DrayTek

Vigor2120 系列

寬頻防護路由器

Your reliable networking solutions partner

使 用 手 冊

V1.2

Vigor2120 系列
寬頻防護路由器
使用手冊

版本: 1.2

韌體版本: V3.7.8

(請造訪居易網站，隨時獲取更新資訊)

日期: 2016 年 5 月 5 日

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, Vista, 7 以及其 Explorer 均屬微軟公司商標
- Apple 以及 Mac OS 均屬蘋果電腦公司的註冊商標
- 其他產品則爲各自生產廠商之註冊商標

安全說明和保障

安全說明

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

保固

自使用者購買日起二年內爲保固期限(保固: 原廠一年，需線上註冊加給一年,合計二年)，請將您的購買收據保存二年，因爲它可以證明您的購買日期。當本產品發生故障乃導因於製作及(或)零件上的錯誤，只要使用者在保固期間內出示購買證明，居易科技將採取可使產品恢復正常之修理或更換有瑕疵的產品(或零件)，且不收取任何費用。居易科技可自行決定使用全新的或是同等價值且功能相當的再製產品。

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

成爲一個註冊用戶

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

韌體及工具的更新

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

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: Vigor2120 系列路由器

DrayTek 公司聲明 Vigor2120 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干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。

法規資訊

聯邦通信委員會干擾聲明

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

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

此產品符合 FCC 規定的第 15 部分。其運作將有以下兩個情況：

(1) 此產品不會造成有害的干擾，並且

(2) 此產品可能會遭受其他接收到的干擾，包括那些可能造成不良運作的干擾。

無線天線與人體間的距離至少要達 20 公分以上。

請造訪 http://www.draytek.com/user/SupportDLRTTECE.php#

本產品針對 2.4 /5 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 簡介

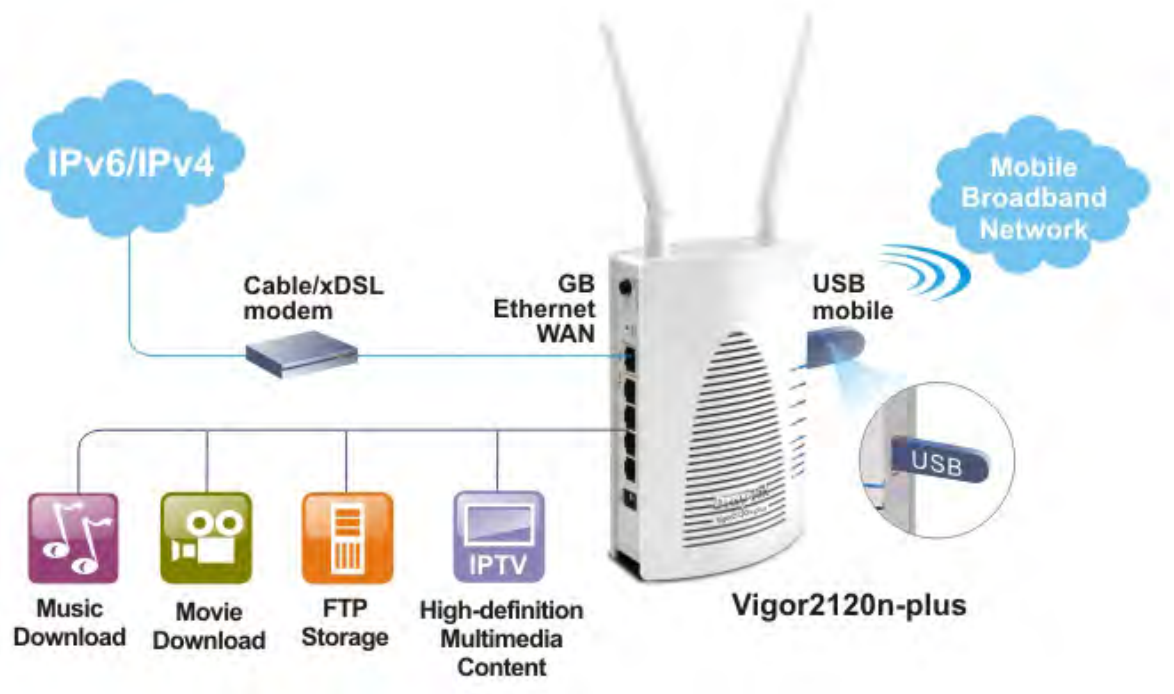
Vigor2120 系列爲寬頻路由器，整合 IP 層級的 QoS、NAT 連線數/頻寬管理等功能，讓使用者能以較大的頻寬進行工作調配的需要。

藉由採用硬體 VPN 平臺及 AES/DES/3DS 硬體加密方式，Vigor2120 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。

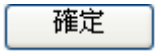
物件式防火牆相當具有彈性，可讓您的網路更加的安全，此外，Vigor2120 系列支援 USB 介面，可供連接 USB 印表機分享列印或是 USB 儲存裝置分享檔案。

Vigor2120 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。

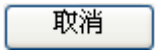


1.1 網頁設定按鈕說明

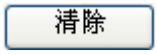
在路由器的網頁設定中，有數種常見的按鈕，其定義如下所示：



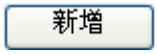
儲存並套用目前的設定。



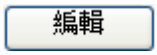
取消目前設定並回復先前的設定值。



捨棄目前設定值並允許使用者重新輸入。



指定項目新增設定。



編輯選定項目的設定。

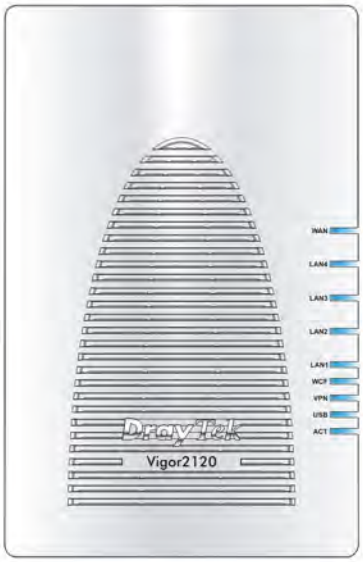
刪除選定項目及相關設定。

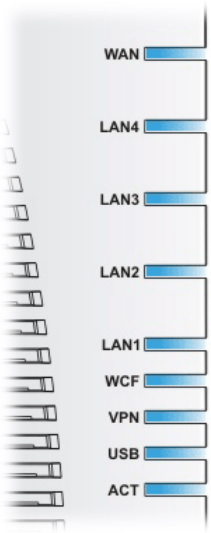
附註:有關網頁上所出現的其他按鈕，請參考第三章。

1.2 LED 指示燈與介面說明

不同機種路由器之 LED 顯示面板以及背板連接介面有些許的差異，詳列如下：

1.2.1 Vigor2120

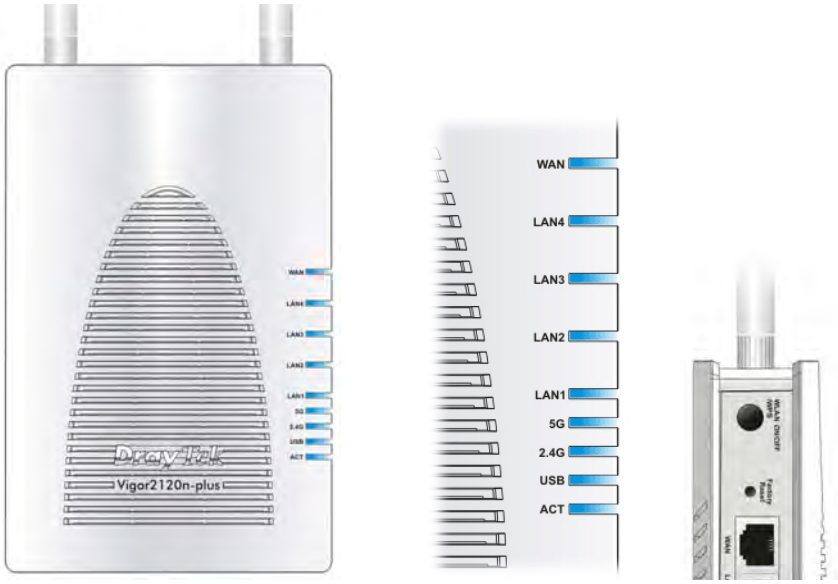




LED	狀態	說明
ACT	閃爍	路由器已開機並可正常運作。
	熄燈	路由器已關機。
USB	亮燈	USB 裝置已連接並運作中。
	閃爍	正在傳輸資料中。
VPN	亮燈	VPN 通道已建立。
WCF	亮燈	網頁內容過濾器已啓動(此功能是在**防火牆>>基本設定**中所驅動)。
LAN1 ~ LAN4	亮燈	乙太網路已連接。
	熄燈	乙太網路未連接。
WAN1 ~ WAN2	亮燈	WAN 介面已連接。
	熄燈	WAN 介面未連接。
	閃爍	資料封包傳輸中。

介面	說明
	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。
WAN	連接到 ADSL 或是 Cable Modem 裝置。
LAN 1- 4	連接到電腦或網路設備。
	PWR: 連接電源變壓器。
	連接到 USB 3G Modem 或是印表機。
	ON/OFF: 電源開關。

1.2.1 Vigor2120n-plus



LED	狀態	說明
ACT	閃爍	路由器已開機並可正常運作。
	熄燈	路由器已關機。
USB	亮燈	USB 裝置已連接並運作中。
	閃爍	正在傳輸資料中。
2.4G /5G	亮燈	無線網路功能已啓用並可正常運作。
	熄燈	無線網路功能關閉。
	閃爍	正在傳輸資料中。
LAN1 ~ LAN4	亮燈	乙太網路已連接。
	熄燈	乙太網路未連接。
WAN1 ~ WAN2	亮燈	WAN 介面已連接。
	熄燈	WAN 介面未連接。
	閃爍	資料封包傳輸中。

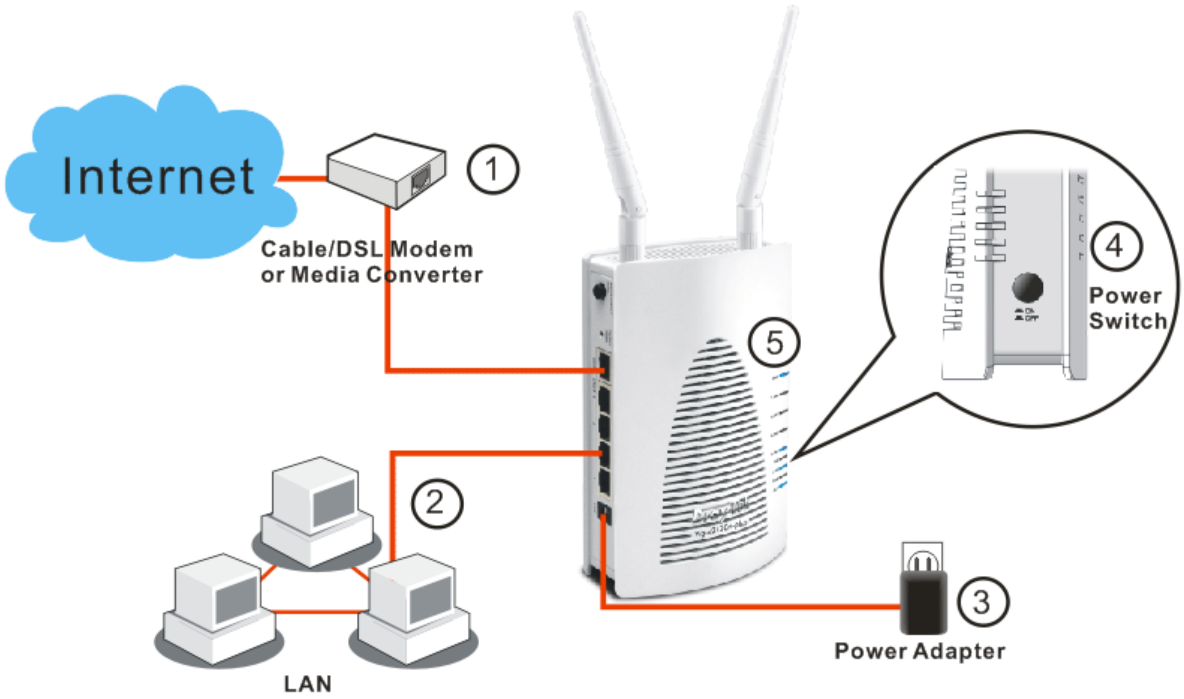
介面	說明
WLAN ON/OFF WPS	WLAN On- 按下此鈕並在二秒鐘內放開，可開啓無線功能。 無線功能開啓時，前面板將亮起 2.4G/5G 藍色 LED 燈號。 WLAN Off - 按下此鈕並在二秒鐘內放開，可關閉無線功能。無線功能關閉時，前面板的 2.4G/5G LED 燈號將熄滅。 WPS - 當 WPS 功能已經透過網頁設定介面啓動，可按壓此鈕超過二秒，路由器將等待無線用戶端進行遠端連線。
Factory Reset	還原成出廠預設值。 用法：當路由器正在運作時（ACT LED 燈號閃爍），利用尖銳的物品（例如：原子筆）壓住 Factory Reset 超過 5 秒；當 ACT 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。
WAN	連接到 ADSL 或是 Cable Modem 裝置。
LAN 1- 4	連接到電腦或網路設備。
PWR	PWR: 連接電源變壓器。
USB	連接到 USB 3G Modem 或是印表機。
ON OFF	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。

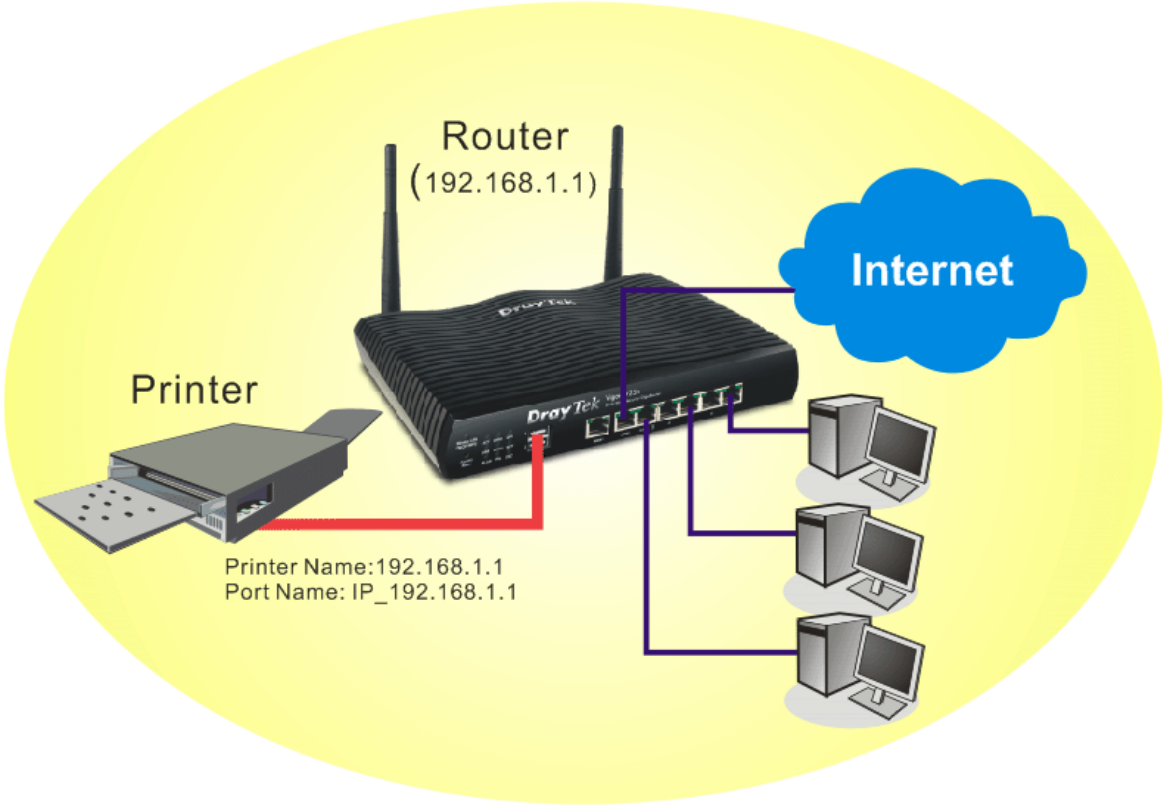
1. 利用乙太網路纜線(RJ-45)將數據機 / 路由器連接到本裝置的 WAN 連接埠。
2. 利用乙太網路纜線(RJ-45)一端連接 PC 的乙太網路連接埠，一端連接到路由器任何一個 **LAN** 連接埠。
3. 將電源線一端連接到路由器，另一端連接到牆上電源輸出孔。
4. 按路由器的電源開關。
5. 系統開始初始化，系統測試完畢後，**ACT** 燈號將會亮起，並持續閃爍。

(有關燈號的詳細說明，請參考 1.2 一節)



1.4 印表機安裝

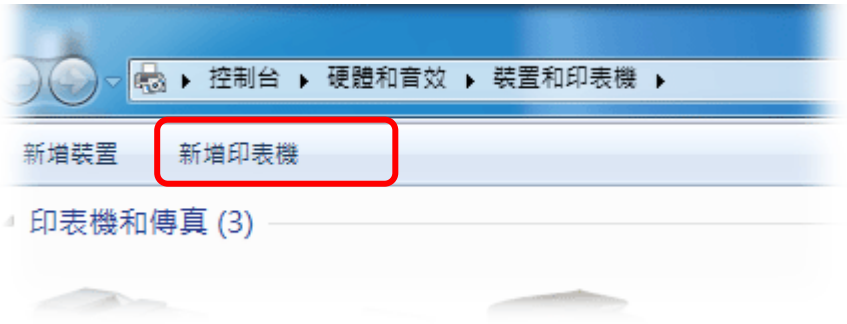
您可以在路由器上連接印表機來分享列印功能，這樣路由器的區域網路上所有的電腦都可透過它列印文件，以下設定範例是以 Windows 7 爲主，如果您使用的是其他 Windows 系統，請造訪居易網站 www.draytek.com 取得您所需要的安裝資訊。



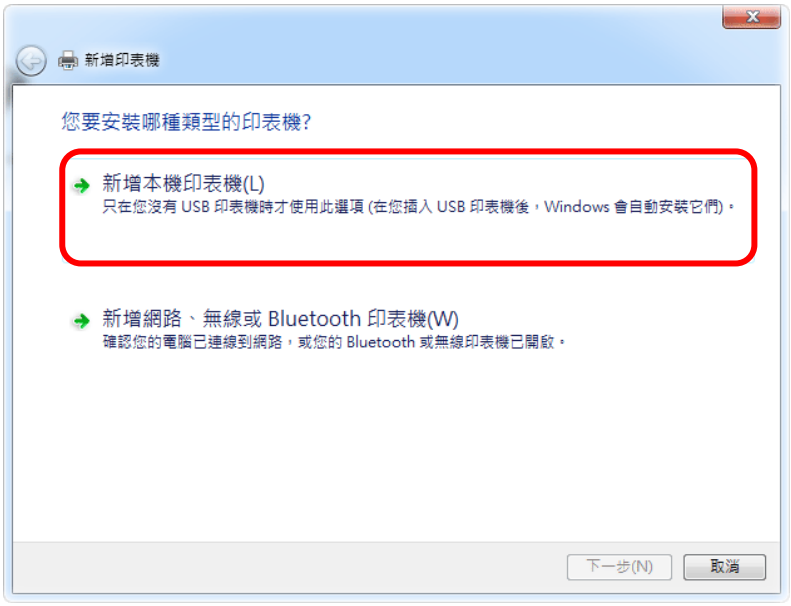
使用之前，請務必按照下列步驟來設定您的電腦（或無線用戶）：

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

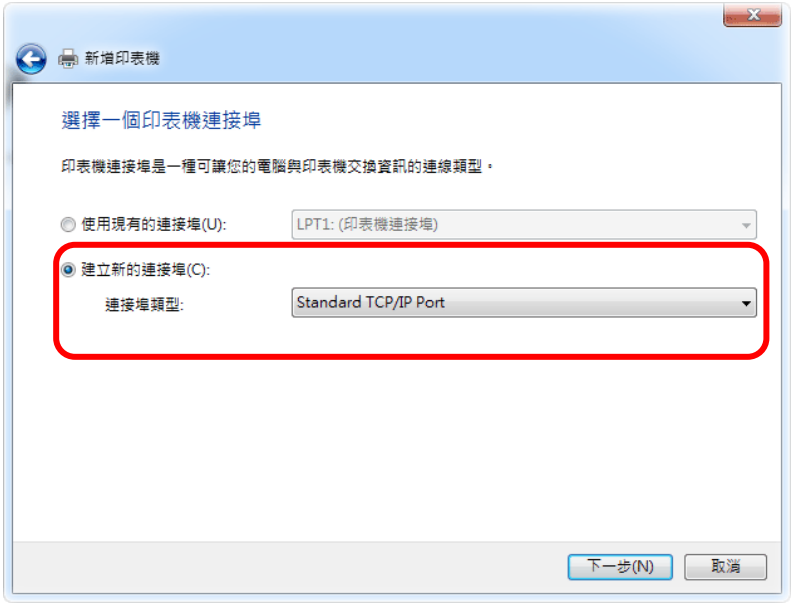
3. 按下新增印表機。



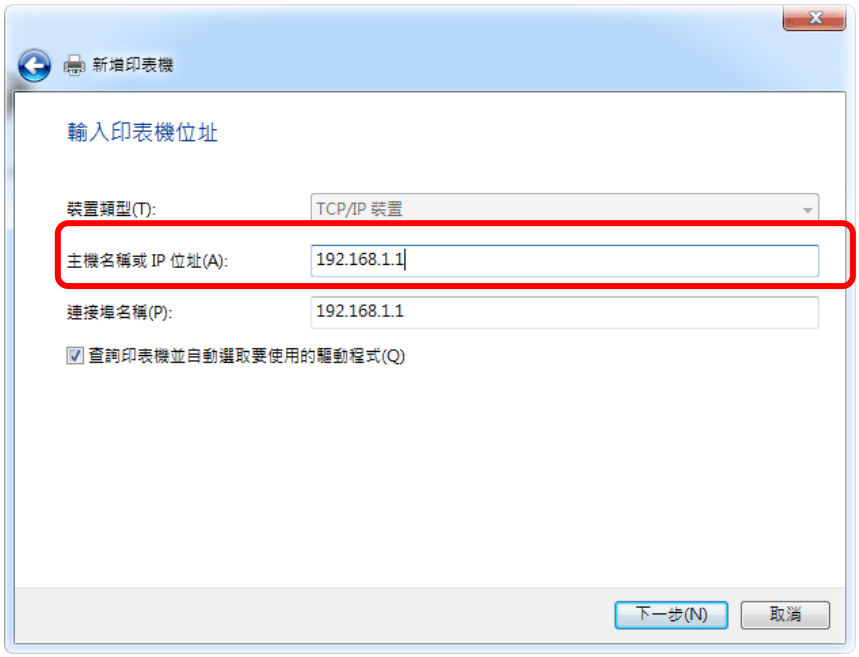
4. 選擇 “**新增本機印表機.**” 並按下**一步**。



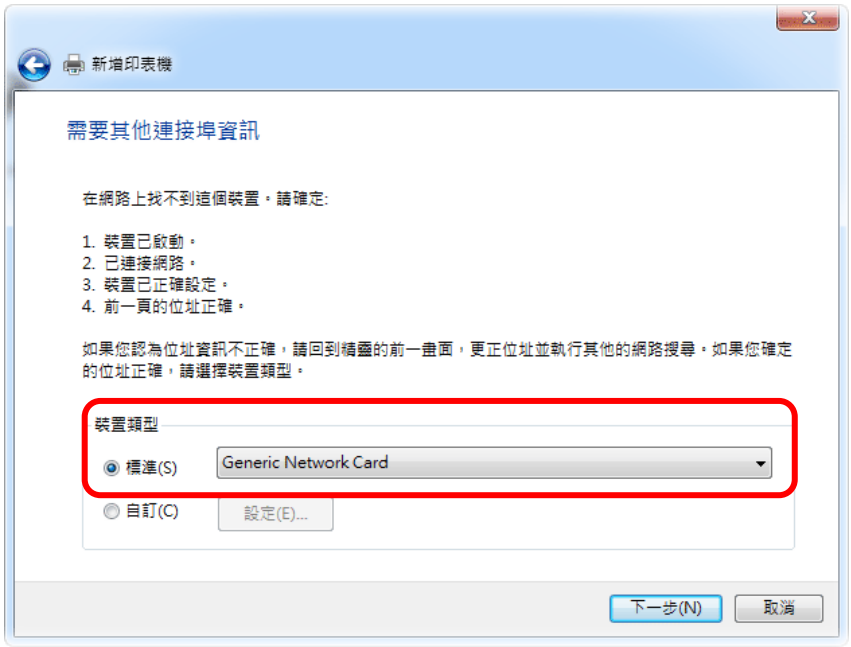
5. 接著請選擇 “**建立新的連接埠**”，用下拉式選項選擇“**Standard TCP/IP Port**”，按下**一步**。



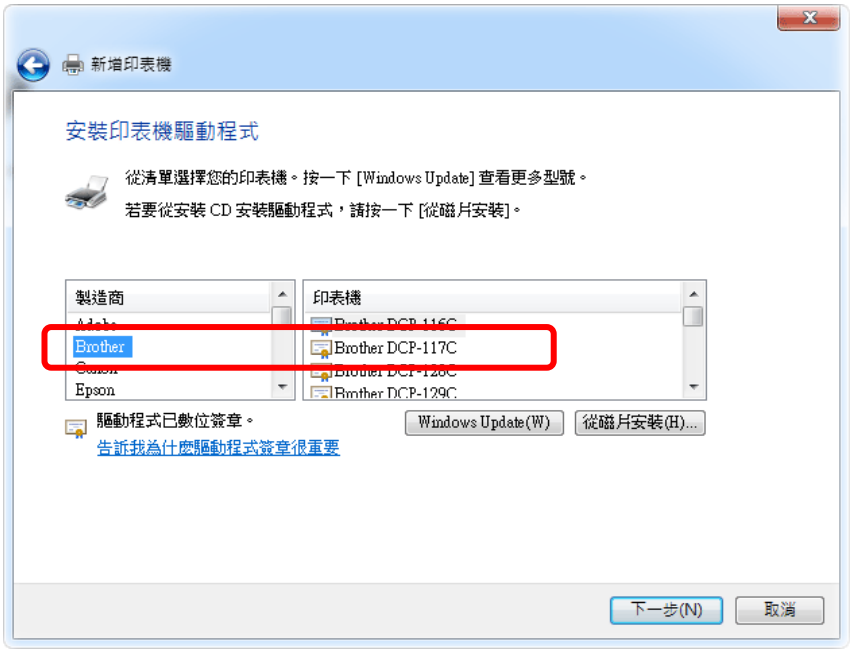
6. 在下面的對話方塊中，請在主機名稱或 IP 位址欄位輸入 **192.168.1.1** (路由器的 LAN IP)，再按**下一步**。



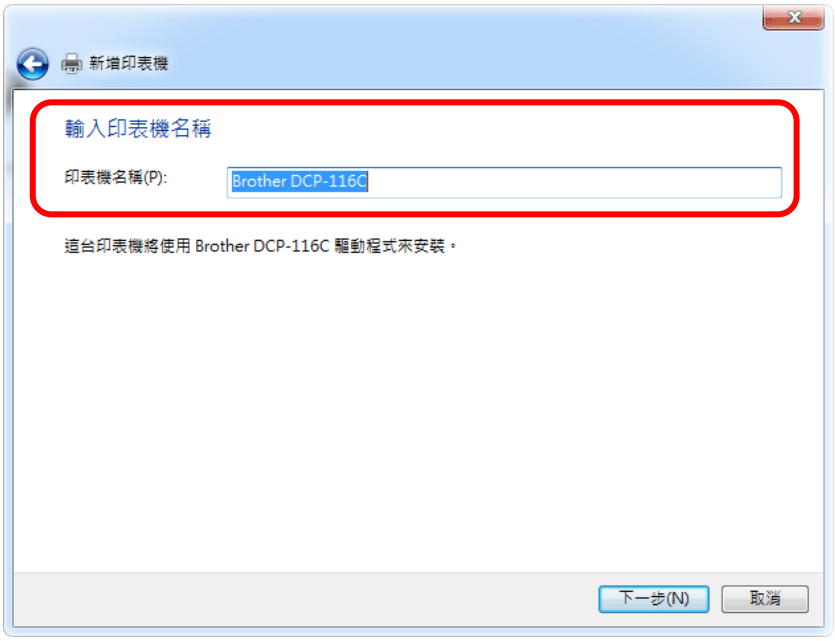
7. 請選擇**標準**，並自下拉式選項中選取 **Generic Network Card**，再按**下一步**。



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



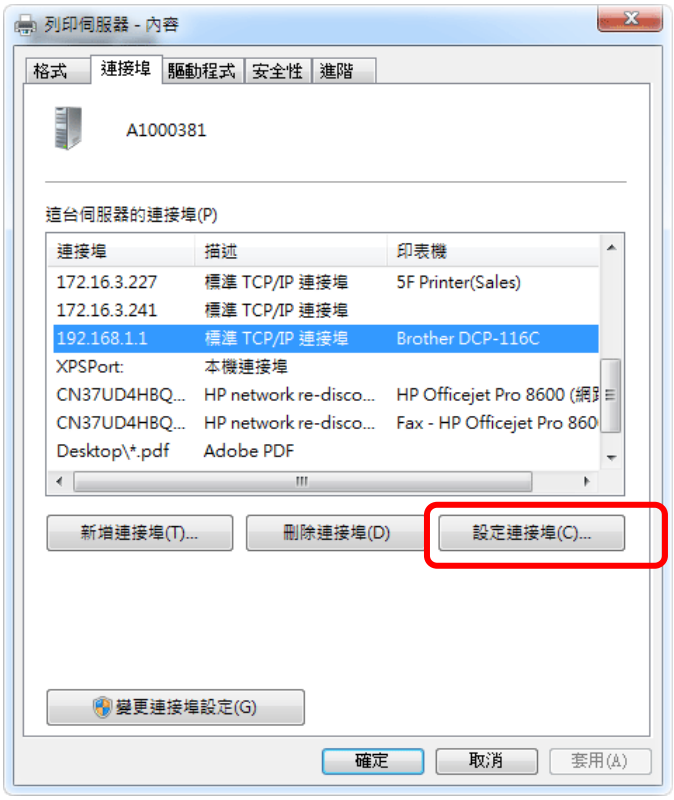
9. 輸入印表機名稱，繼續按**下一步**。



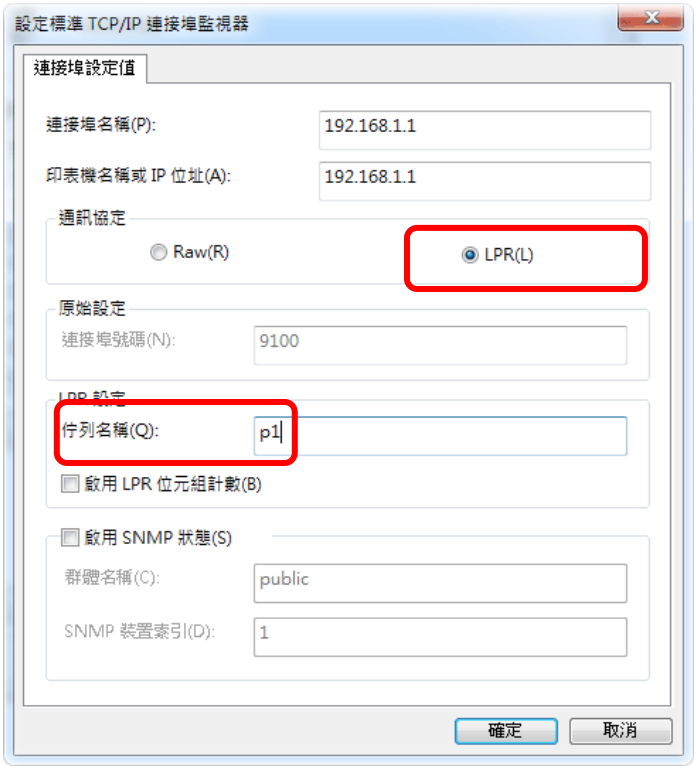
10. 在如下的對話盒，請按**完成**。

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

12. 如下頁面出現後，請按**設定連接埠**，編輯新增印表機的內容。



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



您現在可以使用新增的印表機了，大多數的印表機都與 Vigor 路由器相容。

注意 1: 此路由器仍不支援市面上某些印表機，如果您不知道自己所購買的印表機有無在支援之列，請造訪 www.draytek.com，上面可輕易取得您想知道的訊息，開

啓**技術支援>>技術問答**，按下 **USB 設定**連結，接著再按下 **Vigor router 相容印表機列表?** 連結，即可獲得您要的內容。

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

1.5 進入設定網頁

1. 確保您的電腦已經和路由器正確的連接。

> **附註:** 您可以選擇直接設定電腦的網路設定爲動態取得 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。

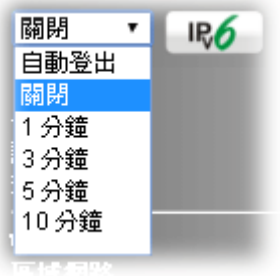
3. 請輸入“admin/admin”，再按下**登入**進入路由器網頁設定畫面。

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

4. 現在，設定介面的主選單會出現。

> **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。

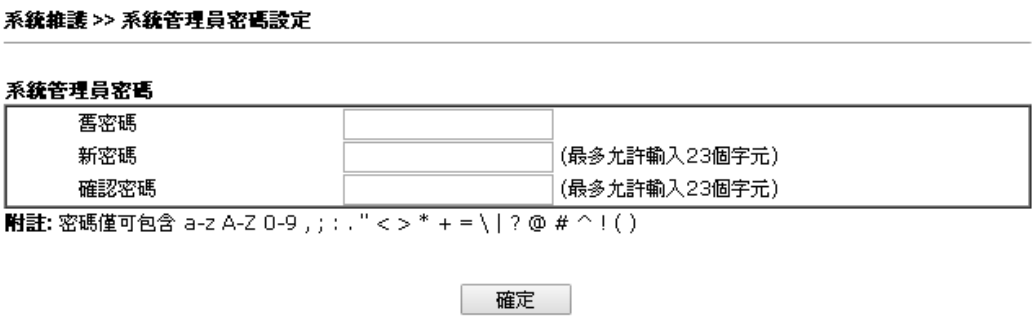
5. 網頁將會依照您所選擇的條件開啓不同的頁面，預設值通常爲自動登出，若操作者沒有進行任何動作時，網頁會在 5 分鐘後自動離開，您可以視需要改變登出的時間設定。



1.6 變更密碼

爲了路由器的安全起見，建議您將先行變更密碼。

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，
3. 進入**系統維護(System Maintenance)**頁面並選擇**系統管理員密碼(Administrator Password Setup)**。



4. 輸入**舊密碼(Old Password**, 預設值爲空白)。 在**新密碼(New Password)**及**確認密碼(Confirm Password)**輸入您想要設定的密碼，然後按**確定(OK)**儲存設定。
5. 現在您已經完成變更密碼設定。請記得在下一次登入設定介面時使用新的密碼。

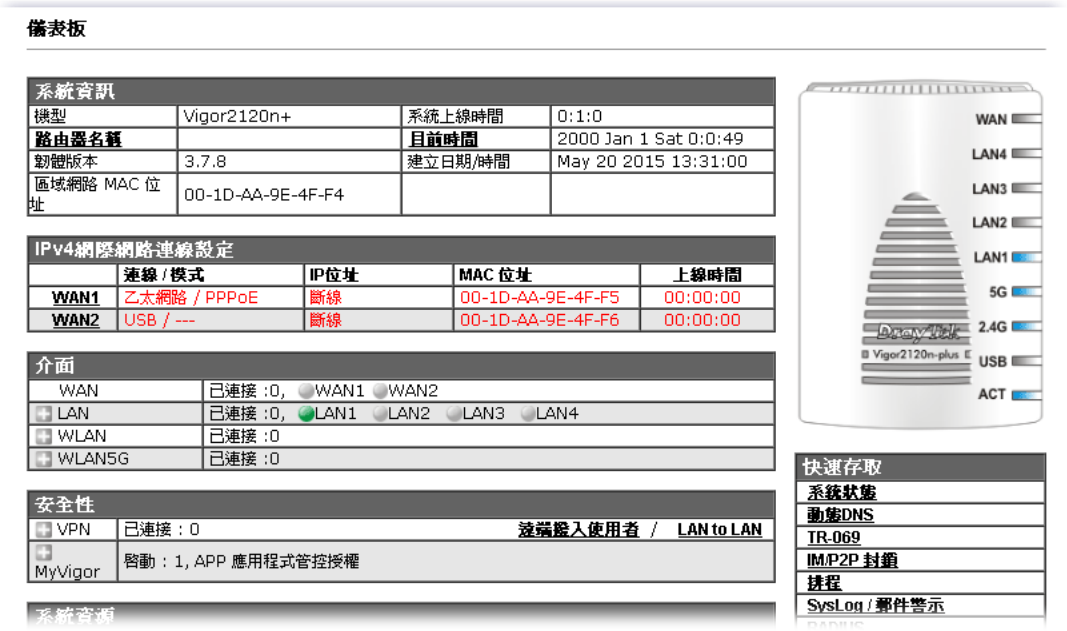
注意：即使密碼已經變更，登入使用者介面的使用者名稱仍然爲“admin。

1.7 儀表板(Dashboard)簡介

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

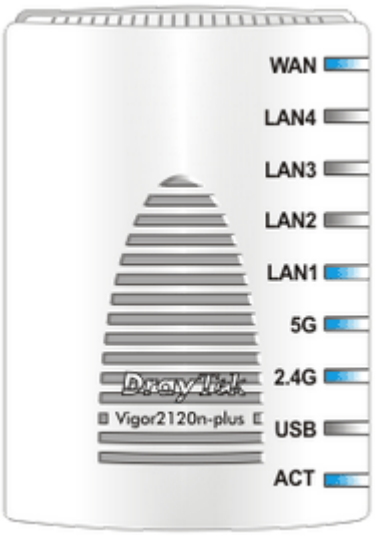
自左手邊的主選單上按下儀表板功能。

預設值網頁將會顯示在螢幕上，請參考下圖：



1.7.1 虛擬面板

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



有關燈號的詳細說明，請參考 **1.2 LED 指示燈與介面說明**一節。

1.7.2 底線連結

任何一個名稱下方含有底線者(如路由器名稱、目前時間、WAN1/2/3 等等.)表示您可以按下該連結開啓設定頁面。

儀表板

系統資訊			
機型	Vigor2120n+	系統上線時間	0:1:0
路由器名稱		目前時間	2000 Jan 1 Sat 0:0:49
韌體版本	3.7.8	建立日期/時間	May 20 2015 13:31:00
區域網路 MAC 位址	00-1D-AA-9E-4F-F4		

IPv4網際網路連線設定				
	連線 / 模式	IP位址	MAC 位址	上線時間
WAN1	乙太網路 / PPPoE	斷線	00-1D-AA-9E-4F-F5	00:00:00
WAN2	USB / ---	斷線	00-1D-AA-9E-4F-F6	00:00:00

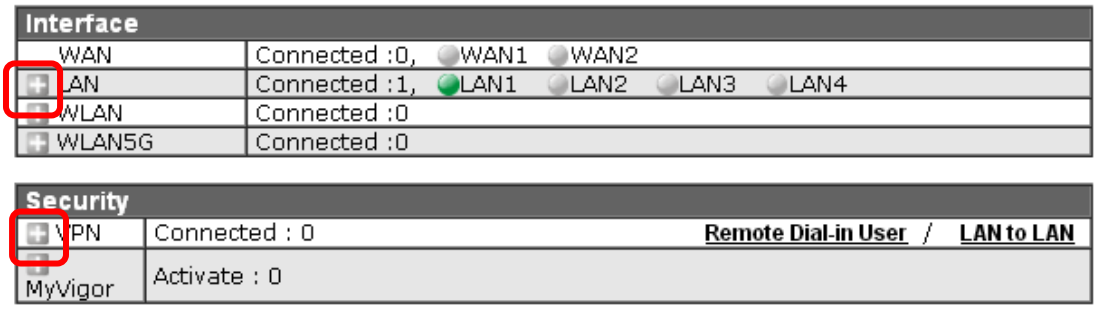
1.7.3 常用功能的快速存取

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

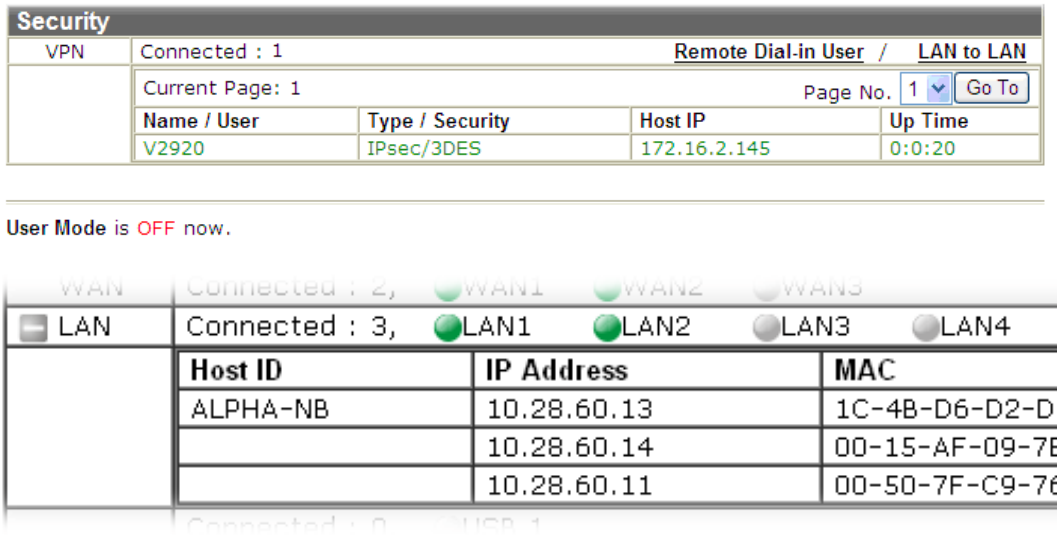
請移動前往儀表板的右邊，您可以在**快速存取(Quick Access)**一區中看到常用功能群。

本區將系統狀態(System Status)、動態 DNS (Dynamic DNC)、TR-069、IM/P2P 封鎖(IM/P2P Block)、排程(Schedule)、Syslog/郵件警示(Syslog/Mail Alert)、RADIUS、防火牆物件設定(Firewall Object Setting)以及資料流量監控(Data Flow Monitor)等常用連結歸納於此，移動您的滑鼠至任何一個連結在輕輕按下，相應頁面即可立刻開啓。

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



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



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

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

1.7.4 圖形介面地圖(GUI Map)

路由器支援的全部功能可在此頁面下全部呈現出來，使用者可以按此功能連結進入相關頁面進行細部設定。

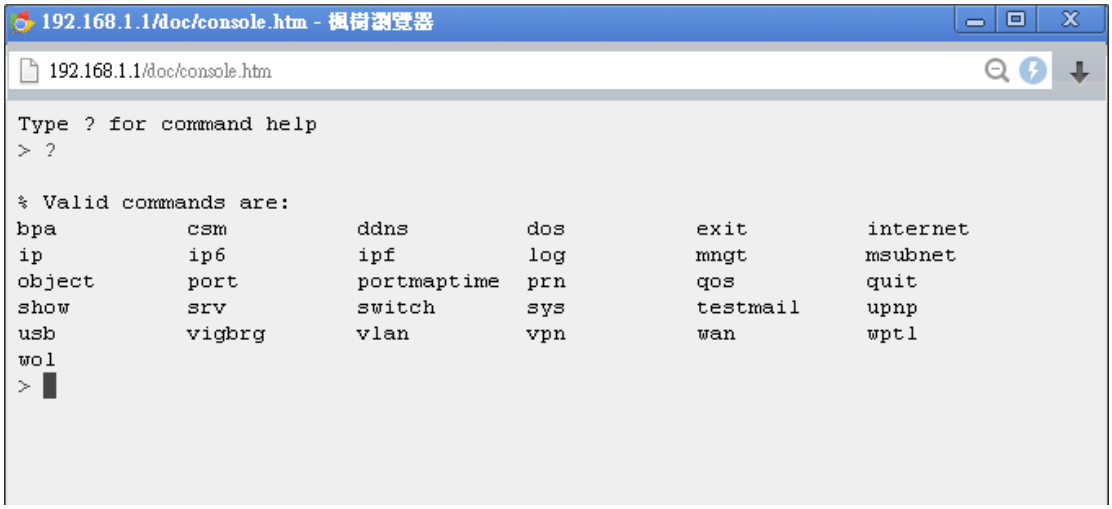
GUI 地圖

儀表板		**憑證管理**	
設定精靈			**本地憑證**
	快速設定精靈		**具公信力之 CA 憑證**
	服務啓動精靈		**憑證備份**
	VPN 用戶端設定精靈	**無線區域網路 (2.4 GHz)**	
	VPN伺服器設定精靈		**基本設定**
線上狀態			**安全性**
	實體連線		**連線控制**
	虛擬 WAN		**WPS**
WAN			**WDS**
	基本設定		**進階設定**
	網際網路連線		**WMM 設定**
	多重 VLAN		**搜尋無線基地台**
LAN			**無線用戶端列表**
	基本設定		**無線用戶端管理**
	固定路由	**無線區域網路 (5 GHz)**	
	VLAN		**基本設定**
	綁定 IP 與 MAC 位址		**安全性**
	LAN 埠號監控		**連線控制**
	客製化入口網站設定		**WPS**
NAT			**WDS**
	通訊埠重導向		**進階設定**
	DMZ 主機		**WMM 設定**
	開放通訊埠		**搜尋無線基地台**
	位址對應		**無線用戶端列表**
	埠號觸發		**無線用戶端管理**

1.7.5 網頁操作台(Web Console)

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

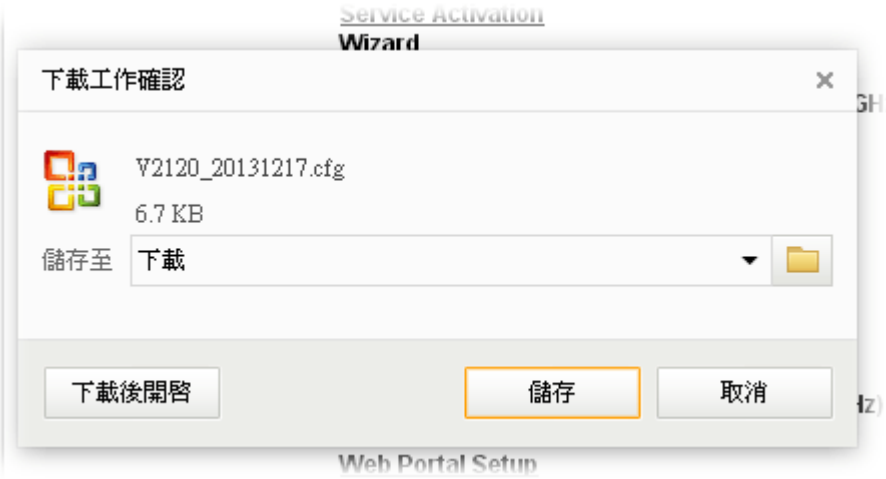
請按主頁面上方的 **Web Console** 圖示即可開啓如下視窗。



1.7.6 設定備份(Config Backup)

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

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



按下**儲存**將設定儲存起來。

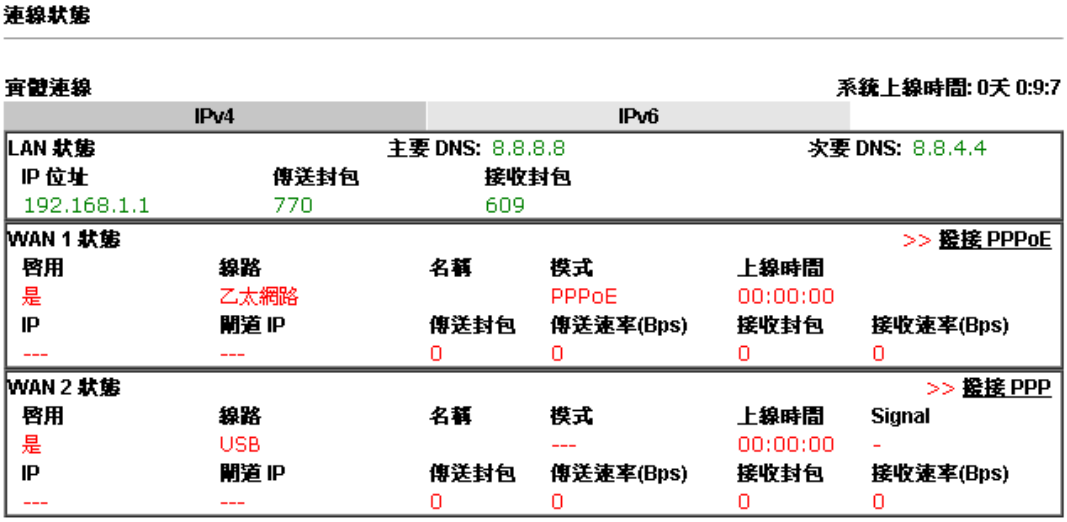
1.7.7 登出

登出按鈕即可離開此使用者設定介面。

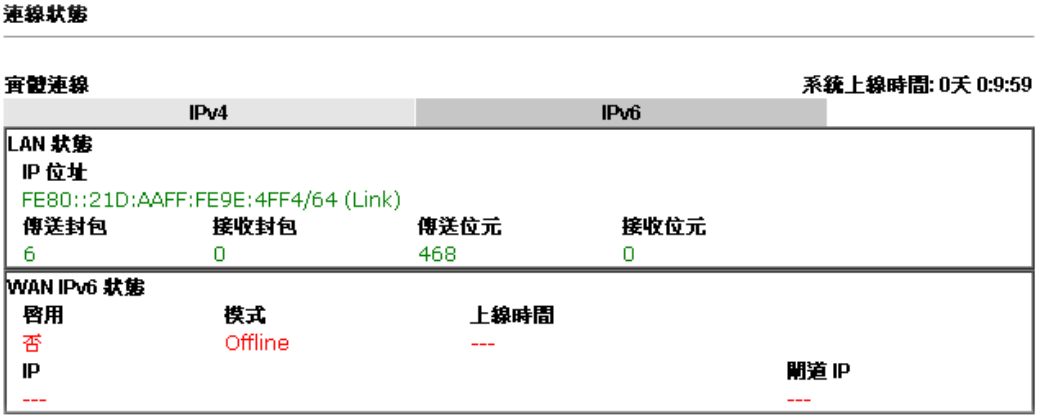
1.8 連線狀態

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

1.8.1 IPv4 協定的實體連線



1.8.2 IPv6 協定的實體連線



詳細說明於後(IPv4):

項目	說明
LAN 狀態	**主要 DNS**- DNS.顯示主要 DNS 的 IP 位址。 **次要 DNS**- 顯示次要 DNS 的 IP 位址。 **IP 位址**- 顯示 LAN 介面的 IP 位址。 **傳送封包** - 顯示在區域網路全部的傳送封包量。。 **接收封包**- 顯示區域路網路中全部的接收封包量。
WAN 1 狀態 ~ WAN 3 狀態	**啓用 – 是**(紅色字體) 表示此介面可以運用但尚未連接，**是**(藍色字體) 表示此介面已連接。 **線路**- 顯示此介面的實體連線類型。 **名稱**- 顯示 WAN1~WAN3 網頁上所顯示的名稱。

項目	說明
	模式 - 顯示 WAN 連線的模式類型(例如 PPPoE)。 **上線時間** - 顯示介面上全部的上傳時間。 **IP** - 顯示 WAN 介面的 IP 位址。 **閘道 IP** - 顯示預設閘道的 IP 位址。 **傳送位元** - 顯示 WAN 介面上全部傳送的封包數。 **傳送速率** - 顯示 WAN 介面上全部傳送速率位元數。 **接收位元** - 顯示 WAN 介面上全部接收的封包數。 **接收速率** - 顯示 WAN 介面上全部接收速率位元數。

詳細說明於後(IPv6):

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

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

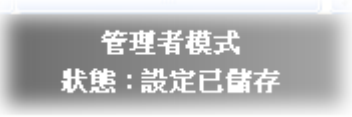
1.8.3 虛擬 WAN(Virtual WAN)

本頁顯示虛擬 WAN 連線的相關資訊。

虛擬 WAN 連線用於 TR-069 管理、VoIP 等服務上。

1.9 儲存設定

每當您按下網頁上的確定按鈕以儲存檔案，您都可以見到如下的訊息，此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。

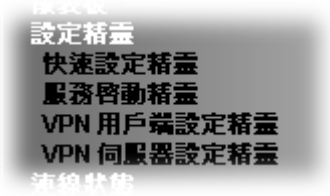
2 快速設定

系統提供您數種設定精靈讓您能輕鬆且快速的設定路由器。

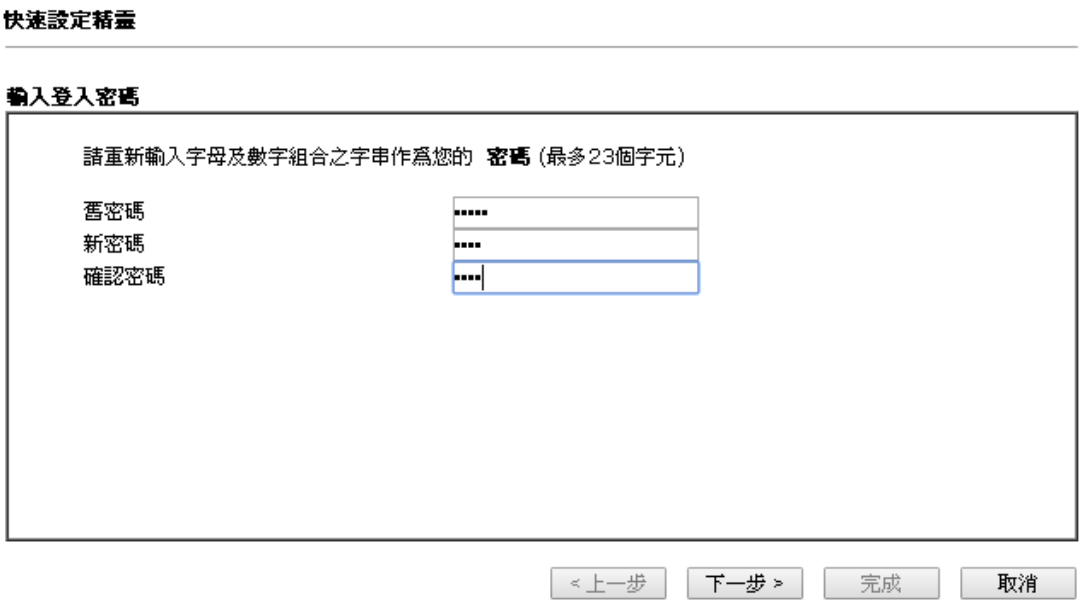
- **快速設定精靈** – 用於建立網際網路連線。
- **服務啓用精靈** – 用於啓動網頁內容過濾器服務機制。
- **VPN 用戶端精靈** – 用於建立 VPN 連線，路由器被視之爲 VPN 用戶端。
- **VPN 伺服器端精靈** – 用於建立 VPN 連線，路由器被視之爲 VPN 伺服器端。

2.1 快速設定精靈

快速設定精靈主要設計目的是爲了讓您能夠以簡易的步驟快速設定路由器連上網際網路。請開啓**精靈設定>>快速設定精靈**。



您可以依照下列的步驟使用快速設定精靈設定您的路由器。快速設定精靈的第一個畫面會要求您輸入密碼，輸入密碼之後，請按**下一步(Next)**。



在下述頁面，請選擇使用的 WAN 介面，如果使用的是乙太網路介面，請選擇 WAN1，若使用的是 3G USB 數據機，請選擇 WAN2，然後按**下一步**。

WAN1 與 WAN2 帶來的設定頁面所不同，請參考下述細部說明。

2.1.1 對於 WAN1 介面(乙太網路)

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

請依照 ISP 業者提供給您的資訊選擇適當的網際網路連線類型，舉例來說，如果 ISP 提供給您的是 PPPoE 介面，您應該選擇 PPPoE 模式，然後按**下一步(Next)**繼續進行。

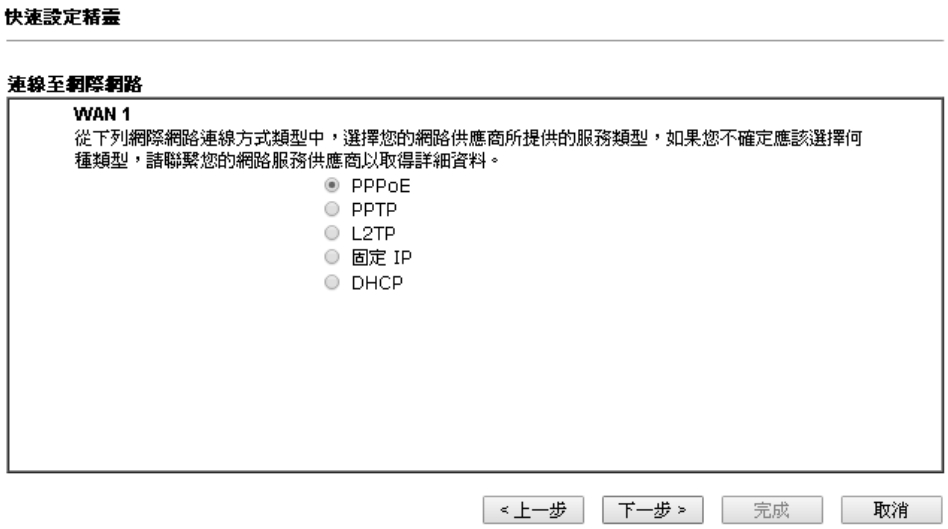
2.1.1.1 PPPoE

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。

1. 開啓**設定精靈>>快速設定精靈**。輸入密碼之後，按**下一步(Next)**。

2. 選擇 **WAN1** 作爲 WAN 介面，按**下一步(Next)**。

3. 下圖將會出現讓您指定網際網路連線類型。選擇 **PPPoE** 然後按**下一步(Next)**。

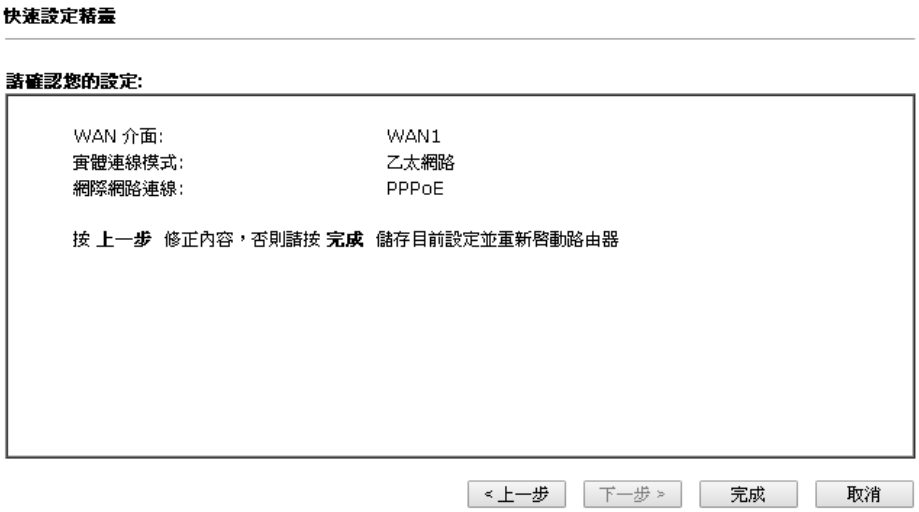


4. 請依照您的 ISP 業者提供的資料輸入使用者名稱與密碼。輸入完畢，按**下一步(Next)**。

可用設定說明如下：

項目	說明
服務名稱 (Service Name)	輸入得以辨識服務供應商的資訊。
使用者名稱 (Username)	指定 ISP 提供之有效使用者名稱。
密碼 (Password)	指定 ISP 提供之有效密碼。
確認密碼 (Confirm Password)	重新輸入密碼以確認。
上一步(Back)	按此鈕回到上一頁面。
下一步(Next)	按此鈕進入下一頁面。
取消(Cancel)	按此鈕放棄快速設定精靈。

5. 連線摘要內容將顯示如下。



6. 按**完成**，**快速設定精靈安裝完畢**頁面將會出現。

7. 現在您可以遨遊網際網路了。

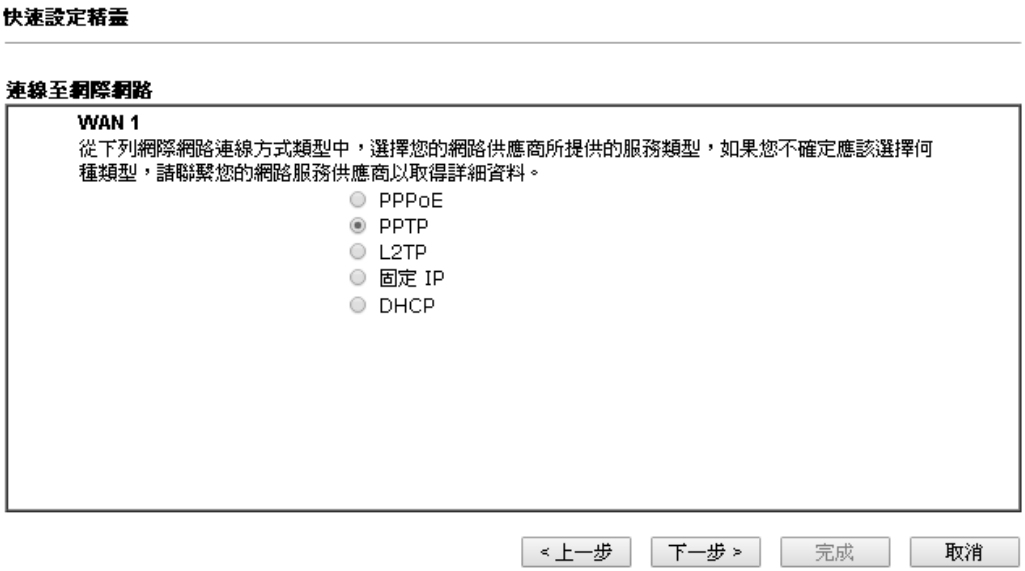
2.3.1.2 PPTP/L2TP

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

1. 開啓**設定精靈>>快速設定精靈**。輸入密碼之後，按**下一步(Next)**。

2. 選擇 **WAN1** 作爲 WAN 介面，按**下一步(Next)**。

3. 下圖將會出現讓您指定網際網路連線類型。選擇 **PPTP/L2TP** 然後按**下一步(Next)**。



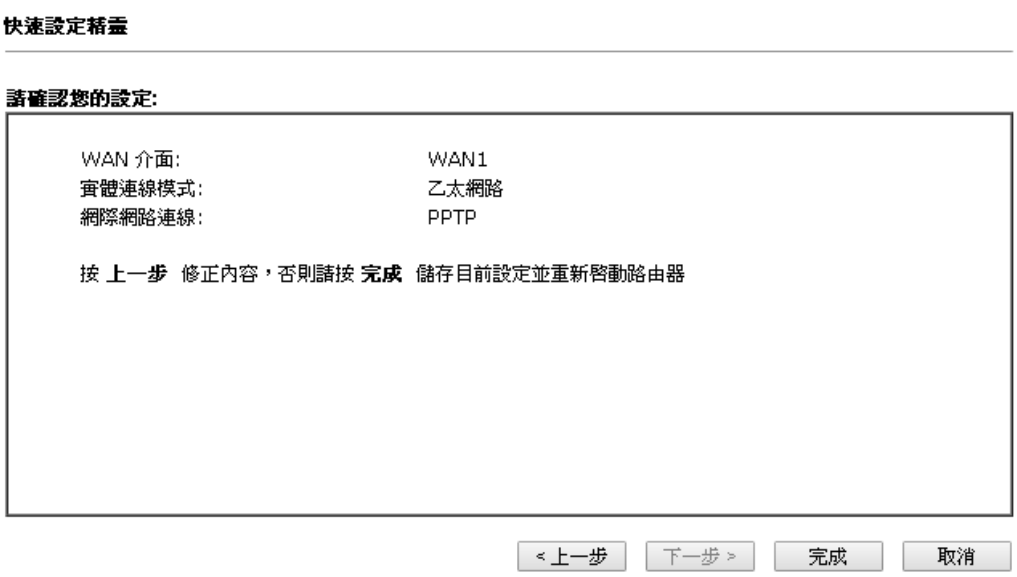
4. 請依照您的 ISP 業者提供的資料輸入相關資訊。輸入完畢，按**下一步(Next)**。

可用設定說明如下：

項目	說明

使用者名稱 (User Name)	指定 ISP 提供之有效使用者名稱。
密碼 (Password)	指定 ISP 提供之有效密碼。
確認密碼 (Confirm Password)	重新輸入密碼以確認。
WAN IP 組態設定 (WAN IP Configuration)	**自動取得 IP 位址 (Obtain an IP address automatically)**– 路由器可自 DHCP 伺服器自動取得 IP 位址。 **指定 IP 位址(Specify an IP address)** – 使用者須手動輸入相關設定。 **IP 位址(IP Address)** – 輸入 IP 位址。 **子網路遮罩(Subnet Mask)**– 輸入子網路遮罩。 **閘道(Gateway)** –輸入閘道 IP 位址。 **主要 DNS(Primary DNS)** – 輸入路由器主要的 DNS IP 位址。 **次要 DNS (Second DNS)**– 必要時輸入路由器次要的 DNS IP 位址。
PPTP 伺服器 / L2TP 伺服器 (PPTP Server / L2TP Server)	輸入伺服器的 IP 位址。
上一步(Back)	按此鈕回到上一頁面。
下一步(Next)	按此鈕進入下一頁面。
取消(Cancel)	按此鈕放棄快速設定精靈。

5. 連線摘要內容將顯示如下。

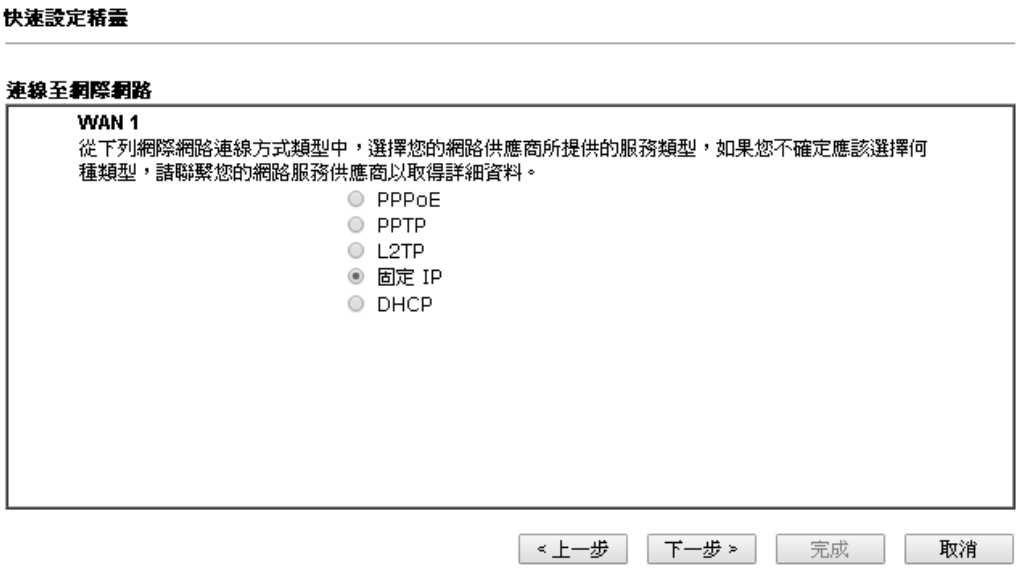


6. 按**完成**，**快速設定精靈安裝完畢**頁面將會出現。
7. 現在您可以遨遊網際網路了。

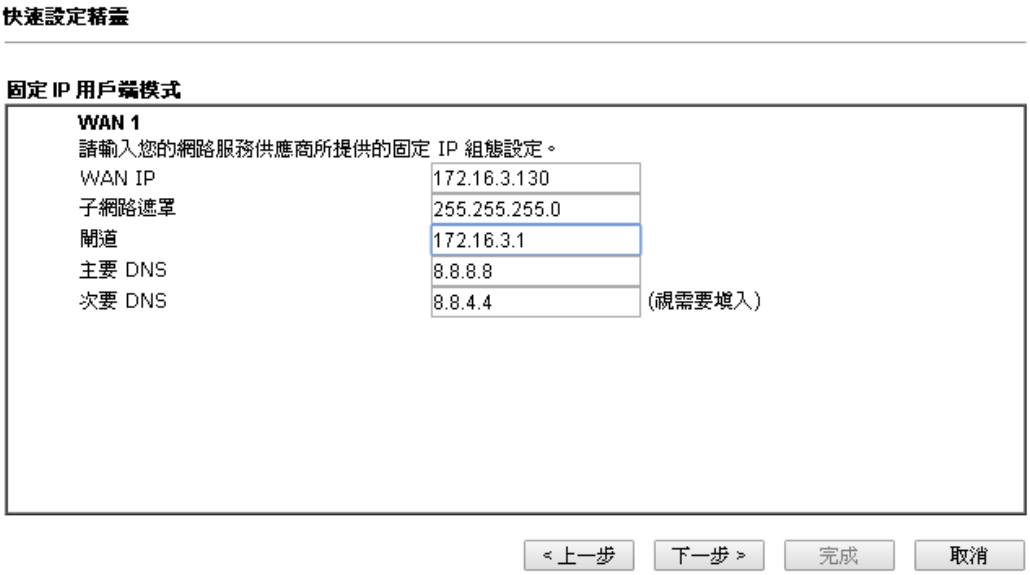
2.1.1.3 固定 IP

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

1. 開啓**設定精靈>>快速設定精靈**。輸入密碼之後，按**下一步(Next)**。
2. 選擇 **WAN1** 作爲 WAN 介面，按**下一步(Next)**。
3. 下圖將會出現讓您指定網際網路連線類型。選擇**固定 IP** 然後按**下一步(Next)**。



4. 請依照您的 ISP 業者提供的資料輸入相關資訊。輸入完畢，按**下一步(Next)**。



可用設定說明如下：

項目	說明
WAN IP	輸入 IP 位址。
子網路遮罩 (Subnet Mask)	輸入子網路遮罩。
閘道 (Gateway)	輸入閘道 IP 位址。
主要 DNS (Primary DNS)	輸入路由器主要的 DNS IP 位址。
次要 DNS (Secondary DNS)	必要時輸入路由器次要的 DNS IP 位址。
上一步 (Back)	按此鈕回到上一頁面。
下一步 (Next)	按此鈕進入下一頁面。
取消 (Cancel)	按此鈕放棄快速設定精靈。

5. 連線摘要內容將顯示如下。

6. 按**完成**，**快速設定精靈安裝完畢**頁面將會出現。

7. 現在您可以遨遊網際網路了。

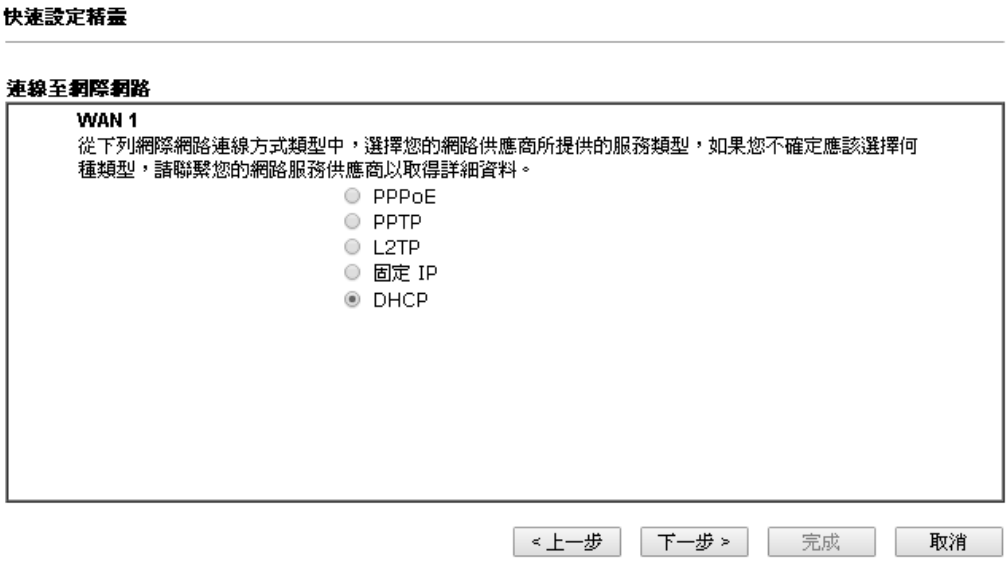
2.1.1.4 DHCP

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。.

1. 開啓**設定精靈>>快速設定精靈**。輸入密碼之後，按**下一步(Next)**。

2. 選擇 **WAN1** 作爲 WAN 介面，按**下一步(Next)**。

3. 下圖將會出現讓您指定網際網路連線類型。選擇 **DHCP** 然後按**下一步(Next)**。



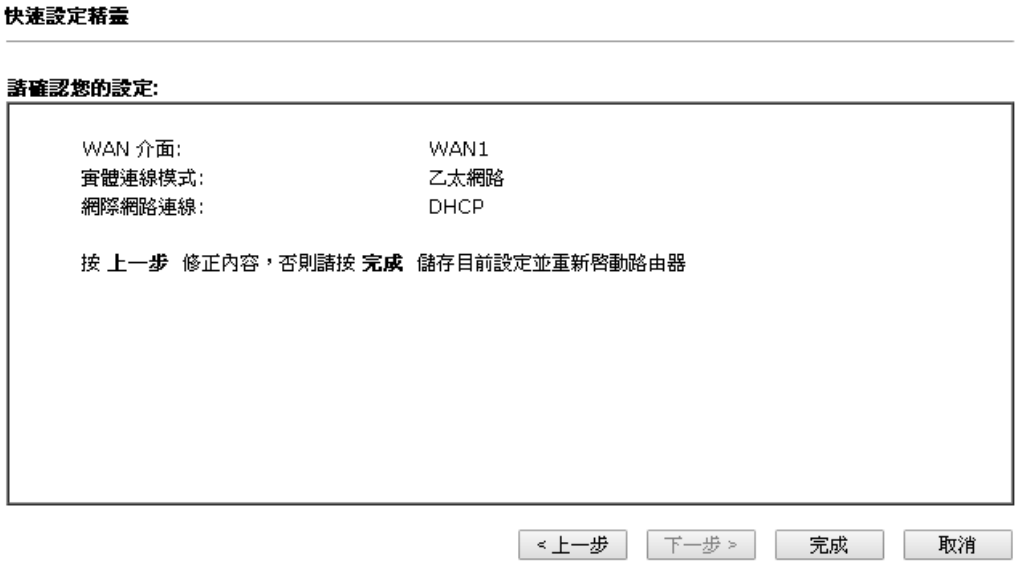
4. 請依照您的 ISP 業者提供的資料輸入相關資訊。輸入完畢，按**下一步(Next)**。

可用設定說明如下：

項目	說明
主機名稱 (Host Name)	輸入主機名稱。

MAC	某些纜線服務供應商會要求提供 MAC 位址作爲驗證，在此情況下，請於此欄位輸入 MAC 位址。
上一步 (Back)	按此鈕回到上一頁面。
下一步 (Next)	按此鈕進入下一頁面。
取消 (Cancel)	按此鈕放棄快速設定精靈。

5. 連線摘要內容將顯示如下。



6. 按**完成**，**快速設定精靈安裝完畢**頁面將會出現。

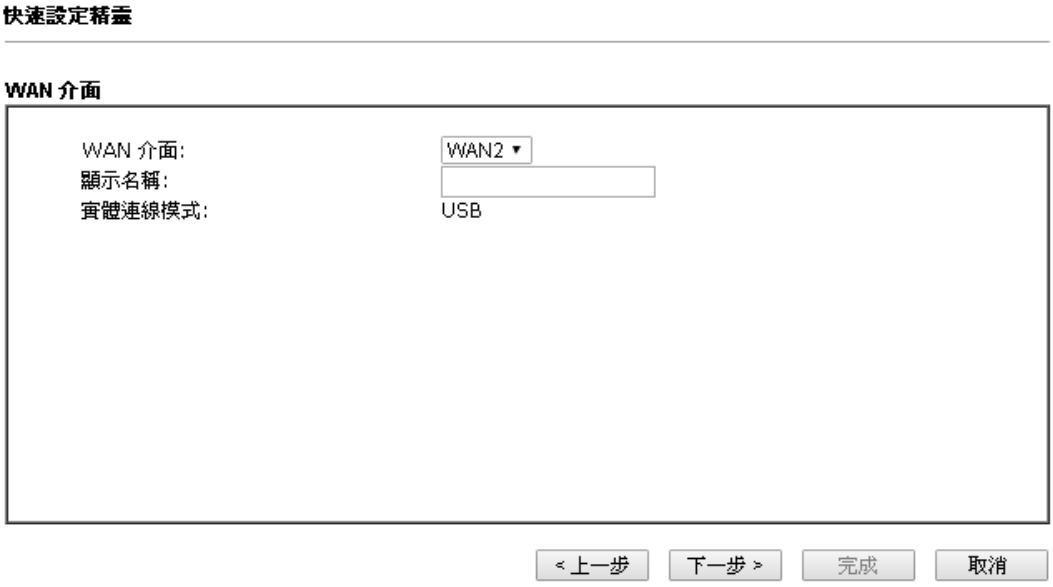
7. 現在您可以遨遊網際網路了。

2.1.2 對於 WAN2 介面 (USB)

如果要使用 3G USB 數據機進行網路連線，請選擇 WAN2。

1. 開啓**設定精靈>>快速設定精靈**。輸入密碼之後，按**下一步(Next)**。

2. 選擇 **WAN2** 作爲 WAN 介面，按**下一步(Next)**。



3. 在出現的頁面中，輸入 3G/4G USB 數據機所需的相關資訊，再按**下一步**。

可用設定說明如下：

項目	說明
網際網路連線 (Internet Access)	選擇存取網際網路的連線模式。
3G/4G USB 數據機	**SIM Pin 碼 (SIM Pin code)** – 輸入用來登入網際網路之

(PPP 模式) **(3G/4G USB Modem (PPP mode))**	SIM 卡的 PIN 代碼，最大長度爲 15 個字元。 **數據機初始字串 (Modem Initial String)** – 這個數值，用來初始化 USB 數據機，請使用預設值，如果您有任何疑問，請與當地 ISP 業者聯絡。 **APN 名稱 (APN Name)** – APN 表示基地台的名稱，通常是由 ISP 業者提供並要求您在此輸入，請輸入相關名稱並按下**套用**按鈕。
4G USB 數據機 (DHCP 模式) **(4G USB Modem (DHCP mode))**	**SIM PIN 碼(SIM Pin code)** – 輸入用來登入網際網路之 SIM 卡的 PIN 代碼，最大長度爲 15 個字元。 **網路模式(Network Mode)** – 強迫路由器以此處指定的模式進行網際網路連線，如果您選擇了 4G/3G/2G 做爲網路模式，路由器將會依照實際網路信號自動選擇適當的模式。 **APN 名稱(APN Name)** – APN 表示基地台的名稱，通常是由 ISP 業者提供並要求您在此輸入，請輸入相關名稱。

4. 連線摘要內容將顯示如下。

5. 按**完成**，**快速設定精靈安裝完畢**頁面將會出現。

快速設定精靈設定完成!

