DrayTek

Vigor2920 系列

雙WAN安全防護路由器

Your reliable networking solutions partner

使 用 手 冊

V1.0

Vigor2920 系列
雙 WAN 安全防護路由器
使用手冊

版本: 1.0

韌體版本:V3.3.3.1

日期: 26/07/2010

版權資訊

版權聲明

商標

本手冊內容使用以下商標:

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

安全說明和保障

安全說明

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

保固

自使用者購買日起二年內爲保固期限，請將您的購買收據保存二年，因爲它可以證明您的購買日期。當本產品發生故障乃導因於製作及(或)零件上的錯誤，只要使用者在保固期間內出示購買證明，居易科技將採取可使產品恢復正常之修理或更換有瑕疵的產品(或零件)，且不收取任何費用。居易科技可自行決定使用全新的或是同等價值且功能相當的再製產品。

下列狀況不在本產品的保固範圍內：(1)若產品遭修改、錯誤(不當)使用、不可抗力之外力損害，或不正常的使用，而發生的故障；(2) 隨附軟體或是其他供應商提供的授權軟體；(3) 未嚴重影響產品堪用性的瑕疵。

成爲一個註冊用戶

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

韌體及工具的更新

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

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: Vigor2920 系列路由器

DrayTek 公司聲明 VigorPro 2920 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。

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幹擾合法通信；經發現有幹擾現象時，應立即停用，並改善至無幹擾時方得繼續使用。

法規資訊

聯邦通信委員會幹擾聲明

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。這些限制是爲居住環境不受有害的幹擾，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幹擾。然而，我們並不保證在特殊安裝下，不會產生幹擾。如果此產品確實對無線電或電視接受造成了有害的幹擾（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幹擾：

- 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幹擾，並且

(2) 此產品可能會遭受其他接收到的幹擾，包括那些可能造成不良運作的幹擾。

請造訪 http://www.DrayTek.com/user/AboutRegulatory.php

本產品針對 2.4 GHz 無線網路而設計，適用範圍遍及歐洲共同體及瑞士，法國地區則有部分的限制。

目錄

1 前言

Vigor2920 系列爲寬頻路由器，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，Vigor2920 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，Vigor2920 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。

Vigor2920 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。

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：

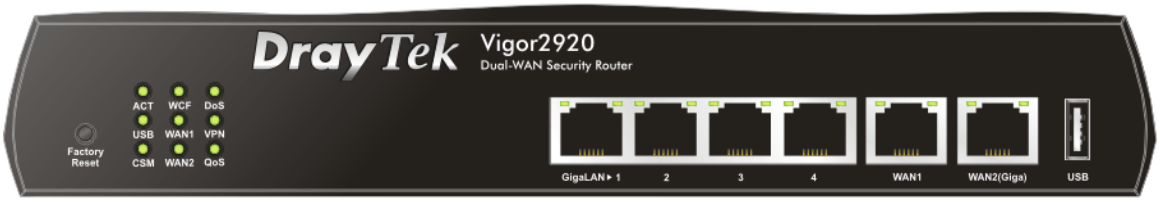
確定	儲存並套用目前的設定。
取消	取消目前設定並回復先前的設定值。
清除	捨棄目前設定值並允許使用者重新輸入。
新增	指定項目新增設定。
編輯	編輯選定項目的設定。
刪除	刪除選定項目及相關設定。

附註:有關網頁上所出現的其他按鈕，請參考第四章。

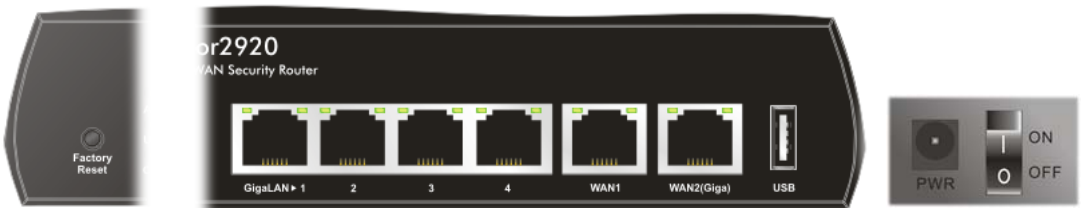
1.2 LED 指示燈與介面說明

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 Vigor2920

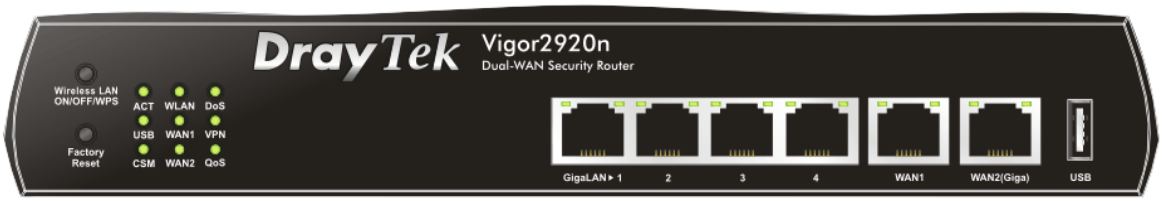


LED		狀態	說明
ACT (活動)		閃爍	路由器已開機並可正常運作。
		暗	路由器已關機。
USB		亮	USB 裝置已連接並運作中。
		閃爍	正在傳輸資料中。
CSM		亮	關於 IM/P2P、URL/網頁內容過濾器的 CSM (數位內容安全設定)之設定檔，啓動機制在**防火牆>>基本設定**中，(此類設定檔的建立必須在**數位內容安全設定**功能表單下。)
WCF		亮	網頁內容過濾器已啓動(此功能是在**防火牆>>基本設定**中所驅動)。
WAN1/2		亮	WAN1 或 WAN2 介面已連接。
		閃爍	資料封包傳輸中。
DoS		亮	DoS/DDoS 功能已啓動。
		閃爍	檢測到正受到外部攻擊。
VPN		亮	VPN 通道已建立。
QoS		亮	QoS 功能已開啓。
連介面上的燈號			
WAN 1	左 LED (綠)	亮	介面網路已連接。
		暗	介面網路未連接。
		閃爍	正在傳輸資料中。
	右 LED (綠)	亮	介面的連接速度爲 1000Mbps。
		暗	介面的連接速度爲 100Mbps。
WAN 2 (Giga)	左 LED (綠)	亮	介面網路已連接。
		暗	介面網路未連接。
		閃爍	正在傳輸資料中。
	右 LED (綠)	亮	介面的連接速度爲 1000Mbps。
		暗	介面的連接速度爲 100Mbps。
GigaLAN 1/2/3/4	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	介面的連接速度爲 1000Mbps。
		暗	介面的連接速度爲 100Mbps。

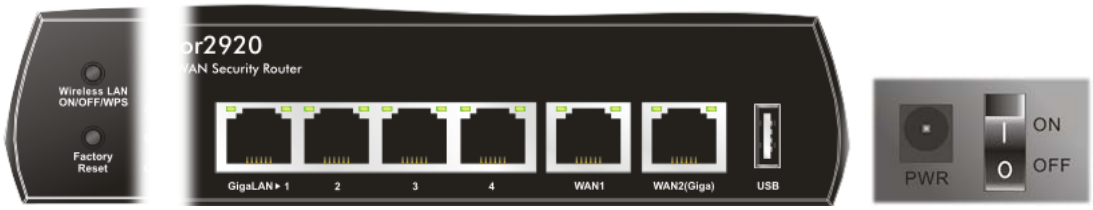


介面	說明
Factory Reset	還原成出廠預設值。 用法：當路由器正在運作時（ACT LED 燈號閃爍），利用尖銳的物品（例如：原子筆）壓住 Factory Reset 超過 5 秒；當 ACT LED 燈號開始迅速閃爍時，鬆開此動作，路由器將會還原成出廠預設值。
GigaLAN (1-4)	連接到電腦或網路設備。
WAN1/WAN2(Giga)	連接到 ADSL 或是 Cable Modem 裝置。
USB	連接到 USB 3G Modem 或是印表機。
PWR	連接電源變壓器。
ON/OFF	電源開關，“1” 爲開，“0” 爲關。

1.2.2 Vigor2920n



LED		狀態	說明
ACT (活動)		閃爍	路由器已開機並可正常運作。
		暗	路由器已關機。
USB		亮	USB 裝置已連接並運作中。
		閃爍	正在傳輸資料中。
CSM		亮	關於 IM/P2P、URL/網頁內容過濾器的 CSM (數位內容安全設定)之設定檔，啓動機制在**防火牆 >>基本設定**中，(此類設定檔的建立必須在**數位內容安全設定**功能表單下。)
WLAN		亮	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，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)。
WAN1/2		亮	WAN1 或 WAN2 連線預備妥當可以使用。
		閃爍	正在傳輸資料中。
DoS		亮	DoS/DDoS 功能已啓動。
		閃爍	刪除攻擊的檔案中。
VPN		亮	VPN 通道已建立。
QoS		亮	QoS 功能已開啓。
連介面上的燈號			
WAN 1	左 LED (綠)	亮	介面網路已連接。
		暗	介面網路未連接。
		閃爍	正在傳輸資料中。
	右 LED (綠)	亮	介面的連接速度爲 1000Mbps。
		暗	介面的連接速度爲 100Mbps。
WAN 2 (Giga)	左 LED (綠)	亮	介面網路已連接。
		暗	介面網路未連接。
		閃爍	正在傳輸資料中。
	右 LED (綠)	亮	介面的連接速度爲 1000Mbps。
		暗	介面的連接速度爲 100Mbps。
GigaLAN 1/2/3/4	Left LED (Green)	亮	乙太網路已連接。
		暗	乙太網路未連接。
		閃爍	正在傳輸資料中。
	Right LED (Green)	亮	介面的連接速度爲 1000Mbps。
		暗	介面的連接速度爲 100Mbps。



Interface	Description
Wireless LAN ON/OFF/WPS	按此鈕一次，等待用戶裝置透過 WPS 執行網路連線，當燈號亮起時，即表示 WPS 連線成功。 按此鈕二次可啓動(WLAN LED 亮燈)或關閉(WLAN LED 暗燈)無線連線功能。
Factory Reset	還原成出廠預設值。 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。
GigaLAN (1-4)	連接到電腦或網路設備。
WAN1/WAN2(Giga)	連接到 ADSL 或是 Cable Modem 裝置。
USB	連接到 USB 3G Modem 或是印表機。
PWR	連接電源變壓器。
ON/OFF	電源開關。

1.2.3 Vigor2920Vn

LED		狀態	說明
ACT (活動)		閃爍	路由器已開機並可正常運作。
		暗	路由器已關機。
USB		亮	USB 裝置已連接並運作中。
		閃爍	正在傳輸資料中。
CSM		亮	關於 IM/P2P、URL/網頁內容過濾器的 CSM (數位內容安全設定)之設定檔，啓動機制在**防火牆>>基本設定**中，(此類設定檔的建立必須在**數位內容安全設定**功能表單下。)
WLAN		亮	無線 AP 預備妥當可以使用。
		閃爍	資料傳送時，燈號成閃爍狀態。 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)。
WAN1/2		亮	WAN1 或 WAN2 介面已連接。
		閃爍	資料封包傳輸中。
Line		On	PSTN 電話撥進或撥出，當電話斷線時，LED 燈號即會熄滅。
		Off	目前沒有 PSTN 電話。
Phone 1/2		亮	連接本埠之電話使用中。
		暗	連接本埠之電話未被使用。
		閃爍	電話來電。
連介面上的燈號			
WAN 1/ WAN2 (Giga)	左 LED (綠)	亮	介面網路已連接。
		暗	介面網路未連接。
		閃爍	正在傳輸資料中。
	右 LED (綠)	亮	介面的連接速度爲 1000Mbps。
		暗	介面的連接速度爲 100Mbps。
GigaLAN 1/2/3/4	Left LED (Green)	亮	介面網路已連接。
		暗	介面網路未連接。
		閃爍	正在傳輸資料中。
	Right LED (Green)	亮	介面的連接速度爲 1000Mbps。
		暗	介面的連接速度爲 100Mbps。

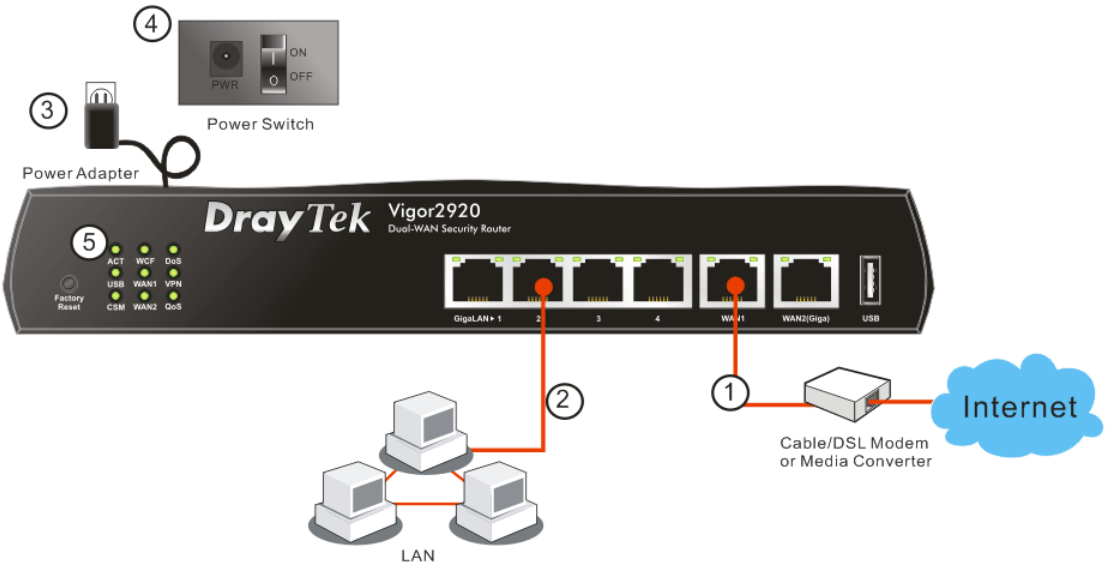
Interface	Description
Wireless LAN ON/OFF/WPS	按此鈕一次，等待用戶裝置透過 WPS 執行網路連線，當燈號亮起時，即表示 WPS 連線成功。 按此鈕二次可啓動(WLAN LED 亮燈)或關閉(WLAN LED 暗燈)無線連線功能。
Factory Reset	還原成出廠預設值。 使用方法：開啓路由器（ACT LED 閃動）。用圓珠筆按下小孔內的按鈕，然後維持 5 秒左右。當您發現 ACT LED 快速閃動時，請鬆開按鈕。路由器隨後將重新啓動，並回復出廠預設值。
Phone 1/2	連接類比電話機，以便使用 VoIP 通話功能。
Line	連接 PSTN life 線。
GigaLAN (1-4)	連接到電腦或網路設備。
WAN1/WAN2(Giga)	連接到 ADSL 或是 Cable Modem 裝置。
USB	連接到 USB 3G Modem 或是印表機。
PWR	連接電源變壓器。
ON/OFF	電源開關。

1.3 硬體安裝

設定路由器前，請先將裝置確實連接，並參考以下步驟操作。

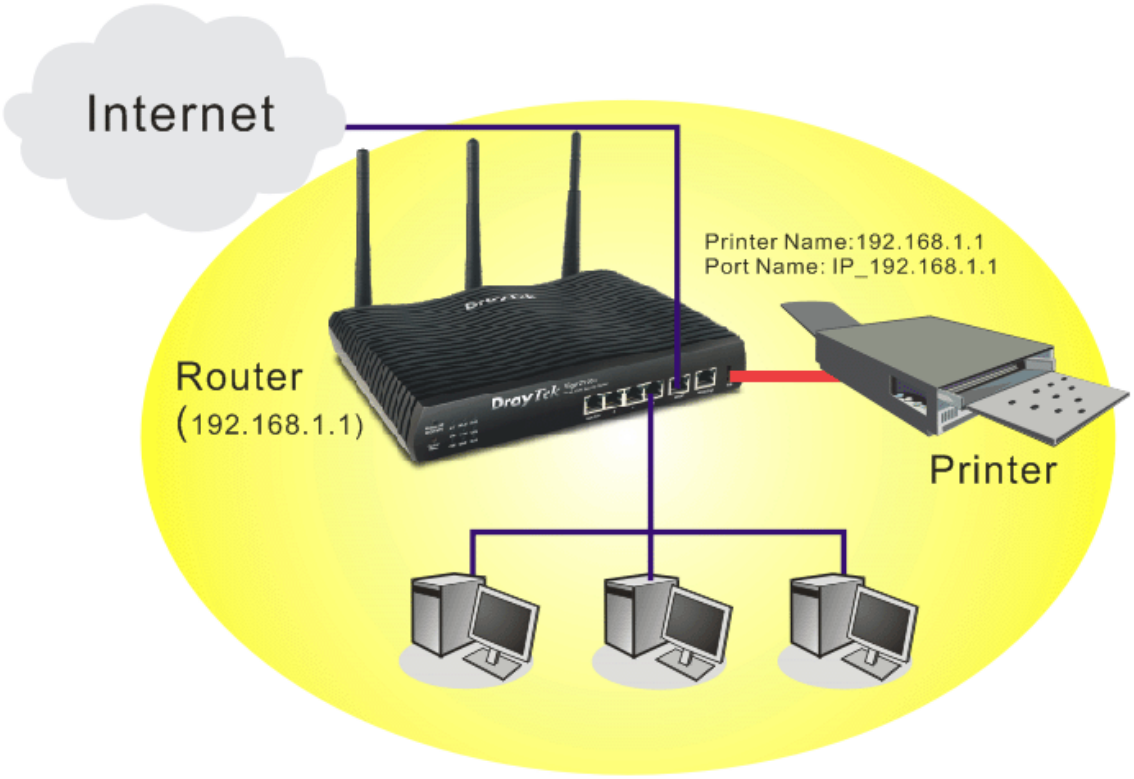
1. 利用乙太網路纜線(RJ-45)將數據機 / 路由器連接到本裝置的 WAN 連接埠。
2. 利用乙太網路纜線(RJ-45)一端連接 PC 的乙太網路連接埠，一端連接到路由器任何一個 **LAN** 連接埠。
3. 將電源線一端連接到路由器，另一端連接到牆上電源輸出孔。
4. 按路由器背後的電源開關。
5. 系統開始初始化，系統測試完畢後，**ACT** 燈號將會亮起，並持續閃爍。

(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，以下設定範例是以 Windows XP/2000 爲主，如果您使用的是 Windows 98/SE/Vista，請造訪居易網站 www.draytek.com 取得您所需要的安裝資訊。

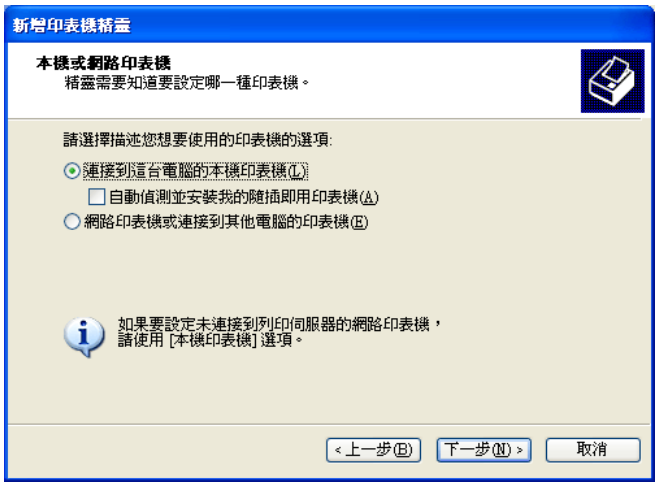


使用之前，請務必按照下列步驟來設定您的電腦（或無線用戶）：

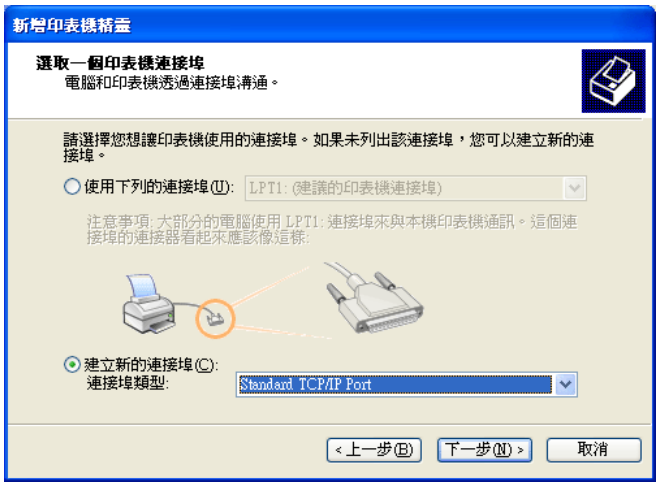
2. 請透過 USB 連接埠連接印表機與路由器。
3. 開啓**開始>>設定>>印表機和傳真**。

4. 開啓**檔案>>新增印表機**，設定精靈將會出現，請按**下一步**。

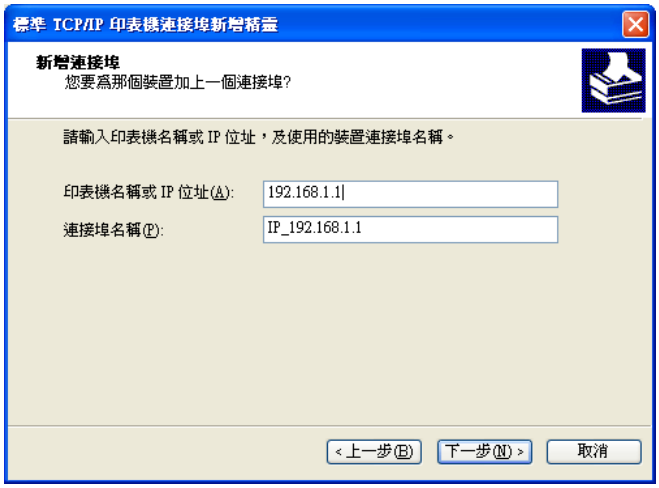
4. 選擇“**連接到這台....**”並按**下一步**。



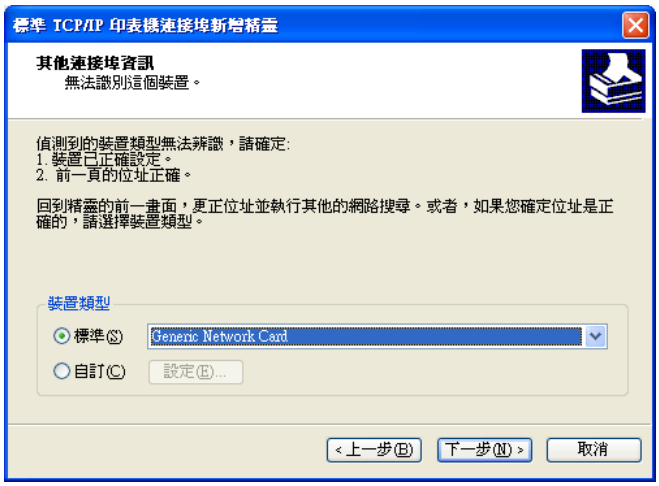
5. 接著請選擇“**建立新的連接埠**”，用下拉式選項選擇“**Standard TCP/IP Port**”， 按**下一步**。



6. 在下麵的對話方塊中，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**。

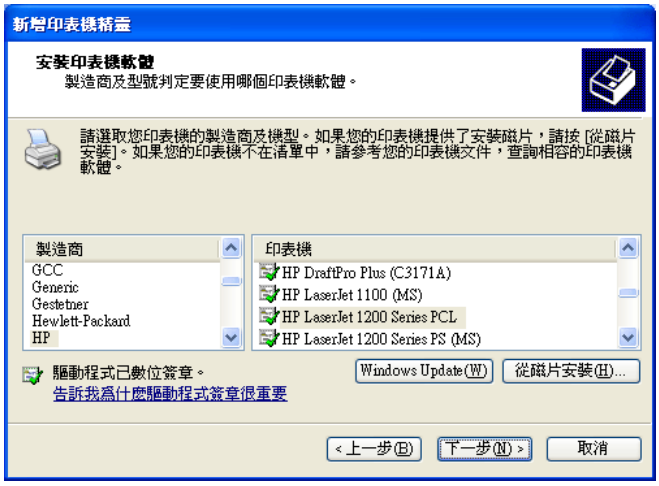


7. 請選擇**標準**，並自下拉式選項中選取 **Generic Network Card**。

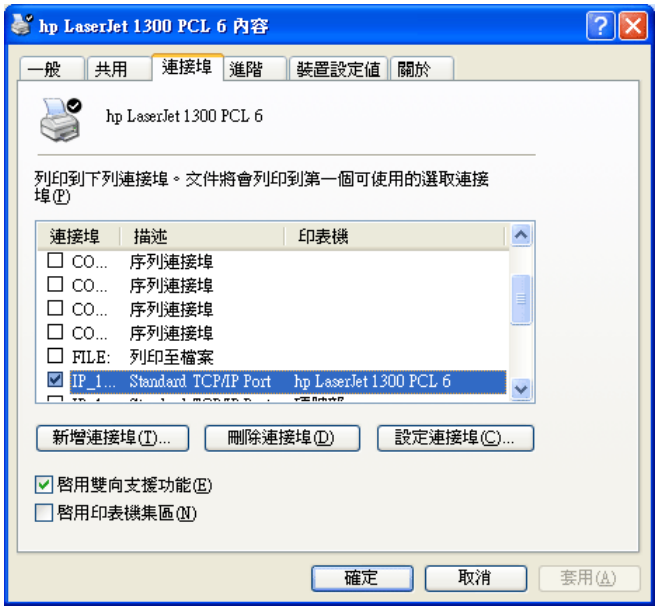


8. 當下列畫面出現時，請按**完成**。

9. 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**。



10. 最後請您回到**印表機和傳真**頁面，編輯您新增印表機的內容。



11. 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，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?** 連結，即可獲得您要的內容。

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。

本頁空白

2 基本設定

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

2.1 二層式管理

本章將會說明如何設定管理者/ 使用者之密碼，以及如何調整基本/進階設定以便成功存取網際網路。

2.2 進入設定網頁

1. 確保您的電腦已經和路由器正確的連接。

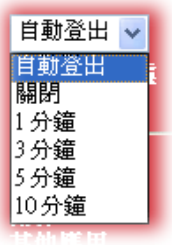
附註: 您可以選擇直接設定電腦的網路設定爲動態取得 IP 位址 (DHCP)，或者是將 IP 設定爲和 IP 分享器的預設 IP 位址 (**192.168.1.1**) 於同一個子網路。如需更多訊息，請參考後面的章節 – 疑難排解。

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. 以使用者模式操作者，請勿輸入任何資料，直接按下**登入**即可進行簡易的網路設定。不過，若要以管理者模式來操作，則請輸入“admin/admin”，再按下**登入**進入路由器網頁設定畫面。

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

4. 網頁將會依照您所選擇的條件開啓不同的頁面，預設值通常爲自動登出，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。



2.3 變更密碼

無論是使用者操作模式或是管理者操作模式，建議您將密碼先行變更。

1. 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。
2. 請輸入 “admin/admin”進入管理者模式，或將欄位元空白什麼都不要輸入，以進入使用者模式，然後按下**登入**進入網頁。
3. 現在，設定介面的主選單會出現。

管理者操作模式主畫面 (完整設定)

使用者操作模式主畫面 (簡易設定)

注意： 因爲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。

4. 進入**系統維護**頁面並選擇**系統管理員/使用者密碼**。

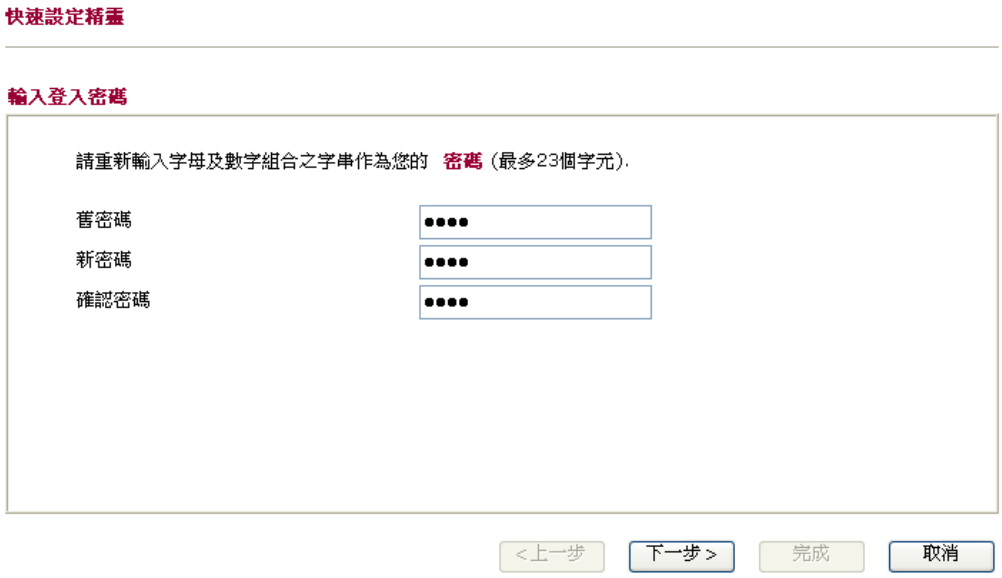
5. 輸入舊密碼 (預設值爲空白)。 在**新密碼**及**確認密碼**輸入您想要設定的密碼，然後按**確定**儲存設定。

6. 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。

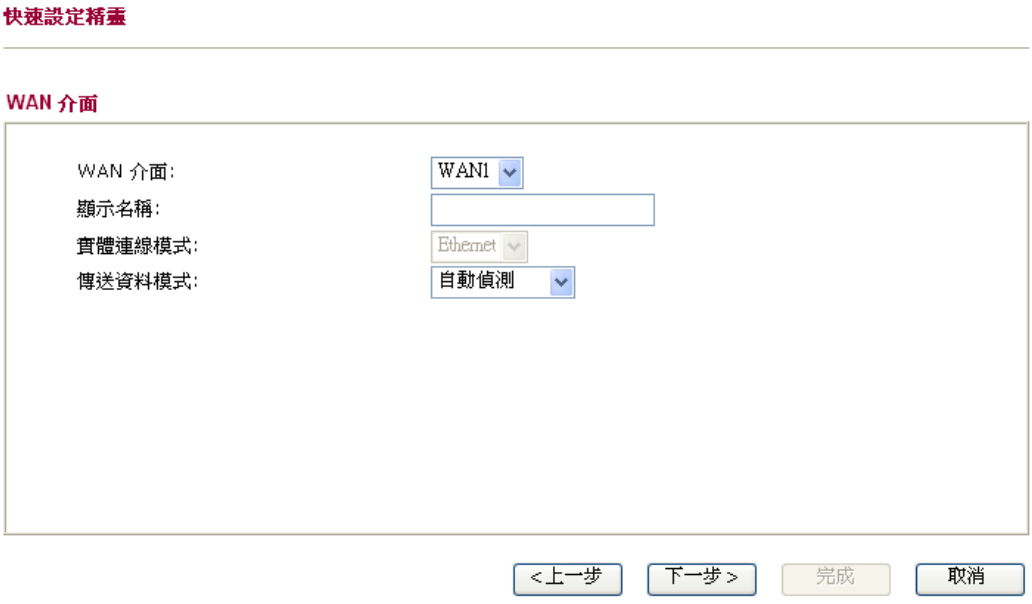
2.4 快速設定精靈

注意:快速安裝精靈在使用者模式中的操作與管理者模式下操作是相同的。

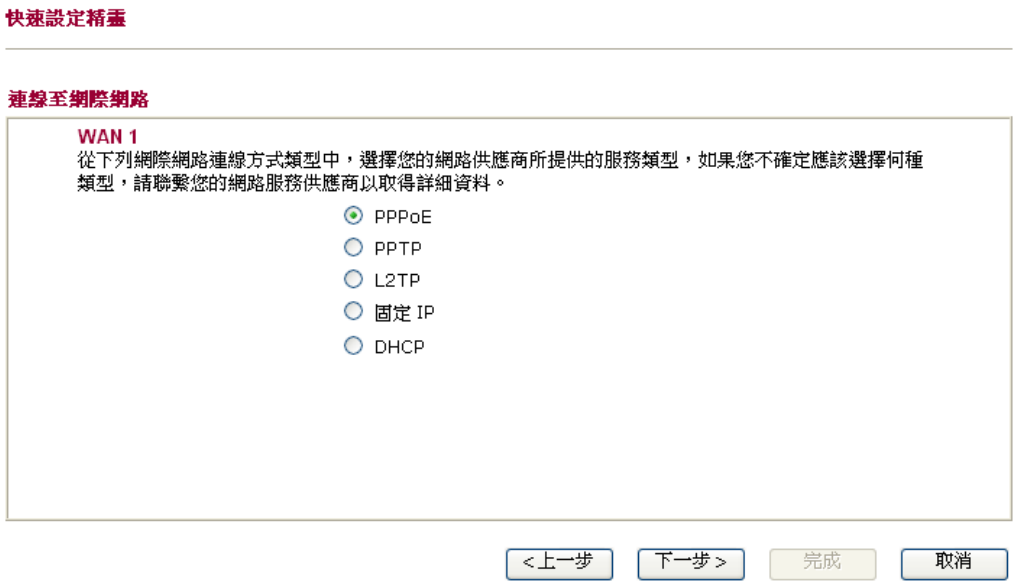
如果您打算佈建此路由器在現成的高速 NAT 網路結構中，您可以依照下列的步驟使用快速設定精靈設定您的路由器。快速設定精靈的第一個畫面會要求您輸入密碼，輸入密碼之後，請按**下一步**。



在下述頁面，請選擇使用的 WAN 介面，並選擇**自動偵測**作爲路由器的傳送資料模式，然後按**下一步**。



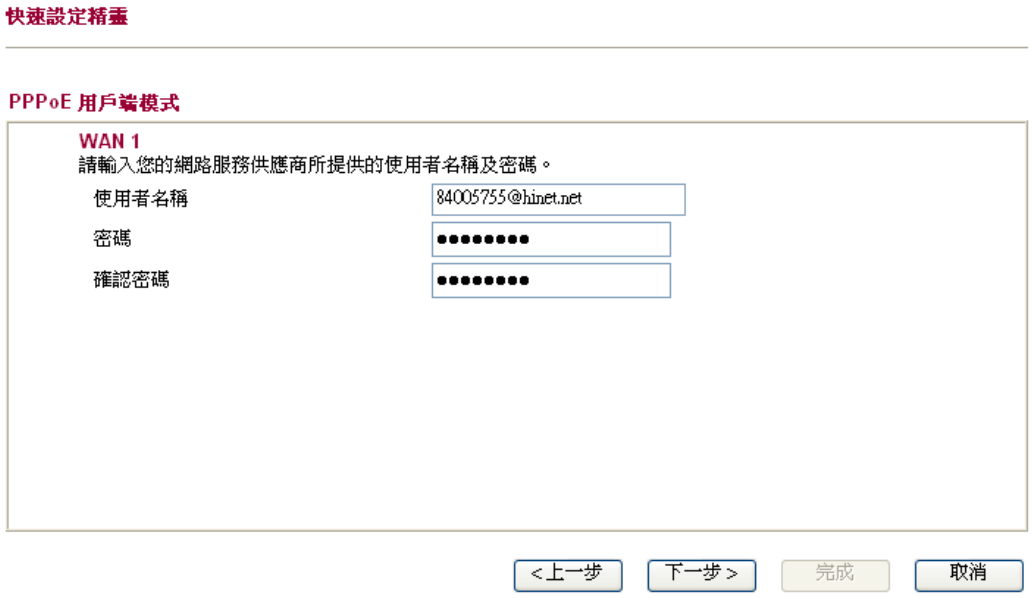
在下圖顯示中，請依照您的 ISP 提供的資料，選擇適當的網際網路連線類型，例如 ISP 提供您 PPPoE 介面的資訊，您就應該選擇 PPPoE 模式。接著按**下一步**進行。



2.4.1 PPPoE

PPPoE 爲 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。

如果您的 ISP 業者提供您 PPPoE 連線方式， 請先在視窗中選擇適當的模式，然後輸入相關資訊：

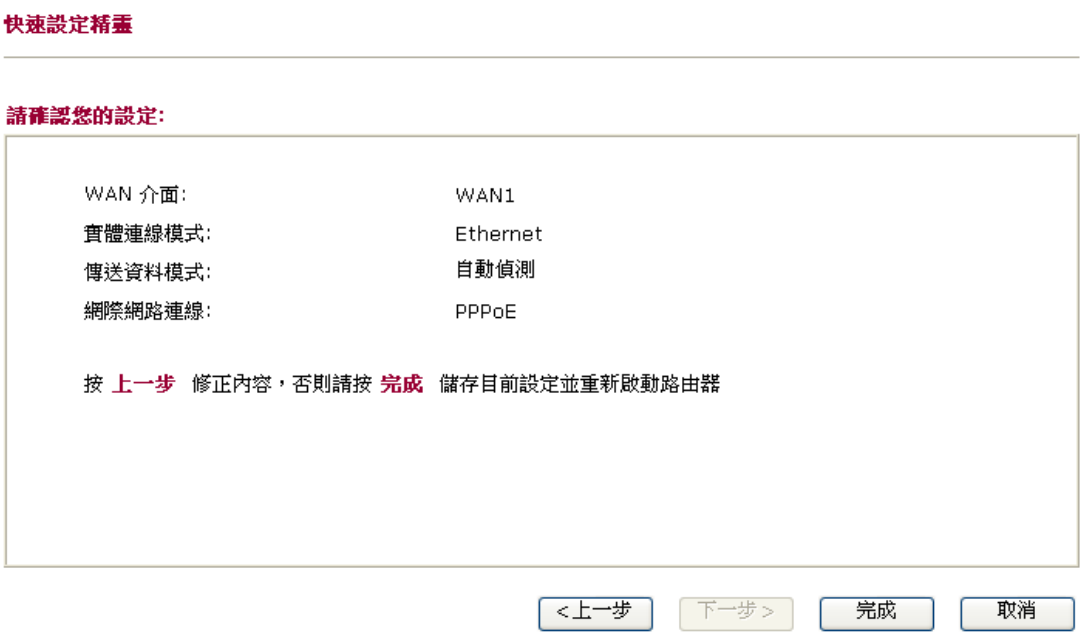


使用者名稱 指定 ISP 提供之有效使用者名稱。

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。

按**下一步**檢視此連線的設定狀態。

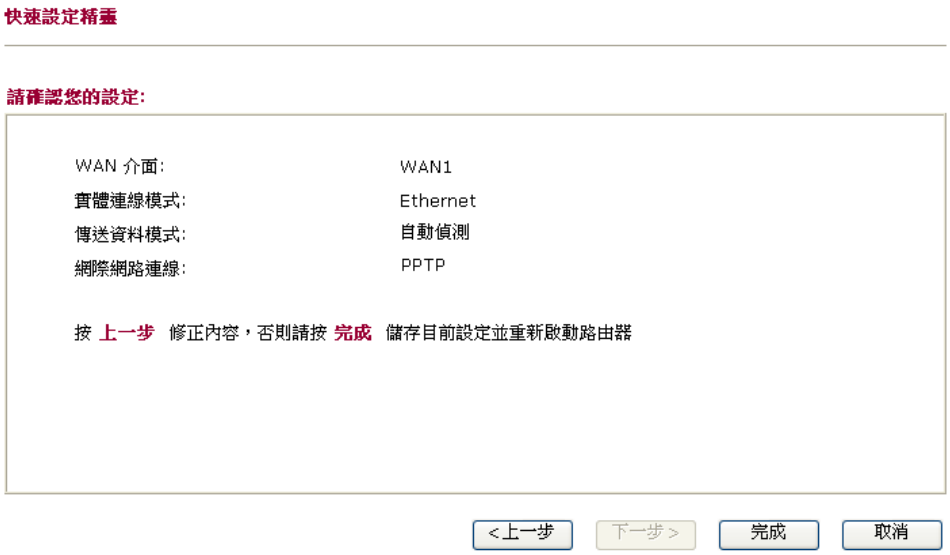


按**完成**，快速設定精靈安裝完畢將會出現。

2.4.2 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。一但 Tunnel 建立後，這種 DSL 數據機會將 PPP Session 送往 ISP。當 PPP Session 建立後，當地的使用者共用這個 PPP Session 存取 Internet。如果您需要使用 PPPTP 連線，請先在視窗中選擇適當的模式，然後輸入相關資訊：

按**下一步**檢視此連線的設定狀態。



按**完成**，快速設定精靈安裝完畢將會出現。

2.4.3 固定 IP

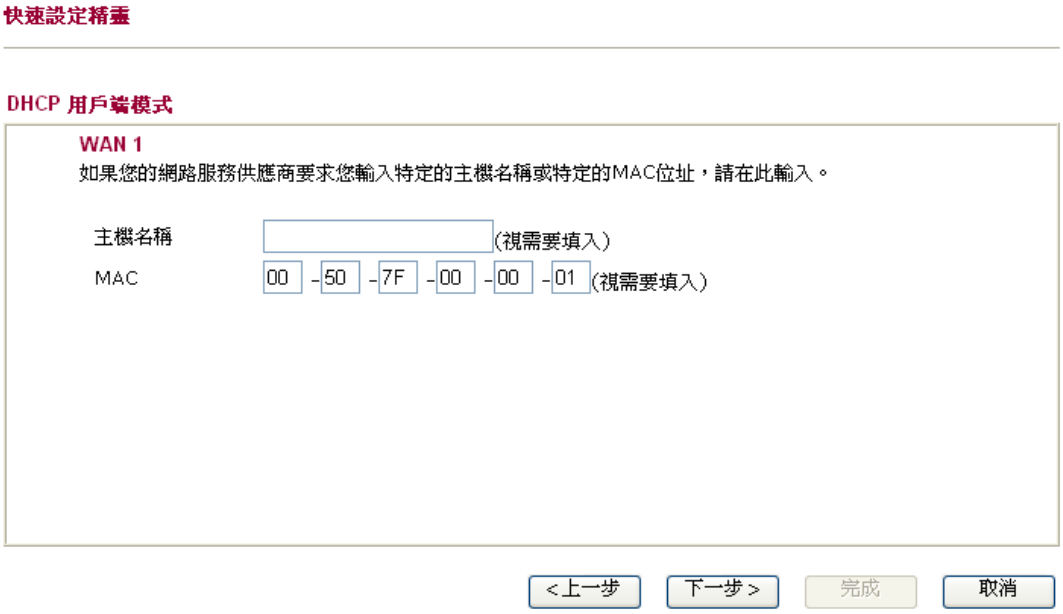
在這種應用當中，您會從 ISP 取得一個固定真實 IP 位址或一個真實子網路(多個公開 IP 位址)。通常纜線(Cable) ISP 會提供一個固定的真實 IP，而 DSL ISP 則有可能會提供一個真實子網路。如果您擁有一個真實子網路，您可以選擇一個或多個 IP 位址設定在 WAN 介面。如果您需要使用固定 IP / 動態 IP，請先在視窗中選擇適當的模式，然後輸入相關資訊：

設定輸入完畢之後，按**下一步**檢視此連線的設定狀態。

按**完成**，快速設定精靈安裝完畢將會出現。

2.4.4 DHCP

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



設定輸入完畢之後，按**下一步**檢視此連線的設定狀態。

按**完成**，快速設定精靈安裝完畢將會出現。

2.5 線上狀態

線上狀態顯示出系統目前執行的情形，WAN 連接狀況，ADSL 資訊和其他與路由器有關的訊息。如果您選擇 PPPoE 作爲通訊協定，您可發現頁面上出現一個 **Dial PPPoE** 或 **Drop PPPoE** 的按鈕。

詳細說明於後：

主要 DNS 顯示主要 DNS 的 IP 位址。

次要 DNS 顯示次要 DNS 的 IP 位址。

區域網路狀態

IP 位址 顯示區域網路介面的 IP 位址。

傳送封包 顯示在區域路中全部的傳送封包量。

接收封包 顯區域路中全部的接收封包量。

WAN 狀態

實體模式 顯示實體介面連線的狀態。

顯示名稱 顯示 WAN1/WAN 網頁上所顯示的名稱。

模式 顯示 WAN 連接(PPPoE)的類型。

連線時間 顯示介面上全部的上傳時間。

IP 顯示 WAN 介面的 IP 位址。

閘道 IP 顯示預設閘道的 IP 位址。

傳送封包 顯示 WAN 介面上全部傳送的封包數。

傳送速率 顯示 WAN 介面上全部傳送速率位元元數。

接收封包 顯示 WAN 介面上全部接收的封包數。

接收速率　　顯示 WAN 介面上全部接收速率位元元數。

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。

2.6 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，此爲系統提供的狀態通知。

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。

本頁空白

3 使用者操作模式

本章將導引使用者執行簡易的設定操作，有關其他的應用範例，可參考第 5 章。

1. 開啓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. **請勿**輸入任何文字，直接按**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爲何，本例中應該出現“使用者模式”。

3.1 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。

3.1.1 IP 網路的基本概念

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

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

什麼是真實 IP 位址和虛擬 IP 位址

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

取得 ISP 提供的真實 IP 位址

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

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

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 2910 新增了 3G 網路通訊功能。藉著連接 3G USB Modem 至 Vigor2920 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 Vigor2920n 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 Vigor2920n 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 及被視爲第二個 WAN 埠，雖然如此原本的乙太網路 WAN1 仍可作爲負載平衡之用，此外 3G USB Modem 也可被視爲備存裝置。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。

下圖爲 WAN 的功能項目：

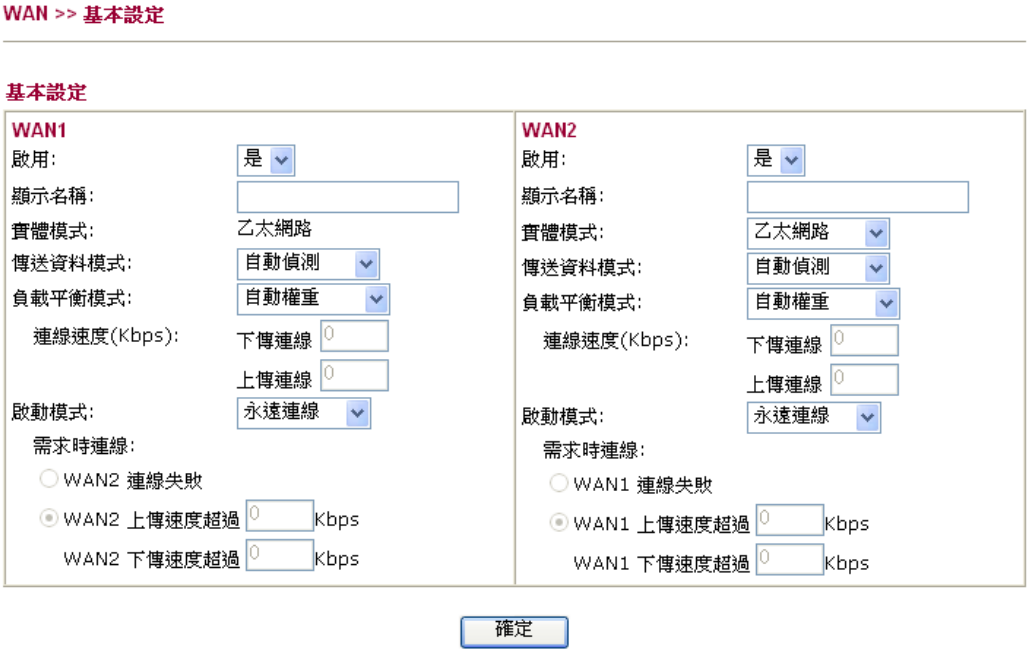
3.1.2 基本設定

本節介紹數種網際網路的一般設定，並詳細說明 WAN1 和 WAN2 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。

網頁允許您個別設定 WAN1 和 WAN2 的一般設定。

注意: WAN1 預設狀態是啓動的，而 WAN2 則是視情況選擇的項目。



啓用 選擇**是**啓動此 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。

實體模式 對 WAN1 而言，實體連線是透過 ADSL 連接埠來完成，不過 WAN2 的實體連接則是透過乙太網路/3G USB 模式來完成。

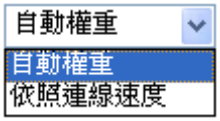
欲透過 3G USB 模式使用 3G 網路連線，選擇 **3G USB 模式**作爲 **WAN2** 的實體模式，接著開啓 **WAN>> 網際網路連線**. 在WAN2 上就可以看到 3G USB Modem 模式了，您可以使用 **PPP** 作爲**連線模式**再按下**細節設定**作進一步調整。

傳送資料模式

您可以改變 WAN2 的連線模式，或是選擇**自動偵測**讓系統自行處理。

負載平衡模式

如果您知道 WAN 介面的實際頻寬，請選擇**依照連線速度**。否則請選擇**自動權重**，讓路由器來完成最佳的平衡結果。



連線速度

如果您選擇**依照連線速度**作爲負載平衡模式，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。

啓動模式

選擇**永遠連線**讓 WAN 連接(WAN1/WAN2)能永遠啓動運作；或是選擇**需求時連線**，讓 WAN 連接在有需要時才連上線。

如果您選擇的是需求時連線，即可爲 PPPoE 和 PPTP 存取模式設定閒置逾時之時間，此外有三種選項供不同目的之需要來設定。

WAN2 連線失敗 – 表示 WAN1 在 WAN2 失敗時即自動連線。

WAN2 上傳速度超過 XX kbps – 表示當 WAN2 上傳速度超過指定數值 15 秒過後，WAN1 便自動連線。

WAN2 下傳速度超過 XX kbps – 表示當 WAN2 下載傳速度超過指定數值 15 秒過後，WAN1 便自動連線。

WAN1 連線失敗– 表示 WAN2 在 WAN1 失敗時即自動連線。

WAN1 上傳速度超過 XX kbps – 表示當 WAN1 上傳速度超過指定數值 15 秒過後，WAN2 便自動連線。

WAN1 下傳速度超過 XX kbps – 表示當 WAN1 下載傳速度超過指定數值 15 秒過後，WAN2 便自動連線。

3.1.3 網際網路連線控制

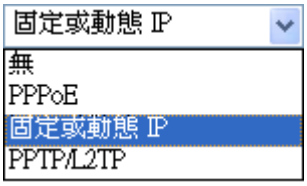
因爲路由器支援雙 WAN 口功能，使用者得以設定不同的 WAN 設定供網際網路存取之用，又因爲 WAN1 與 WAN2 的實體連線並不同，二者的連線模式也會有些差異。

索引　顯示路由器支援的 WAN 模式，WAN1 是預設的 WAN 介面，WAN2 爲 WAN1 無法運作時的選項介面。

顯示名稱　顯示 WAN1/WAN2 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（乙太網路）/ WAN2(乙太網路或 3G USB 模式) 實體連線。

網路連線模式　使用下拉式清單選擇適當的網際網路連線模式，接著按右邊的**細節設定**以設定詳細內容。



網頁提供三種網際網路連線模式。

細節設定　此按鈕將依照您在 WAN1 或 WAN2 所選擇的連線模式展現不同的網頁內容。

PPPoE 細節設定

如果想要使用 PPPoE 作爲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。

PPPoE 用戶端模式 按下**啓用**按鈕可啓動此功能，如果您選的是**停用**，此項功能將會關閉，全部調整過的設定也都將立即失效。

ISP 存取設定 輸入使用者名稱、密碼和驗證參數，按照 ISP 所提供給您的訊息。
使用者名稱 –在本區請輸入 ISP 提供的使用者名稱。
密碼 – 在本區請輸入 ISP 提供的密碼。
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**應用-排程**網頁中事先設定完畢，您可在此輸入該排程的索引編號。

WAN 連線檢測 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。
模式 – 選擇 **ARP Detect 或 Ping Detect** 執行 WAN 檢測動作。
Ping IP – 如果您選擇 **Ping Detect** 作爲檢測模式，您必須在本區輸入 IP 位址作爲 Ping 檢測之用。
TTL (Time to Live) – 顯示數值供您參考，TTL 數值是利用 Telnet 指令始可設定。

MTU 代表封包的最大傳輸單位，預設值爲 1442。

PPP/MP 設定 **PPP 驗證** – 選擇 **PAP** 或是 **PAP 或 CHAP**。如果您想要永遠連接網際網路，請勾選**永遠連線**。
閒置逾時 – 設定網際網路在經過一段沒有任何動作的時間後自動斷線的時間。

IP 位元址指派方式 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。

(IPCP)

您只要在固定 IP 位址欄位中輸入 IP 位址就可以達成上述的目的。詳情請聯絡您的 ISP 業者。

WAN IP 別名 - 如果您有數個真實 IP 位址且想要在 WAN 介面上使用，請使用此功能。除了目前使用的這一組之外，您還可以設定多達 8 組的真實 IP 位址。

固定 IP 位址 – 按**是**使用此功能並輸入一個固定的 IP 位址。

預設 MAC 位址 – 您可以使用預設 MAC 位址或是在此區域中填入另一組位址。

指定 MAC 位址 – 手動輸入路由器的 MAC 位址。

在您完成上述的設定之後，請按**確定**按鈕來啓動設定。

固定或動態 IP 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** 爲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。

固定或動態 IP (DHCP 用戶端)

按**啓用**以啓動此功能，如果您按的是**停用**，此功能將會關閉，您在此頁面所完成的全部設定都將失效。

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，因爲某些 ISP 會在一段時間沒有任何回應時中斷連線。請勾選**啓用 PING 以保持常態連線**。

