your future life

3WAN 1LAN 網路安全路由器

具負載平衡，頻寬管理，與網路安全功能

繁體中文使用手冊

產品功能說明手冊使用許可協定

《產品功能說明手冊（以下稱”手冊”）使用許可協定》（以下稱”協定”）是用戶與俠諾科技股份有限公司（以下稱”俠諾”）關於手冊許可使用及相關方面的權利義務、以及免除或者限制俠諾責任的免責條款。直接或間接取得本手冊檔案以及享有相關服務的用戶，都必須遵守此協定。

重要須知：俠諾在此提醒用戶在下載、閱讀手冊前閱讀本《協定》中各條款。請您審閱並選擇接受或不接受本《協定》。除非您接受本《協定》條款，否則請您退回本手冊及其相關服務。您的下載、閱讀等使用行為將視為對本《協定》的接受，並同意接受本《協定》各項條款的約束。

【1】知識產權聲明

手冊內任何文字表述及其組合、圖示、介面設計、印刷材料、或電子檔等均受我國著作權法和國際著作權條約以及其他知識產權法律法規的保護。當用戶複製"手冊"時，也必須複製並標示此知識產權聲明。否則，俠諾視其為侵權行為，將適時予以依法追究。

【2】"手冊"授權範圍：

用戶可以在配套使用的電腦上安裝、使用、顯示、閱讀本"手冊"。

【3】用戶使用須知

用戶在遵守法律及本協定的前提下可依本《協定》使用本"手冊"。用戶若是違反本《協定》，俠諾將中止其使用權力並立即銷毀此"手冊"的複本。本手冊"紙質或電子檔案"，僅限於為資訊和非商業或個人之目的使用，並且不得在任何網路電腦上複製或公佈，也不得在任何媒體上傳播;及不得對任何"檔案"作任何修改。為任何其他目的之使用,均被法律明確禁止,並可導致嚴重的民事及刑事處罰。違反者將在可能的最大程度上受到指控。

【4】法律責任與免責聲明

【4-1】俠諾將全力檢查文字及圖片中的錯誤，但對於可能出現的疏漏，用戶或相關人士因此而遭受的直接或間接的經濟損失、資料損毀或其他連帶的商業損失，俠諾及其經銷商與供應商不承擔任何責任。

【4-2】俠諾為了保障公司業務發展和調整的自主權，俠諾擁有隨時自行修改或中斷軟體 / 手冊授權而不需通知用戶的權利，產品升級或技術規格如有變化，恕不另行通知，如有必要，修改或中斷會以通告形式公佈於俠諾網站的相關區塊。

【4-3】所有設定參數均為範例，僅供參考，您也可以對本手冊提出意見或建議，我們會參考並在下一版本作出修正。

【4-4】本手冊為解說同系列產品所有的功能設定方式，產品功能會按實際機種型號不同而有部份差異，因此

部分功能可能不會出現在您所購買的產品上。

【4-5】俠諾保留此手冊檔案內容的修改權利，並且可能不會即時更新手冊內容，欲進一步瞭解產品相關更新訊息，請至俠諾官方網站流覽。

【4-6】俠諾（和/或）其各供應商特此聲明，對所有與該資訊有關的保證和條件不負任何責任，該保證和條件包括關於適銷性、符合特定用途、所有權和非侵權的所有默示保證和條件。所提到的真實公司和產品的名稱可能是其各自所有者的商標，俠諾（和/或）其各供應商不提供其他公司之產品或軟體等。在任何情況下,在由於使用或檔案上的資訊所引起的或與該使用或運行有關的訴訟中, 俠諾和/或其各供應商就因喪失使用、資料或利潤所導致的任何特別的、間接的或衍生性的損失或任何種類的損失，均不負任何責任，無論該訴訟是合同之訴、疏忽或其他侵權行為之訴。

【5】其他條款

【5-1】本協定高於任何其他口頭的說明或書面紀錄，所定的任何條款的部分或全部無效者，不影響其他條款的效力。

【5-2】本協定的解釋、效力及糾紛的解決，適用於臺灣法律。若用戶和俠諾之間發生任何糾紛或爭議，首先應友好協商解決。若協商未果，用戶在完全同意將糾紛或爭議提交俠諾所在地法院管轄。中國則以「中國國際經濟貿易仲裁委員會」為仲裁機構。

目 錄

1、簡介

3WAN 1LAN 網路安全路由器（以下稱路由器）是一台專為小型網咖，企業，社區，以及學校部門單位等級而設計，符合經濟實惠且高效能整合的全功能路由器。此路由器具備兩個廣域網埠，並具有高效能線路負載平衡模式的功能，達到對外連線的流量負載平衡。廣域網端的對外連線能力滿足絕大多數寬頻市場都適用的規格。區域網端 （LAN）內建 1 埠自動偵測 10/100Mbps 乙太網路交換機，可以連接額外的交換機以連接更多的上網設備。

內建防火牆系統，以滿足多數企業對防禦外部網路攻擊的市場需求。防火牆系統除了 NAT 之外，還具備有防止阻斷服務攻擊 （DoS，Denial of Service），以及封包主動偵測檢驗技術，可以預設自動偵測並阻擋外部網路攻擊。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的使用而遭受潛在的危機。

獨特的頻寬管理功能，功能強大但是設定簡單，可以讓管理者對有限的網路資源做合理而且有效的分配。對外不需要無限制的擴充頻寬而花費過多的金錢，也不會因為少數幾人的下載而搶佔所有的頻寬，造成內部其他上網用戶的抱怨。管理者可以選擇以流量控制或是優先權方式管理頻寬，設定規則，即可達成最有效率的運用。

網路位址轉換 NAT 除了可以做 Private 與 Public IP 轉換，讓您只需要一個 Public IP 就可以讓多人同時連上 Internet。區域網內的 IP 位址支援 Class C 等級，DHCP 自動分派 IP，以及簡單勾選的 IP 與 MAC 位址綁定讓網路環境架構具有彈性，易於規劃管理。

此外，路由器還包含虛擬伺服器，一對一 NAT 應用功能，可以滿足在區域網架設對外伺服器的需求，讓網路架設更簡單靈活。管理工具容易理解與設定，網路管理者可以 Web 流覽器輕易的做功能的設定與管理。同時，透過線上多樣化的系統日誌記錄，管理者可以清楚的知道網路活動，據此擬定訪問 Internet 存取資源管理的明確策略，並以此來調整設定，達到網路的使用更安全且更有效率。

此說明書主要是用來說明每一個功能的設定方法與細節，若是您對於路由器如何連上 Internet 的設定並不十分清楚，建議您先閱讀“快速安裝說明”，可以讓您快速的將路由器連上 Internet，並在必要時取得技術人員的遠端支持。

您可登錄 www.Qno.com.tw 進行線上查尋，也可參考附錄三：Qno 技術支援資訊，查詢相關資訊以及聯繫相關技術服務人員，以取得最新俠諾產品訊息及應用實例，更加善用您的俠諾產品。

2、硬體安裝

本章介紹產品的硬體介面以及實體安裝。

2.1 路由器 LED 顯示燈

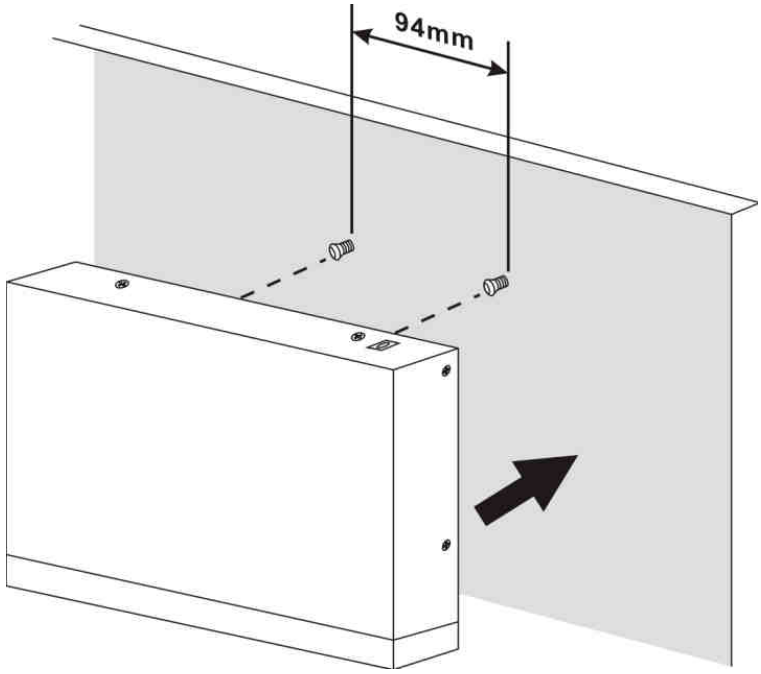
LED Status-面板燈號

LED 燈號	顏色	意義
Power-電源	綠燈	綠燈亮：電源開啟連接
DIAG-自我測試	橘燈	橘燈亮：系統尚未完成開機自我檢測功能。 橘燈熄滅：系統已經正常完成開機自我檢測功能。
Link/ACT-連線/動作	綠燈	綠燈亮：乙太網路連線正常 綠燈閃爍：乙太網路埠口正在傳送/接收封包資料傳輸
100Mbps / 10Mbps	橘燈	黃燈亮：乙太網路連線在 100Mbps 的速度 黃燈熄滅：乙太網路連線在 10Mbps 的速度
Connect-連接	綠燈	綠燈亮：當 WAN 端連線並取得 IP 位址。 綠燈熄滅：當 WAN 端連線並未取得 IP 位址

硬體恢復（Reset）按鍵

動作	描述
按下 Reset 按鈕 5 秒	熱開機，重新啟動路由器 DIAG 燈號：橘色燈號慢慢閃爍
按下 Reset 按鈕 10 秒以上	恢復原出廠預設值(Factory Default) DIAG 燈號：橘色燈號快閃

將路由器安裝在牆上

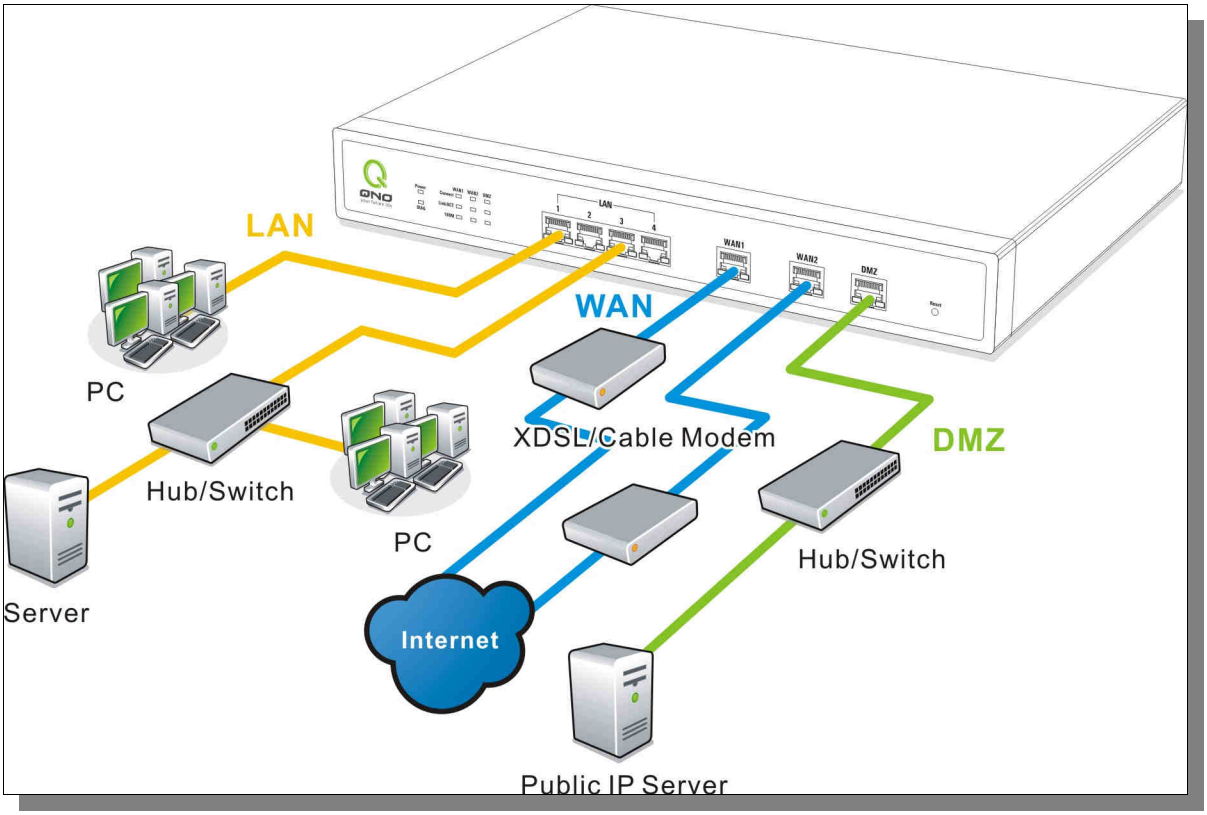


於路由器機器底部有二個十字孔位，壁掛孔圓心間距為 94mm，您可以使用一般螺絲先旋轉鎖進牆壁上，確認牢固後，再將路由器的底部二個十字孔位準確的掛在此二顆螺絲上即可完成安裝。

注意：螺絲釘高度請勿突出壁掛孔防靜電蓋，以避免發生產品損害。

2.2 連接路由器到您的網路上

路由器各網路埠口的使用拓墣範例如下圖：



廣域網路連線：連接 xDSL Modem 或光纖轉換器來連通網際網路。或是連接交換機或外部路由器來連通您現有的網路。

區域網路連線：連接交換機或電腦。

3、快速連網設定

本章介紹登錄軟體設定畫面，說明首頁的顯示訊息，以及基本連網設定。

3.1 登錄到軟體設定畫面

在連接到路由器 LAN 端的電腦上開啟網頁流覽器(如 IE)，在網址欄輸入 192.168.1.1 (路由器的預設閘道)，會出現以下的登錄畫面：

路由器路由器預設的使用戶名與密碼皆為 “admin”，您可以於稍後設定時更改此登錄密碼。

注意！

為了安全起見，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畫面，必須按下面板上的 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。

3.2 首頁顯示

首頁顯示路由器目前系統所有參數以及狀態顯示資訊。若您想進一部查詢該細部相關設定的話，可以按下各細部選項的超連結按鈕，即可快速立即進入該選項設定當中。

3.2.1 系統訊息

產品序號： 此為顯示路由器的產品序號

韌體版本： 此為顯示路由器目前使用的韌體版本

中央處理器： 此為顯示路由器使用的 CPU

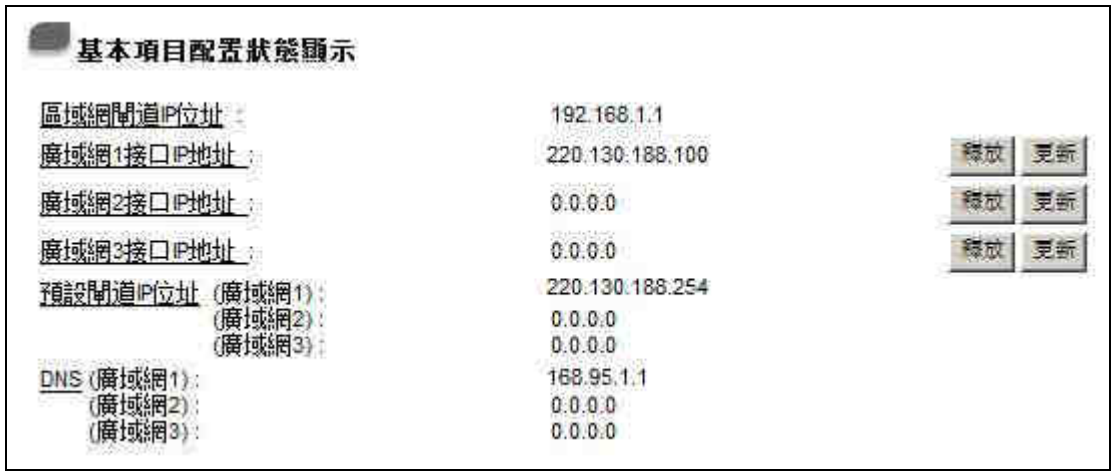
運作時間： 此為顯示路由器目前已經開機的時間

系統時間： 此為顯示路由器目前正確時間，但是必須注意，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

3.2.2 硬體埠口-狀態即時顯示

在此畫面會顯示系統各埠口目前即時狀態顯示（連線，啟用，關閉)。

3.2.3 一般設定狀態顯示



區域網介面 IP 位址(LAN IP)：此為顯示路由器路由器本身的 LAN 端目前 IP 位址，系統預設為 192.168.1.1，可以按下該超連結直接進入該設定項目中做修改。

廣域網 1/2/3 介面 IP 位址(WAN1 IP)：此為顯示路由器路由器的 WAN1 端目前的 IP 位址資訊，並且可以按下該超連結直接進入該設定項目中。當使用者選擇自動取得 IP 位址時，畫面上會顯示二個按鈕分別為釋放 Release 與更新 Renew。使用者可以按下 Release 按鈕去做釋放 ISP 端所核發的 IP 位址，以及按下 Renew 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，它會變為顯示 Connected 與 Disconnect。

預設閘道 IP 位址(Default Gateway)：此為顯示路 ISP 分配給路由器路由器 WAN1 及 WAN2 的閘道 IP 位址資訊，並且可以按下該超連結直接進入該設定項目中。

DNS：此為顯示路由器的 DNS(Domain Name Server)的 IP 位址資訊，並且可以按下該超連結直接進入該設定項目中。

3.2.4 進階設定狀態顯示

DMZ Host : 此為顯示路由器的 DMZ 功能選項是否啟動，並且可以按下該超連結直接進入該設定項目中。系統預設此功能為關閉。

路由器工作模式：此為顯示路由器的目前工作模式(可為 NAT Gateway 或是 Router 路由模式)，並且可以按下該超連結直接進入該設定項目中，系統預設此功能為 NAT Gateway 模式。

動態網域解析服務：此為顯示路由器的 DDNS 動態 DNS 功能選項是否啟動，並且可以按下該超連結直接進入該設定項目中。系統預設此功能為關閉。

3.2.5 防火牆設定狀態顯示

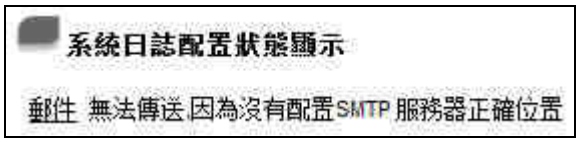
SPI 主動封包偵測過濾防火牆功能：此為顯示路由器的 SPI(Stateful Packet Inspection)主動封包偵測過濾防火牆功能選項是否開啟。可以按下該超連結直接進入該設定項目中。系統預設此功能為開啟。

