your future life

5WAN 5LAN ALL Gigabit QoS Router

全千兆 QoS 安全旗舰路由

具负载平衡，带宽管理，网络安全等功能

简体中文使用手册

www.Qno.cn

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

一、简介 1
二、多 WAN 路由器配置操作流程 3
2.1 系统性配置流程的需要 3
2.2 配置流程表 3
三、硬件安装 5
3.1 路由器 LED 显示灯 5
3.2 连接路由器到您的网络上 7
四、登录路由器 8
五、确定设备规格、状态显示以及登录密码和时间的设定 10
5.1 首页显示 10
5.2 登录密码及时间的修改和设定 15
六、进行网络连线配置 18
6.1 网络设定 18
6.2 多 WAN 设定 34
七、内部局域网络配置 52
7.1 网络端口管理配置 52
7.2 网络端口状态实时显示 54
7.3 DHCP 发放 IP 服务器 55
7.4 DHCP 状态显示 57
7.5 IP 及 MAC 地址绑定 58
7.6 IP 与服务通讯端口群组管理 62
7.7 服务通讯端口 群组管理 65
八、QoS 带宽管理功能 67
8.1 带宽设置(QoS) 68
8.2 联机数管控 79
8.3 硬件加速服务 82
九、防火墙配置 84
9.1 基本设置 84
9.2 访问规则设置 90
9.3 网页内容管制 94
十、其它进阶高级功能设置 99
10.1 DMZ/虚拟服务主机 99
10.2 路由通讯协议 104

10.3 一对一 NAT 对应 107
10.4 DDNS-动态域名解析 110
10.5 广域网接口 MAC 地址设定 112
十一、工具程序功能设定 113
11.1 在线联机测试 113
11.2 系统固件升级 115
11.3 系统设定参数存储 116
11.4 SNMP 网络管理设定 117
11.5 系统恢复 119
11.6 备援功能 121
十二、日志功能设定 125
12.1 系统日志 125
12.2 系统状态实时监控 128
12.3 流量统计 129
12.4 特定 IP 及端口状态 130
12.5 QRTG (Qno Router Traffic Grapher) 132
十四、注销 137
附录一、配置界面及使用手册章节对照 138
附录二：产品中有毒有害物质或元素表 140
附录三：常见问题解决 141
（1） QQ 容易掉线问题 141
（2） 挡基本 BT 下载方式 143
（3） 冲击波及蠕虫病毒的防制 144
（4） 阻止 QQLive 视屏直播设定 146
（5） ARP 病毒攻击防制 148
附录四：Qno 技术支持资讯 156

一、简介

新一代全千兆 QoS 安全旗舰路由是因应高效能路由器市场需求，为满足网吧大型化、宽带应用增加、带宽管理需要而设计的经济实惠且高效能整合的全功能千兆网络安全路由器。新一代全千兆网络安全路由器，针对中国多运营商环境及用户带宽管理需求，结合千兆骨干组网方案，支持硬件端口镜像、智能型带宽管理、多 WAN 负载均衡、线路备援、强效防火墙、等功能。

具备 5 个千兆骨干 WAN 连接端口，并具有高效能线路负载平衡模式的功能，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。此外，DMZ 端口可以连接具有公网 IP 地址的对外服务器。局域端内建 5 个千兆骨干 LAN 连接端口，自适应 10/100/1000Mbps 以太网络交换器，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，方便建立千兆骨干，加速企业网络效能，带宽成长空间大。提供硬件 USB 人性化界面，将来可以外接支持 USB 相关的装置，扩充功能或数据储存容量等。

独特的 QoS 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的金钱，也不会因为少数几人的下载而强占所有的带宽，造成内部的抱怨。简化了用户设置，不需要一一设规则，即可依整体使用情况，优化带宽利用，并只针对大量占用者加以限制，节省运算资源，可达成最有效率的运用。同时提供智能带宽管理通过简单的设置完成内网带宽管理，达到有效率的带宽使用，简化管理，提高工作效率。

本系列旗舰路由更具备了独家的硬件加速服务，将带宽管理、优化流量使用分配等相关动作，直接以硬件执行，除了可达到保障并加速内网的重要服务流量的使用，即使是在带宽全部满载的状况下，仍然可以顺畅的使用这些重要的服务不会中断；更可以大幅减少 CPU 与整体系统资源的消耗，使路由器更能承受庞大的连线数量与计算机数量，提供绝佳且稳定的网络使用环境。

负载均衡模式支持智能线路、IP 地址、策略路由三种带宽均衡模式，提供弹性灵活的网络联机需求设置，来进行流量的负载均衡控制，可保证所有线路畅通。策略路由设置简化无需导入 IP 地址文件，自动判别对外网络数据包，分流电信网通线路，确保跨网联机反应快速、通行无碍，可汇聚同运营商的线路带宽，作负载均衡控制，大大提升网络资源运用的灵活度。

强效的防火墙系统，以满足多数企业对防御外部网络攻击的市场需求。主动式封包检测功能，经由对网络层联机的动态俭测，拒绝或阻挡非标准通信协议的联机要求。只需单向启动各式黑客攻击、蠕虫病毒、ARP 攻击防护功能，即可简易完成配置，有效防止内外网恶意攻击，确保网络安全。防火墙系统除了 NAT 之外，还具备有防止阻断服务攻击。功能完整的存取规则设定，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。

网络地址转换(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 就可以让多人同时连上网络。局域网内的 IP 地址支持 Class B 等级，DHCP 自动分配 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。

此说明书主要是用来说明每一个功能的设定方法与细节，若是您对于路由器如何连上网络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网络，并在必要时取得技术人员的远程支持。您可上网 www.Qno.cn 进行在线登录，技术支持部份可登录 http://www.Qno.cn/forum/，以取得最新侠诺产品信息及应用实例，更加善用您的侠诺产品。

此为 FCC Class A 级产品，在生活环境中该产品可能会造成无线电干扰，在这种情况下可能需要用户对其干扰采取确实可行措施。

二、多 WAN 路由器配置操作流程

本章节介绍用户整体配置多 WAN 路由器操作流程，通过对路由器多 WAN 配置流程的了解可以很轻松的配置我们的网络，来有效的管理我们的网络，使路由器达到应有的功能，使路由器的效能达到最高。

2.1 系统性配置流程的需要

用户可以通过以下操作流程配置我们的网络，能够使我们的网络能够有效利用带宽，网络效能达到理想的效果，同时可以阻断一些攻击与预防一些安全隐患，通过流程配置更加方便用户的安装与操作，简化维护管理的难度，使得用户的网络配置一次到位。配置主要流程如下：

1、 硬件安装。

2、 登录配置窗口。

3、 确定设备规格及进行密码和时间设置。

4、 进行广域网联机的配置：进行内部联机的配置。

5、 进行内部联机的配置：实体线路配置及 IP 地址配置

6、 进行 QoS 带宽管理配置：防止带宽占用情况。

7、 进行防火墙配置：预防攻击及不当存取网络资源。

8、 其它特别配置：开放服务器、UPnP、DDNS、MAC 克隆。

9、 管理维护的配置系统日志、SNMP、及设定参数备份注销配置窗口。

10、 注销配置窗口

2.2 配置流程表

下表主要阐述每个配置流程相对应的路由器管理内容以及此配置所达到的目的，如需详细了解每步过程以及后面章节介绍所对应的内容可参考（附录一、配置界面及使用手册章节对照）。

#	配置	内容	目的
1	硬件安装	构造用户需要的网络	根据用户实地网络的要求来安装路由器硬件。

2	登录配置窗口	从计算器 Web 接入路由器配置窗口，了解系统信息	登录路由器的 Web 管理页面。
3	确定设备规格	确定产品软件版本以及路由工作情况	确定路由器规格，系统软件版本，以及路由器工作状况。
	进行密码及时间设置	设定时间及修改密码	安全的考虑修改登录密码。 设定路由器时间与广域网络同步。
4	进行广域网联机的配置	确定广域网线路配置、带宽调配、及协议绑定	连接广域网络，通过带宽的配置等能更好的利用带宽，优化数据转发能力。
5	进行内部联机的配置：实体线路配置及 IP 地址配置	端口镜像及 VLAN 配置。内部用户 IP 的分配群组及管理	应地区需求提供端口镜像功能，同时改进端口管理及 VLAN 的配置满足内网相关需求，弹性提供固定 IP/DHCP 自动 IP 地址分配，方便用户在不同网络环境的需要。IP 群组管理对一组 IP 地址做相同配置，简化管理工作。
6	进行 QoS 带宽管理配置，防止带宽占用情况的发生	广域网端口、内部用户或应用流量及联机数的限制	确保网络重要信息不致延迟、确保网络重要应用服务联机顺畅；进一步针对现有的带宽进行管理运用，让有限的带宽资源发挥最大的效用。
7	进行防火墙配置，预防攻击及不当存取网络资源	攻击阻挡、访问规则及网页存取限制	当内网用户使用 BT、点点通影响其它人上网、员工上班时间不正当上网以及使用 MSN、QQ、Skype 影响工作效率；当网速因被黑客攻击而受影响或内网用户常被蠕虫及 ARP 软件所苦；网管可依据需求设置内外网络存取规则，以进一步管控员工个别上网行为。
8	其它特别配置：开放服务器、UPnP、DDNS、MAC 克隆	针对内部设定开放服务器、UPnP、路由模式、多广域网 IP、DDNS、Mac 克隆	高级管理配置完成对网络的更高一步要求，构建内部开放服务器，虚拟服务器，UPnP 通讯协议的设置，配置动态路由或者静态路由，一对一 NAT 配置，动态域名解析服务与 Mac 地址克隆。
9	管理维护的配置：系统日志、SNMP、及设定参数备份	路由器工作情况监测、系统参数的备份	网管可藉此功能查看系统日志、即时监控系统状态及内外流量，确保内网运作无误。
10	注销配置窗口	离开配置窗口	注销退出路由器 Web 管理页面。

下面我们就根据这个流程来配置完成我们的网络设置。

三、硬件安装

本章介绍产品的硬件接口以及实体安装。

3.1 路由器 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.
DMZ-DMZ 口联机状态	绿灯	绿灯亮： 以太网络联机正常 绿灯闪烁： 以太网络端口正在传送/接收封包数据传输
100M-百兆	橘灯	橘灯亮： 以太网络联机在 100Mbps 的速度
1000M-千兆	绿灯	绿灯亮： 以太网络联机在 1000Mbps 的速度
WAN1 ~ WAN5-广域端口	绿灯	绿灯亮： 广域端口 WAN 口已经联机并取得 IP 地址

硬件恢复 (Reset) 按键

动作	意义
点击 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
点击 Reset 按钮 10 秒以上	恢复原出厂默认值 DIAG 灯号： 橘色灯号快闪

系统内建电池

路由器内建有系统时间的电池，此电池的寿命约为 1～2 年，当电池已经无法充电或是使用寿命到达后，路由器将无法记录时间或是连接互联网同步 NTP 时间服务器。您必须与您的供应商联系，以便取得更换电池技术。

注意！

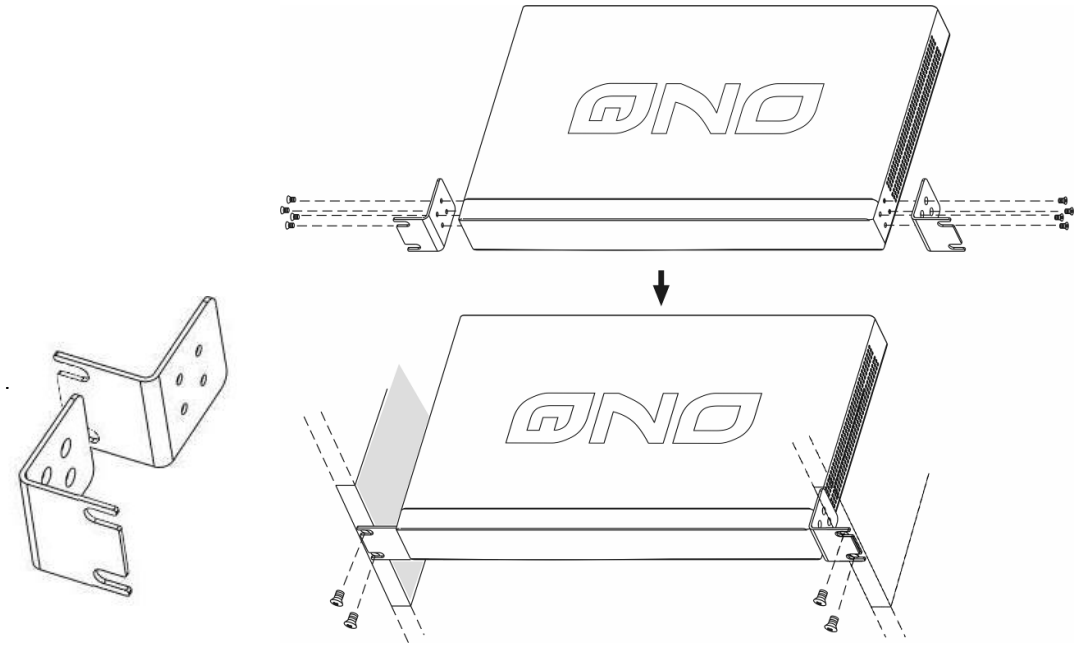
为了产品的正常运行，请勿自行更换电池，以免造成产品无法恢复的损坏！

将路由器安装在 19”标准机架上

建议您可以将路由器放置于桌上使用，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。

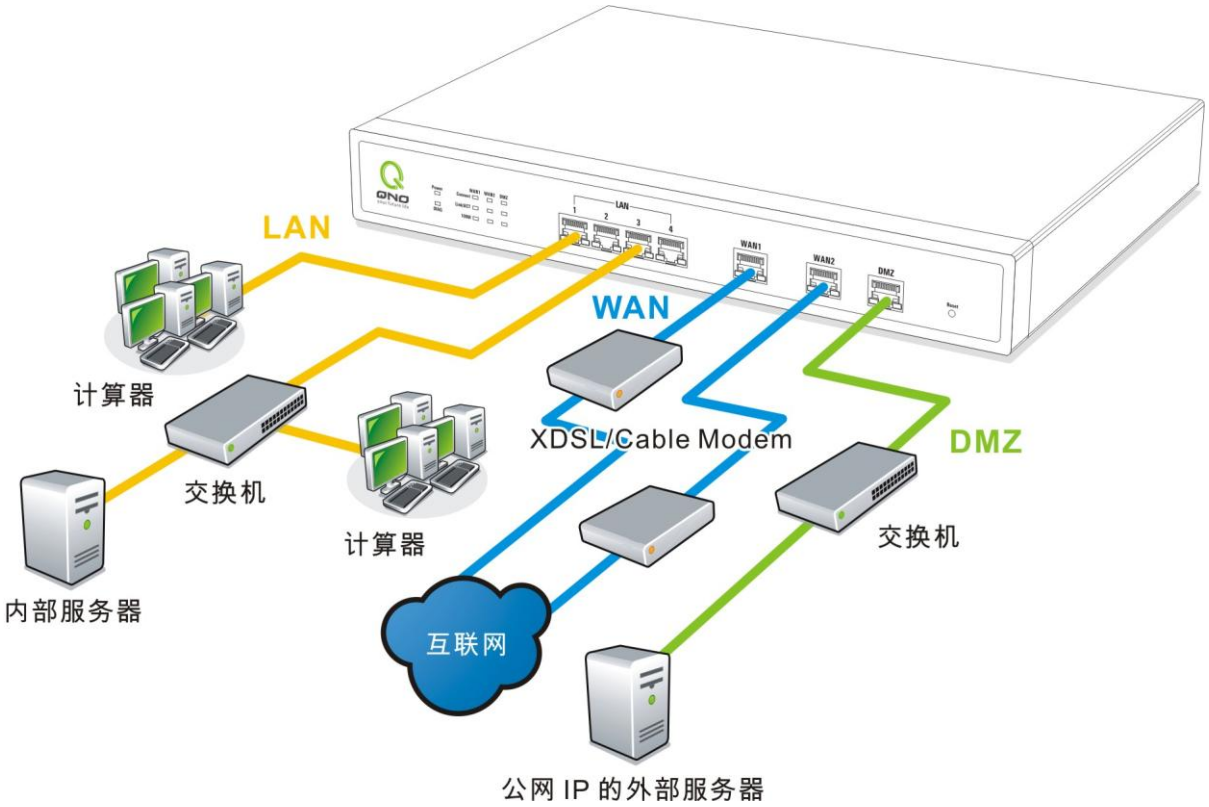
每一台路由器都有配备专用连接机架配件，包含 2 只 L 型锁附架以及八颗专用螺丝，用来将路由器安装在机架上使用。安装于您的 19 吋标准机架上的方法如下图所示：



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！

3.2 连接路由器到您的网络上



广域网络联机：WAN 端口可以连接如 xDSL Modem 等接入互联网。

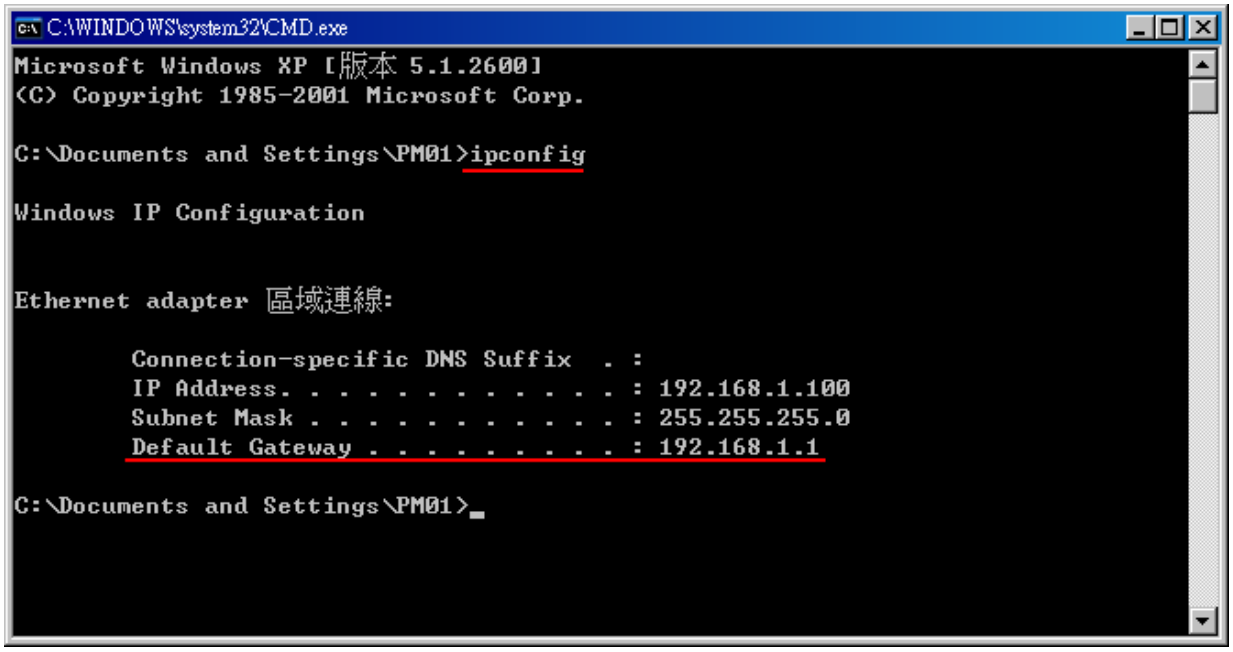
局域网络联机：LAN 端口可以连接如 Switch HUB 或是 PC 联机及内部服务器。LAN 1 端口可以设定为镜像端口，请在“网络端口管理”中做设定，设定完成即可直接将监控或过滤服务器接在此端口使用。

DMZ 端口：此端口可以连接如 Switch HUB 或是具有外部合法 IP 地址的服务器，如网页服务器以及电子邮件服务器等。

四、登录路由器

本章主要是在客户连接好路由器后，通过连接路由器的计算机登录路由器的 Web 管理页。

首先在连接到路由器 LAN 端的计算机（确定计算机是自动获得 IP 地址）上的 DOS 下查找路由器的 IP 地址，点开始→运行，输入 cmd 进入 DOS 操作，再输入 ipconfig→确认，查到默认网关（Default Gateway）地址如图，192.168.1.1。确认默认网关也就是路由器的默认 IP 地址。



注意！

当 “ipconfig” 不能获得 IP 地址以及默认网关的情况，或者获得的 IP 地址为 0.0.0.0 以及 169.X.X.X 的情况，就是路由器并没有分配到 IP 地址，建议用户检查线路是否有问题，计算机网卡是否接好等。

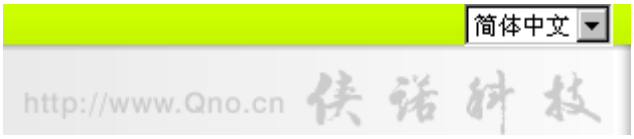
然后开启网页浏览器 (如 IE)，在网址栏输入 192.168.1.1 (路由器的默认网关)，会出现以下的登录窗口：

路由器路由器默认的使用者名称(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录密码。

注意！

为了安全，我们强烈建议您务必在登录之后更改管理密码！密码请牢记，若是密码忘记，将无法再登录至路由器的设定窗口，必须点击面板上的 Reset 按键十秒以上，恢复到出厂值，其所有配置将需要重新设定。

登录后，就会显示路由器的 Web 管理页面，在其页面的右上角选择路由器操作的语言模式，选中的图标将变成蓝色，这里选择“**简体**”（简体中文版本），如图。



五、确定设备规格、状态显示以及登录密码和时间的设定

本章介绍登录软件设定窗口后进入首页可以了解到的设备规格以及设备工作状态信息，还有因安全考虑需要用户即时修改登录密码与系统时间设定。

5.1 首页显示

首页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。

5.1.1 系统信息

广域网 P 地址(WAN1～5 IP)： 此为显示路由器路由器的 WAN 端目前的 IP 地址信息。

预设网关 IP 地址： 此为显示 ISP 分配给路由器路由器 WAN1～WAN5 的网关 IP 地址信息。

域名解析服务地址： 此为显示路由器的 DNS 的 IP 地址信息。

联机状态： 此为显示路由器路由器每个 WAN 目前的联机数目。

下载带宽使用率： 此为显示路由器路由器每个 WAN 目前的下载带宽使用比例。

上传带宽使用率： 此为显示路由器路由器每个 WAN 目前的上传带宽使用比例。

动态域名解析： 此为显示路由器的 DDNS 是否启动的状态信息。系统默认此功能为关闭。

网络质量服务配置(QoS)： 此为显示路由器的网络质量服务(QoS)是否开启。

手动联机： 当使用者选择自动取得 IP 地址时，他会显示二个按钮分别为释放与更

新。使用者可以点击释放按钮去做释放 ISP 端所核发的 IP 地址，以及点击更新按钮去做更新 ISP 端所核发的 IP 地址。当选择 WAN 端联机使用如 PPPoE 或是 PPTP 的话，它会变为显示“连机”与“中断”。

DMZ IP 地址 (WAN/DMZ 切换)： 此为显示路由器 DMZ 目前的 IP 地址设定信息。

5.1.2 硬件端口状态实时显示

端口即时状态

端口号	1	2	3	4	5
接口位置	局域网				
状态	联机	联机	联机	联机	联机

端口号	Internet	Internet	Internet	Internet	Internet
接口位置	WAN1	WAN2	WAN3	WAN4	WAN5
状态	联机	联机	联机	联机	联机

此窗口会显示系统各端口目前实时状态：(**联机**-已经连接，**激活**-此端口处于开启状态，**关闭**-此端口处于关闭状态)。您可以点击此状态按钮，在弹出的窗口中查看各端口更详细的资料显示。如下图：

广域网1信息

摘要信息

网路连接状态	10Base-T / 100Base-TX / 1000Base-T
接口位置	广域网
线路连线状态	激活
端口即时状态	端口激活
优先权	一般
网路连接速率	100 Mbps
半双/全双工模式	全双工
自动侦测模式	激活

流量即时显示

接收封包统计	84684951
封包接收Byte数量	18446744072983501965
传送封包统计	78205205
封包传送Byte数量	18446744072527202969
错误封包统计	0

刷新 关闭

此表会显示目前该端口设定状态，如网路连接状态(10Base-T/100Base-TX/1000Base-T)，接口位置(广域网 1 ～5 / 局域网 1 ～5/DMZ)，线路连接状态(激活/关闭)，端口配置状态(端口激活/端口关闭)，高低优先权(高级/一般)，网络连接速率(10Mbps/100Mbps)，工作模式(半双工/全双工)，以太网自动侦测(激活/关闭) 。 于此项目表格中，会显示此端口的接收和传送的封包数以及封包传送 Byte 数及封包错误率等并计算总数量。

5.1.3 本机信息

局域网接口 IP 地址： 此为显示路由器路由器本身的 LAN 端目前 IP 地址，系统默认为 192.168.1.1。

工作模式： 此为显示路由器的目前工作模式(可为 NAT 模式或是路由模式)。系统默认此功能为 NAT Gateway 模式。

主机工作时间：此为显示路由器 目前已经开机的时间。

主机序列号：此为显示路由器 的产品序号。

硬件版本信息： 此为显示路由器 目前使用的硬件版本。

目前正确时间：此显示路由器 目前正确时间，但必须注意，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。

CPU 使用率：目前路由器消耗 CPU 的使用率。

实体记忆体使用率：目前路由器消耗实体记忆体的使用率。

目前总连线数量：目前路由器网络连线总数。

5.1.4 网络安全信息

网路安全讯息

防火墙配置	状态
SPI主动封包检测	激活
防止DoS攻击	激活
阻断广域端口回应	激活
防止ARP攻击	激活
远程管理	激活
访问规则设置	0 条规则设置

SPI 主动封包侦测： 此为显示路由器的 SPI 主动封包侦测过滤防火墙功能选项是否激活(激活/关闭)。系统默认此功能为关闭。

防止 DoS 攻击： 此为显示路由器的阻断来自网络上的 DoS 攻击功能选项是否开启(激活/关闭)。系统默认此功能为关闭。

阻断广域网端口回应： 此为显示路由器的阻断来自网络 上的 ICMP-Ping 的响应功能选项是否激活(激活/关闭)。系统默认此功能为关闭。

防止 ARP 攻击： 此为显示路由器防止 ARP 攻击的功能选项是否激活(激活/关闭)。系统默认此功能为关闭。

远程配置管理： 此为显示路由器的远程管理功能选项是否启动(激活/关闭)。系统默认此功能为关闭。

访问规则设置： 此为显示路由器的访问规则设置的数目。

5.1.5 日志记录配置状态显示

日志

传送日志到	关闭 ()
E-mail 传送日志	关闭 ()

传送日志到： 此为显示您所设定路由器的日志记录接收的服务器。

E-mail 传送日志： (未來支持)
此为显示您所设定的 E-mail 地址，路由器的日志记录经由此 E-mail 传送出去。

E-Mail 的链接将会连到系统日志设定窗口中：

1. 若您没有设定电子邮件服务器于系统日志设定中，将显示 “**邮件无法传送,因为没有配置 SMTP 服务器正确地址**”——表示您没设定电子邮件服务器所以无法发送系统日志电子邮件。
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送的条件时,将显示“**邮件设定已经配置**”——表示您的电子邮件服务器已经设置，但是日志尚未达到设定传送的条件时。

3. 若您已经设定电子邮件服务器于系统日志设定中，日志也已经传送出去时，它将显示 “**邮件设定已经配置并正常发送**”——表示您的电子邮件服务器已经设置，并且已经发送。

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送出去时，它将显示 “**邮件不能发送，请使用正确的配置**”——电子邮件服务器已经设置，但是无法传送出去，可能是设定有问题。

5.2 登录密码及时间的修改和设定

5.2.1 密码设定

当您每次登录路由器的设定窗口时，必须输入密码。路由器的用户名和密码出厂值均为“**admin**”。考虑安全因素，我们强烈建议您务必在第一次登录并完成设定之后更改管理密码！密码请牢记，若是密码忘记，将无法再登录路由器的设定窗口，必须点击路由器前面板上的 **Reset** 按键十秒以上，恢复到出厂值，所有设定值将需要重新设定。

