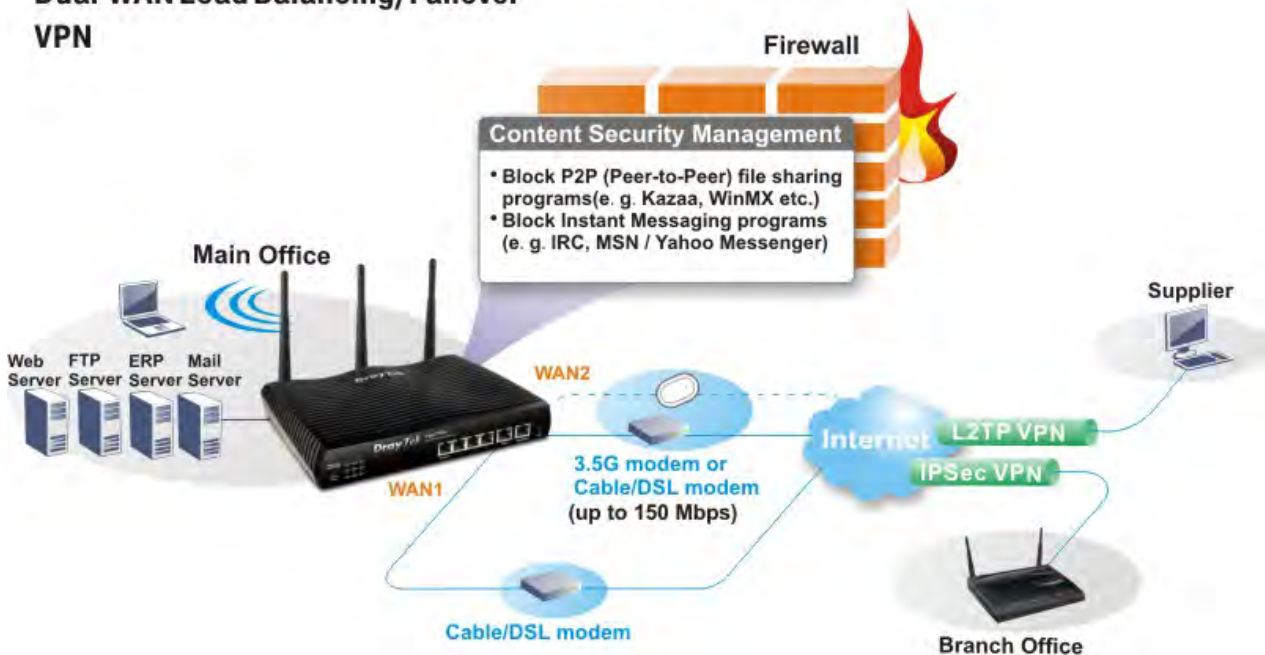
藉由採用硬體 VPN 平臺及 AES/DES/3DS 硬體加密方式，Vigor2925 系列大大提昇了 VPN 的效用，並在 VPN 通道中提供數種協定(諸如 IPSec/PPTP/L2TP) 應用。

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。

物件式防火牆相當具有彈性，可讓您的網路更加的安全，此外，Vigor2925 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。

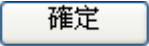


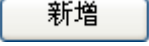
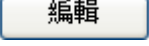

Vigor2925 系列提供二層式管理簡化網路連線設定，使用者模式讓使用者透過簡易設定達到存取網頁的目的，若是使用者想設定進階功能，可以透過管理者模式來處理。

## Security & Firewall Dual-WAN Load Balancing/Failover VPN



## 1.1 網頁設定按鈕說明

在路由器的網頁設定中，有數種常見的按鈕，其定義如下所示：

	儲存並套用目前的設定。
	取消目前設定並回復先前的設定值。
	捨棄目前設定值並允許使用者重新輸入。
	指定項目新增設定。
	編輯選定項目的設定。
	刪除選定項目及相關設定。

**附註:**有關網頁上所出現的其他按鈕，請參考第三章。

## 1.2 LED 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：

### 1.2.1 Vigor2925



LED	狀態	說明
ACT (活動)	閃爍	路由器已開機並可正常運作。
	熄燈	路由器已關機。
WAN1 ~ WAN2	亮燈	WAN 介面已連接。
	熄燈	WAN 介面未連接。
	閃爍	資料封包傳輸中。
QoS	亮燈	QoS 功能已開啓。
USB1~USB2	亮燈	USB 裝置已連接並運作中。
	閃爍	正在傳輸資料中。
WCF	亮燈	網頁內容過濾器已啓動(此功能是在 <b>防火牆 &gt;&gt;基本設定</b> 中所驅動)。
VPN	亮燈	VPN 通道已建立。
DMZ	亮燈	DMZ 子網路功能已啓用
	熄燈	DMZ 子網路功能尚未啓用
	閃爍	資料傳輸中。

#### 連接介面上的燈號

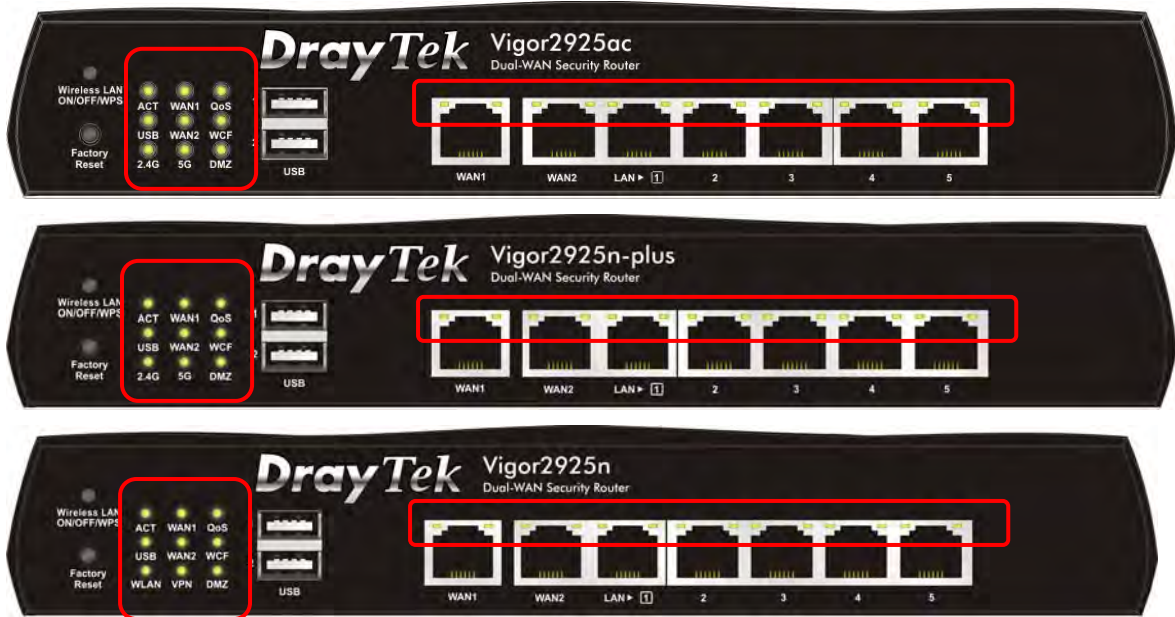
WAN1~ WAN2	左 LED (綠)	亮燈	介面網路已連接。
		熄燈	介面網路未連接。
		閃爍	正在傳輸資料中。
	右 LED (綠)	亮燈	介面的連接速度為 1000Mbps。
		熄燈	介面的連接速度為 100Mbps。
		閃爍	正在傳輸資料中。
LAN1~ LAN5	左 LED (綠)	亮燈	乙太網路已連接。
		熄燈	乙太網路未連接。
		閃爍	正在傳輸資料中。
	右 LED (綠)	亮燈	介面的連接速度為 1000Mbps。
		熄燈	介面的連接速度為 100Mbps。
		閃爍	正在傳輸資料中。



介面	說明
Factory Reset	還原成出廠預設值。 用法：當路由器正在運作時（ACT LED 燈號閃爍），利用尖銳的物品（例如：原子筆）壓住 Factory Reset 超過 5 秒；當 ACT LED 燈號開始迅速閃爍時，鬆開此動作，路由器將會還原成出廠預設值。
USB1~USB2	連接到 USB 3G/4G 數據機、印表機或是環境溫度計。
WAN1~WAN2	連接到 ADSL 或是 Cable Modem 裝置。
LAN1~LAN5	連接到電腦或網路設備。
PWR	連接電源變壓器。
ON/OFF	電源開關，“1” 為開，“0” 為關。



## 1.2.2 Vigor2925ac / Vigor2925n-plus / Vigor2925n

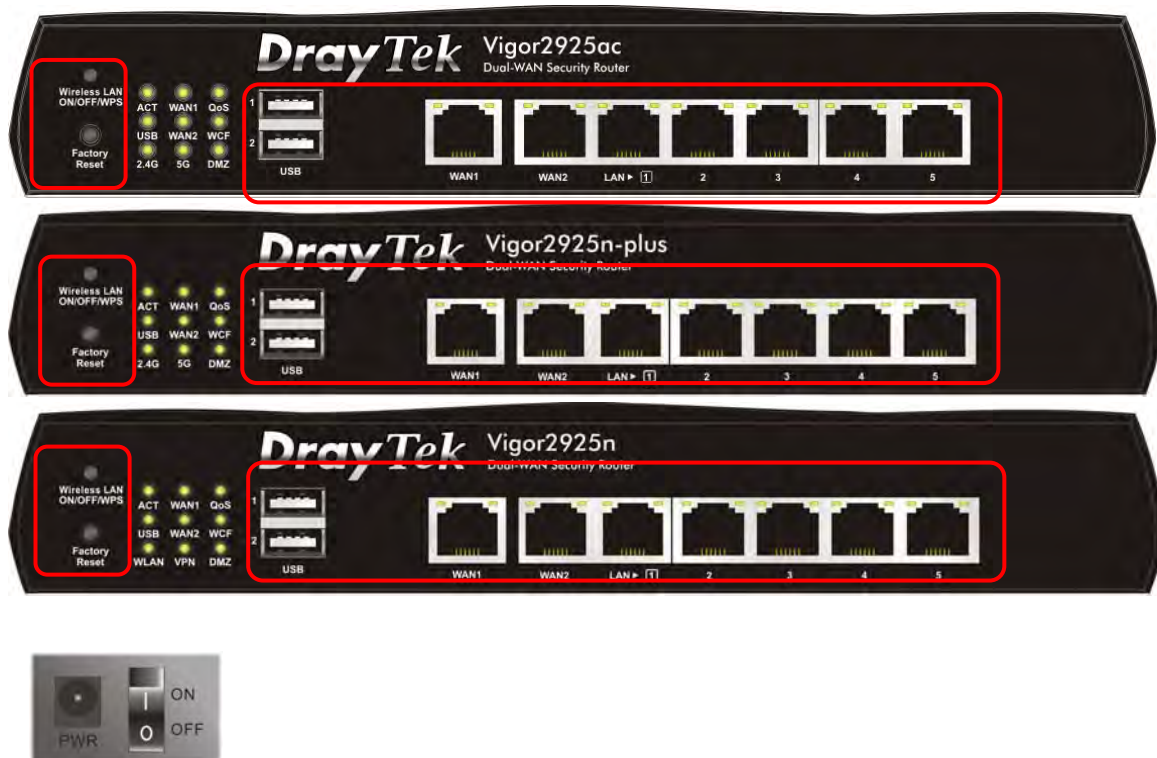


LED	狀態	說明
ACT (活動)	閃爍	路由器已開機並可正常運作。
	熄燈	路由器已關機。
WAN1~WAN2	亮燈	WAN 介面已連接。
	熄燈	WAN 介面未連接。
	閃爍	資料封包傳輸中。
QoS	亮燈	QoS 功能已開啓。
USB	亮燈	USB 裝置已連接並運作中。
	閃爍	正在傳輸資料中。
WCF	亮燈	網頁內容過濾器已啓動(此功能是在 <b>防火牆 &gt;&gt;基本設定</b> 中所驅動)。
2.4G/5G/WLAN	亮燈	2.4G/5G: 無線基地台(頻寬為 2.4G/5G)已準備妥當, 等待使用中。 WLAN: 無線基地台準備妥當。
	閃爍	無線資料傳輸時, 此燈號會慢速閃爍。 當 WPS 運作時, 如果 ACT 及 WLAN 燈號同時快速閃爍, 那麼大約 2 分鐘後會回到正常狀態 (您必須在 2 分鐘內設定完畢 WPS 功能)。
VPN	亮燈	VPN 通道已建立。
	熄燈	停用 VPN 服務。
	閃爍	系統正透過 VPN 通道進行資料運送。
DMZ	亮燈	DMZ 子網路功能已啓用
	熄燈	DMZ 子網路功能尚未啓用
	閃爍	資料傳輸中。

### 連接介面上的燈號

	左 LED (綠)	亮	介面網路已連接。
--	-----------	---	----------

WAN2		暗	介面網路未連接。
		閃爍	正在傳輸資料中。
	右 LED (綠)	亮	介面的連接速度為 1000Mbps。
		暗	介面的連接速度為 100Mbps。
LAN1~ LAN5	左 LED (綠)	亮	乙太網路已連接。
		暗	乙太網路未連接。
		閃爍	正在傳輸資料中。
	右 LED (綠)	亮	介面的連接速度為 1000Mbps。
		暗	介面的連接速度為 100Mbps。



介面	說明
Wireless LAN ON/OFF/WPS	<p>針對 Vigor2925n:</p> <ul style="list-style-type: none"> <li>● 按下此鈕並在二秒鐘內放開，可開啓無線功能。WLAN LED 亮綠燈。</li> <li>● 按下此鈕並在二秒鐘內放開，可關閉無線功能。WLAN LED 熄燈。</li> </ul> <p>針對 Vigor2925ac/Vigor2925n-plus :</p> <p>依照按壓及釋放按鈕的方式來切換不同的無線頻寬，例如</p> <ul style="list-style-type: none"> <li>● 2.4G (亮燈)及 5G (亮燈) – 此為預設值。</li> <li>● 2.4G (熄燈)及 5G (亮燈) – 按壓及釋放按鈕一次。僅開啓 5G 無線功能。</li> <li>● 2.4G (亮燈)及 5G (熄燈) – 按壓及釋放按鈕二次。僅開啓 2.4G 無線功能。</li> <li>● 2.4G (熄燈)及 5G (熄燈) – 按壓及釋放按鈕三次。關閉無線功能。</li> </ul> <p>WPS - 當 WPS 功能已經透過網頁設定介面啓動，可按壓此鈕超過二秒，路由器將等待無線用戶端進行遠端連線。</p>
Factory Reset	<p>還原成出廠預設值。</p> <p>用法：當路由器正在運作時（ACT LED 燈號閃爍），利用尖銳的物品（例如：原子筆）壓住 Factory Reset 超過 5 秒；當 ACT LED 燈號開始迅速閃爍時，鬆開此動作，路由器將會還原成出廠預設值。</p>
USB1~USB2	<p>連接到 USB 3G/4G 數據機、印表機或是環境溫度計。</p>
WAN1~WAN2	<p>連接到 ADSL 或是 Cable Modem 裝置。</p>
LAN1~LAN5	<p>連接到電腦或網路設備。</p>
PWR	<p>連接電源變壓器。</p>
ON/OFF	<p>電源開關，“1” 為開，“0” 為關。</p>

### 1.2.3 Vigor2925Vac/ Vigor2925Vn-plus



LED	狀態	說明
ACT (Activity)	閃爍	路由器已開機並可正常運作。
	熄燈	路由器已關機。
WAN1~WAN2	亮燈	WAN 介面已連接。
	熄燈	WAN 介面未連接。
	閃爍	資料封包傳輸中。
Line	亮燈	PSTN 電話撥進或撥出，當電話斷線時，LED 燈號即會熄滅。
	熄燈	目前沒有 PSTN 電話。
USB	亮燈	USB 裝置已連接，等待使用中
	閃爍	正在傳輸資料中。
Phone1/2	亮燈	連接本埠之電話使用中。
	熄燈	連接本埠之電話未被使用。
	亮燈	電話來電。
2.4G/5G	亮燈	無線基地台已準備妥當，等待使用中。
	閃爍	無線資料傳輸時，此燈號會慢速閃爍。當 WPS 運作時，ACT 和 WLAN 燈號會同時快速閃爍，2 分鐘後會回到正常狀態(您需要在 2 分鐘內設定 WPS。)

#### 連接介面上的燈號

WAN1~ WAN2	左 LED (綠燈)	亮燈	介面網路已連接。
		熄燈	介面網路未連接。
		閃爍	正在傳輸資料中。
	右 LED (綠燈)	亮燈	介面的連接速度為 1000Mbps。
		暗	介面的連接速度為 10/100Mbps。
LAN1~ LAN5	左 LED (綠燈)	亮燈	介面網路已連接。
		熄燈	介面網路未連接。
		閃爍	正在傳輸資料中。
	右 LED (綠燈)	亮燈	介面的連接速度為 1000Mbps。
		熄燈	介面的連接速度為 10/100Mbps。





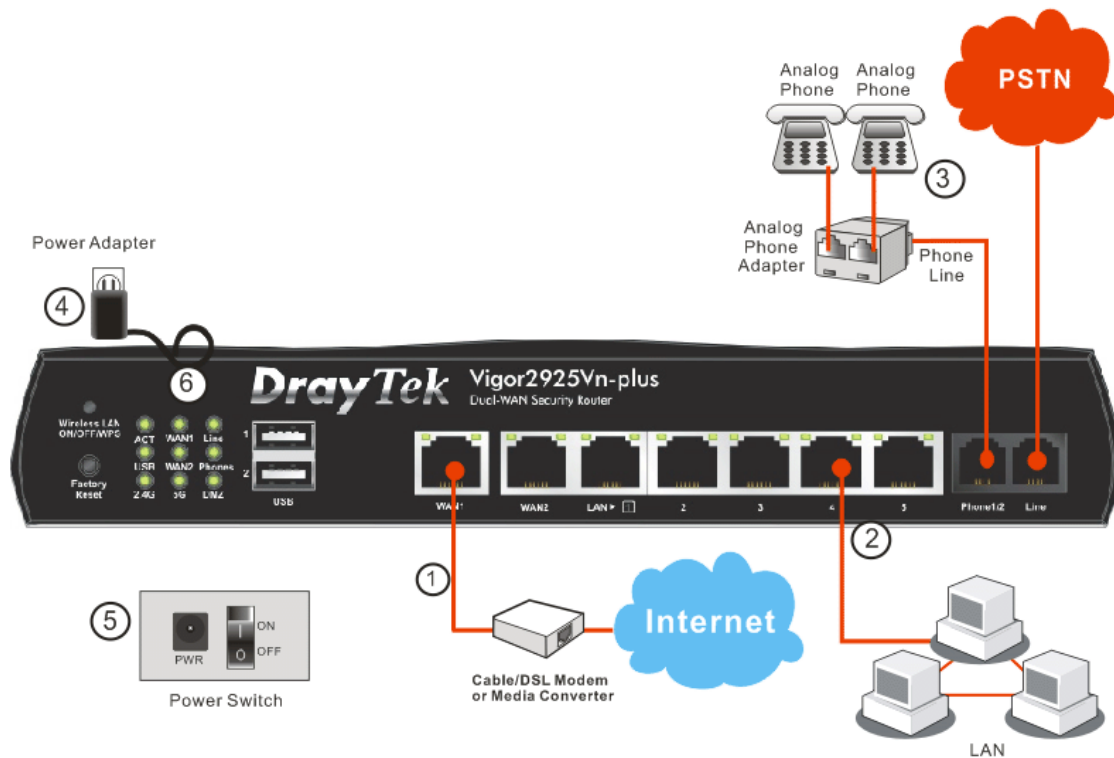
介面	說明
Wireless LAN ON/OFF/WPS	<p>依照按壓及釋放按鈕的方式來切換不同的無線頻寬，例如</p> <ul style="list-style-type: none"> <li>● 2.4G (亮燈)及 5G (亮燈) – 此為預設值。</li> <li>● 2.4G (熄燈)及 5G (亮燈) – 按壓及釋放按鈕一次。僅開啓 5G 無線功能。</li> <li>● 2.4G (亮燈)及 5G (熄燈) – 按壓及釋放按鈕二次。僅開啓 2.4G 無線功能。</li> <li>● 2.4G (熄燈)及 5G (熄燈) – 按壓及釋放按鈕三次。關閉無線功能。</li> </ul> <p>WPS - 當 WPS 功能已經透過網頁設定介面啓動，可按壓此鈕超過二秒，路由器將等待無線用戶端進行遠端連線。</p>
Factory Reset (出廠預設值按鈕)	<p>還原成出廠預設值。</p> <p>使用方法：開啓路由器 (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。路由器隨後將重新啓動，並回復出廠預設值。</p>
USB1~USB2	連接到 USB 3G 數據機、印表機或是環境溫度計。
WAN1~WAN2	連接到 ADSL 或是 Cable Modem 裝置。
LAN1~LAN5	連接到電腦或網路設備。
Phone 1/2	連接類比電話機，以便使用 VoIP 通話功能。
PWR	連接電源變壓器。
ON/OFF	電源開關，“1” 為開，“0” 為關。

## 1.3 硬體安裝

設定路由器前(以 Vigor2925Vn-Plus 為例)，請先將裝置確實連接，並參考以下步驟操作。

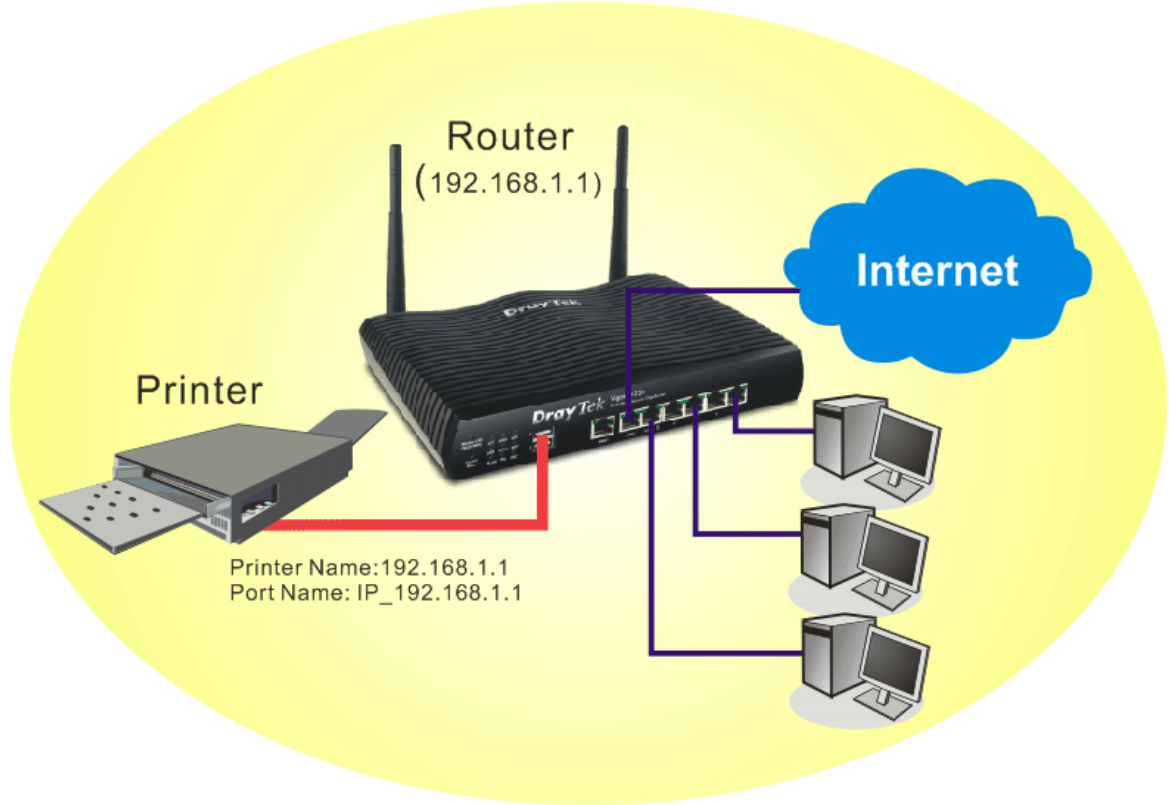
1. 使用乙太網路線(RJ-45)連接數據機/DSL 數據機/Media Converter 至本裝置的 WAN 連接埠。
2. 利用 RJ-45 纜線連接路由器(LAN 連接埠中選定其中一個)與您的電腦。
3. 利用使用纜線連接 Analog Phone Adapter 與路由器(Phone1/2 的接孔)，Adapter 的另一端連接一般話機。
4. 將電源轉換器一端連接至路由器，另一端則連至牆上電源輸出孔。
5. 開啓路由器電源。
6. 檢查 ACT 與 LAN 燈號是否亮燈以確保連線無誤。

(有關燈號的詳細說明，請參考 1.2 一節)



## 1.4 印表機安裝

您可以在路由器上連接印表機來分享列印功能，這樣路由器的區域網路上所有的電腦都可透過它列印檔案，以下設定範例是以 Windows XP/2000 為主，如果您使用的是 Windows 98/SE/Vista，請造訪居易網站 [www.draytek.com](http://www.draytek.com) 取得您所需要的安裝資訊。



使用之前，請務必按照下列步驟來設定您的電腦（或無線用戶）：

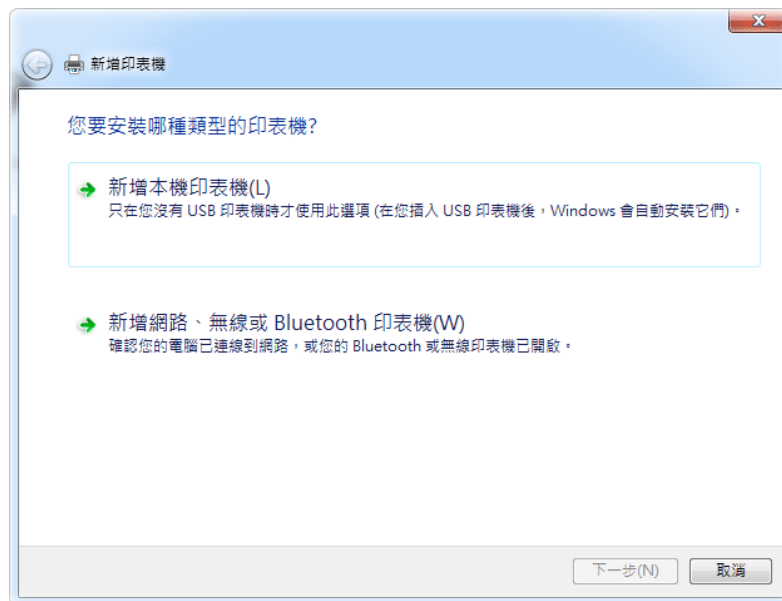
1. 請透過 USB 連接埠連接印表機與路由器。
2. 開啓開始>>所有程式>>裝置和印表機。



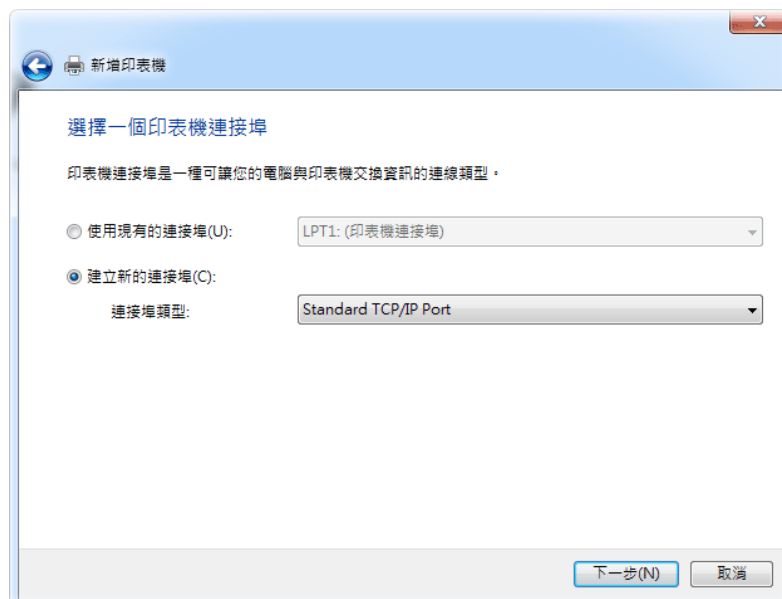
3. 按下新增印表機。



4. 選擇“新增本機印表機”並按下一步。

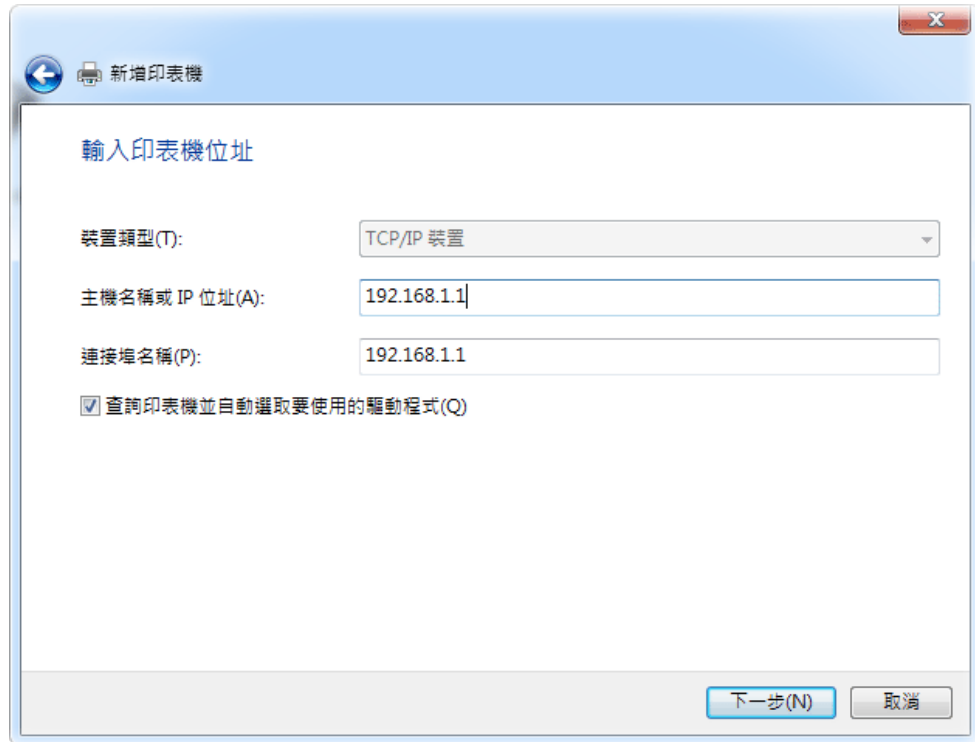


5. 接著請選擇“建立新的連接埠”，用下拉式選項選擇“Standard TCP/IP Port”，按下一步。

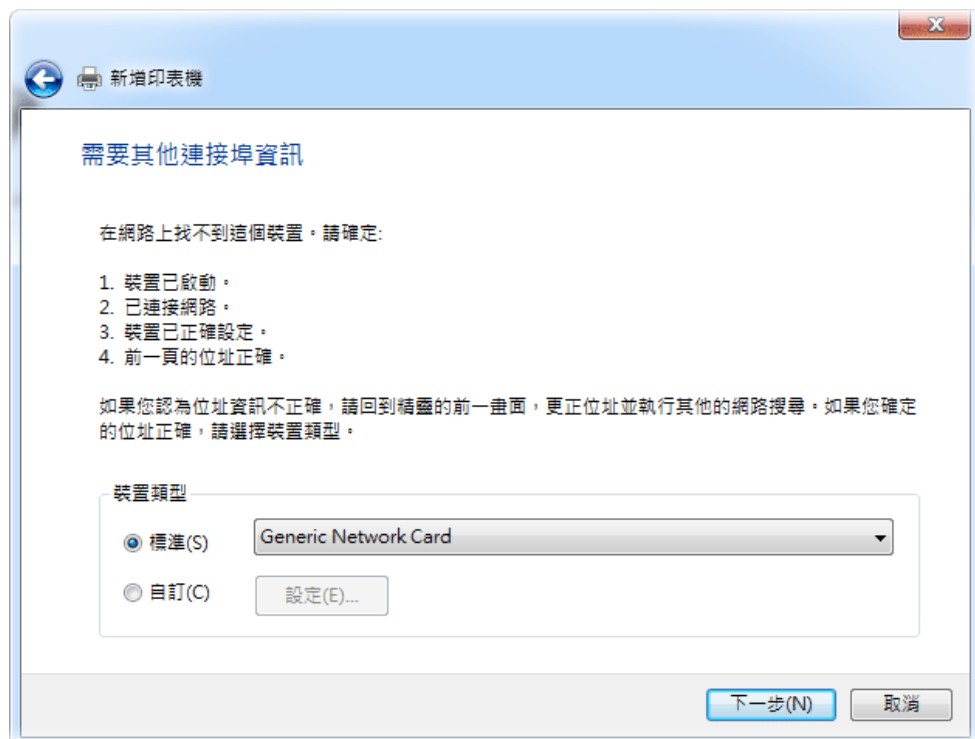




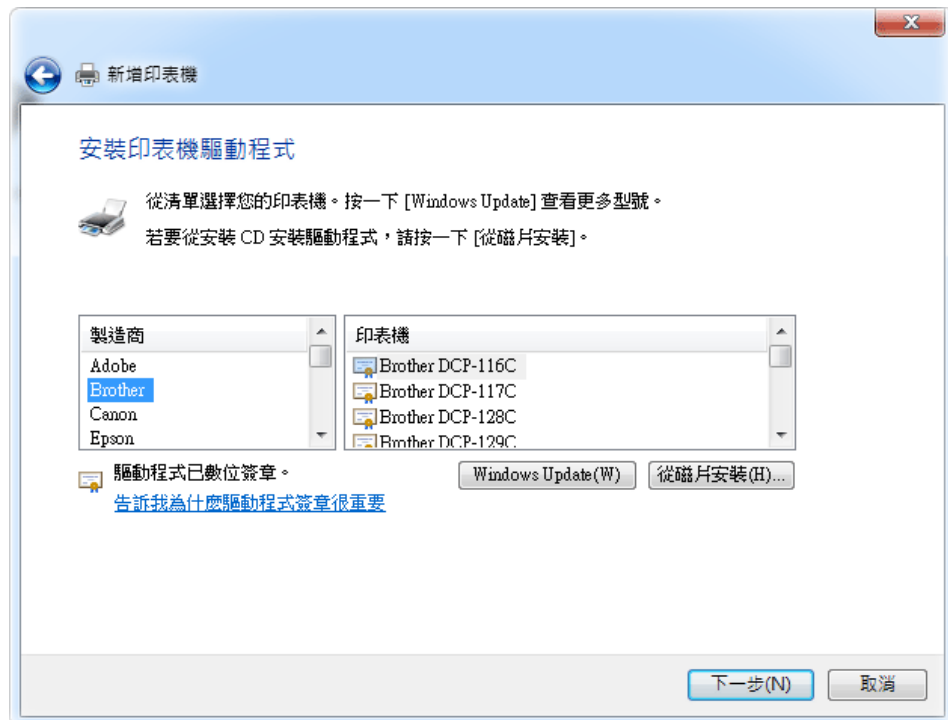
6. 在下面的對話方塊中，請在主機名稱或 IP 位址欄位輸入 **192.168.1.1** (路由器的 LAN IP)，再按下一步。請輸入 **192.168.1.1** (路由器的 LAN IP)，**IP\_192.168.1.1** 會自動帶出，再按下一步。



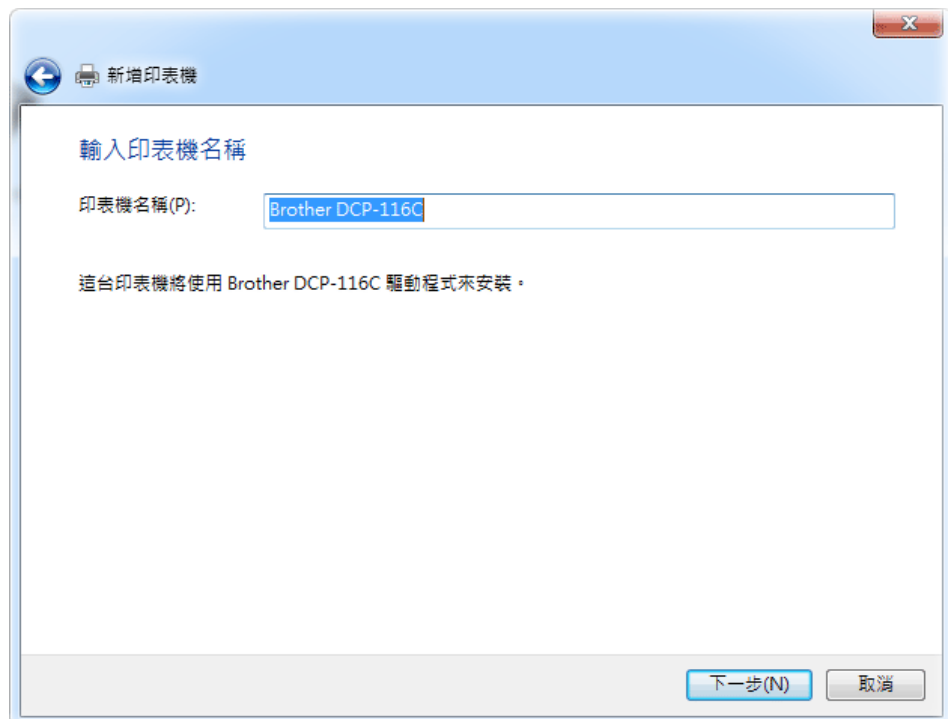
7. 請選擇**標準**，並自下拉式選項中選取 **Generic Network Card**，再按下一步。



8. 現在系統將會要求您選擇您安裝至路由器上的印表機名稱，這個步驟可以讓您的電腦安裝正確的驅動程式，當您完成項目選擇之後，請按下一步。



9. 輸入印表機名稱，繼續按下一步。



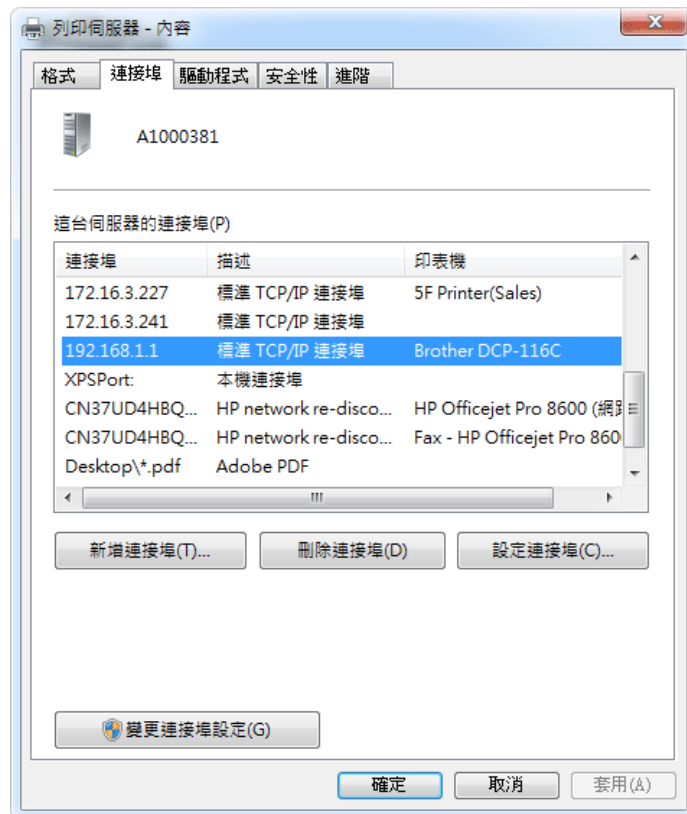
10. 在如下的對話盒，請按**完成**。



11. 新的印表機圖示已出現在**印表機和傳真**區域中，請按新圖示然後在按下列**印伺服器內容**標籤。



12. 如下頁面出現後，請按**設定連接埠**，編輯新增印表機的內容。



13. 在通訊協定欄位中，選擇**"LPR"**，佇列名稱則請輸入”p1”，按下**確定**鈕。



您現在可以使用新增的印表機了，大多數的印表機都與 Vigor 路由器相容。

**注意 1:** 此路由器仍不支援市面上某些印表機，如果您不知道自己所購買的印表機有無在支援之列，請造訪 [www.draytek.com](http://www.draytek.com)，上面可輕易取得您想知道的訊息，開啓技術支援>>技術問答，按下 **USB 設定** 連結，接著再按下 **Vigor router 相容印表機列表?** 連結，即可獲得您要的內容。

The screenshot shows the DrayTek website's technical support section. The breadcrumb trail is: 首頁 > 技術支援 > 技術問答 > USB 設定. The main heading is 'USB 設定'. Below it is a list of six articles:

Article Title	Date
1. Vigor Router 支援 3.5G 數據機列表	2012/08/15
2. Vigor Router 相容印表機列表?	2012/11/28
3. Vigor Router 支援 WiMAX 列表	2011/09/27
4. Vigor Router 支援 3.5G 行動電話列表	2011/06/29
5. 在Windows7環境下，如何新增印表機	2011/03/03
6. 如何設定 USB Disk for FTP 功能?	2011/01/26

**注意 2:** Vigor 路由器支援來自 LAN 端的列印要求，但不支援來自 WAN 端的列印要求。

## 1.5 進入設定網頁

1. 確保您的電腦已經和路由器正確的連接。



**附註:** 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。

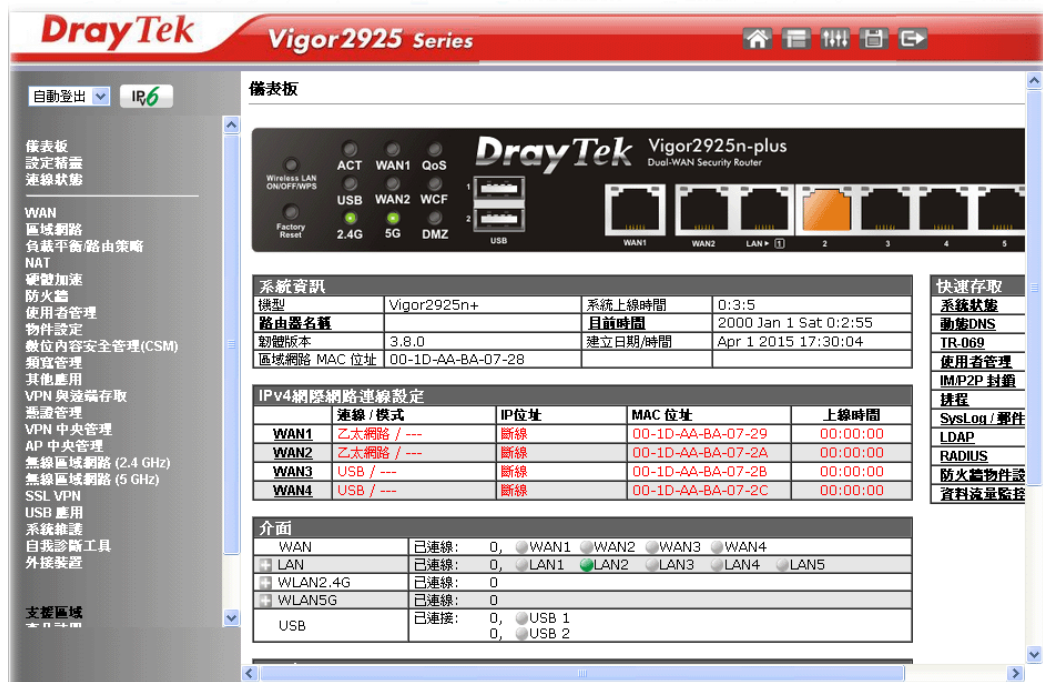
2. 開啓網頁瀏覽器並輸入位址 <http://192.168.1.1>，登入視窗將會出現。

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



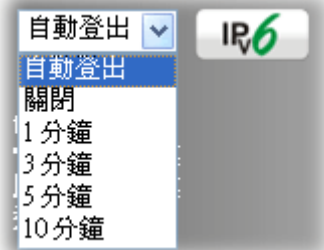
**注意:** 如果您無法進入網頁設定畫面，請參考“疑難排解”以解決您所面臨的問題。

- 現在，設定介面的主選單會出現。



**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。

- 網頁將會依照您所選擇的條件開啓不同的頁面，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。



## 1.6 變更密碼

為了路由器的安全起見，建議您將先行變更密碼。

- 開啓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。
- 請輸入“admin/admin”進入管理者模式，
- 進入系統維護頁面並選擇系統管理員密碼。

系統管理員密碼

舊密碼	<input type="text"/>
新密碼	<input type="text"/>
確認密碼	<input type="text"/>

附註:密碼只能包含 a-z A-Z 0-9 , ; : . " < > \* + = \ | ? @ # ^ ! ( )

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. 現在您已經完成變更密碼設定。請記得在下一次登入設定介面時使用新的密碼。



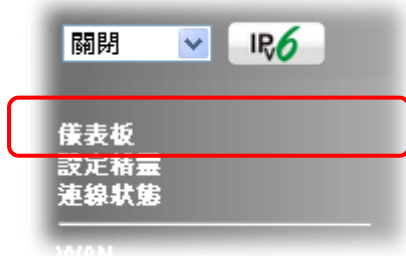
The image shows the login page for the DrayTek Vigor2925 Series. At the top, there is a red banner with the DrayTek logo and 'Vigor2925 Series'. Below this is a black header with the word 'Login' in white. The main area contains three input fields: '使用者名稱' (Username) with 'admin' entered, '密碼' (Password) with masked characters, and '群組' (Group) with a dropdown arrow. A '登入' (Login) button is positioned to the right of the fields. At the bottom, there is a copyright notice: 'Copyright © 2013 DrayTek Corp. All Rights Reserved.'

**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”。

## 1.7 儀表板簡介

儀表板顯示各種連線狀態，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：





系統資訊			
機型	Vigor2925n+	系統上線時間	0:6:45
路由器名稱		目前時間	2000 Jan 1 Sat 0:6:35
韌體版本	3.8.0	建立日期/時間	Apr 1 2015 17:30:04
區域網路 MAC 位址	00-1D-AA-BA-07-28		

快速存取
<a href="#">系統狀態</a>
<a href="#">動態DNS</a>
<a href="#">TR-069</a>
<a href="#">使用者管理</a>
<a href="#">IM/P2P 封鎖</a>
<a href="#">排程</a>
<a href="#">SysLog / 郵件警示</a>
<a href="#">LDAP</a>
<a href="#">RADIUS</a>
<a href="#">防火牆物件設定</a>
<a href="#">資料流量監控</a>

IPv4 網際網路連線設定				
	連線 / 模式	IP位址	MAC 位址	上線時間
WAN1	乙太網路 / ---	斷線	00-1D-AA-BA-07-29	00:00:00
WAN2	乙太網路 / ---	斷線	00-1D-AA-BA-07-2A	00:00:00
WAN3	USB / ---	斷線	00-1D-AA-BA-07-2B	00:00:00
WAN4	USB / ---	斷線	00-1D-AA-BA-07-2C	00:00:00

介面	
WAN	已連線: 0, <input type="radio"/> WAN1 <input type="radio"/> WAN2 <input type="radio"/> WAN3 <input type="radio"/> WAN4
LAN	已連線: 0, <input type="radio"/> LAN1 <input checked="" type="radio"/> LAN2 <input type="radio"/> LAN3 <input type="radio"/> LAN4 <input type="radio"/> LAN5
WLAN2.4G	已連線: 0
WLAN5G	已連線: 0
USB	已連接: 0, <input type="radio"/> USB 1 <input type="radio"/> USB 2

### 1.7.1 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。

#### Dashboard



燈號位置	顏色顯示	說明
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。
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。

有關燈號的詳細說明，請參考 **1.2 LED 指示燈與介面說明** 一節。

## 1.7.2 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、WAN1/2/3 等等.)表示您可以按下該連結開啓設定頁面。

系統資訊				
機型	Vigor2925n	系統上線時間	25:15:10	
<u>路由器名稱</u>		<u>目前時間</u>	2000 Jan 2 Sun 1:15:0	
韌體版本	3.7.2.2	建立日期/時間	Aug 22 2013 16:44:25	
區域網路 MAC 位址	00-1D-AA-AC-19-C8			

IPv4網際網路連線設定				
	連線 / 模式	IP位址	MAC 位址	上線時間
<u>WAN1</u>	乙太網路 / PPPoE	斷線	00-1D-AA-AC-19-C9	00:00:00
<u>WAN2</u>	乙太網路 / ---	斷線	00-1D-AA-AC-19-CA	00:00:00
<u>WAN3</u>	USB / ---	斷線	00-1D-AA-AC-19-CB	00:00:00

## 1.7.3 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，系統提供一個更爲方便快速快速的方式來開啓。

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。

快速存取
<u>系統狀態</u>
<u>動態 DNS</u>
<u>TR-069</u>
<u>使用者管理</u>
<u>IM/P2P 封鎖</u>
<u>排程</u>
<u>SysLog / 郵件警示</u>
<u>LDAP</u>
<u>RADIUS</u>
<u>防火牆物件設定</u>
<u>資料流量監控</u>

本區將系統狀態、動態 DNS、TR-069、使用者管理、IM/P2P 封鎖、排程、Syslog/郵件警示、LDAP、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在輕輕按下，相應頁面即可立刻開啓。

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。

介面	
WAN	Connected : 1, <input checked="" type="radio"/> WAN1 <input type="radio"/> WAN2 <input type="radio"/> WAN3
<input checked="" type="checkbox"/> LAN	Connected : 0, <input type="radio"/> LAN1 <input type="radio"/> LAN2 <input type="radio"/> LAN3 <input checked="" type="radio"/> LAN4 <input type="radio"/> LAN5
USB	Connected : 0, <input type="radio"/> USB 1 0, <input type="radio"/> USB 2

安全性設定	
<input checked="" type="checkbox"/> VPN	已連線 : 0 <span style="float: right;">遠端撥入使用者 / LAN to LAN</span>

請注意畫面上 VPN/LAN 的左邊有個小小的加號(+)圖示，按此圖示可以檢查目前使用中的 VPN 連線內容。

安全性設定			
<input checked="" type="checkbox"/> VPN	已連線 : 0 <span style="float: right;">遠端撥入使用者 / LAN to LAN</span>		
目前頁面: 1 <span style="float: right;">頁面編號 1 <input type="button" value="前往"/></span>			
名稱 / 使用者	類型 / 安全性	主機 IP	上線時間

介面							
WAN	Connected : 1, <input checked="" type="radio"/> WAN1 <input type="radio"/> WAN2 <input type="radio"/> WAN3						
<input checked="" type="checkbox"/> LAN	Connected : 1, <input type="radio"/> LAN1 <input type="radio"/> LAN2 <input type="radio"/> LAN3 <input checked="" type="radio"/> LAN4 <input type="radio"/> LAN5						
	<table border="1"> <thead> <tr> <th>Host ID</th> <th>IP Address</th> <th>MAC</th> </tr> </thead> <tbody> <tr> <td>CARRIE-0C7CB251</td> <td>192.168.1.10</td> <td>E0-CB-4E-DA-48-79</td> </tr> </tbody> </table>	Host ID	IP Address	MAC	CARRIE-0C7CB251	192.168.1.10	E0-CB-4E-DA-48-79
Host ID	IP Address	MAC					
CARRIE-0C7CB251	192.168.1.10	E0-CB-4E-DA-48-79					
USB	Connected : 0, <input type="radio"/> USB 1 0, <input type="radio"/> 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。

## 1.7.4 圖形介面地圖(GUI Map)



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


<b>儀表板</b> <b>Wizards</b>	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	<b>憑證管理</b>	本地憑證 具公信力之 CA 憑證 憑證備份
<b>線上狀態</b>	實體連線 虛擬 WAN	<b>VPN 中央管理</b>	基本設定 CPE 管理 VPN 管理 紀錄與警示
<b>WAN</b>	基本設定 網際網路連線 多重 VLAN WAN 額度	<b>AP 中央管理</b>	狀態 無線區域網路設定 AP 維護 流量圖表 非法 AP 偵測 負載平衡 功能支援清單
<b>LAN</b>	基本設定 固定路由	<b>無線網路(2.4GHz)</b>	

## 1.7.5 網頁操作台(Web Console)



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 **Web Console** 圖示即可開啓如下視窗。



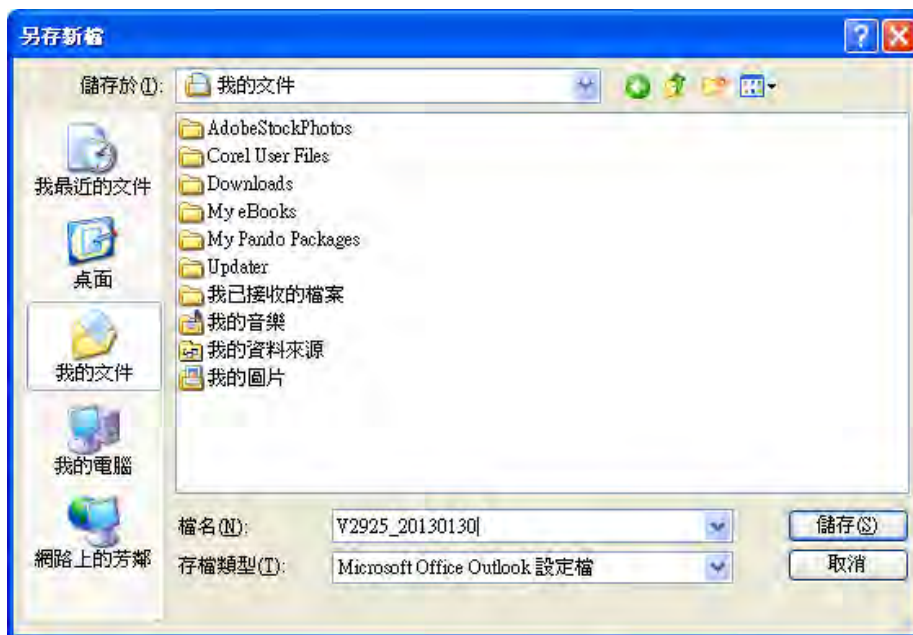
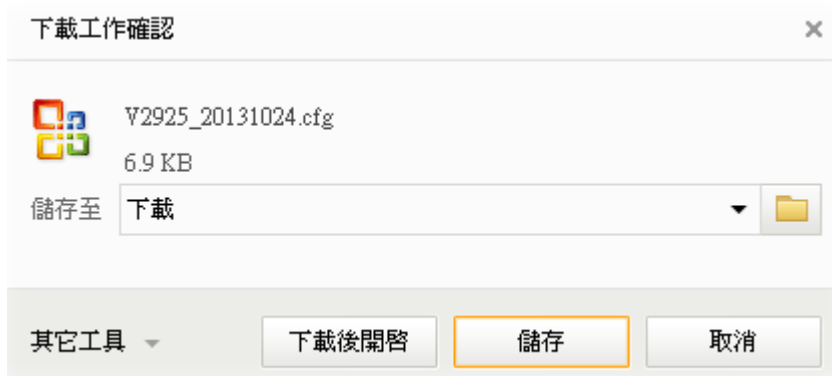
```
192.168.1.1/doc/console.htm  极速
Type ? for command help
> ?
% Valid commands are:
bpa          csm          ddns         dos          exit         internet
ip           ip6          ipf          log          mngt        msubnet
object       port         portmuptime ppa          prn          qos
quit         show         srv          switch       sys          testmail
upnp        vigbrg      vlan         vpn          wan          wptl
wol         user         nand
> █
```

## 1.7.6 設定備份(Config Backup)



快速儲存目前使用中的設定可以透過設定備份(**Config Backup**)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>>設定備份**來還原。

請按主頁面上方的 **Config Backup** 圖示即可開啓如下視窗。



按下**儲存**將設定儲存起來。

## 1.7.7 登出



登出按鈕即可離開此使用者設定介面。

## 1.8 連線狀態

服務啟用精選  
**連線狀態**  
 實體連線  
 虛擬 WAN

### 1.8.1 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

##### 連線狀態

實體連線		系統上線時間: 0天 0:10:24				
IPv4		IPv6				
<b>LAN 狀態</b>		主要 DNS: 8.8.8.8		次要 DNS: 8.8.4.4		
IP 位址	傳送封包	接收封包				
192.168.1.1	1526	996				
<b>WAN 1 狀態</b>						
啟用	線路	名稱	模式	上線時間		
是	乙太網路		---	00:00:00		
IP	開道 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	
<b>WAN 2 狀態</b>						
啟用	線路	名稱	模式	上線時間		
是	乙太網路		---	00:00:00		
IP	開道 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	
<b>WAN 3 狀態</b>						
啟用	線路	名稱	模式	上線時間	信號	
是	USB		---	00:00:00	-	
IP	開道 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	
<b>WAN 4 狀態</b>						
啟用	線路	名稱	模式	上線時間	信號	
是	USB		---	00:00:00	-	
IP	開道 IP	傳送封包	傳送速率(Bps)	接收封包	接收速率(Bps)	
---	---	0	0	0	0	

## IPv6 協定的實體連線

### 線上狀態

#### 實體連線

系統上線: 0日 0:11:0

IPv4		IPv6	
<b>LAN 狀態</b>			
IP 位址 FE80::21D:A AFF:FEBA:728/64 (Link)			
傳送封包	接收封包	傳送位元	接收位元
7	0	746	0
<b>WAN1 IPv6 狀態</b>			
啟用	模式	上線時間	
否	Offline	---	
IP			開道 IP
---			---
<b>WAN2 IPv6 狀態</b>			
啟用	模式	上線時間	
否	Offline	---	
IP			開道 IP
---			---
<b>WAN3 IPv6 狀態</b>			
啟用	模式	上線時間	
否	Offline	---	
IP			開道 IP
---			---

詳細說明於後(IPv4):

項目	說明
<b>LAN 狀態</b>	<p><b>主要 DNS</b>- DNS.顯示主要 DNS 的 IP 位址。</p> <p><b>次要 DNS</b>- 顯示次要 DNS 的 IP 位址。</p> <p><b>IP 位址</b>- 顯示 LAN 介面的 IP 位址。</p> <p><b>傳送封包</b> - 顯示在區域網路全部的傳送封包量。</p> <p><b>接收封包</b>- 顯示區域路網路中全部的接收封包量。</p>
<b>WAN 1 狀態 ~ WAN 4 狀態</b>	<p><b>啟用</b> - 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。</p> <p><b>線路</b>- 顯示此介面的實體連線類型。</p> <p><b>名稱</b>- 顯示 WAN1~WAN3 網頁上所顯示的名稱。</p> <p><b>模式</b>- 顯示 WAN 連線的模式類型(例如 PPPoE)。</p> <p><b>上線時間</b> - 顯示介面上全部的上傳時間。</p> <p><b>IP</b> - 顯示 WAN 介面的 IP 位址。</p> <p><b>開道 IP</b> - 顯示預設開道的 IP 位址。</p> <p><b>傳送位元</b> - 顯示 WAN 介面上全部傳送的封包數。</p> <p><b>傳送速率</b> - 顯示 WAN 介面上全部傳送速率位元數。</p> <p><b>接收位元</b> - 顯示 WAN 介面上全部接收的封包數。</p> <p><b>接收速率</b> - 顯示 WAN 介面上全部接收速率位元數。</p>

詳細說明於後(IPv6):

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

**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。



## 1.8.2 虛擬 WAN

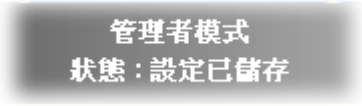
本頁顯示虛擬 WAN 介面的資訊，虛擬 WAN 用於 TR-069 管理、VoIP 服務等方面，應用一欄可顯示此 WAN 連線的目的地。

### 連線狀態

虛擬 WAN						系統上線時間: 1:28:55
<b>WAN 5 狀態</b>						
啟用	線路	名稱	模式	上線時間	應用	
是	乙太網路		---	00:00:00	管理	
IP	兩道 IP	傳送封包	傳送速率(Bps)	接收封包	接收速率(Bps)	
---	---	0	0	0	0	
<b>WAN 6 狀態</b>						
啟用	線路	名稱	模式	上線時間	應用	
是	乙太網路		---	00:00:00	管理	
IP	兩道 IP	傳送封包	傳送速率(Bps)	接收封包	接收速率(Bps)	
---	---	0	0	0	0	
<b>WAN 7 狀態</b>						
啟用	線路	名稱	模式	上線時間	應用	
是	乙太網路		---	00:00:00	管理	
IP	兩道 IP	傳送封包	傳送速率(Bps)	接收封包	接收速率(Bps)	
---	---	0	0	0	0	

## 1.9 儲存設定

每當您按下網頁上的確定按鈕以儲存檔案，您都可以見到如下的訊息，此為系統提供的狀態通知。



管理者模式  
狀態：設定已儲存

預備表示系統處於預備狀態隨時可以輸入設定。

設定已儲存表示您按了完成或是確定按鈕之後，系統已儲存該設定。

本頁留白

# 2

## 快速設定

設定精靈提供數種不同的簡易方式讓您能快速進行路由器設定。

按我欲  
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  
連線狀態

- **快速設定精靈(Quick Start Wizard)** – 用於建立網路連線以及網際網路存取等。
- **服務啟動精靈(Service Activation Wizard)** – 用於啟動網頁內容過濾器服務。
- **VPN 用戶端設定精靈(VPN Client Wizard)** – 用於建立 VPN 用戶端的 VPN 通道。
- **VPN 伺服器設定精靈(VPN Server Wizard)** – 用於建立 VPN 伺服器端的 VPN 通道。
- **無線設定精靈(Wireless Wizard)** – 用於建立無線網路連線。
- **VoIP 設定精靈(VoIP Wizard)** – 用於建立 VoIP 設定檔。

## 2.1 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，請按下一步。

### 快速設定精靈

#### 輸入登入密碼

請重新輸入字母及數字組合之字串作為您的 **密碼** (最多23個字元)

舊密碼	<input type="password"/>
新密碼	<input type="password"/>
確認密碼	<input type="password"/>

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/WAN2(以硬體連線為基準)，若使用的是 3G/4G USB 數據機，請選擇 WAN3/WAN4。並選擇自動偵測作為路由器的傳送資料模式，然後按下一步。

### 快速設定精靈

#### WAN 介面

WAN 介面:	<input type="text" value="WAN1"/>
顯示名稱:	<input type="text"/>
實體連線模式:	乙太網路
傳送資料模式:	<input type="text" value="自動偵測"/>

WAN1/WAN2 與 WAN3/WAN4 帶來的設定頁面所不同，請參考下述細部說明。

## 2.1.1 對於 WAN1/WAN2 介面(乙太網路)

WAN1/WAN2 專用於乙太網路的實體連線模式，如果您選擇 WAN1/WAN2，請先指定傳送資料模式，然後按下一步。

### 快速設定精靈

#### WAN 介面

WAN 介面:	WAN1 ▾
顯示名稱:	<input type="text"/>
實體連線模式:	乙太網路
傳送資料模式:	自動偵測 ▾

< 上一步   下一步 >   完成   取消

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，然後按下一步繼續進行。

### 2.1.1.1 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/WAN2 作為 WAN 介面，按下一步按鈕後，下圖將會出現讓您指定網際網路連線類型。

### 快速設定精靈

#### 連線至網際網路

**WAN 1**  
從下列網際網路連線方式類型中，選擇您的網路供應商所提供的服務類型，如果您不確定應該選擇何種類型，請聯繫您的網路服務供應商以取得詳細資料。

- PPPoE
- PPTP
- L2TP
- 固定 IP
- DHCP

< 上一步   下一步 >   完成   取消

2. 選擇 **PPPoE** 然後按下一步開啓如下頁面。

**快速設定精靈**

**PPPoE 用戶端模式**

**WAN 1**  
請輸入您的網路服務供應商所提供的使用者名稱及密碼。

使用者名稱	<input type="text" value="77484727@hinet.net"/>
密碼	<input type="password" value="••••••"/>
確認密碼	<input type="password" value="••••••"/>

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。
上一步	按此鈕回到上一頁面。
下一步	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。

#### 快速設定精靈

##### 請確認您的設定：

WAN 介面：	WAN1
實體連線模式：	乙太網路
傳送資料模式：	自動偵測
網際網路連線：	PPPoE

按 **上一步** 修正內容，否則請按 **完成** 儲存目前設定並重新啟動路由器

< 上一步

下一步 >

完成

取消

4. 按完成，快速設定精靈安裝完畢頁面將會出現。

#### 快速設定精靈設定完成!

5. 現在您可以遨遊網際網路了。

### 2.1.1.2 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。一旦 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 PPTP 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/WAN2** 作為 WAN 介面，按**下一步**按鈕後，下圖將會出現讓您指定網際網路連線類型。

#### 快速設定精靈

##### 連線至網際網路

**WAN 1**  
從下列網際網路連線方式類型中，選擇您的網路供應商所提供的服務類型，如果您不確定應該選擇何種類型，請聯繫您的網路服務供應商以取得詳細資料。

PPPoE  
 PPTP  
 L2TP  
 固定 IP  
 DHCP

< 上一步    下一步 >    完成    取消

2. 選擇 **PPTP/L2TP** 然後按**下一步**開啓如下頁面。

#### 快速設定精靈

##### PPTP 用戶端模式

**WAN 1**  
請輸入您的網路服務供應商所提供的使用者名稱、密碼、WAN IP 組態設定及 PPTP 網路服務供應商所提供的伺服器 IP。

使用者名稱

密碼

確認密碼

**WAN IP 組態設定**

自動取得 IP 位址  
 指定 IP 位址

IP 位址

子網路遮罩

關道

主要 DNS

次要 DNS

PPTP 伺服器

< 上一步    下一步 >    完成    取消



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 組態設定	<p>自動取得 IP 位址- 路由器可自 DHCP 伺服器自動取得 IP 位址。</p> <p>指定 IP 位址 - 使用者須手動輸入相關設定。</p> <p>IP 位址 - 輸入 IP 位址。</p> <p>子網路遮罩 - 輸入子網路遮罩。</p> <p>閘道 - 輸入閘道 IP 位址。</p> <p>主要 DNS - 輸入路由器主要的 DNS IP 位址。</p> <p>次要 DNS - 必要時輸入路由器次要的 DNS IP 位址。</p>
PPTP 伺服器 / L2TP 伺服器	輸入伺服器的 IP 位址。
上一步	按此鈕回到上一頁面。
下一步	按此鈕進入下一頁面。
取消	按此鈕放棄快速設定精靈。

- 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。

#### 快速設定精靈

請確認您的設定：

WAN 介面:	WAN1
實體連線模式:	乙太網路
傳送資料模式:	自動偵測
網際網路連線:	PPTP
按 <b>上一步</b> 修正內容，否則請按 <b>完成</b> 儲存目前設定並重新啟動路由器	

< 上一步

下一步 >

完成

取消

- 按完成，快速設定精靈安裝完畢頁面將會出現。

**快速設定精靈設定完成!**

5. 現在您可以遨遊網際網路了。

### 2.1.1.3 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/WAN2** 作為 WAN 介面，按**下一步**按鈕後，下圖將會出現讓您指定網際網路連線類型。

#### 快速設定精靈

##### 連線至網際網路

**WAN 1**  
從下列網際網路連線方式類型中，選擇您的網路供應商所提供的服務類型，如果您不確定應該選擇何種類型，請聯繫您的網路服務供應商以取得詳細資料。

PPPoE  
 PPTP  
 L2TP  
 固定 IP  
 DHCP

<上一步    下一步>    完成    取消

2. 選擇**固定 IP** 然後按**下一步**開啓如下頁面。

#### 快速設定精靈

##### 固定 IP 用戶端模式

**WAN 1**  
請輸入您的網路服務供應商所提供的固定 IP 組態設定。

WAN IP	<input type="text" value="192.16.3.138"/>
子網路遮罩	<input type="text" value="255.255.255.0"/>
閘道	<input type="text" value="172.16.3.1"/>
主要 DNS	<input type="text" value="8.8.8.8"/>
次要 DNS	<input type="text" value="8.8.4.4"/> (視需要填入)

<上一步    下一步>    完成    取消

可用設定說明如下：

項目	說明
WAN IP	輸入 IP 位址。
子網路遮罩	輸入子網路遮罩。

閘道	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。
上一步	按此鈕回到上一頁面。
下一步	按此鈕進入下一頁面。
取消	按此鈕放棄快速設定精靈。

- 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。

#### 快速設定精靈

##### 請確認您的設定：

WAN 介面：	WAN1
實體連線模式：	乙太網路
傳送資料模式：	自動偵測
網際網路連線：	Static IP

按 **上一步** 修正內容，否則請按 **完成** 儲存目前設定並重新啟動路由器

- 按**完成**，**快速設定精靈安裝完畢**頁面將會出現。

#### 快速設定精靈設定完成!

- 現在您可以遨遊網際網路了。

## 2.1.1.4 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**下一步**按鈕後，下圖將會出現讓您指定網際網路連線類型。

### 快速設定精靈

#### 連線至網際網路

**WAN 1**  
從下列網際網路連線方式類型中，選擇您的網路供應商所提供的服務類型，如果您不確定應該選擇何種類型，請聯繫您的網路服務供應商以取得詳細資料。

PPPoE  
 PPTP  
 L2TP  
 固定 IP  
 DHCP

< 上一步    下一步 >    完成    取消

2. 選擇 **DHCP** 並按**下一步**按鈕。

### 快速設定精靈

#### DHCP 用戶端模式

**WAN 1**  
如果您的網路服務供應商要求您輸入特定的主機名稱或特定的 MAC 位址，請在此輸入。

主機名稱  (視需要填入)  
MAC  -  -  -  -  -  (視需要填入)

< 上一步    下一步 >    完成    取消

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。
上一步	按此鈕回到上一頁面。
下一步	按此鈕進入下一頁面。
取消	按此鈕放棄快速設定精靈。

- 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。

#### 快速設定精靈

##### 請確認您的設定：

WAN 介面：	WAN1
實體連線模式：	乙太網路
傳送資料模式：	自動偵測
網際網路連線：	DHCP

按 **上一步** 修正內容，否則請按 **完成** 儲存目前設定並重新啟動路由器

- 按完成，快速設定精靈安裝完畢頁面將會出現。

#### 快速設定精靈設定完成!

- 現在您可以遨遊網際網路了。

## 2.1.2 對於 WAN3/WAN4 介面 (USB)

如果要使用 3G /4G USB 數據機進行網路連線，請選擇 WAN3/WAN4。

- 選擇 WAN3/WAN4 作為 WAN 介面。

#### 快速設定精靈

##### WAN 介面

WAN 介面：	WAN3 ▾
顯示名稱：	<input type="text"/>
實體連線模式：	USB

2. 按下一步，系統將會出現讓您指定網際網路連線類型。

快速設定精靈

連接至網際網路

<b>WAN 3</b>	
網際網路連線模式：	3G/4G USB 數據機(PPP模式) <input type="button" value="v"/>
<b>3G/4G USB 數據機(PPP模式)</b>	
SIM PIN 碼	<input type="text"/>
數據機初始字串	<input type="text" value="AT&amp;FE0V1X1&amp;D2&amp;C1S0=0"/> (Default: AT&FE0V1X1&D2&C1S0=0)
APN 名稱	<input type="text"/> <input type="button" value="套用"/>

可用設定說明如下：

項目	說明
網際網路連線模式	選擇存取網際網路的連線模式。
<b>3G/4G USB 數據機 (PPP 模式)</b>	<p><b>SIM PIN 碼</b> – 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。</p> <p><b>數據機初始字串</b> – 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。</p> <p><b>APN 名稱</b> – 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<b>套用</b>按鈕。</p>
<b>3G/4G USB 數據機 (DHCP 模式)</b>	<p><b>SIM PIN 碼</b> – 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。</p> <p><b>網路模式</b> – 選擇適用的連線模式。</p> <p><b>APN 名稱</b> – 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。</p>

- 按下一步檢視此連線的設定狀態。

#### 快速設定精靈

##### 請確認您的設定：

WAN 介面：	WAN3
實體連線模式：	USB
網際網路連線：	PPP

按 **上一步** 修正內容，否則請按 **完成** 儲存目前設定並重新啟動路由器

<上一步

下一步 >

完成

取消

- 按完成，快速設定精靈安裝完畢頁面將會出現。

#### 快速設定精靈設定完成!

- 現在您可以遨遊網際網路了。

## 2.2 服務啟動精靈

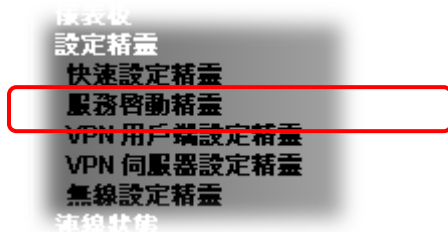
服務啟用精靈可利用快速及簡便方式，幫助您啟用網頁內容過濾器服務機制(WCF)。

**注意:** 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。

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。

1. 開啟服務啟動精靈。



2. 服務啟用精靈畫面顯示如下，請選擇其中一個項目(例如本例使用**免費試用版**)，按下一步。

### 服務啟動精靈

#### 選擇您想要啟動的服務類型

此精靈用來啟動  
- 網頁內容過濾器  
請選擇所需的版本

免費試用版

下一步 >

完成

取消

**注意：**免費試用版提供短期試用期限讓您熟悉 WCF 功能。



3. 在下列頁面中，您可以同時或是分別啓動不同的 WCF 過濾服務，完成選擇後，請按下一步。

**服務啓動精靈**

**選擇您想要啓動的服務類型**

This product provides 30 days of free trial, please choose the item(s) you want to use.

WCF service:

Web Content Filter (BPjM)  
BPjM is the web content filter based on service operated in Germany. We recommend only users live in Germany to try the BPjM WCF service. This is a free service without guarantee.  
啓動日期: 2013-06-19

Web Content Filter (Commtouch) [License Agreement](#)  
Commtouch is the web content filter based on Commtouch operated in the worldwide. There is a 30-day trial period. After trial, you can purchase DrayTek's prepared Commtouch GlobalView WCF package from retailing outlets.  
啓動日期: 2013-06-19

Web Content Filter (fragFINN) [License Agreement](#) 啓動日期: 2013-06-19

我已閱讀並接受上述同意聲明(請勾選)。

附註: 啓用日期由伺服器自動帶出，且無法變更。

< 上一步    **下一步 >**    完成    取消

Commtouch 為一個能在全球運作的網頁內容過濾器，系統提供您 30 天的試用期，試用完畢後，您可以洽詢經銷商購買一套 Commtouch GlobalView WCF 授權書。

適用德國地區的用戶，fragfINN 對德語用戶屬於白名單，對於家中有青少年的家庭來說 BPjM 可以提供更為安全的網際網路連線。

自 2015 年元月起，fragFINN 服務已不再支援。

4. 設定確認頁面顯示如下所述，按下一步。

**服務啓動精靈**

**請確定您的設定**

服務類型: 試用版  
服務已啓動: Web Content Filter ( Commtouch )

請按 [上一頁](#) 以重新選擇想要啓動的服務

< 上一頁    **下一頁 >**    完成    取消

5. 請等候直到以下頁面出現。

**服務啟動精靈**

**連線成功!**

請勾選下列項目，以啟動路由器提供的服務。

啟動網頁內容過濾器

下一步 >

完成

當此頁面出現時，您可啟用或是關閉服務，視您實際情況需要而定，然後按下**完成**。

**注意：**此服務可以啟用並當成**防火牆>>基本設定**的預設規則。

6. 現在，網頁上將依照您的設定顯示出啟用服務的細節內容，試用版的有效時間通常為 30 天。

**服務啟動精靈**

**伺服器已啟動!**

**DrayTek 服務啟用表**

服務名稱	起始日期	到期日期	狀態
網頁內容過濾器	2013-06-19	2013-07-20	Commtouch

請確認授權碼是否與特徵碼之服務供應商相符合，為了確保路由器能正常操作，建議您再次更新特徵碼。

版權所有 2009, 居易科技股份有限公司

## 2.3 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. 開啓 **VPN 與遠端存取>VPN 用戶端設定精靈**，設定頁面如下所示：

### VPN 用戶端設定精靈

#### 選擇 VPN 建立環境

LAN-to-LAN VPN用戶模式選項:  ▾

請選擇一組 LAN-to-LAN 設定檔:

**附註:** 針對典型LAN-to-LAN通道，請使用路由模式。  
如果遠端網路僅供單一用戶或是IP使用，且未定為子網路由，請選擇NAT模式。  
若您不確定設定的內容，請選擇路由模式。

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。 <input type="button" value="路由模式"/> ▾ 路由模式 NAT模式
請選擇 LAN-to-LAN 設定檔	共有 32 個 VPN 設定檔可以供使用者選擇來設定。

[編號]	[狀態]	[名稱]
1	x	???
2	x	???
3	x	???
4	x	???
5	x	???
6	x	???
7	x	???
8	x	???
9	x	???
10	x	???
11	x	???
12	x	???
13	x	???
14	x	???
15	x	???
16	x	???
17	x	???
18	x	???
19	x	???
20	x	???
21	x	???
22	x	???
23	x	???

2. 選擇好模式與設定檔選項之後，請按下一頁開啓下一個頁面。

VPN 及遠端存取 >> VPN 用戶端設定精靈

#### VPN 連線設定

<b>安全等級 (1 最高; 5 最低)</b> 1. L2TP over IPsec 2. IPsec 3. PPTP (加密) 4. L2TP 5. PPTP (未加密)	<b>總吞吐量等級 (1 最高; 5 最低)</b> 1. PPTP (未加密) 2. L2TP 3. IPsec 4. L2TP over IPsec 5. PPTP (加密)
--	--

選擇 VPN 類型:

- PPTP (未加密)
- PPTP (加密)**
- IPsec
- L2TP
- L2TP over IPsec (建議選項)
- L2TP over IPsec (必須)

< 上一頁    下一頁 >    完成    取消

在本頁中，您必須針對 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：

**注意：**以下提供的 VPN 類型說明以路由模式為基準。

- 當您選擇 **PPTP (None Encryption)** 或 **PPTP (Encryption)**時，您會看到如下頁面：

VPN 及遠端存取 >> VPN 用戶端設定精靈

VPN 用戶端 PPTP 加密設定

設定檔名稱	???
VPN 撥出經由介面	WAN1 優先
<input type="checkbox"/> 永遠連線	
伺服器 IP位址/VPN的主機名稱 (例如, draytek.com 或 123.45.67.89)	draytek.com
使用者名稱	marketing
密碼	*****
遠端網路 IP	192.168.1.6
遠端網路遮罩	255.255.255.0

< 上一頁    下一頁 >    完成    取消

- 當您選擇 **IPSec** 您看到的頁面如下：

VPN 及遠端存取 >> VPN 用戶端設定精靈

VPN 用戶端 IPsec 設定

設定檔名稱	???
VPN 撥出經由介面	WAN1 優先
<input type="checkbox"/> 永遠連線	
伺服器 IP位址/VPN的主機名稱 (例如, draytek.com 或 123.45.67.89)	
IKE 驗證模式	
<input checked="" type="radio"/> 預先共用金鑰	
確認預先共用金鑰	
<input type="radio"/> 數位簽章(X.509)	
對方 ID	無
本機 ID	
<input type="radio"/> 替代主體名稱優先	
<input type="radio"/> 主體名稱優先	
本地憑證	無
IPsec 安全防護方式	
<input checked="" type="radio"/> 中 (AH)	
<input type="radio"/> 高 (ESP)	DES 無驗證
遠端網路 IP	0.0.0.0
遠端網路遮罩	255.255.255.0

< 上一頁    下一頁 >    完成    取消

- 當您選擇 **L2TP** 您看到的頁面如下：

VPN 及遠端存取 >> VPN 用戶端設定精靈

#### VPN 用戶端 L2TP 設定

設定檔名稱	???
VPN 撥出經由介面	WAN1 優先
<input type="checkbox"/> 永遠連線	
伺服器 IP位址/VPN的主機名稱 (例如: draytek.com 或 123.45.67.89)	
使用者名稱	???
密碼	
遠端網路 IP	0.0.0.0
遠端網路遮罩	255.255.255.0

< 上一頁    下一頁 >    完成    取消

- 當您選擇 **L2TP over IPsec (Nice to Have)** 或是 **L2TP over IPsec (Must)**，您看到的頁面如下：

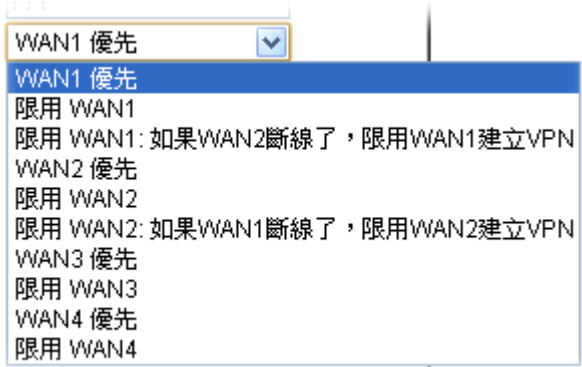
VPN 及遠端存取 >> VPN 用戶端設定精靈

#### VPN 用戶端 L2TP over IPsec (建議選項) 設定

設定檔名稱	???
VPN 撥出經由介面	WAN1 優先
<input type="checkbox"/> 永遠連線	
伺服器 IP位址/VPN的主機名稱 (例如: draytek.com 或 123.45.67.89)	
IKE 驗證模式	
<input checked="" type="radio"/> 預先共用金鑰	
確認預先共用金鑰	
<input type="radio"/> 數位簽章(X.509)	
對方 ID	無
本機 ID	
<input type="radio"/> 替代主體名稱優先	
<input type="radio"/> 主體名稱優先	
本地憑證	無
IPsec 安全防護方式	
<input checked="" type="radio"/> 中 (AH)	
<input type="radio"/> 高 (ESP)	DES 無驗證
使用者名稱	???
密碼	
遠端網路 IP	0.0.0.0
遠端網路遮罩	255.255.255.0

< 上一頁    下一頁 >    完成    取消

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。
VPN 連線經由介面	<p>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。</p>  <p><b>WAN1 優先/ WAN2 優先/ WAN3 優先</b>- 連線時，路由器會將 WAN1 視為 VPN 連線的首要選擇，如果 WAN1/WAN2/WAN3 連線失敗，路由器將使用其他 WAN 介面來取代。</p> <p><b>限用 WAN1/限用 WAN2/限用 WAN3</b> - 連線時，路由器會將 WAN1/WAN2/WAN3 視為 VPN 連線的唯一選擇。</p> <p><b>限用 WAN1:如果 WAN2 斷線了</b> – 當 WAN2 斷線時，此 VPN 通道會經由 WAN1 連線撥打出去，亦即 WAN1 為 WAN2 的備援介面。</p> <p><b>限用 WAN2: 如果 WAN1 斷線了</b>-當 WAN1 斷線時，此 VPN 通道會經由 WAN2 連線撥打出去，亦即 WAN2 為 WAN1 的備援介面。</p>
永遠連線	勾選此方塊讓路由器永遠保持 VPN 連線。
伺服器 IP/ VPN 的主機名稱	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	<p><b>預先共用金鑰</b>- 勾選此方塊啓用此功能並按 <b>IKE 預先共用金鑰</b> 按鈕輸入金鑰及確認金鑰。</p> <p><b>數位簽章 (X.509)</b> –勾選此方塊啓用此功能並選擇一組事先定義的簽章內容 (在 <b>VPN 和遠端存取&gt;&gt;IPSec 端點辨識</b> 中設定)。</p>
數位簽章 (X.509)	<p>點選<b>數位簽章</b>啓用此功能。</p> <p><b>對方 ID</b> –自下拉式清單中選擇對方的 ID。</p> <p><b>本機 ID</b> – 選擇替代主體名稱優先或是主體名稱優先。</p> <p><b>本地憑證</b> –自下拉式清單中選擇一種憑證，您必須事先在<b>憑證管理&gt;&gt;本機憑證</b>中設定至少一組的憑證，否則無憑證可以使用。</p>
IPSec 安全防護方	對 IPSec 通道和 L2TP 含 IPSec 原則來說，本區為必要設

式	<p>定。</p> <p><b>中級 (AH)</b> 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。</p> <p><b>高級 (ESP-Encapsulating Security Payload)</b> 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：</p> <p><b>DES 無驗證</b> - 使用 DES 加密演算式，但不採用任何驗證計畫。</p> <p><b>DES 有驗證</b> - 使用 DES 加密演算式，且採用 MD5 或 SHA-1 驗證計畫。</p> <p><b>3DES 無驗證</b> - 使用三重 DES 加密演算式，但不採用任何驗證計畫。</p> <p><b>3DES 有驗證</b> - 使用三重 DES 加密演算式，且採用 MD5 或 SHA-1 驗證計畫。</p> <p><b>AES 無驗證</b> - 使用 AES 加密演算式，但不採用任何驗證計畫。</p> <p><b>AES 有驗證</b> - 使用 AES 加密演算式，且採用 MD5 或 SHA-1 驗證計畫。</p>
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。

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。

**VPN 及遠端存取 >> VPN 用戶端設定精靈**

**請確認您的設定**

LAN-to-LAN 編號:	2
設定檔名稱:	VPN-2
VPN 連線類型:	L2TP over IPSec (建議選項)
VPN 撥出經由介面:	WAN1 優先
永遠連線:	否
伺服器 IP/主機名稱:	draytek.com
IKE 驗證方法:	預先共用金鑰
IPsec 安全防護方式:	AH-SHA1
遠端網路 IP:	192.168.1.211
遠端網路遮罩:	255.255.255.0

按 **上一頁** 修正內容，否則請按 **完成** 以儲存目前設定並進行下一個動作：

- 進入 VPN 連線管理
- 進行另一個 VPN 用戶端設定精靈
- 檢視細節設定



可用設定說明如下：

項目	說明
進入 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。
執行另一個 VPN 伺服器精靈設定	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。
檢視設定詳細內容	按此鈕進入 VPN 及遠端存取>> LAN to LAN 以檢視細節內容。

## 2.4 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)。

1. 開啓 VPN 與遠端存取>VPN 伺服器設定精靈，設定頁面如下所示：

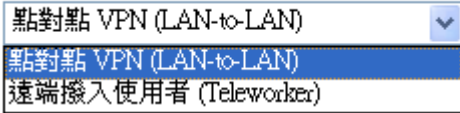
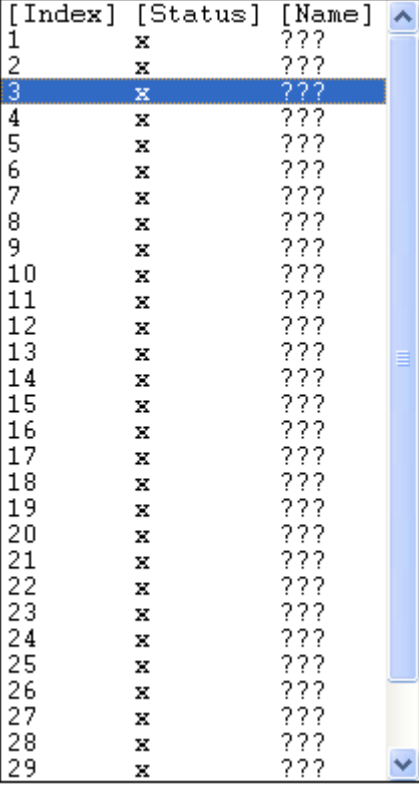
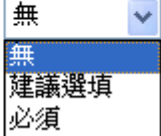
### VPN 及遠端存取 >> VPN 伺服器設定精靈

#### 選擇 VPN 建立環境

VPN 伺服器模式選項:	<input type="text" value="點對點 VPN (LAN-to-LAN)"/>
請選擇一組 LAN-to-LAN 設定檔:	<input type="text" value="2 x ???"/>
請選擇一個撥入使用者帳號:	<input type="text" value="[Index] [Status] [Name]"/>
允許撥入類型:	<input type="checkbox"/> PPTP <input type="checkbox"/> IPsec <input type="checkbox"/> 具有 IPsec 原則的 L2TP <input type="text" value="無"/>

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。 <b>點對點 VPN</b> – 想要自動設定 LAN-to-LAN 設定檔，請選擇 <b>點對點 VPN</b> 。 <b>/遠端撥入使用者</b> – 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。

	 <p>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。</p>																																																																																										
<p>請選擇 LAN-to-LAN 設定檔</p>	<p>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 32 個 VPN 設定檔可以供使用者選擇並設定。</p>  <table border="1" data-bbox="683 577 1104 1361"> <thead> <tr> <th>[Index]</th> <th>[Status]</th> <th>[Name]</th> </tr> </thead> <tbody> <tr><td>1</td><td>x</td><td>???</td></tr> <tr><td>2</td><td>x</td><td>???</td></tr> <tr><td>3</td><td>x</td><td>???</td></tr> <tr><td>4</td><td>x</td><td>???</td></tr> <tr><td>5</td><td>x</td><td>???</td></tr> <tr><td>6</td><td>x</td><td>???</td></tr> <tr><td>7</td><td>x</td><td>???</td></tr> <tr><td>8</td><td>x</td><td>???</td></tr> <tr><td>9</td><td>x</td><td>???</td></tr> <tr><td>10</td><td>x</td><td>???</td></tr> <tr><td>11</td><td>x</td><td>???</td></tr> <tr><td>12</td><td>x</td><td>???</td></tr> <tr><td>13</td><td>x</td><td>???</td></tr> <tr><td>14</td><td>x</td><td>???</td></tr> <tr><td>15</td><td>x</td><td>???</td></tr> <tr><td>16</td><td>x</td><td>???</td></tr> <tr><td>17</td><td>x</td><td>???</td></tr> <tr><td>18</td><td>x</td><td>???</td></tr> <tr><td>19</td><td>x</td><td>???</td></tr> <tr><td>20</td><td>x</td><td>???</td></tr> <tr><td>21</td><td>x</td><td>???</td></tr> <tr><td>22</td><td>x</td><td>???</td></tr> <tr><td>23</td><td>x</td><td>???</td></tr> <tr><td>24</td><td>x</td><td>???</td></tr> <tr><td>25</td><td>x</td><td>???</td></tr> <tr><td>26</td><td>x</td><td>???</td></tr> <tr><td>27</td><td>x</td><td>???</td></tr> <tr><td>28</td><td>x</td><td>???</td></tr> <tr><td>29</td><td>x</td><td>???</td></tr> </tbody> </table>	[Index]	[Status]	[Name]	1	x	???	2	x	???	3	x	???	4	x	???	5	x	???	6	x	???	7	x	???	8	x	???	9	x	???	10	x	???	11	x	???	12	x	???	13	x	???	14	x	???	15	x	???	16	x	???	17	x	???	18	x	???	19	x	???	20	x	???	21	x	???	22	x	???	23	x	???	24	x	???	25	x	???	26	x	???	27	x	???	28	x	???	29	x	???
[Index]	[Status]	[Name]																																																																																									
1	x	???																																																																																									
2	x	???																																																																																									
3	x	???																																																																																									
4	x	???																																																																																									
5	x	???																																																																																									
6	x	???																																																																																									
7	x	???																																																																																									
8	x	???																																																																																									
9	x	???																																																																																									
10	x	???																																																																																									
11	x	???																																																																																									
12	x	???																																																																																									
13	x	???																																																																																									
14	x	???																																																																																									
15	x	???																																																																																									
16	x	???																																																																																									
17	x	???																																																																																									
18	x	???																																																																																									
19	x	???																																																																																									
20	x	???																																																																																									
21	x	???																																																																																									
22	x	???																																																																																									
23	x	???																																																																																									
24	x	???																																																																																									
25	x	???																																																																																									
26	x	???																																																																																									
27	x	???																																																																																									
28	x	???																																																																																									
29	x	???																																																																																									
<p>請選擇撥入使用者帳號</p>	<p>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 32 個不同的 VPN 通道供用戶設定使用。</p>																																																																																										
<p>允許的撥入類型</p>	<p>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）。</p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> PPTP</li> <li><input checked="" type="checkbox"/> IPsec</li> <li><input checked="" type="checkbox"/> 具有 IPsec 原則的 L2TP</li> </ul>  <p>不同的撥入類型所帶出的設定頁面也會有些許的差異。</p>																																																																																										

2. 在選擇完畢後，請按下一步，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點對點 VPN 作為 VPN 伺服器模式選項。
- 當您勾選了 PPTP 之後，您會看到如下頁面：

VPN及遠端存取 >> VPN 伺服器設定精靈

VPN 驗證設定

設定檔名稱	???
PPTP / L2TP / L2TP over IPsec 驗證	
使用者名稱	???
密碼	
對方 IP/VPN 用戶端 IP	
點對點資訊	
遠端網路 IP	0.0.0.0
遠端網路遮罩	255.255.255.0

< 上一頁    下一頁 >    完成    取消

- 當您選擇 PPTP, IPSec, L2TP 或 PPTP, IPSec 或 L2TP with Policy (建議選填/必須)，您看到的頁面如下：

VPN及遠端存取 >> VPN 伺服器設定精靈

VPN 驗證設定

設定檔名稱	???
PPTP / L2TP / L2TP over IPsec 驗證	
使用者名稱	???
密碼	
IPsec / L2TP over IPsec 驗證	
<input checked="" type="checkbox"/> 預先共用金鑰	
確認預先共用金鑰	
<input type="checkbox"/> 數位簽章 (X.509)	
對方 ID	無
本機 ID	
<input type="radio"/> 替代主體名稱優先	
<input type="radio"/> 主體名稱優先	
對方 IP/VPN 用戶端 IP	
對方 ID	
點對點資訊	
遠端網路 IP	0.0.0.0
遠端網路遮罩	255.255.255.0

< 上一頁    下一頁 >    完成    取消

- 當您選擇 IPsec，您看到的頁面如下：

VPN及遠端存取 >> VPN 伺服器設定精靈

VPN 驗證設定

設定檔名稱	???
IPsec / L2TP over IPsec 驗證	
<input checked="" type="checkbox"/> 預先共用金鑰	
確認預先共用金鑰	
<input type="checkbox"/> 數位簽章 (X.509)	
對方 ID	無
本機 ID	
<input checked="" type="radio"/> 替代主體名稱優先	
<input type="radio"/> 主體名稱優先	
對方 IP/VPN 用戶端 IP	
對方 ID	
點對點資訊	
遠端網路 IP	0.0.0.0
遠端網路遮罩	255.255.255.0

< 上一頁      下一頁 >      完成      取消

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。
預先共用金鑰	為了驗證 IPsec/L2TP IPsec，請輸入金鑰內容。
確認預先共用金鑰	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 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。
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。

3. 完成配置後，請按下一步，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。

## 請確認您的設定

VPN 環境:	點對點 VPN (LAN-to-LAN)
編號:	4
設定檔名稱:	VPN_Ser1
使用者名稱:	gary
允許服務:	IPsec+L2TP+L2TP with IPsec Policy
對方 IP/VPN 用戶端 IP:	192.168.1.48
對方 ID:	remote
遠端網路 IP:	192.168.1.89
遠端網路遮罩:	255.255.255.0

按 **上一頁** 修正內容，否則請按 **完成** 以儲存目前設定並進行下一個動作：

- 進入 VPN 連線管理
- 進行下一個 VPN 伺服器設定精靈
- 檢視細節設定

&lt; 上一頁

下一頁 &gt;

完成

取消

可用設定說明如下：

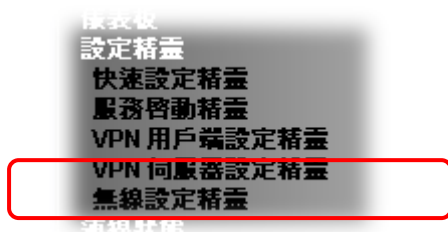
項目	說明
進入 VPN 連線管理	按此鈕進入 VPN 及遠端存取>>連線管理頁面檢視 VPN 連線狀態。
執行另一個 VPN 伺服器精靈設定	按此鈕以便利用 VPN 伺服器設定精靈設定另一個 VPN 伺服器設定檔。
檢視設定詳細內容	按此鈕進入 VPN 及遠端存取>> LAN to LAN 以檢視細節內容。

## 2.5 無線設定精靈

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. 開啓無線設定精靈。



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。因 n、n-plus 機種帶出的畫面會有些許差異，本範例以 n-plus 機種之相關畫面進行解說。

### 無線設定精靈

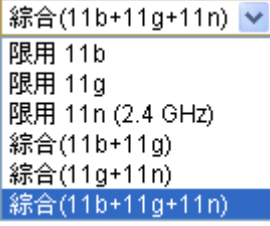
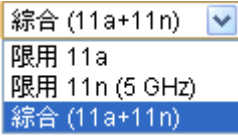
#### 主機 AP 設定

<b>無線網路 2.4GHz 設定</b>	
名稱:	DrayTek
模式:	綜合(11b+11g+11n) ▾
頻道:	頻道 6, 2437MHz ▾
安全性密鑰:	*****
<b>無線網路 5GHz 設定</b>	
<input type="checkbox"/> 使用與上述相同的 SSID與安全性密鑰	
名稱:	DrayTek_5G
模式:	綜合 (11a+11n) ▾
頻道:	頻道 36, 5180MHz ▾
安全性密鑰:	*****
<b>附註:</b> 此處設定的主機 AP 主要用於家庭或是公司內網。	

< 上一頁   下一頁 >   完成   取消

可用設定說明如下：

項目	說明
<b>無線 2.4GHz 設定</b>	
名稱	輸入無線 2.4GHz 的 SSID 名稱，預設值為 DrayTek，如有必要，請更換名稱。
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。

	
<b>頻道</b>	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。
<b>安全性密鑰</b>	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...”。
<b>無線 5GHz 設定</b>	
<b>使用上述相同的 SSID 與安全性密鑰</b>	勾選此框即可使用與上述相同的設定值。
<b>名稱</b>	輸入無線 5GHz 的 SSID 名稱，預設值為 DrayTek_5G，如有必要，請更換名稱。
<b>模式</b>	目前可用的模式如下所列。 
<b>頻道</b>	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。
<b>安全性密鑰</b>	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...”。
<b>下一頁</b>	按此進入下一個設定頁面。
<b>取消</b>	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，按下一步。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。

### 無線設定精靈

#### 客戶 AP 設定

**無線網路 2.4GHz 設定**

啟用  停用

SSID:

安全性密鑰:

流量控制:  啟用 上傳  kbps 下載  kbps

**無線網路 5GHz 設定**

啟用  停用

使用與上述相同的 SSID與安全性密鑰

SSID:

安全性密鑰:

流量控制:  啟用 上傳  kbps 下載  kbps

**附註:**設定完成的客戶 AP將無法登入區域網路，VPN 連線或與連接至路由器其他AP的無線裝置通訊，此 AP 介面僅適用網際網路連線。

可用設定說明如下：

項目	說明
<b>無線網路 2.4GHz 設定</b>	
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)。
安全性密鑰	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...”。
流量控制	控制透過無線連線的資料傳輸速度。 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。 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。
<b>無線網路 5GHz 設定</b>	
啟用/停用	啟用或是停用本頁的設定。
使用上述相同的 SSID 與安全性密鑰	勾選此框即可使用與上述相同的設定值。



<b>SSID</b>	輸入路由器的 SSID 名稱(SSID2)。
<b>安全性密鑰</b>	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...”。
<b>流量控制</b>	控制透過無線連線的資料傳輸速度。 <b>上傳</b> – 勾選啓用方塊之後，接著輸入資料上傳的速度，預設值為 30,000 kbps。 <b>下載</b> – 勾選啓用方塊之後，接著輸入資料下載的速度，預設值為 30,000 kbps。
<b>下一頁</b>	按此進入下一個設定頁面。
<b>取消</b>	按此離開設定精靈，任何設定變更將無法儲存。

- 輸入完上述資訊之後，按下一步。
- 接著螢幕會顯示無線設定的摘要內容。

#### 無線設定精靈

##### 設定摘要

無線網路 2.4GHz 設定	無線網路 5GHz 設定
模式:綜合(11b+11g+11n) 頻道:頻道 6, 2437MHz	模式:綜合(11a+11n) 頻道:頻道 36, 5180MHz
主機 AP SSID 名稱:DrayTek 安全性密鑰:*****	主機 AP SSID 名稱:DrayTek_5G 安全性密鑰:*****
客戶 AP 狀態:停用 SSID 名稱:DrayTek_Guest 安全性密鑰:***** 流量控制:停用	客戶 AP 狀態:停用 SSID 名稱:DrayTek_5G_Guest 安全性密鑰:***** 流量控制:停用

- 若無任何疑問，按下**完成**按鈕來結束設定。

#### 無線設定精靈

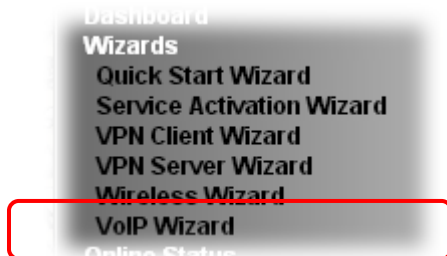
**無線設定精靈設定完成!**

## 2.6 VoIP 設定精靈

Vigor 路由器提供可以快速設定 VoIP 運用的設定精靈。

**附註：**此設定精靈僅適用“V”系列機型。

1. 開啓設定精靈>>VoIP 設定精靈。



2. **VoIP Wizard** 設定精靈出現如下：

**VoIP Wizard**

---

**Set VoIP service provider domain**

VoIP service provider	draytel.org	draytel.org	(63 char max).
SIP Port	5060		

**Set Account quickly**

Phone 1 (default mapping to Account 1)		
Account Number/Name	---	(63 char max).
Password		(63 char max).
Phone 2 (default mapping to Account 2)		
<input checked="" type="checkbox"/> use the same Account as phone1		
Account Number/Name	---	(63 char max).
Password		(63 char max).

