2WAN / 4LAN QoS 安全路由器

简体中文版使用手册

产品功能说明手册使用许可协议

《产品功能说明手册（以下称”手册”）使用许可协议》（以下称”协议”）是用户与侠诺科技股份有限公司（以下称”侠诺”）关于手册许可使用及相关方面的权利义务、以及免除或者限制侠诺责任的免责条款。直接或间接取得本手册档案以及享有相关服务的用户，都必须遵守此协议。

重要须知：侠诺在此提醒用户在下载、阅读手册前阅读本《协议》中各条款。请您审阅并选择接受或不接受本《协议》。除非您接受本《协议》条款，否则请您退回本手册及其相关服务。您的下载、阅读等使用行为将视为对本《协议》的接受，并同意接受本《协议》各项条款的约束。

【1】知识产权声明

手册内任何文字表述及其组合、图标、界面设计、印刷材料、或电子文件等均受我国著作权法和国际著作权条约以及其它知识产权法律法规的保护。当用户复制"手册"时，也必须复制并标示此知识产权声明。否则，侠诺视其为侵权行为，将适时予以依法追究。

【2】"手册"授权范围：

用户可以在配套使用的计算机上安装、使用、显示、阅读本"手册"。

【3】用户使用须知

用户在遵守法律及本协议的前提下可依本《协议》使用本"手册"。用户若是违反本《协议》，侠诺将中止其使用权力并立即销毁此"手册"的复本。本手册"纸质或电子档案"，仅限于为信息和非商业或个人之目的使用，并且不得在任何网络计算机上复制或公布，也不得在任何媒体上传播;及不得对任何"档案"作任何修改。为任何其它目的之使用,均被法律明确禁止,并可导致严重的民事及刑事处罚。违反者将在可能的最大程度上受到指控。

【4】法律责任与免责声明

【4-1】侠诺将全力检查文字及图片中的错误，但对于可能出现的疏漏，用户或相关人士因此而遭受的直接或间接的经济损失、数据损毁或其它连带的商业损失，侠诺及其经销商与供货商不承担任何责任。

【4-2】侠诺为了保障公司业务发展和调整的自主权，侠诺拥有随时自行修改或中断软件 / 手册授权而不需通知用户的权利，产品升级或技术规格如有变化，恕不另行通知，如有必要，修改或中断会以通告形式公布于侠诺网站的相关版块。

【4-3】所有设置参数均为范例，仅供参考，您也可以对本手册提出意见或建议，我们会参考并在下一版本作出修正。

【4-4】本手册为解说同系列产品所有的功能设置方式，产品功能会按实际机种型号不同而有部份差异，因此部分功能可能不会出现在您所购买的产品上。

【4-5】侠诺保留此手册档案内容的修改权利，并且可能不会实时更新手册内容，欲进一步了解产品相关更新讯息，请至侠诺官方网站浏览。

【4-6】侠诺（和/或）其各供货商特此声明，对所有与该信息有关的保证和条件不负任何责任，该保证和条件包括关于适销性、符合特定用途、所有权和非侵权的所有默示保证和条件。所提到的真实公司和产品的名称可能是其各自所有者的商标，侠诺（和/或）其各供货商不提供其它公司之产品或软件等。在任何情况下,在由于使用或档案上的信息所引起的或与该使用或运行有关的诉讼中, 侠诺和/或其各供货商就因丧失使用、数据或利润所

导致的任何特别的、间接的或衍生性的损失或任何种类的损失，均不负任何责任，无论该诉讼是合同之诉、疏忽或其它侵权行为之诉。

【5】其它条款

【5-1】本协议高于任何其它口头的说明或书面纪录，所定的任何条款的部分或全部无效者，不影响其它条款的效力。

【5-2】本协议的解释、效力及纠纷的解决，适用于台湾法律。若用户和侠诺之间发生任何纠纷或争议，首先应友好协商解决。若协商未果，用户在完全同意将纠纷或争议提交侠诺所在地法院管辖。中国则以「中国国际经济贸易仲裁委员会」为仲裁机构

目录大纲

一、简介 (Introduction)

2WAN / 4LAN QoS 安全路由器是专为中小型企业，网吧与小区，以及学校等单位而设计，符合经济实惠且高效能整合的全功能路由器。此路由器具备两个 WAN 端口，并具有高效能线路负载平衡模式 (Intelligent Load Balancing) 的功能，达到对外联机的流量负载平衡。WAN 端的对外联机能力满足绝大多数宽带市场都适用的规格。第二个 WAN Port 可选择性设定为硬件 DMZ (configurable hardware DMZ port)。局域网端 (LAN)内建 4 端口 10/100Mbps 以太网络交换器 (4 Port 10BasedT/TX Ethernet Switch)，每个端口都可以连接额外的交换器以连接更多的上网设备。

内建防火墙系统，以满足多数企业对防御外部网络攻击的市场需求。防火墙系统除了 NAT 之外，还具备有防止阻断服务攻击 (DoS，Denial of Service)，以及封包主动侦测检验技术(Stateful Packet Inspection)，可以预设自动侦测并阻挡外部网络攻击。功能完整的存取规则设定 (Access Rule)，可让管理者选择应该禁止或开放存取的网络服务，限制或禁止局域网内使用者的网络使用权限，以避免占用网络资源或是不当使用而遭受潜在的危机。

独特的带宽管理功能，功能强大但是设定简单，可以让管理者对有限的网络资源做合理而且有效的分配。对外不需要无限制的扩充带宽而花费过多成本，也不会因为少数几人的下载而尽占所有的带宽，造成内部上网用户的抱怨。管理者可以选择以流量控制或是优先权 (Rating & Priority)方式管理带宽，设定规则，即可达成最有效率的运用。

网络地址转换 Network Address Translation (NAT) 除了可以做私网与公网的 IP 转换，让您只需要一个公网 IP(Public IP)就可以让多人同时连上互联网。局域网内的 IP 地址支持 Class B 等级，DHCP 自动分派 IP，以及简单勾选的 IP 与 MAC 地址绑定让网络环境架构具有弹性，易于规划管理。

此外，路由器还包含虚拟服务器，一对一对应等 NAT 应用功能，可以满足在局域网架设对外服务器的需求，让网络架设更简单灵活。管理工具容易理解与设定，网络管理者可以通过 Web 浏览器轻易的做功能设定与管理。同时，通过在线多样化的日志 (SysLog) 纪录，管理者可以清楚的知道网络活动，据此拟定对 Internet 存取资源管理的明确策略，并以此来调整设定，达到网络的使用更安全且更有效率。

此说明书主要是用来说明每一个功能的设定方法与细节，若您对于路由器如何连上互联网的设定并不十分清楚，建议您先阅读「快速安装说明」，可以让您快速的将路由器连上互联网，并在必要时取得技术人员的远程支持。

您可以登陆 www.Qno.com.tw，以取得最新侠诺产品讯息及应用实例或是技术支持，更加善用您的网络。

二、硬件安装 (Hardware Installation)

本章介绍产品的硬件接口以及实体安装。

2.1 路由器板以及 LED 显示灯

LED 灯号说明

LED	颜色	意义
Power-电源	绿灯	绿灯亮： 电源开启连接
DIAG-自我测试	橘灯	橘灯亮： 系统尚未完成开机自我检测功能.
		橘灯熄灭： 系统已经正常完成开机自我检测功能.
Link/Act-联机/动作	绿灯	绿灯亮： 以太网络联机正常
		绿灯闪烁： 以太网络端口口正在传送/接收封包数据传输
Speed-速度	绿灯	绿灯亮： 以太网络联机在 100Mbps 的速度
		绿灯熄灭： 以太网络联机在 10Mbps 的速度
Connect-互联网	绿灯	绿灯亮： 广域端口已经联机并取得 IP 地址

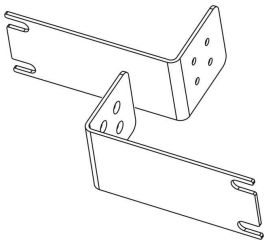
硬件回复 (Reset) 按键

Action	Description
按下 Reset 按钮 5 秒	热开机，重新启动路由器
	DIAG 灯号： 橘色灯号慢慢闪烁
按下 Reset 按钮 10 秒以上	回复原出厂默认值(Factory Default)
	DIAG 灯号： 橘色灯号快闪

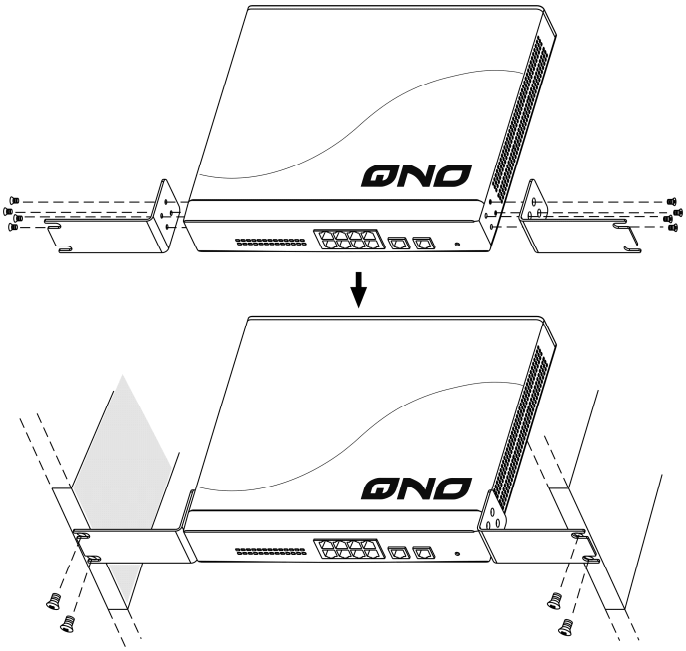
将路由器安装在 19 吋标准机架上

建议您可以将路由器放置于桌上使用，挂在墙上，或是您有机房专用 19 吋标准机架的话，可以将路由器安装于机架上，每一台路由器都有配备专用连接机架配件。当您安装路由器于机架上的时候，请注意不要将其它过重的物品堆栈或是放置于机器上，以免因重量过重无法承受而发生危险或是损伤机器本体。

每一台路由器都有配备专用连接机架配件，包含 2 只 L 型锁附架以及八颗专用螺丝，用来将路由器安装在机架上使用。路由器

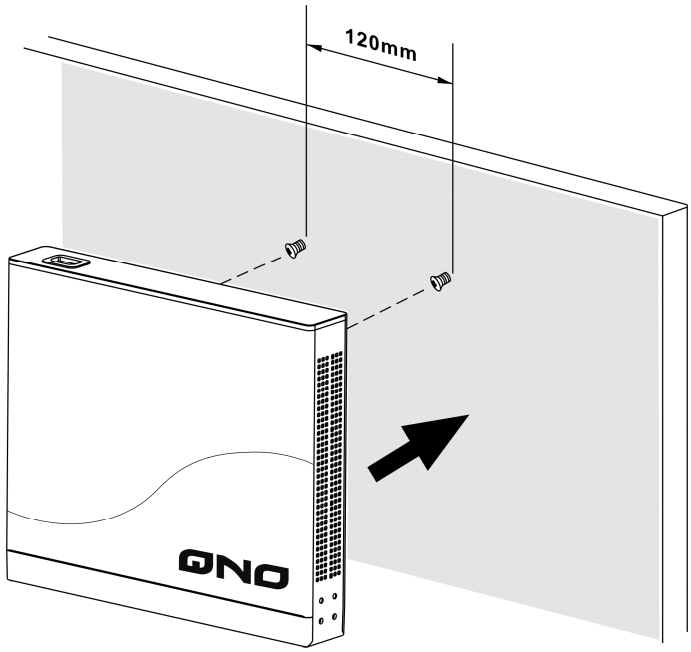


安装于您的 19 吋标准机架上的方法如下图所示：



挂在墙上的安装方法如下图所示：

于路由器机器底部有二个十字孔位，您可以使用一般螺丝先旋转锁进墙壁上，确认牢固后，再将路由器的底部二个十字孔位准确的挂在此二颗螺丝上即可完成安装。

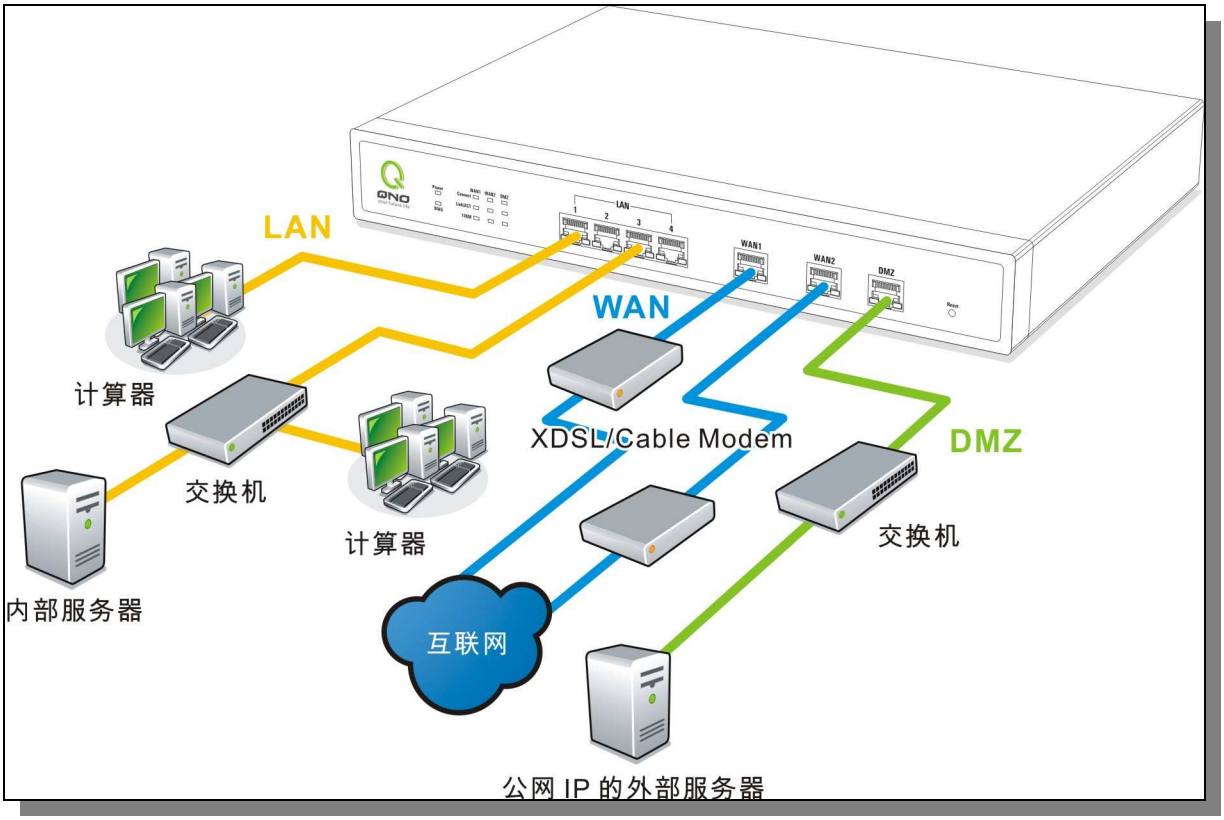


注意！

为了产品的稳定运行，无论您是如何放置路由器，请不要阻塞产品两侧通风口的任何一侧，并保持通风口有 10 厘米以上的通风空间！

2.2 连接路由器到你的网络上

路由器设计了一个可选择作为 WAN2 或是 DMZ 的广域网接口 (此功能是经由软件设定，请参考下一章节的基本设定说明)，各端口的使用拓墣范例如下图：



广域网络联机(WAN connection)： WAN 端口可以连接如 xDSL Modem，Switch HUB 或是外部路由器。

局域网络联机(LAN connection)： LAN 端口可以连接如 Switch HUB 或是直接与 PC 联机。

DMZ 埠口： 此端口口可以经由软件设定 WAN2 (第二个 WAN)或是 DMZ 端口。当设定为 DMZ 模式时(图 2)， 此端口可以连接具有外部合法 IP 位置的服务器， 如网页 (Web) 服务器以及电子邮件服务器(Mail servers)等。

三、首页与基本连网设定 (Home & Basic Configuration)

本章介绍登入软件设定画面，说明首页的显示讯息，以及基本连网设定。若是您对于路由器如何连上互联网的设定并不十分清楚，建议您进行完整的阅读，并依照步骤一步一步做设定。

3.1 登入到软件设定画面

在连接到路由器 LAN 端的计算机上开启网页浏览器 (如 IE)，在网址栏输入 192.168.1.1 (路由器的预设网关)，会出现以下的登入画面：

路由器路由器预设的使用者名称(User Name)与使用者密码(Password)皆为「admin」，您可以于稍后设定时更改此登入密码。

注意！

为了安全理由，我们强烈建议您务必在登入之后更改管理密码！密码请牢记，若是密码忘记，将无法再登入至路由器的设定画面，必须按下面板上的 Reset 按键十秒以上，回复到出厂值(Factory Default)。

3.2 首页显示 (Home)

首页 (Home)显示路由器防火墙路由器目前系统所有参数以及状态显示信息。若您想进一部查询该细部相

关设定的话，可以按下各细部选项前端(有底线的文字)的超级链接按钮，即可快速立即进入该选项设定当中。

3.2.1 系统信息

主机序列号(Serial Number)：此为显示路由器 的产品序号。

当前软件版本资讯(Firmware version)： 此为显示路由器 目前使用的软件版本。

中央处理器(CPU)：此为显示路由器 使用的 CPU。

内存(SDRAM): 此为显示路由器 使用的内存容量。

闪存(Flash): 此为显示路由器 使用的 Flash Memory 容量。

主机工作时间(System active time)：此为显示路由器 目前已经开机的时间。

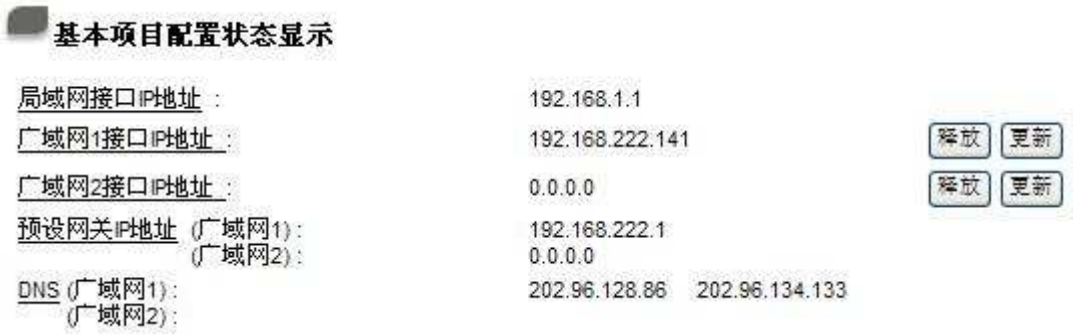
目前正确时间(Current time)：此为显示路由器 目前正确时间，但是必须注意，您需要正确设定与远程 NTP 服务器的时间同步后才会正确显示。

3.2.2 端口-Port 状态实时显示(Port Statistics)

在此画面会显示系统各端口(Port)目前实时状态显示 (联机-已经连接，启用-开启，关闭)。使用者可以按下此狀态按钮，查看各端口更详细的资料显示。

此表会显示目前该端口设定狀态如，网络連接 Link (up or down)，埠口 Port 开启 Enabled 或关闭 Disable，高低优先权 Priority (高 High or 一般 Normal)，連接速率 Speed Status(10Mbps or 100Mbps)，工作模式 DuplexStatus (半双工 half or 全双工 full)，以太网路自动侦测 Auto negotiation (Enabled or Disabled)。 于此项目表格中(statistics table)，他将会显示此端口的接收 receive/传送 transmit 的封包數以及 Byte 數/封包错误率等并计算总數量。

3.2.3 一般设定状态显示(General Setting Status)



局域网接口 IP 地址(LAN IP)：此为显示路由器路由器本身的 LAN 端目前 IP 位置，系统预设为 192.168.1.1，可以按下该超级链接直接进入该设定项目中做修改。

广域网 1 接口 IP 地址(WAN1 IP)：此为显示路由器路由器的 WAN 1 端目前的 IP 地址信息，并且可以按下该超级链接直接进入该设定项目中。当使用者选择自动取得 IP 位置时(Obtain an IP automatically)，他会显示二个按钮分别为释放（release） 与更新（renew）。使用者可以按下释放（release）按钮去做释放 ISP 端所核发的 IP 位置，以及按下更新（renew）按钮去做更新 ISP 端所核发的 IP 位置。当选择 WAN 端联机使用如 PPPoE 或是 PPTP 的话，它会变为显示连接（Connect）与中断联机（Disconnect）。

广域网 2 接口 IP 地址(WAN2/DMZ IP)：此为显示路由器的 WAN 2 端或是 DMZ 目前的 IP 地址设定信息，并且可以按下该超级链接直接进入该设定项目中。

预设网关 IP 地址(Default Gateway)： 此为显示 ISP 分配给路由器路由器 WAN1 及 WAN2 的网关 IP 地址信息，并且可以按下该超级链接直接进入该设定项目中。

名称解析服务器地址(DNS)： 此为显示路由器的 DNS(Domain Name Server)的 IP 地址信息，并且可以按下该超级链接直接进入该设定项目中。

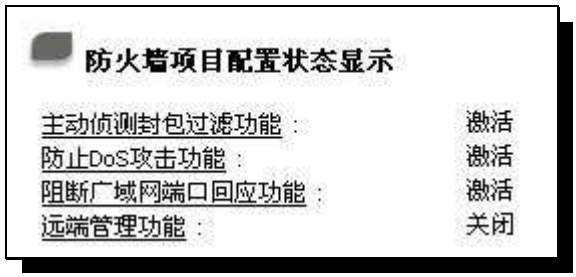
3.2.4 进阶设定状态显示(Advanced Setting Status)

DMZ 服务器地址设置： 此为显示路由器的 DMZ 功能选项是否启动，并且可以按下该超级链接直接进入该设定项目中。系统预设此功能为关闭。

路由器操作模式(Working Mode)： 此为显示路由器的目前工作模式(可为 NAT Gateway 或是 Router 路由模式)，并且可以按下该超级链接直接进入该设定项目中.系统预设此功能为 NAT Gateway 模式。

