EDIMAX
NETWORKING PEOPLE TOGETHER

VR-042

使用手冊

04-2012 / v1.0

EDIMAX
NETWORKING PEOPLE TOGETHER

COPYRIGHT

Edimax Technology Co., Ltd. makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability, or fitness for any particular purpose. Any software described in this manual is sold or licensed as is. Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Edimax Technology Co., Ltd. reserves the right to revise this publication and to make changes from time to time in the contents hereof without the obligation to notify any person of such revision or changes.

The product you have purchased and the setup screen may appear slightly different from those shown in QIG. For more information about this product, please refer to the user manual on the CD-ROM. The software and specifications are subject to change without notice. Please visit our website www.edimax.com for updates. All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

Edimax Technology Co., Ltd.
Add: No. 3, Wu-Chuan 3rd Rd., Wu-Ku Industrial Park, New Taipei City, Taiwan
Tel: +886-2-77396888
Email: sales@edimax.com.tw

Notice According to GNU General Public License Version 2

This product includes software that is subject to the GNU General Public License version 2. The program is free software and distributed without any warranty of the author. We offer, valid for at least three years, to give you, for a charge no more than the costs of physically performing source distribution, a complete machine-readable copy of the corresponding source code.

Content

I. 產品介紹

雙 WAN 安全路由器具備預設 2 組 10/100 Base-T/TX 乙太網路廣域網埠口及 3 組 10/100 Base-T/TX 乙太網路區域網埠口。這是一台能有效整合新一代網路的雙 WAN 企業等級安全路由器，可以滿足中小企業、網咖、校園、宿舍及社區網路的需求。

此路由器採用 64 位元多核心硬體加速高階網路專用處理器，封包處理快速穩定。內建高規格大容量記憶體，長時間高負載運作穩定可靠。

此路由器不僅支援 VPN 連線，並且具備現代企業廣泛使用的 VPN 硬體加速模式。

IPSec VPN 支援 DES、3DES、AES-128 加密，MD5、SH1 認證，IKE Pre-Share Key、或是手動設定的密鑰交換。支援 Aggressive Mode，斷線後自動重新連線，以及網路芳鄰透通。支持群組式浮動 IP 用戶端與總部進行虛擬私有網連線。另具備 PPTP 伺服器功能，具備連線狀態顯示。每個 WAN 口可同時建立多種 DDNS 設定，可使用動態 IP 建立 VPN 連線。

強效的防火牆系統，以滿足多數企業對防禦外部網路攻擊的市場需求。主動式封包檢測功能，經由對網路層連線的動態檢測，拒絕或阻擋非標準通信協定的連線要求。只需單向啓動各式駭客攻擊、蠕蟲病毒、ARP 攻擊防護功能，即可簡易完成配置，有效防止內外網惡意攻擊，確保網路安全。防火牆系統除了 NAT 之外，還具備有防止阻斷服務攻擊。功能完整的存取規則設定，可讓管理者選擇應該禁止或開放存取的網路服務，限制或禁止區域網內使用者的網路使用權限，以避免佔用網路資源或是不當使用而遭受潛在的危機。

此路由器可以完整的保障企業總部及分支的通訊安全，阻絕來自外部的駭客攻擊。透過 Web 呈現的使用者介面設定，網管可以不需要具備專業的網路知識就可以達到輕易設定及使用防火牆的需求。不僅 Microsoft Internet Explorer，也同樣支援 Netscape、Firefox 及 MAC 系統的 Safari 瀏覽器。

II. 雙 WAN 路由器配置操作流程

本章節介紹用戶整體配置雙 WAN 路由器操作流程，通過對路由器雙 WAN 配置流程的瞭解可以很輕鬆的配置我們的網路，來有效的管理我們的網路，使路由器達到應有的功能，使路由器的效能達到最高。

2.1 系統性配置流程的需要

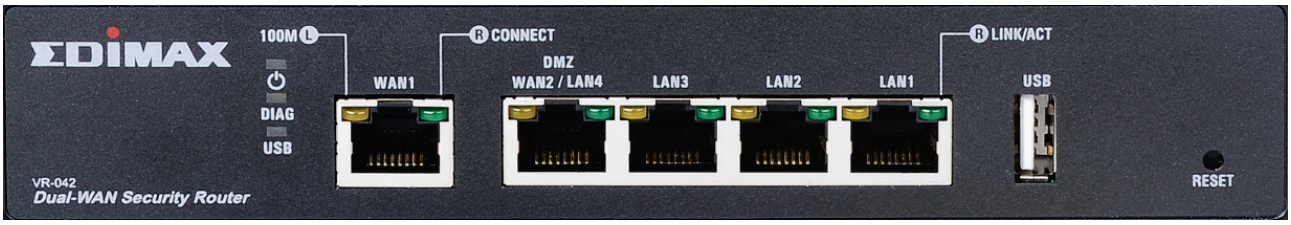
用戶可以通過以下操作流程配置我們的網路，能夠使我們的網路能夠有效利用頻寬，網路效能達到理想的效果，同時可以阻斷一些攻擊與預防一些安全隱患，通過流程配置更加方便用戶的安裝與操作，簡化維護管理的難度，使得用戶的網路配置一次到位。配置主要流程如下：

1. 硬體安裝。
2. 登錄配置視窗。
3. 確定設備規格及進行密碼和時間設置。
4. 進行廣域網連線的配置：進行內部連線的配置。
5. 進行內部連線的配置：實體線路配置及 IP 位址配置
6. 進行 QoS 頻寬管理配置：防止頻寬佔用情況。
7. 進行防火牆配置：預防攻擊及不當存取網路資源。
8. 其他特別配置：開放伺服器、DDNS、MAC Clone。
9. 管理維護的配置系統日誌、SNMP、及設定參數備份登出配置視窗。
10. VPN 虛擬私有網路功能設定。
11. 登出配置視窗。

III. 硬體安裝

本章介紹產品的硬體界面以及實體安裝。

3.1 路由器前面板以及 LED 顯示燈



LED Signal Description

LED/顏色	意義
⏻ -電源 (綠燈)	電源開啓連接
DIAG-自我測試 (橘燈)	橘燈閃：系統尚未完成開機自我檢測功能. 橘燈亮：系統當機. 橘燈熄滅：系統已經正常完成開機自我檢測功能.
WAN/ DMZ: Link/Act (綠燈)	綠燈亮：埠已經連線並取得 IP 位址 綠燈閃爍：埠正在傳送/接收封包資料傳輸 綠燈熄滅：埠無法取得 IP 位址
LAN: Link/Act	綠燈亮：埠已經連線 綠燈閃爍：埠正在傳送/接收封包資料傳輸
WAN/LAN/DMZ: Speed (橘燈)	橘燈亮：乙太網路連線在 100Mbps 的速度 橘燈熄滅：乙太網路連線在 10Mbps 的速度
USB (綠燈)	綠燈亮：USB 設備可支援且已連接 綠燈閃爍：USB 設備正在傳送/接收封包資料傳輸 綠燈熄滅：USB 設備不被支援

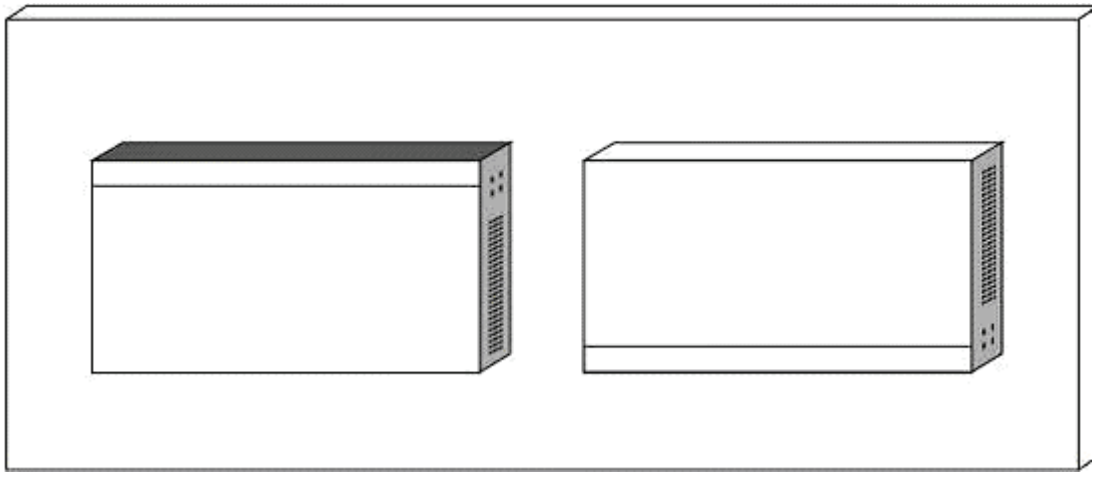
硬體恢復 (Reset) 按鍵

動作	意義
按住 Reset 按鈕 5 秒	熱開機，重新啓動路由器 DIAG 燈號：橘色燈號慢慢閃爍

按住 Reset 按鈕 10 秒以上	恢復原出廠預設值 DIAG 燈號：橘色燈號快閃

將路由器壁掛在牆上

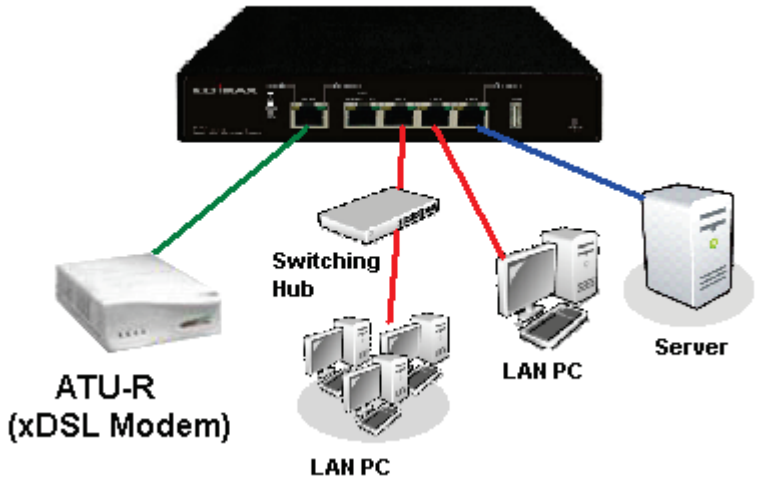
路由器底部有兩個壁掛槽。基於安全考量，請確認路由器在壁掛安裝時路由器的散熱孔方向如下圖所示。因不安全的壁掛方式而造成設備的損失，訊舟科技將不負責。



操作溫度需求

操作需求	操作溫度 0ºC to 40ºC (32ºF to 104ºF) 儲存溫度 0ºC to 70ºC (32ºF to 158ºF) 操作溼度 10% to 85% Non-Condensing 儲存溼度 5% to 90% Non-Condensing

3.2 將路由器連接至您的網路上



廣域網路連線：WAN 埠可以連接如 xDSL Modem 等接入互聯網。

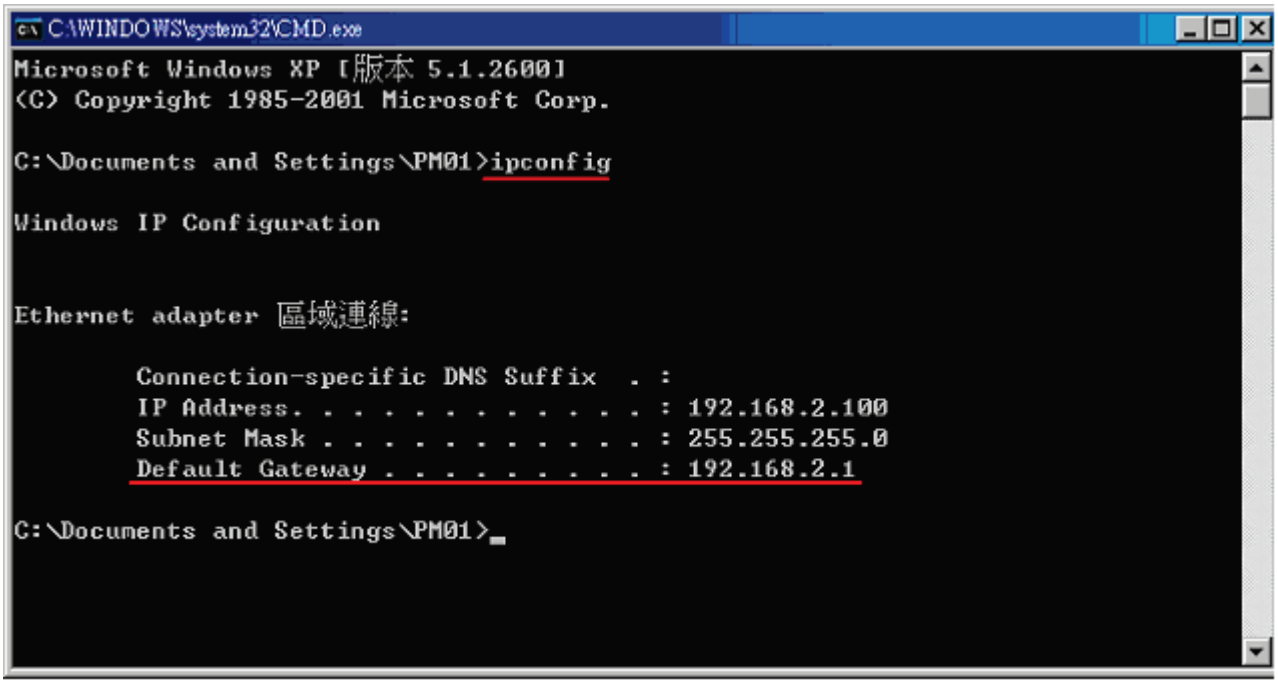
區域網路連線：LAN 埠可以連接如 Switch HUB 或是 PC 連線及內部伺服器。

DMZ 埠：此埠可以連接如 Switch HUB 或是具有外部合法 IP 位址的伺服器，如網頁伺服器以及電子郵件伺服器等。

IV. Login - 登入路由器

本章主要是在客戶連接好路由器後，通過連接路由器的電腦登錄路由器的 Web 管理頁。

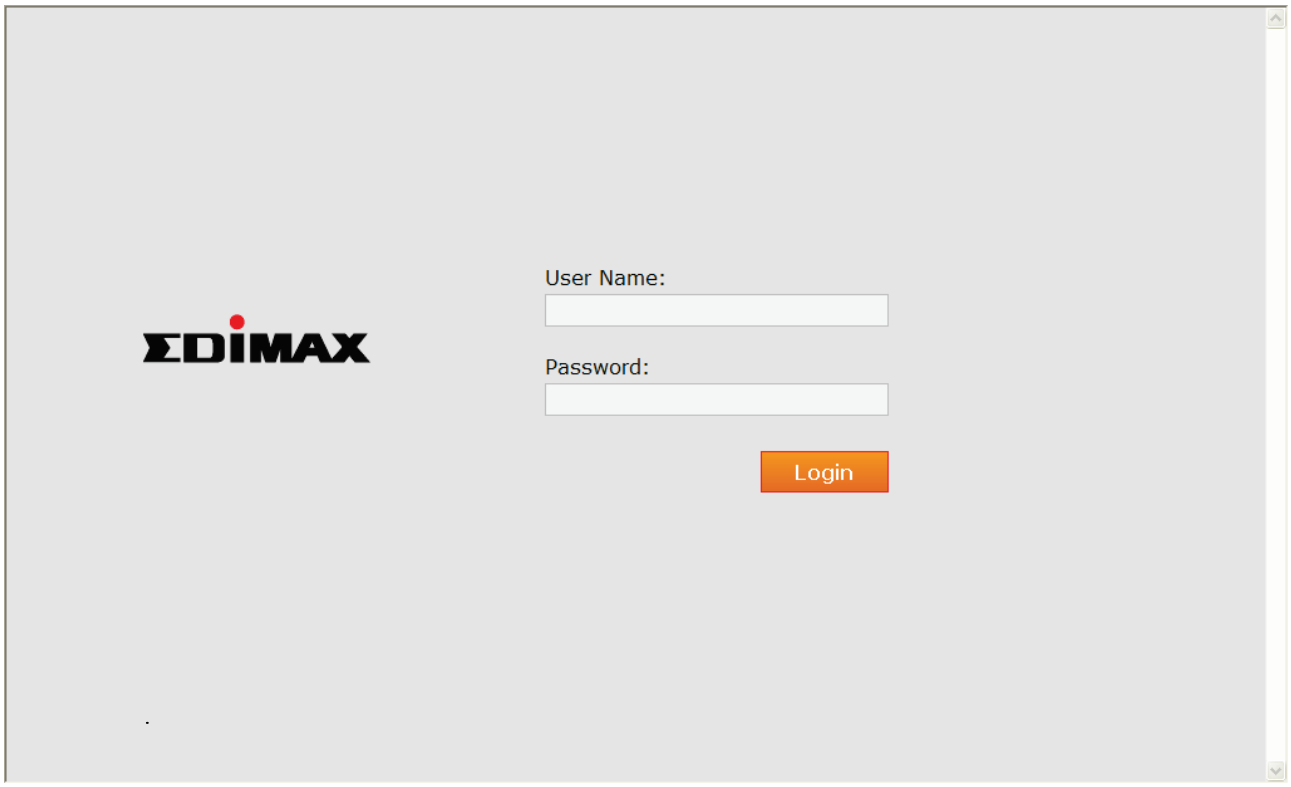
首先在連接到路由器 LAN 端的電腦（確定電腦是自動獲得 IP 地址）上的 DOS 下查找路由器的 IP 位址，點開始→運行，輸入 **cmd** 進入 DOS 操作，再輸入 **ipconfig**→確認，查到預設閘道（Default Gateway）地址如圖，**192.168.2.1**。確認預設閘道也就是路由器的預設 IP 地址。



注意！

當 “ipconfig” 不能獲得 IP 位址以及預設閘道的情況，或者獲得的 IP 地址爲 0.0.0.0 以及 169.X.X.X 的情況，就是路由器並沒有分配到 IP 地址，建議用戶檢查線路是否有問題，電腦網卡是否接好等。

然後開啓網頁流覽器 (如 IE)，在網址欄輸入 192.168.2.1 (路由器的預設閘道)，會出現以下的登錄視窗：



路由器預設的使用者名稱(User Name)爲"**admin**"，預設使用者密碼(Password)爲"**1234**"，您可以於稍後設定時更改此登錄密碼。

注意！

爲了安全，我們強烈建議您務必在登錄之後更改管理密碼！密碼請牢記，若是密碼忘記，將無法再登錄至路由器的設定視窗，必須點擊面板上的 Reset 按鍵十秒以上，恢復到出廠值，其所有配置將需要重新設定。

登錄後，就會顯示路由器的 Web 管理頁面。

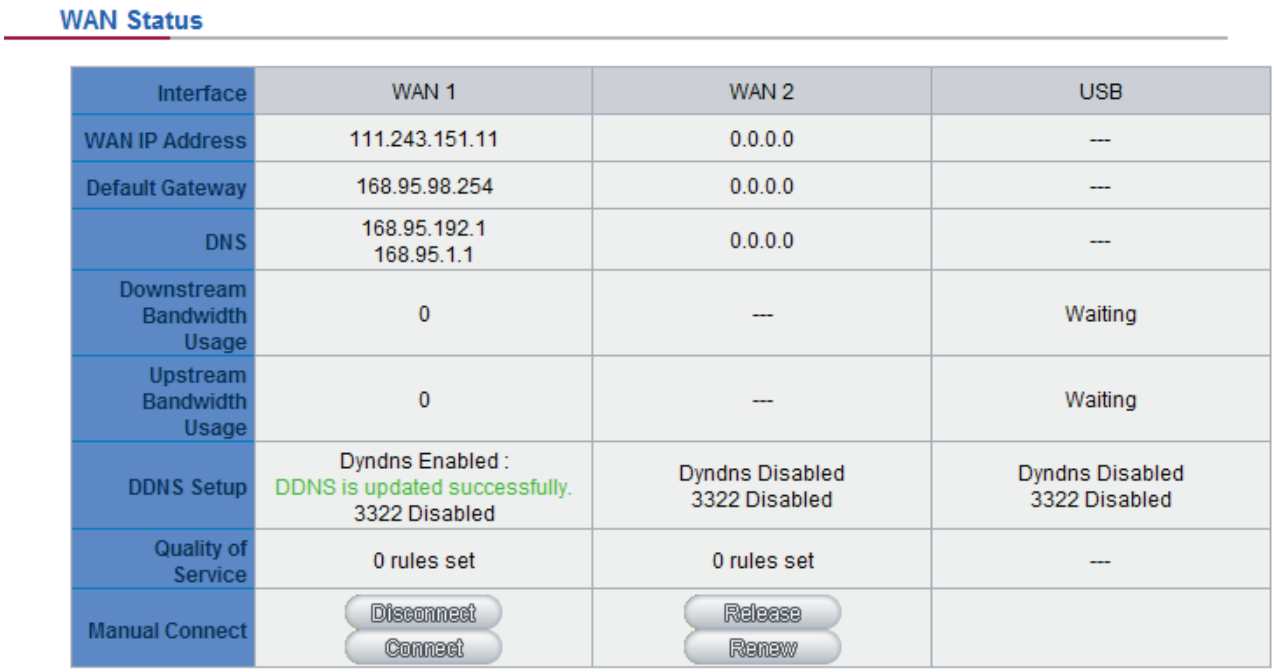
V. 確定設備規格、狀態顯示以及登錄密碼和時間的設定

本章介紹登錄軟體設定視窗後進入首頁可以瞭解到的設備規格以及設備工作狀態資訊，還有因安全考慮需要用戶即時修改登錄密碼與系統時間設定。

5.1 Home - 首頁顯示

首頁顯示安全路由器目前系統所有參數以及狀態顯示資訊。

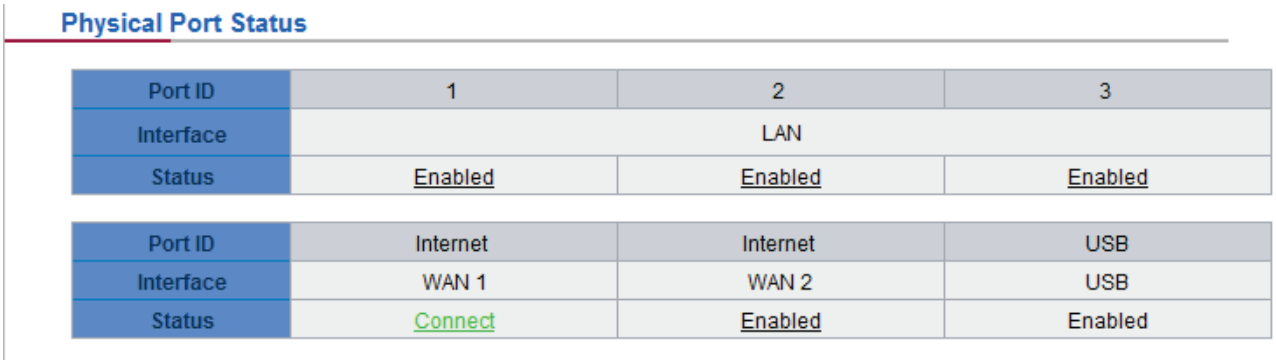
5.1.1 廣域網狀態



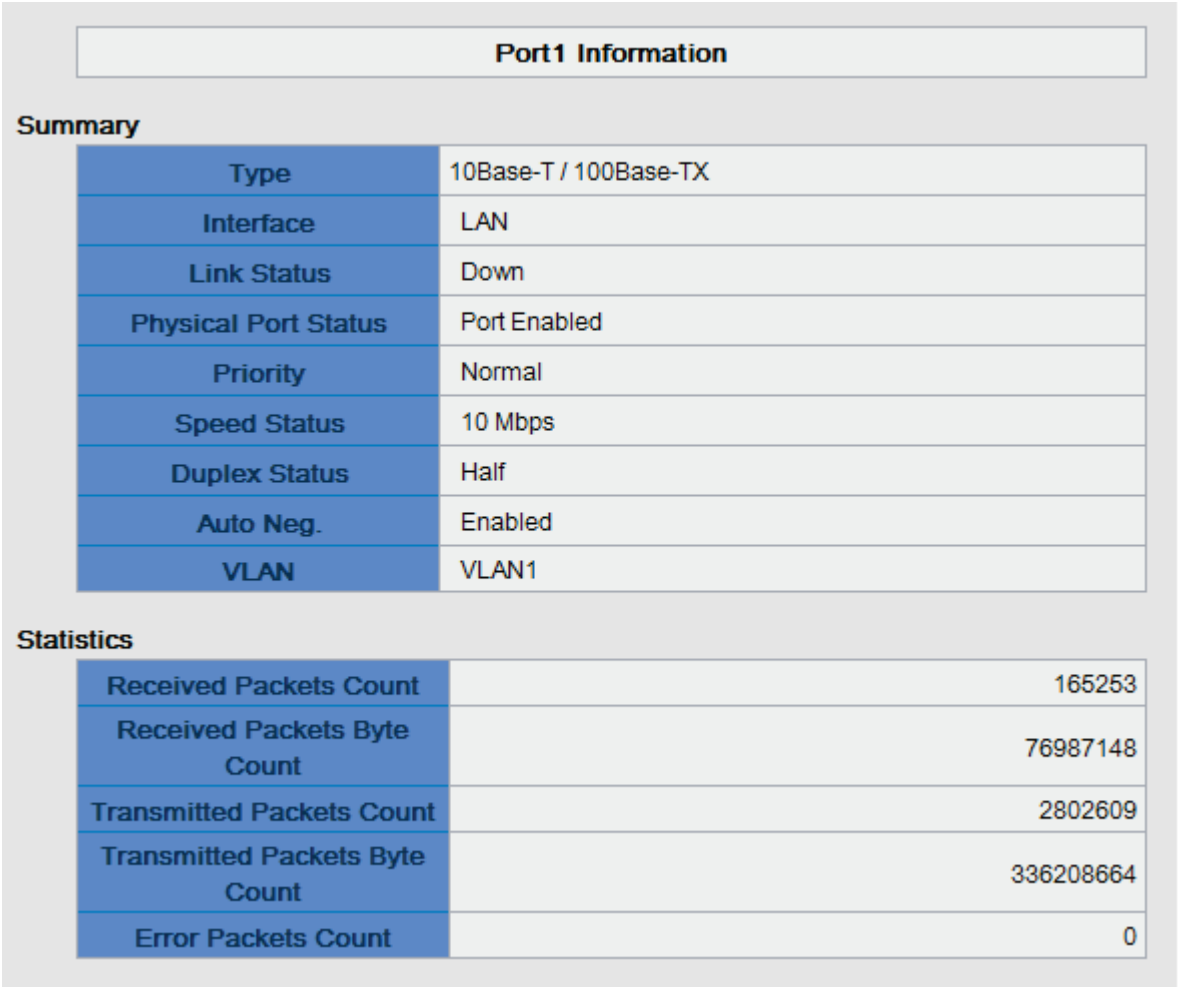
WAN IP Address (廣域網路 IP 位址)	此爲顯示路由器的 WAN 端目前的 IP 位址資訊。
Default Gateway (預設閘道)	此爲顯示 ISP 分配給路由器 WAN1、WAN2 的閘道 IP 位址資訊。
DNS (網域名稱伺服器)	此爲顯示路由器的 DNS 的 IP 位址資訊。
Downstream Bandwidth Usage (下載頻寬使用率)	此爲顯示路由器每個 WAN 目前的下載頻寬使用比例。
Upstream Bandwidth Usage	此爲顯示路由器每個 WAN 目前的上傳頻寬使用比例。

(上傳頻寬使用率)	
DDNS Setup (DDNS 設定)	此爲顯示路由器的 DDNS 是否啓動的狀態資訊。系統預設此功能爲關閉。
Quality of Service (網路品質服務配置)	此爲顯示路由器的網路品質服務(QoS)是否開啓。
Manual Connect (手動連線)	當使用者選擇自動取得 IP 位址時，他會顯示二個按鈕分別爲釋放與更新。使用者可以點擊釋放按鈕去做釋放 ISP 端所核發的 IP 位址，以及點擊更新按鈕去做更新 ISP 端所核發的 IP 位址。當選擇 WAN 端連線使用如 PPPoE 或是 PPTP 的話，它會變爲顯示“Connect”與“Disconnect”。
DMZ IP 位址	此爲顯示路由器 DMZ 目前的 IP 位址設定資訊。

5.1.2 Physical Port Status - 硬體埠狀態即時顯示



此視窗會顯示系統各埠目前即時狀態：(**Connect**-已經連接，**Enabled**-此埠處於開啓狀態，**Disabled**-此埠處於關閉狀態)。您可以點擊此狀態按鈕，在彈出的視窗中查看各埠更詳細的資料顯示。如下圖：



Port1 Information

Summary

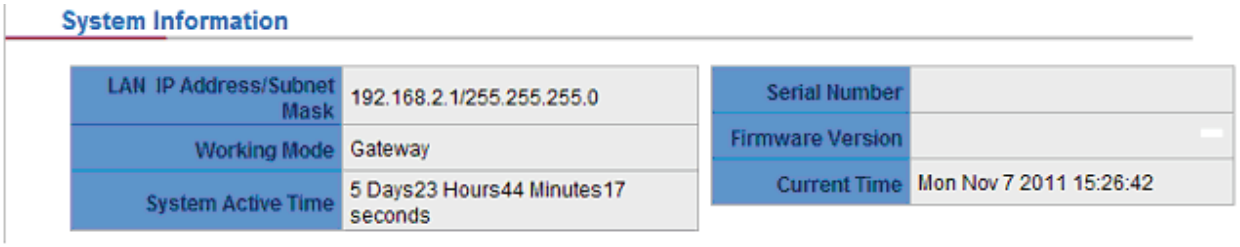
Type	10Base-T / 100Base-TX
Interface	LAN
Link Status	Down
Physical Port Status	Port Enabled
Priority	Normal
Speed Status	10 Mbps
Duplex Status	Half
Auto Neg.	Enabled
VLAN	VLAN1

Statistics

Received Packets Count	165253
Received Packets Byte Count	76987148
Transmitted Packets Count	2802609
Transmitted Packets Byte Count	336208664
Error Packets Count	0

此表會顯示目前該埠設定狀態，如網路連接狀態(10Base-T/100Base-TX)，界面位置(廣域網１～2/DMZ) (區域網１～2)，線路連接狀態(啓動/關閉)，埠配置狀態(埠啓動/埠關閉)，高低優先權(高級/一般)，網路連接速率(10Mbps/100Mbps)，工作模式(半雙工/全雙工)，乙太網自動偵測(啓動/關閉) 。 於此專案表格中，會顯示此埠的接收和傳送的封包數以及封包傳送 Byte 數及封包錯誤率等並計算總數量。

5.1.3 System Information - 系統資訊



System Information

LAN IP Address/Subnet Mask	192.168.2.1/255.255.255.0
Working Mode	Gateway
System Active Time	5 Days23 Hours44 Minutes17 seconds

Serial Number	
Firmware Version	
Current Time	Mon Nov 7 2011 15:26:42

LAN IP/Subnet Mask：此爲顯示路由器本身的 LAN 端目前 IP 位址，系統預設爲 192.168.2.1。

Working Mode：此爲顯示路由器的目前工作模式(可爲 Gateway 模式(NAT)或是 Router 模式)。系統預設此功能爲 NAT Gateway 模式。

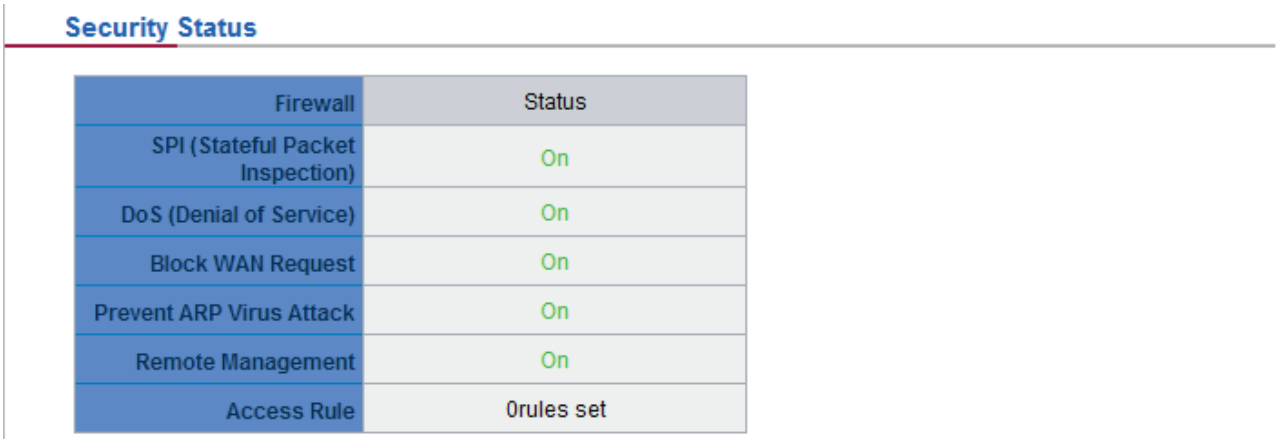
System Active Time：此爲顯示路由器目前已經開機的時間。

Serial Number：此爲顯示路由器的產品序號。

Firmware Version：顯示目前使用的韌體版本。

Current Time：此顯示路由器目前正確時間，但必須注意，您需要正確設定與遠端 NTP 伺服器的時間同步後才會正確顯示。

5.1.4 Security Status - 網路安全資訊



SPI (Stateful Packet Inspection)：SPI 封包狀態偵測，此爲顯示路由器的 SPI 封包偵測過濾防火牆功能選項是否啓動(On/Off 啓動/關閉)。系統預設此功能爲”On”啓動。

DoS (Denial of Service)：防止 DoS 攻擊，此爲顯示路由器的阻斷來自網路上的 DoS 攻擊功能選項是否開啓(On/Off 啓動/關閉)。系統預設此功能爲”On”啓動。

Block WAN Request：不回應廣域網路端請求，此爲顯示路由器的阻斷來自網路上

的 ICMP-Ping 的回應功能選項是否啓動(On/Off 啓動/關閉)。系統預設此功能爲”On”啓動。

Prevent ARP Virus Attack：防止 ARP 攻擊，此爲顯示路由器防止 ARP 攻擊的功能選項是否啓動(On/Off 啓動/關閉)。系統預設此功能爲”Off”關閉。

Remote Management: 遠距管理，此爲顯示路由器的遠端管理功能選項是否啓動(On/Off 啓動/關閉)。系統預設此功能爲”Off”關閉。

Access Rule：訪問規則設定，此爲顯示路由器的訪問規則設置的數目。

5.1.5 VPN Status - VPN 虛擬私有網狀態

顯示可支援及使用中的隧道數量。

VPN Status

IPSec VPN Setting	Status
Tunnel(s) Used	0
Tunnel(s) Available	20

5.1.6 Log Setting Status - 日誌記錄配置狀態顯示

Log

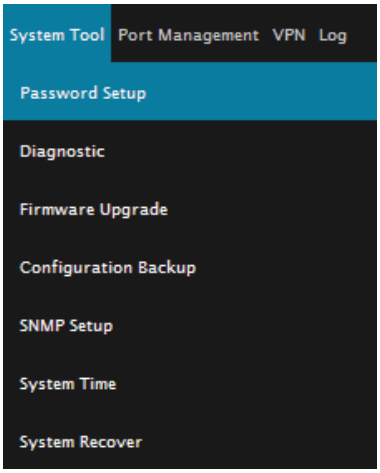
Send Log To	Disabled

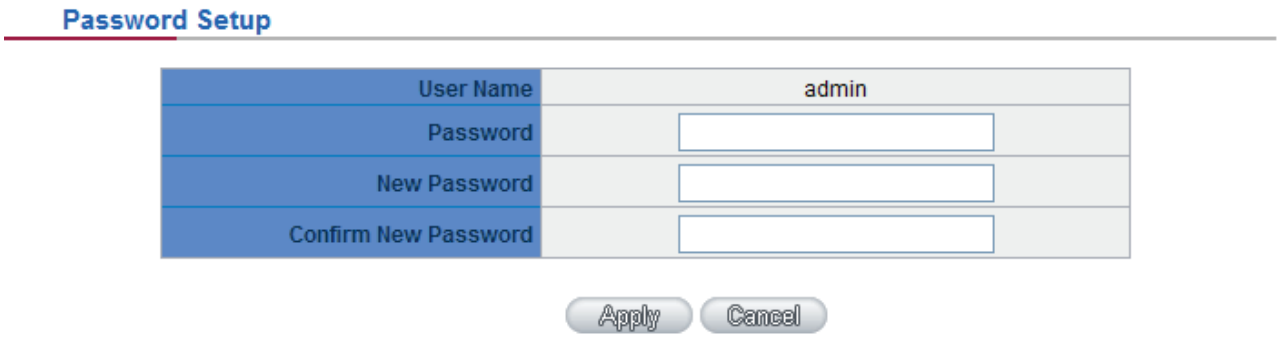
Send Log to **傳送日誌到**	此爲顯示您所設定路由器的日誌記錄接收的伺服器。

5.2 登錄密碼及時間的修改和設定

5.2.1 Password Setup – 密碼設定

當您每次登錄安全路由器的設定視窗時，必須輸入密碼。安全路由器的用戶名和密碼出廠值爲“admin / 1234”。考慮安全因素，我們強烈建議您務必在第一次登錄並完成設定之後更改管理密碼！密碼請牢記，若是密碼忘記，將無法再登錄路由器的設定窗口，必須點擊路由器前面板上的 Reset 按鍵十秒以上，恢復到出廠值，所有設定值將需要重新設定。





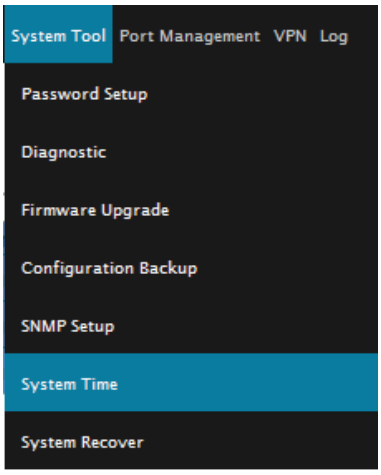
User Name **使用者名稱**	出廠初始值預設爲 admin。
Old Password **舊密碼**	填寫原本舊密碼（出廠初始值預設爲“1234”）。
New User Name **新使用者名稱**	輸入新用戶名

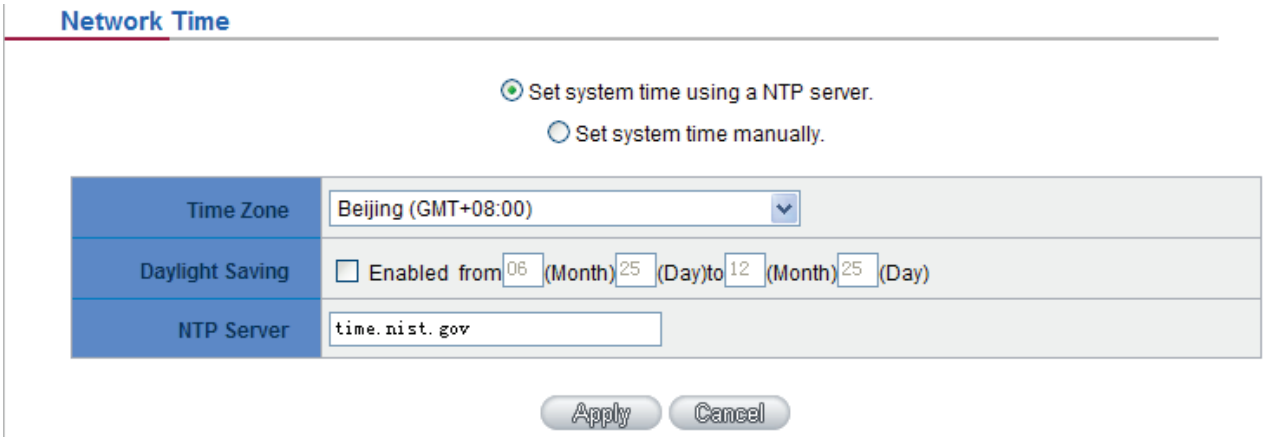
New Password **新密碼**	填寫新密碼。
Confirm New Password **確認新密碼**	再次輸入新密碼。
Apply **確認**	點擊此按鈕“Apply”儲存剛才所修改設定的內容參數。
Cancel **取消**	點擊此按鈕“Cancel”清除剛才所修改設定的內容參數，此操作必須於“確定” 儲存動作之前才會有效。

5.2.2 Time - 系統時間設定

路由器可以設定時間，讓您在查看路由器的系統紀錄或設置網路存取的時間設定時，可以瞭解事件發生的正確時間，以及作爲關閉存取或是開放存取網路資源的依據條件。您可以選擇與路由器內建的外部時間伺服器(NTP 伺服器)取得時間同步，或自己設定正確時間參數。

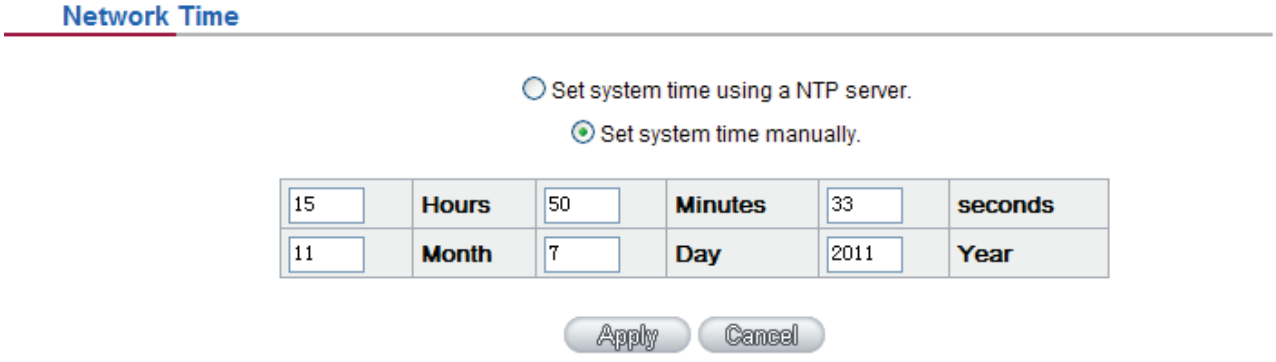
Set system time using a NTP server：開啓與外部時間服務器同步，路由器有內建的網路時間伺服器，會自動同步時間。





Time Zone **時區選擇**	點開下拉功能表選擇您所在地點的時區以正確顯示當地時間。
Daylight Saving **日光節約時間**	若是您所的地區有實施日光節約時間，可以輸入實施的日期範圍，路由器會在此日期範圍自動調整時間。
NTP Server **時間伺服器位址**	若是您自己有偏愛使用的時間伺服器，可以輸入該伺服器的位址。
Apply **確認**	點擊此按鈕即會儲存剛才所變動的修改設定內容參數。
Cancel **取消**	點擊此按鈕即會清除剛才所變動的修改設定內容參數，此操作必須於確認儲存動作之前才會有效。

Select the Local Time Manually: 手動配置時間，在這輸入正確的時間：小時、分鐘、秒、月份、日與年份。

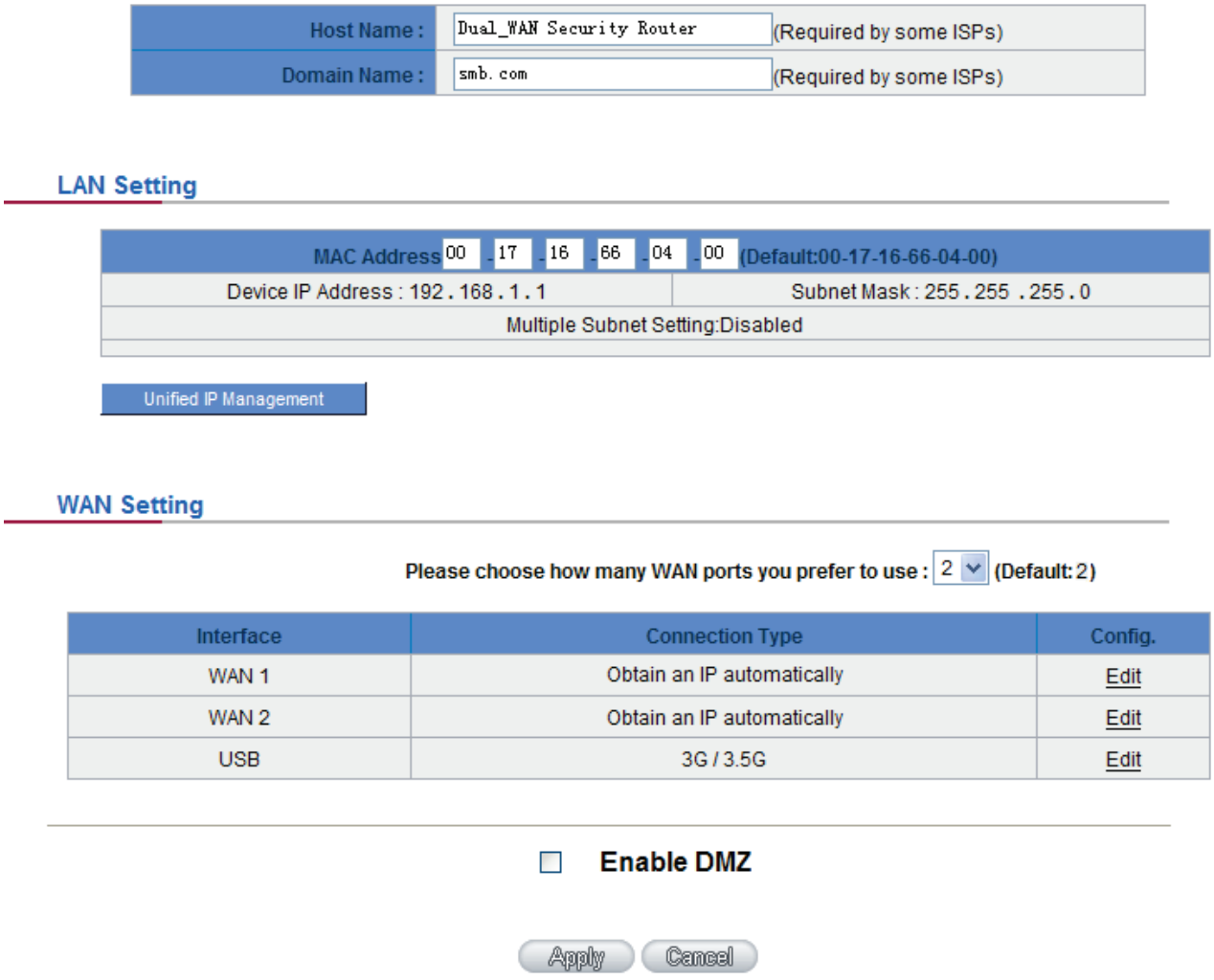


點擊“**Apply**”按鈕即會儲存剛才所修改的設定內容參數，點擊此按鈕“**Cancel**”即會清除剛才所修改的設定內容參數，此操作必須於確認儲存動作之前才會有效。

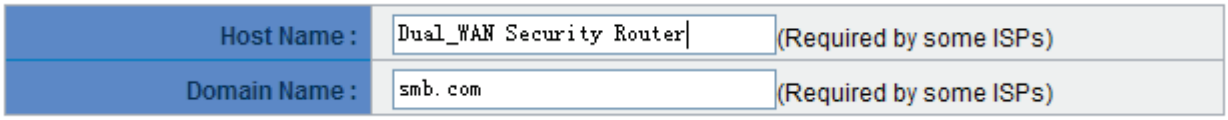
VI. Network – 網路設定

本章節講述基本的網路設置，對大多數的用戶來說，通過本章節完成基本的設定已經足夠連接網路。網路的連接需要一些 ISP 所提供的進一步詳細資訊。其詳細項目設定，請參考以下各節說明：

6.1 Network Connection – 網路連線



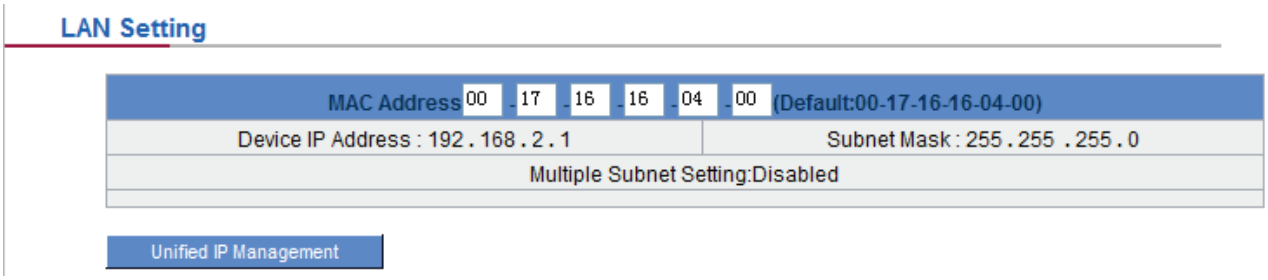
6.1.1 Host Name and Domain Name – 主機名稱及網域名稱



可輸入路由器的名稱（主機名稱）以及網域名稱，此設定在大多數環境中不需要做任何設定即可使用，除非特殊 ISP 需求！

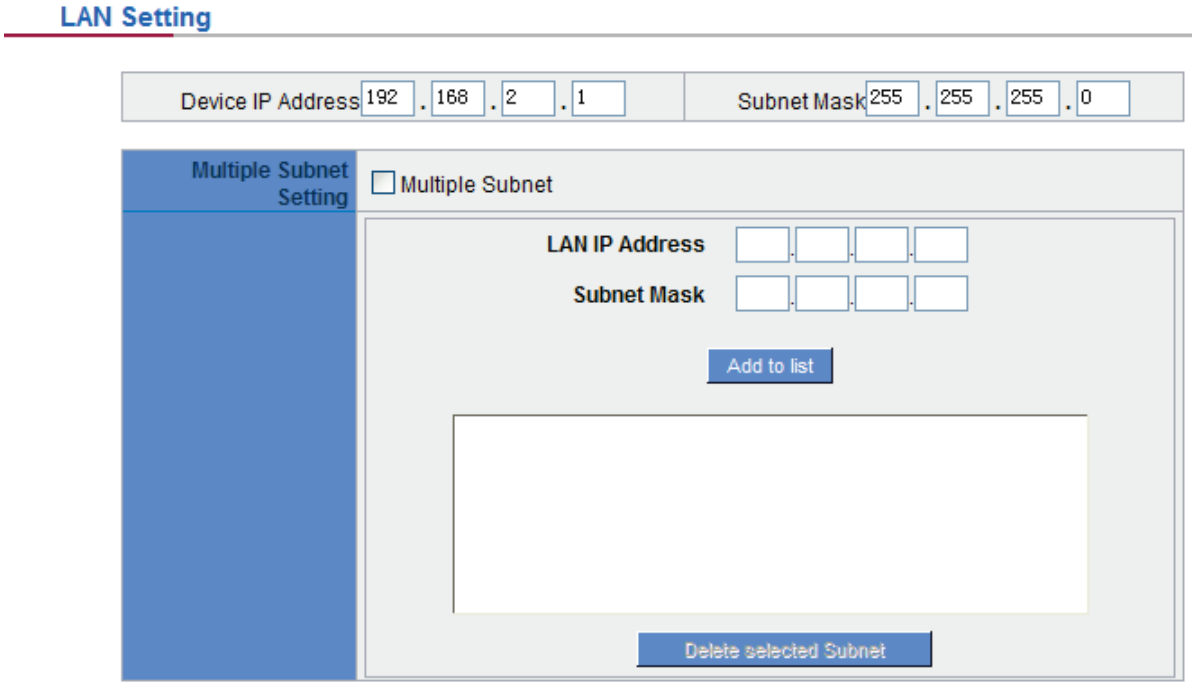
6.1.2 LAN Setting – 區域網路設定

系統預設 LAN IP 爲 192.168.2.1，子網路遮罩爲 255.255.255.0，您可以依照實際網路架構做變動。



Multiple-Subnet Setting - 多子網配置

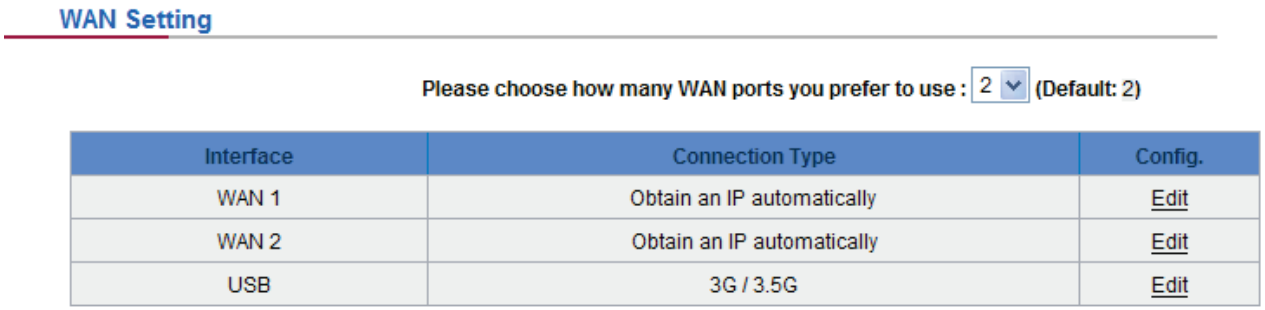
勾選 “**Unified IP Management**” 進入設定頁面，如下圖所示. 輸入想要增加的 IP 及子網路遮罩。



此功能是將不同于路由器區域網段的其他網段 IP 加入到路由器認可的區域網段中，這樣區域網中的 PC 若是已經設定的 IP 所在的網段不同于路由器的區域網段也可以直接上網。舉例來說，原來內部環境已經有多組不同的 IP 網段，例如 192.168.3.0， 192.168.20.0，192.168.150.0 等等，將這些網段加入到子網中，則這些網段的內部電腦不需做任何修改就可以上網，這裏可以依照您的實際網路架構運作。

6.1.3 WAN & DMZ Settings - 廣域網路 WAN 及非軍事區設定

WAN Setting - 廣域網設定



Interface: 廣域網連線所在 WAN 界面位置。

Connection Type: 此項顯示該廣域網口目前設定的連線狀態。安全路由器提供五種連線狀態設定：自動取得 IP 地址；指定 IP 地址；PPPoE 撥號連線；PPTP 撥號連線；以及透通