6. 現在您可以遨遊網際網路了。

2.2 服務啟動精靈

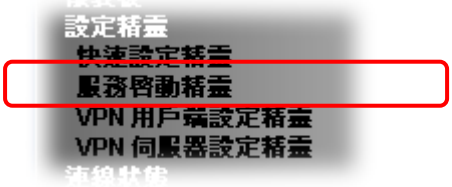
服務啓用精靈可利用快速及簡便方式，幫助您啓用網頁內容過濾器服務機制(WCF)。

> **注意:** WCF 並非 Vigor 路由器的內建機制，該服務是由 Commtouch 公司所提供，如果您想要使用此類服務(試用版或是正式版)，您必須先進行啓用的程序。若您想要使用正式版，請先與經銷商聯絡，獲取更多更詳細的 WCF 資訊。

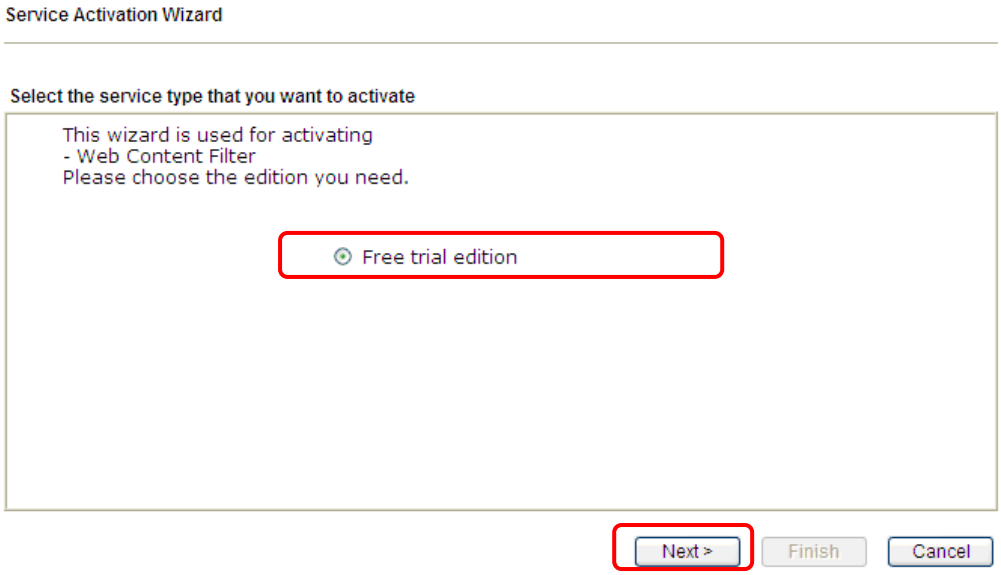
服務啓用精靈是一個提供您使用試用版 WCF 授權憑證的工具，有了這項工具，您可不需要進入位於 http://myvigor.draytek.com 中的伺服器(***MyVigor***)。關於使用網頁內容過濾器的設定檔，請參考後續網頁內容過濾一節。

現在，請參考下述步驟進行啓用 WCF 功能作業。

1. 開啓**設定精靈>>服務啓動精靈**。

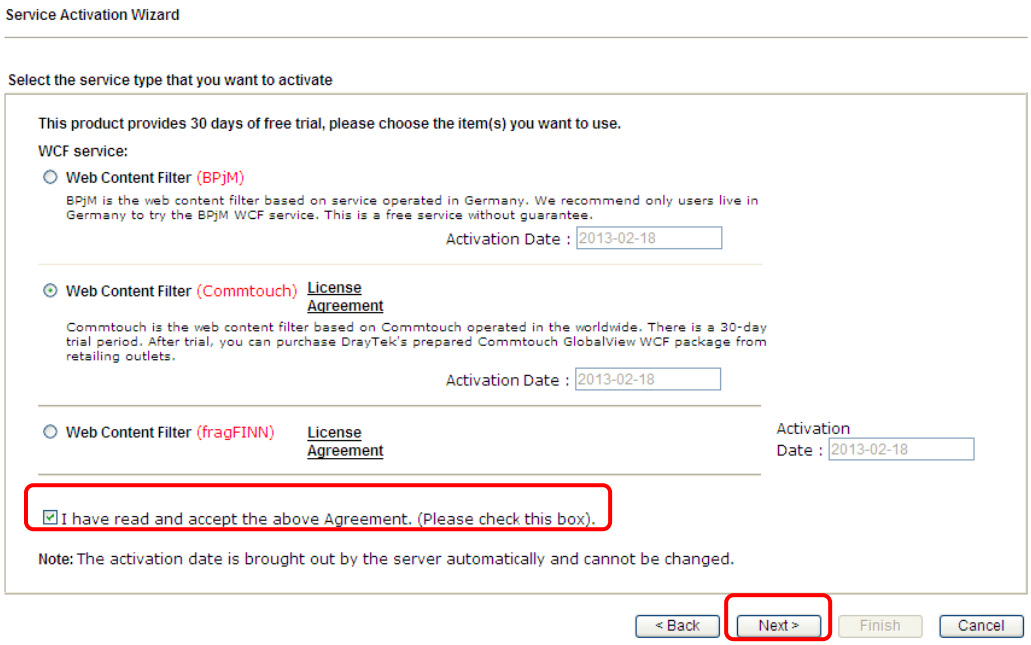


2. 服務啓用精靈畫面顯示如下，請選擇其中一個項目(例如本例使用**免費試用版**)，按**下一步**。



免費試用版: 提供短期試用期限讓您熟悉 WCF 功能。

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

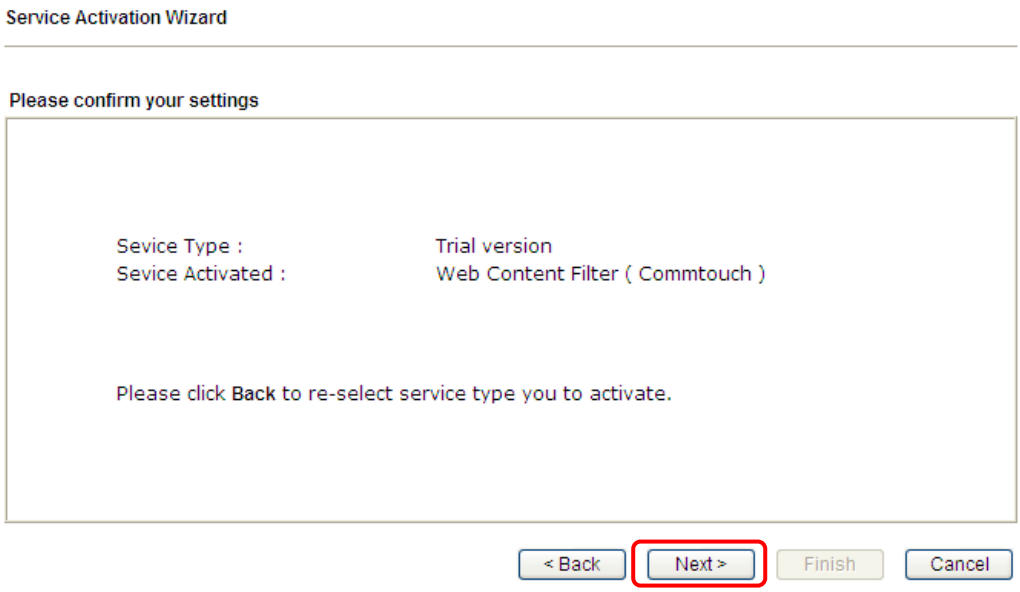


Commtouch 爲一個能在全球運作的網頁內容過濾器，系統提供您 30 天的試用期，試用完畢後，您可以洽詢經銷商購買一套 Commtouch GlobalView WCF 授權書。

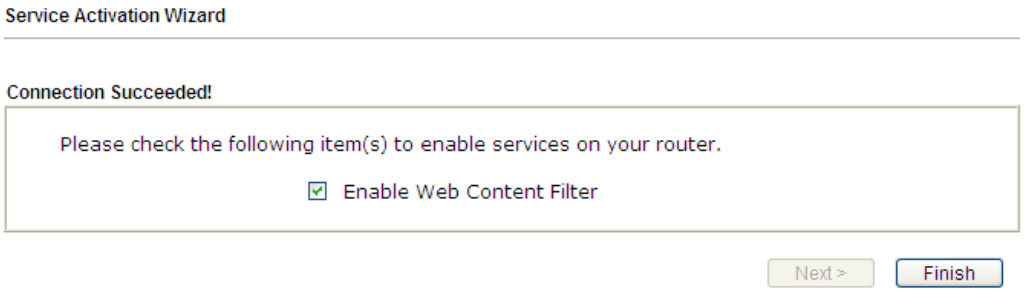
適用德國地區的用戶，fragFINN 對德語用戶屬於白名單，對於家中有青少年的家庭來說 BPjM 可以提供更爲安全的網際網路連線。

自 2015 年 1 月 1 日起，系統已不在支援 fragFINN 服務。

4. 設定確認頁面顯示如下所述，按**下一步(Next)**。



5. 請等候直到以下頁面出現。

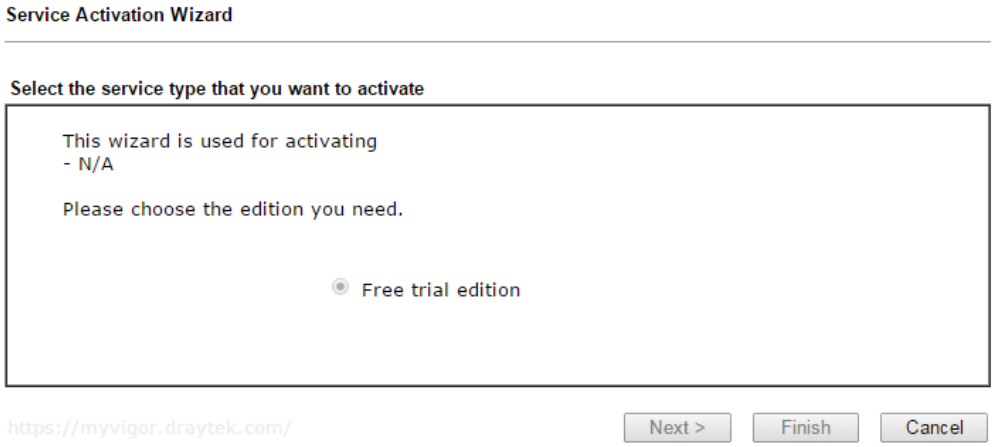


當此頁面出現時，您可啓用或是關閉服務，視您實際情況需要而定，然後按下**完成**。

注意: 此服務可以啓用並當成**防火牆>>基本設定**的預設規則。

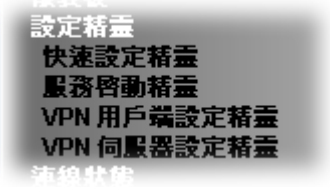
6. 現在，網頁上將依照您的設定顯示出啓用服務的細節內容，試用版的有效時間通常爲 30 天。

當網頁內容過濾器所有試用版皆已啓動，服務啓動精靈(Service Activation Wizard) 將不再有效，參考下圖。

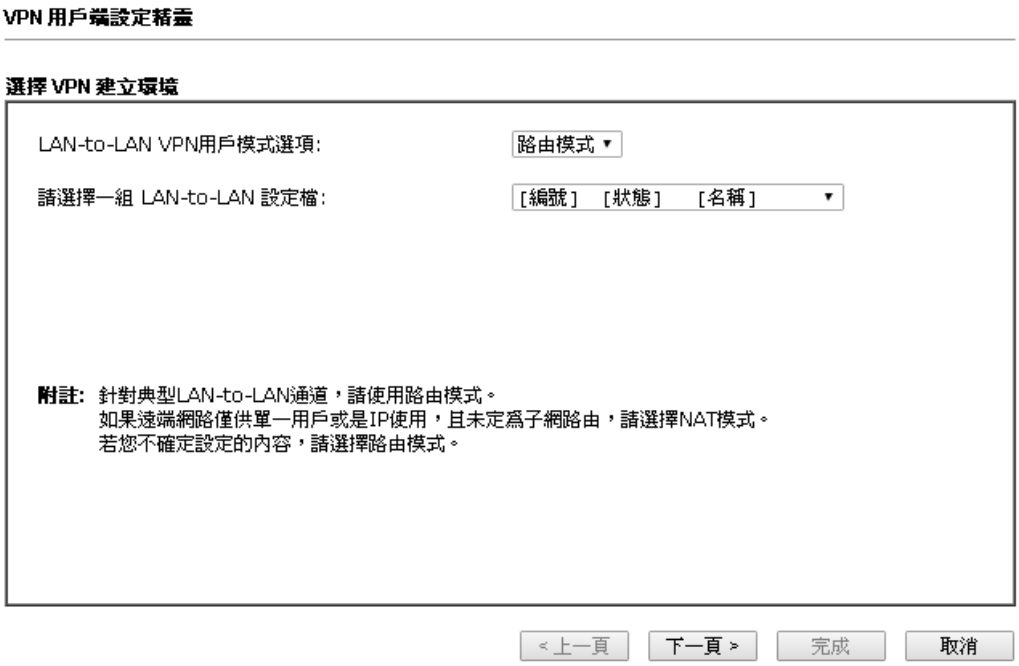


2.3 VPN 用戶端精靈

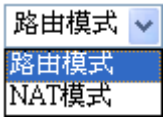
此精靈用來設定 VPN 用戶端所需的 VPN 設定，精靈將引導您一步步建立 VPN 撥出方向的 LAN-to-LAN 設定檔(從伺服器到用戶端)。

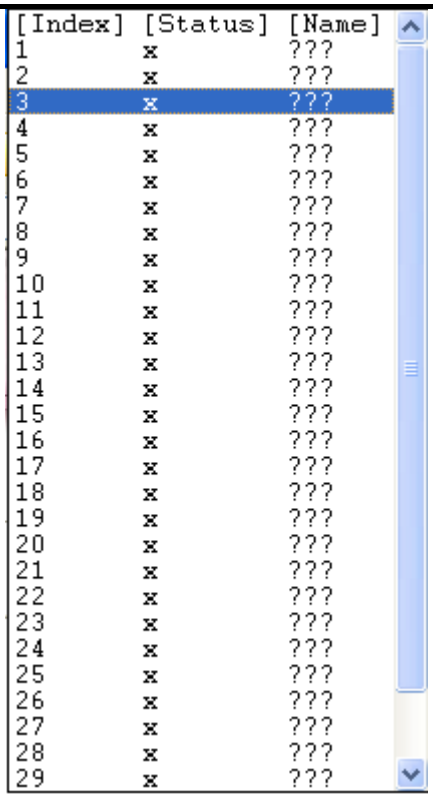


1. 開啓 **VPN 與遠端存取>VPN 用戶端設定精靈(VPN and Remote Access>>VPN Client Wizard)**，設定頁面如下所示：



可用設定說明如下：

項目	說明
LAN-to-LAN 用戶端模式選項 (LAN-to-LAN Client Mode Selection)	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 (Please choose a LAN-to-LAN Profile)	共有 32 個 VPN 設定檔可以供使用者選擇來設定。



2. 選擇好模式與設定檔選項之後，請按**下一頁(Next)**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(Next)**，根據您所選擇的條件，您將會看到不同的配置畫面：

注意：以下提供的 VPN 類型說明以**路由模式**爲基準。

- 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：

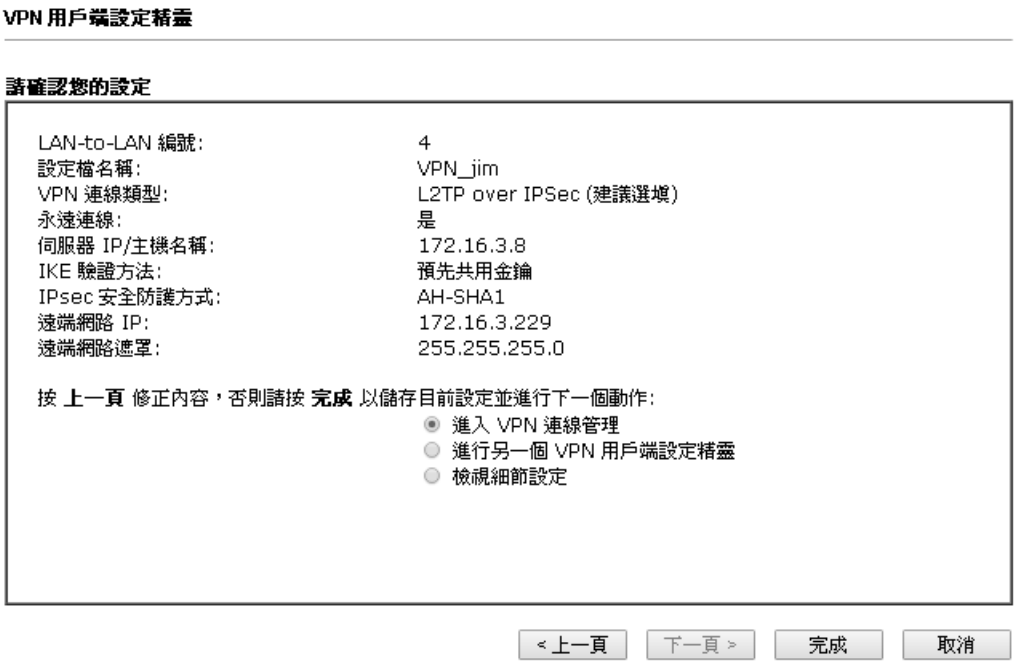
- 當您選擇 **L2TP over IPSec (Nice to Have)** 或是 **L2TP over IPSec (Must)**，您看到的頁面如下：

可用設定說明如下：

項目	說明
設定檔名稱 (Profile Name)	請輸入設定檔的檔名，檔案的長度限制在 10 的字元間。
永遠連線 (Always On)	勾選此方塊讓路由器永遠保持 VPN 連線。
伺服器 IP/ VPN 的主機名稱 (Server IP/Host Name for VPN)	輸入伺服器的 IP 位址或是輸入此 VPN 設定檔的主機名稱。
IKE 驗證方式 (IKE Authentication Method)	**預先共用金鑰(Pre-Shared Key)-** 勾選此方塊啓用此功能並按 **IKE 預先共用金鑰**按鈕輸入金鑰及確認金鑰。 **數位簽章 (X.509) –**勾選此方塊啓用此功能並選擇一組事先定義的簽章內容 (在 **VPN 和遠端存取>>IPSec 端點辨識**中設定)。 ● **對方 ID** –自下拉式清單中選擇對方的 ID。 ● **本機 ID** – 選擇**替代主體名稱優先**或是**主體名稱優先**。 ● **本地憑證** –自下拉式清單中選擇一種憑證，您必須事先在**憑證管理>>本機憑證**中設定至少一組的憑證，否則無憑證可以使用。
IPSec 安全防護方式 (IPsec Security Method)	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 (User Name)	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 (Password)	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 (Remote Network 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 (Remote Network Mask)	請輸入區域網路遮罩（依照遠端主機實際位置）建立 VPN 連線。

3. 完成配置後，請按**下一頁(Next)**，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(Finish)**進行另一個 VPN 設定。

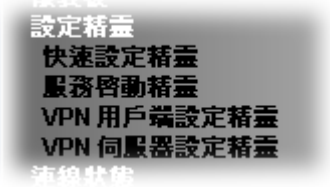


可用設定說明如下：

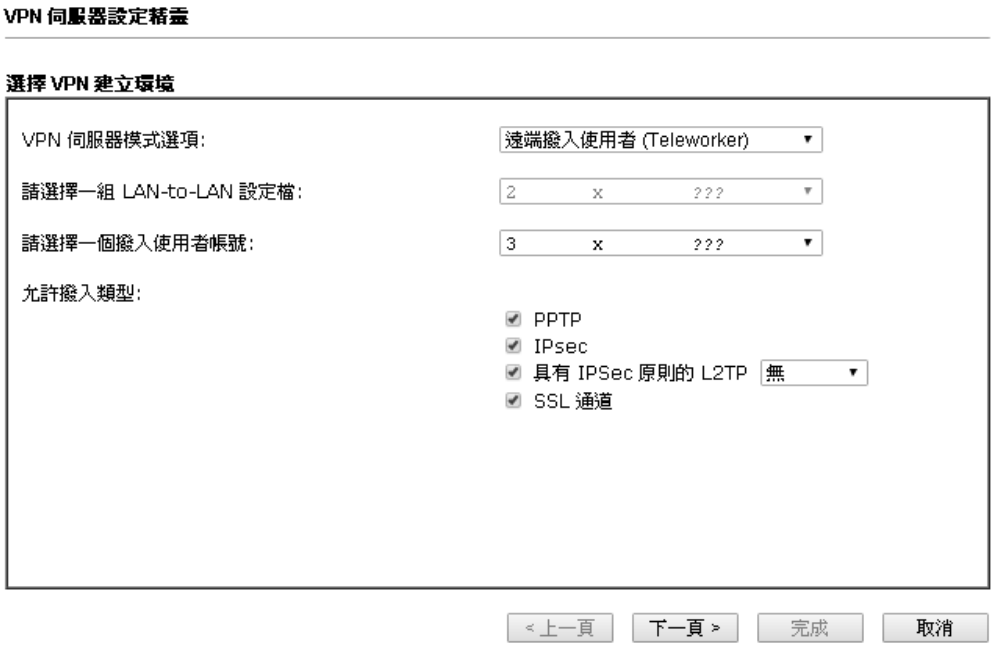
項目	說明
進入 VPN 連線管理 (Go to the VPN Connection Management)	按此鈕進入 VPN 及**遠端存取>>連線管理(VPN and Remote Access>>Connection Management)**頁面檢視 VPN 連線狀態。
執行另一個 VPN 伺服器精靈設定 (Do another VPN Server Wizard Setup)	按此鈕以便利用 VPN 伺服器設定精靈設定另一個 VPN 伺服器設定檔。
檢視設定詳細內容 (View more detailed configuration)	按此鈕進入 **VPN 及遠端存取>> LAN to LAN(VPN and Remote Access>>LAN to LAN)**以檢視細節內容。

2.4 VPN 伺服器端精靈

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

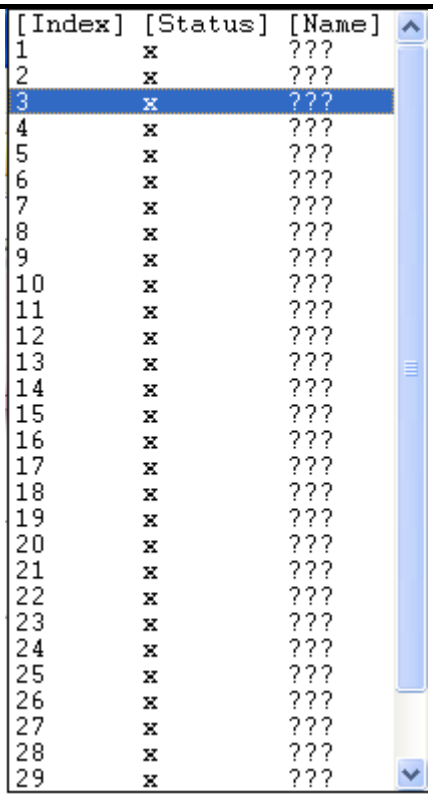
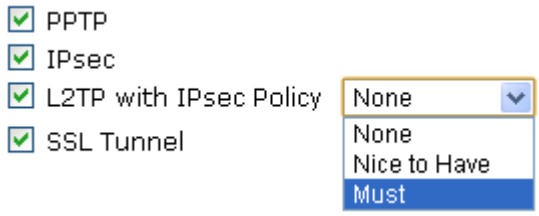


1. 開啓 **VPN 與遠端存取>VPN 伺服器設定精靈(VPN and Remote Access>>VPN Server Wizard)**，設定頁面如下所示：



可用設定說明如下：

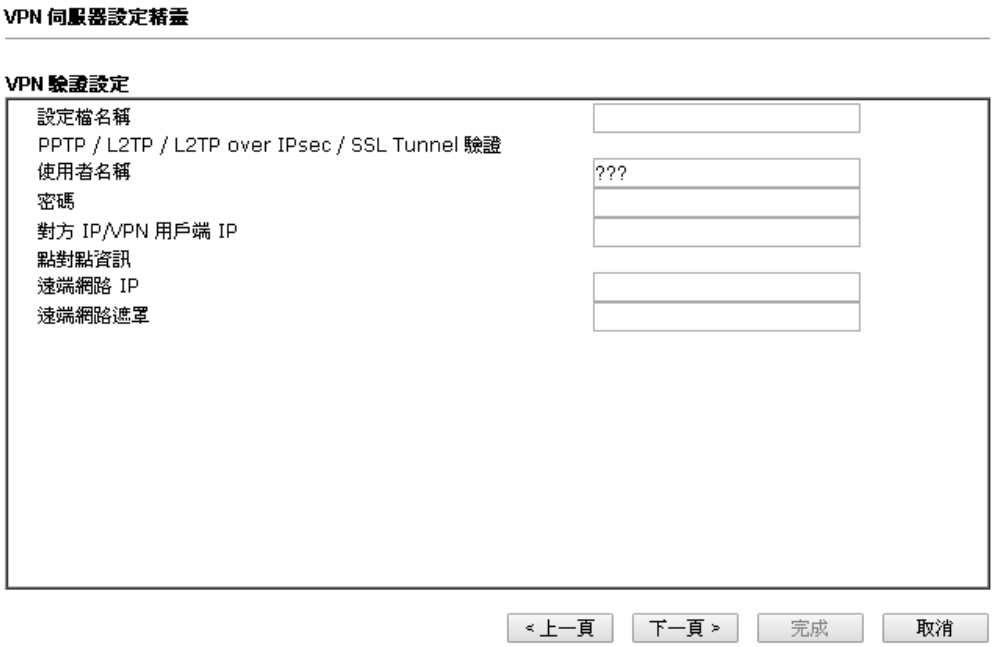
項目	說明
VPN 伺服器模式選項 **(VPN and Remote Access>>VPN Server Wizard)**	請選擇 VPN 伺服器的方向。 **點對點 VPN (Site to Site VPN)**– 想要自動設定 LAN-to-LAN 設定檔，請選擇**點對點 VPN**。 **遠端撥入使用者(Remote Dial-in User)**– 管理遠端使用者設定檔表格來管理遠端用戶的存取狀態，使用者透過 VPN 連線存取網路時，必須接受驗證過程。 **注意**: VPN 伺服器設定精靈畫面會依據所選擇的 VPN 伺服器模式而有所不同。
請選擇 LAN-to-LAN 設定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

Profile)	
請選擇撥入使用者帳號 (Please choose a Dial-in User Accounts)	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 (Allowed Dial-in Type)	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。

2. 在選擇完畢後，請按**下一步(Next)**，根據您所選擇的條件，您將會看到不同的配置畫面。

   此處所舉的範例是**以點對點 VPN(Site-to-Site VPN)**作爲 **VPN 伺服器模式 (VPN Server Mode)** 選項。

- 當您勾選了 PPTP 之後，您會看到如下頁面：



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

- 當您選擇 **IPSec**，您看到的頁面如下：

可用設定說明如下：

項目	說明
設定檔名稱 (Profile Name)	請輸入設定檔的檔名，檔案的長度限制在 10 的字元間。
使用者名稱 (User Name)	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 (Password)	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 (Pre-Shared Key)	爲了驗證 IPSec/L2TP IPSec，請輸入金鑰內容。
確認預先共用金鑰 (Confirm Pre-Shared Key)	再輸入一次金鑰內容確認。
數位簽章 (X.509) (Digital Signature (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 (Peer IP/VPN Client 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 (Peer ID)	請輸入遠端用戶的 ID 名稱。
遠端網路 IP (Remote Network 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 (Remote Network Mask)	請輸入區域網路遮罩（依照遠端主機實際位置）建立 VPN 連線。

3. 完成配置後，請按**下一步(Next)**，確定頁面將顯示如下，如果沒有任何問題的話，您可以按下面可至不同設定頁面的按鈕，然後按**完成**進行另一個 VPN 設定。

可用設定說明如下：

項目	說明
進入 VPN 連線管理 (Go to the VPN Connection Management)	按此鈕進入 **VPN 及遠端存取>>連線管理(VPN and Remote Access>>Connection Management)**頁面檢視 VPN 連線狀態。
執行另一個 VPN 伺服器精靈設定 (Do another VPN Server Wizard Setup)	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 (View more detailed configuration)	按此鈕進入 **VPN 及遠端存取>> LAN to LAN(VPN and Remote Access>>LAN to LAN)**以檢視細節內容。

2.5 註冊 Vigor 路由器

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

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

2. 按下位於首頁上的**支援區域>>產品註冊**。

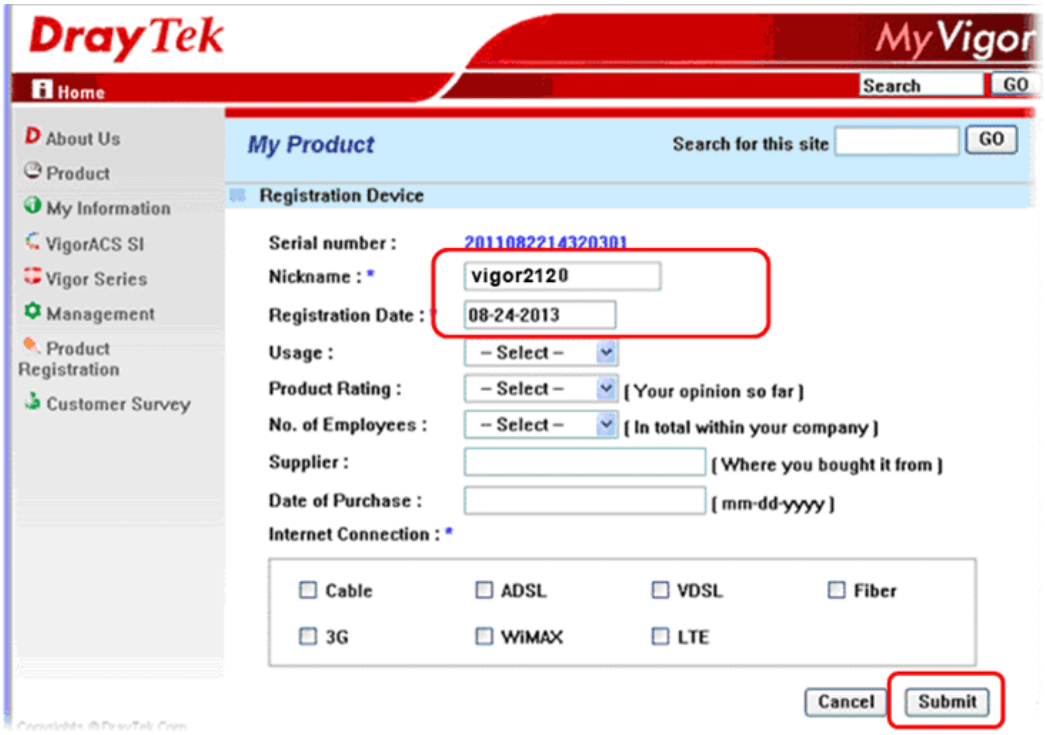
3. 登入頁面出現如下圖，請輸入您先前即建立的帳號與密碼，然後按下**登入**。

附註：如果您尚未申請過帳號與密碼，您可以按此頁下方**“現在就建立一個帳號”**連結先建立個人的帳密，期間務必仔細閱讀使用者權利聲明，。

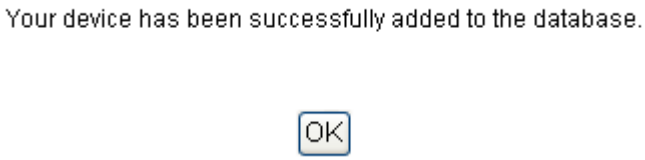
4. 按下登入後，將會出現如下的畫面，請按下**新增(Add)**。

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

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

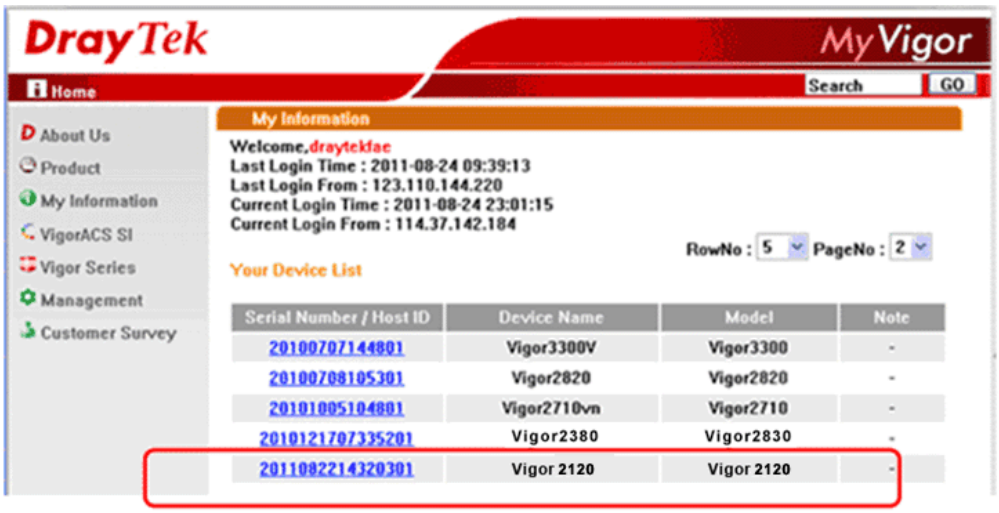


6. 下述頁面出現後，您的路由器資訊已經加入 MyVigor 的資料庫中。



7. 現在您已經完成產品註冊。

8. 按下確定**(OK)**，回到 **My Information** 網頁。看看 **My Information** 網頁，新增的路由器將會列在 **Your Device List** 清單中。



3 應用與練習

3.1 如何設定 IPv6 服務

面臨 IPv4 位址即將用罄的問題，各國紛紛開始推廣使用 IPv6，但爲了能持續利用 IPv4 上既有的豐富資源，IPv6 和 IPv4 網路必須藉由一些互通機制使二個世界的成員互相通訊，以分階段逐步完成 IPv4->IPv6 的移轉工作。目前常見的互通機制分爲三類：

- **雙堆疊(Dual Stack)**

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

- **建立通道(Tunnel)**

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

- **轉換(Translation)**

  讓僅支援 IPv4 的使用者，可以與僅支援 IPv6 的使用者互相通訊。

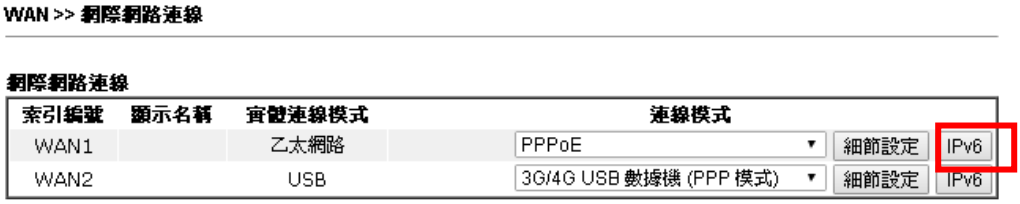
在開始進行 Vigor292 的設定之前，您必須知道您所申請的 IPv6 服務，是屬於哪種連線類型(Connection Type)。

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

I. 進行 WAN 設定

Vigor2120 的 IPv6 WAN 設定，共提供了 5 種連線類型：PPP、TSPC、AICCU、DHCPv6 Client 和 Static IPv6。

1. 進入 Vigor2120 的網頁設定介面，開啓 **WAN>>網際網路連線(WAN>> Internet Access)**，選擇一個 WAN 介面，選擇 **PPPoE** 作爲**連線模式**然後按下**細節設定**按鈕。按下 **IPv6** 按鈕。



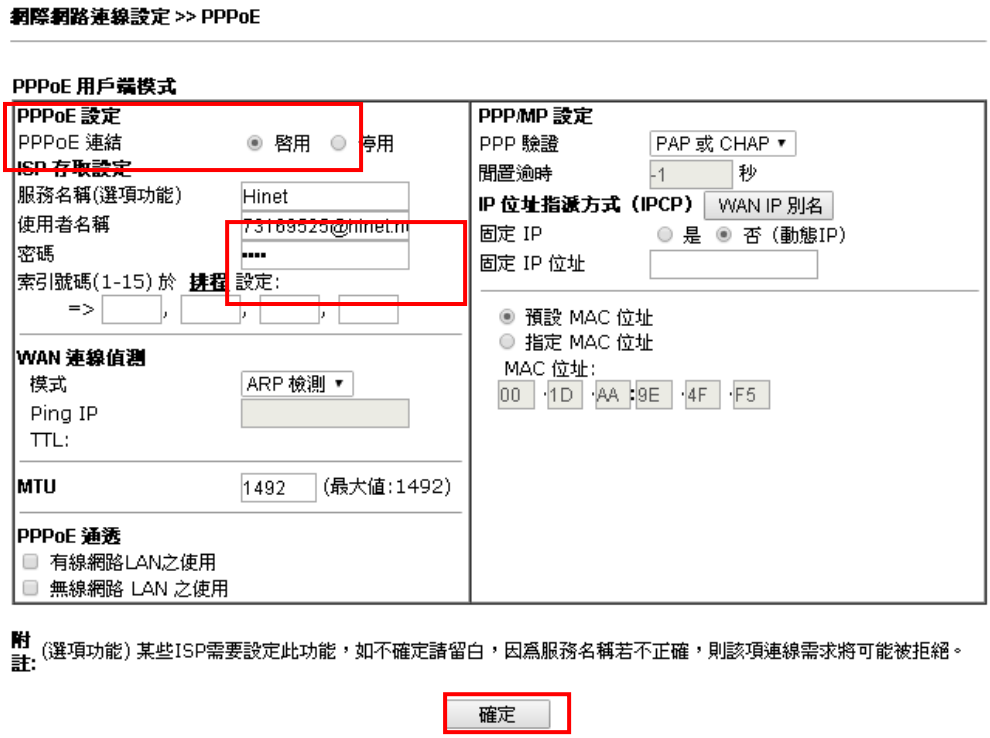
> **注意**：在同一時間裡，只有一個 WAN 介面可以使用 IPv6 功能。本例我們選擇 WAN2。

2. 在此頁面中，自下拉式清單選擇您所使用的連線類型。

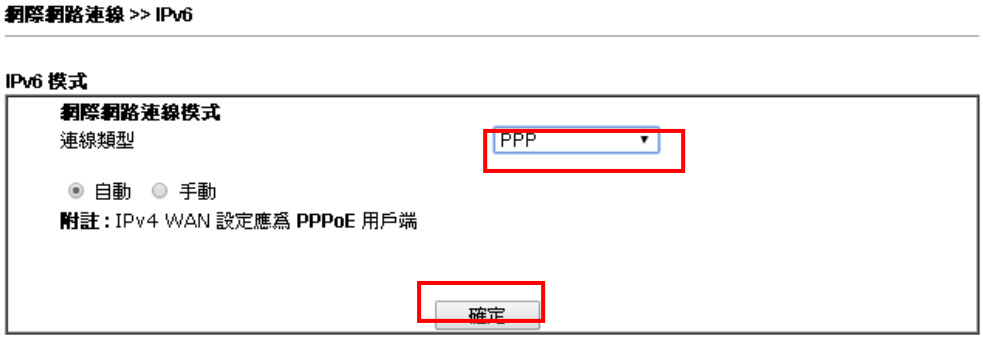
不同的連線類型可帶出不同的設定畫面，分述如下：

- **PPP -雙堆疊(Dual Stack)的應用，可同時使用 IPv4 與 IPv6 網路**

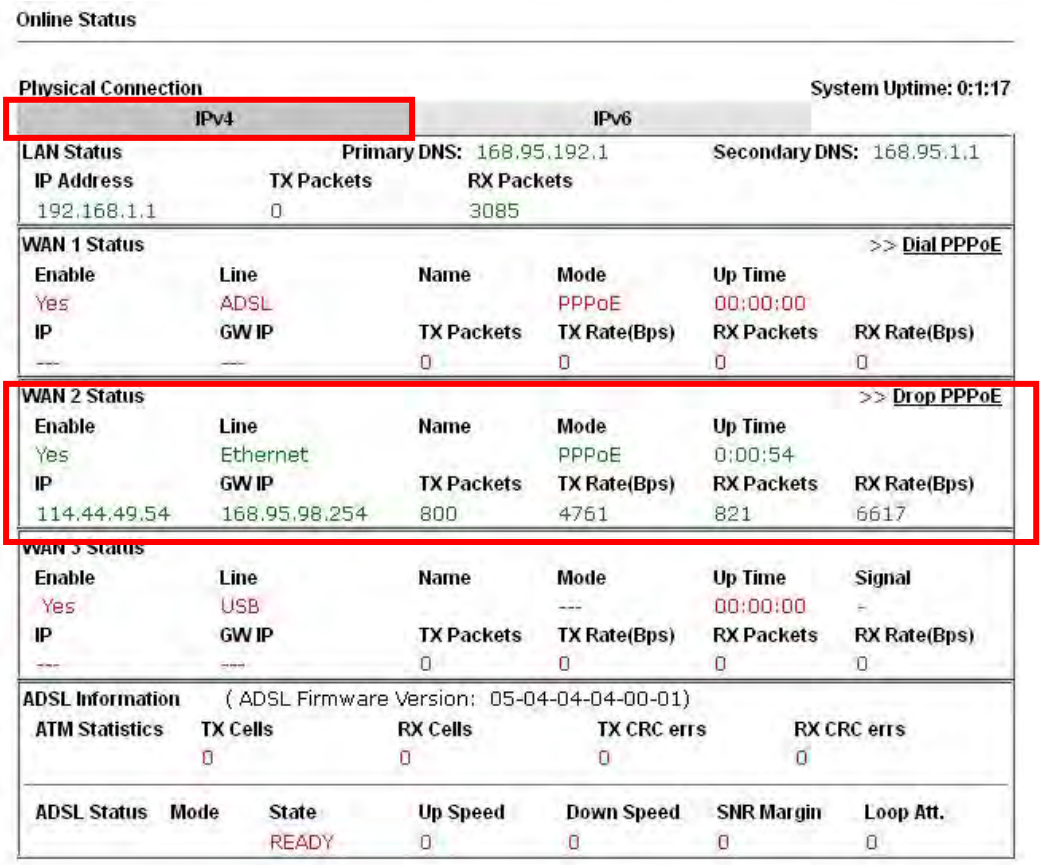
  選擇 PPP 並輸入 IPv4 PPPoE 的相關資訊。

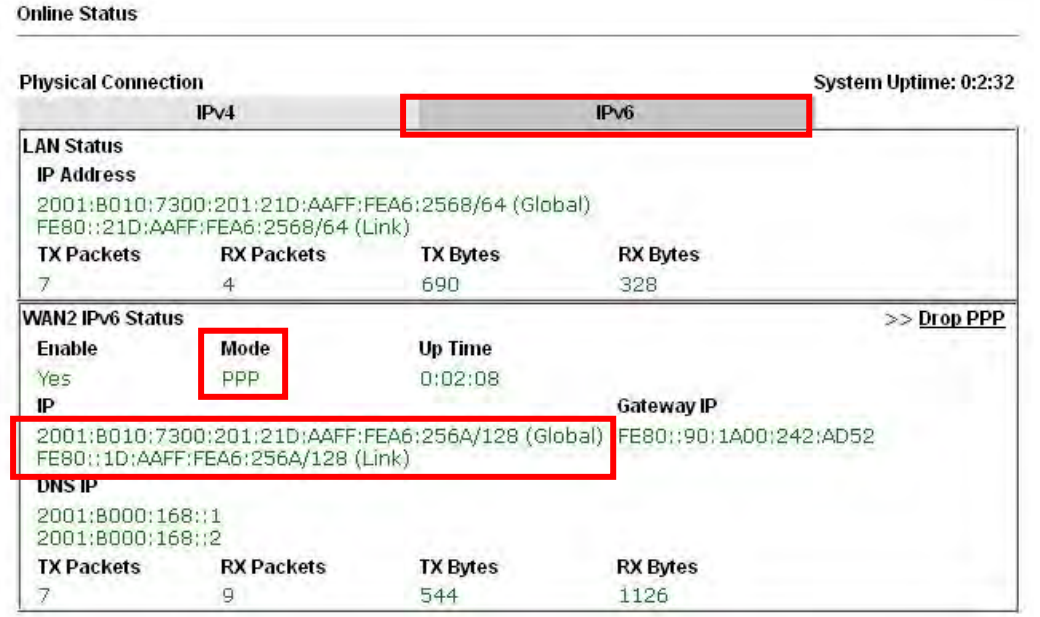


進入 IPv6 服務的設定頁面，您不需要進行任何設定。



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



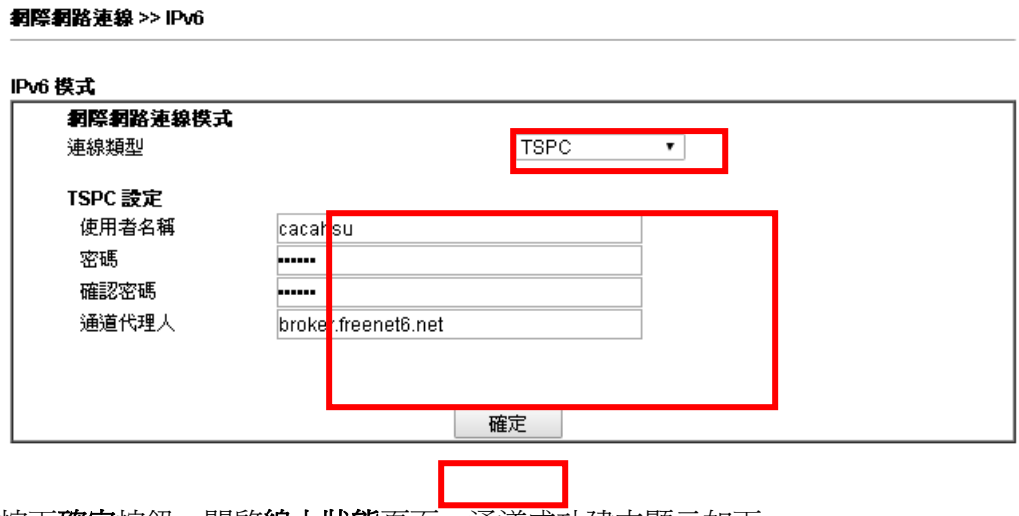


- **TSPC -通道(Tunnel)的應用，兩台 IPv6 主機透過現有 IPv4 網路環境進行通訊**

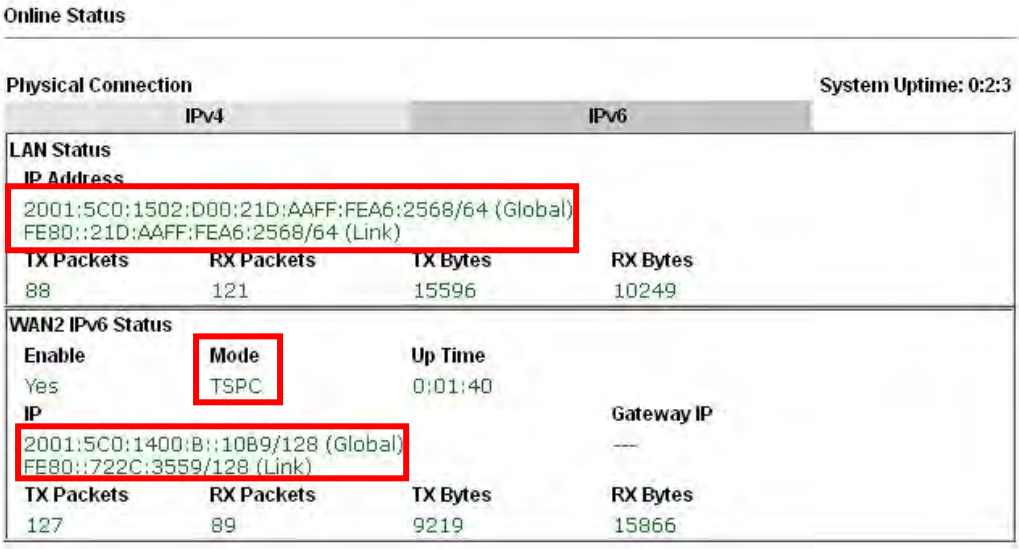
選擇 TSPC 類型，並輸入您所申請的 TSPC 服務資訊。

注意：使用此模式時，必須確認您的 IPv4 網路是連線的狀態。

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



按下**確定**按鈕，開啓**線上狀態**頁面，通道成功建立顯示如下。

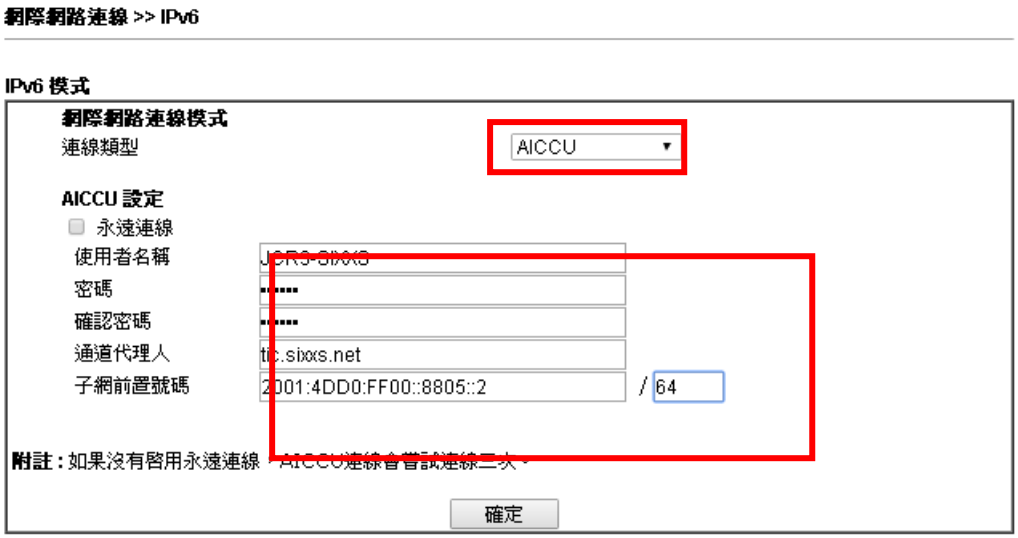


- **AICCU - 通道(Tunnel)的應用**

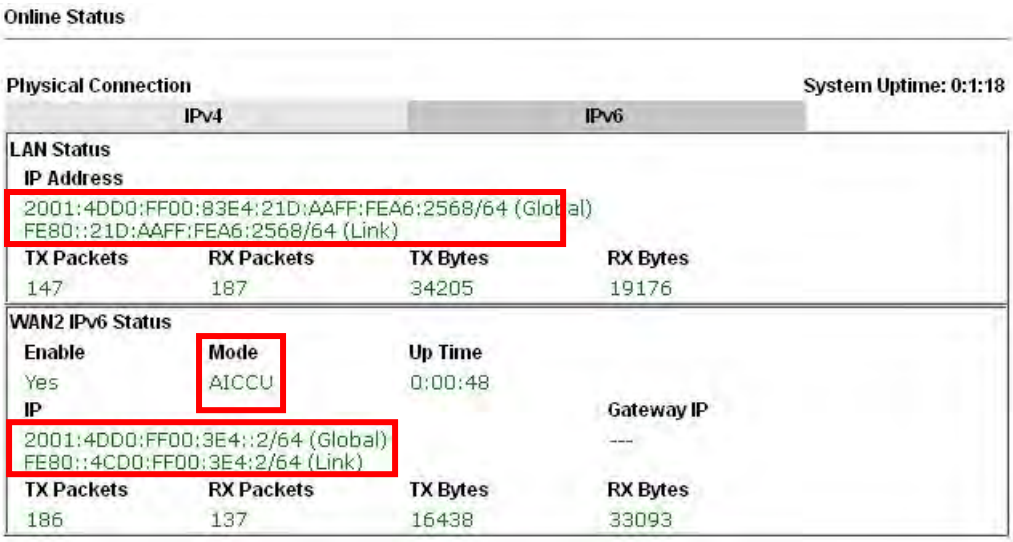
選擇 AICCU 類型，並輸入您所申請的 AICCU 服務資訊。

注意：使用此模式時，必須確認您的 IPv4 網路是連線的狀態。

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



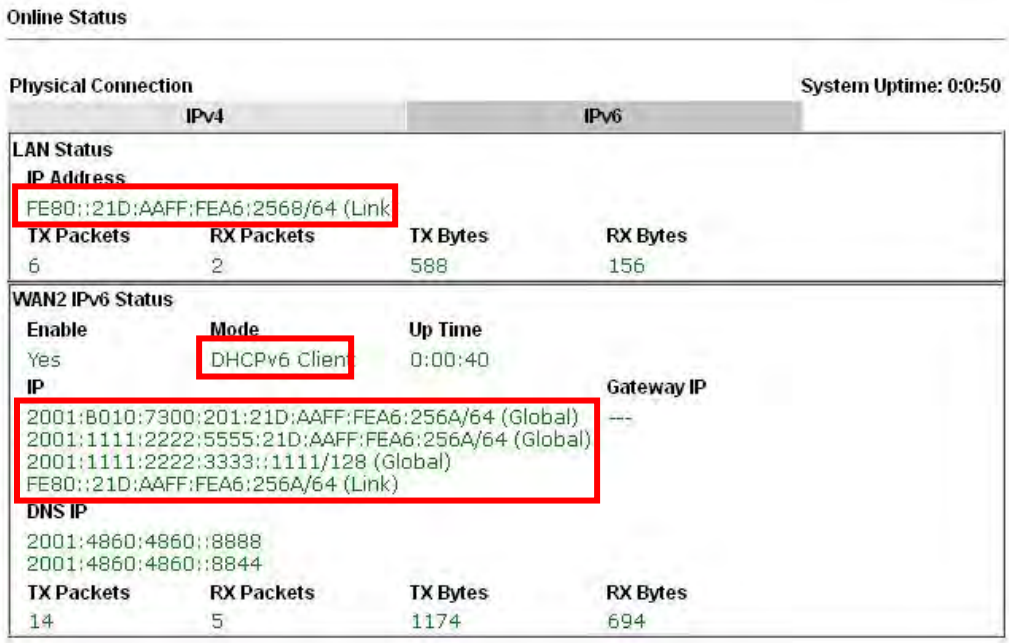
按下**確定**按鈕，開啓**線上狀態**頁面，通道成功建立顯示如下。



- **DHCPv6 用戶端**

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

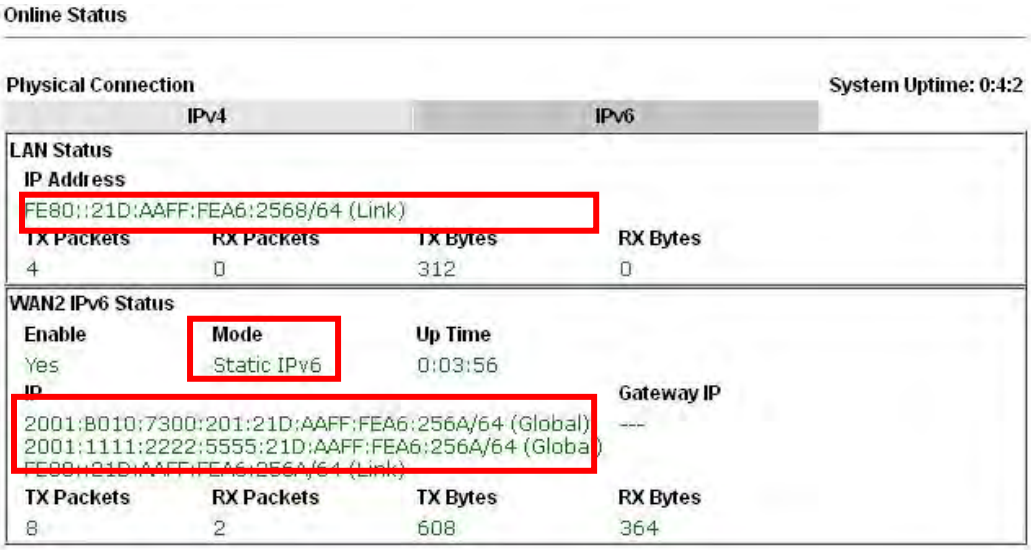
按下**確定**按鈕，開啓**線上狀態**頁面，通道成功建立顯示如下。



- **固定 IPv6**

選擇**固定 IPv6** 類型，並輸入 IPv6 位址、前置號碼長度和閘道位址。

按下**確定**按鈕，開啓**連線狀態**頁面，通道成功建立顯示如下：



II. 進行 LAN 設定

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

1. 進入 Vigor2120 的網頁設定介面，開啓**區域網路>>基本設定(LAN>>General Setup)**，按下 **IPv6** 按鈕，開啓如下畫面。

> **注意**：只有 LAN1 子網支援 IPv6。

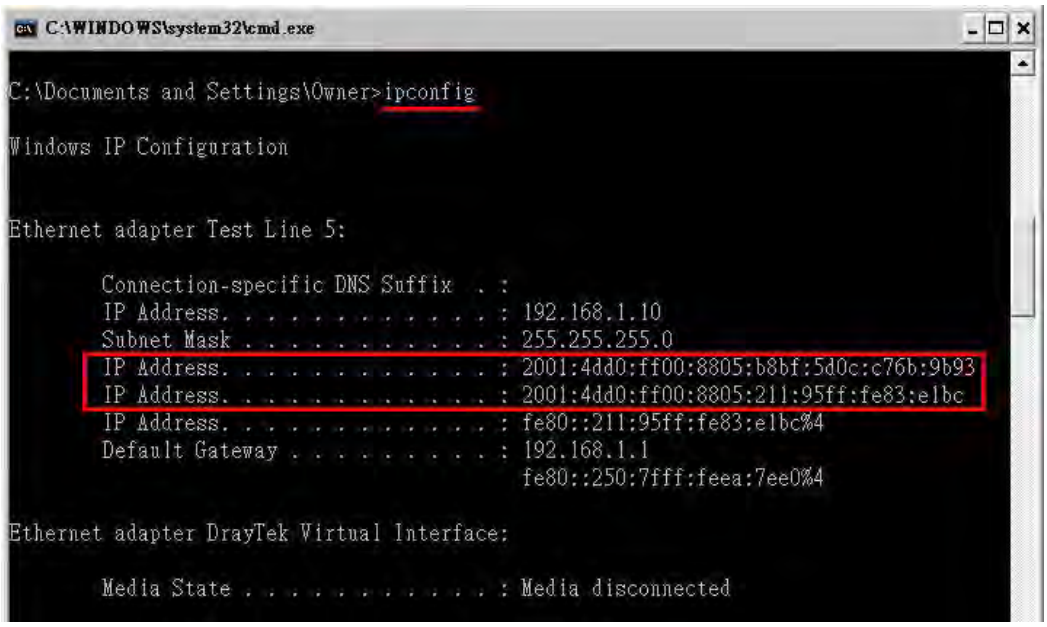
2. 在 **RADVD 設定(Router Advertisement Server)**區域中，預設值是**啓用**的，用戶端的電腦將會自動要求 RADVD 服務所需的 IPv6 位址的前置號碼長度，並產生一組介面 ID 以便組合完整的 IPv6 位址。

3. 在 **DHCPv6 伺服器設定(DHCPv6 Server)**區域中，當啓用 DHCPv6 服務時，您可以在此自行指定可用的 IPv6 位址。

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

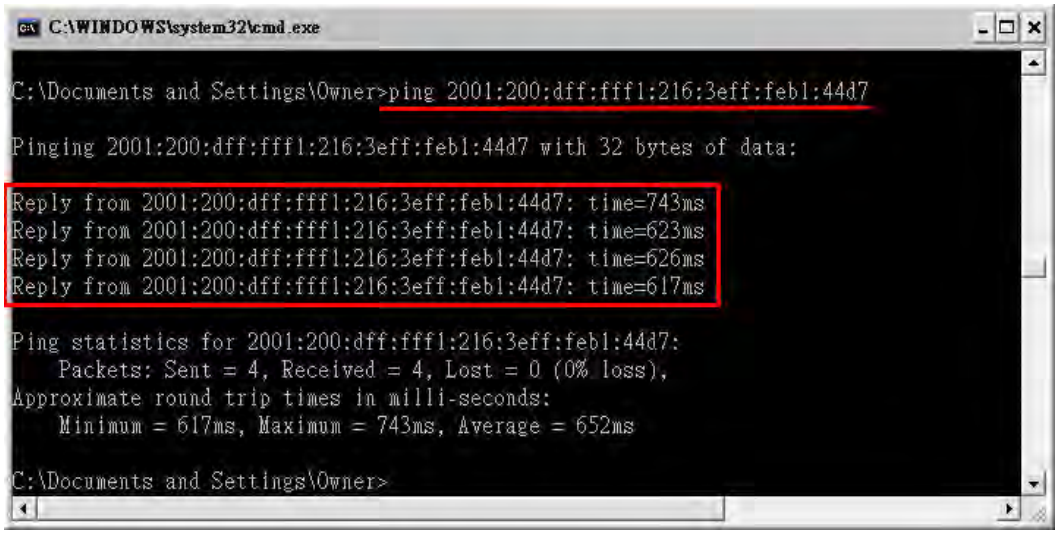
III. 確認 IPv6 服務可成功運作

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



從上圖中，我們可以看到系統偵測到的 IPv6 位址。

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



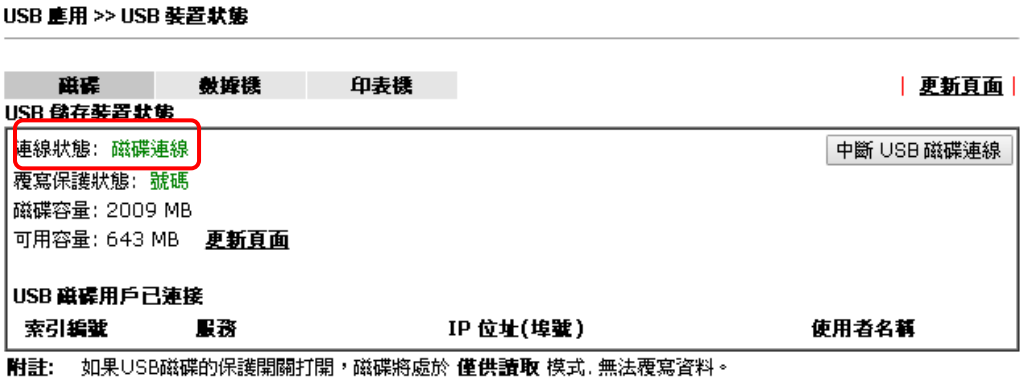
在您看到如上的訊息之後，即表示 IPv6 服務已經成功啓動了。

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

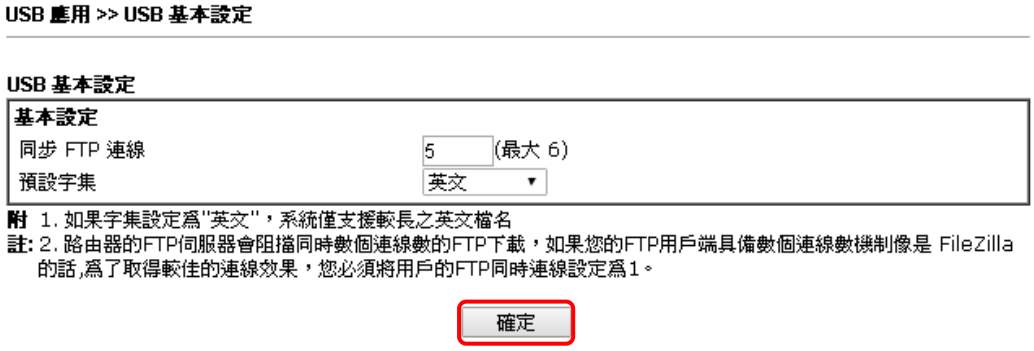
如果您在畫面上確實看到跳舞的小烏龜，就表示 IPv6 服務已經準備妥當，可供您存取使用。

3.2 如何取得連接至 Vigor 路由器的 USB 裝置內的檔案?

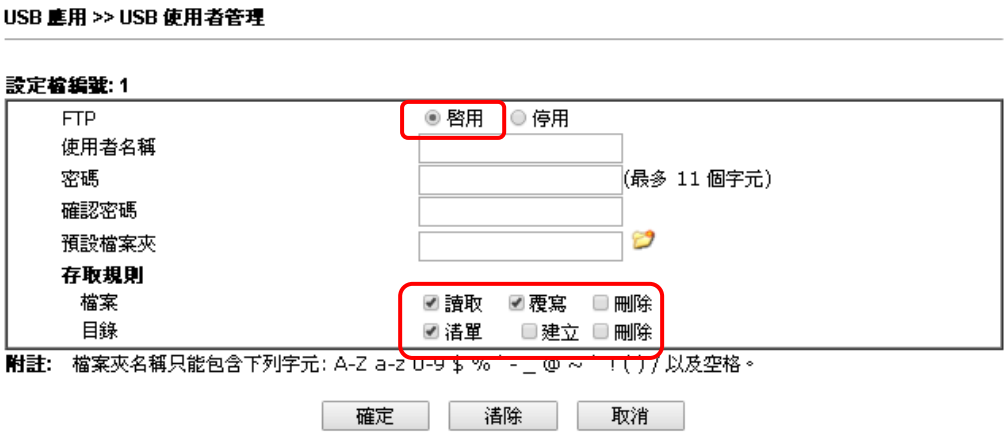
1. 將 USB 裝置連接至路由器的 USB 埠口，務必確認連線狀態欄位中出現**磁碟連線(Disk Connected)**的訊息，如下所示：



2. 開啓 **USB 應用>>USB 基本設定(USB Application>>USB General Settings)**以檢查一般設定，按下**確定(OK)**。

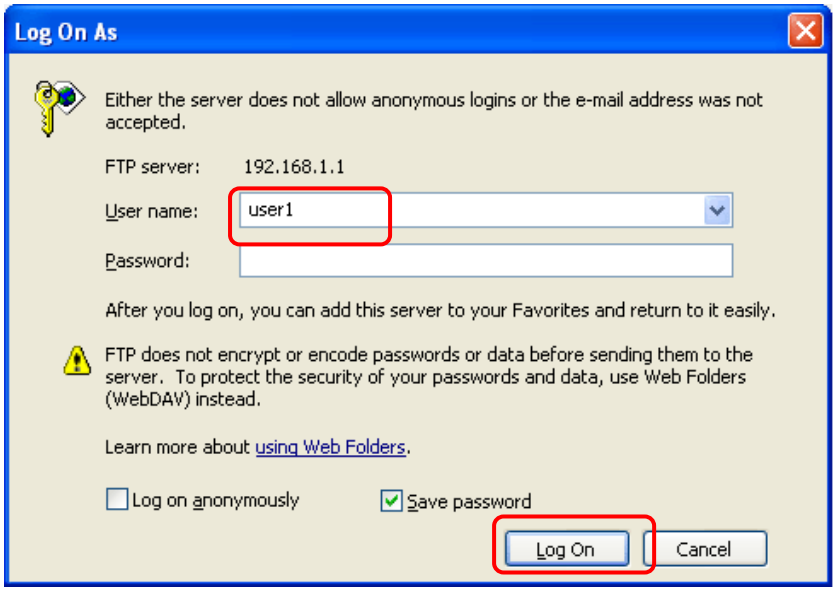


3. 在**USB 應用>>USB 使用者管理(USB Application >>USB User Management)**設定一組使用 FTP 服務的使用者帳號，按下**啓用**以便啓動此 FTP 使用者帳號，此例我們新增一個名爲 user1 的帳號，給予讀取、覆寫、清單的權限。

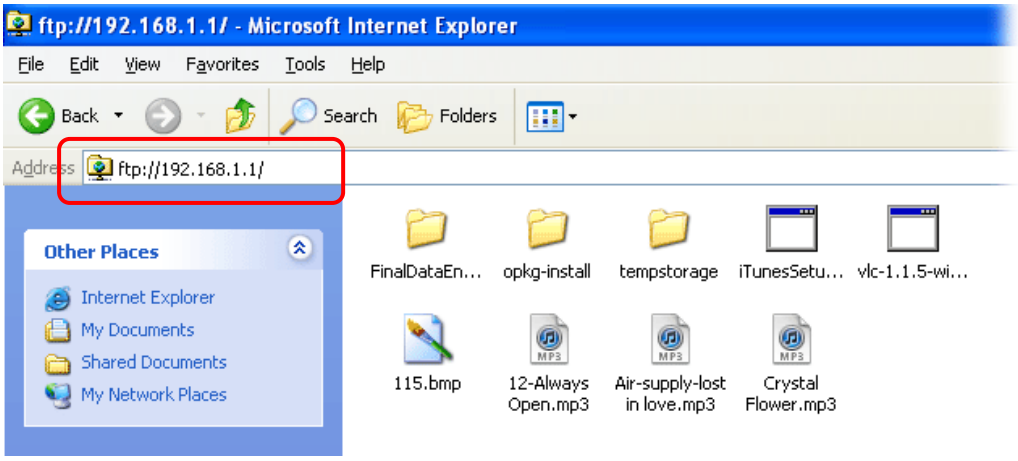


4. 按下**確定(OK)**按鈕儲存設定。

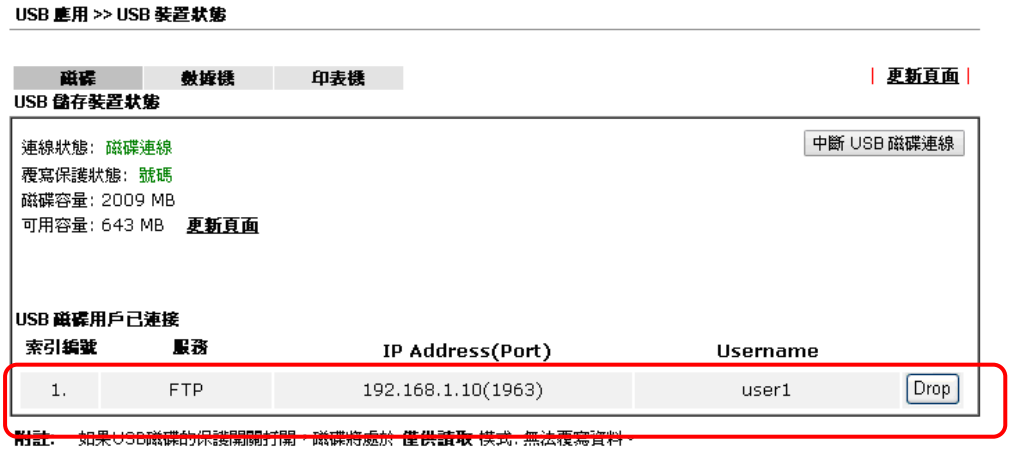
5. 確認 FTP 服務可以順利運作，請開啓任一瀏覽器並鍵入 *ftp://192.168.1.1*。使用帳號 **user1** 來登入。



6. 當下列視窗出現時，即表示 FTP 服務可正常運作。



7. 回到 **USB 應用>>USB 磁碟狀態(USB Application >> USB Disk Status)**，FTP 伺服器資訊將會顯示如下圖：



現在，路由器 LAN 端的使用者可以存取 USB 裝置內容，只要在瀏覽器輸入 ftp://192.168.1.1 即可，使用者可以新增或移除檔案/目錄，相關權限視 **USB 應用>>USB 使用者管理(USB Application >>USB User Management)**中對於 FTP 帳戶設定所做的存取規則而定。

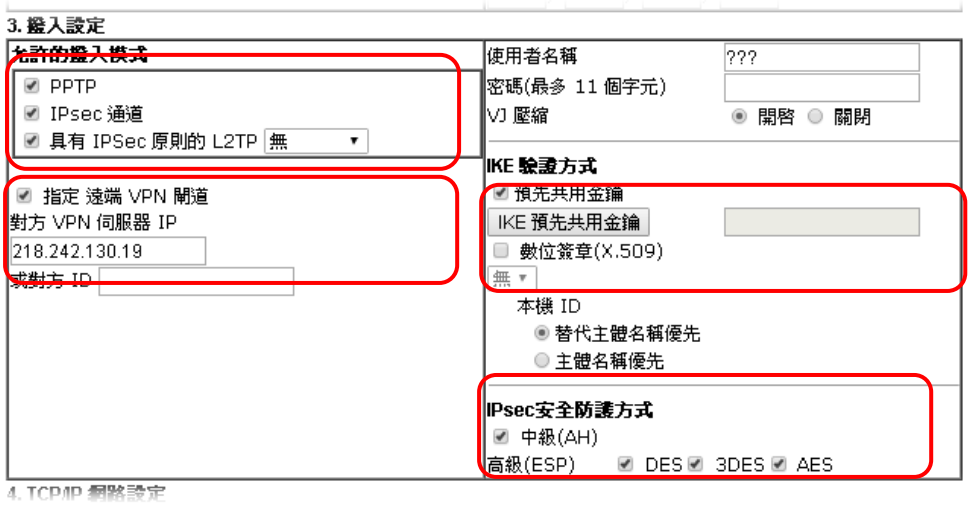
3.3 如何在總公司與遠端分公司建立 LAN-to-LAN VPN 連線通道(透過 Main 模式)

總公司的 Vigor 路由器設定

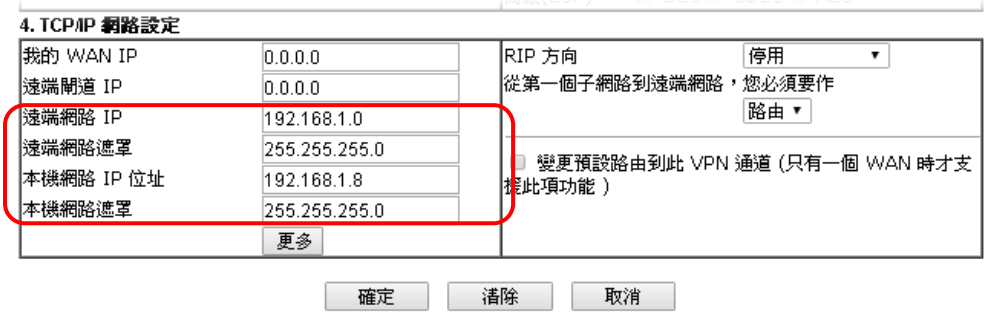
1. 登入路由器的使用者介面。
2. 開啓 **VPN 與遠端存取>>LAN to LAN (VPN and Remote Access>>LAN to LAN)** 建立一個設定檔。

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

4. 現在往下瀏覽設定頁面，在**撥入設定(Dial-In Settings)**中，勾選 PPTP、IPsec 通道以及 L2TP，勾選**指定遠端 VPN 閘道(Specify Remote…)**，然後輸入對方 VPN 伺服器 IP 位址(例如本例使用的 218.242.130.19)，按下 **IKE 預先共用金鑰(IKE Pre-Shared Key)**按鈕設定金鑰 PSK 再勾選**中級(AH)**或是**高級(ESP)**安全防護方式。

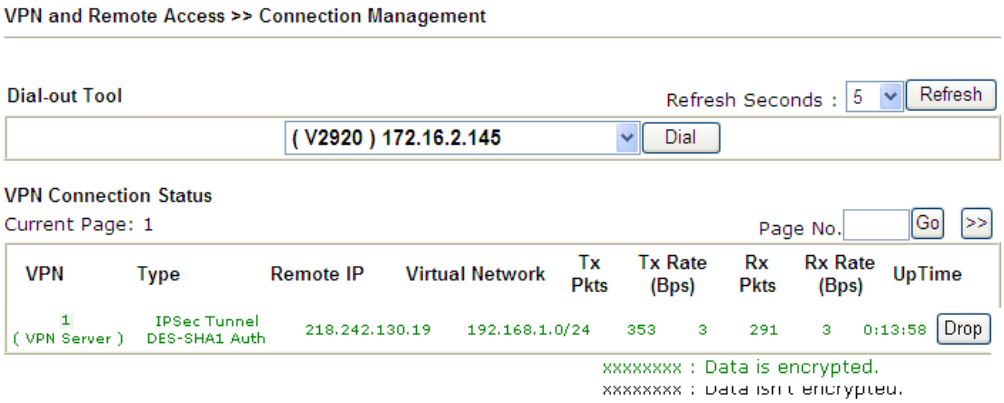


5. 繼續往下瀏覽設定頁面至 **TCP/IP 網路設定(TCP/IP Network Settings)**區域，設定遠端的 LAN IP 位址。



6. 按下**確定(OK)**儲存。

7. 開啓 **VPN 與遠端存取>>連線管理(VPN and Remote Access>>Connection Management)**檢查撥入連線的狀態(資料來自分公司)。



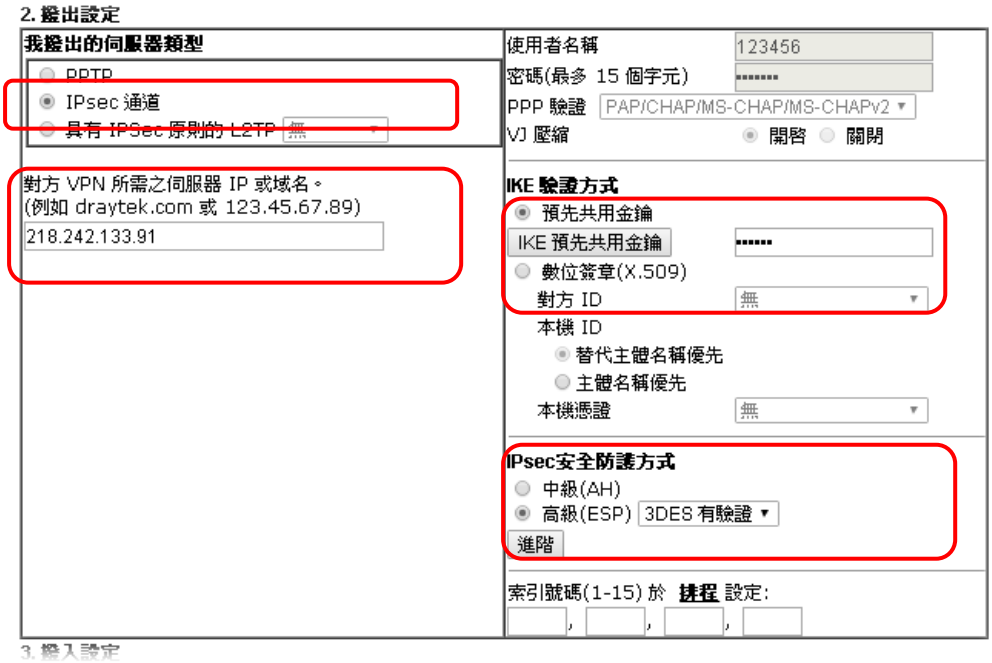
分公司的 Vigor 路由器設定

1. 登入路由器的使用者介面。

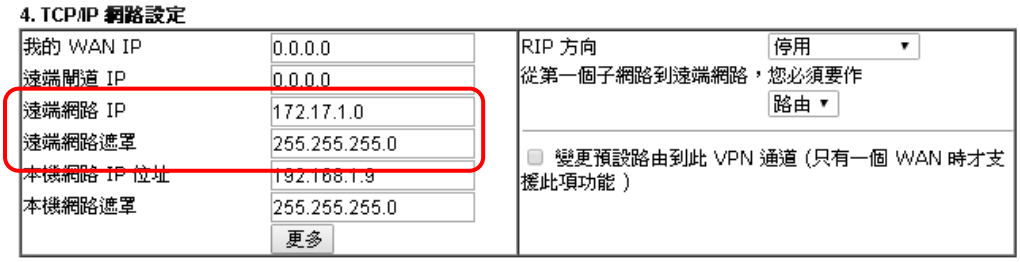
2. 開啓 **VPN 與遠端存取>>LAN to LAN (VPN and Remote Access>>LAN to LAN)** 建立一個設定檔。

3. 按下任何一個索引編號開啓設定頁面。輸入容易辨識的檔案名稱(本例我們使用 VPN Client)然後勾選**啓用此設定檔(Enable This Profile)**方塊。由於路由器準備被視爲用戶端，因此撥號方向應設定爲**撥出(Dial-out)**並勾選**永遠連線(Always on)**。

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

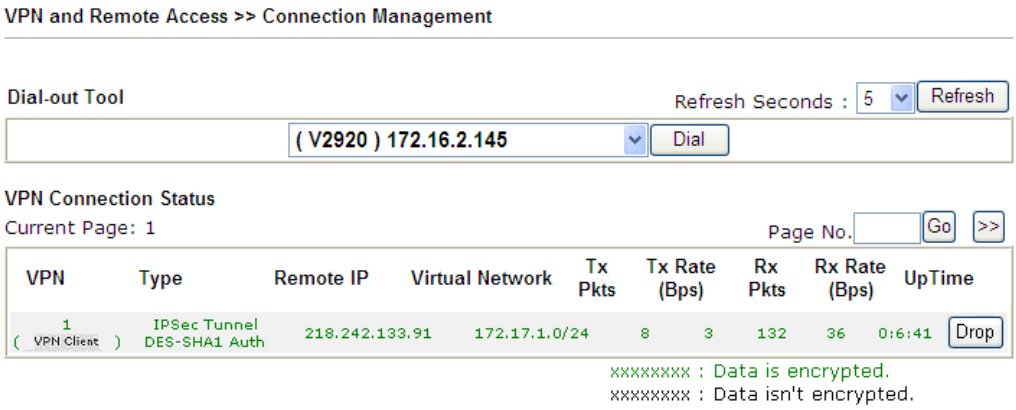


5. 繼續往下瀏覽設定頁面至 **TCP/IP 網路設定(TCP/IP Network Settings)**區域，設定遠端的 LAN IP 位址。



6. 按下**確定(OK)**儲存。

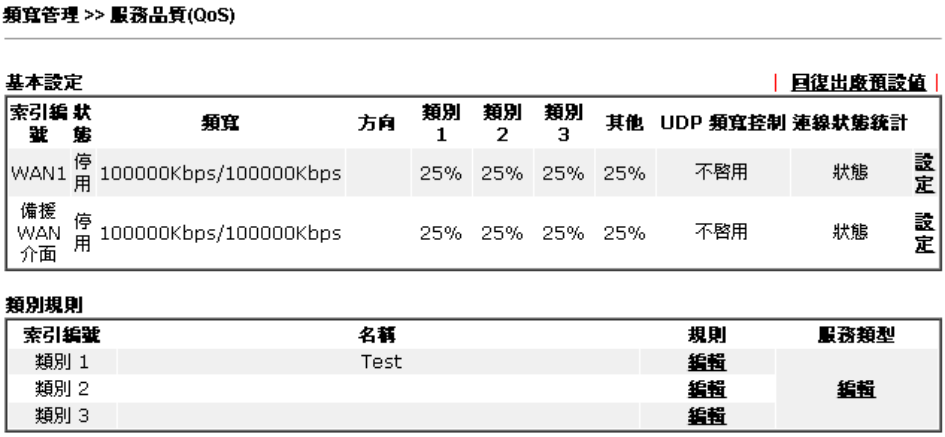
7. 開啓 **VPN 與遠端存取>>連線管理(VPN and Remote Access>>Connection Management)**檢查撥入連線的狀態(資料來自總公司)。



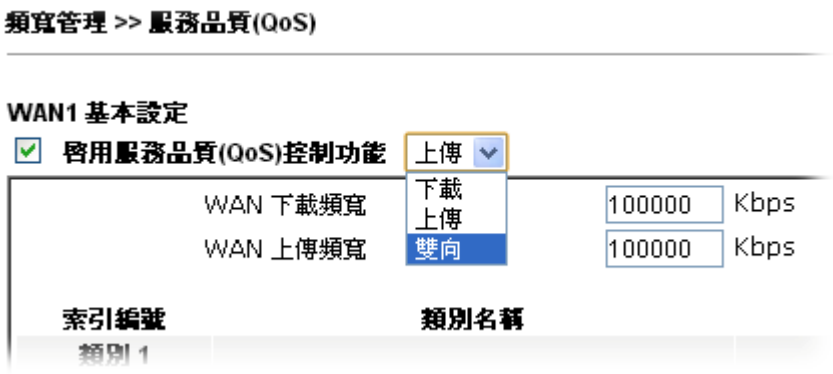
3.4 QoS 設定範例

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

1. 進入**頻寬管理**之**服務品質(Bandwidth Management>> Quality of Servic)**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。



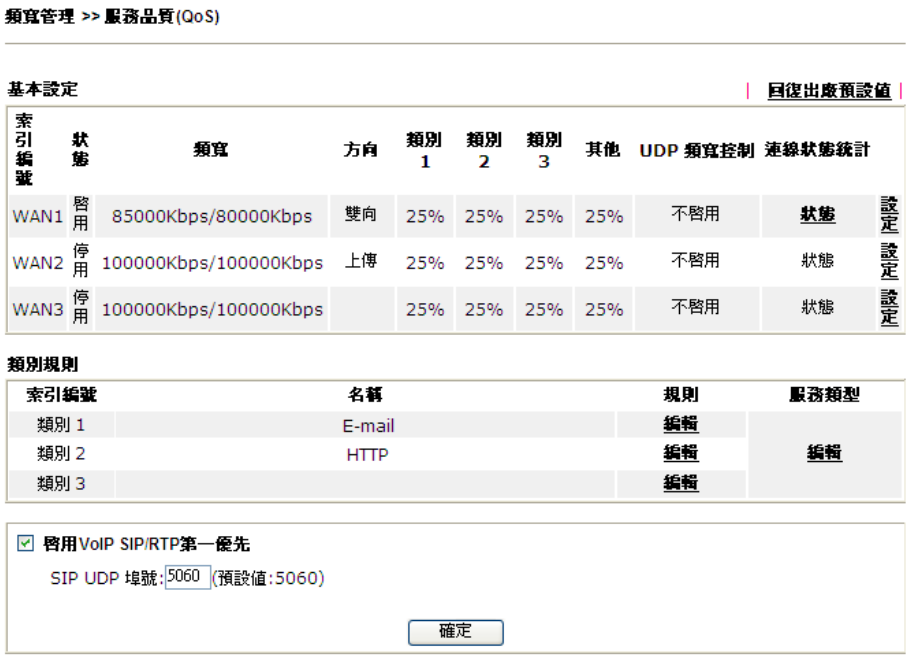
3. 設定下載/上傳頻寬。

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**。

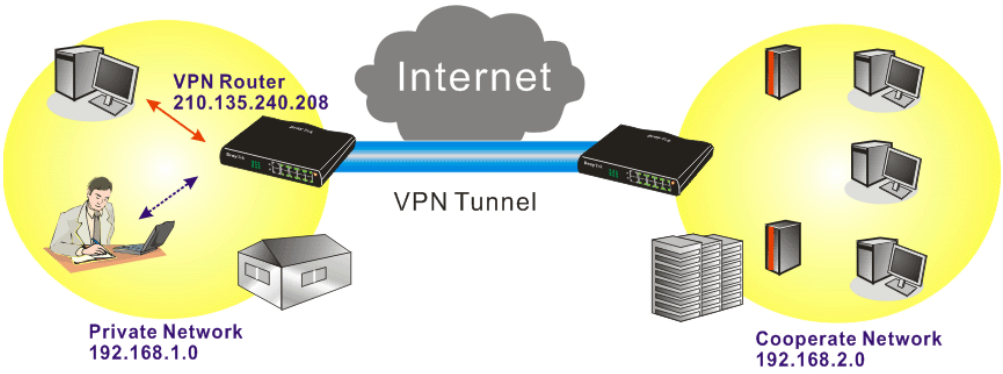
5. 使用者可設定保留頻寬(例如 25%) 給予透過POP3 和SMTP通訊協定來傳送的電子郵件。參考下圖。

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**。於此類別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。



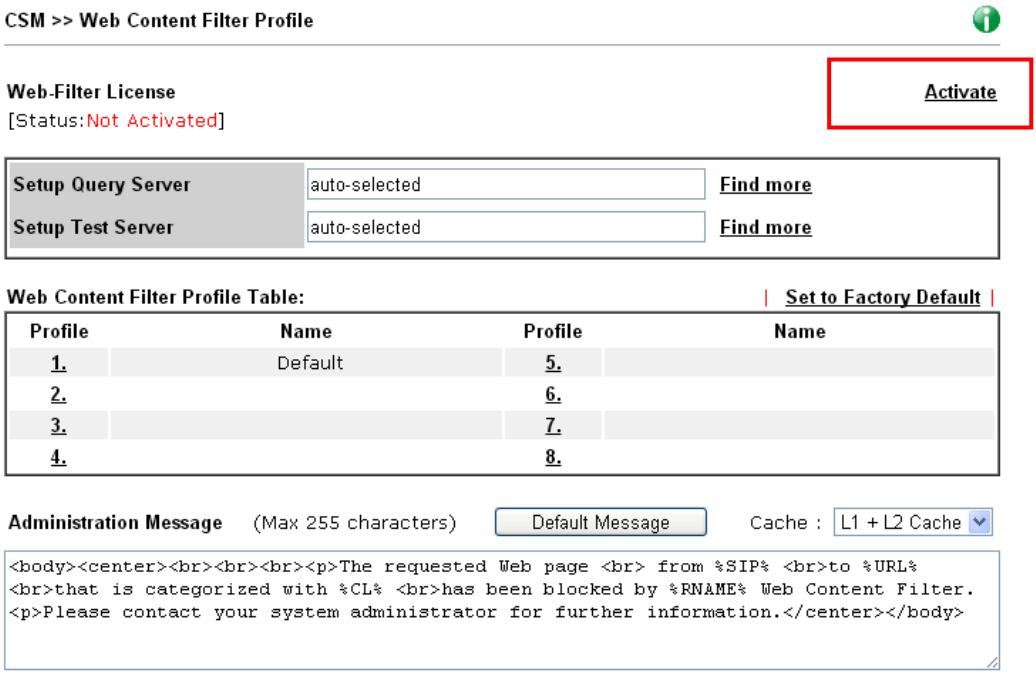
3.5 如何建立一個 MyVigor 帳號

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

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

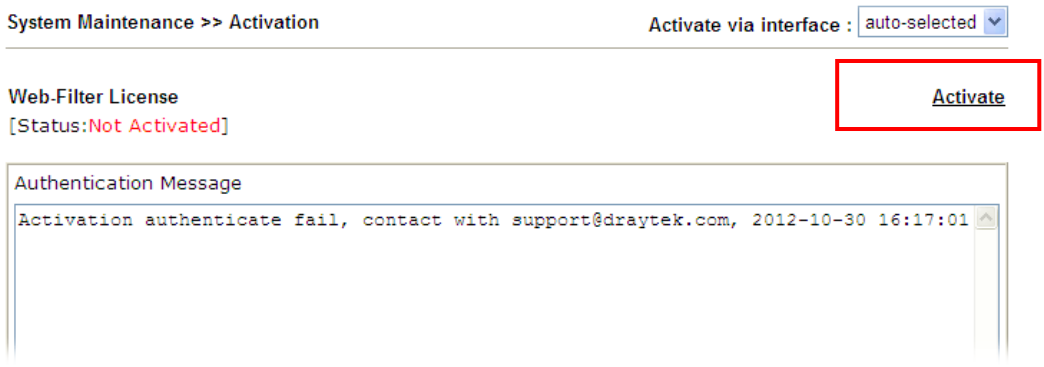
3.5.1 透過 Vigor 路由器來建立

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



或是

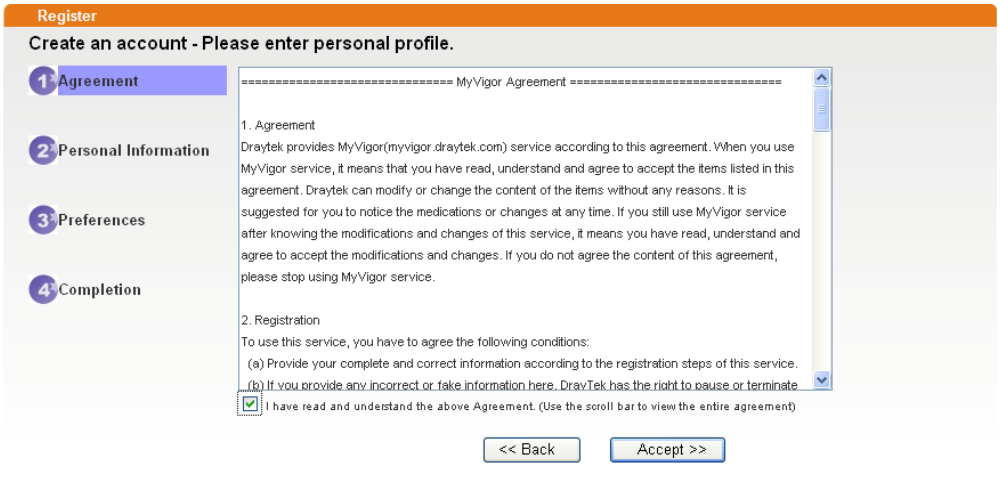
開啓**系統維護>>開啓授權碼(System Maintenance>>Activation)**