动态名称解析服务 DDNS： 此为显示路由器的 DDNS 动态 DNS 功能选项是否启动，并且可以按下该超级链接直接进入该设定项目中。系统预设此功能为关闭。

3.2.5 防火墙设定状态显示(Firewall Setting Status)



主动侦测封包过滤功能 SPI (Stateful Packet Inspection)： 此为显示路由器的 SPI(Stateful Packet Inspection)主动封包侦测过滤防火墙功能选项是否开启 (开启-On / 关闭-Off)。可以按下该超级链接直接进入该设定项目中。系统预设此功能为激活-On。

DoS 防御功能 DoS (Deny of Service)： 此为显示路由器的阻断来自 Internet 上的 DoS 攻击功能选项是否开启 (开启-On / 关闭-Off)。可以按下该超级链接直接进入该设定项目中。系统预设此功能为激活-On。

关闭广域网响应功能 Block WAN Request： 此为显示路由器的阻断来自 Internet 上的 ICMP-Ping 的响应功能选项是否开启(开启-On / 关闭-Off)。可以按下该超级链接直接进入该设定项目中。系统预设此功能为激活-On。

远程管理功能 Remote Management： 此为显示路由器的远程管理功能选项是否启动(开启-On / 关闭-Off)。可以按下该超级链接直接进入该设定项目中。系统预设此功能为关闭-Off。

3.2.6 日志记录配置状态显示(Log Setting Status)

E-Mail 的超链接将会连到系统日志设定画面中：

1.若您无设定电子邮件服务器于系统日志设定中，将显示您无设定电子邮件服务器所以无法传送系统日志电子邮件-**「邮件无法传输，因为没有配置 SMTP 服务器正确位置（E-mail cannot be sent because you have not specified an outbound SMTP server address）」。**

2.若您已经设定电子邮件服务器于系统日志设定中，但是日志尚未达到设定传输的条件时，它将显示电子邮件服务器已经设定-**「邮件设定已经配置（E-mail settings have been configured）」。**

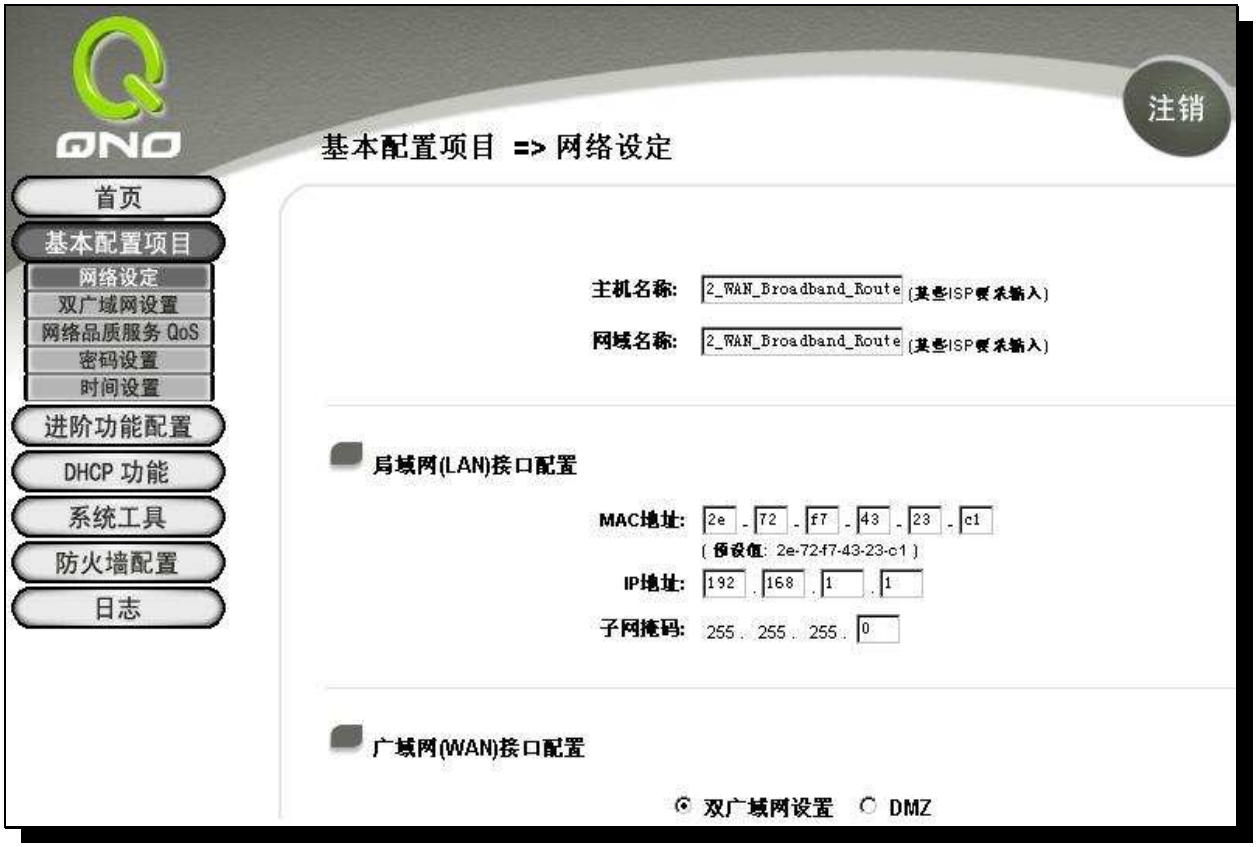
3.若您已经设定电子邮件服务器于系统日志设定中，日志也已经传输出去时，它将显示电子邮件服务器已经设定，并且已经传送-**「邮件设定已经配置并且已经传送（E-mail settings have been configured and sent out normally）」。**

4.若您已经设定电子邮件服务器于系统日志设定中，但是日志无法正确传输出去时，它将显示电子邮件服务器已经设定，但是无法传输出去，可能是设定有问题-**「邮件无法传送已经设定好邮件可能使用不正确的设定（E-mail cannot be sent out，probably use incorrect settings）」。**

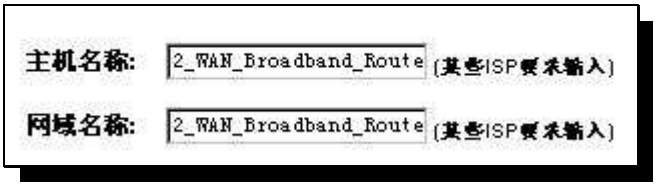
3.3 基本配置项目(General Setting)

基本配置项目(General Setting)提供路由器路由器基本的网络连接设定内容。对大多数的用户来说，完成基本的设定已经足够连接互联网。互联网的连接需要一些 ISP 所提供的进一步详细信息。其详细细部设定，请参考以下各节说明：

3.3.1 网络设定(Configure)



主机名称及网域名称： 可输入路由器的名称-Host name 以及网域名称-Domain Name，于大多数的环境中不需做任何设定即可使用，除非特殊 ISP 需求！



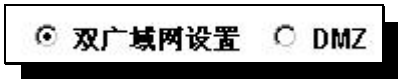
局域网设定(LAN Setting)：

此为设定路由器的 LAN 内部网络的 IP 地址，系统预设为 192.168.1.1，子网掩码为 255.255.255.0.，现在路由器可以支持到 Class C，您可以依照实际网络架构做更动！

此外，MAC 地址功能是为了方便使用者，在内网计算机设了 static ARP 之后，若换上路由器并且将局域网络(LAN) 端口的 MAC 修改成和以前的网关一樣时，就不需要个别将原本既有的计算机重新设定 Static IP，修改 static ARP 的 IP 与 MAC 对应。

第二条 WAN 及非军事区设定(Dual-WAN / DMZ Setting)

路由器提供可以选择为广域网 WAN 2 或是 DMZ 的接口。请先选择要设定为第二条 WAN 或是定义其使用模式为 DMZ 非军事管制区型态，再继续以下的设定。



非军事区(DMZ)：

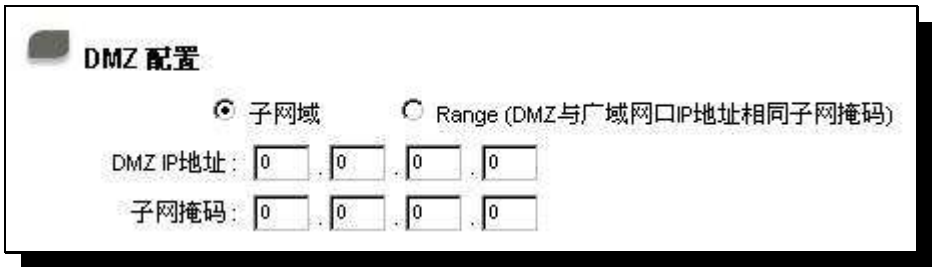
对于某些网络环境应用来说，可能会需要用到独立的 DMZ 非军事管制区接口来置放对外服务器，如 Http 网页服务器与 Mail 电子邮件服务器等等；路由器 提供一组独立的 DMZ 接口来设定连接有合法 IP 地址的

服务器，此 DMZ 接口为从 Internet 或从局域网络存取服务器内容的沟通桥梁。

此 DMZ 的设定可分为 Subnet 及 Range 两种：

Subnet：

DMZ 与广域网络 WAN 要在不同的子网络 Subnet 中，也就是若 ISP 端分配给你 16 个合法 IP 如：220.243.230.1-16 / Mask： 255.255.255.240 时，你必须将此 16 个 IP 再切两组变成 220.243.230.1-8 / Mask：255.255.255.248 及另一组 220.243.230.9-16 / Mask： 255.255.255.248，然后 Router 及 Gateway 是在同一组，再将另一组设定在 DMZ 中。



Range：

DMZ 与广域网络 WAN 位在相同的子网络 Subnet。

IP 地址范围：输入位在 DMZ 端口的 IP 范围。

设定完成请按下「确定」按钮储存网络设定变更或是按下「取消」按钮不做任何设定变更。

广域网络 Internet 联机型态设定(WAN Connection Type)：

自动取得 IP 位置(Obtain an IP automatically)：

此为路由器系统预设的联机方式，此联机方式为 DHCP 客户端自动取得 IP 模式，多为应用于如 Cable Modem 或是 DHCP 客户端 联机型态等连接，若您的联机为其它不同的方式，请选取相关的设定并依照以下的介绍做设定。

在自动取得 IP 模式，你可以使用自订 DNS 的 IP 地址(Use the Following DNS Server Address)，于此选项勾选并填入你要使用的 DNS IP 地址。

使用以下的 DNS 服务器 IP 地址： 选择使用自订的 DNS 服务器 IP 地址。

DNS 服务器： 输入您的 ISP 所提供的名称解析服务器 IP 地址，最少填入一组，最多可填二组。

共享式广域网环境： 若您的广域网线路有连接至交换机(Switch)，可以点选「是」 将此功能开启，来屏避掉不需要的广播封包，增加您网络使用的效能与安全性，默认值「否」则是将此功能关闭。

MTU： MTU 为 Maximum Transmission Unit 的缩写，一般默认值为 1500。但是在不同的网络环境中，可能会使用不同的数值，尤以 ADSL PPPoE 的状况为最多 (ADSL PPPoE MTU Size：1492)。不过许多的 Server 与 ADSL PPPoE 用户的 MTU Size 相同，一般使用预设自动（Auto）即可，不需做任何调整。

指定固定 IP 地址(Static IP)：

若您的 ISP 有核发固定的 IP 地址给您(如 1 个 IP 或是 8 个 IP 等)，请您选择此种方式联机，将 ISP 所核发的 IP 地址信息分别依照以下介绍填入相关设定参数中

注意！

有一些 ISP 虽会提供固定一个 IP 地址给您，但是有可能是使用如 DHCP 自动取得 IP 或是 PPPoE 拨接取得一个固定 IP 模式，虽是每次都取得相同 IP 地址，但联机模式您依然要选择相关之模式才可以！

广域网 IP 地址： 输入您的 ISP 所核发的可使用固定 IP 地址的其中一个。

子网掩码： 输入您的 ISP 所核发的可使用固定 IP 地址的子网掩码，如：
发放 8 个固定 IP 地址：255.255.255.248
发放 16 个固定 IP 地址：255.255.255.240

预设网关： 输入您的 ISP 所核发的可使用固定 IP 地址的预设通讯关口，若您是使用 ADSL 的话，一般说来都是 ATU-R 的 IP 地址。

DNS 服务器： 输入您的 ISP 所规定的名称解析服务器 IP 地址，最少请填入一组，最多可填二组。

共享式广域网环境： 若您的广域网线路有连接至交换机(Switch)，可以点选「是」将此功能开启，来屏避掉不需要的广播封包，增加您网络使用的效能与安全性，默认值「否」则是将此功能关闭。

MTU： MTU 为 Maximum Transmission Unit 的缩写，一般默认值为 1500。
但是在不同的网络环境中，可能会使用不同的数值，尤以 ADSL PPPoE 的状况为最多 (ADSL PPPoE MTU Size：1492)。不过许多的 Server 与 ADSL PPPoE 用户的 MTU Size 相同，一般使用预设自动（Auto）即可，不需做任何调整。

PPPoE 拨号联机(Point-to-Point Protocol over Ethernet)：

此项为 ADSL 计时制使用(适用于 ADSL PPPoE)，这里的 MTU 可单独设定 WAN1 或 WAN2。填入 ISP 给予的使用者联机名称与密码并以路由器内建的 PPP Over Ethernet 软件联机，若是您的计算机之前已经有安装由 ISP 所给予的 PPPoE 拨号软件的话，请将其移除，不需要再使用此个别连接网络。

使用者名称： 输入您的 ISP 所核发的使用者名称。

密码： 输入您的 ISP 所核发的使用密码。

闲置（）分钟自动断线： 此功能能够让您的 PPPoE 拨接连线能够使用自动拨号功能，当使用端若是有上网需求时，路由器 会自动向预设的 ISP 自动拨号联机，当网络一段时间闲置无使用时，则系统会自动离线。无封包传送的自动离线时间预设为 5 分钟，你可以自行输入所需要的自动离线等待时间。

保持联机： 此功能能够让您的 PPPoE 拨接连线能够断线自动重拨，而且可以自行设定重新拨接的时间，默认值为 30 秒。

共享式广域网环境： 若您的广域网线路有连接至交换机(Switch)，可以点选「是」将此功能开启，来屏避掉不需要的广播封包，增加您网络使用的效能与安全性，默认值「否」则是将此功能关闭。

MTU： MTU 为 Maximum Transmission Unit 的缩写，一般默认值为 1500。
但是在不同的网络环境中，可能会使用不同的数值，尤以 ADSL PPPoE 的状况为最多 (ADSL PPPoE MTU Size：1492)。不过许多的 Server 与 ADSL PPPoE 用户的 MTU Size 相同，一般使用预设自动（Auto）即可，不需做任何调整。

PPTP 拨号联机(Point-to-Point Tunneling Protocol)：

此项为 PPTP (Point to Point Tunneling Protocol)计时制使用，填入 ISP 给予的使用者联机名称与密码并以路由器内建的 PPTP 软件联机。

广域网 IP 地址： 输入您的 ISP 所核发的可使用固定 IP 地址的其中一个。

子网掩码： 输入您的 ISP 所核发的可使用固定 IP 地址的子网掩码。

预设网关： 输入您的 ISP 所核发的可使用固定 IP 地址的预设通讯闸，若您是使用 ADSL 的话，一般说来都是 ATU-R 的 IP 地址。

使用者名称： 输入您的 ISP 所核发的使用者名称。

密码： 输入您的 ISP 所核发的使用密码。

闲置（）自动断线： 此功能能够让您的 PPTP 拨接连线能够使用自动拨号功能，当使用端若是有上网需求时，路由器 会自动向预设的 ISP 自动拨号联机，当网络一段时间闲置无使用时，则系统会自动离线。无封包传送的自动离线时间预设为 5 分钟，你可以自行输入所需要的自动离线等待时间。

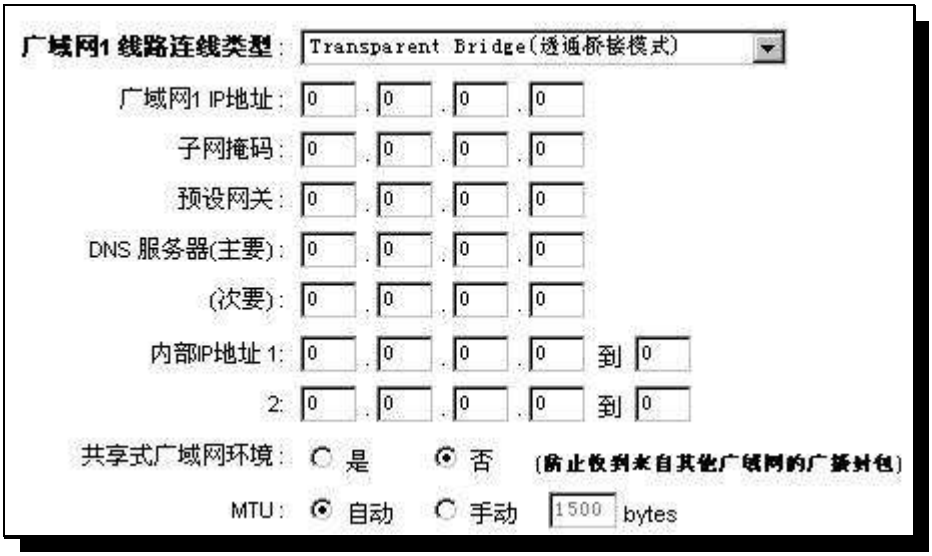
保持联机： 此功能能够让您的 PPTP 拨接连线能够断线自动重拨，而且可以自行设定重新拨接的时间，默认值为 30 秒。

共享式广域网环境： 若您的广域网线路有连接至交换机(Switch)，可以点选「是」将此功能开启，来屏避掉不需要的广播封包，增加您网络使用的效能与安全性，默认值「否」则是将此功能关闭。

MTU： MTU 为 Maximum Transmission Unit 的缩写，一般默认值为 1500。
但是在不同的网络环境中，可能会使用不同的数值，尤以 ADSL PPPoE 的状况为最多 (ADSL PPPoE MTU Size：1492)。不过许多的 Server 与 ADSL PPPoE 用户的 MTU Size 相同，一般使用预设自动（Auto）即可，不需做任何调整。

透明桥接模式(Transparent Bridge Mode)：

当您内网的计算机 IP 已经都是公网 IP 而不希望将内网都改成私网 IP(例如 192.168.1.X)时，此功能可以让您不需更动原有架构，立即整合到既有网络中。选择广域网联机方式为透明桥接模式(Transparent Bridge Mode)，这样您可以保留内网计算机的 IP 设定为原本的公网 IP 仍然可以正常上网。
当您设定两个广域网时，广域网的联机模式选择此种透明桥接模式，还可以做到负载平衡。



广域网 IP 地址： 输入您的 ISP 所核发的可使用固定 IP 地址的其中一个。

子网掩码： 输入您的 ISP 所核发的可使用固定 IP 地址的子网掩码，如：

预设网关： 输入您的 ISP 所核发的可使用固定 IP 地址的预设通讯关口，若您是使用 ADSL 的话，一般说来都是 ATU-R 的 IP 地址。

DNS 服务器： 输入您的 ISP 所规定的名称解析服务器 IP 地址，最少请填入一组，最多可填二组。

内部 IP 地址： 输入您的 ISP 所核发的可使用固定 IP 地址范围。

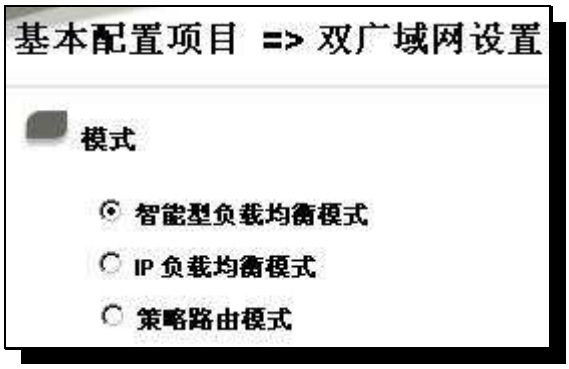
共享式广域网环境： 若您的广域网线路有连接至交换机(Switch)，可以点选「是」将此功能开启，来屏避掉不需要的广播封包，增加您网络使用的效能与安全性，默认值「否」则是将此功能关闭。

MTU： MTU 为 Maximum Transmission Unit 的缩写，一般默认值为 1500。
但是在不同的网络环境中，可能会使用不同的数值，尤以 ADSL PPPoE 的状况为最多 (ADSL PPPoE MTU Size：1492)。不过许多的 Server 与 ADSL PPPoE 用户的 MTU Size 相同，一般使用预设自动（Auto）即可，不需做任何调整。

以上设定完成请按下「确定」按钮储存网络设定变更或是按下「取消」按钮不做任何设定变更。

3.3.2 双 WAN 设定(Dual WAN)

如果你在 「基本配置项目(Configure)」中的“双广域网/DMZ 模式”选择了「双广域网」，才可以进行此选项设定。



智能负载均衡模式 (Auto Load Balance)：当您选用智能负载均衡模式，路由器将以联机数并依据您广域网线路的带宽来自动分派联机，达到联机的负载均衡。线路的带宽是依据你所填入的带宽设定(请参考下一小节设定说明)，例如当两条广域网都为上行 512Kbit/sec 时，其自动负载比例为 1:1，当一条线路的上行带宽为 1024kbit/sec 另一条为 512kbit/sec 时，则此自动负载比例为 2:1，所以为了确保你的路由器达到实际线路负载能够均衡，请填入实际上行下载带宽 (请参考下一节最小带宽设定说明)。

IP 负载均衡(IP Balance)：当您选用 IP 负载均衡模式，路由器将以联机的 IP 数并依据您广域网线路的带宽来自动分派联机，达到联机的负载均衡。线路的频宽是依据你所填入的带宽设定(请参考下一小节设定说明)，例如当两条广域网都为上行 512Kbit/sec 时，其分配 IP 联机均衡的比例为 1:1，当一条线路的上行带宽为 1024kbit/sec 另一条为 512kbit/sec 时，则此负载均衡的 IP 分配比例为 2:1，所以为了确保你的路由器达到实际线路负载能够均衡，请填入实际上行下载带宽 (请参考下一小节带宽设定说明)。

提示！

不论是智能负载均衡或是 IP 负载均衡方式，搭配「通讯协议绑定」可以有更弹性运用您的带宽，您可将特定的内网 IP，使用特定应用服务埠作访问，或特定的目的地 IP 经由您指定的广域网来访问外网。