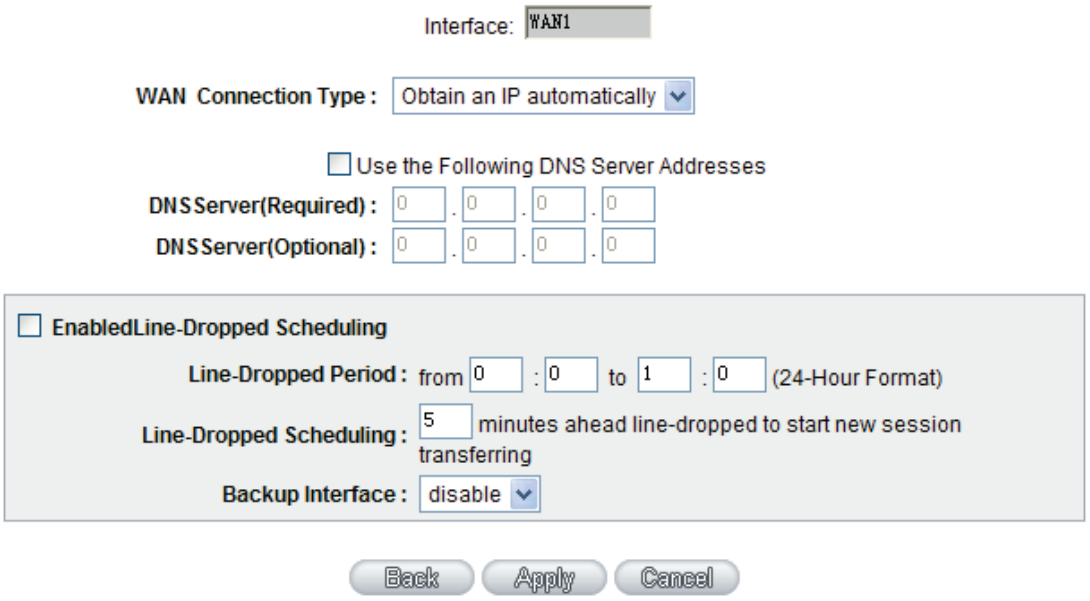
橋接模式。

Config.: 點擊“**Edit**”按鈕可以進入廣域網連線狀態的設置視窗。各類型的連線狀態設定請參考以下的說明，並選擇配合 ISP 所給您的連線狀態來做設置。

Obtain an Automatic IP automatically – 自動取得 IP 地址

此爲路由器系統預設的連線方式，此連線方式爲 DHCP 用戶端自動取得 IP 模式，多爲應用於如線纜數據機或是 DHCP 用戶端連線狀態等連接，若您的連線爲其他不同的方式，請選取相關的設定並參考以下的介紹做設置。

在自動取得 IP 模式，您可以使用自定 DNS 的 IP 位址，勾選此選項並填入您要使用的 DNS 伺服器 IP 位址。



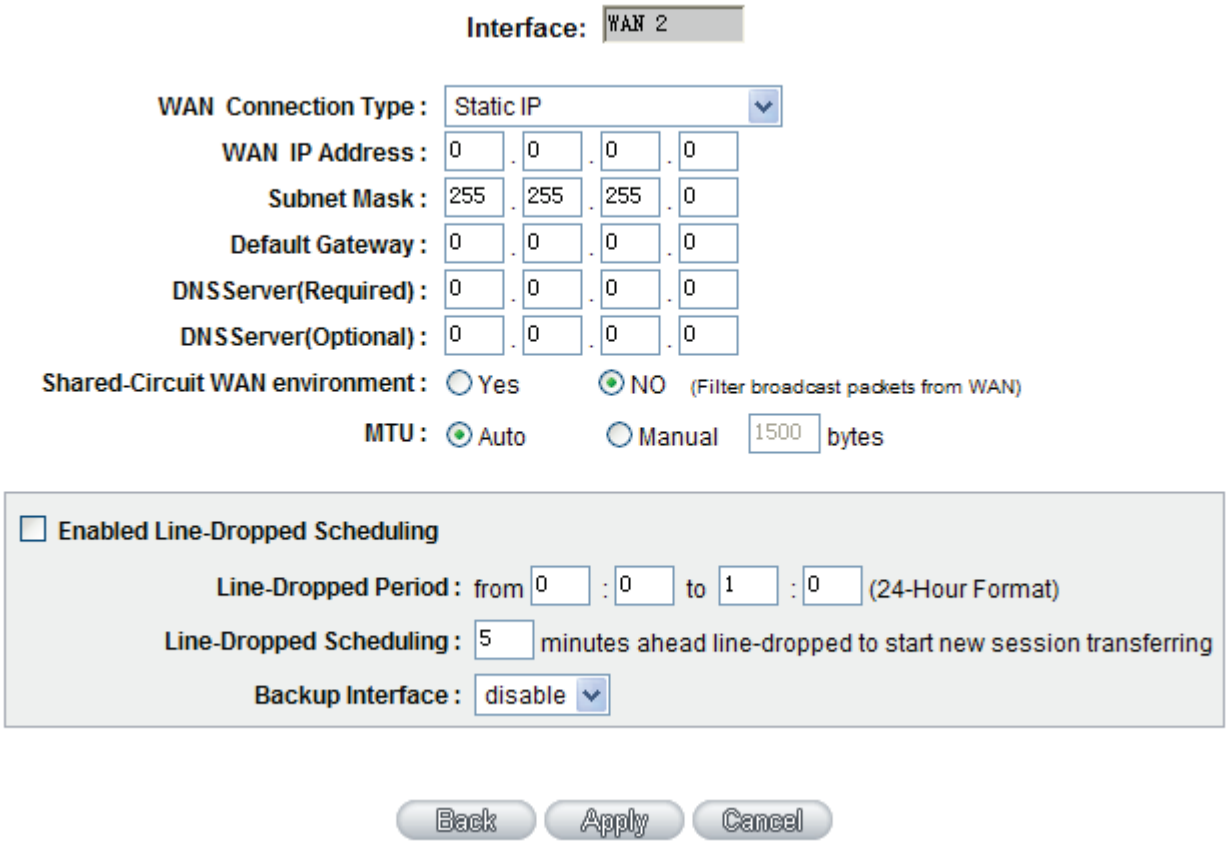
Use the following DNS Server Addresses	選擇使用自定的 DNS 伺服器 IP 地址。
DNS Server：	輸入您的 ISP 所提供的網域名稱解析伺服器 IP 位址，最少填入一組，最多可填二組。 選擇”是”可防止收到來自其他廣域網的廣播封包。

Enable Line-Dropped Scheduling：	勾選此功能會啓用廣域網中斷連線排程的機制。在某些區域，廣域網的連線服務會有時間的限制，例如從凌晨 12：00 到清晨 6：00 之間六個小時，光纖連線服務會中斷。雖然路由器有備援機制，此操作當此廣域網斷線的瞬間，所有經由該廣域網對外訪問的連線也會因此中斷，重新連接時，才會經由備援機制走其他廣域網出去。因此，爲了避免在廣域網斷線的瞬間大量的連線被切斷，您可以啓用此機制在此廣域網斷線前一段時間，先將新增的連線經由其他廣域網出去外網訪問，可以減少此廣域網斷線時的衝擊。
Line-Dropped Period：	輸入此廣域網中斷連接服務的規則時間。
Line-Dropped Scheduling：	輸入您希望在此廣域網中斷連接服務之前多長時間開始將新增的連線經由其他廣域網出去外網訪問。
Backup Interface：	若是此廣域網有設定通訊埠綁定，請選擇要由哪一個廣域網口做備援。通常您應該選擇與此廣域網同一個 ISP 連線的廣域網口。

點擊“**Apply**”按鈕即會儲存剛才所修改的設定內容參數，點擊此按鈕“**Cancel**”即會清除剛才所修改的設定內容參數，此操作必須於確認儲存動作之前才會有效。

Static IP – 固定 IP

若您的 ISP 有核發固定的 IP 地址給您，請您選擇此種方式連線，將 ISP 所核發的 IP 資訊分別參照以下介紹填入相關設定參數中。



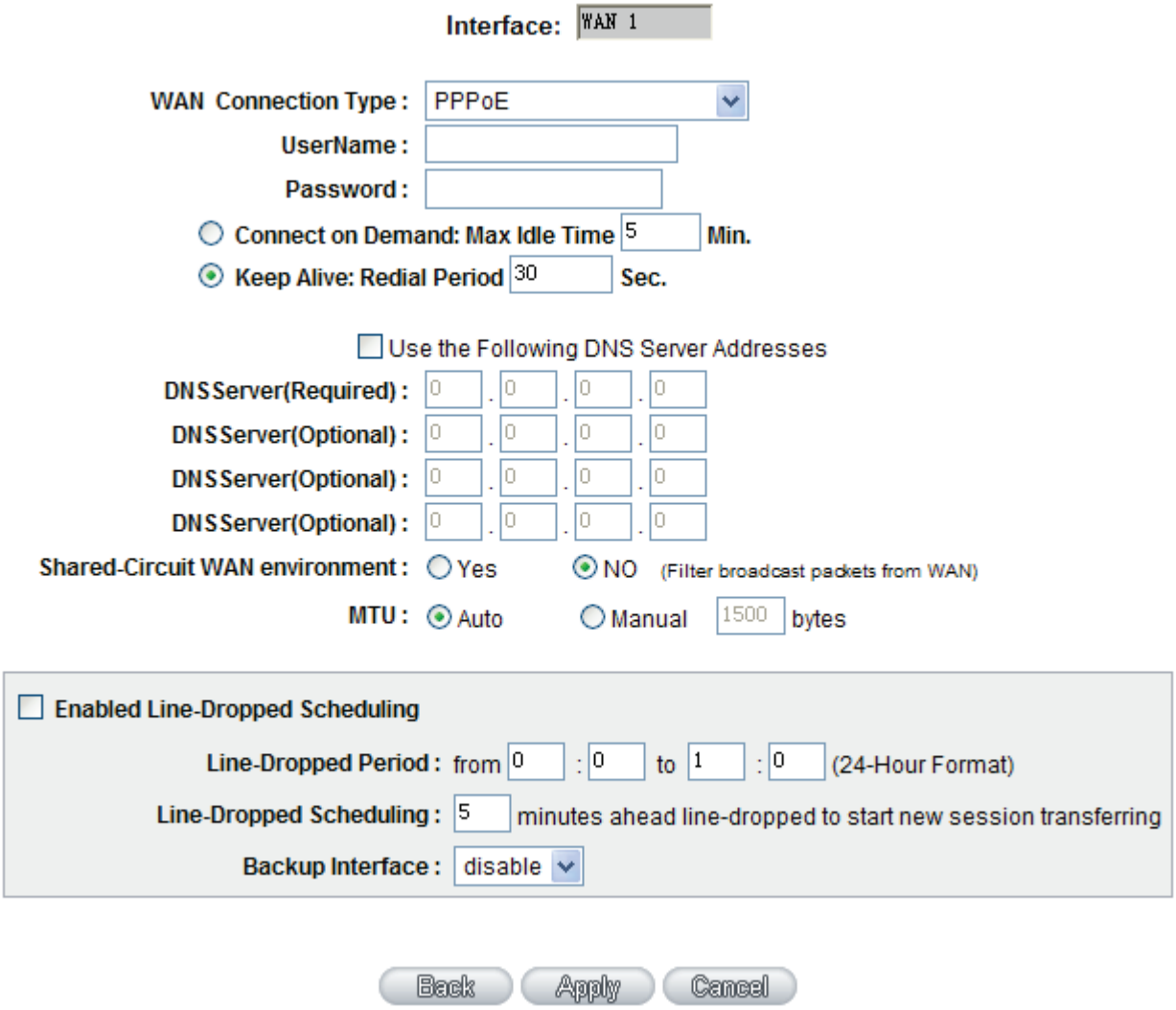
WAN IP address	輸入您的 ISP 所核發的可使用固定 IP 位址的其中一個。
Subnet Mask	輸入您的 ISP 所核發的可使用固定 IP 位址的子網路遮罩，如： 發放 8 個固定 IP 地址：255.255.255.248 發放 16 個固定 IP 地址：255.255.255.240
Default Gateway	輸入您的 ISP 所核發的可使用固定 IP 位址的預設閘道，若您是使用 ADSL 的話，一般說來都是 ADSL 資料機（ATU-R）的 IP 位址。
DNS Server	輸入您的 ISP 所規定的名稱解析伺服器 IP 地址，最少填入一組，最多可填二組。 選擇"是"可防止收到來自其他廣域網的廣播封包。

Enable Line-Dropped Scheduling	勾選此功能會啓用廣域網中斷連線排程的機制。在某些區域，廣域網的連線服務會有時間的限制，例如從凌晨 12：00 到清晨 6：00 之間六個小時，光纖連線服務會中斷。雖然路由器有備援機制，此操作當此廣域網斷線的瞬間，所有經由該廣域網對外訪問的連線也會因此中斷，重新連接時，才會經由備援機制走其他廣域網出去。因此，爲了避免在廣域網斷線的瞬間大量的連線被切斷，您可以啓用此機制在此廣域網斷線前一段時間，先將新增的連線經由其他廣域網出去外網訪問，可以減少此廣域網斷線時的衝擊。
Line-Dropped Period	輸入此廣域網中斷連接服務的規則時間。
Line-Dropped Scheduling	輸入您希望在此廣域網中斷連接服務之前多長時間開始將新增的連線經由其他廣域網出去外網訪問。
Backup Interface	若是此廣域網有設定通訊埠綁定，請選擇要由哪一個廣域網口做備援。通常您應該選擇與此廣域網同一個 ISP 連線的廣域網口。

點擊“**Apply**”按鈕即會儲存剛才所修改的設定內容參數，點擊此按鈕“**Cancel**”即會清除剛才所修改的設定內容參數，此操作必須於確認儲存動作之前才會有效。

PPPoE

此項爲 ADSL 虛擬撥號使用(適用於 ADSL PPPoE)，填入 ISP 給予的使用者連線名稱與密碼並以路由器內建的 PPP Over Ethernet 軟體連線，若是您的 PC 之前已經有安裝由 ISP 所給予的 PPPoE 撥號軟體的話，請將其移除，不需要再使用此個別連接網路。



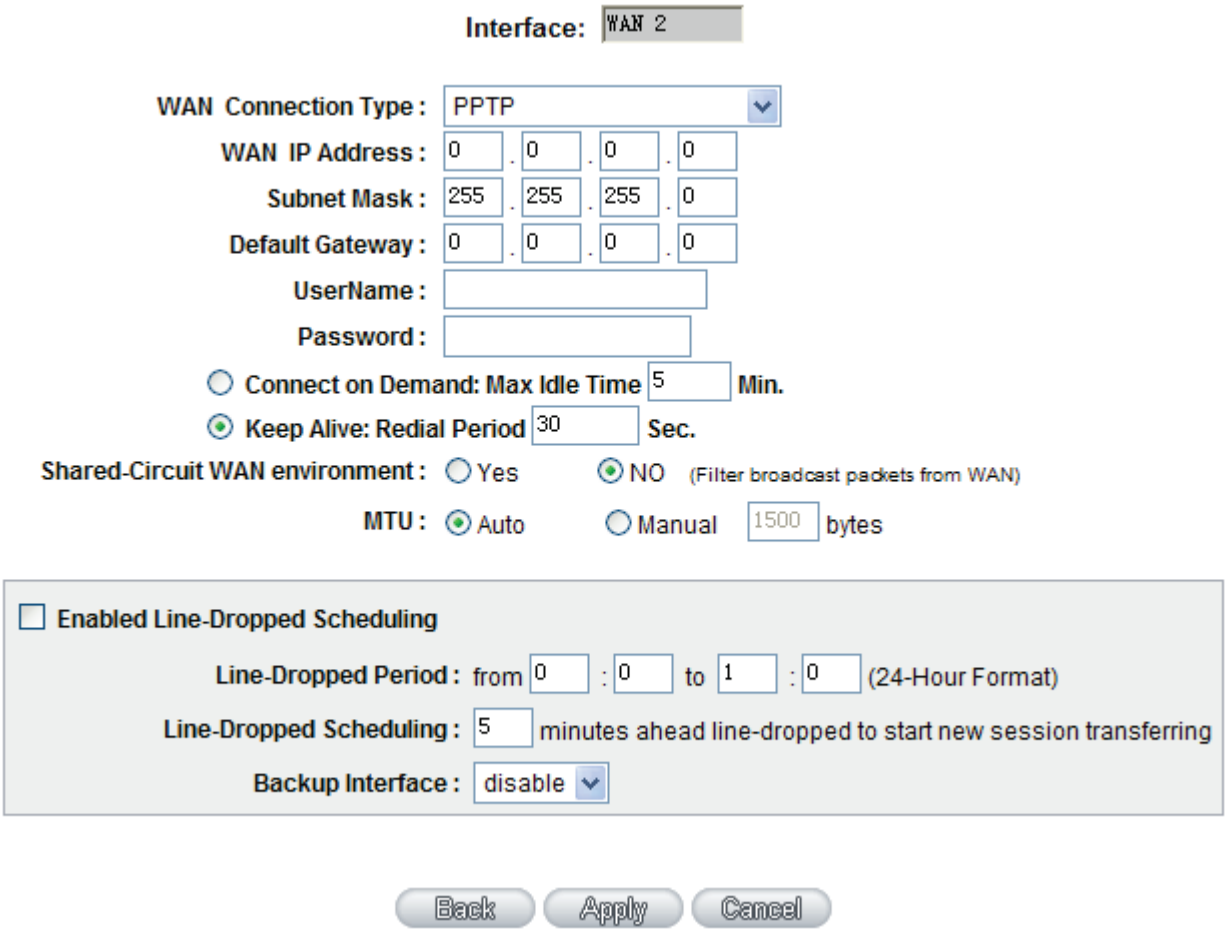
User Name	輸入您的 ISP 所核發的使用者名稱。
Password	輸入您的 ISP 所核發的使用密碼。
Connect on Demand	此功能讓路由器可自動啓動 PPPoE 撥號功能。當用戶端欲連至網際網路時，路由器會自動進行撥號。當流量已閒置一段時間後，系統會自動斷線。(系統預設五分鐘沒有封包傳輸後進行斷線)
Keep Alive	此功能能夠讓您的 PPPoE 撥接連線能夠斷線自動重撥，您可以自行設定重新撥接的時間，預設值爲 30 秒。
DNS Server	輸入您的 ISP 所規定的名稱解析伺服器 IP 地址，最少填入一組，最多可填二組。 選擇"Yes"可防止收到來自其他廣域網的廣播封包。

Enable Line-Dropped Scheduling	勾選此功能會啓用廣域網中斷連線排程的機制。在某些區域，廣域網的連線服務會有時間的限制，例如從凌晨 12：00 到清晨 6：00 之間六個小時，光纖連線服務會中斷。雖然路由器有備援機制，此操作當此廣域網斷線的瞬間，所有經由該廣域網對外訪問的連線也會因此中斷，重新連接時，才會經由備援機制走其他廣域網出去。因此，爲了避免在廣域網斷線的瞬間大量的連線被切斷，您可以啓用此機制在此廣域網斷線前一段時間，先將新增的連線經由其他廣域網出去外網訪問，可以減少此廣域網斷線時的衝擊。
Line-Dropped Period	輸入此廣域網中斷連接服務的規則時間。
Line-Dropped Scheduling	輸入您希望在此廣域網中斷連接服務之前多長時間開始將新增的連線經由其他廣域網出去外網訪問。
Backup Interface	若是此廣域網有設定通訊埠綁定，請選擇要由哪一個廣域網口做備援。通常您應該選擇與此廣域網同一個 ISP 連線的廣域網口。

點擊“**Apply**”按鈕即會儲存剛才所修改的設定內容參數，點擊此按鈕“**Cancel**”即會清除剛才所修改的設定內容參數，此操作必須於確認儲存動作之前才會有效。

PPTP

此項爲 PPTP (Point to Point Tunneling Protocol) 計時制使用，填入 ISP 給予的使用者連線名稱與密碼並以路由器內建的 PPTP 軟體連線。



WAN IP Address	輸入您的 ISP 所核發的可使用固定 IP 位址的其中一個。
Subnet Mask	輸入您的 ISP 所核發的可使用固定 IP 位址的子網路遮罩。
Default Gateway	輸入您的 ISP 所核發的可使用固定 IP 位址的預設閘道，若您是使用 ADSL 的話，一般說來都是 ATU-R 的 IP 位址。
User Name	輸入您的 ISP 所核發的使用者名稱。
Password	輸入您的 ISP 所核發的使用密碼。
Connect on Demand	此功能能夠讓您的 PPTP 撥接連線能夠使用自動撥號功能，當使用端若是有上網需求時，路由器會自動向預設的 ISP 自動撥號連線，當網路一段時間閒置無使用時，則系統會自動離線。無封包傳送的自動離線時間預設為 5 分鐘，您可以自行輸入所需要的自動離線等待時間。
Keep Alive	此功能能夠讓您的 PPTP 撥接連線能夠斷線自動重撥，而且可以自行設定重新撥接的時間，預設值為 30 秒。

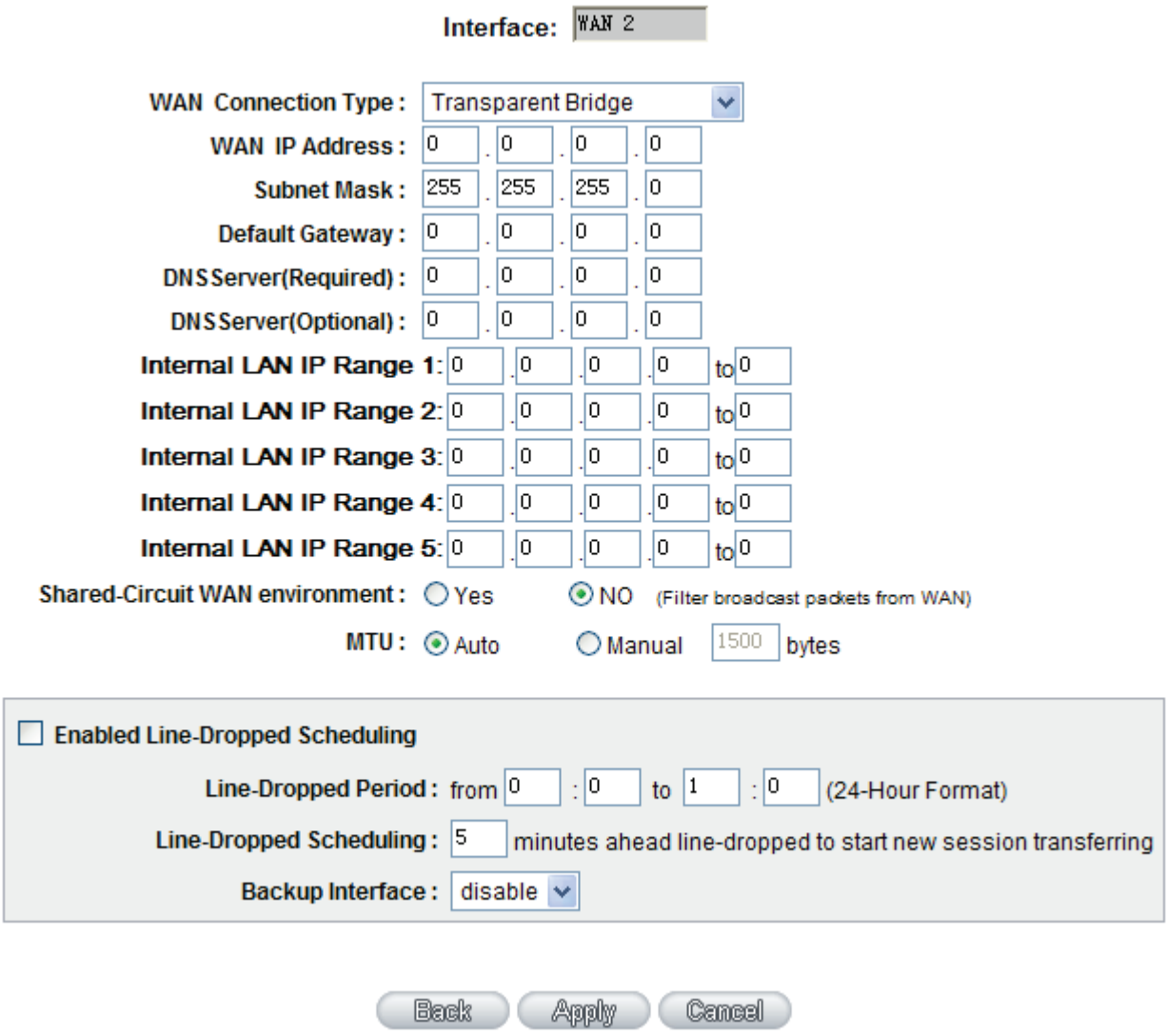
Enable Line-Dropped Scheduling	勾選此功能會啓用廣域網中斷連線排程的機制。在某些區域，廣域網的連線服務會有時間的限制，例如從凌晨 12：00 到清晨 6：00 之間六個小時，光纖連線服務會中斷。雖然路由器有備援機制，此操作當此廣域網斷線的瞬間，所有經由該廣域網對外訪問的連線也會因此中斷，重新連接時，才會經由備援機制走其他廣域網出去。因此，爲了避免在廣域網斷線的瞬間大量的連線被切斷，您可以啓用此機制在此廣域網斷線前一段時間，先將新增的連線經由其他廣域網出去外網訪問，可以減少此廣域網斷線時的衝擊。
Line-Dropped Period	輸入此廣域網中斷連接服務的規則時間。
Line-Dropped Scheduling	輸入您希望在此廣域網中斷連接服務之前多長時間開始將新增的連線經由其他廣域網出去外網訪問。
Backup Interface	若是此廣域網有設定通訊埠綁定，請選擇要由哪一個廣域網口做備援。通常您應該選擇與此廣域網同一個 ISP 連線的廣域網口。

點擊“**Apply**”按鈕即會儲存剛才所修改的設定內容參數，點擊此按鈕“**Cancel**”即會清除剛才所修改的設定內容參數，此操作必須於確認儲存動作之前才會有效。

Transparent Bridge – 透通橋接模式

當您內網的電腦 IP 已經都是公網 IP 而不希望將內網都改成私網 IP(例如 192.168.2.X)時，此功能可以讓您不需更動原有架構，立即整合到既有網路中。選擇廣域網連線方式爲透通橋接模式，這樣您可以保留內網電腦的 IP 設定爲原本的公網 IP 仍然可以正常上網。

當您設定兩個廣域網時，廣域網的連線模式選擇此種透明橋接模式，還是可以做到負載均衡。



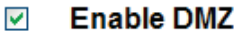
WAN IP Address	輸入您的 ISP 所核發的可使用固定 IP 位址的其中一個。
Subnet Mask	輸入您的 ISP 所核發的可使用固定 IP 位址的子網路遮罩，如：255.255.255.240
Default Gateway Address	輸入您的 ISP 所核發的可使用固定 IP 位址的預設閘道，若您是使用 ADSL 的話，一般說來都是 ATU-R 的 IP 位址。
DNS Server	輸入您的 ISP 所規定的名稱解析伺服器 IP 地址，最少填入一組，最多可填二組。

Internal LAN IP Range	輸入您的 ISP 所核發的可使用固定 IP 範圍。若是您的 ISP 分給您兩個不連續的 IP 位址範圍，您可以分別填入“內部 IP 位址 1 ~ 5”。
Enable Line-Dropped Scheduling	勾選此功能會啓用廣域網中斷連線排程的機制。在某些區域，廣域網的連線服務會有時間的限制，例如從凌晨 12：00 到清晨 6：00 之間六個小時，光纖連線服務會中斷。雖然路由器有備援機制，此操作當此廣域網斷線的瞬間，所有經由該廣域網對外訪問的連線也會因此中斷，重新連接時，才會經由備援機制走其他廣域網出去。因此，爲了避免在廣域網斷線的瞬間大量的連線被切斷，您可以啓用此機制在此廣域網斷線前一段時間，先將新增的連線經由其他廣域網出去外網訪問，可以減少此廣域網斷線時的衝擊。
Line-Dropped Period	輸入此廣域網中斷連接服務的規則時間。
Line-Dropped Scheduling	輸入您希望在此廣域網中斷連接服務之前多長時間開始將新增的連線經由其他廣域網出去外網訪問。
Backup Interface	若是此廣域網有設定通訊埠綁定，請選擇要由哪一個廣域網口做備援。通常您應該選擇與此廣域網同一個 ISP 連線的廣域網口。

點擊“**Apply**”按鈕即會儲存剛才所修改的設定內容參數，點擊此按鈕“**Cancel**”即會清除剛才所修改的設定內容參數，此操作必須於確認儲存動作之前才會有效。

DMZ Setting – 非軍事區

對於某些網路環境應用來說，可能會需要用到獨立的 DMZ 非軍事管制區界面來置放對外服務伺服器，如 WWW 網頁伺服器與 Mail 電子郵件伺服器等等。安全路由器提供您獨立的 DMZ 界面來設定連接有合法 IP 位址的伺服器。此 DMZ 界面是從網路或區域網存取對外伺服器內容的溝通橋樑。



DMZ Setting

Interface	IP Address	Config.
DMZ	0.0.0.0	Edit

IP address: 此項顯示您給予 DMZ 埠的 IP 地址或範圍。

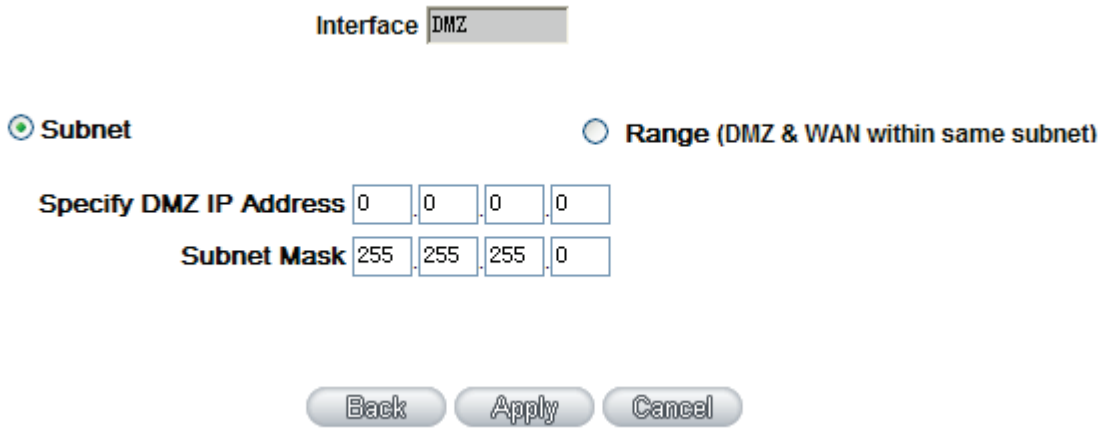
Config.: 點擊“Edit”按鈕可以進入 DMZ 的設置視窗。請參考以下的設定說明。

此 DMZ 的設定可分爲 Subnet、Range 兩種:

Subnet：

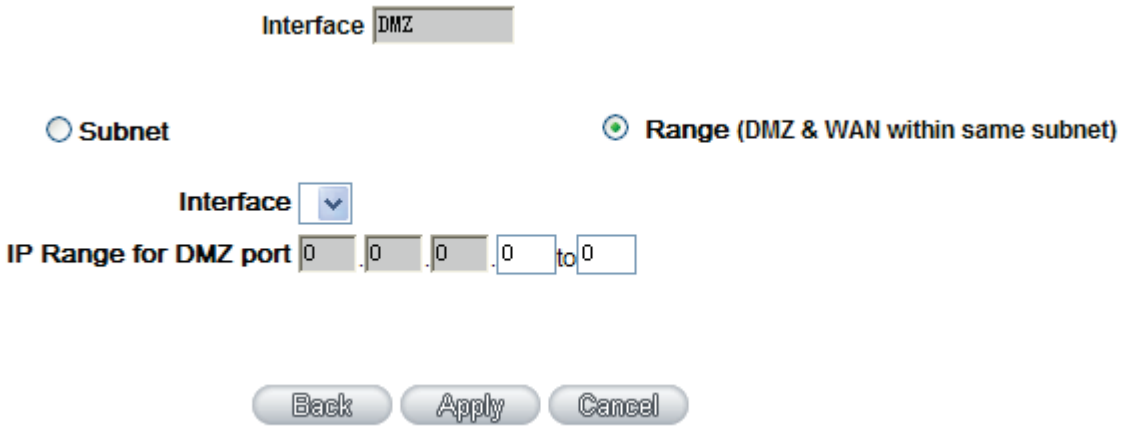
DMZ 與廣域網路 WAN 要在不同的子網路 Subnet 中。

就是若ISP端分配給您16個合法IP如:220.243.230.1-16/子網路遮罩:255.255.255.240時，您必須將此 16 個 IP 再切兩組變成 220.243.230.1-8 /子網路遮罩：255.255.255.248 及另一組 220.243.230.9-16/子網路遮罩：255.255.255.248，然後路由器及閘道是在同一組，再將另一組設定在 DMZ 中。



Range：

DMZ 與廣域網路 WAN IP 地址在相同的子網路 Subnet。

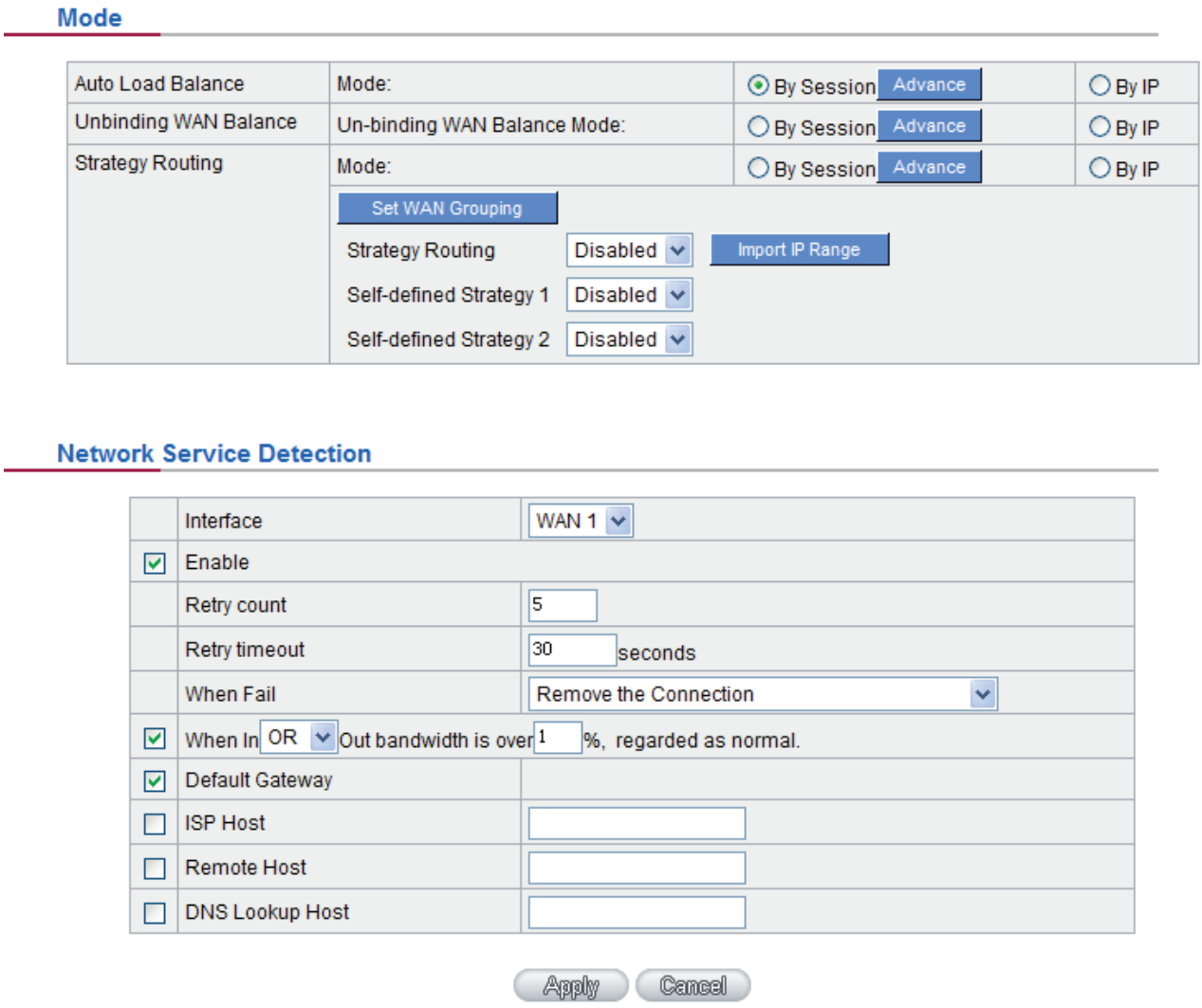


IP Range: 輸入在 DMZ 埠的 IP 範圍。

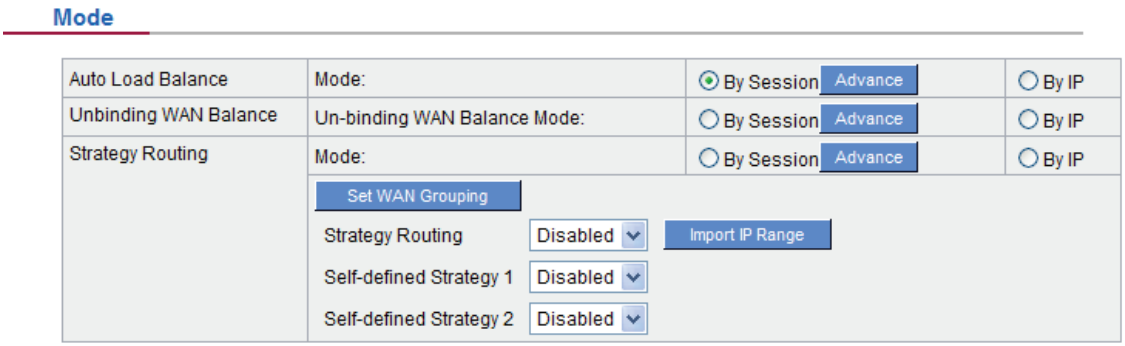
點擊“**Apply**”按鈕即會儲存剛才所修改的設定內容參數，點擊此按鈕“**Cancel**”即會清除剛才所修改的設定內容參數，此操作必須於確認儲存動作之前才會有效。

6.2 Dual-WAN Setting – 雙 WAN 設定

當用戶的連線是採用雙 WAN 的線路設計，管理人員可以進入網路連線配置流量管理以及協定綁定(Protocol Binding)項目對路由器的負載均衡模式(Load Balance)等進行配置，使路由器達到最優資料轉發、網路頻寬效能達到最高。



6.2.1 Load Balance Mode – 負載均衡模式



Auto Load Balance Mode – 智能負載均衡模式

當您選用智能負載均衡模式，路由器將以連線數或是 IP 連線數爲基礎，並依據您廣域網線路的頻寬來自動分配連線，達到對外連線的負載均衡。線路的頻寬是依據您所填入的頻寬設定(請參考下一小節設定說明)，例如當兩條廣域網都爲上行 512Kbit/sec 時，其自動負載比例爲 1:1，當一條線路的上行頻寬爲 1024kbit/sec 另一條爲 512kbit/sec 時，則此自動負載比例爲 2:1，所以爲了確保您的路由器達到實際線路負載能夠均衡，請填入實際上行下載頻寬。

- **By Session (連線數均衡)**：當您選用連線數均衡模式，路由器將以連線數爲基礎，並依據您廣域網線路的頻寬來自動分配連線，達到連線的負載均衡。
- **By IP (IP 均衡)**：當您選用 IP 負載均衡模式，路由器將以連線的 IP 數爲基礎，並依據您廣域網線路的頻寬來自動分配連線，達到連線的負載均衡。

提示！

不論是連線數均衡或是 IP 負載均衡方式，搭配“通訊協定綁定”可以有更彈性運用您的頻寬，您可將特定的內網 IP，使用特定應用服務埠作訪問，或特定的目的地 IP 經由您指定的廣域網來訪問外網。

譬如您希望指定 IP 192.168.2.100 訪問外網的時候走廣域網 1，或內網所有 IP 去訪問服務埠 80 時都是經過廣域網 2，或是內網所有 IP 去目的地 IP 211.1.1.1 訪問時要從廣域網 1 去訪問等等，都可以經由設定此“通訊協定綁定”功能來達到您的需求。請注意，當使用智慧負載均衡方式搭配“通訊協定綁定”功能時，除了您指定的訪問會按照您的規則出去訪問外網，其他未被指定的 IP 或服務埠的訪問還是按照路由器的機制做智慧負載均衡。

關於如何設定“通訊協定綁定”功能，以及智慧負載均衡方式搭配“通訊協定綁定”的範例，請參考 （6.2.3 節的 **Configuring Protocol Binding** 設定說明）。

Un-Binding WAN Balance Mode – 未綁定介面均衡模式

若是有部分廣網埠並沒有被指定，例如廣域網 2 並沒有指定特定的 IP、服務埠、或目的 IP 來使用，這些廣域網埠仍然會依據路由器的負載均衡機制來分配連線。均衡機制如下：

- **連機數均衡**：當您選用連線數均衡模式，路由器將以連線數爲基礎，並依據您廣域網線路的頻寬來自動分配連線，達到連線的負載均衡。
- **IP 均衡**：當您選用 IP 負載均衡模式，路由器將以連線的 IP 數爲基礎，並依據您廣域網線路的頻寬來自動分配連線，達到連線的負載均衡。

提示！

此指定路由必須配合“通訊協定綁定”功能才能發揮作用。例如指定讓內網去訪問服務埠 80 時都要從廣域網 1 去訪問，或內網去目的地 IP 211.1.1.1 訪問時要從廣域網 1 去訪問等等，必須要在“通訊協定綁定”功能中做設定。要注意，當使用指定路由(Specify WAN Binding)模式，以上述的例子來看，除了您指定的訪問必須按照您的規則出去訪問外網都走廣域網 1 以外，其他未被指定的 IP 或服務埠則經由路由器負載均衡的機制使用其他的廣域網出去。

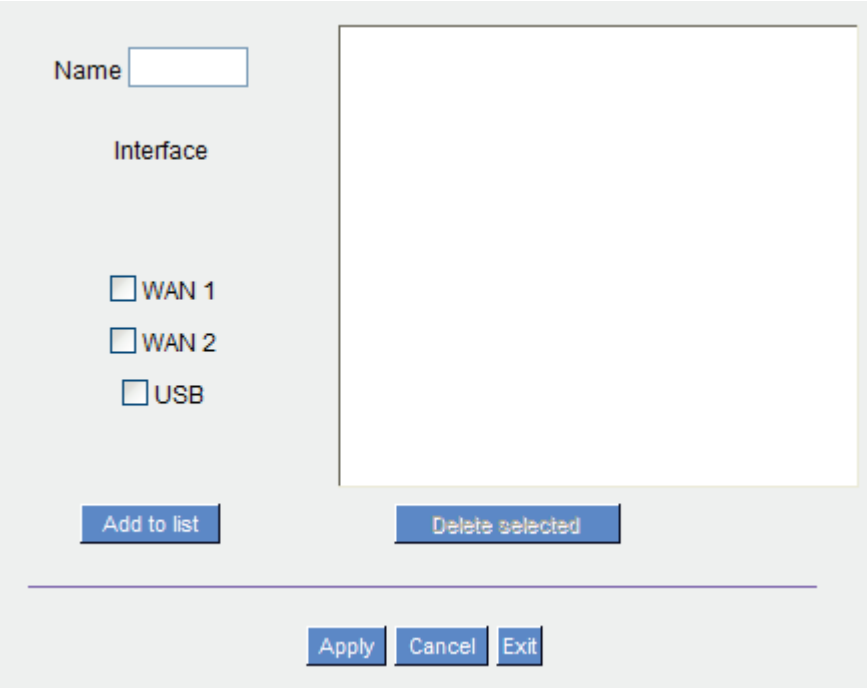
關於如何設定“通訊協定綁定”功能，以及指定路由模式搭配“通訊協定綁定”的範例，請參考（6.2.3 節的 **Configuring Protocol Binding** 說明）。

Strategy Routing Mode – 策略路由

當您選用策略路由模式，路由器會依照內建的策略(電信網通分流，用在中國大陸的環境)自動分配連線。您只需選擇網通線路接入的廣域網口(或廣域網組合)，路由器會自動將該走網通線路去外網訪問的流量都從網通的廣域網出去，對該走電信線路去外網訪問的流量也都會往電信的廣域網出去，達到“電信走電信，網通走網通”的分流策略。

Set WAN Grouping: -廣域網組合：

當您所接的網通線路不只一條，則需要做廣域網的組合，以便將兩個以上的廣域網口合在一起做相同的策略分流。點擊“廣域網組合”會彈出以下的對話視窗。

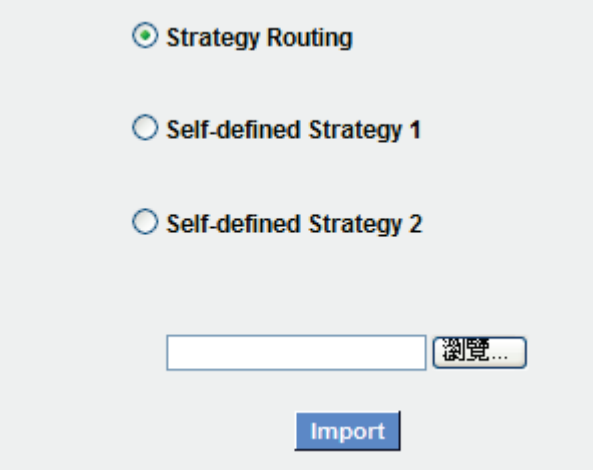


Name **名稱**	在此自定的廣域網組合名稱，如“Education”等，用來辨識廣域網群組。
Interface **介面**	在此勾選要設在此組合的廣域網口。
Add To List **加入清單**	增加到廣域網組合列表。
Delete selected **刪除選擇項目**	刪除所選擇的廣域網組合內容。
Apply **確認**	點擊此按鈕“**確認**”即會儲存剛才所變動的修改設定內容參數。
Cancel **取消**	點擊此按鈕“取消”即會清除剛才所變動的修改設定內容參數，此操作必須於確認儲存動作之前才會有效。

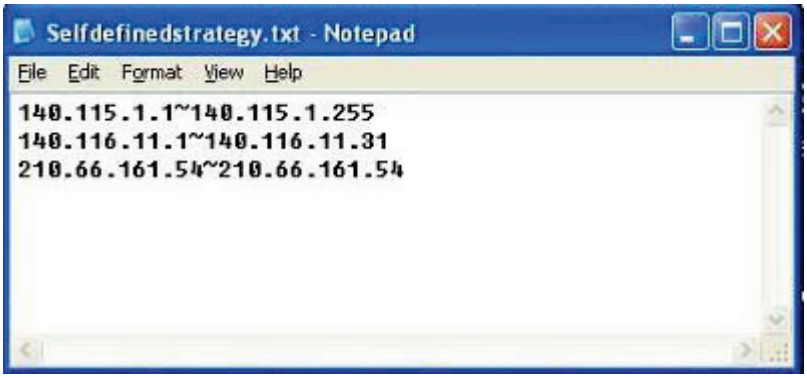
設定完成後，您就可以在網通策略的選擇中選取您的網通界面的廣域網組合。

Import Strategy – 匯入策略

此外，您也可以自己建立分流策略。在“Import Strategy”中選擇要指定的廣域網口或廣域網組合(例如廣域網 1)，然後點擊“Import IP Range”的按鍵，會出現匯入策略檔的對話視窗。策略檔是一個可編輯的文字檔案，應含有您指定的目的 IP 位址。將檔匯入路徑選擇好之後，點擊“import”，並在設定窗口的最下方點擊“Apply”，路由器就會將要往指定目的 IP 的流量從您指定的廣域網(例如廣域網 1)或廣域網組合出去。



策略檔的建立可以用純文本編輯軟體來撰寫，例如使用 Windows 系統內建的 “記事本” 來建立。將您要指定的目的 IP 位址按照下圖的格式寫入，例如您要指定的目的 IP 位址範圍是從 140.115.1.1 到 140.115.1.255，則在“記事本”中輸入 140.115.1.1～140.115.1.255。下一個目的 IP 位址範圍則要換行輸入。**請注意！**若是只有一個目的 IP 位址，也需要以同樣的格式來書寫。例如指定的目的 IP 位址是 210.66.161.54，則必須寫成 210.66.161.54～210.66.161.54 格式。儲存檔後(副檔名應該是.txt)即可匯入自定策略的更新網段。

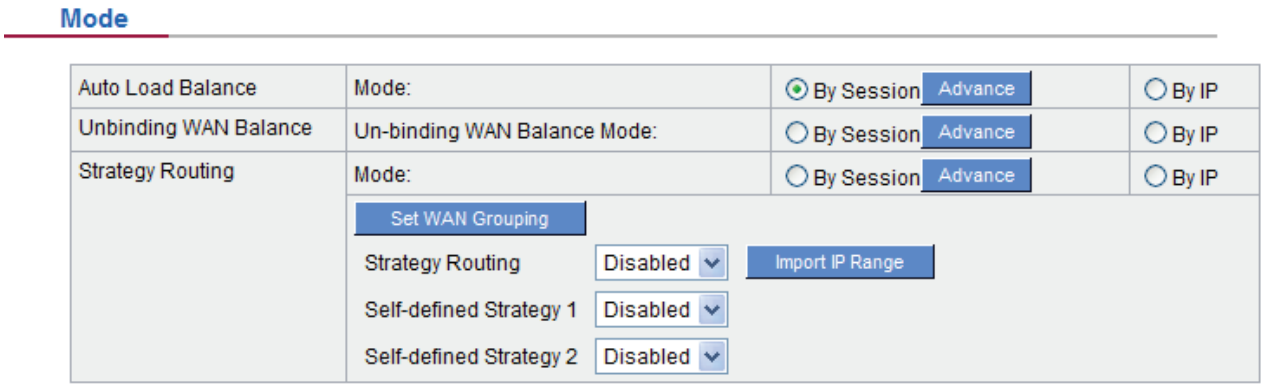


Session Balance Advanced Function – 連機數均衡進階設定

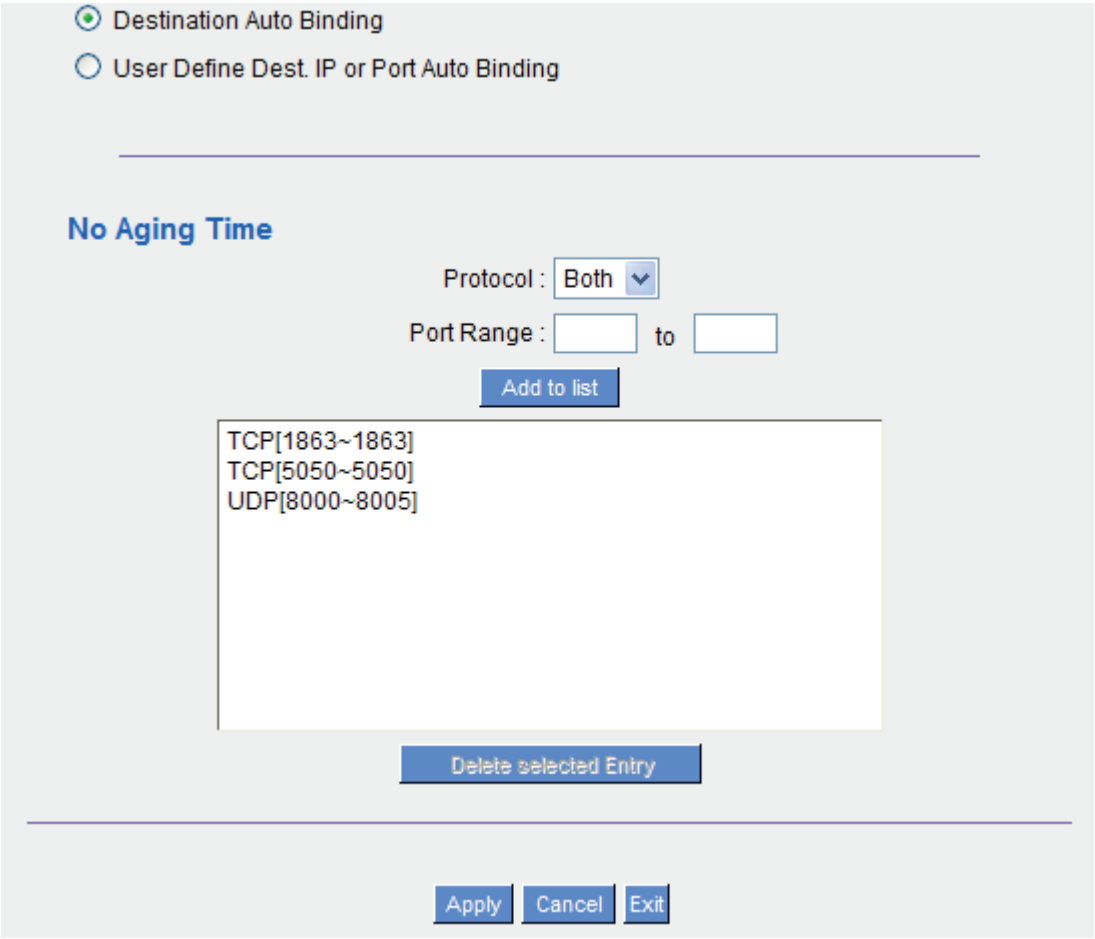
一般連機數均衡是平均與隨機分配每個內網 IP 的連線數量，但是某些較特殊的連線例如網路銀行的加密連線 (Https、TCP443) 需要固定從同一個 WAN IP 建立才能夠正常操作，所以當同一個內網 IP 訪問網路銀行網站，訪問操作動作被連線數均衡機制分配到不同 WAN IP 去建立連線時，有可能就會在操作過程中發生斷線或不正常的狀況，而連線平衡的進階設定功能就是用來解決這個問題。

進階設定可以設定同一個內網 IP，在以某個特殊的服務通訊埠建立連線時，固定從某一個 WAN IP 去建立，其他類型的服務通訊埠連線仍然照原來的平衡機制隨機平均分配，除了可達成原來連線數平衡所帶來的效用之外，也可確定一些較特殊的服務通訊埠連線時能正常