PING 到指定的 IP – 如果您啓用此功能，請指定 IP 位址讓系統可以 PING 到該 IP 以保持連線

PING 間隔 - 輸入間隔時間讓系統得以執行 PING 動作。

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。

模式 – 選擇 **ARP Detect 或 Ping Detect** 執行 WAN 檢測動作。

Ping IP – 如果您選擇 **Ping Detect** 作爲檢測模式，您必須在本區輸入 IP 位址作爲 Ping 檢測之用。

TTL (Time to Live) – 顯示數值供您參考，TTL 數值是利用 Telnet 指令始可設定。

MTU

代表封包的最大傳輸單位，預設值爲 1442。

RIP 協定

指名路由器是如何變更路由表格資訊，勾選此項目以啓動此功能。

WAN IP 網路設定

這個區域允許您自動取得 IP 位址並讓您手動輸入 IP 位址。

WAN IP 別名 - 如果您有多個真實 IP 位址，想要在 WAN 介面上利用這些 IP，請使用 WAN IP 別名。除了目前使用的 IP 外，

您還可以另外設定 8 組真實 IP，要注意的是，本項設定僅針對 WAN1 有效用。

自動取得 IP 位址 – 如果您想要使用**動態 IP** 模式，按此鈕以自動取得 IP 位址。

路由器名稱: 輸入 ISP 的路由器名稱。

網功能變數名稱稱: 輸入指定的網功能變數名稱稱。

指定 IP 位址 – 按此鈕指定 IP 位址讓資料通過。

IP 位址:輸入 IP 位址。

子網路遮罩:輸入子網路遮罩。

閘道 IP 位址: 輸入閘道 IP 位址。

預設 MAC 位址: 按此鈕使用預設的 MAC 位址。

指定 MAC 位址: 部分 Cable 服務供應商會指定 MAC 位址作爲存取驗證之用，此時您需要按下此鈕並在下方區域輸入 MAC 位址。

DNS 伺服器 IP 位址 若要使用固定 IP 模式，請輸入路由器的主要 IP 位址，如有必要，在將來，您也可以輸入次要 IP 位址以符合所需。

PPTP/L2TP 細節設定

若要使用 **PPTP/L2TP** 爲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。

PPTP/L2TP 用戶端模式

啓用 PPTP - 選擇此鈕已啓用 PPTP 用戶端建立通往 WAN 介面的 DSL 數據機之通道。

啓用 L2TP - 選擇此鈕已啓用L2TP 用戶端建立通往WAN介面的 DSL 數據機之通道。

停用 - 選擇此鈕停用 PPTP 或 L2TP 連線通道。

伺服器位址 - 指定 PPTP/ L2TP 伺服器的 IP 位址。

指定閘道 IP 位址 - 針對 PTP/L2TP 伺服器指定閘道 IP 位址。

ISP 存取設定

使用者名稱 - 輸入 ISP 業者提供給您的使用者名稱。

密碼 - 輸入 ISP 業者提供的密碼。

MTU

代表封包的最大傳輸單位，預設值爲 1442。

PPP 設定

PPP 驗證 – 選擇 **PAP** 或是 **PAP 或 CHAP**。如果您想要永遠連接網際網路，請勾選**永遠連線**。

閒置逾時 – 設定網際網路在經過一段沒有任何動作的時間後自動斷線的時間。

IP 位元址指派方式 (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。

PPP 細節設定

如果要使用 **PPP** (針對 3G USB Modem) 做爲網際網路連線協定，請自 **WAN** 中選擇**網際網路連線**，接著在 WAN2 介面上選擇 **PPP**，即可出現下圖。

PPP 用戶端模式 選擇**啓用**以啓動此項模式。

SIM 卡 PIN 碼 輸入 SIM 卡 PIN 碼，以便連線網際網路。

數據機初始化字串 這個數值，用來初始化 USB 數據機，請使用預設值，如果您有任何疑問，請與當地 ISP 業者聯絡。

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 使用者名稱 輸入 PPP 使用者名稱 (視您實際需要而設定)。

PPP 密碼 輸入 PPP 密碼 (視您實際需要而設定)。

3.1.4 負載平衡原則

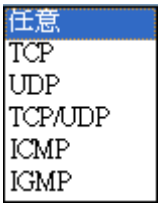
路由器支援負載平衡功能，可以將通訊協定之類型、指定主機的 IP 位址、主機子網路以及通訊埠範圍指派至 WAN1 或是 WAN2 介面。使用者可以指定流量的類型並基於此網頁之設定，強迫封包前往特定網路介面。本路由器支援 20 組的原則。

注意:負載平衡原則只在 WAN1 和 WAN2 都啓動的情形下才能執行。

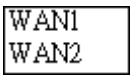
索引編號 按下任何一個索引號碼以進入負載平衡原則設定頁面。

啓用 勾選此方塊以啓用此原則。

通訊協定 使用下拉式功能以變更 WAN 介面的通訊協定。



WAN 使用下拉式功能以變更 WAN 介面。



來源 IP 起點 顯示來源 IP 起點的 IP 位址。

來源 IP 終點 顯示來源 IP 終點的 IP 位址。

目標 IP 起點 顯示目標 IP 起點的 IP 位址。

目標 IP 終點 顯示目標 IP 終點的 IP 位址。

目標通訊埠起點 顯示目標通訊埠起點的埠號。

目標通訊埠終點 顯示目標通訊埠終點的埠號。

上移/下移 使用**上移**或**下移**連結移動原則的先後順序。

按**索引編號 1** 進入下述頁面設定負載平衡原則。

啓用 勾選此方塊以啓動此原則。

通訊協定 使用下拉式選項選擇 WAN 介面適合的通訊協定。

綁定 WAN 介面 選擇一個 WAN 介面(WAN1 或 WAN2)作爲綁定介面。
自動備援到其他 WAN 網路 – 當選定的 WAN 介面出現問題時，若您有勾選此按鈕，即可將資料透過另一個 WAN 介面來傳輸。

來源 IP 起點 輸入指定 WAN 介面的來源 IP 起點位址。

來源 IP 終點 輸入指定 WAN 介面的來源 IP 終點位址。 如果本區空白，即表示區域網路中全部的來源 IP 位元址都可由此 WAN 介面通過。

目標 IP 起點 輸入指定 WAN 介面的目標 IP 起點位址。

目標 IP 終點 輸入指定 WAN 介面的目標 IP 終點位址。如果本區空白，即表示區域網路中全部的目標 IP 位元址都可由此 WAN 介面通過。

目標通訊埠起點 輸入目標通訊埠的起點埠號。

目標通訊埠終點 輸入目標通訊埠的終點埠號。如果本區空白，即表示區域網路中全部的目標通訊埠都可由此 WAN 介面通過。

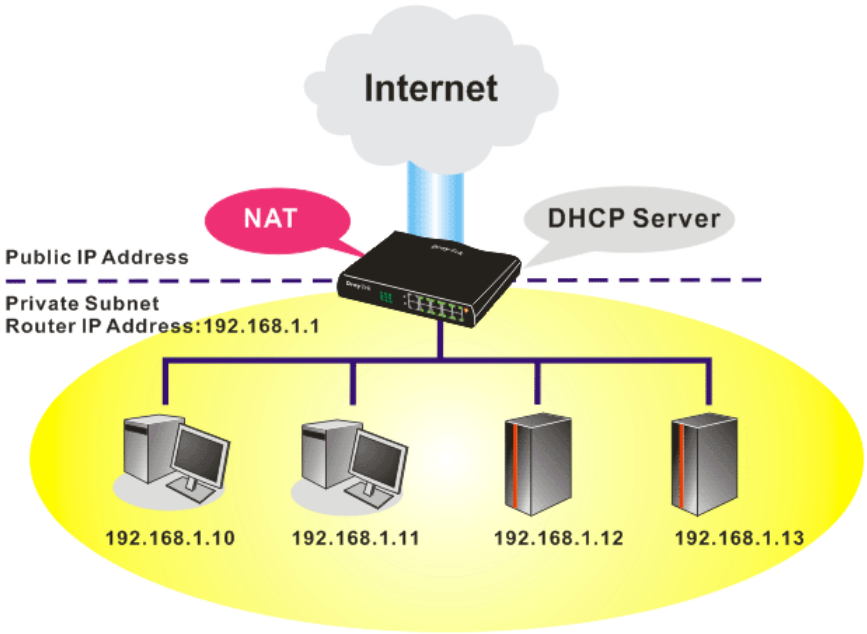
3.2 區域網路(LAN)

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。

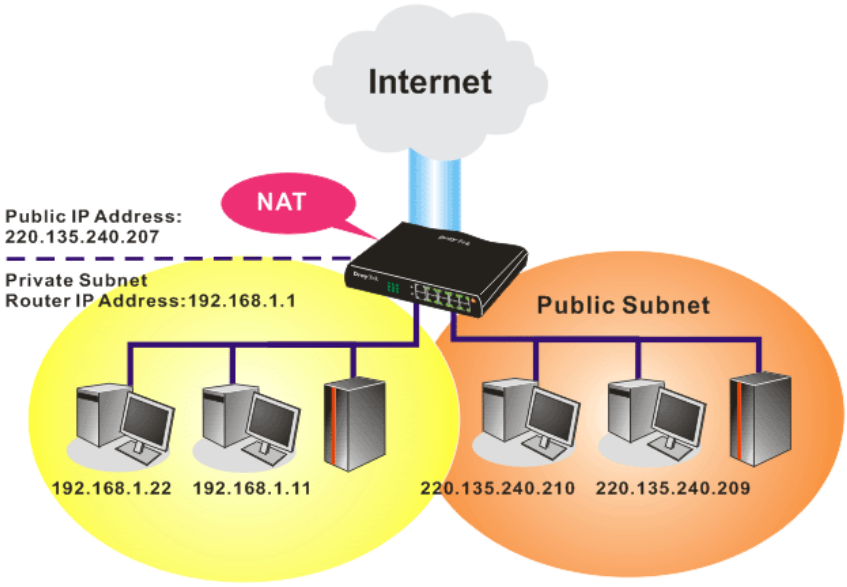
區域網路
基本設定

3.2.1 區域網路基本概念

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

3.2.2 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**。

第一 IP 位址 請輸入虛擬 IP 地址以便連接區域虛擬網路(預設值爲 192.168.1.1)。

第一子網路遮罩 請輸入決定網路大小的位址 (預設值爲 255.255.255.0/ 24)。

供 IP 路由使用 按下**啓用**以啓動此功能，此功能預設值是**停用**。此應用視情況需要而設定。

第二 IP 位址 請輸入第二組 IP 地址以便連接至子網路(預設值爲 192.168.2.1)。

第二子網路遮罩 請輸入第二組決定網路大小的位址碼(預設值爲 255.255.255.0/24)。

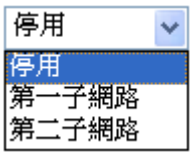
第二子網路遮罩 DHCP 伺服器 您可以將路由器設定爲 DHCP 伺服器，提供服務予第二組子網路。

起始 IP 位址：輸入 IP 位址 pool 數值做爲 DHCP 伺服器指定 IP 位址時的起始點，如果路由器的第二組 IP 位址爲 220.135.240.1,，起始 IP 位址可以是 220.135.240.2 或是更高一些，但比 220.135.240.254 小。

IP 配置數量：輸入 IP 地址的數量，最大值爲 10，例如您若輸入 3 而第二組 IP 地址爲 220.135.240.1，DHCP 伺服器的 IP 地址範圍即爲 220.135.240.2 到 220.135.240.4。

MAC 位址：請一個個輸入主機的 MAC 地址，按**新增**來建立主機清單以便指定、刪除或是編輯上述範圍中的 IP 地址。設定第二組 DHCP 伺服器所需的 MAC 位址清單，可幫助路由器指定正確的 IP 地址及子網路至正確的主機上。這樣在第二子網路上的主機便不會得到屬於第一組子網路的 IP 地址。

RIP 協定控制 **停用** – 關閉 RIP 協定，可讓不同路由器之間資訊交換暫停 (此爲預設值)。



第一子網路-選擇路由器以交換第一子網路和鄰近路由器間的 RIP 資訊。

第二子網路-選擇路由器以交換第二子網路和鄰近路由器間的 RIP 資訊。

DHCP 伺服器組態

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

如果您想要使用網路上另外的 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。

啓用 - 讓路由器指定 IP 地址到區域網路上的每個主機上。

停用 – 讓您手動指定 IP 地址到區域網路上的每個主機上。

DHCP 中繼代理位元址 - (第一子網路/第二子網路**)** 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。

起始 IP 位址 -輸入 DHCP 伺服器的 IP 位址配置的數值作爲指定 IP 位址的起始點，如果第路由器的第一個 IP 位址爲 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。

IP 配置數量 -輸入您想要 DHCP 伺服器指定 IP 地址的最大數量，預設值爲 50，最大值爲 253。

閘道 IP 位址 -輸入 DHCP 伺服器所需的閘道 IP 位址，這項數值通常與路由器的第一組 IP 位址相同，表示路由器爲預設的閘道。

中繼代理程式 IP 位元址 -設定您預備使用的 DHCP 伺服器 IP 位址，讓中繼代理可以協助傳送 DHCP 需求至伺服器上。

DNS 伺服器組態

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。

使用 DNS 手動設定 – 強迫路由器使用本頁所指定的 DNS 伺服器而非使用網際網路存取伺服器所提供的 DNS 伺服器 (PPPoE, PPTP, L2TP 或 DHCP 伺服器).

主要 IP 位址 -您必須在此指定 DNS 伺服器的 IP 位址，因爲通常您的 ISP 應該會提供一個以上的 DNS 伺服器，如果您的 ISP 並未提供，路由器會自動採用預設的 DNS 伺服器 IP 地址 194.109.6.66，放在此區域。

次要 IP 位址 - 您可以在此指定第二組 DNS 伺服器 IP 位址，因爲 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 位址爲 194.98.0.1，放在此區域。

預設 DNS 伺服器 IP 位址可在線上狀態上查看:

如果主要和次要 IP 地址區都是空白的，路由器將會指定其本身的 IP 位址給予本地使用者作爲 DNS 代理伺服器並且仍保有 DNS 快速緩衝貯存區。

如果網功能變數名稱稱的 IP 位址已經在 DNS 快速緩衝貯存區內，路由器將立即 resolve 網功能變數名稱稱。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。

第五章中舉出常見的區域網路設定腳本供您參考，有關設定範例部份，如有需求請參考該章以取得更多的訊息。

3.3 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，因此您必須爲此負擔費用，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爲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，成爲真實 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：

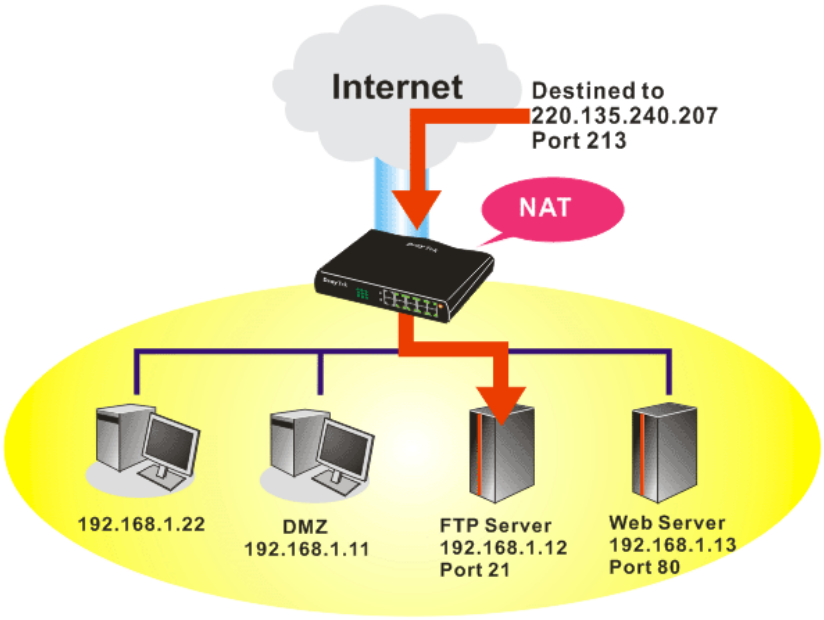
- **於應用真實 IP 位址上節省花費以及有效利用 IP 位址** NAT 允許本機中的 IP 位址轉成真實 IP 位址，如此一來您可以一個 IP 位址來代表本機。
- **利用隱匿的 IP 位址強化內部網路的安全性** 有很多種攻擊行動都是基於 IP 位址而對受害者發動的，既然駭客並不知曉任何虛擬 IP 位址，那麼 NAT 功能就可以保護內部網路不受此類攻擊。

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。

下圖爲 NAT 功能項目：

3.3.1 通訊埠重導向

通訊埠重導向通常是爲了本地區域網路中的網頁伺服器、FTP 伺服器、E-mail 伺服器等相關服務而設定，大部分的情形是您需要給每個伺服器一個真實 IP 位址，此一真實 IP 位址/網功能變數名稱稱可以爲所有使用者所辨識。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。

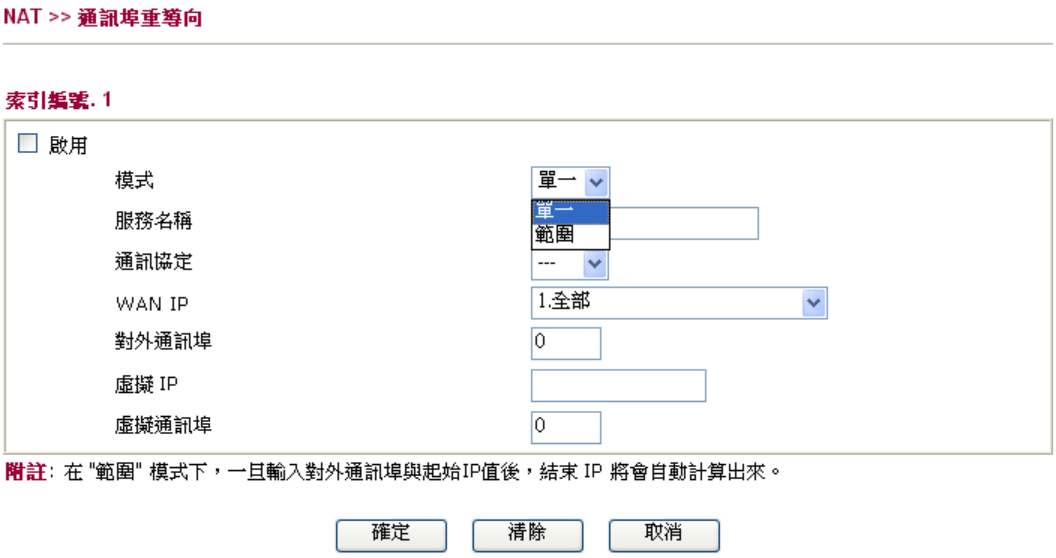
NAT >> 通訊埠重導向

通訊埠重導向 | 回復出廠預設值 |

索引編號	服務名稱	對外通訊埠	虛擬 IP	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 >>

請按索引編號下任一個連結開啓設定頁面。



啓用 勾選此方塊啓用通訊埠重導向設定。

模式 有二種模式可以供使用者選擇 - **單一**與**範圍**，如欲設定範圍給予指定服務，請選擇**範圍**。在"範圍" 模式下，若 IP 位元址與第一個對外通訊埠號皆填入之後，系統將自動計算並顯示第二個對外通訊埠值。

服務名稱 輸入特定網路服務的名稱。

通訊協定 選擇傳送層級的通訊協定(TCP 或 UDP)。

WAN 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**全部**，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**範圍**作爲重導向模式，您將會在此看見二個方塊，請在第一個方塊輸入需要的數值，系統將會自動指定數值予第二個方塊。

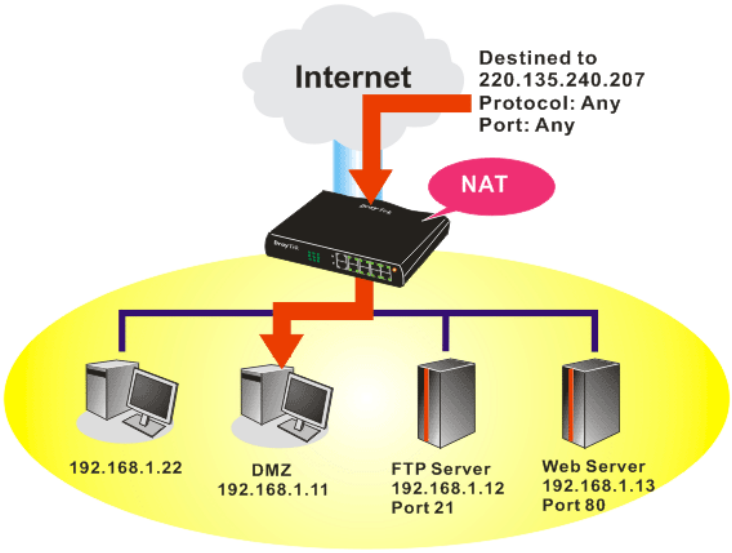
虛擬 IP 指定提供服務的主機之 IP 位址，如果您選擇**範圍**作爲重導向模式，您將會在此看見二個方塊，請在第一個方塊輸入完整的 IP 位址 (作爲起點)，在第二個方塊輸入四位數字(作爲終點)。

虛擬通訊埠 指定內部主機提供服務之虛擬通訊埠號

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

3.3.2 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：

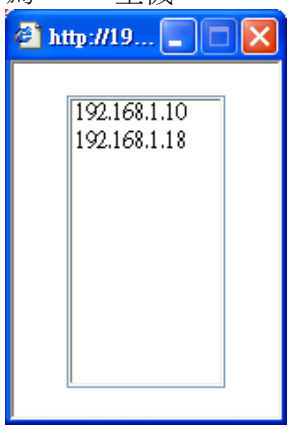
如果您在**網際網路連線設定**選擇 **PPPoE/固定 IP/PPTP**，並且設定 **WAN 別名**，您將可在此頁面發現**輔助 WAN IP** 項目。

開啓 勾選此項以啓動 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**選擇 PC** 開啓另一頁面來選擇。

選擇電腦 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 位址作爲 DMZ 主機。



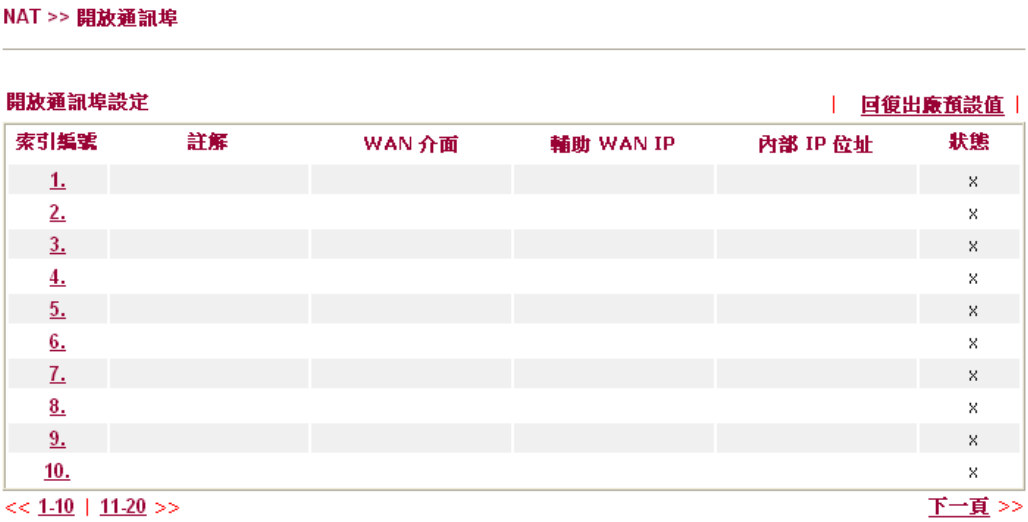
當您已經從上面的視窗選好了虛擬 IP 位址時，該 IP 位址將會顯示在下麵的螢幕上，請按**確定**儲存這些設定。

3.3.3 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。



索引編號 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。

WAN 介面 顯示此通訊埠經由介面。

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。

啓用開放通訊埠 勾選此項以啓動此功能。

說明 請爲所定義的網路應用/服務命名。

WAN 介面 指定該項設定之 WAN 介面。

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 位元址。

本機電腦 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。

3.4 其他應用

下圖顯示**應用**的功能項目：

3.4.1 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 可讓您指派一個網功能變數名稱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功能變數名稱稱，並利用網際網路存取路由器或是內部虛擬的伺服器資料。如果您的主機擁有網路伺服器、FTP 伺服器或是其他路由器後方提供的伺服器，這項設定就特別有幫助也有意義。

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

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功能變數名稱稱(例如 hostname.dyndns.org)，且獲得一個帳號，其使用者名稱爲 *test*；密碼爲: *test*。
2. 自**應用**群組選擇**動態 DNS** 設定，下述頁面即會出現在螢幕上。

回復出廠預設值 清除全部設定資料並回復到出廠的設定。

啓用動態 DNS 設定 勾選此方塊啓用此功能。

自動更新間隔 輸入動態 DNS 伺服器的自動更新的間隔時間。

索引編號 按下方的號碼連結進入 DDNS 設定頁面，以設定帳戶。

WAN 介面 顯示此設定所使用的 WAN 介面。

網功能變數名稱稱	顯示您在 DDNS 設定頁面上所設定的網功能變數名稱稱。
啓用	顯示此帳號目前是啓用或是停用狀態。
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。

3. 選擇索引號碼 1，爲您的路由器新增一個帳號。勾選**啓用動態 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)，並於網功能變數名稱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)。

啓用動態 DNS 帳號	勾選此方塊以啓用目前帳號，如果您勾選此方塊，您可在步驟 2 中的網頁上看到啓動欄位出現勾選標示。
WAN 介面	**選擇套用此設定的 WAN 介面。**
服務供應商	爲此 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**，您可以修正網功能變數名稱稱區域中所選定的網域資料。
網功能變數名稱稱	輸入您所申請的網功能變數名稱稱。請使用下拉式選項選擇想要使用的一個名稱。
登入名稱	輸入您在申請網功能變數名稱稱時所設定之登入名稱。
密碼	輸入您在申請網功能變數名稱稱時所設定之密碼。
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。

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。

萬用字元與**備份 MX** 並非所有的動態 DNS 服務商都有支援，有關此部分內容，請您自服務商的網站上取得更詳盡的資訊。

關閉此功能並清除全部動態 DNS 帳號

取消勾選**啓用動態 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

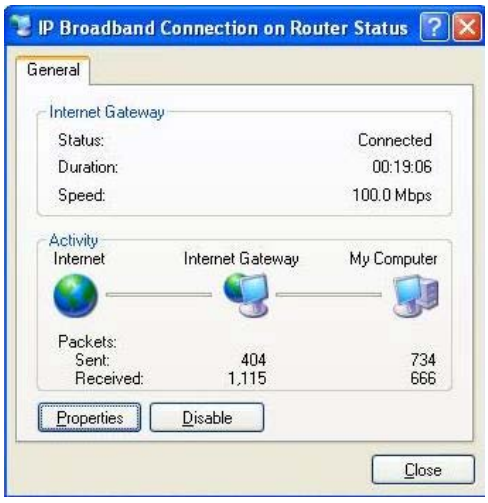
在**動態 DNS 設定**頁面上，請按您想要刪除之帳號的索引號碼，然後按**清除全部**按鈕即可刪除該帳號。

3.4.2 UPnP

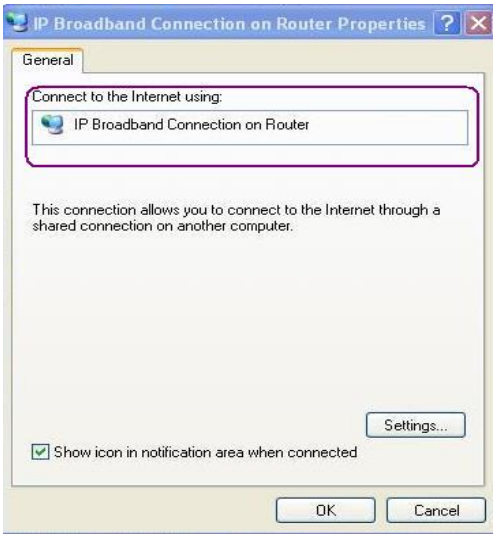
UPnP 協定爲網路連線裝置提供一個簡易安裝和設定介面，爲 Windows 隨插即用系統上的電腦週邊設備提供一個直接連線的方式。使用者不需要手動設定**通訊埠對應**或是 **DMZ**，**UPnP** 只在 Windows XP 系統下可以運作，路由器提供相關的支援服務給 MSN Messenger，允許完整使用聲音、影像和訊息特徵。

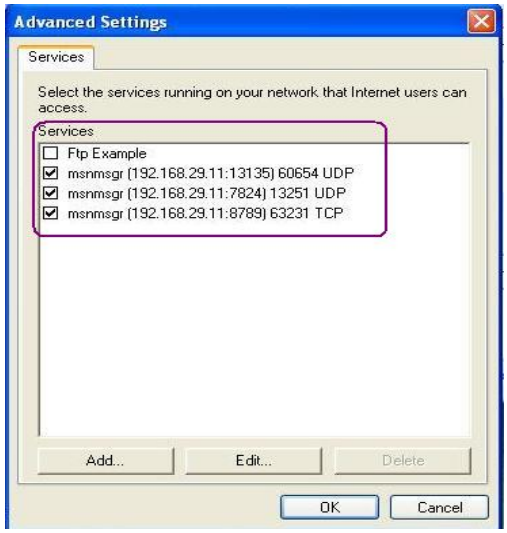
啓用 UPnP 服務　　您可以視情況勾選**啓用連線控制服務**或是**啓用連線狀態服務**。

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，這是因爲這些應用程式會擋掉某些網路通訊埠的存取能力。

安全考量

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

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

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

3.5 VoIP

注意:此功能僅適用“V”機型。

Voice over IP network (VoIP)可讓您使用寬頻網際網路連線撥打網路電話。

有很多種不同的電話信號協定、方法可讓 VoIP 裝置使用以便與對方溝通聯繫，最普遍的協定有 SIP、MGCP、Megaco 和 H.323，這些協定彼此都不完全相容(除非是透過軟體伺服器的掌控)。

Vigor V 系列機種支援 SIP 協定，因爲此種協定對 ITSP (Internet Telephony Service Provider)而言是很理想也很方便，支援也最廣。SIP 是一種端對端信號協定，可建立使用者於 VoIP 結構中之出席情形和機動性。每個想要使用 SIP 相同資源辨識器之用戶都可使用標準的 SIP URI 格式

sip: user:password @ host: port

某些區域可能有不同的使用方式，一般來說主機指的是網域，使用者資訊包含有使用者名稱區、密碼區，@符號則緊跟在後，這種格式和 URL 很相似，所以有些人以 SIP URL

來稱呼它。SIP 支援點對點直接撥號，同時也可透過 SIP 代理伺服器(角色雷同 H.323 Gatekeeper)來撥號，而 MGCP 協定則是使用用戶-伺服器結構，撥號方式和目前 PSTN 網路是相同的。

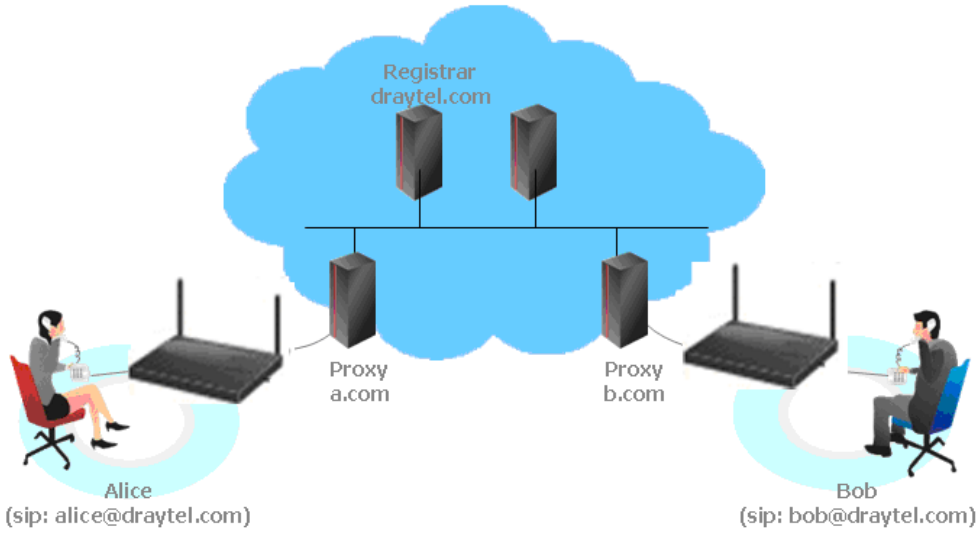
在撥號設定之後，聲音是透過 RTP (Real-Time Transport Protocol)來傳送的，不同的 codecs(用來壓縮和解壓縮聲音)可以包覆於 RTP 封包中，Vigor V 機種提供不同的 codecs 包括 G.711 A/μ-law, G.723, G.726 和 G.729 A & B，每個 codecs 都使用不同頻寬，因此可以提供不同等級的聲音品質。Codec 使用的頻寬越多，聲音品質越好，雖然如此還是應該配合您的網際網路頻寬選擇適宜的 codec 才恰當。

通常有二種撥號類型，說明如下：

- **透過 SIP 伺服器撥號**

  首先 Vigor V 機種必須先向 SIP 註冊，傳送註冊訊息才可生效，然後雙方的 SIP 代理商將轉送一系列訊息給與撥號者，以便建立完整的 session。

  如果雙方都向相同 ISP 業者註冊，那麼我們可以下圖來做簡單說明：



  這種模式最主要的好處是您不必去記朋友的 IP 位址(因爲它可能常常會改變，如果該位址是浮動的位址的話)，相反的您只要使用撥號計畫或是直接撥朋友的帳號名稱就可以了。

- **點對點**

  我們的 Vigor V 機種首先採用有效之 codecs，但同時也擔保自動 QoS 的功能，QoS 擔保可以協助指定聲音流量較高之優先權，您對聲音所需求之 inbound 和 outbound 頻寬永遠擁有優先處理權，但是您的資料處理就會有些慢，不過還在忍受範圍內。

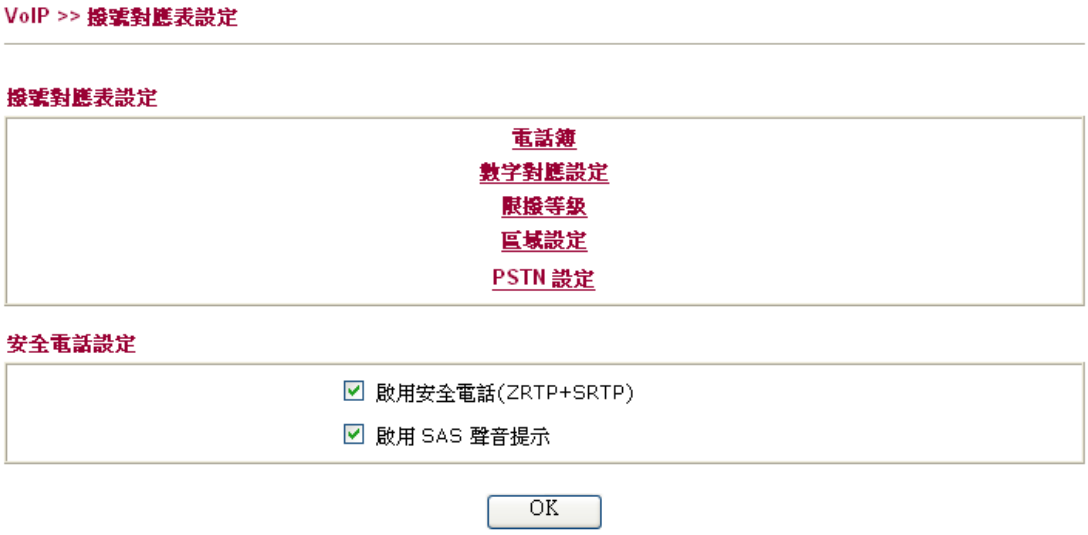
我們的 Vigor V 機種首先採用有效之 codecs，但同時也擔保自動 QoS 的功能，QoS

擔保可以協助指定聲音流量較高之優先權，您對聲音所需求之 inbound 和 outbound 頻寬永遠擁有優先處理權，但是您的資料處理就會有些慢，不過還在忍受範圍內。

下圖爲 VoIP 的功能項目：

3.5.1 撥號對應表

本頁讓使用者設定 VoIP 功能所需的電話簿及數字對應設定。請按頁面上的連結進入下一層設定頁面。



啓用安全電話 利用相同的通訊協定(ZRTP+SRTP)讓使用者能有加密的 RTP stream 與遠端通訊，請勾選此方塊啓動此安全電話功能。

啓用 SAS 聲音提示 若啓動此項目，每一次雙邊都會聽見 SAS 提示音，若沒有啓動，就再也不會聽到提示音。

安全電話的應用

啓用 SAS 聲音提示，例如路由器 A **啓用安全電話**與**啓用 SAS 聲音提示**並打電話給路由器 B：

1. 在連線建立後，路由器 A 將會傳送 SAS 聲音提示訊息給予 A，路由器 B 傳送 SAS 聲音提示訊息給予 B。
2. 此時，RTP 流量是受到安全保護的，直到電話通訊結束。
3. 如果路由器 A 想要下次再打給路由器 B，即使在網頁上已經勾選了**啓用 SAS 聲音提示**，這次不會再聽到任何聲音提示了，亦即只有第一通電話才會有聲音提示的功能。

啓用 SAS 聲音提示，例如路由器 A **啓用安全電話**，但未**啓用 SAS 聲音提示**並打電話給路由器 B：

1. 在連線建立後，路由器 A 將**不會**傳送 SAS 聲音提示訊息給予 A，路由器 B **也不會**傳送 SAS 聲音提示訊息給予 B。
2. 即使沒有聲音提示，RTP 流量仍然受到安全保護，直到電話通訊結束。

注意: 如果來電或去電並不符電話簿上的任何一個設定，路由器將會嘗試讓該通電話先具備一定的保護，但是如果該通電話是以未受保護的情況下結束（例如對方並不支援 ZRTP+SRTP 功能），路由器將不會播放任何警告訊息。

電話簿

在本節中，您可以設定 VOIP 電話，這個設定可以幫助用戶以最快且最簡單的方式撥出電話號碼。本頁總共提供 60 組號碼給用戶儲存朋友以及家人的 SIP 位址。

按任何一個索引標號進入下一個設定頁面。

啓用 勾選此方塊啓用此號碼。

電話號碼	此索引編號的快速撥號號碼，任何號碼都可以使用，範圍是數字 **0-9** 以及*****。
顯示名稱	您想要在朋友的電話螢幕上顯示出來的名稱，可讓您的朋友容易知道是誰打的電話。
SIP URL	請輸入朋友的 SIP 位址。
撥出帳號	選擇 SIP 帳號供此設定檔使用，對在不同 SIP 伺服器註冊的雙方，此設定相當有用。如果撥號者與接號者沒有使用相同的 SIP 伺服器，有時候 VoIP 電話連線可能不會成功，但使用指定的撥號帳號，就可確保網路電話得以成功連線。
電話介接	可選擇的項目如下: 
備援電話號碼	當 VoIP 電話受到幹擾或是網際網路因爲某種原因而中斷，備援電話將可撥出以替代 VoIP 網路電話。此時，電話會依照所選擇的電話介接方向從 VoIP 電話轉變成爲 PSTN 電話。請注意，在電話交換期間，電話的嘟嘟聲響也會短暫出現，當 VoIP 電話切換成 PSTN 電話後，電信公司就會向您收取連線的費用。請在此輸入備援電話號碼(PSTN)。

數字對應設定

爲了使用者的方便，本頁允許使用者以新號碼來編輯 SIP 帳號的前置號碼，或是取代該號碼等等，這個設定可以提供用戶一個透過 VoIP 介面快速且簡單的撥號方式。

啓用 按此方塊啓動此功能。

前置號碼 此處所設定的號碼可用來新增，取代變更之號碼。

模式

無 – 無動作。

新增 -當您選擇此模式時，變更號碼將會增加前置號碼於前面，並藉由選定的 VoIP 介面撥出。

卸除 -當您選擇此模式時，變更號碼將會被刪除。參考上圖所示，變更號碼 886 將被完全刪除。

取代- 當您選擇此模式時，透過指定的 VoIP 介面之變更號碼將會被前置號碼所取代，當您選擇此模式時，透過指定的 VoIP 介面之變更號碼將會被前置號碼所取代，參考上圖所示，號碼 *03* 將被取代爲變更號碼 *8863*。

變更號碼 您在此處所輸入的號碼是您想要執行特殊功用的帳號前半部份(依據選擇的模式而定)。

最小長度 設定撥號的最小長度以套用前置號碼之設定，參考上圖所示，如果號碼介於 7 和 9，那麼該號碼可以就能套用此處所設定的前置號碼設定。

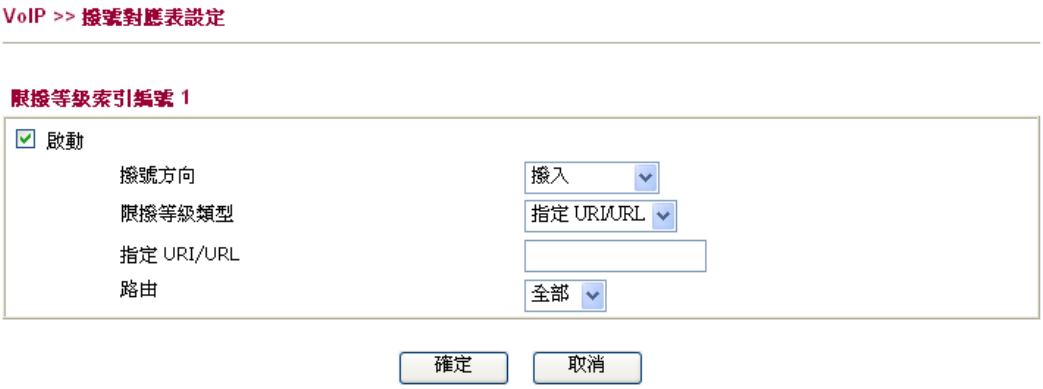
最大長度 設定撥號的最大長度以套用前置號碼之設定。

介面 請自預設的六組 SIP 帳號中選擇一個您想要啓動前置號碼設定的介面。

限撥等級

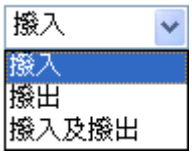
限撥等級用來阻擋不受歡迎的來電。

按任何一個索引標號進入下一個設定頁面。



啓動 按此方塊啓動此功能。

撥號方向 決定電話的撥打方向。撥入- 來電，撥出-去電，撥入及撥出–來電與去電。



限撥等級類型　　決定 VoIP 電話類型爲 URI/URL 或是號碼。

指定 URI/URL 或指定號碼　本區依照您在限撥等級類型中所選擇的內容而有所不同。

介面　　**全部**表示全部的電話都會被此機制阻擋。

此外，您也可以將**限撥等級**做進一步的設定諸如匿名封鎖、未知網域封鎖或是封鎖 IP 位址等等。按下相關連結即可開啓網頁。

針對**封鎖匿名**部分 – 此功能可封鎖沒有顯示身分的任何來電，此項設定也可依照事先設定的排程來控制。

針對**封鎖未知網域**部分 - 此功能可封鎖未在 SIP 帳號中指定的網域之來電，此項設定也可依照事先設定的排程來控制。

針對**封鎖 IP 位元址**部分 - 此功能可封鎖來自 IP 位址之來電，此項設定也可依照事先設定的排程來控制。

區域設定

本頁可讓您處理某些區域的來電與去電，預設值(大部分地區的常用值)顯示在網頁上，您可以依照路由器放置的地點，視需要去改變相關號碼。

回撥最後來電 [漏接] 有時候，人們會漏接某些電話，您可撥打此區所設定的號碼，查看最後的來電是誰打的，然後撥打回去。

回撥最後來電[撥入] 您剛完成來電通話，但爲了某些原因你需要再通話一次，請撥打此區所設定的號碼，即可撥打給剛剛通話的人員。

回撥最後來電 [撥出] 請撥打此區所設定的號碼，再次撥打剛剛去電的人員。

來電跟隨 [全部][執行] 請撥打此區所設定的號碼，轉送全部來電給指定的位置。

來電跟隨 [解除] 請撥打此區所設定的號碼，解除來電跟隨功能。

來電跟隨 [忙線][執行] 電話忙線時，請撥打此區所設定的號碼，轉送來電給指定的位置。

來電跟隨 [無回應][執行] 來電欲連接的電話沒有回應時，請撥打此區所設定的號碼，轉送所有來電至指定位址。

勿打擾 [執行] 請撥打此區所設定的號碼，執行請勿打擾功能。

勿打擾 [解除] 請撥打此區所設定的號碼，解除請勿打擾功能。

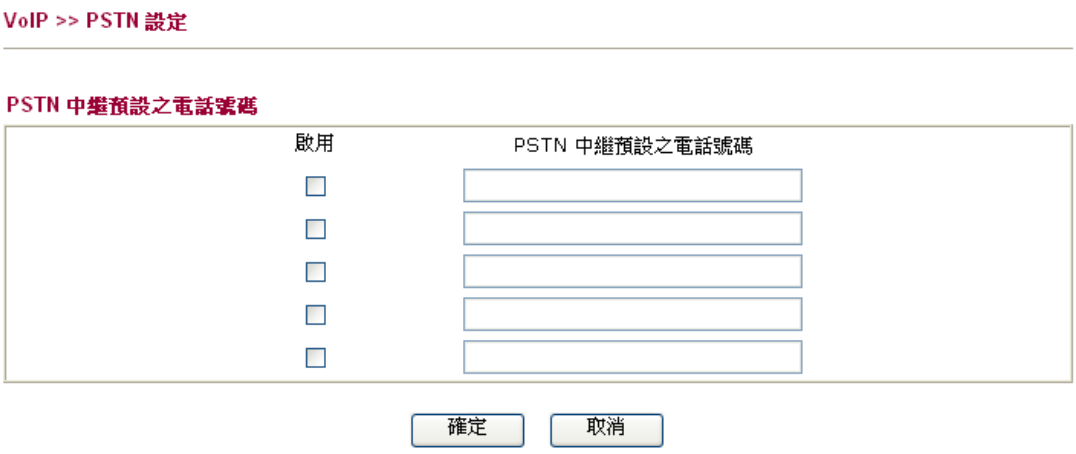
隱藏撥號身分 [執行] 請撥打此區所設定的號碼，讓您的電話號碼不會顯示在對方的顯示面板上。

隱藏撥號身分 [解除] 請撥打此區所設定的號碼，解除此項功能。

來電待接 [執行]	請撥打此區所設定的號碼，讓所有的來電等待您的回應。
來電待接 [解除]	請撥打此區所設定的號碼，解除此項功能。
封鎖匿名 [執行]	請撥打此區所設定的號碼，封鎖所有未之身分的來電。
封鎖匿名 [解除]	請撥打此區所設定的號碼，解除此項功能。
封鎖不明網域 [執行]	請撥打此區所設定的號碼，封鎖所有未知網域的來電。
封鎖不明網域 [解除]	請撥打此區所設定的號碼，解除此項功能。
封鎖 IP 來電 [執行]	請撥打此區所設定的號碼，封鎖所有自 IP 位址的來電。
封鎖 IP 來電 [解除]	請撥打此區所設定的號碼，解除此項功能。
封鎖最後來電 [執行]	請撥打此區所設定的號碼，封鎖最後的來電。

PSTN 設定

一些無法利用 VoIP 撥打的緊急電話(例如 119)或是特殊的電話僅能使用 PSTN 線路撥打出去，爲瞭解決這個問題，這個頁面讓您設定五組 PSTN 號碼，以便在網路斷線時可以撥打出去。請在 **PSTN 中繼電話號碼**欄位中輸入電話號碼。



接著請勾選**啓用**方塊讓 PSTN 號碼在您需要時可以撥打出去。

3.5.2 SIP 帳號

在此頁面中，您可以調整自己的 SIP 設定，當您申請一個帳號時，您的 ISP 服務供應商會給您一個帳號名稱或是使用者名稱、SIP 登錄者、代理人和網功能變數名稱稱(最後三種在某些條件下，有可能是完全相同的)，您可以告訴您的成員有關您的 SIP 位址，表示法爲**帳號名稱@網功能變數名稱稱**。

當路由器打開時，將以使用帳號名稱@網功能變數名稱稱來登錄，之後，您的電話將由 SIP 代理者以帳號名稱@網功能變數名稱稱傳送至目的地作爲辨識之用。

注意: 振鈴通訊埠的項目會依照您所使用的路由器而有所差異。

索引 按此鈕進入下一層設定頁面設定 SIP 帳號。

設定檔 顯示帳號的設定檔名稱。

網域 顯示 SIP 註冊伺服器的網功能變數名稱稱或是 IP 位址。

伺服器 顯示 SIP 伺服器的網功能變數名稱稱或是 IP 位址。

帳號名稱 顯示@前面的 SIP 位址帳號名稱。

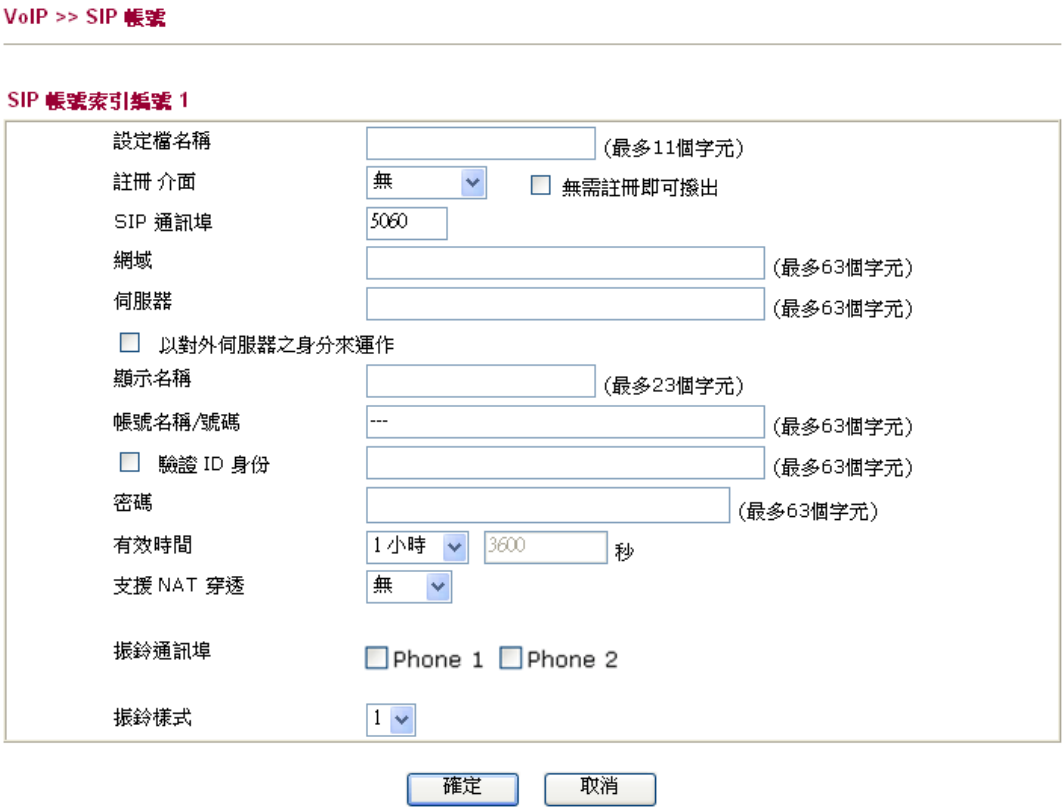
振鈴通訊埠 指定接收電話時由哪一個通訊埠響鈴。

狀態 顯示相關 SIP 帳號的狀態，**R** 表示此帳號已註冊成功，**–** 表示尚未成功註冊。

STUN 伺服器 輸入 STUN 伺服器的 IP 位址或是網域。

外部 IP 輸入閘道 IP 位址。

SIP PING 間隔 預設值爲 150 秒，對 Nortel 伺服器而言這項設定是相當有用的。



設定檔名稱

指定一個名稱作爲辨識之用，您可以使用與網域類似的名稱，例如網功能變數名稱稱爲 *draytel.org*,您就可以在本區中設定 *draytel-1*。

註冊介面

指定您申請註冊時所透過的介面爲何，如果您不想註冊個人資料而直接使用 VoIP 撥號功能，請選擇**無**。某些 SIP 伺服器允許使用者不須登錄即可使用 VoIP 功能，針對這類伺服器，請您選擇**自動**，系統將爲您選擇最佳方式作爲 VoIP 撥號之用。

SIP 通訊埠

通訊埠號用來傳送/接收 SIP 訊息以建立通訊，雖然預設值爲 5060，您仍可將之變更爲其他數字。不過在這種情形下，還需要對方也同時變更爲相同的數字才行。這時

網域

輸入註冊 SIP 伺服器的網功能變數名稱稱或 IP 位址。

伺服器

您可以輸入 SIP 代理伺服器的 IP 位址(或網功能變數名稱稱如 iptel.org)，所有在上述的**網域**區域中指定的訊息來說 Vigor 路由器將之傳送至代理者，由代理者來轉送此訊息。您可以在網功能變數名稱稱後面輸入通訊埠號，指定該埠號爲資料傳輸的目的地 (例如 nat.draytel.org**:5065**)。

以對外伺服器之身份來運

勾選此方塊以啓用伺服器成爲對外伺服器。

作

顯示名稱 您想要在朋友的電話顯示螢幕上出現的名稱。

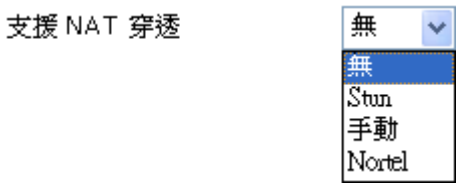
帳號名稱/號碼 輸入 SIP 位址的帳號名稱，例如@之前的文字。

驗證 ID 身分 勾選此方塊啓用此功能並輸入名稱或號碼供 SIP 驗證，如果設定值與帳戶名稱相同，您就不必勾選此方塊另設數值。

密碼 當您以 SIP 服務註冊時所需提供的密碼。

有效時間 爲 SIP 伺服器提保存使用者註冊帳號的有效時間。在到期之前，路由器將會再次傳送另一個註冊需求給予 SIP 登錄伺服器。

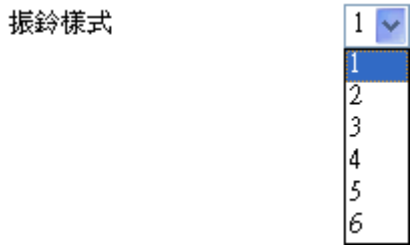
NAT 穿透 如果路由器(寬頻路由器)是透過其他裝置連接上網際網路，您就必須設定此功能。



無 –.關閉此功能。
Stun –若路由器支援 Stun 伺服器，請選擇此項目。
手動 –若您想要指定外部 IP 位址作爲 NAT transversal 支援，請選擇此項目。
Nortel – 如果軟體支援 nortel 方案，您可以選擇此項目。