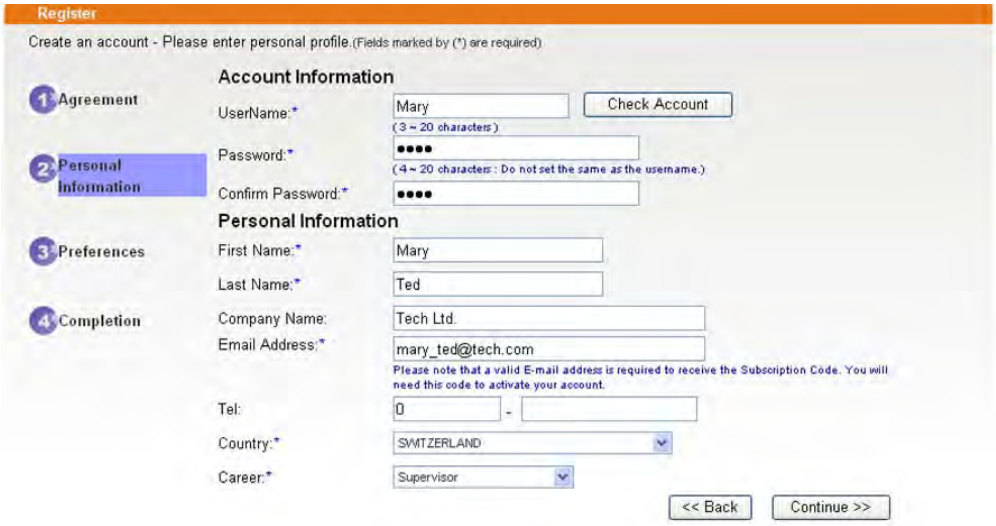
2. 按下**啓動(Activate)**連結，MyVigor 登入視窗將會自動跳出。

3. 按下 **Create an account now** 連結。

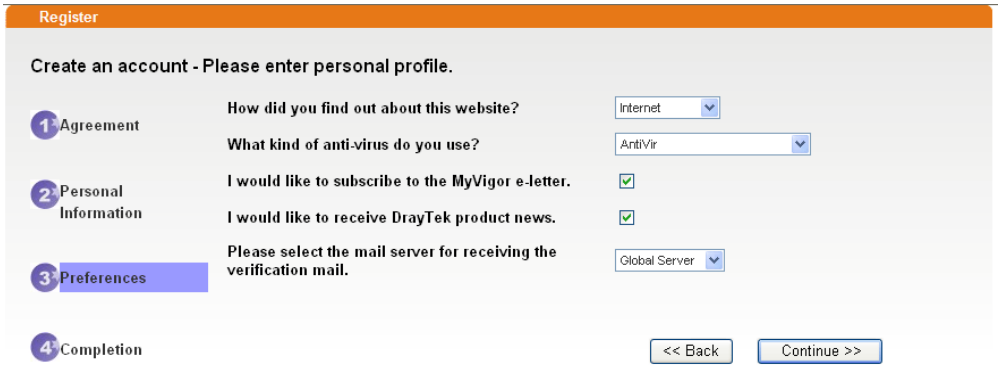
4. 確認您已同意畫面上的聲明並勾選同意方塊，接著按下 **Accept**。



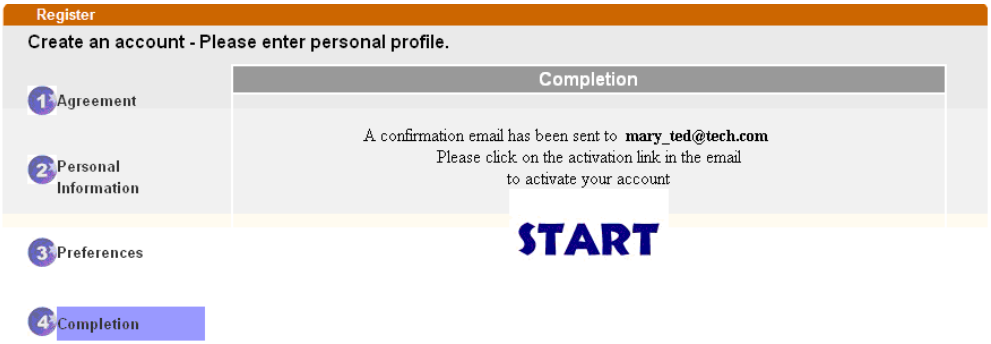
5. 輸入個人資訊並按下 **Continue**。



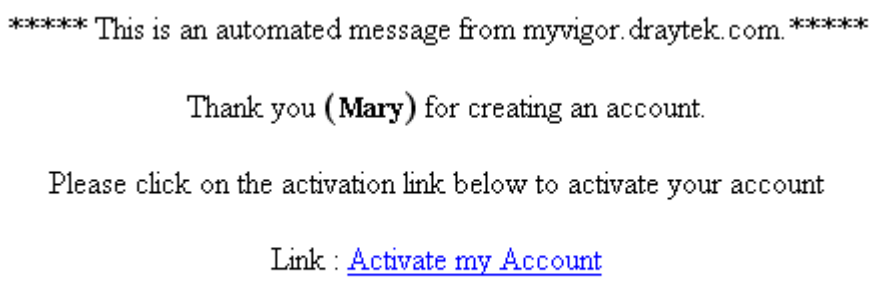
6. 選擇適合您的電腦的選項，再按下 **Continue**。



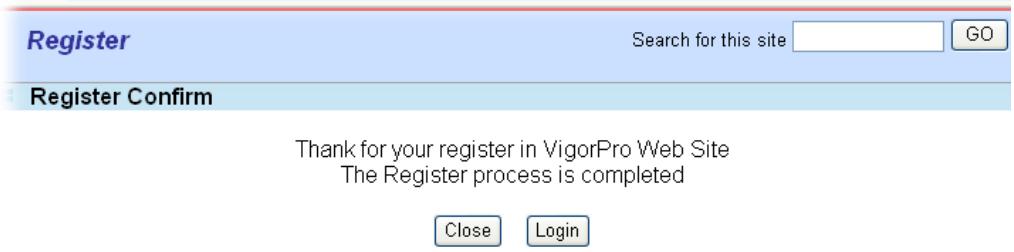
7. 現在您已經成功建立一個帳號了，請按 **START**。



8. 請先去信箱查看郵件，是否收到標題爲 **New Account Confirmation Letter from myvigor.draytek.com** 的信件。



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

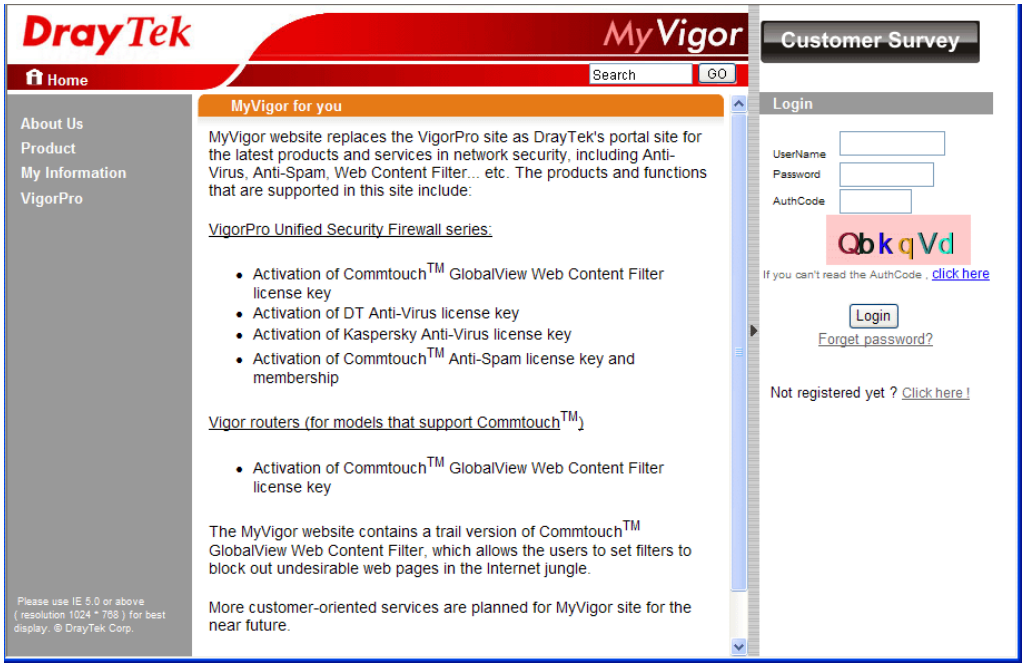


10. 當您看看如下頁面時，請輸入帳號與密碼(您剛剛在前述步驟中建立)。

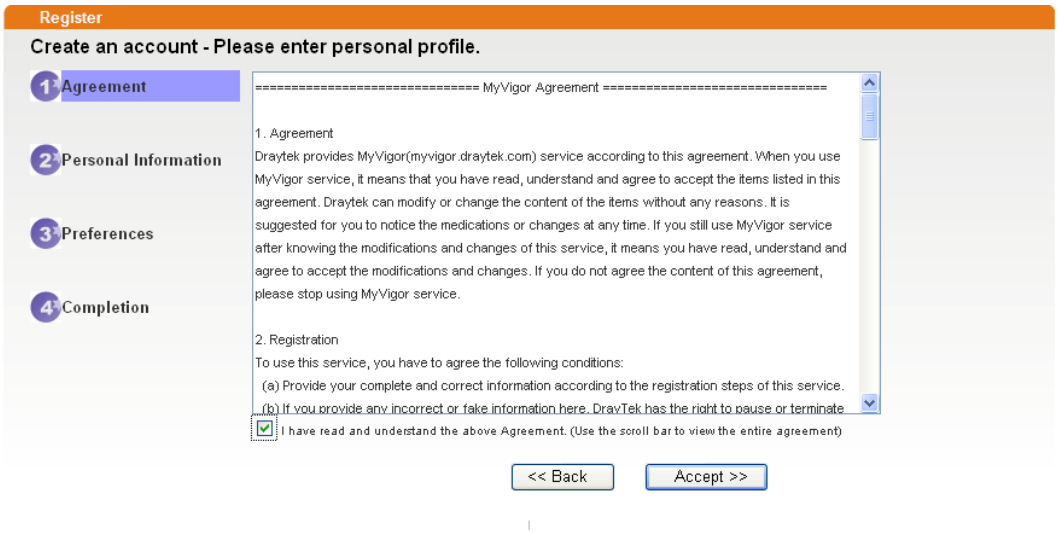
11. 輸入驗證碼之後，按下 Login。系統將帶您進入 MyVigor 伺服器。

3.5.2 透過 MyVigor 網站來建立

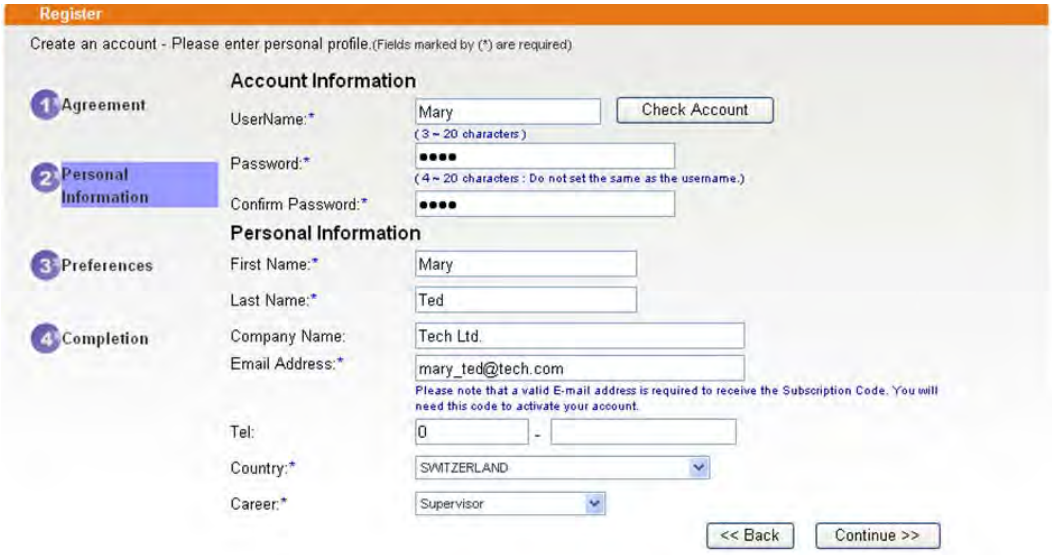
1. 登入 http://myvigor.draytek.com，找到 **Not registered yet?** 這行之後，按下旁邊的 **Click here!** 連結進入下一個畫面。



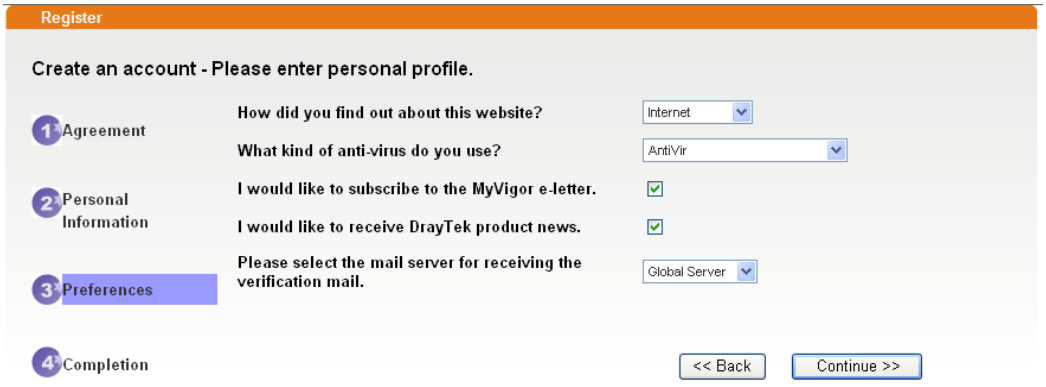
2. 確認您已同意畫面上的聲明並勾選同意方塊，接著按下 **Accept**。



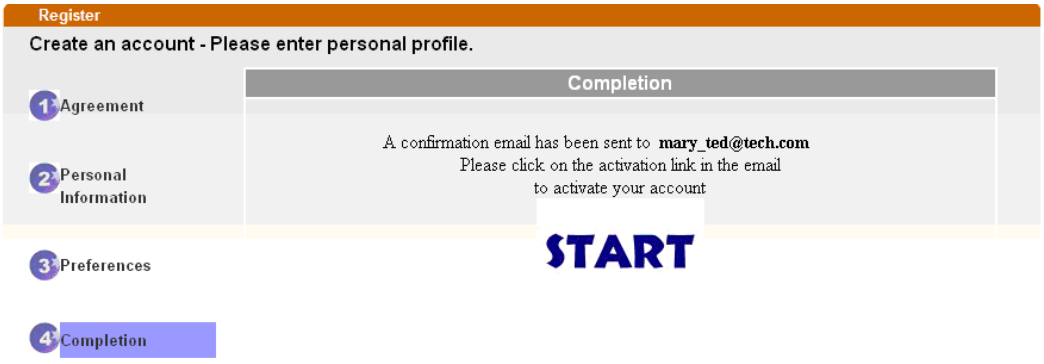
3. 輸入個人資訊並按下 **Continue**。



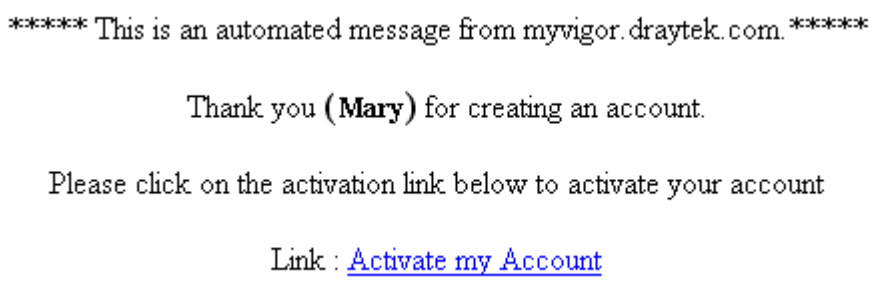
4. 選擇適合您的電腦的選項，再按下 **Continue**。



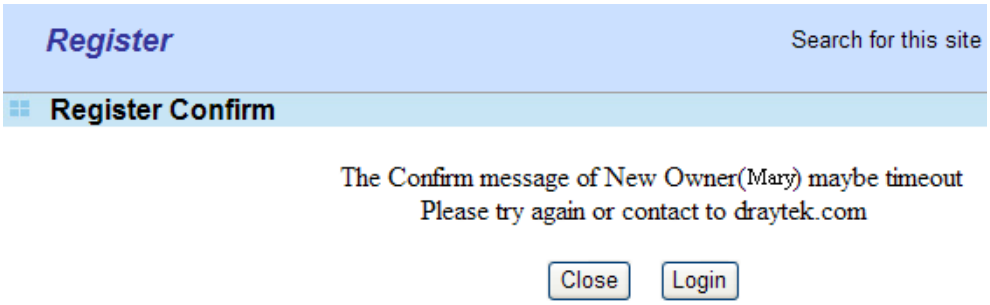
5. 現在您已經成功建立一個帳號了，請按 **START**。



6. 請先去信箱查看郵件，是否收到標題爲 **New Account Confirmation Letter from myvigor.draytek.com** 的信件。



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



8. 當您看看如下頁面時，請輸入帳號與密碼(您剛剛在前述步驟中建立)。

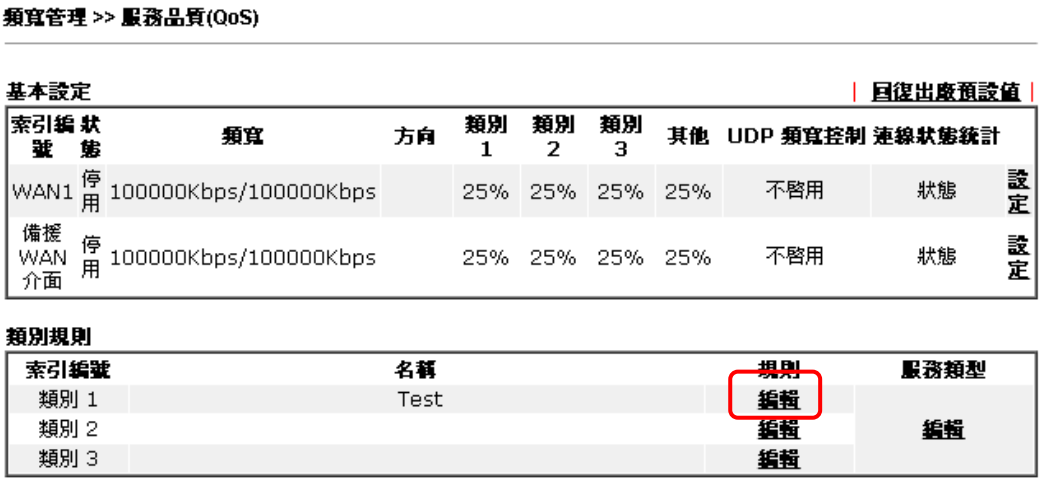
輸入驗證碼之後，按下 Login。系統將帶您進入 MyVigor 伺服器。

3.6 如何利用 QoS 來最佳化頻寬管理

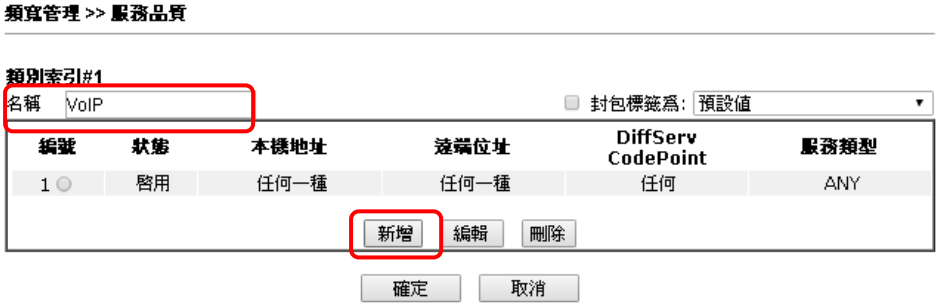
您是否有過上傳/下載檔案(聲音、影像或是電子郵件、資料等等)時受到網際網路連線的頻寬限制或頻寬過窄的問題? Vigor 路由器進階版的 QoS 技術可幫助您依據實際需要分派不同比例的頻寬於不同的用途上。

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

1. 開啓**頻寬管理>>服務品質(Bandwidth Management>> Quality of Service)** 。
2. 看到如下頁面之後，請按**類別 1** 的**編輯(Edit)**按鈕。

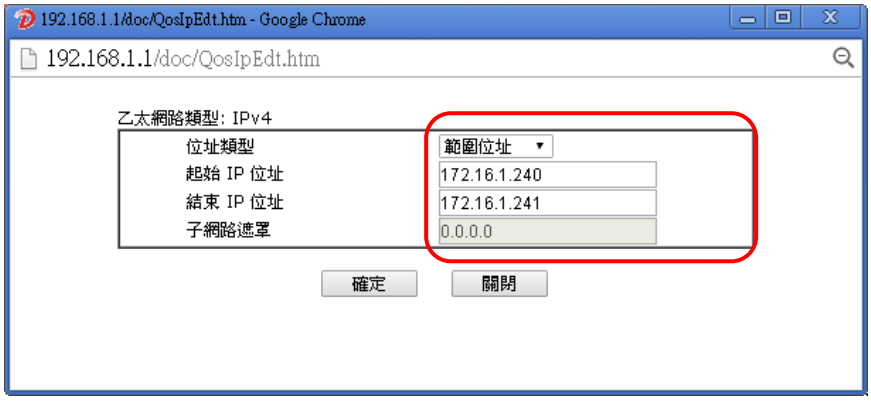


3. 在**名稱**欄位請輸入 VoIP，然後按下**新增(Add)**按鈕。



4. 勾選**啓用(ACT)**方塊，在本機地址欄位中按下**編輯(Edit)**按鈕。

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

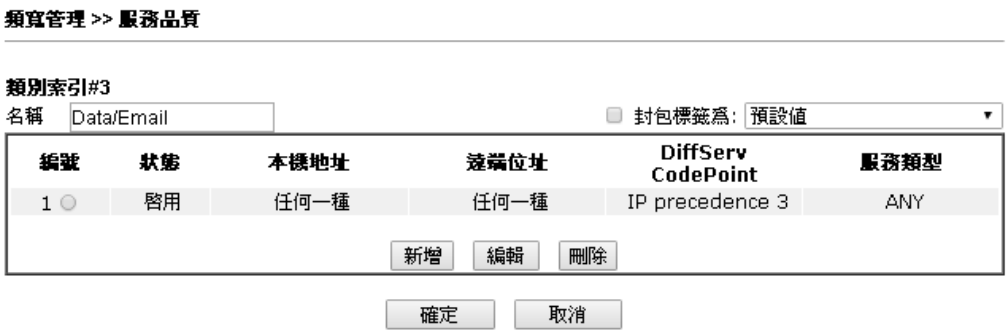


6. 再次按下**確定(OK)**儲存設定。

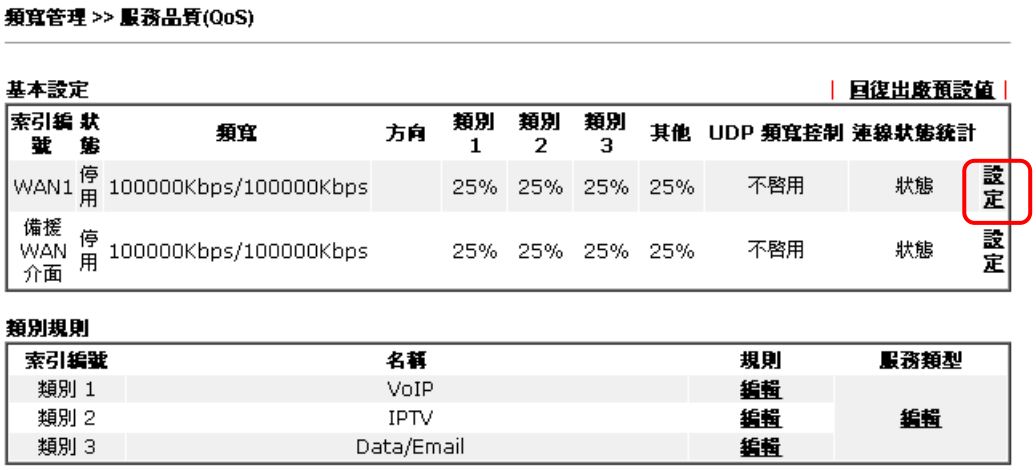
7. VoIP 類別規則已經設定完畢，按下**確定(OK)**回到前一個頁面。

8. 採取同樣的步驟分別再設定 IPTV 與資料/電子郵件傳輸的類別內容。

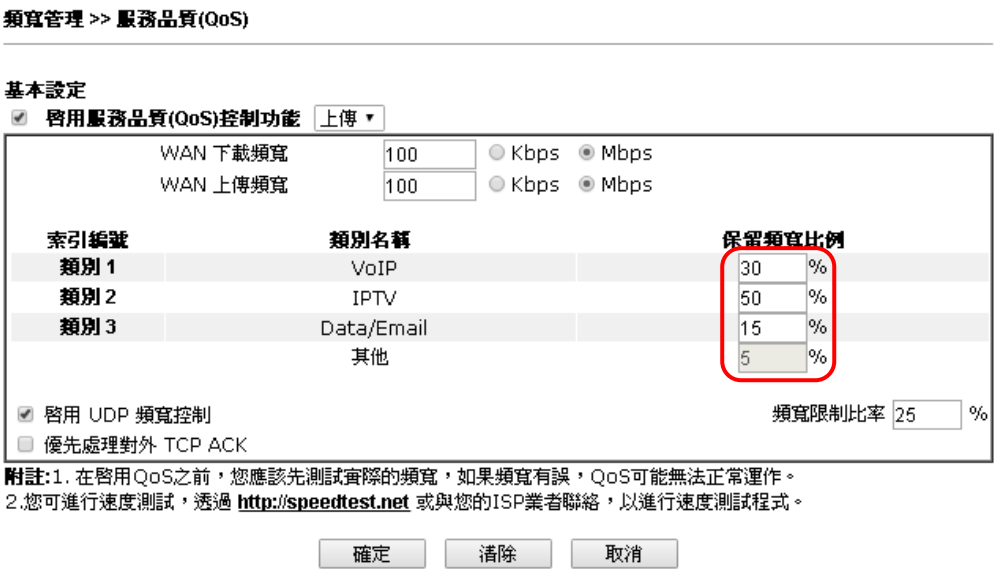
以及



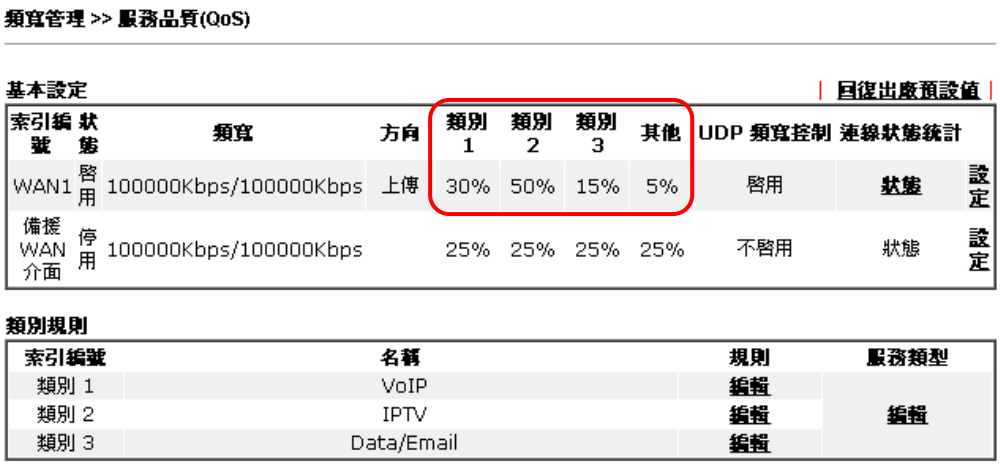
9. 假使您的網路連線有 2MB/512Kb，您可以按下 WAN1 的**設定(Setup)**連結來設定上述不同群組的個別頻寬。



10. 在設定頁面上，勾選**啓用服務品質控制功能(Enable the QoS Control)**方塊，三個類別中分別輸入 30, 50 與 15 等比例，如下圖所示。記得勾選**啓用 UDP 頻寬控制(nable UDP Bandwidth Control)**。



11. 按下**確定(OK)**儲存，WAN1 的類別設定定義將呈現如下：



頻寬管理 >> 服務品質(QoS)

基本設定 | 回復出廠預設值 |

索引編號	狀態	頻寬	方向	類別 1	類別 2	類別 3	其他	UDP 頻寬控制	連線狀態統計	
WAN1	啓用	100000Kbps/100000Kbps	上傳	30%	50%	15%	5%	啓用	狀態	設定
備援 WAN 介面	停用	100000Kbps/100000Kbps		25%	25%	25%	25%	不啓用	狀態	設定

類別規則

索引編號	名稱	規則	服務類型
類別 1	VoIP	編輯	
類別 2	IPTV	編輯	編輯
類別 3	Data/Email	編輯	

3.7 當 WAN 斷線時如何使用 SMS 簡訊服務寄發通知至指定的電話號碼

請參考下列步驟：

1. 登入路由器的網頁設定介面。

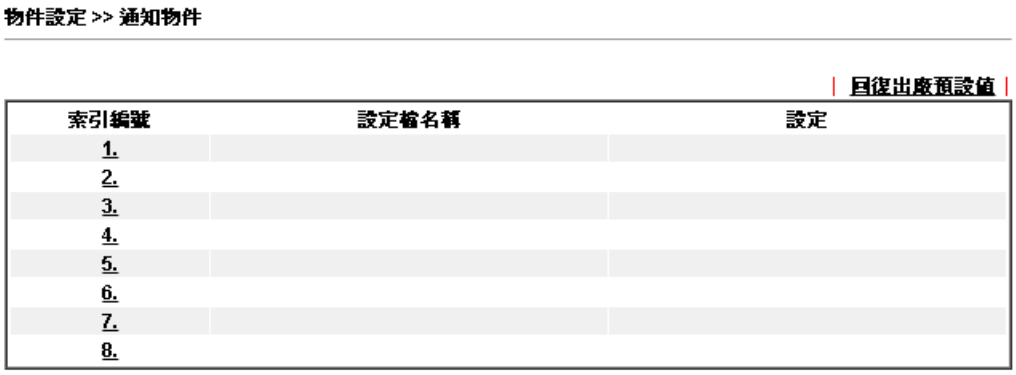
2. 先設定相關物件。首先開啓**物件設定>>簡訊(SMS)/郵件服務物件(Object Settings>>SMS/Mail Server Object)**頁面。

索引編號 1~8 可以讓使用者選取內建的 SMS 簡訊服務供應商，若您所使用的簡訊服務供應商不在內建的清單中，即可使用索引編號 9 與 10 來新增您的 SMS 簡訊服務供應商（請參考備註）。

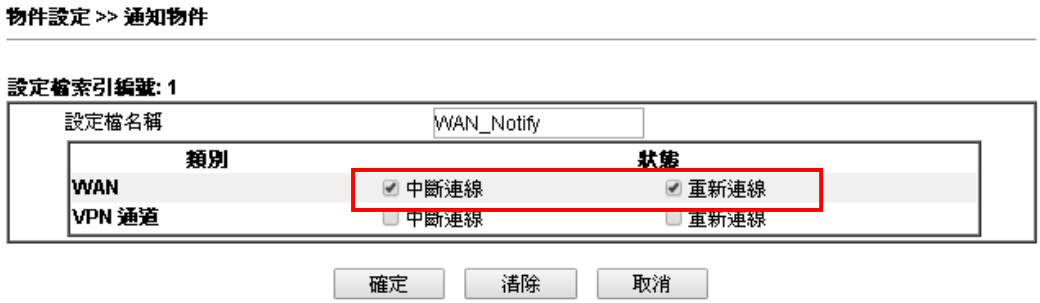
3. 選擇任何一個索引編號(例如本例使用編號 1)進行簡訊服務供應商設定，在下列開啓的頁面中，請填入您的帳號密碼，並設定此路由器可發送的簡訊則數。

4. 設定完畢之後，按下**確定(OK)**回到上頁，便完成簡訊服務供應商的設定。

5. 接著開啓**物件設定>>通知物件(Object Settings>>Notification Object)**，設定通知的事件內容。



6. 選擇任何一個索引編號(例如本例使用編號 1)進行通知發送的條件設定，在下列開啓的頁面中，輸入設定檔名稱，再勾選 WAN 類別中的**中斷連線**與**重新連線(**Disconnected and Reconnected**)**來呼應本文的主題。



7. 設定完畢之後，按下**確定(OK)**回到上頁，便完成通知設定檔的設定。

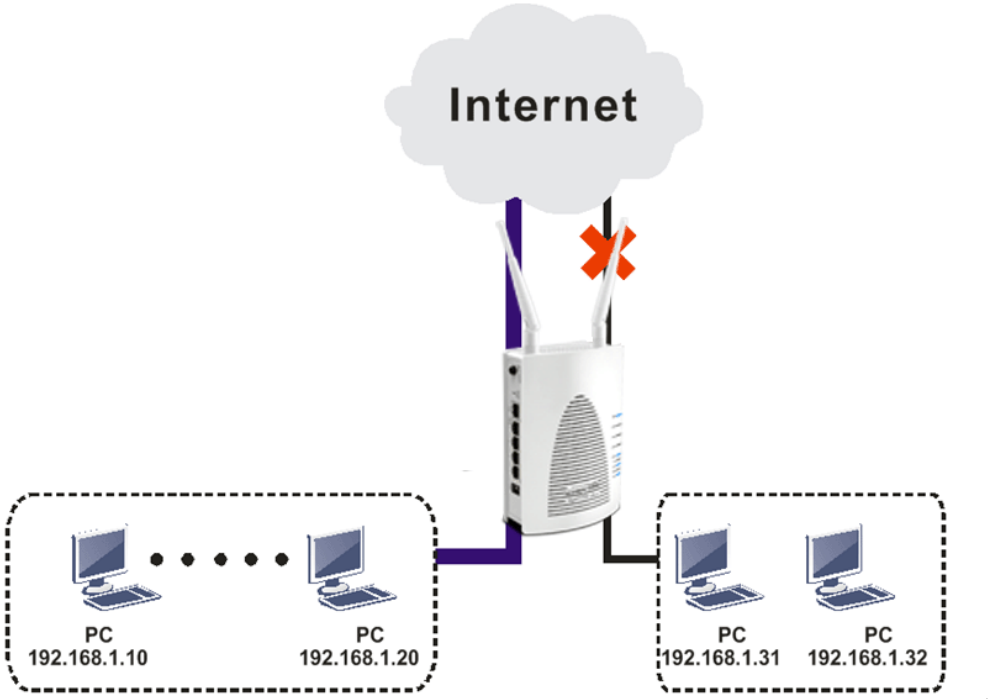
8. 現在，開啓**其他應用>>簡訊(SMS) / 郵件警告服務(Application >> SMS / Mail Alert Service)**頁面。分別自下拉式清單中選擇您需要的簡訊服務供應商與通知設定檔(設定使用簡[訊發送通知的事件)等設定，然後在**收信人(Recipient)**欄位中填入您欲接收簡訊通知的號碼。

備註：如何自訂簡訊服務供應商

開啓**物件設定>>簡訊(SMS)/郵件服務物件(Object Settings>>SMS/Mail Service Object)**，選取任一可自訂的索引連結(例如索引編號 9 或 10)，在開啓的頁面中填入您的簡訊服務供應商的 URL 字串並填入您的帳號密碼，即可新增您所使用的簡訊服務供應商來寄發簡訊 SMS 通知。

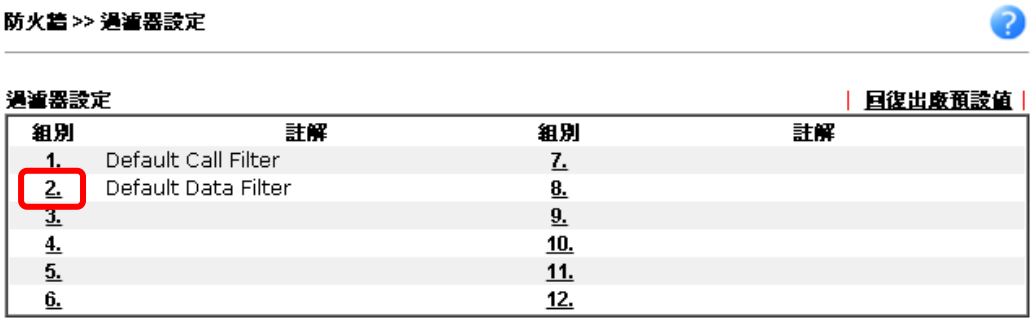
3.8 如何限定特定電腦存取網際網路

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

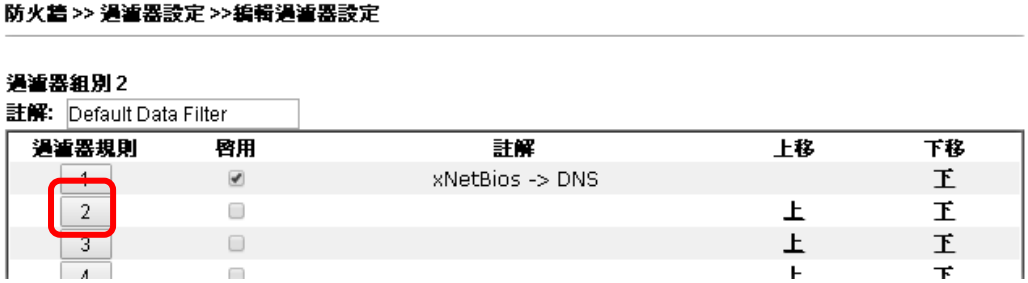


使用的方法是透過防火牆設定二條規則，在**防火牆>>過濾器設定(Firewall>>Filter Setup)**下的規則 1 設定 2 被用來當成預設值設定，我們必須從規則 2 中的設定 2 另外建立新的規則。

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



3. 再選擇**過濾器規則 2 (Filter Rule 2)**按鈕 。



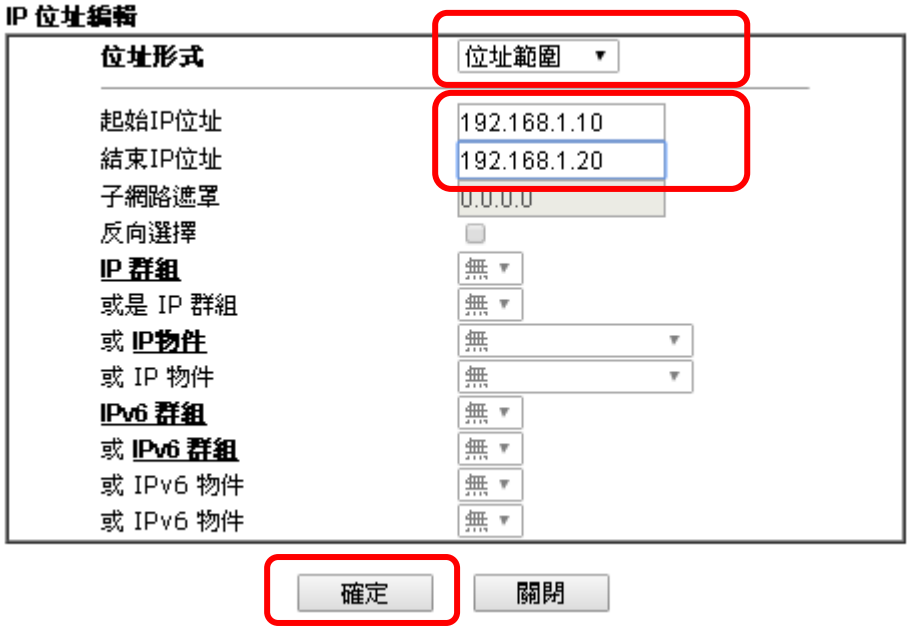
4. 勾選**啓用過濾規則(Check to enable the Filter Rule)**，輸入註解內容(例如 **block_all**)，選擇**若無符合其餘規則即封鎖(Block If No Further Match)**作爲過濾器規則，然後按下**確定(OK)**。

附註:在預設狀態下，路由器檢查封包的順序會以組別 2，過濾器規則 2 開始依序檢查到規則 7，如果您在此選擇了**若無符合其餘規則即封鎖(Block If No Further Match)**作爲過濾器規則，路由器的防火牆檢查封包時將會從規則 3 開始直到規則 7，封包不符合規則就會依照規則 2 的規定來處理。

5. 接著，設定另一條規則，同樣開啓**防火牆>>過濾器設定(Firewall>>Filter Setup)**，按下**組別 2(Set 2)**連結並選擇**過濾器規則 3(Filter Rule 3)**的按鈕。

6. 勾選**啓用過濾規則(Check to enable the Filter Rule)**，輸入註解內容(例如 **open_ip**)，按下**來源 IP(Source IP)**的**編輯(Edit)**按鈕。

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



8. 現在，檢查**來源 IP(Source IP)**的內容是否正確，過濾器的動作/設定爲**立刻通過(Pass Immediately)**，接著按**確定(OK)**儲存。

9. 二個過濾器規則皆已設定完成，請再次按下**確定(OK)**按鈕。

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

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

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

網頁內容過濾器(WCF),

優點：簡單迅速套用至您想要阻擋的類別/網站

附註：需搭配授權碼

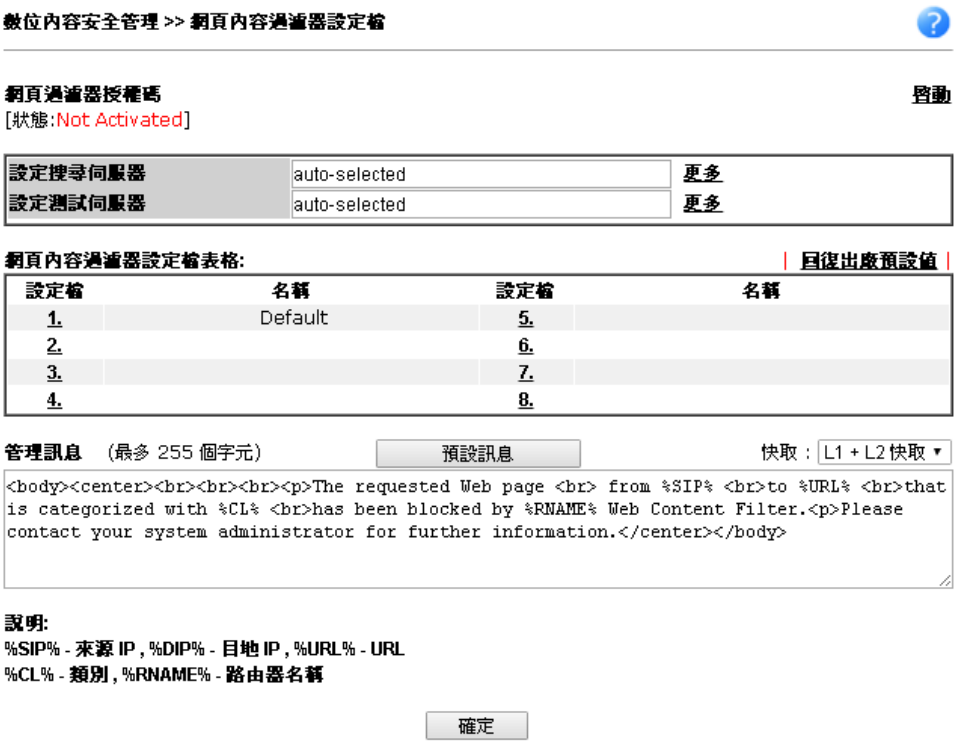
URL 內容過濾器,

優點：免費，對於客製化網頁具有彈性

附註：須手動調整設定 (例如一個網站設定一個關鍵字等)

I.透過網頁內容過濾器(WCF)

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



2. 開啓**數位內容安全管理(CSM) >> 網頁內容過濾器設定檔(CSM >> Web Content Filter Profile)**建立新的 WCF 設定檔，請勾選**社交網路(Social Networking)**，**動作**請選擇**封鎖(Block)**。

3. 在**防火牆>>基本設定>>預設規則(Firewall>>General Setup>>Default Rule)**這個頁面當中，請用剛剛設定的設定檔。

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

II. 透過 URL 內容過濾器

A. 阻擋存取 Facebook 字眼的網頁

1. 開啓**物件設定>>關鍵字物件(Object Settings>>Keyword Object)**，按下任一索引連結以進入設定頁面。

2. 在**內容(Contents)**區域中，輸入 *facebook*，參考下圖所示。按下**確定(OK)**儲存。

3. 開啓**數位內容安全管理>>URL 內容過濾器設定檔(CSM>>URL Content Filter Profile)**，按下任一索引連結開啓設定頁面。

4. 請按下圖所示輸入內容。

5. 完成上述設定之後，按下**確定(OK)**儲存。接著開啓**防火牆>>基本設定(Firewall>>General Setup)**。

6. 選擇**預設規則(Default Rule)**標籤，在開啓的頁面上，於 **URL 內容過濾器(URL Content Filter)**選項中選擇剛剛設定的設定檔。按下**確定(OK)**儲存。

現在，使用者將無法開啓任何含有 facebook 字眼的網頁。

B. 阻擋使用者使用 Facebook 的小遊戲

1. 開啓**物件設定>>關鍵字物件(Object Settings>>Keyword Object)**，按下任一索引連結以進入設定頁面。

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

3. 開啓**數位內容安全管理>>URL 內容過濾器設定檔(CSM>>URL Content Filter Profile)**，按下任一索引連結開啓設定頁面。

4. 請按下圖所示輸入內容。

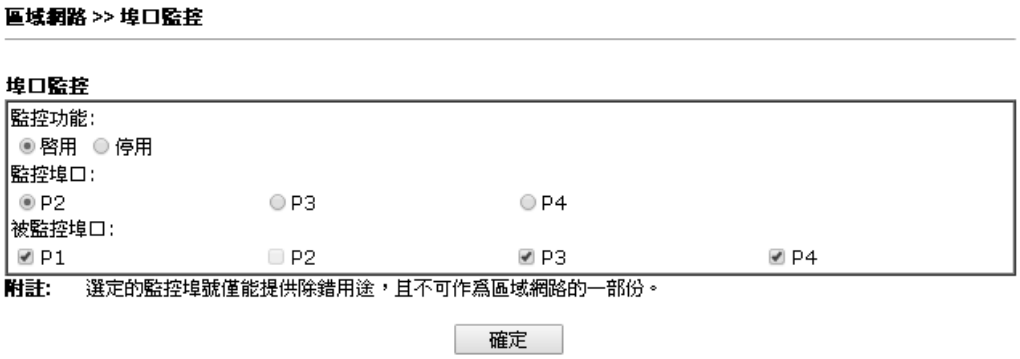
5. 完成上述設定之後，按下**確定**儲存。接著開啓**防火牆>>基本設定(Firewall>>General Setup)**。

6. 選擇**預設規則(Default Rule)**標籤，在開啓的頁面上，於 **URL 內容過濾器**(URL **Content Filter)**選項中選擇剛剛設定的設定檔。按下**確定(OK)**儲存，才能阻擋 apps.facebook 字眼的網址。

3.10 如何在 Vigor2120 系列中搭配使用 SmartMonitor

在支援 SmartMonitor 的機種中，使用者只要將裝有 SmartMonitor 的電腦接到路由器的監控埠口便可以使用。但是 Vigor2120 系列並沒有監控埠口，因此我們必須先到 Vigor2120 的網頁設定畫面設定對應埠以便裝有 SmartMonitor 的電腦可以連接。

1. 在路由器的網頁設定頁面中，請開啓**區域網路 > LAN 埠口監控(LAN > LAN Port Mirror)**。



2. 啓動**埠口監控(Port Mirror)**功能，請選擇**啓用(Enable)**按鈕。

3. 設定監控埠號和被監控埠號。被監控埠號會將所有的封包都轉送到監控埠號。以上圖爲例，若將監控埠號設定爲 P2，而被監控埠號爲 P1、P3 和 P4，那麼 P1、P3 和 P4 的流量都會傳送到 P2。

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

> **附註:** 必須注意的是被設定爲監控埠號的連接埠將無法由 Vigor2120 取得 IP，也就是說連接到監控埠號的電腦將無法存取 Vigor2120 或是網際網路，而只能當做監控電腦來使用。

4 進階設定

本章將導引使用者執行完整的設定操作，有關其他的應用範例，可參考第 3 章。

1. 開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 2925 新增了 3G 網路通訊功能。藉著連接 3G USB Modem 至 Vigor2120 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 Vigor2120n 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 Vigor2120n 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。

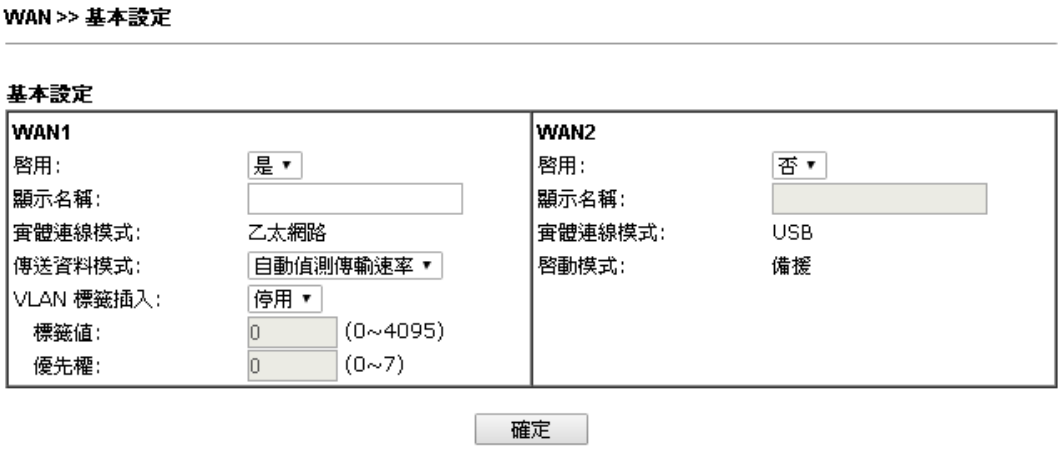
在連接上路由器後，3G USB Modem 及被視爲第二個 WAN 埠，雖然如此原本的乙太網路 WAN1 仍可作爲負載平衡之用，此外 3G USB Modem 也可被視爲備存裝置。因此當 WAN1 無法使用時，路由器將自動改用 3G USB Modem 以應需要。目前路由器支援哪些 3G USB Modem，可在居易網站上取得，歡迎造訪 www.draytek.com。

下圖爲 WAN 的功能項目：

4.1.2 基本設定(General Setup)

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。



可用設定說明如下：

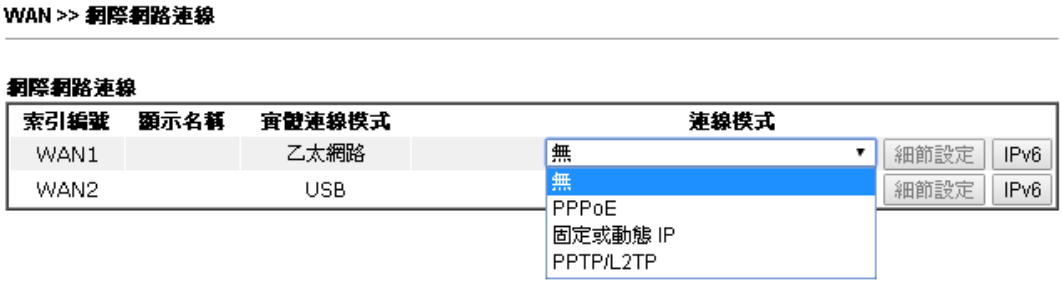
項目	說明
啓用(Enable)	按下**是(Yes)**啓用此 WAN 界面設定；按下**否(No)**停用此 WAN 界面設定。
顯示名稱 (Display Name)	輸入此 WAN 介面的說明名稱。
實體連線模式 (Physical Mode)	顯示此 WAN 介面的實體模式。
傳送資料模式 (Physical Type)	您可以改變 WAN2 的傳送資料模式，或是選擇**自動偵測 (Auto negotiation)**讓系統自行處理。 
VLAN 標籤插入 (VLAN Tag insertion)	**啓用(Enable)** – 啓動夾帶標籤的 VLAN 設定。 路由器將會加上特定的 VLAN 號碼於所有透過此 WAN 口傳出的封包上。 請輸入標籤值並指定由此 WAN 口傳送的封包的優先順序。 **停用(Disable)** – 停止夾帶標籤的 VLAN 設定。

	標籤值(Tag value) –.輸入準備作爲 VLAN ID 編號的數值，可填範圍爲 0 到 4095。 **優先權(Priority)** –.輸入此 VLAN 設定的優先權限，可選範圍從 0 到 7。
啓動模式(Active Mode)	顯示此 WAN 介面目前是主動裝置或是備援裝置。

在您完成上述的設定之後，請按**確定(OK)**按鈕來啓動設定。

4.1.3 網際網路連線控制(Internet Access)

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。



可用設定說明如下：

項目	說明
索引(Index)	顯示路由器支援的 WAN 介面。
顯示名稱(Display Name)	顯示 WAN1/WAN2 於一般設定中所輸入的名稱。
實體連線模式 (Physical Mode)	按照實際網路連線狀況來顯示 WAN1（乙太網路）/ WAN2(3G USB 模式) 實體連線。
連線模式 (Access Mode)	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。
細節設定 (Details Page)	此按鈕將依照您在 WAN1/WAN2 所選擇的連線模式展現不同的網頁內容。
IPv6	此按鈕將會開啓不同的網頁(以實體連線模式爲基準)，針對 WAN 介面設定 IPv6 網際網路存取模式。 如果在 WAN 介面中 IPv6 已經啓動了，那麼您可以在網頁上看到綠色的 IPv6 字樣。

4.1.3.1 WAN1 中的 PPPoE 模式細節設定

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。

可用設定說明如下：

項目	說明
PPPoE 連結 **(PPPoE Link)**	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 **(ISP Access Setup)**	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(Username)** –在本區請輸入 ISP 提供的使用者名稱。 **密碼(Password)** – 在本區請輸入 ISP 提供的密碼。 **索引號碼(1-15) 於排程設定(Index (1-15) in Schedule Setup)** -可以輸入四組時間排程，全部的排程都是在**其他應用>>排程**網頁中事先設定完畢，您可在此輸入該排程的索引編號。
WAN 連線檢測 **(WAN Connection Detection)**	這個功能讓您檢查目前網路是否還在連線中。可透過 ARP 檢測或是 Ping Detect 來完成。 **模式(Mode)** – 選擇 **ARP 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。
PPPoE 通透 (PPPoE Pass-through)	路由器提供 PPPoE 撥號連線。此外您也可以利用路由器直接從本地用戶端與 IPS 建立 PPPoE 連線，當選擇了 PPPoA 協定時，透過電腦傳輸的 PPPoE 封包將轉爲 PPPoA 封包然後送往 WAN 伺服器，如此一來電腦可以利用此方向存取網際網路。 **有線網路 LAN 之使用(For Wired LAN)** – 如果您勾選此選框，位於相同網路中的電腦可以使用另一組 PPPoE 連線數(不同於主機電腦)以登入網際網路。 **無線網路 LAN 之使用(For Wireless LAN)**–如果您勾選此選框，位於相同無線網路的電腦可以使用另一組 PPPoE 連線數(不同於主機電腦)以登入網際網路。
PPP/MP 設定 (PPP/MP Setup)	**PPP 驗證 (PPP Authentication)**– 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(Idle Timeout)** – 設定網際網路在經過一段沒有任何動作的時間後自動斷線的時間。
IP 位址指派方式 (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 (WAN IP Alias) -** 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 (Fixed IP)**– 按**是**使用此功能並輸入一個固定的 IP 位址。 **預設 MAC 位址 (Default MAC Address)** – 您可以使用預設 MAC 位址或是在此區域中填入另一組位址。

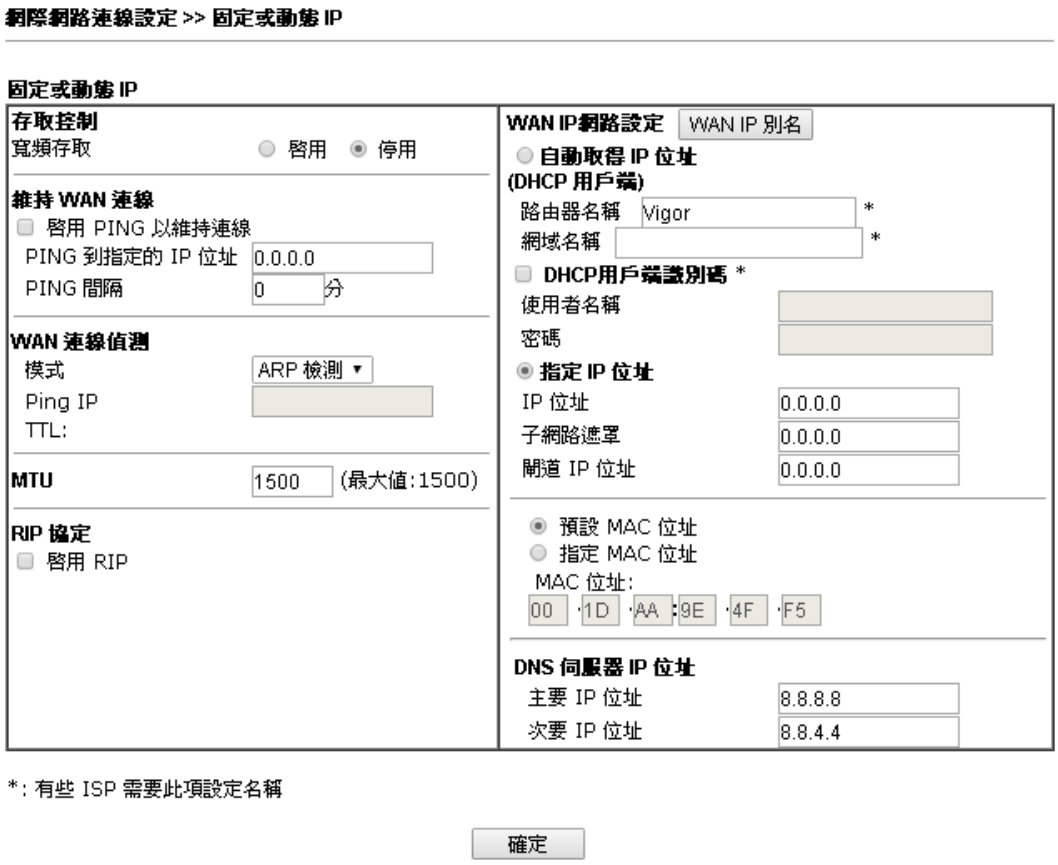
	指定 MAC 位址(Specify a MAC Address) – 手動輸入路由器的 MAC 位址。

在您完成上述的設定之後，請按**確定**按鈕來啓動設定。

4.1.3.2 WAN1 中的固定或動態 IP 模式細節設定

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

若要使用**固定或動態 IP(Static or Dynamic 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(Static or Dynamic IP)**，即可出現下圖。



可用設定說明如下：

項目	說明
寬頻存取 (Broadband Access)	按下**啓用(Enable)**按鈕可啓動此設定，如果您選的是**停用(Disable)**，此項設定將會關閉，全部調整過的配置也都將立即失效。
維持 WAN 連線 (Keep WAN Connection)	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 以維持連線(Enable PING to keep alive)**。 **PING 到指定的 IP 位址 (PING to the IP)–** 如果您啓用

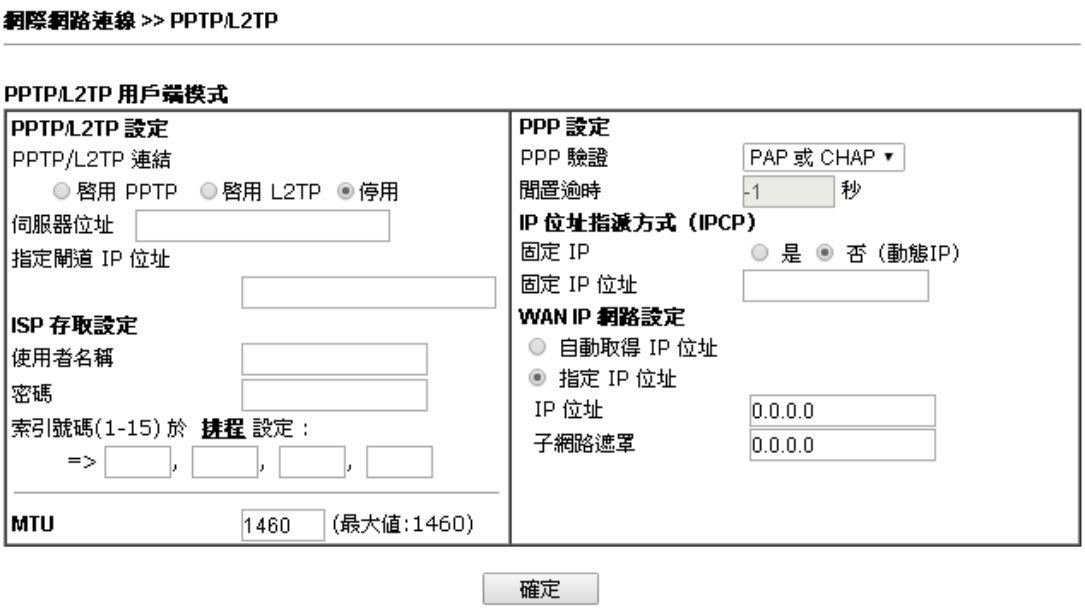
	此功能，請指定 IP 位址讓系統可以 PING 到該 IP 以保持連線 **PING 間隔 (PING Interval)-** 輸入間隔時間讓系統得以執行 PING 動作。
WAN 連線檢測 **(WAN Connection Detection)**	這個功能讓您檢查目前網路是否還在連線中。可透過 ARP 檢測或是 Ping Detect 來完成。 **模式(Mode)** – 選擇 **ARP Detect 或 Ping Detect** 執行 WAN 檢測動作。 **Ping IP** – 如果您選擇 **Ping Detect** 作爲檢測模式，您必須在本區輸入 IP 位址作爲 Ping 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。
RIP 協定(RIP Protocol)	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 **(WAN IP Network Settings)**	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 (WAN IP Alias)-** 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(Obtain an IP address automatically)** – 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(Router Name)**: 輸入 ISP 的路由器名稱。 ● **網域名稱(Domain Name)**: 輸入指定的網域功能變數名稱。 **DHCP 用戶端識別碼** **(DHCP Client Identifier for some ISP)** ● **啓用(Enable):**勾選此方塊，指定使用者名稱與密碼作爲 DHCP 用戶端的辨識依據。 ● **使用者名稱(Username):** 輸入任何名稱，最大長度不要超過 63 個字元。 ● **密碼(Password):** 輸入任何密碼，最大長度不要超過 62 個字元。 **指定 IP 位址(Specify an IP address)** – 按此鈕指定 IP 位址讓資料通過。 ● **IP 位址(IP Address)**:輸入 IP 位址。 ● **子網路遮罩(Subnet Mask)**:輸入子網路遮罩。 ● **閘道 IP 位址(Gateway IP Address)**: 輸入閘道 IP 位址。 **預設 MAC 位址(Default MAC Address)**: 按此鈕使用預

	設的 MAC 位址。 **指定 MAC 位址(Specify a MAC Address)**: 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 (DNS Server IP Address)	若要使用固定 IP 模式，請輸入路由器的主要 IP 位址，如有必要，在將來，您也可以輸入次要 IP 位址以符合所需。

在您完成上述的設定之後，請按**確定(OK)**按鈕來啓動設定。

4.1.3.3 WAN1 中的 PPTP/L2TP 模式細節設定

若要使用 **PPTP/L2TP** 爲網際網路的連線協定，請選擇 **PPTP/L2TP**，即可出現下圖。



可用設定說明如下：

項目	說明
PPTP/L2TP 設定 (PPTP/L2TP Link)	**啓用 PPTP(Enable 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 (Enable 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(Disable)** - 選擇此鈕停用 PPTP 或 L2TP 連線通道。 **伺服器位址(Server Address)** - 指定 PPTP/ L2TP 伺服器的 IP 位址。 **指定閘道 IP 位址(Specify Gateway IP Address)**- 針對 PTP/L2TP 伺服器指定閘道 IP 位址。

ISP 存取設定 **(ISP Access Setup)**	**使用者名稱(Username) -** 輸入 ISP 業者提供給您的使用者名稱。 **密碼(Password) -** 輸入 ISP 業者提供的密碼。 **索引號碼 (1-15) 於排程設定(Index (1-15) in Schedule Setup) -** 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 1460。
PPP 設定 **(PPP Setup)**	**PPP 驗證(PPP Authentication)** – 選擇 **PAP** 或是 **PAP 或 CHAP**。 **閒置逾時(Idle Timeout) -** 閒置逾時表示路由器在一段時間內都沒有運作時，就會中斷連線。
IP 位址指派方式 (IPCP)	通常每次的連線，ISP 會隨機指派 IP 位址給您，在某些情況下，您的 ISP 可以提供給您相同的 IP 位址，不論您何時提出要求。您只要在固定 IP 位址欄位中輸入 IP 位址就可以達成上述的目的。詳情請聯絡您的 ISP 業者。 **固定 IP (Fixed 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(Fixed IP Address)** – 請輸入固定 IP 位址。
WAN IP 網路設定 **(WAN IP Network Settings)**	**自動取得 IP 位址(Obtain an IP address automatically)** – 按此鈕以自動取得 IP 位址。 **指定 IP 位址(Specify an IP address)** – 按此鈕以指定 IP 位址。 ● **IP 位址(IP Address)** – 輸入 IP 位址。 ● **子網路遮罩(Subnet Mask)** – 輸入子網路遮罩。

在您完成上述的設定之後，請按**確定(OK)**按鈕來啓動設定。

4.1.3.4 WAN2 的 PPP 模式細節設定(3G/4G USB 數據機)

如果要使用 3G/4G USB 數據機 (PPP 模式) (**3G/4G USB Modem (PPP mode)**) 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 **3G/4G USB 數據機(PPP 模式)**，即可出現下圖。

可用設定說明如下：

項目	說明
3G /4G USB 數據機 (PPP 模式) **(3G /4G USB Modem (PPP mode))**	選擇**啓用(Enable)**，開啓此功能。如果您選的是**停用(Disable)**，此功能將不再運作，所有設定也都會失效。
SIM PIN 碼(SIM PIN code)	輸入 SIM 卡 PIN 碼，以便連線網際網路。
數據機初始化字串 **(Modem Initial String)**	這個數值，用來初始化 USB 數據機，請使用預設值，如果您有任何疑問，請與當地 ISP 業者聯絡。
APN 名稱 **(APN Name)**	APN 代表接入點名稱(Access Point Name)是由您的 ISP 所提供的，必要時請輸入 ISP 提供的資料，然後按下**套用**即可。
數據機初始化字串 2 **(Modem Initial String2)**	初始化字串 1 是與 APN 搭配使用。 但在某些情況下，使用者可能會使用另外的初始化 AT 指令來限制 3G 頻寬或是其他特殊事宜。此時即可設定第二個數據機初始化字串。

數據機撥號字串 (Modem Dial String)	這個數值，目的是在 USB 模式下撥號使用，請使用預設值，如果您有任何疑問，請與當地 ISP 業者聯絡。
服務名稱(Service Name)	輸入指定網路服務的相關說明。
PPP 使用者 (PPP Username)	輸入 PPP 使用者名稱 (視您實際需要而設定)。
PPP 密碼 (PPP Password)	輸入 PPP 密碼 (視您實際需要而設定)。
PPP 驗證 (PPP Authentication)	選擇 **PAP** 或是 **PAP 或 CHAP**。
索引號碼(1-15) (Index (1-15) in Schedule Setup)	可以輸入四組時間排程，全部的排程都是在**其他應用>> 排程(Application >> Schedule)**網頁中事先設定完畢，您可在此輸入該排程的索引編號。
WAN 連線偵測 (WAN Connection Detection)	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。

在您完成上述的設定之後，請按**確定(OK)**按鈕來啓動設定。

4.1.3.5 WAN2 的 DHCP 模式細節設定(3G/4G USB 數據機)

如果要使用 4G USB 數據機 (DHCP 模式)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 **4G USB 數據機(DHCP 模式) (3G/4G USB Modem (DHCP mode))**，即可出現下圖。

可用設定說明如下：

項目	說明
3G/4G USB 數據機 (DHCP 模式) **(3G/4G USB Modem(DHCP mode)**	選擇**啓用**，開啓此功能。如果您選的是**停用**，此功能將不再運作，所有設定也都會失效。
SIM PIN 碼 **(SIM PIN code)**	輸入 SIM 卡 PIN 碼，以便連線網際網路。
網路連線模式 **(Network Mode)**	強迫路由器以此處指定的模式進行網際網路連線，如果您選擇了 4G/3G/2G 做爲網路模式，路由器將會依照實際網路信號自動選擇適當的模式。
APN 名稱 **(APN Name)**	APN 代表接入點名稱(Access Point Name)是由您的 ISP 所提供的，必要時請輸入 ISP 提供的資料，然後按下**套用**即可。
MTU	代表封包的最大傳輸單位。
WAN 連線偵測	這個功能讓您檢查目前網路是否還在連線中。可透過 ARP 檢測或是 Ping Detect 來完成。 **模式(Mode)** – 選擇 **ARP 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。

在您完成上述的設定之後，請按**確定(OK)**按鈕來啓動設定。

4.1.3.6 WAN1/WAN2 的斷線模式細節設定(IPv6)

當選擇**斷線(Offline)**時，IPv6 連線是中斷的。

4.1.3.7 WAN1/WAN2 的 TSPC 模式細節設定(IPv6)

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

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

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

可用設定說明如下：

項目	說明
使用者名稱 (Username)	輸入您自通道代理人取得的名稱，建議您先進入此網站 http://gogonet.gogo6.com/page/freenet6-account 申請一個使用者名稱以及密碼。

密碼 (Password)	請輸入搭配使用者名稱所分派的密碼。
確認密碼 (Confirm Password)	請再次輸入上述密碼。
通道代理人 (Tunnel Broker)	輸入通道代理人的的 IP 位址、FQDN 或是選項埠號。

在您完成上述的設定之後，請按**確定(OK)**按鈕來啓動設定。

4.1.3.8 WAN1/WAN2 的 AICCU 模式細節設定(IPv6)

可用設定說明如下：

項目	說明
永遠連線 (Always On)	勾選此方塊讓系統隨時保持連線。
使用者名稱 (Username)	輸入通道代理人提供的名稱，請先自此網站 http://www.sixxs.net/申請使用者名稱與密碼。
密碼 (Password)	請輸入搭配使用者名稱所分派的密碼。
確認密碼 (Confirm Password)	請再次輸入上述密碼。
通道代理人 (Tunnel Broker)	輸入通道代理人的的 IP 位址、FQDN 或是選項埠號。
子網前置號碼 (Subnet Prefix)	輸入得自服務供應商所取得之前置號碼位址。

在您完成上述的設定之後，請按**確定(OK)**按鈕來啓動設定。

4.1.3.9 WAN1 的 PPP 模式細節設定(IPv6)

在 IP4v4 PPPoE 連線中，我們可以在閘道器與 Vigor 路由器之間透過 IPv6CP 取得 IPv6 連線的本地位址。之後，使用 DHCPv6 或是 Accep5 RA 來取得 IPv6 的前置碼位址(像是 2001:B010:7300:200::/64 等)，這些是由 ISP 所提供的。另外，在區域網路端的電腦也可以透過處理過的前置碼而擁有實際 IPv6 位址以便存取網際網路。

在 PPP 模式之下，不需進行任何設定。

下圖顯示 PPP 模式下，成功的 IPv6 連線運作範例圖。

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

4.1.3.10 WAN1 的 DHCPv6 用戶端模式細節設定(IPv6)

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

可用設定說明如下：

項目	說明
身分聯結 (Identify Association)	選擇**前置號碼授權**或是**非暫時位址**作爲身分連結選項。
IAID	輸入號碼做爲辨識之用。

在您完成上述的設定之後，請按**確定(OK)**按鈕來啓動設定。

4.1.3.11 WAN1 的固定 IPv6 模式細節設定(IPv6)

這個類型可以您針對 WAN 介面設定固定的 IPv6 位址。

可用設定說明如下：

項目	說明
固定 IPv6 位址設定 **(Static IPv6 Address configuration)**	**IPv6 位址(IPv6 Address) –** 輸入固定的 IPv6 位址。 **前置號碼長度(Prefix Length) –**輸入前置號碼長度固定值。 **新增(Add) –**按下此鈕新增位址。 **刪除(Delete) –** 按下此鈕刪除現存的位址。
目前 IPv6 位址表格 **(Current IPv6 Address Table)**	顯示目前 IPv6 位址的介面。

在您完成上述的設定之後，請按**確定(OK)**按鈕來啓動設定。

4.1.3.12 WAN1 的 6in4 固定通道模式細節設定(IPv6)

這個類型可以您針對 WAN 介面設定 6in4 固定通道的 IPv6 位址。

此模式讓路由器透過 IPv6 網路存取 IPv4 網路。

不過，6in4 提供前置碼設定，您可以使用固定的端點而不必使用隨機端點，此模式具有較高的可靠度。

可用設定說明如下：

項目	說明
遠端終點 IPv4 位址 (Remote Endpoint IPv4 Address)	輸入遠端伺服器的固定 IPv4 位址。
6in4 IPv6 位址 (6in4 IPv6 Address)	輸入 IPv4 通道所需的固定 IPv6 位址，以及前置碼長度值。
LAN 路由前置碼 (LAN Routed Prefix)	輸入 LAN 路由所需的固定 IPv6 位址，以及前置碼長度值。
通道 TTL (Tunnel TTL)	輸入通道中資料存活時間數。

在您完成上述的設定之後，請按**確定(OK)**按鈕來啓動設定。

4.1.3.13 WAN1 的 6rd 模式細節設定(IPv6)

這個類型可以您針對 WAN 介面進行 6ird 設定。

可用設定說明如下：

項目	說明
6rd 模式 **(6rd Mode)**	**自動 6rd (Auto 6rd) –** 自動從 6rd 服務供應商處取得 6rd 前置碼，IPv4 的 WAN 介面請先設定爲 DHCP。 **固定 6rd (Static 6rd)-**手動輸入 6rd 選項資料。
IPv4 Border 中繼 **(IPv4 Border Relay)**	針對給定的 6rd 網域，輸入 6rd Border 中繼所需的 IPv4 位址。
IPv4 遮罩長度 **(IPv4 Mask Length)**	針對給定的 6rd 網域，輸入所有 IPv4 地址皆可跨越的高位元數值。 可用數值介於 0 和 32 之間。
6rd 前置代碼 **(6rd Prefix)**	輸入 IPv6 位址。
6rd 前置代碼長度 **(6rd Prefix Length)**	輸入 6rd 所需的長度值。

在您完成上述的設定之後，請按**確定(OK)**按鈕來啓動設定。

4.1.4 多重 VLAN (Multi-VLAN)

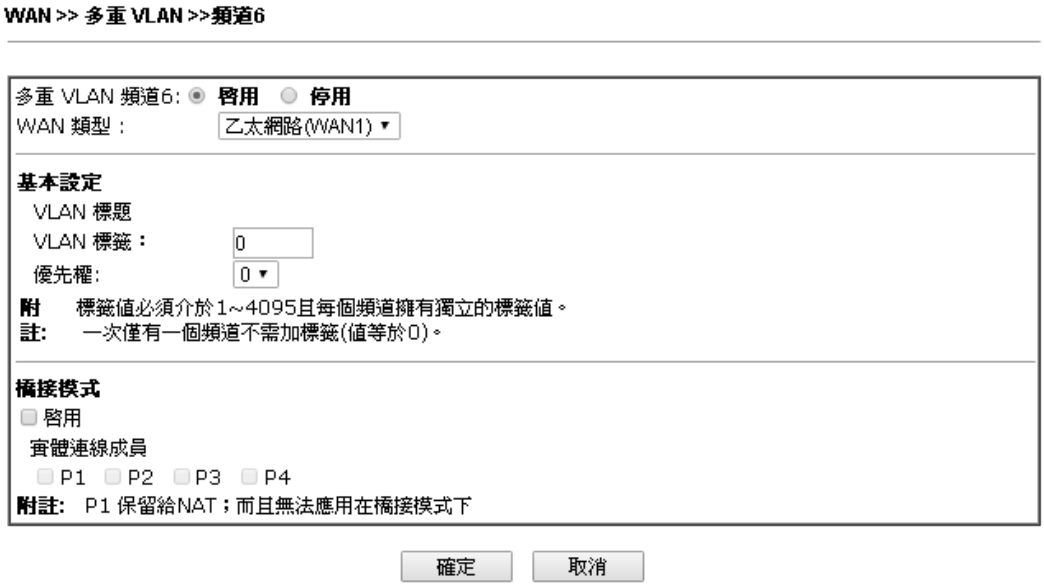
多重 VLAN 可讓用戶針對 WAN 介面建立設定檔與橋接連線，以便用於需要高度網路流量的應用上。

本頁顯示每個頻道的基本設定值。

可用設定說明如下：

項目	說明
頻道(Channel)	顯示每個頻道的編號。 頻道 1 與 2 專屬於網際網路使用者介面，因此在此處是不可以修訂的。 頻道 3 到 8 是可以設定調整的。
啓用(Enable)	顯示此頻道的設定是啓用(Yes 是)還是停用(No 否)。
WAN 類型 **(WAN Type)**	顯示頻道使用的實體介面類型。
VLAN 標籤 **(VLAN Tag)**	顯示用於此頻道封包傳輸攜帶的 VLAN 標籤值。
埠號橋接 **(Port-based Bridge)**	系統可透過個別 VLAN 標籤值來辨識每個頻道網路流量，不同頻道即使利用相同 WAN 介面，也不可採用相同的 VLAN 標籤值。 **啓用(Enable)** - 勾選此方塊以便啓用該頻道的埠號橋接功能。 **P1 ~ P4** – 選需要的埠號以便建立區域網路端的橋接連線。

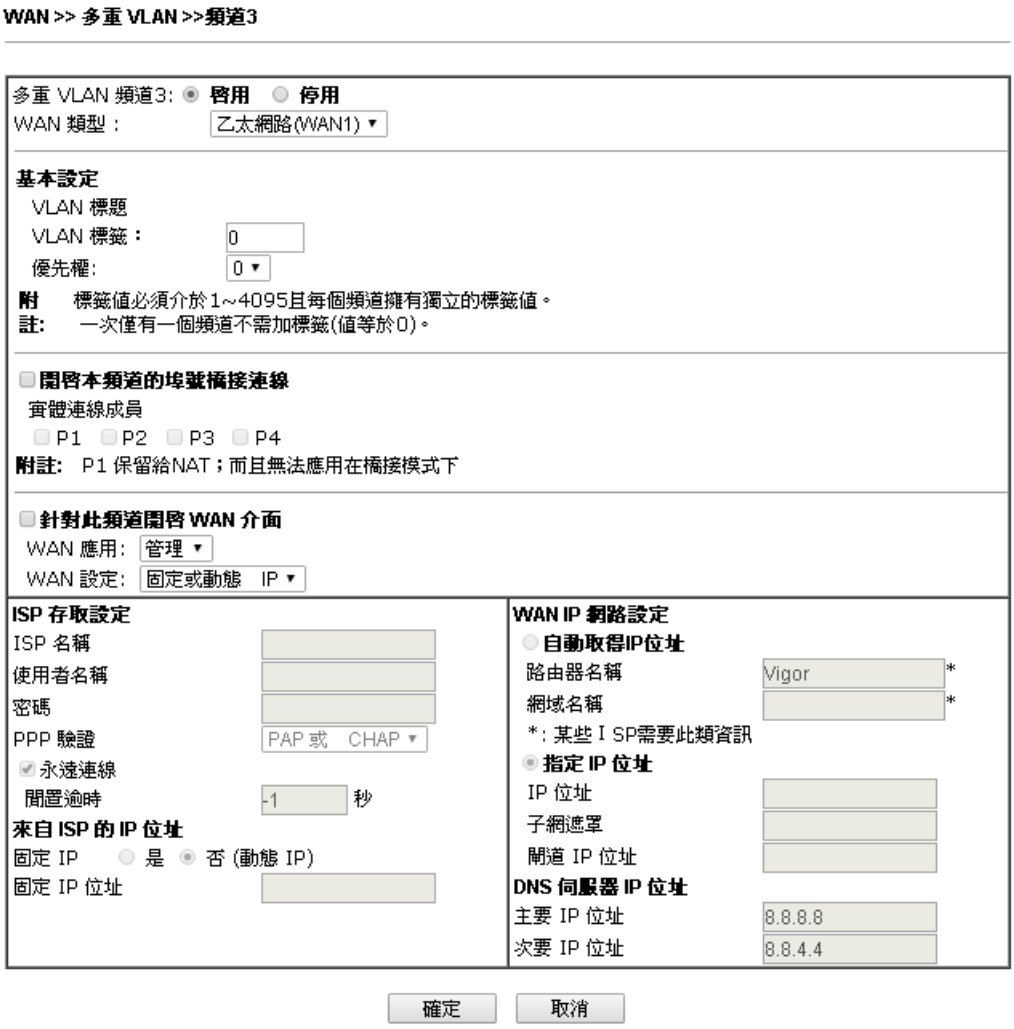
按下索引編號(6~8)可以看到如下頁面：



可用設定說明如下：

項目	說明
多重 VLAN 頻道 (6~8) **(Multi-VLAN Channel (6~8))**	**啓用(Enable) –** 選擇此項啓用此頻道設定。 **停用(Disable) –** 選擇此項停止使用此頻道設定。
WAN 類型 **(WAN Type)**	每個頻道連線與介面都可透過選擇一個特定的 WAN 類型來建立。在多重 VLAN 應用中，只有乙太網路 WAN 類型可以使用，使用者可選擇實體 WAN 介面。
基本設定 **(General Settings)**	**VLAN 標籤(VLAN Tag) –** 輸入 VLAN ID 號碼，可設定範圍自 1 到 4095，系統可透過 VLAN 標籤來辨識每個頻道，使用相同 WAN 類型的頻道不可設定相同的 VLAN 標籤值。 **優先權(Priority) –** 選擇一個號碼來決定此 VLAN 封包的優先權爲何，可設定範圍自 0 到 7。
橋接模式 **(Bridge mode)**	**啓用(Enable) –** 選擇此項啓用此頻道設定的橋接模式。 **實體連線成員(Physical Members) –** 勾選您想要群組的埠號，使其套用橋接模式連線。

另外，3~5 的 WAN 連結主要用於路由器的應用，例如 **TR-069**。這邊的設定值必須取自 ISP 業者，且只能套用在該 ISP 業者。如果有特殊需要，請與您的 ISP 業者聯絡，然後再至此設定此三個頻道。



可用設定說明如下：

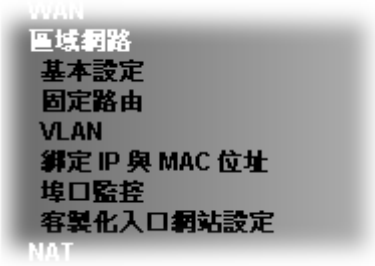
項目	說明
多重 VLAN 頻道(3~5) **(Multi-VLAN Channel (3~5))**	**啓用(Enable) –** 選擇此項啓用此頻道設定。 **停用(Disable)–** 選擇此項停止使用此頻道設定。
WAN 類型 **(WAN Type)**	每個頻道連線與介面都可透過選擇一個特定的 WAN 類型來建立。在多重 VLAN 應用中，只有乙太網路 WAN 類型可以使用，使用者可選擇實體 WAN 介面。
基本設定 **(General Settings)**	**VLAN 標籤(VLAN Tag) –** 輸入 VLAN ID 號碼，可設定範圍自 1 到 4095，系統可透過 VLAN 標籤來辨識每個頻道，使用相同 WAN 類型的頻道不可設定相同的 VLAN 標籤值。 **優先權(Priority) –** 選擇一個號碼來決定此 VLAN 封包的優先權爲何，可設定範圍自 0 到 7。
開啓本頻道的埠號橋接連線 **(Open Port-based Bridge Connection for this**	.此處設定將會在 LAN 埠口間與 WAN 口建立橋接連線，橋接連線建立在選定的 WAN 介面並使用 VLAN 標籤值。 **實體連線成員(Physical Members) –** 勾選您想要群組的

Channel)	埠號，使其套用橋接模式連線。
針對此頻道開啓 WAN 介面 **(Open WAN Interface for this Channel)**	勾選選框啓用相關功能。 **WAN 應用 – 管理(WAN for Router-borne Application - Management)**可指定爲一班管理之用(網頁設定/telnet/TR069)，如果您選擇此項，此 VLAN 設定將僅對網頁設定/telnet/TR069 產生作用。 **WAN 應用 – IPTV** - 允許 WAN 介面傳送 IGMP 封包到 IPTV 伺服器。 **WAN 設定(WAN Setup)** – 選擇 PPPoE/PPPoA 或是固定或動態 IP 設定(Dynamic IP)，以便決定哪個 WAN 介面需要設定。
ISP 存取設定、WAN IP 網路設定等等 **(ISP Access Setup, IP Address From ISP, WAN IP Network Settings, DNS Server IP Address)**	WAN1 有關其他設定，請參考 WAN1 底下 PPPoE/固定 IP 或動態 IP 的細部設定**(Details Page for PPPoE / Static or Dynamic IP in WAN1.)**。

在您完成上述的設定之後，請按**確定(OK)**按鈕來啓動設定。

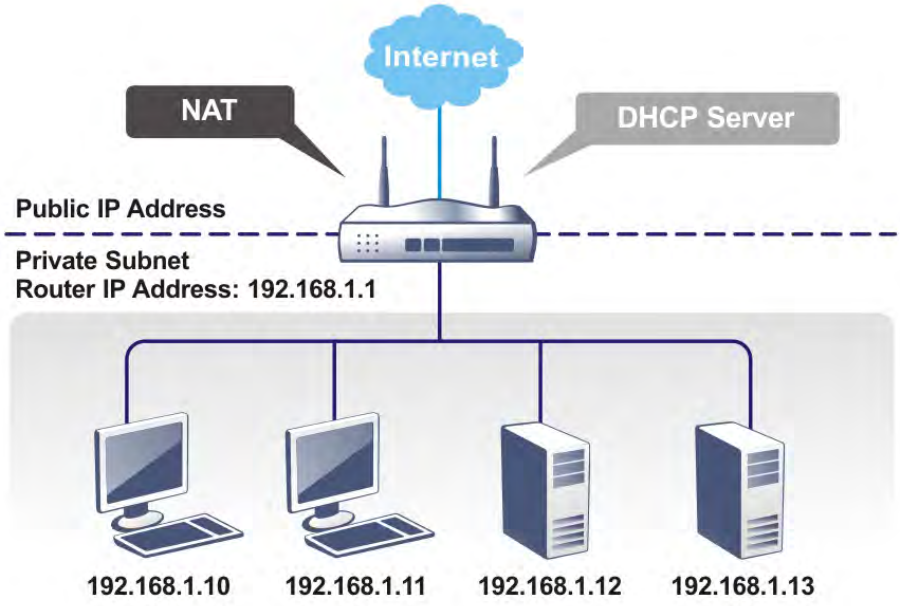
4.2 區域網路(LAN)

