



SL1200

Internet 安全路由器

用户手册

C2923/2007 年 1 月

版权信息

C2923

第一版

2007年1月

版权所有·不得翻印 © 2006华硕电脑

在未获得华硕电脑公司（以下称华硕）书面许可的情况下，本手册中的任何部分，包括所述产品和软件，均不得通过任何手段以任何形式进行复制，转换格式，转译，翻译以及保存于公共资源系统中。本手册仅作为用户购货时附带的说明文档。

若出现以下情况，恕不再提供产品的质保或服务：(1) 产品已由未经华硕书面授权与维修商进行维修，改装；或 (2) 产品序列号无法辨识或已丢失。

华硕提供本手册不代表华硕作出任何隐含或直接的保证，这些保证包括但不限于隐含的质保承诺，产品的畅销性，或针对某种需求的必然适应性。在任何情况下，华硕电脑公司，其领导层，其各级官员和职员，以及其代理商对于本产品造成的任何间接的、特殊的、意外的或后续的损害（包括利润损失、业务损失、数据丢失、业务中断等类似损失）均不承担责任，即使华硕已经事先接到通知提醒，本产品或手册中的错误或缺陷可能导致上述损失。

本手册中的规格和信息仅供参考，并以华硕最新修订版本为准，并且华硕无需对本手册内容的修改进行通知。华硕对本手册中任何错误或不精确的数据均不承担责任，其中包括产品以及所述软件。

本手册中出现的产品和公司名可能是其各自公司的注册商标或版权，华硕在手册中的引用仅作为方便用户进行识别或解释的一种手段，并非对相关公司的侵权行为。

华捷联合信息（上海）有限公司（莘庄）

电话：021-54421616
传真：021-54420066/88/99
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
传真：020-85572352/55
地址：广州市中山大道西高新技术工业园建工路 12 号 1-2 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
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 号
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：北京市海淀区海淀路 52 号太平洋科技大厦 12 层
邮编：100080

华硕技术支持:

免费咨询电话：800-8206655

技术咨询服务：<http://www.asus.com.cn/email>

目录

第一章 简介.....	1
1.1 特色.....	1
1.2 系统需求.....	1
1.3 关于本用户手册.....	2
1.1.1 注意事项.....	2
1.1.2 印刷提示.....	2
1.1.3 提示符号.....	2
第二章 认识华硕 SL1200.....	3
2.1 包装内容.....	3
2.2 前面板.....	3
2.3 后面板.....	3
2.4 主要功能.....	5
2.4.1 防火墙功能.....	5
2.4.2 VPN.....	9
第三章 快速安装指南.....	10
3.1 第一部分 — 连接硬件.....	10
3.1.1 连接 ADSL 或 cable modem.....	10
3.1.2 连接电脑或局域网.....	10
3.1.3 连接电源适配器.....	11
3.1.4 开启华硕 SL1200 的电源.....	11
3.2 第二部分 — 设置您的电脑.....	12
3.2.1 在您开始的前.....	12
3.2.2 Windows® XP PC.....	13
3.2.3 Windows® 2000 PC.....	13
3.2.4 Windows® 95, 98 与 ME PC.....	14
3.2.5 Windows® NT 4.0 工作站.....	15
3.2.6 为您的电脑分配 IP 地址.....	15
3.3 第三部分 — 华硕 SL1200 的快速设置.....	16
3.3.1 设置向导 (Setup Wizard) 中使用的按钮.....	16
3.3.2 设置华硕 SL1200.....	17
3.3.3 测试您的设置.....	23
3.3.4 路由器的默认设置.....	23

第四章 使用设置管理界面	25
4.1 登录设置管理界面.....	25
4.2 设置页结构.....	27
4.2.1 菜单导航.....	27
4.2.2 常用的按钮与图标.....	28
4.3 设置管理界面主页.....	29
4.4 系统设置概观.....	29
第五章 局域网 (LAN) 设置	30
5.1 局域网的 IP 地址.....	30
5.1.1 局域网 IP 设置参数.....	31
5.1.2 设置局域网 IP 地址.....	31
5.2 动态主机控制协议 (DHCP).....	32
5.2.1 何谓 DHCP 服务器?.....	32
5.2.2 为何要使用 DHCP 服务器?.....	33
5.2.3 设置 DHCP 服务器.....	33
5.2.4 查看目前分配的 DHCP 地址.....	35
5.3 DNS.....	36
5.3.1 关于 DNS.....	36
5.3.2 分配 DNS 地址.....	36
5.3.3 设置 DNS 中继 (Relay).....	37
5.4 查看局域网统计值.....	38
第六章 广域网 (WAN) 设置	39
6.1 WAN 连接模式.....	39
6.2 PPPoE.....	40
6.2.1 WAN PPPoE 设置参数.....	40
6.2.2 WAN PPPoE 设置.....	41
6.3 动态 IP.....	42
6.3.1 WAN 动态 IP 设置参数.....	42
6.3.2 设置 WAN 动态 IP.....	42
6.4 静态 IP.....	43
6.4.1 WAN 静态 IP 设置参数.....	43
6.4.2 设置 WAN 静态 IP.....	44
6.5 查看 WAN 统计值.....	45

第七章 设置路由器	46
7.1 IP 路由概述.....	46
7.1.1 我需要定义静态路由吗？.....	46
7.2 RIP 动态路由.....	47
7.2.1 动态路由 (RIP) 设置参数.....	47
7.2.2 设置 RIP.....	48
7.3 静态路由.....	49
7.3.1 静态路由设置参数.....	49
7.3.2 新增一个静态路由.....	50
7.3.3 删除一个静态路由.....	50
7.3.4 查看路由表.....	51
第八章 设置 DDNS	52
8.1 DDNS 设置参数.....	54
8.2 访问 DDNS 设置页面.....	54
8.3 设置 HTTP DDNS 客户端.....	55
第九章 防火墙 /NAT 设置	56
9.1 防火墙概述.....	56
9.1.1 状态封包检测.....	56
9.1.2 DoS 攻击防范.....	57
9.1.3 防火墙与访问控制列表 (ACL).....	57
9.1.4 默认的 ACL 规则.....	57
9.2 NAT 概述.....	58
9.2.1 静态 (一对一) NAT.....	58
9.2.2 动态 NAT.....	60
9.2.3 NAT(Network Address and Port Translation) 或 PAT(Port Address Translation).....	61
9.2.4 反向静态 NAT.....	62
9.2.5 反向 NAT / 虚拟服务器.....	62
9.3 设置传入 ACL 规则.....	62
9.3.1 传入 ACL 规则设置参数.....	63
9.3.2 访问传入 ACL 规则设置页面 - (Firewall -> Inbound ACL).....	67
9.3.3 新增传入 ACL 规则.....	67
9.3.4 修改传入 ACL 规则.....	68
9.3.5 删除传入 ACL 规则.....	68

9.3.6 显示传入 ACL 规则	68
9.4 设置传出 ACL 规则	69
9.4.1 传出 ACL 规则设置参数	70
9.4.2 访问传出 ACL 规则设置页面 - (Firewall -> Outbound ACL)	73
9.4.3 新增传出 ACL 规则	73
9.4.4 修改传出 ACL 规则	74
9.4.5 删除传出 ACL 规则	74
9.4.6 显示传出 ACL 规则	75
9.5 设置 URL 过滤	75
9.5.1 URL 过滤设置参数	75
9.5.2 访问 URL 过滤设置页面 - (Firewall -> URL Filter) ..	76
9.5.3 新增 URL 过滤规则	76
9.5.4 修改 URL 过滤规则	77
9.5.5 删除 URL 过滤规则	77
9.5.6 查看已设置的 URI 过滤规则	77
9.5.7 URL 过滤规则范例	77
9.6 设置高级防火墙功能 - (Firewall -> Advanced)	78
9.6.1 设置自我访问 (Self Access) 规则	79
9.6.2 服务列表设置	81
9.6.3 DoS 设置	84
9.7 防火墙策略列表 - (Firewall -> Policy List)	88
9.7.1 设置 IP 地址池	88
9.7.2 设置 NAT 地址池	92
9.7.3 设置时间范围 (Time Range)	96
9.8 防火墙统计 - Firewall -> Statistics	100
第十章 设置 VPN	103
10.1 默认参数	101
10.2 VPN 隧道 (Tunnel) 设置参数	105
10.3 用自动密钥建立 VPN 连接	109
10.3.1 用预共享密钥 (Pre-shared key) 为 VPN 连接新增规 则	109
10.3.2 修改 VPN 规则	111
10.3.3 删除 VPN 规则	111
10.3.4 查看 VPN 规则	111
10.4 VPN 统计值	112

10.5 VPN 连接范例.....	114
10.5.1 内部网络 - 防火墙 + VPN，无需 NAT.....	114
10.5.2 外部网络 - 防火墙 + 静态 NAT + VPN.....	120
第十一章 系统管理.....	128
11.1 设置系统服务.....	128
11.2 更改登录密码.....	129
11.3 修改系统信息.....	130
11.4 设置日期与时间.....	131
11.4.1 查看系统日期与时间.....	131
11.5 SNMP 设置.....	132
11.5.1 SNMP 设置参数.....	132
11.5.2 设置 SNMP.....	132
11.6 系统设置管理.....	133
11.6.1 复位系统设置.....	133
11.6.2 备份系统设置.....	134
11.6.3 恢复系统设置.....	135
11.7 固件升级.....	136
11.8 复位 SL1200 路由器.....	137
11.9 登出设置管理界面.....	138
第十二章 ALG 设置.....	139
第十三章 IP 地址、网络掩码与子网.....	143
13.1 IP 地址.....	143
13.1.1 IP 地址结构.....	143
13.2 网络类别.....	144
13.3 子网掩码.....	145
第十四章 疑难排解.....	148
14.1 使用 IP 工具诊断问题.....	149
14.1.1 封包探测 (Ping).....	149
14.1.2 nslookup.....	150
第十五章 术语表.....	153

图片目录

图 2.1 前面板 LED 灯	3
图 2.2 后面板端口.....	4
图 3.1 硬件连接示意图.....	11
图 3.2 登录画面.....	17
图 3.3 设置向导主画面.....	18
图 3.4 设置向导 - 密码设置页面.....	18
图 3.5 设置向导- 系统信息设置页面.....	19
图 3.6 设置向导 - 日期/时间设置页面	19
图 3.7 设置向导 - LAN IP 设置页面	20
图 3.8 设置向导 - DHCP 服务器设置页面.....	20
图 3.9 设置向导 - WAN PPPoE 设置页面.....	21
图 3.10 设置向导- WAN 动态 IP 设置页面.....	21
图 3.11 设置向导- WAN 静态 IP 设置页面.....	22
图 4.1 设置管理界面登录窗口.....	26
图 4.2 典型的设置管理页面.....	27
图 4.3 设置向导主页.....	29
图 4.4 系统信息页面.....	29
图 5.1 局域网 IP 地址设置页面.....	31
图 5.2 DHCP 设置页面	33
图 5.3 局域网统计值页面.....	38
图 6.1 WAN PPPoE 设置页面	39
图 6.2 WAN 动态 IP (DHCP 客户端) 设置页面.....	43
图 6.3 WAN 静态 IP 设置页面.....	44
图 6.4 WAN 统计值页面.....	45
图 7.1 RIP 设置	48
图 7.2 静态路由设置.....	50
图 7.3 路由表.....	51

图 8.1 HTTP DDNS 网络图	53
图 8.2 HTTP DDNS 设置页面.....	55
图 9.1 静态 NAT - 将四个专有网络 IP 地址映射至四个全球有效的 IP 地址.....	59
图 9.2 动态 NAT - 四个专有 IP 地址映射至三个全球有效的 IP 地址.....	60
图 9.3 动态 NAT - 在 PC-B 断开连接后, PC-A 才能获得 NAT 连接.....	60
图 9.4 NAT - 将所有的内部网络 PC 映射至同一个全球有效的 IP 地址	61
图 9.5 反向静态 NAT - 将一个全球有效的 IP 地址映射至一台内部网络电脑.....	61
图 9.6 反向 NAT - 根据协议、端口号或 IP 地址中继传入的封包至内部主机.....	61
图 9.7 传入 ACL 设置页面.....	63
图 9.8 传入 ACL 设置范例.....	67
图 9.9 传出 ACL 设置页面.....	69
图 9.10 传出 ACL 设置范例.....	74
图 9.11 URL 过滤设置页面	76
图 9.12 URL 过滤规则范例	78
图 9.13 自我访问规则设置页面	79
图 9.14 服务列表设置页面	81
图 9.15 DoS 设置页面	87
图 9.16 IP 地址池设置页面.....	89
图 9.17 IP 地址池设置图.....	90
图 9.18 IP 地址池范例 - 新增两个 IP 地址池 - MISgroup1 与 MISgroup2.....	91
图 9.19 IP 地址池范例 - MISgroup1 禁用 QUAKE-II 连接.....	91
图 9.20 NAT 地址池设置页面.....	93
图 9.21 NAT 地址池设置图.....	94
图 9.22 NAT 地址池范例 - 新增一个静态 NAT 地址池	95
图 9.23 NAT 地址池范例 - 将 NAT 地址池附加到 ACL 规则 ...	95

图 9.24 时间范围设置页面	97
图 9.25 时间范围范例 - 新增时间范围	98
图 9.26 时间范围范例 - MISgroup1 禁止在工作时间访问 FTP	99
图 9.27 防火墙活动连接统计值	100
图 10.1 VPN 隧道(Tunnel)设置页面 - Pre-shared Key 模式	110
图 10.2 VPN 状况页面	114
图 10.3 典型的内部网络图	115
图 10.4 ISR1 的内部 VPN 策略设置	116
图 10.5 ISR2 的内部 VPN 策略设置	118
图 10.6 典型的外部网络图	120
图 10.7 外部网络范例 - ISR1 的 VPN 策略设置	122
图 10.8 外部网络范例 - ISR1 传出 NAT 地址池设置	122
图 10.9 外部网络范例 - ISR1 的传入 NAT 地址池设置	123
图 10.10 外部网络范例 - ISR1 的传出 ACL 规则	123
图 10.11 外部网络范例 - ISR1 的传入 ACL 规则	124
图 10.12 外部网络范例 - ISR2 的 VPN 策略设置	124
图 10.13 外部网络范例 - ISR2 传出 NAT 地址池设置	125
图 10.14 外部网络范例 - ISR2 的传入 NAT 地址池设置	125
图 10.15 外部网络范例 - ISR2 的传出 ACL 规则	126
图 10.16 外部网络范例 - ISR2 的传入 ACL 规则	126
图 11.1 系统服务设置页面	129
图 11.2 密码设置界面	129
图 11.3 系统信息设置页面	130
图 11.4 日期与时间设置页面	131
图 11.5 SNMP 设置	133
图 11.6 既有的 SNMP 设置	133
图 11.7 默认值设置页面	134
图 11.8 备份系统设置页面	135
图 11.9 恢复系统设置页面	135

图 11.10 Windows 文件浏览.....	136
图 11.11 固件升级页面.....	136
图 11.12 设置管理界面复位页面.....	137
图 11.13 设置管理界面登出页面.....	138
图 11.14 确认关闭浏览器 (IE).....	138
图 14.1 使用封包探测工具.....	149
图 14.2 使用 nslookup 工具.....	150

表格目录

表 2.1 前面板标示与 LED 灯.....	3
表 2.2 后面板标示.....	4
表 2.3 DoS 攻击.....	7
表 2.4 VPN 功能.....	9
表 3.1 LED 指示灯.....	12
表 3.2 默认设置概要.....	24
表 4.1 常用按钮和图标说明.....	28
表 5.1 局域网 IP 设置参数.....	31
表 5.2 DHCP 设置参数.....	34
表 5.3 分配 DHCP 地址.....	35
表 6.1 WAN PPPoE 设置参数.....	40
表 6.2 WAN 动态 IP 设置参数.....	42
表 6.3 WAN 静态 IP 设置参数.....	43
表 7.1 动态路由 (RIP) 设置参数.....	47
表 7.2 静态路由设置参数.....	49
表 8.1 DDNS 设置参数.....	54
表 9.1 传入 ACL 规则设置参数.....	63
表 9.2 传出 ACL 规则设置参数.....	70
表 9.3 URL 过滤设置参数.....	75

表 9.4 自我访问设置参数.....	79
表 9.5 服务列表设置参数.....	82
表 9.6 DoS 防范设置参数.....	85
表 9.7 IP 地址池设置参数.....	88
表 9.8 NAT 地址池设置参数.....	92
表 9.9 时间范围设置参数.....	96
表 10.1 路由器的默认连接.....	101
表 10.2 路由器默认的 IKE 设置.....	102
表 10.3 路由器默认的 IPSec 设置.....	103
表 10.4 VPN 隧道(Tunnel)设置参数.....	105
表 10.5 VPN 统计值.....	112
表 10.6 ISR1 上 VPN 封包的传出未转译防火墙规则.....	117
表 10.7 ISR1 上 VPN 封包的传入未转译防火墙规则.....	117
表 10.8 ISR2 上 VPN 封包的传出未转译防火墙规则.....	119
表 10.9 ISR2 上 VPN 封包的传入未转译防火墙规则.....	119
表 11.1 SNMP 参数设置.....	132
表 12.1 支持的 ALG.....	139
表 13.1 IP 地址结构.....	144
表 14.1 问题与建议解决方法.....	146

第一章 简介

感谢您购买华硕 SL1200 Internet安全路由器!