使用者名称： 出厂初始值默认为 admin。

旧密码： 填写原本旧密码（出厂初始值默认为“admin”）。

输入新使用者名称： 输入新用户名，如 Qno。

输入新密码： 填写要更改的新密码。

再次输入新密码： 再次填写更改的新密码以确认。

确定： 点击此按钮“**确定**”存储刚才所修改设定的内容参数。

取消： 点击此按钮“**取消**”清除刚才所修改设定的内容参数，此操作必须于“确定” 存储动作之前才会有效。

如果用户已经修改了密码，需要恢复到出厂时的用户名及密码，需要用现有用户名登录后输入新用户名以及新密码分别为“admin”，再点击按钮“**确定**”即会存储刚才所变动的修改设定内容参数；点击 “**取消**” 按钮即会清除刚才所变动的修改设定内容参数，此操作必须于确认存储动作之前才会有效。如下图：

5.2.2 系统时间设定

路由器 可以设定时间，让您在查看路由器的系统纪录或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网络资源的依据条件。您可以选择与路由器内建的外部时间服务器(NTP 服务器)取得时间同步，或自己设定正确时间参数。

设定自动与网络上的 NTP 服务器同步时间：路由器 有内建的网络时间服务器，会自动同步时间。

时区选择： 点开下拉菜单选择您所在地点的时区以正确显示当地时间。

日光节约时间： 若是您所的地区有实施日光节约时间，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。

时间服务器地址： 若是您自己有偏爱使用的时间服务器，可以输入该服务器的地址。

确定： 点击此按钮即会存储刚才所变动的修改设定内容参数。

取消： 点击此按钮即会清除刚才所变动的修改设定内容参数，此操作必须于确认存储动作之前才会有效。

手动输入日期时间参数： 在这输入正确的时间：小时、分钟、秒、月份、日与年份。

点击“**确认**”按钮即会存储刚才所修改的设定内容参数，点击此按钮“**取消**”即会清除刚才所修改的设定内容参数，此操作必须于确认存储动作之前才会有效。

六、进行网络连线配置

本章节讲述基本的网络联机设置，对大多数的用户来说，通过本章节完成基本的设定已经足够连接网络。网络的连接需要一些 ISP 所提供的进一步详细信息。其详细项目设定，请参考以下各节说明：

6.1 网络设定

6.1.1 主机名称及网域名称

可输入路由器的名称（主机名称）以及网域名称，此设定在大多数环境中不需要做任何设定即可使用，除

非特殊 ISP 需求！

6.1.2 局域 LAN 接口配置

此为显示并设定路由器的 LAN 端内部网络的设定。LAN 端 MAC 地址可以做修改，通常用在替换旧的路由器设备时，将 LAN 端的 MAC 地址改为与旧的路由器相同，LAN 端 PC 所做的 Gateway ARP 绑定就不需要再重新设定过。若要做修改，请按下”IP 整合管理”，在弹出窗口做设定。

IP 整合管理：

IP 整合管理的设置窗口可以设定局域网络(LAN) IP、动态 IP(DHCP)发放范围。

局域网络(LAN)设定：

系统默认 LAN IP 为 192.168.1.1，子网掩码为 255.255.255.0，您可以依照实际网络架构做变动。

Multiple-Subnet 多子网配置：

勾选“多个子网”，并填入您想要增加的子网络 IP 地址以及子网掩码，即可增加新的子网在局域网络。此功能是将不同于路由器局域网段的其它网段 IP 加入到路由器认可的局域网段中，这样局域网中的 PC 若是已经设定的 IP 所在的网段不同于路由器的局域网段也可以直接上网。举例来说，原来内部环境已经有多组不同的 IP 网段，例如 192.168.3.0， 192.168.20.0， 192.168.150.0 等等，将这些网段加入到子网中，则这些网段的内部计算机不需做任何修改就可以上网，这里可以依照您的实际网络架构运作。

动态 IP：

QOS 安全路由器有四组 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 地址，当计算机开机后，就可从 QOS 安全路由器自动取得 IP 地址，管理方便。

起始 IP 地址： 系统默认为四个网段从 192.168.1.100、192.168.2.100、192.168.3.100、192.168.4.100 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： 系统默认为四个网段 192.168.1.149、192.168.2.149、192.168.3.149、192.168.4.149IP 地址为最后发放 IP，也就是说出厂设定值每个网段可供 50 台计算机自动取得 IP 地址，四个网段共 200 台计算机自动取得 IP 地址。您可以依照实际需求来设定。

6.1.3 广域网络 WAN 及非军事区设定

广域网网络联机型态设定：

接口位置：广域网连线所在 WAN 接口位置。

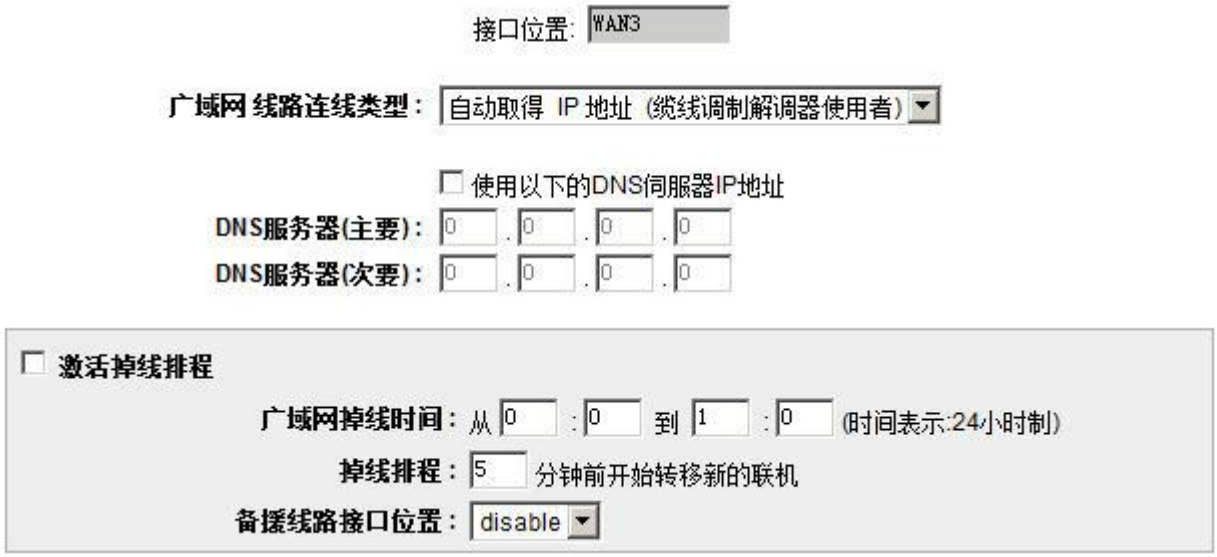
线路联机状态：此项显示该广域网口目前设定的联机状态。路由器提供五种联机状态设定：自动取得 IP 地址；固定 IP 地址；PPPoE 拨号联机；PPTP 拨号联机以及透明桥接模式。

配置：点击“编辑”按钮可以进入广域网联机状态的设置窗口。各类型的联机状态设定请参考以下的说明，并选择配合 ISP 所给您的联机状态来做设置。

自动取得 IP 地址：

此为路由器系统默认的联机方式，此联机方式为 DHCP 客户端自动取得 IP 模式，多为应用于如线缆调制解调器或是 DHCP 客户端联机状态等连接，若您的联机为其它不同的方式，请选取相关的设定并参考以下的介绍做设置。

在自动取得 IP 模式，您可以使用自定 DNS 的 IP 地址，勾选此选项并填入您要使用的 DNS 服务器 IP 地址。



使用以下的 DNS 服务器 IP 地址： 选择使用自定的 DNS 服务器 IP 地址。

DNS 服务器： 输入您的 ISP 所提供的动态域名解析服务器 IP 地址，最少填入一组，最多可填二组。

广域网掉线排程： 勾选此项目会启用广域网掉线排程的机制。在某些区域，广域网的联机服务会有时间的限制，例如从凌晨 12:00 到清晨 6:00 之间六个小时，光纤联机服务会中断。虽然 QoS 安全路由器有备援机制，此操作当此广域网断线的瞬间，所有经由该广域网对外访问的联机也会因此中断，重新连接时，才会经由备援机制走其它广域网出去。因此，为了避免在广域网断线的瞬间大量的联机被切断，您可以启用此机制在此广域网断线前一段时间，先将新增的联机经由其它广域网出去外网访问，可以减少此广域网断线时的冲击。

广域网掉线时间： 输入此广域网中断连接服务的规则时间。

掉线排程： 输入您希望在此广域网中断连接服务之前多长时间开始将新增的联机经由其它广域网出去外网访问。

指定备援接口： 若是此广域网有设置端口绑定，请选择要由哪一个广域网口做备援。通常您应该选择与此广域网同一个 ISP 联机的广域网口。

点击此按钮“**确认**”即会存储刚才所变动的修改设定内容参数，点击此按钮“**取消**”即会清除刚才所变动的修改设定内容参数，此操作必须于确认存储动作之前才会有效。

固定 IP 地址联机：

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 信息分别参照以下介绍填入相关设定参数中。

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 地址的默认网关，若您是使用 ADSL 的话，一般说来都是 ADSL 数据机（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，最少填入一组，最多可填二组。

广域网掉线排程： 勾选此项目会启用广域网掉线排程的机制。在某些区域，广域网的联机服务会有时间的限制，例如从凌晨 12:00 到清晨 6:00 之间六个小时，光纤联机服务会中断。虽然 QoS 安全路由器有备援机制，此操作当此广域网断线的瞬间，所有经由该广域网对外访问的联机也会因此中断，重新连接时，才会经由备援机制走其它广域网出去。因此，为了避免在广域网断线的瞬间大量的联机被切断，您可以启用此机制在此广域网断线前一段时间，先将新增的联机经由其它广域网出去外网访问，可以减少此广域网断线时的冲击。

广域网掉线时间： 输入此广域网中断连接服务的规则时间。

掉线排程： 输入您希望在此广域网中断连接服务之前多长时间开始将新增的联机经由其它广域网出去外网访问。

指定备援接口： 若是此广域网有设置端口绑定，请选择要由哪一个广域网口做备援。通常您应该选择与此广域网同一个 ISP 联机的广域网口。

点击此按钮“**确认**”即会存储刚才所变动的修改设定内容参数，点击此按钮“**取消**”即会清除刚才所变动的修

改设定内容参数，此操作必须于确认存储动作之前才会有效。

PPPoE 拨号联机：

此项为 ADSL 虚拟拨号使用(适用于 ADSL PPPoE)，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 PC 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 会自动向默认的 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。您可以自行输入所需要的无封包传送自动离线等待时间，默认为 5 分钟。

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

广域网掉线排程： 勾选此项目会启用广域网掉线排程的机制。在某些区域，广域网的联机服务会有时间的限制，例如从凌晨 12:00 到清晨 6:00 之间六个小时，光纤联机服务会中断。虽然 QoS 安全路由器有备援机制，此操作当此广域网断线的瞬间，所有经由该广域网对外访问的联机也会因此中断，重新连接时，才会经由备援机制走其它广域网出去。因此，为了避免在广域网断线的瞬间大量的联机被切断，您可以启用此机制在此广域网断线前一段时间，先将新增的联机经由其它广域网出去外网访问，可以减少此广域网断线时的冲击。

广域网掉线时间： 输入此广域网中断连接服务的规则时间。

掉线排程： 输入您希望在此广域网中断连接服务之前多长时间开始将新增的联机经由其它广域网出去外网访问。

指定备援接口： 若是此广域网有设置端口绑定，请选择要由哪一个广域网口做备援。通常您应该选择与此广域网同一个 ISP 联机的广域网口。

点击此按钮“**确认**”即会存储刚才所变动的修改设定内容参数，点击此按钮“**取消**”即会清除刚才所变动的修改设定内容参数，此操作必须于确认存储动作之前才会有效。

PPTP 拨号联机：

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。

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。

默认网关： 输入您的 ISP 所核发的可使用固定 IP 地址的默认网关，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 会自动向默认的 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默认为 5 分钟，您可以自行输入所需要的自动离线等待时间。

保持连线： 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。

广域网掉线排程： 勾选此项目会启用广域网掉线排程的机制。在某些区域，广域网的联机服务会有时间的限制，例如从凌晨 12:00 到清晨 6:00 之间六个小时，光纤联机服务会中断。虽然 QoS 安全路由器有备援机制，此操作当此广域网断线的瞬间，所有经由该广域网对外访问的联机也会因此中断，重新连接时，才会经由备援机制走其它广域网出去。因此，为了避免在广域网断线的瞬间大量的联机被切断，您可以启用此机制在此广域网断线前一段时间，先将新增的联机经由其它广域网出去外网访问，可以减少此广域网断线时的冲击。

广域网掉线时间： 输入此广域网中断连接服务的规则时间。

掉线排程： 输入您希望在此广域网中断连接服务之前多长时间开始将新增的联机经由其它广域网出去外网访问。

指定备援接口： 若是此广域网有设置端口绑定，请选择要由哪一个广域网口做备援。通常您应该选择与此广域网同一个 ISP 联机的广域网口。

点击此按钮“**确认**”即会存储刚才所变动的修改设定内容参数，点击此按钮“**取消**”即会清除刚才所变动的修改设定内容参数，此操作必须于确认存储动作之前才会有效。

透明桥接模式：

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，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，还是可以做到负载均衡。

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：255.255.255.240

预设网关： 输入您的 ISP 所核发的可使用固定 IP 地址的默认网关，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 范围。若是您的 ISP 分给您两个不连续的 IP 地址范围，您可以分别填入“内部 IP 地址 1”以及“内部 IP 地址 2”。

广域网掉线排程： 勾选此项目会启用广域网掉线排程的机制。在某些区域，广域网的联机服务会有时间的限制，例如从凌晨 12:00 到清晨 6:00 之间六个小时，光纤联机服务会中断。虽然 QoS 安全路由器有备援机制，此操作当此广域网断线的瞬间，所有经由该广域网对外访问的联机也会因此中断，重新连接时，才会经由备援机制走其它广域网出去。因此，为了避免在广域网断线的瞬间大量的联机被切断，您可以启用此机制在此广域网断线前一段时间，先将新增的联机经由其它广域网出去外网访问，可以减少此广域网断线时的冲击。

广域网掉线时间： 输入此广域网中断连接服务的规则时间。

掉线排程： 输入您希望在此广域网中断连接服务之前多长时间开始将新增的联机经由其它广域网出去外网访问。

指定备援接口： 若是此广域网有设置端口绑定，请选择要由哪一个广域网口做备援。通常您应该选择与此广域网同一个 ISP 联机的广域网口。

点击此按钮“**确认**”即会存储刚才所变动的修改设定内容参数，点击此按钮“取消”即会清除刚才所变动的修改设定内容参数，此操作必须于确认存储动作之前才会有效。

路由 NAT 混合模式：

当您申请的线路联机方式是使用公网 IP 而且必须使用路由模式来与局端联机，此功能可以让您内网计算机的 IP 设定为这条线路所需要使用的公网 IP 来正常上网，其余设为私有 IP 的计算机一样可以经由 NAT 方式来正常上网。

当您设定多个广域网时，广域网的联机模式选择此种路由 NAT 混合模式，还是可以做到负载均衡。

广域网络 IP 地址： 输入您的 ISP 所提供与局端联机的路由 IP 地址。

子网掩码： 输入您的 ISP 所提供与局端联机的路由 IP 地址的子网掩码，如：255.255.255.240

广域网默认网关： 输入您的 ISP 所所提供与局端联机的路由 IP 地址的默认网关。

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

路由网关： 输入您的 ISP 所核发的可使用固定 IP 范围的其中一个 IP 地址作为预设网关。

公网 IP 地址范围： 输入您的 ISP 所核发的可使用固定 IP 范围。若是您的 ISP 分给您两个不连续的 IP 地址范围，您可以分别填入“局域网 IP 地址范围 1”以及“局域网 IP 地址范围 2”。

若是您的 ISP 分给您多个不同子网段的 IP 地址范围，您可以填入其它的”局域网络由预设网关”以及” 局域网 IP 地址范围”。

广域网掉线排程： 勾选此项目会启用广域网掉线排程的机制。在某些区域，广域网的联机服务会有时间的限制，例如从凌晨 12:00 到清晨 6:00 之间六个小时，光纤联机服务会中断。虽然 QoS 安全路由器有备援机制，此操作当此广域网断线的瞬间，所有经由该广域网对外访问的联机也会因此中断，重新连接时，才会经由备援机制走其它广域网出去。因此，为了避免在广域网断线的瞬间大量的联机被切断，您可以启用此机制在此广域网断线前一段时间，先将新增的联机经由其它广域网出去外网访问，可以减少此广域网断线时的冲击。

广域网掉线时间： 输入此广域网中断连接服务的规则时间。

掉线排程： 输入您希望在此广域网中断连接服务之前多长时间开始将新增的联机经由其它广域网出去外网访问。

指定备援接口： 若是此广域网有设置端口绑定，请选择要由哪一个广域网口做备援。通常您应该选择与此广域网同一个 ISP 联机的广域网口。

點擊此按鈕“**確認**”即會存儲剛才所變動的修改設定內容參數，點擊此按鈕“**取消**”即會清除剛才所變動的修改設定內容參數，此操作必須於確認存儲動作之前才會有效。

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服务器，如 WWW 网页服务器与 Mail 电子邮件服务器等等。路由器 提供您独立的 DMZ 接口来设定连接有合法 IP 地址的服务器。此 DMZ 接口是从网络或局域网存取对外服务器内容的沟通桥梁。

在某些型号上，WAN 与 DMZ 端口是互相切换，您可以依据实际需要来选择使用 WAN 或是独立的 DMZ 接口。

IP 地址：此项显示您给予 DMZ 端口的 IP 地址或范围。

配置：点击“编辑”按钮可以进入 DMZ 的设置窗口。请参考以下的设定说明。

此 DMZ 的设定可分为 **Subnet**、**Range**、以及 **与路由 NAT 混合模式局域网 IP 同网段** 三种：

Subnet：

DMZ 与广域网络 WAN 要在不同的子网络 Subnet 中。

就是若 ISP 端分配给您 16 个合法 IP 如：220.243.230.1-16/子网掩码：255.255.255.240 时，您必须将此 16 个 IP 再切两组变成 220.243.230.1-8 /子网掩码：255.255.255.248 及另一组 220.243.230.9-16/子网掩码：255.255.255.248，然后路由器及网关是在同一组，再将另一组设定在 DMZ 中。

DMZ IP 地址： 输入在 DMZ 端口的 IP 代表地址。

子网掩码： 输入在 DMZ 端口的 IP 子网掩码。

广域网共享式带寬特殊應用： 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数据包，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。

Range：

DMZ 与广域网络 WAN 位在相同的子网络 Subnet。

接口位置： 选择 DMZ 是与哪一个 WAN 口的 IP 地址在相同的子网掩码。

IP 地址范围： 输入在 DMZ 端口的 IP 范围。

广域网共享式带寬特殊應用： 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数据包，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。

DMZ 与路由 NAT 混合模式局域网 IP 同网段：

DMZ 与路由 NAT 混合模式的局域网 IP 地址在相同的子网段。

局域网络由预设网关： 输入您在”路由 NAT 混合模式”所设定的局域网路由预设网关。

局域网 IP 地址范围：	输入您的 ISP 所核发的可使用固定 IP 范围中您要用来作为 DMZ 服务器的 IP 范围。 若是您的 ISP 分给您多个不同子网段的 IP 地址范围，您可以填入其它的”局域网络由预设网关”以及” 局域网 IP 地址范围”。
广域网共享式带寬特殊應用：	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数据包，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。

点击此按钮“**确认**”即会存储刚才所变动的修改设定内容参数，点击此按钮“**取消**”即会清除刚才所变动的修改设定内容参数，此操作必须于确认存储动作之前才会有效。

6.2 多 WAN 设定

当用户的连线是采用多 WAN 的线路设计，管理人员可以进入网络连线配置流量管理以及协议绑定栏目对路由器的负载均衡模式等进行配置，使路由器达到最优数据转发是网络带宽效能达到最高。

6.2.1 负载均衡模式

智能型负载均衡模式：

当您选用智能负载均衡模式，路由器将以联机数或是 IP 联机数为基础，并依据您广域网线路的带宽来自动分配联机，达到对外联机的负载均衡。线路的带宽是依据您所填入的带宽设定(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，所以为了确保您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)。

联机数均衡：当您选用联机数均衡模式，路由器将以联机数为基础，并依据您广域网线路的带宽来自动分配联机，达到联机的负载均衡。

IP 均衡：当您选用 IP 负载均衡模式，路由器将以联机的 IP 数为基础，并依据您广域网线路的带宽来自动分配联机，达到联机的负载均衡。

提示！

不论是联机数均衡或是 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。

譬如您希望指定 IP 192.168.1.100 访问外网的时候走广域网 1，或内网所有 IP 去访问服务端口 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”功能来达到您的需求。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，除了您指定的访问会按照您的规则出去访问外网，其它未被指定的 IP 或服务端口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（6.2.3 节的**通讯协议绑定**设定说明）。

指定路由：

这个模式让您对特定的内网 IP、特定要访问的应用服务端口、或特定目的地 IP 经由您指定的广域网对外网做访问。且一经指定后，该广域网也只能让这些指定的内网 IP、特定要访问的应用服务端口、或特定目的地 IP 使用。其它不在这些指定的内网 IP、特定要访问的应用服务端口、或特定目的地 IP 都会从其它的广域网出去访问。对于没有被指定的广域网，您可以选择他们的负载均衡模式是以联机数作为负载均衡的基础，还是以 IP 联机数作为负载均衡的基础。

在“指定路由”的负载均衡模式下，第一个广域网口会保留给没有指定到其它广域网口(WAN2～WAN5)的 IP 或应用服务端口(服务端口)经由此广域网(WAN1)进出。因此建议您在此模式下将您的其中一条线路接在第一个广域网口。当您其它的广域网口(WAN2～WAN5)断线时，而您在线路侦测机制下选择移除有问题线路，流量就会转移到第一个广域网口(WAN1)。此外，若是第一个广域网口(WAN1)断线，则流量会依次转移到其它广域网口，例如转移到 WAN2，WAN2 也断线则转移到 WAN3 等等。

未绑定端口均衡模式：若是有部分广网端口并没有被指定，例如广域网 3 与广域网 4 并没有指定特定的 IP、服务端口、或目的 IP 来使用，这些广域网端口(广域网 3 与 4)仍然会依据路由器的负载均衡机制来分配联机。均衡机制如下：

连机数均衡：当您选用联机数均衡模式，路由器将以联机数为基础，并依据您广域网线路的带宽来自动分配联机，达到联机的负载均衡。

IP 均衡：当您选用 IP 负载均衡模式，路由器将以联机的 IP 数为基础，并依据您广域网线路的带宽来自动分配联机，达到联机的负载均衡。

提示！

此指定路由必须配合“通讯协议绑定”功能才能发挥作用。例如指定让内网去访问服务端口 80 时都要从广域网 1 去访问，或内网去目的地 IP 211.1.1.1 访问时要从广域网 1 去访问等等，必须要在“通讯协议绑定”功能中做设定。要注意，当使用指定路由(Specify WAN Binding)模式，以上述的例子来看，除了您指定的访问必须按照您的规则出去访问外网都走广域网 1 以外，其它未被指定的 IP 或服务端口则经由路由器负载均衡的机制使用其它的广域网出去。

关于如何设定“通讯协议绑定”功能，以及指定路由模式搭配“通讯协议绑定”的范例，请参考（6.2.3 节的通讯协议绑定设定说明）。

策略路由：

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)自动分配联机。您只需选择网通线路接入的广域网口(或广域网组合)，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。

广域网组合：

当您所接的网通线路不只一条，则需要做广域网的组合，以便将两个以上的广域网口合在一起做相同的策略分流。点击“广域网组合”会弹出以下的对话窗口。

名称： 在此自定的广域网组合名称，如“教育”等，用来辨识广域网群组。

接口位置： 在此勾选要设在此组合的广域网口。

增加到对应列表： 增加到广域网组合列表。

删除所选服务： 删除所选择的广域网组合内容。

确定： 点击此按钮“**确认**”即会存储刚才所变动的修改设定内容参数。

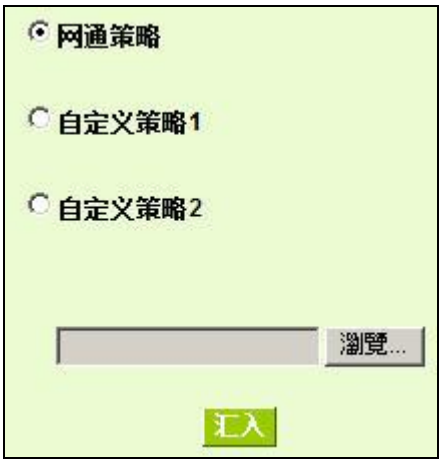
取消： 点击此按钮“取消”即会清除刚才所变动的修改设定内容参数，此操作必须于确认存储动作之前才会有效。

离开： 离开此功能设定窗口。

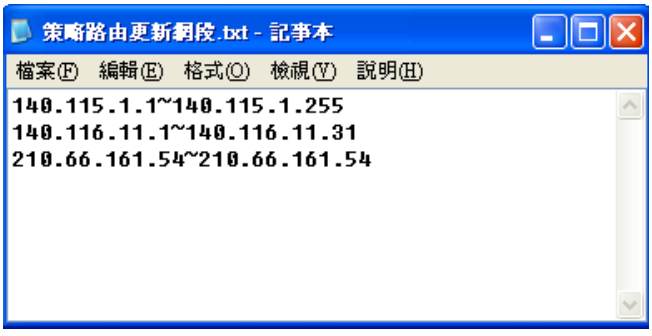
设定完成后，您就可以在网通策略的选择中选取您的网通接口的广域网组合。

自定策略：

此外，您也可以自己建立分流策略。在“自定策略”中选择要指定的广域网口或广域网组合(例如广域网 1)，然后点击“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本文件，应含有您指定的目的 IP 地址。将文件汇入路径选择好之后，点击“汇入”，并在设定窗口的最下方点击“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)或广域网组合出去。



策略文件的建立可以用纯文本编辑软件来撰写，例如使用 Windows 系统自带的文本编辑程序“记事本”来建立。将您要指定的目的 IP 地址按照下图的格式写入，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 格式。存储文件后(扩展名应该是.txt)即可汇入自定策略的更新网段。



提示！

网通策略与自定策略可以同时存在，但当某一个目的 IP 同时在网通策略以及自定策略中，则会以网通策略优先

执行。也就是说要往该目的 IP 的流量会从网通策略的广域网(或广域网组合)出去外网。

连线数均衡高级设定

一般连线数均衡是平均与随机分配每个内网 IP 的连线数量，但是某些较特殊的连线例如网络银行的加密连线(Https、TCP443) 需要固定从同一个 WAN IP 建立才能够正常操作，所以当同一个内网 IP 访问网络银行网站，访问操作动作被连线数均衡机制分配到不同 WAN IP 去建立连线时，有可能就会在操作过程中发生断线或不正常的状况，而连线均衡的高级设定功能就是用来解决这个问题。

高级设定可以设定同一个内网 IP，在以某个特殊的服务通讯端口建立连线时，固定从某一个 WAN IP 去建立，其它类型的服务通讯端口连线仍然照原来的均衡机制随机平均分配，除了可达成原来连线数均衡所带来的效用之外，也可确定一些较特殊的服务通讯端口连线时能正常运作。

点选高级设定进入设定选单：

目的地联关担入自动绑定： 选择此选项表示到目的地 IP 地址位于同一个 Class B 范围子网时，就固定从同一个 WAN IP 建立连线。

举例来说，总共两个 WAN1 200.10.10.1 与 WAN2 200.10.10.2，内网两个 IP 192.168.1.100 与 192.168.1.101，192.168.1.100 首次去访问外网 61.222.81.100 时，被随机分配到以 WAN1 200.10.10.1 建立连线，当 192.168.1.100 有下一笔连线目的地是 61.222.81.101 (在同一个 Class B 子网范围) 时，也一样会以 WAN1 200.10.10.1 去建立连线，但是若是去到别的目的地 IP (不在 61.222.81.100 同一个 Class B 子网范围) 则依然以原来连线数均衡的机制随机平均分配。

另一个内网 IP 192.168.1.101，首次去访问外网 61.222.81.101 时，被随机分配到以 WAN2 200.10.10.2 建立连线，当 192.168.1.101 有下一笔连线目的地是 61.222.81.100 (在同一个 Class B 子网范围) 时，也一样会以 WAN2 200.10.10.2 去建立连线，但是若是去到别的目的地 IP (不在 61.222.81.100 同一个 Class B 子网范围) 则依然以原来连线数均衡的机制随机平均分配。