譬如您希望指定 IP 192.168.1.100 访问外网的时后走广域网 1，或内网所有 IP 去访问服务埠 80 时都是经过广域网 2，或是内网所有 IP 去目的地 IP 211.1.1.1 访问时要从广域网 1 去访问等等，都可以经由设定此「通讯协议绑定」功能来达成你的需求。请注意，当使用智能负载均衡方式搭配「通讯协议绑定」功能时，除了您指定的服务会按照您的规则出去访问外网，其它未被指定的 IP 或服务埠的访问还是按照路由器的机

制做智能负载均衡。

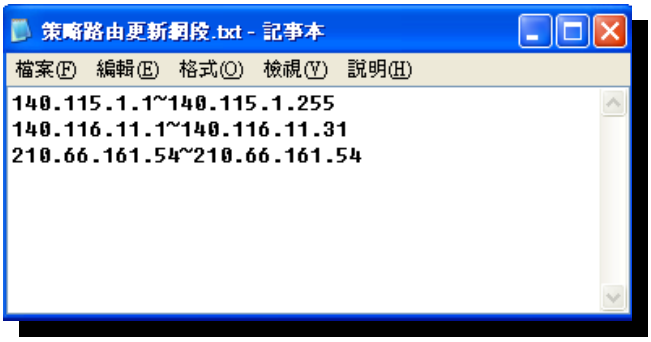
关于如何设定「通讯协议绑定」功能，以及智能负载均衡方式搭配「通讯协议绑定」的范例，请参考 3.3.3 节的 通讯协议绑定 设定说明。

策略路由(Strategic Routing)：当您选用策略路由模式，路由器会依照内建的策略(电信网通分流，用在中国大陆的环境)自动分派联机。您只需选择网通线路接入的广域网口，路由器会自动将该走网通线路去外网访问的流量都从网通的广域网出去，对该走电信线路去外网访问的流量也都会往电信的广域网出去，达到「电信走电信，网通走网通」的分流策略。

此外，您也可以自己建立分流策略。在「自订策略」中选择要指定的广域网口(例如广域网 1)，然后按下「更新网段」的按键，会出现汇入策略文件的对话窗口。策略文件是一个可编辑的文字文件，应含有您指定的目的 IP 地址。将文件汇入路径选择好之后，按下「汇入」，并在设定画面的最下方按下「确定」，路由器就会将要往指定目的 IP 的流量从您指定的广域网 (例如广域网 1) 出去。

策略文件的建立可以用纯文字编辑软件来撰写，例如使用 (Windows)系统内建的「记事本」来建立。将您要指定的目的IP地址依下图的格式写入，例如您要指定的目的IP地址范围是从140.115.1.1到140.115.1.255，

则在「记事本」中输入 140.115.1.1~140.115.1.255。下一个目的 IP 地址范围则要换行输入。请注意！若是只有一个目的 IP 地址，也需要以同样的格式来书写。例如指定的目的 IP 地址是 210.66.161.54，则必须写成 210.66.161.54~210.66.161.54。储存档案之后(扩展名应该是.txt)即可汇入自订策略的更新网段。



提示！

网通策略与自订策略不能同时存在。在任一个策略选项中指定广域网，另一个策略就会显示为关闭。

网络对外联机侦测(Network Service Detection)

激活线路侦测机制： 网络对外服务侦测机制。若勾选此项设定，则会出现 Retry Count， Retry Timeout 等以下的讯息。当使用两条广域网做对外连结线路时一定将此 NSD 启用，以避免因为广域埠流量过大时造成路由器的误判将此线路判断为断线。

重新尝试联机次数： 对外联机侦测重试次数，默认值为五次。若是于此设定次数当中，Internet 没

有回应的话，就判断为对外线路中断！

响应延迟时间： 对外联机侦测逾时时间(秒)，默认值为 30.秒。于此设定秒数之后重新测试对外联机。

当重新联机失败时： **(1)储存纪录到日志（Generate the Error Condition in the System Log）：**在系统日志中会产生错误讯息的信息：当侦测到与 ISP 连结失败时，系统就会在系统日志中将这项错误讯息纪录下来，但依旧保持此线路不会移除，所以会有些原来使用此条线路上的 User 无法正常使用。

此选项适用在当某条广域网联机失败时，从这个广域网去访问的目的地地址是无法从另一条线路去访问的时候，就可以用此选项。例如若是要访问 10.0.0.1 到 10.254.254.254 时一定要走广域网 1 去访问，而且广域网 2 是无法访问到此网段，那就可以使用此选项。因为若广域网 1 掉线后走广域网 2 也无法去访问到 10.0.0.1 到 10.254.254.254，就不需要在广域网 1 断线时将此线路移除。

(2)移除该条线路（Remove the Connection）：当侦测到与 ISP 连结失败时，系统不会在系统日志中将这项错误讯息纪录下来，原本使用此 WAN 端的封包传递会自动转换到另一条广域埠.等到原本断线的广域端口恢复后会自行重新连结，则封包传递会自动转换回来。

此此选项适用在若某条广域网联机失败时，从这个广域网去访问的目的地位置是可以从另一条线路去访问的时候，就要用此选项。如此可以让任何一条广域网断线的时候，另一条可以做备援，将流量转移到还在联机的广域网。

侦测以下可回应的服务器：

预设网关： 近端的预设通讯网关位置，如 ADSL 路由器的 IP 位置，此为 Router 自动填入，所以只须打勾选择是否启用。注意！有部分的 ADSL 线路的网关是不会响应侦测封包，或是当您是使用光纤盒，或是运营商发给您的是固定的公网 IP 且网关就是在您网咖这端而不是在运营商那端时，此选项不要启动。

ISP 服务器： ISP 端的侦测位置，如 ISP 的 DNS 服务器 IP 位置等。在设定此 IP 地址时请确认此 IP 地址是可以且稳定快速的得到响应 (建议填入 ISP 端 DNS IP)。

远程服务器： 远程的网络节点侦测位置，此 Remote Host IP 地址最好也是可以且稳定快速的得到响应(建议填入 ISP 端 DNS IP)。

DNS 服务器： 网域名称端 DNS 的侦测位置(此字段只许填入网址如「www.hinet.net」，请勿填 IP 地址)。另外，两条 WAN 的此字段不可以填入相同的网址。

确定： 按下此按钮「确定」即会储存刚才所变动的修改设定内容参数。

取消： 按下此按钮「取消」即会清除刚才所变动的修改设定内容参数，但是必须于确定 储存动作之前才会有效。

频宽设定(Bandwidth)

路由器路由器会依照你实际输入的上传频宽数据做为两条广域端口自动负载平衡的比例依据。例如当两条广域网都为上传 512Kbit/sec 时，其自动负载比例为 1：1。当一条线路的上传频宽为 1024kbit/sec 另一条为 512kbit/sec 时，则此自动负载比例为 2：1。所以为了确保你的路由器达到实际线路负载能够均衡，请填入实际上下载频宽。另外，此字段也关系到 QoS 的设定，请参考 QoS 设定。

3.3.3 通讯协议绑定(Protocol Binding)

使用者可将特定的 IP 或特定的应用服务埠(Service port)经由您限定的 WAN 出去。其它没有做绑定的 IP 或 Service 还是会进行广域网的负载平衡。

服务端口： 在此选择欲开启的绑定服务埠(Service Port)，从下拉式选单中可以选择预设列表(如 All -TCP&UDP 0~65535，WWW 为 80~80，FTP 为 21~21 等等)，预设的 Service 为 All 0~65535。

Service Management (服务选单列表)：按下此按钮可以进入服务端口(Service Port)设定画面，进行新增或删除选单中预设的服务埠(Service Port)。

来源 IP 地址： 使用者可以指定特定的内部虚拟 IP 地址的封包经由特定的广域埠出去。在此填上内部虚拟 IP 地址范围，例如 192.168.1.100 到 150.则 IP 地址 100 到 150 为绑定范围。如果使用者只需要设定特定的服务埠(Service Port)而不需指定特定的 IP 地址， 则在 IP 的字段皆填入 0。

目的 IP 地址： 在此填上外部固定 IP 地址，例如若有一目标地址 210.11.1.1，要连接此地址的使用者限定只能从广域端口 1 到达此目标地址，则在此填上外部固定 IP 地址 210.11.1.1 到 210.11.1.1。如果使用者要设定一个范围的目的地位置，则填入方式可以为 210.11.1.1 到 210.11.255.254，则表示整组 210.11.x.x 的 Class B 网段都限制走某一条广域网，若只需要设定特定的应用而不需指定特定的 IP 地址，则在 IP 的字段皆填入 0.0.0.0。

接口位置： 选择你所要绑定此条规则在哪一个 WAN Port。

启用： 启用此规则。

加入到对应列表： 增加此条规则到列表。

删除所选的项目： 删除在服务列表里所选择的规则。

确定： 按下此按钮「确定」即会储存刚才所变动的修改设定内容参数。

取消： 按下此按钮「取消」即会清除刚才所变动的修改设定内容参数，但是必须于确定 储存动作之前才会有效。

注意！

通讯绑定协议所设的规则在路由器执行时也有优先级的，在列表上最上方那条会先执行,然后依序往下。

新增或删除管理服务埠号

若您欲开启的 Service Port 项目没有在表列中，您可以按下「服务端口管理表」新增或删除管理服务端口号列表功能达成，如以下所述：

服务端口名称： 在此自订欲开启的服务端号名称加入列表中，如 BT 等。

通讯协议： 在此选择欲开启的服务端口号的封包格式为 TCP 或 UDP。

服务端口范围： 将你所需新增加的服务端口范围填入。

加入到对应列表： 增加到开启服务项目内容列表，最多可新增 100 组。

删除所选择的项目： 删除所选择的开启服务项目之一笔内容。

确定： 按下此按钮「确定」即会储存刚才所变动的修改设定内容参数。

取消： 按下此按钮「取消」即会清除刚才所变动的修改设定内容参数，但是必须于确定 储存动作之前才会有效。

关闭： 离开此功能设定画面。

使用智能负载均衡模式时其通讯协议绑定协议设定方式：

智能负载均衡方式搭配「通讯协议绑定」可以有更弹性运用您的频宽，您可将特定的内网 IP，使用特定应用服务端口作访问，或特定的目的地 IP 经由您指定的广域网来访问外网。

范例一、若要指定内网 IP 192.168.1.100 去外网访问都走广域网 2，那通讯协议绑定设定方式?

如以下范例所示，服务端选择「All Traffic」，在来源 IP 地址填入 192.168.1.100 到 100，目的 IP 地址保留原本的数值 0.0.0.0 (表示所有的外网地址)。接口位置选则广域网 2，然后勾选启动。最后点击「新增」即可将此规则加入。

范例二、若要指定内网 IP192.168.1.150 到 200 去外网访问 80 端口都走只能走广域网 2 去访问,那通讯协议绑定设定方式?

如以下范例所示，服务端选择「HTTP[TCP/80~80]」，在来源 IP 地址填入 192.168.1.150 到 200，目的 IP 地址保留原本的数值 0.0.0.0 (表示所有的外网地址)。接口位置选则广域网 2，然后勾选启动。最后点击「新增」即可将此规则加入。

范例三：若要指定内网所有 IP 去外网访问 80 断口都走只能走广域网 2，但其余服务都走广域网 1 时，通讯协议绑定设定方式?

如以下范例所示，要设置两条规则，第一条规则服务端选择「HTTP[TCP/80~80]」，在来源 IP 地址填入 192.168.1.0 到 0(表示所有的内网地址)，目的 IP 地址保留原本的数值 0.0.0.0 (表示所有的外网地址)。接口位置选则广域网 2，然后勾选启动。最后点击「新增」即可将此规则加入。路由器会将所有用 80 埠去外网访问的流量都走广域网 2，但是不是用 80 埠的流量根据路由器的自动负载平衡演算，还是有可能会走广域网

2，因此还需要再设第二条规则，服务端选择「All Traffice [TCP&UDP/1~65535]」，在来源 IP 地址填入 192.168.1.2 到 254，目的 IP 地址保留原本的数值 0.0.0.0 (表示所有的外网地址)。接口位置选则广域网 1，然后勾选启动。最后点击「新增」即可将此规则加入。这时路由器会将不是用 80 端口去外网访问的流量都走广域网 1。

3.3.4 联机数管控(Session Limit)

联机数管控可以控制内网的计算器最多能同时建立的联机数。这个功能对网管人员在控制内网使用 P2P 软件如 BT、迅雷、emule 等会造成大量发出联机数 session 的软件提供了非常有效的管理。设置恰当的容许联机数可以有效控制 P2P 软件时所能产生的联机数，相对也使带宽使用量达到一定的限制作用。

另外，若计算机中了类似冲击波的病毒而产生大量对外发联机请求时，也可以达到抑制作用。

关闭： 不使用此联机数管控功能。

每一个 IP 对外联机数最多不可超过： 此选项为限制每一台内网的计算机最大可建立的对外联机数，当用户计算机使用联机数到达此限制值时，要建立新的联机必须等到之前的联机结束后才能再建立。例如，当用户使用 BT 或 P2P 等下载时且联机数超过此设定值后，当用户又要再开其它服务时会无法使用，除非将使用中的 BT 或 P2P 软件关闭。

若有 IP 对外联机数到达：

阻挡此 IP 建立新联机达 5 **分钟：** 此选项为当客户端计算机使用的联机数到达您的设定数值时，此用户在 5 分钟之内将不能再增加新联机，就算旧联机已经结束，也必须等到设定时间过后才能再建立新的联机。

封锁此 IP 所有联机达 5 **分钟：** 此选项为当客户端计算机使用的联机数到达您的设定数值时，此用户正在使用的所有联机都将被清除，且在 5 分钟之内将不能建立任何联机(不能上网)，必须等到设定时间过后才能再建立新的联机。

3.3.5 带宽管理(QoS)

带宽管理 QoS 为 Quality of Service 缩写，其功能主要为限制某些服务及 IP 的带宽使用量，以满足特定应用程序或服务所需要的带宽或优先权，并让其余的使用者共享带宽，才能有比较稳定、可靠的数据传送服务。网络管理人员应该针对公司、小区、或是网吧的实际需求，对各种不同网络环境、应用程序或服务来进行带宽管理，才能充分且有效率的达到网络带宽使用。

带宽设定

WAN1 及 WAN2 的带宽数据请填入您所申请的宽带网络实际上传及下载带宽，QoS 的带宽控制会依照您所填入的带宽作为计算依据。例如说每个 IP 及 Service Port 可以保障使用的上传或下载的最小带宽会依照此 WAN1 及 WAN2 的实际带宽相加来换算实际可保障的大小。例如上传带宽若两条都为 512Kbit/Sec，那实际上传带宽就为 WAN1+WAN2=1024Kbit/Sec，所以若有 50 个 IP 在内部网络，若要保证每人最小可使用的上传带宽，则就把 1024Kbit/50=20Kbit，这样每人可以保证的 Mini.Rate 就可以填 20kbit/Sec，下载同此换算方式。

注意！

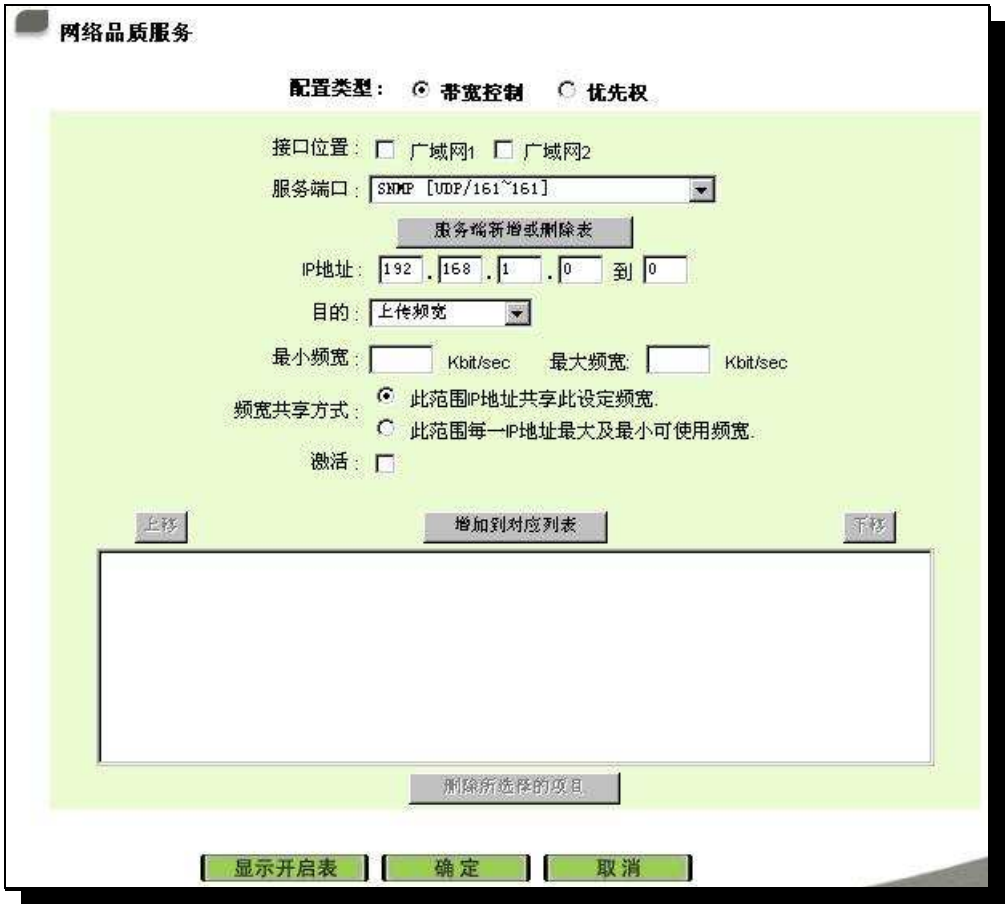
这里的数值单位是 kbit，有些应用软件显示下载/上传速度单位为 KB，两个数值之间的换算方式为 1KB=8kbit。

QoS 设定

QoS 可以选择两种方式，无法同时使用，一为流量控制(Rate Control)，另一个为优先权控制(Priority Control)，设定人员可以依照自己内网需求做两种模式灵活运用。

带宽控制 (Rate Control) – 按使用量做管理：

网管人员可以按照您现有的带宽大小做每一个 IP 或一组 Range 做使用量限制或保障带宽。另外也可以针对服务端口(Service Port)去做带宽控制。若是内部有架设服务器的话，也可控制或保障其对外带宽。



接口位置： 勾选此条 QoS 设定要控制在哪条 WAN 执行，可单独或全部勾选。

服务端口： 选择此条 QoS 所要设定的带宽控制为何，若您是要针对每个 IP 的所有服务的使用带宽，则将此选择在 All Traffic(TCP&UDP)1~65535。若您只要针对譬如 FTP 上传或下载，其余服务不限制，则选择 FTP Port21~21，可参考服务号码预设列表。

IP 地址： 此为选择你所要限制的使用者为何?若您只限制单一 IP，则直接将此 IP 填入，如：192.168.1.100 到 100，则此规则就是针对 192.168.1.100 此 IP 做控制。若是要限制一组 IP 范围，则填入如 192.168.1.100 到 150，这样此规则就是针对 192.168.1.100 到 150 做限制。若是此条频宽限制是针对所有人也就是接在路由器内网的所有 User 则可在 IP 的字段皆填入 0，也就是 192.168.1.0 到 0，这样就表示所有 IP 都受此规则限制。另外此 QoS 是可以控制到 Class B 的范围。

目的： 上传(Upstream)： 指对内网 IP 的上传带宽 下

下载(Downstream)：指对内网 IP 的下载带宽

虚拟服务器上传(Server in LAN，Upstream)：若你有架设对外的 Server 网站在路由器内部，则此选项为控制外部访问此服务器的带宽控制.

虚拟服务器下载(Server in LAN，Downstream)：若你有架设网站在路由器内网，则此选项为控制外部对此服务器上传数据时的频宽控制，例如网吧很多都有架设游戏服务器，若外部要来做数据升级更新时，可以用此控制做带宽管理，才不会影响内部使用者上网玩游戏。

保证频宽 & 最大可用频宽 (Kbit/Sec)：

保证频宽：此为限制或保证此条规则的最小可使用带宽。

最大可用频宽：此为限制此条规则的最大可使用带宽，也就是最大不会超过此设定值。

请注意！这里填入的数值单位是 kbit，有些应用软件显示下载/上传速度单位为 KB，两个数值之间的换算方式为 1KB=8kbit。

频宽共享方式：

此范围 IP 地址共享此设定频宽(Share total bandwidth with all IP addresses)：

若选择此规则的话，其表示所有 IP 或此 Service Port 共享这段(Mini 到 Max.Rtae)带宽范围。

此范围每一 IP 地址皆套用此设定频宽(Assign bandwidth for each IP address)：

若选择此规则的话，其表示每一个 IP 或这一段 Service Port 都可以有此 (保证频宽到最大可用带宽) 频宽范围，例如若是针对每台计算机 (IP 地址) 做的规则设定，则每台计算机(IP 地址)都可以有这么大的带宽。

请注意！当您选择带宽的共享方式时，要留意实际应用的情况，以避免选择不恰当的方式而造成带宽太小无法正常使用网络。例如，内网多人使用 FTP 做档下载，若是您希望 FTP 不会占用掉大部分的带宽，您就可以选择共享带宽，不论内网有多少人使用 FTP 做档下载，总和所占用的带宽是固定的。

激活： 启用此规则。

加入到对应列表： 增加此条规则到列表。

上移 &下移： 由于 QoS 的每条规则执行的优先级为由列表的最下面那条往上执行，也就是越后面设定的规则会优先执行，所以你可以自行调整每条规则先后执行顺序。通常将要限制带宽的 Service Port 移至最下方如 BT，e-mule 等..，然后将针对限制 IP 带宽的规则往上移。

删除所选择的项目： 删除在服务列表里所选择的项目内容。

显示开启表： 可以显示出您所有在 Rate Control 设定的规则，并可直接按下「Edit」做修改。

确定： 按下此按钮「确定」即会储存刚才所变动的修改设定内容参数。

取消： 按下此按钮「取消」即会清除刚才所变动的修改设定内容参数，但是必须于确定 储存动作之前才会有效。

范例一：若希望内网去做 ftp 下载都只能共同使用 50kbit 下载频宽要如何设定?