从现在开始，您的局域网(LAN)将可以通过高速宽带连接如 ADAL 或 Cable Modem 访问Internet。

此用户手册将介绍如何安装与设置华硕 SL1200，以更好地使用其功能。

1.1 特色

- 10/100Base-T 以太网路由器，可为局域网（LAN）内所有电脑提供 Internet 连接。
- 防火墙、NAT (网络地址转译) 及 IPSec VPN 功能，让您的局域网可以更安全地访问 Internet。
- 由 DHCP 服务器自动分配网络地址
- IP 路由、DNS 和 DDNS 设置、RIP、IP 性能监控等服务
- 预装设置程序，可通过网页浏览器访问，如 Microsoft Internet Explorer 5.5、Netscape 7.0.2 或更高版本。

1.2 系统需求

为使用华硕 SL1200 访问 Internet，您必须具备：

- ADSL 或 cable modem，并已开通了相应的服务。您的广域网至少需要有一个公共 Internet 地址。
- 一台或多台电脑，每台都配备有 Ethernet 10Base-T/100Base-T 网卡。
- (可选)若您要将设备连接到以太网中四台以上的电脑，则您需要有一台以太网集线器/交换机。
- 网页浏览器，如 Netscape 7.0.2，Microsoft Internet Explorer v5.5 或更高版本。

1.3 关于本用户手册

1.3.1 注意事项

- 本手册将在缩写词第一次出现时解释其含义，并将其含义解释收入术语表中。
- 为了方便起见，在本手册中，华硕 SL1200 简称为“本路由器”。

- 术语“LAN（局域网）”和“网络”在本手册中将交替使用，表示某个区域内由以太网连接的一组电脑。

1.3.2 印刷提示

- **斜体字** 表示该文字在术语表中有解释。
- **粗体字** 表示该文字是您从菜单或下拉菜单中选择的项目，或是需要您输入的内容。

1.3.3 提示符号

在本用户手册中会出现以下的图标及说明文字，请您特别注意这些重点事项，这些图标所代表的含义如下：



注意：提供对当前所述内容的说明或额外信息。



定义：解释用户可能不了解或不熟悉的术语或缩写。这些术语均可在术语表中查到。



警告：高重要性的信息，包括涉及人身安全和系统完整性的信息。

第二章 认识华硕 SL1200

2.1 包装内容

安装前，请检查包装盒内是否包含以下物品：

- 华硕 SL1200
- 电源适配器
- 以太网线（直通型）
- (选购) 管理接口连接线 (RJ-45)



以上各项若有损坏或缺失，请联系您的经销商。

2.2 前面板

前面板包含了一组 LED 指示灯，用于显示设备的状态。



图 2.1. 前面板 LED 灯

表 2.1. 前面板标示与 LED 灯

标示	颜色	功能
POWER	绿色	恒亮：设备电源已开启 熄灭：设备电源关闭
WAN	绿色	恒亮：WAN 连接已建立并处于活动状态 闪烁：数据正通过 WAN 连接进行传输 熄灭：未建立 WAN 连接
LAN1- LAN4	绿色	恒亮：LAN 连接已建立并处于活动状态 闪烁：数据正通过 LAN 连接进行传输 熄灭：未建立 LAN 连接

2.3 后面板

后面板包含连接端口与电源插孔。

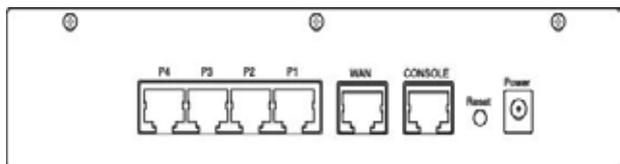


图 2.2. 后面板端口

表 2.2. 后面板标示

标示	功能
POWER	连接电源适配器
Reset	复位设备
CONSOLE	RJ-45 端口用于终端控制界面管理
WAN	连接您的 WAN 设备，如 ADSL 或 cable modem。
P1-P4	连接到您 PC 的以太网端口，或用线缆连接到您的局域网集线器/交换机的 uplink 端口。

2.4 主要功能

2.4.1 防火墙功能

华硕 SL1200 的防火墙可让您的网络免受攻击，且不会成为攻击的跳板。

防火墙功能包括：

- 地址分享与管理
- 封包过滤
- 状态封包检测
- DoS 攻击防范
- 应用程序内容过滤
- 记录与警报
- 远程访问
- URL 关键词过滤

2.4.1.1 地址分享与管理

华硕 SL1200 的防火墙可提供网络地址转译 (NAT) 功能，以分享单个高速 Internet 连接，节省局域网主机多重连接的连接成本。它可以隐藏网络地址避免其公开。它将与局域网连接的未注册主机的 IP 地址映射至可访问 Internet 的合法地址。

本路由器的防火墙还可提供反向 NAT 功能，让 SOHO 用户架设如 e-mail 服务器、web 服务器在内的多种服务。NAT 路由器将依据 NAT 规则执行转译机制。

本路由器可支持下列 NAT 类型：

- **静态 NAT:** 将一个内部的主机地址映射至一个全球有效的 Internet 地址 (一对一映射)。所有的封包都直接被转译。
- **动态 NAT:** 将一个内部主机地址动态映射至全球有效的 Internet 地址 (m 对 n 映射)。此映射通常包含一个内部 IP 地址池(m)与一个合法的 Internet IP 地址池(n)，m 的数值一般都大于 n。每一个内部 IP 地址将被映射至一个外部 IP 地址，采取先到先服务的机制。
- **NAPT(网络地址与端口转译)：**亦被称为 IP 伪装。将多个内部主机映射至一组全球有效的 IP 地址来连接至 Internet。而这项映射工作通常都是通过一个用来转译的网络端口地址池来进行。每一个封包都是通过此一全球有效的 IP 地址进行传输。

- **反向静态 NAT:** 此为传入映射，将一个全球有效的 Internet IP 地址映射至一个内部主机地址。所有传输至此外部 IP 地址的封包都会被传输至这个内部主机地址。当服务是由同一台主机主导时，这项功能是非常有用的。
- **反向 NAT:** 亦被称为传入映射、端口映射或虚拟服务器。任何来到路由器的封包都可依照映射规则中指定的协议、端口号或 IP 地址传输至内部主机。当多重服务是由不同的内部主机主导时，这项功能是非常有用的。



所有可支持的 NAT ALG 完整列表，请参考 **第十二章：ALG 设置**。

2.4.1.1 访问控制列表 (ACL)

防水墙可监控每一个独立的封包，并解读其传出与传入的包头信息。这项功能可以根据封包的来源地址、目的地地址、来源端口号、目的地端口号、协议与其他标准（如 ACL 规则定义的应用程序过滤与时间范围等）来阻止或允许封包传递。

ACL 能提供一个子网与另一个子网的隔离保护，从而达到被保护的网路堵塞回传的具体封包类型，能被用来作网路里的第一道防守线，让电脑免受威胁。

本路由器支持的防火墙 ACL 规则包括：

- 基于目的地与来源 IP 地址、端口号与协议的过滤方式
- 使用 wild card 组成过滤规则
- 过滤规则优先权定义
- 基于时间的过滤规则
- 应用程序的特定过滤规则
- 远程访问时基于用户群组的过滤规则

2.4.1.2 状态封包检测

华硕 SL1200 的防火墙采用“状态封包检测”功能，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连接尝试所需要的信息。它允许动态连接，这样除了需要的端口的外，其余端口就无须打开。这提供了高度安全的解决方式和可量测性及可扩展性。

2.4.1.3 DoS 攻击防范

华硕 SL1200 的防火墙具有攻击防范功能，用以保护内部网络免于遭受来自 Internet 已知类型的攻击。本功能提供对于阻绝服务攻击（DoS attack）的保护，像是 SYN Flooding（泛洪）、IP Smurfing（伪装）、LAND、Ping of Death 与所有可能被假定的攻击。它会丢弃 ICMP 重定向封包与 IP 松/严格来源路由封包。举例来说，SL1200 的防火墙功能提供对于“WinNuke”一种被广泛用来自远程 Internet 瘫痪窗口操作系统的攻击。此外，本路由器的防火墙功能也提供多种来自 Internet 的攻击，像是 IP spoofing、Ping of Death、Land Attack、封包重组与 SYN flooding（泛洪）攻击。

表 2.3 中所列举者为 SL1200 可防范的攻击类型。

表 2.3. DoS 攻击

攻击类型	攻击名称
封包重组式攻击	Bonk, Boink, Teardrop (New Tear), Overdrop, Opentear, Syndrop, Jolt
ICMP 攻击	Ping of Death, Smurf, Twinge
Flooders 攻击	ICMP Flooder, UDP Flooder, SYN Flooder
端口扫描	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 规则的保护	Echo-Chargen, Ascend Kill
其他类型的攻击	IP Spoofing, LAND, Targa, Tentacle MIME Flood, Winnuke, FTP Bounce, IP unaligned time stamp attack

2.4.1.4 应用层网关 (ALG)

应用程序如 FTP、游戏等，打开了基于各自应用参数的动态连接。属于应用程序的封包，若要通过路由器上的防火墙，需要一个相应的允许规则。当缺少这种规则时，这些封包将被路由器的防火墙丢弃。由于为多个应用程序动态地建立规则（同时不影响安全性）并不可行，因此，以应用层网关（ALG, Application Level Gateway）的形式为应用程序解析封包与打开动态连接成为一种智慧型解决方案。本路由器的防火墙功能为常用的应用程序，如 FTP、H.323、RTSP、Microsoft Games、SIP 等，提供了相应的 ALG 规则。

2.4.1.5 URL 过滤

您可以定义一组不允许在 URL（一致性资源定址器，俗称网址，如 www.yahoo.com）中出现的关键词。任何包含一个或多个被禁止关键词的 URL 将被封锁。这是一个独立于规则的功能，并没有与 ACL 规则相关联。此功能可以单独开启或关闭，但只有在防火墙开启的状况下才有效。

2.4.1.6 记录与警告

网络中可能会影响安全性的事件，都被记录在路由器的系统日志文件中。事件的详细内容被记录为 WebTrends Enhanced Log Format (WELF) 格式，因此可以用状态统计工具来产生客户报告。防火墙也可以将系统日志 (Syslog) 传给专用网络的 Syslog 服务器。

华硕 SL1200 的防火墙支持：

- 用电子邮件向网络管理员传送警告。
- 日志详细内容至少包括封包到达时间、防火墙动作记录与动作原因在内。
- 支持 UNIX Syslog 格式。
- 依照网络管理员设置的时间表，或依照默认的设置，当系统日志文件满时通过电子邮件来传送系统日志。
- 所有信息都以 WELF 格式传送。
- ICMP logging 显示代码与类型。

2.4.2 VPN

被广泛使用的公共网络，例如 Internet 给用户带来了诸多好处，同时也带来了许多风险。这些风险包括传送数据缺乏保密性，以及数据交换各方缺乏身份验证。华硕 SL1200 支持的 VPN 功能就能解决这些问题。

本路由器支持的 VPN 功能可兼容于 IPSec。通过 VPN 传送的封包经过了加密，以确保其保密性。接着，已加密的封包在公共网络中传送。应用此功能，用户可获得与专用网络成员相同的安全性及功能。

表 2.4 列出了本路由器支持的 VPN 功能。

表 2.4. VPN 功能

功能	
传输模式 (Transport Mode) 用于客户端- 客户端连接	
隧道模式 (Tunnel Mode) 用于网络- 网络连接	
IP 分割与重组	
IPSec	支持
硬件加密演算法	DES, 3DES
硬件认证演算法	MD5, SHA-1
转换	ESP, AH
密钥管理	IKE (Pre-shared key)
IKE 模式设置	Main Mode, Aggressive Mode, Quick Mode



网站至网站 VPN 连接 是一种可供选择的 WAN 结构，用于连接各办公室分部、家庭办公室或生意各方网站到公司的全部或部分网络。

第三章 快速安装指南

本章节提供了将华硕 SL1200 连接至电脑或局域网的基本说明。

- 第一部分 讲述如何连接硬件。
- 第二部分 讲述如何在您的电脑上进行 Internet 选项的设置。
- 第三部分 引导您对 SL1200 进行基础设置，让您的局域网可以连接到 Internet。



本章节假设您已经与您的 Internet 服务供应商 (ISP) 建立 ADSL 或者 Cable Modem 服务。这些安装指导提供的是一些基本的设置，适合家庭网络或小型办公网络。如需要其他的设置信息，请参考后续章节。

3.1 第一部分 — 连接硬件

本部分将介绍将本设备连接到 ADSL 或 Cable Modem (已连接电话线或是有线电视线缆)，并连接电源与您的个人电脑的相关说明。



在您开始的前，请关闭所有设备的电源，包括您的电脑，局域网集线器/交换机 (如果可行)，以及 SL1200 路由器。

3.1.1 连接 ADSL 或 cable modem

连接路由器

请将以太网线的一端连接到本设备后面板标示有 WAN 的端口，并将网线的另一端连接到 ADSL 或 Cable modem 的以太网端口。

3.1.2 连接电脑或局域网

若您的局域网中的电脑只有四台或更少，您可以以太网线将它们直接连接到设备内建的交换机。您必须将以太网线的一端连接到设备后面板标示有 LAN1 - LAN4 的任意一个端口，另一端连接到电脑的以太网端口。

若您的局域网中的电脑多于四台，您可将以太网线的一端连接到集线器或交换机，可以是一个 uplink 端口(请参考集线器或交换机的说明)，另一端连接到路由器上的以太网交换端口(标示为 LAN1 - LAN4)。



您可以使用交叉型或直通型以太网线来连接内建的交换机、电脑、集线器或交换机。

3.1.3 连接电源适配器

请将 AC 电源适配器的一端连接到本设备后方的 POWER 电源插座，并将电源供应器另一端的插头插到室内插座上。

3.1.4 开启华硕 SL1200 的电源

插好电源后，路由器电源将自动开启。此时请开启您的 ADSL 或 cable modem、电脑与您的局域网设备（如集线器或交换机）的电源。

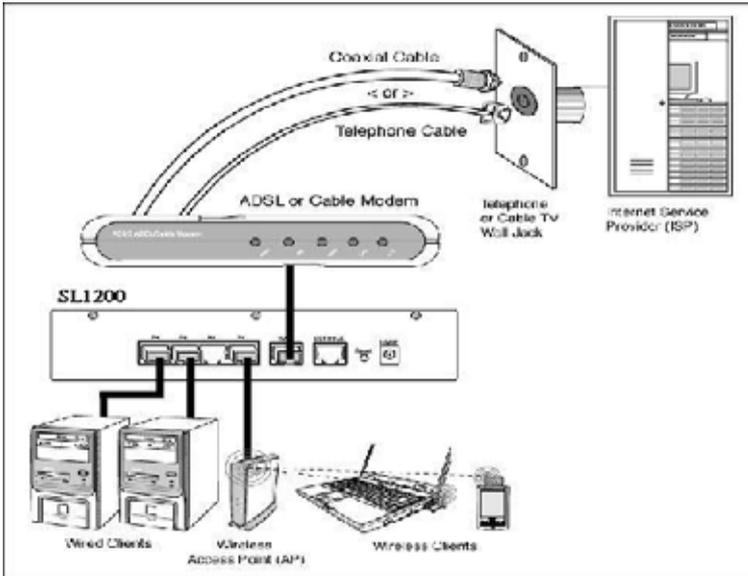


图 3.1. 硬件连接示意图



请参列表 3.1 检查 LED 指示灯的状态，以确定设备硬件是否运作正常。

表 3.1. LED 指示灯

LED	说明
POWER	稳定的绿色代表设备已开启。若此灯不亮，请检查电源适配器是否已正确连接电源。
LAN1 - LAN4	稳定的绿色代表路由器可以与局域网通信，闪烁代表路由器正在传送数据至 LAN 设备，或从 LAN 设备接收数据。
WAN	稳定的绿色代表设备已成功与您的 ISP 建立连接，闪烁则代表设备正在与Internet传送或接收数据。

3.2 第二部分 — 设置您的电脑

本部分将介绍如何进行电脑的 Internet 设置，以使其与路由器协同工作。

3.2.1 在您开始的前

在默认情况下，华硕 SL1200 会自动为您的 PC 进行所有需要的 Internet 设置。您只需在设置完成后，让您的 PC 接受这些设置。



在有些情况下，您可能需要手动为某些电脑进行网络设置，而不是让 Internet 安全路由器来做。请参考 3.2.6 为您的 PC 分配静态 IP 地址 部分的说明。

若您已通过以太网连接了您的 PC 与路由器，请根据您所安装的操作系统，依照下列说明进行操作。

3.2.2 Windows® XP PC

1. 在 Windows 任务栏，点击 **开始** -> **控制面板**。
2. 双击 **网络连接** 图标。
3. 在 **局域网或高速 Internet** 窗口中，用鼠标右键点击您的网络接口卡 (NIC) 所对应的图标，接着选择 **属性**。此图标通常被标记为 **本地连接**。
本地连接 对话框显示了当前已安装的所有网络项目列表。
4. 请确保您勾选了 **Internet Protocol(TCP/IP)**，选中此项目，接着按下 **<属性>**。
5. 在 **Internet 协议 (TCP/IP) 属性** 对话框中，选择 **自动获得 IP 地址**。同时选择 **自动获得 DNS 服务器地址**。
6. 按下 **<确定>** 两次以确认您所作的变更，然后关闭 **控制面板**。

3.2.3 Windows® 2000 PC



检查 IP 协议，如果需要，请安装。

1. 在 Windows 任务栏，点击 **开始** -> **控制面板**。
2. 双击 **网络与拨号连接** 图标。
3. 在 **网络与拨号连接** 窗口，用鼠标右键点击 **本地连接** 图标，然后选择 **属性**。
本地连接 对话框显示了当前已安装的所有网络项目列表。若此列表中已经包含 **Internet 协议 (TCP/IP)**，则代表此协议已经可用。请跳至第 10 步。
4. 若 **Internet 协议 (TCP/IP)** 没有显示在已安装项目中，请点击 **<安装>**。
5. 在 **选择网络组件类型** 对话框中，选择 **协议**，接着点击 **<添加>**。
6. 在 **选择网络协议** 窗口中选择 **Internet 协议 (TCP/IP)**，接着点击 **<确定>**。
系统可能会提示您从 Windows 2000 安装光盘或其他媒体中安装文件。请依照说明来安装文件。
7. 若提示您重新启动电脑，请选择 **<确定>**。
接下来，设置让 PC 接受路由器分配的 IP 地址。
8. 在 **控制面板** 中，双击 **网络与拨号连接** 图标。
9. 在 **网络与拨号连接** 窗口中，用鼠标右键点击 **本地连接** 图标，然后选择 **属性**。
10. 在 **本地连接** 对话框中，选择 **Internet Protocol (TCP/IP)**，接着点击 **<属性>**。
11. 在 **Internet Protocol (TCP/IP) 属性** 对话框中，选择 **自动获得 IP 地址**。同时选择 **自动获得 DNS 服务器地址**。

12. 按下 <确定> 两次以确认您所作的变更，然后关闭 控制面板。

3.2.4 Windows® 95, 98 与 Me PC

1. 在 Windows 任务栏，点击 开始 -> 设置 -> 控制面板。
2. 双击 网络 图标。

在 网络 对话框中，寻找一个以 “TCP/IP ->” 与您的网卡名称开头的项目，接着按下<内容>。您可能需要向下拉动右边的卷轴来找到这个项目。

若列表中包含这一项目，则代表 TCP/IP 协议已经可用。请跳至第 8 步。
3. 若 Internet 协议 (TCP/IP) 没有显示在已安装的项目中，请点击 <添加>。
4. 在 选择网络组件类型 对话框中，选择 协议，接着按下 <新增>。
5. 在 制造商 列表中选择 Microsoft，然后在 网络协议 列表中选择 TCP/IP，接着按下 <确定>。

系统可能会提示您从 Windows 95, 98 或 Me 安装光盘或其他媒体中安装文件。请依照说明来安装文件。
6. 若提示您重新启动电脑，请选择 <确定>。

接下来，设置让 PC 接受路由器分配的 IP 地址。
7. 在 控制面板 中，双击 网络 图标。
8. 在 网络 对话框中，找到一个以 “TCP/IP ->” 与您的网卡名称开头的项目，接着按下<属性>。
9. 在 Internet Protocol (TCP/IP) 内容 对话框中，选择 自动获得 IP 地址。
10. 在 Internet Protocol (TCP/IP) 内容 对话框中，点击 默认网关 标签页。