可用設定說明如下：

項目	說明
<b>Set VoIP service provider domain</b>	<b>VoIP service provider</b> – 使用下拉式清單列出可以選擇的 VoIP 服務供應商選項。 <b>SIP Port</b> – 使用預設埠號設定 (5060)。
<b>Set Account quickly</b>	<b>Account Number/Name</b> – 輸入於 ISP 註冊的帳號與名稱。 <b>Password</b> – 輸入於 ISP 註冊的密碼。 <b>Use the same Account as phone 1</b> – 如果不需要設定 Phone 2 的內容，請勾選此方框。
<b>下一頁(Next)</b>	按此進入下一個設定頁面。

**取消(Cancel)**

按此取消設定並離開此設定精靈。

- 完成設定之後，按下一頁檢視連線的設定總結內容。

**VoIP Wizard**

**Please confirm your settings:**

VoIP Service Provider	draytel.org
SIP Port	5060
Phone 1 Account	5633s
Phone 2 Account	5633s

Click **Back** to modify changes if necessary. Otherwise, click **Finish** to save current settings.

< Back

Next >

Finish

Cancel

- 按完成。

**VoIP Wizard Setup OK!**

## 2.7 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**支援區域>>產品註冊**。

支援區域  
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**。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。



請花一點時間進行註冊。

會員登記，授權您為您所購買的產品升級韌體和接收即將推出的產品和服務的最新消息！

一旦您成為居易會員，歡迎您登入網站，告訴我們您對居易產品的看法，您的寶貴意見將成為本公司未來創新與強化產品的重要依據。



如果您在登入時遇到困難，請與我們的客服連絡。

客服專線： (03) 597-2727 或

寄送電子郵件至： [webmaster@draytek.com](mailto:webmaster@draytek.com)

4. 按下登入後，將會出現如下的畫面，請按下**新增(Add)**。

The screenshot shows the DrayTek MyVigor user interface. The top navigation bar includes the DrayTek logo, a 'Home' button, and a search field. The left sidebar contains a menu with items like 'About Us', 'Product', 'My Information', 'VigorACS SI', 'Vigor Series', 'Management', 'Product Registration', and 'Customer Survey'. The 'Product Registration' item is highlighted with a red box. The main content area is titled 'My Information' and displays user details for 'james\_fae', including last and current login times and IP addresses. Below this is a 'Your Device List' section with a table of registered devices. The 'Add' button is highlighted with a red box.

Serial Number / Host ID	Device Name	Model	Note
<a href="#">104001703857</a>	Vigor2710	Vigor2710	-
<a href="#">200807100001</a>	VigorPro5300	VigorPro5300	-
<a href="#">200911030001</a>	ryan	VigorPro5300	-

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

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

The screenshot shows the 'Registration Device' form in the DrayTek MyVigor interface. The form includes fields for 'Serial number', 'Nickname', 'Registration Date', 'Usage', 'Product Rating', 'No. of Employees', 'Supplier', and 'Date of Purchase'. The 'Nickname' field contains 'vigor2920' and the 'Registration Date' field contains '08-24-2011'. Both fields are highlighted with red boxes. Below these fields are radio button options for 'Internet Connection' types: Cable, ADSL, VDSL, Fiber, 3G, WIMAX, and LTE. The 'Submit' button is highlighted with a red box.

6. 下述頁面出現後，您的路由器資訊已經加入 MyVigor 的資料庫中。

Your device has been successfully added to the database.

OK

7. 現在您已經完成產品註冊。
8. 按下確定(OK)，回到 **My Information** 網頁。看看 **My Information** 網頁，新增的路由器將會列在 **Your Device List** 清單中。

The screenshot shows the MyVigor web interface. The top navigation bar includes the DrayTek logo and 'MyVigor' text. A search bar is present. The left sidebar contains navigation links: Home, About Us, Product, My Information, VigorACS SI, Vigor Series, Management, and Customer Survey. The main content area is titled 'My Information' and displays user details: 'Welcome, draytekfae', 'Last Login Time : 2011-08-24 09:39:13', 'Last Login From : 123.110.144.220', 'Current Login Time : 2011-08-24 23:01:15', and 'Current Login From : 114.37.142.184'. Below this is the 'Your Device List' section, which includes a table with columns: Serial Number / Host ID, Device Name, Model, and Note. The table contains five rows of device information. The last row, with Serial Number 2011082214320301 and Device Name Vigor2920, is highlighted with a red box.

Serial Number / Host ID	Device Name	Model	Note
20100707144801	Vigor3300V	Vigor3300	-
20100708105301	Vigor2820	Vigor2820	-
20101005104801	Vigor2710vn	Vigor2710	-
2010121707335201	Vigor2380	Vigor2830	-
2011082214320301	Vigor2920	Vigor2920	-

如果您尚未透過**服務啟動精靈**啟動網頁內容過濾服務，您可以利用此步驟來啟動相關服務，請按下序號連結。

9. 從下述開啓的頁面中，按下 **Trial** 按鈕。

The screenshot shows the 'My Product' page in the MyVigor interface. It displays 'Device Information' for a Vigor2850 router, including the nickname, serial number (2011031609200201), and model. Below this are buttons for 'Rename', 'Transfer', and 'Back'. The 'Device's Service' section is active, showing a table with columns: Service, Provider, Action, Status, Start Date, and Expired Date. The table has one row for 'WCF Commtouch' with a 'Trial' button highlighted in a red box and a status of 'On'. Below the table is a blue link: 'The Commtouch GlobalView Web Filter is provided for Vigor router with only 1-month trial. After trial period, please purchase the official package from your local DrayTek dealer/distributor.' A note at the bottom states: 'BPJM is the web content filter based on service operated in Germany. We recommend only users live in Germany to try the BPJM WCF service. This is a free service without guarantee.'

Service	Provider	Action	Status	Start Date	Expired Date
WCF Commtouch		Trial	On	-	-

10. 在接下來的頁面中，勾選“**I have read and accept the above Agreement**”方塊，再按 **Next**，系統將尋找適當的日期來啟動此服務。



11. 當如下頁面出現是，按下 **Register** 即可。



12. 請稍待系統運作直到看到下述頁面。

**DrayTek Service Activation**

Service Name	Start Date	Expire Date	Status
Web Content filter	2011-03-28	2011-04-27	Commtouch

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.

Copyright © DrayTek Corp. All Rights Reserved.

Close

13. 最後按下關閉 **Close** 本設定。

本頁留白



# 3

## 應用與練習

### 3.1 如何設定 IPv6 服務

面臨 IPv4 位址即將用罄的問題，各國紛紛開始推廣使用 IPv6，但為了能持續利用 IPv4 上既有的豐富資源，IPv6 和 IPv4 網路必須藉由一些互通機制使二個世界的成員互相通訊，以分階段逐步完成 IPv4->IPv6 的移轉工作。目前常見的互通機制分為三類：

- **雙堆疊(Dual Stack)**

讓使用者同時可以使用 IPv4 與 IPv6 網路的技術。在原有網路層(Network Layer)上，增加一個 IPv6 堆疊，讓主機同時具備 IPv4 及 IPv6 通訊能力。

- **建立通道(Tunnel)**

讓兩台 IPv6 主機透過現有 IPv4 網路環境進行通訊。將 IPv6 封包封裝在 IPv4 標頭中，使 IPv4 路由器可以藉由判讀取 IPv4 標頭，進行封包的轉送，待抵達位於 IPv4 與 IPv6 網路之間的邊緣路由器時，將 IPv4 標頭移除，以 IPv6 位址將 IPv6 封包轉送至 IPv6 網路中的目的地。

- **轉換(Translation)**

讓僅支援 IPv4 的使用者，可以與僅支援 IPv6 的使用者互相通訊。

在開始進行 Vigor292 的設定之前，您必須知道您所申請的 IPv6 服務，是屬於哪種連線類型(Connection Type)。

**注意：**針對 IPv6 服務，您需要設定 WAN/LAN 才能正常使用。

#### I. 進行 WAN 設定

Vigor2925 的 IPv6 WAN 設定，共提供了 5 種連線類型：PPP、TSPC、AICCU、DHCPv6 Client 和 Static IPv6。

1. 進入 Vigor2925 的網頁設定介面，開啓 **WAN>> Internet Access**，選擇一個 WAN 介面，選擇 **PPPoE** 作為**連線模式**然後按下**細節設定**按鈕。按下 **IPv6** 按鈕。

#### WAN >> 網際網路連線

##### 網際網路連線

索引編號	顯示名稱	實體連線模式	連線模式		
WAN1		乙太網路	固定或動態 IP	細節設定	IPv6
WAN2		乙太網路	無	細節設定	IPv6
WAN3		USB	無	細節設定	IPv6
WAN4		USB	無	細節設定	IPv6

**注意：**1. USB埠口1上的裝置套用 WAN3 設定。  
USB埠口2上的裝置套用 WAN4 設定。

**進階** 您可在此設定 DHCP 用戶端選項

**注意：**在同一時間裡，只有一個 WAN 介面可以使用 IPv6 功能。本例我們選擇 WAN2。

- 在此頁面中，自下拉式清單選擇您所使用的連線類型。

WAN >> 網際網路連線



WAN 2

PPPoE	固定或動態 IP	PPTP/L2TP	IPv6
<b>網際網路連線模式</b>			
連線類型		<div style="border: 1px solid black; padding: 2px;">           斷線            斷線  <b>PPP</b>            TSPC            AICCU            DHCPv6 用戶端            固定 IPv6            6in4 固定通道            6rd         </div>	
<input type="button" value="確定"/>			

不同的連線類型可帶出不同的設定畫面，分述如下：

- **PPP - 雙堆疊(Dual Stack)的應用**，可同時使用 IPv4 與 IPv6 網路  
選擇 PPP 並輸入 IPv4 PPPoE 的相關資訊。

WAN >> 網際網路連線

WAN 2

PPPoE	固定或動態 IP	PPTP/L2TP	IPv6
<input type="radio"/> 啟用 <input checked="" type="radio"/> 停用			
<b>ISP 存取設定</b> 使用者名稱: <input type="text" value="73768635@hinet.net"/> 密碼: <input type="password" value="••••"/> 索引號碼(1-15) 於 排程 設定: => <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>		<b>PPP/MP 設定</b> PPP 驗證: <input type="text" value="PAP 或 CHAP"/> 閒置逾時: <input type="text" value="-1"/> 秒 <b>IP 位址指派方式 (IPCP)</b> <input type="text" value="WAN IP別名"/> 固定 IP: <input type="radio"/> 是 <input checked="" type="radio"/> 否 (動態IP) 固定 IP 位址: <input type="text"/>	
<b>WAN 連線偵測</b> 模式: <input type="text" value="ARP 偵測"/> Ping IP: <input type="text"/> TTL: <input type="text"/>		<input checked="" type="radio"/> 預設 MAC 位址 <input type="radio"/> 指定 MAC 位址 MAC 位址: <input type="text" value="00"/> . <input type="text" value="1D"/> . <input type="text" value="AA"/> . <input type="text" value="AC"/> . <input type="text" value="1A"/> . <input type="text" value="3A"/>	
MTU: <input type="text" value="1442"/> (最大:1492)			
<input type="button" value="確定"/> <input type="button" value="取消"/>			

進入 IPv6 服務的設定頁面，您不需要進行任何設定。

WAN >>網際網路連線設定

WAN 2

PPPoE	固定或動態 IP	PPTP/L2TP	IPv6
-------	----------	-----------	------

網際網路連線模式  
 連線類型 PPP

附註：IPv4 WAN 設定應為 PPPoE 用戶端

確定
取消

按下**確定**按鈕，開啓**線上狀態**頁面，連線成功後，即可同時獲得 IPv4 和 IPv6 位址。

Online Status

Physical Connection		System Uptime: 0:1:17	
IPv4		IPv6	
<b>LAN Status</b>		Primary DNS: 168.95.192.1	
Secondary DNS: 168.95.1.1			
IP Address	TX Packets	RX Packets	
192.168.1.1	0	3085	
<b>WAN 1 Status</b>		>> <a href="#">Dial PPPoE</a>	
Enable	Line	Name	Mode
Yes	ADSL		PPPoE
	Up Time		00:00:00
IP	GW IP	TX Packets	TX Rate(Bps)
---	---	0	0
	RX Packets		RX Rate(Bps)
	0		0
<b>WAN 2 Status</b>		>> <a href="#">Drop PPPoE</a>	
Enable	Line	Name	Mode
Yes	Ethernet		PPPoE
	Up Time		0:00:54
IP	GW IP	TX Packets	TX Rate(Bps)
114.44.49.54	168.95.98.254	800	4761
	RX Packets		RX Rate(Bps)
	821		6617
<b>WAN 3 Status</b>			
Enable	Line	Name	Mode
Yes	USB		---
	Up Time		00:00:00
IP	GW IP	TX Packets	TX Rate(Bps)
---	---	0	0
	RX Packets		RX Rate(Bps)
	0		0
<b>ADSL Information</b>		(ADSL Firmware Version: 05-04-04-04-00-01)	
<b>ATM Statistics</b>			
TX Cells	RX Cells	TX CRC errs	RX CRC errs
0	0	0	0
<b>ADSL Status</b>	Mode	State	Up Speed
		READY	0
	Down Speed	SNR Margin	Loop Att.
	0	0	0

Online Status

Physical Connection

System Uptime: 0:2:32

IPv4	IPv6		
<b>LAN Status</b>			
<b>IP Address</b>			
2001:B010:7300:201:21D:AFF:FEA6:2568/64 (Global)			
FE80::21D:AFF:FEA6:2568/64 (Link)			
<b>TX Packets</b>	<b>RX Packets</b>	<b>TX Bytes</b>	<b>RX Bytes</b>
7	4	690	328
<b>WAN2 IPv6 Status</b>		<a href="#">Drop PPP</a>	
<b>Enable</b>	<b>Mode</b>	<b>Up Time</b>	
Yes	PPP	0:02:08	
<b>IP</b>		<b>Gateway IP</b>	
2001:B010:7300:201:21D:AFF:FEA6:256A/128 (Global)		FE80::90:1A00:242:AD52	
FE80::1D:AFF:FEA6:256A/128 (Link)			
<b>DNS IP</b>			
2001:8000:168::1			
2001:8000:168::2			
<b>TX Packets</b>	<b>RX Packets</b>	<b>TX Bytes</b>	<b>RX Bytes</b>
7	9	544	1126

- TSPC -通道(Tunnel)的應用，兩台 IPv6 主機透過現有 IPv4 網路環境進行通訊  
選擇 TSPC 類型，並輸入您所申請的 TSPC 服務資訊。

**注意：**使用此模式時，必須確認您的 IPv4 網路是連線的狀態。

(圖中所設定的 TSPC 資訊，是向 <http://gogo6.com/> 網站申請的)

WAN >>網際網路連線設定

WAN 2

PPPoE	固定或動態 IP	PPTP/L2TP	IPv6
<b>網際網路連線模式</b>			
連線類型		TSPC	
<b>TSPC 設定</b>			
使用者名稱	cacahsu		
密碼	●●●●●●		
確認密碼	●●●●●●		
通道代理人	broker.freenet6.net		
<input type="button" value="確定"/> <input type="button" value="取消"/>			

按下**確定**按鈕，開啓**線上狀態**頁面，通道成功建立顯示如下。

Online Status

Physical Connection System Uptime: 0:2:3

IPv4		IPv6	
<b>LAN Status</b>			
<b>IP Address</b>			
2001:5C0:1502:D00:21D:AFF:FEA6:2568/64 (Global)		FE80::21D:AFF:FEA6:2568/64 (Link)	
<b>TX Packets</b>	<b>RX Packets</b>	<b>TX Bytes</b>	<b>RX Bytes</b>
88	121	15596	10249
<b>WAN2 IPv6 Status</b>			
<b>Enable</b>	<b>Mode</b>	<b>Up Time</b>	
Yes	TSPC	0:01:40	
<b>IP</b>		<b>Gateway IP</b>	
2001:5C0:1400:8::10B9/128 (Global)		---	
FE80::722C:3559/128 (Link)			
<b>TX Packets</b>	<b>RX Packets</b>	<b>TX Bytes</b>	<b>RX Bytes</b>
127	89	9219	15866

- AICCU - 通道(Tunnel)的應用

選擇 AICCU 類型，並輸入您所申請的 AICCU 服務資訊。

**注意：**使用此模式時，必須確認您的 IPv4 網路是連線的狀態。

(圖中資訊是向 <https://www.sixxs.net/main/> 網站所申請的)

WAN >>網際網路連線設定

WAN 2

PPPoE	固定或動態 IP	PPTP/L2TP	IPv6
<b>網際網路連線模式</b>			
連線類型		AICCU	
<b>AICCU 設定</b>			
<input type="checkbox"/> 永遠連線			
使用者名稱	JCR3-SIXXS		
密碼	••••		
確認密碼	••••		
通道代理人	tic.sixxs.net		
子網前置號碼	2001:4DD0:FF00:8805::2		/ 64

附註：如果永遠連線未被啟動，AICCU 連線就只會嘗試連線三次

按下**確定**按鈕，開啓**線上狀態**頁面，通道成功建立顯示如下。

Online Status

Physical Connection System Uptime: 0:1:18

IPv4		IPv6	
<b>LAN Status</b>			
<b>IP Address</b>			
2001:4DD0:FF00:83E4:21D:AFF:FEA6:2568/64 (Global)			
FE80::21D:AFF:FEA6:2568/64 (Link)			
<b>TX Packets</b>	<b>RX Packets</b>	<b>TX Bytes</b>	<b>RX Bytes</b>
147	187	34205	19176
<b>WAN2 IPv6 Status</b>			
<b>Enable</b>	<b>Mode</b>	<b>Up Time</b>	
Yes	AICCU	0:00:48	
<b>IP</b>		<b>Gateway IP</b>	
2001:4DD0:FF00:3E4::2/64 (Global)		---	
FE80::4CD0:FF00:3E4:2/64 (Link)			
<b>TX Packets</b>	<b>RX Packets</b>	<b>TX Bytes</b>	<b>RX Bytes</b>
186	137	16438	33093

- DHCPv6 用戶端

選擇 DHCPv6 用戶端類型和哪種身分聯結方式，並輸入 IAID(辨識聯結 ID)。

WAN >> 網際網路連線設定

WAN 2

PPPoE	固定或動態 IP	PPTP/L2TP	IPv6
網際網路連線模式			
連線類型		DHCPv6 用戶端	
DHCPv6 用戶端設定			
身分聯結		<input checked="" type="radio"/> 前置號碼授權 <input type="radio"/> 非暫時位址	
IAID (辨識聯結 ID)		156010287	
<input type="button" value="確定"/> <input type="button" value="取消"/>			

按下**確定**按鈕，開啓**線上狀態**頁面，通道成功建立顯示如下。

Online Status

Physical Connection System Uptime: 0:0:50

IPv4		IPv6	
<b>LAN Status</b>			
<b>IP Address</b>			
FE80::21D:AFF:FEA6:2568/64 (Link)			
<b>TX Packets</b>	<b>RX Packets</b>	<b>TX Bytes</b>	<b>RX Bytes</b>
6	2	588	156
<b>WAN2 IPv6 Status</b>			
<b>Enable</b>	<b>Mode</b>	<b>Up Time</b>	
Yes	DHCPv6 Client	0:00:40	
<b>IP</b>		<b>Gateway IP</b>	
2001:8010:7300:201:21D:AFF:FEA6:256A/64 (Global)		---	
2001:1111:2222:5555:21D:AFF:FEA6:256A/64 (Global)			
2001:1111:2222:3333::1111/128 (Global)			
FE80::21D:AFF:FEA6:256A/64 (Link)			
<b>DNS IP</b>			
2001:4860:4860::8888			
2001:4860:4860::8844			
<b>TX Packets</b>	<b>RX Packets</b>	<b>TX Bytes</b>	<b>RX Bytes</b>
14	5	1174	694



- 固定 IPv6

選擇固定 IPv6 類型，並輸入 IPv6 位址、前置號碼長度和閘道位址。

WAN >> 網際網路連線設定

WAN 2

PPPoE      固定或動態 IP      PPTP/L2TP      IPv6

**網際網路連線模式**

連線類型

**固定 IPv6 位址設定**

IPv6 位址  / 前置號碼長度

**目前 IPv6 位址表格**

索引編號	IPv6 位址 / 前置號碼長度	範圍
1	2001:B010:7300:201:21D:AFF:FEA6:256A/64	Global
2	2001:1111:2222:5555:21D:AFF:FEA6:256A/64	Global
3	FE80::21D:AFF:FEA6:256A/64	Link

**固定 IPv6 閘道設定**

IPv6 閘道位址

按下**確定**按鈕，開啓**連線狀態**頁面，通道成功建立顯示如下：

Online Status

Physical Connection System Uptime: 0:4:2

IPv4		IPv6	
<b>LAN Status</b>			
IP Address			
FE80::21D:AFF:FEA6:2568/64 (Link)			
TX Packets	RX Packets	TX Bytes	RX Bytes
4	0	312	0
<b>WAN2 IPv6 Status</b>			
Enable	Mode	Up Time	
Yes	Static IPv6	0:03:56	
IP		Gateway IP	
2001:B010:7300:201:21D:AFF:FEA6:256A/64 (Global)		---	
2001:1111:2222:5555:21D:AFF:FEA6:256A/64 (Global)		---	
FE80::21D:AFF:FEA6:256A/64 (Link)		---	
TX Packets	RX Packets	TX Bytes	RX Bytes
8	2	608	364



## II. 進行 LAN 設定

完成 IPv6 的 WAN 設定後，接下來設定 LAN 的部份，讓路由器的用戶端，也能夠獲得 IPv6 位址。

1. 進入 Vigor2925 的網頁設定介面，開啓**區域網路>>基本設定**，按下 **IPv6** 按鈕，開啓如下畫面。

**注意：**只有 LAN1 子網支援 IPv6。

區域網路 >> 基本設定

---

LAN 1 區域網路 TCP/IP 與 DHCP 設定      LAN 1 IPv6 設定

**RADVD 設定**

啓用     停用

廣播有效時間 1800 秒數 (範圍：600 - 9000)

**DHCPv6 伺服器設定**

啓用伺服器     停用

起始 IPv6 位址                    2001:1111:2222:3333:1111

結束 IPv6 位址                    2001:1111:2222:3333:2222

**DNS 伺服器 IPv6 位址**

主要 DNS 伺服器                    2001:4860:4860:9999

次要 DNS 伺服器                    2001:4860:4860:8844

**固定 IPv6 位址設定**

IPv6 位址                            / 前置號碼長度

    /        

**目前 IPv6 位址表格**

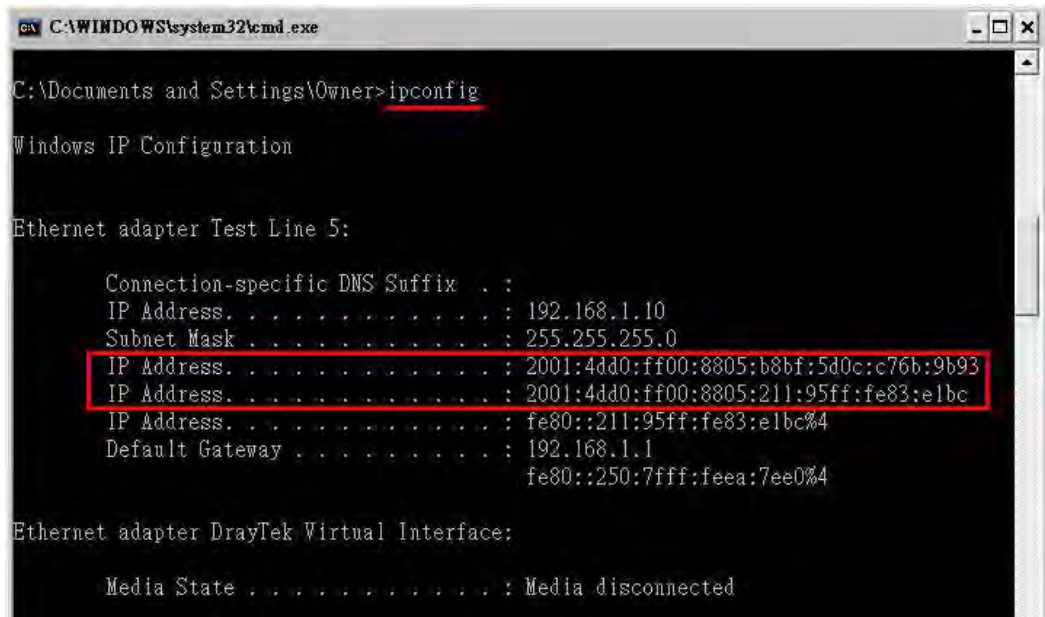
索引編號	IPv6 位址/前置號碼長度	範圍
1	FE80::21D:AAFF:FEAC:1A38/64	Link

2. 在 **RADVD 設定** 區域中，預設值是**啓用**的，用戶端的電腦將會自動要求 RADVD 服務所需的 IPv6 位址的前置號碼長度，並產生一組介面 ID 以便組合完整的 IPv6 位址。
3. 在 **DHCPv6 伺服器設定** 區域中，當啓用 DHCPv6 服務時，您可以在此自行指定可用的 IPv6 位址。

**注意：**當二種機制都啓用時，用戶端可以自行決定要使用哪種機制(例如 Window7 的預設機制為 RADVD)。

### III. 確認 IPv6 服務可成功運作

1. 請確認您已獲得正確的 IPv6 位址，進入 MS-DOS 畫面並輸入指令 ipconfig，參考下圖：



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Owner>ipconfig

Windows IP Configuration

Ethernet adapter Test Line 5:

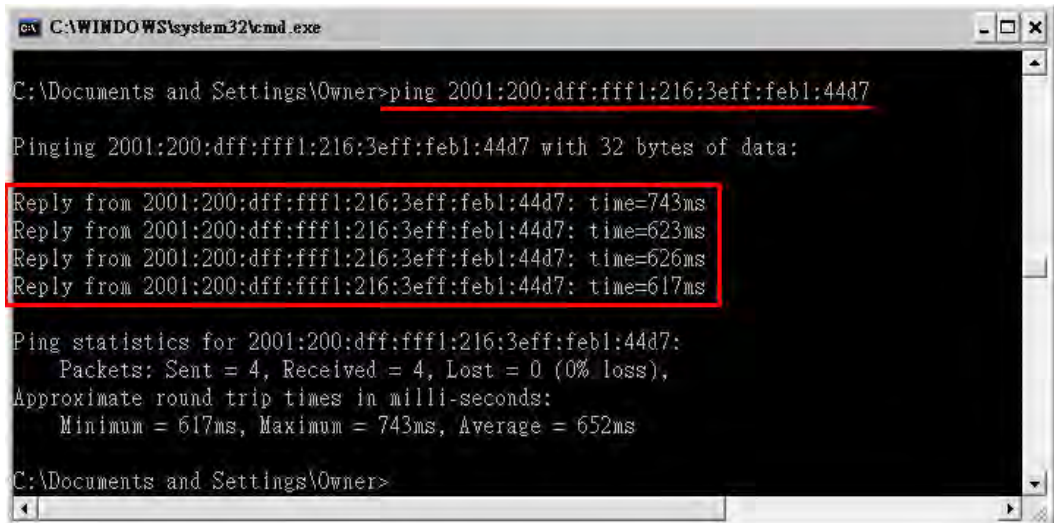
    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 192.168.1.10
    Subnet Mask . . . . .             : 255.255.255.0
    IP Address. . . . .               : 2001:4dd0:ff00:8805:b8bf:5d0c:c76b:9b93
    IP Address. . . . .               : 2001:4dd0:ff00:8805:211:95ff:fe83:e1bc
    IP Address. . . . .               : fe80::211:95ff:fe83:e1bc%4
    Default Gateway . . . . .         : 192.168.1.1
                                         fe80::250:7fff:feea:7ee0%4

Ethernet adapter DrayTek Virtual Interface:

    Media State . . . . .             : Media disconnected
```

從上圖中，我們可以看到系統偵測到的 IPv6 位址。

2. 使用 Ping 指令來檢查 IPv6 網站的 IPv6 位址，例如 [www.kame.net](http://www.kame.net) 是一個支援 IPv4 與 IPv6 服務的網站，其 IPv6 位址會以 2001:200:dff:fff1:216:3eff:feb1:44d7 這樣的格式出現。



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Owner>ping 2001:200:dff:fff1:216:3eff:feb1:44d7

Pinging 2001:200:dff:fff1:216:3eff:feb1:44d7 with 32 bytes of data:

Reply from 2001:200:dff:fff1:216:3eff:feb1:44d7: time=743ms
Reply from 2001:200:dff:fff1:216:3eff:feb1:44d7: time=623ms
Reply from 2001:200:dff:fff1:216:3eff:feb1:44d7: time=626ms
Reply from 2001:200:dff:fff1:216:3eff:feb1:44d7: time=617ms

Ping statistics for 2001:200:dff:fff1:216:3eff:feb1:44d7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 617ms, Maximum = 743ms, Average = 652ms

C:\Documents and Settings\Owner>
```

在您看到如上的訊息之後，即表示 IPv6 服務已經成功啟動了。

3. 連接到 IPv6 網站，開啓網頁瀏覽器並輸入 IPv6 的 URL 內容例如 [www.kame.net](http://www.kame.net)，如果您的電腦乃利用 IPv6 位址來存取網站，您可再螢幕上看見一隻跳舞的小烏龜，否則您只會看見靜止的小烏龜。



如果您在畫面上確實看到跳舞的小烏龜，就表示 IPv6 服務已經準備妥當，可供您存取使用。

## 3.2 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**磁碟連線**的訊息，如下所示：

USB 應用 >> USB 磁碟狀態

---

**USB 儲存裝置狀態**

連線狀態: **磁碟連線** 中斷 USB 磁碟連線

磁碟容量: 0 MB

可用容量: 2009 MB [更新頁面](#)

USB 磁碟用戶已連接 | [更新頁面](#) |

索引編號	服務	IP 位址(埠號)	使用者名稱
------	----	-----------	-------

**附註：** 如果USB磁碟的保護開關打開，磁碟將處於 **僅供讀取** 模式，無法覆寫資料。

2. 開啓 **USB 應用>>USB 基本設定**以檢查一般設定，按下**確定**。

USB 應用 >> USB 基本設定

---

**USB 基本設定**

**基本設定**

同步 FTP 連線  (最大 6)

預設字集  ▼

**Samba 服務設定(網路芳鄰)**

啟用  停用

**存取模式**

限用 LAN  LAN 與 WAN

**NetBios 命名服務**

工作群組名稱

主機名稱


- 附註：**
1. 如果字集設定為"英文"，系統僅支援較長之英文檔名
  2. 路由器的FTP伺服器會阻擋同時數個連線數的FTP下載，如果您的FTP用戶端具備數個連線數機制像是 FileZilla的話，為了取得較佳的連線效果，您必須將用戶的FTP同時連線設定為1。
  3. 工作群組名稱不可與主機名稱相同，工作群組最多可以有15個字元而與主機名稱最多可以有23 個字元，但二者都不能包含下述字元: . ; : " < > \* + = / \ | ? .

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**啓用**以便啓動此 FTP/Samba 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。

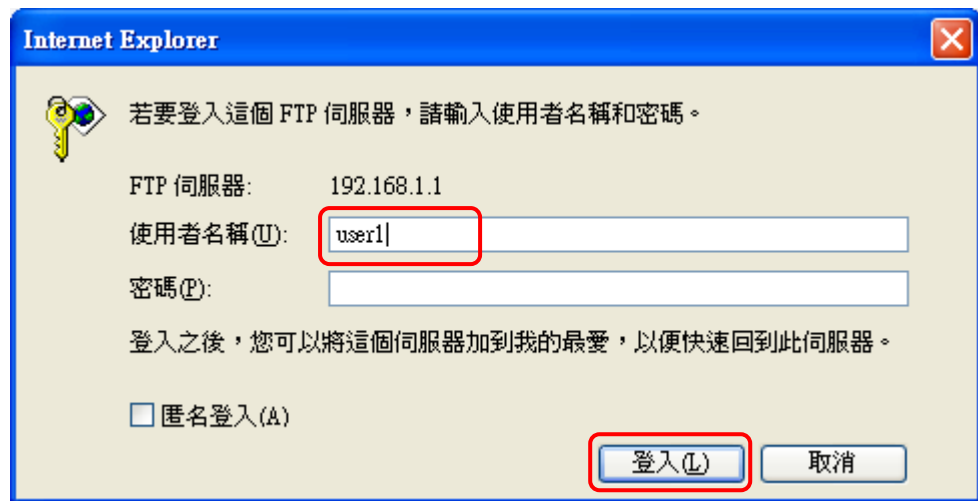
#### USB 應用 >> USB 使用者管理

##### 設定檔編號: 1

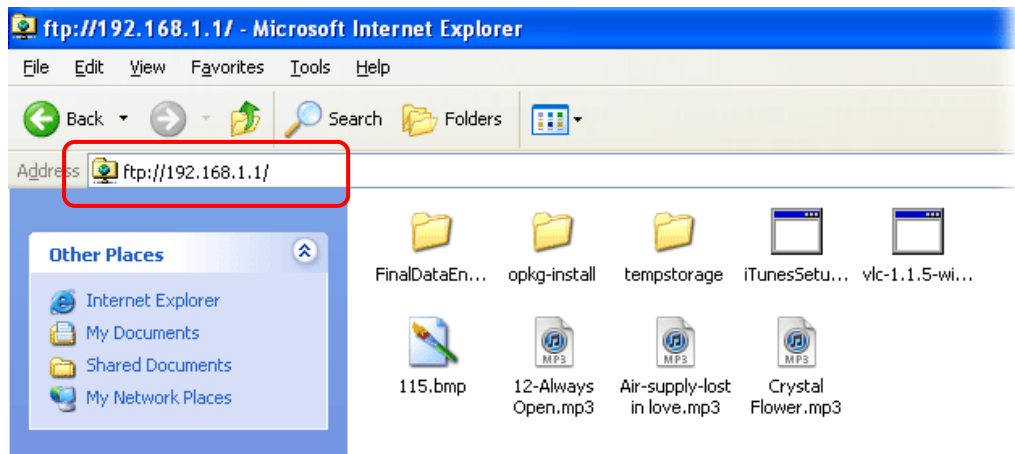
FTP/Samba 使用者	<input checked="" type="radio"/> 啓用 <input type="radio"/> 停用
使用者名稱	<input type="text"/>
密碼	<input type="text"/> (最多 11 個字元)
確認密碼	<input type="text"/>
預設檔案夾	<input type="text"/> 
<b>存取規則</b>	
檔案	<input type="checkbox"/> 讀取 <input type="checkbox"/> 覆寫 <input type="checkbox"/> 刪除
目錄	<input type="checkbox"/> 清單 <input type="checkbox"/> 建立 <input type="checkbox"/> 刪除

附註: 檔案夾名稱只能包含下列字元: A-Z a-z 0-9 \$ % ' - \_ @ ~ ! ( ) / 以及空格。

4. 按下**確定**按鈕儲存設定。
5. 確認 FTP 服務可以順利運作，請開啓任一瀏覽器並鍵入 <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。

### 3.3 如何在總公司與遠端分公司建立 LAN-to-LAN VPN 連線通道(透過 Main 模式)



#### 總公司的 Vigor 路由器設定

1. 登入路由器的使用者介面。
2. 開啓 VPN 與遠端存取 >> LAN to LAN 建立一個設定檔。

#### VPN 與遠端存取 >> LAN to LAN

LAN-to-LAN 設定檔: | 回復出廠預設值 |

檢視:  全部  線上  下線  Trunk 搜尋

索引編號	名稱	使用中	狀態	索引編號	名稱	使用中	狀態
1.	???	<input type="checkbox"/>	---	17.	???	<input type="checkbox"/>	---
2.	???	<input type="checkbox"/>	---	18.	???	<input type="checkbox"/>	---
3.	???	<input type="checkbox"/>	---	19.	???	<input type="checkbox"/>	---
4.	???	<input type="checkbox"/>	---	20.	???	<input type="checkbox"/>	---
5.	???	<input type="checkbox"/>	---	21.	???	<input type="checkbox"/>	---
6.	???	<input type="checkbox"/>	---	22.	???	<input type="checkbox"/>	---
7.	???	<input type="checkbox"/>	---	23.	???	<input type="checkbox"/>	---
8.	???	<input type="checkbox"/>	---	24.	???	<input type="checkbox"/>	---
9.	???	<input type="checkbox"/>	---	25.	???	<input type="checkbox"/>	---

3. 按下任何一個索引編號開啓設定頁面。輸入容易辨識的檔案名稱(本例我們使用 VPN Server)然後勾選啓用此設定檔方塊。由於路由器準備被視為伺服器，因此撥號方向應設定為撥入且閒置逾時設定為 0。

#### VPN 與遠端存取 >> LAN to LAN

設定檔索引: 1

1. 一般設定

設定檔名稱: VPN Server

啓用此設定檔

撥號方向:  雙向  撥出  撥入

永遠連線

閒置逾時:  秒

啓用 PING 以維持連線

指定 IP 位址:

VPN 撥出經由介面: WAN1 優先

Netbios 命名封包:  通過  封鎖

經由 VPN 執行多重播送:  通過  封鎖  
(針對某些 IGMP, IP-Camera, DHCP Relay 等而言)

2. 撥出設定



- 現在往下瀏覽設定頁面，在撥入設定中，勾選 PPTP、IPsec 通道以及 L2TP，勾選指定遠端 VPN 閘道，然後輸入對方 VPN 伺服器 IP 位址(例如本例使用的 218.242.130.19)，按下 **IKE 預先共用金鑰** 按鈕設定金鑰 PSK 再勾選中級(AH)或是高級(ESP)安全防護方式。

3. 撥入設定

<p><b>允許的撥入模式</b></p> <p><input checked="" type="checkbox"/> PPTP</p> <p><input checked="" type="checkbox"/> IPsec 通道</p> <p><input checked="" type="checkbox"/> 具有 IPsec 原則的 L2TP <span>無</span></p>	<p>使用者名稱 <input type="text" value="12345688"/></p> <p>密碼(最多 11 個字元) <input type="password" value="*****"/></p> <p>VJ 壓縮 <input checked="" type="radio"/> 開啟 <input type="radio"/> 關閉</p>
<p><input checked="" type="checkbox"/> 指定 遠端 VPN 閘道</p> <p>對方 VPN 伺服器 IP <input type="text" value="218.242.130.19"/></p> <p>或對方 ID <input type="text"/></p>	<p><b>IKE 驗證方式</b></p> <p><input checked="" type="checkbox"/> 預先共用金鑰</p> <p><input type="button" value="IKE 預先共用金鑰"/> <input type="password" value="*****"/></p> <p><input type="checkbox"/> 數位簽章(X.509)</p> <p><span>無</span></p> <p>本機 ID</p> <p><input checked="" type="radio"/> 替代主體名稱優先</p> <p><input type="radio"/> 主體名稱優先</p>
	<p><b>IPsec 安全防護方式</b></p> <p><input checked="" type="checkbox"/> 中級(AH)</p> <p>高級(ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES</p>

4. GRE over IPsec 設定

- 繼續往下瀏覽設定頁面至 TCP/IP 網路設定區域，設定遠端的 LAN IP 位址。

4. GRE over IPsec 設定

啟用 IPsec 撥出功能 GRE over IPsec

合理流量 我的 GRE IP  對方 GRE IP

5. TCP/IP 網路設定

<p>我的 WAN IP <input type="text" value="0.0.0.0"/></p> <p>遠端閘道 IP <input type="text" value="0.0.0.0"/></p> <p>遠端網路 IP <input type="text" value="192.168.1.10"/></p> <p>遠端網路遮罩 <input type="text" value="255.255.255.0"/></p> <p>本機網路 IP 位址 <input type="text" value="192.168.1.1"/></p> <p>本機網路遮罩 <input type="text" value="255.255.255.0"/></p> <p><input type="button" value="更多"/></p>	<p>RIP 方向 <span>停用</span></p> <p>從第一個子網路到遠端網路，您必須要作 <span>路由</span></p> <p><input type="checkbox"/> 變更預設路由到此 VPN 通道 (只有一個 WAN 支援此項功能)</p>
--	---

- 按下**確定**儲存。



- 開啓 VPN 與遠端存取>>連線管理檢查撥入連線的狀態(資料來自分公司)。

VPN 與遠端存取 >> 連線管理

撥出工具 更新間隔秒數: 10

基本模式: ( V2920 ) 172.16.2.145 <input type="button" value="撥號"/>
備援模式: <input type="button" value="撥號"/>
負載平衡模式: <input type="button" value="撥號"/>

VPN 連線狀態 目前所在頁面 1  頁面編號  >>

VPN	類型	遠端 IP	虛擬網路	傳送封包數	傳送速率 (Bps)	接收封包數	接收速率 (Bps)	運作時間
1 VPN Server )	IPSec Tunnel DES-SHA1 Auth	218.242.130.19	192.168.1.0/24	353	3	291	3	0:13:58 <input type="button" value="Drop"/>

xxxxxxxx:資料已加密。  
 xxxxxxxx:資料未加密。

### 分公司的 Vigor 路由器設定

- 登入路由器的使用者介面。
- 開啓 VPN 與遠端存取>>LAN to LAN 建立一個設定檔。

VPN 與遠端存取 >> LAN to LAN

LAN-to-LAN 設定檔: | 回復出廠預設值 |

檢視:  全部  線上  下線  Trunk

索引編號	名稱	使用中	狀態	索引編號	名稱	使用中	狀態
1.	???	<input type="checkbox"/>	---	17.	???	<input type="checkbox"/>	---
2.	???	<input type="checkbox"/>	---	18.	???	<input type="checkbox"/>	---
3.	???	<input type="checkbox"/>	---	19.	???	<input type="checkbox"/>	---
4.	???	<input type="checkbox"/>	---	20.	???	<input type="checkbox"/>	---
5.	???	<input type="checkbox"/>	---	21.	???	<input type="checkbox"/>	---
6.	???	<input type="checkbox"/>	---	22.	???	<input type="checkbox"/>	---

- 按下任何一個索引編號開啓設定頁面。輸入容易辨識的檔案名稱(本例我們使用 VPN Client)然後勾選啓用此設定檔方塊。由於路由器準備被視為用戶端，因此撥號方向應設定為撥出並勾選永遠連線。

VPN 與遠端存取 >> LAN to LAN

設定檔索引: 1

1. 一般設定

設定檔名稱 <input type="text" value="VPN Client"/> <input checked="" type="checkbox"/> 啟用此設定檔	撥號方向 <input type="radio"/> 雙向 <input checked="" type="radio"/> 撥出 <input type="radio"/> 撥入 <input checked="" type="checkbox"/> 永遠連線 閒置逾時 <input type="text" value="-1"/> 秒 <input type="checkbox"/> 啟用 PING 以維持連線 指定 IP 位址 <input type="text" value=""/>
VPN 撥出經由介面 <input type="text" value="WAN1 優先"/>	
Netbios 命名封包 <input checked="" type="radio"/> 通過 <input type="radio"/> 封鎖 經由 VPN 執行多重播送 <input type="radio"/> 通過 <input checked="" type="radio"/> 封鎖 <small>(針對某些 IGMP, IP-Camera, DHCP Relay 等而言)</small>	

- 現在往下瀏覽設定頁面，在**撥出設定**中，勾選 **IPsec 通道**，然後輸入遠端伺服器主機名稱/IP 位址(例如本例使用的 218.242.133.91)，按下 **IKE 預先共用金鑰** 按鈕設定金鑰 PSK 再勾選**中級(AH)**或是**高級(ESP)**安全防護方式。

#### 2. 撥出設定

<b>我撥出的伺服器類型</b> <input type="radio"/> PPTP <input checked="" type="radio"/> <b>IPsec 通道</b> <input type="radio"/> 具有 IPsec 原則的 L2TP <span style="border: 1px solid gray; padding: 0 5px;">無</span>		使用者名稱 <input type="text" value="???"/> 密碼(最多 15 個字元) <input type="password" value="....."/> PPP 驗證 <span style="border: 1px solid gray; padding: 0 5px;">PAP/CHAP</span> VJ 壓縮 <input checked="" type="radio"/> 開啟 <input type="radio"/> 關閉
對方 VPN 所需之伺服器 IP 或域名。 (例如 draytek.com 或 123.45.67.89) <input type="text" value="218.242.133.91"/>		<b>IKE 驗證方式</b> <input checked="" type="radio"/> <b>預先共用金鑰</b> <input type="radio"/> 數位簽章(X.509) 對方 ID <span style="border: 1px solid gray; padding: 0 5px;">無</span> 本機 ID <input checked="" type="radio"/> 替代主體名稱優先 <input type="radio"/> 主體名稱優先 本機憑證 <span style="border: 1px solid gray; padding: 0 5px;">無</span>
		<b>IPsec安全防護方式</b> <input type="radio"/> 中級(AH) <input checked="" type="radio"/> <b>高級(ESP)</b> <span style="border: 1px solid gray; padding: 0 5px;">DES 無驗證</span> <input type="button" value="進階"/>
索引號碼(1-15) 於 <b>排程</b> 設定: <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>		

- 繼續往下瀏覽設定頁面至 **TCP/IP 網路設定**區域，設定遠端的 LAN IP 位址。

#### 4. GRE over IPsec 設定

<input type="checkbox"/> 啟用 IPsec 撥出功能 GRE over IPsec
<input type="checkbox"/> 合理流量
我的 GRE IP <input type="text"/>
對方 GRE IP <input type="text"/>

#### 5. TCP/IP 網路設定

我的 WAN IP <input type="text" value="0.0.0.0"/>	RIP 方向 <span style="border: 1px solid gray; padding: 0 5px;">停用</span>
遠端開道 IP <input type="text" value="0.0.0.0"/>	從第一個子網路到遠端網路，您必須要作
<b>遠端網路 IP</b> <input type="text" value="127.17.1.0"/>	<span style="border: 1px solid gray; padding: 0 5px;">路由</span>
<b>遠端網路遮罩</b> <input type="text" value="255.255.255.0"/>	<input type="checkbox"/> 變更預設路由到此 VPN 通道 (只有一個 WAN 時才支援此項功能)
本機網路 IP 位址 <input type="text" value="192.168.1.9"/>	
本機網路遮罩 <input type="text" value="255.255.255.0"/>	
<input type="button" value="更多"/>	

- 按下**確定**儲存。

7. 開啓 VPN 與遠端存取>>連線管理檢查撥入連線的狀態(資料來自總公司)。

VPN 與遠端存取 >> 連線管理

撥出工具

更新間隔秒數: 10

基本模式:	( V2920 ) 172.16.2.145	<input type="button" value="撥號"/>
備援模式:		<input type="button" value="撥號"/>
負載平衡模式:		<input type="button" value="撥號"/>

VPN 連線狀態

目前所在頁面 1

頁面編號

VPN	類型	遠端 IP	虛擬網路	傳送封包數	傳送速率 (Bps)	接收封包數	接收速率 (Bps)	運作時間
1 ( VPN-Client )	IPSec Tunnel DES-SHA1 Auth	218.242.133.91	172.17.1.0/24	8	3	132	36	0:6:41 <input type="button" value="Drop"/>

xxxxxxxx:資料已加密。  
xxxxxxxx:資料未加密。

### 3.4 QoS 設定範例

假定電信工作人員有時在家中工作並且需要照料小孩，在工作時間，工作人員可使用家中的路由器，透過 HTTPS 或是 VPN 連接上總部的伺服器，來檢查電子郵件並存取公司內部的資料庫訊息，同時，小朋友也可以在休息室透過 VoIP 或是 Skype 彼此交談。

1. 進入**頻寬管理之服務品質**頁面。

頻寬管理 >> 服務品質(QoS)

---

基本設定 | 回復出廠預設值 |

索引編號	狀態	頻寬	方向	類別 1	類別 2	類別 3	其他	UDP	頻寬控制	連線狀態統計	
WAN1	啟用	100000Kbps/100000Kbps	上傳	25%	25%	25%	25%		不啟用	狀態	設定
WAN2	停用	100000Kbps/100000Kbps	上傳	25%	25%	25%	25%		不啟用	狀態	設定
WAN3	停用	100000Kbps/100000Kbps		25%	25%	25%	25%		不啟用	狀態	設定

類別規則

索引編號	名稱	規則	服務類型
類別 1		編輯	
類別 2		編輯	編輯
類別 3		編輯	

啟用VoIP SIP/RTP第一優先  
 SIP UDP 埠號:  (預設值: 5060)

2. 按WAN1 的**設定連結**開啓頁面，請確定左上角的**啟用服務品質(QoS)控制功能**已經勾選，選擇**雙向**作為方向。

頻寬管理 >> 服務品質(QoS)

---

WAN1 基本設定

啟用服務品質(QoS)控制功能 上傳 ▾

WAN 下載頻寬	下載	<input type="text" value="100000"/>	Kbps
WAN 上傳頻寬	上傳	<input type="text" value="100000"/>	Kbps
	雙向		

索引編號	類別名稱
類別 1	

3. 設定下載/上傳頻寬。

WAN1 基本設定

啟用服務品質(QoS)控制功能 雙向 ▾

WAN 下載頻寬	<input type="text" value="85000"/>	Kbps
WAN 上傳頻寬	<input type="text" value="80000"/>	Kbps

**注意:** 下載/上傳速率必須小於實際的頻寬，以確保正確計算服務品質(QoS)數值，建議以 ISP 業者提供的實際網路速度之 80% - 85% 設定頻寬值，取得最大的成效。

4. 回至上一層，按類別 1 的**編輯**連結以輸入索引類別 1 的名稱“E-mail”，再按**確定**。

類寬管理 >> 服務品質

類別索引#1

名稱   封包標籤為: 預設值

編號	狀態	本機地址	遠端位址	DiffServ CodePoint	服務類型
1	<input type="radio"/>	任何一種	任何一種	ANY	ANY

5. 使用者可設定保留頻寬(例如 25%) 給予透過POP3 和SMTP通訊協定來傳送的電子郵件。參考下圖。

類寬管理 >> 服務品質(QoS)

WAN1 基本設定

啟用服務品質(QoS)控制功能 雙向

WAN 下載頻寬  Kbps  
WAN 上傳頻寬  Kbps

索引編號	類別名稱	保留頻寬比例
類別 1	E-mail	<input type="text" value="25"/> %
類別 2		<input type="text" value="25"/> %
類別 3		<input type="text" value="25"/> %
	其他	<input type="text" value="25"/> %

啟用 UDP 頻寬控制  
 優先處理對外 TCP ACK

頻寬限制比率  %

6. 回至上一層，按類別 2 的**編輯**連結以輸入索引類別 2 的名稱“HTTP”，再按**確定**。於此類別中我們可以設定保留頻寬(例如 25%)給予**HTTP**。

類寬管理 >> 服務品質(QoS)

基本設定 | 回復出廠預設值 |

索引編號	狀態	頻寬	方向	類別 1	類別 2	類別 3	其他	UDP 頻寬控制	連線狀態統計
WAN1	啟用	85000Kbps/80000Kbps	雙向	25%	25%	25%	25%	不啟用	狀態 <input type="button" value="設定"/>
WAN2	停用	100000Kbps/100000Kbps	上傳	25%	25%	25%	25%	不啟用	狀態 <input type="button" value="設定"/>
WAN3	停用	100000Kbps/100000Kbps		25%	25%	25%	25%	不啟用	狀態 <input type="button" value="設定"/>

類別規則

索引編號	名稱	規則	服務類型
類別 1	E-mail	<input type="button" value="編輯"/>	<input type="button" value="編輯"/>
類別 2	HTTP	<input type="button" value="編輯"/>	
類別 3		<input type="button" value="編輯"/>	

啟用 VoIP SIP/RTP 第一優先  
SIP UDP 埠號:  (預設值: 5060)

7. 選擇WAN1 的設定連結。勾選**啟用UDP頻寬控制**防止VoIP大量的UDP資料影響其他的應用程式。

頻寬管理 >> 服務品質(QoS)

WAN1 基本設定

啟用服務品質(QoS)控制功能 雙向 ▾

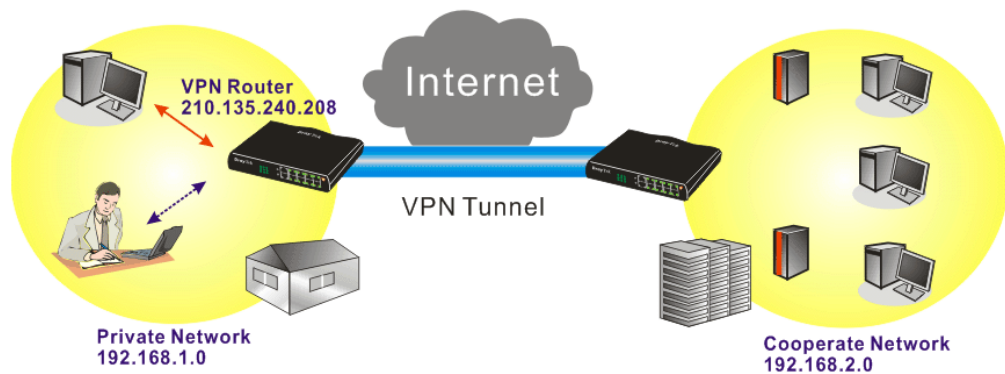
WAN 下載頻寬	85000	Kbps
WAN 上傳頻寬	80000	Kbps
索引編號	類別名稱	保留頻寬比例
類別 1	E-mail	25 %
類別 2	HTTP	25 %
類別 3		25 %
	其他	25 %
<input checked="" type="checkbox"/> 啟用 UDP 頻寬控制		頻寬限制比率 25 %
<input type="checkbox"/> 優先處理對外 TCP ACK		

確定

清除

取消

8. 如果工作人員利用主機對主機的VPN通道，連上了總公司，(詳細設定請參考VPN一節)他可能已設定了相關的索引內容，請輸入索引編號 3 的類別名稱，在此類別中，工作人員將可完成一條VPN通道的保留頻寬設定。

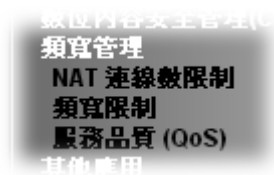


### 3.5 如何利用 QoS 來最佳化頻寬管理

您是否有過上傳/下載檔案(聲音、影像或是電子郵件、資料等等)時受到網際網路連線的頻寬限制或頻寬過窄的問題? Vigor 路由器進階版的 QoS 技術可幫助您依據實際需要分派不同比例的頻寬於不同的用途上。

假設您自 ISP 獲得的連線速度為 2MB/512Kb，家中需要用到 VoIP 網路電話、IPTV 機上盒以及一般的網路資料傳送，您希望整個頻寬中有 30% 用在 VoIP 網路電話，50% 用在 IPTV，15% 用在網路資料傳送，剩下的 5% 用作其他用途，那麼您可以參考下述的作法：

1. 開啓**頻寬管理**>>**服務品質(QoS)**。



2. 看到如下頁面之後，請按**類別 1**的**編輯**按鈕。

頻寬管理 >> 服務品質(QoS)

基本設定 | 回復出廠預設值 |

索引編號	狀態	頻寬	方向	類別 1	類別 2	類別 3	其他	UDP 頻寬控制	連線狀態統計	
WAN1	啟用	100000Kbps/100000Kbps	上傳	25%	25%	25%	25%	不啟用	狀態	設定
WAN2	停用	100000Kbps/100000Kbps	上傳	25%	25%	25%	25%	不啟用	狀態	設定
WAN3	停用	100000Kbps/100000Kbps		25%	25%	25%	25%	不啟用	狀態	設定

類別規則

索引編號	名稱	規則	服務類型
類別 1		編輯	
類別 2		編輯	編輯
類別 3		編輯	

啟用VoIP SIP/RTP第一優先

SIP UDP 埠號:  (預設值:5060)

3. 在**名稱**欄位請輸入 VoIP，然後按下**新增**按鈕。

頻寬管理 >> 服務品質

類別索引#1

名稱   封包標籤為:

編號	狀態	本機地址	遠端位址	DiffServ CodePoint	服務類型
1	空白	-	-	-	-

4. 勾選**啟用**方塊，在本機地址欄位中按下**編輯**按鈕。

頻寬管理 >> 服務品質

**編輯規則**

<input checked="" type="checkbox"/> 啟用	<input type="checkbox"/> 硬體加速
乙太網路類型	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
本機地址	Any <input type="button" value="編輯"/>
遠端地址	Any <input type="button" value="編輯"/>
DiffServ CodePoint	ANY
服務類型	---Predefined---

附註：請先選擇/設定 **服務類型**！

5. 於跳出視窗中，選擇**範圍位址**作為**位址類型**，輸入起始 IP 位址以及結束 IP 位址，最後按下**確定**儲存設定並離開此視窗。

192.168.1.3/doc/QosIpEdt.htm - 楓樹瀏覽器

192.168.1.3/doc/QosIpEdt.htm

乙太網路類型: IPv4

位址類型	範圍位址
起始 IP 位址	172.16.1.240
結束 IP 位址	172.16.1.241
子網路遮罩	0.0.0.0

6. 再次按下**確定**儲存設定。

頻寬管理 >> 服務品質

**編輯規則**

<input checked="" type="checkbox"/> 啟用	<input type="checkbox"/> 硬體加速
乙太網路類型	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
本機地址	172.16.1.240~172.16.1.241 <input type="button" value="編輯"/>
遠端地址	Any <input type="button" value="編輯"/>
DiffServ CodePoint	ANY
服務類型	---Predefined---

附註：請先選擇/設定 **服務類型**！



7. VoIP 類別規則已經設定完畢，按下**確定**回到前一個頁面。

類寬管理 >> 服務品質

類別索引#1

名稱   封包標籤為:

編號	狀態	本機地址	遠端位址	DiffServ CodePoint	服務類型
1 <input type="radio"/>	啟用	172.16.1.240 ~ 172.16.1.241	任何一種	ANY	ANY

8. 採取同樣的步驟分別再設定 IPTV 與資料/電子郵件傳輸的類別內容。

類寬管理 >> 服務品質

類別索引#2

名稱   封包標籤為:

編號	狀態	本機地址	遠端位址	DiffServ CodePoint	服務類型
1 <input type="radio"/>	啟用	172.16.1.242 ~ 172.16.1.249	任何一種	ANY	ANY

以及

類寬管理 >> 服務品質

類別索引#3

名稱   封包標籤為:

編號	狀態	本機地址	遠端位址	DiffServ CodePoint	服務類型
1 <input type="radio"/>	啟用	任何一種	任何一種	IP precedence 2	ANY

9. 假使您的網路連線有 2MB/512Kb，您可以按下 WAN1 的設定連結來設定上述不同群組的個別頻寬。

頻寬管理 >> 服務品質(QoS)

基本設定 | 回復出廠預設值 |

索引編號	狀態	頻寬	方向	類別 1	類別 2	類別 3	其他	UDP 頻寬控制	連線狀態統計	
WAN1	啟用	100000Kbps/100000Kbps	上傳	25%	25%	25%	25%	不啟用	狀態	設定
WAN2	停用	100000Kbps/100000Kbps	上傳	25%	25%	25%	25%	不啟用	狀態	設定
WAN3	停用	100000Kbps/100000Kbps		25%	25%	25%	25%	不啟用	狀態	設定

類別規則

索引編號	名稱	規則	服務類型
類別 1		編輯	
類別 2		編輯	編輯
類別 3		編輯	

10. 在設定頁面上，勾選啟用服務品質控制功能方塊，三個類別中分別輸入 30, 50 與 15 等比例，如下圖所示。記得勾選啟用 UDP 頻寬控制。

頻寬管理 >> 服務品質(QoS)

WAN1 基本設定

啟用服務品質(QoS)控制功能 上傳

WAN 下載頻寬  Kbps

WAN 上傳頻寬  Kbps

索引編號	類別名稱	保留頻寬比例
類別 1	VoIP	<input type="text" value="30"/> %
類別 2	IPTV	<input type="text" value="50"/> %
類別 3	Data Email	<input type="text" value="15"/> %
	其他	<input type="text" value="5"/> %

啟用 UDP 頻寬控制 頻寬限制比率  %

優先處理對外 TCP ACK

確定 清除 取消

11. 按下確定儲存，WAN1 的類別設定定義將呈現如下：

頻寬管理 >> 服務品質(QoS)

基本設定 | 回復出廠預設值 |

索引編號	狀態	頻寬	方向	類別 1	類別 2	類別 3	其他	UDP 頻寬控制	連線狀態統計	
WAN1	啟用	100000Kbps/100000Kbps	上傳	30%	50%	15%	5%	不啟用	狀態	設定
WAN2	停用	100000Kbps/100000Kbps	上傳	25%	25%	25%	25%	不啟用	狀態	設定
WAN3	停用	100000Kbps/100000Kbps		25%	25%	25%	25%	不啟用	狀態	設定

### 3.6 如何客製化登入頁面

按照管理者的需要，我們可以客製化登入頁面。

1. 開啓**使用者管理>>基本設定**，選擇**使用者模式**，按下**確定**按鈕儲存設定。

**使用者管理 >> 基本設定**

#### 基本設定

模式:

網頁驗證:

**注意:**

1. 使用者管理將會參考資料過濾器中可用的規則，將之視為白名單與黑名單。  
在**使用者模式**之**防火牆**
2. 符合上述清單中的使用者將不需要通過驗證。  
**防火牆規則策略**仍有效
3. 不符合上述清單中的使用者則需要通過**路由器驗證**。  
**使用者設定檔**中的**防火牆規則**仍然有效。

指定首頁 (最多 255 個字元) | [上一頁](#) | [回復出廠預設值](#) |

```
<body stats=1><script language='javascript'>
window.location='http://www.draytek.com'</script></body>
```

2. 開啓**使用者管理>>使用者設定檔**，建立一個新的使用者設定檔案。

**使用者管理 >> 使用者設定檔**

#### 使用者設定檔列表

[回復出廠預設值](#)

設定檔	名稱	設定檔	名稱
<a href="#">1.</a>	admin	<a href="#">17.</a>	
<a href="#">2.</a>	Dial-In User	<a href="#">18.</a>	
<a href="#">3.</a>		<a href="#">19.</a>	
<a href="#">4.</a>		<a href="#">20.</a>	
<a href="#">5.</a>		<a href="#">21.</a>	
<a href="#">6.</a>		<a href="#">22.</a>	
<a href="#">7.</a>		<a href="#">23.</a>	
<a href="#">8.</a>		<a href="#">24.</a>	
<a href="#">9.</a>		<a href="#">25.</a>	
<a href="#">10.</a>		<a href="#">26.</a>	
<a href="#">11.</a>		<a href="#">27.</a>	
<a href="#">12.</a>		<a href="#">28.</a>	
<a href="#">13.</a>		<a href="#">29.</a>	
<a href="#">14.</a>		<a href="#">30.</a>	
<a href="#">15.</a>		<a href="#">31.</a>	
<a href="#">16.</a>		<a href="#">32.</a>	

<< [1-32](#) | [33-64](#) | [65-96](#) | [97-128](#) | [129-160](#) | [161-192](#) | [193-200](#) >>

[下一頁](#) >>

- 按下任一連結(例如#3)開啓如下頁面，輸入使用者名稱以及密碼，然後按下**確定**按鈕儲存。

使用者管理 >> 使用者設定檔

索引編號 3

<input checked="" type="checkbox"/>	啓動此帳號	
	使用者名稱	<input type="text" value="carrie"/>
	密碼	<input type="password" value="*****"/>
	確認密碼	<input type="password" value="*****"/>
	閒置逾時	<input type="text" value="10"/> 分鐘, 0:無限制
	最多登入使用者數目	<input type="text" value="0"/> 0:無限制
	原則	<input type="text" value="預設值"/>
	記錄	<input type="text" value="無"/>
	快顯瀏覽器追蹤視窗	<input checked="" type="checkbox"/>
	驗證	<input checked="" type="checkbox"/> 網頁 <input checked="" type="checkbox"/> 警告工具 <input checked="" type="checkbox"/> Telnet
	指定首頁	<input type="checkbox"/>
	索引號碼(1-15) 於 <b>捷程</b> 設定:	<input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>
<input type="checkbox"/>	啓用時間額度	0 分 <input type="text" value="0"/> 分
<input type="checkbox"/>	啓用資料額度	0 MB <input type="text" value="0"/> MB

選擇項目必須同規則般建立，且不可設定為目前使用中。

- 開啓**系統維護**>>**登入頁面設定**，勾選**啓用**方塊，輸入於登入對話盒顯示的頁面標題(例如 *Just for Carrie*)，接著按下**確定**。

系統維護 >> 登入頁面設定

登入頁面設定

<input checked="" type="checkbox"/>	啓用
	登入頁面標題 <input type="text" value="Just for Carrie"/> (最多 31 個字元)
	歡迎訊息與佈告欄 (文長最多 511 個字元) <span style="float: right;">預覽   回復出廠預設值  </span>
	<pre>&lt;h1&gt;&lt;b&gt;&lt;font color=red&gt;Welcome Message&lt;/font&gt;&lt;/b&gt;&lt;/h1&gt;&lt;p&gt;This welcome message is displayed in the Login page of the router. Replace this text with your own message. &lt;/p&gt;&lt;ol&gt;&lt;li&gt;The welcome message can be written in HTML so lists such as this one can be created &lt;/li&gt;&lt;li&gt;Other markup tags such as p, font or img can be used&lt;/li&gt;&lt;/ol&gt;</pre>
	歡迎訊息範例: <h1><b><font color=red>Welcome Message</font></b></h1> <p>訊息</p>

注意切勿在佈告欄方塊中輸入 URL 重新導向連結。

- 在相同的瀏覽器(IE 7.0/FireFox 或更新版本)下開啓另外一個視窗，或是開啓新的瀏覽器。
- 請嘗試登入 Vigor 路由器的網頁設定介面(例如 192.168.1.1)，在登入對話盒中可看到剛剛設定的標題“*Just for Carrie*”顯示在螢幕上。



7. 在您輸入使用者名稱與密碼(於**使用者管理**>>**使用者設定檔**頁面中定義)後，按下**登入**按鈕，您可以存取網際網路或是登入您在**使用者管理**>**基本設定**頁面中所啓用的指定首頁。

### 3.7 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. 先設定相關物件。首先開啓物件設定>>簡訊(SMS)/郵件服務物件頁面。

物件設定 >> 簡訊(SMS) / 郵件服務物件

索引編號	設定檔名稱	簡訊服務(SMS)供應商
1.		kotsms.com.tw (TW)
2.		kotsms.com.tw (TW)
3.		kotsms.com.tw (TW)
4.		kotsms.com.tw (TW)
5.		kotsms.com.tw (TW)
6.		kotsms.com.tw (TW)
7.		kotsms.com.tw (TW)
8.		kotsms.com.tw (TW)
9.	Custom 1	
10.	Custom 2	

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，在下列開啓的頁面中，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(SMS) / 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)
使用者名稱	line1
密碼	****
簡訊則數	10
寄送間隔時間	3 (秒數)

確定 清除 取消

- 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。

物件設定 >> 簡訊(SMS) / 郵件服務物件

簡訊服務(SMS)供應商		郵件伺服器	回復出廠預設值
索引編號	設定檔名稱	簡訊服務(SMS)供應商	
1.	Local number	kotsms.com.tw (TW)	
2.		kotsms.com.tw (TW)	
3.		kotsms.com.tw (TW)	
4.		kotsms.com.tw (TW)	
5.		kotsms.com.tw (TW)	
6.		kotsms.com.tw (TW)	
7.		kotsms.com.tw (TW)	
8.		kotsms.com.tw (TW)	
9.	Custom 1		
10.	Custom 2		

- 接著開啓物件設定>>通知物件，設定通知的事件內容。

物件設定 >> 通知物件

索引編號	設定檔名稱	設定	回復出廠預設值
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			

- 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，在下列開啓的頁面中，輸入設定檔名稱，再勾選 WAN 類別中的**中斷連線**與**重新連線**來呼應本文的主題。

物件設定 >> 通知物件

設定檔索引編號: 1

設定檔名稱:

類別	狀態	
WAN	<input checked="" type="checkbox"/> 中斷連線	<input checked="" type="checkbox"/> 重新連線
VPN 通道	<input type="checkbox"/> 中斷連線	<input type="checkbox"/> 重新連線
溫度警示	<input type="checkbox"/> 超出範圍	

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。

物件設定 >> 通知物件

回復出廠預設值		
索引編號	設定檔名稱	設定
1.	WAN_Notify	WAN
2.		
3.		
4.		
5.		
6.		
7.		
8.		

8. 現在，開啓**其他應用>>簡訊(SMS) / 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**收信人**欄位中填入您欲接收簡訊通知的號碼。

其他應用 >> 簡訊(SMS) / 郵件警告服務

簡訊(SMS)服務供應商		郵件伺服器		回復出廠預設值	
索引編號	簡訊(SMS)服務供應商	收信人	通知設定檔	排程(1-15)	
1 <input checked="" type="checkbox"/>	1 - Local number	0955201340	1 - WAN_Notify	<input type="text"/>	<input type="text"/>
2 <input type="checkbox"/>	1 - Local number	<input type="text"/>	1 - WAN_Notify	<input type="text"/>	<input type="text"/>
3 <input type="checkbox"/>	2 - ???	<input type="text"/>	1 - WAN_Notify	<input type="text"/>	<input type="text"/>
4 <input type="checkbox"/>	3 - ???	<input type="text"/>	1 - WAN_Notify	<input type="text"/>	<input type="text"/>
5 <input type="checkbox"/>	4 - ???	<input type="text"/>	1 - WAN_Notify	<input type="text"/>	<input type="text"/>
6 <input type="checkbox"/>	5 - ???	<input type="text"/>	1 - WAN_Notify	<input type="text"/>	<input type="text"/>
7 <input type="checkbox"/>	6 - ???	<input type="text"/>	1 - WAN_Notify	<input type="text"/>	<input type="text"/>
8 <input type="checkbox"/>	7 - ???	<input type="text"/>	1 - WAN_Notify	<input type="text"/>	<input type="text"/>
9 <input type="checkbox"/>	8 - ???	<input type="text"/>	1 - WAN_Notify	<input type="text"/>	<input type="text"/>
10 <input type="checkbox"/>	9 - Custom 1	<input type="text"/>	1 - WAN_Notify	<input type="text"/>	<input type="text"/>
	10 - Custom 2	<input type="text"/>	1 - WAN_Notify	<input type="text"/>	<input type="text"/>
	1 - Local number	<input type="text"/>	1 - WAN_Notify	<input type="text"/>	<input type="text"/>
	1 - Local number	<input type="text"/>	1 - WAN_Notify	<input type="text"/>	<input type="text"/>
	1 - Local number	<input type="text"/>	1 - WAN_Notify	<input type="text"/>	<input type="text"/>



➤ 備註：如何自訂簡訊服務供應商

開啓物件設定>>簡訊(SMS)/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)，在開啓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。

物件設定 >> 簡訊(SMS) / 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	clickatell
<div style="border: 1px solid black; height: 50px; width: 100%;"></div>	
請與您的簡訊服務供應商連絡，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###	
使用者名稱	ilan1234
密碼	*****
簡訊則數	10
寄送間隔時間	3 (秒數)

確定 清除 取消

### 3.8 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。

#### 3.8.1 透過 Vigor 路由器來建立

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

數位內容安全管理 >> 網頁內容過濾器設定檔

---

網頁過濾器授權碼 啓動  
[狀態:Commtouch] [起始日期:2013-02-25 到期日期:2013-03-27]

設定搜尋伺服器	auto-selected	更多
設定測試伺服器	auto-selected	更多

測試站點，檢查該站是否已被歸類

網頁內容過濾器設定檔表格: | 回復出廠預設值 |

設定檔	名稱	設定檔	名稱
1.	Default	5.	
2.		6.	
3.		7.	
4.		8.	

管理訊息 (最多 255 個字元) 預設訊息 快捷: L1 + L2 快捷 ▾

```
<body><center><br><br><br><p>The requested Web page <br> from %SIP% <br>to %URL% <br>that is categorized with %CL% <br>has been blocked by %RNAME% Web Content Filter.<p>Please contact your system administrator for further information.</center></body>
```

或是

開啟**系統維護>>開啓授權碼**，

系統維護 >> 開啓授權碼 啓動經由介面: 自動選取 ▾

---

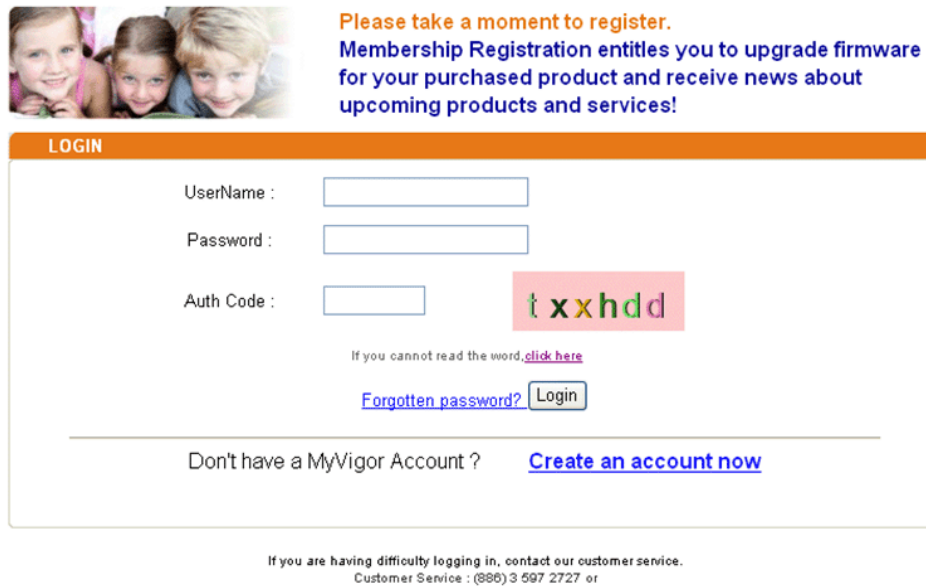
網頁過濾器授權碼 啓動  
[狀態:Not Activated]

驗證訊息

附註: 如果您想要使用郵件警示或Syslog，請設定 **SysLog郵件警示設定** 頁面。  
如果您變更了服務供應商，必須重新配置功能設定。

確定 取消

2. 按下 **啓動** 連結，MyVigor 登入視窗將會自動跳出。



Please take a moment to register.  
Membership Registration entitles you to upgrade firmware for your purchased product and receive news about upcoming products and services!

**LOGIN**

UserName :

Password :

Auth Code :  **t x x h d d**

If you cannot read the word, [click here](#)

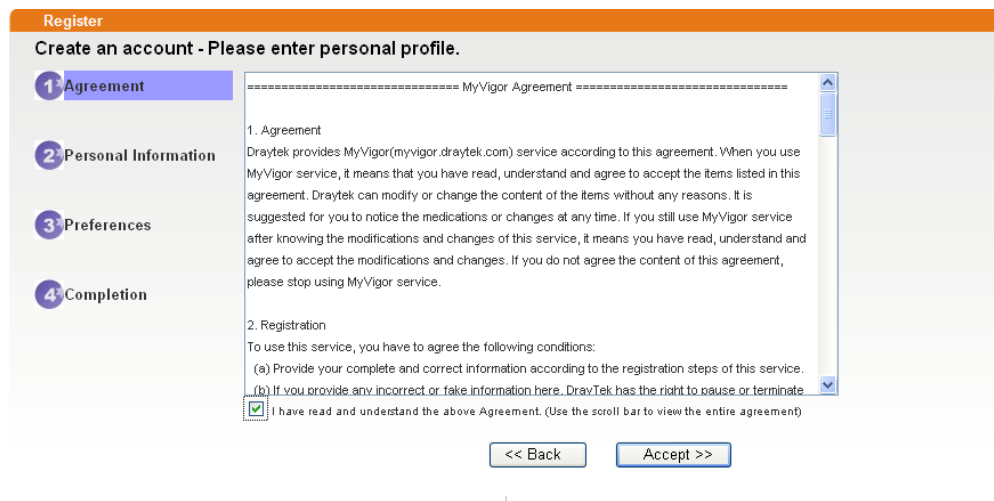
[Forgotten password?](#)

---

Don't have a MyVigor Account ? [Create an account now](#)

If you are having difficulty logging in, contact our customer service.  
Customer Service : (886) 3 597 2727 or

3. 按下 **Create an account now** 連結。
4. 確認您已同意畫面上的聲明並勾選同意方塊，接著按下 **Accept**。



**Register**

Create an account - Please enter personal profile.

- 1 Agreement
- 2 Personal Information
- 3 Preferences
- 4 Completion

===== MyVigor Agreement =====

1. Agreement  
Draytek provides MyVigor(myvigor.draytek.com) service according to this agreement. When you use MyVigor service, it means that you have read, understand and agree to accept the items listed in this agreement. Draytek can modify or change the content of the items without any reasons. It is suggested for you to notice the modifications or changes at any time. If you still use MyVigor service after knowing the modifications and changes of this service, it means you have read, understand and agree to accept the modifications and changes. If you do not agree the content of this agreement, please stop using MyVigor service.

2. Registration  
To use this service, you have to agree the following conditions:  
(a) Provide your complete and correct information according to the registration steps of this service.  
(b) If you provide any incorrect or fake information here, DrayTek has the right to pause or terminate your account.

I have read and understand the above Agreement. (Use the scroll bar to view the entire agreement)

5. 輸入個人資訊並按下 **Continue**。

Register

Create an account - Please enter personal profile. (Fields marked by (\*) are required)

1 Agreement

2 **Personal Information**

3 Preferences

4 Completion

**Account Information**

UserName: \* Mary (3 ~ 20 characters)

Password: \* \*\*\*\* (4 ~ 20 characters: Do not set the same as the username.)

Confirm Password: \* \*\*\*\*

**Personal Information**

First Name: \* Mary

Last Name: \* Ted

Company Name: Tech Ltd.

Email Address: \* mary\_ted@tech.com

Please note that a valid E-mail address is required to receive the Subscription Code. You will need this code to activate your account.

Tel: 0 -

Country: \* SWITZERLAND

Career: \* Supervisor

<< Back 

6. 選擇適合您的電腦的選項，再按下 **Continue**。

Register

Create an account - Please enter personal profile.

1 Agreement

2 Personal Information

3 **Preferences**

4 Completion

How did you find out about this website? Internet

What kind of anti-virus do you use? AntiVir

I would like to subscribe to the MyVigor e-letter.

I would like to receive DrayTek product news.

Please select the mail server for receiving the verification mail. Global Server

<< Back 

7. 現在您已經成功建立一個帳號了，請按 **START**。

Register

Create an account - Please enter personal profile.

1 Agreement

2 Personal Information

3 Preferences

4 **Completion**

Completion

A confirmation email has been sent to mary\_ted@tech.com  
Please click on the activation link in the email  
to activate your account

**START**

- 請先去信箱查看郵件，是否收到標題為 **New Account Confirmation Letter from [myvigor.draytek.com](http://myvigor.draytek.com)** 的信件。

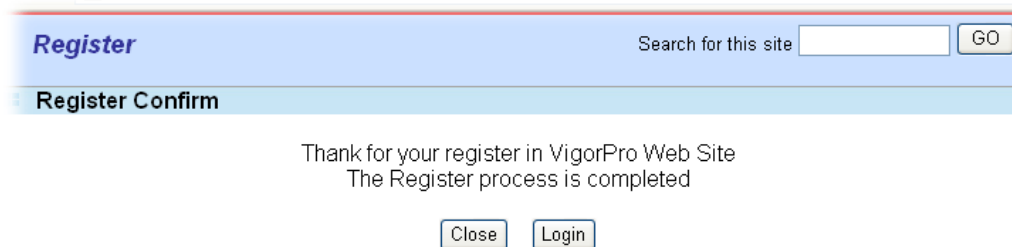
\*\*\*\*\* This is an automated message from myvigor.draytek.com. \*\*\*\*\*

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

Please click on the activation link below to activate your account

Link : [Activate my Account](#)

- 若已收到，請按下 **Activate my Account** 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**。



**Register** Search for this site

**Register Confirm**

Thank for your register in VigorPro Web Site  
The Register process is completed

- 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)。



**LOGIN**

Please take a moment to register.  
Membership Registration entitles you to upgrade firmware  
for your purchased product and receive news about  
upcoming products and services!

UserName :

Password :

Auth Code :  

If you cannot read the word, [click here](#)

[Forgotten password?](#)

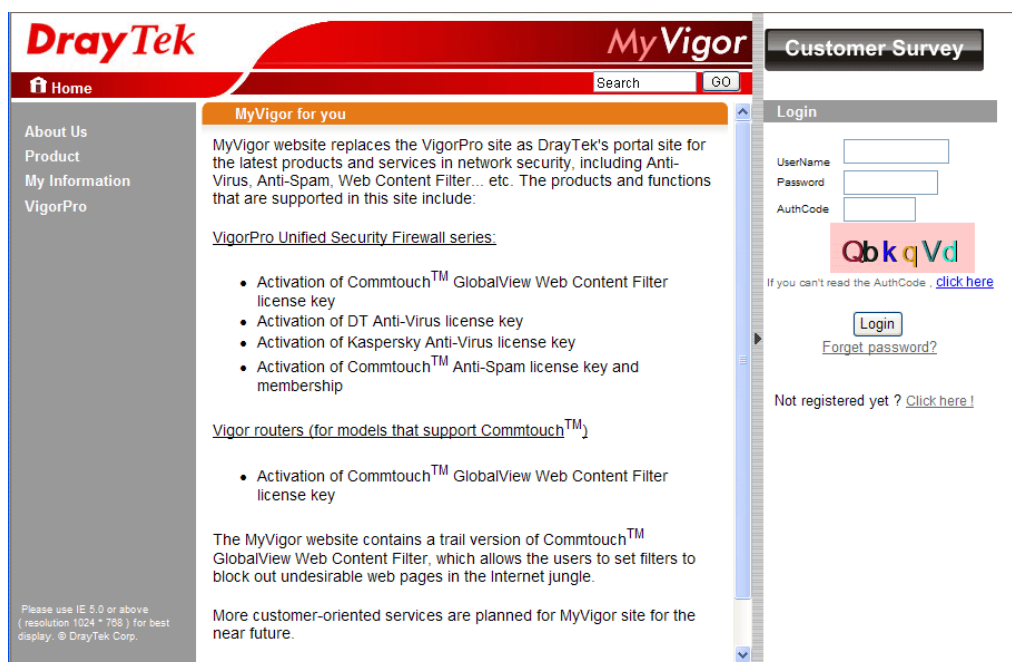
Don't have a MyVigor Account ? [Create an account now](#)

If you are having difficulty logging in, contact our customer service.  
Customer Service : (886) 3 597 2727 or

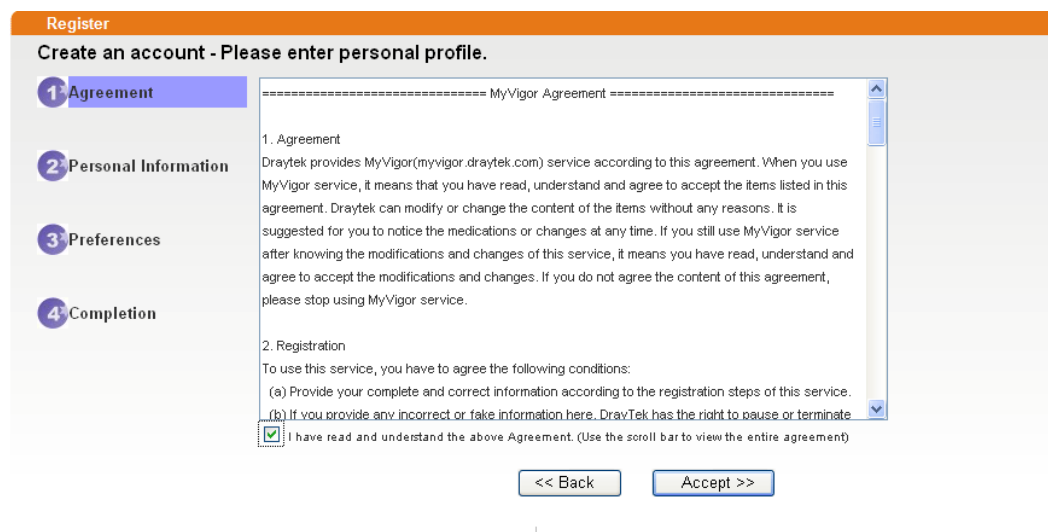
- 輸入驗證碼之後，按下 **Login**。系統將帶您進入 MyVigor 伺服器。

### 3.8.2 透過 MyVigor 網站來建立

1. 登入 <http://myvigor.draytek.com>，找到 **Not registered yet?** 這行之後，按下旁邊的 **Click here!** 連結進入下一個畫面。



2. 確認您已同意畫面上的聲明並勾選同意方塊，接著按下 **Accept**。



3. 輸入個人資訊並按下 **Continue**。

Register

Create an account - Please enter personal profile. (Fields marked by (\*) are required)

1 Agreement

2 Personal Information

3 Preferences

4 Completion

**Account Information**

UserName:\* Mary

(3 ~ 20 characters)

Password:\* \*\*\*\*

(4 ~ 20 characters : Do not set the same as the username.)

Confirm Password:\* \*\*\*\*

**Personal Information**

First Name:\* Mary

Last Name:\* Ted

Company Name: Tech Ltd.

Email Address:\* mary\_ted@tech.com

Please note that a valid E-mail address is required to receive the Subscription Code. You will need this code to activate your account.

Tel: 0 -

Country:\* SWITZERLAND

Career:\* Supervisor

<< Back    Continue >>

4. 選擇適合您的電腦的選項，再按下 **Continue**。

Register

Create an account - Please enter personal profile.

1 Agreement

2 Personal Information

3 Preferences

4 Completion

How did you find out about this website? Internet

What kind of anti-virus do you use? AntiVir

I would like to subscribe to the MyVigor e-letter.

I would like to receive DrayTek product news.

Please select the mail server for receiving the verification mail. Global Server

<< Back    Continue >>

5. 現在您已經成功建立一個帳號了，請按 **START**。

Register

Create an account - Please enter personal profile.

1 Agreement

2 Personal Information

3 Preferences

4 Completion

**Completion**

A confirmation email has been sent to mary\_ted@tech.com  
Please click on the activation link in the email  
to activate your account

**START**

6. 請先去信箱查看郵件，是否收到標題為 **New Account Confirmation Letter from [myvigor.draytek.com](http://myvigor.draytek.com)** 的信件。

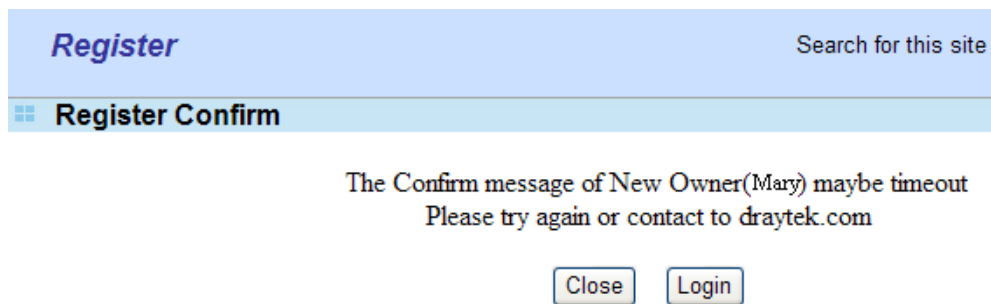
\*\*\*\*\* This is an automated message from myvigor.draytek.com.\*\*\*\*\*

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

Please click on the activation link below to activate your account

Link : [Activate my Account](#)

7. 若已收到，請按下 **Activate my Account** 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**。



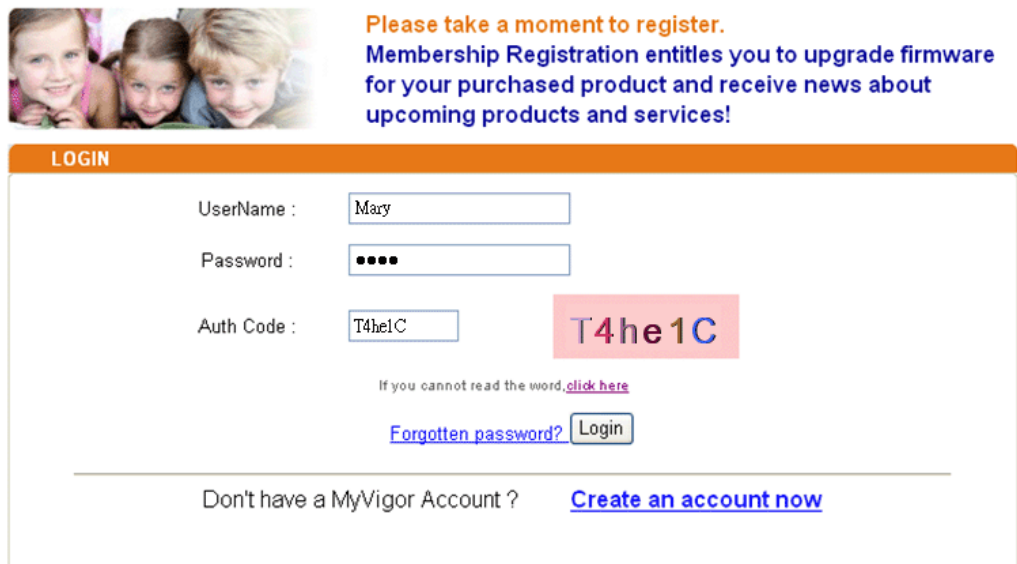
**Register** Search for this site


---

**Register Confirm**

The Confirm message of New Owner(Mary) maybe timeout  
Please try again or contact to draytek.com

8. 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)。



 **Please take a moment to register.**  
Membership Registration entitles you to upgrade firmware for your purchased product and receive news about upcoming products and services!

**LOGIN**

UserName :

Password :

Auth Code :  **T4he1C**

If you cannot read the word, [click here](#)

[Forgotten password?](#)

---

Don't have a MyVigor Account ? [Create an account now](#)

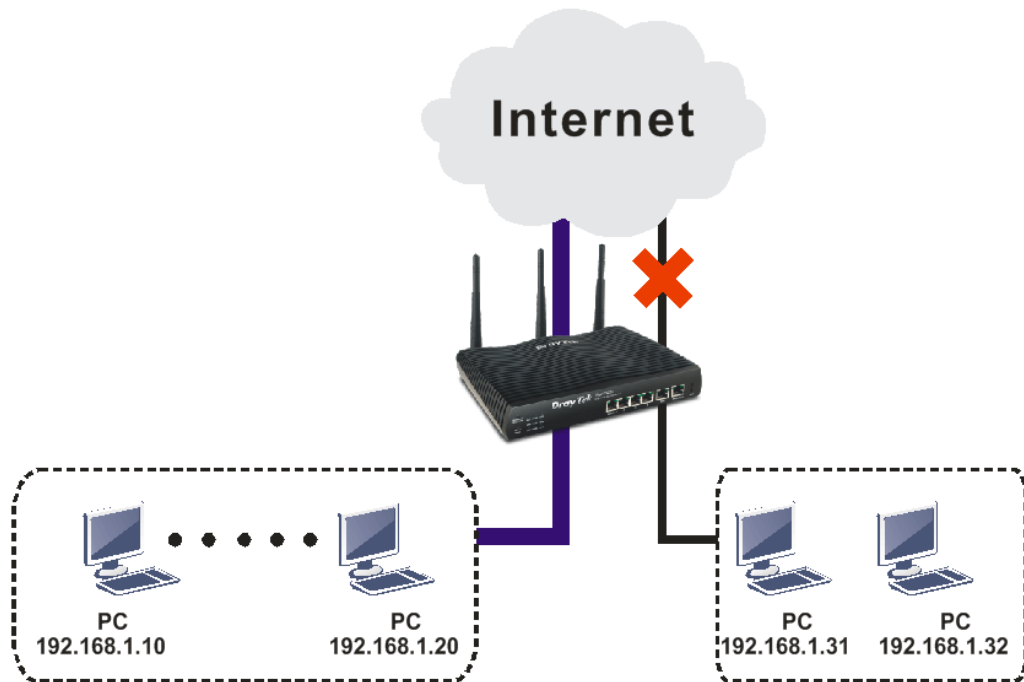
If you are having difficulty logging in, contact our customer service.  
Customer Service : (888) 3 597 2727 or

輸入驗證碼之後，按下 **Login**。系統將帶您進入 MyVigor 伺服器。



### 3.9 如何限定特定電腦存取網際網路

我們可以指定某些電腦(例如 192.168.1.10 ~ 192.168.1.20)透過 Vigor 路由器登入網際網路，其他的電腦(例如 192.168.1.31 與 192.168.1.32)只能存取區域網路內的資訊。



使用的方法是透過防火牆設定二條規則，在**防火牆>>過濾器設定**下的規則 1 設定 2 被用來當成預設值設定，我們必須從規則 2 中的設定 2 另外建立新的規則。

1. 登入路由器的網頁設定介面。
2. 開啓**防火牆>>過濾器設定**，按下**組別 2** 連結。

**防火牆 >> 過濾器設定**

**過濾器設定**

[回復出廠預設值](#)

組別	註解	組別	註解
1.	Default Call Filter	7.	
2.	Default Data Filter	8.	
3.		9.	
4.		10.	
5.		11.	
6.		12.	

