RX3041H

高速路由器

用户手册

1.0 版

华硕的联络信息

华捷联合信息（上海）有限公司（莘庄）

电话：021-54421515/1616/4949/2424

传真：021-54420088/0099/0066

地址：上海市莘庄工业区春东路508号

邮编：201108

华捷联合科技（广州）有限公司

电话：020-85572366/70/71

传真：020-85572352/2355

地址：广州中山大道西高新技工业园建工路12号1-3楼

邮编：510665

华捷联合信息(上海)有限公司成都办事处

电话：028-82916655/56/58

传真：028-82916659

地址：成都市一环路南三段22号世纪电脑城三楼B座

邮编：610041

华捷联合信息（上海）有限公司沈阳办事处

电话：024-23988728

传真：024-23988563

地址：沈阳市和平区南三好街55号沈阳信息产业大厦1808

邮编：110004

华捷联合信息（上海）有限公司北京海淀分公司

电话：010-82667575

传真：010-82689352

地址：北京市海淀路52号太平洋科技大厦13层

邮编：100080

华硕技术支持：

免费咨询电话：800-8206655

Email:tsd@asus.com.cn

NetQ论坛：Netq.asus.com.cn

华硕工程师提供在线技术支持

目 录

手册中图的索引

手册中表格的索引

1 产品介绍

首先，恭喜您成为华硕 RX3041H 网际网络安全路由器的用戶！您局域网络（LAN）内的计算机现在将可如同那些使用 ADSL 或 cable modem 的计算机一样，拥有高速的宽频联线来接入网际网络。

此外，本用户手册也将指导您如何安装这台高性能的网际网络安全路由器，并针对您自己的需要设定各项功能，让本产品可以发挥最大的效能。

1.1 产品功能

- 10/100Base-T 以太网络由器为您局域网络（LAN）内的所有计算机提供网际网络联机。
- 防火墙、NAT（网络地址转换）功能为您的局域网络（LAN）提供安全的网络联机。
- 透过 DHCP 服务器提供自动的网络地址分配。
- 服务包括 IP 路由、DNS 和 DDNS 设定、 RIP 及 IP 性能监控。
- 本产品的设定全部透过浏览器完成，您必须具备网页浏览器互聯網 Explorer 软件，版本在 5.5 以上，或者 Netscape 浏览器，版本在 7.0.2 以上。

1.2 系统需求

您在使用本网际网络安全路由器接入网际网络时，请注意以下事项：

- 具备可使用的 ADSL 或是 cable modem 宽频服务，并具备至少一个公共的网际网络地址指定给您的广域网（WAN）使用。
- 一台以上具备 10Base-T/100Base-T 以太网络适配卡（NIC）的计算机。
- 如果您需要将本产品连接在超过四台计算机的以太网络上，您必须另外选购一台以太网络集线器/交换器。
- 本产品的设定全部透过浏览器完成，您必须具备网页浏览器互聯網 Explorer 软件，版本在 5.5 以上，或者 Netscape 浏览器，版本在 7.0.2 以上。

1.3 关于这本用户手册

1.3.1 提示符号的说明

- 本手册将在缩写词第一次出现时解释其意义，并将其意义解释收入术语表中。
- 为简洁起见，“网际网络安全路由器”有时简称为“路由器”。
- 在提到某个地方的一组以太网联机的计算机时，术语***局域网络（LAN）***和***网络（network）***将交替使用。

1.3.2 印刷样式的说明

- *斜体*用来标出术语表解释的术语。
- **黑体字** 表示在菜单或其它计算机显示页面中选中的选项。

1.3.3 特别信息

这本手册使用下列图标来提醒您注意特殊的说明和解释。

注意

向您提供有助于完成某项工作的诀窍或其它额外的信息。

名词解释

向您阐释多数用户不太熟悉的术语或缩写词，这些术语解释也将在术语表中集中出现。

小心

提醒您在进行某项工作时要注意的重要信息，包括要请您注意个人安全和勿伤害系统完整的信息。

2 认识 RX3041H 高速路由器

2.1 零件目录表

除本手册之外，您的包装盒内还应包含以下配件：

- RX3041H 高速路由器
- 电源供应器
- 以太网络线（straight-through）
- （可选）主控台（console）埠线缆（RJ-45）

2.2 前面板

请参考下图。前面板包括数个 LED 指示灯，显示各项操作状态。

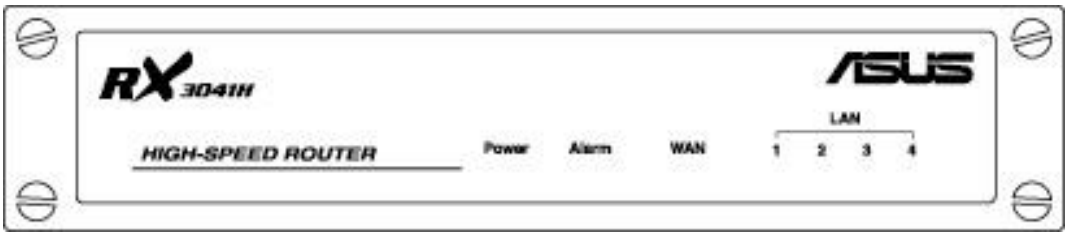


图 2.1. 前面板 LED 指示灯

表 2.1. 前面板标签和 LED 指示灯

指示灯	颜 色	功 能
POWER	绿 灯	灯亮：电源开启 灯灭：电源关闭
ALARM	绿 灯	（仅在工厂测试使用）
WAN	绿 灯	灯亮：WAN 有联机 闪烁：资料正透过 WAN 传输 灯灭：WAN 无联机
LAN1 – LAN4	绿 灯	灯亮：LAN 有联机 闪烁：资料正透过 LAN 传输 灯灭：LAN 无联机

2.3 后面板

请参考下图。后面板包括各种连接埠。

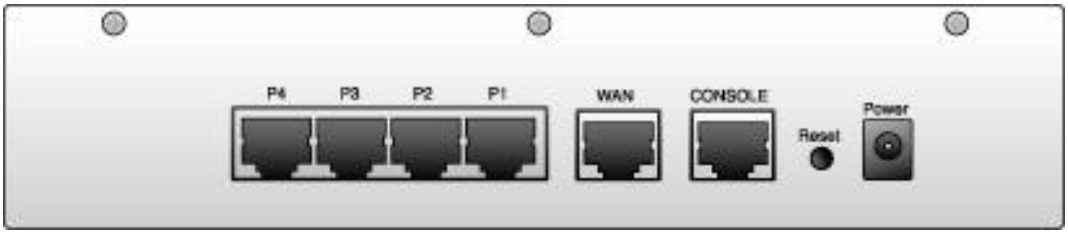


图 2.2. 后面板连接埠

表 2.2. 后面板标签和 LED 指示灯

标 签	功 能
⏻	电源开关
POWER	电源插座，连接电源供应器
Reset	重置键
CONSOLE	RJ-45 埠联机主控台
WAN	RJ-45 埠连接您的 WAN 装置，譬如 ADSL 或 cable modem
P1 – P4	RJ-45 埠连接您 PC 的以太网接口，或是连接至局域网络（LAN）集线器/交换器等接口，请使用本产品所附的网络线。

2.4 主要规格

2.4.1 防火墙规格

应用于路由器的防火墙提供下列规格来保护网络不受攻击，以及确保您的网络不被用作攻击的跳板。

- 地址分享及管理（Address Sharing and Management）
- 封包过滤（Packet Filtering）
- 状态封包检测（SPI）
- 防止拒绝服务攻击（Defense against Denial of Service Attacks）
- 应用程序内容过滤（Application Content Filtering）
- 记录与警报（Log and Alert）
- 远程访问（Remote Access）
- URL 过滤关键词（Keyword based URL Filtering）

2.4.1.1 地址分享及管理（Address Sharing and Management）

网际网络安全路由器防火墙提供 NAT（网络地址转换）来分享单一的高速网际网络联机，以及为您节省局域网络（LAN）部分联机至网际网络安全路由器时的多重联机增加的额外成本。此特性隐藏了网络地址，并阻止它们公开。它为主机联机到 LAN 的未注册的 IP 地址对应有效地址以接入网际网络。网际网络安全路由器防火墙更提供反向 NAT 能力，让 SOHO 用户也能享有多种服务，如 e-mail、网页浏览等。NAT 规则决定着 NAT 路由器的转换机制。网际网络安全路由器支持下列 NAT 形式：

- 静态 NAT – 对应从内部主机地址到全球有效网际网络地址图（一对一）。所有的封包用映像中包含的信息直接转换。
- 动态 NAT – 动态对应从内部主机地址到全球有效网际网络地址图。映像中一般包含多个内部 IP 地址池和全球有效网际网络 IP 地址池，数量上内部 IP 地址往往多于全球有效网际网络 IP 地址。在先到先服务的基础上，每个内部 IP 地址与一个外部 IP 地址相连。
- 网络地址与埠转换（NAPT ，Network Address and Port Translation）– 对应从多个内部主机地址到一个全球有效网际网络地址图。映像中一般包含多个用来转换的网络端口。每个封包用全球有效网际网络地址进行转换。
- 反向静态 NAT – 本形式为入站地址映像，它对应了从全球有效网际网络地址到内部主机地址图（一对一）。到达外部地址的所有封包均传递至内部地址。本形式将在主机由内部机器提供服务时发挥作用。
- 反向 NAPT – 亦被称为入站地址映像、埠地址映像及虚拟服务器。任何抵达路由器的封包均能传递至基于协议、端口号或规则中指定的 IP 地址的内部主机。本形式将在主机由不同的内部机器提供多重服务时发挥作用。


注意

欲知所有支持的 NAT ALG 服务的详尽列表，请参考附录 A "ALG 设定"。

2.4.1.2 访问控制表（ACL，Access Control List）

ACL 规则是网络安全的一个基本组成部分。防火墙监控着 ACL 规则允许范围内的单个封包，解释着入站和出站通信的重要信息，以及或是防止封包传递，或是允许封包传递某些基于来源地址、目标地址、来源端口、目标端口、协议和其它规范等基础之上的内容，例如过滤申请、时间变更等。

ACL 是保持子网之间独立性的合适的措施。它可以被用作阻止某些类型的入站封包抵达受保护网络的的第一道防线。

网际网络安全路由器防火墙的 ACL 方法支持：

- 基于目标和来源 IP 地址、端口号及协议的过滤
- 使用百搭牌来组成过滤规则
- 过滤规则优先次序
- 基于时间的过滤器
- 应用特殊的过滤器
- 远程访问用户群组过滤器

2.4.1.2 封包状态检查（Stateful Packet Inspection）

网际网络安全路由器防火墙利用"封包状态检查"工具来提取封包安全判断需要的与状态有关的信息和维持评估后续联机尝试所需要的信息。它允许动态联机，这样除了需要的埠之外，其余埠就无须打开。这提供高度安全的解决方式和可量测性及可扩展性。

2.4.1.3 防止 DoS 攻击（Defense against DoS Attacks）

网际网络安全路由器防火墙具有防止攻击的引擎，可保护内部网络免于网际网络可知类型的攻击。它提动了防止"拒绝服务"（Denial of Service，DoS）攻击的保护，例如 SYN flooding、IP smurfing、LAND、Ping of Death 以及所有合成型的攻击。它能够让 ICMP 停止改变方向，以及停止 IP 来源路由封包。例如，网际网络安全路由器防火墙提供防止 WinNuke——网际网络中一个广泛应用的远程攻击未受保护的 Windows 的程序——的保护。网际网络安全路由器防火墙还能够提供防止多种多样的普通网际网络攻击的保护，例如 IP Spoofing、 Ping of Death、Land Attack、Reassembly 以及 SYN flooding。

网际网络安全路由器防火墙提供的攻击保护详见下面的表 2.3.

表2.3. DoS 攻击

攻击类型	攻击名称
Re-assembly攻击	Bonk, Boink, Teardrop (New Tear), Overdrop, Opentear, Syndrop, Jolt
ICMP 攻击	Ping of Death, Smurf, Twinge
Flooders	ICMP Flooder, UDP Flooder, SYN Flooder
Port Scans	TCP XMAS Scan, TCP Null Scan TCP SYN Scan, TCP Stealth Scan
TCP 攻击	TCP sequence number prediction, TCP out-of sequence attacks
PF规则提供的保护	Echo-Chargen, Ascend Kill
其它种类的攻击	IP Spoofing, LAND, Targa, Tentacle MIME Flood, Winnuke, FTP Bounce, IP unaligned time stamp attack

2.4.1.4 应用程序命令过滤（Application Command Filtering）

网际网络安全路由器防火墙允许网络管理员阻止、监控和报告网络用户访问非商业和被禁止的网页的内容。这种高性能访问内容管理导致了激增的生产力、低带宽使用和渐少的法律责任。

网际网络安全路由器防火墙有能力处理在某些应用协议下的现行内容过滤，例如 HTTP、FTP、SMTP 和 RPC。

- HTTP – 您能定义 HTTP 扩展名基础上的模块化过滤进度表
  - ActiveX
  - Java Archive
  - Java Applets
  - Microsoft Archives
  - 档案扩展名基础上的 URLs
- FTP – 允许您详细说明和加强站点或用户群组的档案传输协议
- SMTP – 允许您过滤某些泄露了接收者过多信息的操作，例如 VRFY、EXPN 等
- RPC – 允许您过滤基于 RPC 程序序号的程序

2.4.1.5 应用程序标准网关（ALG，Application Level Gateway）

应用程序例如 FTP 、游戏等，打开了基于各自应用参数的动态联机。为透过网际网络安全路由器防火墙，封包属于应用程序，因而就要求一个相应的允许规则。当缺少这个规则时，封包将被网际网络安全路由器防火墙阻止。因为为多种应用程序创建新的动态协议并不可行（在缺乏折衷安全性的同时），应用程序标准网关（ALG，Application Level Gateway）形式的智能地用来为应用程序解析封包和打开动态联系。网际网络安全路由器防火墙为流行的应用程序如 FTP、H.323、RTSP、Microsoft Games、SIP 等，提供 ALG 的一个序号 。

2.4.1.6 URL 过滤

我们可以定义不该在 URL（Uniform Resource Locator，例如 www.yahoo.com）中出现的关键词。任何包含一个或多个此类关键词的 URL 都将被阻止。这是一个规则独立的特性，例如，它并未与 ACL 规则想关联。这个特性能被独立地开启或关闭，但是只能在防火墙开启的情况下工作。

2.4.1.7 记录与警报（Log and Alert）

可能影响安全性的网络事件将被记录在网际网络安全路由器的日志档案里。事件细节以（WELF WebTrends Enhanced Log Format）格式记录下来以便统计工具能被用来制作例行报告。网际网络安全路由器防火墙还能促使私人网络内的 Syslog 服务器产生 Syslog 信息。

网际网络安全路由器防火墙支持：

- 用 e-mail 向管理员发送警报
- 维持最小数量的日志细节，例如封包抵达时间、防火墙运作描述及运作原因
- 支持 UNIX Syslog 格式
- 按网络管理员的日程安排发送日志报告 e-mail，或者在日志档案已满时按默认值设定发送
- 所有的信息都按照 WELF 格式发送
- ICMP 日志记录展示代码和类型

2.4.1.8 远程访问（Remote Access）

网际网络安全路由器防火墙允许网络管理员将用户社区按访问规则分割为一个个访问群组。用户可以联机上主机使用登入接口。当用户成功透过识别之后，网际网络安全路由器防火墙动态地激活用户群访问规则设定。

接下来，这些规则将得到加强，直到用户离开，或是直到非活动性的休息过程已经停止。

3 快速安装指南

本安装指南将告诉您如何连接本产品至您的计算机及局域网络（LAN），并联机至网际网络。

- 第一部分提供您设定硬件的说明。
- 第二部分告诉您如何在您的个人计算机上设定网际网络参数。
- 第三部分引导您正确设定网际网络安全路由器的基本设定，将局域网络接入网际网络。

在您设定好各项设备之后，您就可以参照第 20 页的说明来检查本产品是否正常运作。

本快速安装指南假定您已经透过您的网络服务供货商（ISP）安装了 ADSL 或是 cable modem。这些说明提供的基本设定方法都必须与您家里或小型办公室的网络设定一致。请参阅后面的章节来获得更多的设定指导。

3.1 第一部分 — 连接硬件

在第一部分，请您先将本产品连接至 ADSL 或是 cable modem（也就是连接到电话线或是线缆接头上）、连接电源线以及个人计算机，或是其它网络装置。

小心

连接各项设备之前，请将所有设备电源开关关闭，包括您的计算机、局域网络（LAN）集线器/交换器，以及网际网络安全路由器。

图 3.1 图解了硬件之间的连接。请参考并按照下列步骤操作。

3.1.1 Step 1. 连接 ADSL 或 cable modem

将以太网络线的一端连接到本产品后面板的 WAN 的连接埠，另一端连接到 ADSL 或是 cable modem 的以太网络端口。

3.1.2 Step 2. 连接个人计算机或局域网络（LAN）

如果您的局域网络连接的计算机不超过四台，请直接将每台计算机以太网络线连接到本产品后面板的 LAN 连接埠（P1—P4）即可。每一台计算机用一条以太网络线连接到本产品后面板标示为 P1—P4 的任意一个 LAN 连接埠。

如果您的局域网络联机的计算机超过四台，您必须用以太网络线一端连接一台选购的集线器/交换器（可能是上行线连接埠，请参考该集线器/交换器用户手册），另一端连接至本产品后面板的 LAN 连接埠（标示为 P1—P4）。

注意：本产品可以使用交叉的或是直的以太网络线。

3.1.3 Step 3. 连接电源供应器

请将电源线的一端连接到本产品后面板标示为 POWER 的电源插座，另一端请连接到墙壁上的电源插座。

3.1.4 Step 4. 开启网际网络安全路由器、ADSL 或是 cable modem 的电源，并打开您的个人计算机

请按下本产品后面板的电源开关至 ON 位置，开启 ADSL 或是 cable modem 的电源，并打开每一台连接到路由器上的个人计算机，打开任何 LAN 设备（如集线器/交换器）的电源。

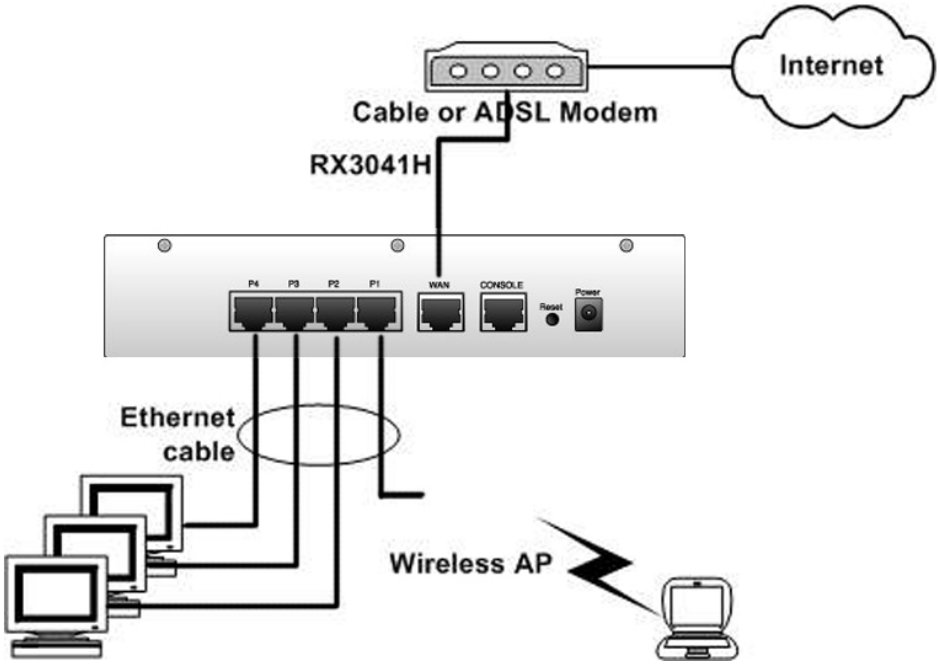


图 3.1. 硬件连接概况

您必须确认 LED 指示灯是否如表 3.1 所示运作正常。

表 3.1. LED 指示灯

指示灯	状 态
POWER	亮绿灯显示电源连接正常；倘若灯不亮，请检查电源线是否有连接到墙壁上的电源插座，连接至本产品后面板电源插座的电源线是否连接妥当。
LAN1—LAN4	亮绿灯显示本产品可以正常地与您的局域网络设备联线；闪烁代表本产品正在与您的局域网络设备传送或接受信息。
WAN	亮绿灯显示本产品已与您的网际网络服务供货商联线；闪烁代表本产品正在从网际网络传送或接收信息。

若指示灯如上表预期一样运作正常，则代表本产品已妥当连接且运作正常。

3.2 第二部分 — 设定网际网络参数

第二部分告诉您如何在您的个人计算机上设定网际网络参数以与网际网络安全路由器协调工作。

3.2.1 在您开始之前

本产品默认值将会自动设定您的计算机所有必需的网络设定，您只需要让您的计算机接受这些设定即可。


注意

在某些状况下，您可能希望手动设定某几台或是所有计算机的相关网络设定参数，而不接受网际网络安全路由器的自动设定值，请参考第 13 页"手动静态 IP 地址设定"的说明。

- 如果您已经透过以太网络将您的个人计算机与网际网络安全路由器相连，请参考以下不同操作系统的操作步骤来设定您的参数。

3.2.2 Windows® XP：

1. 在 Windows 桌面任务列中点选 **<开始>** ，然后点选 **<控制台>**。
2. 双击 **<网络联机>** 图标。
3. 在 **<LAN> 或<高速互聯網>** 窗口，在您的个人计算机相关的网络适配卡（NIC）图标（通常显示为 **<区域联机>**）按下右键，点选 **<内容>**。

<区域联机 内容> **对话窗将列出一串目前已经安装的网络选项。**

4. 请确认 **<互聯網协议（TCP/IP）>** 左边的选取方块为打勾，点选该选项，然后点选 **<内容>** 。
5. 在 **<互聯網协议（TCP/IP）>** 对话窗，点选 **<自动取得 IP 地址>**，再点选 **<自动取得 DNS 服务器地址>**。
6. 点选 **<确定>** 两次，以保存您的设定，并关闭 **<控制台>**。

3.2.3 Windows® 2000：

首先请确定系统是否安装了**互聯網协议（TCP/IP）**，若无则必须安装：

1. 在 Windows 桌面任务列中点选 **<开始>** ，再点选 **<设定>**，然后点选 **<控制台>**。
2. 双击 **<网络和拨号联机>** 图标。
3. 在 **<网络和拨号联机>** 窗口，在 **<区域联机>** 图标按下右键，点选 **<内容>**。

<区域联机 内容> **对话窗将列出一串目前已经安装的网络选项，若**互聯網协议（TCP/IP）**在已安装的列表中，请跳至步骤 10。**

4. 若**互聯網协议（TCP/IP）**不在已安装的列表中，请点选 **<安装>** 。
5. 在 **<选择网络组件类型>** 对话窗，请点选 **<通讯协议>** ，然后点选 **<新增>** 。
6. 在**通讯协议**列表中，点选 **<互聯網协议（TCP/IP）>**，然后点选 **<确定>** 。

安装程序可能需要您将 Windows 2000 安装光盘放入光驱中，请依照屏幕指示操作。

7. 在接下来的对话窗，点选 **<确定>**，用新的设定重新激活计算机。

接下来，设定您的计算机以接受网际网络安全路由器的自动设定：

8. 在控制台窗口，双击 **<网络和拨号联机>** 图标
9. 在 **<网络和拨号联机>** 窗口，在 **<区域联机>** 图标按下右键，点选 **<内容>**。
10. 在 **<区域联机 内容>** 对话窗，点选**互聯網协议（TCP/IP），**然后点选 **<内容>**。
11. 在 **<互聯網协议（TCP/IP）>** 对话窗，点选 **<自动取得 IP 地址>**，再点选 **<自动取得 DNS 服务器地址>**。
12. 点选 **<确定>** 两次，以保存您的设定，并关闭 **<控制台>**。

3.2.4 Windows® 95/ 98/ Me：

1. 在 Windows 桌面任务列中点选 **<开始>** ，再点选 **<设定>**，然后点选 **<控制台>** 。
2. 双击 **<网络>** 图标。

<网络 内容> **对话窗将列出一串目前已经安装的网络选项，请寻找** <TCP/IP> **开头，且字符串中显示您的网络配置卡的选项。若** <TCP/IP> **在已安装的列表中，请跳至步骤 9。**

3. 若 **<TCP/IP>** 不在已安装的列表中，请点选 **<确定>**。
4. 在 **<选择网络组件类型>** 对话窗，请点选 **<通讯协议>** ，然后点选 **<新增>**。
5. 在**制造厂商**部分点选 **Microsoft**，在**网络通讯协议**中，点选 **< TCP/IP>**，然后点选 **<确定>**。

安装程序可能需要您将 Windows 95、98 或 ME 安装光盘放入光驱中，请依照屏幕指示操作。

6. 在接下来的对话窗，点选 **<确定>**，用新的设定重新激活计算机。

接下来，设定您的计算机以接受网际网络安全路由器的自动设定：

7. 在控制台窗口，双击 **<网络>** 图标。
8. 在 **<网络 内容>**窗口，点选 **<TCP/IP>** 开头，且字符串中显示您的网络配置卡的选项，然后点选 **<内容>**。

   倘若您有不只一个 **<TCP/IP>** 网络组件，请选择属于您的网络配置卡相关的组件。

9. 在 **<TCP/IP 内容>** 窗口，点选 **<TCP/IP>** 索引卷标，点选 **<自动取得 IP 地址>**。
10. 在 **<TCP/IP 内容>** 窗口，点选 **<预设网关>** 索引卷标，在 **<新的网关>** 字段输入 **192.168.1.1**，然后点选 **<新增>**。
11. 点选 **<确定>** 两次，以储存您的设定，并关闭 **<控制台>**。
12. 如果系统要您重新开机，请点选 **<是>** ，重新激活计算机。

3.2.5 Windows® NT 4.0 工作站：

首先请确定系统是否安装了**互聯網协议（TCP/IP）**，若无则必须安装：

1. 在 Windows 桌面任务列中点选 **<开始>** ，再点选 **<设定>**，然后点选 **<控制台>**。

2. 在控制台窗口，双击 **<网络>** 图标。

3. 在 **<网络>** 窗口，点选 **<协议>** 图标。

<协议> **对话窗将列出一串目前已经安装的网络选项，若**互聯網协议（TCP/IP）**在已安装的列表中，请跳至步骤 9。**

4. 若**互聯網协议（TCP/IP）**不在已安装的列表中，请点选 **<新增>**。

5. 在**通讯协议**列表中，点选 **<互聯網协议（TCP/IP）>**，然后点选 **<确定>**。

安装程序可能需要您将 Windows NT 安装光盘放入光驱中，请依照屏幕指示操作。

当所有的档案都安装好后，屏幕上会跳出窗口提醒您，被称为 DHCP 的 TCP/IP 服务已創建来动态分配 IP 信息。

6. 点选 **<是 >** 继续，再点选 **<确定>**，用新的设定重新激活计算机。

接下来，设定您的计算机以接受网际网络安全路由器的自动设定：

7. 打开**控制台**窗口，双击 **<网络>** 图标。

8. 在 **<网络>** 窗口，点选 **<协议>** 图标。

9. 在 **<协议>** 对话窗，点选 **Internet 协议（TCP/IP），**然后点选 **<内容>**。

10. 在 **<TCP/IP 内容>** 窗口，点选 **<TCP/IP>** 索引卷标，点选 **<从 DHCP 服务器自动取得 IP 地址>** 。

11. 点选 **<确定>** 两次，以保存您的设定，并关闭 **<控制台>**。

3.2.6 手动固定 IP 地址设定

在某些状况下，您可能希望手动设定某几台或是所有计算机的相关网络设定，而不接受网际网络安全路由器的自动设定值。在下列情况中，这种状况是有需求的，但并非必需：

- 您已经获得了一个或多个公共 IP 地址，而且您希望经常性地与某些特定的计算机联系（例如，您将计算机用作公共网络服务器）。
- 您在局域网络（LAN）内设有子网络。

本产品预设的局域网络地址是 192.168.1.1，无论如何，第一次设定本产品时，您必须将您的计算机的 IP 地址指定在 192.168.1.0 子网络下（譬如 192.168.1.2）以創建本产品与您计算机的联线。子网掩码必须输入 255.255.255.0，预设网关设定为 192.168.1.1 ，这些设定可以稍后再修改以符合真实的网络环境。

对那些欲设定静态 IP 地址的计算机，请参考第 11 到 14 页的方法，将原本**自动设定 IP 地址**的部分，改成**指定 IP 地址**，并输入子网掩码 255.255.255.0，预设网关 192.168.1.1 。


注意

每一台计算机都必须设定不同的 IP 地址，但都必须在 192.168.1.0 子网络下（譬如192.168.1.2…）。如果您要为所有的局域网络计算机设定 IP 信息，您可以按照第五章的说明来相应地更改局域网络接口 IP 地址。

3.3 第三部分 — 快速设定网际网络安全路由器

第三部分将带您登入网际网络安全路由器设定管理程序，进行相关的基本设定。您的网络服务供货商已经提供了一些相关信息可以完成本基本设定。本快速安装仅提供基本设定指南，详细的设定及高级功能请参考相应章节。

3.3.1 设定按钮说明

本产品提供一个预先安装的设定管理程序（Configuration Manager），可以让您透过浏览器设定您的网际网络安全路由器。设定精灵将带领您一步一步的完成设定，以下是您在设定过程中将会遇到的按钮说明。

按钮	*功 能*
Next	点选此按钮跳到下一个设定步骤，倘若该页设定不需任何修改，可以直接按下此按钮，跳到下一个步骤。
Back	点选此按纽跳回上一个设定步骤。

3.3.2 设定网际网络安全路由器

请参考下列步骤：

1. 在登入本产品设定页面之前，请您务必关闭 HTTP 代理服务器。点选 IE 浏览器的**工具 ➔ 网络选项 ➔ 联机 ➔ 局域网络设定**，将**为 LAN 使用代理服务器**复选框取消。
2. 在任何一台连接本产品的网络计算机上，请打开网络浏览器输入以下网址，然后按下 **<Enter>**：

   http://192.168.1.1

   这是预先定义好设在互联网安全路由器 LAN 埠的 IP 地址 。

   将会出现如 登入页面：

图 3.2. 登入页面

倘若您无法联机到网际网络安全路由器，未出现登入页面，您必须确认该计算机是否已接受网际网络安全路由器自动设定的 IP 地址，另一个方法是手动设定该计算机的 IP 地址在 192.168.1.0 的子网络下，譬如将 IP 地址设定为 192.168.1.2。

3. 第一次登入时，请在上图登入页面输入以下预设的姓名及密码，然后点选 OK 。登入之后您可以自行修改密码。

User Name 默认值： admin

Password 默认值： admin

注意

您可以随时更改密码（请参考第 124 页 11.1.1 更改登入密码）

登入之后将出现以下设定主页面 （请参看第 15 页**錯誤! 找不到參照來源。**）。

图 3.3. 设定主页面

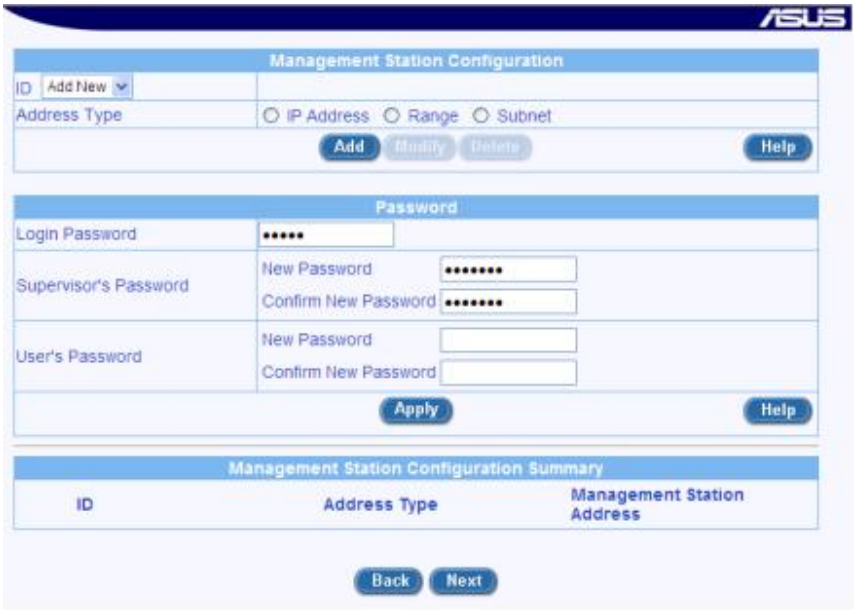


图 3.4. 密码设定页面

4. 点选 Next 按钮进入图 3.4 密码设定页面，若不想修改密码，请按下 Next 按钮。
   改变密码前，首先要在 **login password** 字段输入目前的密码，在 **New Password** 及 **Confirm New Password** 字段输入新的密码，然后点选 Apply 按钮以保存设定。
5. 出现图 3.5 所示页面，请在各字段输入相关信息，然后点选 Apply 按钮以保存设定。否则，按下 Next 按钮，直接跳到下一个设定页面。

图 3.5. 系统信息设定页面

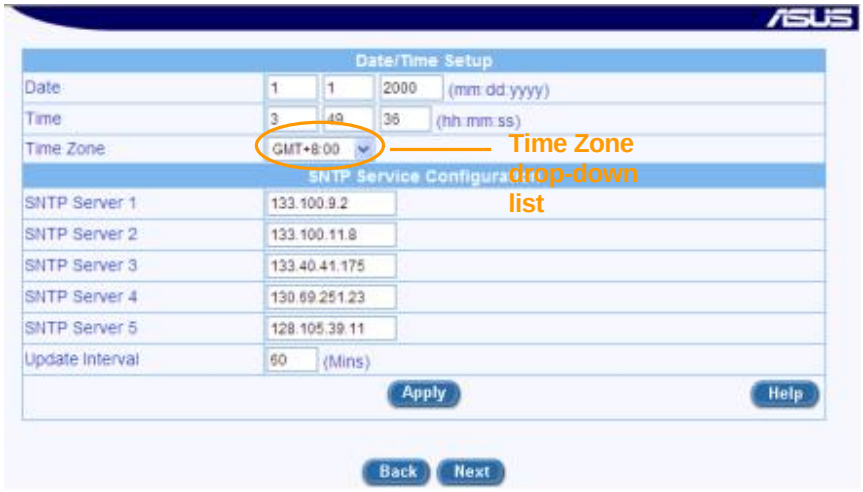


图 3.6. 日期 / 时间设定页面

6. 在图 3.6 页面，请在 Time Zone 字段右边按下拉式选单选取本产品所在时区，然后点选 Apply 按钮以保存设定。点选 Next 按钮跳到下一个设定页面。

   本产品内部并无时钟，系统的日期 / 时间是透过外部的网络服务器管理，因此不需要在此处设定日期 / 时间，除非您无法进入外部的网络服务器，或是您想透过网际网络安全路由器来管理日期 / 时间。

7. 出现图 3.7 局域网络 IP 设定页面，请勿现在更改预设的局域网络 IP 地址，直到您完成以下设定，并确认您的网际网络操作正常。点选 Next 按钮跳到下一个设定页面。

图 3.7. 局域网络 IP 设定页面

图 3.8. DHCP 服务器设定页面

8. 在图 3.6 DHCP 服务器设定页面，请勿修改 DHCP 服务器默认值，直到您完成以下设定，并确认您的网际网络操作正常。点选 Next 按钮跳到下一个设定页面。

9. 图 3.7. 是网际网络安全路由器的广域网 WAN 设定，本项目视您的网络服务供货商 ISP 提供的联机模式而定，您可以从图 3.9 connection mode 下拉式菜单的三个选项中选择一设定 ：PPPoE、Dynamic 和 Static。

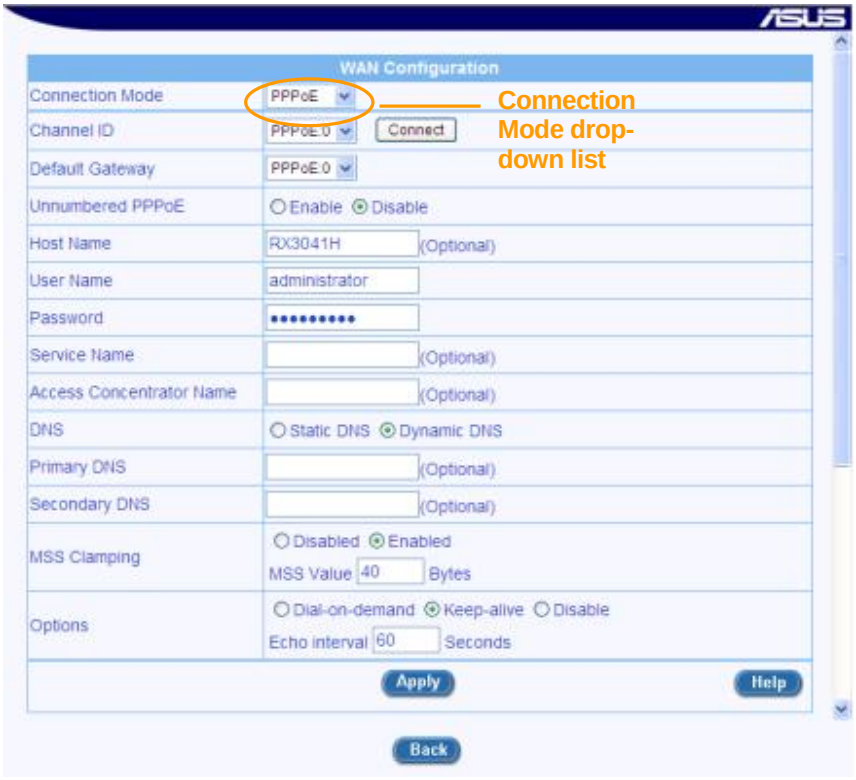


图 3.9. WAN PPPoE 设定页面

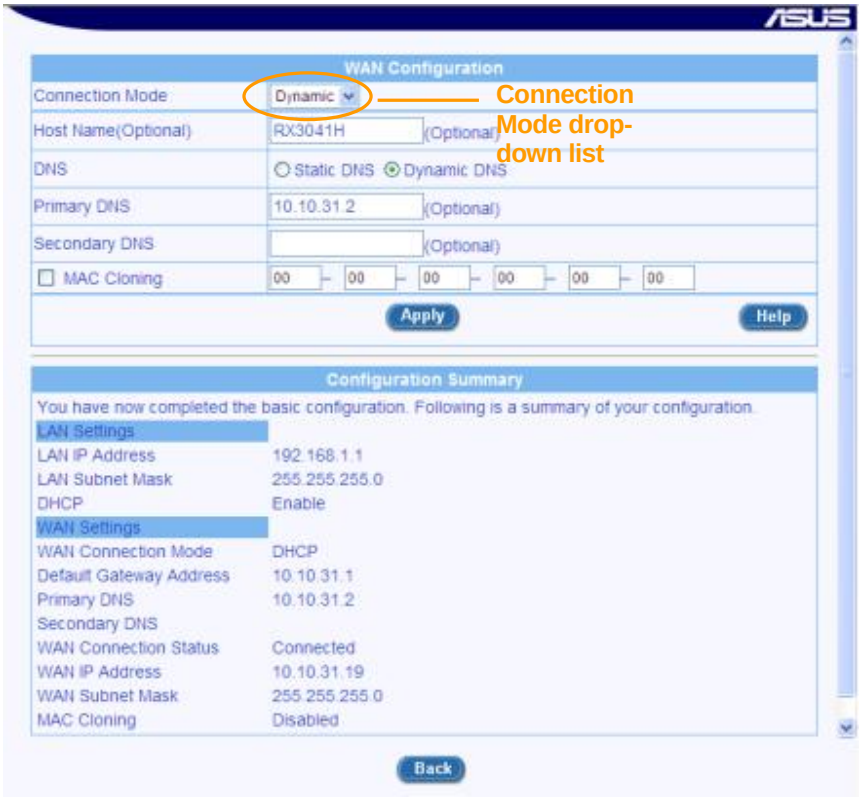


图 3.8. WAN 动态 IP 设定页面

a) PPPoE 联机模式（参看图 3.9）

- 您不需输入 primary/secondary DNS IP 地址，PPPoE 联机模式可自动从您的 ISP 获得相关信息，若您想用您惯用的 DNS 服务器，您可以在此输入地址。
- Host name 非必要，若您的 ISP 并未提供 host name，该处可以留下空白。
- 在 user name 及 password 字段输入您的 ISP 提供的 user name 及 password。
- 点选 Apply 按钮以保存 PPPoE 设定。

b) 动态 IP 联机模式（参看 图 3.8）

- 您不需输入 primary/secondary DNS IP 地址，DHCP 客户端可自动从您的 ISP 获得相关信息，若您想用您惯用的 DNS 服务器，您可以在此自行输入地址。
- Host name 非必要，若您的 ISP 并未提供 host name，该处可以留下空白。
- 倘若您事先已在 ISP 设定了 MAC 地址以连上网际网络，请在 MAC cloning 字段输入该 MAC 地址，并记得点选左边的选取方块。
- 点选 Apply 按钮以保存动态 IP 设定。