在 新网关 栏位输入 192.168.1.1 (路由器默认的 LAN 端口 IP 地址)，接着按下 <新增> 以增加这个默认的网关项目。
11. 按下 <确定> 两次以确认您所作的变更，然后关闭 控制面板。
12. 若提示您重新启动电脑，请选择 <确定>。

3.2.5 Windows® NT 4.0 工作站



检查 IP 协议，如果需要，请安装。

1. 在 Windows NT 任务栏，点击 **开始** -> **设置** -> **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，点击 **协议** 标签页。
协议标签页显示了当前已安装的所有网络项目列表。若此列表中已经包含 TCP/IP 协议，则代表此协议已经可用。请跳至第 9 步。
4. 若 TCP/IP 协议没有显示在已安装的项目中，请点击 **<新增>**。
5. 在 **选择网络协议** 对话框中，选择 TCP/IP，接着点击 **<确定>**。
系统可能会提示您从 Windows NT 安装光盘或其他媒体中安装文件。请依照说明来安装文件。
所有文件安装完成后，会出现一个窗口，告知您可以安装一项被称为 DHCP 的 TCP/IP 服务，这项服务可动态分配 IP 地址。
6. 点击 **<是>** 继续安装，若提示您重新启动电脑，请选择 **<确定>**。
接下来，设置让 PC 接受路由器分配的 IP 地址。
7. 在 **控制面板** 中，双击 **网络** 图标。
8. 在 **网络** 对话框中，点击 **协议** 标签页。
9. 在协议标签页中，选择 TCP/IP，接着按下 **<属性>**。
10. 在 Microsoft TCP/IP 协议 对话框中，选择 **从 DHCP 服务器获得 IP 地址**。
11. 按下 **<确定>** 两次以确认您所作的变更，然后关闭 **控制面板**。

3.2.6 为您的电脑分配 IP 地址

在某些情况下，您可能需要直接分配某些或全部 PC 的 IP 地址（称为“静态”），而不是由华硕 SL1200 来分配。此选项可能在下列情况下需要（并不是必须）：

- 您已经获得了一个或多个公共 IP 地址，您想要将它（们）分配给特定的电脑（如，您的一台电脑正作为公共网络服务器使用）。
- 您的局域网包含不同的子网。

尽管如此，在您首次设置路由器时，您必须将 PC 的 IP 地址设置在 192.168.1.0 网段内，如 192.168.1.2。这是因为您需要建立路由器与 PC 的连接，而路由器的默认 LAN IP 已经设为 192.168.1.1。在子网掩码栏位输入 255.255.255.0，默认网关栏位输入 192.168.1.1。首次设置完成后，您可以依据实际的网络环境来更改这些设置。

在您希望分配静态 IP 地址的每台 PC 上，依照第 13 页至第 15 页的说明来检查该 PC 是否已安装 IP 协议。若已安装，请依照说明让其显示 Internet Protocol (TCP/IP) 的各项内容。选择 **使用下面的 IP 地址** 来手动设置 IP 地址，子网掩码与默认网关。



您的 PC 的 IP 地址必须与路由器 LAN 端口的 IP 地址位于同一子网中。若您想要手动分配所有局域网 PC 的 IP 地址，您可以参考第五章的说明来设置 LAN IP 地址。

3.3 第三部分 — 华硕 SL1200 的快速设置

本部分将介绍如何登录设置管理界面 (Configuration Manager)，一个已预先安装于华硕 SL1200 的网页界面管理程序。本部分还将给出有关 Internet 连接设置的基本说明。您需要向您的 ISP 获得必要的信息才能完成此部分设置。



本部分旨在快速设置华硕 SL1200 以使其运作，因此这里只提供了一些简要的说明。详细内容您可以参考相应的章节。

3.3.1 设置向导 (Setup Wizard) 中使用的按钮

华硕 SL1200 预装了一个称为设置管理界面 (Configuratin Manager) 的应用程序，可让您通过网页浏览器对路由器进行设置。您在使用本设备的前最可能需要更改的设置都被归入到一系列设置页面，并由设置向导引导您完成这些更改。下表列出了您在使用设置向导时会用到的按钮。

按钮	功能
	点击此一按钮可保存信息并进入下一个设置页面。
	点击此一按钮可返回上一设置页面。

3.3.2 设置华硕 SL1200

设置路由器

1. 在访问路由器的设置管理界面（Configuration Manager）的前，请确保您浏览器的 HTTP 代理已被关闭。在 IE 中，点击 工具 -> Internet 选项 -> 连接 -> 局域网设置，接着取消勾选 为 LAN 使用代理服务。
2. 在任何一台连接了路由器 LAN 端口的 PC 上，打开网页浏览器，并在网址栏内输入以下的 URL，并按下 <Enter>:

http://192.168.1.1

这是路由器 LAN 端口默认的 IP 地址。此时将出现一个登录画面，如图 3.2 所示。



图 3.2. 登录画面

若您在连接路由器时遇到了问题，您可以：检查您的 PC 是否设置为接受路由器分配的 IP 地址，或您 PC 的 IP 地址是否位于 192.168.1.0 网段内，如 192.168.1.2。

3. 输入用户名称与密码，接着点击 <OK> 以登录设置管理界面（Configuration Manager）。当您首次登录时，请使用下面的设置：

默认的用户名称: admin

默认的密码: admin

当您每次登录设置管理界面（Configuration Manager）时，都会显示设置向导主画面。



图 3.3. 设置向导主画面

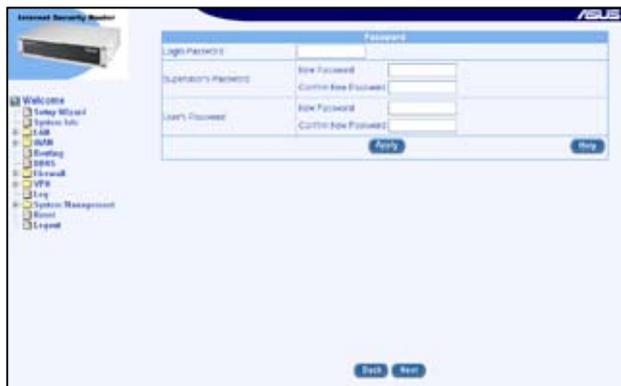


图 3.4. 设置向导 - 密码设置页面

4. 点击 <Next> 进入图 3.4 所示的密码设置页面。如果需要，您可以更改密码。否则，请点击 <Next> 进入下一个设置页面。
在更改密码时，请确认在 Login Password（登录密码）栏位输入原来的登录密码，更改密码后点击 <Apply> 保存您所做的变更。

- 在 System Information Setup (系统信息设置) 页面, 输入所需的信息, 接着点击 <Apply> 保存变更。否则, 点击 <Next> 进入下一个设置页面。



图 3.5. 设置向导 - 系统信息设置页面



图 3.6. 设置向导 - 日期/时间设置页面

- 在 Date/Time Setup (日期/时间设置) 页面, 从时区下拉式菜单中选择您所在的时区。点击 <Apply> 保存您所做的变更, 接着点击 <Next> 进入下一个设置页面。



路由器内部没有实时钟。系统日期与时间由外部网络时间服务器来保持。您没有必要在这里设置日期与时间, 除非您无法访问时间服务器, 而需要让路由器保持自己的时间。

7. 我们建议您此时先保留默认的 LAN IP 设置，直到您完成剩下的设置，并确认您的 Internet 连接运作正常。
点击 <Next> 进入下一个设置页面。

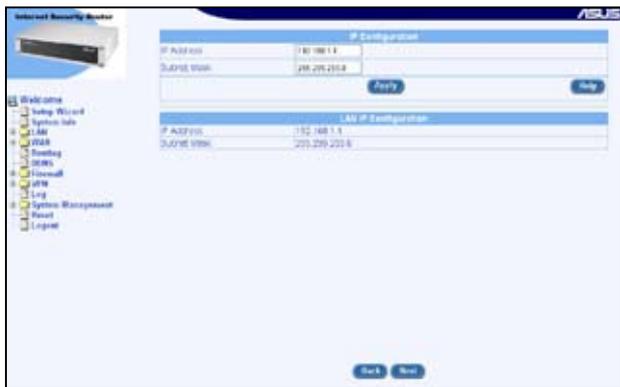


图 3.7. 设置向导 - LAN IP 设置页面



图 3.8. 设置向导 - DHCP 服务器设置页面

8. 我们建议您此时先保留默认的 DHCP 服务器设置，直到您完成剩下的设置，并确认您的 Internet 连接运作正常。
点击 <Next> 进入下一个设置页面。
9. 在 WAN Configuration (WAN 设置) 页面，您可以进行路由器的 WAN 设置。根据您的 ISP 提供的连接模式，您可以从 Connection Mode 下拉式菜单的三种连接模式中选择一个(如图 10)：PPPoE，Dynamic (动态) 与 Static (静态)。

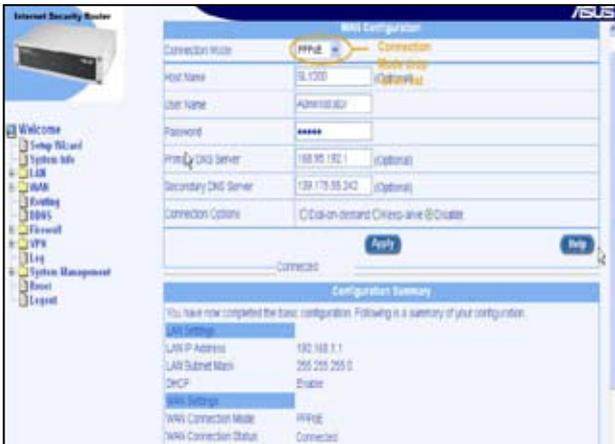


图 3.9. 设置向导 - WAN PPPoE 设置页面



图 3.10. 设置向导 - WAN 动态 IP 设置页面

a) PPPoE 连接模式 (如图 3.9)

- 您不需要输入主要 / 次要 DNS 服务器的 IP 地址。PPPoE 能够自动从您的 ISP 那里获得这些信息。但是，若您希望使用某特定的 DNS 服务器，您也可以在相应栏位输入服务器地址。
- Host name (主机名) 是选填的。若您的 ISP 没有提供此信息，您可以不填写这个栏位。
- 输入由 ISP 提供的用户名称与密码。
- 点击 <Apply> 保存 PPPoE 设置。

b) 动态 IP 连接模式 (如图 3.10)

- 您不需要输入主要 / 次要 DNS 服务器的 IP 地址。DHCP 客户端能够自动从您的 ISP 那里获得这些信息。但是，若您希望使用某特定的 DNS 服务器，您也可以在相应栏位输入服务器地址。
- Host name (主机名) 是选填的。若您的 ISP 没有提供此信息，您可以不填写这个栏位。
- 若您的前已向您的 ISP 注册了一个 MAC 地址用于 Internet 连接，请输入此注册的 MAC 地址，并确保您勾选了 MAC Cloning 复选框。
- 点击 <Apply> 保存动态 IP 设置。



图 3.11. 设置向导 - WAN 静态 IP 设置页面

c) 静态 IP 连接模式 (如图 3.11)

- 在 IP Address 栏位输入 WAN IP 地址。此信息由您的 ISP 提供。
- 为 WAN 指定 Subnet Mask (子网掩码)。此信息由您的 ISP 提供。通常情况下, 为 255.255.255.0。
- 输入由您的 ISP 提供的网关地址。
- 您至少需要输入 ISP 提供的主要 DNS 服务器的 IP 地址。此要 DNS 服务器的 IP 地址是选填的。若您的 ISP 提供了此信息, 请将其填入指定栏位。
- 点击 <Apply> 保存静态 IP 设置。

您已经完成了基本的设置。现在, 您可以在您的 PC 或局域网中用华硕 SL1200, 通过华硕 ADSL 或 cable modem, 连接到 Internet。

3.3.3 测试您的设置

现在, 路由器应该可允许局域网中的任何一台电脑通过路由器的 ADSL 或 cable modem 连接来访问 Internet。

您可以输入任意一个外部 URL (如 <http://www.yahoo.com>) 来测试网络连接。若标示为 WAN 的 LED 灯快速闪烁并变为稳定, 代表设备已连接至网络。您应该可以用网页浏览器来浏览网页。

若 LED 灯没有像预期的一样亮起, 或网页无法显示, 请参见第十四章的疑难排解。

3.3.4 路由器的默认设置

除了您的 ISP 所提供的 DSL 连接服务外, 本路由器为您的网络提供了多种服务。本设备默认的设置适用于典型的家庭或小型办公室网络。

表 3.2 列出了一些最重要的默认设置。这些与其他的特性都会在其后的章节中详细叙述。若您熟悉网络设置, 请对照表 3.2 来检查它们是否符合您的网络需求。如果需要, 您可以依照说明来更改设置。若您不熟悉这些设置, 您可以使用本设备默认的设置, 或联系您的 ISP 以寻求帮助。

在您更改任何设置的前, 请先查阅第四章关于访问与使用设置管理界面的说明。我们强烈建议您在更改默认设置前, 先与您的 ISP 联系。

表 3.2. 默认设置概要

栏位	默认设置	解释/说明
DHCP (动态主机设置协议)	DHCP 服务器开启, 地址池: 192.168.1.10 至 192.168.1.108	Internet 安全路由器拥有一个专用 IP 地址池, 可动态分配给您的局域网电脑。为使用这项服务, 您必须允许您的电脑动态接受 IP 地址, 如快速安装指南中的第二部分所述。DHCP 服务的相关说明请参考 5.2 章节的说明。
LAN 端口 IP 地址	静态 IP 地址: 192.168.1.1 子网掩码: 255.255.255.0	这是 Internet 安全路由器 LAN 端口的 IP 地址。LAN 端口连接您的设备至以太网。一般情况下, 您不需要更改这个地址。请参考 5.1 LAN IP 地址部分的相关说明。

第四章 使用设置管理界面

华硕 SL1200 预装了设置管理界面(Configuration Manager)，可让您按照您的网络需求设置此设备。您可以通过任何一台连接到路由器局域网（LAN）或广域网（WAN）端口的电脑的网页浏览器来访问此设置管理界面。

本章节将会针对使用设置管理界面功能有一基本的描述与指导。

4.1 登录设置管理界面

设置管理界面为预先安装于 SL1200 中的工具程序。如欲进入此程序，您需要具备以下条件：

- 如同快速安装指南一章中的叙述，您需拥有一台连接至 SL1200 上的局域网（LAN）或广域网（WAN）端口的个人电脑。
- 电脑中安装有网页浏览器。如 Microsoft Internet Explorer 5.5、Netscape 7.0.2 或更高版本。

您可以通过任何一台连接到路由器局域网（LAN）或广域网（WAN）端口的电脑的网页浏览器来访问此设置管理界面。这里的说明是以连接于 SL1200 局域网（LAN）端口的电脑进行步骤式解说。

通过局域网（LAN）端口进行连接

1. 从一部局域网中的电脑，开启网络浏览器并在浏览器的地址栏输入下列网址（或位置），接着按下 <Enter> 键：

`http://192.168.1.1`

这是在 SL1200 上的局域网端口所默认的IP 地址。接着会显示出登录窗口，如图 4.1 所示。



图 4.1. 设置管理界面登录窗口

2. 输入您的用户名称与密码，接着点击 <OK>。

当您首次登录时，请使用下面的默认设置：

默认的用户名称: admin

默认的密码: admin



您可以随时更改密码。请参考 11.2 更改登录密码 部分的说明。

当您每次登录设置管理界面时，设置向导页面都会出现，如图 4.3 所示。

4.2 设置页结构

典型的设置管理界面包含两个独立部分：左侧栏与右侧栏。

左侧栏，如图 4.2 所示，包含所有的菜单与设备可用的设置。菜单由文件图标所指示，相关的菜单被分为一个类型，如 LAN 与 WAN，由相应的扩展文件夹图标所指示。您可以点击任何一个文件夹来显示相关设置页面。

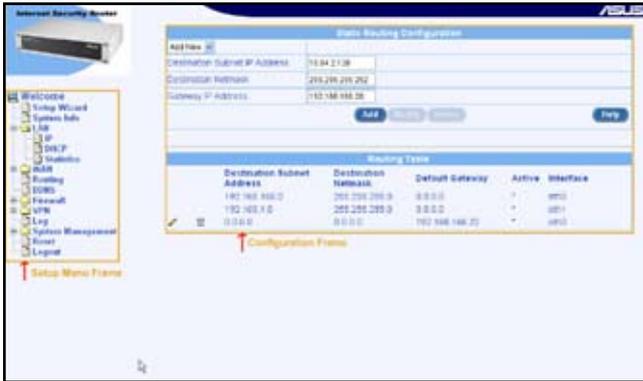


图 4.2. 典型的设置管理页面

右侧栏显示了所选设置页面的相关信息。

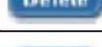
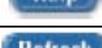
4.2.1 菜单导航

- 开启相关的扩展菜单，点击相应文件夹图标 旁边的加号(+)。
- 要收回一组相关菜单，点击相应已开启的文件夹 旁边的减号(-)。
- 要开启一个特定的设置页面，点击所需菜单项目旁边的文件图标 。

4.2.2 常用的按钮与图标

下面是一些在设置管理界面中经常用到的按钮或图标。下表描述了每个按钮或图标的功能。

表 4.1. 常用按钮和图标说明

按钮 / 图标	功能
	保存您对当前页面的所有更改。
	在系统中新增设置，如静态路由或防火墙 ACL 规则。
	修改系统中一已存在的设置，如静态路由或防火墙 ACL 规则。
	删除所选项目，如静态路由或防火墙 ACL 规则。
	在单独的浏览器窗口开启当前主题线上说明。任何主要的主题页面都可以使用说明功能。
	用更新后的状态或设置重新显示当前页面。
	选择需要编辑的项目。
	删除所选项目。

4.3 设置管理界面主页

当您首次访问设置管理界面时，设置向导（Setup Wizard）主页会出现。



图 4.3. 设置向导主页

4.4 系统设置概观

要查看系统整体的设置，请先登录设置管理界面，接着请点击 System Info 菜单。图 4.4 所示即为系统信息 (System Info) 页面可获得的信息。



图 4.4. 系统信息页面

第五章 局域网 (LAN) 设置

本章节将描述如何为路由器进行基本的局域网设置。您将会了解到如何设置 IP 地址、DHCP 与 DNS 服务器的基本内容。

5.1 局域网的 IP 地址

若您想使用路由器连接局域网中的多台电脑，您必须通过本设备的内建交换机的以太网端口来连接局域网电脑。您必须为局域网中的每台电脑分配一个特定的 IP 地址。SL1200 作为网络中的一个节点，其 IP 地址必须与局域网内 PC 的 IP 地址位于同一子网下。SL1200 的默认 IP 地址为 192.168.1.1。