DoS 防止 DoS 攻擊功能：此為顯示路由器的阻斷來自 Internet 上的 DoS 攻擊功能選項是否開啟。可以按下該超連結直接進入該設定項目中。系統預設此功能為開啟。

關閉廣域網回應功能：此為顯示路由器的阻斷來自 Internet 上的 ICMP-Ping 的回應功能選項是否開啟。可以按下該超連結直接進入該設定項目中。系統預設此功能為開啟。

遠端管理功能：此為顯示路由器的遠端管理功能選項是否啟動。可以按下該超連結直接進入該設定項目中。系統預設此功能為關閉。

3.2.6 日誌記錄配置狀態顯示



顯示電子郵件告警功能是否設置。

E-Mail 的超鏈結將會連到系統日誌設定畫面中：

1.若您無設定電子郵件伺服器於系統日誌設定中，將顯示您無設定電子郵件伺服器所以無法傳送系

統日誌電子郵件-「郵件無法傳輸，因為没有配置 SMTP 伺服器正確位置」。

2.若您已經設定電子郵件伺服器於系統日誌設定中，但是日誌尚未達到設定傳輸的條件時，它將顯示電子郵件伺服器已經設定-「郵件設定已經配置」。

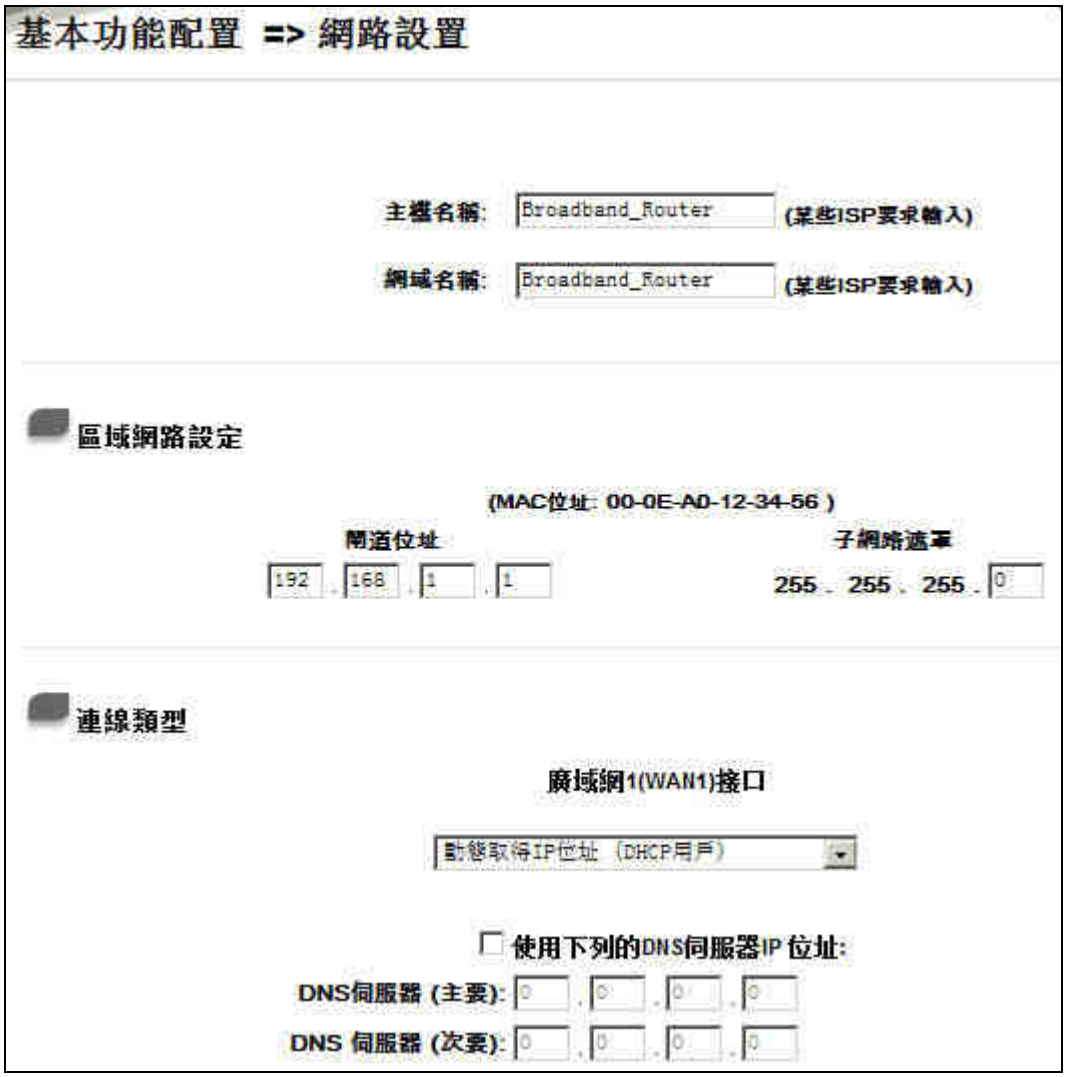
3.若您已經設定電子郵件伺服器於系統日誌設定中，日誌也已經傳輸出去時，它將顯示電子郵件伺服器已經設定，並且已經傳送-「郵件設定已經配置並且已經傳送」。

4.若您已經設定電子郵件伺服器於系統日誌設定中，但是日誌無法正確傳輸出去時，它將顯示電子郵件伺服器已經設定，但是無法傳輸出去，可能是設定有問題-「郵件無法傳送已經設定好郵件可能使用不正確的設定」。

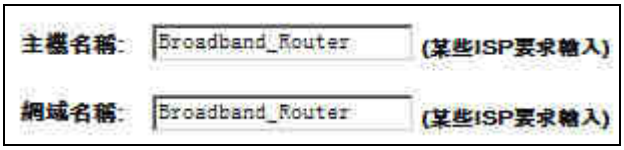
3.3 基本連線設定

基本連線設定提供路由器路由器基本的網路連接設定內容，對大多數的用戶來說，完成基本的設定已經足夠連接 Internet 而不需做任何變更。Internet 的連接需要一些 ISP 所提供的進一步詳細資訊，其詳細細部設定，請參考以下各節說明：

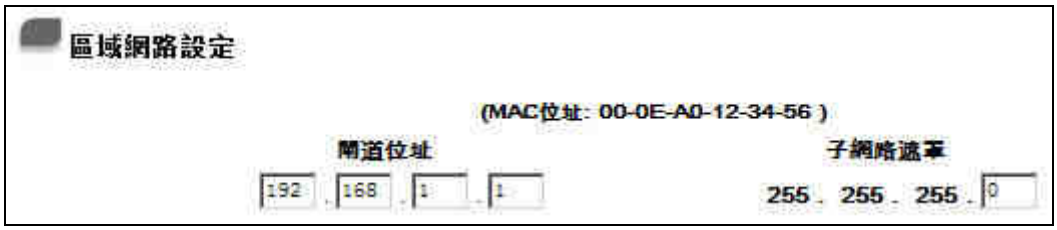
3.3.1 基本功能配置



主機名稱及網域名稱：可輸入路由器的名稱以及網域名稱，於大多數的環境中不需做任何設定即可使用，除非特殊 ISP 需求！



區域網 LAN 設定：此為設定路由器的 LAN 端內部網路的 IP 位址，系統預設為 192.168.1.1，子網路遮罩為 255.255.255.0，路由器區域網 IP 位址可支援 Class C 等級，您可以依照實際網路架構做改動！



廣域網路 Internet 連線形態設定：

動態取得 IP 位址：

此為路由器系統預設的連線方式，此連線方式為 DHCP Client 自動取得 IP 模式，多為應用於如 Cable Modem 或是 DHCP Client 連線形態等連接，若您的連線為其他不同的方式，請選取相關的設定並依照以下的介紹做設定.

在自動取得 IP 模式，您可以使用自訂 DNS 的 IP 位址，於此選項勾選並填入您要使用的 DNS IP 位址。

使用下列的 DNS 伺服器 IP 位址： 選擇使用自訂的 DNS 伺服器 IP 位址。

DNS 伺服器： 輸入您的 ISP 所提供的 DNS 伺服器 IP 位址，最少填入一組，最多可填二組。

設定完成請按下確認按鈕儲存網路設定變更。若是不想進行變更，請在按下確認儲存動作之前按下取消按鈕，將不做任何設定變更。

Static IP 固定 IP 位址連線：

若您的 ISP 有核發固定的 IP 位址給您(如 1 個 IP 或是 8 個 IP 等)，請您選擇此種方式連線，將 ISP 所核發的 IP 資訊分別依照以下介紹填入相關設定參數中。

IP 位址： 輸入您的 ISP 所核發的可使用固定 IP 位址的其中一個。

子網路遮罩： 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 位址：255.255.255.248
發放 16 個固定 IP 位址：255.255.255.240

預設閘道： 輸入您的 ISP 所核發的可使用固定 IP 位址的預設通訊閘，若您是使用 ADSL 的話，一般說來都是 ATU-R 的 IP 位址。

DNS 伺服器： 輸入您的 ISP 所規定的名稱解析伺服器 IP 位址，最少請填入一組，最多可填二組。

設定完成請按下確認按鈕儲存網路設定變更。若是不想進行變更，請在按下確認儲存動作之前按下取消按鈕，將不做任何設定變更。

PPPoE 撥號連線：

此項為 ADSL 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 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。

使用者名稱： 輸入您的 ISP 所核發的使用者名稱。

密碼： 輸入您的 ISP 所核發的使用密碼。

閒置____分鐘自動斷線： 此功能能夠讓您的 PPPoE 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。

保持連線：自動重撥於斷線後____秒： 此功能能夠讓您的 PPPoE 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。

設定完成請按下確認按鈕儲存網路設定變更。若是不想進行變更，請在按下確認儲存動作之前按下取消按鈕，將不做任何設定變更。

3.3.2 多 WAN 設定

當用戶的連線是採用多 WAN 的線路設計，管理人員可以進入基本功能設定的負載平衡設定與協議綁定，對路由器的負載平衡模式等進行設定，使路由器達到最優資料轉發是網路頻寬效能達到最高。

智能型負載平衡模式：

當您選用智能型負載平衡模式，路由器將以連線數或是 IP 位址連線數為基礎，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平衡。線路的頻寬是依據您所填入的頻寬設定，例如當兩條廣域網都為上傳 512Kbit/sec 時，其自動負載比例為 1：1，當一條線路的上傳頻寬為 1024kbit/sec 另一條為 512kbit/sec 時，則此自動負載比例為 2：1，所以為了確保您的路由器達到實際線路負載能夠平衡，請填入實際上傳下載頻寬。

依連線數平衡：當您選用連線數平衡模式，路由器將以連線數為基礎，並依據您廣域網線路的頻寬來自動分配連線，達到連線的負載平衡。

依 IP 位址平衡：當您選用 IP 負載平衡模式，路由器將以連線的 IP 數為基礎，並依據您廣域網線路的頻寬來自動分配連線，達到連線的負載平衡。

提示！

不論是連線數平衡或是 IP 負載平衡方式，搭配“通訊協議綁定”可以有更彈性運用您的頻寬，您可將特定的內網 IP，使用特定應用通訊埠作訪問，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 192.168.1.100 訪問外網的時候走廣域網 1，或內網所有 IP 去訪問通訊埠 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“通訊協議綁定”功能來達到您的需求。請注意，當使智能型負載平衡模式搭配“通訊協議綁定”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 或通訊埠的訪問還是按照 VPN 防火牆的機制做智能負載平衡。

Network Service Detection 線路偵測機制

啟用線路偵測機制：　網路對外線路偵測機制。若勾選此項設定，則會出現 Retry Count、Retry Timeout 等以下的訊息。當使用兩條廣域網做對外連接線路時

	一定將此 NSD 啟用，以避免因為廣域埠流量過大時造成路由器的誤判將此線路判斷為斷線。
重新嘗試連線次數：	對外連線偵測重試次數，預設值為五次。若是於此設定次數當中，Internet 沒有回應的話，就判斷為對外線路中斷！
延遲時間：	對外連線偵測逾時時間(秒)，預設值為 30.秒。於此設定秒數之後重新測試對外連線。
當重新連線失敗時：	(1) Generate the Error Condition in the System Log 在系統日誌中會產生錯誤訊息的資訊：當偵測到與 ISP 連接失敗時，系統就會在系統日誌中將這項錯誤訊息記錄下來，但依舊保持此線路不會移除，所以會有些原來使用此條線路上的 User 無法正常使用。 (2) Remove the Connection 移除有問題線路：當偵測到與 ISP 連接失敗時，系統不會在系統日誌中將這項錯誤訊息記錄下來，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接，則封包傳遞會自動轉換回來。
偵測以下可回應的伺服器：	
預設閘道：	近端的預設通訊閘道位置，如 ADSL 路由器的 IP 位址，此為路由器自動填入，所以只需打勾選擇是否啟用。
ISP 伺服器：	ISP 端的偵測位置，如 ISP 的 DNS 伺服器 IP 位址等。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)。
遠端伺服器：	遠端的網路節點偵測位置,此遠端伺服器 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)。
DNS 伺服器做名稱解析：	網域名稱 DNS 的偵測位置(此欄位只許填入網址如 www.hinet.net，請勿填 IP 位址)。另外，兩條 WAN 的此欄位不可以填入相同的網址。

設定完成請按下確認按鈕儲存網路設定變更。若是不想進行變更，請在按下確認儲存動作之前按下取消按鈕，將不做任何設定變更。

Bandwidth 頻寬設定

路由器路由器會依照您實際輸入的上傳頻寬資料做為兩條廣域埠自動負載平衡的比例依據。例如當兩條廣域網都為上傳 512Kbit/sec 時，其自動負載比例為 1:1。當一條線路的上傳頻寬為 1024kbit/sec 另一條為 512kbit/sec 時，則此自動負載比例為 2:1。所以為了確保您的路由器達到實際線路負載能夠均衡，請填入實際上下載頻寬。另外，此欄位也關係到 QoS 的設定，請參考 QoS 設定章節說明。

3.3.3 通訊協定埠綁定

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

通訊埠： 在此選擇欲開啟的綁定服務埠(Service Port)，從下拉式選單中可以選擇預設列表(如 All -TCP&UDP 0~65535， WWW 為 80~80， FTP 為 21~21 等等)，預設的 Service 為 All 0~65535。

Service Management：按下此按鈕可以進入服務埠設定畫面，進行新增或刪除選單中預設的服務埠。

來源 IP 位址： 使用者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 192.168.1.100~150. 則 IP 位址 100~150 為綁定範圍。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。

目的 IP 位址： 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，則填入方式可以為 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。

接口位置： 選擇您所要綁定此條規則在哪一個 WAN 埠。

啟用： 啟用此規則。

加入到對應列表： 增加此條規則到列表。

刪除點選的項目： 刪除在服務列表裏所選擇的規則。

設定完成請按下確認按鈕儲存網路設定變更。若是不想進行變更，請在按下確認儲存動作之前按下取消按鈕，將不做任何設定變更。

通訊埠設定

若您欲開啟的服務埠項目沒有在表列中，您可以按下通訊埠設定，新增或刪除管理服務埠號列表功能達到，如以下所述：

服務名稱： 在此自訂欲開啟的服務名稱加入列表中，如 BT 等。

通訊協議： 在此選擇欲開啟的服務的封包格式為 TCP 或 UDP。

通訊埠範圍： 將您所需新增加的服務埠範圍填入。

加入到對應列表： 增加到開啟服務項目內容列表，最多可新增 100 組。

刪除點選的項目： 刪除所選擇的開啟服務項目之一筆內容。

確定： 按下此按鈕"確定"即會儲存剛才所變動的修改設定內容參數。

取消： 按下此按鈕"取消"即會清除剛才所變動的修改設定內容參數，但是必須於確定儲存動作之前才會有效。

離開： 離開此功能設定畫面。

3.3.4 頻寬管理(QoS)

頻寬管理 QoS 為 Quality of Service 縮寫，其功能主要為限制某些服務及 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公司、社區、或是網咖的實際需求，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。

ISP 實際可用頻寬：請填入 ISP 線路實際可供使用頻寬

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為計算依據。例如說每個 IP 及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為 512Kbit/Sec，那實際上傳頻寬就為 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/上傳速度單位為 KB，兩個數值之間的換算方式為 1KB=8kbit。

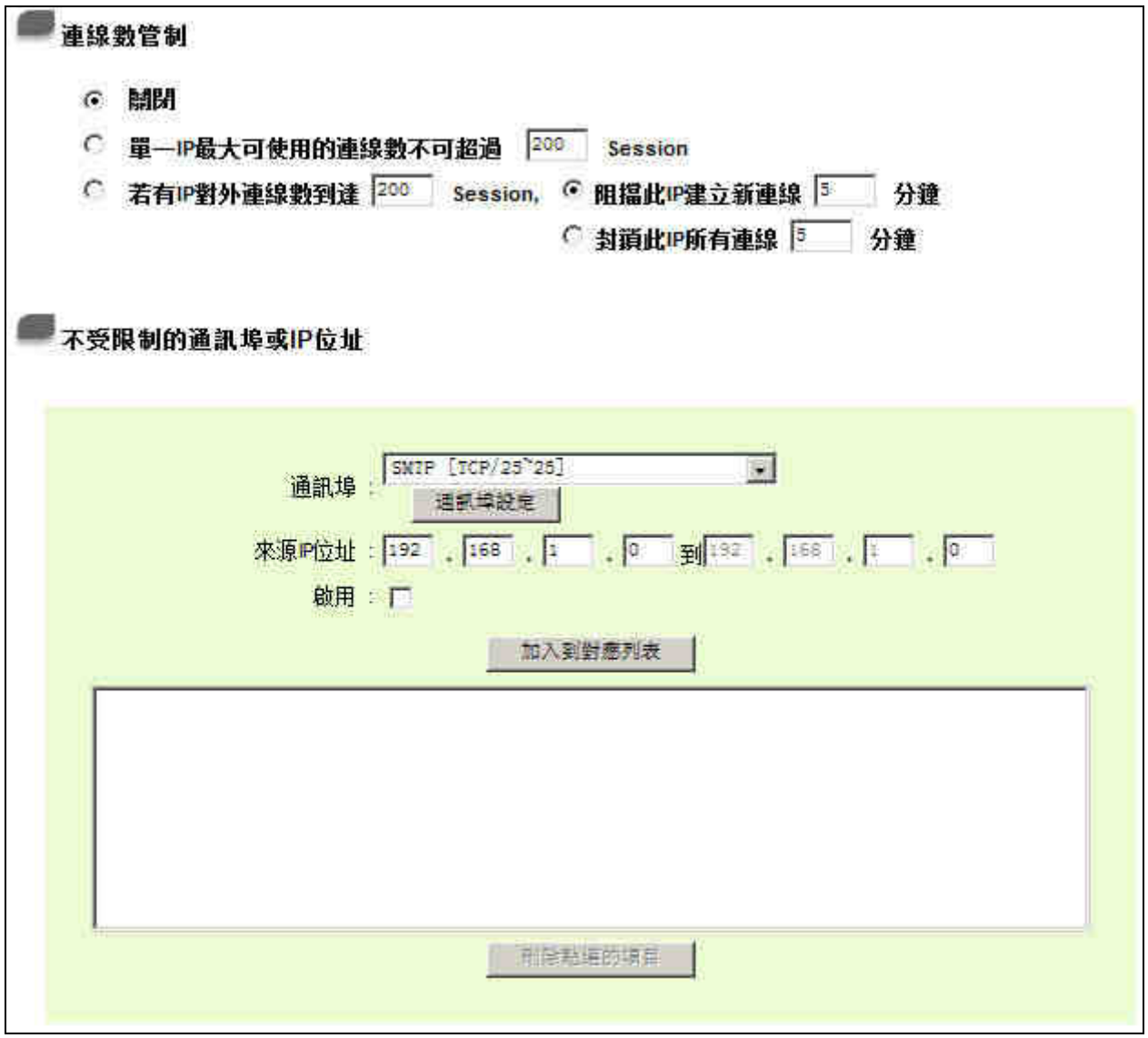
注意！

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

Session Limit 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 session 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。