※请注意！

并不是「所有内网 IP」到某一「相同 Class B 范围」都固定以某个 WAN IP 进行连线，而是看「每一个内网

IP」第一次被随机分配到以那一个 WAN IP 进行连线，之后遇到目的地是相同 Class B 范围，再「个别」按照同一个 WAN IP 进行连线。

用户自定义目的地及服务端口绑定：

这边是设定单一内网 IP，以某个自定义的特殊服务通讯向某个目的地 IP (或 IP 范围) 进行连线时，固定以同一个 WAN IP 进行连线。

您可以自行设定服务通讯端口与目的地 IP 内容 (目的地 IP 范围若设定成 0.0.0.0 到 0 表示到「任何一个目的地 IP 范围」

※请注意！

「用户自定义目的地及服务端口绑定」与「目的地连线登入自动绑定」两者只能同时使用其中一种！

以出厂预设已有设定的规则举例：

(如下图)

表示内网任何单一 IP，在以 TCP 443 Port 与任何目的地 (0.0.0.0 到 0 表示任何目的地) 进行连线时，都固定以同一个 WAN IP 进行连线，至于各个内网 IP 的选择是固定在那一个 WAN IP，则是以第一次被原本连

线数均衡机制所随机分配到的 WAN IP 为准，举例来说两个内网 IP 192.168.100.1 与 192.168.100.2，当个别第一次进行 TCP 443 Port 连线时，192.168.100.1 被随机平均分配到以 WAN 1 IP 连线，192.168,100.2 被随机分配到以 WAN2 IP 连线，则只要之后 192.168.100.1 有任何 TCP 443 Port 的连线，就会固定以 WAN 1 IP 连线；192.168.100.2 有任何 TCP 443 Port 的连线，就会固定以 WAN 2 IP 连线。

此预设规则虽然出厂默认值就有，但是您可以视自己的需求取消/删除此规则的应用，或新增其它新的规则以符合实际的连线需求。

6.2.2 线路侦测机制

若勾选此项设定，则会显示出重新发起测试次数，响应延长时间等信息。当使用两条广域网做对外联结线路时一定将此 NSD 启用，以避免因为广域端口流量过大时造成路由器的误判将此线路判断为断线。

接口位置： 选择您要设定线路侦测的广域网口。

重新发起测试次数： 对外联机侦测重试次数，默认值为五次。如果联机侦测重试次数超过设定次数，网络没有回应的话，则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。

线路连接失败时： 线路连接失败时的处理方式，有两种：

（1）只选择存储到日志记录文件：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信息纪录下来，但保持此线路不会移除，所以会导致有些原来使用此条线路上的用户无法正常使用。

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）删除该线路：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信息纪录下来，原本使用此 WAN 端的封包传递会自动转换到另一条广域端口.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。

有流量时不进行侦测： 当下载 或 / 与 上传流量超过带宽的百分之（ ）时，表示线路仍在联机运作，不必再一直送出 NSD 侦测要求数据包

侦测以下可回应的服务器：

预设网关： 近端的默认通讯网关位置，如 ADSL 路由器的 IP 地址，此为路由自动填入，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，且网关就是在您网吧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 地址等。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)。

使用 DNS 服务器做域名解释： 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： 点击此按钮“**确认**”即会存储刚才所变动的修改设定内容参数。

取消： 点击此按钮“取消”即会清除刚才所变动的修改设定内容参数，此操作必须于确认存储动作之前才会有效。

注意！

在“指定路由”的负载均衡模式下，第一个广域网口会保留给没有指定到其它广域网口(WAN2～WAN5)的 IP 或应用服务端口(服务端口)经由此广域网(WAN1)进出。因此建议您在此模式下将您的其中一条线路接在第一个广域网口。当您其它的广域网口(WAN2～WAN5)断线时，而您在线路侦测机制下选择移除有问题线路，流量就会转移到第一个广域网口(WAN1)。此外，若是第一个广域网口(WAN1)断线，则流量会依次转移到其它广域网口，例如转移到 WAN2，WAN2 也断线则转移到 WAN3 等等。

6.2.3 WAN 口带宽与协议绑定设置

接口配置

路由器最多可以设置五个广域网接口，每个广域网的带宽以及是否真正可以对外联机会影响路由器的负载均衡机制，因此您需要分别对每个广域网口做带宽设定，并正确的设置该广域网口的线路侦测机制。

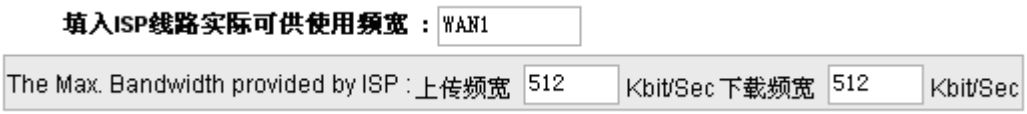
在“接口配置”中，点击“编辑”按钮即可进入该广域网口的配置窗口。

接口位置

接口位置	模式	配置
广域网1	全自动	编辑
广域网2	全自动	编辑
广域网3	全自动	编辑
广域网4	全自动	编辑
广域网5	全自动	编辑

带宽设定

路由器路由器会依照您实际输入的上传带宽数据作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。所以为了确保您的路由器达到实际线路负载能够均衡，请填入实际上下载带宽。另外，此字段也关系到 QoS 的设定，请参考相关 QoS 设定章节。



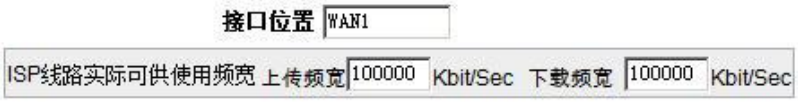
协议绑定

使用者可将特定的 IP 或特定的应用服务端口(服务端口)经由您限定的 WAN 出去。其它没有做绑定的 IP 或

服务器还是会进行广域网的负载平衡。

注意！

在“指定路由”的负载均衡模式下，第一个广域网口(WAN1)是不能被指定的，保留给没有指定到其它广域网口(WAN2～WAN5)的 IP 或应用服务端口(服务端口)经由此广域网(WAN1)进出。也就是说第一个广域网口(WAN1)不能设置通讯协议绑定的规则，以避免所有的广域网口都被指定有特定的内网 IP、应用服务端口、目的地 IP，导致其它的 IP 或应用服务端口没有广域网口可以使用。



服务端：	在此选择欲开启的绑定服务端口，从下拉式选单中可以选择默认列表(如 All -TCP&UDP 0～65535， WWW 为 80～80， FTP 为 21～21 等等)，默认的服务为 All 0～65535。 点击“服务端新增或删除表”按钮可以进入服务端口设定窗口，进行新增或删除选单中默认的服务端口。
来源 IP 地址：	您可以指定特定的内部虚拟 IP 地址的封包经由特定的广域端口出去。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端口而不需指定特定的 IP 地址， 则在 IP 的字段皆填入 0。您也可以选择 IP 群组的方式来指定来源 IP。关于 IP 群组的设定，请参考（“7.6 IP 群组管理”的说明）。
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 C 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：	选择您所要绑定此条规则在哪一个 WAN 端口。
激活：	启用此规则。
增加到对应列表：	增加此条规则到列表。
删除所选服务：	删除在服务列表里所选择的规则。
上移 & 下移：	由于每条规则执行的优先级为由列表的最上面那条往下执行，也就是越后面设定的规则会越后执行，所以您可以自行调整每条规则先后执行顺序。
确定：	点击此按钮“**确认**”即会存储刚才所变动的修改设定内容参数。
取消：	点击此按钮“**取消**”即会清除刚才所变动的修改设定内容参数，此操作必须于确认存储动作之前才会有效。

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，由上到下，在列表上最上方那条会先执行，然后依序往下。

优先权：

点击右上方的“优先权”按钮，会出现以下的对话窗口。您可以选择以“优先权”来显示排列的顺序，或是以“接

口位置”来显示排列的顺序。点击“刷新”可以重新显示窗口，点击“关闭”将结束这个对话窗口。

优先权	接口位置	服务端	来源IP地址	目的IP地址	激活	配置
1	广域网2	所有端口[TCP&UDP/1~65535]	192.168.1.2~192.168.1.254	0.0.0.0~0.0.0.0	激活	编辑
2	广域网2	HTTP[TCP/80~80]	192.168.5.0~192.168.5.0	0.0.0.0~0.0.0.0	激活	编辑

新增或删除管理服务端口号

若您欲开启的服务端口项目没有在表列中，您可以点击“服务端新增或删除表”按钮，新增或删除管理服务端口号列表，如以下所述：

服务端口名称： 在此自定欲开启的服务端口号名称加入列表中，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。

服务端口的位置范围： 填入您将新增加的服务端口范围。

增加到对应列表： 增加到开启服务项目内容列表，最多可新增 100 组。

删除所选服务端口列表： 删除所选择的开启服务项目内容。

确定： 点击此按钮“**确认**”即会存储刚才所变动的修改设定内容参数。

取消： 点击此按钮“**取消**”即会清除刚才所变动的修改设定内容参数，此操作必须于确认存储动作之前才会有效。

离开： 离开此功能设定窗口。

使用“智能型”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带宽，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“所有端口”，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，然后勾选激活。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是怎样设定?

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，然后勾选激活。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 端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是怎样设定?

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，然后勾选激活。最后点击“新增”即可将此规则加入。路由器会将所有用 80 端口去外网访问的流量都走广域网 2，但是不是用 80 端口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。

第二条规则，服务端选择“所有端口[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，然后勾选激活。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。

使用“指定路由”的负载均衡模式时其通讯协议绑定协议设定方式：

IP 群组-依使用者(IP Group)的模式让您对特定的内网 IP、特定要访问的应用服务端口或特定目的地 IP 经由您指定的广域网对外网做访问。且一经指定后，该广域网也只能让这些指定的内网 IP、特定要访问的应用服务端口、或特定目的地 IP 使用。其它不在这些指定内的内网 IP、特定要访问的应用服务端口或特定目的地 IP 都会从另一条广域网出去访问。此模式必须配合“通讯协议绑定”功能才能发挥作用。

范例一：若要指定内网所有 IP 去外网访问 80 端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是怎样设定?

如以下范例所示设置规则，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，然后勾选激活。最后点击“新增”即可将此规则加入。此时广域网 2 只会有访问外网 80 端口的流量，其余流量都只走广域网 1。

范例二：若要指定内网所有 IP 去外网访问 IP 211.1.1.1 到 211.254.254.254 还有 60.1.1.1 到 60.254.254.254 整组 A 类段时都走走广域网 2 去访问，但去其余不是这几个目的地 IP 段时都走广域网 1 时，那通讯协议绑定设定方式如何设定?

如以下范例所示设置两条规则：

第一条规则中服务端选择“所有端口[TCP&UDP/1~65535]”，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 地址填入 211.1.1.1 到 211.254.254.254。接口位置选则广域网 2，然后勾选激活。最后点击“新增”即可将此规则加入。

第二条规则中服务端选择“所有端口[TCP&UDP/1~65535]”，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 地址填入 60.1.1.1 到 60.254.254.254。接口位置选则广域网 2，然后勾选激活。最后点击“新增”即可将此规则加入。此时，除了上述两条规则所涵盖的目的 IP，其余去外网访问的流量都只走广域网 1。


优先权
服务端 :
所有端口 [TCP&UDP/1~65535]
服务端新增或删除表
来源IP地址 :
192 . 168 . 1 . 0 到 0 / 群组
目的IP地址 :
0 . 0 . 0 . 0 到
0 . 0 . 0 . 0
接口位置 :
广域网2
激活 :
上移
增加到对应列表
下移
所有端口 [TCP&UDP/1~65535]->192.168.1.0~0(211.1.1.1~211.254.254.254)广域网2
所有端口 [TCP&UDP/1~65535]->192.168.1.0~0(60.1.1.1~60.254.254.254)广域网2
删除所选择服务
返回
確定
取消

七、内部局域网络配置

通过本章节可以对端口进行配置管理，了解如何配置内部局域网络的 IP 地址。

7.1 网络端口管理配置

路由器路由器中，管理者可以设定网络实体联机于每一个以太网络端口，如连接速率，工作模式，优先权，自动侦测或是 VLAN 等以太网络端口的功能。

镜像端口：勾选“**激活端口 1 为端口镜像**”可以将局域网的第一个端口设定为镜射端口，所有从内网到外网访问的流量都会复制到镜射端口。因此您可以将监控或是过滤服务器直接接在镜射端口，来达到监控或是过滤网络封包的目的。

关闭端口： 此为设定以太网络的 LAN 端口开启或是关闭的功能，若是打勾的话，则此以太网络端口立即被关闭无法连接使用。默认为开启无打勾。

优先权设定： 此为设定此以太网络的 LAN 端口封包传送优先权设定，若是此端口设定为高的话，则最优先使用传送封包的权利，默认优先级为一般。

网络端口连接速度： 此为设定此以太网络的端口网络实体连接速率选项，您可以设定为 10Mbps 或是 100Mbps 连接速度。默认为自动侦测。

半双/全双工模式： 此为设定此以太网络的端口网络实体连接速率工作模式选项，您可以设定为半双工模式或是全双工模式运作。默认为自动侦测。

自动侦测模式： 此为设定以太网络的端口网络实体连接速率自动侦测模式，若是勾选的话，自动侦测所有连接端口的信号与调整。

VLAN： 此功能可以让网管人员在自己的局域网内将每一个局域网端口设定 1 个或多个不同网段且无法互通的局域网端口，但都可以通过路由器上网络。在同一个网段内的成员(在同一个 VLAN 局域网络内)可互相沟通并看得到对方，若不在同一个 VLAN 群组内的成员则无法得知其它成员的存在。使用者可为每一个 LAN 端口选定为哪一个 VLAN 局域网络群组， 最多可设定为 8 个局域网络群组。

VLAN All： 当网管人员在内网设定了多个 VALN 端口，且不在同一个 VLAN 群组内无法互访，可是内网又需要架设服饰器让内网所有 VLAN 群组都可以访问此服务器。此时可以将某一局域网端口设定为 VLAN All，将此服务器接入此 VLAN All 的端口，这样就可以让所有不同 VLAN 群组的计算机都可以访问到此服务器。

7.2 网络端口状态实时显示

此项功能可以让网络管理者查看每个实体端口的详细信息。

摘要信息

网路连接状态	10Base-T / 100Base-TX / 1000Base-T
接口位置	局域网
线路连线状态	激活
端口即时状态	端口激活
优先权	一般
网路连接速率	1000 Mbps
半双/全双工模式	全双工
自动侦测模式	激活
VLAN	VLAN1

流量即时显示

接收封包统计	12650
封包接收Byte数量	1468887
传送封包统计	22048
封包传送Byte数量	15737539
错误封包统计	0

整体资讯项目：

网路连接状态（10Base-T / 100Base-TX / 1000Base-T），接口位置（局域网/广域网络 1~5/DMZ），线路连线状态(激活/关闭)，端口配置状态（端口激活/端口关闭），优先权设定（高级/一般），网路连接速率（10Mbps/100Mbps/1000Mbps），半双/全双工模式(半双工/全双工)，自动侦测模式（激活/关闭），VLAN（VLAN1~5/ VLAN All）。

端口流量即时显示：

即时显示路由器工作状态下的接收和传送封包计算、封包接收和传送 Byte 数以及错误封包统计实际数值。

7.3 DHCP 发放 IP 服务器

路由器有四组 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 地址，当计算机开机后，就可从路由器自动取得 IP 地址，管理方便。

动态 IP 服务：

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

起始 IP 地址： 系统默认为四个网段从 192.168.0.100、192.168.1.100、192.168.2.100、192.168.3.100 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： 系统默认为四个网段 192.168.0.149、192.168.1.149、192.168.2.149、192.168.3.149IP 地址为最后发放 IP，也就是说出厂设定值每个网段可供 50 台计算机自动取得 IP 地址，四个网段共 200 台计算机自动取得 IP 地址。您可以依照实际需求来设定。

域名解析服务地址：

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。

域名解析服务器 (DNS)(主要) 1： 输入 DNS 网域服务器的 IP 位置。

域名解析服务器 (DNS)(次要) 1： 输入 DNS 网域服务器的 IP 位置。

WINS 服务器：

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。

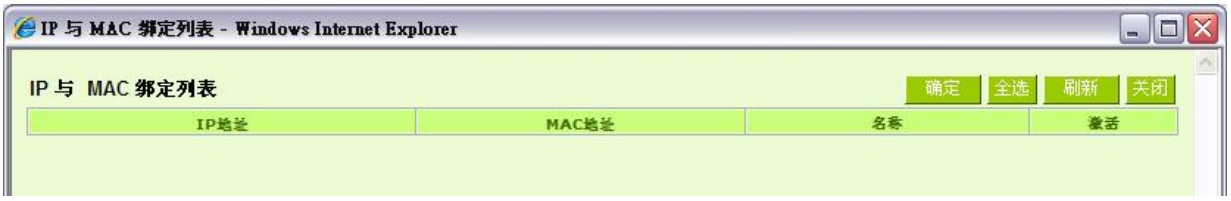
WIN 服务器： 输入 WINS 网域服务器的 IP 位置。

确定： 点击此按钮“确认”即会存储刚才所变动的修改设定内容参数。

取消： 点击此按钮“取消”即会清除刚才所变动的修改设定内容参数，此操作必须于确认存储动作之前才会有效。

显示表格：

此功能可以列出所有现在已经设定好的 MAC 绑定及 IP 绑定的状态，并且可以选择“编辑”做修改。



7.4 DHCP 状态显示

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。

状态

子网段：	子网段1	子网段2	子网段3	子网段4
DHCP服务功能：	192.168.1.1	192.168.2.1	192.168.3.1	192.168.4.1
已使用的动态IP数量：	1	0	0	0
已发放的固定IP数量：	0	0	0	0
DHCP服务器剩余可用的IP数量：	49	50	50	50
DHCP服务器可发放的IP总量：	50	50	50	50

DHCP服务器发放IP对应表

子网段1

主机名称	IP地址	MAC地址	租约到期时间	删除
4_WAN_QoS_Router	192.168.1.103	00:17:16:00:fc:48	22 时, 38 分, 17 秒	

刷新

DHCP 服务器 IP 地址: 目前 DHCP 服务器的 IP 地址。

已经使用 IP 数量: 目前 DHCP 服务器已经发放动态 IP 的数量。

发放固定 IP 数量: 目前 DHCP 服务器已经发放固定 IP 的数量。

尚可使用的 IP 地址: 目前 DHCP 服务器可以还可发放的 IP 数量。

配发 DHCP IP 地址总量: 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。

目前租约时间: DHCP 目前核发 IP 地址的租约时间。

删除: 删除此笔核发 IP 纪录。

7.5 IP 及 MAC 地址绑定

在许多的大中型网吧及企业网络中，网管人员可以设定路由器所提供的 IP & MAC 绑定功能，达到用户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。另外通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。

您可以以两种方式来设定这个功能：

限定可以使用网络的 MAC 地址

此功能主要目的是限制只有在列表里面的 MAC 地址才可以得到 DHCP 分配的 IP 地址上网，未在此列表的计算机都无法取得 IP 上网。当使用此功能时，切记要将静态 IP 地址填 0.0.0.0 不可以空白，另外将“封锁不在对应列表中的 MAC 地址”选项勾选才可以执行。如下图中范例所示：

IP 及 MAC 地址绑定

此功能主要目的是让指定的 MAC 地址计算机在每次开机都会要到同一个指定 IP。此外，若将“封锁在对应列表中 IP 地址错误的 MAC 地址”功能启用，那么设定为固定 IP 的计算机或通过此功能已发给特定 IP 的计算机擅自更改 IP 为非指定的 IP 地址时，则会无法上网。

静态 IP 地址设定： 此字段有两种填入方式：

1. 若您只要限制 MAC 地址可以跟 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，则将您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。

添入 IP 地址相应 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。

增加到对应列表: 增加或修正此设定到列表中。

删除所选择对应项目: 删除列表中所选择的绑定。

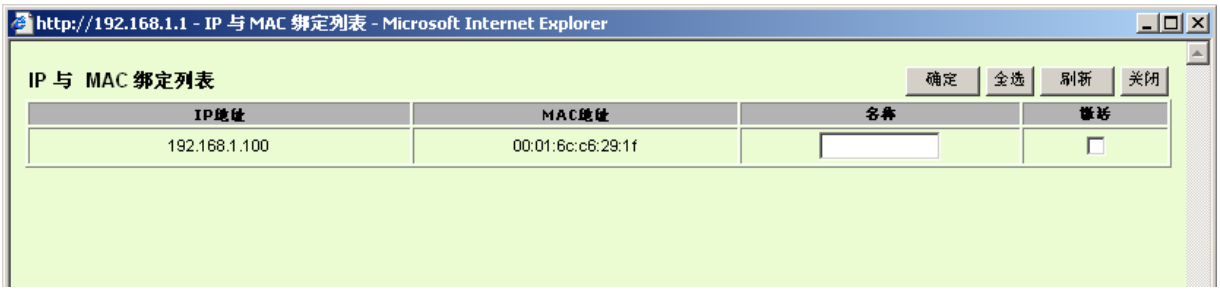
新增: 当列表中有绑定规则后，右下角会出现此按钮，可点击增加新的绑定。

封锁在对应列表中 IP 地址错误的 MAC 地址: 此选项打勾后，只要是 User 自行更改计算机的 IP 或不是列表设定的 IP 将无法上网。

封锁不在对应列表中的 MAC 地址：此选项打勾后，只要不在列表中的 MAC 地址都无法上网。

显示出还未做绑定或新加入的 IP 及其 MAC 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 地址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 地址，然后直接在此表格做绑定动作即可。另外，若您发现此表格出现已经绑定的某组 MAC 又出现在此表格，则表示此用户试图修改不是您指定的 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。

激活 勾选您所要绑定的目标。

确定: 将您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。

刷新: 更新此列表。

关闭: 关闭此列表。

7.6 IP 与服务通讯端口群组管理

IP 群组功能可以让您将数个 IP 地址或 IP 地址范围组合成一个群组。当您以 IP 地址来管理使用者的网络存取权限的时候，您可以将具有相同使用权限的使用者设定在同一个 IP 群组里，并在各个管理功能中选择以 IP 群组的方式来做设定，可以减少以单一 IP 来做设定的规则数。例如在“通讯协议绑定”的设定，“带宽管理(QoS)”的设定，以及“访问规则”的设定中，都可以选择以 IP 群组的方式来做设定，如此就不需要再以单一 IP 来设定，减少所需要的规则数。

IP 群组有分成本地 IP 群组与远程 IP 群组，本地群组是指局域网内的来源 IP 群组，远程群组是指广域网外的目的地 IP 群组；本地群组的用户 IP 编辑清单，会自动学习有流量经过防火墙的 IP 地址，并且如果用户更动 IP，清单内的 IP 也会跟着变动，但是已经加入群组的 IP 数据，不会随着左方 IP 清单的改变而自动变更群组内容，必须由管理使用者手动进行更改。

用户 IP 编辑: 除了原本在左下方就会出现的自动学习 IP 清单，也可以自行手动设定 IP 地址。

名称：	输入下方输入 IP 地址 (或范围) 所代表的名称。
IP 地址：	输入 IP 地址 (或范围) 内容。例如 192.168.1.200 到 250。
加入 IP 列表：	设定完 IP 地址的名称与内容后，按下此按钮将数据加入下方 IP 列表，若此 IP (或范围) 已在列表中是无法加入的。
本地群组设定：	设定本地 IP 群组，可以直接从左方的 IP 清单中拉选成 IP 群组组合。
IP 群组：	在此字段选择您要修改的 IP 群组内容名称，若是要新增群组，请按下旁边的「新增群组」按钮。
群组名称：	会在此字段显示群组名称内容，在新增群组的时候，也请注意要输入群组名称在该字段中。
删除群组：	从下拉式选单选择欲删除的群组内容，并按下「删除群组」按钮，此时系统会再确认一次是否删除该群组，按下确认后就会删除该群组内容。
>>>> **按钮：**	可以由左方 IP 清单一次点选多个 IP 后，按下此按钮加入右方的群组内容清单中。
delete **：**	将自定义的 IP 或是 IP 范围进行删除。
确定：	点击此按钮“**确认**”即会存储刚才所变动的修改设定内容参数。
取消：	点击此按钮“**取消**”即会清除刚才所变动的修改设定内容参数，此操作必须于“确定”存储动作之前才会有效。

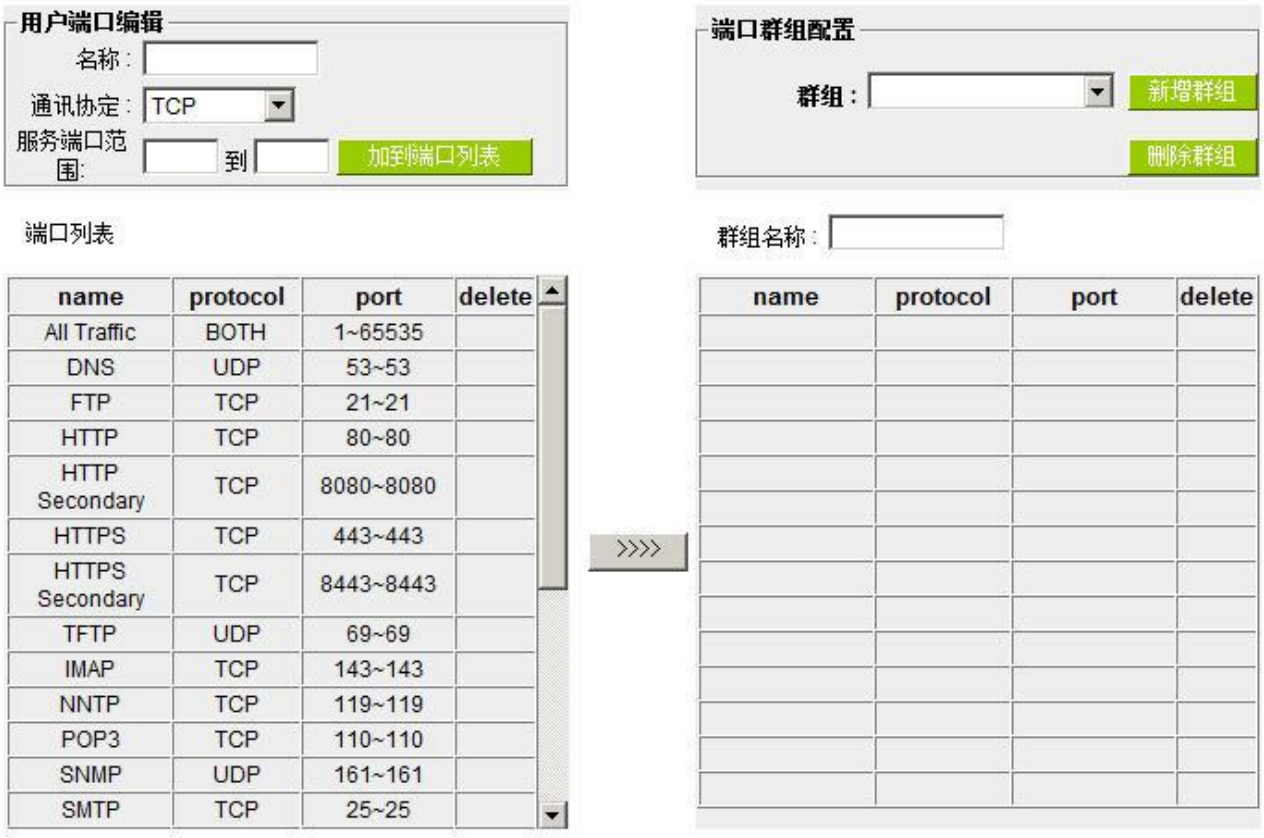
远程 IP 组管理：

基本上远程 IP 组设定的方式与本地 IP 组管理设定方式完全相同，但由于是远程 IP，所以并没有自动学习功能，并需自己手动定义远程的 IP 地址、范围与群组，例如 220.130.188.1 到 200 (范围)。