- 再選擇**過濾器規則 2** 按鈕。

防火牆 >> 過濾器設定 >> 編輯過濾器設定

#### 過濾器組別 2

註解: Default Data Filter

過濾器規則	啟用	註解	上移	下移
1	<input checked="" type="checkbox"/>	xNetBios -> DNS		⌵
2	<input type="checkbox"/>		上	⌵
3	<input type="checkbox"/>		上	⌵
4	<input type="checkbox"/>		上	⌵
5	<input type="checkbox"/>		上	⌵
6	<input type="checkbox"/>		上	⌵
7	<input type="checkbox"/>		上	

下一個過濾器組別 無

確定 清除 取消

- 勾選**啟用過濾器規則**，輸入註解內容(例如 **block\_all**)，選擇**若無符合其餘規則即封鎖**作為過濾器規則，然後按下**確定**。

防火牆 >> 編輯過濾器設定 >> 編輯過濾器規則

#### 過濾器組別 2 規則 2

啟用過濾器規則

註解: block\_all

索引號碼(1-15) 於 **排程** 設置: [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ]

啟用排程時，清除連線數:  啟用

方向: LAN/DMZ/RT/VPN -> WAN

來源 IP: Any [編輯]

目的 IP: Any [編輯]

服務類型: Any [編輯]

片段: 忽略

**應用程式**

過濾器: 若無符合其餘規則即封鎖

分至其他過濾器設定: 無

連線數控制: 0 / 60000

IP 與 MAC 綁定: 不嚴格的

**Syslog**

**附註:**在預設狀態下，路由器檢查封包的順序會以組別 2，過濾器規則 2 開始依序檢查到規則 7，如果您在此選擇了**若無符合其餘規則即封鎖**作為過濾器規則，路由器的防火牆檢查封包時將會從規則 3 開始直到規則 7，封包不符合規則就會依照規則 2 的規定來處理。

- 接著，設定另一條規則，同樣開啓**防火牆>>過濾器設定**，按下**組別 2** 連結並選擇**過濾器規則 3** 的按鈕。
- 勾選**啟用過濾器規則**，輸入註解內容(例如 **open\_ip**)，按**來源 IP** 的**編輯**按鈕。

過濾器規則 2 規則 3

<input checked="" type="checkbox"/> 啟用過濾規則		
註解:	open_ip	
索引號碼(1-15) 於 排程 設置:	, , , ,	
啟用排程時，清除連線數:	<input type="checkbox"/> 啟用	
方向:	LAN/DMZ/RTWPN -> WAN	
來源 IP:	Any	編輯
目的 IP:	Any	編輯
服務類型:	Any	編輯
片段:	忽略	
<b>應用程式</b>	<b>動作設定</b>	<b>Syslog</b>
過濾器:	立刻通過	<input type="checkbox"/>
分至其他過濾器設定	無	
連線數控制	0 / 60000	<input type="checkbox"/>
IP 與 MAC 綁定	不嚴格的	<input type="checkbox"/>
服務品質	無	<input type="checkbox"/>

7. 如下的對話盒將會跳出，請選擇**位址範圍**為**位址形式**。在起始 IP 位址區域輸入 192.168.1.10，結束 IP 位址區域輸入 92.168.1.20，接著按下**確定**按鈕儲存。位於此範圍中的電腦都能登入網際網路。

**IP 位址編輯**

<b>位址形式</b>	位址範圍
起始IP位址	192.168.1.10
結束IP位址	192.168.1.20
子網路遮罩	0.0.0.0
反向選擇	<input type="checkbox"/>
<b>IP 群組</b>	無
或是 IP 群組	無
或 IP 物件	無
或 IP 物件	無
<b>IPv6 群組</b>	無
或 IPv6 群組	無
或 IPv6 物件	無
或 IPv6 物件	無

8. 現在，檢查**來源 IP**的內容是否正確，過濾器的動作/設定為**立刻通過**，接著按**確定**儲存。

防火牆 >> 編輯過濾器設定 >> 編輯過濾器規則

---

**過濾器組別 2 規則 3**

啟用過濾規則

註解: open\_ip

索引號碼(1-15)於 排程 設置:  ,  ,  ,

啟用排程時，清除連線數:  啟用

---

方向: LAN/DMZ/RT/VPN -> WAN

來源 IP: Any

目的 IP: 192.168.1.10~192.168.1.20

服務類型: Any

片段: 忽略

---

**應用程式**

過濾器: 立刻通過

分至其他過濾器設定:

連線數控制: 0 / 60000

**動作設定**

Syslog

9. 二個過濾器規則皆已設定完成，請再次按下**確定**按鈕。

防火牆 >> 過濾器設定 >> 編輯過濾器設定

過濾器組別 2

註解: Default Data Filter

過濾器規則	啟用	註解	上移	下移
1	<input checked="" type="checkbox"/>	xNetBios -> DNS		上
2	<input checked="" type="checkbox"/>	block_all	上	上
3	<input checked="" type="checkbox"/>	open_ip	上	上
4	<input type="checkbox"/>		上	上
5	<input type="checkbox"/>		上	上
6	<input type="checkbox"/>		上	上
7	<input type="checkbox"/>		上	

下一個過濾器組別 無

確定 清除 取消

10. 所有設定皆已完備，只要位在 192.168.1.10 ~ 192.168.1.20 之間的位址的電腦都可以透過路由器存取網際網路。

### 3.10 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)

- 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。

[數位內容安全管理 >> 網頁內容過濾器設定檔](#)

#### 網頁過濾器授權碼

啓動

[狀態:Commtouch] [起始日期:2013-02-25 到期日期:2013-03-27]

設定搜尋伺服器	auto-selected	<a href="#">更多</a>
設定測試伺服器	auto-selected	<a href="#">更多</a>
測試站點，檢查該站是否已被鎖類		

#### 網頁內容過濾器設定檔表格:

[回復出廠預設值](#)

設定檔	名稱	設定檔	名稱
1.	Default	5.	
2.		6.	
3.		7.	
4.		8.	

管理訊息 (最多 255 個字元)

[預設訊息](#)

快取: [L1 + L2 快取](#)

```
<body><center><br><br><br><p>The requested Web page <br> from %SIP% <br>to %URL% <br>that is categorized with %CL% <br>has been blocked by %RNAME% Web Content Filter.<p>Please contact your system administrator for further information.</center></body>
```

2. 開啓數位內容安全管理(CSM) >> 網頁內容過濾器設定檔建立新的 WCF 設定檔，請勾選社交網路，動作請選擇封鎖。

動作: 封鎖

群組

兒童防護

選擇全部

清除全部

分類

酒精與菸

仇恨與無法容忍

色情與性

校園作弊

虐待兒童圖片

犯罪活動

非法藥品

暴力

性教育

賭博

裸露

武器

粗俗不雅

休閒

選擇全部

清除全部

娛樂

旅行

遊戲

娛樂休閒

運動

時裝美容

商務

選擇全部

清除全部

商務

求職

電子信箱服務

聊天

選擇全部

清除全部

聊天

即時通訊

網際網路

選擇全部

清除全部

匿名者

下載網站

搜尋引擎、入口網站

惡意程式軟體

不合法軟體

論壇與新聞群組

影音串流下載

社交網路

殭屍網路

資訊安全

電腦

網絡釣魚及欺詐

垃圾網站

駭客

點對點

其他

廣告與文體式規章

藝術

運動

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。

防火牆 >> 基本設定

基本設定

基本設定 預設規則

預設規則之動作:

應用程式	動作設定	Syslog
過濾器	通過	<input type="checkbox"/>
連線數控制	0 / 60000	<input type="checkbox"/>
服務品質	無	<input type="checkbox"/>
負載平衡原則	自動選擇	<input type="checkbox"/>
使用者管理	無	<input type="checkbox"/>
應用程式管控	無	<input type="checkbox"/>
URL內容過濾器	無	<input type="checkbox"/>
網頁內容過濾器	無	<input type="checkbox"/>
進階設定	建立新設定 1-Default 2-social	

確定 取消

- 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

- 開啓物件設定>>關鍵字物件，按下任一索引連結以進入設定頁面。
- 在內容區域中，輸入 *facebook*，參考下圖所示。按下**確定**儲存。

物件設定 >> 關鍵字物件設定

索引編號: 1

名稱	Facebook
內容	facebook

內容限制: 最多 3 個字及 63 個字元  
字與字間以空格來區別

您可以使用%HEX來取代字元  
範例:  
內容: backdoo%72 virus keep%20out

執行結果:  
1. backdoor  
2. virus  
3. keep out

確定

清除

取消

- 開啓數位內容安全管理>>URL 內容過濾器設定檔，按下任一索引連結開啓設定頁面。
- 請按下圖所示輸入內容。



索引編號: 1

設定檔名稱:

優先權:  記錄:

**1.URL 存取控制**

啟用URL存取控制  防止透過IP位址對網站進行存取

動作:

群組/物件選項

**2.網頁特徵**

啟用限制網頁特徵

動作:   Cookie  伺服器  上傳

副檔名設定檔:

5. 完成上述設定之後，按下**確定**儲存。接著開啓**防火牆>>基本設定**。
6. 選擇**預設規則**標籤，在開啓的頁面上，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。

防火牆 >> 基本設定

基本設定

基本設定 預設規則

預設規則之動作:	動作設定	Syslog
應用程式過濾器	<input type="text" value="通過"/>	<input type="checkbox"/>
連線數控制	<input type="text" value="0 / 60000"/>	<input type="checkbox"/>
服務品質	<input type="text" value="無"/>	<input type="checkbox"/>
負載平衡原則	<input type="text" value="自動選擇"/>	<input type="checkbox"/>
使用者管理	<input type="text" value="無"/>	<input type="checkbox"/>
應用程式管控	<input type="text" value="無"/>	<input type="checkbox"/>
URL內容過濾器	<input type="text" value="1-Facebook"/>	<input type="checkbox"/>
網頁內容過濾	<input type="text" value="無"/>	<input type="checkbox"/>

進階設定

現在，使用者將無法開啓任何含有 facebook 字眼的網頁。

## B. 阻擋使用者使用 Facebook 的小遊戲

1. 開啓物件設定>>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。

物件設定 >> 關鍵字物件設定

索引編號: 2

名稱	facebook-apps
內容	apps.facebook
<b>內容限制:</b> 最多 3個 字及 63個 字元 字與字間以空格來區別	
您可以使用 %HEX 來取代字元 範例: 內容: backdoo%72 virus keep%20out	
執行結果: 1. backdoor 2. virus 3. keep out	

確定 清除 取消

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

數位內容安全管理 >> URL 內容過濾器設定檔

索引編號: 2

設定檔名稱:	face.apps		
優先權:	二者選一: URL存取控制優先	記錄:	無
<b>1.URL 存取控制</b>			
<input checked="" type="checkbox"/> 啓用URL存取控制		<input type="checkbox"/> 防止透過IP位址對網站進行存取	
動作: 封鎖		群組/物件選項 facebook..	
<b>2.網頁特徵</b>			
<input type="checkbox"/> 啓用限制網頁特徵			
動作: 通過			
<input type="checkbox"/> Cookie <input type="checkbox"/> 伺服器 <input type="checkbox"/> 上傳			
副檔名設定檔: 無			

確定 清除 取消

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

6. 選擇預設規則標籤，在開啓的頁面上，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。

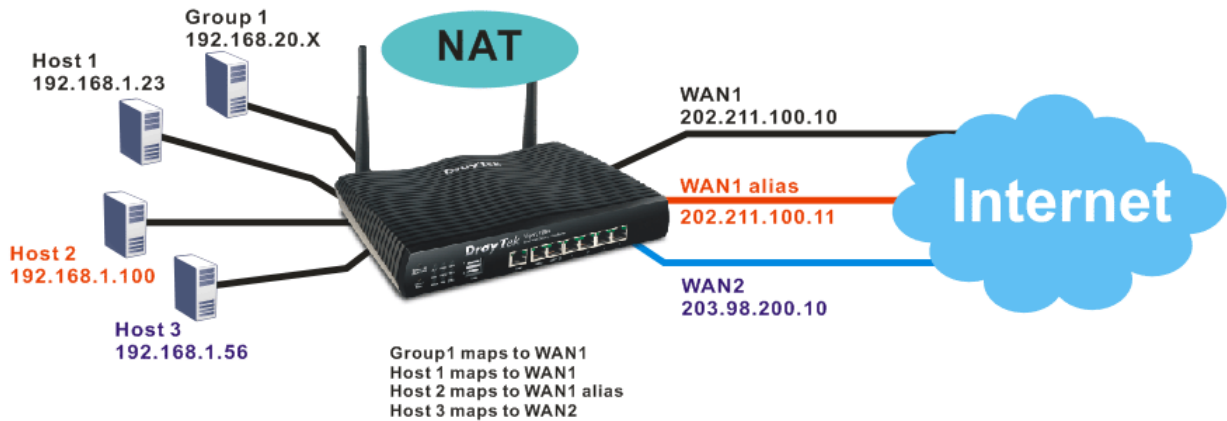
防火牆 >> 基本設定

基本設定

基本設定	預設規則	
預設規則之動作:		
應用程式	動作設定	Syslog
過濾器	通過	<input type="checkbox"/>
連線數控制	0 / 60000	<input type="checkbox"/>
服務品質	無	<input type="checkbox"/>
負載平衡原則	自動選擇	<input type="checkbox"/>
使用者管理	無	<input type="checkbox"/>
應用程式管控	無	<input type="checkbox"/>
URL 內容過濾器	2-face.apps	<input type="checkbox"/>
網頁內容過濾	無	<input type="checkbox"/>
進階設定 <input type="button" value="編輯"/>		

### 3.11 如何讓內部電腦對應到某個 WAN IP

位址對應可針對 NAT 子網內指定的虛擬 IP 或是虛擬 IP 範圍對應到特定的 WAN IP(或是 WAN IP 別名)，參考下圖範例：



假設路由器的 WAN 端設定如下：

WAN1: 202.211.100.10, WAN1 別名: 202.211.100.11

WAN2: 203.98.200.10

在沒有位址對應功能之前，當 NAT 主機含有某個 IP 位址，假設是 192.168.1.10 傳送一組封包到 WAN 端(或是網際網路)，NAT 主機的來源 IP 位址不是被對應到 202.211.100.10 就是被對應到 203.98.200.10(其 IP 或是對應功能是由內部負載平衡演算等方式來決定的)。

不過，如果是透過位址對應功能，您可以手動設定任何一台主機對應到任何 WAN 介面以符合您實際的需要。在上述的圖例中，您可以設定 NAT 主機 1 永遠對應到 202.211.100.10 (WAN1)；主機 2 則永遠對應到 202.211.100.11 (WAN1 別名 alias)；主機 3 則是永遠對應到 203.98.200.10 (WAN2)以及群組 1 永遠對應到 202.211.100.10 (WAN1)。

NAT 位址對應功能可讓您針對某個內部 IP 位址或是一組內部 IP 位址，指定對外輸出的 IP 位址。

如何使用此項功能，請看看如下的範例說明。

1. 登入路由器的網頁設定介面。
2. 開啓 **WAN >> 網際網路連線**，對於 WAN1，請選擇**固定或動態 IP** 作為**連線模式**。

#### WAN >> 網際網路連線

##### 網際網路連線

索引編號	顯示名稱	實體連線模式	連線模式	細節設定	IPv6
WAN1		乙太網路	固定或動態 IP	細節設定	IPv6
WAN2		乙太網路	無	細節設定	IPv6
WAN3		USB	固定或動態 IP	細節設定	IPv6
			PPTP/L2TP		

注意：一次僅有一個 WAN 可以支援 IPv6。

- set main WAN IP address as 202.211.100.10. 按下 WAN1 的**細節設定**，從下述開啓頁面，將主要 WAN IP 位址設定爲 202.211.100.10。

WAN >> 網際網路連線

**WAN 1**

PPPoE	固定或動態 IP	PPTP/L2TP	IPv6
<input checked="" type="radio"/> 啓用 <input type="radio"/> 停用	<b>維持 WAN 連線</b> <input type="checkbox"/> 啓用 PING 以保持常態連線 PING 到指定的 IP 位址: <input type="text"/> PING 間隔: 0 分	<b>WAN IP 網路設定</b> <span>WAN IP 別名</span> <input type="radio"/> 自動取得 IP 位址 路由器名稱: Vigor* 網域名稱: <input type="text"/> <small>*: 有些 ISP 需要此項設定名稱</small> <b>某些ISP需要 DHCP用戶端辨識碼</b> <input type="checkbox"/> 啓用 使用者名稱: <input type="text"/> 密碼: <input type="text"/>	<input checked="" type="radio"/> 指定 IP 位址 IP 位址: 202.211.100.10 子網路遮罩: 255.255.255.0 關道 IP 位址: <input type="text"/>
<b>WAN 連線偵測</b> 模式: ARP 偵測 Ping IP: <input type="text"/> TTL: <input type="text"/>	<b>MTU</b> : 1442 (最大:1500)	<input checked="" type="radio"/> 預設 MAC 位址 <input type="radio"/> 指定 MAC 位址 MAC 位址: 00 · 1D · AA · AC · 19 · C9	
<b>RIP 協定</b> <input type="checkbox"/> 啓用 RIP			

接著按下 **WAN IP 別名** 按鈕進行其他 IP 設定(如 202.211.100.11)，注意勿勾選加入 NAT IP 配置群方框，按下**確定**按鈕儲存並離開。

**WAN1 IP 別名 (多重NAT)**

索引編號	啓用	輔助 WAN IP	加入 NAT IP 配置群
1.	<input checked="" type="checkbox"/>	202.211.100.10	<input type="checkbox"/>
2.	<input checked="" type="checkbox"/>	202.211.100.11	<input type="checkbox"/>
3.	<input type="checkbox"/>	0.0.0.0	<input type="checkbox"/>
4.	<input type="checkbox"/>	0.0.0.0	<input type="checkbox"/>
5.	<input type="checkbox"/>	0.0.0.0	<input type="checkbox"/>
6.	<input type="checkbox"/>	0.0.0.0	<input type="checkbox"/>
7.	<input type="checkbox"/>	0.0.0.0	<input type="checkbox"/>
8.	<input type="checkbox"/>	0.0.0.0	<input type="checkbox"/>

4. 完成上述設定之後，開啓**負載平衡/路由策略**頁面。

**負載平衡/路由策略**

策略路由 | 回復出廠預設值 |

索引編號	啓用	協定	介面	介面位址	來源 IP 起點	來源 IP 終點	目標 IP 起點	目標 IP 終點	目標埠號起點	目標埠號終點	上下移
1	<input type="checkbox"/>	任意	WAN1	202.211.100.10							上
2	<input type="checkbox"/>	任意	WAN1	202.211.100.10							上下
3	<input type="checkbox"/>	任意	WAN1	202.211.100.10							上下
4	<input type="checkbox"/>	任意	WAN1	202.211.100.10							上下
5	<input type="checkbox"/>	任意	WAN1	202.211.100.10							上下
6	<input type="checkbox"/>	任意	WAN1	202.211.100.10							上下
7	<input type="checkbox"/>	任意	WAN1	202.211.100.10							上下
8	<input type="checkbox"/>	任意	WAN1	202.211.100.10							上下
9	<input type="checkbox"/>	任意	WAN1	202.211.100.10							上下
10	<input type="checkbox"/>	任意	WAN1	202.211.100.10							上下

<< 1-10 | 11-20 | 21-30 | 31-40 | 41-50 >> 下一頁 >>

確定

5. 按下索引編號 1 與 2 設定細節內容，分別參考下圖完成設定之後，按**確定**儲存。

**負載平衡/路由策略**

索引編號: 1

啓用

**設定原則**

協定: 任意

來源 IP:  任意  來源 IP 起點 來源 IP 終點  
192.168.1.16 ~ 192.168.1.31

目的地 IP:  任意  目標 IP 起點 目標 IP 終點

目的地埠號:  任意  目標埠號起點 目標埠號終點

**若符合上述原則，請傳往**

介面: WAN1

介面位址: 1-202.211.100.10

閘道 IP:  預設閘道  指定閘道

**更多...**

自動備援至其它 WAN

封包轉送至 WAN:  強迫 NAT  強迫路由

確定

清除

取消

以及

負載平衡/路由策略

索引編號: 2

啟用

**設定原則**

---

協定: 任意

來源 IP:  任意  
 來源 IP 起點 來源 IP 終點  
192.168.1.100 ~ 192.168.1.100

目的地 IP:  任意  
 目標 IP 起點 目標 IP 終點  
~

目的地埠號:  任意  
 目標埠號起點 目標埠號終點  
~

**若符合上述原則，請傳往**

---

介面: WAN1

介面位址: 2-202.211.100.11

閘道 IP:  預設閘道  
 指定閘道

**更多...**

自動備援至其它 WAN 封包轉送至 WAN

強迫 NAT  
 強迫路由

確定 清除 取消

6. 完成上述設定之後，您已經針對某些電腦指定了對外輸出的 IP 位址，參考下圖。

負載平衡/路由策略

策略路由 | 回復出廠預設值

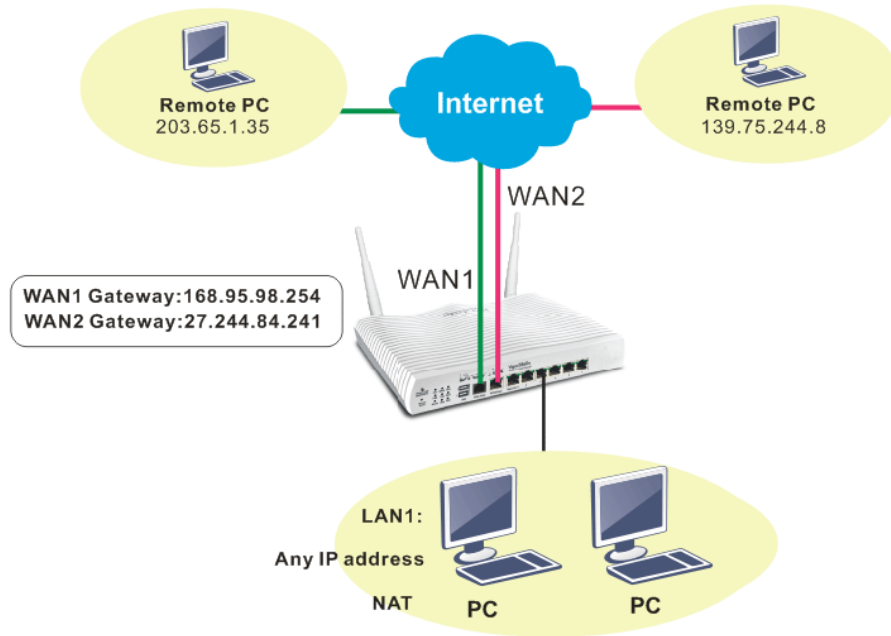
索引編號	啟用	協定	介面	介面位址	來源 IP 起點	來源 IP 終點	目標 IP 起點	目標 IP 終點	目標埠號起點	目標埠號終點	上下移
1	<input checked="" type="checkbox"/>	任意	WAN1	202.211.100.10	192.168.1.16	192.168.1.31	任意	任意	任意	任意	上下
2	<input checked="" type="checkbox"/>	任意	WAN1	202.211.100.11	192.168.1.100	192.168.1.100	任意	任意	任意	任意	上下
3	<input type="checkbox"/>	任意	WAN1	202.211.100.10							上下
4	<input type="checkbox"/>	任意	WAN1	202.211.100.10							上下
5	<input type="checkbox"/>	任意	WAN1	202.211.100.10							上下
6	<input type="checkbox"/>	任意	WAN1	202.211.100.10							上下
7	<input type="checkbox"/>	任意	WAN1	202.211.100.10							上下
8	<input type="checkbox"/>	任意	WAN1	202.211.100.10							上下
9	<input type="checkbox"/>	任意	WAN1	202.211.100.10							上下
10	<input type="checkbox"/>	任意	WAN1	202.211.100.10							上下

<< 1-10 | 11-20 | 21-30 | 31-40 | 41-50 >> 下一頁 >>

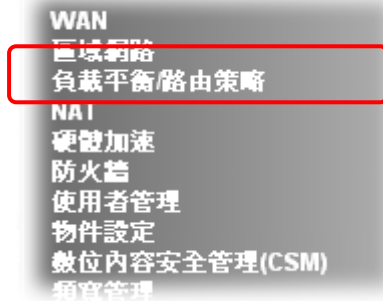
確定

### 3.12 如何設定封包負載平衡？

下圖顯示負載平衡的簡易應用，WAN1 與 WAN2 可用來登入網際網路，在 LAN1 上的電腦可以透過指定的 WAN1 介面傳送資料至遠端的電腦。



1. 登入網頁設定介面，開啓**負載平衡/路由策略**。





2. 從下圖中，請按索引編號 1。

負載平衡/路由策略

策略路由 | 回復出廠預設值 |

索引編號	啟用	協定	介面	介面位址	來源 IP 起點	來源 IP 終點	目標 IP 起點	目標 IP 終點	目標埠號起點	目標埠號終點	上下移
1	<input type="checkbox"/>	任意	WAN1	202.211.100.10							上
2	<input type="checkbox"/>	任意	WAN1	202.211.100.10							上
3	<input type="checkbox"/>	任意	WAN1	202.211.100.10							上
4	<input type="checkbox"/>	任意	WAN1	202.211.100.10							上
5	<input type="checkbox"/>	任意	WAN1	202.211.100.10							上
6	<input type="checkbox"/>	任意	WAN1	202.211.100.10							上
7	<input type="checkbox"/>	任意	WAN1	202.211.100.10							上
8	<input type="checkbox"/>	任意	WAN1	202.211.100.10							上
9	<input type="checkbox"/>	任意	WAN1	202.211.100.10							上
10	<input type="checkbox"/>	任意	WAN1	202.211.100.10							上

<< 1-10 | 11-20 | 21-30 | 31-40 | 41-50 >> >> 下一頁 >>

確定

3. 在開啓的設定頁面中，請勾選啟用，目的 IP 位址設定為 203.65.1.35；選擇 WAN1 為介面；選擇預設閘道；勿勾選自動備援至其它 WAN。

負載平衡/路由策略

索引編號: 1

啟用 設定原則

---

協定: 任意

來源 IP:  任意  
 來源 IP 起點 ~ 來源 IP 終點

目的地 IP:  任意  
 目標 IP 起點 ~ 目標 IP 終點  
 203.65.1.35 ~ 203.65.1.35

目的地埠號:  任意  
 目標埠號起點 ~ 目標埠號終點

若符合上述原則，請傳往

介面: WAN1

介面位址: 2-202.211.100.11

閘道 IP:  預設閘道  
 指定閘道

更多...

自動備援至其它 WAN

封包轉送至 WAN:  強迫 NAT  
 強迫路由

確定 清除 取消

4. 設定完畢之後，按下**確定**儲存。

**負載平衡路由策略**

策略路由 | 回復出廠預設值 |

索引編號	啟用	協定	介面	介面位址	來源 IP 起點	來源 IP 終點	目標 IP 起點	目標 IP 終點	目標埠號起點	目標埠號終點	上下移
1	<input checked="" type="checkbox"/>	任意	WAN1	202.211.100.11	任意	任意	203.65.1.35	203.65.1.35	任意	任意	上
2	<input type="checkbox"/>	任意	WAN1	202.211.100.10							上
3	<input type="checkbox"/>	任意	WAN1	202.211.100.10							上
4	<input type="checkbox"/>	任意	WAN1	202.211.100.10							上
5	<input type="checkbox"/>	任意	WAN1	202.211.100.10							上
6	<input type="checkbox"/>	任意	WAN1	202.211.100.10							上
7	<input type="checkbox"/>	任意	WAN1	202.211.100.10							上
8	<input type="checkbox"/>	任意	WAN1	202.211.100.10							上
9	<input type="checkbox"/>	任意	WAN1	202.211.100.10							上
10	<input type="checkbox"/>	任意	WAN1	202.211.100.10							上

<< 1-10 | 11-20 | 21-30 | 31-40 | 41-50 >> 下一頁 >>

確定

現在，傳送至遠端電腦(IP 位址為 203.65.1.35)的封包都會強迫透過 WAN1 來傳送。

### 3.13 如何透過使用者管理驗證用戶端

在開始設定**使用者管理**功能時，請先確認已經將模式更改為**使用者模式**(於**使用者管理 >> 基本設定**網頁下)。

**使用者管理 >> 基本設定**

**基本設定**

模式:

網頁驗證:

**注意:**

1. 使用者管理將會參考資料過濾器中可用的規則，將之視為白名單與黑名單。  
在**使用者模式**之**防火牆**
2. 符合上述清單中的使用者將不需要通過驗證。  
防火牆規則策略仍有效
3. 不符合上述清單中的使用者則需要通過**路由器**驗證。  
使用者設定檔中的**防火牆**規則仍然有效。

指定首頁 (最多 255 個字元) [上一頁](#) | [回復出廠預設值](#) |

```
<body stats=1><script language='javascript'>
window.location='http://www.draytek.com'</script></body>
```

利用**使用者管理**功能，在未提供正確的使用者帳號與密碼之前，任何一個用戶都不允許利用此路由器存取網際網路。系統提供三種驗證方式供用戶參考使用**網頁**、**Telnet** 以及**警告工具**。

**使用者管理 >> 使用者設定檔**

**索引編號 3**

啟動此帳號

使用者名稱:

密碼:

確認密碼:

閒置逾時:  分鐘, 0:無限制

最多登入使用者數目:  0:無限制

原則:  選擇項目必須同規則般建立，且不可設定為目前使用中。

記錄:

快顯瀏覽器追蹤視窗:

**驗證:**  網頁  警告工具  Telnet

禁止自具:

索引號碼(1-15) 於 **捷程** 設定:  ,  ,  ,

啟用時間額度 0 分    分

啟用資料額度 0     MB

當時間排程到期時，重新設定額度為預設值

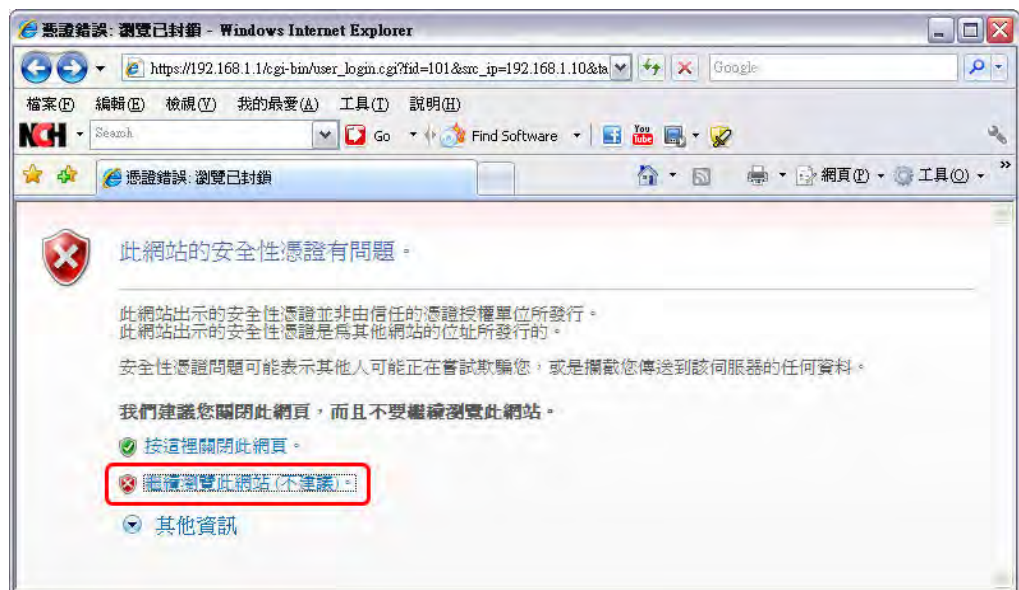
啟用 預設時間額度  分 預設資料額度  MB

## 透過網頁驗證

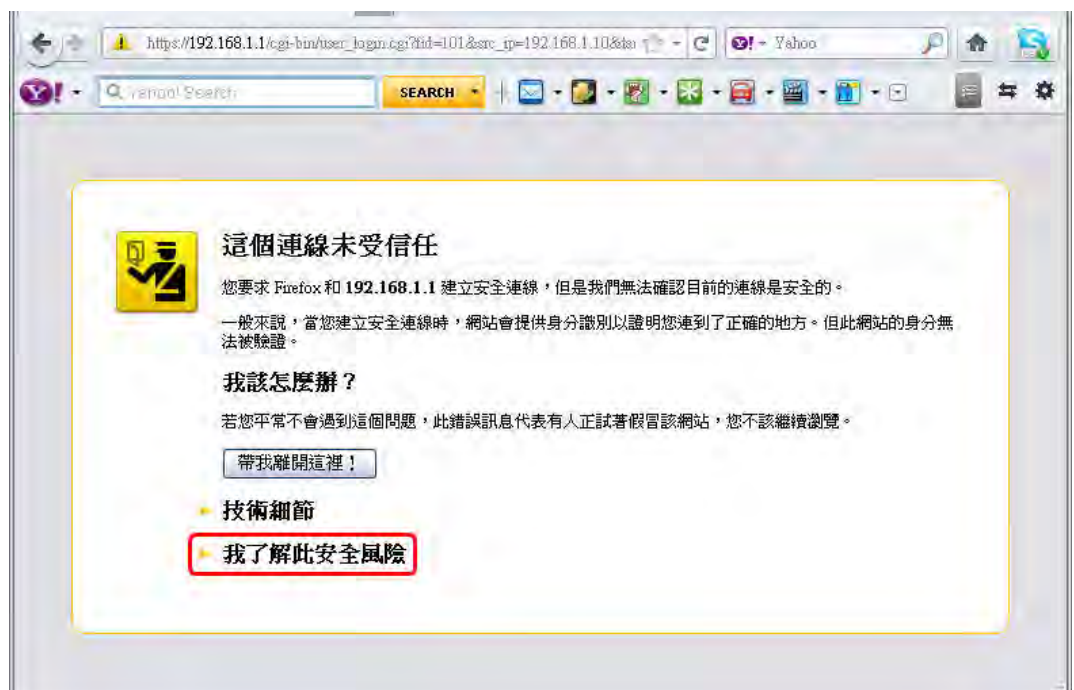
透過網頁驗證有三個層面需注意：

- 假如區域網路用戶在沒有通過驗證的情形下，利用瀏覽器開啓某個外部網站，他會被系統先導引至路由器的網頁驗證介面，用戶可能會嘗試存取 <http://www.draytek.com> 網站，但系統會他帶至路由器的驗證頁面。由於這種連線屬於 SSL 連線方式，某些網頁瀏覽器可能會在驗證頁面出現之前，先出現警告訊息。參考下述：

- 如果使用的是微軟的 Internet Explorer 瀏覽器，您看到的警告訊息顯示如下圖，請按下**繼續瀏覽此網站(不建議)**。



- 如果使用的是 Mozilla Firefox 瀏覽器，您看到的警告訊息顯示如下圖，請選擇 **我了解此安全風險**。



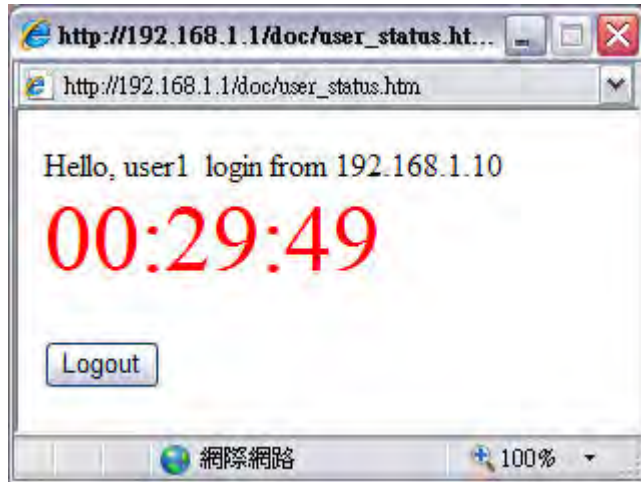
- 如果使用的是 Chrome 瀏覽器，您看到的警告訊息顯示如下圖，請按**仍要繼續**。



之後，網頁驗證視窗就會打開，請輸入您在**使用者管理**所定義的使用者名稱及密碼，然後按下**登入(Login)**。

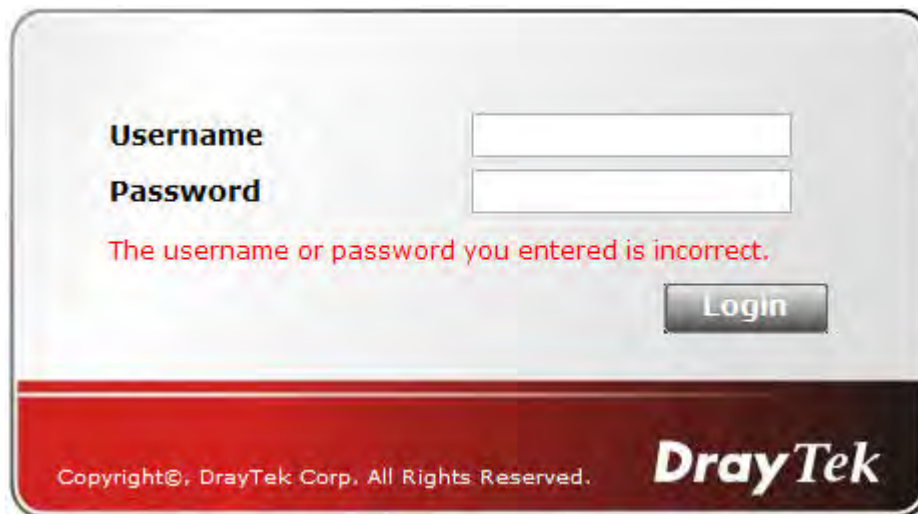


如果驗證成功，用戶即可被導引至想要進入的網站，例如本例中所說的 <http://www.draytek.com>，接著，使用者還可以看到如下圖所示的視窗，後續就可以進入網際網路瀏覽所需的網頁了。



請注意，如果您有設定不准網頁瀏覽器跳出任何視窗，這個視窗便不會正常顯示出來。

如果驗證失敗，您會看到畫面出現錯誤訊息如: **The username or password you entered is incorrect.**，請再輸入一次使用者名稱及密碼。





- 在上述說明中，您想進入外部網站因而啓動驗證程序，您也可以直接進入路由器的網頁介面進行驗證動作，HTTP 與 HTTPS 這二種協定系統都有支援，例如 <http://192.168.1.1> 或 <https://192.168.1.1>。如果您的路由器 LAN IP 位址不是 192.168.1.1，您可以替換成實際的位址，預設的管理埠號若已變更，也請在網址後面加上埠號。

若驗證成功，您可以看到**使用者管理>>基本設定**中所輸入的歡迎訊息。

**使用者管理 >> 基本設定**

**基本設定**

模式:

---

網頁驗證:

**注意:**

1. 使用者管理將會參考資料過濾器中可用的規則，將之視為白名單與黑名單。  
在使用者模式之防火牆
2. 符合上述清單中的使用者將不需要通過驗證。  
防火牆規則策略仍有效
3. 不符合上述清單中的使用者則需要通過路由器驗證。  
使用者設定檔中的防火牆規則仍然有效。

指定首頁 (最多 255 個字元) < 上一頁 | 回復出廠預設值 |

```
<body stats=1><script language='javascript'>
window.location='http://www.draytek.com'</script></body>
```

因為歡迎訊息的預設內容是 `<body stats=1><script language='javascript'>window.location='http://www.draytek.com'</script></body>` 之故，您將被導引至 <http://www.draytek.com>，如有需要，您可以更改本區的內容。例如在歡迎訊息中輸入 **Login Successful**，等下看到的歡迎訊息就會變成下圖所示的內容：



如果您沒有設定不准網頁瀏覽器跳出任何視窗，您還會看到上面所提到的跳出視窗。

- 請勿讓**使用者管理**的使用者設定檔，與 VPN 遠端撥入帳號使用者設定檔使用相同的帳號名稱(使用者名稱)，否則，您可能會收到不預期的結果，因為 VPN 遠端撥入使用者設定檔可以讓**使用者管理**中的設定檔延伸驗證之用，如果您需要更進一步的說明，可以參考**預設使用者設定檔的用法**。

當 VPN 設定檔與使用者管理帳號共享相同的使用者名稱時：

- 假設 VPN 設定檔中**啟動了 SSL Tunnel 或 SSL Web Proxy 類型**，**使用者管理(User Management)**中的設定檔就無法用來驗證，例如您建立一個使用者設定檔，帳號/密碼設定為 **chaochen/test**，而 VPN 遠端撥入帳號設定檔使用相同的使用者名稱(**chaochen**)，但密碼改設為 1234，透過網頁驗證程序，您只會收到一個錯誤訊息--**The username or password you entered is incorrect**。

VPN 與遠端存取 >> 遠端撥入使用者

索引編號 1

<b>使用者帳號與認證</b> <input checked="" type="checkbox"/> 開啟這個帳號 閒置逾時 <input type="text" value="300"/> 秒		使用者名稱 <input type="text" value="chaochen"/> 密碼(最多 19 個字元) <input type="password" value="*****"/> <input type="checkbox"/> 啟動行動動態密碼系統(mOTP) PIN 碼 <input type="text"/> 密鑰 <input type="text"/>
<b>允許的撥入模式</b> <input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPsec 通道 <input checked="" type="checkbox"/> 具有 IPsec 原型的 L2TP <input type="text" value="無"/> <input checked="" type="checkbox"/> <b>SSL 通道</b>		<b>IKE 認證方式</b> <input checked="" type="checkbox"/> 預先共用金鑰 IKE 預先共用金鑰 <input type="text"/> <input type="checkbox"/> 數位簽章(X.509) <input type="text" value="無"/>
<input type="checkbox"/> 指定遠端節點 遠端用戶 IP <input type="text"/> 或對方 ID <input type="text"/> Netbios 命名封包 <input checked="" type="radio"/> 通過 <input type="radio"/> 封鎖 經由 VPN 執行多重播送 <input type="radio"/> 通過 <input checked="" type="radio"/> 封鎖 (針對某些 IGMP,IP-Camera,DHCP Relay等而言)		<b>IPsec 安全性模式</b> <input checked="" type="checkbox"/> 中級(AH) 高級(ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES 本機 ID (視需要填入) <input type="text"/>
<b>子網路遮罩</b> <input type="text" value="LAN 1"/> <input type="checkbox"/> 指定固定 IP 位址 <input type="text" value="0.0.0.0"/>		

- 假設 VPN 設定檔中**並未啟動 SSL Tunnel 或 SSL Web Proxy 類型**，**使用者管理與 VPN 遠端撥入使用者設定檔**就能使用相同的使用者名稱 (**chaochen**)，即使密碼不同也沒關係。不過，我們仍然建議您在不同的**使用者管理**設定檔與 VPN 設定檔中，使用不同的使用者名稱(帳號)。



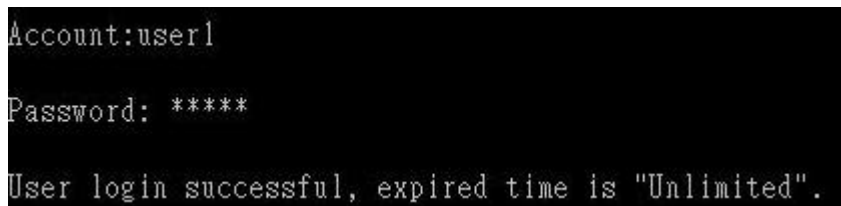
## 透過 Telnet 驗證

區域網路端的用戶也可以透過 Telnet 使用其帳戶。

1. 請利用 Telnet 打上 LAN IP 位址進入路由器 Telnet 相關頁面，輸入帳號名稱，以便執行驗證。



2. 輸入密碼執行驗證並按下 **Enter** 鍵，畫面出現 **User login successful** 以及有效時間(若有事先設定)。



**注意：**有效時間若是設定為 **Unlimited**，即表示時間定額(Time Quota)功能並未啟動，在您登入後，該帳號在未登出之前都是有效的。

3. 在路由器的網頁設定上，**時間額度**的設定畫面如下：

使用者管理 >> 使用者設定檔

索引編號 3

<input checked="" type="checkbox"/> 啟動此帳號	
使用者名稱	user1
密碼	*****
確認密碼	*****
閒置逾時	10 分鐘, 0:無限制
最多登入使用者數目	0 0:無限制
原則	預設值
記錄	無
快顯瀏覽器追蹤視窗	<input checked="" type="checkbox"/>
驗證	<input checked="" type="checkbox"/> 網頁 <input checked="" type="checkbox"/> 警告工具 <input checked="" type="checkbox"/> Telnet
指定首頁	<input type="checkbox"/>
索引號碼(1-15) 於 捷程 設定:	
<input checked="" type="checkbox"/> 啟用時間額度 10 分	+ - 10 分
<input type="checkbox"/> 啟用資料額度 0 MB	+ - 0 MB
當時間排程到期時，重新設定額度為預設值	
<input type="checkbox"/> 啟用	預設時間額度 0 分 預設資料額度 0 MB

確定 更新頁面 清除 取消

4. 如果您勾選了啓動**時間額度**並將時間設定爲 **0**，即表示該帳號沒有時間限制。

```
Account:user1
Password: *****
User's time is up, or it has not enough time quota.
```

如果**時間額度**已啓動，且設定了時間。

使用者管理 >> 使用者設定箱

索引編號 3

<input checked="" type="checkbox"/>	啓動此帳號					
使用者名稱	<input type="text" value="user1"/>					
密碼	<input type="password" value="*****"/>					
確認密碼	<input type="password" value="*****"/>					
間置逾時	<input type="text" value="10"/> 分鐘，0:無限制					
最多登入使用者數目	<input type="text" value="0"/> 0:無限制					
<b>原則</b>	<input type="text" value="預設值"/>					
	選擇項目必須同規則般建立，且不可設定為目前使用中。					
記錄	<input type="text" value="無"/>					
快顯瀏覽器追蹤視窗	<input checked="" type="checkbox"/>					
驗證	<input checked="" type="checkbox"/> 網頁 <input checked="" type="checkbox"/> 警告工具 <input checked="" type="checkbox"/> Telnet					
<b>指定首頁</b>	<input type="checkbox"/>					
索引號碼(1-15) 於 <b>排程</b> 設定:	<input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>					
<input checked="" type="checkbox"/>	啓用時間額度	40 分	<input type="button" value="+"/>	<input type="button" value="-"/>	<input type="text" value="40"/>	分
<input type="checkbox"/>	啓用資料額度	0 MB	<input type="button" value="+"/>	<input type="button" value="-"/>	<input type="text" value="0"/>	MB
當時間排程到期時，重新設定額度為預設值						
<input type="checkbox"/>	啓用	預設時間額度	<input type="text" value="0"/> 分		預設資料額度	<input type="text" value="0"/> MB

在您登入 telnet 之後即可看見時間限制。

```
Account:user1
Password: *****
User login successful, expired time is "12-23 10:21:33".
```

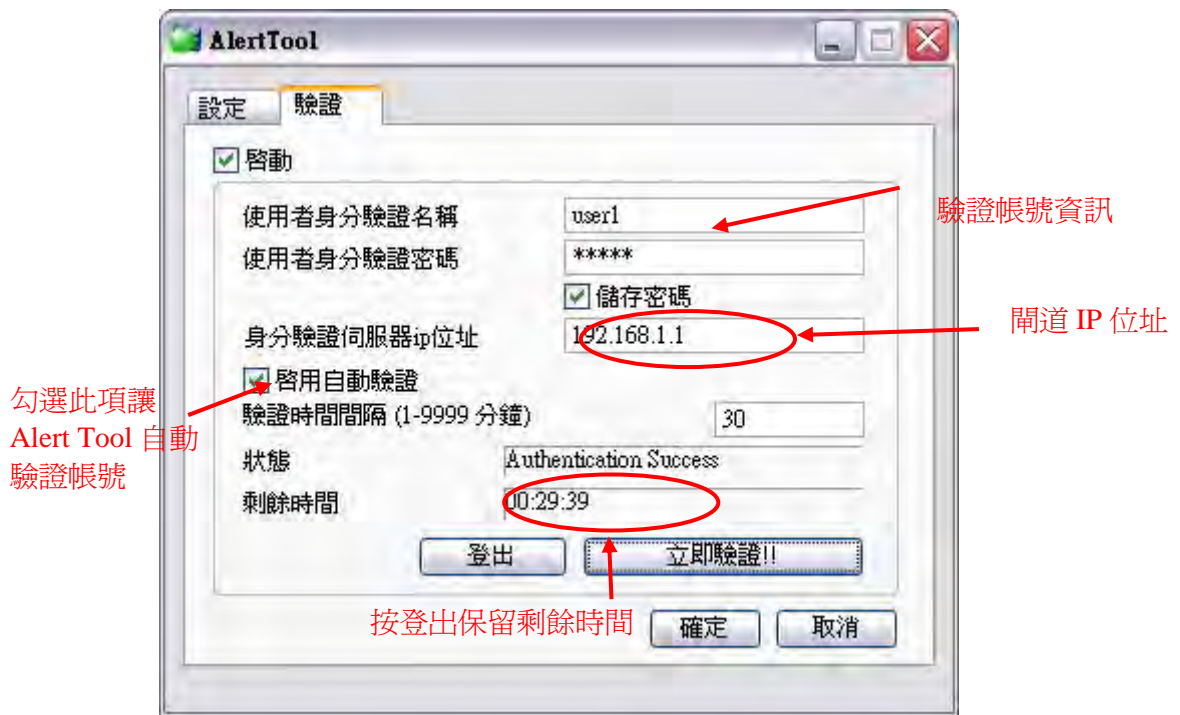
在經過系統允許的時間後，您就無法使用這個帳號了，除非讓管理者為使用者手動增加使用時間。

## 透過 VigorPro Alert Notice Tool 驗證

透過網頁或 Telnet 驗證使用者是很方便沒錯，但有些限制存在。如果利用 VigorPro Alert Notice Tool 來操作驗證程序，最大的優勢就是可以自動登入。當路由器為使用者帳號所設定的逾時時間到達時，路由器將停止用戶端電腦進入網際網路，直到該用戶再執行一次驗證程序，透過 VigorPro Alert Notice Tool 的驗證程序可以讓使用者設定重新驗證的間隔，這樣一來，工具會定期傳送驗證需求，讓用戶不必一次又一次不斷的提出驗證需求。

VigorPro Alert Notice Tool 的設定如下：

1. 按 **Authenticate Now!!** 開始執行驗證動作。



2. 請自居易官網取得 **VigorPro Alert Notice Tool** 工具：  
<http://www.draytek.com>

### 注意:

- 任何一次的防火牆策略修正都會中斷目前使用中的使用者網路連線，使用者必須重新驗證才能繼續使用網際網路。
- 管理者可以從**使用者線上狀態**檢查目前的使用者使用情形。

#### User Management >> User Online Status

Current Time : 02-22 02:00:09 Refresh Seconds: 10 Page: 1 | Refresh |

Index	Active User	IP Address	Last Login Time	Expired Time	Idle Time	Action
1	admin	192.168.1.11	02-22 01:59:21	Unlimited	Unlimited	Block Logout
2	user1	192.168.1.10	02-22 01:59:14	Unlimited	00:00:13	Block Logout

### 3.14 如何使用 DNS 過濾器

DNS 過濾器可以在 UDP 埠號 53 之下監控 DNS 的諮詢要求，且可讓 DNS 諮詢資訊傳至網頁內容過濾器(WCF)幫助分門別類 HTTPS URL 等相關網頁。

**附註：**由於 DNS 過濾器使用 WCF 服務的設定檔來過濾封包，因此必須先啓用 WCF 授權碼，否則 DNS 過濾器將無法對封包產生任何作用。

以下的範例，我們將封鎖搜尋引擎(例如 www.google.com)與社交網站(例如 https://facebook.com)。

1. 開啓數位內容安全管理>>網頁內容過濾器設定檔(CSM>>Web Content Filter Profile)設定類別，務必確定已經啓用了 WCF 授權碼。

數位內容安全管理 >> 網頁內容過濾器設定檔



網頁過濾器授權碼

啓動

[狀態:Not Activated]

設定搜尋伺服器	auto-selected	更多
設定測試伺服器	auto-selected	更多

網頁內容過濾器設定檔表格:

| 回復出廠預設值 |

設定檔	名稱	設定檔	名稱
<b>1.</b>	Default	5.	
2.		6.	
3.		7.	
4.		8.	

2. 按下索引編號設定檔 1 連結，開啓如下頁面，先停用所有的類別。然後，啓用搜尋引擎、入口網站與社交網路。

休閒  
 娛樂  遊戲  運動  
 旅行  娛樂休閒  時裝美容  
選擇全部 清除全部

商務  
 商務  求職  電子信箱服務  
選擇全部 清除全部

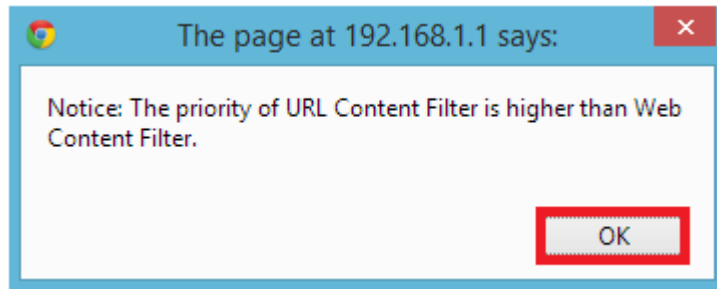
聊天  
 聊天  即時通訊  
選擇全部 清除全部

網際網路  
 匿名者  論壇與新聞群組  電腦  
 下載網站  影音串流下載  網絡釣魚及欺詐  
 搜尋引擎、入口網站  社交網路  垃圾網站  
 惡意程式軟體  殭屍網路  駭客  
選擇全部 清除全部

3. 按下**確定**儲存。



4. 以下訊息將會出現，提醒您 URL 內容過濾器的優先權高於網頁內容過濾器。您只要按下確定(OK)即可。



5. 開啓數位內容安全管理>>DNS 過濾器(CSM>>DNS Filter)，啓用 DNS 過濾器，Syslog 部分選擇封鎖；接著選擇 WCF-1 Default。

數位內容安全管理 >> DNS 過濾器

DNS 過濾器設定檔表 | 回復出廠預設值 |

設定檔	名稱	設定檔	名稱
1.		5.	
2.		6.	
3.		7.	
4.		8.	

DNS過濾器本地設定

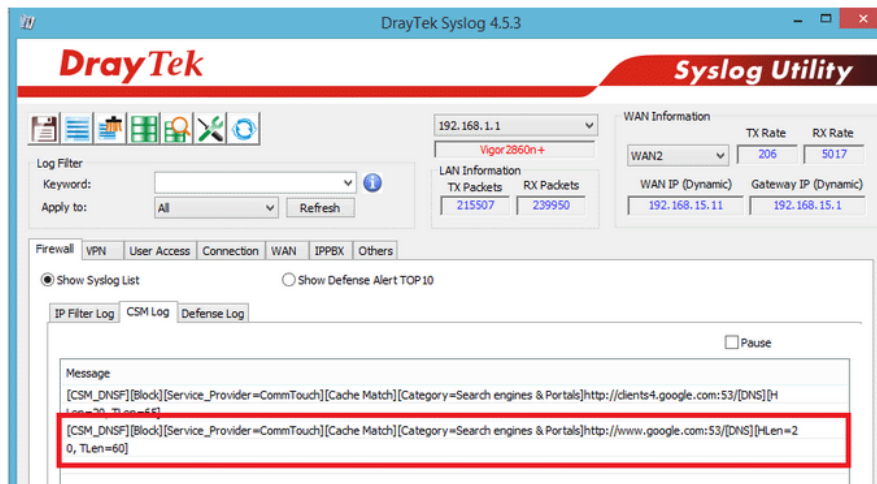
DNS 過濾器	<input checked="" type="checkbox"/> 啟用
Syslog	封鎖 ▾
WCF	WCF-1 Default ▾
UCF	無 ▾
啟用封鎖頁面	<input checked="" type="checkbox"/> 啟用

6. 按下**確定(OK)**儲存相關設定。

現在，所有關於封鎖搜尋引擎與社交網路的設定已經完成，請嘗試登入 [www.google.com](http://www.google.com) (搜尋引擎) 看看成果。



From the Syslog, we can find out “google” is blocked.



### 3.15 CVM 應用 – 如何透過 Vigor2925 管理 CPE (路由器)?

欲透過 Vigor2925 管理 CPE，您必須先設定 CPE 的 ACS URL 再設定 Vigor2925 的使用者名稱與密碼，這個範例中，我們使用 Vigor2830 系列來說明。

#### 3.15.1 設定 Vigor2925

1. 登入 Vigor2925 的網頁使用者設定介面。
2. 開啓 **VPN 中央管理>>基本設定(Central VPN Management>>General Setup)**。
3. 在如下頁面中，勾選 CVM 埠號與 CVM SSL 埠號以便啓用該埠號設定，分別輸入 CVM 埠號值、CVM SSL 埠號值、使用者名稱與密碼，請記住本頁設定的內容。

VPN 中央管理 >> 基本設定

基本設定	IPsec VPN 設定
<input checked="" type="checkbox"/>	CVM SSL 埠號: <input type="text" value="8443"/>
<input checked="" type="checkbox"/>	CVM 埠號: <input type="text" value="8000"/>
遠端連線需求之 WAN IP:	<input type="text" value="WAN1"/> / <input type="text" value="---"/>
<b>複製 下述 URL 以貼至 遠端裝置的 ACS 伺服器 URL</b>	
"http://[hostname or IP address]:8000/ACSServer/services/ACSServlet"	
"https://[hostname or IP address]:8443/ACSServer/services/ACSServlet"	
使用者名稱:	<input type="text" value="acs"/>
密碼:	<input type="password" value="*****"/>
Polling 間隔:	<input type="text" value="600"/> 秒
<b>附註:</b>	
1. 預啟用 CVM 功能，埠號必須啟用！	
2. 如果您選擇使用 CVM 埠號，介於 CVM 伺服器與 CPE 用戶之間的資料，將明文轉換且可透漏與 ISP 業者知曉。	

確定

4. 按下**確定**儲存。

### 3.15.2 設定 CPE

1. 在連接 CPE 的電腦端，開啓任一網頁瀏覽器(例如 IE, Mozilla Firefox 或 Netscape)，網址欄處輸入 **http://192.168.1.1**。
2. 開啓 **System Maintenance >> TR-069**。



3. 在 ACS Server 欄位中，請輸入 Vigor2925 的 URL (格式爲 **http://{IP address of Vigor2925}:{CVM port}/ACSServer/services/ACSServlet**)並在 Vigor2925 的 **Central VPN Management>>General Setup** 頁面中輸入與此相同的使用者名稱及密碼資訊，接著，CPE Client 項目按下 **Enable**，再按下 **OK** 儲存設定。

#### System Maintenance >> TR-069 Setting

##### ACS and CPE Settings

ACS Server On		Internet
<b>ACS Server</b>		
URL	http://172.17.1.182:9000	
Username	acs	
Password	*****	
<b>CPE Client</b>		
<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
URL	http://172.17.1.208:8069/cwm/CRN.html	
Port	8069	
Username	vigor	
Password	*****	

##### Periodic Inform Settings

<input type="radio"/> Disable	
<input checked="" type="radio"/> Enable	
Interval Time	60 second(s)

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



5. 勾選 **Allow management from the Internet** 以設定管理存取控制，按**確定**儲存。

System Maintenance >> Management

**IPv4 Management Setup** | **IPv6 Management Setup**

Router Name:

**Management Access Control**

Allow management from the Internet

FTP Server

HTTP Server

HTTPS Server

Telnet Server

SSH Server

Disable PING from the Internet

**Access List**

List	IP	Subnet Mask
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>

**Management Port Setup**

User Define Ports  Default Ports

Telnet Port:  (Default: 23)

HTTP Port:  (Default: 80)

HTTPS Port:  (Default: 443)

FTP Port:  (Default: 21)

SSH Port:  (Default: 22)

OK

6. 開啓 **WAN>>Internet Access**，在 WAN1 項目下使用 **Access Mode** 下拉式清單，選擇 **MPoA (RFC1483/2684)**模式，接著按下 **Details Page**。
7. 按下 **Specify an IP address**，輸入有關 CPE 正確的 WAN IP 位址，子網遮罩以及閘道 IP 位址，再按下 **OK** 儲存。

WAN >> Internet Access

**WAN 1**

**PPPoE / PPPoA** | **MPoA (RFC1483/2684)** | **IPv6**

Enable  Disable

**DSL Modem Settings**

Multi-PVC channel:

Encapsulation:

VPI:

VCI:

Modulation:

**WAN Connection Detection**

Mode:

Ping IP:

TTL:

**RIP Protocol**

Enable RIP

**Bridge Mode**

Enable Bridge Mode

**WAN IP Network Settings** | **WAN IP Alias**

Obtain an IP address automatically

Specify an IP address

IP Address:

Subnet Mask:

Gateway IP Address:

Router Name:

Domain Name:

\* : Required for some ISPs

Default MAC Address

Specify a MAC Address

MAC Address:

**DNS Server IP Address**

Primary IP Address:

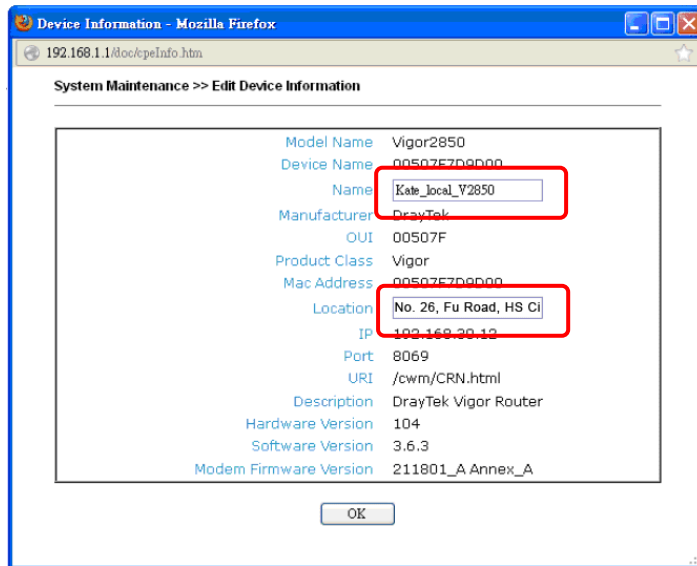
Secondary IP Address:

OK | Cancel

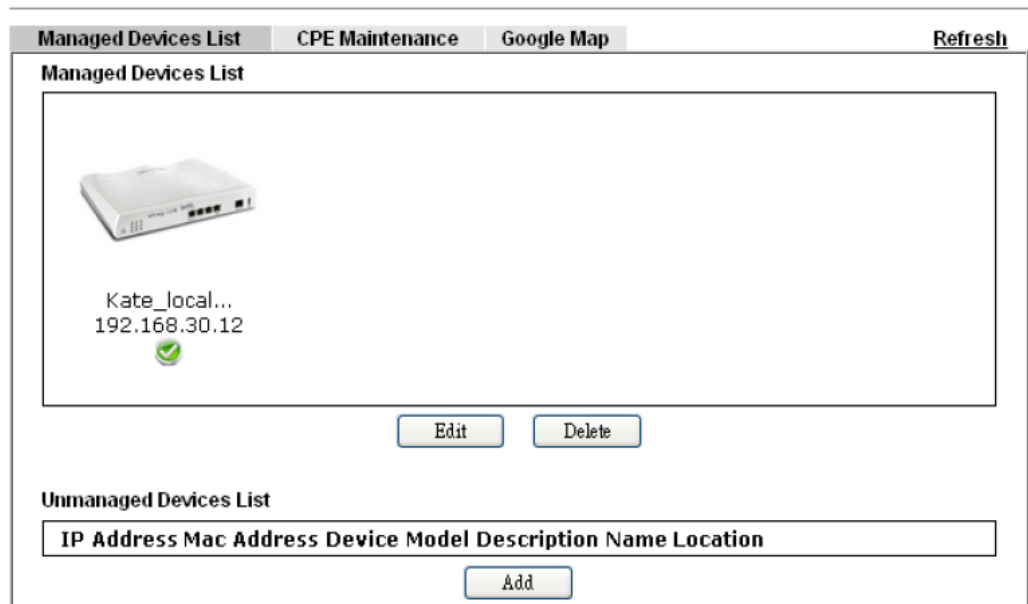
**注意：** 啓動 CPE 並重新登入 Vigor2925，已經登錄至 Vigor2925 的 CPE 將立刻由系統擷取相關資料並會顯示在 Vigor2925 網頁使用者設定介面之 **VPN 中央管理>>CPE 管理** 頁面中。

### 3.15.3 檢查 CPE 管理頁面

1. 回到 Vigor2925 的網頁使用者設定介面。
2. 開啓 **VPN 中央管理>>CPE 管理**。現在已經有一台 CPE 在 Vigor2925 的管理下。
3. 自 Unmanaged Devices List 中選擇一 CPE 並按下**新增**，下述畫面將會出現，請分別輸入路由器名稱與位置，按**確定**儲存。



4. 選定的 CPE 將可移往並顯示在 Managed Devices List 區域中，此即表示該裝置已經在 Vigor2925 的管理下。



### 3.16 CVM 應用 – 如何於 Vigor2925 與遠端設備之間建立 VPN 連線？


當遠端設備已被納入 Vigor2925 管理之下，我們可以很輕易的在這二者之間建立一條 VPN 連線。

1. 登入 Vigor2925 系列的網頁使用者設定介面。
2. 開啓 **VPN 中央管理>>CPE 管理**。

CVM >> VPN Management


---

VPN Management



CPE VPN Connection List


VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate(Bps)	Rx Pkts	Rx Rate(Bps)	Up Time

3. 按下遠端設備圖示(標示 )並按下 **PPTP** 或是 **IPsec** 按鈕。
4. 請耐心等待，如果 VPN 連線建立成功，相關資訊將會顯示在畫面下方的**已連接裝置(CPE VPN Connection List)** 區域。

CVM >> VPN Management

---

VPN Management



CPE VPN Connection List

VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate(Bps)	Rx Pkts	Rx Rate(Bps)	Up Time
1 (cvm_7D9D00)	PPTP/MPPE	192.168.30.12 via WAN2	192.168.50.1/24	805	3	1088	3	0:40:30

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

**VPN and Remote Access >> LAN to LAN**

**LAN-to-LAN Profiles:**  
View:  All  Trunk

Index	Name	Active	Status	Index	Name	Active	Status
<u>1.</u>	cvm_7D9D00	<input checked="" type="checkbox"/>	online	<u>17.</u>	???	<input type="checkbox"/>	---

↓

**Profile Index : 1**

**1. Common Settings**

Profile Name: <input type="text" value="cvm_7D9D00"/>	Call Direction: <input type="radio"/> Both <input type="radio"/> Dial-Out <input checked="" type="radio"/> Dial-in
<input checked="" type="checkbox"/> Enable this profile	<input type="checkbox"/> Always on
VPN Dial-Out Through: <input type="text" value="WAN1 First"/>	Idle Timeout: <input type="text" value="0"/> second(s)
Netbios Naming Packet: <input checked="" type="radio"/> Pass <input type="radio"/> Block	<input type="checkbox"/> Enable PING to keep alive
Multicast via VPN: <input type="radio"/> Pass <input checked="" type="radio"/> Block <small>(for some IGMP,IP-Camera,DHCP Relay..etc.)</small>	PING to the IP: <input type="text"/>

**3. Dial-In Settings**

<b>Allowed Dial-In Type</b>	Username: <input type="text" value="7D9D00"/>
<input checked="" type="checkbox"/> PPTP	Password(Max 11 char): <input type="text" value="●●●●●●"/>
<input type="checkbox"/> IPsec Tunnel	VJ Compression: <input checked="" type="radio"/> On <input type="radio"/> Off
<input type="checkbox"/> L2TP with IPsec Policy: <input type="text" value="None"/>	<b>IKE Authentication Method</b>

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

### 3.17 CVM 應用 – 如何透過 Vigor2925 更新遠端 CPE 韌體？

自居易官網下載 Vigor2925 管理下的裝置(例如 Vigor2850)最新的韌體並放置於 USB 儲存碟內。

1. 將 USB 隨身碟插入 Vigor2925 中(可透過 USB 介面)，務必確認 USB 儲存碟已正確插入，否則韌體更新將無法成功。
2. 登入 Vigor2925 的網頁設定介面，開啓 **VPN 中央管理>>CPE 維護(Central VPN Management>>CPE Management)** 並按下 **CPE 維護(CPE Maintenance)**標籤。

CVM >> CPE 管理 >> CPE 維護

受管理的裝置清單 | CPE 維護 | Google 地圖 | 更新頁面

USB 磁碟: 磁碟使用狀況: USB 儲存中斷

| 回復出廠預設值 |

索引編號	設定檔名稱	裝置名稱	動作	檔案/路徑	排程	
1.					0 0	現在
2.					0 0	現在
3.					0 0	現在
4.					0 0	現在
5.					0 0	現在
6.					0 0	現在
7.					0 0	現在
8.					0 0	現在

<< 1-8 | 9-16 >>

**附註:** 預啟用排程設定，USB 儲存槽 **必須** 插入路由器中。  
此動作加入工作序列，稍候您可以開啟 CVM >> 警告/紀錄頁面檢查運作結果。

3. 按下任一索引編號例如 1 連結。
4. 維護設定檔畫面如下顯示。

VPN 中央管理 >> CPE 管理 >> 維護設定檔

設定檔名稱:

啟用

裝置名稱:

路由器名稱:

路由器型號:

動作類型:

檔案 路徑:

索引編號 排程:

**附註:** 忽略動作與閒置逾時設定。

在設定檔名稱區中，輸入此維護設定檔名稱，勾選啟用；然後選擇**韌體更新**項目，輸入新韌體之檔案/路徑或是按選擇按鈕來挑選，指定排程設定檔，最後，按下**確定**。

- 現在您已經完成建立新的維護設定檔。

CVM >> CPE 管理 >> CPE 維護

受管理的裝置清單    CPE 維護    Google 地圖    更新頁面

USB 磁碟: 磁碟使用狀況:

| 回復出廠預設值 |

索引編號	設定檔名稱	裝置名稱	動作	檔案/路徑	排程	現在
1.	V2850	00507F7D900	Firmware Upgrade		<input type="checkbox"/> <input type="checkbox"/>	現在
2.					<input type="checkbox"/> <input type="checkbox"/>	現在
3.					<input type="checkbox"/> <input type="checkbox"/>	現在
4.					<input type="checkbox"/> <input type="checkbox"/>	現在
5.					<input type="checkbox"/> <input type="checkbox"/>	現在
6.					<input type="checkbox"/> <input type="checkbox"/>	現在
7.					<input type="checkbox"/> <input type="checkbox"/>	現在
8.					<input type="checkbox"/> <input type="checkbox"/>	現在


<< 1-8 | 9-16 >>

**附註:** 預啟用排程設定，USB 儲存槽 **必須** 插入路由器中。  
此動作加入工作序列，稍候您可以開啟 CVM >> 警告/紀錄頁面檢查運作結果。


- 按下**現在**按鈕可立即進行 Vigor2850 的韌體更新，如有需要的話。
- 請等數分鐘讓系統完成更新。
- 接著檢查裝置的相關資訊，看看韌體更新是否成功，可按下 **Managed Devices List** 標籤來檢視。

Managed Devices List    CPE Maintenance    Google Map    Refresh

**Managed Devices List**



Kate\_local...  
192.168.30.12



**Unmanaged Devices List**

IP Address	Mac Address	Device Model	Description	Name	Location
------------	-------------	--------------	-------------	------	----------

按下代表 CPE 的小圖示並按下編輯按鈕，即可檢視軟體目前的版本狀態，另一個方法是打開 **VPN 中央管理>>紀錄與警示**亦可檢查韌體更新的狀態。

### 3.18 如何在 Vigor2925 系列中搭配使用 SmartMonitor

在支援 SmartMonitor 的機種中，使用者只要將裝有 SmartMonitor 的電腦接到路由器的監控埠口便可以使用。但是 Vigor2925 系列並沒有監控埠口，因此我們必須先到 Vigor2925 的網頁設定畫面設定對應埠以便裝有 SmartMonitor 的電腦可以連接。

1. 在路由器的網頁設定頁面中，請開啓**區域網路 > LAN 埠號監控**。

區域網路 >> LAN 埠號監控

LAN 埠號監控

埠號監控：  
 啟用  停用

監控埠號：  
 P2  P3  P4  P5

被監控埠號：  
 P1  P2  P3  P4  P5

確定

2. 啓動**埠號監控**功能，請選擇**啟用**按鈕。
3. 設定**監控埠號**和**被監控埠號**。被監控埠號會將所有的封包都轉送到監控埠號。以上圖為例，若將**監控埠號**設定為 P2，而被**被監控埠號**為 P1、P3 和 P4，那麼 P1、P3 和 P4 的流量都會傳送到 P2。

LAN 埠號監控功能設定完成之後，只要將安裝了 SmartMonitor 的電腦接到設定為**監控埠號**的連接埠就可以了。

**附註：**必須注意的是被設定為**監控埠號**的連接埠將無法由 Vigor2925 取得 IP，也就是說連接到**監控埠號**的電腦將無法存取 Vigor2925 或是網際網路，而只能當做**監控電腦**來使用。

本頁留白



# 4

## 進階設定

本章將導引使用者執行完整的設定操作，有關其他的應用範例，可參考第 3 章。

1. 開啟電腦的網頁瀏覽器並輸入 **http://192.168.1.1**，螢幕將會出現使用者名稱與密碼輸入的要求對話方塊。
2. 請輸入“admin/admin”，再按**登入**。

現在主要視窗出現如下，請注意左下角會告訴您目前所使用的操作模式為何，本例中應該出現“管理者模式”。

The screenshot shows the DrayTek Vigor2925 Series web management interface. The top navigation bar includes the DrayTek logo and 'Vigor2925 Series'. The main content area is titled '儀表板' (Dashboard) and features a central status panel with indicators for Wireless LAN, ACT, WAN1, QoS, USB, WAN2, WCF, and Factory Reset. Below this, there are three tables: '系統資訊' (System Information), 'IPv4 網際網路連線設定' (IPv4 Internet Connection Settings), and '介面' (Interfaces). The '系統資訊' table lists model, version, and MAC address. The 'IPv4 網際網路連線設定' table shows WAN1-WAN4 configurations with their respective modes and MAC addresses. The '介面' table shows LAN and WLAN2.4G connection status. A '快速存取' (Quick Access) menu is located on the right side of the dashboard.

### 4.1 WAN

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

#### 4.1.1 IP 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 and 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：

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

什麼是真實 IP 位址和虛擬 IP 位址

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

### 取得 ISP 提供的真實 IP 位址

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

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

### 3G USB Modem 網路連線

由於透過基地台 3G 行動通訊越來越普遍，因而 Vigor 2925 新增了 3G 網路通訊功能。藉著連接 3G USB Modem 至 Vigor2925 的 USB 埠，路由器可支援 HSDPA/UMTS/EDGE/GPRS/GSM 以及未來 3G 標準(HSUPA, etc)，有了 3G USB Modem 的 Vigor2925n 可讓您隨時隨地接收 3G 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。使用者可以利用四個區域網路 LAN 埠連上網際網路，此外也可以透過 Vigor2925n 的 11n 無線功能存取網路資料，享受路由器強大的防火牆、頻寬管理、VPN、VoIP 等功能。



在連接上路由器後，3G 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 USB Modem 也可被視為備用裝置。因此當 WAN1 無法使用時，路由器將自動改用 3G USB Modem 以應需要。目前路由器支援哪些 3G USB Modem，可在居易網站上取得，歡迎造訪 [www.draytek.com](http://www.draytek.com)。

下圖為 WAN 的功能項目：

WAN  
基本設定  
網際網路連線  
多重 VLAN  
WAN 計量收費

## 4.1.2 基本設定

本節介紹數種網際網路的一般設定，並詳細說明 WAN1、WAN2、WAN3 與 WAN4 介面。路由器支援雙 WAN 口功能，可讓使用者存取網際網路並整合雙 WAN 口的頻寬以加速網路資料傳輸。每個 WAN 連接埠(WAN1--透過 WAN 連結埠/WAN2--透過 LAN1 連接埠)可以連接到不同的 ISP，即使 ISP 使用不同的技術提供不同的電信服務(如 DSL, Cable 數據機等等)也都沒有問題。如果任何一個 ISP 連線出了問題，全部的傳輸動作都將引導並切換至正常的 WAN 口連接埠並繼續運行。

本頁讓您分別設定 WAN1、WAN2、WAN3 與 WAN4 介面的基本資訊，在預設值中，WAN2 是停用的，如果您想要啓用該 WAN 口，點入該連結然後再選擇是即可啓用。

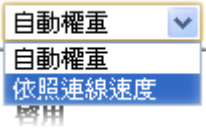
WAN >> 基本設定

負載平衡模式:

索引編號	啟用	實體模式/類型	線路速度(Kbps) 下行/上行	啟動模式
WAN1	✓	乙太網路/自動偵測傳輸速率	0 / 0	永遠連線
WAN2	✓	乙太網路/自動偵測傳輸速率	0 / 0	永遠連線
WAN3	✓	USB/-	0 / 0	永遠連線
WAN4	✓	USB/-	0 / 0	永遠連線

附註：WAN介面的線路速度設定僅在負載平衡模式選擇依照連線速度時，始可使用。

可用設定說明如下：

項目	說明
負載平衡模式	這個選項主要是對多重 WAN 設定中提供每個 WAN 口足夠的頻寬。如果您知道使用 WAN 埠口實際的頻寬，請選擇 <b>依照連線速度</b> ，否則請勾選 <b>自動權重</b> 讓系統決定最佳的負載量。 
索引編號	按下 WAN 介面連結，進入 WAN 介面設定網頁。
啟用	✓ 表示此 WAN 介面目前是啓用狀態，且可作為連線之用。
實體模式/類型	顯示此 WAN 介面的實體模式以及實體類型。
線路速度	顯示此 WAN 介面下載速率與上傳速率。
啟動模式	顯示此 WAN 介面目前是主動裝置或是備援裝置。

**注意：**預設狀態下，每個 WAN 都是啓動的。

### 乙太網路的 WAN1/WAN2 介面

WAN1/WAN2 介面的實體模式固定為乙太網路。


## WAN 1

啟用:	<input type="button" value="是"/>
顯示名稱:	<input type="text"/>
實體連線模式:	乙太網路
傳送資料模式:	<input type="button" value="自動偵測傳輸速率"/>
連線速度(Kbps):	
下行	<input type="text" value="0"/>
上行	<input type="text" value="0"/>
VLAN 標籤插入:	<input type="button" value="停用"/> (請先設定網際網路連線設定)
標籤值:	<input type="text" value="0"/> (0~4095)
優先權:	<input type="text" value="0"/> (0~7)
啟動模式:	<input type="button" value="備援"/> <input checked="" type="checkbox"/> 負載平衡: <input checked="" type="checkbox"/>
	<input type="checkbox"/> WAN 1 <input type="checkbox"/> WAN 2 <input type="checkbox"/> WAN 3
備援類型 (只有在作為多重WAN的備援情況下):	<input checked="" type="radio"/> 當任何一個 WAN 介面中斷連線時 <input type="radio"/> 當所有的 WAN 介面皆中斷連線時

附註：1.WAN介面的線路速度設定僅在負載平衡模式選擇依照連線速度時始可使用。



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/WAN2 的說明內容。
實體連線模式	顯示此 WAN 介面的實體連線模式。
傳送資料模式	您可以改變 WAN2 的傳送資料模式，或是選擇自動偵測讓系統自行處理。 
連線速度	如果您選擇依照連線速度作為負載平衡模式，請您輸入連線速度以便透過 WAN1/WAN2 介面上傳下載資料。單位是 kbps。
VLAN 標籤插入	<p><b>啟用</b> – 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。</p> <p><b>停用</b> – 停止夾帶標籤的 VLAN 設定。</p> <p><b>標籤值</b> – 輸入準備作為 VLAN ID 編號的數值，可填範圍為 0 到 4095。</p>

	<p><b>優先權</b> – 輸入此 VLAN 設定的優先權限，可選範圍從 0 到 7。</p>
<p><b>啓動模式</b></p>	<p>選擇<b>永遠連線</b>讓 WAN 連接(WAN1/WAN2)能永遠啓動運作；或是選擇<b>備援連線</b>，讓 WAN 連接在有需要時才連上線。</p> 
<p><b>備援連線</b></p>	<p>如果您選擇<b>備援</b>作為<b>啓動模式</b>，<b>備援類型</b>選項將會出現在畫面上，請指定哪個 WAN 介面要做為備援 WAN 介面。</p>  <p><b>當任何一個 WAN 介面中斷連線時</b> – 當任何一個主要的 WAN 介面突然中斷連線時，此備援 WAN 介面將會立即啓動。</p> <p><b>當所有的 WAN 介面皆中斷連線時</b> – 當所有的主要 WAN 介面都中斷連線時，此備援 WAN 介面將會立即啓動。</p> <p><b>負載平衡</b>: 勾選此方塊開啓此 WAN 介面的自動負載平衡功能。</p> <p>當資料量很大的時候，含此功能的 WAN 介面會自動將資料傳輸平均分配於所有有連線的 WAN 介面上。</p>

完成上述設定之後，請按下**確定**儲存。

## USB 的 WAN3/WAN4 介面

如果要透過 3G/4G USB 數據機來使用 3G/4G 網路連線，請設定 WAN3/WAN4 介面：


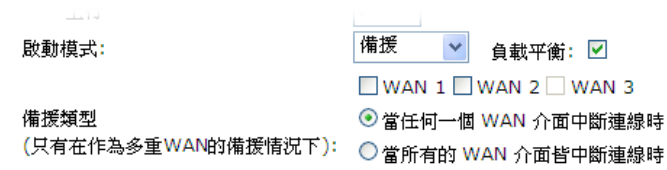
### WAN >> 基本設定

#### WAN 3

啟用:	<input type="button" value="是"/>
顯示名稱:	<input type="text"/>
實體連線模式:	USB
連線速度(Kbps):	
下行	<input type="text"/>
上行	<input type="text"/>
啟動模式:	<input type="button" value="備援"/> 負載平衡: <input checked="" type="checkbox"/>
	<input type="checkbox"/> WAN 1 <input type="checkbox"/> WAN 2 <input type="checkbox"/> WAN 3
備援類型 (只有在作為多重WAN的備援情況下):	<input checked="" type="radio"/> 當任何一個 WAN 介面中斷連線時 <input type="radio"/> 當所有的 WAN 介面皆中斷連線時

附註：1.WAN介面的線路速度設定僅在負載平衡模式選擇依照連線速度時始可使用。

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 WAN3/WAN4 的說明內容。
實體連線模式	顯示此 WAN 介面的實體連線模式。
連線速度	如果您選擇依照連線速度作為負載平衡模式，請您輸入連線速度以便透過 WAN1/WAN2 介面上傳下載資料。單位是 kbps。
啟動模式	選擇永遠連線讓 WAN 連接(WAN1/WAN2)能永遠啟動運作；或是選擇備援連線，讓 WAN 連接在有需要時才連上線。 
備援連線	如果您選擇備援作為啟動模式，備援類型選項將會出現在畫面上，請指定哪個 WAN 介面要做為備援 WAN 介面。 

當任何一個 WAN 介面中斷連線時 – 當任何一個主要



	<p>的 WAN 介面突然中斷連線時，此備援 WAN 介面將會立即啓動。</p> <p><b>當所有的 WAN 介面皆中斷連線時</b> – 當所有的主要 WAN 介面都中斷連線時，此備援 WAN 介面將會立即啓動。</p> <p><b>負載平衡:</b> 勾選此方塊開啓此 WAN 介面的自動負載平衡功能。</p> <p>當資料量很大的時候，含此功能的 WAN 介面會自動將資料傳輸平均分配於所有有連線的 WAN 介面上</p>
--	---

完成上述設定之後，請按下**確定**儲存。

### 4.1.3 網際網路連線控制

因為路由器支援雙 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/WAN2 與 WAN3/WAN4 的實體連線並不同，二者的連線模式也會有些差異。

#### WAN >> 網際網路連線

##### 網際網路連線

索引編號	顯示名稱	實體連線模式	連線模式	細節設定	IPv6
WAN1		乙太網路	無	細節設定	IPv6
WAN2		乙太網路	無	細節設定	IPv6
WAN3		USB	無 PPPoE 固定或動態 IP PPTP/L2TP	細節設定	IPv6
WAN4		USB		細節設定	IPv6

**注意:** 1. USB埠口1上的裝置套用 WAN3 設定。  
USB埠口2上的裝置套用 WAN4 設定。

**進階** 您可在此設定 DHCP 用戶端選項

與

#### WAN >> 網際網路連線

##### 網際網路連線

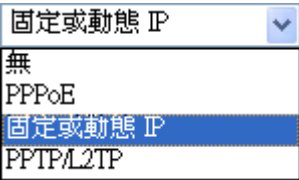
索引編號	顯示名稱	實體連線模式	連線模式	細節設定	IPv6
WAN1		乙太網路	無	細節設定	IPv6
WAN2		乙太網路	無	細節設定	IPv6
WAN3		USB	無	細節設定	IPv6
WAN4		USB	無 3G/4G USB 數據機(PPP 模式) 3G/4G USB 數據機 (DHCP模式)	細節設定	IPv6

**注意:** 1. USB埠口1上的裝置套用 WAN3 設定。  
USB埠口2上的裝置套用 WAN4 設定。

**進階** 您可在此設定 DHCP 用戶端選項

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 WAN1/WAN2/WAN3/WAN4 於一般設定中所輸入的名稱。										
實體連線模式	按照實際網路連線狀況來顯示 WAN1/WAN2 (乙太網路) / WAN3(3G USB 模式) 實體連線。										
連線模式	<p>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<b>細節設定</b>以設定詳細內容。</p>  <p>網頁提供數種網際網路連線模式。</p>										
細節設定	此按鈕將依照您在 WAN1/WAN2/WAN3 所選擇的連線模式展現不同的網頁內容。										
IPv6	<p>此按鈕將會開啓不同的網頁(以實體連線模式為基準)，針對 WAN 介面設定 IPv6 網際網路存取模式。</p> <p>如果在 WAN 介面中 IPv6 已經啓動了，那麼您可以在網頁上看到綠色的 IPv6 字樣。</p>										
進階(Advanced)	<p>讓您設定 DHCP Client Option 內容，此功能若是啓用，DHCP 封包可以另外加上 option 號碼以及數據資訊作加密處理。</p> <div data-bbox="710 1115 1398 1630" style="border: 1px solid black; padding: 5px;"> <p>WAN &gt;&gt; Internet Access</p> <p>DHCP Client Options Status</p> <table border="1" data-bbox="715 1176 1393 1332"> <thead> <tr> <th>Enable</th> <th>Interface</th> <th>Option</th> <th>Type</th> <th>Data</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table> <p>Enable: <input checked="" type="checkbox"/></p> <p>Interface: <input type="checkbox"/> All <input checked="" type="checkbox"/> WAN1 <input type="checkbox"/> WAN2 <input type="checkbox"/> WAN3 <input type="checkbox"/> WAN4 <input type="checkbox"/> WAN5 <input type="checkbox"/> WAN6 <input type="checkbox"/> WAN7</p> <p>Option Number: <input type="text"/></p> <p>DataType: <input checked="" type="radio"/> ASCII Character (EX: Option:18, Data:/path) <input type="radio"/> Hexadecimal Digit (EX: Option:18, Data:2f70617468) <input type="radio"/> Address List (EX: Option:44, Data:172.16.2.10,172.16.2.20...)</p> <p>Data: <input type="text"/></p> <p style="text-align: right;"><input type="button" value="Add"/> <input type="button" value="Update"/> <input type="button" value="Delete"/></p> <p><small>Note: Option 61 has been given a default value. You can configure option 61(Client Identifier) in "WAN &gt;&gt; Interface Access" page. If you choose to configure option 61 here, the settings in "WAN &gt;&gt; Interface Access,Details Page" will be overwritten. Option 12 is reserved, you cannot configure it here but you can configure it in "Router Name" field of "WAN &gt;&gt; Interface Access".</small></p> <p style="text-align: center;"><input type="button" value="OK"/></p> </div> <p><b>啓用/停用(Enable/Disable)</b> – 勾選啓用(Enable)方塊啓用 DHCP Option 功能。每個 DHCP option 都是由號碼與數據組合而成。例如</p> <p style="padding-left: 40px;">Option number:100</p> <p style="padding-left: 40px;">Data: abcd</p> <p>當功能啓用之後，即可在 DHCP 回覆封包上看見指定數值。</p> <p><b>介面(Interface)</b> – 指定將要套用 DHCP Option 設定的 WAN 介面，其中 WAN5 ~ WAN7 指的是存在于</p>	Enable	Interface	Option	Type	Data	<input type="checkbox"/>				
Enable	Interface	Option	Type	Data							
<input type="checkbox"/>											



WAN>>Multi-VLAN 中的介面。

選項號碼(Option Number) –請輸入號碼。

附註：如果您選擇設定 Option 61，那麼在頁面上所設定的相關資訊將據此改寫。

資料類型(Data Type) – 選擇儲存數據的類型 (ASCII, 16 進位或是 IP 位址。)

資料(Data) –輸入 DHCP option 功能所能處理的數據之實際內容。

## WAN1/WAN2 中的 PPPoE 模式細節設定

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，接著在 WAN1 中選擇 PPPoE 模式，下面的細節設定網頁將會出現。


WAN >>網際網路連線

WAN 1

PPPoE	固定或動態 IP	PPTP/L2TP	IPv6
<input type="radio"/> 啟用 <input checked="" type="radio"/> 停用			
<b>ISP 存取設定</b> 使用者名稱 <input type="text"/> 密碼 <input type="text"/> 索引號碼(1-15) 於 <b>排程</b> 設定： => <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>		<b>PPP/MP 設定</b> PPP 驗證 <input type="text" value="PAP或CHAP"/> 閒置逾時 <input type="text" value="-1"/> 秒 <b>IP 位址指派方式 (IPCP)</b> <input type="text" value="WAN IP別名"/> 固定 IP: <input type="radio"/> 是 <input checked="" type="radio"/> 否 (動態IP) 固定 IP 位址 <input type="text"/>	
<b>WAN 連線偵測</b> 模式 <input type="text" value="ARP 偵測"/> Ping IP <input type="text"/> TTL: <input type="text"/>		<input checked="" type="radio"/> 預設 MAC 位址 <input type="radio"/> 指定 MAC 位址 MAC 位址: <input type="text" value="00"/> . <input type="text" value="1D"/> . <input type="text" value="AA"/> : <input type="text" value="AC"/> . <input type="text" value="1A"/> . <input type="text" value="39"/>	
MTU <input type="text" value="1442"/> (最大:1492)			

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。 <b>使用者名稱</b> –在本區請輸入 ISP 提供的使用者名稱。 <b>密碼</b> – 在本區請輸入 ISP 提供的密碼。 <b>索引號碼(1-15) 於排程設定</b> -可以輸入四組時間排程，全部的排程都是在 <b>其他應用&gt;&gt;排程</b> 網頁中事先設定完畢，您可在此輸入該排程的索引編號。

<p><b>WAN 連線檢測</b></p>	<p>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。</p> <p>模式 – 選擇 <b>ARP Detect</b> 或 <b>Ping Detect</b> 執行 WAN 檢測動作。</p> <p><b>Ping IP</b> – 如果您選擇 <b>Ping Detect</b> 作為檢測模式，您必須在本區輸入 IP 位址作為 Ping 檢測之用。</p> <p><b>TTL (Time to Live)</b> – 顯示數值供您參考，TTL 數值是利用 Telnet 指令始可設定。</p>
<p><b>MTU</b></p>	<p>代表封包的最大傳輸單位，預設值為 1442。</p>
<p><b>PPP/MP 設定</b></p>	<p><b>PPP 驗證</b> – 選擇 <b>PAP</b> 或是 <b>PAP</b> 或 <b>CHAP</b>。如果您想要永遠連接網際網路，請勾選<b>永遠連線</b>。</p> <p><b>閒置逾時</b> – 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。</p>
<p><b>IP 位址指派方式 (IPCP)</b></p>	<p>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。</p> <p><b>WAN IP 別名</b> - 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。</p>  <p><b>固定 IP 位址</b> – 按是是使用此功能並輸入一個固定的 IP 位址。</p> <p><b>預設 MAC 位址</b> – 您可以使用預設 MAC 位址或是在此區域中填入另一組位址。</p> <p><b>指定 MAC 位址</b> – 手動輸入路由器的 MAC 位址。</p>

在您完成上述的設定之後，請按**確定**按鈕來啟動設定。

## WAN1/WAN2 中的固定或動態 IP 模式細節設定

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**固定或動態 IP** 為網際網路的連線協定，請自 WAN 中選擇**網際網路連線**，接著選擇**固定或動態 IP**，即可出現下圖。

### WAN >> 網際網路連線

**WAN 1**

PPPoE	固定或動態 IP	PPTP/L2TP	IPv6
<input type="radio"/> 啟用 <input checked="" type="radio"/> 停用	<p><b>維持 WAN 連線</b></p> <input type="checkbox"/> 啟用 PING 以保持常態連線 PING 到指定的 IP 位址 <input type="text"/> PING 間隔 <input type="text" value="0"/> 分	<p><b>WAN IP 網路設定</b> <span>WAN IP 別名</span></p> <input type="radio"/> 自動取得 IP 位址 路由器名稱 <input type="text" value="Vigor"/> * 網域名稱 <input type="text"/> * * : 有些 ISP 需要此項設定名稱 <b>某些ISP需要 DHCP用戶端辨識碼</b> <input type="checkbox"/> 啟用 使用者名稱 <input type="text"/> 密碼 <input type="text"/> <input checked="" type="radio"/> 指定 IP 位址 IP 位址 <input type="text"/> 子網路遮罩 <input type="text"/> 關道 IP 位址 <input type="text"/>	
	<p><b>WAN 連線偵測</b></p> 模式 <input type="text" value="ARP 偵測"/> Ping IP <input type="text"/> TTL: <input type="text"/>	<input checked="" type="radio"/> 預設 MAC 位址 <input type="radio"/> 指定 MAC 位址 MAC 位址: <input type="text" value="00"/> <input type="text" value="1D"/> <input type="text" value="AA"/> <input type="text" value="AC"/> <input type="text" value="19"/> <input type="text" value="C9"/>	
	<p><b>MTU</b></p> <input type="text" value="1442"/> (最大:1500)	<p><b>DNS 伺服器 IP 位址</b></p> 主要 IP 位址 <input type="text" value="8.8.8.8"/> 次要 IP 位址 <input type="text" value="8.8.4.4"/>	
	<p><b>RIP 協定</b></p> <input type="checkbox"/> 啟用 RIP		

附註：當啟用了硬體加速時，系統支援的最大MTU設定值為1496。

確定

取消

可用設定說明如下：

項目	說明
啟用/停用	按下 <b>啟用</b> 按鈕可啟動此功能，如果您選的是 <b>停用</b> ，此項功能將會關閉，全部調整過的設定也都將立即失效。
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 <b>啟用 PING 以保持常態連線</b> 。 <b>PING 到指定的 IP</b> - 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 <b>PING 間隔</b> - 輸入間隔時間讓系統得以執行 PING 動作。
WAN 連線檢測	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。

	<p>模式 – 選擇 <b>ARP Detect</b> 或 <b>Ping Detect</b> 執行 WAN 檢測動作。</p> <p><b>Ping IP</b> – 如果您選擇 <b>Ping Detect</b> 作為檢測模式，您必須在本區輸入 IP 位址作為 Ping 檢測之用。</p> <p><b>TTL (Time to Live)</b> – 顯示數值供您參考，TTL 數值是利用 Telnet 指令始可設定。</p>
<b>MTU</b>	代表封包的最大傳輸單位，預設值為 1442。
<b>RIP 協定</b>	指名路由器是如何變更路由表格資訊，勾選此項目以啟動此功能。
<b>WAN IP 網路設定</b>	<p>這個區域允許您自動取得 IP 位址並讓您手動輸入 IP 位址。</p> <p><b>WAN IP 別名</b> - 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，要注意的是，本項設定僅針對 WAN1 有效用。</p> <p><b>自動取得 IP 位址</b> – 如果您想要使用<b>動態 IP</b> 模式，按此鈕以自動取得 IP 位址。</p> <ul style="list-style-type: none"> <li>● <b>路由器名稱:</b> 輸入 ISP 的路由器名稱。</li> <li>● <b>網域功能變數名稱:</b> 輸入指定的網域功能變數名稱。</li> </ul> <p><b>某些 ISP 需要 DHCP 用戶端辨識碼</b></p> <ul style="list-style-type: none"> <li>● <b>啟用:</b>勾選此方塊，指定使用者名稱與密碼作為 DHCP 用戶端的辨識依據。</li> <li>● <b>使用者名稱:</b> 輸入任何名稱，最大長度不要超過 63 個字元。</li> <li>● <b>密碼:</b> 輸入任何密碼，最大長度不要超過 62 個字元。</li> </ul> <p><b>指定 IP 位址</b> – 按此鈕指定 IP 位址讓資料通過。</p> <ul style="list-style-type: none"> <li>● <b>IP 位址:</b>輸入 IP 位址。</li> <li>● <b>子網路遮罩:</b>輸入子網路遮罩。</li> <li>● <b>閘道 IP 位址:</b> 輸入閘道 IP 位址。</li> </ul> <p><b>預設 MAC 位址:</b> 按此鈕使用預設的 MAC 位址。</p> <p><b>指定 MAC 位址:</b> 部分 Cable 服務供應商會指定 MAC 位址作為存取驗證之用，此時您需要按下此鈕並在下方區域輸入 MAC 位址。</p>
<b>DNS 伺服器 IP 位址</b>	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。