图 3.9. WAN 静态 IP 设定页面

c) 静态 IP 联机模式

- 在 IP Address 字段里输入 WAN IP 地址，本信息由您的 ISP 提供。

- 在 Subnet Mask 字段输入子网掩码，本信息由您的 ISP 提供，通常是 255.255.255.0。
- 在 gateway address 字段输入网关地址，本信息由您的 ISP 提供。
- 在 primary DNS IP 字段输入您的 ISP 提供的 IP 地址，Secondary DNS IP 非必要，若您的 ISP 有提供再填。
- 点选 

按钮以保存固定的 IP 设定。

您已经完成本产品的基本设定。请参考以下部分确定您是否已经连入网际网络。

3.3.3 测试您的设定

您已经完成本产品的基本设定，连接在本产品的局域网络上的计算机可以透过网际网络安全路由器所连接的 ADSL 或是 cable modem 联机到网际网络。

打开您局域网络上计算机的网络浏览器，输入任何一个外部网站（譬如 *http://www.asus.com*），标示为 WAN 的指示灯将会快速闪烁，等到连上之后就会保持亮灯状态，您将可以看到网页页面。

倘若指示灯并未闪烁或亮灯网页也未出现，请参考附录 15 “解决问题” 章节内容中更为详尽的说明。

3.3.4 路由器预设设定

除了控制 DSL 联机到 ISP 上之外，网际网络安全路由器还能为您提供多种多样的网络服务。您的路由器已经预设好了适合典型家庭和小型办公室网络应用的预设设定。

表 3.2 列出了一些最重要的预设设定。这些设定和其它一些规格将在下面的章节中详尽介绍。如果您熟悉您的网络预设设定，请查看表 3.2 中的设定来确定它们是否符合您网络的要求。如需要，请根据说明来更改设定。如果您对设定不太熟悉，那么请勿更改设定，或者请联络您的网络供货商 ISP 寻求帮助。

在您更改任何设定之前，请参考第 4 章获取联机和使用 Configuration Manager program（设定管理器程序）的综合信息。我们强烈推荐您在更改预设设定之前联络您的网络供货商！

表 3.2. 预设设定摘要

选 项	预设设定	解释 / 说明
DHCP（主机动态设定协议）	DHCP 伺服器在以下地址起作用： 192.168.1.10 透过 192.168.1.108	网际网络安全路由器为您的局域网络（LAN）中的计算机提供一些私人 IP 地址的动态分配。要享受此项功能带来的好处，您必须按照“快速安装指南” 第二部分中描述的那样设定您的计算机，以便能够动态地接收 IP 信息。请参看第 5.2 节中关于 DHCP 服务器的说明。
LAN 埠 IP 地址	静态 IP 地址：192.168.1. 1 子网掩码：255.255.255.0	这是 LAN 端口在网际网络安全路由器上的 IP 地址。LAN 端口将您的计算机接入以太网络。一般来说，您并不需要改变这个地址。请参考第 5.1 节中局域网络（LAN）地址的说明。

4 从设定管理器程序安装

网际网络安全路由器已经预先安装了一个名为 *设定管理器* 的程序，这个程序提供本产品已安装好的软件接口。它能让您设定本产品来符合您网络的要求。您可以从任何以 LAN 或 WAN 接入网际网络安全路由器的 PC 上的网页浏览器接入。

本章将帮助您使用设定管理器来安装。

4.1 登入设定管理器

设定管理器程序已经预先[illegible]您需要：

- 接入网际网络安全路由[illegible]章"快速安装指南"。
- 在计算机上安装网页浏[illegible]件，版本在 5.5 以上，或者 Netscape 浏览器，版[illegible]

您可以从任何透过 LAN 或[illegible]入该程序。但是，我们在这里提供的说明仅针对透过 LAN 端[illegible]

1. 将计算机接入 LAN，[illegible]键：

   这是预先定义好的网际[illegible]如图 4.1 所示：

图 4.1. 设定管理器登入页面

2. 输入您的 user name 和 password，然后点选 OK。

   在您第一次进入程序时，请选择下列默认值：

   Default User Name: admin
   Default Password: admin

4.1.1 您可以在任何时候更改 password（请参看第 124 页 11.1.1 节 变更登入密码

注意

当您第一次登入设定管理员，您可以使用预设的用户名称与密码:admin 与 admin 。系统会允许两种用户登入，分别为系统管理员（administrator: username:admin）与访客（guest:username:guest）。其中系统管理员具有权力去修改设定，而访客则只能检视系统设定。至于这两组用户的密码则为 admin 与 guest，系统管理员可针对密码进行变更。

此处的用户名称与密码只用来登入设定管理员之用，此一帐号密码

Note *与您用来与 ISP 联机的帐号密码不同。*

请依照下列步骤来变更密码:

1. 藉由点选 System **Management ➔ Password** 选单来开启密码设定页面。
2. 输入既有的密码在 **Login Password** 字段。
3. 在 New **Password** 字段输入新的密码，并在 Confirm **New Password** 字段重新输入一次密码。

   密码可以是十六位数字，当您登入时，您必需在上方与下方的字段输入新的密码。

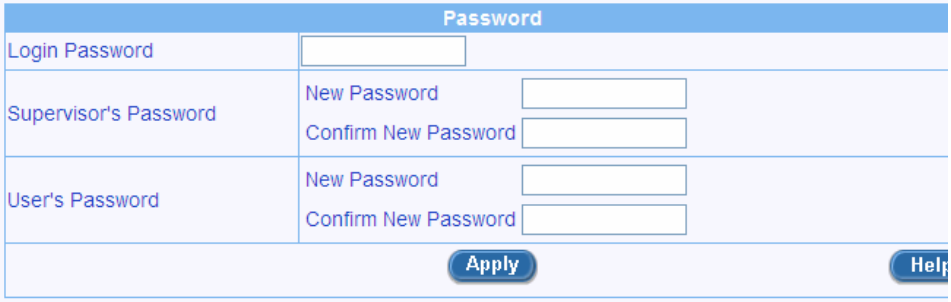


图 11.2. 密码设定

4. 点选 Apply 按键来储存新的密码。请注意只有在密码输入正确并在正确的字段才会生效。

4.1.2 设定管理站

有时候，您可能想要限制主机对路由器进行设定。在默认值中，只要输入的帐号与密码正确，则可让系统管理员从任何计算机登入。这样的作法可让未经认证者在知道设定管理员接口的帐号与密码的情况下进行登入。在此设定页面中您可利用输入单一 IP 地址、IP 地址范围或网络地址与子网掩码，最多设定八组的管理站。

WARNING

若管理站群组未经设定，则管理员可从任何地方登入路由器。然而，若有一组或更多的管理站群组被设定，则只有经过设定之特定管理站群组可以设定路由器。若您忘记管理群组的设定，您将无法存取路由器的设定管理员接口，除非按下路由器的重置键进行重置。

i) 管理站参数设定

表 11.1 叙述管理站设定页面中可进行设定的参数。

表 11.1. 管理站参数设定

字段	叙述
ID	
Add New	点选此选项来新增一组新的管理群组。
Number	从下拉式选单中选择管理群组以变更设定。

Address Type 本选项可让您选择您要如何指定管理站群组使用的IP地址。在此共有三种选项可供设定，分别是: IP 地址、范围与子网络。	
IP Address	本选项可让您指定管理站的IP地址。
Address	指定一组适当的IP地址。
Range	本选项可让您从管理站群组指定IP地址范围。当本选项被选择，则以下的字段便可以进行设定:
Begin	输入起始的IP地址范围。
End	输入中止的IP地址范围。
Subnet	本选项可让您指定所有连接到相同IP子网络的计算机作为一管理站群组。当本选项被选择，则以下的项目便可以加以输入:
Network Address	输入适当的IP地址。
Subnet Mask	输入对应的子网掩码。

i) 新增一组管理站群组

请依照以下介绍来新增一组管理站群组:

5. 藉由点选 System **Management ➔ Password** 选单来开启密码设定页面。
6. 从“ID”下拉式选单中选取 “Add **New**” 。
7. 在以下三选项选择 “Address Type”（地址类型） – **IP Address, Range** 与 **Subnet** ，接着请输入您想要输入的 IP 地址信息。

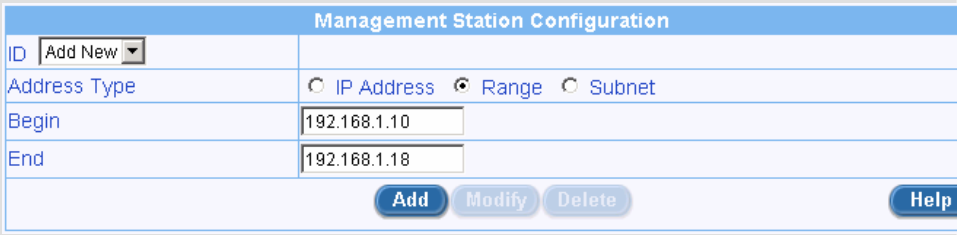


图 11.3. 管理站设定

8. 点选 

按键来新增一组新的管理站群组。您将可看到新增的管理站群组摘要显示在同一设定页面。

图 11.4. 管理站摘要

i) 变更管理站群组

请依照以下介绍来变更管理站群组:

9. 藉由点选 System **Management ➔ Password** 选单来开启密码设定页面。
10. 从 ID 下拉式选单中选择一管理群组。
11. 请在“Address **Type”项目中设定想要进行的变更并输入对应的** IP 地址信息。
12. 点选 Modify 按键来变更设定。

i) 删除管理站群组

如欲删除管理站群组，您只要点选选项前的 图标 (在管理站摘要列表中)即可加以删除，或是依照以下介绍进行删除:

13. 藉由点选 System **Management ➔ Password** 选单开启密码设定页面。
14. 从“ID”下拉式选单中选择一组管理群组的号码。
15. 点选 Delete 按键来删除管理站群组。

当您每次登入程序时，设定页都会出现。（请参看第 23 页）

4.2 功能性设定

一般来说，设定管理器页面包括两个独立的页面，如图 4.2 所示，左边的页面包括所有的设备设定。菜单将会用图标 提示您，相关的菜单将分类标出，例如 LAN、WAN 等等。基于菜单中是否有子资料夹，分别以不同的数据夹图标 或 标出。您可以点选任意的菜单来进入特定的设定页。

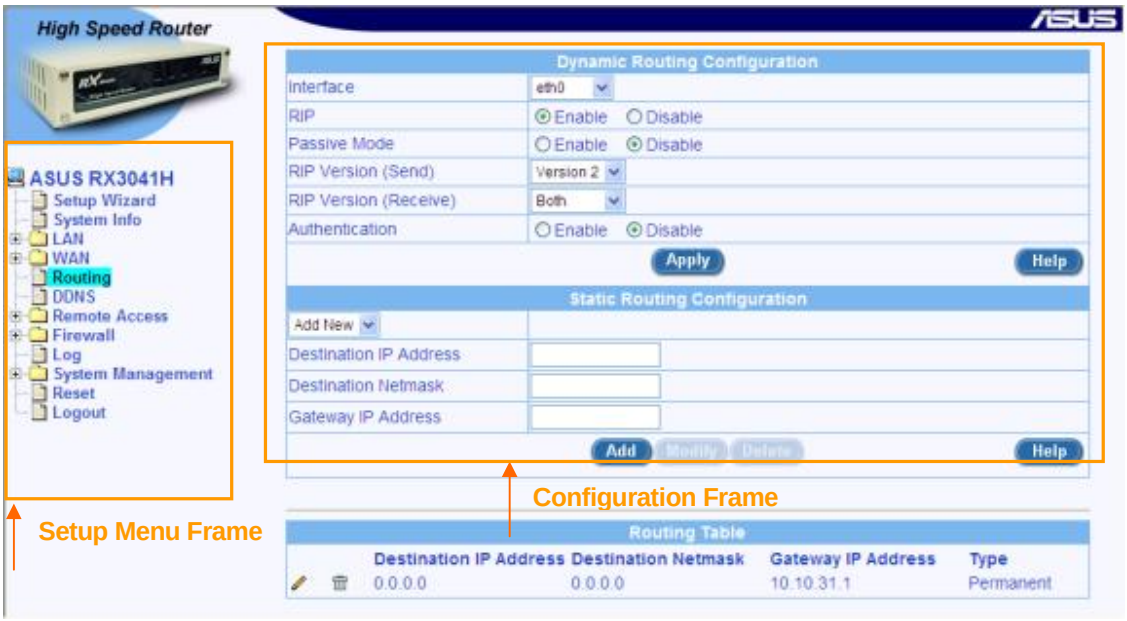


图 4.2. 一般设定管理器页面

每个菜单都会显示右边页面中的独立页面。例如，图 4.2 中的设定页面表示 DHCP 设定。

4.2.1 創建菜单导航提示

- 要扩展到一系列相关的菜单：点选 **+**，然后点选相应数据夹的图标  。
- 要缩短显示的相关菜单：点选 **–**，然后点选打开的数据夹图标  。
- 要打开特定的设定页，点选数据图标  ，然后进入您的目标选项。

4.2.2 经常用到的按钮和图标

下面的按钮和图标将在很多地方用到。下表列出了每个按钮和图标的功能。

表 4.1. 经常用到的按钮和图标

按钮/图标	*功 能*
Apply	随时保存您在当前页面上所做的任何更改。
Add	将现有的设定保存至系统，例如，静态路由线路或防火墙 ACL 规则等等。
Modify	更改系统现有的设定，例如，静态路由线路或防火墙 ACL 规则等等。
Delete	删除已选的选项，例如静态路由线路或防火墙 ACL 规则等等。
Help	在独立的浏览器窗口中开启为现有主题设定的在线帮助。任何主要主题的帮助页面均可用。
Refresh	重新显示现有页面升級后的统计表或设定。
	选择要编辑的选项。
	删除已选的选项。

4.3 系统设定概述

要概览整个系统设定，请以管理员身份登入设定管理器，然后点选**系统信息**菜单。 图 4. 显示了系统信息页面的一些信息。


High Speed Router
ASUS
ASUS RX3041H
Setup Wizard
System Info
LAN
WAN
Routing
DDNS
Remote Access
Firewall
Log
System Management
Reset
Logout
System Information
Software Version RX3041H.1.1.30a.410, Aug 12 2004, 10:43:09
Lan IP Address 192.168.1.1
WAN Port MAC Address 00:0c:6e:3c:51:5d
LAN Port MAC Address 00:b0:3b:00:00:01
System Up Time 0 Day(s), 4 Hr(s), 3 Min(s), 13 Sec(s)
System Name RX3041H
System Location
System Contact
LAN Settings
LAN IP Address 192.168.1.1
LAN Subnet MasK 255.255.255.0
WAN Settings
WAN Connection Mode DHCP
WAN Connection Status Connected
WAN IP Address 10.10.31.19
WAN Subnet Mask 255.255.255.0
Default Gateway Address 10.10.31.1
Primary DNS 10.10.31.2
Secondary DNS
MAC Cloning Disabled
System Services
Firewall Enabled
DHCP Enabled
DNS Enabled
DDNS Disabled
RIP Disabled
SNTP Disabled
Revert back to the factory default by using the Reset Button Enabled

图 4.3. 系统信息页

5 设定局域网络 LAN

本章将向您说明如何设定连接您的 LAN 计算机的网际网络安全路由器 LAN 接口的 LAN 属性。在本章，您将学会如何为您的局域网络设定 IP 地址、DHCP 和 DNS 服务器。

5.1 局域网络（LAN） IP 地址

如果您将多台 PC 连入网际网络安全路由器，您必须透过内建的以太网交换器上的以太网局域网络（LAN）埠连接。您必须指派一个唯一的 IP 地址给每个连接到局域网络（LAN）的设备。局域网络（LAN）的 IP 地址把网际网络安全路由器认作您网络的一个节点。那就是说，它的 IP 地址必须与您的 PC 处于相同的局域网络（LAN）的子网络中。网际网络安全路由器预设的局域网络（LAN）IP 地址为 192.168.1.1。

名词解释

*当某一设备联机进入网络，它就可以被认为是**网络节点**，例如网际网络安全路由器的 LAN 埠，PC 的网络适配卡等，请参考附录 A 对子网络的解释。*

您可以将默认值按照您想要使用的网络 IP 地址改变。

注意

网际网络安全路由器自身能够为您接入局域网络的计算机起到 DHCP 服务器的作用，正如第 5.2.2 节 设定，但是不能作为它自身的LAN 埠。

5.1.1 局域网络（LAN） IP 设定参数

表 5.1说明了局域网络（LAN） IP 设定的现有参数。

表 5.1. 局域网络（LAN） IP 设定参数

设定	**说明**
IP 地址	网际网络安全路由器的局域网络（LAN）IP 地址。此 IP 被您的计算机用来识别网际网络安全路由器的 LAN 埠。请注意，您的网络供货商指派给您的公共 IP 地址**并非**您的局域网络（LAN）的 IP 地址。公共 IP 地址确认进入网际网络的安全路由器上的 WAN 埠。
子网掩码	局域网络（LAN）的子网掩码确认局域网络（LAN）的 IP 地址的哪个部分整体提及您的网络，以及哪个部分特别提及网络的节点。您的设备已经预先设定好了预设的子网掩码 255.255.255.0。

5.1.2 设定局域网络（LAN）的 IP 地址

请参照以下步骤来更改预设的局域网络（LAN）IP 地址：

1. 以管理员身份登入设定管理员程序，然后点选 LAN 菜单。

   当 LAN 设定的子菜单出现时，点选 IP 子菜单以显示如图 5.1 所示的设定页面。

图 5.1. LAN IP 地址设定页面

2. 进入 LAN 的 IP 地址和网际网络安全路由器提供的子网掩码。
3. 点选 Apply 以保存局域网络（LAN）IP 地址。

   倘若您正在使用过去的以太联机，并已经改变了 IP 地址，那么联机将被中断。
4. 如需要，请预先设定您的 PC，使他们的 IP 地址将他们置于与 LAN 埠的新 IP 地址相同的子网络下。 请参看“快速安装指南”一章的第二部分 。
5. 在您的网页浏览器/地址中输入新的 IP 地址，登入设定管理器。

5.2 DHCP （动态主机控制协议）

5.2.1 简介

5.2.1.1 什么是 DHCP?

DHCP 是一种网络协议，它能使网络管理员集中管理网络中计算机 IP 信息的指派和分配。

当您在网络上启动 DHCP 时，您的设备 — 例如网际网络安全路由器 — 就可以给您的计算机分配临时的 IP 地址，无论它们是否接入了网络。分配的设备称为 *DHCP 服务器*， 接收设备称为 *DHCP 客户端*。

注意

倘若您遵照“快速安装指南”的说明行事，您要么已经为局域网络中的每台 PC 都设定了 IP 地址，要么您已经认定 PC 将动态（自动）接收 IP 信息。倘若您选择动态接收信息，那么，您就已经将您的计算机设定为 DHCP 客户端，它将接受 DHCP 服务器（例如网际网络安全路由器）指派的 IP 地址。

DHCP 服务器掌握了一系列特定的 IP 地址，然后，当您需要接入网际网络时，再在特定的时间把它们“释放”给您的计算机。

在启动了 DHCP 的网络上，IP 信息是 *动态* 而不是 *静态* 地分配的。每次连入网络时，DHCP 客户端分配到的地址都不同。

5.2.1.2 为什么使用 DHCP?

DHCP 允许您透过网际网络安全路由器管理和分配 IP 地址。如果没有 DHCP，您就得逐一为每台计算机设定 IP 地址和相关的信息了。DHCP 常被用于大型网络和频繁扩张或升級的网络。

5.2.2 设定 DHCP 服务器

注意

网际网络安全路由器已经被预设定义为 LAN 领域的 DHCP 服务器，其预先定义的 IP 地址为透过 192.168.1.42（子网掩码 255.255.255.0）的 192.168.1.10。要改变地址域，请按照本节中说明的程序进行。

5.2.2.1 DHCP 参数设定

表 5.2 叙述在 DHCP 服务中可进行设定的相关参数

表 5.2. DHCP 设定参数

选项	说明
IP 开始/结束的地址池	**指定了 DHCP 地址池中开始和结束的地址 。**
子网掩码	**输入 DHCP 地址池使用的子网络屏蔽。**
租用的时间	指派地址租用的时间将被连接到 LAN 的设备使用。
预设的网关 IP 地址	**接收 IP 地址的计算机网关的预设地址在本领域。预设的网关是 DHCP 客户端最先联机到网际网络的设备。一般来说，将会是网际网络安全路由器的局域网络（LAN）埠的 IP 地址。**
Primary/Secondary DNS 服务器 IP 地址	***网域名称系统*** **服务器的 IP 地址将被从本领域接收 IP 地址的计算机使用。DNS 服务器会把您输入网页浏览器的普通网际网络名称转换为相同意义的 IP 地址。一般来说，服务器由您的网络供货商设定，然而，您可以输入网际网络安全路由器局域网络（LAN）的 IP 地址，因为它是 LAN 计算机的 DNS 代理，并且促使 DNS 指令从 LAN 传递至 DNS 服务器，以及把结果传回 LAN 计算机。请注意，Primary 和 secondary DNS 服务器均为可选选项。**
Primary/Secondary WINS 服务器 IP 地址 (可选)	**从 DHCP 服务器的 IP 地址域接收 IP 地址的计算机将使用 IP WINS 服务器的地址。直到您的网络拥有 WINS 服务器后，您才需要输入此信息。**

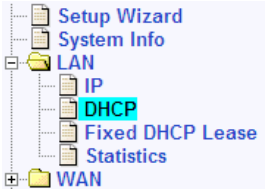
6. 点选 Apply 以保存 DHCP 服务器设定。

5.2.2.2 设定 DHCP 服务器


注意

网际网络安全路由器已经被预设定义为 LAN 领域的 DHCP 服务器，其预先定义的 IP 地址为透过 192.168.1.42（子网掩码 255.255.255.0）的 192.168.1.10。要改变地址域，请按照本节中说明的程序进行。

首先，您必需设定让您的 PC 可以接受由 DHCP 服务器所指派的 DHCP 信息:



7. 藉由点选 **LAN ➔ DHCP** 选单来开启 DHCP 服务器设定页面。在此您将可看到既有的 DHCP 服务器设定信息，与当您开启本页面时的 IP 租用列表。

8. 输入供 **IP 地址池 (Begin/End Address)**, **Subnet Mask**, **Lease Time** and **Default Gateway IP Address** 的相关信息于对应的字段; 至于其它像是 **Primary/Secondary DNS 服务器的 IP 地址** 与 **Primary/Secondary WINS 服务器的 IP 位置** 则非必需输入的. 然而，我们仍建议在 primary DNS 服务器的字段输入对应的 IP 地址。此外，您可能需要输入 LAN IP 地址或是您 ISP 的 DNS IP 地址在 primary DNS 服务器的 IP 地址字段中。如欲取得更多关于设定此参数的相关信息，请参阅表 5.2 的介绍。

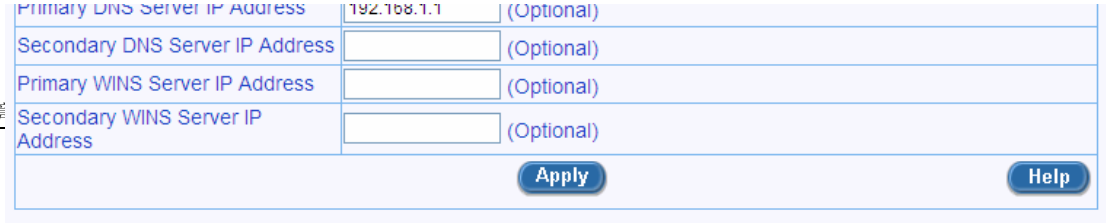


图 5.2. DHCP 设定

9. 点选 Apply 以储存 DHCP 服务器的设定值。

5.2.2.3 查看目前已租用的 IP 地址

当在您的局域网络中 RX3041H 的功能是作为 DHCP 服务器的功能使用，则其将会租用 IP 地址给予您的计算机。如欲查看目前以租用的租用列表，只要藉由点选 **LAN → DHCP** 选单以开启 DHCP 服务器设定页面。接下来，如图图 5.3 l 所示的列表将会显示在 DHCP 设定页面的下半部。

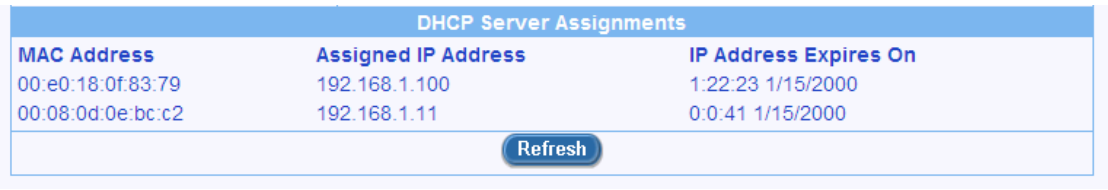


图 5.3. DHCP 租用范例列表

在 DHCP 服务器租用列表中将会显示目前所有提供给局域网络装置的 IP 地址。 表 5.3 叙述每一个 DHCP 租用列表中的参数信息。

表 5.3. 指定 DHCP 地址参数

Field	Description
MAC Address	DHCP 服务器中每一个装置的硬件 ID。
Assigned IP Address	从地址池中所租用的地址。
IP Address Expired on	租用地址的中止时间。

5.2.3 固定 DHCP 租用

固定 DHCP 租用功能是当主机需要自 DHCP 服务器中取得一组固定的 IP 地址时使用。要使用本功能，首先您需要设定您的 PC，使其可以接受 DHCP 服务器所指派的 DHCP 信息。

5.2.3.1 固定 DHCP 租用参数设定

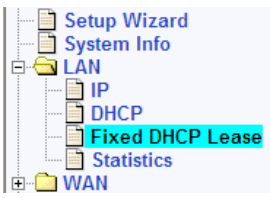
表 5.4 叙述在 DHCP 租用功能中可以进行设定的参数。

表 5.4. 固定 DHCP 租用功能参数设定 s

字段	叙述
Fixed DHCP Lease MAC	需要自 DHCP 服务器中取得一组固定 IP 地址的硬件装置 ID (MAC 地址)。
Fixed DHCP Lease IP	自 DHCP 服务器中所租用的 IP 地址。本字段建议设定 DHCP IP 地址池以外的 IP 地址。

5.2.3.2 新增一组固定 DHCP 租用

请依照下列的介绍来新增一组新的 DHCP 租用:



10. 藉由点选 **LAN ➔ Fixed DHCP Lease** 选单来开启固定的 DHCP 租用设定页面。
11. 输入主机要求之固定 IP 地址与 MAC 地址。关于每一项参数设定的细节，请参阅表表 5.4.。

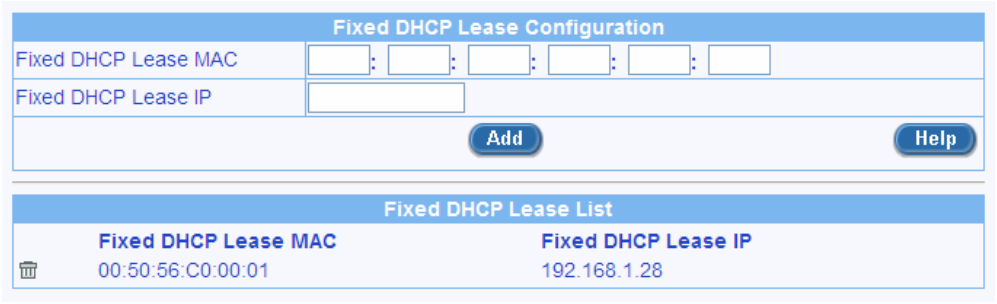


图 5.4. 固定 DHCP 租用设定页面

12. 点选 Add 按键以新增一组固定的 DHCP 租用登录。

5.2.3.3 删除一组固定的 DHCP 租用设定

如欲删除一组固定的 DHCP 租用设定，您只需点选 DHCP 租用列表中的 图标即可。

5.2.3.4 检视固定的 DHCP 租用列表

如欲检视既有的固定 DHCP 租用列表，您只要藉由点选 **LAN ➔ Fixed DHCP Leas** 选单来开启固定 DHCP 租用设定页面。

5.3 DNS

5.3.1 关于 DNS

网域名称系统（DNS，Domain Name System）用来将用户输入到网页浏览器的（例如，yahoo.com）网域名称转换为可用来网际网络路由的相同意义的 IP 地址。

当 PC 用户把网域名称输入浏览器时，PC 必须首先输送要求至 DNS 服务器以获得相同意义的 IP 地址。DNS 服务器将在自己的数据库中检查网域名称，当它无法在本地找到这个名称时，将会去与更高级的 DNS 服务器沟通。当找到地址时，它会把信息反馈给 PC，然后与余下的 IP 封包参考沟通。

5.3.2 指派 DNS 地址

当任何一台服务器死机或遇到阻塞时，提供多个 DNS 地址的选择将十分有用。一般来说，网络供货商提供 Primary 和 Secondary DNS 地址，还可能提供附加的地址。您的局域网络 PC 将会用下列方式中的一种获得 DNS 地址：

- **静态:** 倘若您的网络供货商提供给了您 DNS 服务器的地址，您就可以透过修改 PC 的 IP 属性而将它们指派给每台 PC。
- **动态（从 DHCP 地址池开始）：** 您可以设定 DHCP 服务器和创建将 DNS 地址分配至 PC 的地址池。如何创建 DHCP 地址池，请参考第 27 页设定 DHCP 服务器的部分。

您可以指定真实的网络供货商 DNS 服务器地址（在 PC 上或在 DHCP 地址池内），或指定网际网络 LAN 端口的地址（例如，192.168.1.1）。当您指定了 LAN 埠的 IP 地址，路由器就会进行 *DNS 传递* 了，具体请参考接下来的部分。

的 DNS 地址，

5.3.3

当您自动进行“DNS 传递”。因为设备自身并的 DNS 服务器。然后，它把 DNS 服

当进的 IP 地址。它能用下列两种方式获得

- （请参考第 6.2.2 节 为广域网动态 IP ）联机到网络供货商 ISP 改变他们的 DNS 地址，
- ISP 的 DNS 地址，如

- 图 6.1.，图 6.2. WAN 动态 IP (DHCP 客户端，或 图 6.3. WAN 静态。

请按照下列步骤设定您的 DNS 传递：

1. 在 DHCP 设定页面的 DNS 服务器 IP 地址中输入 LAN IP，如**錯誤! 找不到參照來源。**所示。
2. 为局域网络 PC 设定使用网际网络安全路由器的 DHCP 服务器指派的 IP 地址，或将网际网络安全路由器的局域网络 IP 地址作为 DNS 服务器地址，然后为局域网络内的所有 PC 手动输入。

注意

指派给优先进行 DNS 传递的局域网络 PC 的 DNS 地址将持续作用直至 PC 重启。DNS 传递只在 PC 的 DNS 地址为局域网络的 IP 地址时启动。

类似的，在开始 DNS 传递之后，如果您在 DHCP 地址池或 PC 上动态地指定 DNS 地址 (而不是局域网络 IP 地址)，那么这个地址将取代 DNS 传递地址而被使用。

5.4 查看 LAN 统计表

您可以在您的网际网络安全路由器上查看 LAN 通信量的统计表。您并非需要经常查看此资料，但是当您协助网络供货商查找网络和网际网络数据传输问题时，会发现统计表十分有用。

想要查看 LAN IP 统计表，请点选 LAN 子菜单的统计表，图 5.5 是 LAN 统计表页面：

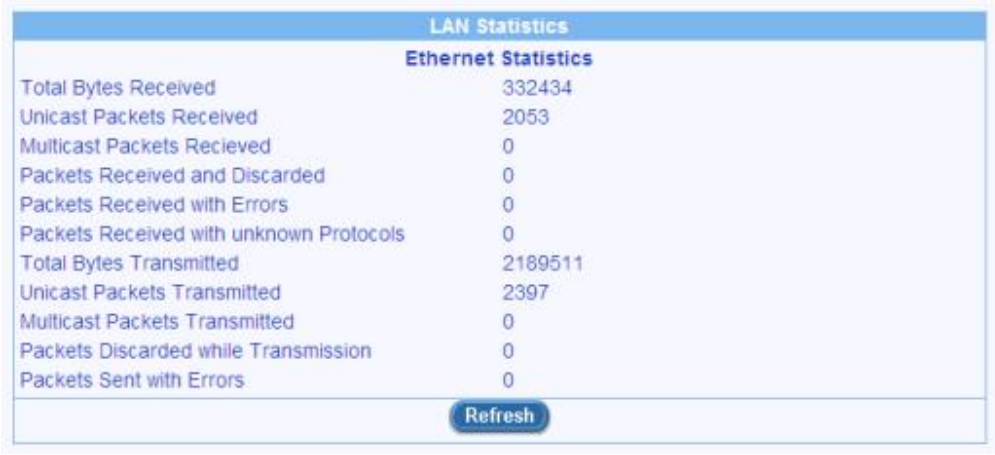


图5.5. LAN 统计表页面

想要显示升級后的统计表，点选 Refresh 。

6 设定广域网

本章将向您说明如何为与网络供
为您的 WAN 设定 IP 地址、DHCP 和

6.1 广域网（WAN）联机

网际网络安全路由器支持 WAN
种您的网络供货商支持的模式，参考

图 6.1。

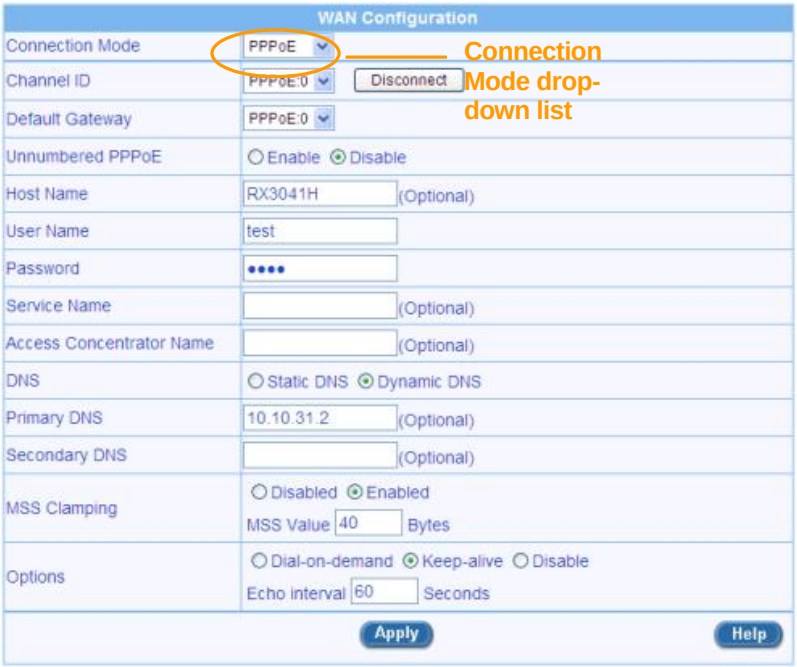


图 6.1. WAN PPPoE 设定页面

6.2 PPPoE

6.2.1 广域网（WAN） PPPoE 设定参数

表 6.1说明了PPPoE 联机模式需要的设定参数。

表 6.1. WAN PPPoE 设定参数

设定	说明
Channel ID	选择一 PPPoE 频道作为本 PPPoE 交谈层之用。请注意，本项只支持两组并存的 PPPoE 频道。
Default Gateway	由于在同一时间内可以有一组以上的 PPPoE 交谈层是动作的，因此必需选择一组预设的网关器给予一路由封包，而此一路由封包指向一在路由列表中未被列出的网络接口。请由下拉选单中选择欲作为预设网关器的设定。
Unnumbered PPPoE	点选 “Enable” 或 “Disable” 按键以开启或关闭本选项。一般来说，每一网络介必需有一组独立的 IP 地址。然而，一组未被编号的接口则无法具备独立的 IP 地址，这也就是说当本项目设定为开启，则 WAN 与 LAN 使用相同的 IP 地址。也因为越少的 IP 地址被使用且路由列表较小，所以网络资源得以被保留。
Host Name	请输入由您 ISP 所提供的主机名称。此项目非必需填入，但某些 ISP 要求需要填入本项。
User Name and Password	输入您登入 ISP 的 Username 和 Password 。（注意：这和您登入设定管理器的信息不相同。）
Service Name	输入由您 ISP 所提供的服务名称。本项目非必需填入，但某些 ISP 要求需要填入本项。
Access Concentrator Name	输入由您 ISP 所提供的存取集讯器名称。本项目非必需填入，但某些 ISP 要求需要输入本项。
Primary/ Secondary DNS	Primary 和/或 Secondary DNS 的 IP 地址可选，并且 PPPoE 将自动侦测您的 ISP 设定的 DNS IP 地址。然而，如果您使用了其它的 DNS 服务器，请输入空间提供的 IP 地址。
MSS Clamping	点选 “Disable” 或 “Enable” 按键来关闭或激活本项目。MSS (最大分割容量) 是用来告知远程网络不要传送超过 MTU（最大传输单位）与 MSS 所指定容量的封包。 举例来说，以太网络的 MTU 为 1500 bytes 而若您指定 40 bytes 作为 MSS ，则您便是告诉其它网络不要传送容量大于 1460 bytes (如 1500 – 40)的封包。
Value	若 MMS 选项设定开启，则本项目是用来输入 MMS clamping 的数值。

设定	说明
Dial-On-Demand	此项请输入您想要网际网络联机中断传输的时间。中断联机时间设定的最小值为 30 秒，而 RIP 与 SNTP 服务若设定为动作则可能受到本项设定的影响。请确认已变更系统日期与时间的间隔（于 System Management / Date/Time Setup configuration 页面） – 请见 11.3 设定系统辨识 一些特定的系统信息，像是系统名称（本装置的特定名称）、系统位置（本装置的所在位置），与在装置中的个人联络信息都可以在系统辨识设定页面中进行设定。 请依照以下介绍来变更特定的系统信息: 3. 藉由点选 System **Management ➔ System Identity** 选单来开启系统辨识设定页面。 4. 变更系统名称、系统位置与联络信息等想要进行的设定。请注意！在此字段
Keep Ali	也请启动本选项。输入 预设的“响应间隔”值为 60

6.2.2

请按

1.
2.
3.
4. ，可能您必须在 PPPoE 设定 Password ，如

5. 图 6.1 所示。
6. （可选）如果您希望使用您喜爱的 DNS 服务器，请输入 Primary 和 Secondary DNS 服务器 IP 地址；否则，跳过此步骤。
7. 选择联机选项，如需要，输入合适的设定。默认值为“Disable”。
8. 当您完成设定后，点选 Apply 以保存 PPPoE 设定。您将在设定页面的下半页看到 WAN 设定的摘要。注意：若预设网关地址没有立即显示，请点选 WAN 菜单再次打开 WAN 设定页面。

6.3 动态 IP

6.3.1 广域网（WAN） 动态 IP 设定参数

表 6.2 说明了动态IP联机模式的可选设定参数。

表 6.2. WAN 动态 IP 设定参数

选项	说明
主机名称	主机名称可选，但某些 ISP 可能有特定要求。
Primary/ Secondary DNS	Primary 和/或 Secondary DNS 的 IP 地址可选，并且 DHCP 将自动侦测您的 ISP 设定的 DNS IP 地址。然而，如果您使用了其它的 DNS 服务器，请输入空间提供的 IP 地址。
MAC Cloning	预设的使用 WAN 接口的 MAC 地址。然而，如果您事先已经在 ISP 注册了 MAC 地址，您需要在这里输入这个 MAC 地址。

6.3.2 为广域网（WAN）设定动态 IP

请按照下列步骤来设定动态 IP：

1. 从图 6.2 所示的联机模式列表中选择动态。
2. （可选）若 ISP 要求，请输入空间提供的主机名称。
3. （可选）如果您希望使用您喜爱的 DNS 服务器，请输入 Primary 和 Secondary DNS 服务器 IP 地址；否则，跳过此步骤。
4. 如果您已经事先在 ISP 注册了特别的 MAC 地址来接入网际网络，，请确认您已经把 MAC cloning 打勾。
5. 当您完成设定后，点选 Apply 以保存动态 IP 设定。您将在设定页面的下半页看到 WAN 设定的摘要。注意：若预设网关地址没有立即显示，请点选 WAN 菜单再次打开 WAN 设定页面。

图 6.2. WAN 动态 IP (DHCP 客户端) 设定页面

6.4 静态 IP

6.4.1 广域网（WAN） 静态 IP 设定参数

表 6.3说明了静态IP联机模式的可选设定参数。

表 6.3. WAN 静态IP 设定参数

设定	说明
IP 地址	WAN 的 IP 地址由您的 ISP 提供。
子网掩码	WAN 的子网掩码由您的 ISP 提供。一般来说，设定为 255.255.255.0。
网关地址	网关 IP 地址由您的 ISP 提供。它必须与路由器处于相同的子网络中。
Primary/ Secondary DNS	您必须至少要输入 Primary DNS 服务器的 IP 地址。Secondary DNS 可选。

6.4.2 为广域网（WAN）设定静态 IP

图 6.3. WAN 静态IP 设定页面

请按照下列步骤来设定静态 IP：

1. 从图 6.3 所示的联机模式列表中选择静态。
2. 在 IP 地址栏中输入 WAN IP 地址。地址信息应由您的 ISP 提供。
3. 输入 WAN 的子网掩码。屏蔽由您的 ISP 提供。一般来说，设定为 255.255.255.0。
4. 输入您的 ISP 提供的网关地址。
5. 输入 Primary DNS 服务器的 IP 地址。地址信息应由您的 ISP 提供。Secondary DNS 服务器可选。
6. 当您完成设定后，点选 Apply 以保存动态 IP 设定。您将在设定页面的下半页看到 WAN 设定的摘要。

6.5 查看 WAN 统计表

您可以在您的网际网络安全路由器上查看 WAN 通信量的统计表。您并非需要经常查看此资料，但是当您协助网络供货商查找网络和网际网络数据传输问题时，会发现统计表十分有用。

想要查看 WAN IP 统计表，请点选 WAN 子菜单的统计表，图 6.4 是 WAN 统计表页面：

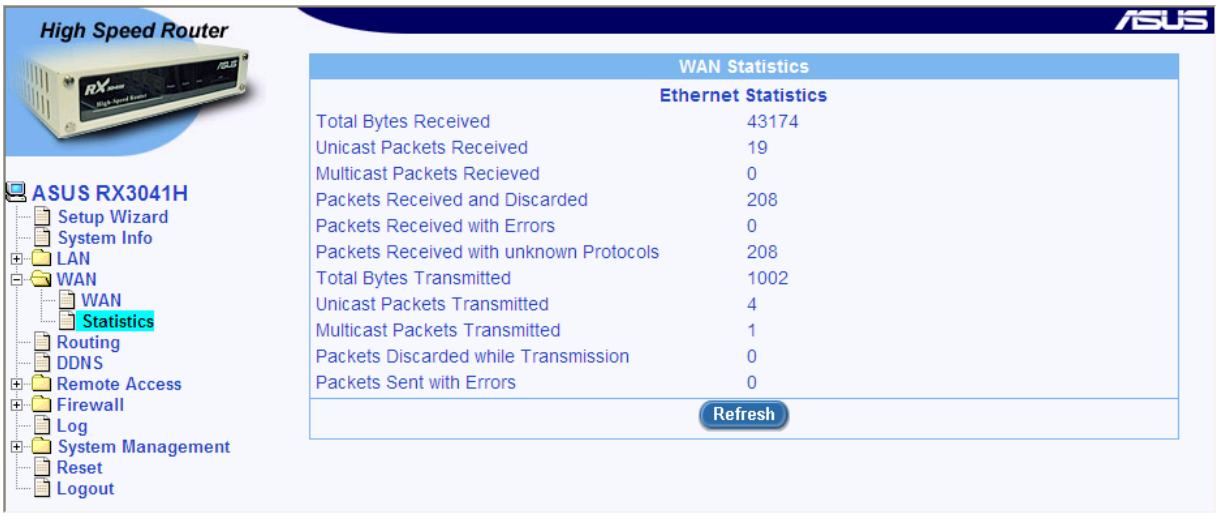


图 6.4. WAN 统计表页面

想要显示更新后的统计表，点选 Refresh 。

7 设定路径

您可利用设定管理器来为您的网际网络和网络数据通讯定义特别的路径。本章将向您说明基础的路由概念以及指导您创建路由路径。

注意：大多数的用户并不需要定义路径。

7.1 IP 路径总览

路由器遇到的核心挑战是：当它接收到有特定传输目标的资料时，何者为它应该把资料传递过去的下一个设备呢？当您定义了 IP 路径，您就提供了网际网络安全路由器做出决定的规则。

7.1.1 我需要定义 IP 路径吗?