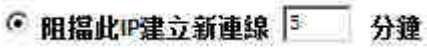
另外，若內網有電腦中了類似衝擊波的病毒而產生大量對外發連線請求時，也可以達到抑制作用。



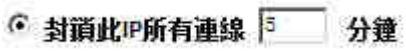
關閉： 不使用此連線數管控功能。

單一IP最大可使用的連線數不可超過： 此選項為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。

若有 IP 對外連線數到達__Session：



此選項為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。



此選項為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。

不受限制的通訊埠或 IP 位址： 可以將公司，企業等重要服務或者用戶 IP 位址加入不受連線數限制

通訊埠設定： 選擇不受連線限制的服務埠

來源 IP 位址： 添加內不受限制的 IP 位址或範圍

啟用： 勾選啟動加入的規則

加入到對應列表： 將添加的規則增加到列表中

刪除點選的項目： 刪除所選擇的項目之一筆內容。

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

QoS 設定

QoS 可以選擇兩種方式並且同時使用，一為流量控制(Rate Control)，另一個為優先權控制(Priority Control)，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-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 或一段 IP 做使用量限制或保障頻寬。另外也可以針對服務埠(Service Port)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。

接口位置： 勾選此條 QoS 設定要控制在哪條 WAN 執行，可單獨或全部勾選。

通訊埠設定： 選擇此條 QoS 所要設定的頻寬控制為何，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 位址： 此為選擇您所要限制的使用者為何?若您只限制單一 IP，則直接將此 IP 填入，如：192.168.1.100~100，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 192.168.1.100~150，這樣此規則就是針對 192.168.1.100~150 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 192.168.1.0~0，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。

目的：	**上傳：**指對內網 IP 的上傳頻寬 **下載：**指對內網 IP 的下載頻寬 **虛擬伺服器上傳：**若您有架設對外的伺服器網站在路由器內部，則此選項為控制外部用戶下載訪問伺服器的頻寬控制。 **虛擬伺服器下載：**若您有架設網站在路由器內網，則此選項為控制外部用戶對此伺服器上傳資料時的頻寬控制，例如網咖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更新時，可以用此控制做頻寬管理，才不會影響內部使用者上網玩遊戲。
保證頻寬與最大可用頻寬： (Kbit/Sec)	保證頻寬：此為限制或保證此條規則的最小可使用頻寬 最大可用頻寬：此為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
頻寬分配方式：	**此範圍所有 IP 位址共享此設定頻寬：**若選擇此規則的話，其表示所有 IP 或此 Service Port 共用這段頻寬範圍。 **此範圍每一 IP 位址獨享此設定頻寬：**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。
啟用：	啟用此規則。
加入到對應列表：	增加此條規則到列表。
上移 / 下移：	由於 QoS 的每條規則執行的優先順序為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。
刪除點選的項目：	刪除在服務列表裏所選擇的項目內容。
顯示列表：	可以顯示出您所有在頻寬控制設定的規則，並可直接按下 Edit 編輯做修改。

設定完成請按下確認按鈕儲存網路設定變更。若是不想進行變更，請在按下確認儲存動作之前按下取消按鈕，將不做任何設定變更。

Priority 優先權-依優先順序做管理：

優先順序顧名思義就是可以將您選定想要的服務做先後順序的調配，也就是可以直接選擇服務埠將其優先順序做一分配。

路由器會將頻寬做 60%(High-最高)，10%(Low-最低) 的頻寬分配，也就是若您將 Port 80 選擇為 High，那麼路由器只要遇到 Port 80 的封包就會給予 60%的頻寬出去，若您將 FTP Port 21 設定為 Low，那當有人使用 Port 21 時，路由器只會給它 10%的頻寬使用，其餘未做分配的 Service 就使用 30%頻寬。

接口位置： 勾選此條優先權的設定要控制在哪條 WAN 執行。

通訊埠： 在此選擇此條優先權所要設定的服務埠為何，要針對譬如 FTP 上傳或下載，則選擇 FTP Port21~21，可參考服務號碼預設列表。

目的： 上傳：指標對此服務埠的上傳做優先權控制。

下載：指標對此服務埠的下載做優先權控制。

優先權： 高級：此為保證 60%的頻寬給此服務埠使用。

低級：此為只給 10%的頻寬給此服務埠使用。

啟用： 啟用此規則。

加入到對應列表： 增加此條規則到列表。

刪除點選的項目： 刪除所選擇在服務列表裏的項目內容。

顯示列表： 可以顯示出您所有在優先權設定的規則，並可直接按下 Edit 編輯做修改。

設定完成請按下確認按鈕儲存網路設定變更。若是不想進行變更，請在按下確認儲存動作之前按下取消按鈕，將不做任何設定變更。

3.3.5 Password 密碼設定

當您每次登錄至路由器的設定畫面時，必須輸入密碼。路由器的密碼出廠值為"admin"。為了安全起見，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，將無法再登錄至路由器的設定畫面，必須恢復到出廠值。

使用者名稱： 預設為 admin 。

密碼： 填寫原本舊密碼。

輸入新密碼： 填寫所更改密碼。

再次輸入新密碼： 再填寫確認一次更改密碼。

設定完成請按下確認按鈕儲存網路設定變更。若是不想進行變更，請在按下確認儲存動作之前按下取消按鈕，將不做任何設定變更。

3.3.6 Time 系統時間設定

路由器可以設定時間，讓您在看路由器的系統記錄或是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，以及作為關閉存取或是開放存取 Internet 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取得時間同步，或是自己設定正確時間參數。

Set the local time using Network Time Protovol (NTP) automatically 設定自動與網路上的 NTP 伺服器同步時間：路由器有內建的網路時間伺服器，會自動同步時間。

Set the local time Manually 設手動輸入日期時間參數：與此輸入正確的時間。

設定完成請按下確認按鈕儲存網路設定變更。若是不想進行變更，請在按下確認儲存動作之前按下取消按鈕，將不做任何設定變更。

4、Advanced Setting 進階功能設定

本章介紹路由器進階功能的設定，包括開啟虛擬伺服器的連接，路由設定，實體 IP 與虛擬 IP 對應，以及設置動態網域名稱解析服務等功能。

4.1 DMZ 伺服器位址配置

當您將路由器內部的某台 PC 的虛擬 IP 填入到此 DMZ 選項時，路由器 WAN1 及 WAN2 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。

於使用 "DMZ Host" 功能後，若您要取消此功能必須於在設定虛擬 IP 位址地方填入"0" 的參數，才會停止此功能使用。

設定完成請按下確認按鈕儲存網路設定變更。若是不想進行變更，請在按下確認儲存動作之前按下取消按鈕，將不做任何設定變更。

4.2 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為－虛擬的位置，利用路由器的外部合法 IP 位址，經過服務埠的轉換，（如 WWW 為 Port 80），直接存取到內部虛擬 IP 的伺服器的服務。例如在設定畫面中，選項填入伺服器位置，如 192.168.1.2 且埠是 80 的話，當 Internet 外部要進來存取這個網頁時只要鍵入：

如：http://220.130.188.45 (假設此為路由器外部合法 IP 位址)

此時，就會透過路由器的公網 IP 位址去轉換到 192.168.1.2 的虛擬主機上的 Port 80 讀取網頁了。

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

通訊埠： 在此選擇欲開啟的虛擬伺服器的服務埠號。碼預設列表，如 WWW 為 80(80~80)， FTP 為 21~21，可參考服務號碼預設列表！

IP 位址： 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。

啟用： 開啟此服務功能。

通訊埠設定： 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端號列表。

加入到對應列表： 增加到開啟服務項目內容。

設定完成請按下確認按鈕儲存網路設定變更。若是不想進行變更，請在按下確認儲存動作之前按下取消按鈕，將不做任何設定變更。

特殊應用軟體配置 (Port Triggering)：

有一些特殊應用軟體其進出 Internet 的服務埠號為非對稱的，此時您必須使用此功能選項將一些特殊應用程式使用的服務埠號填入相關設定中，如以下畫面所示：

特殊應用程式名稱： 您可以自訂此特殊應用軟體名稱，方便管理使用！

實際對外的通訊埠範圍： 輸入由路由器出 Internet 的使用埠編號(如 9000~10000)

內部映射的通訊埠範圍： 輸入由 Internet 進入的使用埠編號. (如 2004~2005)

加入到對應列表： 增加到開啟服務項目內容列表

刪除點選的項目： 刪除所選擇的開啟服務項目之一筆內容

顯示列表： 按下此按鈕即會顯示 Table 上的所有設定項目內容參數

設定完成請按下確認按鈕儲存網路設定變更。若是不想進行變更，請在按下確認儲存動作之前按下取消按鈕，將不做任何設定變更。

4.3 UPnP 通訊協議

UPnP (Universal Plug and Play) 是微軟 Microsoft 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 WindowsXP) 而且您的電腦 UPnP 功能有開啟，您可以將路由器路由器的 UPnP 功能啟動。

UPnP 功能包含有 UPnP Forwarding 的功能，如您要在內網設置虛擬伺服器，您可以在前章節介

紹的 Forwarding 功能設置，或是在此 UPnP Forwarding 中設置。不過請不要重複輸入造成衝突。

通訊埠： 在此選擇欲開啟的 UPnP 的服務號碼預設列表，如 WWW 為 80(80~80)， FTP 為 21~21，可參考服務號碼預設列表

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

啟用： 開啟此服務功能

通訊埠設定： 新增或刪除管理服務端口號列表

加入到對應列表： 增加到開啟服務項目內容

刪除點選的項目： 刪除所選擇的開啟服務項目之一筆內容

顯示列表： 顯示目前所開啟設定的 UpnP 服務列表

設定完成請按下確認按鈕儲存網路設定變更。若是不想進行變更，請在按下確認儲存動作之前按下取消按鈕，將不做任何設定變更。

4.4 Routing 路由通訊協定

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為兩種方式，一是在內網中連接不同網段或路由器，一是在廣域網的環境中讓路由器知道去那個目地位址時就要走那條廣域網。例如常常會遇到路由器不同的廣域網申請不同家的 ISP 的線路，為了避免有些伺服器，如：Mail 伺服器或遊戲伺服器是架設在不同一的 ISP 環境而且 ISP 之間無法彼此互通，此時去 Mail 伺服器或是去遊戲伺服器就應該走不同的廣域網，而避免繞遠路。這個用意跟協議綁定是有相似的做用。

目的地 IP 位址與子網路遮罩： 填入目的地的遠端網路 IP 節點與子網路節點位址。

預設閘道：	從此網路節點到目的遠端網路路由的預設閘道位址。
中繼路由節點：	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，此應填為 2，預設為 1.（最大為 15）。
接口位置：	此網路節點的連接位置，位於 WAN 端亦或是 LAN 端。
加入到對應列表：	增加此路徑規則到列表中。
刪除點選的項目：	刪除在表中所選擇的路徑表。
顯示列表：	顯示目前最新的路徑表。
確認：	按下此按鈕"確認"即會儲存剛才所變動的修改設定內容參數。
取消：	按下此按鈕"取消"即會清除剛才所變動的修改設定內容參數，但是必須於確認儲存動作之前才會有效。

4.5 一對一 NAT 對應

當您的 ISP 線路為固定制時，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廣域網埠以及光纖轉換器或 ATU-R(Gateway) 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為虛擬 IP，但當做了 One to One 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伺服器 IP 位址使用！

範例：如您有 5 個合法 IP 位址，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 位址不能被涵蓋在 One to One NAT 的 IP 範圍設定中。

一對一 NAT 對應設定: 選擇是否開啟此一對一 NAT 功能開啟 /關閉

內部起使 IP 位址: 虛擬 IP 位址起始 IP 位址

外部起使 IP 位址: 外部合法 IP 位址起始 IP

對應範圍 IP 數量: 填入您同時要有多少個外部合法 IP 位址需要對應

加入到對應列表: 加入此設定到一對一 NAT 列表中

刪除點選的項目: 刪除所選擇的一對一 NAT 規則

設定完成請按下確認按鈕儲存網路設定變更。若是不想進行變更，請在按下確認儲存動作之前按下取消按鈕，將不做任何設定變更。

注意！

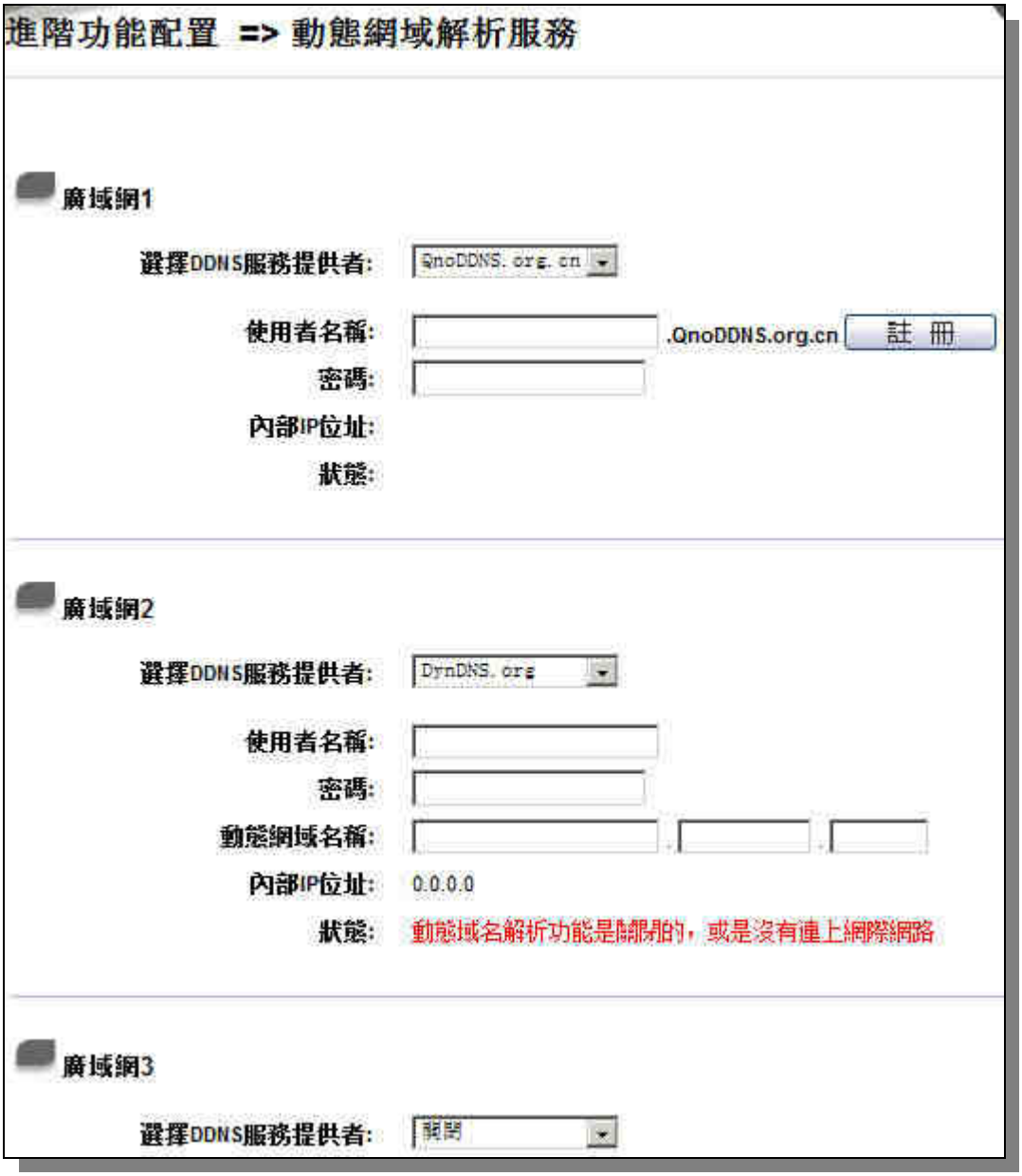
一對一的 NAT 模式將會改變防火牆運作的方式，您若設定了此功能，區域網端所對應 Public IP 的伺服器或電腦將會曝露到 Internet 上。若要阻絕 Internet 的使用者主動連線到

一對一 NAT 的伺服器或電腦，請到防火牆的”存取規則設定”中設定適當的拒絕存取規則條件。

4.6 DDNS-動態網域名稱解析

DDNS 功能可以支援 Dyndns.org、3322.org 與 Qno DDNS 的動態網域名稱解析功能，其目的是為了讓使用動態 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 Router 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.3322.org”，將其設定在 DDNS 設定中，則在遠程只要去 Ping abc.3322.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，Internet 使用者只要在網址打上 abc.3322.org 就可以直接進入到您內部架設的 WEB。在設定此功能之前，請向 www.dyndns.org 或是 www.3322.org 提出申請，是完全免費的！