在您完成上述的設定之後，請按**確定**按鈕來啟動設定。

## WAN1/WAN2 中的 PPTP/L2TP 模式細節設定

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，接著選擇 PPTP/L2TP，即可出現下圖。

WAN >> 網際網路連線

WAN 1

PPPoE	固定或動態 IP	PPTP/L2TP	IPv6
<input type="radio"/> 啟用 PPTP <input type="radio"/> 啟用 L2TP <input checked="" type="radio"/> 停用 伺服器位址 <input type="text"/> 指定閘道 IP 位址 <input type="text" value="172.16.3.1"/>		<b>PPP 設定</b> PPP 驗證 <input type="text" value="PAP 或 CHAP"/> 閒置逾時 <input type="text" value="-1"/> 秒 <b>IP 位址指派方式 (IPCP)</b> <input type="text" value="WAN IP 別名"/> 固定 IP: <input type="radio"/> 是 <input checked="" type="radio"/> 否 (動態 IP) 固定 IP 位址 <input type="text"/> <b>WAN IP 網路設定</b> <input type="radio"/> 自動取得 IP 位址 <input checked="" type="radio"/> 指定 IP 位址 IP 位址 <input type="text" value="172.16.3.130"/> 子網路遮罩 <input type="text" value="255.255.255.0"/>	
<b>ISP 存取設定</b> 使用者名稱 <input type="text"/> 密碼 <input type="text"/> 索引號碼(1-15) 於 排程 設定: => <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>			
MTU <input type="text" value="1442"/> (最大:1460)			

可用設定說明如下：

項目	說明
啟用/停用	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 PPTP/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。 索引號碼 (1-15) 於排程設定 - 您可以輸入四組時間排程設定，所有的排程都是在時間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，預設值為 1442。
PPP 設定	PPP 驗證 - 選擇 PAP 或是 PAP 或 CHAP。 閒置逾時 - 閒置逾時表示路由器在一段時間內都沒有運作時，就會中斷連線。

## IP 位址指派方式 (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，要注意的是，本項設定僅針對 WAN1 有效用。



**固定 IP** - 通常每一次您要求連線時，ISP 會浮動指定 IP 位址給您使用，但在某些情況下，ISP 總是提供相同的 IP 位址予您，因此您可以在固定 IP 位址區域中輸入此 IP 位址，在您輸入並使用此項功能之前，請先聯絡您的 ISP 業者取得相關資訊，再選擇是並輸入固定 IP 位址以便使用。

**固定 IP 位址** - 請輸入固定 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。
- **子網路遮罩** - 輸入子網路遮罩。

在您完成上述的設定之後，請按**確定**按鈕來啟動設定。

## WAN3/WAN4 的 3G/4G USB 數據機(PPP 模式)細節設定

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，接著在 WAN2 介面上選擇 3G/4G USB 數據機(PPP 模式)，即可出現下圖。

WAN >> 網際網路連線

### WAN 3

<b>3G/4G USB數據機 (PPP 模式)</b>		<input type="radio"/> 啟用 <input checked="" type="radio"/> 停用
SIM PIN 碼	<input type="text"/>	
數據機初始化字串	<input type="text" value="AT&amp;FE0V1X1&amp;D2&amp;C1S0=0"/>	(預設值:AT&FE0V1X1&D2&C1S0=0)
APN 名稱	<input type="text"/>	<input type="button" value="套用"/>
數據機初始化字串 2	<input type="text" value="AT"/>	
數據機撥號字串	<input type="text" value="ATDT*99#"/>	(預設值:ATDT*99#, CDMA:ATDT#777, TD-SCDMA:ATDT*98*1#)
PPP 使用者	<input type="text"/>	(視需要填入)
PPP 密碼	<input type="text"/>	(視需要填入)
PPP 驗證	<input type="text" value="PAP 或 CHAP"/>	
索引號碼(1-15) 於 <b>排程</b> 設定:		
=> <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>		
<b>WAN 連線偵測</b>		
模式	<input type="text" value="ARP 檢測"/>	
Ping IP	<input type="text"/>	
TTL:	<input type="text"/>	

可用設定說明如下：

項目	說明
<b>3G /4G USB 數據機 (PPP 模式)</b>	選擇啟用，開啓此功能。如果您選的是 <b>停用</b> ，此功能將不再運作，所有設定也都會失效。
<b>SIM PIN 碼</b>	輸入 SIM 卡 PIN 碼，以便連線網際網路。
<b>數據機初始化字串</b>	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。
<b>APN 名稱</b>	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 <b>套用</b> 即可。
<b>數據機初始化字串 2</b>	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。
PPP 使用者	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 <b>PAP</b> 或是 <b>PAP 或 CHAP</b> 。
索引號碼(1-15)	可以輸入四組時間排程，全部的排程都是在 <b>其他應用&gt;&gt;排程</b> 網頁中事先設定完畢，您可在此輸入該排程的索引編號。
WAN 連線檢測	<p>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。</p> <p><b>模式</b> – 選擇 <b>ARP Detect</b> 或 <b>Ping Detect</b> 執行 WAN 檢測動作。</p> <p><b>Ping IP</b> – 如果您選擇 <b>Ping Detect</b> 作為檢測模式，您必須在本區輸入 IP 位址作為 Ping 檢測之用。</p> <p><b>TTL (Time to Live)</b> – 顯示數值供您參考，TTL 數值是利用 Telnet 指令始可設定。</p>

在您完成上述的設定之後，請按**確定**按鈕來啟動設定。

### WAN3/WAN4 的 3G/4G USB 數據機(DHCP 模式)細節設定

欲使用 3G/4G USB 數據機(DHCP 模式)作為網際網路的存取協定，請開啓 **WAN>>網際網路連線**，然後自 WAN3/WAN4 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：

WAN >> 網際網路連線 

---

WAN 4

3G/4G USB 數據機 (PPP 模式)    3G/4G USB數據機 (DHCP 模式)    IPv6

| 數據機支援清單 |

**3G/4G USB數據機 (DHCP 模式)**     啟用     停用

SIM PIN 碼   

網路連線模式    4G/3G/2G  (預設值: 4G/3G/2G)

APN 名稱   

MTU     (預設值: 1380)

LTE 軟體版本    ---

LTE 硬體版本    ---

---

**WAN 連線偵測**

模式     ARP 偵測


附註: 請注意，某些例子當中，USB埠口連線會被暫時中止以便啟動新的設定。

可用設定說明如下：

項目	說明
數據機支援清單	列出此路由器支援的數據機清單。



	 <p>3G/4G 數據機支援列表(DHCP模式)</p> <p>下述相容性測試，列出在特殊環境或是國家中，Vigor 路由器支援的3.5G/LTE數據機。如果您擁有的 LTE 數據機在清單上，但無法正常運作，請逕寄信至 support@draytek.com 或是與經銷商聯絡。</p> <table border="1"> <thead> <tr> <th>品牌</th> <th>機型</th> <th>LTE</th> <th>狀態</th> </tr> </thead> <tbody> <tr> <td>Alcatel</td> <td>Alcatel L100V</td> <td>✔</td> <td>Y</td> </tr> <tr> <td>Alcatel</td> <td>Alcatel L800</td> <td>✔</td> <td>Y</td> </tr> <tr> <td>Alcatel</td> <td>Alcatel W100</td> <td>✔</td> <td>Y</td> </tr> <tr> <td>Alcatel</td> <td>Alcatel W800</td> <td>✔</td> <td>M</td> </tr> <tr> <td>Huawei</td> <td>Huawei E303</td> <td></td> <td>Y</td> </tr> <tr> <td>Huawei</td> <td>Huawei E3131</td> <td></td> <td>Y</td> </tr> </tbody> </table>	品牌	機型	LTE	狀態	Alcatel	Alcatel L100V	✔	Y	Alcatel	Alcatel L800	✔	Y	Alcatel	Alcatel W100	✔	Y	Alcatel	Alcatel W800	✔	M	Huawei	Huawei E303		Y	Huawei	Huawei E3131		Y
品牌	機型	LTE	狀態																										
Alcatel	Alcatel L100V	✔	Y																										
Alcatel	Alcatel L800	✔	Y																										
Alcatel	Alcatel W100	✔	Y																										
Alcatel	Alcatel W800	✔	M																										
Huawei	Huawei E303		Y																										
Huawei	Huawei E3131		Y																										
<b>3G/4G USB 數據機 (DHCP 模式)</b>	按 <b>啟用</b> 啟動此功能，如果您選擇 <b>停用</b> ，此功能將會關閉，所有本頁的設定也將立即失效。																												
<b>SIM PIN 碼</b>	輸入 SIM 卡 PIN 碼，以便連線網際網路。																												
<b>網路連線模式</b>	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。																												
<b>APN 名稱</b>	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 <b>套用</b> 即可。																												
<b>MTU</b>	代表封包的最大傳輸單位。																												
<b>WAN 連線偵測</b>	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。 <b>模式</b> – 選擇 <b>ARP Detect</b> 或 <b>Ping Detect</b> 執行 WAN 檢測動作。 <b>Ping IP</b> – 如果您選擇 <b>Ping Detect</b> 作為檢測模式，您必須在本區輸入 IP 位址作為 Ping 檢測之用。 <b>TTL (Time to Live)</b> – 顯示數值供您參考，TTL 數值是利用 Telnet 指令始可設定。																												

在您完成上述的設定之後，請按**確定**按鈕來啟動設定。

## WAN1/WAN2/WAN3/WAN4 的斷線模式細節設定(IPv6)

當選擇斷線時，IPv6 連線是中斷的。

WAN >> 網際網路連線設定

WAN 1

PPPoE	固定或動態 IP	PPTP	IPv6
<b>網際網路連線模式</b>			
連線類型		<input type="text" value="斷線"/>	

## WAN1/WAN2 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 Accep5 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。

WAN >>網際網路連線設定

WAN 1

PPPoE	固定或動態 IP	PPTP	IPv6
<b>網際網路連線模式</b>			
連線類型	PPP		
附註：IPv4 WAN 設定應為 PPPoE 用戶端			

確定 取消

下圖顯示 PPP 模式下，成功的 IPv6 連線運作範例圖。

Online Status

Physical Connection		System Uptime: 0:2:32	
IPv4	IPv6		
<b>LAN Status</b>			
<b>IP Address</b>			
2001:B010:7300:201:21D:AFF:FEA6:2568/64 (Global)			
FE80::21D:AFF:FEA6:2568/64 (Link)			
<b>TX Packets</b>	<b>RX Packets</b>	<b>TX Bytes</b>	<b>RX Bytes</b>
7	4	690	328
<b>WAN2 IPv6 Status</b> >> <a href="#">Drop PPP</a>			
<b>Enable</b>	<b>Mode</b>	<b>Up Time</b>	
Yes	PPP	0:02:08	
<b>IP</b>		<b>Gateway IP</b>	
2001:B010:7300:201:21D:AFF:FEA6:256A/128 (Global)		FE80::90:1A00:242:AD52	
FE80::1D:AFF:FEA6:256A/128 (Link)			
<b>DNS IP</b>			
2001:8000:168::1			
2001:8000:168::2			
<b>TX Packets</b>	<b>RX Packets</b>	<b>TX Bytes</b>	<b>RX Bytes</b>
7	9	544	1126

**注意：**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。

## WAN1/WAN2/WAN3/WAN4 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。

WAN >>網際網路連線設定

WAN 1

PPPoE	固定或動態 IP	PPTP	IPv6
<b>網際網路連線模式</b>			
連線類型		TSPC	
<b>TSPC 設定</b>			
使用者名稱	<input type="text"/>		
密碼	<input type="text"/>		
確認密碼	<input type="text"/>		
通道代理人	<input type="text"/>		

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 <a href="http://gogonet.gogo6.com/page/freenet6-account">http://gogonet.gogo6.com/page/freenet6-account</a> 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。
確認密碼	請再次輸入上述密碼。
通道代理人	輸入通道代理人的 IP 位址、FQDN 或是選項埠號。

在您完成上述的設定之後，請按**確定**按鈕來啟動設定。

## WAN1/WAN2/WAN3/WAN4 的 AICCU 模式細節設定(IPv6)

WAN >>網際網路連線設定

### WAN 1

PPPoE	固定或動態 IP	PPTP	IPv6
<b>網際網路連線模式</b>			
連線類型		AICCU	
<b>AICCU 設定</b>			
<input type="checkbox"/> 永遠連線			
使用者名稱	<input type="text"/>		
密碼	<input type="password"/>		
確認密碼	<input type="password"/>		
通道代理人	tic.sixxs.net		
子網前置號碼	<input type="text"/> / <input type="text"/>		

附註：如果永遠連線未被啟動，AICCU 連線就只會嘗試連線三次

確定

取消

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 <a href="http://www.sixxs.net/">http://www.sixxs.net/</a> 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。
確認密碼	請再次輸入上述密碼。
通道代理人	輸入通道代理人的 IP 位址、FQDN 或是選項埠號。
子網前置號碼	輸入得自服務供應商所取得之前置號碼位址。

在您完成上述的設定之後，請按**確定**按鈕來啟動設定。

## WAN1/WAN2 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。

WAN >>網際網路連線設定

WAN 1

PPPoE	固定或動態 IP	PPTP	IPv6
<b>網際網路連線模式</b>			
連線類型		DHCPv6 用戶端	
<b>DHCPv6 用戶端設定</b>			
身分連結		<input checked="" type="radio"/> 前置號碼授權 <input type="radio"/> 非暫時位址	
IAID (辨識連結 ID)	998429928		

確定 取消

可用設定說明如下：

項目	說明
身分連結	選擇前置號碼授權或是非暫時位址作為身分連結選項。
IAID	輸入號碼做為辨識之用。

在您完成上述的設定之後，請按**確定**按鈕來啟動設定。

## WAN1/WAN2 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 IPv6 位址。

WAN >> 網際網路連線設定

WAN 1

PPPoE	固定或動態 IP	PPTP	IPv6			
<b>網際網路連線模式</b>						
連線類型 <span style="float: right;">固定 IPv6</span>						
<b>固定 IPv6 位址設定</b>						
IPv6 位址 / 前置號碼長度						
<input type="text"/> / <input type="text"/> <span style="float: right;">新增 刪除</span>						
<b>目前 IPv6 位址表格</b>						
索引編號 IPv6 位址 / 前置號碼長度 範圍						
<table border="1" style="width: 100%; height: 100px;"><thead><tr><th>索引編號</th><th>IPv6 位址 / 前置號碼長度</th><th>範圍</th></tr></thead><tbody></tbody></table>				索引編號	IPv6 位址 / 前置號碼長度	範圍
索引編號	IPv6 位址 / 前置號碼長度	範圍				
<b>固定 IPv6 閘道設定</b>						
IPv6 閘道位址						
<input type="text" value="::"/>						

確定 取消

可用設定說明如下：

項目	說明
固定 IPv6 位址設定	<b>IPv6 位址</b> - 輸入固定的 IPv6 位址。 <b>前置號碼長度</b> - 輸入前置號碼長度固定值。 <b>新增</b> - 按下此鈕新增位址。 <b>刪除</b> - 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。
固定 IPv6 閘道設定	<b>IPv6 閘道設定</b> - 請在此輸入 IPv6 閘道的位址。

在您完成上述的設定之後，請按**確定**按鈕來啟動設定。

## WAN1/WAN2 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。

WAN >> 網際網路連線



WAN 1

PPPoE	固定或動態 IP	PPTP/L2TP	IPv6
<b>網際網路連線模式</b>			
連線類型 <span style="float: right;">6in4 固定通道</span>			
<b>6in4 固定通道</b>			
遠端終點 IPv4 位址 <input type="text"/>			
6in4 IPv6 位址 <input type="text"/> / <input type="text" value="64"/> (預設值:64)			
LAN路由前置代碼 <input type="text"/> / <input type="text" value="64"/> (預設值:64)			
通道 TTL <input type="text" value="255"/> (預設值:255)			
<b>WAN 連線檢測</b>			
模式 <span style="float: right;">永遠連線</span>			

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。可透過 ARP 檢測或是 Ping Detect 來完成。 <b>模式</b> – 選擇 <b>永遠連線</b> 或 <b>Ping Detect</b> 執行 WAN 檢測動作。 <b>Ping IP</b> – 如果您選擇 <b>Ping Detect</b> 作為檢測模式，您必須在本區輸入 IP 位址作為 Ping 檢測之用。 <b>TTL (Time to Live)</b> – 顯示數值供您參考，TTL 數值是利用 Telnet 指令始可設定。

在您完成上述的設定之後，請按**確定**按鈕來啟動設定。

下圖顯示以此模式為基準，成功設定的 IPv6 連線範例。

#### Online Status

Physical Connection		System Uptime: 0day 0:4:16	
IPv4	IPv6		
<b>LAN Status</b>			
<b>IP Address</b>			
2001:4DD0:FF00:83E4:21D:AAFF:FE83:11B4/64 (Global)			
FE80::21D:AAFF:FE83:11B4/64 (Link)			
<b>TX Packets</b>	<b>RX Packets</b>	<b>TX Bytes</b>	<b>RX Bytes</b>
14	80	1244	6815
<b>WAN1 IPv6 Status</b>			
<b>Enable</b>	<b>Mode</b>	<b>Up Time</b>	
Yes	6in4 Static Tunnel	0:04:07	
<b>IP</b>		<b>Gateway IP</b>	
2001:4DD0:FF10:83E4::2131/64 (Global)		---	
FE80::C0A8:651D/128 (Link)			
<b>TX Packets</b>	<b>RX Packets</b>	<b>TX Bytes</b>	<b>RX Bytes</b>
3	26	211	2302

## WAN1/WAN2 的 6rd 模式細節設定(IPv6)

頁讓您針對 WAN 界面設定 6rd 模式。

WAN >> 網際網路連線



#### WAN 1

PPPoE	固定或動態 IP	PPTP/L2TP	IPv6
<b>網際網路連線模式</b>			
連線類型		6rd	
<b>6rd 設定</b>			
6rd 模式		<input checked="" type="radio"/> 自動 6rd <input type="radio"/> 固定 6rd	
附註：請先將 IPv4 WAN 設定為 DHCP，以便進行自動 6rd 連線。			
<b>WAN 連線檢測</b>			
模式		永遠連線	

確定

取消

可用設定說明如下：

項目	說明
<b>6rd 模式</b>	<b>自動 6rd</b> – 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。 <b>固定 6rd</b> - 手動設定 6rd 選項。
<b>IPv4 Border 中繼</b>	選擇 <b>固定 6rd</b> 模式之後，針對 6rd 網域提供 IPv4 位址作為 6rd Border 的中繼。
<b>IPv4 遮罩長度</b>	選擇 <b>固定 6rd</b> 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。



<b>6rd 前置代碼</b>	選擇 <b>固定 6rd</b> 模式之後，輸入 6rd IPv6 位址。
<b>6rd 前置代碼長度</b>	選擇 <b>固定 6rd</b> 模式之後，輸入 6rd IPv6 前置代碼需求的長度數字。
<b>WAN 連線偵測</b>	<p>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。</p> <p><b>模式</b> – 選擇<b>永遠連線</b>或 <b>Ping Detect</b> 執行 WAN 檢測動作。</p> <p><b>Ping IP</b> – 如果您選擇 <b>Ping Detect</b> 作為檢測模式，您必須在本區輸入 IP 位址作為 Ping 檢測之用。</p> <p><b>TTL (Time to Live)</b> – 顯示數值供您參考，TTL 數值是利用 Telnet 指令始可設定。</p>

在您完成上述的設定之後，請按**確定**按鈕來啟動設定。

下圖顯示以此模式為基準，成功設定的 IPv6 連線範例。

**Online Status**

Physical Connection		System Uptime: 0day 0:9:15	
IPv4		IPv6	
<b>LAN Status</b>			
<b>IP Address</b>			
2001:E41:A865:1D00:21D:AAFF:FE83:11B4/64 (Global)			
FE80::21D:AAFF:FE83:11B4/64 (Link)			
<b>TX Packets</b>	<b>RX Packets</b>	<b>TX Bytes</b>	<b>RX Bytes</b>
15	113	1354	18040
<b>WAN1 IPv6 Status</b>			
<b>Enable</b>	<b>Mode</b>	<b>Up Time</b>	
Yes	6rd	0:09:06	
<b>IP</b>		<b>Gateway IP</b>	
2001:E41:A865:1D01:21D:AAFF:FE83:11B5/128 (Global)		---	
FE80::C0A8:651D/128 (Link)			
<b>TX Packets</b>	<b>RX Packets</b>	<b>TX Bytes</b>	<b>RX Bytes</b>
13	29	967	2620

## 4.1.4 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，以使用於需要高度網路流量的應用上。

本頁顯示每個頻道的基本設定值。

WAN >> 多重 VLAN

### 多重 VLAN

基本					
頻道	啟用	WAN 類型	VLAN 標籤	埠號橋接	
1	是	乙太網路(WAN1)	無		
2	是	乙太網路(WAN2)	無		
5. WAN5	否	乙太網路(WAN1)	無	<input type="checkbox"/> 啟用	<input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4 <input type="checkbox"/> P5
6. WAN6	否	乙太網路(WAN1)	無	<input type="checkbox"/> 啟用	<input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4 <input type="checkbox"/> P5
7. WAN7	否	乙太網路(WAN1)	無	<input type="checkbox"/> 啟用	<input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4 <input type="checkbox"/> P5
8.	否	乙太網路(WAN1)	無	<input type="checkbox"/> 啟用	<input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4 <input type="checkbox"/> P5
9.	否	乙太網路(WAN1)	無	<input type="checkbox"/> 啟用	<input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4 <input type="checkbox"/> P5
10.	否	乙太網路(WAN1)	無	<input type="checkbox"/> 啟用	<input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4 <input type="checkbox"/> P5

#### 附註：

頻道 3 與頻道 4 保留予 USB WAN。

確定

取消

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 與 2 專屬於網際網路使用者介面，因此在此處是不可以修訂的。 頻道 5 到 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 ~ P5 - 選需要的埠號以便建立區域網路端的橋接連線。

按下索引編號(8, 9 與 10)可以看到如下頁面：

多重 VLAN 頻道8:  啟用  停用

WAN 類型:

---

**基本設定**

VLAN 標題

VLAN 標籤:

優先權:

**附註:** 標籤值必須介於1~4095且每個頻道擁有獨立的標籤值。  
一次僅有一個頻道不需加標籤(值等於0)。

---

**橋接模式**

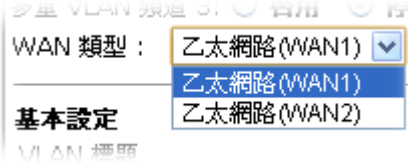
啟用

實體連線成員

P1  P2  P3  P4  P5

**附註:** P1 保留給NAT; 而且無法應用在橋接模式下

可用設定說明如下：

項目	說明
多重 VLAN 頻道 8/9/10	<p><b>啟用</b> – 選擇此項啟用此頻道設定。</p> <p><b>停用</b> – 選擇此項停止使用此頻道設定。</p>
WAN 類型	<p>每個頻道連線與介面都可透過選擇一個特定的 WAN 類型來建立。在多重 VLAN 應用中，只有乙太網路 WAN 類型可以使用，使用者可選擇實體 WAN 介面。</p> 
基本設定	<p><b>VLAN 標籤</b> – 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。</p> <p><b>優先權</b> – 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。</p>
橋接模式	<p><b>啟用</b> – 選擇此項啟用此頻道設定的橋接模式。</p> <p><b>實體連線成員</b> – 勾選您想要群組的埠號，使其套用橋接模式連線。</p>

另外，5、6 與 7 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。

WAN >> 多重 VLAN >> 頻道 5

多重 VLAN 頻道 5:  啟用  停用

WAN 類型:

---

**基本設定**

VLAN 標題

VLAN 標籤:

優先權:

附註: 1. 標籤值必須介於 1~4095 之間，每個頻道的標籤值都是獨一的。  
 一次只能有一個頻道是不加標籤值(等於 0)的。

---

關閉本頻道的埠號橋接連線

實體連線成員

P1  P2  P3  P4  P5

附註: 3.P1 保留給 NAT；而且無法應用在橋接模式下。

---

針對此頻道關閉 WAN 介面

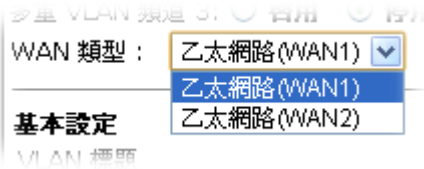
路由器應用之 WAN 介面:

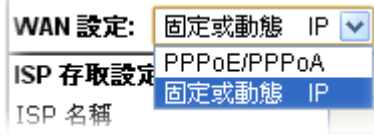
WAN 設定:

---

<p><b>ISP 存取設定</b></p> <p>ISP 名稱: <input type="text"/></p> <p>使用者名稱: <input type="text"/></p> <p>密碼: <input type="text"/></p> <p>PPP 驗證: <input type="text" value="PAP 或 CHAP"/></p> <p><input checked="" type="checkbox"/> 永遠連線</p> <p>閒置逾時: <input type="text" value="-1"/> 秒</p> <p><b>來自 ISP 的 IP 位址</b></p> <p>固定 IP <input type="radio"/> 是 <input checked="" type="radio"/> 否 (動態 IP)</p> <p>固定 IP 位址: <input type="text"/></p>	<p><b>WAN IP 網路設定</b></p> <p><input type="radio"/> 自動取得 IP 位址</p> <p>路由器名稱: <input type="text" value="Vigor"/> *</p> <p>網域名稱: <input type="text"/> *</p> <p>*: 某些 ISP 需要此類資訊</p> <p><input checked="" type="radio"/> 指定 IP 位址</p> <p>IP 位址: <input type="text"/></p> <p>子網遮罩: <input type="text"/></p> <p>閘道 IP 位址: <input type="text"/></p> <p><b>DNS 伺服器 IP 位址</b></p> <p>主要 IP 位址: <input type="text" value="8.8.8.8"/></p> <p>次要 IP 位址: <input type="text" value="8.8.4.4"/></p>
--	--

可用設定說明如下：

項目	說明
多重 VLAN 頻道 5/6/7	<p>啟用 – 選擇此項啟用此頻道設定。</p> <p>停用 – 選擇此項停止使用此頻道設定。</p>
WAN 類型	<p>每個頻道連線與介面都可透過選擇一個特定的 WAN 類型來建立。在多重 VLAN 應用中，只有乙太網路 WAN 類型可以使用，使用者可選擇實體 WAN 介面。</p> 
基本設定	<p><b>VLAN 標籤</b> – 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。</p> <p><b>優先權</b> – 選擇一個號碼來決定此 VLAN 封包的優先權</p>

項目	說明
	為何，可設定範圍自 0 到 7。
開啓本頻道的埠號橋接連線	<p>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。</p> <p><b>實體連線成員</b> – 勾選您想要群組的埠號，使其套用橋接模式連線。</p>
針對此頻道開啓 WAN 介面	<p>勾選選框啓用相關功能。</p> <p><b>路由器應用之 WAN 介面 – 管理</b>可指定為一班管理之用(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。</p> <p><b>VoIP</b> - 允許 WAN 介面傳送 SIP 註冊的封包與其他 VoIP 管理封包。</p> <p><b>IPTV</b> - 允許 WAN 介面傳送 IGMP 封包到 IPTV 伺服器。</p> <p><b>WAN 設定</b> – 選擇 PPPoE/PPPoA 或是固定或動態 IP 設定，以便決定哪個 WAN 介面需要設定。</p> 
ISP 設定等等	WAN1 有關其他設定，請參考 WAN1 底下 PPPoE 的細部設定。

在您完成上述的設定之後，請按**確定**按鈕來啓動設定。

#### 4.1.5 WAN 計量收費

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。

#### 基本設定

WAN >> WAN計量收費

基本設定		監控頁面			
索引編號	啟用	額度	當超過額度時	時間週期	期間
WAN1	x	0MB/0MB			0/00/00 00:00~0/00/00 00:00
WAN2	x	0MB/0MB			0/00/00 00:00~0/00/00 00:00
WAN3	x	0MB/0MB			0/00/00 00:00~0/00/00 00:00
WAN4	x	0MB/0MB			0/00/00 00:00~0/00/00 00:00

附註: 1. 此處提供之預算流量資訊僅供參考使用，請連絡您的ISP業者以便取得實際的流量運用與費用。  
2. 當使用硬體加速功能時，受監控的WAN或是以太網路WAN介面的流量可能會有些不準確。

按下 WAN1/WAN2/WAN3/WAN4 連結以便開啓如下頁面。

## WAN 1

啟用

**準則和動作**

額度限制:  MB

當額度超過:

關閉 WAN 介面

傳送郵件至管理者

傳送簡訊至管理者

**每月**      **使用者定義**

選擇月份中的某一天讓資料重新設定。

結算週期起始於  日

- 附註:
1. 請確保 **時間與日期** 路由器已經設定完畢。
  2. 按下確定之後，此WAN介面的WAN額度計數器將重新設定。

確定

取消

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	請輸入最大的網路流量限制(單位是百萬位元或是 GB)。
當額度超過	<p>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。</p> <p><b>關閉 WAN 介面</b> – 所有透過此 WAN 介面的對外流量都將中止。</p> <p><b>傳送郵件至管理者</b>– 系統將發送警告訊息予管理者，雖然額度已快用完，但是連線費用仍然持續計算。</p> <p><b>傳送簡訊至管理者</b> – 系統將發送簡訊予管理者，雖然額度已快用完，但是連線費用仍然持續計算。</p>
每月	<p>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。</p> <p><b>每月</b>      <b>使用者定義</b></p> <p>選擇月份中的某一天讓資料重新設定。</p> <p>結算週期起始於 <input type="text" value="1"/> 日 <input type="text" value="00:00"/></p> <p><b>結算週期起始於 ...</b> – 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。</p>
使用者定義	<p>此設定可讓 ISP 業者依照實際的需要定義所需的結算週期。</p> <p>WAN 計量收費可以經過一個週期間隔之後重新起算。</p> <p><b>使用者定義</b> – 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<b>使用者定義</b>，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</p>

外您也可以指定目前週期內的天數為幾天。

每月

使用者定義

選擇特定天數的某一天讓資料重新設定。

結算週期:  日期與  小時

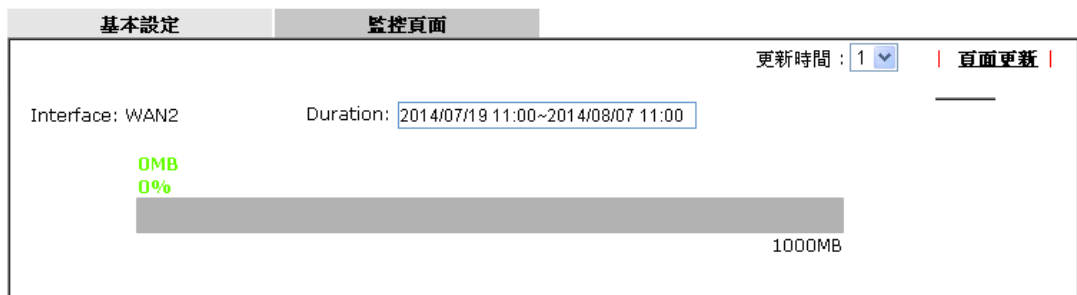
目前週期內的天數:

- **結算週期：** 指定重設流量紀錄的期間。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。
- **目前週期內的天數** – 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。

## 監控頁面

監控頁面顯示 WAN 計量收費的狀態，包括期間與用量。

WAN >> WAN計量收費



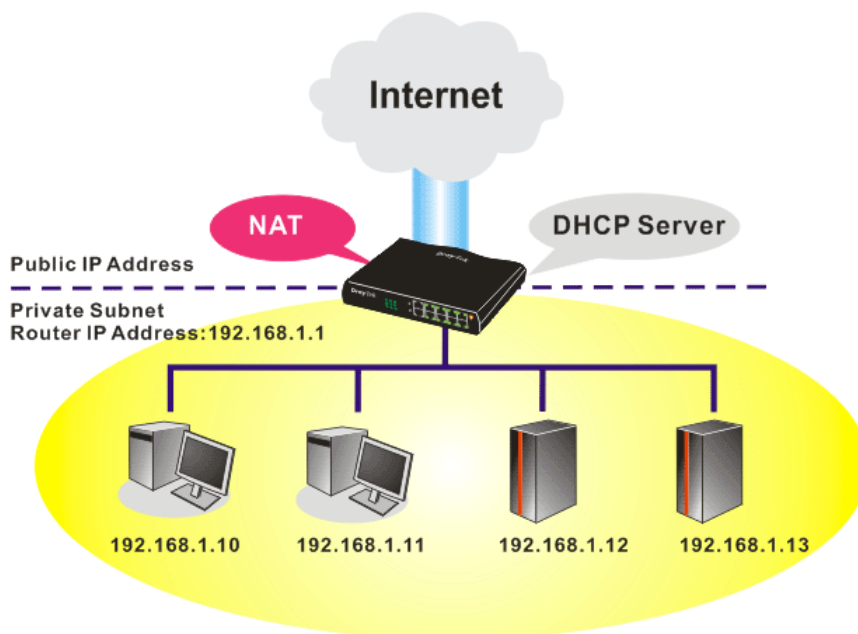
## 4.2 區域網路(LAN)

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

WAN  
區域網路  
基本設定  
固定路由  
VLAN  
綁定 IP 與 MAC 位址  
埠口監控  
有線 802.1x  
客製化入口網站設定

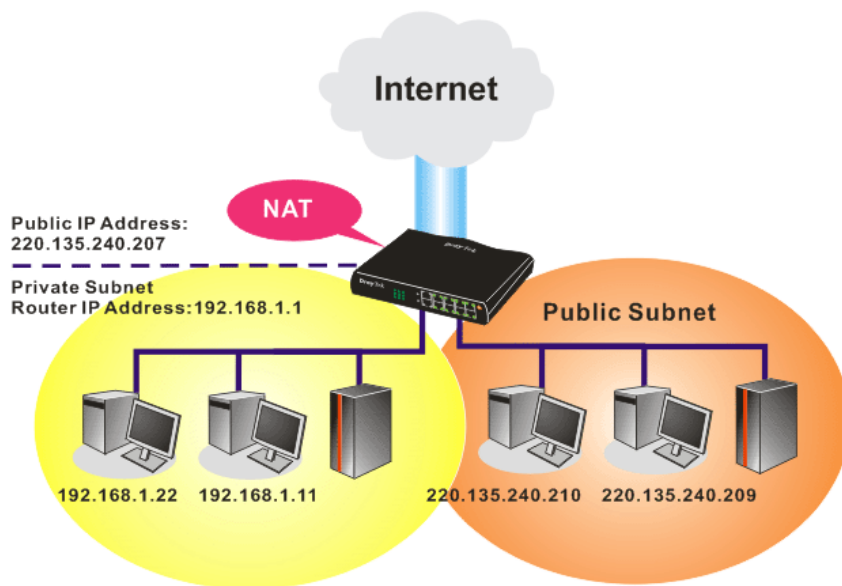
### 4.2.1 區域網路基本概念

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)

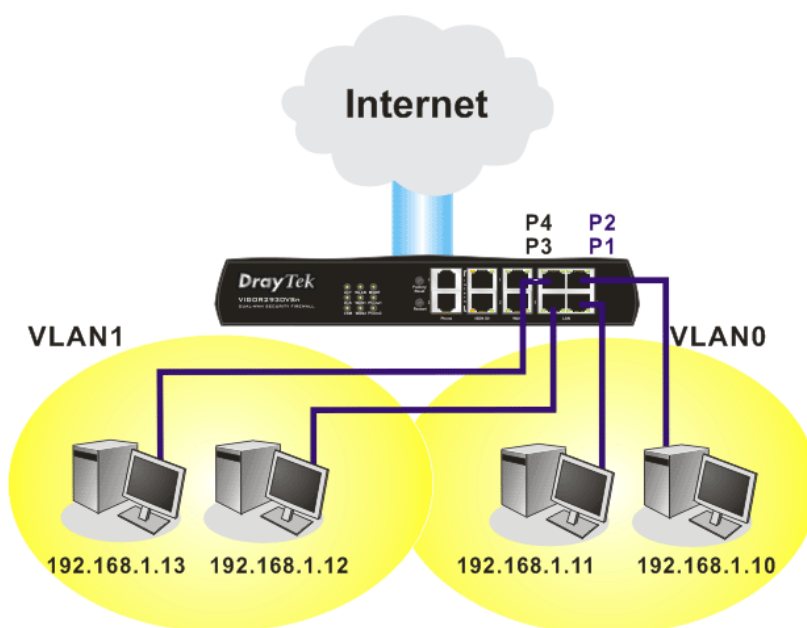
Vigor 路由器可利用 RIP 與鄰近路由器交換路由資訊，達到 IP 路由的目的。這樣可讓使用者變更路由器的資訊，例如 IP 地址，且路由器還會自動通知雙方此類訊息。

### 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)

您可以利用實體的连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。



## 4.2.2 基本設定

本頁提供您區域網路的基本設定。按**區域網路**開啓區域網路設定並選擇**基本設定**。

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 設定固定爲 NAT 模式專用，LAN2 至 LAN5 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。

區域網路 >> 基本設定

### 基本設定

索引編號	狀態	DHCP	IP 位址		
LAN 1	<input checked="" type="checkbox"/>	-	192.168.1.1	<a href="#">細節設定</a>	<a href="#">IPv6</a>
LAN 2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.2.1	<a href="#">細節設定</a>	
LAN 3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.3.1	<a href="#">細節設定</a>	
LAN 4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.4.1	<a href="#">細節設定</a>	
LAN 5	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.5.1	<a href="#">細節設定</a>	
DMZ	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.6.1	<a href="#">細節設定</a>	
IP 路由子網	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.0.1	<a href="#">細節設定</a>	

[進階](#) 您可以在此設定 DHCP options。

強迫路由器使用 "DNS 伺服器 IP 位址" 設定 [LAN1](#)

### Inter-LAN 路由

子網路	LAN 1	LAN 2	LAN 3	LAN 4	LAN 5
LAN1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LAN2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LAN3	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LAN4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
LAN5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

附註: 當VLAN啓用時，LAN 2/3/4/5 都是可用的  
DMZ 子網域設值綁定至P1，且將會改寫LAN>>VLAN頁面中關於P1的設定。

[確定](#)

可用設定說明如下：

項目	說明
基本設定	<p>允許針對個別子網設定不同內容。</p> <p><b>索引編號</b> - 顯示全部的 LAN 項目。</p> <p><b>狀態</b> - 基本上 LAN1 狀態於預設時是啓用的，LAN2 之後與 IP 路由子網只有在狀態欄位已勾選時，始可查閱。</p> <p><b>DHCP</b>- 預設狀態下，LAN1 設定爲 DHCP 模式，如果有必要，請針對每個 LAN 勾選此方塊。</p> <p><b>IP 位址</b> - 顯示每個 LAN 的 IP 位址。</p> <p><b>細節設定</b> - 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。</p> <p><b>IPv6</b> - 按下此鈕進入 IPv6 設定頁面。</p>
進階	DHCP 封包可以利用新增選項號碼與資訊做額外處理。

## DHCP 伺服器客製化狀態

啟用	介面	選項	類型	資料
<input checked="" type="checkbox"/>	全部 <input type="checkbox"/> LAN1 <input type="checkbox"/> LAN2 <input type="checkbox"/> LAN3 <input type="checkbox"/> LAN4 <input type="checkbox"/> LAN5 <input type="checkbox"/> DMZ <input type="checkbox"/> IP 路由子網 <input type="checkbox"/>			
下一個伺服器 IP 位址/SIAddr: <input type="text"/> Option 編號: <input type="text"/> 資料類型: <input checked="" type="radio"/> ASCII 字元 (例如 :Option:18, 資料:./path) <input type="radio"/> 十六進位數字 (例如 Option:18, 資料:2F70617468) <input type="radio"/> 位址清單 (例如 :Option:44, 資料:172.16.2.10,172.16.2.20...) 資料: <input type="text"/>				
<input type="button" value="新增"/> <input type="button" value="更新"/> <input type="button" value="刪除"/> <input type="button" value="重新設定"/>				

**啟用/停用** – 啟用或是停用 DHCP 選項功能，每個 DHCP 選項都是由一個 Option Number 與資料組合而成。例如

Option number: 100

資料: abcd

當此功能啟用時，即可在 DHCP 回覆封包中見到此處指定的內容。

**介面**: 指定此功能將會覆寫的 WAN/LAN 介面。

**下一個伺服器 IP 位址**: 輸入下一個可使用的 DHCP 伺服器的 IP 位址。

**Option 編號** – 輸入一組號碼。

**附註**: 如果您選擇設定 option 61，那麼在 **WAN>> 網際網路連線** 內的設定也會被同步改寫掉。

**資料類型** – 選擇儲存資料的類型(ASCII、十六進位或是位址)。

**資料** – 輸入 DHCP 選項功能必須處理的資料內容。

**強迫路由器使用 DNS 伺服器 IP 位址設定**

勾選此項可以迫使路由器改運用 LAN1/LAN2/LAN3/LAN4/LAN5 中的 DNS 伺服器的設定。

**Inter-LAN 路由**

勾選方塊來連結二個或是多個不同的子網(LAN 與 LAN 間)。

在您完成上述的設定之後，請按**確定**按鈕來啟動設定。

## LAN1 - 區域網路 TCP/IP 與 DHCP 設定的細節設定

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：

區域網路 >> 基本設定

LAN 1 區域網路 TCP /IP 與 DHCP 設定	LAN 1 IPv6 設定
<b>網路設定</b> 供 NAT 使用 IP 位址 <input type="text" value="192.168.1.1"/> 子網路遮罩 <input type="text" value="255.255.255.0"/> RIP 協定控制 <input type="button" value="停用"/>	<b>DHCP 伺服器組態</b> <input type="radio"/> 啟用伺服器 <input checked="" type="radio"/> 停用 <input type="checkbox"/> 啟用中繼代理位址 起始 IP 位址 <input type="text" value="192.168.1.10"/> IP 配置數量 <input type="text" value="200"/> 開道 IP 位址 <input type="text" value="192.168.1.1"/> 租約時間 <input type="text" value="86400"/> (s) <b>DNS 伺服器 IP 位址</b> 主要 IP 位址 <input type="text"/> 次要 IP 位址 <input type="text"/>

確定

可用設定說明如下：

項目	說明
網路設定	<p><b>針對 NAT 用途,</b></p> <p><b>IP 位址</b> - 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)。</p> <p><b>子網路遮罩</b> - 請輸入決定網路大小的位址代碼(預設值為 255.255.255.0/ 24)。</p> <p><b>RIP 協定控制,</b></p> <p><b>停用</b> - 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)。</p> <p><b>啟用</b> - 啟動此協定。</p>
DHCP 伺服器組態	<p>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。</p> <p>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。</p> <p><b>啟用</b> - 讓路由器指定 IP 地址到區域網路上的每個主機上。</p> <p><b>停用</b> - 讓您手動指定 IP 地址到區域網路上的每個主機上。</p> <p><b>啟動中繼代理</b> - 指定某個 DHCP 伺服器所在的子網路讓中繼代理重新引導 DHCP 需求至該處。</p>

	<p><b>DHCP 伺服器 IP 位址</b> – 當您勾選了<b>啟動中繼代理</b>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。</p> <p><b>起始 IP 位址</b> -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，如果第路由器的第一個 IP 位址為 192.168.1.1，起始 IP 位址可以是 192.168.1.2 或是更高一些，但比 192.168.1.254 小。</p> <p><b>IP 配置數量</b> -輸入您想要 DHCP 伺服器指定 IP 地址的最大數量，預設值為 50，最大值為 253。</p> <p><b>閘道 IP 位址</b> -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。</p> <p><b>租約時間</b> - 輸入 DHCP 伺服器可以使用來分派 IP 位址的時間長度。</p>																
<p><b>DNS 伺服器組態</b></p>	<p>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。</p> <p><b>主要 IP 位址</b> -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。</p> <p><b>次要 IP 位址</b> - 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。</p> <p>預設 DNS 伺服器 IP 位址可在線上狀態上查看：</p> <div data-bbox="699 1294 1396 1456" style="border: 1px solid black; padding: 5px;"> <p>Online Status</p> <hr/> <p>Physical Connection <span style="float: right;">System Uptime: 22:22:45</span></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 25%;">IPV4</th> <th style="width: 25%;">IPV6</th> <th colspan="2"></th> </tr> </thead> <tbody> <tr> <td>LAN Status</td> <td>Primary DNS: 8.8.8.8</td> <td colspan="2">Secondary DNS: 8.8.4.4</td> </tr> <tr> <td>IP Address</td> <td>TX Packets</td> <td>RX Packets</td> <td></td> </tr> <tr> <td>192.168.1.1</td> <td>0</td> <td>41533</td> <td></td> </tr> </tbody> </table> </div> <p>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 快速緩衝儲存區。</p> <p>如果網域名稱的 IP 位址已經在 DNS 快速緩衝儲存區內，路由器將立即 resolve 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。</p>	IPV4	IPV6			LAN Status	Primary DNS: 8.8.8.8	Secondary DNS: 8.8.4.4		IP Address	TX Packets	RX Packets		192.168.1.1	0	41533	
IPV4	IPV6																
LAN Status	Primary DNS: 8.8.8.8	Secondary DNS: 8.8.4.4															
IP Address	TX Packets	RX Packets															
192.168.1.1	0	41533															

在您完成上述的設定之後，請按**確定**按鈕來啟動設定。

### LAN1 – IPv6 的細節設定

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。下圖為 IPv6 的設定頁面。

LAN 1 區域網路 TCP/IP 與 DHCP 設定	LAN 1 IPv6 設定						
<b>RADVD 設定</b> <input checked="" type="radio"/> 啟用 <input type="radio"/> 停用 廣播有效時間 <input type="text" value="1800"/> 秒數 (範圍: 600 - 9000)							
<b>DHCPv6 伺服器設定</b> <input type="radio"/> 啟用伺服器 <input checked="" type="radio"/> 停用 起始 IPv6 位址 <input type="text"/> 結束 IPv6 位址 <input type="text"/> <b>DNS 伺服器 IPv6 位址</b> 主要 DNS 伺服器 <input type="text"/> 次要 DNS 伺服器 <input type="text"/>							
<b>固定 IPv6 位址設定</b> IPv6 位址 <input type="text"/> / 前置號碼長度 <input type="text"/> <input type="button" value="新增"/> <input type="button" value="刪除"/> <b>目前 IPv6 位址表格</b> <table border="1"> <thead> <tr> <th>索引編號</th> <th>IPv6 位址 / 前置號碼長度</th> <th>範圍</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>FE80::21D:AAFF:FEAC:19C8/64</td> <td>Link</td> </tr> </tbody> </table>		索引編號	IPv6 位址 / 前置號碼長度	範圍	1	FE80::21D:AAFF:FEAC:19C8/64	Link
索引編號	IPv6 位址 / 前置號碼長度	範圍					
1	FE80::21D:AAFF:FEAC:19C8/64	Link					

本頁面提供二種 LAN 端 IPv6 位址設定，一種為 **RADVD**，另一種為 **DHCPv6 伺服器**。可用設定說明如下：

項目	說明
<b>RADVD 設定</b>	<p><b>啟用</b> – 啟動 RADVD 伺服器，路由器 RADVD 定期傳送 RFC2461 指定的訊息至本地乙太網路 LAN 端，這些訊息乃是因應 IPv6 無狀態自動設定的需求。</p> <p><b>停用</b> – 停用 RADVD 伺服器的運作。</p> <p><b>廣播有效時間</b> - 預設路由器的有效時間以秒計算，用來控制前置號碼的有效期間，最大值可對應至 18.2 小時。數值設定為 0 表示路由器並非預設的路由器，且也不會出現在預設路由器的清單內。</p>
<b>DHCPv6 伺服器設定</b>	<p><b>啟用伺服器</b> – 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。</p> <p><b>停用伺服器</b> – 停用 DHCPv6 伺服器的運作。</p> <p><b>起始 IPv6 位址 / 結束 IPv6 位址</b> – 分別輸入起始以及結束的 IP 位址。</p>
<b>DNS 伺服器 IPv6 位址</b>	<p><b>主要 DNS 伺服器</b> – 輸入主要 DNS 伺服器的 IPv6 位址。</p> <p><b>次要 DNS 伺服器</b> – 輸入次要 DNS 伺服器的 IPv6 位址。</p>

項目	說明
固定 IPv6 位址設定	<b>IPv6 位址</b> - 輸入區域網路所需的固定 IPv6 位址。 <b>前置號碼長度</b> - 輸入前置號碼固定的長度值。 <b>新增</b> - 新增新的位址資料並顯示在位址表格中。 <b>刪除</b> - 刪除位址表格中選定的位址資料。
目前 IPv6 位址表格	顯示目前使用的 IPv6 位址。

在您完成上述的設定之後，請按**確定**按鈕來啟動設定。

## LAN2 ~ LAN5 與 DMZ 的細節設定

區域網路 >> 基本設定

### LAN 2 乙太網路 TCP / IP 與 DHCP 設定

<b>網路設定</b> <input type="radio"/> 啟用 <input checked="" type="radio"/> 停用 <input checked="" type="radio"/> 供 NAT 使用 <input type="radio"/> 用於路由 IP 位址 <input type="text" value="192.168.2.1"/> 子網路遮罩 <input type="text" value="255.255.255.0"/>		<b>DHCP 伺服器設定</b> <input checked="" type="radio"/> 啟用伺服器 <input type="radio"/> 停用伺服器 <input type="checkbox"/> 啟用中繼伺服器 起始 IP 位址 <input type="text" value="192.168.2.10"/> IP 配置數量 <input type="text" value="100"/> 開道 IP 位址 <input type="text" value="192.168.2.1"/> 租約時間 <input type="text" value="259200"/> (s)	
		<b>DNS 伺服器 IP 位址</b> 主要 IP 位址 <input type="text" value="0.0.0.0"/> 次要 IP 位址 <input type="text" value="0.0.0.0"/>	

**確定**

可用設定說明如下：

項目	說明
網路設定	<b>啟用/停用</b> - 選擇 <b>啟用</b> 來啟動此設定，按下 <b>停用</b> 則關閉此設定。 <b>供 NAT 用途</b> - 選擇此鈕讓設定資料供 NAT 使用。 <b>用於路由</b> - 選擇此鈕讓設定資料套用於路由。 <b>IP 位址</b> - 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)。 <b>子網路遮罩</b> - 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	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。 <b>啟用伺服器</b> - 讓路由器指定 IP 地址到區域網路上的每個主機上。



項目	說明																
	<p><b>停用伺服器</b> – 讓您手動指定 IP 地址到區域網路上的每個主機上。</p> <p><b>啟動中繼代理</b> – 指定某個 DHCP 伺服器所在的子網路讓中繼代理重新引導 DHCP 需求至該處。</p> <p><b>DHCP 伺服器 IP 位址</b> – 當您勾選了<b>啟動中繼代理</b>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。</p> <p><b>起始 IP 位址</b> -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，如果第路由器的第一個 IP 位址為 192.168.1.1，起始 IP 位址可以是 192.168.1.2 或是更高一些，但比 192.168.1.254 小。</p> <p><b>IP 配置數量</b> -輸入您想要 DHCP 伺服器指定 IP 地址的最大數量，預設值為 50，最大值為 253。</p> <p><b>閘道 IP 位址</b> -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。</p> <p><b>租約時間</b> - 輸入 DHCP 伺服器可以使用來分派 IP 位址的時間長度。</p>																
<b>DNS 伺服器 IP 位址</b>	<p>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。</p> <p><b>主要 IP 位址</b> -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。</p> <p><b>次要 IP 位址</b> - 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。</p> <div data-bbox="703 1503 1394 1659" style="border: 1px solid black; padding: 5px;"> <p>Online Status</p> <hr/> <p>Physical Connection <span style="float: right;">System Uptime: 22:22:45</span></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th colspan="2">IPv4</th> <th colspan="2">IPv6</th> </tr> </thead> <tbody> <tr> <td>LAN Status</td> <td></td> <td>Primary DNS: 8.8.8.8</td> <td>Secondary DNS: 8.8.4.4</td> </tr> <tr> <td>IP Address</td> <td>TX Packets</td> <td>RX Packets</td> <td></td> </tr> <tr> <td>192.168.1.1</td> <td>0</td> <td>41533</td> <td></td> </tr> </tbody> </table> </div> <p>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 快速緩衝儲存區。</p> <p>如果網功能變數名稱的 IP 位址已經在 DNS 快速緩衝儲存區內，路由器將立即 resolve 網功能變數名稱。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。</p>	IPv4		IPv6		LAN Status		Primary DNS: 8.8.8.8	Secondary DNS: 8.8.4.4	IP Address	TX Packets	RX Packets		192.168.1.1	0	41533	
IPv4		IPv6															
LAN Status		Primary DNS: 8.8.8.8	Secondary DNS: 8.8.4.4														
IP Address	TX Packets	RX Packets															
192.168.1.1	0	41533															

在您完成上述的設定之後，請按**確定**按鈕來啟動設定。



## IP 路由子網的細節設定

區域網路 >> 基本設定

### IP 路由子網所需的 TCP/IP 與 DHCP 設定

<b>網路設定</b> <input type="radio"/> 啟用 <input checked="" type="radio"/> 停用 用於路由 IP 位址 <input type="text" value="192.168.0.1"/> 子網路遮罩 <input type="text" value="255.255.255.0"/> RIP 協定控制 <input type="text" value="停用"/>	<b>DHCP 伺服器設定</b> 起始 IP 位址 <input type="text"/> IP 配置數量 <input type="text" value="0"/> (最大 10) 租約時間 <input type="text" value="259200"/> (s) <input type="checkbox"/> 使用 LAN 埠 <input checked="" type="checkbox"/> P1 <input checked="" type="checkbox"/> P2 <input checked="" type="checkbox"/> 使用 MAC 位址 <table border="1"><thead><tr><th>索引編號</th><th>符合的 MAC 位址</th><th>給定 IP 位址</th></tr></thead><tbody></tbody></table> MAC 位址 : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> <input type="button" value="新增"/> <input type="button" value="刪除"/> <input type="button" value="編輯"/> <input type="button" value="取消"/>	索引編號	符合的 MAC 位址	給定 IP 位址
索引編號	符合的 MAC 位址	給定 IP 位址		

可用設定說明如下：

項目	說明
網路設定	<p><b>啟用/停用</b> - 選擇<b>啟用</b>來啟動此設定，按下<b>停用</b>則關閉此設定。</p> <p><b>IP 位址</b> - 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)。</p> <p><b>子網路遮罩</b> - 請輸入決定網路大小的位址代碼(預設值為 255.255.255.0/ 24)。</p> <p><b>RIP 協定控制</b>,</p> <ul style="list-style-type: none"><li>● <b>停用</b> - 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)。</li><li>● <b>啟用</b> - 啟動此協定。</li></ul>
DHCP 伺服器設定	<p>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。</p> <p><b>起始 IP 位址</b> - 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，如果第路由器的第一個 IP 位址為 192.168.1.1，起始 IP 位址可以是 192.168.1.2 或是更高一些，但比 192.168.1.254 小。</p> <p><b>IP 配置數量</b> - 輸入您想要 DHCP 伺服器指定 IP 地址的</p>

---

最大數量。

**租約時間** - 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** - 指定一個 IP 位址供 IP 路由子網使用，如果啓用此埠，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。

**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。

---

在您完成上述的設定之後，請按**確定**按鈕來啓動設定。

### 4.2.3 固定路由

進入區域網路群組並選擇固定路由，開啓如下的畫面。

#### 固定路由(IPv4)

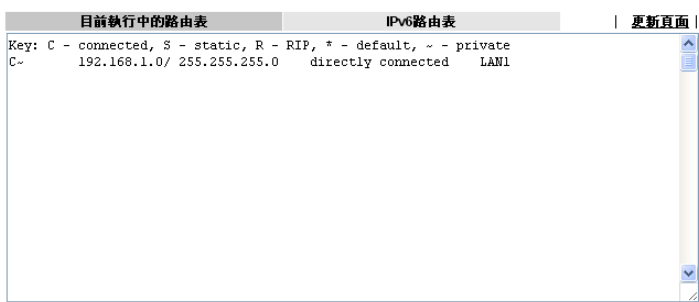
區域網路 >> 固定路由設定

IPv4			IPv6			回復出廠預設值	檢視路由表
索引編號	目的位址	狀態	索引編號	目的位址	狀態		
1.	???	?	6.	???	?		
2.	???	?	7.	???	?		
3.	???	?	8.	???	?		
4.	???	?	9.	???	?		
5.	???	?	10.	???	?		

<< 1-10 | 11-20 | 21-30 >> 下一頁 >>

狀態: v — 使用中, x — 未使用, ? — 空白

可用設定說明如下：

項目	說明
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	<p>開啓如下畫面檢視目前的路由狀況。</p> <p>自我診斷工具 &gt;&gt; 檢視路由表</p> 
索引編號	索引編號下方的號碼(1 到 10)允許您開啓下一層頁面以設定固定路由。
目標位址	顯示固定路由的目標位址。
狀態	顯示固定路由的狀態。

按下任一索引編號開啓如下頁面：

## 索引編號 1

<input checked="" type="checkbox"/> 啟用	
目的 IP 位址	???
子網路遮罩	
閘道 IP 位址	
網路介面	LAN1

可用設定說明如下：

項目	說明
啟用	勾選此方塊以啟動此設定檔。
目的 IP 位址	輸入此固定路由作為目的需求的 IP 位址。
子網路遮罩	輸入此固定路由的子網遮罩。
閘道 IP 位址	輸入此固定路由的閘道 IP 位址。
網路介面	使用下拉式清單指定單一介面作為固定路由的通過介面。

在您完成上述的設定之後，請按**確定**按鈕來啟動設定。

## 固定路由(IPv6)

按下 IPv6 標籤開啓下述頁面，您可以設定多達 40 組設定檔。

區域網路 >> 固定路由設定

IPv4			IPv6			回復出廠預設值	檢視 IPv6 路由表格
索引編號	目的位址	狀態	索引編號	目的位址	狀態		
<a href="#">1.</a>	::/0	x	<a href="#">11.</a>	::/0	x		
<a href="#">2.</a>	::/0	x	<a href="#">12.</a>	::/0	x		
<a href="#">3.</a>	::/0	x	<a href="#">13.</a>	::/0	x		
<a href="#">4.</a>	::/0	x	<a href="#">14.</a>	::/0	x		
<a href="#">5.</a>	::/0	x	<a href="#">15.</a>	::/0	x		
<a href="#">6.</a>	::/0	x	<a href="#">16.</a>	::/0	x		
<a href="#">7.</a>	::/0	x	<a href="#">17.</a>	::/0	x		
<a href="#">8.</a>	::/0	x	<a href="#">18.</a>	::/0	x		
<a href="#">9.</a>	::/0	x	<a href="#">19.</a>	::/0	x		
<a href="#">10.</a>	::/0	x	<a href="#">20.</a>	::/0	x		

<< [1 - 20](#) | [21 - 40](#) >>

[下一頁 >>](#)

狀態: v --- 使用中, x --- 不使用, ? --- 空白

可用設定說明如下：

項目	說明
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 路由表格	顯示路由表格。
索引編號	索引編號下方的數字連結可讓您開啓設定頁面進行路由設定。
目標位址	顯示固定路由的目標位址。
狀態	顯示固定路由的狀態。

按下任一索引編號開啓如下頁面：

區域網路 >> 固定路由設定

### 索引編號 1

<input type="checkbox"/> 啟用	
目的 IPv6 位址 / 前置號碼長度	:: / 0
閘道 IPv6 位址	
網路介面	LAN

確定

取消

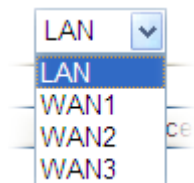
刪除

可用設定說明如下：

項目	說明
啟用	勾選此方塊以啓動此設定檔。
目標 IPv6 位址 / 字首長度	輸入此固定路由的 IP 位址以及字首的長度。
閘道 IPv6 位址	輸入此固定路由的閘道位址。

## 網路介面

使用下拉式清單指定單一介面作為固定路由的通過介面。



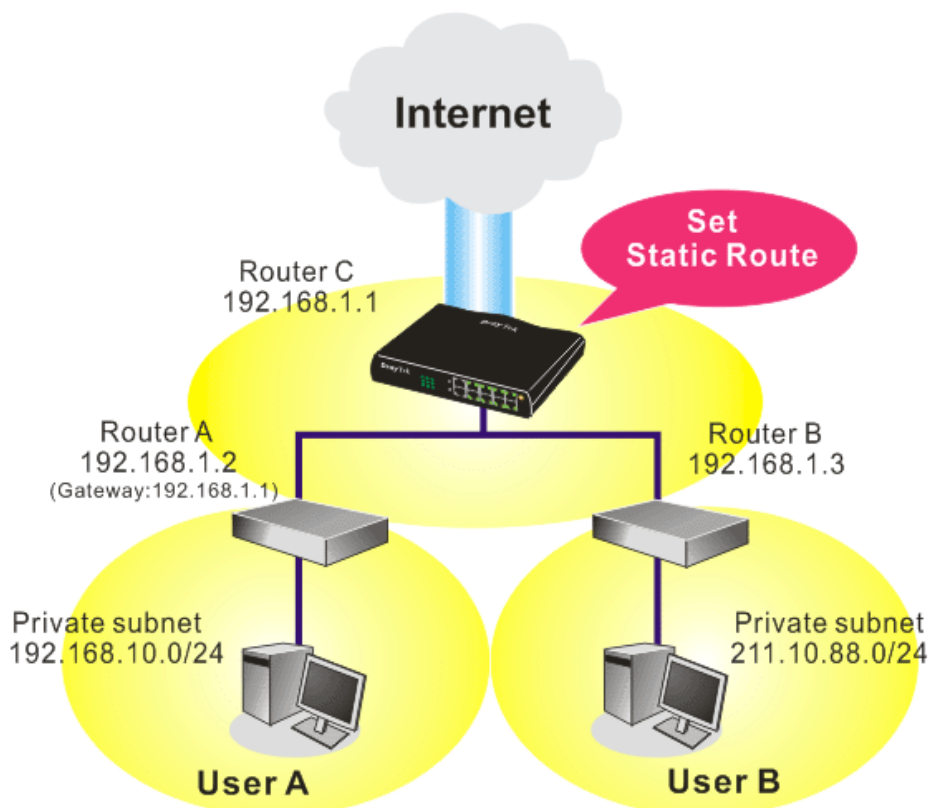
在您完成上述的設定之後，請按**確定**按鈕來啟動設定。

## 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 為路由器 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**群組中，選擇**一般設定**。再選擇第一子網路作為**RIP 協定控制**，然後點選**確定**按鈕。

**注意：**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**區域網路**群組中，選擇固定路由，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**。

**區域網路 >> 固定路由設定**

**索引編號 1**

<input checked="" type="checkbox"/> 啟用	
目的 IP 位址	192.168.1.10
子網路遮罩	255.255.255.0
閘道 IP 位址	192.168.1.2
網路介面	LAN1

3. 回到**固定路由**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**。

**區域網路 >> 固定路由設定**

**索引編號 2**

<input checked="" type="checkbox"/> 啟用	
目的 IP 位址	211.100.88.0
子網路遮罩	255.255.255.0
閘道 IP 位址	192.168.1.3
網路介面	LAN1

4. 按**自我診斷工具**中的**路由表**檢查目前的路由表格。

**自我診斷工具 >> 檢視路由表**

目前執行中的路由表	IPv6路由表	更新頁面
Key: C - connected, S - static, R - RIP, * - default, ~ - private		
S~ 192.168.10.0/ 255.255.255.0	via 192.168.1.2	LAN1
C~ 192.168.1.0/ 255.255.255.0	directly connected	LAN1
S~ 211.100.88.0/ 255.255.255.0	via 192.168.1.3	LAN1

## 4.2.4 VLAN (虛擬區域網路)

過 LAN 端，Vigor 路由器提供任何伺服器或是本地 PC 高速連線進行資料傳輸，在配有無線功能的機種上，每個無線 SSID 亦可分別歸類於 VLAN 之下。

### 以標籤為主的 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

相對於以標籤(Tag)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(P1 ~ P5)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。請開啓區域網路>>VLAN，可出現如下頁面，勾選啓用方塊啓動 VLAN 功能。

區域網路 >> VLAN 設定

#### VLAN 設定

	LAN					無線區域網路(2.4GHz)				無線區域網路(5GHz)				子網路	VLAN 標籤		
	P1	P2	P3	P4	P5	SSID1	SSID2	SSID3	SSID4	SSID1	SSID2	SSID3	SSID4		啟用	VID	優先權
VLAN0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN1	<input type="checkbox"/>	0	0
VLAN1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN1	<input type="checkbox"/>	0	0
VLAN2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN1	<input type="checkbox"/>	0	0
VLAN3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN1	<input type="checkbox"/>	0	0
VLAN4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN1	<input type="checkbox"/>	0	0
VLAN5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN1	<input type="checkbox"/>	0	0
VLAN6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN1	<input type="checkbox"/>	0	0
VLAN7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN1	<input type="checkbox"/>	0	0

允許P1中未加標籤的裝置存取路由器

- 針對每個 VLAN 行列來說，如果勾選了啟用VLAN標籤，那麼相應VID設定將會套用到有線LAN的流量上。
- 無線網路流量通常不含標籤，但仍是選定的VLAN群組的成員。
- 每個 VID都必須是獨一無二。

確定

清除

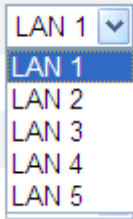
取消

**注意：**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
啓用	勾選此框啓用 VLAN 設定。
LAN	P1 – P5 – 勾選準備納入此 VLAN 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

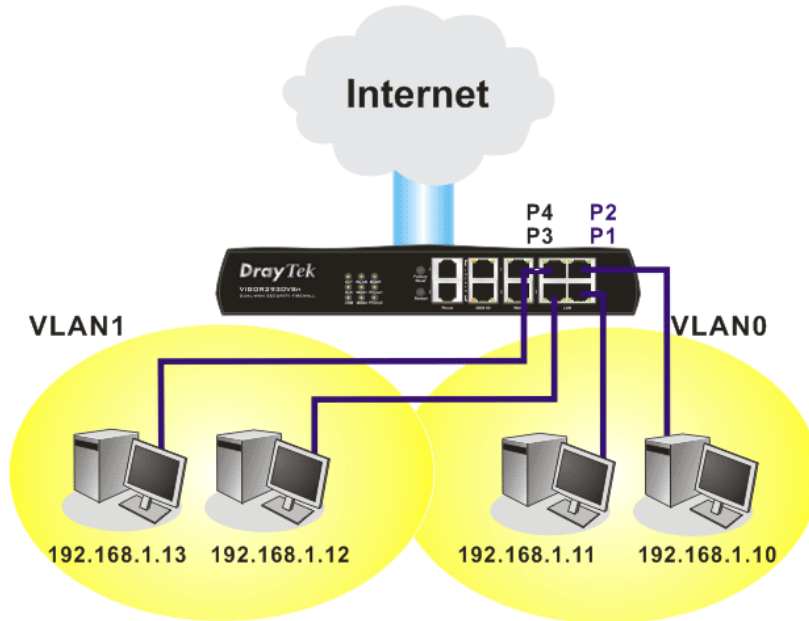


	方框。
無線區域網路(5GHz)	<p><b>SSID1 – SSID4</b> – 勾選準備納入此 VLAN 群組下的 SSID 方框。</p> <p>此項目僅適用 Vigor2925Vn-plus /Vigor2925n-plus。</p>
子網路	<p>選擇其中一個埠口讓選定的 VLAN 僅對應至此。例如，LAN1 指定為 VLAN0，就表示在 VLAN0 底下的電腦可透過此子網來取得 IP 位址。</p> 
VLAN 標籤	<p><b>啓用</b> – 勾選此框啓用 VLAN 標籤功能。</p> <p>區域網路中向外傳送的封包，路由器將指定 VLAN 號碼至全部封包上。</p> <p>請輸入標籤值並指定其優先權。</p> <p><b>VID</b> – 輸入 VLAN ID 號碼值，範圍是 0 到 4095。</p> <p><b>優先權</b> – 選擇此 VLAN 的優先權，範圍是 0 到 7。</p>
允許 P1 中未加標籤的裝置存取路由器	<p>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。建議啓用管理埠口(LAN1)以確保資料傳輸保持暢通。</p>

**注意:**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。

新增或移除 VLAN，請參考下述範例：

- VLAN 0 由 P1 和 P2 組成，VLAN1 由 P3 和 P4 組成。



- 在啓用 VLAN 功能之後，請按照下述範例頁面勾選所需的方塊。

區域網路 >> VLAN 設定

VLAN 設定

VLAN 設定	LAN					無線區域網路(2.4GHz)				無線區域網路(5GHz)				VLAN 標籤			
	P1	P2	P3	P4	P5	SSID1	SSID2	SSID3	SSID4	SSID1	SSID2	SSID3	SSID4	子網路	啟用	VID	優先權
VLAN0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN1	<input type="checkbox"/>	0	0
VLAN1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN2	<input checked="" type="checkbox"/>	10	0
VLAN2	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN3	<input checked="" type="checkbox"/>	20	0
VLAN3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN4	<input checked="" type="checkbox"/>	30	0
VLAN4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN5	<input checked="" type="checkbox"/>	40	0
VLAN5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN1	<input type="checkbox"/>	0	0
VLAN6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN1	<input type="checkbox"/>	0	0
VLAN7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN1	<input type="checkbox"/>	0	0

允許P1中未加標籤的裝置存取路由器

- 針對每個 VLAN 行列來說，如果勾選了啟用VLAN標籤，那麼相應VID設定將會套用到有線LAN的流量上。
- 無線網路流量通常不含標籤，但仍是選定的VLAN群組的成員。
- 每個 VID都必須是獨一無二。

確定 清除 取消

路由器於區域網路端支援高達數個虛擬 IP 子網，每個子網可以是隔離的也可以是共享的，對於公司部門來說是很理想的應用方式。

區域網路 >> 基本設定

基本設定

索引編號	狀態	DHCP	IP 位址		
LAN 1	V	V	192.168.1.1	<a href="#">細節設定</a>	IPv6
LAN 2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.2.1	<a href="#">細節設定</a>	
LAN 3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.3.1	<a href="#">細節設定</a>	
LAN 4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.4.1	<a href="#">細節設定</a>	
LAN 5	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.5.1	<a href="#">細節設定</a>	
DMZ	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.6.1	<a href="#">細節設定</a>	
IP 路由子網	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.0.1	<a href="#">細節設定</a>	

**進階** 您可以在此設定 DHCP options -

強迫路由器使用 "DNS 伺服器 IP 位址" 設定 LAN1

Inter-LAN 路由

子網路	LAN 1	LAN 2	LAN 3	LAN 4	LAN 5
LAN1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LAN2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LAN3	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LAN4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
LAN5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

## 4.2.5 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。當此一功能啓用時，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。

按區域網路並選擇綁定 IP 與 MAC 位址開啓設定網頁。

區域網路 >> 綁定 IP 與 MAC 位址

### 綁定 IP 與 MAC 位址

啟用  停用  限制綁定

#### ARP 表

[全選](#) | [排序](#) | [更新頁面](#)

IP 位址	MAC 位址
192.168.1.5	00-05-5D-E4-D8-EE

#### IP 綁定清單 (限制: 300 輸入項)

[全選](#) | [排序](#)

索引編號	IP 位址	MAC 位址
------	-------	--------

**新增或是更新**

IP 位址:

MAC 位址: -----

說明:

顯示說明

**附註:** IP-MAC 綁定後，DHCP 的配發，將依該清單分配。  
如果選擇了限制綁定項目，任何一個未與 MAC 綁定的 IP 即無法存取網際網路。

可用設定說明如下：

項目	說明
啟用	按此鈕啓用此功能，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。
限制綁定	按此鈕封鎖未列在 IP 綁定清單中的 IP/MAC 位址連線。
ARP 表	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。
全選	按此連結選擇表格內全部內容。
排序	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。

新增與更新	<b>IP 位址</b> - 輸入 IP 位址以作為指定 MAC 位址之用。 <b>MAC 位址</b> - 輸入 MAC 位址以便與指定的 IP 位址綁在一起。
IP 綁定清單	顯示綁定 IP 至 MAC 資訊清單。
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 <b>IP 綁定清單</b> 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 <b>IP 綁定清單</b> 上任何一個項目，選擇您想刪除的項目然後按 <b>刪除</b> 按鈕，選定的項目將自 <b>IP 綁定清單</b> 上刪除。
備份(Backup)	將設定檔儲存成檔案。
還原(Restore)	將原先已存之設定檔套用至本頁。

**附註:** 在您選擇**限制綁定**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。

## 4.2.6 埠口監控

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。

區域網路 >> 埠口監控

### 埠口監控

監控功能:							
<input checked="" type="radio"/> 啟用 <input type="radio"/> 停用							
	Port1	Port2	Port3	Port4	Port5	WAN1	WAN2
監控埠口		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>		
被監控傳輸埠口	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
被監控接收埠口	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**附註:** 已經透過軟體完成WAN1或是WAN2的監控事宜，因此將會使得成效大為降低。

確定

可用設定說明如下：

項目	說明
埠號監控	按下 <b>啟用</b> 可啟動此功能，或是按下 <b>停用</b> 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。
被監控傳輸埠口	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。
---------	------------------------

在您完成上述的設定之後，請按**確定**按鈕來啟動設定。

## 4.2.7 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。

區域網路 >> 有線 802.1x

### 有線 802.1x

LAN 802.1x:

啟用

802.1x 埠號:

P1       P2       P3       P4       P5

請注意，用802.1x 的LAN埠口僅支援一台網路裝置的EAPOL 驗證，因此，啟用802.1x 的LAN埠口於連接至L2交換機時，會出現一些問題，如果您想要802.1x支援多重網路裝置，請在此停用802.1x並在連接的交換器上設定802.1x。此功能支援PEAP 與 EAP-TLS。

確定

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。

在您完成上述的設定之後，請按**確定**按鈕來啟動設定。

## 4.2.8 客製化入口網站設定

本頁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。

### LAN >> 客製化入口網站設定

#### 客製化入口網站清單:

設定檔	狀態	介面	
1.	停用	無	預覽
2.	停用	無	預覽
3.	停用	無	預覽
4.	停用	無	預覽

附註：當準備重新導向網頁時，必須先啟動網際網路連線。

每個項目說明如下：

項目	說明
設定檔	顯示可讓您開啓頁面設定內容的數字連結。
狀態	顯示設定檔的內容(停用、URL 重新導向或是訊息)。
介面	顯示設定檔的套用介面。
預視	依照本頁設定開啓預視窗。

如要設定設定檔，請按下任一索引編號連結開啓如下設定頁面：

### LAN >> 客製化入口網站設定

#### 設定檔索引編號: 1

停用  
 URL 重新導向  
 訊息

例如 http://www.draytek.com  
 附註：如果使用者管理應用已經啓動，將使本頁功能設定失效。

```

<h1><font color="red">Vigor</font></h1><h2> - Reliable connectivity</h2><h2> - Robust firewall protection</h2><h2> - Multi-site secure communication</h2>
          
```

(最多 511 字元)

套用介面

LAN1    LAN2    LAN3    LAN4    LAN5  
 SSID1    SSID2    SSID3    SSID4

可用設定說明如下：

項目	說明
----	----

停用	按下此鈕關閉此功能。
URL 重新導向	任何想要透過此路由器存取網際網路時，都會被導引至此指定的 URL 頁面上，對於打廣告的目的來說可輕易達成效果。例如，強迫旅館內的無線用戶進入旅館業者希望住戶造訪的網頁。
訊息	在此輸入字句，此處所輸入的訊息將會在無線用戶登入網際網路時，顯示在其使用的螢幕上數秒鐘。
套用介面	勾選需要的介面方塊以變套用此設定檔內容。 優點是每個 LAN (1/2/3/4/5) 介面與/或每個無線網路的 SSID (1/2/3/4) 都可分別套用不同的入口網站設定。

在您完成上述的設定之後，請按**確定**按鈕來啟動設定。



## 4.3 負載平衡/策略路由

負載平衡/路由策略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。

### 負載平衡/路由策略



#### 負載平衡/路由策略

10

每頁規則數

回復出廠預設值

索引編號	啟用	協定	介面	優先權	來源 IP 起點	來源 IP 終點	目標 IP 起點	目標 IP 終點	目標埠號起點	目標埠號終點	上移	下移
1	<input type="checkbox"/>	任意	WAN1	200	任意	任意	任意	任意	任意	任意		下
2	<input type="checkbox"/>	任意	WAN1	200	任意	任意	任意	任意	任意	任意	上	下
3	<input type="checkbox"/>	任意	WAN1	200	任意	任意	任意	任意	任意	任意	上	下
4	<input type="checkbox"/>	任意	WAN1	200	任意	任意	任意	任意	任意	任意	上	下
5	<input type="checkbox"/>	任意	WAN1	200	任意	任意	任意	任意	任意	任意	上	下
6	<input type="checkbox"/>	任意	WAN1	200	任意	任意	任意	任意	任意	任意	上	下
7	<input type="checkbox"/>	任意	WAN1	200	任意	任意	任意	任意	任意	任意	上	下
8	<input type="checkbox"/>	任意	WAN1	200	任意	任意	任意	任意	任意	任意	上	下
9	<input type="checkbox"/>	任意	WAN1	200	任意	任意	任意	任意	任意	任意	上	下
10	<input type="checkbox"/>	任意	WAN1	200	任意	任意	任意	任意	任意	任意	上	下

<< 1-10 | 11-20 | 21-30 | 31-40 | 41-50 >>

前一頁 >>

- 精靈設定模式：以三個頁面呈現最常使用的設定
- 進階模式：一頁含全部設定

確定

可用設定說明如下：

項目	說明
索引編號	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。
協定	顯示用於此策略的協定內容。
介面	顯示此策略指定的封包傳送的介面。
介面位址	顯示 WAN IP 或是 WAN IP 別名位址，作為對外封包的來源 IP 位址。
來源 IP 起點	顯示來源 IP 的起始 IP 位址。
來源 IP 終點	顯示來源 IP 的結束 IP 位址。
目標 IP 起點	顯示目標 IP 的起始 IP 位址。
目標 IP 終點	顯示目標 IP 的結束 IP 位址。

目標埠號起點	顯示目標埠號的起始埠號。
目標埠號終點	顯示目標埠號的結束埠號。
上移/下移	使用上移下移連結來移動策略路由的順序。

按下索引編號 1 進入如下頁面進行設定。

#### 負載平衡/路由策略

##### 索引編號: 1

啟用

**設定原則**

---

協定 任意 ▾

來源 IP

任意

來源 IP 起點 來源 IP 終點

[ ] ~ [ ]

目的地 IP

任意

目標 IP 起點 目標 IP 終點

[ ] ~ [ ]

目的地埠號

任意

目標埠號起點 目標埠號終點

[ ] ~ [ ]

**若符合上述原則，請傳往**

---

介面 WAN1 ▾

開道 IP

預設開道

指定開道 [ ]

**更多...**

---

自動備援至其它 WAN 封包轉送至 WAN

強迫 NAT

強迫路由

可用設定說明如下：

項目	說明
啟用	勾選此框啟用此策略。
協定	使用下拉式清單選擇 WAN 介面適當的協定。 
來源 IP	任意 - 任何 IP 都視為來源 IP。 來源 IP 起點 - 輸入來源 IP 起點。 來源 IP 終點 - 輸入來源 IP 終點。
目的 IP	任意 - 任何 IP 都視為目標 IP。

項目	說明
	<b>目標 IP 起點</b> - 輸入目標 IP 起點。 <b>目標 IP 終點</b> - 輸入目標 IP 終點。
目的埠號	<b>任意</b> - 任何埠號都適用。 <b>目標埠號起點</b> - 輸入目標埠號的起點。 <b>目標埠號終點</b> - 輸入目標埠號的終點。
若符合上述原則，請轉往	<b>介面</b> - 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。 <b>閘道 IP</b> - 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。
更多...	<b>自動備援至其它 WAN</b> - 勾選此框可讓選擇的 WAN 口中斷連線時，將資料自動利用其它 WAN 口來傳送。 <b>封包轉送至 WAN</b> - 請選擇 <b>強迫 NAT</b> 或是 <b>強迫路由</b> 。

當您完成設定之後，按下**確定**按鈕儲存並離開此頁面。

## 4.4 NAT

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

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

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。

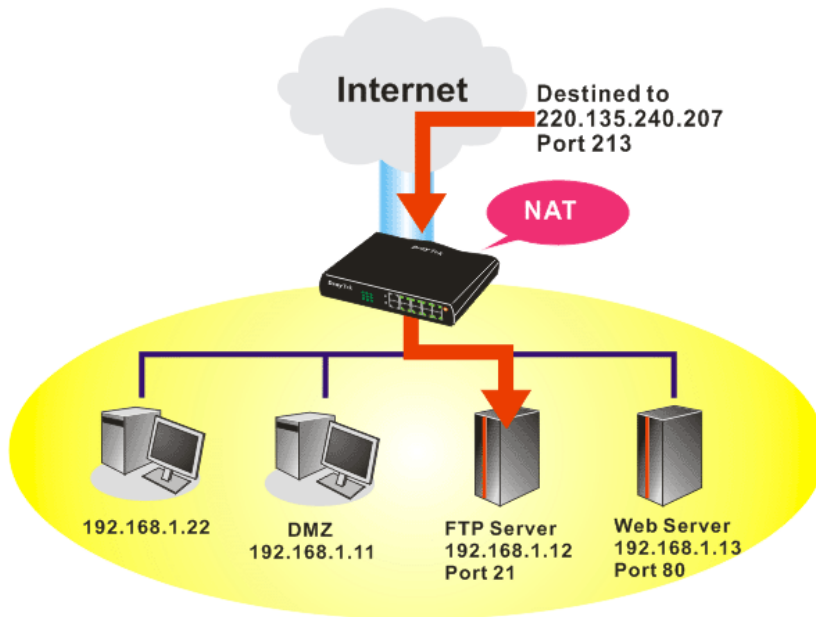
在 NAT 頁面中，您將可看見以 RFC-1918 定義的虛擬 IP 位址，通常我們會使用 192.168.1.0/24 子網路給予路由器使用。就如前所提及的一般，NAT 功能可以對應一或多個 IP 位址和/或服務通訊埠到不同的服務上，換句話說，NAT 功能可以利用通訊埠對應方式來達成。

下圖為 NAT 功能項目：



#### 4.4.1 通訊埠重導向

**通訊埠重導向**通常是為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，請開啓 **NAT** 頁面然後選擇**通訊埠重導向**。**通訊埠重導向**提供 20 組通訊埠對應入口給予內部主機對應使用。

**NAT >>通訊埠重導向**

通訊埠重導向						回復出廠預設值
索引編號	服務名稱	WAN 介面	協定	對外通訊埠	虛擬 IP	狀態
1.		全部				×
2.		全部				×
3.		全部				×
4.		全部				×
5.		全部				×
6.		全部				×
7.		全部				×
8.		全部				×
9.		全部				×
10.		全部				×

<< 1-10 | 11-20 >>

下一頁 >>

可用設定說明如下：

項目	說明
索引編號	顯示設定檔的編號。

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。
協定	顯示使用的協定類別 (TCP 或是 UDP)。
對外通訊埠	顯示將被導引至指定的內部主機的虛擬 IP 及埠口的埠號。
虛擬 IP	顯示提供此服務之內主機的 IP 位址。
狀態	顯示設定檔目前是啟用(v) 或是停用 (x)。

按下索引編號下的號碼連結，進入次層之設定頁面:

#### NAT >> 通訊埠重導向

##### 索引編號. 1

<input type="checkbox"/> 啟用	
模式	單一
服務名稱	單一
通訊協定	範圍
WAN IP	1.全部
對外通訊埠	0
虛擬 IP	
虛擬通訊埠	0

附註：在 "範圍" 模式下，一旦輸入對外通訊埠與起始IP值後，結束 IP 將會自動計算出來。

確定 清除 取消

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 <b>範圍</b> 。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 IP	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 <b>全部</b> ，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。
對外通訊埠	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 <b>範圍</b> 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(作為起點)及第二個方塊(作為終點)輸入需要的數值。
虛擬 IP	指定提供服務的主機之 IP 位址，如果您選擇 <b>範圍</b> 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，稍後系統將自動指定第二個方塊的內容。

## 虛擬通訊埠

指定內部主機提供服務之虛擬通訊埠號。

在您完成上述的設定之後，請按**確定**按鈕來儲存設定。

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。

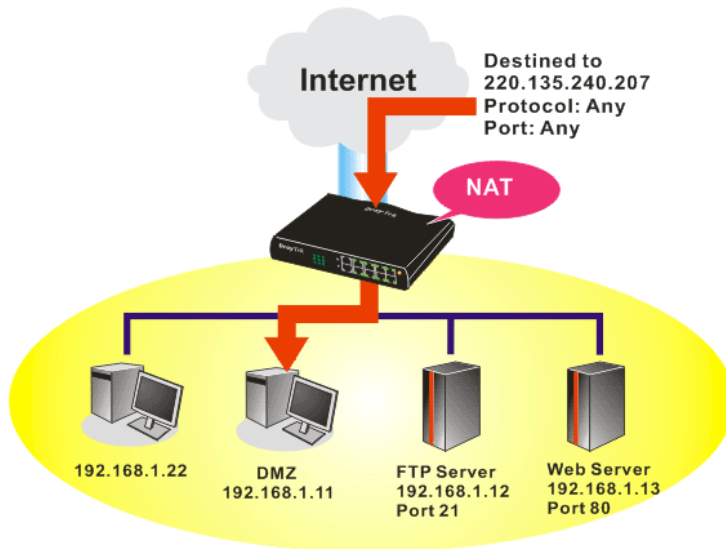
系統維護 >> 管理

IPv4 管理設定		IPv6 管理設定	
路由器名稱 <input type="text"/>		<b>管理通訊埠設定</b>	
<b>管理存取控制</b>		<input checked="" type="radio"/> 使用者定義通訊埠 <input type="radio"/> 預設通訊埠	
<input type="checkbox"/> 允許從網際網路管理		Telnet 通訊埠 <input type="text" value="23"/> (預設值: 23)	
<input type="checkbox"/> FTP 通訊埠		HTTP 通訊埠 <input type="text" value="80"/> (預設值: 80)	
<input checked="" type="checkbox"/> HTTP 通訊埠		HTTPS 通訊埠 <input type="text" value="443"/> (預設值: 443)	
<input checked="" type="checkbox"/> HTTPS 通訊埠		FTP 通訊埠 <input type="text" value="21"/> (預設值: 21)	
<input checked="" type="checkbox"/> Telnet 通訊埠		SSH 通訊埠 <input type="text" value="22"/> (預設值: 22)	
<input type="checkbox"/> SSH 通訊埠			
<input checked="" type="checkbox"/> 停用來自外部網際網路的PING			
<b>存取清單</b>			
清單	IP	子網路遮罩	
1	<input type="text"/>	<input type="text"/>	
2	<input type="text"/>	<input type="text"/>	
3	<input type="text"/>	<input type="text"/>	

確定

## 4.4.2 DMZ 主機設定

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。



**注意：**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。


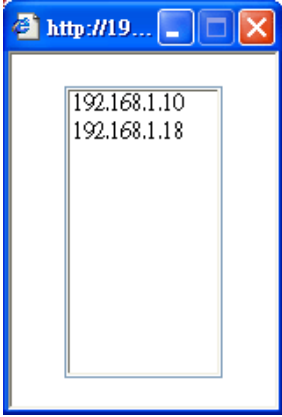
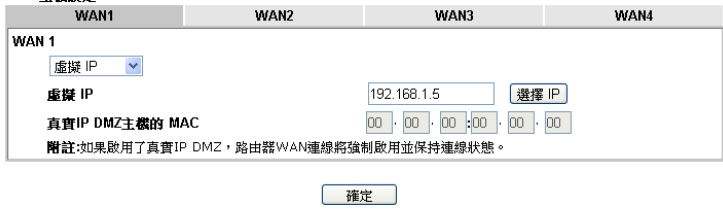
請按 **DMZ 主機設定** 開啓下述頁面，WAN.您可以針對每個 WAN 界面設定不同的 DMZ 主機，按下 WAN 標籤即可切換到各個不同 WAN 設定頁面。

NAT >>DMZ 主機設定

DMZ 主機設定

WAN1	WAN2	WAN3	WAN4
<b>WAN 1</b>			
虛擬 IP <input type="button" value="選擇 IP"/>			
真實 IP DMZ主機的 MAC <input type="text" value="00"/> <input type="text" value="00"/> <input type="text" value="00"/> <input type="text" value="00"/> <input type="text" value="00"/> <input type="text" value="00"/>			
附註:如果啟用了真實IP DMZ，路由器WAN連線將強制啟用並保持連線狀態。			
<input type="button" value="確定"/>			

可用設定說明如下：

項目	說明
	<p>請先選擇<b>虛擬 IP</b> 或是<b>真實 IP</b>。<b>真實 IP</b> 選項僅適用於 WAN1。</p>
<p><b>虛擬 IP</b></p>	<p>輸入 DMZ 主機的<b>虛擬 IP</b> 位址，或是按<b>選擇 PC</b> 開啓另一頁面來選擇。</p>
<p><b>選擇 IP</b></p>	<p>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<b>虛擬 IP</b> 位址清單，請自清單中選擇一個<b>虛擬 IP</b> 位址作為 DMZ 主機。</p>  <p>當您已經從上面的視窗選好了<b>虛擬 IP</b> 位址時，該 IP 位址將會顯示在下面的螢幕上，請按<b>確定</b>儲存這些設定。</p> <p>NAT &gt;&gt;DMZ 主機設定</p> 

WAN2~WAN4 的 DMZ 主機頁面和 WAN1 有些許不同，**真實 IP** 選項僅適用 WAN1。

NAT >>DMZ 主機設定

DMZ 主機設定

WAN1	WAN2	WAN3	WAN4
<p><b>WAN 2</b></p> <p>開啟 <input type="checkbox"/></p>	<p><b>虛擬 IP</b></p> <p>0.0.0.0</p>		<p>選擇 IP</p>
<p>確定</p>			



如果您在網際網路連線設定選擇 PPPoE/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 主機設定

DMZ 主機設定				
WAN1		WAN2		WAN4
<b>WAN 2</b>				
索引編號	開啟	輔助 WAN IP	虛擬 IP	
1.	<input type="checkbox"/>	---	0.0.0.0	<input type="button" value="選擇 IP"/>
2.	<input type="checkbox"/>	192.168.1.56	0.0.0.0	<input type="button" value="選擇 IP"/>

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。																														
輔助 WAN IP	顯示輔助 WAN IP 的位址。																														
虛擬 IP	輸入 DMZ 主機的虛擬 IP 位址，或是按 <b>選擇 PC</b> 開啓另一頁面來選擇。																														
選擇電腦	<p>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。</p>  <p>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<b>確定</b>儲存這些設定。</p> <p>NAT &gt;&gt;DMZ 主機設定</p> <table border="1"> <thead> <tr> <th colspan="5">DMZ 主機設定</th> </tr> <tr> <th colspan="2">WAN1</th> <th colspan="2">WAN2</th> <th>WAN3</th> </tr> </thead> <tbody> <tr> <td colspan="5"><b>WAN 1</b></td> </tr> <tr> <th>索引編號</th> <th>開啟</th> <th>輔助 WAN IP</th> <th>虛擬 IP</th> <th></th> </tr> <tr> <td>1.</td> <td><input type="checkbox"/></td> <td>---</td> <td>0.0.0.0</td> <td><input type="button" value="選擇電腦"/></td> </tr> <tr> <td>2.</td> <td><input checked="" type="checkbox"/></td> <td>192.168.1.55</td> <td>192.168.1.5</td> <td><input type="button" value="選擇電腦"/></td> </tr> </tbody> </table> <p style="text-align: center;"> <input type="button" value="確定"/> <input type="button" value="清除"/> </p>	DMZ 主機設定					WAN1		WAN2		WAN3	<b>WAN 1</b>					索引編號	開啟	輔助 WAN IP	虛擬 IP		1.	<input type="checkbox"/>	---	0.0.0.0	<input type="button" value="選擇電腦"/>	2.	<input checked="" type="checkbox"/>	192.168.1.55	192.168.1.5	<input type="button" value="選擇電腦"/>
DMZ 主機設定																															
WAN1		WAN2		WAN3																											
<b>WAN 1</b>																															
索引編號	開啟	輔助 WAN IP	虛擬 IP																												
1.	<input type="checkbox"/>	---	0.0.0.0	<input type="button" value="選擇電腦"/>																											
2.	<input checked="" type="checkbox"/>	192.168.1.55	192.168.1.5	<input type="button" value="選擇電腦"/>																											

在您完成上述的設定之後，請按**確定**按鈕來儲存設定。

### 4.4.3 開放通訊埠

開放通訊埠允許您開啓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，以免成爲安全事件的受害者。

按**開放通訊埠**連結開啓下麵的網頁。

NAT >>開放通訊埠

開放通訊埠設定						<a href="#">  回復出廠預設值  </a>
索引編號	註解	WAN 介面	輔助 WAN IP	內部 IP 位址	狀態	
<a href="#">1.</a>					X	
<a href="#">2.</a>					X	
<a href="#">3.</a>					X	
<a href="#">4.</a>					X	
<a href="#">5.</a>					X	
<a href="#">6.</a>					X	
<a href="#">7.</a>					X	
<a href="#">8.</a>					X	
<a href="#">9.</a>					X	
<a href="#">10.</a>					X	

<< [1-10](#) | [11-20](#) >> [下一頁 >>](#)

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。
註解	指定特定網路服務的名稱。
輔助 WAN IP	此欄位僅在您已設定輔助 WAN IP 後才會顯示出來。
內部 IP 位址	顯示提供此項服務之本地主機的 IP 位址。
狀態	顯示每項設定的狀態，X 或 V 表示關閉或是啓用狀態。

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。

## 索引編號 2

<input checked="" type="checkbox"/> 啟用開放通訊埠
說明 <input type="text"/>
WAN 介面 <input type="text" value="WAN1"/>
虛擬 IP <input type="text"/> <input type="button" value="選擇 IP"/>

	通訊協定	起始通訊埠	結束通訊埠		通訊協定	起始通訊埠	結束通訊埠
1.	<input type="text" value="-----"/> <input type="button" value="v"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	2.	<input type="text" value="-----"/> <input type="button" value="v"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
3.	<input type="text" value="-----"/> <input type="button" value="v"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	4.	<input type="text" value="-----"/> <input type="button" value="v"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
5.	<input type="text" value="-----"/> <input type="button" value="v"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	6.	<input type="text" value="-----"/> <input type="button" value="v"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
7.	<input type="text" value="-----"/> <input type="button" value="v"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	8.	<input type="text" value="-----"/> <input type="button" value="v"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
9.	<input type="text" value="-----"/> <input type="button" value="v"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	10.	<input type="text" value="-----"/> <input type="button" value="v"/>	<input type="text" value="0"/>	<input type="text" value="0"/>

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。
說明	請為所定義的網路應用/服務命名。
WAN 介面	指定該項設定之 WAN 介面。
WAN IP	如果您在網際網路連線設定選擇 PPPoE/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 位址或是按選擇電腦挑選另外一個。
選擇電腦	按此鈕後另一個視窗即自動跳出並提供本機的虛擬 IP 位址之清單資料，請自清單中選取最適宜的 IP 位址。
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。
起始通訊埠	指定本機所提供之服務的開始通訊埠號。
結束通訊埠	指定本機所提供之服務的結束通訊埠號。

在您完成上述的設定之後，請按**確定**按鈕來儲存設定。

#### 4.4.4 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啓狀態。
- 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啓相關埠口。

- 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 秒

UDP: 180 秒

IGMP: 10 秒

TCP WWW: 60 秒

TCP SYN: 60 秒

**NAT >> 通訊埠觸發**

通訊埠觸發						回復出廠預設值
索引編號	說明	觸發協定	觸發通訊埠	輸入協定	輸入通訊埠	狀態
1.						X
2.						X
3.						X
4.						X
5.						X
6.						X
7.						X
8.						X
9.						X
10.						X

