RX3042H

使用手册

Revision 0.8
May 12, 2005

目录

1 简介 1

1.1 特色 1

1.2 系统需求 1

1.3 如何使用本手册 2

1.3.1 符号意义 2

1.3.2 版面设计意义 2

1.3.3 特殊信息 2

2 了解 RX3042H 3

2.1 部件列表 3

2.2 硬件特色 3

2.3 软件特色 3

2.3.1 NAT 特色 3

2.3.2 防火墙特色 4

2.3.2.1 状态封包检测 4

2.3.2.2 封包过滤 - ACL (访问控制列表) 4

2.3.2.3 DoS 攻击防护 5

2.3.2.4 应用层网关 (ALG) 6

2.3.2.5 系统日志 6

2.4 产品外观 7

2.4.1 前面板 7

2.4.2 后面板 8

2.4.3 底视图 9

2.5 安置选择 9

2.5.1 桌面安置 9
2.5.2 挂壁安装 9
3 快速安装指南 11
3.1 第一部分——连接硬件设备 11
3.1.1 第一步: 连接到 ADSL 或 cable modem 11
3.1.2 第二步: 连接到计算机或网络 12
3.1.3 第三步: 连接 AC 电源适配器 12
3.1.4 第四步: 打开 RX3042H, ADSL 或 cable modem 的电源, 并启动您的计算机 12
3.2 第二部分——设置您的计算机 13
3.2.1 开始设置之前 13
3.2.2 Windows® XP 14
3.2.3 Windows® 2000 14
3.2.4 Windows® 95, 98, 及 ME 15
3.2.5 Windows® NT 4.0 工作站 16
3.2.6 为您的计算机分配静态 IP 地址 17
3.3 第三部分 ——快速设置 RX3042H 18
3.3.1 设置 RX3042H 18
3.3.2 测试设置 20
3.3.3 默认路由器设置 21
4 使用设置管理界面 23
4.1 登录设置管理界面 23
4.2 功能结构 24
4.2.1 导航菜单 25
4.2.2 常用按钮和图标 25

4.3 系统设置简介 26
5 路由器设置 27
5.1 LAN 设置 27
5.1.1 LAN IP 地址 27
5.1.2 LAN 配置参数 27
5.1.3 设置局域网 IP 地址 28
5.2 WAN/DMZ 配置 29
5.2.1 WAN 连接模式 29
5.2.2 PPPoE 30
5.2.2.1 WAN PPPoE 配置参数 31
5.2.2.2 设置 WAN 模式下的 PPPoE 32
5.2.3 PPPoE Unnumbered 33
5.2.3.1 WAN PPPoE Unnumbered 配置参数 34
5.2.3.2 设置 WAN 模式下的 PPPoE Unnumbered 35
5.2.4 动态 IP 36
5.2.4.1 设置 WAN 模式下的动态 IP 地址 36
5.2.5 静态 IP 37
5.2.5.1 WAN 或 DMZ 静态 IP 地址配置参数 37
5.2.5.2 设置 WAN 或 DMZ 模式下的静态 IP 38
5.2.6 PPTP 39
5.2.6.1 WAN PPTP 配置参数 39
5.2.6.2 为 WAN 设置 PPTP 41
5.3 WAN Load Balancing 和 Line Back Up 42
5.3.1 WAN Load Balancing 和 Line Back Up 配置参数 42

5.3.2 设置 WAN Load Balancing 44
5.3.3 设置 WAN Line Back Up 45
6 DHCP 服务器设置 47
6.1 DHCP（动态主机配置协议）..... 47
6.1.1 什么是 DHCP? 47
6.1.2 为什么使用 DHCP? 47
6.1.3 配置 DHCP 服务器 48
6.1.4 查看当前 DHCP 地址分配情况 50
6.1.5 DHCP 固定租约 50
6.1.5.1 进入 DHCP 固定租约配置页面（Advenced -> DHCP server) 50
6.1.5.2 添加一个 DHCP 固定租约 51
6.1.5.3 删除一个 DHCP 固定租约 51
6.1.5.4 查看 DHCP 租约表 52
6.2 DNS 52
6.2.1 关于 DNS 52
6.2.2 分配 DNS 地址 52
6.2.3 设置 DNS Relay 53
7 路由 55
7.1 IP 路由简介 55
7.1.1 我需要设定静态路由吗？ 55
7.2 启用 RIP（路由信息协议）的动态路由 55
7.2.1 RIP 配置参数 56
7.2.2 配置 RIP 57
7.3 静态路由 58

7.3.1 静态路由配置参数 58
7.3.2 添加静态路由 59
7.3.3 删除静态路由 60
7.3.4 查看静态路由表 60
8 配置 DDNS 61
8.1 DDNS 配置参数 62
8.2 配置 HTTP DDNS 客户端 62
9 配置防火墙和 NAT 65
9.1 防火墙简介 65
9.1.1 状态封包检测 66
9.1.2 DoS（拒绝服务）攻击防护 66
9.1.3 防火墙和访问控制列表 (ACL) 66
9.1.3.1 ACL 规则优先级 66
9.1.3.2 连接状态追踪 66
9.1.4 默认 ACL 规则 66
9.2 NAT 简介 67
9.2.1 NAPT（网络地址和端口转换）或 PAT（端口地址转换） 67
9.2.2 Reverse NAPT / 虚拟服务器 69
9.3 防火墙设置（防火墙 /NAT -> 设置） 69
9.3.1 防火墙选项 69
9.3.2 DoS 设置 70
9.3.2.1 DoS 防护配置参数 70
9.3.2.2 设置 DoS 72
9.4 ACL 规则配置参数 72

9.4.1 ACL 规则配置参数 72
9.5 配置 ACL 规则（防火墙 ->ACL) 76
9.5.1 添加 ACL 规则 77
9.5.2 修改 ACL 规则 78
9.5.3 删除 ACL 规则 78
9.5.4 显示 ACL 规则 79
9.6 配置 Self-Access ACL 规则 (Firewall/NAT ->Self-Access ACL) 79
9.6.1 添加 Self-Access 规则 80
9.6.2 修改 Self-Access 规则 81
9.6.3 删除 Self-Access 规则 81
9.6.4 显示 Self-Access 规则 81
9.7 配置虚拟服务器 82
9.7.1 虚拟服务器配置参数 82
9.7.2 虚拟服务器设置范例 1 - Web 服务器 85
9.7.3 虚拟服务器设置范例 2 - FTP 服务器 87
9.7.4 虚拟服务器设置范例 3 - 具有访问控制功能的 FTP 服务器 87
9.8 设置特殊应用程序 89
9.8.1 特殊应用程序配置参数 89
9.8.2 特殊应用程序范例 91
10 系统管理 93
10.1 设置系统服务 93
10.2 登录密码和系统配置参数 94
10.2.1 更改密码 94
10.2.2 设置系统参数 95

10.3 浏览系统信息 95
10.4 设置日期和时间 96
10.4.1 浏览系统日期和时间 98
10.5 SNMP 设置 98
10.5.1 SNMP 配置参数 98
10.5.2 设置 SNMP 98
10.6 日志设置 99
10.6.1 使用 Syslog Server 设置远程日志 99
10.6.2 查看系统日志 100
10.7 系统设置管理 100
10.7.1 将系统配置参数恢复至出厂值 100
10.7.2 备份系统设置 101
10.7.3 恢复系统设置 103
10.8 固件升级 105
10.9 重启系统 107
10.10 退出设置管理界面 108
11 IP 地址，网络掩码，子网 109
11.1 IP 地址 109
11.1.1 IP 地址结构 109
11.2 网络等级 110
11.3 子网掩码 111
12 问题排除 113
12.1 使用 IP 工具诊断问题 115
12.1.1 ping 115
12.1.2 nslookup 116

图片索引

图 2.1 前面板 LED 指示灯 7
图 2.2 后面板标识和接口 8
图 3.1 硬件连接简图 13
图 3.2 登录框 19
图 3.3 系统状态页面 20
图 4.1 Configuration Manager 登录框 24
图 4.2 典型的 Configuration Manager 页面 25
图 4.3 系统状态页面 26
图 5.1 网络设置配置 —— LAN 配置 28
图 5.2 网络设置配置 —— WAN 配置 30
图 5.3 WAN —— PPPoE 配置 30
图 5.4 WAN —— PPPoE Unnumbered 配置 34
图 5.5 WAN —— 动态 IP (DHCP 客户端) 配置 37
图 5.6 WAN —— 静态 IP 配置 38
图 5.7 WAN —— PPTP 配置 42
图 5.8 Load Balancing 配置 45
图 6.1 DHCP 服务器配置页面 48
图 6.2 DHCP 租约表 50
图 6.3 固定的 DHCP Lease Configuration 页面 51
图 7.1 RIP 配置页面 55
图 7.2 静态路由配置页面 57
图 7.3 静态路由配置 58
图 7.4 路由样本表 59

图 8.1 HTTP DDNS 的网络图 60
图 8.2 HTTP DDNS 配置页面 61
图 9.1 NAPT —— 内部 PC 机都使用同一地址 66
图 9.2 反向 NAPT —— 将入站封包传送到基于协议、端口号以及 IP 地址的内部主机上 66
图 9.3 防火墙设置页面 70
图 9.4 ACL 配置页面 75
图 9.5 ACL 配置例图 76
图 9.6 ACL 列表例图 77
图 9.7 Self-Access ACL 配置页面 78
图 9.8 Self-Access ACL 配置举例 79
图 9.9 虚拟服务器配置页面 81
图 9.10 虚拟服务器部署拓扑图 84
图 9.11 虚拟服务器设置范例 1 —— 网页服务器 84
图 9.12 添加一个新的服务 85
图 9.13 虚拟服务器设置范例 2 —— FTP 服务器 86
图 9.14 虚拟服务器设置范例 3 —— FTP 服务器 88
图 9.15 ACL 防火墙虚拟服务器设置范例 —— FTP 服务器 89
图 9.16 特殊应用程序配置页面 91
图 10.1 系统服务配置页面 93
图 10.2 系统管理配置页面 94
图 10.3 系统信息页面 96
图 10.4 时区设置页面 97
图 10.5 SNMP 配置页面 99
图 10.6 Syslog Server 配置 99

图 10.7 日志样本 100
图 10.8 出厂值设置页面..... 101
图 10.9 出厂值设置确认..... 101
图 10.10 出厂值设置倒计时 101
图 10.11 系统设置备份页面 102
图 10.12 系统设置恢复页面 103
图 10.13 从文件管理器中选择系统设置文件..... 103
图 10.14 系统设置恢复页面 104
图 10.15 系统重启倒计时..... 105
图 10.16 固件升级页面 105
图 10.17 从文件管理器中选择固件文件..... 106
图 10.18 固件升级确认 106
图 10.19 固件升级过程 106
图 10.20 固件升级的系统重启倒计时..... 107
图 10.21 重启系统页面 108
图 10.22 设置管理界面退出页面..... 108
图 10.23 确认关闭浏览器（IE）..... 108
图 12.1 使用 ping 工具 115
图 12.2 使用 nslookup 工具 116

表格索引

表 2.1 DoS 攻击.....5
表 2.2 前面板标识和 LED 指示灯 7
表 2.3 后面板标识和 LED 指示灯 8

表 3.1 LED 指示灯 13
表 3.2 默认设置概括 21
表 4.1 常用的按钮和图标 25
表 5.1 LAN 配置参数 28
表 5.2 WAN PPPoE 配置参数 31
表 5.3 WAN PPPoE Unnumbered 配置参数 35
表 5.4 WAN Static IP 配置参数 39
表 5.5 WAN PPTP 配置参数 40
表 5.6 WAN Load Balancing 和 Line Back Up 配置参数 44
表 6.1 DHCP 配置参数 49
表 6.2 固定的 DHCP Lease 配置参数 51
表 7.1 RIP 配置参数 56
表 7.2 静态路由配置参数 58
表 8.1 DDNS 配置参数 62
表 9.1 防火墙的选项参数 69
表 9.2 DoS 攻击定义 70
表 9.3 ACL 规则配置参数 73
表 9.4 服务配置参数 75
表 9.5 虚拟服务器配置参数 83
表 9.6 流行的应用程序的端口号 84
表 9.7 特殊应用程序配置参数 89
表 9.8 流行的应用程序的端口号 90
表 10.1 SNMP 配置参数 98
表 11.1 IP 地址结构 110

第一章 简介

感谢您购买 RX3042H 路由器！现在，您就可以将这台高速宽带路由器与您的 ADSL 或 cable modem 进行连接，尽情享受高速局域网接入的乐趣。

本用户手册旨在引导您按照需要对RX3042H路由器进行设置，从而使本产品在最大程度上满足您的个性需求。

1.1 特色

- LAN: 四个高速以太网交换端口
- WAN: 双 10/100Base-T 以太网端口，为您的局域网中的所有用户提供 Internet 接入
- 防火墙，NAT（网络地址转换）功能为您的局域网提供安全 Internet 接入
- 通过 DHCP 服务器自动分配网络地址
- 包括 IP 路由、DNS 以及 DDNS 配置等的服务
- 用户设置双 WAN 或 WAN 并支持 DMZ
- 支持 USB 存储（通过固件升级来实现）
- 通过网页浏览器（如 Microsoft® Internet Explorer®6.0 及以后版本）进行功能和参数设置

1.2 系统需求

使用 RX3042H 路由器连接到 Internet，您的设备须具备以下条件:

- ADSL 或 cable modem，并且相对的服务已经启用并处于运行中，该服务至少分配了一个公共网络地址作为您的 WAN 地址。
- 具备以太网 10Base-T ／ 100Base-T ／ 1000Base-T 端口的

网卡 (NIC) 的一台或多台电脑

- （可选）以太网集线器。如果您希望在路由器下连接多于四台电脑，您可另外选购以太网集线器以扩充端口。
- 由于系统设置均通过基于网页的图形界面，因此必须具备网页浏览器（如 Internet Explorer 6.0 或以后版本）。

1.3 如何使用本手册

1.3.1 符号意义

- 术语缩写第一次出现时将给出其定义。
- 为简洁起见，RX3042H 在本手册中有时会简称为 “ 路由器 ” 或 “ 网关 ” 。
- 术语 “LAN” 和 “ 网络 ” 在本手册中可以通用，表示在同一地点连接到以太网站点的一组计算机
- 鼠标动作的先后次序用 “->” 符号表示。例如，“ 系统 -> 网络设置 ” 表示先点击 “ 系统 ” 菜单，然后点击 “ 网络设置 ” 子菜单。

1.3.2 版面设计意义

- 粗体字表示菜单及下拉菜单中的内容和程序窗口中须键入的内容字串。

1.3.3 特殊信息

本手册内包含下列图标，它们用来提示一些附注或操作指导。

注意：当前页上有项目解释或非必须的说明信息

定义：解释一些对多数读者不熟悉的术语或缩写的意义。这些属于还将列在术语表中。

警告：提示重要的内容，例如关于人身安全或系统兼容性的信息。

第二章 了解 RX3042H

2.1 部件列表

除了本手册外，RX3042H 的销售包装中还包含以下内容:

- 路由器主机
- AC 电源适配器
- 以太网线（直连式）

2.2 硬件特色

- LAN
- 四端口高速以太网交换机
- 自适应速度
- WAN
- 双 10/100M 以太网端口
- 自动 MDI/MDIX 跳线功能

2.3 软件特色

2.3.1 NAT 特色

RX3042H 提供了 NAT 功能，使您的局域网中的所有电脑能够共享一个高速互联网连接，从而节省了为各个电脑购买 ISP 服务的成本。该特色还能隐藏网络地址，并防止计算机出现在公共网络上。它将局域网中未注册的 IP 地址连接到可获取网络服务的 IP 地址从而实现网络共享。RX3042H 还提供逆向 NAT 功能，这项功能可支持各种服务如邮件服务器，网页服务器等。NAT 规则规定了网络地址转换机制。RX3042H 支持下列几种 NAT。

- NAPT（网络地址和端口转换），亦称 IP 伪装或 ENAT（增

强型 NAT)，可将多个内网主机映射到一个全球有效的 IP 地址。这种映射通常包含网络端口池以用于地址转换。每个封包都转换成带有全球通用的 IP 地址的封包，端口号码则转换成网络端口池中某个未使用的端口。

- 逆向 NAPT，亦称入站映射 , 端口映射，或虚拟服务器。任何进入到路由器中的封包通过这种规则中规定的协议，端口号和 / 或 IP 地址到达内网主机。在内网存在多个主机且需要使用多种服务时将使用这项功能。

2.3.2 防火墙特色

RX3042H 内置的防火墙提供以下特色解决方案来保护您的网络，防止网络遭到攻击和被利用成为攻击傀儡。

- 状态封包检测
- 封包过滤 (ACL)
- 服务拒绝攻击防护
- 日志

2.3.2.1 状态封包检测

RX3042H 防火墙使用 “状态封包检测” 功能，即抽取封包内与状态相关的信息，使用这些信息判断该封包是否安全，并且保存这些信息作为之后判定的依据。它可辨别应用程序并创建动态层，允许动态连接，从而只有被应用程序请求的端口才会开放。这样就为网络提供了一种高度安全且兼具可控性和延展性的解决方案。

2.3.2.2 封包过滤 – ACL（访问控制列表）

ACL 规则是网络安全规范的一个基本模块。防火墙是用来监视每一个封包，解码包头中的出入信息，依据这些信息（源地址，目的地址，源端口，目的端口，ACL 定义协议），防火墙将作出判断和反应，将不安全的封包过滤阻挡，让安全的封包通过。

ACL 是将子网和子网之间进行分隔的有效措施。它可用作网络中的第一道安全防线，将某些特定规则的封包阻挡过滤，从而使内网计算机免受威胁。

RX3042H 内置防火墙的 ACL 策略支持:

- 基于源地址、目的地址、端口号和协议的过滤行为
- 使用通配符编写过滤规则
- 过滤规则优先级定义

2.3.2.3 DoS 攻击防护

RX3042H 防火墙具备了防攻击引擎，可将已知的各种网络攻击手段一一化解。它提供了自动防护功能，阻隔服务拒绝攻击 (DoS)，如 SYN 泛洪，IP 伪装，LAND，死亡之 Ping 和所有的重组攻击。例如，RX3042H 的防火墙提供 “WinNuke” 攻击保护，这种攻击方式以远程方式攻击互联网上未受保护的使用 Windows 操作系统的计算机。RX3042H 防火墙黑提供许多常见的互联网攻击防护，如 IP 伪装，死亡之 ping，LAND 攻击以及重组攻击。

RX3042H 提供的 DoS 攻击防护列于下表（表 2.1）中:

表 2.1 DoS 攻击

攻击类型	攻击名称
重组攻击	Bonk，Boink，Teardrop（New Tear），Overdrop，Opntear，Syndrop，Jolt，IP 碎片攻击
ICMP 攻击	死亡之 ping，伪装，Twinge
洪水攻击	ICMP 洪水，UDP 洪水，SYN 洪水
端口扫描	TCP SYN 扫描，TCP XMAS 扫描，TCP Null 扫描，TCP 秘密端口扫描
PF 规则攻击	回应攻击，Ascend Kill
其他攻击	IP 伪装，LAND，Targa，Winnuke

2.3.2.4 应用层网关（ALG）

一些应用程序，如 FTP 须通过设置相关参数以开启网络连接。为了使属于这些应用程序的封包通过防火墙到达内网，就需要设置相应的允许规则。如果没有这样的允许规则的话，这些封包就会被 RX3042H 的防火墙识别为不安全的封包而被丢弃。由于在防火墙为各种应用程序编写规则（同时不能影响安全性能）并不容易实现，因此，以应用层网关的形式为应用程序解析封包并打开动态连接就成为了一种智能化的解决方案。RX3042H 的 NAT 功能为常用的应用程序，如 FTP, Netmeeting 等提供了相应的 ALG 规则。

2.3.2.5 系统日志

可能会影响到安全的网络事件均被记录在 RX3042H 的系统日志文件中。这项日志在简略的记录了网络活动情况，如封包到达时间，防火墙动作描述，以及动作的原因。

2.4 产品外观

2.4.1 前面板

前面板包含了 LED 指示灯，显示主机工作状态。

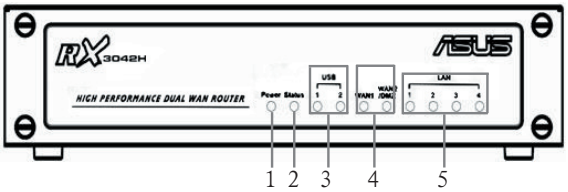


图 2.1 前面板 LED 指示灯

表 2.2 前面板标识和 LED 指示灯

	LED 标识	颜色	状态	表示意义
1	Power	绿色	亮灯	RX3042H 电源已接通
			熄灭	RX3042H 电源未接通
2	Status	绿色		
3	USB			USB 端口已识别
	1-2	绿色	熄灭	未侦测到 USB 设备
			亮灯	侦测到 USB 设备
4	WAN1 及 WAN2/ DMZ		熄灭	未侦测到连接
		绿色	亮灯	侦测到 100Mbps 连接
			闪烁	侦测到 100Mbps 数据传输
		琥珀色	亮灯	侦测到 10Mbps 连接
			闪烁	侦测到 10Mbps 数据传输
5	LAN			LAN 端口已识别
	1-4		熄灭	未侦测到连接
		绿色	亮灯	侦测到 100Mbps 连接
			闪烁	侦测到 100Mbps 数据传输
		琥珀色	亮灯	侦测到 10Mbps 连接
			闪烁	侦测到 10Mbps 数据传输

2.4.2 后面板

后面板包含了主机的数据和电源接口。

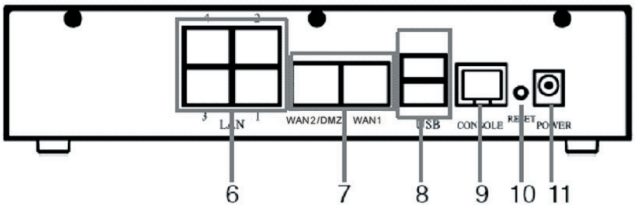
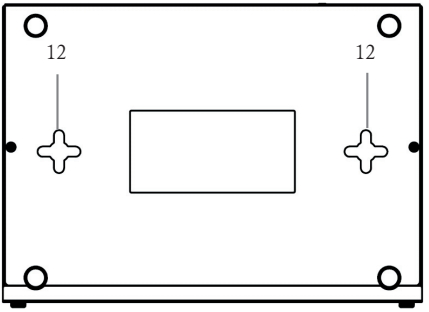


图 2.2 后面板标识和接口

表 2.3 后面板标识和 LED 指示灯

标识		表示意义
6	1–4	LAN 端口：使用以太网线将路由器主机连接到您电脑或局域网中的集线器 / 交换机上的以太网接口
7	WAN1 和 WAN2/DMZ	双 WAN 端口或一个 WAN 端口 + 一个 DMZ 端口：连接到您的 WAN 设备，如 ADSL 或 cable modem 或 DMZ 网络。请注意 DMZ 网络必须连接到标有 WAN2/DMZ 的端口上。
8	USB	USB 端口：连接到 USB 1.1 或 2.0 设备
9	Console	不支持
10	RESET	Reset 按钮: 1. 重新启动路由器 2. 按下按钮超过 5 秒即将路由器恢复为出厂设置
11	POWER	电源接口。连接到附带的 AC 电源适配器

2.4.3 底视图



12. 挂壁沟槽：您可以利用 RX3042H 背面的挂壁沟槽将路由器挂在墙上以节约空间。请根据电源插座位置，电源线长度，网线长度等和您的需要选择合适的壁挂位置。RX3042H 可以四种方向进行壁挂安装：前面板向上，后面板向上，左端向上和右端向上。