振鈴通訊埠 設定 VoIP 1,VoIP 2 作爲 SIP 帳號的預設振鈴通訊埠。

振鈴樣式 選擇 VoIP 電話的振鈴樣式。



3.5.3 電話設定

本頁讓使用者得以個別設定 VoIP 1 和 VoIP 2。

電話清單

通訊埠 – 有種通訊埠類型提供給您選擇。

通話功能 – 這個欄位簡單描述此通電話的功能供使用者參考。

Codec – 每個通訊埠的預設 Codec 設定都會顯示在本區，您可以按索引號碼變更每個電話通訊埠的設定。

音調 – 顯示進階頁面所設定的音調值。

音量 - 顯示進階頁面中 Mic/Speaker 的音量設定。

預設 SIP 帳號 –“draytel_1” 是預設的 SIP 帳號，您可按索引下方的編號變更 SIP 帳號設定。

DTMF 中繼 – 顯示進階頁面中所設定的 DTMF 模式。

RTP

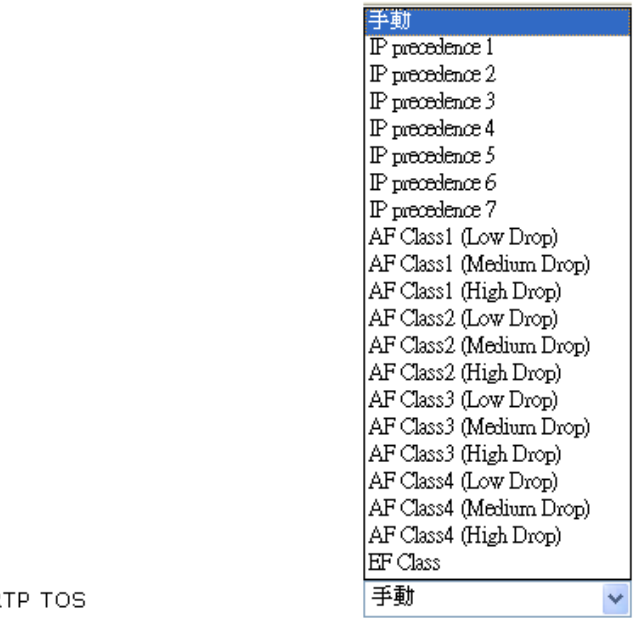
對稱 RTP – 勾選此方塊啓用此功能。若要讓資料傳輸能在本機路由器與遠端路由器之間暢行無阻而不至於因 IP 漏失而誤導的情形發生，請您勾選此方塊解決這個問題。

RTP 通訊埠起點 - 指定 RTP 之通訊埠起點，預設值爲 10050。

RTP 通訊埠終點 - 指定 RTP 之通訊埠終點，預設值爲 15000。

RTP TOS –此項可決定 VoIP 封包的等級，請使用下拉式選

項選擇其中一種。



Phone Port 細節設定

請按索引欄位元下方的 1 或 2 連結進入下麵的設定頁面。

熱線 勾選此方塊啓用此功能，請在本區輸入 SIP URL 讓系統在您拿起話機後自動撥號。

連線數計時器 勾選此方塊啓用此功能，您在本區所設定的限制時間內如果沒有任何回應，連線電話將會自動關閉。

指定轉接 共有四種選項可以選擇，**停用**可關閉此功能，**永遠**則表示來電會一直轉接到 SIP URL 上，**忙線**則表示來電只在本機忙碌時轉接到 SIP URL，**沒回應**則表示來電若未收到任何回應，電話都會在切斷時轉接到 SIP URL 上。

SIP URL – 請輸入 SIP URL (例如 aaa@draytel.org 或 abc@iptel.org) 做爲轉送電話的終點。

逾時 – 設定電話轉接的逾時現制，預設值爲 30 秒。

DND (勿幹擾)

設定一段和平時間不受任何 VoIP 來電的幹擾。在此期間，撥號進來的人會聽到忙線的聲音，而本機用戶則聽不到任何電話鈴聲。

索引(1-60) 於電話簿 - 輸入例外電話於此方塊內，列於此之電話不受勿幹擾的限制。詳細設定請參考**電話簿**一節。

CLIR (隱藏撥號者身分)

勾選此方塊讓撥號者身分不會顯示在話機的顯示面板上。

話中插接

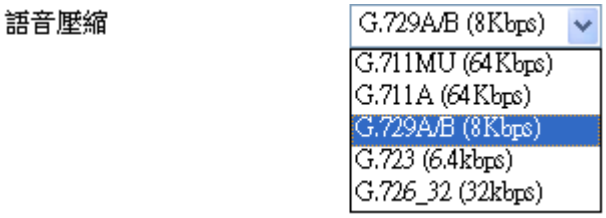
勾選此方塊啓用此功能，提示聲音將會出現以告知使用者有電話在等待。

電話轉接

勾選此方塊啓用此功能，按轉接鍵轉接另一通電話，當電話連線成功時，掛上電話。此時另外二方就可直接溝通。

語音壓縮

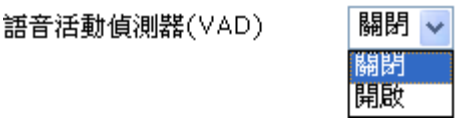
有五種不同的 CODEC 供您選擇，但真正被使用的 CODEC 在通訊建立前是和對方共同商議而得。預設的 CODEC 是 G.729A/B，它佔據較少的頻寬但是卻仍擁有良好的聲音品質，如果您想要使用 G.711，您最好具有至少 256Kbps 的上傳速率。



單一 Codec - 如果勾選此方塊，只有選定的 Codec 會被路由器套用。

語音資料長度 - 資料總數包含單一封包(10, 20, 30, 40, 50 和 60)，預設值爲 20ms，表示資料封包含 20ms 聲音資訊。

語音活動偵測器(AVD) - 選擇**開啓**啓動此項功能，以檢測使用者是否正在交談。如果安靜無聲，路由器將採取行動節省頻寬的使用。



預設 SIP 帳號

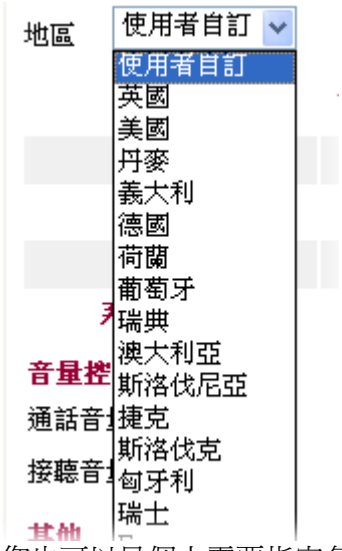
您可以設定 SIP 帳號(最多 6 組)，請使用下拉式清單選擇其中一組作爲預設帳號。

當帳號已經註冊時，才有撥號音 - 勾選此方塊啓用此功能。

此外，您也可以按**進階**按鈕進入深一層的設定。此項設定是爲了符合路由器安裝所在地區的電信習慣而提供，錯誤音調設定可能會造成使用者的不便。關於設定話機的聲音型態，方法很簡單，只要選擇適當的區域讓系統自動尋找事先設定的音調設定和呼叫 ID 類型，或是您也可選擇使用者自訂，然後以手動方式調整音調，T on 1, T off 1, T on 2 和 T off 2 表示音調型態的韻律，T on 1 和 T on 2 表示開啓聲音；T off 1 和 T off 2 則表示關閉聲音。

地區

選擇您目前所處地區，**來電顯示類型**、**撥號音**、**響鈴音**、**忙線音**和**系統擁塞音**都會自動顯示在本頁面上。如果您無法找到適合的地區，請您選擇**使用者自訂**，再自行輸入頁面所需的各式資料



您也可以是個人需要指定各個區域內容，建議您採用預設值作爲 VoIP 通訊之用。

來電顯示類型

此處提供數種標準，以便在電話機面板上顯示來電者的身分，請依照路由器安裝所在地區選擇適合的類型，如果您不知道話機究竟支援哪種標準，請直接採用預設值。

音量控制

請輸入 1- 10 以設定麥克風的音量，數字越大聲音越大。

其他

撥號音量控制 -此項設定用來調整撥號的音量大小，數字越小音量越大，建議使用預設值。

振鈴聲頻率 此項設定用來驅動鈴聲的頻率，建議使用預設值。

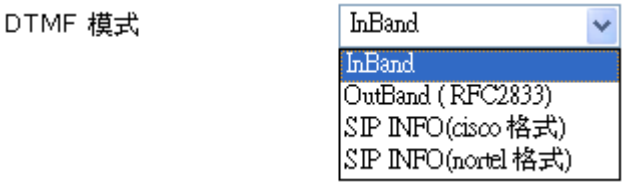
DTMF

DTMF 模式

InBand - 當您按壓電話上的鍵盤時，路由器將會直接以聲音模式傳送 DTMF 音調。

OutBand - 路由器將會抓取您所按壓的鍵盤號碼然後以數位格式傳送至另一端；接收者將會依照所接收的數位格式來產生音調。這個功能在網路擁塞的情形下是很有用處的，因爲它仍可保持 DTMF 音調的準確度。

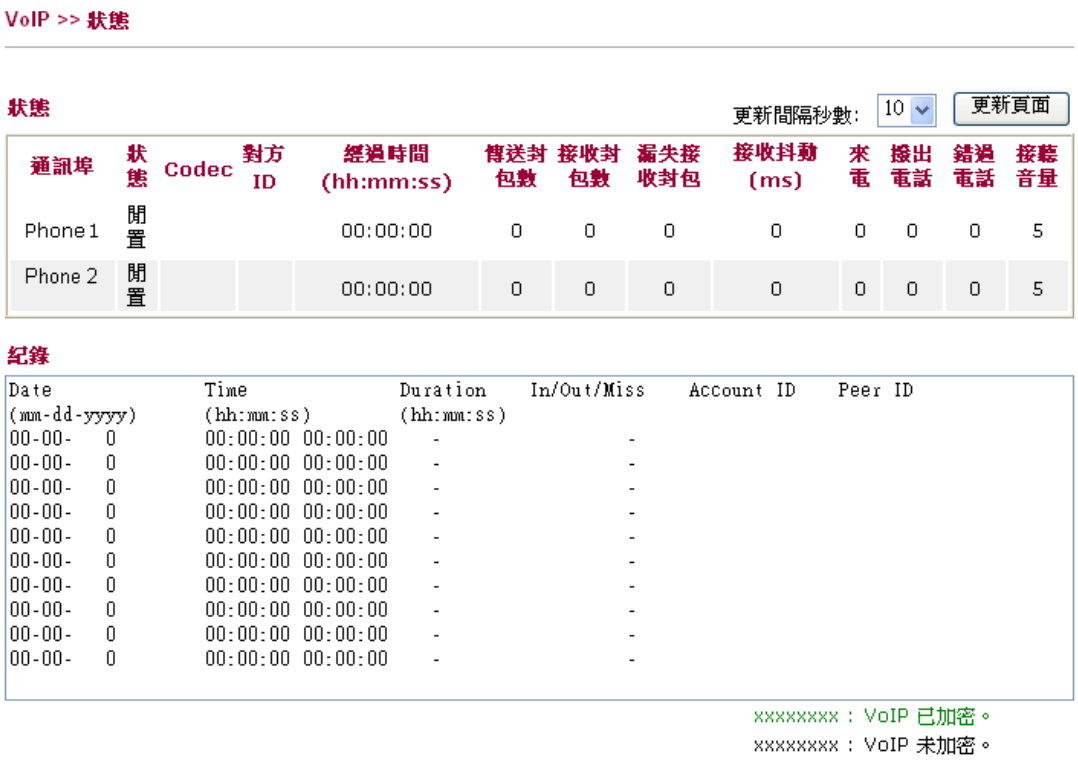
SIP 資訊-路由器將抓取 DTMF 音調然後以 SIP 訊息轉送給遠端用戶。



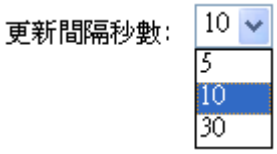
Payload 類型 (RFC2833) - 請自 96 至 127 中選擇一個數字，預設值爲 101，此項設定只對 OutBand (RFC2833)模式有效。

3.5.4 狀態

在 VoIP 撥號狀態下，您可以看見 VoIP 1 和 VoIP 2 的 codec、連線情形和其他重要的撥號狀態資料。



更新間隔秒數 指定更新的間隔秒數以取得最新的 VoIP 撥號資訊，當按下**更新頁面**按鈕時，頁面資訊將會立即更新。



通訊埠 顯示目前 VoIP 電話的連線通訊埠(Phone1 / Phone2)。

狀態 顯示 VoIP 連線狀態。
閒置 -表示 VoIP 功能正處於閒置狀態。
HANG_UP -表示連線並未建立(忙線音調)。
CONNECTING -表示用戶正撥出號碼中。
WAIT_ANS -表示已連線並等待遠端用戶的回答。
ALERTING -表示有來電。
ACTIVE-表示 VoIP 連線啓動。

Codec 表示目前頻道所利用的聲音 codec。

對方 ID 撥進或撥出之對方 ID (格式可以是 IP 位址或是網功能變數名稱稱)。

經過時間 通話時間以秒數計算。

傳送封包數 在連線中全部的傳送封包數量。

接收封包數 在連線中全部的接收封包數量。

漏失接收封包	在連線中漏失的全部封包。
接收抖動	接收聲音封包抖動狀態。
來電	已接來電總數。
撥出電話	撥出電話總數。
錯過電話	漏接電話總數。
接聽音量	電話音量大小。
記錄	顯示 VoIP 電話紀錄。

3.6 無線區域網路設定

本節所提供的資訊僅針對 *n* 系列機型。

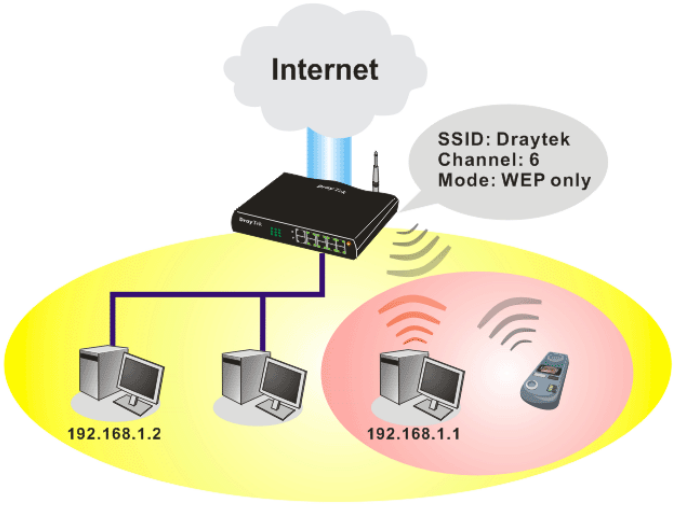
3.6.1 基本觀念

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，又稱爲 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。

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：

3.6.2 基本設定

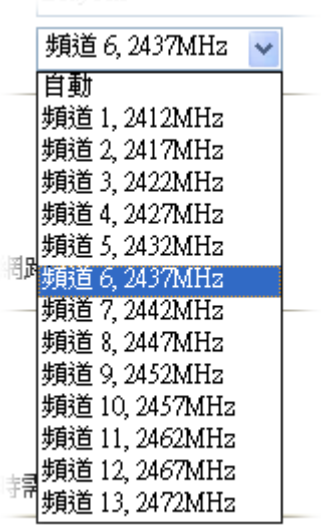
按下**基本設定**連結，新的網頁即會開啓，您可以設定 SSID 和無線頻道資訊，請參考下圖：

啓用 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。目前路由器支援的協定有綜合((11b+11g), 僅 11g, 僅 11b, 綜合((11g+11n), 僅 11n 及綜合((11b+11g+11n)。請選擇綜合 (11b+11g+11n) 模式。

SSID 預設的 SSID 值爲 **DrayTek**，建議您變更爲另一個特殊名稱。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。

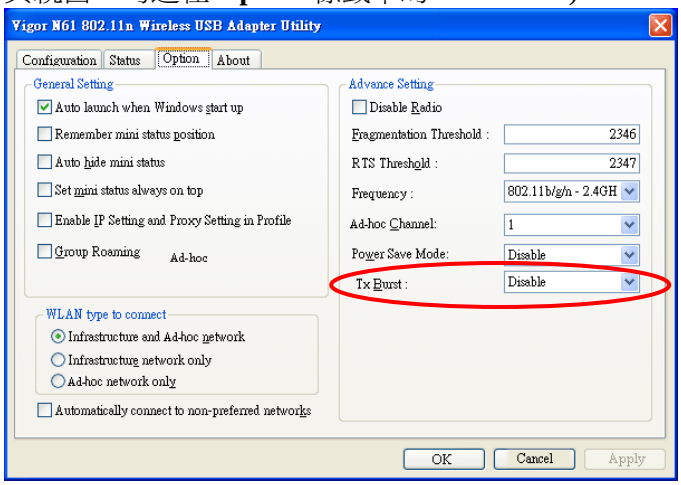
頻道 無線區域網路的通道頻率，預設頻道是 6，如果選定的頻道受到嚴重的幹擾的話，您可自行切換爲其他頻道。



Packet-OVERDRIVE

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 **Tx Burst)**。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。

注意: 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 **Option** 標籤中的 **TxBURST**).



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。

長封包標頭

此選項用來定義 802.11 封包中同步區塊的長度，最新的無線網路以 56 bit 同步區來使用短封包標頭，而不是以 128 bit 同步區來使用長封包標頭。不過，一些原始 11b

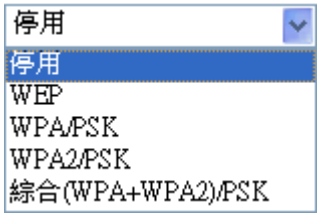
無線網路裝置只有支援長封包標頭而已，因此如果您需要和此種裝置通訊溝通的話，請勾選此方塊。

3.6.3 安全性設定

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。

模式

此一設定有數種模式可供您選擇。



停用 - 關閉加密機制。

WEP - 只接受 WEP 用戶以及僅接受以 WEP 金鑰輸入的加密鑰匙。

WPA/PSK -接受 WPA 用戶，請在 PSK 中輸入加密金鑰。

WPA2/PSK -接受 WPA2 用戶，請在 PSK 中輸入加密金鑰。

綜合 (WPA+ WPA2)/PSK – 同時接受 WPA 與 WPA2 用戶，請在 PSK 中輸入加密金鑰。

WPA

WPA 可藉由金鑰加密每個來自無線網路的訊框，可在本區手動輸入 PSK，或是藉由 802.1x 驗證方式來自動加密。**預先共用金鑰 (PSK)** - 輸入 **8~63** 個 ASCII 字元，

像是 012345678（或是 64 個 16 進位數字，以 0x 開頭，如 0x321253abcde...等）。

WEP

64-Bit - 針對 64 位元的 WEP 金鑰，請輸入 5 個 ASCII 字元，像是 12345（或是 10 個 16 進位數字，以 0x 開頭，如 0x4142434445）。

128-Bit - 針對 128 位元的 WEP 金鑰，請輸入 13 個 ASCII 字元，像是 ABCDEFGHIJKLM（或是 16 個 16 進位數字，以 0x 開頭，如 0x4142434445）。

所有的無線裝置都必須支援相同的 WEP 加密位元大小，並擁有相同的金鑰。這裡可以輸入四組金鑰，但一次只能選擇一組號碼來使用，這些金鑰可以 ASCII 文字或是 16 進位元字元來輸入。請點選您想使用的金鑰組別。

3.6.4 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。只有設定有效的 MAC 位址得以存取無線區域網路介面，請選**連線控制**連結，開啓新的網頁，如同下圖所示，您即可在此頁面上編輯用戶端的 MAC 位址達到控制其存取權的目的。

啓用連線控制 勾選此項以啓動 MAC 位址存取控制作用。

規則 選擇一項規則，請挑選**啓用 MAC 位址過濾器**以便在下方手動輸入其他用戶的 MAC 位址；挑選**隔離無線網路和有線網路**可以 MAC 位址清單爲基礎，自區域網路中隔開所有的無線網路用戶站。

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。

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。

3.6.5 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**新增到連線控制**，這樣就可以了。

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**。

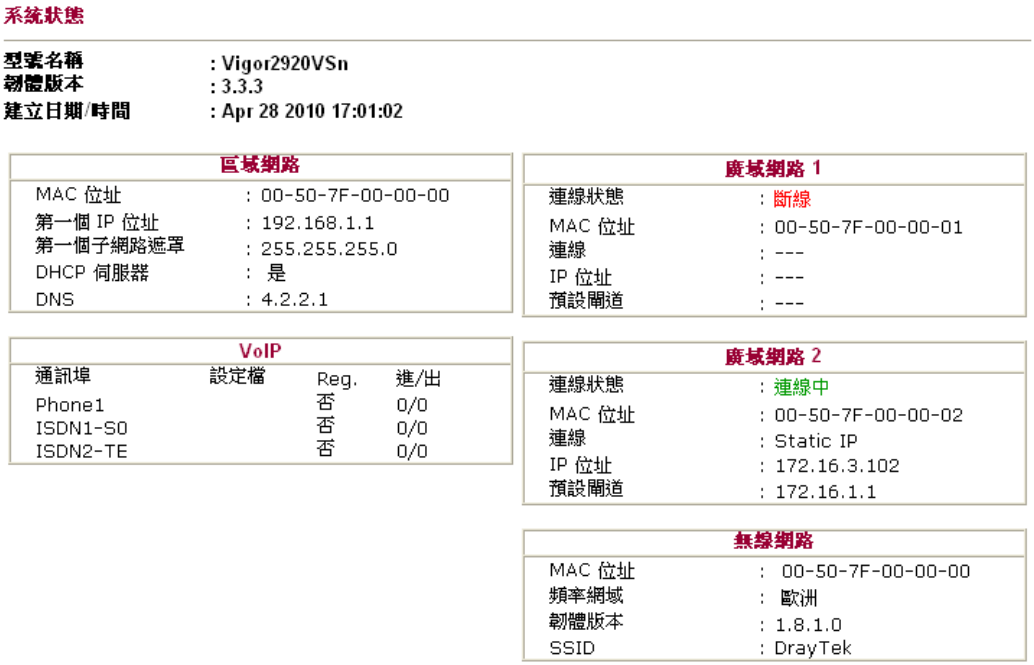
3.7 系統維護

系統設定方面，有數種項目是使用者需要瞭解的：系統狀態、使用者密碼、時間設定、重啓系統等等。

下圖爲系統維護的主要設定功能。

3.7.1 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。



型號名稱 顯示路由器的型號名稱。

韌體版本 顯示路由器的韌體版本。

建立日期與時間 顯示目前韌體建立的日期與時間。

區域網路------

MAC 位址 顯示區域網路介面的 MAC 位址。

第一個 IP 位址 顯示區域網路介面的 IP 位址。

第一個子網路遮罩 顯示區域網路介面的子網路遮罩位址。

DHCP 伺服器 顯示區域網路介面的 DHCP 伺服器目前的狀態。

DNS 顯示主要 DNS 的 IP 位址。

廣域網路------

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

3.7.2 使用者密碼

本頁允許您設定新的密碼。

舊密碼	請輸入舊密碼，出廠預設值是空白的。
新密碼	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。

3.7.3 時間和日期

允許您指定自何處取得路由器時間。

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，作。

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。

時間協定 選擇適合本地的時間協定。

伺服器 IP 位址 輸入時間伺服器的 IP 地址。

時區 選擇路由器所在的時區。

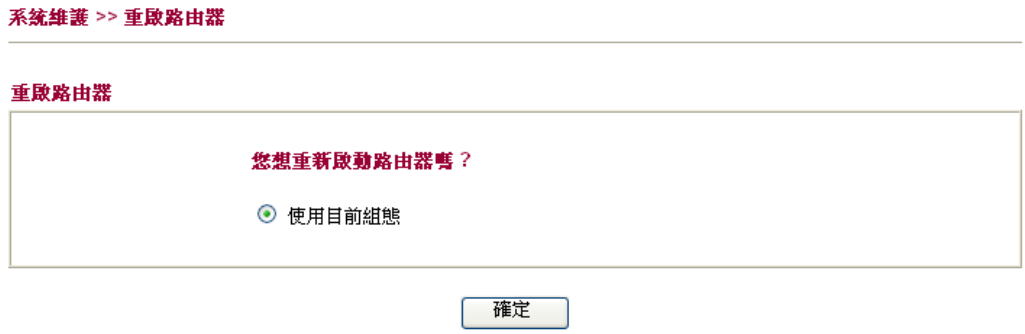
啓用日光節約時間 勾選此方塊啓動日光節約時間，此一設定對某些區域來說是很有用的。

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。

3.7.4 重啓路由器

網路設定完畢之後，可重新啓動路由器，請自**系統維護**中按**重啓路由器**開啓如下頁面。



如果要重設路由器設定回復成爲預設值，請進入管理者模式。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**確定**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。

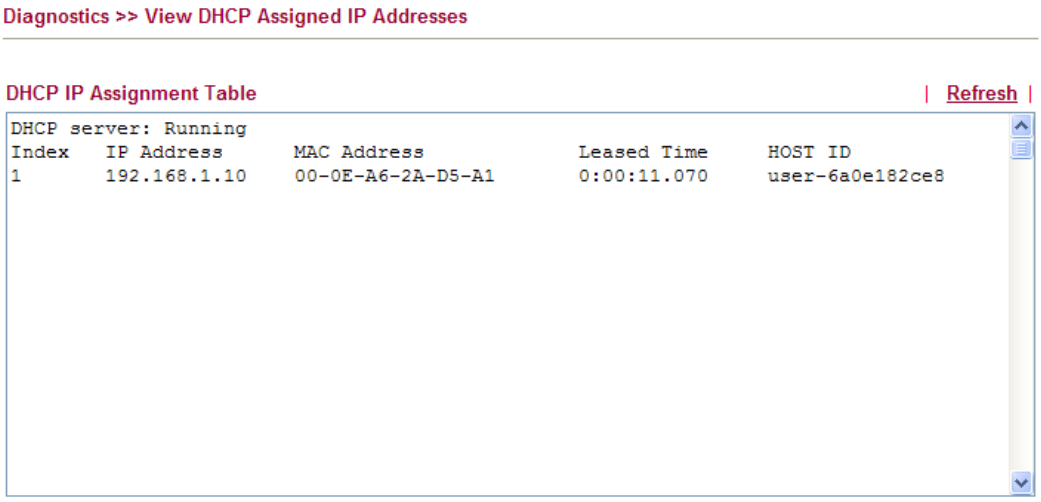
3.8 自我診斷工具

自我診斷工具提供有用的方式供用戶檢視或診斷路由器。下圖爲自我診斷工具的功能項目。

3.8.1 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。



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。

3.8.2 流量圖表

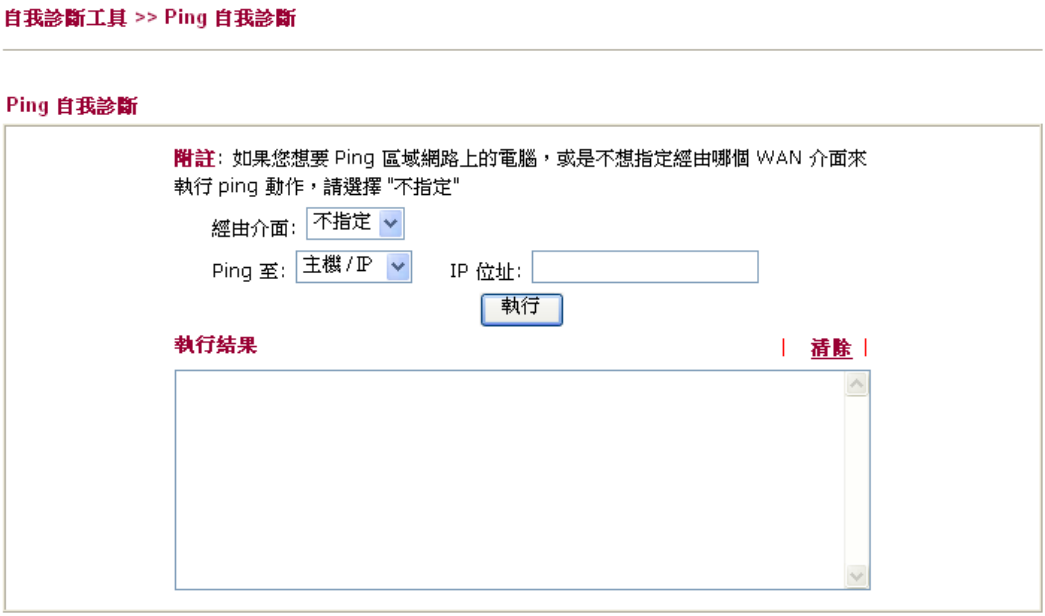
按**自我診斷工具**，選擇**流量圖表**開啓相關網頁。可以選擇 **WAN1 頻寬**或是**連線數**來檢視流量圖表。您可隨時按**更新頁面**重新顯示圖表內容。

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。

3.8.3 Ping 自我診斷

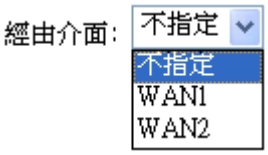
按**自我診斷工具**，選擇 **Ping 自我診斷**開啓相關網頁。



經由介面　　選擇介面以執行此動作。

Ping 至

使用下拉式清單選擇您想要 Ping 的目標。



IP 位址

輸入您想要 Ping 的主機/IP 上的 IP 位址。

執行

按此鈕啓動 Ping 作業，結果將會顯示在螢幕上。

清除

按此連結清除視窗上的結果。

3.8.4 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。

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**不指定**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。

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。

本頁空白

4 管理者操作模式

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 5 章。

1. 開啓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爲何，本例中應該出現 “管理者模式”。

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

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

什麼是真實 IP 位址和虛擬 IP 位址

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

取得 ISP 提供的真實 IP 位址

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

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

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 2910 新增了 3G 網路通訊功能。藉著連接 3G USB Modem 至 Vigor2920 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 Vigor2920n 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 Vigor2920n 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 及被視爲第二個 WAN 埠，雖然如此原本的乙太網路 WAN1 仍可作爲負載平衡之用，此外 3G USB Modem 也可被視爲備存裝置。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。

下圖爲 WAN 的功能項目：

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 和 WAN2 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。

網頁允許您個別設定 WAN1 和 WAN2 的一般設定。

注意: WAN1 預設狀態是啓動的，而 WAN2 則是視情況選擇的項目。

啓用 選擇**是**啓動此 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。

實體模式 對 WAN1 而言，實體連線是透過 ADSL 連接埠來完成，不過 WAN2 的實體連接則是透過乙太網路/3G USB 模式來完成。

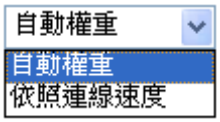
欲透過 3G USB 模式使用 3G 網路連線，選擇 **3G USB 模式**作爲 **WAN2** 的實體模式，接著開啓 **WAN>> 網際網路連線**. 在WAN2 上就可以看到 3G USB Modem 模式了，您可以使用 **PPP** 作爲**連線模式**再按下**細節設定**作進一步調整。

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。

負載平衡模式

如果您知道 WAN 介面的實際頻寬，請選擇**依照連線速度**。否則請選擇**自動權重**，讓路由器來完成最佳的平衡結果。



連線速度

如果您選擇**依照連線速度**作爲負載平衡模式，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。

啓動模式

選擇**永遠連線**讓 WAN 連接(WAN1/WAN2)能永遠啓動運作；或是選擇**需求時連線**，讓 WAN 連接在有需要時才連上線。

如果您選擇的是需求時連線，即可爲 PPPoE 和 PPTP 存取模式設定閒置逾時之時間，此外有三種選項供不同目的之需要來設定。

WAN2 連線失敗 – 表示 WAN1 在 WAN2 失敗時即自動連線。

WAN2 上傳速度超過 XX kbps – 表示當 WAN2 上傳速度超過指定數值 15 秒過後，WAN1 便自動連線。

WAN2 下傳速度超過 XX kbps – 表示當 WAN2 下載傳速度超過指定數值 15 秒過後，WAN1 便自動連線。

WAN1 連線失敗– 表示 WAN2 在 WAN1 失敗時即自動連線。

WAN1 上傳速度超過 XX kbps – 表示當 WAN1 上傳速度超過指定數值 15 秒過後，WAN2 便自動連線。

WAN1 下傳速度超過 XX kbps – 表示當 WAN1 下載傳速度超過指定數值 15 秒過後，WAN2 便自動連線。

4.1.3 網際網路連線控制

因爲路由器支援雙 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，又因爲 WAN1 與 WAN2 的實體連線並不同，二者的連線模式也會有些差異。

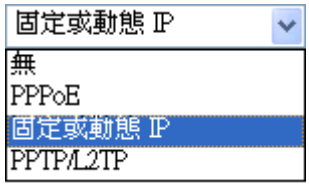
索引　　顯示路由器支援的 WAN 模式，WAN1 是預設的 WAN 介面，WAN2 爲 WAN1 無法運作時的選項介面。

顯示名稱　　顯示 WAN1/WAN2 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（乙太網路）/ WAN2(乙太網路或 3G USB 模式) 實體連線。

乙太網路	乙太網路
3G USB 數據機	乙太網路

連線模式　　使用下拉式清單選擇適當的網際網路連線模式，接著按右邊的**細節設定**以設定詳細內容。



網頁提供數種網際網路連線模式。

細節設定　　此按鈕將依照您在 WAN1 或 WAN2 所選擇的連線模式展現不同的網頁內容。

PPPoE 細節設定

如果想要使用 PPPoE 作爲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。

PPPoE 用戶端模式 按下**啓用**按鈕可啓動此功能，如果您選的是**停用**，此項功能將會關閉，全部調整過的設定也都將立即失效。

ISP 存取設定 輸入使用者名稱、密碼和驗證參數，按照 ISP 所提供給您的訊息。
使用者名稱 –在本區請輸入 ISP 提供的使用者名稱。
密碼 – 在本區請輸入 ISP 提供的密碼。
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**應用-排程**網頁中事先設定完畢，您可在此輸入該排程的索引編號。

WAN 連線檢測 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。
模式 – 選擇 **ARP Detect 或 Ping Detect** 執行 WAN 檢測動作。
Ping IP – 如果您選擇 **Ping Detect** 作爲檢測模式，您必須在本區輸入 IP 位址作爲 Ping 檢測之用。
TTL (Time to Live) – 顯示數值供您參考，TTL 數值是利用 Telnet 指令始可設定。

MTU 代表封包的最大傳輸單位，預設值爲 1442。

PPP/MP 設定 **PPP 驗證** – 選擇 **PAP** 或是 **PAP 或 CHAP**。如果您想要永遠連接網際網路，請勾選**永遠連線**。
閒置逾時 – 設定網際網路在經過一段沒有任何動作的時間後自動斷線的時間。

IP 位元址指派方式 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。

(IPCP)

您只要在固定 IP 位址欄位中輸入 IP 位址就可以達成上述的目的。詳情請聯絡您的 ISP 業者。

WAN IP 別名 - 如果您有數個真實 IP 位址且想要在 WAN 介面上使用，請使用此功能。除了目前使用的這一組之外，您還可以設定多達 8 組的真實 IP 位址。

固定 IP 位址 – 按**是**使用此功能並輸入一個固定的 IP 位址。

預設 MAC 位址 – 您可以使用預設 MAC 位址或是在此區域中填入另一組位址。

指定 MAC 位址 – 手動輸入路由器的 MAC 位址。

在您完成上述的設定之後，請按**確定**按鈕來啓動設定。

固定或動態 IP 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** 爲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。

固定或動態 IP (DHCP 用戶端)

按**啓用**以啓動此功能，如果您按的是**停用**，此功能將會關閉，您在此頁面所完成的全部設定都將失效。

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，因爲某些 ISP 會在一段時間沒有任何回應時中斷連線。請勾選**啓用 PING 以保持常態連線**。

PING 到指定的 IP – 如果您啓用此功能，請指定 IP 位址讓系統可以 PING 到該 IP 以保持連線

PING 間隔 - 輸入間隔時間讓系統得以執行 PING 動作。

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。

模式 – 選擇 **ARP Detect 或 Ping Detect** 執行 WAN 檢測動作。

Ping IP – 如果您選擇 **Ping Detect** 作爲檢測模式，您必須在本區輸入 IP 位址作爲 Ping 檢測之用。

TTL (Time to Live) – 顯示數值供您參考，TTL 數值是利用 Telnet 指令始可設定。

MTU

代表封包的最大傳輸單位，預設值爲 1442。

RIP 協定

指名路由器是如何變更路由表格資訊，勾選此項目以啓動此功能。

WAN IP 網路設定

這個區域允許您自動取得 IP 位址並讓您手動輸入 IP 位址。

WAN IP 別名 - 如果您有多個真實 IP 位址，想要在 WAN 介面上利用這些 IP，請使用 WAN IP 別名。除了目前使用的 IP 外，

您還可以另外設定 8 組真實 IP，要注意的是，本項設定僅針對 WAN1 有效用。

自動取得 IP 位址 – 如果您想要使用**動態 IP** 模式，按此鈕以自動取得 IP 位址。

路由器名稱: 輸入 ISP 的路由器名稱。

網功能變數名稱稱: 輸入指定的網功能變數名稱稱。

指定 IP 位址 – 按此鈕指定 IP 位址讓資料通過。

IP 位址:輸入 IP 位址。

子網路遮罩:輸入子網路遮罩。

閘道 IP 位址: 輸入閘道 IP 位址。

預設 MAC 位址: 按此鈕使用預設的 MAC 位址。

指定 MAC 位址: 部分 Cable 服務供應商會指定 MAC 位址作爲存取驗證之用，此時您需要按下此鈕並在下方區域輸入 MAC 位址。

DNS 伺服器 IP 位址 若要使用固定 IP 模式，請輸入路由器的主要 IP 位址，如有必要，在將來，您也可以輸入次要 IP 位址以符合所需。

PPTP/L2TP 細節設定

若要使用 **PPTP** 爲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**，即可出現下圖。

PPTP/L2TP 用戶端模式

啓用 PPTP - 選擇此鈕已啓用 PPTP 用戶端建立通往 WAN 介面的 DSL 數據機之通道。

啓用 L2TP - 選擇此鈕已啓用L2TP 用戶端建立通往WAN介面的 DSL 數據機之通道。

停用 - 選擇此鈕停用 PPTP 或 L2TP 連線通道。

伺服器位址 - 指定 PPTP/ L2TP 伺服器的 IP 位址。

指定閘道 IP 位址 - 針對 PTP/L2TP 伺服器指定閘道 IP 位址。

ISP 存取設定

使用者名稱 - 輸入 ISP 業者提供給您的使用者名稱。

密碼 - 輸入 ISP 業者提供的密碼。

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，預設值爲 1442。

PPP Setup

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 位元址指派方式 (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。

PPP 細節設定

如果要使用 **PPP** (針對 3G USB Modem) 做爲網際網路連線協定，請自 **WAN** 中選擇**網際網路連線**，接著在 WAN2 介面上選擇 **PPP**，即可出現下圖。

PPP 用戶端模式 選擇**啓用**以啓動此項模式。

SIM 卡 PIN 碼 輸入 SIM 卡 PIN 碼，以便連線網際網路。

數據機初始化字串 這個數值，用來初始化 USB 數據機，請使用預設值，如果您有任何疑問，請與當地 ISP 業者聯絡。

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 使用者名稱 輸入 PPP 使用者名稱 (視您實際需要而設定)。

PPP 密碼 輸入 PPP 密碼 (視您實際需要而設定)。

索引號碼(1-15) 可以輸入四組時間排程，全部的排程都是在**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。

4.1.4 負載平衡原則

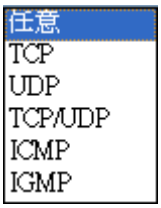
路由器支援負載平衡功能，可以將通訊協定之類型、指定主機的 IP 位址、主機子網路以及通訊埠範圍指派至 WAN1 或是 WAN2 介面。使用者可以指定流量的類型並基於此網頁之設定，強迫封包前往特定網路介面。本路由器支援 20 組的原則。

注意:負載平衡原則只在 WAN1 和 WAN2 都啓動的情形下才能執行。

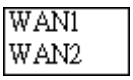
索引編號 按下任何一個索引號碼以進入負載平衡原則設定頁面。

啓用 勾選此方塊以啓用此原則。

通訊協定 使用下拉式功能以變更 WAN 介面的通訊協定。



WAN 使用下拉式功能以變更 WAN 介面。



來源 IP 起點 顯示來源 IP 起點的 IP 位址。

來源 IP 終點 顯示來源 IP 終點的 IP 位址。

目標 IP 起點　　顯示目標 IP 起點的 IP 位址。

目標 IP 終點　　顯示目標 IP 終點的 IP 位址。

目標通訊埠起點　　顯示目標通訊埠起點的埠號。

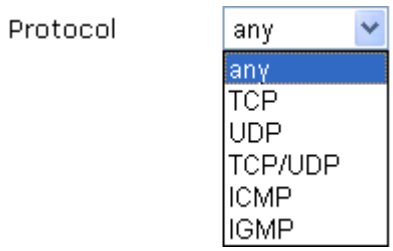
目標通訊埠終點　　顯示目標通訊埠終點的埠號。

上移/下移　　使用**上移**或**下移**連結移動原則的先後順序。

按**索引編號 1** 進入下述頁面設定負載平衡原則。

啓用　　勾選此方塊以啓動此原則。

通訊協定　　使用下拉式選項選擇 WAN 介面適合的通訊協定。



綁定 WAN 介面　　選擇一個 WAN 介面(WAN1 或 WAN2)作爲綁定介面。
Auto failover to other WAN – 當選定的 WAN 介面出現問題時，若您有勾選此按鈕，即可將資料透過另一個 WAN 介面來傳輸。

來源 IP 起點　　輸入指定 WAN 介面的來源 IP 起點位址。

來源 IP 終點　　輸入指定 WAN 介面的來源 IP 終點位址。 如果本區空白，即表示區域網路中全部的來源 IP 位元址都可由此 WAN 介面通過。

目標 IP 起點　　輸入指定 WAN 介面的目標 IP 起點位址。

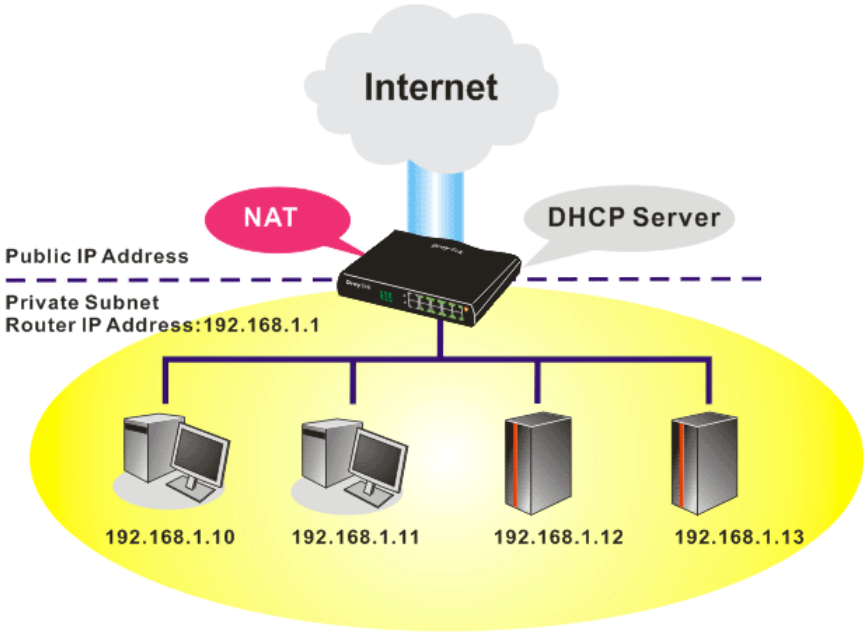
目標 IP 終點	輸入指定 WAN 介面的目標 IP 終點位址。如果本區空白，即表示區域網路中全部的目標 IP 位元址都可由此 WAN 介面通過。
目標通訊埠起點	輸入目標通訊埠的起點埠號。
目標通訊埠終點	輸入目標通訊埠的終點埠號。如果本區空白，即表示區域網路中全部的目標通訊埠都可由此 WAN 介面通過。

4.2 區域網路(LAN)

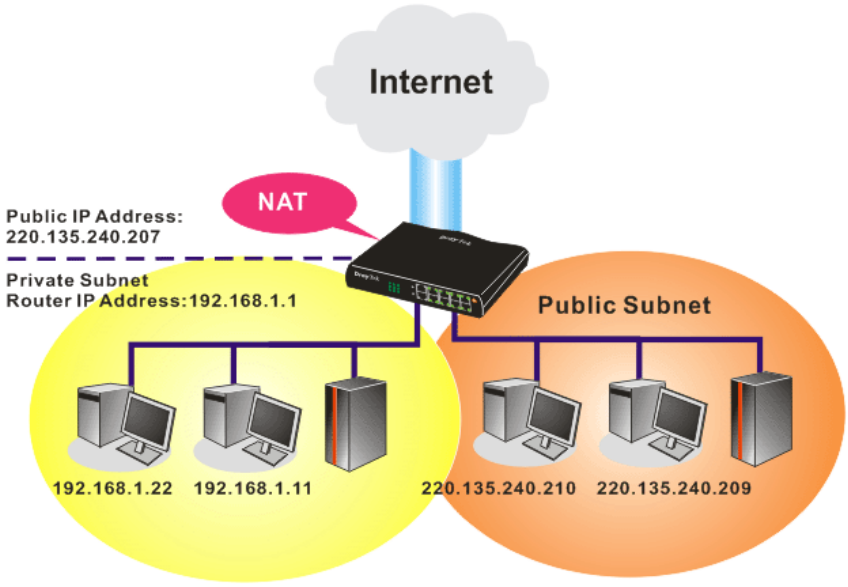
區域網路是由路由器所管理的一群子網路，網路結構設計和您自 ISP 所取得之真實 IP 位址有關。

4.2.1 區域網路基本概念

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



什麼是 RIP(Routing Information Protocol)

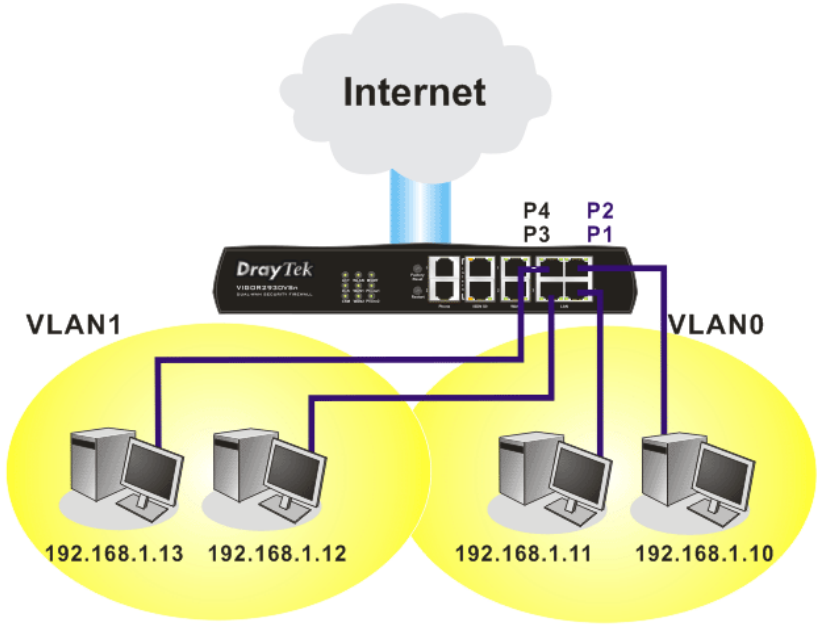
Vigor 路由器可利用 RIP 與鄰近路由器交換路由資訊，達到 IP 路由的目的。這樣可讓使用者變更路由器的資訊，例如 IP 地址，且路由器還會自動通知雙方此類訊息。

什麼是固定路由

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

什麼是虛擬區域網路(VLAN)

您可以利用實體的連接埠將群組區域網路上的主機，然後建立虛擬區域網路，最多可達 4 個。爲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**。

第一 IP 位址 請輸入虛擬 IP 地址以便連接區域虛擬網路(預設值爲 192.168.1.1)。

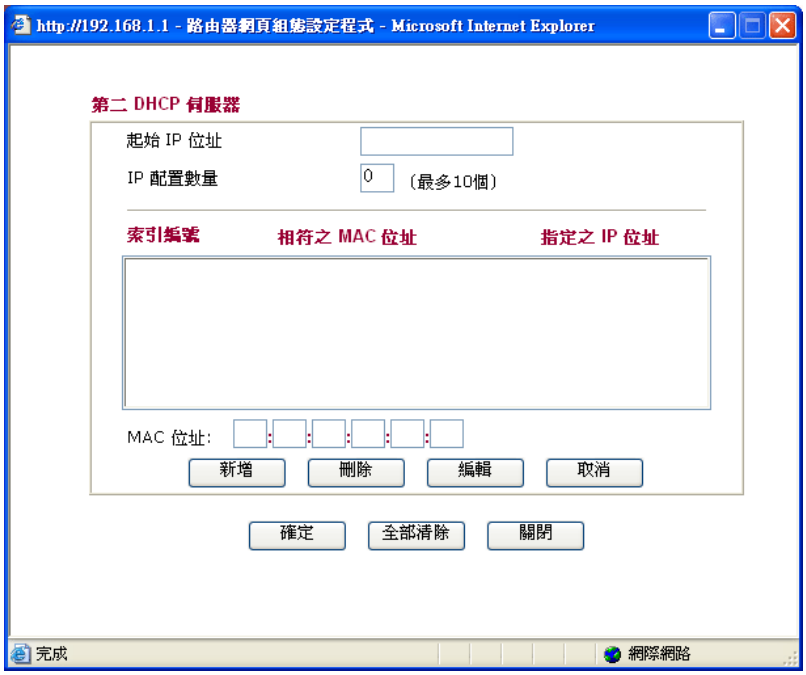
第一子網路遮罩 請輸入決定網路大小的位址碼(預設值爲 255.255.255.0/ 24)。

供 IP 路由使用 按下**啓用**以啓動此功能，此功能預設值是**停用**。此應用視情況需要而設定。

第二 IP 位址 請輸入第二組 IP 地址以便連接至子網路(預設值爲 192.168.2.1)。

第二子網路遮罩 請輸入第二組決定網路大小的位址碼(預設值爲 255.255.255.0/ 24)。

第二子網路遮罩 DHCP 伺服器 您可以將路由器設定爲 DHCP 伺服器，提供服務予第二組子網路。



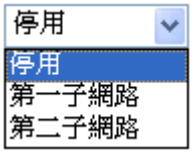
起始 IP 位址：輸入 IP 位址 pool 數值做爲 DHCP 伺服器指定 IP 位址時的起始點，如果路由器的第二組 IP 位址爲 220.135.240.1,，起始 IP 位址可以是 220.135.240.2 或是更高一些，但比 220.135.240.254 小。

IP 配置數量：輸入 IP 地址的數量，最大值爲 10，例如您若輸入 3 而第二組 IP 地址爲 220.135.240.1，DHCP 伺服器的 IP 地址範圍即爲 220.135.240.2 到 220.135.240.4。

MAC 位址：請一個個輸入主機的 MAC 地址，按**新增**來建立主機清單以便指定、刪除或是編輯上述範圍中的 IP 地址。設定第二組 DHCP 伺服器所需的 MAC 位址清單，可幫助路由器指定正確的 IP 地址及子網路至正確的主機上。這樣在第二子網路上的主機便不會得到屬於第一組子網路的 IP 地址。

RIP 協定控制

停用 – 關閉 RIP 協定，可讓不同路由器之間資訊交換暫停 (此爲預設值)。



第一子網路-選擇路由器以交換第一子網路和鄰近路由器間的 RIP 資訊。

第二子網路-選擇路由器以交換第二子網路和鄰近路由器間的 RIP 資訊。

DHCP 伺服器組態

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

If you want to use another DHCP server in the network other than the Vigor Router's, you can let Relay Agent help you to redirect the 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。

啓用 - 讓路由器指定 IP 地址到區域網路上的每個主機上。

停用 – 讓您手動指定 IP 地址到區域網路上的每個主機上。

DHCP 中繼代理位元址 - **(**第一子網路/第二子網路**)** 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。

起始 IP 位址 -輸入 DHCP 伺服器的 IP 位址配置的數值作爲指定 IP 位址的起始點，如果第路由器的第一個 IP 位址爲 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。

IP 配置數量 -輸入您想要 DHCP 伺服器指定 IP 地址的最大數量，預設值爲 50，最大值爲 253。

閘道 IP 位址 -輸入 DHCP 伺服器所需的閘道 IP 位址，這項數值通常與路由器的第一組 IP 位址相同，表示路由器爲預設的閘道。

中繼代理程式 IP 位元址 -設定您預備使用的 DHCP 伺服器 IP 位址，讓中繼代理可以協助傳送 DHCP 需求至伺服器上。

DNS 伺服器組態

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。

使用 DNS 手動設定 – 強迫路由器使用本頁所指定的 DNS 伺服器而非使用網際網路存取伺服器所提供的 DNS 伺服器 (PPPoE, PPTP, L2TP 或 DHCP 伺服器).