<< 1-10 | 11-20 >> >> 下一頁 >>

可用設定說明如下：


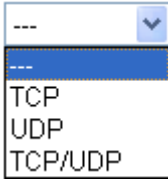

項目	說明
說明	顯示與此規則相關的說明內容。
觸發協定	顯示觸發封包使用的協定。
觸發通訊埠	顯示觸發封包使用的埠號。
輸入協定	顯示觸發設定檔輸入資料使用的協定。
輸入通訊埠	顯示觸發設定檔輸入資料使用的埠號。
狀態	顯示此規則目前是啓用狀態還是停用狀態。

按下任一索引連結開啓設定頁面：

編號. 1

<input type="checkbox"/> 啟用	
服務	使用者定義
說明	
觸發協定	TCP
觸發通訊埠	80
輸入協定	UDP
輸入通訊埠	1024
<p><b>注意:</b>觸發通訊埠與輸入通訊埠應輸入如下形式： 123-456,777-789 (合法),123-456,789 (合法), 但是 123-456-789 (不合法).</p>	

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。 
說明	輸入此設定檔需要特別說明的內容。
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）。 
觸發通訊埠	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。 

輸入通訊埠	輸入封包的埠號或是埠號範圍。
-------	----------------

在您完成上述的設定之後，請按**確定**按鈕來儲存設定。

## 4.5 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，此項功能只支援 128 條連線數的網路流量(進與出)，有三種模式可以選擇，停用、自動及手動。

### 4.5.1 設定

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。開啓硬體加速>>設定。

#### 硬體加速 >> 設定

**模式:**


**協定:**  TCP  UDP

**選項:**
 加速流量最大的連線數  
 應用 **類型規則** (QoS)  
 指定主機:

索引編號	啟用	開始埠號	結束埠號	虛擬 IP
1.	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text"/> <input type="button" value="選擇電腦"/>
2.	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text"/> <input type="button" value="選擇電腦"/>
3.	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text"/> <input type="button" value="選擇電腦"/>
4.	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text"/> <input type="button" value="選擇電腦"/>
5.	<input type="checkbox"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text"/> <input type="button" value="選擇電腦"/>

附註: 若硬體加速已啟用，頻寬管理將失效。

可用設定說明如下：

項目	說明
模式	<p><b>自動</b> - 硬體加速如果採用自動模式，就會加進最重承載連線數以及較低的延遲流量，不過，自動模式不支援 UDP 協定。</p> <p><b>手動</b> - 手動模式會實施三個次要項目-<i>加速流量最大的連線數</i>、<i>應用類型規則 (QoS)</i> 以及<i>指定主機</i>，每個次項都支援 TCP 與 UDP 協定。</p> 
協定	有二種協定可以選擇，TCP 與 UDP。
選項	<p><b>加速流量最大的連線數</b> - 此選項僅適用於自動模式，它也是 UDP 協定唯一支援的選項。</p> <p><b>應用類型規則(QoS)</b> - 使用者可以套用 QoS 所提供的規則。</p> <p><b>注意:</b> 請造訪居易網站可以獲得更多 QoS 相關資訊。</p>

類寬管理 >> 服務品質

**編輯規則**

啟用  硬體加速

乙太網路類型  IPv4  IPv6

本機地址 Any

遠端位址 Any

**指定主機** – 這個選項提供了 5 台主機以便加入 NAT 連線數。由於硬體加速僅支援 128 條連線數，這些主機全都得共享才行，因此，相關運作的成效會比單一主機要來的低。選擇此項目來指定區域網路中特定電腦來套用硬體加速。

- 啟用 – 勾選方框讓指定電腦套用硬體加速功能。
- 開始埠號 – 輸入區域網路中的電腦起始埠號。
- 結束埠號 – 輸入區域網路中的電腦結束埠號。
- 虛擬 IP/選擇電腦 – 輸入選定主機的 IP 位址，或是按下選擇電腦按鈕，開啓小視窗選擇您想要指定的 IP 位址。

### 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
*****
MAN 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
```

## 4.6 防火牆

### 4.6.1 防火牆基本常識

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



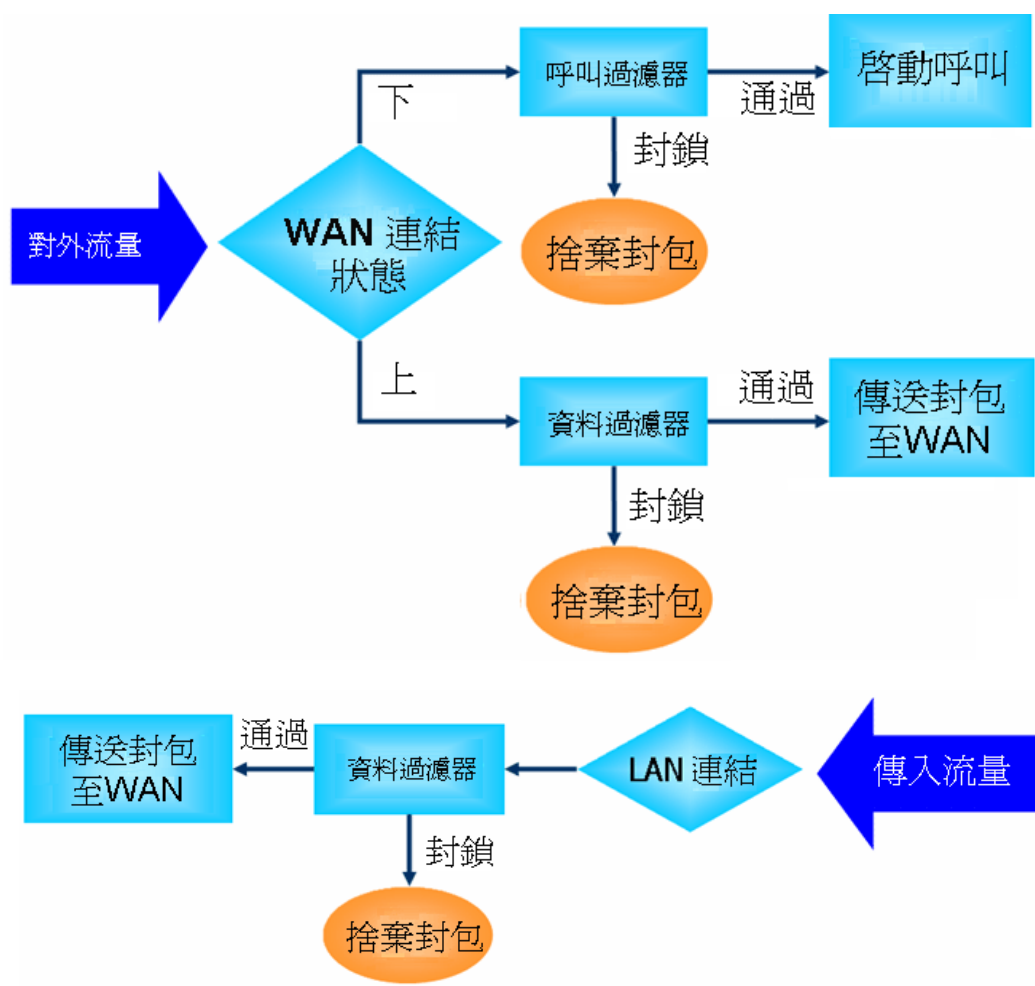
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS)攻擊防禦

## IP 過濾器

依照現有網際網路連線的需求、廣域網路連接狀態(開啓或關閉)的情形，IP 過濾器結構可將資料流量分成二大類：呼叫過濾器和資料過濾器。

- **呼叫過濾器** -當目前沒有任何網際網路連線時，呼叫過濾器可應用在所有的資料運輸流量上，所有的運輸應該是往外送出。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，然後路由器將啓動一次呼叫來建立網際網路連線，再將該封包傳送往網際網路。
- **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 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。

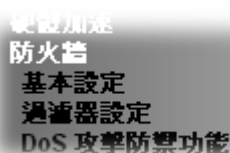
DoS 攻擊防禦功能的引發是以 Vigor 路由器的攻擊特徵值資料庫為基礎，執行每一個封包的檢查，任何可能重複產生以癱瘓主機之惡意封包，在安全的區域網路中都將嚴格阻擋，如果您有設定系統紀錄伺服器，那麼系統紀錄訊息也會傳送警告資訊給您。

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 攻擊  | 9. SYN 封包片段攻         |
| 2. UDP flood 攻擊  | 10. Fraggle 攻擊       |
| 3. ICMP flood 攻擊 | 11. TCP flag scan    |
| 4. Port Scan 攻擊  | 12. Tear drop 攻擊     |
| 5. IP options    | 13. Ping of Death 攻擊 |
| 6. Land 攻擊       | 14. ICMP 封包片段攻       |
| 7. Smurf 攻擊      | 15. 未知通訊協定           |
| 8. 路由追蹤          |                      |

下圖為防火牆的功能項目：



裝置設定  
防火牆  
基本設定  
過濾器設定  
DoS 攻擊防禦功能  
應用程序設定

## 4.6.2 基本設定

基本設定允許您調整 IP 過濾器 and 一般選項的設定內容，在此頁面您可以啓動或是關閉呼叫過濾器或資料過濾器。在某些情況下，您的過濾器可利用連結的方式執行一系列過濾工作，因此在這裡，您只要指定開始過濾器組別即可。當然，您也可以調整紀錄模式設定以及勾選接受流入的 UDP Fragment 封包。

### 基本設定頁面

這個頁面可讓您啓用/停用呼叫過濾器與資料過濾器，決定過濾進出資料的一般規則。

防火牆 >> 基本設定

基本設定

基本設定	預設規則	
呼叫過濾器	<input checked="" type="radio"/> 啟用 <input type="radio"/> 停用	開始過濾器組別 <input type="text" value="組別#1"/>
資料過濾器	<input checked="" type="radio"/> 啟用 <input type="radio"/> 停用	開始過濾器組別 <input type="text" value="組別#2"/>
<input checked="" type="checkbox"/> 接受流入的大量 UDP 或是 ICMP Fragment 封包 (用於某些遊戲中)		
<input checked="" type="checkbox"/> 啟動嚴格安全防火牆策略		
封鎖來自WAN端的路由封包		
<input type="checkbox"/> IPv4 <input checked="" type="checkbox"/> IPv6		
<b>附註:</b> 封包將透過下述各個防火牆功能依序進行過濾：		
1. 資料過濾器設定與規則		
2. 封鎖來自WAN端的路由封包		
3. 預設規則		

可用設定說明如下：

項目	說明
呼叫過濾器	選擇啓用以啓動呼叫過濾器功能，並指定開始過濾器組別。
資料過濾器	選擇啓用以啓動資料過濾器功能，並指定開始過濾器組別。
接受流入的大量 UDP 或是 ICMP Fragment 封包	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，除非您啓動接受流入的大量 UDP 或是 ICMP Fragment 封包，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，您就不要啓動接受流入的大量 UDP 或是 ICMP Fragment 封包功能。

<p><b>啓動嚴格安全防火牆策略</b></p>	<p>爲了安全起見，路由器將會執行嚴格的資料傳輸安全性檢驗動作。</p> <p>此功能在預設狀態下是啓用的，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。</p>
<p><b>封鎖來自 WAN 端的路由封包</b></p>	<p>通常，預設的情況下，系統會接受由 WAN 端流入 LAN 端的 IPv6 網路連線數/流量。</p> <p><b>IPv6</b> - 爲了避免遠端用戶登入 LAN 端的電腦，可勾選此框讓透過 IPv6 而來的封包(由 WAN 端到 LAN 端)可被路由器阻擋下來。對於不由 NAT 轉址而來的路由封包來說這個功能可以有相當不錯的效果。</p> <p><b>IPv4</b> - 爲了避免遠端用戶登入 LAN 端的電腦，可勾選此框讓透過 IPv4 而來的封包可被路由器阻擋下來。對於不由 NAT 轉址而來的路由封包來說這個功能可以有相當不錯的效果。</p>

## 預設規則頁面

本頁讓您選擇過濾設定檔包含 QoS、策略路由、WCF、應用程式管控、URL 內容過濾以便透過路由器進行資料傳輸。

防火牆 >> 基本設定


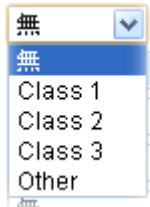
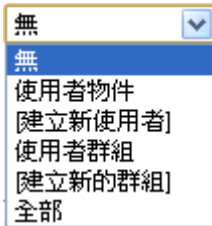
### 基本設定

基本設定		預設規則	
<b>預設規則之動作:</b>			
<b>應用程式</b>	<b>動作/設定</b>		<b>Syslog</b>
<b>過濾器</b>	通過 ▾		<input type="checkbox"/>
<b>連線數控制</b>	0 / 60000		<input type="checkbox"/>
<b>服務品質</b>	無 ▾		<input type="checkbox"/>
<b>使用者管理</b>	無 ▾		<input type="checkbox"/>
<b>應用程式管控</b>	無 ▾		<input type="checkbox"/>
<b>URL 內容過濾器</b>	無 ▾		<input type="checkbox"/>
<b>網頁內容過濾器</b>	無 ▾		<input type="checkbox"/>
<b>DNS 過濾器</b>	無 ▾		<input type="checkbox"/>
進階設定		<input type="button" value="編輯"/>	

確定

取消

可用設定說明如下：

項目	說明
過濾器	<p>本頁可是定預設規則。</p> <p><b>通過</b> - 所有的封包都可通過路由器，不需考慮<b>防火牆</b>&gt;&gt;<b>過濾器</b>的設定內容。</p> <p><b>封鎖</b> - 所有的封包都不許通過路由器，且不需考慮<b>防火牆</b>&gt;&gt;<b>過濾器</b>的設定內容。</p> 
連線數控制	<p>此處輸入的值為全部的封包連線數，預設值為 60000。</p>
服務品質	<p>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。</p> 
使用者管理	<p>本項目僅在<b>使用者管理</b>&gt;&gt;<b>基本設定</b>中選擇<b>規則模式</b>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。</p>  <p><b>注意：</b>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<b>建立新使用者</b>或是<b>建立新的群組</b>選項供您建立新的設定檔。</p>
應用程式管控	<p>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<b>建立新設定</b>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<b>數位內容安全管理</b>&gt;&gt;<b>應用程式管控設定檔</b>章節。</p> <p>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。</p>
URL 內容過濾器	<p>選擇一個 <b>URL 內容過濾器</b>設定檔（在<b>數位內容安全管理 (CSM)</b>&gt;&gt;<b>URL 內容過濾器</b>中所建立），請務必先在<b>數位內容安全管理(CSM)</b>&gt;<b>URL 內容過濾器</b>中設定一個設定檔，或是從下拉式選單中選擇<b>[建立新檔]</b>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/</p>

	郵件警告章節。
網頁內容過濾器	<p>選擇一個<b>網頁內容過濾器</b>設定檔（在<b>數位內容安全管理 (CSM)&gt;&gt; 網頁內容過濾器</b>中所建立），請務必先在<b>數位內容安全管理(CSM)&gt;&gt; 網頁內容過濾器</b>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</p>
DNS 過濾器	<p>選擇一組 DNS 過濾器設定檔(於<b>數位內容安全管理&gt;&gt;DNS 過濾器</b>頁面中建立)，在<b>數位內容安全管理&gt;&gt;網頁內容過濾器設定檔</b>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。</p>
進階設定	<p>按<b>編輯</b>按鈕開啓下述視窗，不過，在此強烈建議您使用預設值為佳。</p> <p><b>防火牆 &gt;&gt; 基本設定</b></p> <div data-bbox="708 869 1385 1120" style="border: 1px solid black; padding: 5px;"> <p>進階設定</p> <p>選擇編碼語系: <input type="text" value="ANSI(1252)-拉丁文 I"/></p> <p>視窗大小: <input type="text" value="65535"/></p> <p>連線數逾時: <input type="text" value="1440"/> 分</p> <p style="text-align: center;"> <input type="button" value="確定"/> <input type="button" value="關閉"/> </p> </div> <p><b>選擇編碼語系</b> - 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。</p> <p>如果您不知道要如何選擇適宜的<b>編碼語系</b>，請開啓 Syslog。從 Setup 對話盒中的<b>編碼語系</b>(codepage)資訊，您將會看到系統建議的 codepage 內容。</p> <div data-bbox="683 1496 1385 1921" style="border: 1px solid gray; padding: 5px;"> </div> <p><b>視窗大小</b> - 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</p>

---

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

---

在您完成上述的設定之後，請按**確定**按鈕來儲存設定。



### 4.6.3 過濾器設定

按**防火牆**並選擇**過濾器設定**以開啓如下的設定網頁。

防火牆 >> 過濾器設定

過濾器設定		回復出廠預設值	
組別	註解	組別	註解
1.	Default Call Filter	7.	
2.	Default Data Filter	8.	
3.		9.	
4.		10.	
5.		11.	
6.		12.	

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**啓用**則可啓動該項規則。

防火牆 >> 過濾器設定 >> 編輯過濾器設定

#### 過濾器組別 1

註解:

過濾器規則	啓用	註解	上移	下移
<input type="button" value="1"/>	<input checked="" type="checkbox"/>	Block NetBios		<input type="button" value="上"/>
<input type="button" value="2"/>	<input type="checkbox"/>		<input type="button" value="上"/>	<input type="button" value="下"/>
<input type="button" value="3"/>	<input type="checkbox"/>		<input type="button" value="上"/>	<input type="button" value="下"/>
<input type="button" value="4"/>	<input type="checkbox"/>		<input type="button" value="上"/>	<input type="button" value="下"/>
<input type="button" value="5"/>	<input type="checkbox"/>		<input type="button" value="上"/>	<input type="button" value="下"/>
<input type="button" value="6"/>	<input type="checkbox"/>		<input type="button" value="上"/>	<input type="button" value="下"/>
<input type="button" value="7"/>	<input type="checkbox"/>		<input type="button" value="上"/>	

下一個過濾器組別

可用設定說明如下：

項目	說明
過濾器規則	請按號碼按鈕(1 ~ 7)編輯過濾器的規則，按下此鈕可以開啓過濾器規則網頁，有關詳細的資訊，請參考稍後的說明。
啓用	啓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。
上移/下移	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。

欲編輯**過濾器規則**，請按過濾器規則索引按鈕以便進入過濾器規則設定網頁。



過濾器組別 1 規則 1

<input checked="" type="checkbox"/> 啟用過濾規則		
註解:	Block NetBios	
索引號碼(1-15) 於 <b>排程</b> 設置:	, , ,	
啟用排程時, 清除連線數:	<input type="checkbox"/> 啟用	
方向:	LAN/DMZ/RT/VPN -> WAN	
來源 IP:	任何	<input type="button" value="編輯"/>
目的 IP:	任何	<input type="button" value="編輯"/>
服務類型:	TCP/UDP, 通訊埠: 自 137~139 至任何	<input type="button" value="編輯"/>
片段:	忽略	
<b>應用程式</b>	<b>動作設定</b>	<b>Syslog</b>
過濾器:	立刻封鎖	<input type="checkbox"/>
分至其他過濾器設定	無	
連線數控制	0 / 60000	<input type="checkbox"/>
IP 與 MAC 綁定	不嚴格的	<input type="checkbox"/>
<b>服務品質</b>	無	<input type="checkbox"/>
<b>使用者管理</b>	無	<input type="checkbox"/>
<b>應用程式管控:</b>	無	<input type="checkbox"/>
<b>URL 內容過濾器:</b>	無	<input type="checkbox"/>
<b>網頁內容過濾器:</b>	無	<input type="checkbox"/>
<b>DNS 過濾器</b>	無	<input type="checkbox"/>
進階設定	<input type="button" value="編輯"/>	

可用設定說明如下：

項目	說明
啟用過濾規則	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。
索引號碼 (1-15)	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 <b>應用-排程</b> 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。
啟用排程時, 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 <b>資料過濾器</b> ，對於 <b>呼叫過濾器</b> 而言，這項設定是不適用的。 <div style="border: 1px solid black; padding: 5px; margin: 5px 0;">                     LAN/DMZ/RT/VPN -&gt; WAN                      LAN/DMZ/RT/VPN -&gt; WAN                      WAN -&gt; LAN/DMZ/RT/VPN                      LAN/DMZ/RT/VPN -&gt; LAN/DMZ/RT/VPN                 </div> 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	按下 <b>編輯</b> 進入如下的畫面，選擇來源/目標 IP 或是 IP 範圍。

### IP 位址編輯

位址形式	任何位址
起始IP位址	0.0.0.0
結束IP位址	0.0.0.0
子網路遮罩	0.0.0.0
反向選擇	<input type="checkbox"/>
IP 群組	無
或是 IP 群組	無
或 IP 物件	無
或 IP 物件	無
IPv6 群組	無
或 IPv6 群組	無
或 IPv6 物件	無
或 IPv6 物件	無

確定 關閉

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，請勾選群組及物件。

任何位址  
任何位址  
單一位址  
位址範圍  
子網路位址  
群組與物件

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。

#### 服務類型編輯

服務類型	使用者自定
協定	TCP/UDP
來源通訊埠	= 137 ~ 139
目的通訊埠	= 1 ~ 65535
服務群組	無
或 服務物件	無
或服務物件	無
或服務物件	無

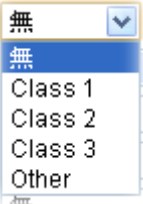
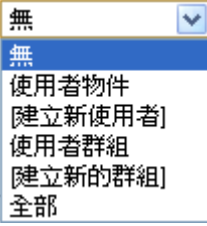
確定 關閉

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，請選擇群組與物件作為服務類型。

使用者自定  
使用者自定  
群組和物件

協定 -指定本過濾器規則套用的協定。

	<p><b>來源/目標通訊埠</b> –</p> <p>(=) – 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。</p> <p>(!=) – 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。</p> <p>(&gt;) – 大於此數值的通訊埠號皆可使用。</p> <p>(&lt;) – 小於此數值的通訊埠號皆可使用。</p> <p><b>服務群組/物件</b> - 使用下拉式選項選擇所需的項目。</p>
片段	<p>指定片段封包的執行動作，這個項目也是僅針對<b>資料過濾器</b>。</p> <p><b>忽略</b> - 不論是怎樣的片端封包，系統皆不採取行動。</p> <p><b>無片段</b> - 應用規則至無片段之封包上。</p> <p><b>片段</b> - 應用規則至片段之封包上。</p> <p><b>太短了</b> - 只有過短無法包含完整封包頭之封包，可應用此規則。</p>
過濾器	<p>指定系統針對符合規則之封包所採取的行動。</p> <p><b>立刻通過</b> - 符合規則之封包可立即通過。</p> <p><b>立刻封鎖</b> - 系統封鎖符合規則之封包。</p> <p><b>若無符合其於規則即通過</b> - 符合限定規則且並未符合其他規則之封包可立即通過。</p> <p><b>若無符合其於規則即封鎖</b> - 系統封鎖符合限定規則且並未符合其他規則之封包。</p> <p>基於疑難排除的需要，您可指定記錄過濾器資訊，只要勾選 <b>Syslog</b> 方框即可。</p>
分至其他過濾器設定	<p>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。</p>
連線數控制	<p>此處輸入的值為全部的封包連線數，預設值為 60000。</p>
IP 與 MAC 綁定	<p><b>嚴格的</b> - 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。</p> <p><b>不嚴格的</b> - 此指完全沒有限制。</p>
服務品質	<p>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。</p>

	
<p><b>使用者管理</b></p>	<p>本項目僅在<b>使用者管理&gt;&gt;基本設定</b>中選擇<b>規則模式</b>時可用，一般防火牆規則將套用在<b>使用者/使用者群組/全部使用者</b>上。</p>  <p><b>注意：</b>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<b>建立新使用者</b>或是<b>建立新的群組</b>選項供您建立新的設定檔。</p>
<p><b>應用程式管控</b></p>	<p>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<b>建立新設定</b>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<b>數位內容安全管理&gt;&gt;應用程式管控設定檔</b>章節。</p> <p>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。</p>
<p><b>URL 內容過濾器</b></p>	<p>選擇一個 <b>URL 內容過濾器</b>設定檔（在<b>數位內容安全管理 (CSM)&gt;&gt; URL 內容過濾器</b>中所建立），請務必先在<b>數位內容安全管理(CSM)&gt; URL 內容過濾器</b>中設定一個設定檔，或是從下拉式選單中選擇<b>[建立新檔]</b>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。</p>
<p><b>網頁內容過濾器</b></p>	<p>選擇一個<b>網頁內容過濾器</b>設定檔（在<b>數位內容安全管理 (CSM)&gt;&gt; 網頁內容過濾器</b>中所建立），請務必先在<b>數位內容安全管理(CSM)&gt;&gt; 網頁內容過濾器</b>中設定一個設定檔，或是從下拉式選單中選擇<b>[建立新檔]</b>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。</p>
<p><b>DNS 過濾器</b></p>	<p>選擇一組 <b>DNS 過濾器</b>設定檔(於<b>數位內容安全管理&gt;&gt;DNS 過濾器</b>頁面中建立)，在<b>數位內容安全管理&gt;&gt;網頁內容過濾器設定檔</b>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 <b>DNS 過濾器</b>連結以重新建立新的設定檔。</p>

## 進階設定

按**編輯**按鈕開啓下述視窗，不過，在此強烈建議您使用預設值為佳。

### 防火牆 >> 設定過濾器 >> 編輯過濾器規則

#### 過濾器組別 1 規則 1

##### 進階設定

選擇編碼語系	ANSI(1252)-拉丁文 I
視窗大小:	65535
連線數逾時:	1440 分
居易標題:	<input checked="" type="checkbox"/>

##### 嚴格安全檢測

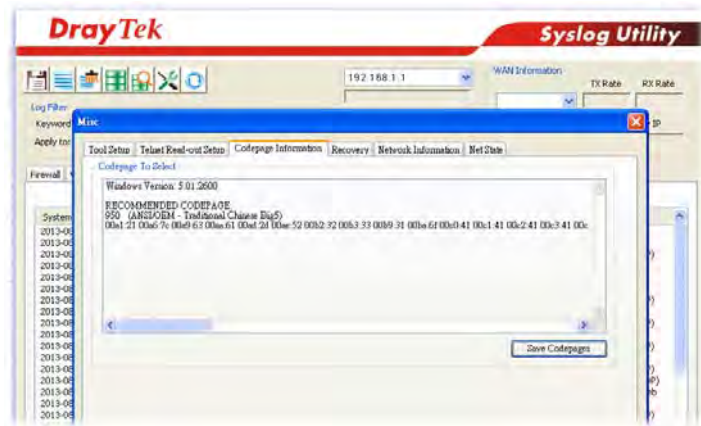
應用程式管控

確定

關閉

**選擇編碼語系** - 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**，請開啓 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。

**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。

**應用程式管控** - 勾選方塊以透過 IM/P2P 嚴格檢查所有傳輸檔案。

## 範例

如上所言，全部的資料傳輸都將以二種 IP 過濾器（呼叫過濾器或是資料過濾器）來分開執行，您可以設定 12 組呼叫過濾器和資料過濾器，每種過濾器設定由 7 種過濾器規則組合而成，這些規則都是事前定義完成。然後在**基本設定**中，您可以指定一組規則予呼叫過濾器與資料過濾器使用。

防火牆 >> 基本設定

**基本設定**

預設規則

呼叫過濾器  啟用  停用  
 資料過濾器  啟用  停用

開始過濾器組別 組別#1  
 開始過濾器組別 組別#2

接受流入的大量 UDP 或是 ICMP Fragment 封包 (用於某些遊戲, 如CS)  
 啟動嚴格安全防火牆策略

確定 取消

防火牆 >> 過濾器設定

組別	註解	組別	註解
1.	Default Call Filter	7.	
2.	Default Data Filter	8.	
3.		9.	
4.		10.	
5.		11.	
6.		12.	

回復出廠預設值

防火牆 >> 過濾器設定 >> 編輯過濾器設定

**過濾器組別 1**  
 註解: Default Call Filter

過濾器規則	啟用	註解
1	<input checked="" type="checkbox"/>	Block NetBios
2	<input type="checkbox"/>	
3	<input type="checkbox"/>	
4	<input type="checkbox"/>	
5	<input type="checkbox"/>	
6	<input type="checkbox"/>	
7	<input type="checkbox"/>	

確定 清除 取消

防火牆 >> 編輯過濾器設定 >> 編輯過濾器規則

**過濾器組別 1 規則 1**

啟用過濾規則

註解: Block NetBios

索引號碼(1-15) 於 捷徑 設置:  ,  ,

啟用排程時, 清除連線數:  啟用

方向: LAN/DMZ/RTMP/N -> WAN

來源 IP: Any

目的 IP: Any

服務類型: TCP/UDP, Port from 137-139 to any

片段: 忽略

**應用程式**

過濾器: 立即封鎖

分至其他過濾器設定: 無

連線數控制: 0 / 60000

IP 與 MAC 綁定: 不嚴格的

**服務品質**

負載平衡原則: 無

自動選擇

**使用者管理**

無

**應用程式管控**

URL 內容過濾器: 無

網頁內容過濾器: 無

進階設定

確定 清除 取消



#### 4.6.4 DoS 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。

按防火牆並選擇 DoS 攻擊防禦功能開啓設定網頁。

防火牆 >> DoS 攻擊防禦功能設定

**DoS 攻擊防禦功能設定**

啓用 DoS 防禦功能

<input type="checkbox"/> 啓用 SYN flood 攻擊防禦功能	臨界值	<input type="text" value="2000"/>	封包 / 秒
	逾時	<input type="text" value="10"/>	秒
<input type="checkbox"/> 啓用 UDP flood 攻擊防禦功能	臨界值	<input type="text" value="2000"/>	封包 / 秒
	逾時	<input type="text" value="10"/>	秒
<input type="checkbox"/> 啓用 ICMP 攻擊防禦功能	臨界值	<input type="text" value="250"/>	封包 / 秒
	逾時	<input type="text" value="10"/>	秒
<input type="checkbox"/> 啓用防禦通訊埠掃描偵測功能	臨界值	<input type="text" value="2000"/>	封包 / 秒
<input type="checkbox"/> 封鎖 IP 選項	<input type="checkbox"/> 封鎖 TCP Flags scan		
<input type="checkbox"/> 封鎖 Land 攻擊	<input type="checkbox"/> 封鎖 Tear Drop 攻擊		
<input type="checkbox"/> 封鎖 Smurf 攻擊	<input type="checkbox"/> 封鎖 Ping of Death 攻擊		
<input type="checkbox"/> 封鎖路由追蹤 (Trace Route)	<input type="checkbox"/> 封鎖 ICMP 封包片段攻擊		
<input type="checkbox"/> 封鎖 SYN Fragment 封包	<input type="checkbox"/> 封鎖不明封包		
<input type="checkbox"/> 封鎖 Fraggle 攻擊			

啓用抵擋DoS攻擊功能，防止外來駭客攻擊。

可用設定說明如下：

項目	說明
啓用	勾選此項以啓動 DoS 攻擊防禦功能。
選擇全部	按下此鈕選擇下列全部項目。
啓用 SYN flood 攻擊防禦功能	勾選此項以啓動 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。
啓用 UDP flood 攻擊防禦功能	勾選此項以啓動 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。 <b>注意：</b> 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。

<p><b>啓用 ICMP Fragment 封包</b></p>	<p>勾選此項以啓動 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。</p>
<p><b>啓用防禦通訊埠掃描偵測功能</b></p>	<p>通訊埠掃描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。勾選此方塊啓動通訊埠掃描檢測功能，當利用通訊埠掃描臨界值速率而檢測出惡意探測之行爲時，Vigor 路由器將傳送警告訊息出去。臨界值的預設值為每秒 2000 個封包。</p>
<p><b>封鎖 IP options</b></p>	<p>勾選此項以啓動阻攔 IP options 功能，Vigor 路由器將會忽略資料封包頭中(含 IP 選項區)的 IP 封包。限制的原因是 IP option 的出現是區域網路安全性中的弱點，因爲它攜帶令人注意的資訊像是安全性、TCC (封閉使用者群組)參數、網際網路位址、路由訊息等等，讓外部的竊聽者有機會取得您虛擬網路的細節內容。</p>
<p><b>封鎖 Land 攻擊</b></p>	<p>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。</p>
<p><b>封鎖 Smurf 攻擊</b></p>	<p>勾選此項以啓動封鎖 Smurf 攻擊功能，Vigor 路由器將忽略任何一次的播送 ICMP 回應需求。</p>
<p><b>封鎖路由追蹤</b></p>	<p>勾選此項以強迫 Vigor 路由器不轉送任何路由封包的行蹤。</p>
<p><b>封鎖 SYN Fragment 封包</b></p>	<p>勾選此項以啓動封鎖 SYN Fragment 的封包功能。Vigor 路由器將會停止任何具有 SYN 旗標及更多的區段設定之封包傳送作業。</p>
<p><b>封鎖 Fraggle 攻擊</b></p>	<p>勾選此項以啓動封鎖 Fraggle 攻擊功能，任何播送來自網際網路的 UDP 封包都會被封鎖起來。</p> <p>啓動 DoS/DDoS 防禦功能可能會阻擋一些合法的封包，例如當您啓動 fraggle 攻擊防禦時，所有來自網際網路的 UDP 封包播送都會被阻擋在外，因此得自網際網路的 RIP 封包全都會被阻擋掉。</p>
<p><b>封鎖 TCP Flags scan</b></p>	<p>勾選此項以啓動阻攔 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 <i>no flag scan</i>, <i>FIN without ACK scan</i>, <i>SYN FINscan</i>, <i>Xmas scan</i> 以及 <i>full Xmas scan</i> 等等。</p>
<p><b>封鎖 Tear Drop 攻擊</b></p>	<p>勾選此項以啓動封鎖 Tear Drop 攻擊功能，很多機器在接收到超過最大值得 ICMP 資料段(封包)時，系統就會當機。爲了避免這類型的攻擊行爲，Vigor 路由器便被設計成具有捨棄片段 ICMP (超過 1024 位元組)封包的能力。</p>

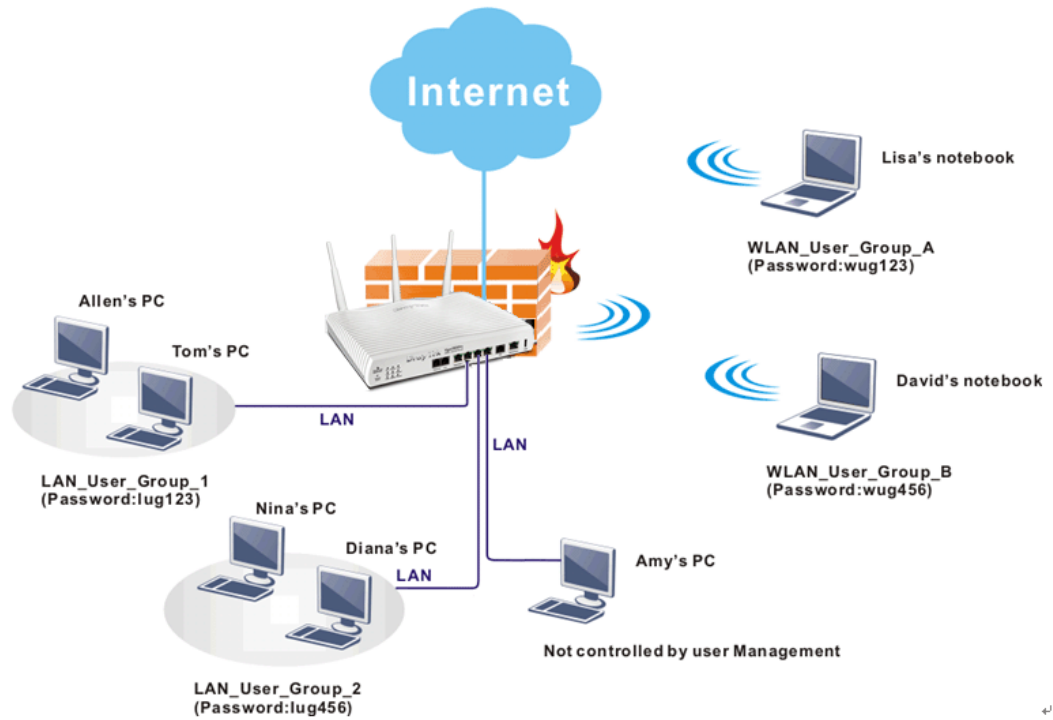


封鎖 Ping of Death 攻擊	勾選此項以啟動封鎖 Ping of Death 攻擊功能，這項攻擊意味著犯罪者傳送重疊封包至目的主機，這些目的主機一旦重新建構封包時就會造成當機現象，Vigor 路由器將會阻擋此種攻擊活動的封包進入。
封鎖 ICMP 封包片段攻擊	勾選此項以啟動封鎖 ICMP 封包片段功能，任何含有多個片段的 ICMP 封包都會被捨棄阻擋。
封鎖不明封包協定封包	勾選此項以啟動封鎖不明封包協定封包功能，個別 IP 封包在資料段封包頭中都擁有一個協定區域，指名該協定於上層運作的類型。
警告訊息	<p>我們提供使用者系統記錄功能以便檢視路由器發出的訊息。作為系統紀錄伺服器，使用者可接收來自路由器(系統紀錄用戶端)傳送之報告。</p> <p>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，所遭受的任何攻擊之名稱即可立即檢測出來。</p> <p>系統維護 &gt;&gt; Syslog / 郵件警示設定</p>  <p>附註：1. 除非在"Syslog儲存至"項目中勾選了USB磁碟，否則郵件 Syslog 不會被啟動。 2. 郵件 Syslog 功能會在 Syslog 檔案尺寸大於 1M時會傳送出來。 3. 我們僅支援埠號465的安全SMTP連線。</p> <p>確定 清除</p> 

在您完成上述的設定之後，請按**確定**按鈕來儲存設定。

## 4.7 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。



**注意：**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。

防火牆  
使用者管理  
基本設定  
使用者設定檔  
使用者群組  
使用者線上狀態  
物件設定

## 4.7.1 基本設定

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**規則模式**還是**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。

使用者管理 >> 基本設定

### 基本設定

**模式選項:**

**規則模式** 乃為基於IP位址的管理方式，管理者可設定不同的防火牆規則因應不同的 IP位址之需。  
 **使用者模式** 是基於使用者設定檔的管理方式，管理者可以設定不同的防火牆規則以便因應不同的使用者。

**驗證頁面:**

網頁驗證:  HTTPS  HTTP

登入頁面 Logo: 預設值  未選擇檔案 (最多 524 X 352 像素)

**登入頁面設定**

顯示出成功登入後，跳出之對話盒的 IP位址。

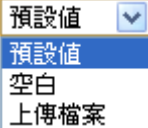
**指定首頁:**

(最多 255 個字元)

```
<body stats=l><script language='javascript'>
window.location='http://www.draytek.com'</script></body>
```

可用設定說明如下：

項目	說明
模式選項	<p>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。</p> <p><b>使用者模式</b> - 如果您選擇此模式，路由器將會套用您在<b>使用者管理&gt;&gt;使用者設定檔</b>中的過濾規則至使用者上。</p> <p><b>規則模式</b> - 如果您選擇此模式，路由器將會套用您在<b>防火牆&gt;&gt;基本設定</b>中的過濾規則至使用者上。</p>

<p><b>驗證頁面</b></p>	<p><b>網頁驗證</b> - 選擇網頁驗證使用的協定(HTTPS/HTTP)。</p> <p><b>登入頁面 Logo</b> - 標識能成為辨識企業的圖示，可以上傳並顯示在登入頁面上，您可以使用預設畫面，空白頁或是上傳其他的影像圖形(尺寸像素大小不要超過 524 × 352)，如此即可針對特定企業給予企業辨識圖示，當然這也帶有廣告的效果。</p>  <p><b>登入頁面設定</b>- 此連結讓您開啓登入頁面設定網頁，詳細資訊請參考<a href="#">系統維護</a>&gt;&gt;<a href="#">登入頁面設定</a>一節。</p> <p><b>顯示出成功登入後.....</b> - 勾選此框以顯示追蹤視窗中用戶端的 IP 位址。</p>
<p><b>指定首頁</b></p>	<p>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。</p>

在您完成上述的設定之後，請按**確定**按鈕來儲存設定。

## 4.7.2 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。開啓**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**

使用者設定檔列表		回復出廠預設值	
設定檔	名稱	設定檔	名稱
<a href="#">1.</a>	admin	<a href="#">17.</a>	
<a href="#">2.</a>	Dial-In User	<a href="#">18.</a>	
<a href="#">3.</a>		<a href="#">19.</a>	
<a href="#">4.</a>		<a href="#">20.</a>	
<a href="#">5.</a>		<a href="#">21.</a>	
<a href="#">6.</a>		<a href="#">22.</a>	
<a href="#">7.</a>		<a href="#">23.</a>	
<a href="#">8.</a>		<a href="#">24.</a>	
<a href="#">9.</a>		<a href="#">25.</a>	
<a href="#">10.</a>		<a href="#">26.</a>	
<a href="#">11.</a>		<a href="#">27.</a>	
<a href="#">12.</a>		<a href="#">28.</a>	
<a href="#">13.</a>		<a href="#">29.</a>	
<a href="#">14.</a>		<a href="#">30.</a>	
<a href="#">15.</a>		<a href="#">31.</a>	
<a href="#">16.</a>		<a href="#">32.</a>	

<< [1-32](#) | [33-64](#) | [65-96](#) | [97-128](#) | [129-160](#) | [161-192](#) | [193-200](#) >> >> 下一頁 >>

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。

**使用者管理 >> 使用者設定檔**

### 索引編號 3

<input checked="" type="checkbox"/>	啓動此帳號	
	使用者名稱	<input type="text"/>
	密碼	<input type="text"/>
	確認密碼	<input type="text"/>
	閒置逾時	<input type="text" value="10"/> 分鐘，0:無限制
	最多登入使用者數目	<input type="text" value="0"/> 0:無限制
	<b>外接伺服器驗證</b>	<input type="text" value="無"/> ▾
	記錄	<input type="text" value="無"/> ▾
	快顯瀏覽器追蹤視窗	<input checked="" type="checkbox"/>
	驗證	<input checked="" type="checkbox"/> 網頁 <input checked="" type="checkbox"/> 警告工具 <input checked="" type="checkbox"/> Telnet
	<b>指定首頁</b>	<input type="checkbox"/>
	索引號碼(1-15) 於 <b>捷程</b> 設定:	<input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>
<input type="checkbox"/>	啓用時間額度	0 分 <input type="text" value="0"/> 分
<input type="checkbox"/>	啓用資料額度	0 MB <input type="text" value="0"/> MB
當時間排程到期時，重新設定額度為預設值		
<input type="checkbox"/>	啓用	預設時間額度 <input type="text" value="0"/> 分 預設資料額度 <input type="text" value="0"/> MB

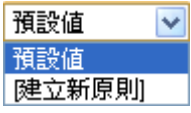
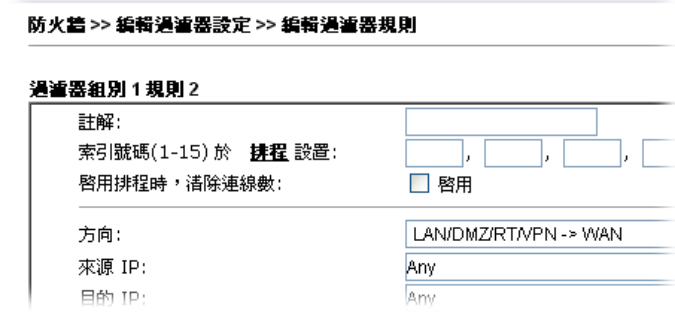
確定

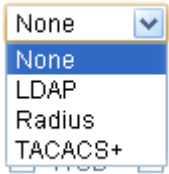


更新頁面

清除

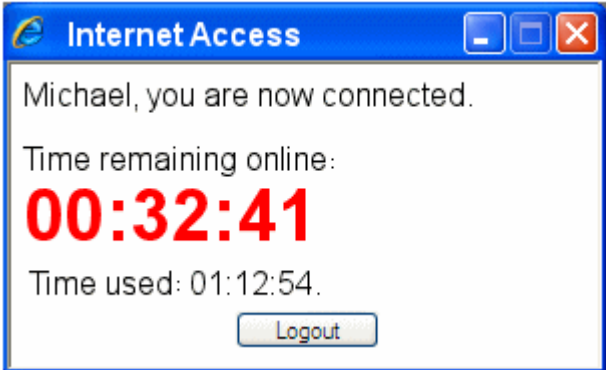
取消

可用設定說明如下：

項目	說明
啓動此帳號	勾選此方塊啓用此設定檔。
使用者名稱	請輸入此使用者設定檔的名稱(例如 <i>LAN_User_Group_1</i> , <i>WLAN_User_Group_A</i> , <i>WLAN_User_Group_B</i> 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 <i>lug123</i> , <i>wug123</i> , <i>wug456</i> 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。
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。
最多登入使用者數目	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。
原則	<p>這個功能只有在<b>使用者管理&gt;&gt;基本設定</b>頁面中選擇了<b>使用者模式</b>才會出現。</p>  <p><b>預設值</b> – 如果您選擇此項, 系統會採用防火牆內事先設定的過濾器規則於此設定檔上。</p> <p><b>建立新原則</b> – 如果您選擇此項, 下述頁面會跳出方便您定義一個新的過濾器規則。</p>  <p>有關詳細的設定內容, 請直接參考<b>防火牆&gt;&gt;過濾器規則</b>一節。在<b>防火牆&gt;&gt;基本設定</b>頁面中<b>預設規則</b>內沒被選上的規則可在<b>使用者管理&gt;&gt;使用者設定檔</b>中運用。</p>
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

	<p>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。</p> 
<p>記錄</p>	<p>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。</p> 
<p>快顯瀏覽器追蹤視窗</p>	<p>如果啓用此功能，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。</p>
<p>驗證</p>	<p>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：</p> <p><b>網頁</b> – 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<b>使用者管理&gt;&gt;基本設定</b>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)。</p> <p><b>警告工具</b> – 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。</p> <p><b>Telnet</b> – 如果選擇此項，使用者可透過 Telnet 指令來進行驗證作業。</p>
<p>指定首頁</p>	<p>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<b>使用者管理&gt;&gt;基本設定</b>中所設定的指定首頁。勾選此方塊可開啓此項功能。</p>
<p>索引號碼(1-15)於排程設定</p>	<p>您可以在此輸入四組時間排程，所有的排程都可在<b>其他應用&gt;&gt;排程</b>頁面事先設定，在本頁您只要將排程的索引編號輸入即可。</p>
<p>啓用時間額度</p>	<p>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，勾選此方塊啓用此功能。</p> <p> – 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。</p>



	<p><input type="button" value="-"/> – 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。</p> <p><b>注意：</b>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。</p>  <p>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。</p>
<p><b>啓用資料額度</b></p>	<p>資料額度表示給予使用者的全部資料傳輸量。</p> <p><input type="button" value="+"/> – 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。</p> <p><input type="button" value="-"/> – 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。</p>
<p><b>當時間排程到期時，重新設定額度為預設值</b></p>	<p>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。</p> <p><b>啓用</b> – 勾選此方框使用預設的時間與資料額度值。</p> <p><b>預設時間額度</b> – 輸入時間額度數值</p> <p><b>預設資料額度</b> – 輸入資料額度數值。</p>

在您完成上述的設定之後，請按**確定**按鈕來儲存設定。



### 4.7.3 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:

[| 回復出廠預設值 |](#)

索引編號	名稱	索引編號	名稱
<a href="#">1.</a>		<a href="#">17.</a>	
<a href="#">2.</a>		<a href="#">18.</a>	
<a href="#">3.</a>		<a href="#">19.</a>	
<a href="#">4.</a>		<a href="#">20.</a>	
<a href="#">5.</a>		<a href="#">21.</a>	
<a href="#">6.</a>		<a href="#">22.</a>	
<a href="#">7.</a>		<a href="#">23.</a>	
<a href="#">8.</a>		<a href="#">24.</a>	
<a href="#">9.</a>		<a href="#">25.</a>	
<a href="#">10.</a>		<a href="#">26.</a>	
<a href="#">11.</a>		<a href="#">27.</a>	
<a href="#">12.</a>		<a href="#">28.</a>	
<a href="#">13.</a>		<a href="#">29.</a>	
<a href="#">14.</a>		<a href="#">30.</a>	
<a href="#">15.</a>		<a href="#">31.</a>	
<a href="#">16.</a>		<a href="#">32.</a>	

按下任何一個索引編號連結開啓如下頁面：

[使用者管理 >> 使用者群組](#)

設定檔編號: 1

名稱:

可用的使用者物件

1-admin  
2-Dial-In User

選定的使用者物件(最多 32 物件)

>>  
<<

可用設定說明如下：

項目	說明
名稱	輸入使用者群組的名稱。
可用的使用者物件	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 <input type="button" value="&gt;&gt;"/> 按鈕將選定的使用者物件移至本區。

在您完成上述的設定之後，請按**確定**按鈕來儲存設定。

#### 4.7.4 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。

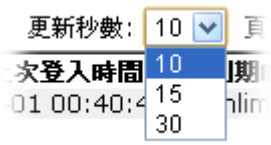
使用者管理 >> 使用者線上狀態

目前時間: 01-01 00:46:24      更新秒數: 10   頁: 1   | [更新頁面](#) |

索引編號	設定檔	IP 位址	使用者	上次登入時間	到期時間	閒置時間	動作
1	admin	192.168.1.10	admin	01-01 00:40:42	Unlimited	Unlimited	封鎖 登出

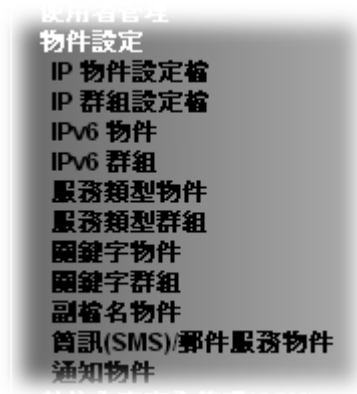
總數：1

可用設定說明如下：

項目	說明
更新秒數	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。
索引編號	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啓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。
閒置時間	顯示設定檔的閒置時間設定。
動作	<b>封鎖</b> - 封鎖使用者使用網路。 <b>解鎖</b> - 解除使用者使用網路 <b>登出</b> - 強迫使用者登出。

## 4.8 物件設定

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爲物件，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 可定義成爲一個 IP 物件(意即 IP 位址範圍)。



### 4.8.1 IP 物件設定檔

您可設定 192 組不同條件的 IP 物件。

物件設定 >> IP 物件設定檔

IP 物件設定檔: | 回復出廠預設值 |

索引編號	名稱	索引編號	名稱
<a href="#">1.</a>		<a href="#">17.</a>	
<a href="#">2.</a>		<a href="#">18.</a>	
<a href="#">3.</a>		<a href="#">19.</a>	
<a href="#">4.</a>		<a href="#">20.</a>	
<a href="#">5.</a>		<a href="#">21.</a>	
<a href="#">6.</a>		<a href="#">22.</a>	
<a href="#">7.</a>		<a href="#">23.</a>	
<a href="#">8.</a>		<a href="#">24.</a>	
<a href="#">9.</a>		<a href="#">25.</a>	
<a href="#">10.</a>		<a href="#">26.</a>	
<a href="#">11.</a>		<a href="#">27.</a>	
<a href="#">12.</a>		<a href="#">28.</a>	
<a href="#">13.</a>		<a href="#">29.</a>	
<a href="#">14.</a>		<a href="#">30.</a>	
<a href="#">15.</a>		<a href="#">31.</a>	
<a href="#">16.</a>		<a href="#">32.</a>	

<< [1-32](#) | [33-64](#) | [65-96](#) | [97-128](#) | [129-160](#) | [161-192](#) >> | 下一頁 >>

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。

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. 設定網頁顯示如下：

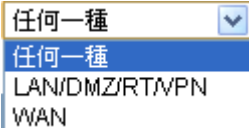
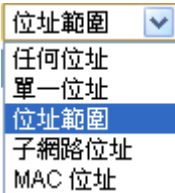
物件設定 >> IP 物件

設定檔索引：1

名稱：	RD Department
介面	任何一種
位址類型	位址範圍
MAC 位址：	00 : 00 : 00 : 00 : 00 : 00
起始 IP 位址	192.168.1.59
結束 IP 位址	192.168.1.65
子網路遮罩	0.0.0.0
反向選擇	<input type="checkbox"/>

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。
介面	<p>請選擇適當的介面。</p>  <p>例如，<b>編輯過濾器規則</b>中的<b>方向</b>設定會要求您針對 WAN 或 LAN/DMZ/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/DMZ/RT/VPN 作為介面，並選擇 LAN/DMZ/RT/VPN 作為<b>編輯過濾器規則</b>中的<b>方向</b>設定，那麼所有的 LAN/DMZ/RT/VPN 介面的 IP 位址通通都會開放予您在<b>編輯過濾器規則</b>頁面上選擇。</p>
位址類型	<p>決定 IP 位址的位址類型。</p> <p>如果物件僅包含 IP 位址的話，請選擇<b>單一位址</b>。</p> <p>如果物件包含某個範圍內數個 IP 位址的話，請選擇<b>範圍位址</b>。</p> <p>如果物件包含 IP 位址的子網路的話，請選擇<b>子網路位址</b>。</p> <p>如果物件包含任何一種 IP 位址的話請選擇<b>任何位址</b>。</p> <p>如果物件包含任何一種 MAC 位址的話請選擇<b>MAC 位址</b>。</p> 
MAC 位址	如果選擇的是 <b>MAC 位址</b> 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。
子網路遮罩	如果選擇的是子網路位址類型，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。

3. 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。

**物件設定 >> IP 物件設定檔**

**IP 物件設定檔:**

索引編號	名稱	索引編號
<u>1.</u>	RD Department	<u>17.</u>
<u>2.</u>		<u>18.</u>
<u>3.</u>		<u>19.</u>
<u>4.</u>		<u>20.</u>
<u>5.</u>		<u>21.</u>
<u>6.</u>		<u>22.</u>

## 4.8.2 IP 群組

本頁可讓您綁定數個 IP 物件成爲一個 IP 群組。

物件設定 >> IP 群組設定檔

IP群組設定檔:		回復出廠預設值	
索引編號	名稱	索引編號	名稱
<a href="#">1.</a>		<a href="#">17.</a>	
<a href="#">2.</a>		<a href="#">18.</a>	
<a href="#">3.</a>		<a href="#">19.</a>	
<a href="#">4.</a>		<a href="#">20.</a>	
<a href="#">5.</a>		<a href="#">21.</a>	
<a href="#">6.</a>		<a href="#">22.</a>	
<a href="#">7.</a>		<a href="#">23.</a>	
<a href="#">8.</a>		<a href="#">24.</a>	
<a href="#">9.</a>		<a href="#">25.</a>	
<a href="#">10.</a>		<a href="#">26.</a>	
<a href="#">11.</a>		<a href="#">27.</a>	
<a href="#">12.</a>		<a href="#">28.</a>	
<a href="#">13.</a>		<a href="#">29.</a>	
<a href="#">14.</a>		<a href="#">30.</a>	
<a href="#">15.</a>		<a href="#">31.</a>	
<a href="#">16.</a>		<a href="#">32.</a>	

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。

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. 設定網頁顯示如下：

物件設定 >> IP 群組

設定檔索引號碼: 1

名稱	<input type="text" value="administration"/>
介面	<input type="button" value="任何一種"/>
可用之 IP 物件	選定 IP 物件
<input type="text" value="1-RD Department"/>	<input type="text"/>
	<input type="button" value="&gt;&gt;"/>
	<input type="button" value="&lt;&lt;"/>
<input type="button" value="確定"/> <input type="button" value="清除"/> <input type="button" value="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。
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。
可用之 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 IP 物件	按下 >> 按鈕來新增選定 IP 物件並呈現在此方塊內。

- 完成設定之後，按下**確定**按鈕儲存相關設定。

### 4.8.3 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:		回復出廠預設值	
索引編號	名稱	索引編號	名稱
<a href="#">1.</a>		<a href="#">17.</a>	
<a href="#">2.</a>		<a href="#">18.</a>	
<a href="#">3.</a>		<a href="#">19.</a>	
<a href="#">4.</a>		<a href="#">20.</a>	
<a href="#">5.</a>		<a href="#">21.</a>	
<a href="#">6.</a>		<a href="#">22.</a>	
<a href="#">7.</a>		<a href="#">23.</a>	
<a href="#">8.</a>		<a href="#">24.</a>	
<a href="#">9.</a>		<a href="#">25.</a>	
<a href="#">10.</a>		<a href="#">26.</a>	
<a href="#">11.</a>		<a href="#">27.</a>	
<a href="#">12.</a>		<a href="#">28.</a>	
<a href="#">13.</a>		<a href="#">29.</a>	
<a href="#">14.</a>		<a href="#">30.</a>	
<a href="#">15.</a>		<a href="#">31.</a>	
<a href="#">16.</a>		<a href="#">32.</a>	

<< [1-32](#) | [33-64](#) >> >> 下一頁 >>

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。

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. 設定網頁顯示如下：

物件設定 >> IPv6 物件

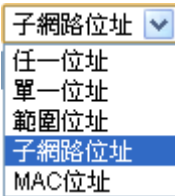
索引編號: 1

名稱:	<input type="text"/>
位址類型:	子網路位址 <input type="button" value="v"/>
MAC位址:	<input type="text" value="00:00:00:00:00:00"/>
起始 IP 位址:	<input type="text"/>
結束 IP 位址:	<input type="text"/>
前置號碼長度:	<input type="text"/>
反向選擇:	<input type="checkbox"/>

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	<p>決定 IPv6 的位址類型。</p> <p>如果此物件僅含一組 IPv6 位址，請選擇<b>單一位址</b>。</p> <p>如果此物件包含數個 IPv6 位址，請選擇<b>範圍位址</b>。</p> <p>如果此物件包含一個 IPv6 子網路位址，請選擇<b>子網路位址</b>。</p> <p>如果此物件包含任何一個 IPv6 位址，請選擇<b>任一位址</b>。</p> <p>如果此物件包含 MAC 位址，請選擇<b>MAC 位址</b>。</p> 
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。

- 完成設定之後，按下**確定**按鈕儲存相關設定。

## 4.8.4 IPv6 群組

本頁可讓您綁定數個 IPv6 物件成爲一個 IPv6 群組。

物件設定 >> IPv6 群組

IPv6 群組表格: | 回復出廠預設值 |

索引編號	名稱	索引編號	名稱
<a href="#">1.</a>		<a href="#">17.</a>	
<a href="#">2.</a>		<a href="#">18.</a>	
<a href="#">3.</a>		<a href="#">19.</a>	
<a href="#">4.</a>		<a href="#">20.</a>	
<a href="#">5.</a>		<a href="#">21.</a>	
<a href="#">6.</a>		<a href="#">22.</a>	
<a href="#">7.</a>		<a href="#">23.</a>	
<a href="#">8.</a>		<a href="#">24.</a>	
<a href="#">9.</a>		<a href="#">25.</a>	
<a href="#">10.</a>		<a href="#">26.</a>	
<a href="#">11.</a>		<a href="#">27.</a>	
<a href="#">12.</a>		<a href="#">28.</a>	
<a href="#">13.</a>		<a href="#">29.</a>	
<a href="#">14.</a>		<a href="#">30.</a>	
<a href="#">15.</a>		<a href="#">31.</a>	
<a href="#">16.</a>		<a href="#">32.</a>	

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並回復出廠預設值。
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。

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. 設定網頁顯示如下：

物件設定 >> IPv6 群組

索引編號: 1

名稱:

可用的 IPv6 物件	選定的 IPv6 物件
<div style="border: 1px solid gray; height: 100px;"></div>	<div style="border: 1px solid gray; height: 100px;"></div>

>> <<

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。
可用的 IPv6 物件	所有可用的 IPv6 物件全都顯示在此方塊中。
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。

#### 4.8.5 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 >> 服務類型物件設定檔

服務類型物件設定檔:		回復出廠預設值	
索引編號	名稱	索引編號	名稱
<u>1.</u>		<u>17.</u>	
<u>2.</u>		<u>18.</u>	
<u>3.</u>		<u>19.</u>	
<u>4.</u>		<u>20.</u>	
<u>5.</u>		<u>21.</u>	
<u>6.</u>		<u>22.</u>	
<u>7.</u>		<u>23.</u>	
<u>8.</u>		<u>24.</u>	
<u>9.</u>		<u>25.</u>	
<u>10.</u>		<u>26.</u>	
<u>11.</u>		<u>27.</u>	
<u>12.</u>		<u>28.</u>	
<u>13.</u>		<u>29.</u>	
<u>14.</u>		<u>30.</u>	
<u>15.</u>		<u>31.</u>	
<u>16.</u>		<u>32.</u>	

<< [1-32](#) | [33-64](#) | [65-96](#) >> << 下一頁 >>

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。

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. 設定網頁顯示如下：

物件設定 >> 服務類型物件設定

設定檔索引：1

名稱	<input type="text" value="www"/>
通訊協定	TCP <input type="text" value="6"/>
來源通訊埠	= <input type="text" value="1"/> ~ <input type="text" value="65535"/>
目的通訊埠	= <input type="text" value="1"/> ~ <input type="text" value="65535"/>

可用設定說明如下：

項目	說明
名稱	輸入此設定檔的名稱。
介面	<p>請選擇此設定檔所要套用的適當介面。</p> 
來源/目標通訊埠	<p>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。</p> <p>(=) – 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。</p> <p>(!=) – 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。</p> <p>(&gt;) – 大於此數值的通訊埠號皆可使用。</p> <p>(&lt;) – 小於此數值的通訊埠號皆可使用。</p>

3. 完成設定之後，按下**確定**按鈕儲存相關設定。

## 物件設定 >> 服務類型物件設定檔

### 服務類型物件設定檔:

索引編號	名稱
<a href="#">1.</a>	www
<a href="#">2.</a>	
<a href="#">3.</a>	

## 4.8.6 服務類型群組

本頁可讓您綁定數個服務類型物件成爲一個群組。

### 物件設定 >> 服務類型群組設定檔

#### 服務類型群組設定檔:

[| 回復出廠預設值 |](#)

群組	名稱	群組	名稱
<a href="#">1.</a>		<a href="#">17.</a>	
<a href="#">2.</a>		<a href="#">18.</a>	
<a href="#">3.</a>		<a href="#">19.</a>	
<a href="#">4.</a>		<a href="#">20.</a>	
<a href="#">5.</a>		<a href="#">21.</a>	
<a href="#">6.</a>		<a href="#">22.</a>	
<a href="#">7.</a>		<a href="#">23.</a>	
<a href="#">8.</a>		<a href="#">24.</a>	
<a href="#">9.</a>		<a href="#">25.</a>	
<a href="#">10.</a>		<a href="#">26.</a>	
<a href="#">11.</a>		<a href="#">27.</a>	
<a href="#">12.</a>		<a href="#">28.</a>	
<a href="#">13.</a>		<a href="#">29.</a>	
<a href="#">14.</a>		<a href="#">30.</a>	
<a href="#">15.</a>		<a href="#">31.</a>	
<a href="#">16.</a>		<a href="#">32.</a>	

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。

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. 設定網頁顯示如下：

設定檔索引號碼: 1

名稱: <input type="text"/>	
可用之服務類型物件 1-www	選定之服務類型物件
<input style="margin-right: 10px;" type="button" value=" &gt;&gt; "/> <input style="margin-left: 10px;" type="button" value=" &lt;&lt; "/>	
<input style="margin-right: 20px;" type="button" value=" 確定 "/> <input style="margin-right: 20px;" type="button" value=" 清除 "/> <input style="margin-left: 20px;" type="button" value=" 取消 "/>	

可用設定說明如下：

項目	說明
名稱	輸入此設定檔的名稱。
可用之服務類型物件	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。
選定之服務類型物件	按下 >> 按鈕來新增選定服務類型並呈現在此方塊內。

- 完成設定之後，按下**確定**按鈕儲存相關設定。

#### 4.8.7 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:		回復出廠預設值	
索引編號	名稱	索引編號	名稱
<a href="#">1.</a>		<a href="#">17.</a>	
<a href="#">2.</a>		<a href="#">18.</a>	
<a href="#">3.</a>		<a href="#">19.</a>	
<a href="#">4.</a>		<a href="#">20.</a>	
<a href="#">5.</a>		<a href="#">21.</a>	
<a href="#">6.</a>		<a href="#">22.</a>	
<a href="#">7.</a>		<a href="#">23.</a>	
<a href="#">8.</a>		<a href="#">24.</a>	
<a href="#">9.</a>		<a href="#">25.</a>	
<a href="#">10.</a>		<a href="#">26.</a>	
<a href="#">11.</a>		<a href="#">27.</a>	
<a href="#">12.</a>		<a href="#">28.</a>	
<a href="#">13.</a>		<a href="#">29.</a>	
<a href="#">14.</a>		<a href="#">30.</a>	
<a href="#">15.</a>		<a href="#">31.</a>	
<a href="#">16.</a>		<a href="#">32.</a>	

<< [1-32](#) | [33-64](#) | [65-96](#) | [97-128](#) | [129-160](#) | [161-192](#) | [193-200](#) >>

[下一頁 >>](#)

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。

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. 設定網頁顯示如下：

物件設定 >> 關鍵字物件設定

索引編號: 1

名稱	<input type="text" value="game"/>
內容	<input type="text"/>

**內容限制:** 最多 3個 字及 63個 字元  
字與字間以空格來區別

您可以使用 %HEX 來取代字元  
範例:  
內容: backdoo%72 virus keep%20out

執行結果:  
1. backdoor  
2. virus  
3. keep out

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 <b>gambling</b> 。當您瀏覽網頁時，含有 <b>gambling</b> (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。

## 4.8.8 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 **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: | 回復出廠預設值 |

索引編號	名稱	索引編號	名稱
<a href="#">1.</a>		<a href="#">17.</a>	
<a href="#">2.</a>		<a href="#">18.</a>	
<a href="#">3.</a>		<a href="#">19.</a>	
<a href="#">4.</a>		<a href="#">20.</a>	
<a href="#">5.</a>		<a href="#">21.</a>	
<a href="#">6.</a>		<a href="#">22.</a>	
<a href="#">7.</a>		<a href="#">23.</a>	
<a href="#">8.</a>		<a href="#">24.</a>	
<a href="#">9.</a>		<a href="#">25.</a>	
<a href="#">10.</a>		<a href="#">26.</a>	
<a href="#">11.</a>		<a href="#">27.</a>	
<a href="#">12.</a>		<a href="#">28.</a>	
<a href="#">13.</a>		<a href="#">29.</a>	
<a href="#">14.</a>		<a href="#">30.</a>	
<a href="#">15.</a>		<a href="#">31.</a>	
<a href="#">16.</a>		<a href="#">32.</a>	

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。

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. 設定網頁顯示如下：

物件設定 >> 關鍵字群組設定

索引編號: 1

名稱:

可用之關鍵字物件

1-game

選定關鍵字物件(最大 16 物件)


>>

<<

確定 清除 取消

可用設定說明如下：



項目	說明
名稱	輸入此設定檔的名稱。
可用之關鍵字物件	您可組合關鍵字物件成爲一個關鍵字群組，所有可用的關鍵字物件都會顯示在本方塊區中。
選定關鍵字物件	按  按鈕增加選定之關鍵字物件於本方塊區中。

- 完成設定之後，按下**確定**按鈕儲存相關設定。

#### 4.8.9 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**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。

物件設定 >> 副檔名物件

副檔名物件設定檔:		回復出廠預設值	
設定檔	名稱	設定檔	名稱
1.		5.	
2.		6.	
3.		7.	
4.		8.	

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。

如欲建立新的設定檔，請依下述步驟進行：

- 按下索引欄位下方的任一編號連結(例如 #1) 進入設定頁面。
- 設定網頁顯示如下：

索引編號: 1      設定檔名稱:

類別	副檔名
影像	<input type="checkbox"/> .bmp <input type="checkbox"/> .dib <input type="checkbox"/> .gif <input type="checkbox"/> .jpeg <input type="checkbox"/> .jpg <input type="checkbox"/> .jpg2 <input type="checkbox"/> .jp2 <input type="checkbox"/> .pct <input type="checkbox"/> .pcx <input type="checkbox"/> .pic <input type="checkbox"/> .pict <input type="checkbox"/> .png <input type="checkbox"/> .tif <input type="checkbox"/> .tiff
<input type="button" value="選擇全部"/> <input type="button" value="清除全部"/>	
影音	<input type="checkbox"/> .asf <input type="checkbox"/> .avi <input type="checkbox"/> .mov <input type="checkbox"/> .mpe <input type="checkbox"/> .mpeg <input type="checkbox"/> .mpg <input type="checkbox"/> .mp4 <input type="checkbox"/> .qt <input type="checkbox"/> .rm <input type="checkbox"/> .wmv <input type="checkbox"/> .3gp <input type="checkbox"/> .3gpp <input type="checkbox"/> .3gpp2 <input type="checkbox"/> .3g2
<input type="button" value="選擇全部"/> <input type="button" value="清除全部"/>	
聲音	<input type="checkbox"/> .aac <input type="checkbox"/> .aiff <input type="checkbox"/> .au <input type="checkbox"/> .mp3 <input type="checkbox"/> .m4a <input type="checkbox"/> .m4p <input type="checkbox"/> .ogg <input type="checkbox"/> .ra <input type="checkbox"/> .ram <input type="checkbox"/> .vox <input type="checkbox"/> .wav <input type="checkbox"/> .wma
<input type="button" value="選擇全部"/> <input type="button" value="清除全部"/>	
Java	<input type="checkbox"/> .class <input type="checkbox"/> .jad <input type="checkbox"/> .jar <input type="checkbox"/> .jav <input type="checkbox"/> .java <input type="checkbox"/> .jcm <input type="checkbox"/> .js <input type="checkbox"/> .jse <input type="checkbox"/> .jsp <input type="checkbox"/> .jtk
<input type="button" value="選擇全部"/> <input type="button" value="清除全部"/>	
ActiveX	

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。
選定關鍵字物件	按 <input type="button" value="&gt;&gt;"/> 按鈕增加選定之關鍵字物件於本方塊區中。

- 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。

## 4.8.10 簡訊(SMS)/郵件服務物件

### 簡訊服務(SMS)供應商

本頁讓您設定 10 組設定檔，後續將運用在應用>>簡訊/郵件警示服務中。

物件設定 >> 簡訊(SMS) / 郵件服務物件

簡訊服務(SMS)供應商	郵件伺服器	回復出廠預設值
索引編號	設定檔名稱	簡訊服務(SMS)供應商
1.		kotsms.com.tw (TW)
2.		kotsms.com.tw (TW)
3.		kotsms.com.tw (TW)
4.		kotsms.com.tw (TW)
5.		kotsms.com.tw (TW)
6.		kotsms.com.tw (TW)
7.		kotsms.com.tw (TW)
8.		kotsms.com.tw (TW)
9.	Custom 1	
10.	Custom 2	

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。
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。

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。

物件設定 >> 簡訊(SMS) / 郵件服務物件

簡訊服務(SMS)供應商	郵件伺服器
索引編號	設定檔名稱
1.	
2.	
3.	
4.	
5.	
6.	

2. 設定網頁顯示如下：

## 設定檔索引編號: 1

設定檔名稱	<input type="text" value="Line_down"/>
服務供應商	<input type="text" value="kotsms.com.tw (TW)"/>
使用者名稱	<input type="text" value="line1"/>
密碼	<input type="password" value="****"/>
簡訊則數	<input type="text" value="10"/>
寄送間隔時間	<input type="text" value="3"/> (秒數)

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。
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。
寄送間隔時間	爲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。

- 完成設定之後，按下**確定**按鈕儲存相關設定。

簡訊服務(SMS)供應商	郵件伺服器	回復出廠預設值
索引編號	設定檔名稱	簡訊服務(SMS)供應商
1.	Line_down	kotsms.com.tw (TW)
2.		kotsms.com.tw (TW)
3.		kotsms.com.tw (TW)
4.		kotsms.com.tw (TW)
5.		kotsms.com.tw (TW)
6.		kotsms.com.tw (TW)
7.		kotsms.com.tw (TW)

## 客製化簡訊服務

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(SMS) / 郵件服務物件

索引編號	設定檔名稱	簡訊服務(SMS)供應商
1.		kotsms.com.tw (TW)
2.		kotsms.com.tw (TW)
3.		kotsms.com.tw (TW)
4.		kotsms.com.tw (TW)
5.		kotsms.com.tw (TW)
6.		kotsms.com.tw (TW)
7.		kotsms.com.tw (TW)
8.		kotsms.com.tw (TW)
9.	Custom 1	
10.	Custom 2	

按下索引編號 9 與 10 開啓設定頁面：

物件設定 >> 簡訊(SMS) / 郵件服務物件

### 設定檔索引編號: 9

設定檔名稱	<input type="text" value="Custom 1"/>
服務供應商	<input type="text"/>
<div style="border: 1px solid black; height: 50px; width: 100%;"></div>	
請與您的簡訊服務供應商連絡，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###	
使用者名稱	<input type="text"/>
密碼	<input type="text"/>
簡訊則數	<input type="text" value="10"/>
寄送間隔時間	<input type="text" value="3"/> (秒數)

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。
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	爲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。

完成設定之後，按下**確定**按鈕儲存相關設定。

## 郵件服務物件

本頁讓您設定 10 組設定檔，後續將運用在**應用>>簡訊/郵件警示服務**中。

**物件設定 >> 簡訊(SMS) / 郵件服務物件**

索引編號	設定檔名稱
1.	
2.	
3.	
4.	
5.	
6.	
7.	
8.	
9.	
10.	

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。
設定檔名稱	顯示物件設定檔的檔名。

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。

物件設定 >> 簡訊(SMS) / 郵件服務物件

簡訊服務供應商	郵件伺服器
<b>索引編號</b>	
<a href="#">1.</a>	
<a href="#">2.</a>	
<a href="#">3.</a>	
<a href="#">4.</a>	

2. 設定網頁顯示如下

物件設定 >> 簡訊(SMS) / 郵件服務物件

設定檔索引編號: 1

設定檔名稱	<input type="text" value="Mail_notify"/>
SMTP伺服器	<input type="text" value="192.168.1.98"/>
SMTP 埠號	<input type="text" value="250"/>
寄件人位址	<input type="text" value="carrieni@draytek.com"/>
<input type="checkbox"/> 使用 SSL	
<input checked="" type="checkbox"/> 驗證	
使用者名稱	<input type="text" value="carrieni"/>
密碼	<input type="password" value="*****"/>
傳送間隔	<input type="text" value="0"/> (秒)

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。
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。
寄件人位址	輸入寄件人的電子郵件位址。
使用 SSL	勾選此方框啟用此功能。
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。 <b>使用者名稱</b> – 請自訂驗證所需的使用者名稱。 <b>密碼</b> – 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。

3. 完成設定之後，按下**確定**按鈕儲存相關設定。

簡訊服務供應商	郵件伺服器	設定檔名稱
1.		Mail_notify
2.		
3.		
4.		
5.		

#### 4.8.11 通知物件

本頁讓您設定 10 組設定檔，後續將運用在應用>>簡訊/郵件警示服務中。

每個物件可以設定不同的監控條件。

物件設定 >> 通知物件

索引編號	設定檔名稱	設定
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		

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。
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。



如欲建立新的設定檔，請依下述步驟進行：

1. 開啓物件設定>>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。

**物件設定 >> 通知物件**

索引編號	設定檔名稱
<a href="#">1.</a>	
<a href="#">2.</a>	
<a href="#">3.</a>	
<a href="#">4.</a>	
<a href="#">5.</a>	

2. 設定網頁顯示如下：

**物件設定 >> 通知物件**

**設定檔索引編號: 1**

設定檔名稱	Notify_discont	
<b>類別</b>	<b>狀態</b>	
WAN	<input checked="" type="checkbox"/> 中斷連線	<input type="checkbox"/> 重新連線
VPN 通道	<input checked="" type="checkbox"/> 中斷連線	<input type="checkbox"/> 重新連線
溫度警示	<input type="checkbox"/> 超出範圍	

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。
類型	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。

**物件設定 >> 通知物件**

索引編號	設定檔名稱	設定
<a href="#">1.</a>	Notify_discont	WAN VPN
<a href="#">2.</a>		
<a href="#">3.</a>		
<a href="#">4.</a>		

[| 回復出廠預設值 |](#)

## 4.9 數位內容安全管理(CSM)設定檔

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

為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為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](http://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。

**注意:** URL 內容過濾器的優先權高於網頁內容過濾器。

## 4.9.1 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>>基本設定**的**預設規則**中，做為主機依循的標準。

**數位內容安全管理 >> 應用程式管控設定檔**

應用程式管控設定檔列表:

[| 回復出廠預設值 |](#)

設定檔	名稱	設定檔	名稱
<a href="#">1.</a>		<a href="#">17.</a>	
<a href="#">2.</a>		<a href="#">18.</a>	
<a href="#">3.</a>		<a href="#">19.</a>	
<a href="#">4.</a>		<a href="#">20.</a>	
<a href="#">5.</a>		<a href="#">21.</a>	
<a href="#">6.</a>		<a href="#">22.</a>	
<a href="#">7.</a>		<a href="#">23.</a>	
<a href="#">8.</a>		<a href="#">24.</a>	
<a href="#">9.</a>		<a href="#">25.</a>	
<a href="#">10.</a>		<a href="#">26.</a>	
<a href="#">11.</a>		<a href="#">27.</a>	
<a href="#">12.</a>		<a href="#">28.</a>	
<a href="#">13.</a>		<a href="#">29.</a>	
<a href="#">14.</a>		<a href="#">30.</a>	
<a href="#">15.</a>		<a href="#">31.</a>	
<a href="#">16.</a>		<a href="#">32.</a>	

可用設定說明如下：

項目	說明
<a href="#">回復出廠預設值</a>	清除全部的設定資料。
<a href="#">設定檔</a>	顯示索引編號連結讓您點選進入設定頁面。
<a href="#">名稱</a>	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啓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：

設定檔編號：1 設定檔名稱：

<b>IM</b>	<b>P2P</b>	<b>協定</b>	<b>其他</b>
<input type="button" value="選擇全部"/>	<input type="button" value="清除全部"/>		

IM			
啟用	APP名稱	版本	附註
<input type="checkbox"/> <input type="button" value="進階"/>	AIM	5.9	
<input type="checkbox"/>	AIM	6/7	Only block Login. If users have already logged in, AIM services can not be blocked.
<input type="checkbox"/>	AliWWW	2008	
<input type="checkbox"/>	Ares	2.0.9	
<input type="checkbox"/>	BaiduHi	37378	
<input type="checkbox"/>	Fetion	2010	
<input type="checkbox"/>	GaduGadu Protocol		
<input type="checkbox"/>	Google Chat		
<input type="checkbox"/>	ICQ	7	In ICQ6, if Videos are blocked, Voices will be blocked at the same time. In ICQ5 or former versions, Videos and Voices can be blocked separately.
<input type="checkbox"/>	ICU2	8.0.6	

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。
啟用	勾選此方框讓路由器封鎖選定的 APP。
進階	用以開啓跳出視窗以指定 APP 的活動內容(如訊息、檔案傳輸、遊戲、會議)。

下圖顯示協定類型中的各個項目：

數位內容安全管理>>應用程式管控設定檔

設定檔編號：1 設定檔名稱：

IM	P2P	協定	其他
<input type="button" value="選擇全部"/>	<input type="button" value="清除全部"/>		
PROTOCOL			
啟用	APP名稱	版本	附註
<input type="checkbox"/>	DB2		DB2 is a relational database management system (RDBMS) offered by IBM.
<input type="checkbox"/>	DNS		Domain Name System (DNS) protocol is used to translate easily memorized domain names to numerical IP addresses needed for the purpose of locating computer services and devices worldwide.
<input type="checkbox"/>	FTP		File Transfer Protocol (FTP) is used to transfer files from one host to another host over networks.
<input type="checkbox"/>	HTTP	1.1	Hypertext Transfer Protocol (HTTP) is the data communication protocol for the World Wide Web.
<input type="checkbox"/>	IMAP	4.1	Internet message access protocol (IMAP) is a protocol for e-mail retrieval.
<input type="checkbox"/>	IRC	2.4.0	Internet Relay Chat (IRC) is a protocol for live interactive Internet text messaging (chat), synchronous conferencing and file sharing.

下圖顯示 P2P 類型中的各個項目：

數位內容安全管理>>應用程式管控設定檔

設定檔編號：1 設定檔名稱：

IM	P2P	協定	其他
<input type="button" value="選擇全部"/>	<input type="button" value="清除全部"/>		
BitTorrent			
啟用	APP名稱	版本	附註
<input type="checkbox"/>	BitTorrent		The encrypted connection can not be 100% blocked. To block BitComet (1.30), BitSpirit (3.2.1), BitTorrent (4.4.1) and UltraTorrent (2.0).
FastTrack			
啟用	APP名稱	版本	附註
<input type="checkbox"/>	FASTTRACK		To block BareShare (6.2.0.45), iMesh (9.1), KazaA (1.0.0.3) and Shareaza (4.1.0).
Gnutella			
啟用	APP名稱	版本	附註

下圖顯示其他類型中的各個項目：

數位內容安全管理>>應用程式管控設定檔

設定檔編號：1 設定檔名稱：

IM P2P 協定 其他

TUNNEL			
啟用	APP名稱	版本	附註
<input type="checkbox"/>	DynaPass	1.5	
<input type="checkbox"/>	FreeU	10	
<input type="checkbox"/>	HTTP Proxy		
<input type="checkbox"/>	HTTP Tunnel	4.4.4000	
<input type="checkbox"/>	Hamachi	1.0.2.5	
<input type="checkbox"/>	Hotspot Shield	3.19	Block Hotspot Shield from establishing VPN connections. Please note that the APP Enforcement needs to be enabled prior than the VPN connections, or the blocking may not be successful.
<input type="checkbox"/>	MS Teredo		
<input type="checkbox"/>	PGPNet	7.0.3	
<input type="checkbox"/>	Ping Tunnel	0.61	
<input type="checkbox"/>	RealTunnel	1.0.1	

## 4.9.2 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。

數位內容安全管理 >> APPE 特徵碼更新

應用程式管控授權

啟用

[狀態: Not Activated]

更新設定

APPE 模組版本: 2.0

自網際網路取得之新版本: -- 下載

透過介面更新: 自動選定

(Waiting for WAN connection...)

設定下載伺服器	auto-selected	更多
特徵碼驗證 / 下載訊息 [2000-01-01 00:00:00] Load APPE signature failed. System will use APPE default signature.		

手動更新	輸入
------	----

自動更新				
<input type="checkbox"/>	排程更新			
<input checked="" type="radio"/>	每:	1 (時)	00 (分鐘過後)	
<input type="radio"/>	每日:	0 (時)	00 (分)	
<input type="radio"/>	每週:	星期日 (日)	0 (時)	00 (分)

OK

可用設定說明如下：

項目	說明
更新設定	<p><b>APPE 模組版本</b> – 顯示 APP 特徵碼目前的版本。</p> <p><b>自網際網路取得之新版本</b>– 下載按鈕僅在 Vigor 路由器偵測出新的 APPE 版本之後才会有作用，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<b>確定</b>按鈕離開該對話盒並開始更新特徵碼。</p> <p><b>透過介面更新</b> – 選擇一個 WAN 介面作為 APP 特徵碼更新的通道。</p>
設定下載伺服器	<p>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。</p> <p><b>特徵碼驗證/下載訊息</b>–顯示 APPE 特徵碼更新時的狀態。</p>
手動更新	<p><b>輸入</b> – 按下此鈕開啓如下頁面，按<b>選擇檔案</b>尋找先前自居易官網下載取得之特徵碼檔案，然後再按<b>更新</b>按鈕，等待系統完成更新作業。</p>

數位內容安全管理 >> APPE 特徵碼更新	
輸入 APPE 特徵碼 選擇特徵碼檔案 <input type="button" value="選擇檔案"/> 未選擇檔案 按下更新以便上傳檔案。 <input type="button" value="更新"/>	
<input type="button" value="Cancel"/>	
自動更新	排成更新 - 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。

### 4.9.3 URL 內容過濾器設定檔

為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為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。

數位內容安全管理 >> URL 內容過濾器設定檔

URL 內容過濾器設定檔表格:

[| 回復出廠預設值 |](#)

設定檔	名稱	設定檔	名稱
1.		5.	
2.		6.	
3.		7.	
4.		8.	

管理訊息 (最多 255 個字元)

```
<body><center><br><p>The requested Web page has been blocked by URL Content Filter.
<p>Please contact your system administrator for further information.</center></body>
```

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。
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	您可以是您的需要輸入所需的訊息。 <b>預設訊息內容</b> - 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 <b>管理訊息</b> 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，開啓如下頁面。

**數位內容安全管理 >> URL 內容過濾器設定檔**

索引編號: 1

設定檔名稱:

優先權: 二者選一: URL存取控制優先  記錄:

**1.URL 存取控制**

啟用URL存取控制       防止透過IP位址對網站進行存取

動作:

群組/物件選項

**2.網頁特徵**

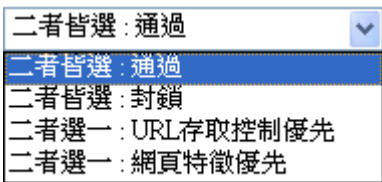


啟用限制網頁特徵

動作:   Cookie  伺服器  上傳      副檔名設定檔:

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。 <b>二者皆選:通過</b> - 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。 <b>二者皆選:封鎖</b> - 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。 <b>二者擇一: URL 存取控制優先</b> - 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。

	<p>二者擇一：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。</p>  <p>二者皆選：通過 二者皆選：封鎖 二者選一：URL存取控制優先 二者選一：網頁特徵優先</p>
<p>紀錄</p>	<p>無 – 沒有任何關於此設定檔的紀錄保留下來。 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。 全部 – 所有的動作(包含通過與封鎖)都會記錄在 Syslog 中。</p>  <p>無 通過 封鎖 全部</p>
<p>URL 存取控制</p>	<p>啟用 URL 存取控制 - 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，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。</p> <p>防止從 IP 位址存取網頁- 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。</p> <p>動作 – 此功能僅在您選擇了二者擇一：URL 存取控制優先或二者擇一：網頁特徵優先時才能使用。</p> <p>通過 - 允許進入含有關鍵字清單中之關鍵字的網頁。 封鎖 - 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。</p>  <p>封鎖 通過 封鎖</p> <p>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。</p>

物件/群組編輯	
關鍵字物件	無
或關鍵字物件	無
或關鍵字物件	無
或關鍵字物件	無
或關鍵字物件	無
或關鍵字物件	無
或關鍵字物件	無
或關鍵字物件	無
或 關鍵字群組	無
或關鍵字群組	無
或關鍵字群組	無
或關鍵字群組	無
或關鍵字群組	無
或關鍵字群組	無
或關鍵字群組	無
或關鍵字群組	無
或關鍵字群組	無

---

<b>網頁特徵</b>	<p><b>啓用限制網頁特徵</b> - 勾選此方塊讓關鍵字被封鎖或是放行。</p> <p><b>動作</b> - 此功能僅在您選擇了二者選一: <b>URL 存取控制優先</b> 或二者選一: <b>網頁特徵優先</b>時才能使用。</p> <p><b>通過</b> - 允許進入含有關鍵字清單中之關鍵字的網頁。</p> <p><b>封鎖</b> - 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。</p> <p><b>Cookie</b> - 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。</p> <p><b>Proxy</b> - 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。</p> <p><b>副檔名設定檔</b> - 請自物件設定&gt;&gt;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。</p> <p><b>副檔名設定檔:</b> <input type="button" value="無"/></p>
-------------	--

完成設定之後，按下**確定**按鈕儲存相關設定。

## 4.9.4 網頁內容過濾器設定檔

有數種方式可以啟動路由器的網頁內容過濾器(WCF) – 透過**服務啟動精靈**、**數位內容安全管理**>>**網頁內容過濾器設定檔**或是**系統維護**>>**開啓授權碼**。

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**)。

不過，如果您使用網頁內容過濾器設定檔來啟動 WCF 功能，您必須登入(**MyVigor**)伺服器，因此，您得先上伺服器註冊一組帳號才能使用相關的服務，請參考如何建立 MyVigor 帳號相關章節。

**注意:** 如果您已經使用服務啟動精靈來啟動 WCF 服務，您可以跳過此節。

WCF 採取特定服務供應商開發的機制來進行，不論是啟動 WCF 功能或是取得新的授權碼，您都必須按下**啟動**才能達成要求，要注意的是符合目前 Vigor 路由器需求的服務供應商提供的是短期的試用版，如果您想要購買正式版本，請與通路商或是經銷商聯絡。

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**開啓設定頁面，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**連結開啓另一視窗然後選擇需要的伺服器。

**注意 1:** WCF 並非 Vigor 路由器的內建機制，該服務是由 Commtouch 公司所提供，如果您想要使用此類服務(試用版或是正式版)，您必須先進行啓用的程序。若您想要使用正式版，請先與經銷商聯絡，獲取更多更詳細的 WCF 資訊。

**注意 2:** Commtouch 已經併入 Cyren，其 GlobalView 服務仍將持續提供強大且以雲端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>

數位內容安全管理 >> 網頁內容過濾器設定檔

### 網頁過濾器授權碼

啓動

[狀態:Commtouch] [起始日期:2013-02-25 到期日期:2013-03-27]

設定搜尋伺服器	auto-selected	更多
設定測試伺服器	auto-selected	更多
測試站點，檢查該站是否已被歸類		

網頁內容過濾器設定檔表格:

| 回復出廠預設值 |

設定檔	名稱	設定檔	名稱
1.	Default	5.	
2.		6.	
3.		7.	
4.		8.	

管理訊息 (最多 255 個字元)

預設訊息

快取: L1 + L2 快取

```
<body><center><br><br><p>The requested Web page <br> from %SIP% <br>to %URL% <br>that is categorized with %CL% <br>has been blocked by %RNAME% Web Content Filter.<p>Please contact your system administrator for further information.</center></body>
```

說明:

%SIP% - 來源 IP, %DIP% - 目的地 IP, %URL% - URL

%CL% - 類別, %RNAME% - 路由器名稱

確定

可用設定說明如下：

項目	說明
----	----

啓動	按下此鈕登入 MyVigor 以便啓動 WCF 服務。
設定搜尋伺服器	建議您使用預設的設定，當您以 WCF 設定檔爲基準，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。
更多	按下此鈕開啓畫面選擇另外的伺服器。
測試站點，檢查該站是否已被歸類	按下此連結進行驗證動作。
回復出廠預設值	按下此連結回復出廠預設值。
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 <b>管理訊息</b> 方框內。
快取	<p><b>無</b> – 路由器將會透過 WCF 機制檢查使用者想要登入的 URL，處理的速度爲一般，這個選項可提供最準確的 URL 過濾作業。</p> <p><b>L1</b> – 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。</p> <p><b>L2</b> – 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。</p> <p><b>L1+L2 快取</b> – 路由器將會以 L1 加上 L2 的功能快速檢查 URL。</p>

您可設定 8 組網頁內容過濾器設定檔，請按索引編號連結，開啓如下頁面。分類中的項目依照不同的服務供應商而有所改變，如果您已經且啓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。

設定檔索引編號: 1

設定檔名稱:

紀錄:

**黑/白名單**

啟用

動作:  群組/物件選項

---

**動作:**

群組	分類
兒童防護 <input type="button" value="選擇全部"/> <input type="button" value="清除全部"/>	<input checked="" type="checkbox"/> 酒精與菸 <input checked="" type="checkbox"/> 仇恨與無法容忍 <input checked="" type="checkbox"/> 色情與性 <input checked="" type="checkbox"/> 校園作弊 <input checked="" type="checkbox"/> 虐待兒童圖片
休閒 <input type="button" value="選擇全部"/> <input type="button" value="清除全部"/>	<input type="checkbox"/> 娛樂 <input type="checkbox"/> 旅行 <input type="checkbox"/> 遊戲 <input type="checkbox"/> 娛樂休閒
商務	<input checked="" type="checkbox"/> 犯罪活動 <input checked="" type="checkbox"/> 非法藥品 <input checked="" type="checkbox"/> 暴力 <input checked="" type="checkbox"/> 性教育
	<input checked="" type="checkbox"/> 賭博 <input checked="" type="checkbox"/> 裸露 <input checked="" type="checkbox"/> 武器 <input checked="" type="checkbox"/> 粗俗不雅 <input type="checkbox"/> 運動 <input type="checkbox"/> 時裝美容

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。
黑名單/白名單	<p><b>啟用</b> – 勾選此方塊啟用過濾機制，利用黑白名單的內文來決定。請按編輯按鈕開啓關鍵字物件/群組視窗，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。</p> <p><b>動作, 通過</b> – 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。</p> <p><b>動作, 封鎖</b> – 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。</p>
動作	<p><b>通過</b> – 允許進入勾選的方塊等相關類型頁面。</p> <p><b>封鎖</b> – 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。</p>
Log(紀錄)	<p><b>無</b> – 沒有任何關於此設定檔的紀錄保留下來。</p> <p><b>通過</b> – 只有通過動作會記錄在 Syslog 中。</p> <p><b>封鎖</b> – 只有封鎖動作會記錄在 Syslog 中。</p> <p><b>全部</b> – 所有的動作(包含通過與封鎖)都會記錄在 Syslog 中。</p> <p>Log: <input type="button" value="封鎖"/></p> <div style="border: 1px solid black; padding: 2px; width: fit-content;"> <p>無</p> <p>通過</p> <p style="background-color: #e0e0e0;">封鎖</p> <p>全部</p> </div>

完成設定之後，按下**確定**按鈕儲存相關設定。



## 4.9.5 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。

**注意：**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。

數位內容安全管理 >> DNS 過濾器

DNS 過濾器設定檔表

[| 回復出廠預設值 |](#)

設定檔	名稱	設定檔	名稱
1.		5.	
2.		6.	
3.		7.	
4.		8.	

DNS 過濾器本地設定

DNS 過濾器	<input type="checkbox"/> 啟用
Syslog	無 <input type="button" value="v"/>
WCF	無 <input type="button" value="v"/>
UCF	無 <input type="button" value="v"/>
啟用封鎖頁面	<input checked="" type="checkbox"/> 啟用

管理訊息 (最多 255 個字元)

[預設訊息](#)