2.5 安置选择

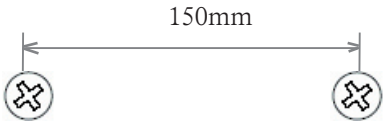
根据实际环境的需要，您可以在以下三种安置选择中选出最适合的方案：桌面摆放，磁吸和挂壁。

2.5.1 桌面安置

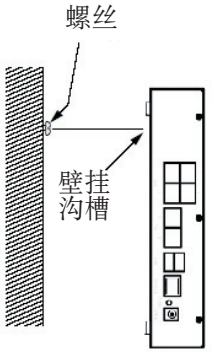
您可以将 RX3042H 摆放在任何水平平整的表面。RX3042H 节约空间的设计仅仅只占用您桌面的一角。

2.5.2 挂壁安装

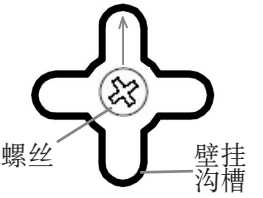
1. 在墙上固定两个螺丝，螺丝中心间距为 150mm，并保证这两个螺丝的直线距离平行于地面。



2. 将 RX3042H 的壁挂沟槽对准墙上的螺丝，并按下图所示将螺丝插入沟槽。壁挂设计可以支持四种不同方向：后面板向上，向下，向左和向右。



将壁挂沟槽对准墙上的螺丝。



如图所示将螺丝嵌入壁挂沟槽中，然后将主机向下推，使螺丝嵌入沟槽上端。

3 快速安装指南

本快速安装指南提供基本的指导，以帮助您将 RX3042H 与您的计算机或互联网进行连接。

- 第一部分：讲述如何连接硬件。
- 第二部分：讲述如何在您的计算机上配置网络属性。
- 第三部分：讲述如何在 RX3042H 进行基本设置，将您的局域网与互联网连接。

当设备的设置动作结束后，您可以参考第 26 页上的说明以确认设定是否有效。

本快速安装指南推测您已经安装了互联网服务供应商（ISP）认可的 ADSL 或 cable modem。这些安装指导所提供的是一些基本的设置，适合于家庭网络和小型办公网络。如需其他设置信息，请参考后续章节。

3.1 第一部分——连接硬件设备

在第一部分，首先您需要将路由器与 ADSL 或 cable modem（这些设备则连接到电话线接口或 cable 缆线接口），电源，和您的计算机或网络一一相连。

警告：*在开始连接之前，请将所有设备的电源断开，这些设备包括您的电脑，LAN 集线器／交换机（如有），以及 RX3042H 路由器。*

图 3.1 显示的是硬件连接方式。请按照下列步骤进行连接。

3.1.1 第一步：连接到 ADSL 或 cable modem

连接 RX3042H 路由器：将以太网线的一头连接到后面板处标记 WAN 的端口，另一头连接到 ADSL 或 cable modem 的以太网端口。

3.1.2 第二步：连接到计算机或网络

如果您的局域网中的计算机不多于 4 台，您可以使用网线将计算机直接连接到路由器主机上的交换端口。请注意，网线的一头接在路由器后面板的 1-4 端口的任何一个上，另一头接到计算机的以太网接口。

如果局域网中的计算机多于 4 台，那么您可以将网线的一头接在集线器或交换机（可能是这些设备的上行端口，具体请参见该集线器或交换机的使用说明），另一头接在 RX3042H 路由器的以太网交换接口（标记为 1-4）。

请注意，直连线和交叉线均可用于将 RX3042H 交换端口与计算机，集线器或交换机。RX3042H 的交换端口可支持这两种线缆。

3.1.3 第三步：连接 AC 电源适配器

将 AC 电源适配器连接到路由器的 “POWER” 接口，然后将适配器电源插头插入电源插座或接线板。

3.1.4 第四步：打开 RX3042H, ADSL 或 cable modem 的电源，并启动您的计算机

将 AC 电源适配器连接到 RX3042H 的电源接口，并开启 ADSL 或 cable modem，然后打开并启动计算机和／或其他局域网设备如无线 AP，集线器或交换机。

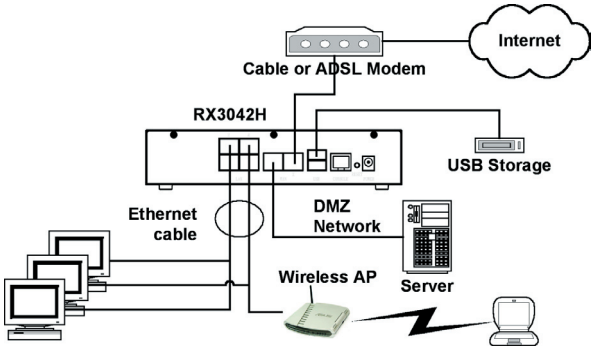


图 3.1 硬件连接简图

您需要确定 LED 指示灯显示情况如下表（表 3.1）。

表 3.1 LED 指示灯

LED:	指示情况:
POWER	绿灯亮表示设备已接通电源。如果指示灯不亮，请检查电源适配器是否已经连接到 RX3042H 路由器和电源插座。
LAN LED	绿灯亮表示设备已经和局域网连通并可以进行信息传输，绿灯闪烁说明路由器正在向／从局域网中的计算机传送或接收数据。
WAN	绿灯亮表示设备已经和服务供应商建立连接，绿灯闪烁说明路由器正在从互联网接收或传送数据。

如果 LED 指示灯显示如上表所列，就表示 RX3042H 已处于正常工作状态。

3.2 第二部分——设置您的计算机

本快速安装指南的第二部分提供关于在您的计算机上设置网络属性的指导，使之与 RX3042H 路由器配合工作。

3.2.1 设置之前

默认情况下，RX3042H 已经自动为您的计算机设定了所有必需的网络设置（如 IP 地址，DNS 服务器 IP 地址，默认网关 IP 地址）。您仅需对您的计算机进行设置，以接受 RX3042H 路由器的网络设置。

注意: *在某些情况下，您可能希望对某些或全部计算机进行手动网络设置，而不是让 RX3042H 来进行设置。在这种情况下, 请参见 17 页的 “为计算机分配静态 IP 地址”。*

- 如果您已经用网线将计算机连接到 RX3042H 路由器，请按照您计算机所使用的操作系统选择相应的设置方案。

3.2.2 Windows® XP

1. 在 Windows 任务栏中单击 < **开始** > 按钮，然后单击**控制面板**;
2. 双击**网络连接**图标;
3. 在 **LAN 或高速 Internet** 窗口，右键单击对应您的网卡(NIC)的图标，并点选**属性**(通常这个图标显示局域网连接) **本地连接**对话框显示目前已经安装的网络设备。
4. 确认 Internet 协议（TCP/IP）的复选框处于选中状态，然后点击 < **属性** > 按钮;
5. 在 Internet 协议（TCP/IP）属性对话框中，点选**自动获得 IP 地址**和**自动获得 DNS 服务器地址**;
6. 点选**确定**按钮两次确认新的设置，然后关闭控制面板。

3.2.3 Windows® 2000

首先，选择 IP 协议并且，如有必要，进行安装:

1. 在 Windows 任务栏中，点击**开始**按钮，指向**设置**，然后点选**控制面板**;
2. 双击**网络和拨号连接**图标;
3. 在**网络和拨号连接**窗口中，右键单击**本地连接**图标，然后选择**属性**;

   本地连接属性对话框显示目前已安装的网络部件。如果列表中包括 Internet 协议 (TCP/IP)，表示协议已经安装，直接跳到第 10 步;
4. 如果 Internet 协议 (TCP/IP) 未显示为已安装状态，请单击**安装**按钮。
5. 在**选择网络部件类型**对话框里，选择**协议**，然后单击**添加**按钮;
6. 在**网络协议**列表中选择 Internet 协议 (TCP/IP)，然后点**确定**按钮;

您可能会看到提示，要求从 Windows 2000 安装光盘或其他媒体安装。请根据提示进行安装。

7. 如果系统提示重新启动，请点**确定**保存设定并重启系统；然后，将计算机设置成接受 RX3042H 分配的 IP 地址。
8. 在控制面板，双击**网络和拨号连接**图标；
9. 在**网络和拨号连接**窗口，右键单击**本地连接**图标，然后选择**属性**。
10. 在**本地连接属性**对话框中，选择 Internet **协议 (TCP/IP)**，然后点击**属性**按钮；
11. 在 Internet **协议（TCP/IP）属性**对话框中，点击**自动获得 IP 地址**和**自动获得 DNS 服务器地址**
12. 点击**确定**按钮两次确认并保存设定，然后关闭控制面板。

3.2.4 Windows® 95，98，和 ME

1. 在 Windows 任务栏中，点击**开始**按钮，指向**设置**，然后点击**控制面板**；
2. 双击**网络**图标；

   在**网络**对话框中，查找以 “TCP/IP ->” 开头的条目和您使用的网络适配器的名称，然后点击**属性**按钮。您可能需要滚动导航条来寻找这些条目。如果列表中包含这些条目，那就表示 TCP/IP 协议已经启用，请跳至第 8 步；
3. 如果列表中没有显示 Internet 协议 (TCP/IP) 已安装，请按下**添加**按钮；
4. 在**选择网络部件类型**对话框中，选择**协议**，然后点击**添加**按钮；
5. 在厂商列表中选择 Microsoft，然后在**网络协议**列表中点击 TCP/IP，并点**确定**按钮；

   您可能会看到提示，要求您从 Windows 95, 98 或 Me 的安装光盘或其他媒体进行安装。请按照提示安装文件。

6. 如果系统提示重新启动，请点**确定**保存设定并重启系统；然后，将计算机设置成接受 RX3042H 分配的 IP 地址。
7. 在控制面板，双击**网络**图标；
8. 在**网络**对话框中，选择以 “TCP/IP –>” 开头的条目，然后点击**属性**按钮；
9. 在 TCP/IP 属性对话框中，点选**自动获得 IP 地址**的条目；
10. 在 TCP/IP 属性对话框中，点击**默认网关**。在**新网关**地址栏中输入 192.168.1.1（局域网中默认的 RX3042H 路由器地址），然后点击**添加**按钮添加默认网关；
11. 点击**确定**按钮两次确认并保存设定，然后关闭控制面板。
12. 如果系统提示重新启动计算机，请按**确定**保存新的设置。

3.2.5 Windows® NT 4.0 工作站

首先，查找 IP 协议，如果必要，请进行安装：

1. 在 Windows NT 任务栏处点击**开始**按钮，指向**设置**，然后点击**控制面板**；
2. 在控制面板窗口，双击**网络**图标；
3. 在**网络**对话框中，点选**协议**；

   协议显示的是当前已经安装的网络协议。如果列表中包括 TCP/IP 协议，那么就表示协议已经安装并启用，请跳至第九步；
4. 如果 TCP/IP 并未列入已安装组件列表，请单击**添加**按钮
5. 在**选择网络协议**对话框中，选择 TCP/IP，然后下**确定**按钮

   您可能会看到提示，要求从 Windows NT 安装光盘或其他媒体进行安装。请根据这些提示安装所需文件。文件安装完毕后，系统会弹出一个窗口通知您有一项称为 DHCP 的 TCP/IP 服务已经可以进行配置，从而实现动态分配 IP

信息。

6. 按**确定**按钮进入下一步，如果系统提示重新启动，请按下**确认**按钮；然后，将计算机设置成接受 RX3042H 分配的 IP 地址。
7. 打开控制面板窗口，然后双击**网络**图标;
8. 在**网络**对话框中，选择**协议**;
9. 在**协议**中，选择 TCP/IP，然后点击**属性**按钮;
10. 在 Microsoft TCP/IP 属性对话框中，单击**从 DHCP 服务器获取 IP 地址**;
11. 双击**确认**按钮确认并保存您的设置更改，然后关闭控制面板。

3.2.6 为您的计算机分配静态 IP 地址

在某些情况下，您可能需要直接对一些或全部的计算机手动分配 IP 地址（通常称为 “静态” 分配），而不是让 RX3042H 进行自动分配。在下列情况下您可能需要使用手动方式来分配静态 IP 地址:

- 您已经获得了一个或一个以上的公网 IP 地址，并且您希望这些地址被指派到专门的计算机上（例如，如果您把计算机作为公共网页服务器使用）。
- 您在局域网中设置了不同的子网。

然而，当您第一次设置 RX3042H 时，您必须为您的计算机设置一个 192.168.1.0 网段的 IP 地址，如 192.168.1.2，这样您才能够在 RX3042H 和您的计算机之间建立连接（这是因为 RX3042H 的默认局域网 IP 为 192.168.1.1）。在子网掩码一栏填入 255.255.255.0，默认网关设为 192.168.1.1。这些设置可以以后更改以反映实际的网络环境。

在为计算机设置静态 IP 信息时，请根据第 16，17 页上检索和

／或安装 IP 协议的步骤。安装完毕后，继续按照指导步骤将 Internet 协议 (TCP/IP) 设置成可见。这时不要启用 IP 地址，DNS 服务器，和默认网关的动态分配功能，按下单选按钮手动输入这些信息。

注意: *您的计算机的 IP 地址须与 RX3042H 的局域网端口的地址处于相同子网网段中。如果您需要手动为局域网中所有计算机设置 IP 信息，您可参考第五章中的内容相应更改局域网端口的 IP 地址。*

3.3 第三部分——快速设置 RX3042H

在第三部分中，您将登录 RX3042H 的设置管理界面，对您的交换机进行基本的设置。进行设置时需要填写您的 ISP 所提供的一些必要的信息。请注意，为了使您尽快地完成安装与设置，以下的提示很简短。如果您需要更多的信息，请查询相应的章节。

3.3.1 设置 RX3042H

请按照以下步骤来设置 RX3042H:

12. 在登录 RX3042H 的设置管理界面以前，请确认 浏览器里的 HTTP 代理器设置已被禁用。在 IE 里，单击**工具 -> Internet 选项 ... -> 连接 -> 局域网设置 ...**，然后不要选中**为 LAN 使用代理服务器**。
13. 打开任何一台已经与 RX3042H 四个 LAN 端口其中之一相连的 PC 机，打开浏览器，然后在地址栏里输入以下 URL:

http://192.168.1.1

这个是 RX3042H 预先为 LAN 端口定义好的 IP 地址。

弹出如图 3.2 所示的登录框:

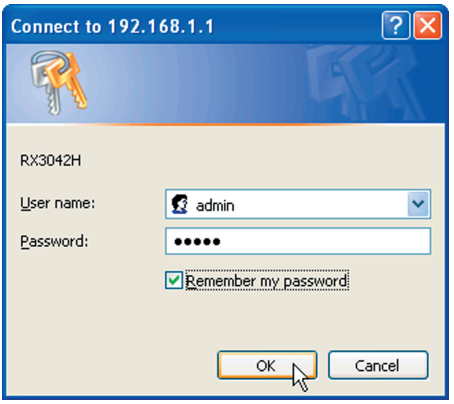


图 3.2 登录框

如果您与 RX3042H 连接不上，您应先检查您的 PC 是否接受 RX3042H 上的 IP 地址。另一个方法是设置您的 PC 机的 IP 地址为 192.168.1.0 网段里的任一 IP 地址，比如 192.168.1.2。

14. 输入您的用户名和密码，然后单击 "OK" 进入设置管理界面。如果您是第一次登录，请使用以下默认的设置:

默认用户名：admin
默认密码：admin

您可以随时更改自己的密码（请参考虑 90 页第 10.2 节登录密码和系统设置）

每当您登录时，都会出现以下系统状态页面（如图 3.3 所示）:

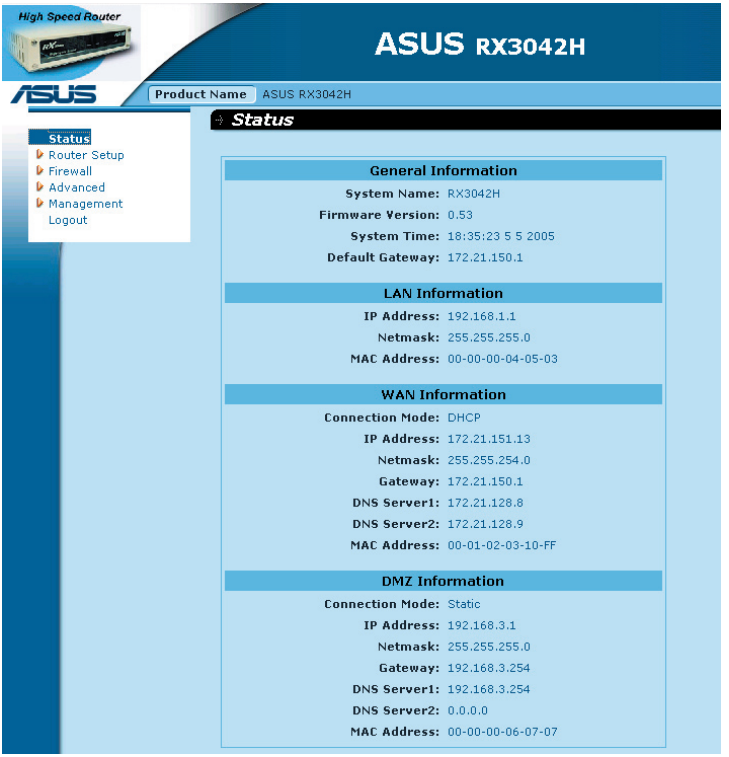


图 3.3 系统状态页面

15. 接着按照第五章 “路由器设置” 来设置 LAN 和 WAN。

当以上 RX3042H 的基本配置完成后，请仔细阅读以下章节来检查您是否可以连接上 Internet。

3.3.2 设置检测

此时，RX3042H 应可允许 LAN 里的任何电脑使用 RX3042H 的 ADSL 或 cable modem 接入互联网。

为了检测是否已成功连上互联网，打开您的浏览器，然后在地址栏输入任一外部网站 URL(如 http://www.asus.com)。WAN 的指示灯快速地闪烁着，当连通后，指示灯将一直亮着。您同样可以通过浏览器浏览到该网站的网页。

如果指示灯没有如上述描述那样亮着，或者网页未能显示，请查阅附录 12 来找寻解决问题的方法。

3.3.3 默认路由器设置

除了能控制与 ISP 的 DSL 连接以外，RX3042H 还能提供很多网络功能。这台机器已为典型的家用或小型办公网络预设了一些功能。

表 3.2 列出了一些非常重要的设置信息；在下面的章节我们将详细阐述这些信息。如果您对网络配置已经相当熟悉，请回顾表 3.2 检验是否与您需求一致。如有需要，请按照以下步骤来更改。如果您不是很熟悉那些设置，请使用但不要改动它们，或者可以联系 ISP 以寻求他们的帮助。

在您更改任何设置以前，请重温一下第四章关于登录和设置管理界面的一些基本信息。对此，我们再次向您提醒，在作任何改动以前，请事先征询 ISP。

表 3.2 默认设置概括

选项	默认设置	描述
DHCP（动态主机配置协议）	DHCP 服务器的 IP 地址为 192.168.1.100 至 192.168.1.200 被启用	RX3042H 保留了一系列自有的 IP 地址，以便能动态分配给 LAN 电脑。为了使用这些服务，您必须在您电脑里设置为动态地接收 IP 信息，正如快速安装指南中的第二部分所描述。请参考 6.1 查看关于 DHCP 的解释。
LAN 端口 IP 地址	静态 IP 地址：192.168.1.1 子网掩码：255.255.255.0	这个是 RX3042H 的 LAN 端口的 IP 地址。这个 LAN 端口把设备与 Ethernet 连接起来。您不需要更改任何有关 IP 地址的设置。请参考 5.1 查看有关 LAN 配置 LAN IP 地址。

4 使用设置管理界面

RX3042H 含有一个设置管理程序，它提供了软件安装的界面。它允许改变设备的设置以满足您的需要。您可以通过任何一台已连上 RX3042H 的 LAN 或 WAN 端口的 PC 机的浏览器登录进入。

本章将详细阐述如何使用设置管理界面。

4.1 登录设置管理界面

设置管理界面已预先安装在 RX3042H 了。为了能登入管理器，您需要先检查以下信息：

- 计算机已经按快速安装指南连接 上 RX3042H 的 LAN 或 WAN 端口
- 系统已经安装浏览器。建议使用 Microsoft Internet Explorer® 6.0 或更高版本。

您需从已连接上 RX3042H 的 LAN 或 WAN 端口的计算机登入管理器。但是，以下信息是针对通过 LAN 端口进入的计算机的:

1. 对于一个 LAN 的计算机，打开您的浏览器，在地址栏中输入以下信息，然后再按 <Enter>:

   http://192.168.1.1

   这个是预先已经设置好的 RX3042H 的 LAN 端口 IP 地址。接着弹出如图 4.1 所示的登录框:

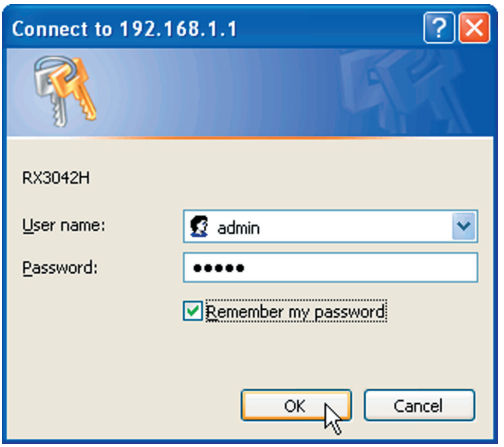


图 4.1 设置管理界面登录框

2. 输入您的用户名和密码，然后按 <ok>。

如果您第一次登录的话，请填入以下默认值:

默认用户名 : admin

默认密码 : admin

注意: *您可以随时更改您的密码（请参考 90 页第 10.2 节 登录密码和系统设置）.*

每一次您登录时，都会出现系统状态页面（如图 26 页的图 4.3 所示）。

4.2 功能结构

典型的配置页面包括广告条，菜单，菜单导航提示，配置信息以及在线帮助。您可以点击菜单上的任意一项来扩展或缩小菜单，或进入某一配置页面。您也可以通过配置窗体来对 RX3042H 进行配置。菜单导航提示会指引您如何通过菜单来获得配置信息。

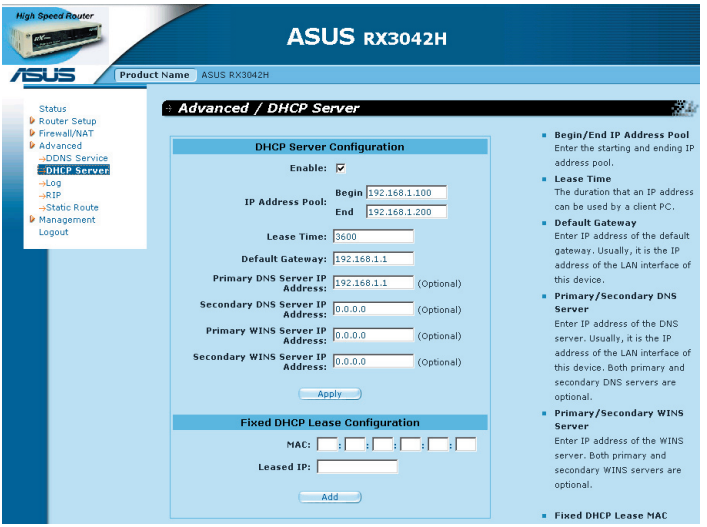


图 4.2 典型的管理设置页面

4.2.1 导航菜单

- 要扩展相关菜单，请双击菜单或图标：
- 要缩短相关菜单，请双击菜单或图标：
- 要打开具体的某一配置信息页面，请双击菜单或图标：

4.2.2 常用的按钮和图标

下列的按钮和图标是经常使用的。下述表格描述了每一个按钮和图标的具体作用。

表 4.1 常用的按钮和图标

按钮	作用
Apply	存储您对当前页所做的改动
Add	添加已有的配置给系统，比如静态的路由或者防火墙 ACL 规则等等
Modify	更改系统中已有的配置，比如静态的路由或者防火墙 ACL 规则等等
Reload	更改设置后刷新显示当前网页
	选中当前组件进行编辑
	删除选中的组件