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。

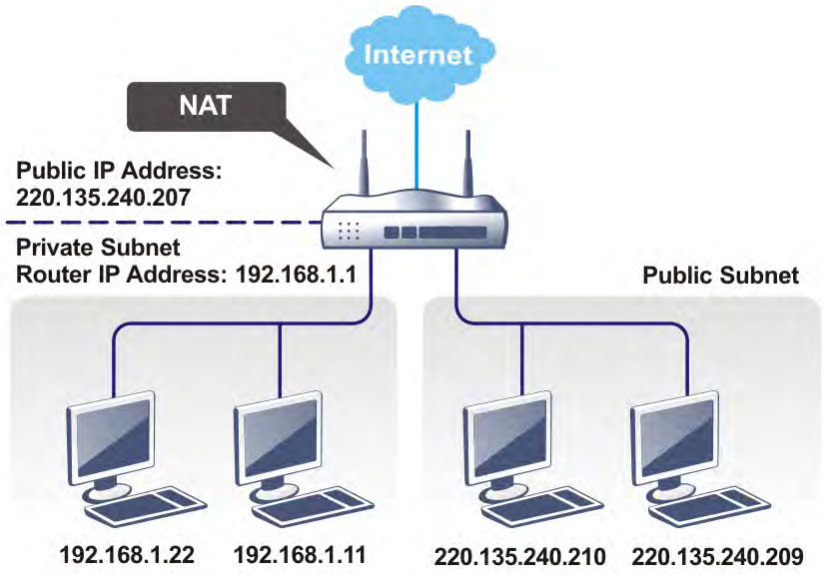


4.2.1 區域網路基本概念

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)

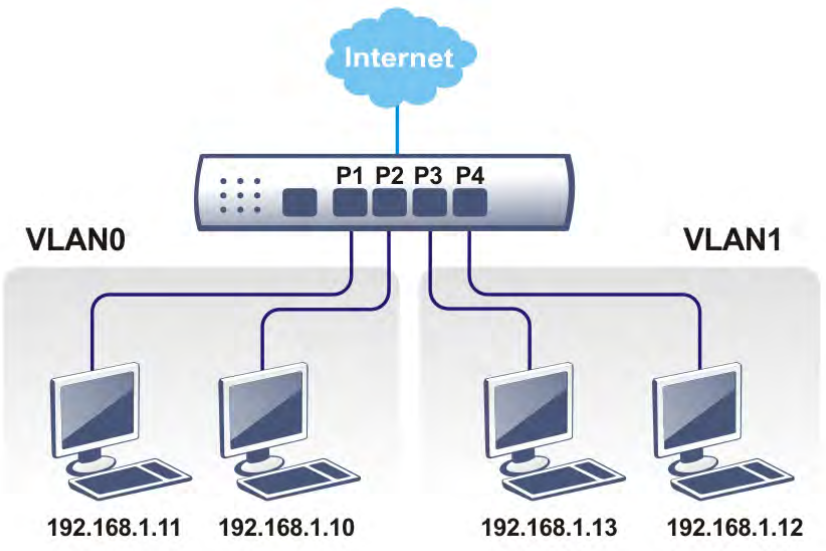
Vigor 路由器可利用 RIP 與鄰近路由器交換路由資訊，達到 IP 路由的目的。這樣可讓使用者變更路由器的資訊，例如 IP 地址，且路由器還會自動通知雙方此類訊息。

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)

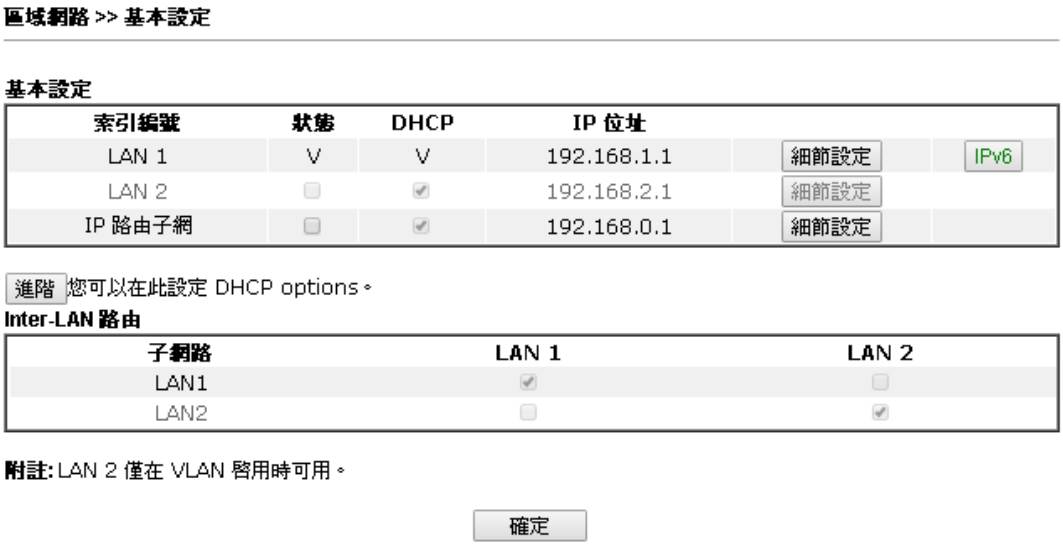
您可以利用實體的連接埠將群組區域網路上的主機，然後建立虛擬區域網路，最多可達 4 個。爲了要管理不同群組間的通訊狀況，請再虛擬區域網路功能上設定一些規則，以及每個網路的傳送速率。



4.2.2 基本設定(General Setup)

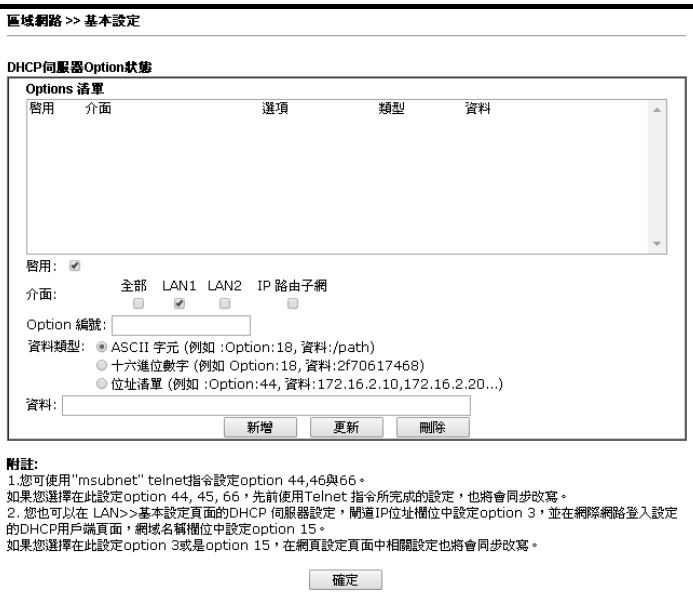
本頁提供您區域網路的基本設定。按**區域網路(LAN)**開啓區域網路設定並選擇**基本設定(General Setup)**。

路由器提供二個子網，讓使用者來區隔，此外，不同子網可透過 Inter-LAN 路由讓彼此互通。目前 LAN1 設定固定爲 NAT 模式專用，LAN2 可用於 NAT 或是路由模式。IP 路由子網則可於路由模式下操作。



可用設定說明如下：

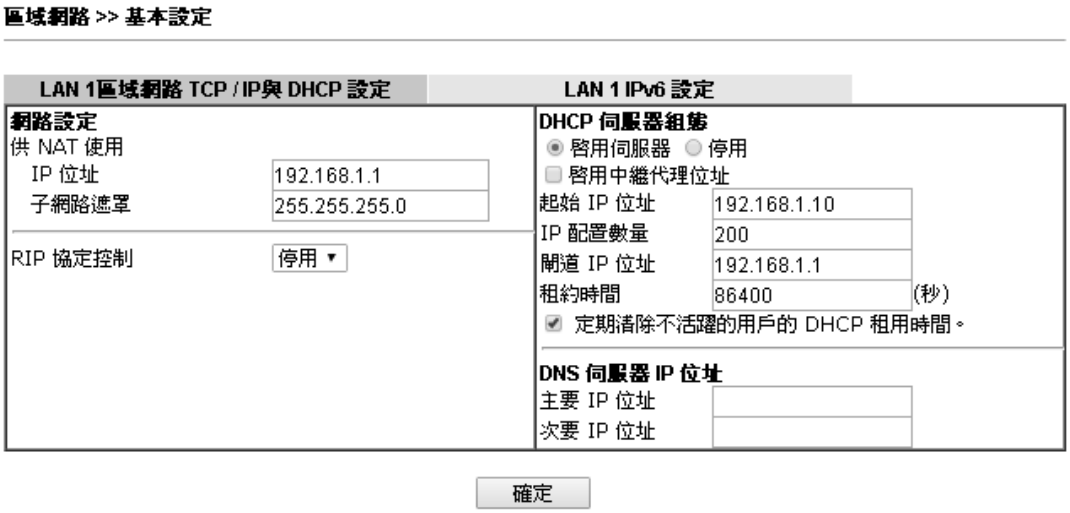
項目	說明
基本設定 (General Setup)	允許針對個別子網設定不同內容。 **索引編號(Index) -**.顯示全部的 LAN 項目。 **狀態(Status) -** 基本上 LAN1 狀態於預設時是啓用的，LAN2 之後與 IP 路由子網只有在狀態欄位已勾選時，始可查閱。 **DHCP(DHCP)-** 預設狀態下，LAN1 設定爲 DHCP 模式，如果有必要，請針對每個 LAN 勾選此方塊。 **IP 位址 (IP Address)-** 顯示每個 LAN 的 IP 位址。 **細節設定(Details Page) -** 按下此鈕可進入設定頁面，每條 LAN 都可以有不同的設定內容，也勾可以設定在不同的子網下。 **IPv6 –** 按下此鈕進入 IPv6 設定頁面。
進階 (Advanced)	DHCP 封包可以利用新增選項號碼與資訊做額外處理。

	 **啓用(Enable)** – 啓用或是停用 DHCP 選項功能，每個 DHCP 選項都是由一個 Option Number 與資料組合而成。例如 Option number:100 資料: abcd 當此功能啓用時，即可在 DHCP 回覆封包中見到此處指定的內容。 **Option Number** – 輸入一組號碼。 **介面(Interface)** – 選擇套用此功能的介面。 **資料類型(DataType)** – 選擇儲存資料的類型(ASCII 或是十六進位)。 **資料(Data)** – 輸入 DHCP 選項功能必須處理的資料內容。
Inter-LAN 路由 (Inter-LAN Routing)	勾選方塊來連結二個或是多個不同的子網(LAN 與 LAN 間)。

在您完成上述的設定之後，請按**確定(OK)**按鈕來啓動設定。

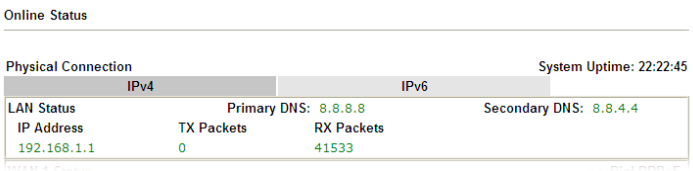
4.2.2.1 LAN1 - 區域網路 TCP/IP 與 DHCP 設定的細節設定

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



可用設定說明如下：

項目	說明
網路設定 **(Network Configuration)**	**供 NAT 使用** **IP 位址(IP Address) -** 請輸入虛擬 IP 位址以便連接區域虛擬網路(預設值爲 192.168.1.1)。 **子網路遮罩(Subnet Mask) -** 請輸入決定網路大小的位址代碼(預設值爲 255.255.255.0/ 24)。 **RIP 協定控制(RIP Protocol Control),** **停用(Disable) –** 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)。 **啓用(Enable) –** 啓動此協定。
DHCP 伺服器組態 **(DHCP Server Configuration)**	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。 **啓用伺服器(Enable Server) -** 讓路由器指定 IP 地址到區域網路上的每個主機上。 **停用(Disable Server) –** 讓您手動指定 IP 地址到區域網路上的每個主機上。 **啓用中繼代理位址(Enable Relay Agent)** – 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。 **中繼代理程式 IP 位址(DHCP Server IP Address)–** 當您勾選了**啓動中繼代理位址**之後，即可見到此項目，設定您準備使用的伺服器 IP 位址讓中繼代理幫忙轉送 DHCP 需求至 DHCP 伺服器上。 **起始 IP 位址(Start IP Address)-**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(IP Pool Counts) -**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(Gateway IP Address) -**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。 **租約時間(Lease Time) -** 輸入 DHCP 伺服器可以使用來分派 IP 位址的時間長度。 **定期清除不活躍的用戶的 DHCP 租用時間 -** 當 DHCP 用戶從 LAN DHCP 伺服器請求 IP 位址時，伺服器會釋放一組 IP 給予該用戶端一段時間(例如一天)。然而，即使該用戶僅使用該 IP 五分鐘，伺服器仍然保留該 IP 給用戶，因爲 DHCP 伺服器僅有限定數量的 IP 數可提供給 DHCP 用戶，很快的所有的 IP 都會被用罄，然後就再也沒人可以從此伺服器取得 IP 位址。因此這個功能可將不再活動的用戶 (例如不使用 IP 但伺服器仍然爲其保留該 IP) 取回 IP。
DNS 伺服器 IP 位址 (DNS Server IP Address)	DNS 是 Domain Name System 的縮寫，每個網際網路的主機都必須擁有獨特的 IP 位址，也必須有人性化且容易記住的名稱諸如 www.yahoo.com 一般，DNS 伺服器可轉換此名稱至相對應的 IP 地址上。 **主要 IP 位址(Primary IP Address) -**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(Secondary IP Address) -** 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。 如果網域名稱的 IP 位址已經在 DNS 快速緩衝貯存區內，路由器將立即處理網域名稱。否則路由器會藉著建立 WAN (例如 DSL/Cable)連線時，傳送 DNS 疑問封包至外部 DNS 伺服器。

在您完成上述的設定之後，請按**確定(OK)**按鈕來啓動設定。

LAN1 – IPv6 的細節設定

LAN1 中有二種設定頁面，一個是乙太網路 TCP/IP 與 DHCP 設定(以 IPv4 爲基準)，另一個是 IPv6 設定。下圖爲 IPv6 的設定頁面。

本頁面提供二種 LAN 端 IPv6 位址設定，一種爲 **RADVD**，另一種爲 **DHCPv6 伺服器 (DHCPv6 Server)**。

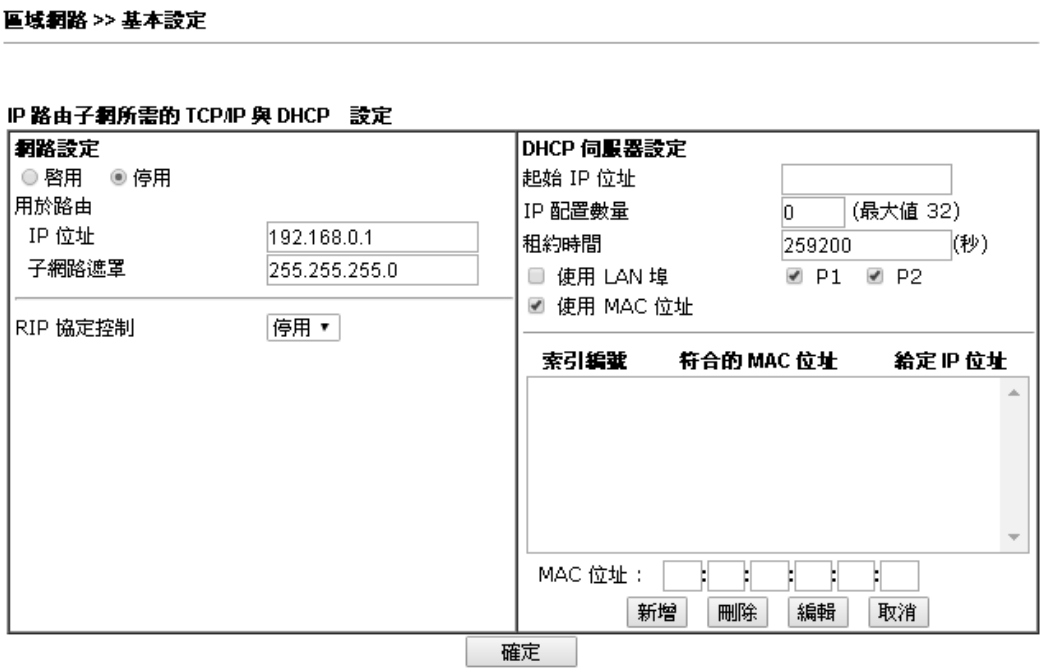
可用設定說明如下：

項目	說明
路由器廣播伺服器 **(Router Advertisement Server)**	**啓用(Enable)** – 啓動 RADVD 伺服器，路由器 RADVD 定期傳送 RFC2461 指定的訊息至本地乙太網路 LAN 端，這些訊息乃是因應 IPv6 無狀態自動設定的需求。 **停用(Disable)** –停用 RADVD 伺服器的運作。 **廣播有效時間(Advertisement Lifetime)** - 預設路由器的

項目	說明
	有效時間以秒計算，用來控制前置號碼的有效期間，最大值可對應至 18.2 小時。數值設定爲 0 表示路由器並非預設的路由器，且也不會出現在預設路由器的清單內。
DHCPv6 伺服器 (DHCPv6 Server Configuration)	**啓用伺服器(Enable Server)** – 啓動 DHCPv6 伺服器，DHCPv6 伺服器可以依照起始/結束 IP 位址設定來分派 IPv6 位址至電腦上。 **停用(Disable Server)** – 停用 DHCPv6 伺服器的運作。 **起始 IPv6 位址 / 結束 IPv6 位址 (Start IPv6 Address / End IPv6 Address)**– 分別輸入起始以及結束的 IP 位址。
DNS 伺服器 IPv6 位址 (DNS Server IPv6 Address)	**主要 DNS 伺服器(Primary DNS Sever)** – 輸入主要 DNS 伺服器的 IPv6 位址。 **次要 DNS 伺服器(Secondary DNS Server)** – 輸入次要 DNS 伺服器的 IPv6 位址。
固定 IPv6 位址設定 (Static IPv6 Address configuration)	**IPv6 位址(IPv6 Address)** – 輸入區域網路所需的固定 IPv6 位址。 **前置號碼長度(Prefix Length) –** .輸入前置號碼固定的長度值。 **新增(Add) –**.新增新的位址資料並顯示在位址表格中。 **刪除(Delete) –** 刪除位址表格中選定的位址資料。
目前 IPv6 位址表格 (Current IPv6 Address Table)	顯示目前使用的 IPv6 位址。

在您完成上述的設定之後，請按**確定(OK)**按鈕來啓動設定。

IP 路由子網的細節設定



可用設定說明如下：

項目	說明
網路設定	**啓用/停用** -選擇**啓用**來啓動此設定，按下**停用**則關閉此設定。 **IP 位址** - 請輸入虛擬 IP 位址以便連接區域虛擬網路(預設值爲 192.168.1.1)。 **子網路遮罩** - 請輸入決定網路大小的位址代碼(預設值爲 255.255.255.0/ 24)。 **RIP 協定控制,** ● **停用** – 關閉 RIP 協定，可讓不同路由器之間資訊交換暫停 (此爲預設值)。 ● **啓用** – 啓動此協定。
DHCP 伺服器設定	DHCP 是 Dynamic Host Configuration Protocol 的縮寫，路由器的出廠預設值可以作爲您的網路的 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。 **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。 **租約時間** - 輸入 DHCP 伺服器可以使用來分派 IP 位址

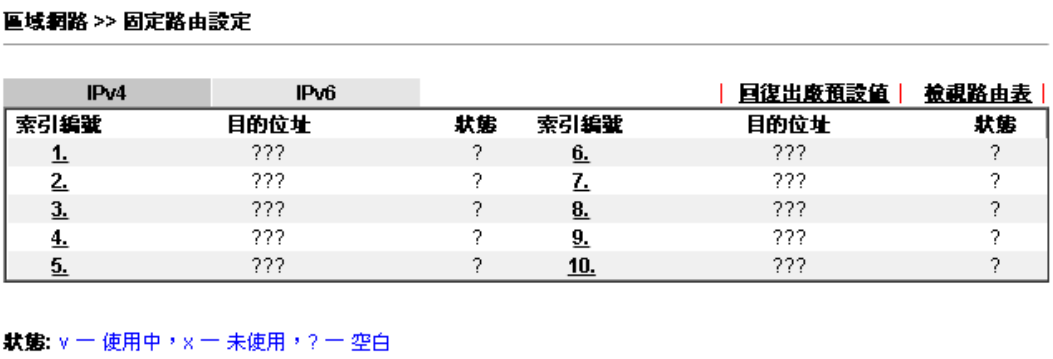
	的時間長度。 **使用 LAN 埠 –** 指定一個 IP 位址供 IP 路由子網使用，如果啓用此埠，DHCP 伺服器將會自動指派一個 IP 位址給予 P1 與/或 P2 的用戶。請勾選準備使用的 LAN 埠口 (P1 與/或 P2)。 **使用 MAC 位址 -**.勾選此方框可指定 MAC 位址。 **MAC 位址-**輸入輸入主機的 MAC 位址然後按下方的新增按鈕，建立伺服器分派位址的主機清單，也可以刪除或編輯清單內容。 **新增 –** 在上方 MAC 位址框中輸入位址內容，按下此鈕之後即可新增。 **刪除** – 刪除上方選定的 MAC 位址。 **編輯** – 編輯上方選定的 MAC 位址。 **取消** – 取消新增、編輯以及刪除等運作。

在您完成上述的設定之後，請按**確定**按鈕來啓動設定。

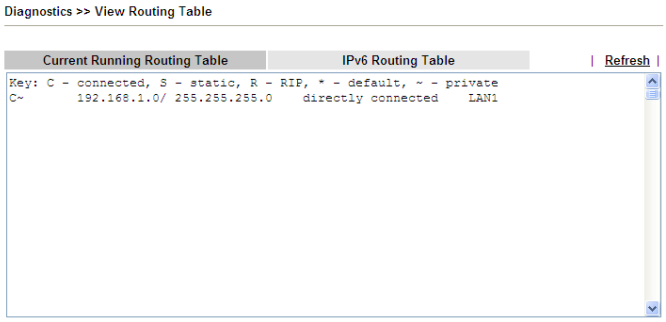
4.2.3 固定路由(Static Route)

進入**區域網路(LAN)**群組並選擇**固定路由(Static Route)**，開啓如下的畫面。

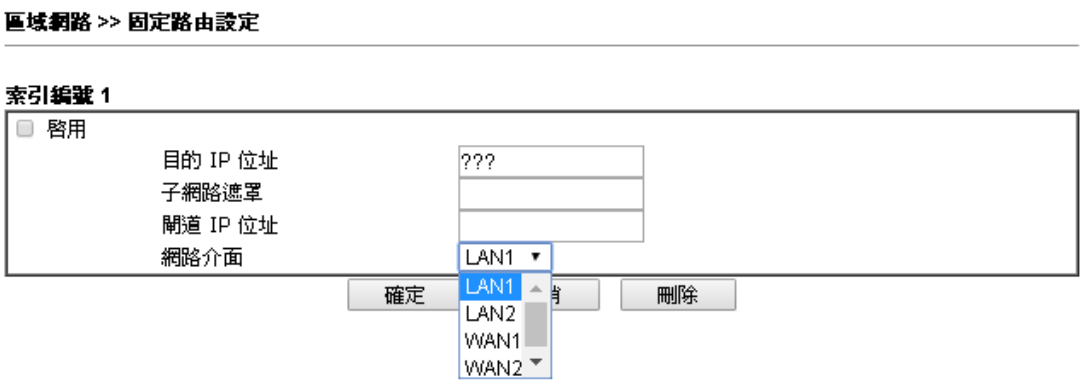
固定路由(IPv4)



可用設定說明如下：

項目	說明
回復出廠預設值 **(Set to Factory Default)**	清除所有設定並回到出廠的設定狀態。
檢視路由表 **(View Routing Table)**	開啓如下畫面檢視目前的路由狀況。 
索引編號 **(Index)**	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。
目的位址 **(Destination Address)**	顯示固定路由的目標位址。
狀態 **(Status)**	顯示固定路由的狀態。

按下任一索引編號開啓如下頁面：



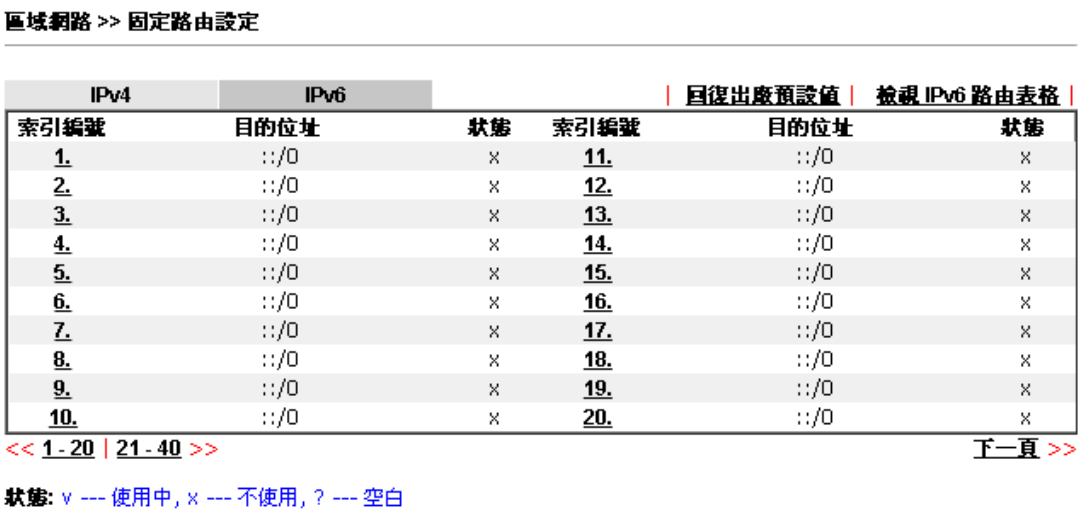
可用設定說明如下：

項目	說明
啓用(Enable)	勾選此方塊以啓動此設定檔。
目的 IP 位址 (Destination IP Address)	輸入此固定路由作爲目的需求的 IP 位址。
子網路遮罩 (Subnet Mask)	輸入此固定路由的子網遮罩。
閘道 IP 位址 (Gateway IP Address)	輸入此固定路由的閘道 IP 位址。
網路介面 (Network Interface)	使用下拉式清單指定單一介面作爲固定路由的通過介面。

在您完成上述的設定之後，請按**確定(OK)**按鈕來啓動設定。

固定路由(IPv6)

按下 IPv6 標籤開啓下述頁面，您可以設定多達 40 組設定檔。



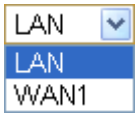
可用設定說明如下：

項目	說明
回復出廠預設值 (Set to Factory Default)	清除所有設定並回到出廠的設定狀態。
檢視 IPv6 路由表格 (Viewing IPv6 Routing Table)	顯示路由表格。
索引編號 (Index)	索引編號下方的數字連結可讓您開啓設定頁面進行路由設定。
目的位址 (Destination Address)	顯示固定路由的目標位址。
狀態(Status)	顯示固定路由的狀態。

按下任一索引編號開啓如下頁面：

可用設定說明如下：

項目	說明
啓用(Enable)	勾選此方塊以啓動此設定檔。

目標 IPv6 位址 / 前置號碼長度 (Destination IPv6 Address / Prefix Len)	輸入此固定路由的 IP 位址以及字首的長度。
閘道 IPv6 位址 (Gateway IPv6 Address)	輸入此固定路由的閘道位址。
網路介面 (Network Interface)	使用下拉式清單指定單一介面作爲固定路由的通過介面。 

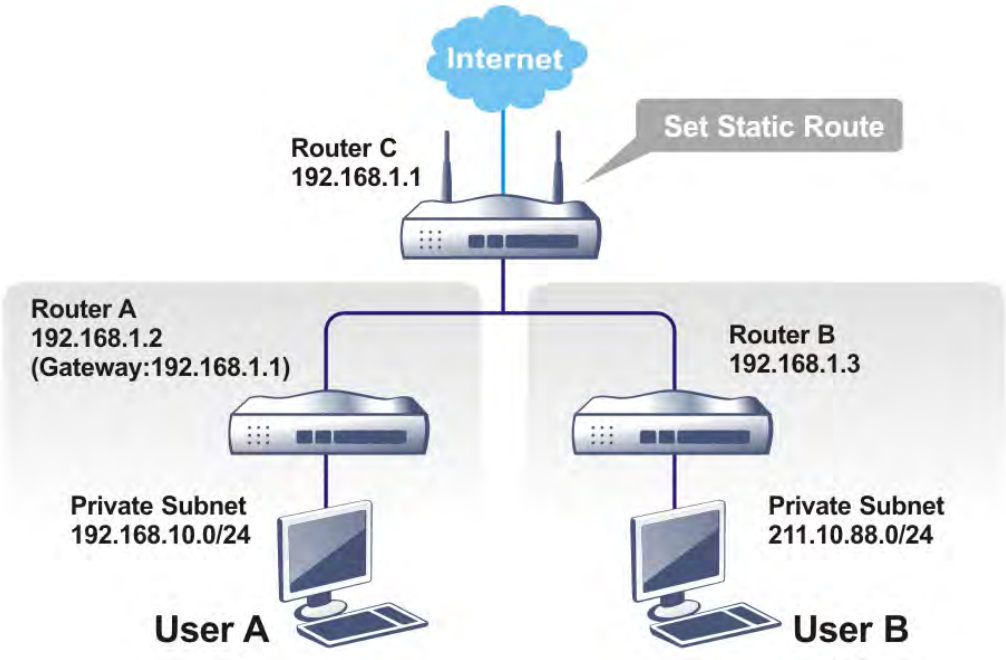
在您完成上述的設定之後，請按**確定(OK)**按鈕來啓動設定。

增加固定路由至虛擬或真實網路上(以 IPv4 爲基準)

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

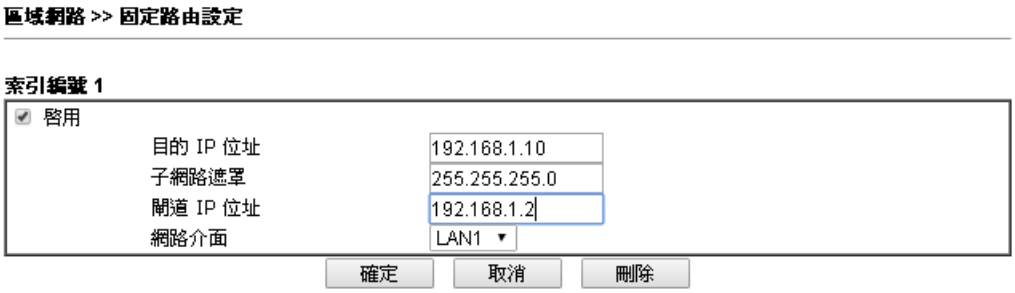
在設定固定路由之前，使用者 A 無法與使用者 B 溝通，因爲路由器 A 只會傳送辨認出的封包至主要路由器的預設閘道。



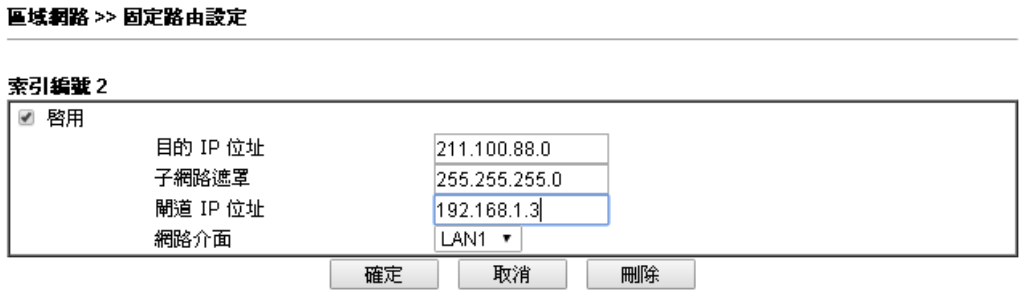
1. 在**區域網路(LAN)**群組中，選擇**基本設定(General Setup)**。再選擇第一子網路作爲 **RIP 協定控制(RIP Protocol Control)**，然後點選**確定(OK)**按鈕。

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。

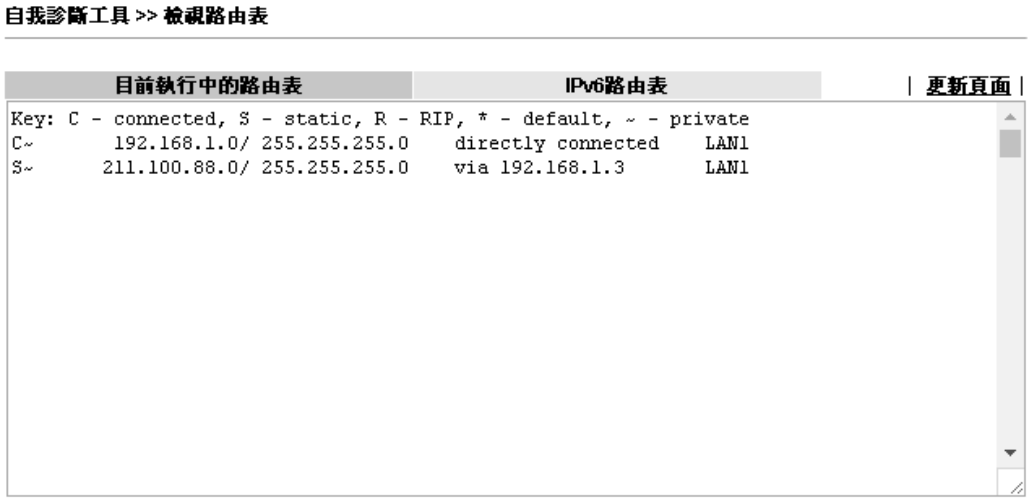
2. 在**區域網路(LAN)**群組中，選擇固定路由**(Static Route)**，按索引編號 1 勾選**啓用(Enable)**方塊， 請以下列數字新增一個固定路由，讓所有應前往 192.168.10.0 的封包都能透過 192.168.1.2 來轉送，接著按**確定(OK)**。



3. 回到**固定路由(Static Route Setup)**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(OK)**。



4. 按**自我診斷工具(Diagnostics)**中的**路由表(Routing Table)**檢查目前的路由表格。



4.2.4 VLAN (虛擬區域網路)

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

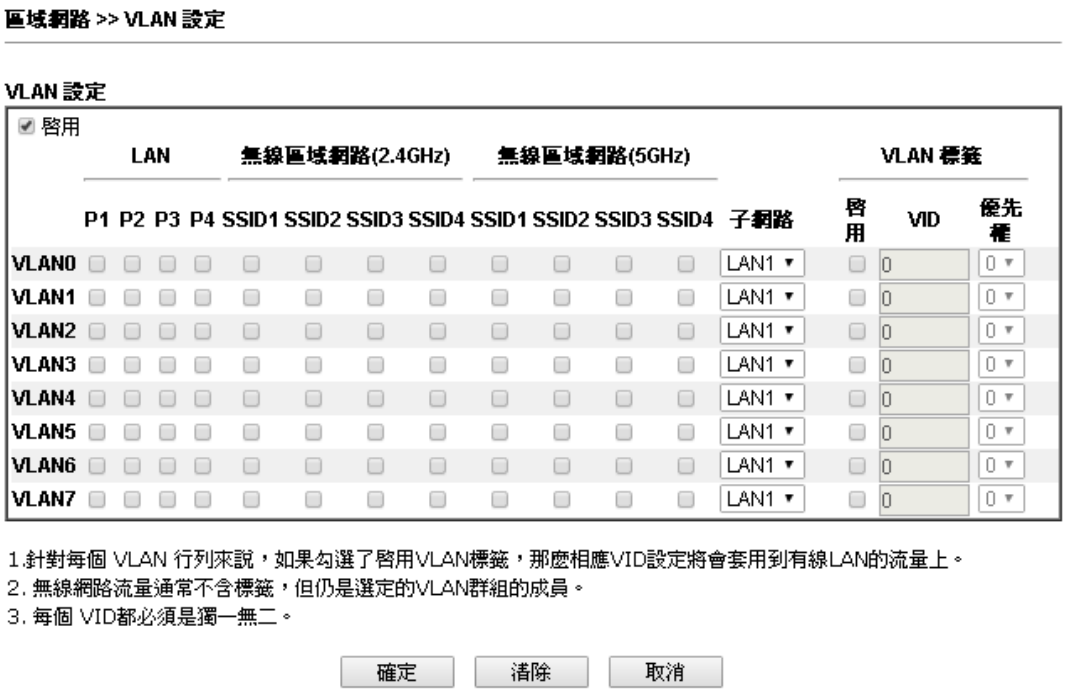
以標籤爲主的 VLAN(Tagged VLAN)

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

以埠口爲主的 VLAN(Port-Based VLAN)

相對於以標籤(Tag)爲主的 VLAN 以標籤來群組用戶，以埠口爲主的 VLAN 使用的是實體的 LAN 埠口(P1 ~ P5)來區分用戶端至不同的 VLAN 群組上。

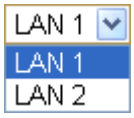
VLAN（虛擬區域網路）的功能提供您一個方便的方式，藉由群組實體通訊埠上的連結主機達到管理的目的。請開啓**區域網路>>VLAN (LAN>>VLAN)**，可出現如下頁面，勾選**啓用(Enable)**方塊啓動 VLAN 功能。



注意: 本頁設定僅能套用於 LAN 埠口而非 WAN 埠口。

可用設定說明如下：

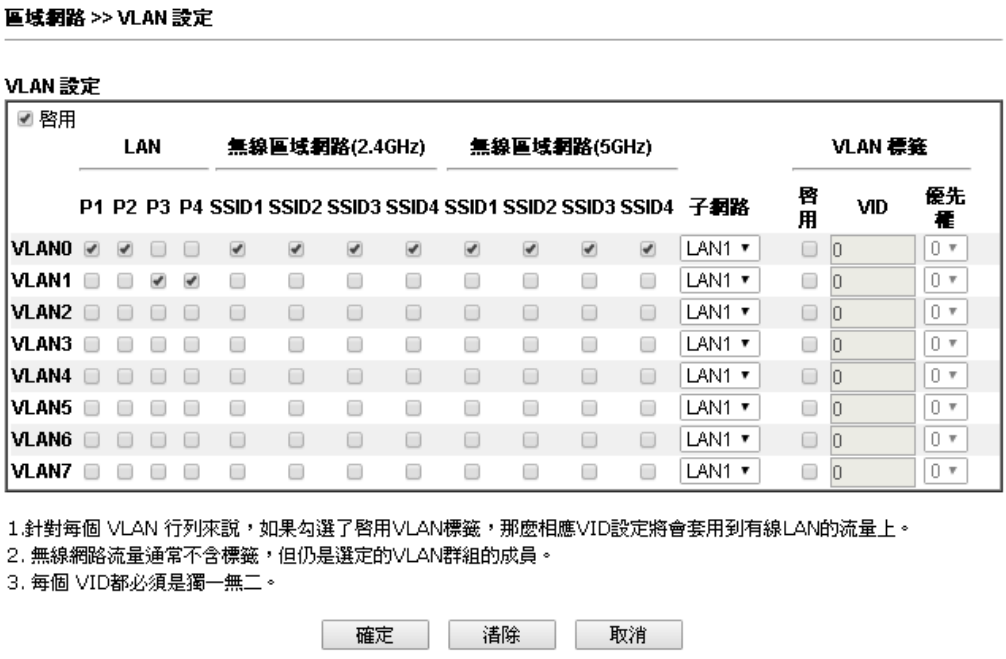
項目	說明
啓用(Enable)	勾選此框啓用 VLAN 設定。
LAN	**P1 – P4 –** 勾選準備納入此 VALN 群組下的 LAN 埠口。
無線區域網路(2.4GHz) (Wireless LAN (2.4GHz))	**SSID1 – SSID4 –** 勾選準備納入此 VLAN 群組下的 SSID 方框。

無線區域網路(5GHz) **(Wireless LAN (5GHz))**	**SSID1 – SSID4 –** 勾選準備納入此 VLAN 群組下的 SSID 方框。
子網路	選擇其中一個埠口讓選定的 VLAN 僅對應至此。例如，LAN1 指定爲 VLAN0，就表示在 VLAN0 底下的電腦可透過此子網來取得 IP 位址。 
VLAN 標籤 **(VLAN Tag)**	**啓用(Enable)** – 勾選此框啓用 VLAN 標籤功能。 區域網路中向外傳送的封包，路由器將指定 VLAN 號碼至全部封包上。 請輸入標籤值並指定其優先權。 **VID** – 輸入 VLAN ID 號碼值，範圍是 0 到 4095。 **優先權(Priority)** – 選擇此 VLAN 的優先權，範圍是 0 到 7。

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

新增或移除 VLAN，請參考下述範例:

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。

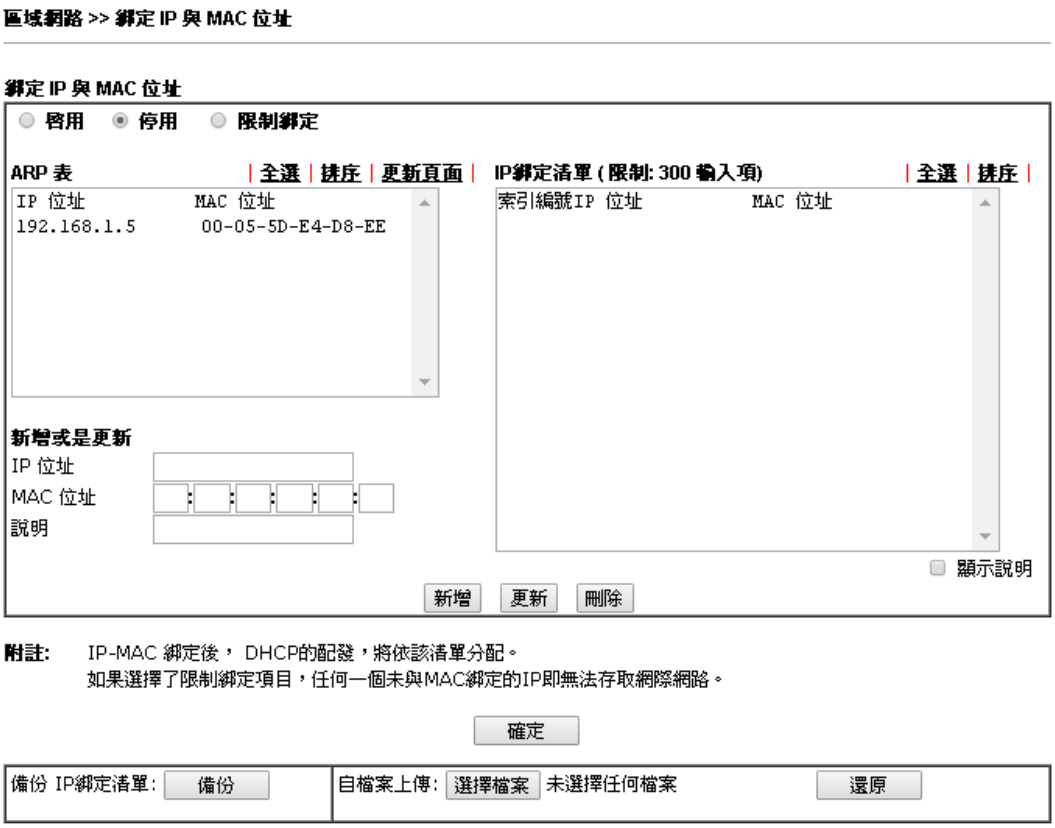


3. 如要移除某條 VLAN，請將該條 VLAN 的選定框全部移除，然後按**確定(OK)**即可。

4.2.5 綁定 IP 與 MAC 位址(Bind IP to MAC)

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(LAN)**並選擇**綁定 IP 與 MAC 位址(Bind IP to MAC)**開啓設定網頁。



可用設定說明如下：

項目	說明
啓用(Enable)	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(Disable)	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(Strict Bind)	按此鈕封鎖未列在 IP 綁定清單中的 IP/MAC 位址連線。
ARP 表(ARP Table)	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(Select All)	按此連結選擇表格內全部內容。
排序(Sort)	按此連結將表格內容按照 IP 位元址重新排序。
更新頁面(Refresh)	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。

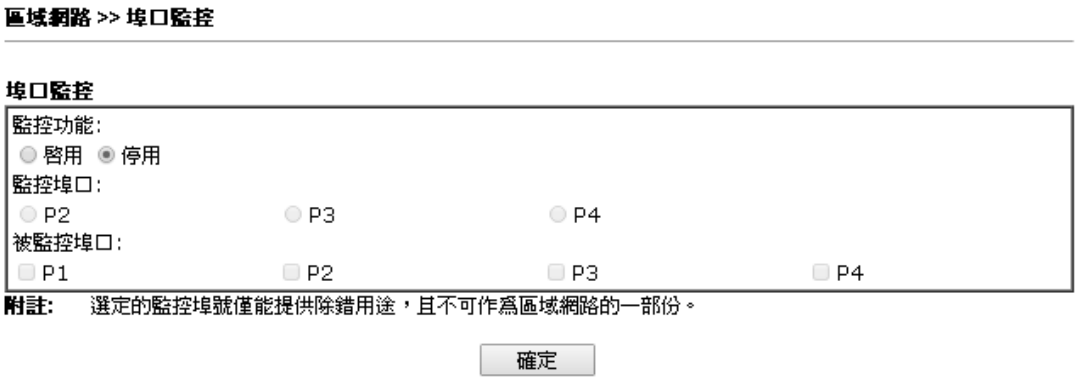
新增或是更新 **(Add or Update)**	**IP 位址**－輸入 IP 位址以作爲指定 MAC 位址之用。 **MAC 位址** －輸入 MAC 位址以便與指定的 IP 位址綁在一起。
IP 綁定清單 **(IP Bind List)**	顯示綁定 IP 至 MAC 資訊清單。
新增 (Add)	允許您將 ARP 表格中所挑選的或是在新增和編輯上所輸入的 IP/MAC 位址新增至 **IP 綁定清單**上。
更新 (Update)	允許您編輯或修正先前所建立的 IP 位址和 MAC 位址。
刪除 (Delete)	您可以刪除 **IP 綁定清單**上任何一個項目，選擇您想刪除的項目然後按**刪除**按鈕，選定的項目將自 **IP 綁定清單**上刪除。
備份(Backup)	將設定檔儲存成檔案。
還原(Restore)	將原先已存之設定檔套用至本頁。

附註: 在您選擇**限制綁定(Strict Bind)**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。

4.2.6 埠口監控(LAN Port Mirror)

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

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



可用設定說明如下：

項目	說明
監控功能 **(Port Mirror)**	按下**啓用**可啓動此功能，或是按下**停用**停止此功能。

監控埠口 (Mirror Port)	選擇任一埠口來檢視來自受控埠口的流量。
被監控埠口 (Mirrored port)	.選擇必須受到監控的埠口，可多選。

在您完成上述的設定之後，請按**確定(OK)**按鈕來啓動設定。

4.2.7 客製化入口網站設定(Web Portal Setup)

本頁可讓您設定數個設定檔，利用指定 URL 的方式，讓無線用戶/LAN 用戶在登入網際網路時連結至指定的頁面。亦即不論該用戶的目的爲何，都會先被強制導入此頁所指定的網頁。換句話說，若公司行號想要爲其產品對用戶進行廣告宣傳，就可利用此頁面達到不錯的效果。

每個項目說明如下：

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

如要設定設定檔，請按下任一索引編號連結開啓如下設定頁面：

可用設定說明如下：

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

在您完成上述的設定之後，請按**確定(OK)**按鈕來啓動設定。

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。

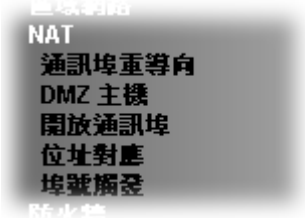
當封包之目的地位址爲網路上某個伺服器時，會先送到路由器，路由器即改變其來源位址，成爲真實 IP 位址，並透過真實通訊埠傳送出去。同時，路由器在連線數表格中列出清單，以記錄位址與通訊埠對應的相關資訊，當伺服器回應時，資料將直接傳回路由器的真實 IP 位址。

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。

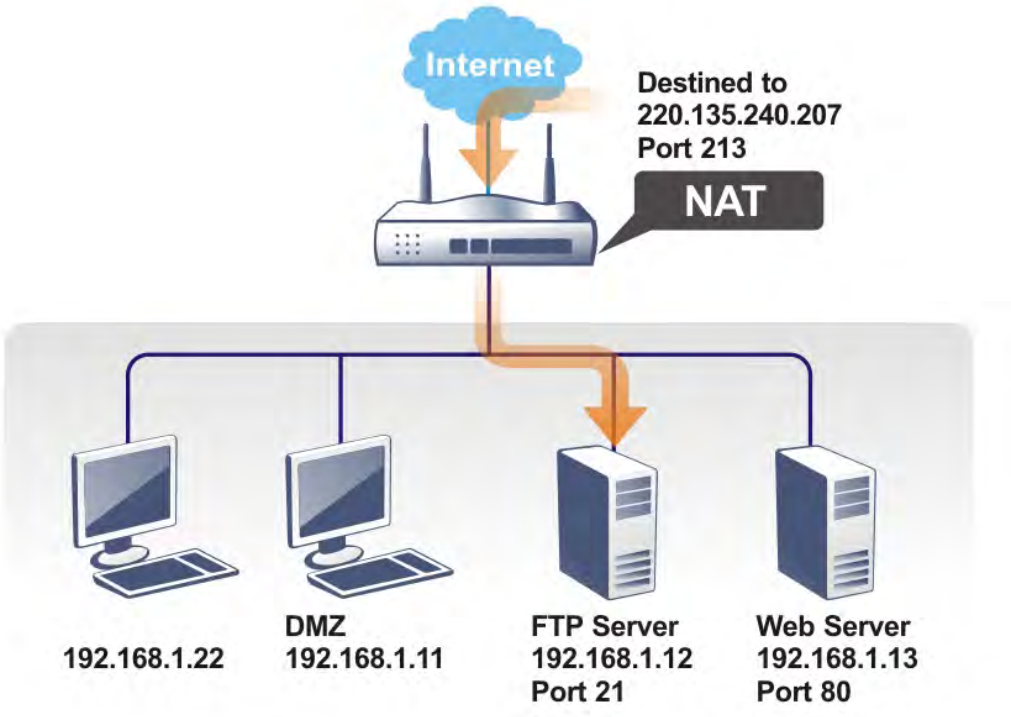
在 NAT 頁面中，您將可看見以 RFC-1918 定義的虛擬 IP 位址，通常我們會使用 192.168.1.0/24 子網路給予路由器使用。就如前所提及的一般，NAT 功能可以對應一或多個 IP 位址和/或服務通訊埠到不同的服務上，換句話說，NAT 功能可以利用通訊埠對應方式來達成。

下圖爲 NAT 功能項目：



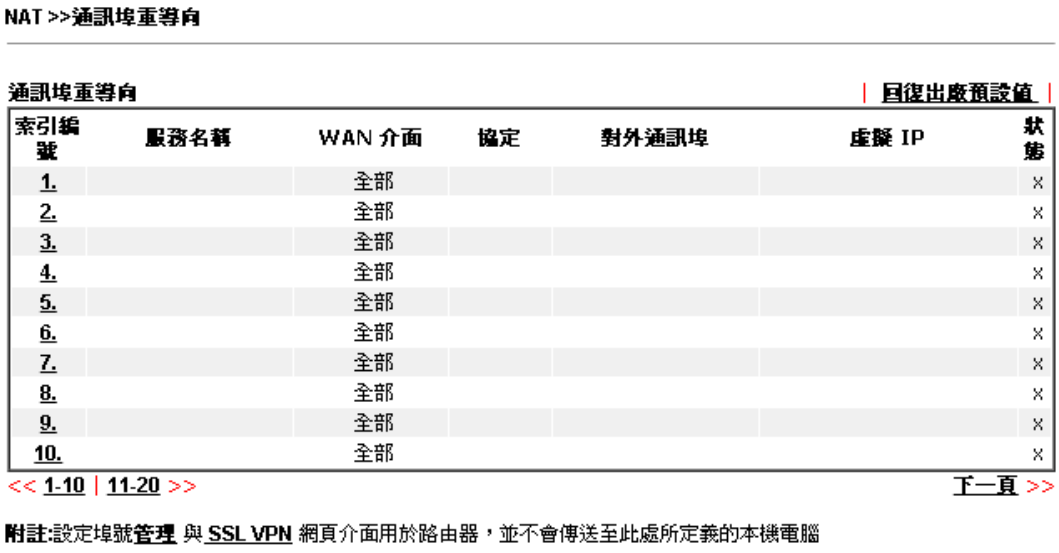
4.3.1 通訊埠重導向(Port Redirection)

通訊埠重導向通常是爲了本地區域網路中的網頁伺服器、FTP 伺服器、E-mail 伺服器等相關服務而設定，大部分的情形是您需要給每個伺服器一個真實 IP 位址，此一真實 IP 位址/網域名稱可以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。



可用設定說明如下：

項目	說明
索引編號(Index)	顯示設定檔的編號。
服務名稱(Service Name)	顯示網路服務的說明。
WAN 介面(WAN Interface)	顯示設定檔使用的 WAN IP 位址。
協定(Protocol)	顯示使用的協定類別（TCP 或是 UDP）。
對外通訊埠(Public Port)	顯示將被導引至指定的內部主機的虛擬 IP 及埠口的埠號。
虛擬 IP(Private IP)	顯示提供此服務之內主機的 IP 位址。
狀態(Status)	顯示設定檔目前是啓用(v) 或是停用 (x)。

按下索引編號下的號碼連結，進入次層之設定頁面:

可用設定說明如下：

項目	說明
啓用(Enable)	勾選此方塊啓用此通訊埠重導向設定。
模式(Mode)	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(Range)**。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(Service Name)	輸入特定網路服務的名稱。
通訊協定(Protocol)	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 (Public Port)	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(Range)**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 (Private 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 (Private Port)	指定內部主機提供服務之虛擬通訊埠號。

在您完成上述的設定之後，請按**確定(OK)**按鈕來儲存設定。

注意路由器有其內建服務(伺服器)諸如 Telnet、HTTP 和 FTP，因爲這些服務(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。

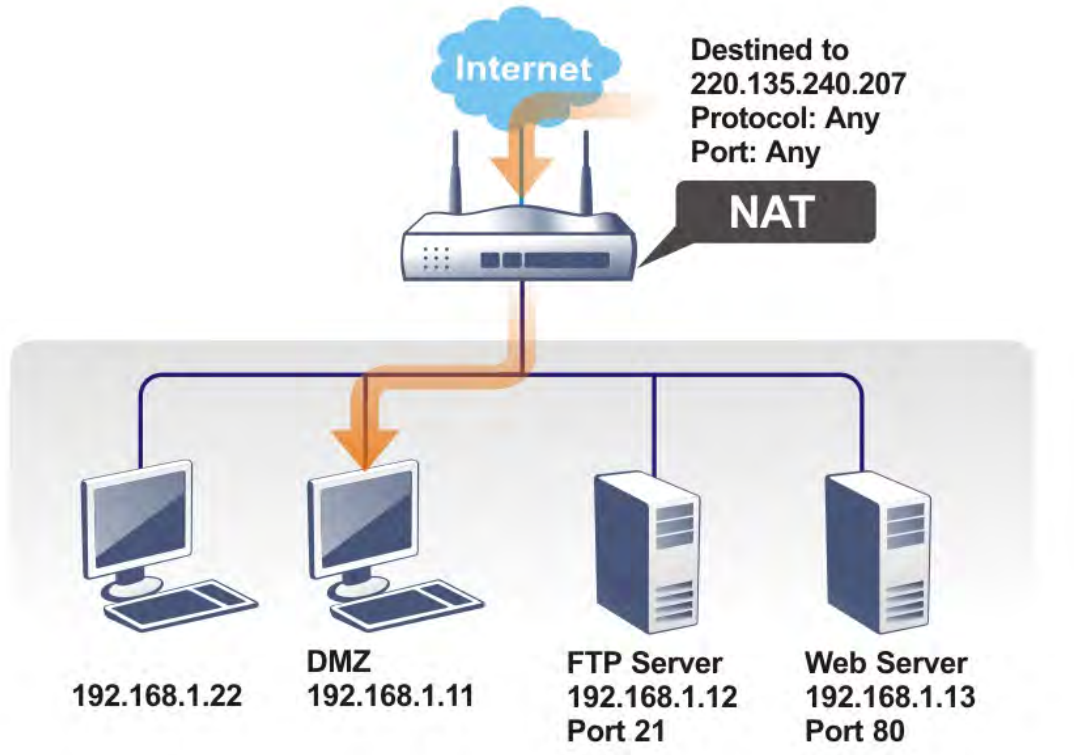
例如，路由器的內建網頁設定給予的設定值是埠號 80，它可能造成與本地網路中網頁伺服器 http://192.168.1.13:80 產生衝突，因此您需要改變路由器的 **http** 通訊埠號，除了 80 以外任何一種都可以（例如 8080），來防止衝突發生。請改登入管理者模式並在系統維護群中的管理設定做調整，接著您可在 IP 位址尾端加入 8080 (如 http://192.168.1.1:8080 而非僅只通訊埠號 80)來進入管理畫面。

系統維護 >> 管理


IPv4 管理設定
IPv6 管理設定
路由器名稱
預設值:停用自動登出
網際網路連線控制
允許從網際網路管理
允許之網域名稱
FTP 通訊埠
HTTP 通訊埠
HTTPS 通訊埠
Telnet 通訊埠
TR-069伺服器
SSH 通訊埠
停用來自外部網際網路的PING
來自網際網路的連線清單
清單
IP
子網路遮罩
1
2
3
管理通訊埠設定
使用者定義通訊埠
預設通訊埠
Telnet 通訊埠 23 (預設值: 23)
HTTP 通訊埠 80 (預設值: 80)
HTTPS 通訊埠 443 (預設值: 443)
FTP 通訊埠 21 (預設值: 21)
TR-069 埠號 8069 (預設值: 8069)
SSH 通訊埠 22 (預設值: 22)
TLS/SSL 加密設定
啓用 SSL 3.0
裝置管理
回應給外接裝置
確定

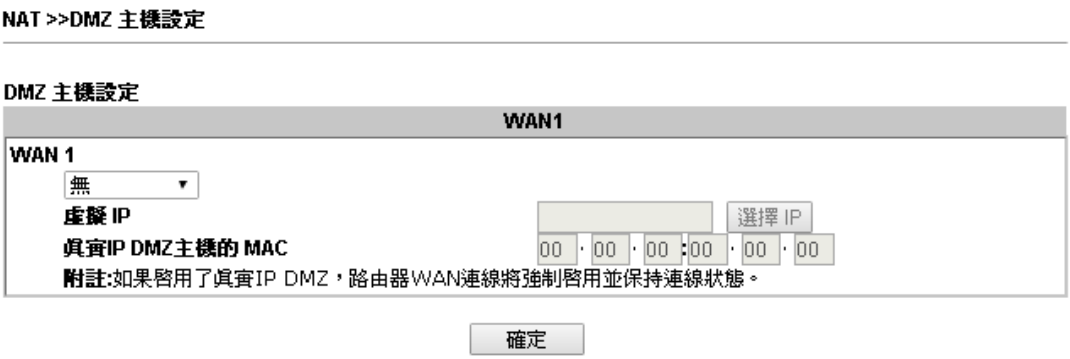
4.3.2 DMZ 主機設定(DMZ Host)

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

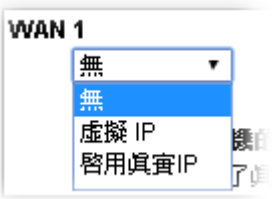
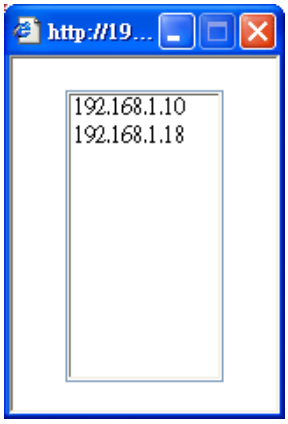
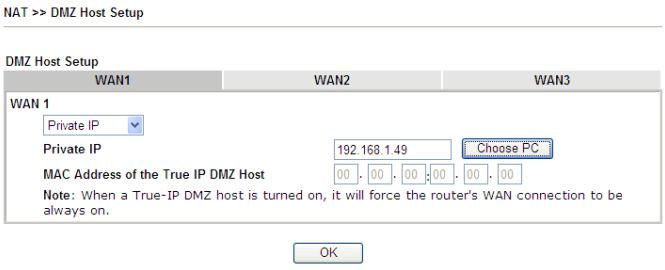


注意：NAT 固有的安全性屬性在您設定 DMZ 主機時稍微被忽略了，建議您另外新增額外的過濾器規則或是第二組防火牆。

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

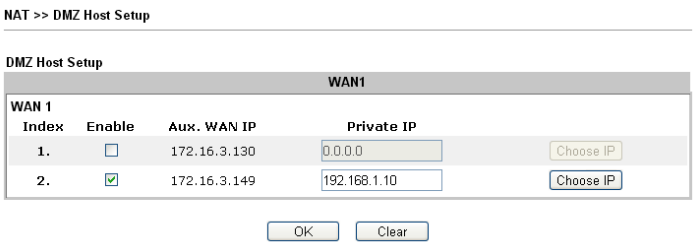


可用設定說明如下：

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

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(WAN Alias)**，您將可在此頁面發現**輔助 WAN IP(Aux. WAN IP)**項目。

可用設定說明如下：

項目	說明
啓用(Enable)	勾選此項以啓動 DMZ 主機功能。
輔助 WAN IP (Aux. WAN IP)	顯示輔助 WAN IP 的位址。
虛擬 IP Private IP)	輸入 DMZ 主機的虛擬 IP 位址，或是按**選擇 IP** 開啓另一頁面來選擇。
選擇 IP (Choose IP)	按下此鈕後，如下視窗立即跳出。此視窗包含您的區域網路中全部主機的虛擬 IP 位址清單，請自清單中選擇一個虛擬 IP 位址作爲 DMZ 主機。  當您已經從上面的視窗選好了虛擬 IP 位址時，該 IP 位址將會顯示在下面的螢幕上，請按**確定(OK)**儲存這些設定。 

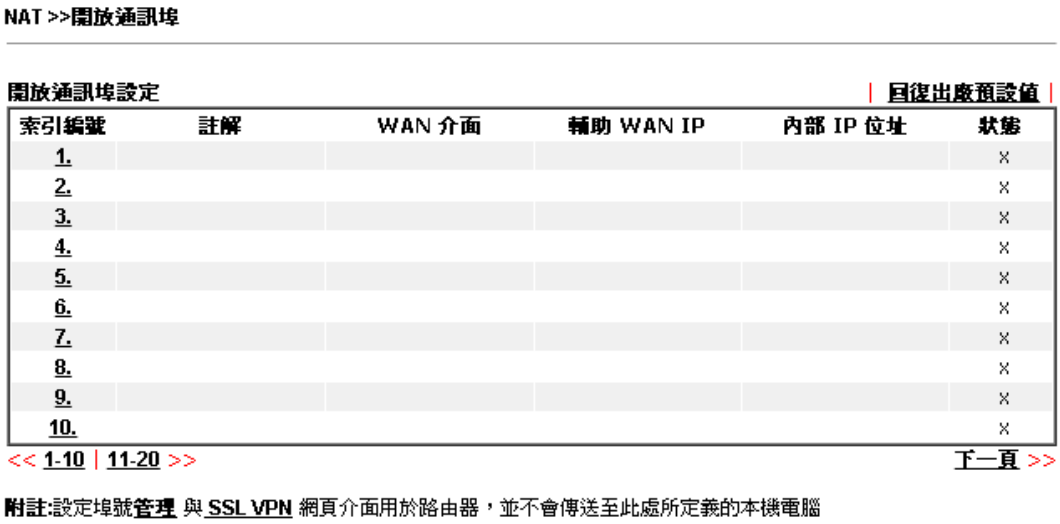
在您完成上述的設定之後，請按**確定(OK)**按鈕來儲存設定。

4.3.3 開放通訊埠(Open Ports)

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(Open Ports)**連結開啓下面的網頁。


NAT >>開放通訊埠

開放通訊埠設定 | 回復出廠預設值 |

索引編號	註解	WAN 介面	輔助 WAN IP	內部 IP 位址	狀態
1.					x
2.					x
3.					x
4.					x
5.					x
6.					x
7.					x
8.					x
9.					x
10.					x

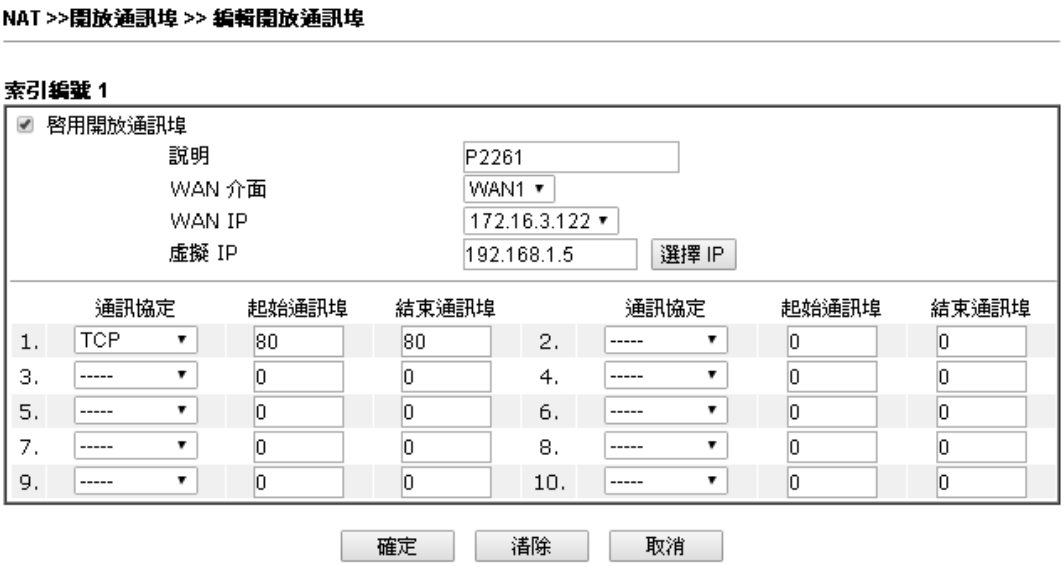
<< 1-10 | 11-20 >> 下一頁 >>

附註:設定埠號管理 與 SSL VPN 網頁介面用於路由器，並不會傳送至此處所定義的本機電腦

可用設定說明如下：

項目	說明
索引編號 (Index)	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(Comment)	指定特定網路服務的名稱。
WAN 介面 (WAN Interface)	顯示此埠號設定檔使用的 WAN 介面。
輔助 WAN IP (Aux. 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 (Local IP Address)	顯示提供此項服務之本地主機的 IP 位址。
狀態 (Status)	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。



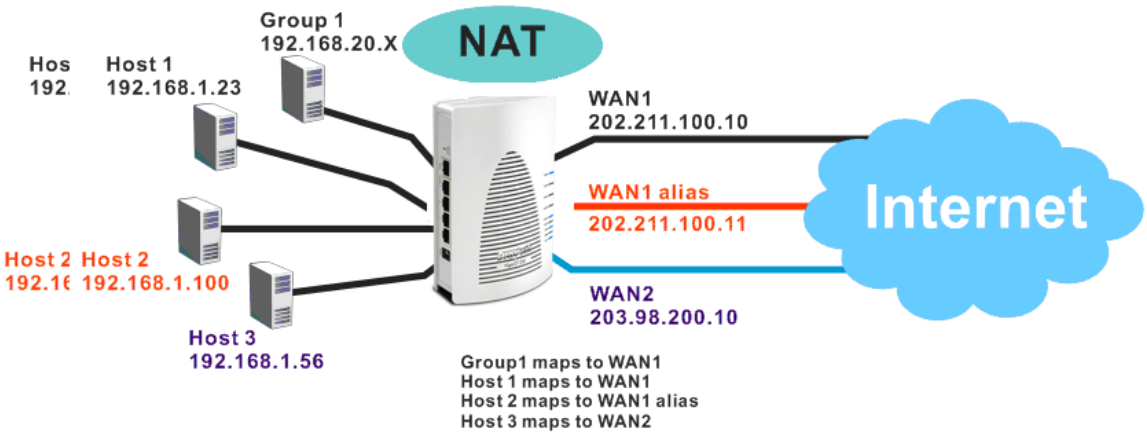
可用設定說明如下：

項目	說明
啓用開放通訊埠 (Enable Open Ports)	勾選此項以啓動此功能。
說明 (Comment)	請爲所定義的網路應用/服務命名。
WAN 介面 (WAN Interface)	指定該項設定之 WAN 介面。
WAN IP	如果您在**網際網路連線設定**選擇 **PPPoE/固定 IP/PPTP**，並且設定 **WAN 別名**，您將可在此頁面發現 **WAN IP** 項目。請自下拉式選項中選擇需要的 IP 位址。
虛擬 IP (Private IP)	**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 (Protocol)	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 (Start Port)	指定本機所提供之服務的開始通訊埠號。
結束通訊埠 (End Port)	指定本機所提供之服務的結束通訊埠號。

在您完成上述的設定之後，請按**確定(OK)**按鈕來儲存設定。

4.3.4 位址對應(Address Mapping)

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

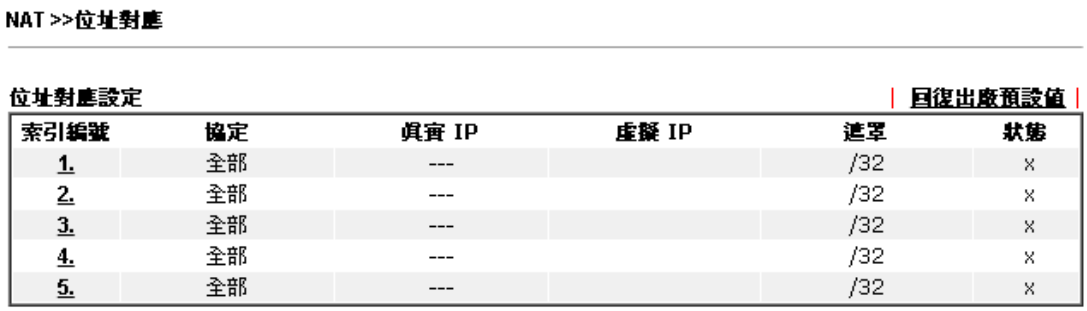


假設路由器的 WAN 端設定如下：

WAN1: 202.211.100.10, WAN1 別名: 202.211.100.11
WAN2: 203.98.200.10

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

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



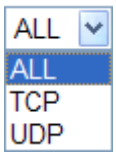
可用設定說明如下：

項目	說明
索引編號(Index)	指示您想要設定的設定檔號碼，您可以按索引編號連結進行編輯相關設定。
協定(Protocol)	顯示此位址對應使用的協定。

真實 IP(Public IP)	顯示此設定檔的真實 IP 位址。
虛擬 IP(Private IP)	顯示此設定檔的虛擬 IP 位址。
遮罩(Mask)	顯示此設定檔的子網遮罩。
狀態(Status)	顯示此設定檔是否啓用或是停用。

按索引連結號碼開啓如下的設定頁面。

可用設定說明如下：

項目	說明
啓用(Enable)	按此啓動此設定檔。
協定(Protocol)	指定傳送層及協定。 
WAN 介面 **(WAN Interface)**	選擇設定檔的 WAN 介面。
WAN IP	此爲 WAN 端擷取封包的來源 IP，由虛擬 IP 指定的 NAT 主機發送。下拉式清單含 WAN 介面 IP 與 WAN 別名 IP。
虛擬 IP **(Private IP)**	此爲 NAT 主機的來源 IP，用來傳送封包至 WAN 端。
子網遮罩 **(Subnet Mask)**	選擇適合虛擬 IP 位址的子網遮罩值。

在您完成上述的設定之後，請按**確定(OK)**按鈕來儲存設定。

4.3.5 埠號觸發(Port Triggering)

埠號觸發式開放通訊埠的變更版。二者最主要的差異是：

- 一旦按下確定按鈕，設定檔即開始生效，開放通訊埠下的埠口永遠呈現開啓狀態。
- 一旦按下確定按鈕，設定檔即開始生效，埠號觸發會在觸發條件符合時嘗試開啓相關埠口。

- 所有埠口的持續開放的時間端賴使用的通訊協定而定，預設時間顯示如下，相關數據可以利用 telnet 指令進行變更。

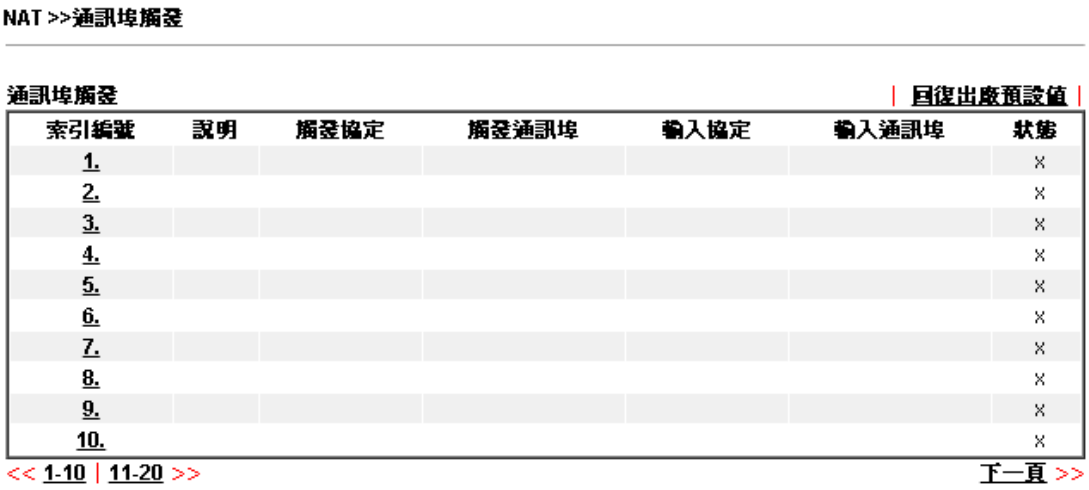
  TCP: 86400 秒

  UDP: 180 秒

  IGMP: 10 秒

  TCP WWW: 60 秒

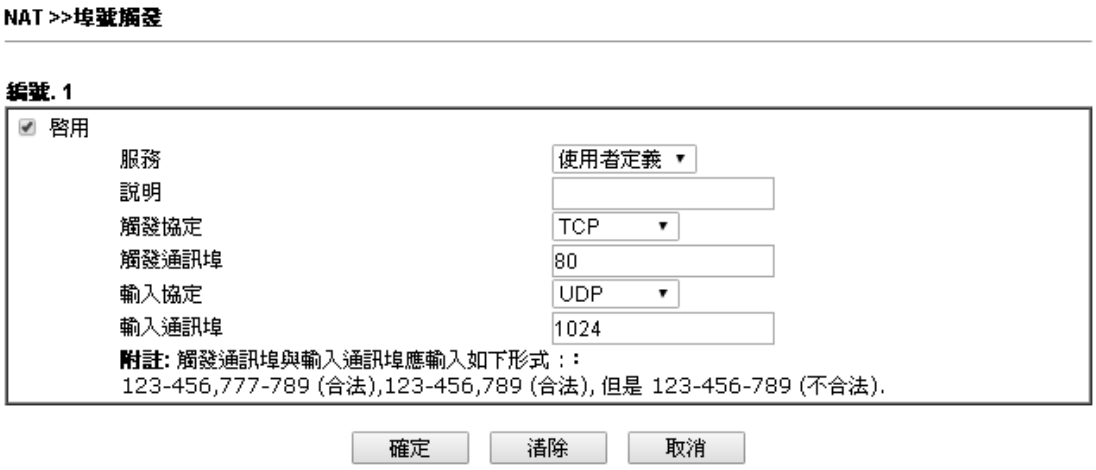
  TCP SYN: 60 秒



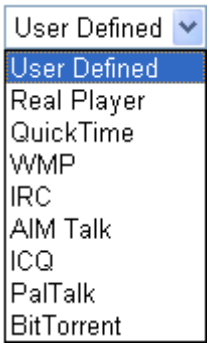
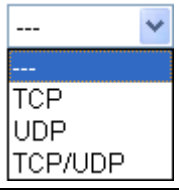
可用設定說明如下：

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

按下任一索引連結開啓設定頁面：



可用設定說明如下：

項目	說明
啓用(Enable)	勾選方框啓用此設定檔。
服務(Service)	您可以選擇事先定義的服務套用到此觸發設定檔。 
說明(Comment)	輸入此設定檔需要特別說明的內容。
觸發協定 (Triggering Protocol)	針對此觸發設定檔選擇適當的協定（如 TCP, UDP 或 TCP/UDP)。 
觸發通訊埠 (Triggering Port)	輸入觸發設定檔的埠號或是埠號範圍。
輸入協定 (Incoming Protocol)	當收到觸發封包時，輸入封包將會利用此處所選擇的協定來處理。 
輸入通訊埠	輸入封包的埠號或是埠號範圍。

(Incoming Port)	

在您完成上述的設定之後，請按**確定(OK)**按鈕來儲存設定。

4.4 防火牆(Firewall)

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：

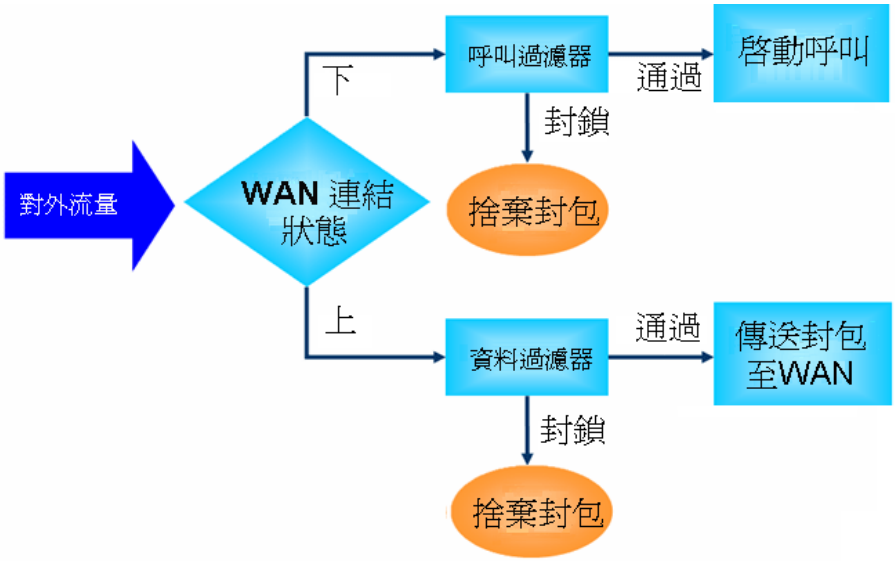
- 用戶設定 IP 過濾器(呼叫過濾器/資料過濾器)
- Stateful Packet Inspection (SPI): 追蹤封包並阻擋未經要求而流入的資料
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS)攻擊防禦

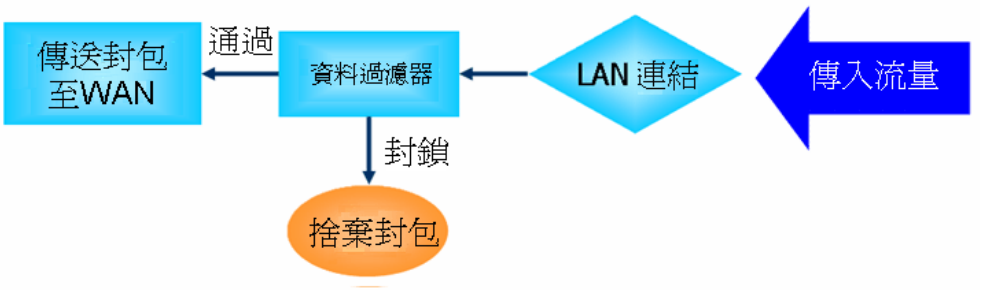
IP 過濾器

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 Defense)

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

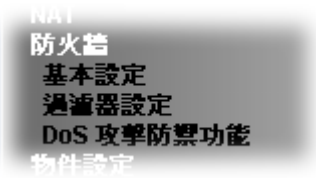
DoS 攻擊防禦功能的引發是以 Vigor 路由器的攻擊特徵值資料庫爲基礎，執行每一個封包的檢查，任何可能重複產生以癱瘓主機之惡意封包，在安全的區域網路中都將嚴格阻擋，如果您有設定系統紀錄伺服器，那麼系統紀錄訊息也會傳送警告資訊給您。

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：

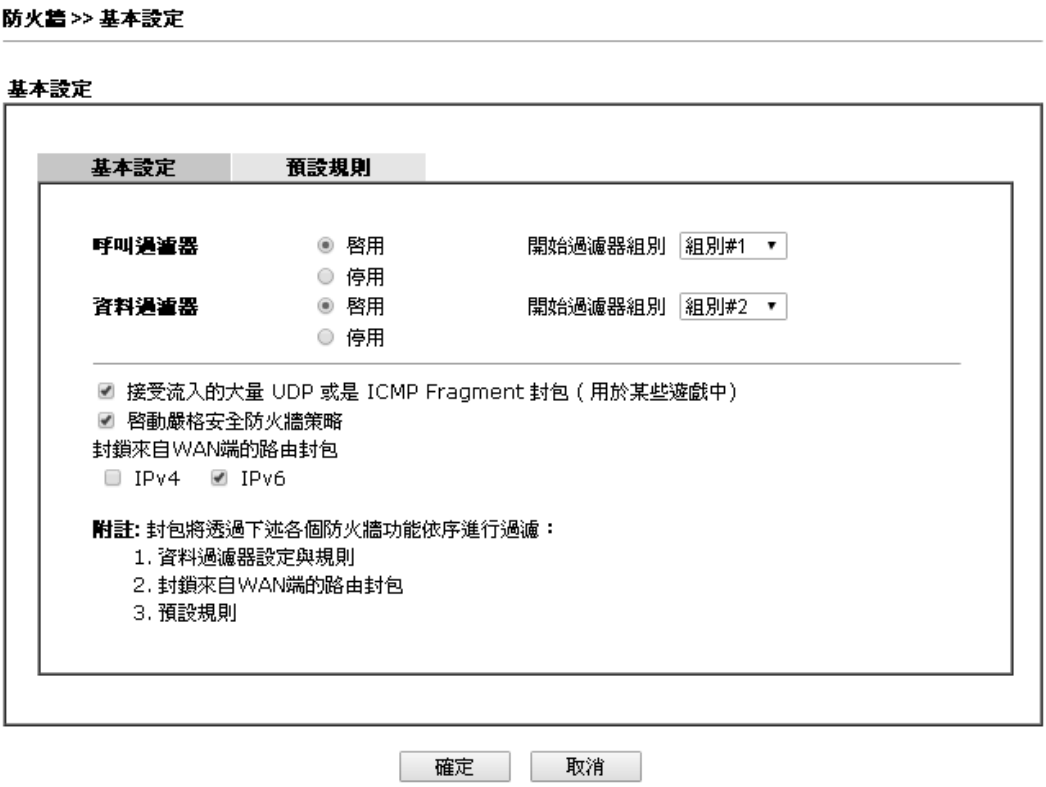


4.4.2 基本設定(General Setup)

基本設定(General Setup)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(Call Filter)**或**資料過濾器(Data Filter)**。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(Apply IP filter to VPN incoming packets)**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(Accept incoming fragmented UDP packets)**。

4.4.2.1 基本設定頁面

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



可用設定說明如下：

項目	說明
呼叫過濾器(Call Filter)	選擇**啓用(Enable)**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(Data Filter)	選擇**啓用(Enable)**以啓動資料過濾器功能，並指定開始過濾器組別。

接受流入的大量 UDP 或是 ICMP Fragment 封包 (Accept large incoming…)	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(Accept large incoming fragmented UDP or ICMP Packets)**勾選此方塊後，您就可以在這些線上遊戲上悠遊。如果安全利害關係具有較高的重要性，您就不要啓動**接受流入的大量 UDP 或是 ICMP Fragment 封包(Accept large incoming fragmented UDP or ICMP Packets)**功能。
啓動嚴格安全防火牆策略 (Enable Strict Security Firewall)	爲了安全起見，路由器將會執行嚴格的資料傳輸安全性檢驗動作。 此功能在預設狀態下是啓用的，所有透過路由器傳送的封包都會經過防火牆過濾一番。如果防火牆系統（例如內容過濾伺服器）並未有任何回應（通過或是封鎖），那麼路由器防火牆會直接封鎖所有的封包。
封鎖來自 WAN 端的路由封包(Block routing packet from WAN)	通常，由 WAN 至 LAN 的 IPv6 網路連線數/流量是允許。 **IPv6** - 勾選此方塊讓路由器得以封鎖透過 IPv6 傳送過來的封包(自 WAN 到 LAN)，這個功能對於封鎖路由封包有效用，但是對於 NAT 過來的封包就沒有作用。 **IPv4** - 勾選此方塊讓路由器得以封鎖透過 IPv4 傳送過來的封包(自 WAN 到 LAN)，這個功能對於封鎖路由封包有效用，但是對於 NAT 過來的封包就沒有作用。

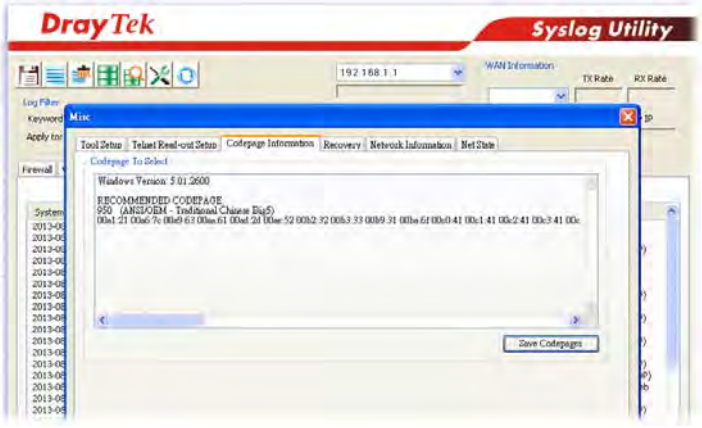
4.4.2.2 預設規則頁面(Default Rule)