```
<body><center><br><br><br><p>The requested Web page <br> from %SIP% <br>to %URL%
<br>that is categorized with %CL% <br>has been blocked by %RNAME% DNS Filter.<p>Please
contact your system administrator for further information.</center></body>
```

說明:


%SIP% - 來源 IP, %URL% - URL

%CL% - 類別, %RNAME% - 路由器名稱

[確定](#)

[取消](#)

可用設定說明如下：

項目	說明
DNS 過濾器設定檔表	<p>顯示不同的 DNS 過濾器設定檔清單資料。</p> <p>按下索引編號連結開啓如下頁面，然後輸入設定檔名稱並依照您的需要指定 WCF/UCF 等過濾器設定檔以資套用。</p> <p>數位內容安全管理 &gt;&gt; DNS 過濾器</p> <p>索引編號 1</p> 

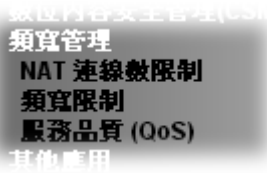
<b>DNS 過濾器本地設定</b>	<p>若尚未設定好任何 DNS 設定檔，此處的基本設定將會套用至 DNS 過濾器。</p> <p><b>DNS 過濾器</b> - 勾選<b>啟用(Enable)</b>以便啟用此功能。</p> <p><b>Syslog</b> - 過濾結果將依照 Syslog 設定來記錄。</p> <ul style="list-style-type: none"> <li>● <b>無(None)</b> - 此設定沒有任何內容會被記錄下來。</li> <li>● <b>通過(Pass)</b> - 只有封包通過的記錄會被轉往 Syslog。</li> <li>● <b>封鎖(Block)</b> - 只有封包被封鎖的記錄會被轉往 Syslog。</li> <li>● <b>全部(All)</b> - 所有的動作(通過與封鎖)記錄都會被轉往 Syslog。</li> </ul> <p><b>WCF</b>- 設定網頁內容過濾器的過濾條件。</p> <p><b>UCF</b> - 設定 URL 內容過濾器的過濾條件。</p> <p><b>啟用封鎖頁面</b> - 勾選後即可封鎖相關頁面。</p>
<b>管理訊息</b>	<p>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。</p>

完成設定之後，按下**確定**按鈕儲存相關設定。



## 4.10 頻寬管理

下面是頻寬管理的設定項目：



### 4.10.1 NAT 連線數限制

擁有虛擬 IP 的電腦可以透過 NAT 路由器存取網際網路，針對此連線需求路由器將會產生 NAT 連線數的紀錄，P2P (Peer to Peer) 應用程式(如 BitTorrent)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。為了解決這種問題，您可以使用連線數限制來限制指定主機的連線數。

在**頻寬管理**群組中，按 **NAT 連線數限制** 開啓如下的網頁。

頻寬管理 >> NAT 連線數限制

#### NAT 連線數限制

啓用  停用

預設最大連線數:

#### 限制清單

索引	起始 IP	結束 IP	最大連線數
----	-------	-------	-------

**指定限制**

起始 IP:  結束 IP:

最大連線數

管理訊息 (最多 256 個字元)

**時間排程**

索引號碼(1-15)於 **排程** 設定: , , ,

**附註:** 排程設定中之動作與間置逾時欄位不適用於此。

如果要啓動限制連線數的功能，只要在此頁面上按**啓用**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	啓用 - 按此鈕啓動連線數限制功能。 停用 - 按此鈕關閉連線數限制功能。

	<b>預設最大連線數</b> - 定義區域網路中每台電腦的預設連線數。
<b>限制清單</b>	顯示網頁中所設定的指定限制之電腦清單資料。
<b>指定限制</b>	<p><b>起始 IP</b> - 定義限制連線數的起始 IP 位址。</p> <p><b>結束 IP</b> - 定義限制連線數的結束 IP 位址。</p> <p><b>最大連線數</b> - 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。</p> <p><b>新增</b> - 新增指定連線數限制並顯示在上面的框框中。</p> <p><b>編輯</b> - 允許您編輯選定的連線數設定。</p> <p><b>刪除</b> - 刪除限制清單上任何一個您所選定的設定。</p>
<b>管理訊息</b>	<p>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。</p> <p><b>預設訊息</b> - 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。</p>
<b>索引號碼(1-15)於排程設定..</b>	您可以輸入四組時間排程，所有的排程都可在 <b>應用-排程</b> 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。

## 4.10.2 頻寬限制

從 FTP,HTTP 或是某些 P2P 應用程式的下行或上行資料會佔據很大的頻寬，並影響其他程式的運作。請使用限制頻寬讓頻寬的應用更有效率。

在**頻寬管理**群組中，按**頻寬限制**開啓如下的網頁。

頻寬管理 >> 頻寬限制

**頻寬限制**

啓用     IP 路由子網     停用  
 預設傳送限制:  Kbps    預設接收限制:  Kbps  
 允許自動調整取得最佳利用 **可用頻寬**.

**限制清單**

索引編號	起始 IP	結束 IP	傳送限制	接收限制	共享

**指定限制**

起始 IP:     結束 IP:   
 每一個     共享傳輸限制:  Kbps    接收限制:  Kbps  
       

**聰明頻寬限制**

對於不在限制清單中的 LAN IP，當連線數超過

傳送限制:  Kbps    接收限制:  Kbps

**附註：**對傳送/接收來說，設定值為 "0" 表示頻寬不受任何限制。

---

**時間排程**

索引號碼(1-15)於 **排程** 設定: , , ,

**附註：**排程設定中之動作與間置逾時欄位不適用於此。

如果要啓動限制頻寬的功能，只要在此頁面上按**啓用**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
<b>頻寬限制</b>	<p><b>啓用</b> - 按此鈕啓動限制頻寬功能。</p> <p><b>應用至第二子網路</b> - 勾選此方塊套用頻寬限制至<b>區域網路 &gt;&gt;基本設定</b>中所指定的第二子網。</p> <p><b>停用</b> - 按此鈕關閉限制頻寬功能。</p> <p><b>預設傳送限制</b> - 定義區域網路中每台電腦預設的上行速度。</p> <p><b>預設接收限制</b> - 定義區域網路中每台電腦預設的下行速度。</p> <p><b>允許自動調整取得最佳利用 可用頻寬</b> - 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。</p>

	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。
<b>限制清單</b>	顯示網頁中所設定的指定限制之電腦清單資料。
<b>指定限制</b>	<p><b>起始 IP</b> - 定義限制頻寬的起始 IP 位址。</p> <p><b>結束 IP</b> - 定義限制頻寬的結束 IP 位址。</p> <p><b>每一個/共用</b> - 選擇 <b>Each</b> 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 <b>Shared</b> 則讓範圍內的 IP 共用傳送限制與接收限制的全部頻寬。</p> <p><b>傳送限制</b> - 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。</p> <p><b>接收限制</b> - 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。</p> <p><b>新增</b> - 新增指定速度限制並顯示在上面的框框中。</p> <p><b>更新</b> - 允許您編輯選定的限制設定。</p> <p><b>刪除</b> - 刪除限制清單上任何一個您所選定的設定。</p>
<b>聰明頻寬限制</b>	<p>勾選此框即可由系統自動控制頻寬。</p> <p><b>傳送限制</b> - 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。</p> <p><b>接收限制</b> - 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。</p>
<b>索引號碼(1-15)於排程設定..</b>	您可以輸入四組時間排程，所有的排程都可在 <b>應用-排程</b> 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。

### 4.10.3 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。

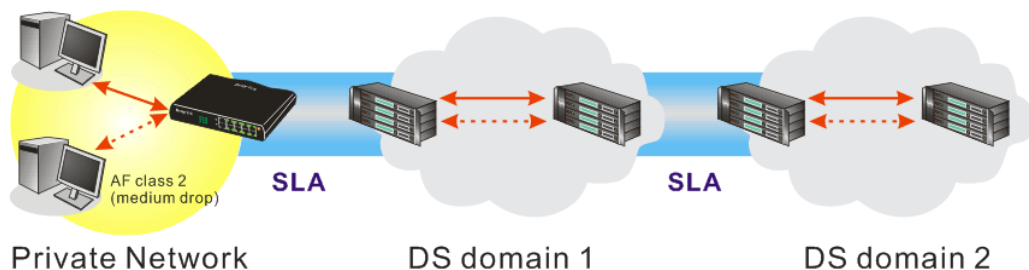
另一個理由是由於網路的擁擠狀況，內部連線迴路速度不符合或是傳輸流量過份聚集，資料封包排隊等候傳送，整個傳輸慢了下來。如果沒有定義後先後順序，以指定在滿檔的隊伍中哪個封包必須丟棄，上述提及的應用程式封包就可能成為被捨棄掉的一個，這樣的話對應用程式的成效會造成令人無法想像的後果。

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，例如為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。



QoS 將以上傳/下載速度比率來定義，我們也會提供一些 QoS 需求應用給您參考，設定數值會依照網路實際狀況而有所改變。

在**頻寬管理**群組中，選擇**服務品質**開啓如下的網頁。

基本設定										回復出廠預設值
索引編號	狀態	類寬	方向	類別 1	類別 2	類別 3	其他	UDP 頻寬控制	連線狀態統計	
WAN1	停用	100000Kbps/100000Kbps		25%	25%	25%	25%	不啟用	狀態	設定
WAN2	停用	100000Kbps/100000Kbps		25%	25%	25%	25%	不啟用	狀態	設定
WAN3	停用	100000Kbps/100000Kbps		25%	25%	25%	25%	不啟用	狀態	設定
WAN4	停用	100000Kbps/100000Kbps		25%	25%	25%	25%	不啟用	狀態	設定

類別規則			
索引編號	名稱	規則	服務類型
類別 1		編輯	編輯
類別 2		編輯	
類別 3		編輯	

<input checked="" type="checkbox"/> 啟用VoIP SIP/RTP第一優先
SIP UDP 埠號: <input type="text" value="5060"/> (預設值:5060)
<input type="button" value="確定"/>

可用設定說明如下：

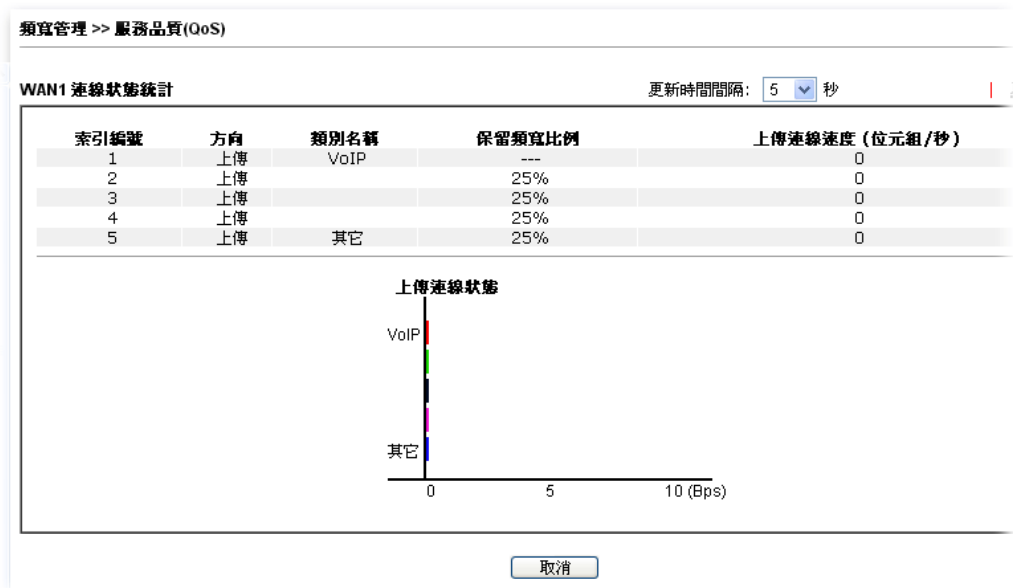
項目	說明
基本設定	<b>索引編號</b> - 顯示 WAN 介面的編號。 <b>狀態</b> - 顯示該 WAN 介面目前是否為停用或是啟用。 <b>頻寬</b> - 顯示該 WAN 介面的上下傳頻寬設定值。 <b>方向</b> - 顯示此功能會影響的上下傳方向。 <b>類別 1/類別 2/類別 3/其他</b> - 顯示每個類別的所佔的頻寬比例。 <b>UDP 頻寬控制</b> - 顯示該控制為啟用或是停用。 <b>連線狀態統計</b> - 顯示 QoS 的連線狀態統計情形。 <b>設定</b> - 允許設定一般 WAN 介面的 QoS 設定。
類別規則	<b>索引編號</b> - 顯示您可以編輯的類別編號。 <b>名稱</b> - 顯示該類別的名稱。 <b>規則</b> - 允許設定該選定類別的細部內容。 <b>服務類型</b> - 允許設定該服務類型的細部內容。
啟用 VoIP SIP/RTP 第一優先	當此功能啟用的時候，VoIP SIP/UDP 封包會以最高優先傳送出去。 <b>SIP UDP 埠號</b> - 設定 SIP 使用的埠號。

本頁顯示 WAN 介面上的 QoS 設定成果，按下**設定**連結進入下一層頁面，至於類別規則，則按下該頁面上的**編輯**按鈕進入另一層畫面來設定即可。

您可以設定 WAN 介面的一般設定，並視您的需要來編輯類別規則並且編輯類別規則的服務類型。

## 連線狀態統計

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 介面已經啓用的狀態下始有作用。



## 基本設定

當您按下**設定**時，您可調整 WAN 介面的 QoS 頻寬比率，系統提供您四種類別作為 QoS 控制之用，前三種(類別 1 到類別 3)可視您的需求來調整，而最後一個則保留給那些不符合上面定義之規則等封包使用。

類寬管理 >> 服務品質(QoS)

### WAN1 基本設定

啓用服務品質(QoS)控制功能 上傳

WAN 下載頻寬	<input type="text" value="100"/>	<input type="radio"/> Kbps <input checked="" type="radio"/> Mbps
WAN 上傳頻寬	<input type="text" value="100"/>	<input type="radio"/> Kbps <input checked="" type="radio"/> Mbps

索引編號	類別名稱	保留頻寬比例
類別 1		<input type="text" value="25"/> %
類別 2		<input type="text" value="25"/> %
類別 3		<input type="text" value="25"/> %
	其他	<input type="text" value="25"/> %

啓用 UDP 頻寬控制 頻寬限制比率  %

優先處理對外 TCP ACK

附註: 1. 在啓用 QoS 之前，您應該先測試實際的頻寬，如果頻寬有誤，QoS 可能無法正常運作。  
2. 您可進行速度測試，透過 <http://speedtest.net> 或與您的 ISP 業者聯絡，以進行速度測試程式。

確定

清除

取消

可用設定說明如下：

項目	說明
啓用服務品質(QoS)控制	預設狀態下，這個功能是啓用的。



	<p>請同時定義 QoS 控制設應所應用的流量方向。</p> <p><b>下載</b>- 僅適用於進入的封包。</p> <p><b>上傳</b>- 僅適用於輸出的封包。</p> <p><b>雙向</b>- 適用於進入與輸出的封包。</p> <p>勾選此方塊並按下<b>確定</b>，<b>連線狀態統計</b>連結即可出現在此頁面上。</p>
<b>WAN 下載頻寬</b>	<p>允許您設定 WAN 資料輸入的連線速度。預設值為 10000kbps。</p>
<b>WAN 上傳頻寬</b>	<p>允許您設定 WAN 資料輸入的連線速度。預設值為 10000kbps。</p> <p>例如，您的 ADSL 支援 1M 的下行與 256K 上行速度，請將 <b>WAN 下載頻寬</b> 設定為 1000kbps 而 <b>WAN 上傳頻寬</b> 設定為 256kbps。</p>
<b>保留頻寬比例</b>	<p>保留作為群組索引所可應用的比率。</p>
<b>啓用 UDP 頻寬控制</b>	<p>勾選此設定並在右邊設定限制的頻寬比率，這是 TCP 應用的一種保護機制，因為 UDP 應用程式會消耗很多的頻寬。</p>
<b>優先處理對外 TCP ACK</b>	<p>下載和上傳之的頻寬在 ADSL2+ 環境中差異是很大的，因為下載速度可能會受到上傳 TCP ACK 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。</p>
<b>限制頻寬比率</b>	<p>此處所輸入的比率保留作為 UDP 應用之需。</p>

**注意:** 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。



## 編輯 QoS 的類別規則

- 前三種(類別 1 到類別 3)可視您的需求來調整，編輯或是刪除類別規則，請按該項類別的編輯連結即可。

類寬管理 >> 服務品質(QoS)

**基本設定** | 回復出廠預設值 |

索引編號	狀態	類寬	方向	類別 1	類別 2	類別 3	其他	UDP	類寬控制	連線狀態統計	
WAN1	停用	100000Kbps/100000Kbps		25%	25%	25%	25%		不啓用	狀態	設定
WAN2	停用	100000Kbps/100000Kbps		25%	25%	25%	25%		不啓用	狀態	設定
WAN3	停用	100000Kbps/100000Kbps		25%	25%	25%	25%		不啓用	狀態	設定
WAN4	停用	100000Kbps/100000Kbps		25%	25%	25%	25%		不啓用	狀態	設定

**類別規則**

索引編號	名稱	規則	服務類型
類別 1		編輯	
類別 2		編輯	編輯
類別 3		編輯	

啓用VoIP SIP/RTP第一優先

SIP UDP 埠號:  (預設值:5060)

- 在您按下編輯連結之後，您可以看到如下的頁面。現在您可以定義該類別的名稱，在本例中，TEST 用來作為類別索引 1 的名稱。

類寬管理 >> 服務品質

**類別索引#1**

名稱   封包標籤為:


編號	狀態	本機地址	遠端位址	DiffServ CodePoint	服務類型
1	<input type="radio"/> 不啓用	任何一種	任何一種	ANY	undefined

- 若要新增一個新的規則，請按**新增**開啓下列畫面。

## 編輯規則

<input checked="" type="checkbox"/> 啟用	<input type="checkbox"/> 硬體加速
以太網路類型	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
本機地址	192.168.1.66 <input type="button" value="編輯"/>
遠端位址	Any <input type="button" value="編輯"/>
DiffServ CodePoint	ANY
服務類型	---Predefined---
<b>附註：</b> 請先選擇/設定 <b>服務類型</b> ！	

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。
硬體加速	勾選此方塊啟用硬體加速功能。
本機位址	按 <b>編輯</b> 按鈕以設定規則的來源位址。
遠端位址	按 <b>編輯</b> 按鈕以設定規則的目標位址。 <b>編輯</b> - 讓您編輯來源/目標位址資訊。
	 <p><b>位址類型</b> - 決定來源位址的位址類型。 關於<b>任何位址</b>，您無須填入起始 IP 位址，由系統決定。 關於<b>單一位址</b>，您可以填入起始 IP 位址。 關於<b>範圍位址</b>，您必須填入起始和終點 IP 位址。 關於<b>子網路位址</b>，您必須填入起始 IP 位址和子網路遮罩。</p>
<b>DiffServ CodePoint</b>	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。
<b>服務類型</b>	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。

- 完成設定之後，按下**確定**按鈕儲存相關設定。

另外，您可以為一種類別指定 20 組規則，如果您想要編輯現存的規則，請點選該項按鈕，然後按下**編輯**鈕開啓編輯視窗以修改該規則。

類別索引#1

名稱   封包標籤為: 預設值 ▼

編號	狀態	本機地址	遠端位址	DiffServ CodePoint	服務類型
1 <input type="radio"/>	不啟用	任何一種	任何一種	ANY	undefined
2 <input type="radio"/>	啟用	192.168.1.66	任何一種	ANY	ANY

### 編輯類別規則的服務類型

- 要新增、編輯或刪除服務類型，請按服務類型區域下方的**編輯**連結。

| [回復出廠預設值](#) |

**基本設定**

索引編號	狀態	類寬	方向	類別 1	類別 2	類別 3	其他	UDP	類寬控制	連線狀態統計	
WAN1	停用	100000Kbps/100000Kbps		25%	25%	25%	25%		不啟用	狀態	設定
WAN2	停用	100000Kbps/100000Kbps		25%	25%	25%	25%		不啟用	狀態	設定
WAN3	停用	100000Kbps/100000Kbps		25%	25%	25%	25%		不啟用	狀態	設定
WAN4	停用	100000Kbps/100000Kbps		25%	25%	25%	25%		不啟用	狀態	設定

**類別規則**

索引編號	名稱	規則	服務類型
類別 1		<a href="#">編輯</a>	
類別 2		<a href="#">編輯</a>	<a href="#">編輯</a>
類別 3		<a href="#">編輯</a>	

啟用VoIP SIP/RTP第一優先

SIP UDP 埠號:  (預設值:5060)

- 在您按下**編輯**按鈕之後，下述畫面將會出現。

**使用者自訂服務類型**

號碼	名稱	通訊協定	通訊埠
1	空白	-	-

- 新增一個規則請按下**新增**按鈕開啓設定頁面，如果您想要編輯現有的服務類型，請選擇該項並按下**編輯**連結開啓如下頁面：

編輯服務類型

服務名稱	<input type="text" value="upload"/>
服務類型	TCP <input type="text" value="6"/>
通訊埠組態	
類型	<input checked="" type="radio"/> 單一 <input type="radio"/> 範圍
通訊埠號	<input type="text" value="0"/> - <input type="text" value="0"/>

可用設定說明如下：

項目	說明
服務名稱	輸入新的服務名稱。
服務類型	請選擇新服務所需的類型(TCP, UDP or TCP/UDP)。
通訊埠組態	<b>類型</b> - 按 <b>單一</b> 或是 <b>範圍</b> ，如果您選擇的是範圍，您必須輸入起始通訊埠號和結束通訊埠號。 <b>通訊埠號</b> -如果您選擇範圍為服務類型，請在此輸入起始和結束通訊埠號。

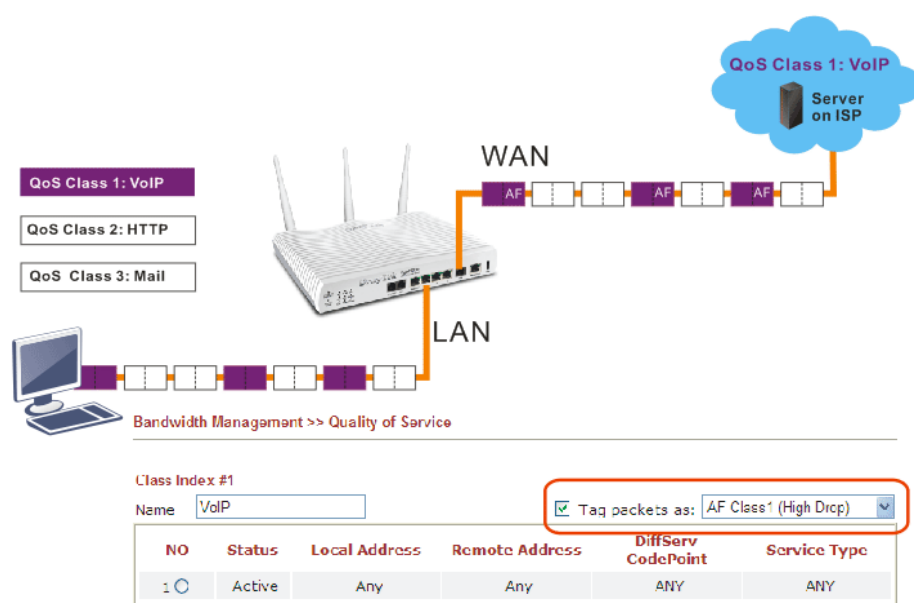
- 完成設定之後，按下**確定**按鈕儲存相關設定。

另外，您可以指定 10 組服務類型，如果您想要編輯或是刪除現存的服務類型，請點選該項按鈕，然後按下**編輯**鈕開啓編輯視窗以修正該服務類型。

## 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)。



## 4.11 其他應用

下圖顯示其他應用的功能項目：



### 4.11.1 動態 DNS

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

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

啓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](http://hostname.dyndns.org))，且獲得一個帳號，其使用者名稱爲 *test*；密碼爲 *test*。
2. 自其他應用群組選擇動態 DNS 設定，下述頁面即會出現在螢幕上。

其他應用 >> 動態 DNS 設定

動態 DNS 設定 | 回復出廠預設值 |

啓用動態 DNS 設定 檢視記錄 強迫更新

自動更新間隔  分鐘 (1~14400)

帳號:

索引編號	WAN 介面	網域名稱	啓用
1.	WAN1 優先		X
2.	WAN1 優先		X
3.	WAN1 優先		X
4.	WAN1 優先		X
5.	WAN1 優先		X
6.	WAN1 優先		X

可用設定說明如下：

項目	說明
回復出廠預設值	清除全部設定資料並回復到出廠的設定。
啟用動態 DNS 設定	勾選此方塊啟用此功能。
檢視記錄	可開啓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。
網域名稱	顯示您在 DDNS 設定頁面上所設定的網域名稱。
啟用	顯示此帳號目前是啟用或是停用狀態。

3. 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)。

其他應用 >> 動態 DNS 設定 >> 動態 DNS 帳號設定

索引編號: 1

<input checked="" type="checkbox"/> 啟用動態 DNS 帳號	
WAN 介面	WAN1 優先
服務供應商	dyndns.org (www.dyndns.org)
服務類型	動態
網域名稱	chronic6653 . dyndns.org dyndns.org
登入名稱	chronic6653 (最多 64 個字元)
密碼	***** (最多 23 個字元)
<input type="checkbox"/> 萬用字元	
<input type="checkbox"/> 備份 MX	
郵件延伸程式	
決定真實 WAN IP	WAN IP
	WAN IP
	網際網路 IP
	確定 清除 取消

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	選擇適合的介面以套用相關設定。 <b>WAN1/WAN2/WAN3/WAN4 優先</b> - 連線時，路由器將使用 WAN1/WAN2/WAN3/WAN4 作為此帳號第一頻道，如果 WAN1/WAN2/WAN3/WAN4 連線失敗，路由器將使用其他的 WAN 介面來連線。 <b>限用 WAN1/WAN2/WAN3/WAN4</b> - 連線時，路由器將使用 WAN1/WAN2/WAN3/WAN4 作為此帳號唯一的連線頻道。

	<div style="border: 1px solid black; padding: 2px;">         WAN1 優先          限用 WAN1          WAN2 優先          限用 WAN2          WAN3 優先          限用 WAN3          WAN4 優先          限用 WAN4       </div>
服務供應商	為此 DDNS 帳號選擇適當的服務供應商。
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。
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。
決定真實 WAN IP	<p>如果路由器安裝在 NAT 路由器的後端，您可以啓用此功能來定位真實的 WAN IP 位址。</p> <p>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。</p> <p>有二種方法可以選擇</p> <div style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <div style="border-bottom: 1px solid black; padding: 2px;">WAN IP <span style="float: right;">▼</span></div> <div style="border-bottom: 1px solid black; padding: 2px;">WAN IP</div> <div style="padding: 2px;">網際網路 IP</div> </div> <p><b>WAN IP</b> - 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。</p> <p><b>網際網路 IP</b> - 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。</p>

4. 按**確定**按鈕啓動此設定，您將會看到所做的設定已被儲存。



## 關閉此功能並清除全部動態 DNS 帳號

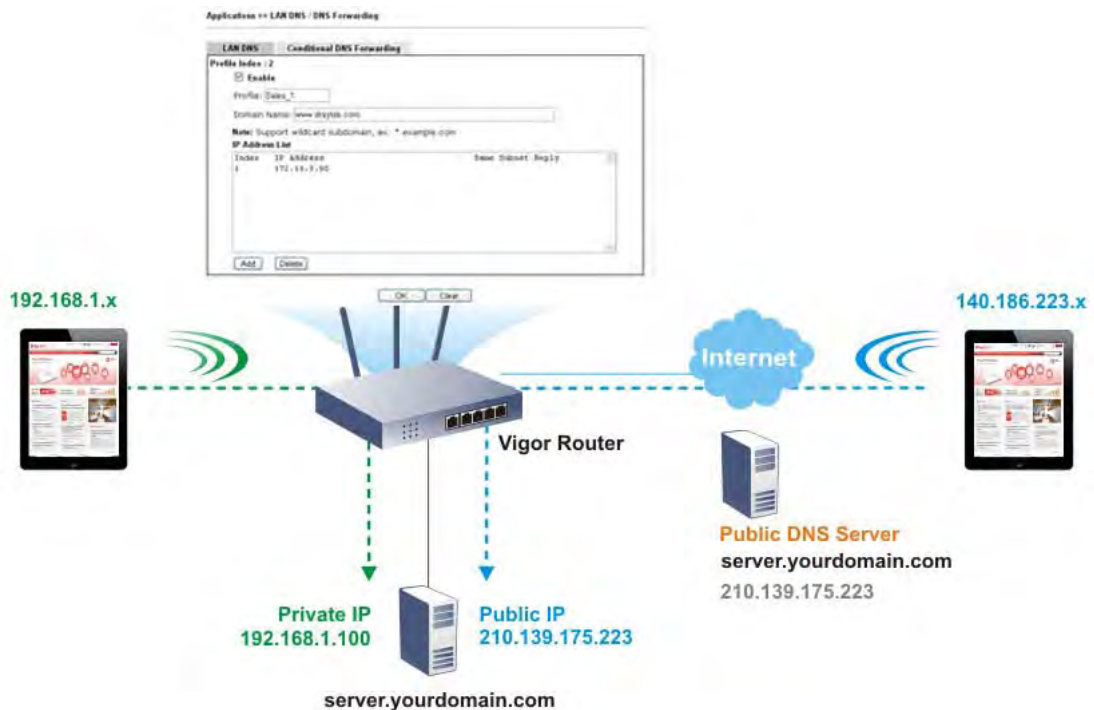
取消勾選**啟用動態 DNS 帳號**，並按下**清除全部**按鈕停用此功能以及清除路由器內所有的帳號。

## 刪除動態 DNS 帳號

在**動態 DNS 設定**頁面上，請按您想要刪除之帳號的索引號碼，然後按**清除全部**按鈕即可刪除該帳號。

### 4.11.2 LAN DNS / DNS 轉送

LAN DNS 是簡單版的 DNS 伺服器，使用者不需要在區域網路端建立額外的 DDNS 伺服器，透過此功能，使用者可以針對某些服務(如 ftp, www, 或是資料庫)設定容易登入的網域名稱。



開啓**其他應用**>>**LAN DNS/DNS 轉送**頁面。

**其他應用** >> **LAN DNS / DNS 轉送**

**LAN DNS 決議 / 條件式 DNS 轉送**

啟用	索引編號	設定檔	網域名稱	轉送	DNS 伺服器
<input type="checkbox"/>	1.			-	
<input type="checkbox"/>	2.			-	
<input type="checkbox"/>	3.			-	
<input type="checkbox"/>	4.			-	
<input type="checkbox"/>	5.			-	
<input type="checkbox"/>	6.			-	
<input type="checkbox"/>	7.			-	
<input type="checkbox"/>	8.			-	
<input type="checkbox"/>	9.			-	
<input type="checkbox"/>	10.			-	

<< 1-10 | 11-20 >>

確定

每個項目說明如下：

項目	說明
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。
啟用	勾選此方框啟用選定的設定檔。
索引編號	按下索引編號下方的號碼連結可進入設定頁面。
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。

您可以設定 20 組 20 LAN DNS 設定檔。

建立 LAN DNS 設定檔，請依下述步驟來進行：

1. 按下任何一個索引編號，本例採用 1。
2. 細部設定頁面呈現如下圖：

其他應用 >> LAN DNS / DNS 轉送

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。
網域名稱	輸入此設定檔的網域名稱。
<b>CNAME (Alias Domain Name)</b>	CNAME 用於記錄網域名稱或是主機別名。 <b>新增</b> – 按此鈕新增新的主機。 <b>刪除</b> – 按此鈕移除設定。

## 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 IP 位址。



- **當傳送者再相同子網時....** – 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。

3. 按下**確定**按鈕儲存設定。
4. 如果您需要設定 LAN DNS 設定，請按下索引編號(例如#1)編輯剛剛完成的 LAN DNS 設定檔，或是，您可以按索引編號(#2)使用該設定檔做為條件式 DNS 轉送設定檔。

其他應用 >> LAN DNS / DNS 轉送

LAN DNS	條件式 DNS 轉送
設定檔索引編號: 1	
<input type="checkbox"/> 啟用	
設定檔: <input type="text"/>	
網域名稱: <input type="text"/>	
附註: 支援萬用字元子網，例如: *.example.com	
DNS 伺服器 IP 位址: <input type="text"/>	
<input type="button" value="確定"/> <input type="button" value="清除"/>	

可用設定說明如下：

項目	說明
啟用	勾選此框啟用此功能。
設定檔	輸入設定檔的檔名。 <b>附註:</b> 如果您在此輸入設定檔名並按下 <b>確定</b> 按鈕儲存，此處設定檔的名稱會自動套用到 LAN DNS 設定頁面(相同的索引編號)。

網域名稱	輸入設定檔需求的網域名稱。
DNS 伺服器 IP 位址	輸入 DNS 伺服器的 IP 位址，以便作為 DNS 轉送功能之 DNS 伺服器。

5. 按下**確定**按鈕儲存設定。
6. 新建立的 LAN DNS 設定檔完成如下。

### 4.11.3 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**以開啓時間設定頁面，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啓動路由器，時鐘的時間也會重新啓動。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。

**其他應用 >> 排程**

排程: | 回復出廠預設值 |

索引編號	狀態	索引編號	狀態
<u>1.</u>	×	<u>9.</u>	×
<u>2.</u>	×	<u>10.</u>	×
<u>3.</u>	×	<u>11.</u>	×
<u>4.</u>	×	<u>12.</u>	×
<u>5.</u>	×	<u>13.</u>	×
<u>6.</u>	×	<u>14.</u>	×
<u>7.</u>	×	<u>15.</u>	×
<u>8.</u>	×		

狀態: v --- 啟用, x --- 不啟用

每個項目說明如下：

項目	說明
回復出廠預設值	清除全部設定資料並回復到出廠的設定。
索引編號	按下方的號碼進入排程設定頁面。
狀態	顯示排程設定是啓動還是關閉。

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：

1. 請按任何一個索引號碼，這裡舉索引編號 1 為例。
2. 其呼叫排程的細部設定顯示如下：

索引編號 1

啟用排程設定

開始日期 (yyyy-mm-dd)    2000 - 1 - 1

開始時間 (hh:mm)        0 : 0

持續時間 (hh:mm)        0 : 0

動作                        強迫啟用

閒置逾時                    最大值255，預設值0

---

頻率

一次

週期

週日    週一    週二    週三    週四    週五    週六

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。
開始日期 (yyyy-mm-dd)	指定排程的開始日期。
開始時間 (hh:mm)	指定排程的開始時間。
持續時間 (hh:mm)	指定排程的持續時間。
動作	指定呼叫排程能採用的方式： <b>強迫啟用</b> - 強迫連線永遠存在。 <b>強迫停用</b> - 強迫連線永遠停止。 <b>啟用隨選撥接</b> - 指定隨選播接連線以及閒置的時間。 <b>停用隨選撥接</b> - 一旦超過閒置時間都沒有任何資料傳輸動作發生，該連線將會停止且在時間排程內都不會再啟用。
閒置逾時	若超過指定時間而沒有任何傳輸動作，系統將中斷連線。
頻率	指定套用的排程頻率。 <b>一次</b> - 此計劃的頻率只會應用一次。 <b>週期</b> - 指定一週當中哪些日子需要執行此項排程作業。

3. 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 都能保持開啓狀態 (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。

#### 4.11.4 RADIUS/TACACS+

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

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

其他應用 >> RADIUS/TACACS+

RADIUS 設定	TACACS+ 設定
<input type="checkbox"/> 啟用	
伺服器 IP 位址	<input type="text"/>
目的通訊埠	<input type="text" value="1812"/>
共享密鑰	<input type="text"/>
確認共享密鑰	<input type="text"/>

可用設定說明如下：

項目	說明
啟用	勾選此項以啟動 RADIUS 設定。
伺服器 IP 位址	輸入 RADIUS 伺服器的 IP 位址。
目的通訊埠	輸入 RADIUS 伺服器所使用的 UDP 通訊埠號，基於 RFC 2138，預設值為 1812。
共享密鑰	RADIUS 伺服器和用戶共用一個用來驗證二者之間傳遞訊息的密鑰，雙方都必須設定相同的共用密鑰。
確認共享密鑰	請重新輸入共用密鑰以確認。

完成上述設定之後，請按下**確定**儲存。

按下 TACACS+ 設定標籤開啓如下頁面：

其他應用 >> RADIUS/TACACS+

RADIUS 設定      TACACS+ 設定

啟用

伺服器 IP 位址

目的通訊埠 49

類型 ASCII

共享密鑰

確認共享密鑰

確定    清除    取消

可用設定說明如下：

項目	說明
啟用	勾選此項以啓動 TACACS+設定。
伺服器 IP 位址	輸入 TACACS+伺服器的 IP 位址。
目的通訊埠	輸入 TACACS+所使用的 UDP 通訊埠號，基於 RFC 2138，預設值為 1812。
共享密鑰	RADIUS 伺服器和用戶共用一個用來驗證二者之間傳遞訊息的密鑰，雙方都必須設定相同的共用密鑰。
確認共享密鑰	請重新輸入共用密鑰以確認。

完成上述設定之後，請按下**確定**儲存。

#### 4.11.5 Active Directory/ LDAP

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

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

##### 基本設定

本頁可讓您啓用功能並設定 LDAP 伺服器一般內容資訊。

Active Directory /LDAP | 回復出廠預設值 |

基本設定
Active Directory / LDAP 設定檔

啟用

綁定類型 簡易模式 ▾

伺服器位址

目標通訊埠

使用 SSL

Regular DN

Regular 密碼

附註: 完成LDAP設定檔內容之後，可在右述頁面中看到 **VPN 及遠端存取 >> PPP 基本設定**。如果您想使用設定檔進行VPN驗證，請勾選PPTP LDAP 設定檔下方陳列的設定檔方框 **VPN 及遠端存取 >> PPP 基本設定**。

可用設定說明如下：

項目	說明
啟用	勾選此框啟用此功能。
綁定類型	<p>有三種綁定類型可以選擇：</p> <div style="border: 1px solid black; padding: 2px; margin-bottom: 5px;"> <p>簡易模式 ▾</p> <p>簡易模式</p> <p>匿名</p> <p>Regular 模式</p> </div> <p><b>簡易模式</b> – 不用進行任何搜尋動作，直接綁定驗證。</p> <p><b>匿名</b> – 先以匿名帳號執行搜尋動作，再進行綁定驗證。</p> <p><b>Regular 模式</b> – 大部分皆與匿名模式相同，不同之處再於伺服器將會先檢查是否具備搜尋權限。</p> <p>對於 <b>Regular 模式</b>，您需要輸入 <b>Regular DN</b> 以及 <b>Regular 密碼</b>。</p>
伺服器位址	輸入 LDAP 伺服器的 IP 位址。
目標通訊埠	輸入 LDAP 伺服器之目的埠號。
使用 SSL	勾選此方框使用 SSL 需求的埠號。
Regular DN	如果選擇 <b>Regular 模式</b> 為綁定類型，請在此輸入 DN 設定。
Regular 密碼	如果選擇 <b>Regular 模式</b> 為綁定類型，請在此輸入密碼設定。

完成上述設定之後，請按下**確定**儲存。



## 設定檔

您可以設定 8 組 AD/LDAP 設定檔，這些設定檔將用於使用者管理中以因應不同管理目的。

[其他應用 >> Active Directory /LDAP](#)

Active Directory /LDAP[| 回復出廠預設值 |](#)

基本設定	Active Directory / LDAP 設定檔																											
	<table border="1" style="width: 100%; border-collapse: collapse;"><thead><tr><th style="width: 15%;">索引編號</th><th style="width: 45%;">名稱</th><th style="width: 40%;">網域名稱(DN)</th></tr></thead><tbody><tr><td>1.</td><td></td><td></td></tr><tr><td>2.</td><td></td><td></td></tr><tr><td>3.</td><td></td><td></td></tr><tr><td>4.</td><td></td><td></td></tr><tr><td>5.</td><td></td><td></td></tr><tr><td>6.</td><td></td><td></td></tr><tr><td>7.</td><td></td><td></td></tr><tr><td>8.</td><td></td><td></td></tr></tbody></table>	索引編號	名稱	網域名稱(DN)	1.			2.			3.			4.			5.			6.			7.			8.		
索引編號	名稱	網域名稱(DN)																										
1.																												
2.																												
3.																												
4.																												
5.																												
6.																												
7.																												
8.																												

**附註:** 完成LDAP設定檔內容之後，可在右述頁面中看到 [VPN 及遠端存取 >> PPP 基本設定](#)。如果您想使用設定檔進行VPN驗證，請勾選PPTP LDAP 設定檔下方陳列的設定檔方框 [VPN 及遠端存取 >> PPP 基本設定](#)。

按下任一索引編號開啓下述頁面：

[其他應用 >> Active Directory /LDAP>>伺服器設定檔](#)

**索引編號 1**


名稱	<input type="text"/>
共同名稱識別(CN ID)	<input type="text"/>
基礎網域名稱(BaseDN)	<input type="text"/>
額外的過濾器	<input type="text"/>

**附註:** 針對BaseDN搜尋需求，輸入額外的過濾器內容。  
例如，  
1) For OpenLDAP: (gidNumber=500)  
2) For AD: (msNPAllowDialin=TRUE)

群組網域名稱(GroupDN)	<input type="text"/>
-----------------	----------------------

可用設定說明如下：

項目	說明
名稱	輸入設定檔的名稱。
共同名稱識別(CN ID)	輸入或是編輯 LDAP 伺服器的名稱識別碼，通用名稱爲 cn。
額外的過濾器	輸入額外過濾需求的條件。

<b>基礎網域名稱(BaseDN) / 群組網域名稱(Group DN)</b>	輸入或是編輯用於查詢 LDAP 伺服器中條目可分辨的名稱。 有時候，您可能會因為名稱太長而忘記 Distinguished Name，那麼您可按下  按鈕列出 AD/LDAP 伺服器全部的 帳號資訊，幫助您完成設定。
--	--

完成上述設定之後，請按下**確定**儲存，新的設定檔即可完成。

#### 4.11.6 UPnP

**UPnP** 協定為網路連線裝置提供一個簡易安裝和設定介面，為 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。

其他應用 >> UPnP

**UPnP**

開啓 UPnP 服務 預設WAN ▾

啓用連線控制服務

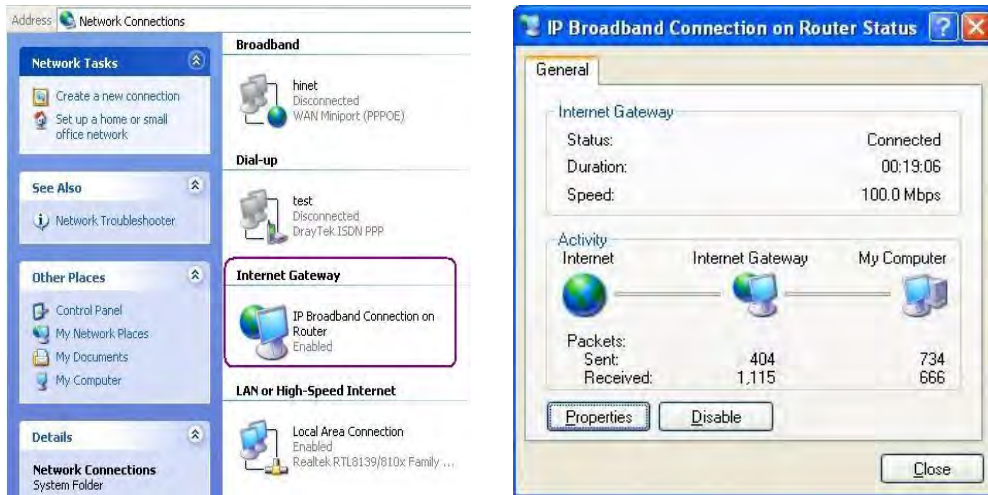
啓用連線狀態服務

**附註：**如果您想在您的區域網路中執行 UPnP 服務，您必須勾選上面相對應的服務及UPnP設定，以便進行控制。

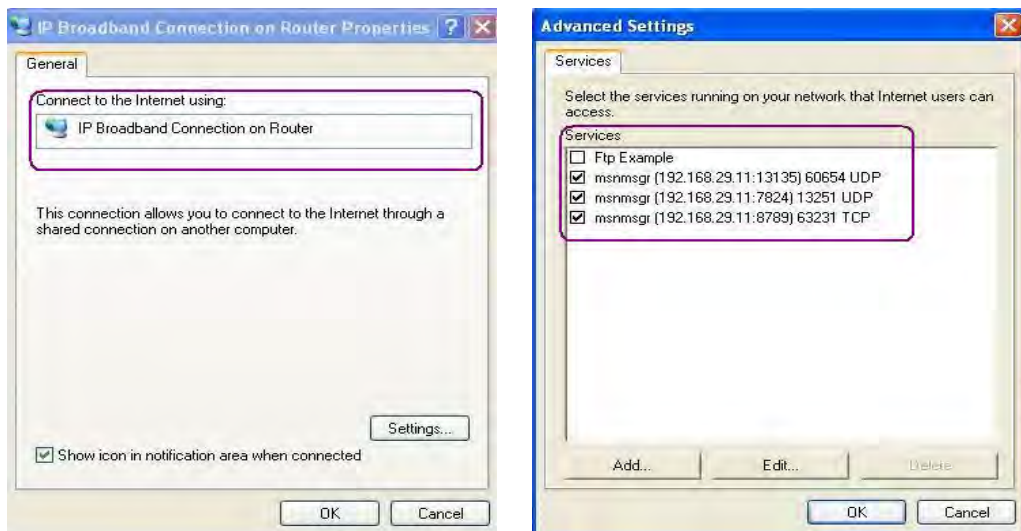
可用設定說明如下：

項目	說明
啓用 UPnP 服務	您可以視情況勾選 <b>啓用連線控制服務</b> 或是 <b>啓用連線狀態服務</b> 。
預設 WAN	用來指定套用此功能的 WAN 介面。

在設定**啓用 UPnP 服務**後，在 Windows XP/網路連線上會出現一個 **IP Broadband Connection on Router** 圖示，連線狀態和控制狀態將可開啓使用，NAT Traversal of UPnP 可啓動應用程式中的多媒體特徵，必須手動設定通訊埠對應或是使用其他類似的方法來設定，以下顯示此項功能的範例圖形。



在路由器上的 UPnP 功能，允許應用程式(像是 MSN Messenger, 可察覺出 UPnP 功能) 找到隱藏在 NAT 路由器之下的是什麼，此應用程式也會記住外部 IP 位址並且在路由器上設定通訊埠對應，結果這種能力可將封包自路由器的外部通訊埠傳送到應用程式所使用的內部通訊埠。



有關防火牆與 UPnP 功能之提示-

### 無法與防火牆軟體配合

在您的電腦上啓用防火牆有可能造成 UPnP 不正常運作，這是因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

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

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

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

#### 4.11.7 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。

其他應用 >> IGMP

##### IGMP

啟用 IGMP 伺服器 WAN1 ▾

如果您想存取多重播送群組，請啟用 IGMP 伺服器，以便在 LAN 端讓 IGMP 以多重播送伺服器來運作。但此功能在橋接模式啟用時是沒有作用的。

啟用 IGMP Snooping

啟用 IGMP Snooping，多重播送流量僅會被轉送至該群組成員中  
停用 IGMP Snooping，多重播送流量將視為一般廣播流量。

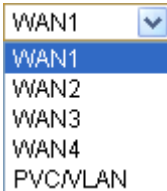
確定

取消

更新頁面

可運作之多重播送群組						
索引編號	群組 ID	P1	P2	P3	P4	P5

可用設定說明如下：

項目	說明
啟用 IGMP 伺服器	勾選此方塊啟用此功能。多重播送的應用透過 WAN 埠來執行，另外，此功能在 NAT 模式下始可作用。 
啟用 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。
更新頁面	按此連結重新整理並顯示多重播送群組的狀態。
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 P5	多重播送群組中所使用的 LAN 連接埠。

完成上述設定之後，請按下**確定**儲存。

### 4.11.8 網路喚醒(WOL)

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

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

其他應用 >> 網路喚醒(WOL)

**網路喚醒(WOL)**

附註：網路喚醒與 **綁定 IP 與 MAC 位址** 功能整合，只有綁定 IP 的電腦能透過 IP 來喚醒。

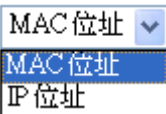
喚醒方式  ▾

IP 位址  ▾

MAC 位址:  :  :  :  :  :

執行結果

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 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。
網路喚醒	按此鈕可以喚醒選定的電腦，喚醒結果將會顯示在方框內。

#### 4.11.9 簡訊(SMS) / 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。

##### 簡訊(SMS)服務供應商

本頁讓您指定簡訊服務供應商、收信人為何以及收信內容。

其他應用 >> 簡訊(SMS) / 郵件警示服務

簡訊(SMS)服務供應商		郵件伺服器		回到出廠預設值	
索引編號	簡訊(SMS)服務供應商	收信人	通知設定檔	排程(1-15)	
1 <input checked="" type="checkbox"/>	1 - Line_down	0955201340	1 - Notify_discont	<input type="text"/>	<input type="text"/>
2 <input type="checkbox"/>	1 - Line_down	<input type="text"/>	1 - Notify_discont	<input type="text"/>	<input type="text"/>
3 <input type="checkbox"/>	1 - Line_down	<input type="text"/>	1 - Notify_discont	<input type="text"/>	<input type="text"/>
4 <input type="checkbox"/>	1 - Line_down	<input type="text"/>	1 - Notify_discont	<input type="text"/>	<input type="text"/>
5 <input type="checkbox"/>	1 - Line_down	<input type="text"/>	1 - Notify_discont	<input type="text"/>	<input type="text"/>
6 <input type="checkbox"/>	1 - Line_down	<input type="text"/>	1 - Notify_discont	<input type="text"/>	<input type="text"/>
7 <input type="checkbox"/>	1 - Line_down	<input type="text"/>	1 - Notify_discont	<input type="text"/>	<input type="text"/>
8 <input type="checkbox"/>	1 - Line_down	<input type="text"/>	1 - Notify_discont	<input type="text"/>	<input type="text"/>
9 <input type="checkbox"/>	1 - Line_down	<input type="text"/>	1 - Notify_discont	<input type="text"/>	<input type="text"/>
10 <input type="checkbox"/>	1 - Line_down	<input type="text"/>	1 - Notify_discont	<input type="text"/>	<input type="text"/>

可用設定說明如下：

項目	說明
索引編號	勾選此方框啓用設定檔。
簡訊(SMS)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 <b>簡訊(SMS)服務供應商</b> 連結來定義 SMS 簡訊伺服器。
收信人	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 <b>通知設定檔</b> 連結來定義簡訊的內容。
排程	輸入簡訊發出的時間排程編號。 您可點 <b>排程(1-15)</b> 連結來定義排程內容。

完成上述設定之後，請按下**確定**儲存。

## 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。

其他應用 >> 簡訊(SMS) / 郵件警示服務

SMS 警示	郵件警示	回復出廠預設值		
索引編號	郵件服務	收信人	通知設定檔	排程(1-15)
1 <input type="checkbox"/>	1 - ???		1 - ???	
2 <input type="checkbox"/>	1 - ???		1 - ???	
3 <input type="checkbox"/>	1 - ???		1 - ???	
4 <input type="checkbox"/>	1 - ???		1 - ???	
5 <input type="checkbox"/>	1 - ???		1 - ???	
6 <input type="checkbox"/>	1 - ???		1 - ???	
7 <input type="checkbox"/>	1 - ???		1 - ???	
8 <input type="checkbox"/>	1 - ???		1 - ???	
9 <input type="checkbox"/>	1 - ???		1 - ???	
10 <input type="checkbox"/>	1 - ???		1 - ???	

附註: 如果使用相同的郵件伺服器，所有的郵件警示設定檔皆分享相同的傳送間隔設定。

確定

取消

可用設定說明如下：

項目	說明
索引編號	勾選此方框啓用設定檔。
郵件服務	使用下拉式清單選擇郵件服務供應商。 您可以點 <b>郵件服務</b> 連結來定義郵件伺服器。
收信人	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 <b>通知設定檔</b> 連結來定義簡訊的內容。
排程	輸入簡訊發出的時間排程編號。 您可點 <b>排程(1-15)</b> 連結來定義排程內容。

完成上述設定之後，請按下**確定**儲存。



## 4.11.10 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。

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

### 其他應用 >> Bonjour

#### Bonjour 設定

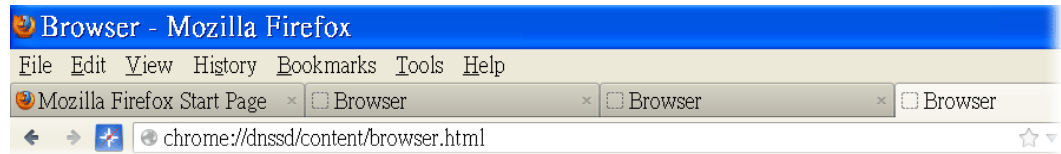
<input checked="" type="checkbox"/>	啓用 Bonjour 服務
<input type="checkbox"/>	HTTP 伺服器
<input type="checkbox"/>	Telnet 伺服器
<input type="checkbox"/>	FTP 伺服器
<input type="checkbox"/>	SSH 伺服器
<input type="checkbox"/>	LPR 印表機伺服器

確定

取消

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，您可以開啓相關網頁並看到如下的結果：



### DNSSD for Firefox

Interface	Name	Type	Domain	Service Info
2	DS1010Plus	_http._tcp.	local.	Select a service on the left to view further details.
2	DS1010Plus(WebDAV)	_http._tcp.	local.	
2	HP LaserJet 1300	_ipp._tcp.	local.	
2	tctseng-virtual-machine	_udisks-ssh._tcp.	local.	
2	tctseng-virtual-machine [00:0c:29:78:bc:24]	_workstation._tcp.	local.	
2	tomkao-desktop [00:0c:29:26:09:5d]	_workstation._tcp.	local.	



3. 開啓系統維護>>管理，輸入路由器名稱(例如 Dray\_2925)，然後按下**確定**儲存。

系統維護 >> 管理

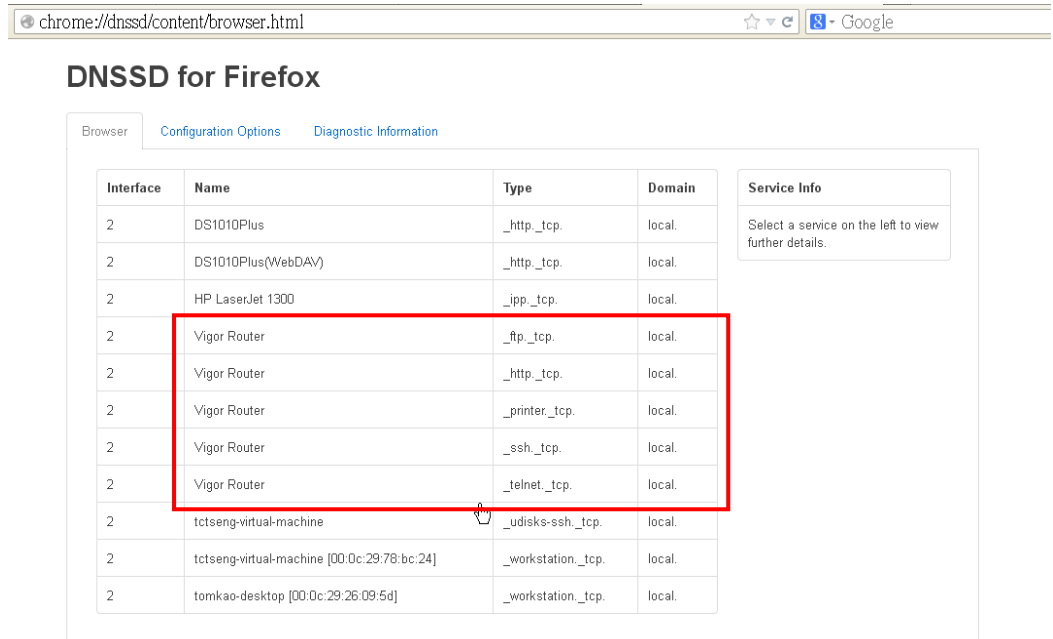
IPv4 管理設定	IPv6 管理設定
路由器名稱 <input type="text" value="Dray_2925"/>	<b>管理通訊埠設定</b> <input checked="" type="radio"/> 使用者定義通訊埠 <input type="radio"/> 預設通訊埠
<b>管理存取控制</b> <input checked="" type="checkbox"/> 允許從網際網路管理 <input type="checkbox"/> FTP 通訊埠 <input checked="" type="checkbox"/> HTTP 通訊埠 <input checked="" type="checkbox"/> HTTPS 通訊埠 <input checked="" type="checkbox"/> Telnet 通訊埠 <input type="checkbox"/> SSH 通訊埠 <input checked="" type="checkbox"/> 停用來自外部網際網路的PING	Telnet 通訊埠 <input type="text" value="23"/> (預設值: 23) HTTP 通訊埠 <input type="text" value="80"/> (預設值: 80) HTTPS 通訊埠 <input type="text" value="443"/> (預設值: 443) FTP 通訊埠 <input type="text" value="21"/> (預設值: 21) SSH 通訊埠 <input type="text" value="22"/> (預設值: 22)
<b>存取清單</b> 清單      IP      子網路遮罩	
1 <input type="text"/> <input type="text"/>	
2 <input type="text"/> <input type="text"/>	
3 <input type="text"/> <input type="text"/>	
<input type="button" value="確定"/>	

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

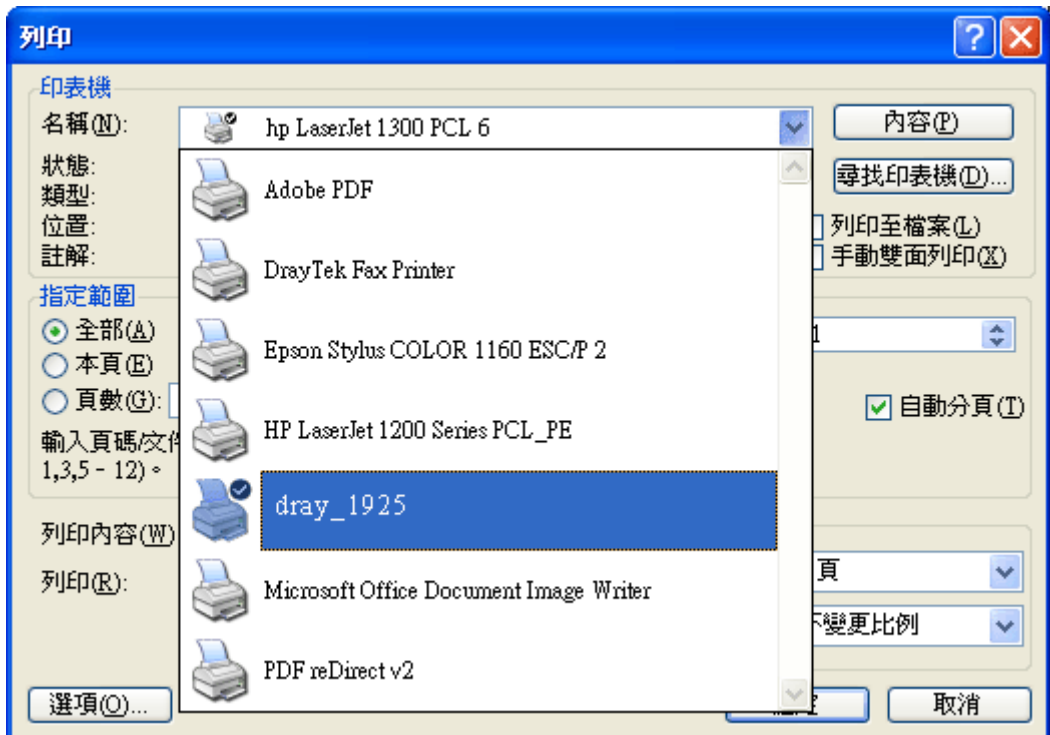
其他應用 >> Bonjour

Bonjour 設定
<input checked="" type="checkbox"/> 啓用 Bonjour 服務 <input checked="" type="checkbox"/> HTTP 伺服器 <input checked="" type="checkbox"/> Telnet 伺服器 <input checked="" type="checkbox"/> FTP伺服器 <input checked="" type="checkbox"/> SSH 伺服器 <input checked="" type="checkbox"/> LPR 印表機伺服器
<input type="button" value="確定"/> <input type="button" value="取消"/>

- 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。



- 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。



## 4.12 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。

下圖為 VPN 與遠端存取的主要功能項目：

- 其他應用
- VPN 與遠端存取
  - 遠端存取控制
  - PPP 基本設定
  - IPsec 基本設定
  - IPsec 端點辨識
  - 遠端登入使用者
  - LAN to LAN
  - VPN TRUNK 管理
  - 連線管理

### 4.12.1 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。

VPN 與遠端存取 >> 遠端存取控制設定

遠端存取控制設定

<input checked="" type="checkbox"/>	啟用 PPTP VPN 服務
<input checked="" type="checkbox"/>	啟用 IPSec VPN 服務
<input checked="" type="checkbox"/>	啟用 L2TP VPN 服務
<input checked="" type="checkbox"/>	啟用 SSL VPN 服務

附註：讓VPN通透至區域網路上個別的VPN伺服器，請停用上述任何一個使用相同協定的服務項目，並確保NAT **開放通訊埠** 或 **通訊埠重導向** 也設定完畢。

可用設定說明如下：

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

完成上述設定之後，請按下**確定**儲存。

## 4.12.2 PPP 基本設定

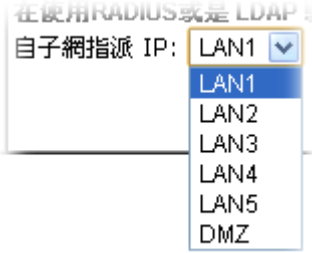
這項功能可以應用在 PPP 相關的 VPN 連線中，諸如 PPTP、L2TP、L2TP over IPsec 等。

VPN 與遠端存取 >> PPP 基本設定

PPP 基本設定																
<p><b>PPP/MP 協定</b></p> <p>撥入 PPP 驗證 <input type="text" value="PAP/CHAP/MS-CHAP/MS-CHAPv2"/></p> <p>撥入 PPP 加密 (MPPE) <input type="text" value="選擇 MPPE"/></p> <p>雙方共同驗證 (PAP) <input type="radio"/> 是 <input checked="" type="radio"/> 否</p> <p>使用者名稱 <input type="text"/></p> <p>密碼 <input type="text"/></p> <p><b>指派 IP 給撥入使用者 (當 DHCP 伺服器關閉時)</b></p> <table border="1"> <tr><td>指派 IP 位址</td><td>LAN 1</td><td>192.168.1.200</td></tr> <tr><td></td><td>LAN 2</td><td>192.168.2.200</td></tr> <tr><td></td><td>LAN 3</td><td>192.168.3.200</td></tr> <tr><td></td><td>LAN 4</td><td>192.168.4.200</td></tr> <tr><td></td><td>LAN 5</td><td>192.168.5.200</td></tr> </table>	指派 IP 位址	LAN 1	192.168.1.200		LAN 2	192.168.2.200		LAN 3	192.168.3.200		LAN 4	192.168.4.200		LAN 5	192.168.5.200	<p><b>PPP 驗證方法</b></p> <p><input checked="" type="checkbox"/> 遠端撥入使用者</p> <p><input checked="" type="checkbox"/> RADIUS</p> <p><input checked="" type="checkbox"/> AD/LDAP</p> <p><b>PPTP LDAP 設定</b></p> <p><b>附註:</b> 如果您想要使用 AD/LDAP 作為 PPP 驗證，請在 '撥入 PPP 驗證' 項目中選擇 '限用 PAP' !!!</p> <p><b>附註:</b> 預設優先權為遠端撥入使用者 &gt; RADIUS &gt; AD/LDAP。</p> <p><b>在使用 RADIUS 或是 LDAP 驗證時:</b></p> <p>子網指派 IP: <input type="text" value="LAN1"/></p>
指派 IP 位址	LAN 1	192.168.1.200														
	LAN 2	192.168.2.200														
	LAN 3	192.168.3.200														
	LAN 4	192.168.4.200														
	LAN 5	192.168.5.200														
<input type="button" value="確定"/>																

可用設定說明如下：

項目	說明
撥入 PPP 驗證	<p><b>PAP</b> - 選擇此項目強迫路由器以 PAP 協定來驗證撥入使用者。</p> <p><b>PAP 或 CHAP</b> - 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。</p>
撥入 PPP 加密 (MPPE)	<p>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。</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>選擇 MPPE <input type="text" value="選擇 MPPE"/></p> <p>選擇 MPPE</p> <p>MPPE (40/128 bit)</p> <p>MPPE (128 bit)</p> </div> <p><b>MPPE (40/128bit)</b> - 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。</p> <p><b>MPPE (128bit)</b> - 此選項指出路由器將會使用 MPPE 最大值 (128 bits) 來加密資料。</p>
雙方共同驗證 (PAP)	<p>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</p>

	定使用者名稱和密碼。
指派 IP 位址	輸入撥入 PPP 連線的 IP 位址，您應該自本地虛擬網路中選擇一個 IP 位址，例如假設本地虛擬網路為 192.168.1.0/255.255.255.0，您可以選擇 192.168.1.200 做為起始 IP 位址，但您必須注意到前二個 IP 位址 192.168.1.200 和 192.168.1.201 乃是保留作為 ISDN 遠端撥入使用者所使用。
PPP 驗證方法	設定完成的 LDAP 設定檔將列於此處，勾選您想要用來進行 PPP 驗證的 LDAP 設定檔即可。
PPTP LDAP 設定檔	連結可由此建立新的設定檔供您使用。
在使用 RADIUS 或 LDAP 驗證時	<p>如果 PPP 連線將透過 RADIUS 伺服器或是 LDAP 設定檔進行驗證，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。</p> 

完成上述設定之後，請按下**確定**儲存。

### 4.12.3 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。

VPN IKE/IPsec 基本設定

遠端撥入使用者及動態 IP 客戶的撥入設定 (LAN to LAN)。

<b>IKE 認證方式</b>	
撥入憑證	無 ▾
<b>預先共用金鑰</b>	
預先共用金鑰	<input type="text"/>
確認預先共用金鑰	<input type="text"/>
<b>IPsec 安全防護方式</b>	
<input checked="" type="checkbox"/> 中級 (AH)	對資料進行認證，但不會進行加密。
高級 (ESP)	<input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES
	對資料進行認證及加密。

可用設定說明如下：

項目	說明
<b>IKE 認證方式</b>	<p>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。</p> <p><b>預先共用金鑰</b> - 只有支援預先共用金鑰，請指定一個金鑰作為 IKE 驗證之用。</p> <p><b>確認預先共用金鑰</b>- 確認您所輸入的共用金鑰。</p>
<b>IPsec 安全防護方式</b>	<p><b>中級 (AH)</b> - 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。</p> <p><b>高級 (ESP)</b> - 表示資料將被加密及驗證，請自下 DES、3DES 或 AES 中選取適合項目。</p>

完成上述設定之後，請按下**確定**儲存。

## 4.12.4 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：

VPN 與遠端存取 >> IPSec 端點辨識

X509 對方 ID 帳號:			回復出廠預設值		
索引編號	名稱	狀態	索引編號	名稱	狀態
<a href="#">1.</a>	???	X	<a href="#">17.</a>	???	X
<a href="#">2.</a>	???	X	<a href="#">18.</a>	???	X
<a href="#">3.</a>	???	X	<a href="#">19.</a>	???	X
<a href="#">4.</a>	???	X	<a href="#">20.</a>	???	X
<a href="#">5.</a>	???	X	<a href="#">21.</a>	???	X
<a href="#">6.</a>	???	X	<a href="#">22.</a>	???	X
<a href="#">7.</a>	???	X	<a href="#">23.</a>	???	X
<a href="#">8.</a>	???	X	<a href="#">24.</a>	???	X
<a href="#">9.</a>	???	X	<a href="#">25.</a>	???	X
<a href="#">10.</a>	???	X	<a href="#">26.</a>	???	X
<a href="#">11.</a>	???	X	<a href="#">27.</a>	???	X
<a href="#">12.</a>	???	X	<a href="#">28.</a>	???	X
<a href="#">13.</a>	???	X	<a href="#">29.</a>	???	X
<a href="#">14.</a>	???	X	<a href="#">30.</a>	???	X
<a href="#">15.</a>	???	X	<a href="#">31.</a>	???	X
<a href="#">16.</a>	???	X	<a href="#">32.</a>	???	X

<< [1-32](#) | [33-64](#) >> >> 下一頁 >>

可用設定說明如下：

項目	說明
回復出廠預設值	按此鈕清除全部設定。
索引編號	請按索引下方的號碼以進入設定頁面。
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???

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。

設定檔索引: 1

設定檔名稱

啓動這個帳號

接收任何對方 ID

接受主體替代名稱

類型

IP

網域名稱

電子郵件

接受主體名稱

國家

省份

居住地區

組織

組織單位

常用名稱

電子郵件

可用設定說明如下：

項目	說明
設定檔名稱	請輸入此設定檔的檔名。
啓動這個帳號	勾選方框啓用帳號設定檔。
接收任何對方 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。

完成上述設定之後，請按下**確定**儲存。



## 4.12.5 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 64 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：

VPN 與遠端存取 >> 遠端撥入使用者

遠端存取用戶帳號: | 回復出廠預設值 |

檢視:  全部  上線  下線

索引編號	用戶	使用中	狀態	索引編號	用戶	使用中	狀態
<a href="#">1.</a>	???	<input type="checkbox"/>	---	<a href="#">17.</a>	???	<input type="checkbox"/>	---
<a href="#">2.</a>	???	<input type="checkbox"/>	---	<a href="#">18.</a>	???	<input type="checkbox"/>	---
<a href="#">3.</a>	???	<input type="checkbox"/>	---	<a href="#">19.</a>	???	<input type="checkbox"/>	---
<a href="#">4.</a>	???	<input type="checkbox"/>	---	<a href="#">20.</a>	???	<input type="checkbox"/>	---
<a href="#">5.</a>	???	<input type="checkbox"/>	---	<a href="#">21.</a>	???	<input type="checkbox"/>	---
<a href="#">6.</a>	???	<input type="checkbox"/>	---	<a href="#">22.</a>	???	<input type="checkbox"/>	---
<a href="#">7.</a>	???	<input type="checkbox"/>	---	<a href="#">23.</a>	???	<input type="checkbox"/>	---
<a href="#">8.</a>	???	<input type="checkbox"/>	---	<a href="#">24.</a>	???	<input type="checkbox"/>	---
<a href="#">9.</a>	???	<input type="checkbox"/>	---	<a href="#">25.</a>	???	<input type="checkbox"/>	---
<a href="#">10.</a>	???	<input type="checkbox"/>	---	<a href="#">26.</a>	???	<input type="checkbox"/>	---
<a href="#">11.</a>	???	<input type="checkbox"/>	---	<a href="#">27.</a>	???	<input type="checkbox"/>	---
<a href="#">12.</a>	???	<input type="checkbox"/>	---	<a href="#">28.</a>	???	<input type="checkbox"/>	---
<a href="#">13.</a>	???	<input type="checkbox"/>	---	<a href="#">29.</a>	???	<input type="checkbox"/>	---
<a href="#">14.</a>	???	<input type="checkbox"/>	---	<a href="#">30.</a>	???	<input type="checkbox"/>	---
<a href="#">15.</a>	???	<input type="checkbox"/>	---	<a href="#">31.</a>	???	<input type="checkbox"/>	---
<a href="#">16.</a>	???	<input type="checkbox"/>	---	<a href="#">32.</a>	???	<input type="checkbox"/>	---

<< [1-32](#) | [33-64](#) >> >> 下一頁 >>

附註：使用者帳號必須加入使用者群組中以便啟動SSL Portal登入。

可用設定說明如下：

項目	說明
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。 下線 – 按此顯示下線使用者帳號。
索引編號	請按索引下方的號碼以進入遠端撥入使用者之設定頁面。
用戶	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???
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。

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。

**VPN 與遠端存取 >> 遠端撥入使用者**

**索引編號 1**

<b>使用者帳號與認證</b> <input type="checkbox"/> 開啓這個帳號 閒置逾時 <input type="text" value="300"/> 秒		使用者名稱 <input type="text" value="???"/> 密碼(最多 19個字元) <input type="text"/> <input type="checkbox"/> 啓動行動動態密碼系統(mOTP) PIN 碼 <input type="text"/> 密鑰 <input type="text"/>	
<b>允許的撥入模式</b> <input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPsec 通道 <input checked="" type="checkbox"/> 具有 IPsec 原則的 L2TP <input type="text" value="無"/> <input type="button" value="v"/> <input checked="" type="checkbox"/> SSL 通道		<b>IKE 認證方式</b> <input checked="" type="checkbox"/> 預先共用金鑰 <input type="text" value="IKE 預先共用金鑰"/> <input type="text"/> <input type="checkbox"/> 數位簽章(X.509) <input type="text" value="無"/> <input type="button" value="v"/>	
<input type="checkbox"/> 指定遠端節點 遠端用戶 IP <input type="text"/> 或對方 ID <input type="text"/> Netbios 命名封包 <input checked="" type="radio"/> 通過 <input type="radio"/> 封鎖 經由 VPN 執行多重播送 <input type="radio"/> 通過 <input checked="" type="radio"/> 封鎖 (針對某些 IGMP,IP-Camera,DHCP Relay等而言)		<b>IPsec 安全性模式</b> <input checked="" type="checkbox"/> 中級(AH) 高級(ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES 本機 ID (視需要填入) <input type="text"/>	
<b>子網路遮罩</b> <input type="text" value="LAN 1"/> <input type="button" value="v"/> <input type="checkbox"/> 指定固定 IP 位址 <input type="text" value="0.0.0.0"/>			

可用設定說明如下：

項目	說明
使用者帳號與驗證	<p><b>開啓這個帳號</b> -勾選此方塊以啓用此功能。</p> <p><b>閒置逾時</b> - 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。</p>
允許撥入類型	<p><b>PPTP</b>-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。</p> <p><b>IPsec 通道</b>-允許遠端撥入使用者透過網際網路觸發 IPsec VPN 連線。</p> <p><b>具有 IPsec 原則的 L2TP</b>-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：</p> <ul style="list-style-type: none"> <li>● <b>無</b> - 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。</li> <li>● <b>建議選填</b> -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</li> </ul>

	<p>連線會成爲一種完全的 L2TP 連線。</p> <ul style="list-style-type: none"> <li>● <b>必須</b> - 此選項可在 L2TP 連線中明確指定所要運用的 IPSec 原則。</li> </ul> <p><b>SSL 通道</b> - 允許遠端撥入用戶透過網際網路進行 SSL VPN 連線。</p> <p><b>指定遠端節點</b>-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<b>基本設定</b>中所設定的驗證方式和安全防護方式。</p> <p><b>Netbios 命名封包</b> -</p> <ul style="list-style-type: none"> <li>● <b>通過</b> - 按此鈕讓資料能在二台主機之間所建立的 VPN 通道上傳輸。</li> <li>● <b>封鎖</b> -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。</li> </ul> <p><b>經由 VPN 執行多重播送</b> -某些程式可透過 VPN 連線進行多重播送封包。</p> <ul style="list-style-type: none"> <li>● <b>通過</b> -點選此鈕讓多重播送封包通過路由器。</li> <li>● <b>封鎖</b> - 此爲預設值。點選此鈕之後,路由器將會封鎖多重播送封包。</li> </ul>
子網路	<p>選擇此 VPN 設定檔所需的子網。</p> <p><b>指定固定 IP 位址</b> - 請輸入固定 IP 位址。</p> <p><b>使用者名稱</b>-當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時,本區是可應用的。</p> <p><b>密碼</b>-當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時,本區是可應用的。</p> <p><b>啓動行動動態密碼系統 (mOTP)</b> - 勾選此框以便利用 mOTP 功能進行驗證。</p> <p><b>PIN 碼</b> - 輸入驗證專用碼(例如 1234)。</p> <p><b>密碼</b> - 使用行動電話中由 mOTP 產生的 32 個數字密碼(例如 e759bb6f0e94c7ab4fe6)。</p>
IKE 認證方式	<p>當您指定遠端節點的 IP 位址時,本區僅適用於 <b>IPsec 通道與具有 IPSec 原則的 L2TP</b> 類型,唯一例外的是當您選擇 <b>IPsec 通道</b>時,不論有無指定 IP 位址,您還可以設定數位簽章(X.509)。</p> <p><b>預先共同金鑰</b>- 勾選此方塊啓用此功能並輸入 1-63 文字做爲預先共同金鑰。</p> <p><b>數位簽章 (X.509)</b>-勾選此方塊啓用此功能並選擇一組事先定義的簽章內容 (在 <b>VPN 和遠端存取&gt;&gt;IPsec 端點辨識</b>中設定)。</p>
IPSec 安全防護方式	<p>對 IPSec 通道和 L2TP 含 IPSec 原則來說,本區爲必要設定。請勾選中級或是高級設定作爲安全防護方式。</p> <p><b>中級 -Authentication Header (AH)</b>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。</p>

---

<p><b>高級 -Encapsulating Security Payload (ESP)</b>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。</p> <p><b>本機 ID(視需要填入)</b>-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。</p>
---

---

完成上述設定之後，請按下**確定**儲存。

## 4.12.6 設定 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，也就是說同時可以支援 2 個 VPN 頻道，下圖顯示設定檔案的清單表格。

VPN 與遠端存取 >> LAN to LAN

LAN-to-LAN 設定檔: | 回復出廠預設值 |

檢視:  全部  線上  下線  Trunk 搜尋

索引編號	名稱	使用中	狀態	索引編號	名稱	使用中	狀態
1.	???	<input type="checkbox"/>	---	17.	???	<input type="checkbox"/>	---
2.	???	<input type="checkbox"/>	---	18.	???	<input type="checkbox"/>	---
3.	???	<input type="checkbox"/>	---	19.	???	<input type="checkbox"/>	---
4.	???	<input type="checkbox"/>	---	20.	???	<input type="checkbox"/>	---
5.	???	<input type="checkbox"/>	---	21.	???	<input type="checkbox"/>	---
6.	???	<input type="checkbox"/>	---	22.	???	<input type="checkbox"/>	---
7.	???	<input type="checkbox"/>	---	23.	???	<input type="checkbox"/>	---
8.	???	<input type="checkbox"/>	---	24.	???	<input type="checkbox"/>	---
9.	???	<input type="checkbox"/>	---	25.	???	<input type="checkbox"/>	---
10.	???	<input type="checkbox"/>	---	26.	???	<input type="checkbox"/>	---
11.	???	<input type="checkbox"/>	---	27.	???	<input type="checkbox"/>	---
12.	???	<input type="checkbox"/>	---	28.	???	<input type="checkbox"/>	---
13.	???	<input type="checkbox"/>	---	29.	???	<input type="checkbox"/>	---
14.	???	<input type="checkbox"/>	---	30.	???	<input type="checkbox"/>	---
15.	???	<input type="checkbox"/>	---	31.	???	<input type="checkbox"/>	---
16.	???	<input type="checkbox"/>	---	32.	???	<input type="checkbox"/>	---

<< 1-32 | 33-64 >> 下一頁 >>

[XXXXXX:此撥出設定檔已加入VPN 負載平衡機制]  
 [XXXXXX:此撥出設定檔已加入VPN 備援機制]  
 [XXXXXX:此撥出設定檔並未加入VPN TRUNK機制]

The following shows profiles joined into VPN Load Balance and VPN Backup mechanism.

VPN 與遠端存取 >> LAN to LAN

LAN-to-LAN 設定檔:

檢視:  全部  線上  下線  Trunk 搜尋

名稱	啓動	成員	狀態
Loadbala1	v	Cathy Jack	Offline Offline

[XXXXXX:此撥出設定檔已經加入VPN 負載平衡機制中]  
 [XXXXXX:此撥出設定檔已經加入 VPN 備援機制中]

可用設定說明如下：

項目	說明
檢視	全部 – 按此顯示全部 LAN to LAN 設定檔。

	<p><b>上線</b> – 按此顯示上線 LAN to LAN 設定檔。</p> <p><b>下線</b> – 按此顯示下線 LAN to LAN 設定檔。</p> <p><b>Trunk</b> – 按此顯示 Trunk 設定檔。</p>
<b>回復出廠預設值</b>	按此鈕清除全部設定。
<b>索引編號</b>	請按索引下方的號碼以進入設定頁面。
<b>名稱</b>	意即 LAN-to-LAN 檔案名稱， <b>???</b> 符號代表該檔案目前是空的。
<b>啓動</b>	表示個別檔案的狀態，符號 <b>V</b> 和 <b>X</b> 分別代表使用中與未使用的檔案。
<b>狀態</b>	<p><b>Online</b> – 表示此 LAN to LAN 設定檔目前運作中。</p> <p><b>Offline</b> – 表示此 LAN to LAN 設定檔目前並未運作，即使已經啓動。</p>

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。

設定檔索引：1

1. 一般設定

設定檔名稱 <input type="text" value="???"/> <input type="checkbox"/> 啟用此設定檔	撥號方向 <input checked="" type="radio"/> 雙向 <input type="radio"/> 撥出 <input type="radio"/> 撥入 <input type="checkbox"/> 永遠連線
VPN 撥出經由介面 <input type="text" value="WAN1 優先"/>	閒置逾時 <input type="text" value="300"/> 秒
Netbios 命名封包 <input checked="" type="radio"/> 通過 <input type="radio"/> 封鎖 經由 VPN 執行多重播送 <input type="radio"/> 通過 <input checked="" type="radio"/> 封鎖 <small>(針對某些 IGMP,IP-Camera,DHCP Relay 等而言)</small>	<input type="checkbox"/> 啟用 PING 以維持連線 指定 IP 位址 <input type="text"/>

2. 撥出設定

<p><b>我撥出的伺服器類型</b></p> <input checked="" type="radio"/> PPTP <input type="radio"/> IPsec 通道 <input type="radio"/> 具有 IPsec 原則的 L2TP <input type="text" value="無"/>	<p>使用者名稱 <input type="text" value="???"/>                  密碼(最多 15 個字元) <input type="text"/>                  PPP 驗證 <input type="text" value="PAP/CHAP"/>                  VJ 壓縮 <input checked="" type="radio"/> 開啓 <input type="radio"/> 關閉</p>
<p>對方 VPN 所需之伺服器 IP 或域名。 (例如 draytek.com 或 123.45.67.89)</p> <input type="text"/>	<p><b>IKE 驗證方式</b></p> <input checked="" type="radio"/> 預先共用金鑰 IKE 預先共用金鑰 <input type="text"/> <input type="radio"/> 數位簽章(X.509) 對方 ID <input type="text" value="無"/> 本機 ID <input checked="" type="radio"/> 替代主體名稱優先 <input type="radio"/> 主體名稱優先 本機憑證 <input type="text" value="無"/>
	<p><b>IPsec 安全方式</b></p> <input checked="" type="radio"/> 中級(AH) <input type="radio"/> 高級(ESP) <input type="text" value="DES 無驗證"/> <input type="button" value="進階"/>
	<p>索引號碼(1-15)於 <b>排程</b> 設定：  <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/></p>

可用設定說明如下：

項目	說明
共同設定	<p><b>設定檔名稱</b> - 針對此 LAN-to-LAN 連線，請指定一個設定檔案名稱。</p> <p><b>啟用此設定檔</b>-按此方塊啟用此設定檔。</p> <p><b>VPN 連線經由介面</b>-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。</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>WAN1 優先</p> <p>WAN1 優先</p> <p>限用 WAN1</p> <p>WAN2 優先</p> <p>僅用 WAN2</p> <p>限用 WAN1 : WAN2 備援</p> <p>限用 WAN2 : WAN1 備援</p> <p>WAN3 優先</p> <p>限用 WAN3</p> </div> <ul style="list-style-type: none"> <li>● <b>WAN1 優先/ WAN2 優先/ WAN3 優先</b>- 連線時，路</li> </ul>

	<p>由器會將 WAN1 視為 VPN 連線的首要選擇，如果 WAN1/WAN2/WAN3 連線失敗，路由器將使用其他 WAN 介面來取代。</p> <p><b>限用 WAN1/限用 WAN2/限用 WAN3</b> - 連線時，路由器會將 WAN1/WAN2/WAN3 視為 VPN 連線的唯一選擇。</p> <p><b>限用 WAN1:備援 WAN2</b> - 當 WAN2 斷線時，此 VPN 通道會經由 WAN1 連線撥打出去，亦即 WAN1 為 WAN2 的備援介面。</p> <p><b>限用 WAN2:備援 WAN1</b> - 當 WAN1 斷線時，此 VPN 通道會經由 WAN2 連線撥打出去，亦即 WAN2 為 WAN1 的備援介面。</p> <p><b>Netbios 命名封包</b></p> <ul style="list-style-type: none"> <li>● <b>通過</b> - 按此鈕讓資料能在二台主機之間所建立的 VPN 通道上傳輸。</li> <li>● <b>封鎖</b> - 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。</li> </ul> <p><b>經由 VPN 執行多重播送</b> - 某些程式可透過 VPN 連線進行多重播送封包。</p> <ul style="list-style-type: none"> <li>● <b>通過</b> - 點選此鈕讓多重播送封包通過路由器。</li> <li>● <b>封鎖</b> - 此為預設值。點選此鈕之後，路由器將會封鎖多重播送封包。</li> </ul> <p><b>撥號方向</b> - 針對此 LAN-to-LAN 連線，請指定允許的撥號方向。</p> <ul style="list-style-type: none"> <li>● <b>雙向</b> - 發話方/接話方</li> <li>● <b>撥出</b> - 發話方</li> <li>● <b>撥入</b> - 接話方</li> </ul> <p><b>永遠連線</b> - 勾選此方塊讓路由器永遠保持 VPN 連線。</p> <p><b>閒置逾時</b> - 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。</p> <p><b>啟用 PING 以維持連線</b> - 此功能可協助路由器決定 IPSec VPN 連線狀態，對不正常的 IPSec VPN 通道中斷尤其有用。詳細內容請參考下面的註解，請勾選此方塊啟動 PING 封包傳輸至指定的 IP 位址。</p> <p><b>指定 IP 位址</b> - 輸入 VPN 通道另一端的主機 IP 位址。</p>
<p><b>撥出設定</b></p>	<p><b>我撥出的伺服器類型</b> -</p> <p><b>PPTP</b>-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。</p> <p><b>IPSec 通道</b>-為伺服器建立一個透過網際網路的 IPSec VPN 連線。</p> <p><b>具有 IPSec 原則的 L2TP</b>-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</p>



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 連線會成爲一種完全的 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。

**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 認證**-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 壓縮可作爲 TCP/IP 協定標頭壓縮之用，通常設定選擇**開啓**以改善頻寬利用的狀況。

**IKE 驗證方式** - 這個功能適用 **IPsec 通道與具有 IPSec 原則的 L2TP**。

- **預先共用金鑰**- 勾選此方塊啓用此功能並按 **IKE 預先共用金鑰** 按鈕輸入金鑰及確認金鑰。
- **數位簽章 (X.509)** - 勾選此方塊啓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(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(替代主體名稱優先或是主體名稱優先)，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。

**IPSec 安全防護方式** -對 IPSec 通道和 L2TP 含 IPSec 原則來說，本區爲必要設定。

- **中級 (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。
- **高級 (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 無驗證** - 使用 DES 加密演算式，但不採用任何驗證計畫。
- **DES 有驗證** - 使用 DES 加密演算式，且採用 MD5 或 SHA-1 驗證計畫。

- **3DES 無驗證** - 使用三重 DES 加密演算式，但不採用任何驗證計畫。
- **3DES 有驗證** - 使用三重 DES 加密演算式，且採用 MD5 或 SHA-1 驗證計畫。
- **AES 無驗證** - 使用 AES 加密演算式，但不採用任何驗證計畫。
- **AES 有驗證** - 使用 AES 加密演算式，且採用 MD5 或 SHA-1 驗證計畫。

**進階**-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，視窗顯示如下：



**IKE 階段 1 模式** – 選擇 **Main 模式**或是 **Aggressive 模式**。比起 **Aggressive 模式**，**Main 模式**顯得更加安全，因為在安全通道中有更多的交換動作於此完成，不過，**Aggressive 模式**是比較快速的模式。路由器的預設值為 **Main 模式**。

- **IKE 階段 1 建議** - 針對 VPN 通道另一方可提供本地有效的驗證計畫及加密演算式，並取得回覆訊息以找出符合的結果。對 **Aggressive 模式**來說有二種有效的組合方式，對 **Main 模式**來說有九種有效的組合方式，建議您選擇能涵蓋多數計畫的組合方式。
- 對 **Aggressive 模式**來說有二種有效的組合方式，對二種模式來說有 3 種有效的組合方式，建議您選擇能涵蓋多數計畫的組合方式。
- **IKE 階段 1 金鑰有效時間**- 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。
- **IKE 階段 2 金鑰有效時間**- 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 900 與 86400 秒之間指定所需的時間值。
- **Perfect Forward Secret (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。

**本機 ID** – 在 **Aggressive 模式**中，當鑑定遠端 VPN 伺服器身分時，本機 ID 代表 IP 位址，ID 長度限制於 47 個字元。

**索引號碼(1-15) 於排程設定** -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。

### 3. 撥入設定

<b>允許的撥入模式</b> <input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPsec 通道 <input checked="" type="checkbox"/> 具有 IPsec 原則的 L2TP <span>無</span> <input type="button" value="v"/>  <input type="checkbox"/> 指定 遠端 VPN 隧道 對方 VPN 伺服器 IP <input type="text"/> 或對方 ID <input type="text"/>	使用者名稱 <input type="text" value="???"/> 密碼(最多 11 個字元) <input type="text"/> VJ 壓縮 <input checked="" type="radio"/> 開啟 <input type="radio"/> 關閉
	<b>IKE 驗證方式</b> <input checked="" type="checkbox"/> 預先共用金鑰 <input type="text" value="IKE 預先共用金鑰"/> <input type="checkbox"/> 數位簽章(X.509) <input type="text" value="無"/> 本機 ID <input checked="" type="radio"/> 替代主體名稱優先 <input type="radio"/> 主體名稱優先
	<b>IPsec 安全方式</b> <input checked="" type="checkbox"/> 中級(AH) 高級(ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES

### 4. GRE over IPsec 設定

<input type="checkbox"/> 啟用 IPsec 撥出功能 GRE over IPsec <input type="checkbox"/> 合理流量	我的 GRE IP <input type="text"/> 對方 GRE IP <input type="text"/>
--	---

### 5. TCP/IP 網路設定

我的 WAN IP <input type="text" value="0.0.0.0"/> 遠端隧道 IP <input type="text" value="0.0.0.0"/> 遠端網路 IP <input type="text" value="0.0.0.0"/> 遠端網路遮罩 <input type="text" value="255.255.255.0"/> 本機網路 IP 位址 <input type="text" value="192.168.1.1"/> 本機網路遮罩 <input type="text" value="255.255.255.0"/> <input type="button" value="更多"/>	RIP 方向 <input type="text" value="停用"/> 從第一個子網路到遠端網路，您必須要作 <input type="text" value="路由"/>  <input type="checkbox"/> 變更預設路由到此 VPN 通道 (只有一個 WAN 時才支援此項功能)
--	---

可用設定說明如下：

項目	說明
撥入設定	<p>允許的撥入類型-以不同類型來決定撥入連線。</p> <ul style="list-style-type: none"> <li>● <b>PPTP</b>-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。</li> <li>● <b>IPSec 通道</b>-允許遠端撥入用戶透過網際網路觸發 IPSec VPN 連線。</li> <li>● <b>具有 IPSec 原則的 L2TP</b>-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：           <ul style="list-style-type: none"> <li>■ <b>無</b> - 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。</li> <li>■ <b>建議選填</b>-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 連線會成爲一種完全的 L2TP 連線。</li> <li>■ <b>必須</b> - 此選項可在 L2TP 連線中明確指定所要</li> </ul> </li> </ul>

	<p>運用的 IPsec 原則。</p> <p><b>指定遠端 VPN 閘道</b> -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。</p> <p>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。</p> <p><b>使用者名稱</b>-當您選擇 PPTP 或是 L2TP 含/不含 IPsec 原則時，本區是可應用的。</p> <p><b>密碼</b>-當您選擇 PPTP 或是 L2TP 含/不含 IPsec 原則時，本區是可應用的。</p> <p><b>VJ 壓縮</b>-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。</p> <p><b>IKE 驗證方式</b> -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)。</p> <ul style="list-style-type: none"> <li>● <b>預先共用金鑰</b>- 勾選此方塊啓用此功能並按 <b>IKE 預先共用金鑰</b> 按鈕輸入金鑰及確認金鑰。</li> <li>● <b>數位簽章 (X.509)</b> -勾選此方塊啓用此功能並自下拉式清單中選擇 <b>VPN 遠端存取控制&gt;&gt;IPsec 端點辨識</b> 中所預先定義的設定檔。</li> </ul> <p><b>本機 ID</b>-指定先檢測下方哪一種類型。</p> <ul style="list-style-type: none"> <li>■ <b>替代主體名稱優先</b> - 先檢測替代主體名稱(於 <b>憑證管理&gt;&gt;本機憑證</b> 中定義)。</li> <li>■ <b>主體名稱優先</b> - 先檢測主體名稱(於 <b>憑證管理&gt;&gt;本機憑證</b> 中定義)。</li> </ul> <p><b>IPsec 安全防護方式</b>-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。</p> <ul style="list-style-type: none"> <li>● <b>中級 (AH)</b> 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。</li> <li>● <b>高級 (ESP-Encapsulating Security Payload)-</b> 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。</li> </ul>
<p><b>GRE over IPsec 設定</b></p>	<p><b>啓用 IPsec 撥出功能 GRE over IPsec</b> - 設定完畢 IPsec 撥出設定之後，勾選此框驗證資料並透過 GRE over IPsec 封包加密技術傳輸資料。雙邊的虛擬 IP 位址必須符合才能溝通。</p> <p><b>合理流量</b> - 此項技術得自 RFC2890，透過 GRE 的特性定義 VPN 通道雙邊的資料傳輸的合理流量，即使駭客可以解開 IPsec 加密內容，也無法要求區域網路站點進行資料傳輸。此功能可確保資料在 VPN 通道中傳輸時，能真正傳達至彼此雙方。這個功能是選填內容，可以設定也可以</p>

	<p>省略，不過如果有一方想要使用，另一方也必須啓用此功能才能運作。</p> <p><b>我的 GRE IP</b> - 輸入路由器本身的虛擬 IP 位址以便讓對方驗證。</p> <p><b>對方 GRE IP</b> - 輸入對方主機的虛擬 IP 位址以便讓路由器驗證。</p>
<p><b>TCP/IP 網路設定</b></p>	<p><b>我的 WAN IP</b>-本區只在您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時有效。預設值為 0.0.0.0，表示 Vigor 路由器在 IPCP 協商階段期間，將從遠端路由器取得您所指定的 IP 位址，請在此輸入 IP 位址。此一地址適用於本機為 VPN client (dial-out) 端時。</p> <p><b>遠端閘道 IP</b>-本區只在您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時有效。預設值為 0.0.0.0，表示 Vigor 路由器在 IPCP 協商階段期間，將發予對方的 IP 位址，請在此輸入發予對方之 IP 位址。此一地址適用於本機為 VPN Server (dial-in) 端時。</p> <p><b>遠端網路 IP/遠端網路遮罩</b> - 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用戶端之身分。</p> <p><b>本機網路 IP 位址/ 本機網路遮罩</b> - 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。</p> <p><b>更多</b>-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。</p>  <p><b>RIP 方向</b>-此選項指定 RIP (路由資訊協定) 封包的方向，您可以啓用也可以停用 RIP 方向，於此，我們提供您四種選擇：TX/RX 二者均有、TX、RX 以及停用。</p> <p><b>從第一個子網路到遠端網路，您必須要作</b> -如果遠端網路</p>

	只允許您以單一 IP 撥號，請選擇 <b>NAT</b> 否則請選擇 <b>路由</b> 。 <b>變更預設路由此 VPN 通道</b> -勾選此方塊變更此 VPN 通道的預設路由。
--	--

2. 完成上述設定之後，請按下**確定**儲存。



## 4.12.7 VPN TRUNK 管理

VPN TRUNK 包含數種功能如 VPN 備援、VPN 負載平衡、GRE over IPSec 以及綁定通道策略等等。

### VPN TRUNK 功能 – VPN 備援機制

VPN TRUNK 管理可以是備援機制，可讓您設定數種 VPN 通道做為備援通道。這項特性可讓網路不至於因為網路環境受到任何理由的封鎖而中斷連線。

- VPN TRUNK-VPN 備援機制可判斷 VPN 伺服器環境的異常現象並修正以便及時完成 VPN 通道的備援任務。
- VPN TRUNK-VPN 備援機制可相容所有 WAN 模式(單一/多重)。
- 撥出連線類型包含 IPSec、PPTP、L2TP、L2TP over IPSec(依照硬體規格而定)。
- 網頁設定易於了解且容易設定
- 與 VPN 伺服器 LAN 單一站點/多重網路完全相容
- 郵件警示支援部份，請參考系統維護>> SysLog/郵件警示。
- Syslog 支援部份，請參考系統維護>>SysLog /郵件警示。
- 特定的 ERD(Environment Recovery Detection 環境回復監測)機制可利用 Telnet 指令來操作。

當初始連線的單一 VPN 通道斷線時，VPN TRUNK-VPN 備援機制設定檔立即啟動，在設定 VPN TRUNK -VPN 備援機制設定檔之前，請至少先完成二組 LAN-to-LAN 設定檔(必須包含完整的撥出設定)，否則您將無任何選項可供成員 1 與會員 2 選擇。

### VPN TRUNK 功能 –VPN 負載平衡機制

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

- 提供三種負載分享演算方式包含循環(Round Robin)、權重循環(Weighted Round Robin)以及速率。
- 綁定通道策略機制允許使用者於傳輸時加密資料，或是指定服務功能並可定義 VPN 通道以便進行有效的頻寬管理。
- 撥出連線類型包含 IPSec、PPTP、L2TP、L2TP over IPSec 以及 GRE over IPSec。
- 網頁設定易於了解且容易設定。
- 利用 VPN TRUNK-VPN 負載平衡機制運作的 TCP 連線數不會因為某條 VPN 通道中斷而丟失，使用者不需要重新設定 TCP/UDP 埠號來重新連線，VPN 負載平衡功能可以讓資料在通道當中維持穩定傳輸。

備援設定檔清單

| 回復出廠預設值 |

附註: [活動中:否] LAN-to-LAN設定檔停用或是目前位於撥入(撥號方向)。

編號.狀態	名稱	成員1(啓用)類型	成員2(啓用)類型

進階

負載平衡設定檔清單

| 回復出廠預設值 |

附註: [活動中:否] LAN-to-LAN設定檔停用或是目前位於撥入(撥號方向)。

編號.狀態	名稱	成員1(啓用)類型	成員2(啓用)類型

進階

基本設定

狀態  啓用  停用

設定檔名稱

成員1

成員2

運作模式  備援  負載平衡

可用設定說明如下：

項目	說明
備援設定檔清單	<p>回復出廠預設值 - 按下此連結清除全部的備援機制設定檔。</p> <p>編號 - 備援機制設定檔的流水編號。</p> <p>狀態 - “v” 表示該設定檔已經啓用；“x”表示該設定檔已被停用。</p> <p>名稱 - 顯示備援機制設定檔的檔名。</p> <p>成員1 -顯示自成員1 下拉式清單中選取出來的撥出設定檔。</p> <p>啓用 - “是” 表示正常，”否” 表示停用或是該 LAN to LAN 設定檔目前的撥號方向為撥入模式。</p> <p>類型 - 顯示設定檔的連線類型諸如 IPSec、PPTP、L2TP、L2TP over IPSec (NICE)、L2TP over IPSec(MUST) 等等。</p> <p>成員2 -顯示自成員2 下拉式清單中選取出來的撥出設定</p>



檔。

**進階** - 此按鈕僅在清單中已建立備援設定檔時始有作用。



此對話盒的詳細資訊，請參考稍後的章節。

### 負載平衡設定檔清單

**回復出廠預設值** - 按下此連結清除全部的負載平衡機制設定檔。

**編號** - 負載平衡機制設定檔的流水編號。

**狀態** - “v” 表示該設定檔已經啟用；“x”表示該設定檔已被停用。

**名稱** - 顯示負載平衡機制設定檔的檔名。

**成員 1** - 顯示自成員 1 下拉式清單中選取出來的撥出設定檔。

**啟用** - “是” 表示正常，”否” 表示停用或是該 LAN to LAN 設定檔目前的撥號方向為撥入模式。

**類型** - 顯示設定檔的連線類型諸如 IPSec、PPTP、L2TP、L2TP over IPSec (NICE)、L2TP over IPSec(MUST) 等等。

**成員 2** - 顯示自成員 2 下拉式清單中選取出來的撥出設定檔。

**進階** - 此按鈕僅在清單中已建立負載平衡設定檔時始有作用。

此對話盒的詳細資訊，請參考稍後的章節。

### 基本設定

**狀態** - 選擇**啟用**啟動上述完成的設定檔，如果您按下**停用**，選定的或是目前使用的 VPN TRUNK 備援/負載平衡機制設定檔就不會產生任何作用。

**設定檔名稱**- 輸入 VPN TRUNK 設定檔名稱，每個設定檔可以群組二個 LAN-to-LAN 連線設定檔，在成員 1 與成員 2 下拉式清單中可以見到已經設定完畢的 LAN-to-LAN 設定檔。

**成員 1/成員 2** - 顯示 LAN-to-LAN 撥出設定檔選項 (於 **VPN 與遠端存取 >> LAN-to-LAN** 中設定)，您可於此二區域選擇放在 VPN TRUNK-VPN 備援/負載平衡機制設定檔中群組下的內容。

- **號碼** - LAN-to-LAN 撥出設定檔的索引編號。
- **名稱** - LAN-to-LAN 撥出設定檔的檔名。

- **連線類型** - LAN-to-LAN 撥出設定檔的連線類型。
- **VPN 伺服器 IP (虛擬網路)** - AN-to-LAN 撥出設定檔的 VPN 伺服器 IP。

**運作模式** - 顯示可用的運作模式（備援或是負載平衡）供您選擇。

**新增** - 新增並儲存新的設定檔至備援設定檔清單或是負載平衡設定檔清單，在新的 VPN TRUNK – VPN 備援機制中的成員就此被鎖定，而在 LAN-to-LAN 中將以紅色字體來顯示；VPN TRUNK – VPN 負載平衡機制中的成員也會被鎖定，且在 LAN-to-LAN 中以藍色字體顯示。

**更新** - 按下此鈕儲存狀態（啟用或停用）、設定檔名稱、成員 1 或是成員 2 的變更。

**刪除** - 按下此鈕刪除選定的 VPN TRUNK 設定檔，群組內相關的成員(LAN-to-LAN 設定檔)都將釋放，在 LAN-to-LAN 設定頁面中改成以黑色字體呈現。

### 啓動 VPN TRUNK – VPN 備援機制設定檔的時機

VPN TRUNK – VPN 備援機制在單一 VPN 通道初始連線因故中斷之後會自動啓動，在 VPN TRUNK – VPN 備援機制設定檔內成員 1/2 的內容與 LAN-to-LAN 頁面中撥出設定檔是相同的；一旦啓動，除非是斷線，VPN TRUNK – VPN 備援機制的備援設定檔會處理所有大小事情。

### 啓動 VPN TRUNK – VPN 負載平衡機制設定檔的時機

在完成一條通道連線之後，另一條通道將會在二秒內自動撥出，因此，您可以在 VPN 負載平衡設定檔中選擇任何一個成員。

### 當 VPN 負載平衡中斷連線時啓動 VPN TRUNK –撥出的時機

由於只有一條通道建立並成功連線，爲了維持二條通道之間負載平衡效果，二秒內系統就會自動撥出。

在負載平衡連線後如要關閉二條通道，請於**基本設定區域的狀態項目選擇停用**。

### 如何設定 VPN TRUNK-VPN 備援/負載平衡機制設定檔？

1. 首先，前往 **VPN 與遠端存取>> LAN-to-LAN**，先設定準備成員 1 與成員 2 可以選擇的 LAN-to-LAN 設定檔（二個或是多個），如果您沒有設定足夠的 LAN-to-LAN 設定檔，您就無法操作 VPN TRUNK – VPN 備援/負載平衡機制。
2. 登入 **VPN 與遠端存取>>VPN TRUNK 管理**。
3. 按下**啓用**按鈕來設定一組 VPN TRUNK – VPN 備援/負載平衡設定檔；輸入設定檔名稱（例如 071023）；自成員 1 清單中選擇一組 LAN-to-LAN 設定檔；自成員 2 清單中也選擇一組 LAN-to-LAN 設定檔，最後按下**新增**。

**General Setup**

Status  Enable  Disable

Profile Name

Member1

Member2

Attribute Mode

No.	<Name>	<Connection-Type>	<VPN ServerIP(Private Network)>
1	To-A Place	IPSec	192.168.2.25(20.20.20.0)
2	To-B Site	IPSec	192.168.2.26(20.20.21.0)

- 先看看 LAN-to-LAN 設定檔，索引編號 1 選擇為成員 1；索引編號 2 選擇為成員 2，因此 LAN-to-LAN 設定檔 1 與 2 都會以紅色表示該檔案已被鎖定。如果您刪除 VPN TRUNK – VPN 備援/負載平衡機制設定檔，選定的 LAN-to-LAN 設定檔就會被釋放出來，並以黑字呈現。

#### VPN 與遠端存取 >> LAN to LAN

##### LAN-to-LAN 設定檔:

檢視:  全部  線上  下線  Trunk

索引編號	名稱	使用中	狀態	索引編號
<u>1.</u>	To-A Place	<input checked="" type="checkbox"/>	offline	<u>17</u>
<u>2.</u>	To-B Site	<input checked="" type="checkbox"/>	offline	<u>18</u>
<u>3.</u>	To-C Place	<input checked="" type="checkbox"/>	offline	<u>19</u>
<u>4.</u>	To-D Site	<input checked="" type="checkbox"/>	offline	<u>20</u>
5.	???	<input type="checkbox"/>	---	21

#### 如何設定 GRE over IPsec 設定檔?

- 先至 LAN to LAN 頁面設定 IPsec 設定檔。
- 如果路由器將被視為 VPN 伺服器(虛擬位址為 192.168.50.200)，請在我的 GRE IP 欄位輸入 192.168.50.200，在對方 GRE IP 欄位輸入用戶端位址 192.168.50.100，參考下圖：

**4. GRE over IPsec 設定**

啟用 IPsec 撥出功能 GRE over IPsec

合理流量

我的 GRE IP  對方 GRE IP

**5. TCP/IP 網路設定**

我的 WAN IP	<input type="text" value="0.0.0.0"/>	RIP 方向	<input type="text" value="停用"/>
遠端開道 IP	<input type="text" value="192.168.1.1"/>	從第一個子網路到遠端網路，您必須要作	
遠端網路 IP	<input type="text" value="192.168.1.0"/>	<input type="text" value="路由"/>	
遠端網路遮罩	<input type="text" value="255.255.255.0"/>	<input type="checkbox"/> 變更預設路由到此 VPN 通道 (只有一個 WAN 時才支援此項功能)	
本機網路 IP 位址	<input type="text" value="192.168.25.1"/>		
本機網路遮罩	<input type="text" value="255.255.255.0"/>		

- 稍後，在對方電腦上(作為 VPN 用戶端)，在我的 GRE IP 欄位中輸入 192.168.50.100，在對方 GRE IP 欄位中則輸入 192.168.50.200。

#### 4. GRE over IPsec 設定

<input checked="" type="checkbox"/> 啟用 IPsec 撥出功能	GRE over IPsec
<input type="checkbox"/> 管理流量	我的 GRE IP 192.168.50.100 對方 GRE IP 192.168.50.200

#### 5. TCP/IP 網路設定

我的 WAN IP	0.0.0.0	RIP 方向	停用
遠端閘道 IP	192.168.25.1	從第一個子網路到遠端網路，您必須要作	路由
遠端網路 IP	192.168.25.0		
遠端網路遮罩	255.255.255.0		
本機網路 IP 位址	192.168.1.1	<input type="checkbox"/> 變更預設路由到此 VPN 通道 (只有一個 WAN 時才支援此項功能)	
本機網路遮罩	255.255.255.0		
	<a href="#">更多</a>		

[確定](#) [清除](#) [取消](#)

## 負載平衡與備援的進階頁面

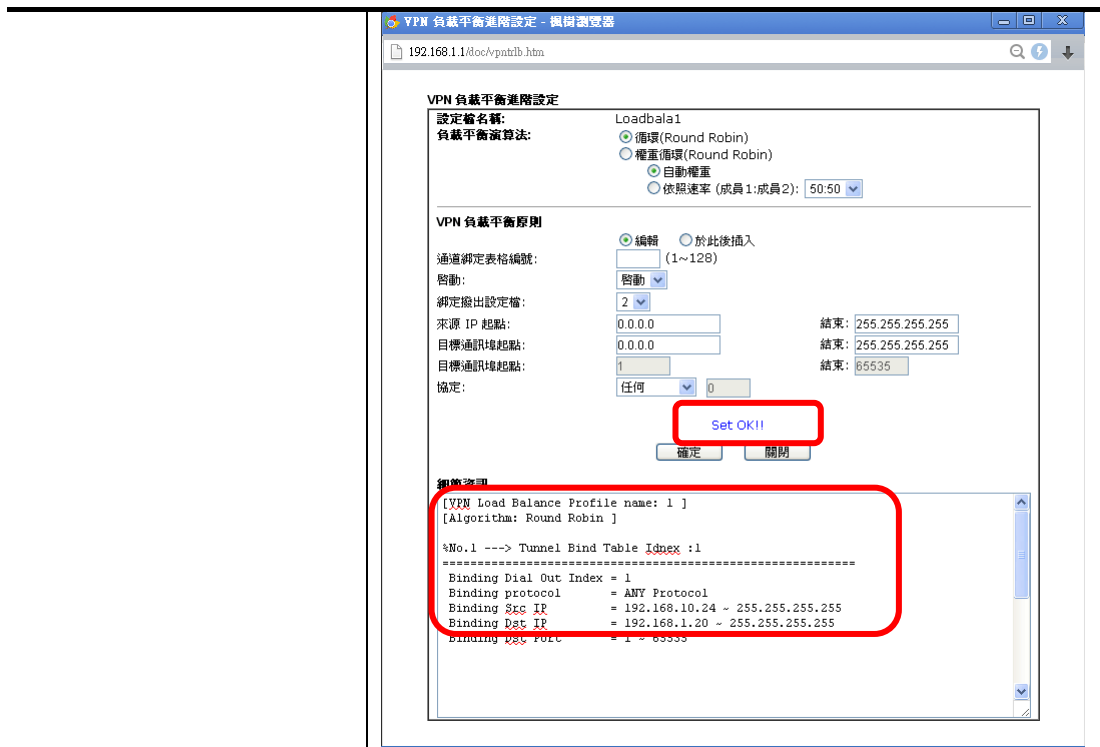
負載平衡設定完畢之後，您可以選擇其中一組設定檔，接著按下**進階**進行更細部的設定。  
負載平衡與備援之**進階**設定視窗有所不同，請參考下述說明。

### 進階負載平衡

可用設定說明如下：

項目	說明
設定檔名稱	顯示設定檔的檔名。
負載平衡演算法	<p><b>循環(Round Robin)</b> – 依照封包的大小而定，二條通道將交替遞送封包，此法可以固定的速率達成平衡傳輸封包。</p> <p><b>權重循環(Weighted Round Robin)</b> – 此法可以利用彈性速率達成平衡傳輸封包，可分為<b>自動權重</b>與<b>依照速率</b>。  <b>自動權重</b>可以固定的比值(3:7)偵測裝置速度(10Mbps/100Mbps)及交換器來進行封包傳輸，如果通道雙邊的速度是相同的，自動權重比值就應該是 5.5。<b>依照</b></p>

	<p><b>速率</b>讓使用者調整適當的速度，成員 1:成員 2 適用的比率有 100 組(範圍從 1:99 到 99:1)。</p>
<p><b>VPN 負載平衡原則</b></p>	<p><b>編輯</b> – 按下此鈕即可設定綁定通道。</p> <p><b>於此後插入</b> – 按下此鈕即可新增一條綁定通道表格。</p> <p><b>通道綁定表格編號</b> - 此裝置提供 128 個綁定通道表格，請予負載平衡設定檔指定通道號碼。</p> <p><b>啓動</b> – 啓動/清除可刪除此綁定通道表格，啓動則是用來啓用此通道表格。</p> <p><b>綁定撥出設定檔</b> – 選擇 LAN to LAN 設定檔索引編號來指定傳輸連線類型。</p> <p><b>來源 IP 起點/結束</b>– 指定來源 IP 起點與終點。</p> <p><b>目標 IP 起點/結束</b>– 指定目標 IP 起點與終點。</p> <p><b>目標通訊埠起點/結束</b>–指定目標通訊服務埠號起點與終點。</p> <p><b>協定</b> – 任何表示當來源 IP、目標 IP、目標通訊埠以及訊框條件符合此處指定的設定時，可依照此處的 TCP Service Port/UDP Service Port/ICMP/IGMP 設定建立綁定通道表格。</p> <p><b>TCP</b> 表示當來源 IP、目標 IP、目標通訊埠以及訊框條件符合此處的設定時，且 TCP 服務埠號也符合此處設定，系統將會建立綁定通道表格。 <b>UDP</b> 表示當來源 IP、目標 IP、目標通訊埠以及訊框條件符合此處的設定時，且 UDP 服務埠號也符合此處設定，系統將會建立綁定通道表格。<b>TCP/UDP</b> 表示當來源 IP、目標 IP、目標通訊埠以及訊框條件符合此處的設定時，且 TCP/UDP 服務埠號也符合此處設定，系統將會建立綁定通道表格。 <b>ICMP</b> 表示當來源 IP、目標 IP、目標通訊埠以及訊框條件符合此處的設定時，且 <b>ICMP</b> 服務埠號也符合此處設定，系統將會建立綁定通道表格。<b>IGMP</b> 表示當來源 IP、目標 IP、目標通訊埠以及訊框條件符合此處的設定時，且 <b>IGMP</b> 服務埠號也符合此處設定，系統將會建立綁定通道表格。 <b>其他</b>表示當來源 IP、目標 IP、目標通訊埠以及訊框條件符合此處的設定，但卻具有不同的 TCP Service Port/UDP Service Port/ICMP/IGMP 埠號，系統將依此建立綁定通道表格。</p>
<p><b>細節資訊</b></p>	<p>本區將顯示綁定通道策略之細節資訊，下圖顯示的是成功的負載平衡綁定通道策略。</p>



**注意:** 欲成功設定綁定通道，您必須輸入綁定來源 IP 範圍(起始與結束)以及綁定目標 IP 範圍(起始與結束)，選擇 TCP/UDP, IGMP/ICMP 或是其他作為綁定協定。

### 進階備援



可用設定說明如下：

項目	說明
設定檔名稱	顯示設定檔的檔名。
ERD 模式	ERD 代表環境回復偵測(Environment Recovers

	<p>Detection)。</p> <p><b>正常</b> – 所有的撥出 VPN TRUNK 備援設定檔會輪流被系統用來重新連線 VPN。</p> <p><b>重新取回</b> – 當 VPN 連線中斷連線時，成員 1 被系統視為最高優先進行 VPN 重新連線。</p>
<b>細節資訊</b>	顯示環境回復偵測的細節內容。



## 4.12.8 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。

### VPN 與遠端存取 >> 連線管理

撥出工具 更新間隔秒數: 10

基本模式:	<input type="text"/>	<input type="button" value="撥號"/>
備份模式:	<input type="text"/>	<input type="button" value="撥號"/>
負載平衡模式:	( Loadbal1 ) draytek.com	<input type="button" value="撥號"/>

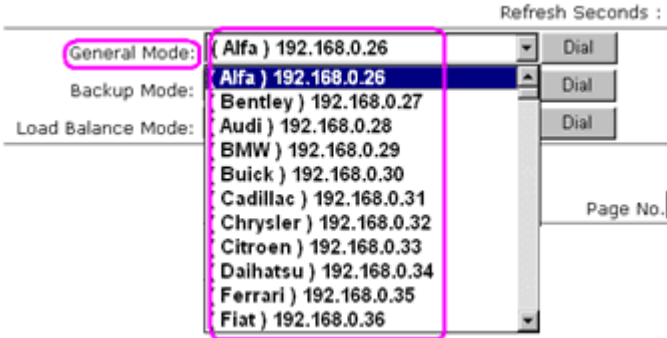
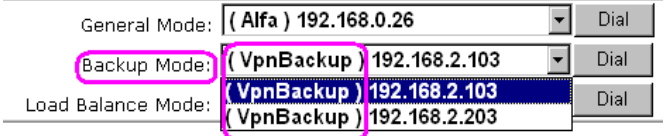
### VPN 連線狀態

目前所在頁面 1

頁面編號   >>

VPN	類型	遠端 IP	虛擬網路	傳送封包數	傳送速率 (Bps)	接收封包數	接收速率 (Bps)	運作時間
				xxxxxxxxx	資料已加密。			
				xxxxxxxxx	資料未加密。			

可用設定說明如下：

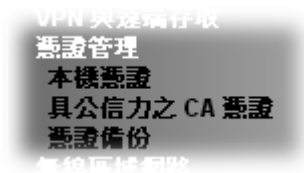
項目	說明
撥號工具	<p><b>基本模式</b> -本區顯示在 LAN-to-LAN 設定的檔案(含索引編號以及 VPN 伺服器 IP 位址)，基本模式所建立的 VPN 連線不支援 VPN 備援功能。</p>  <p><b>備份模式</b> - 本區顯示儲存在 VPN TRUNK 下的設定檔名(含索引編號以及 VPN 伺服器 IP 位址)，備份模式所建立的 VPN 連線支援 VPN 備援功能。</p>  <p><b>撥號</b> - 按此鈕執行撥號功能。</p> <p><b>更新間隔秒數</b>-選擇重新顯示狀態的間隔秒數，有 5、10、30 秒等三種選擇。</p> <p><b>更新頁面</b>-按此鈕以重新顯示整個連線狀態。</p>

## 4.13 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。



### 4.13.1 本機憑證

憑證管理 >> 本機憑證

X509 本機憑證設定

名稱	主體	狀態	修正	
---	---	---	檢視	刪除
---	---	---	檢視	刪除
---	---	---	檢視	刪除

產生 匯入 更新頁面

可用設定說明如下：

項目	說明
產生	按此鈕以開啓產生憑證需求視窗。 輸入全部的資訊，然後再按一次產生按鈕。
匯入	按此鈕以匯入儲存的檔案作為憑證資訊。
更新頁面	按此鈕以更新資訊。

## 檢視

按此鈕以檢視憑證詳細的設定。



**注意:**您必須從上圖視窗中複製憑證需求資訊,接著進入 CA 伺服器並進入憑證需求頁面,將此複製資訊貼上並提交需求,CA 伺服器就會提供您一個新的憑證,請保存起來。

## 刪除

按此鈕刪除選定的憑證及其相關資訊。

## 產生

按下此鈕開啓產生本機憑證需求視窗,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

### 產生憑證需求

憑證名稱	<input type="text"/>
主體替代名稱	
類型	IP 位址 <input type="button" value="v"/>
IP	<input type="text"/>
主體名稱	
國家	<input type="text"/>
省份	<input type="text"/>
居住地區	<input type="text"/>
組織 (O)	<input type="text"/>
組織單位 (OU)	<input type="text"/>
常用名稱	<input type="text"/>
電子郵件	<input type="text"/>
金鑰類型	RSA <input type="button" value="v"/>
金鑰大小	1024 Bit <input type="button" value="v"/>

**注意:** 請注意常用名稱必須設定為路由器的 WAN IP 位址或是網址。

按下產生按鈕之後,憑證產生的資訊就會顯示在畫面上:

X509 本機憑證設定

名稱	主體	狀態	修正
server	/C=TW/ST=Hsinchu/L=Hsinchu/O...	Requesting	<input type="button" value="檢視"/> <input type="button" value="刪除"/>
---	---	---	<input type="button" value="檢視"/> <input type="button" value="刪除"/>
---	---	---	<input type="button" value="檢視"/> <input type="button" value="刪除"/>

匯入

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。

匯入 X509 本機憑證

**上傳本機憑證**

選擇本機憑證檔案  
憑證名稱:  未選擇檔案  
按 [匯入](#) 上傳本機憑證

---

**上傳PKCS12憑證**

選擇 PKCS12檔案  
PKCS12 檔案:  未選擇檔案  
密碼:   
按 [匯入](#) 上傳 PKCS12檔案

---

**上傳憑證以及私人密鑰**

選擇憑證以及搭配的私人密鑰  
憑證名稱:  未選擇檔案  
密鑰檔案:  未選擇檔案  
密碼:   
按 [匯入](#) 上傳本機憑證以及私人密鑰

可用設定說明如下：

項目	說明																
上傳本機憑證	<p>允許使用者輸入路由器產生且 CA 伺服器簽核過的憑證。如果您在憑證產生的步驟中順利完成憑證建立，憑證的狀態欄位下方就會顯示 OK。</p> <p>憑證管理 &gt;&gt; 本機憑證</p> <div style="border: 1px solid black; padding: 5px;"> <p>X509 本機憑證設定</p> <table border="1"> <thead> <tr> <th>名稱</th> <th>主體</th> <th>狀態</th> <th>修正</th> </tr> </thead> <tbody> <tr> <td>server</td> <td>/C=TW/ST=Hsinchu/L=Hsinchu/O...</td> <td>OK</td> <td><input type="button" value="檢視"/> <input type="button" value="刪除"/></td> </tr> <tr> <td>---</td> <td>---</td> <td>---</td> <td><input type="button" value="檢視"/> <input type="button" value="刪除"/></td> </tr> <tr> <td>---</td> <td>---</td> <td>---</td> <td><input type="button" value="檢視"/> <input type="button" value="刪除"/></td> </tr> </tbody> </table> <p><input type="button" value="產生"/> <input type="button" value="匯入"/> <input type="button" value="更新頁面"/></p> </div>	名稱	主體	狀態	修正	server	/C=TW/ST=Hsinchu/L=Hsinchu/O...	OK	<input type="button" value="檢視"/> <input type="button" value="刪除"/>	---	---	---	<input type="button" value="檢視"/> <input type="button" value="刪除"/>	---	---	---	<input type="button" value="檢視"/> <input type="button" value="刪除"/>
名稱	主體	狀態	修正														
server	/C=TW/ST=Hsinchu/L=Hsinchu/O...	OK	<input type="button" value="檢視"/> <input type="button" value="刪除"/>														
---	---	---	<input type="button" value="檢視"/> <input type="button" value="刪除"/>														
---	---	---	<input type="button" value="檢視"/> <input type="button" value="刪除"/>														

<b>上傳 PKCS12 憑證</b>	<p>允許使用者上傳憑證，通常其副檔名為.pfx 或是.p12，且這些憑證需要密碼驗證。</p> <p><b>注意:</b> PKCS12 是安全地儲存私人密鑰以及憑證的標準，它可利用輸入輸出選項於 Netscape 以及 Microsoft Internet Explorer 運用。</p>
<b>上傳憑證及私人密鑰</b>	<p>當使用者有不同的憑證及私人密鑰時，可以使用本區功能來匯入，如果私人密鑰有被加密，那麼還需要輸入密碼以便進行驗證。</p>

### 更新頁面

按下此鈕更新本頁資訊。

### 4.13.2 具公信力之 CA 憑證

具公信力之 CA 憑證列出三組具公信力之 CA 憑證表。

憑證管理 >> 具公信力之 CA 憑證

#### X509 具公信力之 CA 憑證設定

名稱	主體	狀態	編輯
具公信力之 CA-1	---	---	<input type="button" value="檢視"/> <input type="button" value="刪除"/>
具公信力之 CA-2	---	---	<input type="button" value="檢視"/> <input type="button" value="刪除"/>
具公信力之 CA-3	---	---	<input type="button" value="檢視"/> <input type="button" value="刪除"/>

若要輸入事先儲存的具公信力之 CA 憑證，請按**匯入**鈕開啓如下的視窗，並使用**選擇檔案**找到儲存的文字檔案，接著按下**匯入**鈕，您所要匯入的檔案將會列在視窗上，再按一次**匯入**鈕即可使用預先儲存的檔案。

憑證管理 >> 具公信力之 CA 憑證

#### 匯入 X509 具公信力之 CA 憑證

選擇具公信力之 CA 憑證檔案  
 未選擇檔案  
按一下 **匯入** 上傳憑證

如要檢視每個具公信力之 CA 憑證，請按**檢視**按鈕開啓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。

憑證資訊 - 楓樹瀏覽器  
192.168.1.1/doc/XCaCfVi2.htm

**憑證詳細資訊**

憑證名稱:	具公信力之 CA-2
發行者:	<input type="text"/>
主體:	<input type="text"/>
主體替代名稱:	<input type="text"/>
有效期自:	
有效期到:	

### 4.13.3 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。

憑證管理 >> 憑證備份

備份/還原憑證	
<b>備份</b>	
加密密碼	<input type="text"/>
確認密碼:	<input type="text"/>
按 <input type="button" value="備份"/> 下載憑證至本機電腦並存成檔案。	
<b>還原</b>	
選擇備份檔案以還原。	
	<input type="button" value="選擇檔案"/> 未選擇檔案
解密密碼	<input type="text"/>
按 <input type="button" value="還原"/> 上傳檔案。	

### 4.14 VPN 中央管理

Vigor2925 能夠在自身與其他遵循 TR-069 標準的 CPE 之間，透過中央 VPN 連線管理功能建立虛擬私人網路(VPN)。此外，Vigor2925 還可以被視為伺服器(稱為 CVM 伺服器)，管理多重 TR-069 CPE 並定期執行韌體更新、設定備存與設定還原等作業。

#### Central VPN Management



附註：此功能僅能管理透過 WAN 端連接的 CPE。

憑證管理  
VPN 中央管理  
基本設定  
CPE 管理  
VPN 管理  
紀錄與警示  
AD 中央管理

## 4.14.1 基本設定

本頁用來設定用戶向 Vigor 路由器登錄註冊所需的相關內容。按下**基本設定**標籤與**IPsec VPN 設定**標籤設定此機制的基本功能。

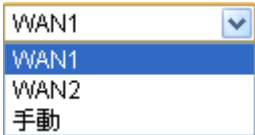
### 4.14.1.1 基本設定

欲啟用 CVM 功能，第一步要做的就是啟用 CVM 埠號與 CVM SSL 埠號設定。

VPN 中央管理 >> 基本設定

基本設定	IPsec VPN 設定
<input type="checkbox"/> CVM SSL 埠號:	<input type="text" value="8443"/>
<input type="checkbox"/> CVM 埠號:	<input type="text" value="8000"/>
遠端連線需求之 WAN IP:	<input type="text" value="WAN1"/> / <input type="text" value="---"/>
<b>複製</b> 下述 URL 以貼至 <b>遠端裝置的 ACS 伺服器 URL</b>	
<code>"http://[hostname or IP address]:8000/ACSServer/services/ACSServlet"</code>	
<code>"https://[hostname or IP address]:8443/ACSServer/services/ACSServlet"</code>	
使用者名稱:	<input type="text" value="acs"/>
密碼:	<input type="password" value="*****"/>
Polling 間隔:	<input type="text" value="600"/> 秒
<b>附註:</b>	
1. 預啟用 CVM 功能， <b>埠號必須啟用</b> ！	
2. 如果您選擇使用 CVM 埠號，介於 CVM 伺服器與 CPE 用戶之間的資料，將明文轉換且可透漏與 ISP 業者知曉。	

可用設定說明如下：

項目	說明
<b>CVM SSL 埠號</b>	勾選此框啟用埠號設定。 於方框內輸入埠號值。
<b>CVM 埠號</b>	勾選此框啟用埠號設定。 於方框內輸入埠號值
<b>遠端連線需求之 WAN IP</b>	Vigor 路由器僅能管理來自 WAN 端的用戶，因此您必須指定準備使用的 WAN 介面，如果您選擇 <b>手動</b> ，您必須指定 WAN IP 位址。 
<b>使用者名稱</b>	輸入任何一台 CPE 嘗試連接至 Vigor 路由器時需要鍵入的使用者名稱。
<b>密碼</b>	輸入任何一台 CPE 嘗試連接至 Vigor 路由器時需要鍵入的密碼。
<b>Polling 間隔</b>	輸入時間值(單位為秒)，可調範圍在 60 ~ 86400 之間。

完成上述設定之後，請按下**確定**儲存。



#### 4.14.1.2 IPsec VPN 設定

VPN 中央管理乃透過 IPsec VPN 連線來操作。

VPN 中央管理 >> 基本設定

基本設定	IPsec VPN 設定
IPsec 模式:	Aggressive模式 ▾
安全性模式:	ESP ▾
加密類型:	AES ▾
本機子網:	手動 ▾
	<input type="text"/> / <input type="text"/>

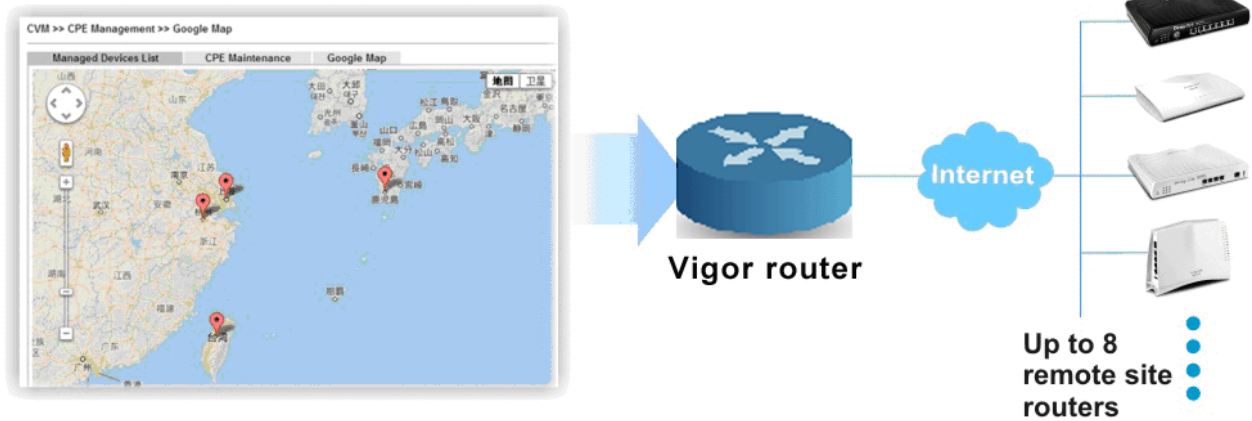
可用設定說明如下：

項目	說明
IPsec 模式	選擇 <b>Aggressive 模式</b> 或是 <b>Main 模式</b> 。
安全性模式	選擇一種方式來維護資料傳送的安全性(AH 或是 ESP)，例如您選擇 AH 即可指定 IPsec 協定，資料將受到驗證但並未加密。
加密類型	自下拉式清單中選擇您需要的加密類型。
本機子網	輸入本機的 IP 位址與子網遮罩。

完成上述設定之後，請按下**確定**儲存。

## 4.14.2 CPE 管理

所有 Vigor2925 管理下的 CPE 都會在本頁中以小圖示的方式呈現出來。  
使用此功能之前，請先確認 CVM 埠號設定已經啟用且已設定妥當。



### 4.14.2.1 受管理的裝置清單

本頁讓您管理連接至 Vigor2925 系列的 CPE 裝置。

- 無 CPE 連接的頁面

CVM >> CPE 管理 >> 受管理的裝置清單

受管理的裝置清單	CPE 維護	Google 地圖	更新頁面	
受管理的裝置清單				
未受管理的裝置清單				
IP 位址	MAC位址	裝置型號	說明名稱	位置
<input type="button" value="新增"/>				

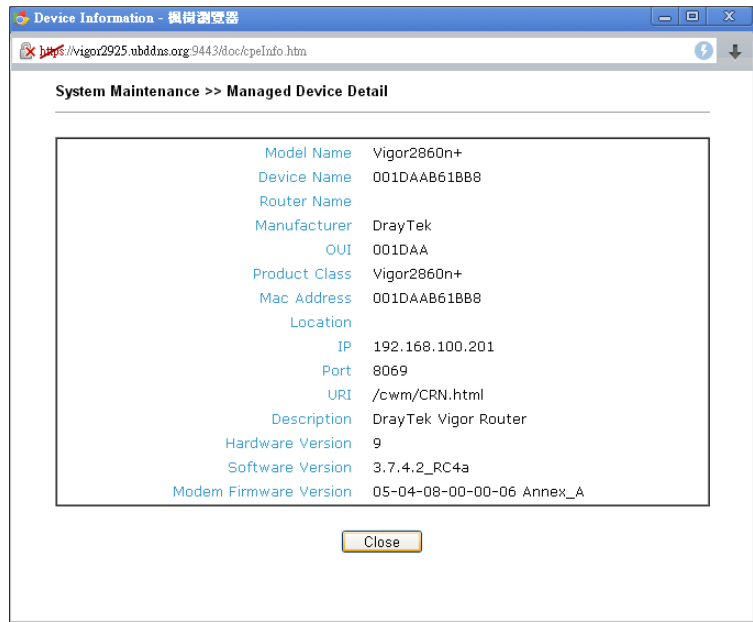
- 已有 CPE 連接的頁面

CVM >> CPE Management >> Managed Devices List

可用設定說明如下：

項目	說明
受管理的裝置清單	<p>本區顯示已在 Vigor2925 管理下的 CPE 裝置圖示(最多可以有 8 個)。</p> <p><b>編輯</b> – 如果要修改 CPE 裝置的名稱或是位置，請選定該圖示然後按下<b>編輯</b>按鈕，螢幕將出現跳出的視窗，即可在此視窗內修改名稱與/或位置。</p> <p><b>刪除</b> – .如果要中斷受管理的 CPE 與 Vigor2925 之間的聯繫，選擇該 CPE 之後，按下<b>刪除</b>按鈕即可。</p> <p><b>附註:</b> 快速按二下 CPE 圖示也可以跳出受管理的 CPE 細節內容，只不過您無法進行任何名稱或位置修改等事</p>

宜。



### 未受管理的裝置清單

任何依循 TR-069 標準的 CPE 裝置都可以在此設定並可由 Vigor2925 系列路由器自動偵測出來。

Vigor2925 一次只會管理最多 8 台遠端裝置，因此其他遠端的裝置如果也被偵測出來，便不會顯示在本區。

**新增** – 將選定的裝置自未受管理的裝置清單區移往受管理的裝置清單區中。

**IP 位址** – 顯示遠端裝置的 IP 位址。

**Mac 位址** – 顯示遠端裝置的 MAC 位址。

**裝置機型** – 顯示遠端裝置的型號資料。

**說明名稱** – 定義 CPE 附加說明的內容以方便辨識。

**位置** – 輸入該 CPE 裝置於 Google Map 顯現出來的位置(位址)。

### 更新頁面

按此連結更新目前頁面。

#### 4.14.2.2 CPE 維護

本區顯示所有套用至受管理裝置之設定檔，本頁可幫助管理者進行維護作業，像是韌體更新、設定備份、設定還原等等。

CVM >> CPE 管理 >> CPE 維護

受管理的裝置清單
CPE 維護
Google 地圖
更新頁面

USB 磁碟: 磁碟使用狀況: USB 儲存中斷

索引編號	設定檔名稱	裝置名稱	動作	檔案/路徑	排程		回復出廠預設值
1.					0	0	現在
2.					0	0	現在
3.					0	0	現在
4.					0	0	現在
5.					0	0	現在
6.					0	0	現在
7.					0	0	現在
8.					0	0	現在

<< 1-8 | 9-16 >>

**附註:** 預啓用排程設定，USB 儲存槽 **必須** 插入路由器中。  
此動作加入工作序列，稍候您可以開啓CVM >> 警告/紀錄頁面檢查運作結果。

可用設定說明如下：

項目	說明
更新頁面	按此更新目前頁面。
USB 磁碟	USB Disk :  - 此即表示 USB 磁碟已經連接上 Vigor2925。 USB Disk :  - 此即表示 USB 磁碟並未連接上 Vigor2925。
磁碟使用狀況	Disk Usage : <span style="color: red;">1084MB / 2009MB</span> - 當 USB 磁碟連接至 Vigor2925 時，磁碟的使用狀況與磁碟的容量都會顯示在螢幕上。 磁碟使用狀況: <span style="color: red;">USB 儲存中斷</span> - 當無任何 USB 磁碟連上 Vigor2925 時，畫面上將出現 USB 磁碟中斷的訊息。
	按此圖示可見 USB 磁碟內容。
回復出廠預設值	按此清除所有頁面上呈現的資料。
索引編號	顯示您可以編輯的設定檔之編號連結。
設定檔名稱	顯示維護設定檔的名稱。
裝置名稱	顯示維護設定檔準備套用的裝置名稱(已接受 Vigor2925 管

	理者)。
動作	顯示該 CPE 準備進行的動作為何。
檔案/路徑	顯示您想要儲存、還原或是更新 CPE 的檔案位置。
排程	顯示此設定檔套用的時間排程為何。
現在	針對選定的 CPE 須執行的動作將會立刻進行。

## 如何新增維護設定檔

請按如下的步驟建立新的設定檔。

1. 按下任一個索引編號連結，例如#1。
2. 系統將出現如下頁面。

VPN 中央管理 >> CPE 管理 >> 維護設定檔

設定檔名稱:

啟用

裝置名稱:

路由器名稱:

路由器型號:

動作類型:

檔案名稱:

索引編號 排程:

**附註:** 忽略動作與間置逾時設定。

可用設定說明如下：

項目	說明
設定檔名稱	輸入維護設定檔的名稱。
啟用	勾選此框啟用此設定檔。
裝置名稱	下拉式清單將會顯示 Vigor2925 偵測到的 CPE 裝置，可從中選取一台裝置來套用此設定檔。
動作類型	<p>有數種類型可供選擇：</p> <ul style="list-style-type: none"> <li>● <b>設定備份(Config Backup)</b> – 表示此設定檔將用於備份選定的 CPE 裝置的設定。</li> <li>● <b>設定還原(Config Restore)</b> – 表示此設定檔將用於還原選定的 CPE 裝置的設定。</li> </ul> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>附註:</b> 當還原某設定至 CPE 時，請務必確認選擇的設定檔早先是從該 CPE 備份下來，因為若將其他機種備份的檔案還原至此 CPE 裝置，將會造成嚴重的後果(像是不同的 CPE 有不同的 ISP 使用者名稱/密碼等等，且還原錯誤的檔案也會造成無法連線登入網際網路)。</p> </div>

	<ul style="list-style-type: none"> <li>● <b>韌體更新(Firmware Upgrade)</b> – 此設定檔將用於韌體更新。</li> </ul>
<b>檔案名稱</b>	輸入您想要儲存還原或是更新 CPE 的檔案名稱。
<b>索引編號排程</b>	路由器依照此處設定的排程計畫執行上述指定的動作。 請在此指定一至二個排程設定檔(以排成索引編號表示)。

3. 輸入所有的設定之後按下**確定**。
4. 新的設定檔建立完成。

#### 4.14.2.3 Google 地圖

如果需要顯示管理下的 CPE 位置鳥瞰圖，請開啓 **VPN 中央管理>>CPE 管理**並按下 **Google 地圖** 標籤。

CVM >> CPE 管理 >> Google 地圖




### 4.14.3 VPN 管理

此功能提供一個簡單又快速的方法來設定 VPN 通道以便在 Vigor2925 系列與其它 Vigor 路由器(被視為 CPE 裝置，VPN 用戶端)之間自動建立 VPN 連線。

- 未連結任何 CPE 裝置之頁面

CVM >> VPN 管理

| [更新頁面](#) |



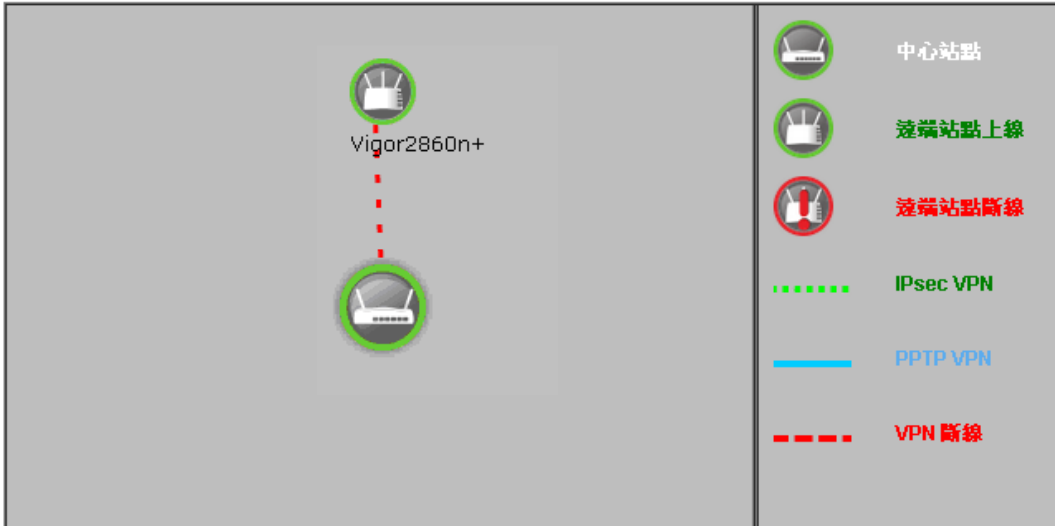
CPE VPN 連線清單

VPN	類型	遠端 IP	虛擬網路	傳送封包	傳送速率 (Bps)	接收封包	接收速率 (Bps)	連線時間

- 已連結 CPE 裝置之頁面

CVM >> VPN 管理

| [更新頁面](#) |

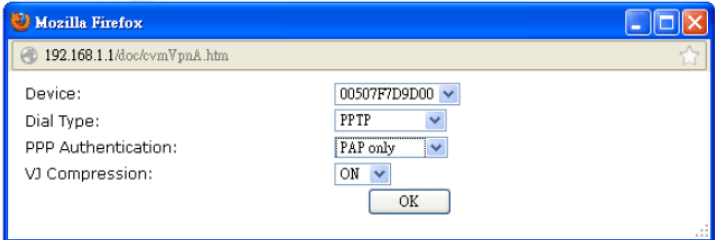


CPE VPN 連線清單

VPN	類型	遠端 IP	虛擬網路	傳送封包	傳送速率 (Bps)	接收封包	接收速率 (Bps)	連線時間



可用設定說明如下：

項目	說明
<b>VPN 管理</b>	
顯示螢幕	一旦某台裝置已可由 Vigor2925 系列管理，相關的圖示就會顯示在此區塊上，若未顯示出來，請參閱第 3.15 如何透過 Vigor2925 管理 CPE (路由器)。
PPTP	欲建立 PPTP 協定之 VPN 連線，請在顯示螢幕下點選欲建立的 CPE 裝置圖示，然後按下此鈕。如果連線成功建立，相關資訊將會顯示在 CPE VPN 連線清單中。
IPsec	欲建立 IPsec 協定之 VPN 連線，請在顯示螢幕下點選欲建立的 CPE 裝置圖示，然後按下此鈕。如果連線成功建立，相關資訊將會顯示在 CPE VPN 連線清單中。
進階	<p>如欲以詳細的設定建立 VPN 連線(像是 PPP 驗證與 VJ 壓縮等等)，請按下<b>進階</b>按鈕。</p>  <p>自裝置的下拉式清單中指定遠端 CPE，再選擇 PPTP 或是 IPsec 做為撥號類型(Dial Type)；接著選擇 PAP only 或是 PAP 或 CHAP 作為 PPP 驗證模式，VJ 壓縮可啟用也可不啟用，之後按下確定按鈕以建立 VPN 連線。</p>
<b>CPE VPN 連線清單</b>	
VPN	顯示 LAN-to-LAN 設定檔的檔名。 當您按下 PPTP/IPsec/進階按鈕以便在 Vigor2925 與遠端 CPE 裝置建立 VPN 連線時，此檔案會自動產生。
類型	顯示撥入類型以及驗證方式。
遠端 IP	顯示遠端 CPE 的 IP 位址與介面。
虛擬網路	顯示 Vigor2925 系列的 IP 位址與子網遮罩。
傳送封包	顯示傳送封包的數量。
傳送速率(Bps)	顯示傳送速率值。
接收封包	顯示接收封包的數量。
接收速率(Bps)	顯示接收速率值。
連線時間	顯示此 VPN 連線的時間。

#### 4.14.4 紀錄與警示

本頁提供簡易資訊用以辨認連接至 Vigor2925 系列的 CPE 為何。

CVM >> 紀錄與警示

記錄		警示		
<a href="#">更新頁面</a>   <a href="#">清除</a>				
顯示模式 <span>永遠紀錄最新事件</span> ▼				
裝置名稱	說明名稱	時間與日期	動作類型	訊息
001DAAB61BB8		2014-08-11 11:02:07	CPE Maintenance	CPE Online
001DAAB61BB8		2000-01-01 00:00:00	CPE Maintenance	Add CPE Successfully

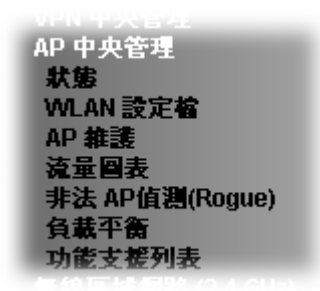
可用設定說明如下：

項目	說明
顯示名稱	選擇一種模式讓系統顯示相關資訊於下表： <ul style="list-style-type: none"><li>● <b>滿碟時停止紀錄</b> – 當紀錄已滿系統將停止紀錄。</li><li>● <b>永遠紀錄最新事件</b> – 系統只紀錄最新事件。</li></ul>
裝置名稱	顯示受管理的 CPE 裝置。
說明名稱	顯示受管理的 CPE 裝置的簡要說明。
時間與日期	顯示路由器掃描偵測出的 CPE 裝置的時間與日期。
動作類型	顯示路由器對 CPE 所進行的動作類型。
訊息	顯示每種事件的簡易資訊。

警示頁面主要提供簡易資訊，以辨識連接至路由器的 CPE 裝置為何。

## 4.15 AP 中央管理

透過 AP 中央管理功能，Vigor2925 能管理支援 AP 管理特性的 VigorAP 基地台。



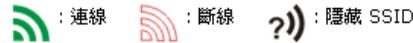
### 4.15.1 狀態

本頁顯示 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)。可進入 **AP 中央管理>>功能支援列表**，檢查支援的 AP 機種有哪些。

AP 中央管理 >> 狀態

索引編號	裝置名稱	IP 位址	SSID	Encryption	頻道	無線用戶端	版本	密碼
------	------	-------	------	------------	----	-------	----	----

附註:



最大支援 20 AP

當 AP 裝置透過媒介之交換器進行連線時，請務必確定 **UDP:4944** 埠號以及 **HTTP** AP 裝置埠號並未被封鎖，因此仍可取回 AP 的操作狀態。

可用設定說明如下：

項目	說明
索引編號	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。
Encryption	顯示 AP 基地台使用的加密模式。
頻道	顯示 AP 基地台使用的頻道。
無線用戶端	顯示連接至 AP 基地台的無線用戶端編號。 其中，0/64 表示最高系統允許 64 台用戶連接至此基地台，但目前尚未有任何無線用戶連接至該基地台。 顯示在左邊的號碼代表 2.4GHz；顯示在右邊的號碼代表 5GHz。
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。

## 4.15.2 WLAN 設定檔

無線網路(WLAN)設定檔可套用至選定的 AP 基地台，無需開啓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。

AP 中央管理 >>無線區域網路設定檔

							回復出廠預設值
<input type="checkbox"/>	設定檔名稱	主要 SSID	安全性	多重 SSID	WLAN ACL	流量控制	
<input type="checkbox"/>	Default	DrayTek-LAN-A	WPA+WPA2/PSK	啟用	無	無	
<input type="checkbox"/>	---	---	---	---	---	---	
<input type="checkbox"/>	---	---	---	---	---	---	
<input type="checkbox"/>	---	---	---	---	---	---	
<input type="checkbox"/>	---	---	---	---	---	---	

複製

編輯

取消

套用至裝置

勾選左邊的核取方塊以指定設定檔，並修改該設定檔的內容。**複製**、**編輯**與**套用至裝置**按鈕於勾選核取方塊後即可使用。

AP 中央管理 >>無線區域網路設定檔

							回復出廠預設值
<input type="checkbox"/>	設定檔名稱	主要 SSID	安全性	多重 SSID	WLAN ACL	流量控制	
<input checked="" type="checkbox"/>	Default	DrayTek-LAN-A	WPA+WPA2/PSK	啟用	無	無	
<input type="checkbox"/>	---	---	---	---	---	---	
<input type="checkbox"/>	---	---	---	---	---	---	
<input type="checkbox"/>	---	---	---	---	---	---	
<input type="checkbox"/>	---	---	---	---	---	---	

複製

編輯

取消

套用至裝置

可用設定說明如下：

項目	說明
設定檔名稱	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。
流量控制	顯示上傳與/或下載的傳輸速率。
複製	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 <b>複製</b> 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**更名如**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。

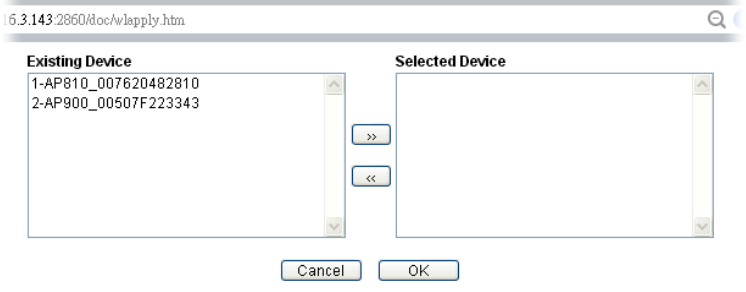
新的設定檔(含有原始設定檔的設定)即可完成建立。

**編輯**

讓您修改現存的無線設定檔或是建立一個新的無線設定檔。

**套用至裝置**

按此鈕可套用選定的無線設定檔至指定的 AP 基地台。



自**現有裝置**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啓動。

## 如何編輯無線區域網路設定檔？

1. 勾選選定之設定檔左邊的方框。
2. 按下編輯按鈕以顯示如下頁面。

AP 中央管理 >> 無線區域網路設定檔

### WLAN 設定檔編輯

裝置設定	
設定檔名稱	Default <input type="checkbox"/> 自動設定
管理者	admin
密碼	*****
第二子網	<input checked="" type="radio"/> 啟用 <input type="radio"/> 停用
操作模式	基地台

2.4G WLAN 基本設定	
無線區域網路	<input type="radio"/> 啟用 <input checked="" type="radio"/> 停用
2.4G 模式	綜合(11b+11g+11n)
2.4G 頻道	2462MHz (頻道 11)
WMM	<input type="radio"/> 啟用 <input checked="" type="radio"/> 停用
傳輸電力	100%

5G WLAN 基本設定	
無線區域網路	<input type="radio"/> 啟用 <input checked="" type="radio"/> 停用
5G 模式	綜合(11a+11n)
5G 頻道	5180MHz (頻道36)

3. 完成基本設定之後，按下一頁開啓如下頁面進行 2.4G 無線安全性設定。

AP 中央管理 >>無線區域網路設定檢視

SSID1	SSID2	SSID3	SSID4
<b>2.4G SSID</b>			
使用中	<input checked="" type="radio"/> 啓用 <input type="radio"/> 停用		
SSID	DrayTek-LAN-A	LAN-A	<input type="checkbox"/> 隱藏 SSID
VLAN	0 (0:不加標籤)		
隔離	<input type="checkbox"/> 從成員		
<b>安全性設定</b>			
加密	WPA+WPA2/PSK		
	安裝 <b>RADIUS</b> 伺服器 若 802.1X 已啓用。		
	<b>WPA</b> WPA 演算方式 <input type="radio"/> TKIP <input type="radio"/> AES <input checked="" type="radio"/> TKIP/AES 網路安全性金鑰 <input type="text" value="*****"/> 金鑰更新間隔 <input type="text" value="3600"/> 秒		
	<b>WEP</b> 設定 <b>WEP</b> 金鑰 若 WEP 已啓用。 802.1X WEP <input type="radio"/> 啓用 <input checked="" type="radio"/> 停用		
<b>連線控制</b>			
模式	無		
清單			
	用戶端 MAC 位址: <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> <input type="button" value="新增"/> <input type="button" value="刪除"/> <input type="button" value="編輯"/> <input type="button" value="取消"/>		
<b>頻寬限制</b>			
狀態	<input type="radio"/> 啓用 <input checked="" type="radio"/> 停用		自動調整 <input type="radio"/> 啓用 <input checked="" type="radio"/> 停用
上傳	<input type="text" value="0"/> Kbps	下載	<input type="text" value="0"/> Kbps
<input type="button" value="上一頁"/> <input type="button" value="取消"/> <input type="button" value="下一頁"/>			
備份ACL設定:	<input type="button" value="備份"/>	自檔案上傳: <input type="button" value="選擇檔案"/> 未選擇檔案	<input type="button" value="還原"/>

4. 完成上述的頁面設定之後，按下一頁開啓如下頁面進行 5G 無線安全性設定。

5G SSID1	5G SSID2	5G SSID3	5G SSID4
<b>5G SSID</b>			
使用中	<input checked="" type="radio"/> 啓用 <input type="radio"/> 停用		
SSID	DrayTek-5G	LAN-A	<input type="checkbox"/> 隱藏SSID
VLAN	0 (0:不加標籤)		
隔離	<input type="checkbox"/> 從成員		
<b>安全性設定</b>			
加密	停用		
	安裝 <b>RADIUS</b> 伺服器 若 802.1X 已啓用		
	<b>WPA</b> WPA 演算方式 <input type="radio"/> TKIP <input type="radio"/> AES <input checked="" type="radio"/> TKIP/AES 網路安全性金鑰 <input type="text" value=""/> 金鑰更新間隔 <input type="text" value="3600"/> 秒		
	<b>WEP</b> 安裝 <b>WEP 金鑰</b> 若 WEP 已啓用 802.1X WEP <input type="radio"/> 啓用 <input checked="" type="radio"/> 停用		
<b>連線控制</b>			
模式	無		
清單			
	用戶端 MAC 位址 : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> <input type="button" value="新增"/> <input type="button" value="刪除"/> <input type="button" value="編輯"/> <input type="button" value="取消"/>		
<b>頻寬限制</b>			
狀態	<input type="radio"/> 啓用 <input checked="" type="radio"/> 停用		自動調整 <input type="radio"/> 啓用 <input checked="" type="radio"/> 停用
上傳	<input type="text" value="0"/> Kbps	下載	<input type="text" value="0"/> Kbps
<input type="button" value="上一頁"/> <input type="button" value="取消"/> <input type="button" value="完成"/>			
備份 ACL設定 : <input type="button" value="備份"/>		自檔案上傳: <input type="button" value="選擇檔案"/> 未選擇檔案 <input type="button" value="還原"/>	

附註：5G SSID 設定僅能與 VigorAP800 v1.1.1 及含有最新 APM 用戶搭配運作。

5. 完成全部的設定之後，按下**完成**可離開此設定頁面並回到第一頁。修改後的無線網路設定檔也會顯示在畫面上。



### 4.15.3 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、韌體更新與遠端重啓等作業，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。

**附註：**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、韌體更新與遠端重啓則可一次針對數台 AP 進行)。

AP 中央管理 >> AP 維護

**AP 維護**

**選擇動作**

動作類型: 設定備份  檔案

檔案/路徑:

**選擇裝置**

現存裝置

選定裝置

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，分別是設定備份、設定配置還原、韌體更新與遠端重啓。
檔案/路徑	指定設定配置還原以及韌體更新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。

#### 4.15.4 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。

**附註：** 啟用/停用此功能將會啟用/停用外接裝置功能。

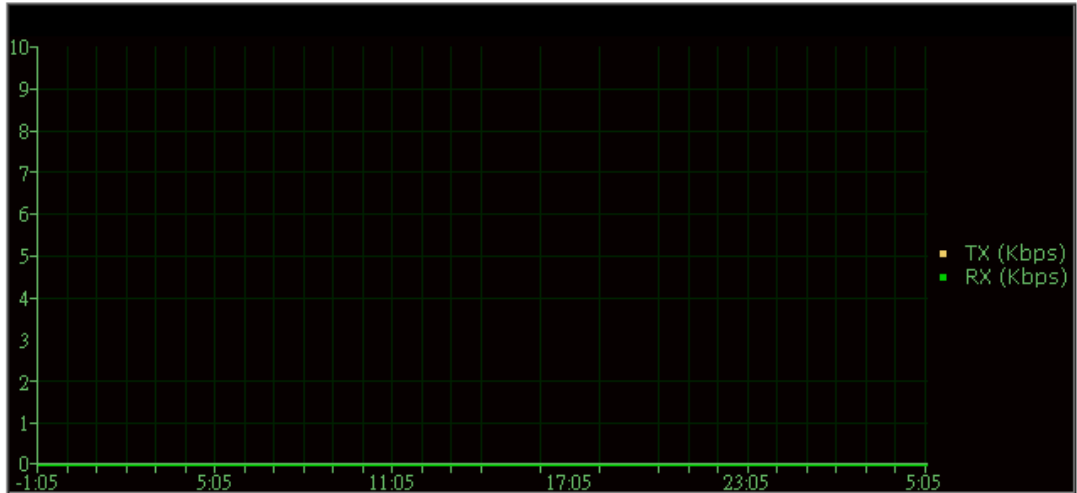
AP 中央管理 >> 流量圖表

啟用

顯示圖表:

更新時間(分):

| [更新頁面](#) |



**附註：** 啟用/停用 AP 流量圖表也會同時啟用/停用外接裝置功能。

水平軸代表時間；垂直軸代表傳輸速率(單位 kbps)。

#### 4.15.5 非法 AP 偵測(Rogue)

本頁顯示路由器偵測到的 AP 基地台，這些基地台皆以不同的顏色區分類型分別是友善 AP、非法 AP 以及未知 AP。

AP 中央管理 >> 非法 AP 偵測(Rogue)

非法 AP 偵測(Rogue)

啟用:  鄰近 AP 偵測  本機無線區域網路偵測

更新時間(分):

| [更新頁面](#) |

頻道	SSID	模式	BSSID	安全性	訊號 (%)	信標(Beacon) 期間	最末刪除
----	------	----	-------	-----	--------	---------------	------

**附註:**

:友善 AP :非法 AP(Rogue) :未知 AP

Vigor2925 不允許套用安全性策略於非法 AP清單上。

下圖顯示按下**確定**按鈕後系統偵測到的 AP 基地台資料。

AP 中央管理 >>非法 AP 偵測(Rogue)

非法 AP 偵測(Rogue)

啟用:  鄰近 AP 偵測  本機無線區域網路偵測

全部 AP 更新時間(分): 1

頻道	SSID	模式	BSSID	安全性	訊號 (%)	信標(Beacon) 期間	最末刪除
11		AP	00:1d:aa:b6:1b:b8	Mixed	37	100	Jan 01,05:07:26
10	BOX102	AP	54:d0:ed:70:07:b0	WPA2PSK	18	100	Jan 01,05:07:26
6	DrayTek	AP	00:1d:aa:d7:eb:f0	Mixed	42	100	Jan 01,05:07:26
1	staffs_4F	AP	00:1d:aa:9c:fb:28	Mixed	13	100	Jan 01,05:07:26
1	staffs	AP	02:1d:aa:75:da:38	Mixed	57	100	Jan 01,05:07:26
1	guests_5F	AP	02:1d:aa:74:da:38	Mixed	57	100	Jan 01,05:07:26
1	staffs_5F	AP	00:1d:aa:74:da:38	Mixed	47	100	Jan 01,05:07:26

附註:  
 :友善 AP :非法 AP(Rogue) :未知 AP

Vigor2925 不允許套用安全性策略於非法 AP清單上。

可用設定說明如下：

項目	說明
啟用	<p><b>鄰近 AP 偵測</b>– 登錄至 Vigor2925 路由器的 AP 基地台被用來偵測其他的基地台，並傳送掃描結果至 Vigor2925 路由器，之後，掃描的結果會顯示在本頁。</p> <p><b>本區無線區域網路偵測</b> – 路由器透過無線區域網路連線偵測所有的 AP 基地台。</p>
全部 AP	AP 被區分為數種類別，請指定其中一種以顯示在畫面上。
更新時間(分)	使用下拉式清單指定更新此頁面的需求時間。
更新頁面	按此連結可立即更新此頁面。
頻道	顯示被偵測到之 AP 基地台使用的頻道。
SSID	顯示被偵測到之 AP 基地台指定的 SSID。
模式	顯示被偵測到之 AP 基地台使用的模式(AP 或是 Ad Hoc)。
BSSID	顯示被偵測到之 AP 基地台的 MAC 位址。
安全性	顯示 AP 基地台使用的加密模式。
訊號 (%)	顯示 AP 基地台發送出來的訊號強度(以百分比表示)。

信標(Beacon)期間	顯示信標的期間，信標訊號將會定期發送出去。
最末偵測	顯示此 AP 基地台被路由器偵測到的最近一次日期與時間。

Vigor 路由器偵測出的所有 AP 基地台都將被視為未知 AP，您必須分別指定哪些為友善 AP 哪些為非法 AP，請依照下列步驟執行分類事宜。

1. 選定其中一個 AP 基地台，按下左邊的按鈕，在本例中，選擇的是 guest\_5F。

AP 中央管理 >> 非法 AP 偵測(Rogue)

非法 AP 偵測(Rogue)

啟用:  鄰近 AP 偵測  本機無線區域網路偵測

全部 AP

頻道	SSID	模式	BSSID	安全性	訊號 (%)	信標(Beacon) 期間	最末 刪除
<input type="radio"/> (?)	11	AP	00:1d:aa:b6:1b:b8	Mixed	37	100	Jan 01,05:07:26
<input type="radio"/> (?)	10	BOX102	54:d0:ed:70:07:b0	WPA2PSK	18	100	Jan 01,05:07:26
<input type="radio"/> (?)	6	DrayTek	00:1d:aa:d7:eb:f0	Mixed	42	100	Jan 01,05:07:26
<input type="radio"/> (?)	1	staffs_4F	00:1d:aa:9c:fb:28	Mixed	13	100	Jan 01,05:07:26
<input type="radio"/> (?)	1	staffs	02:1d:aa:75:da:38	Mixed	57	100	Jan 01,05:07:26
<input checked="" type="radio"/> (?)	1	guests_5F	02:1d:aa:74:da:38	Mixed	57	100	Jan 01,05:07:26
<input type="radio"/> (?)	1	staffs_5F	00:1d:aa:74:da:38	Mixed	47	100	Jan 01,05:07:26

2. 稍後，頁面底部出現細部選項。

<input checked="" type="radio"/> (?)	1	guests_5F	AP	02:1d:aa:74:da:38	Mixed	57	100	Jan 01,05:07:26
<input type="radio"/> (?)	1	staffs_5F	AP	00:1d:aa:74:da:38	Mixed	47	100	Jan 01,05:07:26

AP的 MAC位址:  AP的 SSID

加入友善 AP:  非法 AP(Rogue):

自非法 AP(Rogue)刪除:  友善 AP:

附註:

可用設定說明如下：

項目	說明
AP 的 MAC 位址	選定 AP 基地台的 MAC 位址將會自動顯示出來。
AP 的 SSID	選定 AP 基地台的 SSID 將會自動顯示出來。
新增	加入友善 AP – 若選定 AP 基地台將被視為友善 AP，請按下新增鈕，系統即會將其分至友善 AP 類別。 非法 AP (Rogue) - 若選定 AP 基地台將被視為非法 AP，請按下新增鈕，系統即會將其分至非法 AP 類別。
自非法 AP 刪除/ 自友善 AP 刪除	非法 AP - 如果您想要變更非法 AP 的類別，請選擇該非法 AP 並按下刪除，之後頁面將會更新，該 AP 自動還原為未知 AP。 友善 AP - 如果您想要變更友善 AP 的類別，請選擇該友善 AP 並按下刪除，之後頁面將會更新，該 AP 自動還原為未知 AP。

3. 按下**確定**儲存設定。

下圖以不同顏色呈現不同類別的 AP 基地台之相關資訊。

### 非法 AP 偵測(Rogue)

啓用:  鄰近 AP 偵測  本機無線區域網路偵測



全部 AP

更新時間(分): 1

[更新頁面](#)

頻道	SSID	模式	BSSID	安全性	訊號 (%)	信標(Beacon) 期間	最末刪除
 36	PQC PBX Test Plan 5G	AP	00:1d:aa:d7:ec:72	N/A	5	100	Jan 01,05:09:09
 153	staffs_5G	AP	02:1d:aa:74:da:3a	N/A	94	100	Jan 01,05:09:09
 153	staffs_5F5G	AP	00:1d:aa:74:da:3a	N/A	93	100	Jan 01,05:09:09
 11		AP	00:1d:aa:b6:1b:b8	Mixed	37	100	Jan 00,00:00:00
 10	BOX102	AP	54:d0:ed:70:07:b0	WPA2PSK	18	100	Jan 01,05:12:05
 6	DrayTek	AP	00:1d:aa:d7:eb:f0	Mixed	42	100	Jan 01,05:12:05
 1	staffs_4F	AP	00:1d:aa:9c:fb:28	Mixed	13	100	Jan 01,05:07:26
 1	staffs	AP	02:1d:aa:75:da:38	Mixed	57	100	Jan 01,05:12:05
 1	guests_5F	AP	02:1d:aa:74:da:38	Mixed	57	100	Jan 01,05:12:05
 1	staffs_5F	AP	00:1d:aa:74:da:38	Mixed	47	100	Jan 01,05:12:05

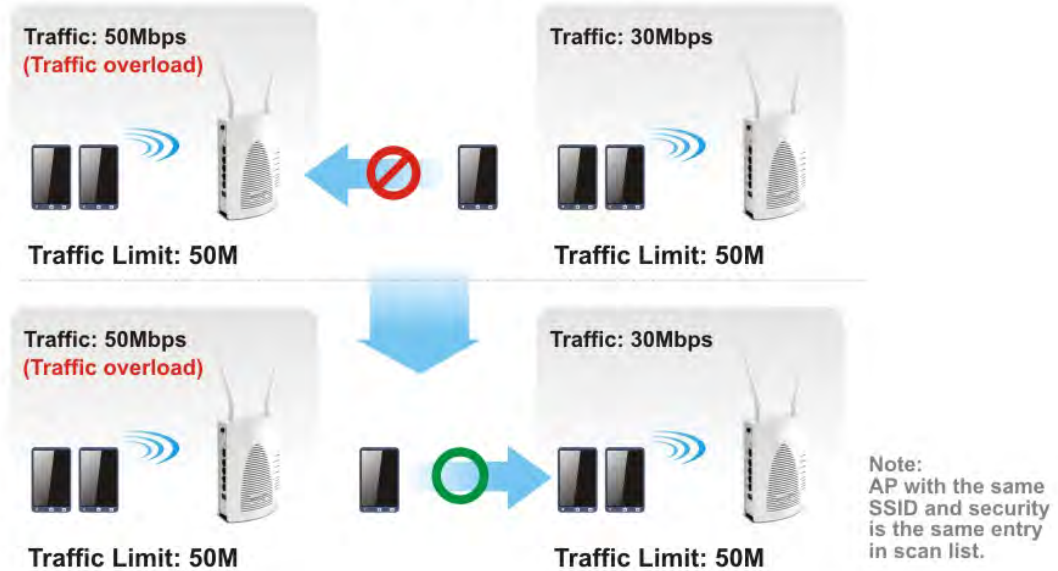
附註:

 :友善 AP  :非法 AP(Rogue)  :未知 AP

## 4.15.6 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。

### AP Load Balance (Traffic overload)



AP 中央管理 >> 負載平衡

啟用:

模式:  透過無線用戶數  
(由此偵測過載) 最多無線用戶數:

無線網路 (2.4GHz)  (3-64)

無線網路 (5GHz)  (3-64)

透過流量

上傳限制   bps (預設單位: K)

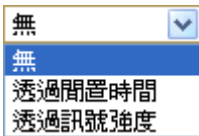
下載限制   bps (預設單位: K)

強迫過載分離:

附 如果VigorAP900的韌體版本為1.1.4.1或是更早之前的版本，無線網路(2.4GHz)中的最多無線用戶數設定將同時適用無線網路註: (2.4GHz)與無線網路(5GHz)。

可用設定說明如下：

項目	說明
啟用	勾選此方況啓用此功能。
模式	此選項用來決定系統用來偵測過載已啓用負載平衡的模式。 <b>透過無線用戶數</b> – 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。

	<p><b>透過流量</b> – 依照本頁的流量設定執行負載平衡的運作。</p> <ul style="list-style-type: none"> <li>● <b>上傳限制</b> – 使用下拉式清單指定上傳的網路流量限制。</li> <li>● <b>下載限制</b> – 使用下拉式清單指定下載的網路流量限制。</li> </ul>
<b>強迫過載分離</b>	<p><b>透過閒置時間</b> - 當 AP 基地台過載的時候(例如達到無線用戶數限制或是網路流量限制)，系統將會中止閒置時間過長的網路用戶連線。</p> <p><b>透過訊號強度</b> - 當 AP 基地台過載的時候(例如達到無線用戶數限制或是網路流量限制)，系統將會中止訊號過弱的網路用戶連線。</p> 

完成上述設定之後，按下**確定**儲存。

#### 4.15.7 功能支援列表

按下**用戶端**標籤列出 AP 基地台各個不同的韌體下，支援的管理功能有哪些。

按下**伺服器**標籤列出 Vigor 路由器在不同的韌體下，支援的 AP 管理功能有哪些。

AP 中央管理 >> 功能支援列表

功能名稱	用戶端		伺服器					
			型號名稱					
			AP800			AP900		AP810
		1.0.5	1.1.0	1.1.1	1.1.0	1.1.1	1.1.0	1.1.1
<b>註冊</b>								
DHCP		√	√	√	√	√	√	√
固定 IP				√		√	√	√
<b>設定檔</b>								
2.4GHz		√	√	√	√	√	√	√
5GHz				√	√	√	√	√
AP 模式		√	√	√	√	√	√	√
Repeater 模式				√	√	√	√	√
用戶端停用自動設定				√		√	√	√
WLAN 啟用/停用						√	√	√
<b>無線用戶端列表</b>								
無線用戶端列表				√	√	√	√	√
<b>負載平衡</b>								
負載平衡						√		√
<b>流量圖表</b>								
流量圖表				√	√	√	√	√
<b>非法 AP 偵測(Rogue)</b>								



## 4.16 無線區域網路設定

本節所提供的資訊僅針對 *n* 系列機型。

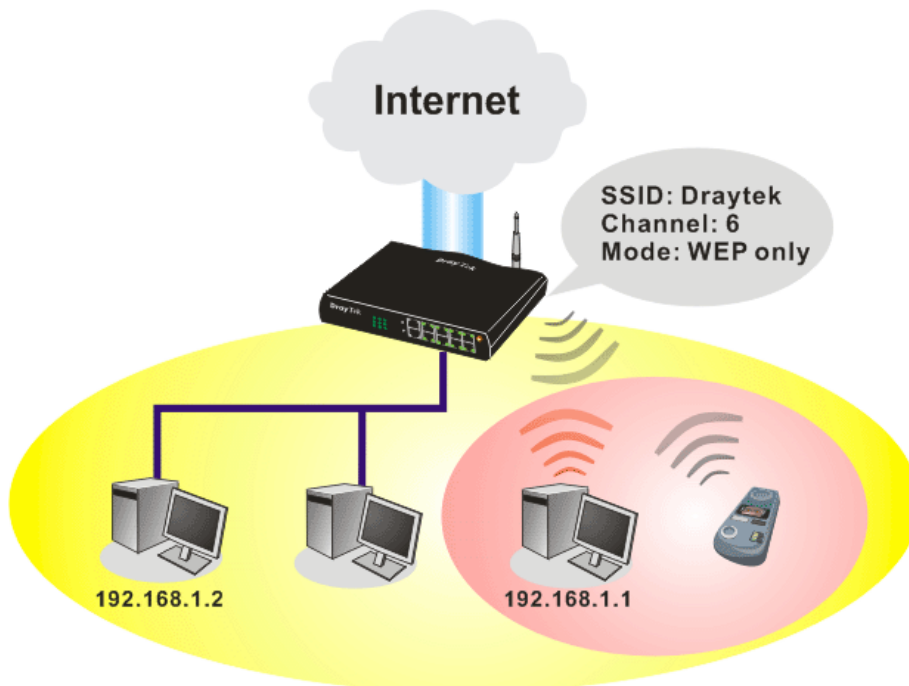
### 4.16.1 基本觀念

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，被設計成爲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。

**注意：**\*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。

### 安全防護概要



**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:** 爲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 或稱爲 WPA Pre-Share Key (WPA/PSK)以及 WPA-Enterprise 又稱爲 WPA/802.1X。

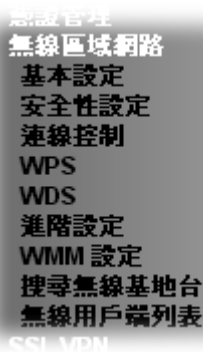
在 WPA-Personal 機制中，會應用一個事先定義的金鑰來加密傳輸中的資料，WPA 採用 Temporal Key Integrity Protocol (TKIP) 加密資料而 WPA2 則是採用 AES，WPA-Enterprise 不只結合加密也還涵括驗證功能。

由於 WEP 已被證明是有弱點的，您可以考慮使用 WPA 作爲安全連線之用。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。

**分隔無線與有線區域網路 - 無線區域網路隔離**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，您可以爲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爲。

**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。

以下爲**無線區域網路**下的功能項目：



- 無線區域網路
- 基本設定
- 安全性設定
- 連線控制
- WPS
- WDS
- 進階設定
- WMM 設定
- 搜尋無線基地台
- 無線用戶端列表
- SSL VPN

## 4.16.2 基本設定

按下**基本設定**連結，新的網頁即會開啓，您可以設定 SSID 和無線頻道資訊，請參考下圖：

無線區域網路 >> 基本設定

**基本設定 (IEEE 802.11)**

啟用無線 LAN

模式 綜合(11b+11g+11n) ▼

---

索引(1-15) 於 **排程** 設定:  ,  ,  ,

只有設定"強迫停用"之排程設定檔會應用至無線網路，其他動作皆省略。

---

啟動	隱藏 SSID	SSID	隔離成員	隔離 VPN
<input checked="" type="checkbox"/>	<input type="checkbox"/>	DrayTek	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	DrayTek_Guest	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>

**隔離成員:**相同 SSID 之無線用戶(stations)彼此無法存取對方。  
**隔離 VPN:**隔離遠端登入與 LAN to LAN 之間的虛擬連線。

---

頻道: 頻道 6, 2437MHz ▼ 長封包標頭

長封包標頭: 某些舊式 802.11 b 裝置需要此項設定(效能較低)

---

Packet-OVERDRIVE™

Tx Burst

**附註:**  
用戶端必需支援相同技術才能提升無線網路的效能。

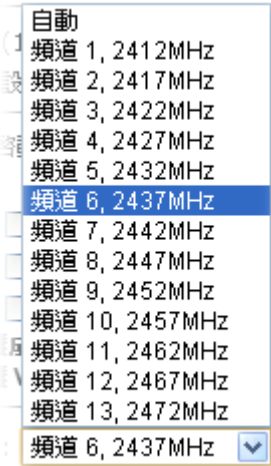
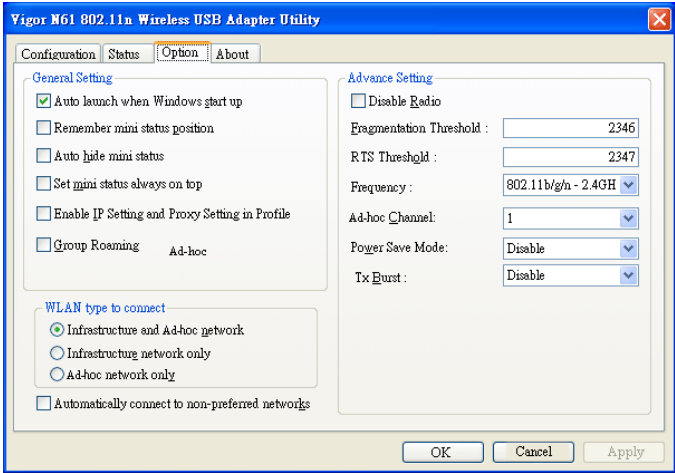
---

流量控制	啟動	上傳	下載
SSID 1	<input type="checkbox"/>	<span style="border: 1px solid black; padding: 2px;">30000</span> kbps	<span style="border: 1px solid black; padding: 2px;">30000</span> kbps
SSID 2	<input type="checkbox"/>	<span style="border: 1px solid black; padding: 2px;">30000</span> kbps	<span style="border: 1px solid black; padding: 2px;">30000</span> kbps
SSID 3	<input type="checkbox"/>	<span style="border: 1px solid black; padding: 2px;">30000</span> kbps	<span style="border: 1px solid black; padding: 2px;">30000</span> kbps
SSID 4	<input type="checkbox"/>	<span style="border: 1px solid black; padding: 2px;">30000</span> kbps	<span style="border: 1px solid black; padding: 2px;">30000</span> kbps

**附註:** 範圍 100~50,000 kbps

可用設定說明如下：

項目	說明
啟用	勾選此方塊啓動無線功能。
模式	請選擇一個適當的無線模式。
索引(1-15)	設定無線區域網路在特定的時間間隔中運作。您可以從 <b>應用的排程設定</b> 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。
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。
SSID	預設的 SSID 值為 <b>DrayTek</b> ，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。
隔離	<b>VPN</b> – 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。

	<p>成員- 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。</p>
<p>頻道</p>	<p>無線區域網路的通道頻率，預設頻道是 6，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。</p> 
<p>長封包標頭</p>	<p>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。</p>
<p>Packet-OVERDRIVE</p>	<p>這個功能可以強化資料傳輸的效果，約可提升 40%以上(務必勾選 <b>Tx Burst</b>)。只有在無線基地台與用戶雙方同時都啓用此項功能時，才會產生作用，也就是說無線用戶端必須支援並啓用此項功能。</p> <p><b>注意:</b> Vigor N61 無線轉接器支援此項功能。因此您可以使用並安裝在您的電腦上以便符合 Packet-OVERDRIVE 的需要(參考下圖 Vigor N61 無線工具視窗，勾選在 <b>Option</b> 標籤中的 <b>TxBURST</b>)。</p> 

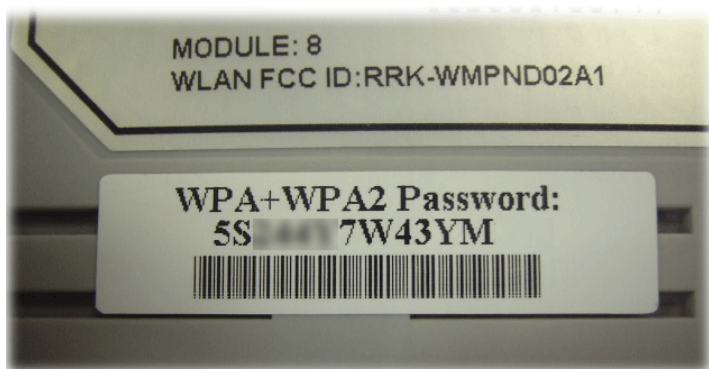
<b>流量控制</b>	可控制透過無線連線傳輸的資料傳送速率。 <b>上傳</b> – 勾選啓用方塊並輸入傳輸速率作為上傳資料之速率，預設值為 30,000 kbps。 <b>下載</b> – 勾選啓用方塊並輸入傳輸速率作為下載資料之速率，預設值為 30,000 kbps。
-------------	---

完成上述設定之後，請按下**確定**儲存。

### 4.16.3 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。



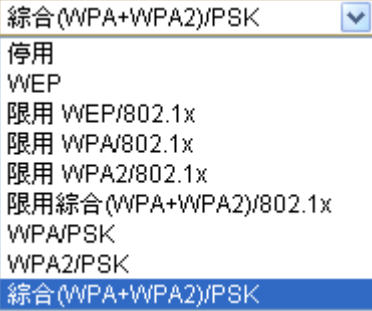
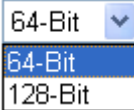
選擇**安全性設定**後，新的網頁將會出現，您可以在此頁面上調整 WEP 和 WPA 設定。

無線區域網路 >> 安全性設定

SSID 1	SSID 2	SSID 3	SSID 4
模式 <input type="text" value="綜合(WPA+WPA2)/PSK"/>			
設定 <b>RADIUS 伺服器</b> 若您已啓用 802.1x 功能			
<b>WPA:</b>			
加密模式		WPA 之 TKIP/WPA2 之 AES	
預先共用金鑰(PSK):		<input type="text" value="*****"/>	
輸入 8~63 ASCII 字元或是 64 個十六進位數字 "0x"，例如 "cfs01a2..." or "0x655abcd..."。			
<b>WEP:</b>			
加密模式		<input type="text" value="64 位元"/>	
<input checked="" type="radio"/> 金鑰 1		<input type="text" value="*****"/>	
<input type="radio"/> 金鑰 2		<input type="text" value="*****"/>	
<input type="radio"/> 金鑰 3		<input type="text" value="*****"/>	
<input type="radio"/> 金鑰 4		<input type="text" value="*****"/>	
<b>就 64-bit WEP 金鑰而言</b>			
輸入 5 個 ASCII 字元或 10 個十六進位數字 "0x"，例如 "AB312" 或 "0x4142333132"。			
<b>就 128-bit WEP 金鑰而言</b>			
輸入 13個 ASCII 字元或是 26 個十六進位數字 "0x"，例如 "0123456789abc" 或 "0x30313233343536373839414243"。			
<input type="button" value="確定"/>		<input type="button" value="取消"/>	

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。

	 <p><b>注意:</b>若您選擇了 802.1x 模式，您就必須同時設定 RADIUS 伺服器的內容。</p> <p><b>停用</b> - 關閉加密機制。</p> <p><b>WEP</b> - 只接受 WEP 用戶以及僅接受以 WEP 金鑰輸入的加密金鑰。</p> <p><b>WEP/802.1x Only</b> - 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。</p> <p><b>WPA/802.1x Only</b> - 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。</p> <p><b>WPA2/802.1x Only</b> - 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。</p> <p><b>Mixed (WPA+WPA2/802.1x only)</b> - 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。</p> <p><b>WPA/PSK</b> -接受 WPA 用戶，請在 PSK 中輸入加密金鑰。</p> <p><b>WPA2/PSK</b> -接受 WPA2 用戶，請在 PSK 中輸入加密金鑰。</p> <p><b>綜合 (WPA+ WPA2)/PSK</b> - 同時接受 WPA 與 WPA2 用戶，請在 PSK 中輸入加密金鑰。</p>
<p><b>WPA</b></p>	<p>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。<b>預先共用金鑰 (PSK)</b> - 輸入 <b>8~63</b> 個 ASCII 字元，像是 012345678 (或是 64 個 16 進位數字，以 0x 開頭，如 0x321253abcde...等)。</p>
<p><b>WEP</b></p>	<p><b>64-Bit</b> - 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)。</p> <p><b>128-Bit</b> - 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)。</p>  <p>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。</p>

完成上述設定之後，請按下**確定**儲存。

## 4.16.4 連線控制

爲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。

黑白名單的設定也可以同時包含 SSID 與 MAC 位址。

無線區域網路 >> 連線控制

**連線控制**

啟動 MAC 位址過濾器
  SSID 1 
 SSID 2 
  
 SSID 3 
 SSID 4

**MAC 位址過濾器**

索引	特性	MAC 位址	套用 SSID
<div style="border: 1px solid black; width: 100%; height: 100%;"></div>			

客戶端的 MAC 位址：

套用 SSID： SSID 1  SSID 2  SSID 3  SSID 4

特性： s: 將此無線站台和有線網路隔離

可用設定說明如下：

項目	說明
啟動 MAC 位址過濾器	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	顯示之前編輯的全部 MAC 位元址。
客戶端的 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。
特性	s - 勾選此項以便隔離無線用戶端之無線連線。
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。
全部清除	按此鈕儲存連線控制清單。

完成上述設定之後，請按下**確定**儲存。

#### 4.16.5 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。

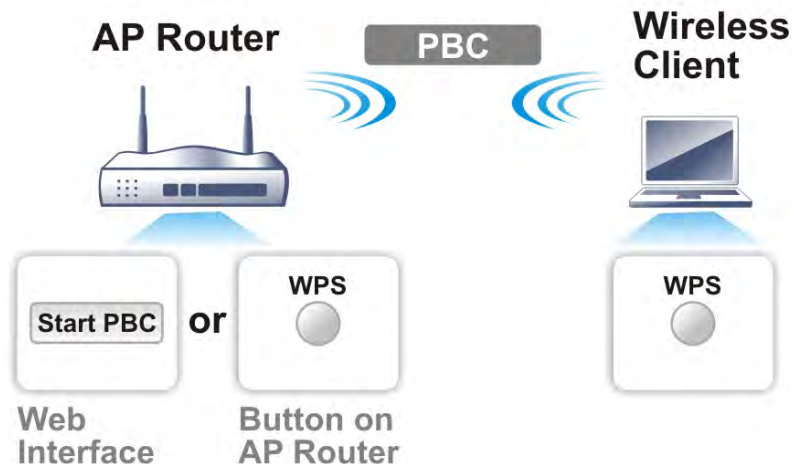


**注意：**此功能僅在無線用戶端也支援 WPS 功能時可用。

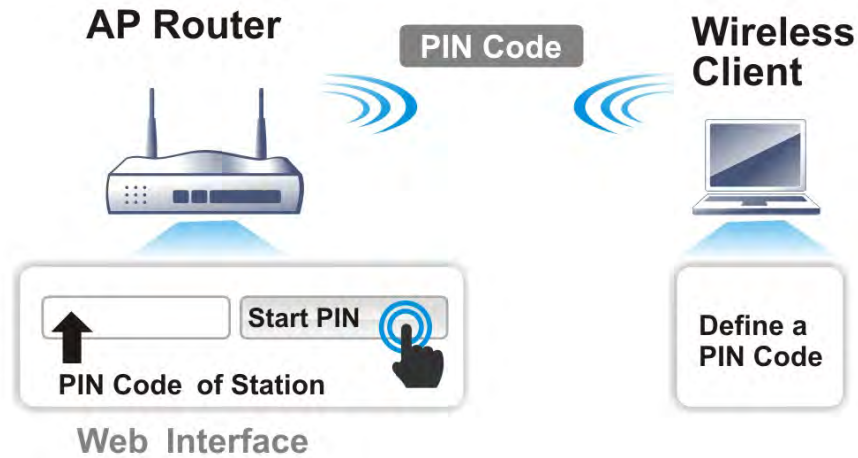
建立無線網路用戶與Vigor路由器之間的連線有個快速及簡單的方式，使用者不需要每次都必須選擇加密模式，或輸入任何長篇的資料以建立無線連線。使用者只要按下無線用戶端中的一個小小按鈕，WPS功能就會替他/她自動建立一個無線連線。

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 **Start PBC** 按鈕，一個是利用 **PIN Code** 來進行。

- Vigor 2925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 **Start 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 **Start PBC** 按鈕。



- 如果您想要使用 PIN 碼，您必須知道無線用戶所指定的 PIN 碼，然後將此資料在提供給您想要連線的 Vigor 路由器。



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>>安全性設定選擇此模式，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>>安全性設定頁面，選擇 WPA-PSK 或 WPA2-PSK 模式，再進入 WPS 頁面。

下圖為線區域網路>>WPS 網頁畫面。

**無線區域網路 >> WPS (Wi-Fi 保護設定)**

啟用 WPS

**Wi-Fi 保護設定資訊**

<b>WPS 狀態</b>	已設定
<b>SSID</b>	DrayTek
<b>驗證模式</b>	Mixed(WPA+WPA2)/PSK

**裝置設定**

<b>藉由 Push 按鈕來設定</b>	<input type="button" value="啟動 PBC"/>
<b>藉由用戶端 PinCode 來設定</b>	<input type="text"/> <input type="button" value="啟動 PIN"/>

狀態: 預備

**附註:** WPS 可讓無線用戶端自動連接至基地台。

: WPS 關閉

: WPS 已啟動

: 等待無線用戶端傳來的WPS需求

可用設定說明如下：

項目	說明
----	----

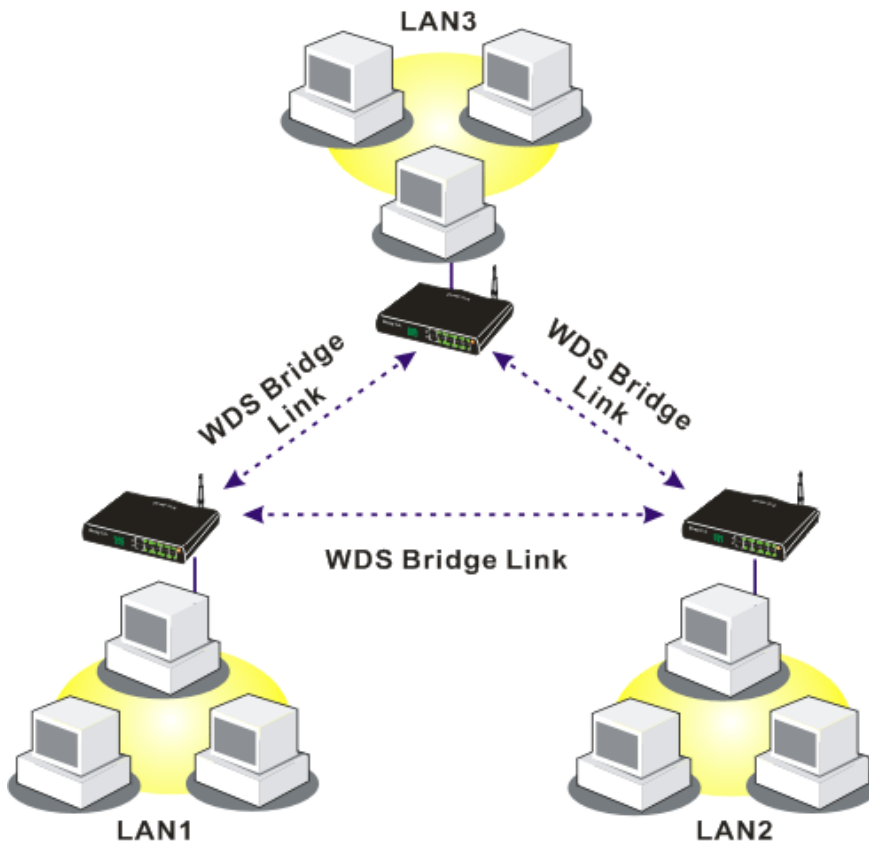
<b>啓用 WPS</b>	勾選此方塊啓動 WPS 設定。
<b>WPS 狀態</b>	顯示 WPS 相關的系統訊息，如果無線安全性(加密)功能已設定，您可以在這裡看到”設定完畢”等訊息。
<b>SSID</b>	顯示路由器的 SSID1 名稱，WPS 僅在 SSID1 中可用。
<b>驗證模式</b>	顯示路由器目前的驗證模式，請注意僅有 WPA2/PSK 和 WPA/PSK 支援 WPS。
<b>藉由 Push 按鈕來設定</b>	請按啓動 <b>PBC</b> 啓用 Push-Button 式的 WPS 設定程式，路由器將會等待 2 分鐘取得無線用戶傳送過來的 WPS 需求，當 WPS 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)。
<b>藉由用戶端 PinCode 來設定</b>	請輸入您想要連接的無線用戶所指定的 PIN 碼，在按啓動 <b>PIN</b> 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)。

#### 4.16.6 WDS

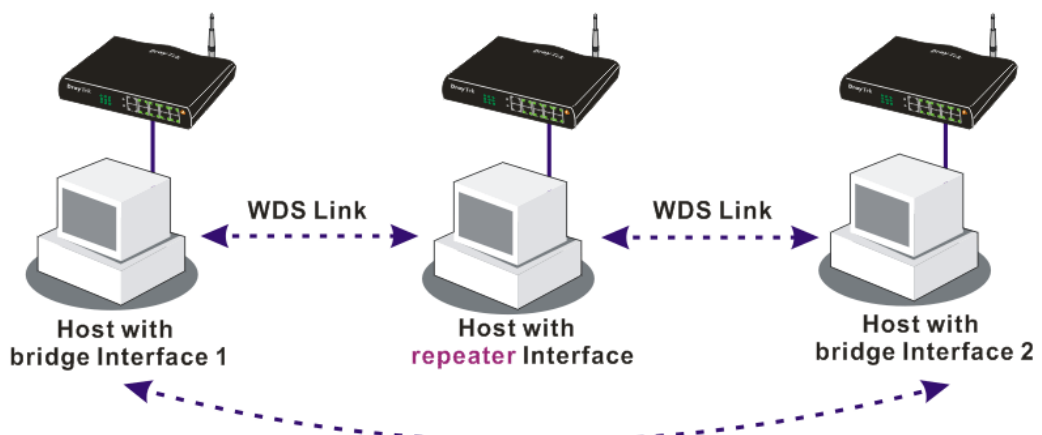
WDS 表示無線分派系統，是一個連結二個無線基地台的通訊協定，通常可以下列二種方式來應用。

- 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

迎合以上的需要，路由器可應用二種 WDS 模式，一為橋接一為中繼，下圖顯示 WDS 橋接介面的功能：

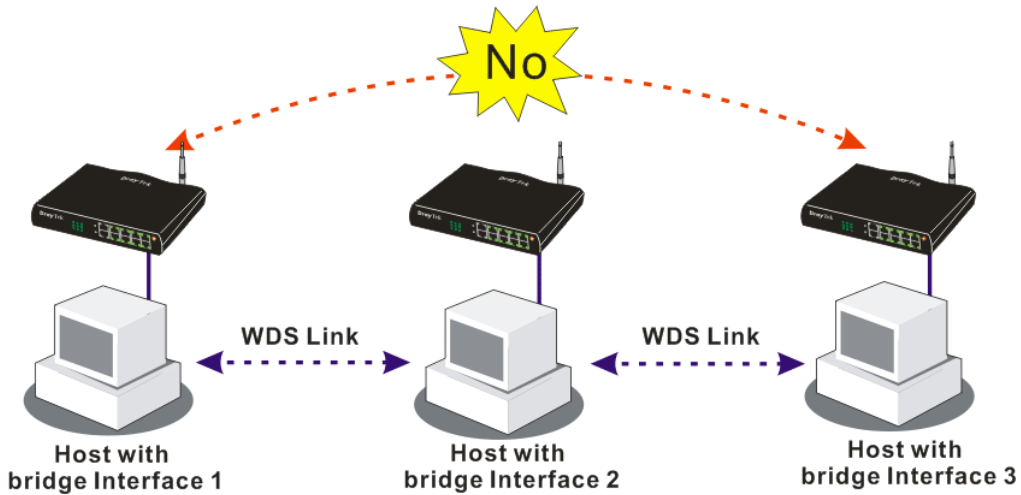


WDS-中繼模式的應用則描繪如下：



二種模式的主要不同點在於：**中繼**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。換言之，只有此模式能完成 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：

**無線區域網路 >> WDS 設定**

WDS 設定		回復出廠預設值
<b>模式:</b> <input type="button" value="停用"/>		<b>橋接</b> 啟用對方的 MAC 位址 <input type="checkbox"/> <input type="checkbox"/> : <input type="checkbox"/> : <input type="checkbox"/> : <input type="checkbox"/> : <input type="checkbox"/> : <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> : <input type="checkbox"/> : <input type="checkbox"/> : <input type="checkbox"/> : <input type="checkbox"/> : <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> : <input type="checkbox"/> : <input type="checkbox"/> : <input type="checkbox"/> : <input type="checkbox"/> : <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> : <input type="checkbox"/> : <input type="checkbox"/> : <input type="checkbox"/> : <input type="checkbox"/> : <input type="checkbox"/> <b>附註:</b> 為提升效率, 將中斷未使用的連線。
<b>安全性:</b> <input checked="" type="radio"/> 停用 <input type="radio"/> WEP <input type="radio"/> 預先共用金鑰 (PSK)		
<b>WEP:</b> 使用相同 WEP 金鑰設定於 <b>安全性設定</b> 。		
<b>預先共用金鑰 (PSK)</b> 類型: <input type="radio"/> WPA <input checked="" type="radio"/> WPA2 金鑰: <input type="text" value="*****"/> <b>附註:</b> WPA 與 WPA2 與居易 WPA 不相容  輸入 8 到 63 個 ASCII 字元或以 "0x" 開頭的 64 個十六進位字元, 例如: "cfigs01a2..." 或 "0x655abcd...."。		
		<b>中繼</b> 啟用對方的 MAC 位址 <input type="checkbox"/> <input type="checkbox"/> : <input type="checkbox"/> : <input type="checkbox"/> : <input type="checkbox"/> : <input type="checkbox"/> : <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> : <input type="checkbox"/> : <input type="checkbox"/> : <input type="checkbox"/> : <input type="checkbox"/> : <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> : <input type="checkbox"/> : <input type="checkbox"/> : <input type="checkbox"/> : <input type="checkbox"/> : <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> : <input type="checkbox"/> : <input type="checkbox"/> : <input type="checkbox"/> : <input type="checkbox"/> : <input type="checkbox"/>
		<b>無線基地台功能:</b> <input checked="" type="radio"/> 啟用 <input type="radio"/> 停用
		<b>狀態:</b> <input type="checkbox"/> 送出 "Hello" 訊息給對方  <input type="button" value="連線狀態"/> <b>附註:</b> 此功能只有當對方也支援該功能時才有效。
<input type="button" value="確定"/> <input type="button" value="取消"/>		

可用設定說明如下：

項目	說明
模式	選擇 WDS 設定模式，停用將無法啓用任何 WDS 設定；橋接模式乃是設計用來符合第一種實際之應用；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 和預設共用金鑰。您在此處所選擇的設定將會使得 WEP 或是預設共用金鑰有效或是無效。請自三種中挑選出一種。
WEP	勾選此方塊使用 <b>安全性設定</b> 頁面中同樣的金鑰。如果您並未在 <b>安全性設定</b> 頁面中設定任何的金鑰，此方塊將暫時無法使用。
預設共用金鑰	輸入開頭為“0x”之 8 ~ 63 個 ASCII 字元或是 64 的 16 進位的數字。
橋接	如果您選擇橋接做為通訊模式，請在此區輸入對方的 MAC 位址，本頁可讓您一次輸入六個對方 MAC 位址。停用不使用的連結可以取得較好的執行效果，如果您想要啓動對方的 MAC 位址，記得輸入完成後勾選 <b>啓用</b> 方塊。
中繼	如果您選擇 <b>中繼</b> 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，如果您想要啓動對方的 MAC 位址，記得輸入完成後勾選 <b>啓用</b> 方塊。
無線基地台功能	按 <b>啓用</b> 讓路由器提供無線基地台的服務；按 <b>停用</b> 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。

完成上述設定之後，請按下**確定**儲存。

## 4.16.7 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。

無線區域網路 >> 進階設定

### 實體連線模式

操作模式	<input checked="" type="radio"/> 綜合模式 <input type="radio"/> Green Field
頻道頻寬	<input type="radio"/> 20 <input checked="" type="radio"/> 20/40
防護間隔	<input type="radio"/> 長 <input checked="" type="radio"/> 自動
Aggregation MSDU(A-MSDU)	<input type="radio"/> 停用 <input checked="" type="radio"/> 啟用

確定

可用設定說明如下：

項目	說明
操作模式	<b>混合模式</b> – 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。 <b>Green Field</b> – 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	<b>20</b> – 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。 <b>20/40</b> – 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。
防護間隔	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 <b>自動</b> 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。
Aggregation 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 <b>啟用</b> 。

完成上述設定之後，請按下**確定**儲存。



## 4.16.8 WMM 設定

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。

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，此功能是针对大多數支援 VoIP 的行動電話或是無線電話而設計的。

無線區域網路 >> WMM 設定

WMM 設定
| 回復出廠預設值 |

WMM 功能  啟用  停用

APSD 功能  啟用  停用

**無線基地台(AP)之參數**

	Aifsn	CWMin	CWMax	Txop	ACM	AckPolicy
AC_BE	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="6"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>
AC_BK	<input type="text" value="7"/>	<input type="text" value="4"/>	<input type="text" value="10"/>	<input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>
AC_VI	<input type="text" value="1"/>	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="94"/>	<input type="checkbox"/>	<input type="checkbox"/>
AC_VO	<input type="text" value="1"/>	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="47"/>	<input type="checkbox"/>	<input type="checkbox"/>

**基地台(Station)之參數**

	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="10"/>	<input type="text" value="0"/>	<input type="checkbox"/>
AC_BK	<input type="text" value="7"/>	<input type="text" value="4"/>	<input type="text" value="10"/>	<input type="text" value="0"/>	<input type="checkbox"/>
AC_VI	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="94"/>	<input type="checkbox"/>
AC_VO	<input type="text" value="2"/>	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="47"/>	<input type="checkbox"/>

可用設定說明如下：

項目	說明
WMM 功能	在無線資料傳輸中應用 WMM 參數，請按啟用鈕。
APSD 功能	預設值為停用。
Aifsn	可控制用戶等待每筆資料傳輸的時間，請指定一個數值範圍在 1 到 15 之間。此參數將會影響 WMM 存取類型的延遲時間(time delay)。對聲音或是影像服務，請對 AC_VI 與 AC_VO 設定較小的數值，而對於電子郵件或是網路瀏覽，請對 AC_BE 與 AC_BK 設定較大的數值。
CWMin/CWMax	<b>CWMin</b> 表示 contention Window-Min 而 <b>CWMax</b> 表示 contention Window-Max，請指定數值範圍在 1 到 15 之間。注意 CWMax 一值必須大於或等於 CWMin，這二個數值都會影響 WMM 存取類型的延遲時間。AC_Vi 和 AC_VO 類型之間的差異必須小點，AC_BE 和 AC_BK 間的差異就必須大些。
Txop	表示傳輸機會，對於在資料傳輸中需要較高優先權的 AC_VI 與 AC_VO，請設定較大的數值以便取得較高的傳輸優先權，指定的數值範圍在 0 到 65535 之間。

<b>ACM</b>	<p>為 Admission Control Mandatory 的縮寫，可以限制無線用戶僅使用特定類型。</p> <p><b>注意:</b> Vigor2925 提供標準的 WMM 網頁設定，如果您想要修改參數，請參考 Wi-Fi WMM 標準規格來設定。</p>
<b>AckPolicy</b>	<p>“不勾選” (預設值)此方塊表示基地台路由器透過無線連線傳輸 WMM 封包時，將會回應傳輸需求，可確保對方一定收到 WMM 封包。</p> <p>“勾選”此方塊表示基地台路由器傳輸 WMM 封包時，不會回應任何傳輸需求，成效雖然較好但是可靠性較低。</p>

完成上述設定之後，請按下**確定**儲存。

## 4.16.9 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。

[無線區域網路 >> 搜尋無線基地台](#)

**無線基地台列表**

BSSID	頻道	SSID
<div style="border: 1px solid black; width: 100%; height: 100%;"></div>		

檢視 **統計**。

**附註**在搜尋過程中 (少於5秒)，無線站台將無法和基地台連線。

---

**新增 WDS 設定：**

無線基地台的MAC位址  :  :  :  :  :

橋接  中繼

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	顯示基地台所使用的頻道統計資料。 <div style="border: 1px solid black; padding: 5px;"> <p><small>無線區域網路 &gt;&gt; 可用網路統計</small></p> <p>建議使用的頻道:</p> <div style="border: 1px solid black; padding: 5px; text-align: center;"> <p><small>無線基地台數目與頻道的比較</small></p> <p><small>頻道</small></p> </div> <p style="text-align: center;"><input type="button" value="取消"/></p> </div>
新增	如果您想要找到套用 WDS 設定的無線基地台，請在本頁底部輸入該 AP 的 MAC 位址，然後按 <b>新增</b> ，稍後該 MAC 位址即會加入 WDS 設定頁面中。

## 4.16.10 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連線控制，這樣就可以了。

無線區域網路 >> 無線用戶端列表

無線用戶端列表

狀態	MAC 位址	與下述相連
----	--------	-------

**狀態代碼:**  
C: 已連線, 未加密  
E: 已連線, WEP.  
P: 已連線, WPA  
A: 已連線, WPA2  
B: 受到連線控制功能的封鎖  
N: 連線中  
F: 無法通過 WPA/PSK 認證

**附註:** 使用者成功連線至路由器後可能會無預警關閉。在此種情況下，於連線過期前該使用者仍會出現在清單上。

**新增至 連線控制:**

客戶端的 MAC 位址       :  :  :  :  :

可用設定說明如下：

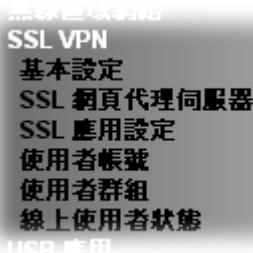
項目	說明
更新頁面	按此鈕更新用戶端的 MAC 位址列表。
新增	按此鈕新增選定之 MAC 位址至連線控制。

## 4.17 SSL VPN

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

SSL VPN 提供的好處有二：

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



### 4.17.1 基本設定

本頁決定 SSL VPN 以及 SSL Tunnel 的基本設定內容。

SSL VPN >> 基本設定

SSL VPN 基本設定

埠號	<input type="text" value="443"/> (預設值: 443)
伺服器憑證	<input type="text" value="自行簽核"/> ▼
加密金鑰演算法	<input type="radio"/> 高 - AES(128 bits)以及 3DES <input checked="" type="radio"/> 預設 - RC4(128 bits) <input type="radio"/> 低 - DES

附註：此設定可作用在所有SSL應用上

確定

取消

可用設定說明如下：

項目	說明
埠號	此埠號設定乃提供與 SSL VPN 伺服器之用，不會影響系統維護>>管理中的 HTTPS 埠號設定。基本上，預設值是 443。
伺服器憑證	若先前已經建立了數項憑證，可透過下拉式清單選擇任何一個使用者定義的憑證，否則請用自行簽核讓路由器使用內建的預設憑證。預設憑證可用於 SSL VPN 伺服器以及 HTTPS 網頁代理伺服器。 但當用戶端未設定任何憑證時，預設憑證將用於 HTTPS 以及 SSL VPN 伺服器。
加密金鑰演算法	選擇用於 SSL VPN 伺服器資料連線時使用的加密等級。

完成全部設定之後，請按**確定**儲存設定值。

## 4.17.2 SSL 網頁代理伺服器

SSL 網頁伺服器可使遠端使用者透過 SSL 登入內部的網站。

SSL VPN >> SSL 網頁代理伺服器

SSL 網頁代理伺服器設定檔: | 回復出廠預設值 |

索引編號	名稱	URL	啓用
1.			X
2.			X
3.			X
4.			X
5.			X
6.			X
7.			X
8.			X
9.			X
10.			X

各個項目說明如下：

項目	說明
名稱	顯示您所建立的設定檔名稱。
URL	顯示 URL。
啓用	顯示設定檔的目前狀態(啓用或是未啓用)。

按下任一索引連結進行細部設定。

SSL VPN >> SSL 網頁代理伺服器

設定檔索引: 1

名稱	<input type="text"/>
URL	<input type="text"/>
主機 IP 位址	<input type="text"/>
存取方式	<input type="button" value="安全通訊埠重導向"/> <input type="button" value="停用"/> <input type="button" value="安全通訊埠重導向"/> <input type="button" value="SSL"/>

附註: URL 必須輸入如下格式 http://ip:port/Domain\_name/directory，其中 Domain\_name 為完整格式的網域名稱(FQDN)。

可用設定說明如下：

項目	說明
名稱	輸入設定檔的名稱。
URL	輸入代理伺服器的位址或是路徑。
主機 IP 位址	如果您輸入功能為 URL，您必須在本區輸入相應的 IP 位址，此區必須符合 URL 設定。

存取方式	<p>有數種方式可使用：</p> <p><b>停用</b> – 設定檔不起作用，如果您選擇停用，在 VPN 遠端撥入網頁中，所有的網頁代理伺服器也都會消失。</p> <p><b>安全通訊埠重導向</b> –1)此項技術套用於將 WAN 埠口對應至私人埠口。此項選擇有二種限制：1)僅適用於 WAN 到 LAN，網頁伺服器需設定在路由器的後端；2)網頁伺服器開道位址必須指向 Vigor 路由器。另外，使用者需再 SSL 用戶端的入口頁面手動執行連線(Connect)。</p> <p><b>SSL</b> – 如果您選擇此項，於 SSL 上的代理伺服器將會應用於 VPN。</p>
------	--

完成全部設定之後，請按**確定**儲存設定值。

### 4.17.3 SSL 應用設定

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

SSL VPN >> SSL 應用設定

SSL 應用設定檔:

[| 回復出廠預設值 |](#)

索引編號	名稱	主機位址	服務	啟用
1.				X
2.				X
3.				X
4.				X
5.				X
6.				X
7.				X
8.				X
9.				X
10.				X

各個項目說明如下：

項目	說明
名稱	顯示您建立的應用設定檔的名稱。
主機位址	顯示 VNC/RDP 的 IP 位址或是 SAMBA 路徑。
服務	顯示選擇的服務類型例如 VNC/RDP/SAMBA
啟用	顯示選定的設定檔目前的狀態(啟用或是不啟用)。

欲建立新的 SSL 應用設定檔：

1. 點選任一索引編號連結。

## SSL VPN >>SSL 應用設定

### SSL 應用設定檔:

索引編號	名稱
1.	
2.	
3.	
4.	

2. 下述頁面將出現：

### SSL VPN >>SSL 應用設定

#### 索引編號: 1

<input type="checkbox"/> 啓動應用服務	
應用名稱	<input type="text"/>
應用	<div style="border: 1px solid black; padding: 2px;">           虛擬網路計算 (VNC)            ---請選擇---            虛擬網路計算 (VNC)            遠端桌面通訊協定 (RDP)            Samba 應用         </div>
IP 位址	
埠號	
閒置逾時	
比例	100%

可用設定說明如下：

項目	說明
啓用應用服務	勾選此框啓用此設定檔。
應用名稱	輸入應用的名稱。
應用	<p>有三種類型可以建立應用設定檔：</p> <div style="border: 1px solid black; padding: 2px; margin-bottom: 5px;">           虛擬網路計算 (VNC)            ---請選擇---            虛擬網路計算 (VNC)            遠端桌面通訊協定 (RDP)            Samba 應用         </div> <p><b>虛擬網路計算 (VNC)</b> – 讓您透過 VNC 協定登入並控制遠端電腦。</p> <p><b>遠端桌面通訊協定 (RDP)</b> – 讓您透過 RDP 協定登入並控制遠端電腦。</p> <p><b>Samba 應用</b> – 讓您透過 Samba 服務登入並控制遠端電腦。</p>
IP 位址	如果您選擇的是 VNC 或是 RDP，您必須在此輸入 IP 位址。
埠號	如果您選擇的是 VNC 或是 RDP，您必須指定用於此協定的埠號，預設值為 5900。
閒置逾時	如果您選擇的是 VNC，您必須指定中斷 SSL VPN 通道



	的時間。
比例	如果您選擇的是 VNC，您必須選擇此應用的比例值 (100%, 80%, 60%)。
螢幕大小	如果您選擇的是 RDP，您必須選擇適合此應用的螢幕大小。
Samba 路徑	如果您選擇的是 Samba，您必須指定 Samba 服務的路徑。

- 輸入必要資訊。
- 完成上述設定之後，按下**確定**儲存並回到上頁。

SSL VPN >> SSL 應用設定

SSL 應用設定檔:

| 回復出廠預設值 |

索引編號	名稱	主機位址	服務	啟用
<u>1.</u>	VNC_1	192.168.1.5:5900	VNC	v
<u>2.</u>				x
<u>3.</u>				x
<u>4.</u>				x
<u>5.</u>				x
<u>6.</u>				x
<u>7.</u>				x
<u>8.</u>				x
<u>9.</u>				x
<u>10.</u>				x

#### 4.17.4 使用者帳號

辨識驗證與管理都是透過使用者管理來進行，因此 SSL VPN 使用者帳號必須與遠端撥入使用者的設定頁面相同。

SSL VPN >> 遠端登入使用者

遠端存取用戶帳號: | 回復出廠預設值 |

檢視:  全部  連線  斷線

索引編號	用戶	使用中	狀態	索引編號	用戶	使用中	狀態
<a href="#">1.</a>	???	<input type="checkbox"/>	---	<a href="#">17.</a>	???	<input type="checkbox"/>	---
<a href="#">2.</a>	???	<input type="checkbox"/>	---	<a href="#">18.</a>	???	<input type="checkbox"/>	---
<a href="#">3.</a>	???	<input type="checkbox"/>	---	<a href="#">19.</a>	???	<input type="checkbox"/>	---
<a href="#">4.</a>	???	<input type="checkbox"/>	---	<a href="#">20.</a>	???	<input type="checkbox"/>	---
<a href="#">5.</a>	???	<input type="checkbox"/>	---	<a href="#">21.</a>	???	<input type="checkbox"/>	---
<a href="#">6.</a>	???	<input type="checkbox"/>	---	<a href="#">22.</a>	???	<input type="checkbox"/>	---
<a href="#">7.</a>	???	<input type="checkbox"/>	---	<a href="#">23.</a>	???	<input type="checkbox"/>	---
<a href="#">8.</a>	???	<input type="checkbox"/>	---	<a href="#">24.</a>	???	<input type="checkbox"/>	---
<a href="#">9.</a>	???	<input type="checkbox"/>	---	<a href="#">25.</a>	???	<input type="checkbox"/>	---
<a href="#">10.</a>	???	<input type="checkbox"/>	---	<a href="#">26.</a>	???	<input type="checkbox"/>	---
<a href="#">11.</a>	???	<input type="checkbox"/>	---	<a href="#">27.</a>	???	<input type="checkbox"/>	---
<a href="#">12.</a>	???	<input type="checkbox"/>	---	<a href="#">28.</a>	???	<input type="checkbox"/>	---
<a href="#">13.</a>	???	<input type="checkbox"/>	---	<a href="#">29.</a>	???	<input type="checkbox"/>	---
<a href="#">14.</a>	???	<input type="checkbox"/>	---	<a href="#">30.</a>	???	<input type="checkbox"/>	---
<a href="#">15.</a>	???	<input type="checkbox"/>	---	<a href="#">31.</a>	???	<input type="checkbox"/>	---
<a href="#">16.</a>	???	<input type="checkbox"/>	---	<a href="#">32.</a>	???	<input type="checkbox"/>	---

<< [1-32](#) | [33-64](#) >> >> 下一頁 >>

附註: 使用者帳號必須加入使用者群組中以便啟動SSL Portal登入。

**注意:** 共有 64 個設定檔可以設定，但是同時進行的連線數最多只達 25 條。

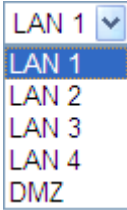
按下任一索引編號編輯遠端使用者設定檔。

## 索引編號 1

<b>使用者帳號與認證</b> <input checked="" type="checkbox"/> 開啓這個帳號 閒置逾時 <input type="text" value="300"/> 秒		使用者名稱 <input type="text" value="???"/> 密碼(最多 19個字元) <input type="text"/> <input type="checkbox"/> 啓動行動動態密碼系統(mOTP) PIN 碼 <input type="text"/> 密鑰 <input type="text"/>	
<b>允許的撥入模式</b> <input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPsec 通道 <input checked="" type="checkbox"/> 具有 IPsec 原則的 L2TP <input type="text" value="無"/> <input type="button" value="v"/> <input checked="" type="checkbox"/> SSL 通道		<b>IKE 認證方式</b> <input checked="" type="checkbox"/> 預先共鑰金鑰 <input type="text" value="IKE 預先共鑰金鑰"/> <input type="text"/> <input type="checkbox"/> 數位簽章(X.509) <input type="text" value="無"/> <input type="button" value="v"/>	
<input checked="" type="checkbox"/> 指定遠端節點 遠端用戶 IP <input type="text"/> 或對方 ID <input type="text"/> Netbios 命名封包 <input checked="" type="radio"/> 通過 <input type="radio"/> 封鎖 經由 VPN 執行多重播送 <input type="radio"/> 通過 <input checked="" type="radio"/> 封鎖 (針對某些 IGMP,IP-Camera,DHCP Relay等而言)		<b>IPsec 安全性模式</b> <input checked="" type="checkbox"/> 中級(AH) 高級(ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES 本機 ID (視需要填入) <input type="text"/>	
<b>子網路遮罩</b> <input type="button" value="v"/> LAN 1 <input type="checkbox"/> 指定固定 IP 位址 <input type="text" value="0.0.0.0"/>			

可用設定說明如下：

項目	說明
使用者帳號與認證	<p><b>開啓這個帳號</b> -勾選此方塊以啓用此功能。</p> <p><b>閒置逾時</b> - 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。</p>
允許的撥入模式	<p><b>PPTP</b> -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。</p> <p><b>IPSec 通道</b>-允許遠端撥入使用者透過網際網路觸發 IPSec VPN 連線。</p> <p><b>具有 IPsec 原則的 L2TP</b>-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：</p> <ul style="list-style-type: none"> <li>● <b>無</b> - 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。</li> <li>● <b>建議選填</b> -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 連線會成爲一種完全的 L2TP 連線。</li> <li>● <b>必須</b> - 此選項可在 L2TP 連線中明確指定所要運用的 IPsec 原則。</li> </ul> <p><b>SSL 通道</b>-允許遠端撥入用戶透過網際網路進行 SSL VPN</p>

項目	說明
	<p>連線。如果您勾選此框，專屬此帳號的 <b>SSL 通道</b> 就會立即啓動。</p> <p><b>指定遠端節點</b>-您可以指定遠端撥入使用者或是對方 <b>ID</b> (應用於 <b>IKE 主動模式</b>中)的 <b>IP 位址</b>。若您不勾選此項，即表示您所選擇的連線類型，將會應用<b>基本設定</b>中所設定的驗證方式和安全防护方式。</p> <p><b>Netbios 命名封包</b></p> <ul style="list-style-type: none"> <li>● <b>通過</b> – 按此鈕讓資料能在二台主機之間所建立的 VPN 通道上傳輸。</li> <li>● <b>封鎖</b> – 當雙方所建立的 VPN 通道連線產生衝突時，此功能可以此通道。</li> </ul> <p><b>經由 VPN 執行多重播送</b> -某些程式可透過 VPN 連線進行多重播送封包。</p> <ul style="list-style-type: none"> <li>● <b>通過</b> -點選此鈕讓多重播送封包通過路由器。</li> <li>● <b>封鎖</b> – 此為預設值。點選此鈕之後，路由器將會封鎖多重播送封包。</li> </ul>
子網路遮罩	<p>選擇此 VPN 設定檔所需的子網。</p>  <p><b>指定固定 IP 位址</b> – 請輸入固定 IP 位址。</p>
使用者名稱	<p>當您選擇 <b>PPTP</b> 或是 <b>L2TP</b> 含/不含 <b>IPSec</b> 原則時，本區是可應用的。請輸入名稱。</p>
密碼	<p>當您選擇 <b>PPTP</b> 或是 <b>L2TP</b> 含/不含 <b>IPSec</b> 原則時，本區是可應用的。請輸入密碼。</p>
啓動行動動態密碼系統 (mOTP)	<p>勾選此框以便利用 <b>mOTP</b> 功能進行驗證。</p> <p><b>PIN 碼</b> – 輸入驗證專用碼 (例如 1234)。</p> <p><b>密鑰</b> – 使用行動電話中由 <b>mOTP</b> 產生的 32 個數字密碼(例如 e759bb6f0e94c7ab4fe6)。</p>
IKE 認證方式	<p>當您指定遠端節點的 <b>IP 位址</b>時，本區僅適用於 <b>IPsec 通道</b> 與具有 <b>IPSec 原則</b>的 <b>L2TP</b> 類型，唯一例外的是當您選擇 <b>IPsec 通道</b>時，不論有無指定 <b>IP 位址</b>，您還可以設定數位簽章(X.509)。</p> <p><b>預先共同金鑰</b>- 勾選此方塊啓用此功能並輸入 1-63 文字做為預先共同金鑰。</p> <p><b>數位簽章 (X.509)</b>-勾選此方塊啓用此功能並選擇一組事先定義的簽章內容 (在 <b>VPN 和遠端存取&gt;&gt;IPSec 端點辨識</b>中設定)。</p>

項目	說明
<b>IPSec 安全性模式</b>	<p>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。</p> <p><b>中級 -Authentication Header (AH)</b>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。</p> <p><b>高級 -Encapsulating Security Payload (ESP)</b>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。</p> <p><b>本機 ID(視需要填入)</b>-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。</p>

完成全部設定之後，請按**確定**儲存設定值。

## 4.17.5 使用者群組

有 10 組使用者群組設定檔可以用來設定，並可運用在使用者管理、VPN 等地方。

SSL VPN >>使用者群組

索引編號	名稱	狀態
1.		X
2.		X
3.		X
4.		X
5.		X
6.		X
7.		X
8.		X
9.		X
10.		X

各個項目說明如下：

項目	說明
回復出廠預設值	按下此連結清除全部設定檔內容。
索引編號	顯示設定檔連結之編號。
名稱	顯示設定檔名稱。

按下任一索引編號編輯遠端使用者設定檔。

SSL VPN >>使用者群組

索引編號 1

啟用

群組名稱

存取權限

SSL 網頁伺服器

SSL 應用

驗證方式

本地使用者資料庫

可用的使用者帳號

選定的使用者帳號

>>

<<

RADIUS

LDAP / Active Directory

確定

清除

取消

可用設定說明如下：

項目	說明				
啓用	勾選此方塊啓用此設定檔。				
群組名稱	輸入此群組設定檔名稱。				
存取權限	<p>指定設定檔名的存取權限。</p> <p>目前，Vigor 路由器允許您建立 SSL 網頁伺服器以及 SSL 應用設定檔，可用的設定檔會顯示在畫面上。</p> <div style="border: 1px solid black; padding: 5px;"> <p><b>存取權限</b></p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;"><input checked="" type="checkbox"/> SSL 網頁伺服器</td> <td style="width: 50%;"><input checked="" type="checkbox"/> SSL 應用</td> </tr> <tr> <td><input type="checkbox"/> SSL_WP_1</td> <td><input type="checkbox"/> Game_APP</td> </tr> </table> </div>	<input checked="" type="checkbox"/> SSL 網頁伺服器	<input checked="" type="checkbox"/> SSL 應用	<input type="checkbox"/> SSL_WP_1	<input type="checkbox"/> Game_APP
<input checked="" type="checkbox"/> SSL 網頁伺服器	<input checked="" type="checkbox"/> SSL 應用				
<input type="checkbox"/> SSL_WP_1	<input type="checkbox"/> Game_APP				
驗證方式	<p>決定設定檔的驗證方法。</p> <p><b>本地使用者資料庫</b> – 系統利用使用者定義的設定檔(在 <b>VPN 與遠端存取&gt;&gt;遠端撥入使用者</b> 頁面)進行驗證，啓用的設定檔將條列在<b>可用的使用者帳號</b>區，如要新增設定檔至群組當中，只要選擇該設定檔名然後按下<b>&gt;&gt;</b>鈕，該選定檔將顯示在<b>選定的使用者帳號</b>區中。</p> <p><b>RADIUS</b> – RADIUS 伺服器利用使用者和密碼進行驗證。</p> <p><b>LDAP / Active Directory</b> – 如果勾選的是此項，LDAP / AD 伺服器會利用選擇的設定檔內容以及帳號密碼來進行驗證。</p> <p>若上述三種選項都啓用時，系統將據此按照順序執行驗證。</p>				

完成全部設定之後，請按**確定**儲存設定值。

## 4.17.6 線上使用者狀態

如果您已經完成 SSL 網頁伺服器的設定，使用者即可登入 DrayTek SSL VPN 入口網站查看相關設定。

DrayTek

Provide SSL VPN

Home SSL Web Proxy SSL Tunnel [logout]

INFO

mike ,  
(172.17.1.42)  
Welcome to DrayTek  
SSL VPN!

Timeout after 5 minutes.  
[Reset]

Main Page:

You have successfully logged in!  
You are given the following privileges:

- SSL Web Proxy
- SSL Tunnel

Copyright © 2006, DrayTek Corp. All Rights Reserved.

接著，使用者可以開啓 **SSL VPN>> 線上使用者狀態** 檢視 SSL VPN 登入狀態。

### SSL VPN >>線上使用者狀態

目前使用者	主機 IP	閒置逾時(秒)	動作
Kate	192.168.30.14	299	Drop

更新秒數: 10 [更新]

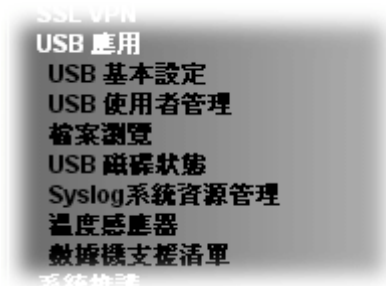
可用設定說明如下：

項目	說明
目前使用者	顯示目前運用 SSL VPN 伺服器的使用者。
主機 IP	顯示主機的 IP 位址。
閒置逾時	顯示強迫登出的剩餘時間。
動作	您可按下 Drop 按鈕中斷利用路由器 SSL 入口網站登入的特定使用者。



## 4.18 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** 頁面所建立的帳號以及密碼，然後，用戶端就可以使用 FTP(USB 儲存碟)或是分享 Samba 服務。



### 4.18.1 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啓用 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)。

USB 應用 >> USB 基本設定

**USB 基本設定**

**基本設定**

同步 FTP 連線  (最大 6)

預設字集

**Samba 服務設定(網路芳鄰)**

啓用  停用

**存取模式**

限用 LAN  LAN 與 WAN

**NetBios 命名服務**

工作群組名稱

主機名稱


**附註:**

1. 如果字集設定為"英文"，系統僅支援較長之英文檔名
2. 路由器的FTP伺服器會阻擋同時數個連線數的FTP下載，如果您的FTP用戶端具備數個連線數機制像是 File Zilla 的話，為了取得較佳的連線效果，您必須將用戶的FTP同時連線設定為 1。
3. 工作群組名稱不可與主機名稱相同，工作群組最多可以有 15個字元而與主機名稱最多可以有 23 個字元，但二者都不能包含下述字元: . ; : " < > \* + = / \ | ? .

確定

可用設定說明如下：

項目	說明
基本設定	<b>同步 FTP 連線</b> - 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。 <b>欲設字集</b> - 目前，Vigor 路由器支援四種語文字集，預

	設字集為英文。 
<b>Samba 服務設定</b>	點選啓用以便透過路由器啓用 samba 服務。
<b>存取模式</b>	限用 LAN – 網際網路使用者不可連接至路由器的 samba 伺服器。 <b>LAN 與 WAN</b> - LAN 與 WAN 端使用者皆可登入路由器的 samba 伺服器。
<b>NetBios 命名服務</b>	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: " < > * + = \   ?。 <b>工作群組名稱</b> – 輸入工作群組的名稱。 <b>主機名稱</b> – 輸入路由器的主機名稱。

完成全部設定之後，請按**確定**儲存設定值。

#### 4.18.2 USB 使用者管理

本頁讓您針對 FTP/Samba 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。

USB 應用 >> USB 使用者管理


USB 使用者管理

[回復出廠預設值](#)

索引編號	使用者名稱	預設檔案夾	索引編號	使用者名稱	預設檔案夾
<a href="#">1.</a>			<a href="#">9.</a>		
<a href="#">2.</a>			<a href="#">10.</a>		
<a href="#">3.</a>			<a href="#">11.</a>		
<a href="#">4.</a>			<a href="#">12.</a>		
<a href="#">5.</a>			<a href="#">13.</a>		
<a href="#">6.</a>			<a href="#">14.</a>		
<a href="#">7.</a>			<a href="#">15.</a>		
<a href="#">8.</a>			<a href="#">16.</a>		

按任一索引號碼連結登入設定頁面。


設定檔編號: 1

FTP/Samba 使用者	<input type="radio"/> 啟用 <input checked="" type="radio"/> 停用
使用者名稱	<input type="text"/>
密碼	<input type="text"/> (最多 11 個字元)
確認密碼	<input type="text"/>
預設檔案夾	<input type="text"/> 
<b>存取規則</b>	
檔案	<input type="checkbox"/> 讀取 <input type="checkbox"/> 覆寫 <input type="checkbox"/> 刪除
目錄	<input type="checkbox"/> 清單 <input type="checkbox"/> 建立 <input type="checkbox"/> 刪除

附註: 檔案夾名稱只能包含下列字元: A-Z a-z 0-9 \$ % ' - \_ @ ~ ` ! ( ) / 以及空格。

可用設定說明如下：

項目	說明
FTP/Samba 使用者	<p><b>啟用</b> – 按此鈕啟動此 FTP 服務或是 Samba 使用者服務設定檔(帳號)，之後，使用者可使用本頁指定的名稱來登入 FTP 伺服器。</p> <p><b>停用</b> – 按下此鈕停用此設定檔。</p>
使用者名稱	<p>輸入 FTP/Samba 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。</p> <p><b>注意:</b> 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 軟體更新時使用。</p> <p><b>注意:</b> 路由器不支援 FTP Passive 模式。請在 FTP 用戶端停用此模式。</p>
密碼	<p>輸入 FTP/Samba 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。</p>
確認密碼	<p>再次輸入密碼確認。</p>
預設檔案夾	<p>此功能決定用戶登入的檔案夾。</p> <p>使用者可以在本區輸入目錄名稱，接著按下<b>確定</b>，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。</p> <p><b>注意:</b> 當 USB 儲存碟的防寫狀態開啓時，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。</p> <p>您可以點  以開啓下述對話盒新增檔案夾作為預設檔案夾。</p>

	
<p><b>存取規則</b></p>	<p>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。</p> <p><b>檔案</b> – 勾選允許開放的項目(讀取、覆寫、刪除)。</p> <p><b>目錄</b> – 勾選允許開放的項目(清單、建立、刪除)。</p>

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。

### 4.18.3 檔案瀏覽

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。

USB 應用 >> 檔案瀏覽

**檔案瀏覽器**

目前路徑: /

名稱	大小	刪除	重新命名
<b>上傳檔案</b>			
選擇檔案:			
<input type="button" value="選擇檔案"/> 未選擇檔案			
<input type="button" value="上傳"/>			

**附註:** 檔案夾內容未清空，無法刪除！

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。

### 4.18.4 USB 磁碟狀態

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 儲存碟，請先按下**中斷 USB 磁碟連線**，然後移除儲存碟。

USB 應用 >> USB 磁碟狀態

**USB 儲存裝置狀態**

連線狀態: 沒有連接任何磁碟

磁碟容量: 0 MB  
 可用容量: 0 MB

**USB 磁碟用戶已連接**

索引編號	服務	IP 位址(埠號)	使用者名稱

**附註:** 如果USB磁碟的保護開關打開，磁碟將處於**僅供讀取**模式，無法覆寫資料。

可用設定說明如下：

項目	說明
----	----

連線狀態	如果路由器沒有連接任何 USB 儲存碟，此處會顯示”沒有連接任何磁碟”。
磁碟容量	顯示 USB 儲存碟的總容量。
可用容量	顯示 USB 儲存碟的目前剩餘的容量。按下 <b>更新頁面</b> 可取得最新的容量資訊。
索引編號	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。

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。

#### 4.18.5 Syslog 系統資源管理


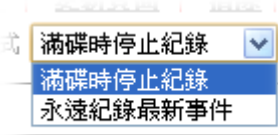
本頁提供即時 Syslog 並顯示相關資訊在螢幕上。

##### 針對網頁 Syslog

自我診斷工具 >> 網頁防火牆 Syslog

網頁 Syslog	USB 紀錄
<input type="checkbox"/> 啟用網頁 Syslog <span style="float: right;">輸出   更新頁面   清除  </span>	
Syslog 類型 <span style="border: 1px solid black; padding: 2px;">使用者</span> 顯示模式 <span style="border: 1px solid black; padding: 2px;">滿碟時停止紀錄</span>	
時間	訊息

可用設定說明如下：

項目	說明
啟用網頁 Syslog	勾選此方框啟用網頁 Syslog 功能。
Syslog 類型	使用下拉式清單指定 Syslog 顯示的類型。 
顯示模式	有二種模式可以選擇。  <p><b>滿碟時停止紀錄</b> – 當 Syslog 紀錄容量滿了之後，系統將會停止紀錄。</p>

	永遠紀錄最新事件 – 系統僅紀錄最新的事件。
時間	顯示事件發生的時間。
訊息	顯示每個事件的資訊。

## 對於 USB Syslog

本頁顯示 USB 儲存碟上的 syslog 紀錄。

自我診斷工具 >> 網頁防火牆 Syslog

網頁 Syslog		USB 紀錄	
附註:儲存的Syslog 檔案若大於1MB，Syslog 將會顯示出來。			
檔案夾: n/a	檔案: n/a	頁: n/a	紀錄類型: n/a
時間	紀錄類型	訊息	

各個項目說明如下：

項目	說明
時間	顯示事件發生的時間。
紀錄類型	顯示紀錄的類型。
訊息	顯示事件的相關資訊。

## 4.18.6 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。

### 溫度感應器設定

USB 應用 >> 溫度感應器設定

溫度感應器設定		溫度圖表	
<b>顯示設定</b>			
溫度校對	<input type="text" value="0.00"/>		
溫度單位	<input checked="" type="radio"/> 攝氏 <input type="radio"/> 華氏		
<b>警示設定</b>			
<input type="checkbox"/> 啟用 Syslog 警示			
溫度上限	<input type="text" value="30.00"/>		
溫度下限	<input type="text" value="18.00"/>		
<input type="button" value="確定"/>			

可用設定說明如下：

項目	說明
顯示設定	<b>溫度校對</b> - 輸入校正溫度錯誤的數值。 <b>溫度單位</b> - 選擇溫度的顯示單位，有二種類型可以選擇。
警示設定	<b>啟用 Syslog 警示</b> - 勾選此框啟用此功能。 <b>溫度上限/溫度下限</b> - 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：

USB 應用 >> 溫度感應器圖表



### 4.18.7 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

下述相容測試條列出含USB數據機/行動裝置的Vigor路由器。  
如果確認為最新版但仍不可使用時，請與居易客服連絡support@draytek.com。

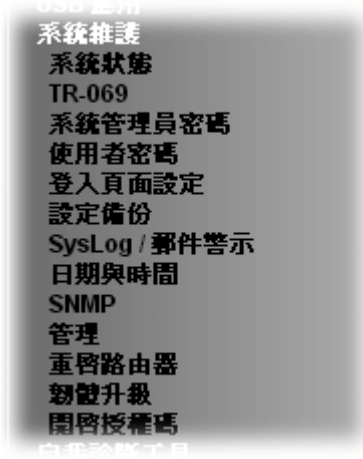
3.5G		
品牌	模組	狀態
Aiko	Aiko 83D	Y
BandRich	Bandlux C170	Y
BandRich	Bandlux C270	Y
BandRich	Bandlux C321	Y
BandRich	Bandlux C331	Y
BandRich	Bandlux C502	Y
Huawei	Huawei E169u	Y
Huawei	Huawei E173	Y
Huawei	Huawei E220	Y
Sony Ericsson	Sony Ericsson MD300	Y
Vodafone	Vodafone K3765-Z	Y
Vodafone	Vodafone K4605	Y
ZTE	ZTE MF626	Y
ZTE	ZTE MF627 plus	Y
ZTE	ZTE MF633	Y
ZTE	ZTE MF636	Y

Y:已測試且已支援  
M:尚未測試但可能已經支援。

## 4.19 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、系統管理員密碼、備份組態、系統紀錄/郵件警示、時間設定、重啓系統及韌體升級等等。

下圖為系統維護的主要設定功能。



### 4.19.1 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 : Vigor2925n  
 韌體版本 : 3.7.2.2  
 建立日期/時間 : Aug 22 2013 16:44:25

區域網路					
	MAC 位址	IP 位址	子網路遮罩	DHCP 伺服器	DNS
區域網路1	00-1D-AA-AC-19-C8	192.168.1.1	255.255.255.0	否	8.8.8.8
LAN2	00-1D-AA-AC-19-C8	192.168.2.1	255.255.255.0	是	8.8.8.8
LAN3	00-1D-AA-AC-19-C8	192.168.3.1	255.255.255.0	是	8.8.8.8
LAN4	00-1D-AA-AC-19-C8	192.168.4.1	255.255.255.0	是	8.8.8.8
LAN5	00-1D-AA-AC-19-C8	192.168.5.1	255.255.255.0	是	8.8.8.8
DMZ PORT	00-1D-AA-AC-19-C8	192.168.6.1	255.255.255.0	是	8.8.8.8
IP 路由子網	00-1D-AA-AC-19-C8	192.168.0.1	255.255.255.0	是	8.8.8.8

無線網路			
MAC 位址	頻率/網域	韌體版本	SSID
	歐洲	2.5.0.11	DrayTek

廣域網路					
	連線狀態	MAC 位址	連線	IP 位址	預設閘道
WAN1	斷線	00-1D-AA-AC-19-C9	---	---	---
WAN2	斷線	00-1D-AA-AC-19-CA	---	---	---
WAN3	斷線	00-1D-AA-AC-19-CB	---	---	---

IPv6			
	位址	範圍	網際網路連線模式
LAN	FE80::21D:AFF:FEAC:19C8/64	Link	---

使用者模式 為 關閉。

各個項目說明如下：

項目	說明
型號名稱	顯示路由器的型號名稱。

<b>韌體版本</b>	顯示路由器的韌體版本。
<b>建立日期與時間</b>	顯示目前韌體建立的日期與時間。
<b>區域網路</b>	<p><b>MAC 位址</b>-顯示區域網路介面的 MAC 位址。</p> <p><b>第一個 IP 位址</b>-顯示區域網路介面的 IP 位址。</p> <p><b>第一個子網路遮罩</b>-顯示區域網路介面的子網路遮罩位址。</p> <p><b>DHCP 伺服器</b>-顯示區域網路介面的 DHCP 伺服器目前的狀態。</p> <p><b>DNS</b>-顯示主要 DNS 的 IP 位址。</p>
<b>無線網路</b>	<p><b>MAC 位址</b>-顯示無線區域網路的 MAC 位址。</p> <p><b>頻率網域</b> -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。</p> <p><b>韌體版本</b> -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。</p> <p><b>SSID</b>-顯示路由器的 SSID。</p>
<b>WAN</b>	<p><b>連線狀態</b>-顯示目前實體連線的狀態。</p> <p><b>MAC 位址</b>-顯示 WAN 介面的 MAC 位址。</p> <p><b>連線</b>-顯示目前連線的類型。</p> <p><b>IP 位址</b>-顯示 WAN 介面的 IP 位址。</p> <p><b>預設閘道</b>-顯示預設閘道指定的 IP 位址。</p>
<b>IPv6</b>	<p><b>位址</b> - 顯示區域網路的 IPv6 位址。</p> <p><b>範圍</b> - 顯示 IPv6 位址範圍，例如 IPv6 Link Local 只能用於直接 IPv6 連線，不可用於 IPv6 網際網路。</p> <p><b>網際網路連線模式</b> - 顯示登入網際網路選擇的連線模式。</p>

## 4.19.2 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。

系統維護 >> TR-069 設定

### ACS 及 CPE 設定

經此連往 ACS 伺服器	網際網路
<b>ACS 伺服器</b>	
URL	<input type="text"/>
使用者名稱	<input type="text"/>
密碼	<input type="text"/>
<b>CPE 用戶端</b>	
<input type="radio"/> 啟用 <input checked="" type="radio"/> 停用	
URL	<input type="text"/>
埠號	8069
使用者名稱	vigor
密碼	*****

### 定期通知設定

<input checked="" type="radio"/> 停用 <input type="radio"/> 啟用	
間隔時間	900 秒(s)

### STUN 設定

<input checked="" type="radio"/> 停用 <input type="radio"/> 啟用	
伺服器位址	<input type="text"/>
伺服器埠號	3478
最小維持連線時間	60 秒(s)
最大維持連線時間	-1 秒(s)

0)

確定

可用設定說明如下：

項目	說明
經此連往 ACS 伺服器	選擇路由器連往 ACS 伺服器的介面。
ACS 伺服器	<b>URL/使用者名稱/密碼</b> – 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。
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。 <b>啟用/停用</b> – 有時候，系統可能會產生埠號衝突，為解決這個問題，您可能需要改變 CPE 的埠號，請勾選 <b>啟用</b> 再變更埠號。
定期通知設定	預設值為 <b>啟用</b> ，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 <b>停用</b> 關閉通知機制。

<b>STUN 設定</b>	<p>預設值是<b>停用</b>，如果您選擇了<b>啓用</b>，請輸入下述相關資料：</p> <p><b>伺服器 IP</b> – 輸入 STUN 伺服器的 IP 位址。</p> <p><b>伺服器埠號</b> – 輸入 STUN 伺服器的埠號。</p> <p><b>最小維持連線時間</b> – 如果啓用了 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。</p> <p><b>最大維持連線時間</b> – 如果啓用了 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。</p>
----------------	---

完成設定之後，按下**確定**按鈕儲存相關設定。

### 4.19.3 系統管理員密碼

本頁允許您設定新的密碼。

系統維護 >> 系統管理員密碼設定

#### 系統管理員密碼

舊密碼	<input type="text"/>
新密碼	<input type="text"/>
確認密碼	<input type="text"/>

附註:密碼只能包含 a-z A-Z 0-9 , ; : . " < > \* + = \ | ? @ # ^ ! ( )

可用設定說明如下：

項目	說明
<b>舊密碼</b>	請輸入舊密碼。
<b>新密碼</b>	請在本區輸入新密碼。
<b>確認密碼</b>	再次輸入新密碼以確認。

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。

## 4.19.4 使用者密碼

本頁允許您設定新的密碼。

系統維護 >> 使用者密碼

啟用使用者模式進行簡易網頁設定

使用者密碼

| 回復出廠預設值 |

密碼	<input type="text"/>
確認密碼	<input type="text"/>

附註： 1.密碼僅能包含 a-z A-Z 0-9 , ; : . " < > \* + = \ | ? @ # ^ ! ( )  
2.密碼不能僅包含\*，例如\*或是\*\*都是不合法的，但是123\*或是\*45是可行的。

確定

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設定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。

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。

以下為使用者範例：

1. 開啓**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**以便啓用使用者模式操作。在**密碼與確認密碼**欄位中輸入新的密碼，然後按下**確定**。

系統維護 >> 使用者密碼

啟用使用者模式進行簡易網頁設定

使用者密碼

| 回復出廠預設值 |

密碼	<input type="password"/>
確認密碼	<input type="password"/>

附註： 1.密碼僅能包含 a-z A-Z 0-9 , ; : . " < > \* + = \ | ? @ # ^ ! ( )  
2.密碼不能僅包含\*，例如\*或是\*\*都是不合法的，但是123\*或是\*45是可行的。

確定

3. 下述畫面顯示出來後，按下**確定**。

系統維護 >> 使用者密碼

使用中的組態

密碼	:*****
----	--------

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啓要求輸入使用者名稱與密碼，輸入新的密碼然後按下**登入**。

The login page for the DrayTek Vigor2925 Series. It features the DrayTek logo and "Vigor2925 Series" in a red header. Below the header is a "Login" section with three input fields: "使用者名稱" (Username), "密碼" (Password), and "群組" (Group). The password field is masked with dots. A "登入" (Login) button is located to the right of the input fields. At the bottom, there is a copyright notice: "Copyright © 2013 DrayTek Corp. All Rights Reserved."/>

**DrayTek** Vigor2925 Series

**Login**

使用者名稱

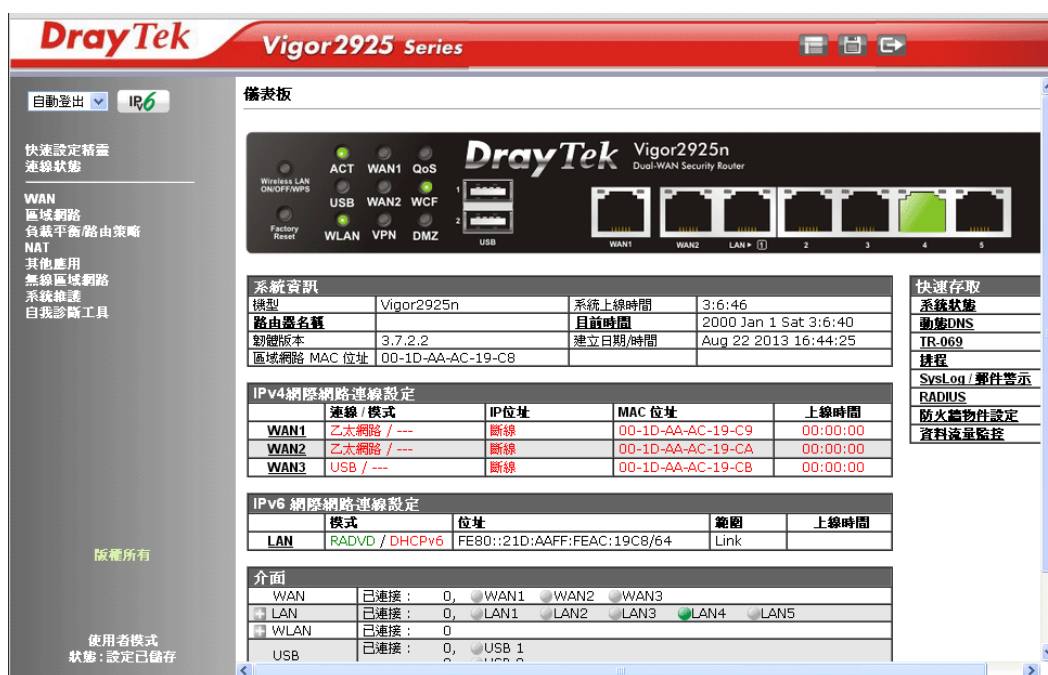
密碼

群組

**登入**

Copyright © 2013 DrayTek Corp. All Rights Reserved.

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。

**注意：**使用者模式中的設定方式如同管理者模式。

#### 4.19.5 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。

系統維護 >> 登入頁面設定

登入頁面設定

啟用

登入頁面標題  (最多 31 個字元)

歡迎訊息與佈告欄 (文長最多 511 個字元) 預覽 | 回復出廠預設值 |