大多数用户并不需要定义 IP 路径。在典型的小型家庭或办公室区域网内，现有的路径为您局域网络和网际网络安全路由器的计算机设立了预设的网关，也将为您所有的网际网络通信量提供最合适的路径。

- 在局域网络计算机内，预设的网关指导着所有的网际网络通信量流向路由器的局域网络埠。如果当您修改局域网络计算机的 TCP/IP 属性时您已经给它们指派了网关，或者如果无论它们何时接入网际网络，您都已经设定它们动态地从服务器接收信息，那么局域网络计算机就知道它们的预设网关了。（每个过程都已在“快速安装指南”的第二部分中说明，请参考。）
- 对于网际网络安全路由器自身，预设的网关已被定义来指导所有要出去的网际网络通信量流向网络供货商的路由器。无论设备何时协商与网际网络联机，预设的网关由网络供货商自动指派。（增加预设路径的过程在第**錯誤! 找不到參照來源。**节 **錯誤! 找不到參照來源。**中详细说明。）

如果您的家里需要两个或更多的网络或子网络，如果您与两个或更多的供货商联机，或者如果您与远程企业局域网络相联机，那么您可能需要定义路径。

7.2 使用 RIP（Routing Information Protocol）的动态路由

RIP（路由信息协议）让路由器之间产生路由信息交换。因此，路径会在不需要人类干预的情况下自动升級。我们推荐您在系统服务设定页面启动 RIP，如图 11.1 所示。

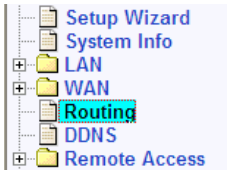
7.2.1 开启/关闭 RIP

请按照下列步骤来开启或关闭 RIP：

1. 在系统服务页面（如图 11.1 所示），根据您想开启或关闭 RIP，点选“Enable” 或 “Disable” 按钮。
2. 点选 Apply 来开启或关闭 RIP。

7.2.2 设定 RIP

请依照以下介绍来设定 RIP:



3. 请藉由点选 **Routing** 选单来开启路由设定页面。
4. 在系统服务设定页面中 (如图 11.1 所示)，依照您要开启或关闭 RIP 服务点选 “Enable” 或 “Disable” 按键。若您已进行设定，请略过此一步骤。

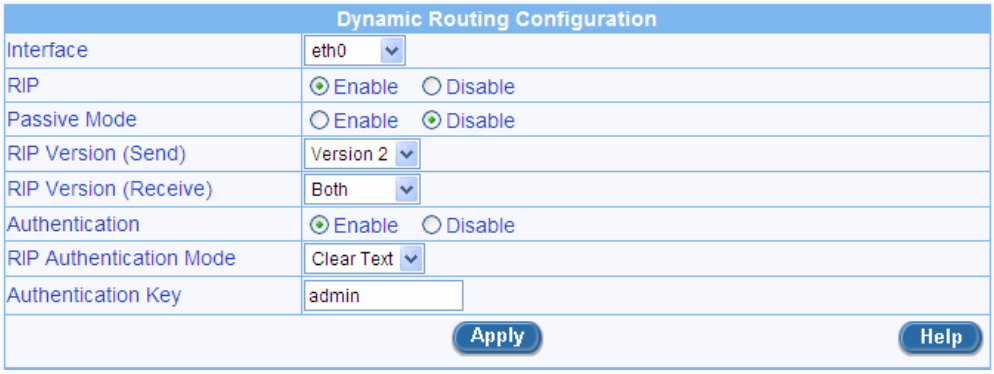


图 7.1. IP 路由列表页面 RIP 设定

5. 从下拉选单选择接口，透过这项设定路由资料便会被变更。
6. 藉由点选 “Enable” 或 “Disable” 按键来开启或关闭关于 RIP 设定的特定选项。
7. 藉由点选“Enable” or “Disable”按键来开启或关闭 RIP passive 模式。
8. 选择 RIP 版本来自下拉式列表中选择传送与接收信息。
9. 藉由点选“Enable” or “Disable” 按键来开启或关闭认证。若认证功能设定为开启，则您必需开启认证模式并输入认证金钥。
10. 若您想设定其它项目以支持路由信息变更，请重复步骤 **錯誤! 找不到參照來源。** 至 9 。
11. 点选 Apply 键来储存 RIP 设定。

7.3 静态路由

7.3.1 静态路径设定参数

下表定义了静态路径设定可供选择的参数。

表 7.1. 静态路由设定参数

选项	说明
目的地 IP 地址	指派目的地计算机或者整个目的地网络的 IP 地址。它亦能全被指派为零以显示此路径应被用来达到其它路径无定义的目的地（这就是創建预设网关的路径）。请注意，IP 目的地必须是网络 ID。预设路径使用的目的地 IP 为 0.0.0.0。请参考附录 A 关于网络 ID 的解释。
目的地网络屏蔽	指出哪部分目的地地址涉及网络，哪部分涉及网络中的计算机。请参考附录 A 关于网络屏蔽的解释。网络屏蔽预设的路径为 0.0.0.0.

选项	说明
网关 IP 地址	网关 IP 地址

7.3.2 增加静态路径

请按照下列步骤来增加静态路径至路径表：

1. 在静态路径设定页面内（如**錯誤! 找不到參照來源。**所示），输入相应选项的静态路由信息，例如目的地 IP 地址、目的地网络屏蔽以及网关 IP 地址。

   请参考表 7.1. 的详细说明。

   想为您的局域网络创建定义预设网关的路径，在目的地 IP 地址和目的地网络屏蔽选项中均输入 0.0.0.0 。

2. 点选 Add 增加新的路径。

7.3.3 删除静态路径

请按照下列步骤来删除路径表中的静态路径：

1. 在静态路径设定页面（如**錯誤! 找不到參照來源。**所示）的服务下拉表中选择路径，或者点选 静态路径表中要删除的路径图标。

2. 点选 Delete 以删除选择的路径。

小心

除非您明确了动作的目的，否则不要移除预设网关的路径。移除预设的路径将导致断开互联网。

7.3.4 查看静态路由表

所有开启 IP 功能的计算机和路由器都保存了用户通常接入的 IP 地址表。对于每个*目的地 IP 地址*，表中列出了资料采取的第一次跳跃的 IP 地址。此表又被称为设备的*路径表*。

想要查看路由器路径表，请点选路径菜单。静态路径表在静态路径页面的下半页，如**錯誤! 找不到參照來源。**所示：

静态路径表中的一行显示了每个现有的路径，路径中包含了目的地网络的 IP 地址、目的地网络的子网掩码以及网关 IP 地址。此表只显示用户增加的路径。

8 设定 DDNS

动态 DNS 是一种允许计算机使用相同网域名称的服务。此项服务甚至在 IP 地址时刻改变时也能提供。（在重启或当 ISP 的 DHCP 服务器重启 IP 租用）。无论 WAN 的 IP 地址是否改变，路由器都联机至动态 DNS 服务器。它支持创建网页服务，例如使用网域名称替代 IP 地址的网页服务器、FTP 服务器。动态 DNS 支持 DDNS 客户端的下列规格：

- 当外部接口出现时，刷新 DNS 记录（增加的）
- 促使 DNS 刷新

动态 DNS 支持两种模式，即 RFC-2136 DDNS 客户端 和 HTTP DDNS 客户端。

RFC-2136 DDNS 客户端

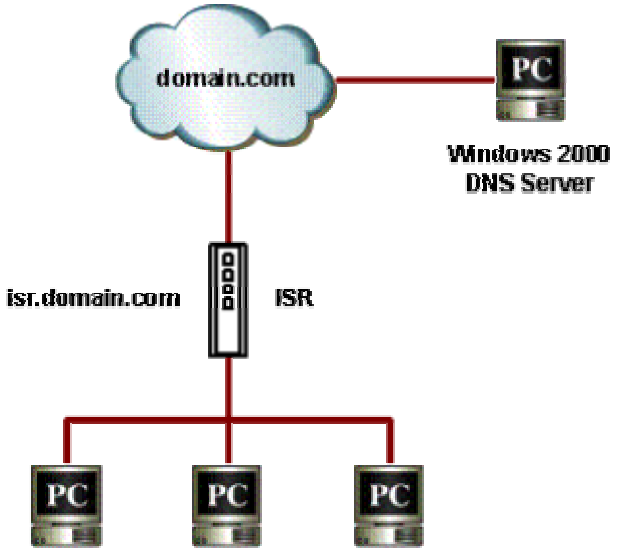


图 8.1. RFC-2136 DDNS 网络拨号

任何外部接口状况的改变都会给 DNS 服务器送出 DDNS 的升級信息。当联机 Primary DNS 服务器的举动失败时，路由器会升級 Secondary DNS 服务器。当管理员迫使 DNS 升級时，升級信息被传送到所有活动的外部服务器。

HTTP 动态 DNS 客户端

HTTP DDNS 客户端利用流行的 DDNS 服务提供商提供的机制来动态地升級 DNS 记录。既然这样，那么服务提供商就可以升級 DNS 中的 DNS 记录了。路由器运用 HTTP 来促进此种升級。

路由器支持下列服务供货商的 HTTP DDNS 升級：

- www.dyndns.org
- www.zoneedit.com
- www.dns-tokyo.jp

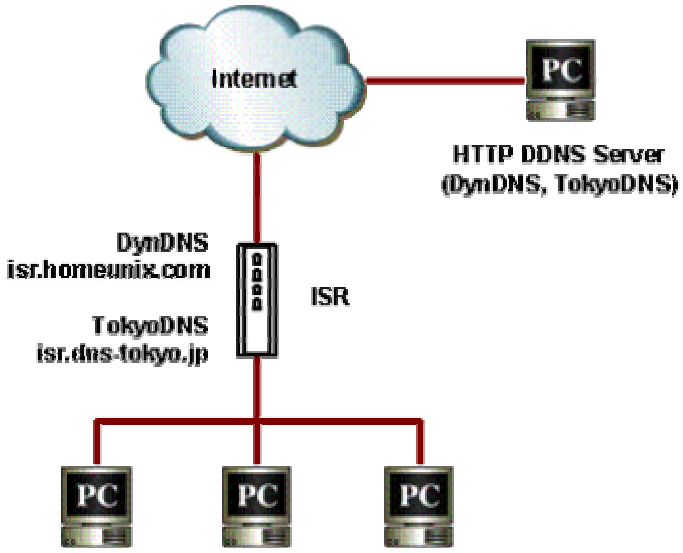


图 8.2. HTTP DDNS 网络拨号

无论已设定的 DDNS 接口的 IP 地址何时更改，DDNS 升級都被送到指派的 DDNS 服务提供商。网际网络安全路由器应该设定好从 DDNS 服务提供商那里获得的 DDNS Username 和 Password。

8.1 DDNS 设定参数

表 8.1 说明了 DDNS 服务的设定参数：

表 8.1. DDNS 设定参数

选项	说明
DDNS 状态	
Enable	点选此按钮来开启DDNS服务
Disable	点选此按钮来关闭DDNS服务
DDNS 类型 – 选择DDNS 服务类型: HTTP 或 RFC-2136 DDNS	
HTTP DDNS	如需要HTTP DDNS，点选此按钮。
RFC-2136 DDNS	如需要RFC-2136 DDNS ，点选此按钮。
DNS Zone Name 在本选项中输入网络服务供货商提供的已注册的网域名称。（注意：路由器的主机名称必须在系统信息设立页面正确地设定好。）例如，如果路由器主机名称为“host1”，DNS Zone 名称为“yourdomain.com”，网域名称的全称（FQDN）为 “host1.yourdomain.com”。	
RFC-2136 DDNS 特殊设定	
Primary/Secondary DNS 服务器 [仅在RFC-2136 DDNS] 在本选项中输入Primary 和 Secondary DNS 服务器的IP地址。这个地址从WAN设定页面得到。除非您想改变WAN的设定，否则请保持不变。	

选项	说明
HTTP DDNS 特殊设定	
DDNS 服务 [仅对 HTTP DDNS]	
dyndns	请访问 http://www.dyndns.org 以获得更多信息。
zoneedit	请访问 http://www.zoneedit.com 以获得更多信息。
dyn-tokyo	请访问 http://www.dns-tokyo.jp 以获得更多信息。
DDNS Username [仅对HTTP DDNS] 在本选项中输入DDNS服务提供商提供的Username。	
DDNS Password [仅对HTTP DDNS] 在本选项中输入DDNS服务提供商提供的Password。	

8.2 设定 RFC-2136 DDNS 客户端

图 8.3. RFC-2136 DDNS 设定页面

请按照下列步骤来设定 RFC-2136 DDNS：

1. 首先您需要要求系统管理员在 DNS 服务器上开启 DNS 动态升級功能。如果您正在运行 Windows 2000/XP/2003 DNS 服务器，请参考 Microsoft 基础知识文章 “*Q317590: Configure DNS Dynamic Update in Windows 2000*”。
2. 请确认您拥有为路由器设定的主机名称；若没有，请至**系统信息设定**页面（系统管理➔系统认证）进行设定。
3. 打开 DDNS 设定页面（参考第**錯誤! 找不到參照來源。**节 **錯誤! 找不到參照來源。**）。
4. 在 DDNS 设定页面，选择“Enable” 的 DDNS 状态和 “RFC-2136 DDNS” 的 DDNS 类型。RFC-2136 DDNS 设定页面如图 8.3 所示。
5. 在 DNS Zone Name 选项栏输入网域名称。
6. 无须改变 Primary 和 Secondary DNS 服务器的 IP 地址。因为这个地址从 WAN 设定页面得到。除非您想改变 WAN 的设定，否则请保留不变。
7. 点选 Apply 按钮向 Primary DNS 和 Secondary DNS 选项指派的 DNS 服务器发送升級 DNS 的要求。注意，无论 WAN 埠状况是否改变，升級 DNS 的要求同样也会自动送给 DNS 服务器 。

8.3 设定 HTTP DDNS 客户端

图 8.4. HTTP DDNS 设定页面

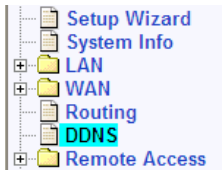
请按照下列步骤来设定 HTTP DDNS：

1. 首先，您应该已经向 DDNS 服务供货商注册了网域名称。如果您还没有注册，请访问 www.dns-tokyo.jp 或 www.dyndns.org 以获得更多信息。
2. 请确认您拥有为路由器设定的主机名称；若没有，请至**系统信息设定**页面（系统管理➔系统认证）进行设定。
3. 打开 DDNS 设定页面（参考第**錯誤! 找不到參照來源。**节 **錯誤! 找不到參照來源。**）。
4. 在 DDNS 设定页面，选择“Enable” 的 DDNS 状态和 “HTTP DDNS” 的 DDNS 类型。HTTP DDNS 设定页面如图 8.4 所示。
5. 在 DNS Zone Name 选项栏输入网域名称。
6. 从 DDNS 服务下拉表中选择 DDNS 服务。
7. 输入 DDNS 服务供货商提供的 Username 和 Password。
8. 点选 Apply 按钮向 DDNS 服务供货商发送升級 DNS 的要求。注意，无论 WAN 埠状况是否改变，升級 DNS 的要求同样也会自动送给 DDNS 服务供货商。

8.4 设定近端主机列表

此为供路由器标示主机名称与其 IP 地址的近端主机列表。本列表可作为您局域网络中的服务器部署之用。举例来说，您可以为您的服务器在这组列表中創建一组主机登录，让局域网络中的主机可以藉由使用主机名称，像是 telnet myServer.myCompany.com.来存取服务器的资料。

8.4.1.1 新增一组主机登录



请依照以下介绍来新增一组主机登录:

9. 藉由点选 **DDNS** 选单来开启 DDNS 设定页面。
10. 自下拉列表中选择 “**Add New**” 。
11. 在对应的字段输入主机名称与对应的 IP 地址。图 8.5 显示使用登录在主机列表中新增一组新主机来标示主机名称，myServer.myCompany.com 与一组 IP 地址 192.168.1.20 。

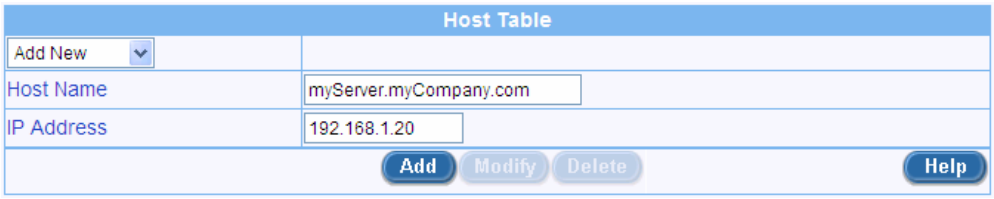


图 8.5. 主机列表设定

12. 点选 Add 键来創建一组新的主机登录。新的主机登录其后会显示在 DDNS 设定页面下方的主机列表中。

图 8.6. 主机列表

8.4.1.2 更改主机列表中的登录

请依照下列介绍来更正主机列表中的登录:

13. 藉由点选 **DDNS** 选单来开启 DDNS 设定页面。
14. 点选主机列表登录中的 图标来从下拉式主机列表中更正主机列表或选择主机列表登录。
15. 接下来您可以在主机名称与 IP 地址进行所想要加以变更的设定。
16. 点选 Modify 键以储存变更。主机列表中新的设定值会显示于 DDNS 设定页面下方的主机列表中。

8.4.1.3 删除主机列表登录

如欲删除主机列表登录，请依照下列介绍的指示点选 图标来进行删除:

17. 藉由点选 **DDNS** 选单来开启 DDNS 设定页面。
18. C 在主机列表中点选 图标以便从下拉式主机列表中选择要加以删除的主机登录。
19. 点选 Delete 键来删除登录。请注意！被删除的主机登录将会自 DDNS 设定页面下方的主机列表中移除。

8.4.1.4 检视主机列表

如欲检视既有的主机列表，您只要藉由点选 **DDNS** 选单来开启 DDNS 设定页面即可。

9 设定防火墙/NAT

网际网络安全路由器提供内建的防火墙/NAT 功能，在提供网际网络访问共享的同时，保护您的系统免受拒绝服务（DoS）的攻击，以及免于对局域网络的其它类型的恶意访问。您亦能指定如何监视攻击企图，以及谁应该被自动通报。

本章说明了如何創建/修改/删除访问控制列表 ACL（Access Control List）规则以控制流经网络的资料。R 您将使用防火墙设定页面来：

- 創建、修改、删除以及检查入站/出站的 ACL 规则。
- 創建、修改及删除预先定义的服务、IP 地址池、NAT 地址池、应用程序过滤以及入站/出站 ACL 设定的时间范围。
- 检查防火墙统计表。

注意: 当您定义 ACL 规则时，您指导路由器来检查封包接收到的每个资料，判断它是否符合规则规定标准的要求。*标准包括它所支持的网络或网际网络协议、它传递的方向（例如，从局域网络到网际网络，反之亦然）、来源计算机的 IP 地址、目的地 IP 地址，以及封包资料的其它特性。*

如果封包符合规则标准的要求，那么根据规则中规定的的动作，封包会被接收（促使它流向目的地），或拒绝（摒弃）。

9.1 防火墙概述

9.1.1 静态封包检查

静态封包检查网际网络安全路由器中的引擎保存的一个状态工作台，这个工作台被用来记录所有流经防火墙的封包的联机状态。如果属于已創建的联机的封包的状态与静态封包检查引擎维护的状态相吻合，防火墙将开“口”允许封包透过。否则，封包会被拒绝透过。这个“口”在联机过程终止时将被关闭。静态封包检查不需要任何设定；当防火墙启动时它自动开启。请参看第**錯誤! 找不到參照來源。**节**錯誤! 找不到參照來源。**以开启或关闭路由器防火墙服务。

9.1.2 拒绝服务（DoS，Denial of Service）保护

拒绝服务的保护和状态封包检查共同承担您网络的第一道防线。两者都不需要进行任何设定，当路由器防火墙启动时它自动开启。防火墙默认值在出厂时就已设置好。请参看第**錯誤! 找不到參照來源。**节 **錯誤! 找不到參照來源。**以开启或关闭路由器防火墙服务。

9.1.3 防火墙及访问控制列表 （ACL，Access Control List）

9.1.3.1 ACL 优先级规则

所有的 ACL 规则都有指派的规则 ID – 规则 ID 越小，优先权越大。防火墙从封包中抽取重要信息，然后透过检视重要信息与 ACL 规则表是否吻合，再摒弃或传送封包，防火墙透过此举监视着流通的信息。请注意，ACL 规则检查从最小的规则 ID 开始，直到出现了两者匹配的信息或所有的 ACL 规则都已检查完毕。如果二者之间并无匹配，那么封包被摒弃；另外，基于匹配的 ACL 规则定义的举动，封包会被摒弃，或被传送。

9.1.3.2 追踪联机状态

防火墙的静态检查引擎持续追踪网络联机的状态进展。透过在状态表中存储所有的联机信息，网际网络安全路由器能快速判断流经防火墙的封包是否属于已創建的联机形式。若是，封包就直接流经防火墙而无须透过 ACL 规则评判。

例如，ACL 规则允许出站的从 192.168.1.1 到 192.168.2.1 的 ICMP 封包。当 192.168.1.1 送出 ICMP 请求至 192.168.2.1 时，192.168.2.1 将送出 ICMP 响应给 192.168.1.1。在网际网络安全路由器中，您无须創建另外的 ACL 规则，因为静态封包检查引擎将记住联机状况，并允许 ICMP 响应透过防火墙。

9.1.4 预设的 ACL 规则

网际网络安全路由器支持三种预设的访问规则：

- 入站访问规则：目的为控制入站区域网计算机的访问。
- 出站访问规则：目的为控制出站局域网络主机至外部网络的访问。
- 自身访问规则：目的为控制对路由器自身的访问。

预设的入站访问规则

无已设定的预设入站访问规则。也就是说，所有从外部主机到内部主机的流通均被拒绝。

预设的出站访问规则

预设的出站访问规则允许所有来自局域网络的信息流通到外部使用 NAT 的网络。

WARNING

您无需把预设的 ACL 规则从 ACL 规则表中移除！創建优先权高于预设 ACL 的规则更佳。

9.2 NAT 总览

网络地址转换允许使用单一设备，例如网际网络安全路由器，扮演网际网络（公共网络）与本地网络之间的代理人。这意味着 NAT 的 IP 地址对外能代表整个计算机群体。NAT 是一种在大型网络中保存已注册的 IP 地址和使 IP 地址管理简单化的机制。因为 IP 地址的转换，NAT 还把您真正的 IP 地址从别人眼前隐藏起来，并提供某种程度的本地网络保护。

NAT 模式支持静态 NAT、动态 NAT、NAPT、反向静态 NAT 以及反向 NAPT。

9.2.1 静态 （一对一）NAT

静态 NAT 对应了从内部主机地址到有效全球网际网络地址（一对一）。而每个封包的 IP 地址都会被直接转换成为一个有效的全球网际网络地址。图 9.1 阐明了四个私人 IP 地址与四个有效全球 IP 地址之间的映像关系。请注意，这种映像是静态的，例如除非管理员手动更改，映像并不随着时间而改变。这意味着主机将对其所有的出站信息一直使用相同的有效全球 IP 地址。

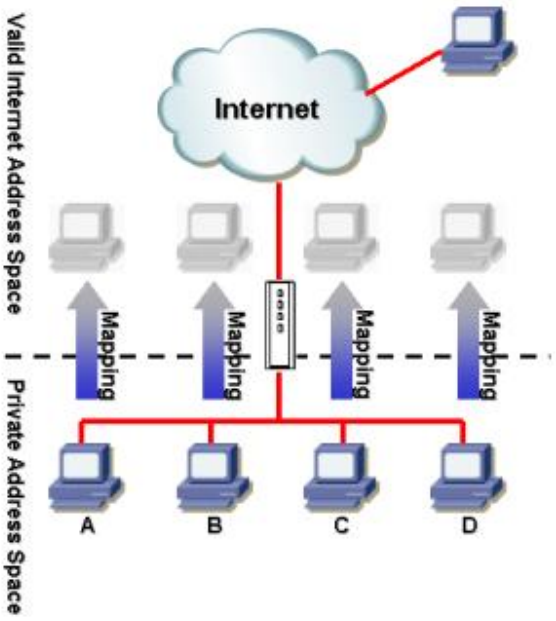


图 9.1 静态 NAT – 对应从四个私人 IP 地址到四个有效全球 IP 地址

9.2.2 动态 NAT

动态 NAT 动态地对应从内部主机到有效全球网际网络地址（m 到 n）。映像常常包含一些内部 IP 地址池（m）和有效全球网际网络 IP 地址（n），且 m 常常大于 n。每个内部 IP 地址都在"先来先服务"的基础上与一个外部 IP 地址相连。图 9.2 显示，PC B、C 和 D 都分别与一个有效全球 IP 地址联机，而 PC A 并不与任何有效全球 IP 地址联机。如果 PC A 想要接入网际网络，它必须等到一个有效全球 IP 地址可用时才行。例如，在图 9.3 中，PC B 必须先从网际网络断开，然后 PC A 才能接入网际网络。

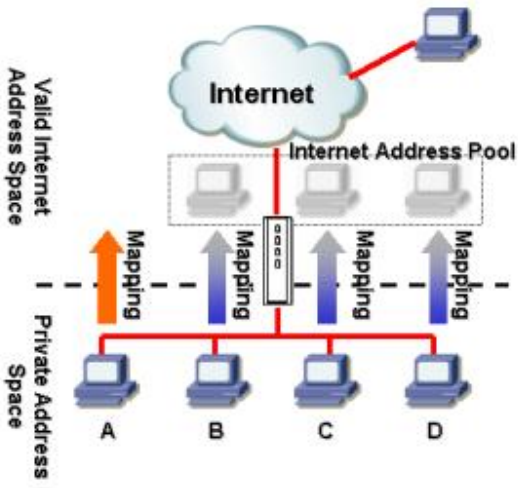


图 9.2 动态 NAT – 从四个私人 IP 地址到三个有效 IP 地址

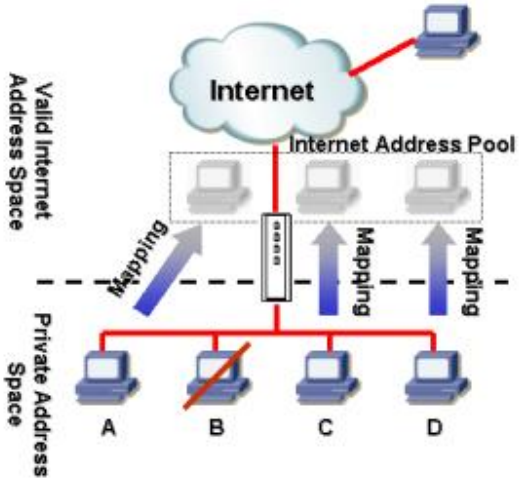


图 9.3 动态 NAT – PC-A 能在 PC-B 断开后得到 NAT 联机

9.2.3 NAPT （Network Address and Port Translation，网络地址和埠转换）或 PAT （Port Address Translation，端口地址转换）

这个特性对应了许多从内部主机到一个有效全球 IP 地址。映像包含被用来转换的一些埠。每个封包都随着有效全球网际网络地址转换，而埠数目则随着一个未用的网络端口转换。图 9.4 显示，所有的本地网络主机都透过网络端口地址池对应外部有效的 IP 地址和不同的端口号来达到连接网际网络的目的。

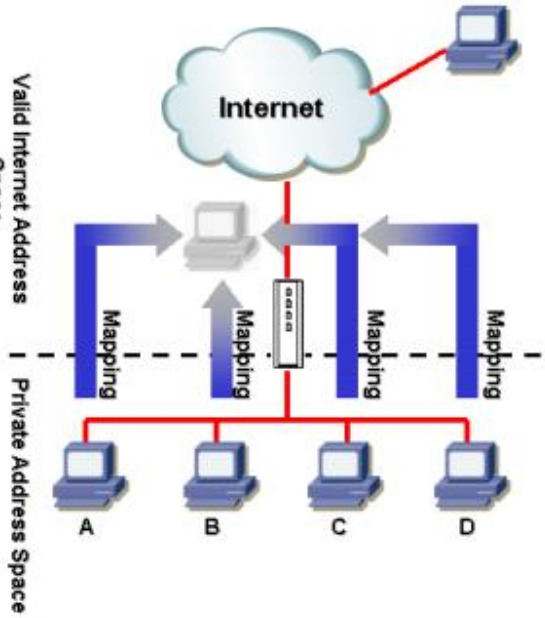


图 9.4 NAPT – 对应从任何内部计算机到单一全球 IP 地址

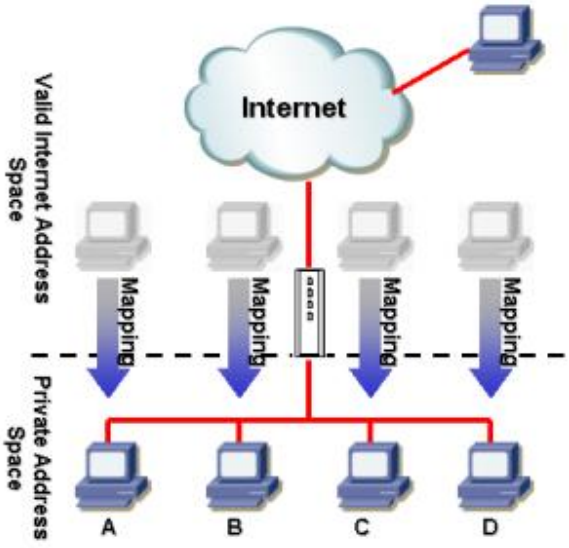


图 9.5 反向 NAT – 对应一个全球 IP 地址到一台内部计算机

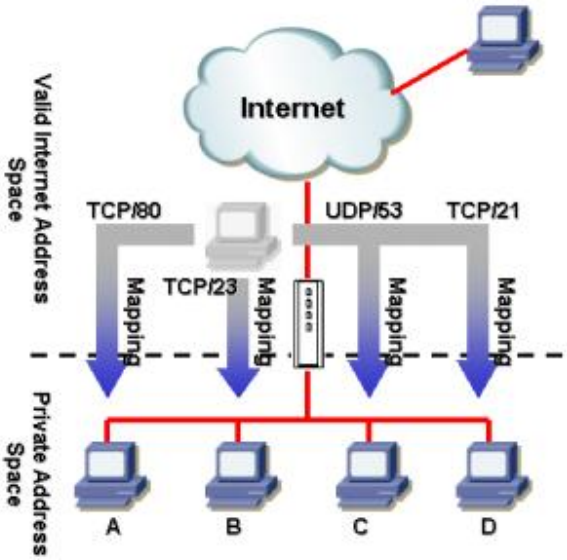


图 9.6 反向 NAPT – 以协议、埠号或 IP 地址为基础转送封包到内部主机

9.2.4 反向静态 NAT

反向静态 NAT 为入站信息对应了从有效全球 IP 地址到内部主机地址映像。所有流向有效全球 IP 地址的封包都传递到网际网络地址上。这在当内部主机提供应用服务时十分有用。图 9.5 显示了从四个有效全球 IP 地址到四个内部网络主机的映像，而且每个都可用作为入站信息的主机服务，例如 FTP 服务器。

9.2.5 反向 NAPT / 虚拟服务器

反向 NAPT 又被称为入站映像、端口对应或虚拟服务器。任何传送到路由器的封包都能被传递到基于协议、埠号和/或在 ACL 规则内指派 IP 地址的内部主机上。这在当不同的内部主机提供多种服务时十分有用。图 9.6 显示了网页服务器（TCP/80）连在 PC A 上，远程网络服务器（TCP/23）在 PC B 上，DNS 服务器（UDP/53）在 PC C 上，FTP 服务器（TCP/21）在 PC D 上。这意味着这四台服务器入站的信息将被直接传导至各自的服务主机。

9.3 ACL 规则参数设定

表 9.2 叙述ACL规则中可以进行的参数设定项。

表 9.1. ACL 规则参数设定

字段	叙述
ID	
Add New	点选此项目以新增一组 ACL 规则
Rule Number	从下拉式列表中选择一项规则，并修改其属性
Action	
Allow	选择此按键以设定像是 **allow** 规则的设定 当符合上述设定之规则的封包将被允许通过
Deny	选择此按键以设定像是 **deny** 规则的设定 当符合上述设定之规则的封包将被阻挡无法通过
Move to 本选项可让您设定本规则的优先权。RX3041H 防火墙是以此一规则的优先权来决定是否让封包通过。您可藉由在规则列表中指定一特定数字来决定规则的优先权。	
1 (First)	本数字代表最高的优先权
Other numbers	选择要指定给其它规则的优先级号码
Source IP 本选项可以让您设定套用该规则的 **来源网络** 。使用下拉式选单来选择下列选项：	
Any	本选项可以让您套用本规则在来源网络中的所有计算机，像是那些网际网络上符合入端口ACL规则者或是局域网络中符合出端口ACL规则者。
IP Address	本选项可让您为套用本规则者指定一组 IP 地址
IP Address	指定适当的网络地址
Subnet	本项目可让您涵盖所有在同一IP子网络内的计算机。当本项目被选定，则以下字段便可以加以输入:

字段	叙述
Address	输入适当的 IP 地址
Mask	输入对应的子网掩码
Range	本项目可让您涵盖所有套用此规则的 IP 地址。当本项目被选定，则以下字段便可以加以输入:
Begin	输入起始的 IP 地址范围
End	输入中止的 IP 地址范围
IP Pool	本项目可以让您以此一规则与预设的 IP 地址池产生关连。您可从 IP地址池下拉式选单列表中选取 IP 地址池。
Destination IP 本项目可让您选择套用此规则的 **目的地网络**。 请使用下拉式选单来选择以下的选项:	
Any	本项目可让您将此规则套用到处在目的地网络下的所有计算机，像是那些局域网络中符合 入端口 ACL 规则的计算机，与网际网络中符合出端口 ACL 规则的计算机。
IP Address, Subnet, Range and IP Pool	请选择这些选项中的任一选项并输入如前述 **Source IP** 一节中所提到的相关细节叙述。
Source Port 本项目可让您设定欲套用此一规则的来源连接端口。请使用下拉式选单来选择以下的选项:	
Any	若您想以任一来源端口号来将此规则套用到应用程序上，则请选择此项目
Single	本项目可让您用特定的来源埠号来套用此规则
Port Number	输入来源埠埠号
Range	若您要将本规则用此连接端口范围套用到应用程序中，请选择本项目。当本项目被选择，则以下的字段将会变成可以进行输入的。
Begin	输入起始连接埠号的范围
End	输入中止连接埠号的范围
目的地连接埠 本选项可让您设定欲套用本规则的目的地连接端口。请使用下拉式来选择以下任一选项：	
Any	若您想要将此一规则利用任一目的地连接埠埠号来套用到所有的应用程序，则请选择本项。
Single, Range	选择任一项并在 **Source Port** 字段输入细节叙述
Service	请在本项目中选择任何的预设服务(自下拉选单中选取)而非自目的地连接埠选取。以下则为服务之范例: BATTLE-NET, PC-ANYWHERE, FINGER, DIABLO-II, L2TP, H323GK, CUSEEME, MSN-ZONE, ILS, ICQ_2002, ICQ_2000, MSN, AOL, RPC, RTSP7070, RTSP554, QUAKE, N2P, PPTP, MSG2, MSG1, IRC, IKE, H323, IMAP4, HTTPS, DNS, SNMP, NNTP, POP3, SMTP, HTTP, FTP, TELNET.