運作。



點選“**Advanced**”進入設定選單



Destination Auto Binding
目的地聯機登入自動綁定

選擇此選項表示到目的地 IP 位址位於同一個 Class B 範圍子網時，就固定從同一個 WAN IP 建立連線。

舉例來說，總共兩個 WAN1 200.10.10.1 與 WAN2 200.10.10.2，內網兩個 IP 192.168.1.100

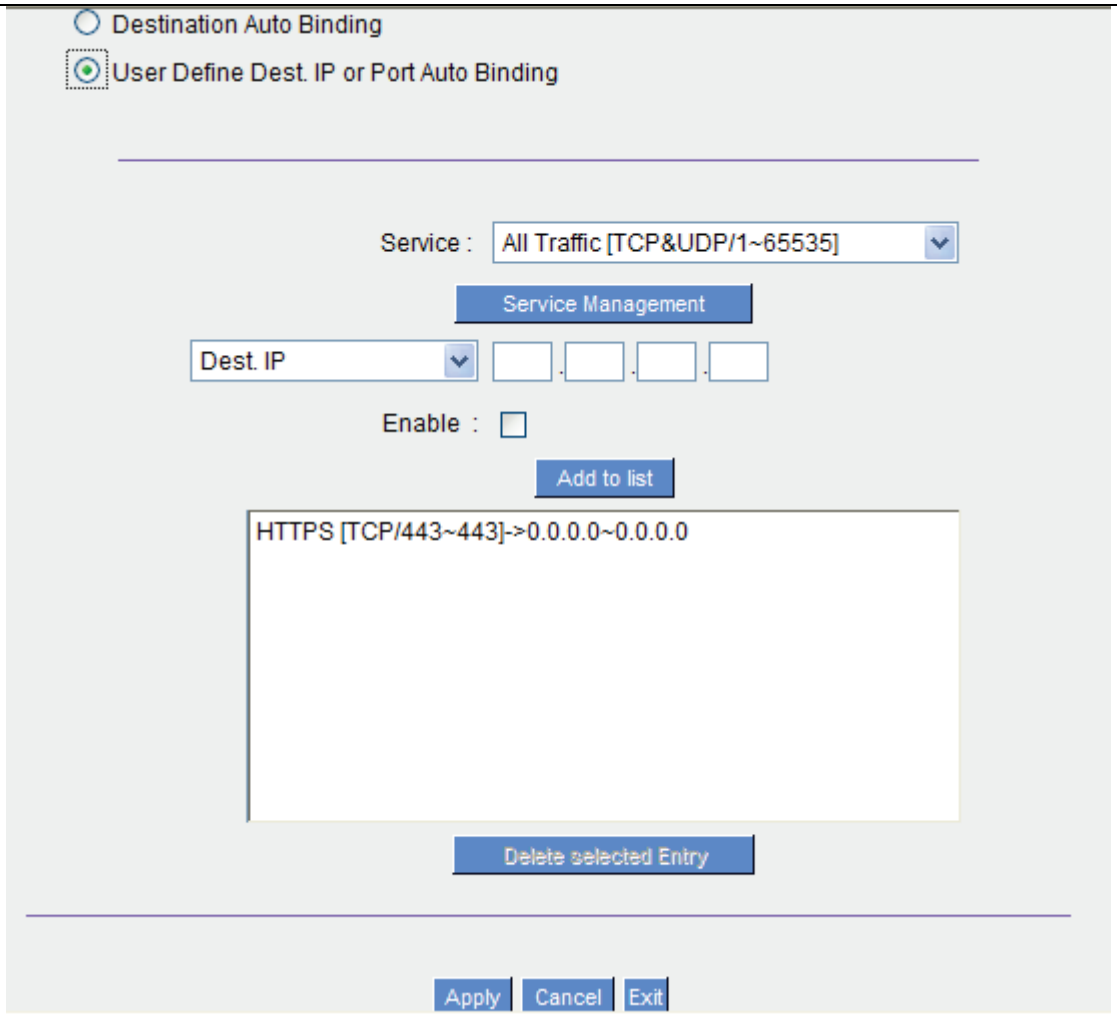
與192.168.1.101，192.168.1.100首次去訪問外網61.222.81.100時，被隨機分配到以WAN1 200.10.10.1 建立連線，當 192.168.1.100 有下一筆連線目的地是 61.222.81.101 (在同一個 Class B 子網範圍) 時，也一樣會以 WAN1 200.10.10.1 去建立連線，但是若是去到別的目的地 IP (不在 61.222.81.100 同一個 Class B 子網範圍) 則依然以原來連線數平衡的機制隨機平均分配

另一個內網 IP 192.168.1.101，首次去訪問外網 61.222.81.101 時，被隨機分配到以 WAN2 200.10.10.2 建立連線，當 192.168.1.101 有下一筆連線目的地是 61.222.81.100 (在同一個 Class B 子網範圍) 時，也一樣會以 WAN2 200.10.10.2 去建立連線，但是若是去到別的目的地 IP (不在 61.222.81.100 同一個 Class B 子網範圍) 則依然以原來連線數平衡的機制隨機平均分配

※請注意！

並不是「所有內網 IP」到某一「相同 Class B 範圍」都固定以某個 WAN IP 進行連線，而是看「每一個內網 IP」第一次被隨機分配到以那一個 WAN IP 進行連線，之後遇到目的地是相同 Class B 範圍，再「個別」按照同一個 WAN IP 進行連線。

User Define Dis. Or Port Auto Binding **用戶自定義目的地及服務端口綁定**	這邊是設定單一內網 IP，以某個自定義的特殊服務通訊向某個目的地 IP (或 IP 範圍) 進行連線時，固定以同一個 WAN IP 進行連線。 您可以自行設定服務通訊埠與目的地 IP 內容 (目的地 IP 範圍若設定成 0.0.0.0 到 0 表示到「任何一個目的地 IP 範圍」 **※請注意！** 「**User define Dest. IP or Port Auto Binding** 用戶自定義目的地及服務端口綁定」與「**Destination Auto Binding** 目的地聯機登入自動綁定」兩者只能同時使用其中一種！
Take default rules for example： 以出廠預設已有設定的規則舉例	(如下圖)



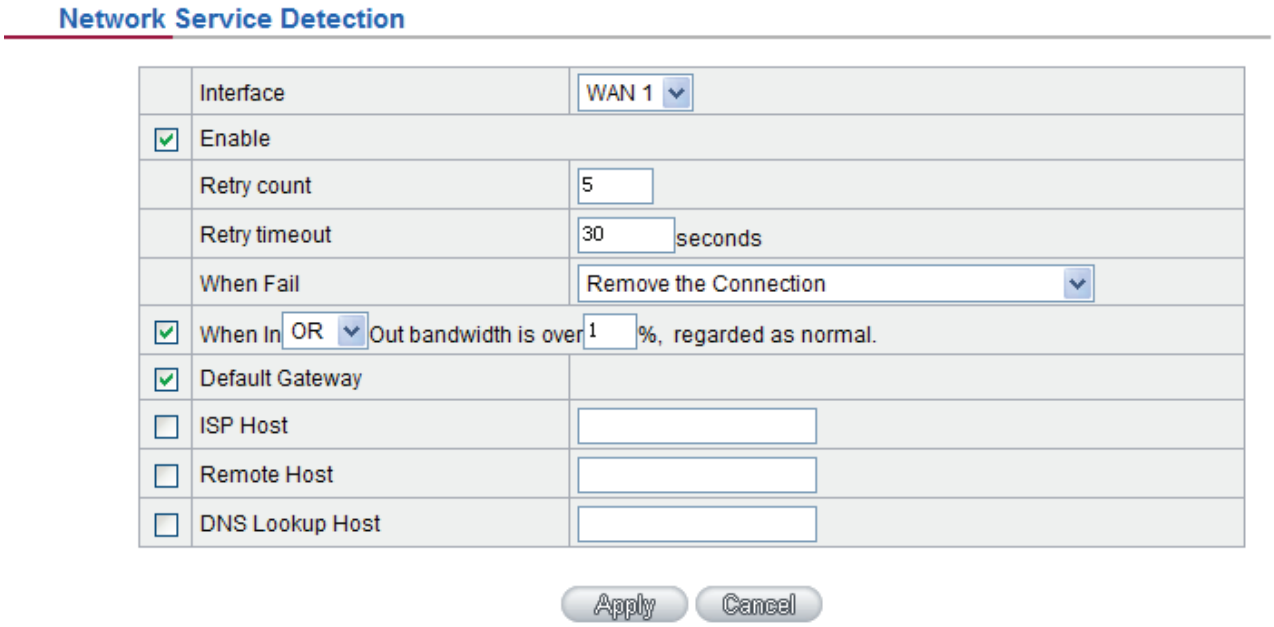
表示內網任何單一 IP，在以 TCP 443 Port 與任何目的地 (0.0.0.0 到 0 表示任何目的地) 進行連線時，都固定以同一個 WAN IP 進行連線，至於各個內網 IP 的選擇是固定在那一個 WAN IP，則是以第一次被原本連線數平衡機制所隨機分配到的 WAN IP 爲準，舉例來說兩個內網 IP 192.168.100.1 與 192.168.100.2，當個別第一次進行 TCP 443 Port 連線時，192.168.100.1 被隨機平均分配到以 WAN 1 IP 連線，192.168,100.2 被隨機分配到以 WAN2 IP 連線，則只要之後 192.168.100.1 有任何 TCP 443 Port 的連線，就會固定以 WAN 1 IP 連線；192.168.100.2 有任何 TCP 443 Port 的連線，就會固定以 WAN 2 IP 連線。

此預設規則雖然出廠預設值就有，但是您可以視自己的需求取消/刪除此規則的應用，或新增其他新的規則以符合實際的連線需求。

6.2.2 Network Service Detection - 線路偵測機制

若勾選此項設定，則會顯示出重新發起測試次數，回應延長時間等資訊。當使用兩條廣

域網做對外聯結線路時一定將此 NSD 啓用，以避免因爲廣域埠流量過大時造成路由器的誤判將此線路判斷爲斷線。



Interface **界面**	選擇您要設定線路偵測的廣域網口。
Retry **重新偵測次數**	對外連線偵測重試次數，預設值爲五次。如果連線偵測重試次數超過設定次數，網路沒有回應的話，則判斷爲對外線路中斷！
Retry Timeout **重新偵測時間間隔**	對外連線偵測逾時時間(秒)，預設值爲 30 秒。於此設定秒數之後重新測試對外連線。
When Fail **斷線時**	(1) **Generate the Error Condition in the System Log (只選擇儲存到日誌記錄檔):** 當偵測到與 ISP 連結失敗時，系統就會在系統日誌中將這項錯誤資訊紀錄下來，但保持此線路不會移除，所以會導致有些原來使用此條線路上的用戶無法正常使用。 此選項適用在當某條廣域網連線失敗時，從這個廣域網去訪問的目的地位址是無法從另一條線路去訪問的時候，就可以用此選項。例如若是要訪問 10.0.0.1 到 10.254.254.254 時一定要走廣域網 1 去訪問，而且廣域網 2 是無法訪問到此網段，那就可以使用此選項。因爲若廣域網 1 掉線後走廣域網 2 也無法去訪問到 10.0.0.1 到 10.254.254.254，就不需要在廣域網 1 斷線時將此線路移除。 (2) **Keep System Log and Remove the**

	Connection (刪除該線路): 當偵測到與 ISP 連結失敗時，系統不會在系統日誌中將這項錯誤資訊紀錄下來，原本使用此 WAN 端的封包傳遞會自動轉換到另一條廣域埠.等到原本斷線的廣域埠恢復後會自行重新連結，則封包傳遞會自動轉換回來。 (3)此選項適用在當某條廣域網連線失敗時，從這個廣域網去訪問的目的地位置是可以從另一條線路去訪問的時候，就要用此選項。如此可以讓任何一條廣域網斷線的時候，另一條可以做備援，將流量轉移到還在連線的廣域網。
Detecting Feedback Servers 偵測以下可回應的伺服器	
Default Gateway **預設閘道**	近端的預設通訊網關位置，如 ADSL 路由器的 IP 位址，此爲路由自動填入，所以只須打勾選擇是否啓用。 **注意！** 有部分的 ADSL 線路的閘道是不會回應偵測封包，或是當您是使用光纖盒，或是 ISP 發給您的是固定的公網 IP，且閘道就是在您網吧這端而不是在 ISP 那端時，此選項不要啓動。
ISP Host **ISP 伺服器**	ISP 端的偵測位置，如 ISP 的 DNS 伺服器 IP 地址等。在設定此 IP 位址時請確認此 IP 位址是可以且穩定快速的得到回應(建議填入 ISP 端 DNS IP)。
Remote Host **遠端伺服器**	遠端的網路節點偵測位置，此 Remote Host IP 位址最好也是可以且穩定快速的得到回應(建議填入 ISP 端 DNS IP)。
使用 DNS 伺服器做網域名稱解析	網域名稱解析服務 DNS 的偵測位置(此欄位只許填入網址如“www.hinet.net”，請勿填 IP 地址)。另外，兩條 WAN 的此欄位不可以填入相同的網址。

注意！

在“指定路由”的負載均衡模式下，第一個廣域網口會保留給沒有指定到其他廣域網口(WAN1～WAN2)的 IP 或應用服務埠(服務埠)經由此廣域網(WAN1)進出。因此建議您在此模式下將您的其中一條線路接在第一個廣域網口。當您其他的廣域網口(WAN2)斷線時，而您在線路偵測機制下選擇移除有問題線路，流量就會轉移到第一個廣域網口(WAN1)。此外，若是第一個廣域網口(WAN1)斷線，則流量會依次轉移到其他廣域網口，例如轉移到 WAN2。

6.2.3 Protocol Binding – 協議綁定設置

界面配置

安全路由器最多可以設置兩個廣域網界面，每個廣域網的頻寬以及是否真正可以對外連線會影響路由器的負載均衡機制，因此您需要分別對每個廣域網口做頻寬設定，並正確的設置該廣域網口的線路偵測機制。

在“**WAN Setting**”中，點擊“**Edit**”按鈕即可進入該廣域網口的配置視窗。

WAN Setting

Please choose how many WAN ports you prefer to use : 2 (Default: 1)

Interface	Connection Type	Config.
WAN 1	PPPoE	Edit
WAN 2	Obtain an IP automatically	Edit
USB	3G / 3.5G	Edit

頻寬設定

WAN 的頻寬資料請填入您所申請的寬頻網路實際上傳及下載頻寬，QoS 的頻寬控制會依照您所填入的頻寬作爲計算依據。例如每個 IP 及服務埠（服務埠）可以保障使用的上傳或下載的最小頻寬會依照此 WAN1 及 WAN2 的實際頻寬相加來換算實際可保障的大小。例如上傳頻寬若兩條都爲 512Kbit/Sec，那實際上傳頻寬就爲 WAN1+WAN2=1024Kbit/Sec，所以若有 50 個 IP 在內部網路，若要保證每人最小可使用的上傳頻寬，則就把 1024Kbit/50=20Kbit，這樣每人可以保證的最小頻寬就可以填 20kbit/Sec，下載同此換算方式。此部份請於 QoS 設定頁面設置，因此請參閱本手冊 **8.1 QoS 頻寬設置**。

The Maximum Bandwidth provided by ISP

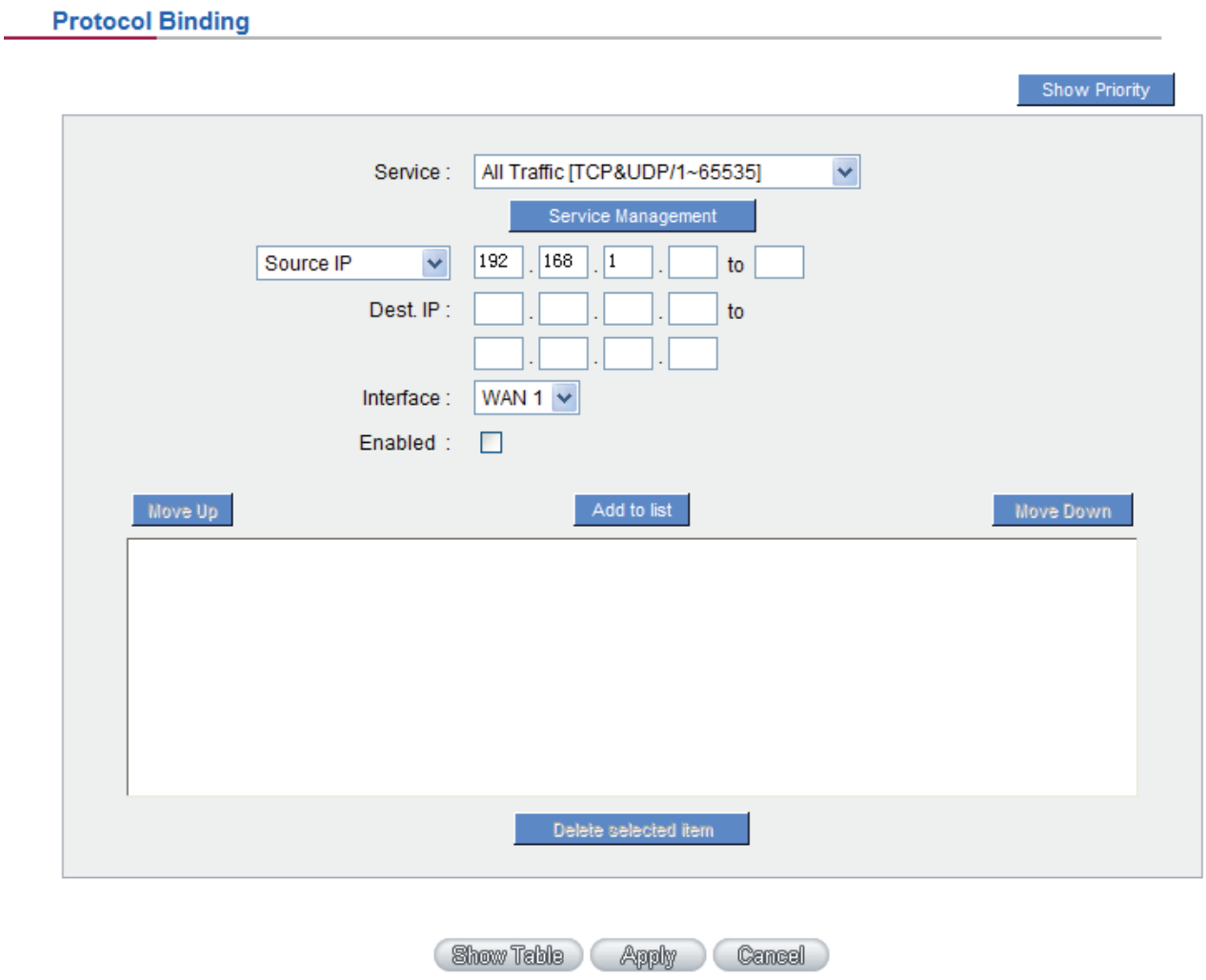
Interface	Upstream (Kbit/sec)	Downstream (Kbit/sec)
WAN 1	1000000	1000000
WAN 2	10000	10000
USB	256	2048

Protocol Binding – 協議綁定

使用者可將特定的 IP 或特定的應用服務埠(服務埠)經由您限定的 WAN 出去。其他沒有做綁定的 IP 或伺服器還是會進行廣域網的負載平衡。

注意！

在“指定路由”的負載均衡模式下，第一個廣域網口(WAN1)是不能被指定的，保留給沒有指定到其他廣域網口(WAN2～WAN4)的 IP 或應用服務埠(服務埠)經由此廣域網(WAN1)進出。也就是說第一個廣域網口(WAN1)不能設置通訊協定綁定的規則，以避免所有的廣域網口都被指定有特定的內網 IP、應用服務埠、目的地 IP，導致其他的 IP 或應用服務埠沒有廣域網口可以使用。



Service:	在此選擇欲開啓的綁定服務埠，從下拉式選單中可以選擇預設列表(如 All -TCP&UDP 0～65535， WWW 爲 80～80， FTP 爲 21～21 等等)，預設的服務爲 All 0～65535。 點擊"服務端新增或刪除表"按鈕可以進入服務埠設定視窗，進行新增或刪除選單中預設的服務埠。
Source IP:	您可以指定特定的內部虛擬 IP 位址的封包經由特定的廣域埠出去。在此填上內部虛擬 IP 位址範圍，例如 192.168.1.100 到 150. 則 IP 地址 100 到 150 爲綁定範圍。如果使用者只需要設定特定的服務埠而不需指定特定的 IP 位址， 則在 IP 的欄位皆填入 0。您也可以選擇 IP 群組的方式來指定來源 IP。關於 IP 群組的設定，請參考（"7.6 IP 群組管理"的說明）。
Dest. IP:	在此填上外部固定 IP 位址，例如若有一目標位址 210.11.1.1，要連接此位址的使用者限定只能從廣域埠 1 到達此目標位址，則在此填上外部固定 IP 位址 210.11.1.1 到 210.11.1.1。如果使用者要設定一個範圍的目的地位置，則填入方式可以爲 210.11.1.1 到 210.11.255.254，則表示整組 210.11.x.x 的 Class C 網段都限制走某一條廣域網，若只需要設定特定的應用而不需指定特定的 IP 位址，則在 IP 的欄位皆填入 0.0.0.0。
Interface:	選擇您所要綁定此條規則在哪一個 WAN 埠。
Enable:	啓用此規則。
Add To List:	增加此條規則到列表。
Delete selected item:	刪除在服務列表裏所選擇的規則。
Moving Up & Down:	由於每條規則執行的優先順序爲由列表的最上面那條往下執行，也就是越後面設定的規則會越後執行，所以您可以自行調整每條規則先後執行順序。

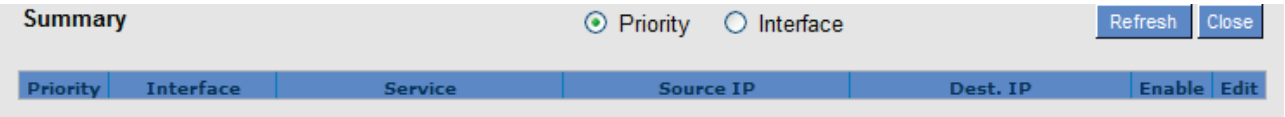
注意！

通訊綁定協定所設的規則在路由器執行時也有優先順序的，由上到下，在列表上最上方那條會先執行，然後依序往下。

Show Priority – 優先權

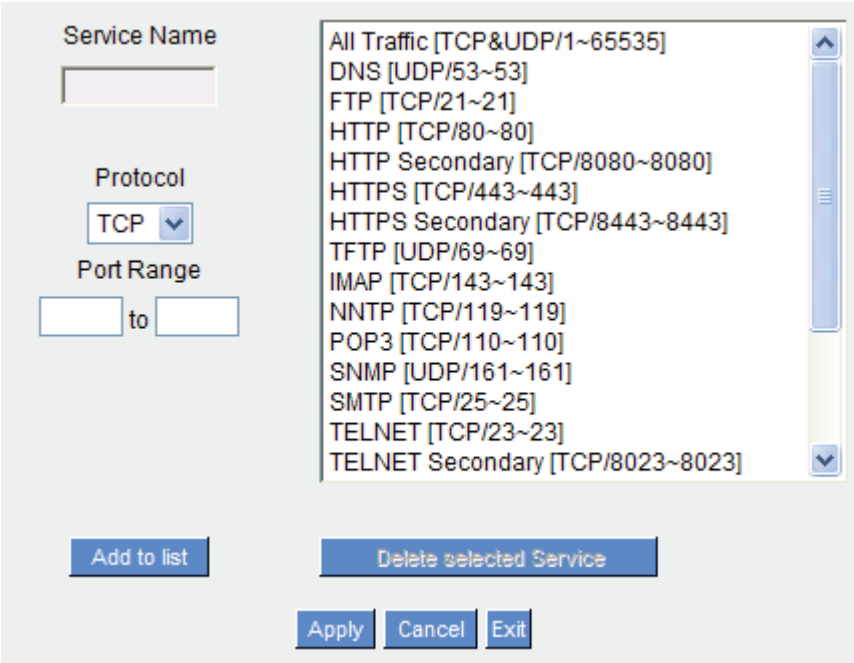
點擊右上方的"**Show Priority**" 按鈕，會出現以下的對話視窗。您可以選擇以"優先權"來

顯示排列的順序，或是以“界面位置”來顯示排列的順序。點擊“**Refresh**” 可以重新顯示視窗，點擊“關閉”將結束這個對話視窗。



Add or Remove Service Port -新增或刪除管理服務埠號

若您欲開啓的服務埠專案沒有在表列中，您可以點擊“**Service Management**” 按鈕，新增或刪除管理服務埠號列表，如以下所述：



Service Name:	在此自定欲開啓的服務埠號名稱加入列表中，如 BT 等。
Protocol:	在此選擇欲開啓的服務埠號的封包格式爲 TCP 或 UDP。
Port range:	填入您將新增加的服務埠範圍。
Add To List:	增加到開啓服務專案內容列表，最多可新增 100 組。
Delete selected service:	刪除所選擇的開啓服務專案內容。
Apply:	點擊此按鈕“**Apply**”即會儲存剛才所變動的修改設定內容參數。
Cancel:	點擊此按鈕“**Cancel**”即會清除剛才所變動的修改設定內容參數，此操作必須於確認儲存動作之前才會有效。

Exit:	離開此功能設定視窗。

使用 Auto Load Balance 時其通訊協定綁定協定設定方式：

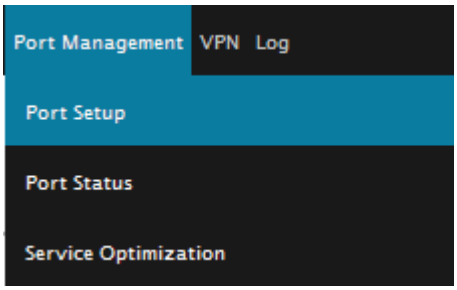
智慧負載均衡方式搭配“通訊協定綁定”可以有更彈性運用您的頻寬，您可將特定的內網 IP，使用特定應用服務埠作訪問，或特定的目的地 IP 經由您指定的廣域網來訪問外網。

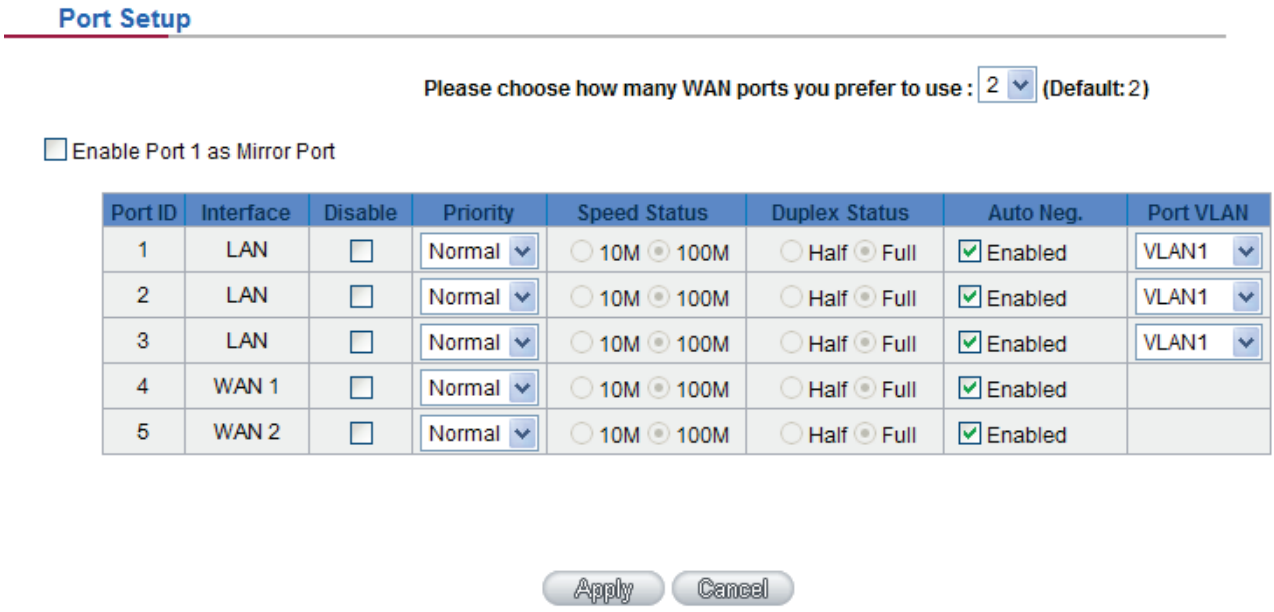
VII. 內部區域網路配置

通過本章節可以對埠進行配置管理，瞭解如何配置內部區域網路的 IP 位址。

7.1 Port Management - 網路埠管理配置

安全路由器中，管理者可以設定網路實體連線於每一個乙太網路埠，如連接速率，工作模式，優先權，自動偵測或是 VLAN 等乙太網路埠的功能。

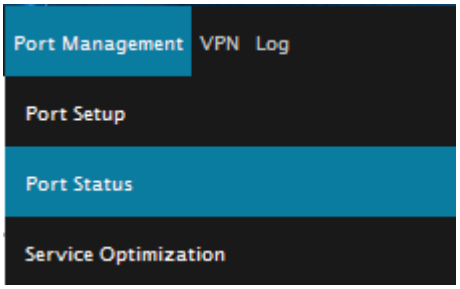




Mirror Port：勾選“**Enable Port 1 as Mirror Port**”可以將區域網的第一個埠設定爲鏡射埠，所有從內網到外網訪問的流量都會複製到鏡射埠。因此您可以將監控或是過濾伺服器直接接在鏡射埠，來達到監控或是過濾網路封包的目的。

Disabled Port **關閉端口**	此爲設定乙太網路的 LAN 埠開啓或是關閉的功能，若是打勾的話，則此乙太網路埠立即被關閉無法連接使用。預設爲開啓無打勾。
Priority **優先權**	此爲設定此乙太網路的 LAN 埠封包傳送優先權設定，若是此埠設定爲高的話，則最優先使用傳送封包的權利，預設優先順序爲一般。
Speed Status **網路連接速度**	此爲設定此乙太網路的埠網路實體連接速率選項，您可以設定爲 10Mbps 或是 100Mbps 連接速度。預設爲自動偵測。
Duplex Status **半雙/全雙工模式**	此爲設定此乙太網路的埠網路實體連接速率工作模式選項，您可以設定爲半雙工模式或是全雙工模式運作。預設爲自動偵測。
Auto Neg. **自動偵測模式**	此爲設定乙太網路的埠網路實體連接速率自動偵測模式，若是勾選的話，自動偵測所有連接埠的信號與調整。
VLAN：	此功能可以讓網管人員在自己的區域網內將每一個區域網埠設定 1 個或多個不同網段且無法互通的區域網埠，但都可以通過安全路由器上網路。在同一個網段內的成員(在同一個 VLAN 區域網路內)可互相溝通並看得到對方，若不在同一個 VLAN 群組內的成員則無法得知其他成員的存在。使用者可爲每一個 LAN 埠選定爲哪一個 VLAN 區域網路群組， 最多可設定爲 3 個區域網路群組。
VLAN All：	當網管人員在內網設定了多個 VALN 埠，且不在同一個 VLAN 群組內無法互訪，可是內網又需要架設服飾器讓內網所有 VLAN 群組都可以訪問此伺服器。此時可以將某一區域網埠設定爲 VLAN All，將此伺服器接入此 VLAN All 的埠，這樣就可以讓所有不同 VLAN 群組的電腦都可以訪問到此伺服器。

7.2 Port Status - 網路埠狀態即時顯示



Summary

Type	10Base-T / 100Base-TX
Interface	LAN
Link Status	Down
Physical Port Status	Port Enabled
Priority Setup	Normal
Speed Status	10 Mbps
Duplex Status	Half
Auto Neg.	Enabled
Port VLAN	VLAN1

Statistics

Received Packets Count	165253
Received Bytes Count	76987148
Transmitted Packets Count	2826351
Transmitted Bytes Count	337205828
Error Packets Count	0

Summary – 摘要

網路連接狀態（10Base-T / 100Base-TX），界面位置（區域網/廣域網路），線路連線狀態(啓動/關閉)，埠配置狀態（埠啓動/埠關閉），優先權設定（高級/一般），網路連接速率

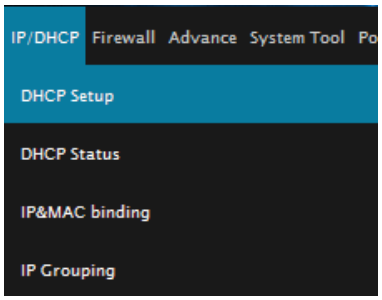
（10Mbps/100Mbps）， 半雙/全雙工模式(半雙工/全雙工)，自動偵測模式（啓動/關閉），VLAN（VLAN1~3/ VLAN All）。

Statistics – 流量即時顯示

即時顯示路由器工作狀態下的接收和傳送封包計算、封包接收和傳送 Byte 數以及錯誤封包統計實際數值。

7.3 IP/ DHCP

安全路由器支援 Class C 的 DHCP 伺服器，預設值是啓動，可以提供區域網路內的電腦自動取得 IP 的功能，(如同 NT 伺服器中的 DHCP 服務)，好處是每台 PC 不用去記錄與設定其 IP 位址，當電腦開機後，就可從安全路由器自動取得 IP 位址，管理方便。



DHCP Dynamic IP

Client Lease Time 1440 Minutes

Subnet :	Subnet1	Subnet2
DHCP Server :	Enabled	Disabled
IP Range Starts :	192.168.1.100	192.168.2.100
IP Range Ends :	192.168.1.149	192.168.2.149
MAC Addresses Pool for this IP Range :	Pool Table	Pool Table

Unified IP Management

DNS

DNS(Required) 1:	0 . 0 . 0 . 0
DNS(Optional) 2:	0 . 0 . 0 . 0

WINS

WINS Server:	0 . 0 . 0 . 0

Dynamic IP – 動態 IP 服務

Client lease Time **租約時間**	此設定爲發給 PC 端 IP 地址的租約時間，預設爲 1440 分鐘(代表時間爲一天)，當租約時間到後，PC 端會重新跟路由再申請一次。您可以依照實際需求來設定。
Range Start **起始 IP 位址**	您可以依照實際需求來設定。
Range End **終止 IP 位址**	您可以依照實際需求來設定。

DNS (Domain Name Service) - 網域名稱解析服務伺服器位址

此設定爲發給 PC 端 IP 位址的 DNS 網域伺服器查詢位址，若您有特定使用的 DNS 伺服器，可以直接輸入此伺服器的 IP 位址，則 PC 端從 DHCP 取得 IP 地址時，也會一併取得指定的 DNS 伺服器地址。

DNS (Required) 1：	輸入 DNS 網域伺服器的 IP 位置。
DNS (Optional) 2：	輸入 DNS 網域伺服器的 IP 位置。

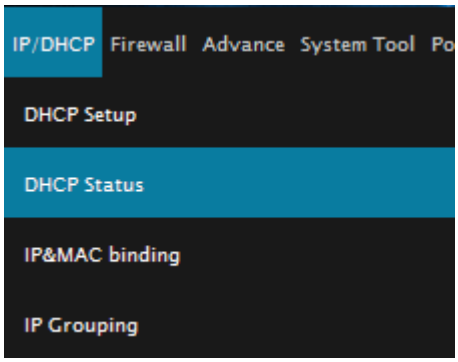
WINS：

若您的網路上有解析 Windows 電腦名稱的伺服器，您可以直接輸入此伺服器的 IP 位址。

WINS Server：	輸入 WINS 網域伺服器的 IP 位置。
Apply：	點擊此按鈕“Apply”即會儲存剛才所變動的修改設定內容參數。
Cancel：	點擊此按鈕“Cancel”即會清除剛才所變動的修改設定內容參數，此操作必須於確認儲存動作之前才會有效。

7.4 DHCP Status – DHCP 狀態顯示

此狀態表爲顯示 DHCP 伺服器的目前使用狀態與設定紀錄等，以便提供管理人員需要時做網路設定參考資料。



Status

Subnet :	Subnet1	Subnet2
DHCP Server :	192.168.1.1	192.168.2.1
Dynamic IP Used :	0	0
Static IP Used :	0	0
DHCP Available :	50	50
Total :	50	50

Client Table

Subnet1

Host Name	IP Address	MAC Address	Client Lease Time	Delete

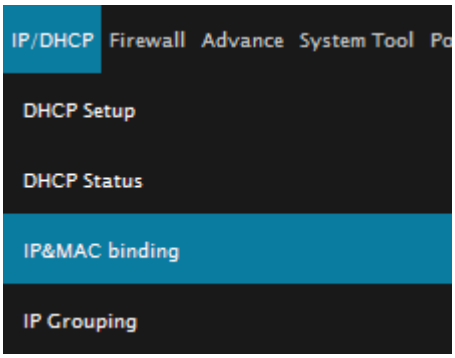
Refresh

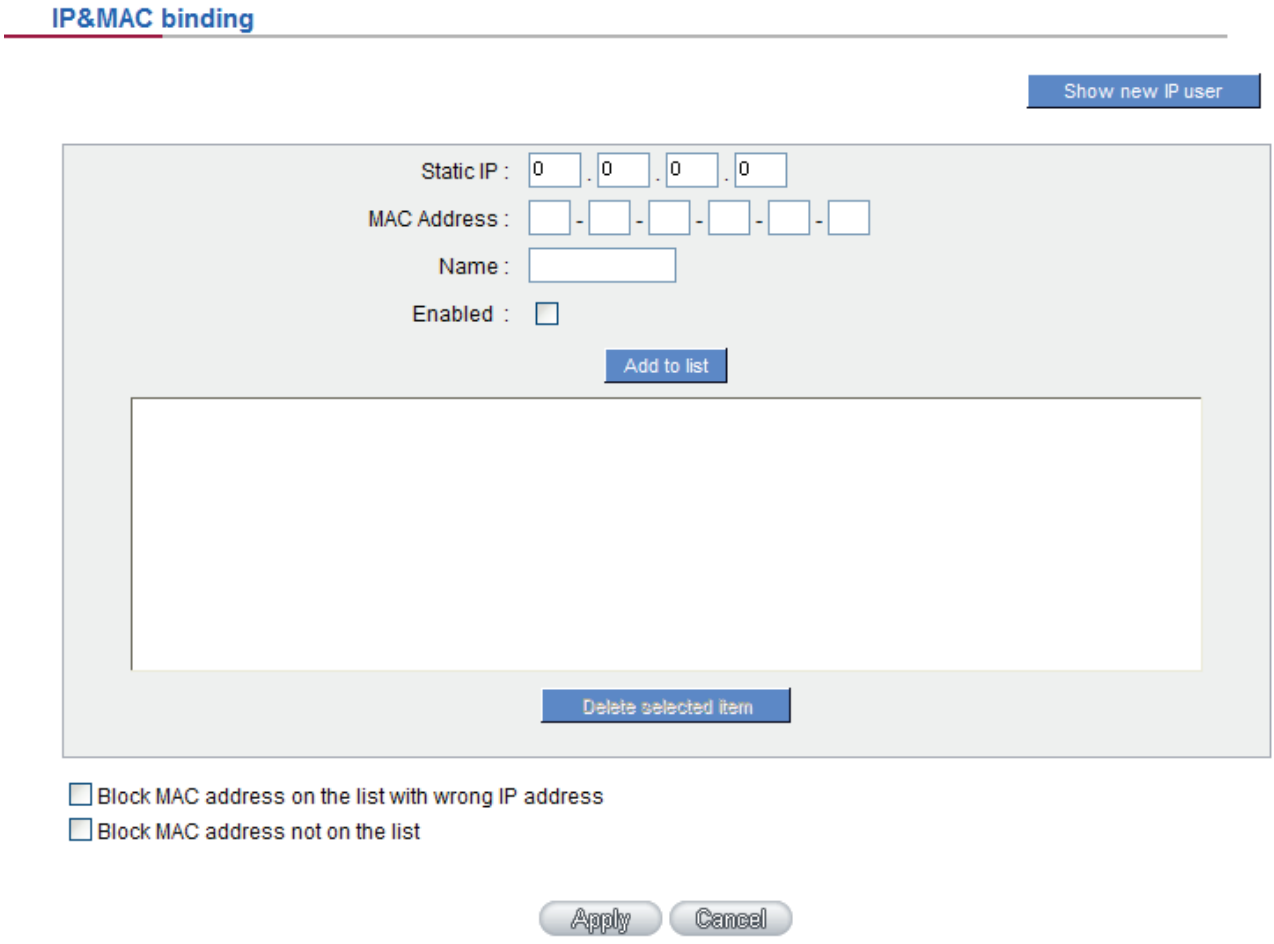
DHCP Server：	目前 DHCP 伺服器的 IP 地址。
Dynamic IP Used：	目前 DHCP 伺服器已經發放動態 IP 的數量。
Static IP Used：	目前 DHCP 伺服器已經發放固定 IP 的數量。

DHCP Available：	目前 DHCP 伺服器可以還可發放的 IP 數量。
Total：	目前 DHCP 伺服器所設定可發放的 IP 總數量。
Host Name：	目前此台電腦的電腦名稱。
IP Address：	目前此台電腦所取得的 IP 位址。
MAC Address：	目前此台電腦的 MAC 網路實體位置。
Client Lease Time：	DHCP 目前核發 IP 地址的租約時間。
Delete：	刪除此筆核發 IP 紀錄。

7.5 IP & MAC Binding - IP 及 MAC 地址綁定

網管人員可以設定安全路由器所提供的 IP & MAC 綁定功能，達到用戶不能自行添加電腦來使用對外網路或是私自擅改 IP 上網影響他人。

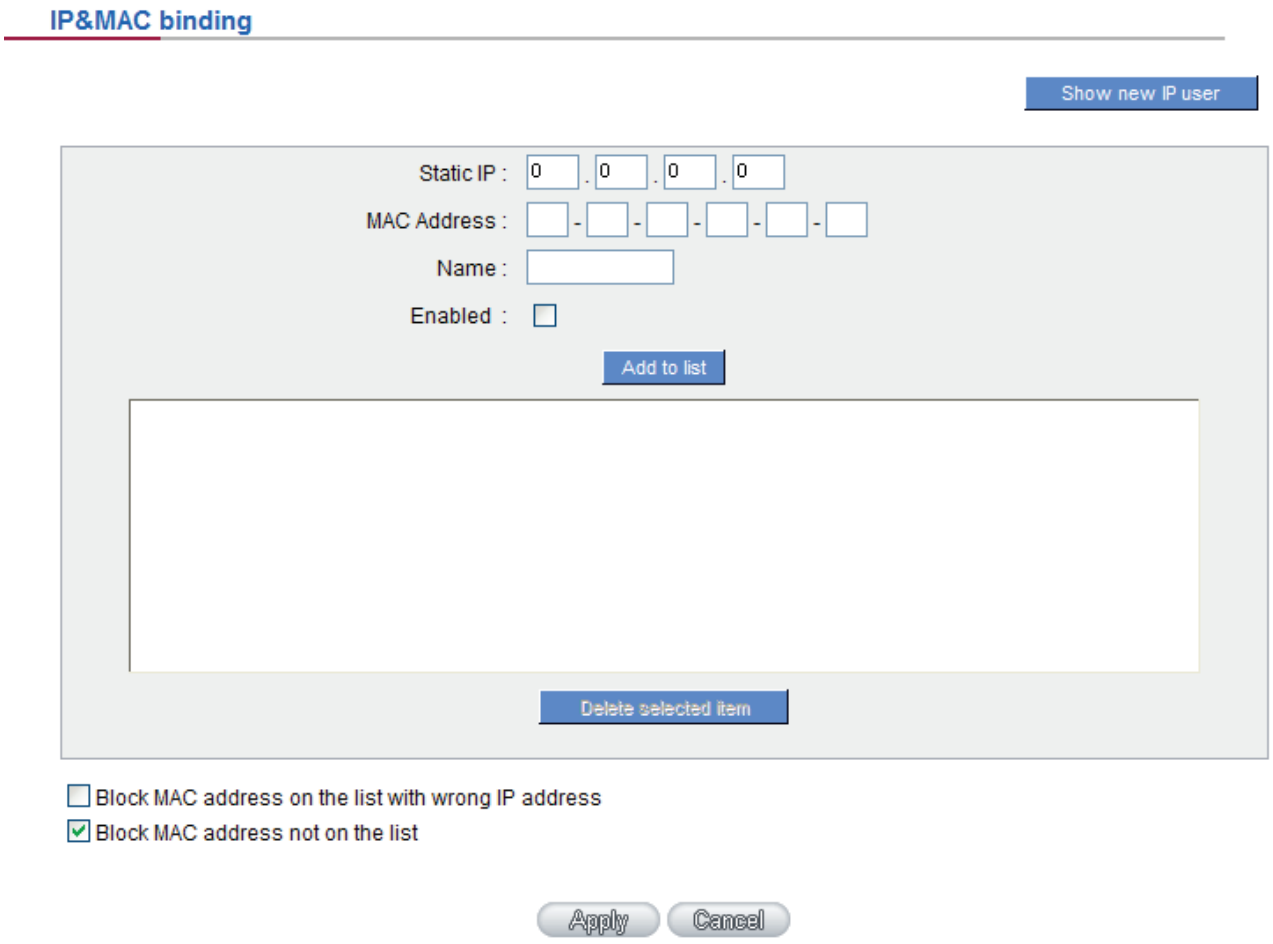




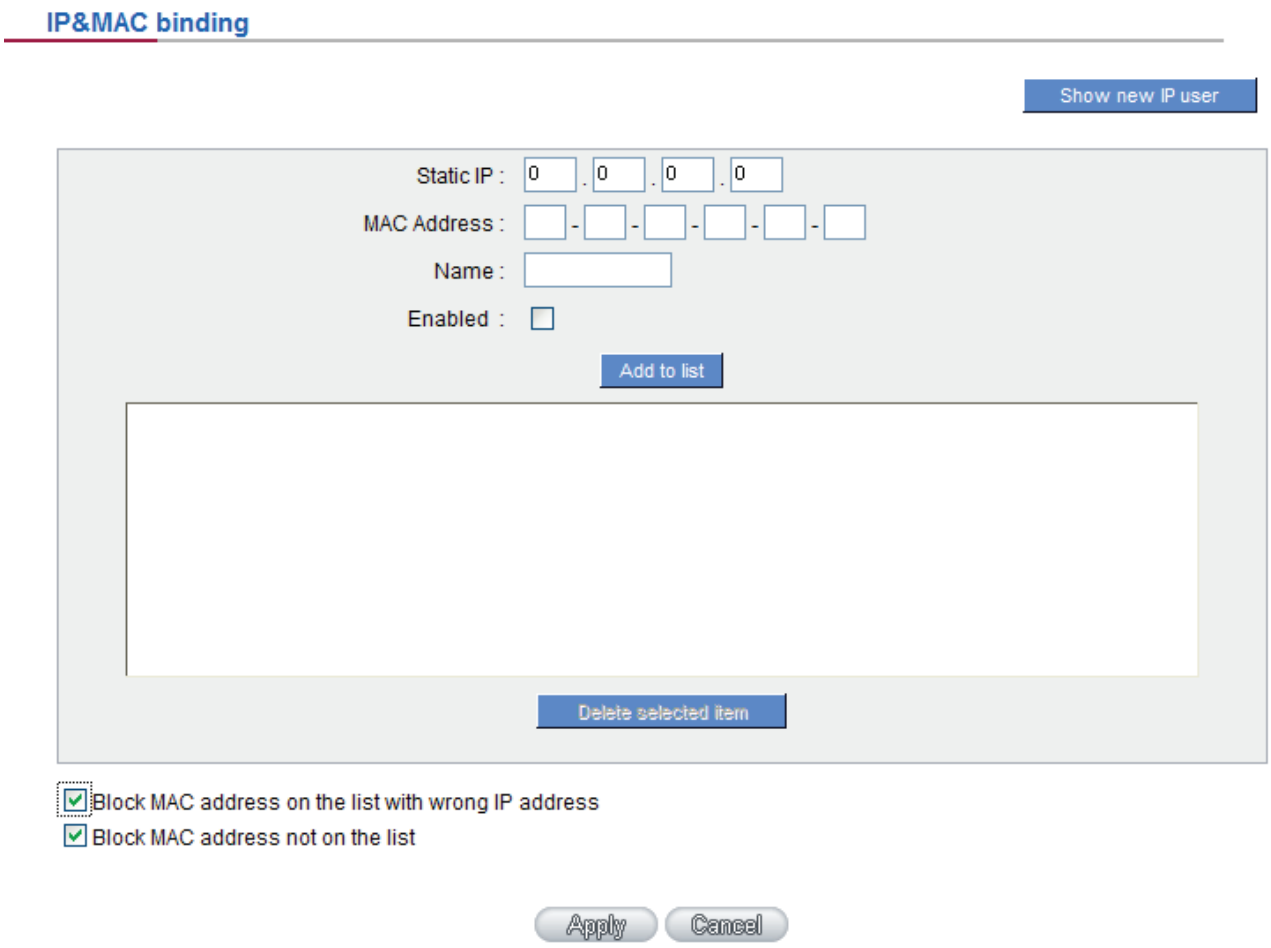
您可以以兩種方式來設定這個功能：

(1) Block MAC address not on the list – 阻擋未在清單 MAC 位址

此功能主要目的是限制只有在列表裏面的 MAC 位址才可以得到 DHCP 分配的 IP 位址上網，未在此列表的電腦都無法取得 IP 上網。當使用此功能時，切記要將靜態 IP 位址填 0.0.0.0 不可以空白，另外將“封鎖不在對應列表中的 MAC 位址”選項勾選才可以執行。如下圖中範例所示：



(2) IP & MAC Binding - IP 及 MAC 地址綁定



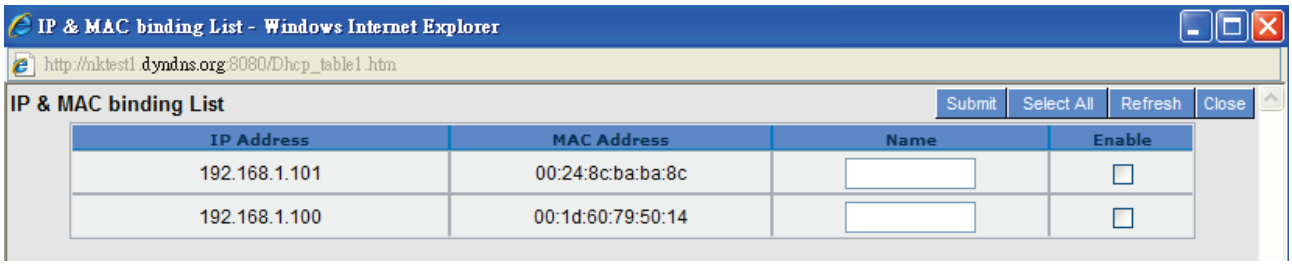
Static IP：	此欄位有兩種填入方式： 1. 若您只要限制 MAC 位址可以跟 DHCP 要 IP 而不一定是指定的那一個 IP，請在此欄位填 0.0.0.0，不可爲空白。 2. 若要求每次此台電腦都要分配到同一個 IP，則將您所要求分配給此台電腦的 IP 位址輸入。這樣所要綁定伺服器或 PC 端每次重啓都會要到固定的同一個虛擬 IP。
MAC Address：	輸入要綁定的伺服器或 PC 端固定實體 MAC(網路卡上的位址)。
Name：	填入您所綁定此用戶的名字或位址做辨識，可輸入 12 個字元，中英文皆可以。
Enabled：	啓用此組設定。

Add to list：	增加或修正此設定到列表中。
Delete selected item：	刪除列表中所選擇的綁定。
Add：	當列表中有綁定規則後，右下角會出現此按鈕，可點擊增加新的綁定。

Block MAC address on the list with wrong IP address：此選項打勾後，只要是 User 自行更改電腦的 IP 或不是列表設定的 IP 將無法上網。

Show New IP user -顯示出還未做綁定或新加入的 IP 及其 MAC 位址

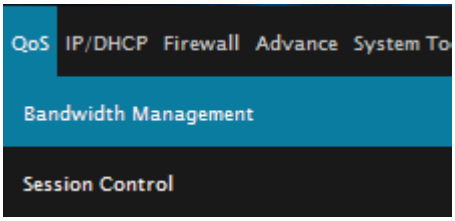
此功能的主要目的是爲了減少網管人員需一一查詢每台電腦的 MAC 位址後才能進行綁定，因爲會非常耗時且困難。再者，將 MAC 位址手動填入列表也很容易出錯。所以只需要查詢此表格，就可以看到所有進出路由器且還未綁定的 MAC 位址，然後直接在此表格做綁定動作即可。另外，若您發現此表格出現已經綁定的某組 MAC 又出現在此表格，則表示此用戶試圖修改不是您指定的 IP 上網。



Name：	可以填入您所綁定此用戶的名字或位址做辨識，可輸入 12 個字元。
Enabled：	勾選您所要綁定的目標。
Apply：	將您所選定好的目標綁定到 IP & MAC 綁定列表。
Select All：	選擇所有在此列表中的目標做綁定。
Refresh：	更新此列表。
Close：	關閉此列表。

VIII. QoS (Quality of Service) - 頻寬管理功能

頻寬管理 QoS 爲 Quality of Service 縮寫，其功能主要爲限制某些服務及 IP 的頻寬使用量，以滿足特定應用程式或服務所需要的頻寬或優先權，並讓其餘的使用者共用頻寬，才能有比較穩定、可靠的資料傳送服務。網路管理人員應該針對網吧、企業等的實際需求，對各種不同網路環境、應用程式或服務來進行頻寬管理，才能充分且有效率的達到網路頻寬使用。



8.1 Bandwidth Management – 頻寬管理

8.1.1 The Maximum Bandwidth provided by ISP – ISP 提供最大頻寬

The Maximum Bandwidth provided by ISP

Interface	Upstream (Kbit/sec)	Downstream (Kbit/sec)
WAN 1	1000000	1000000
WAN 2	10000	10000
USB	256	2048

WAN 的頻寬資料請填入您所申請的寬頻網路實際上傳及下載頻寬，QoS 的頻寬控制會依照您所填入的頻寬作爲計算依據。例如每個 IP 及服務埠（服務埠）可以保障使用的上傳或下載的最小頻寬會依照此 WAN1 及 WAN2 的實際頻寬相加來換算實際可保障的大小。例如上傳頻寬若兩條都爲 512Kbit/Sec，那實際上傳頻寬就爲 WAN1+WAN2=1024Kbit/Sec，所以若有 50 個 IP 在內部網路，若要保證每人最小可使用的上傳頻寬，則就把 1024Kbit/50=20Kbit，這樣每人可以保證的最小頻寬就可以填 20kbit/Sec，下載同此換算方式。