```
<h1><b><font color=red>Welcome Message</font></b></h1><p>This welcome message is displayed in the Login page of the router. Replace this text with your own message. </p><ol><li>The welcome message can be written in HTML so lists such as this one can be created </li><li>Other markup tags such as p, font or img can be used</li></ol>
```

歡迎訊息範例:  

```
<h1><b><font color=red>Welcome Message</font></b></h1>
<p>訊息</p>
```

Available settings are explained as follows:

項目	說明
----	----



啓用	勾選此框啓用登入頁面客製化功能。
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。
回復出廠預設值	按下此連結回到出廠預設值。

下圖顯示客製化登入頁面範例：



## 4.19.6 設定備份

### 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。

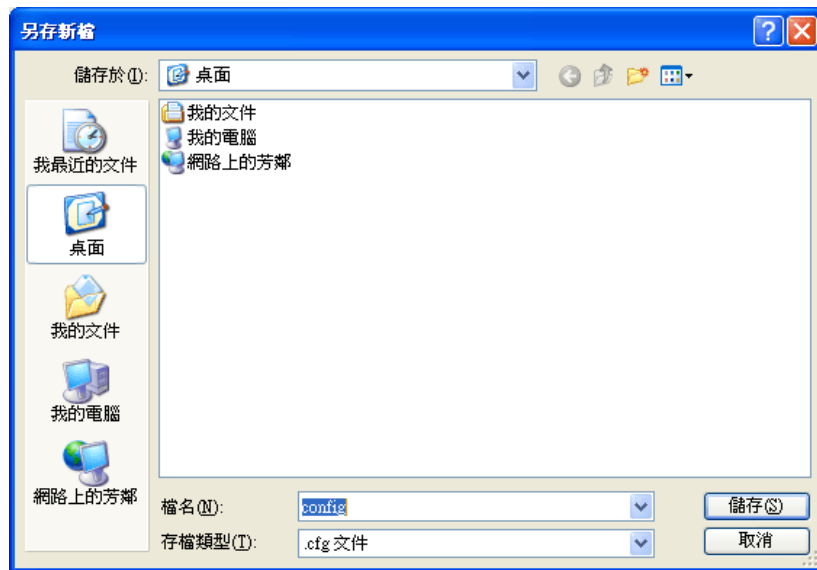
系統維護 >> 備份設定

備份/還原組態設定	
<b>還原</b>	選取一個設定檔。 <input type="button" value="選擇檔案"/> 未選擇檔案 按一下"還原"上傳檔案。 <input type="button" value="還原"/>
<b>備份</b>	按一下"備份"下載目前的設定檔。 <input type="button" value="備份"/> <input type="button" value="取消"/>

2. 按**備份**按鈕進入下一個對話盒，按**儲存**按鈕開啓另一個視窗以儲存設定。



3. 在**另存新檔**對話盒中，預設檔名為 **config.cfg**，您也可以在此輸入不同的檔名。



4. 按下**儲存**按鈕，設定將會以檔名 **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。

**附註:**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。

系統維護 >> 備份設定

### 備份還原組態設定

<b>還原</b>
選取一個設定檔。
<input type="button" value="選擇檔案"/> 未選擇檔案
按一下"還原"上傳檔案。
<input type="button" value="還原"/>
<b>備份</b>
按一下"備份"下載目前的設定檔。
<input type="button" value="備份"/> <input type="button" value="取消"/>

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。

## 4.19.7 Syslog/郵件警示設定

SysLog 在 Unix 系統中是很受歡迎的一種工具，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。此依程式可以在本地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。

系統維護 >> Syslog / 郵件警示設定

Syslog / 郵件警示設定	
<p><b>Syslog 存取設定</b></p> <p><input checked="" type="checkbox"/> 啟用</p> <p>Syslog 儲存至:</p> <p><input checked="" type="checkbox"/> Syslog 伺服器</p> <p><input type="checkbox"/> USB 磁碟</p> <p><b>路由器名稱</b> <input type="text"/></p> <p>伺服器 IP 位址 <input type="text"/></p> <p>目的通訊埠 <input type="text" value="514"/></p> <p>郵件 Syslog</p> <p>啟用 Syslog 訊息:</p> <p><input checked="" type="checkbox"/> 防火牆記錄</p> <p><input checked="" type="checkbox"/> VPN 記錄</p> <p><input checked="" type="checkbox"/> 使用者網路存取紀錄</p> <p><input checked="" type="checkbox"/> WAN 記錄</p> <p><input checked="" type="checkbox"/> 路由器/DSL資訊</p> <p><b>警告紀錄設定</b></p> <p><input type="checkbox"/> 啟用</p> <p>警告紀錄通訊埠 <input type="text" value="514"/></p>	<p><b>郵件警示功能設定</b></p> <p><input checked="" type="checkbox"/> 啟用 <input type="button" value="傳送測試郵件"/></p> <p>SMTP 伺服器 <input type="text"/></p> <p>SMTP 埠號 <input type="text" value="25"/></p> <p>收件人 <input type="text"/></p> <p>回信地址 <input type="text"/></p> <p><input type="checkbox"/> 使用 SSL</p> <p><input type="checkbox"/> 驗證</p> <p>使用者名稱 <input type="text"/></p> <p>密碼 <input type="text"/></p> <p>啟用郵件警示訊息:</p> <p><input checked="" type="checkbox"/> DoS 攻擊</p> <p><input checked="" type="checkbox"/> IM-P2P</p> <p><input checked="" type="checkbox"/> VPN LOG</p>

附註: 1. 除非在 "Syslog儲存至" 項目中勾選了USB磁碟，否則郵件 Syslog 不會被啟動。  
 2. 郵件 Syslog 功能會在 Syslog 檔案尺寸大於 1M時會傳送出來。  
 3. 我們僅支援埠號465的安全SMTP連線。

確定

清除

可用設定說明如下：

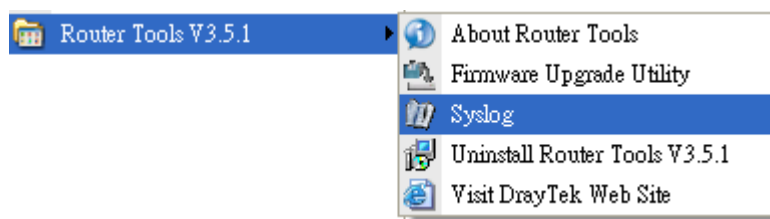
項目	說明
SysLog 存取設定	<p><b>啟用</b> - 勾選啓用以啓動系統記錄服務功能/啓動郵件警示功能。</p> <p><b>Syslog 儲存至</b> - 勾選此框可儲存紀錄至 Syslog 伺服器中。</p> <p><b>USB 磁碟</b> - 勾選此框可儲存紀錄至 USB 儲存碟中。</p> <p><b>路由器名稱</b> - 顯示此路由器於系統維護&gt;&gt;管理頁面中設定的名稱。</p> <p>若此處沒有名稱，請至系統維護&gt;&gt;管理設定路由器名稱。</p> <p><b>伺服器 IP 位址</b>-指定全部系統紀錄訊息傳送前往目的地之 IP 位址。</p> <p><b>目標通訊埠</b>-指定全部系統紀錄訊息傳送前往目的地之通訊埠。</p> <p><b>啟用 syslog 訊息</b>-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。</p>
警告紀錄設定	勾選啓用可啓動警告記錄功能。

	<b>警告紀錄通訊埠</b> - 輸入警告紀錄通訊埠號，預設值為 514。
<b>郵件警示功能設定</b>	<p>勾選啓用以便啓動郵件警示功能。</p> <p><b>傳送測試郵件</b>-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。</p> <p><b>SMTP 伺服器</b> -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。</p> <p><b>收件人</b>-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。</p> <p><b>回信位址</b>-指定另一組信箱的郵件位址，接收因收信人信箱錯誤而造成發生失敗的所有回覆訊息。</p> <p><b>使用 SSL</b> - 勾選此框使用埠號 465 作為 SMTP 伺服器，讓電子郵件伺服器使用 HTTPS 作為傳輸方式。</p> <p><b>驗證</b>-當使用電子郵件應用程式，勾選此方塊可啓動驗證的功能。</p> <ul style="list-style-type: none"> <li>● <b>使用者名稱</b>-輸入驗證所需的使用者名稱。</li> <li>● <b>密碼</b>-輸入驗證所需的密碼。</li> </ul> <p><b>啓用郵件警告訊息</b>-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。</p>

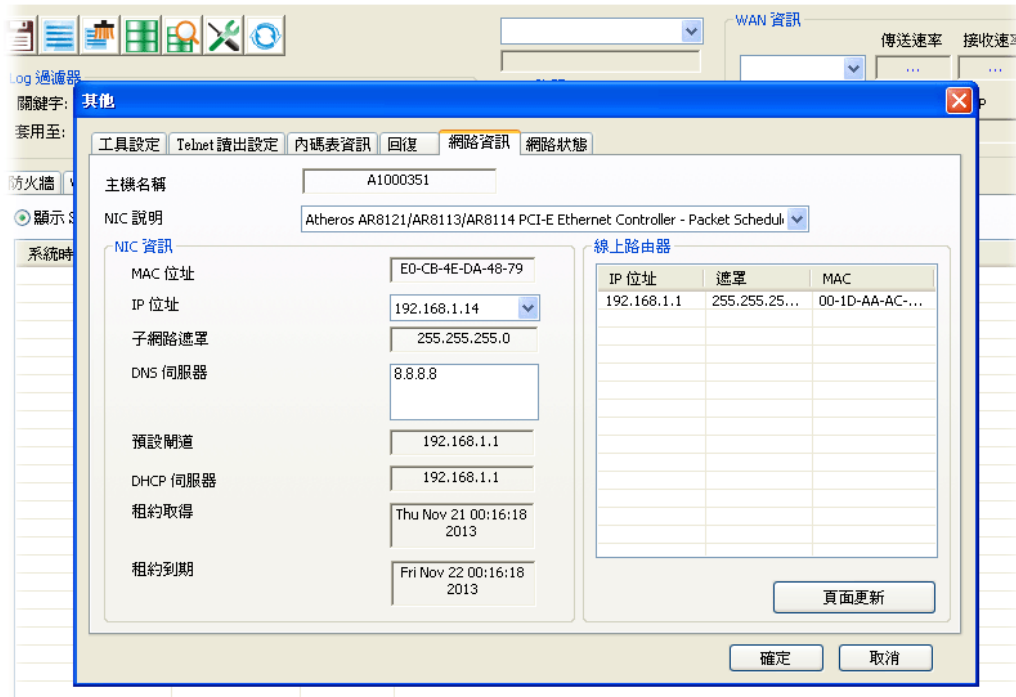
按**確定**儲存所有的設定。

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(**Network Information**)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。



### 4.19.8 時間和日期

允許您指定自何處取得路由器時間。

系統維護 >> 日期與時間

#### 時間資訊

目前系統時間: 2000 Jan 1 Sat 3 : 16 : 49 [取得時間]

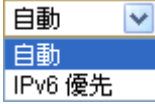
#### 時間設定

使用本台PC的時間  
 使用網際網路時間  
 時間伺服器: pool.ntp.org  
 優先權: 自動  
 時區: (GMT) 格林威治標準時間:都柏林  
 啟用日光節約時間  
 自動更新間隔: 30分鐘

[確定] [取消]

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。
使用本台 PC 的時間	選擇此項以便採用遠端管理者電腦上的瀏覽器時間。
使用網際網路的時間伺服器	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 <b>自動</b> 或是 <b>IPv6 優先</b> 作為優先選項。 
時區	選擇路由器所在的時區。
啓動日光節約時間	勾選此方塊啓動日光節約時間，在某些地區，這個項目是很有用處的。
自動更新間隔	選定時間間隔以供 NTP 伺服器更新之用。

全部設定完成之後，請按**確定**儲存目前的設定。

## 4.19.9 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。

系統維護 >> SNMP

### SNMP 設定



<input checked="" type="checkbox"/> 啟用 SNMP 代理	
取得社群(Get Community)	public
設定社群(Set Community)	private
管理者主機 IP(IPv4)位址	
管理者主機 IP (IPv6)位址	
封鎖社群(Trap Community)	public
通知主機 IP(IPv4) 位址	
通知主機 IP(IPv6)	
封鎖逾時(Trap Timeout)	10
<input type="checkbox"/> 啟用 SNMPV3 代理	
USM 使用者	
驗證演算方式	無驗證
驗證密碼	
隱私演算方式	無隱私
隱私密碼	

確定 取消

可用設定說明如下：

項目	說明
啟用 SNMP 代理程式	勾選此項以啟動此功能。
取得社群 (Get Community)	請輸入適當的文字以設定取得社群名稱，預設名稱爲 <b>public</b> 。
設定社群 (Set Community)	請輸入適當的名稱以設定社群，預設名稱爲 <b>private</b> 。
管理者主機 IP (IPv4)	設定一台主機做爲管理者以便執行 SNMP 功能，請輸入 IP 位址(IPv4)指定特定主機。
管理者主機 IPc	設定一台主機做爲管理者以便執行 SNMP 功能，請輸入 IP 位址(IPv6)指定特定主機。
封鎖社群 (Trap Community)	輸入適當名稱設定封鎖社群，預設名稱爲 <b>public</b> 。
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。
封鎖逾時	預設值爲 10 秒。
啟用 SNMPV3 代理	勾選此框啓用此功能。



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。
驗證演算方式	選擇下列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。
隱私演算方式	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。

全部設定完成之後，請按**確定**儲存目前的設定。

## 4.19.10 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

系統維護 >> 管理

IPv4 管理設定		IPv6 管理設定	
路由器名稱 <input type="text"/>		<b>管理通訊埠設定</b> <input checked="" type="radio"/> 使用者定義通訊埠 <input type="radio"/> 預設通訊埠	
<b>管理存取控制</b> <input checked="" type="checkbox"/> 允許從網際網路管理 <input type="checkbox"/> FTP 通訊埠 <input checked="" type="checkbox"/> HTTP 通訊埠 <input checked="" type="checkbox"/> HTTPS 通訊埠 <input checked="" type="checkbox"/> Telnet 通訊埠 <input type="checkbox"/> SSH 通訊埠 <input checked="" type="checkbox"/> 停用來自外部網際網路的PING		Telnet 通訊埠 <input type="text" value="23"/> (預設值: 23) HTTP 通訊埠 <input type="text" value="80"/> (預設值: 80) HTTPS 通訊埠 <input type="text" value="443"/> (預設值: 443) FTP 通訊埠 <input type="text" value="21"/> (預設值: 21) SSH 通訊埠 <input type="text" value="22"/> (預設值: 22)	
<b>存取清單</b> 清單 IP 子網路遮罩			
1 <input type="text"/> <input type="text"/>			
2 <input type="text"/> <input type="text"/>			
3 <input type="text"/> <input type="text"/>			
<input type="button" value="確定"/>			

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。
管理存取控制	<b>允許從網路管理</b> -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。 <b>斷絕來自網際網路的 PING</b> -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。
存取清單	您可以指定系統管理者只能從指定的主機或是清單定義的網路上登入，您一次最多可定義三個 IP/子網路遮罩於此區域中。 <b>清單 IP</b> – 指定一個允許登入至路由器的 IP 地址。 <b>子網路遮罩</b> -代表允許登入至路由器的子網路遮罩。
管理通訊埠設定	<b>使用者定義通訊埠</b> -勾選此項以指定使用者定義的埠號作為 Telnet、HTTP 和 FTP 伺服器之用。 <b>預設通訊埠</b> -勾選此項以使用標準埠號作為 Telnet 和 HTTP 伺服器之用。

全部設定完成之後，請按**確定**儲存目前的設定。

## 針對 IPv6

系統維護 >> 管理

IPv4 管理設定	IPv6 管理設定
<b>管理存取控制</b> 允許從網際網路管理 <input type="checkbox"/> Telnet 伺服器 (埠號: 23) <input type="checkbox"/> HTTP 伺服器 (埠號: 80) <input type="checkbox"/> 啓用來自外部網際網路的PING	
<b>存取清單</b> 清單 IPv6 位址 / 前置號碼長度 1. <input type="text"/> / <input type="text"/> 2. <input type="text"/> / <input type="text"/> 3. <input type="text"/> / <input type="text"/> <b>附註:</b> Telnet / HTTP 伺服器埠號與 IPv4使用的埠號相同	
<input type="button" value="確定"/>	

可用設定說明如下：

項目	說明
管理存取控制	<b>允許從網際網路管理</b> - 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。 <b>啓用來自外部網際網路的 PING</b> - 勾選此方框可讓系統接受來自外部網際網路的封包檢測，針對安全需要，此功能在預設時是關閉的。
存取清單	您可以指定系統管理者只能從特定主機或是網路登入，一次可設定三組 IP 位址。 <b>IPv6 位址/前置號碼長度</b> - 指定允許登入路由器的 IP 位址。

全部設定完成之後，請按**確定**儲存目前的設定。

## 4.19.11 重啓路由器

網路設定可以用來重新啓動路由器，請自**系統維護**中按**重啓路由器**開啓如下頁面。

**系統維護 >> 重啓路由器**

### 重啓路由器

**您想重新啓動路由器嗎？**

使用目前組態  
 使用原廠預設組態

**立即重啓**

### 自動重啓時間排程

索引號碼(1-15)於 **排程** 設定: , , ,

**附註:** 將忽略動作與間置逾時設定

**確定**

**取消**

**索引編號(1-15)於排程設定** - 您可以輸入四組排程設定檔進行系統重啓作業，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啓動路由器，請勾選**使用目前組態**，然後按**立即重啓**；如果要重設路由器設定回復成爲預設值，請勾選**使用原廠預設組態**，然後按**立即重啓**，路由器將會花 5 秒重新啓動系統。

**注意:** 當系統在您完成網頁設定並跳出**重啓路由器**網頁後，請務必按下**立即重啓**以重新啓動路由器，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。

## 4.19.12 韌體升級

在您更新路由器韌體之前，您必須先行安裝路由器工具。**韌體更新工作**即包含在此工具內，以下的網頁透過範例說明引導您更新韌體，注意此範例是在 Windows 操作系統下完成。

自居易網站或是 FTP 站下載最新的韌體版本，居易網站為 [www.draytek.com](http://www.draytek.com)，FTP 站則是 [ftp.draytek.com](http://ftp.draytek.com)。

請自**系統維護**選擇**韌體升級**以便啓動韌體更新工具。

系統維護 >> 韌體升級

### 網頁韌體升級


選擇韌體檔案 <input type="button" value="選擇檔案"/> 未選擇檔案 按升級以上傳檔案。 <input type="button" value="升級"/>
--

### 從LAN端執行 TFTP 韌體升級

目前韌體版本: 3.7.2.2
<b>韌體升級程序:</b>
<ol style="list-style-type: none"><li>1. 按 "確定" 開啓 TFTP 伺服器。</li><li>2. 開啓韌體升級公用程式或其它協力廠商 TFTP 用戶端軟體。</li><li>3. 檢查韌體檔名是否正確。</li><li>4. 按下韌體更新工具的 "Upgrade" 按鈕啓動更新作業。</li><li>5. 升級完成後，TFTP 伺服器將自動停止執行。</li></ol>
您確定要升級韌體嗎? <input type="button" value="確定"/>

按**選擇檔案**選取正確的韌體版本，然後按**升級**按鈕，系統會自動更新路由器的韌體版本。按**確定**，下述畫面將會出現，之後再使用韌體更新工具完成更新。

系統維護 >> 韌體升級

 TFTP 伺服器運作中。請執行韌體升級公用程式以升級路由器的韌體，當韌體升級完成後，此伺服器將自行關閉。
--

### 4.19.13 開啓授權碼

有三種方式可開啓 Vigor 路由器的網頁內容過濾器服務(WCF)，使用**服務啓動精靈**、透過**數位內容安全管理>>網頁內容過濾器設定檔**或是透過**系統管理>>開啓授權碼**。

在您完成 WCF 設定檔之後，您即可啓動網頁內容過濾服務機制。

按**系統管理>>開啓授權碼**開啓下述頁面以登入 <http://myvigor.draytek.com>。

系統維護 >> 開啓授權碼 啓動經由介面: 自動選取 ▾

---

**網頁過濾器授權碼** **啓動**

[狀態:Commtouch] [起始日期:2013-02-25 到期日期:2013-03-27]

驗證訊息

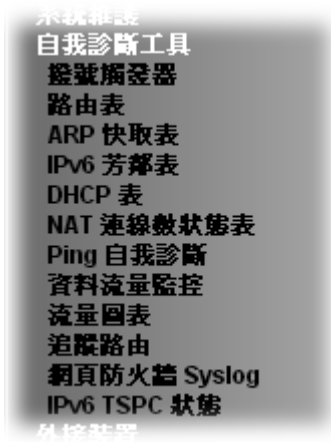
**附註:** 如果您想要使用郵件警示或Syslog，請設定 [SysLog/郵件警示設定](#) 頁面。  
 如果您變更了服務供應商，必須重新配置功能設定。

可用設定說明如下：

項目	說明
啓動經由介面	選擇任何一種介面用以啓動網頁內容過濾器。  <div style="border: 1px solid gray; padding: 5px; width: fit-content; margin: 0 auto;"> <p>啓動經由介面: 自動選取 ▾</p> <ul style="list-style-type: none"> <li>自動選取</li> <li>WAN 1</li> <li>WAN 2</li> <li>WAN 3</li> </ul> </div>
啓動	此連結可讓您登入 <a href="http://www.vigorpro.com">www.vigorpro.com</a> 完成帳號與路由器的啓動作業。
驗證訊息	至於網頁過濾器的驗證資訊，驗證過程會顯示在此框中供您參考。

## 4.20 自我診斷工具

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：



### 4.20.1 撥號觸發器

按自我診斷工具的撥號觸發器開啓網頁，網際網路連線(如 PPPoE)可由來源 IP 位址封包來觸發。

自我診斷工具 >> 撥號觸發

已觸發的撥出封包標頭

[更新頁面](#)

```
十六進制格式:  
00 00 00 00 00 00 00-00 00 00 00 00 00-00 00  
  
00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00  
00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00  
00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00  
00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00  
00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00  
  
已解碼格式:  
  
0.0.0.0 -> 0.0.0.0  
Pr O len 0 (0)
```

各個項目說明如下：

項目	說明
已解碼格式	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	按此鈕重新載入本頁。

## 4.20.2 路由表

按自我診斷工具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。

自我診斷工具 >> 檢視路由表

目前執行中的路由表	IPv6路由表	更新頁面
Key: C - connected, S - static, R - RIP, * - default, ~ - private		
C~ 192.168.1.0/ 255.255.255.0 directly connected LAN1		

自我診斷工具 >> 檢視路由表

目前執行中的路由表	IPv6路由表	更新頁面		
Destination	Interface	Flags	Metric	Next Hop
FE80::/64	LAN	U	256	
FF00::/8	LAN	U	256	

各個項目說明如下：

項目	說明
更新頁面	按此鈕重新載入本頁。



### 4.20.3 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。

自我診斷工具 >> 檢視 ARP 快取表

乙太網路 ARP 快取表 | [清除](#) | [更新頁面](#)

IP Address	MAC Address	Netbios Name	Interface
192.168.1.10	E0-CB-4E-DA-48-79	CARRIE-0C7CB251	LAN1

各個項目說明如下：

項目	說明
更新頁面	按此鈕重新載入本頁。
清除	按此連結清除整個表格。

### 4.20.4 IPv6 芳鄰表

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** 開啓如下頁面。

自我診斷工具 >> 檢視 IPv6 芳鄰表

IPv6 芳鄰表格 | [更新頁面](#)

IPv6 Address	Mac Address	Interface	State
FF02::1	33-33-00-00-00-01	LAN	CONN

各個項目說明如下：

項目	說明
更新頁面	按此鈕重新載入本頁。

## 4.20.5 DHCP 表

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**自我診斷工具**，選擇 **DHCP 表**開啓相關網頁。

自我診斷工具 >> 檢視 DHCP 指派的 IP 位址

DHCP IP 指派表		DHCPv6 IP 指派表			更新頁面
LAN1 : 192.168.1.1/255.255.255.0, DHCP server: On					
Index	IP Address	MAC Address	Leased Time	HOST ID	
1	192.168.1.10	E0-CB-4E-DA-48-79	23:50:00	carrie-0c7cb251	
2	192.168.1.1	00-1D-AA-AC-19-C8			

自我診斷工具 >> 檢視 DHCP 指派的 IP 位址

DHCP IP 指派表		DHCPv6 IP 指派表			更新頁面
DHCPv6 server binding client:					
Index	IPv6 Address	MAC Address	Leased Time		

各個項目說明如下：

項目	說明
Index	顯示連線項目編號。
IP Address	顯示路由器指派給特定電腦的 IP 位址。
MAC Address	顯示 DHCP 指派給特定電腦的 MAC 位址。
Leased Time	顯示指定電腦的租約時間。
HOST ID	顯示指定電腦的主機 ID 名稱。
更新頁面	按此鈕重新載入本頁。

## 4.20.6 NAT 連線數狀態表

按自我診斷工具，選擇 NAT 連線數狀態表開啓相關網頁。



各個項目說明如下：

項目	說明
<b>Private IP:Port</b>	本機電腦的 IP 位址和埠號。
<b>#Pseudo Port</b>	路由器爲了執行 NAT 所使用的暫時通訊埠。
<b>Peer IP:Port</b>	遠端主機的目標 IP 位址與埠號。
<b>Interface</b>	顯示 WAN 連線的介面。
<b>更新頁面</b>	按此鈕重新載入本頁。

## 4.20.7 Ping 自我診斷

按自我診斷工具，選擇 **Ping 自我診斷** 開啓相關網頁。

自我診斷工具 >> Ping 自我診斷

**Ping 自我診斷**

IPV4  IPV6

**附註：**如果您想要Ping一台LAN PC或是不想指定經由哪個WAN介面來執行Ping動作，請選擇“不指定”。

經由介面:

Ping 至:  IP 位址:

**執行結果** | 清除 |

自我診斷工具 >> Ping 自我診斷

**Ping 自我診斷**

IPV4  IPV6

Ping IPv6 位址:

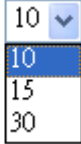
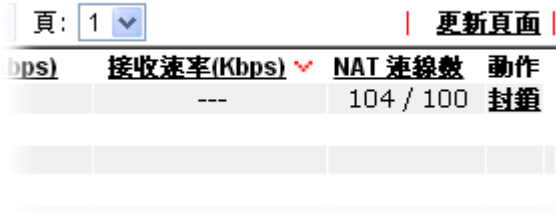
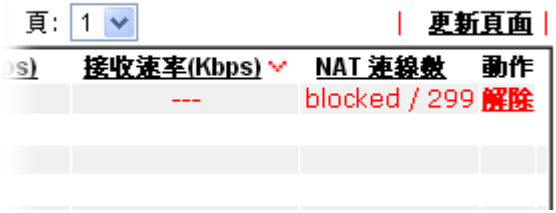
**執行結果** | 清除 |

各個項目說明如下：

項目	說明
<b>IPV4 /IPV6</b>	選擇其中一項以便顯示相應的資訊內容。
<b>經由介面</b>	選擇介面以執行此動作。
<b>Ping 至</b>	使用下拉式清單選擇您想要 Ping 的目標。 <div style="border: 1px solid black; padding: 2px; margin-top: 5px;"> <input type="text" value="不指定"/> <ul style="list-style-type: none"> <li><input checked="" type="text" value="不指定"/></li> <li>WAN1</li> <li>WAN2</li> <li>WAN3</li> </ul> </div>
<b>IP 位址</b>	輸入您想要 Ping 的主機/IP 上的 IP 位址。



各個項目說明如下：

項目	說明
啟用資料流量監控	勾選此方塊以啟動此功能。
更新秒數	<p>使用下拉式選項選擇系統自動更新資料的間隔時間。</p> <p>更新秒數: </p>
更新頁面	按此連結更新本頁。
索引編號	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 (kbps)	顯示被監視裝置的傳送速率。
接收速率 (kbps)	顯示被監視裝置的接收速率。
NAT 連線數	顯示您在連線數限制網頁中所設定的連線數。
動作	<p><b>封鎖</b> – 可以避免指定電腦在 5 分鐘內存取網際網路。</p> <p></p> <p><b>解除</b> – 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。</p> <p></p>
現值/高峰值/速度	<p><b>現值</b>表示目前 WAN1/WAN2 的傳輸速率與接收速率。</p> <p><b>高峰值</b>表示路由器在資料傳輸上所檢測到的最高數值。</p> <p><b>速度</b>表示 <b>WAN&gt;&gt;基本設定</b>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。</p>

## 4.20.9 流量圖表

按自我診斷工具，選擇**流量圖表**開啓相關網頁。可以選擇 **WAN1/WAN2/WAN3 頻寬**、**連線數**、**每日**、**每週**來檢視流量圖表。按下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。

自我診斷工具 >> 流量圖表



水準軸代表時間；而垂直軸代表的意義就很不同了。對 **WAN1 頻寬**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**來說，垂直軸代表的是過去一段時間之內的 NAT 連線數。

## 4.20.10 追蹤路由

按下**診斷工具**，選擇**追蹤路由**開啓相關網頁。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 位址並按下執行按鈕，整個路由狀況都將顯示在螢幕上。

自我診斷工具 >> 追蹤路由

**追蹤路由**

IPv4  IPv6

追蹤經由介面: 不指定

經由介面: ICMP

主機 / IP 位址:

執行

執行結果 | 清除 |

或是

自我診斷工具 >> 追蹤路由

**追蹤路由**

IPv4  IPv6

追蹤主機 / IP 位址:

執行

執行結果 | 清除 |

各個項目說明如下：

項目	說明
IPv4 / IPv6	選擇其中一項以便顯示相應的資訊內容。
經由介面	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 <b>不指定</b> 讓路由器自動決定選擇哪一種介面。
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。



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。

## 4.20.11 網頁防火牆 Syslog

本頁提供即時的 Syslog 並且在頁面上顯示相關資訊。


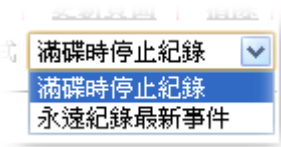
### 針對網頁 Syslog

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。

自我診斷工具 >> 網頁防火牆 Syslog

網頁 Syslog	USB 紀錄
<input type="checkbox"/> 啟用網頁 Syslog	
<a href="#">輸出</a>   <a href="#">更新頁面</a>   <a href="#">清除</a>	
Syslog 類型 <span>使用者</span> 顯示模式 <span>滿碟時停止紀錄</span>	
時間	訊息

可用項目說明如下：

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：  <p><b>滿碟時停止紀錄</b> – 當 syslog 的容量已滿，系統將停止紀錄。  <b>永遠紀錄最新事件</b> – 系統只紀錄最新的事件。</p>
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。

自我診斷工具 >> 網頁防火牆 Syslog

網頁 Syslog		USB 紀錄	
附註:儲存的Syslog 檔案若大於 1MB，Syslog 將會顯示出來。			
檔案夾: n/a	檔案: n/a	頁: n/a	紀錄類型: n/a
時間	紀錄類型	訊息	

可用項目說明如下：

項目	說明
時間	顯示事件發生的時間。
紀錄類型	顯示紀錄的類型。
訊息	.顯示事件發生的相關資訊。

## 4.20.12 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。

自我診斷工具 >> IPv6 TSPC 狀態

WAN1	WAN2	WAN3	更新頁面
TSPC 停用			

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：

自我診斷工具 >> IPv6 TSPC 狀態

WAN1	WAN2	WAN3	更新頁面
<b>TSPC Enabled</b> <b>TSPC Connection Status</b> Local Endpoint v4 Address : 114.44.54.220 Local Endpoint v6 Address : 2001:05c0:1400:000b:0000:0000:0000:10b9 Router DNS name : 888866666.broker.freenet6.net Remote Endpoint v4 Address : 81.171.72.11 Remote Endpoint v6 Address : 2001:05c0:1400:000b:0000:0000:0000:10b8 Tspc Prefix : 2001:05c0:1502:0d00:0000:0000:0000:0000 Tspc Prefixlen : 56 Tunnel Broker : amsterdam.freenet6.net Tunnel Status : <b>Connected</b>			

可用項目說明如下：

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。

## 4.21 外接裝置

Vigor 路由器可以用來連結不同類型的外接裝置，爲了方便管理這些外接裝置，請開啓 **外接裝置** 以便進行細部設定。

外接裝置

自動搜尋外接裝置

外接裝置已連接

以下顯示外接的可用裝置：

**爲了安全性的理由：**

如果您已改變外接裝置的管理者密碼，請按 **帳號** 按鈕重新輸入使用者名稱與密碼，否則路由器無法監督交換器，請按 **清除** 按鈕來清除斷線以及帳號資訊

確定

可用項目說明如下：

項目	說明
----	----

## 自動外接裝置搜尋

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。若有需要，您可以更改處在斷線狀態下的裝置名稱。

### 外接裝置

自動搜尋外接裝置

#### 外接裝置已連接

以下顯示外接的可用裝置：

**上線** Vigor2860 Series, 連線時間:00:00:18  
IP 位址:10.28.60.254

帳號

清除

#### 爲了安全性的理由：

如果您已改變外接裝置的管理者密碼，請按 **帳號** 按鈕重新輸入使用者名稱與密碼，否則路由器無法監督交換器，請按 **清除** 按鈕來清除斷線以及帳號資訊

確定

完成上述設定之後，按**確定**儲存設定。

**注意：**路由器透過此功能所偵測出來的裝置僅包含居易的產品。

# 5

## 疑難排解

這個章節將會指導您，如何解決在完成安裝和設置路由器後依然無法上網的問題。請按以下方法一步一步地進行檢查。

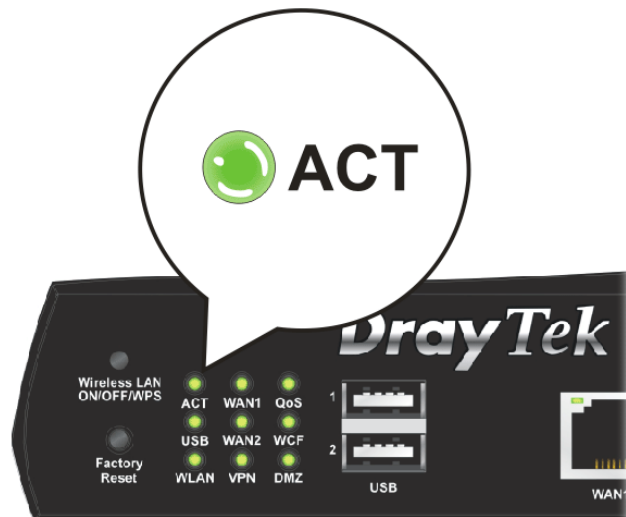
- 檢查路由器硬體狀態是否正常
- 檢查您電腦的網路連接設置是否正確
- 試試看能否從電腦 ping 到路由器
- 檢查 ISP 的設置是否正常
- 必要的話將路由器恢復至預設出廠設置

如果以上步驟仍無法解決您的問題，您需要聯絡代理商取得進一步的協助。

### 5.1 檢查路由器硬體狀態是否正常

按以下步驟檢查硬體狀態。

1. 檢查電源線以及 LAN 的連接。詳細資訊請參考“**1.3 硬體安裝**”。
2. 開啓路由器，確認 **ACT** 指示燈差不多每秒閃爍一次，以及相對應的 **LAN** 指示燈是否亮燈。



3. 如果沒有，意味著路由器的硬體有問題。那麼請回到“**1.3 硬體安裝**”，再重新執行一次硬體安裝，然後再試試。

## 5.2 檢查您電腦的網路連接設置是否正確

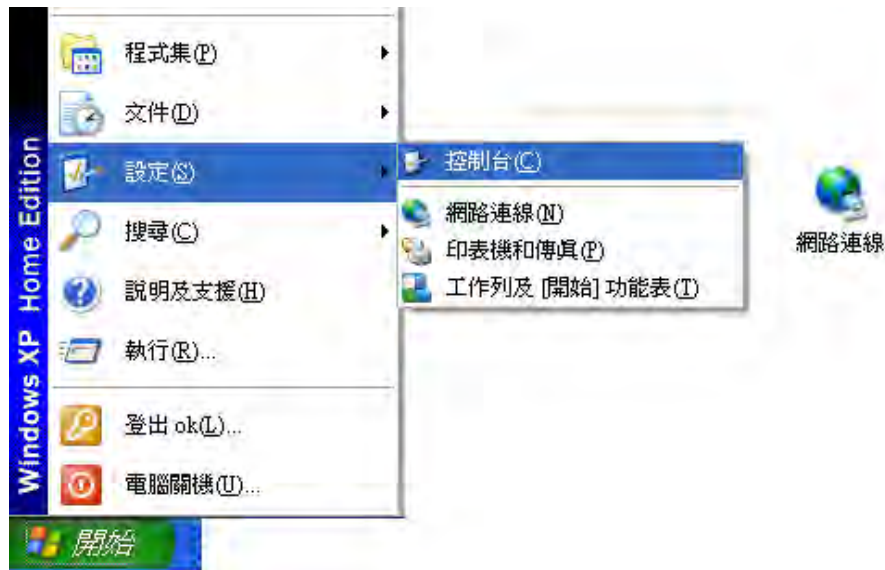
有些時候無法上網是因為網路連接設置錯誤所造成的，若在嘗試過上面的方法，依然無法連接成功，請按以下步驟確認網路連接是否正常。

### 對於 Windows 系統



下列的範例是以 Windows XP 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](http://www.draytek.com.tw) 查閱相關的技術文件說明。

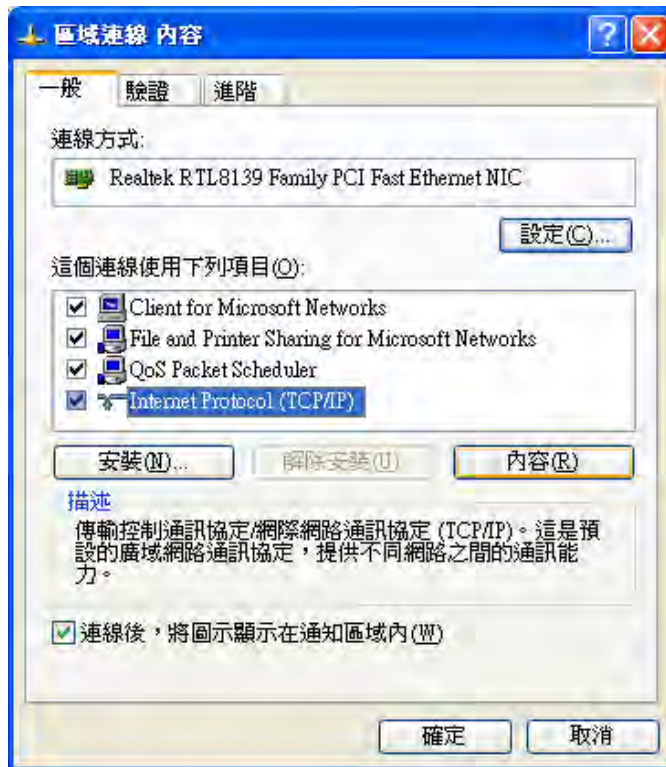
1. 至**控制臺**內，選擇**網路連線**並按滑鼠左鍵二下，進入網路連線畫面。



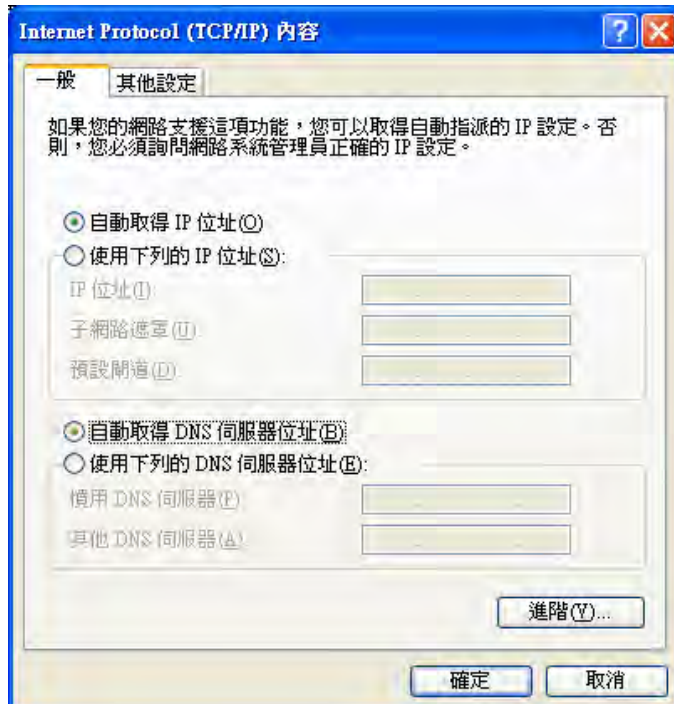
2. 擇**區域連線**按滑鼠右鍵，選擇內容。



3. 進入區域連線內容畫面後，選擇 **Internet Protocol (TCP/IP)**，按下內容鍵



4. 進入 **Internet Protocol (TCP/IP)**內容畫面後，選擇自動取得 IP 位址及自動取得 DNS 伺服器位址，按下**確定**鍵後完成設定



### 對於 Mac 系統

1. 在桌面上選擇目前所使用的 MacOS 磁碟機按滑鼠二下。
2. 選擇應用檔案夾中的網路檔案夾。

3. 進入網路畫面，在設定選項中，選擇使用 DHCP。



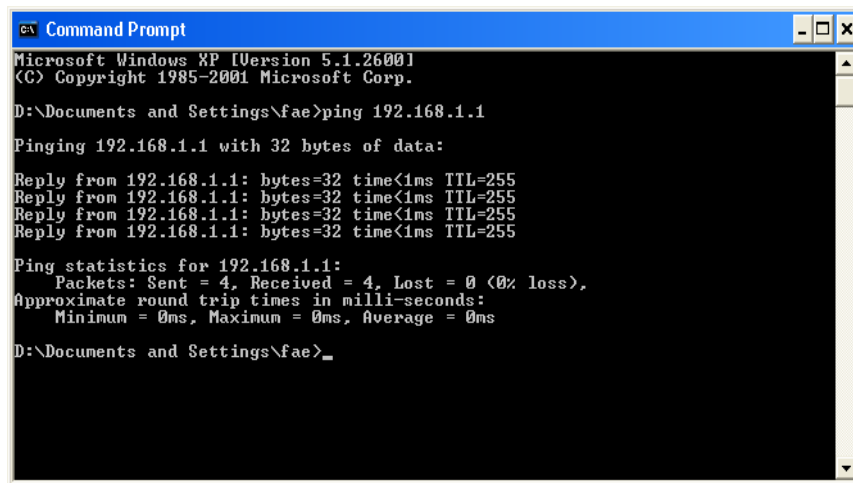


## 5.3 從電腦上 Ping 路由器

路由器的預設閘道為 192.168.1.1。因為某些理由，您可能需要使用 "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 5.2 檢查您個人電腦內的網路連線設定是否正確)，請依照以下的步驟正確地 ping 路由器。

### 對於 Windows 系統

1. 開啓命令提示字元視窗 (功能表選單開始>>執行)。
2. 輸入 **command** (適用於 Windows 95/98/ME) 或 **cmd** (適用於 Windows NT/2000/XP/Vista)。DOS 命令提示字元視窗將會出現。



```
ca Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
D:\Documents and Settings\fae>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
D:\Documents and Settings\fae>_
```

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“**64 bytes from 192.168.1.1: icmp\_seq=0 ttl=255 time=xxxx ms**”的訊息。

```

Terminal - bash - 80x24
Last login: Sat Jan  3 02:24:18 on ttys1
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$

```

## 5.4 檢查 ISP 的設置是否正常

開啟 **WAN>>網際網路連線** 頁面，檢查存取設定模式是否正確，按**細節設定**檢視先前所設定的內容。

**WAN >> 網際網路連線**

### 網際網路連線

索引編號	顯示名稱	實體連線模式	連線模式		
WAN1		乙太網路	固定或動態 IP	細節設定	IPv6
WAN2		乙太網路	無	細節設定	IPv6
WAN3		USB	無	細節設定	IPv6

注意：一次僅有一個 WAN 可以支援 IPv6。

## 5.5 3G 網路連線相關問題

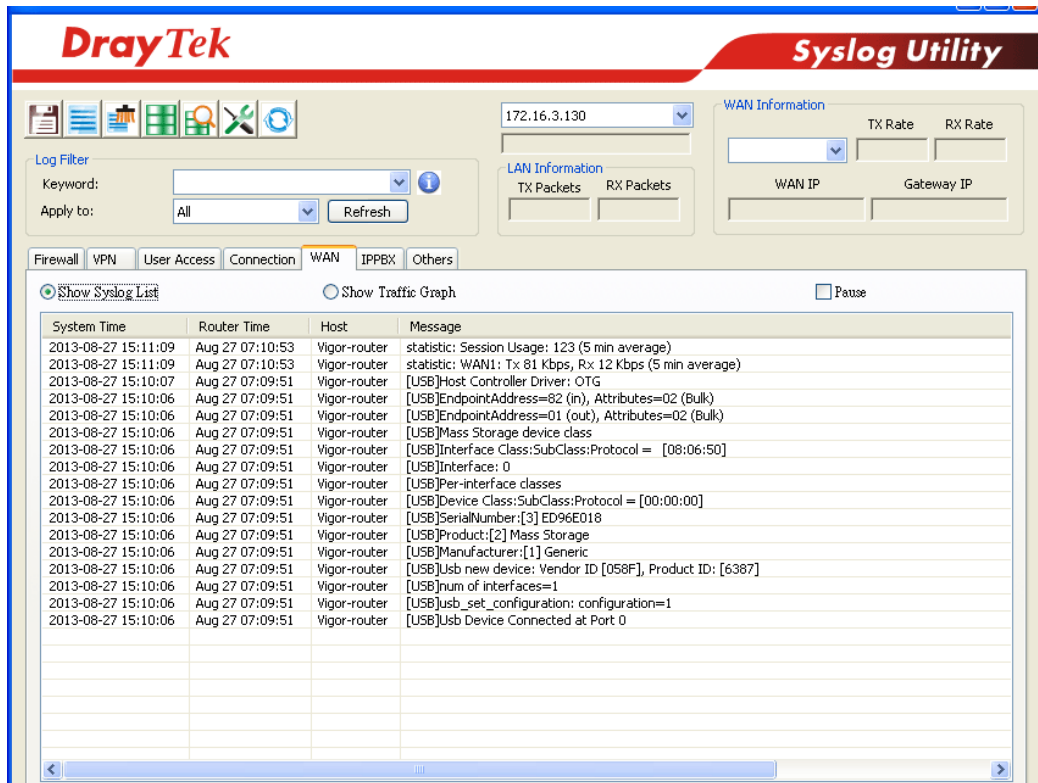
當您使用 3G 網路傳輸發現問題時，請先檢查下列各項：

### 檢查 USB LED 燈號

在插入 3G USB Modem 至 Vigor2925 後，您必須等待 15 秒左右，稍後 USB LED 會亮燈，表示 3G USB Modem 安裝成功。如果 USB LED 燈號未亮，請將 3G 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 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 USB Modem 來測試連線速度，檢查是否這個問題是 Vigor2925 所造成的，此外，請參考 3G 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 USB Modem，請放置在靠窗位置以取得較佳的接收信號。

## 5.6 還原路由器原廠預設組態

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



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

### 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**>>**重啓路由器**，可見下圖。選擇**使用原廠預設組態**，並按下**立即重啓**。幾秒鐘後，路由器就會恢復至出廠預設設定。

### 重啟路由器

您想重新啟動路由器嗎？

- 使用目前組態
- 使用原廠預設組態

立即重啟

### 自動重啟時間排程

索引號碼(1-15)於 **排程** 設定: , , ,

附註: 將忽略動作與閒置逾時設定

確定

取消

## 硬體重新設定

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



恢復至出廠預設值後，您就可以按個人需要，重新設定路由器。

## 5.7 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](mailto:support@draytek.com.tw)。