另外，為了解決 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 DDNS 服務做動態 IP 更新。



選擇 DDNS 服務提供者： 可以選擇 Dyndns.org、3322.org 與 Qno DDNS (可同時使用)

使用者名稱： 向 DDNS 所設定的名稱

●QnoDDNS 使用者名稱要填入完整的網址，如：abc.qnoddns.org.cn

密碼： 向 DDNS 服務提供者所申請的密碼

動態網域名稱： 動態網址名稱： 向 DDNS 所註冊的網址，如：abc.dyndns.org 或

xyz.3322.org

內部 IP 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

狀態： 顯示目前路由器對 DDNS 的更新狀態

設定完成請按下確認按鈕儲存網路設定變更。若是不想進行變更，請在按下確認儲存動作之前按下取消按鈕，將不做任何設定變更。

4.7 MAC Clone 廣域網介面 MAC 位址設定

有些 ISP 會要求提供一固定 MAC 位址(網卡位址)做為 ISP 端分配 IP 給您的認證使用，此大多使用於 Cable Mode 的用戶。若有此需求的話，可使用此功能將提供給 ISP 的網卡位址(MAC Address：00-xx-xx-xx-xx-xx) 填入此項目中，路由器就會以此 MAC Address 做為跟 ISP 請求 IP 時的認證！請注意：路由器只有 WAN1 才能進行此功能的設定。

使用者自訂廣域網介面 MAC 位址設定： 使用者可以自行輸入提供給 ISP 的網卡位址，目前設備出廠預設的 MAC 位置為 WAN 端的 MAC 位址。

設定與此 PC 的 MAC 地址相同： 目前這台 PC 的 MAC 位址。

設定完成請按下確認按鈕儲存網路設定變更。若是不想進行變更，請在按下確認儲存動作之前按下取消按鈕，將不做任何設定變更。

4.8 DHCP 發放 IP 伺服器

路由器有一組 Class C 的 DHCP 伺服器，預設值是啟動，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，就可從路由器自動取得 IP 位址，管理方便。

4.8.1 DHCP Setup

租約到期時間： 此設定為發給 PC 端 IP 位址的租約時間，預設為 1440 分鐘(代表時間為一天)，當租約時間到後，PC 端會重新跟 Router 再申請一次。您可以依照實際需求來設定。

起使 IP 位址： 系統預設為從 192.168.1.100 的 IP 位址開始發放。您可以依照實際需求來設定。

結束 IP 位址： 系統預設為 192.168.1.149 IP 位址為最後發放 IP，也就是說出廠設定值可供 50 台電腦自動取得 IP 位址。您可以依照實際需求來設定。

設定完成請按下確認按鈕儲存網路設定變更。若是不想進行變更，請在按下確認儲存動作之前按下取消按鈕，將不做任何設定變更。

4.8.2 IP & MAC Binding

在許多的企業及社區網路中，網管人員可以設定路由器所提供的 IP & MAC 綁定功能，達到 User 不

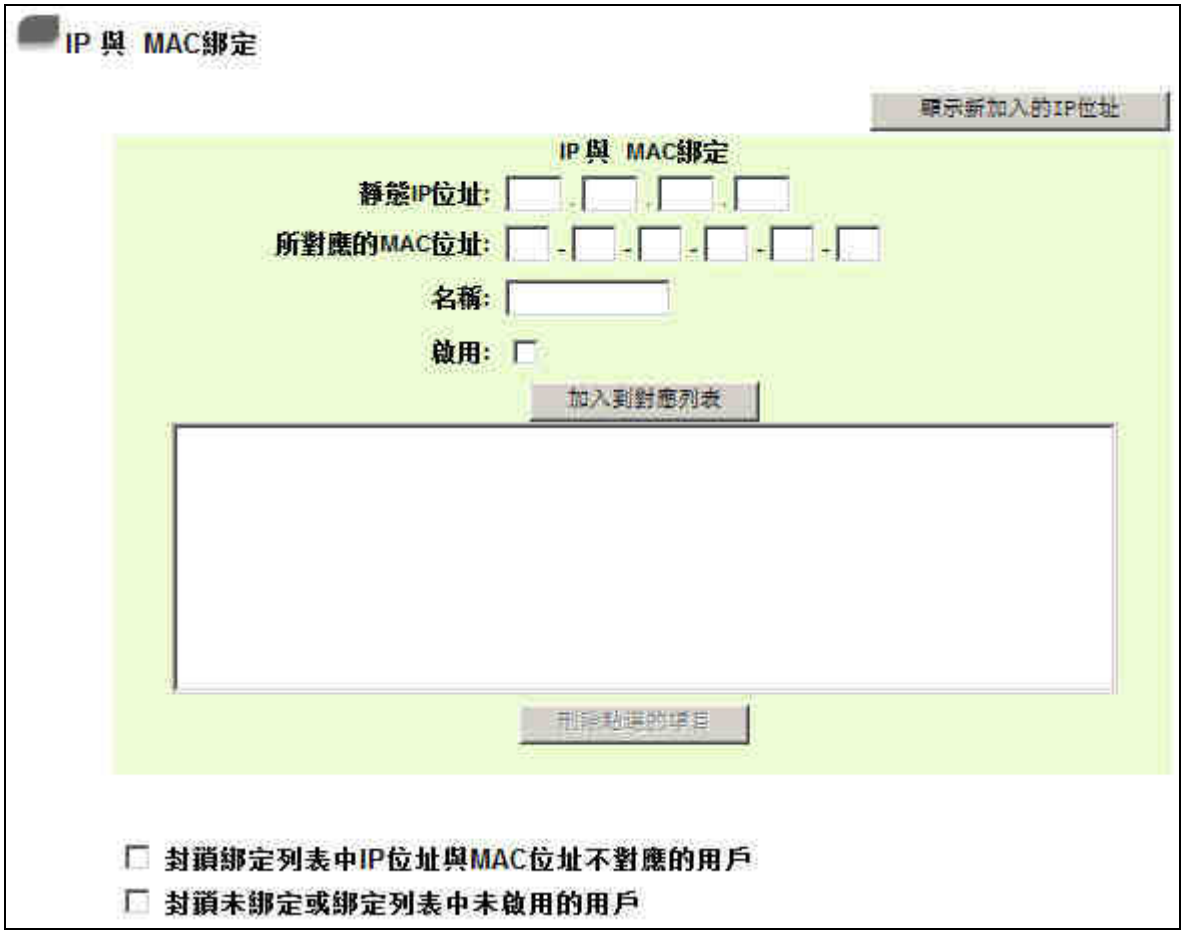
能自行添加電腦來使用對外網路或是私自擅改 IP 上網影響他人。另外透過此功能也可以將每台電腦或伺服器的 MAC 位址綁定，達到電腦或伺服器每次開機或重新要 IP 時，都分配給它相同的一組 IP 位址。

您可以以下兩種方式來設定這個功能：

Block MAC address not on the list 限定可以使用網路的 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 分派的 IP 位址上網，未在此列表的電腦都無法取得 IP 上網。

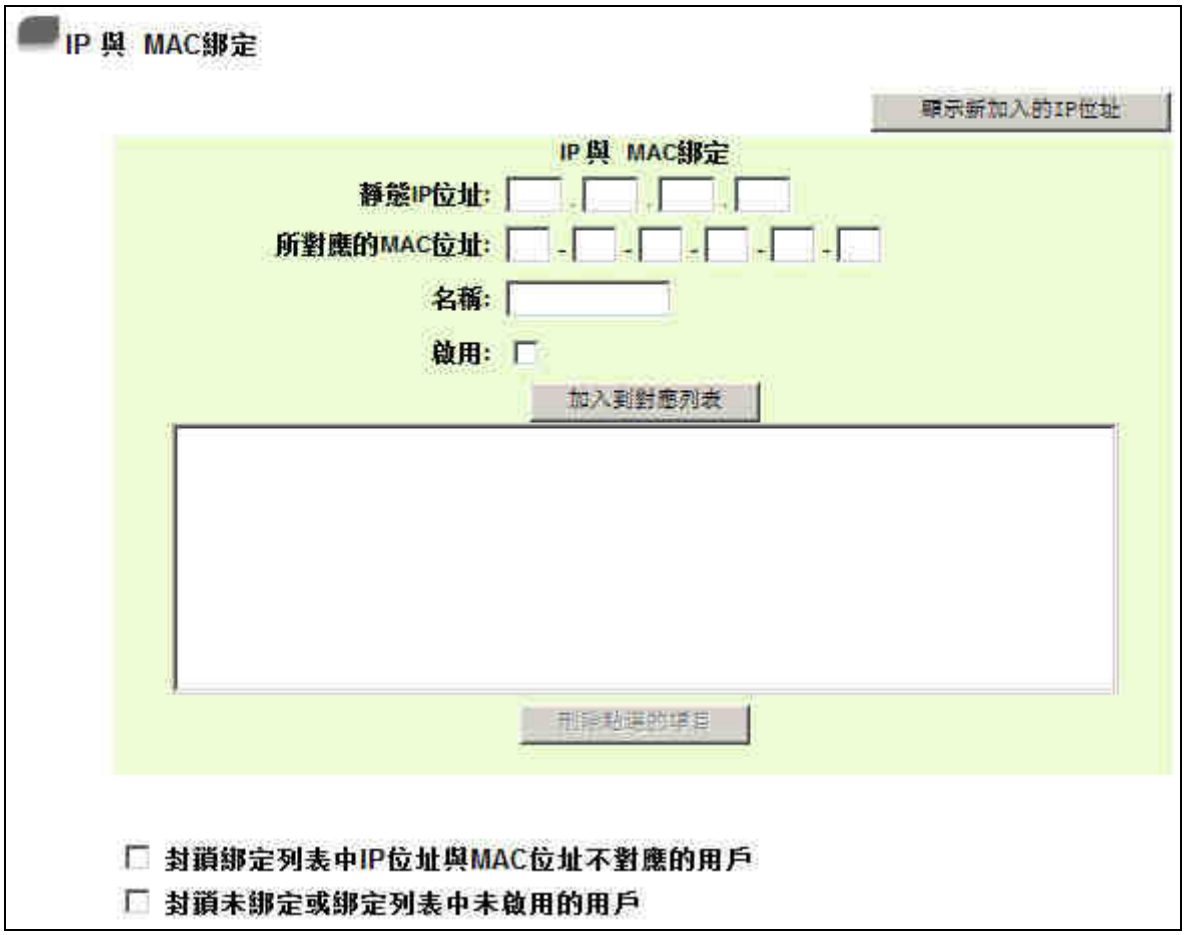
當使用此功能時，切記要將固定 IP 位址填 0.0.0.0 不可以空白，另外將 Block MAC address not on the list 選項打勾才可以執行。如下圖中範例所示：



IP 及 MAC 位址綁定

此功能主要目的是讓指定的 MAC 位址電腦在每次開機都會要到同一個指定 IP。此外，若將 Block

MAC address on the list with wrong IP address (封鎖在對應列表中 IP 位址錯誤的 MAC 位址) 功能啟用，則設定為固定 IP 或以此功能發給特定 IP 的電腦擅自更改 IP 為非指定的 IP 位址時，會無法上網。



靜態 IP 位址：

此欄位有兩種填入方式：

1. 若您只要限制 MAC Address 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，不可為空白。

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 端每次重啟都會要到固定的同一個虛擬 IP。

所對應的 MAC 位址:

輸入要綁定的伺服器或 PC 端固定實體 MAC(網路卡上的位址)。

名稱:

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。

啟用: 啟用此組設定。

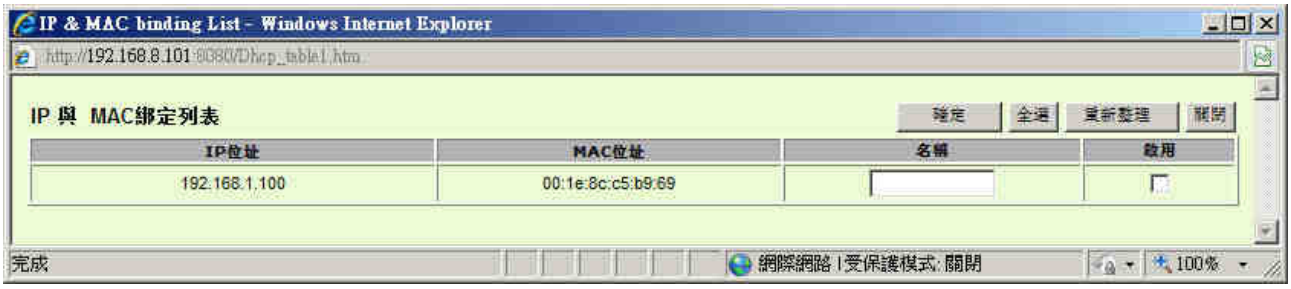
封鎖綁定列表中 IP 位址與 MAC 位址不對應的用戶: 此選項打勾後，只要是用戶自行更改電腦的 IP 或不是列表設定的 IP 將無法上網。

封鎖未綁定或綁定列表中未啟用的用戶: 此選項打勾後，只要不在列表中的 MAC Address 都無法上網。

設定完成請按下確認按鈕儲存網路設定變更。若是不想進行變更，請在按下確認儲存動作之前按下取消按鈕，將不做任何設定變更。

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為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，因為會非常耗時且困難。再者，將 MAC Address 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 Address，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 User 試圖修改不是您指定的 IP 上網。



名稱: 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。

啟用： 勾選您所要綁定的目標。

確定: 將您所選定好的目標綁定到 IP & MAC 綁定列表。

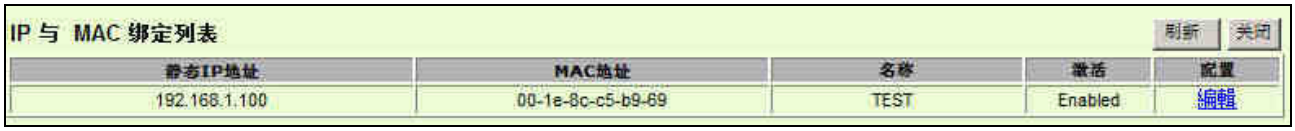
全選 選擇所有在此列表中的目標做綁定。

重新整理： 更新此列表。

關閉: 關閉此列表。

顯示列表

此功能可以列出所有現在已經設定好的 IP/MAC 綁定的狀態，並且可以選擇 Edit 做修改。



4.8.3 DNS 與 WINS 伺服器設定

DNS Server IP：

此設定為發給 PC 端 IP 位址的 DNS 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 位址時，也會一併取得指定的 DNS 伺服器位址。

DNS 伺服器 1： 輸入第一個 DNS 網域伺服器的 IP 位置。

DNS 伺服器 2： 輸入第二個 DNS 網域伺服器的 IP 位置。

WINS 伺服器：

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 伺服器： 輸入 WINS 網域伺服器的 IP 位置。

設定完成請按下確認按鈕儲存網路設定變更。若是不想進行變更，請在按下確認儲存動作之前按下取消按鈕，將不做任何設定變更。

4.8.4 DHCP Status

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

DHCP 伺服器 IP 位址: 目前 DHCP 伺服器的 IP 位址。

已使用的動態 IP 數量： 目前 DHCP 伺服器已經發放動態 IP 的數量。

已發放的固定 IP 數量: 目前 DHCP 伺服器已經發放固定 IP 的數量。

剩餘可用的 IP 數量: 目前 DHCP 伺服器可以還可發放的 IP 數量。

可發放的 IP 總量: 目前 DHCP 伺服器所設定可發放的 IP 總數量。

主機名稱: 目前此台電腦的電腦名稱。

IP 位址: 目前此台電腦所取得的 IP 位址。

MAC 位址: 目前此台電腦的 MAC 網路實體位置。

目前租約剩餘時間: DHCP 目前核發 IP 位址的租約剩餘時間。

刪除: 刪除此筆核發 IP 記錄。

設定完成請按下確認按鈕儲存網路設定變更。若是不想進行變更，請在按下確認儲存動作之前按下取消按鈕，將不做任何設定變更。

5、Tool 系統工具功能設定

此章節介紹用來管理路由器以及測試網路連線的工具。

5.1 Diagnostic 線上連線測試

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。此包含網域名稱查詢測試以及 Ping-封包傳送/接收測試二種。

DNS Name Lookup 網域名稱查詢測試

請於此測試畫面輸入您想查詢的網域主機位置名稱，如 www.abc.com 然後按下 Go 的按鈕開始測試。測試結果會顯示於畫面上。

Ping-封包傳送/接收測試

此項目為主要提供管理者瞭解對外連線的實際狀況，可以藉由此功能瞭解網路上的電腦是否存在！

請於此測試畫面輸入您想測試的主機位置 IP，如 192.168.5.20 按下 Go 的按鈕開始測試，測試結果會顯示於畫面上。

5.2 Restart 重新啟動

您可以於此工具中選擇路由器系統重新開機功能，請按下 Restart Router 按鈕即可重新開機啟動。

5.3 Factory Default 恢復原出廠預設值

若是選擇 Return to Factory Default Setting，路由器會將所有的設定清除，並重新開機。我們建議在做版本升級前請先將路由器現在的設定值存儲到電腦，等做完版本升級後，使用此功能將機器做出廠值設定以確保機器升級後的穩定性，然後再將剛才存在電腦的設定值存回路由器（如何儲存路由器的設定資料及升級完成後如何存回路由器，請參考“系統配置參數檔備份”說明)。

5.4 Firmware Upgrade 系統軟體更新

此功能可以讓路由器在 Web 設定畫面中直接做軟體升級。請您於升級前先確認軟體版本資訊。按下瀏覽按鈕，選擇軟體存放資料夾，並於選擇欲升級的軟體後，按下 Firmware Upgarde Right Now 做升級。

注意！

執行軟體(Firmware)升級前，請詳細閱讀畫面中的注意事項。 正在做軟體(Firmware)升級當中時，請勿離開此升級畫面，否則會造成路由器升級失敗。

5.5 Setting Backup 系統配置參數檔備份

配置參數回復 - 匯入配置檔：

此功能為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 流覽 至備份參數檔案 "config.exp" 存放資料夾，選擇該檔案後，按下匯入按鈕做設定檔案匯入。

配置參數備份 – 匯出：

此功能為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！選擇至備份參數檔案-"config.exp" 存放資料夾位置，按下匯出按鈕即可。

5.6 SNMP 網路管理

SNMP 為 Simple Network Management Protocol 的縮寫，指網路管理通訊協定。此為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。VPN 防火牆支援標準 SNMP v1/v2c，可以搭配標準 SNMP 網路管理軟體來得知目前 VPN 防火牆上的機器運作情況，以便隨時掌握網路資訊。