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

可用設定說明如下：

項目	說明
過濾器(Filter)	本頁可是定預設規則. **通過(Pass) –** 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(Block) -** 所有的封包都不許通過路由器，且不需考慮**防火牆>>過濾器**的設定內容。
連線數控制 (Sessions Control)	此處輸入的值爲全部的封包連線數，預設值爲 60000。
服務品質 (Quality of Service)	選擇一組 QoS 規則作爲防火牆規則，設定 QoS 細節資訊部分，請參考稍後的相關章節。 
應用程式管控 (APP Enforcement)	選擇應用程式管控設定檔來封鎖 IM/P2P 之類的應用，如果沒有任何設定檔可供選擇時，請從下拉式清單中選擇**建立新設定([Create New])**來建立一個新的設定檔。所有區域網路中的主機必須依循應用程式管控設定檔內的標準。有關詳細資訊，請參考**數位內容安全管理>>應用程式管控設定檔(CSM>> APP Enforcement)**章節。 因應疑難排解的需要，您可勾選 IM/P2P 紀錄方塊以便將資

	訊記錄起來，這些紀錄會傳送到 Syslog 伺服器，詳情請參考 **Syslog/郵件警告(Syslog/Mail Alert)**章節。
URL 內容過濾器 (URL Content Filter)	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(CSM>> URL Content Filter))** 中所建立），請務必先在**數位內容安全管理(CSM)> URL 內容過濾器**中設定一個設定檔，或是從下拉式選單中選擇[建立新檔]產生新的設定檔。因應疑難排解的需要，您可勾選紀錄方塊以便將資訊記錄起來，這些紀錄會傳送到 Syslog 伺服器，詳情請參考 **Syslog/郵件警告(Syslog/Mail Alert)**章節。
網頁內容過濾器 (Web Content Filter)	選擇一個**網頁內容過濾器**設定檔（在**數位內容安全管理 (CSM)>> 網頁內容過濾器**中所建立），請務必先在**數位內容安全管理(CSM)>> 網頁內容過濾器**中設定一個設定檔，或是從下拉式選單中選擇[建立新檔]產生新的設定檔。因應疑難排解的需要，您可勾選紀錄方塊以便將資訊記錄起來，這些紀錄會傳送到 Syslog 伺服器，詳情請參考 **Syslog/郵件警告(Syslog/Mail Alert)**章節
DNS 過濾器 (DNS Filter)	選擇一組 DNS 過濾器設定檔(於**數位內容安全管理>>DNS 過濾器**頁面中建立)，在**數位內容安全管理>>網頁內容過濾器設定檔(CSM>> Web Content Filter)**頁面中至少要先建立一個設定檔案以供選擇，或是從下拉式清單中選擇 DNS 過濾器連結以重新建立新的設定檔。
進階設定 (Advance Setting)	按**編輯(Edit)**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(Codepage) -** 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。



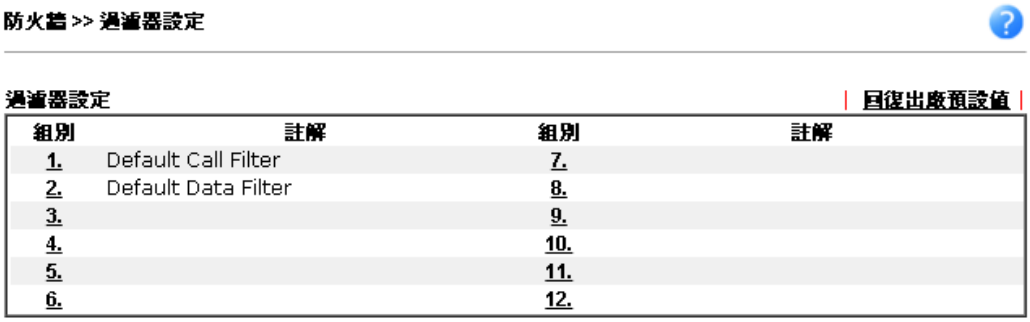
視窗大小(Window size) – 決定 TCP 協定的大小(0~65535)，數值越大，成效越佳，不過網路會較爲不穩定，小的數值比較適合穩定網路。

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

在您完成上述的設定之後，請按**確定(OK)**按鈕來儲存設定。

4.4.3 過濾器設定(Filter Setup)

按**防火牆(Firewall)**並選擇**過濾器設定(Filter Setup)**以開啓如下的設定網頁。

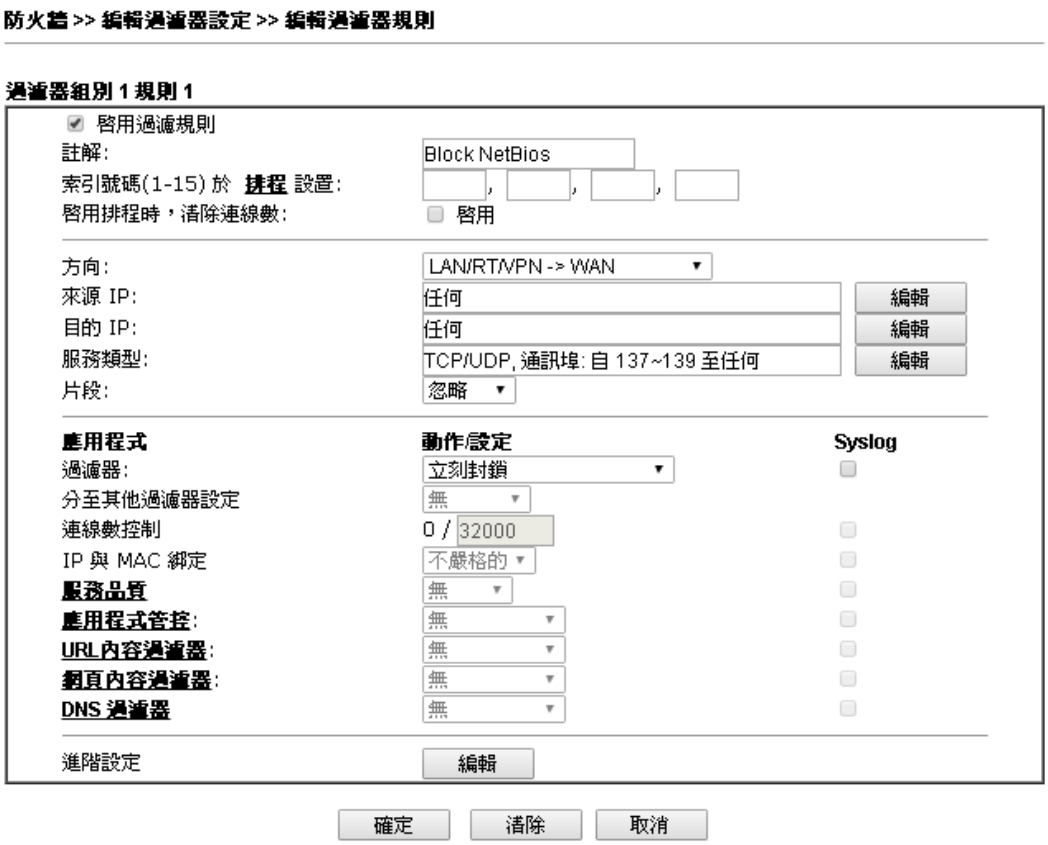


如果要新增一個過濾器，請按組別下方的數字按鈕以便編輯個別設定。如下的頁面將立即出現，每一個過濾器都含有 7 組規則，請按規則按鈕編輯每個規則，勾選**啓用(Active)**則可啓動該項規則。

可用設定說明如下：

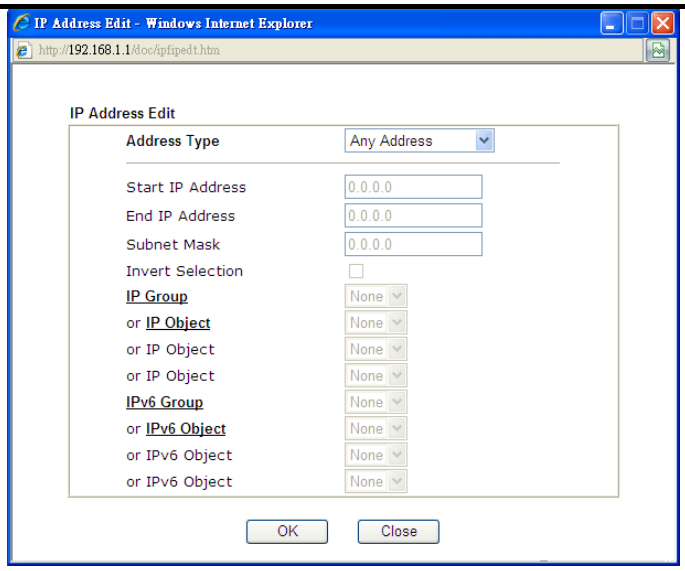
項目	說明
過濾器規則 (Filter Rule)	請按號碼按鈕(1 ~ 7)編輯過濾器的規則，按下此鈕可以開啓過濾器規則網頁，有關詳細的資訊，請參考稍後的說明。
啓用(Active)	啓動或是關閉此項過濾規則。
註解(Comment)	輸入過濾規則註解說明，最大長度可以達到 23 個字元。
上移/下移 (Move Up/Down)	使用上下連結來移動過濾器規則的順序。
下一個過濾器組別 (Next Filter Set)	設定前往下一個執行的過濾器連結，請勿讓多個過濾器設定形成一個迴路。

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

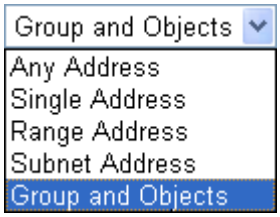


可用設定說明如下：

項目	說明
啓用過濾規則 (Check to enable the Filter Rule)	勾選此項目以啓動過濾規則。
註解(Comments)	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) (Index(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。
啓用排程時，清除連線數 (Clear sessions when schedule ON)	勾選此方框可依據上述排程設定期間清除連線數資料。
方向(Direction)	設定封包流向的方向，此項設定僅適用**資料過濾器**，對於呼叫過濾器而言，這項設定是不適用的。 LAN/DMZ/RT/VPN -> WAN LAN/DMZ/RT/VPN -> WAN WAN -> LAN/DMZ/RT/VPN LAN/DMZ/RT/VPN -> LAN/DMZ/RT/VPN **注意:** RT 表示第二個子網的路由網域或是其他 LAN。
來源/目的 IP (Source/Destination IP)	按下**編輯(Edit)**進入如下的畫面，選擇來源/目標 IP 或是 IP 範圍。



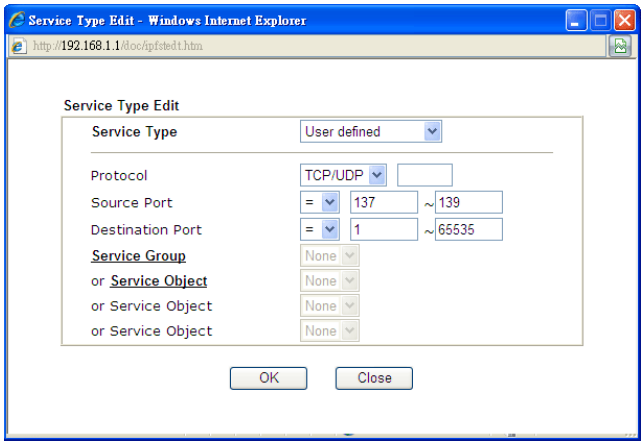
欲手動設定 IP 位址，請選擇**任何位址/單一位址/範圍位址/子網位址(Any Address/Single Address/Range Address/Subnet Address)**作爲位址類型，並在此對話方塊輸入相關內容。此外，如果您想要在定義的群組或物件上使用 IP 範圍，請勾選**群組及物件(Group and Objects)**。



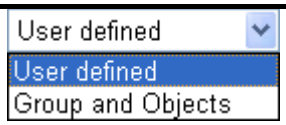
從 **IP 群組(IP Group)**下拉式清單中，選擇您需要應用的群組，或是使用 **IP 物件(IP Object)**下拉式清單，選擇您所需要的物件。

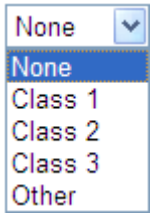
服務類型 (Service Type)

按**編輯(Edit)**進入如下的畫面，以選擇適合之服務類型。



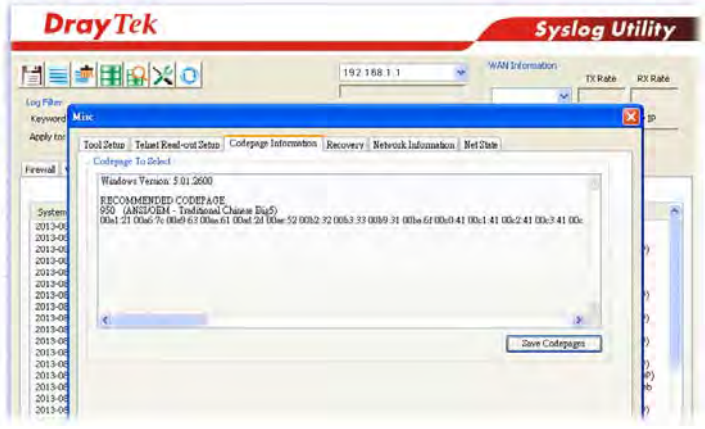
欲手動設定服務類型，請選擇**使用者自訂(User defined)**做爲服務類型，並輸入相關的設定資料，此外如果您想要使用群組或是物件中所定義的服務類型，請選擇**群組與物件**作爲服務類型。

	 **協定(Protocol)** -指定本過濾器規則套用的協定。 **來源/目標通訊埠(Source/Destination Port)** – ***(=)*** – 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 (Service Group/Object)**- 使用下拉式選項選擇所需的項目。
片段(Fragments)	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(*Don't care*)** - 不論是怎樣的片端封包，系統皆不採取行動。 **無片段(*Unfragmented*)** - 應用規則至無片段之封包上。 **片段(*Fragmente*)**- 應用規則至片段之封包上。 **太短了(*Too Short*)** - 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(Filter)	指定系統針對符合規則之封包所採取的行動。 **立刻通過(Pass Immediately)**- 符合規則之封包可立即通過。 **立刻封鎖(Block Immediately)** - 系統封鎖符合規則之封包。 **若無符合其於規則即通過(Pass If No Further Match)** - 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(Block If No Further Match)** - 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 (Branch to other Filter Set)	封包符合過濾器規則，下一個過濾器規則將分至指定之過濾器設定。請自下拉式選項中選擇下一個過濾器規則以便做分支動作，要注意路由器將會採用指定之過濾器規則，且絕對不會回到先前所設定之過濾器規則。
連線數控制 (Sessions Control)	此處輸入的值爲全部的封包連線數，預設值爲 60000。
IP 與 MAC 綁定 (MAC Bind IP)	**嚴格的(Strict)** – 讓 IP 物件中設定來源 IP 與目標 IP 中的 MAC 位址與 IP 位址設定完全綁定，並用於此過濾器規則。

	不嚴格的(No-Strict) -.此指完全沒有限制。
服務品質 **(Quality of Service)**	選擇一組 QoS 規則作爲防火牆規則，設定 QoS 細節資訊部分，請參考稍後的相關章節。 
應用程式管控 **(APP Enforcement)**	選擇應用程式管控設定檔來封鎖 IM/P2P 之類的應用，如果沒有任何設定檔可供選擇時，請從下拉式清單中選擇**建立新設定([Create New])**來建立一個新的設定檔。所有區域網路中的主機必須依循應用程式管控設定檔內的標準。有關詳細資訊，請參考**數位內容安全管理>>應用程式管控設定檔(CSM>> APP Enforcement)**章節。 因應疑難排解的需要，您可勾選 IM/P2P 紀錄方塊以便將資訊記錄起來，這些紀錄會傳送到 Syslog 伺服器，詳情請參考 **Syslog/郵件警告(Syslog/Mail Alert)**章節。
URL 內容過濾器 **(URL Content Filter)**	選擇一個 **URL 內容過濾器**設定檔（在**數位內容安全管理(CSM)>> URL 內容過濾器**中所建立），請務必先在**數位內容安全管理(CSM)> URL 內容過濾器**中設定一個設定檔，或是從下拉式選單中選擇[建立新檔]產生新的設定檔。因應疑難排解的需要，您可勾選紀錄方塊以便將資訊記錄起來，這些紀錄會傳送到 Syslog 伺服器，詳情請參考 **Syslog/郵件警告(Syslog/Mail Alert)**章節。
網頁內容過濾器 **(Web Content Filter)**	選擇一個**網頁內容過濾器**設定檔（在**數位內容安全管理(CSM)>> 網頁內容過濾器**中所建立），請務必先在**數位內容安全管理(CSM)>> 網頁內容過濾器**中設定一個設定檔，或是從下拉式選單中選擇[建立新檔]產生新的設定檔。因應疑難排解的需要，您可勾選紀錄方塊以便將資訊記錄起來，這些紀錄會傳送到 Syslog 伺服器，詳情請參考 **Syslog/郵件警告(Syslog/Mail Alert)**章節。
DNS 過濾器 **(DNS Filter)**	選擇一組 DNS 過濾器設定檔(於**數位內容安全管理>>DNS 過濾器**頁面中建立)，在**數位內容安全管理>>網頁內容過濾器設定檔(CSM>> DNS Filter)**頁面中至少要先建立一個設定檔案以供選擇，或是從下拉式清單中選擇 DNS 過濾器連結以重新建立新的設定檔。
進階設定 **(Advance Setting)**	按**編輯(Edit)**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(Codepage) - 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 (Window size)– 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(Session timeout) – 設定連線數逾時時間可讓網路資源獲得較佳的運用，但是連續暫停僅適用於 TCP 協定，連線數逾時主要是針對符合防火強規則的資料流量而設定。

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

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

應用程式管控(APP Enforcement) – 勾選方塊以透過 IM/P2P 嚴格檢查所有傳輸檔案。

範例

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

4.4.4 DoS 攻擊防禦功能設定(DoS Defense Setup)

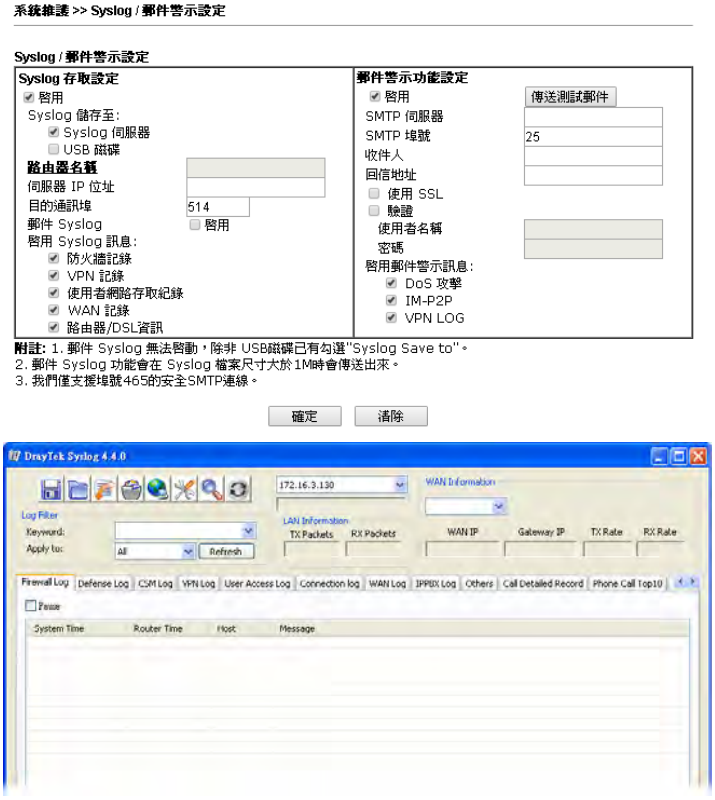
這是 **IP 過濾程式/防火牆**的次功能選項，有 15 種檢測/防禦功能類型，DoS 攻擊防禦功能的預設值是關閉的。

按**防火牆(Firewall)**並選擇 **DoS 攻擊防禦功能(DoS Defense)**開啓設定網頁。

可用設定說明如下：

項目	說明
啓用 DoS 防禦功能 (Enable Dos Defense)	勾選此項以啓動 DoS 攻擊防禦功能。
選擇全部 (Select All)	按下此鈕選擇下列全部項目。
啓用 SYN flood 攻擊防禦功能 (Enable SYN flood defense)	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 2000 個封包和 10 秒。
啓用 UDP flood 攻擊防禦功能 (Enable UDP flood defense)	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 2000 個封包和 10 秒。 **注意**：勾選此項之後，若有大量流量進出，機制啓動時，設備會無法上網，但內網仍可順利連到管理介面。
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，

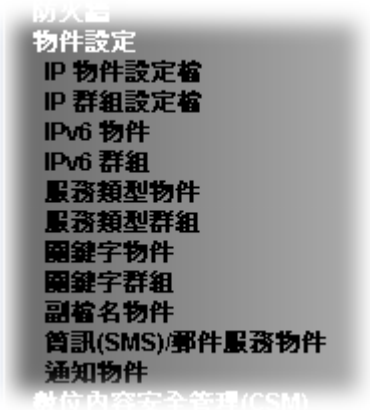
(Enable ICMP flood defense)	路由器便會於所設定之逾時期間，不再回應來自網際網路的 ICMP 需求。臨界值和逾時的預設值分別爲每秒 250 個封包和 10 秒。
啓用防禦通訊埠掃瞄偵測功能 **(Enable PortScan detection)**	通訊埠掃瞄藉由傳送大量封包到數個通訊埠，以嘗試找出未知服務所回應之內容來攻擊 Vigor 路由器。勾選此方塊啓動通訊埠掃瞄檢測功能，當利用通訊埠掃瞄臨界值速率而檢測出惡意探測之行爲時，Vigor 路由器將傳送警告訊息出去。臨界值的預設值爲每秒 2000 個封包。
封鎖 IP 選項 **(Block IP options)**	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 **(Block Land)**	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 **(Block Smurf)**	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 **(Block trace route)**	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 **(Block SYN fragment)**	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 **(Block Fraggle Attack)**	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 **(Block TCP flag 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 **(Block Tear Drop)**	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 **(Block Ping of Death)**	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 (Block ICMP Fragment)	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 (Block Unassigned Numbers)	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 (Warning Messages)	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。 

在您完成上述的設定之後，請按**確定(OK)**按鈕來儲存設定。

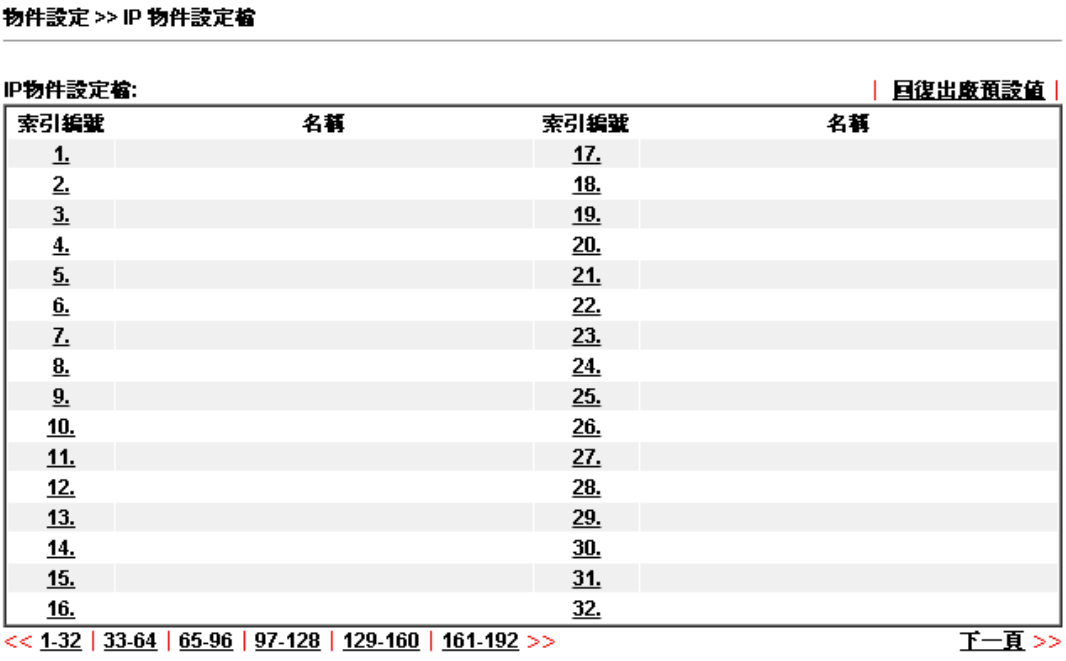
4.5 物件設定(Objects Settings)

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(IP Object)

您可設定 192 組不同條件的 IP 物件。

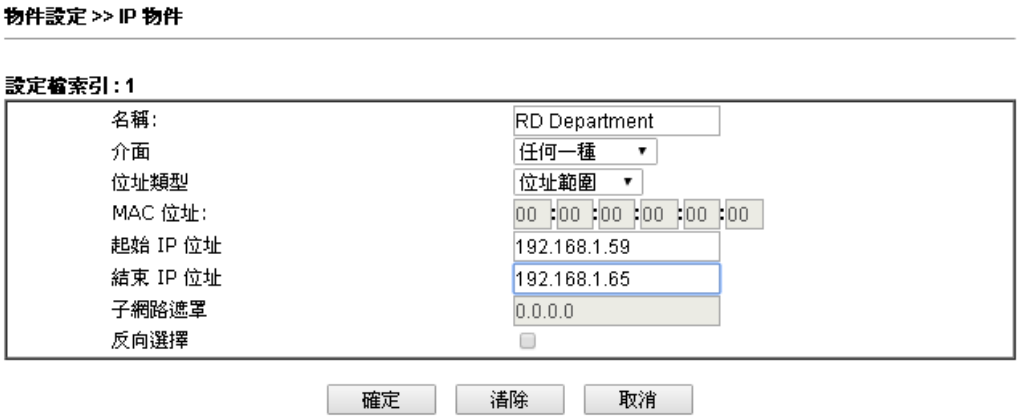


可用設定說明如下：

項目	說明
回復出廠預設值 (Set to Factory Default)	清除全部的設定資料。
索引(Index)	顯示您可以設定的設定檔索引編號。
名稱(Name)	顯示物件設定檔的檔名。

如欲建立新的設定檔，請依下述步驟進行：

1. 按下索引欄位下方的任一編號連結(例如 #1) 進入設定頁面。
2. 設定網頁顯示如下：

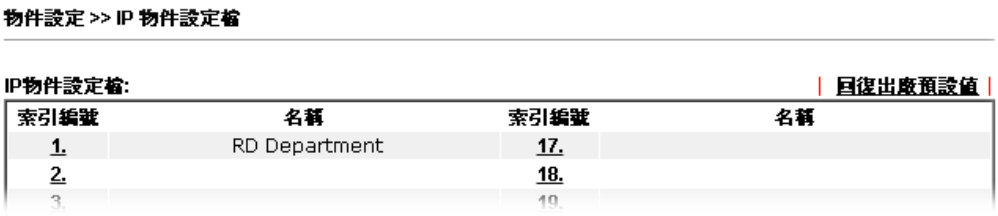


可用設定說明如下：

項目	說明
名稱(Name)	請輸入本設定檔的名稱，最多可以輸入 15 個字元。
介面 (Interface)	請選擇適當的介面。  例如，**編輯過濾器規則(Edit Filter Rule)**中的**方向(Direction)**設定會要求您針對 WAN 或 LAN/DMZ/RT/VPN 介面或是任何 IP 位址，指定一個 IP 或是 IP 範圍，或是任何的 IP 位址，如果您選擇 LAN/DMZ/RT/VPN 作爲介面，並選擇 LAN/DMZ/RT/VPN 作爲**編輯過濾器規則**中的**方向**設定，那麼所有的 LAN/DMZ/RT/VPN 介面的 IP 位址通通都會開放予您在**編輯過濾器規則**頁面上選擇。
位址類型 (Address Type)	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(Single Address)**。 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(Range Address)**。 如果物件包含 IP 位址的子網路的話，請選擇**子網路位址(Subnet Address)**。 如果物件包含任何一種 IP 位址的話請選擇**任何位址(Any Address)**。 如果物件包含任何一種 MAC 位址的話請選擇 **MAC 位址(Mac Address)**。

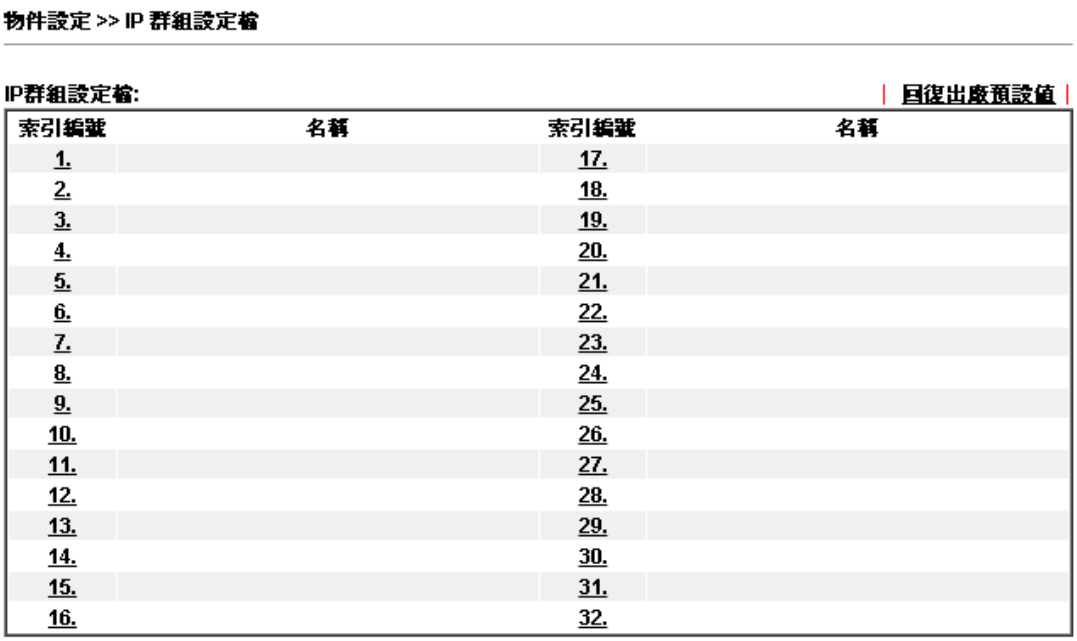
MAC 位址 (MAC Address)	如果選擇的是 **MAC 位址**類型，請輸入網卡的 MAC 位址。
起始 IP 位址 (Start IP Address)	輸入單一位址類型所需的起始 IP 位址。
結束 IP 位址 (End IP Address)	如果選擇的是範圍位址類型，請輸入結束 IP 位址。
子網路遮罩 (Subnet Mask)	如果選擇的是子網路位址**(**Subnet Address**)**類型，請輸入子網路遮罩位址。
反向選擇 (Invert Selection)	如果勾選此項的話，除了上面所提及的以外，其他的 IP 位址將會在被選擇之後全部套用上設定內容。

4. 完成設定之後，按下**確定(OK)**按鈕儲存相關設定，下表為 IP 物件設定的範例之一。



4.5.2 IP 群組設定檔(IP Group)

本頁可讓您綁定數個 IP 物件成爲一個 IP 群組。



可用設定說明如下：

項目	說明
回復出廠預設值 (Set to Factory Default)	清除全部的設定資料。
索引編號(Index)	顯示您可以設定的設定檔索引編號。
名稱(Name)	顯示物件設定檔的檔名。

如欲建立新的設定檔，請依下述步驟進行：

1. 按下索引欄位下方的任一編號連結(例如 #1) 進入設定頁面。
2. 設定網頁顯示如下：

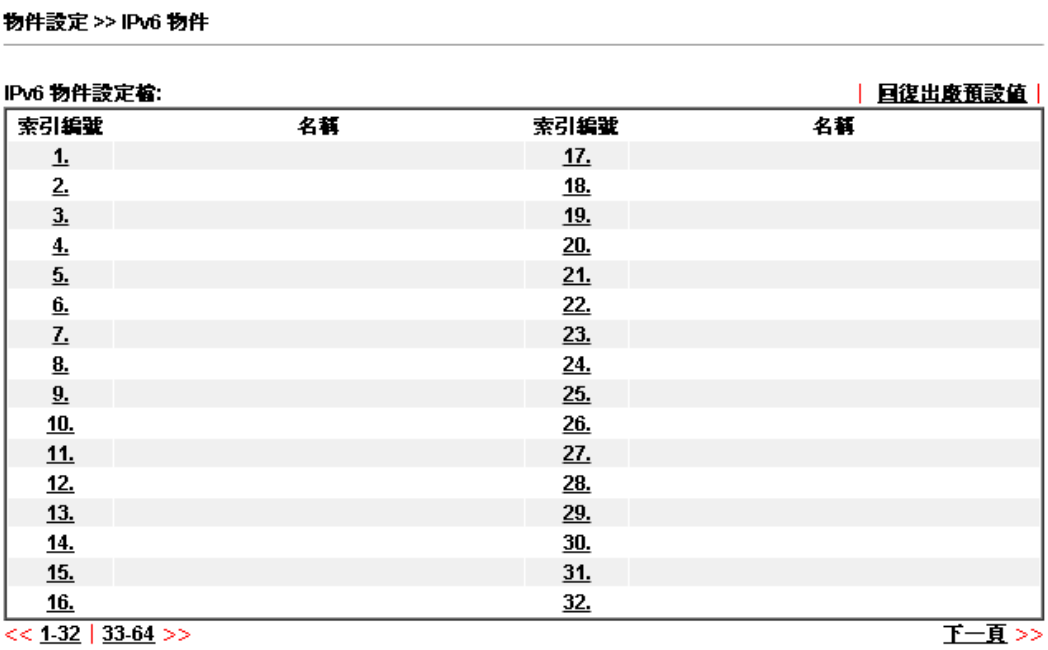
可用設定說明如下：

項目	說明
名稱(Name)	請輸入本設定檔的名稱，最多可以輸入 15 個字元。
介面 (Interface)	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 (Available IP Objects)	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 (Selected IP Objects)	按下 >> 按鈕來新增選定 IP 物件並呈現在此方塊內。

3. 完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

4.5.3 IPv6 物件(IPv6 Object)

您可設定 64 組不同條件的 IPv6 物件。



可用設定說明如下：

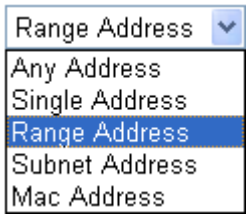
項目	說明
回復出廠預設值 (Set to Factory Default)	清除全部的設定資料。
索引編號(Index)	顯示您可以設定的設定檔索引編號。
名稱(Name)	顯示物件設定檔的檔名。

如欲建立新的設定檔，請依下述步驟進行：

1. 按下索引欄位下方的任一編號連結(例如 #1) 進入設定頁面。
2. 設定網頁顯示如下：

可用設定說明如下：

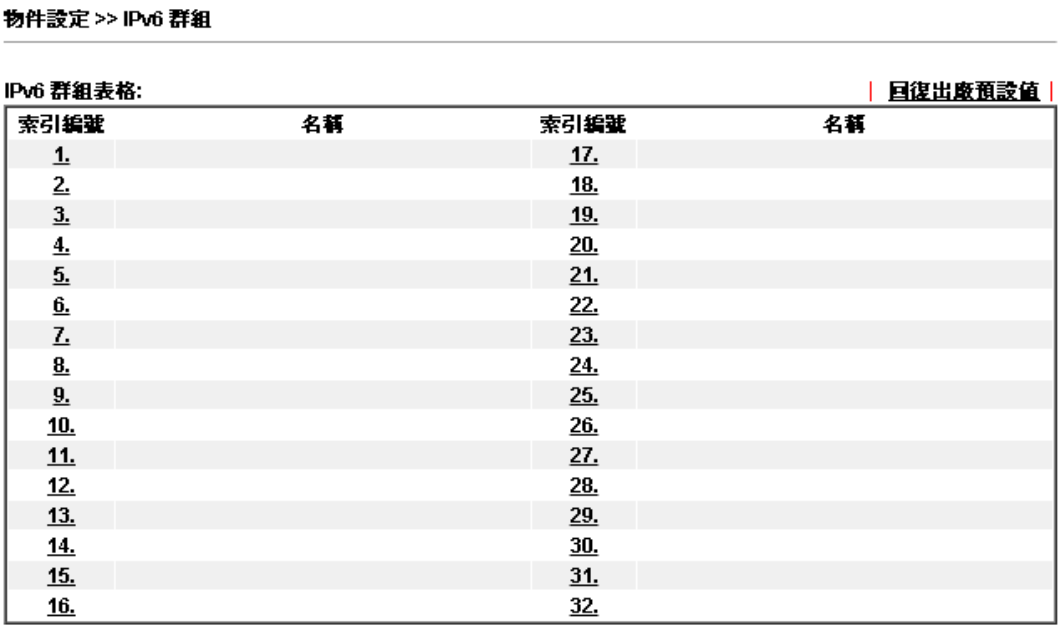
項目	說明

名稱(Name)	輸入設定檔名稱。
位址類型 (Address Type)	決定 IPv6 的位址類型。 如果此物件僅含一組 IPv6 位址，請選擇**單一位址(Single Address)**。 如果此物件包含數個 IPv6 位址，請選擇**範圍位址(Range Address)**。 如果此物件包含一個 IPv6 子網路位址，請選擇**子網路位址(Subnet Address)**。 如果此物件包含任何一個 IPv6 位址，，請選擇**任一位址(Any Address)**。 如果此物件包含 MAC 位址，請選擇 **MAC 位址(Mac Address)**。 
MAC 位址 (Mac Address)	輸入網卡的 MAC 位址。
起始 IP 位址 (Start IP Address)	輸入單一位址/範圍位址的起始 IP 位址。
結束 IP 位址 (End IP Address)	如果選擇範圍位址，請在此輸入結束 IP 位址。
前置號碼長度 (Prefix Len)	輸入 IPv6 位址的前置號碼長度值(例如 64)。
反向選擇 (Invert Selection)	若勾選此項，除了上述以外，全部的 IPv6 位址都將套用此物件規則。

3. 完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

4.5.4 IPv6 群組(IPv6 Group)

本頁可讓您綁定數個 IPv6 物件成爲一個 IPv6 群組。



可用設定說明如下：

項目	說明
回復出廠預設值 (Set to Factory Default)	清除全部的設定資料並回復出廠預設值。
索引編號(Index)	顯示您可以設定的設定檔索引編號。
名稱(Name)	顯示物件設定檔的檔名。

如欲建立新的設定檔，請依下述步驟進行：

1. 按下索引欄位下方的任一編號連結(例如 #1) 進入設定頁面。
2. 設定網頁顯示如下：

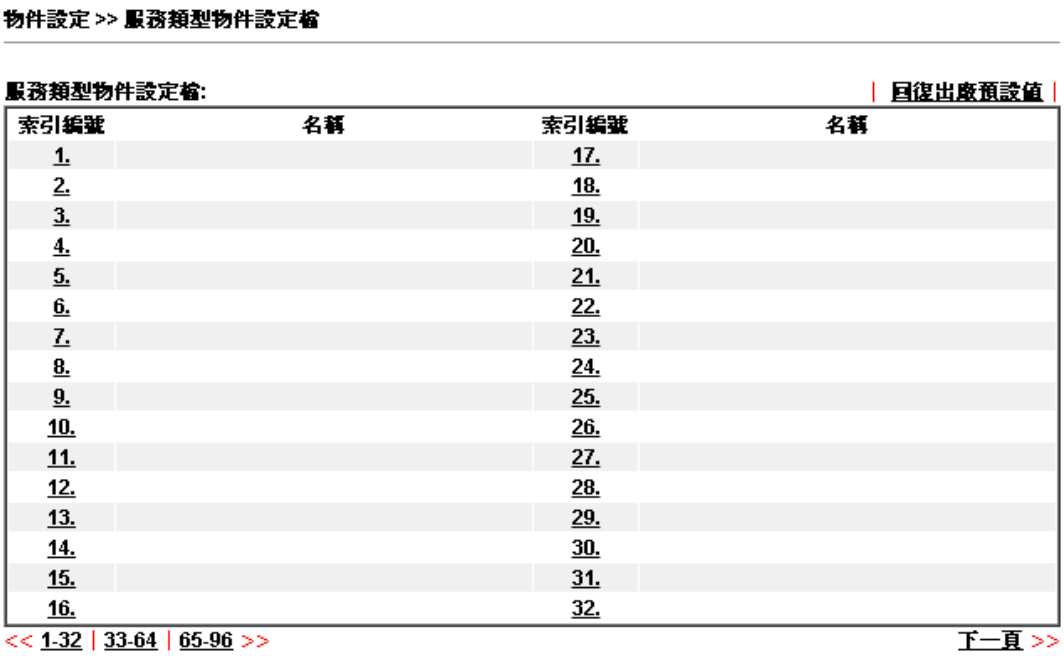
可用設定說明如下：

項目	說明
名稱(Name)	請輸入本設定檔的名稱，最多可以輸入 15 個字元。
可用的 IPv6 物件 (Available IPv6 Objects)	所有可用的 IPv6 物件全都會顯示在此方塊中。
選定的 IPv6 物件 (Selected IPv6 Objects)	按下 >> 按鈕來新增選定 IP IPv6 物件並呈現在此方塊內。

3. 完成設定之後，按下**確定**按鈕儲存相關設定。

4.5.5 服務類型物件(Service Type Object)

您可設定 96 組不同條件的服務類型物件。



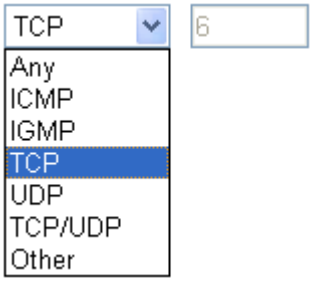
可用設定說明如下：

項目	說明
回復出廠預設值 (Set to Factory Default)	清除全部的設定資料。
索引編號(Index)	顯示您可以設定的設定檔索引編號。
名稱(Name)	顯示物件設定檔的檔名。

如欲建立新的設定檔，請依下述步驟進行：

1. 按下索引欄位下方的任一編號連結(例如 #1) 進入設定頁面。
2. 設定網頁顯示如下：

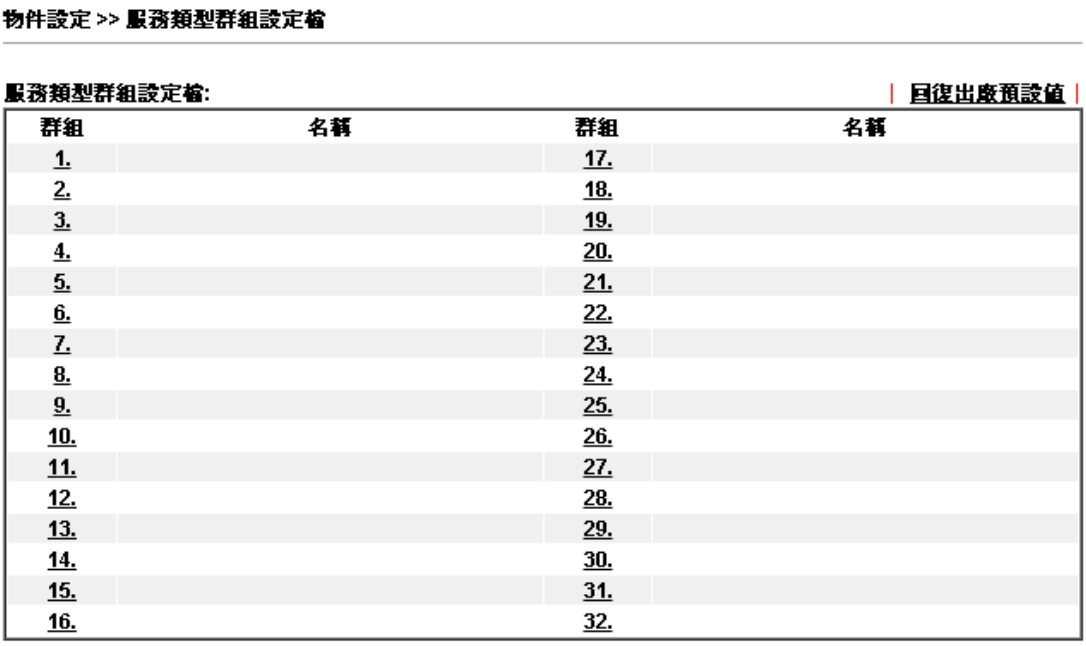
可用設定說明如下：

項目	說明
名稱(Name)	輸入此設定檔的名稱。
通訊協定(Protocol)	請選擇此設定檔所要套用的適當介面。 
來源/目的通訊埠 (Source/Destination Port)	**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。

3. 完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

4.5.6 服務類型群組(Service Type Group)

本頁可讓您綁定數個服務類型物件成爲一個群組。



可用設定說明如下：

項目	說明
回復出廠預設值 (Set to Factory Default)	清除全部的設定資料。
索引(Index)	顯示您可以設定的設定檔索引編號。
名稱(Name)	顯示物件設定檔的檔名。

如欲建立新的設定檔，請依下述步驟進行：

1. 按下索引欄位下方的任一編號連結(例如 #1) 進入設定頁面。
2. 設定網頁顯示如下：

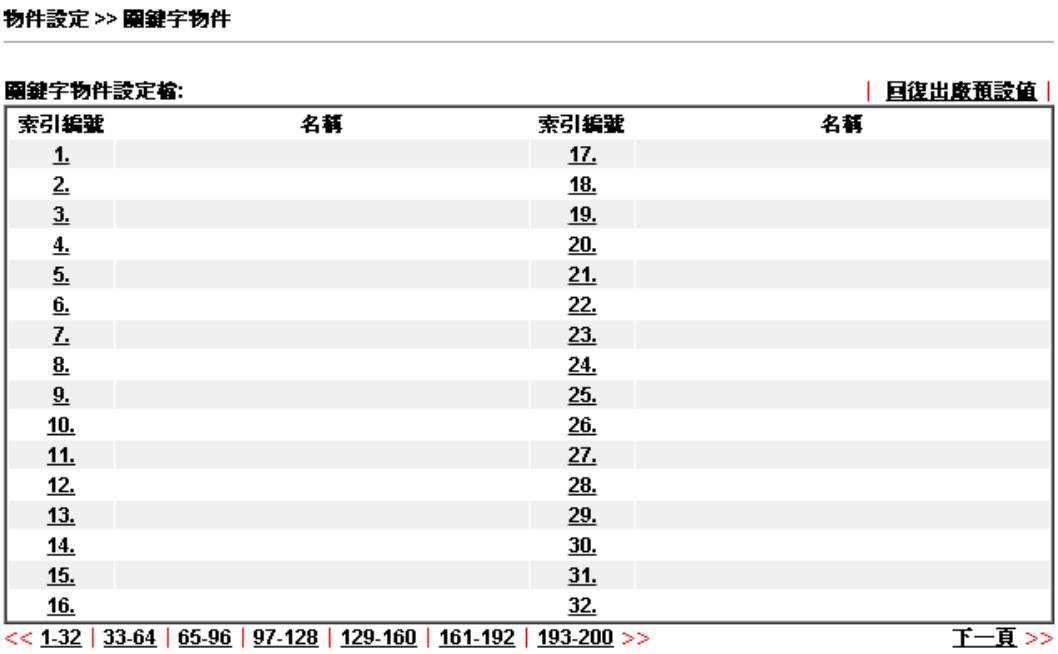
可用設定說明如下：

項目	說明
名稱(Name)	輸入此設定檔的名稱。
可用之服務類型物件 (Available Service Type Objects)	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 (Selected Service Type Objects)	按下 >> 按鈕來新增選定服務類型並呈現在此方塊內。

3. 完成設定之後，按下**確定**按鈕儲存相關設定。

4.5.7 關鍵字物件(Keyword Object)

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(CSM >>URL Web Content Filter Profile)**中選擇作爲黑白名單之用。



可用設定說明如下：

項目	說明
回復出廠預設值 (Set to Factory Default)	清除全部的設定資料。
索引編號(Index)	顯示您可以設定的設定檔索引編號。
名稱(Name)	顯示物件設定檔的檔名。

如欲建立新的設定檔，請依下述步驟進行：

1. 按下索引欄位下方的任一編號連結(例如 #1) 進入設定頁面。
2. 設定網頁顯示如下：

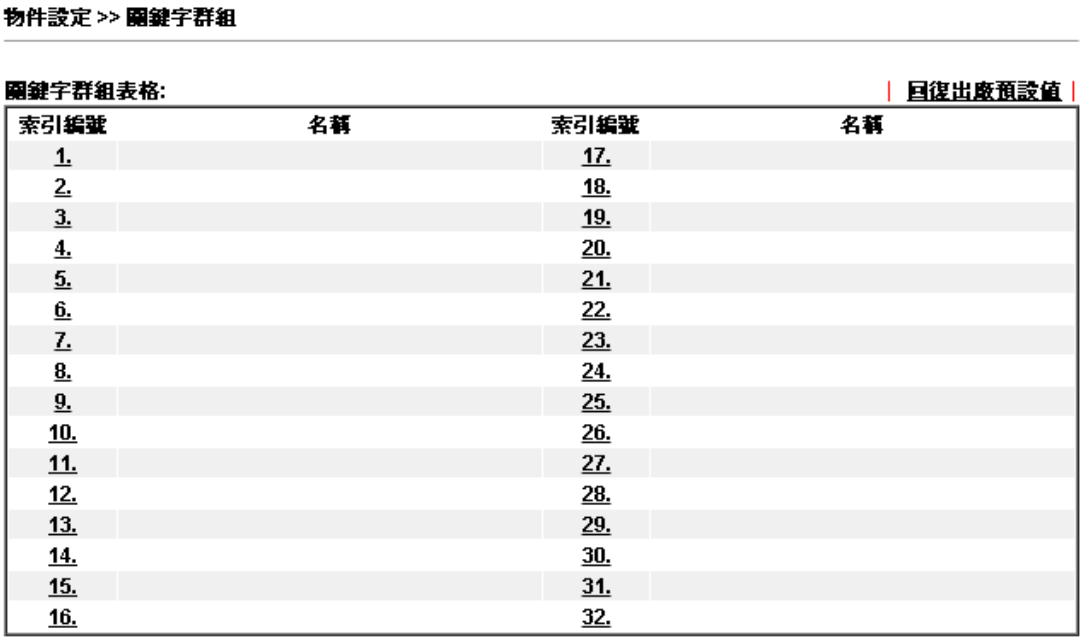
可用設定說明如下：

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

3. 完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

4.5.8 關鍵字群組(Keyword Group)

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(CSM >>URL /Web Content Filter Profile)**中選擇作爲黑白名單之用。



可用設定說明如下：

項目	說明
回復出廠預設值 (Set to Factory Default)	清除全部的設定資料。
索引編號(Index)	顯示您可以設定的設定檔索引編號。
名稱(Name)	顯示物件設定檔的檔名。

如欲建立新的設定檔，請依下述步驟進行：

1. 按下索引欄位下方的任一編號連結(例如 #1) 進入設定頁面。
2. 設定網頁顯示如下：

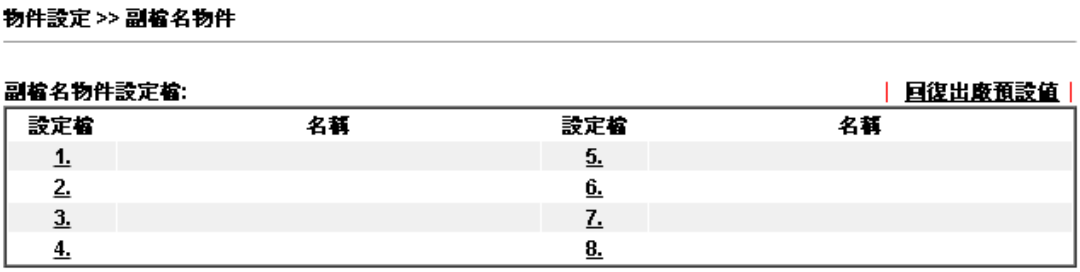
可用設定說明如下：

項目	說明
名稱(Name)	輸入此設定檔的名稱。
可用之關鍵字物件 (Available Keyword Objects)	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 (Selected Keyword Objects)	按  按鈕增加選定之關鍵字物件於本方塊區中。

3. 完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

4.5.9 副檔名物件(File Extension Object)

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(CSM>>URL Content Filter)**中。設定檔中指定之所有含附檔名稱的檔案都可按照所選擇的動作來處理。



可用設定說明如下：

項目	說明
回復出廠預設值 (Set to Factory Default)	清除全部的設定資料。
設定檔(Index)	顯示您可以設定的設定檔索引編號。
名稱(Name)	顯示物件設定檔的檔名。

如欲建立新的設定檔，請依下述步驟進行：

1. 按下索引欄位下方的任一編號連結(例如 #1) 進入設定頁面。

2. 設定網頁顯示如下：

可用設定說明如下：

項目	說明
設定檔名稱(Profile Name)	請輸入此設定檔名稱。

3. 輸入設定檔名稱並勾選路由器會處理的副檔名項目，然後按**確定(OK)**儲存本頁的設定。

4.5.10 簡訊(SMS)/郵件服務物件(SMS/Mail Service Object)

簡訊服務(SMS)供應商

本頁讓您設定 10 組設定檔，後續將運用在**應用>>簡訊/郵件警示服務 (Application>>SMS/Mail Alert Service)**中。

可用設定說明如下：

項目	說明
回復出廠預設值 (Set to Factory Default)	清除全部的設定資料。
索引編號 (Index)	顯示您可以設定的設定檔索引編號。
設定檔名稱 (Profile)	顯示物件設定檔的檔名。
簡訊服務(SMS)供應商 (SMS Provider)	顯示提供簡訊服務的供應商名稱。

如欲建立新的設定檔，請依下述步驟進行：

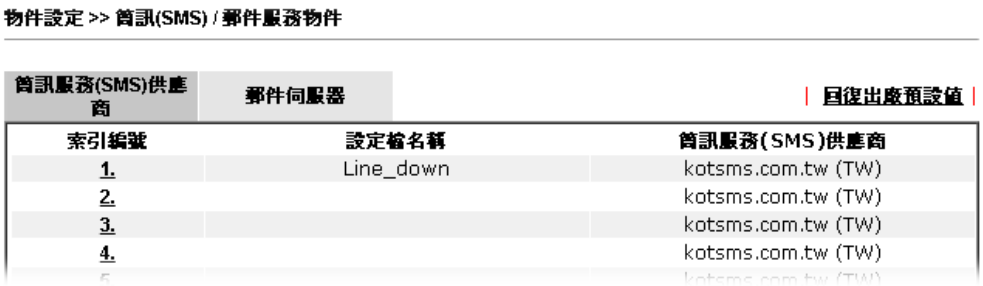
1. 選擇簡訊服務供應商標籤欄，然後按下索引編號欄位下方的任一編號連結(例如 #1)進入設定頁面。

2. 設定網頁顯示如下：

可用設定說明如下：

項目	說明
設定檔名稱 (Profile Name)	請輸入此設定檔名稱。
服務供應商 (Service Provider)	使用下拉式清單選擇提供簡訊服務的服務供應商。
使用者名稱 (Username)	輸入發簡訊人員用來註冊選擇簡訊服務供應商所需的名稱。 使用者名稱長度不可超過 31 個字元。
密碼 (Password)	輸入發簡訊人員用來註冊選擇簡訊服務供應商所需的密碼。 密碼長度不可超過 31 個字元。
簡訊則數 (Quota)	輸入您自服務供應商所購得的簡訊則數。 注意，每則簡訊等於標準路由中所註記的簡訊文字訊息。
寄送間隔時間 (Sending Interval)	爲了防止發信額度太早用罄，請輸入傳送簡訊所需的間隔時間。

3. 完成設定之後，按下**確定(OK)**按鈕儲存相關設定。



客製化簡訊服務(Customized SMS Service)

路由器提供數種簡訊服務供應商的名稱來供應簡訊服務，然而，如果您的服務供應商不在清單上，您可以透過索引編號 9 與 10 自行設定簡訊服務供應商的相關資料。編號 9 與 10 的設定檔名稱是固定無法改變的。

按下索引編號 9 與 10 開啓設定頁面：

可用設定說明如下：

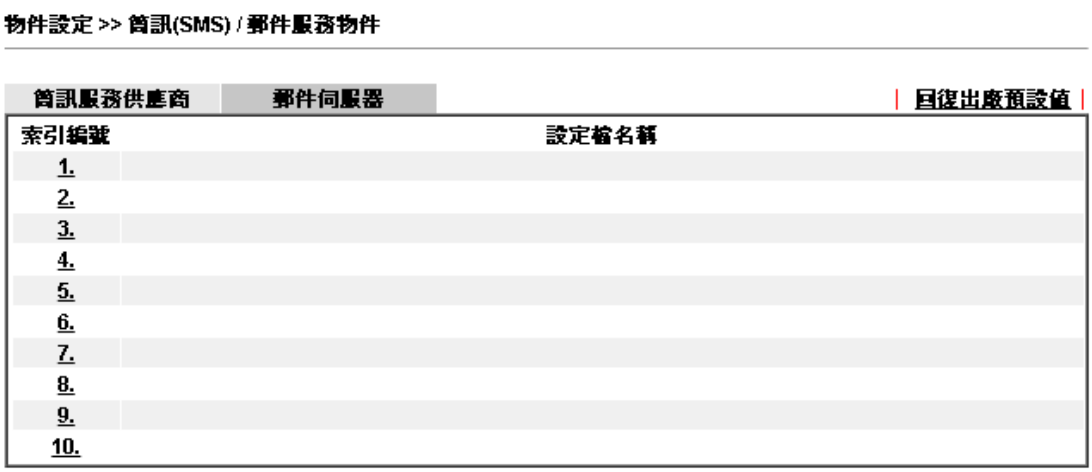
項目	說明
設定檔名稱 (Profile Name)	顯示設定檔名稱。
服務供應商 (Service Provider)	輸入服務供應商的網址。 在此項目的下方區塊中輸入 URL，您必須先與簡訊服務供應商聯絡以便獲得正確的 URL 字串。

使用者名稱 (Username)	輸入發簡訊人員用來註冊選擇簡訊服務供應商所需的名稱。 使用者名稱長度不可超過 31 個字元。
密碼 (Password)	輸入發簡訊人員用來註冊選擇簡訊服務供應商所需的密碼。 密碼長度不可超過 31 個字元。
簡訊則數 (Quota)	輸入您自服務供應商所購得的簡訊則數。 注意，每則簡訊等於標準路由中所註記的簡訊文字訊息。
傳送間隔 (Sending Interval)	爲了防止發信額度太早用罄，請輸入傳送簡訊所需的間隔時間。

完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

郵件服務物件(Mail Service Object)

本頁讓您設定 10 組設定檔，後續將運用在**應用>>簡訊/郵件警示服務 (Application>>SMS/Mail Alert Service)**中。

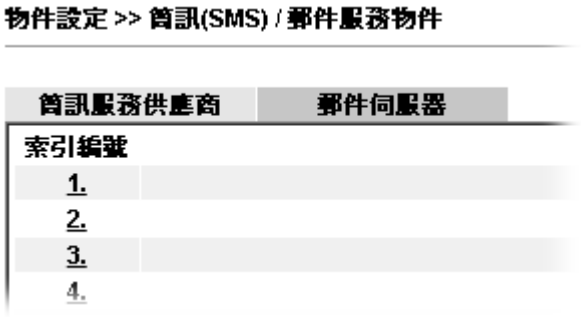


可用設定說明如下：

項目	說明
回復出廠預設值 (Set to Factory Default)	清除全部的設定資料。
索引編號(Index)	顯示您可以設定的設定檔索引編號。
設定檔名稱 (Profile Name)	顯示物件設定檔的檔名。

如欲建立新的設定檔，請依下述步驟進行：

1. 選擇郵件伺服器標籤欄，然後按下索引欄位下方的任一編號連結(例如 #1) 進入設定頁面。



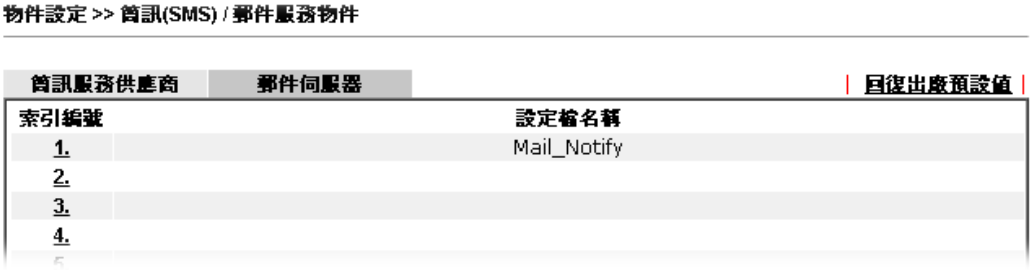
2. 設定網頁顯示如下

可用設定說明如下：

項目	說明
設定檔名稱 (Profile Name)	請輸入此設定檔名稱。
SMTP 伺服器 (SMTP Server)	輸入郵件伺服器的 IP 位址。
SMTP 埠號 (SMTP Port)	輸入 SMTP 伺服器需要的埠號。
寄件人位址 (Sender Address)	輸入寄件人的電子郵件位址。
使用 SSL (Use SSL)	勾選此方框啓用此功能。
驗證 (Authentication)	郵件伺服器必須透過正確的使用者名稱與密碼來進行驗證，才有權利傳送訊息，請勾選方框啓用此功能。 **使用者名稱(Username)** – 請自訂驗證所需的使用者名

	稱。 **密碼(Password)** –請自訂驗證所需的密碼。
傳送間隔 **(Sending Interval)**	請輸入傳送簡訊所需的間隔時間。

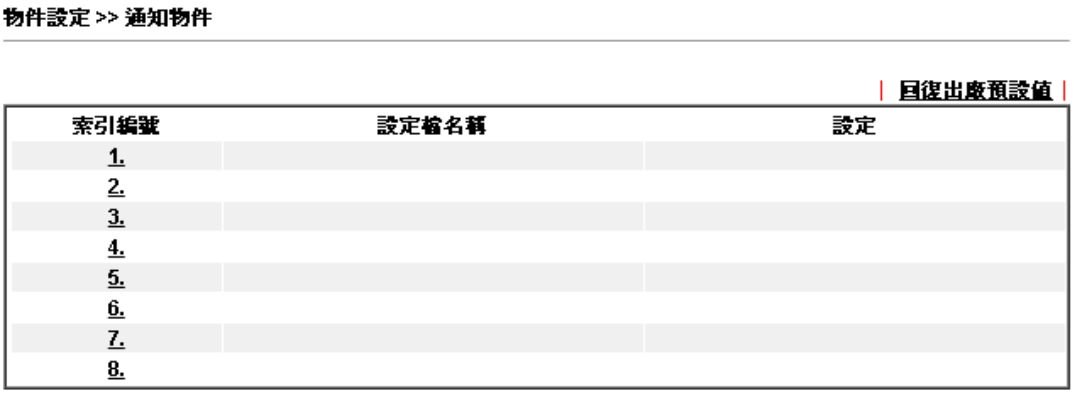
3. 完成設定之後，按下**確定(OK)**按鈕儲存相關設定。



4.5.11 通知物件(Notification Object)

本頁讓您設定 10 組設定檔，後續將運用在**應用>>簡訊/郵件警示服務(Application>>SMS/Mail Alert Service)**中。

每個物件可以設定不同的監控條件。

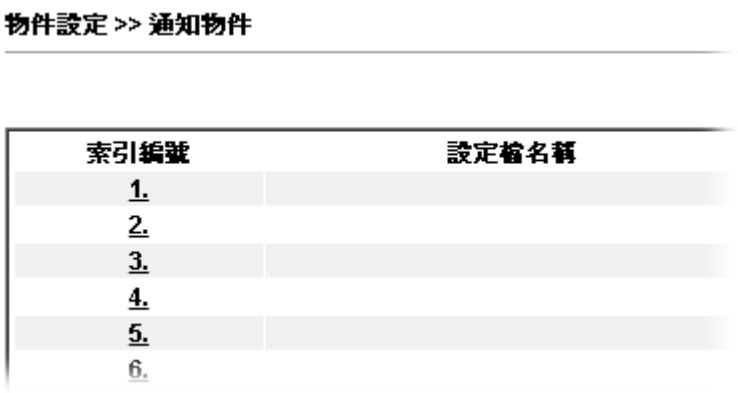


可用設定說明如下：

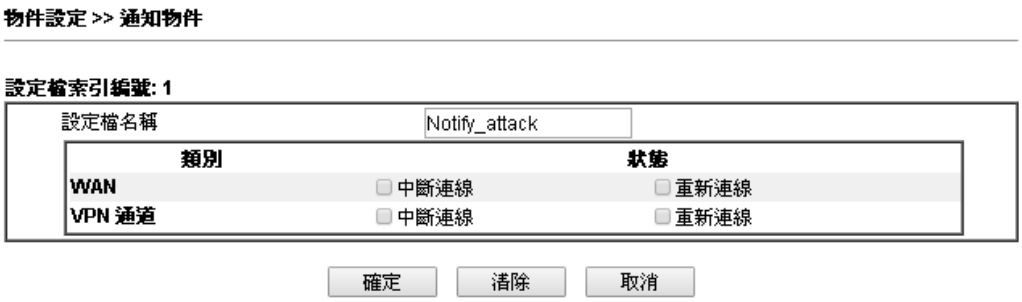
項目	說明
回復出廠預設值 **(Set to Factory Default)**	清除全部的設定資料。
索引編號(Index)	顯示您可以設定的設定檔索引編號。
設定檔名稱 **(Profile Name)**	顯示物件設定檔的檔名。
設定(Settings)	顯示物件設定檔的內容。

如欲建立新的設定檔，請依下述步驟進行：

1. 開啓**物件設定>>通知物件(Object Setting>>Notification Object)**，然後按下索引欄位下方的任一編號連結(例如 #1) 進入設定頁面。



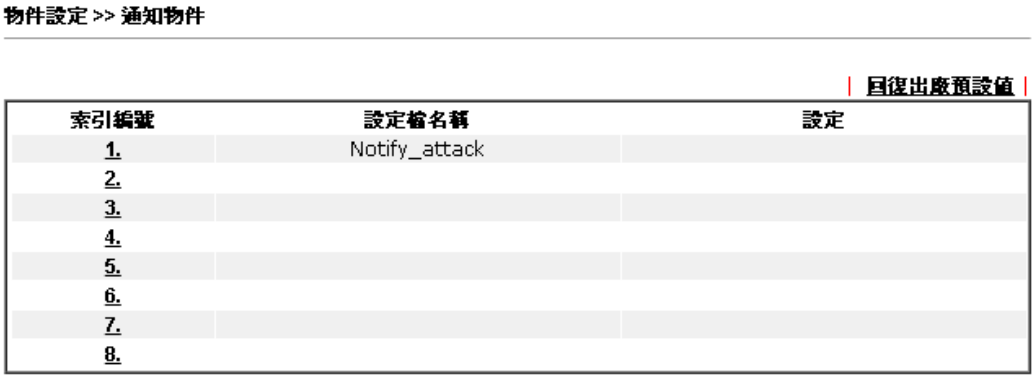
2. 設定網頁顯示如下：



可用設定說明如下：

項目	說明
設定檔名稱 (Profile Name)	請輸入此設定檔名稱。
類型 (Category)	顯示被監控的類型。
狀態 (Status)	顯示類型的狀態，您可以勾選想要監控的類型狀態方塊。

3. 完成設定之後，按下**確定(OK)**按鈕儲存相關設定。



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。

應用程式管控設定檔(APP Enforcement Filter)

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(URL Content Filter)

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。

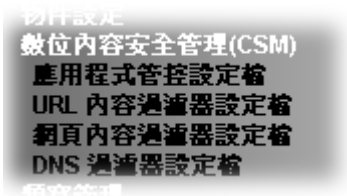
換言之，Vigor 路由器可以防止使用者意外自網頁下載惡意的程式碼。惡意碼隱藏在執行物件當中是一件很普遍的事情，像是 ActiveX、Java Applet、壓縮檔和其他執行檔案。一旦用戶下載這些類型的檔案，用戶便會有這些可能爲系統帶來威脅的風險，例如一個 ActiveX 控制物件通常用於提供網頁人機通信交換功能，萬一裡面隱藏惡意的程式碼的話，該程式碼就可能會佔據使用者的系統。

網頁內容過濾器(Web Content Filter)

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。

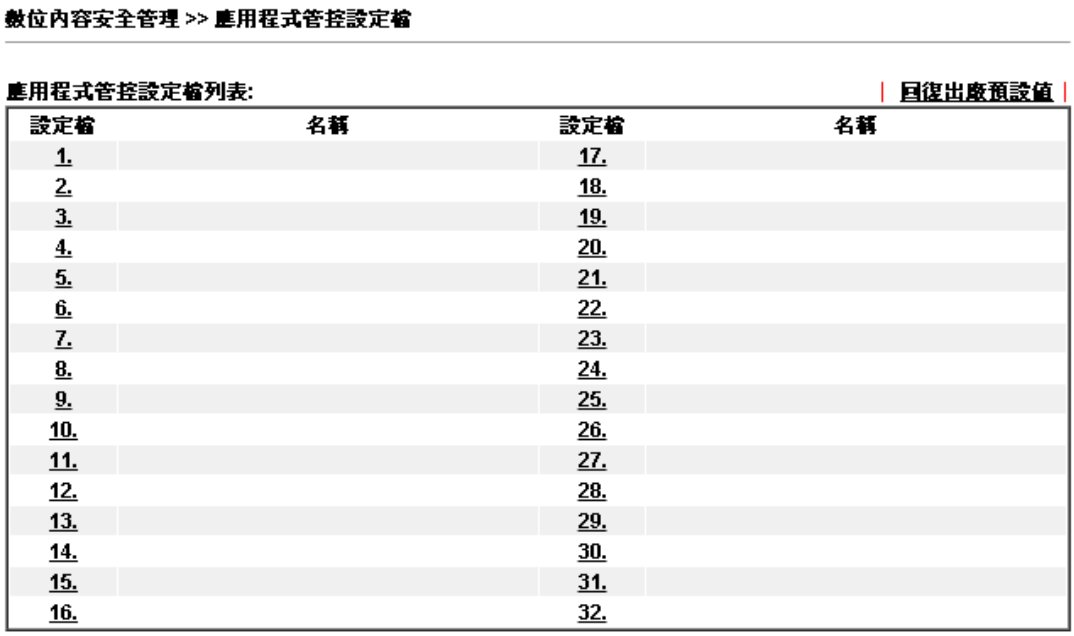
一旦您啓動了網頁內容過濾服務，也選擇一些您想要限制存取的網站目錄，每個 URL 位址需求(例 www.bbc.co.uk) 將在由 SurfControl 所運作的伺服器資料庫中先接受檢測。資料庫涵蓋 70 種語言和 200 個國家，超過 1 億個網頁，區分成 40 種容易瞭解的目錄。此資料庫每一天都由網際網路的國際研究團隊不斷更新，伺服器將查閱 URL 然後傳回其類別給路由器，您的 Vigor 路由器即可按照您所選擇的分類項目來決定是否允許用戶存取該網站，因爲每一個多路負載平衡資料庫伺服器一次可以管理數百萬的分類需求。

注意: URL 內容過濾器的優先權高於網頁內容過濾器。



4.6.1 應用程式管控設定檔(APP Enforcement Profile)

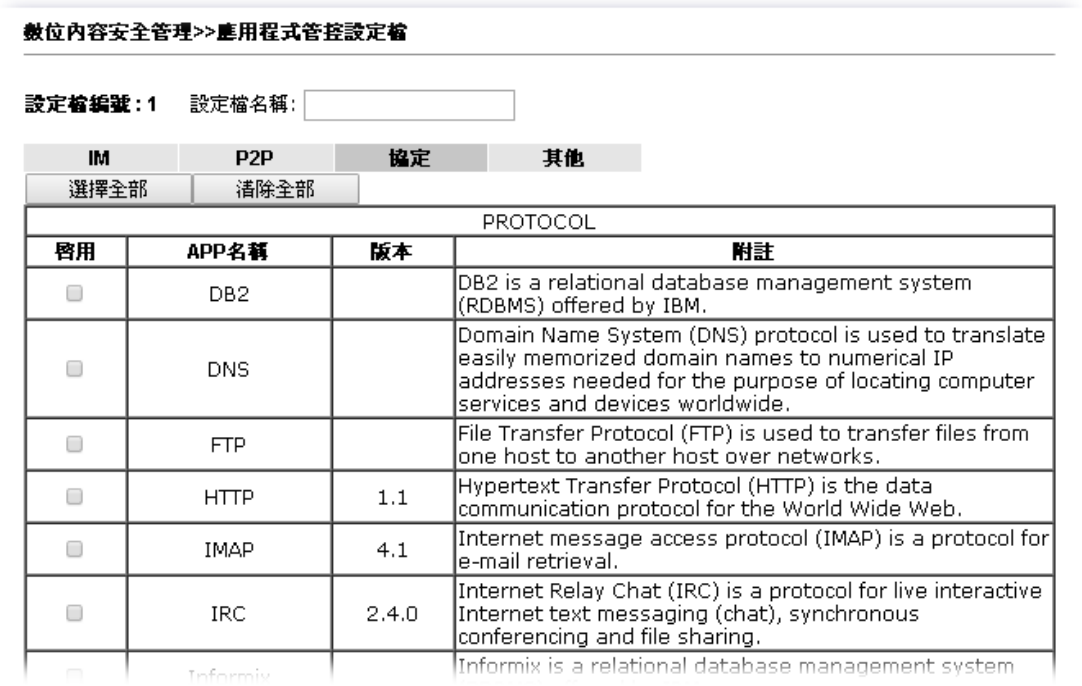
您可針對即時通訊/點對點/通訊協定/其他應用定義不同的策略檔案，以通訊及應用之需要，此處所建立的設定檔可以運用在**防火牆>>基本設定**的**預設規則**中，做爲主機依循的標準。



可用設定說明如下：

項目	說明
回復出廠預設值 (Set to Factory Default)	清除全部的設定資料。
設定檔 (Profile)	顯示索引編號連結讓您點選進入設定頁面。
名稱(Name)	顯示應用程式管控的設定檔名稱。

按索引下方的號碼連結開啓如下視窗進行細節設定。頁面中呈現四種不同的標籤，IM、P2P、協定與其他。下圖顯示協定標籤下的設定內容：



可用設定說明如下：

項目	說明
設定檔名稱 (Profile Name)	請輸入此設定檔名稱。
選擇全部 (Select All)	按此選擇本頁中全部的設定項目。
清除全部 (Clear All)	按此捨棄選擇的項目。

4.6.2 URL 內容過濾器設定檔 (URL Content Filter Profile)

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。

可用設定說明如下：

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

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

可用設定說明如下：

項目	說明
設定檔名稱 (Profile Name)	請輸入此設定檔名稱。
優先權 (Priority)	決定路由器採用的動作順序。 **二者皆選:通過(Both: Pass)** – 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(Both: Block)** – 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(Either: URL Access Control First)** – 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(Either: Web Feature First)** – 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(Log)	**無(None)** – 沒有任何關於此設定檔的紀錄保留下來。 **通過(Pass)** – 只有通過動作會記錄在 Syslog 中。 **封鎖(Block)** – 只有封鎖動作會記錄在 Syslog 中。 **全部(All)** – 所有的動作(包含通過與封鎖)都會記錄在 Syslog 中。

URL 存取控制 (URL Access Control)	**啓用 URL 存取控制(Enable URL Access Control) -** 勾選此方塊啓動 URL 存取控制設定，請注意 **URL 存取控制 (URL Access Control)** 優先權原本就高於**網頁特徵 (Restrict Web Feature)**，如果網頁內容符合 URL 存取控制中的設定，路由器將先執行此區所指定的動作，而忽略網頁特徵中所指定的動作。 **防止透過 IP 位址對網站進行存取(Prevent web access from IP address)-** 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(Action)** – 此功能僅在您選擇了**二擇一: URL 存取控制優先(Either : URL Access Control First)**或**二擇一: 網頁特徵優先(Either : Web Feature First)**時才能使用。 ***通過(Pass)*** **-** 允許進入含有關鍵字清單中之關鍵字的網頁。 ***封鎖(Block)*** **-** 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(Group/Object Selections)** – 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(Enable Restrict Web Feature) -** 勾選此

(Web Feature)	方塊讓關鍵字被封鎖或是放行。 **動作(Action) -** 此功能僅在您選擇了**二者選一: URL 存取控制優先(Either: URL Access Control First)**或**二者選一: 網頁特徵優先(Either: Web Feature First)**時才能使用。 ***通過(Pass)* -** 允許進入含有關鍵字清單中之關鍵字的網頁。 ***封鎖(Block)* -** 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(File Extension Profile) –** 請自**物件設定>>副檔名物件(Object Setting>> File Extension Objects)**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。

完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

4.6.3 網頁內容過濾器設定檔(Web Content Filter Profile)

有數種方式可以啓動路由器的網頁內容過濾器(WCF) – 透過**服務啓動精靈(Service Activation Wizard)**、**數位內容安全管理>>網頁內容過濾器設定檔(CSM>>Web Content Filter Profile)**或是**系統維護>>開啓授權碼(System Maintenance>>Activation)**。

服務啓動精靈讓您使用試用版 WCF 授權碼，無需登入 http://myvigor.draytek.com 的伺服器(***MyVigor***)。

不過，如果您使用網頁內容過濾器設定檔來啓動 WCF 功能，您必須登入(***MyVigor***)伺服器，因此，您得先上伺服器註冊一組帳號才能使用相關的服務，請參考如何建立 MyVigor 帳號相關章節。

注意: 如果您已經使用服務啓動精靈來啓動 WCF 服務，您可以跳過此節。

WCF 採取特定服務供應商開發的機制來進行，不論是啓動 WCF 功能或是取得新的授權碼，您都必須按下**啓動**才能達成要求，要注意的是符合目前 Vigor 路由器需求的服務供應商提供的是短期的試用版，如果您想要購買正式版本，請與通路商或是經銷商聯絡。

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

可用設定說明如下：

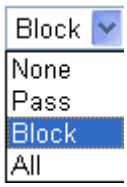
項目	說明
啓動(Activate)	按下此鈕登入 MyVigor 以便啓動 WCF 服務。
設定搜尋伺服器 (Setup Query Server)	建議您使用預設的設定，當您以 WCF 設定檔爲基準，在瀏覽器上輸入 URL 時，您需要指定伺服器來歸類搜尋的內容。
設定測試伺服器 (Setup Test Server)	建議您使用預設的設定。
更多(Find more)	按下此鈕開啓畫面選擇另外的伺服器。
回復出廠預設值 (Set to Factory Default)	按下此連結回復出廠預設值。
預設訊息 (Default Message)	您可以手動輸入訊息或是按下此按鈕取得預設的訊息，並顯示在**管理訊息(Administration Message)**方框內。輸入
快取 (Cache)	**無** – 路由器將會透過 WCF 機制檢查使用者想要登入的 URL，處理的速度爲一般，這個選項可提供最準確的 URL 過濾作業。 **L1** – 路由器將會透過 WCF 機制檢查使用者想要登入的 URL，如果該 URL 早先已經存取過，系統會將此資料在路由器內儲存非常短暫的時間(大約 1 秒)，讓必要時可以快速登入。此選項可以提供速度較快的 URL 過濾作業。 **L2** – 路由器將會透過 WCF 機制檢查使用者想要登入的 URL，如果該 URL 早先已經存取過，系統會將其 IP 位址在路由器內儲存非常短暫的時間(大約 1 秒)，當使用者想要再

	次登入相同的 IP 時，路由器會將其與儲存的內容做比對，如果符合，該頁面就會迅速取回並呈現出來。此選項可以提供速度最快的 URL 過濾作業。 **L1+L2 快取(L1+L2 Cache)** – 路由器將會以 L1 加上 L2 的功能快速檢查 URL。

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

可用設定說明如下：

項目	說明
設定檔名稱 **(Profile Name)**	輸入網頁內容過濾器設定檔的名稱。
黑/白名單 **(Black/White List)**	**啓用(Enable) –** 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(Pass - allow) –** 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(Block - restrict) -** 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。

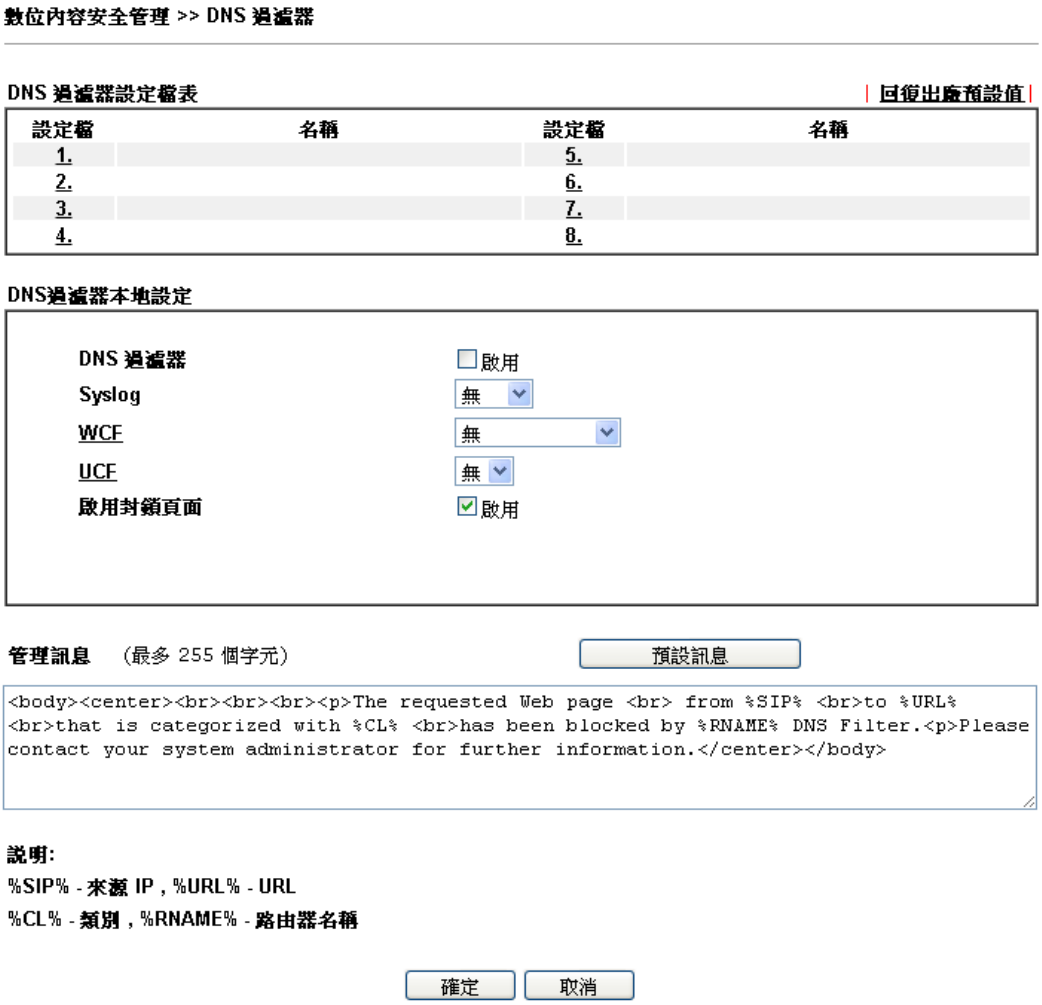
動作(Action)	**通過(Pass)** – 允許進入勾選的方塊等相關類型頁面。 **封鎖(Block)** – 限制進入勾選的方塊等相關類型頁面。如果網頁未符合此處所設定的內容，系統將以反向做爲處理該網頁。
Log(紀錄)	**無(None)** – 沒有任何關於此設定檔的紀錄保留下來。 **通過(Pass)** – 只有通過動作會記錄在 Syslog 中。 **封鎖(Block)** – 只有封鎖動作會記錄在 Syslog 中。 **全部(All)** – 所有的動作(包含通過與封鎖)都會記錄在 Syslog 中。 

完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

4.6.4 DNS 過濾器(DNS Filter)

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

注意: 因爲 DNS 過濾器必須使用 WCF 服務來過濾封包，因此 WCF 授權碼必須事先啓動才行。否則，DNS 過濾器無法對封包產生任何效用。



可用設定說明如下：

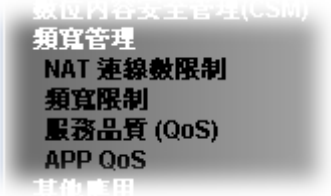
項目	說明
DNS 過濾器設定檔表 (DNS Filter Profile Table)	顯示不同的 DNS 過濾器設定檔清單資料。 按下索引編號連結開啓如下頁面，然後輸入設定檔名稱並依照您的需要指定 WCF/UCF 等過濾器設定檔以資套用。 
DNS 過濾器本地設定	若尚未設定好任何 DNS 設定檔，此處的基本設定將會套

(DNS Filter General Setting)	用至 DNS 過濾器。 **DNS 過濾器(DNS Filter) -** 勾選**啓用(Enable)**以便啓用此功能。 **Syslog -** 過濾結果將依照 Syslog 設定來記錄。 ● **無(None)** –此設定沒有任何內容會被記錄下來。 ● **通過(Pass)** –只有封包通過的記錄會被轉往 Syslog。 ● **封鎖(Block)** –只有封包被封鎖的記錄會被轉往 Syslog。 ● **全部(All)** –所有的動作(通過與封鎖)記錄都會被轉往 Syslog。 **WCF-** 設定網頁內容過濾器的過濾條件。 **UCF -** 設定 URL 內容過濾器的過濾條件。 **啓用封鎖頁面 –** 勾選後即可封鎖相關頁面。
管理訊息 (Administration Message)	輸入文字或是完整句子，當 Vigor 路由器封鎖頁面時將會呈現此管理訊息。

完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

4.7 頻寬管理(Bandwidth Management)

下面是頻寬管理的設定項目:



4.7.1 NAT 連線數限制(Sessions Limit)

擁有虛擬 IP 的電腦可以透過 NAT 路由器存取網際網路，針對此連線需求路由器將會產生 NAT 連線數的紀錄，P2P (Peer to Peer)應用程式(如 BitTorren)經常需要很大的連線數來處理，同時也會佔據很大的資源空間，造成重要的資料存取動作受到嚴重的影響。爲瞭解決這種問題，您可以使用連線數限制來限制指定主機的連線數