主要 IP 位址 -您必須在此指定 DNS 伺服器的 IP 位址，因爲通常您的 ISP 應該會提供一個以上的 DNS 伺服器，如果您的 ISP 並未提供，路由器會自動採用預設的 DNS 伺服器 IP 地址 194.109.6.66，放在此區域。

次要 IP 位址 - 您可以在此指定第二組 DNS 伺服器 IP 位址，因爲 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 位址爲 194.98.0.1，放在此區域。

預設 DNS 伺服器 IP 位址可在線上狀態上查看:

如果主要和次要 IP 地址區都是空白的，路由器將會指定其本身的 IP 位址給予本地使用者作爲 DNS 代理伺服器並且仍保有 DNS 快速緩衝貯存區。

如果網功能變數名稱稱的 IP 位址已經在 DNS 快速緩衝貯存區內，路由器將立即 resolve 網功能變數名稱稱。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。

第五章中舉出常見的區域網路設定腳本供您參考，有關設定範例部份，如有需求請參考該章以取得更多的訊息。

4.2.3 固定路由

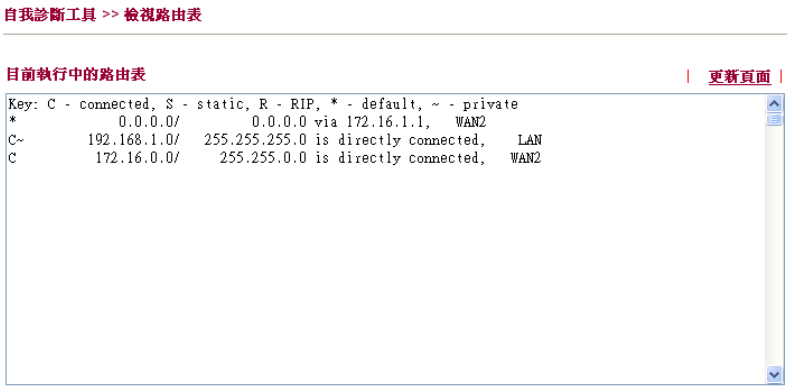
進入**區域網路**群組並選擇**固定路由**，開啓如下的畫面。

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。

檢視路由表 開啓如下畫面檢視目前的路由狀況。

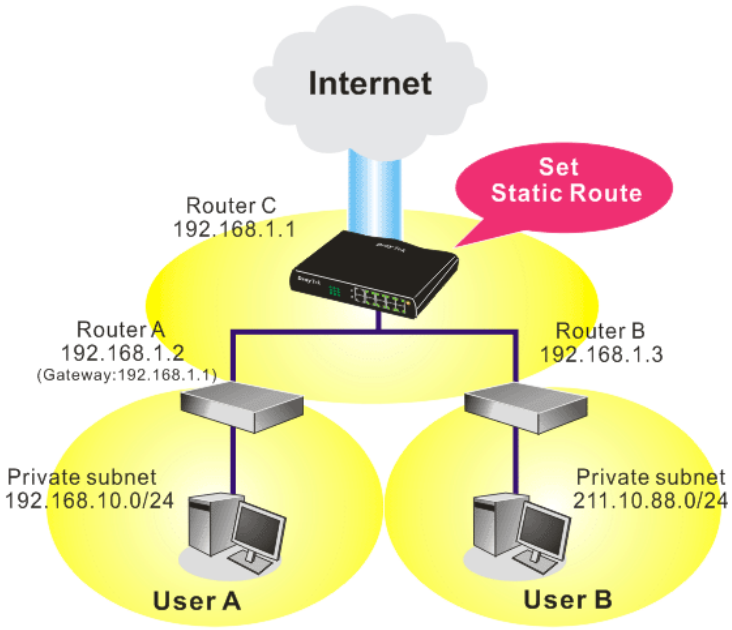


增加固定路由至虛擬或真實網路上

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

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

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



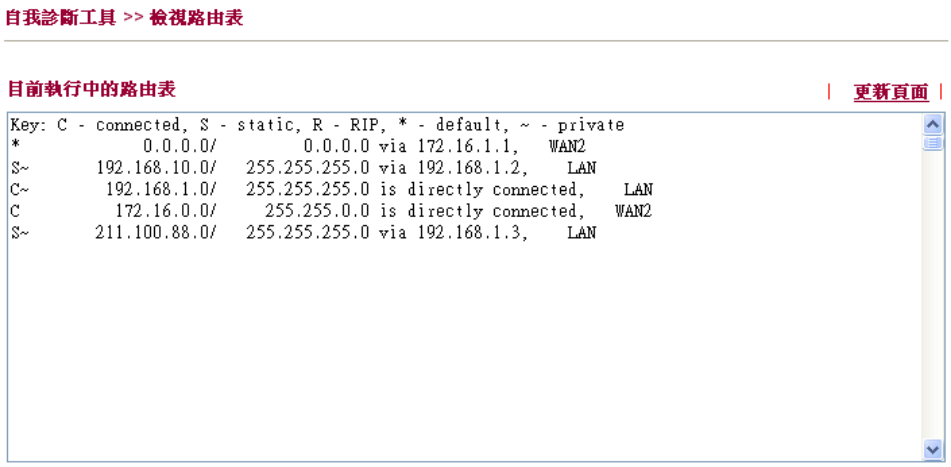
1. 在**區域網路**群組中，選擇**一般設定**。再選擇第一子網路作爲 **RIP 協定控制**，然後點選**確定**按鈕。

> **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**啓用**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**。

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**。

4. 按**自我診斷工具**中的**路由表**檢查目前的路由表格。



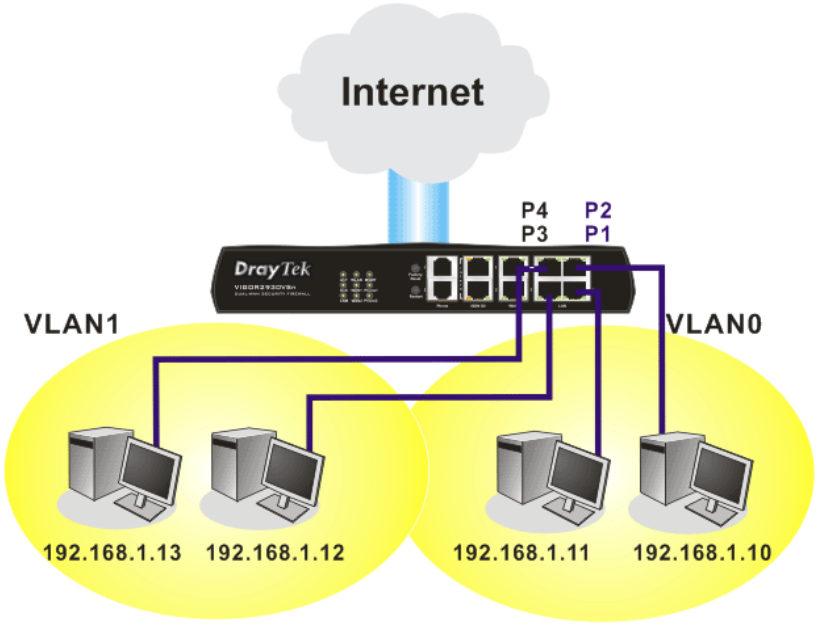
4.2.4 VLAN (虛擬區域網路)

> **注意：**此功能僅適用於 **Vigor2920** 機種，如果您是 Vigor2920n 的用戶，請參考 3.11 一節。

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。

新增或移除 VLAN，請參考下述範例:

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



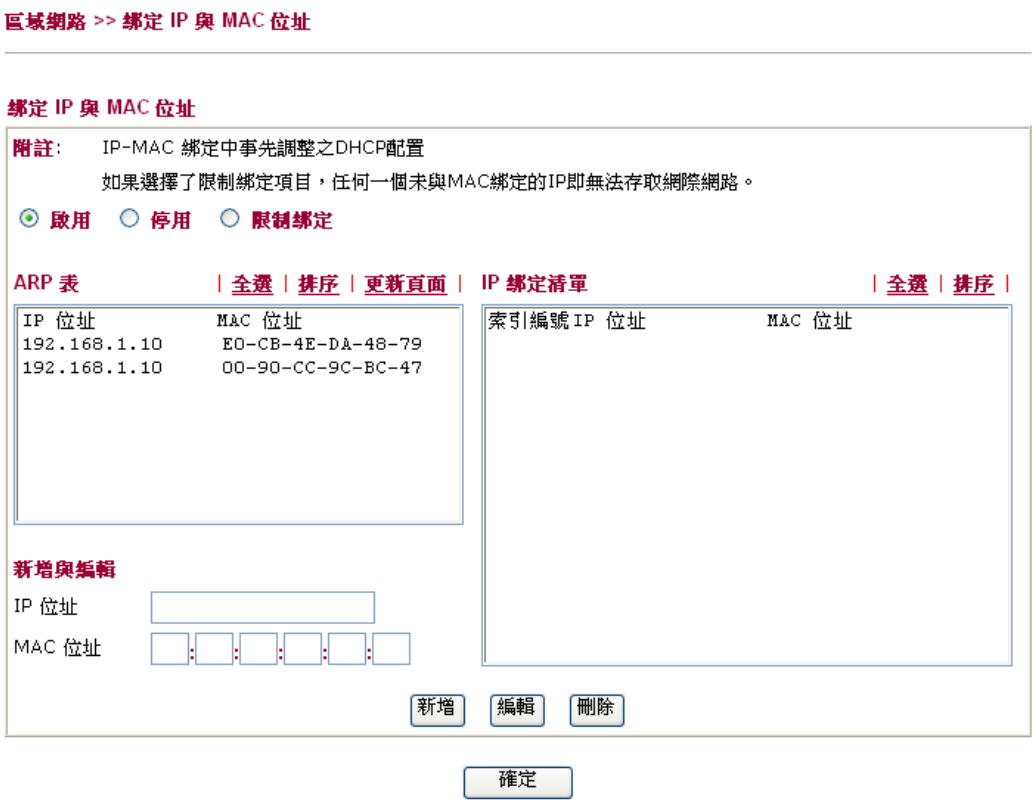
2. 在啓用 VLAN 功能之後，請按照下述範例頁面勾選所需的方塊。

如果要移除 VLAN，請在勾選的方塊上再選一次，然後按**確定**鈕儲存設定。

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。



啓用 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 此表格爲路由器的區域網路 ARP 表，IP 和 MAC 資訊將顯示於本區。列於 ARP 表中的每組 IP 和 MAC 位址都可以爲使用者挑選並透過**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。
新增與編輯	**IP 位址** – 輸入 IP 位址以作爲指定 MAC 位址之用。 **MAC 位址** – 輸入 MAC 位址以便與指定的 IP 位址綁在一起。
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 **IP 綁定清單**上。
編輯	允許您編輯或修正先前所建立的 IP 位址和 MAC 位址。
刪除	您可以刪除 **IP 綁定清單**上任何一個項目，選擇您想刪除的項目然後按**刪除**按鈕，選定的項目將自 **IP 綁定清單**上刪除。

附註: 在您選擇**限制綁定**前，您必須爲一台電腦設定一組 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。

4.3 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，因此您必須爲此負擔費用，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爲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，成爲真實 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：

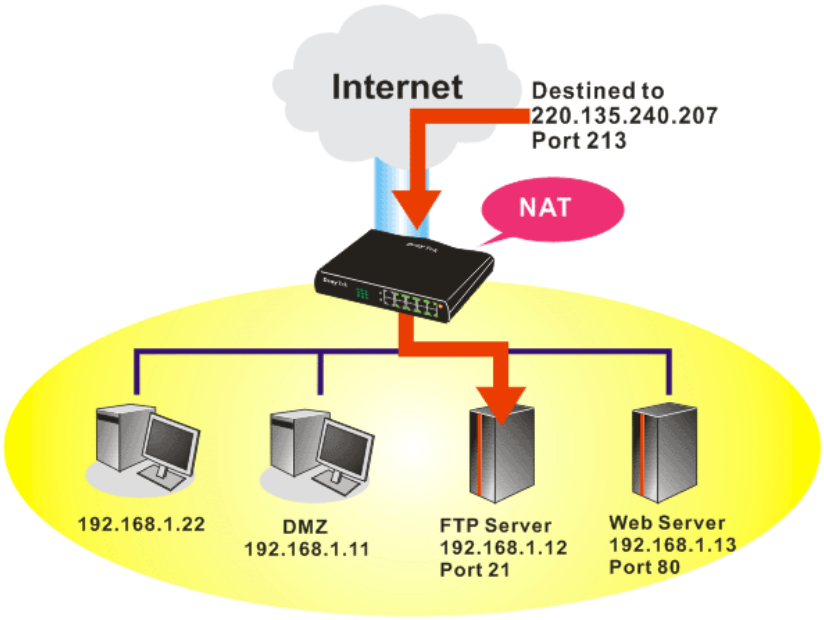
- **於應用真實 IP 位址上節省花費以及有效利用 IP 位址** NAT 允許本機中的 IP 位址轉成真實 IP 位址，如此一來您可以一個 IP 位址來代表本機。
- **利用隱匿的 IP 位址強化內部網路的安全性** 有很多種攻擊行動都是基於 IP 位址而對受害者發動的，既然駭客並不知曉任何虛擬 IP 位址，那麼 NAT 功能就可以保護內部網路不受此類攻擊。

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。

下圖爲 NAT 功能項目：

4.3.1 通訊埠重導向

通訊埠重導向通常是爲了本地區域網路中的網頁伺服器、FTP 伺服器、E-mail 伺服器等相關服務而設定，大部分的情形是您需要給每個伺服器一個真實 IP 位址，此一真實 IP 位址/網功能變數名稱稱可以爲所有使用者所辨識。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	對外通訊埠	虛擬 IP	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 >>

按下索引編號下的號碼連結，進入次層之設定頁面:

啓用 勾選此方塊啓用此通訊埠重導向設定。

模式 有二種模式可以供使用者選擇，如欲設定範圍給予指定服務，請選擇**範圍**。在"範圍" 模式下，若 IP 位元址與第一個對外通訊埠號皆填入之後，系統將自動計算並顯示第二個對外通訊埠值。

服務名稱 輸入特定網路服務的名稱。

通訊協定 選擇傳送層級的通訊協定(TCP 或 UDP)。

WAN 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**全部**，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**範圍**作爲重導向模式，您將會在此看見二個方塊，請在第一個方塊輸入需要的數值，系統將會自動指定數值予第二個方塊。

虛擬 IP 指定提供服務的主機之 IP 位址，如果您選擇**範圍**作爲重導向模式，您將會在此看見二個方塊，請在第一個方塊輸入完整的 IP 位址 (作爲起點)，在第二個方塊輸入四位數字(作爲終點)。

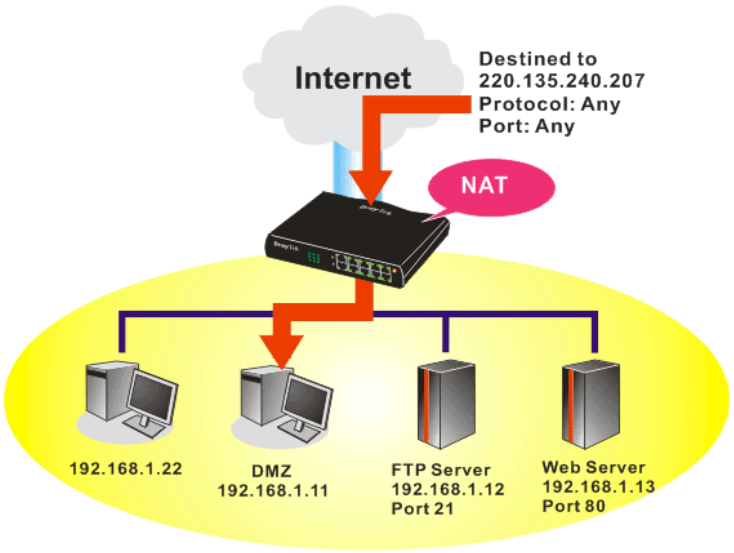
虛擬通訊埠 指定內部主機提供服務之虛擬通訊埠號。

注意路由器有其內建服務(伺服器)諸如 Telnet、HTTP 和 FTP，因爲這些服務(伺服器)的通訊埠號幾乎都相同，因此您可能需要重新啓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。

4.3.2 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：

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。

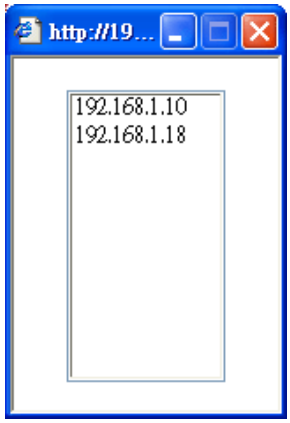
開啓 勾選此項以啓動 DMZ 主機功能。

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**選擇 PC** 開啓另一頁面來選擇。

選擇電腦 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

爲 DMZ 主機。



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

4.3.3 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。

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。

啓用開放通訊埠	勾選此項以啓動此功能。
說明	請爲所定義的網路應用/服務命名。
WAN 介面	指定該項設定之 WAN 介面。
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 位元址。
本機電腦	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。

4.4 防火牆

4.4.1 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：

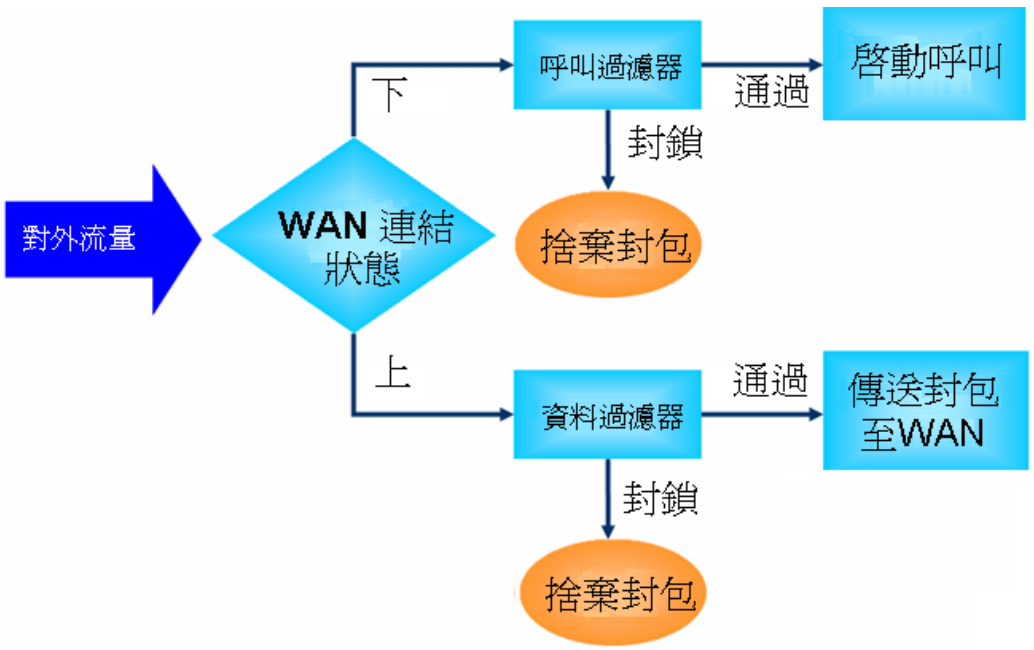
- 用戶設定 IP 過濾器(呼叫過濾器/資料過濾器)
- Stateful Packet Inspection (SPI): 追蹤封包並阻擋未經要求而流入的資料
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS)攻擊防禦

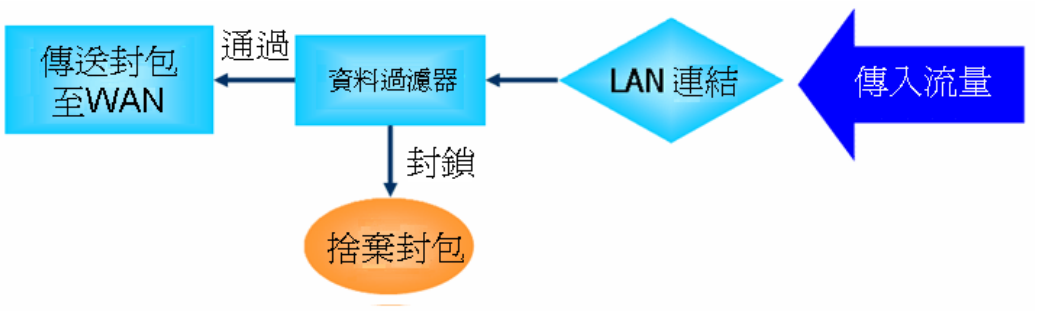
IP 過濾器

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爲基礎，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)，都會被視爲是一種攻擊行爲，Vigor 路由器將啓動防衛機制，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
2. UDP flood 攻擊
3. ICMP flood 攻擊
4. Port Scan 攻擊
5. IP options
6. Land 攻擊
7. Smurf 攻擊
8. 路由追蹤
9. SYN 封包片段攻
10. Fraggle 攻擊
11. TCP flag scan
12. Tear drop 攻擊
13. Ping of Death 攻擊
14. ICMP 封包片段攻
15. 未知通訊協定

下圖爲防火牆的功能項目：

4.4.2 基本設定

基本設定允許您調整 IP 過濾器和一般選項的設定內容，在此頁面您可以啓動或是關閉**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**。

自**防火牆**群中選擇**基本設定**連結。

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。

過濾器 本頁可是定預設規則.
通過 – 所有的封包都可通過路由器，不需考慮**防火牆>>過濾器**的設定內容。
封鎖 - 所有的封包都不許通過路由器，且不需考慮**防火牆>>過濾器**的設定內容。

IM/P2P 過濾器 選擇一個數位內容安全管理(CSM)設定檔作爲 IM/P2P 應用封鎖的依據，所有 LAN 中的主機必須依循此處所選擇的 CSM 設定檔的標準來進行。詳細的內容，可參考 CSM 設定檔單元，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。

URL 內容過濾器

選擇一個 **URL 內容過濾器**設定檔（在**數位內容安全管理(CSM)>> URL 內容過濾器**中所建立），請務必先在**數位內容安全管理(CSM)> URL 內容過濾器**中設定一個設定檔。因應疑難排解的需要，您可勾選紀錄方塊以便將資訊記錄起來，這些紀錄會傳送到 Syslog 伺服器，詳情請參考 Syslog/郵件警告章節。

網頁內容過濾器

選擇一個**網頁內容過濾器**設定檔（在**數位內容安全管理(CSM)>> 網頁內容過濾器**中所建立），請務必先在**數位內容安全管理(CSM)>> 網頁內容過濾器**中設定一個設定檔。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

Syslog

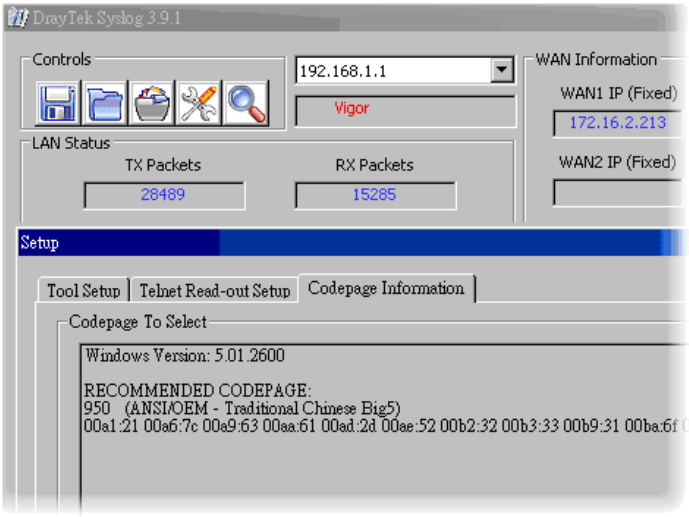
因應疑難排解的需要，您可勾選紀錄方塊以便將資訊記錄起來，紀錄將呈現在 Draytek Syslog 視窗中。

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爲佳。

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。預設值爲 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，不過網路會較爲不穩定，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。

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優遊。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。

4.4.3 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。

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。

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。

啓用過濾規則 勾選此項目以啓動過濾規則。

註解 輸入過濾器設定註解說明，最大長度爲 14 個字元。

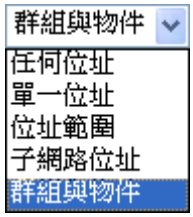
索引號碼 (1-15) 設定區域網路上的電腦工作的時間間隔，您可以輸入四組時間排程，所有的排程都可在**應用-排程**網頁上事先設定完畢，然後在此輸入該排程的對應索引號碼即可。

方向 設定封包流向的方向(LAN->WAN/WAN->LAN)，此項設定僅適用**資料過濾器**，對於呼叫過濾器而言，這項設定是不適用的。

來源/目的 IP 按下**編輯**進入如下的畫面，選擇來源/目標 IP 或是 IP 範圍。

欲手動設定 IP 位址，請選擇**任何位址/單一位址/範圍位址/子網**

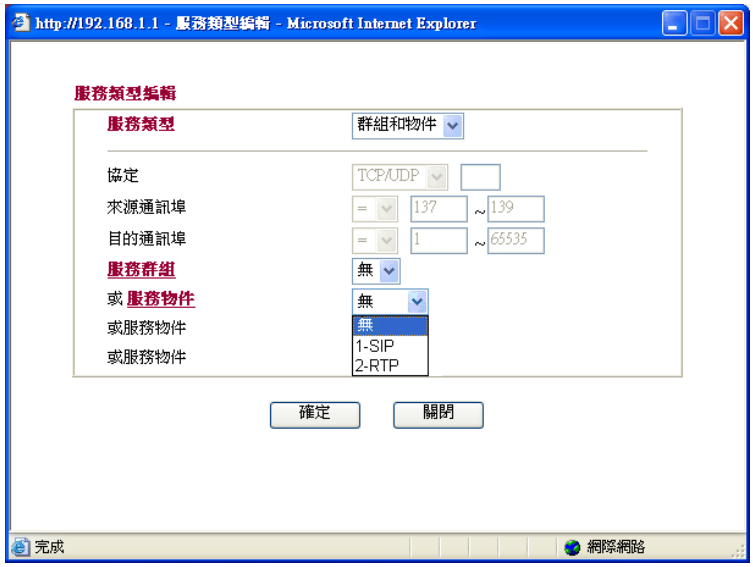
位址作爲位址類型，並在此對話方塊輸入相關內容。此外，如果您想要在定義的群組或物件上使用 IP 範圍，請勾選**群組及物件**。



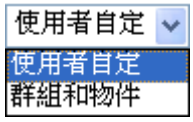
從 **IP 群組**下拉式清單中，選擇您需要應用的群組，或是使用 **IP 物件**下拉式清單，選擇您所需要的物件。

服務類型

按**編輯**進入如下的畫面，以選擇適合之服務類型。



欲手動設定服務類型，請選擇使用者自訂做爲服務類型，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**作爲服務類型。



協定 -指定本過濾器規則套用的協定。

來源/目標通訊埠 -

(=) – 當起始埠號與結束埠號與的數值相同時，此符號表示一個通訊埠。當起始埠號與結束埠號的數值不同時，即表示設定檔所適用的通訊埠範圍。

(!=) –當起始埠號與結束的數值相同時，此符號表示除了這裡所指明的通訊埠以外，全都適用於此設定檔。當起始埠號與結束埠號數值不同時，即除了此處所設定的範圍以外，所有的通訊埠都適用於此設定檔。

(>) – 大於此數值的通訊埠號皆可使用。

(<) – 小於此數值的通訊埠號皆可使用。

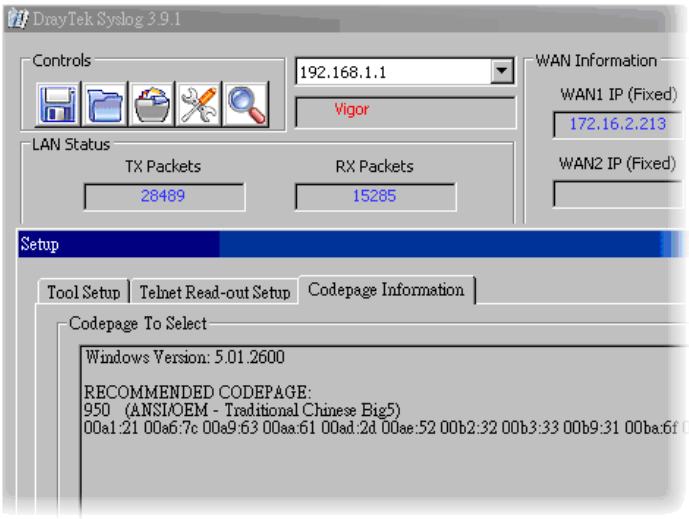
服務群組/物件 - 使用下拉式選項選擇所需的項目。

片段	指定片段封包的執行動作，這個項目也是僅針對**資料過濾器**。 **忽略** - 不論是怎樣的片端封包，系統皆不採取行動。 **無片段** - 應用規則至無片段之封包上。 **片段**- 應用規則至片段之封包上。 **太短了** - 只有過短無法包含完整封包頭之封包，可應用此規則。
過濾器	指定系統針對符合規則之封包所採取的行動。 **立刻通過**- 符合規則之封包可立即通過。 **立刻封鎖** - 系統封鎖符合規則之封包。 **若無符合其於規則即通過** - 符合限定規則且並未符合其他規則之封包可立即通過。 **若無符合其於規則即封鎖** - 系統封鎖符合限定規則且並未符合其他規則之封包。 基於疑難排除的需要，您可指定記錄過濾器資訊，只要勾選 **Syslog** 方框即可。
分至其他過濾器設定	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。
IM/P2 過濾器/ URL 內容過濾器/ 網頁內容過濾器	上述條件所設定範圍內所有的封包/連線都必須依照此處所選擇的設定檔的標準進行，詳細資訊，請參考數位內容安全管理(CSM)設定。
SysLog	基於疑難排除的需要，您可指定記錄過濾器及 CSM 紀錄等資訊，請勾選相關的方塊啓用此紀錄功能。接著您可在 Draytek Syslog 視窗中看到過濾器紀錄及/或 CSM 紀錄。
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爲佳。

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。預設值爲 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。

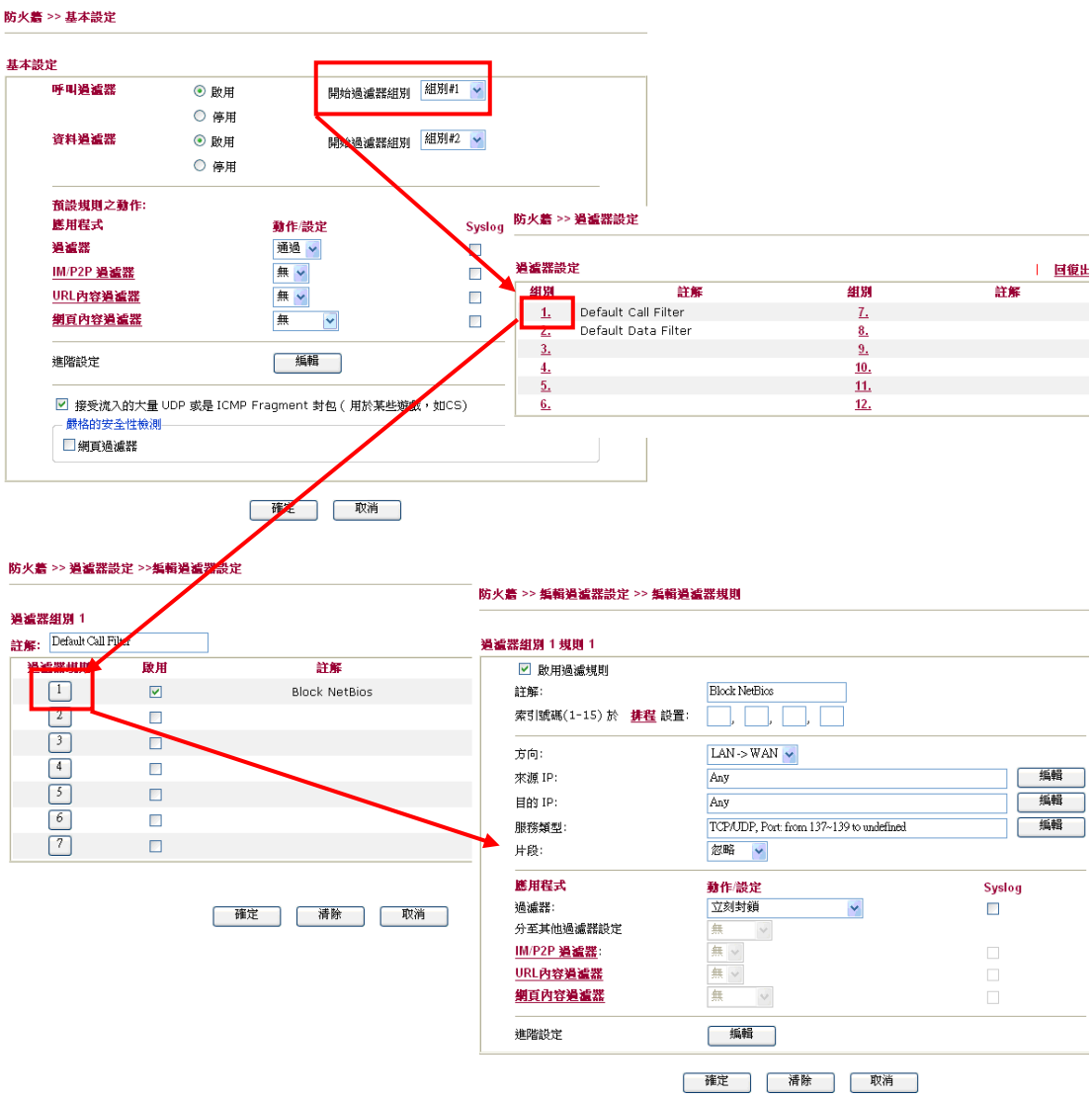


視窗大小 – 決定 TCP 協定的大小(0~65535)，數值越大，成效越佳，不過網路會較爲不穩定，小的數值比較適合穩定網路。

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。

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。



4.4.4 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。

啓用 勾選此項以啓動 DoS 攻擊防禦功能。

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爲每秒 50 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爲每秒 150 個封包和 10 秒。

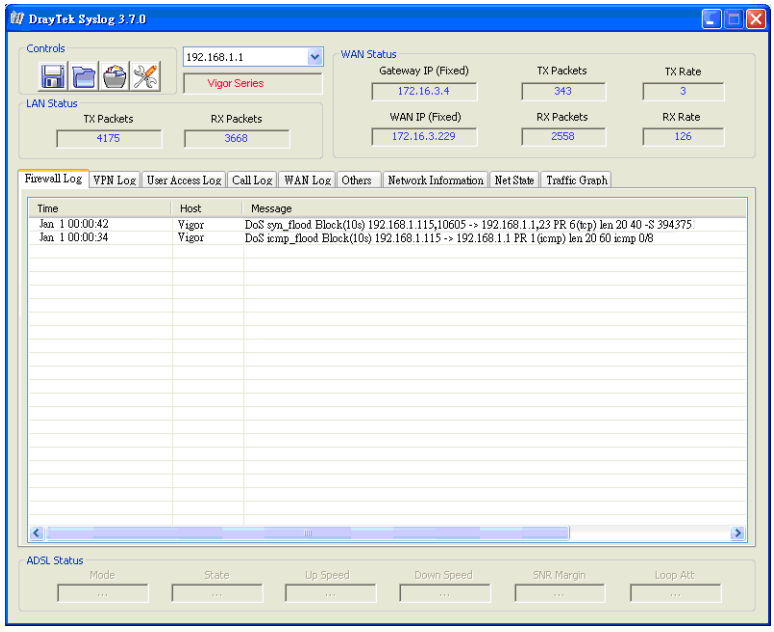
啓用 ICMP Fragment 封包 勾選此項以啓動 ICMP Fragment 封包，與 UDP 攻擊防禦功能相同的是，一旦檢查到 ICMP 封包臨界值超過定義數值，路由器便會於所設定之逾時期間，不再回應來自網際網路的 ICMP 需求。臨界值和逾時的預設值分別爲每秒 50 個封包和 10 秒。

啓用防禦通訊埠掃瞄偵測功能 通訊埠掃瞄藉由傳送大量封包到數個通訊埠，以嘗試找出未知服務所回應之內容來攻擊 Vigor 路由器。勾選此方塊啓動通訊埠掃瞄檢測功能，當利用通訊埠掃瞄臨界值速率而檢測出惡意探測之行爲時，Vigor 路由器將傳送警告訊息出去。臨界值的

	預設值爲每秒 150 個封包。
封鎖 IP options	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。
封鎖 Land 攻擊	勾選此項以強迫 Vigor 路由器防護 Land 攻擊，Land 攻擊結合含 IP spoofing 的 SYN 攻擊技術，當駭客傳送 spoofed SYN 封包(連同相同來源和目的位元址)，以及通訊埠號至受害一方時，Land 攻擊即由此發生。
封鎖 Smurf 攻擊	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。
封鎖路由追蹤	勾選此項以強迫 Vigor 路由器不轉送任何路由封包的行蹤。
封鎖 SYN Fragment 封包	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。
封鎖 Fraggle 攻擊	勾選此項以啓動封鎖 Fraggle 攻擊功能，任何播送來自網際網路的 UDP 封包都會被封鎖起來。 啓動 DoS/DDoS 防禦功能可能會阻擋一些合法的封包，例如當您啓動 fraggle 攻擊防禦時，所有來自網際網路的 UDP 封包播送都會被阻擋在外，因此得自網際網路的 RIP 封包全都會被阻擋掉。
封鎖 TCP Flags scan	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 *no flag scan, FIN without ACK scan, SYN FINscan, Xmas scan* 以及 *full Xmas scan* 等等。
封鎖 Tear Drop 攻擊	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。
封鎖 Ping of Death 攻擊	勾選此項以啓動封鎖 Ping of Death 攻擊功能，這項攻擊意味著犯罪者傳送重疊封包至目的主機，這些目的主機一旦重新建構封包時就會造成當機現象，Vigor 路由器將會阻擋此種攻擊活動的封包進入。
封鎖 ICMP 封包片段攻擊	勾選此項以啓動封鎖 ICMP 封包片段功能，任何含有多個片段的 ICMP 封包都會被捨棄阻擋。
封鎖不明封包協定封包	勾選此項以啓動封鎖不明封包協定封包功能，個別 IP 封包在資料段封包頭中都擁有一個協定區域，指名該協定於上層運作的類型。
警告訊息	我們提供使用者系統記錄功能以便檢視路由器發出的訊息。作爲系統紀錄伺服器，使用者可接收來自路由器(系統紀錄用戶端)傳送之報告。 所有與 DoS 攻擊有關的警告訊息都將傳送與使用者，使用者可以重新檢查其內容，在訊息中尋找關鍵字，所遭受的任何攻擊之名

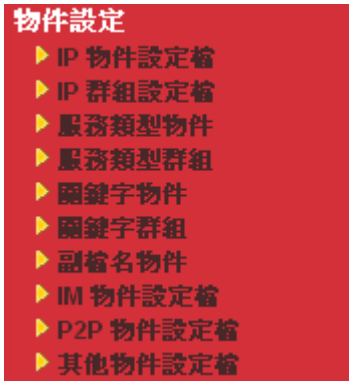
稱即可立即檢測出來。


系統維護 >> Syslog / 郵件警示設定
Syslog / 郵件警示設定
Syslog 存取設定
啟用
伺服器 IP 位址
目的通訊埠
514
啟用 Syslog 訊息:
防火牆記錄
VPN 記錄
使用者網路存取紀錄
通話紀錄
WAN 記錄
路由器/DSL資訊
郵件警示功能設定
啟用
傳送測試郵件
SMTP 伺服器
收件人
回信地址
驗證
使用者名稱
密碼
啟用郵件警告訊息:
DoS 攻擊
IM-P2P
確定
清除
取消


DrayTek Syslog 3.7.0
Controls
192.168.1.1
Vigor Series
WAN Status
Gateway IP (Fixed)
172.16.3.4
TX Packets
343
TX Rate
3
LAN Status
TX Packets
4175
RX Packets
3668
WAN IP (Fixed)
172.16.3.229
RX Packets
2558
RX Rate
126
Firewall Log
VPN Log
User Access Log
Call Log
WAN Log
Others
Network Information
Net State
Traffic Graph
Time
Host
Message
Jan 1 00:00:42
Vigor
DoS syn_flood Block(10s) 192.168.1.115,10605 -> 192.168.1.1,23 PR 6(tcp) len 20 40 -S 394375
Jan 1 00:00:34
Vigor
DoS icmp_flood Block(10s) 192.168.1.115 -> 192.168.1.1 PR 1(icmp) len 20 60 icmp 0/8
ADSL Status
Mode
State
Up Speed
Down Speed
SNR Margin
Loop Att

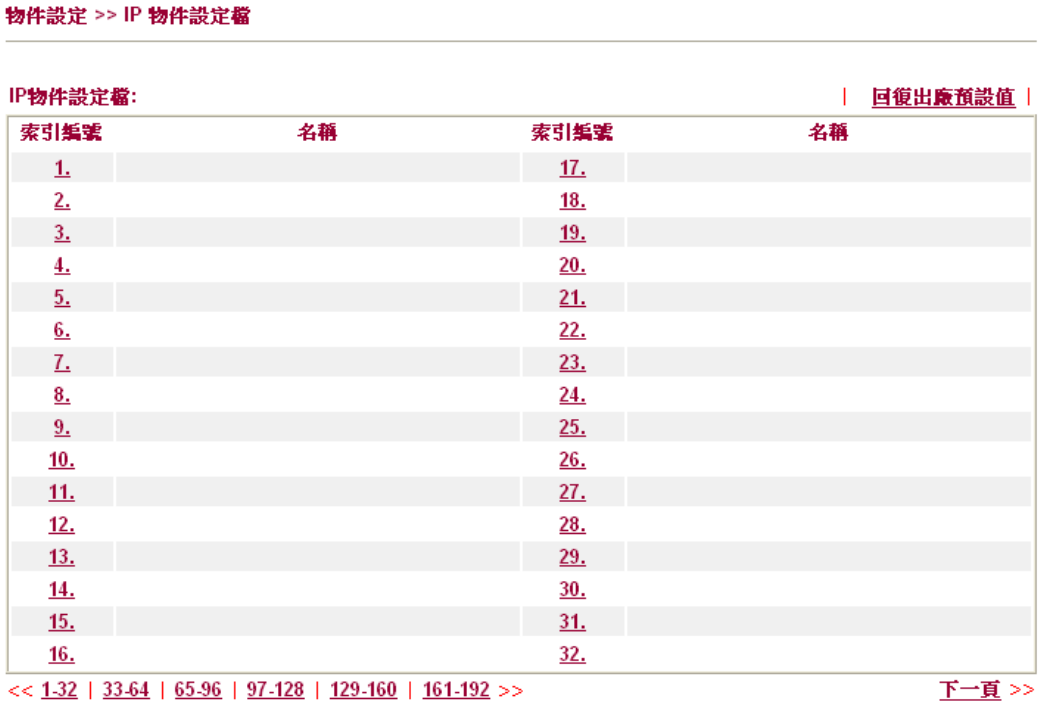
4.5 物件和群組

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)。



4.5.1 IP 物件設定檔

您可設定 192 組不同條件的 IP 物件。



回復出廠預設值　　清除全部的設定資料。

按下任一索引號碼進入下述畫面：

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)。

例如，**編輯過濾器規則**中的**方向**設定會要求您針對 WAN 或 LAN 介面指定一個 IP 或是 IP 範圍，或是任何的 IP 位址，如果您選擇 LAN 作爲介面，並選擇 LAN 作爲**編輯過濾器規則**中的**方向**設定，那麼所有的 LAN 介面的 IP 位址通通都會開放予您在**編輯過濾器規則**頁面上選擇。

位址類型 決定 IP 位址的位址類型。
如果物件僅包含 IP 位址的話，請選擇**單一位址**。
如果物件包含某個範圍內數個 IP 位址的話，請選擇**範圍位址**。
如果物件包含 IP 位址的子網路的話，請選擇**子網路位址**。
如果物件包含任何一種 IP 位址的話請選擇**任何位址**。

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。

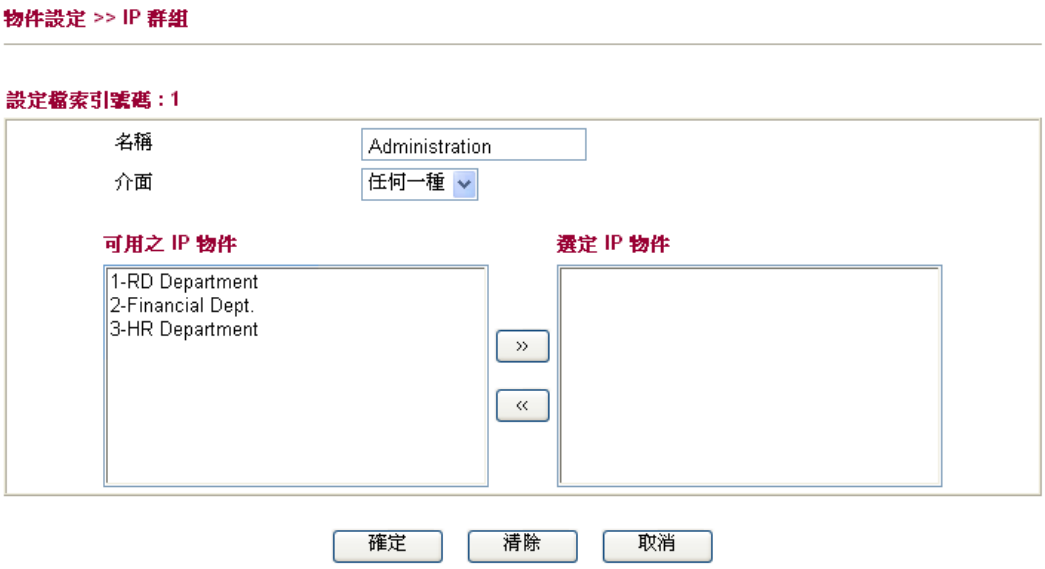
下表爲 IP 物件設定的範例之一。

4.5.2 IP 群組

本頁可讓您綁定數個 IP 物件成爲一個 IP 群組。

回復出廠預設值 清除全部的設定資料。

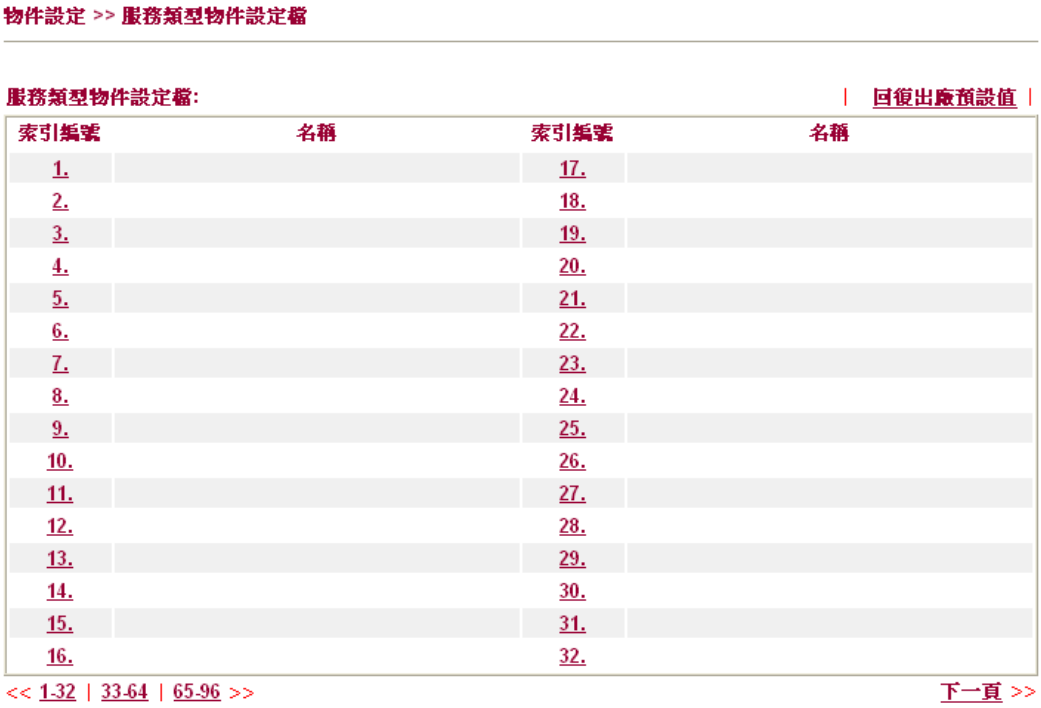
按下任一索引號碼以便完成詳細設定。



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。

4.5.3 服務類型物件

您可設定 96 組不同條件的服務類型物件。

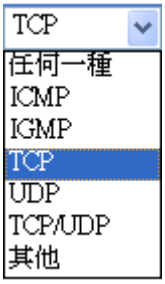


回復出廠預設值 清除全部的設定資料。

按下任一索引號碼進入下述畫面：

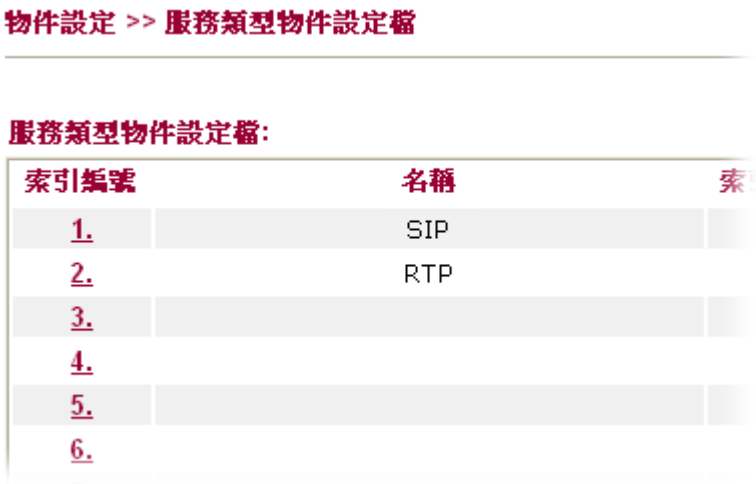
名稱 輸入此設定檔的名稱。

介面 請選擇此設定檔所要套用的適當介面。



來源/目標通訊埠	**來源通訊埠**與**目標通訊埠**欄位皆爲 TCP/UDP 可用之通訊埠，如果是其他的通訊協定，這些欄位即可省略，過濾器規則將可過濾任何一種通訊埠號。 ***(=)*** – 當第一與最後的數值相同時，此符號表示一個通訊埠。當第一與最後的數值不同時，此符號表示此設定檔所適用的通訊埠號範圍。 ***(!=)*** –當第一與最後的數值相同時，此符號表示除了這裡所指明的通訊埠以外，全都適用於此設定檔。當第一與最後的數值不同時，此符號表示所有的通訊埠除了此處所設定的範圍以外，全都適用於此設定檔。 ***(>)*** – 大於此數值的通訊埠號皆可使用。 ***(<)*** – 小於此數值的通訊埠號皆可使用。

下表爲服務類型物件設定的範例之一。



4.5.4 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。

回復出廠預設值 清除全部的設定資料。

按下任一索引號碼進入下述畫面：

名稱 輸入此設定檔名稱。

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。

4.5.5 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**中選擇作爲黑白名單之用。

回復出廠預設值 清除全部的設定資料。

按下任一索引號碼進入下述畫面：

名稱 請輸入此設定檔名稱，例如 game。

內容 輸入此設定檔的實際內容，例如可輸入 gambling。當您瀏覽網頁時，含有 gambling (賭博)等訊息之頁面就會被砍掉，並依照防火牆對此的設定放行/封鎖。

4.5.6 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**中選擇作爲黑白名單之用。

回復出廠預設值　　清除全部的設定資料。

按下任一索引號碼進入下述畫面：

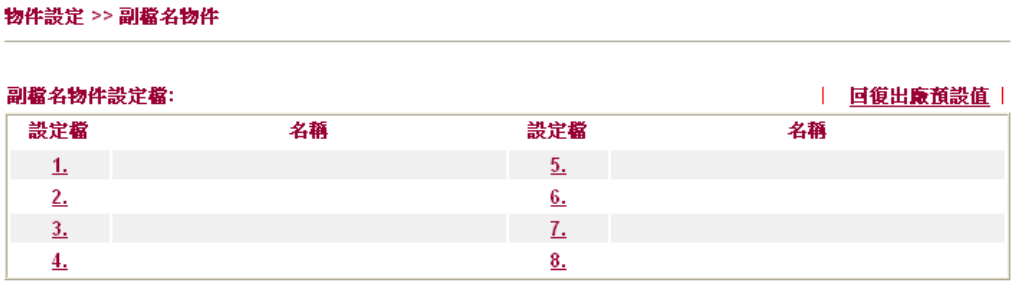
名稱　　輸入此群組名稱。

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。

4.5.7 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。



回復出廠預設值 清除全部的設定資料。

按下任一索引號碼進入下述畫面：

設定檔名稱 請輸入此設定檔名稱。

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。

4.5.8 IM 物件設定檔

本頁允許您設定 32 個即時通訊的設定檔，這些設定檔可應用在**數位內容安全管理(CSM)>>IM/P2P 過濾器設定檔**中做爲過濾之依據。

回復出廠預設值　　清除全部的設定資料。

按設定檔欄位下方的號碼，開啓次一層頁面。目前有數種關於即時通訊的項目提供給您選擇以便阻止用戶使用。請勾選各個不同應用名稱方塊，再按下**確定**即可。稍後，在**數位內容安全管理(CSM)>>IM/P2P 過濾器設定檔**頁面中，您可使用 **IM 物件**下拉式清單選擇適宜的設定檔作爲主機遵循的標準。

設定檔名稱　　請輸入此設定檔名稱。

輸入設定檔名稱並勾選主機將會使用的項目，然後按**確定**儲存本頁的設定。

4.5.9 P2P Object

本頁允許您針對點對點應用設定 32 組設定檔，這些設定檔可應用在**數位內容安全管理(CSM)>>IM/P2P 過濾器設定檔**中做爲過濾之依據。

回復出廠預設值　　清除全部的設定資料。

按設定檔欄位下方的號碼，開啓次一層頁面。目前有數種關於點對點協定的項目提供給您選擇以便阻止用戶使用。請勾選各個不同應用名稱方塊，再按下**確定**即可。稍後，在**數位內容安全設定(CSM)>>IM/P2P 過濾器設定檔**頁面中，您可使用**點對點物件**下拉式清單選擇適宜的設定檔作爲主機遵循的標準。

設定檔名稱　　請輸入此設定檔名稱。

輸入設定檔名稱並勾選不允許主機使用的協定項目，然後按**確定**儲存本頁的設定。

4.5.10 其他物件

本頁允許您針對其他應用設定 32 組設定檔，這些設定檔可應用在 **CSM>>其他過濾器設定檔**中做爲過濾之依據。

回復出廠預設值　　清除全部的設定資料。

按設定檔欄位下方的號碼，開啓次一層頁面。目前有數種關於 tunneling 及 streaming 的項目提供給您選擇以便阻止用戶使用。請勾選各個不同應用名稱方塊，再按下**確定**即可。稍後，在**數位內容安全管理(CSM)>>其他過濾器設定檔**頁面中，您可使用**其他物件**下拉式清單選擇適宜的設定檔作爲主機遵循的標準。