网络节点可以被认为是设备连接至 Internet 的任何接口，如 SL1200 的局域网端口与您 PC 上的网卡。有关子网的说明，请参考第十三章。

您可以更改此默认值，以适应您网络的 IP 地址设置。



SL1200 本身可作为您局域网电脑的 DHCP 服务器来使用，如 5.2.3 设置 DHCP 服务器 章节所述。但不能作为它自身的 LAN 端口的 DHCP 服务器。

5.1.1 局域网 IP 设置参数

表 5.1 所示为局域网 IP 设置可用的设置参数。

表 5.1. 局域网 IP 设置参数

设置	说明
IP Address	本路由器的 IP 地址。此 IP 地址用来表示路由器的局域网 (LAN) 端口。由您的 ISP 分配给您的公共 IP 地址不是您的局域网 IP 地址。公共 IP 地址是用来表示路由器连接至 Internet (WAN) 端口。
Subnet Mask	局域网的子网掩码用来表明局域网 IP 地址中哪些部分是代表网络整体, 哪些部分代表网络中的节点。您设备的默认子网掩码为 255.255.255.0。

5.1.2 设置局域网 IP 地址

更改默认的局域网 IP 地址

1. 以管理员身份登录设置管理界面, 接着点击 LAN 菜单。
当 LAN Configuration 子菜单出现时, 点击 IP 子菜单以显示 IP 地址设置页面, 如图 5.1 所示。



图 5.1. 局域网 IP 地址设置页面

2. 为路由器输入局域网 (LAN) IP 地址与子网掩码。
3. 点击 <Apply> 保存此局域网 (LAN) IP 地址。



若您在使用以太网时更改此 IP 地址，则当前网络连接会中断。

4. 如果需要的话，重新设置您的电脑，以使它们的 IP 地址与路由器新设置的局域网 (LAN) IP 地址位于同一子网内。详细内容请参考 3.2 第二部分 — 设置您的电脑。
5. 在您的网页浏览器网址栏内输入新的 IP 地址，即可登录设置管理界面。

5.2 动态主机控制协议 (DHCP)

5.2.1 何谓 DHCP 服务器？

DHCP 是让网络管理员能够统一管理网络环境中，把 IP 信息配发给电脑的一项协议。

当你开启 DHCP 服务器后，您能让像 SL1200 路由器这类的设备分配暂用的 IP 地址给连接至网络的电脑。这项分配的设备便称做 DHCP 服务器，而接收设备则称做 DHCP 客户端。



如果你依照快速安装指南的介绍操作。您除了可以分配 IP 地址给予局域网中的每一部电脑外，也可以指定其动态（自动）接受 IP 信息。如果您选择动态接收 IP 地址，则您可以设置您的电脑做为 DHCP 客户端来接受像 SL1200 这类设备所配发的 IP 地址。

DHCP 服务器会从一个经过定义的 IP 地址池中在特定的时间内借出这些 IP 地址给提出上网需求的电脑。此外它也会监控、收集，并视需要配发这些 IP 地址。

在启用 DHCP 的网络中，IP 信息是经由动态配发而非静态的。一个 DHCP 客户端当每次进行网络连接时，便会从 DHCP 服务器的 IP 地址池中被动态分配不同的 IP 信息。

5.2.2 为何要使用 DHCP 服务器？

使用 DHCP 服务器可以让您通过使用 SL1200 管理与分配 IP 地址。若是没有 DHCP 服务器，您便需要分别设置每部电脑的 IP 地址与相关信息。在较大的网络环境或是常扩展网络设备的环境中，DHCP 服务器是较常被采用的 IP 配发方式。

5.2.3 设置 DHCP 服务器

 默认值中，在局域网中 SL1200 是被设置做为 DHCP 服务器，使用预先设置从 192.168.1.10 至 192.168.1.42 的地址池（子网掩码则为 255.255.255.0）。若要变更地址范围，请依照本节中接下来所叙述的步骤进行设置。

如何设置 DHCP 服务器

 首先，您必需设置您的个人电脑使其可以接收由 DHCP 服务器。

1. 以管理员身份登录设置管理界面。点击 LAN -> DHCP。此时将出现 DHCP 设置页面，如图 5.2 所示。



图 5.2. DHCP 设置页面

2. 输入 IP 地址池（开始 / 结束地址），子网掩码，IP 租约时间与默认网关地址等信息。其他栏位是选填的，如 主要 / 次要 DNS 服务器 IP 地址与 主要 / 次要 WINS 服务器 IP 地址。但是，我们建议您输入 主要 DNS 服务器 IP 地址。您可以在 主要 DNS 服务器 IP 地址栏位输入局域网 IP 地址，或您的 ISP 提供的 DNS IP 地址。表 5.2 详细说明了 DHCP 设置参数。

表 5.2. DHCP 设置参数

栏位	说明
IP Address Pool Begin/End	指定 DHCP 地址池中最高和最低的地址范围。
Subnet Mask	输入 DHCP 地址池所使用的子网掩码。
Lease Time	指定使用借出 IP 地址的个人电脑使用该 IP 地址的时间。
Default Gateway IP Address	从 IP 地址池中接收 IP 地址的电脑的默认网关地址。默认的网关地址是 DHCP 客户端电脑首先用来连接 Internet 设备的 IP 地址。一般而言，这便是指 SL1200 的局域网端口的 IP 地址。
Primary/Secondary DNS Server IP Address	网域名称系统的 IP 地址是被由地址池中获得 IP 地址的电脑所使用。DNS 服务器会自动转译您输入在网址栏的名称为数字化的 IP 地址。一般来说服务器是位于您的 ISP 那里。但是，您可以输入 SL1200 局域网 IP 地址，来把它当作是局域网电脑的 DNS 代理或是转发来自局域网至 DNS 服务器的 DNS 需求（因为它有 DNS 代理的功能，可以将 DNS 请求提交给 DNS 服务器），并回复结果至局域网的电脑。请注意！无论主要（第一）或次要（第二）的 DNS 服务器都是非必需输入的。
Primary/Secondary WINS Server IP Address (optional)	WINS 服务器的 IP 地址是被由地址池中获得 IP 地址的电脑所使用。您并不需要输入此项信息，除非您的网络环境中存在 WINS 服务器。

3. 点击 <Apply> 来保存 DHCP 服务器的设置。

5.2.4 查看目前分配的 DHCP 地址

当 SL1200 做为您局域网中的 DHCP 服务器使用时，它将会记录借出 IP 地址给予您电脑的时间。若要查看所有 IP 地址的配发列表，只要开启 DHCP 服务器设置页面，在该页的下方显示了所有现存的 DHCP 地址配发状况。

DHCP 服务器地址表列出了所有当前被局域网设备所借出的 IP 地址。

表 5.3 列出了每个借出地址的信息。

表 5.3. 分配 DHCP 地址

栏位	说明
MAC Address	从 DHCP 服务器借出 IP 地址的设备的硬件 ID。
Assigned IP Address	从地址池中借得的 IP 地址。
IP Address Expired on	所借 IP 地址的到期时间。

5.3 DNS

5.3.1 关于 DNS

网域名称系统 (Domain Name System, DNS) 服务器, 提供用户一个相当便利的网址输入方式 (如 "yahoo.com"), 这个网址在实际上等于 Internet 路由中所输入的 IP 地址。

当电脑用户在浏览器中输入一个网域名称, 接着电脑会向 DNS 服务器发出一个请求, 来要求获得相对应的 IP 地址。然后 DNS 服务器会试着在自己的数据库里面找寻此网域名称, 若没找到, 则会向更高一等级的 DNS 服务器提出搜寻的需求。当地址找到的后, 服务器会将找到的 IP 地址传回给电脑, 并同时把它建立在 IP 数据库里面, 以提供下次能更快速搜寻使用。

5.3.2 分配 DNS 地址

多个 DNS 地址是用来防止当某个 DNS 服务器停止动作或超过负荷时, 可以提供替代的用。ISP 一般提供第一 (主要) 和第二 (次要) 个 DNS 地址, 也有可能提供更多地址。您所上网用的电脑, 可经由下面的任一方式来获得 DNS 地址:

- 静态 (固定): 若您的 ISP 提供 DNS 服务器的地址, 您只需要在电脑的 IP 设置中填上即可使用。
- 从 DHCP 服务器中采动态 (浮动) 的方式获得: 您可以在 SL1200 的 DHCP 服务器中设置 DNS 地址, 允许 DHCP 服务器分配 DNS 地址给电脑使用。请参考 5.2.3 节 "设置 DHCP 服务器", 来了解如何设置 DHCP 服务器。

您可以分配 ISP 的 DNS 服务器的物理地址 (在电脑主机上或在 DHCP 服务器的设置画面中), 或者您也可以分配 SL1200 的网络端口的地址 (192.168.1.1)。当您分配网络端口的 IP 地址后, 这个设备就有 DNS relay (中继) 的功能, 关于这项功能, 请参考下一节的介绍。



注意: 若您在电脑或 DHCP 设置中, 分配了物理的 DNS 地址, 则 DNS Relay (中继) 功能没有启用。

5.3.3 设置 DNS 中继 (Relay)

当指定局域网路由器的网络端口的 IP 地址为 DNS 地址后，路由器将会自动地具备 DNS relay (中继) 功能。也就是说，该设备本身不是 DNS 服务器，它只是把网域名称查询的请求从局域网中的电脑传送到 ISP 的 DNS 服务器上，以获得反向的数据后，再把这些数据转给电脑。

当具备 DNS 中继功能时，SL1200 必须保留 DNS 服务器的 IP 地址，它可以从以下两种方式获得地址：

- 从 PPPoE 或动态 IP 连接中获得：若 SL1200 使用 PPPoE (请参考 6.2.2 设置广域网 PPPoE) 或是动态 IP (请参考 5.2.4 设置广域网动态 IP 地址) 连接到 ISP，主要和次要 DNS 地址可以通过 PPPoE 连接来获得。选择这种方式，最大的好处就是当 ISP 更改它们的 DNS 地址时，您可以不用再重新设置电脑这端或 SL1200 的设置。
- 在路由器上设置：您也可以 WAN 设置页面 (如图 6.1 WAN PPPoE 设置页面，图 6.2 WAN 动态 IP (DHCP 客户端) 设置页面，图 6.3 WAN 静态 IP 设置页面) 使用 ISP 的 DNS 地址。

如何设置 DNS 中继

1. 在 DHCP 设置画面的 DNS 服务器的 IP 地址栏中，输入局域网 IP 地址，如图 5.2 所示。
2. 电脑上的网络设置，使用 SL1200 路由器上的 DHCP 服务器所分配的 IP 地址，或者手动将网络上每一部电脑都输入 SL1200 的 IP 地址，作为它们的 DNS 服务器地址。



注意：在电脑重新启动的前，启用 DNS 中继前所分配给网络电脑的 DNS 地址，将会一直有效。当您把电脑的 DNS 地址变更成局域网 IP 地址时，DNS 中继才会生效。

而同样的，在 DNS 中继功能启用的后，您在 DHCP 设置或电脑上分配了一个 DNS 地址 (不同于网络 IP 地址)，接着这个地址会取代 DNS 中继的地址。

5.4 查看局域网统计值

您可以查看路由器的局域网流量的统计值。通常情况下，您不需要查看这个数据，但是当您与您的 ISP 诊断网络或 Internet 传输出现问题时，这个功能是对您很有帮助的。

要查看局域网 IP 统计值，请在 LAN 子菜单中选择 Statistics。图 5.3 所示即为局域网统计值页面。



图 5.3. 局域网统计值页面

在您开启本页面后，若要更新统计值，请点击 <Refresh>。

第六章 广域网 (WAN) 设置

本章节将会叙述如何对 SL1200 连接到您的 ISP 的广域网 (WAN) 界面进行相关的设置。在本节中，您将可以学习到如何为您的广域网 (WAN) 环境设置 IP 地址、DHCP 服务器，与 DNS 服务器。

6.1 WAN 连接模式

本路由器支持三种 WAN 连接模式，分别是 PPPoE，静态 IP 与动态 IP 地址，可依照您 ISP 的连接方式，如图 6.1 所示在网络设置页面中的下拉式菜单，选择对应的连接模式。



图 6.1. WAN PPPoE 设置页面

6.2 PPPoE

6.2.1 WAN PPPoE 设置参数

表 6.1 为 PPPoE 连接模式中用到的设置参数。

表 6.1. WAN PPPoE 设置参数

栏位	说明
Host Name	主机名是选填的，但有些 ISP 可能需要此信息。
User Name and Password	输入用户名称与密码，以登录您的 ISP。这与登录到设置管理界面所用到的信息是不同的。
Primary/ Secondary DNS	主要/次要 DNS 服务器 IP 地址是选填的，因为 PPPoE 会自动侦测由您的 ISP 设置的 DNS IP 地址。但是，若您希望使用其他的 DNS 服务器，请在相应位置输入它的 IP 地址。
Connection Options	此选项的默认设置为“Disable”。若需要的话，您也可以选择 Dial-On-Demand 或 Keep-Alive。Dial-On-Demand 可设置当没有网络流量多少时间后，您希望断开网络连接。此一非活动时间最小的设置值为 30 分钟。RIP 与 SNTP 服务动作可能会影响该功能。请确保系统日期与时间的更新间隔设置（11.4 设置日期与时间）大于此非活动时间的值。
Keep Alive	若您想要在没有网络流量的时候仍保持 Internet 连接，请开启此选项。在“Echo Interval”位置输入您希望路由器周期性传送数据至 ISP 的时间间隔的值。“Echo Interval”的默认值为 60 秒。

6.2.2 WAN PPPoE 设置

如何设置 PPPoE

1. 从连接模式下拉式菜单中选择 PPPoE，如图 6.1 所示。
2. (选填) 如果 ISP 需要，请输入主机名。
3. 若您正在使用 PPPoE 进行 Internet 连接，您可能只需要在图 6.1 所示的 PPPoE 设置页面中输入用户名称和密码，除非您想使用特定的一个 DNS 服务器。
4. (选填) 若您想用特定的 DNS 服务器，您可以输入主要/次要 DNS 服务器 IP 地址，否则，请跳过这一步骤。
5. 如果需要，选择一个连接选项，并输入相应的设置。默认的设置 of “Disable”。
6. 完成设置后，点击 <Apply> 保存 PPPoE 设置。您可以在设置页面的下方看到 WAN 设置的概要。默认网关地址不会立刻显示。点击 WAN 菜单可再次开启 WAN 设置页面。

6.3 动态 IP

6.3.1 WAN 动态 IP 设置参数

表 6.2 描述了动态 IP 连接模式中的设置参数。

表 6.2. WAN 动态 IP 设置参数

栏位	说明
Host Name	主机名是选填的，但有些 ISP 可能需要此信息。
Primary/ Secondary DNS	主要/次要 DNS 服务器 IP 地址是选填的，因为 DHCP 客户端会自动获得由您的 ISP 设置的 DNS IP 地址。但是，若您希望使用其他的 DNS 服务器，请在相应位置输入它的 IP 地址。
MAC Cloning	默认值是使用 WAN 端口的 MAC 地址。但是，若您已经在您的 ISP 处注册了一个 MAC 地址，您可能需要在这里输入该 MAC 地址。

6.3.2 设置 WAN 动态 IP

如何设置动态 IP

1. 从连接模式下拉式菜单中选择 **Dynamic**，如图 6.2 所示。
2. (选填) 如果 ISP 需要，请输入主机名。
3. (选填) 若您想用特定的 DNS 服务器，您可以输入主要/次要 DNS 服务器 IP 地址，否则，请跳过这一步骤。
4. 若您的前已经在 ISP 处注册了一个 MAC 地址用于访问 Internet，输入已注册的 MAC 地址，并确认您勾选了 **MAC cloning** 复选框。
5. 设置完成后，点击 **<Apply>** 保存动态 IP 设置。您可以在设置页面的下方看到 WAN 设置的概要。默认网关地址不会立刻显示。点击 **WAN** 菜单可再次开启 WAN 设置页面。

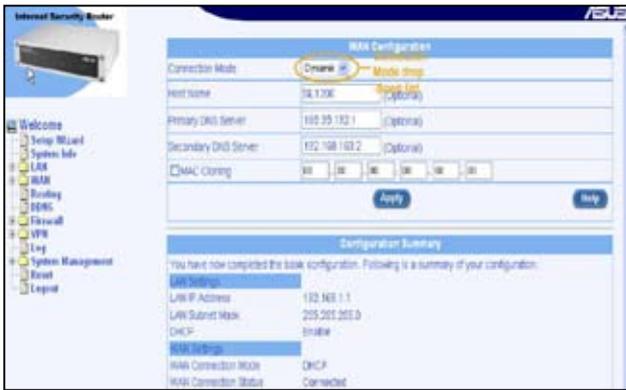


图 6.2. WAN 动态 IP (DHCP 客户端) 设置页面

6.4 静态 IP

6.4.1 WAN 静态 IP 设置参数

表 6.3 描述了静态 IP 连接模式中的设置参数。

表 6.3. WAN 静态 IP 设置参数

栏位	说明
IP Address	由 ISP 提供的 WAN IP 地址。
Subnet Mask	由 ISP 提供的 WAN 子网掩码。通常情况下，为 255.255.255.0。
Gateway Address	由 ISP 提供的网关 IP 地址。这一地址必须与路由器 WAN 端口的 IP 地址位于同一子网下。
Primary/ Secondary DNS	您至少需要输入主要 DNS 服务器的 IP 地址，次要 DNS 服务器的 IP 地址是选填的。

6.4.2 设置 WAN 静态 IP



图 6.3. WAN 静态 IP 设置页面

如何设置静态 IP

1. 从连接模式下拉式菜单中选择 **Static**，如图 6.3 所示。
2. 在 IP 地址栏位输入 WAN IP 地址。此一信息由您的 ISP 提供。
3. 输入 WAN 子网掩码。此一信息由您的 ISP 提供，通常情况下，为 255.255.255.0。
4. 在相应地址输入由您的 ISP 提供的网关 IP 地址。
5. 输入主要 DNS 服务器的 IP 地址。此一信息由您的 ISP 提供。次要 DNS 服务器是选填的。
6. 点击 <Apply> 保存静态 IP 设置。您可以在设置页面的下方看到 WAN 设置的概要。

6.5 查看 WAN 统计值

您可以查看您的 WAN 网络流量的统计值。通常情况下，您不需要查看这个数据，但是当您与您的 ISP 诊断网络或 Internet 传输出现问题时，这个功能是对您很有帮助的。

要查看 WAN IP 统计值，请在 WAN 子菜单中选择 **Statistics**。图 5.3 所示即为局域网统计值页面。图 6.4 显示的即为 WAN 统计值页面。