在**頻寬管理**群組中，按 **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。

可用設定說明如下：

項目	說明

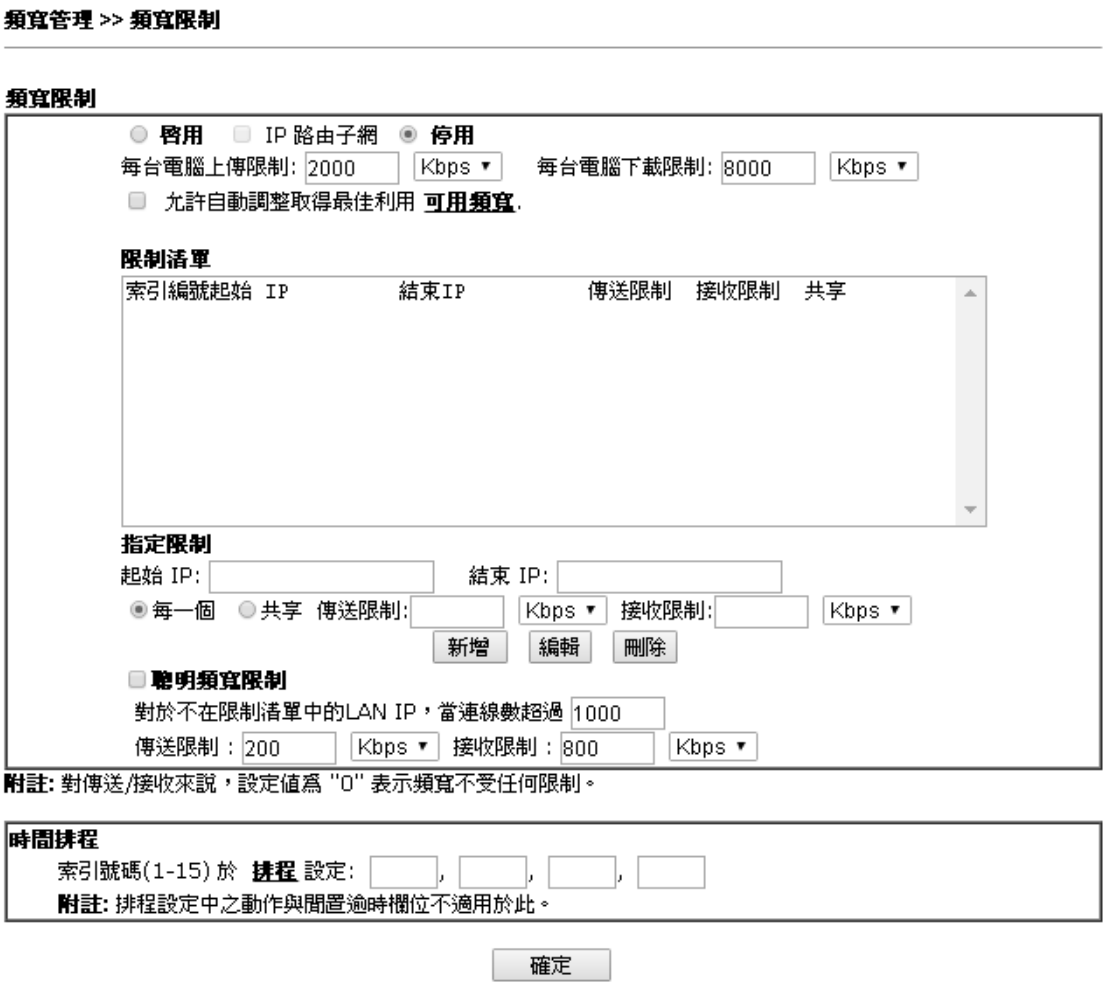
連線數限制 **(Session Limit)**	**啓用(Enable) -** 按此鈕啓動連線數限制功能。 **停用(Disable) -** 按此鈕關閉連線數限制功能。 **預設每台電腦連線數(Default session limit) -**定義區域網路中每台電腦的預設連線數。
限制清單 **(Limitation List)**	顯示網頁中所設定的指定限制之電腦清單資料。
指定限制 **(Specific Limitation)**	**起始 IP (Start IP)-** 定義限制連線數的起始 IP 位址。 **結束 IP(End IP) -**定義限制連線數的結束 IP 位址。 **最大連線數(Maximum Sessions) -** 定義指定 IP 位址的範圍中可用的連線數，如果您沒有在此區設定連線數，系統將會使用此機種所支援之預設連線數。 **新增(Add) -** 新增指定連線數限制並顯示在上面的框框中。 **更新(Update) -** 允許您編輯選定的連線數設定。 **刪除(Delete) -** 刪除限制清單上任何一個您所選定的設定。
管理訊息 **(Administration Message)**	請輸入系統允許的網路連線數屆滿時，顯示在螢幕上的文字。 **預設訊息(Default Message) -** 按下此鈕可以直接使用路由器預設的訊息並顯示在管理訊息框內。
索引號碼(1-15)於排程設定.. **(Time Schedule)**	您可以輸入四組時間排程，所有的排程都可在**應用-排程(Application >> Schedule)**網頁上事先設定完畢，然後在此輸入該排程的對應索引號碼即可。

完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

4.7.2 頻寬限制(Bandwidth Limit)

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(Bandwidth Management)**群組中，按**頻寬限制(Bandwidth Limit)**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。

可用設定說明如下：

項目	說明
頻寬限制 **(Bandwidth Limit)**	**啓用(Enable) -** 按此鈕啓動限制頻寬功能。 **停用(Disable) -** 按此鈕關閉限制頻寬功能。 **每台電腦上傳限制(Default TX limit) -** 定義區域網路中每台電腦預設的上行速度。 **每台電腦下載限制(Default RX limit) -** 定義區域網路中每台電腦預設的下行速度。 **允許自動調整(Allow auto adjustment…) -**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 **(Limitation List)**	顯示網頁中所設定的指定限制之電腦清單資料。
指定限制 **(Specific Limitation)**	**起始 IP (Start IP) -** 定義限制頻寬的起始 IP 位址。 **結束 IP (End IP)-** 定義限制頻寬的結束 IP 位址。 **每一個/共享(Each /Shared) -** 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(TX limit) -** 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(RX limit) -** 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(Add) -** 新增指定速度限制並顯示在上面的框框中。 **編輯(Edit) -** 允許您編輯選定的限制設定。 **刪除(Delete) -** 刪除限制清單上任何一個您所選定的設定。
聰明頻寬限制 **(Smart Bandwidth Limit)**	勾選此框即可由系統自動控制頻寬。 **傳送限制(TX limit) -** 定義上傳速度限制，如果沒有設定限制值，系統將會使用預設的速度。 **接收限制(RX limit) -** 定義下載速度限制，如果沒有設定限制值，系統將會使用預設的速度。
索引號碼(1-15)於排程設定.. **(Time Schedule)**	您可以輸入四組時間排程，所有的排程都可在**應用-排程(Application >> Schedule)**網頁上事先設定完畢，然後在此輸入該排程的對應索引號碼即可。

完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

4.7.3 服務品質(QoS, Quality of Service)

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。

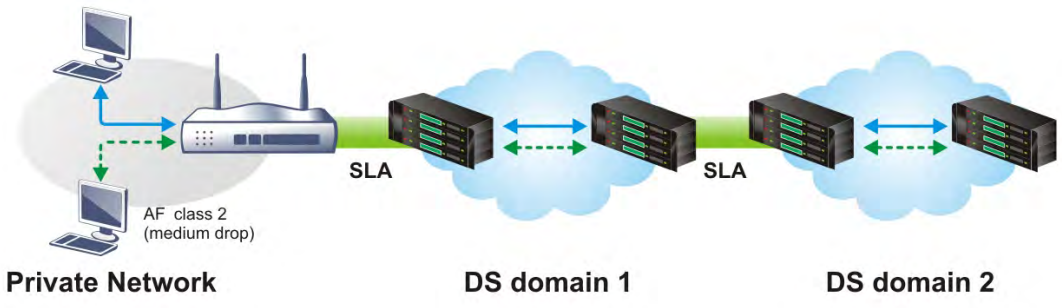
另一個理由是由於網路的擁擠狀況，內部連線迴路速度不符合或是傳輸流量過份聚集，資料封包排隊等候傳送，整個傳輸慢了下來。如果沒有定義後先後順序，以指定在滿檔的隊伍中哪個封包必須丟棄，上述提及的應用程式封包就可能成爲被捨棄掉的一個，這樣的話對應用程式的成效會造成令人無法想像的後果。

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。

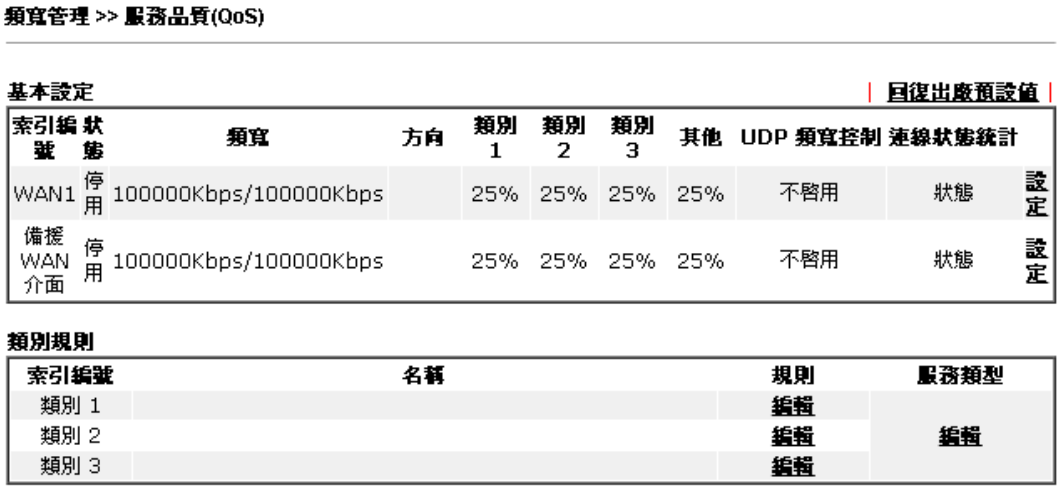
基本 QoS 應用是以 IP 封包頭中之服務類型資訊爲基礎來分類及規劃封包，例如爲了確保封包頭之連線，電信工作人員在執行大量運作時，可能會強迫一個 QoS 控制索引保留頻寬予 HTTP 連線。

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(Bandwidth Management)**群組中，選擇**服務品質(Quality of Service)**開啓如下的網頁。



可用設定說明如下：

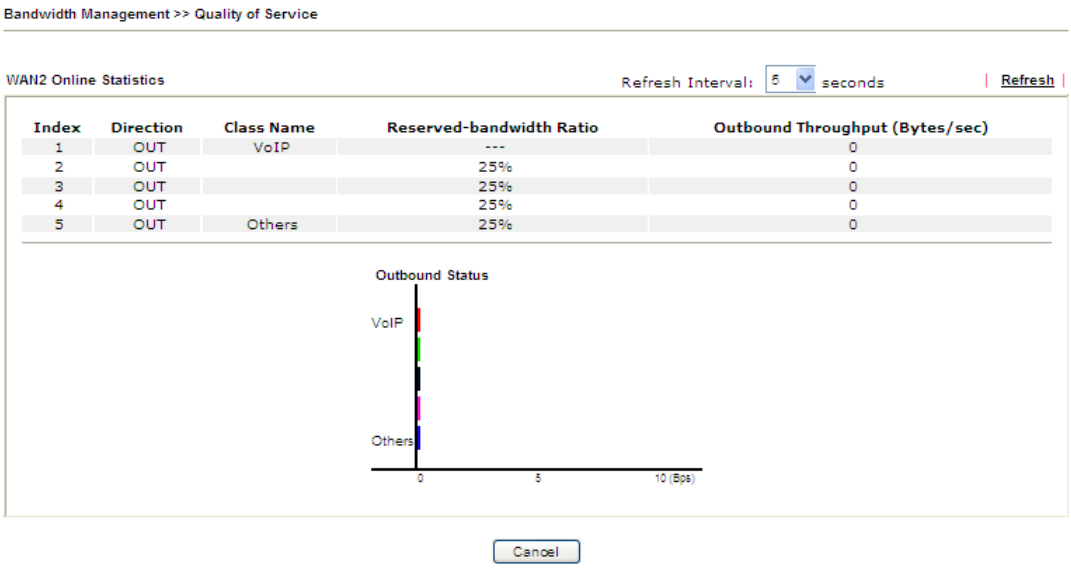
項目	說明
基本設定 (General Setup)	**索引編號(Index)** – 顯示 WAN 介面的編號。 **狀態(Status)** – 顯示該 WAN 介面目前是否爲停用或是啓用。 **頻寬(Bandwidth)** – 顯示該 WAN 介面的上下傳頻寬設定值。 **方向(Direction)** – 顯示此功能會影響的上下傳方向。 **類別 1/類別 2/類別 3/其他(Class 1/Class2/Class 3/Others)** – 顯示每個類別的所佔的頻寬比例。 **UDP 頻寬控制(UDP Bandwidth Control)** – 顯示該控制爲啓用或是停用。 **連線狀態統計(Online Statistics)** – 顯示 QoS 的連線狀態統計情形。 **設定(Setup)** – 允許設定一般 WAN 介面的 QoS 設定。
類別規則 (Class Rule)	**索引編號(Index)** – 顯示您可以編輯的類別編號。 **名稱(Name)** – 顯示該類別的名稱。 **規則(Rule)** – 允許設定該選定類別的細部內容。 **服務類型(Service Type)** – 允許設定該服務類型的細部內容。

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(Edit)**按鈕進入另一層畫面來設定即可。

您可以設定 WAN 介面的一般設定，並視您的需要來編輯類別規則並且編輯類別規則的服務類型。

連線狀態統計

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



基本設定

當您按下**設定(Setup)**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。

可用設定說明如下：

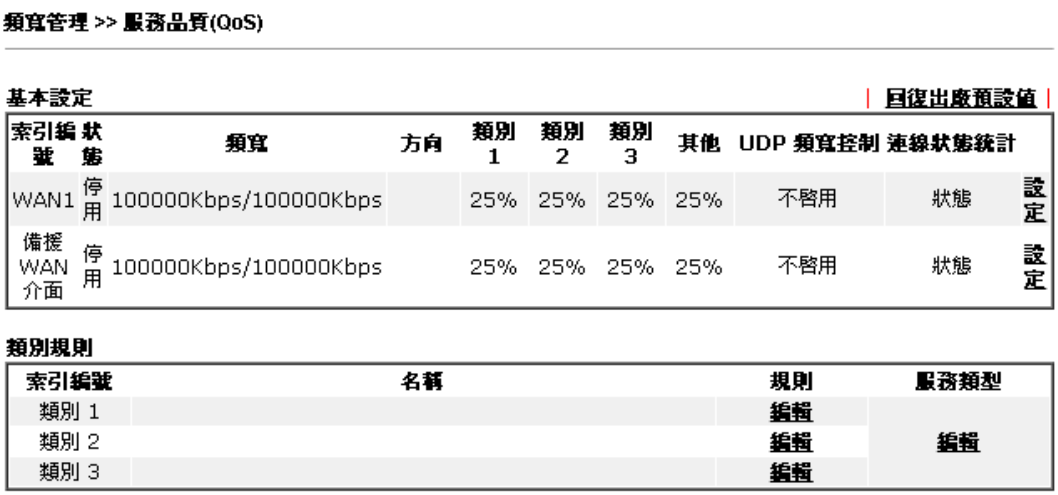
項目	說明
啓用服務品質(QoS)控制功能 **(Enable the QoS Control)**	預設狀態下，這個功能是啓用的。 請同時定義 QoS 控制設應所應用的流量方向。 **下載(IN)-** 僅適用於進入的封包。 **上傳(OUT)-** 僅適用於輸出的封包。 **雙向(BOTH)-** 適用於進入與輸出的封包。

	勾選此方塊並按下**確定(OK)**，**連線狀態統計**連結即可出現在此頁面上。
WAN 下載頻寬 **(WAN Inbound Bandwidth)**	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 **(WAN Outbound Bandwidth)**	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。
保留頻寬比例 **(Reserved Bandwidth Ratio)**	保留作爲群組索引所可應用的比率。
啓用 UDP 頻寬控制 **(Enable UDP Bandwidth Control)**	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 **(Outbound TCP ACK Prioritize)**	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 **(Limited_bandwidth Ratio)**	此處所輸入的比率保留作爲 UDP 應用之需。

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。

編輯 QoS 的類別規則

1. 前三種(類別 1 到類別 3)可視您的需求來調整，編輯或是刪除類別規則，請按該項類別的編輯連結即可。

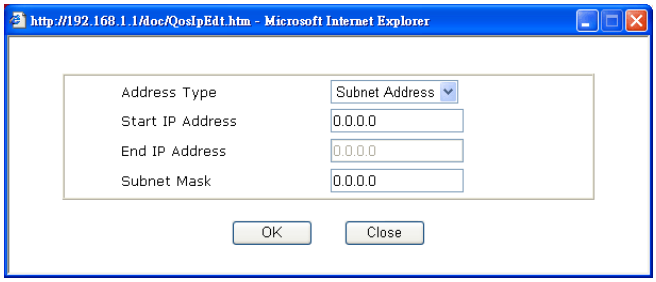


2. 在您按下**編輯(Edit)**連結之後，您可以看到如下的頁面。現在您可以定義該類別的名稱，在本例中，TEST 用來作爲類別索引 1 的名稱。

3. 若要新增一個新的規則，請按**新增(Add)**開啓下列畫面。

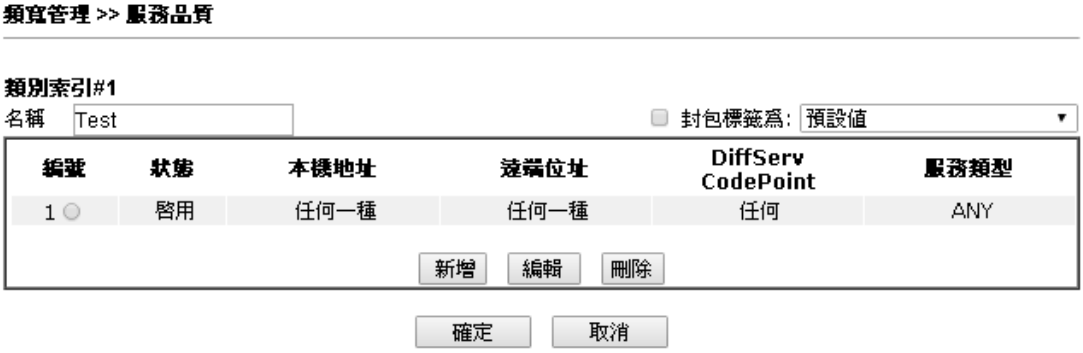
可用設定說明如下：

項目	說明
啓用 (ACT)	勾選此方塊啓用本頁的設定。

本機位址 (Local Address)	按**編輯(Edit)**按鈕以設定規則的來源位址。
遠端位址 (Remote Address)	按**編輯(Edit)**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(Address Type) –** 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(Single Address)**，您可以填入起始 IP 位址。 關於**範圍位址(Range Address,)**，您必須填入起始和終點 IP 位址。 關於**子網路位址(Subnet Addres)**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 (Service Type)	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。

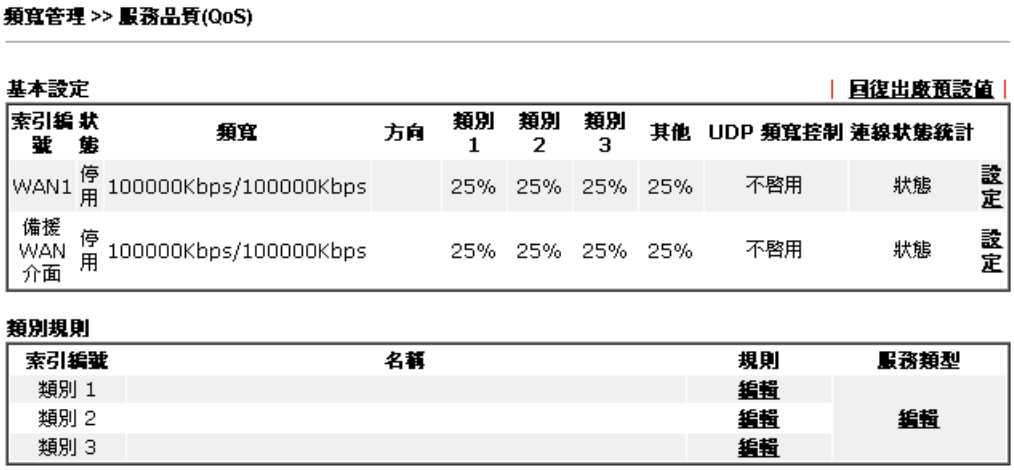
4. 完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

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(Edit)**鈕開啓編輯視窗以修改該規則。



編輯類別規則的服務類型

1. 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(Edit)**連結。



2. 在您按下**編輯**按鈕之後，下述畫面將會出現。

3. 新增一個規則請按下**新增(Add)**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：

可用設定說明如下：

項目	說明
服務名稱 (Service Name)	輸入新的服務名稱。
服務類型 (Service Type)	請選擇新服務所需的類型(TCP, UDP or TCP/UDP)。
通訊埠組態 (Port	**類型(Type)** - 按**單一(Single)**或是**範圍(Range)**，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。

Configuration)	**通訊埠號(Port Number)** –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。

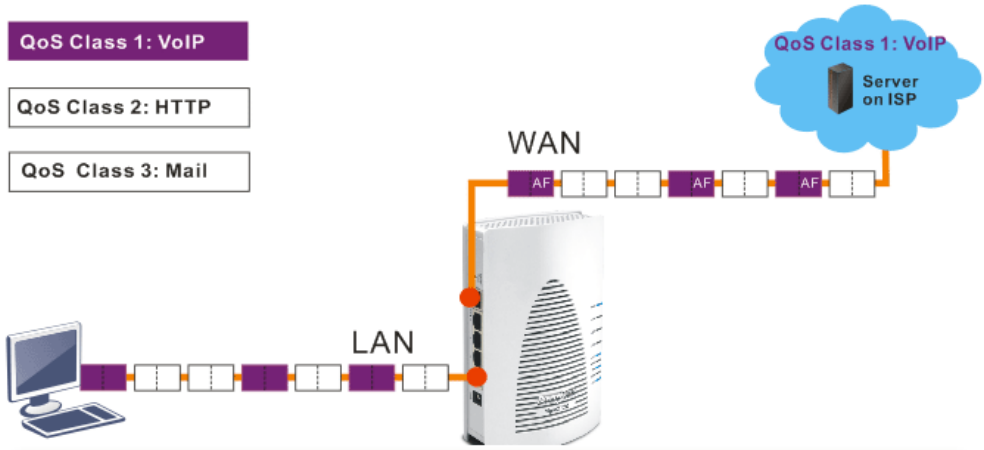
4. 完成設定之後，按下**確定**按鈕儲存相關設定。

另外，您可以指定 10 組服務類型，如果您想要編輯或是刪除現存的服務類型，請點選該項按鈕，然後按下**編輯**鈕開啓編輯視窗以修正該服務類型。

封包重新標籤以供辨識

來自於區域網路 IP 的封包可以透過 QoS 設定封包重新標籤，當該封包透過 WAN 界面傳送出去時，所有的封包都會標示特定的標頭讓 ISP 上的伺服器容易辨識出來。

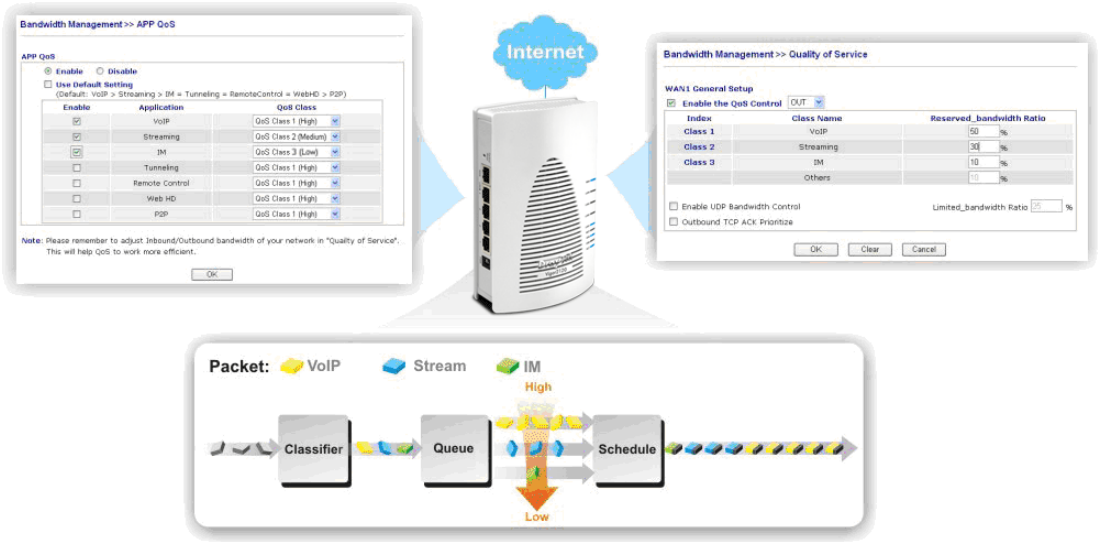
例如，在下述範例圖當中，區域網路端的 VoIP 封包進入路由器時並沒有任何標頭，但是當它們透過路由器轉往 ISP 的伺服器時，所有的封包就都被標示上 AF 標頭(可在頻寬管理>>服務品質(QoS)-- Bandwidth >>QoS>>Class 類別中設定)。



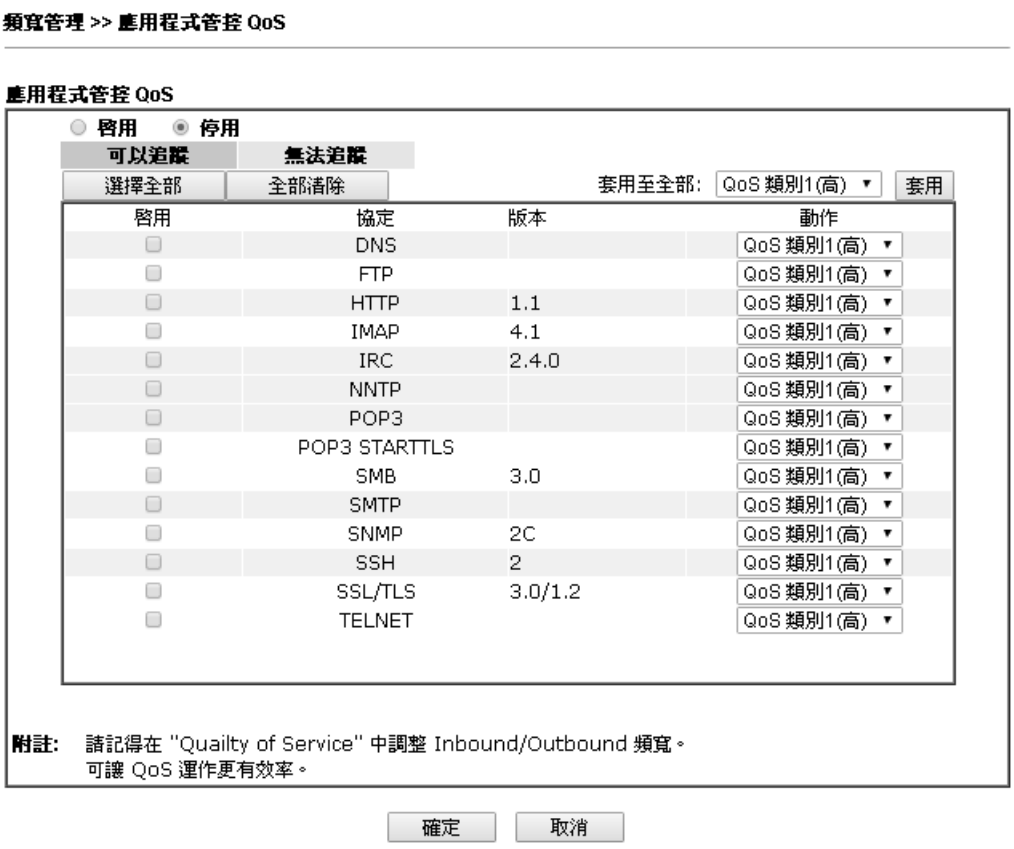
4.7.4 APP QoS

QoS 功能利用指定 IP 或是埠號來管理服務的頻寬。

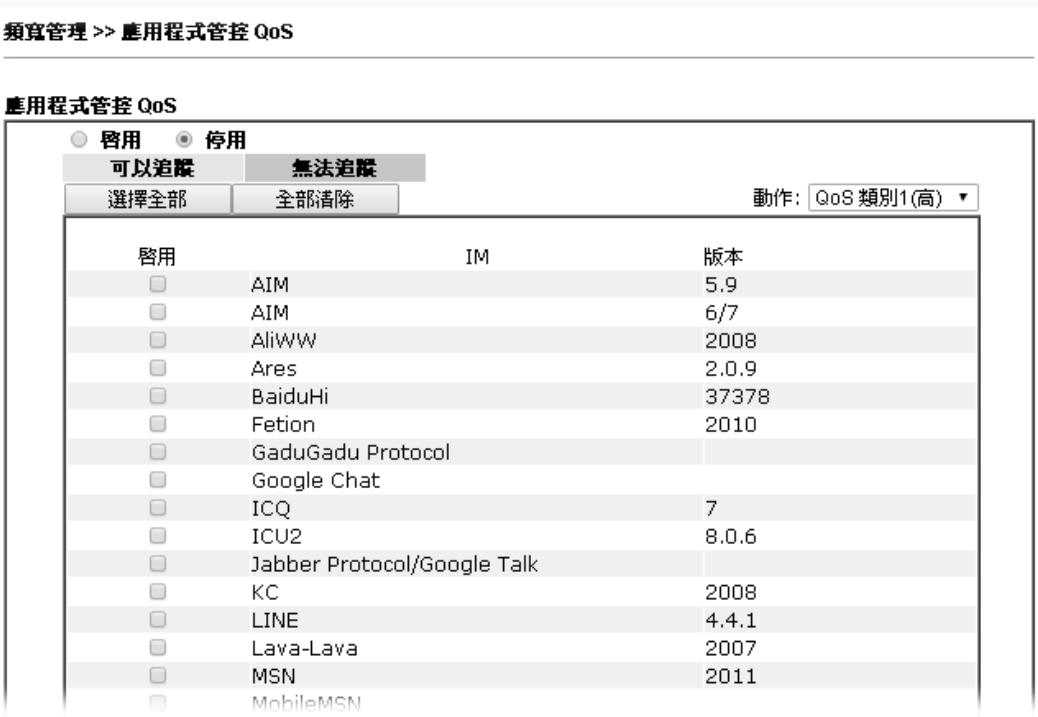
APP QoS 套用應用程式管控功能來偵測數種軟體類型，藉由整合 QoS 功能，Vigor 路由器可以針對 VoIP、字串、IM、P2P 等應用程式進行頻寬管理。



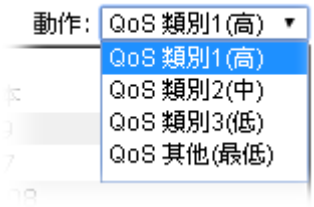
開啓**頻寬管理>> APP QoS(andwidth Management>>APP QoS)**顯示如下的頁面。



下述頁面呈現系統不容易追蹤的應用程式。



可用設定說明如下：

項目	說明
啓用/停用 (Enable/Disable)	選擇**啓用(Enable)**來啓動 APP QoS 功能。 選擇**停用(Disable)**來關閉 APP QoS 功能。
選擇全部(Select All)	按此選擇所有的項目。
清除全部(Clear All)	按此清除全部的選項設定。
動作(Action)	可以如下的 QoS Class 等級來指定 APP。 

4.8 其他應用(Applications)

下圖顯示**其他應用**的功能項目：

4.8.1 動態 DNS(Dynamic DNS)

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

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

啓動此功能並增加一個動態 DNS 帳戶

1. 假設您已經從 DDNS 供應商註冊了一個網域名稱(例如 hostname.dyndns.org)，且獲得一個帳號，其使用者名稱爲 *test*；密碼爲: *test*。
2. 自**其他應用**群組選擇**動態 DNS** 設定，下述頁面即會出現在螢幕上。

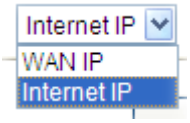
可用設定說明如下：

項目	說明
回復出廠預設值 (Set to Factory Default)	清除全部設定資料並回復到出廠的設定。
啓用動態 DNS 設定 (Enable Dynamic DNS Setup)	勾選此方塊啓用此功能。
檢視記錄 (View Log)	可開啓另一個對話盒並顯示 DDNS 資訊紀錄。
強迫更新 (Force Update)	按此按鈕強迫路由器取得最新的 DNS 資訊。
自動更新間隔 (Auto-Update interval)	輸入動態 DNS 伺服器的自動更新的間隔時間。
索引 (Index)	按下方的號碼連結進入 DDNS 設定頁面，以設定帳戶。
網域 (Domain Name)	顯示您在 DDNS 設定頁面上所設定的網域名稱。
啓用 (Active)	顯示此帳號目前是啓用或是停用狀態。

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(Enable Dynamic DNS)**，然後選擇正確的服務供應商(例 dyndns.org)，輸入註冊的主機名稱(例 hostname)，並於網域名稱區塊中輸入網域的字尾名稱(例 dyndns.org)；接著輸入您的帳號登入名稱(例 dray)和密碼(例 test)。

可用設定說明如下：

項目	說明
啓用動態 DNS 帳號 (Enable Dynamic	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。

DNS Account)	
服務供應商 (Service Provider)	爲此 DDNS 帳號選擇適當的服務供應商。
服務類型 (Service Type)	選擇服務類型(動態、自訂、固定)。如果您選擇的是**自訂**，您可以修正網域名稱區域中所選定的網域資料。
網域名稱 (Domain Name)	輸入您所申請的網域名稱。請使用下拉式選項選擇想要使用的一個名稱。
登入名稱 (Login Name)	輸入您在申請網域名稱時所設定之登入名稱。
密碼 (Password)	輸入您在申請網域名稱時所設定之密碼。
萬用字元及備份 MX (Wildcard and Backup MX)	並非所有的動態 DNS 供應商都支援萬用字元與備份 MX(郵件交換)功能，您可以從其官網取的相關資訊。
郵件延伸程式 (Mail Extender)	某些 DDNS 伺服器可能會要求提供額外的資訊，如電子郵件地址，請您在此輸入必要的電子郵件位址，以配合該 DDNS 伺服器之需要。
決定真實 WAN IP (Determine Real WAN IP)	如果路由器安裝在 NAT 路由器的後端，您可以啓用此功能來定位真實的 WAN IP 位址。 當 Vigor 路由器使用的真實 IP 其實爲虛擬 IP 時，此功能可以偵測出 NAT 路由器使用的真實 IP 並且利用偵測出來的 IP 位址來更新 DDNS。 有二種方法可以選擇  **WAN IP** - 如果選擇此項且路由器的 WAN IP 爲虛擬 IP，那麼 DDNS 更新時就會以偵測到的真實 IP 來替代。 **網際網路 IP (Internet IP)**– 如果選擇此項且路由器的 WAN IP 爲虛擬 IP，在 DDNS 更新之前，它就會被轉換爲真實 IP。

4. 按**確定(OK)**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 LAN DNS

LAN DNS 是簡單版的 DNS 伺服器，使用者不需要在區域網路端建立額外的 DDNS 伺服器，透過此功能，使用者可以針對某些服務(如 ftp, wwww, 或是資料庫)設定容易登入的網域名稱。

每個項目說明如下：

項目	說明
回復出廠預設值 (Set to Factory Default)	清除所有的設定檔內容並回復出廠的預設值。
啓用 (Enable)	勾選此方框啓用選定的設定檔。
索引編號 (Index)	按下索引編號下方的號碼連結可進入設定頁面。
設定檔 (Profile)	顯示 LAN DNS 設定檔的名稱。
網域名稱 (Domain Name)	顯示 LAN DNS 設定檔的網域名稱。

您可以設定 20 組 20 LAN DNS 設定檔。

建立 LAN DNS 設定檔，請依下述步驟來進行：

1. 按下任何一個索引編號，本例採用 1。
2. 細部設定頁面呈現如下圖：

可用設定說明如下：

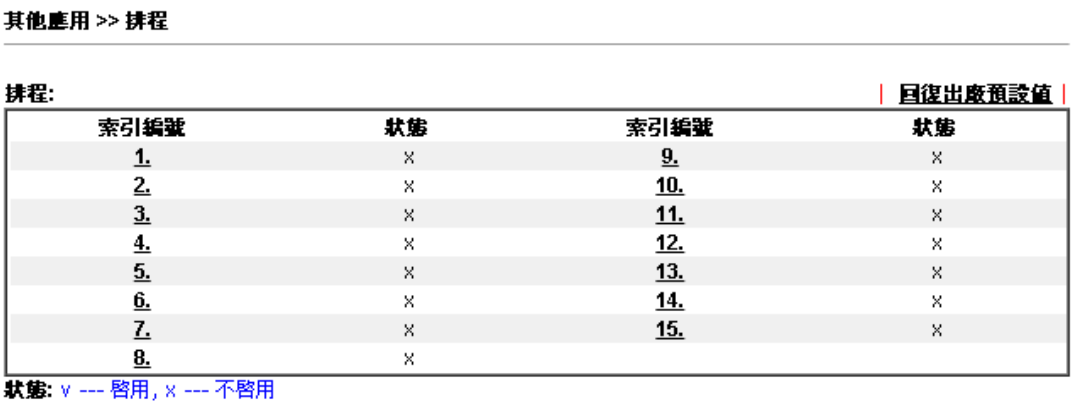
項目	說明
啓用(Enable)	勾選此方框啓用此功能。
設定檔(Profile)	輸入設定檔名。
網域名稱 (Domain Name)	輸入此設定檔的網域名稱。
IP 位址清單 (IP Address List)	IP 位址清單用來對照上述指定的網域名稱，一般來說，一個網域名稱對應一組 IP 位址，如有必要，您可以設定二組 IP 位址給予相同的網域名稱。 **新增(Add)**– 按下此按鈕後會出現如下對話方塊讓您輸入主機的 IP 位址。  ● **當傳送者在相同子網時…. (Only responds to the DNS….)**– 不同區域網路端的電腦以共享相同的網域名稱，但是您必須勾選此方框讓路由器辨認並回應 IP 位址以因應來自區域網路端不同電腦 DNS 詢問要求。 **刪除(Delete)** – 按下此鈕刪除清單中選定的 IP 位址。

3. 按下**確定(OK)**按鈕儲存設定。
4. 新建立的 LAN DNS 設定檔完成如下。

4.8.3 排程(Schedule)

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(System Maintenance>> Time and Date)**以開啓時間設定頁面，按**取得時間(Inquire Time)**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。



每個項目說明如下：

項目	說明
回復出廠預設值 (Set to Factory Default)	清除全部設定資料並回復到出廠的設定。
索引編號(Index)	按下方的號碼進入排程設定頁面。
狀態(Status)	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(Internet Access)**或是**VPN 與遠端存取控制>>LAN-to-LAN(VPN and Remote Access >> LAN-to-LAN)**設定上。

欲新增一個排程：

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

可用設定說明如下：

項目	說明
啓用排程設定 (Enable Schedule Setup)	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 (Action)	指定呼叫排程能採用的方式： **強迫啓用(Force On) -** 強迫連線永遠存在。 **強迫停用(Force Down) -** 強迫連線永遠停止。 **啓用隨選撥接(Enable Dial-On-Demand) -** 指定隨選播接連線以及閒置的時間。 **停用隨選撥接(Disable Dial-On-Demand) -** 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 (Idle Timeout)	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(How often) –** 指定套用的排程頻率。 **一次(Once) -** 此計劃的頻率只會應用一次。 **週期(Weekdays) -** 指定一週當中哪些日子需要執行此項排程作業。

3. 按**確定(OK)**按鈕以儲存設定。

範例

假設您想要控制 PPPoE 網際網路存取連線能夠在每天的 9:00 到 18:00 都能保持開啓狀態(強迫啓用)，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(Force On)**與**強迫停用(Force Down)**來計畫其網際網路連線。

4.8.4 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。

可用設定說明如下：

項目	說明
啓用(Enable)	勾選此項以啓動 RADIUS 設定。
伺服器 IP 位址 (Server IP Address)	輸入 RADIUS 伺服器的 IP 位址。
目的通訊埠 (Destination Port)	輸入 RADIUS 伺服器所使用的 UDP 通訊埠號，基於 RFC 2138，預設值爲 1812。
共享密鑰 (Shared Secret)	RADIUS 伺服器和用戶共用一個用來驗證二者之間傳遞訊息的密鑰，雙方都必須設定相同的共用密鑰。

確認共享密鑰 (Confirm Shared Secret)	請重新輸入共用密鑰以確認。

完成上述設定之後，請按下**確定(OK)**儲存。

4.8.5 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。

注意: 某些應用程式如 PPS, Skype, eMule 等等會需要 UPnP 功能使可運作，但是如果您對 UPnP 並不熟悉，因應安全之故，建議您關閉此功能。

可用設定說明如下：

項目	說明
啓用 UPnP 服務 (Enable UPNP Service)	您可以視情況勾選**啓用連線控制服務(Connection Control Service)**或是**啓用連線狀態服務(Connection Status Service)**。
預設 WAN (Default WAN)	用來指定套用此功能的 WAN 介面。 預設WAN 預設WAN WAN1

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。

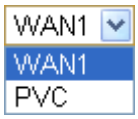
- 某些微軟操作系統已發現到 UPnP 的缺點，因此您需要確定已經應用最新的服務封包。
- 未享有特權的使用者可以控制某些路由器的功能，像是移除和新增通訊埠對應等。

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。

4.8.6 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。

可用設定說明如下：

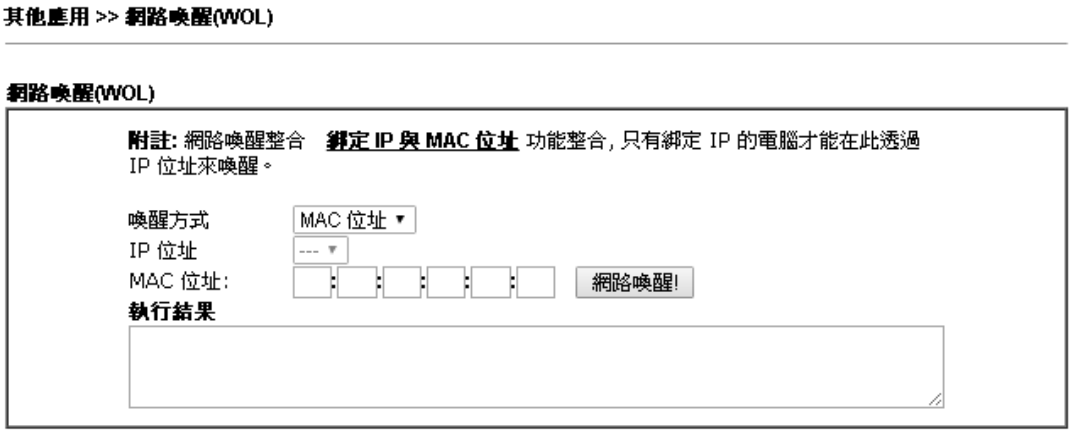
項目	說明
啓用 IGMP 伺服器 (Enable IGMP Proxy)	勾選此方塊啓用此功能。多重播送的應用透過 WAN 埠來執行，另外，此功能在 NAT 模式下始可作用。 
啓用 IGMP Snooping (Enable IGMP Snooping)	勾選此方塊啓用此功能，多重播送流量將會轉送往具有該會員的群組之連接埠中。關閉此功能將會使多重播送流量被視爲一般的廣播播送流量。
更新頁面 (Refresh)	按此連結重新整理並顯示多重播送群組的狀態。
群組 ID (Group ID)	此區顯示多重播送群組的 ID 連接埠，可用範圍爲 224.0.0.0 至 239.255.255.254。
P1 到 P4	多重播送群組中所使用的 LAN 連接埠。

完成上述設定之後，請按下**確定**儲存。

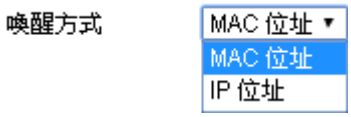
4.8.7 網路喚醒(Wake on LAN)

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

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



可用設定說明如下：

項目	說明
喚醒方式 (Wake by)	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 (IP Address)	已在**防火牆>>綁定 IP 至 MAC(Firewall>>Bind IP to MAC)** 中設定完成的 IP 位址，將會出現在下拉式清單中，請自清單中選取您想要喚醒的電腦 IP。
MAC 位址 (MAC Address)	輸入被綁定之電腦的 MAC 位址。
網路喚醒 (Wake Up)	按此鈕可以喚醒選定的電腦，喚醒結果將會顯示在方框內。

4.8.8 簡訊(SMS) / 郵件警示服務(SMS / Mail Alert Service)

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

Vigor 路由器可讓您設定 10 組簡訊設定檔，可依據不同條件發送出去。

簡訊(SMS)服務供應商

本頁讓您指定簡訊服務供應商、收信人爲何以及收信內容。

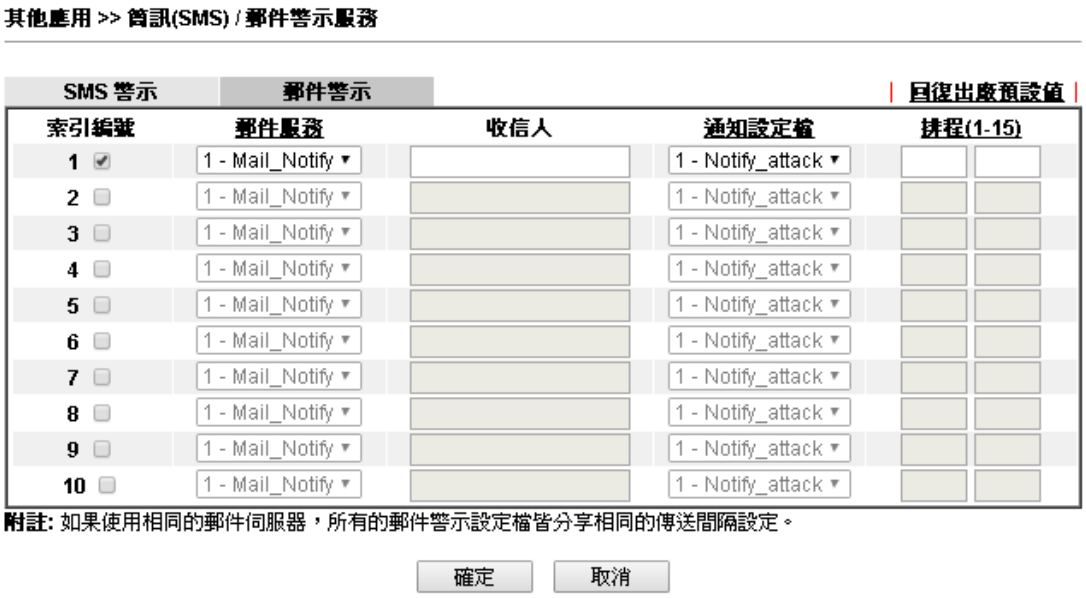
可用設定說明如下：

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

完成上述設定之後，請按下**確定(OK)**儲存。

郵件伺服器(Mail Server)

本頁讓您指定郵件伺服器設定檔，收信人爲何以及收信內容。



可用設定說明如下：

項目	說明
索引編號 (Index)	勾選此方框啓用設定檔。
郵件服務 (Mail Service)	使用下拉式清單選擇郵件服務供應商。 您可以點**郵件服務(Mail Service)**連結來定義郵件伺服器。
收信人 (Recipient)	輸入收信人的電子郵件信箱。
通知設定檔(Notify)	使用下拉式清單選擇訊息設定檔。收信人將會收到通知設定檔內的訊息。 您可以點**通知設定檔(Notify Profile)**連結來定義簡訊的內容。
排程 (1-15) (Schedule)	輸入簡訊發出的時間排程編號。 您可點**排程(1-15)(Schedule(1-15))**連結來定義排程內容。

完成上述設定之後，請按下**確定(OK)**儲存。

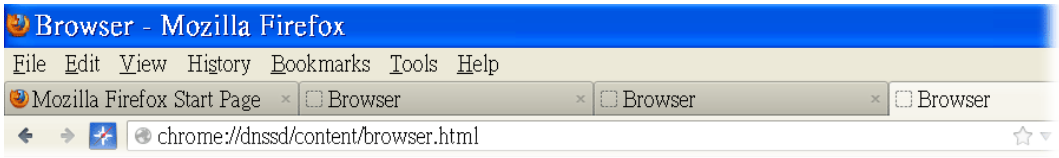
4.8.9 Bonjour

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

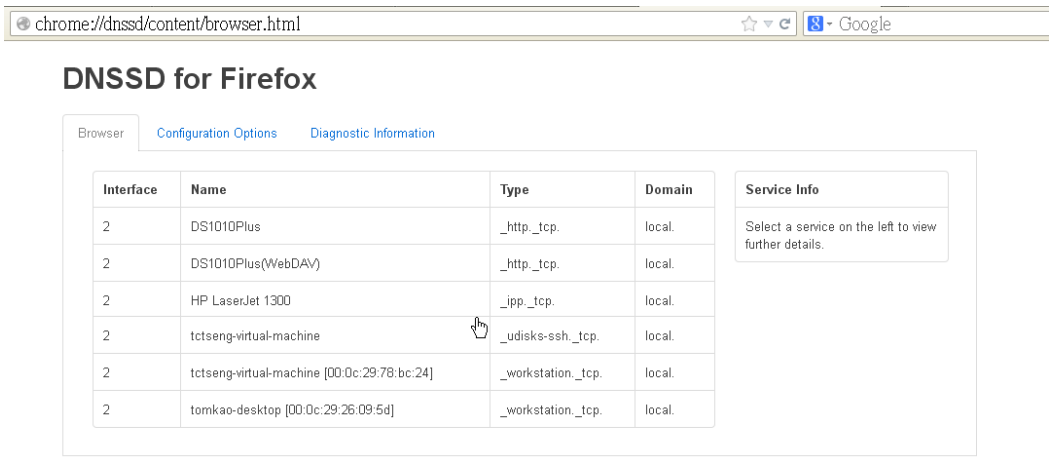
要啓用 Bonjour 服務，請開啓**其他應用>>Bonjour(Application>>Bonjour)**，勾選您想要分享區域網路用戶的服務項目。

下面提供一個簡單的範例來應用 bonjour 功能：

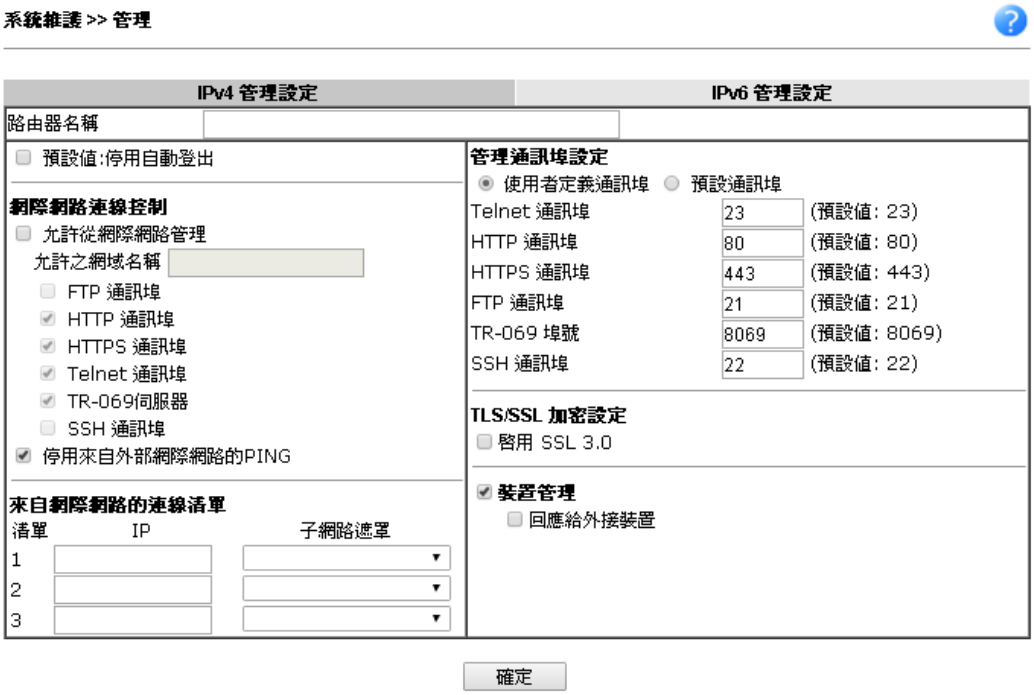
1. 此處我們使用 Firefox 與 DNSSD 來說明，請先確認 Bonjour 用戶端程式與 Firefox 的 DNSSD 已經安裝在電腦上。



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

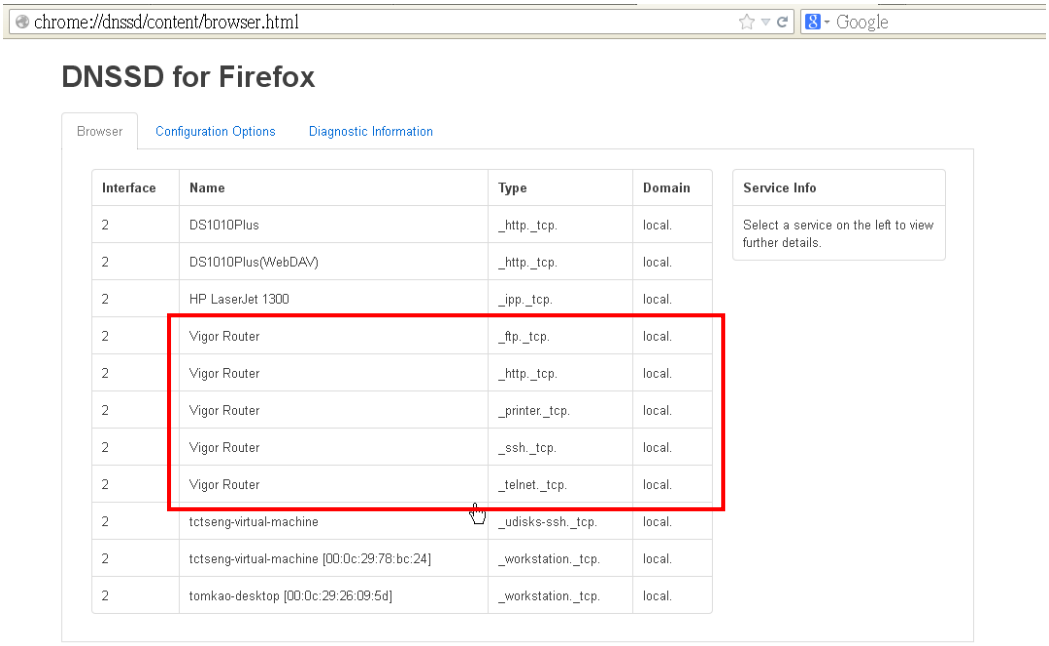


3. 開啓**系統維護>>管理(System Maintenance>>Management.)**，輸入**路由器名稱**(例如 Dray)，然後按下**確定(OK)**儲存。

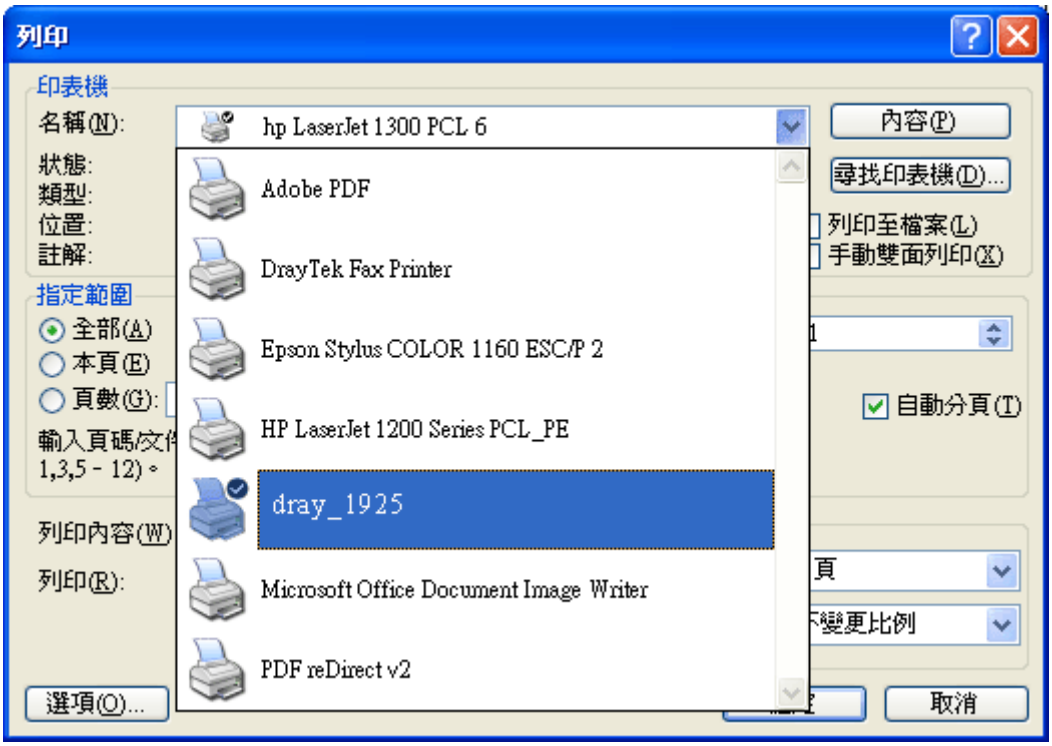


4. 接著，開啓**其他應用>>Bonjour(Applications>>Bonjour)**，勾選您想要透過 Bonjour 分享的服務。

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



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



4.9 VPN 與遠端存取(VPN and Remote Access)

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 遠端存取控制(Remote Access Control)

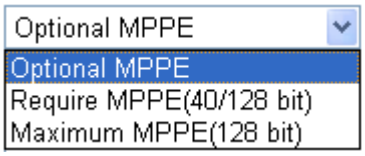
這個設定可以啓動必要的 VPN 服務，如果您想要在區域網路中執行 VPN 伺服器功能，您一定要適度關閉路由器的 VPN 服務，讓 VPN 通道暢通，並關閉類似 DMZ 或是開放埠等 NAT 設定。

完成上述設定之後，請按下**確定(OK)**儲存。

4.9.2 PPP 基本設定(PPP General Setup)

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

可用設定說明如下：

項目	說明
撥入 PPP 驗證 **(Dial-In PPP Authentication)**	**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) **(Dial-In PPP Encryption (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) **(Mutual Authentication (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。
指派 IP 位址 **(Assigned IP Start)**	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。

完成上述設定之後，請按下**確定(OK)**儲存。

4.9.3 IPSec IPSec 基本設定(IPsec General Setup)

在 **IPSec 基本設定**中，有二種主要的配置方式。

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

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

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

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

可用設定說明如下：

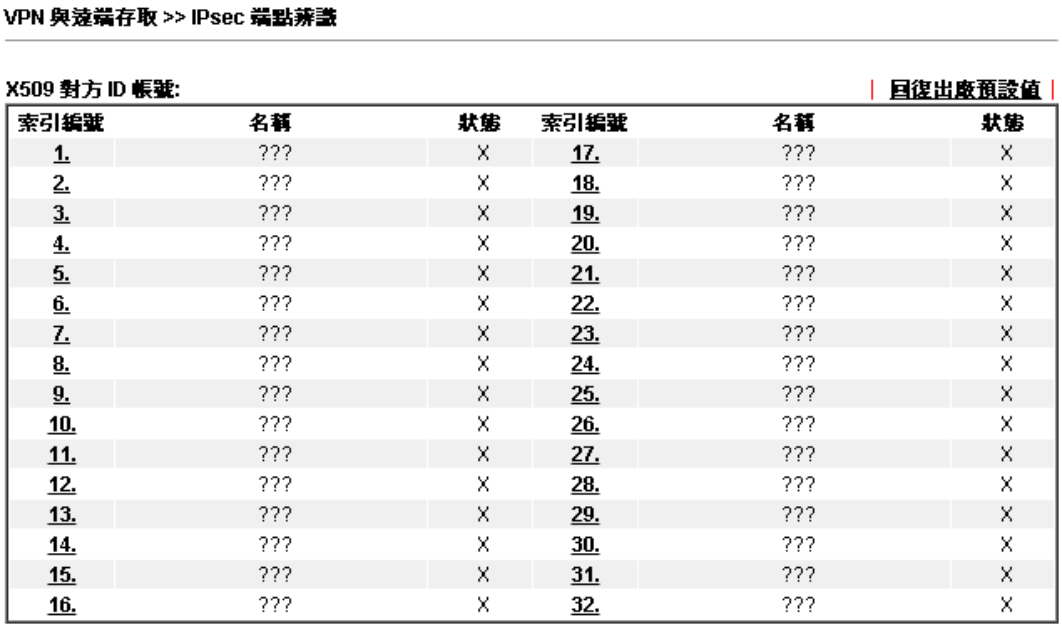
項目	說明
IKE 認證方式 **(IKE Authentication Method)**	通常應用在遠端撥入使用者或是使用動態 IP 位址的節點(LAN-to-LAN)以及 IPSec 相關之 VPN 連線上，像是 L2TP over IPSec 和 IPSec 通道。 **撥入憑證(Certification for Dial-in)** – 選擇一組本地憑證。

	預先共用金鑰(Pre-Shared Key) - 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(Confirm Pre-Shared Key)-** 確認您所輸入的共用金鑰。
IPSec 安全防護方式 (IPsec Security Method)	**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。

完成上述設定之後，請按下**確定(OK)**儲存。

4.9.4 IPSec 端點辨識(IPsec Peer Identity)

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：



可用設定說明如下：

項目	說明
回復出廠預設值 (Set to Factory Default)	按此鈕清除全部設定。
索引編號 (Index)	請按索引下方的號碼以進入設定頁面。
名稱 (Name)	顯示 LAN-to-LAN 設定檔案中特定撥入使用者的使用者名稱，符號**???**代表該設定檔是空的，未做任何設定。

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

可用設定說明如下：

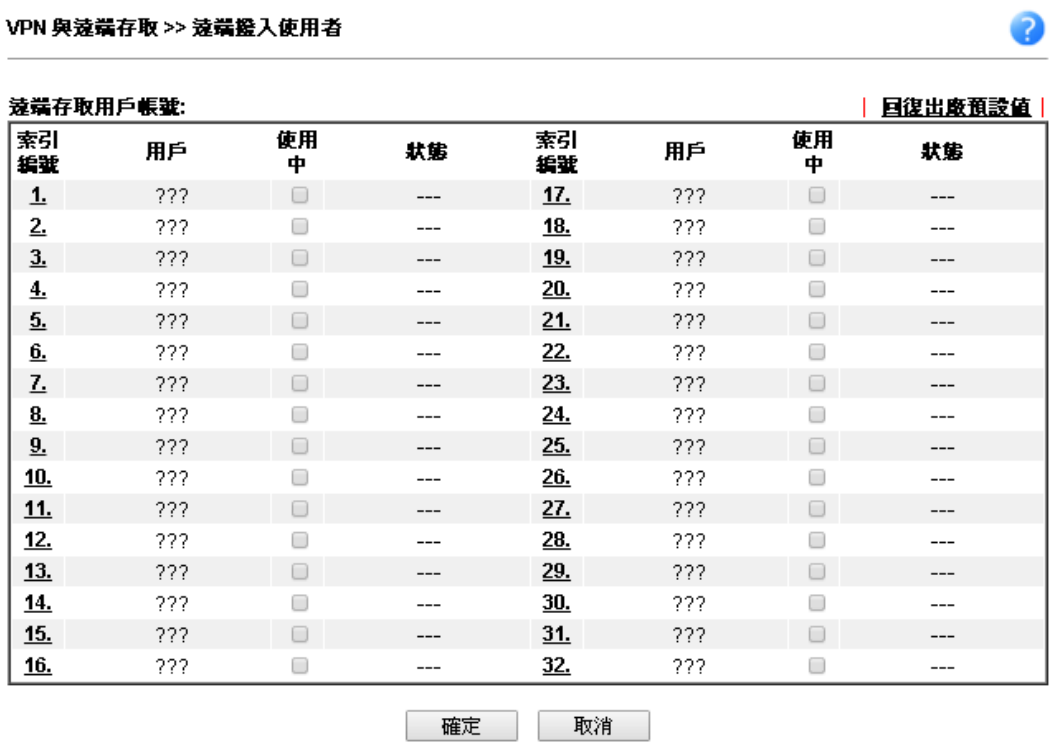
項目	說明
設定檔名稱 (Profile Name)	請輸入此設定檔的檔名。
啓動這個帳號 (Enable this account)	勾選方框啓用帳號設定檔。
接收任何對方 ID (Accept Any Peer ID)	按此鈕可以接受任何一個電腦的連線而不理會它是誰。
接受主體替代名稱 (Accept Subject Alternative Name)	按此鈕以決定特定之數位簽章接受符合要求的對手，本區可以是 IP 位址、網域或是電子郵件，類型下方區域方塊依據您所選的類型而有所不同，請按照實際需要填入必要資訊。
接受主體名稱 (Accept Subject Name)	按此鈕讓特定區域的數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

完成上述設定之後，請按下**確定(OK)**儲存。

4.9.5 遠端撥入使用者(Remote Dial-in User)

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。

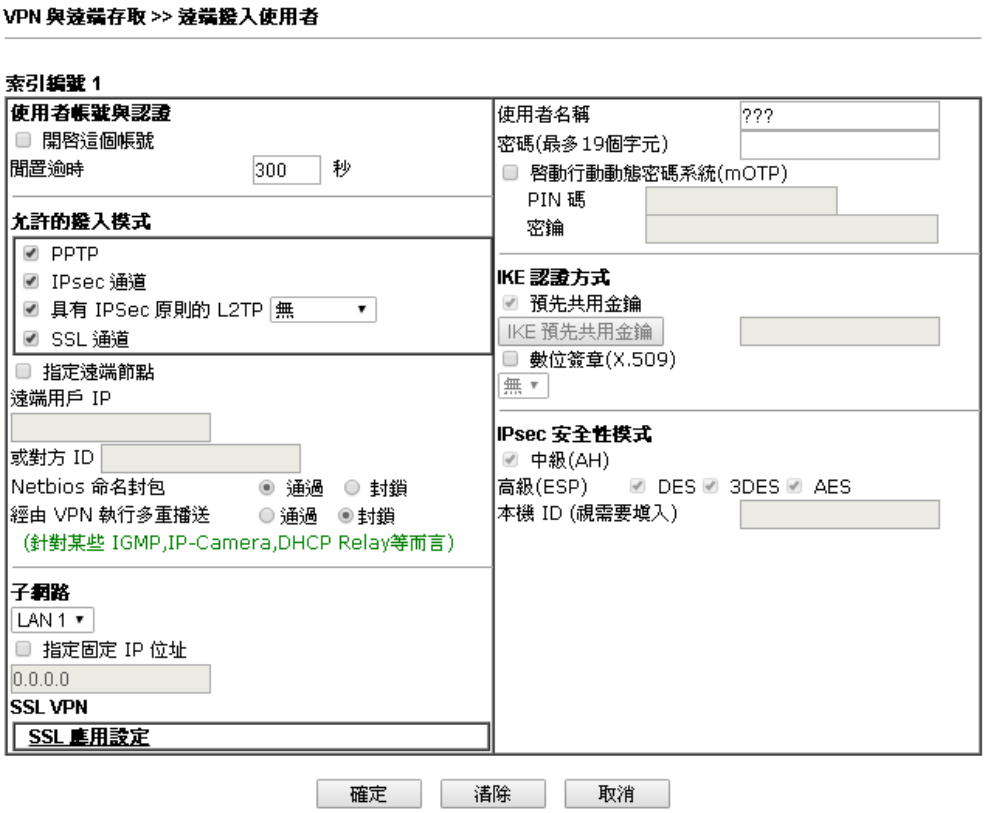
路由器提供 **32** 種存取使用者號碼予撥入用戶，此外經由內建 RADIUS 用戶端功能，您可以將帳號延伸至 RADIUS 伺服器。下圖顯示帳號總表格：



可用設定說明如下：

項目	說明
回復出廠預設值 (Set to Factory Default)	按此鈕清除全部設定。
索引編號 (Index)	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 (User)	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。
使用中 (Active)	勾選方塊以便啓用該設定檔。
狀態 (Status)	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。



可用設定說明如下：

項目	說明
使用者帳號與認證 (User account and Authentication)	**開啓這個帳號(Enable this accoun)** -勾選此方塊以啓用此功能。 **閒置逾時(Idle Timeout)** - 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。
允許的撥入類型 (Allowed Dial-In Type)	**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(IPsec Tunnel)**-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(L2TP with IPsec Policy)**-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(None)** - 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(Nice to Have)** -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(Must) -** 此選項可在 L2TP 連線中明確指定所要運用的 IPSec 原則。 **SSL 通道(SSL Tunnel) –** 允許遠端撥入用戶透過網際網路進行 SSL VPN 連線。 **指定遠端節點(Specify Remote Node)-**您可以指定遠端撥入使用者或是對方 ID (應用於 IKE 主動模式中)的 IP 位址。若您不勾選此項，即表示您所選擇的連線類型，將會應用**基本設定**中所設定的驗證方式和安全防護方式。 **Netbios 命名封包 (Netbios Naming Packet)–** ● **通過(Pass)** – 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(Block)** –當雙方所建立的 VPN 通道連線產生衝突時，此功能可以封鎖此通道。 **經由 VPN 執行多重播送(Multicast via VPN) -**某些程式可透過 VPN 連線進行多重播送封包。 ● **通過(Pass)** –點選此鈕讓多重播送封包通過路由器。 ● **封鎖(Block)** – 此爲預設值。點選此鈕之後，路由器將會封鎖多重播送封包。 **使用者名稱(User Name)-**當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區是可應用的。 **密碼(Password)-**當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區是可應用的。 **啓動行動動態密碼系統 (mOTP)(Enable Mobile One-Time Passwords (mOTP)) -** 勾選此框以便利用 mOTP 功能進行驗證。 **PIN 碼(PIN Code)**– 輸入驗證專用碼（例如 1234）。 **密碼(Secret)** – 使用行動電話中由 mOTP 產生的 32 個數字密碼(例如 e759bb6f0e94c7ab4fe6）。
子網路 (Subnet)	選擇此 VPN 設定檔所需的子網。 **指定固定 IP 位址(Assign Static IP Address)–** 請輸入固定 IP 位址。
SSL VPN	**設定 SSL 應用(SSL Application)** – 選擇 SSL 應用程式設定檔，以便套用至撥入使用者設定檔。
IKE 認證方式 (IKE Authentication Method)	當您指定遠端節點的 IP 位址時，本區僅適用於 **IPsec 通道**與**具有 IPSec 原則的 L2TP** 類型，唯一例外的是當您選擇 **IPsec 通道**時，不論有無指定 IP 位址，您還可以設定數位簽章(X.509)。 **預先共同金鑰(Pre-Shared Key)-** 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)(Digital Signature (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(VPN and Remote Access**

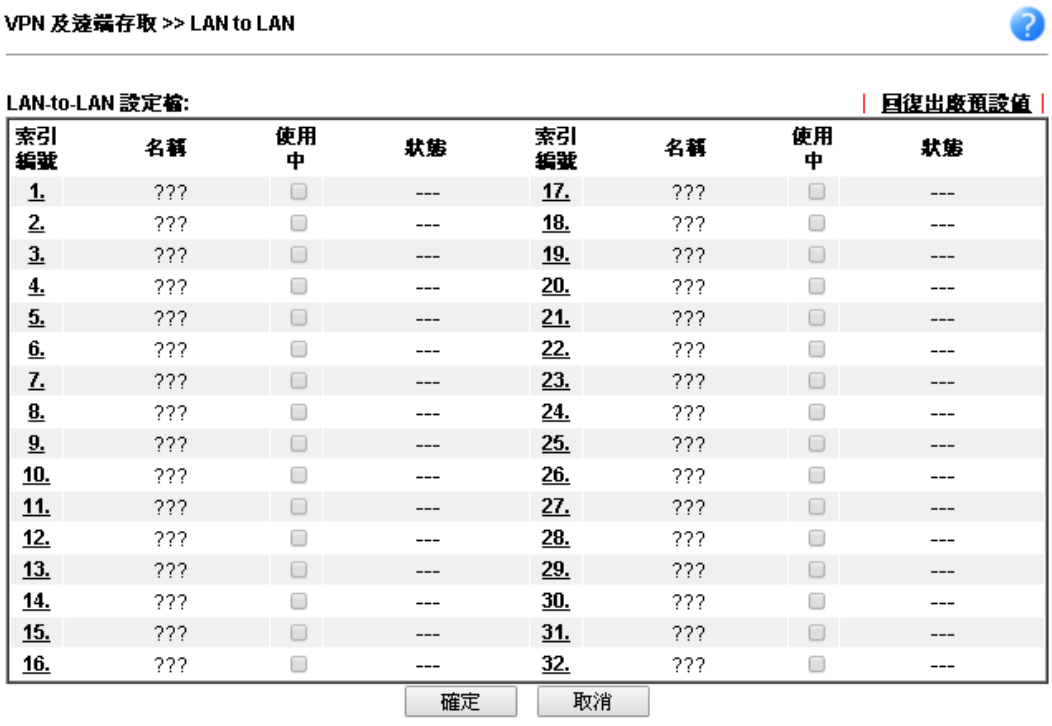
	>>IPsec Peer Identity)中設定)。
IPSec 安全防護方式 **(IPsec Security Method)**	對 IPSec 通道和 L2TP 含 IPSec 原則來說，本區爲必要設定。請勾選中級或是高級設定作爲安全防護方式。 **中級 -Authentication Header (AH)**表示資料將被驗證，但未被加密，此選項的預設時是勾選狀態。 **高級 -Encapsulating Security Payload (ESP)**表示資料將被加密及驗證，請自下拉式清單中選取適合項目。 **本機 ID(視需要填入)**-指定一個本地 ID 以便作爲 LAN-to-LAN 的撥入設定，此項是選擇項目且只能應用在 IKE 主動模式上。

完成上述設定之後，請按下**確定(OK)**儲存。

4.9.6 LAN to LAN 設定

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。



可用設定說明如下：

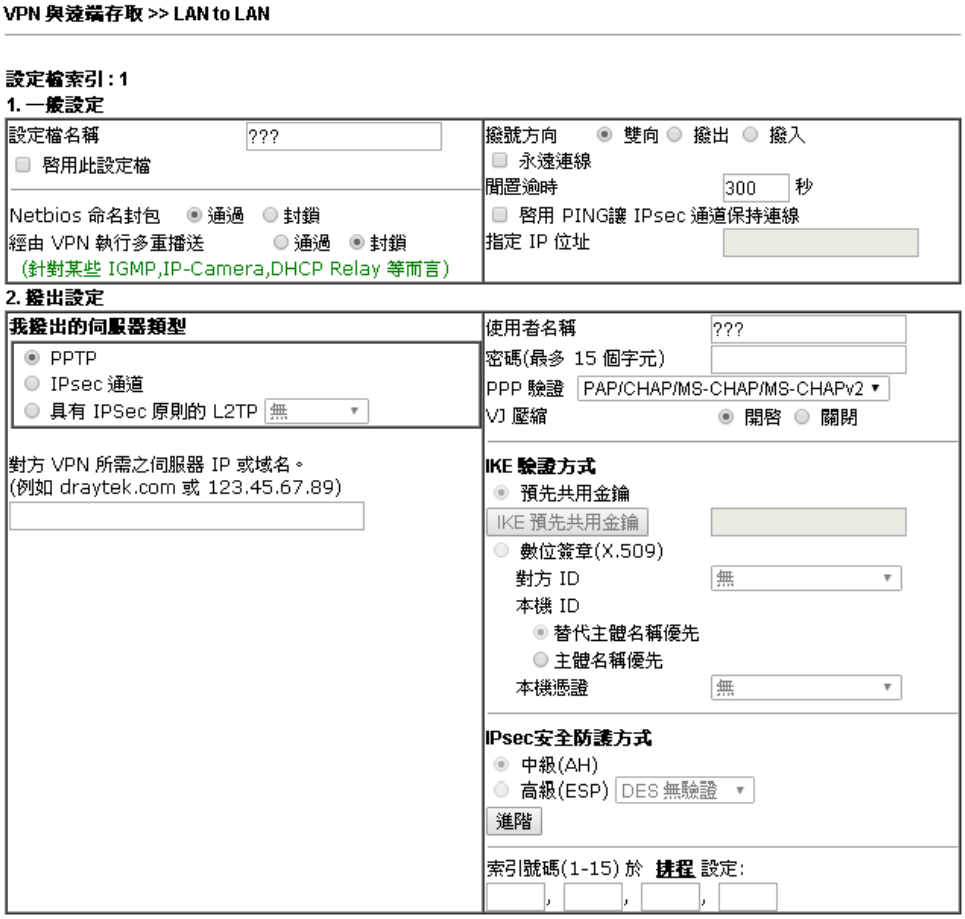
項目	說明
回復出廠預設值 **(Set to Factory Default)**	按此鈕清除全部設定。
索引編號	請按索引下方的號碼以進入設定頁面。

(Index)	
名稱 (Name)	意即 LAN-to-LAN 檔案名稱，**???**符號代表該檔案目前是空的。
使用中 (Active)	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。
狀態 (Status)	Online – 表示此 LAN to LAN 設定檔目前運作中。 Offline – 表示此 LAN to LAN 設定檔目前並未運作，即使已經啓動。

如欲編輯設定檔，請：

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

   由於網頁太長，我們將之切成數個段落來說明。



可用設定說明如下：

項目	說明
一般設定 (Common Settings)	**設定檔名稱(Profile Name) -** 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(Enable this profile)**-按此方塊啓用此設定

	檔。 **Netbios 命名封包** ● **通過(Pass)** – 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(Block)**– 當雙方所建立的 VPN 通道連線產生衝突時，此功能可以封鎖此通道。 **經由 VPN 執行多重播送(Multicast via VPN)** -某些程式可透過 VPN 連線進行多重播送封包。 ● **通過(Pass)** –點選此鈕讓多重播送封包通過路由器。 ● **封鎖(Block)** – 此爲預設值。點選此鈕之後，路由器將會封鎖多重播送封包。 **撥號方向(Call Direction)** -針對此 LAN-to-LAN 連線，請指定允許的撥號方向。 ● **雙向(Both)**– 發話方/接話方 ● **撥出(Dial-Out)** - 發話方 ● **撥入(Dial-In)** - 接話方 **永遠連線(Always On)** – 勾選此方塊讓路由器永遠保持 VPN 連線。 **閒置逾時(Idle Timeout)** - 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(Enable PING to keep alive)** -此功能可協助路由器決定 IPSec VPN 連線狀態，對不正常的 IPSec VPN 通道中斷尤其有用。詳細內容請參考下面的註解，請勾選此方塊啓動 PING 封包傳輸至指定的 IP 位址。 **指定 IP 位址** - 輸入 VPN 通道另一端的主機 IP 位址。
撥出設定 **(Dial-Out Settings)**	**我撥出的伺服器類型(Type of Server I am calling)** – **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(IPsec Tunnel)**-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(L2TP with IPsec Policy)**-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(None)**-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(Nice to Have)** -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(Must)** - 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(User Name)-當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區是可應用的。

密碼(Password)-當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區是可應用的。

PPP 驗證(PPP Authentication)-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(VJ compression)-當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區是可應用的。VJ 壓縮可作爲 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(IKE Authentication Method) - 這個功能適用 **IPsec 通道**與**具有 IPSec 原則的 L2TP**。

- **預先共用金鑰(Pre-Shared Key)**- 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)(Digital Signature (X.509))** –勾選此方塊啓用此功能並選擇一組事先定義的簽章內容(在 **VPN 和遠端存取>>IPSec 端點辨識**中設定)。

  對方 ID(Peer ID) - 自下拉式清單中(設定於 **VPN 與遠端存取>>IPsec 端點辨識(VPN and Remote Access >>IPsec Peer Identity)**)選擇對方的 ID。

  本機 ID(Local ID) –指定一個本機 ID(**替代主體名稱優先- Alternative Subject Name First** 或是**主體名稱優先- Subject Name First)**，用於撥入設定，這個項目是選填項目。
- **本機憑證(Local Certificate)** – 自下拉式清單中選擇一種憑證，您必須事先在**憑證管理>>本機憑證(Certificate Management>>Local Certificate)**中設定至少一組的憑證，否則無憑證正可以使用。

IPSec 安全防護方式(IPsec Security Method) -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*(*DES without Authentication*)*** - 使用 DES 加密演算式，但不採用任何驗證計畫。
- **DES 有驗證 (DES with Authentication)**- 使用 DES 加密演算式，且採用 MD5 或 SHA-1 驗證計畫。
- **3DES 無驗證(3DES without Authentication)** - 使用三重 DES 加密演算式，但不採用任何驗證計畫。

- **3DES 有驗證(3DES with Authentication) -**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(AES without Authenticatio) -** 使用 AES 加密演算式，但不採用任何驗證計畫。
- **AES 有驗證(AES with Authentication) -**使用 AES 加密演算式，且採用 MD5 或 SHA-1 驗證計畫。

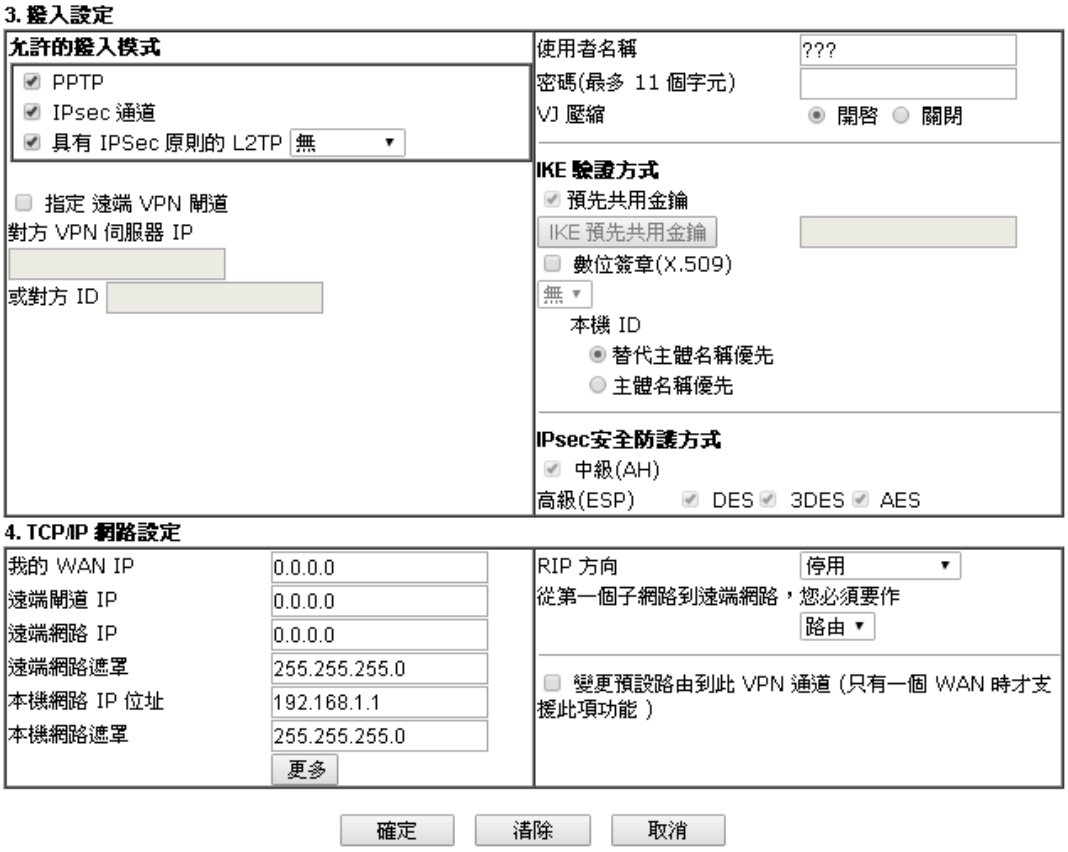
進階(Advanced)-指定模式、建議和 IKE 階段金鑰有效時間等設定，可按**進階**按鈕進入進階設定，視窗顯示如下：

IKE 階段 1 模式(IKE phase 1 mode) – 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(IKE phase 1 proposal) -** 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。
- **IKE 階段 2 建議(IKE phase 2 proposal) -** 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。
- **IKE 階段 1 金鑰有效時間(IKE phase 1 key lifetime)-** 考慮到安全之故，使用者必須訂定有效時間，預設值爲 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(IKE phase 2 key lifetime)-** 考慮到安全之故，使用者必須訂定有效時間，預設值爲 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(Local ID) – 在 **Aggressive 模式**中，當鑑定遠端 VPN 伺服器身分時，本機 ID 代表 IP 位址，ID 長度限制於 47 個字元。

	索引號碼(1-15) 於排程設定(Index(1-15))可以輸入四組時間排程，全部的排程都是在**其他應用>>排程(Applications >> Schedule)**網頁中事先設定完畢，您可在此輸入該排程的索引編號。



可用設定說明如下：

項目	說明
撥入設定 (Dial-In Settings)	**允許的撥入類型(Allowed Dial-In Type)**-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(IPsec Tunnel)**-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(L2TP with IPsec Policy)**-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(None)** - 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(Nice to Have)**-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(Must) -** 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 VPN 閘道(Specify Remote VPN Gateway) -您可勾選此項，並指定遠端撥入用戶的真實 IP 位址或 ID (必須與撥入類型中所設定的 ID 相同)。此外針對 VPN 功能，您應該進一步指定右邊相關安全設定。

如果您不勾選此方框，您上述選定的連線類型將會套用基本設定中所選用的驗證方式及安全性方法。

使用者名稱(User Name)-當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區是可應用的。

密碼(Password)-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(VJ Compression)-當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區是可應用的。VJ 壓縮可作爲 TCP/IP 協定標頭壓縮之用。

IKE 驗證方式(IKE Authentication Method) -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)。

- **預先共用金鑰(Pre-Shared Key)-** 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)(Digital Signature (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(VPN and Remote Access >>IPsec Peer Identity)**中所預先定義的設定檔。
  - **本機 ID(Local ID)**–指定先檢測下方哪一種類型。
  - **替代主體名稱優先(Alternative Subject Name First)** – 先檢測替代主體名稱(於**憑證管理>>本機憑證**中定義)。
  - **主體名稱優先(Subject Name First)** – 先檢測主體名稱(於**憑證管理>>本機憑證(Certificate Management>>Local Certificate)**中定義)。