設定檔名稱　　請輸入此設定檔名稱。

輸入設定檔名稱並勾選不允許主機使用的協定項目，然後按**確定**儲存本頁的設定。

4.6 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。

IM/P2P 過濾器設定檔

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爲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，這是因爲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，因爲檔案分享可以很方便但是同時也很危險。爲了應付這些需求，我們提供了 CSM 阻擋功能。

URL 內容過濾器

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

一旦使用者輸入關鍵字連結，URL 關鍵字阻擋工具將會拒絕該網頁之 HTTP 需求，如此一來使用者即無法存取該網站。您可以這樣想像一下，URL 內容過濾器爲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 內容過濾器爲什麼可以比傳統防火牆在過濾方面提供更好的服務呢？那是因爲它能夠檢查 URL 字串或是一些隱藏在 TCP 封包負載的 HTTP 資料，而一般防火牆僅能以 TCP/IP 封包標頭來檢測封包。

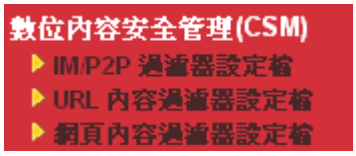
換言之，Vigor 路由器可以防止使用者意外自網頁下載惡意的程式碼。惡意碼隱藏在執行物件當中是一件很普遍的事情，像是 ActiveX、Java Applet、壓縮檔和其他執行檔案。一旦用戶下載這些類型的檔案，用戶便會有這些可能爲系統帶來威脅的風險，例如一個 ActiveX 控制物件通常用於提供網頁人機通信交換功能，萬一裡面隱藏惡意的程式碼的話，該程式碼就可能會佔據使用者的系統。

網頁內容過濾器

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

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



4.6.1 IM/P2P 過濾器設定檔

您可定義不同的策略設定檔案，以因應即時通訊及點對點應用之需要，CSM 設定檔可以在**過濾器設定**頁面中使用。

回復出廠預設值　　清除全部的設定資料。

按索引下方的號碼連結開啓如下視窗進行細節設定。

設定檔名稱　　請輸入此 CSM 設定檔名稱。

每個設定檔包含數種物件設定，IM 物件、P2P 物件協定物件及其他物件。此設定檔將應用於**防火牆>>基本設定**與**防火牆>>過濾器設定**頁面，做爲主機依循的標準。

4.6.2 URL 內容過濾器設定檔

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

一旦使用者輸入關鍵字連結，URL 關鍵字阻擋工具將會拒絕該網頁之 HTTP 需求，如此一來使用者即無法存取該網站。您可以這樣想像一下，URL 內容過濾器爲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 內容過濾器爲什麼可以比傳統防火牆在過濾方面提供更好的服務呢？那是因爲它能夠檢查 URL 字串或是一些隱藏在 TCP 封包負載的 HTTP 資料，而一般防火牆僅能以 TCP/IP 封包標頭來檢測封包。

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

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

此外，Vigor 路由器也會捨棄任何嘗試取回這些惡意程式碼的需求。

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

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。

設定檔名稱

請輸入此設定檔名稱。

優先權

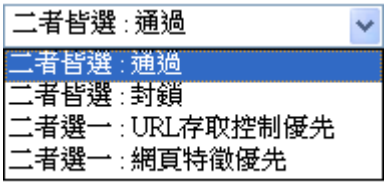
決定路由器採用的動作順序。

二者皆選:通過 – 路由器讓符合 URL 存取控制與網頁特徵所指定條件的封包放行通過，當您選擇此項設定時，本頁針對 URL 存取控制與網頁特徵所設定的限制都將暫停作用。

二者皆選:封鎖 – 路由器封鎖住任何符合 URL 存取控制與網頁特徵所指定條件的封包，當您選擇此項設定時，本頁針對 URL 存取控制與網頁特徵所設定的限制都將暫停作用。

二者擇一: URL 存取控制優先 – 當所有封包皆符合 URL 存取控制與網頁特徵之設定條件時，此功能可以決定先執行的動作爲何。針對此項，路由器將先處理符合 URL 存取控制設定條件下的封包，然後再處理符合網頁特徵條件的封包。

二者擇一: 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爲何。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。



紀錄

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。

URL 存取控制

啓用 URL 存取控制 - 勾選此方塊啓動 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。

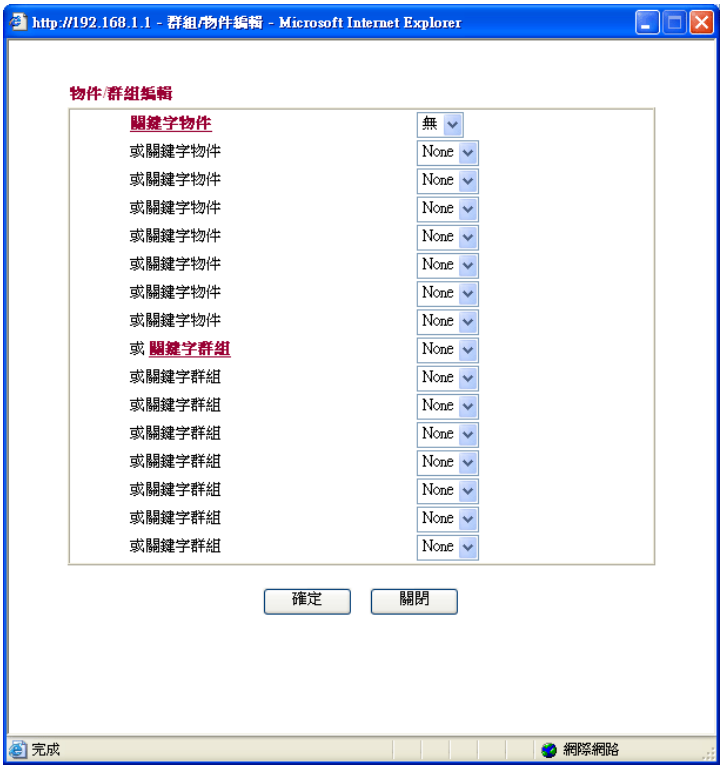
防止從 IP 位址存取網頁- 勾選此方塊拒絕任何使用 IP 位址例如 http://202.6.3.2 來要求存取資料的活動，這個項目可以防止他人躲避 URL 存取控制的監控，您必須先清除瀏覽器的快取資料，讓 URL 內容過濾器工具能夠在您所造訪的網頁上適當的操作。

動作 – 此功能僅在您選擇了**二擇一: URL 存取控制優先**或**二擇一: 網頁特徵優先**時才能使用。

通過 - 允許進入含有關鍵字清單中之關鍵字的網頁。

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。

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爲 32 個字元。指定完關鍵字後，Vigor 路由器將婉拒符合任何使用者定義的關鍵字之網頁的 URL 連線需求。注意，封鎖的關鍵字寫得越簡化，Vigor 路由器執行起來也會更加有效率。



網頁特徵

啓用限制網頁特徵 - 勾選此方塊讓關鍵字被封鎖或是放行。

動作 - 此功能僅在您選擇了**二者選一: URL 存取控制優先**或**二者選一: 網頁特徵優先**時才能使用。
通過 - 允許進入含有關鍵字清單中之關鍵字的網頁。
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。

Cookie - 勾選此方塊從內部到外部過濾 cookie 傳輸資料以保護本地用戶的隱私。

Proxy - 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。

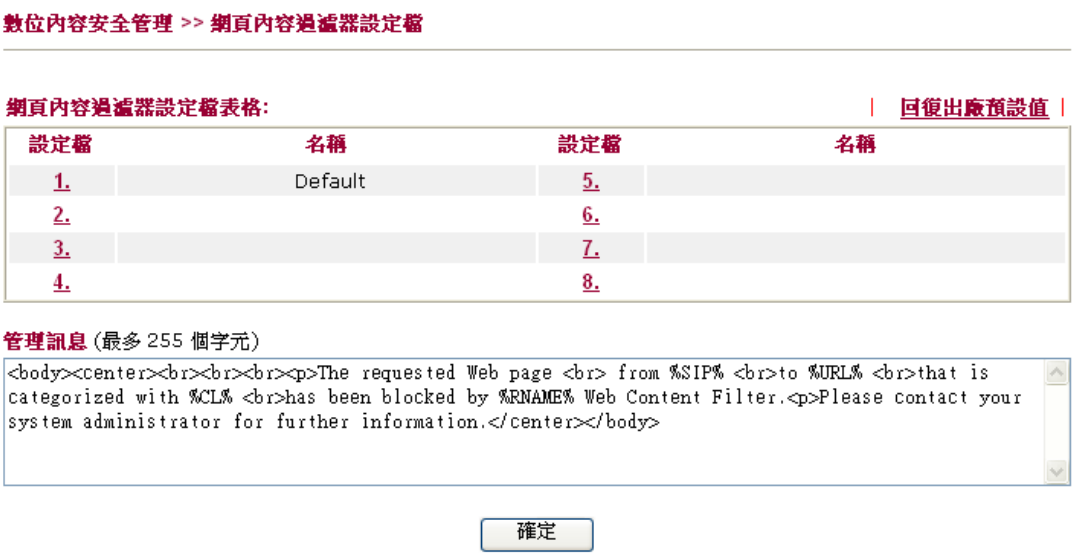
副檔名設定檔 – 請自**物件設定>>副檔名物件**中選擇一個事先設定完成的設定檔，並決定其對檔案下載採取封鎖或是放行的動作。

4.6.3 網頁內容過濾器設定檔

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

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

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



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。

黑名單/白名單

啓用 – 勾選此方塊啓用過濾機制，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爲何。

動作，通過 – 網頁內文符合本區所選定的關鍵字物件/群組內容，於經過路由器時可通行無阻。

動作，封鎖 - 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。

動作

通過 – 允許進入勾選的方塊等相關類型頁面。

封鎖 – 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，系統將以反向做爲處理該網頁。

Log(紀錄)

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。

4.7 頻寬管理

下面是頻寬管理的設定項目:

4.7.1 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 BitTorren)經常需要很大的連線數來處理，同時也會佔據很大的資源空間，造成重要的資料存取動作受到嚴重的影響。為瞭解決這種問題，您可以使用連線數限制來限制指定主機的連線數

在**頻寬管理**群組中，按 **NAT 連線數限制**開啓如下的網頁。

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。

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。
預設最大連線數	定義區域網路中每台電腦的預設連線數。
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。

預設最大連線數	定義區域網路中每台電腦的預設連線數。
最大連線數	定義指定 IP 位址的範圍中可用的連線數，如果您沒有在此區設定連線數，系統將會使用此機種所支援之預設連線數(10000)。
新增	新增指定連線數限制並顯示在上面的框框中。
編輯	允許您編輯選定的連線數設定。
刪除	刪除限制清單上任何一個您所選定的設定。
索引號碼(1-15)於排程設定..	您可以輸入四組時間排程，所有的排程都可在**應用-排程**網頁上事先設定完畢，然後在此輸入該排程的對應索引號碼即可。

4.7.2 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。

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。

啓用	按此鈕啓動限制頻寬功能。 **應用至第二子網路** - 勾選此方塊套用頻寬限制至**區域網路>>基本設定**中所指定的第二子網。
停用	按此鈕關閉限制頻寬功能。
預設傳送限制	定義區域網路中每台電腦預設的上行速度。

預設接收限制	定義區域網路中每台電腦預設的下行速度。
允許自動調整取得最佳利用 可用頻寬.	路由器將會檢查是否保留足夠的頻寬，依照使用者所設定的頻寬限制而定。如果足夠的話，路由器將會調整可用的頻寬給予使用者使用，以便提升整體的效能。
限制清單	顯示網頁中所設定的指定限制之電腦清單資料。
起始 IP	定義限制頻寬的起始 IP 位址。
結束 IP	定義限制頻寬的結束 IP 位址。
每一個/共用	選擇 Each 讓起始 IP 與結束 IP 範圍內的每個 IP 都能享有傳送限制與接收限制中所定義的速度；選擇 **Shared** 則讓範圍內的 IP 共用傳送限制與接收限制的全部頻寬。
傳送限制	定義上行傳送的速度限制，如果您未在此區設定限制的話，系統將使用您在每個索引內容中索引中所預設的限制速度。
接收限制	定義下行傳送的速度限制，如果您未在此區設定限制的話，系統將使用您在每個索引內容中索引中所預設的限制速度。
新增	新增指定速度限制並顯示在上面的框框中。
編輯	允許您編輯選定的限制設定。
刪除	刪除限制清單上任何一個您所選定的設定。
索引號碼(1-15)於排程設定..	您可以輸入四組時間排程，所有的排程都可在**應用-排程**網頁上事先設定完畢，然後在此輸入該排程的對應索引號碼即可。

4.7.3 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 爲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，我們稱之爲 TCP 慢速啓動。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。

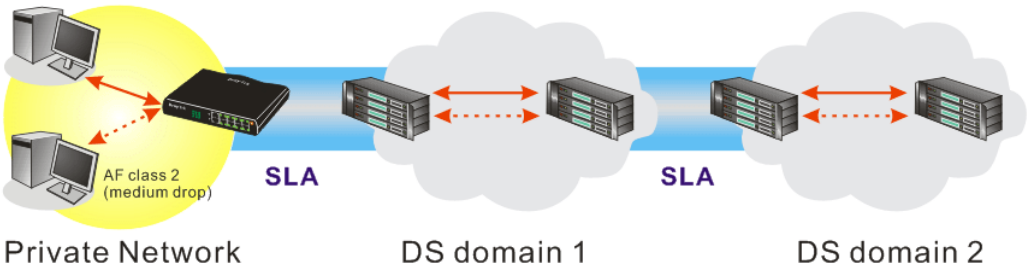
另一個理由是由於網路的擁擠狀況，內部連線迴路速度不符合或是傳輸流量過份聚集，資料封包排隊等候傳送，整個傳輸慢了下來。如果沒有定義後先後順序，以指定在滿檔的隊伍中哪個封包必須丟棄，上述提及的應用程式封包就可能成爲被捨棄掉的一個，這樣的話對應用程式的成效會造成令人無法想像的後果。

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，並標示這些程式爲高優先權服務等級，以便在網路中能夠強迫執行。
- 排定計畫: 以服務等級分類爲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爲基礎來分類及規劃封包，例如爲了確保封包頭之連線，電信工作人員在執行大量運作時，可能會強迫一個 QoS 控制索引保留頻寬予 HTTP 連線。

Vigor 路由器作爲 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 啓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。

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。

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爲 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。

啓用服務品質(QoS)控制..

預設狀態下，這個功能是啓用的。
請同時定義 QoS 控制設應所應用的流量方向。
下載- 僅適用於進入的封包。
上傳- 僅適用於輸出的封包。
雙向- 適用於進入與輸出的封包。
勾選此方塊並按下**確定**，**連線狀態統計**連結即可出現在此頁面上。

WAN 下載頻寬

允許您設定 WAN 資料輸入的連線速度。預設值爲 10000kbps。

WAN 上傳頻寬

允許您設定 WAN 資料輸入的連線速度。預設值爲 10000kbps。

例如，您的 ADSL 支援 1M 的下行與 256K 上行速度，請將 **WAN 下載頻寬** 設定爲 1000kbps 而 **WAN 上傳頻寬** 設定爲 256kbps。

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爲 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。

保留頻寬比例

保留作爲群組索引所可應用的比率。

啓用 UDP 頻寬控制

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，因爲 UDP 應用程式會消耗很多的頻寬。

優先處理對外 TCP ACK

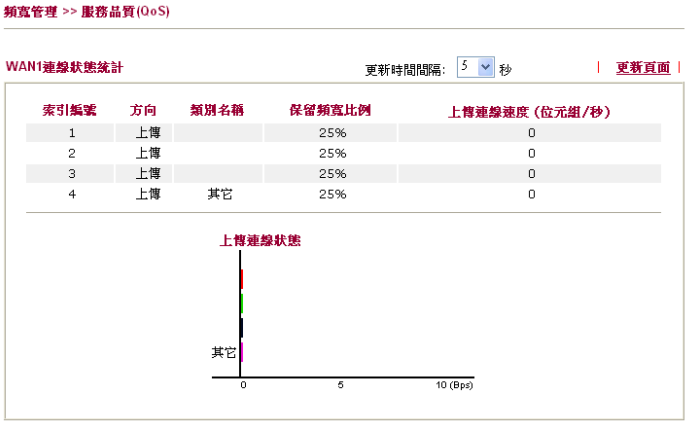
下載和上傳之的頻寬在 ADSL2+ 環境中差異是很大的，因爲下載速度可能會受到上傳 TCP ACK 的影響，您可以勾選此方塊讓 ACK 上傳得快一點，以便讓網路流通的更順暢。

限制頻寬比率

此處所輸入的比率保留作爲 UDP 應用之需。

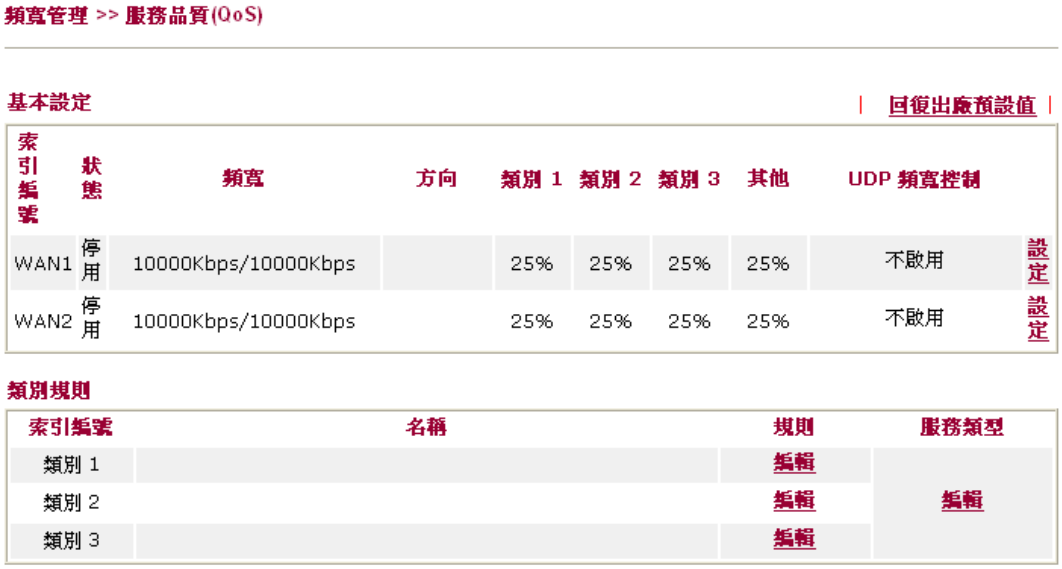
連線狀態統計

顯示服務品質的連線狀態統計圖供使用者參考。



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，請按該項類別的索引連結即可。



在您按下索引連結之後，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 用來作爲類別索引 1 的名稱。

F 若要新增一個新的規則，請按**新增**開啓下列畫面。

啓用 勾選此方塊啓用本頁的設定。

本機位址 按**編輯**按鈕以設定規則的來源位址。

遠端位址 按**編輯**按鈕以設定規則的目標位址。

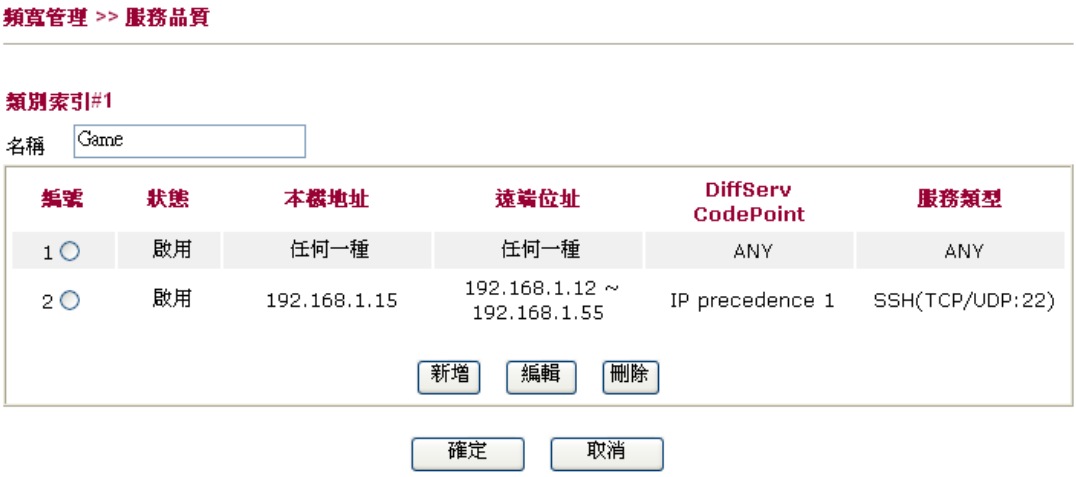
編輯 讓您編輯來源/目標位址資訊。

位址類型 – 決定來源位址的位址類型。
關於**任何位址**，您無須填入起始 IP 位址，由系統決定。
關於**單一位址**，您可以填入起始 IP 位址。
關於**範圍位址**，您必須填入起始和終點 IP 位址。
關於**子網路位址**，您必須填入起始 IP 位址和子網路遮罩 。

DiffServ CodePoint 所有的資料封包將會被切割成不同等級，並且依照系統的等級層別來處理資料封包。請指定資料所需的層級作爲 DoS 控制之用。

服務類型 決定 QoS 控制處理時資料的服務類型，這項類型可以視情況編輯改變，您可以從下拉式選項中選擇事先定義的服務類型，這些類型都是出廠時即設定好的類型，請自行挑選一種想要使用的類型。

另外，您可以爲一種類別指定 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正該規則。



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。

在您按下**編輯**按鈕之後，下麵的畫面將會出現。

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：

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 按**單一**或是**範圍**，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。
通訊埠號 –如果您選擇範圍爲服務類型，請在此輸入起始和結束通訊埠號。

另外，您可以指定 40 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。

4.8 其他應用

下圖顯示**其他應用**的功能項目：

4.8.1 動態 DNS

當您透過 ISP 業者嘗試連接到網際網路時，ISP 業者提供的經常是一個浮動 IP 位址，這表示指派給您的路由器使用之真實 IP 位址每次都會有所不同，DDNS 可讓您指派一個網功能變數名稱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功能變數名稱稱，並利用網際網路存取路由器或是內部虛擬的伺服器資料。如果您的主機擁有網路伺服器、FTP 伺服器或是其他路由器後方提供的伺服器，這項設定就特別有幫助也有意義。

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

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功能變數名稱稱(例如 hostname.dyndns.org)，且獲得一個帳號，其使用者名稱爲 *test*；密碼爲: *test*。
2. 自**應用**群組選擇**動態 DNS** 設定，下述頁面即會出現在螢幕上。

回復出廠預設值	清除全部設定資料並回復到出廠的設定。
啓用動態 DNS 設定	勾選此方塊啓用此功能。
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。
網功能變數名稱稱	顯示您在 DDNS 設定頁面上所設定的網功能變數名稱稱。
啓用	顯示此帳號目前是啓用或是停用狀態。
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。

5. 選擇索引號碼 1，爲您的路由器新增一個帳號。勾選**啓用動態 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)，並於網功能變數名稱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)。

啓用動態 DNS 帳號	勾選此方塊以啓用目前帳號，如果您勾選此方塊，您可在步驟 2 中的網頁上看到啓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。
服務供應商	爲此 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**，您可以修正網功能變數名稱稱區域中所選定的網域資料。
網功能變數名稱稱	輸入您所申請的網功能變數名稱稱。請使用下拉式選項選擇想要使用的一個名稱。
登入名稱	輸入您在申請網功能變數名稱稱時所設定之登入名稱。
密碼	輸入您在申請網功能變數名稱稱時所設定之密碼。
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。

6. 按**確定**按鈕啓動此設定，您將會看到所做的設定已被儲存。

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**啓用動態 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。

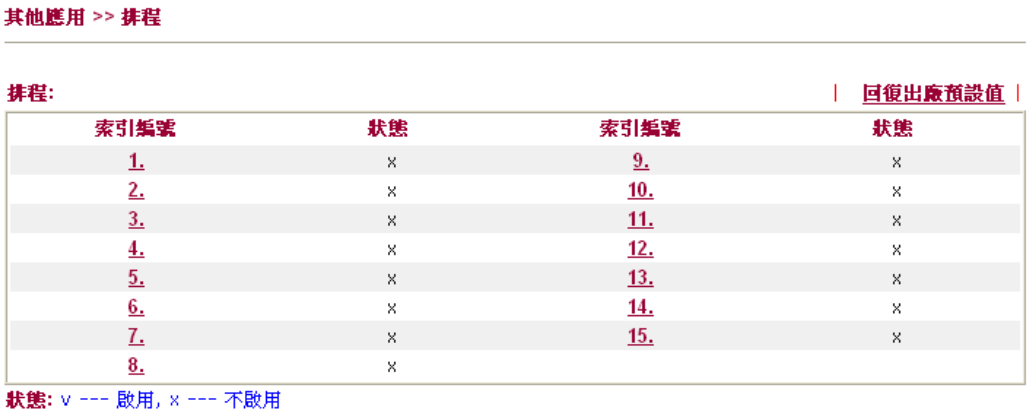
刪除動態 DNS 帳號

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。

4.8.2 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。



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，請按任何一個索引號碼，這裡舉索引編號 1 爲例。其呼叫排程的細部設定顯示如下：

啓用排程設定 勾選此項目以啓動此排程。

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：
強迫啓用 - 強迫連線永遠存在。
強迫停用 - 強迫連線永遠停止。
啓用隨選撥接 - 指定隨選播接連線以及閒置的時間。
停用隨選撥接 - 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啓用。

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 **一次** - 此計劃的頻率只會應用一次。
週期 - 指定一週當中哪些日子需要執行此項排程作業。

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(強迫啓用)，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，

強迫啓用與**強迫停用**來計畫其網際網路連線。

4.8.3 RADIUS

撥接使用者遠端認證服務(RADIUS)是一種用戶端/伺服器端安全性驗證之通訊協定，支援驗證、授權和說明，通常爲網際網路服務供應商所廣泛應用，是用來作爲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。

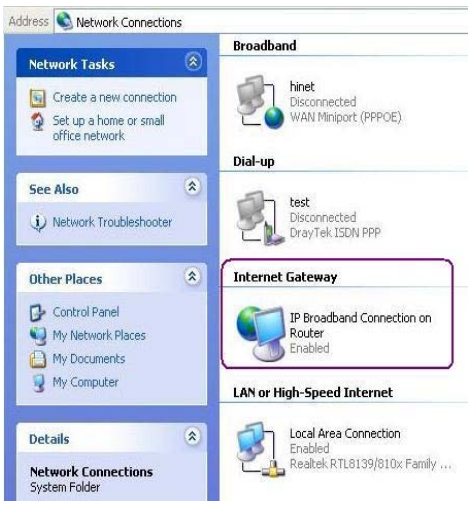
啓用	勾選此項以啓動 RADIUS 設定。
伺服器 IP 位址	輸入 RADIUS 伺服器的 IP 位址。
通訊埠	輸入 RADIUS 伺服器所使用的 UDP 通訊埠號，基於 RFC 2138，預設值爲 1812。
共用密鑰	RADIUS 伺服器和用戶共用一個用來驗證二者之間傳遞訊息的密鑰，雙方都必須設定相同的共用密鑰。
確認共用密鑰	請重新輸入共用密鑰以確認。

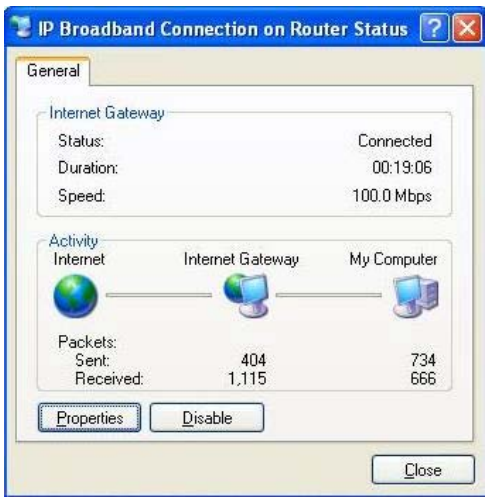
4.8.4 UPnP

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

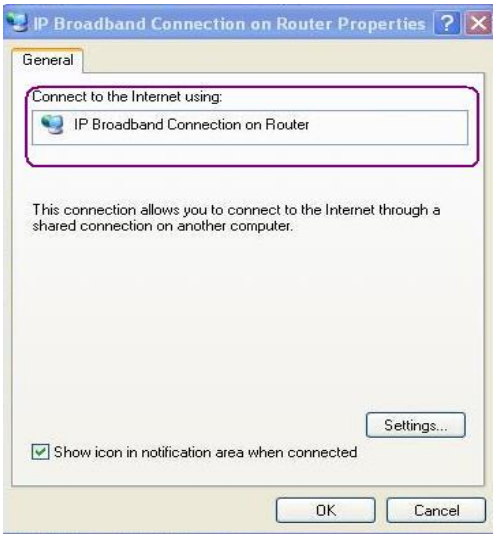
啓用 UPnP 服務　　您可以視情況勾選**啓用連線控制服務**或是**啓用連線狀態服務**。

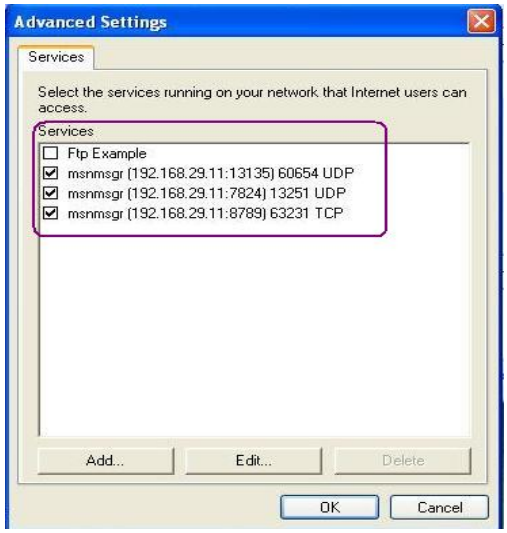
在設定**啓用 UPNP 服務**後，在 Windows XP/網路連線上會出現一個 **IP Broadband Connection on Router** 圖示，連線狀態和控制狀態將可開啓使用，NAT Traversal of UPnP 可啓動應用程式中的多媒體特徵，必須手動設定通訊埠對應或是使用其他類似的方法來設定，以下顯示此項功能的範例圖形。





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，這是因爲這些應用程式會擋掉某些網路通訊埠的存取能力。

安全考量

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

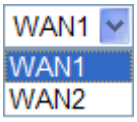
- 某些微軟操作系統已發現到 UPnP 的缺點，因此您需要確定已經應用最新的服務封包。
- 未享有特權的使用者可以控制某些路由器的功能，像是移除和新增通訊埠對應等。

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

4.8.5 IGMP

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

啓用 IGMP 伺服器 勾選此方塊啓用此功能。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。



啓用 IGMP Snooping 勾選此方塊啓用此功能，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爲一般的廣播播送流量。

群組 ID 此區顯示多重播送群組的 ID 連接埠，可用範圍爲 224.0.0.0 至 239.255.255.254。

P1 到 P4 I 多重播送群組中所使用的 LAN 連接埠。

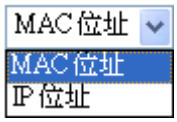
更新頁面 按此連結重新整理並顯示多重播送群組的狀態。

4.8.6 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。

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。

4.9 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。

下圖爲 VPN 與遠端存取的主要功能項目：

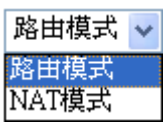
4.9.1 VPN 用戶端設定精靈

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

LAN-to-LAN 用戶端模式選項

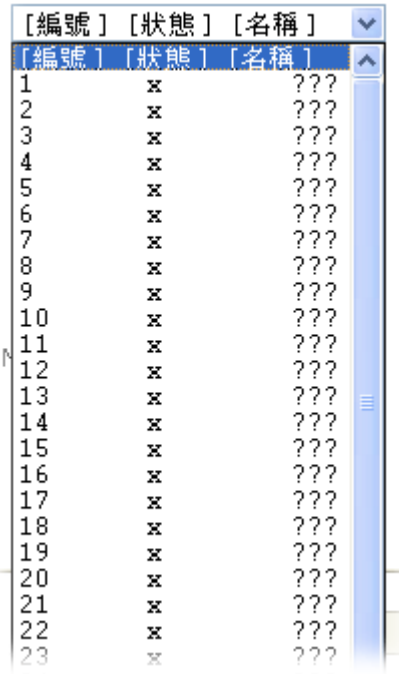
選擇用戶端模式。

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。

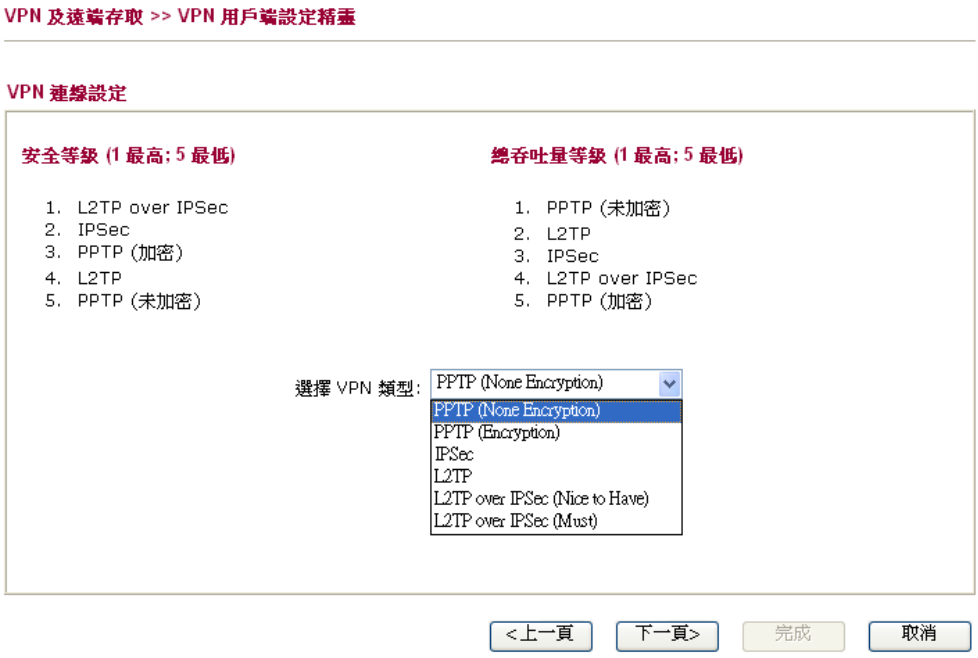


請選擇 LAN-to-LAN 設定檔

共有 32 個 VPN 設定檔可以供使用者選擇來設定。



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。



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：

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

- 當您選擇 **IPSec** 您看到的頁面如下：

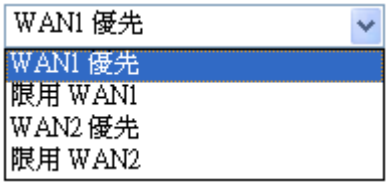
- 當您選擇 **L2TP** 您看到的頁面如下：

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

- 當您選擇 **L2TP over IPSec (Must)** 您看到的頁面如下：

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 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。



WAN1 優先 - 連線時，路由器會將 WAN1 視爲 VPN 連線的首要選擇，如果 WAN1 連線失敗，路由器將使用另一個 WAN 介面來取代。

僅用 WAN1 - 連線時，路由器會將 WAN1 視爲 VPN 連線的唯一選擇。

WAN2 優先 - 連線時，路由器會將 WAN2 視爲 VPN 連線的首要選擇，如果 WAN2 連線失敗，路由器將使用另一個 WAN 介面來取代。

僅用 WAN2 - 連線時，路由器會將 WAN2 視爲 VPN 連線的唯一選擇。

永遠連線 勾選此方塊讓路由器永遠保持 VPN 連線。

IKE 驗證方式 **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)。

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。
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。

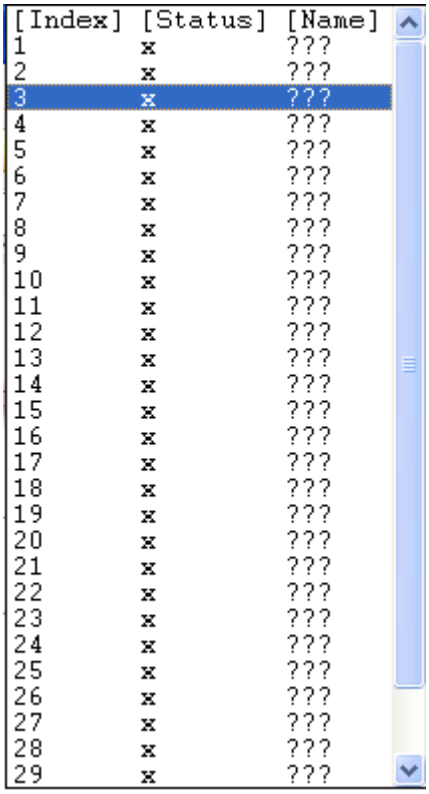
完成配置後，請按**下一頁**，確定頁面將顯示如下，如果沒有任何問題的話，您可以按下面可至不同設定頁面的按鈕，然後按**完成**進行另一個 VPN 設定。

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。

4.9.2 VPN 伺服器端精靈

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

VPN 伺服器模式選項	請選擇 VPN 伺服器的方向 **點對點 VPN** – 想要自動設定 LAN-to-LAN 設定檔，請選擇**點對點 VPN**。 **/遠端撥入使用者**– 管理遠端使用者設定檔表格來管理遠端用戶的存取狀態，使用者透過 VPN 連線存取網路時，必須接受驗證過程。  **注意**: VPN 伺服器設定精靈畫面會依據所選擇的 VPN 伺服器模式而有所不同。
請選擇 LAN-to-LAN 設定檔	當您選擇的是點對點 VPN（LAN-to-LAN）作爲 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。



請選擇撥入使用者帳號

當您選擇了遠端撥入使用者作爲 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。

允許的撥入類型

當您選擇了任何一個撥入使用者帳號設定檔，即可使用此類型設定，您必須針對 VPN 伺服器設定檔選擇適當的撥入類型，此處提供數種可以選擇的項目（類似 VPN 用戶端精靈）。

不同的撥入類型所帶出的設定頁面也會有些許的差異。

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，以下我們舉出數例：

- 當您選擇 **PPTP, IPSec, L2TP** 或 **PPTP, IPSec** 或 **L2TP with Policy (Nice to Have/Must)**，您看到的頁面如下：

- 當您選擇 **PPTP, L2TP** 或 **PPTP** 或 **L2TP with Policy (None)**，您看到的頁面如下：

- 當您選擇 **IPSec**，您看到的頁面如下：

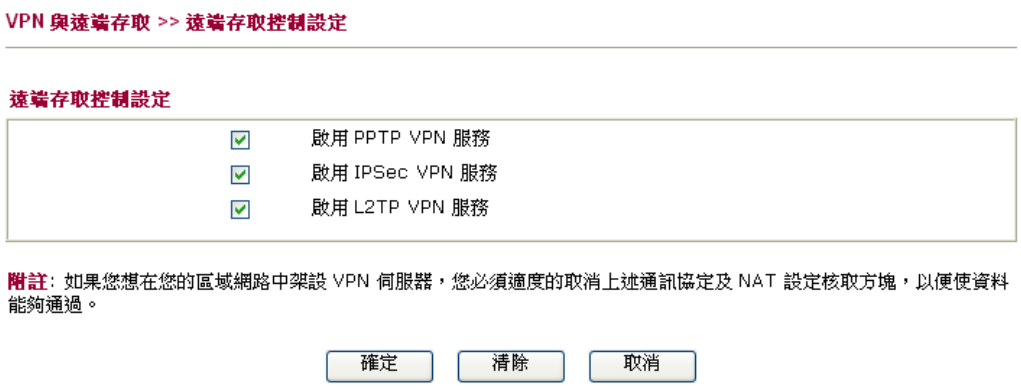
設定檔名稱	請輸入設定檔的檔名，檔案的長度限制在 10 的字元間。
使用者名稱	當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區資料可用來驗證連線。
密碼	當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區資料可用來驗證連線。
預先共用金鑰	爲了驗證 IPSec/L2TP IPSec，請輸入金鑰內容。
確認預先共用金鑰	再輸入一次金鑰內容確認。
數位簽章 (X.509)	勾選此方塊啓用此功能並選擇一組事先定義的簽章內容 (在 **VPN 和遠端存取>>IPSec 端點辨識**中設定)。
對方 IP/VPN 用戶端 IP	請輸入遠端用戶的 WAN IP 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。

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。

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。

4.9.3 遠端存取控制

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



啓用 PPTP VPN 服務	勾選此方塊啓動經由 PPTP 通訊協定之 VPN 服務。
啓用 IPSec VPN 服務	勾選此方塊啓動經由 IPSec 通訊協定之 VPN 服務。
啓用 L2TP VPN 服務	勾選此方塊啓動經由 L2TP 通訊協定之 VPN 服務。

4.9.4 PPP 基本設定

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

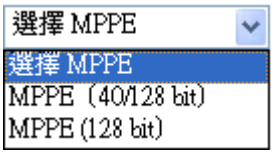
撥入 PPP 驗證

PAP - 選擇此項目強迫路由器以 PAP 協定來驗證撥入使用者。

PAP 或 CHAP - 選擇此項目表示路由器會嘗試先以 CHAP 協定驗證撥入使用者，如果撥入使用者沒有支援此項協定，系統會改用 PAP 協定來驗證使用者。

撥入 PPP 加密(MPPE)

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。



MPPE (40/128bit) - 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。

MPPE (128bit) -此選項指出路由器將會使用 MPPE 最大值(128 bits)來加密資料。

雙方共同驗證 (PAP)

共同驗證功能主要應用於和其他路由器或是需要雙向驗證的用戶連絡，以便取得更佳安全性能，因此當您的對點路由器需要共同驗證時，您就應該啓動此功能，並進一步指定使用者名稱和密碼。

起始 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爲 192.168.1.0/255.255.255.0，您可以選擇 192.168.1.200 做爲起始 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 乃是保留作爲 ISDN 遠端撥入使用者所使用。

4.9.5 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。

IKE 認證方式

通常應用在遠端撥入使用者或是使用動態 IP 位址的節點(LAN-to-LAN)以及 IPSec 相關之 VPN 連線上，像是 L2TP over IPSec 和 IPSec 通道。

預先共用金鑰 - 只有支援預先共用金鑰，請指定一個金鑰作爲 IKE 驗證之用。

確認預先共用金鑰- 確認您所輸入的共用金鑰。

IPSec 安全防護方式

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) - 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。

4.9.6 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爲遠端驗證工具，您可以編輯對方認證表格供後續選擇使用。路由器提供 32 種 IPSec 端點辨識設定檔：

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

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**???**代表該設定檔是空的，未做任何設定。

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

設定檔名稱 請輸入此設定檔的檔名。

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。

4.9.7 遠端撥入使用者

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

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

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 |

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

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**???**代表該設定檔是空的，未做任何設定。

狀態 顯示特定撥入使用者的存取狀態，符號 V 和 X 分別代表活動中與不活動的檔案。

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。

開啓這個帳號

勾選此方塊以啓用此功能。

閒置逾時 - 如果撥入使用者閒置超過所設定的時間，路由器將會自動中斷連線，預設閒置逾時爲 300 秒。

PPTP

爲伺服器建立一個透過網際網路的 PPTP VPN 連線，您必須設定連線類型和身分辨識像是使用者名稱與密碼等，以便驗證遠端伺服器。

IPSec 通道

允許遠端撥入使用者透過網際網路觸發 IPSec VPN 連線。

具有 IPSec 原則的 L2TP

爲伺服器建立一個透過網際網路的 L2TP VPN 連線。您可以選擇使用單獨 L2TP 或是含有 IPSec 的 L2TP，請自下拉式選項選取：

無 - 此選項完全不會應用 IPSec 原則，VPN 連線採用不帶有 IPSec 原則的 L2TP，可以在完全 L2TP 連線中檢視內容。

建議選填 -如果在整個連線過程中完全可以運用，此選項會先應用 IPSec 原則。否則撥入 VPN 連線會成爲一種完全的 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。

指定遠端節點

勾選 - 您可以指定遠端撥入使用者或是對點 ID (應用於 IKE 主動模式中)的 IP 位元址。

不勾選 - 表示您所選擇的連線類型，將會應用**一般設定**中所設定的驗證方式和安全防護方式。

Netbios 命名封包

通過 – 按此鈕讓資料能在二台主機之間所建立的 VPN 通道上傳輸。

封鎖 – 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。

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。
IKE 驗證方式	**預先共同金鑰-** 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。 **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)。
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。請勾選中級或是高級設定作爲安全防護方式。 **中級 -Authentication Header (AH)**表示資料將被驗證，但未被加密，此選項的預設時是勾選狀態。 **高級 -Encapsulating Security Payload (ESP)**表示資料將被加密及驗證，請自下拉式清單中選取適合項目。 **本機 ID -**指定一個本地 ID 以便作爲 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。

4.9.8 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 |

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

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 意即 LAN-to-LAN 檔案名稱，**???**符號代表該檔案目前是空的。

狀態 表示個別檔案的狀態，符號 V 和 X 分別代表使用中與未使用的檔案。

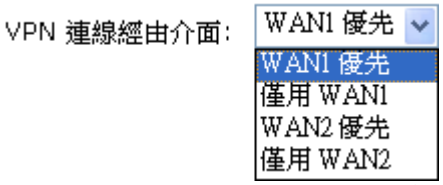
請按索引編號連結以編輯個別設定檔，按下後可看到如下的頁面，每個 LAN-to-LAN 檔案包含有四個子群組，如果該區域是灰色的，即表示您無法在該項目做任何設定，下面的說明可以引導您於各個設定區塊入相關資訊。

由於網頁太長，我們將之切成數個段落來說明。

設定檔名稱 針對此 LAN-to-LAN 連線，請指定一個設定檔案名稱。

啓用此設定檔 按此方塊啓用此設定檔。

VPN 連線經由介面 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。



WAN1 優先 - 連線時，路由器會將 WAN1 視爲 VPN 連線的首要選擇，如果 WAN1 連線失敗，路由器將使用另一個 WAN 介面來取代。

僅用 WAN1 - 連線時，路由器會將 WAN1 視爲 VPN 連線的唯一選擇。

WAN2 優先 - 連線時，路由器會將 WAN2 視爲 VPN 連線的首要選擇，如果 WAN2 連線失敗，路由器將使用另一個 WAN 介面來取代。

僅用 WAN2 - 連線時，路由器會將 WAN2 視爲 VPN 連線的唯一選擇。

Netbios 命名封包 **通過** – 按此鈕讓資料能在二台主機之間所建立的 VPN 通道上傳輸。

	封鎖 – 當雙方所建立的 VPN 通道連線產生衝突時，此功能可以封鎖此通道。
撥號方向	針對此 LAN-to-LAN 連線，請指定允許的撥號方向。 **雙向** – 發話方/接話方 **撥出** - 發話方 **撥入** - 接話方
永遠連線或閒置逾時	**永遠連線** – 勾選此方塊讓路由器永遠保持 VPN 連線。 **閒置逾時** - 預設值爲 300 秒，若連線閒置時間超過此數值，路由器將自動中斷連線。
啓用 PING 以維持連線	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。詳細內容請參考下麵的註解，請勾選此方塊啓動 PING 封包傳輸至指定的 IP 位址。
指定 IP 位址	輸入位於 VPN 通道另一邊的遠端主機的虛擬 IP 位址。
	註解：啓用 PING 以維持連線用來管理不正常的 IPSec VPN 連線中斷，提供一個 VPN 連線狀態供路由器判斷是否需要重撥。 正常而言，如果 VPN 任何一方想要中斷連線，那麼就必須依照封包交換程式通知對方。不過如果另一方在未通知的情況下中斷連線，Vigor 路由器將無從得知此項訊息，爲瞭解決這樣的困境，藉著不斷傳送 PING 封包至遠端主機的方式，路由器就可以知道此項 VPN 通道有無實際運作，這是一種獨立的 DPD (無效對方檢測)。
PPTP	爲伺服器建立一個透過網際網路的 PPTP VPN 連線，您必須設定連線類型和身分辨識像是使用者名稱與密碼等，以便驗證遠端伺服器。
IPSec 通道	爲伺服器建立一個透過網際網路的 IPSec VPN 連線。
具有 IPSec 原則的 L2TP	爲伺服器建立一個透過網際網路的 L2TP VPN 連線。您可以選擇使用單獨 L2TP 或是含有 IPSec 的 L2TP，請自下拉式選項選取： **無** - 此選項完全不會應用 IPSec 原則，VPN 連線採用不帶有 IPSec 原則的 L2TP，可以在完全 L2TP 連線中檢視內容。 **建議選填** -如果在整個連線過程中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。 **一定要有** - 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

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)。

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，因爲在安全通道中有更多的交換動作於此完成，不過，**Aggressive 模式**是比較快速的模式。路由器的預設值爲 **Main 模式**。

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。

果。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，預設值爲 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，預設值爲 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。預設狀況是不啓用此功能。

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。

允許的撥入類型 以不同類型來決定撥入連線。

PPTP 允許遠端撥入用戶透過網際網路達成 PPTP VPN 連線，請設定遠端撥入用戶的使用者名稱和密碼。

IPSec 通道 允許遠端撥入用戶透過網際網觸發 IPSec VPN 連線。

具有 IPSec 原則的 L2TP 允許遠端撥入用戶透過網際網路製造 L2TP VPN 連線，您可以選擇使用單獨 L2TP 或是含有 IPSec 的 L2TP，請自下拉式選項選取：

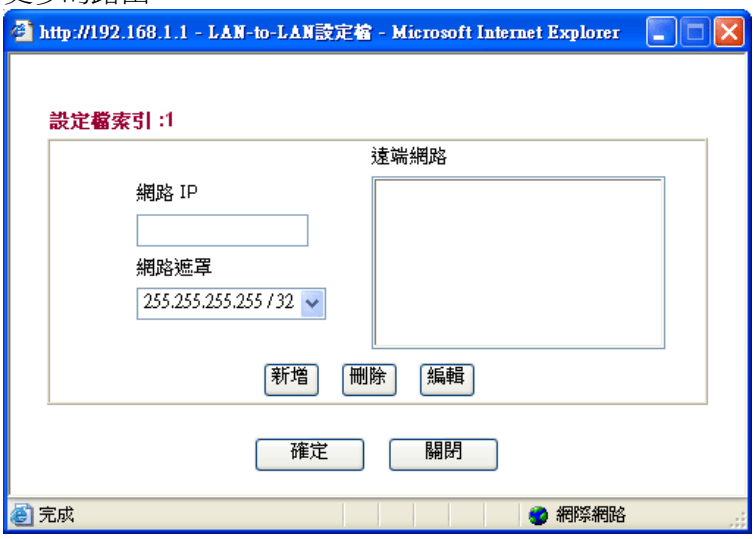
無 - 此選項完全不會應用 IPSec 原則，VPN 連線採用不帶有 IPSec 原則的 L2TP 可以在完全 L2TP 連線中檢視內容。

	建議選填-如果在整個連線過程中是可以運用的情形下，此選項會先應用 IPSec 原則。否則撥出 VPN 連線會成爲一種完全的 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。
指定 ISDN CLID 或 遠端 VPN 閘道	您可勾選此項，並指定遠端撥入用戶的真實 IP 位址或 ID (必須與撥入類型中所設定的 ID 相同)。 若您選擇 ISDN 類型，請於此輸入對方的 ISDN 號碼， (適用於 *i* 機型)。 此外針對 VPN 功能，您應該進一步指定右邊相關安全設定。
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。
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。
IKE 驗證方式	當您指定遠端節點的 IP 位址時，IKE 驗證可套用在 IPSec 通道和含 IPSec 原則之 L2TP 上。不過，不管有沒有指定遠端節點的 IP 位址予 IPSec 通道使用，您仍然可以設定數位簽章(X.509)。 **預先共同金鑰-** 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自下拉式清單中選擇 **VPN 遠端存取控制>>IPSec 端點辨識**中所預先定義的設定檔。
IPSec 安全防護方式	當您指定遠端模式時，對 IPSec 通道和 L2TP 含 IPSec 原則來說，本區爲必要設定。 **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。
我的 WAN IP	本區只在您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時有效。預設值爲 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。此一位址適用於本機爲 VPN client (dial-out) 端時。
遠端閘道 IP	本區只在您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時有效。預設值爲 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。此一位址適用於本機爲 VPN Server (dial-in) 端時。
遠端網路 IP/遠端網路遮罩	新增一個靜態路由以便透過網際網路，引導遠端網路 IP 位址/遠端網路遮罩預定之全部傳輸流量。對 IPSec 而言，這