注意！

這裏的數值單位是 kbit，有些應用軟體顯示下載/上傳速度單位爲 KB，兩個數值之間的換算方式爲 1KB=8kbit。

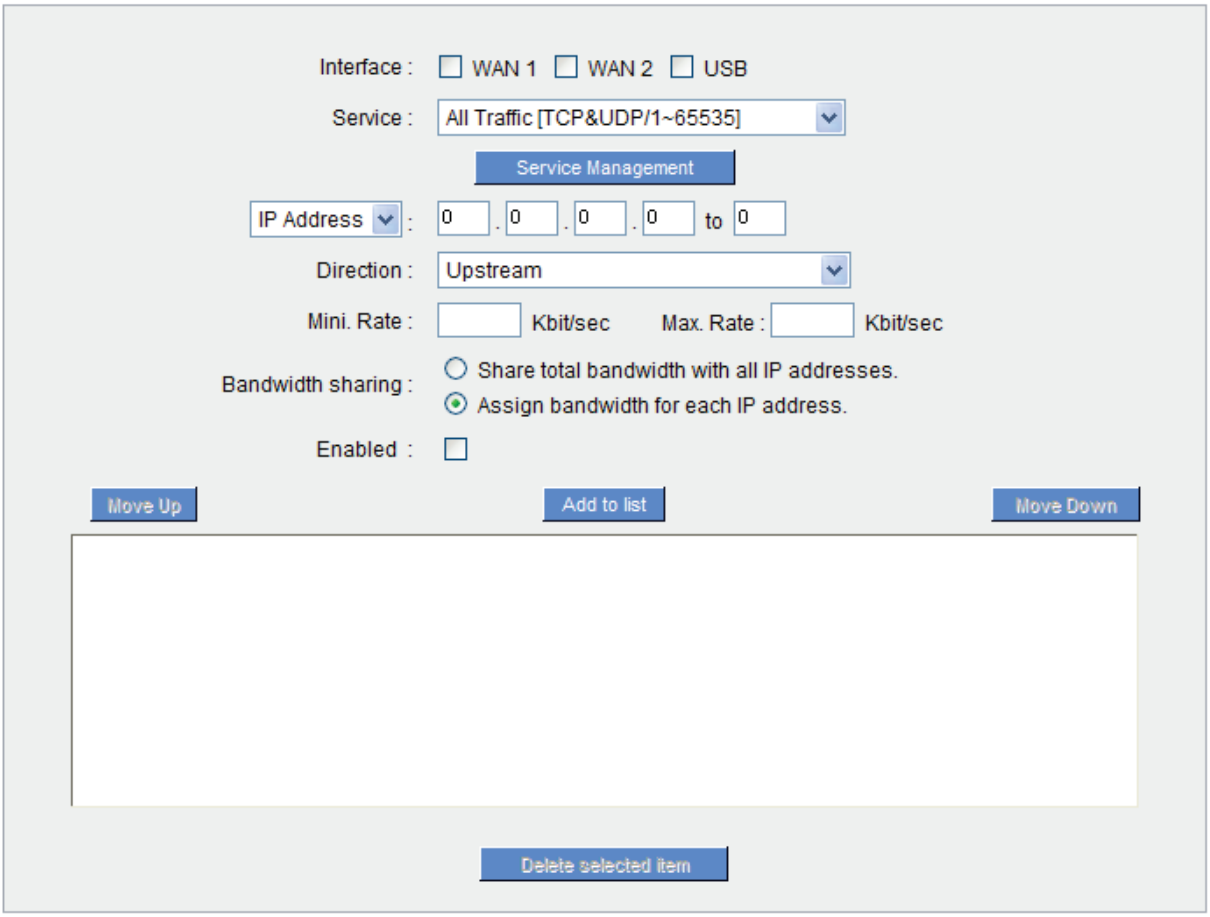
8.1.2 QoS

QoS 可以選擇兩種方式，無法同時使用，一爲流量控制(頻寬管理)，另一個爲優先權控制，設定人員可以依照自己內網需求做兩種模式靈活運用。

Rate Control - 頻寬控制 (頻寬管理) - 依使用量做管理

網管人員可依照您現有的頻寬大小做每一個 IP 或一個範圍的 IP 的使用量限制或保障頻寬。另外也可以針對服務埠去做頻寬控制。若是內部有架設伺服器的話，也可控制或保障其對外頻寬。

Quality of Service



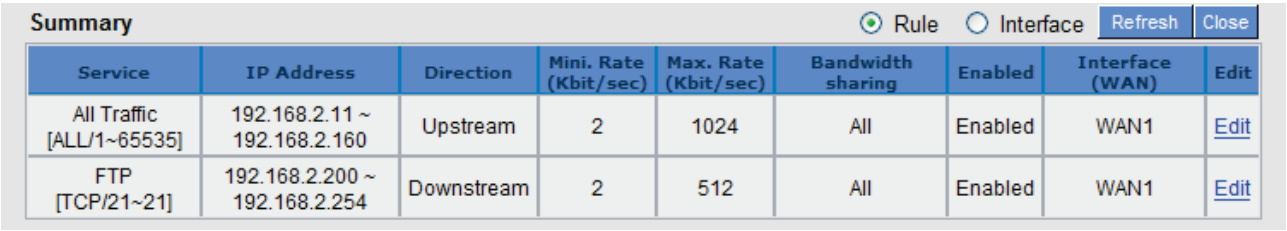
Interface **界面**	勾選此條 QoS 設定要控制在哪條 WAN 執行，可單獨或全部勾選。
Service Port **服務端口**	選擇此條 QoS 所要設定的頻寬控制爲哪個，若您是要針對每個 IP 的所有服務的使用頻寬，則將此選擇在 All(TCP&UDP)1~65535。若您只要針對譬如 FTP 上傳或下載，其餘服務不限制，則選擇 FTP Port21~21，可參考服務號碼預設列表。

IP Address	此爲選擇您所要限制的使用者爲哪些?若您只限制單一 IP，則直接將此 IP 填入，如：192.168.1.100 到 100，則此規則就是針對 192.168.1.100 此 IP 做控制。若是要限制一組 IP 範圍，則填入如 192.168.1.100 到 150，這樣此規則就是針對 192.168.1.100 到 150 做限制。若是此條頻寬限制是針對所有人也就是接在路由器內網的所有 User 則可在 IP 的欄位皆填入 0，也就是 192.168.1.0 到 0，這樣就表示所有 IP 都受此規則限制。另外此 QoS 是可以控制到 Class C 的範圍。
Direction 目的	**Upstream 上傳**：指對內網 IP 的上傳頻寬 **Downstream 下載**：指對內網 IP 的下載頻寬 虛擬伺服器上傳(Server in LAN，上傳)：若您有架設對外的 Server 網站在路由器內部，則此選項爲控制外部訪問此 Server 的頻寬控制。 虛擬伺服器下載(Server in LAN，下載)：若您有架設網站在路由器內網，則此選項爲控制外部對此伺服器上傳資料時的頻寬控制，例如網吧很多都有架設遊戲伺服器，若外部要來做此遊戲伺服器做資料升級時，可以用此控制做頻寬管理，才不會影響內部使用者上網打遊戲。
Min. & Max. Rate： **(Kbit/Sec)**	最小頻寬：此爲限制或保證此條規則的最小可使用頻寬。 最大頻寬：此爲限制此條規則的最大可使用頻寬，也就是最大不會超過此設定值。 **請注意！**這裏填入的數值單位是 kbit，有些應用軟體顯示下載/上傳速度單位爲 KB，兩個數值之間的換算方式爲 1KB=8kbit。

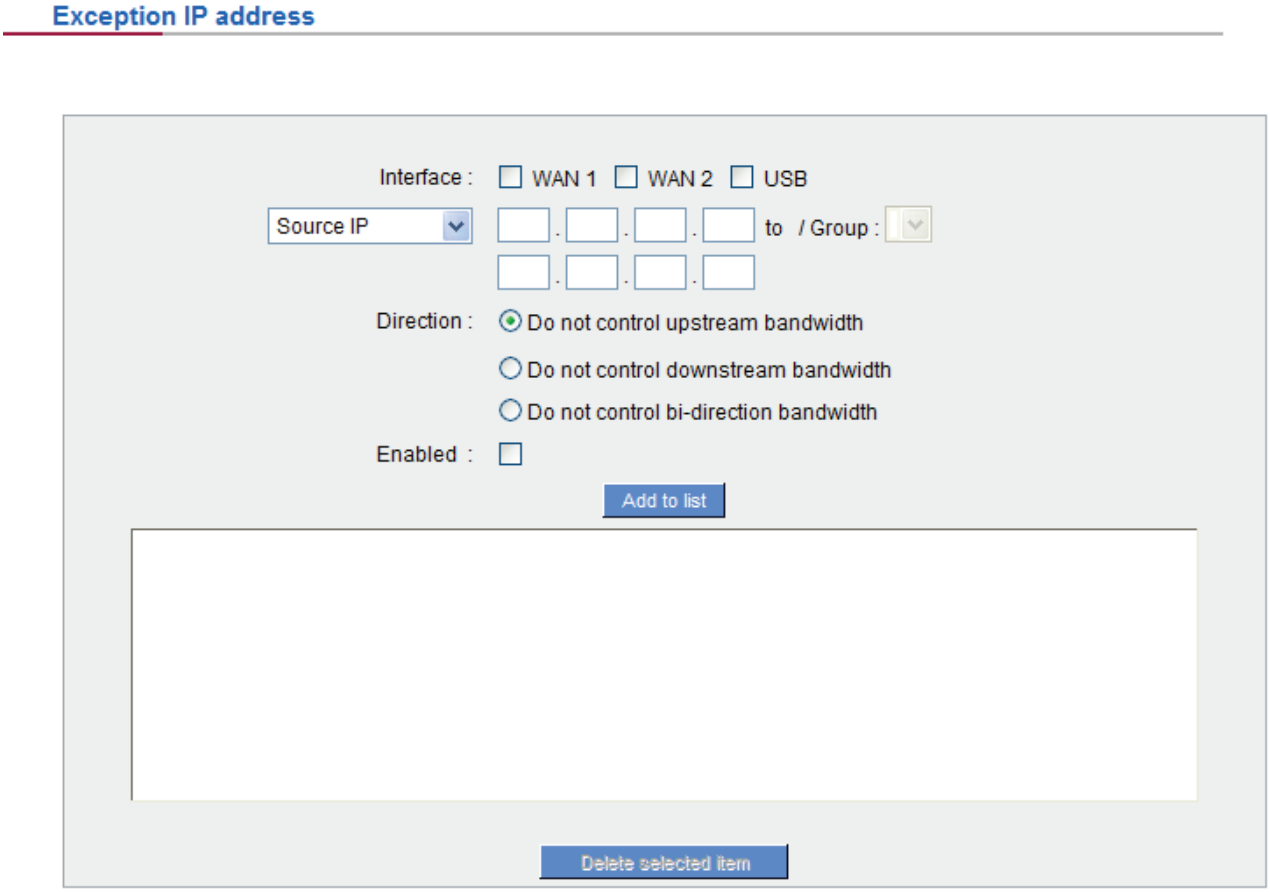
Bandwidth sharing **頻寬共享**	**所有 IP 範圍分享總頻寬：** 若選擇此規則的話，其表示所有 IP 或此服務埠共用這段(最小頻寬到最大頻寬)頻寬範圍。 **指定每一 IP 之可用頻寬：** 若選擇此規則的話，其表示每一個 IP 或這一段服務埠都可以有此(Mini 到 Max.Rtae)頻寬範圍，例如若是針對每台電腦 (IP 位址)做的規則設定，則每台電腦(IP 位址)都可以有這麼大的頻寬。 **請注意！**當您選擇頻寬的共用方式時，要留意實際應用的情況，以避免選擇不恰當的方式而造成頻寬太小無法正常使用網路。例如，內網多人使用 FTP 做檔下載，若是您希望 FTP 不會佔用掉大部分的頻寬，您就可以選擇共用頻寬，不論內網有多少人使用 FTP 做檔下載，總和所佔用的頻寬是固定的。
Enable	啓用此規則。
Add to list	增加此條規則到列表。
Move up & Move down	由於 QoS 的每條規則執行的優先順序爲由列表的最下面那條往上執行，也就是越後面設定的規則會優先執行，所以您可以自行調整每條規則先後執行順序。通常將要限制頻寬的服務埠移至最下方如 BT，e-mule 等，然後將針對限制 IP 頻寬的規則往上移。
Delete selected items	刪除在服務列表裏所選擇的專案內容。
Show Table	可以顯示出您所有在頻寬管理設定的規則，並可直接點擊“編輯”做修改（見表後詳解）。
Apply	點擊此按鈕“**確認**”即會儲存剛才所變動的修改設定內容參數。
Cancel	點擊此按鈕“**取消**”即會清除剛才所變動的修改設定內容參數，此操作必須於確認儲存動作之前才會有效。

Show Table：[Tina1]

點擊左下方的“**Show Table**”按鈕，會出現以下的對話視窗。您可以選擇以“**Rule**”來顯示已設定的規則，或是以“**Interface**”來顯示已設定的規則。點擊“**Refresh**”可以重新顯示視窗，點擊“**Close**”將結束這個對話視窗。可直接點擊“**Edit**”做修改。



Exception IP Address – 例外 IP 位址



Interface：	勾選哪些廣域網口不受限制。
Source IP：	輸入不受限制的 IP 位址範圍，或者選擇不受限制的 IP 群組。
Direction	可以選擇不管制上傳、不管制下載，或是雙向都不管制。
Enabled：	選擇啓動這個規則設定。
Add to list：	將添加的規則增加到列表中。

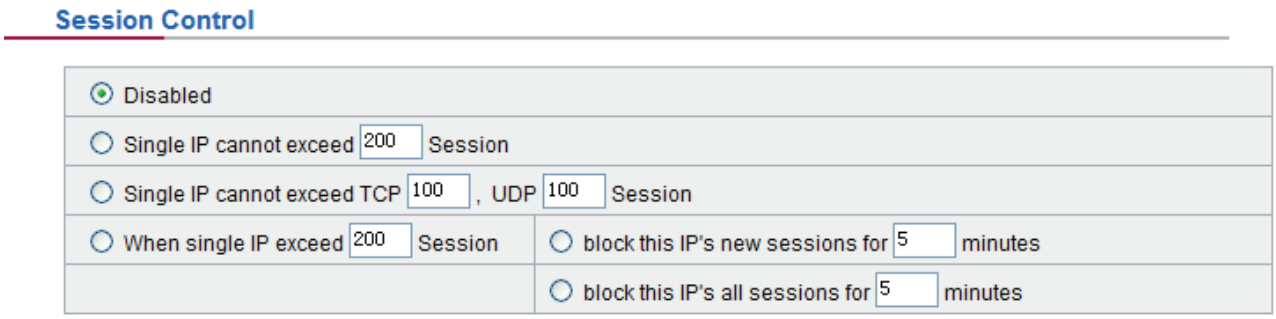
Delete seleted item：	選擇列表中的規則，刪除選中的規則。
Apply：	點擊此按鈕“**Apply**”即會儲存剛才所變動的修改設定內容參數。
Cancel：	點擊此按鈕“**Cancel**”即會清除剛才所變動的修改設定內容參數，此操作必須於確認儲存動作之前才會有效。

8.2 Session control – 連線數管控

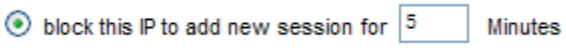
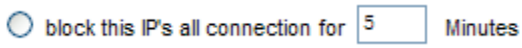
連線數管控可以控制內網的計算器最多能同時建立的連線數。這個功能對網管人員在控制內網使用 P2P 軟體如 BT、迅雷、emule 等會造成大量發出連線數的軟體提供了非常有效的管理。設置恰當的容許連線數可以有效控制 P2P 軟體時所能產生的連線數，相對也使頻寬使用量達到一定的限制。

另外，若電腦中了類似衝擊波的病毒而產生大量對外發連線請求時，也可以達到抑制做用。

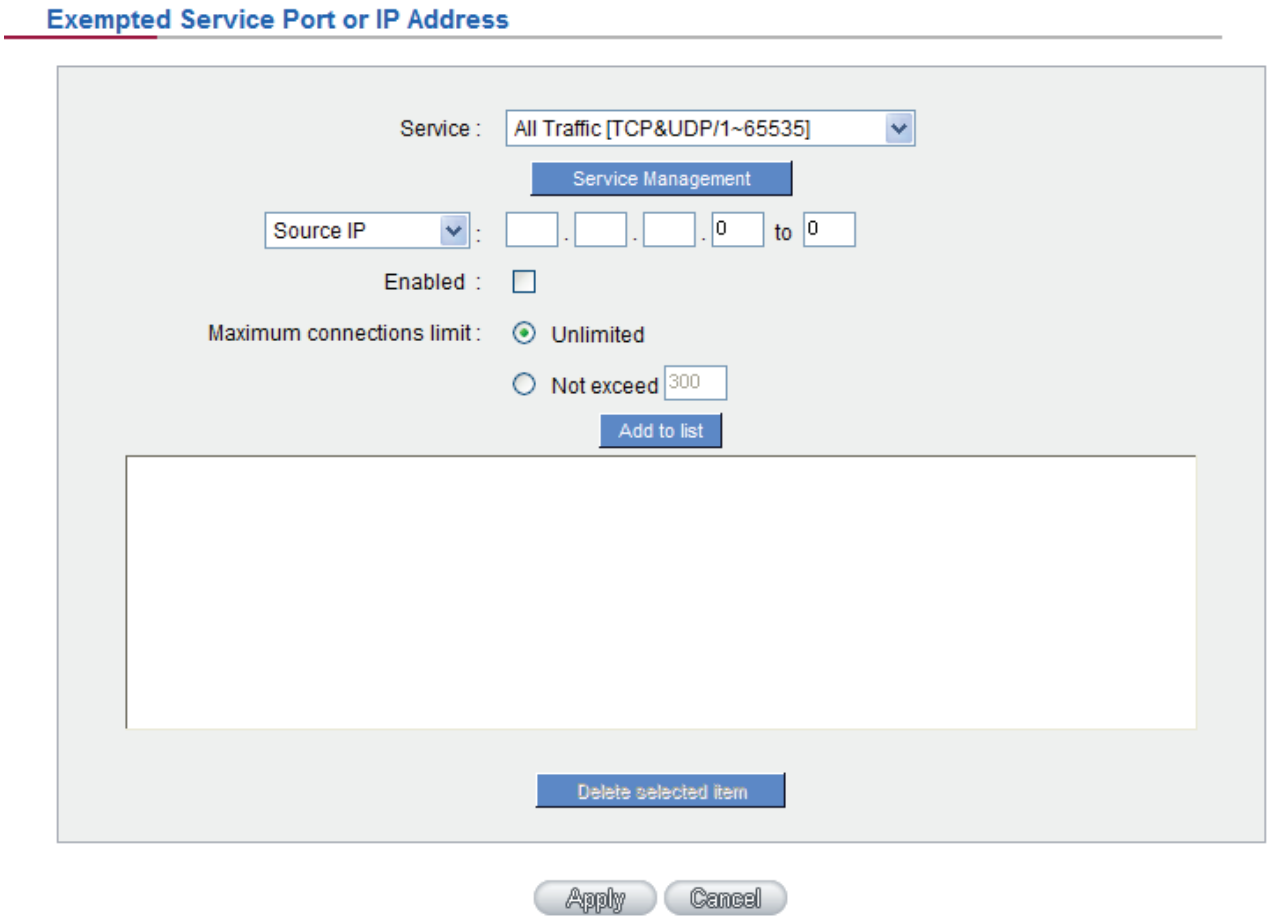
Session Control and Scheduling：



Disabled：	不使用此連線數管控功能。
Single IP cannot exceed __ session：每一區域網路 IP 最大對外 Session 不可超過__連線狀態	此選項爲限制每一台內網的電腦最大可建立的對外連線數，當用戶電腦使用連線數到達此限制值時，要建立新的連線必須等到之前的連線結束後才能再建立。例如，當用戶使用 BT 或 P2P 等下載時且連線數超過此設定值後，當用戶又要再開其他服務時會無法使用，除非將使用中的 BT 或 P2P 軟體關閉。

When single IP exceed __ : 當單一個 IPSession 數到達__連線狀態	 此選項爲當用戶端電腦使用的連線數到達您的設定數值時，此用戶在 5 分鐘之內將不能再增加新連線，就算舊連線已經結束，也必須等到設定時間過後才能再建立新的連線。  此選項爲當用戶端電腦使用的連線數到達您的設定數值時，此用戶正在使用的所有連線都將被清除，且在 5 分鐘之內將不能建立任何連線(不能上網)，必須等到設定時間過後才能再建立新的連線。
Apply：	點擊此按鈕“**Apply**”即會儲存剛才所變動的修改設定內容參數。
Cancel：	點擊此按鈕“**Cancel**”即會清除剛才所變動的修改設定內容參數，此操作必須於確認儲存動作之前才會有效。

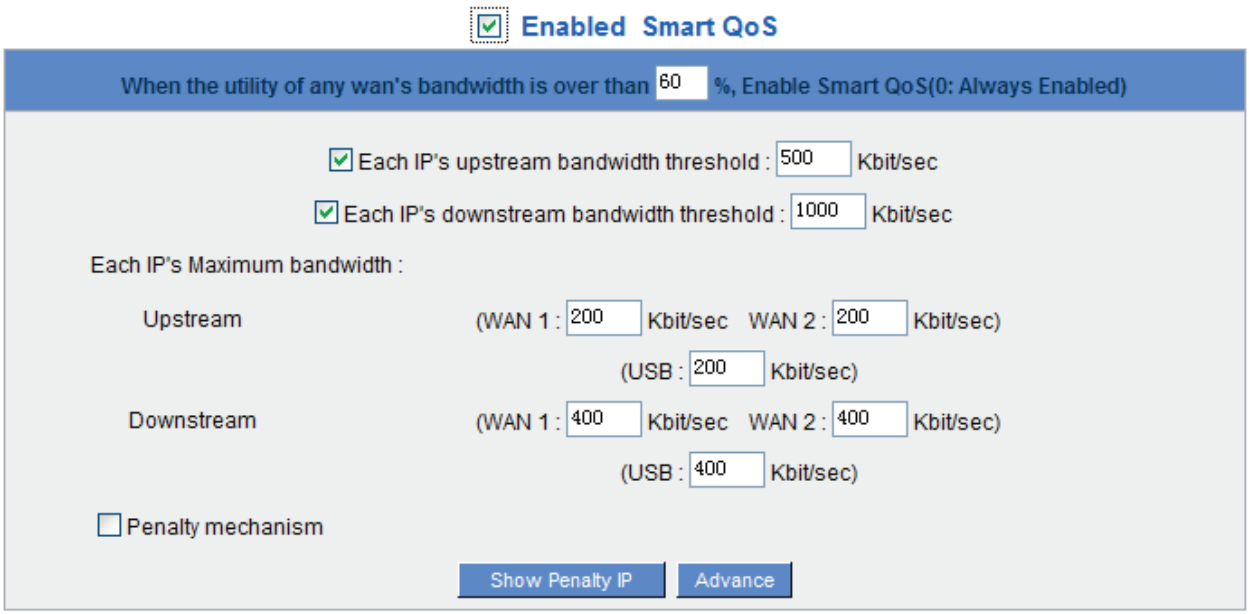
Exempted Service Port or IP Address -不受限制的服務或 IP 位址



Service Port	選擇不受限制的服務埠。
Source IP	輸入不受限制的 IP 位址範圍，或者選擇不受限制的 IP 群組。
Enabled	啓用此規則。
Add to list	將添加的規則增加到列表中。
Delete seleted item	選擇列表中的規則，刪除選中的規則。
Apply	點擊此按鈕“**Apply**”即會儲存剛才所變動的修改設定內容參數。
Cancel	點擊此按鈕“**Cancel**”即會清除剛才所變動的修改設定內容參數，此操作必須於確認儲存動作之前才會有效。

8.3 Smart QoS – 動態智能 QoS

無需網管進行配置的智慧型頻寬管理 Smart QoS 功能，自動壓抑佔用頻寬用戶，來解決內網 QoS 管理簡化網管的管理工作。



Enabled QoS **啓用動態智慧 QoS**	勾選 **Enabled QoS**。
When the usage of any WAN's bandwidth is over than___%, Enable Smart QoS **總頻寬利用率達到___%時，啓動動態智慧型 QoS**	當頻寬使用率到達實際頻寬的一個%比時，將啓用活智慧 QoS，您可輸入需要的數值，系統預設是 60%。
Each IP's upstream bandwidth threshold (for all WAN) **最大整體使用上傳頻寬**	當頻寬使用率超過設定的啓動百分比時，系統自動檢查單一 PC IP 的上傳下載使用頻寬，若超過設定的值，將給予懲罰，請填入內網 IP 上傳最大容許使用頻寬。 由於 Smart QoS 進行頻寬檢查時，可能會消耗影響部分系統效能，所以假設不太需要管制上傳頻寬，您可以取消勾選此項目表示不檢查上傳頻寬的使用狀態。

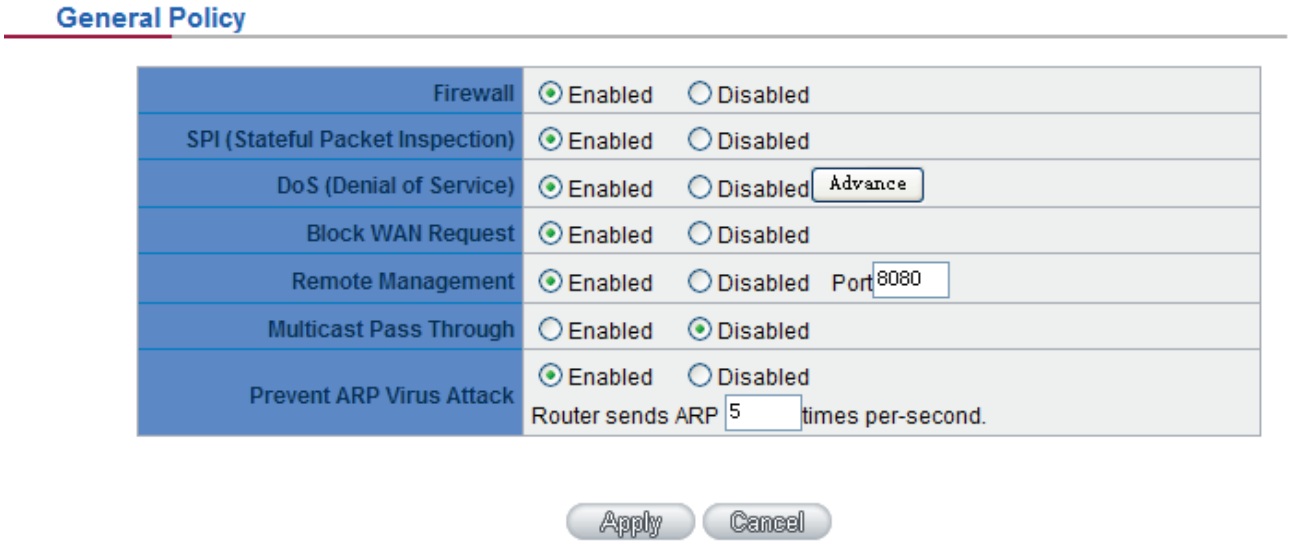
Each IP's downstream bandwidth threshold (for all WAN) **最大整體使用下載頻寬**	當頻寬使用率超過設定的啓動百分比時，系統自動檢查單一 PC IP 的上傳下載使用頻寬，若超過設定的值，將給予懲罰，請填入內網 IP 下載最大容許使用頻寬。 由於 Smart QoS 進行頻寬檢查時，可能會消耗影響部分系統效能，所以假設不太需要管制下載頻寬，您可以取消勾選此項目表示不檢查下載頻寬的使用狀態。
If any IP's bandwidth is over maximum threshold, its maximum bandwidth will remain **當任一 IP 使用超過上述設定上傳或下載頻寬時，此 IP 則使用下列指定頻寬**	當任一 IP 使用超過上述設定上傳或下載頻寬時，就實行懲罰措施，並以各個廣域網路的上傳 / 下載分別設定，懲罰後允許使用的頻寬是多少
Enabled Penalty Mechanism **啓用懲罰機制**	點選勾選"**Enabled Penalty Mechanism**"後，內部設置好二次懲罰條件，當內部網路上網用戶上網過程中的上傳與下載達到內部條件將執行二次懲罰。
Show Penalty IP **顯示處罰列表**	點選後，在彈出的對話方塊中將會顯示處罰中的 IP，上行限制中，下載限制中以及二次懲罰資訊。
Scheduling **排程**	假如選取"**Always**"，此規則將永遠被執行。 選取"**From…**"，此規則將根據輸入的時間範圍執行，例如設定週一至週五 8:00am to 6:00pm。

IX. Firewall - 防火牆

本章節介紹防火牆設定的選項，以及網路存取控制的設定，保證網路的安全性。

9.1 General Policy – 基本設置

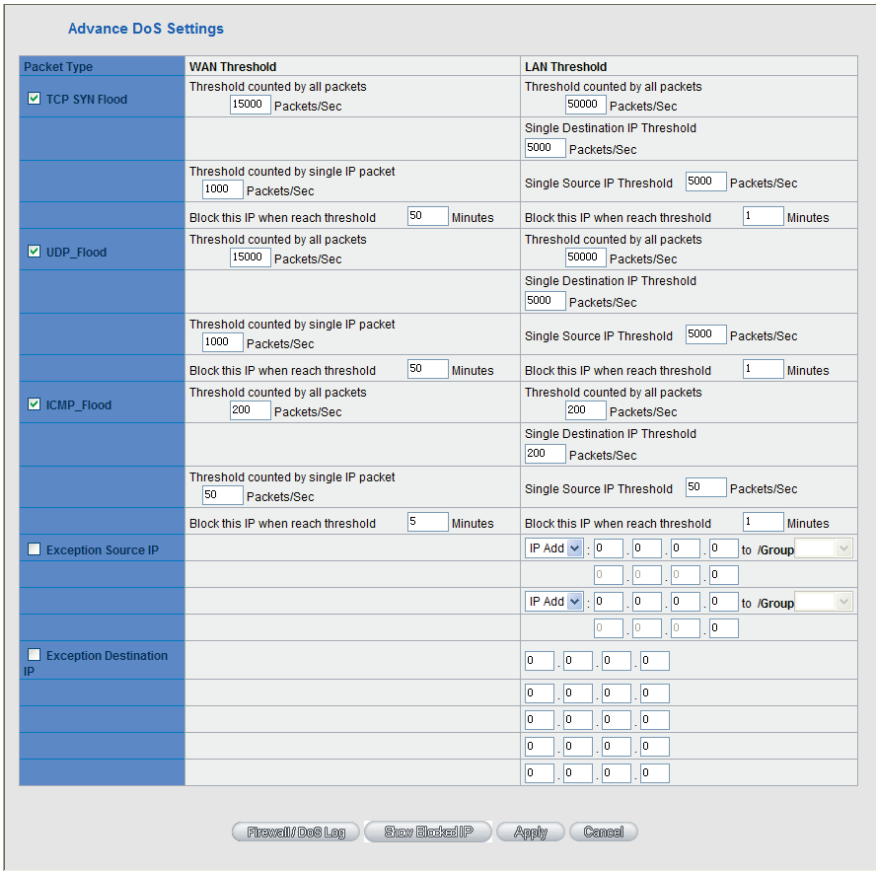
從防火牆功能的一般設定選項當中， 您可以控制開啓或是關閉這些選項功能。出廠預設值是將防火牆開啓，並關閉不必要的回應。



Firewall：	此爲選擇開啓或關閉防火牆功能。預設啓動。
SPI (Stateful Packet Inspection)： **SPI 封包狀態檢測功能**	此爲封包主動偵測檢驗技術，防火牆主要運作在網路層，但是藉由執行對每個連結的動態檢驗，也擁有應用程式的警示功能。同時，封包檢驗型防火牆可以拒絕非標準的通訊協定所使用的連結。預設啓動。
DoS (Denial of Service) **防止 DoS 攻擊**	此爲保護 DoS 攻擊，如 SYN Flooding，Smurf，LAND，Ping of Death， IP Spoofing 等。預設啓動。
Block WAN request **不回應廣域網路端請求**	若是選擇啓動的話，則路由器會關閉對外的 ICMP 與不正常連線的封包回應，所以若是您從外部去 ping 此台路由器的 WAN IP 是無法 ping 通的，預設值爲開啓拒絕對外回應的功能。
Remote Management **遠距管理功能**	遠端管理功能，若您要通過遠端網路 直接連線進入路由器的設定視窗，必需將此功能開啓，並于遠端於流覽器網址填入路由器的外部合法 IP 位址(WAN IP)，並加上預設可修改的控制埠(預設爲 80，可更改)。

Multicast Pass Through **允許 Multicast 封包穿透模式**	網路上有許多影音串流媒體，使用廣播方式可以讓用戶端接收此類封包訊息格式。預設爲關閉
Prevent ARP Virus Attack **ARP 攻擊防禦**	此功能爲防止內網遭受 ARP 欺騙攻擊而造成電腦無法上網，此 ARP 病毒欺騙大多在網吧環境發生，會讓所有上網電腦一瞬間掉線或部份電腦無法上網。開啓此功能可以避免此種病毒攻擊。

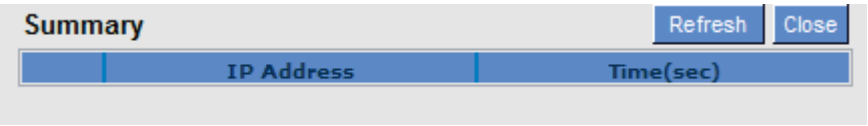
Advanced Setting
高階設定



封包類型: 路由器提供三種資料封包傳輸類型，包括 TCP-SYN-Flood、UDP-Flood 以及 ICMP-Flood。

廣域網值設定：防止來自外部網路的攻擊。設定"所有封包閥值"（即外部攻擊的所有封包資料），當其達到一個最大值（預設 15000pakets/Sec），路由器將只允許通過所設定最大值的封包數。當單一封包閥值（外部單一一個 IP 位址攻擊的封包資料）達到一個最大值（預設 1000pakets/Sec），就會阻擋此 IP 上網（預設是 50 分鐘），禁止其訪問伺服器，限制其流量和連接數，從而有效保證網路的安全。這裏您可以根據需要調整你的閥值以及阻擋時間來達到對外網攻擊的有效防護，建議其閥值從大到小來調節，避免閥值過小影響正常網路的運行。

區域網路閥值設定：防止來自內部網路的攻擊。同樣，當所有封包閥值（即外部攻擊的所有封包資料）達到一個最大值（預設 50000pakets/Sec），路由器將只允許通過所設定最大值的封包數。當單一封包閥值（內部單一一個 IP 位址攻擊的封包資料）達到一個最大值（預設 5000pakets/Sec），就會阻擋此 IP 上網（預設是 1 分鐘），禁止其訪問伺服器，限制其流量和連接數，從而有效保證網路的安全。您可以根據需要調整你的閥值以及阻擋時間來達到對內網攻擊的有效防護，建議其閥值從大到小來調節，避免閥值過小影響正常網路的運行。

Exception Source IP **例外來源 IP**	指定某些來源端的 IP 地址/群組 不受到閾值的限制。
Exception Dest. IP **例外目的 IP**	指定某些目的端的 IP 位址/群組 不受到閾值的限制。
Show Blocked IP **顯示被阻擋的 IP**	 顯示被 DOS 防禦功能所阻擋的 IP 位址，以及該 IP 位址還剩餘多少時間解除阻擋。
Apply：	點擊此按鈕“**Apply**”即會儲存剛才所變動的修改設定內容參數。
Cancel：	點擊此按鈕“**Cancel**”即會清除剛才所變動的修改設定內容參數，此操作必須於“確定”儲存動作之前才會有效。

9.2 Access Rule – 訪問規則設置

安全路由器設計有簡而易懂的網路存取規則條例工具，管理者可以用來對不同的使用者設定不同的存取規則條件，來管理使用者對網路的存取許可權。存取規則可以依據不同的條件來過濾，例如可以設定封包要管制的進出方向是從內部到外部還是從外部到內部，或是設定以使 IP 位址、目地端 IP 位址、IP 通訊協定狀態等條件來做管制，管理者可以依照實際的需求調性設置。

管理者定訂的網路存取規則條例，可以選擇關閉或是允許來調整使用者對網路的存取。以下就針對路由器的網路存取規則條例做一說明：

路由器預設的網路存取規則條例：

*從 LAN 端到 WAN 端的所有封包可以通過-All traffic from the LAN to the WAN is allowed

*從 WAN 端到 LAN 端的所有封包不可以通過-All traffic from the WAN to the LAN is denied

*從 LAN 端到 DMZ 端的所有封包不可以通過-All traffic from the LAN to the DMZ is denied

*從 DMZ 端到 LAN 端的所有封包不可以通過-All traffic from the DMZ to the LAN is denied

*從 WAN 端到 DMZ 端的所有封包不可以通過-All traffic from the WAN to the DMZ is denied

*從 DMZ 端到 WAN 端的所有封包不可以通過-All traffic from the DMZ to the WAN is denied

管理者可以自定存取規則並且超越路由器的預設存取條件規則，但是以下的四種額外服務專案

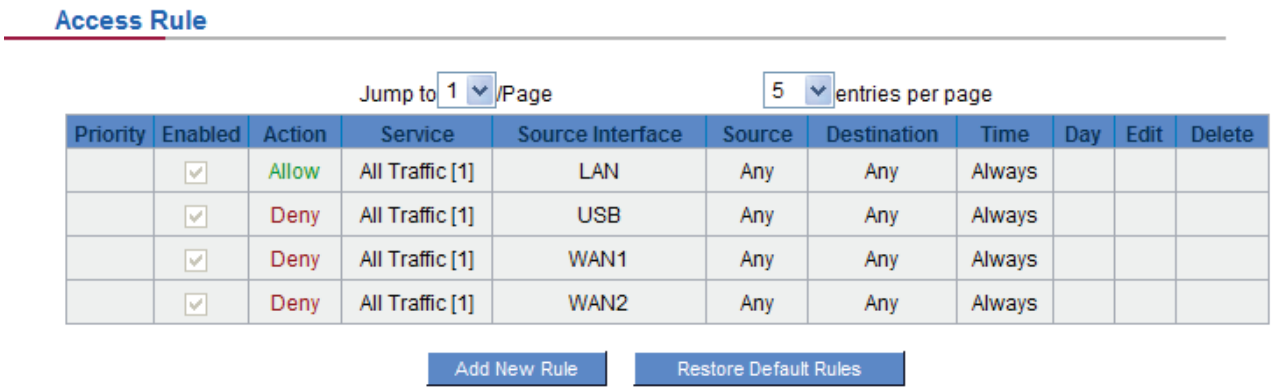
爲永遠開啓，不受其他自定規則所影響：

* HTTP 的服務從 LAN 端到路由器預設爲開啓的 (爲了管理路由器使用)。

* DHCP 的服務從 LAN 端到路由器預設爲開啓的 (爲了從路由器自動取得 IP 位址使用)。

* DNS 的服務從 LAN 端到路由器預設爲開啓的 (爲了解析 DNS 服務使用)。

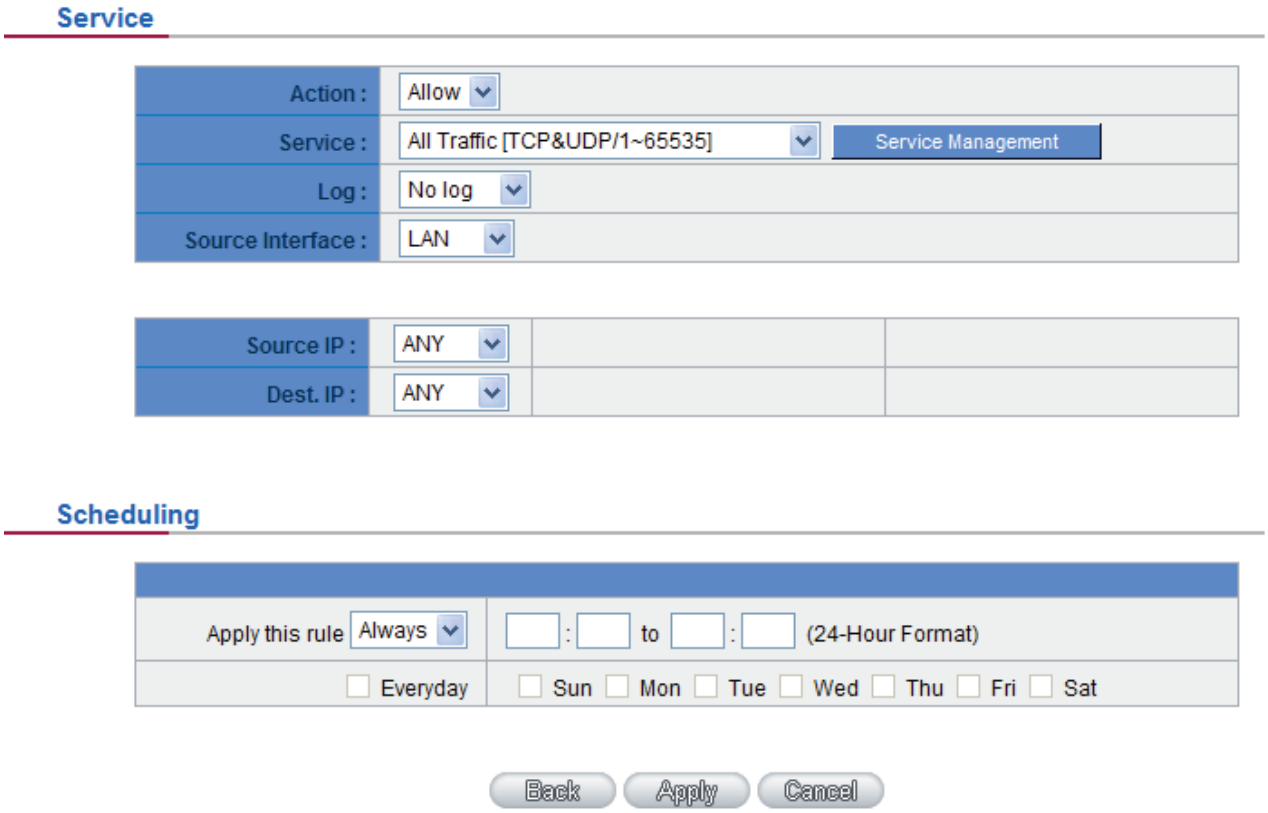
* Ping 的服務從 LAN 端到路由器預設爲開啓的 (爲了連通測試路由器使用)。



除了預設規則以外， 所有的網路存取規則都會顯示於此規則列表中，您可以自己選擇高低優先權於每一個網路存取規則專案中。路由器在做規則確認時是依照優先權。依序做規則判斷，所以優先權是讓您在做存取規則的設定規劃中必須要考慮的，以避免您想開啓或關閉的功能失效。

Edit **編輯**	可以設定網路存取規則專案。
Delete **垃圾桶圖像**	可以刪除網路存取規則專案。
Add New Rule **增加新的管制規則**	新增新的網路存取規則按鈕可以新增一項新的存取規則。
Restore to Default Rule **恢復到出廠預設值**	可以恢復到出廠原有預設存取規則專案並刪除所有的自定規則內容。

9.2.1 Add New Access Rule - 增加新的管制規則

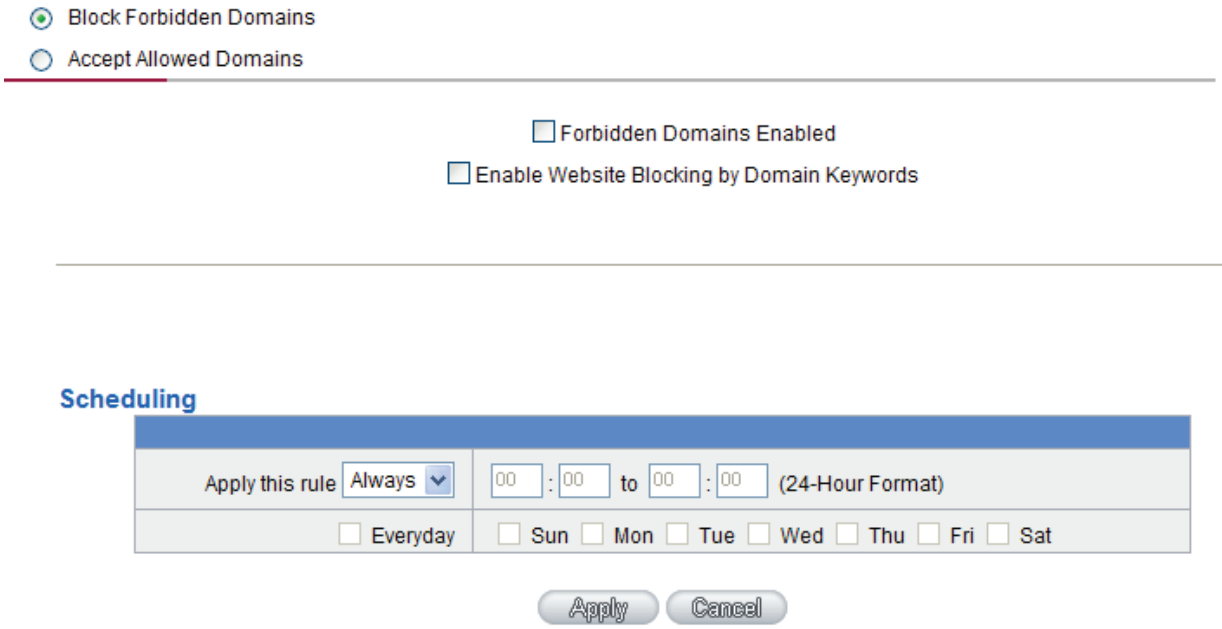


Action **啓動**	Allow： 允許符合此管制條例行爲的封包通過。 Deny： 不允許符合此管制條例行爲的封包通過。
Service **服務埠口**	從下拉式選單中選擇您所要允許或不允許的服務埠服務專案內容。
Service Management **服務埠增刪表**	若是您想要管制的服務埠服務內容沒有存在於預設列表內的話，您可以點擊右方的服務端新增或刪除表來新增一個服務內容。於彈出視窗中輸入一個服務名稱以及通訊協定與埠，點擊“Add to list”按鈕即可新增一個管制服務專案內容。
Log **日誌**	Create Log when matched: 依據此規則發生的相關事件將在日誌中記錄。 No Log: 依據此規則發生的相關事件不會日誌中記錄。
Source Interface **來源界面**	選擇您所要允許或不允許的來源封包界面(例如是從 LAN，WAN1， WAN2 還是任何的)，可以從下拉式選單中選擇。
Source IP **來源 IP 地址**	選擇來源封包的 IP 範圍(如任何的，單獨或者範圍)，若是選擇單獨是範圍的話，請輸入此單一或是一區段範圍的 IP 位址。
Dest. IP **目的 IP 位址**	選擇目的端封包的 IP 範圍(如任何的，單獨或者範圍)，若是選擇單獨是範圍的話，請輸入此單一或是一區段範圍的 IP 位址。

Scheduling **時間管制設定**	您可以將此條規則依照您所需要的執行時間來做控管。例如您可以設定此規則每天上午 8：00 開始執行下午 17：00 結束，或 24 小時都執行管制。
Apply this rule **應用此存取規則**	選擇“Always”表示都 24 小時都執行此規則(預設)，或是可以選擇從幾點到幾點”From”，以及設定是每天還是某幾天做管制。
… to …	…to…： 此管制規則有時間限制，設定方式爲 24 小時制，如 08：00 到 18：00 (早上 8 點到下午 6 點)。
Day Control **管制天數**	勾選“Everyday”是表示每一天的這段時間都受控管，若是只針對一星期特定星期幾，可以直接選擇星期。
Apply：	回到訪問規格設定頁面。
Cancel：	點擊此按鈕“**Apply**”即會儲存剛才所變動的修改設定內容參數。
	點擊此按鈕“**Cancel**”即會清除剛才所變動的修改設定內容參數，此操作必須於確認儲存動作之前才會有效。

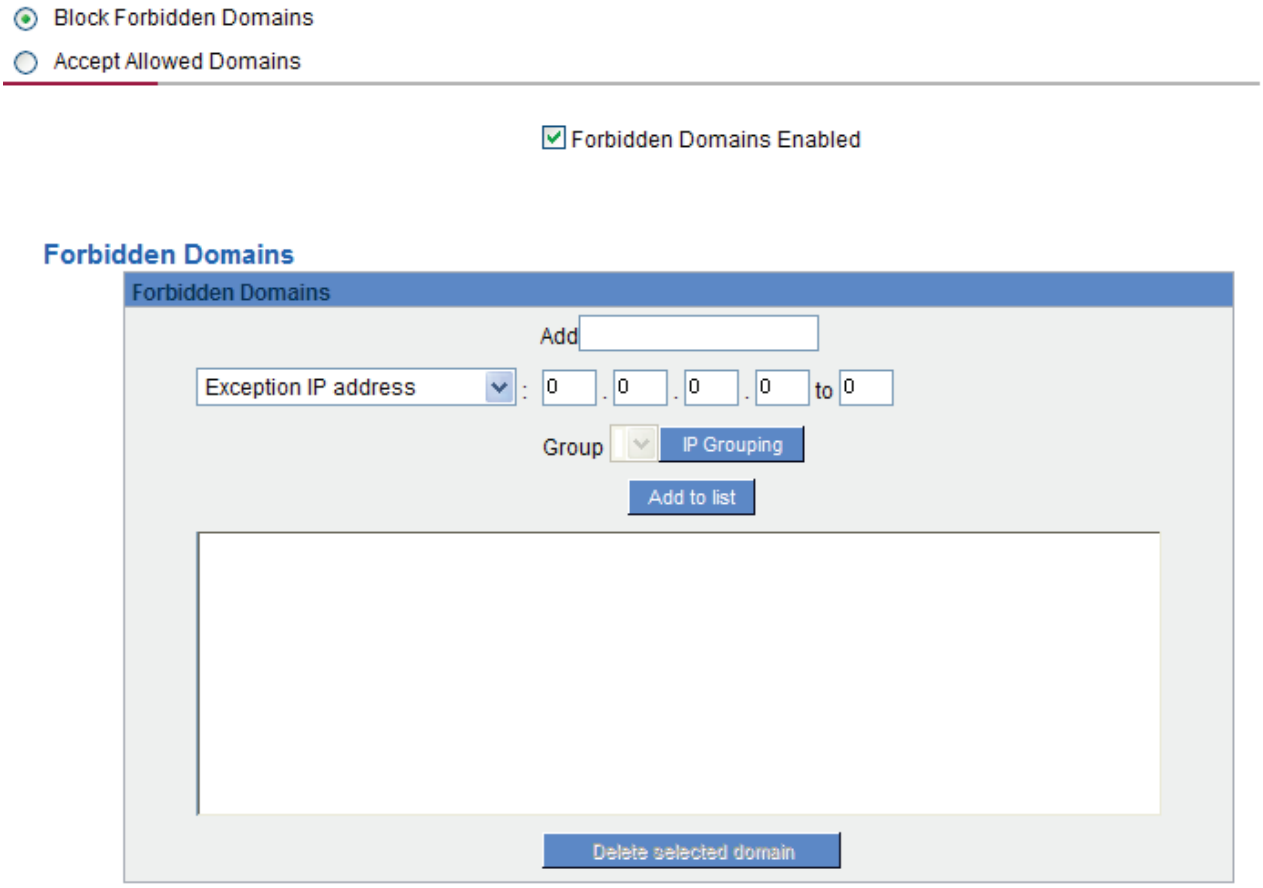
9.3 URL Filter - 網頁內容管制

路由器的網頁內容管制可支援兩種模式的網頁管制，一爲 **Block Forbidden Domains** - 封鎖不允許訪問的網址，另一個爲 **Accept Allowed Domains** - 允許訪問的網站，此兩種模式只能使用一種。



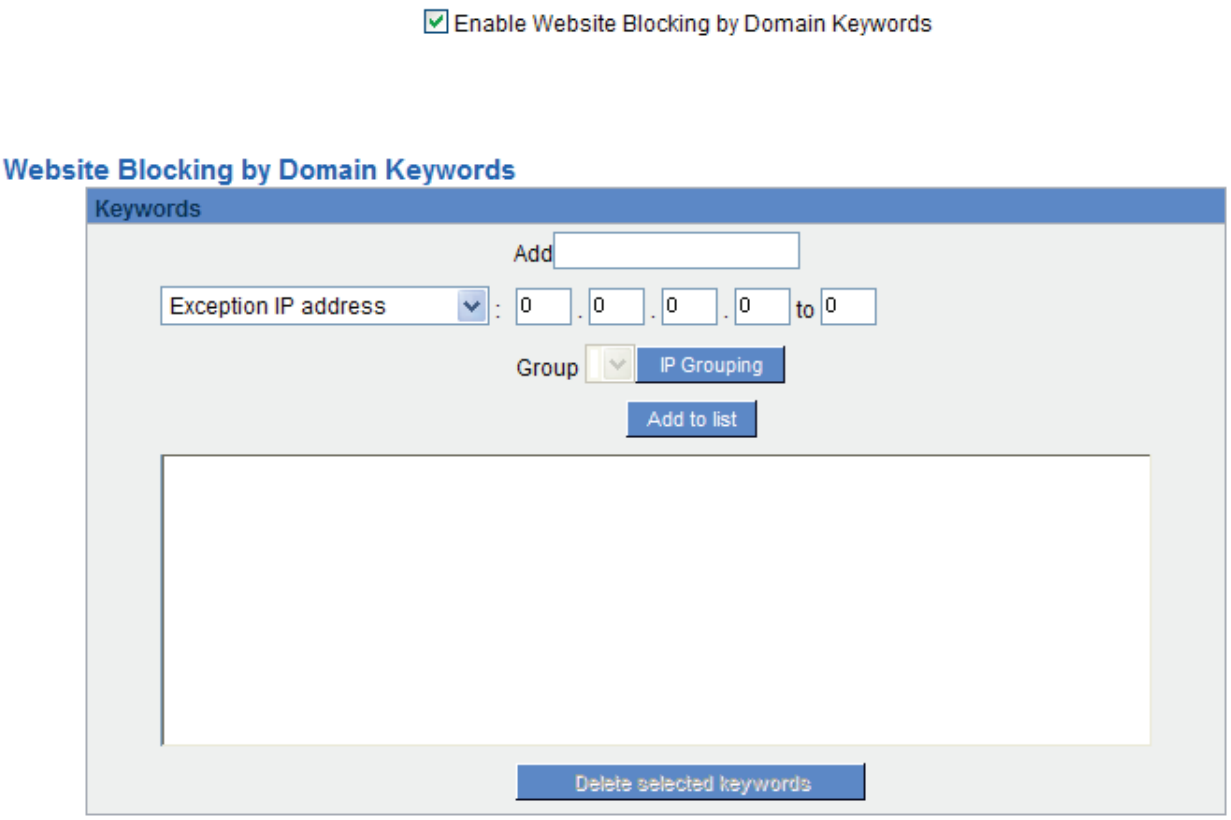
Block Forbidden Domain -封鎖不允許訪問的網址

此功能需將完整的網址如 www.sex.com 填入，即可封鎖此網站。



Add：	填寫欲管制的網址，如 www.playboy.com。
Add to list：	點擊”**Add to list**”按鈕新增此一欲管制的網址。
Delete selected item：	可以使用滑鼠點選一個或多個管制的網址，然後點擊即可刪除。