4.3 系统设置简介

如果想查看全部的系统配置的话，请登录设置管理界面，或者登录后单击状态目录。图 4.3 显示出了载有一些可用信息的系统状态页面。

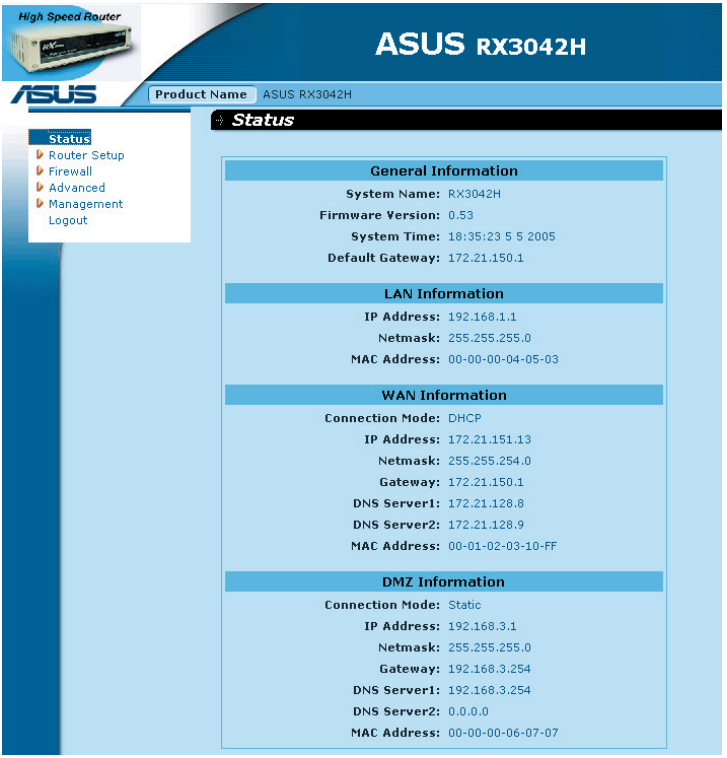


图 4.3 系统状态页面

5 路由器设置

本章将阐述如何使局域网中的计算机进行相互交流以及接入互联网 , 以及如何设置您的路由器。网络设置包括 LAN 和 WAN 的设置。

5.1 LAN 设置

5.1.1 LAN IP 地址

如果您所处的局域网中存在计算机，就需要把局域网上的各台计算机连接到以太网交换机的交换端口上。并且要为每一台设备都分配一个唯一的 IP 地址。LAN IP 地址用来标记 RX3042H 作为网络的一个节点，它必须具有同 PC 机一样的子网。默认的 RX3042H 的 LAN IP 地址是 192.168.1.1。

***定义**：一个网络节点可以被看作是设备与网络相连接的接口，比如说 RX3042H 的 LAN 端口以及 PC 机上的网络接口卡。请参考附录 11 中关于子网的介绍。*

您可以将默认 IP 地址改为您想使用的真实的 IP 地址。

5.1.2 LAN 配置参数

表 5.1 列出了 LAN IP 设置有效的配置参数。

表 5.1 LAN 配置参数

字段	描述
Host Name (主机名)	用于辨认主机身份
IP Address (IP 地址)	RX3042H 的 LAN IP 地址。这个 IP 地址是用来鉴别您的 RX3042H LAN 端口的。请注意您的 ISP 提供给您的公共 IP 地址不是您的 LAN IP 地址。公共 IP 地址是用来鉴别 RX3042H 上的 WAN 端口的。

字段	描述
Subnet Mask（子网掩码）	LAN 的子网掩码是用来区分哪一部分 LAN IP 地址属于网络地址，哪一部分是主机地址。默认的子网掩码是 255.255.255.0。

5.1.3 设置 LAN IP 地址

请按以下步骤来改变您默认的 LAN IP 地址:

1. 点击 Router Setup->Connection 菜单，打开连接配置页面，如下图 5.1 所示。

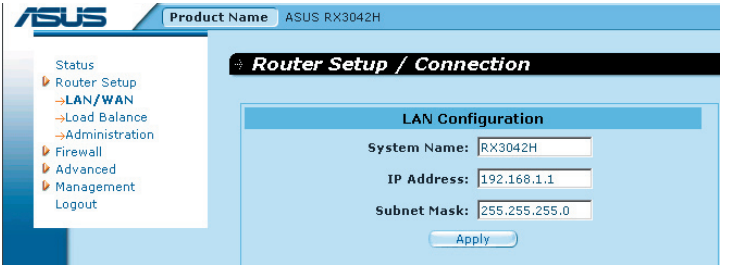


图 5.1 网络设置配置 - LAN 配置

2. （可选）给 RX3042H 输入一个主机名。请注意，主机名只是为了区分所用，没有其他特殊意义。
3. 在空白框里输入 RX3042H 的 LAN IP 地址以及子网掩码。
4. 如果您还没有设置 WAN 端口的话，请接着设置 WAN。
5. 点击 Apply 保存这些设置。如果当前正在使用以太网连接，改变了 IP 地址或子网掩码后，连接将会中断。
6. 接着您会看见以下所显示的信息:

7. 如果连接超时，您只需重新登录即可继续进行设置。

5.2 WAN/DMZ 配置

本节将阐述怎样为 RX3042H 配置 WAN / DMZ 以便与 ISP 交流。您将了解如何配置 WAN 的 IP 地址，DHCP 和 DNS 服务器。

DMZ 是位于企业内部网络和外部网络如 Internet 之间的一台主机或一个小型网络。在这个网络区域内可以放置一些公开的服务器设施，如 Web 服务器，FTP 服务器，SMTP (e-mail) 服务器以及 DNS 服务器。DMZ 区域内不包含任何机密信息。这样，即使 DMZ 内的信息处于公开状态，公司其他机密信息也不会被暴露。

注意：只有静态 IP 连接模式支持 DMZ。

5.2.1 WAN 连接模式

RX3042H 支持五种 WAN 连接模式：静态 IP，动态 IP，PPPoE (multi-session)，PPPoE unnumbered 以及 PPTP。您可根据您 ISP 所要求，从图 5.2 所示的网络设置页面的 connection mode 下拉列表中选择一种 WAN 连接模式。

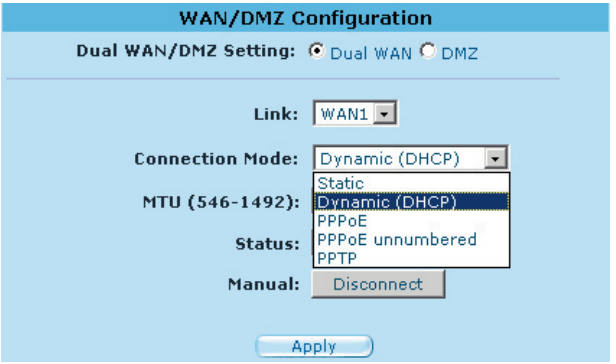


图 5.2 网络设置页面——WAN 配置

5.2.2 PPPoE

PPPoE 连接是 ADSL 服务提供提供的最常见的连接方式。

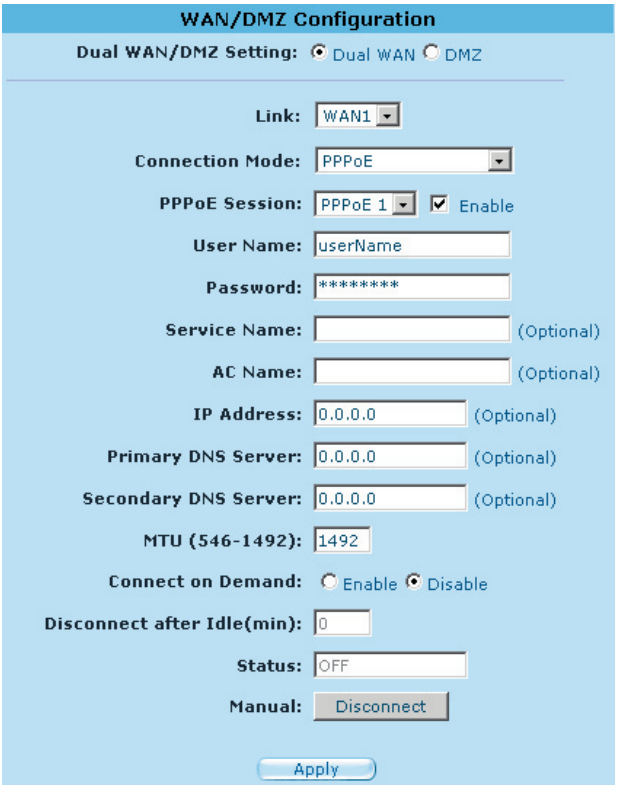


图 5.3. WAN—— PPPoE 配置

5.2.2.1 WAN PPPoE 配置参数

表 5.2 列举出了 PPPoE 连接模式的配置参数。

表 5.2. WAN PPPoE 配置参数

字段	描述
link	选择一个端口进行配置。可选的选项有 WAN1，WAN2 或 DMZ。
connection mode（连接模式）	从 connection mode 下拉列表中选择 PPPoE。

字段	描述
PPPoE Session	为 PPPoE session 选择一个 PPPoE session ID 。请注意只能同时支持两种 PPPoE sessions。
Enable（启用）	选中或不选中复选框来激活或停止 PPPoE session 功能。
User Name and Password（用户名、密码）	输入您登录 ISP 时所用的用户名和密码。（请注意这与您登录设置管理界面的用户名和密码是不一样的。）
Service Name（服务名称）	输入 ISP 提供的服务名称。服务名称可以不用填写，不过有些 ISP 要求必须填。
AC Name（AC 名）	输入您 ISP 提供的接入集中器名称。此项可选填，但是有些 ISP 要求必须填。
IP Address（IP 地址）	如果您的 ISP 允许 WAN 使用同样的 IP 地址，请在此输入。
Primary /Secondary DNS Server（第一 / 第二 DNS 服务器）	第一和 / 或第二个 DNS 服务器的 IP 地址可选填，因为 PPPoE 将自动地检测您的 ISP 设置的 DNS IP 地址。尽管如此，如果您想要使用其它的 DNS 服务器，在此输入其 IP 地址。
MTU	您可以指定传送的数据包的最大大小。对于 PPPoE 来说，MTU 值的范围是从 546 到 1492。默认值是 1492。
Connect on Demand（仅在需要时连接）	点击 Enable 或 Disnable 按钮来启用或禁用这项功能。
Disconnect after idle (min.)（空闲断开时间（分））	输入不活动超时时间，用于没有流量时可自动断开网络连接。数字 0 表示没有超时时间。请注意如果 SNTP 启用的话，它会干扰这项功能。

字段	描述
Status (状态)	On: PPPoE 连接活动中。 Off: PPPoE 连接已停止。 Connecting: RX3042H 正尝试用 PPPoE 模式连接您的 ISP。
Manual Disconnect /Connect (手动断开 / 连接)	点击 Disconnect 或 Connect 按钮来断开或连接 PPPoE 连接。

5.2.2.2 设置 WAN 模式下的 PPPoE

请按照以下步骤配置 PPPoE:

1. 点击 Router Setup -> Connection 菜单，打开 Network Setup 设置页面。
2. 为 PPPoE connection mode 选择一个 WAN 端口进行配置 (WAN1/WAN2) 。
3. 如图 5.3 所示，从 WAN connection mode 下拉列表中选择 PPPoE 。
4. 从 PPPoE session ID 下拉列表中选择 PPPoE session ID 。目前，每个 WAN 端口支持两个 session。
5. 若 ISP 要求，请输入服务名。(可选)
6. 如果您的 ISP 要求的话, 请输入服务名和 / 或 AC 名。(可选)
7. 如果 ISP 允许您为 WAN 使用同样的 IP 地址的话，请在 IP 地址栏输入。否则，跳过此步。(可选)
8. 如果您想使用首选的 DNS 服务器，请为第一和 / 或第二个 DNS 服务器输入 IP 地址。否则，跳过此步。(可选)
9. 若需要请更改 MTU 值。如果您不知道填什么值，请保留原值。对于动态 IP 连接模式来说，MTU 值的范围是从 546 到 1492。默认值是 1492。
10. 为 Disconnect after Idle (min) 以及 Connect on Demand

输入合适的连接设置。

11. 点击 Apply 保存设置。

5.2.3 PPPoE Unnumbered

一些 ADSL 服务提供商会提供 PPPoE unnumbered 服务。如果您的 ISP 提供了这项服务，请选择这种连接模式。

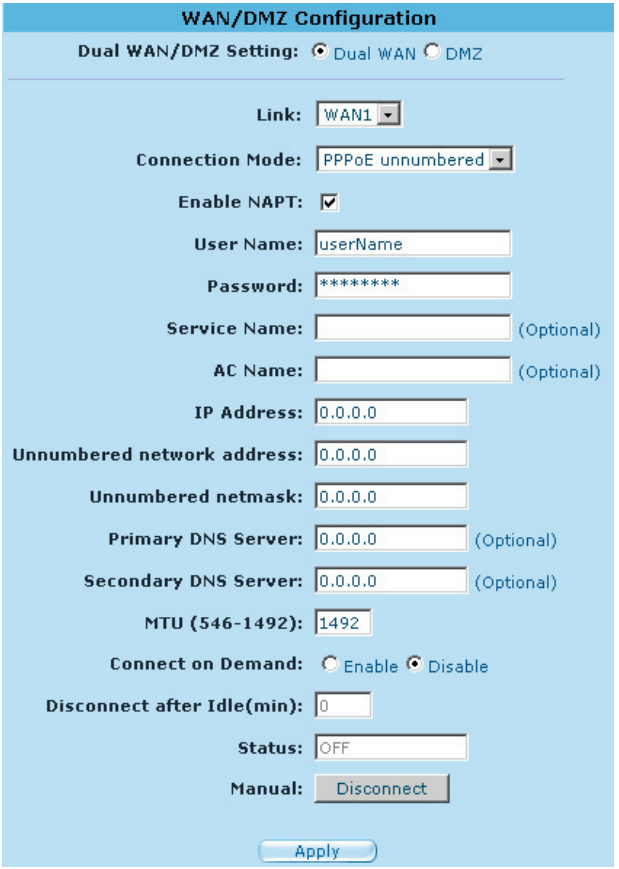


图 5.4. WAN —— PPPoE Unnumbered 配置

5.2.3.1 WAN PPPoE Unnumbered 配置参数

表 5.3 列举出了 PPPoE Unnumbered 连接模式的配置参数:

表 5.3. WAN PPPoE Unnumbered 配置参数

字段	描述
Link	选择一个端口进行配置。可选的选项有 WAN1，WAN2 或 DMZ。
connection mode（连接模式）	从 connection mode 下拉列表中选择 PPPoE Unnumbered。一般说来，每一个网络接口必须有一个独一无二的 IP 地址。但是，unnumbered 接口就不一定有。这样，当此选项被选后，WAN 和 LAN 就使用同一 IP 地址。因此网络 IP 地址使用得更少，路由表更小，从而更加节省网络资源。
Enable NAPT（启用 NAPT）	点选或不点选此项来启用或禁用 NAPT 功能。
User Name and Password（用户名和密码）	输入您登录 ISP 时所用的用户名和密码。（请注意这与您登录设置管理界面的用户名和密码是不一样的。）
Service Name（服务名）	输入 ISP 提供的服务名。服务名可以不用填写，不过有些 ISP 要求必须填。
AC Name（AC 名）	输入您 ISP 提供的接入集中器名称。此项可选填，但是有些 ISP 要求必须填。
IP Address（IP 地址）	为 PPPoE unnumbered 连接输入一个静态的 IP 地址。此 IP 地址必须由您的服务提供商提供。
Unnumbered Network Address（Unnumbered 网络地址）	输入您 ISP 提供的网络地址。

字段	描述
Primary / Secondary DNS Server (第一 / 第二 DNS 服务器)	第一和 / 或第二个 DNS 服务器的 IP 地址可选填，因为 PPPoE 将自动地检测您的 ISP 设置的 DNS IP 地址。尽管如此，如果您想要使用其它的 DNS 服务器，在此输入其 IP 地址。
MTU	您可以指定传送的数据包的大小上限。对于 PPPoE 来说，MTU 的范围是从 546 到 1492。默认值是 1492。
Connect on Demand (仅在需要时连接)	点击 Enable 或 Disnable 按钮来启用或禁用这项功能。
Disconnect after Idle (min.) (空闲断开时间(分钟))	输入不活动超时时间，用于没有流量时可自动断开网络连接。数字 0 表示没有超时时间。请注意如果 SNTP 启用的话，它会干扰这项功能。
Status（状态）	On: PPPoE unnumbered 连接活动中。 Off: PPPoE unnumbered 连接已停止。 Connecting: RX3042H 正尝试用 PPPoE unnumbered 模式连接到您的 ISP。
Manual Disconnect / Connect（手动断开 / 连接）	点击 Disconnect 或 Connect 按钮来断开或连接 PPPoE unnumbered。

5.2.3.2 设置 WAN 模式下 PPPoE Unnumbered

按照以下步骤来设置 PPPoE unnumbered:

1. 点击 Router Setup -> Connection 菜单，打开网络设置页面。
2. 为 PPPoE unnumbered connection mode 选择一个 WAN 端口进行配置 (WAN1/WAN2)。
3. 如图 5.4 所示，从 WAN connection mode 下拉列表中选择 PPPoE Unnumbered。

4. 如果连接使用了 NAT 的话，请选择 NAPT 。
5. 输入 ISP 提供的用户名和密码。
6. 如果您的ISP 要求的话, 请输入服务名和／或 AC 名。(可选)
7. 输入 ISP 提供的 IP 地址，unnumbered 网络地址，以及 unnumbered 子网掩码。
8. 如果您想使用首选的 DNS 服务器，请为第一和／或第二个 DNS 服务器输入 IP 地址。否则，跳过此步。(可选)
9. 若需要请更改 MTU 值。如果您不知道填什么值，请保留原值。对于 dynamic IP 连接模式来说，MTU 值的范围是从 546 到 1492。默认值是 1492。
10. 为 Disconnect after Idle (min) 以及 Connect on Demand 设定合适的连接设置。
11. 点击 Apply 保存设置。

5.2.4 动态 IP

动态 IP 通常由 cable modem 服务提供商使用。

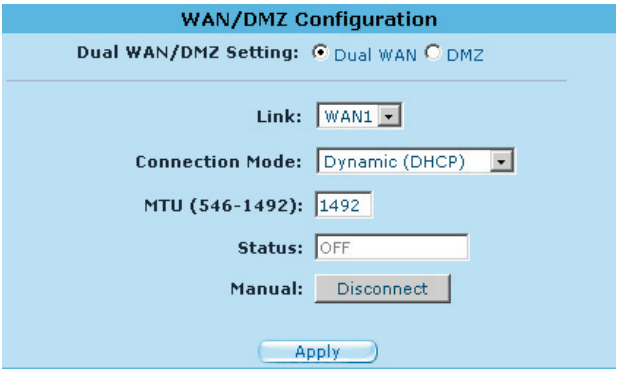


图 5.5. WAN —— 动态 IP (DHCP 客户端) 配置

5.2.4.1 设置 WAN 模式下的动态 IP 地址

请按照以下步骤配置动态 IP:

1. 点击 Router Setup -> Connection 菜单，打开网络设置页面。

2. 为动态 IP 连接模式选择一个 WAN 端口进行设定（WAN1/WAN2）。
3. 如图 5.5 所示，从 WAN connection mode 下拉列表中选择动态。请注意第一个 IP 地址和（或）第二个 DNS 服务器是由您的 ISP 的 DHCP 服务器自动分配的。
4. 若需要请更改 MTU 值。如果您不知道填什么值，请保留原值。对于动态 IP 连接模式来说，MTU 值的范围是从 546 到 1500。默认值是 1500。
5. 点击 Apply 保存设置。

5.2.5 静态 IP

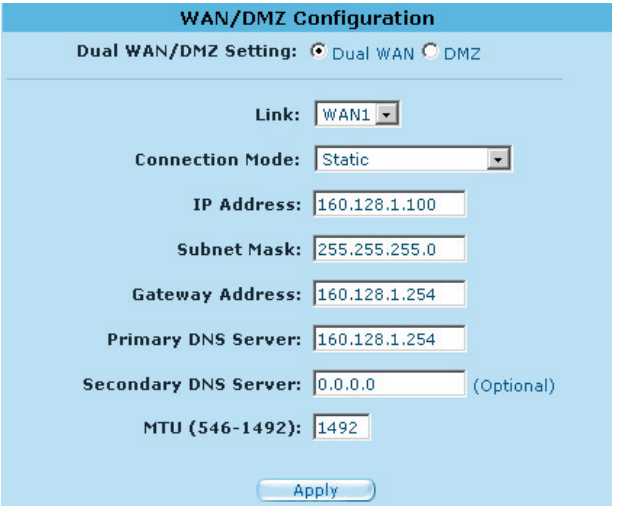


图 5.6. WAN——静态 IP 配置

5.2.5.1 WAN 或 DMZ 静态 IP 的配置参数

表 5.4 列举出了静态 IP 的配置参数:

表 5.4. WAN 静态 IP 配置参数

字段	描述
Link	选择一个端口进行配置。可选的选项有 WAN1/WAN2 或 WAN/DMZ。
connection mode (连接模式)	从 connection mode 下拉列表中选择 static
IP 地址 (IP Address)	WAN/DMZ IP 地址。请注意 WAN IP 地址是由您的 ISP 提供的公网地址，而 DMZ IP 地址则是网内地址。
子网掩码 (Subnet Mask)	您的 ISP 提供的 WAN 子网掩码。 一般来说，默认为 255.255.255.0。
网关地址 (Gateway Address)	您的 ISP 提供的网关 IP 地址。它同 RX3042H 的 WAN 的子网是一样的。
第一 / 第二 DNS 服务器 (Primary/Secondary DNS server)	您必须至少输入第一个 DNS 服务器的 IP 地址。第二个选填。
MTU	您可以指定传送的数据包的最大大小。对于静态 IP 连接而言，MTU 的范围是从 546 到 1500。默认值是 1500。

5.2.5.2 设置 WAN 或 DMZ 模式下的静态 IP 地址

请按照以下步骤配置静态 IP:

1. 点击 Router Setup -> Connection 菜单，打开 Network Setup 设置页面。
2. 为 static connection mode 选择一个 WAN (WAN1/WAN2) 端口或 DMZ 端口进行配置 。
3. 如图 5.6 所示，从 WAN connection mode 下拉列表中选择 static。
4. 在 IP 地址框中输入 WAN IP 地址。该地址应由您的 ISP 提供。
5. 输入 WAN 的子网掩码。该信息也应由您的 ISP 提供。一般来说，默认为 255.255.255.0。

6. 在空白框中输入 ISP 提供的网关地址。
7. 输入第一 DNS 服务器的 IP 地址。该信息应由您的 ISP 提供。第二和第三 DNS 服务器为选填。
8. 若需要请更改 MTU 值。如果您不知道填什么值，请保留原值。对于动态 IP 连接模式来说，MTU 值的范围是从 546 到 1500。默认值是 1500。
9. 单击 Apply 保存设置。