IPSec 安全防護方式(IPsec Security Method)-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。

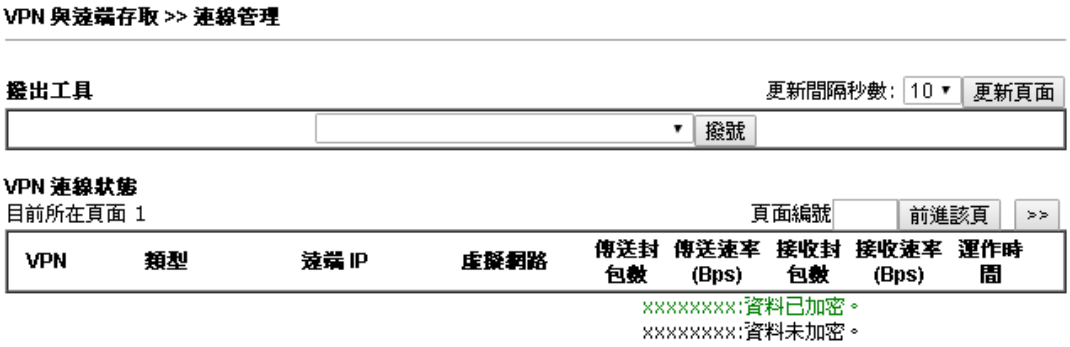
- **中級(Medium)-** 表示資料將被驗證，但未被加密，此選項的預設時是勾選狀態。
- **高級(High) -** 表示資料將被加密及驗證，請自下拉式清單中選取適合項目。

TCP/IP 網路設定 **(TCP/IP Network Settings)**	**我的 WAN IP(My 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(Remote Gateway 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(Remote Network IP/ Remote Network Mas)** - 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。 **本機網路 IP 位址/ 本機網路遮罩(Local Network IP / Local Network Mask) –** 顯示 TCP / IP 設定中的本機網路 IP 位址與遮罩，如有必要，您可以修改設定。 **更多(More)**-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(RIP Direction)**-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(From first subnet to remote network, you have to do)** -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(Route)**。 **變更預設路由此 VPN 通道(Change default route to this VPN tunnel)** -勾選此方塊變更此 VPN 通道的預設路由。

2. 完成上述設定之後，請按下**確定(OK)**儲存。

4.9.7 連線管理(Connection Management)

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



可用設定說明如下：

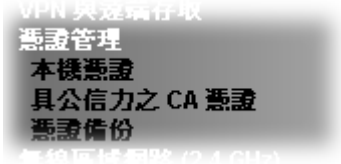
項目	說明
撥號工具(Dial-out Tool)	**撥號(Dial) -** 按此鈕執行撥號功能。 **更新間隔秒數(Refresh Second)-**選擇重新顯示狀態的間隔秒數，有 5、10、30 秒等三種選擇。 **更新頁面(Refresh)-**按此鈕以重新顯示整個連線狀態。

4.10 憑證管理(Certificate Management)

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(Local Certificate)

可用設定說明如下：

項目	說明
產生 **(Generate)**	按此鈕以開啓**產生憑證需求(Generate Certificate Request)**視窗。 輸入全部的資訊，然後再按一次**產生(Generate)**按鈕。
匯入 **(Import)**	按此鈕以匯入儲存的檔案作爲憑證資訊。
更新頁面 **(Refresh)**	按此鈕以更新資訊。
檢視 **(View)**	按此鈕以檢視憑證詳細的設定。  **注意:**您必須從上圖視窗中複製憑證需求資訊，接著進入 CA 伺服器並進入憑證需求頁面，將此複製資訊貼上並提交需求，CA 伺服器就會提供您一個新的憑證，請保存起來。
刪除 **(Delete)**	按此鈕刪除選定的憑證及其相關資訊。

產生(GENERATE)

按下此鈕開啓**產生本機憑證需求(Generate Certificate Signing Request)**視窗，輸入所有必要資訊，例如檔名(用來分辨憑證)、主體替代名稱類型以及相關的設定內容，然後按最下方的**產生(GENERATE)**按鈕。

注意: 請注意常用名稱(Common Name)必須設定爲路由器的 WAN IP 位址或是網址。

按下**產生(GENERATE)**按鈕之後，憑證產生的資訊就會顯示在畫面上：

匯入(IMPORT)

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

按下此鈕後可以匯入檔案作爲憑證資訊，有三種本機憑證類型可以運用。

可用設定說明如下：

項目	說明
上傳本機憑證 **(Upload Local Certificate)**	允許使用者輸入路由器產生且 CA 伺服器簽核過的憑證。 如果您在憑證產生的步驟中順利完成憑證建立，憑證的狀態欄位下方就會顯示 OK。
上傳 PKCS12 憑證 **(Upload PKCS12 Certificate)**	允許使用者上傳憑證，通常其副檔名爲.pfx 或是.p12，且這些憑證需要密碼驗證。 **注意:** PKCS12 是安全地儲存私人密鑰以及憑證的標準，它可利用輸入輸出選項於 Netscape 以及 Microsoft Internet Explorer 運用。
上傳憑證及私人密鑰 **(Upload Certificate and Private Key)**	當使用者有不同的憑證及私人密鑰時，可以使用本區功能來匯入，如果私人密鑰有被加密，那麼還需要輸入密碼以便進行驗證。

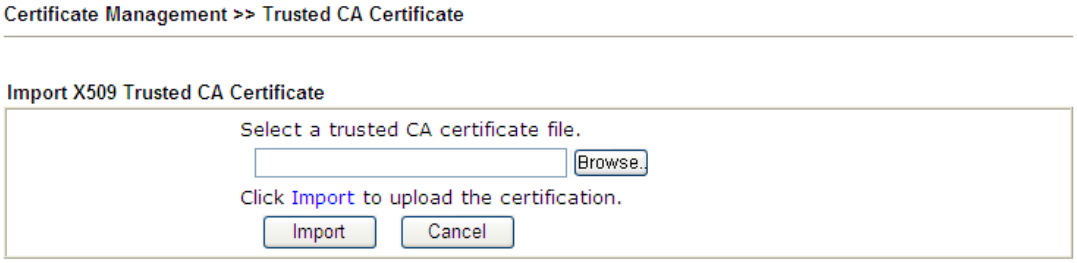
更新頁面

按下此鈕更新本頁資訊。

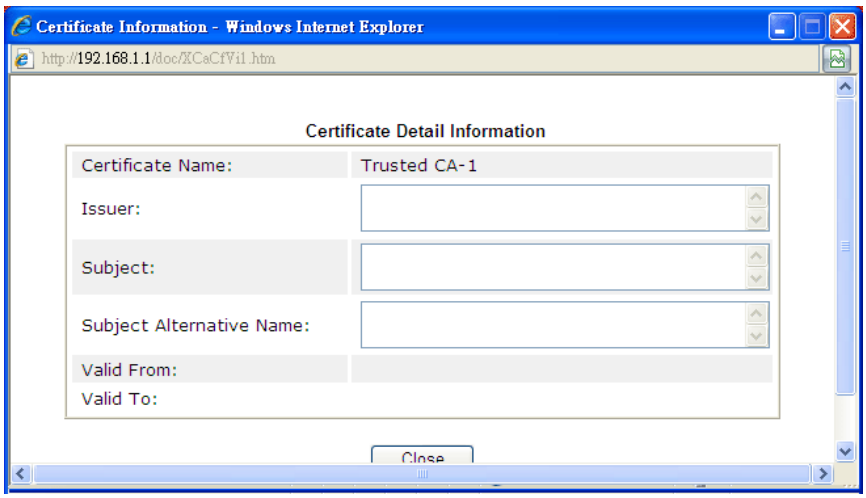
4.10.2 具公信力之 CA 憑證(Trusted CA Certificate)

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(IMPORT)**鈕開啓如下的視窗，並使用**選擇檔案(Browse…)**找到儲存的文字檔案，接著按下**匯入(Import)**鈕，您所要匯入的檔案將會列在視窗上，再按一次**匯入(Import)**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(View)**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(Delete)**按鈕，所有相關的憑證資訊即可刪除。



4.10.3 憑證備份(Certificate Backup)

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(Encrypt password)**與**確認密碼(Retype password)**二欄中輸入所需的字元。

4.11 無線區域網路設定(2.4GHz/5GHz)

本節所提供的資訊僅針對 *n/n-plus* 系列機型。

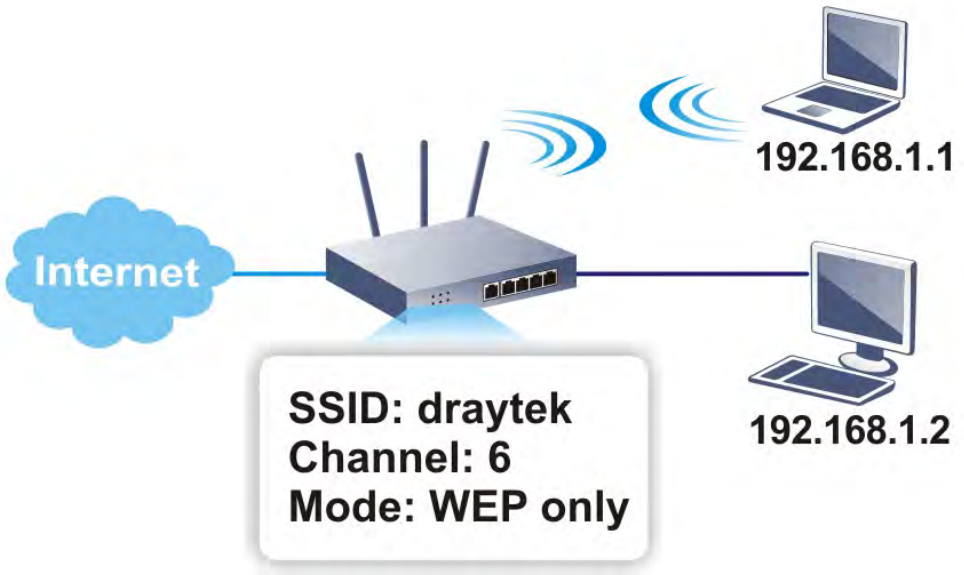
4.11.1 基本觀念

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。

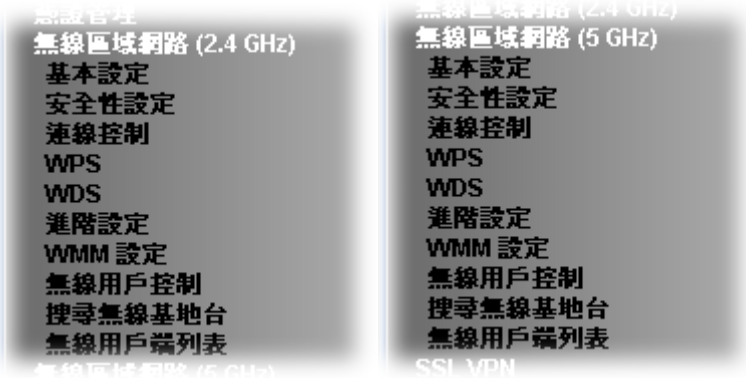
在 WPA-Personal 機制中，會應用一個事先定義的金鑰來加密傳輸中的資料，WPA 採用 Temporal Key Integrity Protocol (TKIP) 加密資料而 WPA2 則是採用 AES，WPA-Enterprise 不只結合加密也還涵括驗證功能。

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：

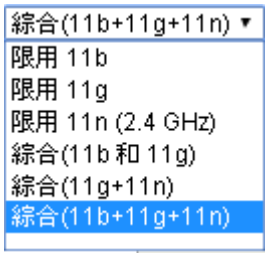
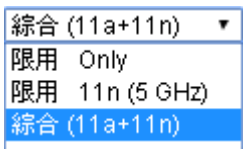


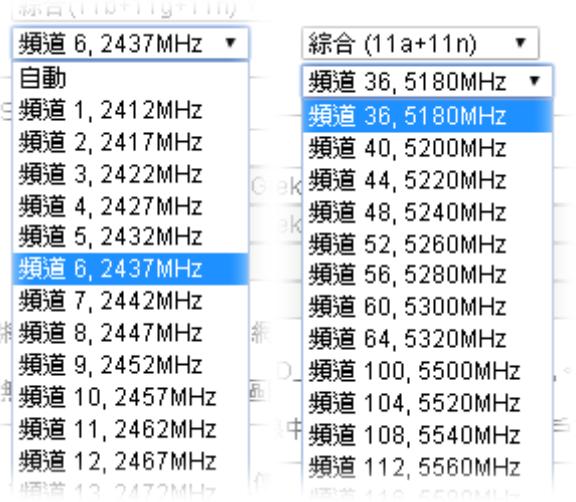
本節以 Wireless LAN (2.4GHz)下的功能當成解說範例。

4.11.2 基本設定(General Setup)

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：

可用設定說明如下：

項目	說明
啓用 **(Enable Wireless LAN)**	勾選此方塊啓動無線功能。
模式 **(Mode)**	請選擇一個適當的無線模式。   2.4G 5G
頻道 **(Channel)**	無線區域網路的通道頻率，預設頻道是 6，如果選定的頻道受到嚴重的干擾的話，您可自行切換爲其他頻道。

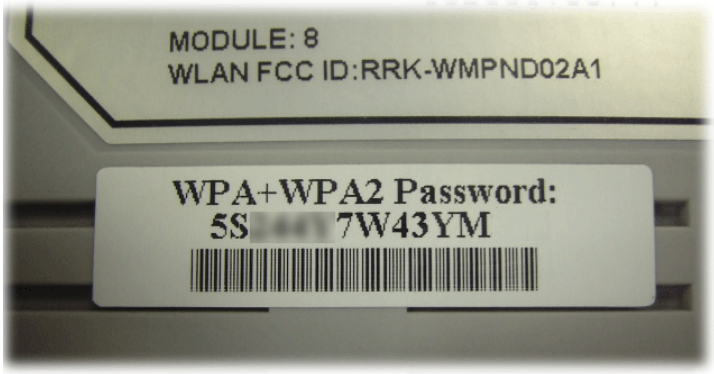
	 2.4G 5G
隱藏 SSID (Hide SSID)	勾選此方塊，防止他人得知 SSID 值，未知此路由器的 SSID 之無線用戶在搜尋網路時，看不到 Vigor 無線路由器的訊息。
SSID	預設的 SSID 值爲 **DrayTek**，建議您變更爲另一個特殊名稱。它是無線區域網路的身分辨識碼，SSID 可以是任何文字、數字或是各種特殊字元。
隔離 (Isolate)	**VPN** – 勾選此方塊讓使用相同 VPN 的無線用戶無法存取彼此的電腦資料。 **成員(Member)**– 勾選此方塊讓使用相同 SSID 的無線用戶彼此無法存取對方資料。
流量控制 (Rate Control)	可控制透過無線連線傳輸的資料傳送速率。 **上傳(Upload)** – 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(Download)**–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。
排程索引	設定無線區域網路在特定的時間間隔中運作。您可以從**應用**的**排程設定(Applications >> Schedule)**頁面上，自 15 個排程中選擇 4 個，本區預設值是空白的，表示無線功能是永遠可以運作的狀態。

完成上述設定之後，請按下**確定(OK)**儲存。

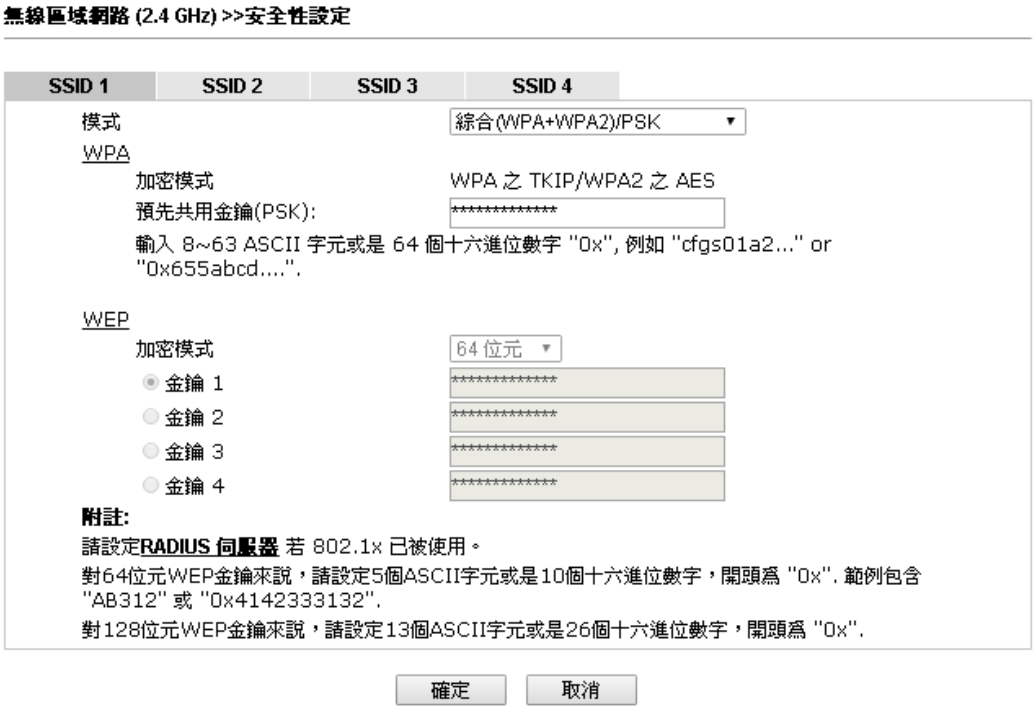
4.11.3 安全性設定(Security)

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

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

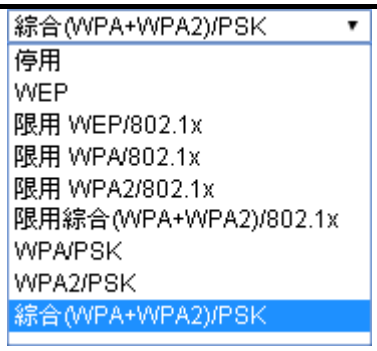
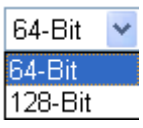


選擇**安全性設定**後，新的網頁將會出現，您可以在此頁面上調整 WEP 和 WPA 設定。



可用設定說明如下：

項目	說明
模式 (Mode)	此一設定有數種模式可供您選擇。

	 **注意:**若您選擇了 802.1x 模式，您就必須同時設定 RADIUS 伺服器的內容。 **停用(Disable) -** 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。 **WEP/802.1x Only -** 僅接受 WEP 用戶端以及得自 RADIUS 伺服器(含 802.1X 協定)動態分配之密鑰。 **WPA/802.1x Only -** 僅接受 WPA 用戶端以及得自 RADIUS 伺服器(含 802.1X 協定)動態分配之密鑰。 **WPA2/802.1x Only -** 僅接受 WPA2 用戶端以及得自 RADIUS 伺服器(含 802.1X 協定)動態分配之密鑰。 **Mixed (WPA+WPA2/802.1x only) -**.同時接受 WPA 與 WPA2 用戶端以及得自 RADIUS 伺服器(含 802.1X 協定)動態分配之密鑰。 **WPA/PSK -**接受 WPA 用戶，請在 PSK 中輸入加密金鑰。 **WPA2/PSK -**接受 WPA2 用戶，請在 PSK 中輸入加密金鑰。 **Mixed (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。

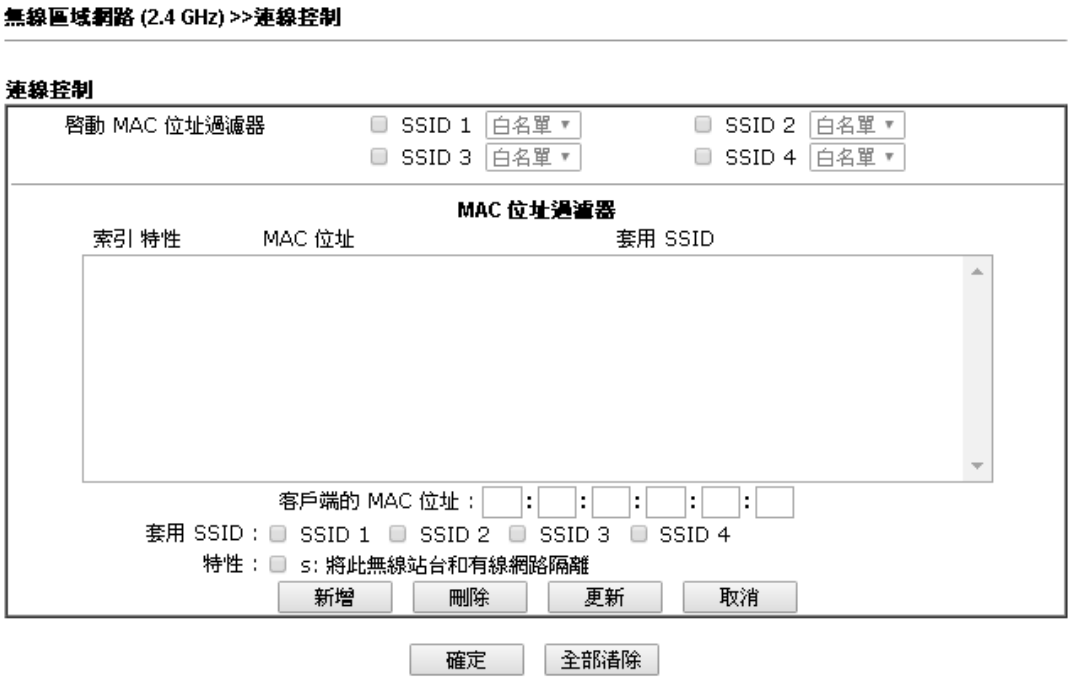
完成上述設定之後，請按下**確定(OK)**儲存。

4.11.4 連線控制(Access Control)

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

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

黑白名單的設定也可以同時包含 SSID 與 MAC 位址。



可用設定說明如下：

項目	說明
啓動 MAC 位址過濾器 (Enable Mac Address Filter)	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 (MAC Address Filter)	顯示之前編輯的全部 MAC 位元址。
客戶端的 MAC 位址 (Client's MAC Address)	請手動輸入無線用戶端的 MAC 位址。
套用 SSID (Apply SSID)	輸入用戶的 MAC 位址之後，勾選 SSID 的方框即可將其與 MAC 位址同時套入連線控制。

特性 (Attribute)	**s** -勾選此項以便隔離無線用戶端之無線連線。
新增 (Add)	新增新的 MAC 位址於清單上。
刪除 (Delete)	刪除清單中選定的 MAC 位址。
編輯 (Edit)	編輯清單中選定的 MAC 位址。
取消 (Cancel)	放棄連線控制設定。
確定 (OK)	按此鈕儲存連線控制清單。
全部清除 (Clear All)	按此鈕儲存連線控制清單。

完成上述設定之後，請按下**確定(OK)**儲存。

4.11.5 WPS

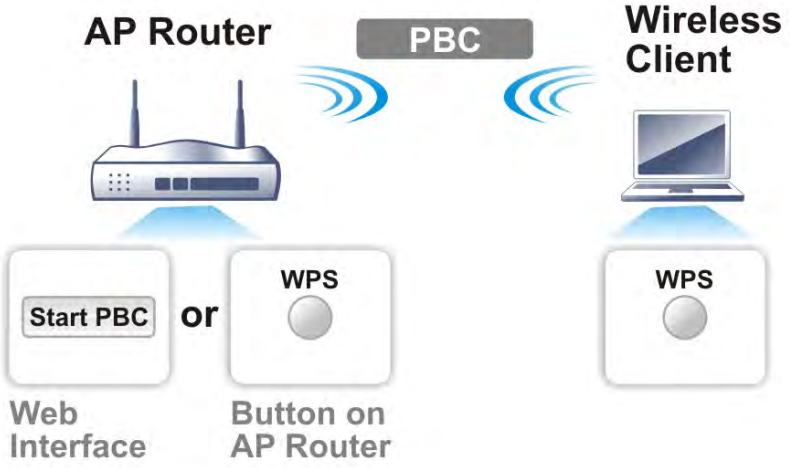
WPS (Wi-Fi Protected Setup) 提供簡易操作流程，讓無線用戶與無線基地台之間以WPA和WPA2之加密方式，成功完成網路連線。

注意: 此功能僅在無線用戶端也支援 WPS 功能時可用。

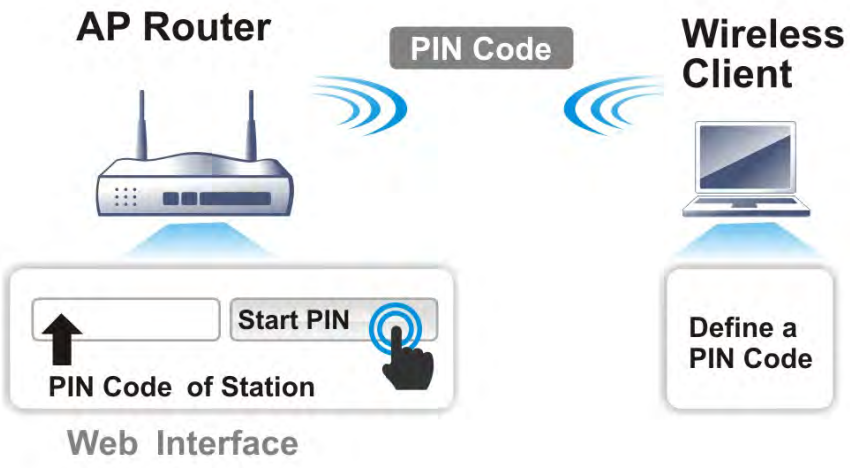
建立無線網路用戶與Vigor路由器之間的連線有個快速及簡單的方式，使用者不需要每次都必須選擇加密模式，或輸入任何長篇的資料以建立無線連線。使用者只要按下無線用戶端中的一個小小按鈕，WPS功能就會替他/她自動建立一個無線連線。

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。

- Vigor2120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(Wireless LAN>>Security)**選擇此模式，您會看到如下的訊息:

請按下**確定(OK)**鈕，然後回到**無線區域網路>>安全性設定(Wireless LAN>>Security)**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 (Wireless LAN>>WPS)**網頁畫面。

可用設定說明如下：

項目	說明
啓用 WPS (Enable WPS)	勾選此方塊啓動 WPS 設定。
WPS 狀態 (WPS Status)	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 (Authentication Mode)	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 (Configure via Push Button)	請按**啓動 PBC(Start 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 (Configure via Client PinCode)	請輸入您想要連接的無線用戶所指定的 PIN 碼，在按**啓動 PIN(Start 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)。

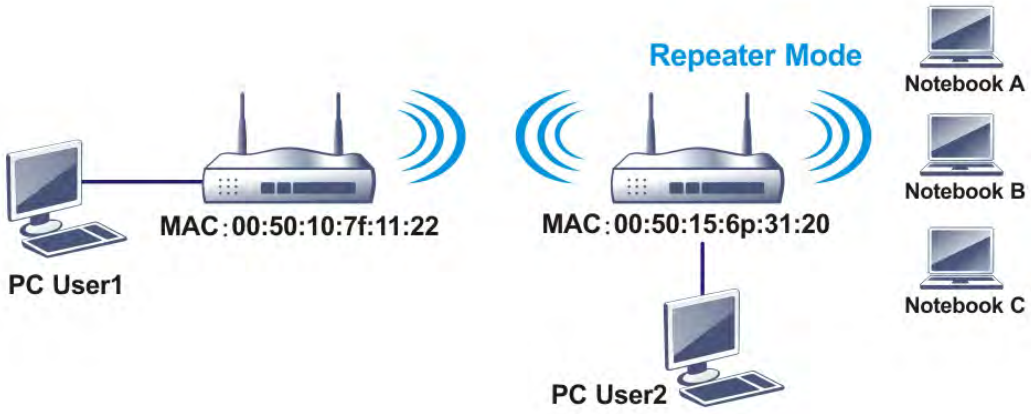
4.11.6 WDS

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

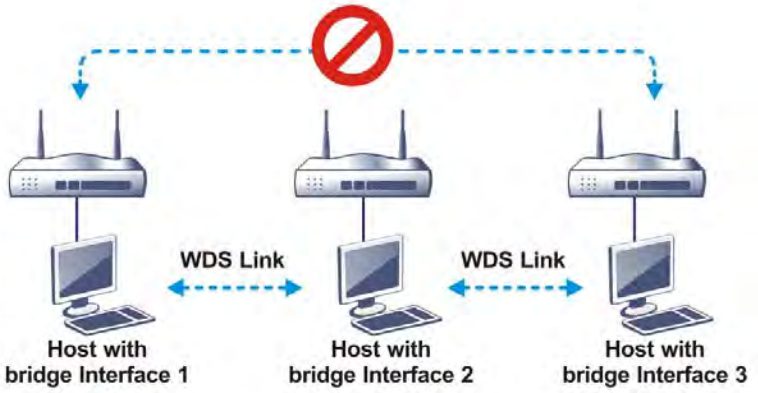
迎合以上的需要，路由器可應用二種 WDS 模式，一爲**橋接(Bridge)**一爲**中繼(Repeater)**，下圖顯示 WDS 橋接介面的功能：

WDS-中繼模式的應用則描繪如下：

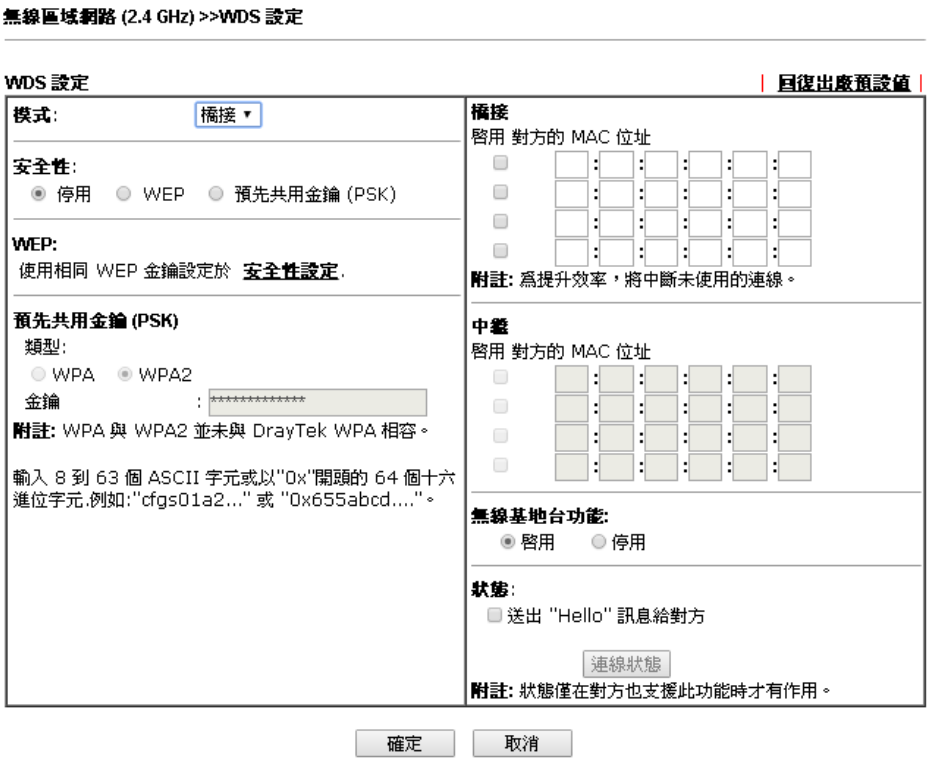


二種模式的主要不同點在於：**中繼**模式下，從一端 AP 過來的封包可以透過 WDS 連結再另一個 AP 上重複產生，WDS 連結傳送過來的封包只能轉送至本機有線或無線的主機。換言之，只有此模式能完成 WDS 到 WDS 封包轉送的工作

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(Wireless LAN)**中的 **WDS** 功能以出現如下畫面：



可用設定說明如下：

項目	說明
模式 (Mode)	選擇 WDS 設定模式，停用將無法啓用任何 WDS 設定；橋接**(Bridge)**模式乃是設計用來符合第一種實際之應用；中繼**(Repeater)**模式則是設計用來符合第二種實際之應用。 橋接 停用 橋接 中繼
安全性 (Security)	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。

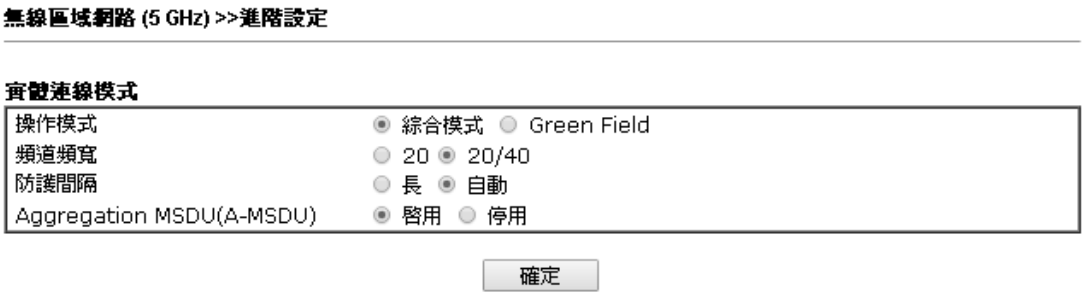
WEP	勾選此方塊使用**安全性設定**頁面中同樣的金鑰。如果您並未在**安全性設定**頁面中設定任何的金鑰，此方塊將暫時無法使用。
預設共用金鑰 (Pre-shared Key)	輸入開頭爲“0x”之 8 ~ 63 個 ASCII 字元或是 64 的 16 進位的數字。
橋接 (Bridge)	如果您選擇橋接做爲通訊模式，請在此區輸入對方的 MAC 位址，本頁可讓您一次輸入六個對方 MAC 位址。停用不使用的連結可以取得較好的執行效果，如果您想要啓動對方的 MAC 位址，記得輸入完成後勾選**啓用**方塊。
中繼 (Repeater)	如果您選擇**中繼**做爲通訊模式，請在此區輸入對方的 MAC 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(Enable)**方塊。
無線基地台功能 (Access Point Function)	按**啓用(Enable)**讓路由器提供無線基地台的服務；按**停用(Disable)**取消此功能。
狀態 (Status)	允許使用者傳送招呼訊息給對方，然而則此功能僅在對方也支援時才有效用。

完成上述設定之後，請按下**確定(OK)**儲存。

4.11.7 進階設定(Advanced Setting)

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

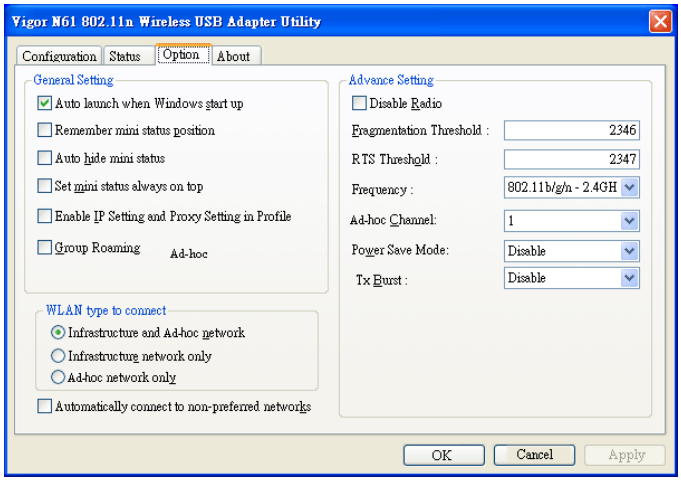
2.4G



5G

可用設定說明如下：

項目	說明
操作模式 (Operation Mode)	**綜合模式(Mixed Mode)** – 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 (Channel Bandwidth)	**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 (Guard Interval)	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(auto)**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。

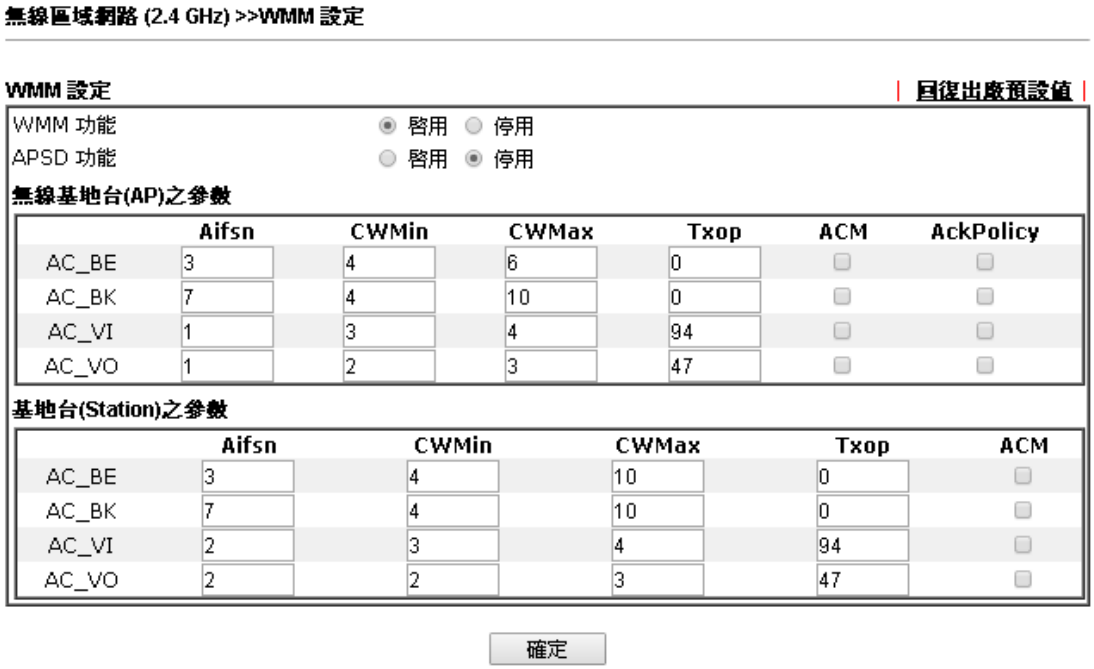
Aggregation MSDU	Aggregation MSDU 可整合不同大小的選框，用來改善某些品牌用戶的 MAC 層級成效，預設值爲**啓用(Enable)**。
長封包標頭 (Long Preamble)	此選項用來定義 802.11 封包中同步區塊的長度，最新的無線網路以 56 bit 同步區來使用短封包標頭，而不是以 128 bit 同步區來使用長封包標頭。不過，一些原始 11b 無線網路裝置只有支援長封包標頭而已，因此如果您需要和此種裝置通訊溝通的話，請勾選此方塊。
Packet-OVERDRIVE	這個功能可以強化資料傳輸的效果，約可提升 40%以上(務必勾選 **Tx Burst)**。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**). 
傳送速率(Tx Power)	設定裝置的傳輸訊號的電力百分比，數值越大，訊號密度越高。

完成上述設定之後，請按下**確定(OK)**儲存。

4.11.8 WMM 設定(WMM Configuration)

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。



可用設定說明如下：

項目	說明
WMM 功能 (WMM Capable)	在無線資料傳輸中應用 WMM 參數，請按**啓用(Enable)**鈕。
APSD 功能 (APSD Capable)	預設值爲**停用(Disable)**。
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:** Vigor2120 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。

完成上述設定之後，請按下**確定(OK)**儲存。

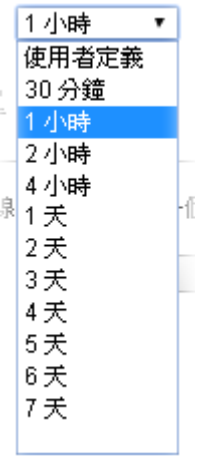
4.11.9 無線用戶控制(Station Control)

無線用戶控制(Station Control)用於指定無線用戶連接與重新連接 Vigor 路由器的時間，如果沒有啓用此功能，無線用戶可以一直連線路由器，直到路由器關機爲止。

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

附註：Vigor 路由器支援最多可達 300 個無線用戶。

可用設定說明如下：

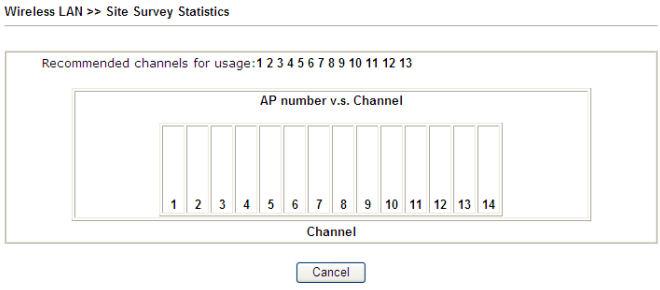
項目	說明
SSID	顯示無線用戶連接 Vigor 路由器使用的 SSID。
啓用(Enable)	勾選此框啓用此功能。
連線時間/重新連線時間 (Connection Time / Reconnection Time)	使用下拉式清單選擇連線/重新連線 Vigor 路由器的時間，如果選擇**使用者設定(User defined)**，請手動輸入連線時間。 
顯示全部無線用戶控制清單(Display All Station Control List)	顯示所有透過此 SSID 連線至 Vigor 路由器的無線用戶清單。
入口網站設定(WEB Portal Setup)	按下此連結開啓相關頁面，以修改 **LAN>>網頁入口設定(LAN>>Web Portal Setup)**設定。

4.11.10 搜尋無線基地台(AP Discovery)

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。

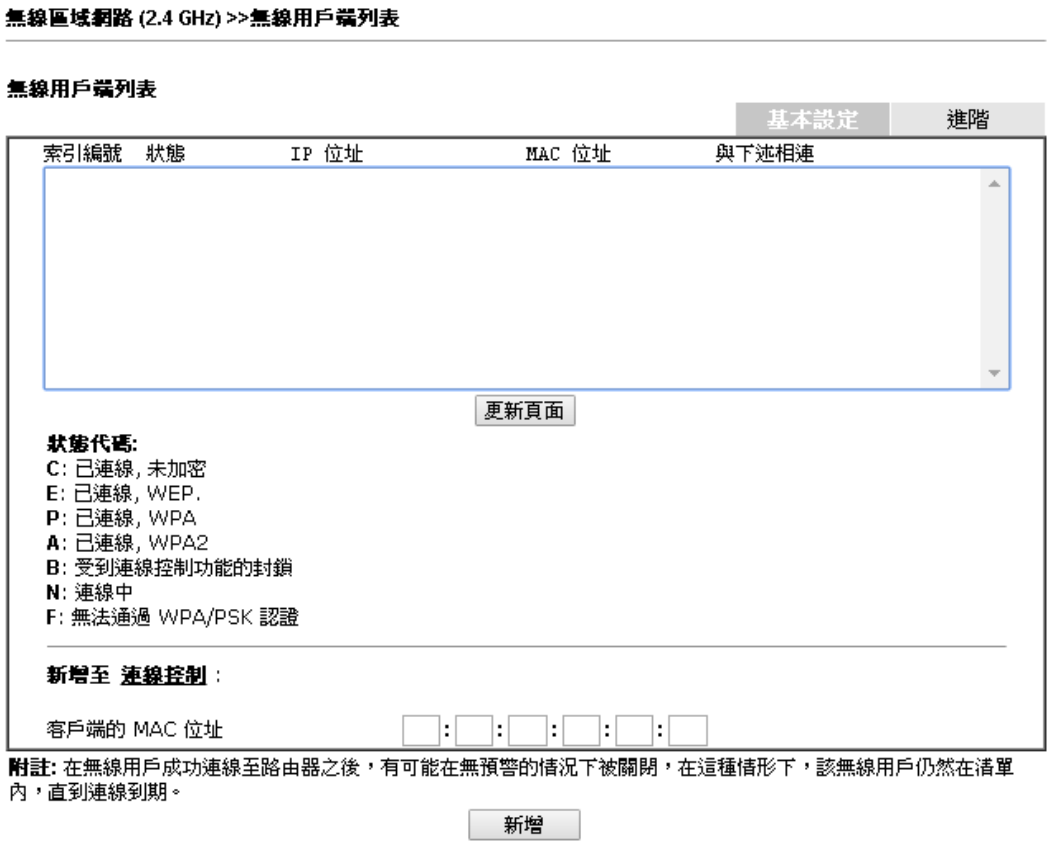
本頁可用來掃描無線區域網路中的無線基地台的存在，不過只有與路由器相同頻道的無線基地台可以被發現，請按**掃描(Scan)**按鈕尋找所有相連的無線基地台。

可用設定說明如下：

項目	說明
掃描 **(Scan)**	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 **(Statistics)**	顯示基地台所使用的頻道統計資料。 
新增 **(Add to)**	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。

4.11.11 無線用戶端列表(Station List)

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(Add to Access Control)**，這樣就可以了。



可用設定說明如下：

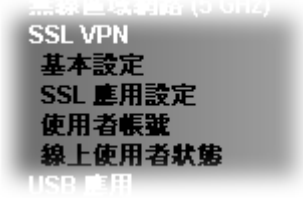
項目	說明
更新頁面 (Refresh)	按此鈕更新用戶端的 MAC 位址列表。
新增 (Add)	按此鈕新增選定之 MAC 位址至**連線控制(Access Control)**。

4.12 SSL VPN

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

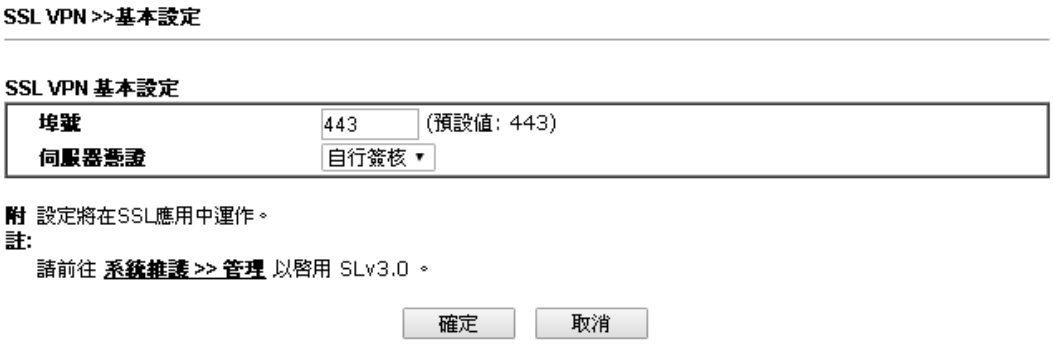
SSL VPN 提供的好處有二：

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



4.12.1 基本設定

本頁決定 SSL VPN 以及 SSL Tunnel 的基本設定內容。



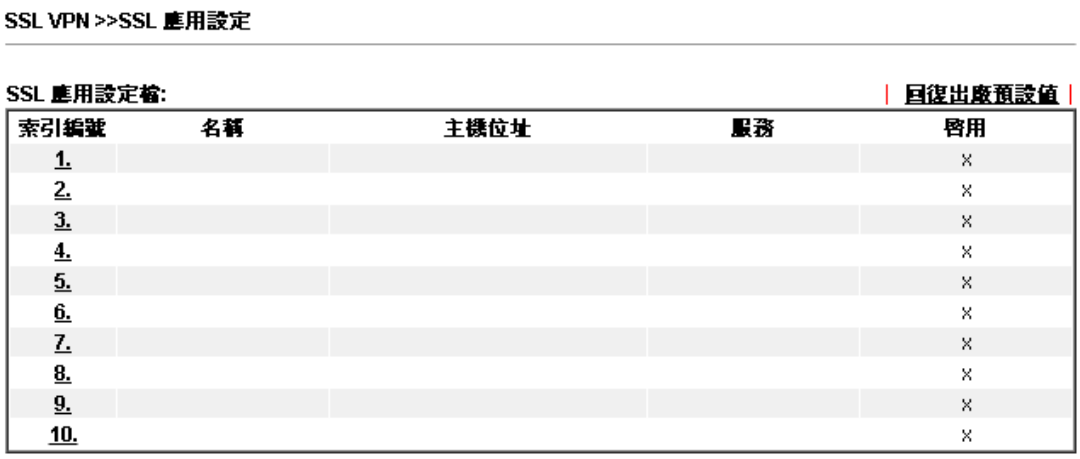
可用設定說明如下：

項目	說明
埠號 (Port)	此埠號設定乃提供與 SSL VPN 伺服器之用，不會影響**系統維護>>管理(System Maintenance>>Management)**中的 HTTPS 埠號設定。基本上，預設值是 443。
伺服器憑證 (Server Certificate)	若先前已經建立了數項憑證，可透過下拉式清單選擇任何一個使用者定義的憑證，否則請用**自行簽核(Self-signed)**讓路由器使用內建的預設憑證。預設憑證可用於 SSL VPN 伺服器以及 HTTPS 網頁代理伺服器。 但當用戶端未設定任何憑證時，預設憑證將用於 HTTPS 以及 SSL VPN 伺服器。

完成全部設定之後，請按**確定(OK)**儲存設定值。

4.12.2 SSL 應用設定(SSL Application)

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

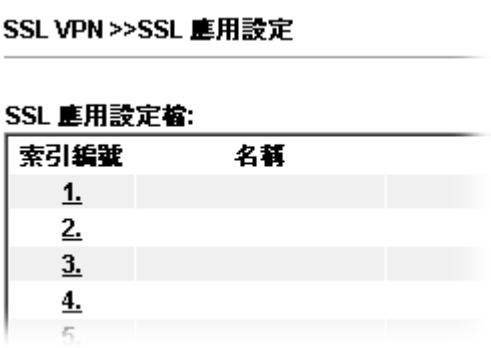


各個項目說明如下：

項目	說明
名稱 (Name)	顯示您建立的應用設定檔的名稱。
主機位址 (Host Address)	顯示 VNC/RDP 的 IP 位址。
服務 (Service)	顯示選擇的服務類型例如 VNC/RDP。
啓用 (Active)	顯示選定的設定檔目前的狀態(啓用或是不啓用)。

欲建立新的 SSL 應用設定檔：

1. 點選任一索引編號連結。



2. 下述頁面將出現：

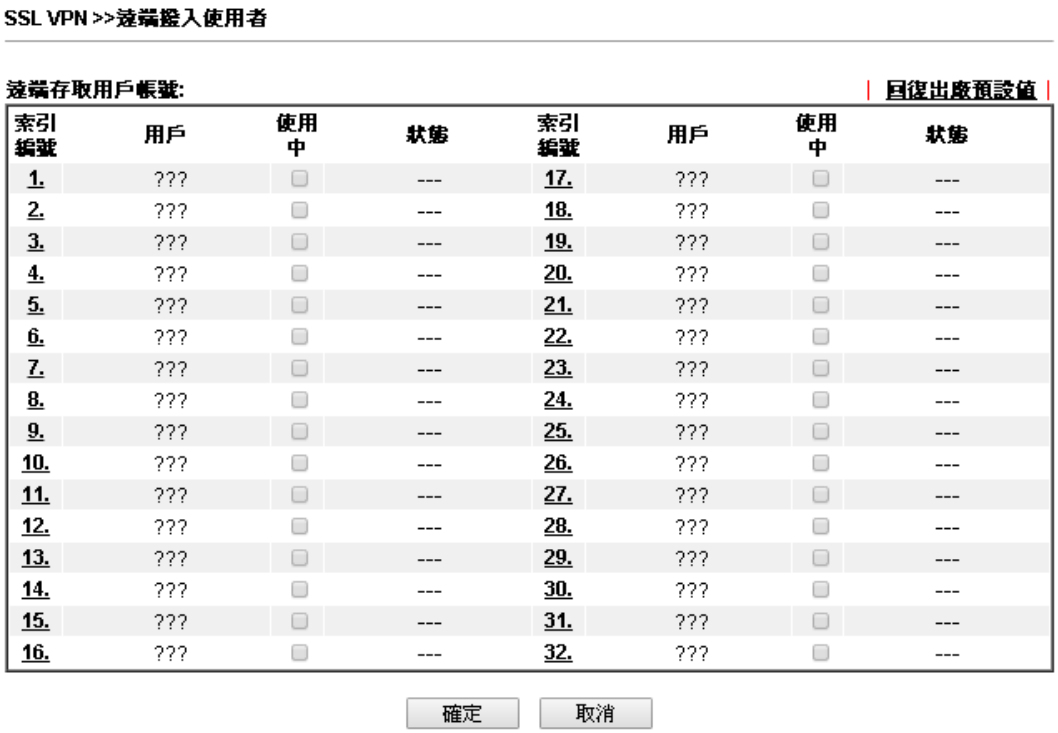
可用設定說明如下：

項目	說明
啓動應用服務 (Enable Application Server)	勾選此框啓用此設定檔。
應用名稱 (Application Name)	輸入應用的名稱。
應用 (Application)	有三種類型可以建立應用設定檔： 遠端桌面通訊協定 (RDP) ---請選擇--- 虛擬網路計算 (VNC) 遠端桌面通訊協定 (RDP) **虛擬網路計算 (VNC，Virtual Network Computing)** – 讓您透過 VNC 協定登入並控制遠端電腦。 **遠端桌面通訊協定 (RDP，Remote Desktop Protocol)** – 讓您透過 RDP 協定登入並控制遠端電腦。
IP 位址 (IP Address)	如果您選擇的是 VNC 或是 RDP，您必須在此輸入 IP 位址。
埠號 (Port)	如果您選擇的是 VNC 或是 RDP，您必須指定用於此協定的埠號，預設值爲 5900。
閒置逾時 (Idle Timeout)	如果您選擇的是 VNC，您必須指定中斷 SSL VPN 通道的時間。
比例 (Scaling)	如果您選擇的是 VNC，您必須選擇此應用的比例值 (100%, 80%, 60%)。
螢幕大小 (Screen Size)	如果您選擇的是 RDP，您必須選擇適合此應用的螢幕大小。

3. 輸入必要資訊。
4. 完成上述設定之後，按下**確定(OK)**儲存並回到上頁。

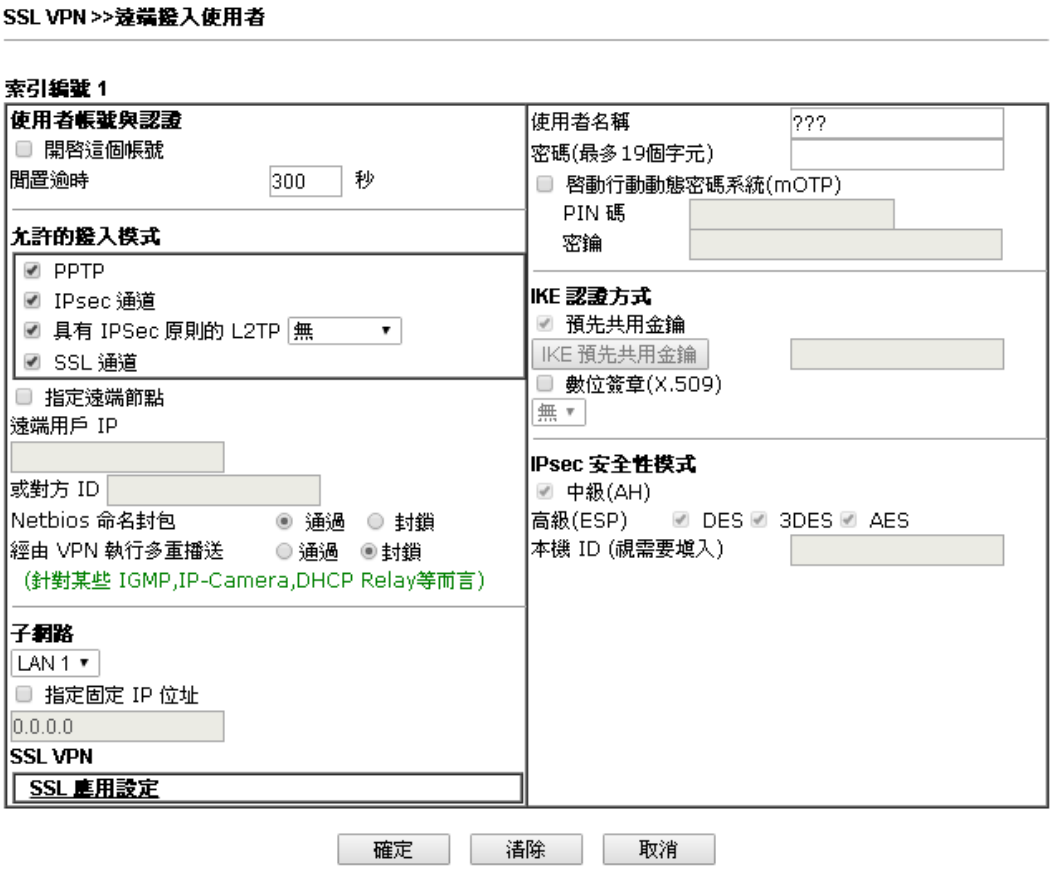
4.12.3 使用者帳號(User Account)

辦識驗證與管理都是透過使用者管理來進行，因此 SSL VPN 使用者帳號必須與遠端撥入使用者的設定頁面相同。



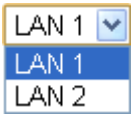
注意: 共有 32 個設定檔可以設定，但是同時進行的連線數最多只達 16 條。

按下任一索引編號編輯遠端使用者設定檔。



可用設定說明如下：

項目	說明
使用者帳號與認證 (User account and Authentication)	**開啓這個帳號(Enable this account) -**勾選此方塊以啓用此功能。 **閒置逾時(Idle Timeout) -** 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。
允許的撥入模式 (Allowed Dial-In Type)	**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(IPSec Tunnel)-**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(L2TP with IPSec Policy)-**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(None)-** 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(Nice to Have) -**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。

項目	說明
	● **必須(Must) -** 此選項可在 L2TP 連線中明確指定所要運用的 IPSec 原則。 **SSL 通道(Must)**-允許遠端撥入用戶透過網際網路進行 SSL VPN 連線。如果您勾選此框，專屬此帳號的 SSL 通道就會立即啓動。 **指定遠端節點(Specify Remote Node)**-您可以指定遠端撥入使用者或是對方 ID (應用於 IKE 主動模式中)的 IP 位址。若您不勾選此項，即表示您所選擇的連線類型，將會應用**基本設定**中所設定的驗證方式和安全防護方式。 **Netbios 命名封包(Netbios Naming Packet)** ● **通過(Pass)**– 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(Block)** – 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。 **經由 VPN 執行多重播送(Multicast via VPN)** -某些程式可透過 VPN 連線進行多重播送封包。 ● **通過(Pass)** –點選此鈕讓多重播送封包通過路由器。 ● **封鎖(Block)** – 此爲預設值。點選此鈕之後，路由器將會封鎖多重播送封包。
子網路 **(Subnet)**	選擇此 VPN 設定檔所需的子網。  **指定固定 IP 位址 (Assign Static IP Address) –** 請輸入固定 IP 位址。
SSL VPN	**設定 SSL 應用(Set SSL Application)** – 選擇一組 SSL 應用設定檔套用至目前的撥入使用者設定檔中。
使用者名稱 **(User Name)**	當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區是可應用的。請輸入名稱。
密碼 **(Password)**	當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區是可應用的。請輸入密碼。
啓動行動動態密碼系統 **(mOTP)**	勾選此框以便利用 mOTP 功能進行驗證。 **PIN 碼(PIN Code)** – 輸入驗證專用碼（例如 1234）。 **密鑰(Secret)** – 使用行動電話中由 mOTP 產生的 32 個數字密碼(例如 e759bb6f0e94c7ab4fe6）。
IKE 認證方式 **(IKE Authentication Method)**	當您指定遠端節點的 IP 位址時，本區僅適用於 **IPsec 通道**與**具有 IPSec 原則的 L2TP** 類型，唯一例外的是當您選擇 **IPsec 通道**時，不論有無指定 IP 位址，您還可以設定數位簽章(X.509)。 **預先共用金鑰(Pre-Shared Key)**- 勾選此方塊啓用此功能並

項目	說明
	輸入 1-63 文字做爲預先共同金鑰。 **數位簽章 (X.509) (Digital Signature (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(VPN and Remote Access >>IPSec Peer Identity)**中設定)。
IPSec 安全性模式 (IPSec Security Method)	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(Local 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。

完成全部設定之後，請按**確定(OK)**儲存設定值。

4.12.4 線上使用者狀態(Online User Status)

如果您已經完成 SSL 網頁伺服器的設定，使用者即可登入 DrayTek SSL VPN 入口網站查看相關設定。

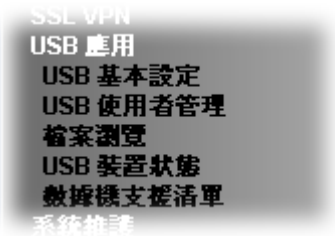
接著，使用者可以開啓 **SSL VPN>> 線上使用者狀態(SSL VPN>> Online Status t)**檢視 SSL VPN 登入狀態。

可用設定說明如下：

項目	說明
目前使用者 (Active User)	顯示目前運用 SSL VPN 伺服器的使用者。
主機 IP (Host IP)	顯示主機的 IP 位址。
閒置逾時 (Time out)	顯示強迫登出的剩餘時間。
動作 (Action)	您可按下 Drop 按鈕中斷利用路由器 SSL 入口網站登入的特定使用者。

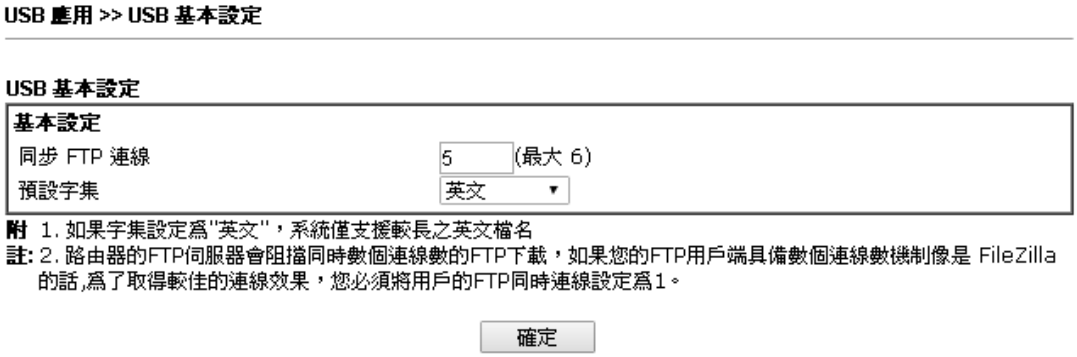
4.13 USB 應用(USB Application)

連接至路由器的 USB 存取磁碟可以被視爲伺服器的一種。透過 Vigor 路由器，區域網路端的用戶可以透過不同的應用程式登入、寫入並讀取儲存在 USB 儲存碟內的資料。在完成 USB 應用設定之後，您可以在用戶端軟體上輸入路由器的 IP 位址，以及在 **USB 應用>>USB 使用者管理(USB Application>>USB User Management)**頁面所建立的帳號與密碼，然後，用戶端就可以使用 FTP(USB 儲存碟)或是分享檔案服務。

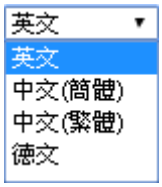


4.13.1 USB 基本設定(USB General Settings)

本頁決定同步 FTP 連線的數目以及預設字集伺服器，目前，Vigor 路由器可支援格式爲 FAT16 與 FAT32 的 USB 儲存碟，因此在連接 USB 儲存碟之前，請務必確認記憶格式是 FAT16 還是 FAT32。建議您使用 FAT32 來檢視檔案名稱(FAT16 不支援長檔名) 。



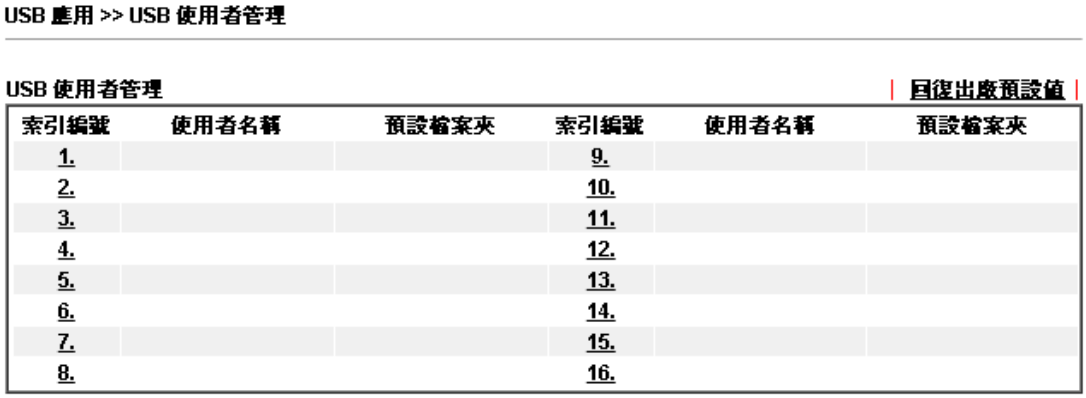
可用設定說明如下：

項目	說明
基本設定 (General Settings)	**同步 FTP 連線(Simultaneous FTP Connections) -** 此區用來指定 FTP 連線數總量，路由器允許一次連接 USB 儲存碟數量，最多可達 6 個 FTP 連線數。 **預設字集(Default Charset) -** 目前，Vigor 路由器支援四種語文字集，預設字集爲英文。 

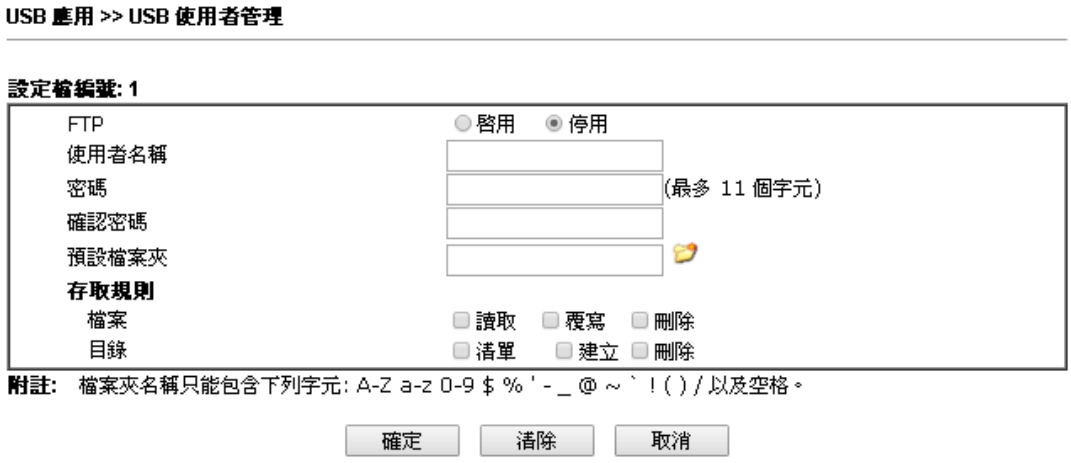
完成全部設定之後，請按**確定(OK)**儲存設定值。

4.13.2 USB 使用者管理(USB User Management)

本頁讓您針對 FTP/Samba 使用者設定數個設定檔，任何想要登入 USB 儲存碟的使用者，必須鍵入與本頁設定相同的使用者名稱與密碼。在新增或是修正本頁設定之前，請先插入 USB 儲存碟，否則系統會出現錯誤訊息。

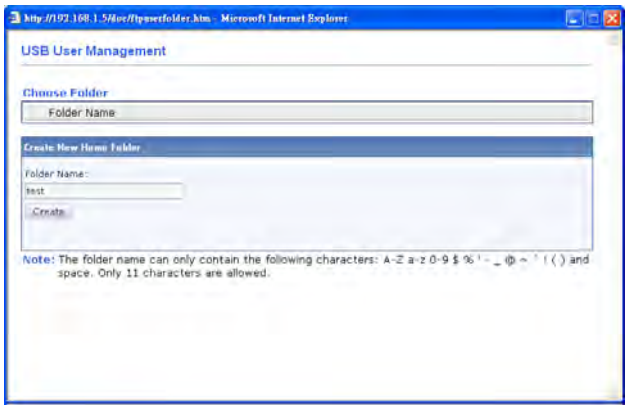


按任一索引號碼連結登入設定頁面。



可用設定說明如下：

項目	說明
FTP	**啓用(Enable)** – 按此鈕啓動此 FTP 服務設定檔，之後，使用者可使用本頁指定的名稱來登入 FTP 伺服器。 **停用(Disable)** – 按下此鈕停用此設定檔。
使用者名稱 (Username)	輸入 FTP/Samba 使用者的使用者名稱以登入 FTP 伺服器(USB 儲存碟)，注意，使用者不可以匿名方式登入 USB 儲存碟，之後您可以打開 FTP 用戶軟體再輸入此處指定的使用者名稱，即可登入 USB 儲存碟。 **注意:** 此處的使用者名稱不可輸入“Admin” ，因爲該名稱是用來登入路由器的使用者介面，同時，該名稱也供 FTP 韌體更新時使用。 **注意:** 路由器不支援 FTP Passive 模式。請在 FTP 用戶端停用此模式。
密碼 (Password)	輸入 FTP/Samba 使用者的密碼以登入 FTP 伺服器(USB 儲存碟)，之後您可以打開 FTP 用戶軟體再輸入此處指定

	的密碼，即可登入 USB 儲存碟。
確認密碼 **(Confirm Password)**	再次輸入密碼確認。
預設檔案夾 **(Home Folder)**	此功能決定用戶登入的檔案夾。 使用者可以在本區輸入目錄名稱，接著按下**確定(OK)**，路由器將會在 USB 儲存碟中建立特定/新的檔案夾，此外，如果使用者輸入“/”，就能進入 USB 儲存碟中所有的檔案夾觀看檔案。 **注意:** 當 USB 儲存碟的防寫狀態開啓時，您就無法在此輸入新檔案夾名稱，在此情況下只有“/”可以運用。 您可以點  以開啓下述對話盒新增檔案夾作爲預設檔案夾。 
存取規則 **(Access Rule)**	此功能決定設定檔的權限，任何使用此設定檔以便登入 USB 儲存碟的使用者必須遵循此處設定的規則。 **檔案(File)** – 勾選允許開放的項目(讀取、覆寫、刪除)。 **目錄(Directory)** – 勾選允許開放的項目(清單、建立、刪除)。

在您按下**確定(OK)**之後，您必須在路由器的 USB 介面插入 USB 儲存碟，否則您無法儲存設定。

4.13.3 檔案瀏覽(File Explorer)

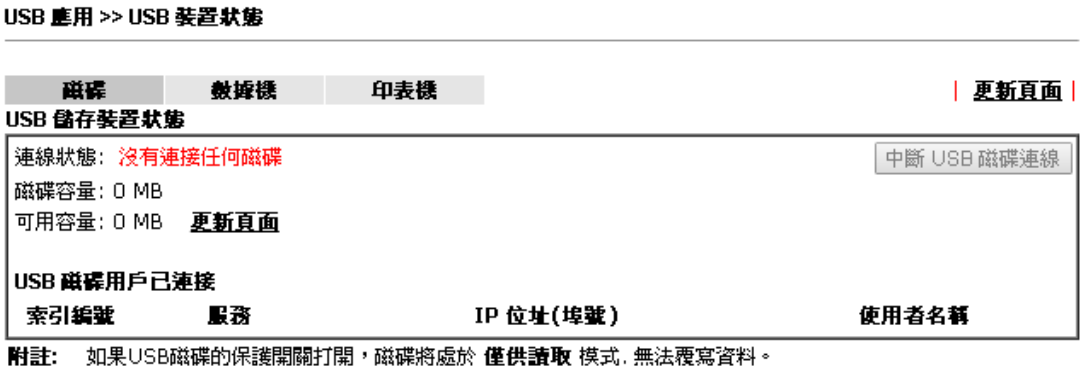
檔案瀏覽提供一個很簡易的方式讓使用者檢視及管理 USB 儲存碟(連接至 Vigor 路由器)的內容。

可用設定說明如下：

項目	說明
更新(Refresh)	按此圖示更新檔案清單。
上層(Back)	按此圖示回到上一層目錄。
建立(Create)	按此圖示新增檔案夾。
目前路徑 (Current Path)	顯示目前檔案夾的位址。
上傳 (Upload)	按此鈕上傳選定檔案至 USB 儲存碟，在碟內要上傳的檔案可以給其他 FTP 使用者分享。

4.13.4 USB 磁碟狀態(USB Device Status)

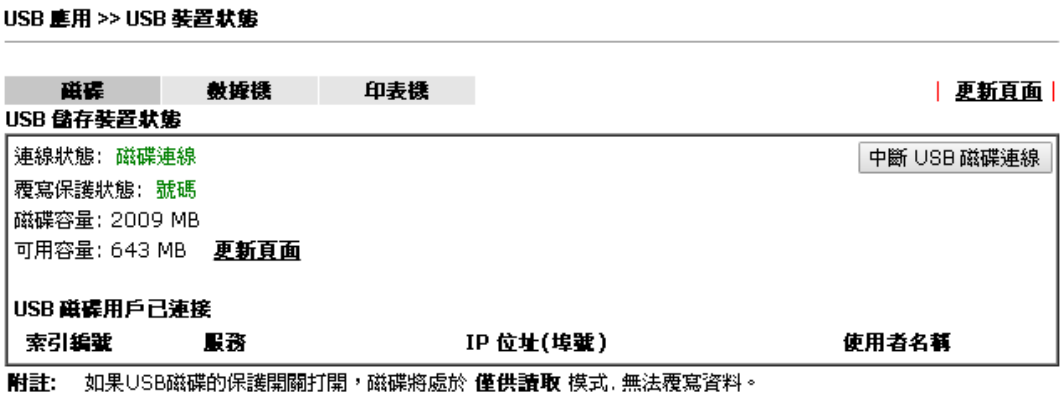
本頁用來監督透過 Vigor 路由器來存取 FTP 或是 Samba 伺服器的使用者狀態，如果您想要從路由器移除 USB 儲存碟，請先按下**中斷 USB 磁碟連線(Disconnect USB Disk)**，然後移除儲存碟。



可用設定說明如下：

項目	說明
連線狀態 (Connection Status)	如果路由器沒有連接任何 USB 儲存碟，此處會顯示”**沒有連接任何磁碟**”(“**No Disk Connected**”)。
磁碟容量 (Disk Capacity)	顯示 USB 儲存碟的總容量。
可用容量 (Free Capacity)	顯示 USB 儲存碟的目前剩餘的容量。按下**更新頁面 (Refresh)**可取得最新的容量資訊。
索引編號 (Index)	顯示使用 USB 儲存碟服務的用戶編號。
IP 位址 (IP Address)	顯示使用 USB 儲存碟服務的用戶的 IP 位址。
使用者名稱 (Username)	顯示使用 USB 儲存碟服務的用戶登入時使用的名稱。

當您將 USB 儲存碟插入 Vigor 路由器時，系統將會在數秒鐘內尋找此裝置。



4.13.5 數據機支援清單(Modem Support List)

本頁提供 Vigor 路由器支援的 USB 數據機的品牌與型號等相關資訊。

USB 應用 >> 數據機支援清單

下述相容性測試，列出在特殊環境或是國家中， **Vigor 路由器皆支援的3.5G/LTE數據機。** 如果您擁有的 LTE 數據機在清單上，但無法正常運作，請逕寄信至 support@draytek.com 或是與經銷商聯絡。

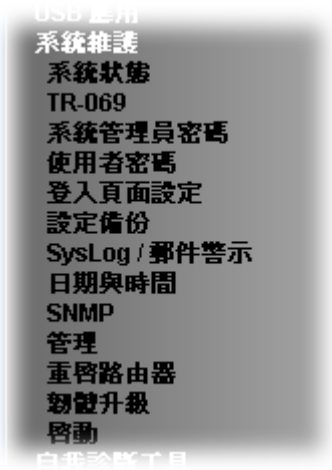
PPP 模式 | DHCP模式

品牌	機型	LTE	狀態
Aiko	Aiko 83D		Y
Alcatel	Alcatel L100V	✓	Y
Alcatel	Alcatel W100	✓	Y
BandRich	Bandluxe C170		Y
BandRich	Bandluxe C270		Y
BandRich	Bandluxe C321		Y
BandRich	Bandluxe C330		Y
BandRich	Bandluxe C502		Y
D-Link	D_LINK DWM221 B1	✓	Y
Huawei	Huawei E169u		Y
Huawei	Huawei E220		Y
Huawei	Huawei E303D		Y
Huawei	Huawei E3131		Y
Huawei	Huawei E3372	✓	Y
Huawei	Huawei E392	✓	Y
Huawei	Huawei E398	✓	Y

4.14 系統維護(System Maintenance)

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。



4.14.1 系統狀態(System Status)

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

系統狀態

型號名稱 : **Vigor2120n+**
韌體版本 : **3.7.8**
建立日期/時間 : **May 20 2015 13:31:00**

區域網路

	MAC 位址	IP 位址	子網路遮罩	DHCP 伺服器	DNS
區域網路 1	00-1D-AA-9E-4F-F4	192.168.1.1	255.255.255.0	是	8.8.8.8
LAN2	00-1D-AA-9E-4F-F4	192.168.2.1	255.255.255.0	是	8.8.8.8
IP 路由子網	00-1D-AA-9E-4F-F4	192.168.0.1	255.255.255.0	是	8.8.8.8

無線網路

MAC 位址	頻率網域	韌體版本	SSID
00-1D-AA-9E-4F-F4	歐洲	2.7.1.5	DrayTek

無線網路(5GHz)

MAC 位址	頻率網域	韌體版本	SSID
00-1D-AA-9E-4F-F6	歐洲	2.7.1.5	DrayTek_5G

廣域網路

	連線狀態	MAC 位址	連線	IP 位址	預設閘道
WAN1	斷線	00-1D-AA-9E-4F-F5	PPPoE	---	---
WAN2	斷線	00-1D-AA-9E-4F-F6	---	---	---

IPv6

	位址	範圍	網際網路連線模式
LAN	FE80::21D:AAFF:FE9E:4FF4/64	Link	---

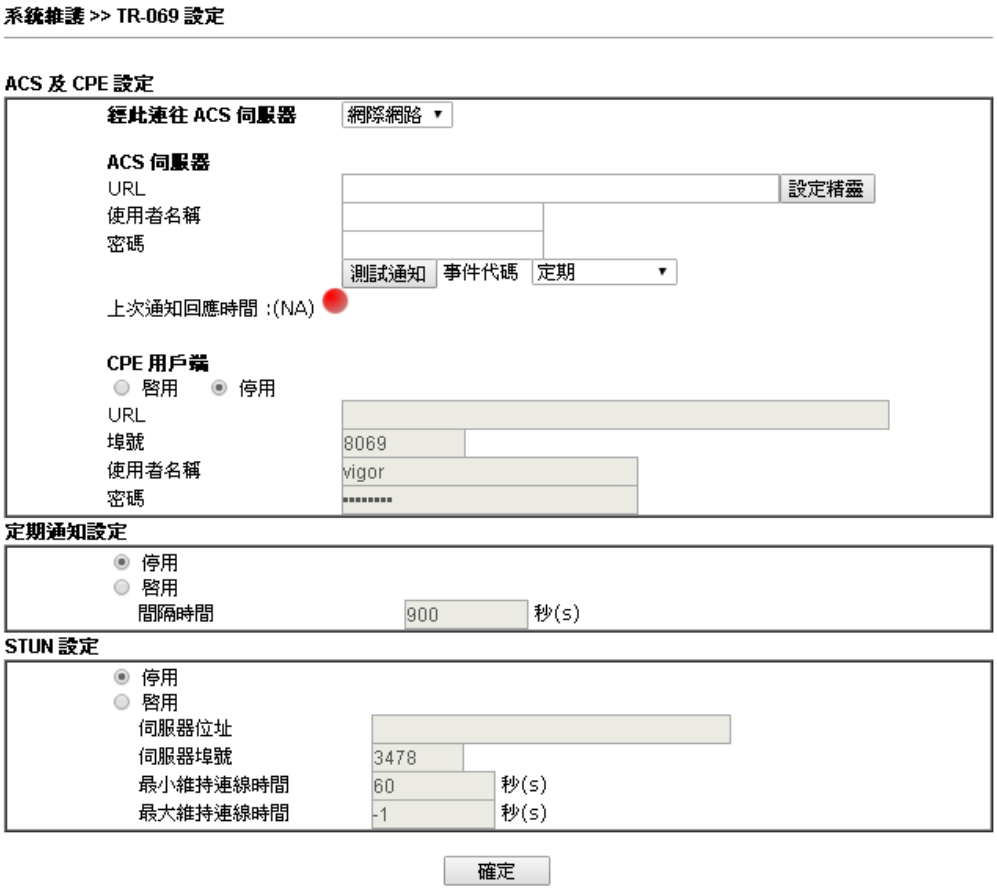
使用者模式 爲 **關閉** .