如以下范例所示设置规则，接口位置勾选广域网 1 以及广域网 2，服务端口选择「 FTP[TCP /21~21」，在

IP 地址填入 0.0.0.0 到 0(表示所有的地址)，目的选择下载。最小带宽填入 2 kbit/sec，表示 FTP 下载保证有 2kbit/sec 的带宽。最大带宽填入 50kbit/sec，表示 FTP 下载最多只能使用到 50kbit/sec 的带宽。带宽共享方式选择「此 IP 地址共享此设定带宽」，如此不论内网有多少人使用 FTP，所有 FTP 下载的带宽总和最多只能使用 50kbit/sec。勾选启动，最后点击「新增」即可将此规则加入。

范例二：若希望内网所有 IP 每人最大下载使用频宽只能有 512Kbit，需要一个 IP 一个 IP 设定吗?

如以下范例所示设置规则，接口位置勾选广域网 1 以及广域网 2，服务端口选择「Not Check Port [TCP&UDP /0~0] 」，在 IP 地址填入 192.168.1.2 到 254(要作限制的地址范围)，目的选择下载。最小带宽填入 2 kbit/sec，表示每个 IP 保证有 2kbit/sec 的带宽。最大带宽填入 512kbit/sec，表示每个 IP 最多只能使用到 50kbit/sec 的

带宽。带宽共享方式选择「此范围每一 IP 地址最大及最小可用带宽」，如此每一个 IP 最小一定有 2kbit/sec 的保证。勾选启动，最后点击「新增」即可将此规则加入。

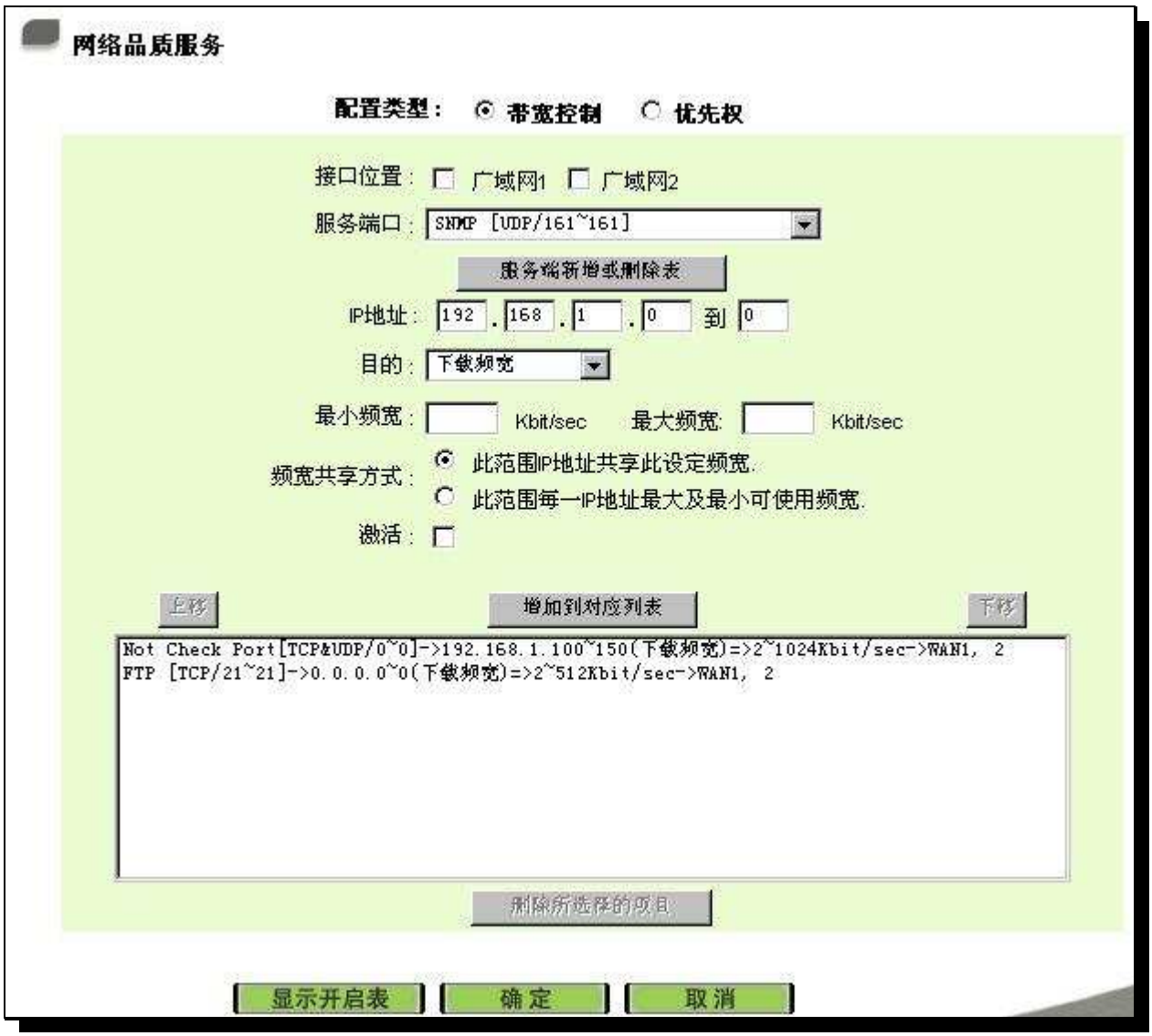
范例三：若希望内网所有 IP192.168.1.100-150 每人最大下载使用频宽只能有 1M，但当使用 ftp 下载时都只能共享 512Kbit 时要如何设定?

如以下范例所示设置两条规则，第一条规则接口位置勾选广域网 1 以及广域网 2，服务端口选择「Not Check Port [TCP&UDP /0~0]」，在 IP 地址填入 192.168.1.100 到 150(要作限制的地址范围)，目的选择下载。最小带宽填入 2 kbit/sec，表示每个 IP 保证有 2kbit/sec 的带宽。最大带宽填入 1024kbit/sec，表示每个 IP 最多只能使用到 1M/sec 的频宽。带宽共享方式选择「此范围每一 IP 地址最大及最小可用带宽」，如此每一个 IP 最

小一定有 2kbit/sec 的保证。勾选启动，最后点击「新增」即可将此规则加入。

第二条规则接口位置勾选广域网 1 以及广域网 2，服务端口选择「FTP[TCP /21~21」，在 IP 地址填入 0.0.0.0 到 0(表示所有的地址)，目的选择下载。最小带宽填入 2 kbit/sec，表示 FTP 下载保证有 2kbit/sec 的带宽。最大带宽填入 512kbit/sec，表示 FTP 下载最多只能使用到 512kbit/sec 的带宽。带宽共享方式选择「此 IP 地址共享此设定带宽」，如此不论内网有多少人使用 FTP，所有 FTP 下载的带宽总和最多只能使用 50kbit/sec。勾选启动，最后点击「新增」即可将此规则加入。

请注意！QoS 带宽管理的执行顺序为由列表最下面那一条往上做执行动作，所以要将先执行的规则往最下面移。以这个范例来说，先执行 FTP 的共享带宽，在执行每个 IP 的保证以及最大可用带宽。因此若是内网有人使用 FTP 下载，就会先受到第一条规则的限制，最大只能用到 512kbit/sec。若是将规则反过来，将上述的第一条规则移到最下方来先执行，则每个 IP 最大可用到 1M 的带宽，此时用 FTP 下载也就可以用到 1M 的频宽，那么后执行的 FTP 频宽限制在 512kbit 就不会执行，也就没有意义了！



优先权 (Priority Control) - 依优先级做管理：

优先级顾名思义就是可以将你选定想要的服务做先后顺序的调配，也就是可以直接选择 Service Port 将其优先级做一分配。

路由器会将频宽做 60%(最高)、10%(最低)的带宽分配，也就是若您将 Port 80 选择为高，那么路由器只要遇到 Port 80 的封包就会给予 60%的带宽出去，若您将 FTP Port 21 设定为低，那当有人使用 Port 21 时，路由器只会给它 10%的带宽使用，其余未做分配的服务就使用 30%带宽。

接口位置： 勾选此条 Priority 优先权的设定要控制在哪条 WAN 执行。

服务端： 在此选择此条优先权所要设定的 Service Port 为何，要针对譬如 FTP 上传或下载，则选择 FTP Port21~21，可参考服务号码预设列表。

目的： 上传(Upstream)： 指对内网 IP 的上传频带宽

下载(Downstream)：指对内网 IP 的下载带宽

虚拟服务器上传(Server in LAN，Upstream)：若你有架设对外的网站服务器在路由器内部，则此选项为控制外部访问此服务器的带宽控制

虚拟服务器下载(Server in LAN，Downstream)：若你有架设网站在路由器内网，则此选项为控制外部对此服务器上传数据时的频宽控制，例如网吧很多都有架设游戏服务器，若外部要来做此游戏服务器做数据 Update 时，可以用此控制做带宽管理，才不会影响内部使用者上网玩游戏。

优先权： 高： 此为保证 60%的带宽给此服务端口使用。

低： 此为只给 10%的带宽给此服务端口使用。

启动： 启用此规则。

加入到对应列表： 增加此条规则到列表。

删除所选的项目： 删除所选择在服务列表里的项目内容。

显示开启表： 可以显示出您所有在 Priority 设定的规则，并可直接按下「Edit」做修改。

确定： 按下此按钮「确定」即会储存刚才所变动的修改设定内容参数。

取消： 按下此按钮「取消」即会清除刚才所变动的修改设定内容参数，但是必须于确定储存动作之前才会有效。

3.3.6 密码设定(Password)

当您每次登入至路由器的设定画面时，必须输入密码。路由器的密码出厂值为「admin」。为了安全理由，我们强烈建议您务必在第一次登入并完成设定之后更改管理密码！密码请牢记，若是密码忘记，将无法再登入至路由器的设定画面，必须回复到出厂值(Factory Default)。

使用者名称： 预设为 admin 。

密码： 填写原本旧密码。

输入新的使用者名称： 输入使用者要建立的新用户的名称。

输入新密码： 填写所更改密码。

再次输入新密码： 再填写确认一次更改密码。

确定： 按下此按钮「确定」即会储存刚才所变动的修改设定内容参数。

取消： 按下此按钮「取消」即会清除刚才所变动的修改设定内容参数，但是必须于确定 储存动作之前才会有效。

3.3.7 系统时间设定(Time)

路由器 可以设定时间，让您在看路由器的系统纪录或是设置网络存取的时间设定时，可以了解事件发生的正确时间，以及作为关闭存取或是开放存取 Internet 资源的依据条件。您可以选择与路由器内建的外部时间服务器(NTP Server)取得时间同步，或是自己设定正确时间参数。

设定与外部时间服务器 NTP 同步 (Set the local time using Network Time protocol (NTP) automatically)：

路由器 有内建的网络时间服务器，会自动同步时间。

请于时区选取选项选取您所在区域的时间参数以及日照时间，若是您所在的地区有实施日光节约时间，您可以输入实施的日期范围，路由器会在此日期范围自动调整时间。若是您有专属使用的时间服务器地址的话，您可以输入此时间同步服务器（NTP）的 IP 地址。

设定修改完成请按下「确定」按钮储存网络设定变更或是按下「取消」按钮不做任何设定变更。

手动设定时间 (Manual)：

于此输入正确的小时(Hours)， 分钟(Minutes)， 秒(Seconds)， 月份(Month)， 日(Day) 与年(Year)。

设定完成请按下「确定」按钮储存网络设定变更。若是不想进行变更，请在按下「确定」储存动作之前按下 「取消」按钮，将不做任何设定变更。

四、进阶功能设定 (Advanced Configuration)

本章介绍路由器进阶功能的设定，包括开启虚拟服务器的连接，路由设定，实体 IP 与虚拟 IP 对应，以及设置动态域名解析等功能。

4.1 DMZ Host-(Demilitarized Zone)

当您将路由器内部的某台 PC 的虚拟 IP 填入到此 DMZ 选项时，路由器 WAN1 及 WAN2 的合法 IP 地址会直接对应给此台 PC 使用，也就是说从 WAN 端进来的封包，若是不属于内部的任何一台 PC，都会传送到这台 PC 上。

于使用「DMZ Host」功能后，若您要取消此功能必须于在设定虚拟 IP 地址地方填入「0」的参数，才会停止此功能使用。

按下此按钮「确定」即会储存刚才所变动的修改设定内容参数. 按下「取消」即会清除刚才所变动的修改设定内容参数，但是必须在「确定」储存动作之前才会有效。

4.2 虚拟服务器设定(Forwarding)

若是您在内网需架设服务器（意指对外部的服务主机 WEB， FTP， Mail 等），这个功能可将虚拟服务器主机视为一虚拟的位置，利用路由器的外部合法 IP 地址，经过服务端口 Service Port 的转换，（如 WWW 为 port 80），直接存取到内部虚拟 IP 的服务器的服务。例如在设定画面中，选项填入服务器位置，如 192.168.1.2 且 port 是 80 的话，当 Internet 外部要进来存取这个网页时只要键入：

http：//220.130.188.45 (假设此为路由器的外部合法 IP 地址)
此时，就会通过路由器的 Public IP 位置去转换到 192.168.1.2 的虚拟主机上的 Port 80 读取网页了。

其它种类的服务器设定，都如以上设定；只要将所用的 Server 的 Service Port 以及虚拟主机的 IP 位置填入即可！

服务端口号： 在此选择欲开启的虚拟服务器的服务埠号。码预设列表，如 WWW 为 80(80~80)， FTP 为 21~21，可参考服务号码预设列表！

IP 地址： 在此填上虚拟服务器所要相对应的内部虚拟 IP 位置，如 192.168.1.100。

激活： 开启此服务功能。

服务端口管理表： 若您所需要的服务埠没有在列表里面，可以利用此功能新增或删除管理服务埠号列表。

增加对应列表： 增加到开启服务项目内容。

删除所选泽的项目： 删除所选择在服务列表里的项目内容。

特殊应用软件配置 (Port Triggering)：

有一些特殊应用软件其进出 Internet 的服务端口号(Port Number)为非对称的，此时您必须使用此功能选项将一些特殊应用程序使用的服务端口号填入相关设定中，如以下画面所示：

特殊应用程序名称： 您可以自订此特殊应用软件名称，方便管理使用！

出去服务位置范围： 输入由路由器出 Internet 的使用端口(Port Number)编号(如 9000~10000)。

进入服务位置范围： 输入由 Internet 进入的使用端口(Port Number)编号. (如 2004~2005) 。

加入到对应列表： 增加到开启服务项目内容列表。

删除所选择的项目： 删除所选择的开启服务项目之一笔内容。

显示开启表： 按下此按钮即会显示 Table 上的所有设定项目内容参数。

确定： 按下此按钮「确定」即会储存刚才所变动的修改设定内容参数。

取消： 按下此按钮「取消」即会清除刚才所变动的修改设定内容参数，但是必须于确定 储存动作之前才会有效。

以下为一些常用的端号需设定到此功能项目中的清单：

Application	Outgoing Control	Incoming Data
Battle.net	6112	6112
DialPad	7175	51200，51201，51210
ICU II	2019	2000-2038，2050-2051 2069，2085，3010-3030
MSN Gaming Zone	47624	2300-2400，28800-29000

4.3 UPnP- Universal Plug and Play

UPnP (Universal Plug and Play) 是微软 Microsoft 所制定的一项通讯协议标准，若是您使用的计算机有支持 UPnP 机制的话(如 WindowsXP)而且您的计算机 UpnP 功能有开启，您可以将路由器路由器的 UPnP 功能启动，可以从您的计算机上开启或关闭 UPnP Forwarding 的选项。

UPnP 功能包含有 UPnP Forwarding 的功能，如您要在内网设置虚拟服务器，您可以在之前章节介绍的 Forwarding 功能设置，或是在此 UPnP Forwarding 中设置。不过请不要重复输入造成冲突。

服务端口： 在此选择欲开启的 UPnP 的服务号码预设列表，如 WWW 为 80(80~80)， FTP 为 21~21，可参考服务号码预设列表！

主机名称或 IP 地址： 在此填上 UPnP 相对应的内部虚拟 IP 地址或名称，如 192.168.1.100。

激活： 开启此服务功能。

服务端口管理表： 新增或删除管理服务埠号列表。

加入到对应列表： 增加到开启服务项目内容。

删除所选服务埠列表： 删除所选择的开启服务项目之一笔内容。

显示开启表： 显示目前所开启设定的 UpnPForwarding 列表。

确定： 按下此按钮「确定」即会储存刚才所变动的修改设定内容参数。

取消： 按下此按钮「取消」即会清除刚才所变动的修改设定内容参数，但是必须于确定 储存动作之前才会有效。

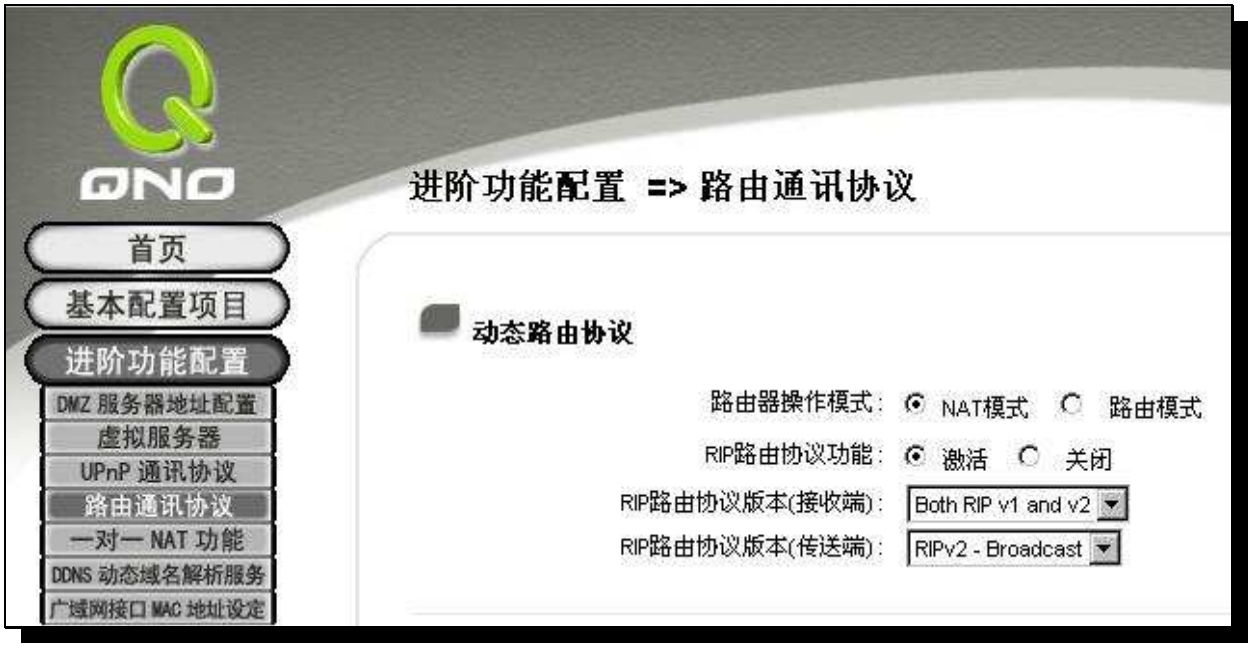
4.4 路由通讯协议(Routing)

此节介绍 动态路由协议(Dynamic Routing) 以及 静态路由(Static Routing)的设定。

4.4.1 动态路由设定(Dynamic Routing)

RIP 是 Routing Information Protocol 的简称，有 RIP I / RIP II 两个版本。对于一般使用的网络中，大多只有一个路由器(或是网关器)，所以大部份的情况是不需要使用这个功能。RIP 的使用时机是您的网络中有数个路由器，此台路由器是其中之ㄧ，此时若是不想手动设置每台路由器的绕径表(Routing Table) ，可以启动此功能，自动将所有路径更新！

RIP 是一个很非常简单的路由协议(Routing Protocol)，采用 Distance Vector 的方式以封包到达目的地之前需要经过的 Router 的个数来作为传送距离的判断， 而不以实际联机的速率来作判断。所以所选的路径是经过最少的 Router， 但是并不一定反应速度最快的 Router 及路径。



路由器操作模式： 选取路由器运作模式为 NAT 模式或是路由模式。

RIP 路由协议功能： 选取按钮「**启用**」选取使用 RIP 动态路由通讯。

RIP 路由协议版本(接收端)： 可用上下选取按钮选取使用动态路由通讯 None， RIPv1， RIPv2， Both RIPv1 and v2 为传输动态路由通讯协议的「RX」功能。

RIP 路由协议版本(传送端)： 可用上下选取按钮选取使用动态路由通讯 None， RIPv1， RIPv2-Broadcast， RIPv2-Multicast， 为接收动态路由通讯协议的「TX」

功能。

4.4.2 静态路由设定(Static Routing)

静态路由(Static Routing)是以手动设置路由表的方式来达成封包绕路。在此路由器的应用可分为两种方式，一是在内网中连结不同网段或路由器，一是在 Multi-WAN 的环境中让路由器知道去那个目地地址时就要走那条 WAN。例如常常会遇到位路由器不同的 WAN 申请不同家的 ISP 的线路，为了避免有些服务像是 Mail，或 Game Server 是架设在不同一的 ISP 环境而且 ISP 之间无法彼此互通，此时去 Mail Server 或是去 Game Server 就应该走不同的 WAN，而避免绕远路。它跟 Protocol Binding 是有相似的作用。

目的 IP 地址和子网掩码： 填入目的地的远程网络 IP 节点与子网络节点地址。

预设网关： 从此网络节点到目的远程网络欲绕径的预设网关器地址。

中继路由节点： 从此网络节点到目的远程网络所经过路由器层数，如是在路由器下的二个路由器之一，此应填为 2，预设为 1 (最大为 15)。

接口位置：	此网络节点的连接位置，是位于广域网 WAN 端亦或是局域网 LAN 端。
加入到对应列表：	增加此路径规则到列表中。
删除所选择的项目：	删除在表中所选择的路径表。
显示开启路由表：	显示目前最新的路径表。
确定：	按下此按钮「确定」即会储存刚才所变动的修改设定内容参数。
取消：	按下此按钮「取消」即会清除刚才所变动的修改设定内容参数，但是必须于确定 储存动作之前才会有效。

4.5 一对一 NAT 对应(One-to-One NAT)