设定方式一样也是设定好左方单一远程 IP 地址或范围的内容后，于右方设定拉选要加入某群组的 IP 地址数据。

7.7 服务通讯端口 群组管理

除了 IP 地址可以成为群组设定外，服务埠也可以群组起来，方便对于 QoS、防火墙访问规则设置等功能的设定。



用户端口编辑: 针对所需的服务埠手动进行设定，依序为名称、通讯协议、服务端口范围。

名称： 将此服务端口命名以识别其属性。例如：Virus135

通讯协议： 设定服务埠属于 TCP 或 UDP 或 TCP&UDP 那种通讯协议。

服务端口范围： 设定服务埠 (Port) 范围。例如 135 到 135

加到端口列表： 设定服务端口的名称、通讯协议与端口范围后，按下此按钮就会加入到下方的埠列表，并且此埠可以成为某个埠群组的内容。

群组名称： 会在此字段显示端口群组名称内容，在新增群组的时候，也请注意要输入群组名称在该字段中。例如 Virus。

删除群组： 从下拉式选单选择欲删除的群组内容，并按下「删除群组」按钮，此时系统会再确认一次是否删除该群组，按下确认后就会删除该群组内容。

>>>> 按钮： 可以由左方服务端口清单一次点选多个服务端口后，按下此按钮加入右方的群组内容清单中。

delete：　　将自定义的服务埠或是服务埠范围进行删除。

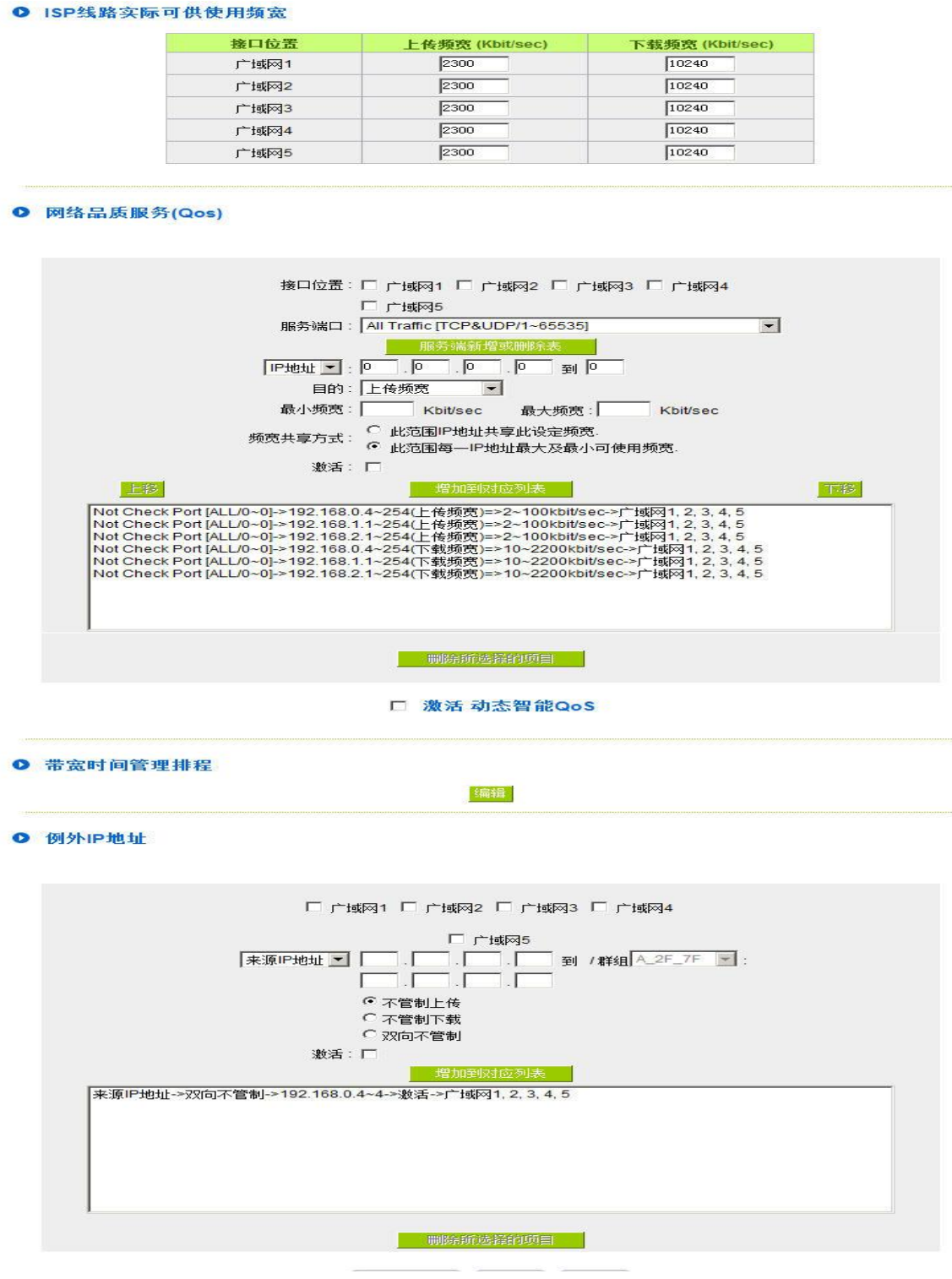
确定：　　点击此按钮“**确认**”即会存储刚才所变动的修改设定内容参数。

取消：　　点击此按钮“**取消**”即会清除刚才所变动的修改设定内容参数，此操作必须于“确定”存储动作之前才会有效。

八、QoS 带宽管理功能

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网吧、企业等的实际需求，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。

8.1 带宽设置(QoS)


ISP线路实际可供使用频宽
接口位置
上传频宽 (Kbit/sec)
下载频宽 (Kbit/sec)
广域网1 2300 10240
广域网2 2300 10240
广域网3 2300 10240
广域网4 2300 10240
广域网5 2300 10240
网络品质服务(Qos)
接口位置： 广域网1 广域网2 广域网3 广域网4 广域网5
服务端口： All Traffic [TCP&UDP/1~65535]
服务端新增或删除表
IP地址 0.0.0.0 到 0
目的： 上传频宽
最小频宽： Kbit/sec 最大频宽： Kbit/sec
频宽共享方式： 此范围IP地址共享此设定频宽.
此范围每一IP地址最大及最小可使用频宽.
激活：
上移
增加到对应列表
下移
Not Check Port [ALL/0~0]->192.168.0.4~254(上传频宽)=>2~100kbit/sec->广域网1, 2, 3, 4, 5
Not Check Port [ALL/0~0]->192.168.1.1~254(上传频宽)=>2~100kbit/sec->广域网1, 2, 3, 4, 5
Not Check Port [ALL/0~0]->192.168.2.1~254(上传频宽)=>2~100kbit/sec->广域网1, 2, 3, 4, 5
Not Check Port [ALL/0~0]->192.168.0.4~254(下载频宽)=>10~2200kbit/sec->广域网1, 2, 3, 4, 5
Not Check Port [ALL/0~0]->192.168.1.1~254(下载频宽)=>10~2200kbit/sec->广域网1, 2, 3, 4, 5
Not Check Port [ALL/0~0]->192.168.2.1~254(下载频宽)=>10~2200kbit/sec->广域网1, 2, 3, 4, 5
删除所选择的项目
激活 动态智能QoS
带宽时间管理排程
编辑
例外IP地址
广域网1 广域网2 广域网3 广域网4 广域网5
来源IP地址 到 /群组 A_2F_7F
不管制上传
不管制下载
双向不管制
激活：
增加到对应列表
来源IP地址->双向不管制->192.168.0.4~4->激活->广域网1, 2, 3, 4, 5
删除所选择的项目

8.1.1 带宽设定

ISP线路实际可供使用频宽

接口位置	上传频宽 (Kbit/sec)	下载频宽 (Kbit/sec)
广域网1	2300	10240
广域网2	2300	10240
广域网3	2300	10240
广域网4	2300	10240
广域网5	2300	10240

WAN 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。例如每个 IP 及服务端口（服务端口）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最小带宽就可以填 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。

8.1.2 QoS 设定

QoS 可以选择两种方式，无法同时使用，一为流量控制(带宽管理)，另一个为优先权控制，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 (带宽管理) - 依使用量做管理：

网管人员可依照您现有的带宽大小做每一个 IP 或一个范围的 IP 的使用量限制或保障带宽。另外也可以针对服务端口去做带宽控制。若是内部有架设服务器的话，也可控制或保障其对外带宽。

网络品质服务(Qos)

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： 选择此条 QoS 所要设定的带宽控制为哪个，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(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，可参考服务号码默认列表。

IP 地址：

此为选择您所要限制的使用者为哪些?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。若是此条带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 C 的范围。

您也可以选择 IP 群组的方式来指定来源 IP。关于 IP 群组的设定，请参考（“5.4 IP 群组管理”的说明）。

目的：

上传： 指对内网 IP 的上传带宽

下载： 指对内网 IP 的下载带宽

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

虚拟服务器下载(Server in LAN，下载)：若您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带宽控制，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升级时，可以用此控制做带宽管理，才不会影响内部使用者上网打游戏。

最小带宽 & 最大带宽： (Kbit/Sec)

最小带宽：此为限制或保证此条规则的最小可使用带宽。

最大带宽：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。

管制时间：

选择“**全部**”，此 QoS 设定在所有时间都有效果，如果选择“**从___:___到___:___**”填入时间段（24 小时记时制，例如 19：00 到 24：00）， 以及勾选“**每天/周日/周一/周二/周三/周四/周五/周六**”的某一天或者几天，其 QoS 设定只在所勾选设定的特定时间段内有效。

带宽共享方式：

此范围 IP 地址共享此设定带宽：

若选择此规则的话，其表示所有 IP 或此服务端口共享这段(最小带宽到最大带宽)带宽范围。

此范围每一 IP 地址最大或最小可使用带宽：

若选择此规则的话，其表示每一个 IP 或这一段服务端口都可以有此(Mini 到 Max.Rtae)带宽范围，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 做文件下载，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 做文件下载，总和所占用的带宽是固定的。

激活： 启用此规则。

增加到对应列表： 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，所以您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服务端口移至最下方如 BT，e-mule 等，然后将针对限制 IP 带宽的规则往上移。

删除所选服务： 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带宽管理设定的规则，并可直接点击“编辑”做修改（见表后详解）。

确定： 点击此按钮“**确认**”即会存储刚才所变动的修改设定内容参数。

取消： 点击此按钮“**取消**”即会清除刚才所变动的修改设定内容参数，此操作必须于确认存储动作之前才会有效。

显示开启表：

点击左下方的“显示开启表”按钮，会出现以下的对话窗口。您可以选择以“规则”来显示已设定的规则，或是以“接口位置”来显示已设定的规则。点击“刷新”可以重新显示窗口，点击“关闭”将结束这个对话窗口。可直接点击“编辑”做修改。

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

如以下范例所示设置规则，接口位置勾选广域网 1、2、3、4、5，服务端选择“ 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。勾选激活，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 每人最大下载使用带宽只能有 512Kbit，需要一个 IP 一个 IP 设定吗?

不需要一个 IP 一个 IP 设定。如以下范例所示设置规则，接口位置勾选广域网 1、2、3、4、5，服务端选择“No 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 512kbit/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。勾选激活，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。

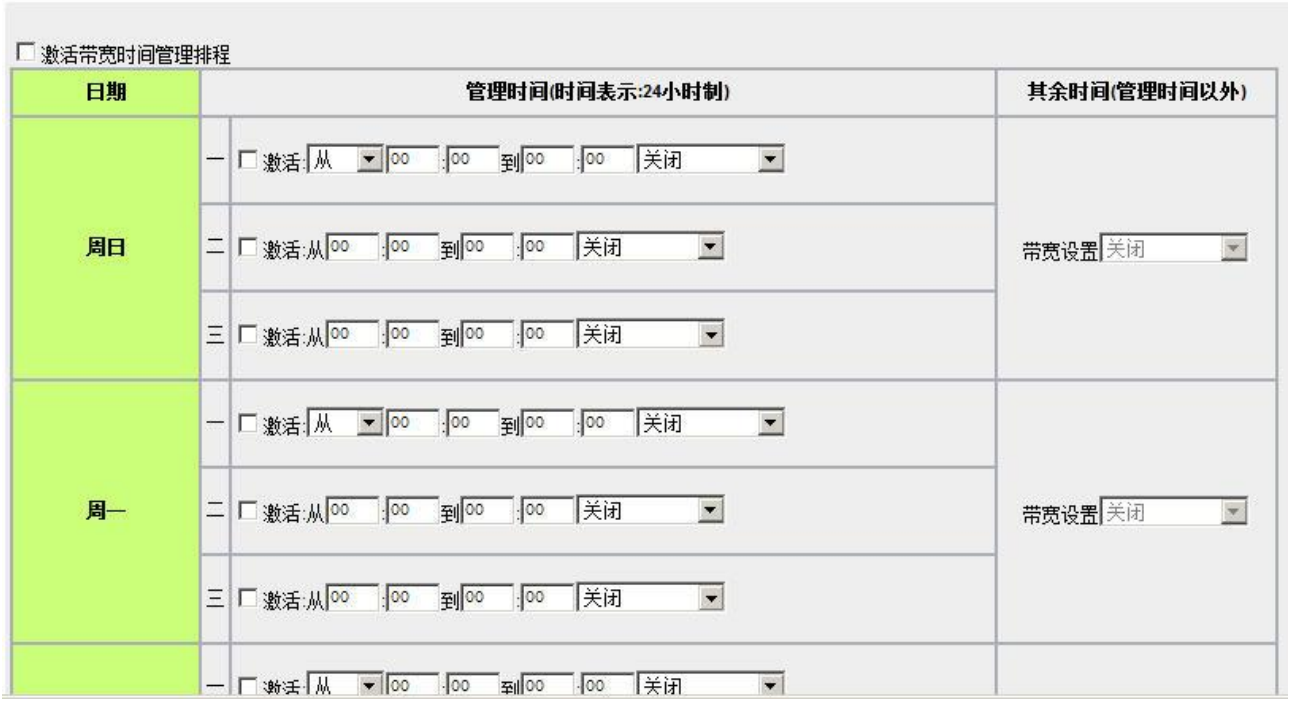
8.1.3 动态智能 QoS

动态智能 QoS 无需网管对每一个 IP 或是一个范围的 IP 地址进行配置，又可以达到带宽管理的效果。这个功能可以在内网使用人数少的时候可以使用较大的带宽，内网使用人数多的时候自动压抑占用带宽用户，非常具有弹性又同时简化网管的管理工作，并让内网所有的人都可以有带宽可以使用。

激活动态智能 QoS:	勾选激活动态智能 QoS。
当任一广域网带宽使用率到达 ____%时，激活智能 QoS	当带宽使用率到达实际带宽的一个%比时，将启动活智能 QoS，您可输入需要的数值，系统默认是 60%。
内网 IP 在所有广域网最大容忍上传带宽 ：	填入内网 IP 上行最大容忍使用带宽。
内网 IP 在所有广域网最大容忍下载带宽 ：	填入内网 IP 下载最大容忍使用带宽。
当任一 IP 使用超过上述设定上传或下载带宽时，此 IP 则使用下列指定带宽（带宽）：	当任一 IP 使用超过上述设定上传或下载带宽时，就实行惩罚措施，并以各个广域网络的上传 / 下载分别设定 ,惩罚后允许使用的带宽是多少
激活二次性惩罚：	点击勾选"激活二次性惩罚："后，内部设置好二次惩罚条件，当内部网络上网用户上网过程中的上传与下载达到内部条件将执行二次惩罚。
显示处罚列表：	点击后，在弹出的对话框中将会显示惩罚中的 IP，上行限制中，下载限制中以及二次惩罚信息。

8.1.4 带宽时间管理排程

在每天以及一周内不同的时间可能需要根据带宽的运用来采用不同的带宽管理方式，网管可以使用这个功能来排出不同的时间区段的带宽管理模式，让有限的带宽可以发挥最大的效用。



启用带宽管理时间排程: 勾选启用带宽管理时间排程。

日期: 从周日到周六的一周内，每天都可以依据情况设置管理时间。

管理时间(时间表示为 24 小时制): 每天可以指定三个时段的管理时间，时间的填入方式必须为 24 小时制。若是在第一个时间段里选择 “全天”，则当天其余时间段会呈现灰色不能再做选择。每个段的时间范围不能重复。每段管理时间可以选择“**关闭**”、 “QoS”、 “**智能** QoS”的带宽管理模式。

其余时间(时间管理以外) : 除了指定的管理时间之内，剩余的时间也可以选择“**关闭**”、“QoS”、 “**智能** QoS”的带宽管理模式。

确定: 点击此按钮“**确认**”即会存储刚才所变动的修改设定内容参数。

取消: 点击此按钮“**取消**”即会清除刚才所变动的修改设定内容参数，此操作必须于确认存储动作之前才会有效。

离开: 点击此按钮“**离开**”即不存储刚才所变动的修改设定内容参数，并离开此设定页面。

8.1.5 不受限制的 IP 地址

若是有内网的使用者不需要受到 QoS 的限制，可以用这个功能将这个使用者的 IP 排除再带宽管理的限制之内。

广域网： 勾选哪些广域网口不受限制。

来源 IP 地址/群组： 输入不受限制的 IP 地址范围，或者选择不受限制的 IP 群组。

不管制的方向： 可以选择不管制上传、不管制下载，或是双向都不管制。

激活： 选择激活这个规则设定。

增加到对应列表： 将添加的规则增加到列表中。

删除所选服务： 选择列表中的规则，删除选中的规则。

确定： 点击此按钮“**确认**”即会存储刚才所变动的修改设定内容参数。

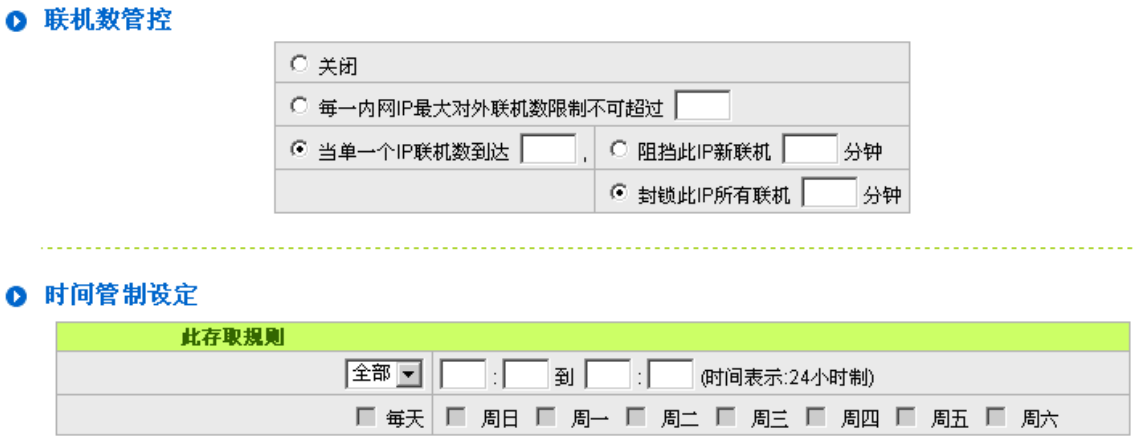
取消： 点击此按钮“**取消**”即会清除刚才所变动的修改设定内容参数，此操作必须于确认存储动作之前才会有效。

8.2 联机数管控

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。

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，也可以达到抑制做用。

联机管制设定以及时间管制



关闭： 不使用此联机数管控功能。

每一内网 IP 最大对外联机数限制不可超过： 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。

当单一个 IP 联机数到达：

阻挡此 IP 新联机 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 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。

时间管制设定： 选择“**全部**”，此 QoS 设定在所有时间都有效果，如果选择“**从___:___到___:___**”填入时间段（24 小时记时制，例如 19：00 到 24：00），以及勾选“**每天/周日/周一/周二/周三/周四/周五/周六**”的某一天或者几天，其 QoS 设定在所勾选设定的特定时间段内有效。

确定： 点击此按钮“**确认**”即会存储刚才所变动的修改设定内容参数。

取消： 点击此按钮“**取消**”即会清除刚才所变动的修改设定内容参数，此操作必须于确认存储动作之前才会有效。

不受限制的服务或 IP 地址

当有的用户以及 IP（比如公司管理层等），或者是特定需要不受限制的服务（公司财务数据的传输，邮件的传输等），管理人员可以设定这些服务或者 IP 不受联机管制。

服务端： 选择不受限制的服务端口。

来源 IP 地址： 输入不受限制的 IP 地址范围，或者选择不受限制的 IP 群组。

激活： 启用此规则。

增加到对应列表： 将添加的规则增加到列表中。

删除所选服务： 选择列表中的规则，删除选中的规则。

确定： 点击此按钮“**确认**”即会存储刚才所变动的修改设定内容参数。

取消： 点击此按钮“**取消**”即会清除刚才所变动的修改设定内容参数，此操作必须于确认存储动作之前才会有效。

8.3 硬件加速服务(未來支持)

本系列全千兆旗舰路由，除了原本就具有极高的处理效能外，也提供了带宽控管、流量优化相关的「硬件加速」功能，此功能的主要目的在于直接使用硬件来处理、加速不同带宽管理相关的功能，优化流量的分配使用，完全不会消耗到 CPU 与系统整体的资源，使路由器的整体处理速度更快，更能承受大量的联机数量与计算机数量，提供绝佳且稳定的网络使用环境。

(1) 视频游戏加速：

将网络游戏或是视频软件所使用的服务端口，做流量的最高优先保证，这可以路由器在流量满载的状况下，优先处理这些最高优先权的游戏或视频流量，使游戏与视频软件即使是在流量满载的状况下仍然使用顺畅不断线。

MAC 地址： 下拉式选单项目表示如下

【1】来源 MAC 地址：流量条件需符合所设定来源 MAC 地址内容，保障优先流量硬件加速功能才会生效。

【2】目的 MAC 地址：流量条件需符合所设定来目的 MAC 地址内容，保障优先流量硬件加速功能才会生效。

【3】无或不需检查：流量条件不需要符合、也不检查任何 MAC 地址内容。

IP 地址： 下拉式选单项目表示如下

【1】来源 IP 地址：流量条件需符合所设定来源 IP 地址内容，保障优先流量硬件加速功能才会生效。

【2】目的 IP 地址：流量条件需符合所设定目的 IP 地址内容，保障优先流量硬件加速功能才会生效。

【3】无或不需检查：流量条件不需要符合、也不检查任何 IP 地址内容。

通讯协议： 需优先保障、加速的游戏、视频或是其它网络应用的服务端口协议。

可选择 TCP 或 UDP 其中一种协议。

服务端口： 输入需优先保障、加速的游戏、视频或是其它网络应用的服务端口号，范围为 1~65535。

激活： 勾选表示激活此条规则，取消勾选表示不激活此条规则

增加到对应列表： 将添加的规则增加到列表中。

删除所选服务： 选择列表中的规则，删除选中的规则。

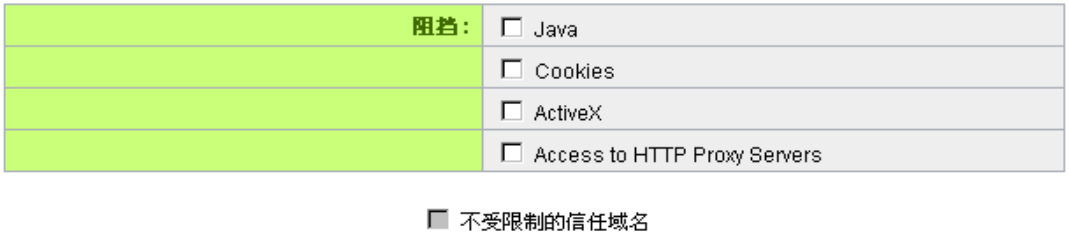
九、防火墙配置

本章节介绍防火墙设定的选项，以及网络存取控制的设定，保证网络的安全性。

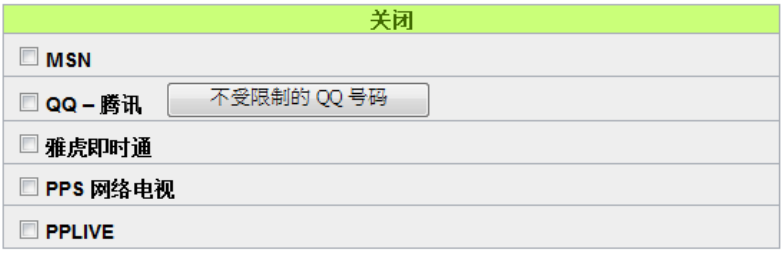
9.1 基本设置

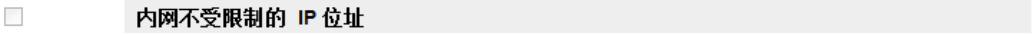
从防火墙功能的一般设定选项当中，您可以控制开启或是关闭这些选项功能。出厂默认值是将防火墙开启，并关闭不必要的响应。

禁止特殊应用



阻挡特定服务





防火墙功能：	此为选择开启或关闭防火墙功能。默认激活。
SPI 封包主动侦测检验功能:	此为封包主动侦测检验技术，防火墙主要运作在网络层，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。默认激活。
DoS 侦测功能:	此为保护 DoS 攻击，如 SYN Flooding， Smurf， LAND， Ping of Death， IP Spoofing 等。默认激活。
关闭对外封包回应:	若是选择激活的话，则路由器 会关闭对外的 ICMP 与不正常联机的封包响应，所以若是您从外部去 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。
远程配置管理功能:	远程管理功能，若您要通过远程网络 直接联机进入路由器的设定窗口，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 地址(WAN IP)，并加上默认可修改的控制端口(默认为 80，可更改)。
允许 Multicast 封包穿透模式：	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。默认为关闭
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 病毒欺骗大多在网吧环境发生，会让所有上网计算机一瞬间掉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。

高级设定

封包类型：路由器提供三种数据封包传输类型，包括 TCP-SYN-Flood、UDP-Flood 以及 ICMP-Flood。

广域网络阀值设定：防止来自外部网络的攻击。设定“所有封包阀值”（即外部攻击的所有封包数据），当其达到一个最大值（默认 15000pakets/Sec），路由器将只允许通过所设定最大值的封包数。当单一封包阀值（外部单一一个 IP 地址攻击的封包数据）达到一个最大值（默认 2000pakets/Sec），就会阻挡此 IP 上网 5 分钟（默认是 5 分钟），禁止其访问服务器，限制其流量和连接数，从而有效保证网络的安全。这里您可以根据需要调整你的阀值以及阻挡时间来达到对外网攻击的有效防护，建议其阀值从大到小来调节，避免阀值过小影响正常网络的运行。

局域网络阀值设定：防止来自内部网络的攻击。同样，当所有封包阀值（即外部攻击的所有封包数据）达到一个最大值（默认 15000pakets/Sec），路由器将只允许通过所设定最大值的封包数。当单一封包阀值（内部单一一个 IP 地址攻击的封包数据）达到一个最大值（默认 2000pakets/Sec），就会阻挡此 IP 上网 5 分钟（默认是 5 分钟），禁止其访问服务器，限制其流量和连接数，从而有效保证网络的安全。您可以根据需要调整你的阀值以及阻挡时间来达到对内网攻击的有效防护，建议其阀值从大到小来调节，避免阀值过小影响正常网络的运行。