5.2.6 PPTP

一些服务提供商要求用户通过 PPTP 进行连接。

5.2.6.1 WAN PPTP 配置参数

表 5.5 列举了 PPTP 连接模式的有效配置参数。

表 5.5. WAN PPTP 配置参数

字段	描述
Link	选择一个端口进行配置。可选的选项有 WAN1, WAN2 或 DMZ。
connection mode (连接模式)	从连接下拉列表中选择 PPTP 。
WAN Interface IP	选择 WAN IP 地址如何配置——静态 (手动设置 IP 地址) 或动态 (自动从 DHCP 服务器获取)
Static (静态)	如果 WAN IP 是您 ISP 提供的固定的 IP，那么请选择这种连接模式。
IP Address (IP 地址)	输入您的 ISP 提供的 WAN IP 的地址。
Subnet Mask (子网掩码)	输入您的 ISP 提供的 WAN IP 的子网掩码地址。
Gateway Address (网关地址)	输入您的 ISP 提供的 WAN 的网关 IP 地址。
Dynamic (DHCP) (动态 DHCP)	如果您的 WAN IP 地址是自动的从您 ISP 的 DHCP 服务器上获得的话，请选择这种 连接模式。

字段	描述
User Name and Password (用户名和密码)	输入您用来登录 ISP 的用户名和密码 (注意: 与您登录设置管理界面的密码是不一样的。)
Server IP Address (服务器 IP 地址)	输入 ISP 提供的 PPTP 服务器 IP 地址。
MTU	您可以指定传送的数据包的最大大小。对于 PPTP，MTU 值的范围是从 546 到 1460。默认值是 1460。
MPPE	MPPE 表示微软点对点加密协议 (Microsoft Point-to-Point Encryption protocol)。如果数据包使用此协议加密的话，请选中此项。
Connect on Demand (仅在需要时连接)	点击 Enable 或 Disable 按钮来启用或禁用这项功能。
Disconnect after Idle (min) 空闲断开时间 (分)	输入不活动超时时间，用于没有流量时可自动断开网络连接。数字 0 表示没有超时时间。请注意如果 SNTP 启用的话，它会干扰这项功能。
Status (状态)	On: PPTP 连接活动中。 Off: PPTP 连接已停止活动。 Connecting: RX3042H 正尝试使用 PPTP 模式连接到 ISP。
Manual Disconnect /Connect (手动断开 / 连接)	点击 Disconnect 或 Connect 按钮断开 / 连通 PPTP 连接。

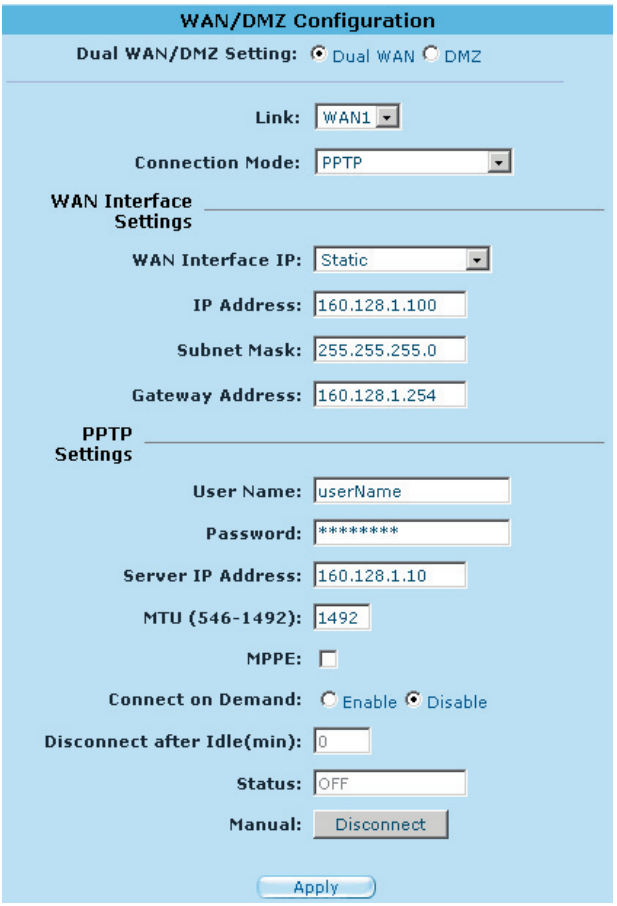


图 5.7. WAN —— PPTP 配置

5.2.6.2 设置 WAN 模式下的 PPTP

请按照以下步骤来进行 PPTP 设置:

1. 点击 Router Setup ->Connection 菜单，打开网络设置页面。
2. 为 PPTP 连接模式选择一个 WAN 端口进行配置（WAN1/WAN2）。

3. 如图 5.7 所示，从 WAN connection mode 下拉列表中选择 PPTP。
4. 选择获取 WAN IP 的方式——静态或动态。如果 ISP 提供固定的 IP 地址，请在 WAN Interface IP 下拉列表中选择 Static。如果您不能确认，请咨询您的服务 ISP。
5. 如果您的 WAN IP 是手动设置的话，请输入 IP 地址、子网掩码以及网关 IP 地址。
6. 输入 ISP 提供的用户名和密码。
7. 输入 ISP 提供的 PPTP 服务器 IP 地址。
8. 若需要请更改 MTU 值。如果您不知道填什么值，请保留原值。对于 PPTP 连接模式来说，MTU 值的范围是从 546 到 1460。默认值是 1460。
9. 如果数据包使用 MPPE 协议进行加密，请选择 MPPE。
10. 定义 Disconnect after Idle（min）和 Connect on Demand。
11. 点击 Apply 保存设置。

5.3 WAN Load Balancing 和 Line Back Up

在 WAN 连接中，RX3042H 支持 load balancing 以及 line back up 动能。只有当在 Router Connection（路由连接）设置页面中选择 Dual-WAN 后（点击 Router Setup ->Connection 菜单），才能启用这些功能。

通过 RX3042H 上的两个 WAN 端口，WAN load balancing 根据预设的带宽需求来处理通信活动。另一个特性是可支持 WAN 端口的故障恢复（fail-over）功能。如果 WAN 连接停止活动的话，RX3042H 将把停止活动的端口上的数据流量引导至另一个端口上。

line back up 是另外一个用于保证连续 Internet 接入的功能。当第一个 WAN 端口连接中止，Internet 访问将自动转到备份的 WAN 端口连接上。

5.3.1 WAN Load Balancing 和 Line Back Up 配置参数

表 5.6 列举出了 WAN load balancing 以及 line back up 的有效配置参数。

表 5.6. WAN Load Balancing 和 Line Back Up 配置参数

字段	描述
Load Balance (负载均衡)	选择下面三项中的其中一项: Disable: 禁用 WAN load balancing 和 line back up 功能。 Auto Mode: 如果需要 load balancing 的话, 选择此项。此选项对 load balancing 是很有用的。 Line Backup: 如果需要 line backup 的话, 选择此项。在默认情况下, 第一个连接总是设为 WAN1 , 备份连接设为 WAN2。
WAN1/WAN2 Bandwidth (WAN1/WAN2 带宽)	输入您想要分配到每个 WAN 端口的流量大小比率。比率值在 0 与 100% 之间。比如, WAN1 80% 和 WAN2 20% 表示有 80% 的流量分配给 WAN1, 有 20% 的流量分配给 WAN2。
Connectivity Check (连接检查)	点击 Enable 或 Disable 按钮来启用或禁用这项功能。连通性检查是用于监控 WAN 端口的连接状态。如果此功能禁用, RX3042H 将不能实施故障恢复 (fail-over)。这样, 如果其中一个 WAN 连接中止, 该端口上的数据流量就不能转到正常工作的端口上。所以您应该选择此项以保持此功能启用。但是, 如果网关或一些特定的网络设备不响应 ping 的话, 您需要禁用此项功能。否则, 对于 WAN 连接状态, RX3042H 会做出不正确的判断, 因此影响到 load balancing 或 line back up 的动作。
Connectivity Check Interval (连接检查间隔时间)	RX3042H 检查 WAN 连接状态的间隔时间。可填的值在 1 到 60 秒之间。

字段	描述
Connectivity Check IP Address (WAN1) (连接检查 IP 地址 WAN1)	输入流量通过的特定网络设备的 IP 地址。此项为可选填。一般来说，您不需要在此填入任何 IP 地址，除非您知道流量必须通过哪个特定的网络设备。
Connectivity Check IP Address (WAN2) (连接检查 IP 地址 WAN2)	输入流量通过的特定网络设备的 IP 地址。此项为可选填。一般来说，您不需要在此填入任何 IP 地址，除非您知道流量必须通过哪个特定的网络设备。

5.3.2 设置 WAN Load Balancing

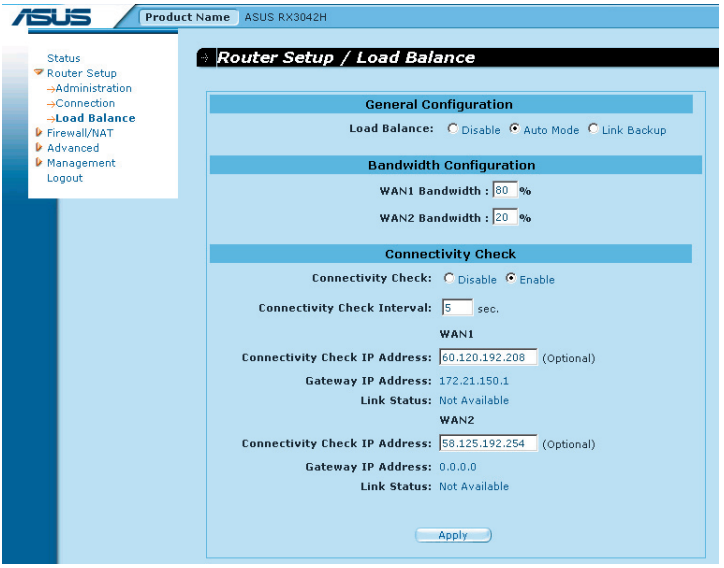


图 5.8. Load Balancing 配置

请按照以下步骤来设置 WAN load balancing:

1. 点击 Router Setup –>Load Balance 菜单，打开负载均衡配置页面。
2. 在 Load Balance 框中选择 Auto Mode。
3. 输入您想要分别分配到两个 WAN 端口的流量大小比率。

比率值在 0 与 100% 之间。两个值总和是 100%。

4. 选择您是否需要启用或禁用连接性检查功能。如果此功能启用的话，请输入以下信息:

   a) 输入连接性检查间隔时间。

   b) 输入 WAN1 和 / 或 WAN2 连接性检查的 IP 地址。(可选)

5. 点击 Apply 保存设置。

5.3.3 设置 WAN Line Back Up

请按照以下步骤设置 line backup:

1. 点击 Router Setup –>Load Balance 菜单，打开 Load Balancing 设置页面。
2. 在 Load Balance 框中选择 Line Backup。
3. 选择您是否需要启用或禁用连接性检查功能。如果此功能启用的话，请输入以下信息:

   a) 输入连接性检查间隔时间。

   b) 输入 WAN1 和 / 或 WAN2 连接性检查的 IP 地址。(可选)

4. 点击 Apply 保存设置。

6 DHCP 服务器设置

6.1 DHCP（Dynamic Host Control Protocol，动态主机配置协议）

6.1.1 什么是 DHCP?

DHCP 是一种协议，它允许网络管理员集中管理 IP 地址分配给网络上的计算机。

当您启用了 DHCP 以后，您允许类似 RX3042H 这样的设备分配临时 IP 地址给已连网的计算机。这种分配 IP 的设备就叫 DHCP 服务器，而接收 IP 的设备叫 DHCP 客户端。

注意: *如果按照快速安装指南的指示进行，您可以给每一个 LAN PC 机配置一个 IP 地址，或者可以让它动态地（自动地）接收 IP 信息。如果选择动态分配，您需要把 PC 机设置为 DHCP 客户端，这样它才能接收从类似 RX3042H 的 DHCP 服务器发来的 IP 地址。*

DHCP 服务器内有 IP 地址，当计算机向它发出需求请求时，它会暂时 “借” 出一会。它会根据需要，掌控、收集和重新分配这些地址。

在启用 DHCP 的网络中，IP 的信息动态地被分配。每次 DHCP 客户端连上网络时，它都会被动态地分配不同的地址。

6.1.2 为什么使用 DHCP?

DHCP 允许您通过 RX3042H 管理和分配 IP 地址。如果没有 DHCP，您必须为每一台计算机单独配置 IP 地址和相关信息。DHCP 通常用于大型网络以及那些经常需要扩大或升级的网络。

6.1.3 配置 DHCP 服务器

注意：按默认设置，RX3042H 被设为 LAN 上的 DHCP 服务器，且已被分配有从 192.168.1.100 到 192.168.1.149 的 IP 地址（子网掩码是 255.255.255.0）。若要改变地址的范围，请按照本节所描述的步骤进行。

首先，您必须把您的计算机设置为接受 DHCP 服务器 IP 地址分配的模式:

1. 单击 Advanced-> DHCP Server 菜单，打开 DHCP Server 配置页面，如下图 6.1 所示。

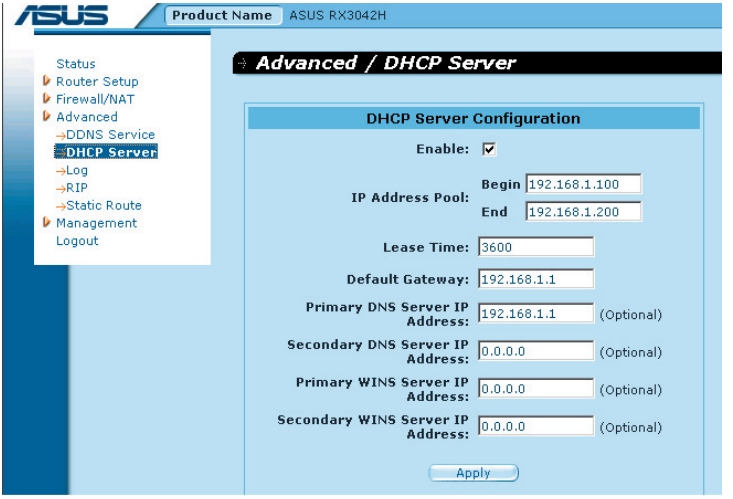


图 6.1. DHCP 服务器配置页面

2. 输入 IP 地址池（开始／结束地址），子网掩码，借出时间以及默认网关 IP 地址，范围等信息，以及其它信息都是可选填的，如第一／第二 DNS 服务器 IP 地址，第一／第二 WINS 服务器 IP 地址。但是，第一 DNS 服务器的 IP 地址是必须填的。您可以在其框里输入 LAN IP 或 ISP 的 DNS IP。表 6.1 详细列举出了 DHCP 配置参数。

表 6.1. DHCP 配置参数

字段	描述
Enable （启用）	激活或不激活 DHCP 服务器服务
IP Address Pool Begin/End （IP 地址池开始／结束）	定义 DHCP 地址池的最低和最高的地址
Lease Time （租约时间）	被分配的地址会被设备所使用的时间
Default Gateway IP Address （默认网关 IP 地址）	从地址池接收 IP 地址的默认网关的地址。默认网关是 DHCP 客户端最初与互连网相通的设备。一般来说，这个地址是 RX3042H 的 LAN 端口的 IP 地址。
Primary/ Secondary DNS Server IP Address （第一／第二 DNS 服务器 IP 地址）	用来接收 IP 地址的域名服务器（DNS）的 IP 地址。DNS 服务器把您在浏览器地址栏中输入的通用网址转换成自己能识别的数字 IP 地址。一般说来，DNS 服务器都在 ISP 那里。但是，您可以输入 RX3042H 的 LAN IP 地址，因为它有 DNS 代理的功能，能将 DNS 请求提交给 DNS 服务器，然后把反馈结果转交给 LAN 计算机。请注意第一个和第二个 DNS 服务器都是选填的。
第一／第二 WINS 服务器的 IP 地址（选填）	用来接收 IP 地址的 WINS 的 IP 地址。您不需要输入此信息除非网络中有 WINS 服务器。

3. 点击 Apply 保存 DHCP 服务器配置信息。

6.1.4 查看当前 DHCP 地址分配情况

当 RX3042H 作为一个 DHCP 服务器运作时，它保存了分配给计算机的所有地址的记录。如想查看所有当前 IP 地址分配情况表，只需要打开 DHCP 服务器配置页面，然后点击位于页面底部的链接 Current DHCP Lease（当前 DHCP 租约表）。即可出现如图 6.2 所示的页面。

DHCP 租约表列举出了所有已分配的 IP 地址以及相对应的 MAC 地址。

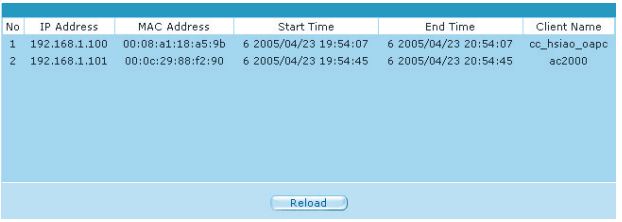


图 6.2. DHCP 租约表

6.1.5 DHCP 固定租约

DHCP 固定租约主要用于主机需要从 DHCP 服务器获取固定 DHCP 地址的情况。首先，设置计算机使其能够接受 DHCP 服务器分配的 DHCP 信息。

6.1.5.1 进入 DHCP 固定租约配置页面——（Advanced-> DHCP Server）

打开 Fixed DHCP Lease（DHCP 固定租约）配置页面，如图 6.3 所示，单击 Advanced-> DHCP Server 菜单。

请注意当您打开 DHCP 固定租约设置页面时，如图 6.3 所示，一张当前使用的租约表将显示在配置页面的下方。

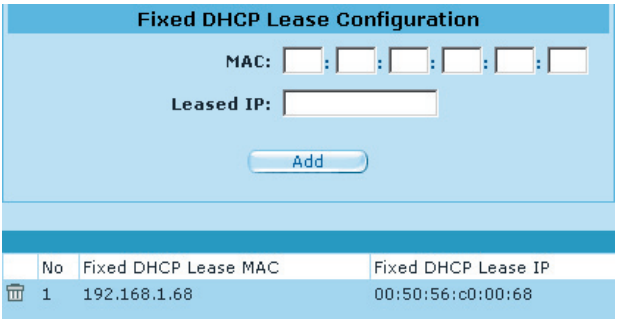


图 6.3. DHCP 固定租约设置页面

6.1.5.2 添加一个 DHCP 固定租约

若想要添加一个 DHCP 固定租约，请按以下步骤进行:

1. 点击 Advanced-> DHCP Server 菜单，如图 6.3 所示，打开 Fixed DHCP Lease 设置页面。
2. 输入 MAC 地址以及主机所需要的固定 IP 地址。表 6.2 详细列举出了 DHCP 固定租约配置参数 。

表 6.2. DHCP 固定租约配置参数

字段	描述
Fixed DHCP Lease MAC (DHCP 固定租约 MAC 地址)	需从 DHCP 服务器获得固定 IP 地址的设备的 MAC 地址
Fixed DHCP Lease IP (DHCP 固定租约 IP)	从 DHCP 服务器获取的固定 IP 地址。请注意这个 IP 地址必须是 DHCP IP 池以外的 IP 地址。

3. 点击 Add 按钮把新的 DHCP 租约项添加进去。

6.1.5.3 删除一个 DHCP 固定租约

删除一个DHCP固定租约, 点击该租约项前面的 按钮即可。

6.1.5.4 查看 DHCP 固定租约表

如想查看 DHCP 固定租约，点击 Advanced–> DHCP Server 菜单，即可打开固定 DHCP Lease 设置页面。

6.2 DNS

6.2.1 关于 DNS

域名系统（Domain Name System，DNS）服务器向用户提供了一种友好的网址输入方式（如 “yahoo.com”），这网址实质上等同于 Internet 路由中的数字 IP 地址。

当 PC 用户在浏览器中输入一个域名，PC 机首先向 DNS 服务器发出一个请求，要求获取等同的 IP 地址。接着 DNS 服务器试着在自己的数据库里查找此域名，若没有找到，将向更高一级的 DNS 服务器提出查找请求。当地址找到以后，服务器将找到的 IP 地址返回给 PC 机，同时把其放在 IP 包中，以便下次查找所用。

6.2.2 分配 DNS 地址

多个 DNS 地址是用来以备某个 DNS 服务器停止或超负荷时可提供代替之用。ISP 一般提供了第一个和第二个 DNS 地址，也有可能会提供更多地址。您的 LAN PC 机从下面其中一种途径获得 DNS 地址:

- 静态: 如果您的 ISP 提供了 DNS 服务器的地址，您只需在 PC 机 IP 设置中填上即可。
- 从 DHCP 服务器中动态获得: 您可以在 RX3042H 的 DHCP 服务器中设置 DNS 地址，允许 DHCP 服务器分配 DNS 地址给 PC 机。请参考第 6.1.3 节 “设置 DHCP 服务器”，了解如何设置 DHCP 服务器。

同样，您可以指定 ISP 的 DNS 服务器的具体地址（在 PC 机上或在 DHCP 服务器的配置页面中），或者您可以指定 RX3042H 的 LAN 端口的地址（如 192.168.1.1）。当您指定

LAN 端口的 IP 地址后，这设备有了 DNS relay 功能，关于这功能下节将详细阐述。

注意: *如果您在 PC 机上或 DHCP 池中指定了具体的 DNS 地址，DNS relay 功能将不会被启用。*

6.2.3 设置 DNS Relay（DNS 转送功能）

当指定局域网内路由器的 LAN 端口 IP 地址为 DNS 地址后，路由器将会自动地具有 DNS relay 功能。也就是说，该设备本身不是 DNS 服务器，它只是把域名查询请求从局域网中的计算机机送到 ISP 的 DNS 服务器，获得反馈数据后，再把这些数据转送给计算机。

当具有 DNS relay 功能时，RX3042H 必须保留 DNS 服务器的 IP 地址。它可从以下两种方式获取地址:

- 从 PPPoE 或动态 IP 连接中获取: 如果 RX3042H 使用 PPPoE（请参考第 5.2.2 节 PPPoE 或第 5.2.3 节 PPPoE Unnumbered）或者动态 IP（请参考第 5.2.4 动态 IP）连接到 ISP，第一个和第二个 DNS 地址可通过 PPPoE 协议获得。选用这种方式，最大的优点是当 ISP 改变他们的 DNS 地址时，您可以不用重新设置 PC 机或 RX3042H 。
- 设置 RX3042H: 如图 5.3，5.4，5.5 和 5.6 所示，您可以在 WAN 设置页面指定 ISP 的 DNS 地址。

请按以下步骤来设置 DNS relay:

1. 如图 6.1 所示，在 DHCP 设置页面的 DNS 服务器的 IP 地址框中输入 LAN IP。
2. 设置 LAN 计算机机使用网络安全路由器上 DHCP 服务器分配的 IP 地址，或者手动地为 LAN 上每一台计算机都输入网络安全路由器的 LAN IP 地址 ，作为它们的 DNS 服务器地址。

注意: *PC 机重启以前，启用 DNS relay 前所分配给 LAN PC 的 DNS 地址将一直有效。只有当计算机的 DNS 地址变成 LAN IP 地址时，DNS*

relay 才会生效。

同理，在 DNS relay 启用以后，您在 DHCP 池或 PC 机上指定了一个 DNS 地址（不同于 LAN IP 地址），接着这个地址将会取替 DNS relay 的地址。