字段	叙述
	Note: 本服务是通讯协议与连接端口号的结合。这些项目只有当您在 “Firewall Service” 设定页面加以新增后才会出现。
Protocol 本项目可让您从下拉式选单中选择通讯协议类型。这边可供选择的设定有 All, TCP, UDP, ICMP, AH 与 ESP。请注意！若您选择 “service” 作为目的连接端口，则本选项将无法进行设定。	
NAT 本项目可以让您选择 NAT 传输的类型。	
None	若您不想要在此 ACL 规则中使用 NAT，则请选择本项目。
IP Address	**作为入端口 ACL 规则:** 若您想要外来传输可被侦测，请选择本项以指定计算机的 IP 地址 (通常是您局域网络中的服务器) 。请注意！本项目又被称作反向 NAPT 或是虚拟服务器。 **作为出端口 ACL 规则:** 若您想使用出埠传输，则请选择本项目。请注意！本项目又被称作 NAPT 或是 Overload。
NAT Pool	选择本项目来与预设的 NAT 地址池創建关连。**作为入端口 ACL 规则，** 只有反向静态 NAT 与反向 NAPT 地址池可被使用。**作为出端口 ACL 规则，** 只有静态、动态与 Overload的 NAT 地址池可被使用。
Interface (Outbound ACL only)	**本项目仅可用于出端口 ACL 规则。** 选择本选项以使用广域网络WAN外部 IP 地址做为出端口传输之用。请注意！广域网络IP必需先被设定方可设定本选项。本项目共有三个选项可供选择：eth0, pppoe0 and pppoe1。若您的广域网络WAN使用固定或动态IP 则请选择 eth0 ;若您使用PPPoE 方式联机，则请选择pppoe0，而若是使用 PPPoE1接口，则请选择 pppoe1。
先Time Ranges 选择预设的时间范围，在此一范围中规则是生效的。选择 “Always” 可让规则一直生效无时间限制	
Application Filtering 本项目可让您从下拉选单中选择预设的 FTP, HTTP, RPC 与/或 SMTP 应用程序过滤功能	
Log 点选 “Enable” 或 “Disable” 按键以开启或关闭登入此一 ACL 规则者	

9.4 设定入站 ACL 规则

在入站ACL设定页面創建ACL规则，如图 9.7所示，您可控制对您局域网络计算机的访问（允许或拒绝）。

本设定页面的选项有：

- 增加规则，并设定参数
- 修改现有的规则
- 删除现有的规则
- 检查设定的 ACL 规则

图 9.7. 入站 ACL 设定页面

9.4.1 入站 ACL 规则设定参数

表 9.2 说明了防火墙入站ACL规则可供选择的设定参数。

表 9.2. 入站 ACL 规则设定参数

选项	说明
ID	
Add New	点选本选项以增加新的“基本”防火墙规则。
Rule Number	从列表中选择规则，修改属性。
Action	
Allow	按此按钮以设定**允许**的规则。 当限制为防火墙时，此规则将允许匹配的封包透过。
Deny	按此按钮以设定**拒绝**的规则。 当限制为防火墙时，此规则将**不**允许匹配的封包透过。
Move to 本选项允许您设立规则的优先级。路由器防火墙在优先级规则基础上作用于封包。请以它在规则表的位置的指定序号为基础设立优先级：	
1 (First)	此序号表示最高优先权：
Other numbers	选择其它的数字以说明您想要指定的优先级。
Source IP 本选项允许您设定规则必须应用的**来源网络**。请从下表中选择选项：	
Any	本选项允许您将本规则应用到所有来源网络的计算机上，例如那些接入网际网络的计算机。

选项	说明
IP Address	本选项允许您指定规则应用的IP地址。
IP Address	指定合适的网络地址。
Subnet	本选项允许将所有联机到同一IP子网掩码的计算机都包括进来。当选择了本选项时，下列栏目可选：
Address	输入合适的IP地址。
Mask	输入相应的子网掩码。
Range	本选项允许将范围内的IP地址都包括进应用规则。当选择了本选项时，下列栏目可选：
Begin	输入范围起始的IP地址。
End	输入范围结束的IP地址。
IP 地址池	本选项允许您将预先设定好的IP地址池与规则相连结。您可在下表中选择IP地址池。
Destination IP 本选项允许您设定能应用本规则的**目的地网络**。请在下表的选项中选择：	
Any	本选项允许您将规则应用到本地网络所有的计算机上。
IP Address, Subnet, Range and IP 地址池	请按照上文**Source IP**部分的说明选择任一选项，并输入详细信息。
Source Port 本选项允许您设定本规则得以应用的来源埠。请在下表的选项中选择：	
Any	如果您希望将本规则应用到所有任意来源端口号的应用程序上，请选择本选项。
Single	本选项允许您将本规则应用到某一指定来源端口号的应用程序上。
Port Number	输入来源埠号
Range	如果您希望将本规则应用到本埠范围的应用程序上，请选择本选项。当选择了本选项时，下列栏目可选：
Begin	输入范围的起始埠号
End	输入范围的结束埠号
Destination Port 本选项允许您设定能应用本规则的**目标端口**。请在下表的选项中选择：	
Any	本选项允许您将规则应用到所有任意来源端口号的应用程序上。
Single, Range	请按照上文**Source Port**部分的说明选择任一选项，并输入详细信息。
Service	本选项允许您选择任何预先设定好的服务（请从下表中选择），而不是目

选项	说明
	标端口。下面列出了一些服务选项： BATTLE-NET, PC-ANYWHERE, FINGER, DIABLO-II, L2TP, H323GK, CUSEEME, MSN-ZONE, ILS, ICQ_2002, ICQ_2000, MSN, AOL, RPC, RTSP7070, RTSP554, QUAKE, N2P, PPTP, MSG2, MSG1, IRC, IKE, H323, IMAP4, HTTPS, DNS, SNMP, NNTP, POP3, SMTP, HTTP, FTP, TELNET. **注意：**服务是协议与埠号的结合。它们将在您把它们增加进设定页面的“Firewall Service”后出现。
Protocol 本选项允许您从下表中选择协议的类型。可供选择的设定为All, TCP, UDP, ICMP, AH 和 ESP。注意，如果您为目标端口选择 “service”，本选项将不可用。	
NAT 本选项允许您选择入站信息NAT的类型。	
None	如果您不想在入站ACL规则里启用NAT，请选择此选项。
IP Address	选择本选项以指定您期望入站信息流向的计算机（通常是局域网络中的服务器）的IP地址。注意，此选项被称为反向NAPT 或虚拟服务器。
NAT 地址池	选择本选项来指定预先设定好的NAT地址池接入规则。注意，只有反向静态NAT和反向NAPT域才能用来联机入站ACL的规则 。
Time Ranges 选择预先设定好的规则起作用的时间范围。选择“Always”来使规则一直起作用。	
Application Filtering 本选项允许您选择下拉表中预先设定好的FTP, HTTP, RPC 和/或 SMTP 应用程序过滤器。	
Log 点选 “Enable” 或 “Disable” 按钮以开启或关闭ACL规则logging功能。	

图 9.8. 入站 ACL 设定实例

9.4.2 增加入站 ACL 规则

想要增加入站 ACL 规则，请参考下列步骤：

1. 打开入站 ACL 规则设定页面（请参考第**錯誤! 找不到參照來源。**节 **錯誤! 找不到參照來源。**）。
2. 在“**ID**”表中选择 “**Add New**” 。
3. 从“**Action**”表中设定期望的动作（允许或拒绝）。
4. 改动任一或所有下列栏目：source/destination IP, source/destination port, protocol, port mapping, time ranges, application filtering, log。请参考表 9.2 中对这些栏目的解释。
5. 透过选择 “**Move to**” 表中的序号来为规则指定优先级。注意，序号 1 表示优先劝最高。防火墙将按照优先劝的高低进行检查。

6. 点选 Add 按钮以創建新的 ACL 规则。新的 ACL 规则同时在入站 ACL 设定页面下半页的“入站访问控制表”中出现。

图 9.8 说明了如何創建接受入站 HTTP （例如，网页服务器） 服务的规则。 此规则允许入站 HTTP 信息流向 IP 地址 192.168.1.28 的主机。

9.4.3 修改入站 ACL 规则

想要修改入站 ACL 规则，请参考下列步骤：

1. 打开入站 ACL 规则设定页面（请参考第 **錯誤! 找不到參照來源。** 节 **錯誤! 找不到參照來源。**）。
2. 点选 图标，修改入站 ACL 表的规则或从“**ID**”表中选择规则序号。
3. 改动任一或所有下列栏目：action, source/destination IP, source/destination port, protocol, port mapping, time ranges, application filtering, log。请参看表 9.2 中对这些栏目的解释。
4. 点选 Add 按钮以修改 ACL 规则。新的 ACL 规则设定同时在入站 ACL 设定页面下半页的“入站访问控制表”中出现。

9.4.4 删除入站 ACL 规则

想要删除入站 ACL 规则，请点选待删规则前面的图标，并参考下列步骤：

1. 打开入站 ACL 规则设定页面（请参考第**錯誤! 找不到參照來源。** 节 **錯誤! 找不到參照來源。**）。
2. 点选 图标，删除待删的入站 ACL 表的规则或从“**ID**”表中选择规则序号。
3. 点选 Delete 按钮以删除 ACL 规则。新的 ACL 规则设定同时在入站 ACL 设定页面下半页的“入站访问控制表”中出现。

9.4.5 入站 ACL 规则展示

想要参看现有的入站 ACL 规则，您只需打开入站 ACL 规则设定页面，如第***錯誤! 找不到參照來源。*** 节 ***錯誤! 找不到參照來源。*** 所示。

9.5 设定出站 ACL 规则

在出站ACL设定页面創建ACL规则，如图 9.9所示，您可控制对您局域网络计算机对网际网络或外部网络的访问（允许或拒绝）。

本设定页面的选项有：

- 增加规则，并设定参数
- 修改现有的规则
- 删除现有的规则
- 检查设定的 ACL 规则

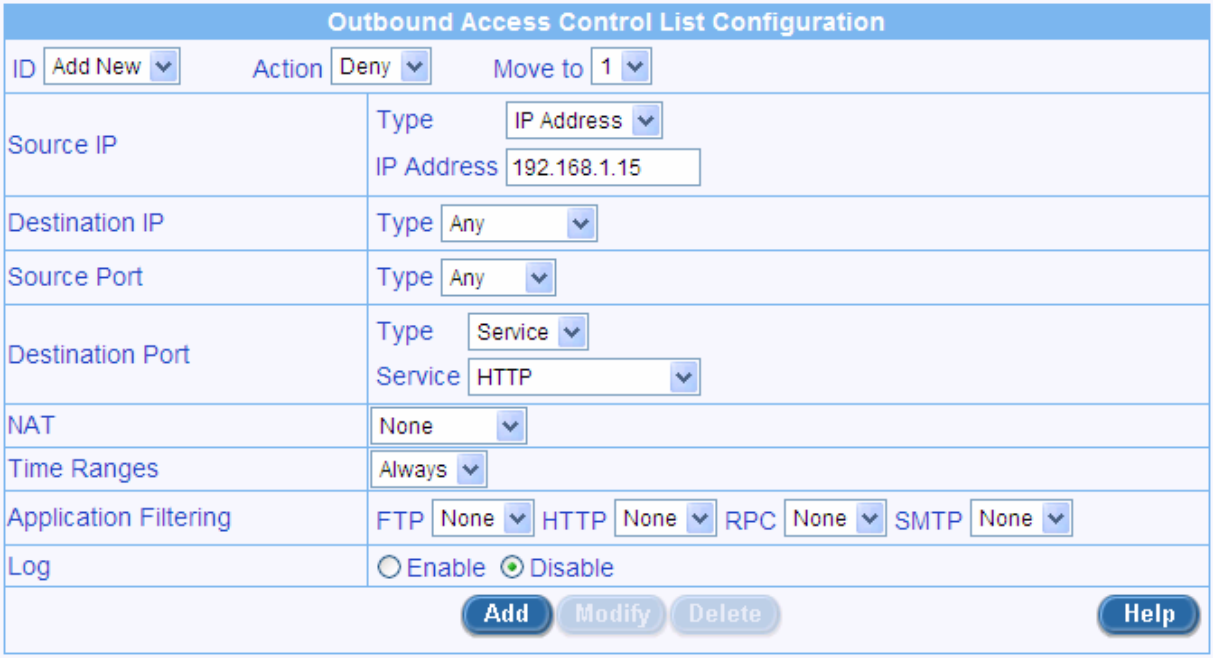


图 9.9. 出站 ACL 设定页面

9.5.1 出站 ACL 规则设定参数

表 9.3 说明了防火墙出站ACL规则可供选择的设定参数。

表 9.3. 出站 ACL 规则设定参数

选项	说明
ID	
Add New	点选本选项以增加新的“基本”防火墙规则。
Rule Number	从列表中选择规则，修改属性。
Action	
Allow	按此按钮以设定**允许**的规则。 当限制为防火墙时，此规则将允许匹配的封包透过。
Deny	按此按钮以设定**拒绝**的规则。 当限制为防火墙时，此规则将**不**允许匹配的封包透过。
Move to 本选项允许您设立规则的优先级。路由器防火墙在优先级规则基础上作用于封包。请以它在规则表的位置的指定序号为基础设立优先级：	
1 (First)	此序号表示最高优先权：
Other numbers	选择其它的数字以说明您想要指定的优先级。

选项	说明
Source IP 本选项允许您设定规则必须应用的**来源网络**。请从下表中选择选项：	
Any	本选项允许您将本规则应用到所有来源网络的计算机上，例如那些接入网际网络的计算机。
IP Address	本选项允许您指定规则应用的IP地址。
IP Address	指定合适的网络地址。
Subnet	本专案允许将所有联机到同一IP子网掩码的计算机都包括进来。当选择了本选项时，下列栏目可选：
Address	输入合适的IP地址。
Mask	输入相应的子网掩码。
Range	本选项允许将范围内的IP地址都包括进应用规则。当选择了本选项时，下列栏目可选：
Begin	输入范围起始的IP地址。
End	输入范围起始的IP地址。
IP 地址池	本选项允许您将预先设定好的IP地址池与规则相连结。您可在下表中选择IP地址池。
Destination IP 本选项允许您设定能应用本规则的**目的地网络**。请在下表的选项中选择：	
Any	本选项允许您将规则应用到本地网络所有的计算机上。
IP Address, Subnet, Range and IP 地址池	请按照上文**Source IP**部分的说明选择任一选项，并输入详细信息。
Source Port 本选项允许您设定本规则得以应用的来源埠。请在下表的选项中选择：	
Any	如果您希望将本规则应用到所有任意来源端口号的应用程序上，请选择本选项。
Single	本选项允许您将本规则应用到某一指定来源端口号的应用程序上。
Port Number	输入来源埠号。
Range	如果您希望将本规则应用到本埠范围的应用程序上，请选择本选项。当选择了本选项时，下列栏目可选：
Begin	输入范围的起始埠号。

选项	说明
End	输入范围的结束埠号。
Destination Port 本选项允许您设定能应用本规则的**目标端口**。请在下表的选项中选择:	
Any	本选项允许您将规则应用到所有任意来源端口号的应用程序上。
Single, Range	请按照上文**Source Port**部分的说明选择任一选项，并输入详细信息。
Service	本选项允许您选择任何预先设定好的服务（请从下表中选择），而不是目标端口。下面列出了一些服务选项: BATTLE-NET, PC-ANYWHERE, FINGER, DIABLO-II, L2TP, H323GK, CUSEEME, MSN-ZONE, ILS, ICQ_2002, ICQ_2000, MSN, AOL, RPC, RTSP7070, RTSP554, QUAKE, N2P, PPTP, MSG2, MSG1, IRC, IKE, H323, IMAP4, HTTPS, DNS, SNMP, NNTP, POP3, SMTP, HTTP, FTP, TELNET. **注意:** 服务是协议与埠号的结合。它们将在您把它们增加进设定页面的 “Firewall Service” 后出现。
Protocol 本选项允许您从下表中选择协议的类型。可供选择的设定为All, TCP, UDP, ICMP, AH 和 ESP。注意，如果您为目标端口选择 “service” ，本选项将不可用。	
NAT 本选项允许您选择出站信息NAT的类型。	
None	如果您不想在出站ACL规则里启用NAT，请选择此选项。
IP Address	选择本选项以指定您期望出站信息流向的计算机（通常是局域网络中的服务器）的IP地址。注意，此选项被称为反向NAPT 或虚拟服务器。
NAT 地址池	选择本选项来将预先设定好的NAT地址池接入规则。注意，只有反向静态NAT和反向NAPT域才能用来联机出站ACL的规则。
Interface	选择本选项为出站信息选择WAN接口IP地址。注意，WAN IP必须事先设定再选择此项。
Time Ranges 选择预先设定好的规则起作用的时间范围。选择“Always”来使规则一直起作用。	
Application Filtering 本选项允许您选择下表中预先设定好的FTP, HTTP, RPC 和/或 SMTP 应用程序过滤器。	
Log 点选 “Enable” 或 “Disable” 按钮来开启或关闭ACL规则logging功能。	

9.5.2 增加出站 ACL 规则

想要增加出站 ACL 规则，请参考下列步骤：

1. 打开出站 ACL 规则设定页面（请参考第 9.4.2 节**錯誤! 找不到參照來源。**）。
2. 在“**ID**”表中选择 “**Add New**” 。
3. 从“**Action**”表中设定期望的动作（允许或拒绝）。
4. 改动任一或所有下列栏目：source/destination IP, source/destination port, protocol, port mapping, time ranges, application filtering, log。请参考表 9.2 中对这些栏目的解释。
5. 透过选择 “**Move to**” 表中的序号来为规则指定优先级。注意，序号 1 表示优先劝最高。防火墙将按照优先劝的高低进行检查。
6. 点选 Add 按钮以創建新的 ACL 规则。新的 ACL 规则同时在出站 ACL 设定页面下半页的“出站访问控制表”中出现。

图 9.10 说明了如何創建接受出站 HTTP （例如，网页服务器） 服务的规则。 此规则允许出站 HTTP 信息流向主机 WAN/ IP 地址 192.168.1.15。

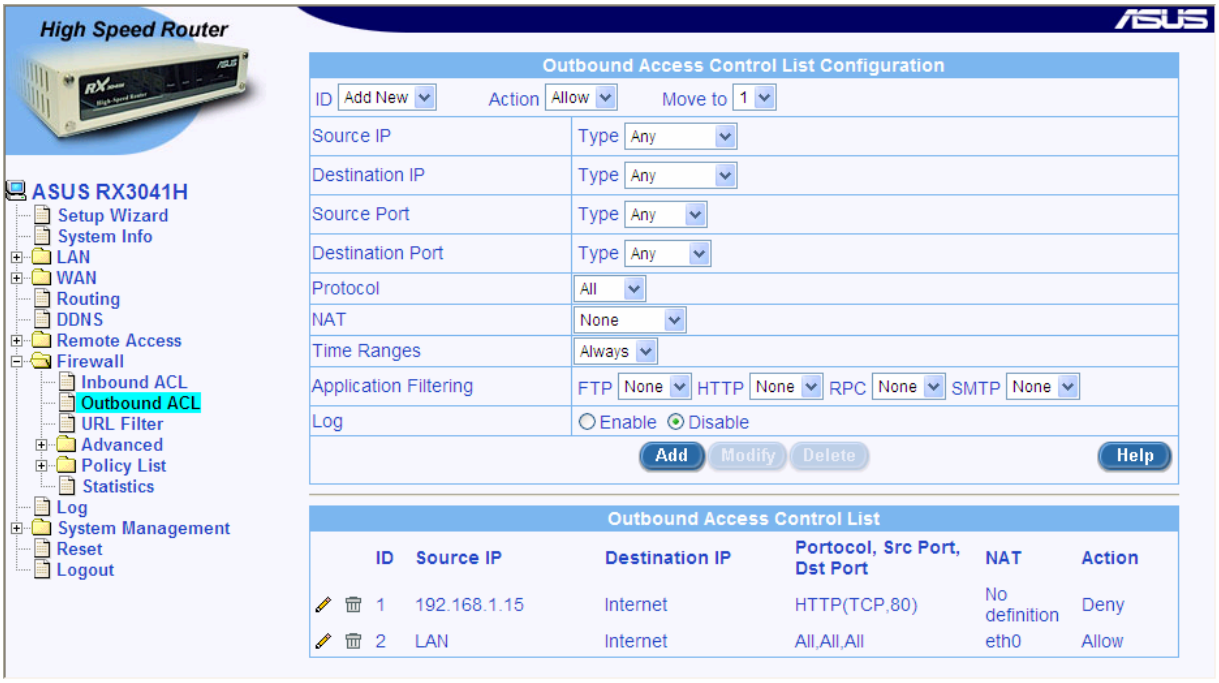


图 9.10. 出站 ACL 设定页面

9.5.3 修改出站 ACL 规则

想要修改出站 ACL 规则，请参考下列步骤：

1. 打开出站 ACL 规则设定页面（请参考第**錯誤! 找不到參照來源。**节 **錯誤! 找不到參照來源。**）。
2. 点选 图标，修改出站 ACL 表的规则或从“**ID**”表中选择规则序号。

3. 改动任一或所有下列栏目：action, source/destination IP, source/destination port, protocol, port mapping, time ranges, application filtering, log。请参看表 9.2 中对这些栏目的解释。

4. 点选 Modify 按钮以修改 ACL 规则。新的 ACL 规则设定同时在出站 ACL 设定页面下半页的“出站访问控制表”中出现。

9.5.4 删除出站 ACL 规则

想要删除出站 ACL 规则，请点选待删规则前面的图标，并参考下列步骤：

1. 打开出站 ACL 规则设定页面（请参考第**錯誤! 找不到參照來源。**节 **錯誤! 找不到參照來源。**）。

2. 点选 图标，删除待删的出站 ACL 表的规则或从“**ID**”表中选择规则序号。

3. 点选 Delete 按钮以删除 ACL 规则。新的 ACL 规则设定同时在出站 ACL 设定页面下半页的“出站访问控制表”中出现。

9.5.5 出站 ACL 规则展示

想要参看现有的出站 ACL 规则。您只需打开出站 ACL 规则设定页面，如第**錯誤! 找不到參照來源。**节 **錯誤! 找不到參照來源。** 所示。

9.6 设定 URL 过滤器

以 URL（Uniform Resource Locator，例如 www.yahoo.com）为基础的关键词过滤允许您定义一个或多个不应在 URL 出现的关键词。任何 URL 都包含一个或多个将被锁定的关键词。这是一个独立的特性，例如它与 ACL 规则没有关联。此特性能被独立地开启/关闭，但是只在开启防火墙的状态下工作。

9.6.1 URL 过滤器设定参数

表 9.4 说明 了URL过滤规则可供选择的设定参数。

表 9.4. URL 过滤器设定参数

选项	说明
URL过滤器状态	点选“Enable” 或 “Disable” 按钮开启或 关闭URL过滤功能。
代理服务器端口	输入为您网页浏览器设定的代理服务器（网页服务器）埠号。注意，代理服务器端口的改变需要您关闭再开启防火墙来使其生效。
ID	
Add New	点选本选项以增加新的URL过滤器规则。
Rule Number	从下表中选择规则修改属性。
Keyword	定义一个不会在URL中出现的关键词。

9.6.2 增加 URL 过滤器规则

想要增加 URL 过滤器，请参考下列步骤：

1. 打开 URL 设定页面（请参考第 9.5.2 节**錯誤! 找不到參照來源。** ）。

2. 在“**ID**”表中选择 “**Add New**” 。
3. 在关键词栏目中输入关键词。
4. 点选 Add 按钮以创建 URL 过滤器规则。新的规则同时在 URL 过滤器设定摘要表中出现。

9.6.3 修改 URL 过滤器规则

想要修改 URL 过滤器规则，您必须首先删除现有的 URL 过滤器规则（参看第 9.6.4 节），然后增加新的（参看第 9.6.2 节 增加 URL）。

9.6.4 删除 URL 过滤器规则

想要删除 URL 过滤器规则，请点选待删规则前面的图标，并参考下列步骤：

1. 打开 URL 设定页面（请参考第**錯誤! 找不到參照來源。**节 **錯誤! 找不到參照來源。**）。
2. 点选 图标，删除待删的 URL 过滤器设定摘要表的规则或从“**ID**”表中选择规则序号。
3. 点选 Delete 按钮以删除 URL 规则。

9.6.5 检查设定的 URL 过滤器规则

想要检查现有的 URL 过滤器规则，您只需打开 URL 过滤器设定页面，如第**錯誤! 找不到參照來源。**节 **錯誤! 找不到參照來源。**所示。

9.6.6 URL 过滤器规则实例

图 9.11 显示了 URL 过滤器规则实例，它示范了：

- 如何增加关键词“abcnews”，任何 URL 包含的关键词都会被锁定。
- 设定代理网页服务器序号到 80（您可以为您的代理服务器使用不同的埠号）。这意味着 URL 过滤器规则应用的范围将超过代理服务器端口 80，以防万一代理网页服务器已被使用。如果您没有为您的浏览器使用代理服务器，此设定将被忽略。注意，在做此改变之前您必须先关闭然后再打开防火墙。请参考第**錯誤! 找不到參照來源。**节 **錯誤! 找不到參照來源。**中对开启和关闭防火墙服务的详细说明。

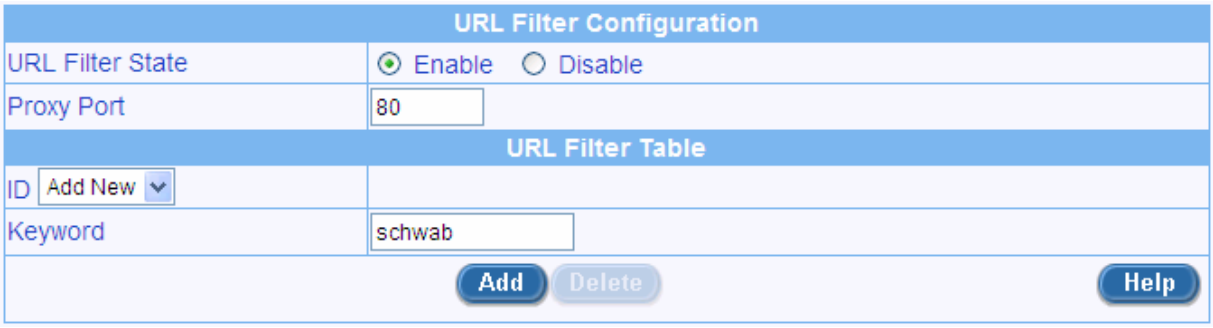


图 9.11. URL 过滤器规则实例

9.7 设定高级防火墙规格 – （防火墙 ➔ 高级）

本选项将在屏幕上显示下列子栏目供您设定高级防火墙规则：

- 自我访问（self Access） – 本选项允许您针对目标为路由器本身的封包去设定规则。

- 服务（Services） – 选择本选项来设定服务（应用程序使用指定的端口号）。每个服务记录都包含了服务名称、IP 协议值以及相应的埠号。
- DoS – 选择本选项来设定 DoS – 拒绝服务 – 参数。此选项列出了反抗路由器防火墙保护的 DoS 攻击的预设设定。

下列章节说明了这些选项的用法

9.7.1 设定自我访问（Self Access）规则

自我访问（Self Access）规则控制对网际网络安全路由器自身的访问。您可以使用自我访问规则设定页面，如图 9.12 所示，进行下列步骤：

- 增加自我访问规则，并设定参数
- 修改现有的自我访问规则
- 删除现有的自我访问规则
- 检查现有的自我访问规则

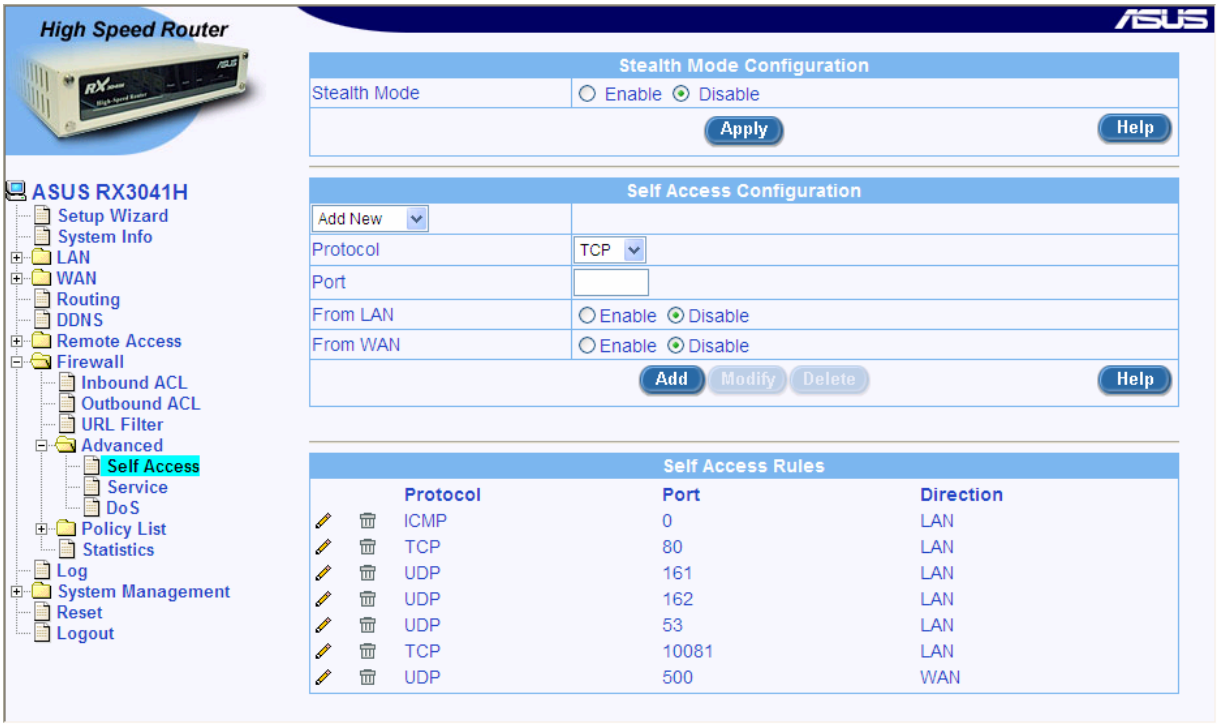


图 9.12. 自我访问规则设定页面

9.7.1.1 自我访问设定参数

表 9.5 说明了自我访问设定页面可供选择的设定参数。

表 9.5. 自我访问设定参数

选项	说明
Protocol	从下表中选择协议- TCP/ UDP/ICMP
Port	输入埠号。
Direction 选择信息被允许流通的方向。	

选项	说明
From LAN	选择Enable 或 Disable来允许或拒绝从局域网络（内部网络）到路由器的通信方向。
From WAN	选择Enable 或 Disable来允许或拒绝从WAN（外部网络）到路由器的通信方向。

9.7.1.2 增加自我访问规则

想要增加自我访问规则，请参考下列步骤：

1. 打开自我访问规则设定页面（请参考第 9.6.1.2 节**錯誤! 找不到參照來源。** ）。
2. 从自我访问规则下拉表中选择 “**Add New**” 。
3. 从协议的下拉表中选择一项，如果您选择了 TCP 或 UDP 协议，您将需要输入埠号。
4. 点选 Add 按钮以創建新的自我访问规则。新的规则同时在自我访问列表下半页的“自我访问规则设定页面”中出现。

实例

图 9.12 显示了屏幕上的条目用来：

- ► 增加新的自我访问规则到：
  - 允许 TCP 埠 80 从 LAN 流过来的通信量（例如 HTTP 通信量），以及拒绝从 WAN 端口（例如外部网络）流向网际网络安全路由器的 HTTP 通信量。

9.7.1.3 修改自我访问规则

想要修改自我访问规则，请参考下列步骤：

1. 打开自我访问规则设定页面（请参考第**錯誤! 找不到參照來源。**节 **錯誤! 找不到參照來源。** ）。
2. 点选 图标，修改自我访问规则表或从自我访问下拉表中选择自我访问规则。
3. 您可以从 LAN 或 WAN 或二者同时来开启或关闭通信。注意，如果 TCP 或 UCP 协议已选的话，埠号不能再更改。想要修改埠号，您必须首先删除现有的自我访问规则以及增加新的自我访问规则代替。
4. 点选 Modify 按钮以保存更改。新的自我访问规则设定同时在自我访问规则设定页面下半页的自我访问规则表中出现。

9.7.1.4 删除自我访问规则

想要删除自我访问规则，请点选待删规则前面的图标，并参考下列步骤：

1. 打开自我访问规则设定页面（请参考第**錯誤! 找不到參照來源。**节 **錯誤! 找不到參照來源。**）。
2. 点选 图标，删除待删的自我访问规则表或从自我访问规则下拉表中选择自我访问规则。
3. 点选 Delete 按钮以删除规则。注意，已删除的规则将从设定页面下半页的自我访问规则表中移除。

9.7.1.5 检查设定的自我访问规则

想要检查现有的自我访问规则，您只需打开自我访问规则设定页面，如第**錯誤! 找不到參照來源。**节 ***錯誤! 找不到參照來源。***所示。

9.7.2 设定服务列表

服务是协议和埠号的联合，被用在入站和出站ACL规则设定中。您可以使用服务设定页面来：

- 增加自我访问规则，并设定参数
- 修改现有的自我访问规则
- 删除现有的自我访问规则
- 检查现有的自我访问规则

图 9.13 显示了防火墙列表的设定页面。已设定的服务在页面的下半页显示：

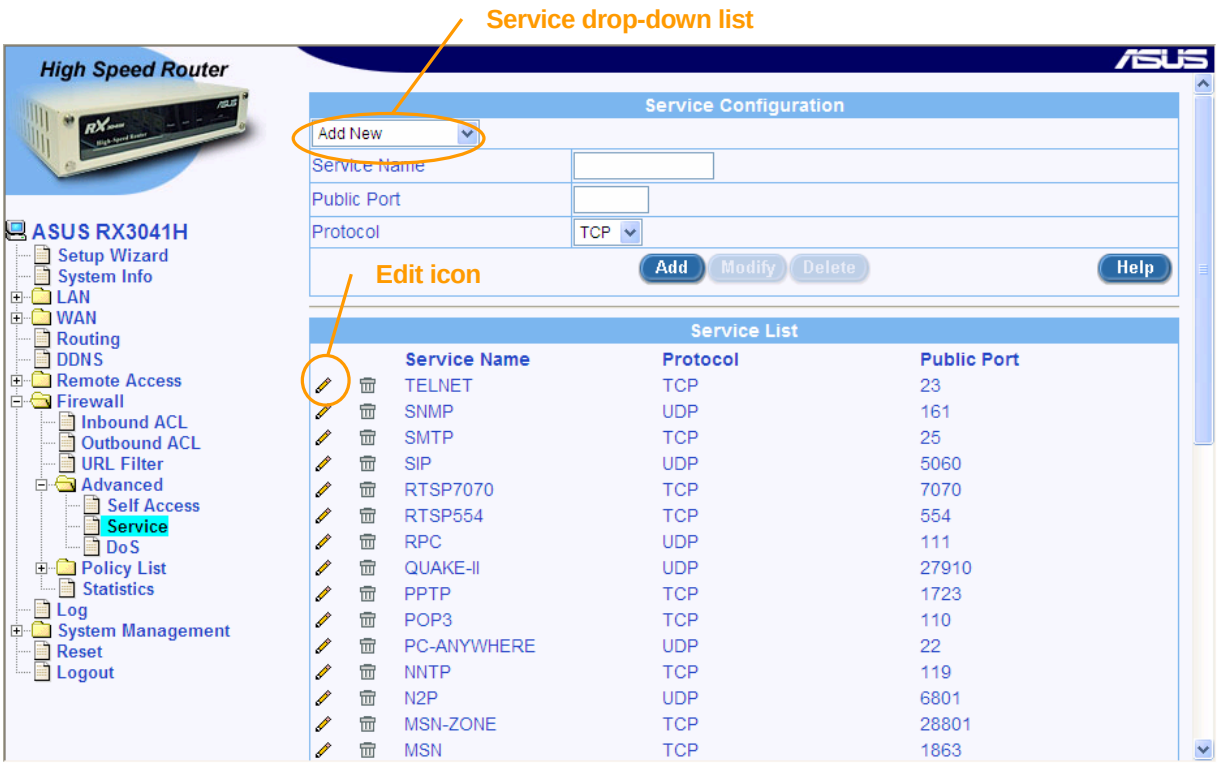


图 9.13. 服务列表设定页面

9.7.2.1 服务列表参数设定

表 9.6 说明了防火墙服务列表可供选择的设定参数。

表 9.6. 服务列表参数设定

选项	说明
Service Name	输入待增加的服务名称，注意，名称只由文字与数字组成。
Protocol	输入服务使用的协议的类型。
Port	输入为服务设立的埠号。

9.7.2.2 增加服务选项

想要增加服务选项，请参考下列步骤：

1. 打开服务列表设定页面（请参考第 9.6.2.2 节**錯誤! 找不到參照來源。**）。
2. 从服务下拉表中选择 “**Add New**” 。
3. 在 “**Service Name**” 栏目输入您想要的名称，最好是能表现出服务特性的有意义的名称。注意，名称只由文字与数字组成。
4. 更改下列任一或所有栏目：public port 和 protocol。请参看表 9.6 中对本栏目的解释。
5. 点选 Add 按钮以創建新的服务选项。新的服务选项同时在服务设定页面下半页的服务列表中出现。

9.7.2.3 修改服务选项

想要修改服务选项，请参考下列步骤：

1. 打开服务列表设定页面（请参考第**錯誤! 找不到參照來源。**节 **錯誤! 找不到參照來源。**）。
2. 从服务下拉表中选择服务选项，或者点选服务列表中需要修改的 图标。
3. 更改下列任一或所有栏目：service name, public port 和 protocol。请参看表 9.6 中对本栏目的解释。
4. 点选 Modify 按钮以保存更改。新的服务设定同时在服务设定页面下半页的服务列表中出现。

9.7.2.4 删除服务选项

想要删除自我访问规则，请参考下列步骤：

1. 打开服务列表设定页面（请参考第**錯誤! 找不到參照來源。**节 **錯誤! 找不到參照來源。**）。
2. 从服务下拉表中选择服务选项，或者点选服务列表中需要删除的 图标。
3. 点选 Delete 按钮以删除规则。注意，已删除的规则将从设定页面下半页的服务列表中移除。

9.7.2.5 检查设定的服务选项

想要检查现有的服务列表，请参考下列步骤：

1. 打开服务列表设定页面（如第**錯誤! 找不到參照來源。**节 **錯誤! 找不到參照來源。**所示）。
2. 服务列表在服务设定页面下半页出现，显示了所有已设定好的服务选项。

9.7.3 设定 DoS

网际网络安全路由器拥有一个专用的抵御攻击的引擎，能保护内部网络免受 DoS（拒绝服务）攻击，例如 SYN flooding, IP smurfing, LAND, Ping of Death 以及所有封包重组的攻击。这个引擎还能丢弃 ICMP 的重寄及拒绝 IP loose/strict 来源路由封包。例如，路由器防火墙提供防止“WinNuke”的保护的安全设备，网际网络中远程攻击未受保护的 Windows 系统的一个广泛应用的程序。网际网络安全路由器还提供对多种普通网际网络攻击的保护，例如 IP Spoofing, Ping of Death, Land Attack, Reassembly 以及 SYN flooding。要参考路由器提供的 DoS 保护完全列表，请看表 2.3。