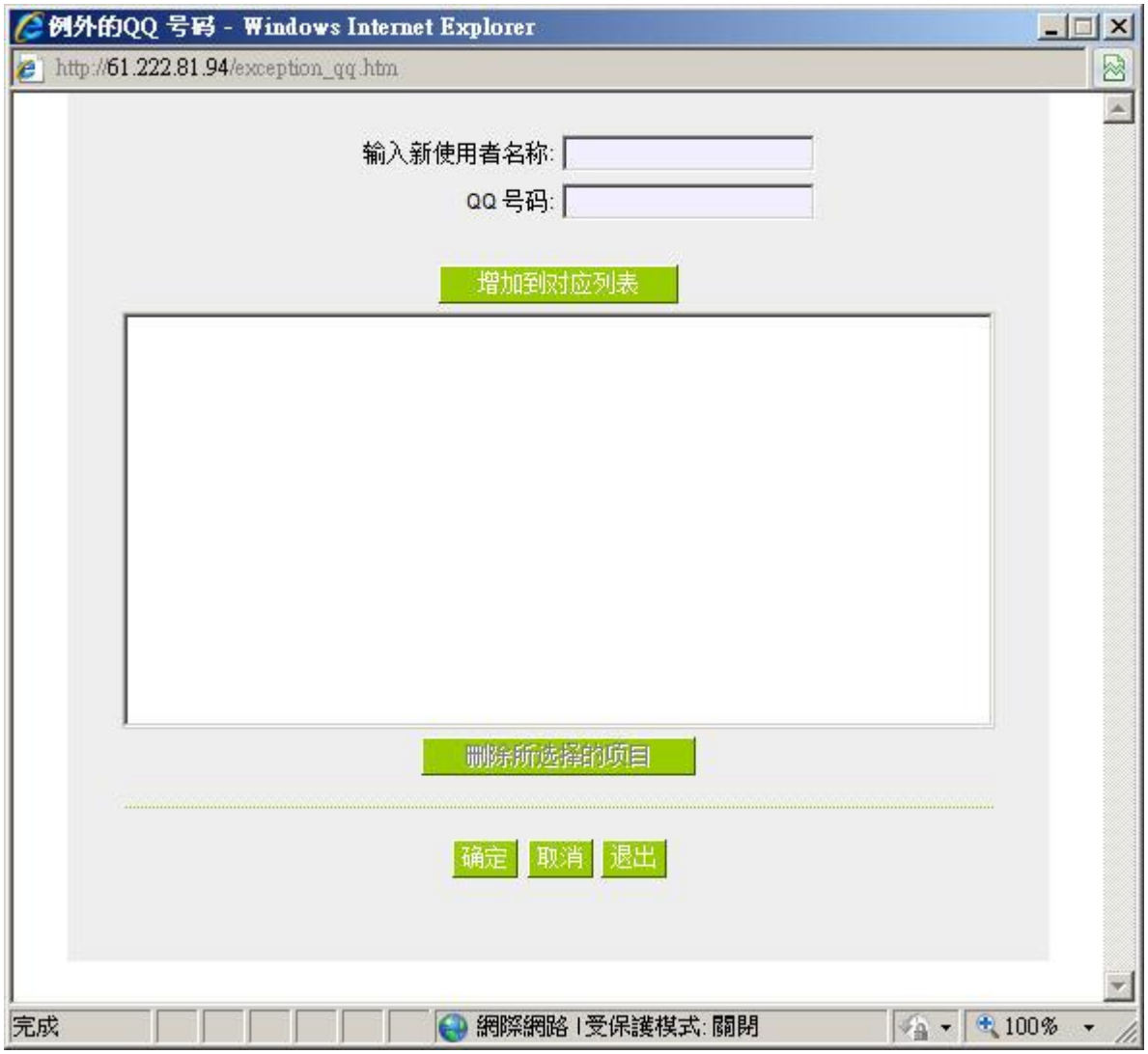
例外的来源 IP：指定某些来源端的 IP 地址/群组 不受到阈值的限制。

例外的目的 IP：指定某些目的端的 IP 地址/群组 不受到阈值的限制。

阻挡特定服务： 针对目前较多人使用的应用服务进行封锁管制，例如实时通讯 IM、P2P 下载软件或网络视讯软件等。

Skype-不受限制的目的地 IP 网域： 进行 Skype 封锁，有可能会影响部分网站的正常访问或登录，所以当封锁 Skype 应用程序后，建议将常会用到的网站或是必要的网站加入例外清单之中，以避免无法正常访问网站或是登录该网站相关服务。

QQ-不受限制的 QQ 号码： 进行 QQ 封锁之后，仍可以针对不需受到限制的使用者开放 QQ 服务，此时就要将这些使用者 QQ 号码加入到不受限制的 QQ 号码清单之中，如下图：



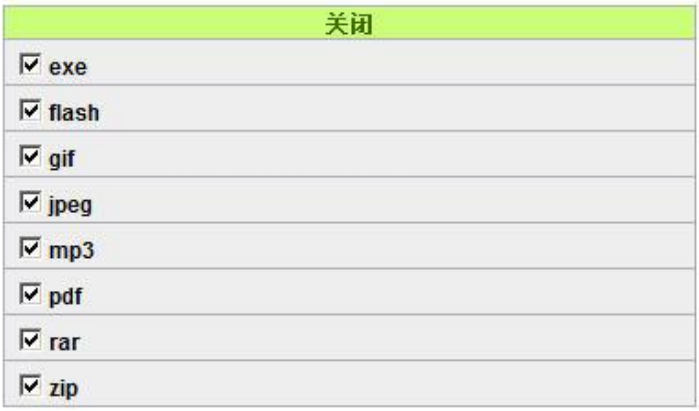
内网不受限制的 IP 地址： 针对以上所封锁的服务，开放内网不受限制的使用者 IP / IP 范围。

特定服务： 选择某个封锁的服务应用，进行不受限制的内网 IP 设定。

不受限制的 IP 地址： 针对上方所选的已封锁的应用服务，设定那些 IP 可以开放使用不受限制。

Block Filte Type： 封锁一些常用的档案格式传输，例如 exe 执行档、zip 压缩档等。

Block File Type



内网不受限制的 IP 地址： 针对以上所封锁的特殊档案格式，开放内网不受限制的使用者 IP / IP 范围。

确定: 点击此按钮“**确定**”即会存储刚才所变动的修改设定内容参数。

取消: 点击此按钮“**取消**”即会清除刚才所变动的修改设定内容参数，此操作必须于“确定”存储动作之前才会有效。

9.2 访问规则设置

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还是从外部到内部，或是设定以使 IP 地址、目地端 IP 地址、IP 通讯协议状态等条件来做管制，管理者可以依照实际的需求调性设置。

9.2.1 默认管制规则

管理者定订的网络存取规则条例，可以选择关闭或是允许来调整使用者对网络的存取。以下就针对路由器的网络存取规则条例做一说明：

路由器默认的网络存取规则条例：

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

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

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

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

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

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

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

* HTTP 的服务从 LAN 端到路由器 默认为开启的 (为了管理路由器使用)。

* DHCP 的服务从 LAN 端到路由器 默认为开启的 (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 默认为开启的 (为了解析 DNS 服务使用)。

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

访问规则设置

跳到 1 / 页　　5 每页显示的字段

优先权	激活	管制动作	服务端口	来源端口	来源位置	目的位置	管制时间	日		删除
	☑	允许	所有端口 [1]	局域网	任何的	任何的	所有时间			
	☑	关闭	所有端口 [1]	广域网1	任何的	任何的	所有时间			

增加新的管制规则　　回复原出厂预设值

除了默认规则以外， 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优先权 1-2-3…。依序做规则判断，所以优先权是让您在做存取规则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。

增加新的管制规则： 新增新的网络存取规则按钮可以新增一项新的存取规则。

恢复到出厂默认值： 可以恢复到出厂原有默认存取规则项目并删除所有的自定规则内容。

9.2.2 增加新的管制规则

存取服务规则设定

管制动作：	允许
服务端口：	All Traffic [TCP&UDP/1~65535]　服务端新增或删除表
日志：	关闭
来源接口：	局域网

来源IP地址：	单独	. . .
目的IP地址：	范围	. . . 到 . . .

时间管制设定

此存取规则	
全天	: 到 : (时间表示:24小时制)
每天	周日 周一 周二 周三 周四 周五 周六

返回　　确定　　取消

管制动作:

允许： 允许符合此管制条例行为的封包通过。

关闭： 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您所要允许或不允许的服务端口服务项目内容。

服务端新增或删除表: 若是您想要管制的服务端口服务内容没有存在于默认列表内的话，您可以点击右方的服务端新增或删除表来新增一个服务内容。于弹出窗口中输入一个服务名称以及通讯协议与端口，点击“新增”按钮即可新增一个管制服务项目内容。

日志: 允许: 依据此规则发生的相关事件将在日志中记录。
关闭: 依据此规则发生的相关事件不会日志中记录。

来源接口: 选择您所要允许或不允许的来源封包接口(例如是从 LAN， WAN1， WAN2 还是任何的)，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(如任何的，单独或者范围)，若是选择单独是范围的话，请输入此单一或是一区段范围的 IP 地址。
您也可以选择 IP 群组的方式来指定来源 IP。关于 IP 群组的设定，请参考(“7.6 IP 群组管理”说明)。

目的 IP 地址: 选择目的端封包的 IP 范围(如任何的，单独或者范围)，若是选择单独是范围的话，请输入此单一或是一区段范围的 IP 地址。

时间管制设定: 您可以将此条规则依照您所需要的执行时间来做控管。例如您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。

应用此存取规则: 选择“全部”表示都 24 小时都执行此规则(默认)，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…: …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: 点击此按钮“**确认**”即会存储刚才所变动的修改设定内容参数。

取消: 点击此按钮“**取消**”即会清除刚才所变动的修改设定内容参数，此操作必须于确认存储动作之前才会有效。

范例 1：若要将病毒端口 TCP 135-139 封锁要如何配置?

首先在服务端口新增部份加入 TCP 135-139 端口(请参考如何新增服务端口的章节)，然后进行以下的设定：

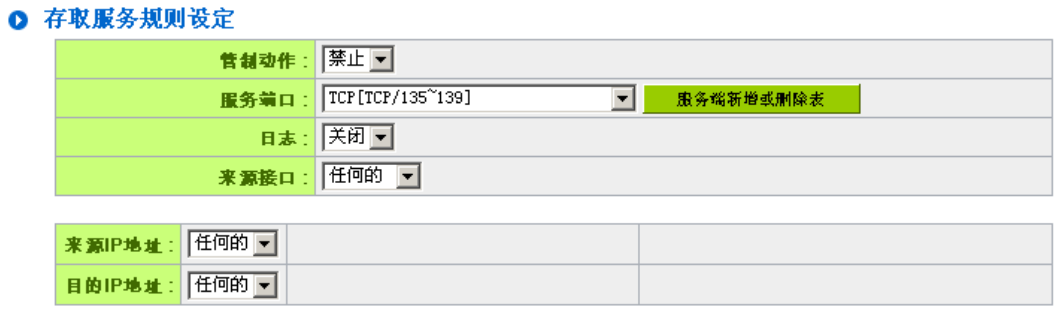
管制动作：禁止

服务端口：TCP135-139

来源接口：任何的(此意思为封锁由内网往外网以及从外网攻击内网的任何此端口)

来源 IP 地址：任何的(此意思为封锁由内网往外网以及从外网攻击内网的任何此端口)

目的 IP 地址：任何的(此意思为封锁由内网往外网以及从外网攻击内网的任何此端口)



范例 2：若要禁止内网 IP 段 192.168.1.200 到 192.168.1.230 禁止访问 80 端口要如何配置?

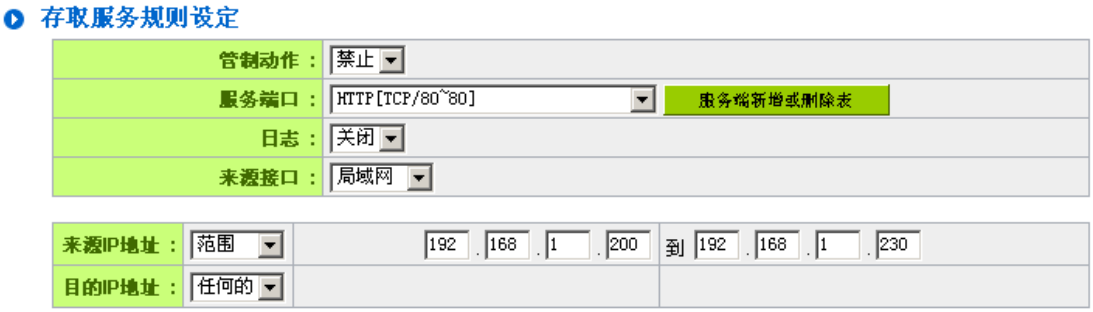
管制动作：:禁止

服务端口：TCP 80

来源界面：局域网(此意思为封锁由内网往外网的 80 端口)

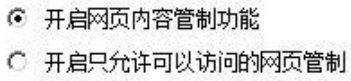
来源 IP 地址：范围 192.168.1.200 到 192.168.1.230

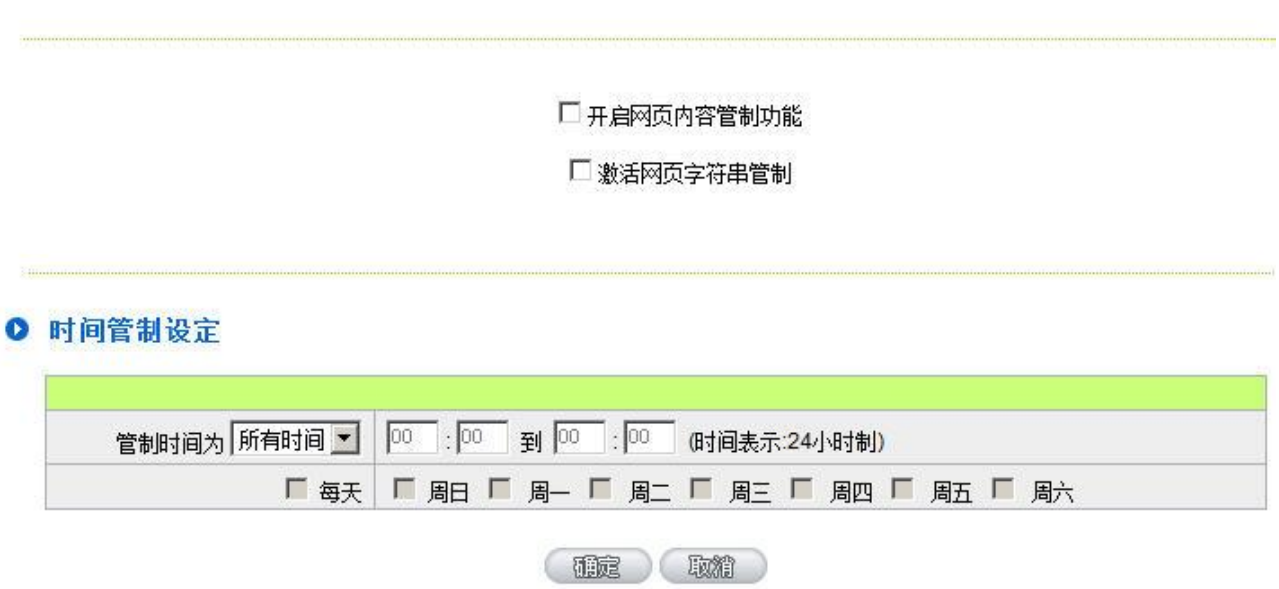
目的 IP 地址：任何的(此意思为封锁由 192.168.1.200 到 192.168.1.230 内网往外网任何 80 端口)



9.3 网页内容管制

路由器的网页内容管制可支持两种模式的网页管制，一为封锁不允许访问的网址，另一个为允许访问的网站，此两种模式只能使用一种。





封锁不允许访问的网址

此功能需将完整的网址如 www.sex.com 填入，即可封锁此网站。

网页内容管制

开启网页内容管制功能: 选择打勾开启网页内容管制功能，默认为关闭。

开启网页内容管制功能: 网页管制内容项目。

新增: 填写欲管制的网址，如 www.playboy.com。

例外 IP 地址/群组 可以填入不受管制的 IP 地址或是选择不受限制的 IP 群组。

增加到对应列表: 点击“增加到对应表”按钮新增此一欲管制的网址。

删除所选择的过滤项目: 可以使用鼠标点选一个或多个管制的网址，然后点击即可删除。

网页字符串管制：

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: 输入关键词。

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。

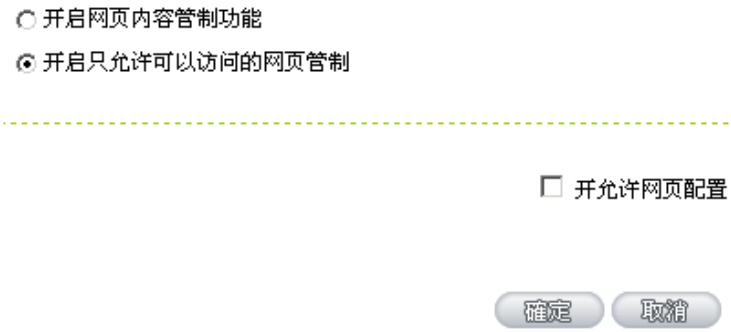
删除所选择的内容: 选择删除服务项目内容从服务表列内。

确定: 点击此按钮“**确定**”即会存储刚才所变动的修改设定内容参数。

取消: 点击此按钮“**取消**”即会清除刚才所变动的修改设定内容参数，此操作必须于“确定” 存储动作之前才会有效。

允许访问的网站

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。



勾选“开允许网页配置”，将显示如下图的设置窗口：

允许网页配置： 选择打勾开启允许网址管制功能，默认为关闭。

新增： 填写欲管制的允许网址，如 www.playboy.com。

增加到对应列表： 点击此按钮新增此欲管制的允许网址。

删除所选择的内容： 可以使用鼠标点选一个或多个管制的允许网址，然后点击即可删除。

不受限制的 IP

若是有 IP 地址或是 IP 群组不希望受到”允许网页”的管制，可以在这里将这些 IP 排除。

例外

例外 IP 地址/群组 可以填入不受管制的 IP 地址或是选择不受限制的 IP 群组。

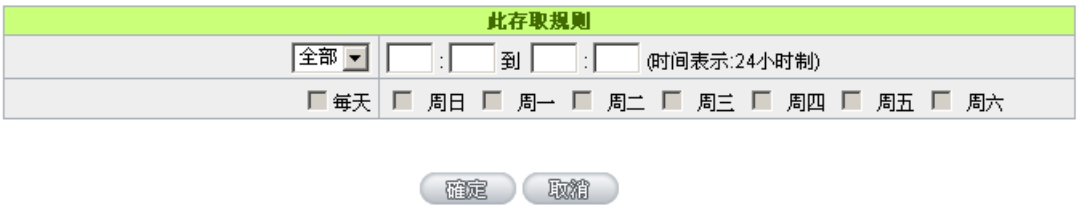
增加到对应列表: 点击此按钮新增此不受限制的 IP 或 IP 群组。

删除所选择的内容: 可以使用鼠标点选一个或多个不受限制的 IP 或 IP 群组，然后点击即可删除。

管制内容排程时间

当选择为“全部”时，表示此条规则 24 小时执行。若选择“…到…”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，您可以参考以下图例来管制。

时间管制设定



全部: 表示此管制规则 24 小时开启。

…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。

十、其它进阶高级功能设置

本章介绍路由器进阶功能的设定，如果内网需要设置服务器提供 Web/FTP 服务等，可以通过虚拟服务器的连接配置设置完成，同时应部分用户需要提供静态路由以及动态路由协议的设定，一对一 NA 功能的设定解决实体 IP 与虚拟 IP 对应，以及设置动态域名解析服务满足用户获得 ISP 的动态公网 IP 情况下需要建设 Web/FTP 服务器等要求。

10.1 DMZ/虚拟服务主机

10.1.1 DMZ 设定

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。

在使用“DMZ 主机”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。

点击此按钮“**确认**”即会存储刚才所变动的修改设定内容参数。 点击“**取消**” 即会清除刚才所变动的修改设定内容参数，此操作必须在确认存储动作之前才会有效。

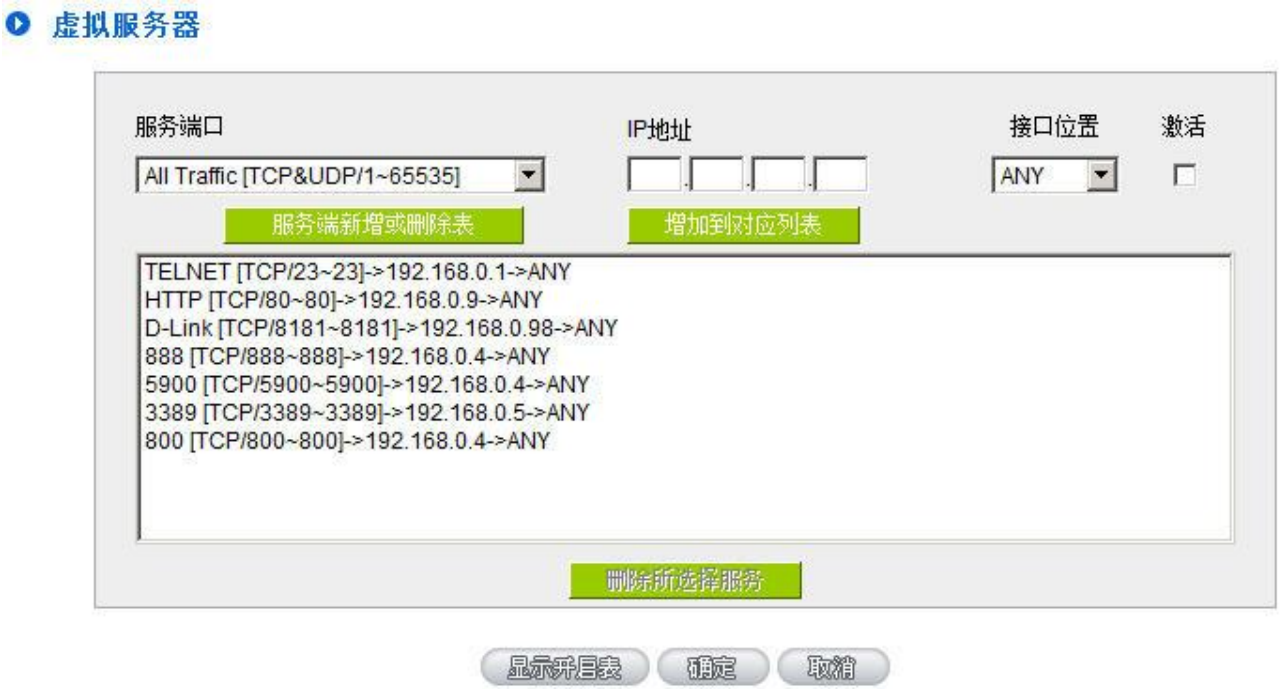
10.1.2 虚拟服务器设定

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，经过服务端口的转换，（如 WWW 为 80 端口），直接存取到内部虚拟 IP 的服务器的服务。例如在设定窗口中，选项填入服务器位置，如 192.168.1.2 且端口是 80 的话，当外部网络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，就会通过路由器的公网 IP 地址去转换到 192.168.1.2 的虚拟主机上的 80 端口读取网页了。

其它种类的服务器设定，都如以上设定；只要将所用服务器的服务端口以及虚拟主机的 IP 地址填入即可！



服务端口号： 在此选择欲开启的虚拟服务器的服务端口号码默认列表，如 WWW 为 80(80~80)， FTP 为 21~21，可参考服务号码默认列表！

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

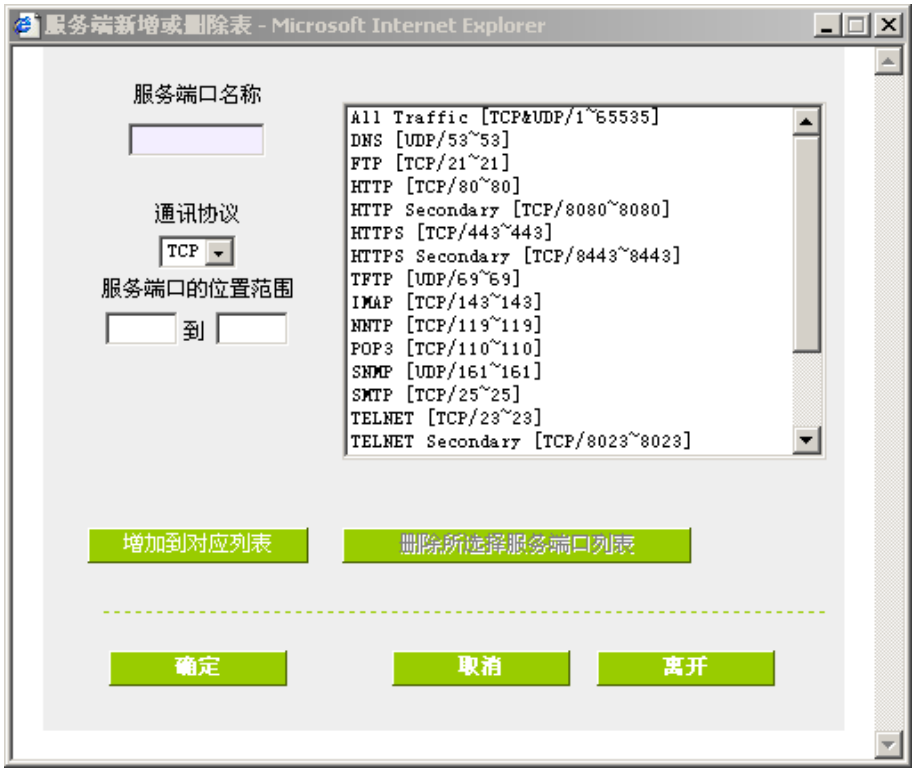
激活： 开启此服务功能。

服务端口新增或删除表： 若您所需要的服务端口没有在列表里面，可以利用此功能新增或删除管理服务端口号列表。

增加对应列表： 增加到开启服务项目内容。

新增或删除管理服务端口号

若您欲开启的服务端口项目没有在表列中，您可以点击“服务端新增或删除表”新增或删除管理服务端口号列表，如下图所示：



服务端口名称： 在此自定欲开启的服务端口号名称加入列表中，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。

服务端口的位置范围： 将您所需新增加的服务端口范围填入。

增加到对应列表： 增加到开启服务项目内容列表，最多可新增 100 组。

删除所选服务端口列表： 删除所选择的开启服务项目之一笔内容。

确定： 点击此按钮“**确认**”即会存储刚才所变动的修改设定内容参数。

取消： 点击此按钮“**取消**”即会清除刚才所变动的修改设定内容参数，此操作必须于确认存储动作之前才会有效。

离开： 离开此功能设定窗口。

10.1.3 特殊应用软件配置：

有一些特殊应用软件其进出互联网的服务端口号为非对称的，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，如以下窗口所示：

特殊应用软件名称： 您可以自定此特殊应用软件名称，方便管理使用！

出去服务端口的位置范围： 输入由路由器出互联网的使用端口(Port Number)编号(如9000~10000)。

进入服务端口的位置范围： 输入由互联网进入的使用端口(Port Number)编号。 (如2004~2005) 。

增加到对应列表： 增加到开启服务项目内容列表。

删除所选已开启服务端口项目： 删除所选择的开启服务项目之一笔内容。

显示开启表： 点击此按钮即会显示列表上的所有设定项目内容参数。可以以“虚拟主机服务器”和“特殊应用软件”分别来查看列表。

确定： 点击此按钮“**确认**”即会存储刚才所变动的修改设定内容参数。

取消：	点击此按钮“**取消**”即会清除刚才所变动的修改设定内容参数，此操作必须于确认存储动作之前才会有效。

10.2 路由通讯协议

此节介绍动态路由协议以及静态路由的设定。

动态路由协议

指定路由协议

10.2.1 动态路由设定

RIP 是路由通讯协议 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丨，此时若是不想手动设置每台路由器的绕径表，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，采用距离向量的方式以封包到达目的地之前需要经过的路由的个数来做传送距离的判断，而不以实际联机的速率来做判断。所以所选的路径是经过最少的路由，但是并不一定反应速度最快的路由及路径。

选择路由器运作模式： 选择路由器运作模式为 NAT 模式或是路由模式。

动态路由通讯协议 RIP 功能： 选择按钮“激活”开启使用 RIP 动态路由通讯。

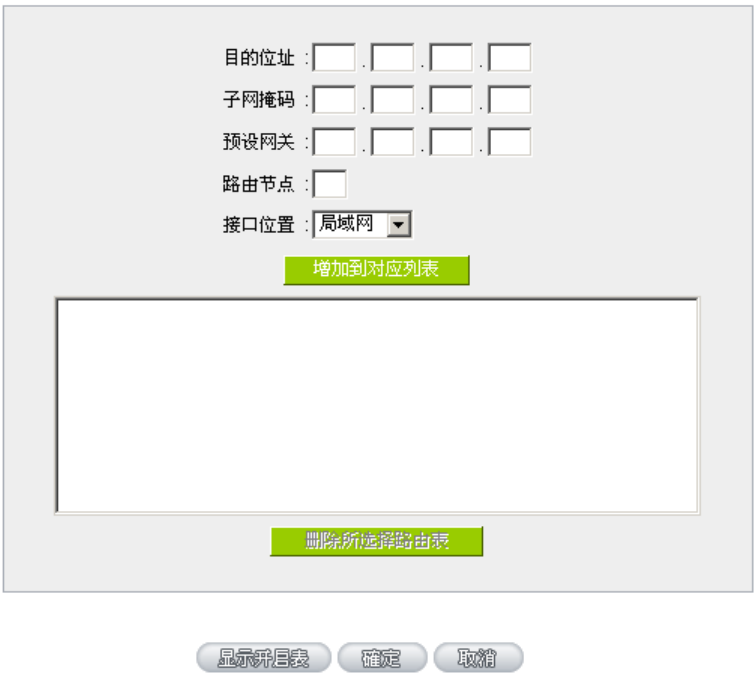
传送动态路由通讯协议功能： 可于上下选择按钮选择使用动态路由通讯 None， RIPv1， RIPv2， Both RIPv1 and v2 作为传送动态路由通讯协议格式。

接收动态路由通讯协议功能： 可于上下选择按钮选择使用动态路由通讯 None， RIPv1， RIPv2-Broadcast， RIPv2-Multicast， 为接收动态路由通讯协议格式。