当您的 ISP 线路为固定制 (如 ADSL 固定 IP) 时，通常 ISP 会给您多个合法 IP 地址。路由器提供你可将除了路由器本身 WAN Port 以及光纤盒或 ATU-R (Gateway) 各使用一个合法 IP 地址后，所剩的合法 IP 地址可以直接对应到路由器内部的计算机使用，也就是这些计算机在内网虽为虚拟 IP，但当做了 One to One 对应后，这些对应到的计算机去外部访问时都是有自己的合法 IP。

例如，当您公司内部环境需有两台或两台以上的「WEB Server」时，由于需要两个或两个以上的合法 IP 地址，所以可以利用此功能达到将外部多个合法 IP 地址直接对应到内部多个虚拟服务服务器 IP 地址使用！

范例：如您有 5 个合法 IP 地址，分别是 210.11.1.1~6，而 210.11.1.1 已经给路由器的 WAN1 使用，另外还有其它四个合法 IP 可以分别设定到 One-to-One NAT 当中，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 地址不被涵盖在 One to One NAT 的 IP 范围设定中。

一对一 NAT 对应设定： 选择是否开启此一对一 NAT 功能

内部起始 IP 地址： 虚拟 IP 地址起始 IP 地址。

外部起始 IP 地址： 外部合法 IP 地址起始 IP。

对应范围的 IP 数量： 填入你同时要有多少个外部合法 IP 地址需要对应。

加入到对应列表： 加入此设定到一对一 NAT 列表中。

删除所选择的项目： 删除所选择的一对一 NAT 规则。

确定： 按下此按钮「确定」即会储存刚才所变动的修改设定内容参数。

取消： 按下此按钮「取消」即会清除刚才所变动的修改设定内容参数，但是必须于「确定」储存动作之前才会有效。

注意！

一对一的 NAT 模式(One-to-One NAT))将会改变防火墙运作的方式，您若设定了此功能， LAN 端所对应

有 Public IP 的服务服务器或计算机将会曝露到 Internet 上。若要阻绝 Internet 的使用者主动联机到一对一 NAT 的服务服务器或计算机，请到防火墙的 Access Rule 中设定适当的拒绝存取规则条件。

4.6 DDNS-动态网域名称解析

DDNS 支援 QnoDDNS.org.cn、3322.org、DynDNS.org 以及 DtDNS.com 的动态网址转换功能，其目的是为了让使用动态 IP 地址架设网站或是远程监控还有动态 IP 下需以 VPN 的联机为目的，如 ADSL PPPoE 计时制或是 Cable Modem 的使用者的合法 IP 地址都会随时间而改变，当此使用者欲架设网站之类的服务，但是因 IP 会随时变动，所以本装置提供了动态网址转换功能，此服务可向 www.qno.cn/ddns、www.3322.org、www.dyndns.org 或 www.dtdns.com 提出申请，是完全免费的！

另外，为了解决 DDNS 服务器可能会发生不稳定的情况，现在路由器每个 WAN 都可同时对 DDNS 做动态 IP Upgrade。

DDNS 动态名称解析服务： 可以选择 QnoDDNS.org.cn、Dyndns.org 、3322.org、Dtdns.com 等(可以同时使用)。

使用者名称： 向 DDNS 服务提供者所申请的使用者名称。

密码： 向 DDNS 服务提供者所申请的密码。

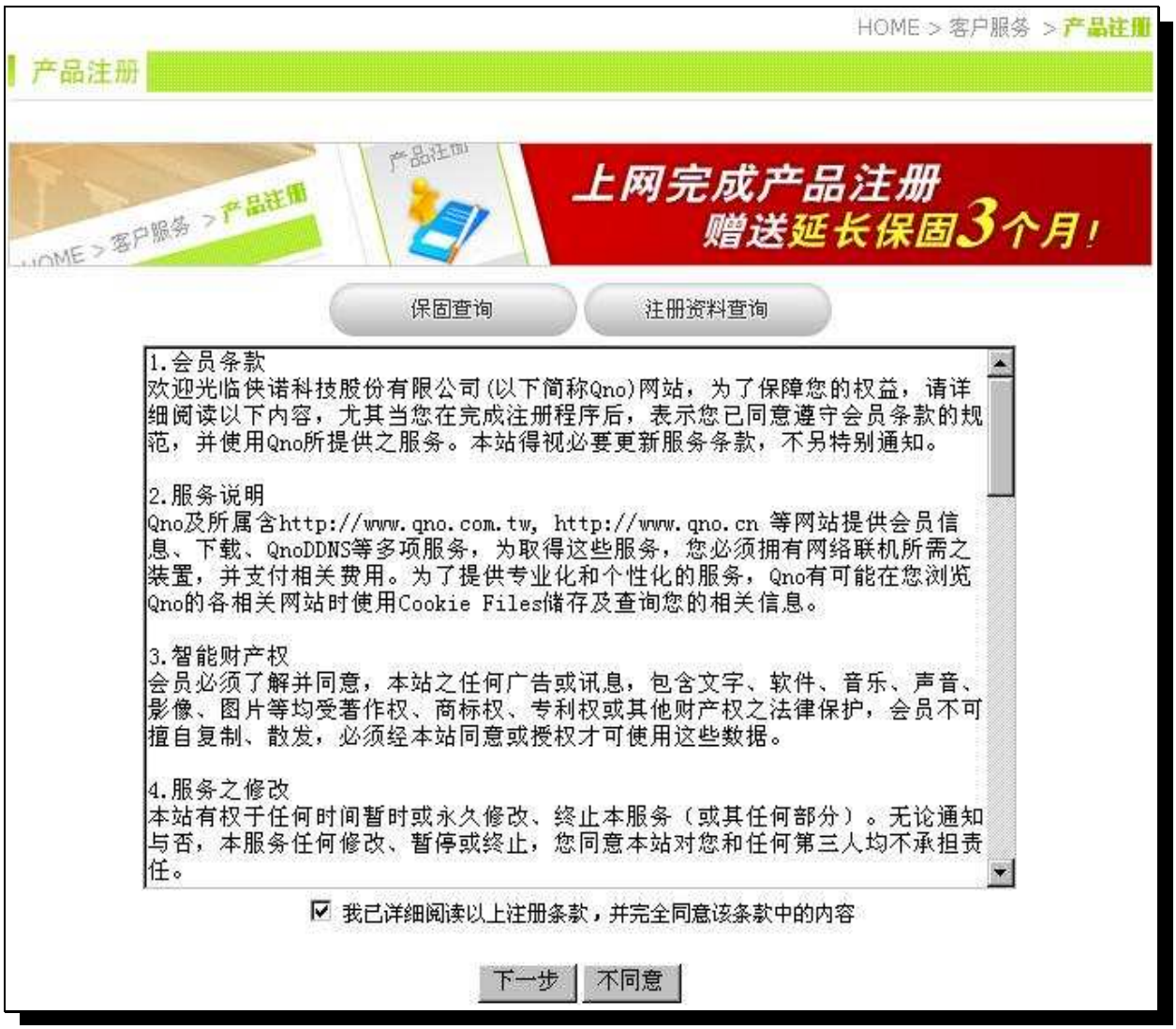
服务器名称： 动态网址名称： 向 DDNS 所注册的网址，如 abc.dyndns.org or abc.dtdns.net。

内部 IP 地址： 目前此条 WAN 所取得的 ISP 之动态合法 IP 地址，当路由器得到 ISP 端给的合法 IP 位置后会自动显示于此。

状态： 显示目前路由器对 DDNS 的更新状态。

※注册 QnoDDNS 侠诺动态网域

【1】请先登陆 Qno 侠诺官方网站，进行产品注册：http：//www.qno.com.tw



【2】依据产品注册使用的电子邮件以及产品序号，登入 QnoDDNS 侠诺动态网域服务系统；请确认电子邮件可以确实收信，以便注册网域后，可收到系统寄出的启用 QnoDDNS 服务密码。

【3】网域申请规则：

- 网域最少需为 4 个字，最多 63 个字。
- 网域只能由 a-z (英文小写)、0-9 (数字) 所组成，**且第一个字需为英文字母**。
- 网域不得有特殊象征式 (例如 "."；"-"；"_"等等) 。
- 2 Wan 系列产品最多申请 2 个 DDNS 设定。
- 4 Wan 系列产品最多申请 4 个 DDNS 设定。
- 8 Wan 系列产品(含以上)最多申请 4 个 DDNS 设定。


登 出
QnoDDNS
侠 诺 动 态 域 名
Qno Dynamic DNS Service
:: 用户数据 ::
姓名
Email
序列号
型号
Wan数量
目前登入IP
服务器时间
:: 申请规则 ::
1. 如果您申请QnoDDNS服务，代表"您无条件同意" Qno侠诺科技动态域名服务条款。
2. "用户名称" 最少需要4个字，最多63个字(4-63个字)。
3. "用户名称" 只能由a-z(英文小写)、0-9(数字)所组成，且第一个字需为英文字母。
4. "用户名称" 内不允许含有 'qno'、'dns' 的英文字母在内！
5. "用户名称" 不得有特殊符号(例如："."；"-"；"_"…等等)。(范例)
6. 2 Wan 系列产品最多申请 2 组DDNS设定。
7. 4 Wan 系列产品最多申请 4 组DDNS设定。
8. 8 Wan 系列产品最多申请 4 组DDNS设定。
9. 设定 QnoDDNS 之前，请先确认产品之 "系统时间" 正确，请参考系统时间、时间设置。
10. 如果您无法透过网络使用NTP服务来更新路由器时间，请参考服务器时间来手动更新。
11. Qno NTP Server：1. ntp.qnoddns.org.cn 2. ntp.ddns.org.cn
12. 其他NTP Server：1. 香港天文台 2. 台湾中华电信研究所 3. 国际亚洲NTP Server。
13. 其他注意事项请参考 QnoDDNS服务使用教学。
:: 用户名称测试 ::
已输入0个字
测试 用户名称： 域名： qnoddns.org.cn 发送 重设
尚可申请 4 组DDNS
已输入0个字
第1组 用户名称： 域名： qnoddns.org.cn 申请
已输入0个字
第2组 用户名称： 域名： qnoddns.org.cn
已输入0个字
第3组 用户名称： 域名： qnoddns.org.cn
已输入0个字
第4组 用户名称： 域名： qnoddns.org.cn

4.7 广域网接口 MAC 地址设定(MAC Clone)

有些 ISP 会要求提供一固定 MAC 地址(网卡地址)做为 ISP 端分配 IP 给您的认证使用，它大多使用于 Cable Mode 的用户。若有此需求，可使用此功能将提供给 ISP 的网卡地址(MAC Address：00-xx-xx-xx-xx-xx)填入此项目中，路由器就会以此 MAC Address 做为跟 ISP 请求 IP 时的认证！

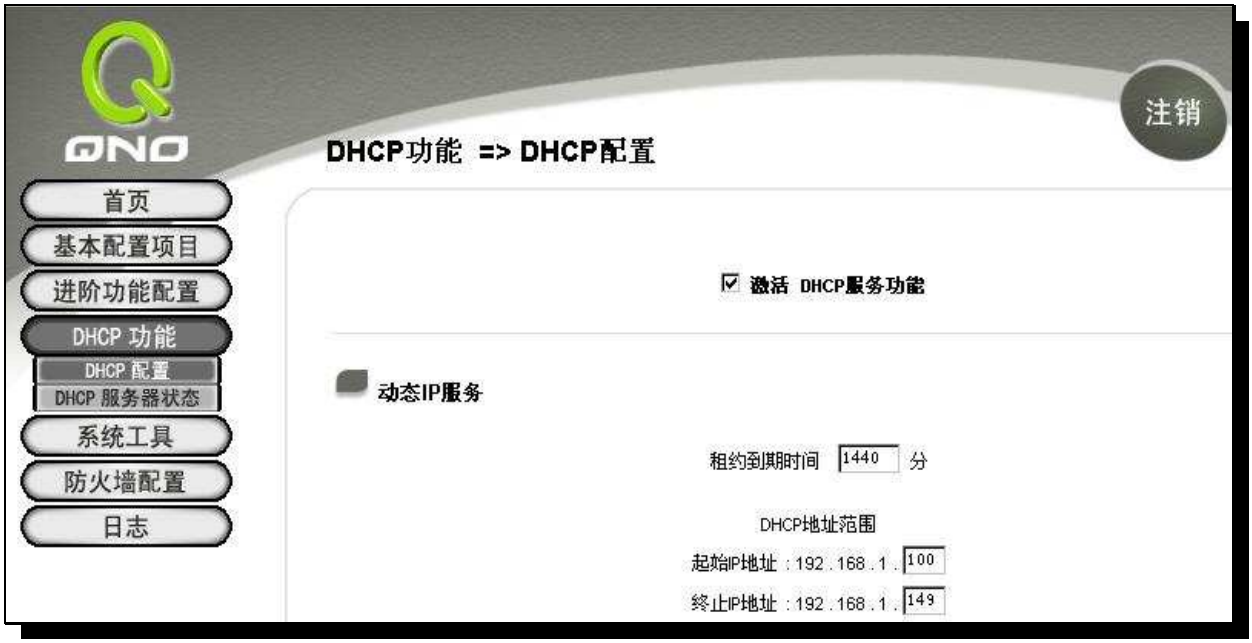
使用者自订广域网接口 MAC 地址： 使用者可以自行输入提供给 ISP 的网卡地址，目前设备出厂预设的 MAC 位置为 WAN 端的 MAC 地址。

设定与此 PC 的 MAC 地址相同： 目前这台 PC 的 MAC 地址。

4.8 DHCP 发放 IP 服务器

路由器有一组 Class C 的 DHCP 服务器，默认值是启动，可以提供局域网络内的计算机自动取得 IP 的功能，（如同 NT 服务器中的 DHCP 服务），好处是每台 PC 不用去记录与设定其 IP 位置，当计算机开机后，就可从路由器自动取得 IP 地址，管理方便。

4.8.1 动态 IP (Dynamic IP)



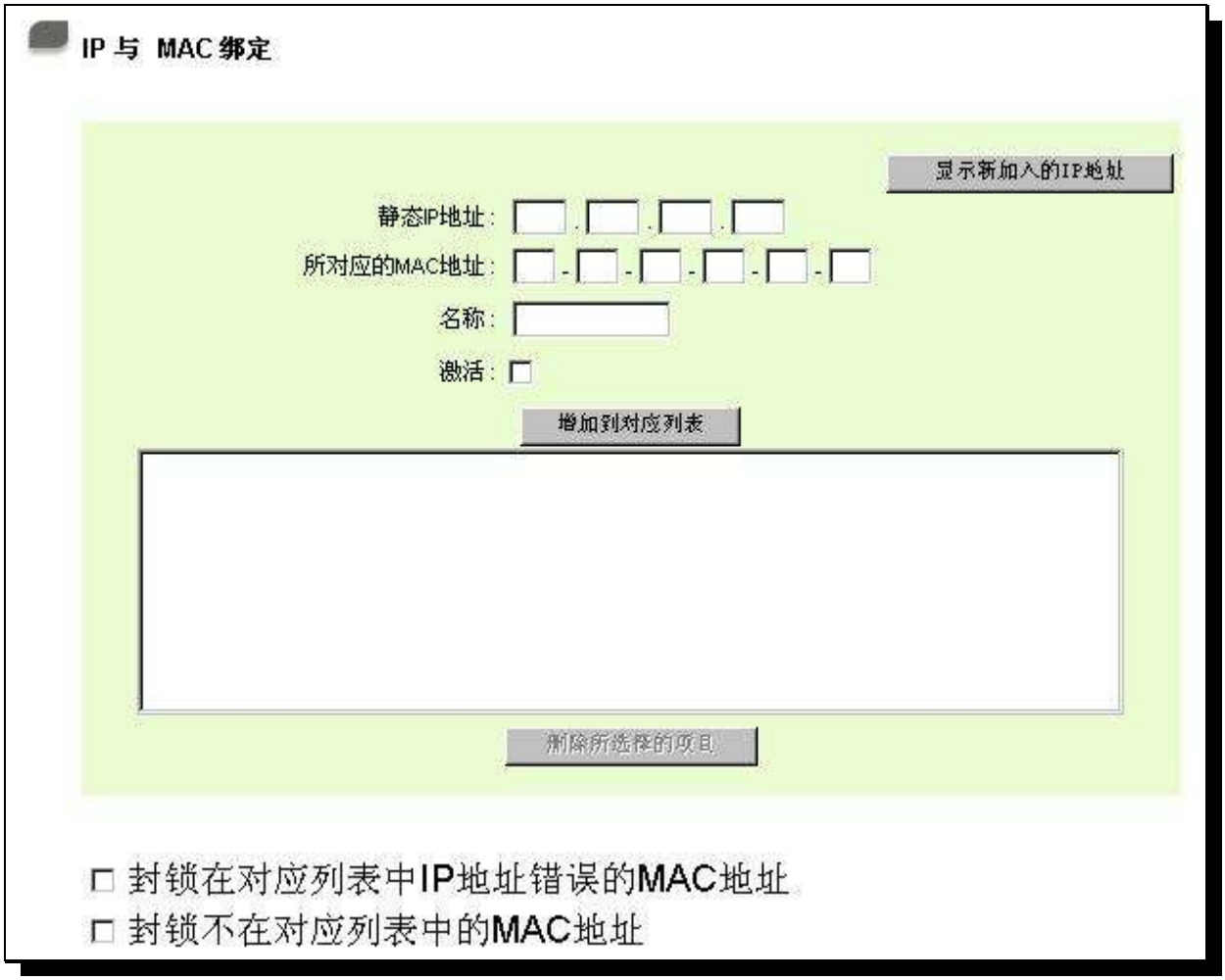
租约到期时间： 此设定为发给 PC 端 IP 地址的租约时间，预设为 1440 分钟(代表时间为一天)，当租约时间到后，PC 端会重新跟 Router 再申请一次。您可以依照实际需求来设定。

起始 IP 地址： 系统预设为从 192.168.1.100 的 IP 地址开始发放。您可以依照实际需求来设定。

终止 IP 地址： 系统预设为 192.168.1.149 IP 地址为最后发放 IP，也就是说出厂设定值可供 50 台计算机自动取得 IP 地址。您可以依照实际需求来设定。

4.8.2 IP 及 MAC 地址绑定(IP & MAC Binding)

在许多的企业及小区网络中，网管人员可以设定路由器所提供的 IP & MAC 绑定功能，达到 User 不能自行添加计算机来使用对外网络或是私自擅改 IP 上网影响他人。另外透过此功能也可以将每台计算机或服务器的 MAC 地址绑定，达到计算机或服务器每次开机或重新要 IP 时，都分配给它相同的一组 IP 地址。



静态 IP 地址： 此字段元有两种填入方式：

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个 IP，请在此字段填 0.0.0.0，不可为空白。

2. 若要求每次此台计算机都要分配到同一个 IP，则将你所要求分配给此台计算机的 IP 地址输入。这样所要绑定服务器或 PC 端每次重启都会要到固定的同一个虚拟 IP。

所对应的 MAC 地址： 输入要绑定的服务器或 PC 端固定实体 MAC (网络卡上的地址)。

名称： 填入您所绑定此用户的名字或地址做辨识，可输入 12 个字符，中英文皆可以。

激活： 启用此组设定。

加入到对应列表： 加入或修正此设定到列表中。

删除所选择的项目： 删除列表中所选择的绑定。

封锁在对应列表中 IP 此选项打勾后，只要是 User 自行变更计算机的 IP 或不是清单设定的 IP 将

地址错误的 MAC 地址： 无法上网

封锁不在对应列表中的 MAC 地址： 此选项打勾后，只要不在清单中的 MAC Address 都无法上网

显示新加入的 IP 地址：

此功能的主要目的是为了减少网管人员需一一查询每台计算机的 MAC 地址后才能进行绑定，因为会非常耗时且困难。再者，将 MAC Address 手动填入列表也很容易出错。所以只需要查询此表格，就可以看到所有进出路由器且还未绑定的 MAC Address，然后直接在此表格做绑定动作即可.另外，若你发现此表格出现已经绑定的某组 MAC 又出现在此表格，则表示此 User 试图修改不是你指定的 IP 上网

名称： 可以填入您所绑定此用户的名字或地址做辨识，可输入 12 个字符。

启用： 勾选你所要绑定的目标。

确定： 将你所选定好的目标绑定到 IP & MAC 绑定列表。

全选： 选择所有在此列表中的目标做绑定。

更新： 更新此列表。

关闭： 关闭此列表。

显示表格(Show Tables)

此功能可以列出所有现在已经设定好的 MAC Binding 及 IP Binding 的状态，并且可以选「编辑」做修改

4.8.3 DNS 与 WINS 服务器设定(DNS & WINS Server)

网域解析服务地址(DNS Server)：

此设定为发给 PC 端 IP 地址的 DNS 网域服务器查询地址，若您有特定使用的 DNS 服务器，可以直接输入此服务器的 IP 地址，则 PC 端从 DHCP 取得 IP 地址时，也会一并取得指定的 DNS 服务器地址。

DNS 服务器 (主要) 1： 输入 DNS 网域服务器的 IP 地址。

DNS 服务器 (次要) 2： 输入 DNS 网域服务器的 IP 地址。

WINS Server：

若您的网络上有解析 Windows 计算机名称的服务器，您可以直接输入此服务器的 IP 地址。

WIN 服务器： 输入 WINS 网域服务器的 IP 地址。

确定： 按下此按钮「确定」即会储存刚才所变动的修改设定内容参数。

取消： 按下此按钮「取消」即会清除刚才所变动的修改设定内容参数，但是必须于确定 储存动作之前才会有效。

4.8.4 DHCP 状态显示(DHCP Status)

此状态表为显示 DHCP 服务器的目前使用状态与设定纪录等，以便提供管理人员需要时做网络设定参考数据。

DHCP 服务器 IP 地址： 目前 DHCP 服务器的 IP 地址。

已使用的动态 IP 数量： 目前 DHCP 服务器已经发放动态 IP 的数量。

已发放的固定 IP 数量： 目前 DHCP 服务器已经发放固定 IP 的数量。

剩余可用的 IP 数量： 目前 DHCP 服务器可以还可发放的 IP 数量。

可发放的 IP 总量： 目前 DHCP 服务器所设定可发放的 IP 总数量。

主机名称： 目前此台计算机的计算机名称。

IP 地址： 目前此台计算机所取得的 IP 地址。

MAC 地址： 目前此台计算机的 MAC 网络实体位置。

租约到期时间： DHCP 目前核发 IP 位置的租约到期时间。

删除： 删除此笔核发 IP 纪录。

五、工具程序功能设定 (Tool Configuration)