9.7.3.1 DoS 保护设定参数

表 9.7 说明了DoS保护可供使用的设定参数。

表 9.7. DoS 保护设定参数

选项	说明
SYN Flooding	打勾或不打勾本选项以开启或关闭防止SYN Flood攻击的保护功能。此攻击包括向服务器发出联机要求，但是不全部完成联机。当不能从有效的用户那里接收联机时，这将导致一些计算机陷入“当机状态”（SYN是SYNchronize的简写；是打开网际网络联机的第一步）。如您期望保护网络免受TCP SYN flooding攻击，您可选择此项。SYN Flood保护预设为开启状态。
Winnuke	打勾或不打勾本选项以开启或关闭防止Winnuke攻击的保护功能。一些Microsoft Windows操作系统的较老版本易遭受此项攻击。如果局域网络计算机的操作系统没有及时下载最新的版本/补丁来升級，那么我们建议您开启此项保护功能。
MIME Flood	打勾或不打勾本选项以开启或关闭防止MIME攻击的保护功能。您可选择本选项以保护您网络内的邮件服务器免受MIME flooding的攻击。
FTP Bounce	打勾或不打勾本选项以开启或关闭防止FTP Bounce攻击的保护功能。简言之，攻击在误用FTP协议中的PORT命令时才发生。攻击者能創建FTP服务器与另一系统中任意端口的联机。此联机可被用来绕开访问控制。
IP Unaligned Time Stamp	打勾或不打勾本选项以开启或关闭防止unaligned IP time stamp攻击的保护功能。 某些操作系统在接收到未在32位边界内的IP timestamp选项时会崩溃。
Sequence Number Prediction Check	打勾或不打勾本选项以开启或关闭防止TCP Sequence Number Prediction攻击的保护功能。对于TCP封包而言，Sequence Number 是被用来阻止对任意资料的接收或当Initial Sequence Number（ISN）随意产生时被攻击者恶意使用。因为拥有有效的Sequence Number的伪造封包可骗取接收主机的信任。如此一来，攻击者就能够进入系统。请注意！此种攻击只影响开始或终止于网际网络安全路由器的TCP封包。
Sequence Number Out of Range Check	打勾或不打勾本选项以开启或关闭防止TCP out of range sequence number攻击的保护功能。攻击者可送出一个TCP封包，导致入侵侦测系统（IDS）在联机中变得与资料不同步。后来在此联机中发出的信框就可能被IDS忽略。这可能暗示着一次不成功的对TCP对话的抢夺企图。
ICMP Verbose	打勾或不打勾本选项以开启或关闭防止ICMP错误消息攻击的保护功能。ICMP讯息可使用非期望的通信量来泛流您的网络。本选项默认值为开启状态。
Maximum IP Fragment Count	输入防火墙允许每个IP封包的片段的最大数目。当您与ISP的联机透过PPPoE进行时，本选项十分需要。此资料在传输或接收IP片段时使用。当大尺寸的封包透过路由器送出时，封包被分解为最大传输单元（MTU，

选项	说明
	Maximum Transmission Unit）大小的片段。分解的数目预设为45。如果接口的MTU为1500（以太网预设），那么每个IP封包的最大片段数为45。如果MTU越小，那么片段的数目会越大。
Minimum IP Fragment Size	输入防火墙允许每个IP封包的片段的最小数目。此限制不会在封包最后的片段上强制执行。如果网际网络通信量在产生了很多小的片段时，此数值将变小。此种情况在有多个封包遗失、速度变慢和日志（log）经常产生的情况下（片段的大小比设定好的最小片段的大小还要小）常常出现。

9.7.3.2 设定 DoS

大多数支持的攻击类型 DoS 保护都预设开启。图 9.14 显示了 DoS 的预设设定。您可打勾或不打勾个别的攻击保护类别以开启或关闭针对特殊攻击类型的保护。

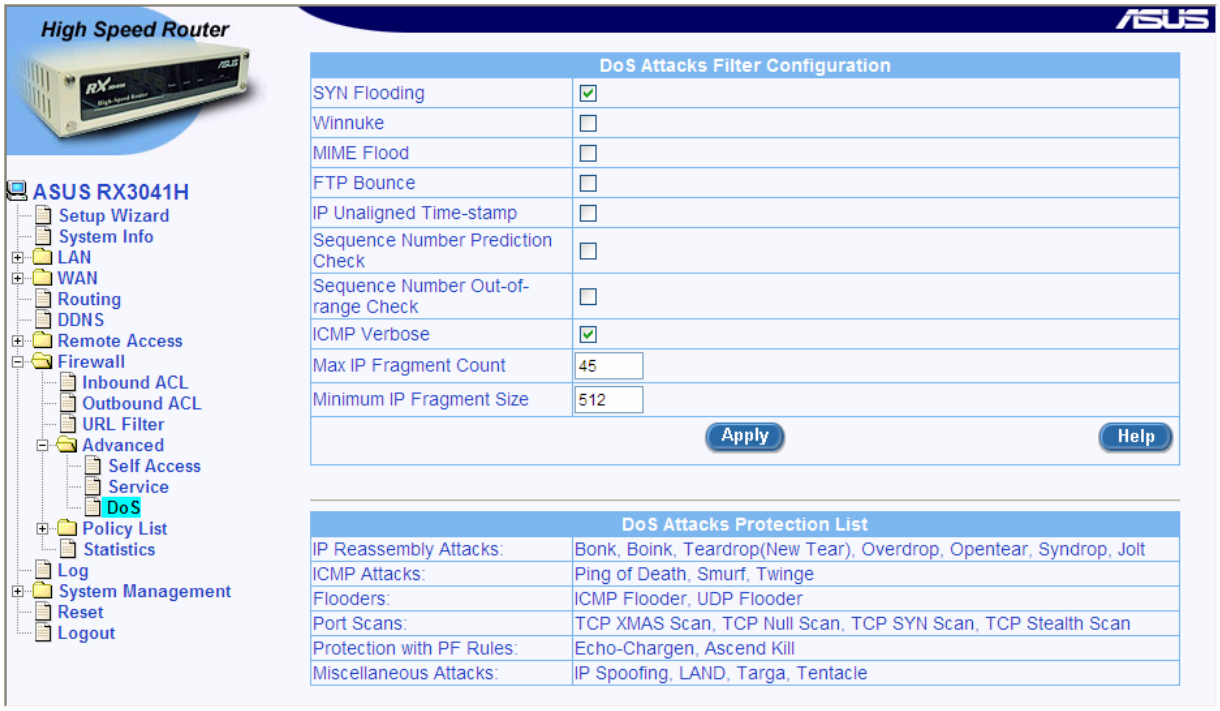


图 9.14. DoS 设定页面

9.8 防火墙规则列表 – （防火墙 ➔ 规则列表）

防火墙规则列表提供了管理防火墙 ACL 规则（入站/出站 ACL 规则和群组 ACL 规则）的方便之路。

- 应用程序过滤器 – 本选项允许您为 FTP, HTTP, RPC 和 SMTP 应用程序设定命令过滤器。在这里，在它们隶属于规则之前设定过滤器。
- IP 地址池 – 本选项允许您为 IP 地址池设置逻辑名称，以及设定合适的 IP 地址。每个记录都包含了 IP 记录的名称和 IP 地址的类型（单个的 IP 地址或 IP 地址域或子网络地址）。

- NAT 地址池 – 本选项允许您设定确保对应从内部 IP 地址到公共 IP 地址映像的 NAT 地址池 。在这里，在它们隶属于规则之前设定 NAT 地址池。
- 时间范围 – 本选项允许您为用户透过路由器访问网络设定时间窗口。

9.8.1 设定应用程序过滤器

应用程序过滤器允许网络管理员阻止、监视，以及报告网络用户访问非商业和不良内容。此高性能内容访问管理将有助于生产力的提高、占用更低的频宽使用以及减少法律责任。

网际网络安全路由器具备控制积极和过滤某些应用程序协议内容的能力，例如 HTTP, FTP, SMTP 和 RPC。

- HTTP – 您能定义以阻止过滤 HTTP 扩展名

  ActiveX – *.ocx

  Java Archive – *.jar

  Java Applets – *.class

  Microsoft Archives – *.msar

  其它的以档案扩展名为基础的 URL。
- FTP – 允许您为站点和用户群定义和强制执行档案传送规则
- SMTP – 允许您过滤揭示关于接收者超量信息的操作，例如 VRFY, EXPN 等。
- RPC – 允许您过滤以指定的 RPC 程序号码为基础的程序。

9.8.1.1 应用程序过滤器设定参数

表 9.8 说明了应用程序过滤器可供选择的设定参数。

表 9.8. 应用程序过滤器设定参数

选项	说明
Filter Type	选择过滤器的类型： FTP, HTTP, RPC 和 SMTP。
Filter Name	为过滤器输入名字。
Protocol	选择应用程序过滤器使用的协议（TCP/UDP）。
Port	输入应用程序过滤器使用的端口号。
Log 本选项包括开启和关闭登入应用程序过滤器的按钮。	
Enable	选择本选项以开启登入应用程序过滤器。
Disable	选择本选项以关闭登入应用程序过滤器。
Action	
Allow	按此按钮以设定**允许**的规则。 当限制为防火墙时，此规则将允许匹配的封包透过。
Deny	按此按钮以设定**拒绝**的规则。 当限制为防火墙时，此规则将**不**允许匹配的封包透过。
Filter Commands	

选项	说明
本选项允许您输入各自应用程序的命令。所支持的每个应用程序的命令列表如下所示：	
FTP Commands	增加下列命令至FTP过滤器到：
CWD	允许或拒绝改变目录。
LIST	允许或拒绝档案/目录列表。
MKD	允许或拒绝创建目录。
NLST	允许简要的目录内容列表。
PASV	允许被动资料内容的开始。
PORT	允许或拒绝参与主动的资料联机的端口号。
RETR	允许或拒绝从FTP服务器获得档案。
RMD	允许移除目录。
RNFR	允许重新命名自。
RNTO	允许重新命名到。
DELE	允许删除档案。
SITE	允许设定站点参数（FTP服务器提供的特殊服务）。
STOR	允许或拒绝把档案传送至FTP服务器。
SMTP Commands	增加下列命令至SMTP过滤器到：
MAIL	允许或拒绝开始邮件处理。
RCPT	允许或拒绝识别邮件资料的个别接收。
DATA	允许或拒绝邮件资料。
VRFY	允许或拒绝核实用户的存在。
EXPN	允许或拒绝邮寄表的鉴别。
TURN	允许或拒绝客户端与服务器交换角色而寄送反向邮件。
SEND	允许或拒绝开始邮件处理。
HTTP (Deny Following Files)	增加下列命令至HTTP过滤器到：
Java Applet	拒绝所有 *.class 档案。
Java-archive	拒绝所有*.jar档案。
MS Archive	拒绝所有*.msar档案。
ActiveX	拒绝所有*.ocx档案。
RPC Numbers	
RPC numbers	增加此命令至RPC过滤器以允许或拒绝RPC程序数目。

9.8.1.2 访问应用程序过滤器设定页面 – （防火墙 ➔ 规则列表 ➔ 应用程序过滤器）

以管理员身份登入设定管理器，点选 **Firewall** 菜单，点选 **Policy List** 子菜单，然后点选 **Application Filter** 子菜单。应用程序过滤器设定页面将如图 9.9 所示。

注意，当您打开应用程序过滤器设定页面时，现有的应用程序过滤器规则同时在设定页面的下半页出现，如图 9.9 所示。

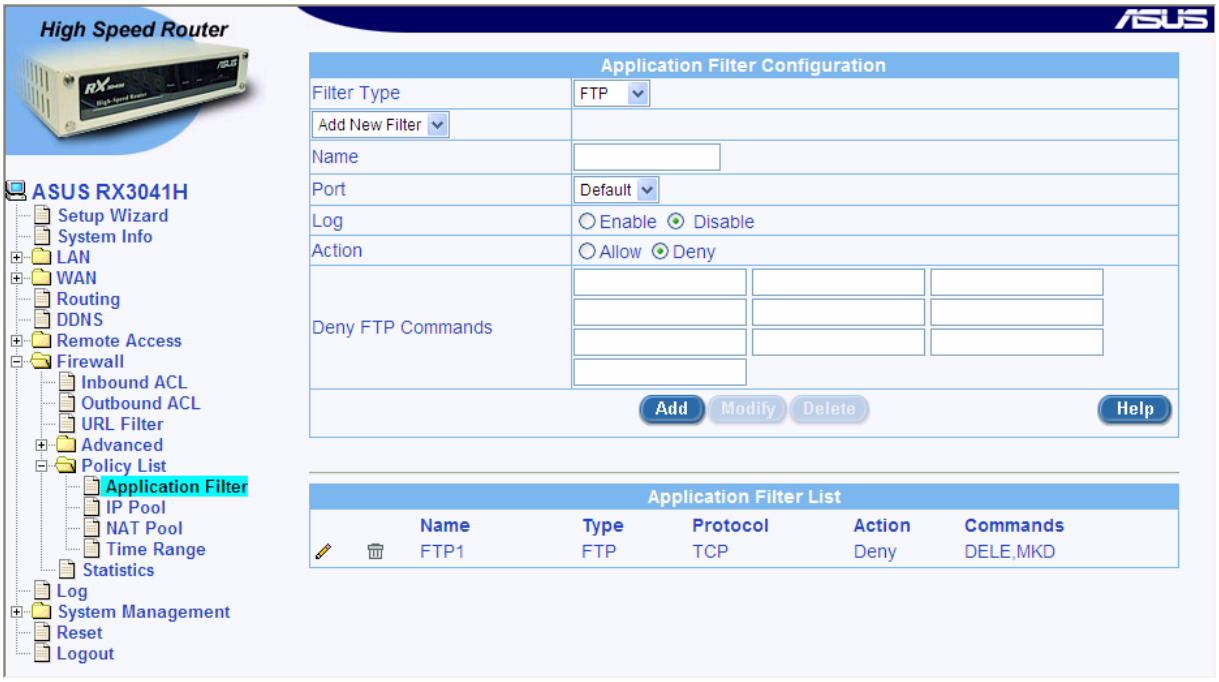


图 9.15. 应用程序过滤器设定页面

9.8.1.3 增加应用程序过滤器

应用程序过滤器设定最好用一些实例来阐释。注意，为 RPC 和 SMTP 进行的设定 FTP 相类似，这里将不 提及。

1) FTP 实例：增加 FTP 过滤器规则以阻止 FTP 删除命令

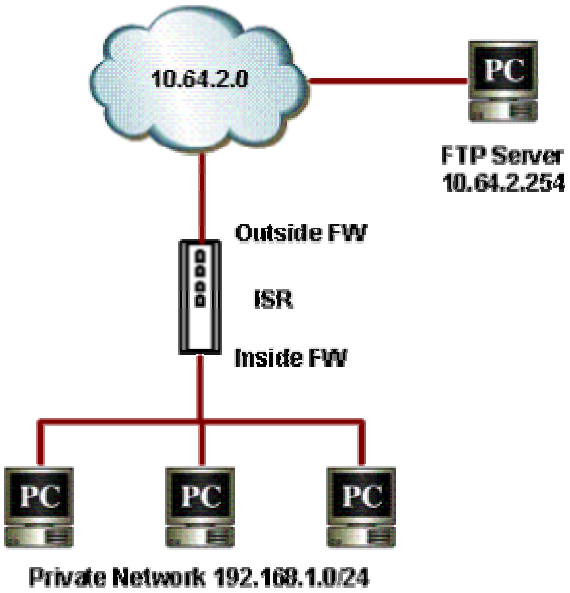


图 9.16 对 FTP 过滤器实例进行的网络诊断 – 阻止 FTP 删除命令

1. 打开应用程序过滤器规则设定页面（防火墙 ➔ 规则列表 ➔ 应用程序过滤器）

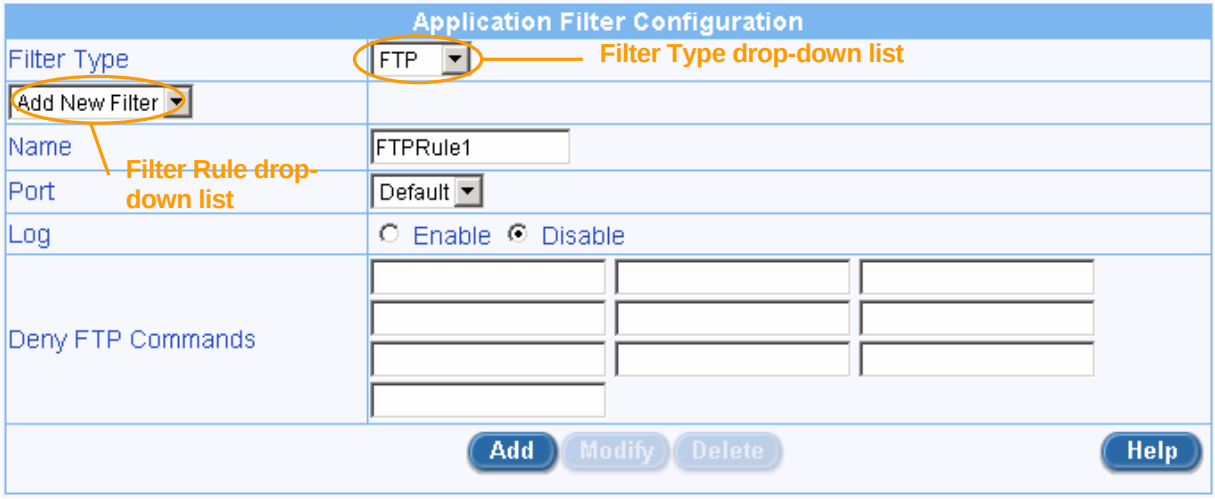


图 9.17. FTP 过滤器实例 – 设定 FTP 过滤器规则

2. 从过滤器程序下拉表中选择 FTP。
3. 从过滤器规则下拉表中选择 “Add New Filter” 。
4. 为规则输入名称 – 在此实例中，为 FTPRule1。
5. 如需要，改变埠号。然而，我们推荐您保持预设的设定值不变。
6. 选择开启或关闭登入选项，预设的设定是关闭。
7. 点选第一个 FTP 命令栏目，防火墙设定助手页面将出现。

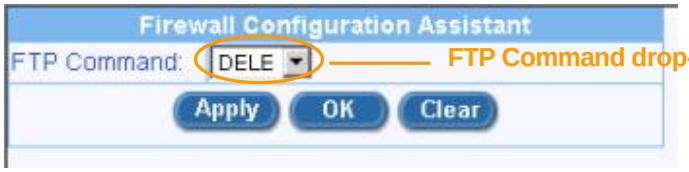


图 9.18 FTP 过滤器实例 – 防火墙设定助手

8. 从 FTP 命令下拉表中选择您需要的 FTP 命令，然后点选 OK 按钮。选中的 FTP 命令将被添加到已选的拒绝 FTP 命令栏目中。

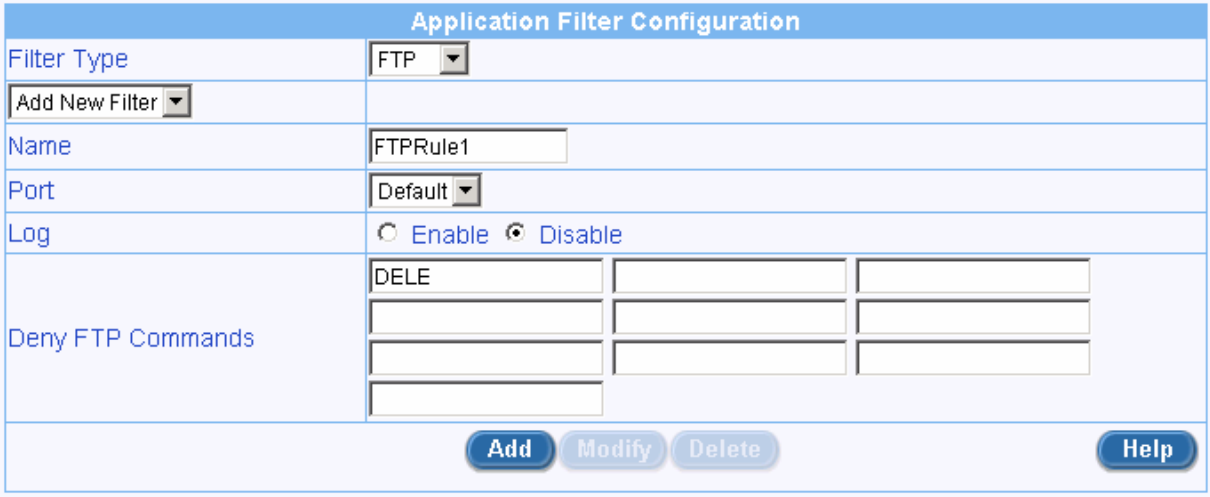


图 9.19 FTP 过滤器实例 – 增加 FTP 过滤器以拒绝 FTP 删除命令

9. 如果需要添加更多的命令，请重复步骤；否则，请继续下一步。

10. 点选 Add 按钮以创建 FTP 应用程序过滤器规则。

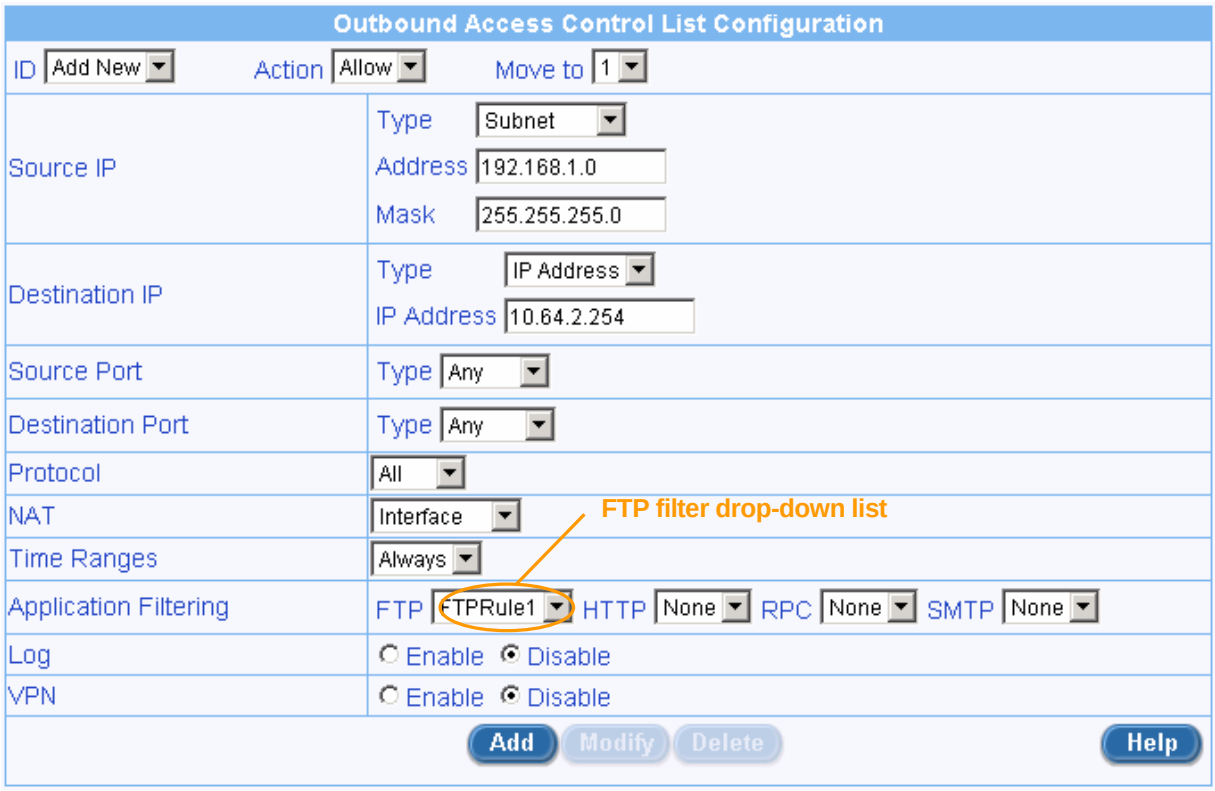


图 9.20. FTP 过滤器实例 – 联合 FTP 过滤器至 ACL 规则

11. 透过从 FTP 过滤器下拉表（参考图 9.20）中选择 FTP 过滤器，联合新近增加的 FTP 应用程序过滤器至防火墙 ACL 规则（入站、出站或群组 ACL）上，然后点选 Add 或 Modify 按钮以保存设定。

1) HTTP 实例：增加 HTTP 过滤器规则以 阻止 JAVA Applet 以及 Java archive 程序

1. 打开应用程序过滤器规则设定页面（防火墙 ➔ 规则列表 ➔ 应用程序过滤器）

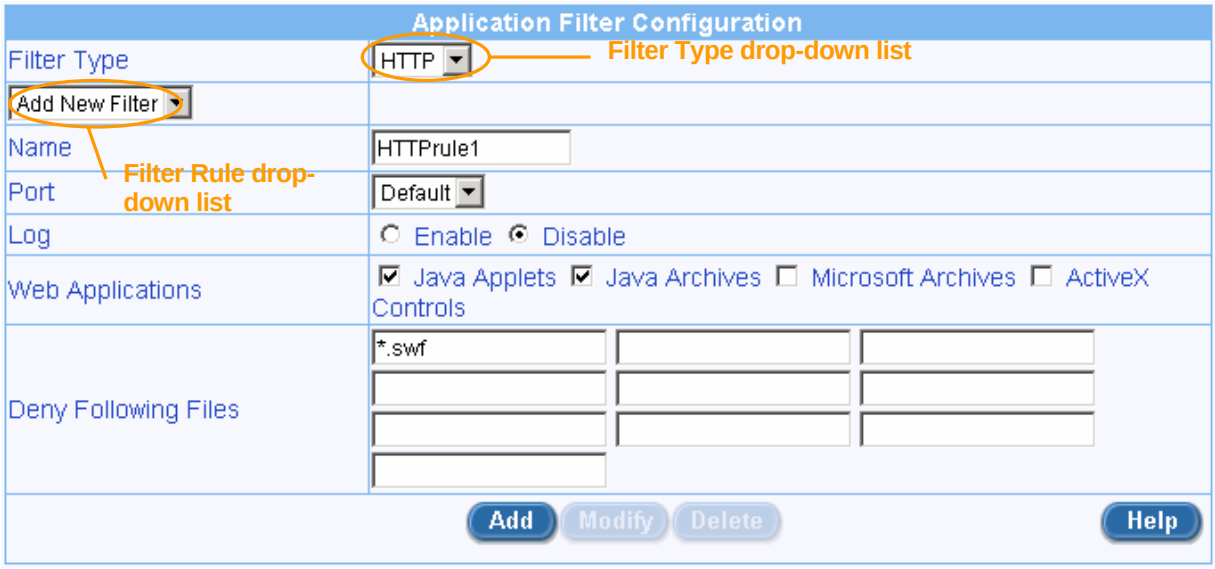


图 9.21. HTTP 过滤器实例 – 设定 HTTP 过滤器规则

2. 从过滤器程序下拉表中选择 HTTP。
3. 从过滤器规则下拉表中选择 “Add New Filter” 。
4. 为规则输入名称 – 在此实例中，为 HTTPrule1。
5. 如需要，改变埠号。然而，我们推荐您保持预设的设定值不变。
6. 选择开启或关闭登入选项，预设的设定是关闭。
7. 检查网页应用程序档案以阻止 – 在本例中，为 JAVA Applet 程序以及 Java archive 档案。
8. 输入附加的网页应用程序档案以阻止。如需要，在“Deny Following Files”栏目输入档案扩展名。图 9.21 显示了除了 JAVA Applet 及 Java archive 档案之外，被阻止的 flash 档案（档案的扩展名为 *.swf）。
9. 点选 Add 按钮以创建 HTTP 应用程序过滤器规则。
10. 透过从 HTTP 过滤器下拉表（参考图 9.20）中选择 HTTP 过滤器，联合新近增加的 HTTP 应用程序过滤器至防火墙 ACL 规则（入站、出站或群组 ACL）上，然后点选 Add 或 Modify 按钮以保存设定。

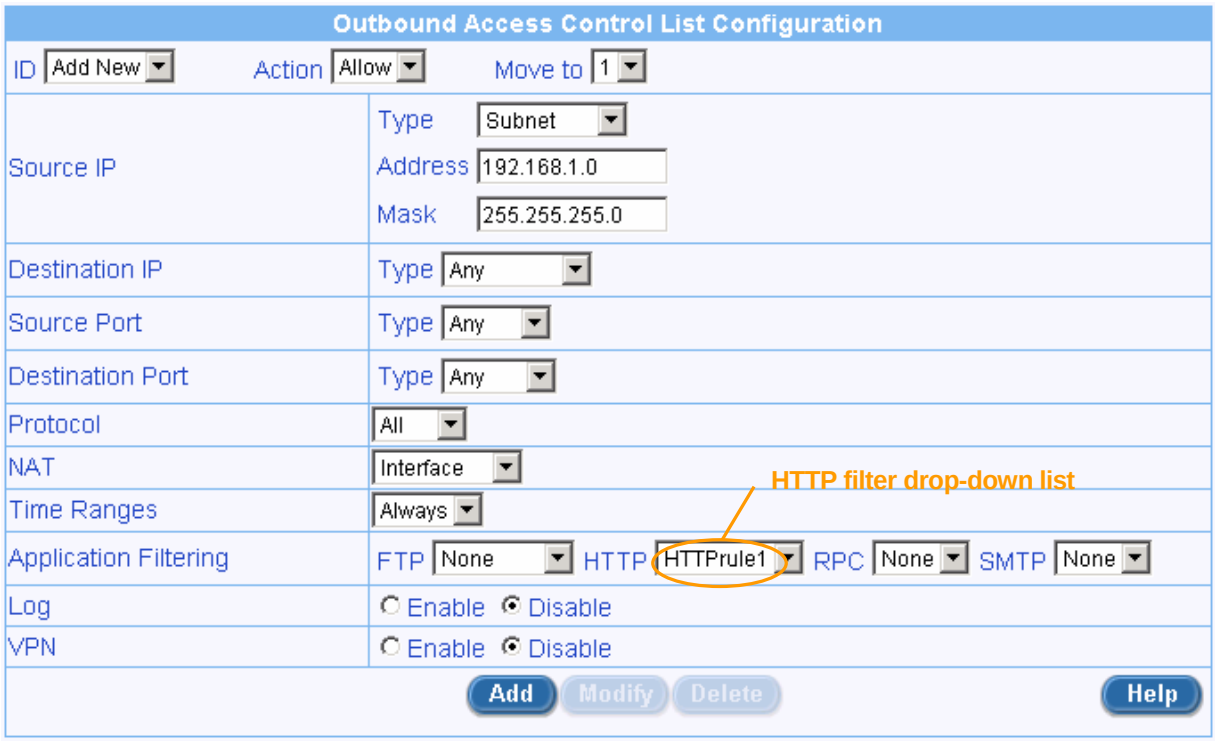


图 9.22. HTTP 过滤器实例 – 联合 HTTP 过滤器规则至 ACL 规则

9.8.1.4 修改应用程序过滤器

想要修改 IP 地址池，请参考下列步骤：

1. 打开应用程序过滤器设定页面（请参考第**錯誤! 找不到參照來源。**节 访问应用程序过滤器设定页面 – （防火墙 ➔ 规则列表 ➔）。

2. 选择要修改的应用程序过滤器，点选应用程序过滤器列表中将要修改的应用程序过滤器的 图标，或者从过滤器类型下拉表中选择过滤器类型，然后从过滤器规则下拉表中选择过滤器规则。
3. 对下列栏目做您想要的修改：Port number, logging option 等。
4. 点选 Modify 按钮以保存新的设定。应用程序过滤器的新的设定将显示在应用程序过滤器列表中。

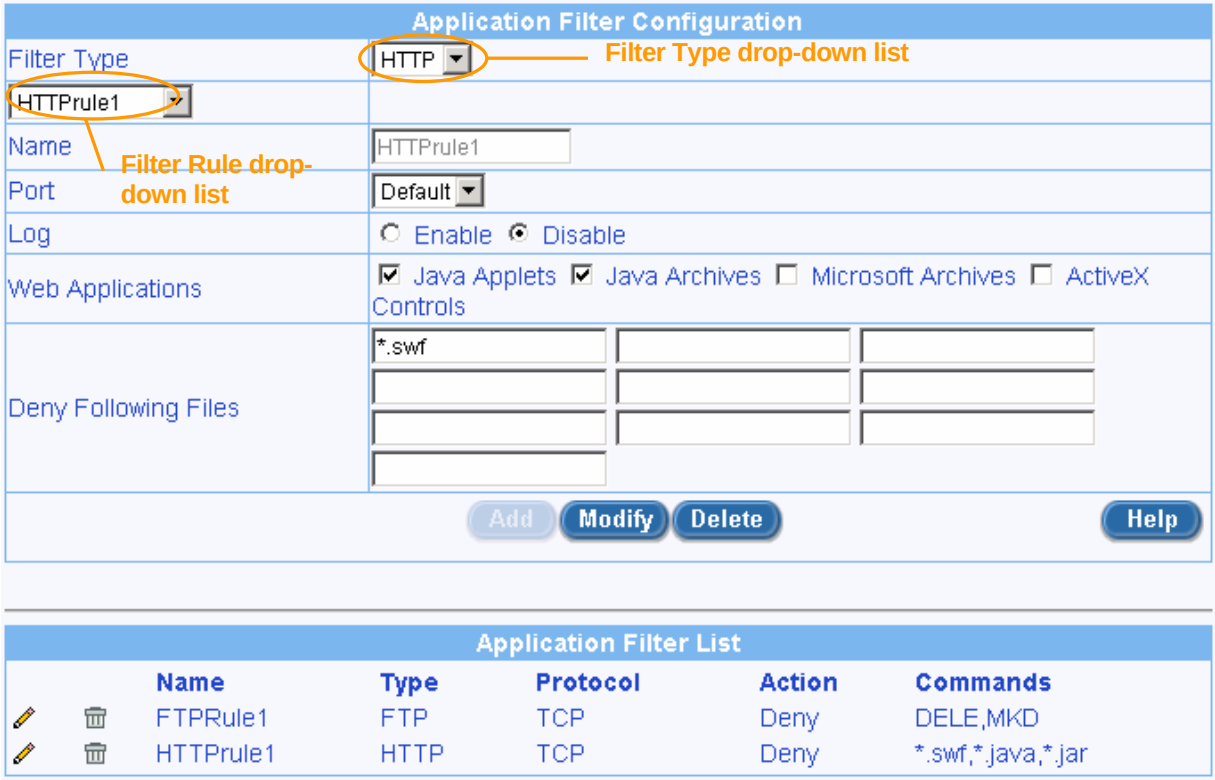


图 9.23. 修改应用程序过滤器

9.8.1.5 删除应用程序过滤器

想要删除应用程序过滤器，请点选待删过滤器前面的 图标，并参考下列步骤：

1. 打开应用程序过滤器设定页面（请参考第**錯誤! 找不到參照來源。**节 访问应用程序过滤器设定页面 – （防火墙 ➔ 规则列表 ➔）。
2. 选择要删除的应用程序过滤器，点选应用程序过滤器列表中将要删除的应用程序过滤器的 图标，或者从过滤器类型下拉表中选择过滤器类型，然后从过滤器规则下拉表中选择过滤器规则。
3. 点选 Delete 按钮以删除过滤器。

9.8.2 设定 IP 地址池

9.8.2.1 IP 地址池设定参数

表 9.9 说明了IP地址池可供使用的设定参数。

表 9.9. IP 地址池设定参数

选项	说明

选项	说明
IP Pool Name	输入本地 IP 名字。
IP Pool Type	选择 IP 地址池的类型。
IP Range	本选项允许您设定 IP 地址的范围。
Start IP	输入 IP 范围的起始地址。
End IP	输入 IP 范围的终止地址。
Subnet	本选项允许您把所有联机到 IP 子网的计算机都包括进来。
Subnet Address	输入合适的 IP 地址。
Subnet Mask	输入相应的屏蔽。
IP Address	本选项允许您设定单一的 IP 地址。
IP Address	输入 IP 地址。

9.8.2.2 修改 IP 地址池

想要修改 IP 地址池，请参考下列步骤：

1. 打开 IP 地址池设定页面（请参考第**錯誤! 找不到參照來源。** 节**錯誤! 找不到參照來源。**）。
2. 从 IP 地址池下拉表中选择 IP 地址池，或者点选 IP 地址池列表中需要修改的 IP 地址池 图标。
3. 更改下列任一或所有栏目： 地址池 name、地址池 type 和 IP address。
4. 点选 Modify 按钮以保存更改。新的设定同时在 IP 地址池列表中出现。

9.8.2.3 删除 IP 地址池

想要删除 IP 地址池，请点选待删 IP 地址池前面的 图标，或者参考下列步骤：

1. 打开 IP 地址池设定页面（请参考第**錯誤! 找不到參照來源。** 节**錯誤! 找不到參照來源。**）。
2. 点选待删 IP 地址池列表前面的 图标，或者从 IP 地址池下拉表中选择 IP 地址池。
3. 点选 Delete 按钮以删除 IP 地址池。

9.8.2.4 IP 地址池实例

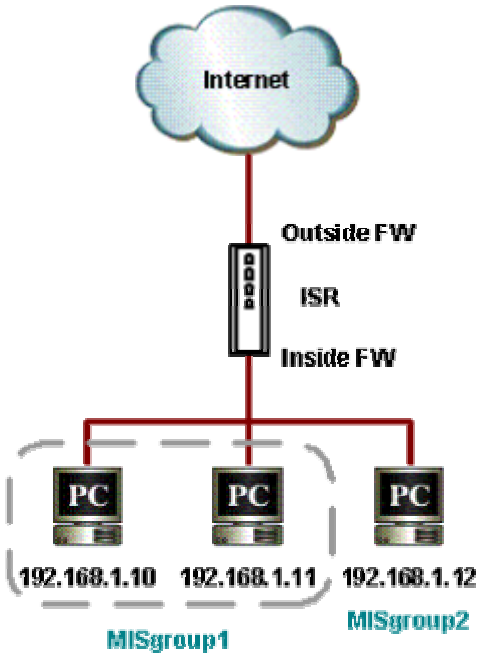


图 9.24.网络诊断对 IP 地址池的设定

1. 打开 IP 地址池设定页面以創建两个 IP 地址池 – 请参看图 9.25。

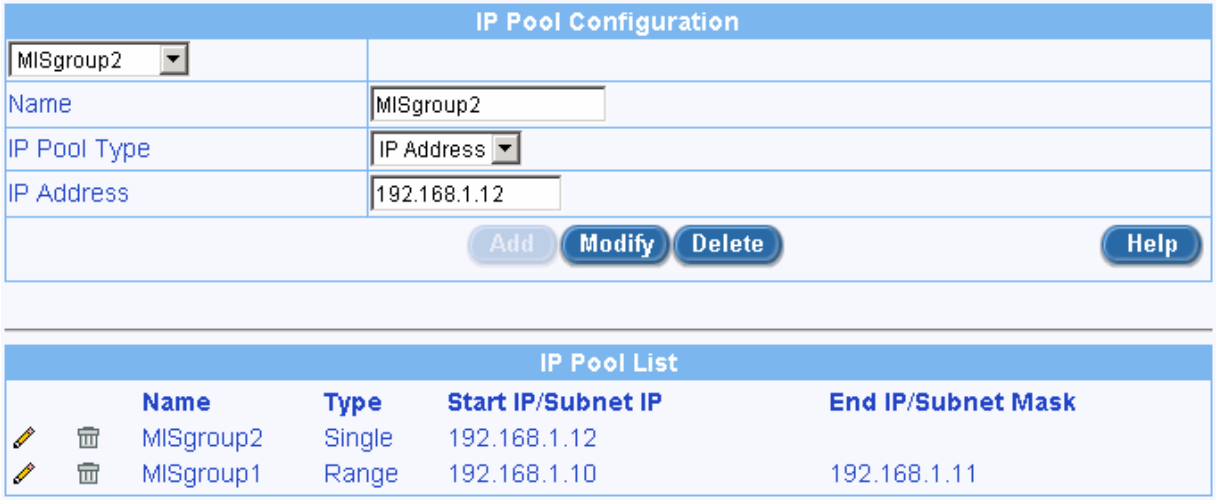


图 9.25. IP 地址池实例 – 增加两个 IP 地址池 – MISgroup1 和 MISgroup2

2. 透过从来源 IP 类型下拉表中选择“IP 地址池”，把 IP 地址池联合到防火墙 ACL 规则 – 入站、出站或者群组 ACL，然后从 IP 地址池下拉表中选择 IP 地址池。在这个实例，IP 地址池被用来与来源 IP 相联合；另外，它还可被用来与目的地 IP 联合。正如图 9.26，MISgroup1 不允许玩网络游戏，Quake-II 何时都行。