10.2.2 静态路由设定

静态路由是以手动设置路由表的方式来达成封包路由。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邮件服务器，或游戏服务器是架设在不同一 ISP 环境而且 ISP 之间无法彼此互通，此时去邮件服务器或是去游戏服务器就应该走不同的 WAN，而避免绕远路。这个用意跟协议绑定是有相似的做用。

指定路由通讯协议



目的地址和子网掩码： 填入目的地的远程网络 IP 节点与子网络节点地址。

默认网关： 从此网络节点到目的远程网络欲绕径的默认网关器地址。

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，默认为 1。(最大为 15)。

接口位置： 此网络节点的连接位置，是位于广域端口 WAN 端亦或是局域端口 LAN 端。

增加到对应列表： 增加此路径规则到列表中。

删除所选路由表： 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： 点击此按钮“**确认**”即会存储刚才所变动的修改设定内容参数。

取消： 点击此按钮“**取消**”即会清除刚才所变动的修改设定内容参数，此操作必须于确认存储动作之前才会有效。

10.3 一对一 NAT 对应

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。路由器提供您可将除了路由器本身 WAN 端口以及光纤盒或 ATU-R(网关) 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，但当做了一对一对应后，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 服务器”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 地址不能被涵盖在一对一 NAT 的 IP 范围设定中。

一对一 NAT 功能: 选择是否开启此一对一 NAT 功能 “激活”开启 “禁止”关闭。

内部范围 IP 地址: 虚拟 IP 地址起始 IP 地址。

外部范围 IP 地址: 外部合法 IP 地址起始 IP。

对应 IP 数量: 填入您同时要有多少个外部合法 IP 地址需要对应。

增加到对应列表: 加入此设定到一对一 NAT 列表中。

删除所选对应列表: 删除所选择的一对一 NAT 规则。

确定: 点击此按钮“**确认**”即会存储刚才所变动的修改设定内容参数。

取消: 点击此按钮“**取消**”即会清除刚才所变动的修改设定内容参数，此操作必须于“确定”存储动作之前才会有效。

注意！

一对一的 NAT 模式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 公网 IP 的服务服务器

或计算机将会曝露在互联网上。若要阻绝网络的使用者主动联机到一对一 NAT 的服务服务器或计算机，请到防火墙的存取规则中设定适当的拒绝存取规则条件。

多对一 NAT 对应

当您需要设定某部分内网 IP 地址 / 范围，固定转 NAT 某个 WAN IP 出去，用来注册特别的服务或是网络架构，就可以透过多对一 NAT 对应进行设定。

启用多对一 NAT 功能: 选择是否开启此多对一 NAT 功能 “启动”开启 “禁止”关闭。

内部 IP 地址范围: 内网虚拟 IP 地址范围。

对应的广域网 IP 地址: 设定固定对应的广域网 (WAN) IP 地址，需搭配下方所选择的广域网界面，若该 IP 地址不在该广域网界面包含的范围之内，设定是无效的。

界面: 选择广域网 IP 所对应的界面，，若上方对应 WAN IP 地址不在该广域网界面包含的范围之内，设定是无效的。

增加到对应列表: 加入此设定到一对一 NAT 列表中。

删除所选对应列表:	删除所选择的一对一 NAT 规则。
确定:	点击此按钮“**确认**”即会存储刚才所变动的修改设定内容参数。
取消:	点击此按钮“**取消**”即会清除刚才所变动的修改设定内容参数，此操作必须于“确定”存储动作之前才会有效。

10.4 DDNS-动态域名解析

此路由器的 “DDNS” 功能可以支持 QnoDDNS.org.cn、Dyndns.org 与 3322.org 三家的动态域名解析功能，其目的是为了让使用动态 IP 地址(也就是无法有固定 IP 的环境)来架设虚拟服务器、建立企业 VPN 使用、及远程监控时查询现在的路由器 IP。如 ADSL PPPoE 计时制或是 Cable Modem 的使用者的 WAN IP 地址都会随 ISP 端要求而改变，当此时使用者申请了 DDNS 后，如“qno. QnoDDNS.org.cn”，将其设定在 DDNS 设定中，则在远程只要去 Ping QnoDDNS.org.cn 则可以知道现在路由器的实际 IP。且若是内部有架设网站之类的服务，网络使用者只要在网址打上 qno. QnoDDNS.org.cn 就可以直接进入到您内部架设的 WEB。在设定此功能之前，请向 www.qno.cn/ddns、www.dyndns.org 或是 www.3322.org 提出申请，此三个服务是完全免费的！

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 都可同时对此三家 DDNS 做动态 IP 升级。

DDNS动态域名解析

接口位置	状态	主机名称	配置
广域网1	Dyndns 关闭 3322 关闭 Qnoddns 关闭	Dydns:--- 3322:--- Qno:---	编辑
广域网2	Dyndns 关闭 3322 关闭 Qnoddns 关闭	Dydns:--- 3322:--- Qno:---	编辑
广域网3	Dyndns 关闭 3322 关闭 Qnoddns 关闭	Dydns:--- 3322:--- Qno:---	编辑
广域网4	Dyndns 关闭 3322 关闭 Qnoddns 关闭	Dydns:--- 3322:--- Qno:---	编辑
广域网5	Dyndns 关闭 3322 关闭 Qnoddns 关闭	Dydns:--- 3322:--- Qno:---	编辑

选择您要配置的广域网端口，比如“广域网 1”，点击“编辑”进入广域网 1 的 DDNS 配置窗口，对要设置的 WAN 口的 DDNS 方式进行勾选。

接口位置 显示使用者所选取的广域端口

DDNS 动态域名解析服务： 可以选择 QnoDDNS.org.cn、Dyndns.org 以及 3322.org 等三家(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。QnoDDN 使用者名称要填入完整的网址，如：abc.qnoddns.org.cn。

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.QnoDDNS.org.cn 或者 abc.dyndns.org。

内部地址： 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 地址后会自动显示于此。

状态： 显示目前路由器对 DDNS 的更新状态。

确定： 点击此按钮“**确认**”即会存储刚才所变动的修改设定内容参数。

取消： 点击此按钮“**取消**”即会清除刚才所变动的修改设定内容参数，此操作必须于确认存储动作之前才会有效。

10.5 广域网接口 MAC 地址设定

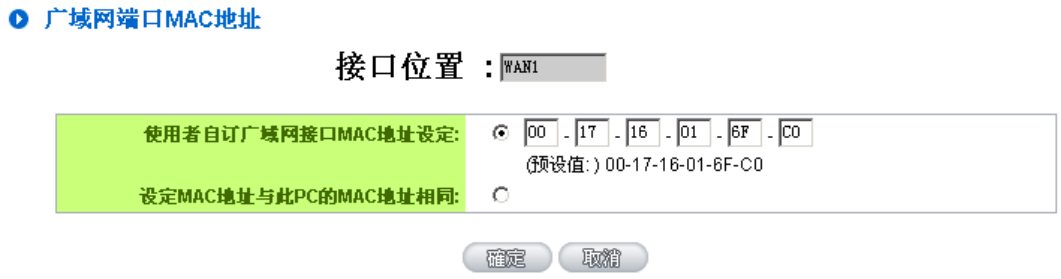
有些 ISP 会要求提供一固定 MAC 地址(网卡物理地址)做为 ISP 端分配 IP 给您的认证使用，此大多适用于 Cable Mode 的用户。若有此需求的话，可使用此功能将提供给 ISP 的网卡物理地址(MAC 地址：00-xx-xx-xx-xx-xx)填入此项目中，路由器就会以此 MAC 地址作为跟 ISP 请求 IP 时的认证！

广域网端口MAC地址

接口位置	MAC地址	配置
广域网1	00-17-16-F0-65-21	编辑
广域网2	00-17-16-F0-65-22	编辑
广域网3	00-17-16-F0-65-23	编辑
广域网4	00-17-16-F0-65-24	编辑
广域网5	00-17-16-F0-65-25	编辑

选择您要配置的广域网端口，比如“广域网 1”，点击“编辑”进入广域网 1 的端口 MAC 地址配置窗口，使用者可以自行输入提供给 ISP 的网卡物理地址 MAC，点击此按钮“**确认**”即会存储刚才所变动的修改设定内容参数，点击此按钮“**取消**”即会清除刚才所变动的修改设定内容参数，此操作必须于确认存储动作之前才会有效。

目前设备出厂默认的 MAC 位置为 WAN 端的 MAC 地址。



十一、工具程序功能设定

此章节介绍用来管理路由器以及测试网络联机的工具。

考虑安全的因素，建议修改密码。关于登录密码与路由器时间的设定已经在第五章 5.2 节已经介绍，在此就不做重复介绍了。

11.1 在线联机测试

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

网域名称查询测试

请于此测试窗口输入您想查询的网域主机位置名称，如 www.abc.com 然后点击开始的按钮开始测试。测试结果会显示于此窗口上。

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，可以由此功能了解网络上的计算机是否存在！

请于此测试窗口输入您想测试的主机位置 IP，如 168.95.1.1 点击开始的按钮开始测试，测试结果会显示在窗口上。

11.2 系统固件升级

此功能可以让路由器 在 Web 设定窗口中直接做固件升级。请您于升级前先确认固件版本信息。 点击“浏览”按钮，选择固件存放数据夹，并于选择欲升级的固件后，**点击立即系统软件更新**做升级。

注意！

执行固件升级前，请详细阅读窗口中的注意事项。

正在做固件升级当中时，请勿离开此升级窗口，否则会造成路由器升级失败。

11.3 系统设定参数存储

配置文件设定文件汇入：

此功能将之前所存储在计算机的备份设定参数内容回存到路由器中！选择“浏览”至备份参数文件“config.exp”存放数据夹，选择该文件后，点击“汇入”按钮做设定文件汇入。

系统配置参数文件存储：

此功能为存储网管人员在路由器的设定参数备份到计算机中，通常做路由器版本升级前，请务必将您现在的路由器设定文件用此功能存储在计算机中！点击存储按钮，选择至备份参数文件“config.exp”存放数据夹位置，点击存储即可。

系统配置设定文件文件储存：

此功能为 IP & MAC Binding、QoS、Protocol Binding 三个功能的规则设定值储存，可以单独将这些设定规则汇出储存或是汇入路由器 (上方汇入设定文件功能)。

11.4 SNMP 网络管理设定

SNMP 为 Simple Network Management Protocol 的缩写，指网络管理通讯协议。此为互联网上使用的一个管理工具，通过此 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之通讯使用。VPN QOS 安全路由器支持标准 SNMP v1/v2c，可以搭配标准 SNMP 网络管理软件来得知目前 VPN QOS 安全路由器上的机器运作情况，以便随时掌握网络信息。

激活： 将 SNMP 功能开启或关闭。系统默认为开启此功能。

系统名称： 设置机器的名称，如 VPN Firewall。

联系方式： 设置机器的管理联系人员名称。

系统地址： 设置机器的目前所在位置。

Get Community Name： 设置一组管理者参数可以取得此机器的项目信息，系统默认"Public"。

Set Community Name： 设置一组管理者参数可以设置此机器的项目信息，系统默认"Private"。

Trap Community Name： 设置一组管理者参数可以传送 Trap 的信息。

Send SNMP Trap 到： 设置一组 IP 地址或是域名名称的接收 Trap 讯号主机。

确定： 点击此按钮"确认"即会存储刚才所变动的修改设置内容参数。

取消：

点击此按钮"取消"即会清除刚才所变动的修改设置内容参数，此操作必须于确认存储动作之前才会有效。

11.5 系统恢复

您可以于此工具中选择路由器系统重新开机功能，请点击“系统重新启动(Reset)”的“立即重新激活)” 按钮即可重新开机启动。

系统重新启动

如图，如果点击系统启动下的“立即重新激活”,会弹出提对话框提示是否重新启动路由器，确定路由器就做重新启动操作。

恢复原出厂默认值

若是选择重新恢复“立即重新激活”， 会弹出提对话框提示是否恢复出厂值，确定后路由器将做恢复出厂值操作。

我们建议在做版本升级前请先将路由器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(如何存储路由器的设定数据及升级完成后如何存回路由器，请参考 11.3 系统设定参数存储说明)。

11.6 备援功能

High Availability 备援功能一般是使用于需要架构容错与备援机制的网络环境，通常是透过两个一模一样的设备互作备援，平时由其中一台设备做主要的网络传输，另一台为闲置直到负责主要传输的设备发生网络传输问题时，才马上运做起来使网络传输与相关服务不致中断，也提供网络管理人员更多处理问题的机会与时间，不会因为只有一台设备而导致发生问题时无从下手。

除了提供一般市面规格的 HA 外，侠诺也提供了两台设备能够同时进行网络传输与备援功能的进阶 HA 功能，不用将另外一台设备完全闲置，完全充分利用两台设备的成本效益，并且也不一定必须是要同一种设备，只要都是侠诺且都有支持 HA 的功能设备即可达成。

备援功能： 激活：表示启用 HA 备援功能。

关闭：表示关闭 HA 备援功能。

备援模式： (1) 硬件备份模式：

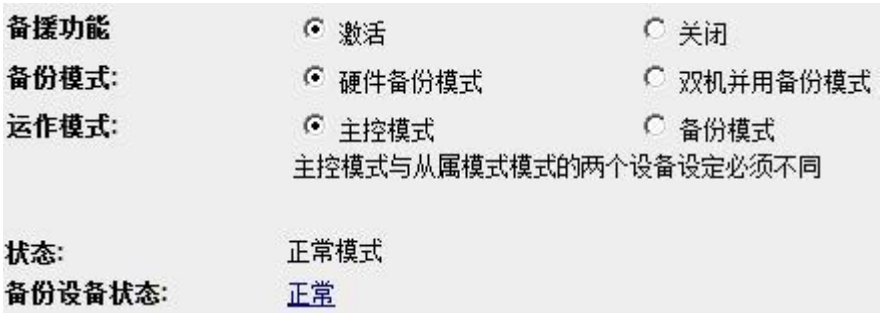
为一般规格的备援模式，即两台设备一台负责主要的网络传输，一台完全闲置，直到负责主要传输的设备发生问题，会发出讯息告知闲置的设备立即接手网络传输工作。

(2) 双机并行备援模式：

网络的应用架构是两个设备会同时担负对外连线任务，但仍然会有主要与备援模式分别，主控模式设备在正常状态下为主要 DHCP IP 配发者，备份模式设备在正常状态下则会自动关闭 DHCP 服务器不提供 DHCP 配发 IP 服务，直到主控模式设备发生问题，由备份设备接手所有对外连线任务时，备份模式的设备才会激活 DHCP 服务器提供配发 IP 服务。

以下就以此两个不同模式分别进行说明：

硬件备份模式

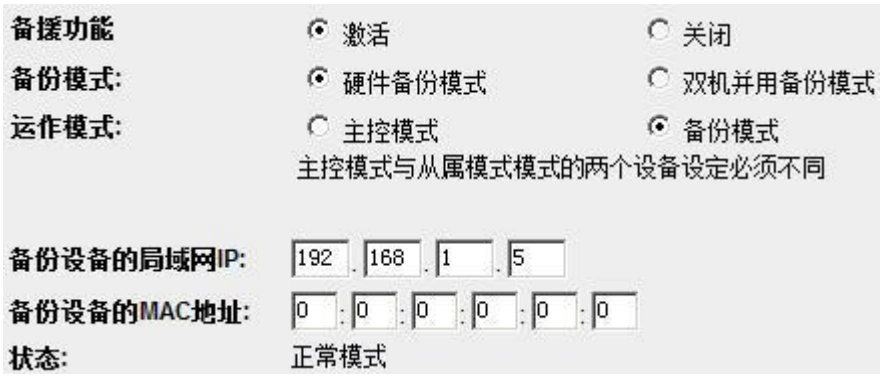


※选择运作－主控模式： 表示负责所有对外网络连线工作，发生问题时由另一台设备接手备援

状态： 「状态－正常模式」表示一切运作正常。

备份设备状态： 显示目前负责备援的设备状态是否正常，若正常则可以点选链接直接从远程进入负责备援设备进行管理（另一台必须开启远程管理功能）。

「状态－异常」表示负责备援的另一台设备无法侦测到或不存在，需检查另一台设备目前的状况。



※选择运作－备份模式： 表示此设备是负责当「主控模式」发生问题时的接手备援任务，所以此设备的广域网 WAN 与局域网 LAN IP 设定必须与「主控模式」设备的设定完全相同，并且此备援设备平时不负责对外的网络传输以及 DHCP 配发 IP 任务。

※若原本的局域网 LAN 是用「主控模式」的 DHCP 配发 IP，那么「备份模式」设备的 DHCP 服务器设定也要与「主控模式」的 DHCP 服务器设定完全相同，这样才能在备援模式真正进行备援动作时，让 DHCP 工作继续正常并且局域网络对外连线不中断。

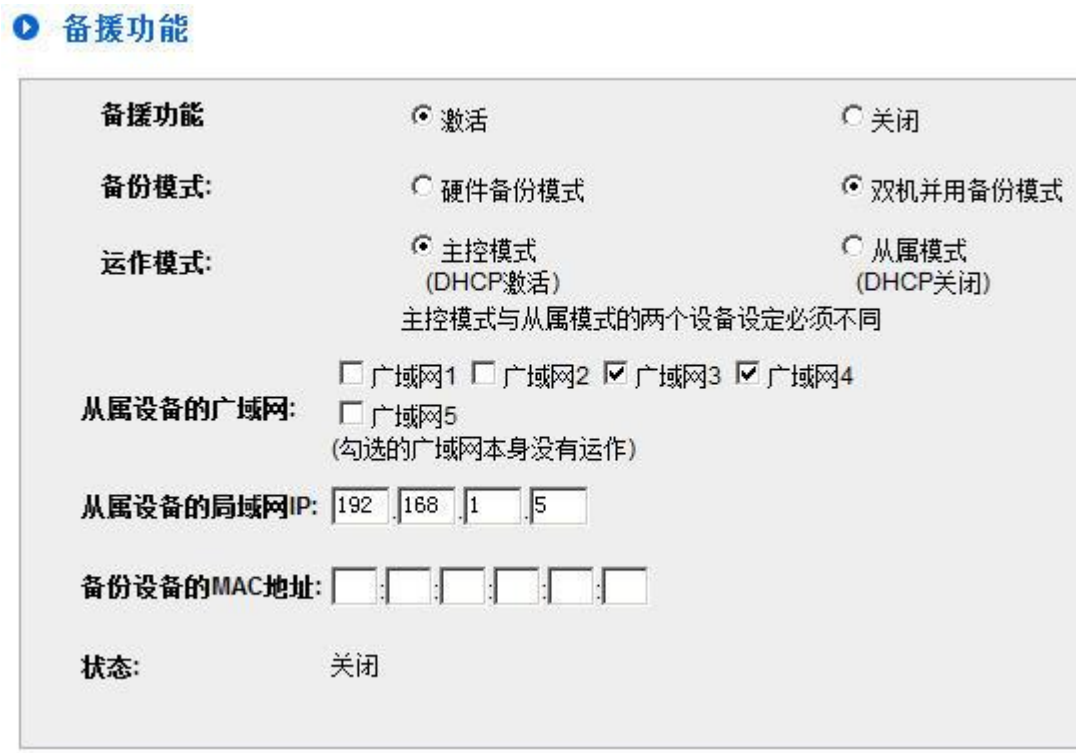
备份设备的局域网 IP： 请填入「主控模式」设备的 LAN IP 地址。(因为是「被」备援)

备份设备的 MAC 地址： 请填入「主控模式」设备的 MAC 地址。(因为是「被」备援)

状态： 「状态－正常模式」表示目前此备援设备完全闲置，「主控模式」设备工作正常；

「状态－备援模式」表示目前此设备已进入接手备援状态负责全部网络传输，「主控模式」设备发生问题，直到 「主控模式」设备正常启动并且发送讯息告知此设备，状态才会恢复成「状态－正常模式」闲置状态。

双机并行备份模式：



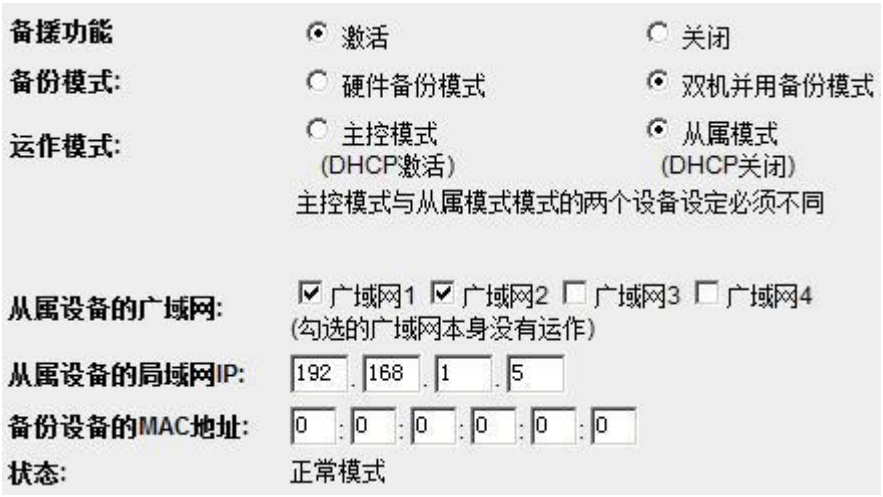
※运作模式－主控模式： 表示虽然与另一台共同负责对外网络连线工作，但是更多了一个 DHCP 配发 IP 的任务，因为从属模式的设备虽然也有对外连线，但是 DHCP 服务器是不启用的。

从属设备的广域网：
(勾选的广域网本身没有运作) 勾选本身没有运作交给另外一台负责的广域网 WAN 连线，譬如总共四条线路，本身是负责 WAN1 与 WAN2 的对外连线，WAN3 与 WAN4 则交给另外一台负责，则此时就要勾选 WAN3 与 WNA4。

从属设备的局域网 IP： 设定另一台从属模式设备所使用的局域网 IP 地址，必须与本身(主控模式)的局域网 IP 不同。

备份设备的 MAC 地址： 设定另一台从属模式设备所使用的局域网 MAC 地址，必须与本身(主控模式)的局域网 IP 不同。

状态： 「状态－正常模式」表示两台设备目前运作正常；「状态－备援模式」表示另一台 (从属模式) 设备发生问题，本机已启用备援功能，接手进行需要备援的广域网连线。



※运作模式－从属模式： 表示虽然与另一台共同负责对外网络连线工作，但是本身的 DHCP 服务器功能是关闭的，所以局域网 LAN 的用户要从从属模式设备的广域网 WAN 传输流量，需要在确认从属模式设备的局域网 LAN IP，与「主控模式」设备的局域网 LAN IP 不同，但是要在同一个子网络中。

举例来说，若主控模式设备的 DHCP 服务器 IP 地址为 192.168.1.1 子网掩码 255.255.255.0，则另一台从属模式的设备也必须与 192.168.1.1 在同一个子网络中如 192.168.1.2。

从属设备的广域网：(勾选的广域网本身没有运作) 勾选本身没有运作交给另外一台负责的广域网 WAN 连线，譬如总共四条线路，本身是负责 WAN1 与 WAN2 的对外连线，WAN3 与 WAN4 则交给另外一台负责，则此时就要勾选 WAN3 与 WNA4。

从属设备的局域网 IP： 设定另一台主控模式设备所使用的局域网 IP 地址，必须与本身(从属模式)的局域网 IP 不同。(但是一定要在同一个子网络中)

备份设备的 MAC 地址： 设定另一台主控模式设备所使用的局域网 MAC 地址，必须与本身(从属模式)的局域网 IP 不同。

状态： 「状态－正常模式」表示两台设备目前运作正常；「状态－备援模式」表示另一台（主控模式）设备发生问题，本机已启用备援功能，接手进行需要备援的广域网连线，并启用 DHCP 服务器功能。

十二、日志功能设定

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

12.1 系统日志

路由器的日志记录提供三种设定：系统日志， 电子邮件通知，以及选择日志的类别。

系统日志

激活系统日志: 若是勾选此选项的话，系统日志功能将被开启。

系统日志服务器: 路由器 提供了外部系统日志服务器收集系统信息功能。系统日志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 的系统日志 提供了包含动作中的联机来源位置与目地位置，服务编号以及状态。输入您要接收系统日志的服务器名称或是 IP 地址于“系统日志服务器”的空格字段内。

系统日志配置

路由器 提供了包含以下的告警内容信息，您只要打勾点选即可包含在日志信息中。

Syn Flooding：	即在短时间内传送大量的 syn 封包，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，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，造成系统当机。
登录认证错误：	当系统发现有企图登录路由器的入侵者时，就会将信息传到系统日志中。

一般系统日志信息

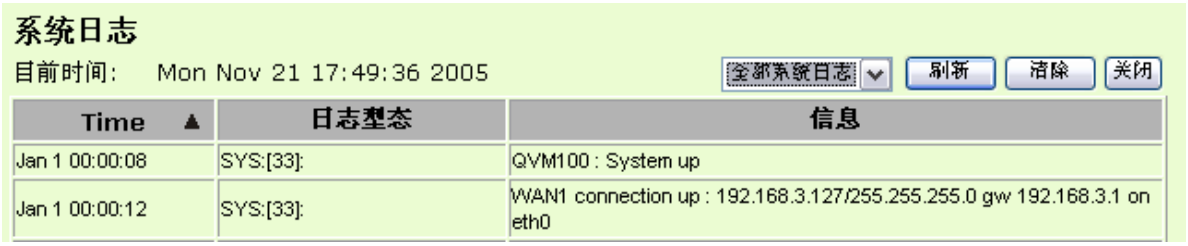
路由器 提供了包含以下的一般性内容信息，您只要打勾点选即可。系统错误信息，被阻挡的管制条例，允许通过的管制条例，认证登录，系统配置变更。

被阻挡的管制条例：	当有用户试图进行存取规则中不允许的规则时，此信息会传送到系统日志中。
允许通过的管制条例：	当用户进行存取规则所允许的规则时，此信息会传送到系统日志中。
认证登录：	每一个成功登录系统的 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日志的按钮，分别叙述如下：

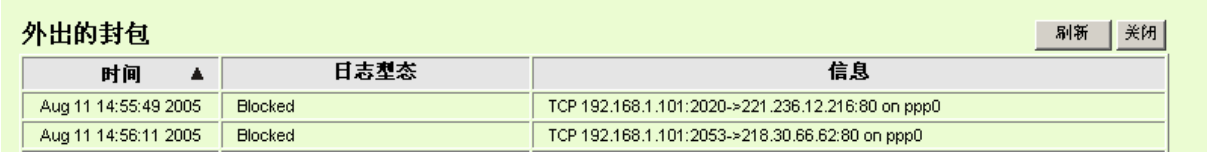
查看系统日志：

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，包含所有信息， 系统日志，防火墙日志，VPN 日志。选择“刷新”按钮可以刷新日志显示窗口，“清除”按钮可以清除所有日志记录。如下图所示：



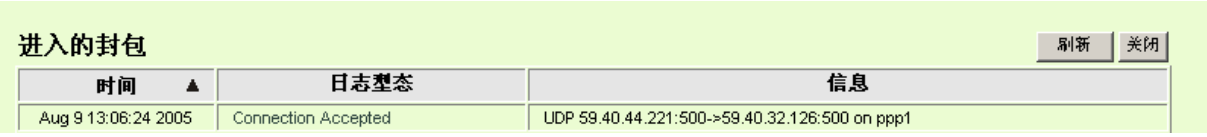
外出的封包：

查看内部 PC 出互联网 的系统封包日志，此日志包含内部网络地址，目的地地址以及所使用的通讯服务端口号、类型等信息。



进入的封包：

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， 目的地地址与通讯端口号等信息。



清除日志：

此按钮为清除所有目前路由器的日志相关信息。

12.2 系统状态实时监控

路由器的系统状态实时监控管理功能可以提供系统目前的运作信息，包含局域或广域端口名称，目前端口联机状态，IP 地址，网络实体位置(MAC 地址)，子网掩码，默认网关，域名解析服务器(DNS)，网络侦测，收到的封包数量，传送的封包数量，全部的进出封包数量统计，收到的封包 Byte 流量统计，传送的封包 Byte 流量统计，全部进出的封包 Byte 流量统计，收到的错误封包统计以及端口丢弃的封包统计，联机数，新联机数，上传带宽使用率，下载带宽使用率等信息。