此章节介绍用来管理路由器以及测试网络联机的工具。

5.1 网络管理设定(SNMP)

SNMP 为 Simple Network Management Protocol 的缩写，意指网络管理通讯协议。此为网络上使用的一个管理工具。SNMP 通讯协议可以让已经具备有网络管理的程序(如 SNMP Tools-HP Open View)等网管程序做实时管理通讯使用。路由器支持标准 SNMP v1/v2c，可以搭配标准 SNMP 网络管理软件来得知目前路由器上的机器运作情况，以便随时掌握网络信息。

激活 SNMP 网络管理协议： 将 SNMP 功能开启或关闭。系统预设为开启此功能。

系统名称： 设定机器的名称

连络方式： 设定机器的管理联系人员名称。

系统地址： 设定机器的目前所在位置。

Get Community Name： 设定一组管理者参数可以取得此机器的项目信息，系统预设「Public」。

Set Community Name： 设定一组管理者参数可以设定此机器的项目信息，系统预设「Private」。

Trap Community Name： 设定一组管理者参数可以传送 Trap 的信息。

Send SNMP Trap to： 设定一组 IP 位置或是 Domain Name 名称的接收 Trap 讯号主机。

5.2 在线联机测试 (Diagnostic)

路由器 提供简易的在线测试机制，方便在测试线路质量时使用。此包含 DNS Lookup 以及 Ping 二种。

网域名称查询测试 (DNS Name Lookup)：

请于此测试画面输入您想查询的网域主机位置名称，如 www.abc.com 然后按下“开始”的按钮开始测试。测试结果会显示于此画面上。

Ping-封包传送 / 接收测试：

此项目为主要提供管理者了解对外联机的实际状况，可以藉由此功能了解网络上的计算机是否存在！

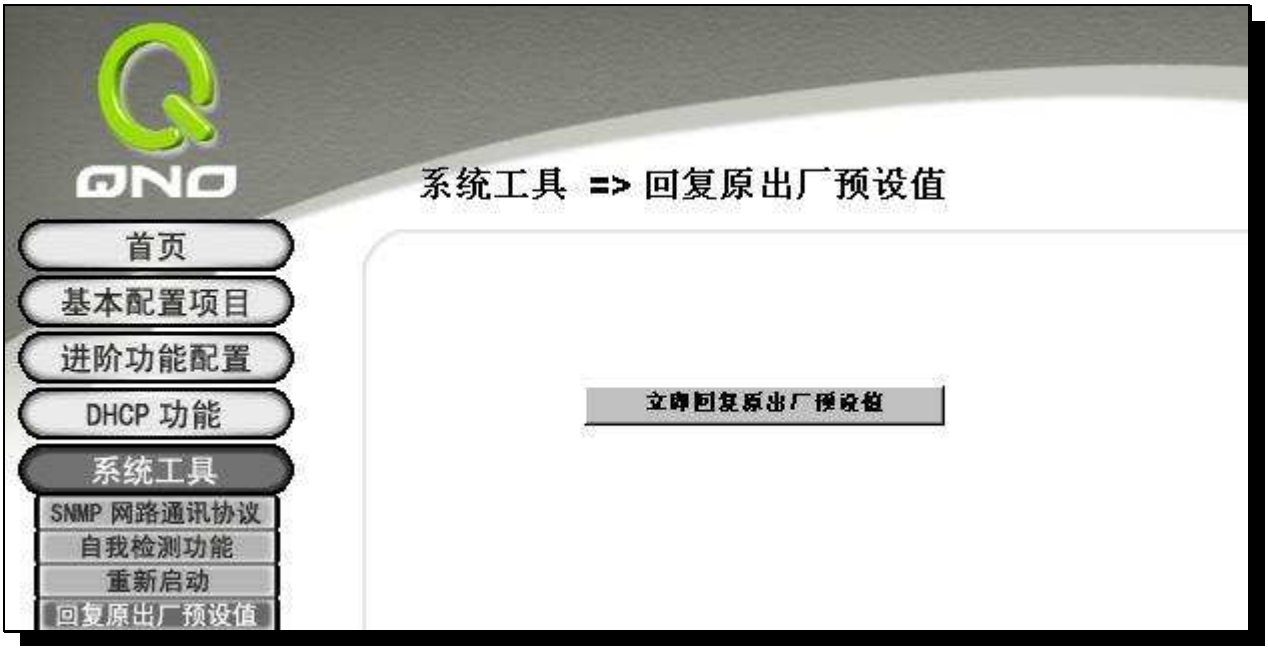
请于此测试画面输入您想测试的主机位置 IP，如 192.168.5.20 按下 Go 的按钮开始测试，测试结果会显示于此画面上。

5.3 重新启动(Restart)

您可以于此工具中选择路由器系统重新开机功能，请按下「立即重新启动」按钮即可重新开机启动。

5.4 回复原出厂默认值 (Factory Default)

若是选择「立即回复出厂默认值」， 路由器会将所有的设定清除，并重新开机。我们建议在做版本升级前请先将 Router 现在的设定值存在计算机，等做完版本升级后，使用此功能将机器做出厂值设定以确保机器升级后的稳定行，然后再将刚才存在计算机的设定直存回路由器 (如何储存路由器的设定数据及升级完成后如何存回路由器，请参考 Setting Backup 说明)。



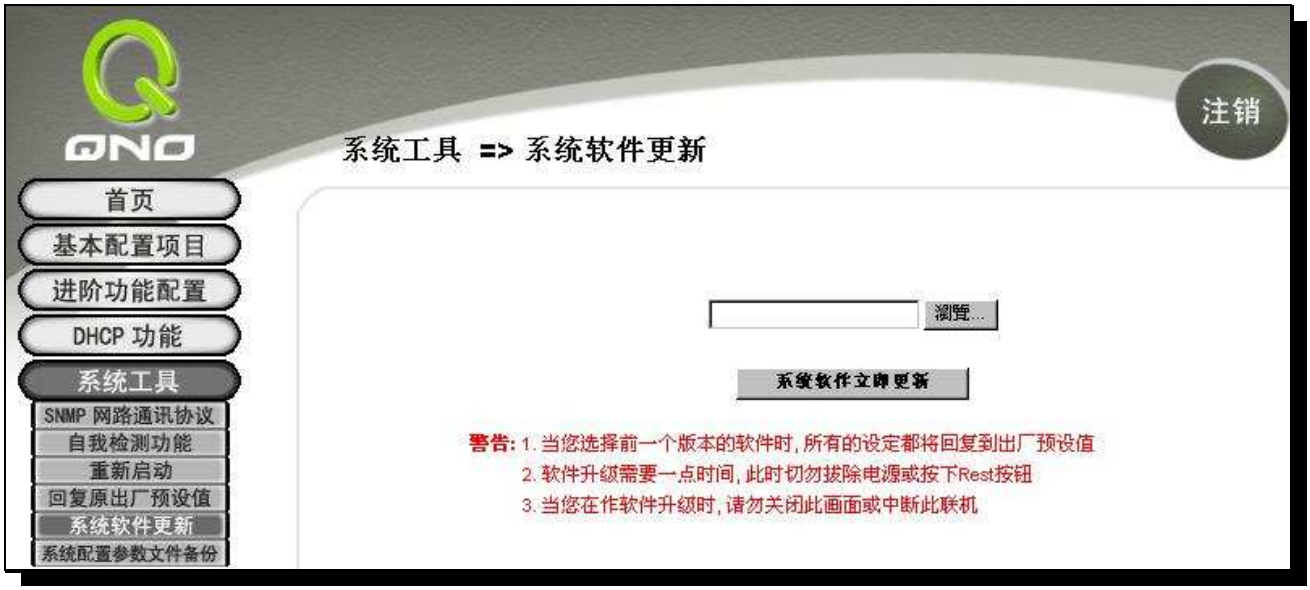
5.5 系统软件升级 (Firmware Upgrade)

此功能可以让路由器在 Web 设定画面中直接做软件升级。请您于升级前先确认软件版本信息。按下「浏览」按钮，选择软件(Firmware)存放文件夹，并于选择欲升级的软件后，按下「系统软件立即更新」做升级。

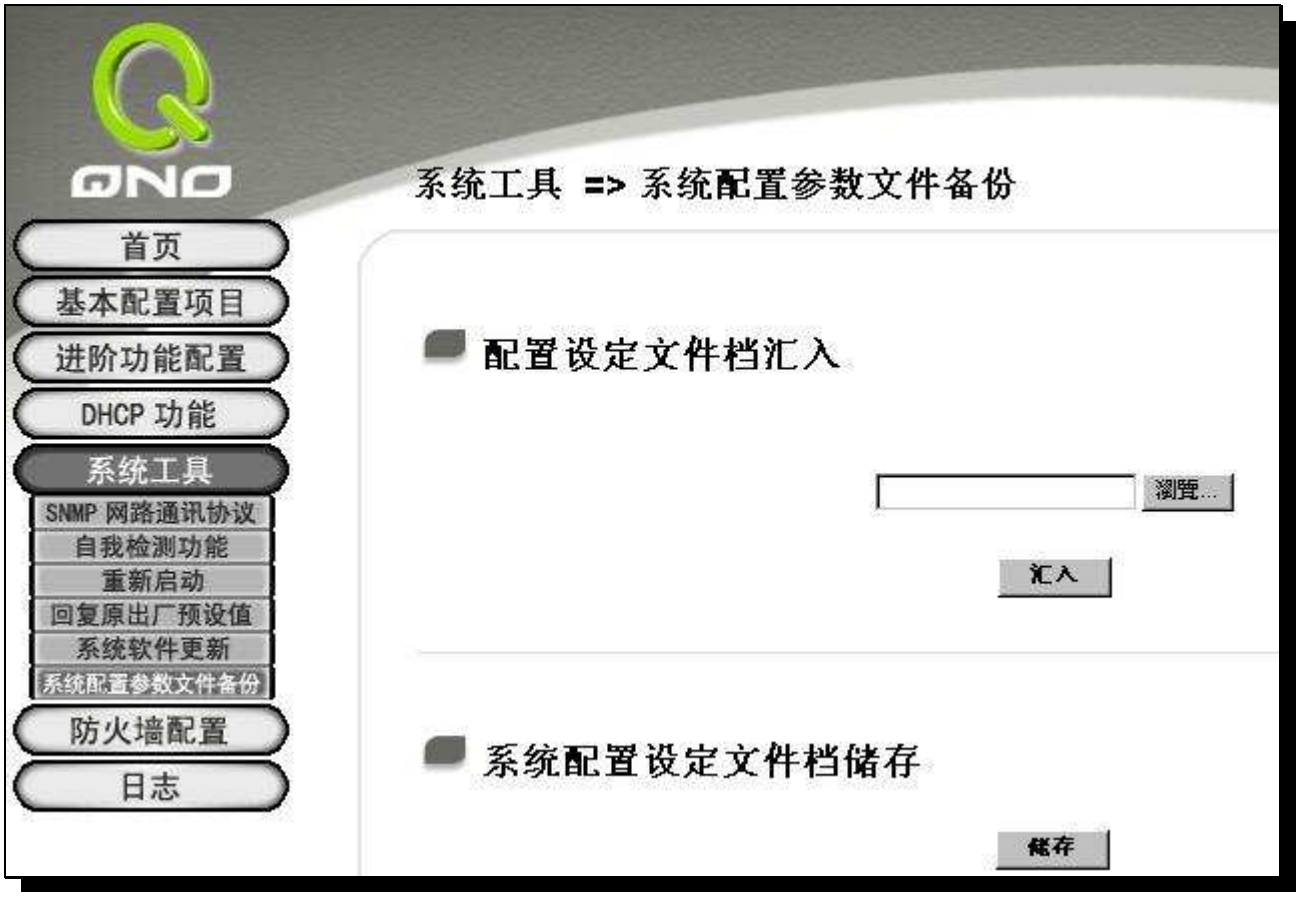
注意！

执行升级操作前，请详细阅读画面中的注意事项。

若正处于升级进程中，请勿离开此升级画面，否则会造成路由器升级失败。



5.6 系统设定参数储存 (Setting Backup)



配置设定文件文件汇入 (Import Configuration File)：

此功能为将之前所储存在计算机的备份设定参数内容回存到路由器中！选择「浏览」至备份参数档案-「config.exp」存放数据夹，选择该档案后，按下汇入按钮做设定档案汇入。

系统配置设定文件文件储存 (Export Configuration File)：

此功能为储存网管人员在路由器的设定参数备份到计算机中，通常做 Router 版本升级前，请务必将您现在的路由器设定文件用此功能储存在计算机中！ 按下 Export 按钮，选择至备份参数档案-「config.exp」存放文件夹位置，按下储存即可。

六、防火墙功能设定 (Firewall Configuration)

本章节介绍防火墙设定的选项，以及网络存取控制的设定。

6.1 防火墙一般设定(General)

从防火墙功能的一般设定选项当中， 您可以控制启用或是关闭这些选项功能。出厂默认值是将防火墙开启，并关闭不必要的响应。

防火墙功能： 此为选择开启或关闭防火墙功能。

SPI 主动侦测封包过滤功能： 此为封包主动侦测检验技术(Stateful Packet Inspection)，防火墙主要运作在网络的层级，但是藉由执行对每个连结的动态检验，也拥有应用程序的警示功能。同时，封包检验型防火墙可以拒绝非标准的通讯协议所使用的连结。

DoS 防御功能： 此为保护 DoS 攻击，如 SYN Flooding， Smurf， LAND， Ping of Death， IP Spoofing 等。

DOS 防御功能进阶设定：

封包类别：

路由器提供三种最常使用的攻击封包检测，含括 TCP-SYN-Flood、UDP-Flood 以及 ICMP-Flood

TCP-SYN-Flood 封包是利用 TCP 协议三次交握的方式制造大量虚拟造的 TCP 联机，大量占用被攻擊方资源而造成网络线路拥塞或者不通。

UDP-Flood，一种基与 UDP 协议的攻擊模式，利用 UDP 联机产生大量的联机数来达到占用网络资源进行攻擊，造成网络执行不正常。

ICMP-Flood，一种基与 ICMP 协议的攻擊模式，比如大量的 Ping 联机路由器占用频宽，造成带宽拥塞来进行攻擊，造成网络执行不正常。

广域网络门坎值设定：

所有封包门坎值：当外部攻擊的所有封包数据达到设定的最大值（预设 15000pakets/Sec），则采取阻挡联机的行动。

单一 IP 封包门坎值：当外部单一一个 IP 地址所产生攻擊的封包数据达到设定

的最大值（预设 2000pakets/Sec），则采取阻挡联机的行动。

达到门坎值则阻挡此 IP 5 分（预设是 5 分钟）：当达到上述的封包最大值条件后，要阻挡此攻击 IP 地址进行联机的时间。

您可以根据需要，调整你的门坎值以及阻挡时间来达到对外部攻擊的有效防护，建议其门坎值从大到小来调节。

局域网络门坎值设定：

所有封包门坎值：当内部攻擊的所有封包数据达到设定的最大值（预设 15000pakets/Sec），则采取阻挡联机的行动。

单一 IP 封包门坎值：当外部单一一个 IP 地址所产生攻擊的封包数据达到设定的最大值（预设 2000pakets/Sec），则采取阻挡联机的行动。

达到门坎值则阻挡此 IP 5 分（预设是 5 分钟）：当达到上述的封包最大值条件后，要阻挡此攻击 IP 地址进行联机的时间。

您可以根据需要，调整你的门坎值以及阻挡时间来达到对外部攻擊的有效防护，建议其门坎值从大到小来调节。

不受限制的来源 IP 地址：

输入不要被 DOS 防御门坎值所限制的局域网来源 IP 地址或是范围

不受限制的目的 IP 地址：

输入不要被 DOS 防御门坎值所限制的目的 IP 地址(从局域网发出的封包)

显示开启表：

显示被 DOS 防御功能所阻挡的 IP 地址，以及该 IP 地址还剩余多少时间解除阻挡

关闭广域网响应功能：

若是选择启用的话，则路由器 会关闭对外的 ICMP 与不正常联机的封包响应，所以若是你从外部去 ping 此台路由器的 WAN IP 是无法 ping 通的，默认值为开启拒绝对外响应的功能。

远程管理功能：

远程管理功能，若您要透过远程 Internet 直接联机进入路由器的设定画面，必需将此功能开启，并于远程于浏览器网址填入路由器的外部合法 IP 位置(WAN IP)，并加上预设可修改的控制端口 (预设为 80，可更改)。

允许 Multicast 封包穿透功能：

网络上有许多影音串流媒体，使用广播方式可以让客户端接收此类封包讯息格式。默认值为关闭这个功能。

防止 ARP 病毒攻击：

此功能为防止内网遭受 ARP 欺骗攻击而造成计算机无法上网，此 ARP 病毒欺骗大多在网咖环境发生，会让所有上网计算机一瞬间断线或部份计算机无法上

	网。开启此功能可以避免此种病毒攻击。
每秒主动发送（ ）笔 ARP 封包：	网络内广播发包防止 ARP 攻擊。
特殊网页存取限制：	路由器支持封锁下列几种的方式连结：Java，Cookies，Active X， Access to HTTP Proxy Servers。
不需关闭 Java/ActiveX/Cookies 代理服务器、存取信任的网域：	若启动这项功能，使用者可以将信任的网站或者 IP 地址加入可信任的网域中，则路由器就不会去阻挡可信任网域的网页中所带有的 Java/ActiveX/Cookies 等项目。
确定:	按下此按钮「确定」即会储存刚才所变动的修改设定内容参数。
取消:	按下此按钮「取消」即会清除刚才所变动的修改设定内容参数，但是必须于「确定」储存动作之前才会有效。

6.2 网络存取规则(Access Rule)

路由器设计有简而易懂的网络存取规则条例工具，管理者可以用来对不同的使用者设定不同的存取规则条件，来管理使用者对网络的存取权限。存取规则可以依据不同的条件来过滤，例如可以设定封包要管制的进出方向是从内部到外部 (Inside-LAN to Outside-WAN) 还是从外部到内部 (Outside-WAN to Inside-LAN)，或是设定以使用者的 IP address(源 IP 地址)、Destination IP address(目的 IP 地址)、IP protocol type(IP 通讯协议型态)等条件来做管制，管理者可以依照实际的需求调性设置。

管理者定订的网络存取规则条例，可以选择关闭(deny)或是允许(allow)来调整使用者对因特网 Internet 的存取。以下就针对路由器的网络存取规则条例做一说明：

路由器预设的网络存取规则条例：

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

管理者可以自定存取规则并且超越路由器 的预设存取条件规则，但是以下的四种额外服务项目为永远开启，不受其它自订规则所影响：

* HTTP 的服务从 LAN 端到路由器 预设为开启的 (为了管理路由器使用)。
* DHCP 的服务从 LAN 端到路由器 预设为开启的 (为了从路由器自动取得 IP 地址使用)。
* DNS 的服务从 LAN 端到路由器 预设为开启的 (为了解析 DNS 服务使用)。

* Ping 的服务从 LAN 端到路由器 预设为开启的 (为了连通测试路由器使用)。

除了预设规则以外，所有的网络存取规则都会显示于此规则列表中，您可以自己选择高低优先权 (Priority) 于每一个网络存取规则项目中。路由器在做规则确认时是依照 Priority 1、2、3 依序做规则判断，所以 Priority 是让您在做 Access Rule 的设定规划中必须要考虑的，以避免您想开启或关闭的功能失效。

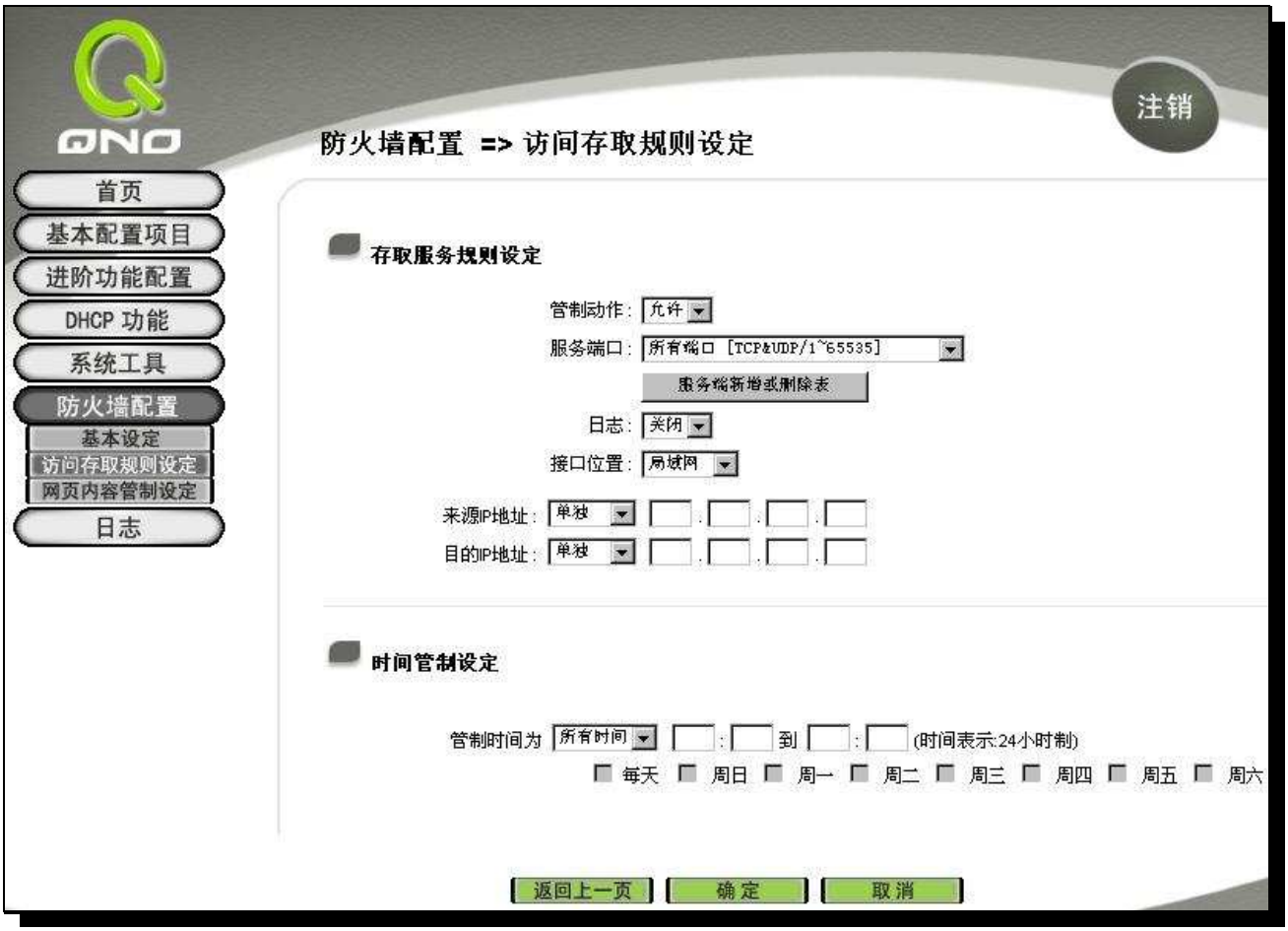
编辑： 可以设定网络存取规则项目。

垃圾桶图像： 可以删除网络存取规则项目。

加入新的规则： 新增新的网络存取规则按钮可以新增一项新的存取规则。

回复到出厂默认值： 可以回复到出厂原有预设存取规则项目并删除所有的自订规则内容。

6.2.1 增加新的管制规则(Add a new Rule)