啟用： 將 SNMP 功能開啟或關閉。系統預設為開啟此功能。

系統名稱： 設定機器的名稱。

連絡方式： 設定機器的管理聯繫人員名稱。

系統地址： 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。

確定： 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。

取消：

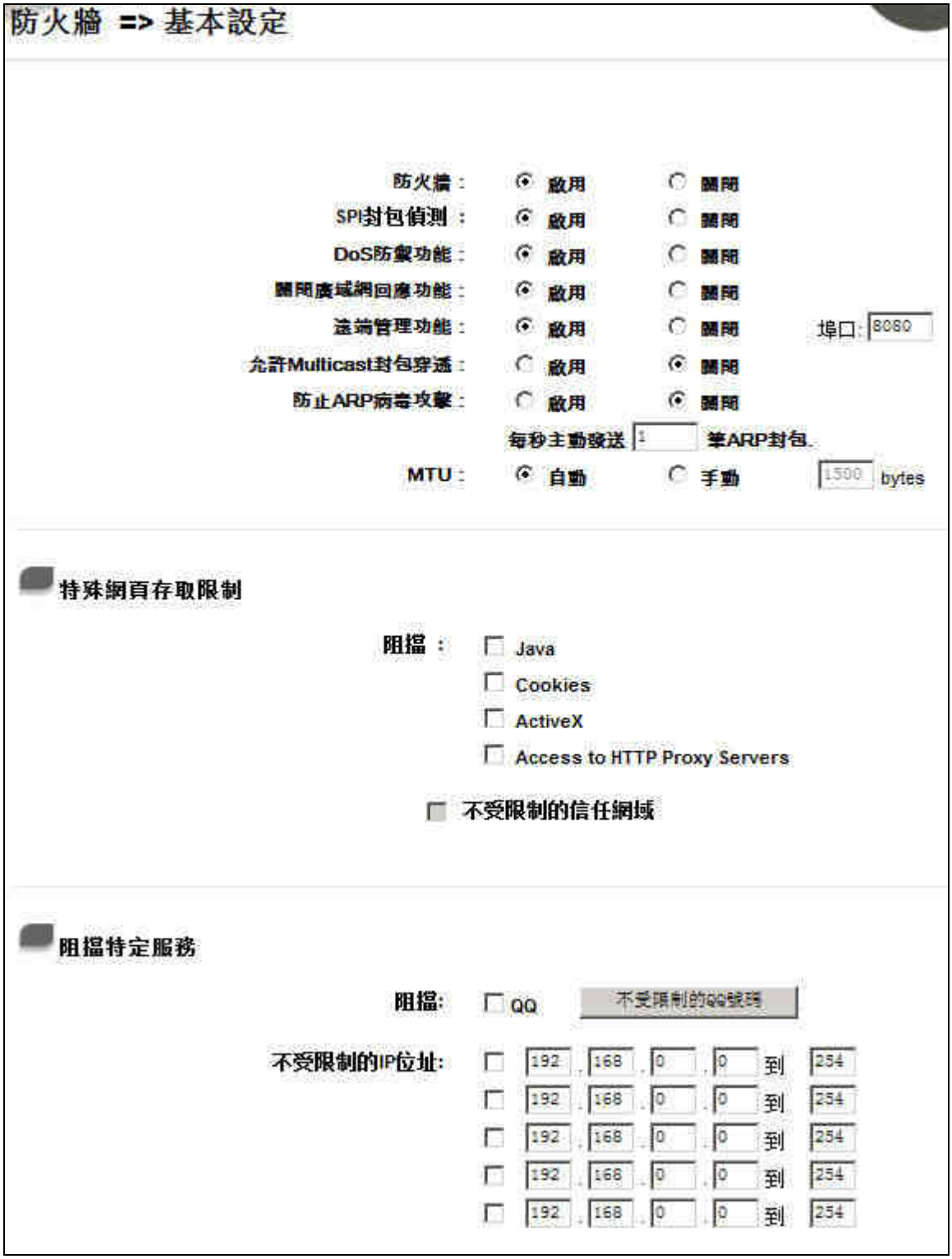
點選此按鈕"取消"即會清除剛才所變動的修改設定內容參數，此操作必須於確認儲存動作之前才會有效。

6、Firewall 防火牆功能設定

本章節介紹防火牆設定的選項，以及網路存取控制的設定。

6.1 基本設定

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



防火牆：　　此為選擇開啟或關閉防火牆功能。

SPI 封包偵測:　　此為封包主動偵測檢驗技術，防火牆主要運作在網路的層

	級，但是藉由執行對每個連接的動態檢驗，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接。
DoS 防禦功能:	此為保護 DoS 攻擊，如 SYN Flooding，Smurf，LAND，Ping of Death，IP Spoofing 等。
關閉廣域網回應功能:	若是選擇啟動的話，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，預設值為開啟拒絕對外回應的功能。
遠端管理功能:	遠端管理功能，若您要透過遠端 Internet 直接連線進入路由器的設定畫面，必需將此功能開啟，並於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(預設為 8080，可更改)。
允許 Multicast 封包穿透：	網路上有許多影音串流媒體，使用廣播方式可以讓 Client 端接收此類封包訊息格式。預設值為關閉這個功能。
防止 ARP 病毒攻擊	此功能為防止內網遭受 ARP 欺騙攻擊而造成電腦無法上網，此 ARP 病毒欺騙大多在網咖環境發生，會讓所有上網電腦一瞬間掉線或部份電腦無法上網。開啟此功能可以避免此種病毒攻擊。
MTU:	MTU 為 Maximum Transmission Unit 的縮寫，一般預設為 1,500。但是在不同的網路環境中， 可能會使用不同的數值。尤以 ADSL PPPoE 的狀況為最多(ADSL PPPoE MTU Size：1492)。不過許多的 Server 與 ADSL PPPoE 用戶的 MTU Size 相關，一般使用預設 Auto 即可，不需做任何調整。
特殊網頁存取限制：	路由器支援封鎖下列幾種的方式連接：Java，Cookies，Active X， Access to HTTP Proxy Servers。
不受限制的信任網域:	若啟動這項功能，使用者可以將信任的網站或者 IP 位址加入可信任的網域中，則路由器就不會去阻擋可信任網域的網頁中所帶有的 Java/ActiveX/Cookies 等項目。
阻擋特定服務：	安全路由器提供一指封 QQ 的服務功能，可以通過設定將 QQ

服務擋住，以方便用戶的管理設定。

另外，若啟用封鎖 QQ 服務，也可以針對某些 QQ 號碼或 IP 範圍能夠不受封鎖做設定，按下”不受限制的 QQ 號碼”，跳出以下視窗即可將不受封鎖限制的 QQ 號碼輸入，增加到下方清單以內：

設定完成請按下確認按鈕儲存網路設定變更。若是不想進行變更，請在按下確認儲存動作之前按下取消按鈕，將不做任何設定變更。

6.2 Access Rule 網路存取規則

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，或是設定以使用者的 IP 位址、目地端 IP 位址、IP

通訊協定形態等條件來做管制，管理者可以依照實際的需求調整設置。

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 Internet 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：

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

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項目為永遠開啟，不受其他自訂規則所影響：

- HTTP 的服務從 LAN 端到路由器預設為開啟的（為了管理路由器使用)。
- DHCP 的服務從 LAN 端到路由器預設為開啟的（為了從路由器自動取得 IP 位址使用)。
- DNS 的服務從 LAN 端到路由器預設為開啟的（為了解析 DNS 服務使用)。
- Ping 的服務從 LAN 端到路由器預設為開啟的（ 為了連通測試路由器使用)。

防火牆 => 存取規則設定

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項目中。路由器在做規則確認時是依照優先權利 1-2-3…..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，以避免您想開啟或關閉的功能失效。

編輯： 可以設定網路存取規則項目。

垃圾桶圖像： 可以刪除網路存取規則項目。

加入新規則： 新增新的網路存取規則按鈕可以新增一項新的存取規則。

回復出廠預設值： 可以恢復到出廠原有預設存取規則項目並刪除所有的自訂規則內容。

增加新的管制規則

管制動作: 此為設定此規則的管制條例動作：

允許：允許符合此管制條例行為的封包通過。

禁止：不允許符合此管制條例行為的封包通過。

通訊埠: 從下拉式選單中選擇您所要允許或不允許的服務埠項目。

日誌： 啟用： 依據此規則發生的相關事件將在日誌中記錄。

關閉： 依據此規則發生的相關事件不會日誌中記錄。

通訊埠設定: 若是您想要管制的服務埠沒有存在於預設列表內的話，您可以按下右方的"服務埠管理" 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口，按下 Add-新增按鈕即可新增一個管制服務項目內容。

接口位置: 選擇您所要允許或不允許的來源封包介面(例如是從 LAN，WAN1，WAN2 或是任何)，可以從下拉式選單中選擇。

來源 IP 位址: 選擇來源封包的 IP 範圍(如任何，單一，或範圍)，若是選擇單一或是範圍的話，請輸入此單一或是一區段範圍的 IP 位址。

目的 IP 位址: 選擇目的端封包的 IP 範圍(如任何，單一，或範圍)，若是選擇單一或是範圍的話，請輸入此單一或是一區段範圍的 IP 位址。

時間排程設定: 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。

加入到對應列表: 可選擇 ”所有時間” 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，以及設定是每天還是某幾天做管制。

____到____: …到….： 此管制規則有時間限制，設定方式為 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 每天 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，可以直接做個別選擇。

設定完成請按下確認按鈕儲存網路設定變更。若是不想進行變更，請在按下確認儲存動作之前按下取消按鈕，將不做任何設定變更。

6.3 網頁內容管制

路由器的網頁內容管制設定可支援兩種模式的網頁管制，一為開啟網頁內容管制功能封鎖不允許訪問的網址，另一個為開啟只允許可以訪問的網頁管制允許訪問的網站，此兩種模式只能使用一種。

設定禁止連接的網域

此功能需將完整的網址如 www.sex.com 填入，即可封鎖此網站。

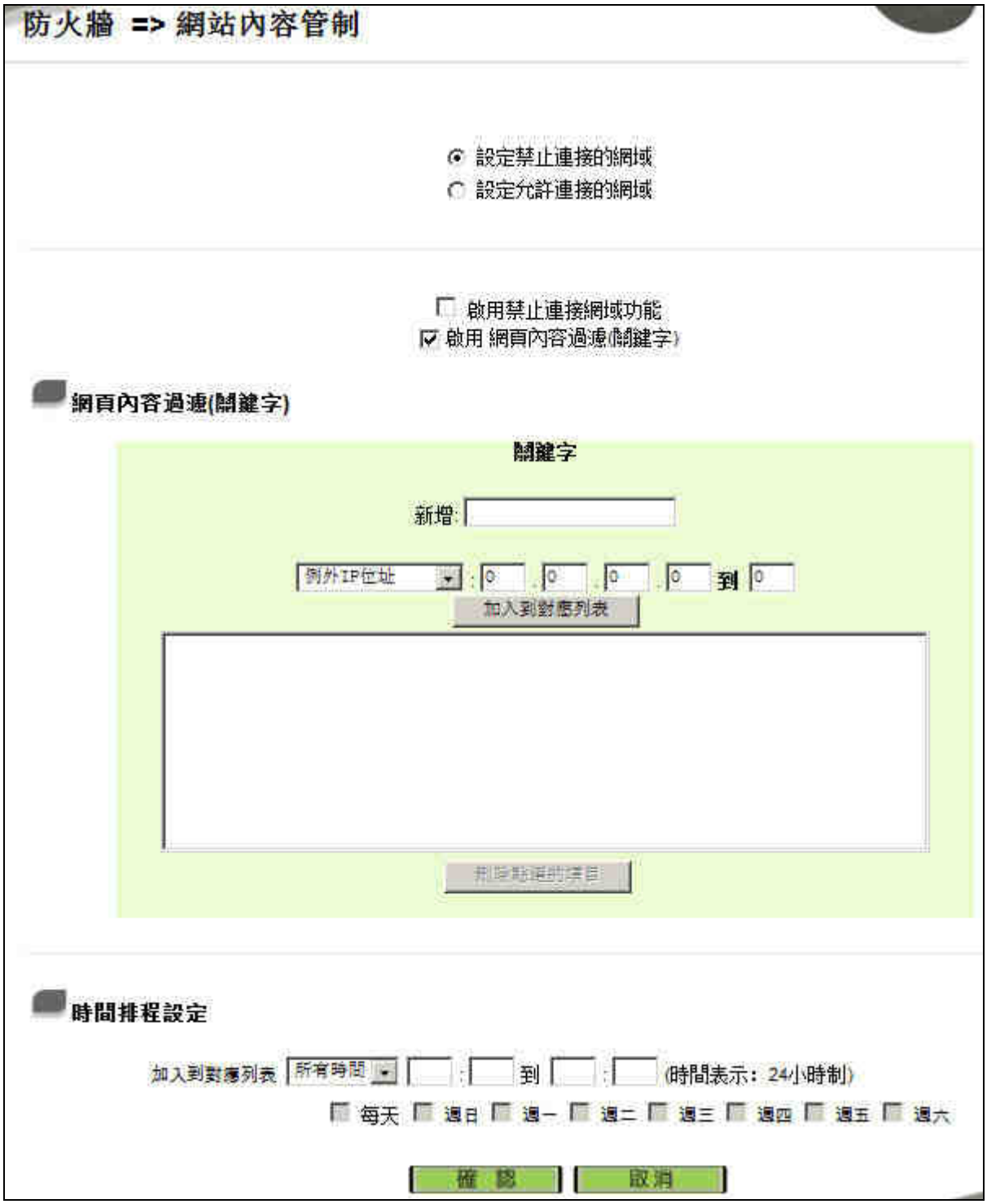
啟用禁止連接網域功能: 選擇打勾功能變數名稱過濾功能，預設為關閉。

禁止連接的網域名稱: 網頁管制內容項目。

加入到對應列表: 填寫欲管制的網址，如 www.playboy.com。

網頁關鍵字串過濾管制：

只要輸入如“sex”的字元，那所有在網址裏面有“sex”的網站都會被封鎖。



啟用網頁內容過濾（關鍵字）： 選擇打勾網頁關鍵字串功能，預設為關閉。

當此項功能啟動後，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。

新增關鍵字: 輸入關鍵字。

允許連接的網域

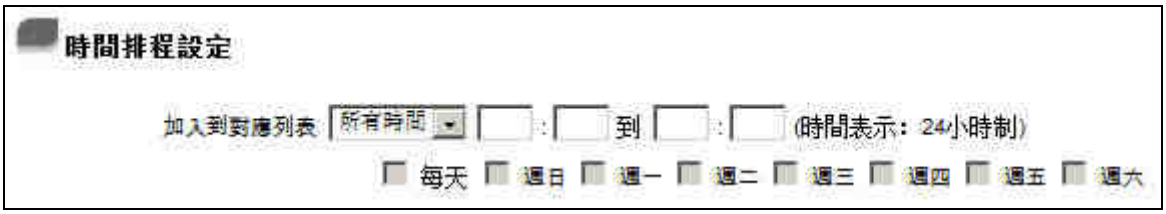
此功能的目的是設定只能去訪問的網址，在有些公司或學校中，會只允許員工或學生只能去哪些網站，就可以用此功能來達成。

允許連接的網域： 選擇打勾開啟允許網址管制功能，預設為關閉。

新增: 填寫欲管制的允許網址，如 www.playboy.com。

時間排程設定

當選擇為 "所有時間" 時，表示此條規則 24 小時執行。若選擇從時，此管制條例會依據所設定的生效時間去執行此條規則，如管制時間為週一到週五，早上八點到下午六點，您可以依照以下圖例來管制。



所有時間: 表示此管制規則 24 小時開啟。

____到____: ...到....： 此管制規則有時間限制，設定方式為 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 "每天"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。

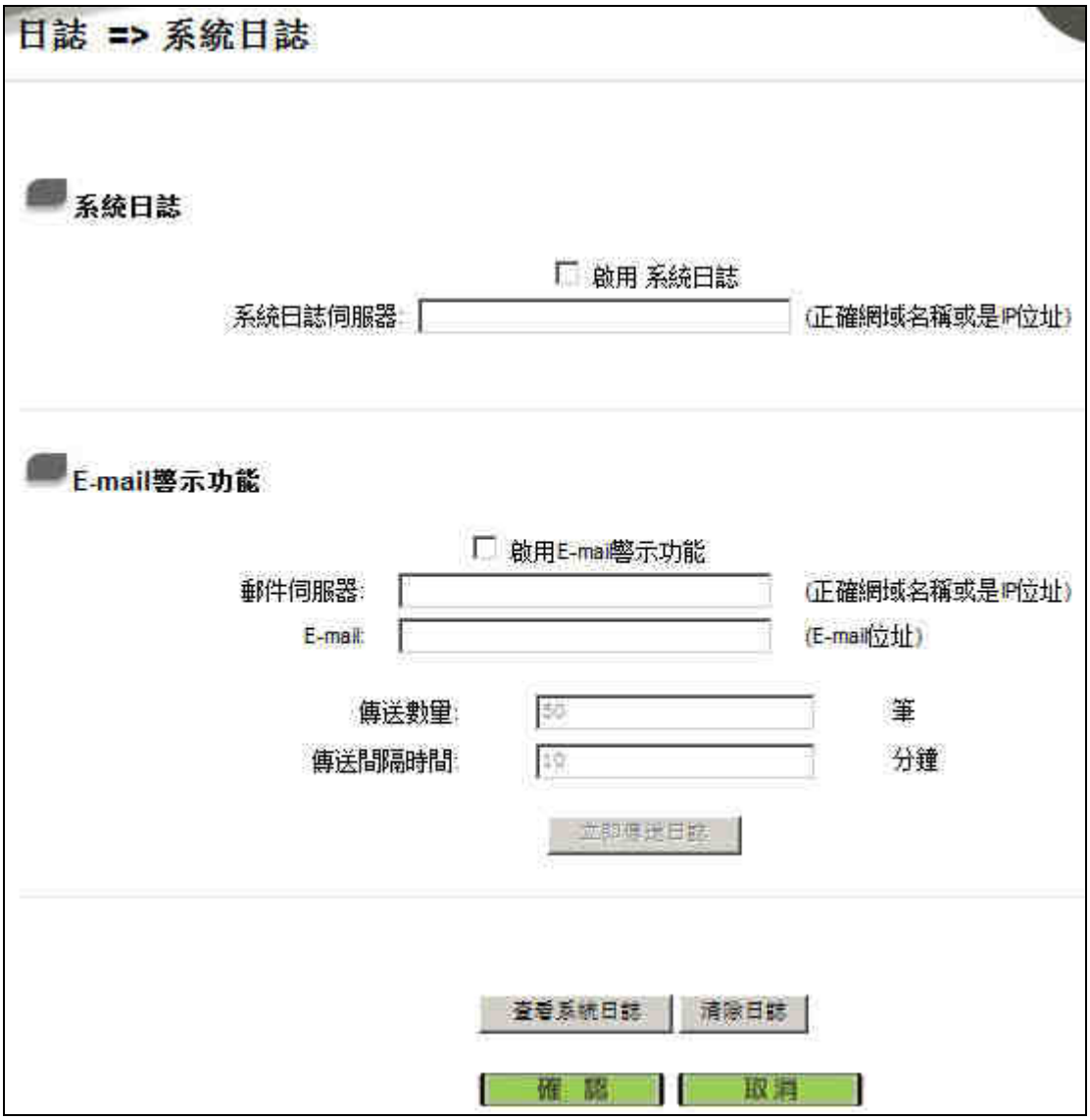
設定完成請按下確認按鈕儲存網路設定變更。若是不想進行變更，請在按下確認儲存動作之前按下取消按鈕，將不做任何設定變更。