各個項目說明如下：

項目	說明
型號名稱 (Model Name)	顯示路由器的型號名稱。
韌體版本 (Firmware Version)	顯示路由器的韌體版本。
建立日期與時間 (Build Date/Time)	顯示目前韌體建立的日期與時間。
區域網路 (LAN)	**MAC 位址(MAC Address)**-顯示區域網路介面的 MAC 位址。 **IP 位址(IP Address)**-顯示區域網路介面的 IP 位址。 **子網路遮罩(Subnet Mask)**-顯示區域網路介面的子網路遮罩位址。 **DHCP 伺服器(DHCP Server)**-顯示區域網路介面的 DHCP 伺服器目前的狀態。 **DNS**-顯示主要 DNS 的 IP 位址。
無線網路 (WAN)	**MAC 位址(MAC Address)**-顯示無線區域網路的 MAC 位址。 **頻率網域(Frequency Domain)** -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(Firmware Versio)** -表示配備 WLAN miniPCi 卡的詳細資訊，同時可以提供該卡相關的特徵訊息。 **SSID**-顯示路由器的 SSID。
WAN	**連線狀態(Link Status)**-顯示目前實體連線的狀態。 **MAC 位址(MAC Address)**-顯示 WAN 介面的 MAC 位址。 **連線(Connection)**-顯示目前連線的類型。 **IP 位址(IP Address)**-顯示 WAN 介面的 IP 位址。 **預設閘道(Default Gateway)**-顯示預設閘道指定的 IP 位址。
IPv6	**位址(Address) -** .顯示區域網路的 IPv6 位址。 **範圍(Scope) -** 顯示 IPv6 位址範圍，例如 IPv6 Link Local 只能用於直接 IPv6 連線，不可用於 IPv6 網際網路。 **網際網路連線模式(Internet Access Mode) –** 顯示登入網際網路選擇的連線模式。

4.14.2 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。



可用設定說明如下：

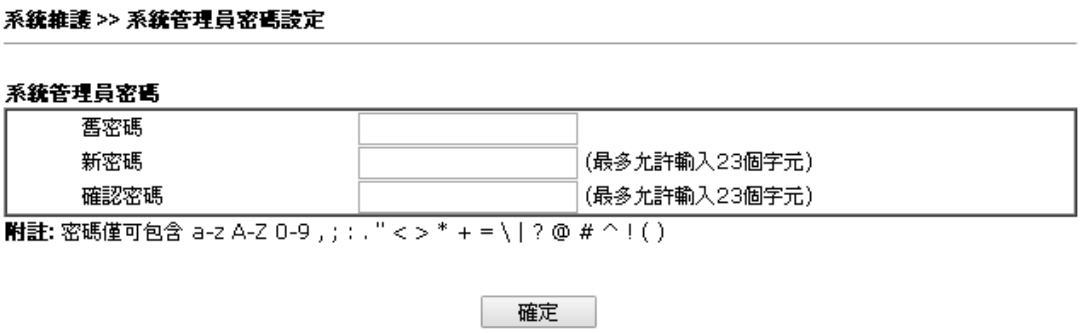
項目	說明
經此連往 ACS 伺服器 (ACS Server On)	選擇路由器連往 ACS 伺服器的介面。
ACS 伺服器 (ACS Server)	**URL/使用者名稱/密碼(URL/Username/Password) –** 此資料必須依照您想要連結的 ACS 內容來輸入，請參考 ACS 使用者取得詳細的資訊。 **測試通知 (Test With Inform) –** 按此傳送訊息，訊息以選定的事件代碼爲發送的基準以測試該 CPE 能與 VigorACS SI 伺服器溝通無礙。 **事件代碼(Event Code) –** 使用下拉式清單指定執行測試的條件爲何。 **上次通知回應時間(Last Inform Response Time) –** 顯示 VigorACS 伺服器在接收到來自 CPE 的通知訊息並給予回覆的時間。

CPE 用戶端 **(CPE Client)**	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(Enable/Disable)** – 有時候，系統可能會產生埠號衝突，爲解決這個問題，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 **(Periodic Inform Settings)**	預設值爲**啓用(Enable)**，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(Disable)**關閉通知機制。
STUN 設定 **(STUN Settings)**	預設值是**停用(Disable)**，如果您選擇了**啓用(Enable)**，請輸入下述相關資料： **伺服器 IP(Server IP) –** 輸入 STUN 伺服器的 IP 位址。 **伺服器埠號(Server Port) –** 輸入 STUN 伺服器的埠號。 **最小維持連線時間(Minimum Keep Alive Period) –** 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。 **最大維持連線時間(Maximum Keep Alive Period) –** 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。

完成設定之後，按下**確定(OK)**按鈕儲存相關設定。

4.14.3 系統管理員密碼(Administrator Password)

本頁允許您設定新的密碼。



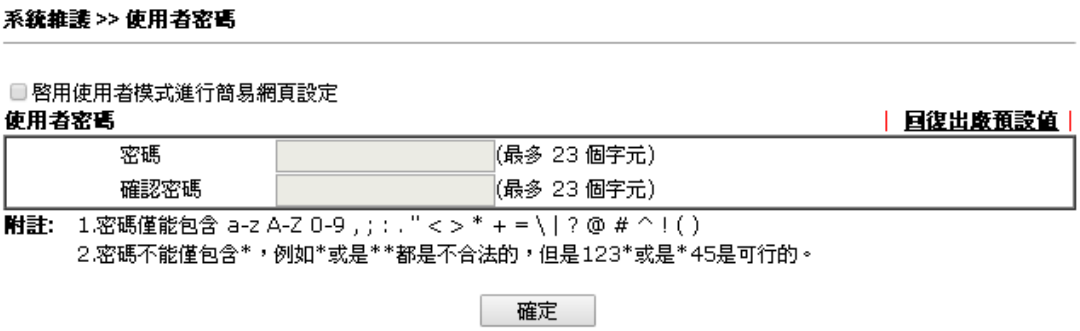
可用設定說明如下：

項目	說明
舊密碼 (Old Password)	請輸入舊密碼。
新密碼 (New Password)	請在本區輸入新密碼。
確認密碼 (Confirm Password)	再次輸入新密碼以確認。

當您按下**確定(OK)**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。

4.14.4 使用者密碼(User Password)

本頁允許您設定新的密碼。



可用設定說明如下：

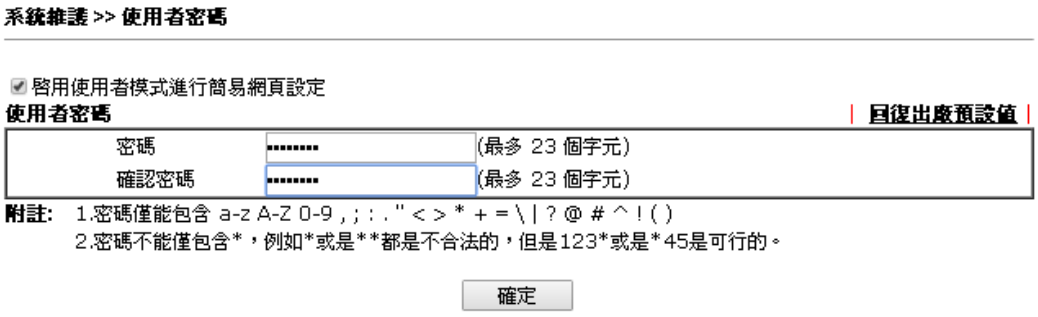
項目	說明
啓用使用者模式進行簡易網頁設定 **(Enable User Mode for simple web configuration)**	勾選此框之後，您可以透過此處輸入的密碼登入網頁使用者介面進行簡易設定。 簡易網頁使用者介面設定與透過管理者密碼登入的完整使用者介面有些不同。
密碼 **(Password)**	請在本區輸入新密碼。
確認密碼 **(Confirm Password)**	再次輸入新密碼以確認。

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

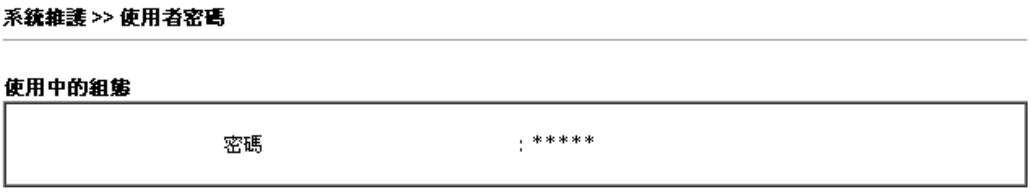
以下爲使用者範例：

1. 開啓**系統維護>>使用者密碼(System Maintenance>>User Password)**。

2. 勾選啓用使用者模式進行簡易網頁設定**(Enable User Mode for simple web configuration)**以便啓用使用者模式操作。在**密碼**與**確認密碼**欄位中輸入新的密碼，然後按下**確定(OK)**。



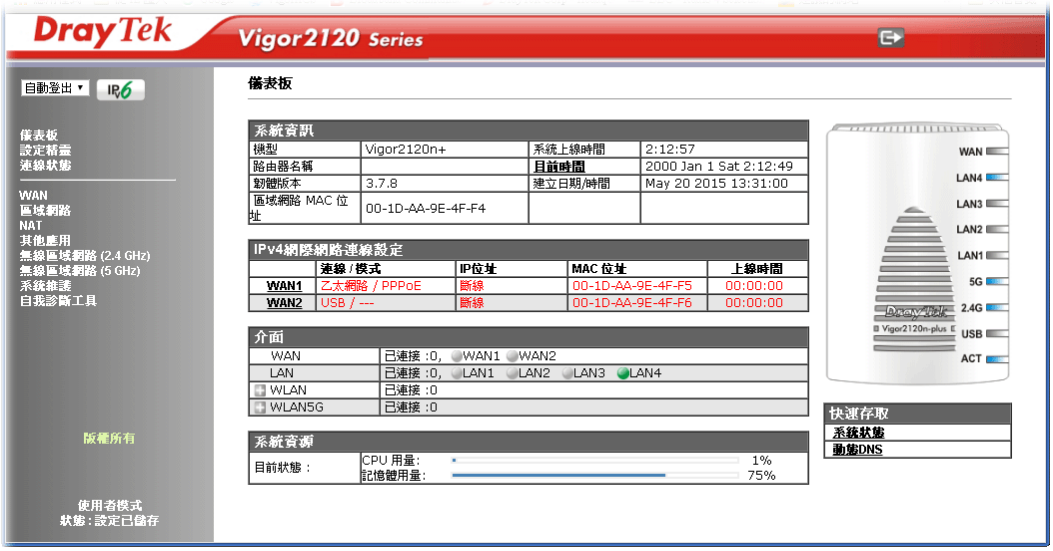
3. 下述畫面顯示出來後，按下**確定(OK)**。



4. 按**登出(Logout)**按鈕離開 Vigor 路由器網頁使用者介面。

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

6. 使用者模式的主要畫面顯示如下：



使用者模式中的設定少於管理者模式，只包含基本設定。

注意：使用者模式中的設定方式如同管理者模式。

4.14.5 登入頁面設定(Login Page Greeting)

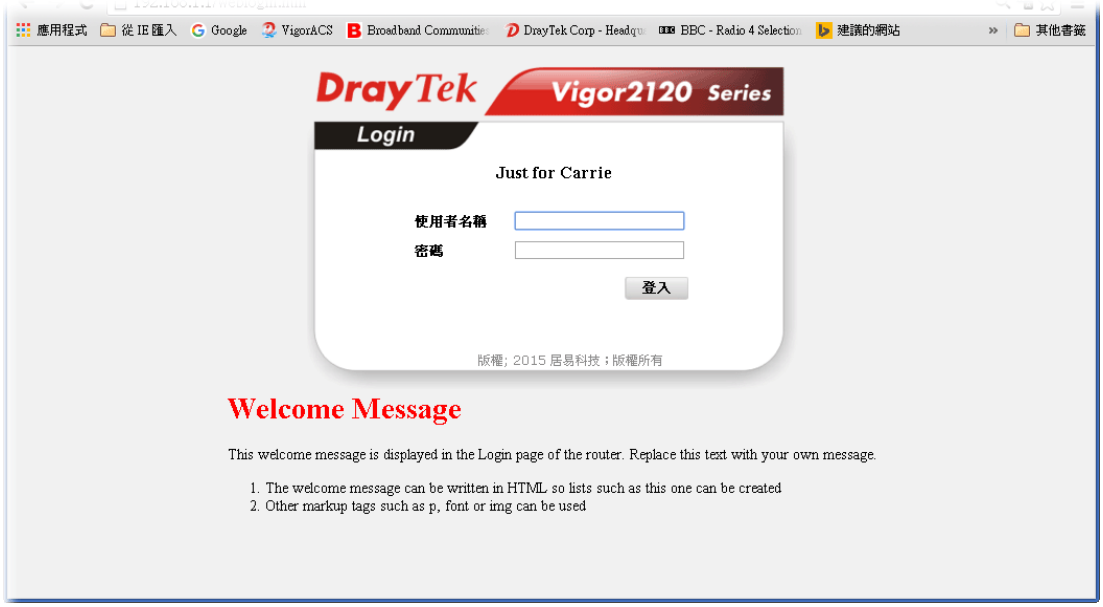
當您想要登入路由器的網頁使用者介面，系統將詢問您提供使用者名稱與密碼，登入視窗網頁的背景是空白且沒有標題在其上，如有需求本頁可讓您在登入視窗中指定登入 URL 以及標題。

Available settings are explained as follows:

項目	說明
啓用(Enable)	勾選此框啓用登入頁面客製化功能。
登入頁面標題	輸入簡短說明(例如 Welcome to DrayTek)使其顯示在登

(Login Page Title)	入對話盒的標題上。
歡迎訊息與佈告欄 **(Welcome Message and Bulletin)**	輸入文字或文句，這些文字將會出現在佈告訊息欄中，此外，也可以顯示登入對話盒的下方。 注意您不可在此輸入 URL 重導向連結。
預覽 **(Preview)**	按下此連結顯示以本頁設定爲基準的登入視窗的預覽畫面。
回復出廠預設值 **(Set to Factory Default)**	按下此連結回到出廠預設值。

下圖顯示客製化登入頁面範例：



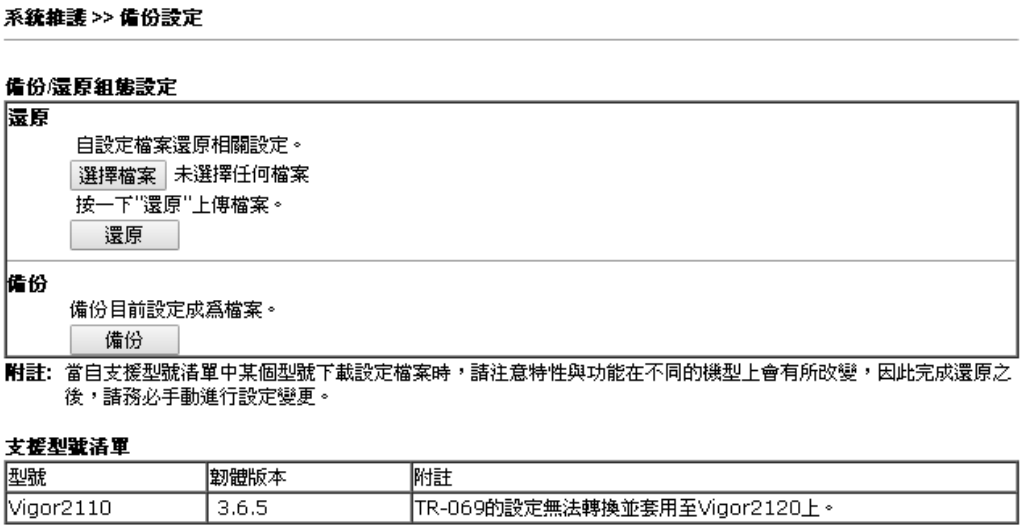
4.14.6 設定備份(Configuration Backup)

這個功能可以將 Vigor2120 內的網頁設定儲存檔案套用到 Vigor2120，節省使用者重新設定的時間。

設定備份

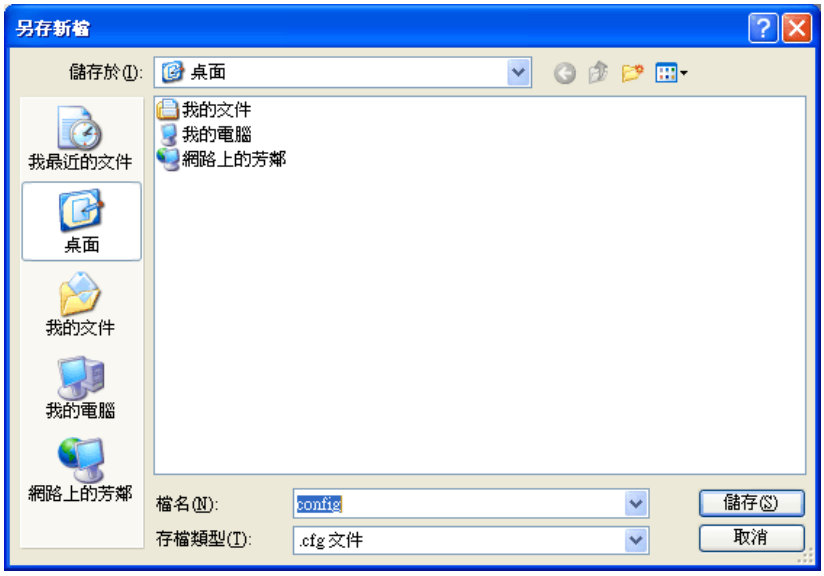
請依照下列步驟備份您的路由器設定。

1. 在**系統維護**群組中按**設定備份(System Maintenance >> Configuration Backup)**，您將可看見如下視窗。



2. 按**備份(Backup)**按鈕進入下一個對話盒，按**儲存(Save)**按鈕開啓另一個視窗以儲存設定。

3. 在**另存新檔(Save As)**對話盒中，預設檔名爲 **config.cfg**，您也可以在此輸入不同的檔名。



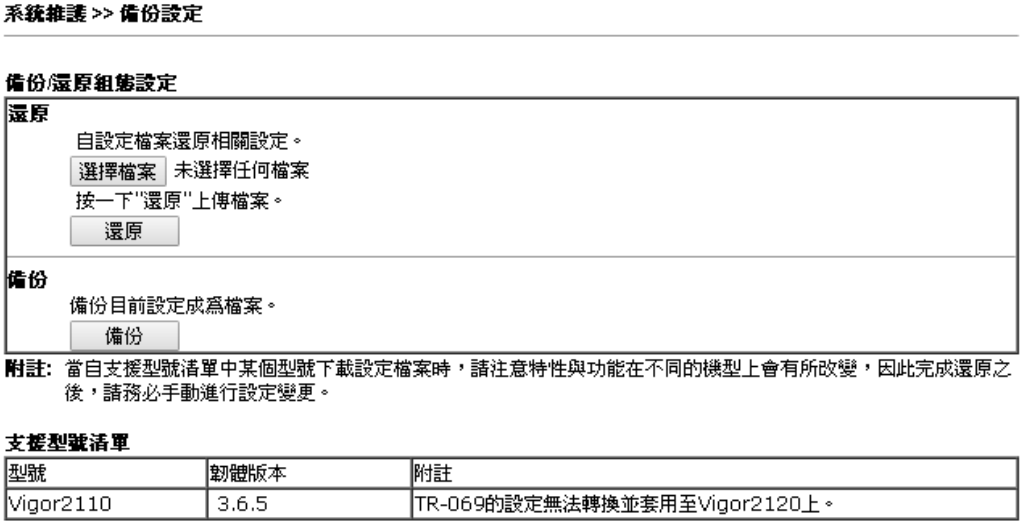
4. 按下**儲存(Save)**按鈕，設定將會以檔名 **config.cfg** 自動下載至電腦上。

上述範例是以 Windows 平臺來完成，對於 **Macintosh** 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

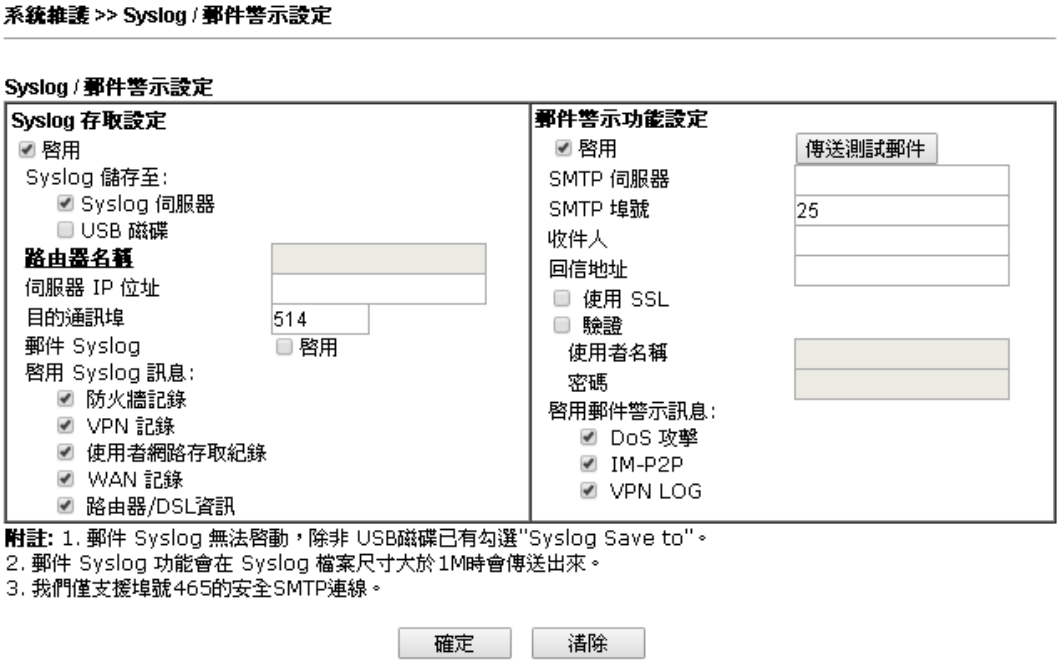
1. 在**系統維護**群組中按**設定備份(System Maintenance >> Configuration Backup)**，您將可看見如下視窗。



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

4.14.7 Syslog/郵件警示設定(Syslog/Mail Alert)

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。



可用設定說明如下：

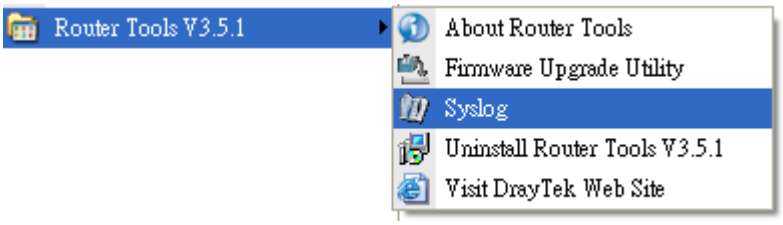
項目	說明
SysLog 存取設定 (SysLog Access Setup)	**啓用(Enable) -** 勾選**啓用**以啓動系統記錄服務功能/啓動郵件警示功能。 **Syslog 儲存至(Syslog Save to)** – 勾選此框可儲存紀錄至 Syslog 伺服器中。 **USB 磁碟(USB Disk) -** 勾選此框可儲存紀錄至 USB 儲存碟中。 **路由器名稱(Router Name)** – 顯示此路由器於**系統維護>>管理(System Maintenance>>Management)**頁面中設定的名稱。 若此處沒有名稱，請至**系統維護>>管理**設定路由器名稱。 **伺服器 IP 位址(Server IP Address)**-指定全部系統紀錄訊息傳送前往目的地之 IP 位址。 **目的通訊埠(Destination Port)**-指定全部系統紀錄訊息傳送前往目的地之通訊埠。 **郵件 Syslog(Mail Syslog) –** 郵件事件紀錄至 Syslog 上。 **啓用 Syslog 訊息(Enable syslog message)**-勾選此頁面上所列的小方塊，傳送防火牆、VPN、使用者存取、撥號、WAN、路由器/DSL 等資訊紀錄至 Syslog 上。

郵件警示功能設定 **(Mail Alert Setup)**	勾選**啓用(Enable)**以便啓動郵件警示功能。 **傳送測試郵件(Send a test e-mail)**-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/埠號(SMTP Server/SMTP Port)** -指定 SMTP 伺服器的 IP 位址/埠號，直接傳送來自 Vigor 路由器的郵件至收信人的信箱。 **收件人(Mail To)**-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(Return-Path)**-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。 **使用 SSL(Use SSL)** - 勾選此框使用埠號 465 作爲 SMTP 伺服器，讓電子郵件伺服器使用 HTTPS 作爲傳輸方式。 **驗證(Authentication)**-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(User Name)**-輸入驗證所需的使用者名稱。 ● **密碼(Password)**-輸入驗證所需的密碼。 **啓用郵件警示訊息(Enable E-mail Alert)**-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。

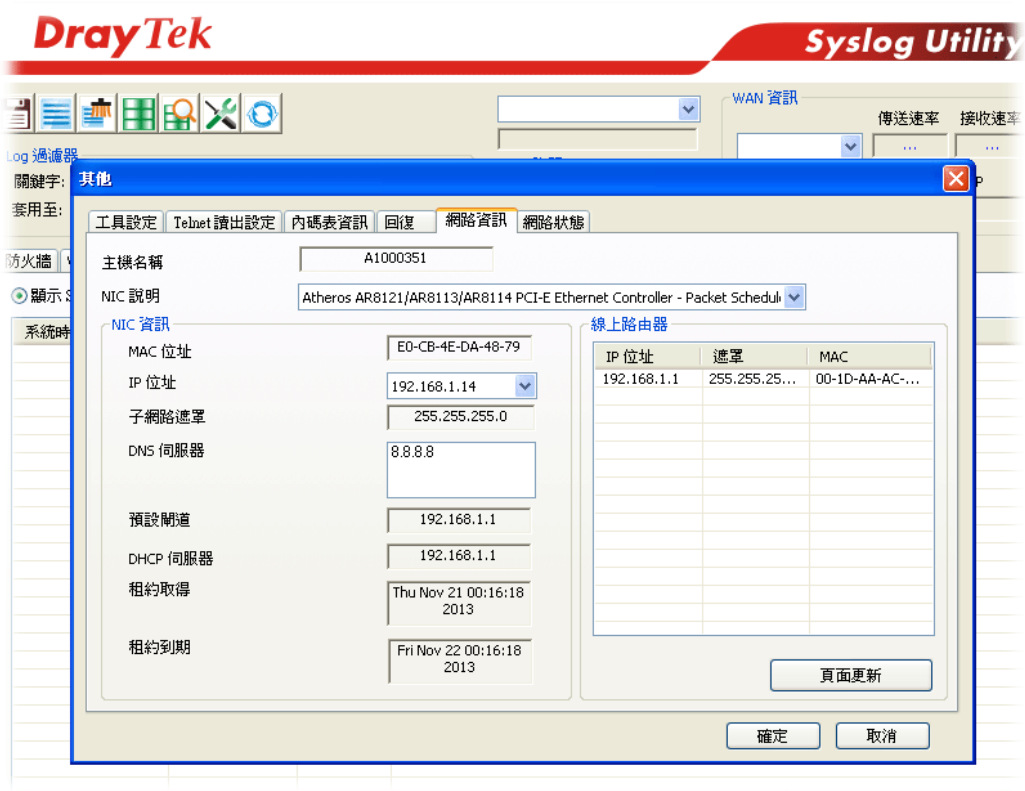
按**確定(OK)**儲存所有的設定。

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**。

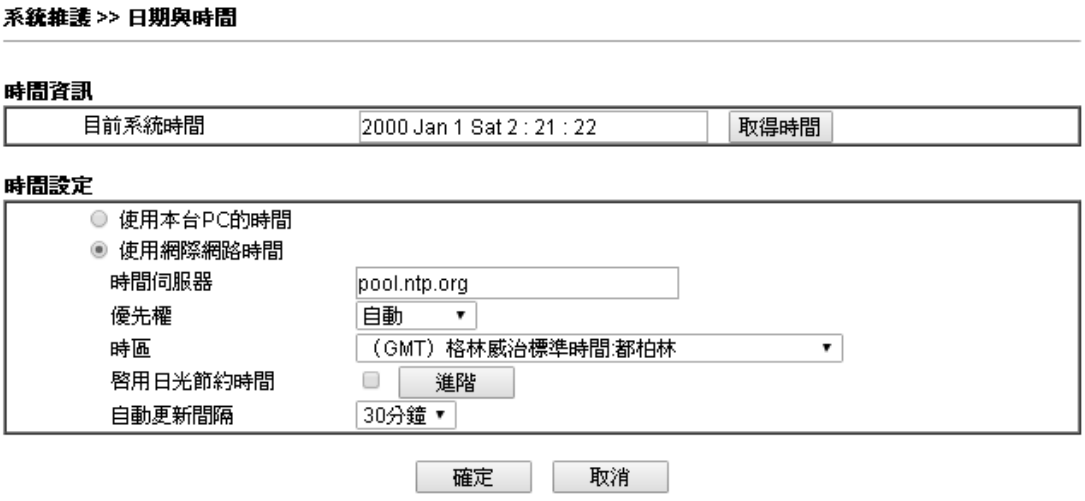


3. 自 Syslog 畫面上，選擇您想要監視的路由器。請記住在**網路資訊(Network Information)**中，選擇用來連接路由器的網路交換器，否則您無法成功檢索來自路由器的資訊。



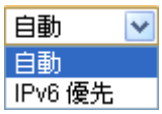
4.14.8 時間和日期(Time and Date)

允許您指定自何處取得路由器時間。



可用設定說明如下：

項目	說明
目前系統時間 (Current System Time)	按**取得時間(Inquire Time)**按鈕取得目前時間。
使用本台 PC 的時間 (Use Browser Time)	選擇此項以便採用遠端管理者電腦上的瀏覽器時間。

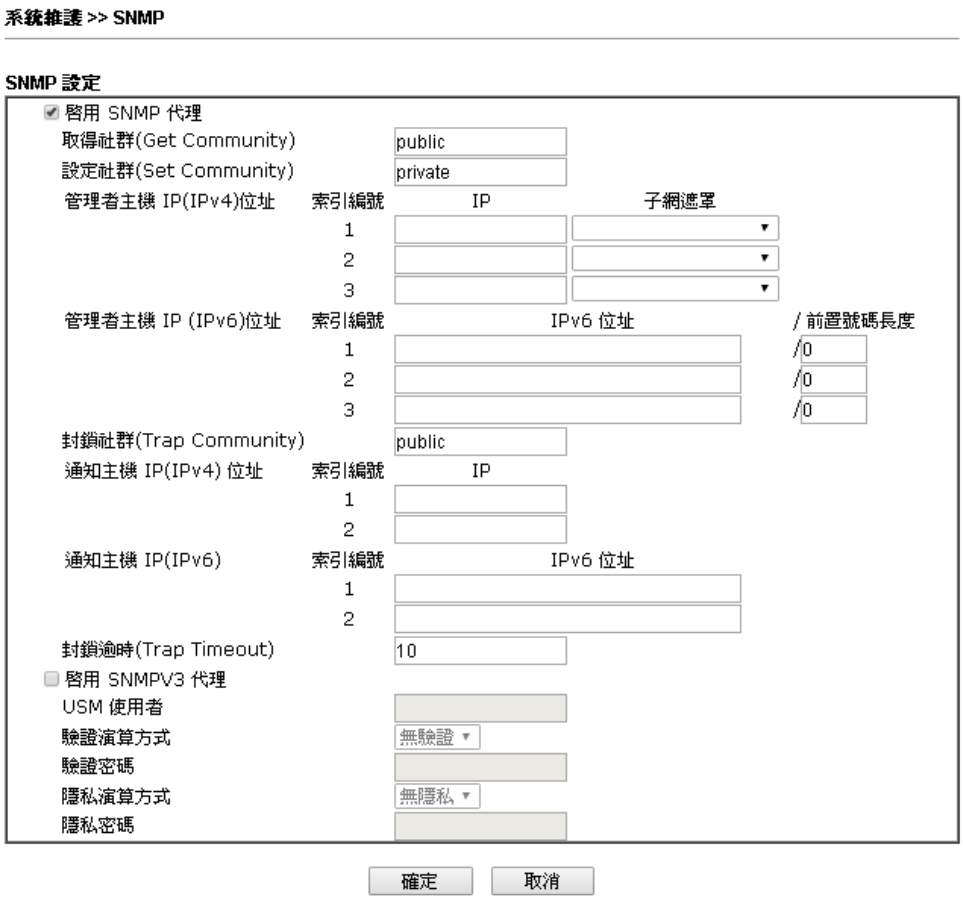
使用網際網路時間 (Use Internet Time)	選擇此項以便自網際網路上的時間伺服器選擇所需的時間資訊。
時間伺服器 (Time Server)	輸入時間伺服器所需的 IP 位址或網址。
優先權 (Priority)	選擇**自動(Auto)**或是 **IPv6 優先(IPv6 First**，時間伺服器以支援 IPv6 的網域名稱來設定**)**作爲優先選項。 
時區 (Time Zone)	選擇路由器所在的時區。
啓動日光節約時間 (Enable Daylight Saving)	勾選此方塊啓動日光節約時間，在某些地區，這個項目是很有用處的。
自動更新間隔 (Automatically Update Interval)	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(OK)**儲存目前的設定。

4.14.9 SNMP

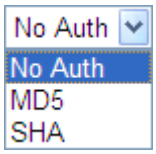
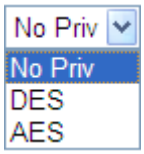
本頁讓您設定 SNMP 與 SNMP3 服務的相關設定。

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



可用設定說明如下：

項目	說明
啓用 SNMP 代理 (Enable SNMP Agent)	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 (IPv4) (Manager Host IP (IPv4))	設定一台主機做爲管理者以便執行 SNMP 功能，請輸入 IP 位址(IPv4)指定特定主機。
管理者主機(IPv6) (Manager Host IP (IPv6))	設定一台主機做爲管理者以便執行 SNMP 功能，請輸入 IP 位址(IPv6)指定特定主機。

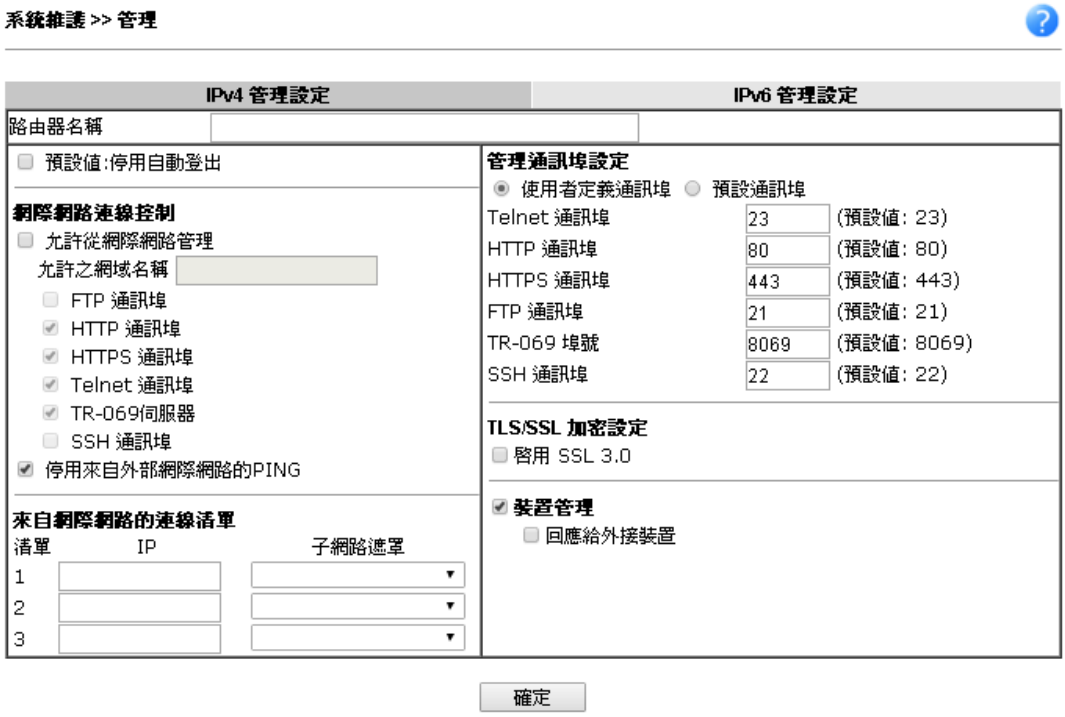
封鎖社群 **(Trap Community)**	輸入適當名稱設定封鎖社群，預設名稱爲 **public**。
通知主機 IP(IPv4) **(Notification Host IP (IPv4))**	設定主機的 IP 位址(IPv4)接收封鎖社群的資料。
通知主機 IP (IPv6) **(Notification Host IP (IPv6))**	設定主機的 IP 位址(IPv6)接收封鎖社群的資料。
封鎖逾時 **(Trap Timeout)**	預設值爲 10 秒。
啓用 SNMPV3 代理 **(Enable SNMPV3 Agent)**	勾選此框啓用此功能。
USM 使用者 **(USM User)**	USM 代表使用者爲主的安全模式。 輸入做爲驗證之用的使用者名稱。
驗證演算方式 **(Auth Algorithm)**	選擇下列任一種方式作爲驗證演算法。 
驗證密碼 **(Auth Password)**	輸入驗證需求的密碼。
隱私演算方式 **(Privacy Algorithm)**	選擇下列任一種方式作爲隱私演算法。 
隱私密碼 **(Privacy Password)**	輸入隱私需求的密碼。

全部設定完成之後，請按**確定(OK)**儲存目前的設定。

4.14.10 管理(Management)

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

針對 IPv4



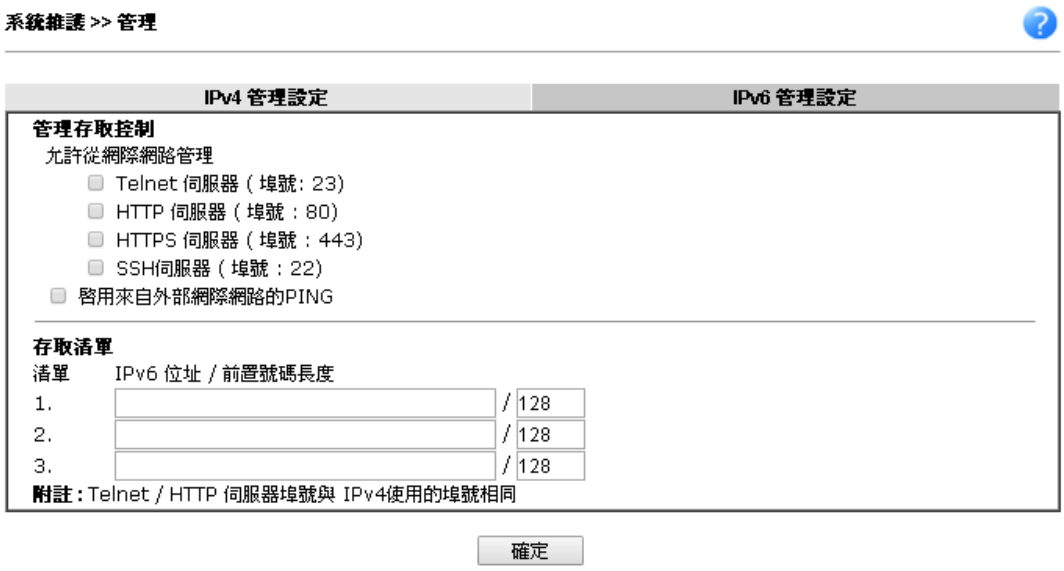
可用設定說明如下：

項目	說明
路由器名稱 (Router Name)	輸入路由器的名稱。
預設值:停用自動登出 (Default: Disable Auto-Logout)	如果啓用此功能，網頁設定介面就無法使用自動登出離開設定畫面。  除非您按下登出圖示，否則網頁設定介面將會處於一直開啓狀態。 

網際網路連線控制 **(Internet Access Control)**	**允許從網際網路管理(Allow management from the Internet) -**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。 **停用來自外部網際網路的 PING(Disable PING from the Internet) -**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。
來自網際網路的連線清單 **(Access List from the Internet)**	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(List IP) –** 指定一個允許登入至路由器的 IP 地址。 **子網路遮罩(Subnet Mask) -**代表允許登入至路由器的子網路遮罩。
管理通訊埠設定 **(Management Port Setup)**	**使用者定義通訊埠(User Define Ports)-**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(Default Ports)-**勾選此項以使用標準埠號作爲 Telnet 和 HTTP 伺服器之用。
TLS/SSL 加密設定 **(TLS/SSL Encryption Setup)**	**啓用 SSL3.0(Enable SSL 3.0) –** 如有需要，可勾選此方塊啓用 SSL3.0 的功能。 考量到網路安全性之故，路由器內建 HTTPS 與 SSL VPN 伺服器皆已經更新改用 TLS1.x 協定。但是有些情況例外，例如您使用的是舊型瀏覽器(如 IE6)或是舊版 SmartVPN Client，或許會有需要啓動 SSL3.0 來確保連線。雖然如此，我們不建議您這樣處理。
裝置管理 **(External Device Control)**	**回應給外接裝置(No respond to External Device) –** 勾選此方況可讓路由器爲其他路由器偵測到時，不會以外接裝置的身分呈現在其他路由器的設定介面上。

全部設定完成之後，請按**確定(OK)**儲存目前的設定。

針對 IPv6



可用設定說明如下：

項目	說明
管理存取控制 (Management Access Control)	**允許從網際網路管理(Allow management from the Internet)** - 勾選下述方框可讓系統管理者自網際網路登入此路由器設定介面，有數種伺服器可以選擇讓您來管理。 **啓用來自外部網際網路的 PING (Enable PING from the Internet)**- 勾選此方框可讓系統接受來自外部網際網路的封包檢測，針對安全需要，此功能在預設時是關閉的。
存取清單 (Access List)	您可以指定系統管理者只能從特定主機或是網路登入，一次可設定三組 IP 位址。 **IPv6 位址/前置號碼長度(IPv6 Address /Prefix Length)** - 指定允許登入路由器的 IP 位址。

全部設定完成之後，請按**確定(OK)**儲存目前的設定。

4.14.11 重啓路由器(Reboot System)

網路設定可以用來重新啓動路由器，請自**系統維護(System Maintenance)**中選擇**重啓路由器(Reboot System)**開啓如下頁面。

索引編號(1-15)於排程設定(Index (1-15) in Schedule Setup) - 您可以輸入四組排程設定檔進行系統重啓作業，所有的排程都可以在**其他應用>>排程(Applications >> Schedule)**頁面中先行設定。

如果您想要使用目前的設定來重新啓動路由器，請勾選**使用目前組態(Using current configuration)**，然後按**立即重啓(Reboot Now)**；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(Using factory default configuration)**，然後按**立即重啓(Reboot Now)**，路由器將會花 5 秒重新啓動系統。

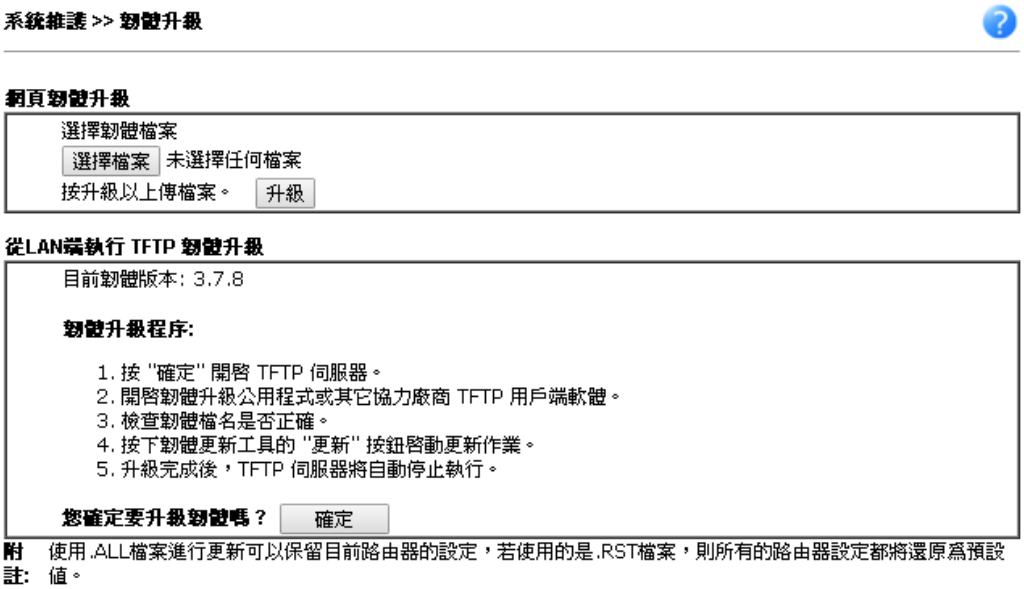
注意:.當系統在您完成網頁設定並跳出**重啓路由器**網頁後，請務必按下**立即重啓(Reboot Now)**以重新啓動路由器，這個動作可以確保系統的操作正常，且可避免未來發生不預期的錯誤。

4.14.12 韌體升級(Firmware Upgrade)

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。

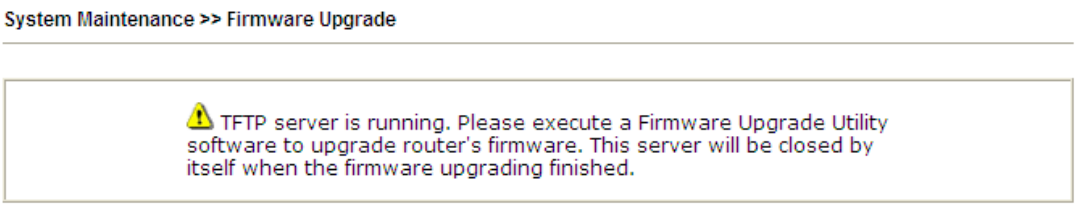
自居易網站或是 FTP 站下載最新的韌體版本，居易網站爲 www.draytek.com，FTP 站則是 ftp.draytek.com。

請自**系統維護**選擇**韌體升級**以便啓動韌體更新工具。



按**選擇檔案**選取正確的韌體版本，然後按**升級(Upgrade)**按鈕，系統會自動更新路由器的韌體版本。

按**確定**，下述畫面將會出現，之後再使用韌體更新工具完成更新。



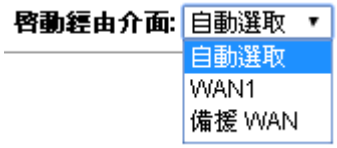
4.14.13 開啓授權碼(Activation)

有三種方式可開啓 Vigor 路由器的網頁內容過濾器服務(WCF)，使用**服務啓動精靈(Service Activation Wizard)**、透過**數位內容安全管理>>網頁內容過濾器設定檔(CSM>>Web Content Filter Profile)**或是透過**系統管理>>開啓授權碼(System Maintenance>>Activation)**。

在您完成 WCF 設定檔之後，您即可啓動網頁內容過濾服務機制。

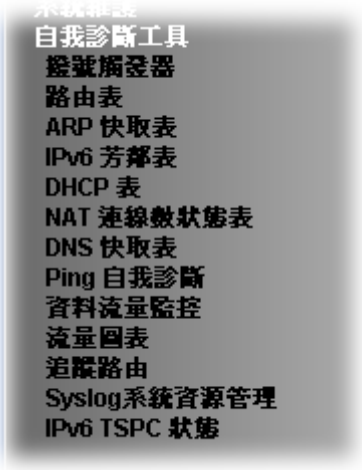
按**系統管理>>開啓授權碼(System Maintenance>>Activation)**開啓下述頁面以登入 http://myvigor.draytek.com。

可用設定說明如下：

項目	說明
啓動經由介面 (Activate via Interface)	選擇任何一種介面用以啓動網頁內容過濾器。 
啓動 (Activate)	此連結可讓您登入 www.vigorpro.com 完成帳號與路由器的啓動作業。
驗證訊息 (Authentication Message)	至於網頁過濾器的驗證資訊，驗證過程會顯示在此框中供您參考。

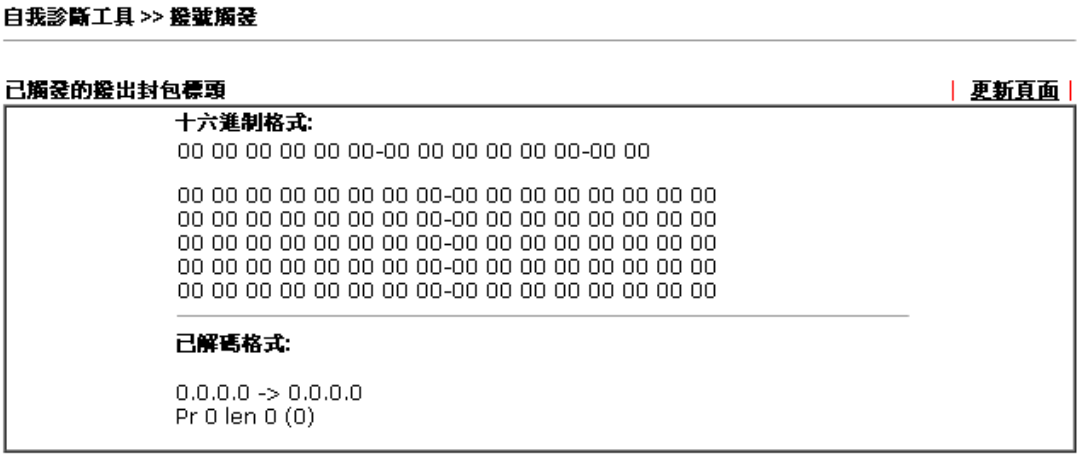
4.15 自我診斷工具(Diagnostics)

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：



4.15.1 撥號觸發器(Dial-out Triggering)

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。

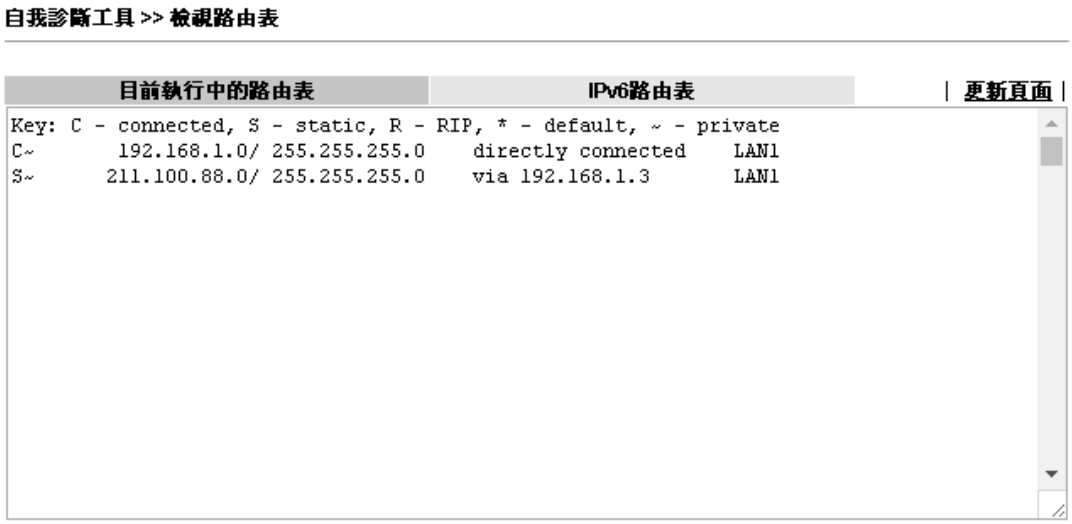


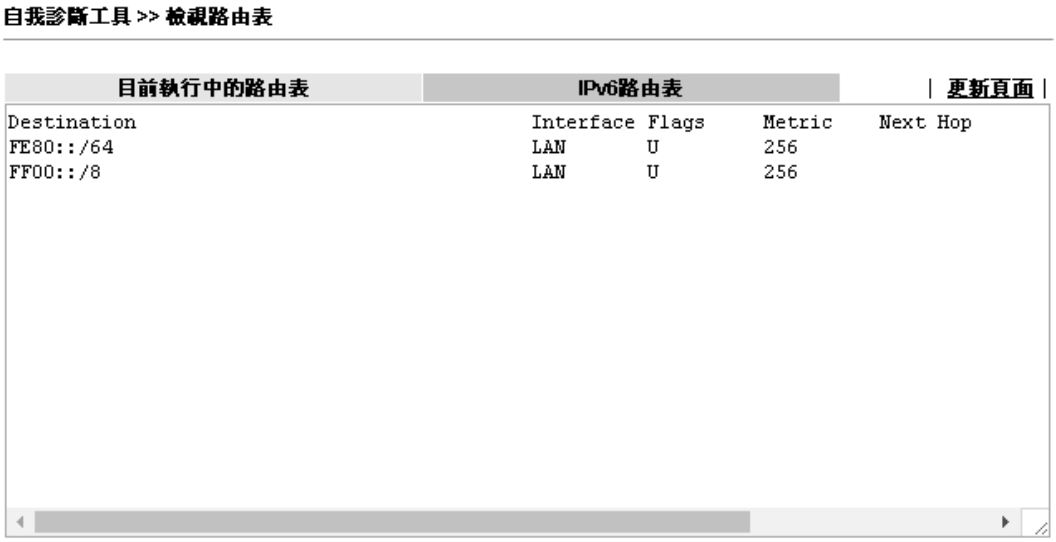
各個項目說明如下：

項目	說明
已解碼格式 (Decoded Format)	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 (Refresh)	按此鈕重新載入本頁。

4.15.2 路由表(Routing Table)

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





各個項目說明如下：

項目	說明
更新頁面 (Refresh)	按此鈕重新載入本頁。

4.15.3 ARP 快取表(ARP Cache Table)

按**自我診斷工具(Diagnostics)**的 **ARP 快取表(ARP Cache Table)**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。

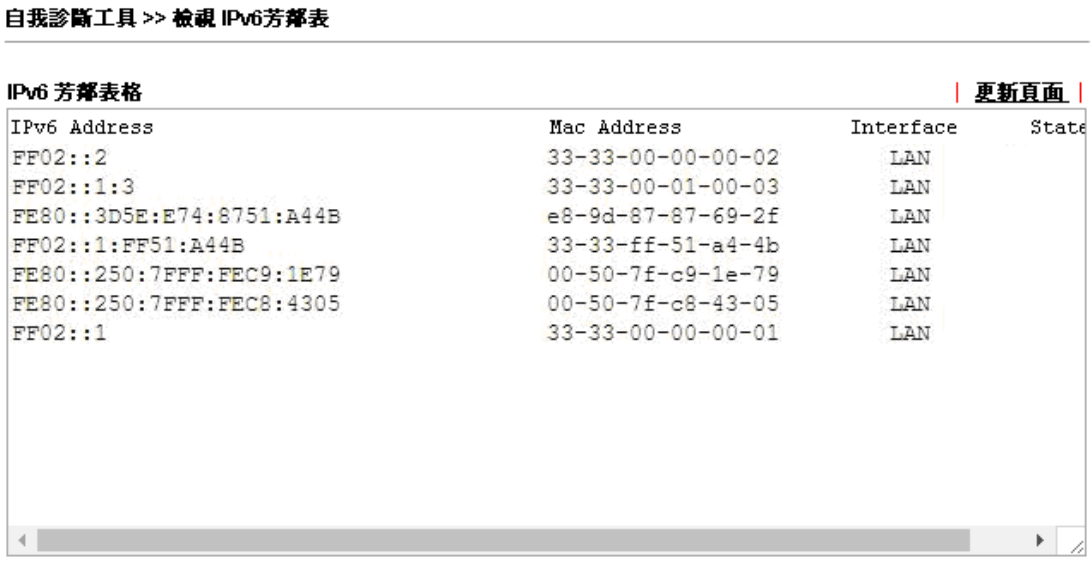
各個項目說明如下：

項目	說明
更新頁面(Refresh)	按此鈕重新載入本頁。

4.15.4 IPv6 芳鄰表(IPv6 Neighbour Table)

表格顯示乙太網路硬體位址(MAC 位址)與 IPv6 位址之間的對應關係，此項資訊對於診斷網路問題諸如 IP 位址衝突等方面很有幫助。

按**自我診斷工具>> IPv6 芳鄰表(Diagnostics>> IPv6 Neighbour Table)**開啓如下頁面。



各個項目說明如下：

項目	說明
更新頁面 (Refresh)	按此鈕重新載入本頁。

4.15.5 DHCP 表(DHCP Table)

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(Diagnostics)**，選擇 **DHCP 表(DHCP Table)**開啓相關網頁。

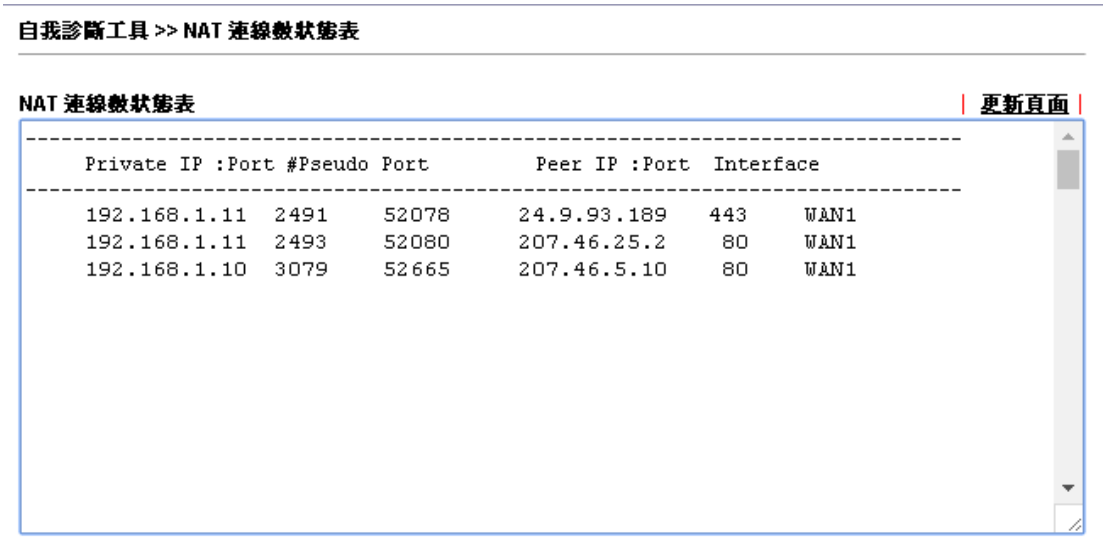
各個項目說明如下：

項目	說明
Index	顯示連線項目編號。
IP Address	顯示路由器指派給特定電腦的 IP 位址。
MAC Address	顯示 DHCP 指派給特定電腦的 MAC 位址。
Leased Time	顯示指定電腦的租約時間。

HOST ID	顯示指定電腦的主機 ID 名稱。
更新頁面 (Refresh)	按此鈕重新載入本頁。

4.15.6 NAT 連線數狀態表(NAT Sessions Table)

按**自我診斷工具(Diagnostics)**，選擇 **NAT 連線數狀態表(NAT Sessions Table)**開啓相關網頁。



各個項目說明如下：

項目	說明
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。
更新頁面 (Refresh)	按此鈕重新載入本頁。

4.15.7 DNS 快取表

按下**自我診斷工具>>DNS 快取表(Diagnostics>>DNS Cache Table)** 開啓設定網頁。

回應 LAN 端的 DNS 詢問的網域名稱與對應 IP 位址記錄，將會儲存在 Vigor 路由器暫存器並顯示於本頁面。

各個項目說明如下：

項目	說明
清除(Clear)	按此連結移除畫面上全部的結果。
更新頁面(Refresh)	按此鈕重新載入本頁。
當 TTL 值大於..(When an entry's TTL is larger than….)	勾選此框並輸入 TTL 值，按下確定(OK)按鈕之後，即可啓用此功能。 此數值表示當每個 DNS query 達到 TTL 值，相應的紀錄將自路由器的暫存器中自動刪除。

4.15.8 Ping 自我診斷(Ping Diagnosis)

按**自我診斷工具(Diagnostics)**，選擇 **Ping 自我診斷(Ping Diagnosis)**開啓相關網頁。

各個項目說明如下：

項目	說明
IPV4 /IPV6	選擇其中一項以便顯示相應的資訊內容。
Ping 至 **(Ping to)**	使用下拉式清單選擇您想要 Ping 的目標。
IP 位址 **(IP Address)**	輸入您想要 Ping 的主機/IP 上的 IP 位址。
Ping IPv6 位址 **(Ping IPv6 Address)**	輸入您想要 Ping 的主機/IP 上的 IPv6 位址。
執行 **(Run)**	按此鈕啓動 Ping 作業，結果將會顯示在螢幕上。

清除 (Clear)	按此連結清除視窗上的結果。

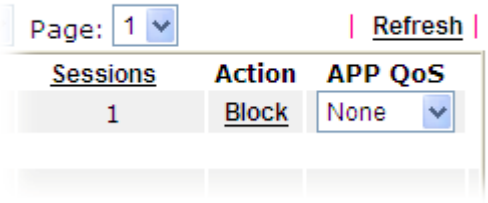
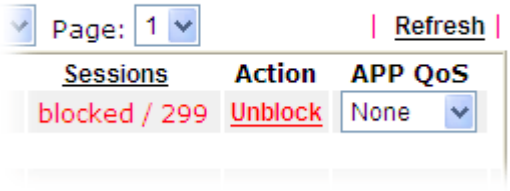
4.15.9 資料流量監控(Data Flow Monitor)

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(Diagnostics)**，選擇**資料流量監控(Data Flow Monitor)**開啓相關網頁。您可按下 **IP 位址**、**傳送速率**、**接收速率**或是 **NAT 連線數(IP Address, TX rate, RX rate** 或 **Session)**來排列資料。

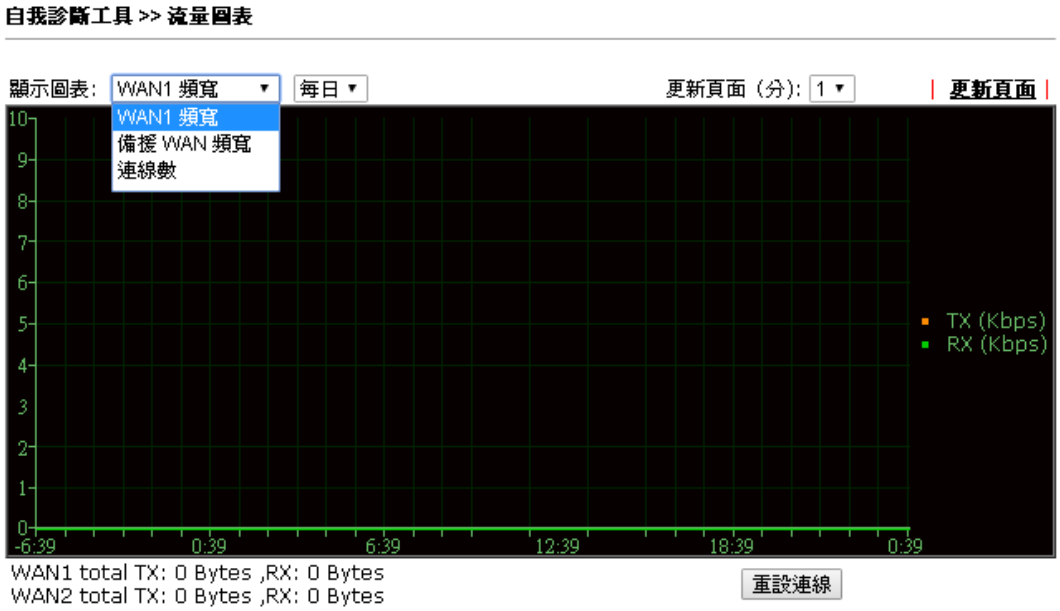
各個項目說明如下：

項目	說明
啓用資料流量監控 (Enable Data Flow Monitor)	勾選此方塊以啓動此功能。

更新秒數 (Refresh Seconds)	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 (Refresh)	按此連結更新本頁。
索引編號 (Index)	顯示資料流量的項目筆數。
IP 位址 (IP Address)	顯示被監視裝置的 IP 位址。
傳送速率 (kbps) (TX rate (kbps))	顯示被監視裝置的傳送速率。
接收速率 (kbps) (RX rate (kbps))	顯示被監視裝置的接收速率。
NAT 連線數 (Sessions)	顯示您在連線數限制網頁中所設定的連線數。
動作 (Action)	**封鎖(Block)** – 可以避免指定電腦在 5 分鐘內存取網際網路。  **解除(Unbloc)** – 指定 IP 位址的裝置將在五分鐘內封鎖起來，剩餘時間將顯示在 NAT 連線數欄位中。按下此鈕可以取消封鎖 IP 位址。 
現值/高峰值/速度 (Current /Peak/Speed)	**現值(Current)**表示目前 WAN1/WAN2 的傳輸速率與接收速率。 **高峰值(Peak)**表示路由器在資料傳輸上所檢測到的最高數值。 **速度(Speed)**表示 **WAN>>基本設定(WAN>>General Setup)** 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。

4.15.10 流量圖表(Traffic Graph)

按**自我診斷工具(Diagnostics)**，選擇**流量圖表(Traffic Graph)**開啓相關網頁。可以選擇**WAN1/WAN2/WAN3 頻寬**、**連線數**、**每日**、**每週**來檢視流量圖表。按下**重新設定(Reset)**可以將累計的傳送/接收資料全部歸零。您可隨時按**更新頁面(Refresh)**重新顯示圖表內容。

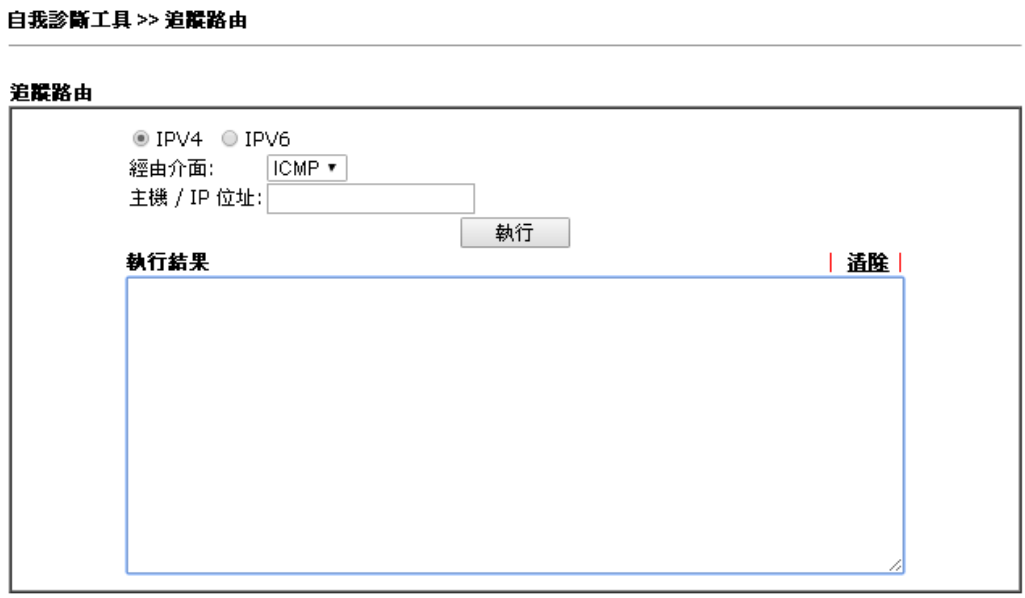


水準軸代表時間；而垂直軸代表的意義就很不同了。對 **WAN1 頻寬**而言，垂直軸代表的是過去所傳送與接收封包的數量。

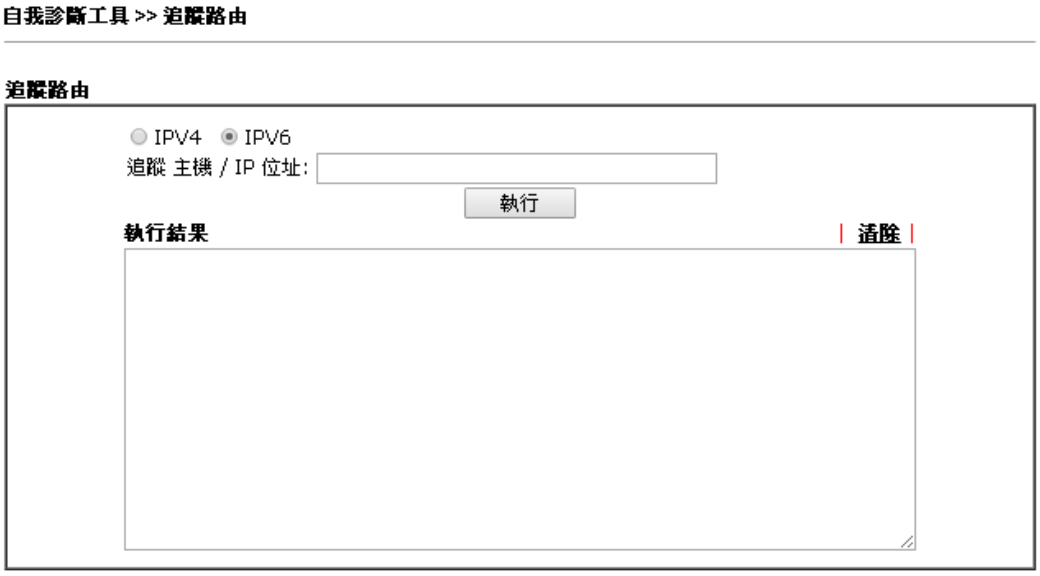
但對**連線數**來說，垂直軸代表的是過去一段時間之內的 NAT 連線數。

4.15.11 追蹤路由(Trace Route)

按下**診斷工具(Diagnostics)**，選擇**追蹤路由(Trace Route)**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(Run)**按鈕，整個路由狀況都將顯示在螢幕上。



或是



各個項目說明如下：

項目	說明
IPv4 / IPv6	選擇其中一項以便顯示相應的資訊內容。
經由介面 (Protocol)	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 (Host/IP Address)	指明主機的 IP 位址。

追蹤主機/IP 位址 (Trace Host/IP Address)	指明主機的 IPv6 位址。
執行(Run)	按此鈕開始路由追蹤動作。
清除(Clear)	按此連結刪除視窗上的結果。

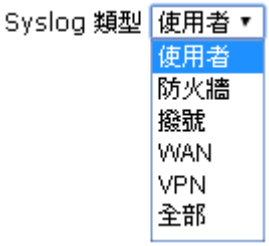
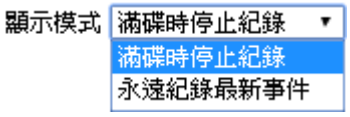
4.15.12 Syslog 系統資源管理 (System Explorer)

本頁提供即時的 Syslog 並且在頁面上顯示相關資訊。

針對網頁 Syslog

本頁顯示使用者/防火牆/電話/WAN/VPN 等設定的時間與訊息，您可以勾選啓用網頁 Syslog 方塊，指定 Syslog 的類型，並選擇顯示的模式。之後，特定類型事件的 Syslog 資料將會顯示於頁面上。

可用項目說明如下：

項目	說明
啓用網頁 Syslog (Enable Web Syslog)	勾選此方塊可啓動網頁 Syslog 記錄功能。
Syslog 類型 (Syslog Type)	使用下拉式清單指定準備顯示出來的 Syslog 的類型。 
輸出(Export)	按下此連結可以將本頁紀錄的內容儲存成檔案。
更新頁面(Refresh)	按下此連結可以手動更新本頁紀錄的內容。
清除(Clear)	按下此連結可以清除本頁紀錄的內容。
顯示模式 (Display Mode)	有二種模式可以選擇：  **滿碟時停止紀錄(Stop record when fulls) –** 當 syslog 的容量已滿，系統將停止紀錄。 **永遠紀錄最新事件(Always record the new event)–** 系統只

	紀錄最新的事件。
時間(Time)	顯示事件發生的時間。
訊息(Message)	.顯示事件發生的相關資訊。

針對 USB Syslog

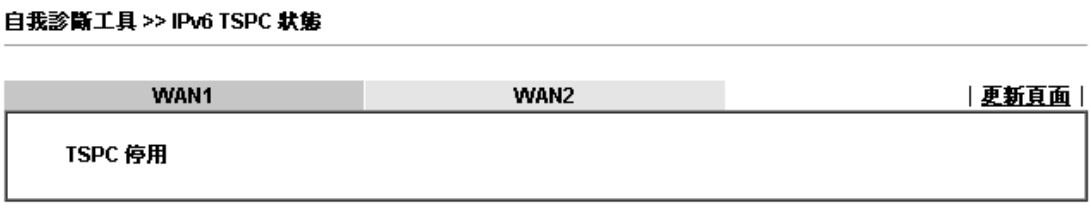
本頁顯示暫存在 USB 儲存碟內的 Syslog 紀錄。

可用項目說明如下：

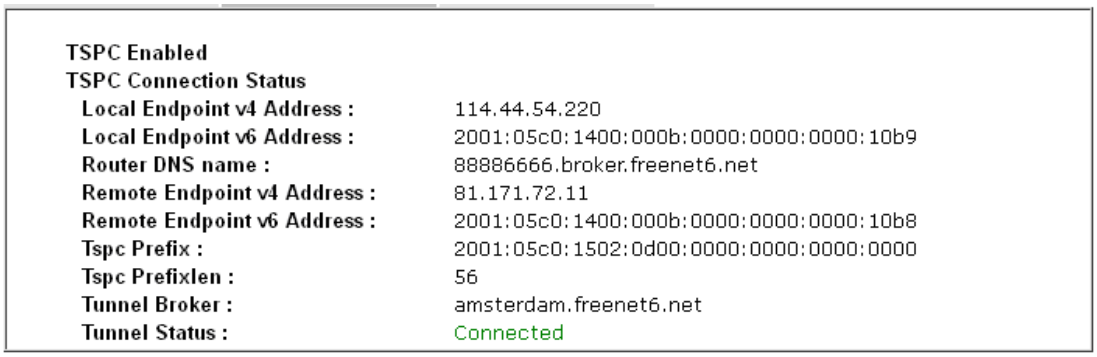
項目	說明
時間(Time)	顯示事件發生的時間。
紀錄類型(Log Type)	顯示紀錄的類型。
訊息(Message)	顯示事件發生的相關資訊。

4.15.13 IPv6 TSPC 狀態(IPv6 TSPC Status)

IPv6 TSPC 狀態頁面可以幫助您診斷 TSPC 的連線狀態是否正常。



如果 TSPC 設定無誤，當使用者成功連上通道的時候，路由器將會顯示如下頁面：



可用項目說明如下：

項目	說明
更新頁面 (Refresh)	按下此連結可以手動更新本頁紀錄的內容。

本頁留白

5 疑難排解

這個章節將會指導您，如何解決在完成安裝和設置路由器後依然無法上網的問題。請按以下方法一步一步地進行檢查。

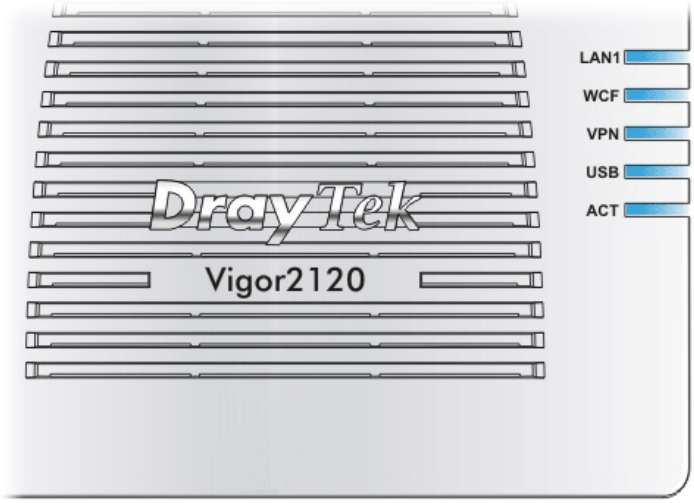
- 檢查路由器硬體狀態是否正常
- 檢查您電腦的網路連接設置是否正確
- 試試看能否從電腦 ping 到路由器
- 檢查 ISP 的設置是否正常
- 必要的話將路由器恢復至預設出廠設置

如果以上步驟仍無法解決您的問題，您需要聯絡代理商取得進一步的協助。

5.1 檢查路由器硬體狀態是否正常

按以下步驟檢查硬體狀態。

1. 檢查電源線以及 LAN 的連接。詳細資訊請參考“**1.3 硬體安裝**”。
2. 開啓路由器，確認 **ACT** 指示燈差不多每秒閃爍一次，以及相對應的 **LAN** 指示燈是否亮燈。



3. 如果沒有，意味著路由器的硬體有問題。那麼請回到“**1.3 硬體安裝**”，再重新執行一次硬體安裝，然後再試試。

5.2 檢查您電腦的網路連接設置是否正確

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

對於 Windows 系統

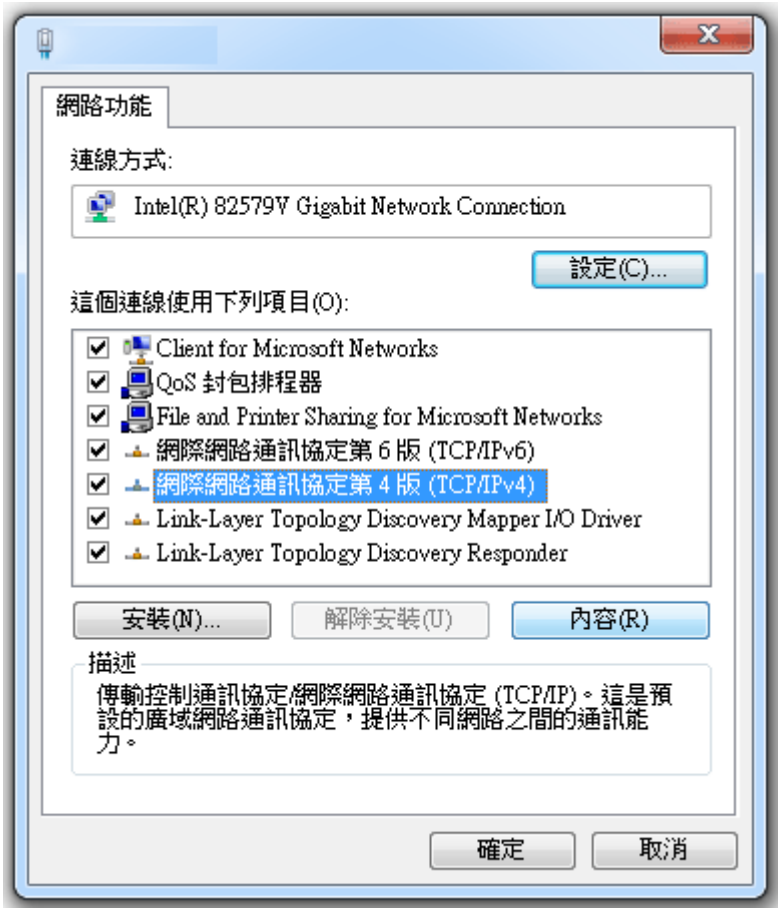
> 下列的範例是以 Windows 7 作業系統爲基礎而提供。若您的電腦採用其他的作業系統，請參照相似的步驟或至 www.draytek.com.tw 查閱相關的技術文件說明。

1. 開啓程式集>>控制台，按網路和共用中心。

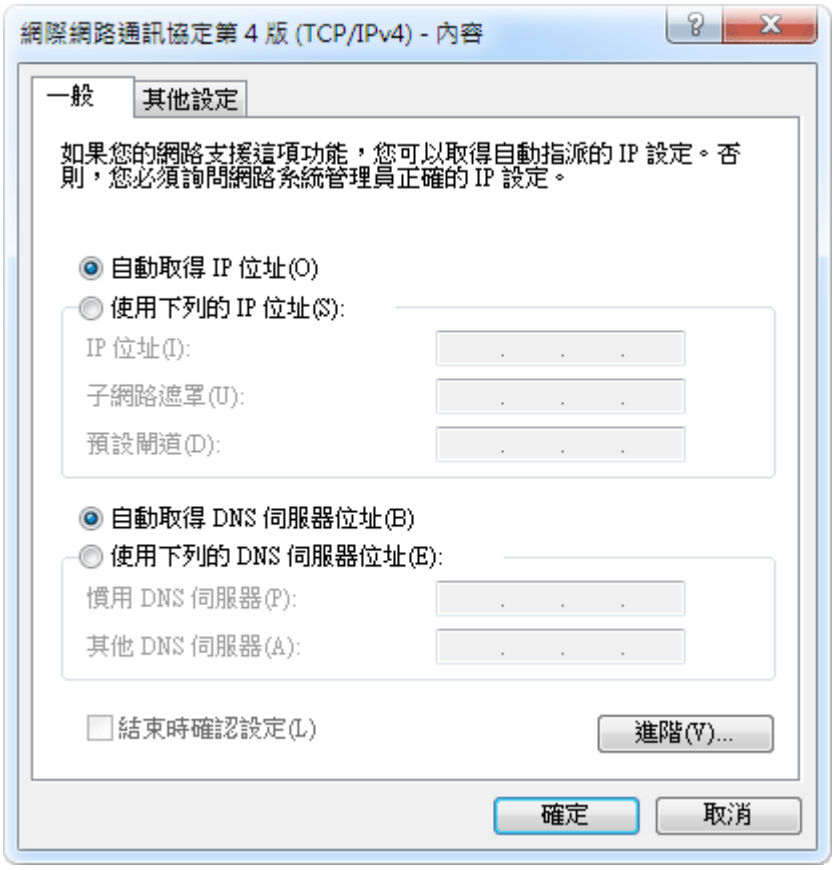
2. 在開啓的畫面上，按下變更介面卡設定連結。

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

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



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



對於 Mac 系統

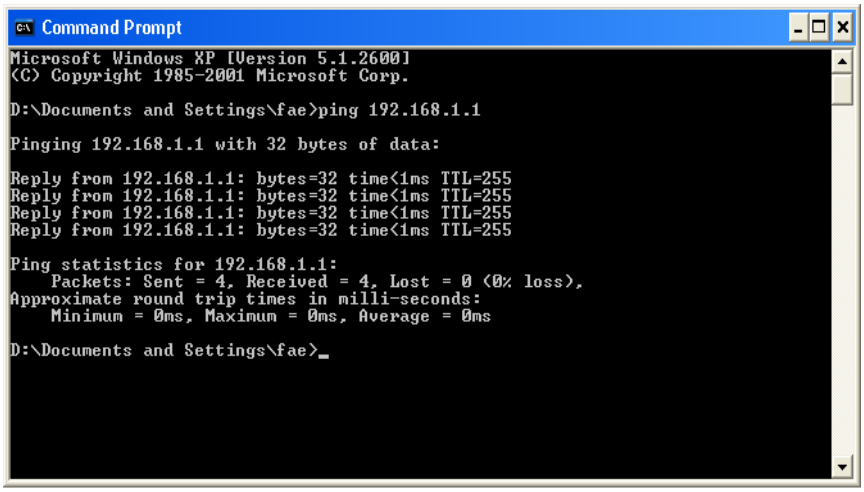
1. 在桌面上選擇目前所使用的 MacOS 磁碟機按滑鼠二下。
2. 選擇**應用**檔案夾中的**網路**檔案夾。
3. 進入**網路**畫面，在**設定**選項中，選擇**使用 DHCP**。

5.3 從電腦上 Ping 路由器

路由器的預設閘道爲 192.168.1.1. 因爲某些理由，你可能需要使用 " ping " 指令檢查路由器的連結狀態。比較重要的是電腦是否收到來自 192.168.1.1 的回應，如果沒有，請檢查個人電腦上的 IP 位址。我們建議您將網際網路連線設定爲自動取得 IP 位址。(請參照 5.2 檢查您個人電腦內的網路連線設定是否正確)，請依照以下的步驟正確地 ping 路由器。

對於 Windows 系統

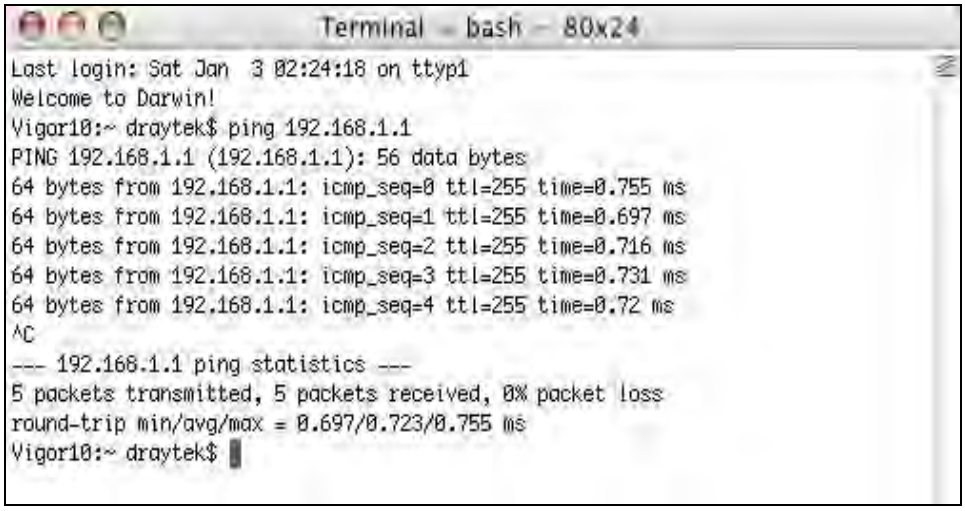
1. 開啓**命令提示字元視窗** (功能表選單**開始>>執行**) 。
2. 輸入 **command** (適用於 Windows 95/98/ME)或 **cmd** (適用於 Windows NT/ 2000/XP/Vista)。DOS 命令提示字元視窗將會出現。



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

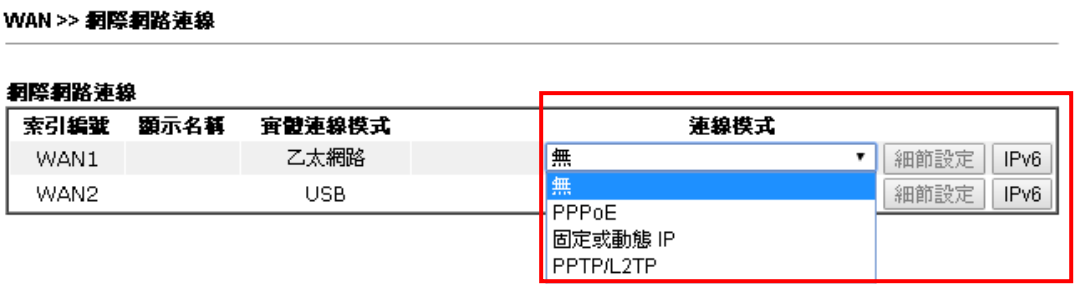
1. 在桌面上選擇目前所使用的 Mac OS 磁碟機，並在上面按滑鼠二下。
2. 選擇 **Applications** 檔案夾中的 **Utilities** 檔案夾。
3. 滑鼠按二下 **Terminal**；終端機的視窗將會跳出並顯現在螢幕上。
4. 輸入 **ping 192.168.1.1** 並且按下 **Enter** 鍵。如果連結正常，終端機視窗會出現“**64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=xxxx ms**” 的訊息。



5.4 檢查 ISP 的設置是否正常

如果 WAN 連不起來，檢查燈號是否正確(依照前述 LED 說明檢查)，若燈號未亮則

- 檢查 ISP 提供設定是否正確
- **Physical Type** 將預設 **Auto negotiation** 變更爲其他數值(例如 100M 全雙工)
- 其次檢查 ISP 提供的 modem(例如 DSL/FTTX(GPON)/Cable modem)將其速度設定爲相對應的速度，並確定路由器的燈號是否亮燈
- 若完成上述步驟仍未亮燈，則請安裝另外的 switch 串聯二端(路由器與 ISP 提供的 modem)，並確認燈號是否已亮燈
- 若上述步驟仍無法解決燈號問題，請立刻與最近的 reseller 連絡，或是寫信至居易技術服務部門尋求協助
- 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。



5.5 3G/4G 網路連線相關問題

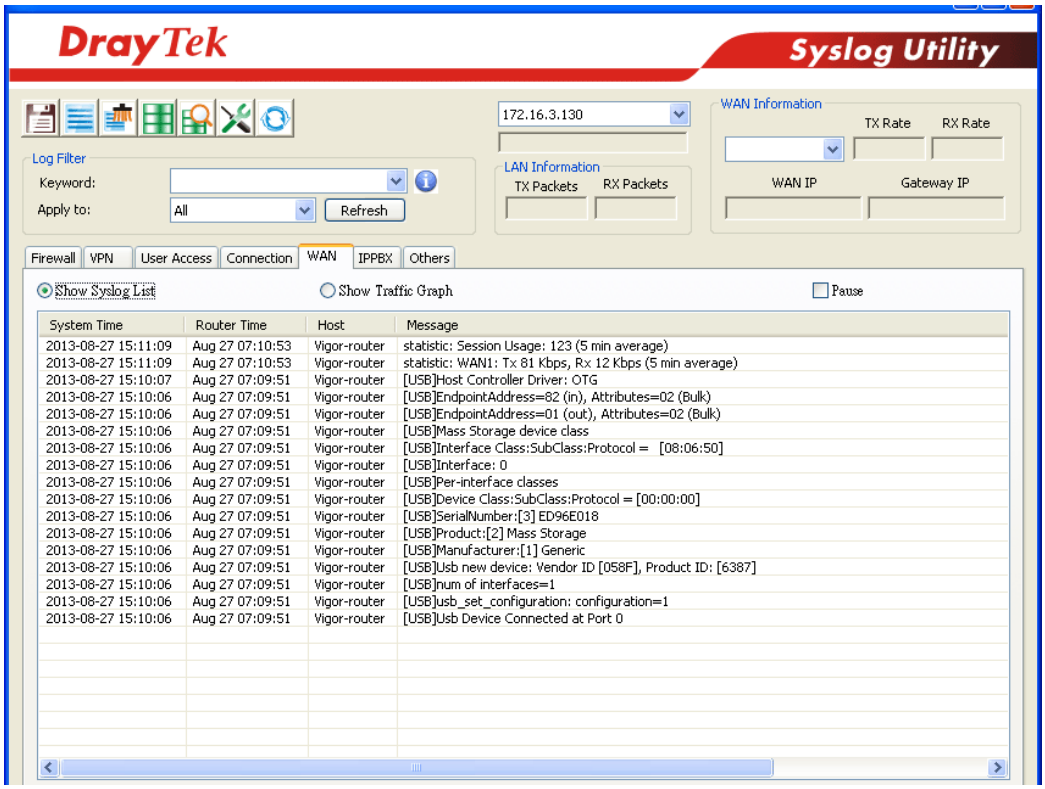
當您使用 3G/4G 網路傳輸發現問題時，請先檢查下列各項：

檢查 USB LED 燈號

在插入 3G/4G USB Modem 至 Vigor2120 後，您必須等待 15 秒左右，稍後 USB LED 會亮燈，表示 3G/4G USB Modem 安裝成功。如果 USB LED 燈號未亮，請將 3G/4G USB Modem 移除再重新插入，如果仍然失敗，請重新啓動路由器。

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/4G USB Modem 的工具關閉 PIN 碼然後再試一次。如果還是不行，那就可能是系統的相容性問題，麻煩開啓 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/4G USB Modem 來測試連線速度，檢查是否這個問題是 Vigor2120 所造成的，此外，請參考 3G/4G USB Modem 手冊中燈號意義，確保數據機是透過 HSDPA 模式連接網際網路。如果您想要在室內使用 3G/4G USB Modem，請放置在靠窗位置以取得較佳的接收信號。

5.6 還原路由器原廠預設組態

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

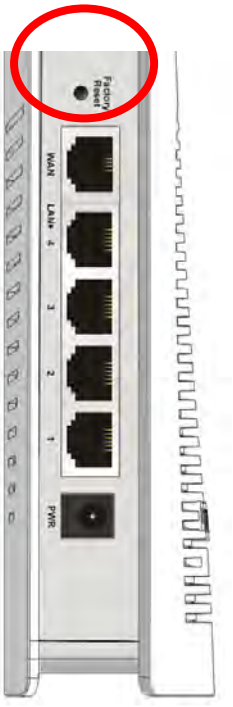
警告： 在使用原廠預設組態後，您之前針對分享器所調整的設定都將恢復成預設值。請確實記錄之前路由器所有的設定。

軟體重新設定

請進入管理者模式，再到網頁介面上的**系統維護>>重啓路由器(System Maintenance>> Reboot System)**，可見下圖。選擇**使用原廠預設組態(sing factory default configuration)**，並按下**立即重啓(Reboot Now)**。幾秒鐘後，路由器就會恢復至出廠預設設定。

硬體重新設定

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



恢復至出廠預設值後，您就可以按個人需要，重新設定路由器。

5.7 聯絡居易

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