7 路由

您可以使用设置管理界面来设定互联网和局域网之间数据交流的具体路径。本章将阐述基本的路由选择概念，并介绍如何创建静态路由。请注意大多数用户不需要定义静态路由。

7.1 IP 路由简介

对于路由器来说，最大的挑战是：当它接收到欲达到某一特定地点的数据，它应该下一步把数据送到哪个设备上呢？ 当您定义 IP 路由时，您便提供了 RX3042H 做决定的规则。

7.1.1 我需要定义静态路由吗？

大多数用户不需要定义静态路由。在典型的小型家用或公司网络中，已有的路由可以为您的 LAN 计算机和 RX3042H 设立网关，可以为您提供最合适的路由路径。

- 对于局域网中的计算机，默认的网关可以把所有的网络流量引导到 RX3042H 的 LAN 端口上。局域网中的计算机通过默认网关（通过分配或更改 TCP/IP 属性）或设置为连接时动态地从服务器获取信息（具体的设置步骤请查看在快速安装指南的第二部分）
- 对于 RX3042H，默认的网关被定义为把所有的外部流量全引导到 ISP 的路由器上。当 RX3042H 一与网络连接上时，ISP 自动地把默认网关分配给了 RX3042H。（具体的添加默认路由的步骤请查看第 7.3.2 节添加静态路由）

如果您家里设置了两个或更多网络（或子网），如果您有两个或更多的 ISP 服务商，如果您连接着一个远程公司的 LAN，那么您需要定义静态路由。

7.2 启用 RIP（Routing Information Protocol，路由信息协议）的动态路由

RIP 允许在路由器间交换路由信息；因此，路由可以不用人工操作即可自动更新。如图 10.1 所示，您可以在 System Services（系统服务）配置页面中启动 RIP。

RIP 允许在路由器间交换路由信息；因此，路由可以不用人工操作即可自动升级。如图 10.1 所示，您可以在 System Services（系统服务）配置页面中启动 RIP。

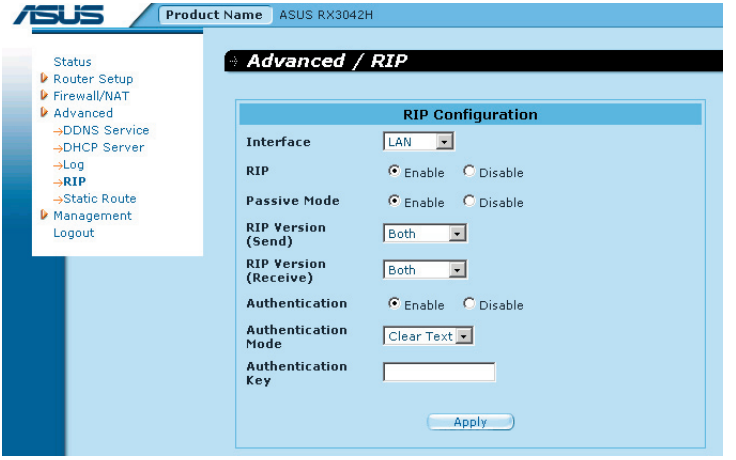


图 7.1. RIP 配置页面

7.2.1 RIP 配置参数

下表列举出了 RIP 的配置参数。

表 7.1. RIP 配置参数

字段	描述
Interface（界面）	选择一个路由信息交换的接口。可选的有 LAN, WAN1, WAN2, PPPoE1, PPPoE2, PPPoE3 以及 PPPoE4。
RIP（路由信息协议）	点击 Enable 或 Disable 按钮来启用或禁用 “RIP” 功能。请注意您必须先启用 Management/System Service 配置页面中的 RIP 服务。

字段	描述
Passive Mode（被动模式）	如果 RIP 设置接口只能接收其他路由器发来的信息不能发送的话，请启用这种模式。如果您希望接口既能接收又能发送信息给其它路由器的话，请禁用这种模式。
RIP Version (Send)（RIP 版本（发送））	选择发送路由信息的 RIP 版本。有三个版本可选：版本 1，版本 2 和两者同时。
RIP Version (Receive)（RIP 版本（接收））	选择接收路由信息的 RIP 版本。有三个版本可选：版本 1，版本 2 和两者同时。
Authentication（鉴定）	点击 Enable 或 Disable 按钮来启用或禁用信息交换的鉴定功能。请注意所有的路由器交换信息时必须使用同样的鉴定密码。
Authentication Mode（鉴定模式）	从下拉列表中选择 RIP 的鉴定模式。支持 Clear Text 和 MD5 两种模式。
Authentication Key（鉴定密码）	输入路由器交换信息时共同使用的鉴定密码。

7.2.2 配置 RIP

请按照以下步骤来启用或禁用 RIP:

1. 在 System Services（系统服务配置）页面中（如图 10.1 所示），点击 Enable 或 Disable 按钮来启用或禁用 RIP 功能。
2. 在下拉列表中选择路由信息交换的接口。
3. 点击 Enable 按钮来为选择接口启用 RIP。
4. 点击 Enable 或 Disable 按钮来决定是否启用被动模式。
5. 选择发送和接收路由信息的 RIP 版本。有三个版本可选：：版本 1，版本 2 和两者均可。

6. 点击 Enable 或 Disable 按钮来决定是否需要启用鉴定功能。
7. 如果鉴定功能启用了的话，您必须选择一种鉴定模式，并填入鉴定密码。（可选）
8. 点击 Apply 来保存这些设置。

7.3 静态路由

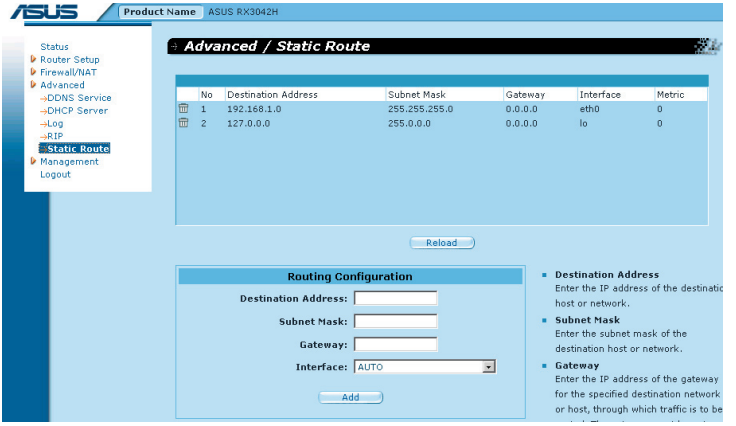


图 7.2. 静态路由配置页面

7.3.1 静态路由配置参数

下表列举出了静态路由配置的配置参数。

表 7.2. 静态路由配置参数

字段	描述
Destination Address（目标地址）	为目标计算机或目标网络指定 IP 地址。同时也能全设置为 0，表示这个路由可以用于所有未被其它路由定义的网络（这个路由创建了默认网关）。请注意目标 IP 必须是网络 ID。默认路由使用 0.0.0.0 作为目标 IP。请参考附录 11 中关于网络 ID 的解释。

字段	描述
Subnet Mask (子网掩码)	指明哪一部分地址是网络地址，哪一部分地址是主机地址。请参考附录 11 中关于子网掩码的解释。默认的路由使用 0.0.0.0 作为子网掩码。
Gateway (网关)	网关 IP 地址
Interface (接口)	可选的选项有 AUTO, Eth0 (LAN), Eth1 (WAN), PPPoE:0 (unnumbered), PPPoE:1 (1st PPPoE session), PPPoE:2 (2nd PPPoE session)。这些选项均可从下拉表中选择。如果选择 AUTO 的话，路由器将自动地分配接口给基于网关 IP 地址的包

7.3.2 添加静态路由

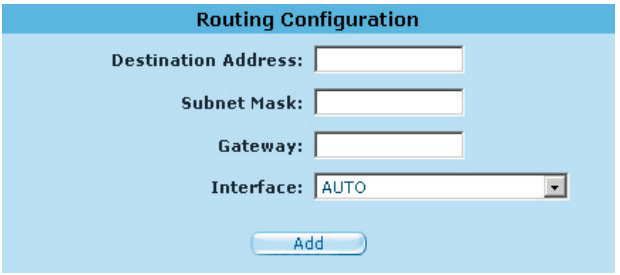


图 7.3. 静态路由配置

请按照以下步骤来为路由表添加一个静态路由:

1. 点击 Advanced -> Static Route 菜单，打开静态路由配置页面。
2. 在相应的框中输入 Destination Address(目标 IP 地址)、Subnet Mask(目标子网掩码)、Gateway(网关)IP 地址以及 Interface(接口) 等静态路由信息。

   详细情况请查看表 7.2. 静态路由配置参数。

   如想创建一个有默认网关的路由，请在目标 IP 地址和子网掩码框中都输入 0.0.0.0。
3. 点击 Add 按钮来添加一个路由。

7.3.3 删除静态路由

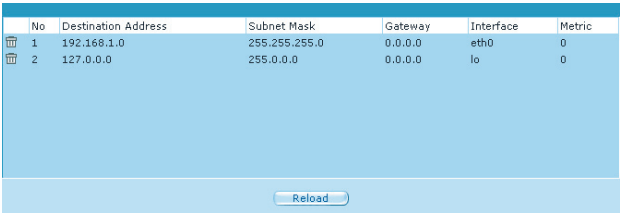


图 7.4. 路由样本

按照以下步骤从路由表中删除一个静态路由:

1. 点击 Advanced -> Static Route 菜单打开静态设置页面。
2. 点击路由项前面的 图标。

警告: *不要删除带有默认网关的路由除非您知道您在做什么。删除默认网关将会导致网络连接断开。*

7.3.4 查看静态路由表

所有支持 IP 的计算机和路由器都有一张供用户使用的 IP 地址表。对于每一个目标 IP 地址，表上都列举出了数据应通过的第一个 IP 地址。这张表通常也称作设备路由表。

如要查看 RX3042H 的路由表，点击 Advanced->Static Route 菜单。如图 7.2 所示，路由表会出现在静态路由设置页面的上方。

路由表会显示出包含目标网络的 IP 地址、子网掩码以及网关的 IP 等的路由信息。

8 配置 DDNS

动态 DDS（Dynamic DNS，DDNS）允许计算机在 IP 地址发生变换时（重启，ISP 的 DHCP 服务器 IP 租约重设时）仍使用同样的域名。无论何时 WAN IP 地址变化，RX3042H 都与 DDNS 服务提供商相连。它支持 Web 服务器以及 FTP 服务器使用域名。同时它也支持 DDNS 客户端具有以下特征:

- 当外部界面出现时，可更新 DNS 记录（额外的）
- 手动 DNS 更新

HTTP DDNS 客户端

HTTP DDNS 客户端使用的是 DDNS 服务提供商提供的动态更新 DNS 记录的服务。这样，服务提供商可以在 DNS 上更新 DNS 的记录。而 RX3042H 则通过 HTTP 来触发这种更新。RX3042H 支持以下服务提供商提高的HTTP DDNS更新服务:

- www.dyndns.org

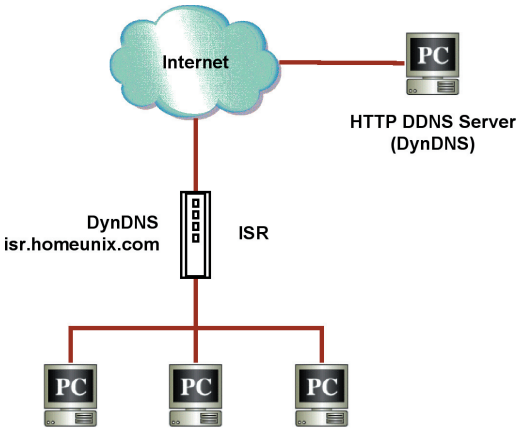


图 8.1. HTTP DDNS 的网络图

当 DDNS 端口的 IP 地址变化时，DDNS 都会将更新发送至制定的 DDNS 服务供应商。对 RX3042H 进行设置时，需要填入 DDNS 服务提供商提供的 DDNS 用户名和密码。

8.1 DDNS 配置参数

表 8.1 列举出了 DDNS 服务的配置参数:

表 8.1. DDNS 配置参数

字段	描述
Interface (界面)	选择 DDNS 服务所使用的接口。
Status (状态)	显示 DDNS 当前状态。
Enable DDNS (启用 DDNS)	选中复选框启用 DDNS 服务，否则反之。
Domain Name (域名)	在框中输入已注册的域名。例如，如果 RX3042H 的主机名是 “host1”，域名是 “yourdomain.com”，那么全域名（fully qualify domain name，FQDN）是 “host1.yourdomain.com”。
Username (用户名)	在框中输入 DDNS 服务提供商提供的用户名。
Password (密码)	在框中输入 DDNS 服务提供商提供的密码。

8.2 配置 HTTP DDNS 客户端

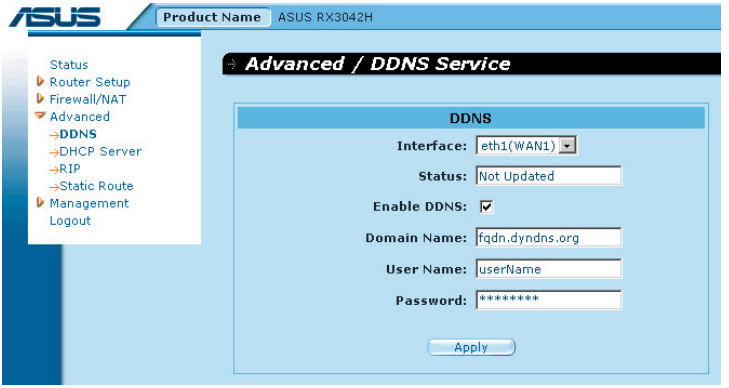


图 8.2. HTTP DDNS 配置页面

请按照以下步骤来配置 HTTP DDNS:

1. 首先，您需要有一个已在 DDNS 服务提供商 dyndns 处注册了的域名。如果没有的话，请访问 www.dyndns.org 查阅详情。
2. 点击 Advanced -> DDNS 菜单，打开 DDNS configuration（DDNS 配置）页面。
3. 选择 DDNS 服务所使用的接口。
4. 选中 Enable DDNS 的复选框来启用 DDNS 服务。
5. 在域名框中输入已注册的域名。
6. 输入 DDNS 服务提供商提供的用户名和密码。
7. 点击 Apply 按钮，将 DNS 更新请求发送至 DDNS 服务提供商。请注意当 WAN 端口状态改变时，DNS 更新请求将会自动地发送给 DDNS 服务提供商。

9 配置防火墙和 NAT

RX3042H 提供了内置的防火墙 /NAT 功能，使系统可以防范服务拒绝（DoS）攻击以及黑客的恶意侵入。您同样可以定义需要进行自动监控的对象。

本章阐述了如何创建 / 更改 / 删除 ACL（Access Control List, 访问控制列表）规则，从而控制进入网络的数据。您将使用防火墙配置页面来实现以下功能:

- 配置防火墙全球的和 DoS 设置
- 创建、修改、删除和查看 ACL 规则

注意: 当定义一个 ACL 规则时，即让 RX3042H 去检查每一个它接收的数据包，确认它是否符合规则的标准。这标准应该包括数据包携带的网络或 internet 协议，它传送的方向（比如说，从 LAN 到 Internet 或反之），发送数据包的计算机的 IP 地址，目标 IP 地址，以及数据包的其它特征。

如果这个数据包符合规则中的所有标准，则该包可以通过（发送至目的主机），否则被拒绝（丢弃）。这完全取决于规则中的定义内容。

9.1 防火墙简介

9.1.1 状态封包检测

RX3042H 中的状态封包检测（SPI）建立了一张状态表，其中记录了所有允许通过防火墙的数据包的连接状态。如果包的连接状态与 SPI 状态表相符的话，防火墙将开放一个通道允许包通过。否则，此包将会被丢弃。当连接终止时，通道也会关闭。SPI 不需要做任何设置；当防火墙启动时，SPI 也会自动启用。请参考第 9.3.1 节 “防火墙选项”，查看如何启用或禁用 RX3042H 的防火墙服务。

9.1.2 DoS（服务拒绝）攻击防护

DoS 攻击防护和状态封包检测都为您的网络提供了第一线的防护措施。两者均不用设置；只要防火墙一启用，您的网络就已在严严的防护之中了。按默认来说，出厂以前防火墙已开始启用。请参考第 9.3.1 节 “防火墙选项”，查看如何启用或禁用 RX3042H 的防火墙服务。

9.1.3 防火墙和访问控制列表

9.1.3.1 ACL 规则优先级

所有的 ACL 规则都分配有一个 ID——ID 越小，优先级越高。防火墙先从数据包中抽取包头信息，然后根据信息是否与 ACL 规则相符来决定是丢弃或通过这个包。请注意 ACL 规则检查会先从最小的 ID 开始，直到有符合的匹配出现，或者所有的 ACL 规则都已经检查完毕。如果没有符合规则的匹配出现，包将会被丢弃；包被丢弃或通过取决于是否有符合 ACL 规则。

9.1.3.2 连接状态追踪

防火墙中的状态封包检测引擎记录下了网络连接的状态、进程等。由于在状态表中存储了每次连接的信息，RX3042H 能很快地决定入站封包是否属于已建立的连接。如果是的话，此包可以不用经过 ACL 规则检查即可通过。

举个例，一个 ACL 规则允许从 192.168.1.1 发送 ICMP 数据包到 192.168.2.1。当 192.168.1.1 发送了一个 ICMP echo 请求（如一个 ping 包）到 192.168.2.1，192.168.2.1 会发送一个 ICMP echo 回复给 192.168.1.1。您不需要在 RX3042H 中再建一个 ACL 规则，因为 状态封包检测引擎已经记下了连接状态，允许 ICMP echo 回复通过防火墙。

9.1.4 默认 ACL 规则

RX3042H 支持两种访问规则:

- ACL 规则：用来控制 LAN 和 DMZ 上所有访问计算机的权限，以及控制 LAN 和 DMZ 上所有访问外部网络的主机的权限。
- Self-Access 规则：用来控制访问 RX3042H 自己的权限。

默认的访问权限

- 所有的从外网主机访问 LAN 和 DMZ 的主机的流量被阻止。
- 所有的从 LAN 来的流量通过使用 NAT 访问外网。

***注意：** 不要把默认的 ACL 规则从 ACL 规则表中删除！ 更好的方法是创建更高优先级的 ACL 规则优先于默认的规则。*

9.2 NAT 简介

网络地址转换允许使用单独的设备，比如说 RX3042H，在 Internet（公共网络）和内部（或私人）网络之间扮演着一个代理的角色。意思是从外部网络来看，一个 NAT IP 地址就能代表整个组的计算机。网络地址转换（NAT）是一种在大型网络之间转换注册 IP 地址的方法，能简化 IP 地址的管理。因为 IP 的转换，NAT 可以隐藏内部网络的真实地址，从而降低了内部网络受攻击的风险，提高了安全性。

支持的 NAT 模式有静态 NAT，动态 NAT，NAPT，反向静态 NAT 以及反向 NAPT。

9.2.1 NAPT（Network Address and Port Translation，网络地址和端口转换）或 PAT（Port Address Translation，端口地址转换）

NAPT 也称为 IP 伪装，它只需要一个有效的 IP 地址就可以让很多电脑连接到 Internet。NAPT 还需要对端口进行转换。IP 包会被转换成全球有效的 Internet 地址，同时，端口则会被转换成内部网中没有使用的端口。图 9.1 显示了内部网中的所有主机通过一个 IP 地址进入 Internet 的情况，也显示了不同端口转换成一个空闲端口的情况。

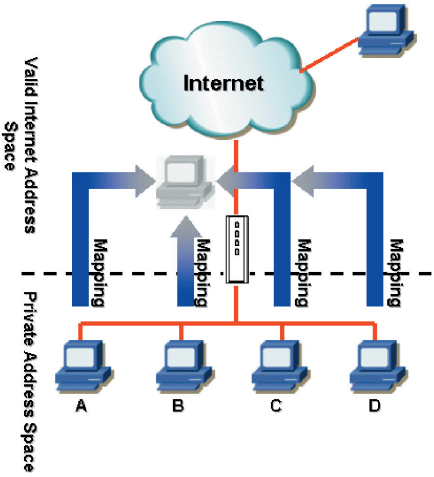


图 9.1 NAPT——内部 PC 机都使用同一 IP 地址

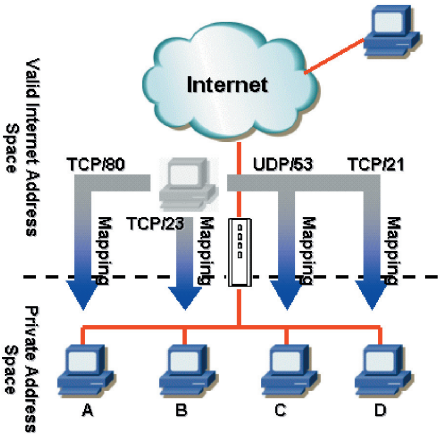


图 9.2 反向 NAPT——将入站封包传送到基于协议、端口号以及 IP 地址的内部主机上

9.2.2 Reverse NAPT（反向 NAPT）/ 虚拟服务器

反向 NAPT 又称作入站映射，端口映射，或虚拟服务器。任何传送到 RX3042H 的封包都会被传送到基于协议、端口号和 / 或在 ACL 规则中指派的 IP 地址的内部主机上。这个功能对于内网中多个主机请求多种服务时十分有用。图 9.2 显示了网页服务器（TCP/80）连在 PC A 上，telnet 服务器（TCP/23）连在 PC B 上，DNS 服务器（UDP/53）连在 PC C 上，以及 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分别传送至各自请求的主机。

9.3 防火墙设置 ——（Firewall/NAT -> Settings）

9.3.1 防火墙选项

表 9.1 列举出了防火墙的选项参数。

表 9.1. 防火墙的选项参数

字段	描述
DoS Check（DoS 检测）	启用或禁用 DoS check 功能。当 DoS check 处于禁用状态时，以下功能也随之禁用: • 状态封包监测 • 跳过所有的 DoS 攻击检查
Default NAT（默认 NAT）	
Log Port Probing（端口检测记录）	如果这项功能启用的话，所有对于禁用端口的尝试连接将会被记入日志中。
Stealth Mode（秘密模式）	启用时，RX3042H 不会对远程连接尝试发送回应。

请按照以下步骤来配置防火墙:

1. 点击 Firewall/NAT-> Settings 菜单，如图 9.3 所示，打开 Firewall Settings（防火墙配置）设置页面。
2. 选中或不选中每一个相对应的选项。

3. 点击 Apply 保存设置。

9.3.2 DoS 设置

RX3042H 有一个专用的防攻击引擎，它能保护内部网络免受服务拒绝（DoS）攻击，如 SYN flooding，IP smurfing，LAND，Ping of Death 以及所有的封包重组类型的攻击。这个设置功能还能丢弃 ICMP 重寄及 IP loose/strict 来源路由封包。例如，RX3042H 的防火墙提供了能防止 “WinNuke” 的安全功能，它是一种广泛应用的程序，被用来远程攻击没有保护的系统。同时，RX3042H 防火墙还提供了多种针对普通 Internet 攻击的保护，如 IP Spoofing，Ping of Death，Land Attack 以及封包重组攻击。请参考表 2.1 中 RX3042H 提供的 DoS 保护完全列表。