項設定是第二階段快速模式的目的用戶端之身分。

更多

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。



RIP 方向

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。

從第一個子網路到遠端網路，您必須要作

如果遠端網路只允許您以單一 IP 撥號，請選擇 **NAT** 否則請選擇**路由**。

變更預設路由此 VPN 通道

勾選此方塊變更此 VPN 通道的預設路由。

4.9.9 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。

撥號 按此鈕執行撥號功能。

更新間隔秒數 選擇重新顯示狀態的間隔秒數，有 5、10、30 秒等三種選擇。

更新頁面 按此鈕以重新顯示整個連線狀態。

4.10 憑證管理

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

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

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

4.10.1 本機憑證

產生　　按此鈕以開啓**產生憑證需求**視窗。

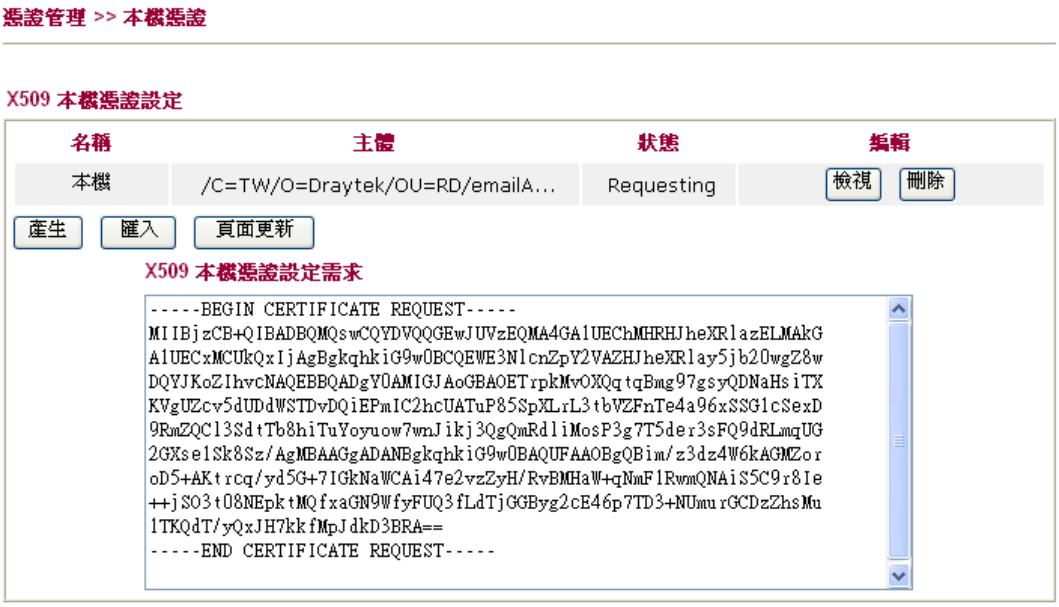
輸入全部的資訊，然後再按一次**產生**按鈕。

匯入　　按此鈕以匯入儲存的檔案作爲憑證資訊。

頁面更新　　按此鈕以更新資訊。

檢視　　按此鈕以檢視憑證詳細的設定。

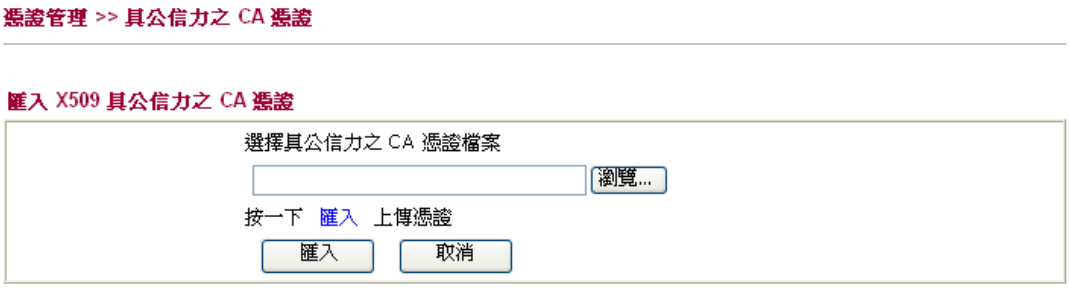
在按下**產生**按鈕之後，產生後的資訊將會顯示在視窗上，見下圖：



4.10.2 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。

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**瀏覽...**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。



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

4.10.3 憑證備份

路由器的本機憑證與具公信力之 CA 憑證可以儲存爲一個檔案，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。

4.11 VoIP

注意:此功能僅適用“V”機型。

Voice over IP network (VoIP)可讓您使用寬頻網際網路連線撥打網路電話。

有很多種不同的電話信號協定、方法可讓 VoIP 裝置使用以便與對方溝通聯繫，最普遍的協定有 SIP、MGCP、Megaco 和 H.323，這些協定彼此都不完全相容(除非是透過軟體伺服器的掌控)。

Vigor V 系列機種支援 SIP 協定，因爲此種協定對 ITSP (Internet Telephony Service Provider)而言是很理想也很方便，支援也最廣。SIP 是一種端對端信號協定，可建立使用者於 VoIP 結構中之出席情形和機動性。每個想要使用 SIP 相同資源辨識器之用戶都可使用標準的 SIP URI 格式

sip: user:password @ host: port

某些區域可能有不同的使用方式，一般來說主機指的是網域，使用者資訊包含有使用者名稱區、密碼區，@符號則緊跟在後，這種格式和 URL 很相似，所以有些人以 SIP URL 來稱呼它。SIP 支援點對點直接撥號，同時也可透過 SIP 代理伺服器(角色雷同 H.323 Gatekeeper)來撥號，而 MGCP 協定則是使用用戶-伺服器結構，撥號方式和目前 PSTN 網路是相同的。

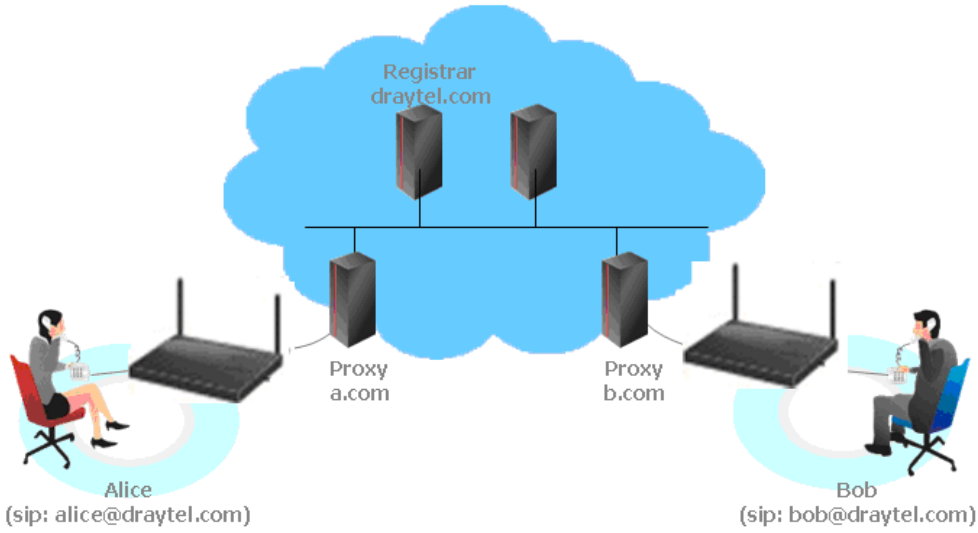
在撥號設定之後，聲音是透過 RTP (Real-Time Transport Protocol)來傳送的，不同的 codecs(用來壓縮和解壓縮聲音)可以包覆於 RTP 封包中，Vigor V 機種提供不同的 codecs 包括 G.711 A/μ-law, G.723, G.726 和 G.729 A & B，每個 codecs 都使用不同頻寬，因此可以提供不同等級的聲音品質。Codec 使用的頻寬越多，聲音品質越好，雖然如此還是應該配合您的網際網路頻寬選擇適宜的 codec 才恰當。

通常有二種撥號類型，說明如下：

- **透過 SIP 伺服器撥號**

  首先 Vigor V 機種必須先向 SIP 註冊，傳送註冊訊息才可生效，然後雙方的 SIP 代理商將轉送一系列訊息給與撥號者，以便建立完整的 session。

  如果雙方都向相同 ISP 業者註冊，那麼我們可以下圖來做簡單說明：



  這種模式最主要的好處是您不必去記朋友的 IP 位址(因爲它可能常常會改變，如果該位址是浮動的位址的話)，相反的您只要使用撥號計畫或是直接撥朋友的帳號名稱就可以了。

- **點對點**

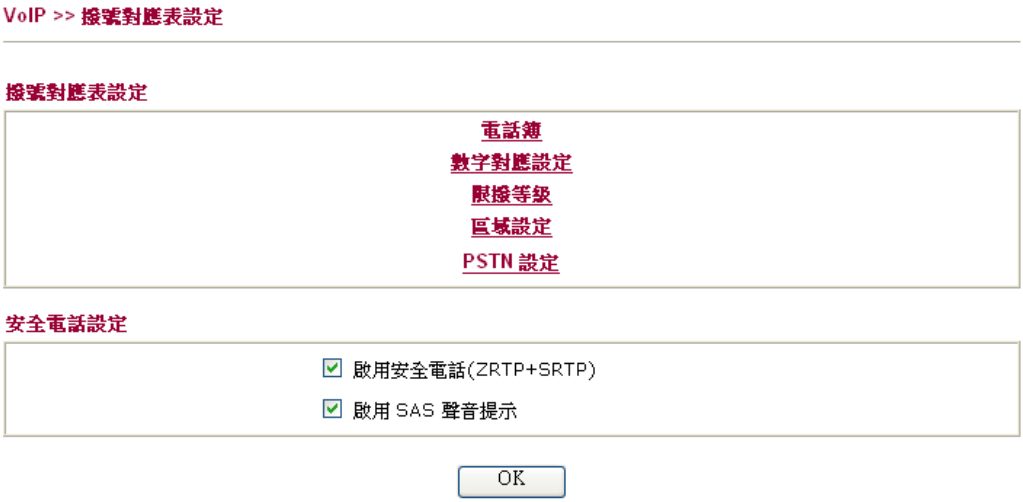
  在撥打電話之前，您必須知道朋友的 IP 位址，Vigor VoIP 路由器會建立雙方間的連線。

  我們的 Vigor V 機種首先採用有效之 codecs，但同時也擔保自動 QoS 的功能，QoS 擔保可以協助指定聲音流量較高之優先權，您對聲音所需求之 inbound 和 outbound 頻寬永遠擁有優先處理權，但是您的資料處理就會有些慢，不過還在忍受範圍內。

  下圖爲 VoIP 的功能項目：

4.11.1 撥號對應表

本頁讓使用者設定 VoIP 功能所需的電話簿及數字對應設定。請按頁面上的連結進入下一層設定頁面。



啓用安全電話 利用相同的通訊協定(ZRTP+SRTP)讓使用者能有加密的 RTP stream 與遠端通訊，請勾選此方塊啓動此安全電話功能。

啓用 SAS 聲音提示 若啓動此項目，每一次雙邊都會聽見 SAS 提示音，若沒有啓動，就再也不會聽到提示音。

安全電話的應用

啓用 SAS 聲音提示，例如路由器 A **啓用安全電話**與**啓用 SAS 聲音提示**並打電話給路由器 B：

1. 在連線建立後，路由器 A 將會傳送 SAS 聲音提示訊息給予 A，路由器 B 傳送 SAS 聲音提示訊息給予 B。
2. 此時，RTP 流量是受到安全保護的，直到電話通訊結束。
3. 如果路由器 A 想要下次再打給路由器 B，即使在網頁上已經勾選了**啓用 SAS 聲音提示**，這次不會再聽到任何聲音提示了，亦即只有第一通電話才會有聲音提示的功能。

啓用 SAS 聲音提示，例如路由器 A **啓用安全電話**，但未**啓用 SAS 聲音提示**並打電話給路由器 B：

1. 在連線建立後，路由器 A 將**不會**傳送 SAS 聲音提示訊息給予 A，路由器 B **也不會**傳送 SAS 聲音提示訊息給予 B。
2. 即使沒有聲音提示，RTP 流量仍然受到安全保護，直到電話通訊結束。

注意: 如果來電或去電並不符電話簿上的任何一個設定，路由器將會嘗試讓該通電話先具備一定的保護，但是如果該通電話是以未受保護的情況下結束（例如對方並不支援 ZRTP+SRTP 功能），路由器將不會播放任何警告訊息。

電話簿

在本節中，您可以設定 VOIP 電話，這個設定可以幫助用戶以最快且最簡單的方式撥出電話號碼。本頁總共提供 60 組號碼給用戶儲存朋友以及家人的 SIP 位址。

按任何一個索引標號進入下一個設定頁面。

啓用 勾選此方塊啓用此號碼。

電話號碼 此索引編號的快速撥號號碼，任何號碼都可以使用，範圍是數字 **0-9** 以及*****。

顯示名稱 您想要在朋友的電話螢幕上顯示出來的名稱，可讓您的朋友容易知道是誰打的電話。

SIP URL 請輸入朋友的 SIP 位址。

撥出帳號 選擇 SIP 帳號供此設定檔使用，對在不同 SIP 伺服器註冊的雙方，此設定相當有用。如果撥號者與接號者沒有使用相同

的 SIP 伺服器，有時候 VoIP 電話連線可能不會成功，但使用指定的撥號帳號，就可確保網路電話得以成功連線。

電話介接

可選擇的項目如下:

備援電話號碼

當 VoIP 電話受到幹擾或是網際網路因爲某種原因而中斷，備援電話將可撥出以替代 VoIP 網路電話。此時，電話會依照所選擇的電話介接方向從 VoIP 電話轉變成爲 PSTN 電話。請注意，在電話交換期間，電話的嘟嘟聲響也會短暫出現，當 VoIP 電話切換成 PSTN 電話後，電信公司就會向您收取連線的費用。請在此輸入備援電話號碼(PSTN)。

數字對應設定

爲了使用者的方便，本頁允許使用者以新號碼來編輯 SIP 帳號的前置號碼，或是取代該號碼等等，這個設定可以提供用戶一個透過 VoIP 介面快速且簡單的撥號方式。

啓用

按此方塊啓動此功能。

前置號碼

此處所設定的號碼可用來新增，取代變更之號碼。

模式

無 – 無動作。

新增 -當您選擇此模式時，變更號碼將會增加前置號碼於前面，並藉由選定的 VoIP 介面撥出。

卸除 -當您選擇此模式時，變更號碼將會被刪除。參考上圖所示，變更號碼 886 將被完全刪除。

取代- 當您選擇此模式時，透過指定的 VoIP 介面之變更號碼將會被前置號碼所取代，當您選擇此模式時，透過指定的 VoIP 介面之變更號碼將會被前置號碼所取代，參考上圖所示，號碼 *03* 將被變更號碼 *8863* 取代。

變更號碼 您在此處所輸入的號碼是您想要執行特殊功用的帳號前半部份(依據選擇的模式而定)。

最小長度 設定撥號的最小長度以套用前置號碼之設定，參考上圖所示，如果號碼介於 7 和 9，那麼該號碼可以就能套用此處所設定的前置號碼設定。

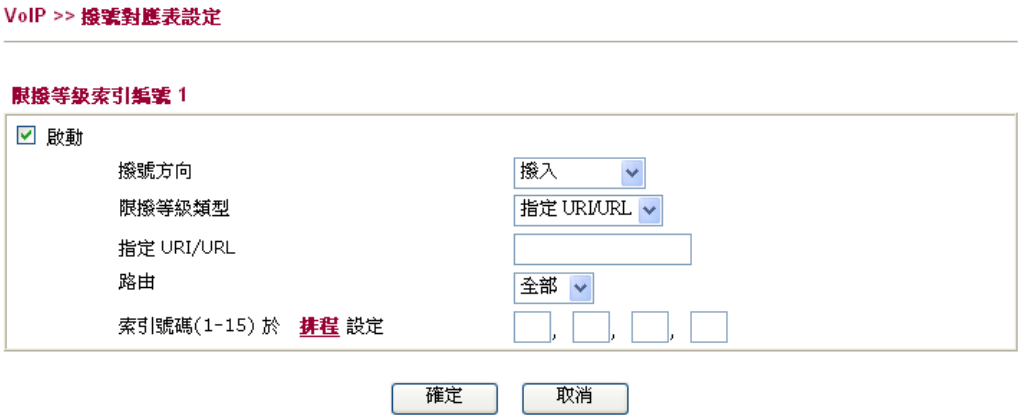
最大長度 設定撥號的最大長度以套用前置號碼之設定。

介面 請自預設的六組 SIP 帳號中選擇一個您想要啓動前置號碼設定的介面。

限撥等級

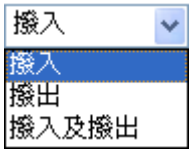
限撥等級用來封鎖不受歡迎的來電。

按任一索引編號，開啓下述頁面。



啓用 勾選此方塊啓用此設定。

撥號方向 決定電話的撥打方向。撥入- 來電，撥出-去電，撥出及撥出–來電與去電。



限定類型 決定 VoIP 電話的類型，URI/URL 或號碼。

指定 URI/URL 或指定號碼 本區依照您在限撥等級類型中所選擇的內容而有所不同。

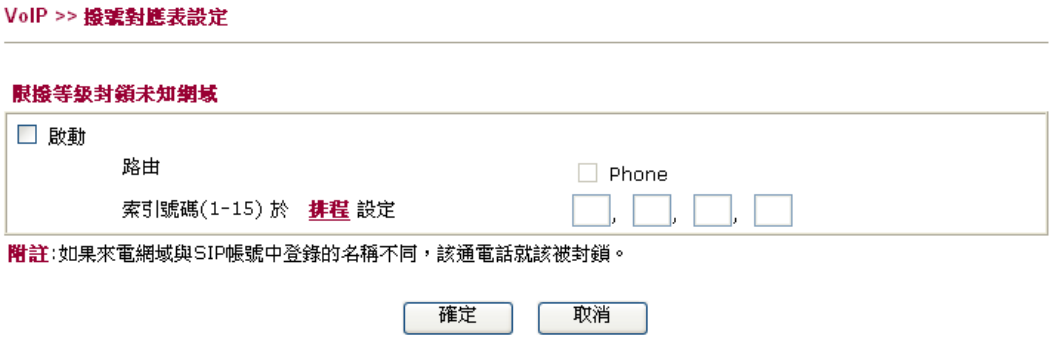
介面 **全部**表示全部的電話都會被此機制阻擋。

索引 (1-15) 於排程設定… 依照事先設定完成之排程，在此輸入排程計畫的索引編號以控制勿打擾模式。詳細設定請參考**排程**一節。

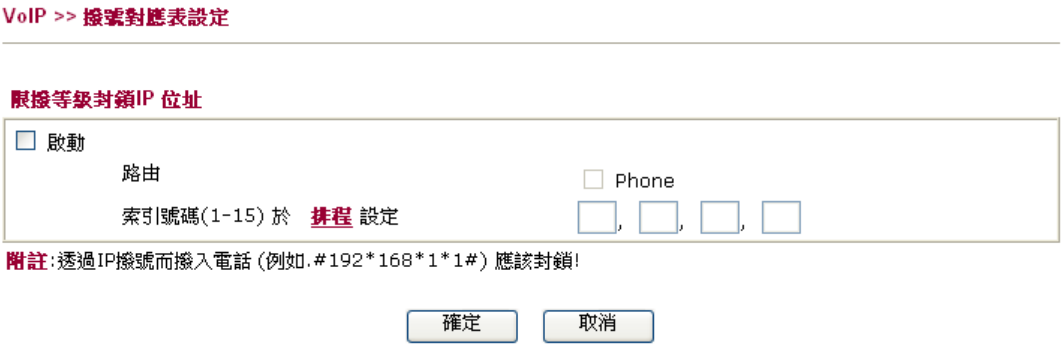
此外，您也可以將限撥等級做進一步的設定諸如匿名封鎖、未知網域封鎖或是封鎖 IP 位址等等。按下相關連結即可開啓網頁。

針對**封鎖匿名**部分 – 此功能可封鎖沒有顯示身分的任何來電，此項設定也可依照事先設定的排程來控制。

針對**封鎖未知網域**部分 - 此功能可封鎖未在 SIP 帳號中指定的網域之來電，此項設定也可依照事先設定的排程來控制。



針對**封鎖 IP 位元址**部分 - 此功能可封鎖來自 IP 位址之來電，此項設定也可依照事先設定的排程來控制。



區域設定

本頁可讓您處理某些區域的來電與去電，預設值(大部分地區的常用值)顯示在網頁上，您可以依照路由器放置的地點，視需要去改變相關號碼。

回撥最後來電 [漏接] 有時候，人們會漏接某些電話，您可撥打此區所設定的號碼，查看最後的來電是誰打的，然後撥打回去。

回撥最後來電 [撥入] 您剛完成來電通話，但爲了某些原因你需要再通話一次，請撥打此區所設定的號碼，即可撥打給剛剛通話的人員。

回撥最後來電 [撥出] 請撥打此區所設定的號碼，再次撥打剛剛去電的人員。

來電跟隨 [全部][執行] 請撥打此區所設定的號碼，轉送全部來電給指定的位置。

來電跟隨 [解除] 請撥打此區所設定的號碼，解除來電跟隨功能。

來電跟隨 [忙線][執行] 電話忙線時，請撥打此區所設定的號碼，轉送來電給指定的位置。

來電跟隨 [無回應][執行] 來電欲連接的電話沒有回應時，請撥打此區所設定的號碼，轉送所有來電至指定位址。

勿打擾 [執行] 請撥打此區所設定的號碼，執行請勿打擾功能。

勿打擾 [解除] 請撥打此區所設定的號碼，解除請勿打擾功能。

隱藏撥出號碼 [執行] 請撥打此區所設定的號碼，讓您的電話號碼不會顯示在對方的顯示面板上。

隱藏撥出號碼 [解除] 請撥打此區所設定的號碼，解除此項功能。

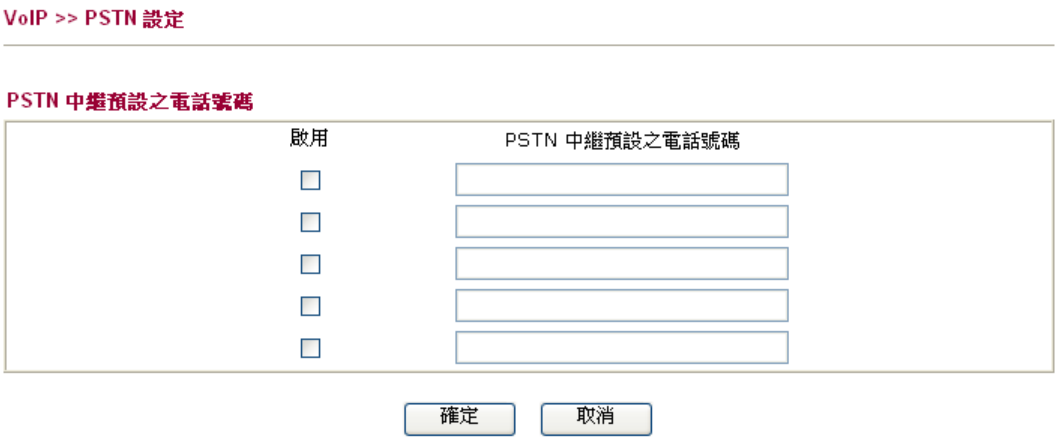
來電待接 [執行] 請撥打此區所設定的號碼，讓所有的來電等待您的回應。

來電待接 [解除] 請撥打此區所設定的號碼，解除此項功能。

封鎖匿名 [執行]	請撥打此區所設定的號碼，封鎖所有未之身分的來電。
封鎖匿名 [解除]	請撥打此區所設定的號碼，解除此項功能。
封鎖不明網域 [執行]	請撥打此區所設定的號碼，封鎖所有未知網域的來電。
封鎖不明網域 [解除]	請撥打此區所設定的號碼，解除此項功能。
封鎖 IP 來電 [執行]	請撥打此區所設定的號碼，封鎖所有自 IP 位址的來電。
封鎖 IP 來電 [解除]	請撥打此區所設定的號碼，解除此項功能。
封鎖最後來電 [執行]	請撥打此區所設定的號碼，封鎖最後的來電。

PSTN 設定

一些無法利用 VoIP 撥打的緊急電話(例如 119)或是特殊的電話僅能使用 PSTN 線路撥打出去，爲瞭解決這個問題，這個頁面讓您設定五組 PSTN 號碼，以便在網路斷線時可以撥打出去。請在 **PSTN 中繼電話號碼**欄位中輸入電話號碼。



接著請勾選**啓用**方塊讓 PSTN 號碼在您需要時可以撥打出去。

4.11.2 SIP 帳號

在此頁面中，您可以調整自己的 SIP 設定，當您申請一個帳號時，您的 ISP 服務供應商會給您一個帳號名稱或是使用者名稱、SIP 登錄者、代理人和網功能變數名稱稱(最後三種在某些條件下，有可能是完全相同的)，您可以告訴您的成員有關您的 SIP 位址，表示法爲**帳號名稱@網功能變數名稱稱**。

當路由器打開時，將以使用帳號名稱@網功能變數名稱稱來登錄，之後，您的電話將由 SIP 代理者以帳號名稱@網功能變數名稱稱傳送至目的地作爲辨識之用。

注意: 振鈴通訊埠的項目會依照您所使用的路由器而有所差異。

索引 按此鈕進入下一層設定頁面設定 SIP 帳號。

設定檔 顯示帳號的設定檔名稱。

網域 顯示 SIP 註冊伺服器的網功能變數名稱稱或是 IP 位址。

伺服器 顯示 SIP 伺服器的網功能變數名稱稱或是 IP 位址。

帳號名稱 顯示@前面的 SIP 位址帳號名稱。

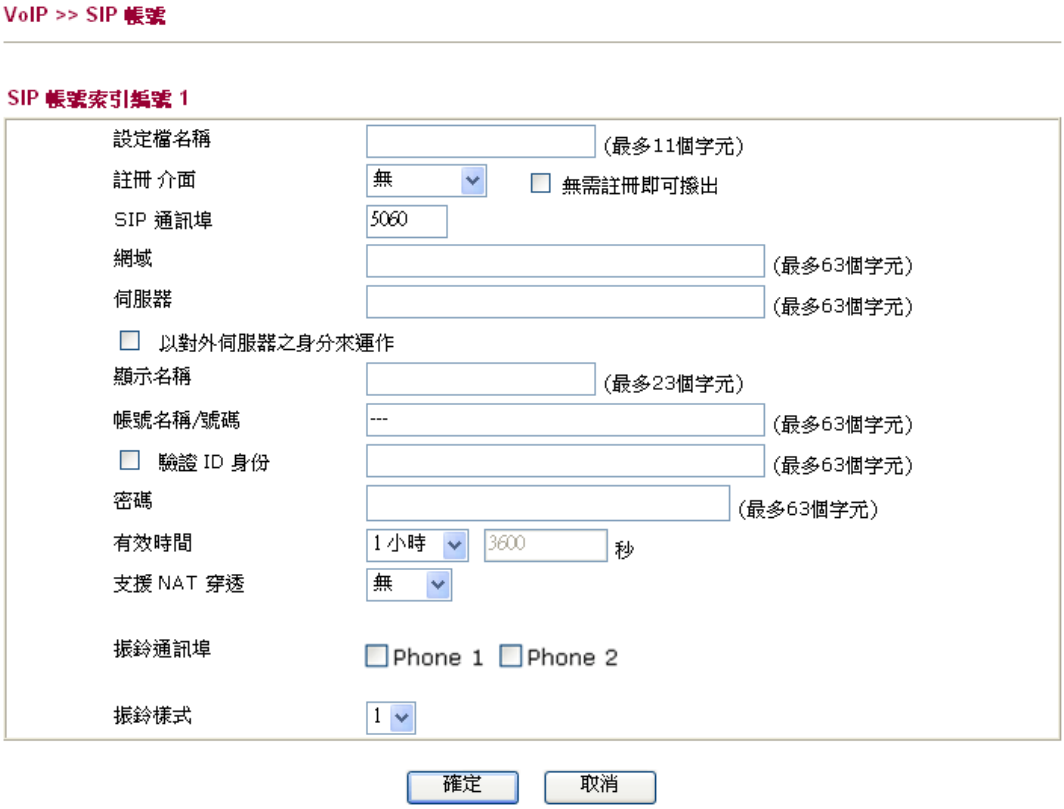
振鈴通訊埠 指定接收電話時由哪一個通訊埠響鈴。。

狀態 顯示相關 SIP 帳號的狀態，**R** 表示此帳號已註冊成功，**–** 表示尚未成功註冊。

STUN 伺服器 輸入 STUN 伺服器的 IP 位址或是網域。

外部 IP 輸入閘道 IP 位址。

SIP PING 間隔 預設值爲 150 秒，對 Nortel 伺服器而言這項設定是相當有用的。



設定檔名稱

指定一個名稱作爲辨識之用，您可以使用與網域類似的名稱，例如網功能變數名稱稱爲 *draytel.org*,您就可以在本區中設定 *draytel-1*。

由此註冊

指定您申請註冊時所透過的介面爲何，如果您不想註冊個人資料而直接使用 VoIP 撥號功能，請選擇**無**。某些 SIP 伺服器允許使用者不須登錄即可使用 VoIP 功能，針對這類伺服器，請您選擇**自動**，系統將爲您選擇最佳方式作爲 VoIP 撥號之用。

設定檔名稱

指定一個名稱作爲辨識之用，您可以使用與網域類似的名稱，例如網功能變數名稱稱爲 *draytel.org*,您就可以在本區中設定 *draytel-1*。

由此註冊

指定您申請註冊時所透過的介面爲何，如果您不想註冊個人資料而直接使用 VoIP 撥號功能，請選擇**無**。某些 SIP 伺服器允許使用者不須登錄即可使用 VoIP 功能，針對這類伺服器，請您選擇**自動**，系統將爲您選擇最佳方式作爲 VoIP 撥號之用。

以對外伺服器之身份來運作

勾選此方塊以啓用伺服器成爲對外伺服器。

顯示名稱 您想要在朋友的電話顯示螢幕上出現的名稱。

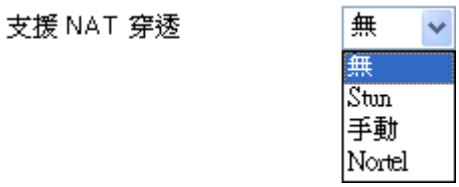
帳號名稱/號碼 輸入 SIP 位址的帳號名稱，例如@之前的文字。

驗證 ID 身分 勾選此方塊啓用此功能並輸入名稱或號碼供 SIP 驗證，如果設定值與帳戶名稱相同，您就不必勾選此方塊另設數值。

密碼 當您以 SIP 服務註冊時所需提供的密碼。

有效時間 爲 SIP 伺服器提保存使用者註冊帳號的有效時間。在到期之前，路由器將會再次傳送另一個註冊需求給予 SIP 登錄伺服器。

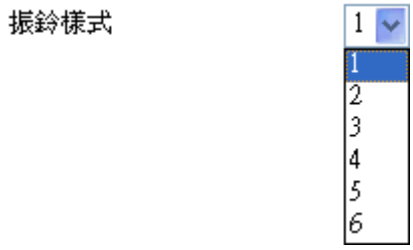
NAT 穿透 如果路由器(寬頻路由器)是透過其他裝置連接上網際網路，您就必須設定此功能。



無 –.關閉此功能。
Stun –若路由器支援 Stun 伺服器，請選擇此項目。
手動 –若您想要指定外部 IP 位址作爲 NAT transversal 支援，請選擇此項目。
Nortel – 如果軟體支援 nortel 方案，您可以選擇此項目。

振鈴通訊埠 設定 VoIP 1,VoIP 2 作爲 SIP 帳號的預設振鈴通訊埠。

振鈴樣式 選擇 VoIP 電話的振鈴樣式。



4.11.3 電話設定

本頁讓使用者得以個別設定 Phone 1 和 Phone 2 。

電話清單

通訊埠 – 有種通訊埠類型提供給您選擇。

通話功能 – 這個欄位簡單描述此通電話的功能供使用者參考。

Codec – 每個通訊埠的預設 Codec 設定都會顯示在本區，您可以按索引號碼變更每個電話通訊埠的設定。

音調 – 顯示進階頁面所設定的音調值。

音量 - 顯示進階頁面中 Mic/Speaker 的音量設定。

預設 SIP 帳號 – “draytel_1” 是預設的 SIP 帳號，您可按索引下方的編號變更 SIP 帳號設定。

DTMF 中繼 –顯示進階頁面中所設定的 DTMF 模式。

RTP

對稱 RTP – 勾選此方塊啓用此功能。若要讓資料傳輸能在本機路由器與遠端路由器之間暢行無阻而不至於因 IP 漏失而誤導的情形發生，請您勾選此方塊解決這個問題。

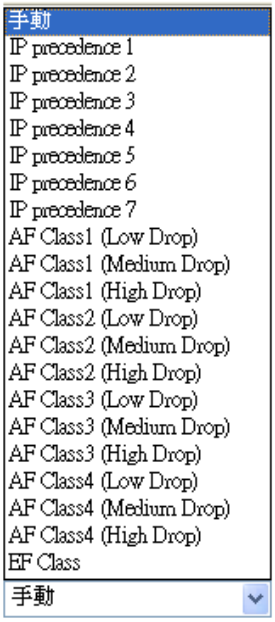
RTP 通訊埠起點 - 指定 RTP 之通訊埠起點，預設值爲 10050。

RTP 通訊埠終點 - 指定 RTP 之通訊埠終點，預設值爲 15000。

RTP TOS –此項可決定 VoIP 封包的等級，請使用下拉式選

項選擇其中一種。

RTP TOS



Phone Port 細節設定

請按索引欄位元下方的 1 或 2 連結進入下麵的設定頁面。

熱線　勾選此方塊啓用此功能，請在本區輸入 SIP URL 讓系統在您拿起話機後自動撥號。

連線數計時器　勾選此方塊啓用此功能，您在本區所設定的限制時間內如果沒有任何回應，連線電話將會自動關閉。

指定轉接　共有四種選項可以選擇，**停用**可關閉此功能，**永遠**則表示來電會一直轉接到 SIP URL 上，**忙線**則表示來電只在本機忙碌時轉接到 SIP URL，**沒回應**則表示來電若未收到任何回應，電話都會在切斷時轉接到 SIP URL 上。

SIP URL – 請輸入 SIP URL (例如 aaa@draytel.org 或 abc@iptel.org) 做爲轉送電話的終點。
逾時 – 設定電話轉接的逾時現制，預設值爲 30 秒。

DND (勿幹擾)　設定一段和平時間不受任何 VoIP 來電的幹擾。在此期間，撥號進來的人會聽到忙線的聲音，而本機用戶則聽不到任何電話鈴聲。

索引(1-60) 於電話簿 - 輸入例外電話於此方塊內，列於此之電話不受勿幹擾的限制。詳細設定請參考**電話簿**一節。

CLIR (隱藏撥號者身分)　勾選此方塊讓撥號者身分不會顯示在話機的顯示面板上。

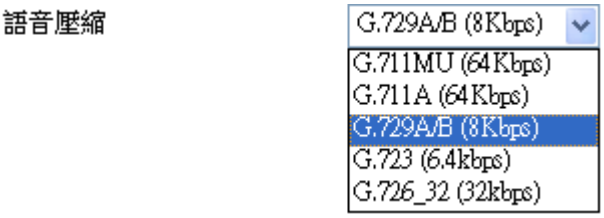
話中插接　勾選此方塊啓用此功能，提示聲音將會出現以告知使用者有電話在等待。

電話轉接

勾選此方塊啓用此功能，按轉接鍵轉接另一通電話，當電話連線成功時，掛上電話。此時另外二方就可直接溝通。

語音壓縮

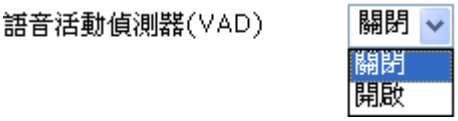
有五種不同的 CODEC 供您選擇，但真正被使用的 CODEC 在通訊建立前是和對方共同商議而得。預設的 CODEC 是 G.729A/B，它佔據較少的頻寬但是卻仍擁有良好的聲音品質，如果您想要使用 G.711，您最好具有至少 256Kbps 的上傳速率。



單一 Codec - 如果勾選此方塊，只有選定的 Codec 會被路由器套用。

語音資料長度 - 資料總數包含單一封包(10, 20, 30, 40, 50 和 60)，預設值爲 20ms，表示資料封包含 20ms 聲音資訊。

語音活動偵測器(AVD) - 選擇**開啓**啓動此項功能，以檢測使用者是否正在交談。如果安靜無聲，路由器將採取行動節省頻寬的使用。



預設 SIP 帳號

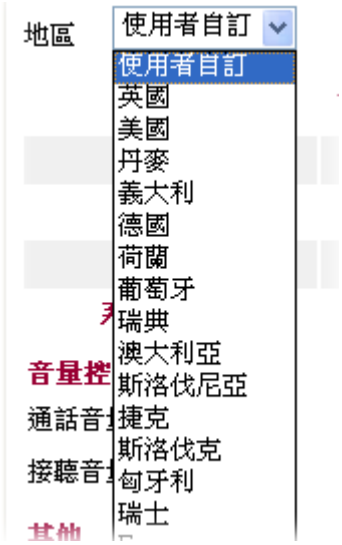
您可以設定 SIP 帳號(最多 6 組)，請使用下拉式清單選擇其中一組作爲預設帳號。

當帳號已經註冊時請使用撥號音 - 勾選此方塊啓用此功能。

此外，您也可以按**進階**按鈕進入深一層的設定。此項設定是爲了符合路由器安裝所在地區的電信習慣而提供，錯誤音調設定可能會造成使用者的不便。關於設定話機的聲音型態，方法很簡單，只要選擇適當的區域讓系統自動尋找事先設定的音調設定和呼叫 ID 類型，或是您也可選擇使用者自訂，然後以手動方式調整音調，TOn1, TOff1, TOn2 和 TOff2 表示音調型態的韻律，TOn1 和 TOn2 表示開啓聲音；TOff1 和 TOff2 則表示關閉聲音。

地區

選擇您目前所處地區，**來電顯示類型**、**撥號音**、**響鈴音**、**忙線音**和**系統擁塞音**都會自動顯示在本頁面上。如果您無法找到適合的地區，請您選擇**使用者自訂**，再自行輸入頁面所需的各式資料。



您也可以是個人需要指定各個區域內容，建議您採用預設值作爲 VoIP 通訊之用。

來電顯示類型

此處提供數種標準，以便在電話機面板上顯示來電者的身分，請依照路由器安裝所在地區選擇適合的類型，如果您不知道話機究竟支援哪種標準，請直接採用預設值。

音量控制

請輸入 1- 10 以設定麥克風的音量，數字越大聲音越大。

雜項

撥號音量控制 -此項設定用來調整撥號的音量大小，數字越小音量越大，建議使用預設值。

振鈴聲頻率 此項設定用來驅動鈴聲的頻率，建議使用預設值。

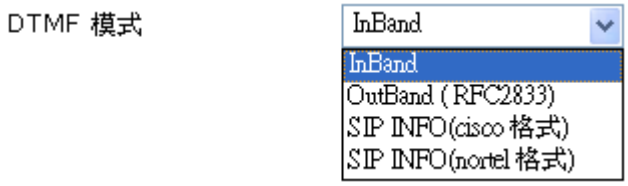
DTMF

DTMF 模式

InBand - 當您按壓電話上的鍵盤時，路由器將會直接以聲音模式傳送 DTMF 音調。

OutBand - 路由器將會抓取您所按壓的鍵盤號碼然後以數位格式傳送至另一端；接收者將會依照所接收的數位格式來產生音調。這個功能在網路擁塞的情形下是很有用處的，因*爲它仍可保持 DTMF 音調的準確度。*

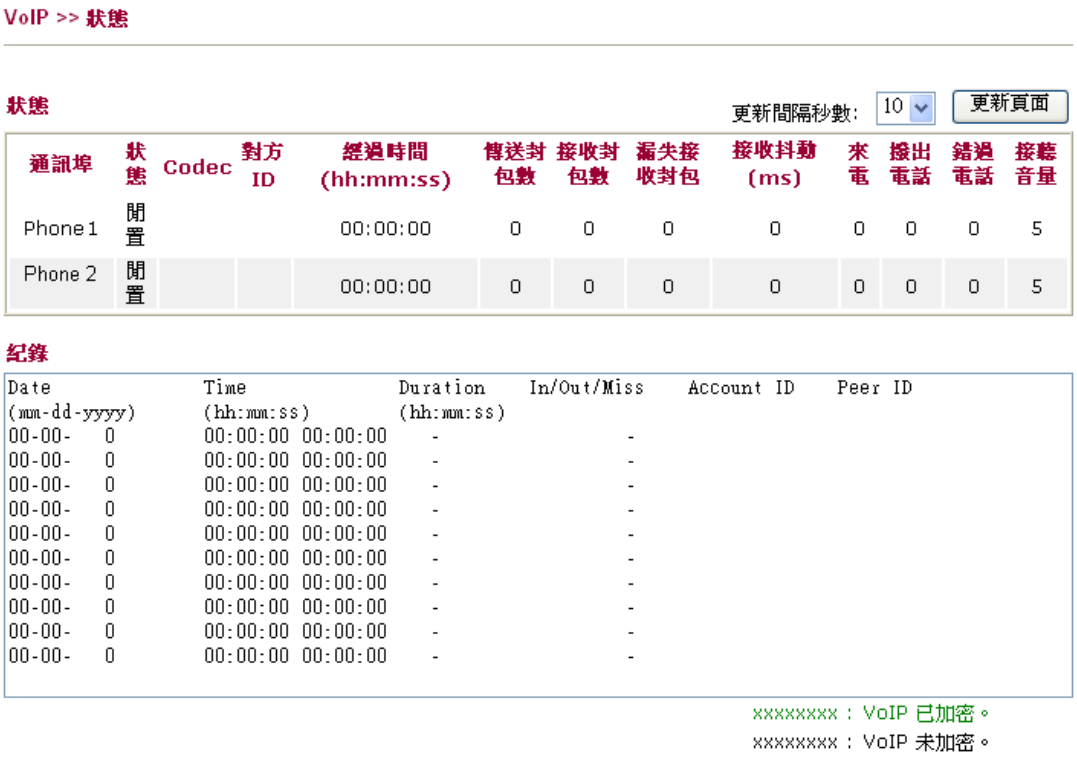
SIP 資訊-路由器將抓取 DTMF 音調然後以 SIP 訊息轉送給遠端用戶。

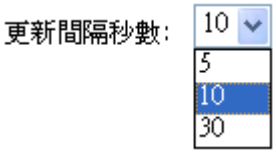


Payload 類型 (rfc2833) - 請自 96 至 127 中選擇一個數字，預設值爲 101，此項設定只對 OutBand (RFC2833)模式有效。

4.11.4 狀態

在 VoIP 撥號狀態下，您可以看見 VoIP 1 和 VoIP 2 的 codec、連線情形和其他重要的撥號狀態資料。



更新間隔秒數	指定更新的間隔秒數以取得最新的 VoIP 撥號資訊，當按下**更新頁面**按鈕時，頁面資訊將會立即更新。 
通訊埠	顯示目前 VoIP 電話的連線通訊埠。
狀態	顯示 VoIP 連線狀態。 **閒置** -表示 VoIP 功能正處於閒置狀態。 **HANG_UP** -表示連線並未建立(忙線音調)。 **CONNECTING** -表示用戶正撥出號碼中。 **WAIT_ANS** -表示已連線並等待遠端用戶的回答。 **ALERTING** -表示有來電。 **ACTIVE**-表示 VoIP 連線啓動。
Codec	表示目前頻道所利用的聲音 codec。
對方 ID	撥進或撥出之對方 ID (格式可以是 IP 位址或是網功能變數名稱稱)。
經過時間	通話時間以秒數計算。
傳送封包數	在連線中全部的傳送封包數量。
接收封包數	在連線中全部的接收封包數量。
漏失接收封包	在連線中漏失的全部封包。
接收抖動	接收聲音封包抖動狀態。
來電	已接來電總數。
撥出電話	撥出電話總數。
接聽音量	電話音量大小。
記錄	顯示 VoIP 電話紀錄。

4.12 無線區域網路設定

本節所提供的資訊僅針對 *n* 系列機型。

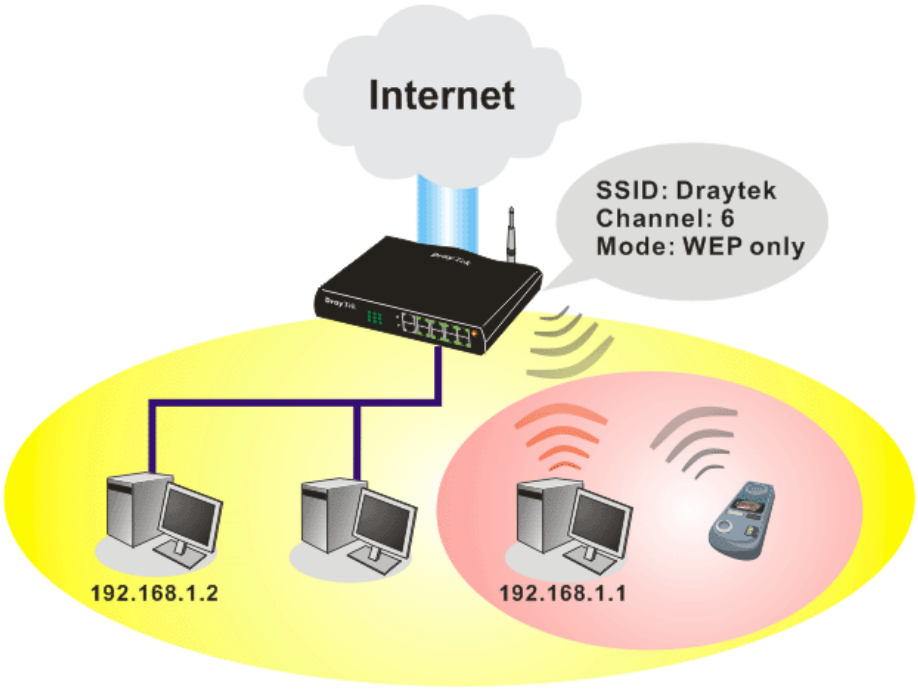
4.12.1 基本觀念

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，又稱爲 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：

4.12.2 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：

啓用 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。目前路由器支援的協定有綜合(11b+11g)，僅 11g，僅 11b，綜合((11g+11n)，僅 11n 及綜合((11b+11g+11n)。請選擇綜合 (11b11g+11n) 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**應用**的**排程設定**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 值爲 **DrayTek**，建議您變更爲另一個特殊名稱。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

LAN – 勾選此方塊讓使用相同 SSID 的無線用戶無法存取 LAN 端有線連線的電腦資料。

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。

頻道

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幹擾的話，您可自行切換爲其他頻道。

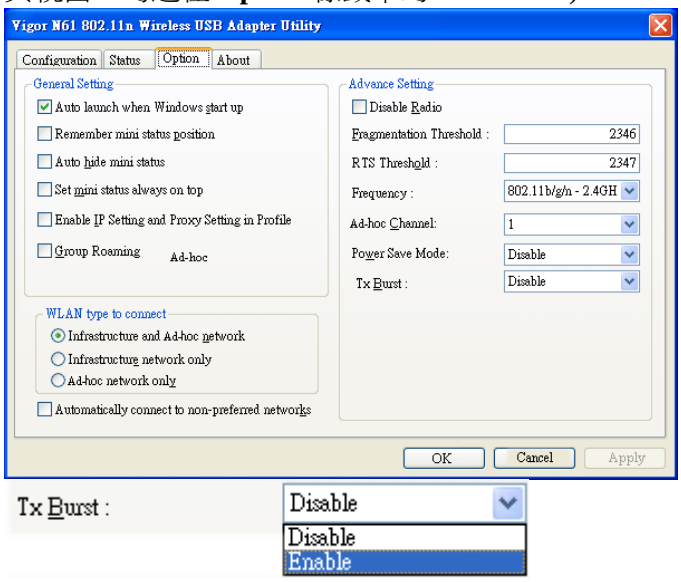
長封包標頭

此選項用來定義 802.11 封包中同步區塊的長度，最新的無線網路以 56 bit 同步區來使用短封包標頭，而不是以 128 bit 同步區來使用長封包標頭。不過，一些原始 11b 無線網路裝置只有支援長封包標頭而已，因此如果您需要和此種裝置通訊溝通的話，請勾選此方塊。

Packet-OVERDRIVE

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 **Tx Burst)**。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。

注意: 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 **Option** 標籤中的 **TxBURST**).