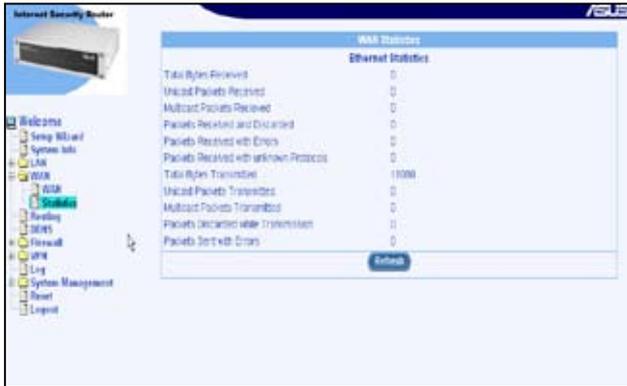


图 6.4. WAN 统计值页面

若您已开启此页面，只需点击 <Refresh> 即可查看更新后的统计值。

第七章 设置路由器

您可以使用设置管理界面来为您的 Internet 与局域网数据通信定义特定的路由。本章节将描述基本的路由概念并指导您如何新增路由。

7.1 IP 路由概述

对于路由器来说的一大挑战是：当路由器接受到需送至一特定目的地的数据时，它需要将这份数据送至哪一个设备？当您定义 IP 路由，您便需要提供这些相关规则来让 SL1200 可以用来做出传输数据到何处的决定。

7.1.1 我需要定义静态路由吗？

大多数用户都不需要设置 IP 路由。在一个典型的小型办公室或家庭网络中，既存的路由为您的局域网电脑和路由器建立起了默认网关，为您网络中 Internet 流量提供最适当的路由。

- 在您局域网中的电脑，一组默认的网关会将所有 Internet 传输的数据传送到 SL1200 的局域网端口。而由于您在 TCP/IP 内容所分配的地址，或是您设置局域网的电脑使其连接到 Internet 时动态地自一服务器获得，因此您局域网中的电脑可以查知默认的网关地址。详细内容请参考 3.2 第二部分 -- 设置您的电脑。
- 在 SL1200 本身，一组默认的网关被定义用来导引所有传出的 Internet 传输到您的 ISP 的路由器。当设备开始与 Internet 连接进行传输时，此一默认的网关会由您的 ISP 自动分配。关于新增默认路由的步骤在 7.3.2 新增静态路由 一节中有进一步的介绍。

若您的家用设置包含有两组或更多的网络或子网、连接到两个或以上的 ISP 服务，或是连接到一远程办公室的局域网，则您需要定义静态路由。

7.2 RIP 动态路由

RIP (Routing Information Protocol, 路由信息协议) 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。注意：若您想要与其他路由器交换路由信息，您必须首先在 System Management->System Services 设置页面中启动 RIP 的功能。

7.2.1 动态路由 (RIP) 设置参数

表 7.1 描述了动态路由设置参数。

表 7.1. 动态路由 (RIP) 设置参数

栏位	说明
Interface	选择一个路由信息交换的连接方式，您可以设置全部或部分界面支持路由信息交换
RIP	点击 Enable 或 Disable 按钮来开启或关闭”RIP”功能。请注意，您必须先启用 System Management->System Services 设置页面中的 RIP 服务。默认的设置 为 Enable。
Passive Mode	若要将 RIP 设置成只能接收其他路由器所发送的信息，而不能发送信息的话，请设置启用这个模式。 若您希望 RIP 模式既能够接收又能够发送信息给其他路由器的话，请关闭 (Disable) 这个模式。
RIP Version (Send)	选择发送路由信息的 RIP 版本，有三个版本可供您选择：Version 1、Version 2，和 Both。默认设置为 Version 2。
RIP Version (Receive)	选择接收路由信息的 RIP 版本，有三个版本可供您选择：Version 1、Version 2，和 Both。默认设置为 Both。

栏位	说明
Authentication	点击 Enable 或 Disable 按钮来开启或关闭信息交换的验证功能。请注意，所有的路由器交换信息时，必须使用相同的验证密码。默认设置为 Disable。
RIP Authentication Mode	从下拉式菜单中，选择 RIP 的验证模式。支持 Clear Text 和 MD5 两种模式。默认设置为 Clear Text。
Authentication Key	输入路由器交换信息时，所共同使用的验证密码。默认验证密码为 admin。

7.2.2 设置 RIP

设置 RIP

1. 点击 Routing 菜单以开启路由设置页面。
2. 在 RIP 设置页面中，点击 Enable 或 Disable 按钮，来开启或关闭 RIP 功能。若您已经完成这一动作，请跳过这一步骤。



图 7.1. RIP 设置

3. 在下拉式菜单列表中，选择路由与交换的连接界面。
4. 点击 Enable 或 Disable 按钮来开启或关闭指定界面的 RIP 功能。
5. 点击 Enable 或 Disable 按钮，来决定是否启用被动模式。
6. 接着从下拉式菜单中选择发送与接收路由信息的 RIP 版本。
7. 点击 Enable 或 Disable 按钮，来决定是否要启用验证功能。若启用了验证功能，接着就必须选择其中一种验证模式，并填入验证密码。

8. 若您想要设置另一个界面使其支持路由信息交换，请重复步骤 1 - 5。
9. 点击 <Apply> 保存 RIP 设置。

7.3 静态路由

7.3.1 静态路由设置参数

表 7.2 描述了静态路由的设置参数。

表 7.2. 静态路由设置参数

栏位	说明
Destination IP Address	分配目的地电脑或整个目的地网络的 IP 地址。该设置可以都设置为 0 来代表此路由可用于所有未经定义的地址。(这便是建立为默认网关的路由)。请注意！目的地 IP 必需为一网络 ID。默认路由采用 0.0.0.0 的目的地 IP 地址，请参考 13.1 IP 地址部分的解释。
Destination Netmask	表明目的地地址中的哪部分指网络，哪部分指网络中的电脑默认路由使用的网络掩码为 0.0.0.0。请参考 13.3 子网掩码部分的解释。
Gateway IP Address	网关 IP 地址。

7.3.2 新增一个静态路由

如何新增一个静态路由至路由表

1. 点击 Routing 菜单以开启路由设置页面。
2. 在相应栏位输入静态路由信息，如目的地 IP 地址，目的地网络掩码与网关 IP 地址。
这些栏位的说明，请参考表 7.2. 静态路由设置参数。
如要为您的局域网建立默认网关的路由，请在 Destination IP Address 与 Destination Netmask 栏位都输入 0.0.0.0。
3. 点击 <Add> 新增此路由。



图 7.2. 静态路由设置

7.3.3 删除一个静态路由

如何从路由表中删除一个静态路由

1. 在如图 7.2 所示的静态路由设置页面中，从下拉式菜单中选择路由，或在路由表中点击想要删除的路由图标。
2. 点击 <Delete> 删除所选路由。



通常情况下，请不要删除默认网关的路由。删除默认路由将导致无法访问 Internet。

7.3.4 查看路由表

所有开启 IP 功能的电脑与路由器都保存有一份被其用户共同使用的 IP 地址表。对于每一个目的地 IP 地址，此表会列出传输数据要经过的第一个跳跃点 (hop)，此表便被称作设备的路由表。

为了查看 SL1200 的路由表，请点击 Route 菜单以开启路由设置页面。接着路由表将会如图 7.3 所示，被显示在静态路由设置页面的下方。

Routing Table			
Destination Subnet Address	Destination Netmask	Default Gateway	Active Interface
192.168.1.0	255.255.255.0	0.0.0.0	* eth1

图 7.3. 路由表

路由表会以列显示的方式显示每一个包含目的地网络 IP 地址、目的地网络子网掩码，与转发传输数据的网关 IP 地址。

第八章 设置 DDNS

动态 DNS 是一种可让不同的电脑在 IP 地址不断变动的状况下（当重新启动电脑或当 ISP 的 DHCP 服务器重新配发 IP）使用相同网域名称的服务。当 WAN IP 地址变更时，SL1200 便会连接到一动态 DNS 服务提供者。本功能可以设置使用网域名称而非 IP 地址的 WEB、FTP 服务器等网络服务。此外，动态 DNS 也支持 DDNS 客户端以下功能：

- 更新 DNS 记录(额外的)
- 强制 DNS 更新

HTTP 动态 DNS 客户端

HTTP DDNS 客户端使用 DNS 服务提供者所提供的结构来动态升级 DNS 记录。在此状况下，服务提供者会更新 DNS 中的 DNS 记录。SL1200 使用 HTTP 来启动更新作业。

SL1200 支持以下列的服务提供者进行 HTTP DDNS 更新。

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

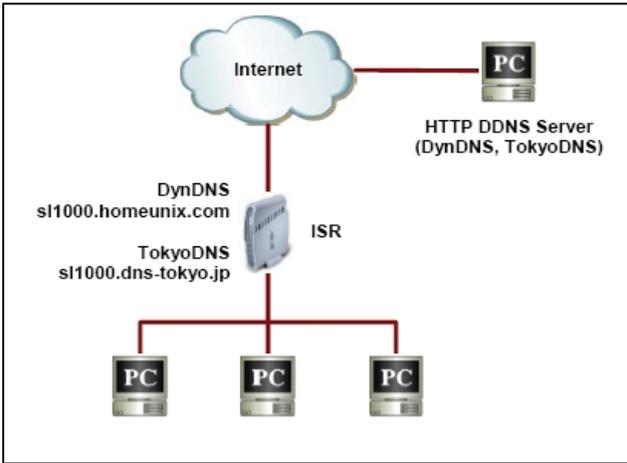


图 8.1. HTTP DDNS 网络图

每当 DDNS 界面的 IP 地址变更，则 DDNS 更新会传送到指定的 DDNS 服务提供者。SL1200 应使用由您 DDNS 服务提供者处所获得的 DDNS 用户名与密码进行设置。

8.1 DDNS 设置参数

表 8.1 描述了 DDNS 服务参数。

表 8.1. DDNS 设置参数

栏位	说明
DDNS State (DDNS 状态)	
Enable	点击此按钮以开启 DDNS 服务。
Disable	点击此按钮以关闭 DDNS 服务。
DDNS Type - 选择 DDNS 服务类型：HTTP 或 RFC-2136 DDNS	
HTTP DDNS	若您需要 HTTP DDNS，请点击此按钮。
DNS Zone Name(DNS 网域名称)	
请将由您的 ISP 所提供的已注册的网域名称填入此栏位。路由器的主机名必须已在系统信息页面中设置好。举例来说，若您的 SL1200 的主机名称是“host1”，DNS 网域名称是“yourdomain.com”，则具备完整资格的网域名称 (FQDN) 便是“host1.yourdomain.com”。	
HTTP DDNS 特别设置	
DDNS Service [仅用于 HTTP DDNS]	
dyndns	详情请参考 http://www.dyndns.org 。
zoneedit	详情请参考 http://www.zoneedit.com 。
dyn-tokyo	详情请参考 http://www.dns-tokyo.jp 。
DDNS User name [仅用于 HTTP DDNS]	
在此栏位输入由您的 DDNS 服务提供商所提供的用户名称。	
DDNS Password [仅用于 HTTP DDNS]	
在此栏位输入由您的 DDNS 服务提供商所提供的密码。	

8.2 访问 DDNS 设置页面

以管理员身份登录设置管理界面，接着点击 DDNS 菜单。此时将出现 DDNS 设置页面，如图 8.2 所示。当您开启 DDNS 设置页面时，已存在的 DDNS 设置会列在设置页面的下方，如图 8.2 所示。

8.3 设置 HTTP DDNS 客户端



图 8.2. HTTP DDNS 设置页面

如何设置 HTTP DDNS

1. 首先，您应已至 DDNS 服务提供者处注册网域名称。若您还未进行注册，请造访 <http://www.dns-tokyo.jp> 或 <http://www.dyndns.org> 以获得更多相关信息。
2. 确认您为路由器设置了主机名 (host)。否则，请至 System Management -> System Identity 进行设置。
3. 开启 DDNS 设置页面。请参考 8.2 访问 DDNS 设置页面。
4. 在 DDNS 设置页面中，将 DDNS State 设置为 Enable，DDNS type 设置为 HTTP DDNS。此时将出现 HTTP DDNS 设置，如图 8.2 所示。
5. 在 DNS Zone Name (网域名称) 栏位输入您所注册的网域名称。
6. 从 DDNS 服务下拉式菜单中选择一个 DDNS 服务。
7. 输入由您的 DDNS 服务提供者所提供的用户名与密码。
8. 点击 <Apply> 键来传送 DNS 更新需求到您的 DDNS 服务提供者。当 WAN 端口状态有更新时，DNS 更新请求会自动传送至您的 DDNS 服务提供者处。

第九章 防火墙 /NAT 设置

SL1200 提供内建防火墙/ NAT 的功能，这项功能可以让您分享Internet连接的同时，也保护您局域网内的电脑免于遭受阻绝服务（DoS）攻击与其他类型来自Internet的恶意访问动作。此外，您也可以指定如何监控这些攻击行为，并设置当这些攻击发生时报告网络地址。

本章节将叙述如何设置网络路由的安装设置与建立/修改/删除 ACL（Access Control List）规则，来控制通过您网络环境的数据。您将会使用防火墙设置页面进行：

- 建立、修改、删除与查看传入/传出 ACL规则。
- 建立、修改、删除在传入/传出 ACL 设置中用到的预定义的服务，IP 地址池，NAT 池，应用程序过滤及时间范围。
- 查看防火墙状态。



当你定义一个 ACL 规则，便是指示 SL1200 查看每一个它所接收的数据封包并决定该封包是否符合继续向前传送的标准。这项标准可以包括网络或 Internet 协议，包括传送封包的电脑 IP 地址、目的地的 IP 地址、与其他封包数据的特性（举例来说，由局域网至 Internet，或反之亦然）。

若是该封包符合已建立规则的标准，则封包便可被接受（继续向前传送至目的地），或是遭到拒绝（放弃），而这些决定要视您所建立的规则而定。

9.1 防火墙概述

9.1.1 状态封包检测

在 SL1200 中的状态封包检测引擎存有一状态列表，而这份列表是被追踪所有通过防火墙的封包的连接状态。若封包属于符合状态封包检测引擎中规则的类型，则防火墙会开启一个“通道”来让该封包通过；否则，该封包便会被丢弃。而当该通过封包的连接中止这个“通道”便会被关闭。您无需对状态封包检测进行任何设置，因为这项功能是在防火墙功能启动时便默认为启动的。请参阅 11.1 系统服务设置 一节中的介绍来开启或关闭 SL1200 的防火墙服务。

9.1.2 DoS 攻击防范

DoS 攻击防范与状态封包检测皆提供您网络环境的第一线防护。当 SL1200 的防火墙功能被启动后，您无需设置即可开启上述两项服务。而在默认值中，防火墙功能是被设置为开启的。请参阅 11.1 系统服务设置 一节中的介绍来开启或关闭 SL1200 的防火墙服务。

9.1.3 防火墙与访问控制列表 (ACL)

9.1.3.1 ACL 规则的优先顺序

所有的 ACL 规则都有被指定的规则 ID — 较低的规则 ID，拥有较高优先顺序。防火墙会以解读封包包头信息的方式来监控网络传输，接着，这些包头信息会被检查是否符合 ACL 规则列表中的规则，来决定该封包是被放行继续前往目的地，或是被丢弃。ACL 规则检查从具有最小 ID 的规则开始，直到找到一个符合的规则，或全部规则检查完毕。若没有符合任何规则，则这个封包将被丢弃。否则，将根据符合的 ACL 规则中的动作定义来决定放行或丢弃该封包。

9.1.3.2 连接状态追踪

在防火墙中的状态封包检测引擎，会保持追踪网络连接的状态与进展。通过在状态列表中关于每一连接的保存信息，SL1200 可以很快地决定封包是否由一已建立的连接通过。若结果是肯定的，则封包便可以在无需经过 ACL 规则的状态下通过防火墙。

举例来说，一个 ACL 规则可以允许自 192.168.1.1 至 192.168.2.1 的 ICMP 封包通过。当 192.168.1.1 传送一个 ICMP echo (如 ping 封包) 至 192.168.2.1，则 192.168.2.1 将回应一个 ICMP echo 至 192.168.1.1。在 SL1200 中，您无需另外建立另一个传入规则，因为状态封包检测引擎追踪记住连接状态，并允许 ICMP echo 可以通过防火墙回复。

9.1.4 默认的 ACL 规则

SL1200 支持 3 种类型的默认访问规则：

- Inbound Access Rules (传入访问规则) :用来控制外部对您的局域网中电脑的访问。
- Outbound Access Rules (传出访问规则) : 用来控制您的局域网主机对外部网络的访问。
- Self Access Rules (自我访问规则) : 作为控制 SL1200 自身访问动作的用途。

默认的传入访问规则

没有设置默认的传入访问规则。所有来自外部主机来访问局域网的流量都会被阻止。

默认的传出访问规则

默认的传出访问规则可允许由您局域网中电脑通过 NAT 访问外部网络的所有流量。



您无需自 ACL 规则列表中移除默认的 ACL 规则！建议设置更高优先权的 ACL 规则来取代默认的规则。

9.2 NAT 概述

网络地址转译允许使用单一设备，例如 SL1200，担任Internet（对外网络）与本地网络（专用网络）的代理。这也就是说 NAT 的 IP 地址可以对外部网络代表内部局域网一整个群组的电脑。网络地址转译（NAT）可以节省广大网络环境下已注册的 IP 地址使用，并可以简化 IP 地址的管理工作。由于 IP 地址的转译，NAT 也可以隐蔽网络地址并对局域网提供某种程度的安全保障。

本路由器可支持的 NAT 模式有：静态 NAT, 动态 NAT, NAPT, 反向静态 NAT, 与反向 NAPT。

9.2.1 静态（一对一）NAT

静态 NAT 将一个内部的主机地址映射至一个全球有效的 Internet 地址（一对一映射）。在映射中，所有的封包都直接被转译为全球有效的 Internet 地址。图 9.1 所示为四个专有网络地址与四个全球有效的 Internet IP 地址的间的映射关系。