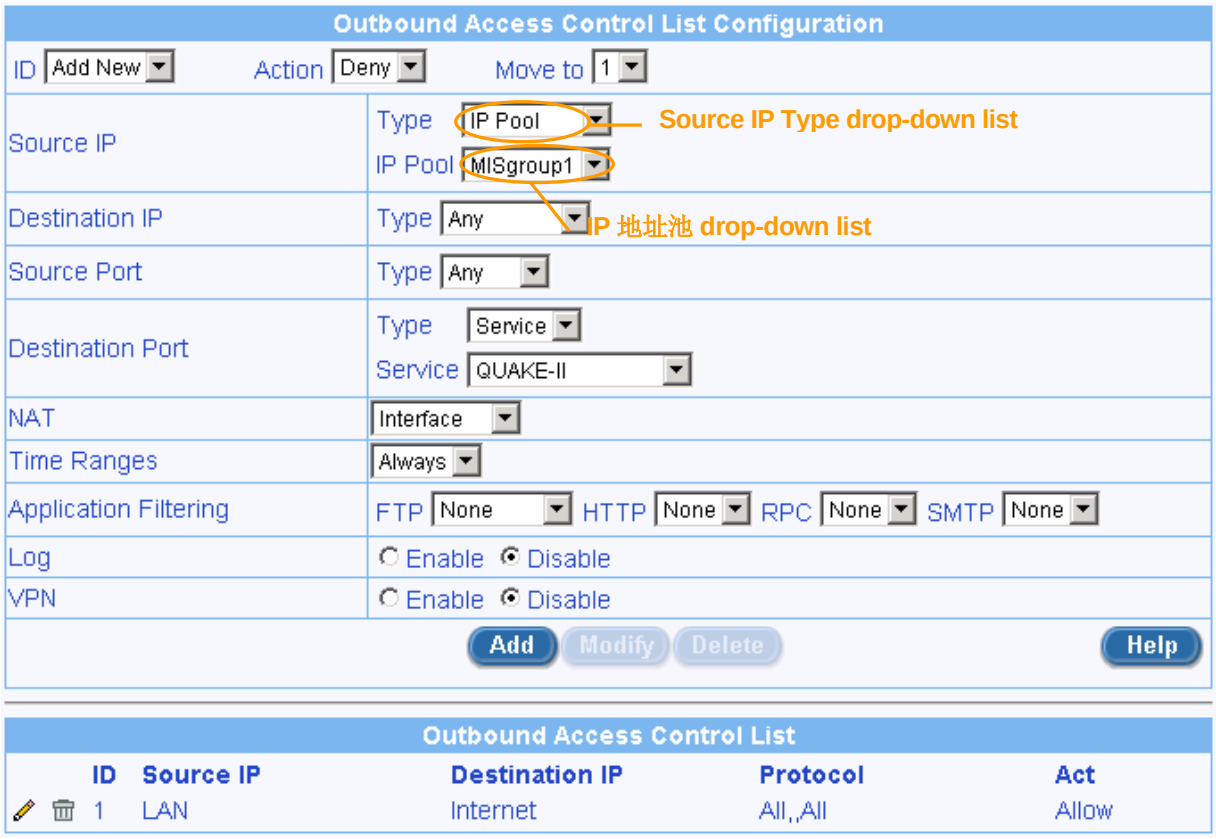


图 9.26. IP 地址池实例 – 拒绝 QUAKE-II 与 MISgroup1 的联机

9.8.3 设定 NAT 地址池

9.8.3.1 NAT 地址池设定参数

表 9.10 说明了NAT地址池可供使用的设定参数。

表 9.10. NAT 地址池设定参数

选项	说明
NAT Pool Name	输入NAT地址池的名字。
NAT Pool Type	选择NAT地址池的类型并創建合适的IP地址的条目。
Static 选择 NAT 类型以设定网际网络地址与外部地址之间一对一的映像。	
LAN IP range	为网际网络地址而设
Start IP	输入起始的IP地址。
End IP	输入终止的IP地址。
互聯網 IP Range	为外部地址而设
Start IP	输入起始的IP地址。
End IP	输入终止的IP地址。

选项	说明
Dynamic 选择本 NAT 类型以对应一套从内部（企业）计算机到公共IP地址的映像。请确保LAN IP范围与网际网络IP范围如上所述。	
Overload 选择本 NAT 类型以使用单一的公共IP地址来连接多个内部（LAN）计算机到外部（网际网络）网络。	
NAT IP Address	对于overload，输入NAT IP地址。

9.8.3.2 增加 NAT 地址池

想要增加 NAT 地址池，请参考下列步骤：

1. 打开 NAT 地址池设定页面（请参考第 9.7.3.2 节**錯誤! 找不到參照來源。**）。
2. 在 NAT 地址池下拉表中选择“**Add New Pool**”。
3. 在名称栏目中输入一个地址池名。
4. 从类型下拉表中选择一个地址池类型。
5. 如果选择的是 “Static” 或者 “Dynamic” 地址池类型，输入起始的 IP 地址和终止的 IP 地址，并对应起始的 IP 地址和终止的 IP 地址映像。如果选择的是 “Overload” 地址池类型，输入 NAT IP 地址。如果您想使用与 NAT IP 地址一样为 WAN 埠指定的 IP 地址，选择 Interface 地址池类型。
6. 点选 Add 按钮以創建新的 NAT 地址池。新的 NAT 地址池同时在 NAT 地址池列表中出现。

9.8.3.3 修改 NAT 地址池

想要修改 NAT 地址池，请参考下列步骤：

1. 打开 NAT 地址池设定页面（请参考**錯誤! 找不到參照來源。 錯誤! 找不到參照來源。**）。
2. 从 NAT 地址池下拉表中选择 NAT 地址池，或者点选 NAT 地址池列表中需要修改的 NAT 地址池 图标。
3. 更改下列任一或所有栏目： 地址池 name, 地址池 type 和 IP address。
4. 点选 Modify 按钮以保存更改。新的设定同时在 NAT 地址池列表中出现。

9.8.3.4 删除 NAT 地址池

想要删除 NAT 地址池，请点选待删 NAT 地址池前面的 图标，或者参考下列步骤：

1. 打开 NAT 地址池设定页面（请参考第 9.7.3.2 节**錯誤! 找不到參照來源。**）。
2. 点选待删 NAT 地址池列表前面的 图标，或者从 NAT 地址池下拉表中选择 NAT 地址池。
3. 点选 Delete 按钮以删除 NAT 地址池。

9.8.3.5 NAT 地址池实例

图 9.27 显示了网络诊断的 NAT 地址池实例。

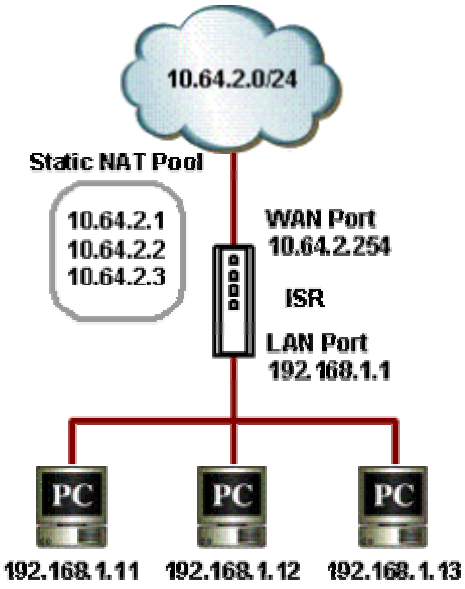


图 9.27. 网络诊断 NAT 地址池实例

1. 为静态 NAT 創建 NAT 地址池 – 参看图 9.28。

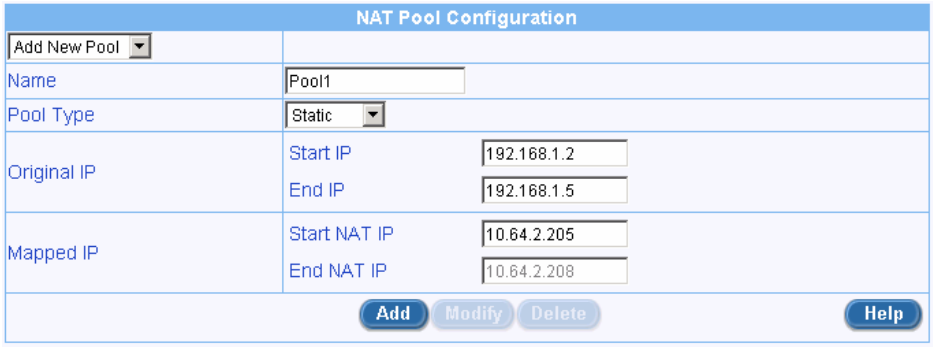


图 9.28. NAT 地址池实例 – 創建静态 NAT 地址池

2. 透过从 NAT 类型下拉表中选择“NAT 地址池”，把 NAT 地址池联合到出站 ACL 规则，然后从 NAT 地址池下拉表中选择现有的 NAT 地址池。

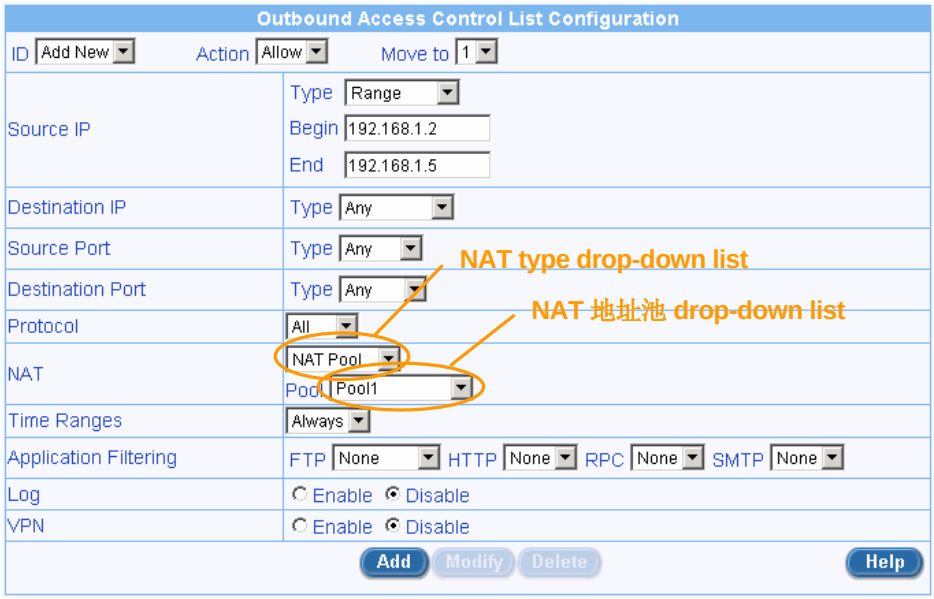


图 9.29. NAT 地址池实例 – 联合 NAT 地址池 ACL 规则

9.8.4 设定时间范围

为与 ACL 规则創建永久性的联系，您可利用本项目来设定访问时间范围。与时间范围相联合的 ACL 规则将只在预定的时段内有效。如果 ACL 规则在从 10:00hrs 到 18:00hrs 之间拒绝了 HTTP 访问，那么，在 10:00hrs 之前和 18:00hrs 之后，HTTP 流量将允许透过。一个时间范围能包含三个时间段。例如：

工作日的办公时间可能包含下列时间段：

- 9:00 到 13:00 Hrs 之间的午餐前时间段
- 14:00 到 18:30 Hrs 之间的午餐后时间段

周末的办公时间可能包含下列时间段：

- 从 9:00 到 12:00 Hrs

这个变动的时间段能设定成单一的时间范围。访问规则可在时间段的基础上激活。

9.8.4.1 时间范围设定参数

表 9.11 说明了可供时间范围使用的设定参数。

表 9.11. 时间范围设定参数

选项	说明
Time Range drop-down list	选择 "Add New Time Range" 以增加新的时间范围或从下拉表中选择现有的时间范围。
Time Range Name	为时间范围输入名字。
Schedule drop-down list	选择 "Add New Schedule" 以增加新的日程表或从下拉表中选择日程表。
Days of Week	为日程表设定天数。
Time (hh:mm)	为日程表以hh:mm格式设定时间窗口。

9.8.4.2 增加时间范围

想要增加时间范围，请参考下列步骤：

1. 打开时间范围设定页面（请参考第 9.7.4.2 节**錯誤! 找不到參照來源。**））。
2. 在时间范围下拉表中选择“**Add New Time Range**”。
3. 在时间范围名称栏目中输入一个网域名称。
4. 在日程表下拉表中选择 “**Add New Schedule**”。
5. 选择一周内的某天。例如，从周日到周六。
6. 输入一天中的时间段。例如，从 08:00 到 18:00。
7. 点选 Add 按钮以創建新的日程表。

9.8.4.3 修改时间范围

想要修改时间范围，请参考下列步骤：

1. 打开时间范围设定页面（请参考**錯誤! 找不到參照來源。 錯誤! 找不到參照來源。**））。
2. 从时间范围下拉表中选择时间范围，或者点选时间范围列表中需要修改的时间范围的 图标。
3. 从时间范围下拉表中选择日程表。
4. 更改下列任一或所有栏目： Days of week and hours。
5. 点选 Modify 按钮以保存新的设定。

9.8.4.4 删除时间范围

想要删除时间范围，请点选待删时间范围前面的 图标。

9.8.4.5 在时间范围内删除日程表

想要在时间范围内删除日程表，请参考下列步骤：

1. 打开时间范围设定页面（请参考第 9.7.4.2 节**錯誤! 找不到參照來源。**））。
2. 点选待删时间范围列表前面的 图标，或者从时间范围下拉表中选择时间范围。
3. 从下拉表中选择日程表。
4. 点选 Delete 按钮以删除日程表。

9.8.4.6 时间范围实例

1. 創建时间范围 – 请参看图 9.28。

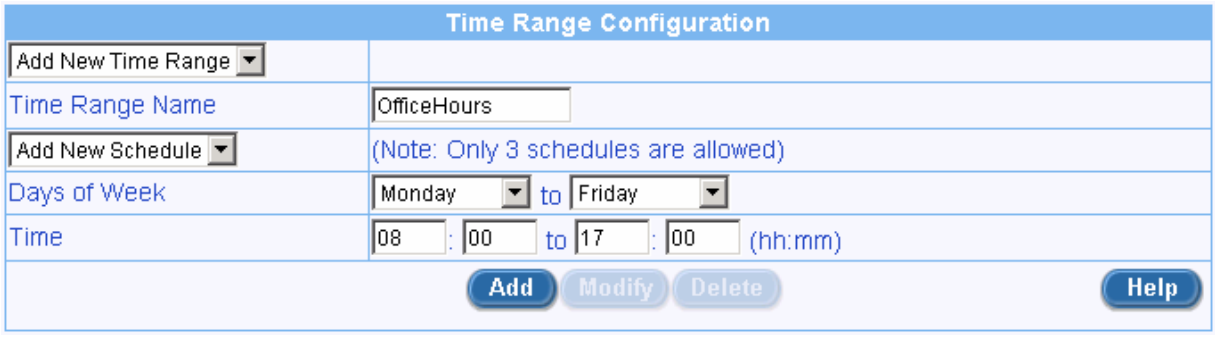


图 9.30. 时间范围实例 – 創建时间范围

2. 透过从时间范围下拉表中选择现有的时间范围，将时间范围联合到出站 ACL 规则。图 9.31 显示了 MISgroup1 在办公时间内拒绝了 FTP 访问。

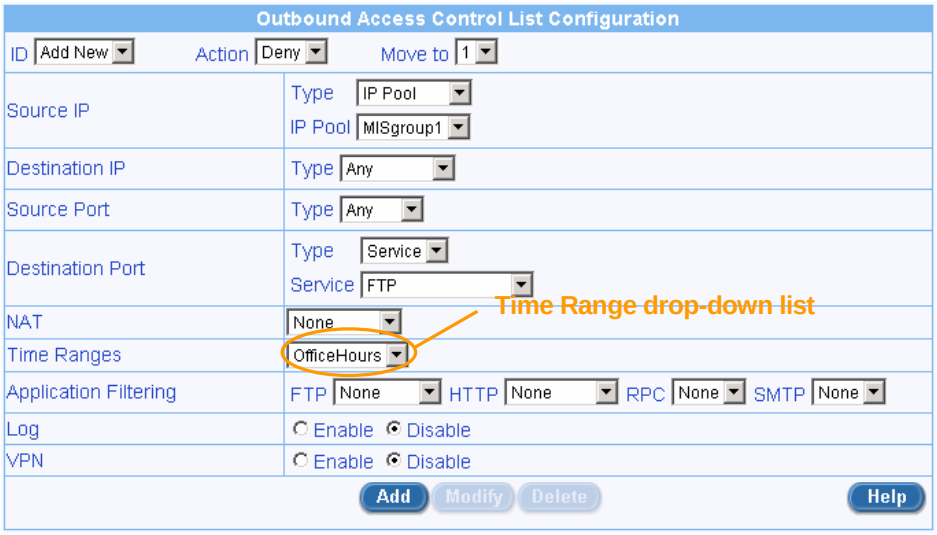


图 9.31. 时间范围实例 – 为 MISgroup1 在办公时间内拒绝 FTP 访问

9.9 防火墙统计表 – 防火墙 ➔ 统计表

防火墙统计表页面说明了关于活动联机的细节内容。图 9.32 显示了一个典型的防火墙对活动联机的统计表。要想参看已升級的统计表，点选 Refresh 按钮。

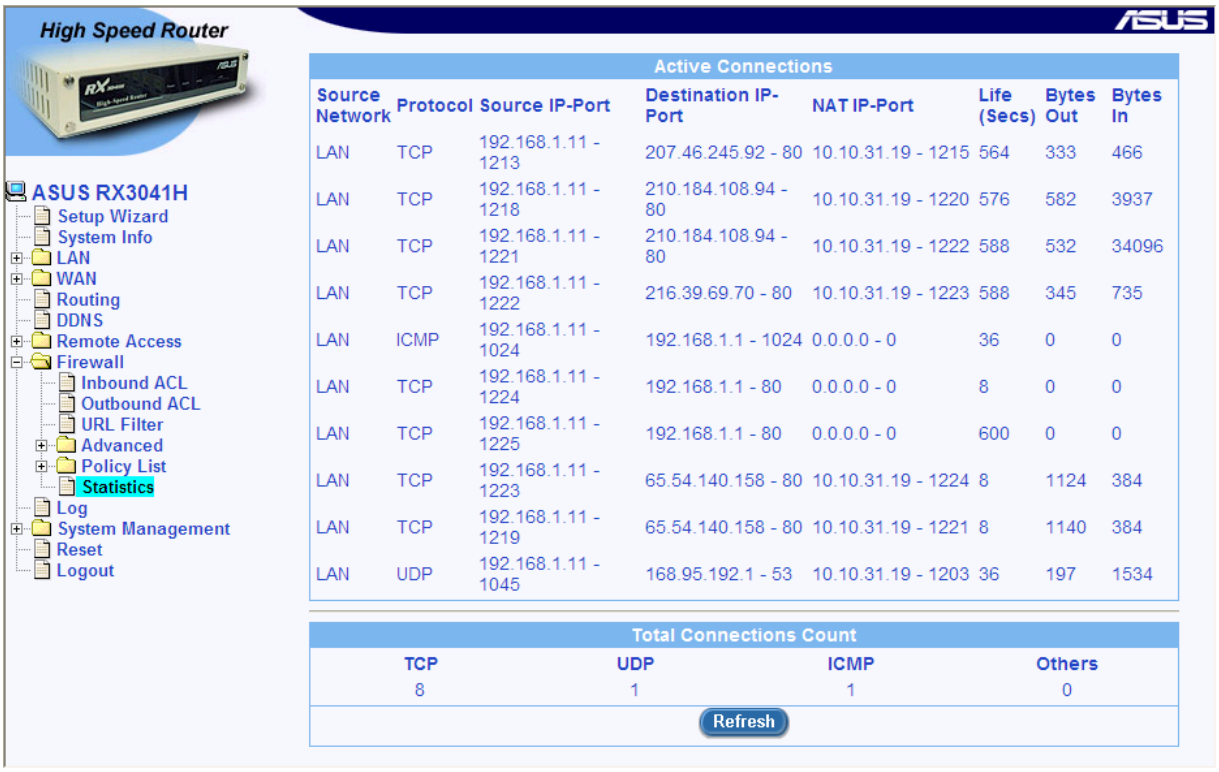


图 9.32. 防火墙活动联机统计表

10 设定远程访问

10.1 远程访问

网际网络安全路由器防火墙允许远距离工作者们利用以群组、用户与访问规则为基础的远程访问机制安全地访问企业内部网络。每个群组都与属于群组的用户登入之后启动的一套访问原则相关联。网际网络安全路由器保留了为远程访问群组定义的访问规则细节。这些访问列表定义了远程用户被允许访问的资源和应用到所有群组用户的休止时间。

当属于某群组的用户透过网际网络或本地网络登入，网际网络安全路由器防火墙启动了与群组想关联的访问规则，并創建了与用户相关联的动态规则。这些动态规则可资每个与用户的联机参考。一旦用户脱离了网际网络安全路由器或以防休止时间的来临，它们将被删除。

一个典型的为远程访问进行的设定包括下列举措：

- 增加/修改/删除新用户群组和群组用户的信息（包括用户名、密码等）。
- 增加/修改/删除群组访问规则。

10.2 管理用户群组以及用户

远程访问选项允许您设定用户和群组。

10.2.1 用户群组设定参数

表 100.1说明了可供远程访问用户群组以及用户使用的设定参数。

表 100.1. 用户群组设定参数

选项	说明
User Group	
User Group Drop-down list	选择 “Add New User Group” 以增加新的群组或从下拉表中选择一个现有的群组。
User Group Name	为您将要增加的群组输入一个独有的用户群组名。
Group State	点选Enable 或 Disable 按钮以开启或关闭群组。关闭群组将迫使所有的用户从已登入的用户群组中断开。所有用户的进一步注册将被关闭。开启群组将允许所有的群组用户登入。
Inactivity Timeout	输入终止的时间段长度，当无信息流经联机时，此长度将被用来删除与用户相关的会议。
User	
User Drop-down list	选择 “Add New User” 以增加新的用户或从下拉表中选择一个现有的用户。
User Name	为您将要增加的群组输入一个独有的用户名。

选项	说明
User State	点选Enable 或 Disable 按钮以开启或关闭用户。关闭用户将迫使用户断开。那个特定用户的进一步注册将被关闭。开启用户将允许那个特定用户登入。
Password	输入用户密码。

10.2.2 增加用户群组与/或用户

想要增加用户群组与新用户，请参考下列步骤：

1. 打开用户群组设定页面（请参考第 10.2.2 节**錯誤! 找不到參照來源。**）。
2. 从用户群组下拉表中选择 “**Add New User Group**” 。
3. 在用户群组名称栏目中输入一个名字。请确认此名字在现有的群组中无重名。注意，群组名字 is case sensitive。例如， Group1 与 group1 被视作独立的群组。
4. 在群组状态区目中点选 “Enable” 或 “Disable” 按钮以开启或关闭本群组。
5. 输入休止时间段长度。预设的长度为 300 秒。
6. 如果您想要增加用户到新创建的群组，请继续下列步骤；否则，请跳至第 12 步来完成设定。
7. 从用户下拉表中选择 “**Add New User**”。
8. 在用户名称栏目中输入一个独有的名字。
9. 在用户状态区目中点选 “Enable” 或 “Disable” 按钮以开启或关闭此用户。
10. 在密码栏目中输入此用户的密码。
11. 再次确认用户密码。请确认您与上步输入的是相同的密码。
12. 点选 Add 按钮以創建新的群组与新用户。

想要增加新用户，请参考下列步骤：

1. 打开用户群组设定页面（请参考第 11.2.2 节**錯誤! 找不到參照來源。**））。
2. 从用户群组下拉表中选择一个现有的群组。
3. 在用户下拉表中选择 “**Add New User**”。
4. 在用户名称栏目中输入一个独有的名字。
5. 在用户状态区目中点选 “Enable” 或 “Disable” 按钮以开启或关闭此用户。
6. 在密码栏目中输入此用户的密码。
7. 再次确认用户密码。请确认您与上步输入的是相同的密码。
8. 点选 Add 按钮以增加新用户。

10.2.3 修改用户群组或用户

想要修改用户群组与/或用户，请参考下列步骤：

1. 打开用户群组设定页面（请参考第 11.2.2 节**錯誤! 找不到參照來源。**））。
2. 从用户群组下拉表中选择一个现有的群组。如果您只是想修改现有用户的属性，请跳至第 4 步。

3. 在群组状态与/或休止时间栏目中进行您想要的更改。如果您并不想修改现有群组中用户的属性请跳至第 6 步。注意，群组名不能作任何更改。要想改变群组名字，您必须首先删除现有的群组，并用您想要的名字创建一个新的群组。
4. 从用户下拉表中选择一个现有的用户。
5. 在用户状态、密码和密码确认栏目中进行您想要的更改。注意，用户名不能作任何更改。要想改变用户名字，您必须首先删除现有的用户，并用您想要的名字创建一个新的用户。
6. 点选 Modify 按钮以保存新的设定。

10.2.4 删除用户群组或用户

想要删除用户群组，请参考下列步骤：

1. 打开用户群组设定页面（请参考第 11.2.2 节**錯誤! 找不到參照來源。**））。
2. 从用户群组下拉表中选择一个现有的用户群组。
3. 点选 Delete 按钮以删除此用户群组。注意，用户群组只有在所有属于群组的用户都被删除后才能删除。

想要删除用户，您只需点选用户群组设定页面远程用户表中待删用户的 图标，或参考下列步骤：

1. 打开用户群组设定页面（请参考第 11.2.2 节**錯誤! 找不到參照來源。**））。
2. 点选远程用户表中待删用户的 图标，或从用户下拉表中选择一个用户。
3. 点选 Delete 按钮以删除此用户。

10.2.5 用户群组和用户设定实例

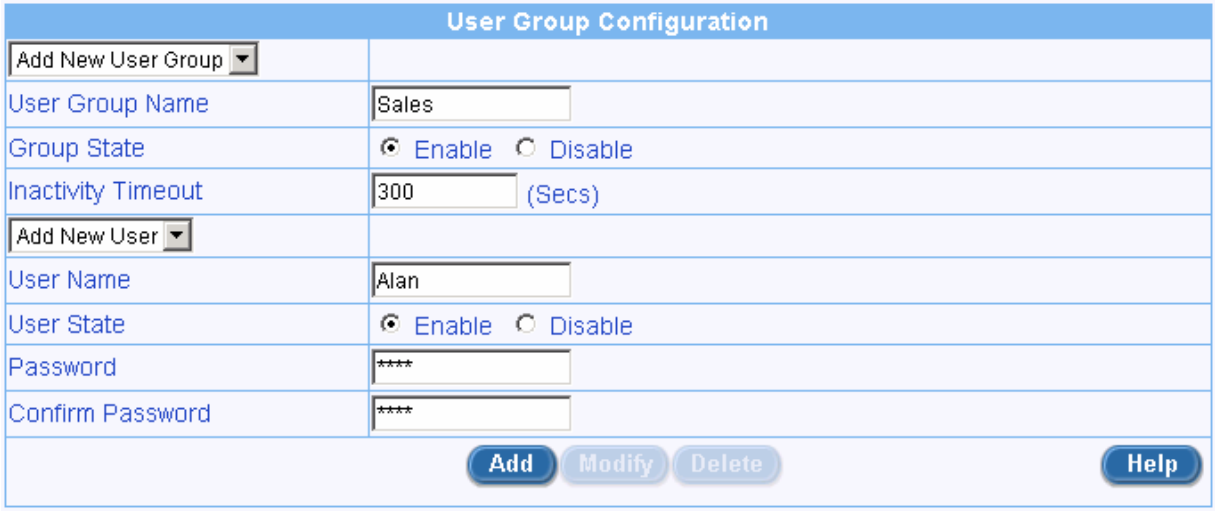


图 10.1. 用户群组和用户设定实例

实例

图 10.1 显示了屏幕上的条目：

- 增加新的用户群组和新用户
  - 群组 “Sales”

- 用户 “Alan”

10.3 设定群组 ACL 规则

群组 ACL 用来控制本地或远程群组访问的特权。除了两个附加选项（规则类型和群组名字，请参看**錯誤! 找不到參照來源。**）之外，它的设定与防火墙入站/出站 ACL 规则十分类似。关于设定群组 ACL 规则的详细步骤，请参考第 9.4 或 9.5 节。

10.3.1 群组 ACL 特殊设定参数

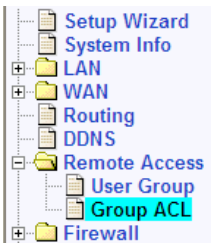
表 10.2 说明了群组 ACL 规则的特殊设定参数。剩下的设定参数与防火墙入站/出站ACL 规则相同。请参考表 9.2 和 表 9.3 以获得普通设定参数的详细信息。

表 10.2. 群组 ACL 特殊设定参数

选项	说明
Type 选择本规则所应用的流量的类型。	
Inbound	若规则为入站信息设定时请选择此项。
Outbound	若规则为出站信息设定时请选择此项。
Group 从群组下拉表中选择本规则应用的对象。注意，想要设定群组ACL规则，必须先设定好用户群组。请参考第 **錯誤! 找不到參照來源。** 节来进行用户群组设定。	

10.3.2 新增群组的 ACL 规则 Add a Group ACL

请依照下列介绍来新增一组群组 ACL 规则:



4. 藉由点选 **Firewall ➔ Remote Access ➔ Group ACL** 选单的方式来开启时间范围设定页面。
5. 自下拉式选单中选择 “**Add New**” 。
6. 从“**Action**”下拉式选单中设定您所要进行设定的动作 (Allow 或 Deny)。
7. 从规则类型的下拉式选单中选择 Outbound 或 Inbound 规则。
8. 从群组下拉式选单中选择一个群组。
9. 从以下字段中进行变更设定: 来源/目的地 IP, 来源/目的地连接端口, 通讯协议, NAT, 时间范围, 应用程序过滤, 与 登录。 请参阅 表 9.2 中关于这些字段的解释。图 9.10 是表示如何創建一规则来自 IP 地址 192.168.1.15 的主机拒绝一出端口 HTTP 传输。

图 10.2. 群组 ACL 设定范例

10. 藉由从下拉式选单中的“**Move to**”选项来指定一组规则的优先级。请注意！选单中的数字代表优先顺位的高低，其中数字 1 代表优先级最高者。优先级越高者将比优先级越低者较先受到防火墙的检查。

11. 点选 Add 按键以创建一组新的 ACL 规则。新的 ACL 规则将会被显示在 ACL 设定页面下方的 ACL 群组列表中。

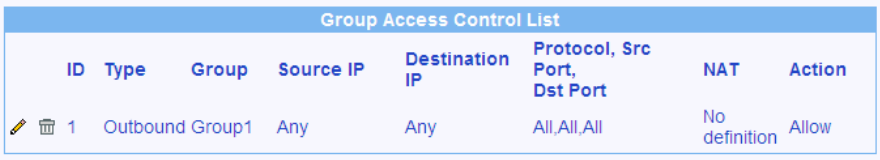


图 10.3. ACL 群组列表

10.3.3 修改 ACL 群组规则

请依照下列介绍来修改 ACL 群组规则:

12. 藉由点选手动 **Firewall ➔ Remote Access ➔ Group ACL** 选单来开启时间范围设定页面。

13. 请点选 图标来修改 ACL 列表中的规则，或是从下拉式选单中的“**ID**”项目来选择规则所代表的号码。

14. 在以下各字段中进行您所要进行的设定: 动作, 群组规则类型, 群组, 来源/目的地 IP 地址, 来源/目的地连接端口, 通讯协议, NAT, 时间范围, 应用程序过滤, 与登录。请参考表 9.2 与表 10.2 中针对这些字段的解释。

15. 点选 Modify 按键来变更此一 ACL 规则。针对此一 ACL 规则的新设定将会显示在 ACL 群组设定页面下半部的 ACL 群组列表中。

10.3.4 删除 ACL 群组规则

如欲删除 ACL 群组规则，您只要依照下列指示点选规则前方的 图标即可进行删除。:

16. 藉由点选 **Firewall ➔ Remote Access ➔ Group ACL** 选单来开启时间范围设定页面。

17. 点选规则中的 图标来删除 ACL 群组列表中的规则，或是从下拉式选单中的“**ID**” 项目选择代表规则的号码。

18. 点选 Delete 按键来删除此一 ACL 规则。请注意！被删除的 ACL 规则将会自设定页面下半部的 ACL 群组列表中删除。

10.3.5 显示既有的 ACL 规则

如欲查看既有的 ACL 规则，您只要藉由点选开启 **Firewall ➔ Remote Access ➔ Group ACL** 选单来开启 ACL 群组设定页面。

10.4 远程用户登入步骤

对于属于某个用户群组联机到路由器上的用户而言，他/她必须首先进行特别的登入以激活用户群组规则；否则，路由器将拒绝所有用户的联机请求。为登入路由器和激活有关的访问原则，某个用户群组的用户可在浏览器内输入下列 URL。

http://<IP Address>/login

登入控制台将出现，如图 10.4 所示

图 10.4. 登陆控制台

在成功登入之后，屏幕将如图 10.5 所示。

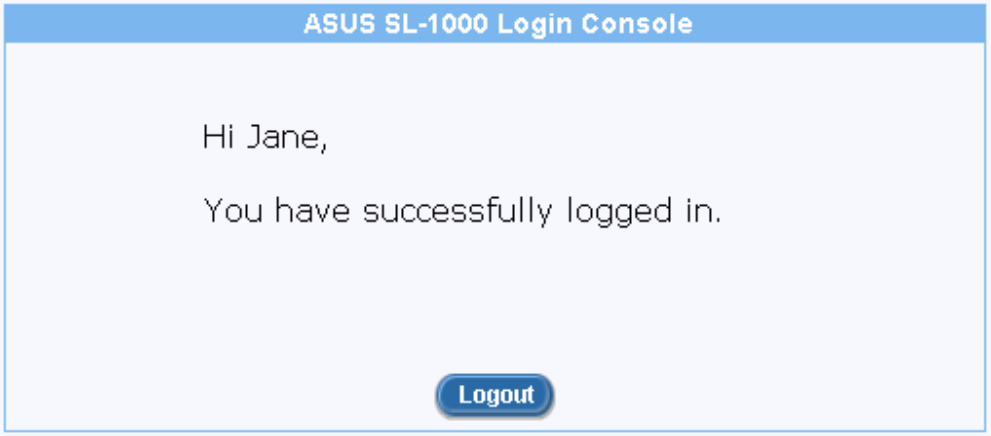


图 10.5. 登入状况屏幕

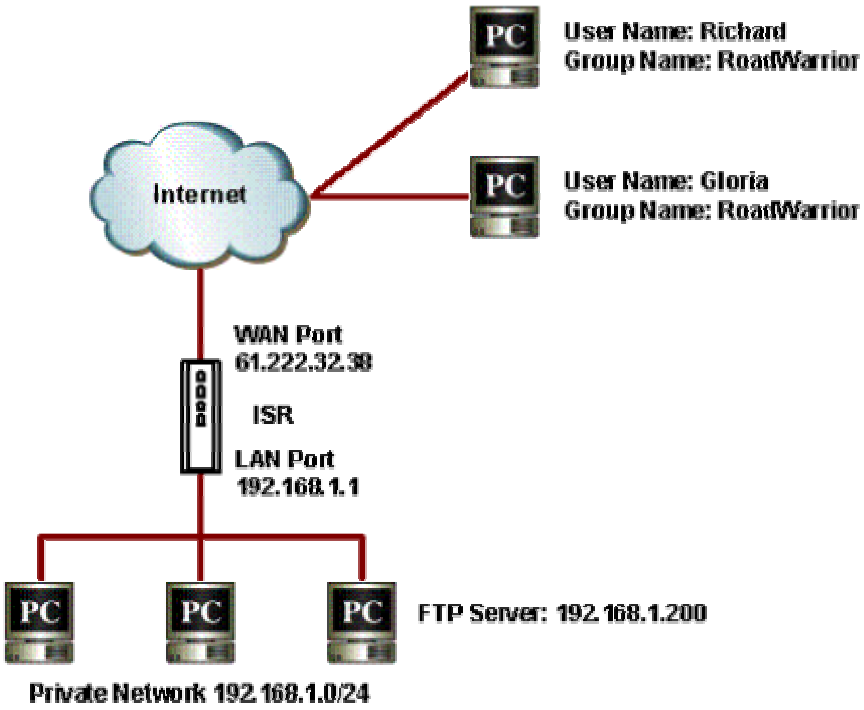


图 10.6. 对入站远程访问进行的网络诊断

10.5 为远程访问设定防火墙

远程访问常被用来支持企业的移动用户访问公司的网络而不牺牲掉安全性。远程访问所需要的设定路由器的步骤最好由一个实例来解释。下文说明了远程用户 Richard 和 Gloria 访问处于被保护的网络（例如公司局域网络）之内的 FTP 服务器时对路由器进行设定所需要的步骤。图 10.6 显示了对此实例进行的网络诊断。

1. 如需要创建远程访问用户和群组。图 10.7 说明了创建一个新用户 Gloria 的过程。想要知晓关于如何为远程访问增加新用户与/或新用户群组更多细节，请参考第**錯誤! 找不到參照來源。**节 **錯誤! 找不到參照來源。**。

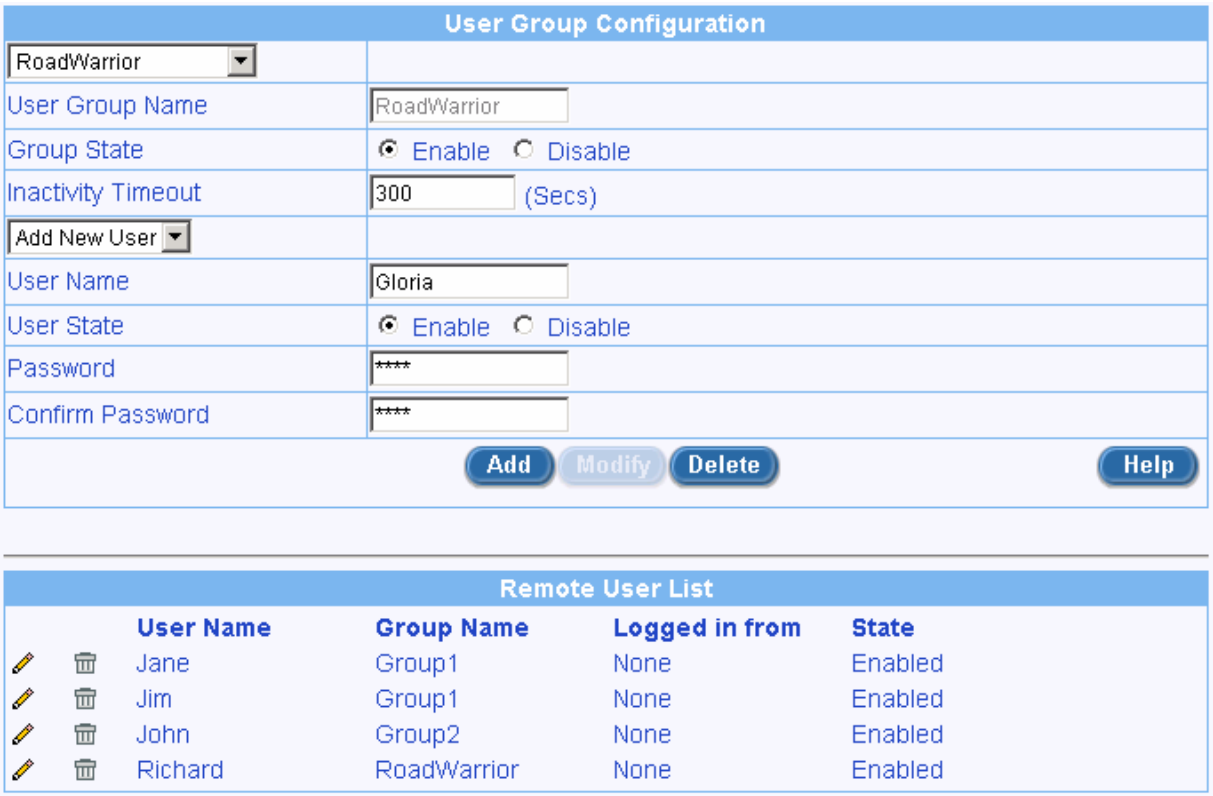


图 10.7. 用户与用户群组设定实例

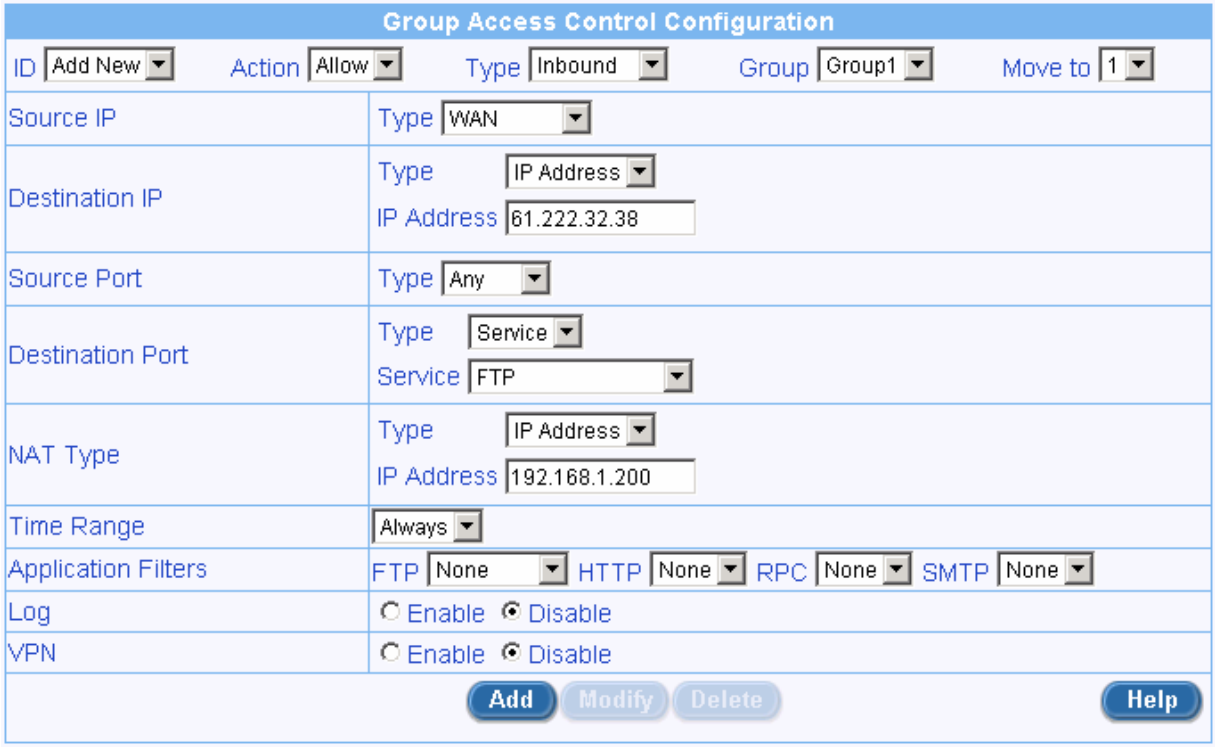


图 10.8. 群组 ACL 设定实例

2. 創建入站群组 ACL 规则（请参看图 10.8）以允许远程访问用户 Richard 和 Gloria 访问企业网络内的 FTP 服务器。
3. 远程用户 Richard 和 Gloria 可在浏览器内输入下列 URL，以登入到路由器上访问 FTP 服务器：

http://61.222.32.38/login

11 系统管理

本章说明了您可利用设定管理器完成的管理任务：

- 设定系统服务
- 修改密码
- 修改系统信息
- 修改系统日期和时间
- 重新设定、备份和保存系统设定
- 升级韧体
- 退出设定管理器

您可从系统管理菜单访问这些任务。

11.1 设定系统服务

如图 11.1 所示，您可使用系统服务设定页面来开启或关闭网际网络安全路由器支持的服务功能。所有的服务, 防火墙, DNS, DHCP 和 RIP 都在这里被开启。想要关闭或开启个人服务，请参考下列步骤：