流量控制

可控制透過無線連線傳輸的資料傳送速率。

上傳 – 勾選啓用方塊並輸入傳輸速率作爲上傳資料之速率，預設值爲 30,000 kbps。

下載–勾選啓用方塊並輸入傳輸速率作爲下載資料之速率，預設值爲 30,000 kbps。

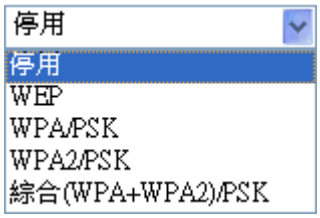
4.12.3 安全性設定

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。

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。

模式

此一設定有數種模式可供您選擇。



停用 - 關閉加密機制。

WEP - 只接受 WEP 用戶以及僅接受以 WEP 金鑰輸入的加密鑰匙。

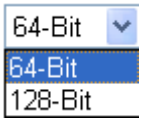
WPA/PSK -接受 WPA 用戶，請在 PSK 中輸入加密金鑰。

WPA2/PSK -接受 WPA2 用戶，請在 PSK 中輸入加密金鑰。

綜合 (WPA+ WPA2)/PSK – 同時接受 WPA 與 WPA2 用戶，請在 PSK 中輸入加密金鑰。

WPA

WPA 可藉由金鑰加密每個來自無線網路的訊框，可在本區手動輸入 PSK，或是藉由 802.1x 驗證方式來自動加密。**預先共用金鑰 (PSK)** - 輸入 **8~63** 個 ASCII 字元，像是 012345678（或是 64 個 16 進位數字，以 0x 開頭，如 0x321253abcde...等）。

WEP	**64-Bit** - 針對 64 位元的 WEP 金鑰，請輸入 5 個 ASCII 字元，像是 12345（或是 10 個 16 進位數字，以 0x 開頭，如 0x4142434445）。 **128-Bit** - 針對 128 位元的 WEP 金鑰，請輸入 13 個 ASCII 字元，像是 ABCDEFGHIJKLM（或是 16 個 16 進位數字，以 0x 開頭，如 0x4142434445）。  所有的無線裝置都必須支援相同的 WEP 加密位元大小，並擁有相同的金鑰。這裡可以輸入四組金鑰，但一次只能選擇一組號碼來使用，這些金鑰可以 ASCII 文字或是 16 進位元字元來輸入。請點選您想使用的金鑰組別。

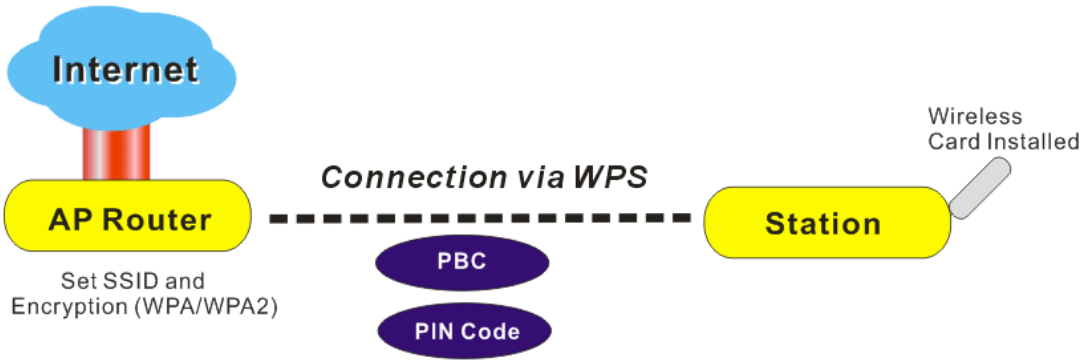
4.12.4 連線控制

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。只有設定有效的 MAC 位址得以存取無線區域網路介面，請選**連線控制**連結，開啓新的網頁，如同下圖所示，您即可在此頁面上編輯用戶端的 MAC 位址達到控制其存取權的目的。

啓動 Mac 位址過濾器	請勾選任一 SSID 1 到 4 中以啓動無線 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。
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。

4.12.5 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。

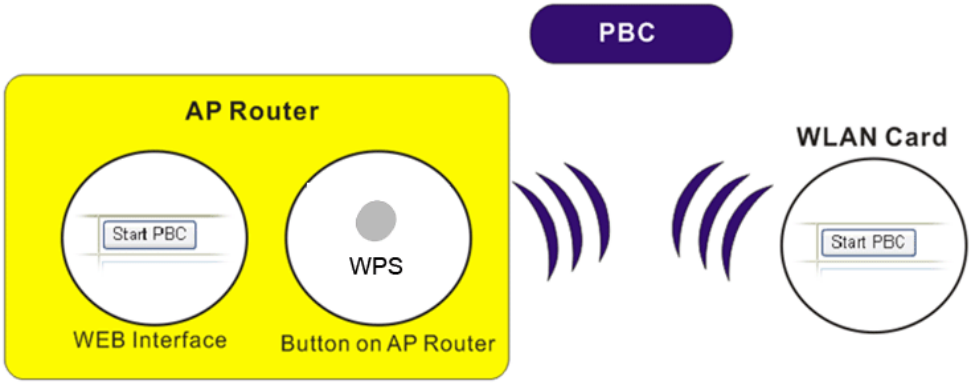


注意: 此功能僅在無線用戶端也支援 WPS 功能時可用。

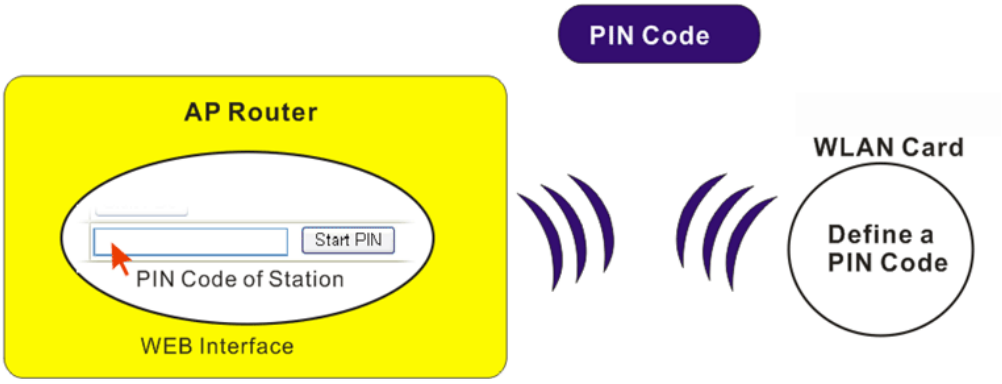
建立無線網路用戶與Vigor路由器之間的連線有個快速及簡單的方式，使用者不需要每次都必須選擇加密模式，或輸入任何長篇的資料以建立無線連線。使用者只要按下無線用戶端中的一個小小按鈕，WPS功能就會替他/她自動建立一個無線連線。

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 2920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** 按扭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。



因爲 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。

下圖爲**線區域網路>>WPS** 網頁畫面。

啓用 WPS 勾選此方塊啓動 WPS 設定。

WPS 狀態 顯示 WPS 相關的系統訊息，如果無線安全性(加密)功能已設定，您可以在此看到"設定完畢"等訊息。

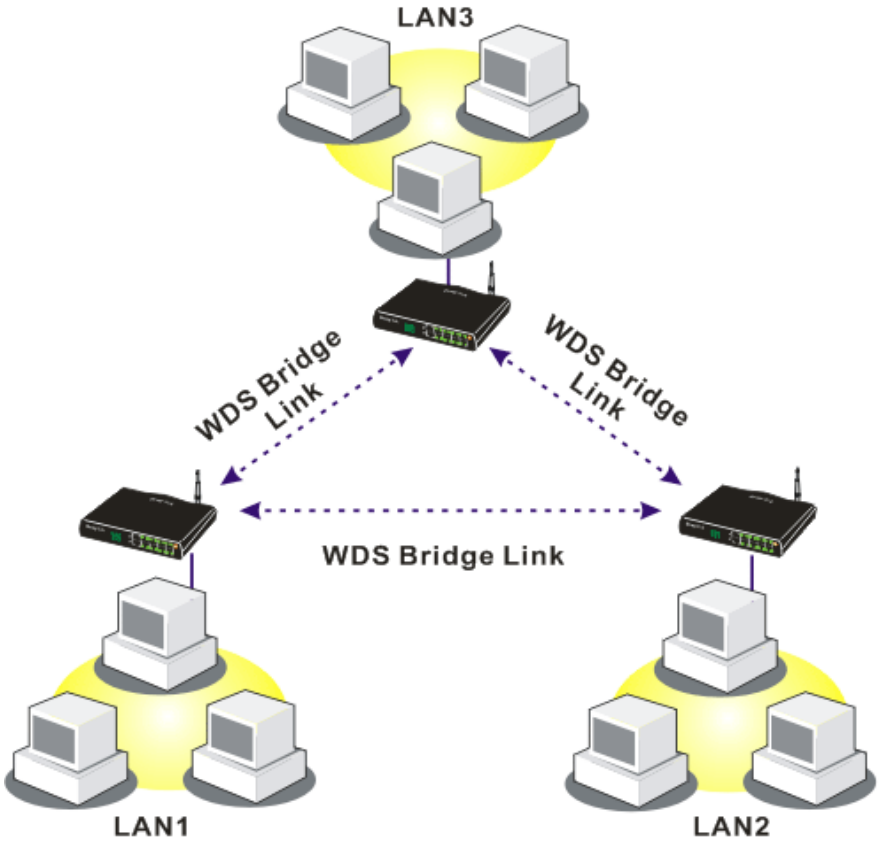
SSID	顯示路由器的 SSID1 名稱，WPS 僅在 SSID1 中可用。
驗證模式	顯示路由器目前的驗證模式，請注意僅有 WPA2/PSK 和 WPA/PSK 支援 WPS。
藉由 Push 按鈕來設定	請按**啓動 PBC** 啓用 Push-Button 式的 WPS 設定程式，路由器將會等待 2 分鐘取得無線用戶傳送過來的 WPS 需求，當 WPS 運作時，WLAN 燈號將會快速閃爍，2 分鐘後，路由器會回復一般的運作(您必須在 2 分鐘內設定 WPS)。
藉由用戶端 PinCode 來設定	請輸入您想要連接的無線用戶所指定的 PIN 碼，在按**啓動 PIN** 按鈕。當 WPS 運作時，WLAN 燈號將會快速閃爍，2 分鐘後，路由器會回復一般的運作(您必須在 2 分鐘內設定 WPS)。

4.12.6 WDS

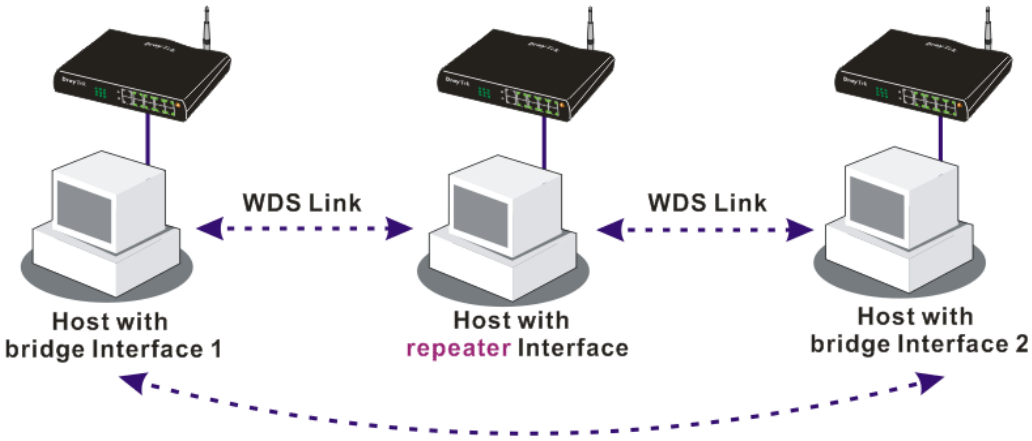
WDS 表示無線分派系統，是一個連結二個無線基地台的通訊協定，通常可以下列二種方式來應用。

- 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，一爲**橋接**一爲**中繼**，下圖顯示 WDS 橋接介面的功能：

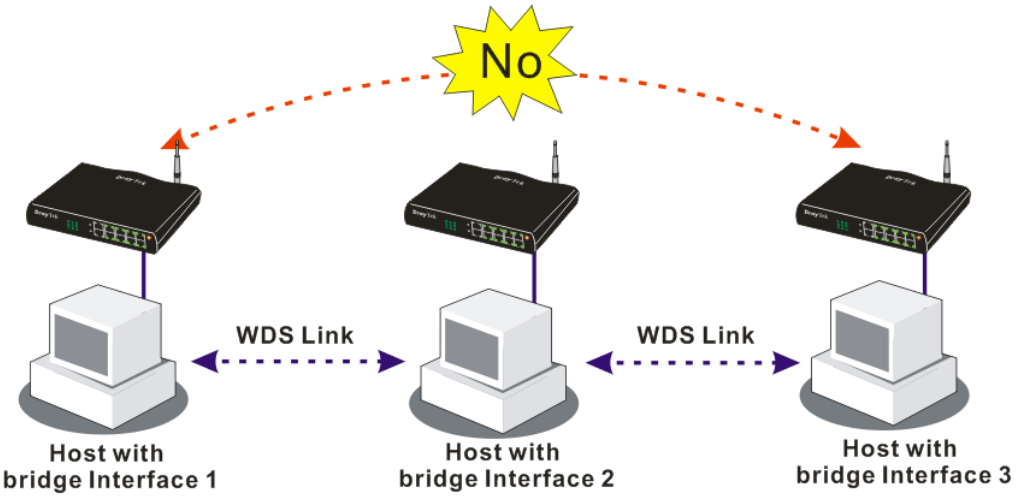


WDS-中繼模式的應用則描繪如下：



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：

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**安全性設定**頁面中同樣的金鑰。如果您並未在**安全性設定**頁面中設定任何的金鑰，此方塊將暫時無法使用。

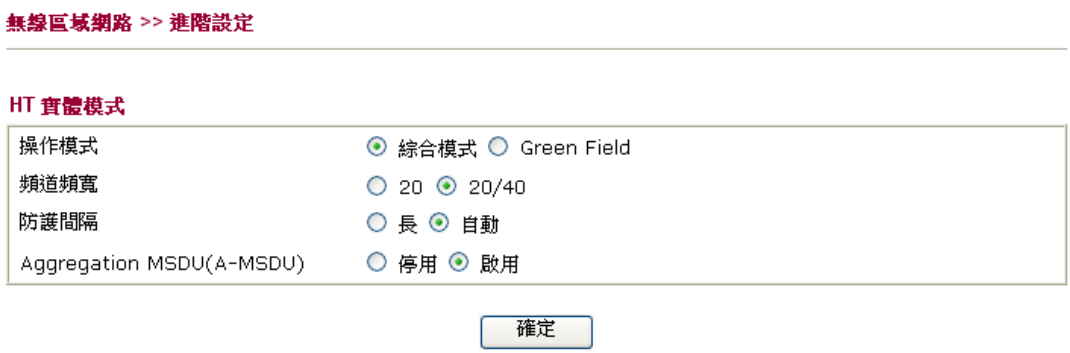
預設共用金鑰 輸入開頭爲“0x”之 8 ~ 63 個 ASCII 字元或是 64 的 16 進位的數字。

橋接 如果您選擇橋接做爲通訊模式，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**啓用**方塊。

中繼	如果您選擇**中繼**做爲通訊模式，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**啓用**方塊。
無線基地台功能	按**啓用**讓路由器提供無線基地台的服務；按**停用**取消此功能。
狀態	允許使用者傳送招呼訊息給對方，然而則此功能僅在對方也支援時才有效用。

4.12.7 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。



操作模式	**混合模式** – 路由器可以 802.11a/b/g 和 802.11n 標準所支援的方式來傳送資料，但是若 802.11g 或 802.11b 無線用戶連接上此路由器的話，整個網路傳輸速率將會降低。 **Green Field** – 爲了取得較高的處理能力，請選擇此項模式。此模式僅讓資料在 11n 系統中傳輸。另外，此模式也沒有防護機制好避免與相鄰採用 802.11a/b/g 的裝置產生衝突。
頻道頻寬	**20-** 路由器使用 20Mhz 作爲基地台與無線用戶之間傳輸的資料速度。 **20/40 –** 路由器使用 20Mhz 或 40Mhz 作爲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**自動**的話，基地台路由器將依照無線用戶的能力，選擇較短的間隔(增加無線性能-)或是較長的間隔來傳輸資料。
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，預設值爲**啓動**。

4.12.8 WMM 設定

WMM 爲 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，此功能是針對大多數支援 VoIP 的行動電話或是無線電話而設計的。

WMM 功能 在無線資料傳輸中應用 WMM 參數，請按**啓用**鈕。

APSD 功能 預設值爲**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 **CWMin** 表示 contention Window-Min 而**CWMax**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。

ACM	爲 Admission Control Mandatory 的縮寫，可以限制無線用戶僅使用特定類型。 **注意:** Vigor2920 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。
AckPolicy	**“**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。 “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。

4.12.9 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。

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。

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**新增**，稍後該 MAC 位址即會加入 WDS 設定頁面中。

4.12.10 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。

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**。

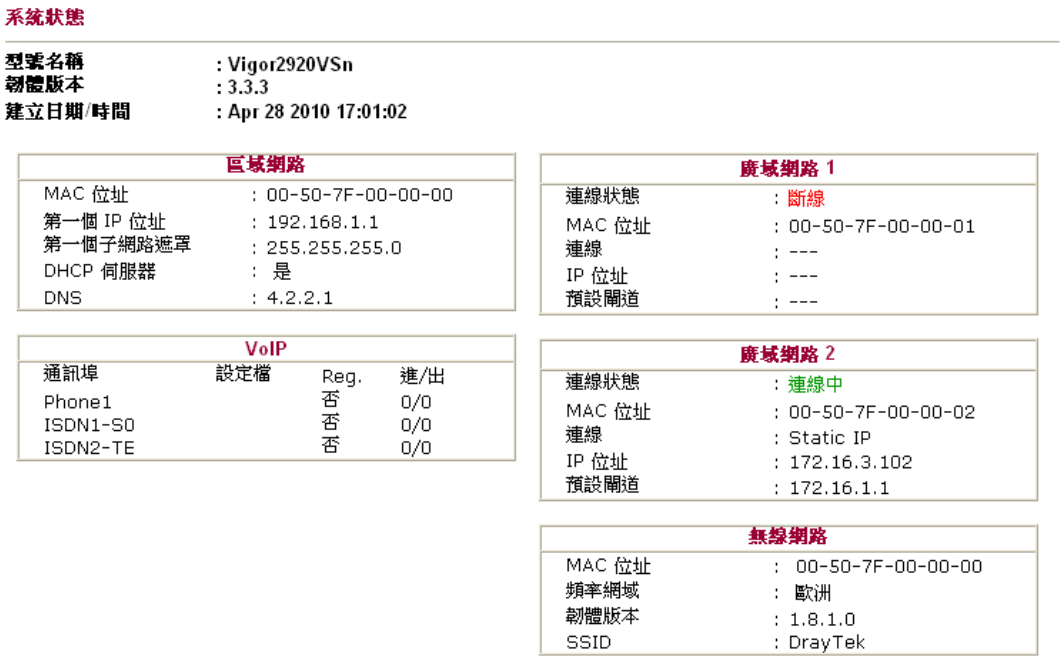
4.13 系統維護

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。

下圖爲系統維護的主要設定功能。

4.13.1 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。



型號名稱 顯示路由器的型號名稱。

韌體版本 顯示路由器的韌體版本。

建立日期與時間 顯示目前韌體建立的日期與時間。

區域網路------

MAC 位址 顯示區域網路介面的 MAC 位址。

第一個 IP 位址 顯示區域網路介面的 IP 位址。

第一個子網路遮罩 顯示區域網路介面的子網路遮罩位址。

DHCP 伺服器 顯示區域網路介面的 DHCP 伺服器目前的狀態。

DNS 顯示主要 DNS 的 IP 位址。

廣域網路------

連線狀態 顯示目前實體連線的狀態。

MAC 位址 顯示 WAN 介面的 MAC 位址。

連線 顯示目前連線的類型。

IP 位址 顯示 WAN 介面的 IP 位址。

預設閘道 顯示預設閘道指定的 IP 位址。

無線網路------

MAC 位址 顯示無線區域網路的 MAC 位址。

頻率網域 網域可以是歐洲(13 個可用頻道)，美國(11 個可用頻道)，無線產品所支援之可用頻道在不同的國家下是不相同的。

韌體版本 表示配備 WLAN miniPCi 卡的詳細資訊，同時可以提供該卡相關的特徵訊息。

SSID 顯示路由器的 SSID。

4.13.2 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。

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

URL/使用者名稱/密碼 – 此資料必須依照您想要連結的 ACS 內容來輸入，請參考 ACS 使用者取得詳細的資訊。

CPE 用戶端 基本上您不需要在此輸入任何資料，因爲這邊的資料主要是提供給 ACS 伺服器參考使用的。

啓用/停用 – 有時候，系統可能會產生埠號衝突，爲瞭

解決這個問題，您可能需要改變 CPE 的埠號，請勾選**啓用**再變更埠號。

定期通知設定　預設值爲**啓用**，請設定間隔時間或是排程時間，讓路由器傳送通知訊息給 CPE 端，或是選**停用**關閉通知機制。

STUN 設定　預設值是**停用**，如果您選擇了**啓用**，請輸入下述相關資料：

伺服器 IP – 輸入 STUN 伺服器的 IP 位址。

伺服器埠號 – 輸入 STUN 伺服器的埠號。

最小維持連線期間 – 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。請輸入數字作爲最小的維持時間，預設值爲 60 秒。

最大維持連線期間 – 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。請輸入數字作爲最大的維持時間，數值-1 表示未指定最大維持時間。

4.13.3 系統管理員密碼

本頁允許您設定新的密碼。

舊密碼　請輸入舊密碼，出廠預設值是空白的。

新密碼　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。

4.13.4 使用者密碼

本頁允許您設定新的密碼。

舊密碼	請輸入舊密碼，出廠預設值是空白的。
新密碼	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。

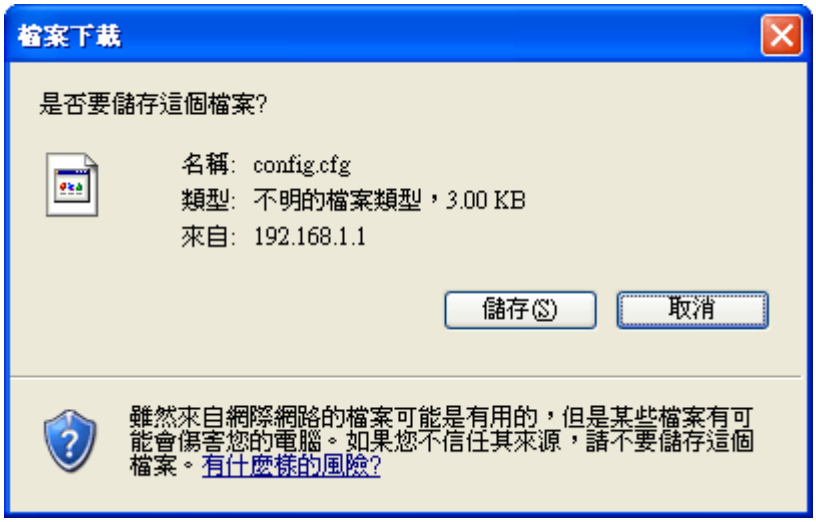
4.13.5 設定備份

設定備份

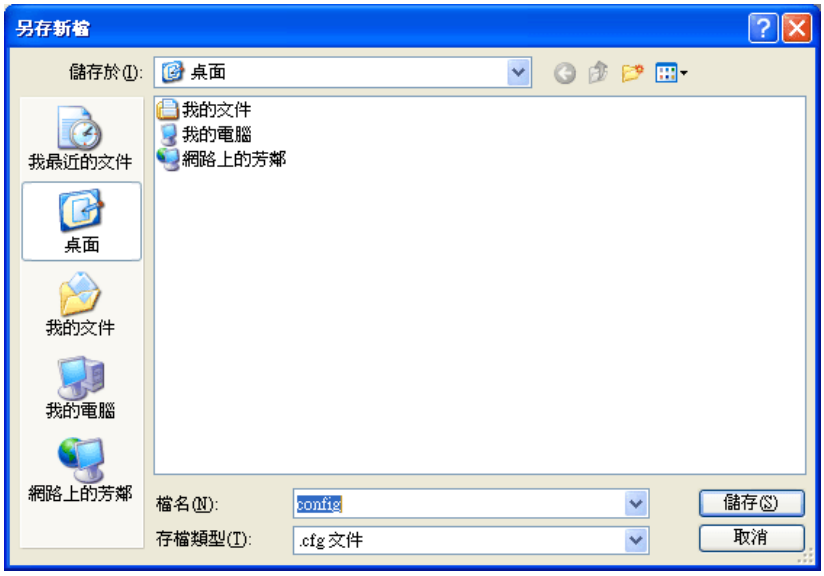
請依照下列步驟備份您的路由器設定。

1. 在**系統維護**群組中按**設定備份**，您將可看見如下視窗。

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，預設檔名爲 **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。

2. 按**瀏覽**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。

4.13.6 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。

啓用 勾選**啓用**以啓動系統記錄服務功能/啓動郵件警示功能。

伺服器 IP 位元址 指定全部系統紀錄訊息傳送前往目的地之 IP 位址。

目標通訊埠 指定全部系統紀錄訊息傳送前往目的地之通訊埠。

啓用 syslog 訊息 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。

傳送測試郵件 執行一個簡單的電子郵件測試，請於下方先指定郵件地址，然後在按此測試鈕，以檢查此電子郵件地址是否可用。

SMTP 伺服器 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。

收件人 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。

回信位址 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。

驗證 當使用電子郵件應用程式，勾選此方塊可啓動驗證的功能。

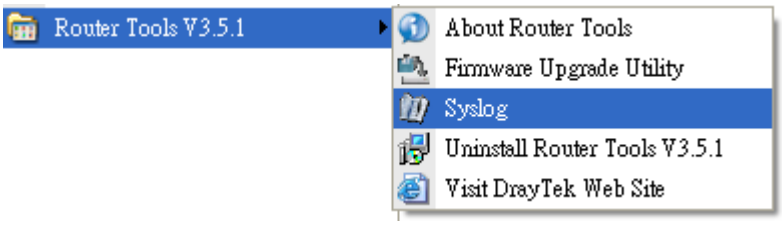
使用者名稱 輸入驗證所需的使用者名稱。

密碼	輸入驗證所需的密碼。
啓用郵件警告訊息	勾選此方塊以便在路由器檢測到相關項目時，自動傳送警告訊息至郵件信箱。

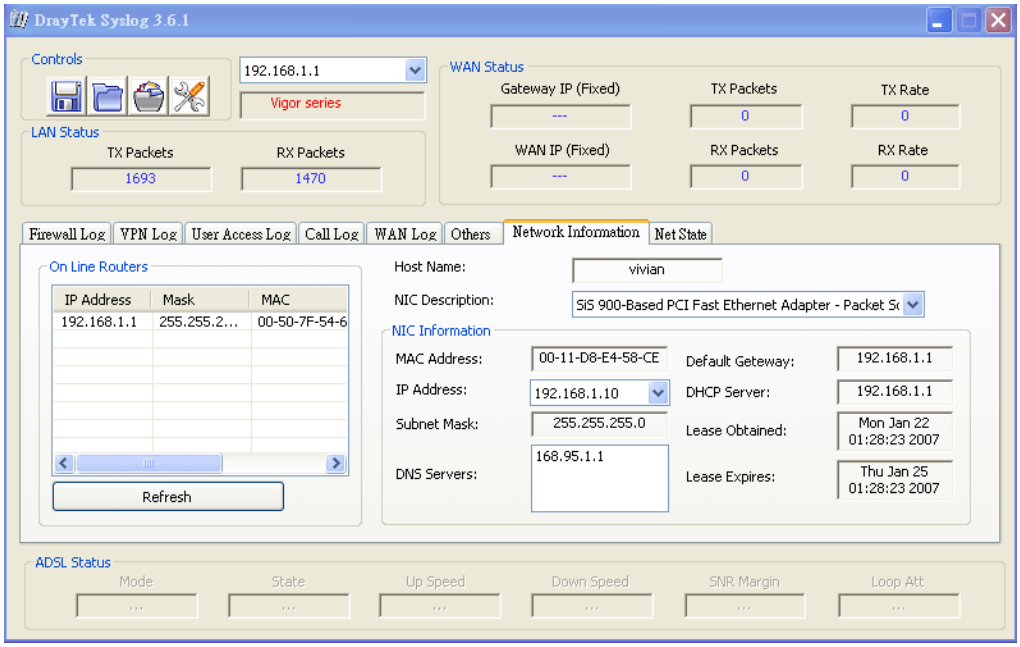
按**確定**儲存所有的設定。

如欲檢視系統紀錄，請依照下述步驟進行：

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

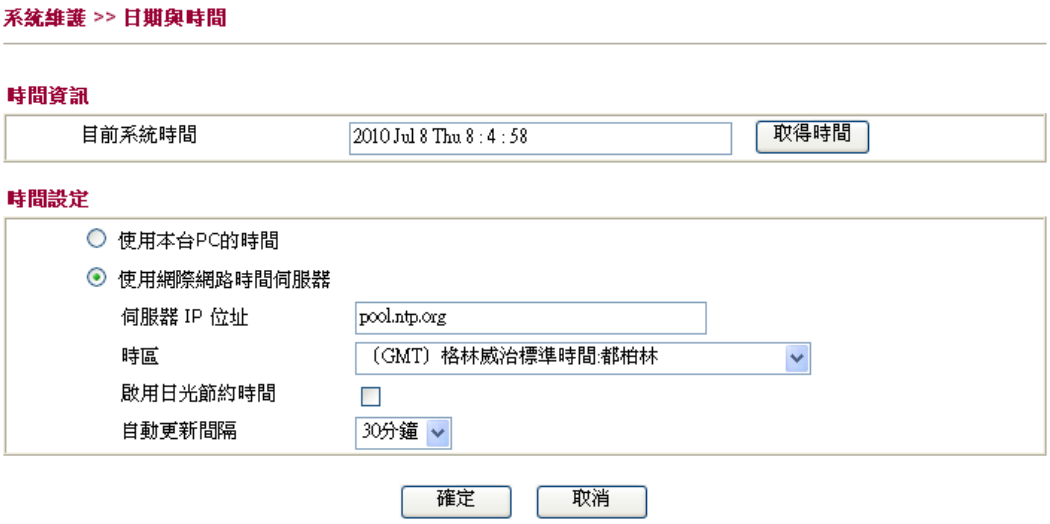


3. 自 Syslog 畫面上，選擇您想要監視的路由器。請記住在網路資訊**(Network Information)**中，選擇用來連接路由器的網路交換器，否則您無法成功檢索來自路由器的資訊。



4.13.7 時間和日期

允許您指定自何處取得路由器時間。



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，作。

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。

伺服器 IP 位址 輸入時間伺服器的 IP 地址。

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。

4.13.8 管理

本頁讓您管理存取控制、存取清單、通訊埠設定以及 SNMP 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。

允許從網路管理 勾選此方塊允許系統管理者自網際網路登入。系統提供數種不同的伺服器供您選擇作爲網路管理介面，請勾選所需的項目。

斷絕來自網際網路的 PING 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啓動的。

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。

清單 IP – 指定一個允許登入至路由器的 IP 地址。

子網路遮罩 -代表允許登入至路由器的子網路遮罩。

使用者定義通訊埠 勾選此項以指定使用者定義的埠號作爲 Telnet、HTTP 和 FTP 伺服器之用。

預設通訊埠 勾選此項以使用標準埠號作爲 Telnet 和 HTTP 伺服器之用。

啓用 SNMP 代理程式 勾選此項以啓動此功能。

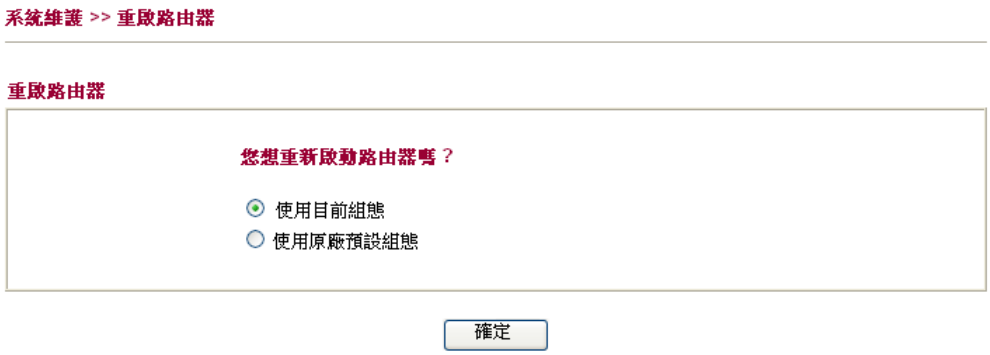
取得社群 (Get Community) 請輸入適當的文字以設定取得社群名稱，預設名稱爲 **public**。

設定社群 (Set Community) 請輸入適當的名稱以設定社群，預設名稱爲 **private**。

管理者主機 IP	設定一台主機做爲管理者以便執行 SNMP 功能，請輸入 IP 位址指定特定主機。
封鎖社群(Trap Community)	輸入適當名稱設定封鎖社群，預設名稱爲 **public**。
通知主機 IP	設定主機的 IP 地址接收封鎖社群的資料。
封鎖逾時	預設值爲 10 秒。

4.13.9 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。



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**確定**；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**確定**，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**確定**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。

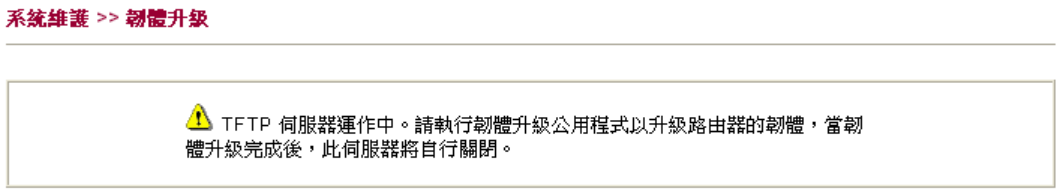
4.13.10 韌體升級

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，居易網站爲 www.draytek.com，FTP 站則是 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。

按**確定**，下述畫面將會出現，請先使用韌體更新工具完成更新。



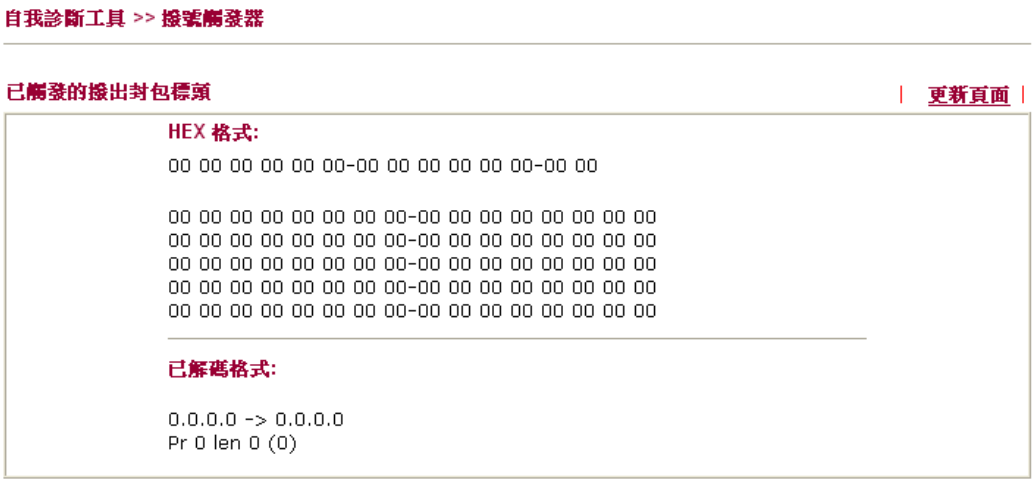
有關韌體更新的詳細資訊，請參考第五章。

4.14 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。以下爲自我診斷的選單項目：

4.14.1 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。

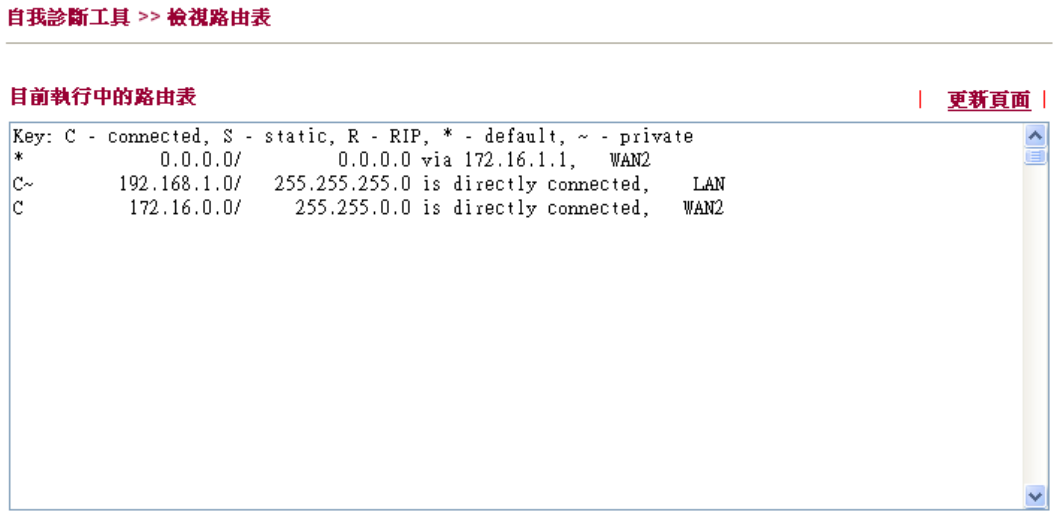


已解碼格式　　顯示來源 IP 位址、目標 IP 位址、通訊協定和封包的長度。

更新頁面　　按此鈕重新載入本頁。

4.14.2 路由表

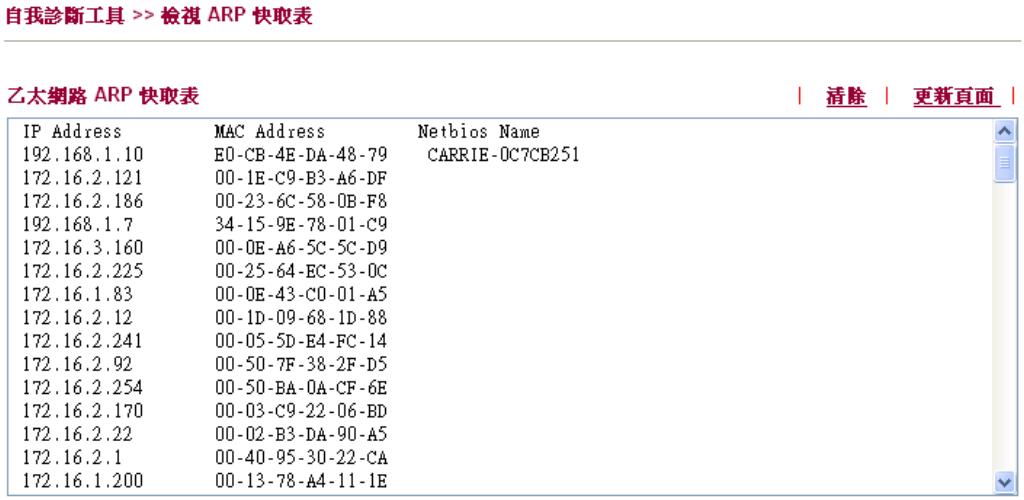
按**自我診斷工具**的**路由表**檢視路由器的路由表格，此表格可提供目前的 IP 路由資訊。



更新頁面 按此鈕重新載入本頁。

4.14.3 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。



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。

4.14.4 DHCP 表

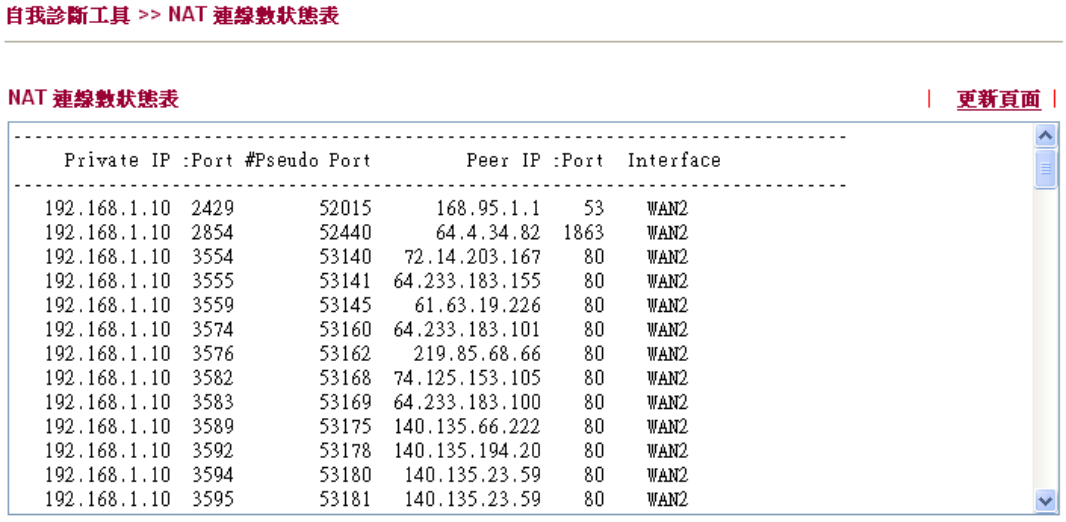
此工具提供指派 IP 位址的相關資訊，這項資訊對於診斷網路問題像是 IP 位址衝突等是很有幫助的。

按**自我診斷工具**，選擇 **DHCP 表**開啓相關網頁。

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。

4.14.5 NAT 連線數狀態表

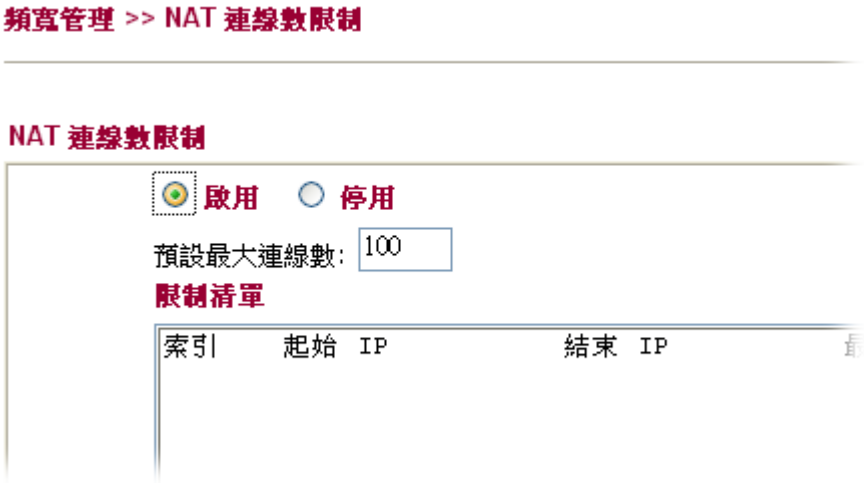
按**自我診斷工具**，選擇 **NAT 連線數狀態表**開啓相關網頁。



Private IP:Port	本機電腦的 IP 位址和埠號。
#Pseudo Port	路由器爲了執行 NAT 所使用的暫時通訊埠。
Peer IP:Port	遠端主機的目標 IP 位址與埠號。
Interface	顯示 WAN 連線的介面。
更新	按此鈕重新載入本頁。

4.14.6 資料流量監控

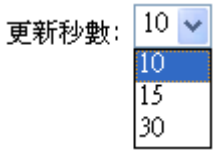
本頁顯示所監視的 IP 位址執行的過程，並在數秒的間隔後重新更新頁面，此處所列出的 IP 位址是在頻寬管理中設定完成的，在啓動資料流量監控之前，您必須啓動 IP 頻寬限制以及 IP 連線數限制。若沒有這麼做的話，系統會出現知會畫面提醒您先啓動相關設定。



按**自我診斷工具**，選擇**資料流量監控**開啓相關網頁。您可按下 IP 位元址、**TX 速率**、**RX 速率**或是**連線數**來排列資料。

啓用資料流量監控　　勾選此方塊以啓動此功能。

更新秒數　　使用下拉式選項選擇系統自動更新資料的間隔時間。



更新頁面　　按此連結更新本頁。

索引編號　　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

封鎖 – 可以避免指定電腦在 5 分鐘內存取網際網路。

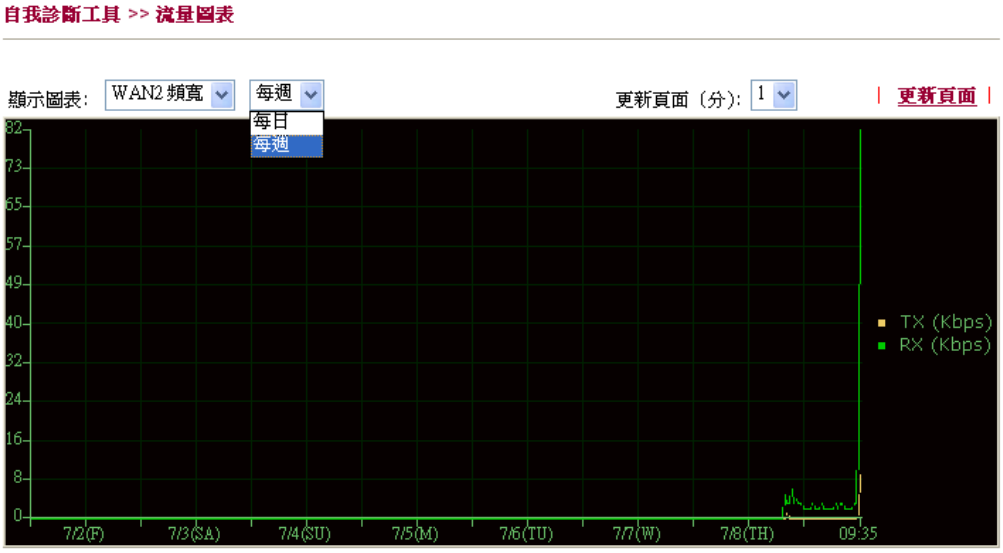
解除 – 指定 IP 位址的裝置將在五分鐘內封鎖起來，剩餘時間將顯示在 NAT 連線數欄位中。

現值/高峰值/速度

現值表示目前 WAN1/WAN2 的傳輸速率與接收速率。
高峰值表示路由器在資料傳輸上所檢測到的最高數值。
速度表示 **WAN>>基本設定**中所指定的線路速度，如果您未指定任何速率，這邊將顯示自動，以說明速率由系統自行指定。

4.14.7 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 頻寬**或是**連線數**來檢視流量圖表。您可隨時按**更新頁面**重新顯示圖表內容。

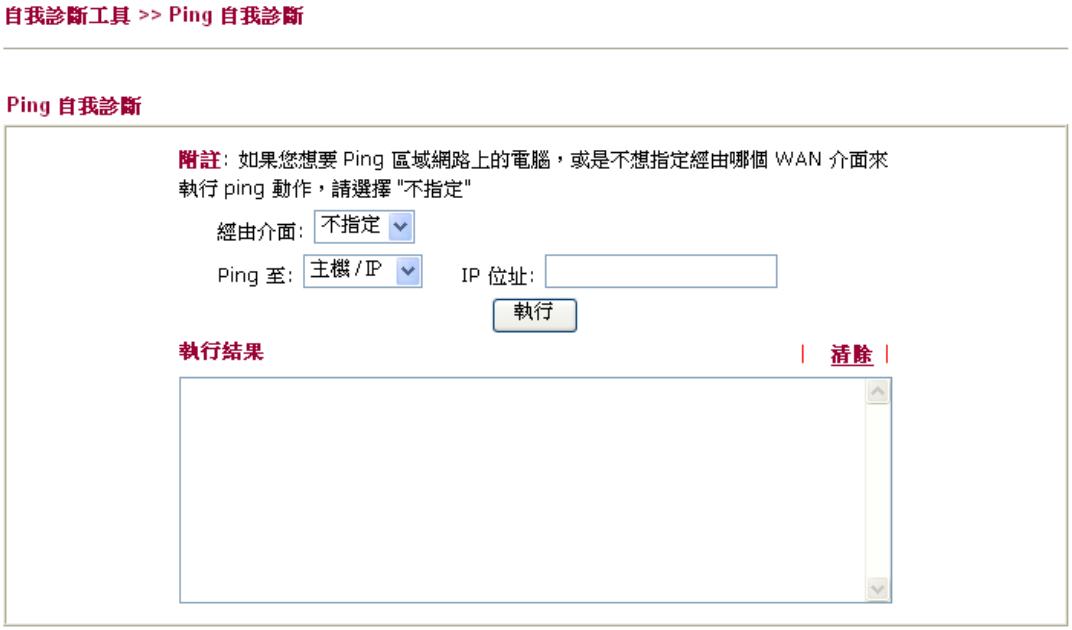


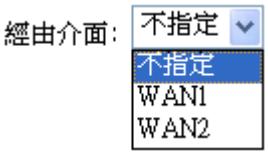
水準軸代表時間；而垂直軸代表的意義就很不同了。對 **WAN1 頻寬**而言，垂直軸代表的是過去所傳送與接收封包的數量。

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。

4.14.8 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。



經由介面	選擇介面以執行此動作。
Ping 至	使用下拉式清單選擇您想要 Ping 的目標。 
IP 位址	輸入您想要 Ping 的主機/IP 上的 IP 位址。
執行	按此鈕啓動 Ping 作業，結果將會顯示在螢幕上。
清除	按此連結清除視窗上的結果。

4.14.9 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。

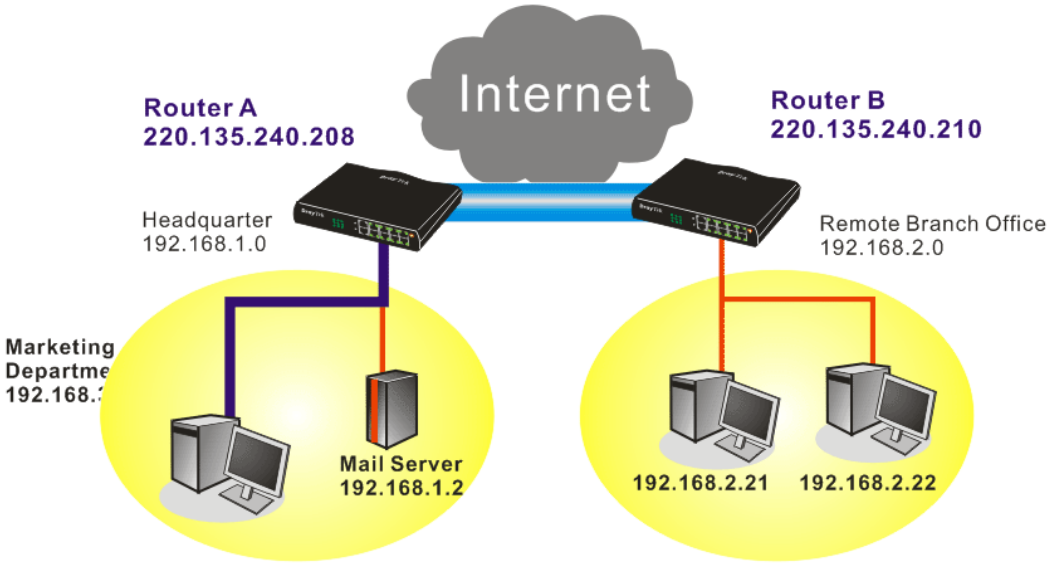
經由介面	使用下拉式清單選擇您想要經由其處來追蹤的 WAN 介面，或使用**不指定**讓路由器自動決定選擇哪一種介面。
主機/IP 位址	指明主機的 IP 位址。
執行	按此鈕開始路由追蹤動作。
清除	按此連結刪除視窗上的結果。

本頁空白

5 應用與範例

5.1 建立遠端辦公室與總公司之間的 LAN-to-LAN 連線

最常見的範例是例如遠端分公司與總公司之間的安全連線，依照下圖所顯示的網路結構，您可以遵循提供的步驟來建立 LAN-to-LAN 設定檔案，這二個區域網路不可具有相同的網路位址。



在總部辦公室內路由器 A 的設定:

1. 開啓 **VPN 與遠端存取設定**群中並選擇**遠端存取控制**，啓用必須的 VPN 服務並按下**確定**。
2. 接著，使用 PPP 爲主的服務，像是 PPTP、L2TP 等，您必須在 **PPP 基本設定**調整設定值。

針對使用 IPSec 爲主的服務，像是 IPSec 或是以 IPSec 原則爲主的 L2TP，您必須在 **VPN IKE/ IPSec 基本設定**調整設定值，諸如雙方皆須知曉的預先共用金鑰。

3. 至 **LAN-to-LAN 設定檔案**，選擇索引號碼以便編輯檔案。
4. 將一般設定如下調整，您應該啓動 VPN 連線，因爲任何一方都可啓動 VPN 連線。

5. **撥出設定**按下圖所示調整，以便使用選定的**撥出設定**方式主動撥號連接路由器 B。如果選擇的服務項目是 ***IPSec***，您可以爲此撥號連線進一步指定遠端相對的 IP 位址、IKE 認證方式和 IPSec 安全防護方式。

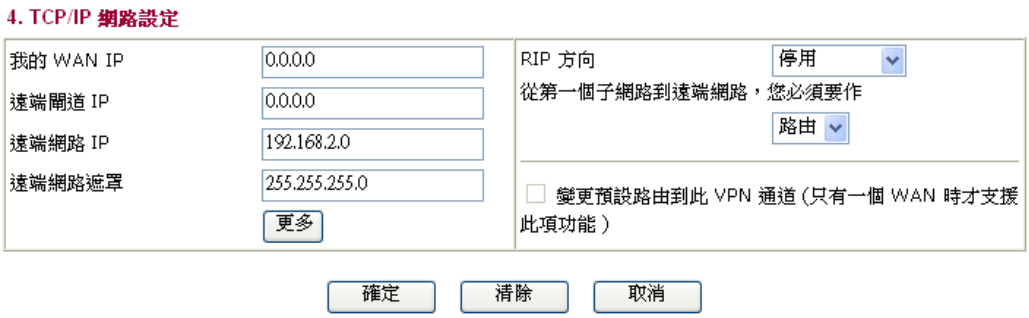
如果選擇的服務項目是 ***PPTP***，您可以爲此撥號連線進一步指定相對 IP 位址、使用者名稱、密碼和 VJ 壓縮等。

6. 將**撥入設定**按下圖所示調整以便路由器 B 建立 VPN 連線。

如果選擇的服務項目是 ***IPSec***，您可以爲此撥號連線進一步指定遠端相對的 IP 位元址、認證方式和 IPSec 安全防護方式，否則系統將自動爲您採用上述 **IPSec 一般設定**頁面所定義的設定。

如果選擇的服務項目是 ***PPTP***，您可以爲此撥號連線進一步指定相對 IP 位址、使用者名稱、密碼和 VJ 壓縮等。

7. 最後在 **TCP/IP 網路設定**欄位中設定遠端網路 IP/子網路，如此一來，路由器 A 可以透過 VPN 連線直接將封包導引至路由器 B 之遠端網路上。



在遠端辦公室內路由器 B 的設定:

1. 開啓 **VPN 與遠端存取設定**群中並選擇**遠端存取控制**，啓用必須的 VPN 服務並按下**確定**。
2. 接著，使用 PPP 爲主的服務，像是 PPTP、L2TP 等，您必須在 **PPP 一般設定** 調整設定值。

針對使用 IPSec 爲主的服務，像是 IPSec 或是以 IPSec 政策爲主的 L2TP，您必須在 **VPN IKE/ IPSec 基本設定**調整設定值，諸如雙方皆須知曉的預先共用金鑰。

3. 至 **LAN-to-LAN 設定檔案**，選擇索引號碼以便編輯檔案。

4. 將一般設定如下調整，您應該啓動 VPN 連線，因爲任何一方都可啓動 VPN 連線。

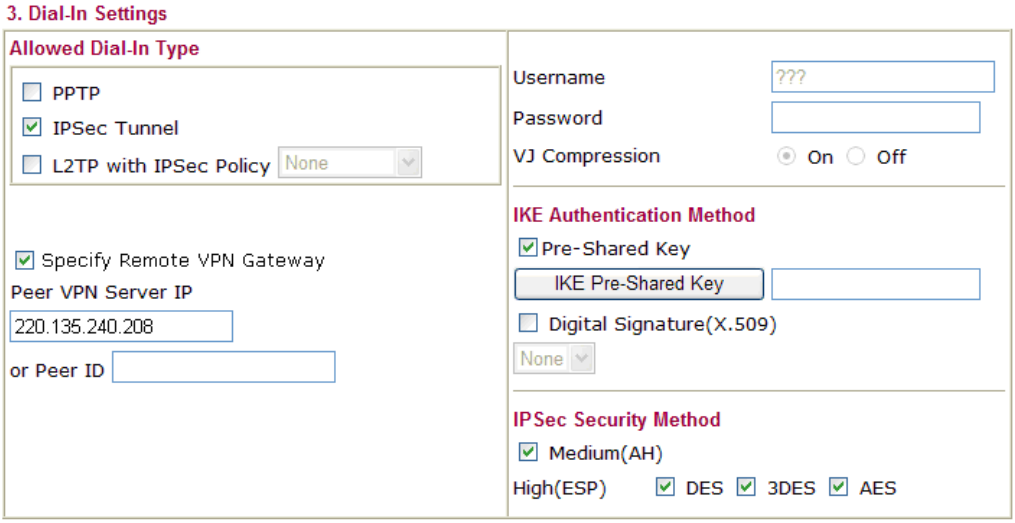
5. **撥出設定**按下圖所示調整，以便使用選定的**撥出設定**方式主動撥號連接路由器 B。

如果選擇的服務項目是 ***IPSec***，您可以爲此撥號連線進一步指定遠端相對的 IP 位址、IKE 認證方式和 IPSec 安全防護方式。

如果選擇的服務項目是 ***PPTP***，您可以爲此撥號連線進一步指定對方 IP 位址、使用者名稱、密碼和 VJ 壓縮等。

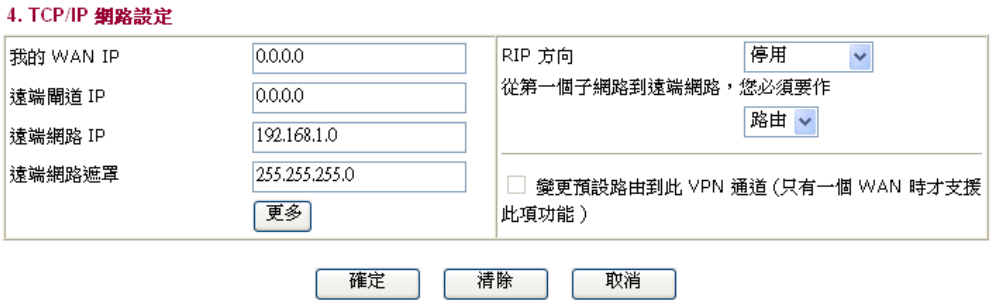
6. 將**撥入設定**按下圖所示調整以便路由器A建立 VPN 連線。

如果選擇的服務項目是 ***IPSec***，您可以爲此撥號連線進一步指定遠端相對的 IP 位元址、認證方式和 IPSec 安全防護方式，否則系統將自動爲您採用上述 **IPSec 基本設定**頁面所定義的設定。



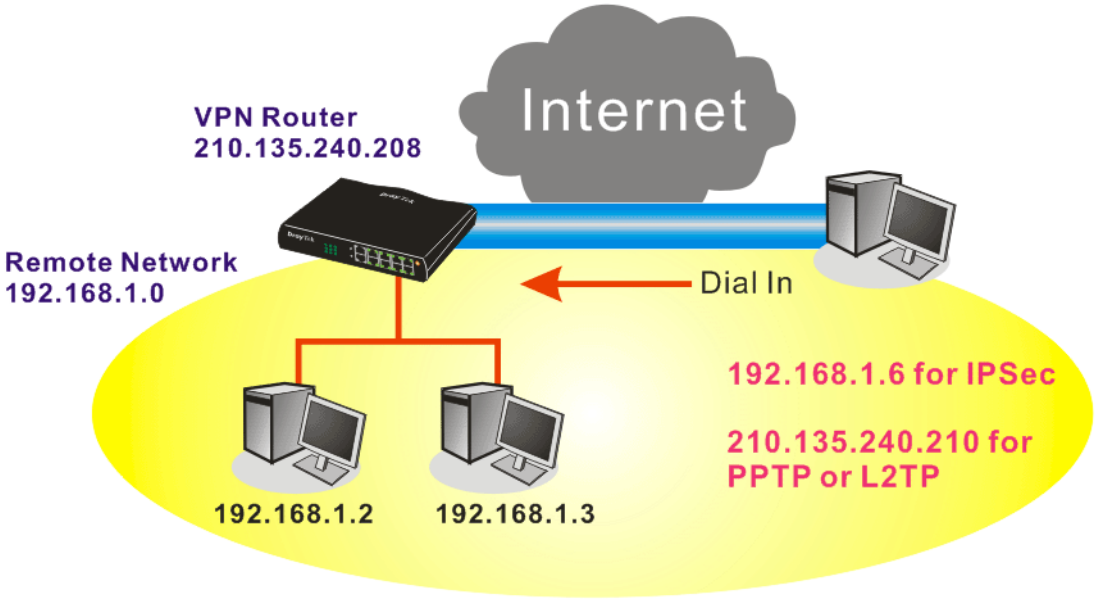
如果選擇的服務項目是 ***PPTP***，您可以爲此撥號連線進一步指定相對 IP 位址、使用者名稱、密碼和 VJ 壓縮等。