这个映射是静态的。这个映射不会随时间而变化，直到此映射被管理员手动修改。这意味着主机传出的流量将一直使用同一个 IP 地址。

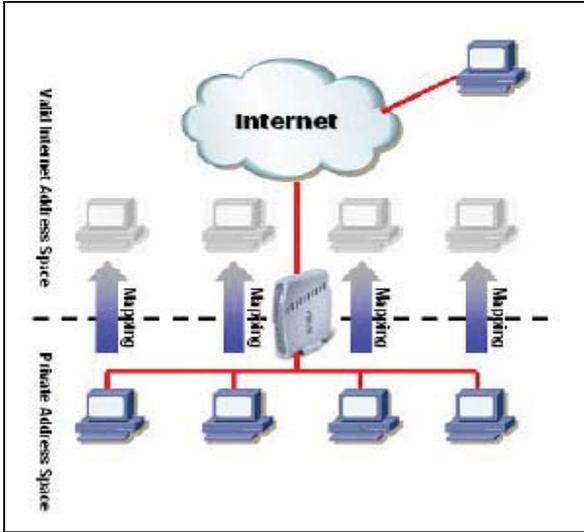


图 9.1 静态 NAT - 将四个私有网络 IP 地址映射至四个全球有效的 IP 地址

9.2.2 动态 NAT

将一个内部主机地址动态映射至全球有效的 Internet 地址(m 对 n 映射)。此映射通常包含一个内部 IP 地址池(m)与一个合法的 Internet IP 地址池(n), m 的数值一般都大于 n。每一个内部 IP 地址将被映射至一个外部 IP 地址, 采取先到先服务的机制。图 9.2 所示为 PC B, C 与 D 被分别映射至一个全球有效的 IP 地址, 而 PC A 没有映射至任何全球有效的 IP 地址。若 PC A 想要访问 Internet, PC A 必须等到有一个全球有效的 IP 地址不被占用。如, 图 9.3 中, PC B 必须先从 Internet 断开, PC A 才可以访问 Internet。

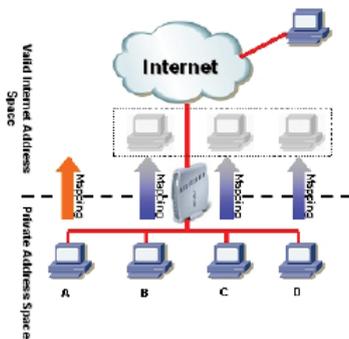


图 9.2 动态 NAT - 四个专有 IP 地址映射至三个全球有效的 IP 地址

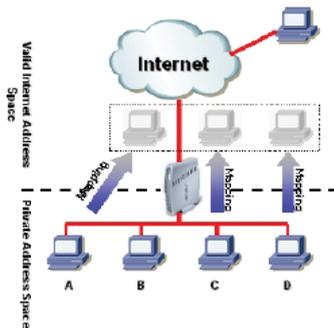


图 9.3 动态 NAT - 在 PC-B 断开连接后, PC-A 才能获得 NAT 连接

9.2.3 NAPT(Network Address and Port Translation) 或 PAT(Port Address Translation)

NAPT 也称作 IP 伪装，这项功能可以将许多内部主机对应到一个有效的对外 Internet 地址。这项映射包含有一组用来转译的网络端口。每一个封包都会通过这个有效的对外网络地址来传送，而端口的号码也被一组网络端口中未使用的端口加以转译。图 9.4 显示所有本地网络的主机通过对应到一个全球通用 IP 地址的方式来连接 Internet，而端口号码与自由的网络端口不同。

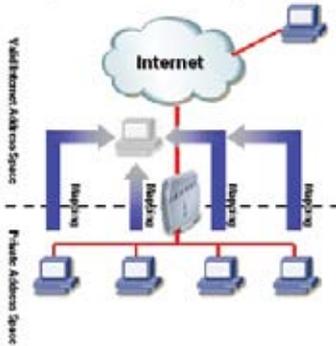


图 9.4 NAPT - 将所有的内部网络 PC 映射至同一个全球有效的 IP 地址

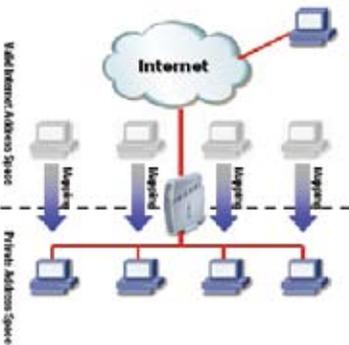


图 9.5 反向静态 NAT - 将一个全球有效的 IP 地址映射至一台内部网络电脑

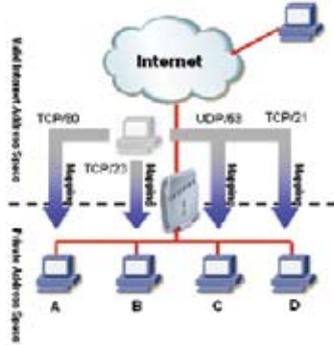


图 9.6 反向 NAPT - 根据协议、端口号或 IP 地址中继传入的封包至内部主机

9.2.4 反向静态 NAT

反向静态 NAT 将一个全球有效的 Internet IP 地址映射至一个内部主机地址。所有传输至此外部 IP 地址的封包都会被传输至这个内部主机地址。当服务是由同一台主机主导时，这项功能是非常有用的。图 9.5 所示为四个全球有效的 IP 地址被映射至四台内部网络中的主机，每一台主机都可用来主导传入的流量，如 FTP 服务器。

9.2.5 反向 NAPT / 虚拟服务器

反向 NAPT 也被称作传入映射，端口映射，或是虚拟服务器。任何来到 SL1200 的封包，都会依照协议、端口号码或 IP 地址，或依照特定的 ACL 规则被加以分配。当多重服务是由不同的内部主机所负责时，这项功能是相当有用的。图 9.6 显示网页服务器 (TCP/80) 是由 PC A 所负责、telnet 服务 (TCP/23) 为 PC B 所负责、DNS 服务器 (UDP 53) 为 PC C 负责，而 FTP 服务器 (TCP/21) 则为 PC D 负责。这也就是说，这四种服务的传入传输将会被导向对应这些服务的主机。

9.3 设置传入 ACL 规则

通过在 Inbound ACL configuration (传入 ACL 设置) 页面建立 ACL 规则，如图 9.7 所示，您可以控制 (允许或阻止) 外部对您局域网中电脑的攻击。

这个设置页面的选项可让您：

- 新增一条规则，并设置该项规则的参数
- 修改已存在的规则
- 删除已存在的规则
- 查看已设置的 ACL 规则

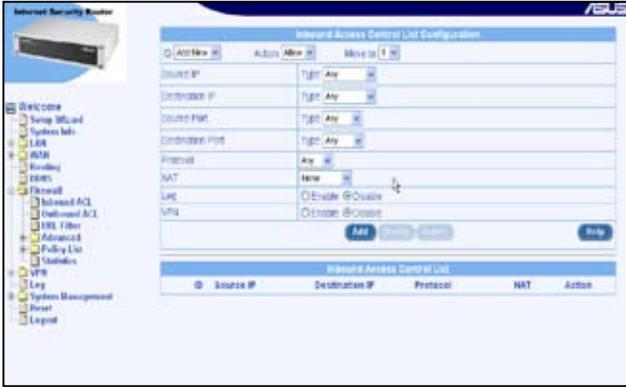


图 9.7. 传入 ACL 设置页面

9.3.1 传入 ACL 规则设置参数

表 9.1 描述了防火墙传入 ACL 规则的设置参数。

表 9.1. 传入 ACL 规则设置参数

栏位	说明
ID	
Add New	点击本选项来新增 ACL 规则。
Rule Number	从下拉式菜单中选择一个规则，并修改它的设置。
Action	
Allow	点击本按钮来设置此规则为允许规则。当本规则与防火墙结合可让符合此规则的封包通过防火墙。
Deny	点击本按钮来设置此规则为阻止规则。当本规则与防火墙结合便不会让符合此规则的封包通过防火墙。
Move to	此选项允许您设置本规则的优先等级。SL1200 防火墙根据规则的优先顺序来决定是否让封包通过。您可以指定规则列表中一个特定数字，来决定规则的优先顺序。选项包括：
1 (First)	本数字代表最高优先的等级。
Other numbers	选择一个数字来指定您希望分配给规则的优先顺序。

栏位	说明
Source IP 本项目可让您设置套用此规则的来源网络。请使用下拉式菜单来选择下列选项：	
Any	本项目可以让您套用这项规则到来源网络中的所有电脑，就像那些做为传入传输的 Internet 电脑或是所有做为传出传输的本地端网络电脑。
IP Address	本项目可以让您分配一组 IP 地址，在这组 IP 地址上套用该规则。
IP Address	分配合适的 IP 地址
Subnet	本项目可让您包括所有连接到 IP 子网的电脑。当本选项被选择，则下列栏位将会变成可以填入数值。
Address	输入合适的 IP 地址。
Mask	输入对应的子网掩码。
Range	本选项可让您选择套用此规则的 IP 地址范围。当此项被选择时，下面的两个项目将变为可设置：
Begin	输入此范围的起始 IP 地址
End	输入此范围的结束 IP 地址
IP Pool	本选项可让您将预先设置的 IP 地址池与此规则相关联。可用的 IP 地址池可以从下拉式菜单中选择。
Destination IP 本项目可以让您设置套用该项规则的目地网络。请使用下拉式菜单来选择下列项目：	
Any	本项目可以让您套用该规则到所有的本地端电脑。
IP Address, Subnet, Range and IP Pool	选择这些项目并如上面的 Source IP 部分所叙述地一样输入相关细节。
Source Port 本项目可以让您设置套用该规则的来源端口。请使用下拉式菜单来从下列选项选择一项您想选择的设置值：	
Any	若您想将本规则套用到具有任意来源端口号码的所有应用程序，请选择本项目。

栏位	说明
Single	若您想将本规则套用到具有特定端口号码的一个应用程序，则请选择本项目。
Port Number	输入来源端口号码
Range	如果你想要这个规则套用到符合此端口范围的应用程序，请选择本项目。而选择本项目后，下列栏位便可以输入设置数值。
Begin	输入端口范围开始的号码
End	输入端口范围结束的号码
Destination Port 本项目可以让您设置套用该规则的目的地端口。请使用下拉式菜单来从下列选项选择一项您想选择的设置值：	
Any	若您想将本规则套用到具有任意来源端口号码的所有应用程序，请选择本项目。
Single, Range	选择其中某个项目并如上面的 Source Port 部分所叙述地一样输入相关细节。
Service	本选项可让您从下拉式菜单中选择预先设置的服务。以下是一些服务的例子： 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：服务是协议与端口号的组合。当您在 防火墙 服务 设置页面将它们加入后，您将可以看到这些服务。
Protocol 本选项可让您从下拉式菜单中选择协议类型。可选的设置有：All, TCP, UDP, ICMP, AH 与 ESP。若您在 Destination port 栏位选择“service”，本选项将不能设置。	

栏位	说明
NAT	
本选项可让您为传入的网络流量选择 NAT 类型。	
None	若您不想在这个传入 ACL 规则中使用 NAT，请选择此选项。
IP Address	选择此选项指定传入的流量中继到网络中特定一台电脑的 IP 地址（通常为您局域网中的服务器）。这一选项被称为 反向 NAPT 或虚拟服务器。
NAT Pool	选择此项目来将一个预先设置的 NAT 地址池结合到规则中。只有反向静态 NAT 与反向 NAPT 地址池可与一个传入 ACL 规则相结合。
Time Ranges	
选择一个预先设置的时间范围，在这个时间范围内规则是有效的。选择 “Always” 使规则一直有效。	
Log	
选择 “Enable” 或 “Disable” 按钮来开启或关闭 ACL 规则的记录日志 (logging)。	
VPN	
若您想要让流量通过VPN，请点击 “Enable”。否则，请选择 “Disable”。	

9.3.2 访问传入 ACL 规则设置页面 - (Firewall -> Inbound ACL)

以管理员身份登录设置管理界面。点击 Firewall -> Inbound ACL。

防火墙传入 ACL 设置页面出现，如图 9.7 所示。

当您开启传入 ACL 设置页面时，已存在的 ACL 规则也会同时显示在设置页面的下方，如图 9.8 所示。



图 9.8. 传入 ACL 设置范例

9.3.3 新增传入 ACL 规则

如何新增传入 ACL 规则

1. 开启传入 ACL 规则设置页面。请参考 9.3.2 访问传入 ACL 规则设置页面。
2. 在 ID 下拉式菜单中选择 Add New。
3. 从 Action 下拉式菜单中选择所需要的动作（允许或阻止）。
4. 修改下面这些栏位：来源 / 目标 IP、来源 / 目标端口、协议、端口映射、时间范围，应用程序过滤与 VPN。关于这些栏位的解释请参考表 9.1。
5. 从“Move to”的下拉式菜单中选择号码来为这些规则指定优先顺序。请注意！这些号码便是代表优先顺序，其中以 1 的优先顺序最高。防火墙会先检查较高优先顺序的规则。
6. 点击 <Add> 键可以建立新的 ACL 规则。新的 ACL 规则稍后会显示在传入 ACL 设置页面中下方的传入 ACL 访问控制列表。

图 9.8 所示为如何新增规则以允许传入 HTTP（如网络服务器）服务。此规则可允许传入 HTTP 流量直接传至 IP 地址为 192.168.1.28 的主机。

9.3.4 修改传入 ACL 规则

如何修改传入 ACL 规则

1. 开启传入 ACL 规则设置页面。请参考 9.3.2 访问传入 ACL 规则设置页面。
2. 点击规则中的  图标来修改传入 ACL 列表，或从 "ID" 下拉式菜单选择规则编号。
3. 修改下面这些栏位:来源 / 目标 IP、来源 / 目标端口、协议、端口映射，时间范围，应用程序过滤与 VPN。关于这些栏位的解释请参考表 9.1。
4. 点击 <Modify> 键可以修改 ACL 规则。新的 ACL 规则稍后会显示在传入 ACL 设置页面中下方的传入 ACL 访问控制列表。

9.3.5 删除传入 ACL 规则

如何删除传入 ACL 规则

1. 开启传入 ACL 规则设置页面。请参考 9.3.2 访问传入 ACL 规则设置页面。
2. 点击规则中的  图标来修改传入 ACL 列表，或从 "ID" 下拉式菜单选择规则编号。
3. 点击 <Delete> 键删除 ACL 规则。被删除的 ACL 规则将会从传入 ACL 设置页面中下方的传入 ACL 访问控制列表中移除。

9.3.6 显示传入 ACL 规则

要查看已存在的传入 ACL 规则，请开启 Inbound ACL Rule Configuration 页面，如 9.3.2 访问 Inbound ACL Rule Configuration 页面。

9.4 设置传出 ACL 规则

通过在传出 ACL 规则设置页面新增 ACL 规则，如图 9.9 所示，您可以控制（允许或阻止）局域网中的电脑对 Internet 或外部网络的访问。

这个设置页面中的选项可让您：

- 新增一个规则，并为其设置参数
- 修改一个已存在的规则
- 删除一个已存在的规则
- 查看一个已设置的 ACL 规则

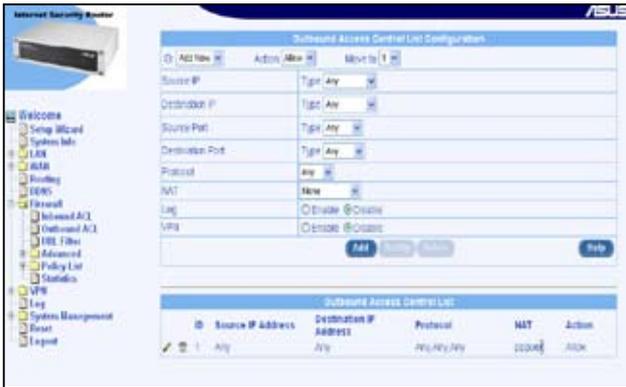


图 9.9. 传出 ACL 设置页面

9.4.1 传出 ACL 规则设置参数

表 9.2 描述了防火墙传出 ACL 规则的设置参数。

表 9.2. 传出 ACL 规则设置参数

栏位	说明
ID	
Add New	点击此选项以新增一个新的“基本”防火墙规则。
Rule Number	从下拉式菜单中选择一个规则并修改其内容。
Action	
Allow	点击本按键来设置此规则为允许规则。当本规则与防火墙结合可让符合此规则的封包通过防火墙。
Deny	点击本按键来设置此规则为阻止规则。当本规则与防火墙结合便不会让符合此规则的封包通过防火墙。
Move to	
此选项允许您设置本规则的优先等级。SL1200 防火墙根据规则的优先顺序来决定是否让封包通过。您可以指定规则列表中一个特定数字，来决定规则的优先顺序。选项包括：	
1 (First)	本数字代表最高优先的等级。
Other numbers	选择一个数字来指定您希望分配给规则的优先顺序。
Source IP	
本项目可让您设置套用此规则的来源网络。请使用下拉式菜单来选择下列选项：	
Any	本项目可以让您套用这项规则到局域网中的所有电脑
IP Address	本项目可以让您分配一组 IP 地址，在这组 IP 地址上套用该规则。
IP Address	分配合适的 IP 地址
Subnet	本项目可让您含括所有连接到 IP 子网的电脑。当本选项被选择，则下列栏位将会变成可以填入数值。
Address	输入合适的 IP 地址。
Mask	输入对应的子网掩码。

栏位	说明
Range	本选项可让您选择套用此规则的 IP 地址范围。当此项被选择时，下面的两个项目将变为可设置：
Begin	输入此范围的起始 IP 地址
End	输入此范围的结束 IP 地址
IP Pool	本选项可让您将预先设置的 IP 地址池与此规则相关联。可用的 IP 地址池可以从下拉式菜单中选择。
Destination IP	
本项目可让您设置套用该项规则的目的网络。请使用下拉式菜单来选择下列项目：	
Any	本项目可让您套用该规则到所有目的地网络中的电脑，如 Internet 中的电脑。
IP Address, Subnet, Range and IP Pool	选择这些项目并如上面的 Source IP 部分所叙述地一样输入相关细节。
Source Port	
本项目可让您设置套用该规则的来源端口。请使用下拉式菜单来从下列选项选择一项您想选择的设置值：	
Any	若您想将本规则套用到具有任意来源端口号码的所有应用程序，请选择本项目。
Single	若您想将本规则套用到具有特定端口号码的一个应用程序，则请选择本项目。
Port Number	输入来源端口号码
Range	如果你想要这个规则套用到符合此端口范围的应用程序，请选择本项目。而选择本项目后，下列栏位便可以输入设置数值。
Begin	输入端口范围开始的号码
End	输入端口范围结束的号码
Destination Port	
本项目可让您设置套用该规则的目的地端口。请使用下拉式菜单来从下列选项选择一项您想选择的设置值：	
Any	若您想将本规则套用到具有任意来源端口号码的所有应用程序，请选择本项目。
Single, Range	选择其中某个项目并如上面的 Source Port 部分所叙述地一样输入相关细节。