9.3.2.1 DoS 防护配置参数

表 9.2 提供了各种 DoS 攻击的详细阐述。您可以选中或不选中复选框来启用或禁用每一项 DoS 攻击的保护功能。

表 9.2. DoS 攻击定义

字段	描述
IP Source Route (IP 源路由)	为了侵入目标系统，侵入者使用 “源路由”。
IP Spoofing (伪 IP)	伪 IP 技术是一种冒充使用别人的 IP 地址发送 TCP/IP 数据包至网络端的技术。伪劣 IP 技术是应用非常广泛的一种技术。
Land	攻击者通过使用同样的源地址及目标 IP 地址，向目标发送数据包，导致目标计算机不断地循环发送和接收该数据包，消耗大量系统资源，从而造成计算机运算速度急剧下降。
Ping of Death (死亡之 ping)	攻击者通过发送大于 64KB 的数据包（超过允许的最大值），造成系统崩溃。

字段	描述
Smurf（Smurf 攻击）	攻击者向广播地址发送一个 ICMP echo 请求。每一个数据包都带有被攻击主机的伪 IP 地址。广播地址将带有伪 IP 的包发送给子网的主机。大多数的主机都会对 ICMP 做出回应，并将回应包发送给被攻击主机，从而造成大量数据涌向被攻击主机，导致网络或主机崩溃。
SYN/ ICMP/ UDP Flooding（SYN/ ICMP/ UDP 洪水）	选中或不选中此选项来启用或禁用记录 SYN/ ICMP/UDP 洪水攻击的功能。这些攻击行为是在极短时间内向目标主机发送大量的 TCP SYN/ ICMP/UDP 数据包。为了防止影响到网络的正常运作，RX3042H 绝不会错过这些数据包。
TCP XMAS/ NULL/ FIN Scan（TCP XMAS/ NULL/ FIN 扫描）	黑客通过发送特定格式的数据包来扫描您的系统，查看是否有可以利用的服务。有时黑客预先扫描为将来攻击作准备，有时则看您系统中是否有漏洞可攻击。 XMAS 扫描: TCP 数据包是由一串 “ 0” 以及 FIN, URG, 和 PUSH 标志组成。 NULL 扫描 TCP 数据包是由一串 “ 0” 组成。 FIN 扫描: 黑客使用 “stealth” 方法扫描目标计算机，想发现他们是否可以不用真正连接系统即可进入目标系统。它会尝试关闭一个不存在的连接，即使这是错的，系统也会根据服务做出不同的回应。
Re-assembly（重组攻击）	在攻击中，攻击者的 IP 地址的第二或第三片段含有复杂的碎片。如果系统不能处理这种情况的话，将会造成系统崩溃。
WinNUKE	选中或不选中此选项来启用或禁用防止 Winnuke 攻击的保护功能－些 Microsoft Windows 操作系统的较老版本易遭受此攻击。如果您的计算机没有升级到最新的版本或补丁，我们建议您最好开启此项功能。

9.3.2.2 设置 DoS

请按照一下步骤来设置 DoS:

1. 点击 Firewall -> Security 菜单，如图 9.3 所示，打开防火墙设置主页面。
2. 选中或不选中相对应的 DoS 保护功能。
3. 点击 Apply 来保存设置。

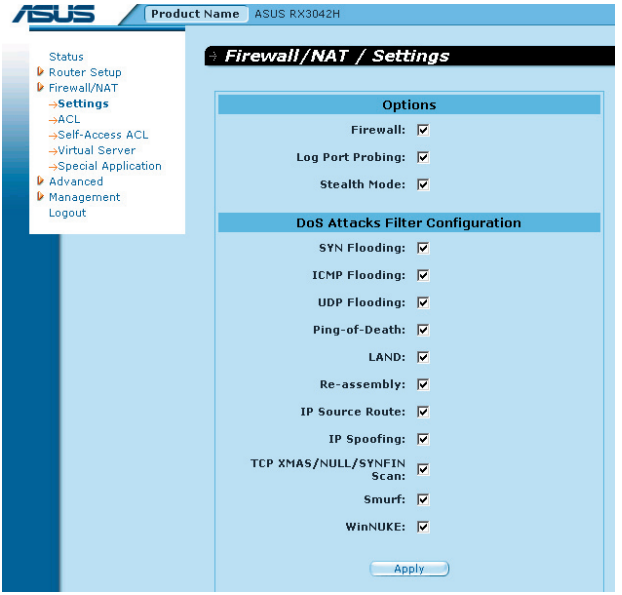


图 9.3. 防火墙设置页面

9.4 ACL 规则配置参数

9.4.1 ACL 规则配置参数

表 9.3 列举出了防火墙进站、出站以及 Self-Access 的 ACL 规则配置参数。

表 9.3. ACL 规则配置参数

字段	描述
交通方向 – 从下拉菜单列表中选择适当的选项来设置 ACL。 配置双 WAN 有两个选项可选: LAN ->WAN 以及 WAN ->LAN。 配置 WAN + DMZ 有六个选项可选: LAN ->WAN, WAN ->LAN, LAN ->DMZ, DMZ->LAN, WAN ->DMZ 以及 DMZ ->WAN。	
ID	
新增	点选此项目以新增一组 ACL 规则
规则编号	从下拉列表中选择一项规则, 并修改其属性
路由 此选项允许您设定本规则的优先级。RX3042H 防火墙根据规则的优先级来决定是否让封包通过。您可以指定规则列表中一特定数字来决定规则的优先级。选项包括: AUTO,eth1 (WAN1), eth2 (WAN2), PPP1 (WAN1-unnumbered), PPP2 (WAN2-unnumbered),PPP3 (WAN1-PPPoE1), PPP4 (WAN1-PPPoE2), PPP5 (WAN2-PPPoE1), PPP6 (WAN2-PPPoE2)。若 WAN 端口设置为 DMZ 模式, 则只有 AUTO, eth1, PPP1/3/4。	
1 (最初)	本数字代表最高优先级
其他数字	选择要指定给其它规则的优先级号码
日志 勾选此复选框即激活 ACL 规则的日志功能, 若要禁用这项功能, 去掉复选框中的勾即可。	
动作	
允许	选择此按钮以设定为允许规则设定 符合规则的封包将被允许通过
拒绝	选择此按钮以设定为拒绝规则设定 符合规则的封包将被阻挡无法通过
路由 • 保持 “自动” 设置, 除非 封包将至特定的接口。 在这儿可以选择 PPPoE unnumbered 或 PPPoE multi-session 需要的路由方式。可选项包括 AUTO, PPP1/2 (PPPoE unnumbered), PPP1/2/3/4 (PPPoE multi-session)。这些选项均可从下拉菜单中选择。如果选择 “自动”, 路由器会根据路由表中的信息为封包进行路由寻址。	

字段	描述
NAT	
无	若您不想在 ACL 规则中使用 NAT，请选择本项目。
IP 地址	若您想外出流量使用源 IP 地址的话，请指定计算机的 IP 地址。请注意此选项已选。
IP 地址	输入 IP 地址
自动	RX3042H 自动地使用流量来源 IP 的 IP 地址。请注意，如果 NAT 用于流出流量的话，请选择此项。
来源网络 此选项可以让您设定套用该规则的来源网络。请在下拉列表中选择下列选项:	
任意	本选项可以让您套用该规则于源网络中的所有计算机，像那些在 Internet 上符合入站规则的计算机，或那些在局域网中符合出站规则的计算机。
IP 地址	本选项可以让您为套用本规则者指定一组 IP 地址。
IP 地址	指定适当的网络地址。
子网	本选项可以让您涵盖在同一 IP 子网内的所有计算机。当此项被选择时，以下字段可以填入:
地址	指定适当的网络地址。
掩码	输入相对应的子网掩码。
MAC 地址	本选项可以让您为套用本规则者指定 MAC 地址。
MAC	输入所需的 MAC 地址。
目标网络 本选项可以让您设定套用该规则的目标网络。请在下拉列表中选择下列选项:	
任意	本选项可以让您套用该规则于源网络中的所有计算机，像那些在 Internet 上符合出站规则的计算机，或那些在局域网中符合入站规则的计算机。
IP 地址，子网	请选择任一选项并输入如前述来源 IP 一节中所提到的相关细节描述。
服务 从下拉列表中选择套用该规则的服务。如果所需服务没有列出，点击 “Edit” 按钮创建一个新的服务。	

字段	描述
时间 选择运用规则的一个时间点。	
启用	如果您想要在特定的时间启动 ACL 规则的话，请选择此项。去掉复选框中的对勾即在任何时间均应用此规则。
日期和时间	检查 ACL 规则所需的时间和日期。

表 9.4. 服务配置参数

字段	描述
服务名 输入一个服务名以区分新的服务。	
协议 从下拉列表中选择一种协议。可选的有 All，TCP，UDP，ICMP，IGMP，AH ESP 以及 TCP/UDP。	
端口 本选项可以让您指定套用该规则的目标端口号。请在下拉列表中选择下列选项:	
任意	若服务要指定一个应用程序，请选择此项。
单一	若服务需要使用制定的端口号，请选择此项
端口号	输入端口号
范围	若服务需要使用某个范围内的端口号，请选择此项。当此项选择以后，接着后面的字段变成可以输入的。
起始端口	输入起始端口范围的第一个端口号
结束端口	输入结束端口范围的最后一个端口号

字段	描述
本选项可以让您选择一种ICMP信息类型。支持的ICMP 信息类型有 • Any (default) • 0: Echo reply • 1: Type 1 • 2: Type 2 • 3: Dst unreach: destination unreachable • 4: Src quench: source quench • 5: Redirect • 6: Type 6 • 7: Type 7 • 8: Echo req: • 9: Router advertisement • 10: Router solicitation • 11: Time exceed: time exceeded • 12: Parameter problem • 13: Timestamp request • 14: Timestamp reply • 15: Info request: information request • 16: Info reply: information reply • 17: Addr mask req: address mask request • 18: Addr mask reply: address mask reply	

9.5 配置 ACL 规则 (Firewall ->ACL)

如图 9.4所示，通过在 ACL 设置页面创建 ACL 规则，您可以将访问控制（允许或拒绝）运用于可信任和不可信任的网络。您可以通过配置页面的选项:

- 添加一个规则，并为它配置参数
- 修改现有的规则
- 删除现有的规则
- 查看已配置的 ACL 规则

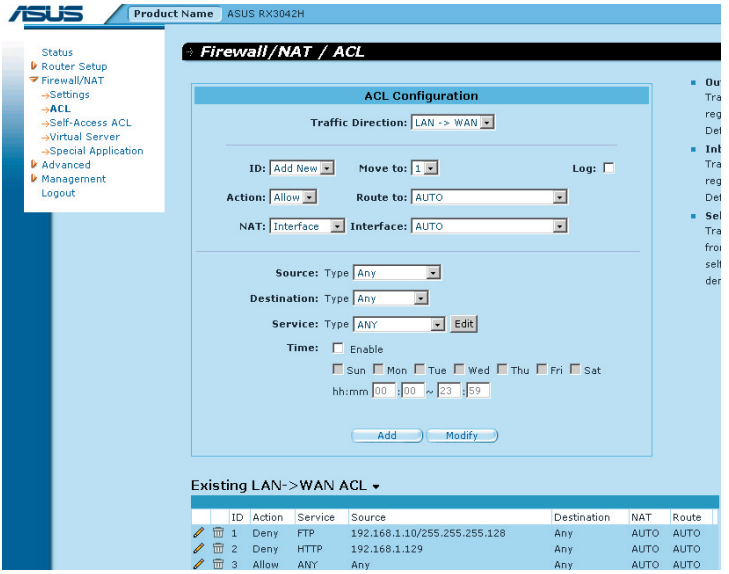


图 9.4. ACL 配置页面

9.5.1 添加 ACL 规则

请按照以下步骤来添加一个 ACL 规则:

1. 点击 Firewall -> ACL 菜单，如图 9.4 所示，打开 ACL 规则配置页面。
2. 从 Traffic Direction 下拉列表中选择一个选项。例如，如果您想要创建一个 ACL 来过滤从 LAN 到 WAN 的流量，请选择 LAN ->WAN 选项。
3. 从 ID 下拉列表中选择 Add New。
4. 从 Action 下拉列表中选择所需的动作（允许或拒绝）。
5. 从 Route To 下拉列表中选择您想要流量流至哪个指定的接口。如果您想要 RX3042H 自动引导流量，请选择 AUTO。
6. 选择 NAT 类型，并输入所对应的信息。
7. 对以下字段作更改 来源 / 目标 IP，来源 / 目标端口，协议，

ICMP 信息类型以及日志。请参考表 9.3 中关于这些字段的详细阐述。

8. 从 Move to 下拉列表中选择数字，为该规则赋于一个优先级。请注意数字 1 表示最高优先级。防火墙会优先检查高优先级规则，再检查低优先级的。

9. 点击 Add 按钮来创建一个新的 ACL 规则。新的 ACL 规则将会显示在 Inbound ACL（入站 ACL）配置页面底部的入站访问控制列表中。

图 9.5 描绘出了如何创建一个起始于 IP 为 192.168.1.129 的主机，拒绝出站 HTTP 流量的规则 。

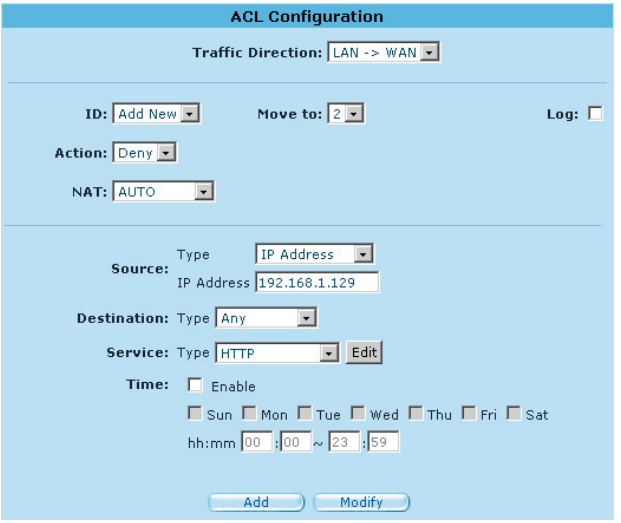


图 9.5. ACL 配置例图

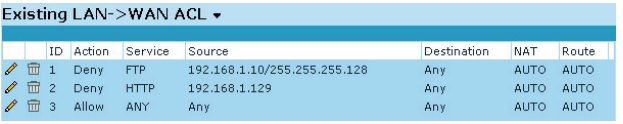


图 9.6. ACL 列表例图

9.5.2 更改 ACL 规则

请按照以下步骤来更改 ACL 规则:

1. 点击 Firewall/ACL -> ACL 菜单, 打开 ACL 规则设置页面。
2. 点击 更改 ACL 表的规则, 或从 ID 下拉列表中选择规则的数字。
3. 根据需要对下列字段做出更改 动作, 来源 / 目标 IP, 服务, 时间, 以及日志。请参考表 9.3 中关于这些字段的详细阐述。
4. 点击 Modify 按钮来更改 ACL 规则。新的 ACL 规则设置将会显示在 ACL 配置页面底部的入站访问控制列表中。

9.5.3 删除 ACL 规则

删除 ACL 规则时, 请点击规则前面的 。

9.5.4 显示 ACL 规则

要查看现有的 ACL 规则, 请点击 Firewall/NAT -> ACL 菜单, 打开 ACL 规则设置页面, 然后从 Traffic Direction 下拉列表中选择流量的方向。

9.6 配置 Self-Access ACL 规则 (Firewall/ NAT -> Self-Access ACL)

Self-Access(自我访问) 规则 控制对 RX3042H 自身的访问。您可以使用 Self-Access Rule configuration 页面, 如图 9.7 所示, 进行以下步骤:

- 添加一个 Self-Access 规则
- 修改现有的 Self-Access 规则
- 删除现有的 Self-Access 规则
- 查看现有的 Self-Access 规则

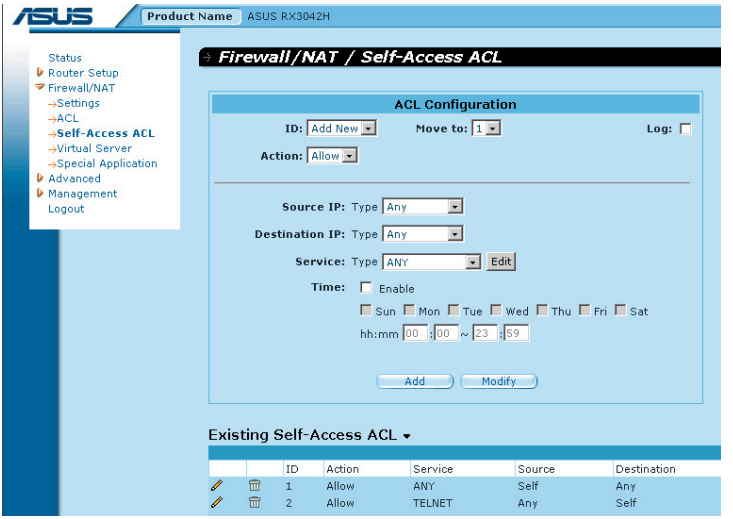


图 9.7. Self-Access ACL 配置页面

9.6.1 添加一个 Self-Access 规则

请按照以下步骤添加一个 Self-Access 规则:

1. 点击 Firewall/NAT ->Self-Access ACL 菜单，打开 Self-Access 规则设置页面。
2. 从 ID 下拉菜单中选择 Add New。
3. 从 Action 下拉列表中选择所需的动作（允许或拒绝）。
4. 从 Move to 下拉列表中选择数字，为该规则赋于一个优先级。请注意数字 1 表示最高优先级。防火墙会优先检查高优先级规则，再检查低优先级的。
5. 根据需要对下列字段做出更改：来源 / 目标 IP 服务，时间，以及日志。请参考表 9.3 中关于这些字段的详细阐述。
6. 点击 Add 按钮来创建一个新的 ACL 规则。新的 ACL 规则将会显示在 Self-Access ACL 设置页面底部的 Self-Access ACL 列表中。

例如:

图 9.8 显示了一个允许任何来源到 RX3042H 的 HTTP 流量的 Self-Access ACL 配置。

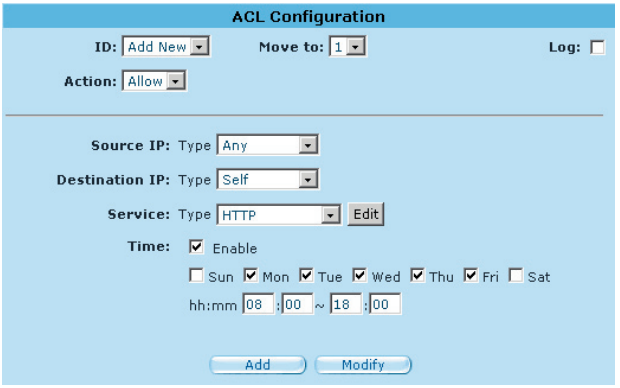


图 9.8. Self-Access ACL 配置举例

9.6.2 修改 Self-Access 规则

请按照以下步骤修改一个 Self-Access 规则:

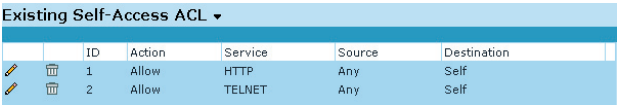
1. 点击 Firewall/NAT -> Self-Access ACL 菜单，打开 Self-Access ACL 规则设置页面。
2. 点击 更改 Existing Self-Access ACL 表的规则，或从 ID 下拉列表中选择规则的数字。
3. 根据需要对下列字段做出更改 动作, 来源 / 目标 IP, 服务, 时间, 以及日志。请参考表 9.3 中关于这些字段的详细阐述。
4. 点击 Modify 按钮来更改 ACL 规则。新的 ACL 规则设置将会显示在 Self-Access ACL 设置页面底部的 Existing Self-Access ACL 列表中。

9.6.3 删除 Self-Access 规则

请点击规则前面的 ，删除 Self-Access 规则。

9.6.4 显示 Self-Access 规则

要查看现有的 Self-Access 规则，请点击 Firewall/NAT -> Self-Access ACL 菜单，打开 Self-Access ACL 规则设置页面。



9.7 配置虚拟服务器

虚拟服务器可以让您设置十个服务器，如 Web，E-mail，FTP 服务器以及其它外部用户可使用的服务器。每一个服务都是由有固定 IP 地址的服务器提供的。对于外部用户来说没，尽管内部服务地址不易看到，但是路由器可以根据服务端口号区分服务请求，然后将请求引导至合适的内部服务器。

注意：RX3042H 一次只能支持一种类型的服务器。

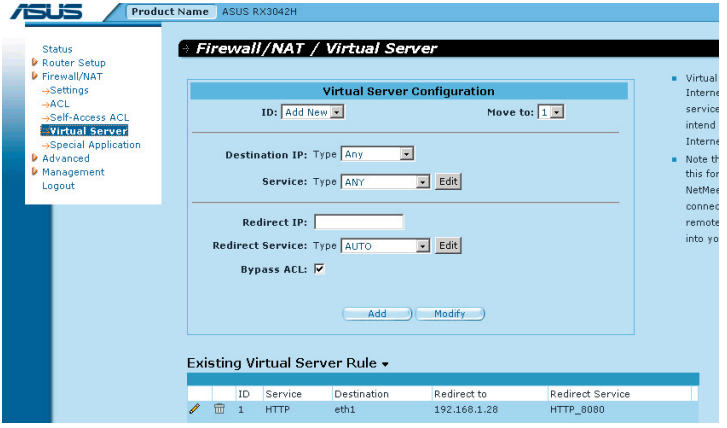


图 9.9. 虚拟服务器配置页面

9.7.1 虚拟服务器配置参数

表 9.5 列举出虚拟服务器配置参数。

表 9.5. 虚拟服务器配置参数

字段	描述
ID	
新增	点击此选项来新增一个虚拟服务器。
数字	从下拉列表中选择虚拟服务器的 ID，更改它的设置。
转移到 此选项允许您设定虚拟服务器规则检查的优先级。NAT 根据规则的优先级来决定是否对 IP 和（或）端口进行检测。您可以指定规则列表中一特定数字来决定规则的优先级。	
1（最初）	本数字代表最高优先级
其它数字	选择要指定给其它规则的优先级号码
目标 IP 此选项可以让您设定套用该规则的来源网络。请在下拉列表中选择下列选项:	
任意	
IP 地址	如果虚拟服务器有已知公共 IP 地址，请输入此 IP 地址。
接口	使用已选择的接口的 IP 地址作为目标 IP 地址。可选的选项有: eth1 (WAN1) eth2 (WAN2) ppp1 (WAN1 unnumbered) ppp2 (WAN2 unnumbered) ppp3 (WAN1 PPPoE 1) ppp4 (WAN1 PPPoE 2) ppp5 (WAN2 PPPoE 1) ppp6 (WAN2 PPPoE 2)
Service	从下拉菜单中选择一个套用此规则的服务。如果没有所需的服务，请点击 “Edit” 按钮来创建一个新的服务。
Redirect IP	输入您希望的目的计算机的 IP 地址（通常是 LAN 中的服务器）。例如，如果 LAN 中的网页服务器的 IP 地址是 192.168.1.28，请输入 192.168.1.28。

字段	描述
Redirect Service	从下拉菜单中选择一个套用此规则的服务。如果没有所需的服务，请点击 Edit 按钮来创建一个新的服务。
Bypass ACL (旁路 ACL)	如果您不希望防火墙控制虚拟服务器的访问权限的话，请选择此选项。意思是虚拟服务器将允许所有用户访问提供的服务。如果您希望能控制谁可以访问服务器的话，请不要选择此项，然后创建一个合适的 ACL 规则来控制访问。