1. 以管理员身份登入设定管理器，点选 **System Management** 菜单，然后点选 **System Services** 子菜单。系统服务设定页面将如图 9.9 所示。
2. 点选相应的“Enable” 或 “Disable” 按钮以开启或关闭您想要的服务。
3. 点选 Apply 按钮以保存修改。

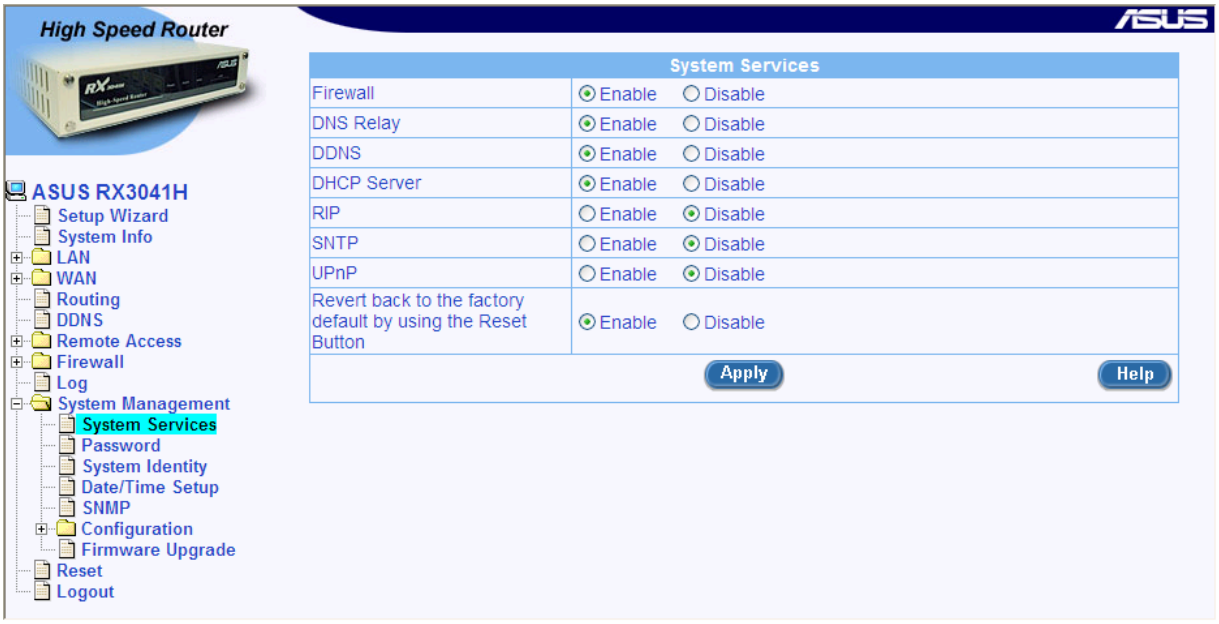


图 11.1. 系统服务设定页面

11.1.1 变更登入密码

当您第一次登入设定管理员，您可以使用预设的用戶名称与密码:admin 与 admin 。系统会允许两种用戶登入，分别为系统管理员（administrator: username:admin）与访客（guest:username:guest）。其中系统管理员具有权力去修改设定，而访客则只能检视系统设定。至于这两组用戶的密码则为 admin 与 guest，系统管理员可针对密码进行变更。

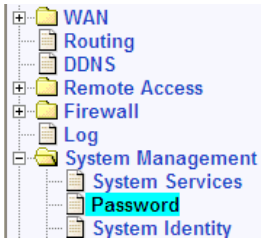

Note

此处的用戶名称与密码只用来登入设定管理员之用，此一帐号密码与您用来与 ISP 联机的帐号密码不同。

请依照下列步骤来变更密码:

4. 藉由点选 **System Management ➔ Password** 选单来开启密码设定页面。
5. 输入既有的密码在 **Login Password** 字段。
6. 在 **New Password** 字段输入新的密码，并在 **Confirm New Password** 字段重新输入一次密码。

   密码可以是十六位数字，当您登入时，您必需在上方与下方的字段输入新的密码。



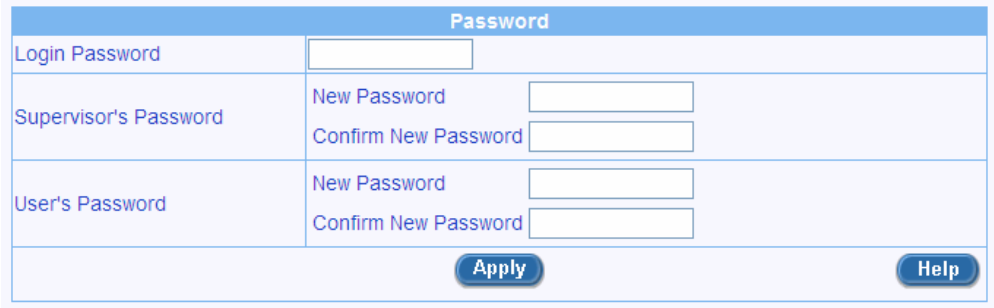


图 11.2. 密码设定

7. 点选 Apply 按键来储存新的密码。请注意只有在密码输入正确并在正确的字段才会生效。

11.1.2 设定管理站

有时候，您可能想要限制主机对路由器进行设定。在默认值中，只要输入的帐号与密码正确，则可让系统管理员从任何计算机登入。这样的作法可让未经认证者在知道设定管理员接口的帐号与密码的情况下进行登入。在此设定页面中您可利用输入单一 IP 地址、IP 地址范围或网络地址与子网掩码，最多设定八组的管理站。


WARNING

若管理站群组未经设定，则管理员可从任何地方登入路由器。然而，若有一组或更多的管理站群组被设定，则只有经过设定之特定管理站群组可以设定路由器。若您忘记管理群组的设定，您将无法存取路由器的设定管理员接口，除非按下路由器的重置键进行重置。

(i) 管理站参数设定

表 11.1 叙述管理站设定页面中可进行设定的参数。

表 11.1. 管理站参数设定

字段	叙述
ID	
Add New	点选此选项来新增一组新的管理群组。
Number	从下拉式选单中选择管理群组以变更设定。
Address Type 本选项可让您选择您要如何指定管理站群组使用的IP地址。在此共有三种选项可供设定，分别是: IP 地址、范围与子网络。	
IP Address	本选项可让您指定管理站的IP地址。
Address	指定一组适当的IP地址。
Range	本选项可让您从管理站群组指定IP地址范围。当本选项被选择，则以下的字段便可以进行设定:
Begin	输入起始的IP地址范围。
End	输入中止的IP地址范围。
Subnet	本选项可让您指定所有连接到相同IP子网络的计算机作为一管理站群组。当本选项被选择，则以下的项目便可以加以输入:
Network Address	输入适当的IP地址。
Subnet Mask	输入对应的子网掩码。

(ii) 新增一组管理站群组

请依照以下介绍来新增一组管理站群组:

8. 藉由点选 **System Management ➔ Password** 选单来开启密码设定页面。
9. 从“**ID**”下拉式选单中选取 “**Add New**” 。
10. 在以下三选项选择 “Address Type”（地址类型） – **IP Address**, **Range** 与 **Subnet**， 接着请输入您想要输入的 IP 地址信息。

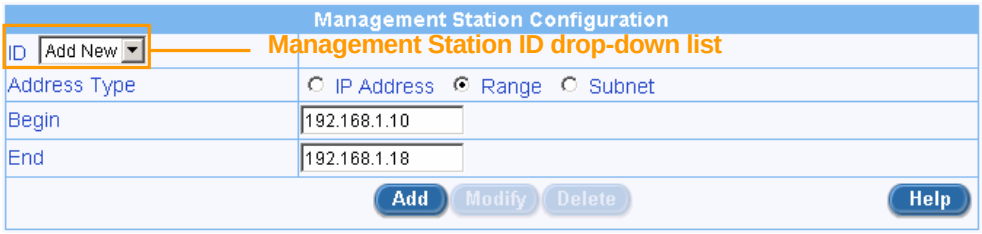


图 11.3. 管理站设定

11. 点选 Add 按键来新增一组新的管理站群组。您将可看到新增的管理站群组摘要显示在同一设定页面。

图 11.4. 管理站摘要

(i) 变更管理站群组

请依照以下介绍来变更管理站群组:

12. 藉由点选 **System Management ➔ Password** 选单来开启密码设定页面。
13. 从 **ID** 下拉式选单中选择一管理群组。
14. 请在“**Address Type**”项目中设定想要进行的变更并输入对应的 IP 地址信息。
15. 点选 Modify 按键来变更设定。

(i) 删除管理站群组

如欲删除管理站群组，您只要点选选项前的 图标 (在管理站摘要列表中)即可加以删除，或是依照以下介绍进行删除:

16. 藉由点选 **System Management ➔ Password** 选单开启密码设定页面。
17. 从“**ID**”下拉式选单中选择一组管理群组的号码。
18. 点选 Delete 按键来删除管理站群组。

11.2 修改系统信息

如图 11.5 所示，您可利用系统信息设定页面来输入系统的特定信息，如系统名称（对于设备来说的唯一的名称）、系统位置（设备摆放的位置）以及设备联系人的信息。注意，所有的栏目都只允许字符名称。当您完成了系统特定信息的输入之后，请点选 Apply 按钮以保存修改。

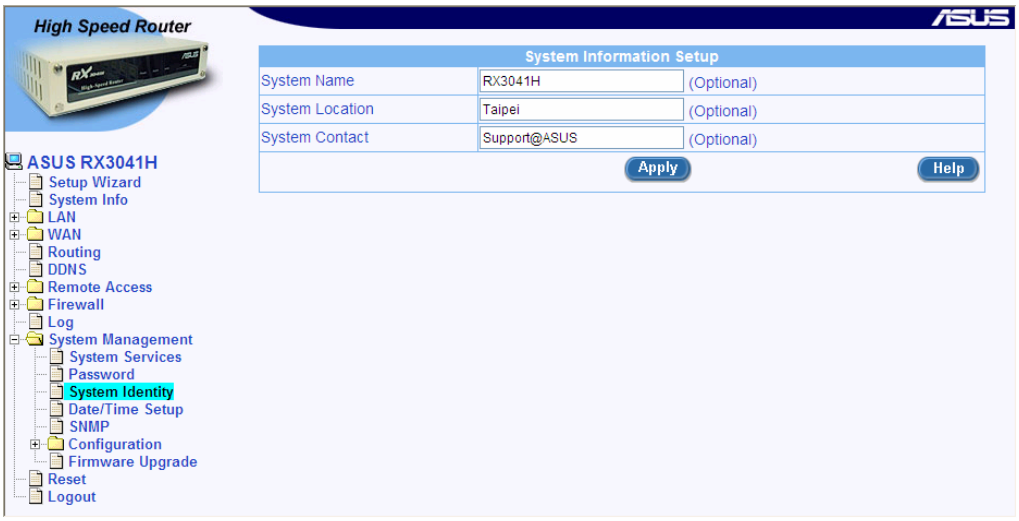
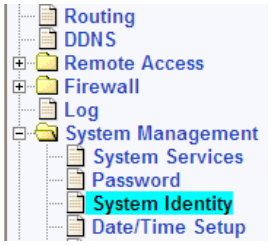


图 11.5. 系统信息设定页面

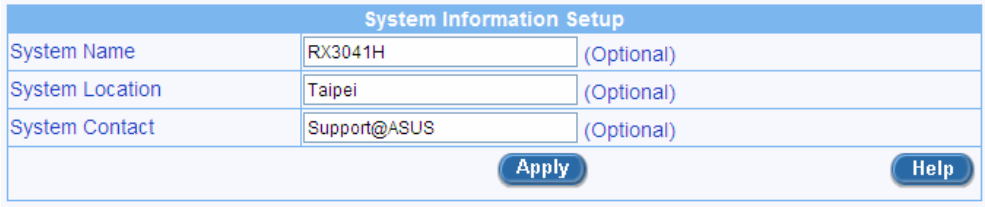
11.3 设定系统辨识

一些特定的系统信息，像是系统名称（本装置的特定名称）、系统位置（本装置的所在位置），与在装置中的个人联络信息都可以在系统辨识设定页面中进行设定。

请依照以下介绍来变更特定的系统信息:



19. 藉由点选 **System Management ➔ System Identity** 选单来开启系统辨识设定页面。
20. 变更系统名称、系统位置与联络信息等想要进行的设定。请注意！在此字段中，您可输入任何数字字母。
21. 点选 Apply 按键来储存设定值。



11.4 设定时间与日期

在路由器中会储存目前日期与时间的纪录，而这份资料是用来计算与回报关于系统运作的资料之用。

Note

变更路由器上的日期与时间并不会同时变更您 PC 上的日期与时间。

在路由器中，便没有实时时钟，然而，路由器可由外部时间服务器取得正确的日期与时间信息。您可以设定最多五组时间服务器。请注意！在 **System Services** 设定页面中的 SNTP 服务必需开启，如此路由器才能存取外部时间服务器的资料。

11.4.1 日期/时间 参数设定

以下列表叙述参数设定中可供设定的日期与时间设定。

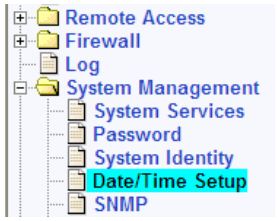
表 11.2. 日期/时间 参数设定

字段	叙述
Date	本日期当路由器重置并且无 SNTP 服务时，可以重置到 1/1/2000。若 SNTP 服务字段设定为开启且可存取则正确的时间将会显示在此字段。
Time	当路由器重置或无 SNTP 服务时，可以重置到 00:00:00。若 SNTP 服务字段设定为开启且可存取则正确的时间将会显示在此字段。
Time Zone	输入您所在地的时区。
SNTP Server 1 – 5	输入 SNTP 服务器的 IP 地址。您可以设定最多五组的 SNTP 服务器以取得正确的日期与时间。
Update Interval	以分钟为单位输入路由器从时间服务器中升級日期与时间的间隔。此字段的默认值为 60 分钟。

11.4.2 维护日期与时间

日期与时间可藉由在 **Date** 与 **Time** 字段输入正确的日期与时间设定值来让路由器自身进行维护。请注意！当 RX3041H 路由器每次进行重置动作后，您必需以手动方式再次进行日期与时间的设定。

建议您使用外部时间服务器来协助维护您路由器中正确的日期与时间设定。请依照以下设定来 SNTP 服务器以维护您路由器中的日期与时间设定:



22. 藉由点选 **System Management ➔ Date/Time** 选单来开启日期/时间设定页面。
23. 从"**Time Zone**"下拉式选单中选择您所在地的时区。
24. 输入最多 5 组 SNTP 服务器的 IP 地址来存取您所在地的日期与时间资料。
25. 在"**Update Interval**" 字段输入时间升級的间隔时差。本项目的默认值为 60 分钟。

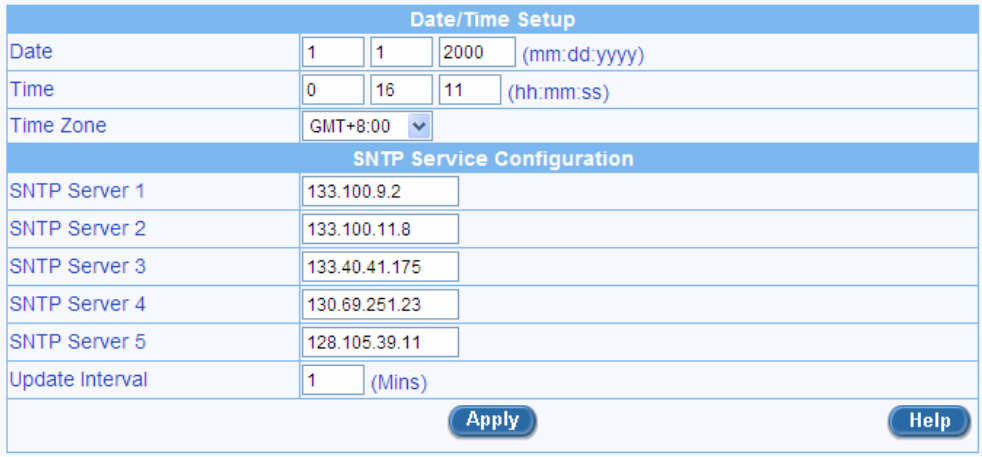


图 11.6. 日期与时间设定页面

26. 点选 Apply 按键以储存设定值。

11.4.3 检视系统的日期与时间

藉由点选 **System Management ➔ Date/Time** 选单来开启日期/时间设定页面，以检视系统的日期与时间。

11.5 SNMP 设定

SNMP (简易网络管理协议) 如同其名称一般主要是用来作为网络管理的用途。您可以利用 SNMP 设定页面来开启或关闭 SNMP 支持功能。

11.5.1 SNMP 参数设定

表 11.3 叙述在 SNMP 设定中可以进行设定的参数项目。

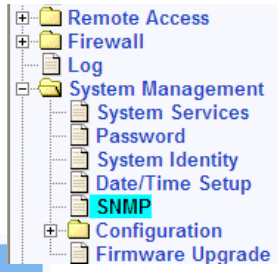
表 11.3. 固定 DHCP Lease 参数设定

字段	叙述
SNMP	点选 “Enable” 或 “Disable” 键来开启或关闭 SNMP 的支持。

字段	叙述
RO Community Name	群组字串为一清楚的文字符串，这些文字符串是被用来作为 SNMP 管理站与 RX3041H 间的密码。此一 “只读” 群组名称是被用来作为 SNMP 管理站在 RX3041H 中读取设定之用。
RW Community Name	群组字符串为一清楚的文字符串，而这些文字符串是作为 SNMP 管理站与 RX3041H 间的密码。此一 “读与写” 群组名称是由 SNMP 管理站使用，用来在 RX3041H 中读取设定之用。
Trap Address	由 RX3041H 所传送的 Trap 讯息，是用来告知 SNMP 管理站 RX3041H 正有某些事件发生。此一字段可用来输入负责接收来自 RX3141H 中 trap 讯息之 SNMP 管理站的 IP 地址。

11.5.2 设定 SNMP

27. 请藉由点选 **System Management ➔ SNMP** 选单来开启 SNMP 设定页面。
28. 点选 “Enable” 或 “Disable” 按键来开启或关闭 SNMP 功能支持。
29. 请输入 RO (只读) 与 R/W (读与写) 的通讯名称。
30. 输入可从 RX3041H 中接收 trap 讯息的 SNMP 管理站 IP 地址。



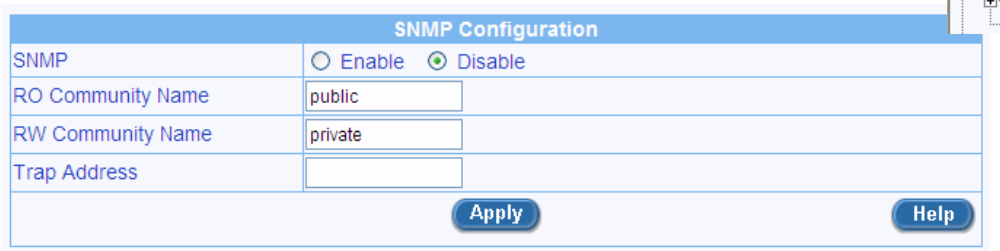


图 11.7. SNMP 设定

31. 请点选 Apply 键来储存设定值。在设定页面下方的设定列表中，您可从既有的 SNMP 设定列表确认您的设定。

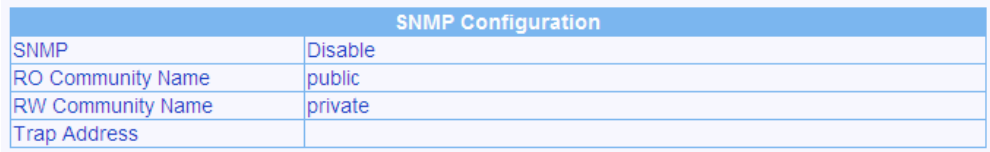


图 11.8. 既有的 SNMP 设定

11.6 系统设定管理

11.6.1 重新进行系统设定

有时，您可能会想要回复设定至出厂预设值的设定来消除由于不正确的系统设定导致的问题。请参考下列步骤来重新启动系统设定：

1. 以管理员身份登入设定管理器，点选 **System Management** 菜单，点选 **Configuration** 子菜单,然后点选 **Default Settings** 子菜单。预设设定的设定页面将如图 9.9 所示。

2. 点选 Apply 按钮来回复系统设定至出厂默认值。注意，网际网络安全路由器将重新启动以使出厂默认值生效。

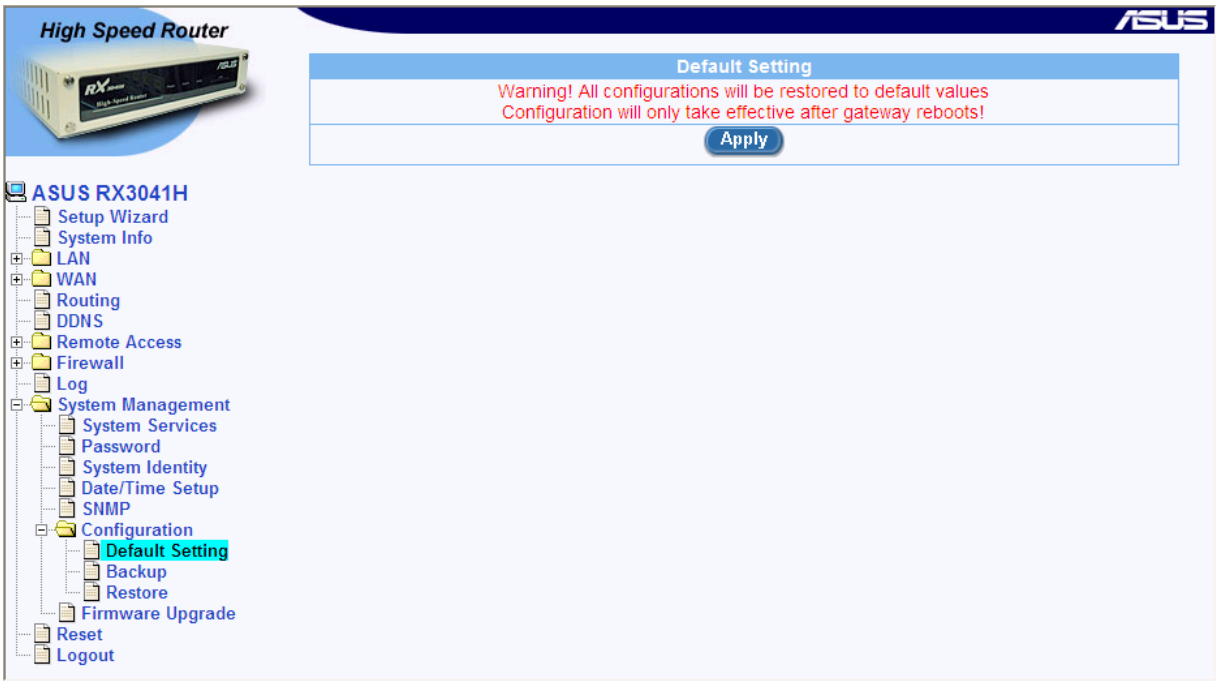


图 11.9. 预设设定的设定页面

有时，您可能会发现您无法访问网际网络安全路由器，例如，您忘记了密码。唯一办法就是重新将系统设定回复至出厂默认值，请参考下列如何使用 Reset 键的步骤：

1. 断开路由器的电源。
2. 重新接上路由器的电源，等待约 5~6 秒后按下 Reset 键.
3. 等待约 5~6 秒后，再次按下 Reset 键。此时网际网络安全路由器将回复至出厂默认值。如果您这时改变了主意，您可再次按下 Reset 键，或关闭电源以取消这次的动作。

11.6.2 备份系统设定

请按照下列步骤来备份系统设定：

1. 以管理员身份登入设定管理器，点选 **System Management** 菜单，点选 **Configuration** 子菜单，然后点选 **Backup** 子菜单。备份系统设定页面将如图 9.9 所示。

2. 点选 Apply 按钮以备份系统设定。

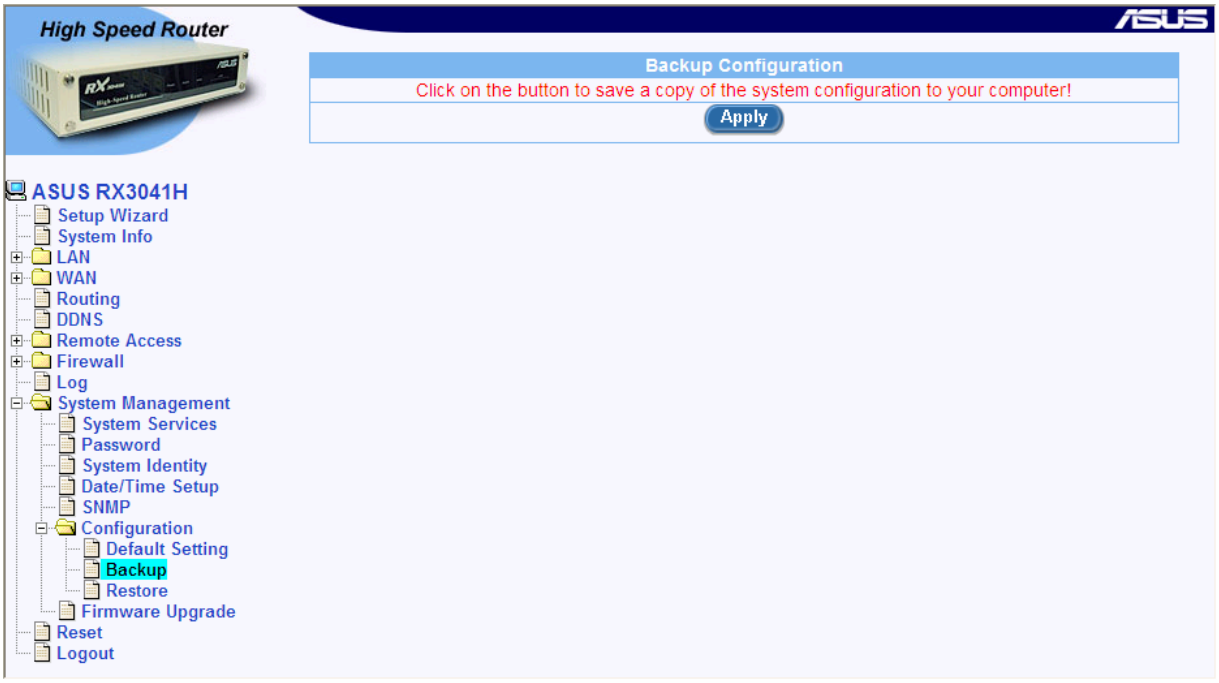


图 11.10. 备份系统设定页面

11.6.3 保存系统设定

请按照下列步骤来保存系统设定：

1. 以管理员身份登入设定管理器，点选 **System Management** 菜单，点选 **Configuration** 子菜单，然后点选 **Restore** 子菜单。保存系统设定页面将如图 9.9 所示。

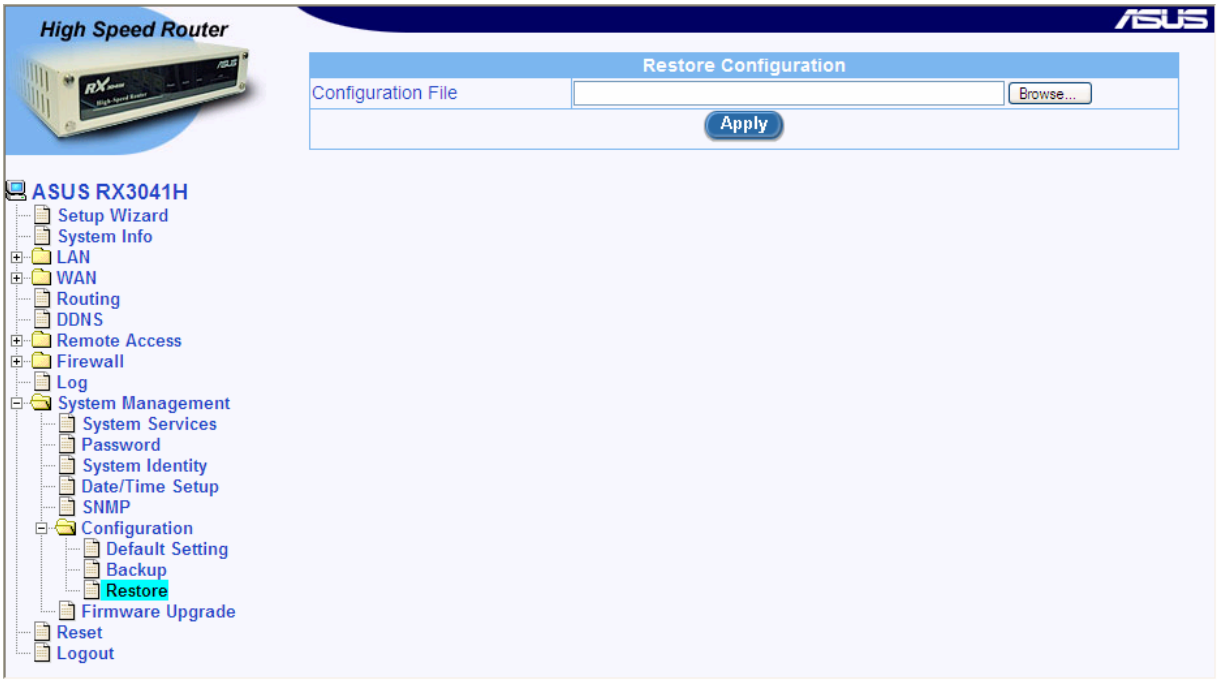


图 11.11. 保存系统设定页面

2. 输入您想保存在 “Configuration File” 中的系统设定档案的路径与名称。 除此之外，您也可以点选 Browse... 按钮以搜寻您硬盘上的系统设定档案。一个类似于图 11.16 的窗口将突然出现，提示您选择要保存的设定档案。

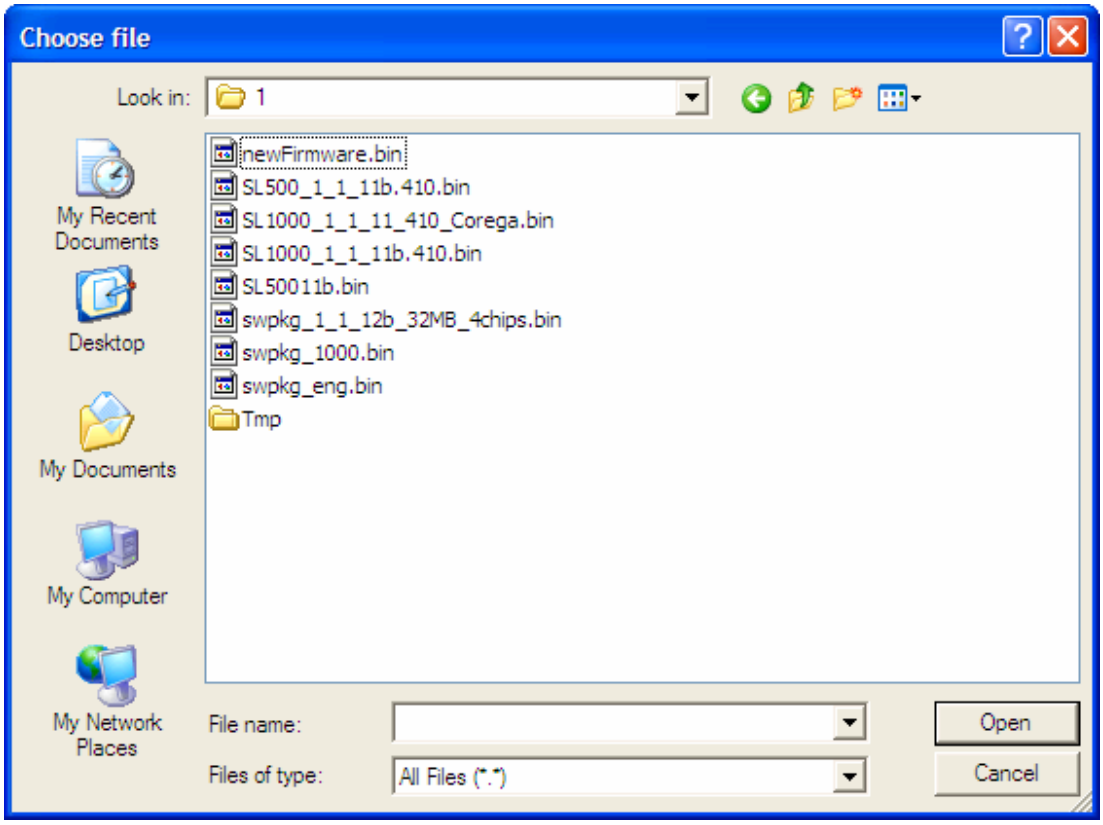


图 11.12. Windows 档案浏览器

3. 点选 Apply 按钮以保存系统设定。注意，网际网络安全路由器将重新启动以使新的系统设定有效。

11.7 升级韧体

华硕有可能不时地提供您升级路由器所运行的韧体的机会。所有的系统软件都被包含在一个单独的档案内，名为 *image*。 设定管理器提供了上传新 image 的简易方法。想要升级 image，请参考下列步骤：

1. 以管理员身份登入设定管理器，点选 **System Management** 菜单，然后点选 **Firmware Upgrade** 子菜单。韧体升级页面将如图 9.9 所示。

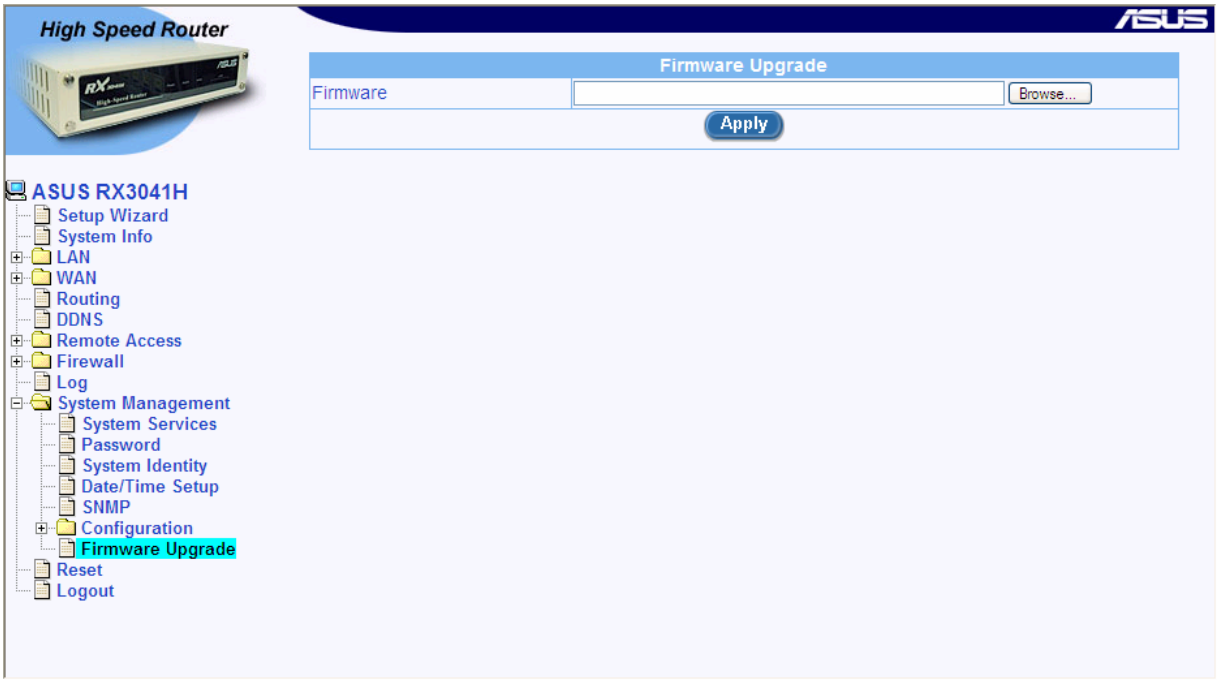


图 11.13. 韧体升级页面

2. 在韧体文字框输入韧体 image 档案的路径与名称。除此之外，您还可以点选 Browse... 按钮以从硬盘内寻找。

3. 点选 Apply 按钮以升级韧体。注意，可能要花费至少 5 分钟的时间来进行韧体升级。在韧体升级过程结束之后，网际网络安全路由器将重启系统以使新韧体生效。

11.8 重新设定 RX3041H 高速路由器

想要重新设定 RX3041H 高速路由器，在设定管理器 Reset 页面点选 Apply 按钮。

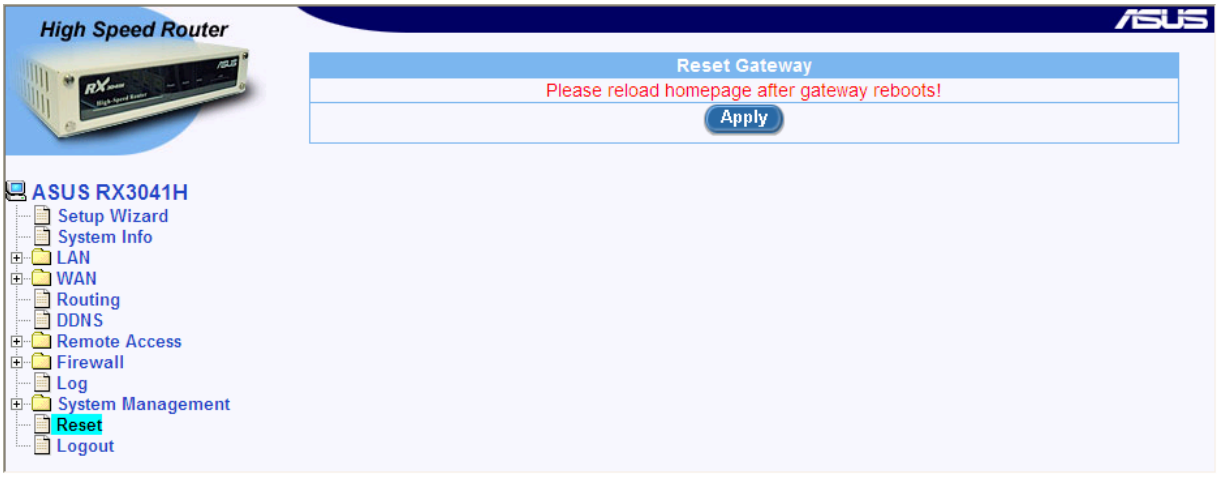


图 11.14. 设定管理器 Reset 页面

11.9 退出设定管理器

想要退出设定管理器，点选设定管理器退出页面的 Apply 按钮。如果您使用 IE 作为您的浏览器，一个类似于图 11.16 的窗口将提示您在关闭浏览器之前确认退出。

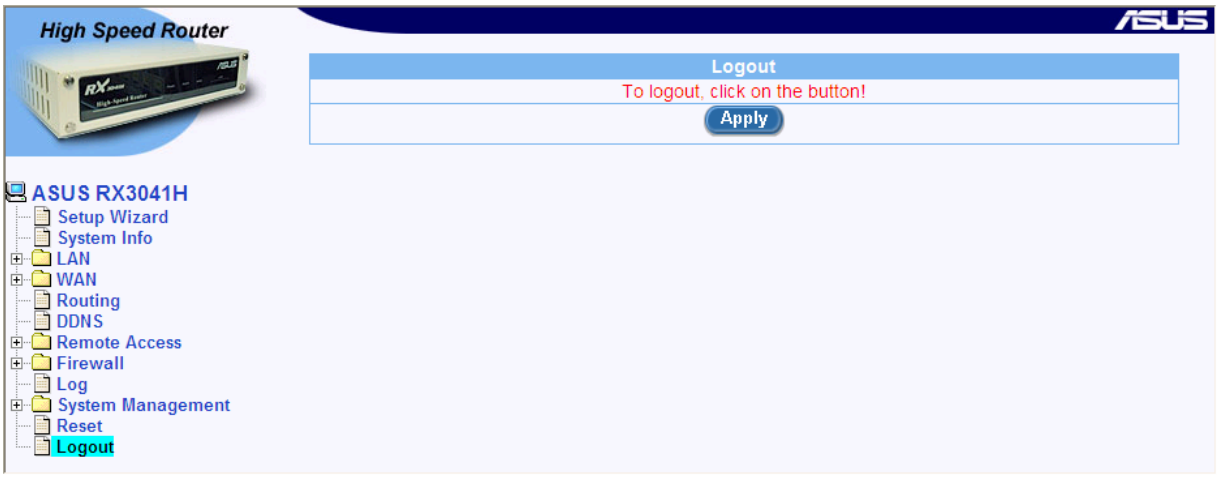


图 11.15. 设定管理器退出页面

图 11.16. 确认退出浏览器（IE）

.