栏位	说明
Service	<p>本选项可让您从下拉式菜单中选择预先设置的服务。以下是一些服务的例子：</p> <p>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。</p> <p>注意：服务是协议与端口号的组合。当您在 防火墙服务 设置页面将它们加入后，您将可以看到这些服务。</p>
<p>Protocol</p> <p>本选项可让您从下拉式菜单中选择协议类型。可选的设置有：All, TCP, UDP, ICMP, AH 与 ESP。若您在 Destination port 栏位选择“service”，本选项将不能设置。</p>	
<p>NAT</p> <p>本选项可让您为传入的网络流量选择 NAT 类型。</p>	
None	<p>若您不想在这个传出 ACL 规则中使用 NAT，请选择此选项。</p>
IP Address	<p>选择此选项指定传出的流量所使用的 IP 地址（通常为您局域网中的服务器）。这一选项被称为反向 NAT 或 overload。</p>
NAT Pool	<p>选择此项目来将一个预先设置的 NAT 地址池结合到规则中。只有静态、动态与 overload 地址池可与一个传出 ACL 规则相结合。</p>
Interface	<p>选择此一项目来让传出流量使用 WAN 端口 IP 地址。若要选择此项目，您必须事先设置好 WAN IP。</p>
<p>Time Ranges</p> <p>选择一个预先设置的时间范围，在这个时间范围内规则是有效的。选择“Always”使规则一直有效。</p>	
<p>Log</p> <p>选择“Enable”或“Disable”按钮来开启或关闭 ACL 规则的记录日志 (logging)。</p>	
<p>VPN</p> <p>若您想要让流量通过 VPN，请点击“Enable”。否则，请选择“Disable”。</p>	

9.4.2 访问传出 ACL 规则设置页面 - (Firewall -> Outbound ACL)

以管理员身份登录设置管理界面。点击 Firewall -> Outbound ACL。防火墙传出 ACL 设置页面出现，如图 9.9 所示。

当您开启传出 ACL 设置页面时，已存在的 ACL 规则也会同时显示在设置页面的下方，如图 9.9 所示。

9.4.3 新增传出 ACL 规则

如何新增传出 ACL 规则

1. 开启传出 ACL 规则设置页面。请参考 9.4.2 访问传出 ACL 规则设置页面。
2. 在 ID 下拉式菜单中选择 Add New。
3. 从 Action 下拉式菜单中选择所需的动作（允许或阻止）。
4. 修改下面这些栏位：来源 / 目标 IP、来源 / 目标端口、协议、NAT、时间范围、应用程序过滤、日志与 VPN。关于这些栏位的解释请参考表 9.2。
5. 从“Move to”的下拉式菜单中选择号码来为这些规则指定优先顺序。请注意！这些号码便是代表优先顺序，其中以 1 的优先顺序最高。防火墙会先检查较高优先顺序的规则。
6. 点击 <Add> 键可以建立新的 ACL 规则。新的 ACL 规则稍后会显示在传出 ACL 设置页面中下方的传出 ACL 访问控制列表。

表 9.10 所示为如何新增规则以允许传出 HTTP 服务。此规则可允许您局域网中 IP 地址为 192.168.1.15 的主机的传出 HTTP 流量直接传至外部网络。

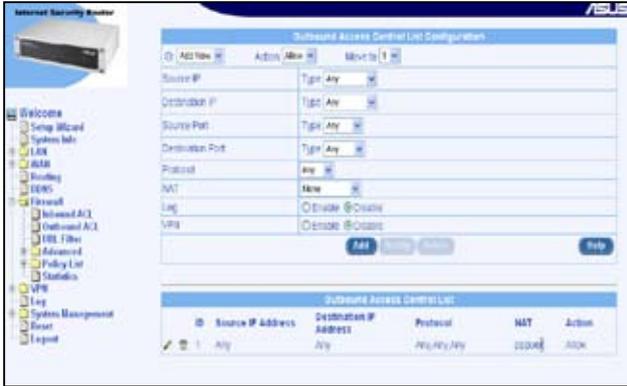


图 9.10. 传出 ACL 设置范例

9.4.4 修改传出 ACL 规则

如何修改传出 ACL 规则

1. 开启传出 ACL 规则设置页面。请参考 9.4.2 访问传出 ACL 规则设置页面。
2. 点击规则中的  图标来修改传出 ACL 列表，或从 "ID" 下拉式菜单选择规则编号。
3. 修改下面这些栏位：动作、来源 / 目标 IP、来源 / 目标端口、协议、NAT，时间范围，应用程序过滤、日志与 VPN。关于这些栏位的解释请参考表 9.2。
4. 点击 <Modify> 键可以修改 ACL 规则。新的 ACL 规则稍后会显示在传出 ACL 设置页面中下方的传出 ACL 访问控制列表。

9.4.5 删除传出 ACL 规则

如何删除传出 ACL 规则

1. 开启传出 ACL 规则设置页面。请参考 9.4.2 访问传出 ACL 规则设置页面。
2. 点击规则中的  图标来修改传出 ACL 列表，或从 "ID" 下拉式菜单选择规则编号。

3. 点击 <Delete> 键删除 ACL 规则。被删除的 ACL 规则将会从传出 ACL 设置页面中下方的传出 ACL 访问控制列表中移除。

9.4.6 显示传出 ACL 规则

要查看已存在的传出 ACL 规则，请开启传出 ACL 规则设置页面，如 9.4.2 访问传出 ACL 规则设置页面。

9.5 设置 URL 过滤

基于 URL（一致性资源定址器，俗称网址，如 www.yahoo.com）的关键词过滤可让您定义一组不允许在 URL 中出现的关键词。任何包含一个或多个这些被禁止关键词的 URL 将被封锁。这是一个独立于规则的功能，并没有与 ACL 规则相关联。此功能可以单独开启或关闭，但只有在防火墙开启的状况下才有效。

9.5.1 URL 过滤设置参数

表 9.3 描述了 URL 过滤规则中的设置参数。

表 9.3. URL 过滤设置参数

栏位	说明
URL Filter State	点击 “Enable” 或 “Disable” 按钮以开启或关闭 URL 过滤功能。
Proxy Server Port	输入您的网页浏览器的代理服务器（网络服务器）端口号码。此代理服务器端口号码更改后，您需要先关闭防火墙，然后再将其开启，以设置生效。
ID	
Add New	点击此选项以新增一个 URL 过滤规则。
Rule Number	从下拉式菜单中选择一个规则，以修改其内容。
Keyword	定义一个不允许出现在 URL 中的关键词。

9.5.2 访问 URL 过滤设置页面 - (Firewall -> URL Filter)

以管理员身份登录设置管理界面。点击 Firewall -> URL filter。防火墙 URL 过滤设置页面出现，如图 9.11 所示。

当您开启 URL 过滤设置页面时，已存在的 URL 过滤规则也会显示在设置页面的下方，如图 9.11 所示。



图 9.11. URL 过滤设置页面

9.5.3 新增 URL 过滤规则

如何新增 URL 过滤

1. 开启 URL 设置页面。请参考 9.5.2 访问 URL 过滤设置页面。
2. 在 ID 下拉式菜单中选择 Add New。
3. 在 Keyword 栏位输入关键词。
4. 点击 <Add> 以新增 URL 过滤规则。新的过滤规则将显示在 URL 过滤设置概要表中。

9.5.4 修改 URL 过滤规则

要修改一个 URL 设置规则，您必须首先删除一个已存在的 URL 过滤规则，然后再新增一个。(请参考 9.5.3 新增 URL 过滤规则)。

9.5.5 删除 URL 过滤规则

如何删除 URL 过滤规则

1. 开启 URL 设置页面。请参考 9.5.2 访问 URL 过滤设置页面。
2. 在 URL 过滤设置概要表中，点击您想要删除的规则的  图标，或在 ID 下拉式菜单中选择规则号码。
3. 点击 <Delete> 删除此规则。

9.5.6 查看已设置的 URL 过滤规则

要查看已存在的 URL 过滤规则，您只需依照 9.5.2 访问 URL 过滤设置页面的说明，开启 URL 过滤设置页面。

9.5.7 URL 过滤规则范例

图 9.12 所示为一个 URL 过滤规则的范例。它表明了：

- 如何新增关键词“abcnews”。任何包含此关键词的 URL 将被封锁。
- 将 web 代理服务器端口号码设为 80 (您也可以为您的代理服务器使用其他端口号码)。这表示若您使用 web 代理服务器，这一 URL 过滤规则将用于代理服务器端口 80。若您没有在浏览器中使用代理服务器，此设置将被忽略。您必须将防火墙关闭并重新开启才能使这项更改生效。请参考 11.1 系统服务设置 来了解开启与关闭防火墙的详细说明。

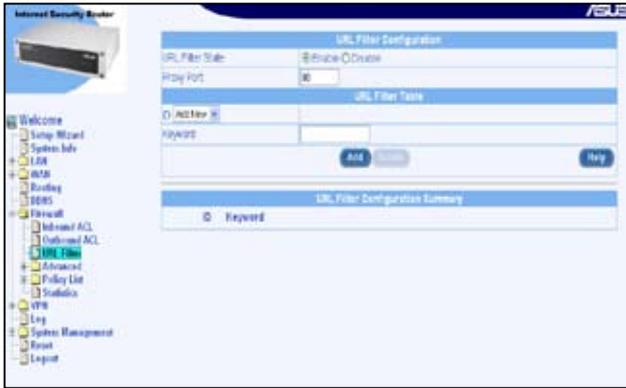


图 9.12. URL 过滤规则范例

9.6 设置高级防火墙功能 - (Firewall -> Advanced)

本选项组包括下面的子选项，用于进行高级防火墙设置：

- **Self Access:** 本选项可让您设置规则来控制目标为 SL1200 路由器本身的封包。
- **Services:** 使用本选项来了设置服务（采用特定端口号码的应用程序）。每个服务记录包含服务名称记录、IP 协议值与相应的端口号码。
- **Denial of Service (DoS):** 使用本选项来设置 DoS 参数。本选项列出了本路由器的防火墙默认可提供的 DoS 攻击防范。

下一章节将介绍这些选项的使用。

9.6.1 设置自我访问 (Self Access) 规则

自我访问 (Self Access) 规则可控制路由器对自身的访问。您可以用自我访问规则页面来:

- 新增自我访问规则，并进行基本参数设置
- 修改已存在的自我访问规则
- 删除已存在的自我访问规则
- 查看已存在的自我访问规则



图 9.13. 自我访问规则设置页面

表 9.4. 自我访问设置参数

栏位	说明
Protocol	从下拉式菜单中选择协议 - TCP/ UDP/ICMP
Port	输入端口号码
Direction	选择被允许的网络流量方向。
From LAN	选择 Enable 或 Disable 来允许或阻止从 LAN (内部网络) 至路由器的流量
From WAN	选择 Enable 或 Disable 来允许或阻止从 WAN (外部网络) 至路由器的流量

9.6.1.2 访问自我访问规则设置页面 - (Firewall -> Advanced -> Self Access)

以管理员身份登录设置管理界面。点击 Firewall -> Advanced -> Self Access。防火墙自我访问规则设置页面出现，如图 9.13 所示。

当您开启自我访问规则设置页面时，已存在的自我访问规则会显示在设置页面的下方，如图 9.13 所示。

9.6.1.3 新增自我访问规则

如何新增自我访问规则

1. 开启自我访问规则设置页面。请参考 9.6.1.2 访问自我访问规则设置页面。
2. 从 Self Access 规则下拉式菜单中选择 Add New。
3. 从 Protocol 下拉式菜单中选择一个协议。若您选择 TCP 或 UDP 协议，您需要输入端口号码。
4. 点击 <Add> 新增自我访问规则。这个新的规则将显示于设置页面下方的自我访问规则列表中。

9.6.1.4 修改自我访问规则

如何修改自我访问规则

1. 开启自我访问规则设置页面。请参考 9.6.1.2 访问自我访问规则设置页面。
2. 点击需要修改的自我访问规则中的  图标来修改规则，或从自我访问规则下拉式菜单选择自我访问规则。
3. 接着您可以关闭或开启来自 LAN 或 WAN 或这两者的流量。若选择了 TCP 或 UCP 协议，则端口号码不能更改。要更改端口号码，您必须首先删除已存在的自我访问规则，接着新增一个新的规则来替代。
4. 点击 <Modify> 保存设置。新的自我设置规则将显示在设置页面下方的自我访问规则表中。

9.6.1.5 删除自我访问规则

如何删除自我访问规则

1. 开启自我访问规则设置页面。请参考 9.6.1.2 访问自我访问规则设置页面。

2. 点击需要删除的自我访问规则中的  图标，或从自我访问规则下拉式菜单选择自我访问规则。
3. 点击 <Delete> 删除规则。被删除的规则将从设置页面下方的自我访问规则表中移除。

9.6.1.6 查看自我访问规则

要查看已存在的自我访问规则，您只需依照 9.6.1.2 访问自我访问规则设置页面 的说明，开启自我访问规则设置页。

9.6.2 服务列表设置

服务是协议与联接端口号码的组合，用于传入与传出 ACL 规则设置。您可以用服务设置页面来：

- 新增服务，并为其设置参数
- 修改已存在的服务
- 删除已存在的服务
- 查看已存在的服务

图 9.14 所示为防火墙服务列表设置页面。已设置的服务被列在同一页面的下方。



图 9.14. 服务列表设置页面

9.6.2.1 服务列表设置参数

表 9.5 描述了防火墙服务列表的设置参数。

表 9.5. 服务列表设置参数

栏位	说明
Service Name	输入需要新增的服务名称。此名称只能使用字母。
Protocol	输入服务使用的协议类型。
Port	输入本服务的端口号码。

9.6.2.2 访问服务列表设置页面 - (Firewall -> Advanced -> Service)

以管理员身份登录设置管理界面。点击 Firewall -> Advanced -> Service。服务列表设置页面出现，如图 9.14 所示。

当您开启服务列表设置页面时，已存在的服务会显示在设置页面的下方，如图 9.14 所示。

9.6.2.3 新增服务

如何新增服务

1. 开启服务列表设置页面。请参考 9.6.2.2 访问服务列表设置页面。
2. 从 Service 下拉式菜单中选择 Add New。
3. 在 Service Name 栏位输入服务的名称，最好使用一个可表示服务性质的名称，此名称仅可使用字母。
4. 更改下列栏位：公共端口与协议。关于这些栏位的解释请参考表 9.5。
5. 点击 <Add> 新增服务。这个新的服务将显示于设置页面下方的服务列表中。

9.6.2.4 修改服务

如何修改服务

1. 开启服务列表设置页面。请参考 9.6.2.2 访问服务列表设置页面。
2. 从服务下拉式菜单中选择服务，或在服务列表中点击需要修改的服务图标。
3. 更改下面的设置：服务名称，公共端口与协议。关于这些栏位的解释请参考表 9.5。
4. 点击 <Modify> 修改服务。这个服务的新设置将显示于设置页面下方的服务列表中。

9.6.2.5 删除服务

如何删除服务

1. 开启服务列表设置页面。请参考 9.6.2.2 访问服务列表设置页面。
2. 从服务下拉式菜单中选择服务，或在服务列表中点击需要删除服务的  图标。
3. 点击 <Delete> 删除服务。删除的服务从设置页面下方的服务列表中移除。

9.6.2.6 查看已设置的服务

如何查看已存在服务列表

1. 开启服务列表设置页面。请参考 9.6.2.2 访问服务列表设置页面。
2. 服务设置页面下方的服务列表将显示所有已设置的服务。

9.6.3 DoS 设置

华硕 SL1200 的防火墙具有攻击防范功能，用以保护内部网络免于遭受来自 Internet 已知类型的攻击。本功能提供对于阻绝服务攻击（DoS attack）的保护，像是 SYN Flooding（泛洪）、IP Smurfing（伪装）、LAND、Ping of Death 与所有可能被假定的攻击。它会丢弃 ICMP 重定向封包与 IP 松／严格来源路由封包。举例来说，SL1200 的防火墙功能提供对于“WinNuke”一种被广泛用来自远程 Internet 瘫痪窗口操作系统的攻击。此外，本路由器的防火墙功能也提供多种来自 Internet 的攻击，像是 IP spoofing、Ping of Death、Land Attack、封包重组与 SYN flooding（泛洪）攻击。表 2.3 中所列举者为 SL1200 可防范的攻击类型。

9.6.3.1 DoS 防范设置参数

表 9.6 描述了 DoS 攻击防范的设置参数。

表 9.6. DoS 防范设置参数

栏位	说明
SYN Flooding	勾选或不勾选此选项可开启或关闭对 SYN 泛洪攻击的防范。这种攻击包含传送连接请求至服务器，但从不完全完成连接。当不能从有效的用户那里接收连接时，这将导致一些电脑陷入“胶着状态”（SYN 是 SYNchronize 的简写）。如果您想要网络免受此类型的攻击，则您可以选择此项。默认情况下，SYN 泛洪防范是开启的。
Winnuke	勾选或取消勾选本选项以开启或关闭对 WinNuke 攻击的防范功能。一些较旧版本的 Microsoft Windows 操作系统可能会遭受这类攻击。如果局域网电脑的操作系统没有及时下载最新版本的修正程序更新，那么建议您开启此项功能。
MIME Flood	勾选或取消勾选本选项以开启或关闭对 MIME 攻击的防范功能。您可以勾选此项以保护您网络中的主服务器免受 MIME 泛洪攻击。
FTP Bounce	勾选或取消勾选本选项以开启或关闭对 FTP bounce 攻击的防范功能。最简单的情形是，这种攻击是由在 FTP 协议中错误使用 PORT 命令。攻击者可在 FTP 服务器与另一个系统中的一个端口建立连接。此连接可能被用来将原本要套用的访问控制忽略。
IP Unaligned Time Stamp	勾选或不勾选本选项以开启或关闭对具有不连续时间信息（unaligned IP timestamp）的封包的攻击防范。某些操作系统当接收到此类封包时，会导致系统损毁。
Sequence Number Prediction Check	勾选或不勾选本选项以开启或关闭对 TCP 序号推断（TCP sequence number prediction）攻击的防范。对于 TCP 封包来说，序号用来防止接收非计划中的数据与攻击者的恶意使用（若 ISP(初始序号) 是随机产生的)。拥有合法序号的伪装封包可获得接收方主机的信任。接着，攻击者就可以访问这个系统。这种攻击只对路由器发出或终止于路由器的 TCP 封包起作用。

栏位	说明
Sequence Number Out of Range Check	勾选或不勾选本选项可开启或关闭对 TCP 超范围序号 (out of range sequence number) 攻击的防范。攻击者可传送一个 TCP 封包以导致侵入侦测系统 (IDS) 与网络连接中的数据不同步。该连接中后来传送的帧可能被 IDS 忽略。这种攻击可能截获一个 TCP 会话 (session)。
ICMP Verbose	勾选或不勾选本选项可开启或关闭对 ICMP 错误信息 (ICMP error message) 攻击。ICMP 信息会用不需要的网络流量使您的网络泛洪。默认情况下, 这一选项是开启的。
Maximum IP Fragment Count	输入防火墙允许每个 IP 封包最多被分为多少段。若您与 ISP 的连接是 PPPoE 方式, 您需要设置这个选项。这个数据在传送或接收 IP 封包段的时候使用。当大的封包通过路由器传送时, 封包被分割为如 MTU (最大传输单元) 大小的若干段。在默认情况下, 这个数值被设为 45。若此端口的 MTU 值为 1500 (以太网的默认值), 则每个 IP 封包最多可分为 45 段。若 MTU 值比这个值要小, 则会封包会被分为更多段, 此时, 这里的设置值也必须增大。
Minimum IP Fragment Size	输入防火墙允许每个 IP 封包段的最小大小。这一限制将不会用于封包的最后一个段。若 Internet 流量会有大量很小的片段, 则这个值应该相应减小。当有大量封包丢失, 速度降低, 或日志中经常有这样的记录: “fragment of size less than configured minimum fragment size detected”, 则您有必要更改这个设置。