表 9.6. 常用的应用程序的端口号

应用程序	服务端口号
AOE II (Server)	2300-2400
AUTH	113
Baldurs Gate II	2300-2400
Battle Isle	3004-3004
Counter Strike	27005-27015
Cu See Me	7648-7648, 56800, 24032
Diablo II	4000-4000
DNS	UDP 53-53
FTP	TCP 21-21
FTP	TCP 20(ALG)-21
GOPHER	TCP 70-70
HTTP	TCP 80-80
THHP8080	TCP 8080-80880
HTTPS	TCP 443-443
I-phone 5.0	TCP/UDP 22555-22555
ISAKMP	UDP 500-500
mirc	66011-700
MSN Messenger	1863 ALG
Need for Speed 5	9400-9400
Netmeeting Audio	TCPP 1731-1731
Netmeeting Call	TCP 1720-1720
Netmeeting Conference	UDP 495000-49700
Netmeeting File Transfer	TCP 1503--1503
Netmeeting or VoIP	1503-1503, 1720(ALG)
NEWS	TCP 119-119

应用程序	服务端口号
PC Anywhere	TCP 5631
PC Anywhere	TCP 5631, UDP 5632
POP3	TCP 110-110
Powwow Chat	13233-13233
Red Alert II	1234-1237
SMTP	TCP 25-25
Sudden Strike	2300-2400
TELNET	TCP 23-23
Win VNC	UDP 5800-5800

9.7.2 虚拟服务器设置范例 1——网页服务器

图 9.10 描绘了网页服务器的网络拓扑结构图。此服务器使用 8080 端口来提供 HTTP 服务。

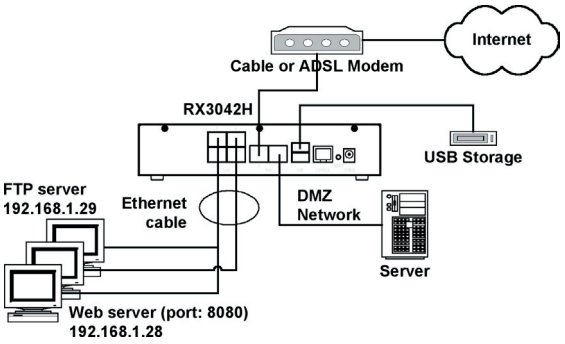


图 9.10. 虚拟服务器部署拓扑图

请按照以下步骤如图 9.10 所示设置网页服务器。

1. 点击 Firewall/NAT->Virtual Server 菜单，如图 9.9 所示，打开虚拟服务器配置页面。
2. 如图 9.11 所示，选择目标 IP 类型及服务类型。

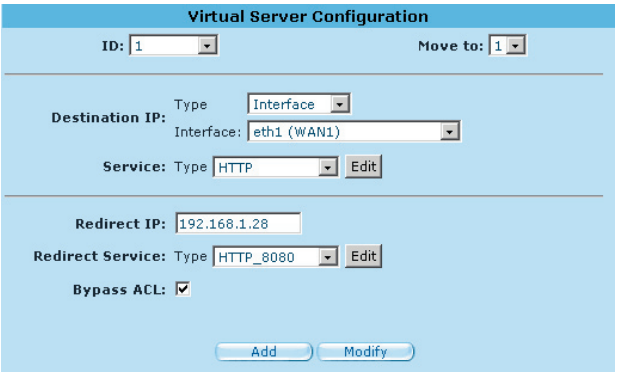


图 9.11. 虚拟服务器设置范例 1 ——网页服务器

3. 把 Redirect IP 框中的 192.168.1.28 作为 IP 地址输入。

4. 因为网页服务器没有使用标准的 TCP 端口（80 端口），所以必须创建一个新的使用 80 端口的 HTTP 服务。点击重定向服务框的 Edit 按钮来创建一个新的服务类型。在弹出的服务配置页面中，如图 9.12 所示输入服务名、协议以及端口号，然后点击 Add to list 创建新的服务名为 HTTP_8080。最后点击 Save & Exit 按钮。

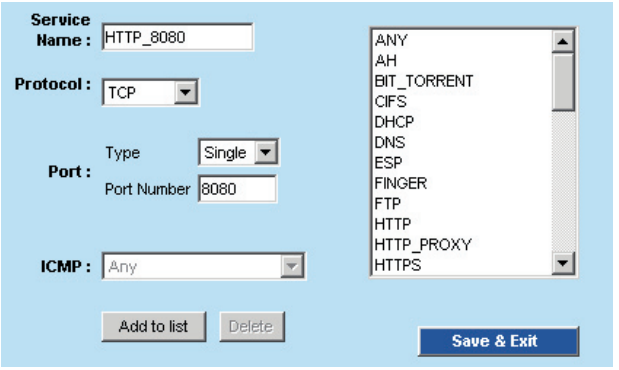


图 9.12. 添加一个新的服务

5. 从重定向下拉列表中选择服务 HTTP_8080。

6. 点击 Add 来保存设置。

9.7.3 虚拟服务器设置范例 2——FTP 服务器

图 9.10 描绘了 FTP 服务器的网络拓扑结构图。FTP 服务器使用标准的 FTP 端口来提供 FTP 服务。

请按照以下步骤如图 9.12 所示设置 FTP 服务器。

1. 点击 Firewall/NAT->Virtual Server 菜单，如图 9.9 所示，打开虚拟服务器配置页面。
2. 如图 9.13 所示，输入所需的信息。
3. 点击 Add 来保存这些设置。

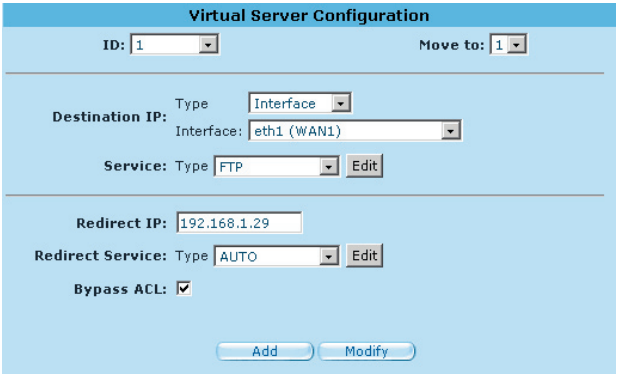


图 9.13. 虚拟服务器设置范例 2 —— FTP 服务器

9.7.4 虚拟服务器设置范例 3 – 具有访问控制功能的 FTP 服务器

本范例与前节 9.7.3 中所述的 “虚拟服务器范例 2——FTP 服务器” 类似，但本范例还另外具备了由防火墙 ACL 规则提供的访问控制功能。在本范例中，我们将 FTP 的访问范围限制在 168.192.128.0 网段中。

以下是如何设立这种 FTP 服务的步骤。

1. 建立一个 FTP 虚拟服务器

a) 点击 Firewall/NAT ->Virtual Server 菜单打开虚拟服务

器设置页面，如图 9.9 所示。

b) 如图 9.13 所示输入信息。

c) 确认 Bypass ACL 复选框未选中。

d) 点 Add 保存虚拟服务器的设置。

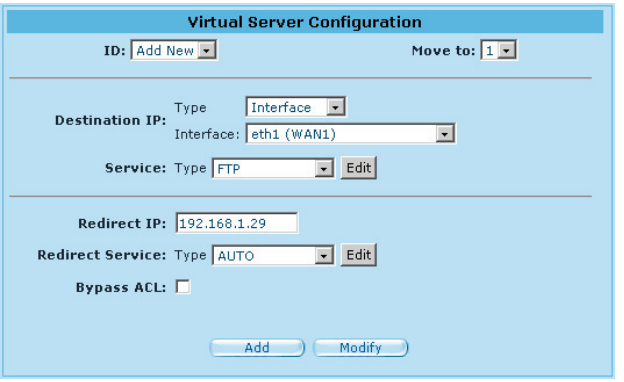


图 9.14. 虚拟服务器范例 3 – FTP 服务器

2. 创建一条控制 FTP 服务器访问范围的 ACL 规则。

a) 点击 Firewall -> ACL 菜单打开 ACL 规则设置页面，如图 9.4 所示。

b) 从 Traffic Direction 下拉菜单中选择 WAN – LAN。

c) 从 ID 下拉菜单中选择 Add New。

d) 从 Action 下拉菜单中选择 Allow。

e) 从 Sourse Type 下拉菜单中选择 Subnet。

f) 在 Sourse Address 和 Mask 框中分别输入 168.192.128.0 和 255.255.255.0。

g) 从 Service Type 下拉菜单中选择 FTP。

h) 在 Move to 下拉菜单中选择数字来设置规则的优先级。请注意图数字 1 表示最高的优先级。防火墙会先检索较高的优先级。

i) 点击 Add 按钮生成新的 ACL 规则。

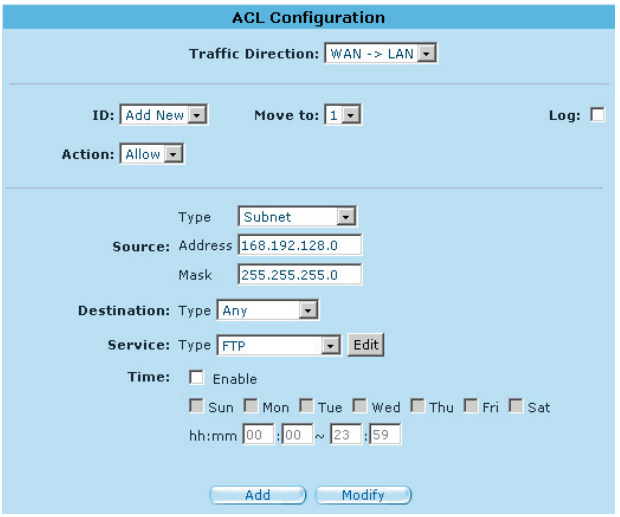


图 9.15. ACL 防火墙虚拟服务器范例 3 – FTP 服务器

9.8 设置特殊应用程序

一些特殊的应用程序使用多个 TCP/UDP 端口来传输数据。由于 NAT 的原因，这些程序不能工作，但通过进行特殊应用程序设置让正常工作。

请注意: *一个计算机一次只能使用一个特殊应用程序。*

9.8.1 特殊应用程序配置参数

表 9.7 列举出了虚拟服务器的配置参数。

表 9.7. 特殊应用程序配置参数

设置	描述
Enabled（启用）	点击此项来启用这项功能
Trigger Protocol（触发协议）	从下拉表中选择协议类型，可选的选项有 TCP, UDP 以及 TCP/UDP。

设置	描述
Outgoing (Trigger) Port (出站（触发）端口)	端口向外发送封包时，出站端口号用作一个触发器。当路由器检测到带有端口号的封包后，它将允许相应的带有入站端口号的入站封包通过路由器。此入站端口号必须在入站端口范围中指定。请参考表 9.8 中流行应用程序的端口号列表。
Incoming Protocol (入站协议)	相应的入站封包使用的协议。可选的选项有: TCP，UDP 以及 TCP/UDP。
Incoming Port (入站端口)	相应的入站封包使用的端口范围。请参考表 9.8 中流行应用程序的端口号列表。请注意端口范围是由一对数字中间加破折号组成，比如 100-200。多个端口范围由逗号隔开，如 100-200，700-800。
Note (备注)	您可以在此输入关于应用程序的描述，比如用于区分的应用程序名。

表 9.8. 常用应用程序的端口号

应用程序	出站端口号	入站端口范围
Battle.net	6112	6112
DialPad	7175	51200, 51201, 51210
ICU II	2019	2000-2038, 2050-2051, 2069, 2085, 3010-3030
MSN Gaming Zone	47624	2300-2400, 28800-29000
PC to Phone	12053	12120, 12122, 150-24220
Quick Time 4	554	6970-6999
wowcall	8000	4000-4020
Yahoo Messenger	5050	5000-5101

9.8.2 特殊应用程序范例

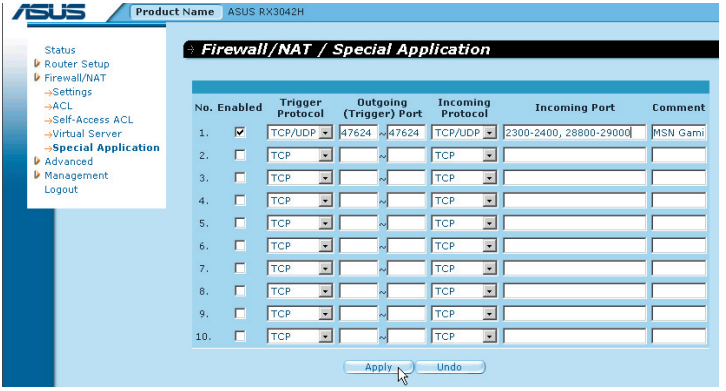


图 9.16. 特殊应用程序配置页面

请按照以下步骤来设置 MSN Gaming Zone 的特殊应用程序。

1. 点击 Firewall/NAT-> Special Application 菜单, 如图 9.14 所示，打开特殊应用程序配置页面。
2. 点击 Enabled。
3. 从触发协议的下拉列表中选择 TCP/UDP。如果您不能确认应用程序是使用 TCP 或 UDP 协议，您可以选择 TCP/UDP。
4. 输入流出端口范围，如：47624 ~ 47624。
5. 从流入协议的下拉列表中选择 TCP/UDP。如果您不能确认应用程序是使用 TCP 或 UDP 协议，您可以选择 TCP/UDP。
6. 输入流入端口范围，如：2300-2400 和 28800-29000。
7. 在备注栏，输入名字 MSN Gaming Zone 以区分程序。
8. 点击 Apply 保存设置。

10 系统管理

本章阐述了您可以利用设置管理器完成以下管理任务:

- 设置系统服务
- 修改密码
- 查看系统信息
- 修改系统日期和时间
- 设置 SNMP
- 恢复系统至出厂设置
- 备份以及恢复系统设置
- 重启系统
- 防火墙升级

10.1 设置系统服务

如图 10.1 所示，您可以通过系统服务配置页面来启用或禁用 RX3042H 支持的服务。除了 DDNS，SNTP，UPnP 以及 RIP，所有服务都在出厂前已被启用。若想作任何更改，请按照以下步骤进行:

1. 点击 Management -> System Service 菜单，打开系统配置页面。
2. 点击相应的 Enable 或 Disable 按钮来启用或禁用相应的服务。
3. 点击 Apply 保存设置。

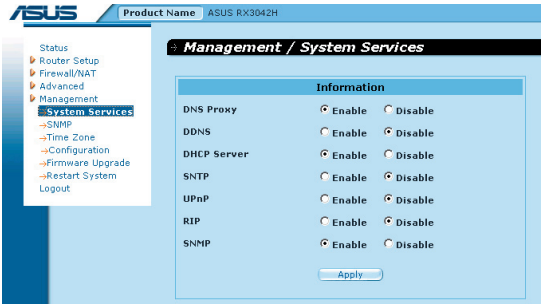


图 10.1. 系统服务配置页面

10.2 登录密码和系统设置

10.2.1 更改密码

当您第一次登录设置管理界面，需使用系统默认的用户名和密码（admin 和 admin）。出于安全原因，您应该更换密码以避免别人更改路由器设置。

注意: *这个用户名和密码仅用于登录设置管理界面，与您连接 ISP 时所用的密码是不同的。*

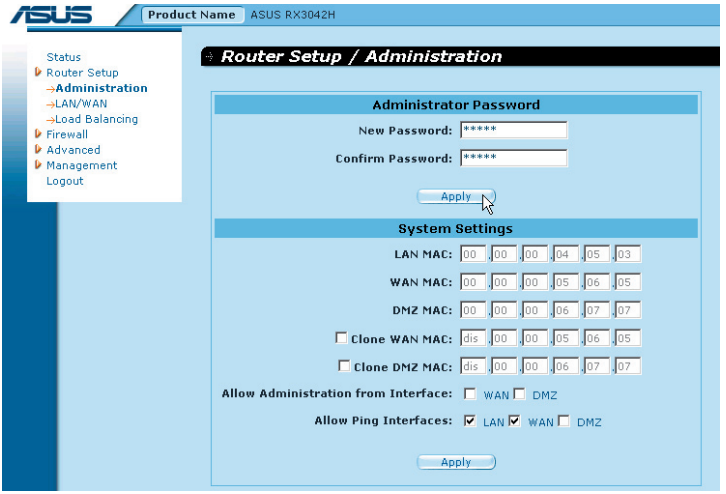


图 10.2. 系统管理配置页面

请按照以下步骤来更改您的密码:

1. 点击 Router Setup -> Administration 菜单，如图 10.2 所示，打开系统管理配置页面。
2. 更换登录密码。

a) 在新的密码文本框中输入新密码，在确认密码文本框中再次输入。密码最长为 16 位。当您再次登录时，请输入您更改后的新密码。

3. 点击 Apply 按钮来保存新密码。

10.2.2 设置系统参数

请按照以下步骤来更改系统设置:

1. 点击 Router Setup -> Administration 菜单，如图 10.2 所示，打开系统管理配置页面。
2. 复制 MAC 地址给 WAN

a) 如果您已经在 ISP 处注册了某一 MAC 地址，请点击 Clone WAN MAC，然后输入已注册的 MAC 地址。

3. 允许 WAN 管理：选中或不选中此选项来启用或禁用通过 WAN 端口的远程管理功能。
4. 允许 Ping 接口：此选项允许用户控制通过 LAN 或 WAN 端口使用 ping 进行路由器访问的权限。分别选中复选框启用 ping 命令。
5. 点击 Apply 保存设置。

10.3 浏览系统信息

您一登录 RX3042H，系统信息页面就会显示出来。同样，您可以点击状态菜单查看系统信息。此页面显示出了所有的系统设置。

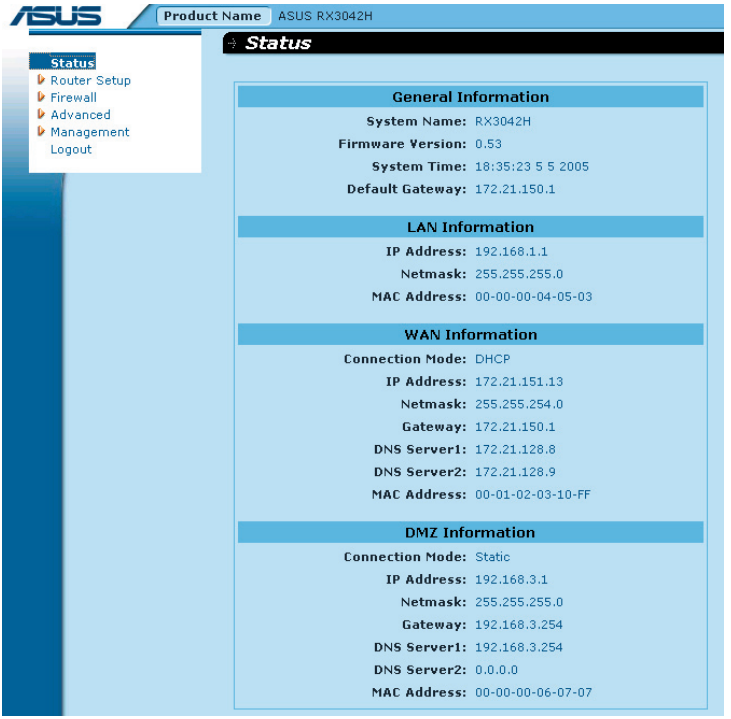


图 10.3. 系统信息页面

10.4 设置日期和时间

RX3042H 保存了当前日期和时间的记录，用于分析和报告数据的变化。尽管在 RX3042H 里有一个时间钟，您也需要设置外部时间服务器来保证正确时间。RX3042H 最多允许您设置三个时间服务器。请点击 Enable 选项来激活 SNTP (Simple Network Time Protocol，简易网络时间协议) 服务。

注意: *改变 RX3042H 上的时间和日期不会影响您 PC 机上的时间和日期。*

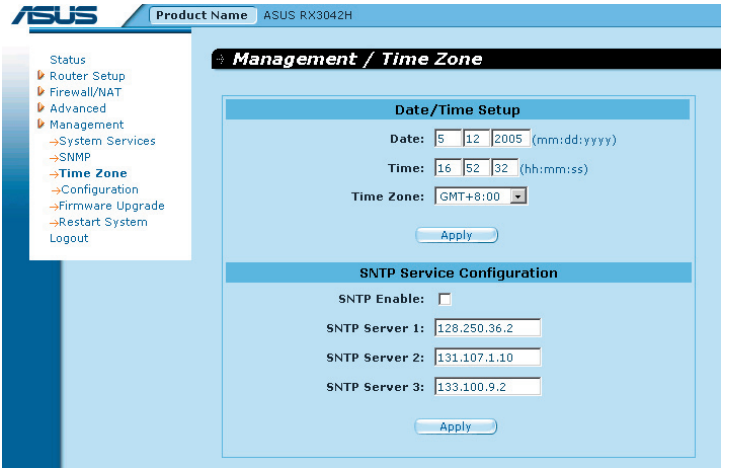


图 10.4. 时区设置页面

请按照以下步骤手动地更改系统时间:

1. 点击 Management -> Zone 菜单打开时区设置页面。
2. 输入当前的时间和日期。
3. 从下拉列表中选择您的时区。
4. 点击 Apply 保存设置。

可按照以下步骤将真正时钟与外部时间服务器设为同步:

1. 点击 Management -> Zone 菜单打开时区设置页面。
2. 从下拉列表中选择您的时区。
3. 点击 Enable 框来激活 SNTP 服务。
4. 输入 SNTP 服务器的 IP 地址来更新系统时间。
5. 点击 Apply 保存设置。

10.4.1 浏览系统日期和时间

若需浏览更新后的系统日期和时间, 先登录设置管理界面, 再点击 Management -> Zone 菜单。

10.5 SNMP 设置

SNMP（Simple Network Management Protocol，简易网络管理协议）是专门设计用于网络管理的。您可以通过 SNMP 配置页面来启用或禁用 SNMP 功能。

10.5.1 SNMP 配置参数

表 10.1 列举出了 SNMP 的配置参数。

表 10.1. SNMP 配置参数

字段	描述
SNMP Enable	选中此项来启用 SNMP 功能；反之亦然。
RO Community Name	Community string 是一串清晰的字符串，用作 SNMP 管理站与 Internet Security Router（网络安全路由器）之间的密码。“只读”（Read Only, RO）community name 是被 SNMP 管理站用来读取 Internet Security Router 的设置。
RW Community Name	Community string 是一串清晰的字符串，用作 SNMP 管理站与 Internet Security Router（网络安全路由器）之间的密码。“读写”（Read and Write, RW）community name 是被 SNMP 管理站用来读取和配置 Internet Security Router 的设置。
Trap Address	Trap message（陷阱信息）是 Internet Security Router 发送给 SNMP 管理站，告诉它路由器上所发生的情况。在此文本框中输入 SNMP 管理器的 IP 地址，用来接收从 Internet Security Router 发来的陷阱信息。

10.5.2 设置 SNMP

1. 点击 Management -> SNMP 菜单，如图 10.5 所示，打开 SNMP 设置页面。

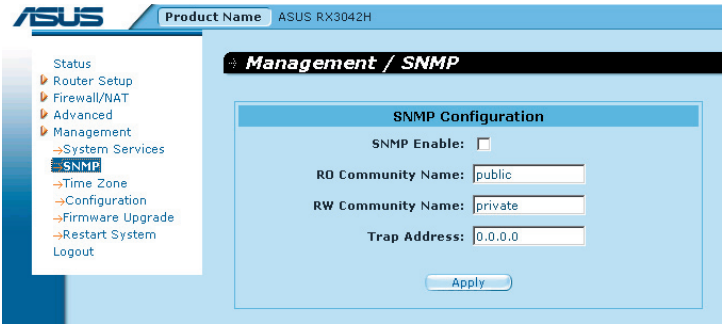


图 10.5. SNMP 配置页面

2. 点击 SNMP Enable 来启用 SNMP 功能；反之亦然。
3. 输入 RO（只读）以及 R/W（读写）。
4. 输入用来接收 RX3042H 发来的 trap 信息的 SNMP 管理站的 IP 地址。
5. 点击 Apply 保存设置。