管制动作： 此为设定此规则的管制条例动作：

允许：允许符合此管制条例行为的封包通过。

禁止：不允许符合此管制条例行为的封包通过。

服务端口： 从下拉式选单中选择你所要允许或不允许的 Service Port 服务项目内容。

服务端口管理表： 若是您想要管制的 Service Port 服务内容没有存在于预设列表内的话，您可以按下右方的 Service Management – 服务管理 来新增一个服务内容。于弹出窗口中输入一个服务名称-Service Name 以及通讯协议与端口口- Protocol & Prot ，按下 Add-新增按钮即可新增一个管制服务项目内容。

日志： 选择该存取规则触发动作时，是否要记录到日志内（关闭 / 启用）

接口位置： 选择你所要允许或不允许的来源封包接口(例如是从 LAN， WAN1， WAN2 还是 Any)，可以从下拉式选单中选择。

来源 IP 地址： 选择来源封包的 IP 范围(如 Any， Single or Range)，若选择 Single 或 Range ，请输入此单一或是一区段范围的 IP 地址。

目的 IP 地址： 选择目的端封包的 IP 范围(如 Any，Single or Range)，若是选择 Single 或是 Range 的话，请输入此单一或是一区段范围的 IP 地址。

时间管制设定： 你可以将此条规则依照你所需要的执行时间来做控管。例如你可以设定此规则每天上午 8：00 开始执行下午 17：00 结束，或 24 小时都执行管制。
可选择所有时间表示 24 小时都执行此规则(预设)，或是可以选择从几点到几点，以及设定是每天还是某几天做管制。

___到___： 此管制规则有时间限制，设定方式为 24 小时制，如 08：00 到 18：00 (早上 8 点到下午 6 点)。

管制天数： 勾选每天是表示每一天的这段时间都受控管，若是只针对一星期特定星期几，可以直接选择星期。

确定： 按下此按钮「确定」即会储存刚才所变动的修改设定内容参数。

取消： 按下此按钮「取消」即会清除刚才所变动的修改设定内容参数，但是必须于确定 储存动作之前才会有效。

6.3 网页内容管制(Content Filter)

路由器的 Content Filter 可支持两种模式的网页管制，一为 Block Forbidden Domains 封锁不允许访问的网址，另一个为 Accept Allowed Domains 允许访问的网站，此两种模式只能使用一种。

设定限制访问的网域 (Block Forbidden Domains)

此功能需将完整的网址如 www.sex.com 填入，即可封锁此网站。

激活限制网域管制功能： 选择打勾开启网页内容管制功能，预设为关闭。

网域名称： 填写欲管制的网址，如 www.playboy.com。

加入到对应列表： 按下「增加到对应表」按钮新增此一欲管制的网址。

删除所选择的项目： 可以使用鼠标点选一个或多个管制的网址，然后按下即可删除。

网页字符串管制 (Website Blocking by keywords)：

只要输入如「sex」的字符，那所有在网址里面有「sex」的网站都会被封锁。

激活网页字符串管制： 当此项功能启动后，当输入网站地址有存在「sex」关键词时，则路由器会将所有有「sex」的网页封锁。

新增： 即增加一个新的网页字符名称

增加到对应列表： 增加此新增的服务项目内容到服务表列内。

删除所选择的项目： 选择删除服务项目内容从服务表列内。

允许访问的网站 (Accept Allowed Domains)

此功能的目的是设定只能去访问的网址，在有些公司或学校中，会只允许员工或学生只能去哪些网站，就可以用此功能来达成。

激活开放网域管制功能： 选择打勾开启允许网址管制功能，预设为关闭。

网域名称： 填写欲管制的允许网址，如 www.playboy.com。

加入到对应列表： 按下 Add 按钮新增此一欲管制的允许网址。

删除所选择的项目： 可以使用鼠标点选一个或多个管制的允许网址，然后按下即可删除。

管制内容排程时间 (Scheduling)

当选择为 Always 时，表示此条规则 24 小时执行。若选择 from 时，此管制条例会依据所设定的生效时间去执行此条规则，如管制时间为周一到周五，早上八点到下午六点，您可以依照以下图例来管制。

全部: 表示此管制规则 24 小时开启。

___到___： ___到___：此管制规则有时间限制，设定方式为 24 小时制，如 08：00 到 18：00 (早上 8 点到下午 6 点)。

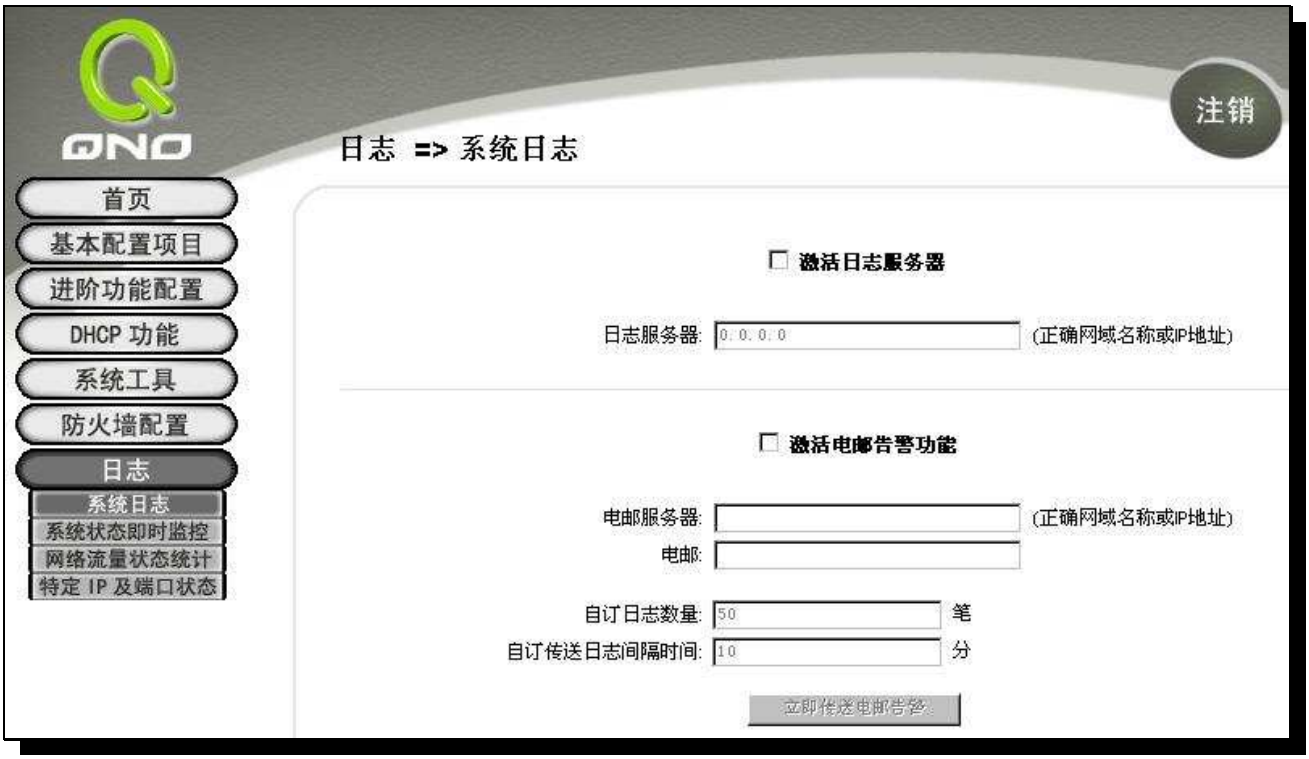
管制天数： 勾选「每天」是表示每一天的这段时间都受控管，若是只针对一星期特定星期几，可以直接选择星期。

七、日志功能设定 (Log Configuration)

日志(Log)功能纪录路由器的运行数据，并以可读的方式呈现再设定画面上提供给您作为参考。您可以依据需求检视这些信息。

7.1 系统日志-System Log

路由器的日志记录提供三种设定：系统日志(Syslog)， 电子邮件通知(E-mail)，以及选择 Log 的类别(Log Setting)。



系统日志 (Syslog)

激活日志服务器： 若是勾选此选项的话，Syslog 功能将被开启。

系统日志服务器： 路由器 提供了外部 Syslog 服务器收集系统信息功能。Syslog 为一项工业标准通讯协议，于网络上动态撷取有关的系统信息。路由器 的 Syslog 提供了包含动作中的联机来源位置(Source IP Address)与目地(Destination IP Address)位置， 服务编号(Port Number)以及型态(IP service)。输入您要接收 Syslog 的服务器名称或是 IP 地址于「Syslog Server」的空格字段内。

电子邮件告警功能 (E-mail Alert)

启用 E-mail 警示功能： 若是勾选此选项的话，电子邮件告警(E-Mail Alert)将会被开启。

邮件服务器： 请输入电子邮件服务器的名称或是 IP 地址，如 mail.abc.com。请注意，您必须有权限经由所填入的电子邮件服务器寄送 Log 电子邮件，否则此 Log 电子邮件将无法被寄出。

E-mail： 此为设定 Log 收件人电子邮件信箱，例如 abc@mail.abc.com。

自订日志数量： 自订 Log 数量，系统预设为 50 个。当到达此数量时，路由器将会自动 Mail 传送 Log。

自订传送日志间隔时间： 自订传送 Log 间隔时间，系统预设为 10 分钟。 当到达此时间时，路由器将会自动 Mail 传送此 Log。

路由器将会自动判别当数量或是间隔时间哪一个参数先到达，就 Mail 传送 Log 讯息给管理者。

立即传送日志： 使用管理者可以直接按此按钮传送 Log。

系统日志配置(Alert Log)

路由器 提供了包含以下的告警内容讯息，您只要打勾点选即可包含在 Log 讯息中。

Syn Flooding： 即在短时间内传送大量的 syn packet，造成系统记录联机的内存溢满。

IP Spoofing： 通过封包监听程序来拦截网络上所传送数据，并在读取后藉由程序修改原发送端地址(source IP address)， 进入原目的端的系统内，存取资源。

Win Nuke： 通过侵入或设陷阱的方式将木马程序送入对方服务器中。

Ping of Death： 通过传送来产生超过 IP 协议所能够允许的最大封包，造成系统死机。

登入认证错误： 当系统发现有企图登入路由器的入侵者时，就会将讯息传到系统日志中。

一般系统日志信息(General Log)

路由器 提供了包含以下的一般性内容讯息，您只要打勾点选即可。系统错误讯息(System Error Messages)，被阻挡的管制条例(Deny Policies)，允许通过的管制条例(Allow Policies)，认证登入(Authorized Login)，系统配置变更(Configuration Changes)。

系统错误讯息： 提供系统中各种错误给系统日志。例如：不正确的设定或是功能异常状况发生。

被阻挡的管制条例： 当有 User 试图进行 Access Rule 不允许的规则时，此信息会传送到系统日志中。

允许通过的管制条例： 当 User 进行 Access Rule 所允许的规则时，此信息会传送到系统日志中。

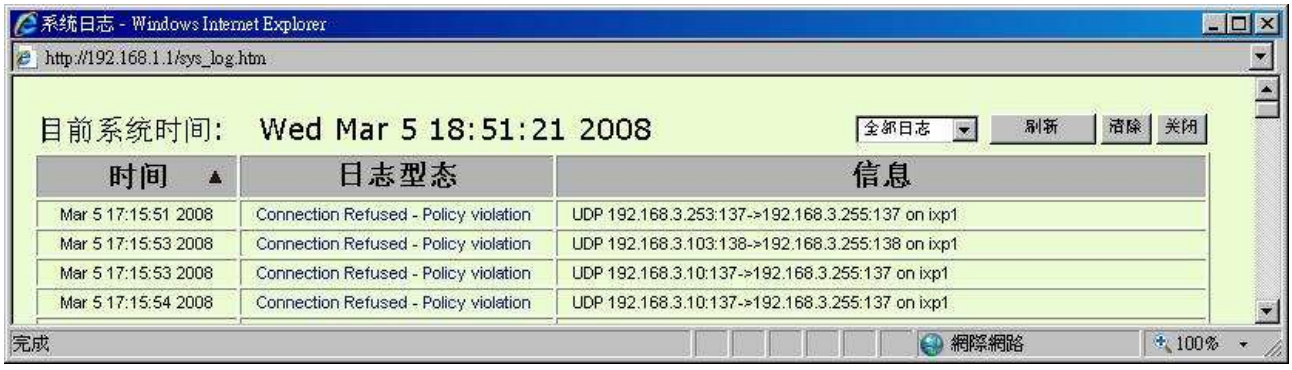
系统配置变更： 当系统的设定值改变时，此信息回传送到系统日志中。

认证登入： 每一个成功登入系统的 IP 地址都会传送并记录到系统日志中。

以下有四个有关查询 Log 的按钮，分别叙述如下：

查看系统日志 (View System Log)：

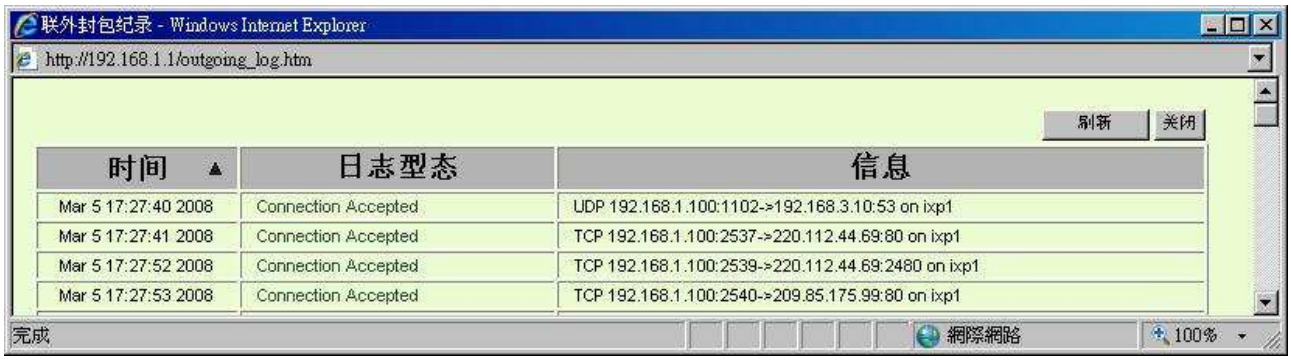
此为查看系统日志使用，其信息内容可以从下拉式选单中分类读取，包含全部日志，系统日志，存取日志，防火墙日志。选择「更新 (Refresh)」按钮可以刷新日志显示画面，「清除 (Clear)」按钮可以清除所有日志记录。如下图所示：



连外封包纪录 (Outgoing Log Table)：

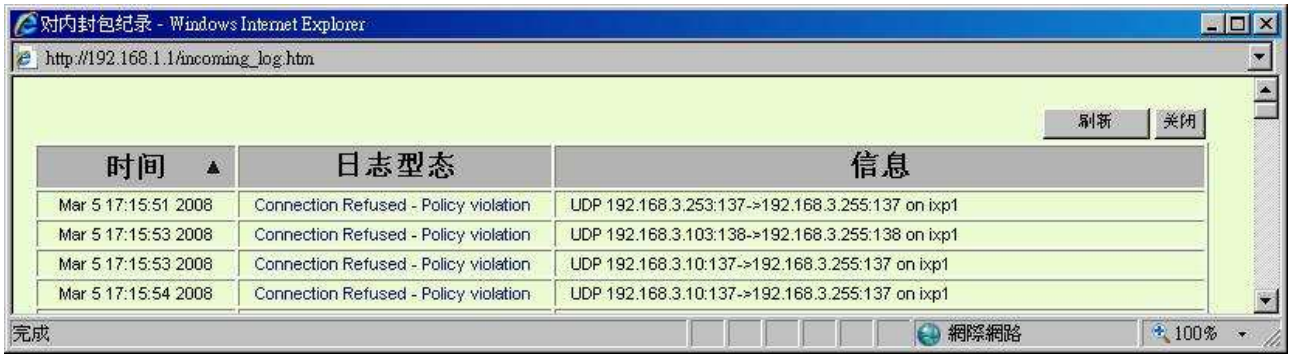
查看内部 PC 出 Internet 的系统封包日志，此日志包含内部网络地址(LAN IP)，目的地地址(Destination URL/IP)

以及所使用的通讯服务端口(Port Number)类型(Type)等信息。



对内封包纪录 (Incoming Log Table)：

查看外部进入路由器的系统封包日志，此日志内涵外部来源网络地址(Source IP 地址)， 目的地地址与通讯端口号(Destination Port Number)等信息。



清除日志 (Clear Log Now)：

此按钮为清除所有目前路由器的 Log 相关信息。

7.2 系统状态实时监控(System Statistics)

路由器 的 System Statistics 管理功能可以提供系统目前运作信息，包含局域或广域埠名称，Status(目前埠联机状态)，IP Address(IP 地址)，MAC Address(网络实体位置)，Subnet Mask(子网掩码)，Default Gateway(预设网关)，DNS(名称解析服务器)，Network Service Detection(线路侦测机制)，Received Packets(接收封包数)，Sent Packets(传送封包数)，Total Packets(全部的进出封包数量)，Received Bytes(收到的封包 Byte 流量统计)，

Sent Bytes(传送的封包 Byte 流量统计)，Total Bytes(全部进出的封包 Byte 流量统计)，Error Packets Received(收到的错误封包统计)以及 Dropped Packets Received(埠丢弃的封包统计)，Current Session(联机数)，New Session(新联机数)，Upstream Bandwidth(上传频宽使用率)，Downstream Bandwidth(下载频宽使用率) 等信息。

日志 => 系统状态即时监控

	广域网1	广域网2	局域网
机器名称	ixp1	ixp2	ixp0
线路连线状态	联机	关闭	联机
IP地址	192.168.3.136	0.0.0.0	192.168.1.1
MAC地址	16-80-d0-20-fe-32	06-3b-19-20-76-29	2e-72-f7-43-23-c1
子网掩码	255.255.255.0	0.0.0.0	255.255.255.0
预设网关	192.168.3.1	0.0.0.0	---
域名解析服务地址(DNS)	192.168.3.10 192.168.3.2	0.0.0.0	192.168.1.1
线路侦测机制	测试成功	测试失败	---
接收封包统计	128691	0	71421
传送封包统计	62023	0	90108
全部封包统计	190714	0	161529
封包接收Byte数量	76406338	0	20733934
封包传送Byte数量	19544022	0	76186773
全部封包Byte数量	95950360	0	96920707
目前接收流量Bytes/Sec	0	0	2686
目前传送流量Bytes/Sec	0	0	3119
错误封包统计	0	0	0
丢弃封包统计	0	0	0
联机数	10	0	---
新联机数/秒	0	0	---
上传带宽使用率(%)	0	0	---
上传带宽使用率(%)	0	0	---

刷新

7.3 流量统计(Traffic Statistic)

路由器提供六种显示流量统计的信息，来提供管理者对于流量有更好的管理与控制。

对内 IP 流量统计 (Inbound IP Source Address)：

在此图表中显示了从外进入内网流量的来源端的 IP 地址，每秒有多少 byte 与所占的百分比。

对外 IP 流量统计 (Outbound IP Source Address)：

在此图表中显示了从内网出去流量的来源端的 IP 地址，每秒有多少 byte 与所占的百分比。

对内服务端口流量统计 (Inbound IP Service)：

在此图表中显示了以网络的服务端口来分类进入内网使用流量统计(每秒)byte 与百分比。

网络流量统计方式: 对内服务端口流量统计

通讯协议	目的端口	bytes/sec	%
TCP	443	529	100

对外服务端口流量统计 (Outbound IP Service)：

在此图表中显示了以网络的服务端口来分类从内网出去的使用流量统计(每秒)byte 与百分比。

网络流量统计方式: 对外服务端口流量统计

通讯协议	目的端口	bytes/sec	%
TCP	1863	66	100

对内联机流量统计 (Inbound IP session)：

在此图表中显示了从广域网络进来的(Dest. IP)地址所联机的局域网络的 IP(Source IP)位置所使用的服务端口(Dest.Port)还有现在使用流量(bytes/sec)与百分比。

网络流量统计方式: 对内联机流量统计

来源IP地址	通讯协议	来源端口	目的IP地址	目的端口	bytes/sec	%
192.168.1.100	TCP	3246	207.46.111.28	1863	62	88
192.168.1.100	TCP	3235	192.168.3.10	443	8	11

对外联机流量统计 (Outbound IP session)：

在此图表中显示了从局域网络的 IP(Source IP)地址对外联机的目的地位置(Dest. IP)IP 及所使用的服务端口(Dest.Port)还有现在使用流量(bytes/sec)与百分比。

网络流量统计方式: 对外联机流量统计

来源IP地址	通讯协议	来源端口	目的IP地址	目的端口	bytes/sec	%
192.168.1.100	TCP	3246	207.46.111.28	1863	66	100

7.4 特定 IP 及端口状态(Specify IP/Port Status)

路由器提供网管人员可以针对某一 IP 或某一特定 Port 去查询此 IP 去访问的目的地址，或是有哪些人使用这个服务端口。其目的可以方便找出某些需要认证的网站无法走 Multi-WAN 而必须走单一个 WAN 端口，网管人员可以查询出此目的地的 IP 做 Protocol Binding 绑定来解决此登入问题。另外，若想查询何人在使用 BT 或 P2P 软件，也可选择 Port 做使用者查询。