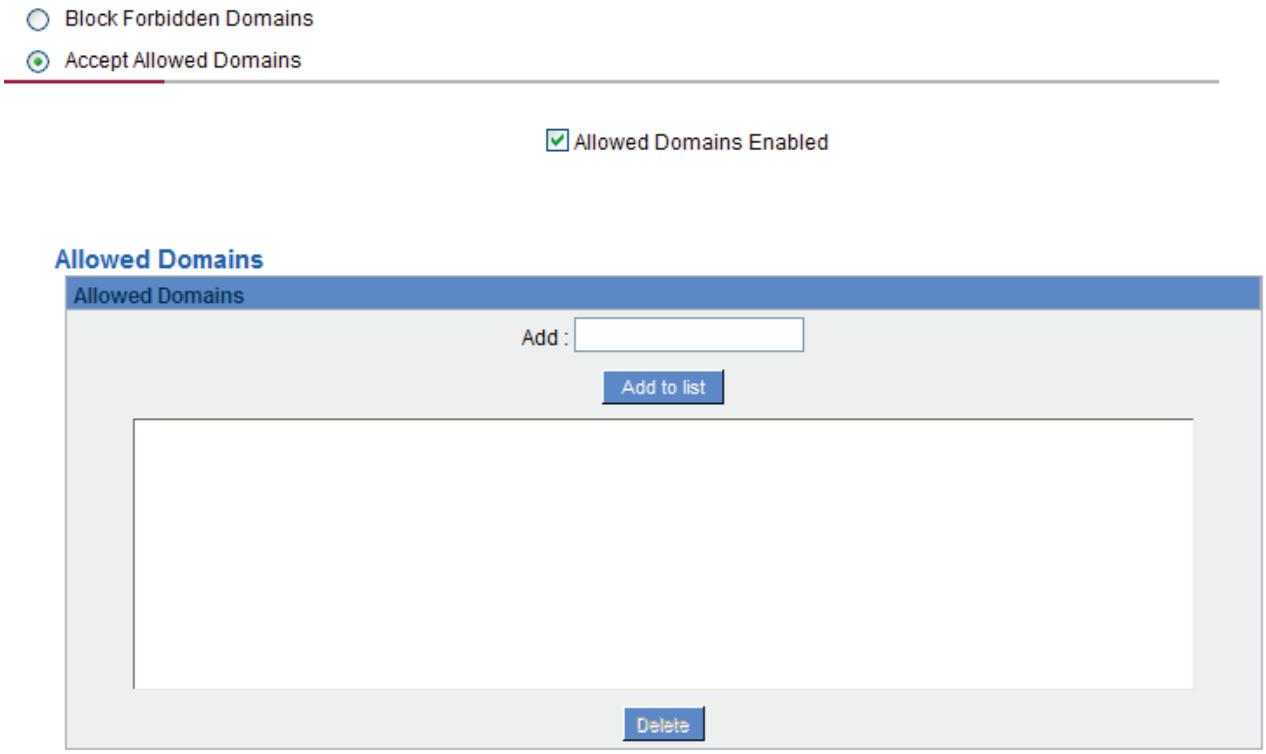
Website Blocking by Keywords -網頁關鍵字管制



Enabled：	當此項功能啓動後，當輸入網站位址有存在“sex”關鍵字時，則路由器會將所有有“sex”的網頁封鎖。
Keywords（Only for English keyword）網頁字串管制 (僅限英文)	輸入關鍵字。
Add to List：	增加此新增的服務專案內容到服務表列內。
Delete selected item：	選擇刪除服務專案內容從服務表列內。
Apply：	點擊此按鈕“**Apply**”即會儲存剛才所變動的修改設定內容參數。
Cancel：	點擊此按鈕“**Cancel**”即會清除剛才所變動的修改設定內容參數，此操作必須於“確定” 儲存動作之前才會有效。

Accept Allowed Domains -允許訪問的網站

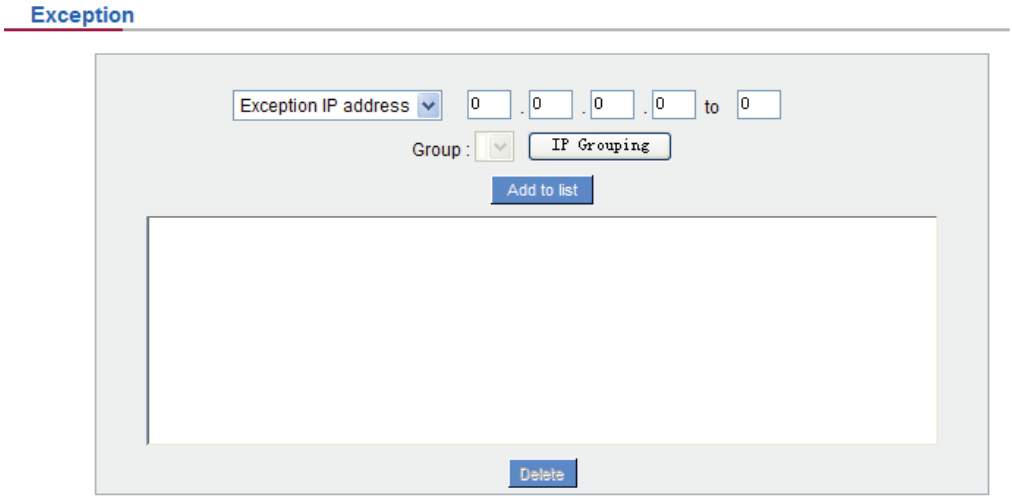
此功能的目的是設定只能去訪問的網址，在有些公司或學校中，會只允許員工或學生只能去哪些網站，就可以用此功能來達成。



Enabled	選擇打勾開啓允許網址管制功能，預設爲關閉。
Add	填寫欲管制的允許網址，如 www.playboy.com。
Add to list	點擊此按鈕新增此欲管制的允許網址。
Delete selected item	可以使用滑鼠點選一個或多個管制的允許網址，然後點擊即可刪除。

Exception IP[Tina2] - 不受限制的 IP

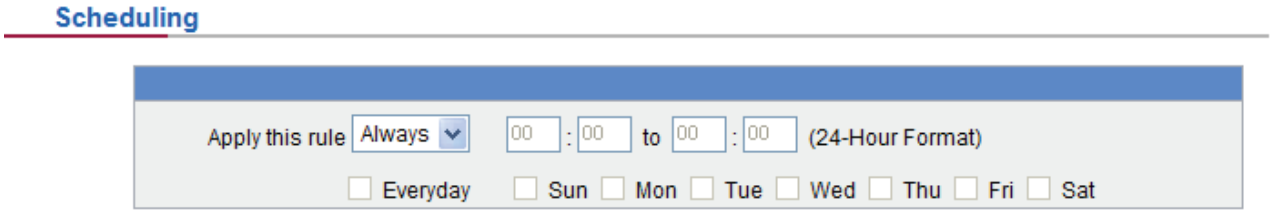
若是有 IP 地址或是 IP 群組不希望受到”Allowed Domains Enabled”的管制，可以在這裡將這些 IP 排除。



Exception IP address **例外 IP 位址/群組**	輸入不受限制的 IP/IP 範圍。
Add to list **增加到對應列表**	點擊此按鈕新增此不受限制的 IP 或 IP 群組。
Delete selected item **刪除所選擇的內容**	可以使用滑鼠點選一個或多個不受限制的 IP 或 IP 群組，然後點擊即可刪除。

Content Filter Scheduling -管制內容排程時間

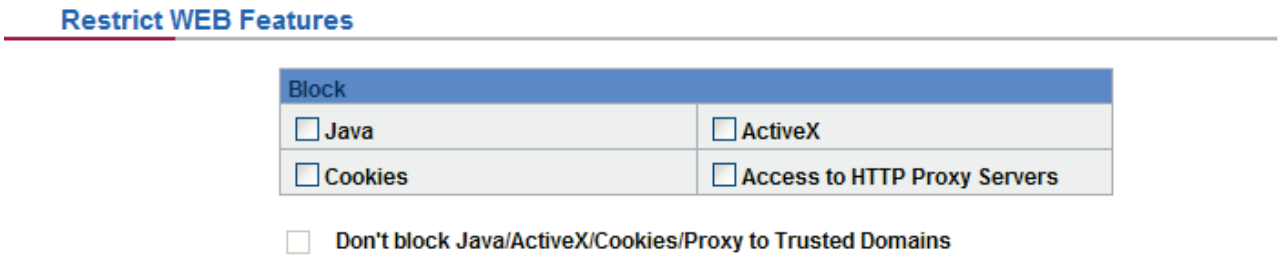
當選擇爲“**Always**”時，表示此條規則 24 小時執行。若選擇“**from**”時，此管制條例會依據所設定的生效時間去執行此條規則，如管制時間爲週一到週五，早上八點到下午六點，您可以參考以下圖例來管制。



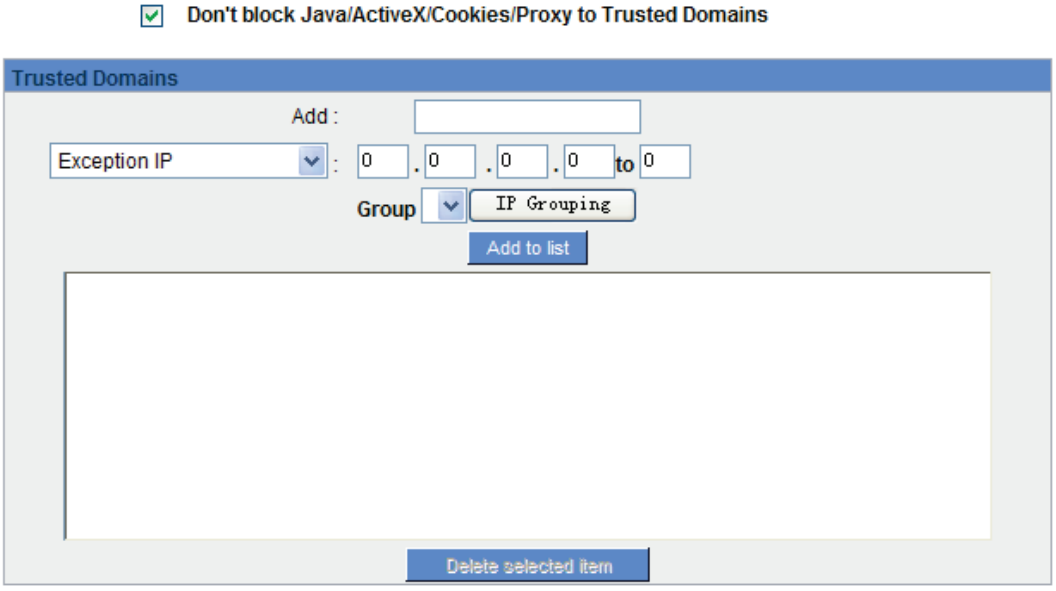
Always	表示此管制規則 24 小時開啓。
from…to…	此管制規則有時間限制，設定方式爲 24 小時制，如 08：00 到 18：00 (早上 8 點到下午 6 點)。
管制天數	勾選“**Everyday**”是表示每一天的這段時間都受控管，若是只針對一星期特定星期幾，可以直接選擇星期。

9.4 Internet Filter – 網際網路過濾功能

Restrict WEB Features – 限制網頁功能

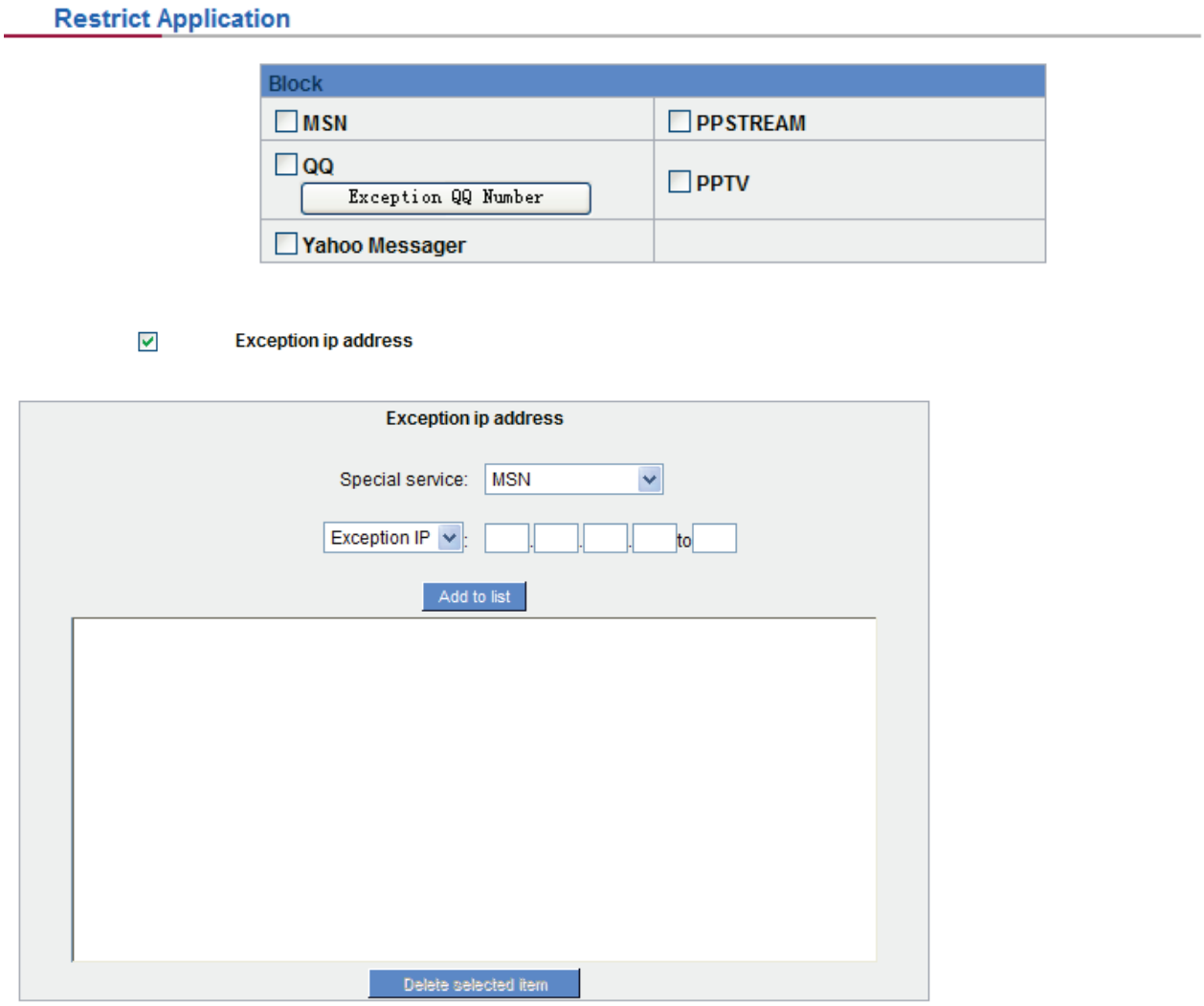


Restricted WEB Features **阻擋特定網頁功能**	可支援阻擋格式如下: Java, Cookies, Active X, and HTTP Proxy access.
Don't block Java/ActiveX/Cookies/Proxy to Trusted Domains **不要阻擋信任網域網頁功能**	加入信任網域，在這些網域中的網頁功能不予阻擋。
Apply：	點擊此按鈕“**Apply**”即會儲存剛才所變動的修改設定內容參數。
Cancel：	點擊此按鈕“**Cancel**”即會清除剛才所變動的修改設定內容參數，此操作必須於“確定”儲存動作之前才會有效。



Restrict Application - 阻擋特定服務

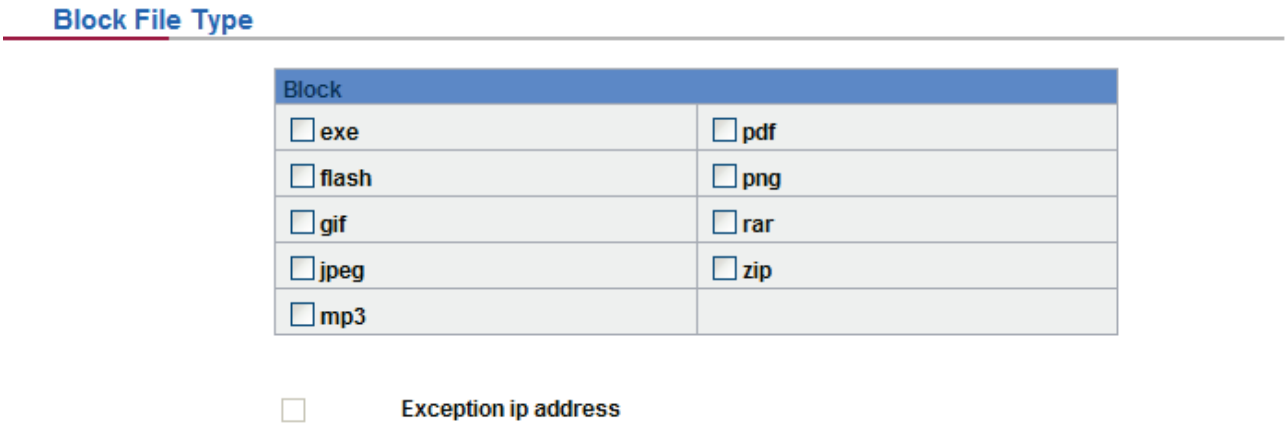
針對目前較多人使用的應用服務進行封鎖管制，例如即時通訊 IM、P2P 下載軟體或網路視訊軟體等。



進行 QQ 封鎖之後，仍可以針對不需受到限制的使用者開放 QQ 服務，此時就要將這些使用者 QQ 號碼加入到不受限制的 QQ 號碼清單之中

User Name 使用者名稱	輸入 QQ 號碼使用者資訊。
Exempted QQ Number 例外 **QQ** 號碼	輸入 QQ 號碼。
Add to list 加入清單	將此號碼加入清單。
Delete selected item 刪除選擇項目	刪除清單中所選擇的號碼。

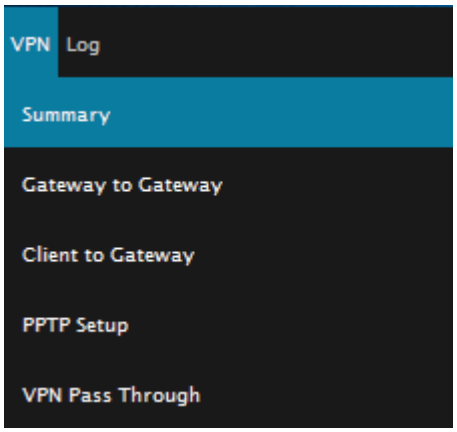
Block File Type – 阻擋特定檔案類型

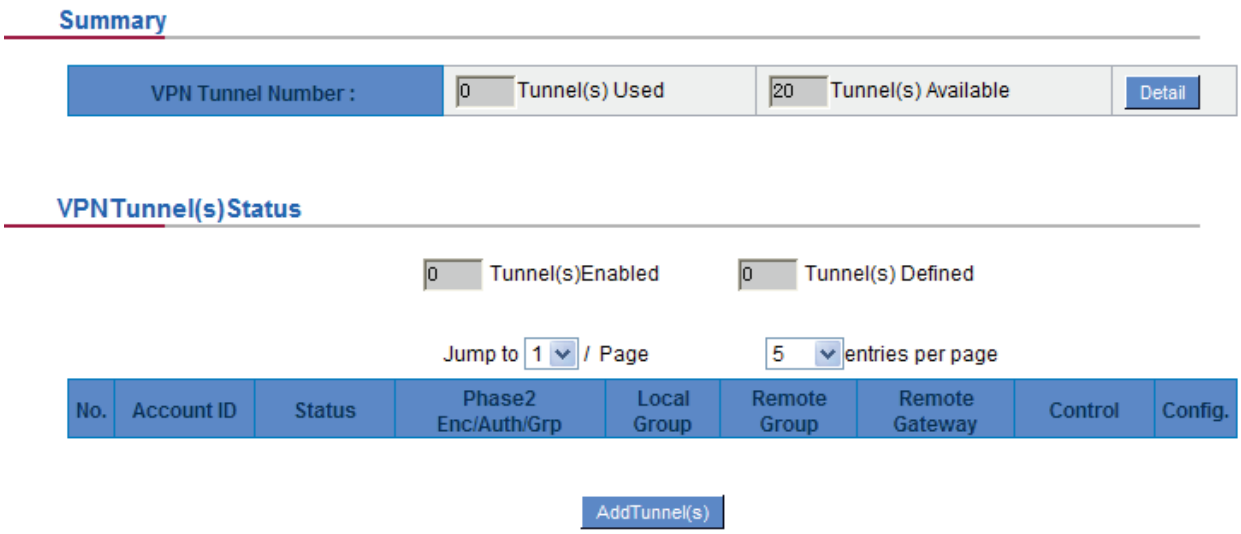


可以選擇特定檔案類型進行阻擋，亦可設置例外 IP。

X. VPN (Virtual Private Network) - 虛擬專用網設置

10.1. VPN



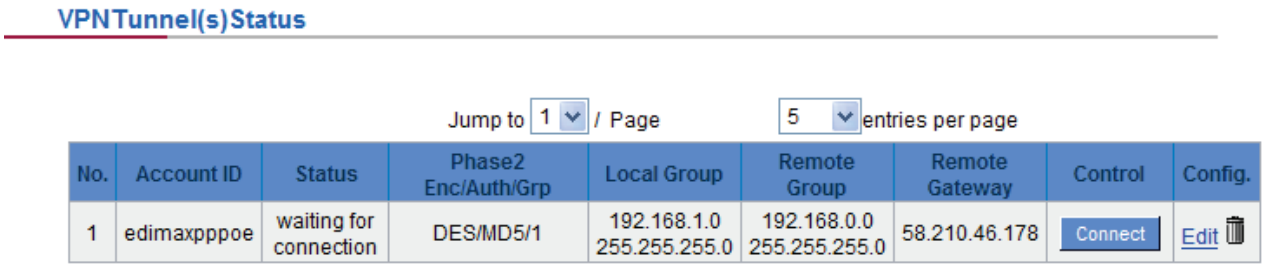


10.1.1. 目前所有的 VPN 狀態顯示

此 VPN 狀態可以顯示目前有關 VPN 方面的即時狀態。

Tunnel Status - **VPN 隧道目前狀態顯示**

以下就針對"VPN Tunnel Status" VPN 隧道目前狀態顯示做完整解說:



__ Tunnel(s) Enabled **_條隧道已啓用** **__ Tunnel(s) Defined** **_條隧道已設定**	顯示多少條隧道已被啓用或設定。
Previous Page/Next Page, Jump to __/__ Page, __ Entries Per Page **上一頁/下一頁、跳到__/__頁、每頁顯示的欄位**	您可以按下上一頁與下一頁按鈕跳到您想監看的VPN隧道畫面上，或者您可以直接選擇每一次所顯示的頁次，來監看您的所有 VPN 隧道狀態，如(3，5，10，20，All)
Tunnel No.	當您設定 VPN 防火牆內建之 VPN 功能時，請選擇您要設定的隧道編號
Status **狀態**	已經連線成功-（Connected） 電腦名稱解析失敗-（Hostname Resolution Failed） 解析電腦名稱（Resolving Hostname） 等待連線-（Waiting for Connection）等資訊 若是用戶選擇手動-Manual 設定 IPSec 隧道，則此狀態會顯示手動-Manual 設定與沒有測試此項手動設定功能狀態模式
Name **帳戶名稱**	目前連線 VPN 隧道連接名稱，如 XXX Office，建議您若是有一個以上的隧道設定的話，務必將每一個隧道名稱都設爲不同，以免混淆
	注意: 此隧道名稱若是您需要連接其他 VPN 設備時，有一些設備規定此隧道名稱要與主控端爲相同名稱並做驗證，此隧

	道才會順利連線開啓
Phase2 Encrypt/Auth/Group	於此顯示加密(DES/3DES)以及驗證(MD5/SHA1)以及群組 Group (1/2/5)等設定模式。
Local Group 本地群組	此爲顯示本地區域端的 VPN 連線安全群組設定。
Remote Group 遠程群組	此爲顯示遠端的 VPN 連線安全群組設定。
Remote Gateway 遠程閘道	此爲設定爲欲與遠端 VPN 設備連線的 IP 位址，請設定爲遠端的 VPN 防火牆的對外合法 IP 位址或是網域名稱等。
Control 連接控制	可以按下“**Connect**”按鈕去驗證此隧道的狀態，測試結果將會更新於此狀態上，你可以點“**Disconnect**”按鈕中斷VPN連接。
Config 配置	設定項目包含”**Edit**”以及刪除圖示。 若您按下”**Edit**” 按鈕，將會連接到此設定的項目當中，您可以修改其中的設定。若您選擇按下垃圾桶圖示的話， 所有此隧道的設定將會被刪除

10.1.2. Add a New VPN Tunnel - 新增一條 VPN 隧道

安全路由器支持閘道對閘道隧道 Gateway to Gateway 或用戶端對閘道隧道 Client to Gateway。

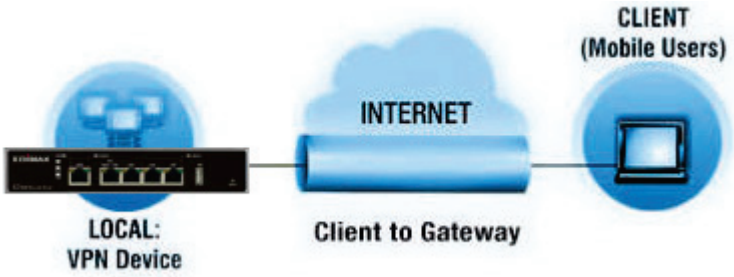
VPN 隧道連接爲 2 台 VPN 路由器，分別通過網際網路 Internet 所組成，當您按下新增一條隧道的話， 將會直接導引到 VPN 閘道對 VPN 閘道的設定或用戶端對 VPN 閘道的設定的頁面上。

Gateway to Gateway – 閘道對閘道 VPN

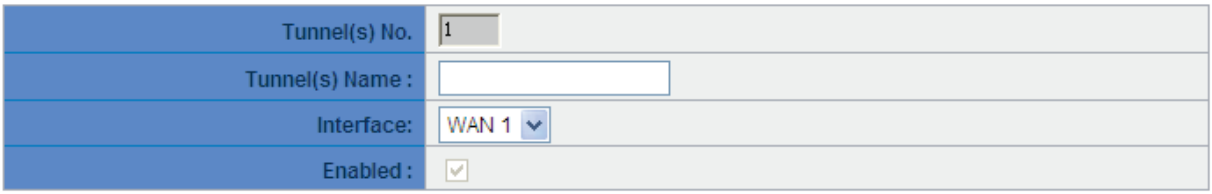
當您按下新增“Add” 的話，將會直接導引到 VPN 閘道對 VPN 閘道的設定頁面上。

Client to Gateway – 用戶端對閘道 VPN

當您按下新增“Add” 的話，將會直接導引到用戶端對 VPN 閘道的設定頁面上。



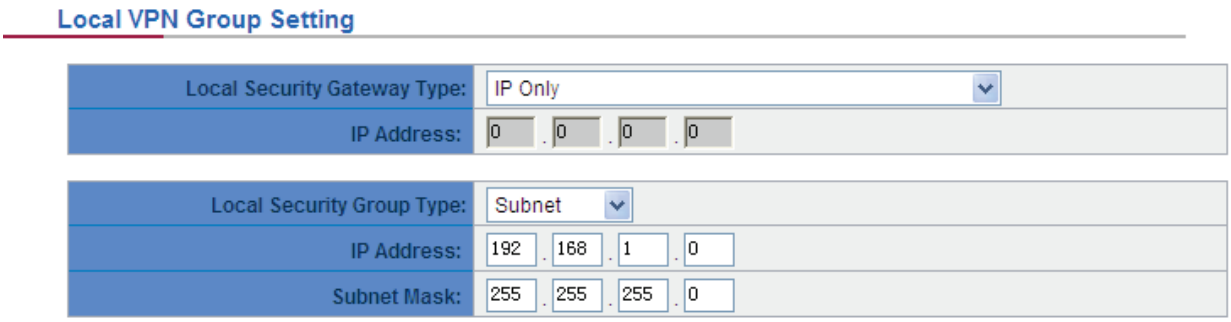
10.1.2.1. Gateway to Gateway Setting - 閘道對閘道設定



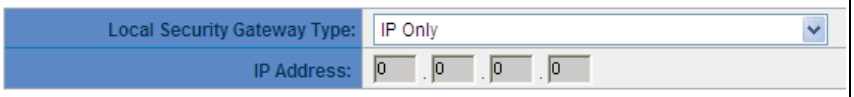
透過以下的設定說明，使用者就可以在兩台 VPN 路由器之間建立一條 VPN 隧道。

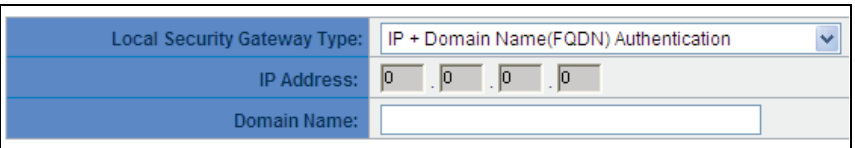
Tunnel No.	當您設定本機內建之 VPN 功能時，請選擇您要設定的 Tunnel 隧道編號
Tunnel Name	設定此隧道連接名稱，如 XXX Office，建議您若是有一個以上的隧道設定的話，務必將每一個隧道名稱都設爲不同，以免混淆
	請注意: 此隧道名稱若是您需要連接其他 VPN 設備(非此路由器)時，有一些設備規定此隧道名稱要與主控端爲相同名稱並做驗證，此隧道才會順利連線開啓！。
Interface **界面**	您可以選擇哪一個介面位置做爲此 VPN 隧道的節點
Enabled **啓動**	勾選啓用選項，將此 VPN 隧道開啓。 此項目爲預設爲啓用，當設定完成後，可以再選擇是否啓用隧道設定

Local Group Setup - 本機用戶群組配置



此項目的本地閘道身分類型(Local Security Gateway Type)必須與連接遠端的閘道身分類型(Remote Security Gateway Type)相同。

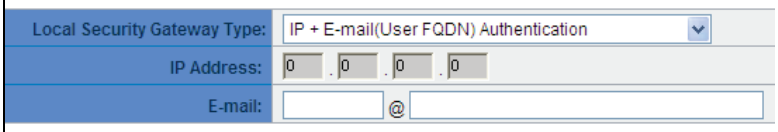
Local Security GatewayType **本地閘道身分類型**	本機閘道認證類型，有五種操作模式項目選擇，分別爲: **IP only** 僅用 IP **IP + Domain Name (FQDN) Authentication** IP + Domain Name(FQDN) 認證 **IP + E-mail Addr. (USER FQDN) Authentication** IP + E-mail (USER FQDN) 認證 **Dynamic IP + Domain Name (FQDN) Authentication** 動態 IP + Domain Name(FQDN) 認證 **Dynamic IP + E-mail Addr. (USER FQDN) Authentication.** 動態 IP + E-mail (USER FQDN) 認證 **(1) IP only** 僅用 IP 若您選擇僅用 IP 類型的話， 只有固定填入此 IP 位址可以存取此隧道，然後路由器的 WAN IP 位址，將會自動填入此項目空格內，您不需要在進行額外設定。  **(2) IP + Domain Name(FQDN) Authentication** + Domain Name(FQDN) 認證 若您選擇 IP+網域名稱類型的話，請輸入您所驗證的網域名稱以及 IP 位址然後路由器的 WAN IP 位址，將會自動填入此項目空格內，您不需要在進行額外設定。 FQDN 是指主機名稱以及網域名稱的結合，也必須存在於 Internet 上可以查詢的到，如 vpn.server.com。此 IP 位址以及網域名稱必須與遠端的 VPN 安全閘道設定類型相同才可以正確連接。



(3) IP + E-mail Addr. (USER FQDN) Authentication.

+ E-mail (USER FQDN) 認證

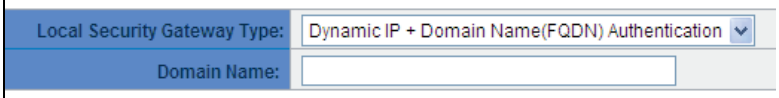
若您選擇 IP 位址加上電子郵件類型的話， 只有固定填入此 IP 位址以及電子郵件位置可以存取此隧道，然後路由器的 WAN IP 位址，將會自動填入此項目空格內，您不需要在進行額外設定。



(4) Dynamic IP + Domain Name(FQDN) Authentication

動態 IP + Domain Name(FQDN) 認證

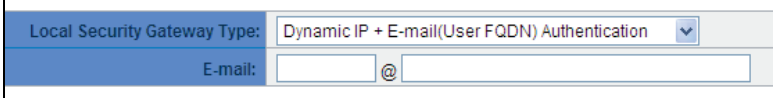
若是您使用動態 IP 位址連接路由器時， 您可以選擇此類型連接 VPN，當遠端的 VPN 閘道要求與路由器作爲 VPN 連線時，路由器將會開始驗證並回應此 VPN 隧道連線; 若您選擇此類型連接 VPN，請輸入網域名稱即可。

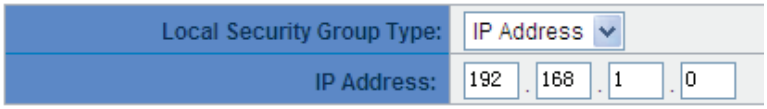
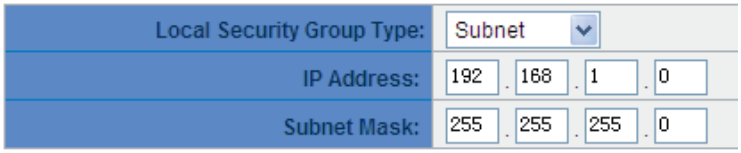


(5) Dynamic IP + E-mail Addr. (USER FQDN) thentication.

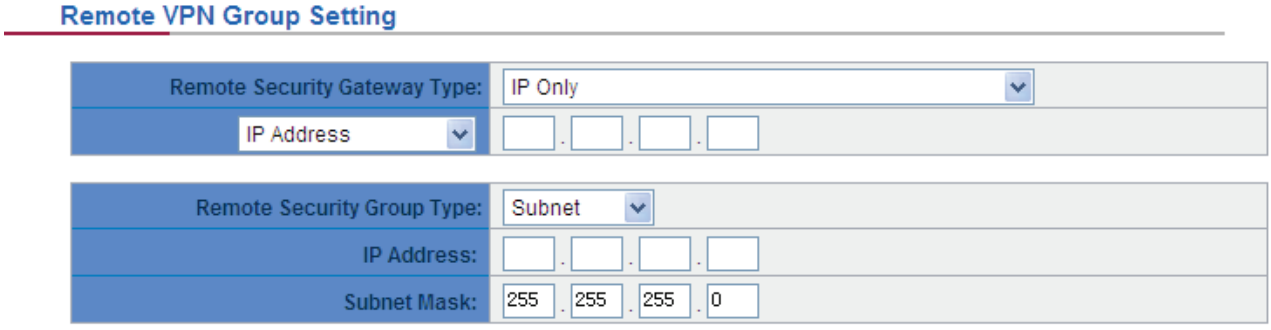
動態 IP + E-mail (USER FQDN) 認證

若是您使用動態 IP 位址連接路由器時， 您可以選擇此類型連接 VPN，使用者不必輸入 IP 位址，當遠端的 VPN 閘道要求與路由器作爲 VPN 連線時，路由器將會開始驗證並回應此 VPN 隧道連線; 若您選擇此類型連接 VPN，請輸入電子郵件認證到 E-Mail 位置空格欄位中即可。

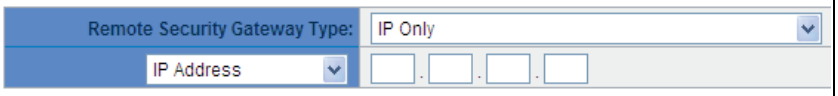
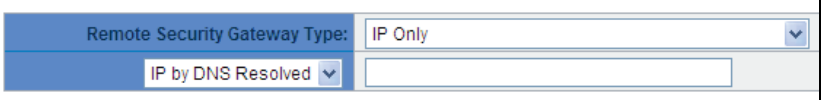


Local Security Group Type **本地安全組類型**	此爲設定本地區域端的 VPN 連線存取類型，以下有幾個關於本地區域端設定的項目，請您選擇並設置適當參數: **1. IP address** 此項目爲允許此 VPN 隧道連線後，只有輸入此 IP 位址的本地端電腦可以連線。  以上的設定參考爲:當此 VPN 隧道連線後，於 192.168.1.0 的此 IP 位址的電腦可以連線。 **2. Subnet** 此項目爲允許此 VPN 隧道連線後，每一台于此網段的本地端電腦都可以連線。  以上的設定參考爲:當此 VPN 隧道連線後，只有 192.168.1.0，子網路遮罩爲 255.255.255.0 的此網段電腦可以與遠端 VPN 連線。

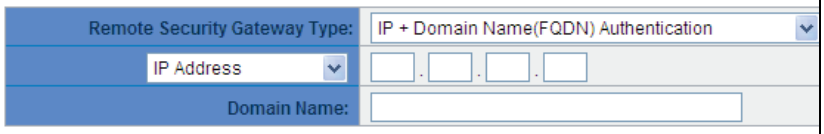
Remote Group Setup - 遠端用戶群組配置



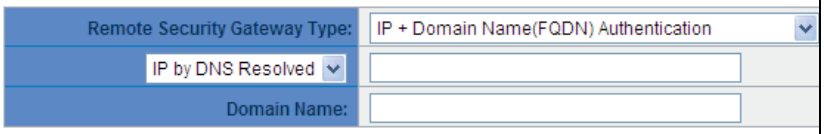
此項目的遠端的閘道身分類型(Remote Security Gateway Type)必須與連接遠端的近端本地閘道身分類型(Local Security Gateway Type)相同。

Remote Security Gateway Type **遠程的閘道身分類型**	遠端的閘道認證類型，有五種操作模式項目選擇，分別爲: **IP only** 僅用 IP **IP + Domain Name (FQDN) Authentication** IP + Domain Name(FQDN) 認證 **IP + E-mail Addr. (USER FQDN) Authentication** IP + E-mail (USER FQDN) 認證 **Dynamic IP + Domain Name (FQDN) Authentication** 動態 IP + Domain Name(FQDN) 認證 **Dynamic IP + E-mail Addr. (USER FQDN) Authentication.** 動態 IP + E-mail (USER FQDN) 認證 **(1) IP only** 僅用 IP 若您選擇僅用 IP 類型的話，只有固定填入此 IP 位址可以存取此隧道，  若是使用者不知道遠端客戶的 IP 位址，則可以通過名稱轉換 DNS Resolve 來將 DNS 轉成 IP 位址。並且在設定完成後在 Summary 的遠端閘道下面顯示出相對應的 IP 位址。  **(2) IP + Domain Name(FQDN) Authentication** IP + Domain Name(FQDN) 認證

若您選擇 IP+網域名稱類型的話，請輸入 IP 位址以及您所驗證的網域名稱 FQDN 是指主機名稱以及網域名稱的結合，使用者可以輸入一個符合 FQDN 的網域名稱即可。此 IP 位址以及網域名稱必須與遠端的 VPN 安全閘道設定類型相同才可以正確連接。



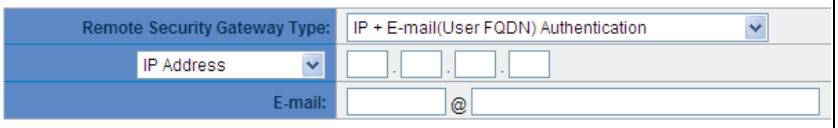
若是使用者不知道遠端的 IP 位址，則可以通過網域名稱轉換 DNS Resolve 來將 DNS 轉成 IP 位址。此網域名稱必須存在 Internet 上可以查詢的到。並且在設定完成後在 Summary 的遠端閘道下面自動顯示出相對應的 IP 位址。



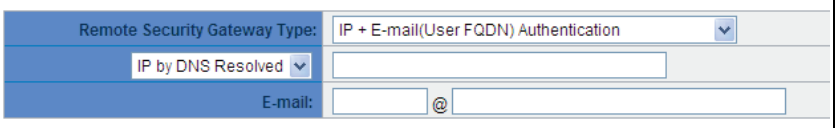
(3)IP + E-mail Addr. (USER FQDN) Authentication:

IP + E-mail(USER FQDN) 認證

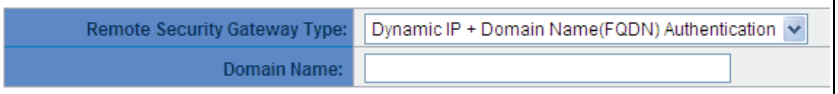
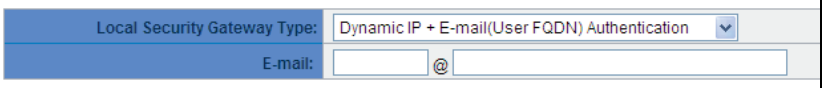
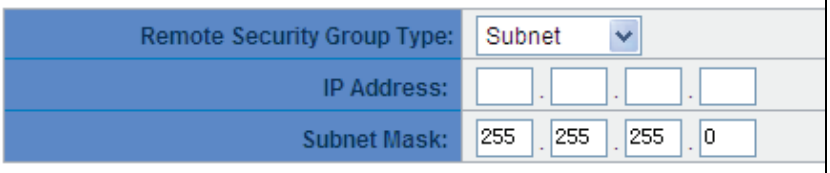
若您選擇 IP 位址加上電子郵件類型的話，只有固定填入此 IP 位址以及電子郵件位置可以存取此隧道，



若是使用者不知道遠端客戶的 IP 位址，則可以透過網域名稱轉換 DNS Resolve 來將 DNS 轉成 IP 位址。並且在設定完成後在 Summary 的遠端閘道下面顯示出相對應的 IP 位址。

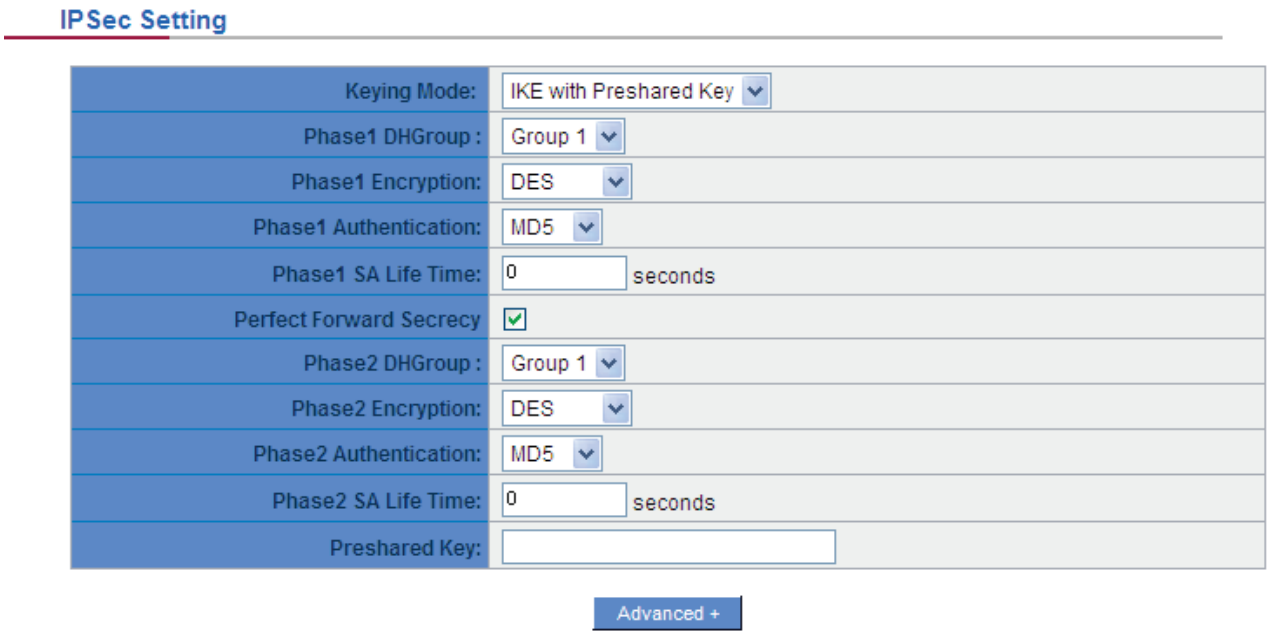


(4)Dynamic IP + Domain Name(FQDN) Authentication:

	動態 IP + Domain Name(FQDN) 認證: 若是您使用動態 IP 位址連接路由器時，您可以選擇動態 IP 位址加上主機名稱以及網域名稱的結合。  **(5) Dynamic IP + E-mail Addr. (USER FQDN) Authentication.** 動態 IP + E-mail (USER FQDN) 認證 若是您使用動態 IP 位址連接本路由器時， 您可以選擇此類型連接 VPN，當遠端的 VPN 閘道要求與路由器作爲 VPN 連線時，路由器將會開始驗證並回應此 VPN 隧道連線; 請輸入電子郵件認證到 E-Mail 位置空格欄位中。 
Remote Security Group Type **遠程安全組類型**	此爲設定遠端端的 VPN 連線存取類型，以下有幾個關於遠端端設定的項目，請您選擇並設置適當參數: **(1) IP address** 此項目爲允許此 VPN 隧道連線後，只有輸入此 IP 位址的本地端電腦可以連線。  以上的設定參考爲:當此 VPN 隧道連線後，於 192.168.2.1 的此 IP 位址範圍的電腦可以連線。 **(2) Subnet** 此項目爲允許此 VPN 隧道連線後，每一台于此網段的本地端電腦都可以連線。  以上的設定參考爲:當此 VPN 隧道連線後，只有 192.168.2.0，子網路遮罩爲 255.255.255.0 的此網段電腦

	可以與遠端 VPN 連線。

IPSec Setup



若是任何加密機制存在的話，此兩個 VPN 隧道的加密機制必須要相同才可以將此隧道連接，並於傳輸資料中加上標準的 IPSec 密鑰，我們稱爲加密密鑰 “key”。

Encryption Management Protocol - 密鑰管理協議

此選項設定爲當您設定此 VPN 隧道使用何種加密模式以及驗證模式後，必須設定一組交換密碼，並請注意此參數必須與遠端的交換密碼參數相同

Use IKE Protocol：

透過 IKE 產生共用的金鑰來加密與驗證遠端的使用者。若將完全順向密鑰 PFS(Perfect Forward Secrecy)啓用後，則會再第二階段的 IKE 協調過程產生的第二把共同金鑰做進一步加密與驗證。當 PFS 啓用後，透過 brute force 來擷取金鑰的駭客(hacker)無法在此短時間內，進一步得到第二把金鑰。

- **Perfect Forward Secrecy 完全順向密鑰:** 若您將 PFS 選項勾選後，記得另外的遠端 VPN 設備或是 VPN Client 也要將 PFS 功能開啓。

- **Phase 1/ Phase 2 DH Group 階段 1/階段 2 DH 協議群組**

  於此選項可以選擇採用 Diffie-Hellman 群組方式: Group1 或是 Group2/Group5。

- **Phase 1/ Phase 2 Encryption 階段 1/階段 2 加密演算法:**

  此加密選項設定爲設定此 VPN 隧道使用何種加密模式，並請注意設置此參數必須與遠端的加密參數相同:**DES**:64-位元元加密模式、**3DES**:128-位元元加密模式、**AES**:用安全碼進行資訊加密的標準，它支持 128 位、192 位和 256 位的密匙。

- **Phase 1/Phase 2 Authentication 階段 1/階段 2 認證演算法:**

  此驗證選項設定爲設定此 VPN 隧道使用何種驗證模式，並請注意設置此參數必須與遠端的驗證模式參數相同:“**MD5**”或“**SHA1**”。

- **Phase 1 SA Life Time 階段 1 SA 有效時間:**

  爲此交換密碼的有效時間，系統預設值爲 28800 秒(8 小時)，於此有效時間內的 VPN 連線，系統會自動的將於有效時間後，自動的生成其他的交換密碼以確保安全。

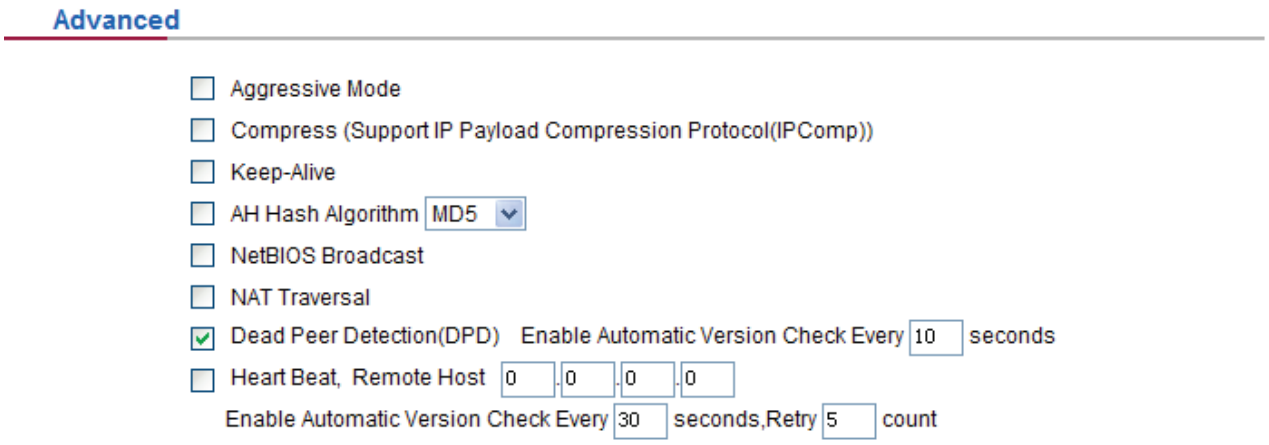
- **Phase2 SA Life Time 階段 2 SA 有效時間:**

  爲此交換密碼的有效時間，系統預設值爲 3600 秒(1 小時)，於此有效時間內的 VPN 連線，系統會自動的將於有效時間後，自動的生成其他的交換密碼以確保安全

- **Preshared Key 共用密鑰：**

  於 Auto (IKE) 選項中，您必須輸入一組交換密碼於 “Pre-shared Key” 的欄位中，在此的範例設定爲 test，您可以輸入數位元或是文字的交換密碼，系統將會自動的將您輸入的數位元或是文字的交換密碼自動轉成 VPN 隧道連接時的交換密碼與驗證機制;此數位元或是文字的交換密碼最高可輸入 30 個文字組合。

Advanced Setting- for IKE Protocol Only



在本機的進階設定項目中，分別有 Main 以及 Aggressive（野蠻模式）模式，Main mode 是本機的預設 VPN 作業模式，而且與大多數的其他 VPN 設備使用連接方式爲相同。

- **Aggressive Mode 野蠻模式:**

  大多爲遠端的設備採用，如使用動態 IP 連接時，是爲了加強其安全控管機制。

- **Use IP Header Compression Protocol 使用 IP Header 壓縮協定:**

  若選擇此項目勾選，則連接的 VPN 隧道中 VPN 防火牆 支援 IP 表頭形態的壓縮 (IP Payload compression Protocol)。

- **Keep Alive 持續保持連線:**

  若選擇此項目勾選，則連接的 VPN 隧道中會持續保持此條 VPN 連接不會中斷，此使用多爲分公司遠端節點對總部的連接使用，或是無固定 IP 位址的遠端使用。

- **AH hash calculation AH 哈希演算法:**

  AH (Authentication Header) 驗證表頭封包格式，可選擇 MD5/DSHA-1。

- **NetBIOS Broadcast 允許 NetBIOS 廣播封包通過:**

  若選擇此項目勾選，則連接的 VPN 隧道中會讓 NetBIOS 廣播封包通過。，有助於微軟的網路鄰居等連接容易，但是相對的佔用此 VPN 隧道的流量就會加大！

- **Dead Peer Detection (DPD) 掉線偵測功能:**

若選擇此項目勾選，則連接的 VPN 隧道中會定期的傳送 HELLO/ACK 訊息封包來偵測是否 VPN 隧道的兩端仍有連線存在。當有一端斷線則 VPN 防火牆會自動斷線，然後再建立新連線。使用者可以選擇每一次 DPD 訊息封包傳遞的時間，預設值爲 10 秒。

- **Heart Beat 心跳：**

  VPN Tunnel 心跳監測功能。

若勾選此項設定，系統會定期傳送 ICMP 給在 VPN 通道遠端的伺服器主機，遠端伺服器收到封包之後也會以封包回應。若偵測次數已超過您所設定的值，而 VPN 遠端伺服器都沒有回應的話，系統會判定此 VPN 通道爲斷線。若您爲主動建立 VPN 通道的一方，系統將自動再一次地重建 VPN 通道；而若您爲被動的一方，系統會等待對方再度建立 VPN 通道。

Remote Host **遠端伺服器**	遠端的網路節點偵測位置，此伺服器位址最好是可以且穩定快速的得到回應(建議可以填入 VPN remote Sever LAN IP，請勿填無法回應 ICMP 的伺服器位址)。
Interval **時間間隔**	對外連線偵測逾時時間(秒)，預設值爲 30 秒。於 VPN 建立後，每隔 30 秒丟 ICMP 偵測與伺服器連線狀態。
Retry **重新偵測次數**	連線偵測重試次數，預設值爲五次。如果連線偵測重試次數超過設定次數，遠端伺服器沒有回應的話，則判斷 VPN 線路中斷！

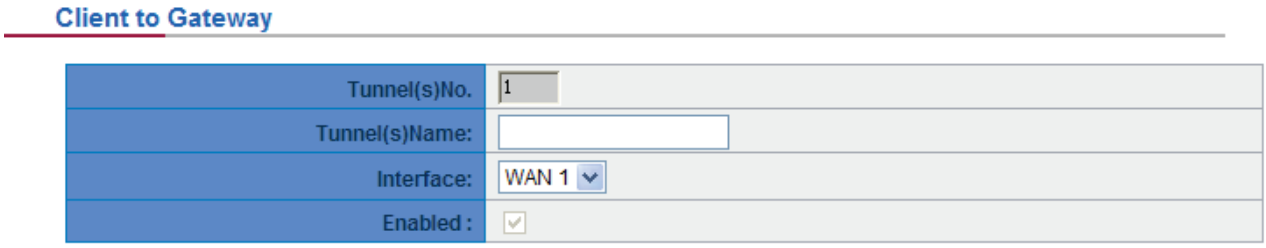
※心跳和 DPD 功能，皆能夠保障 VPN 通道更穩定的連線品質。不同的是，心跳功能不需考慮遠端的 VPN 設備是否具備標準 IPSec 協議，皆能完成 VPN 通道監測，以確定 VPN 通道連線存在、並且流量暢通。

10.1.2.2. Client to Gateway Setting 用戶端對閘道的設定

透過以下的設定說明，管理人員就可以在用戶端與本機之間建立一條 VPN 隧道。

用戶可以選擇這一條 VPN 隧道在用戶端是只供一個客戶所使用(Tunnel)或者是由一群客戶所使用(Group VPN)。若由一群客戶所使用則可以節省個別設定遠端的客戶，只需設定的一條隧道供一組客戶所使用，以節省設定時的麻煩。

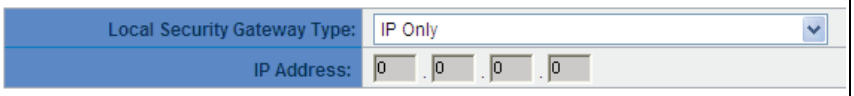
Situation in Tunnel：



Tunnel No.	當您設定本機內建之 VPN 功能時，請選擇您要設定的 Tunnel 隧道編號
Tunnel Name	設定此隧道連接名稱，如 XXX Office，建議您若是有一個以上的隧道設定的話，務必將每一個隧道名稱都設爲不同，以免混淆 **請注意**: 此隧道名稱若是您需要連接其他 VPN 設備(非此路由器)時，有一些設備規定此隧道名稱要與主控端爲相同名稱並做驗證，此隧道才會順利連線開啓！。
Interface **界面**	您可以選擇哪一個介面位置做爲此 VPN 隧道的節點
Enabled **啓動**	勾選啓用選項，將此 VPN 隧道開啓。 此項目爲預設爲啓用，當設定完成後，可以再選擇是否啓用隧道設定

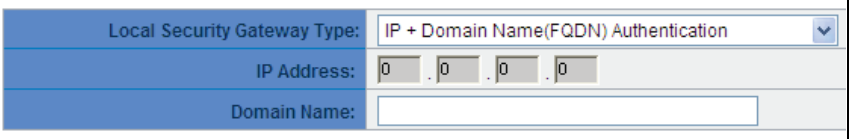
Local Group Setup - 本機用戶群組配置

此項目的本地閘道身分類型(Local Security Gateway Type)必須與連接遠端的閘道身分類型(Remote Security Gateway Type)相同。

Local Security GatewayType **本地閘道身分類型**	本機閘道認證類型，有五種操作模式項目選擇，分別爲: **IP only** 僅用 IP **IP + Domain Name (FQDN) Authentication** IP + Domain Name(FQDN) 認證 **IP + E-mail Addr. (USER FQDN) Authentication** IP + E-mail (USER FQDN) 認證 **Dynamic IP + Domain Name (FQDN) Authentication** 動態 IP + Domain Name(FQDN) 認證 **Dynamic IP + E-mail Addr. (USER FQDN) Authentication.** 動態 IP + E-mail (USER FQDN) 認證 **(1) IP only** 僅用 IP 若您選擇僅用 IP 類型的話， 只有固定填入此 IP 位址可以存取此隧道，然後路由器的 WAN IP 位址，將會自動填入此項目空格內，您不需要在進行額外設定。  **(2) IP + Domain Name(FQDN) Authentication** + Domain Name(FQDN) 認證 若您選擇 IP+網域名稱類型的話，請輸入您所驗證的網域名稱以及 IP 位址然後路由器的 WAN IP 位址，將會自動填入此

項目空格內，您不需要在進行額外設定。

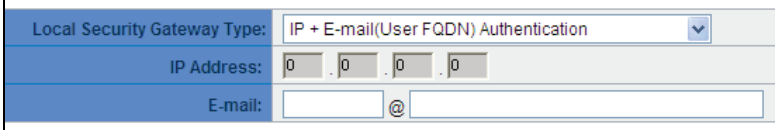
FQDN 是指主機名稱以及網域名稱的結合，也必須存在於 Internet 上可以查詢的到，如 vpn.server.com。此 IP 位址以及網域名稱必須與遠端的 VPN 安全閘道設定類型相同才可以正確連接。



(3) IP + E-mail Addr. (USER FQDN) Authentication.