下一页

接口位置：	广域网1	广域网2	广域网3	广域网4
机器名称：	eth1	ppp2	eth3	eth4
状态：	联机	联机	激活	激活
IP地址：	61.222.81.94	220.138.129.249	0.0.0.0	0.0.0.0
MAC地址：	00-17-16-03-00-91	00-17-16-03-00-92	00-17-16-03-00-93	00-17-16-03-00-94
子网掩码：	255.255.255.0	255.255.255.255	0.0.0.0	0.0.0.0
预设网关：	61.222.81.65	218.160.188.254	0.0.0.0	0.0.0.0
域名解析服务器(DNS)：	168.95.1.1	168.95.192.1	0.0.0.0	0.0.0.0
线路侦测机制：	测试成功	测试成功	测试失败	测试失败
接收封包统计：	20924	7094	0	0
传送封包统计：	16869	596	0	0
全部封包统计：	37793	7690	0	0
封包接收Byte数里：	2081710	706753	0	0
封包传送Byte数里：	16800576	64359	0	0
全部封包Byte数里：	18882286	771112	0	0
目前接收流里 Bytes/Sec：	3985	330	0	0
目前传送流里 Bytes/Sec：	102479	0	0	0
错误封包统计：	0	0	0	0
丢弃封包统计：	0	0	0	0
联机数：	0	0	0	0
新联机数/秒：	0	0	0	0
上传带宽使用率(%)：	1	0	0	0
下载带宽使用率(%)：	0	0	0	0

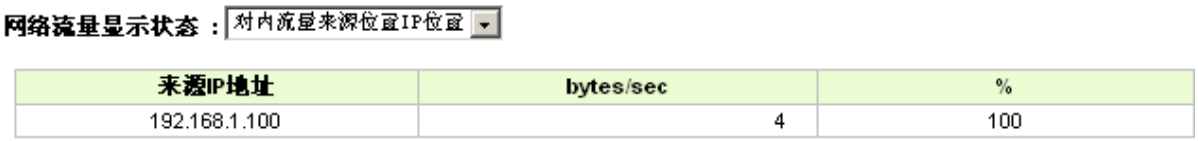
刷新

12.3 流量统计

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。

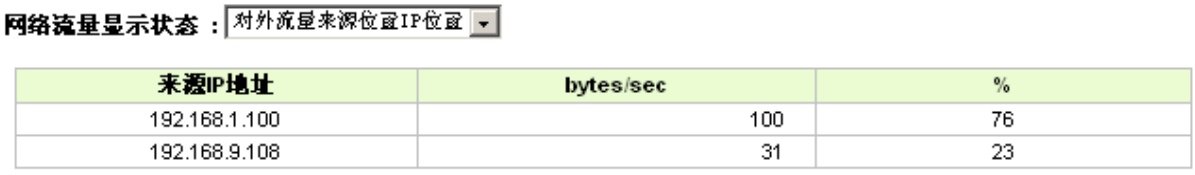
对内流量内网 IP 地址：

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。



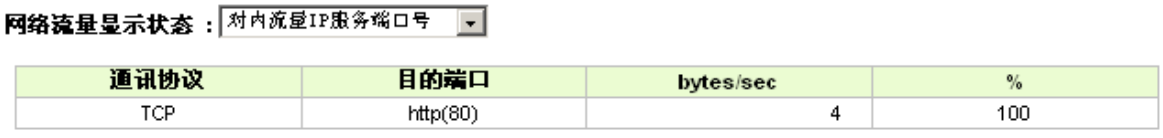
对外流量内网 IP 地址：

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。



对内流量 IP 服务端口号：

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。



对外流量 IP 服务端口号：

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。

网络流量显示状态：对外流量IP服务端口号

通讯协议	目的端口	bytes/sec	%
TCP	http(80)	905	97
UDP	dns(53)	18	2

对内流量 IP 联机数：

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。

网络流量显示状态：对内流量IP联机数

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	1678	202.108.15.42	80	51	76
192.168.1.100	TCP	1672	202.108.9.30	80	4	5

对外流量 IP 联机数：

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。

网络流量显示状态：对外流量IP联机数

来源IP地址	通讯协议	来源端口	目的IP地址	目的端口	bytes/sec	%

12.4 特定 IP 及端口状态

路由器提供网管人员可以针对某一 IP 或某一特定端口去查询此 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多 WAN 端口而必须走单一个 WAN 端口，网管人员可以查询出此目的地的 IP 做协议绑定来解决此登录问题。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。

IP/端口即时状态

IP/端口即时状态 特定IP地址/端口状态 : IP地址 IP地址 : 192 . 168 . 1 . 100 开始

来源IP地址	通讯协议	来源端口	接口位置 (WAN)	目的IP地址	目的端口	下载 Bytes/Sec	上传 Bytes/Sec
192.168.1.100	TCP	1243	WAN3	69.63.178.121	80	0	0
192.168.1.100	TCP	1244	WAN3	69.63.178.121	80	0	0
192.168.1.100	TCP	1240	WAN3	69.63.184.150	80	0	0

刷新

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端口号。

IP/端口即时状态

IP/端口即时状态 特定IP地址/端口状态 : IP地址 IP地址 : 192 . 168 . 1 . 100 开始

来源IP地址	通讯协议	来源端口	接口位置 (WAN)	目的IP地址	目的端口	下载 Bytes/Sec	上传 Bytes/Sec
192.168.1.100	TCP	1243	WAN3	69.63.178.121	80	0	0
192.168.1.100	TCP	1244	WAN3	69.63.178.121	80	0	0
192.168.1.100	TCP	1240	WAN3	69.63.184.150	80	0	0

刷新

特定端口状态：

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

来源IP地址	通讯协议	来源端口	接口位置 (WAN)	目的IP地址	目的端口	下载 Bytes/Sec	上传 Bytes/Sec
192.168.1.101	TCP	4022	WAN1	207.68.178.239	80	0	0
192.168.1.101	TCP	4023	WAN1	207.68.178.239	80	0	0
192.168.1.101	TCP	4027	WAN1	207.46.78.247	80	0	0
192.168.1.101	TCP	4028	WAN1	211.72.248.16	80	0	0
192.168.1.101	TCP	4031	WAN1	220.130.117.62	80	0	0
192.168.1.101	TCP	4032	WAN1	207.46.78.247	80	0	0
192.168.1.101	TCP	4035	WAN1	207.68.178.239	80	0	0
192.168.1.101	TCP	4037	WAN1	65.54.194.118	80	0	0
192.168.1.101	TCP	4038	WAN1	207.68.178.239	80	0	0
192.168.1.101	TCP	4039	WAN1	207.68.178.61	80	0	0
192.168.1.101	TCP	4048	WAN1	207.46.78.247	80	0	0
192.168.1.101	TCP	4050	WAN1	207.68.178.239	80	0	0
192.168.1.101	TCP	4051	WAN1	207.68.178.61	80	0	0
192.168.1.101	TCP	4053	WAN1	65.54.194.118	80	0	0
192.168.1.101	TCP	4054	WAN1	207.68.178.239	80	0	0
192.168.1.101	TCP	4058	WAN1	207.46.78.247	80	0	0

12.5 QRTG (Qno Router Traffic Grapher)

QRTG 是利用动态的图形表示与简单的统计数值，显示目前 Qno 防火墙/路由器系统的工作状态，包括 CPU 使用率、实体内存（Memory）使用率、连线数量（Session）以及每个广域网的流量（WAN Traffic)。

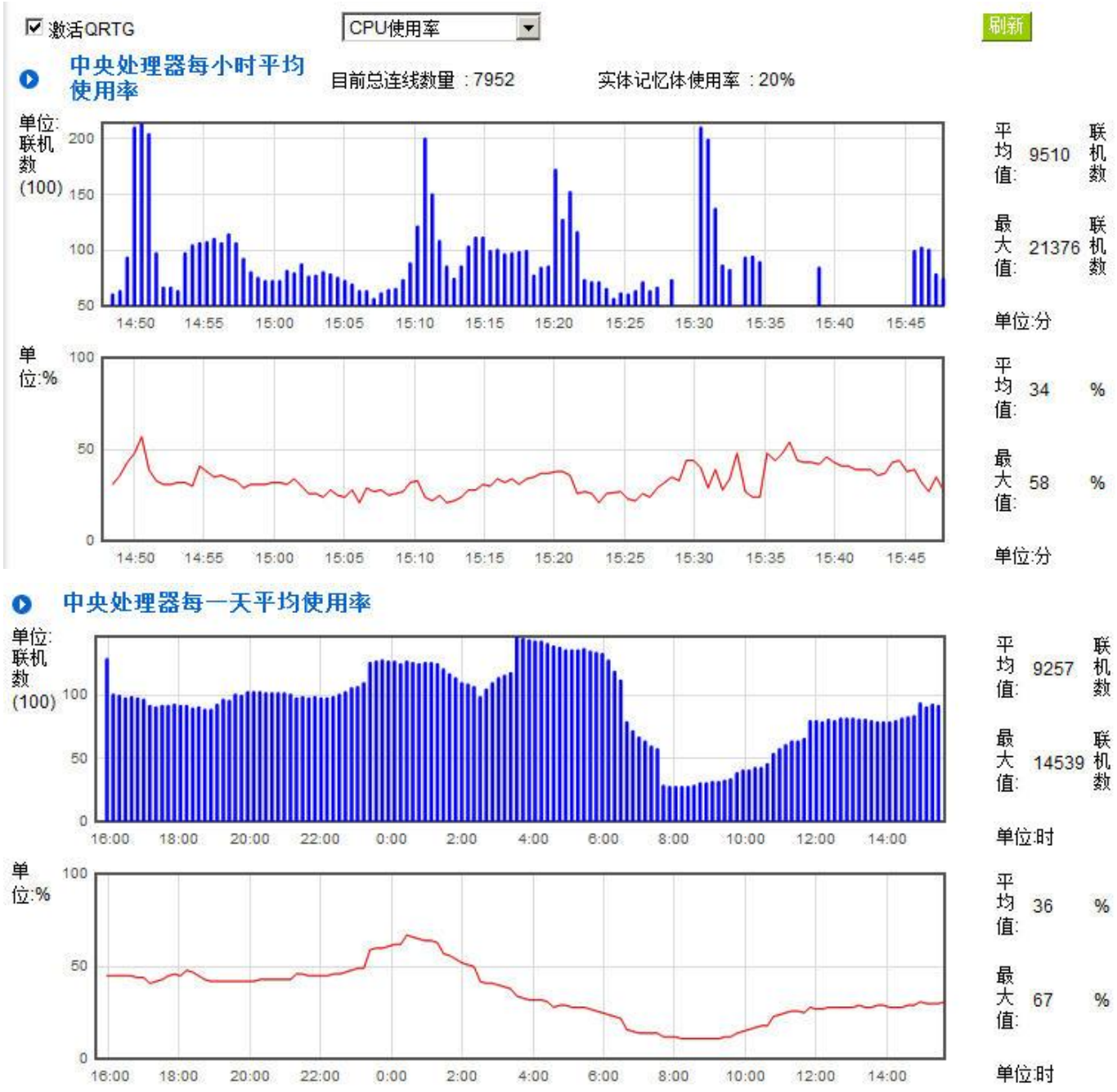
激活 QRTG：QRTG 在系统出厂默认值是不启动的，当您要激活 QRTG 功能时，系统会跳出警告讯息提醒您此功能的激活可能会影响路由器的使用效能。激活之后，您可以透过下拉式选单选择以下项目的目前的状态与统计数值、图形，按下「刷新」按钮会重新更新统计数据与图形内容至最新时间的资料。

一、CPU 使用率 / 连线数量统计（如下图)

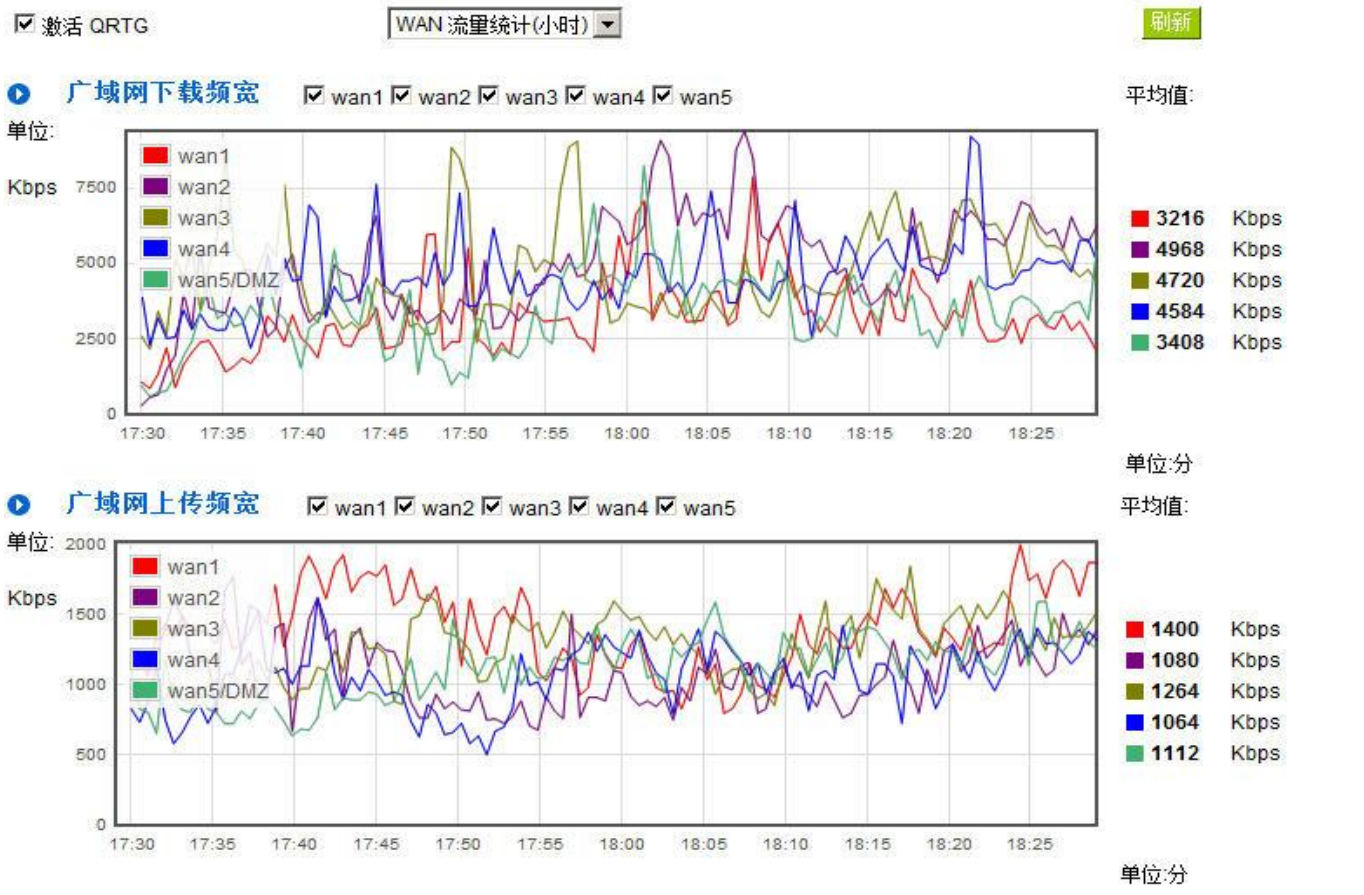
(1) CPU、连线数每小时使用率图形 / 平均值 / 最大值。

(2) CPU、连线数每一天平均使用率图形 / 平均值 / 最大值。

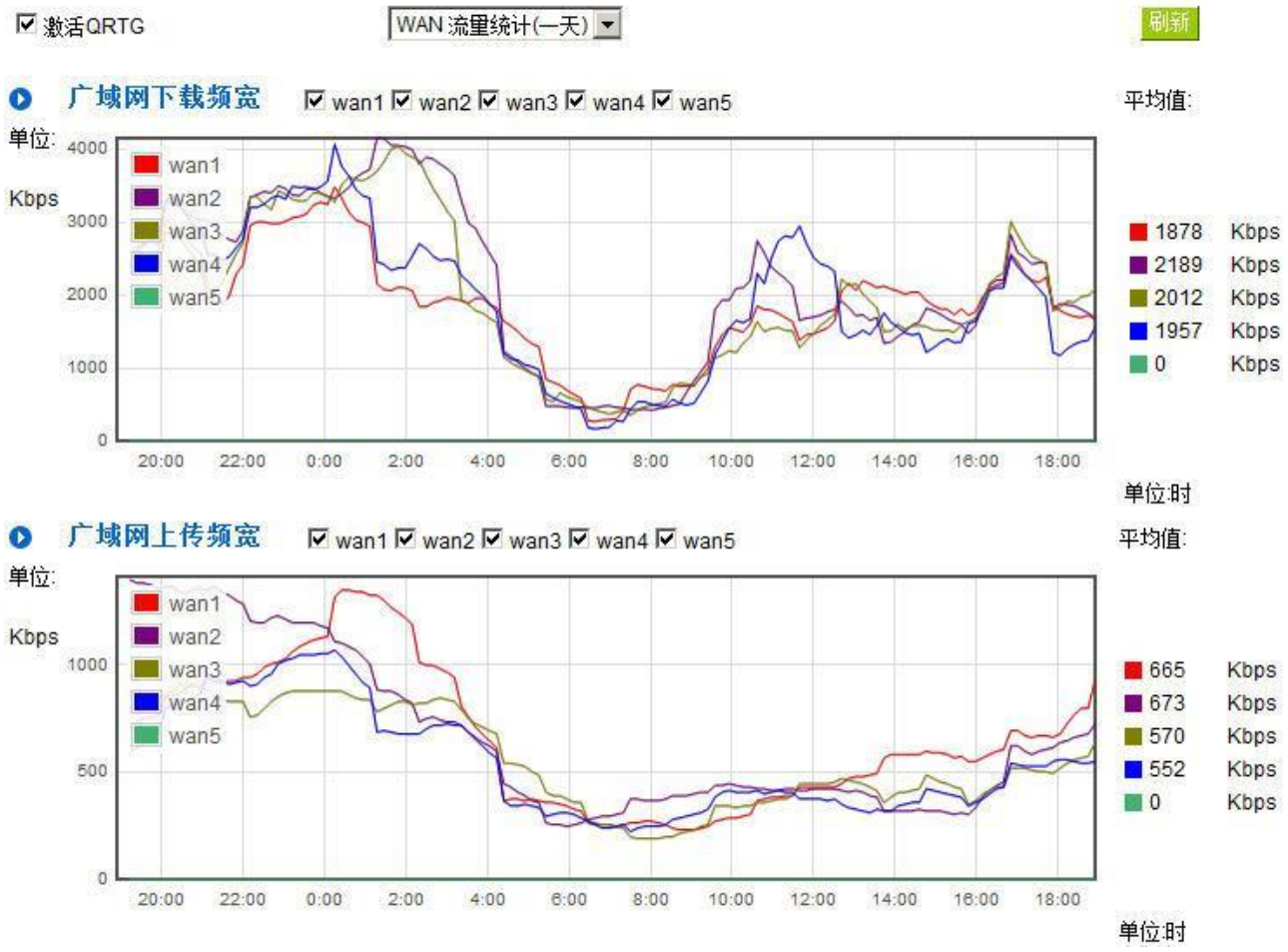
(3) CPU、连线数每一周平均使用率图形 / 平均值 / 最大值。


激活QRTG
CPU使用率
刷新
中央处理器每小时平均使用率
目前总连线数量 : 7952
实体记忆体使用率 : 20%
单位: 联机数 (100)
200
150
100
50
14:50 14:55 15:00 15:05 15:10 15:15 15:20 15:25 15:30 15:35 15:40 15:45
平均值: 9510 联机数
最大值: 21376 联机数
单位:分
单位:%
100
50
0
14:50 14:55 15:00 15:05 15:10 15:15 15:20 15:25 15:30 15:35 15:40 15:45
平均值: 34 %
最大值: 58 %
单位:分
中央处理器每一天平均使用率
单位: 联机数 (100)
100
50
0
16:00 18:00 20:00 22:00 0:00 2:00 4:00 6:00 8:00 10:00 12:00 14:00
平均值: 9257 联机数
最大值: 14539 联机数
单位:时
单位:%
100
50
0
16:00 18:00 20:00 22:00 0:00 2:00 4:00 6:00 8:00 10:00 12:00 14:00
平均值: 36 %
最大值: 67 %
单位:时

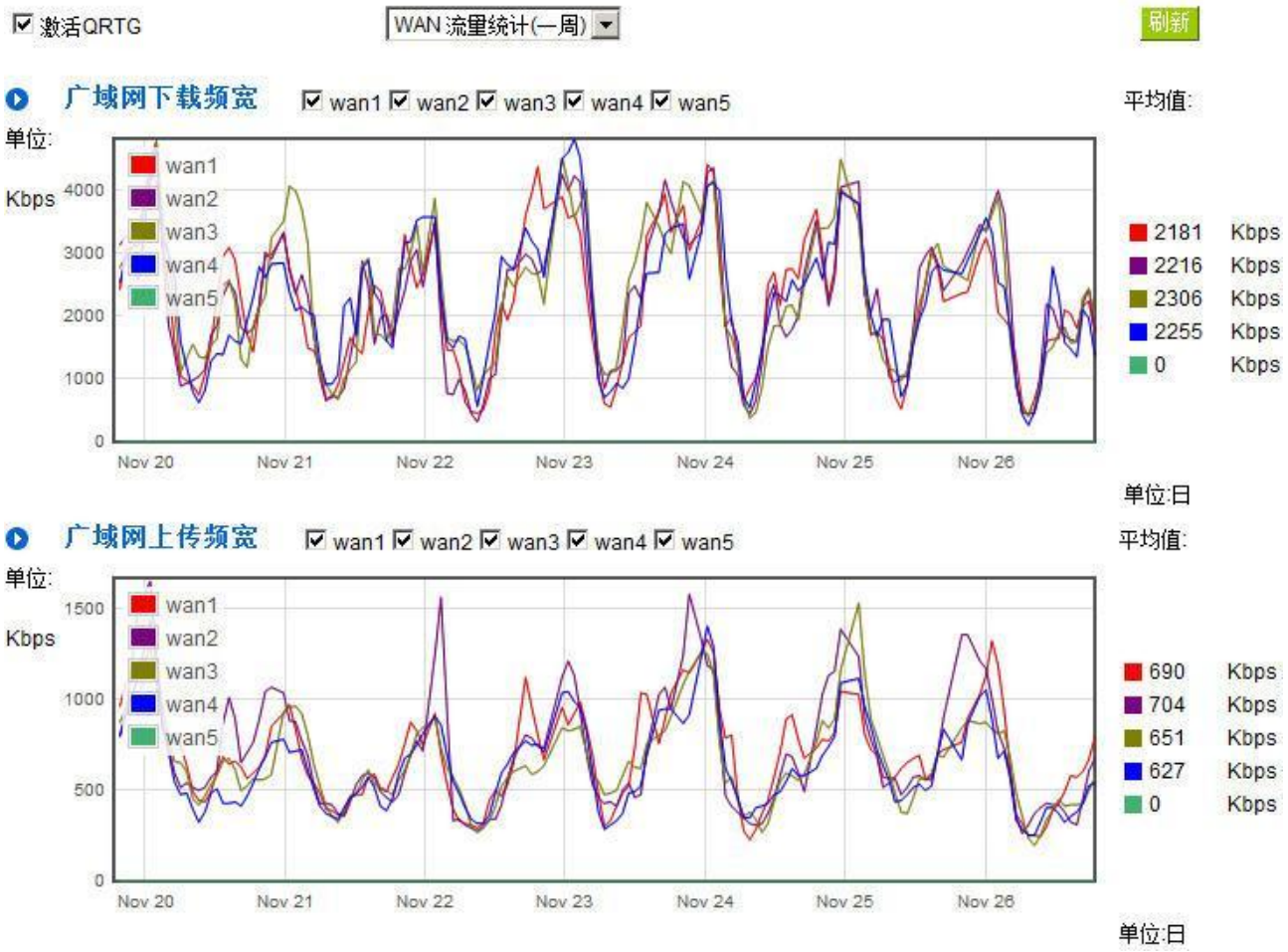
二、每个广域网「每小时」流量统计图形与平均值（上传流量与下载流量)(如下图)



三、每个广域网「每一天」流量统计图形与平均值（上传流量与下载流量)(如下图)



四、每个广域网「每一周」流量统计图形与平均值（上传流量与下载流量)(如下图)



十四、注销

路由器的网页窗口右上方有一个注销的按钮，此按钮为结束管理路由器并关闭此管理窗口。若您下次想再进入路由器管理窗口时，您必须重复登录路由器管理窗口的步骤，并输入管理者的使用名称与密码。

附录一、配置界面及使用手册章节对照

本章主要通过表格的形式把每个章节具体对照路由器 Web 管理页面的链接与界面对照显示，进一步方便用户快速的配置路由器，同时更加了解路由器的工作能力。

路由器整体界面栏目次序图如下。

一级栏目	二级栏目	对应章节
首页		五、确定设备规格、状态显示以及登录密码和时间的设定 5.1 首页显示
网络连接配置		六、进行广域网络连线配置
	网络设置	6.1 网络设定
	流量管理	6.2 多 WAN 设定
	协议绑定	6.2 多 WAN 设定
QoS 带宽管理		八、QoS 带宽管理功能
	带宽设置	8.1 带宽设置(QoS)/ 8.3 智能带宽管理
	联机数设置	8.2 联机数管控
IP/DHCP 配置		七、内部局域网络配置
	DHCP 设置	7.3 DHCP 发放 IP 服务器
	DHCP 服务状态	7.4 DHCP 状态显示

	IP 与 MAC 绑定	7.5 IP 及 MAC 地址绑定
	IP 群组管理	7.6 IP 群组管理
防火墙配置		九、防火墙配置
	基本设置	9.1 基本设置/ 9.2 阻挡特定服务
	访问规则设置	9.3 访问规则设置
	网页内容管制	9.4 网页内容管制
高级设置		十、其它进阶高级功能设置
	DMZ/虚拟服务主机	10.1 DMZ / 虚拟服务主机
	路由通讯协议	10.2 路由通讯协议
	一对一 NAT	101.3 一对一 NAT
	DDNS 动态域名解析	10.4 DDNS-动态域名解析
	广域网端口 MAC 地址	10.5 广域网接口 MAC 地址设定
系统工具		十一、工具程序功能设定/五、确定设备规格、状态显示以及登录密码和时间的设定
	密码设置	5.2 登录密码和时间的设定
	自我诊断	11.1 在线联机测试
	固件更新	11.2 系统硬件升级
	配置参数备份/恢复	11.3 系统设定参数存储
	SNMP 网路管理	11.4 网络管理设定(SNMP)
	时间设置	5.2 登录密码和时间的设定
	系统恢复	11.5 系统恢复
	备援功能	11.6 备援功能
端口管理		七、内部局域网络配置
	端口设置	7.1 网络端口管理配置
	端口状态即时显示	7.2 网络端口状态实时显示
日志		十二、日志功能设定
	系统日志	12.1 系统日志
	系统状态	12.2 系统状态实时监控
	流量统计	12.3 流量统计
	IP/端口自定统计	12.4 特定 IP 及端口状态
	QRTG	12.5 QRTG

附录二：产品中有毒有害物质或元素表

部件名称	有毒有害物质或元素					
	铅(Pb)	汞(Hg)	镉(Cd)	六价铬(Cr(VI))	多溴联苯(PBB)	多溴二苯醚(PBDE)
PCBA	X	O	O	O	O	O

O：表示该有毒有害物质在部件所有均质材料中的含量均在 SJ/T 11363-2006 标准规定的限量要求以下。

X：表示该有毒有害物质至少在该部件的某一均质材料中的含量超出 SJ/T 11363-2006 标准规定的限量要求。

- 电阻内部导通部位为导电银糊剂(含有铅玻璃料)
- 二极管本体有采用含有铅玻璃料

附录三：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 http://www.qno.cn/forum 讨论区或在 http://www.qno.cn/web/faqlist.asp 查找问题解答，或联系技术服务人员，具体可以参考附录五的详细联系方式。