特定 IP 状态：

直接在 IP 地址里填入您想要查询的 IP 地址，就可以显示出此 IP 对外联机的所有目的地及 Port Number。

来源IP地址	通讯协定	来源服务端口	接口位置	目的IP地址	目的服务端口	下载频宽 Bytes/Sec	上传频宽 Bytes/Sec
192.168.1.100	TCP	2197	WAN1	192.168.3.10	443	0	0
192.168.1.100	TCP	2212	WAN1	192.168.3.10	443	0	0
192.168.1.100	TCP	3003	WAN1	207.46.26.35	1863	0	0
192.168.1.100	TCP	3223	WAN1	192.168.3.10	443	8	30
192.168.1.100	TCP	3224	WAN1	192.168.3.10	443	18	4
192.168.1.100	TCP	3234	WAN1	192.168.3.10	443	4	8
192.168.1.100	TCP	3235	WAN1	192.168.3.10	443	0	0
192.168.1.100	TCP	3246	WAN1	207.46.111.28	1863	0	0
192.168.1.100	TCP	3316	WAN1	61.62.57.249	1651	0	0
192.168.1.100	TCP	3322	WAN1	140.135.89.122	2618	0	0

特定埠状态：

直接在「端口」里填入您想要查询的端口号码，就可以显示出此端口现在有哪些 IP 正在使用。

查询方式依 端口 端口：80 查询

来源IP地址	通讯协定	来源服务端口	接口位置	目的IP地址	目的服务端口	下载频宽 Bytes/Sec	上传频宽 Bytes/Sec
192.168.1.100	TCP	3496	WAN1	66.94.234.13	80	0	0
192.168.1.100	TCP	3497	WAN1	202.43.195.52	80	604	18
192.168.1.100	TCP	3498	WAN1	202.43.195.52	80	4	4
192.168.1.100	TCP	3499	WAN1	202.43.197.140	80	5951	513
192.168.1.100	TCP	3500	WAN1	202.43.197.140	80	3361	408
192.168.1.100	TCP	3501	WAN1	74.6.155.239	80	169	70
192.168.1.100	TCP	3502	WAN1	74.6.155.239	80	295	78
192.168.1.100	TCP	3503	WAN1	74.6.155.239	80	394	78
192.168.1.100	TCP	3504	WAN1	203.84.196.97	80	3080	102
192.168.1.100	TCP	3505	WAN1	74.6.155.239	80	265	63
192.168.1.100	TCP	3506	WAN1	203.84.196.242	80	72	56
192.168.1.100	TCP	3507	WAN1	202.43.195.52	80	63	61
192.168.1.100	TCP	3508	WAN1	203.84.204.69	80	54	163
192.168.1.100	TCP	3509	WAN1	203.84.204.69	80	62	247

八、注销(Logout)

路由器的网页画面右上方有一个注销(Logout)的按钮，此按钮为终止管理路由器并结束此管理画面。若您下次想再进入路由器管理画面时，您必须重复进入路由器管理画面的步骤，并再输入管理者使用名称与密码。

附録一： 常见问题解决

注意！
以下是几个常见问题的解决方法，如果有其它的问题出现可以在讨论区寻找信息以及联系技术服务人员，具体方法可以参照附録五：Qno 技术支持信息寻找相关信息以及联系相关技术服务人员，以取得更详细的资料参照。

（1） 阻挡基本 BT 下载方式

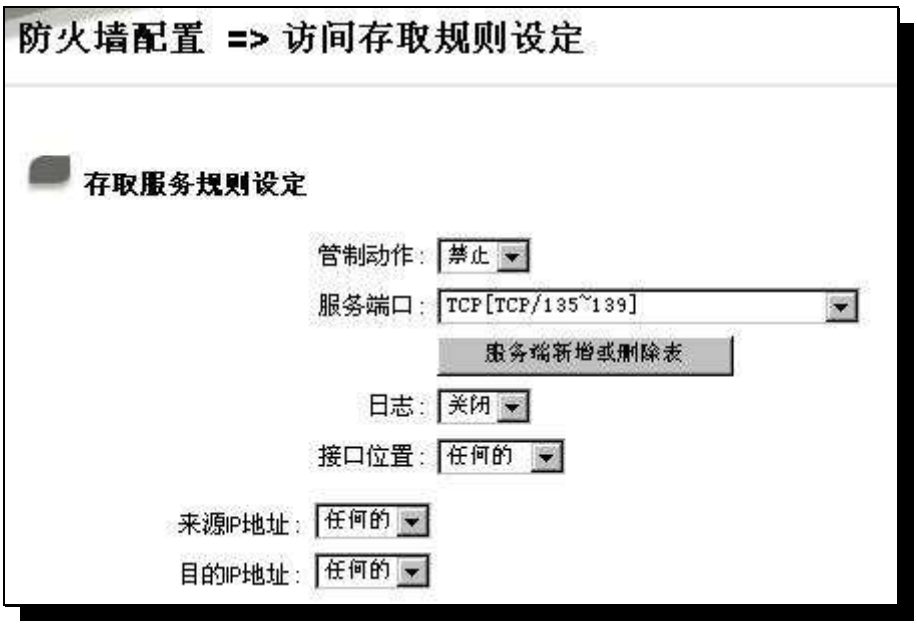
若您想要封锁 BT 种子，不让用户下载，您可以直接在“防火墙配置”有一个“网页内容管制设定”选取“开启网页内容管制功能”后将启动网页字符串管制，打入“.torrent”就可以防止用户下载种子。

（2） 冲擊波及蠕虫病毒的防制

由于近来还是发生有许重使用者内网中冲擊波及蠕虫病毒造成内网存取 Internet 很慢及联机数(Session)大量增加造成路由器大量处理. 所以以下为指导您封锁此病毒相应通讯端口以达到防制目的。

a.增加此 TCP135-139， UDP135-139 还有 TCP445 通讯端口：

b.用防火墙里面的“存取规则”功能将设定好的此三组通讯端口封锁：



用同樣的方法添加好 UDP[UDP135~139]以及 TCP[445~445]通讯端口。

c.将这三组的优先级至于最高：

（3）ARP 病毒攻擊防制

1）. ARP 问题的提出以及相关知识

近期，国内多家网吧出现短时间内断线(全断或部分断)的现象，但会在很短的时间内会自动回复。这是因为 MAC 地址冲突引起的，当带毒机器的 MAC 对映到主机或者路由器之类的 NAT 装置，那么全网断线，如果只对映到网内其它机器，则只有这部分机器出问题。多发于传奇游戏特别是外挂等方面。此类情况就是网络受到了 ARP 病毒攻擊的明显表现，其目的在于，该病毒破解游戏加密解密算法，通过截取局域网络中的数据包，然后解析游戏通讯协议的方法截获用户的信息。执行这个病毒，就可以获得整个局域网络中游戏玩家的详细信息，盗取用户账号信息。下面我们谈谈如何防制这种攻擊。

首先，我们了解下**什么是 ARP**，ARP “Address Resolution Protocol”（地址解析协议），局域网络中，网络中实际传送的是“讯框”，讯框里面是有目标主机的 MAC 地址的。所谓“地址解析”就是主机在传送讯框前将目标 IP 地址转换成目标 MAC 地址的过程。ARP 协议的基本功能就是通过目标装置的 IP 地址，查询目标装置的 MAC 地址，以保证通讯的顺利进行。

ARP 协议的工作原理：在每台安装有 TCP/IP 协议的计算机里都有一个 ARP 缓冲区表，表里的 IP 地址与 MAC 地址是一一对应的，如表所示。

IP 址	MAC 地址
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
……	……

我们以主机 A（192.168.1.5）向主机 B（192.168.1.1）传送数据为例。当传送数据时，主机 A 会在自己的 ARP 缓冲区表中搜寻是否有目标 IP 地址。如果找到了，也就知道了目标 MAC 地址，直接把目标 MAC 地址写入讯框里面传送就可以了；如果在 ARP 缓冲区表中没有找到相对应的 IP 地址，主机 A 就会在网络上传送一个广播，目标 MAC 地址是“FF.FF.FF.FF.FF.FF”，这表示向同一网段内的所有主机发出这样的询问：“192.168.1.1 的 MAC 地址是什么？”网络上其它主机并不响应 ARP 询问，只有主机 B 接收到这个讯框时，才向主机 A 做出这样的因应：“192.168.1.1 的 MAC 地址是 00-aa-00-62-c6-09”。这样，主机 A 就知道了主机 B 的 MAC 地址，它就可以向主机 B 传送信息了。同时它还更新了自己的 ARP 缓冲区表。

再者，我们先简单介绍一下什么是 ARP 病毒攻擊，这种病毒是对内网的 PC 进行攻擊，使内网 PC 机的 ARP 表混乱，在局域网络中，通过 ARP 协议来完成 IP 地址转换为第二层实体地址（即 MAC 地址）的。ARP 协议对网络安全具有重要的意义。通过虚拟造 IP 地址和 MAC 地址实现 ARP 欺骗，能够在网络中产生大量的 ARP 通讯量使网络阻塞。用虚拟造源 MAC 地址传送 ARP 响应包，对 ARP 高速缓冲区机制的攻擊。这些情况主要出现在网咖用户，造成网咖部分机器或全部机器暂时中断联机或者不可以上网，在重新启动后可以解决，但保持不了多久又会出现这样的问题，网咖管理员对每台机器使用 arp －a 指令来检查 ARP 表的时候发现路由

器的 IP 和 MAC 被修改，这就是 ARP 病毒攻擊的典型症状。

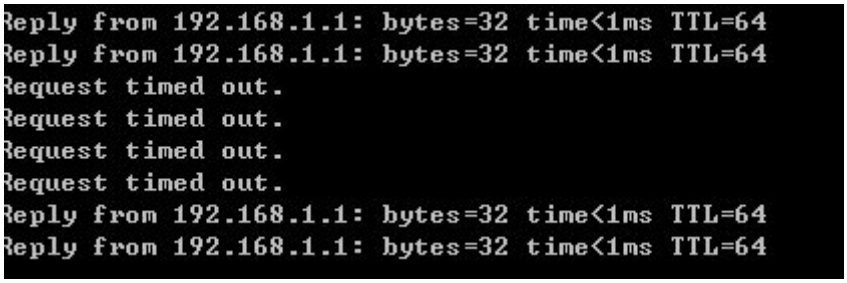
这种病毒的程序如 PWSteal.lemir 或其变种，属于木马程序/蠕虫类病毒，Windows 95/98/Me/NT/2000/XP/2003 将受到影响，病毒攻擊的方式对影响网络联机畅通来看有两种，对路由器的 ARP 表的欺骗和对内网 PC 网关的欺骗，前者是先截获网关数据，再将一家族的错误的内网 MAC 信息不停的传送给路由器，造成路由器发出的也是错误的 MAC 地址，造成正常 PC 无法收到信息。后者 ARP 攻擊是虚拟造网关。它先建立一个假网关，让被它欺骗的 PC 向假网关发数据，而不是通过正常的路由器途径上网。在 PC 看来，就是上不了网了，“网络中断联机了”。

就这两种情况而言，如果对 ARP 病毒攻擊进行防制的话我们必须得做路由器方面和客户端双方的设定才保证问题的最终解决。所以我们选取路由器的话最好看看路由器是否带有防制 ARP 病毒攻擊的功能，Qno 产品正好提供了这样的功能，相比其它产品作业简单易学。

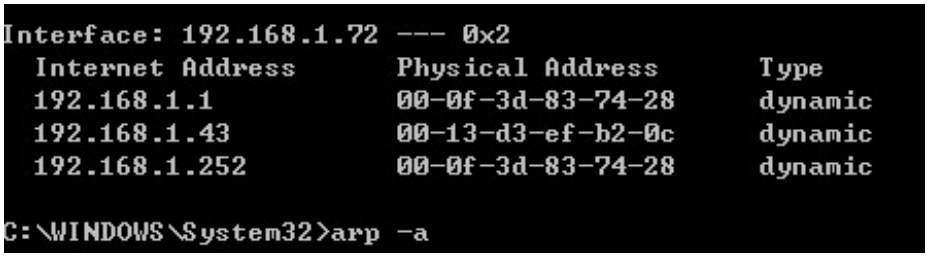
2）. ARP 的判断

如过网络中有一台或多台计算机受到或已经感染了 ARP 病毒，我们就必须学会判断并采取相应的解决方法处理类似问题的发生，下面来谈谈 Qno 技术工程师的 ARP 防制经验谈。

通过对 ARP 工作原理得知，如果系统 ARP 缓冲区表被修改不停的通知路由器一家族错误的内网 IP 或者干脆虚拟造一个假的网关进行欺骗的话，网络就肯定会出现大面积的中断联机问题，这样的情况就是典型的 ARP 攻擊，对遭受 ARP 攻擊的判断，其方法很容易，你找到出现问题的计算机点开始执行进入系统的 DOS 作业。ping 路由器的 LAN IP 丢包情况。输入 ping 192.168.1.1（网关 IP 地址），如图。



内网 ping 路由器的 LAN IP 丢几个包，然后又连上，这很有可能是中了 ARP 攻擊。为了进一步确认，我们可以通过寻找 ARP 表来判断。输入 ARP -a 指令，显示如下图。



可以看出 192.168.1.1 地址和 192.168.252 地址的 IP 的 MAC 地址都是 00-0f-3d-83-74-28，很显然，这就是 ARP 欺骗造成的。

3）. ARP 的解决

我们现在已经理解了 ARP，ARP 欺骗攻擊以及如何判断此类攻擊，下面的问题就是如何找到行之有效的防制办法来防止这类攻擊对网络造成的危害。Qno 的一般处理办法分三个步骤来完成。

a)、启动防止 ARP 病毒攻击：

输入路由器 IP 地址登入路由器的 Web 管理页面，进入“防火墙配置”的“基本页面”，再在右边找到“防止 ARP 病毒攻擊”在这一行的“启动”前面做点选，再在页面最下点擊“确认”，如图。

b)、对每台 pc 上绑定网关的 IP 和其 MAC 地址

进行这样的作业主要防止 ARP 欺骗网关 IP 和其 MAC 地址首先在路由器端寻找网关 IP 与 MAC 地址，如图。

然后在每台 PC 机上开始/执行 cmd 进入 dos 作业，输入 arp －s 192.168.1.1 2e-72-f7-43-23-c1，Enter 后完成 pc01 的连结。如图

针对网络内的其它主机用同样的方法输入相应的主机 IP 以及 MAC 地址完成 IP 与 MAC 连结。但是此动作，如果重起了计算机，作用就会消失，所以可以把此指令做成一个批处理档案，放在操作系统的启动里面，批处理档案可以这样写：

@echo off

arp -d

arp -s 路由器 LAN IP　路由器 LAN MAC

对于已经中了 arp 攻擊的内网，要找到攻擊源。方法：在 PC 上不了网或者 ping 丢包的时候，在 DOS 下打 arp －a 指令，看显示的网关的 MAC 地址是否和路由器真实的 MAC 相同。如果不是，则寻找这个 MAC 地址所对应的 PC，这台 PC 就是攻擊源。

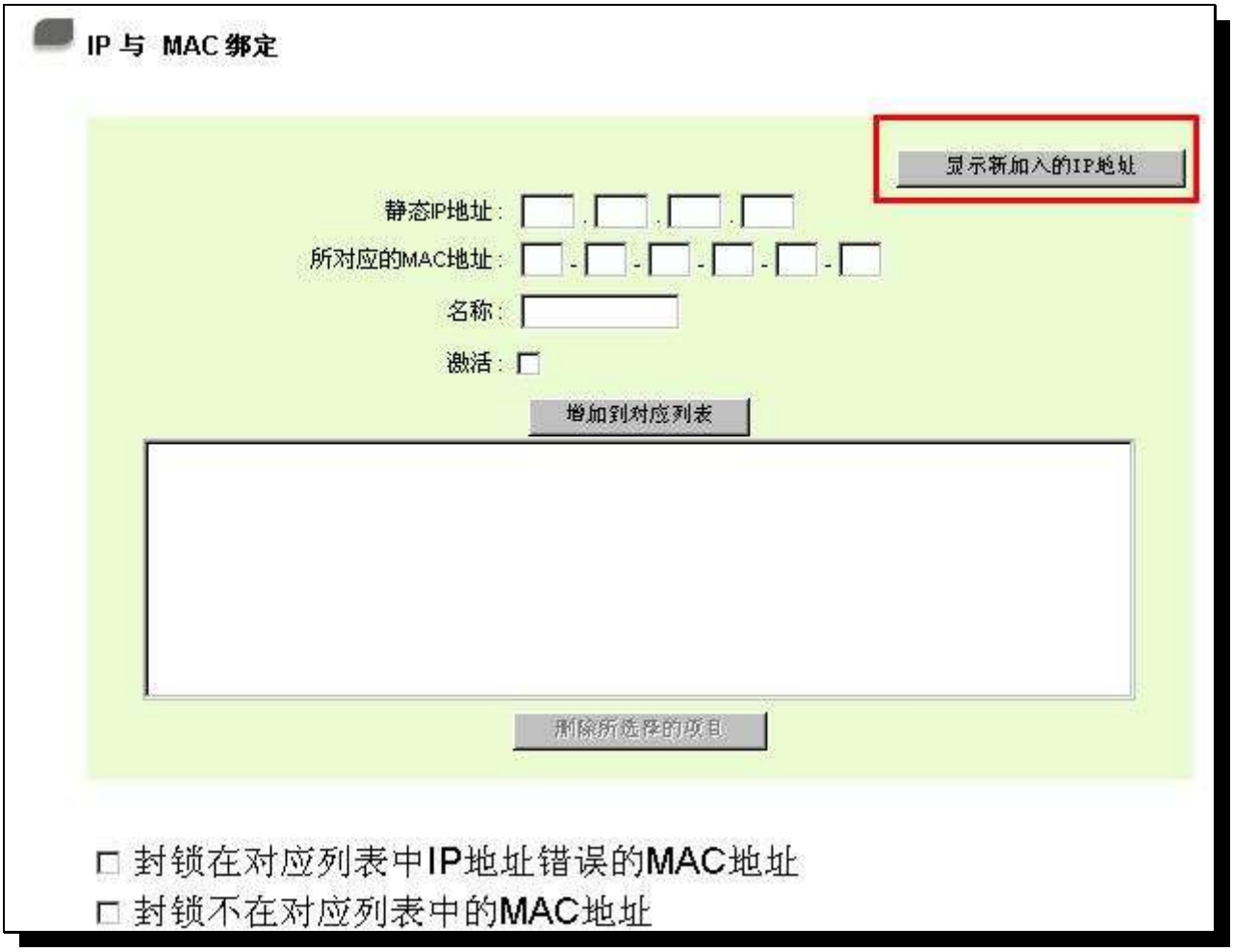
其它的路由器用户的解决方案也是要在路由器和 PC 机端进行双向连结 IP 地址与 MAC 地址来完成相应防制工作的，但在路由器端和 PC 端对 IP 地址与 MAC 地址的连结比对复杂，需要寻找每台 PC 机的 IP 地址与 MAC 加大了工作量，作业过程中还容易出错。

c)、在路由器端绑定用户 IP/MAC 地址：

进入“DHCP 功能”的“DHCP 配置”，在这个页面的右下可以看到一个“IP 与 MAC 连结”你可以在此添加 IP 与 MAC 连结，输入相关参数，在“启动”上点勾选再“添加到对应清单”，重复作业添加内网里的其它 IP 与 MAC 的连结，再点页面最下的“确定”。

当添加了对应清单之后，其对应的信息就会在下面的白色框里显示出来。不过建议不采用此方法，这样作业需要查询网络内所有主机 IP/MAC 地址工作量繁重，还有一种方法来绑定 IP 与 MAC，作业会相对容易，可以减少大量的工作量，节约大量时间，下面就会讲到。

进入“DHCP 功能”的“DHCP 配置”找到 IP 与 MAC 绑定右边有一个“显示新增的 IP 地址”点擊进入。



点擊之后会即现 IP 与 MAC 绑定清单对话框，此对话框里会显示网内未做绑定的 pc 的 IP 与 MAC 地址对应情况，输入计算机“名称”和“启动”上勾选，再在右上角点确定。

此时你所绑定的选项就会出现在 IP 与 MAC 绑定清单框里，如图 5 再点擊“确认/确定”绑定完成。

但是我们单靠这样的作业基本可以解决问题，但 Qno 的技术工程师建议通过进一步通过一些手段来进一步控制 ARP 的攻擊。

1、病毒源，对病毒源头的机器进行处理，杀毒或重新装系统。此作业比较重要，解决了 ARP 攻擊的源头 PC 机的问题，可以保证内网免受攻擊。

2、网吧管理员检查局域网络病毒，安装防毒软件，对机器进行病毒扫描。

3、给系统安装修正程序。通过 Windows Update 安装好系统修正程序(关键更新、安全更新和 Service Pack

4、给系统管理员帐户设定足够复杂的强密码，最好能是 12 位以上，字母+数字+象征式的组合；也可以禁用/移除一些不使用的帐户。

5、经常更新防毒软件（病毒链接库），可设定为每天定时自动更新。安装并使用网络防火墙软件 ，网络防火墙在防病毒过程中也可以起到至关重要的作用，能有效地阻挡自来网络的攻擊和病毒的入侵。部分盗版 Windows 用户无法正常安装修正，不妨通过使用网络防火墙等其它方法来做到一定的防护。

6、关闭一些不需要的服务，条件允许的可关闭一些没有必要的共享，也含括 C$、D$等管理共享。完全单机的用户也可直接关闭服务器的共享服务。

7、不要随便点擊开启 QQ、MSN 等聊天工具上发来的链接信息，不要随便开启或执行陌生、可疑档案和程序，如邮件中的陌生装置，外挂程序等。

4）. 总结

ARP 攻擊防制是一个任重而道远的过程，以上方法基本可以解决 ARP 病毒攻擊对网络造成相关问题，而且用户采取类似的方法也收到了很大的效果，但网络管理人员还是要高度重视这个问题，而且不能大意，我们可以采取以上建议随时警惕 ARP 攻擊，以减少受到的危害，提高工作效率，降低经济损失。

附録二：Qno 技术支持信息

更多有关侠诺产品技术信息可以联系侠诺各经销商技术部门以及侠诺技术中心。

侠诺技术中心：

E-mail：QnoFAE@qno.com.tw