10.6 日志设置

日志信息存储在动态内存中，当系统重启后，日志会消失。如果要保存日志信息，您需要安装一个系统日志服务器（syslog server），让 RX3042H 向服务器发送日志信息。

10.6.1 使用 Syslog Server 设置远程日志

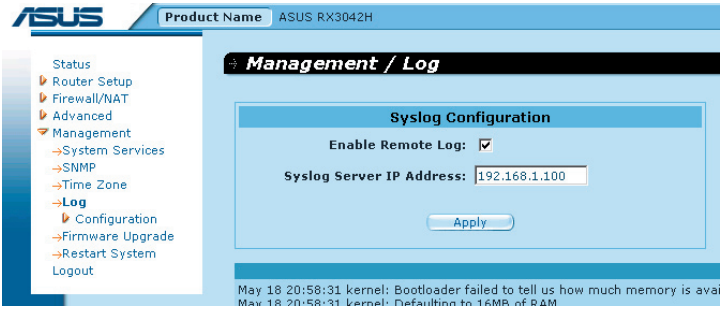


图 10.6. Syslog Server 配置

1. 如图 10.6 所示，点击 Management ->Log 菜单，打开日志配置页面。
2. 点击 Enable Remote Log 复选框来启用远程日志功能。
3. 在 Syslog Server IP Address 框中输入 syslog server 的 IP 地址。
4. 点击 Apply 保存设置。

10.6.2 查看系统日志

您可以点击 Firewall/NAT ->Log **菜单**，打开防火墙日志页面。图 10.7 显示了一个日志样本。您可以点击页面下面的 Reload 按钮查看更新的日志信息。若要清除日志信息，只需点击 Clear Log 按钮。

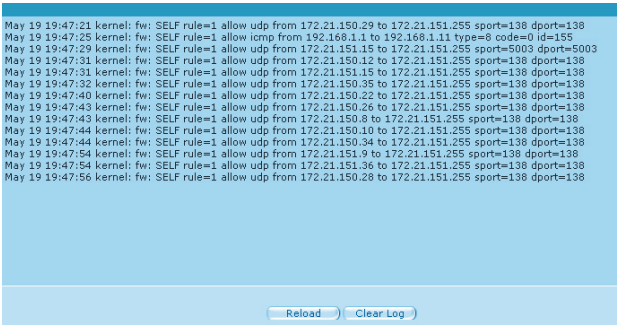


图 10.7 日志范例

10.7 系统设置管理

10.7.1 将系统配置参数恢复至出厂值

有时，由于想解决因不正确设置引起的问题，您想要将系统配置参数恢复至出厂值。请按照以下步骤重新设置系统:

1. 如图 10.8 所示，点击 Management ->Configuration ->Factory Default 菜单打开出厂值设置页面。

图 10.8. 出厂值设置页面

2. 点击 Apply 按钮将系统设置恢复至出厂值。

3. 如图 10.9 将弹出一个对话框，点击 OK 按钮继续，否则，点击 Cancel 按钮中断这次操作。

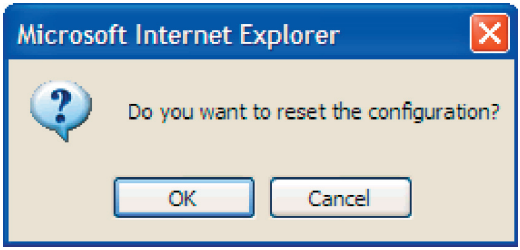


图 10.9. 出厂值设置确认

4. RX3042H 接着将重启使设置生效。请注意，在重启之前，会出现如图 10.10 所示的倒计时提醒您注意。

图 10.10. 出厂值设置倒计时

有时，您会发现您没有访问 RX3042H 的权限，比如 您忘记了自己的密码或 RX3042H 的 IP 地址。如遇这种情况，唯一

的办法就是按重设按钮至少 5 秒钟, 将系统设置恢复至出厂值。RX3042H 重启后， 系统设置就将恢复至出厂值。

10.7.2 系统设置备份

请按照以下步骤来备份系统设置:

1. 点击 Management -> Configuration -> Backup 菜单, 打开系统备份设置页面。
2. 点击 Apply 按钮来备份系统设置。

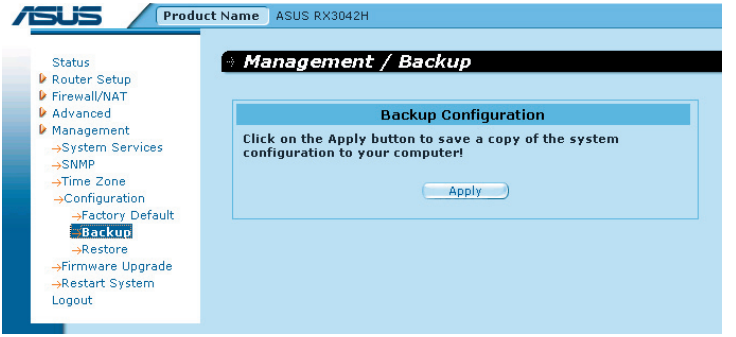
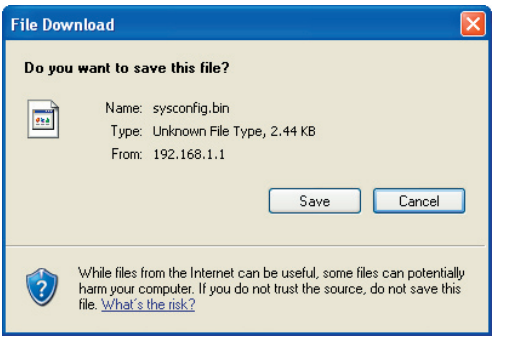
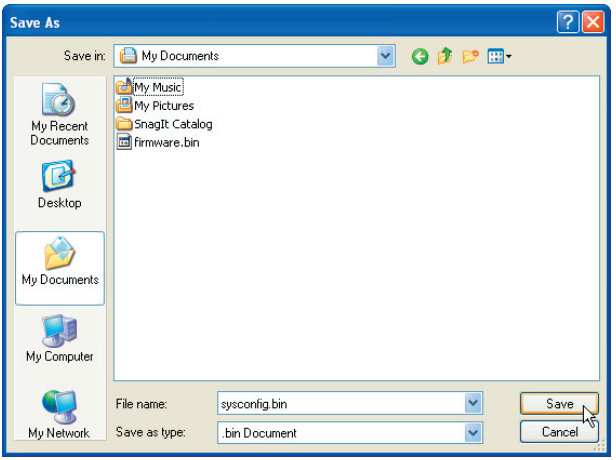


图 10.11. 系统备份设置页面

3. 点击 Save 按钮来备份系统设置。



4. 点击 Save。



10.7.3 恢复系统设置

请按照以下步骤来恢复系统设置:

1. 点击 Management -> Configuration -> Restore 菜单, 打开系统设置恢复页面。

图 10.12. 系统设置恢复页面

2. 在 Configuration File 框中输入您想要恢复的系统设置文件的路径及名字。或者, 您可以点击 Browse 按钮来寻找文件。接着会弹出如图 10.13 的窗口让您选择需要恢复的设置文件。

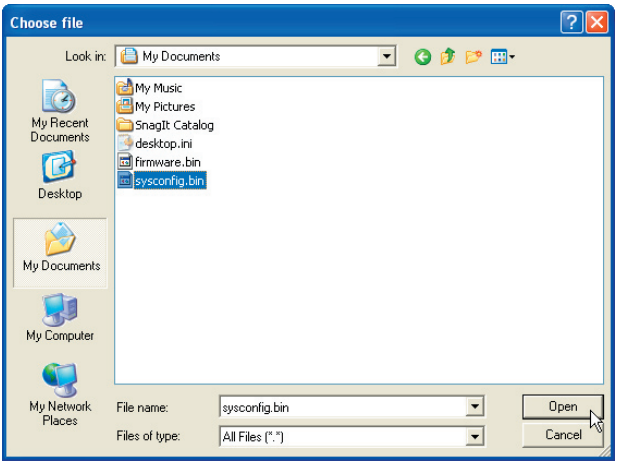


图 10.13. 从文件管理器中选择系统设置文件

3. 点击 Apply 按钮恢复系统设置。接着会弹出如下所示的对话框, 询问您是否确认恢复系统设置。点击 OK 继续, 反之, 点击 Cancel 中断此次操作。请注意, RX3042H 重启以后, 设置才能生效。

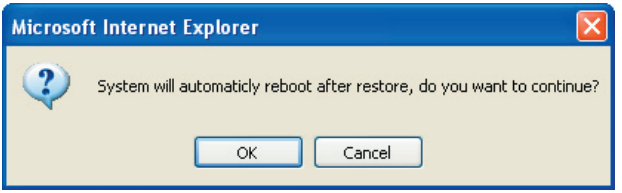


图 10.14. 系统设置恢复页面

4. 如图 10.15, 系统重启倒计时钟将会出现。当倒计时为零时, 您将重新连接 RX3042H 。如果您不希望自动连接的话, 当然您可以手动进行连接。

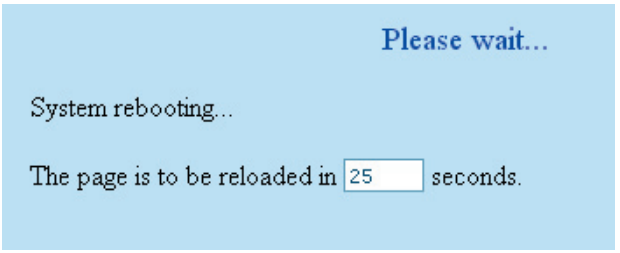


图 10.15. 系统重启倒计时

10.8 固件升级

ASUSTeK 常提供 RX3042H 上固件的升级包。所有的系统软件都放在一个称作 image 的文件内。通过设置管理界面，您可以非常轻易地进行固件升级。请按照以下步骤进行升级:

1. 点击 System ->Fireware Upgrade 菜单, 如图 10.16 所示, 打开固件升级页面。

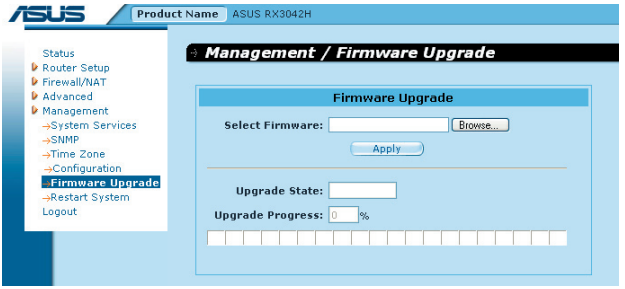


图 10.16. 固件升级页面

2. 在选择固件文字框中，输入固件文件的路径及文件名。或者，您可以点击 Browse 按钮来寻找文件。接着会弹出如图 10.17 的窗口让您选择所需的固件文件。

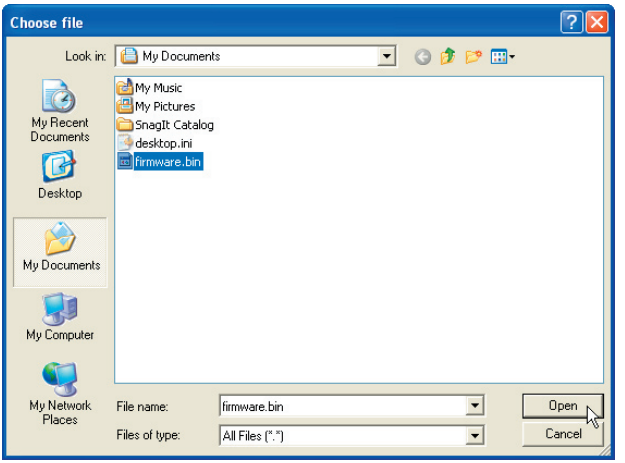


图 10.17. 从文件管理器中选择固件文件

3. 点击 Apply 按钮升级固件。接着将会弹出如下图所示的对话框，询问是否确定升级系统。点击 OK 按钮继续，否则，点击 Cancle 中断此次操作。

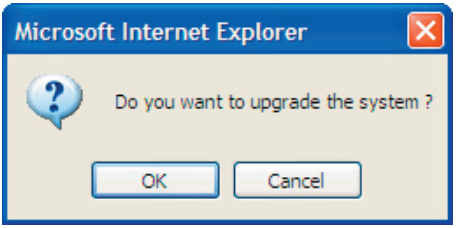


图 10.18. 固件升级确定

4. 固件升级状态及过程如下图 10.19 所示。

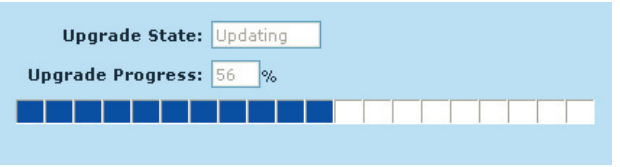


图 10.19. 固件升级过程

5. 如图 10.20, 固件升级完成后，系统重启倒计时时钟将会出现。当倒计时为零时，您将重新连接 RX3042H 。如果您不希望自动连接的话，当然您可以手动进行连接。

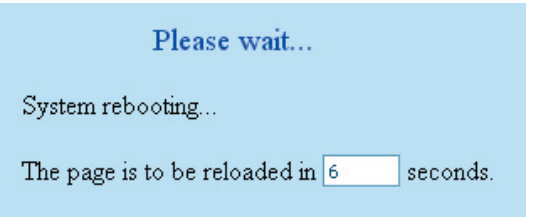


图 10.20. 固件升级的系统重启倒计时

6. 当您重新连接到 RX3042H 后，点击 Status 菜单检查固件是否正确更新。请注意，您需要先清除浏览器中的缓存，然后再查看系统信息页面。请按照以下步骤来清除 Microsoft Internet Explorer 的缓存:

   a) 点击 **工具**菜单。

   b) 点击 Internet **选项** ... 菜单。

   c) 点击 **删除文件** ... 按钮，清除浏览器中的缓存。

10.9 重启系统

1. 点击 Management –> Restart System 菜单，如图 10.21 所示，打开重启系统页面。
2. 点击 Apply 按钮来重启系统。

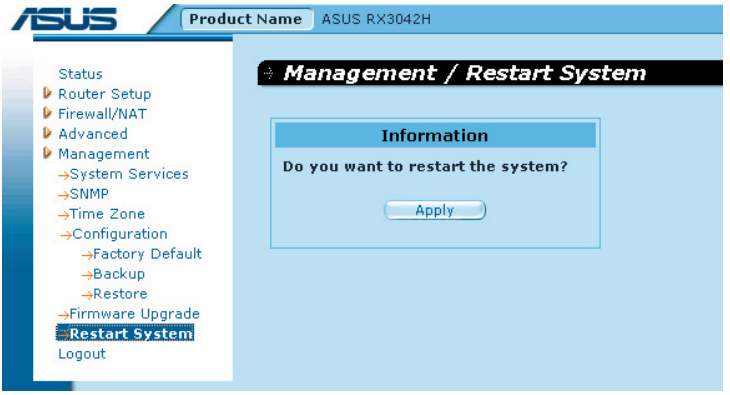


图 10.21. 重启系统页面

10.10 退出设置管理界面

如果要退出设置管理界面，点击退出菜单，然后点击 Apply 按钮打开退出页面。如果您使用的是 IE 浏览器，将弹出如图 10.22 所示的窗口，提醒您是否确认要退出。

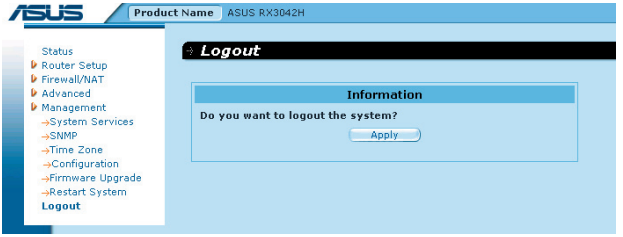


图 10.22. 登出设置管理页面

图 10.23. 确认关闭浏览器 (IE)

11 IP 地址，子网掩码及子网

11.1 IP 地址

注意：本章只适合 IPv4 IP 地址（Internet 协议第 4 版）。IPv6 地址不适用。

在本章中，我们假定您已经掌握了一些基本知识，如二进制数、位（bits）、字节（bytes）。欲知更多细节，请参考附录 11。

IP 地址，类似于 Internet 的电话号码，被用来确定网络上的个人节点（计算机或其它设备）。每个 IP 地址斗殴包括四组数字，每组都是从 0 到底 255，由点（句点）分开，例如 20.56.0.211。这些数字按照从左到右依次被称为 field1，field2，field3 及 field4。

这种用点分开十进制的数字的 IP 地址书写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二一十一”。

11.1.1 IP 地址结构

IP 地址和电话号码相类似，是分等级式设计。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。

同样，IP 地址也包含了两类信息:

- Network ID（网络 ID）

  确定了 Internet 或 Intranet 中的一片特定网络

- Host ID（主机 ID）

  确定了网络中的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网络 ID，其余部分包括了主机 ID。网络 ID 的长度取决于网络等级（请参看下面部分）。表 11.1 说明了 IP 的结构。

表 11.1. IP 地址结构

	Field 1	Field 2	Field 3	Field 4
等级 A	网络 ID	主机 ID		
等级 B	网络 ID		主机 ID	
等级 C	网络 ID			主机 ID

举一些 IP 地址的例子:

等级 A: 10.30.6.125 (网络 = 10, 主机 = 30.6.125)

等级 B: 129.88.16.49 (网络 = 129.88, 主机 = 16.49)

等级 C: 192.60.201.11 (网络 = 192.60.201, 主机 = 11)

11.2 网络等级

常用的三个网络等级是 A，B 和 C。(还有一个等级 D，但是它用途特殊，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 Internet 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 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 Internet 上的局域网络 LAN 通常是等级 C 网络。

下面是一些关于 IP 地址的重要注意事项 :

透过 field1 我们可以很容易地判断网络的等级:

field1 = 1−126: 等级 A

field1 = 128–191: 等级 B

field1 = 192–223: 等级 C

(若 field1 的值没有显示出来 , 则表明被保留以作特定用途)

- 除了所有 field 的值设为 0 或所有的 field 均设为 255 之外 , 主机 ID 能设置成任意值，因为这些值被保留以作特定用途。

11.3 子网掩码

定义: 掩码: 掩码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 地址的哪个部分是网络 ID 以及哪个部分是主机 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 是透过从地址的主机 ID 部分 “借用” 一个或多个 bit 而创建的。子网掩码识别这些主机 ID 的 bit。

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

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 都是网络 ID 的一部分 , 但是请注意 , 掩码是如何指定 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 , 掩码为 :

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。每个子网为主机 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网络 ID bit, 因此就没有子网络。这样的掩码被成为预设的子网掩码。这些掩码为 :

等级 A: 255.0.0.0

等级 B: 255.255.0.0

等级 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。

12 问题排除

本附录为您在安装或使用 RX3042H 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
LEDs	
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 RX3042H 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是否已经安全地连接到了您 ADSL 或 cable modem 的以太网端口和 RX3042H 的广域网端口上面。请确认您的 ADSL 或 cable modem 的电源是开启的。请等待 30 秒的时间，以保证 RX3042H 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 RX3042H 上。请确认 PC 和 / 或集线器已经开启。 请检查您的缆线足够满足您的网络需求。100 Mbit/ 秒的网络 (100BaseTx) 应该使用五类线的缆线。10Mbit/ 秒的网络可以使用品质稍低的缆线。
访问互联网	
PC 无法访问互联网	使用下面即将讨论到的 ping 工具，以检查您的 PC 是否能够与 RX3042H 的 LAN 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有 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 " 第二部分中关于检查 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。

问题	解决方法
PC 无法访问互联网（续）	• 与您的 ISP 联系确认指定给 PC 的 DNS 服务器 是有效的。请改正此地址或将 PC 设定成自动接收信息。 • 请检查网络地址转换 (NAT) 规则是否已经在您的 RX3042H 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 设置您的计算机）。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。
PC 无法显示 Internet 的网页	请检查 PC 指定的 DNS 服务器是正确的，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 ISP 的 DNS 服务器的连通性。
设置管理界面	
您忘记／遗失了您的设置管理界面用户 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。否则，您必须按照第 10.6.1 节 “将系统配置参数恢复至出厂值” 所指来将您的设备重新设定成预设值。 请注意：重新设定将导致原有设定被删除，且所有的设定均恢复至默认值。
从浏览器无法访问设置管理界面	使用下面即将讨论到的 ping 工具，以检查您的 PC 是否能够与 RX3042H 的 LAN 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 Internet Explorer 6.0 或更高版本。同样必须支持 Javascript® 以及 Java®。 请检查 PC 的 IP 地址与指定给路由器局域网络端口的 IP 地址位于相同的子网下。
对设置管理界面的更改没有保存下来	请确认点选了 “**应用**” 按钮以保存更改。

12.1 使用 IP 工具诊断问题

12.1.1 ping

Ping 是用来检查您的 PC 是否能够辨认出您网络或互联网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，您必须知道对方计算机的 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**运行**。在提示符输入下列内容：

ping 192.168.1.1

点选 “确定”。您可用 Internet 站点名称取代任何局域网内的私人 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 12.1 所示。

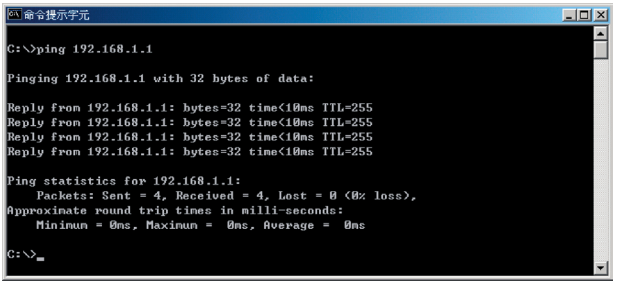


图 12.1. 使用 ping 工具

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

使用 ping 命令，您可以测试到达 RX3042H 的路径是否起作用 (使用预先设定好的 LAN 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) 测试是否能连入 Internet。如果您不知道某个特定的 Internet 位置的 IP 地址，您可使用 nslookup 命令，

详情请参看下面章节。

对于大多数启用 IP 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。

12.1.2 nslookup

您可使用 nslookup 命令来决定与 Internet 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 ISP 上）上查询此名称。如果那个名称并不存在您 ISP 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**运行**。在文字框输入下列内容：nslookup

点选**确定**。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 Internet 地址名称，例如 www.absnews.com。

此窗口将显示相关联的 IP 地址，如图 12.2 所示。

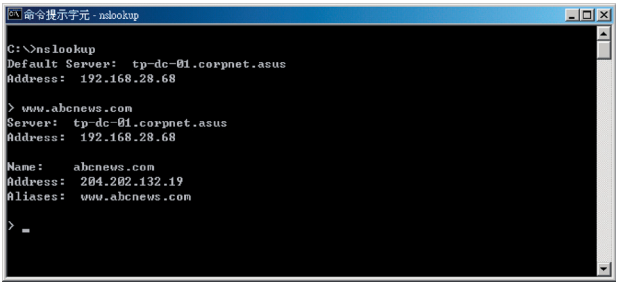


图 12.2. 使用 nslookup 工具

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。