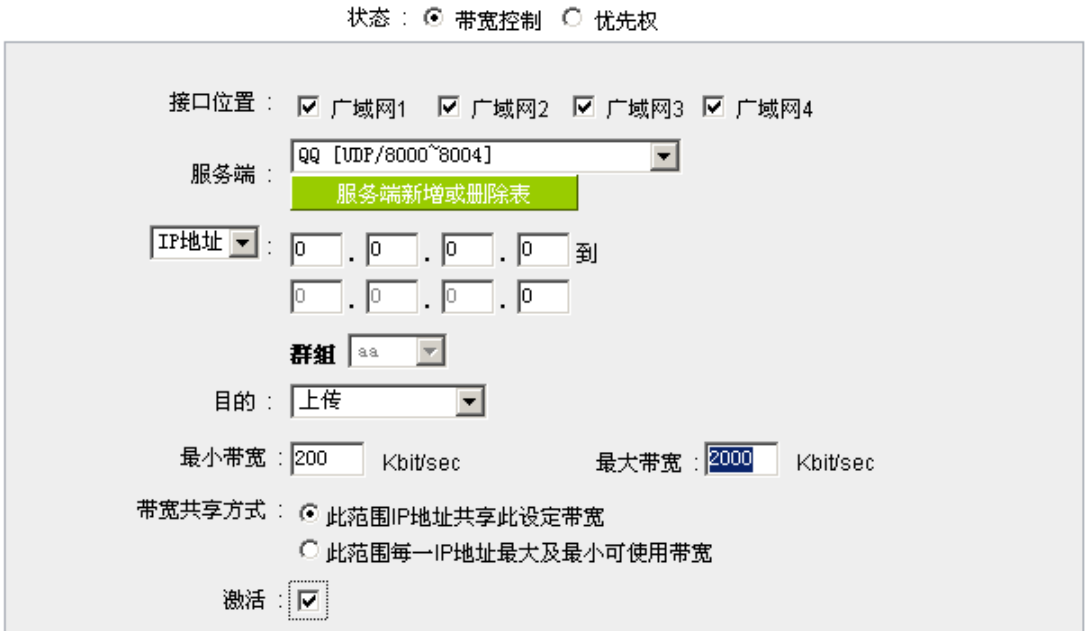
（1） QQ 容易掉线问题

a). 检查 QQ 版本是否为 2006 版，经过 QQ 官方确认使用珊瑚版或是传美版掉线严重。

b). 2 条以上的线路，必须作协议绑定，让 QQ 走固定广域网。绑定 QQ(UDP8000~8004)走固定的广域网参照下图协议绑定设置：

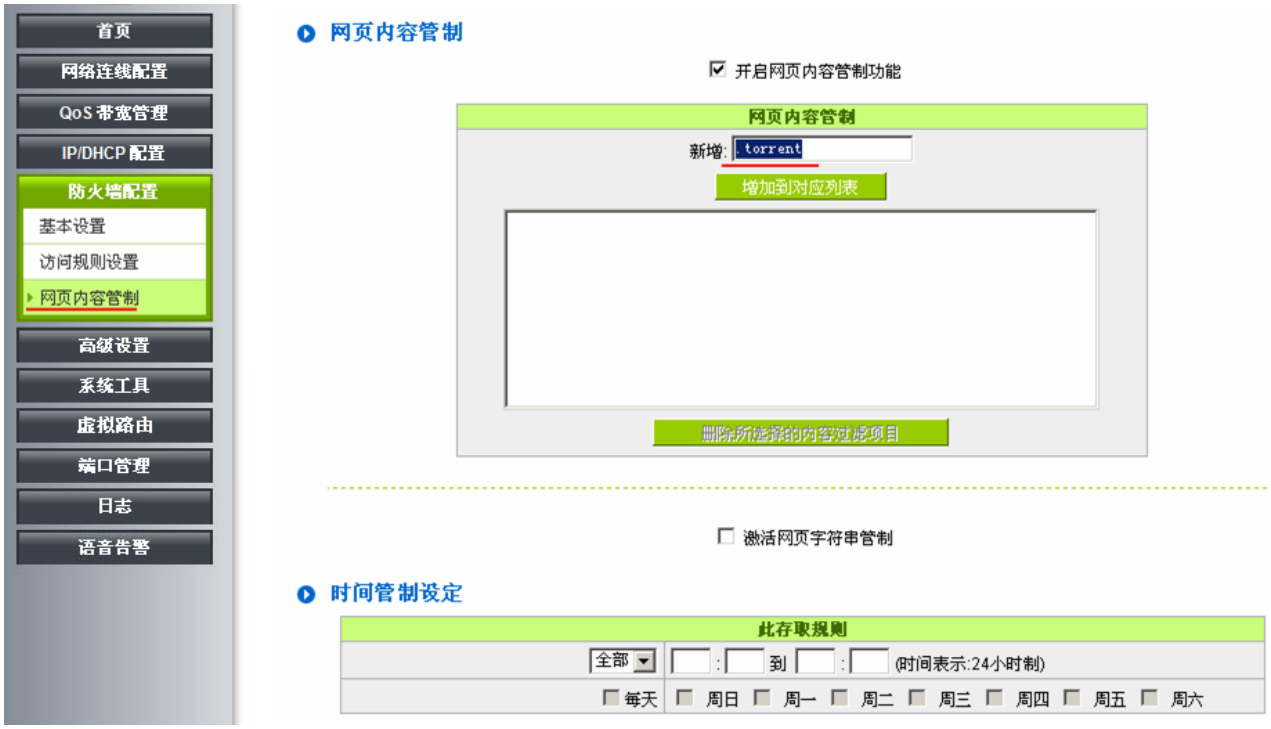
c).保证带宽给 QQ 端口，依照网吧或企业内部实际带宽评估 QoS 所需要设定的最小值与最大值，下图为 10M 光纤保证给 QQ 的方式，上下传都必须设定。

网络品质服务配置(QoS)



（2） 挡基本 BT 下载方式

若您想要将 BT 给挡下，不让用户下载，您可以直接在 "防火墙配置" > "网页内容管制设定" 选择 "开启网页内容管制功能" 后将 "激活网页字符串管制" 打入".torrent"这样就可以防止用户下载种子。

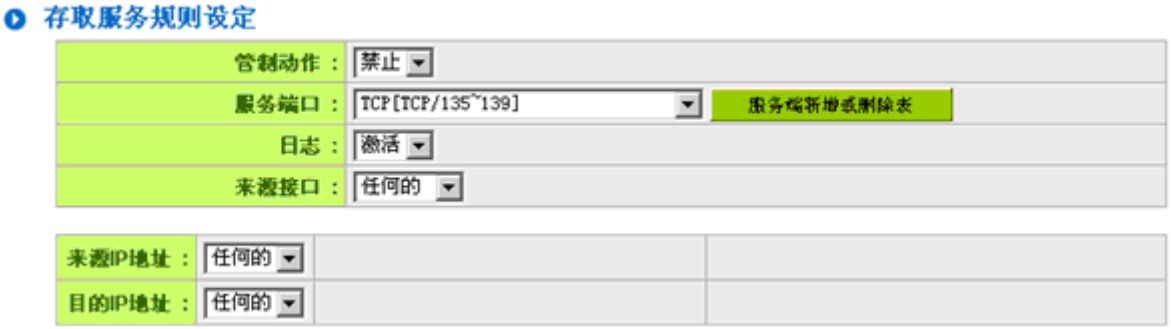


（3） 冲击波及蠕虫病毒的防制

由于近来还是发生有许多用户内网中冲击波及蠕虫病毒造成内网访问互联网很慢及联机数(Session)大量增加造成路由器大量处理，以下将指导您封锁此些病毒相应端口以达到防制目的。

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

b.用防火墙里面的“存取规则”功能将设定好的此三组端口封锁:



用同样的方法添加好 UDP[UDP135~139]以及 TCP[445~445]端口。

c.将这三组的优先级至于最高:

（4） 阻止 QQLive 视屏直播设定

QQLive 视屏直播软件是一种流媒体点播软件，最近好多客户都在头痛一个同样的问题，当内网有多个用户使用 QQLive 视屏直播软件，占用了比较大的带宽，造成路由器的负担过重，使得路由器反应迟钝或瘫痪，如果我们能够封锁 QQLive 的服务器登录过程就可以解决这样的问题，下面就这个问题来结合 Qno 产品的相关功能提出相关的解决方案，来进行路由器配置。

a). 进入路由器 Web 管理页面，再进入“防火墙配置”的“访问存取规则设定”。

b). 再点击“增加新的管制规则”，进入“访问存取规则设定”页面，在“存取服务规则设定”中的“管制动作”选项中选择“禁止”，再在“服务器端口” 选择“所有端口[TCP&UDP/1~65535]”，选择“来源接口”为“任何的”，“来源 IP 地址”选择“任何的”（有相关需求的用户可以选择“单独”或“范围” 阻止单个 IP 或者一段 IP 的 QQLive 的的登录），再在“目的 IP 地址”选择“单独”填入 QQLive 服务器的 IP 地址“58.60.11.145”（QQLive 服务器的 IP 地址不止一个，后面需要重复添加），最后在“时间管制设定”的“此存取规则”选择“全部”对上 QQLive 的登录时间进行设置（如有需要可以具体设置相关时间的设定），“确定”后进入下一步骤。

c). 重复以上的操作在只替换“目的 IP 地址”里分别填入以下 IP 地址：

cache.tv.qq.com	loginqqlivedx.qq.com	qqlive.qq.com
58.60.11.145	219.133.49.159	219.133.62.70
58.60.11.146	loginqqlivewt.qq.com	tv1-3t.qq.com
58.60.11.147	58.251.63.13	221.236.11.40

59.36.97.5	loginqqlivexy.qq.com	tv2.qq.com
59.36.97.7	202.205.3.218	218.17.209.17
59.36.97.37		
219.133.63.48		

访问规则设置

跳到 1 / 页　　20 每页显示的字段　　下一页 >>

优先权	激活	管制动作	服务端口	来源端口	来源位置	目的位置	管制时间	日		删除
1	☑	允许	TCP [445]	*	任何的	任何的	所有时间		编辑	
2	☑	允许	TCP [135]	*	任何的	任何的	所有时间		编辑	
3	☑	允许	TCP [135]	*	任何的	任何的	所有时间		编辑	
4	☑	关闭	所有端口 [1]	*	任何的	218.17.209.17 ~ 218.17.209.17	所有时间		编辑	
5	☑	关闭	所有端口 [1]	*	任何的	221.236.11.40 ~ 221.236.11.40	所有时间		编辑	
6	☑	关闭	所有端口 [1]	*	任何的	219.133.62.70 ~ 219.133.62.70	所有时间		编辑	
7	☑	关闭	所有端口 [1]	*	任何的	202.205.3.218 ~ 202.205.3.218	所有时间		编辑	
8	☑	关闭	所有端口 [1]	*	任何的	38.251.63.13 ~ 38.251.63.13	所有时间		编辑	
9	☑	关闭	所有端口 [1]	*	任何的	219.133.49.159 ~ 219.133.49.159	所有时间		编辑	
10	☑	关闭	所有端口 [1]	*	任何的	219.133.63.48 ~ 219.133.63.48	所有时间		编辑	
11	☑	关闭	所有端口 [1]	*	任何的	59.36.97.37 ~ 59.36.97.37	所有时间		编辑	
12	☑	关闭	所有端口 [1]	*	任何的	59.36.97.7 ~ 59.36.97.7	所有时间		编辑	
13	☑	关闭	所有端口 [1]	*	任何的	59.36.97.5 ~ 59.36.97.5	所有时间		编辑	
14	☑	关闭	所有端口 [1]	*	任何的	58.60.11.145 ~ 58.60.11.147	所有时间		编辑	
	☑	允许	所有端口 [1]	局域网	任何的	任何的	所有时间			

重复添加后可以看到相关 QQLive 的服务器的连接被封锁，点击确认完成对阻止 QQLive 视屏直播设定，此方案是在 QQLive3.1 的版本下测试并完成阻挡的。

（5） ARP 病毒攻击防制

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恢复。这是因为 MAC 地址冲突引起的，当带毒机器的 MAC 映射到主机或者路由器之类的 NAT 设备，那么全网断线，如果只映射到网内其它机器，则只有这部分机器出问题。多发于传奇游戏特别是私服务外挂等方面。此类情况就是网络受到了 ARP 病毒攻击的明显表现，其目的在于，该病毒破解游戏加密解密算法，通过截取局域网中的数据包，然后分析游戏通讯协议的方法截获用户的信息。运行这个病毒，就可以获得整个局域网中游戏玩家的详细信息，盗取用户帐号信息。下面我们谈谈如何防制这种攻击。

首先，我们了解下什么是 ARP，ARP “Address Resolution Protocol”（地址解析协议），局域网中，网络中实际传输的是“帧”，帧里面是有目标主机 MAC 地址的。所谓“地址解析”就是主机在发送帧前将目标 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设备的 IP 地址，查询目标设备的 MAC 地址，以保证通信的顺利进行。

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 缓存表，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）发送数据为例。当发送数据时，主机 A 会在自己的 ARP 缓存表中寻找是否有目标 IP 地址。如果找到了，也就知道了目标 MAC 地址，直接把目标 MAC 地址写入帧里面发送就可以了；如果在 ARP 缓存表中没有找到相对应的 IP 地址，主机 A 就会在网络上发送一个广播，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 接收到这个帧时，才向主机 A 做出这样的回应：“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 发送信息了。同时它还更新了自己的 ARP 缓存表。

再者，我们先简单介绍一下什么是 ARP 病毒攻击，这种病毒是对内网的 PC 进行攻击，使内网 PC 机的 ARP 表混乱，在局域网中，通过 ARP 协议来完成 IP 地址转换为第二层物理地址（即 MAC 地址）的。ARP 协议对网络安全具有重要的意义。通过伪造 IP 地址和 MAC 地址实现 ARP 欺骗，能够在网络中产生大量的 ARP 通信量使网络阻塞。进行 ARP 复位向和嗅探攻击。用伪造源 MAC 地址发送 ARP 响应包，对 ARP 高速缓存机制的攻击。这些情况主要出现在网吧用户，造成网吧部分机器或全部机器暂时掉线或者不可以上网，在重新启动后可以解决，但保持不了多久有会出现这样的问题，网吧管理员对每台机器使用 arp –a 命令来检查 ARP 表的时候发现路由器的 IP 和 MAC 被修改，这就是 ARP 病毒攻击的典型症状。

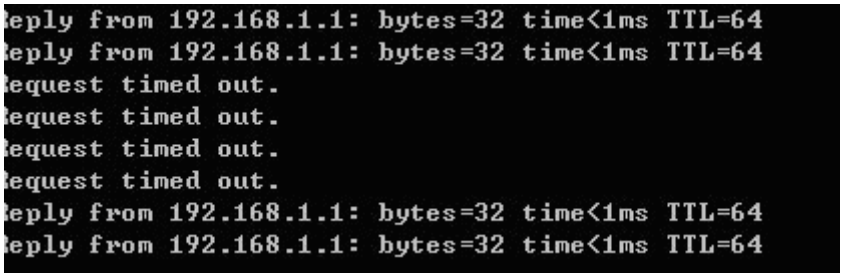
这种病毒的程序如 PWSteal.lemir 或其变种，属于木马程序/蠕虫类病毒，Windows 95/98/Me/NT/2000/XP/2003 将受到影响，病毒攻击的方式对影响网络连接畅通来看有两种，对路由器的 ARP 表的欺骗和对内网 PC 网关的欺骗，前者是先截获网关数据，再将一系列的错误的内网 MAC 信息不停的发送给路由器，造成路由器发出的也是错误的 MAC 地址，造成正常 PC 无法收到信息。后者 ARP 攻击是伪造网关。它先建立一个假网关，让被它欺骗的 PC 向假网关发数据，而不是通过正常的路由器途径上网。在 PC 看来，就是上不了网了，“网络掉线了”。

就这两种情况而言，如果对 ARP 病毒攻击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置才保证问题的最终解决。所以我们选择路由器的话最好看看路由器是否带有防制 ARP 病毒攻击的功能，Qno 产品正好提供了这样的功能，相比其它产品操作简单易学。

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 缓存表被修改不停的通知路由器一系列错误的内网 IP 或者干脆伪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掉线问题，这样的情况就是典型的 ARP 攻击，对遭受 ARP 攻击的判断，其方法很容易，你找到出现问题的计算机点开始运行进入系统的 DOS 操作。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 攻击。为了进一步确认，我们可以通过查找 ARP 表来判断。输入 ARP -a 命令，显示如下图。

```
Interface: 192.168.1.72 --- 0x2
  Internet Address      Physical Address      Type
  192.168.1.1           00-0f-3d-83-74-28     dynamic
  192.168.1.43          00-13-d3-ef-b2-0c     dynamic
  192.168.1.252         00-0f-3d-83-74-28     dynamic

C:\WINDOWS\System32>arp -a
```

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 欺骗攻击以及如何判断此类攻击，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击对网络造成的危害。Qno 的一般处理办法分三个步骤来完成。

a)、激活防止 ARP 病毒攻击：

输入路由器 IP 地址登陆路由器的 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 病毒攻击”在这一行的“激活”前面做点选，再在页面最下点击“确认”，如图。

基本设定

防火墙功能：	◉ 激活 ○ 关闭
SPI封包主动侦测检验功能：	◉ 激活 ○ 关闭
DoS侦测功能：	◉ 激活 ○ 关闭 高级设定
关闭对外的封包回应：	◉ 激活 ○ 关闭
远程配置管理功能：	○ 激活 ◉ 关闭 Port: 80
允许Multicast封包穿透格式：	○ 激活 ◉ 关闭
防止ARP病毒攻击：	◉ 激活 ○ 关闭 防ARP攻击每秒发送 20 笔.

b)、对每台 PC 上绑定网关的 IP 和其 MAC 地址

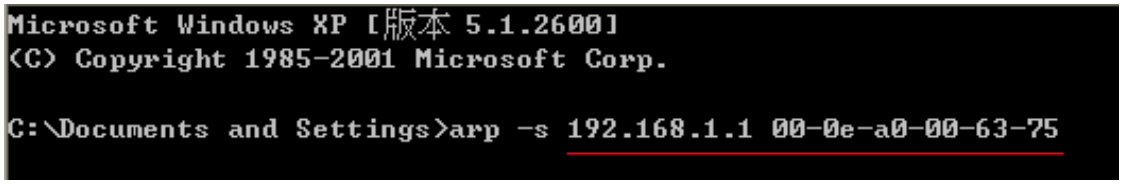
进行这样的操作主要防止 ARP 欺骗网关 IP 和其 MAC 地址首先在路由器端查找网关 IP 与 MAC 地址，如图。

局域网(LAN)接口配置

MAC 地址: 00 - 17 - 16 - 00 - fc - 8c (预设值:00-17-16-00-fc-8c)	
IP地址 : 192 . 168 . 1 . 1	子网掩码 : 255 . 255 . 255 . 0

然后在每台 PC 机上开始/运行 cmd 进入 dos 操作，输入 arp –s 192.168.1.1 0-0e-a0-00-63-75，Enter 后完成

pc01 的绑定。如图 7



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 绑定。但是此动作，如果重起了计算机，作用就会消失，所以可以把此命令做成一个批处理文件，放在操作系统的启动里面，批处理文件可以这样写：

@echo off

arp -d

arp -s 路由器 LAN IP　路由器 LAN MAC

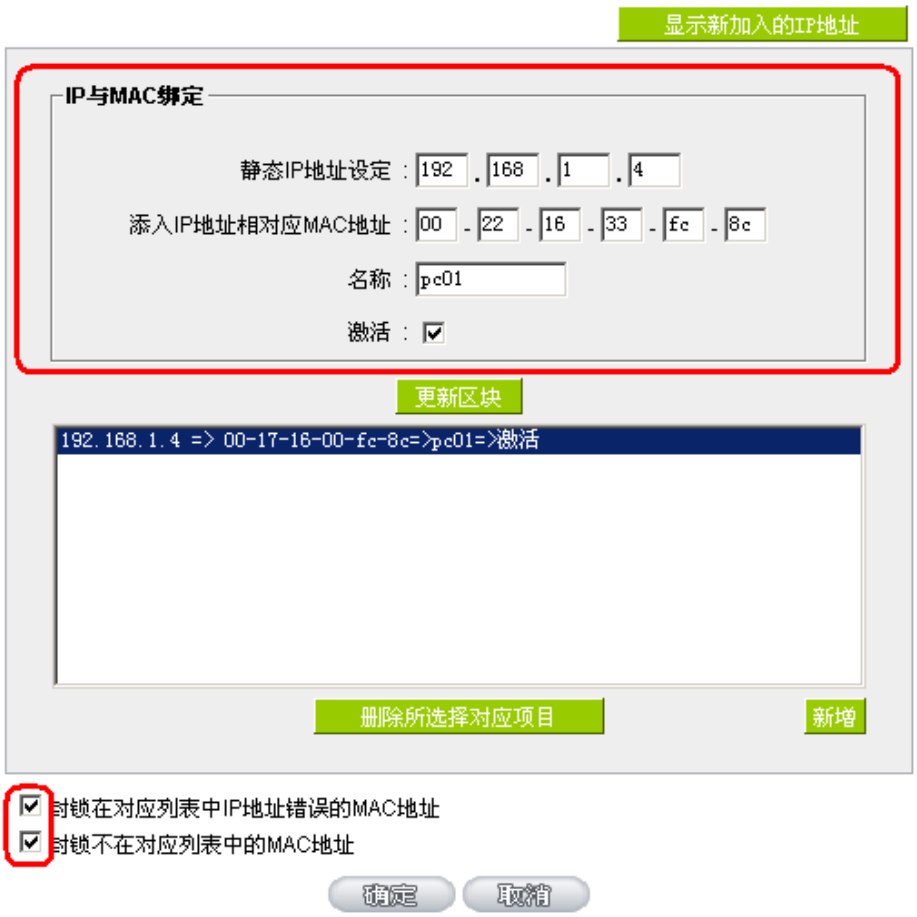
对于已经中了 arp 攻击的内网，要找到攻击源。方法：在 PC 上不了网或者 ping 丢包的时候，在 DOS 下打 arp –a 命令，看显示的网关的 MAC 地址是否和路由器真实的 MAC 相同。如果不是，则查找这个 MAC 地址所对应的 PC，这台 PC 就是攻击源。

其它的路由器用户的解决方案也是要在路由器和 PC 机端进行双向绑定 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 地址的绑定比较复杂，需要查找每台 PC 机的 IP 地址与 MAC 加大了工作量，操作过程中还容易出错。

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 绑定”你可以在此添加 IP 与 MAC 绑定，输入相关参数，在“激活”上点“ √ ”选再“添加到对应列表”，重复操作添加内网里的其它 IP 与 MAC 的绑定，再点页面最下的“确定”。

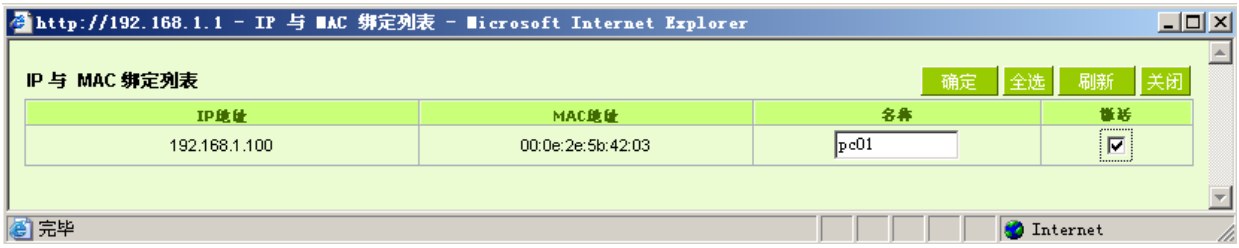
IP与MAC绑定



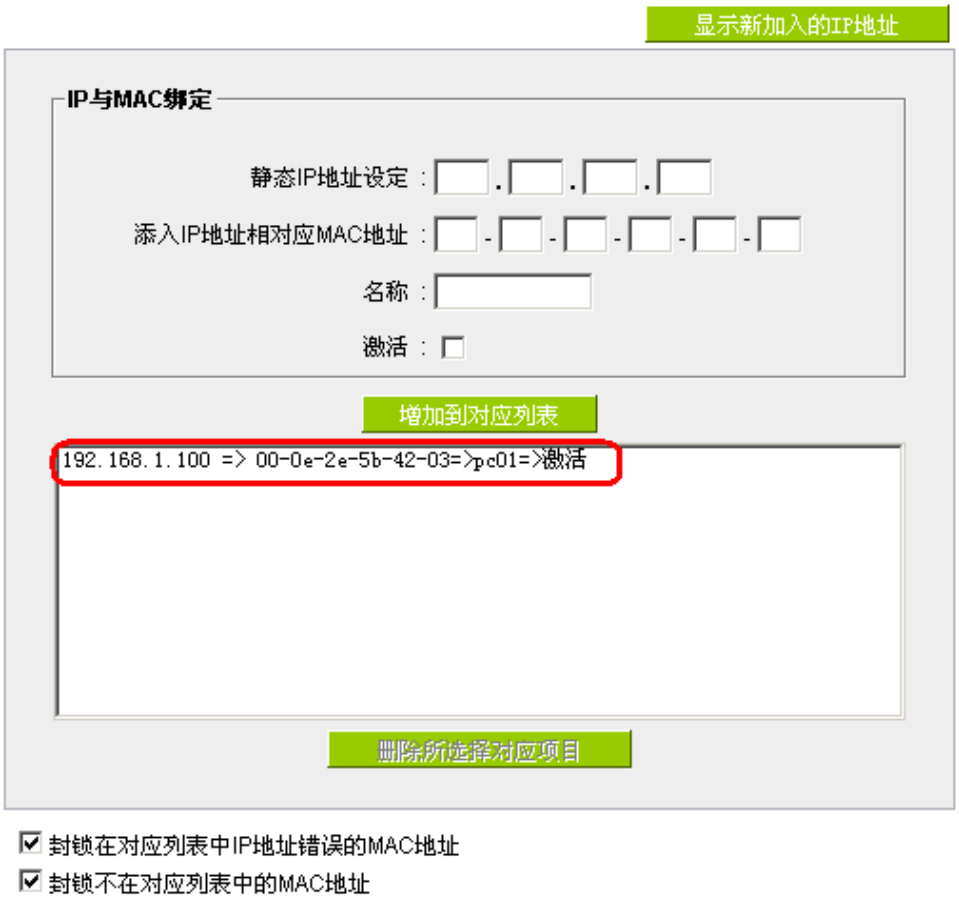
当添加了对应列表之后，其对应的信息就会在下面的白色框里显示出来。不过建议不采用此方法，这样操作需要查询网络内所有主机 IP/MAC 地址工作量繁重，还有一种方法来绑定 IP 与 MAC，操作会相对容易，可以减少大量的工作量，节约大量时间，下面就会讲到。

进入“DHCP 功能”的“DHCP 配置”找到 IP 与 MAC 绑定右边有一个“显示新加入的 IP 地址”点击进入。

点击之后会弹出 IP 与 MAC 绑定列表对话框，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“激活”上“√”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 绑定列表框里，如图 5 再点击“确认/Apply”绑定完成。



但是我们单靠这样的操作基本可以解决问题，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 的攻击。

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

2、网吧管理员检查局域网病毒，安装杀毒软件（金山毒霸/瑞星，必须要更新病毒代码），对机器进行病毒扫描。

3、给系统安装补丁程序。通过 Windows Update 安装好系统补丁程序(关键更新、安全更新和 Service Pack)

4、给系统管理员帐户设置足够复杂的强密码，最好能是 12 位以上，字母+数字+符号的组合；也可以禁用/删除一些不使用的帐户

5、经常更新杀毒软件（病毒库），设置允许的可设置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击和病毒的入侵。部分盗版 Windows 用户不能正常安装补丁，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，也包括 C$、D$等管理共享。完全单机的用户也可直接关闭 Server 服务

7、不要随便点击打开 QQ、MSN 等聊天工具上发来的链接信息，不要随便打开或运行陌生、可疑文件和程序，如邮件中的陌生附件，外挂程序等。

4. 总结

ARP 攻击防制是一个任重而道远的过程，以上方法基本可以解决 ARP 病毒攻击对网络造成相关问题，而且客户采取类似的方法也收到了很大的效果，但还是提醒网落管理人员必须高度重视这个问题，而且不能大意马虎，我们可以采取以上建议随时警惕 ARP 攻击，以减少受到的危害，提高工作效率，降低经济损失。

附录四：Qno 技术支持资讯

更多有关侠诺产品技术资讯，除了可以登录侠诺宽带讨论区、叁照 FTP 服务器的相关实例；或是进一步联系侠诺各经销商技术部门、或侠诺大陆技术中心取得相关协助。

网上讨论区及 FTP 服务器：

讨论区：http://www.Qno.cn/forum

各大经销商服务联系方式：

用户可以登录网站先上服务页面查询各大经销联系方法：

http://www.Qno.cn/web/where_buy.asp

技术中心：

电邮：QnoFAE@qno.com.tw