+ E-mail (USER FQDN) 認證

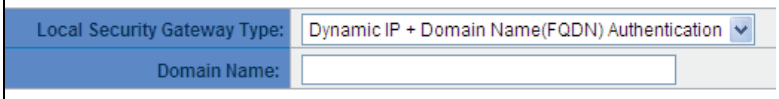
若您選擇 IP 位址加上電子郵件類型的話， 只有固定填入此 IP 位址以及電子郵件位置可以存取此隧道，然後路由器的 WAN IP 位址，將會自動填入此項目空格內，您不需要在進行額外設定。



(4) Dynamic IP + Domain Name(FQDN) Authentication

動態 IP + Domain Name(FQDN) 認證

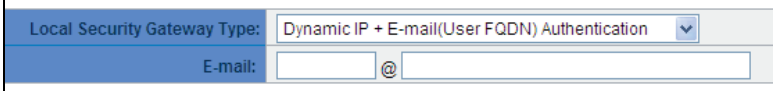
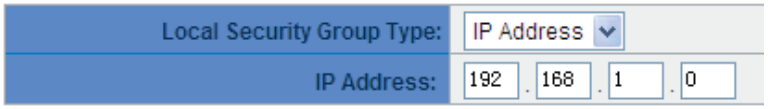
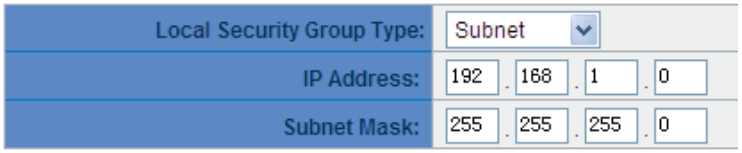
若是您使用動態 IP 位址連接路由器時， 您可以選擇此類型連接 VPN，當遠端的 VPN 閘道要求與路由器作爲 VPN 連線時，路由器將會開始驗證並回應此 VPN 隧道連線; 若您選擇此類型連接 VPN，請輸入網域名稱即可。



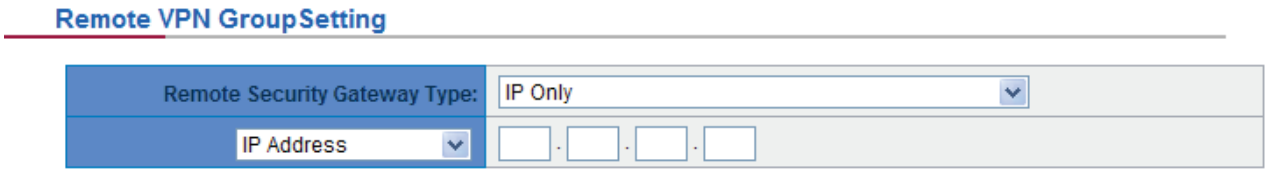
(5) Dynamic IP + E-mail Addr. (USER FQDN) thentication.

動態 IP + E-mail (USER FQDN) 認證

若是您使用動態 IP 位址連接路由器時， 您可以選擇此類型連接 VPN，使用者不必輸入 IP 位址，當遠端的 VPN 閘道要

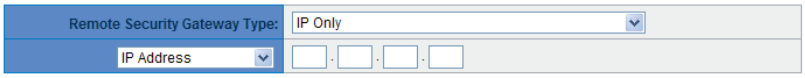
	求與路由器作爲 VPN 連線時，路由器將會開始驗證並回應此 VPN 隧道連線; 若您選擇此類型連接 VPN，請輸入電子郵件認證到 E-Mail 位置空格欄位中即可。 
Local Security Group Type **本地安全組類型**	此爲設定本地區域端的 VPN 連線存取類型，以下有幾個關於本地區域端設定的項目，請您選擇並設置適當參數: **1. IP address** 此項目爲允許此 VPN 隧道連線後，只有輸入此 IP 位址的本地端電腦可以連線。  以上的設定參考爲:當此 VPN 隧道連線後，於 192.168.1.0 的此 IP 位址的電腦可以連線。 **2. Subnet** 此項目爲允許此 VPN 隧道連線後，每一台于此網段的本地端電腦都可以連線。  以上的設定參考爲:當此 VPN 隧道連線後，只有 192.168.1.0，子網路遮罩爲 255.255.255.0 的此網段電腦可以與遠端 VPN 連線。

Remote Group Setup - 遠端用戶群組配置



此項目的遠端的閘道身分類型(Remote Security Gateway Type)必須與連接遠端的近端本地閘道身分類型(Local Security Gateway Type)相同。

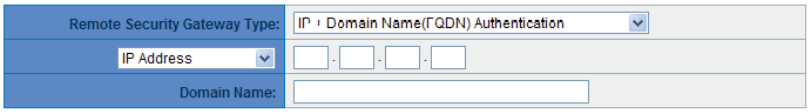
Remote Security Gateway Type **遠程的閘道認證類型**	遠端的閘道認證類型，有五種操作模式項目選擇，分別爲: **IP only** 僅用 IP **IP + Domain Name (FQDN) Authentication** IP + Domain Name(FQDN) 認證 **IP + E-mail Addr. (USER FQDN) Authentication** IP + E-mail (USER FQDN) 認證 **Dynamic IP + Domain Name (FQDN) Authentication** 動態 IP + Domain Name(FQDN) 認證 **Dynamic IP + E-mail Addr. (USER FQDN) Authentication** 動態 IP + E-mail (USER FQDN) 認證 **(1) IP only** 僅用 IP 若您選擇僅用 IP 類型的話，只有固定填入此 IP 位址可以存取此隧道，若是使用者不知道遠端客戶的 IP 位址，則可以通過網域名稱轉換 DNS Resolve 來將 DNS 轉成 IP 位址。並且在設定完成後在 Summary 的遠端閘道下面顯示出相對應的 IP 位址。



(2) IP + Domain Name(FQDN) Authentication

IP + Domain Name(FQDN) 認證

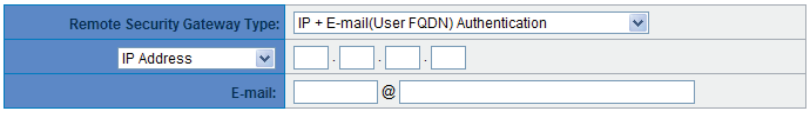
若您選擇 IP+網域名稱類型的話，請輸入 IP 位址以及您所驗證的網域名稱 FQDN 是指主機名稱以及網域名稱的結合，使用者可以輸入一個符合 FQDN 的網域名稱即可。此 IP 位址以及網域名稱必須與遠端的 VPN 安全閘道設定類型相同才可以正確連接。若是使用者不知道遠端客戶的 IP 位址，則可以通過網域名稱轉換 DNS Resolve 來將 DNS 轉成 IP 位址。並且在設定完成後在 Summary 的遠端閘道下面顯示出相對應的 IP 位址。



(3) IP + E-mail Addr. (USER FQDN) Authentication.

IP + E-mail (USER FQDN) 認證

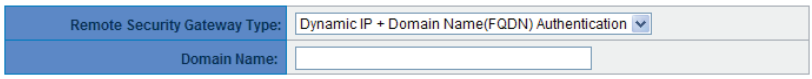
若您選擇 IP 位址加上電子郵件類型的話，只有固定填入此 IP 位址以及電子郵件位置可以存取此隧道，若是使用者不知道遠端客戶的 IP 位址，則可以透過網域名稱轉換 DNS Resolve 來將 DNS 轉成 IP 位址。並且在設定完成後在 Summary 的遠端閘道下面顯示出相對應的 IP 位址。



(4) Dynamic IP + Domain Name(FQDN) Authentication:

動態 IP + Domain Name(FQDN) 認證

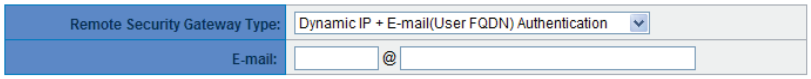
若是您使用動態 IP 位址連接本機時，您可以選擇動態 IP 位址加上主機名稱以及網域名稱的結合。



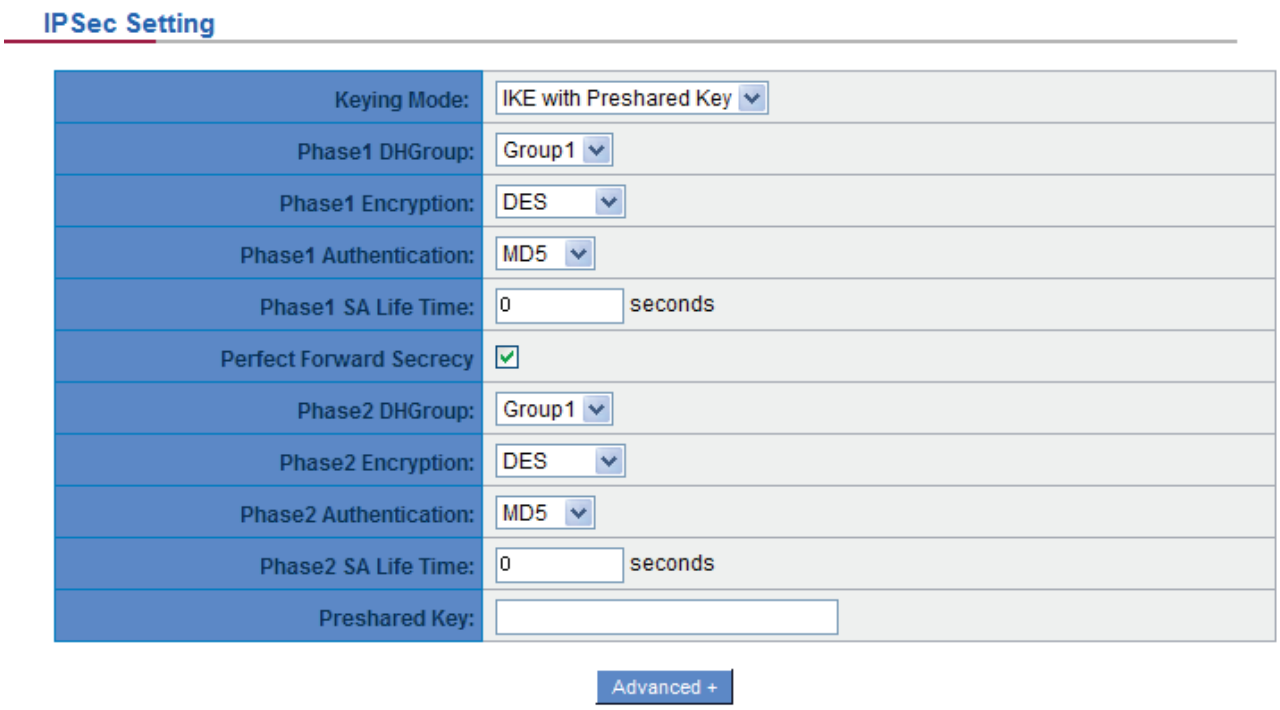
(5) Dynamic IP + E-mail Addr. (USER FQDN) Authentication.

動態 IP + E-mail (USER FQDN) 認證

若是您使用動態 IP 位址連接 VPN 防火牆時， 您可以選擇此類型連接 VPN，當遠端的 VPN 閘道要求與 VPN 防火牆作爲 VPN 連線時， VPN 防火牆 將會開始驗證並回應此 VPN 隧道連線; 請輸入電子郵件認證到 E-Mail 位置空格欄位中。



IPSec Setup



若是任何加密機制存在的話，此兩個 VPN 隧道的加密機制必須要相同才可以將此隧道連

接，並於傳輸資料中加上標準的 IPSec 密鑰，於此我們稱爲加密密鑰 “key”。

Encryption Management Protocol - 密鑰管理協議

此選項設定爲當您設定此 VPN 隧道使用何種加密模式以及驗證模式後，必須設定一組交換密碼，並請注意此參數必須與遠端的交換密碼參數相同

IKE Protocol：

透過 IKE 產生共用的金鑰來加密與驗證遠端的使用者。若將完全順向密鑰 PFS(Perfect Forward Secrecy)啓用後，則會再第二階段的 IKE 協調過程產生的第二把共同金鑰做進一步加密與驗證。當 PFS 啓用後，透過 brute force 來擷取金鑰的駭客(hacker)無法在此短時間內，進一步得到第二把金鑰。

- **Perfect Forward Secrecy 完全順向密鑰:** 若您將 PFS 選項勾選後，記得另外的遠端 VPN 設備或是 VPN Client 也要將 PFS 功能開啓。
- **Phase 1/ Phase 2 DH Group 階段 1/階段 2 DH 協議群組**

  於此選項可以選擇採用 Diffie-Hellman 群組方式: Group1 或是 Group2/Group5。
- **Phase 1/ Phase 2 Encryption 階段 1/階段 2 加密演算法:**

  此加密選項設定爲設定此 VPN 隧道使用何種加密模式，並請注意設置此參數必須與遠端的加密參數相同:**DES**:64-位元元加密模式、**3DES**:128-位元元加密模式、**AES**:用安全碼進行資訊加密的標準，它支持 128 位、192 位和 256 位的密匙。
- **Phase 1/Phase 2 Authentication 階段 1/階段 2 認證演算法:**

  此驗證選項設定爲設定此 VPN 隧道使用何種驗證模式，並請注意設置此參數必須與遠端的驗證模式參數相同:“**MD5**”或“**SHA1**”。
- **Phase 1 SA Life Time 階段 1 SA 有效時間:**

  爲此交換密碼的有效時間，系統預設值爲 28800 秒(8 小時)，於此有效時間內的

VPN 連線，系統會自動的將於有效時間後，自動的生成其他的交換密碼以確保安全。

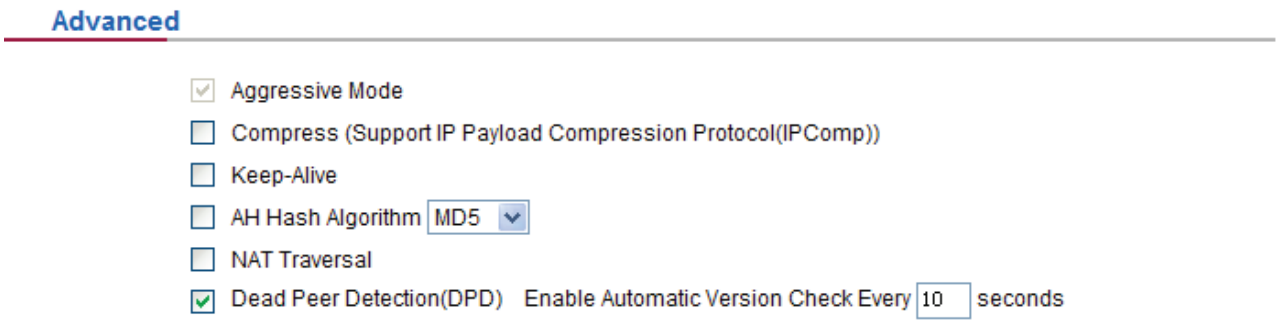
- **Phase2 SA Life Time 階段 2 SA 有效時間:**

  爲此交換密碼的有效時間，系統預設值爲 3600 秒(1 小時)，於此有效時間內的 VPN 連線，系統會自動的將於有效時間後，自動的生成其他的交換密碼以確保安全

- **Preshared Key 共用密鑰：**

  於 Auto (IKE) 選項中，您必須輸入一組交換密碼於 “Pre-shared Key” 的欄位中，在此的範例設定爲 test，您可以輸入數位元或是文字的交換密碼，系統將會自動的將您輸入的數位元或是文字的交換密碼自動轉成 VPN 隧道連接時的交換密碼與驗證機制;此數位元或是文字的交換密碼最高可輸入 30 個文字組合。

Advanced Setting- for IKE Protocol Only



在本機的進階設定項目中，分別有 Main 以及 Aggressive（野蠻模式）模式，Main mode 是本機的預設 VPN 作業模式，而且與大多數的其他 VPN 設備使用連接方式爲相同。

- **Aggressive Mode 野蠻模式:**

  大多爲遠端的設備採用，如使用動態 IP 連接時，是爲了加強其安全控管機制。

- **Use IP Header Compression Protocol 使用 IP Header 壓縮協定:**

  若選擇此項目勾選，則連接的 VPN 隧道中 VPN 防火牆 支援 IP 表頭形態的壓縮 (IP Payload compression Protocol)。

- **Keep Alive 持續保持連線:**

  若選擇此項目勾選，則連接的 VPN 隧道中會持續保持此條 VPN 連接不會中斷，

此使用多爲分公司遠端節點對總部的連接使用，或是無固定 IP 位址的遠端使用。

- **AH hash calculation AH 哈希演算法:**

  AH (Authentication Header) 驗證表頭封包格式，可選擇 MD5/DSHA-1。

- **NetBIOS Broadcast 允許 NetBIOS 廣播封包通過:**

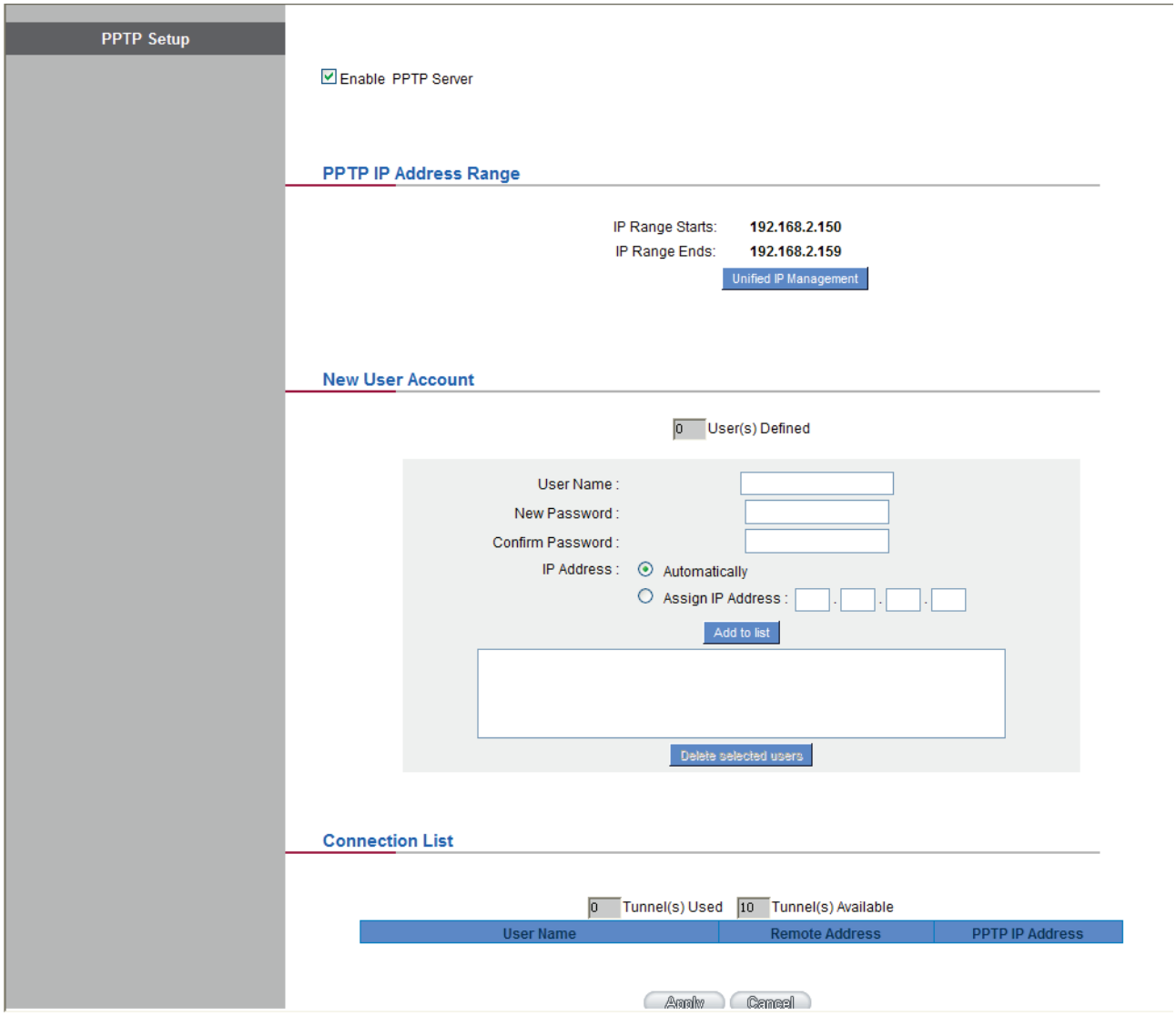
  若選擇此項目勾選，則連接的 VPN 隧道中會讓 NetBIOS 廣播封包通過。，有助於微軟的網路鄰居等連接容易，但是相對的佔用此 VPN 隧道的流量就會加大！

- **Dead Peer Detection (DPD) 掉線偵測功能:**

  若選擇此項目勾選，則連接的 VPN 隧道中會定期的傳送 HELLO/ACK 訊息封包來偵測是否 VPN 隧道的兩端仍有連線存在。當有一端斷線則 VPN 防火牆會自動斷線，然後再建立新連線。使用者可以選擇每一次 DPD 訊息封包傳遞的時間，預設值爲 10 秒。

10.1.3. PPTP Server

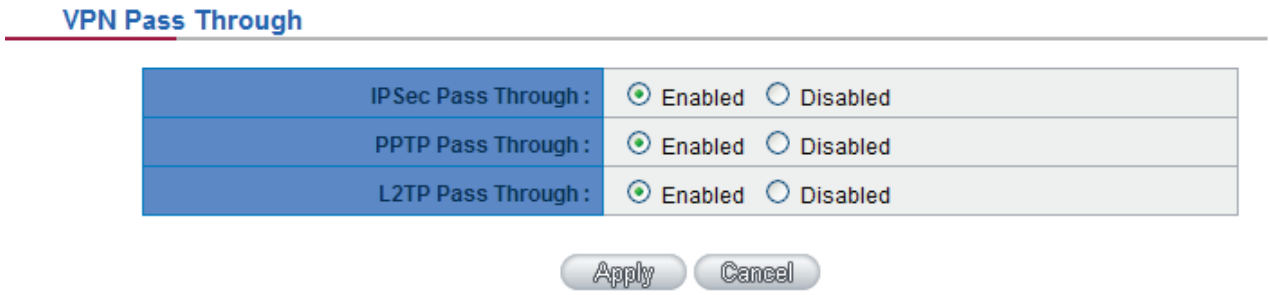
提供支援 Window XP/2000/Vista 的 PPTP 對本路由器做點對點隧道協議，讓遠端單機用戶使用此種協定建立 VPN 連線。



Enabled PPTP Server **啓用 PPTP 服務**	當勾選後即可以啓用點對點隧道協定 PPTP 伺服器。
PPTP IP Address Range **PPTP 用戶使用 IP 範圍**	請輸入近端 PPTP IP 位址的範圍，其目的是要給遠端的使用者一個可進入近端網路的入口 IP。 **※請注意！此範圍不可與 DHCP 伺服器發放 IP 範圍重複！**

User name	請輸入遠端使用者的名稱。
Password **Confirm Password**	輸入遠端使用者帳號密碼，及請再次確認遠端使用者的帳號密碼。
Add to list	將上述設定新增至下方列表之中。
Delete selected item	刪除選取項目。
Connection List	顯示所有連接成功的使用者，包括使用者名稱、遠端 IP 地址和 PPTP 發放的地址

10.1.4. VPN Pass Through - 封包穿透 VPN 防火牆功能

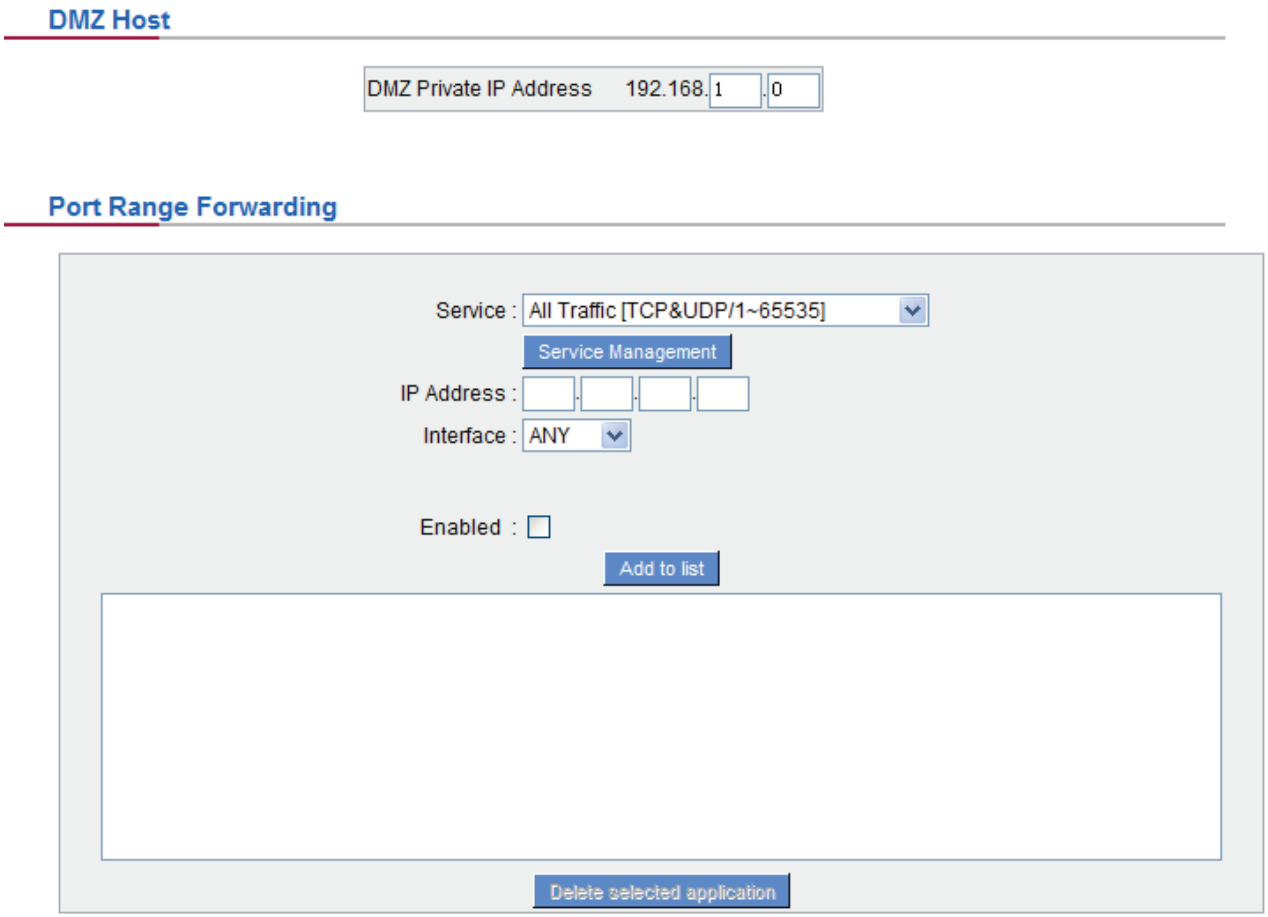


IPSec Pass Through：	若是選擇 **Enabled** 的話，則允許 PC 端使用 VPN- IPSec 封包穿透本機以便與外部 VPN 設備連線。
PPTP Pass Through：	若是選擇 **Enabled** 的話，則允許 PC 端使用 VPN，則允許 PC 端使用 VPN- PPTP 封包穿透本機以便與外部 VPN 設備連線。
L2TP Pass Through：	若是選擇 **Enabled** 的話，則允許 PC 端使用 VPN，則允許 PC 端使用 VPN- L2TP 封包穿透本機以便與外部 VPN 設備連線。

設定修改完成請按下“**Apply**”按鈕儲存網路設定變更或是按下“**Cancel**”按鈕不做任何設定變更。

XI. Advanced Function - 其他進階高級功能設置

11.1 DMZ Host/ Forwarding - DMZ/虛擬伺服器



11.1.1 DMZ Host

當您將安全路由器內部的某台 PC 的虛擬 IP 填入到此 DMZ 選項時，路由器 WAN 端的合法 IP 位址會直接對應給此台 PC 使用，也就是說從 WAN 端進來的封包，若是不屬於內部的任何一台 PC，都會傳送到這台 PC 上。

在使用“DMZ Host”功能後，若您要取消此功能必須於在設定 DMZ IP Address 地方填入“**0**”的參數，才會停止此功能使用。

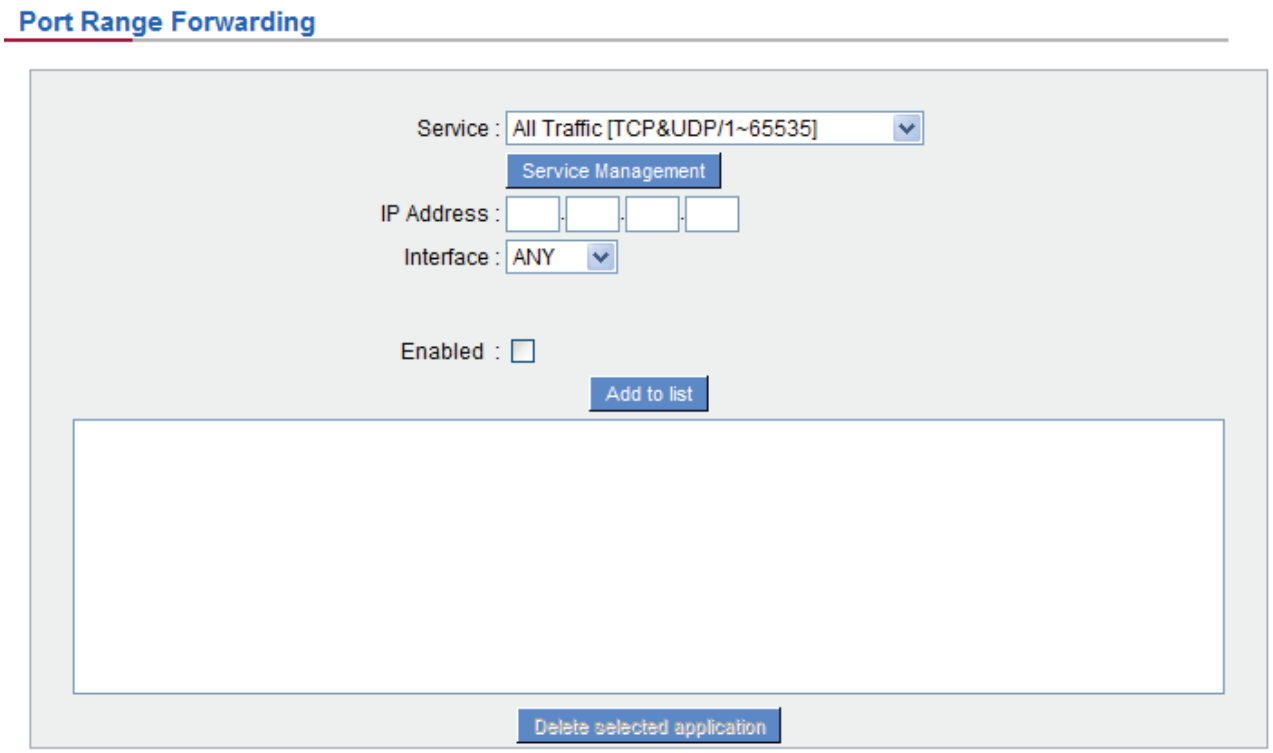
點擊此按鈕“**Apply**”即會儲存剛才所變動的修改設定內容參數。 點擊“**Cancel**” 即會清除剛才所變動的修改設定內容參數，此操作必須在確認儲存動作之前才會有效。

11.1.2 Port Range Forwarding - 虛擬伺服器設定

若是您在內網需架設伺服器（意指對外部的服務主機WEB、FTP、Mail等），這個功能可將虛擬伺服器主機視爲－虛擬的位置，利用安全路由器的外部合法IP位址，經過服務埠的轉換，(如WWW爲 80 埠)，直接存取到內部虛擬IP的伺服器的服務。例如在設定視窗中，選項填入伺服器位置，如 192.168.1.2 且埠是 80 的話，當外部網路要進來存取這個網頁時只要鍵入：例如: http://211.243.220.43.

此時，就會通過安全路由器的公網 IP 位址去轉換到 192.168.1.2 的虛擬主機上的 80 埠讀取網頁了。

其他種類的伺服器設定，都如以上設定；只要將所用伺服器的服務埠以及虛擬主機的 IP 位址填入即可！

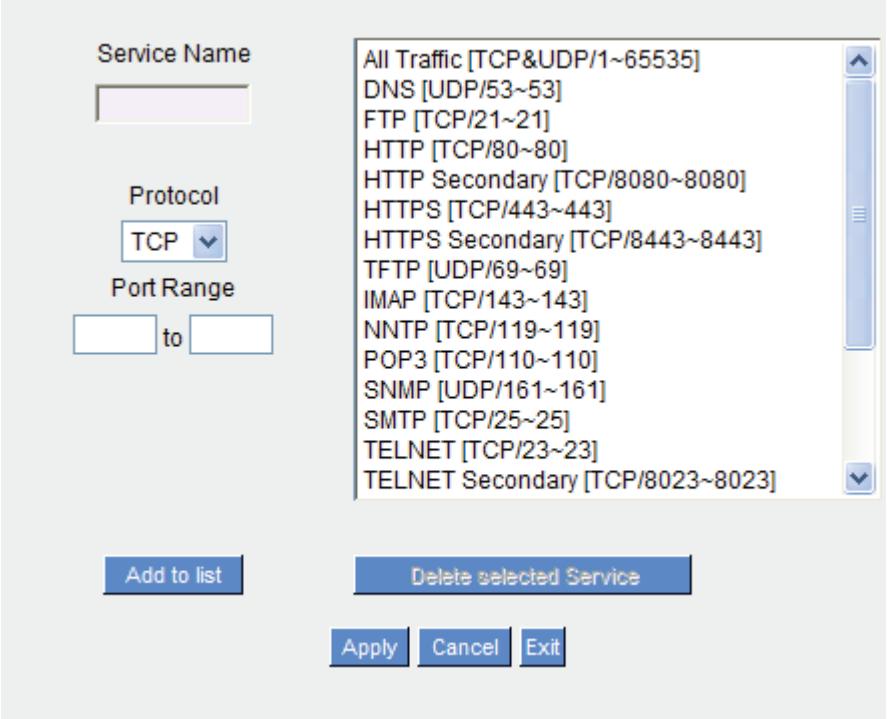


Service **服務端口**	在此選擇欲開啓的虛擬伺服器的服務埠號碼預設列表，如 WWW 爲 80(80~80)， FTP 爲 21~21，可參考服務號碼預設列表！
IP Address	在此填上虛擬伺服器所要相對應的內部虛擬 IP 位址，如 192.168.1.100。
Interface	選擇 WAN 端的界面
Enabled	開啓此服務功能。

Service Port Management **服務埠新增或刪除表**	若您所需要的服務埠沒有在列表裏面，可以利用此功能新增或刪除管理服務埠號列表。
Add to list	增加到開啓服務專案內容。

Service Port Management - 新增或刪除管理服務埠號

若您欲開啓的服務埠專案沒有在表列中，您可以點擊“服務端新增或刪除表”新增或刪除管理服務埠號列表，如下圖所示：

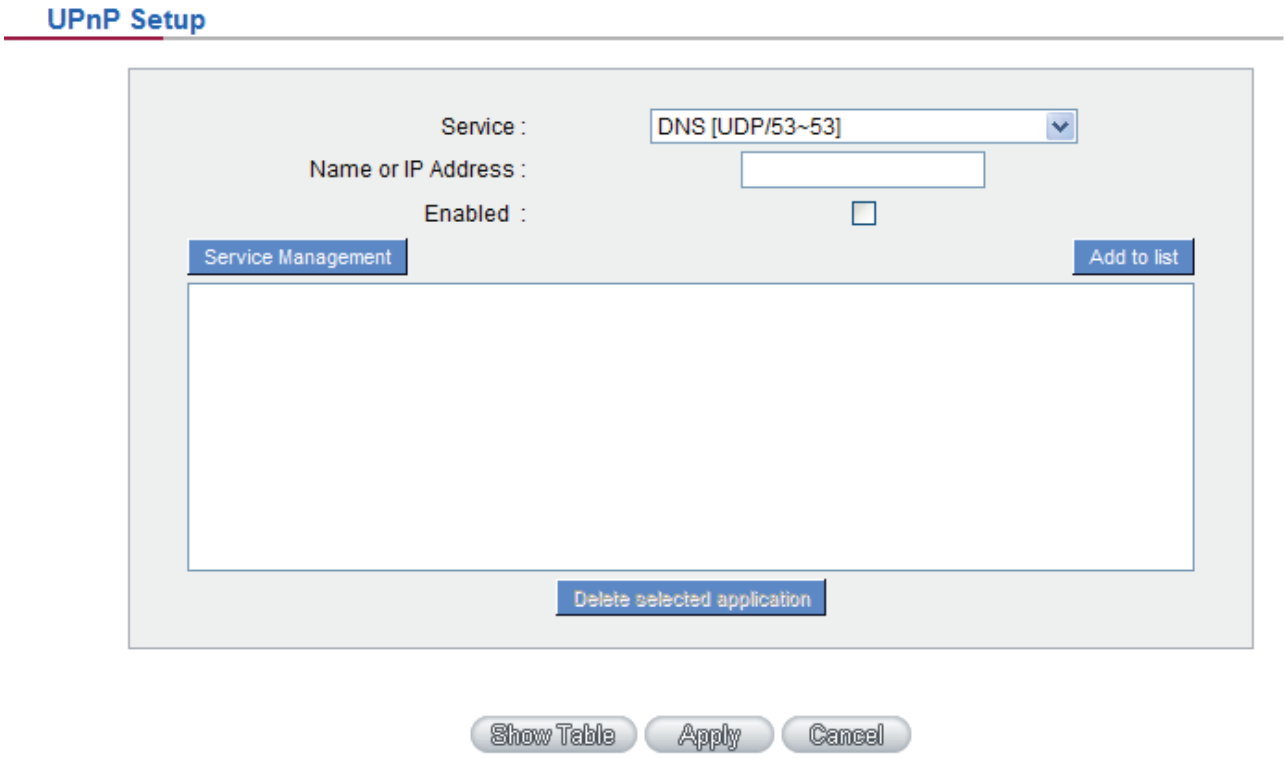


Service Name **服務端口名稱**	在此自定欲開啓的服務埠號名稱加入列表中，如 BT 等。
Protocol **通訊協定**	在此選擇欲開啓的服務埠號的封包格式爲 TCP 或 UDP。
Port Range **服務埠範圍**	將您所需新增加的服務埠範圍填入。
Add to list **增加到對應列表**	增加到開啓服務專案內容列表，最多可新增 100 組。
Delete selected item **刪除選擇服務服務端口**	刪除所選擇的開啓服務專案之一筆內容。

Apply	點擊此按鈕“**Apply**”即會儲存剛才所變動的修改設定內容參數。
Cancel	點擊此按鈕“**Cancel**”即會清除剛才所變動的修改設定內容參數，此操作必須於確認儲存動作之前才會有效。
Close	離開此功能設定視窗。

11.2 UPnP

PnP (Universal Plug and Play) 是微軟所制定的一項通訊協定標準，若是您使用的電腦有支援 UpnP 機制的話(如 Windows XP)而且您的電腦 UpnP 功能有開啓，您可以將本機的 UPnP 功能啓用。

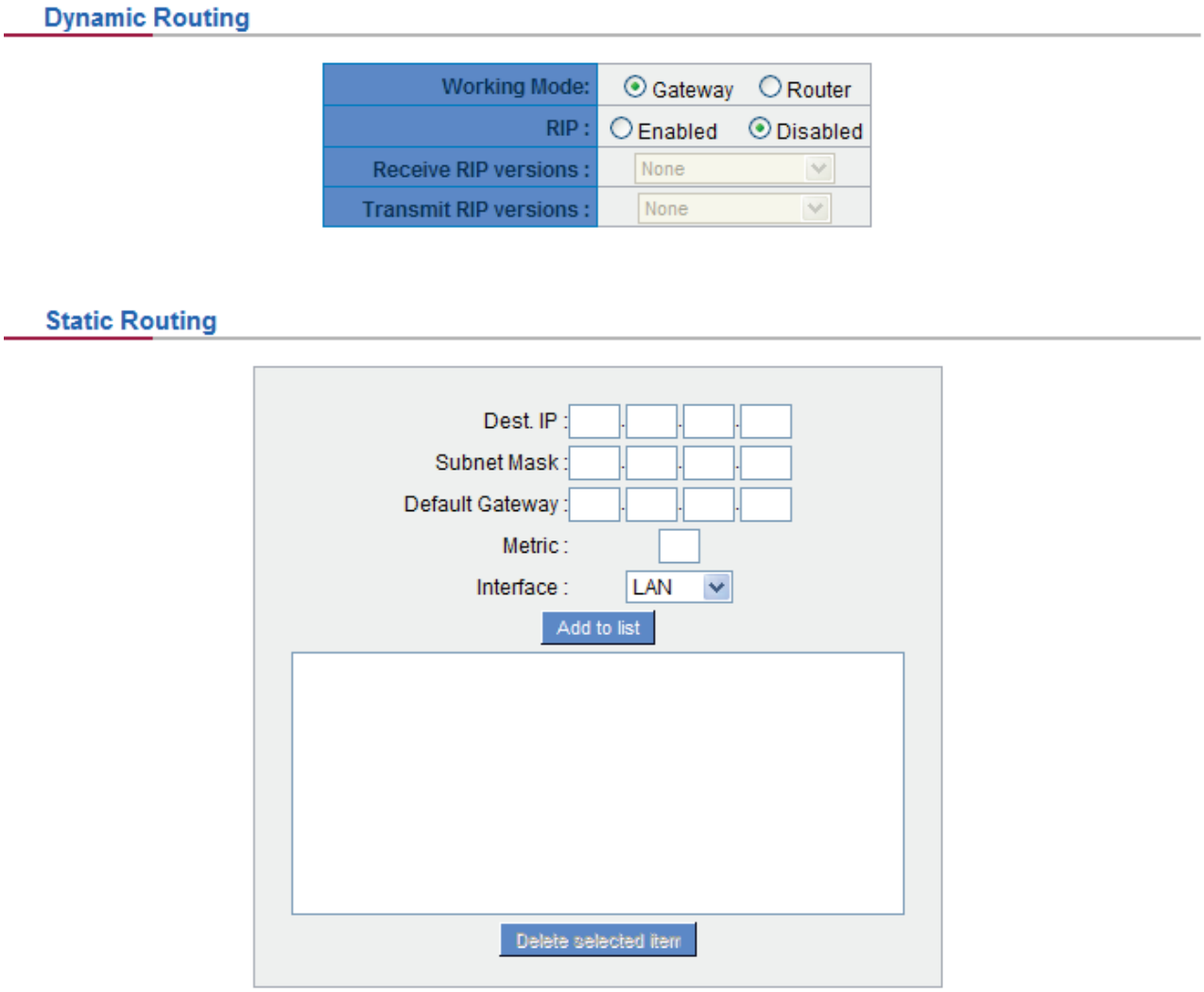


Service Port **通訊埠**	在此選擇欲開啓的 UPnP 的服務號碼預設列表，如 WWW 爲 80(80~80)， FTP 爲 21~21，可參考服務號碼預設列表！
Host Name or IP Address **主機名稱或 IP 位址**	在此填上 UPnP 相對應的內部虛擬 IP 位址或名稱，如 192.168.1.100。
Enabled:	開啓此服務功能。
Service Port Management: **通訊埠增加或刪除表**	新增或刪除管理通訊埠號列表。
Add to List:	增加到開啓服務項目內容。
Delete Selected Item:	刪除所選擇的開啓服務項目之一筆內容。
Show Table:	顯示目前所開啓設定的 UPnP Forwarding 列表。

Apply:	點選此按鈕“Apply”即會儲存剛才所變動的修改設定內容參數。
Cancel:	點選此按鈕“Cancel”即會清除剛才所變動的修改設定內容參數，此操作必須於確認儲存動作之前才會有效。

11.3 Routing - 路由通訊協定

此節介紹動態路由協定以及靜態路由的設定。



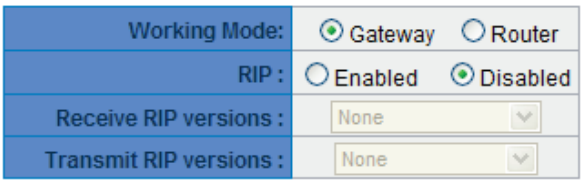
11.3.1 Dynamic Routing - 動態路由設定

RIP 是路由通訊協定 Routing Information Protocol 的簡稱，有 RIP I / RIP II 兩個版本。對於一般使用的網路中，大多只有一個路由器(或是閘道器)，所以大部份的情況是不需要使用這個功能。RIP 的使用時機是您的網路中有數個路由器，此台路由器是其中之一，此時若是不想手動設置每台路由器的繞徑表，可以啓動此功能，自動將所有路徑更新！

RIP 是一個很非常簡單的路由協議，採用距離向量的方式以封包到達目的地之前需要經過的路由的個數來做傳送距離的判斷，而不以實際連線的速率來做判斷。所以所選的路徑是

經過最少的路由，但是並不一定反應速度最快的路由及路徑。

Dynamic Routing

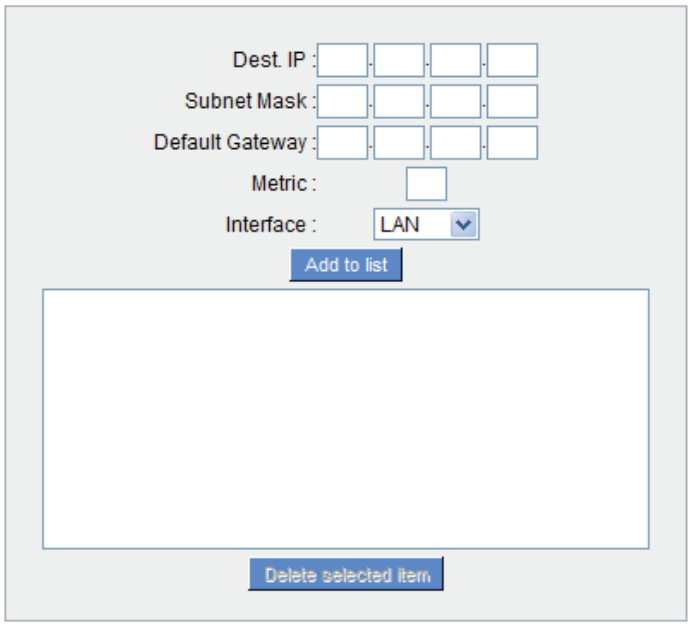


Working Mode **選擇路由器運作模式**	選擇路由器運作模式爲 Gateway (NAT) 模式或是 Router (路由)模式。
RIP	選擇按鈕“Enabled”開啓使用 RIP 動態路由通訊。
Receive RIP versions **接收動態路由通訊協定功能**	可于上下選擇按鈕選擇使用動態路由通訊 None，RIPv1， RIPv2-Broadcast， RIPv2-Multicast， 爲接收動態路由通訊協定格式。
Transmit RIP versions **傳送動態路由通訊協定功能**	可于上下選擇按鈕選擇使用動態路由通訊 None，RIPv1， RIPv2， Both RIPv1 and v2 作爲傳送動態路由通訊協定格式。

11.3.2 Static Routing - 靜態路由設定

靜態路由是以手動設置路由表的方式來達成封包路由。在此路由器的應用可分爲兩種方式，一是在內網中連結不同網段或路由器，一是在 Multi-WAN 的環境中讓路由器知道去那個目地地址時就要走那條 WAN。

Static Routing



Dest. IP **Subnet Mask** **目的地址和子網路遮罩**	填入目的地的遠端網路 IP 節點與子網路節點位址。
Default Gateway **預設閘道**	從此網路節點到目的遠端網路欲繞徑的預設閘道器位址。
Metric **最大跳數**	從此網路節點到目的遠端網路所經過路由器層數，如是在路由器下的二個路由器之一，此應填爲 2，預設爲 1。(最大爲 15)。
Interface **界面位置**	此網路節點的連接位置，是位於廣域埠 WAN 端亦或是區域埠 LAN 端。
Add to List	增加此路徑規則到列表中。
Delete Selected Item	刪除在表中所選擇的路徑表。
Show Table	顯示目前最新的路徑表。
Apply	點擊此按鈕“Apply”即會儲存剛才所變動的修改設定內容參數。
Cancel	點擊此按鈕“Cancel”即會清除剛才所變動的修改設定內容參數，此操作必須於確認儲存動作之前才會有效。