7. 最後在 **TCP/IP Network Settings** 設定遠端網路 IP/子網路，如此一來，路由器 B 可以透過 VPN 連線直接將封包導引至路由器 A 之遠端網路上。



5.2 建立工作者和總部之間的 VPN 遠端撥號連線

另一個常用的範例是：作爲一個工作者，您可能想要安全地連接到企業網路，依照下面所顯示的網路結構，您可以遵照相關的步驟來建立遠端用戶設定檔，並且在遠端主機上安裝 Smart VPN Client。



在辦公室內VPN路由器的設定:

1. 開啓 **VPN 與遠端存取設定**群中並選擇**遠端存取控制**，啓用必須的 VPN 服務並按下**確定**。
2. 接著，使用 PPP 爲主的服務，像是 PPTP、L2TP 等，您必須在 **PPP 基本設定**調整設定值。

如果選擇的服務項目是 ***IPSec***，如 IPsec 或是 IPSec 原則之 L2TP，您必須設定 **IKE/IPSec 基本設定**像是雙方都應知曉的預設共用金鑰。

3. 至**遠端撥入使用者**，按任一索引編號以編輯設定檔。
4. 將**撥入設定**按下圖所示調整，以便遠端使用者建立 VPN 連線。

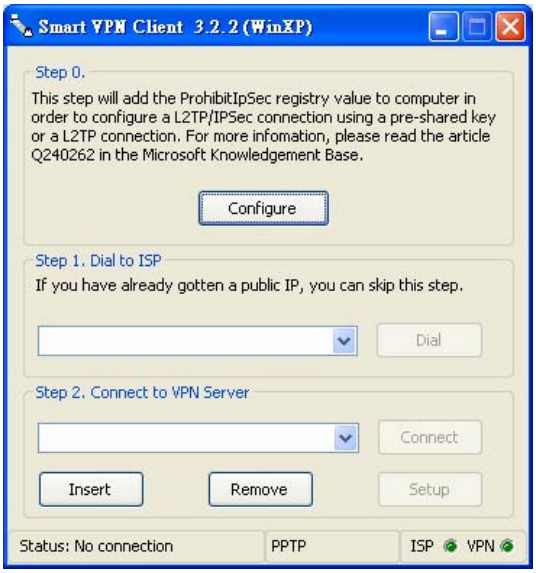
如果選擇的服務項目是 ***IPSec***，您可以爲此撥號連線進一步指定遠端相對的 IP 位址、IKE 認證方式和 IPSec 安全防護方式，否則系統將自動爲您採用上述 **IPSec 基本設定**頁面所定義的設定。

如果選擇的服務項目是 ***PPTP***，您應該爲此撥號連線進一步指定遠端相對的 IP 位址、使用者名稱、密碼以及 VJ 壓縮。

遠端主機上的設定:

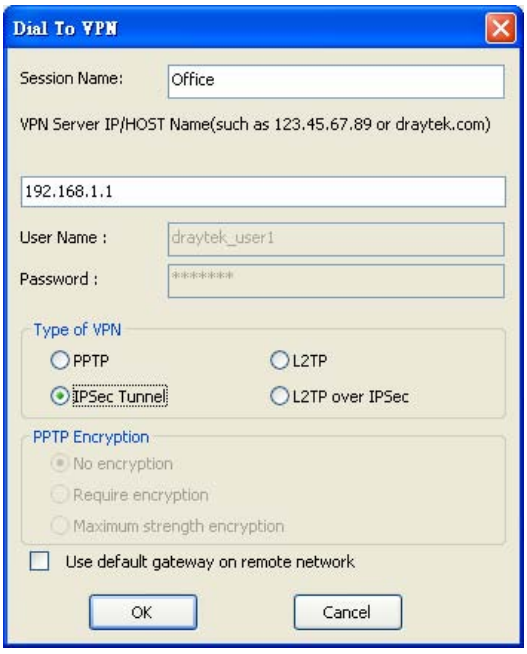
1. 對 Win98/ME 系統而言，您可以使用 Dial-up Networking 建立 PPTP 通道給予路由器；對 Win2000/XP 來說，請使用 Network and Dial-up connections 或是 Smart VPN Client 等軟體幫忙建立 PPTP、L2TP 和 L2TP over IPSec 通道，您可以在包裝的光碟片中找到此軟體或是進入 http://www.draytek.com/ 網站下載中心取得，依照螢幕指示來安裝即可。

2. 在安裝成功之後，對於第一次使用的用戶，必須先按 **Step 0** 中的 **Configure** 按鈕，重新啓動主機。

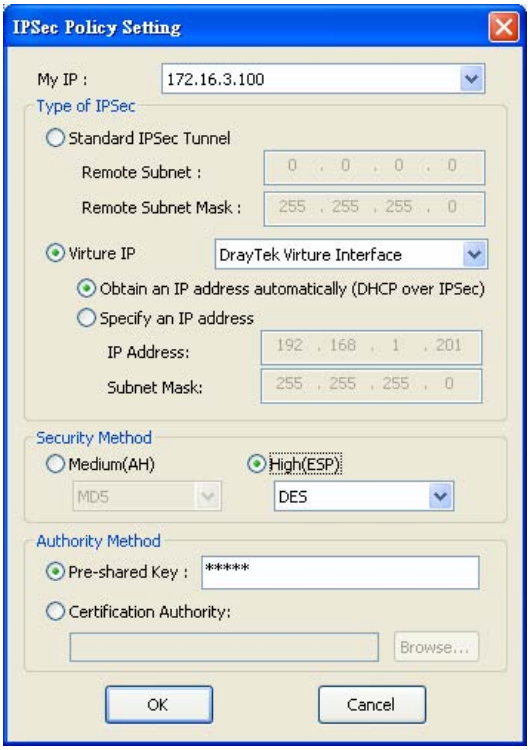


3. 在 **Step 2. Connect to VPN Server** 中，按下 **Insert** 按鈕新增一個新的入口。

如果選擇的服務項目是 ***IPSec Tunnel***，如下圖所示：

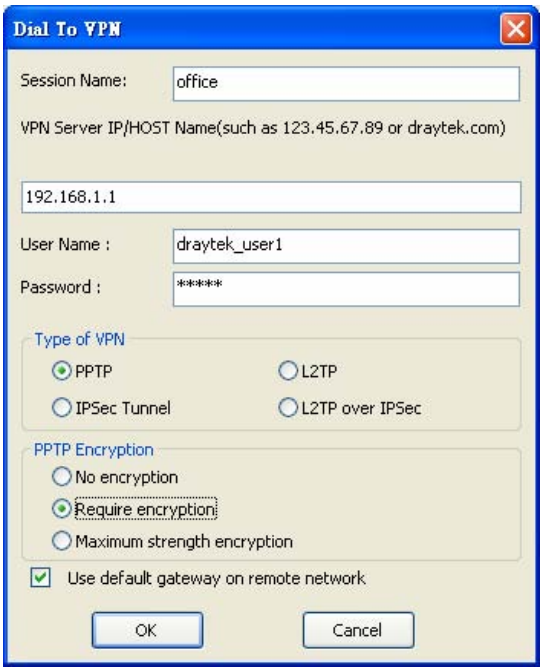


您可以進一步指定取得 IP、安全防護以及驗證的方法。若已選擇 Pre-Shared Key，那麼此設定必須與 VPN 路由器中的設定一致。



如果選擇的服務項目是 ***PPTP***，您可以進一步指定 VPN 伺服器 IP 位址、使用者名稱、密碼和加密方法，使用者名稱和密碼必須和您在 VPN 路由器中所設定的內容一致。如欲使用遠端網路上預設的閘道，表示所有遠端主機上的封包都將會導引至 VPN 伺服器，然後再轉送到網際網路上，這樣會讓遠端主機看起來像是在企業網路

上運作一般。

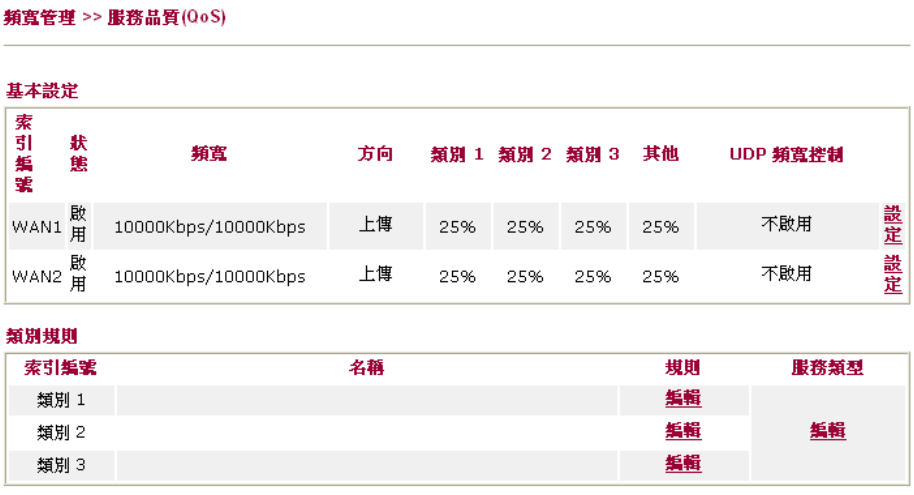


4. 按 **Connect** 按鈕建立連線，當連線成功之時，您可以在右下方角落發現到綠色閃燈。

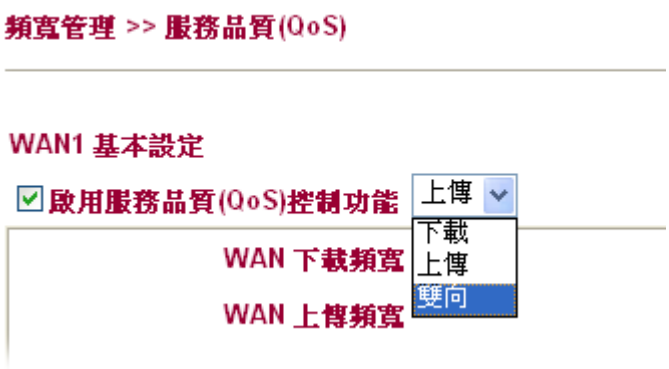
5.3 QoS 設定範例

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。



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



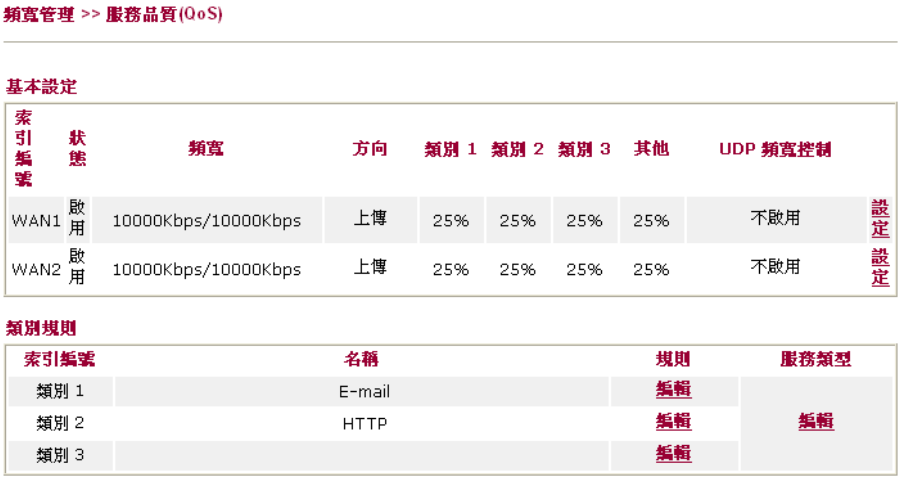
3. 設定下載/上傳頻寬。

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**。

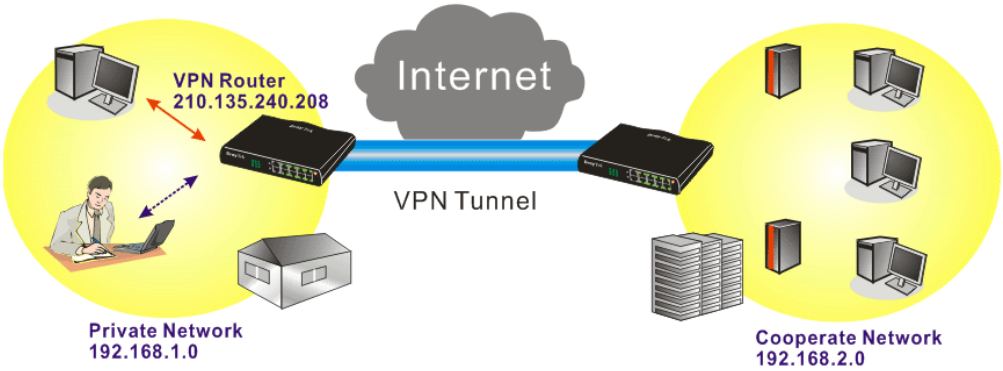
5. 使用者可設定保留頻寬(例如 25%) 給予透過POP3 和SMTP通訊協定來傳送的電子郵件。參考下圖。

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**。於此索引中我們可以設定保留頻寬(例如 25%)給予**HTTP**。



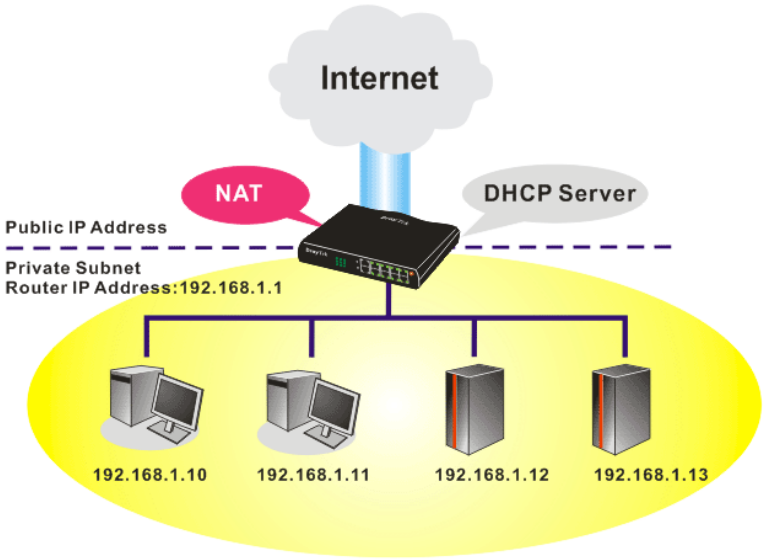
7. 選擇WAN1 的**設定**連結。勾選**啓用UDP頻寬控制**防止VoIP大量的UDP資料影響其他的應用程式。

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。



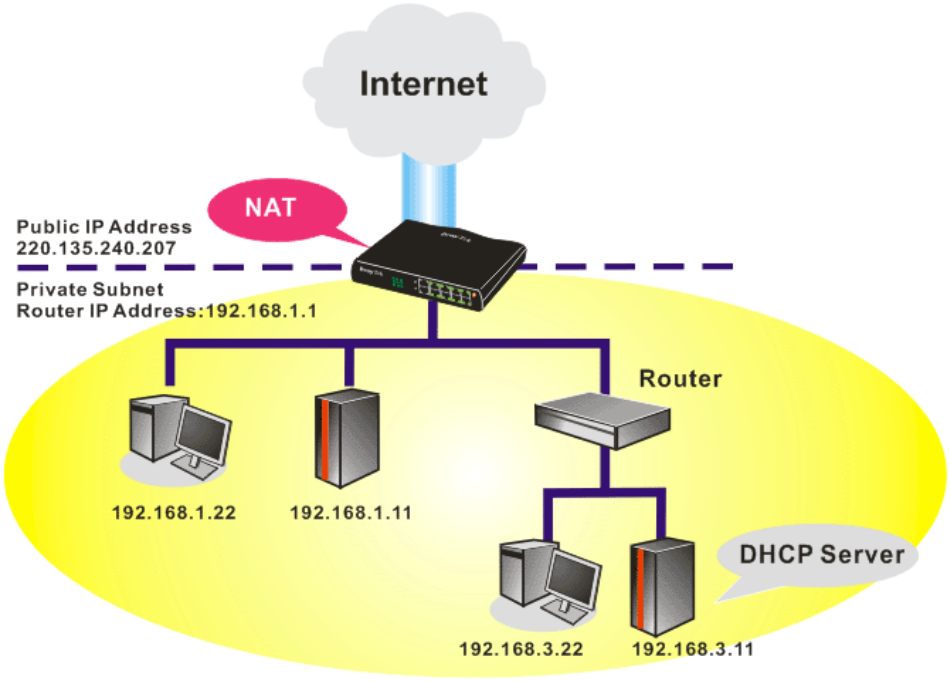
5.4 使用 NAT 來建立區域連線

預設設定和相關應用範例顯示如下，預設路由器之虛擬 IP 位址/子網路遮罩爲 192.168.1.1/255.255.255.0，內建之 DHCP 伺服器已經啓用，因此指定每個已 NAT 的主機一個 192.168.1.x 的 IP 位址，範圍從 192.168.1.10 開始。



只有紅色框內的設定需要調整，以符合 NAT 用途的需求。

如要使用網路中的 DHCP 伺服器而非路由器內建的伺服器，您必須變更設定，如下所示：

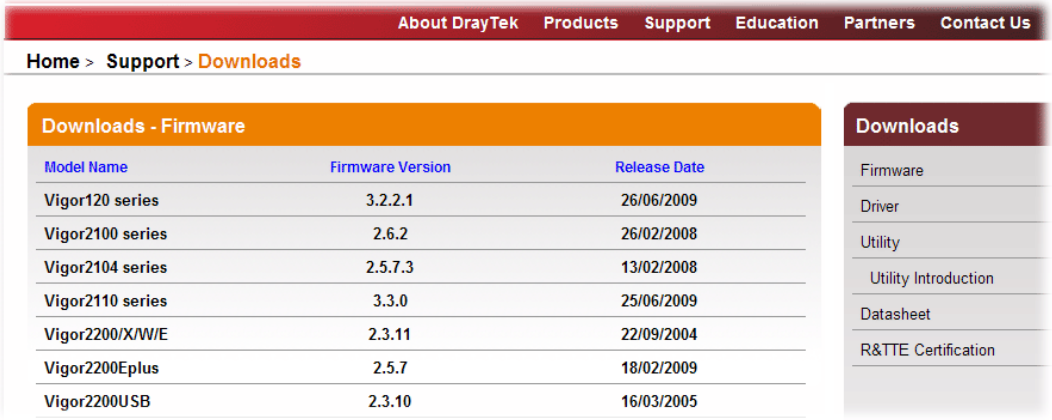


只有紅色框內的設定需要調整，以符合 NAT 用途的需求。

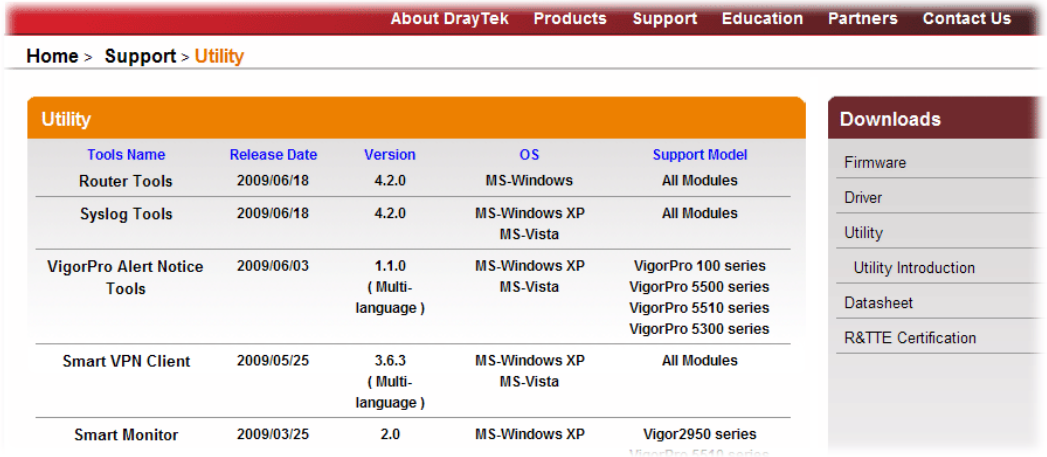
5.5 更新路由器韌體

更新韌體之前，您必須先安裝路由器工具，**Firmware Upgrade Utility** 即包含在 CD 中。

1. 進入 **www.DrayTek.com.**
2. 進入**支援服務** >> **檔案下載**，找到路由器機型名稱之後，選取其相關的韌體連結，並下載最新的韌體。

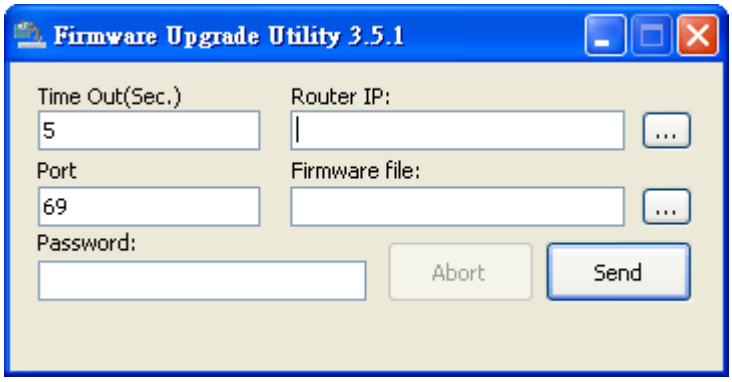


3. 進入**支援服務** >> **檔案下載**， 找到 **Utility** 功能後按下該功能。

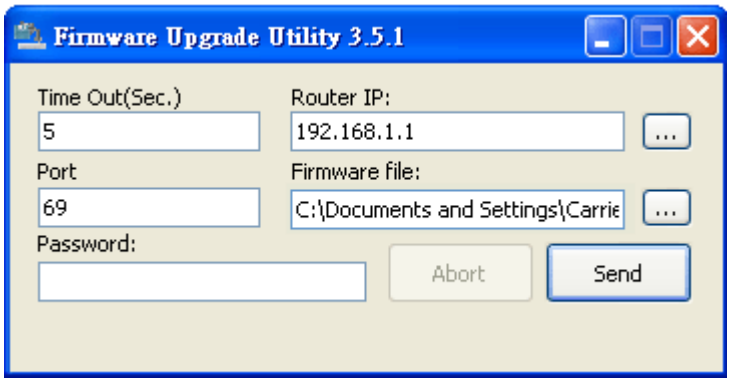


4. 選擇 **Router Tools** 以下載此工具，下載完畢後，請解壓縮檔案放於您的電腦中。
5. 在路由器工具圖示上按二下，安裝精靈將出現如下：

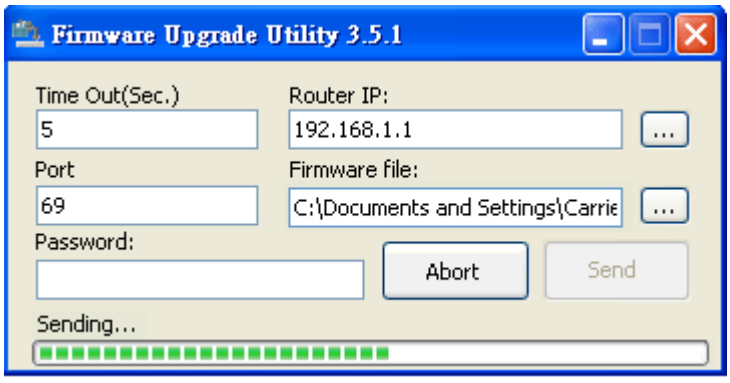
6. 依照螢幕指示安裝此工具，按下 **Finish** 以結束安裝。
7. 自**開始(Start)**選單中，指向**程式集(Programs)**，然後選擇 **Router Tools XXX >> Firmware Upgrade Utility**。



8. 輸入路由器 IP 位址，通常爲 **192.168.1.1**。
9. 按韌體檔案(Firmware file)輸入欄右邊的按鈕，尋找您自公司網站下載之韌體檔案，您會看見二個副檔名不同的檔案：**xxxx.all** (可保持用戶原先的設定)以及 **xxxx.rst** (將用戶設定重新回復預設值)，請按照實際需要選擇任何一個。

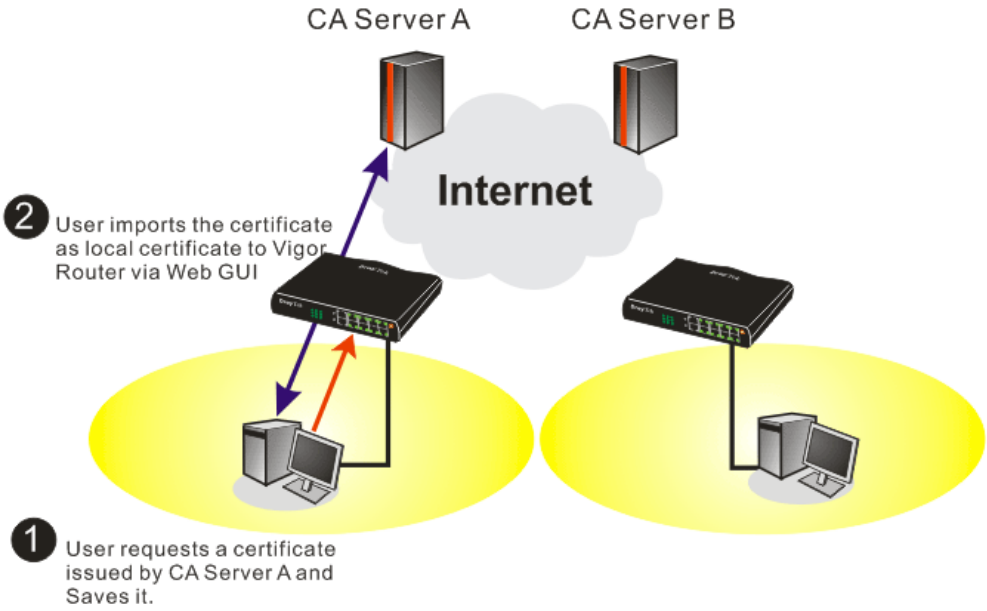


10. 按下 **Send**。



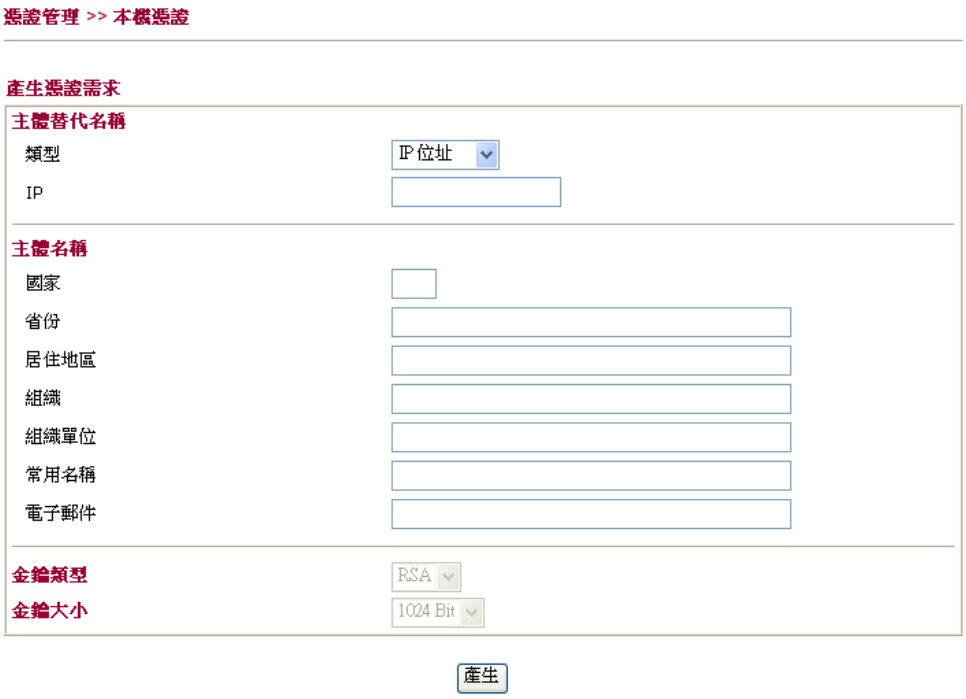
11. 現在韌體更新已完成。

5.6 在 Windows CA 伺服器上提出憑證需求



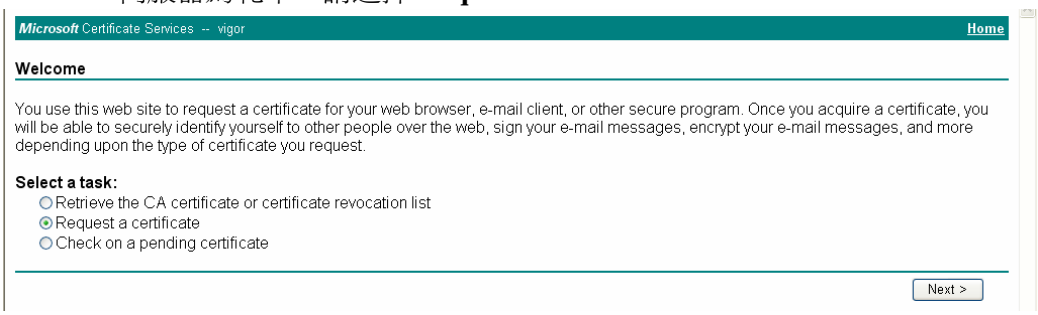
1. 選擇**憑證管理>>本機憑證**。

2. 按**產生**按鈕開始編輯憑證需求，請輸入必要的資訊。

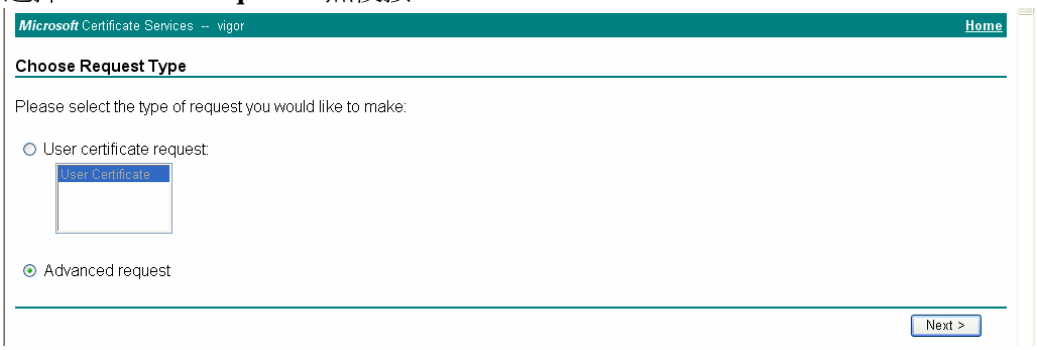


3. 複製並儲存 X509 本機憑證需求，稍後將會應用到此文字檔。

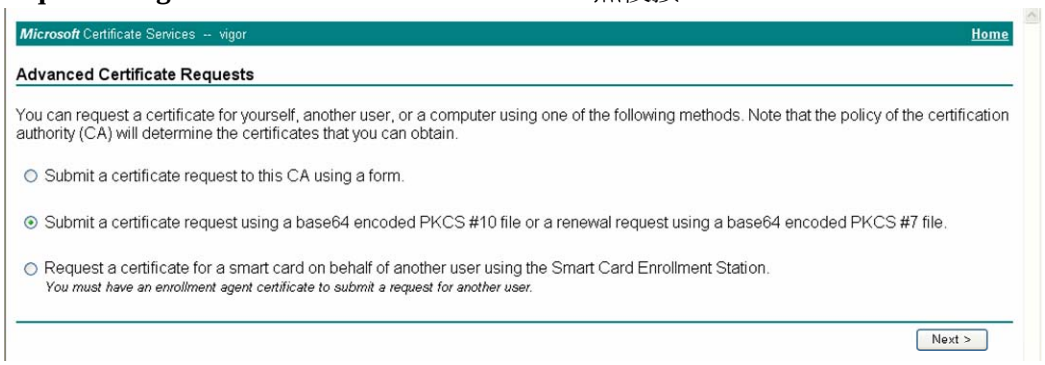
4. 透過網頁瀏覽器連接 CA 伺服器，依照螢幕指示完成需求設定。下圖我們以 Windows 2000 CA 伺服器爲範本，請選擇 **Request a Certificate**。



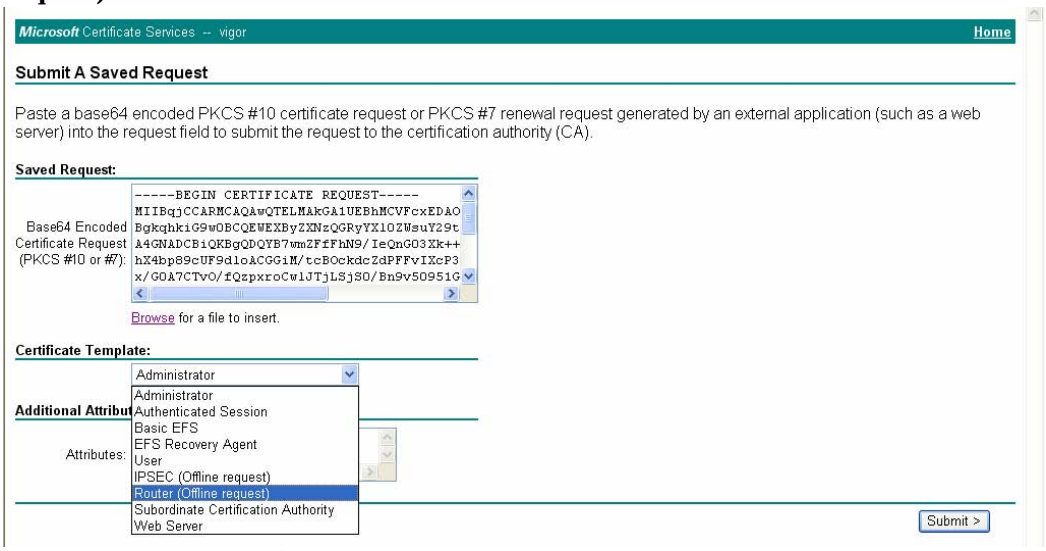
選擇 **Advanced request**，然後按 **Next**。



挑選 **Submit a certificate request a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file**，然後按 **Next**。



匯入 X509 本機憑證文字檔，選擇 **Router (Offline request)** 或 **PSec (Offline request)** 。

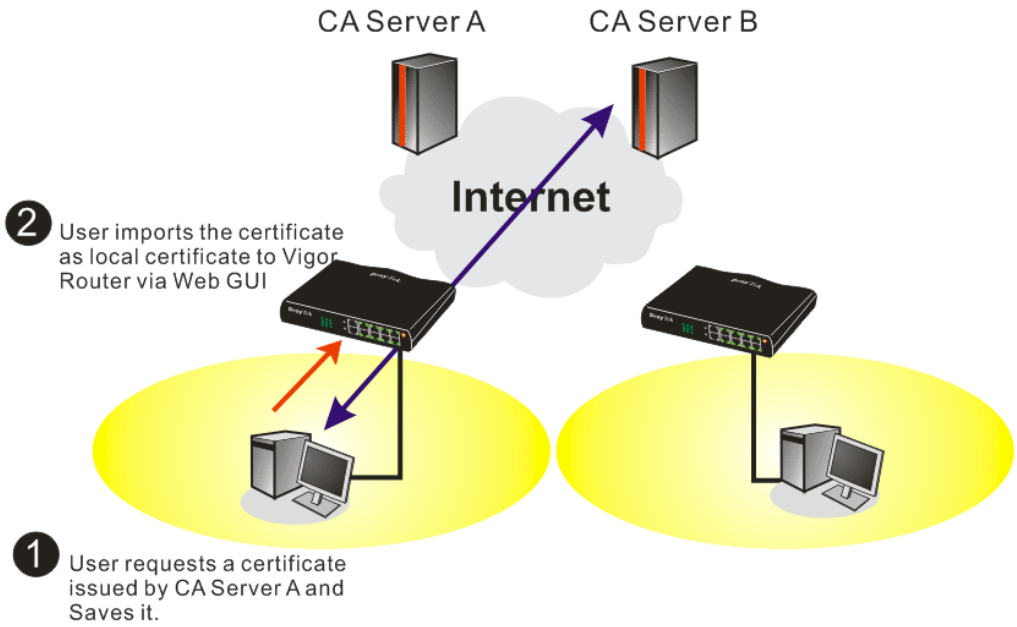


需求提出後，伺服器會給您一個憑證，請選擇 **ase 64 encoded** 憑證及下載該憑證，現在您應該會從伺服器取得一個憑證，請儲存該憑證。

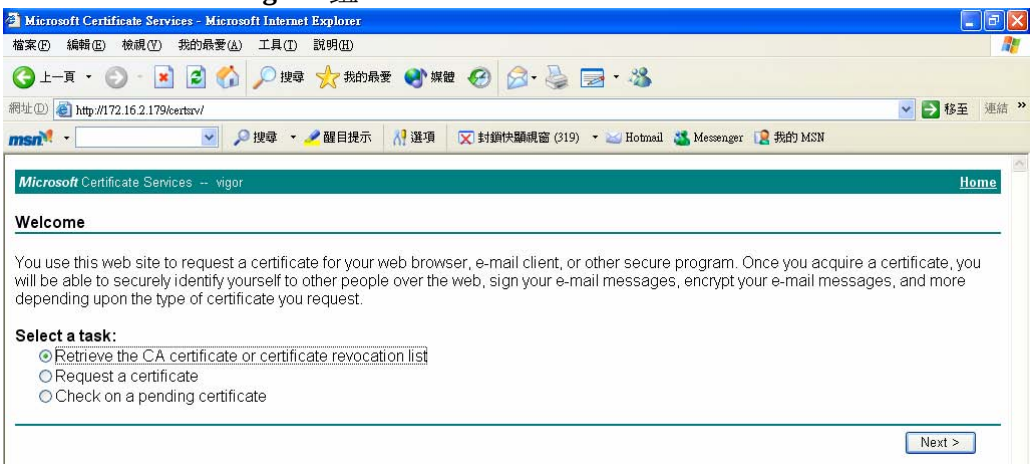
5. 回到路由器畫面，進入**本機憑證**，按下**匯入**按鈕並瀏覽檔案以匯入憑證至路由器中。當您完成這個動作時，請按頁面更新，您就可以看見如下的視窗。

6. 您也可以重新檢視憑證的細節資訊，請按**檢視**按鈕。

5.7 提出 CA 憑證要求並將之設定爲 Windows CA 伺服器上具公信力之憑證



1. 使用瀏覽器連接至 CA 伺服器以取得您想要的憑證。按下 **Retrive the CA certificate or certificate recoring list** 鈕。



2. 在 **Choose file to download** 區中，按 CA Certificate **Current** 以及 **Base 64 encoded**，然後按 **Download CA certificate** 儲存該檔爲 cer. 檔案。

3. 回到路由器網頁設定畫面，進入**具公信力之 CA 憑證**，按**匯入**按鈕並瀏覽檔案以匯入憑證。當您完成這個動作之後，請按更新頁面察看最新的憑證使用狀況。

4. 您也可以重新檢視憑證的細節資訊，請按**檢視**按鈕。

注意:在設定憑證之前，請先至**系統維護>>日期與時間**頁面中重新設定路由器的時間。

6 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。

6.1 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。

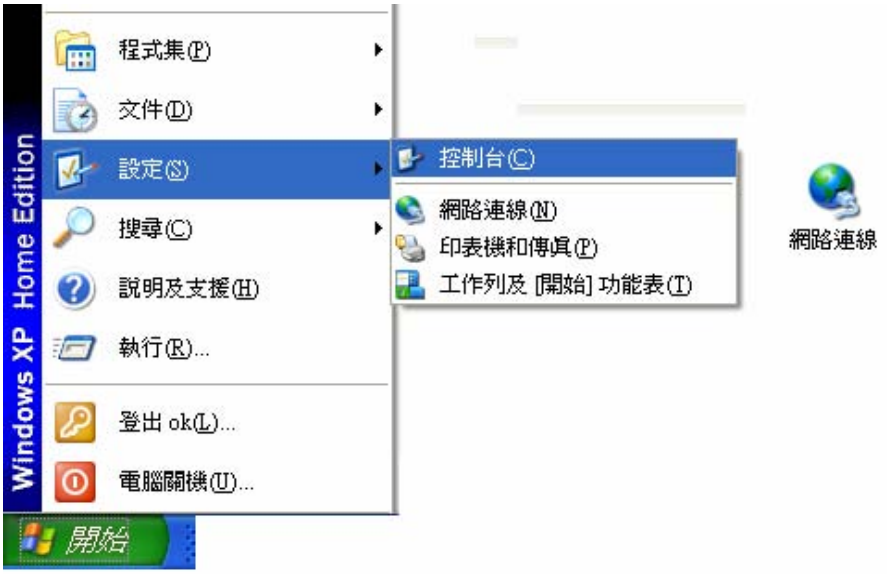
6.2 檢查您電腦的網路連接設置是否正確

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

對於 Windows 系統

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

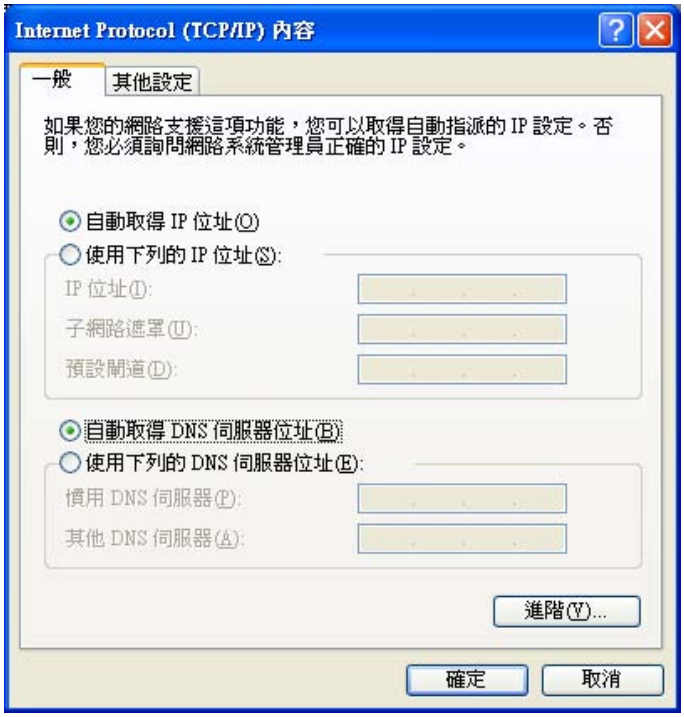
1. 至**控制臺**內，選擇**網路連線**並按滑鼠左鍵二下，進入網路連線畫面。



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

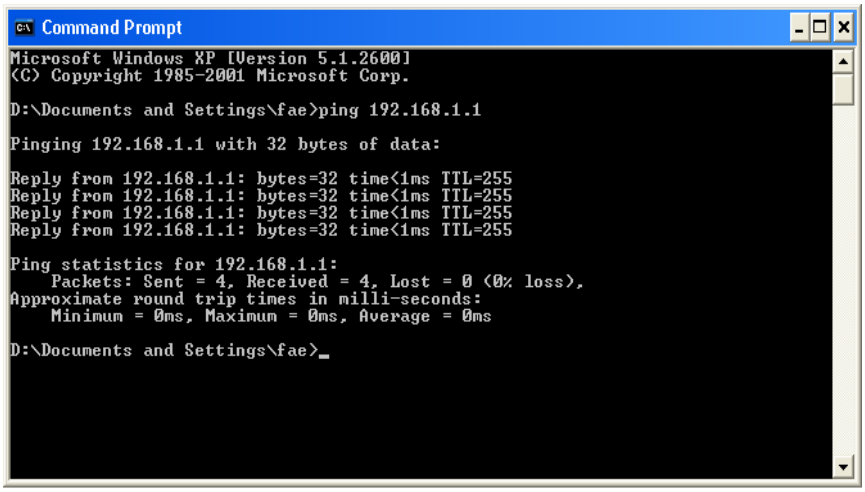
1. 在桌面上選擇目前所使用的 MacOS 磁碟機按滑鼠二下。
2. 選擇**應用**檔案夾中的**網路**檔案夾。
3. 進入**網路**畫面，在**設定**選項中，選擇**使用 DHCP**。

6.3 從電腦上 Ping 路由器

路由器的預設閘道爲 192.168.1.1. 因爲某些理由，你可能需要使用 " ping " 指令檢查路由器的連結狀態。比較重要的是電腦是否收到來自 192.168.1.1 的回應，如果沒有，請檢查個人電腦上的 IP 位址。我們建議您將網際網路連線設定爲自動取得 IP 位址。(請參照 6.2 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

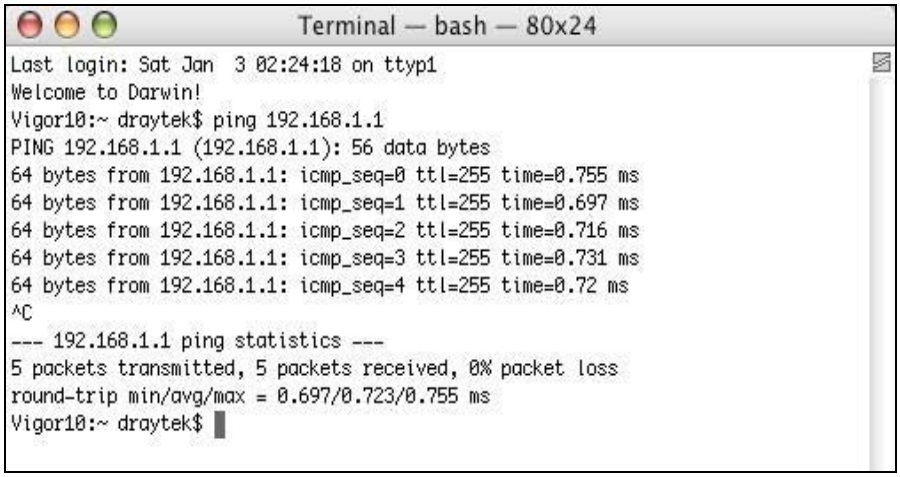
1. 開啓**命令提示字元視窗** (功能表選單**開始**>>**執行**) 。
2. 輸入 **command** (適用於 Windows 95/98/ME)或 **cmd** (適用於 Windows NT/ 2000/XP/Vista)。DOS 命令提示字元視窗將會出現。



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。



6.4 檢查 ISP 的設置是否正常

開啓 **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。

對於 PPPoE 用戶

1. 檢查 PPPoE 是否已**啓用**。
2. 檢查您是否正確地輸入了 **ISP** 提供給您的**使用者名稱**和**密碼**。

對於固定 IP/DHCP 用戶

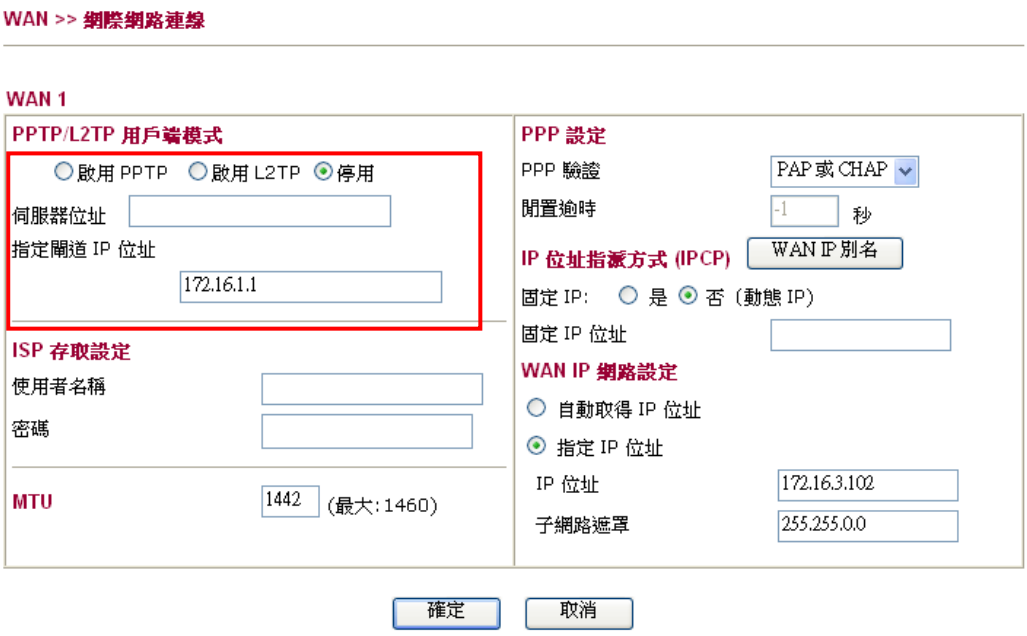
1. 檢查**固定或動態 IP** 是否已**啓用**。

2. 檢查 **WAN IP 網路設定**是否無誤。

3. 若您選擇了**指定 IP 位址**，請檢查 **IP 位址**、**子網路遮罩**和**閘道 IP 地址**是否正確（一定要與您的 ISP 確認相關設置）。

對於 PPTP/L2TP 用戶

1. 檢查 **PPTP/L2TP** 連結是否已**啓用**。



2. 檢查您是否正確地輸入了 **ISP** 提供給您的 **PPTP 伺服器**、**使用者名稱**和**密碼**。

3. 檢查 **WAN IP 網路設定**是否無誤。 若您選擇了**指定 IP 位址**，請檢查 **IP 位址**、**子網路遮罩**和**閘道 IP 地址**是否正確（一定要與您的 ISP 確認相關設置）。

6.5 網路連線相關問題

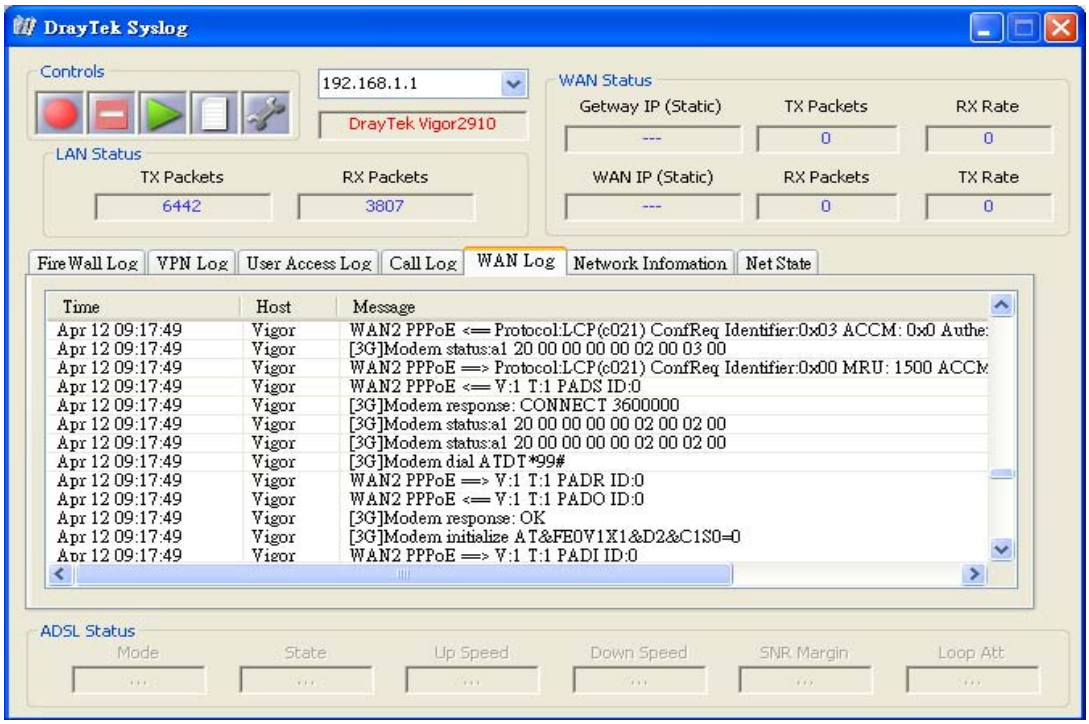
當您使用 3G 網路傳輸發現問題時，請先檢查下列各項：

檢查 USB LED 燈號

在插入 3G USB Modem 至 Vigor2920 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，請重新啓動路由器。

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，麻煩開啓 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 Vigor2910 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 模式連接往際網路。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。

6.6 還原路由器原廠預設組態

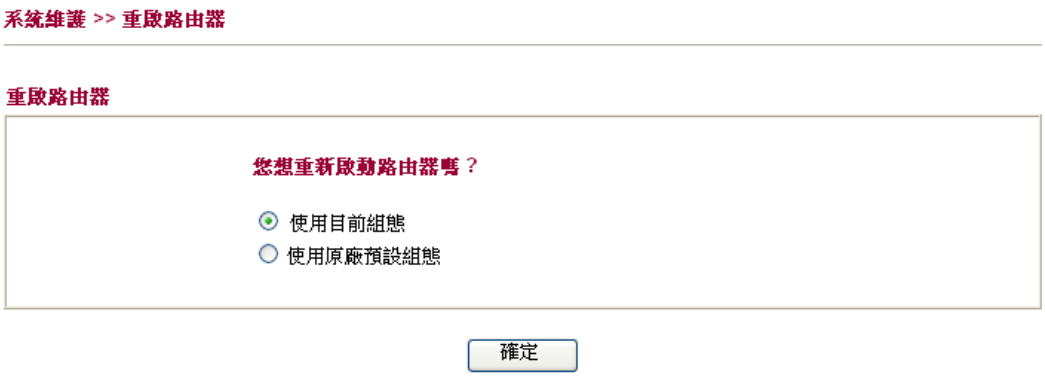
有時，錯誤的連線設定可以藉由還原廠預設組態來重新設定，您可以利用**重啓路由器**或硬體重新設定的方法還原路由器的設定值。此供能僅在**管理者模式**下可以運作。

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。請確實記錄之前分享器所有的設定，預設出廠的密碼爲空白。

軟體重新設定

您可以在路由器的網頁介面上，直接將它回復至出廠預設設置，但須在**管理者模式**下進行。

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**確定**。幾秒鐘後，路由器就會恢復至出廠預設設定。



硬體重新設定

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

恢復至出廠預設值後，您就可以按個人需要，重新設定路由器。

6.7 聯絡您的代理商

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。