7、Log 日誌功能設定

日誌(Log)功能記錄路由器的運行資料，並以可讀的方式呈現再設定畫面上提供給您作為參考。您可以依據需求檢視這些資訊。

7.1 System Log 系統日誌

路由器的日誌記錄提供三種設定：syslog 系統日誌， E-mail Alert 電子郵件通知。



Syslog 系統日誌

啟用系統日誌: 若是勾選此選項的話，系統日誌功能將被開啟。

系統日誌伺服器: 路由器提供了外部系統日誌伺服器收集系統資訊功能。系統日誌為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 IP 位址與目地 IP 位址，服務編號以及形態。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。

E-mail 警示功能

啟用 E-mail 警示功能: 若是此選項勾選的話， 電子郵件告警(E-Mail Alert)將會被開啟

郵件伺服器： 若您希望所有的日誌電子郵件都可以寄出的話，請於此輸入電子郵件伺服器的名稱或是 IP 位址，如：mail.abc.com

E-mail： 此為設定日誌收件人電子郵件信箱，如：abc@mail.abc.com

傳送數量： 自定 Log entries 數量，系統預設為 50 個 entries。 當到達此數量時，路由器 將會自動傳送-Mail 日誌

傳送間隔時間： 自定傳送 Log 間隔時間，系統預設為 10 分鐘。 當到達此時間時，路由器 將會自動傳送-Mail 此日誌

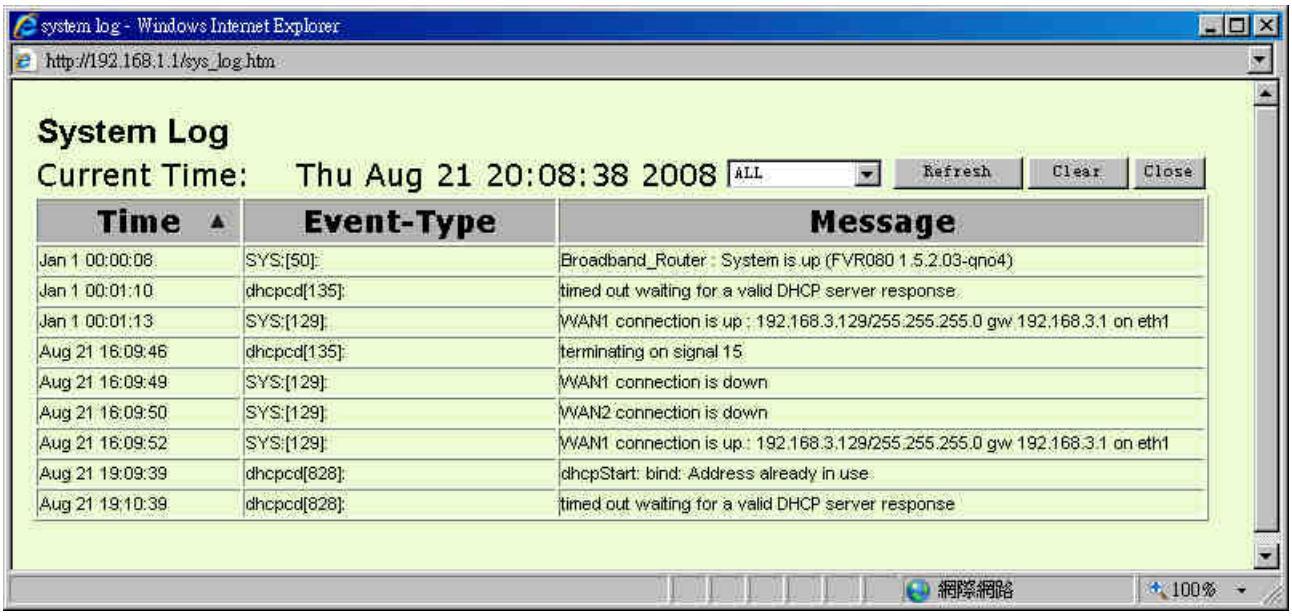
路由器 將會自動判別當 entries 數量或是間隔時間哪一個參數先到達，就傳送-Mail 日誌訊息給用戶

立即傳送日誌: 使用用戶可以即時直接按下此鈕傳送 Log

以下有兩個有關查詢日誌的按鈕，分別敍述如下：

查看系統日誌：

此為查看系統日誌使用，其資訊內容可以從下拉式選單中分類讀取，包含所有訊息-ALL， 系統日誌-System，防火牆日誌-Firewall。選擇"Refresh"按鈕可以刷新日誌顯示畫面，"Clear"按鈕可以清除所有日誌記錄。如下圖所示：



清除日誌：

此按鈕為清除所有目前路由器的日誌相關資訊。

7.2 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運作資訊，包含區域或廣域網埠口名稱，目前埠口連線狀態，IP 位址，網路實體位置，子網路遮罩，預設閘道，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/秒，上傳頻寬使用率(%)，下載頻寬使用率(%)等資訊。

日誌 => 系統狀態

	區域網	廣域網1接口	廣域網2接口	廣域網3接口
裝置名稱	eth0	eth1	eth2	eth3
線路連線狀態	---	連線	Enabled	Enabled
IP位址	192.168.1.1	192.168.8.101	0.0.0.0	0.0.0.0
MAC 位址	00-0E-A0-12-34-56	00-0E-A0-12-34-57	00-0E-A0-12-34-58	00-0E-A0-12-34-59
子網路遮罩	255.255.255.0	255.255.255.0	0.0.0.0	0.0.0.0
預設閘道	---	192.168.8.1	0.0.0.0	0.0.0.0
DNS伺服器	---	192.168.3.10 192.168.3.15	0.0.0.0	0.0.0.0
線路偵測機制	---	測試成功	測試失敗	測試失敗
接收封包數	0	6660	0	0
傳送封包數	0	7065	207	207
全部封包數	0	13725	207	207
接收封包流量	0	775914	0	0
傳送封包流量	0	6075253	122958	122958
全部封包流量	0	6851167	122958	122958
目前接收流量 Bytes/Sec	0	30	0	0
目前傳送流量 Bytes/Sec	0	0	0	0
錯誤封包統計	0	0	0	0
丟棄封包統計	0	0	0	0
連線數	---	12	0	0
新連線數/秒	---	0	0	0
上傳頻寬使用率(%)	---	0	0	0
下載頻寬使用率(%)	---	0	0	0

重新整理

7.3 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。

日誌 => 流量統計

網路流量統計方式 : 依下載流量的IP位置

來源IP位址	bytes/sec	%
192.168.1.100	19	100

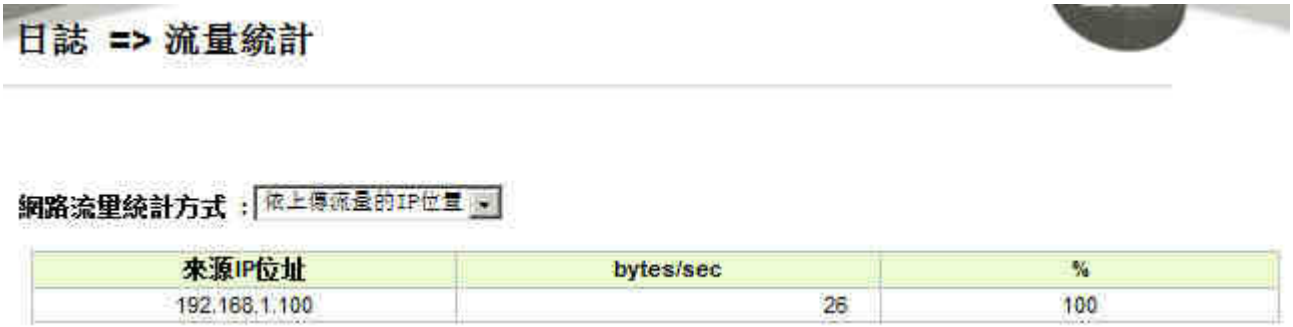
Inbound IP Source Address 對內流量內網 IP 位址：

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

來源IP位址	bytes/sec	%
192.168.1.100	19	100

Outbound IP Source Address 對外流量內網 IP 位址：

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



來源IP位址	bytes/sec	%
192.168.1.100	26	100

Inbound IP Service 對內流量 IP 服務埠號：

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。

通訊協定	目的埠	bytes/sec	%
TCP	http(80)	64351	98
TCP	1155	693	1

Outbound IP Service 對外流量 IP 服務埠號：

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。

通訊協定	目的埠	bytes/sec	%
UDP	514	3478	100

Inbound IP Session 對內流量 IP 連線數：

在此圖表中顯示了來源端的 IP 位址，網路的協定的種類，來源端的埠，目的端 IP 位址， 目的端的埠，每秒有多少 byte 與百分比。

來源IP位址	通訊協定	來源埠	目的IP位址	目的埠	bytes/sec	%
192.168.1.100	TCP	51560	192.168.3.10	1155	19	100

Outbound IP Session 對外流量 IP 連線數：

此圖表中顯示了來源端的 IP 位址，網路的協定的種類，來源端的埠，目的端 IP 位址， 目的端的埠，每秒有多少 byte 與百分比

來源IP位址	通訊協定	來源埠	目的IP位址	目的埠	bytes/sec	%
127.0.0.1	UDP	1024	127.0.0.1	514	5884	99
192.168.1.100	TCP	51560	192.168.3.10	1155	26	0

7.4 Specific IP/Port status 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 Port 去查詢此 IP 去訪問的目的位址，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 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。

來源IP位址	通訊協議	來源通訊埠	接口位置(WAN)	目地IP位址	目地通訊埠	下載頻寬 Bytes/Sec	上傳頻寬 Bytes/Sec
192.168.1.100	TCP	51639	WAN1	207.46.124.196	1863	38	4
192.168.1.100	TCP	51560	WAN1	192.168.3.10	1155	0	0
192.168.1.100	TCP	51563	WAN1	192.168.3.10	1026	0	0
192.168.1.100	TCP	54488	WAN1	65.54.189.113	443	0	0

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服務埠。

來源IP位址	通訊協議	來源通訊埠	接口位置(WAN)	目地IP位址	目地通訊埠	下載頻寬 Bytes/Sec	上傳頻寬 Bytes/Sec
192.168.1.100	TCP	51639	WAN1	207.46.124.196	1863	38	4
192.168.1.100	TCP	51560	WAN1	192.168.3.10	1155	0	0
192.168.1.100	TCP	51563	WAN1	192.168.3.10	1026	0	0
192.168.1.100	TCP	54488	WAN1	65.54.189.113	443	0	0

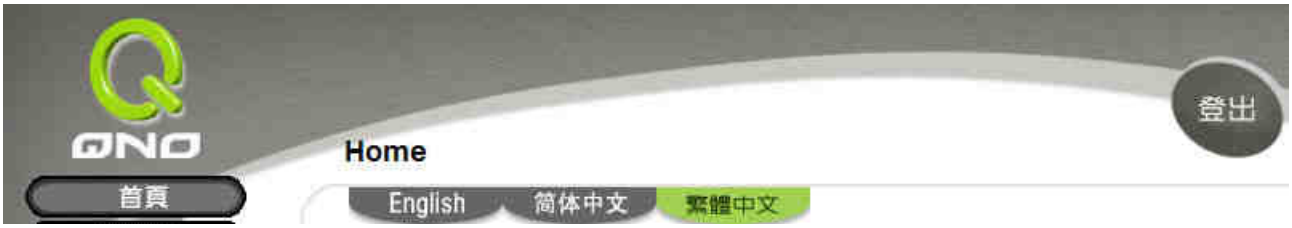
特定埠狀態：

直接在 Port 裏填入您想要查詢的服務埠，就可以顯示出此服務埠現在有哪些 IP 正在使用。

來源IP位址	通訊協議	來源通訊埠	接口位置(WAN)	目地IP位址	目地通訊埠	下載頻寬 Bytes/Sec	上傳頻寬 Bytes/Sec
192.168.1.100	TCP	54684	WAN1	119.160.254.197	80	925	145
192.168.1.100	TCP	54687	WAN1	119.160.254.197	80	284	56
192.168.1.100	TCP	54689	WAN1	119.160.246.241	80	120	75
192.168.1.100	TCP	54693	WAN1	119.160.246.242	80	80	90
192.168.1.100	TCP	54685	WAN1	119.160.246.241	80	82	79
192.168.1.100	TCP	54694	WAN1	203.69.113.27	80	72	63
192.168.1.100	TCP	54692	WAN1	119.160.246.241	80	63	70
192.168.1.100	TCP	54696	WAN1	119.160.245.215	80	4	8
192.168.1.100	TCP	54707	WAN1	119.160.243.113	80	0	0
192.168.1.100	TCP	54697	WAN1	203.69.113.27	80	0	0
192.168.1.100	TCP	54700	WAN1	119.160.254.197	80	0	0
192.168.1.100	TCP	54701	WAN1	119.160.254.197	80	0	0
192.168.1.100	TCP	54705	WAN1	119.160.254.197	80	0	0
192.168.1.100	TCP	54704	WAN1	119.160.254.197	80	0	0

8、Logout 登出

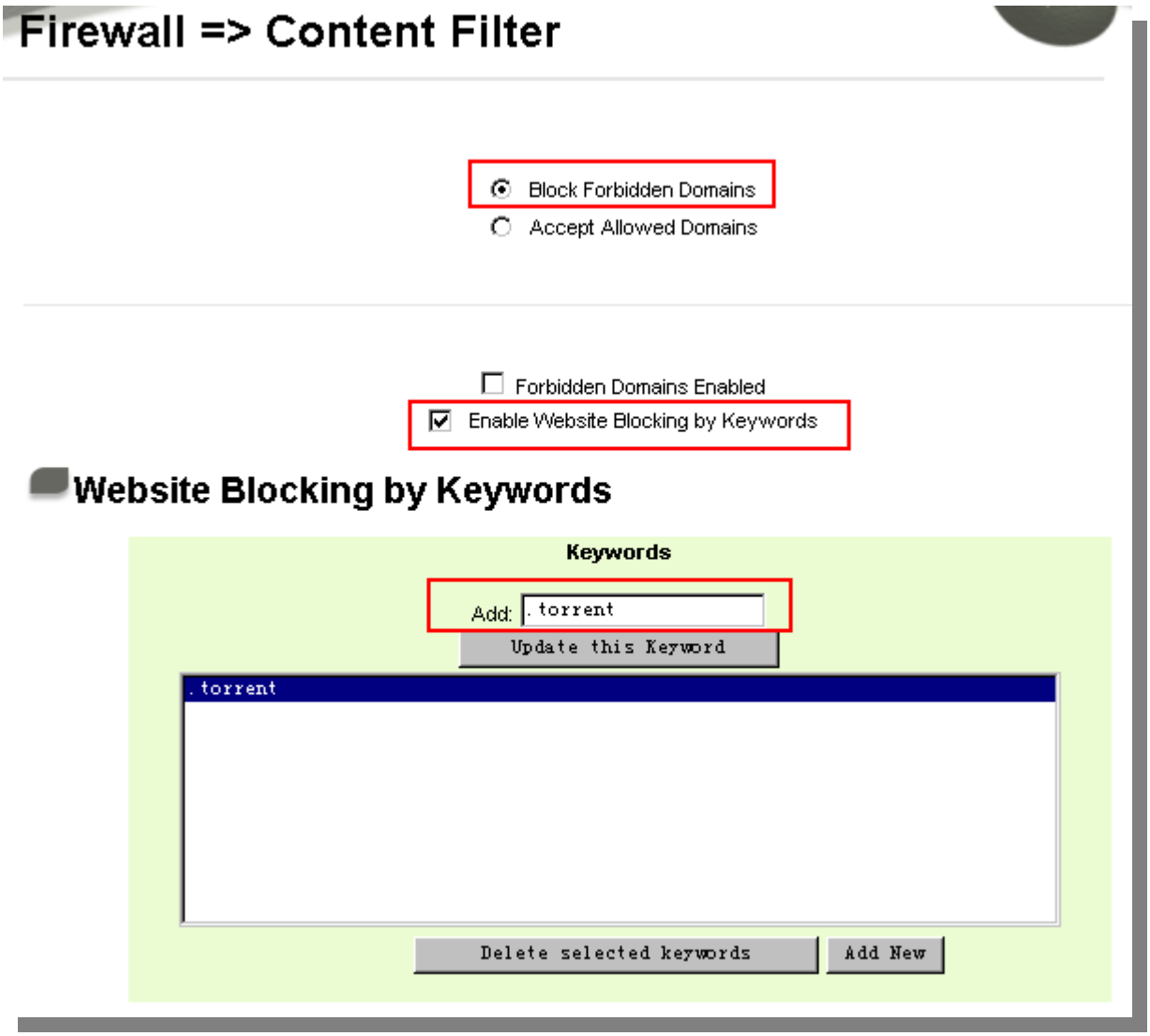
路由器的網頁畫面右上方有一個登出的按鈕，此按鈕為終止管理路由器並結束此管理畫面。若您下次想再進入路由器管理畫面時，您必須重複進入路由器管理畫面的步驟，並再輸入管理者使用名稱與密碼。