11.4 One to One NAT - 一對一 NAT 對應

11.4.1 One to One NAT

當您的 ISP 線路爲固定制(如 ADSL 固定 IP)時，通常 ISP 會給您多個合法 IP 位址。路由器提供您可將除了路由器本身WAN埠以及光纖盒或ATU-R(閘道) 各使用一個合法IP位址後，所剩的合法 IP 位址可以直接對應到路由器內部的電腦使用，也就是這些電腦在內網雖爲虛擬 IP，但當做了一對一對應後，這些對應到的電腦去外部訪問時都是有自己的合法 IP。

例如，當您公司內部環境需有兩台或兩台以上的“WEB 伺服器”時，由於需要兩個或兩個以上的合法 IP 位址，所以可以利用此功能達到將外部多個合法 IP 位址直接對應到內部多個虛擬服務伺服器 IP 位址使用！

範例： 如您有 5 個合法 IP 地址，分別是 210.11.1.1～6，而 210.11.1.1 已經給路由器的 WAN1 使用，另外還有其他四個合法 IP 可以分別設定到 One to One NAT 當中，如下所述：

210.11.1.2→ 192.168.1.3

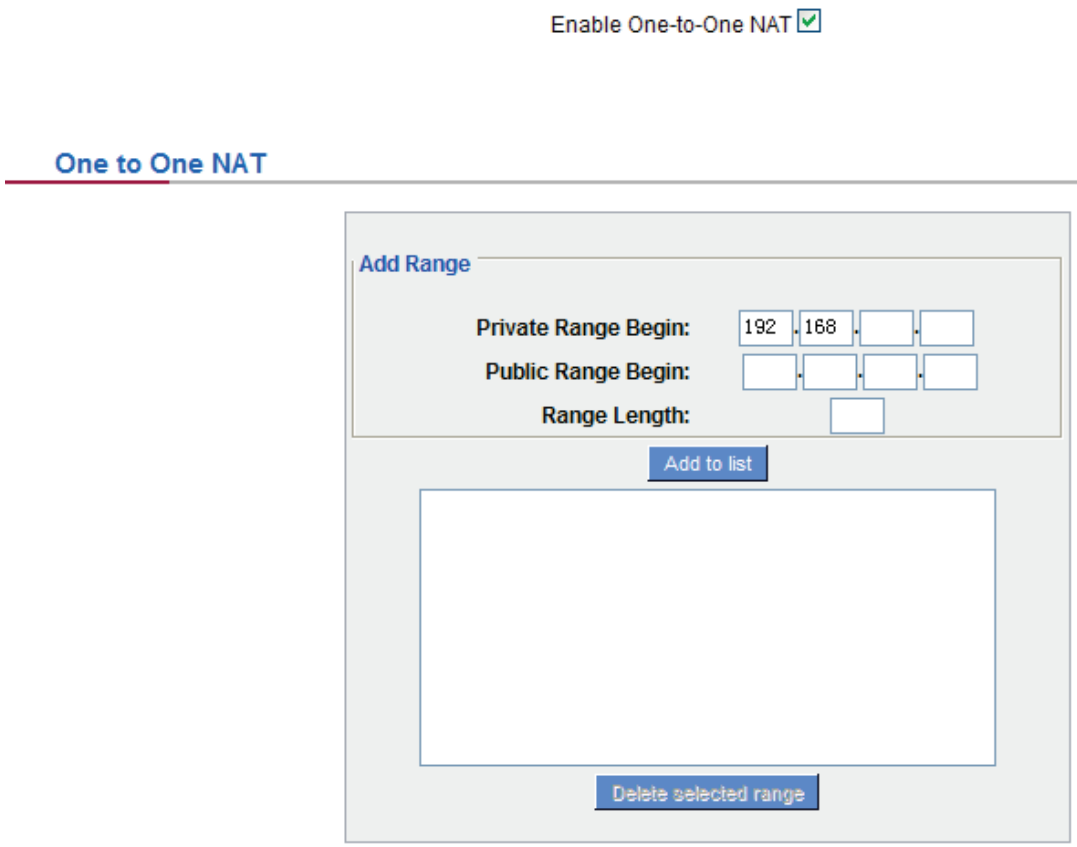
210.11.1.3→ 192.168.1.4

210.11.1.4→ 192.168.1.5

210.11.1.5→ 192.168.1.6

注意！

路由器 WAN IP 地址不能被涵蓋在一對一 NAT 的 IP 範圍設定中。



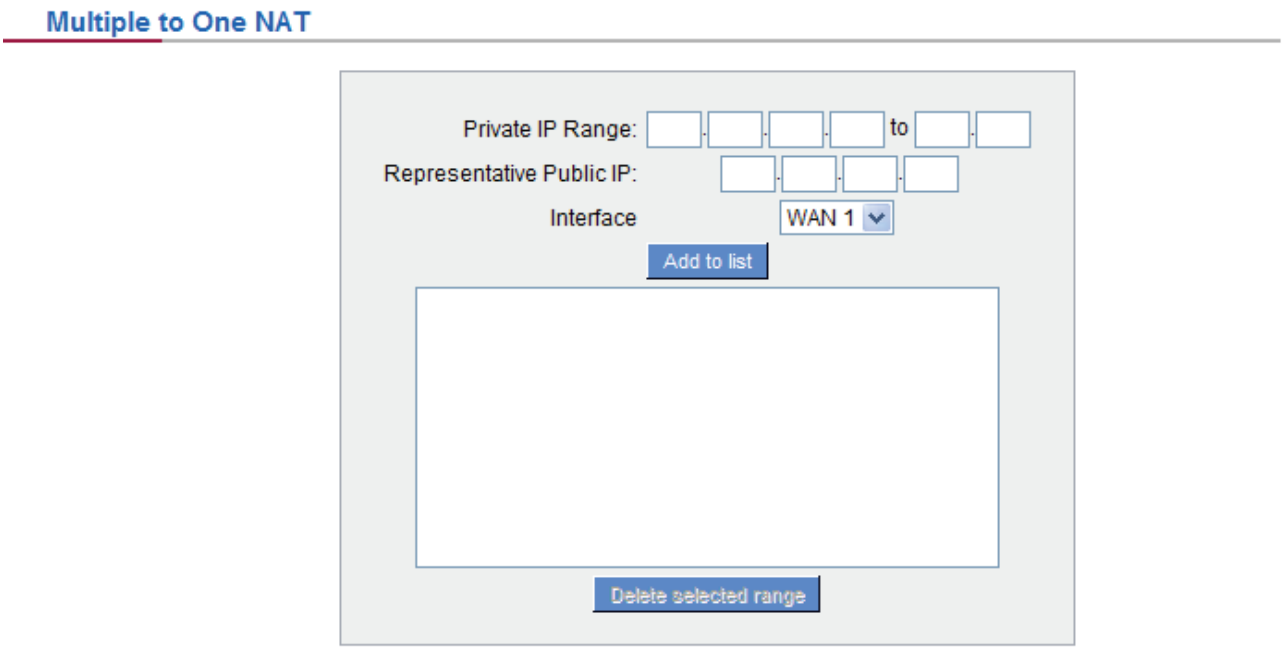
Enable One to One NAT	選擇是否開啓此一對一 NAT 功能。
Private IP Range Begin **內部範圍 IP 地址**	虛擬 IP 位址起始 IP 位址。
Public IP Range Begin **外部範圍 IP 地址**	外部合法 IP 位址起始 IP。
Range Length **對應 IP 數量**	填入您同時要有多少個外部合法 IP 位址需要對應。
Add to List	加入此設定到一對一 NAT 列表中。
Delete Seleted Item	刪除所選擇的一對一 NAT 規則。
Apply	點擊此按鈕“**確認**”即會儲存剛才所變動的修改設定內容參數。
Cancel	點擊此按鈕“**取消**”即會清除剛才所變動的修改設定內容參數，此操作必須於“確定”儲存動作之前才會有效。

注意！

一對一的 NAT 模式將會改變防火牆運作的方式，您若設定了此功能，LAN 端所對應有 公網 IP 的服務伺服器或電腦將會曝露在互聯網上。若要阻絕網路的使用者主動連線到一對一 NAT 的服務伺服器或電腦，請到防火牆的存取規則中設定適當的拒絕存取規則條件。

11.4.2 Multiple to One NAT - 多對一 NAT 對應

當您需要設定某部分內網 IP 位址 / 範圍，固定轉 NAT 某個 WAN IP 出去，用來註冊特別的服務或是網路架構，就可以透過多對一 NAT 對應進行設定。



Enable Multiple to One NAT	選擇是否開啓此多對一 NAT 功能。
Private IP Range Begin **內部範圍 IP 地址**	內網虛擬 IP 位址範圍。
Public IP Range Begin **外部範圍 IP 地址**	設定固定對應的廣域網 (WAN) IP 位址，需搭配下方所選擇的廣域網界面，若該 IP 位址不在該廣域網界面包含的範圍之內，設定是無效的。

Interface **界面**	選擇廣域網 IP 所對應的界面，，若上方對應 WAN IP 位址不在該廣域網界面包含的範圍之內，設定是無效的。
Add to List	加入此設定到多對一 NAT 列表中。
Delete Seleted Item	刪除所選擇的多對一 NAT 規則。
Apply	點擊此按鈕“確認”即會儲存剛才所變動的修改設定內容參數。
Cancel	點擊此按鈕“取消”即會清除剛才所變動的修改設定內容參數，此操作必須於“確定”儲存動作之前才會有效。

11.5 DDNS- Dynamic Domain Name Service -動態網域名稱解析

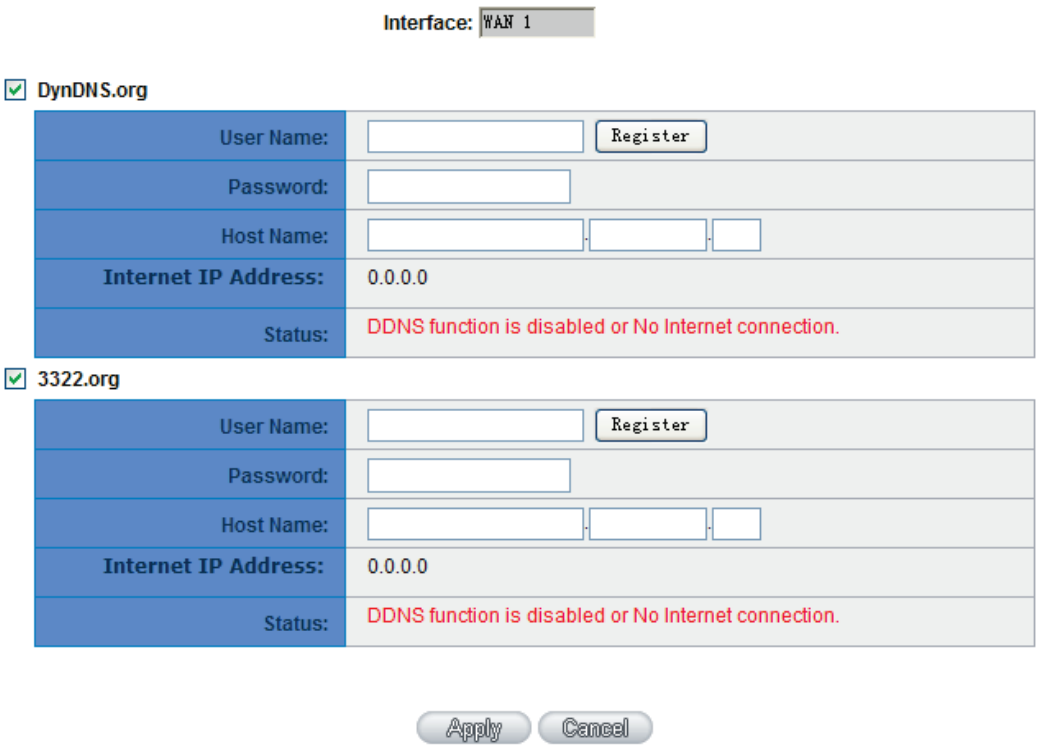
此路由器的 “DDNS” 功能可以支援 Dyndns.org 與 3322.org 兩家的動態網域名稱解析功能，其目的是爲了讓使用動態 IP 位址(也就是無法有固定 IP 的環境)來架設虛擬伺服器、及遠端監控時查詢現在的路由器 IP。如 ADSL PPPoE 計時制或是 Cable Modem 的使用者的 WAN IP 位址都會隨 ISP 端要求而改變，當此時使用者申請了 DDNS 後，如“abc.Dyndns.org”，將其設定在 DDNS 設定中，則在遠程只要去 Ping Dyndns.org 則可以知道現在路由器的實際 IP。且若是內部有架設網站之類的服務，網路使用者只要在網址打上 edimax.Dyndns.org 就可以直接進入到您內部架設的 WEB。

另外，爲了解決 DDNS 伺服器可能會發生不穩定的情況，現在路由器每個 WAN 都可同時對此兩家 DDNS 做動態 IP 升級。

DDNS Setup

Interface	Status	Host Name	Config.
WAN 1	Dyndns Disabled 3322 Disabled	Dydns:--- 3322:---	Edit
WAN 2	Dyndns Disabled 3322 Disabled	Dydns:--- 3322:---	Edit
USB	Dyndns Disabled 3322 Disabled	Dydns:--- 3322:---	Edit

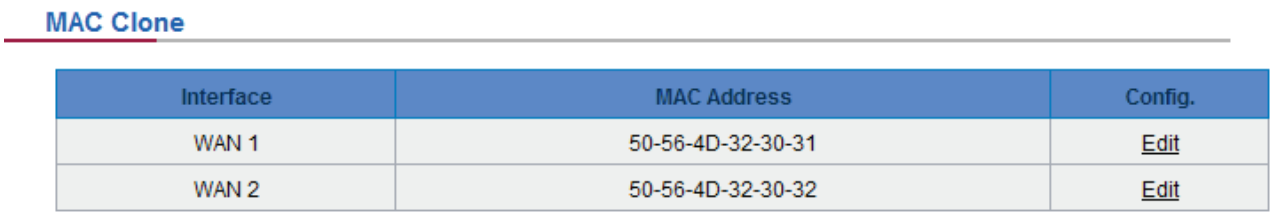
選擇您要配置的廣域網埠，點擊“Edit”進入 DDNS 配置視窗，對要設置的 WAN 口的 DDNS 方式進行勾選。



Interface	顯示使用者所選取的廣域埠。
DDNS	可以選擇 Dyndns.org 以及 3322.org (可以同時使用)。
Username	向 DDNS 服務提供者所申請的使用者名稱。
Password	向 DDNS 服務提供者所申請的密碼。
Host Name	動態網址名稱：向 DDNS 所註冊的網址，如 abc.dynddns.org 或者 abc.3322.org。
Internet IP Address **內部位址**	目前此條 WAN 所取得的 ISP 之動態合法 IP 位址，當路由器得到 ISP 端給的合法 IP 位址後會自動顯示於此。
Status **狀態**	顯示目前路由器對 DDNS 的更新狀態。
Apply	點擊此按鈕“Apply”即會儲存剛才所變動的修改設定內容參數。
Cancel	點擊此按鈕“Cancel”即會清除剛才所變動的修改設定內容參數，此操作必須於確認儲存動作之前才會有效。

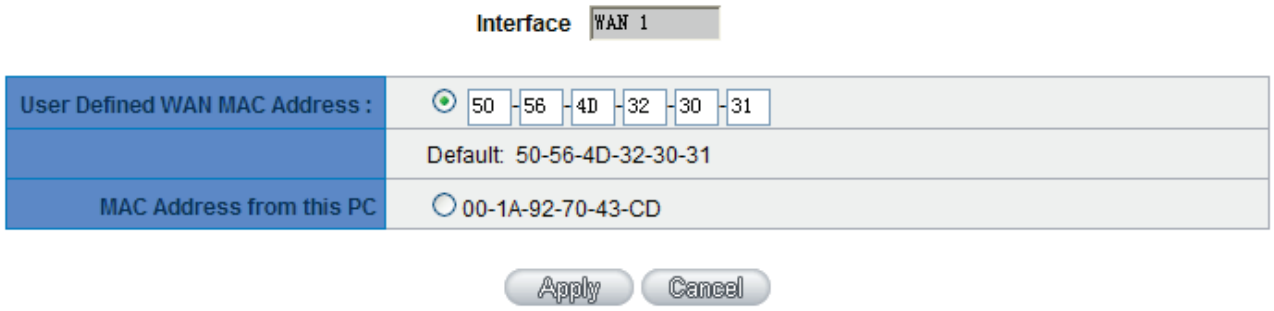
11.6 MAC Clone

有些 ISP 會要求提供一固定 MAC 位址(網卡實體位址)做爲 ISP 端分配 IP 給您的認證使用，此大多適用於 Cable Mode 的用戶。若有此需求的話，可使用此功能將提供給 ISP 的網卡實體位址(MAC 位址：00-xx-xx-xx-xx-xx)填入此項目中，路由器就會以此 MAC 位址作爲跟 ISP 請求 IP 時的認證！



選擇您要配置的廣域網埠，比如“WAN 1”，點擊“編輯”進入 WAN1 的埠 MAC 位址配置視窗，使用者可以自行輸入提供給 ISP 的網卡實體位址 MAC，點擊此按鈕“Apply”即會儲存剛才所變動的修改設定內容參數，點擊此按鈕“Cancel”即會清除剛才所變動的修改設定內容參數，此操作必須於確認儲存動作之前才會有效。

目前設備出廠預設的 MAC 位置爲 WAN 端的 MAC 地址。

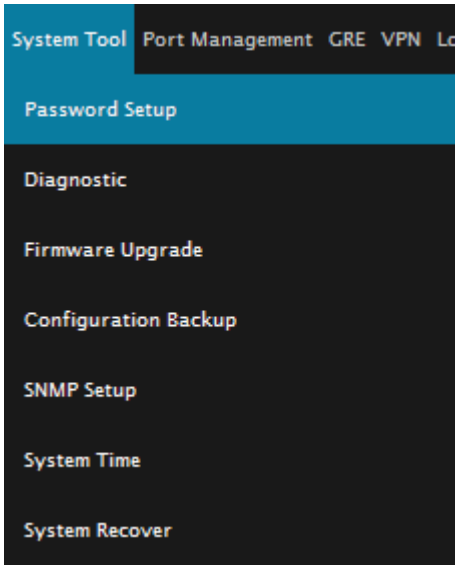


XII. System Tool – 系統工具

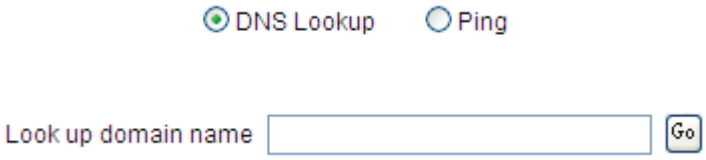
此章節介紹用來管理路由器以及測試網路連線的工具。

考慮安全的因素，建議修改密碼。關於登錄密碼與路由器時間的設定已經在第五章 5.2 節已經介紹，在此就不做重複介紹了。

12.1 Diagnostic

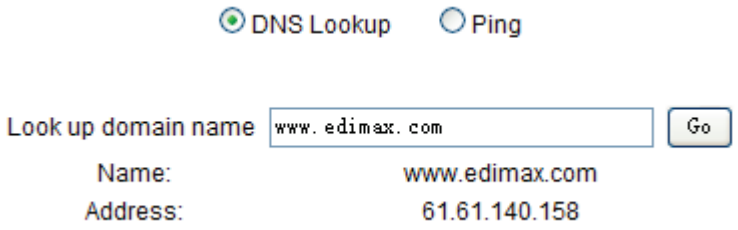


路由器提供簡易的線上測試機制，方便於測試線路品質時使用。此包含 **DNS 查詢**以及 **Ping** 二種。

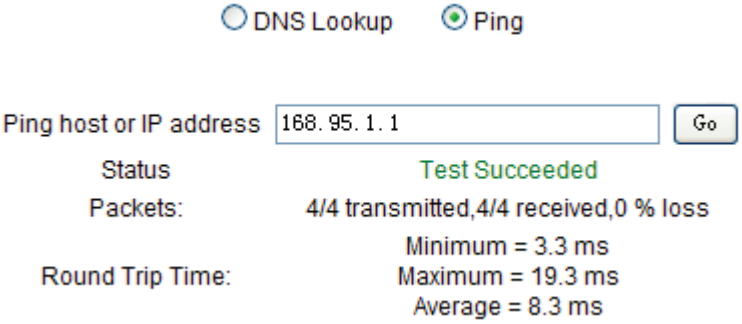


DNS Lookup – DNS 查詢

請於此測試視窗輸入您想查詢的網域主機位置名稱，如 www.edimax.com.tw 然後點擊 **Go** 的按鈕開始測試。測試結果會顯示於此視窗上。



Ping



此專案爲主要提供管理者瞭解對外連線的實際狀況，可以由此功能瞭解網路上的電腦是否存在！

請於此測試視窗輸入您想測試的主機位置 IP，如 168.95.1.1 點擊 **Go** 的按鈕開始測試，測試結果會顯示在視窗上。

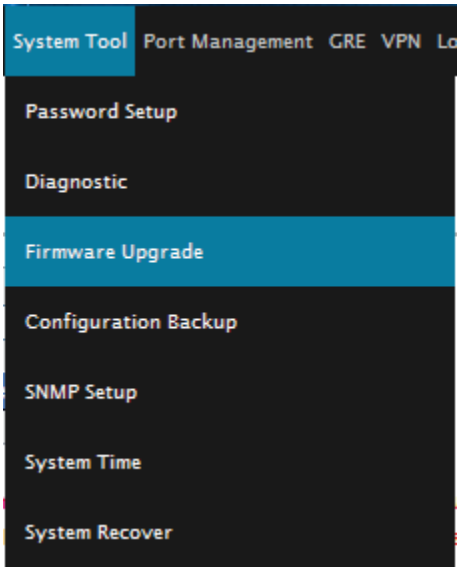
12.2 Firmware Upgrade – 韌體更新

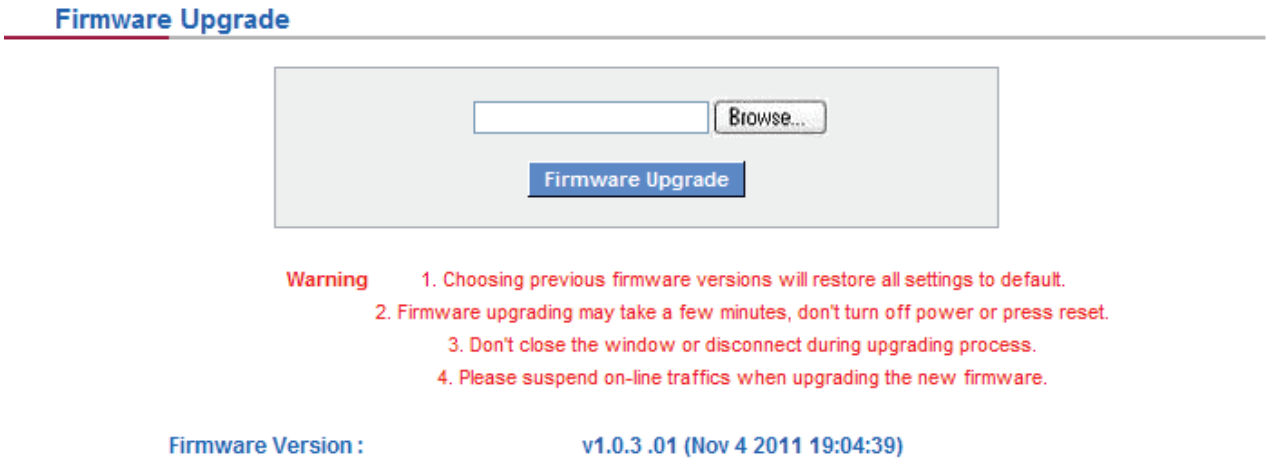
此功能可以讓安全路由器在 Web 設定視窗中直接做韌體升級。請您於升級前先確認韌體版本資訊。 點擊“流覽”按鈕，選擇韌體存放資料夾，並於選擇欲升級的韌體後，點擊 **"Firmware Upgrade Right Now"** 進行更新。

注意！

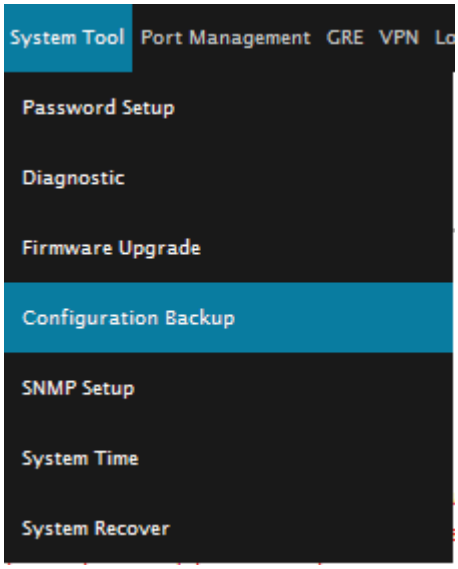
執行韌體升級前，請詳細閱讀視窗中的注意事項。

正在做韌體升級當中時，請勿離開此升級窗口，否則會造成路由器升級失敗。





12.3 Configuration Backup – 設定備份



設定系統配置參數檔匯入：

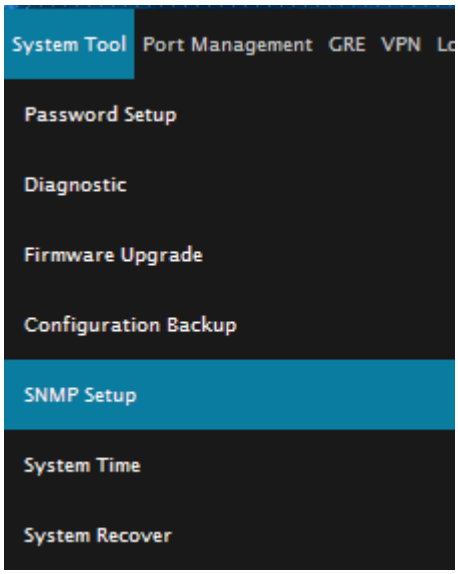
此功能將之前所儲存在電腦的備份設定參數內容回存到路由器中！選擇“Browse”至備份參數檔 “**config.exp**”存放資料夾，選擇該檔後，點擊 **Import** 按鈕做設定檔匯入。

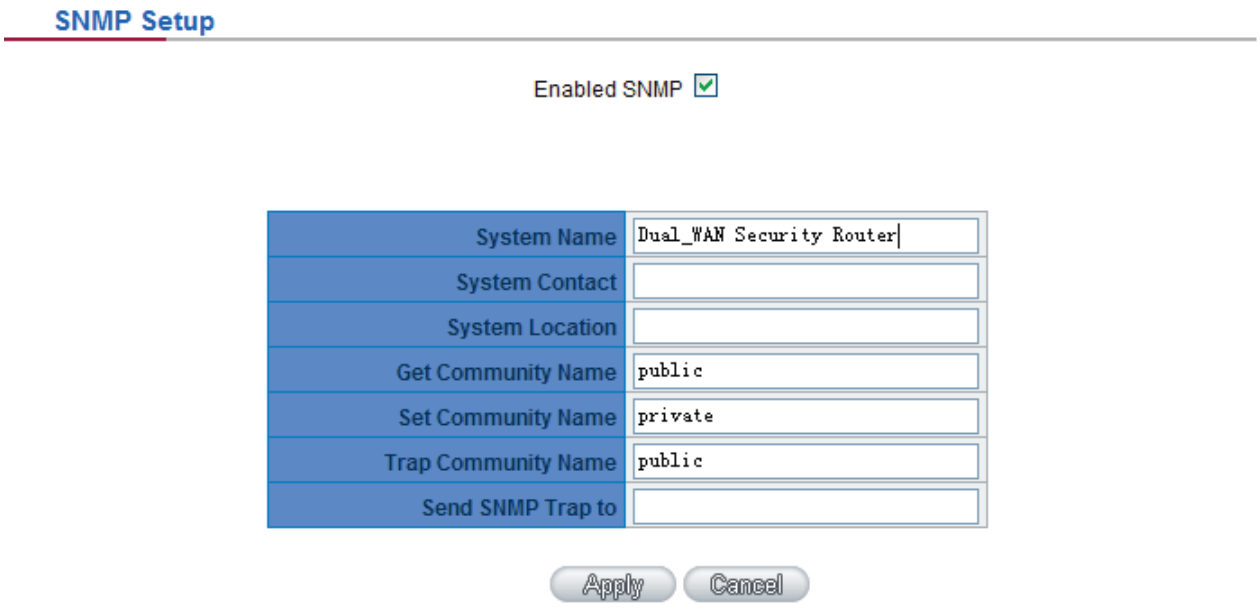
系統配置參數檔儲存：

此功能爲儲存網管人員在路由器的設定參數備份到電腦中，通常做路由器版本升級前，請務必將您現在的路由器設定檔用此功能儲存在電腦中！點擊 **Export** 按鈕，選擇至備份參數檔“**config.exp**”存放資料夾位置，點擊儲存即可。

12.4 SNMP – 簡單網路管理協定設置

SNMP 爲 Simple Network Management Protocol 的縮寫，指網路管理通訊協定。此爲網際網路上使用的一個管理工具。通過此 SNMP 通訊協定，可以讓已經具備有網路管理的程式 (如 SNMP tools-HP Open View) 等網管程式做即時管理之通訊使用。本路由器支援標準 SNMP v1/v2c，可以搭配標準 SNMP 網路管理軟體來得知目前路由器上的機器運作情況，以便隨時掌握網路資訊。

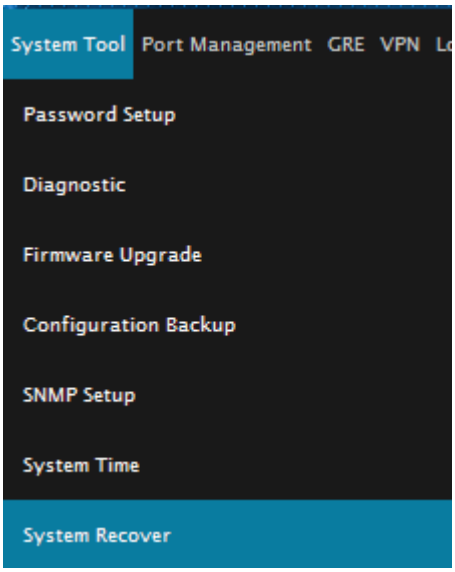


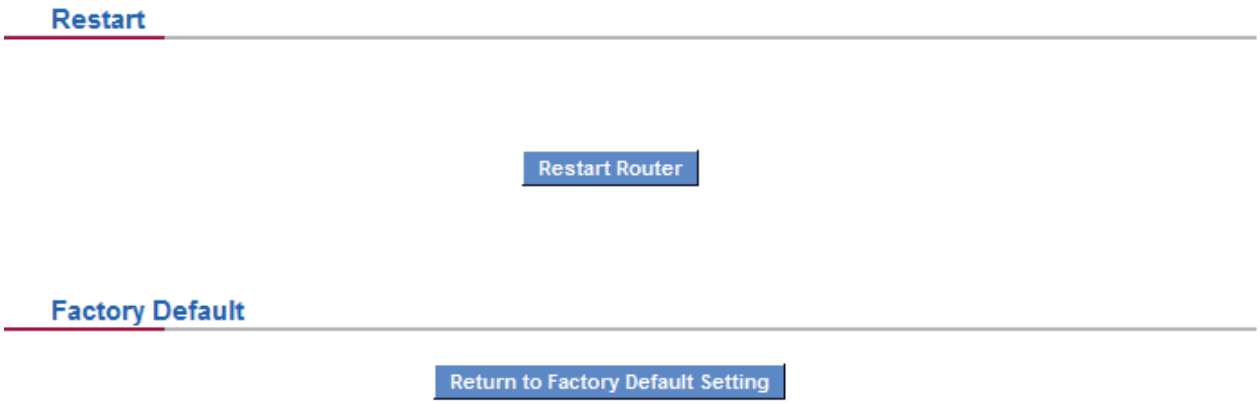


Enabled	將 SNMP 功能開啓或關閉。系統預設爲開啓此功能。
System Name	設定機器的名稱。
System Contact	設定機器的管理聯繫人員名稱。
System Location	設定機器的目前所在位置。
Get Community Name	設定一組管理者參數可以取得此機器的項目資訊，系統預設“Public”。
Set Community Name	設定一組管理者參數可以設定此機器的項目資訊，系統預設“Private”。
Trap Community Name	設定一組管理者參數可以傳送 Trap 的資訊。
Send SNMP Trap to	設定一組 IP 位址或是網域名稱名稱的接收 Trap 訊號主機。
Apply	點選此按鈕“確認”即會儲存剛才所變動的修改設定內容參數。
Cancel	點選此按鈕“取消”即會清除剛才所變動的修改設定內容參數，此操作必須於確認儲存動作之前才會有效。

12.5 System Recover – 系統恢復

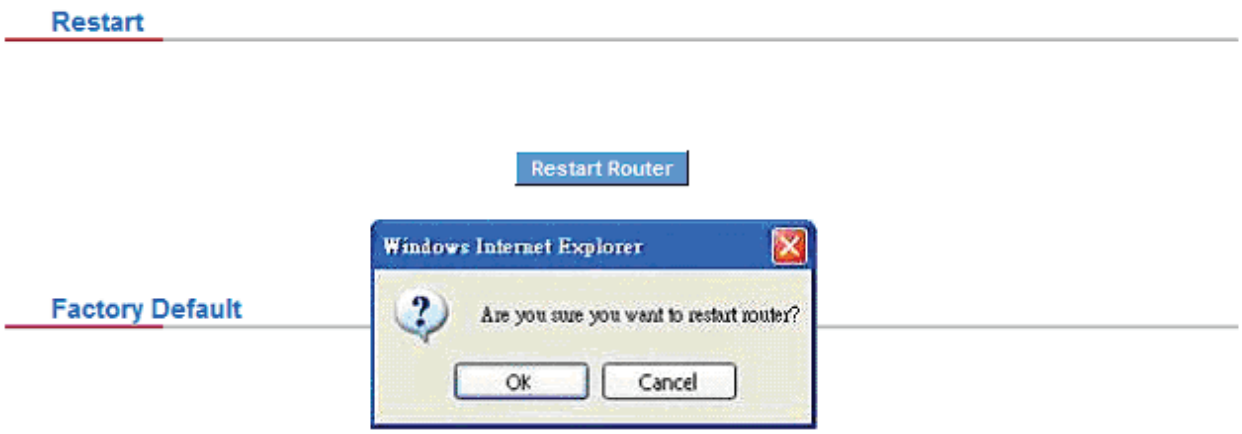
您可以於此工具中選擇路由器系統重新開機功能。





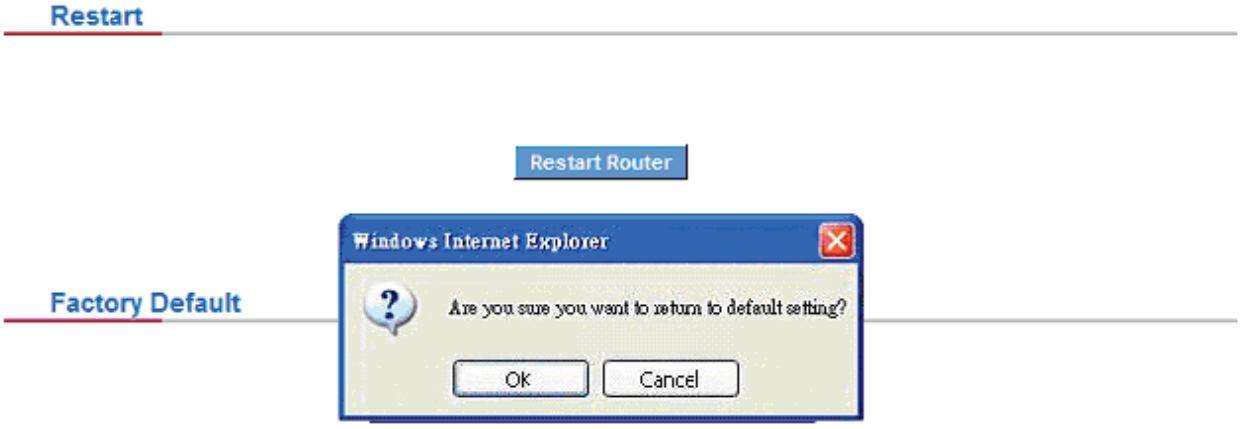
System Recover – 系統重新啓動

如圖，如果點擊系統啓動下的“**Restart Router**”，會彈出提對話方塊提示是否重新啓動路由器，確定路由器就做重新啓動操作。



Return to Factory Default Setting – 回到原廠預設值

若是選擇“**Return to Factory Default Setting**”，會彈出提對話方塊提示是否恢復出廠值，確定後路由器將做恢復出廠值操作。



XIII. USB

本機 USB 可支援 3G 及 WiFi 外接式網卡，進而使安全路由器可以支援 3G 網路以及成爲無線基地台。

13.1 USB 3G

爲了使用 3G 網路功能，您必須具備 3G (WCDMA)網卡以及向電信服務供應商所申請的 SIM 卡。以下將逐步介紹如何進行設定，共有四個步驟如下:

Step 1: USB/3G Connection Setting – USB/3G 連線設定

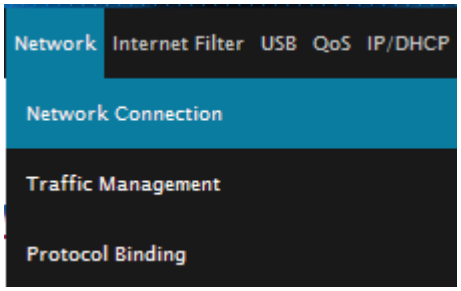
Step 2: Check IP Address for USB/3G Connection – 確認 USB/3G IP 位址

Step 3: Check 3G Info from Service Provider – 確認 3G 服務供應商資訊

Step 4: Configure Advance Setting – 進階設定

13.1.1 Step 1: USB/3G 連線設定

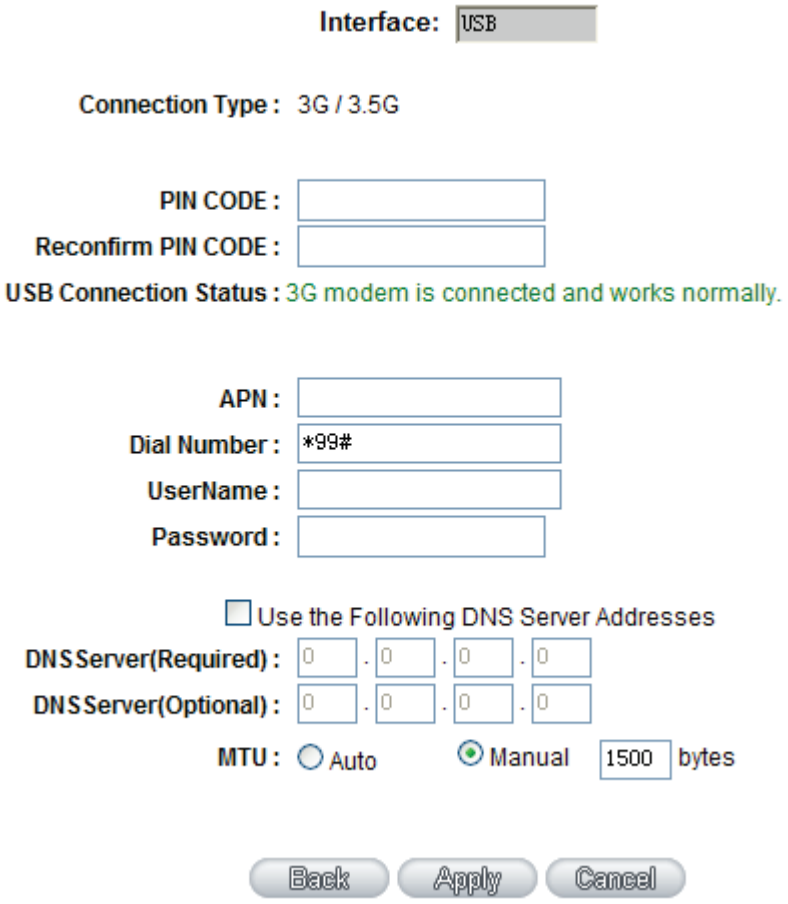
至 Network Connection 選單，於 WAN setting 區塊 USB interface 處按下”**Click**”鈕進行設定。



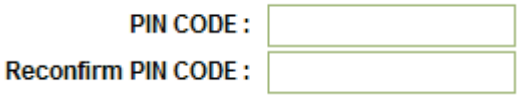
WAN Setting

Please choose how many WAN ports you prefer to use : 2 (Default: 2)

Interface	Connection Type	Config.
WAN 1	Obtain an IP automatically	Edit
WAN 2	Obtain an IP automatically	Edit
USB	3G / 3.5G	Edit



PIN Code – PIN 碼



若您的 SIM 卡具有保護 PIN 碼，請於空格輸入 PIN 碼，若無 PIN 碼則可省略此步驟。

※警告: 當輸入超過三次錯誤的 PIN 碼時，您的 SIM 卡將會被鎖定，並顯示"[PUK] PIN Unlocked Key"。

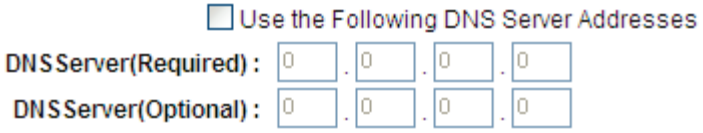
USB Connection Status – USB 連線狀態

特定狀態顯示如下:

- 3G modem is connected and works normally.
  - 3G 網卡已連接並且運作正常。
- 3G modem is connected, but it requires the PIN code to enable the 3G service.
  - 3G 網卡已連接，但需要 PIN 碼啓動。
- 3G modem is connected, but there is no SIM card available. Please insert the SIM card for 3G service.
  - 3G 網卡已連接，但並未偵測到 SIM 卡。請插入 SIM 卡以取得 3G 服務。
- 3G modem is connected, but the SIM card is locked. Please enter the PUK code to unlock.
  - 3G 網卡已連接，但 SIM 卡已被鎖定。請輸入 PUK 碼解鎖。
- 3G modem is not available.
  - 未偵測到 3G 網卡。

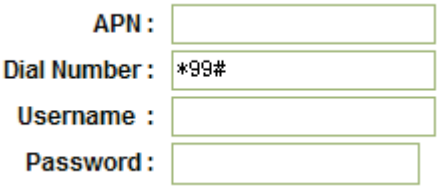
DNS Server – DNS 服務

手動強制路由器使用指派非 ISP 設定之 DNS 服務，部分 ISP 服務會自動指派 DNS。



3G Setting - 3G 設定

填入所有 3G 服務商所提供資訊。



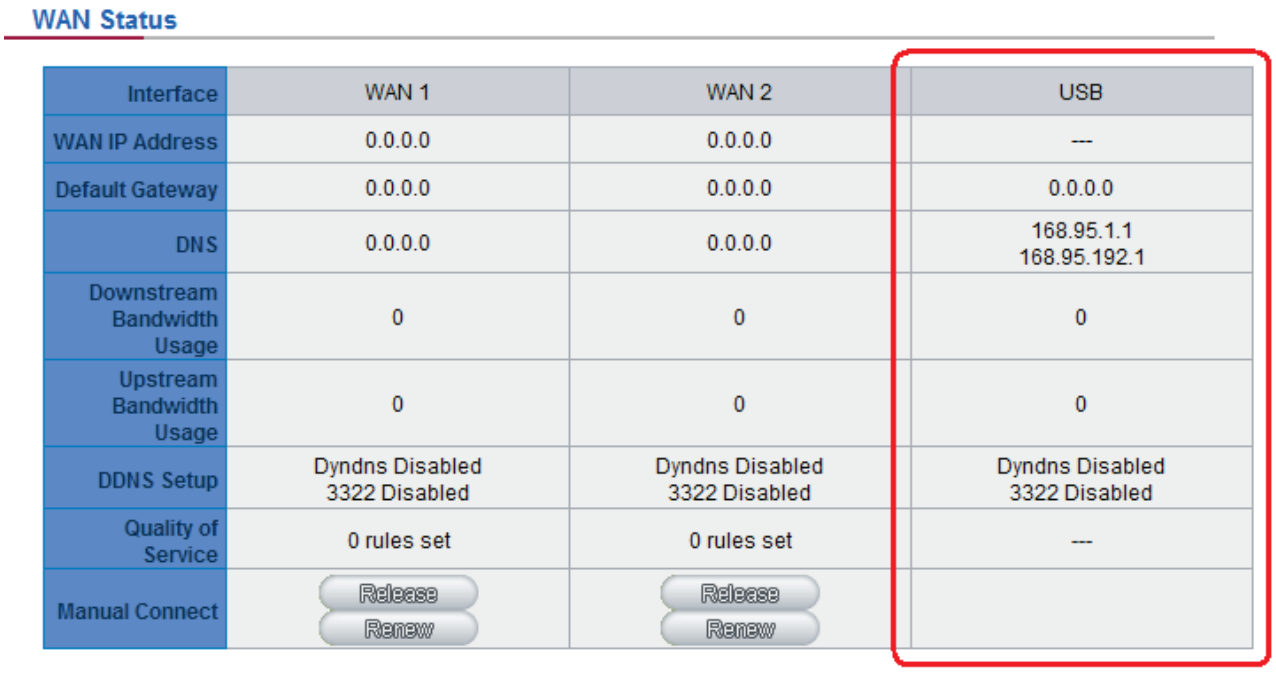
APN: **(Access Point Network)** **行動資料接入點**	大多數服務商預設值爲”**Internet**”。 需要與您的服務供應商確認正確值。

Dial Number **撥接號碼**	WCDMA-UMTS 系統預設值通常爲 ***99#** 。
User name	若有需要輸入使用者名稱。
Password	若有需要輸入密碼。

點擊此按鈕“**Apply**”儲存剛才的設定內容參數。

13.1.2 Step 2: 確認 USB/3G IP 位址

回到首頁並確認 WAN 的狀態。



WAN Status

Interface	WAN 1	WAN 2	USB
WAN IP Address	0.0.0.0	0.0.0.0	---
Default Gateway	0.0.0.0	0.0.0.0	0.0.0.0
DNS	0.0.0.0	0.0.0.0	168.95.1.1 168.95.192.1
Downstream Bandwidth Usage	0	0	0
Upstream Bandwidth Usage	0	0	0
DDNS Setup	Dyndns Disabled 3322 Disabled	Dyndns Disabled 3322 Disabled	Dyndns Disabled 3322 Disabled
Quality of Service	0 rules set	0 rules set	---
Manual Connect	Release Renew	Release Renew	

WAN IP Address	顯示目前 USB 埠的 IP 位址。
Default Gateway	顯示 ISP 的閘道 IP 位址。
Domain Name Server	顯示目前的 DNS IP 位址設定。
Downstream Bandwidth Rate	顯示目前 USB 下載頻寬使用率。
Upstream Bandwidth Rate	顯示目前 USB 下載頻寬使用率。
DDNS Setup	顯示動態域名服務狀態。預設爲”Disabled”。
QoS	Indicate how many QoS rules are set. 顯示目前設定了多少條 QoS 規則。

Manual Connect	Disconnect: 停止目前連線狀態。 Connect:重新啓動連線。

然後確認實體埠狀態 (Physical Port Status)，會顯示目前 USB 埠的狀態。

Connected：3G/3.5G 裝置目前連線中。

Enabled：3G/3.5G 裝置已偵測到，並且等待啓動連線。

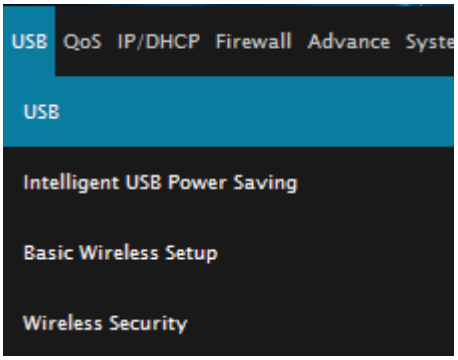
Physical Port Status

Port ID	1	2	3
Interface		LAN	
Status	Connect	Enabled	Enabled

Port ID	Internet	Internet	USB
Interface	WAN 1	WAN 2	USB
Status	Enabled	Enabled	Enabled

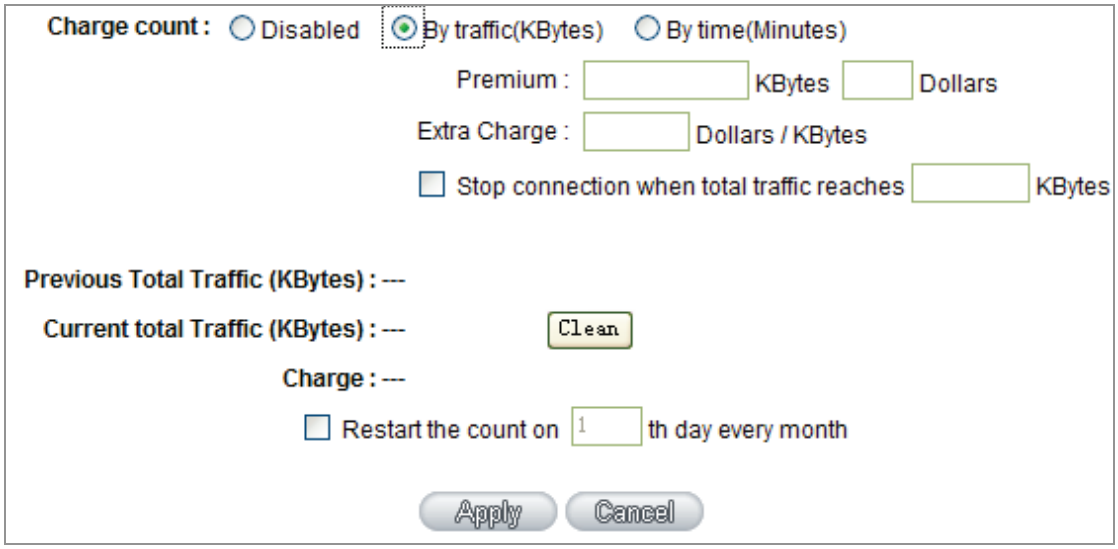
13.1.3 Step 3: 確認 3G 服務供應商資訊

到 USB 選單中進行設定。



Interface	顯示界面爲 USB。
Connection Type **連線類別**	顯示連線類別，預設爲”3G Modem”。
System Provider **系統供應商**	顯示目前系統供應商名稱。
Signal Quality **訊號品質**	顯示目前訊號強度。 按 Refresh 按鈕可更新訊號品質狀態。
Charge count **計費功能**	可依流量或連線時間進行計費。預設值爲”**Disabled**”。

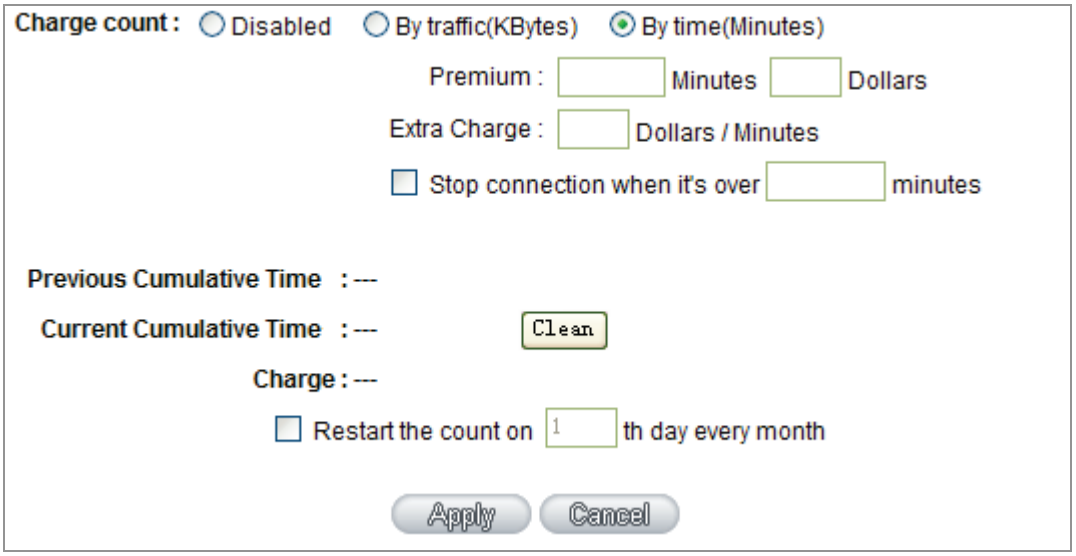
3G service charge by traffic usage – 以流量進行 3G 服務計費



Premium **基本費率**	3G 流量使用基本費率。

Extra charge **超額費用**	當超過基本費率後的額外費用。
Auto Disconnect **自動斷線**	使用者自行定義最大累積流量，以防止 3G 服務費超過預定限制。
Previous Total Traffic **前次使用總流量**	在按下 clean 按鈕前的流量使用記錄。
Current Total Traffic **目前總使用流量**	目前的累積使用流量。
Charge **費用計算**	根據目前總使用流量計算費用。
Restart the count **重新計算**	設定每月重新計費天數。
Clean	手動更新累積記錄。

3G service charge by time usage -以時間進行 3G 服務計費



Premium **基本費率**	3G 流量使用基本費率。
Extra charge **超額費用**	當超過基本可用時間後的額外費用。
Auto Disconnect **自動斷線**	使用者自行定義最大累積可上線時間，以防止 3G 服務費超過預定限制。
Previous Total Traffic **前次使用總流量**	在按下 clean 按鈕前的時間使用記錄。
Current Total Traffic **目前總使用流量**	目前的累積使用時間。
Charge **費用計算**	根據目前總使用時間計算費用。
Restart the count **重新計算**	設定每月重新計費天數。
Clean	手動更新累積記錄。