A. ALG 设定

表 A.1 列出了支持的所有 ALG（Application Layer Gateway）。

表 A.1. 支持的 ALG

ALG/应用程序名称	**协议与埠**	**预先设定的服务名称**	**测试软件版本**
PCAnywhere	UDP/22	PC-ANYWHERE	pcAnywhere 9.0.0
RTSP-554	TCP/554	RTSP554	RealPlayer 8 Plus QuickTime Version 6
	UDP/53	DNS	
	TCP/80	HTTP	
RTSP-7070	TCP/7070	RTSP7070	RealPlayer 8 Plus
	UDP/53	DNS	QuickTime Version 6
	TCP/80	HTTP	
Net2Phone	UDP/6801	N2P	Net2Phone CommCenter Release 1.5.0
	TCP/80	HTTP	
	TCP/443	HTTPS	
	UDP/53	DNS	
CUSeeMe	TCP/7648	CUSEEME	CUSeeMe Version 5.0.0.043
	TCP/80	HTTP	
	UDP/53	DNS	
Netmeeting	TCP/1720	H323	
	UDP/53	DNS	
Netmeeting with ILS	TCP/1720	H323	Windows Netmeeting Version 3.01 Opengk Version 1.2.0
	TCP/389	ILS	
	UDP/53	DNS	
Netmeeting with GK	TCP/1720	H323	
	UDP/1719	H323GK	
	UDP/53	DNS	
SIP	UDP/5060	SIP	SIP User Agent 2.0
Intel Video Phone	TCP/1720	H323	Intel Video Phone Version 5.0
	UDP/53	DNS	
FTP	TCP/21	FTP	WFTPD version 2.03 Redhat Linux 7.3
	UDP/53	DNS	
安全 ALG			

ALG/应用程序名称	协议与埠	预先设定的服务名称	测试软件版本
L2TP	UDP/1701	L2TP	Windows 2000 Server built-in
	UDP/53	DNS	
PPTP	TCP/1723	PPTP	Windows 2000 Server built-in
	UDP/53	DNS	
IPSec (Only Tunnel Mode with ESP)	UDP/500	IKE	Windows 2000 Server built-in
	ESP		
	UDP/53	DNS	
聊天			
AOL Chat	TCP/ 5190	AOL	AOL Instant Messenger Version 5.0.2938
	TCP/80	HTTP	
	UDP/53	DNS	
ICQ Chat NB: Application should be configured to use TCP/5191	TCP /5191	ICQ_2000	ICQ 2000b
	TCP/80	HTTP	
	UDP/53	DNS	
IRC	TCP/ 6667	IRC	MIRC v6.02
	TCP/80	HTTP	
	UDP/53	DNS	
MSIM	TCP/1863	MSN	MSN Messenger Service Version 3.6.0039
	TCP/80	HTTP	
	UDP/53	DNS	
游戏			
Flight Simulator 2002 (Gaming Zone)	TCP/47624	MSG1	Flight Simulator 2002, Professional Edition
	TCP/28801	MSN-ZONE	
	TCP/443	HTTPS	
	TCP/80	HTTP	
	UDP/53	DNS	
Quake II (Gaming Zone)	UDP/ 27910	QUAKE	Quake II
	TCP/28801	MSN-ZONE	
	TCP/443	HTTPS	
	TCP/80	HTTP	
	UDP/53	DNS	
Age Of Empires	TCP/47624	MSG1	Age of Empires, Gold

ALG/应用程序名称	协议与埠	预先设定的服务名称	测试软件版本
(Gaming Zone)	TCP/28801	MSN-ZONE	Edition
	TCP/443	HTTPS	
	TCP/80	HTTP	
	UDP/53	DNS	
Diablo II (BATTLE-NET-TCP, BATTLE-NET-UDP)	TCP/4000	DIABLO-II	Diablo II
	TCP/ 6112	BATTLE-NET-TCP, BATTLE-NET-UDP	
	UDP/53	DNS	
	UDP/6112	Diablo II	
其它的应用程序			
POP3	TCP/110	POP3	Outlook Express 5
	UDP/53	DNS	
IMAP	TCP/143	IMAP4	Outlook Express 5
	UDP/53	DNS	
SMTP	TCP/25	SMTP	Outlook Express 5
	UDP/53	DNS	
HTTPS / TLS / SSL	TCP/443	HTTPS	互聯網 Explorer 5
	TCP/80	HTTP	
	UDP/53	DNS	
LDAP	TCP/389	ILS	Openldap 2.0.25
	UDP/53	DNS	
NNTP	TCP/119	NNTP	Outlook Express 5
	UDP/53	DNS	
Finger	TCP/79	FINGER	Redhat Linux 7.3
	UDP/53	DNS	

B. 系统规格

甲、 硬件规格

表 B.1. 硬件规格

电源供应器	输入	Varied w/ regions. Note your AC adapter only works w/ your region.
	输出	15VAC, 700mA
内存	Flash	4MB
	SDRM	16MB
连接埠	WAN	1 – 10/100Mbps, auto speed negotiation
	LAN	4 – 10/100Mbps, auto MDI/MDIX, auto speed negotiation
	Reset button	For use on system reboot and reset to factory settings
	Console port	For use by ASUS only
环境需求	操作	Temperature: 0°C ~ 40°C (32°F ~ 105°F)
		Humidity: 10% ~ 90%, non-condensing
	放置	Temperature: -20°C ~ 65°C (-4°F ~ 149°F)
		Humidity: 10% ~ 90%, non-condensing

乙、 系统默认值

表 B.2 l 是关于本路由器的默认值。在此表格中并不列出默认值的相关参数。

表 B.2. 系统默认值

局域网络 LAN		
IP	IP Address	192.168.1.1
	Subnet Mask	255.255.255.0
DHCP Server	IP Address Pool	192.168.1.10 ~ 192.168.1.200
	Subnet Mask	255.255.255.0
	Lease Time	14 days
	Default Gateway	192.168.1.1
	Primary DNS	192.168.1.1
广域网络 WAN		
Default Connection Mode		PPPoE
PPPoE (PPPoE:0,	Unnumbered PPPoE	Disable
	Host Name	RX3041H

PPPoE:1)	Obtain DNS	Automatically
	MSS Clamping	Enabled, MSS Value – 40 bytes
	Options	Keep Alive, Echo Interval – 60 seconds
Dynamic (DHCP Client)	Host Name	RX3041H
	Obtain DNS	Automatically
	MAC Cloning	Disable
路由设定		
动态路由	RIP	Enable
	Passive Mode	Disable
	RIP Version (Send)	Version 2
	RIP Version (Receive)	Both
	Authentication	Disable
	RIP Authentication Mode	Clear Text
	Authentication Key	admin
远程访问		
用戶群组	Inactivity Timeout	300 seconds
防火墙		
入埠 ACL		Deny all inbound traffic
出埠 ACL		Allow all outbound traffic, NAT – WAN interface, Time Ranges – always, Application Filtering – none, Log - disable
URL 过滤		Enable
	Proxy Port	80
Advanced ➔ Self Access		From LAN: ICMP; TCP 23, 80, 10081; UDP 161, 162, 53
Advanced ➔ DoS	Enable	SYN Flooding, ICMP Verbose, Max IP Fragment Count – 45, Min IP Fragment Size – 512 bytes
	Disable	Winnuke, MIME Flood, FTP Bounce, IP Unaligned Time-stamp, Sequence Number Prediction Check, Sequence Number Out-of-range Check, ICMP Verbose
Log		
	File	Enable for Access, System and Firewall
	Log File Backup via Email	Disable
	Email	Disable
	Syslog Server	Disable

系统管理		
System Services	Enable	Firewall, DNS Relay, DHCP Server, Revert back to the factory default by using the Reset button
	Disable	DDNS, RIP, SNTP, UPnP
Password	Administrator	Username: admin (cannot be changed)
		Password: admin
	Guest	Username: guest (cannot be changed)
		Password: guest
System Identity	System Name	RX3041H
Date/Time	Date	1/1/2000 (moth/day/year)
	Time	00:00:00 (hour:min:sec)
	Time Zone	GMT+8:00
	SNTP Update Interval	60 minutes
SNMP		Disable
	RO (Read-Only) Community Name	public
	RW (Read-and-Write) Community Name	private

C. IP 地址，网络屏蔽及子网

甲、 IP 地址


注意

本章节只适合 IPv4 IP 地址（网际网络协议第 4 版）。IPv6 地址并不适用。

本章节假定您已经掌握了一些基本知识，如二进制数、字节（byte）、位（bit）。欲知更多细节请参考附录 A。

IP 地址，类似于网际网络的电话号码，被用来确定网际网络上的个人节点（计算机或其它设备）。每个 IP 地址都包括四个数字，每个都是从 0 到 255，由点（句点）分开，例如 20.56.0.211。这些数字按照从左到右的顺序被称为 field1, field2, field3, and field4。

这种用点分开十进制的数字的书写 IP 地址的风格被称为*带点的十进制符号*。IP 地址 20.56.0.211 读作"二十点五十六点零点二一一"。

i. IP 地址结构

IP 地址与电话号码相类似，是一种分等级的设计。例如，一个 7 位数的电话号码，它的前三位确定了成千上万条电话线的一个群组，而后四位数字则确定了群组中的一条特定的电话线。

类似的，IP 地址也包含两类信息。

- *Network ID*
  确定了网际网络或内部网络中的一片特定的网络
- *Host ID*
  确定了网络中一台特定的计算机或其它设备

每个 IP 地址的第一部分都包括了 network ID，其余的部分就包括了 host ID。网络 ID 的长度取决于网络等级 network *class* （请参看下面的部分）。表 C.1 说明了 IP 的结构。

表 C.1. IP 地址结构

	Field1	Field2	Field3	Field4
Class A	Network ID	Host ID		
Class B	Network ID		Host ID	
Class C	Network ID			Host ID

这里有一些有效 IP 地址的实例：

Class A: 10.30.6.125 (network = 10, host = 30.6.125)
Class B: 129.88.16.49 (network = 129.88, host = 16.49)
Class C: 192.60.201.11 (network = 192.60.201, host = 11)

乙、 网络等级

三个常用的网络等级为 A、B 和 C。（还有一个等级 D，但是它有特殊用途，已经超过了本次讨论的范围。）这些等级分别有不同的用途和特性。

等级 A 网络是网际网络最大的网络，每个都拥有超过 1 千 6 百万主机的空间。对于总数超过 20 亿的主机而言，最多可存在 126 个如此巨大的网络。因为它们的超大尺寸，这些网络被用作 WAN 以及被网际网络基础结构水平的组织使用，如您的网络供货商 ISP。

等级 B 网络比 A 稍小一些，但仍旧很大，每个都能容纳 6 万 5 千主机。最多可存在 16,384 个等级 B 的网络。一个等级 B 的网络可适用于大型组织，如商业或政府代理处。

等级 C 网络是最小的一个，最多只能容纳 254 主机，但是等级 C 网络可能的总数可超过 20 亿（确切地说，是 2,097,152）。联机到网际网络上的局域网络 LAN 通常是等级 C 网络。

下面是关于 IP 地址的一些重要的注意事项：

- 透过 field1 我们很容易就可以判断网络的等级：
  field1 = 1-126: Class A
  field1 = 128-191: Class B
  field1 = 192-223: Class C
  （若 field1 的值没有显示出来，则表明被保留以作特定用途 uses）
- host ID 能够拥有任意值，除了所有 field 的值均设为 0 或所有的 field 均设为 255 之外，因为这些值被保留以作特定用途。

丙、 子网掩码

名词解释

屏蔽（mask）

屏蔽看起来很像一个规则的 IP 地址，但是却包含了位（bit）的形态，能够告诉您 IP 地址的哪个部分是 network ID 以及哪个部分是 host ID：bit 设定成 1 表明"此 bit 是 network ID 的一部分"，bit 设定成 0 表明"此 bit 是 host ID 的一部分"。

子网掩码 被用来定义 *子网络* （您在将网络分割成一小片一小片之后所得到的）。子网的网络 ID 是透过从地址的 host ID 部分"借用"一个或多个 bit 而創建的。子网掩码识别这些 host ID 的 bit。

例如，等级 C 网络 192.168.1。想要将它分成两个子网络，您得使用子网掩码：

255.255.255.128

如果我们用二进制来书写，将更容易看到发生了什么：

11111111. 11111111. 11111111.10000000

而对于任意等级 C 地址，从 field1 到 field 3 的所有 bit 都是 network ID 的一部分，但是请注意，屏蔽是如何指定 field 4 的第一个 bit 也包含在内。由于这个额外的 bit 只有两个值（0 和 1），这意味着有两个子网。每个子网为 host ID 使用了 field 4 保留的 7 个 bit，它的范围从 0 到 127（而不是等级 C 通常的 0 到 255）。

类似的，将等级 C 的网络分成四个子网，屏蔽为：

255.255.255.192 或 11111111. 11111111. 11111111.11000000

这两个 field 4 内额外的 bit 有四个值（00, 01, 10, 11），因此有四个子网。每个子网为 host ID 使用了 field 4 保留的 6 个 bit，范围从 0 到 63。


注意

*有时，子网掩码并不特别指定任何额外的 network ID bit，因此就没有子网络。这样的屏蔽被成为*预设的子网掩码。*这些屏蔽为：*

Class A: 255.0.0.0
Class B: 255.255.0.0
Class C: 255.255.255.0

*这些被称为*默认值*是因为它们在当网络预先设定好时被使用，此时它没有子网络。*

D. 解决问题

本附录为您在安装或使用网际网络安全路由器的过程中可能遇到的问题提出了供参考的解决方法，并为如何使用 IP 工具来诊断问题提供了参考说明。

如果下列建议不能为您解决问题，请联系华硕客户服务部门。

问题	解决方法
LED 灯	
Power LED 灯在产品开关打开后不亮。	请检查您是否使用由设备所提供的电源供应器，且安全地联机到网际网络安全器和电源插座上。
LINK WAN LED 灯在以太网线缆联机好后不亮。	请检查设备提供的以太网线缆已经安全地连接到了您 ADSL 或 cable modem 的以太网端口和路由器的广域网埠上面。请确认您的 ADSL 或 cable modem 的电源是开启的。等待 30 秒的时间以允许路由器与您的宽频 modem 有协商时间。
LINK LAN LED 灯在以太网线缆连接好后不亮。	请检查设备提供的以太网线缆已经安全地连接到了您的局域网络集线器或 PC 以及网际网络安全路由器上。请确认 PC 和/或集线器已经开启。 请检查您的缆线足够应付您的网络需求。100 Mbit/秒的网络（100BaseTx）应该使用 Cat 5 的缆线。10Mbit/秒的网络可以接受品质稍低的缆线。
访问互聯網	
PC 无法访问互聯網	使用下面即将讨论到的 ping 工具，以检查您的 PC 是否能够与网际网络安全路由器的局域网络 IP 地址（默认值为 192.168.1.1）通讯。如不能，请检查以太网的缆线。 如果您静态地为计算机指定了一个私人 IP 地址，（并非已注册的公共地址），请检查下列事项： • 检查计算机网关 IP 地址是您的公共 IP 地址，（参看"快速安装指南"一章，第二部分对于检查 IP 信息的说明）。如果不是，那么改正此地址或将 PC 设定成自动接收 IP 信息。 • 与您的网络供货商确认指定给 PC 的 DNS 服务器 是有效的。请改正此地址或将 PC 设定成自动接收 I 信息。 • 请检查网络地址转换(NAT)规则已经在您的网际网络安全路由器上设定好以将私人地址转换成公共 IP 地址。指定的 IP 地址必须包含在指定的 NAT 规则中。或者，设定 PC 接收另一设备指定的地址（参看第 3.2 节 第二部分 设定网际网络参数）。预设的设定包括一个在预先定义好的地址池 内的所有动态指定地址而设定的 NAT 规则。

问题	解决方法
PC 无法显示网际网络的网页。	请检查 PC 指定的 DNS 服务器对您的网络供货商来说是正确的，如上文选项所述。您可使用下面即将讨论到的 ping 工具测试与您网络供货商的 DNS 服务器的连通性。
设定管理员程序	
您忘记/遗失了您的设定管理员用户 ID 或密码。	如果您还未更改预设的密码，请尝试使用"admin"作为您的 用户 ID 以及密码。另外，您可将设备重新设定成预设值（请参考第 **錯誤! 找不到參照來源。** 节"**錯誤! 找不到參照來源。**"提供的说明）。 **小心:** 重新设定本设备将导致原有设定被删除，且所有的设定均回复至默认值。
从您的浏览器无法访问设定管理员。	使用下面即将讨论到的 ping 工具，以检查您的 PC 是否能够与网际网络安全路由器的区域网 IP 地址（默认值为 192.168.1.1）通讯。如不能，请检查以太网的缆线。 请检查您使用的浏览器为互聯網 Explorer v5.5、Netscape 7.0.2 或以上版本。想要使用 Javascript® 必须得到浏览器的支持；想要使用 Java® 同样也需要支持。 请检查 PC 的 IP 地址与指定给路由器局域网络埠的 IP 地址位于相同的子网下。
对设定管理员的更改没有保留下来。	请确认点选了 Apply 按钮以保存更改。

甲、 使用 IP 工具诊断问题

i. ping

Ping 是用来检查您的 PC 是否能够辨认出您网路或网际网络内其它计算机的命令。Ping 命令送出一个讯息到您指定的计算机上。如果计算机接收了讯息，它将送出讯息回复。使用这个工具，您必须知道您与之通讯的计算机的 IP 地址。

对 Windows 系统的计算机，您可从**开始**菜单执行 Ping 命令。点选**开始**按钮，然后点选**执行**。在文字框输入下列内容：

ping 192.168.1.1

点选 OK。您可用网际网络站点名称取代任何局域网络内的私人 IP 地址或公共 IP 地址。

如果目标计算机收到了此信息，命令提示窗口将出现，如图 D.1 所示。

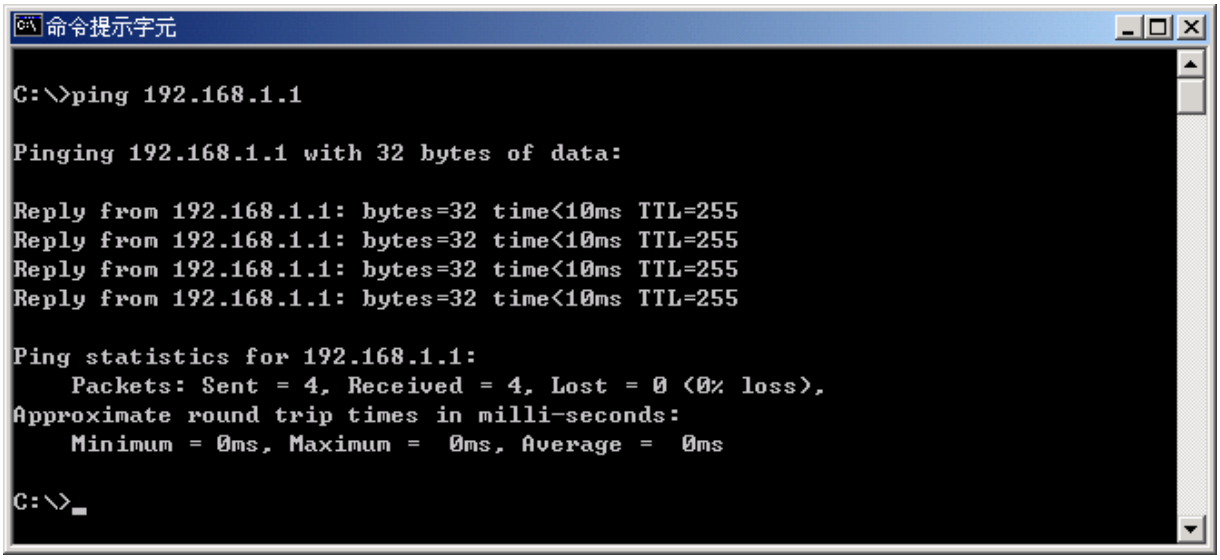


图 D.1. 使用 ping 工具

如果目标计算机不存在，那么您将接收此消息 “Request timed out”。

使用 ping 命令，您可以测试到达路由器的路径是否起作用（使用预先设定好的局域网络 IP 地址 192.168.1.1），或者另外一个您指定的地址。

您还可以透过输入外部地址，例如 www.yahoo.com （216.115.108.243）测试网际网络联机是否来起作用。如果您不知道特定网际网络位置的 IP 地址，您可使用 nslookup 命令，如下面章节的说明。

对于大多数 IP-enabled 的操作系统，您可在命令提示时或透过系统管理工具执行相同的命令。

ii. nslookup

您可使用 nslookup 命令来决定与网际网络站点名称相对应的 IP 地址。您指定了一般的名称，然后使用 nslookup 命令在您的 DNS 服务器（通常放置在您的网络服务供货商）上查询此名称。如果那个名称并不存在您网络服务供应商的 DNS 表格中，那么此请求将涉及另一个更高等级服务器，直到该项目被找到。最后，服务器会响应与该名称相对应的 IP 地址。

对 Windows 系统的计算机，您可从**开始**菜单找到 nslookup 命令并执行之。点选**开始**按钮，然后点选**执行**。在文字框输入下列内容：

nslookup

点选 OK。一个命令提示窗口将与括号同时出现（>）。根据提示，输入您感兴趣的网际网络地址名称，例如 www.absnews.com。

此窗口将显示相关联的 IP 地址，如图 D.2 所示。

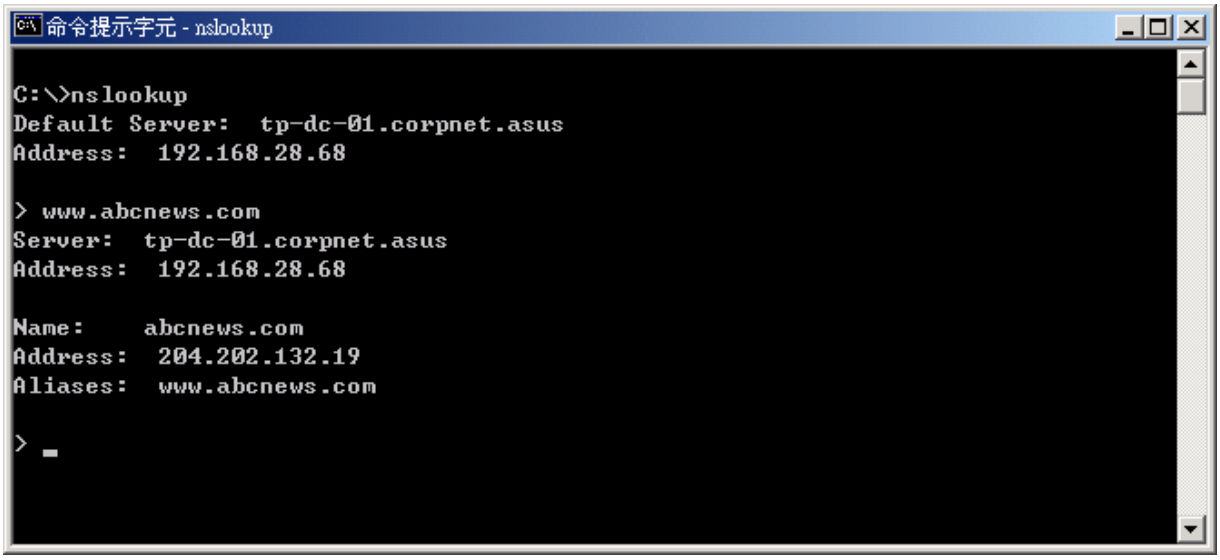


图 D.2. 使用 nslookup 工具

可能会出现很多的 IP 地址名称对应到同一名称。这对经常接收到巨大流量的网页站点来说很平常；他们使用多台的服务器来传递相同的信息。

想要离开 nslookup 模式，请在命令提示页面中输入 **exit**，然后按下 **<Enter>** 键。

E. 术语表

10BASE-T 以太网络使用的配线的名称，数据传输率为 10 Mbps。又被称为 Category 3（CAT 3）配线。*又见数据传输率，Ethernet*。

100BASE-T 以太网络使用的配线的名称，数据传输率为 100 Mbps。又被称为 Category 5（CAT 5）配线。*又见数据传输率，Ethernet*。

ADSL Asymmetric Digital Subscriber Line，非对称式数字用户回路
对于家庭用户来说最常用的 DSL。Asymmetrical 非对称性指的是它不平衡的下载与上载数据传输率（下载速率要比上载速率快）。非对称性有益于家庭用户，因为他们通常下载的资料量要比上载的多得多。

authenticate 用来检验用户的身份，例如提示输入密码。

binary 二进制，两个最基础的数字系统之一，仅使用两个数字（0 和 1）来代表所有的数字。在二进制里，数字 1 写成 1，2 写成 10， 3 写成 11，4 写成 100，如此类推。尽管为方便起见，IP 地址常常用十进制的数字来表达，但实际上，IP 地址是二进制数字；例如，209.191.4.240 在二进制内是 11010001.10111111.00000100.11110000。*又见 bit, IP address, network mask*。

bit 比特，"binary digit，二进制数字" 的简写，一个 bit 其实是有 0 或 1 两个值的数字。*又见 binary*。

bps 每秒比特数

broadband 宽频，一种通讯技术，能够透过相同的媒介传送不同类型的资料。DSL 就是宽频技术的一种。

broadcast 广播，把资料传送到网络中所有的计算机上。

DHCP Dynamic Host Configuration Protocol，动态主机配置协议
DHCP 自动进行地址分配与管理。当计算机联机上局域网络（LAN），DHCP 从共享的 IP 地址地址池中指派 IP 地址；在指定的时间界限结束之后，DHCP 又将地址归还给了地址池。

DHCP relay Dynamic Host Configuration Protocol relay，动态主机配址协议中继
DHCP relay 是指在要求 IP 地址的计算机与指派地址的 DHCP 服务器之间传递 DHCP 信息的计算机。路由器的每个接口都能设定成 DHCP relay。*详见 DHCP 章节*。

DHCP server Dynamic Host Configuration Protocol server，动态主机配址协议服务器
DHCP 服务器是指负责为 LAN 中的计算机指派 IP 地址的计算机。*详见 DHCP 章节*。

DNS Domain Name System，领域名称系统
DNS 将网域名称对应到 IP 地址上去。DNS 信息按等级穿过网际网络分配给称作 DNS 服务器的计算机。当您开始访问网页站点时，DNS 服务器会检查被要求的网域名称，以找到相应的 IP 地址。如果 DNS 服务器不能找到 IP 地址，那么它将与更高一级的 DNS 服务器联络，以确定 IP 地址。*又见 domain name*。

domain name 网域名称，是代替与之相对应的用户容易掌握使用的 IP 地址名称。例如，www.hinet.net 与 IP 地址 168.95.1.88 相关联的网域名称。网域名称必须是独一无二的；它们被国际指派名称与序号的网际网络公司（ICANN）进行分配 。网域名称并非 URL 的要素，URL 在网页站点确认特定的档案，例如， http://www.asus.com。*详见 DNS 章节*。

download 下载，从网际网络传递资料给用户。

DSL Digital Subscriber Line，数字用户回路
一种同时允许数字资料与模拟声音信号透过现有铜制电话线的技术。

Ethernet 以太网，最普遍应用的计算机网络技术，常使用双绞线电缆。以太网数据传输率为 10 Mbps 与 100 Mbps。又见 *10BASE-T, 100BASE-T, twisted pair*。

filtering 过滤，以过滤规则为基础筛选出资料的类型。过滤可被应用在一个方向（上载或下载），或双向。

filtering rule 过滤规则，一个指定路由设备将接收和/或拒绝何种类型的资料的规则。过滤规则被定义为在某一接口（或多个接口）操作且朝着特定的方向（下载、上载，或双向）。

firewall 防火墙，指保护接入网际网络的计算机或局域网络不受外界的侵扰或攻击的任意方法。一些防火墙保护可由封包过滤和网络地址转换服务提供。

FTP File Transfer Protocol，档案传输协议
一个被用来在接入网际网络的计算机之间传递档案的程序。通常的应用包括向网络服务器上载新的或升級后的档案，以及从网络服务器下载档案。

hop 跳跃，当您透过网际网络传送资料时，资料首先从您的计算机传送至路由器，然后从一台路由器传送到另一台，直到最后达到直接联机到接收者的路由器为止。资料的传递旅程中每个单个的"leg" 都被称为一次跳跃。

hop count 跳跃次数，指数据在到达目的地的路径中所经历的跳跃的次数。另外，亦可指一个封包在被丢弃之前被允许经历的最大跳跃次数（*又见 TTL*）。

host 主机，连接到网络的设备（通常是指计算机）。

HTTP Hyper-Text Transfer Protocol，超文字传输协议
HTTP 是用在 Web 浏览器与 Web 服务器之间传输档案（如文字或图片档案）的协议 。*又见 web browser, web site*。

ICMP Internet Control Message Protocol，网际网络控制讯息协议
网络层面的网际网络协议，负责错误报告及提供 IP 封包处理相关的信息。Ping 命令就使用了 ICMP。

IGMP 互聯網 Group Management Protocol，网际网络群组管理协议
一个使计算机能在多点广播内与相邻路由器与分享成员信息的网际网络协议。多点广播群组是指成员已经被认定为愿意从其它计算机那里接收特定内容的信息感兴趣的群组。对 IGMP 群组的多点广播可同时被用来升級移动用户群组地址薄，或将公司的时事通讯传送到名单上的用户。

Internet 互聯網，最大的全球性网络，连接全世界上万个网络，为私人和商业用户使用。

intranet 内部网络，一个私人的，或企业内部的网络，看起来像网际网络的一部分（用户使用网页浏览器访问信息），但是仅为内部成员使用。

IP *见 TCP/IP*。

IP address 互聯網 Protocol address，网际网络协议地址
网际网络上主机（计算机）的地址，由四个数字组成，每个都是从 0 到 255，以点号隔开，例如，209.191.4.240。IP 地址由确认主机所属的特殊网络的 *network ID* 与确认主机自身处于网络的独一无二的 *host ID* 构成。网络屏蔽被用来定义 network ID 与 host ID。因为每个成员的 IP 地址均不相同，所以他们常常拥有相关联可被指定的的网域名称。又见 *domain name, network mask*。

ISP 互聯網 Service Provider，网络服务供货商
提供顾客访问网际网络收费服务的公司。

LAN Local Area Network，局域网
局限于一个小的地理区域的网络，例如，家庭、办公室，或小型建筑。

LED Light Emitting Diode，发光二极管
透过转换电子能量的方式来发射光线的半导体设备。一般硬设备上的状态灯都是典型的 LED。

MAC address Media Access Control address，媒体存取控制地址
由制造商指定的设备的永久硬件地址。MAC 地址用六组字符(byte)来表示。

mask *见 network mask*。

Mbps 每秒百万比特，Megabits per second 的简写。网络数据传输率通常用 Mbps 来表示。

NAT Network Address Translation，网络地址转换
用以减低对 IP 地址必须全球唯一的需求的机制。NAT 透过将地址转换成可在全球传递的地址，使得某一组织联机到网际网络的 IP 地址可以不是全球唯一的。

NAT rule NAT 规则，已定义的在您局域网络的公共与私人 IP 地址之间传输信息的方法。

network 网络，一群可透过传输媒体互相通信的计算机、打印机、交换器及其它的设备。网络可以很小，如局域网络 *LAN*，也可以非常大，如网际网络*互聯網*。

network mask 网络屏蔽，指一系列当忽略掉 host ID 时被应用于 IP 地址选择的一系列 bit。Bit 设定为 1 意味着"选择此位"，而当 bit 设定为 0 则意味着"忽略此位"。例如，如果网络屏蔽 255.255.255.0 应用到 IP 地址 100.10.50.1，那么 network ID 为 100.10.50，host ID 为 1。*又见 binary, IP address, subnet*。

NIC Network Interface Card，网络适配卡
插入您的计算机，并能为网络线缆提供实体接口的适配卡，典型的以太网 NIC 是 RJ-45 连接器。*见 Ethernet, RJ-45*。

packet 封包，在网络上传输资料的单位。每个封包都包含资料、添加的信息例如它从那里来（来源地址）以及将到哪里去（目标地址）。

ping Packet 互聯網 (or Inter-Network) Groper，讯息及其回复
用来检验与 IP 地址相关联的主机是否已联机的程序。它亦能被用来显示给定网域名称的 IP 地址。

port 端口，计算机、路由器等设备的物理接入点，资料透过连接端口来传入和传出此设备。

PPP Point-to-Point Protocol，点对点协议
提供透过同步或异步传输电路路由器对路由器和对主机的联机。广域网（WAN）的路由器接口使用两种形式的 PPP，称为 PPPoA 与 PPPoE。*又见 PPPoA, PPPoE*。

PPPoE Point-to-Point Protocol over Ethernet，以太网的点对点协议
您能定义虚拟电路（VC）的两种 PPP 接口之一，另一种为 PPPoA。您能为每个 VC 定义一个或多个 PPPoE 接口。

protocol 协议，管理设备如何在网络上交换信息的一套规则和规范的正式称呼。

remote 远程，物理上分离的位置。例如，员工在出差的途中登入公司内部网络，为远程用户。

RIP Routing Information Protocol，路由信息协议
最初的 TCP/IP 路由协议。有两个 RIP 版本：版本 I 与版本 II。

RJ-45 8-pin 的插头用来代替电话线传输资料。以太网线缆通常使用此种类型的连接器。

routing 路由，找到一条到达目的地主机路径的程序。在大型网络里，路由是非常复杂的，因为封包在抵达目的地之前，可经过的中间节点非常多。履行路由职责的设备被称为路由器。

rule *见 filtering rule, NAT rule*。

SDNS Secondary Domain Name System （server），二级网域名称系统（服务器）
指在 primary DSN 服务器不可用时，能被使用的 DNS 服务器。*见 DNS*。

SNMP Simple Network Management Protocol，简单网络管理协议
用于网络管理的指 TCP/IP 协议。

subnet 子网，在 IP 网络里，分享某一特别子网地址的网络。子网是由网络管理者为了提供多级、阶层式路由结构，而同时能够避免所附着网络的子网的指定地址的复杂度。*又见 network mask*。

subnet mask 子网掩码，定义子网的屏蔽。*又见 network mask*。

TCP *见 TCP/IP*。

TCP/IP Transmission Control Protocol/互聯網 Protocol，传输控制协议/网际网络协议
网际网络所使用的基本协议。TCP 负责分割需传递资料至封包并在目的地将它们重新组装起来，而 IP 负责将封包从来源地传输至目的地。当 TCP 和 IP 与高级应用程序如 HTTP, FTP, Telnet 等捆绑在一起时，TCP/IP 指的是整套协议。

Telnet 交互式的、通常用在使得用户能登入远程的系统就如同在本地般使用其资源的远程终端机联机。HTTP（网络协议）与 FTP 仅允许您从远程计算机下载档案，而 Telnet 可允许您从远程登入及使用计算机。

TFTP Trivial File Transfer Protocol，简易档案传输协议
FTP 的简化版，允许在网络上传送和接收档案的协议，但是没有 FTP 的功能强大，安全性也较差。

TTL Time To Live，存活时间
IP 表头中的选项，用来指出一个封包被认为有效的时间有多长。TTL 为零时，封包将被丢弃。

twisted pair 双绞线，包含两条被绞成螺旋状绝缘线的低速传输媒体。此绝缘线可以是遮蔽或无遮蔽。双绞线是语音通讯应用中常见的媒体，且日渐在数据网络上逐渐普遍。对于以太网 LAN，一个更高等级的 Category 3 (CAT 3) 正在为 10BASE-T 网络所应用，一个更高等级的 Category 5 (CAT 5)正在为 100BASE-T 网络所应用。又见 *10BASE-T, 100BASE-T, Ethernet*。

upstream 上行，数据传输的方向是从用户到网际网络。

WAN Wide Area Network，广域网
由电信公司所提供，服务于广大区域用戶的数据通讯网络。对于网际网络安全路由器来说，WAN 指整个网际网络。

Web browser 使用档案传输协议 HTTP 来从网络站点下载信息，并为用户显示由档案、图形、音频或视频组成的信息的客户端应用软件。例如，互聯網 Explorer、Mosaic 和 Netscape Navigator。*又见 HTTP, web site, WWW*。

Web page 网页，网站点档案，一般包括文本、图形以及链接到本站点及其它站点的网页的超链接（前后对照）。当用户访问网络站点时，显示的第一个页面称为主页 *home page*。*又见 hyperlink, web site*。

Web site 网络站点，指网际网络上透过网页浏览器分配信息给远程用户、以及从远端用户获得信息的计算机。网络站点一般由包含文本、图形以及超链接的网页组成。*又见 hyperlink, web page*。

WWW World Wide Web，全球信息网
又被成为*环球网*。提供超链接及其它服务给执行像浏览器等客户端软件的网际网络服务器的大型网络。

F. 索引