附錄一：常見問題解決

（1） 阻擋基本 BT 下載方式

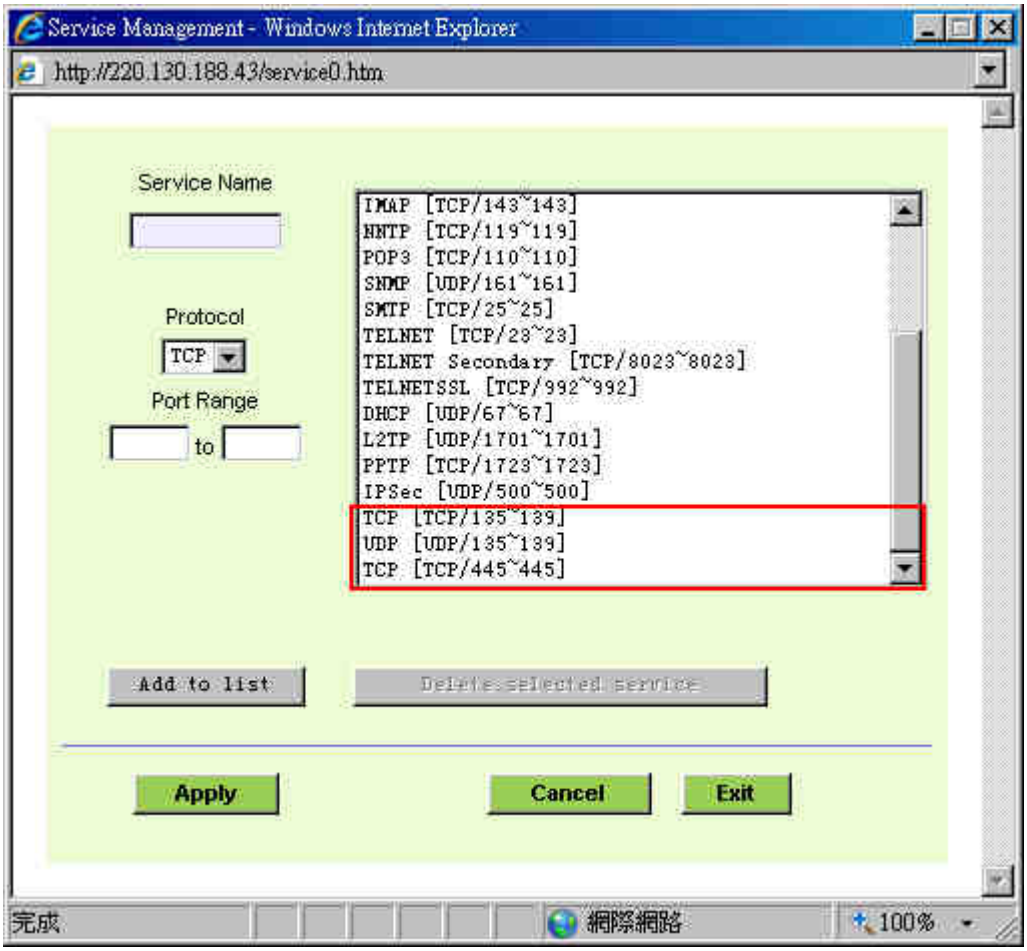
若您想要將 BT 種子給擋下，不讓用戶下載，您可以直接在"Firewall"=>"Content Filter"=>" Block Forbidden Domains"=>"Enable Website Blocking by Keywords "之後，打入".torrent"就可以防止用戶下載種子。



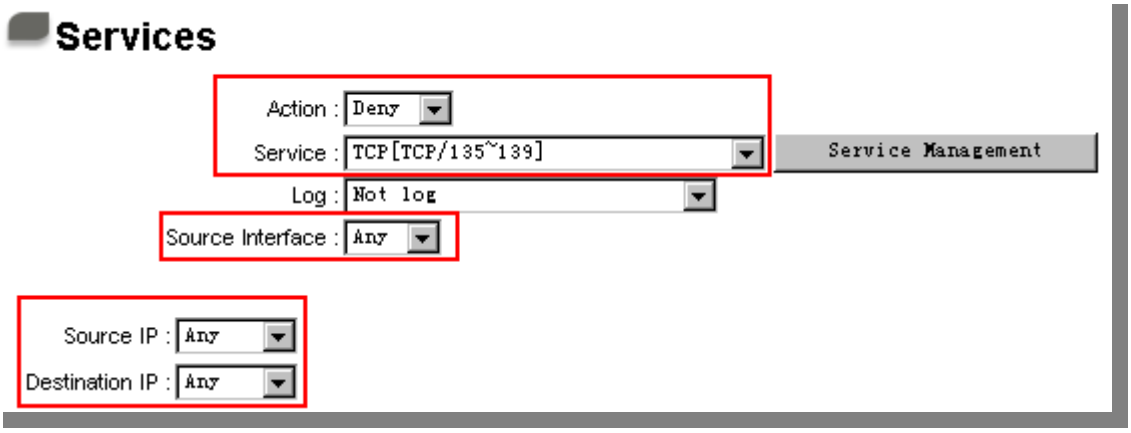
（2） 衝擊波及蠕蟲病毒的防制

由於近來還是發生有許重使用者內網中衝擊波及蠕蟲病毒造成內網存取 Internet 很慢及連線數(Session)大量增加造成路由器大量處理. 所以以下為指導您封鎖此病毒相應通訊埠以達到防制目的。

a. 增加此 TCP135-139， UDP135-139 還有 TCP445 通訊埠：



b. 用防火牆裡面的"Access Rule"功能將設定好的此三組通訊埠封鎖：



用同樣的方法添加好 UDP[UDP135~139]以及 TCP[445~445]通訊埠。

c. 將這三組的優先級至於最高：

Firewall => Access Rule

Jump to 1 / 2 page 5 entries per page Next page >>

Priority	Enable	Action	Service	Source Interface	Source	Destination	Time	Day		Delete
1	☑	Deny	TCP [445]	*	Any	Any	Always		Edit	
2	☑	Deny	UDP [135]	*	Any	Any	Always		Edit	
3	☑	Deny	TCP [135]	*	Any	Any	Always		Edit	
	☑	Allow	All Traffic [1]	LAN	Any	Any	Always			
	☑	Deny	All Traffic [1]	WAN1	Any	Any	Always			

Add New Rule Restore to Default Rules

（3）ARP 病毒攻擊防制

1）. ARP 問題的提出以及相關知識

近期，國內多家網咖出現短時間內斷線(全斷或部分斷)的現象，但會在很短的時間內會自動回復。這是因為 MAC 位址衝突引起的，當帶毒機器的 MAC 對映到主機或者路由器之類的 NAT 裝置，那麼全網斷線，如果只對映到網內其他機器，則只有這部分機器出問題。多發於傳奇游戲特別是外掛等方面。此類情況就是網路受到了 ARP 病毒攻擊的明顯表現，其目的在於，該病毒破解游戲加密解密算法，通過截取區域網路中的資料包，然後解析游戲通訊協定的方法截獲用戶的資訊。執行這個病毒，就可以獲得整個區域網路中游戲玩家的詳細資訊，盜取用戶帳號資訊。下面我們談談如何防制這種攻擊。

首先，我們了解下什麼是 ARP，ARP "Address Resolution Protocol"（位址解析協定），區域網路中，網路中實際傳送的是"訊框"，訊框裡面是有目標主機的 MAC 位址的。所謂"位址解析"就是主機在傳送訊框前將目標 IP 位址轉換成目標 MAC 位址的過程。ARP 協定的基本功能就是通過目標裝置的 IP 位址，查詢目標裝置的 MAC 位址，以保證通訊的順利進行。

ARP 協定的工作原理：在每台安裝有 TCP/IP 協定的電腦裡都有一個 ARP 緩衝區表，表裡的 IP 位址與 MAC 位址是一一對應的，如表所示。

IP 址	MAC 位址
192.168.1.1	00-0f-3d-83-74-28
192.168.1.2	00-aa-00-62-c5-03
192.168.1.3	03-aa-01-75-c3-06
……	……

我們以主機 A（192.168.1.5）向主機 B（192.168.1.1）傳送資料為例。當傳送資料時，主機 A 會在自己的 ARP 緩衝區表中搜尋是否有目標 IP 位址。如果找到了，也就知道了目標 MAC 位址，直接把目標 MAC 位址寫入訊框裡面傳送就可以了；如果在 ARP 緩衝區表中没有找到相對應的 IP 位址，主機 A 就會在網路上傳送一個廣播，目標 MAC 位址是"FF.FF.FF.FF.FF.FF"，這表示向同一網段內的所有主機發出這樣的詢問："192.168.1.1 的 MAC 位址是什麼？"網路上其他主機並不回應 ARP 詢問，只有主機 B 接收到這個訊框時，才向主機 A 做出這樣的因應："192.168.1.1 的 MAC 位址是 00-aa-00-62-c6-09"。這樣，主機 A 就知道了主機 B 的 MAC 位址，它就可以向主機 B 傳送資訊了。同時它還更新了自己的 ARP 緩衝區表。

再者，我們先簡單介紹一下什麼是 ARP 病毒攻擊，這種病毒是對內網的 PC 進行攻擊，使內網 PC 機的 ARP 表混亂，在區域網路中，通過 ARP 協定來完成 IP 位址轉換為第二層實體位址(即 MAC 位址）的。ARP 協定對網路安全具有重要的意義。通過虛擬造 IP 位址和 MAC 位址實現 ARP 欺騙，能夠在網路中產生大量的 ARP 通訊量使網路阻塞。用虛擬造源 MAC 位址傳送 ARP 回應包，對 ARP 高速緩衝區機制的攻擊。這些情況主要出現在網咖用戶，造成網咖部分機器或全部機器暫時中斷連線或者不可以上

網，在重新啓動後可以解決，但保持不了多久又會出現這樣的問題，網咖管理員對每台機器使用 arp –a 指令來檢查 ARP 表的時候發現路由器的 IP 和 MAC 被修改，這就是 ARP 病毒攻擊的典型症狀。

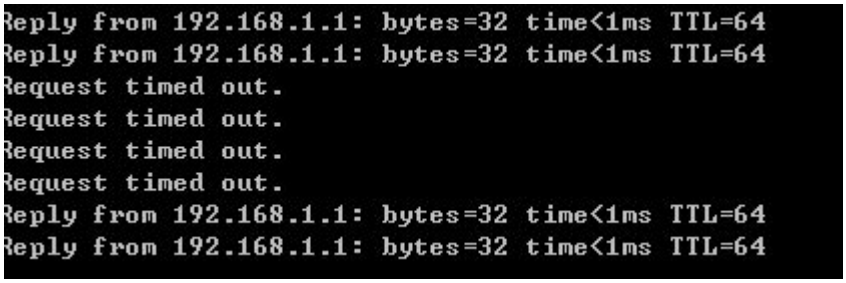
這種病毒的程式如 PWSteal.lemir 或其變種，屬於木馬程式/蠕蟲類病毒，Windows 95/98/Me/NT/2000/XP/2003 將受到影響，病毒攻擊的方式對影響網路連線暢通來看有兩種，對路由器的 ARP 表的欺騙和對內網 PC 閘道的欺騙，前者是先截獲閘道資料，再將一家族的錯誤的內網 MAC 資訊不停的傳送給路由器，造成路由器發出的也是錯誤的 MAC 位址，造成正常 PC 無法收到資訊。後者 ARP 攻擊是虛擬造閘道。它先建立一個假閘道，讓被它欺騙的 PC 向假閘道發資料，而不是通過正常的路由器途徑上網。在 PC 看來，就是上不了網了，"網路中斷連線了"。

就這兩種情況而言，如果對 ARP 病毒攻擊進行防制的話我們必須得做路由器方面和用戶端雙方的設定才保證問題的最終解決。所以我們選取路由器的話最好看看路由器是否帶有防制 ARP 病毒攻擊的功能，Qno 產品正好提供了這樣的功能，相比其他產品作業簡單易學。

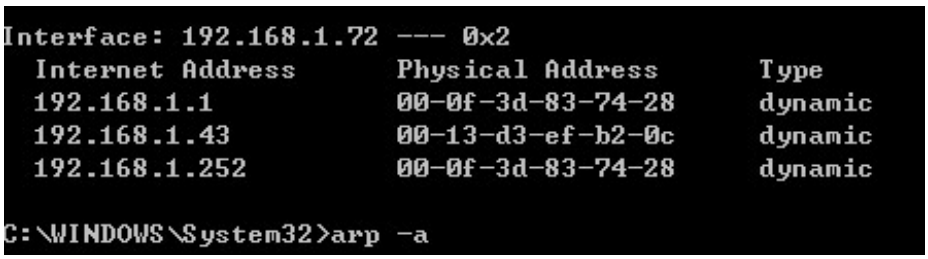
2）. ARP 的判斷

如過網路中有一台或多台電腦受到或已經感染了 ARP 病毒，我們就必須學會判斷並采取相應的解決方法處理類似問題的發生，下面來談談 Qno 技術工程師的 ARP 防制經驗談。

通過對 ARP 工作原理得知，如果系統 ARP 緩衝區表被修改不停的通知路由器一家族錯誤的內網 IP 或者乾脆虛擬造一個假的閘道進行欺騙的話，網路就肯定會出現大面積的中斷連線問題，這樣的情況就是典型的 ARP 攻擊，對遭受 ARP 攻擊的判斷，其方法很容易，你找到出現問題的電腦點開始執行進入系統的 DOS 作業。ping 路由器的 LAN IP 丟包情況。輸入 ping 192.168.1.1（閘道 IP 位址），如圖。



內網 ping 路由器的 LAN IP 丟幾個包，然後又連上，這很有可能是中了 ARP 攻擊。為了進一步確認，我們可以通過尋找 ARP 表來判斷。輸入 ARP -a 指令，顯示如下圖。



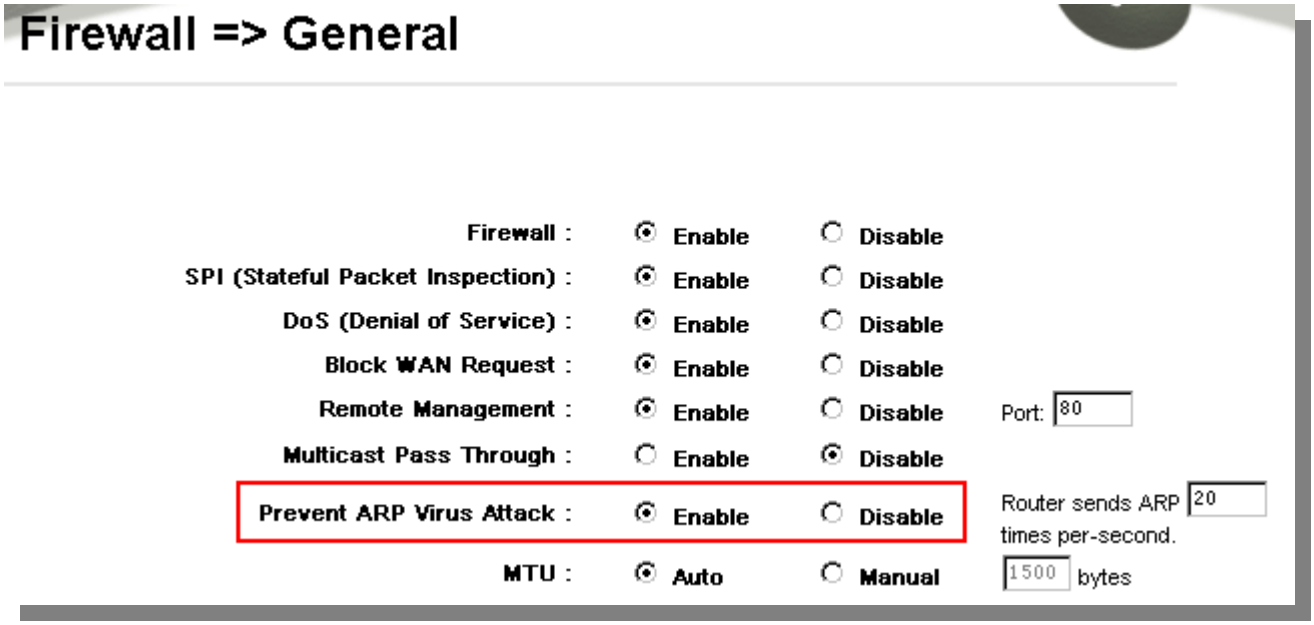
可以看出192.168.1.1位址和192.168.252位址的IP的 MAC位址都是00-0f-3d-83-74-28，很顯然，這就是 ARP 欺騙造成的。

3）. ARP 的解決

我們現在已經理解了 ARP，ARP 欺騙攻擊以及如何判斷此類攻擊，下面的問題就是如何找到行之有效的防制辦法來防止這類攻擊對網路造成的危害。Qno 的一般處理辦法分三個步驟來完成。

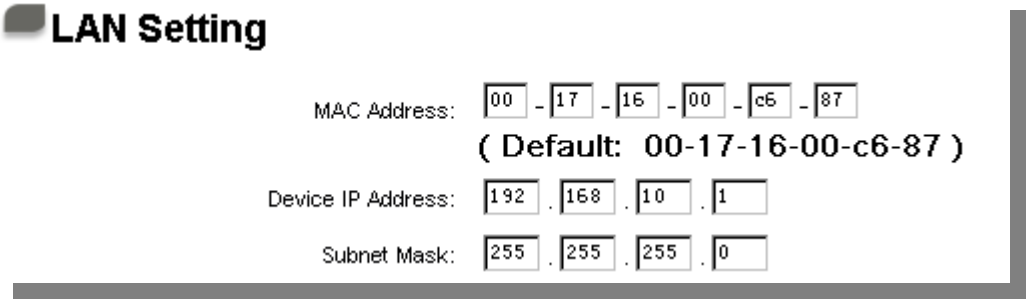
a）、啟動防止 ARP 病毒攻擊：

輸入路由器 IP 位址登入路由器的 Web 管理頁面，進入"Firewall"的"General"，再在右邊找到"Prevent ARP Virus Attack"在這一行的"Enable"前面做點選，再在頁面最下點擊"確認"，如圖。