13.1.4 Step 4: 進階設定

本機支援四種 3G/3.5G USB 接入模式。

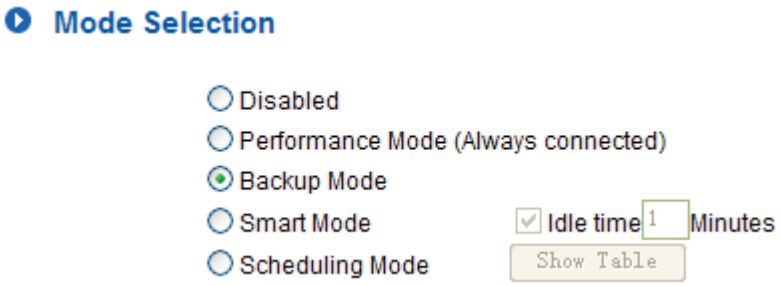
(1) **Disabled**: 3G 服務關閉

(2) **Performance Mode**: 3G 服務永遠連線。

(3) **Backup mode**: 支援 WAN 備援功能，只有在 WAN 埠斷線後才啓動連線。

(4) **Smart mode**: 偵測 WAN 連線狀態以決定 3G/3.5G USB 裝置爲啓動、進入省電模式或是斷電模式。

(5) **Scheduling mode**: 3G 服務按照預先設定排程自動啓動連線或關閉。

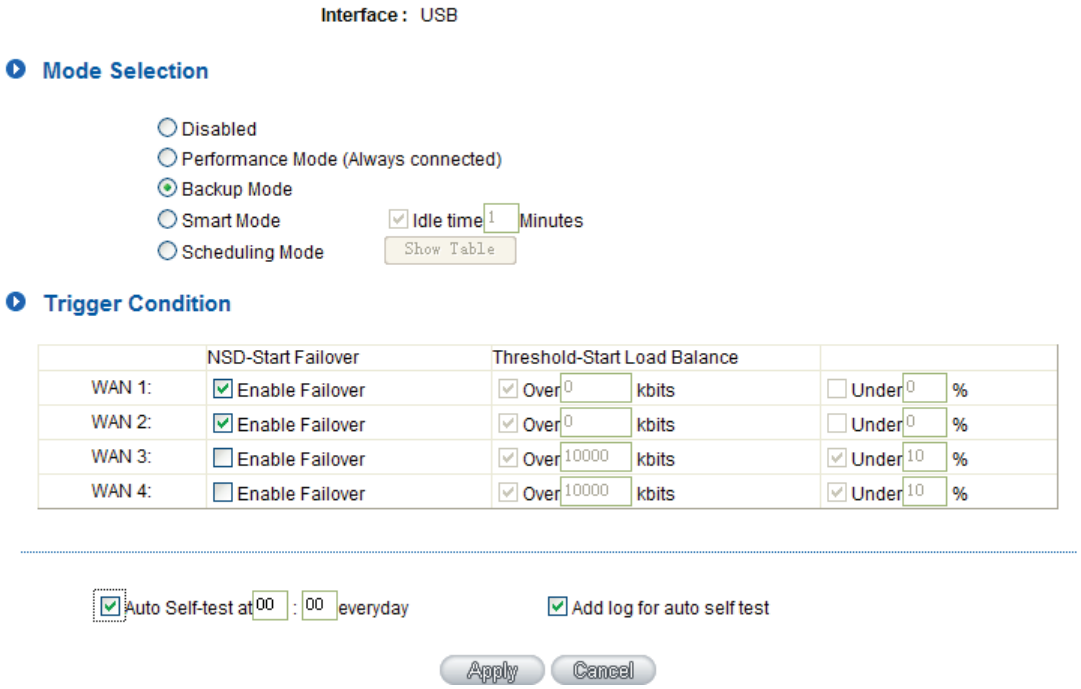


Performance mode

Performance 模式會使 3G/3.5G 服務持續保持在連線狀態，耗電量也高於其他模式。

Backup Mode

當實體 WAN 保持在正常連線狀態下，3G 裝置保持在省電模式。然而當所有的實體 WAN 失效或手動斷線後，3G 服務將會自動進行連線，直到實體 WAN 線路恢復連線。



Trigger Condition – 觸發條件

NSD- Start Failover – 自動偵測啓動備援

1.當選擇的實體 WAN 埠被偵測到斷線

管理者必須至少選擇一個實體 WAN 埠，3G 裝置將會在所選擇的 WAN 埠都已失效後自動進行啓動連線。

2.備援功能

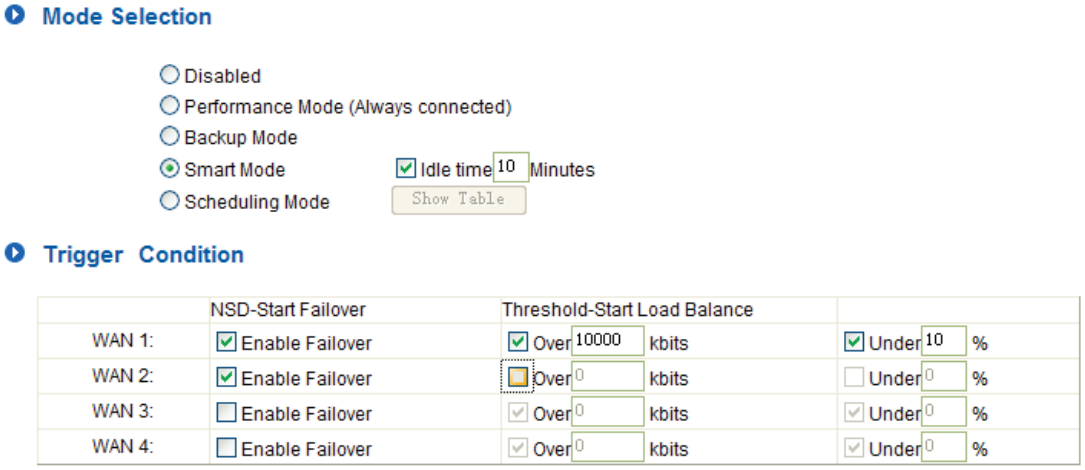
當路由器偵測到所選擇的實體 WAN 埠都已經連線，3G 裝置將會斷線回到省電模式。

Auto self test 自動測試

Interface：USB	顯示界面爲 USB。
☐ Auto Self-test at 00 : 00 everyday	USB 3G/3.5G 裝置將會每天在所設定時間啓動進行連線測試。
Add log for auto self test	在系統日誌中加入測試紀錄。

Smart Mode

路由器會使 3G 裝置在設定的閑置時間內保持在省電模式下。但當所有實體 WAN 連線正常，且超過設定的閑置時間時，路由器將會停止供電給 USB 裝置。但當所有有線 WAN 連線失效或被斷線時，3G 裝置將會自動再啓動進行連線。



Threshold- Start Load Balance: 啓動負載均衡門檻設定

網管除了可以選擇哪個 WAN 埠需要 3G 服務備援，也可設定頻寬門檻來啓動負載均衡功能。當該實體 WAN 埠使用頻寬超過設定數時，3G 裝置也會自動連線與實體 WAN 埠進行負載均衡。

注意! 設定啓動負載均衡門檻前，網管必須勾選 NSD-Start 選項。

1. 設定門檻，啓動負載均衡

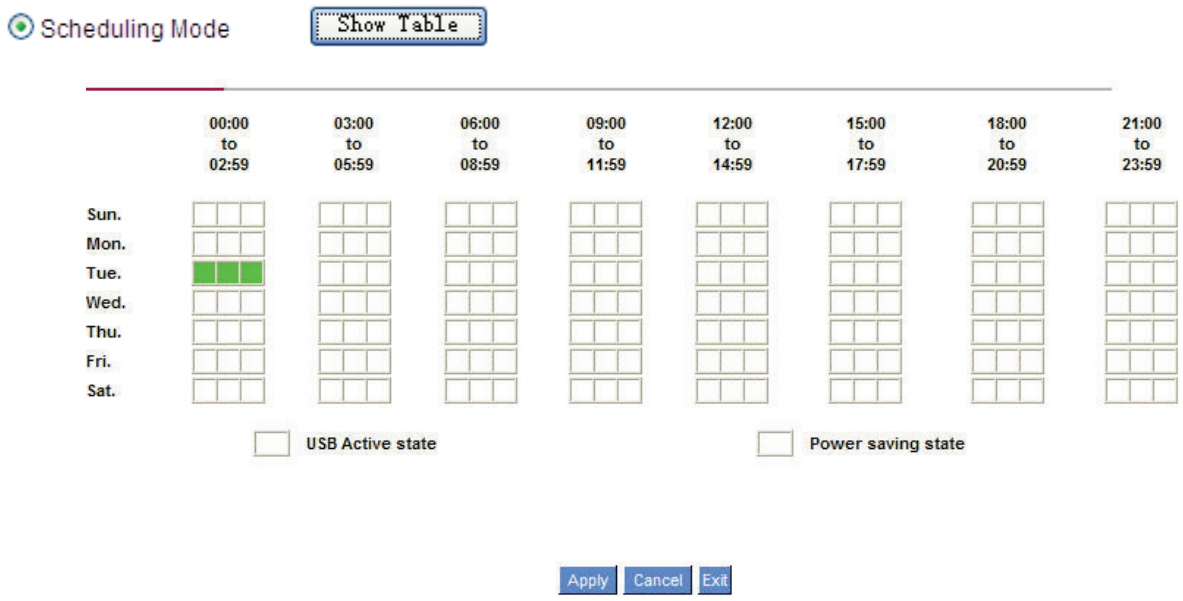
以上面使用者界面截圖爲例，當路由器偵測到 WAN1 流量超過 10000Kbits 時，3G 服務將會啓動進行負載均衡。

2. 回復省電模式

當 3G 裝置已經連線進行負載均衡時，路由器仍會持續偵測 WAN1 的流量使用狀態，當流量低於 10%時，路由器將會讓 3G 裝置回復到省電模式。

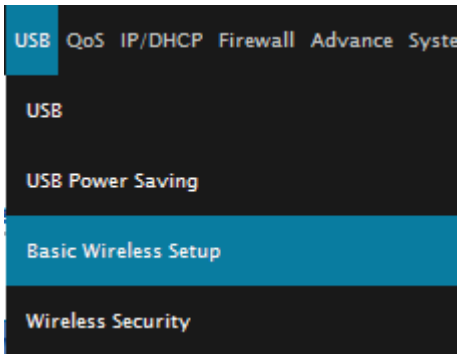
Scheduling Mode

在 Schedule mode 中，網管可以設定 3G/3.5G 的連線時間表，在勾選的時間內，3G 服務將會連線進行負載均衡。

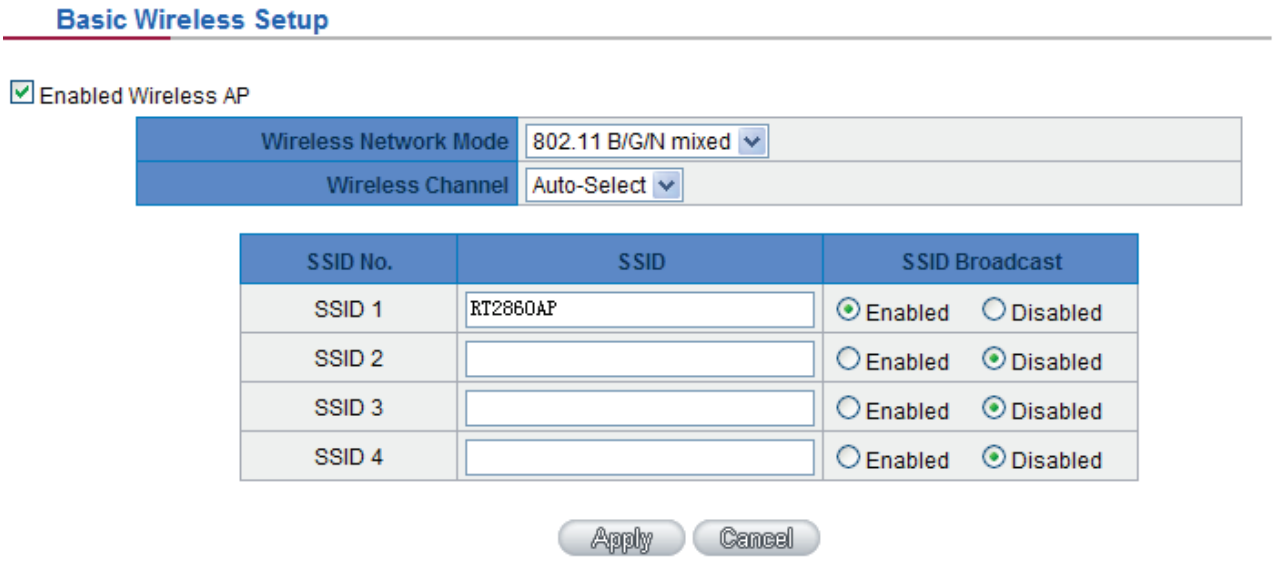


13.2 USB Wireless

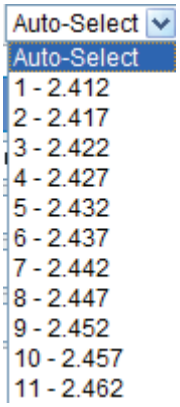
本機 USB 埠亦可支援 Wifi 外接式網卡成爲 WLAN 基地台。以下將介紹如何進行無線網路設定。



13.2.1 Basic Wireless Setup

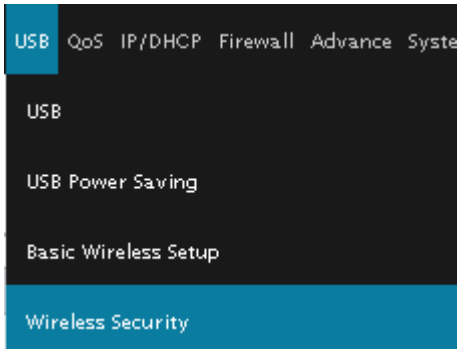


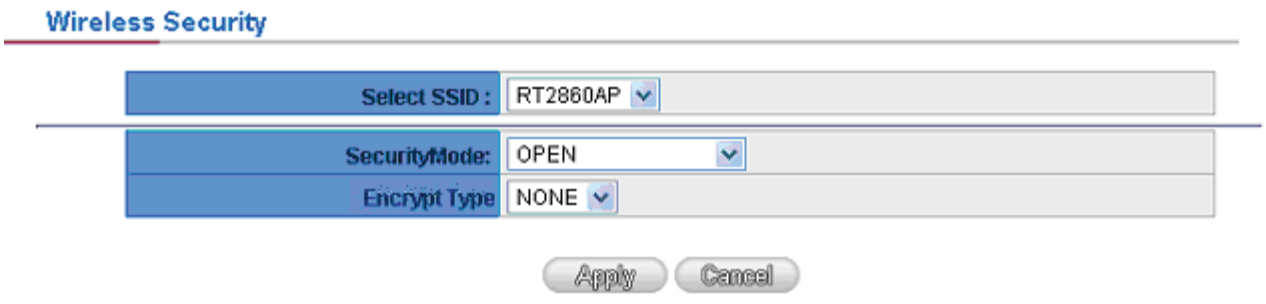
Enabled Wireless AP **啓動無線 AP 功能**	勾選此項目啓動 WiFi AP 功能。
Wireless Network Mode **無線網路模式**	有六種模式可以選擇，預設值爲 **802.11 B/G/N mixed**。

	
Wireless Channel **無線網路頻道**	有 11 個頻道可以選擇，預設值爲 **Auto-Select**。 
SSID	輸入 SSID (服務設定識別碼)並選擇啓動 Enable 或關閉 Disable。

點擊此按鈕**“Apply”**儲存剛才的設定內容參數。

13.2.2 Wireless Security Setting - 安全設定



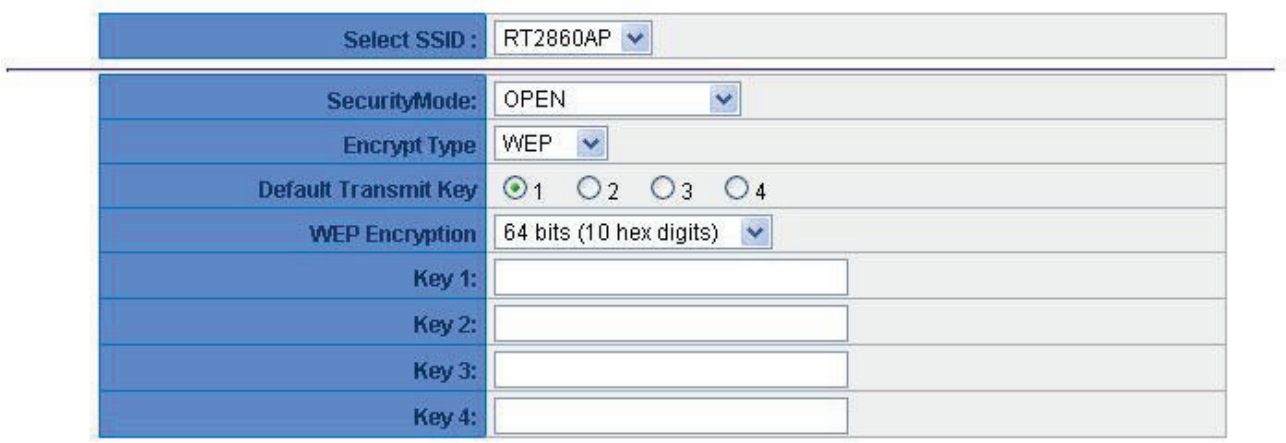


以下開始介紹設定流程:

Select SSID	選擇欲設定的 SSID。
Security Mode	選擇無線網路安全模式。路由器提供九種形式可供設定。 OPEN OPEN SHARED WEPAUTO WPAPSK WPA WPA2PSK WPA2 WPA1WPA2 WPAPSKWPA2PSK

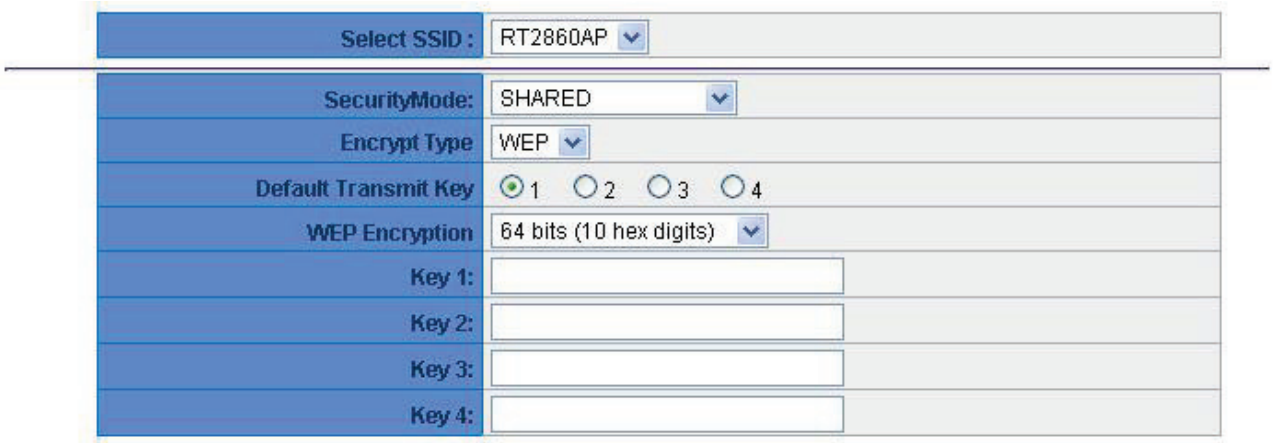
以下將介紹各種安全模式的加密設定。

Open



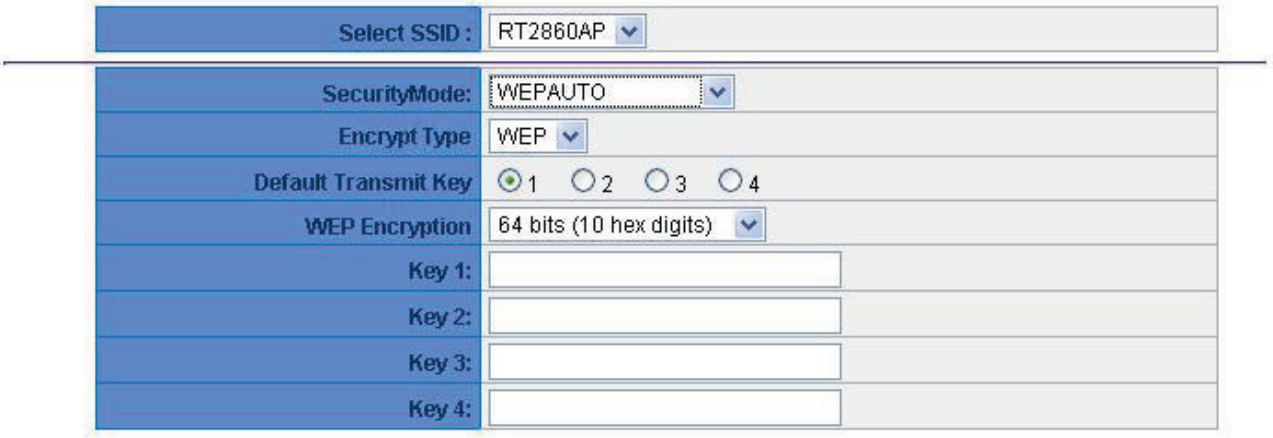
Encrypt Type **加密形式**	可選擇 **None** 及 **WEP**。 若選擇 **None**，將不會進行加密，任何使用者皆可進行無線網路連線，不建議使用此種模式。
Default Transmit Key **預設密鑰**	選擇欲採用哪一組密鑰。
WEP Encryption **WEP 加密**	可選擇 **64 bits** 或 **128 bits**，
Key **密鑰設定**	支援四組安全密鑰。

Shared



Encrypt Type 加密形式	支援 **WEP** 模式。
Default Transmit Key 預設密鑰	選擇欲採用哪一組密鑰。
WEP Encryption **WEP** 加密	可選擇 **64 bits** 或 **128 bits**，
Key 密鑰設定	支援四組安全密鑰。

WEPAUTO



Encrypt Type 加密形式	支援 **WEP** 模式。

Default Transmit Key **預設密鑰**	選擇欲採用哪一組密鑰。
WEP Encryption **WEP 加密**	可選擇 **64 bits** 或 **128 bits**，
Key **密鑰設定**	支援四組安全密鑰。

WPAPSK

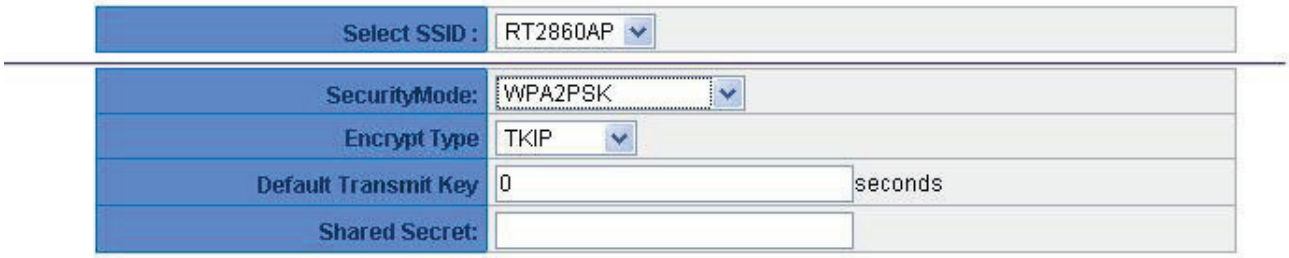
Encrypt Type **加密形式**	支援 **TKIP**, **AES** 及 **TKIPAES** 模式。
Default Transmit Key **預設密鑰**	設定 rekey 時間，預設爲 30 秒。
Shared Secret **密鑰設定**	輸入密鑰，使用者必須要有密鑰才可接入無線網路。

WPA

Encrypt Type **加密形式**	支援 **TKIP**, **AES** 及 **TKIPAES** 模式。
Default Transmit Key	設定 rekey 時間，預設爲 30 秒。

預設密鑰	
Shared Secret 密鑰設定	輸入密鑰，使用者必須要有密鑰才可接入無線網路。

WPA2PSK



Encrypt Type 加密形式	支援 **TKIP**, **AES** 及 **TKIPAES** 模式。
Default Transmit Key 預設密鑰	設定 rekey 時間，預設爲 30 秒。
Shared Secret 密鑰設定	輸入密鑰，使用者必須要有密鑰才可接入無線網路。

WPA2

Encrypt Type 加密形式	支援 **TKIP**, **AES** 及 **TKIPAES** 模式。
Default Transmit Key 預設密鑰	設定 rekey 時間，預設爲 30 秒。
Shared Secret 密鑰設定	輸入密鑰，使用者必須要有密鑰才可接入無線網路。

WPA1WPA2

Encrypt Type 加密形式	支援 **TKIP**, **AES** 及 **TKIPAES** 模式。
Default Transmit Key 預設密鑰	設定 rekey 時間，預設爲 30 秒。
Shared Secret 密鑰設定	輸入密鑰，使用者必須要有密鑰才可接入無線網路。

WPAPSKWPA2PSK

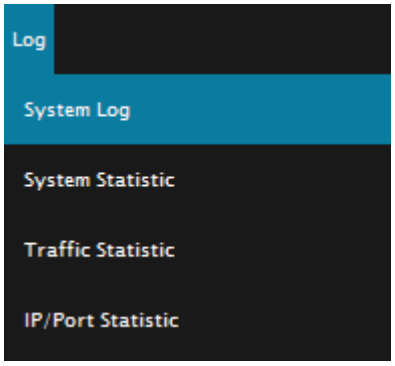
Encrypt Type 加密形式	支援 **TKIP**, **AES** 及 **TKIPAES** 模式。
Default Transmit Key 預設密鑰	設定 rekey 時間，預設爲 30 秒。
Shared Secret 密鑰設定	輸入密鑰，使用者必須要有密鑰才可接入無線網路。

XIV. Log –日誌功能設定

日誌功能紀錄路由器的運行資料，並以可讀的方式呈現再設定視窗上提供給您作爲參考。您可以依據需求檢視這些資訊。

14.1 System Log – 系統日誌

路由器的日誌記錄提供下列設定:

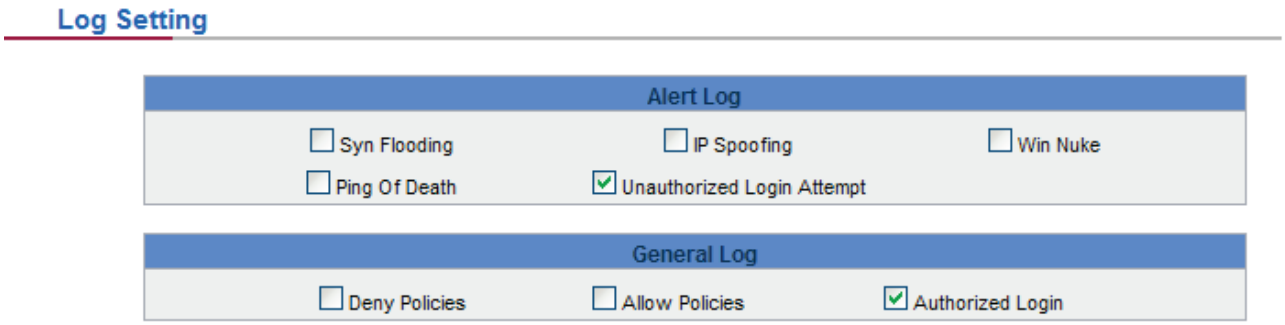


。

System Log – 系統日誌

Enable Syslog **啓動系統日誌**	若是勾選此選項的話，傳送系統日誌功能將被開啓。
Syslog Server **系統日誌伺服器**	提供了外部系統日誌伺服器收集系統資訊功能。系統日誌爲一項工業標準通訊協定，於網路上動態擷取有關的系統資訊。路由器的系統日誌 提供了包含動作中的連線來源位置與目地位置，服務編號以及狀態。輸入您要接收系統日誌的伺服器名稱或是 IP 位址於“**Syslog Server**”的空格欄位內。

Log Setting – 日誌設定



Alert Log – 告警日誌

本路由器提供可勾選下列告警訊息: Syn Flooding, IP Spoofing, Win Nuke, Ping of Death / Unauthorized Login Attempt。

Syn Flooding	在短時間內傳送大量 syn 封包進行阻斷式攻擊，使系統造成負荷過重。
IP Spoofing	駭客藉由封包竊聽攔截在網路中傳送的資料。透過冒充發送者 IP 進行資料攔截。
Win Nuke	伺服器正被木馬程式攻擊。
Ping of Death	傳送資料超過系統可負荷最大封包數導致系統失效。
Unauthorized Login	如發現入侵者企圖登入，將會被系統日誌所記錄。

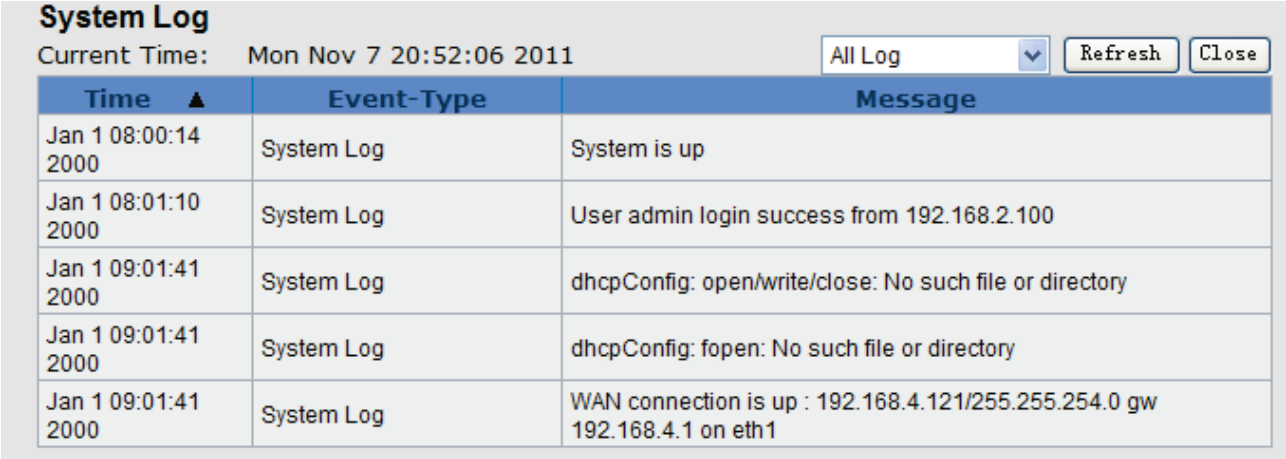
General Log – 一般系統日誌資訊

路由器提供了包含以下的一般性內容資訊，您只要打勾點選即可。系統錯誤資訊，被阻擋的管制條例，允許通過的管制條例，認證登錄，系統配置變更。

Deny Policies **阻擋管制條例**	當有用戶試圖進行存取規則中不允許的規則時，此資訊會傳送到系統日誌中。
Allow Policies **允許管制條例**	當用戶進行存取規則所允許的規則時，此資訊會傳送到系統日誌中。
Authorized Login **認證允許**	每一個成功登錄系統的 IP 位址都會傳送並記錄到系統日誌中。

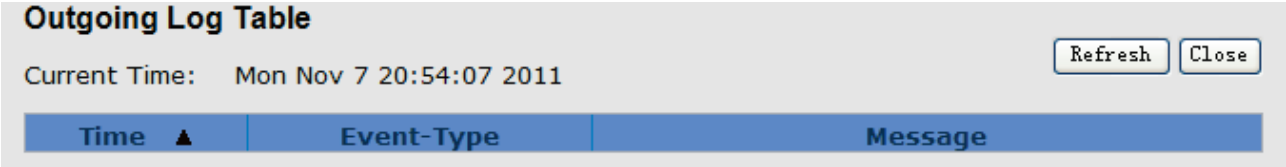
以下有四個有關查詢日誌的按鈕，分別敍述如下：View System Log：

此爲查看系統日誌使用，其資訊內容可以從下拉式選單中分類讀取，包含 **All Log, System Log, Access Log, and Firewall Log**，以下將逐一介紹。



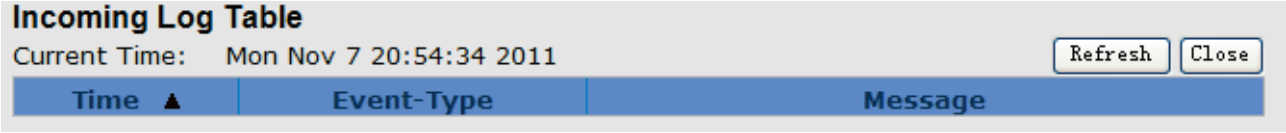
Outgoing Packet Log – 對外封包記錄

查看內部 PC 出互聯網 的系統封包日誌，此日誌包含內部網路位址，目的地位址以及所使用的通訊服務埠號、類型等資訊。



Incoming Packet Log - 進入的封包

查看外部進入路由器的系統封包日誌，此日誌內涵外部來源網路位址， 目的地位址與通訊埠號等資訊。



Clear Log Now – 消除日誌

此按鈕爲清除所有目前路由器的日誌相關資訊。

14.2 System Statistic -系統狀態即時監控

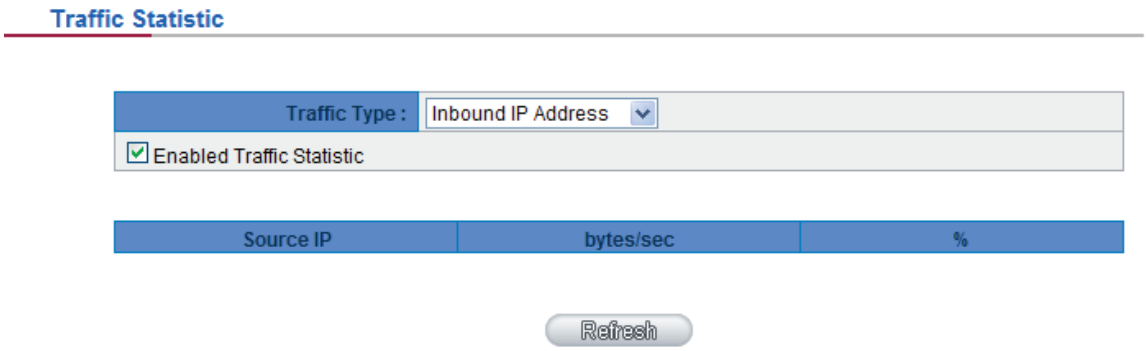
路由器的系統狀態即時監控管理功能可以提供系統目前的運作資訊，包含區域或廣域埠名稱，目前埠連線狀態，IP 位址，網路實體位置(MAC 位址)，子網路遮罩，預設閘道，網域名稱解析伺服器(DNS)，網路偵測，收到的封包數量，傳送的封包數量，全部的進出封包數量統計，收到的封包 Byte 流量統計，傳送的封包 Byte 流量統計，全部進出的封包 Byte 流量統計，收到的錯誤封包統計以及埠丟棄的封包統計，連線數，新連線數，上傳頻寬使用率，下載頻寬使用率等資訊。

System Statistic

Interface	WAN 1	WAN 2	USB	LAN
Device Name	eth1	eth2	ppp3000	eth0
Status	Connect	Enabled	Disabled	---
Device IP Address	192.168.4.121	0.0.0.0	0.0.0.0	192.168.2.1
MAC Address	50-56-4D-32-30-31	50-56-4D-32-30-32	--------	50-56-4D-32-30-30
Subnet Mask	255.255.254.0	0.0.0.0	0.0.0.0	255.255.255.0
Default Gateway	192.168.4.1	0.0.0.0	0.0.0.0	---
DNS	192.168.5.121 192.168.5.120	0.0.0.0	0.0.0.0	---
Network Service Detection	Test Succeeded	Test Failed	---	---
Received Packets	6362	0	---	7245
Transmitted Packets	1264	6	---	33403
Total Packets	7626	6	---	40648
Received Packets Byte	1121248	0	---	760956
Transmitted Packets Byte	234237	468	---	6348779
Total Packets Byte	1355485	468	---	7109735
Received Byte/Sec	319	0	---	4691
Transmitted Byte/Sec	0	0	---	8010
Error Packets	0	0	---	0
Dropped Packets	0	0	---	0
Sessions	0	0	---	---
New Sessions/Sec	0	0	---	---
Upstream Bandwidth Usage	0	0	---	---
Downstream Bandwidth Usage	0	0	---	---

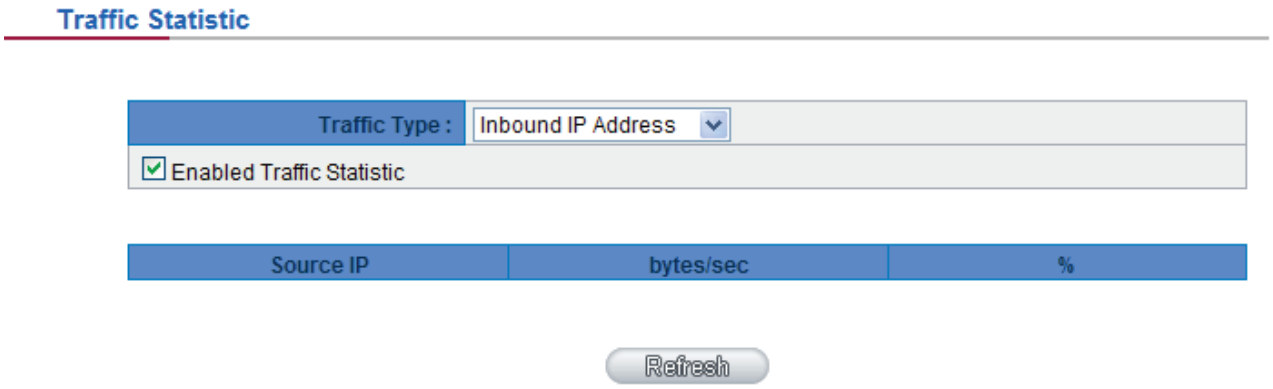
14.3 Traffic Statistic – 流量統計

路由器提供六種顯示流量統計的資訊，來提供管理者對於流量有更好的管理與控制。



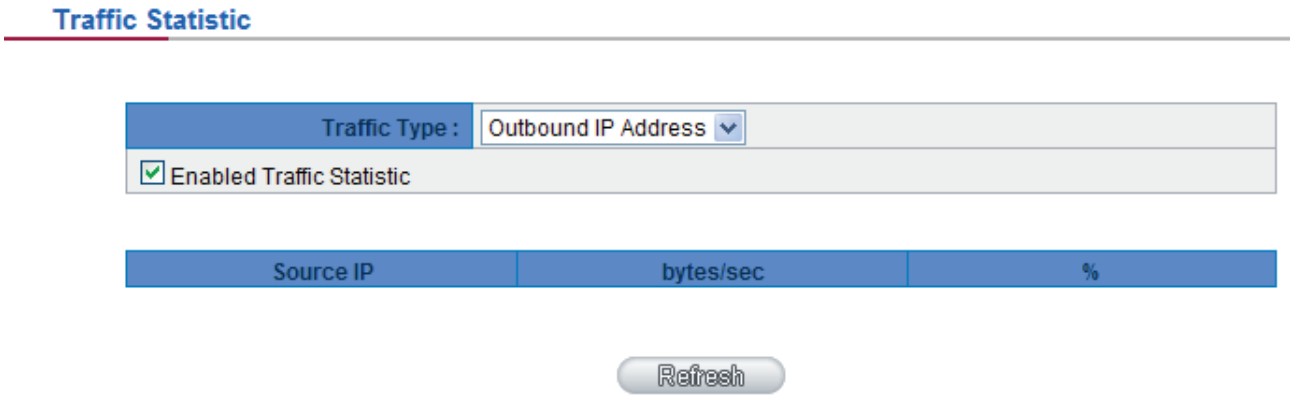
Inbound IP Source Address - 對內 IP 流量統計

在此圖表中顯示了從外進入內網流量的來源端的 IP 地址， 每秒有多少 byte 與所占的百分比。



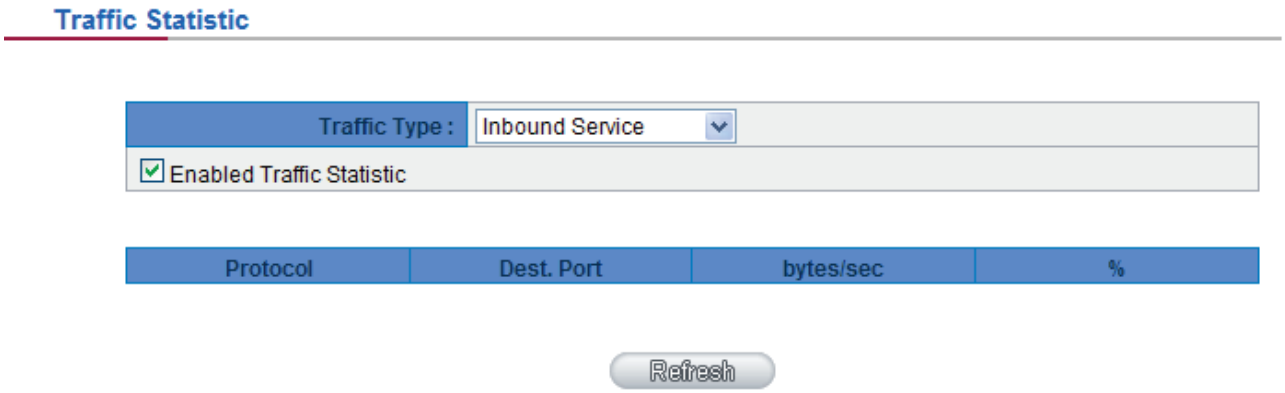
Outbound IP Source Address - 對外 IP 流量統計

在此圖表中顯示了叢內網出去流量的來源端的 IP 地址， 每秒有多少 byte 與所占的百分比。



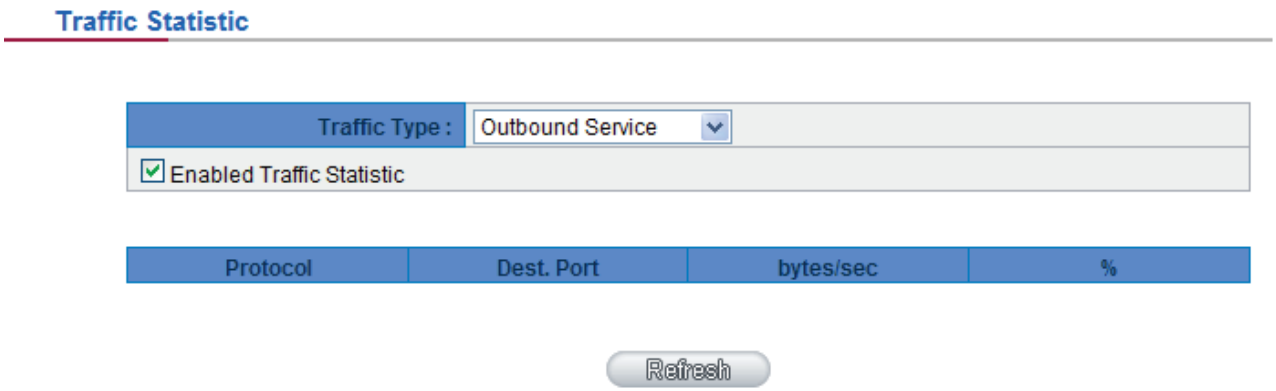
Inbound IP Service - 對內服務端口流量統計

在此圖表中顯示了以網路的服務埠來分類進入內網使用流量統計(每秒)byte 與百分比。



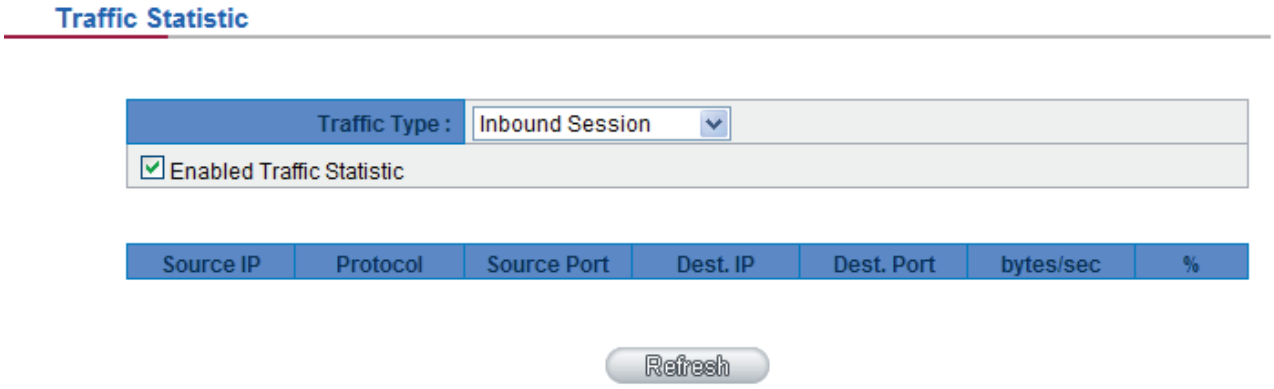
Outbound IP Service - 對外服務端口流量統計

在此圖表中顯示了以網路的服務埠來分類從內網出去的使用流量統計(每秒)byte 與百分比。



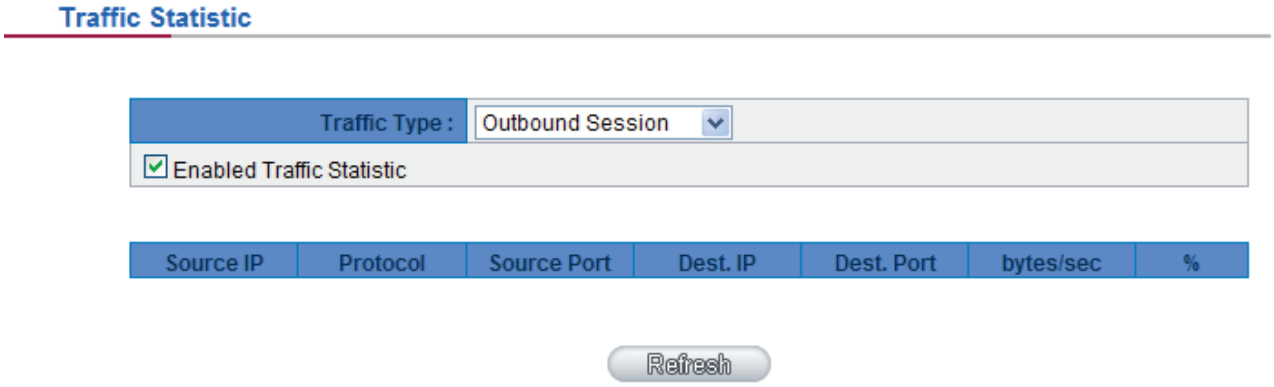
Inbound IP Session - 對內聯機流量統計

在此圖表中顯示了從廣域網路進來的(Dest. IP)位址所連線的區域網路的 IP(Source IP)位置所使用的服務埠(Dest.Port)還有現在使用流量(bytes/sec)與百分比。



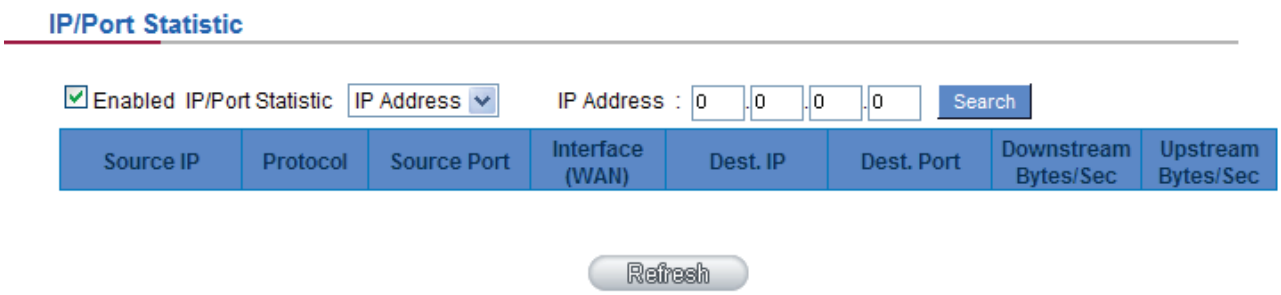
Outbound Session - 對外聯機流量統計

在此圖表中顯示了從區域網路的 IP(Source IP)位址對外連線的目的地位置(Dest. IP)IP及所使用的服務埠(Dest.Port)還有現在使用流量(bytes/sec)與百分比。



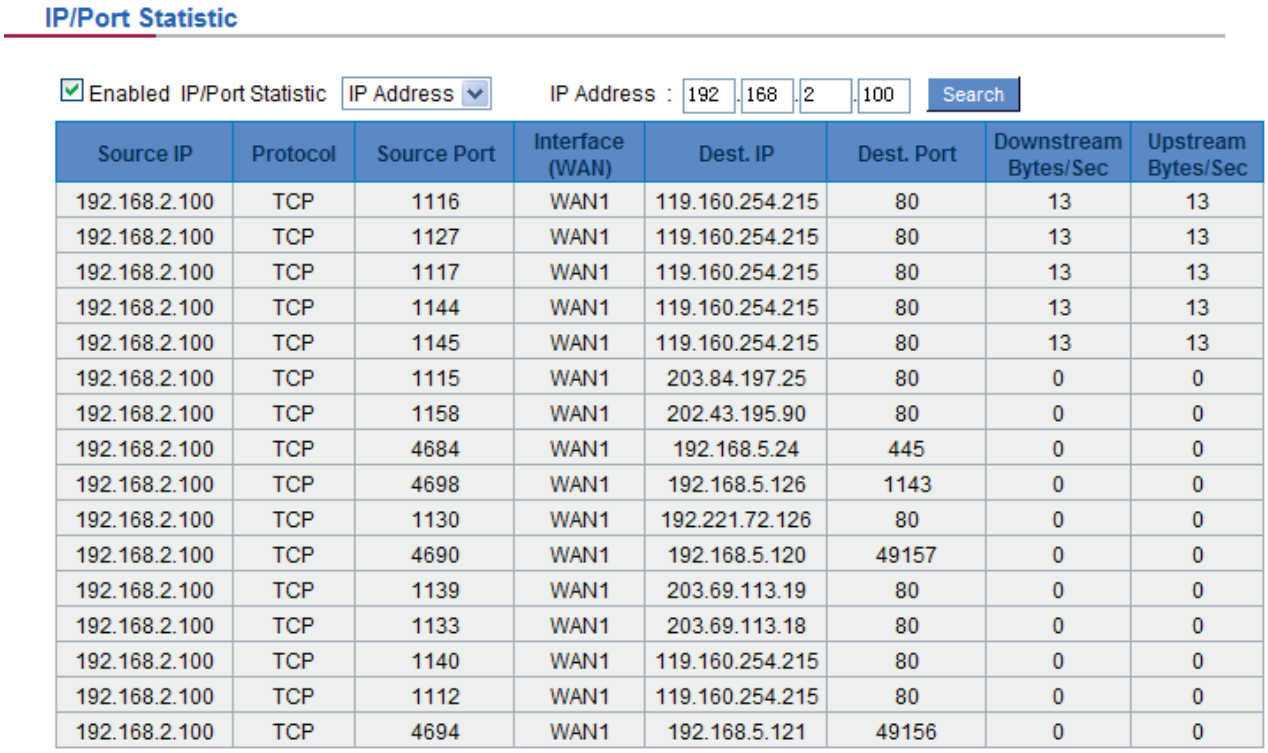
14.4 IP/ Port Statistic - 特定 IP 及埠狀態

路由器提供網管人員可以針對某一 IP 或某一特定埠去查詢此 IP 去訪問的目的地址，或是有哪些人使用這個服務埠。其目的可以方便找出某些需要認證的網站無法走多 WAN 埠而必須走單一個 WAN 埠，網管人員可以查詢出此目的地的 IP 做協議綁定來解決此登錄問題。另外，若想查詢何人在使用 BT 或 P2P 軟體，也可選擇 Port 做使用者查詢。



Specific IP Status – 特定 IP 狀態

直接在 IP 位址裏填入您想要查詢的 IP 位址，就可以顯示出此 IP 對外連線的所有目的地及埠號。



Source IP	Protocol	Source Port	Interface (WAN)	Dest. IP	Dest. Port	Downstream Bytes/Sec	Upstream Bytes/Sec
192.168.2.100	TCP	1116	WAN1	119.160.254.215	80	13	13
192.168.2.100	TCP	1127	WAN1	119.160.254.215	80	13	13
192.168.2.100	TCP	1117	WAN1	119.160.254.215	80	13	13
192.168.2.100	TCP	1144	WAN1	119.160.254.215	80	13	13
192.168.2.100	TCP	1145	WAN1	119.160.254.215	80	13	13
192.168.2.100	TCP	1115	WAN1	203.84.197.25	80	0	0
192.168.2.100	TCP	1158	WAN1	202.43.195.90	80	0	0
192.168.2.100	TCP	4684	WAN1	192.168.5.24	445	0	0
192.168.2.100	TCP	4698	WAN1	192.168.5.126	1143	0	0
192.168.2.100	TCP	1130	WAN1	192.221.72.126	80	0	0
192.168.2.100	TCP	4690	WAN1	192.168.5.120	49157	0	0
192.168.2.100	TCP	1139	WAN1	203.69.113.19	80	0	0
192.168.2.100	TCP	1133	WAN1	203.69.113.18	80	0	0
192.168.2.100	TCP	1140	WAN1	119.160.254.215	80	0	0
192.168.2.100	TCP	1112	WAN1	119.160.254.215	80	0	0
192.168.2.100	TCP	4694	WAN1	192.168.5.121	49156	0	0

Specific Port Status – 特定埠狀態

直接在埠裏填入您想要查詢的埠號，就可以顯示出此埠現在有哪些 IP 正在使用。

IP/Port Statistic

Enabled IP/Port Statistic | Port | Port : 80 | Search

Source IP	Protocol	Source Port	Interface (WAN)	Dest. IP	Dest. Port	Downstream Bytes/Sec	Upstream Bytes/Sec
192.168.2.100	TCP	1130	WAN1	192.221.72.126	80	0	0
192.168.2.100	TCP	1115	WAN1	203.84.197.25	80	0	0
192.168.2.100	TCP	1133	WAN1	203.69.113.18	80	0	0
192.168.2.100	TCP	1139	WAN1	203.69.113.19	80	0	0

XV. Log Out – 登出

若您想登出路由器 WEB UI，只需要關掉瀏覽器視窗即可。若您下次想再進入路由器管理視窗時，您必須重複登錄路由器管理視窗的步驟，並輸入管理者的使用名稱與密碼。

EDIMAX

NETWORKING PEOPLE TOGETHER

Edimax Technology Co., Ltd.
No.3, Wu-Chuan 3rd Road, Wu-Gu,
New Taipei City 24891, Taiwan

Edimax Technology Europe B.V.
Nijverheidsweg 25 5683 CJ Best
The Netherlands

Edimax Computer Company
3350 Scott Blvd., Bldg.15 Santa Clara,
CA 95054, USA