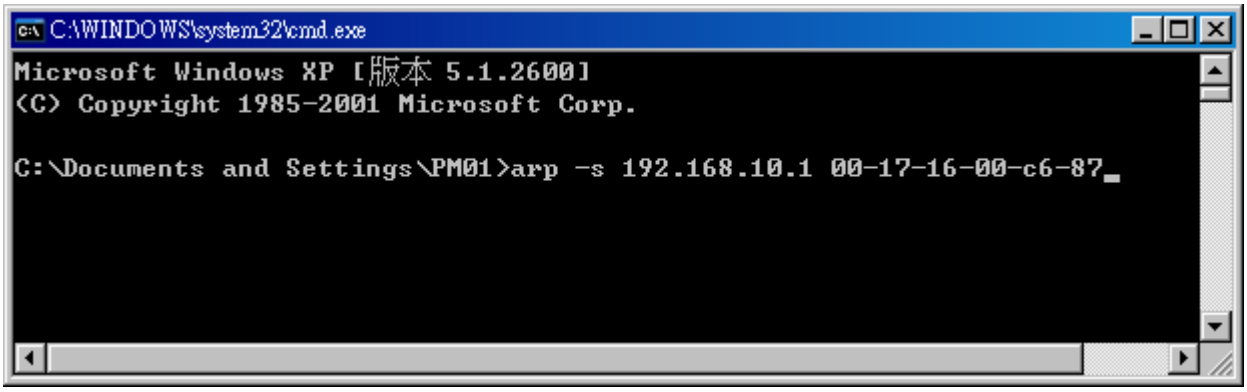


b）、對每台 pc 上連結閘道的 IP 和其 MAC 位址

進行這樣的作業主要防止 ARP 欺騙閘道 IP 和其 MAC 位址首先在路由器端尋找閘道 IP 與 MAC 位址，如圖。



然後在每台 PC 機上開始/執行 cmd 進入 dos 作業，輸入 arp –s　192.168.10.1 00-17-16-00-c6-87，Enter 後完成 pc01 的連結。如圖



針對網路內的其他主機用同樣的方法輸入相應的主機 IP 以及 MAC 位址完成 IP 與 MAC 連結。但是此動作，如果重起了電腦，作用就會消失，所以可以把此指令做成一個批處理檔案，放在作業系統的啓動裡面，批處理檔案可以這樣寫：

@echo off

arp -d

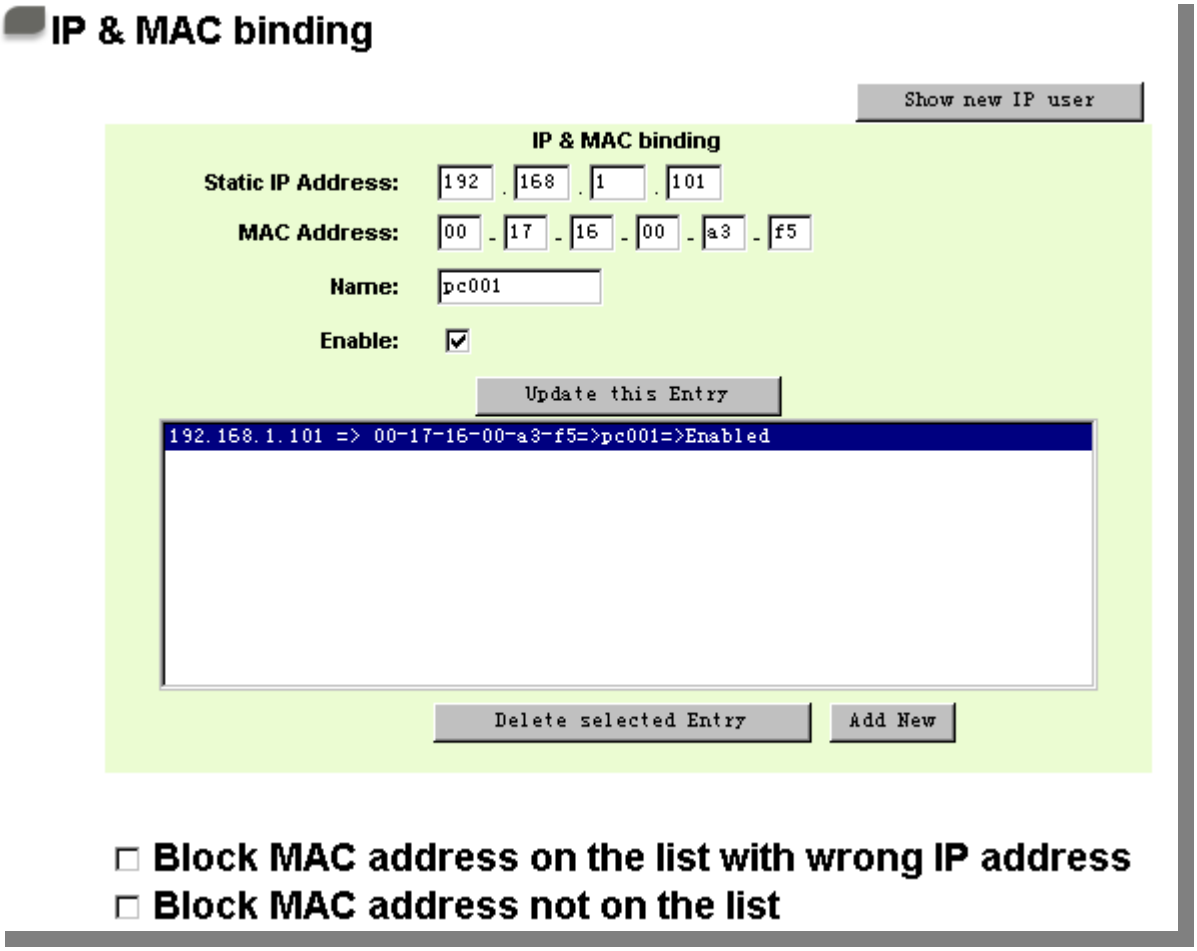
arp –s 路由器 LAN IP　路由器 LAN MAC

對於已經中了 arp 攻擊的內網，要找到攻擊源。方法：在 PC 上不了網或者 ping 丟包的時候，在 DOS 下打 arp –a 指令，看顯示的閘道的 MAC 位址是否和路由器真實的 MAC 相同。如果不是，則尋找這個 MAC 位址所對應的 PC，這台 PC 就是攻擊源。

其他的路由器用戶的解決方案也是要在路由器和 PC 機端進行雙向連結 IP 位址與 MAC 位址來完成相應防制工作的，但在路由器端和 PC 端對 IP 位址與 MAC 位址的連結比對複雜，需要尋找每台 PC 機的 IP 位址與 MAC 加大了工作量，作業過程中還容易出錯。

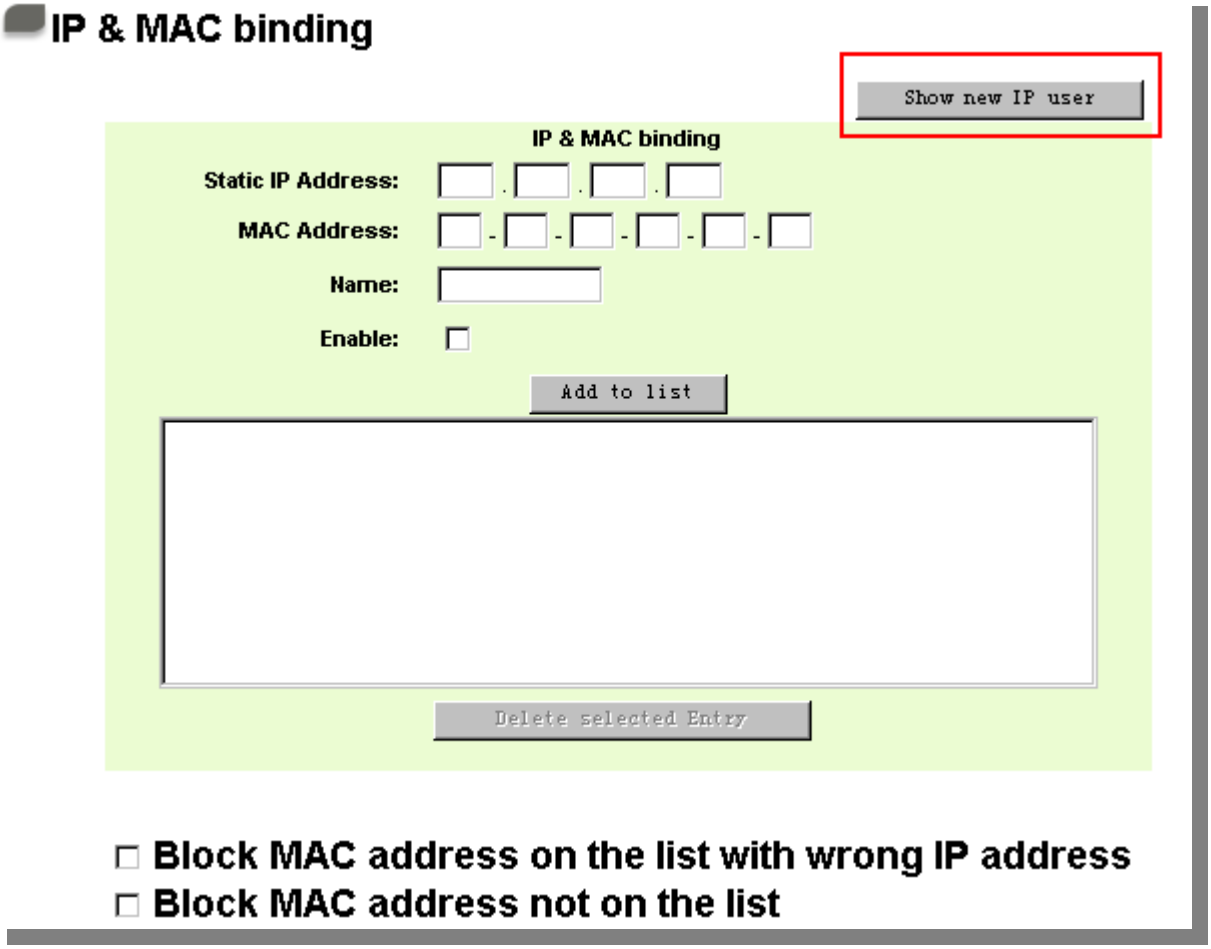
c）、在路由器端連結用戶 IP / MAC 位址：

進入"DHCP"的"DHCP Setup"，在這個頁面的右下可以看到一個"IP & MAC Binding"你可以在此添加 IP 與 MAC 連結，輸入相關參數，在"Enable"上點勾選再"Add to list"，重複作業添加內網裡的其他 IP 與 MAC 的連結，再點頁面最下的"確認"。

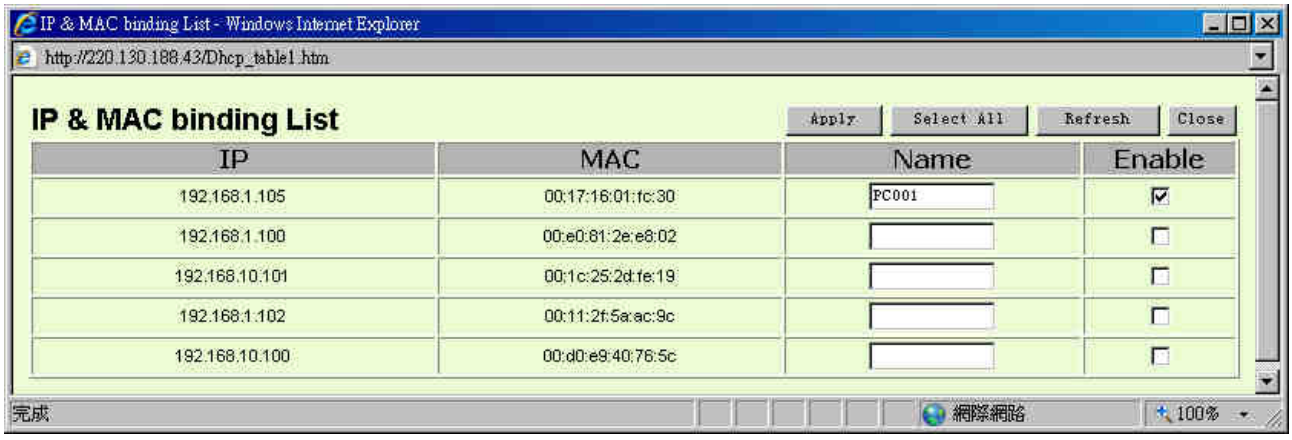


當添加了對應清單之後，其對應的資訊就會在下面的白色框裡顯示出來。不過建議不採用此方法，這樣作業需要查詢網路內所有主機 IP / MAC 位址工作量繁重，還有一種方法來連結 IP 與 MAC，作業會相對容易，可以減少大量的工作量，節約大量時間，下面就會講到。

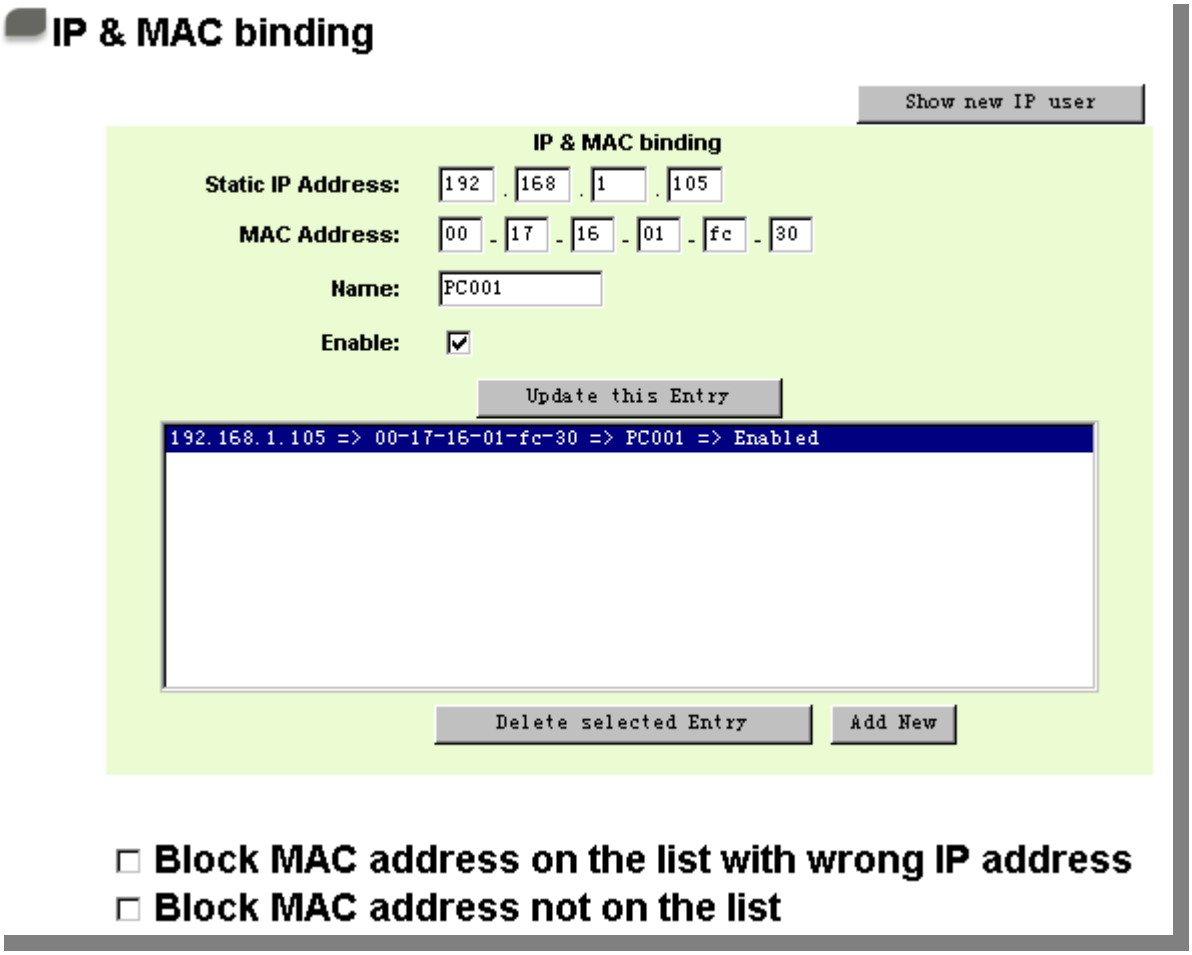
進入"DHCP 功能"的"DHCP Setup"找到 IP 與 MAC 連結右邊有一個"Show New IP User"點擊進入。



點擊之後會即現 IP 與 MAC 連結清單對話方塊，此對話方塊裡會顯示網內未做連結的 pc 的 IP 與 MAC 位址對應情況，輸入電腦"Name－名稱"和"Enable－啟動"上勾選，再在右上角點確認確定。



此時你所連結的選項就會出現在 IP 與 MAC 連結清單框裡，如下圖，在按下方確認確定連結完成。



但是我們單靠這樣的作業基本可以解決問題，但 Qno 的技術工程師建議通過進一步通過一些手段來進一步控制 ARP 的攻擊。

1、病毒源，對病毒源頭的機器進行處理，殺毒或重新裝系統。此作業比較重要，解決了 ARP 攻擊的源頭 PC 機的問題，可以保證內網免受攻擊。

2、網咖管理員檢查區域網路病毒，安裝防毒軟體，對機器進行病毒掃描。

3、給系統安裝修正程式。通過 Windows Update 安裝好系統修正程式(關鍵更新、安全更新和 Service Pack)

4、給系統管理員帳户設定足夠複雜的强密碼，最好能是 12 位以上，字母+數字+象徵式的組合；也可以禁用/移除一些不使用的帳户

5、經常更新防毒軟體（病毒程式庫），設定允許的可設定為每天定時自動更新。安裝並使用網路防火牆軟體，網路防火牆在防病毒過程中也可以起到至關重要的作用，能有效地阻擋自來網路的攻擊和病毒的入侵。部分盜版 Windows 用戶無法正常安裝修正，不妨通過使用網路防火牆等其他方法來做到一

定的防護

6、關閉一些不需要的服務，條件允許的可關閉一些没有必要的共用，也含括 C$、D$等管理共用。完全單機的用戶也可直接關閉 Server 服務

7、不要隨便點擊開啟 QQ、MSN 等聊天工具上發來的鏈結資訊，不要隨便開啟或執行陌生、可疑檔案和程式，如郵件中的陌生裝置，外掛程式等。

4）. 總結

ARP 攻擊防制是一個任重而道遠的過程，以上方法基本可以解決 ARP 病毒攻擊對網路造成相關問題，而且用戶採取類似的方法也收到了很大的效果，但還是提醒網路管理人員必須高度重視這個問題，而且無法大意馬虎，我們可以採取以上建議隨時警惕 ARP 攻擊，以減少受到的危害，提高工作效率，降低經濟損失。

附錄二：Qno 技術支援資訊

更多有關俠諾產品技術資訊可以登錄俠諾寬頻討論區，以及 FTP 伺服器的相關實例，或者聯繫俠諾各經銷商技術部門以及俠諾大陸技術中心聯絡。

俠諾科技官方網站：http://www.Qno.com.tw

台灣技術中心：

電子郵件信箱：QnoFAE@qno.com.tw