9.6.3.2 访问 DoS 设置页面 - (Firewall -> Advanced -> DoS)

以管理员身份登录设置管理界面。点击 Firewall -> Advanced -> DoS。DoS 设置页面出现，如图 9.15 所示。

当您开启服务列表设置页面时，已存在的 DoS 攻击防范会显示在设置页面的下方，如图 9.15 所示。当防火墙打开时，这些防范是默认开启的。

9.6.3.3 DoS 设置

默认情况下，大多数 DoS 防范都是开启的。图 9.15 显示了默认的 DoS 设置。您可以勾选或不勾选一个攻击类型来开启或关闭对这种特定类型攻击的防范。

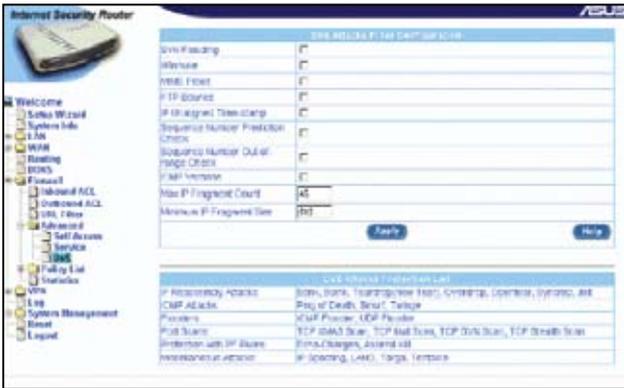


图 9.15. DoS 设置页面

9.7 防火墙策略列表 - (Firewall -> Policy List)

防火墙策略列表提供一种方便的方式来管理防火墙 ACL 规则（传入/传出 ACL 规则，以及群组 ACL 规则）。

- **IP Pools:** 本选项可让您设置 IP 地址池的逻辑名称并设置适当的 IP 地址。每个记录包含了 IP 记录的名称与 IP 地址类型（单个 IP 地址或 IP 地址范围或子网掩码）。
- **NAT Pools:** 本选项可让您设置 NAT 池，确保将内部 IP 地址映射至公共 IP 地址。请首先设置 NAT Pools，然后再将其添加到策略中。
- **Time Ranges:** 本选项可让您设置时间窗口，用于用户通过路由器对网络的访问。

9.7.1 设置 IP 地址池

9.7.1.1 IP 地址池设置参数

表 9.7 描述了 IP 地址池设置参数。

表 9.7. IP 地址池设置参数

栏位	说明
IP Pool Name	输入 IP 地址池的名称。
IP Pool Type	选择 IP 地址池的类型。
IP Range	本选项可让您设置 IP 地址范围。
Start IP	输入此范围的开始 IP 地址。
End IP	输入此范围的结束 IP 地址。
Subnet	本选项可让您将所有连接的电脑包含到一个 IP 子网。
Subnet Address	输入合适的 IP 地址。
Subnet Mask	输入相应的遮罩。
IP Address	本选项可让您设置单个 IP 地址。
IP Address	输入 IP 地址。

9.7.1.2 访问 IP 地址池设置页面 - (Firewall -> Policy List -> IP Pool)

以管理员身份登录设置管理界面。点击 Firewall -> Policy -> IP Pool。IP 地址池设置页面出现，如图 9.16 所示。

当您开启 IP 地址池设置页面时，已存在的 IP 地址池会显示在设置页面的下方，如图 9.16 所示。

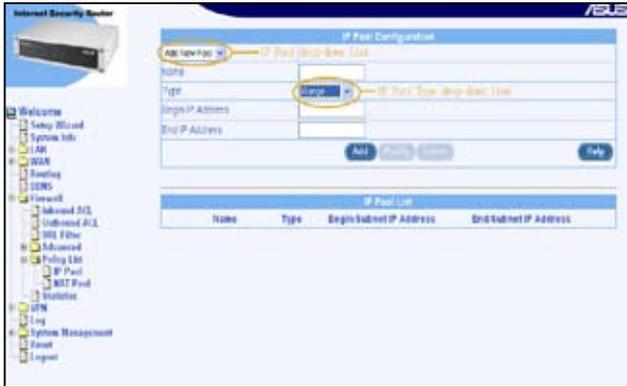


图 9.16 IP 地址池设置页面

9.7.1.3 新增 IP 地址池

如何新增 IP 地址池

1. 开启 IP 地址池设置页面。请参考 9.7.1.2 访问 IP 地址池设置页面。
2. 从 IP Pool 下拉式菜单中选择 Add New Pool。
3. 在 Name 栏位输入地址池的名称。
4. 从 IP Type 下拉式菜单中选择地址池类型。
5. 若选择了“IP Range”地址池类型，请输入开始与结束 IP 地址。若选择了“Subnet”类型，则请输入子网地址与子网掩码。若选择了 IP Address 类型，请输入 IP 地址。
6. 点击 <Add> 新增 IP 地址池。这个新的 IP 地址池将显示于设置页面下方的 IP 地址池列表中。

9.7.1.4 修改 IP 地址池

如何修改 IP 地址池

1. 开启 IP 地址池设置页面。请参考 9.7.1.2 访问 IP 地址池设置页面。
2. 点击需要修改的 IP 地址池的  图标来修改 IP 地址池，或从 IP Pool 下拉式菜单选择 IP 地址池。
3. 对下面的栏位进行修改：地址池名称，地址池类型与 IP 地址。
4. 点击 <Modify> 保存设置。新的 IP 地址池设置规则将显示在设置页面下方的 IP 地址表中。

9.7.1.5 删除 IP 地址池

要删除 IP 地址池，点击想要删除的 IP 地址池的  图标，或依照下面的说明操作：

1. 开启 IP 地址池设置页面。请参考 9.7.1.2 访问 IP 地址池设置页面。
2. 在 IP 地址池列表中点击需要删除的 IP 地址池的  图标，或从 IP Pool 下拉式菜单选择 IP 地址池。
3. 点击 <Delete> 删除此 IP 地址池。

9.7.1.6 IP 地址池范例

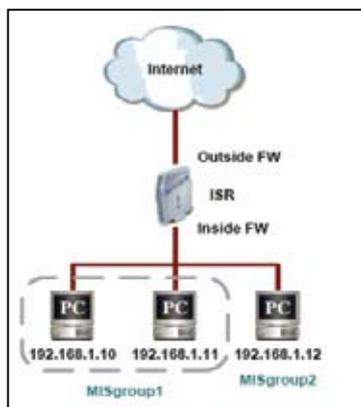


图 9.17. IP 地址池设置图

1. 开启 IP 地址池设置页面以新增两个 IP 群组 - 参见图 9.18。

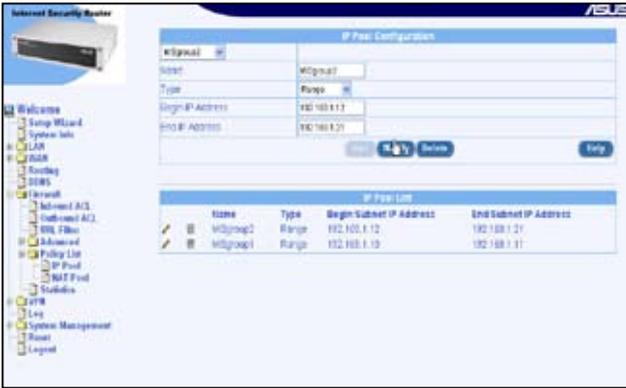


图 9.18. IP 地址池范例 - 新增两个 IP 地址池 - MISgroup1 与 MISgroup2

2. 从 Source IP Type 下拉式菜单中选择 IP Pool，接着从 IP Pool 下拉式菜单中选择一个 IP 地址池，将一个 IP 地址池用到防火墙 ACL 规则中 - 传入、传出或群组。在这个范例中，IP 地址池被用在了来源 IP 中。您也可以将它用于目的地 IP。如图 9.19，MISgroup1 不允许玩网络游戏，禁止使用 Quake-II。

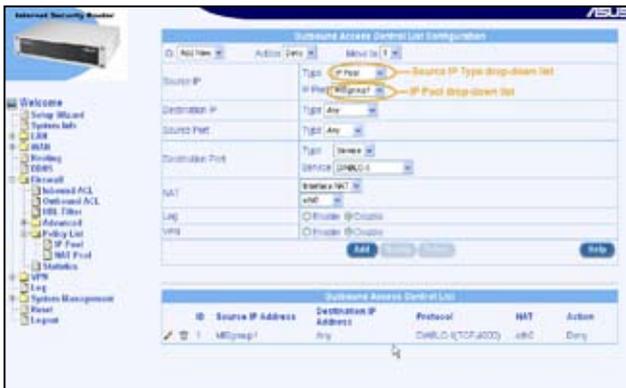


图 9.19. IP 地址池范例 - MISgroup1 禁用 QUAKE-II 连接

9.7.2 设置 NAT 地址池

9.7.2.1 NAT 地址池设置参数

表 9.8 描述了 NAT 地址池设置参数。

表 9.8. NAT 地址池设置参数

栏位	说明
NAT Pool Name	输入 NAT 地址池的名称。
NAT Pool Type	选择 NAT 地址池的类型
Static	
选择这一 NAT 类型以设置内部网络地址与外部网络地址的一对一映射。	
LAN IP range	用于内部地址
Start IP	输入起始 IP 地址
End IP	输入结束 IP 地址
Internet IP Range	用于外部地址
Start IP	输入起始 IP 地址
End IP	输入结束 IP 地址
Dynamic	
选择这一 NAT 类型以将一组内部（公司）地址映射到一组公共 IP 地址。依照上述描述输入 LAN IP Range 与 Internet IP Range 的值。	
Overload	
选择这一 NAT 类型以使用单一的公共 IP 地址来连接多台内部（公司局域网）电脑至外部网络（Internet）。	
NAT IP Address	输入 NAT IP 地址
Interface	
选择这一 NAT 类型以指定一个动态端口，它的 IP 地址须用来将流量导向 NAT。	

9.7.2.2 访问 NAT 地址池设置页面 - (Firewall -> Policy List -> NAT Pool)

以管理员身份登录设置管理界面。点击 Firewall -> Policy List -> NAT Pool。NAT 地址池设置页面出现，如图 9.20 所示。

当您开启 NAT 地址池设置页面时，已存在的 NAT 地址池会显示在设置页面的下方，如图 9.20 所示。

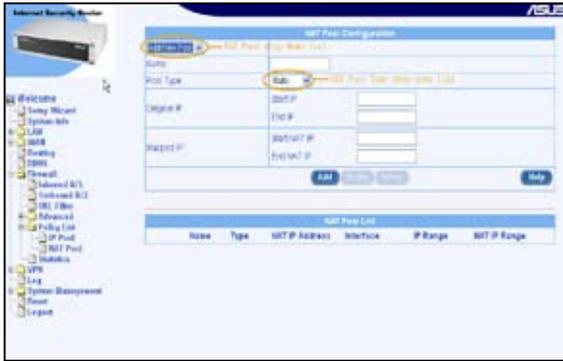


图 9.20. NAT 地址池设置页面

9.7.2.3 新增 NAT 地址池

如何新增 NAT 地址池

1. 开启 NAT 地址池设置页面。请参考 9.7.2.2 访问 NAT 地址池设置页面。
2. 从 NAT Pool 下拉式菜单中选择 Add New Pool。
3. 在 Name 栏位输入地址池的名称。
4. 从 Type 下拉式菜单中选择地址池类型。
5. 若选择了“Static”或“Dynamic”地址池类型，请输入原始 IP 地址（开始与结束 IP 地址）与映射至的 IP 地址（开始与结束 NAT IP 地址）。若选择了“Overload”类型，则请输入 NAT IP 地址。若您想用分配给 WAN 端口的 IP 地址作为 NAT IP 地址，请选择 Interface 类型。
6. 点击 <Add> 新增 NAT 地址池。这个新的 NAT 地址池将显示于设置页面下方的 NAT 地址池列表中。

9.7.2.4 修改 NAT 地址池

如何修改 NAT 地址池

1. 开启 NAT 地址池设置页面。请参考 9.7.2.2 访问 NAT 地址池设置页面。
2. 点击需要修改的 NAT 地址池的  图标来修改 NAT 地址池，或从 NAT Pool 下拉式菜单选择 NAT 地址池。
3. 对下面的栏位进行修改：地址池名称，地址池类型与 IP 地址。
4. 点击 <Modify> 保存设置。新的 NAT 地址池设置规则将显示在设置页面下方的 NAT 地址表中。

9.7.2.5 删除 NAT 地址池

要删除 NAT 地址池，点击想要删除的 IP 地址池的  图标，或依照下面的说明操作：

1. 开启 NAT 地址池设置页面。请参考 9.7.1.2 访问 NAT 地址池设置页面。
2. 在 NAT 地址池列表中点击需要删除的 NAT 地址池的  图标，或从 IP Pool 下拉式菜单选择 NAT 地址池。
3. 点击 <Delete> 删除此 IP 地址池。

9.7.2.6 NAT 地址池范例

图 9.21 所示为这个 NAT 地址池的网络设置图。

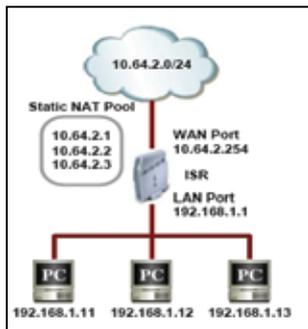


图 9.21. NAT 地址池设置图

1. 新增一个 NAT 地址池，类型为静态 (Static) - 如图 9.22 所示。

The screenshot shows the 'NAT Pool Configuration' window. At the top left, there is a dropdown menu 'Add New Pool' with a downward arrow. Below it, the 'Name' field is set to 'Pool1'. The 'Pool Type' is set to 'Static'. The 'Original IP' section has 'Start IP' at 192.168.1.2 and 'End IP' at 192.168.1.5. The 'Mapped IP' section has 'Start NAT IP' at 10.64.2.205 and 'End NAT IP' at 10.64.2.205. At the bottom, there are buttons for 'Add', 'Modify', 'Delete', and 'Help'.

图 9.22. NAT 地址池范例 - 新增一个静态 NAT 地址池

2. 从 NAT 类型下拉式菜单中选择 NAT Pool，并从 NAT Pool 下拉式菜单中选择一个已存在的 NAT 地址池，将 NAT 地址池附加到一个传出 ACL 规则中。

The screenshot shows the 'Outbound Access Control List Configuration' window. At the top, there are buttons for 'Add New', 'Action' (set to 'Allow'), and 'Move to' (set to '1'). The 'Source IP' section has 'Type' set to 'Range', 'Begin IP Address' at 192.168.1.2, and 'End IP Address' at 192.168.1.5. The 'Destination IP' section has 'Type' set to 'Any'. The 'Source Port' and 'Destination Port' sections both have 'Type' set to 'Any'. The 'Protocol' section has 'Any' selected. The 'NAT' section has 'NAT type' set to 'NAT Pool' and 'Pool' set to 'Pool1'. Two orange arrows point to these dropdown menus with labels: 'NAT type drop-down list' and 'NAT pool drop-down list'. At the bottom, there are buttons for 'Add', 'Modify', 'Delete', and 'Help'.

图 9.23. NAT 地址池范例 - 将 NAT 地址池附加到 ACL 规则

9.7.3 设置时间范围（Time Range）

通过这一选项，您可以设置访问时间范围记录并附加于 ACL 规则。带时间范围记录的 ACL 规则只在设置的时间范围内有效。若 ACL 规则阻止 10:00 至 18:00 的间的 HTTP 访问，则在 10:00 的前或 18:00 的后，HTTP 访问将被允许通过。一个时间范围记录可包含最多三个时间段。如：

工作日（周一至周五）的上班时间可分为以下的时间段：

- 午饭前，从 9:00 到 13:00
- 午饭后，从 14:00 到 18:30

周末（周六和周日）的办公室时间可分为以下的时间段：

- 9:00 到 12:00

这种变化的时间段可以设置为单独的时间范围记录。访问规则可依据这些时间段生效。

9.7.3.1 时间范围设置参数

表 9.9 描述了时间范围的设置参数。

表 9.9. 时间范围设置参数

栏位	说明
Time Range drop-down list	选择“Add New Time Range” 新增一个时间范围或从下拉式菜单中选择一个已存在的时间范围。
Time Range Name	输入此一时间范围的名称。
Schedule drop-down list	选择“Add New Schedule” 来新增一个新的时间表或从下拉式菜单中选择一个已存在的时间表。
Days of Week	设置时间表的日期。
Time (hh:mm)	设置时间表的时间窗口，格式为 hh:mm。

9.7.3.2 访问时间范围设置页面 - (Firewall -> Policy List -> Time Range)

以管理员身份登录设置管理界面。点击 Firewall -> Policy List -> Time Range。时间范围设置页面出现，如图 9.24 所示。

当您开启时间范围设置页面时，时间范围设置会显示在设置页面的下方，如图 9.24 所示。

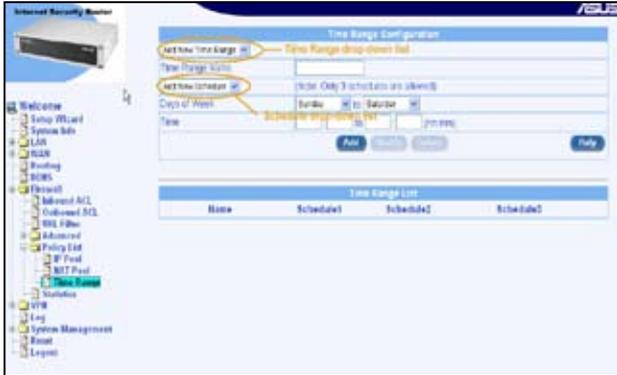


图 9.24. 时间范围设置页面

9.7.3.3 新增时间范围

如何新增时间范围

1. 开启时间范围设置页面。请参考 9.7.3.2 访问时间范围设置页面。
2. 从 Time Range 下拉式菜单中选择 Add New Time Range。
3. 在 Time Range Name 栏位输入名称。
4. 从 Schedule 下拉式菜单中选择 Add New Schedule。
5. 选择一周内的日期。如，从周日到周六。
6. 输入一天内的时间，如从 08:00 到 18:00。
6. 点击 <Add> 新增时间表 (Schedule)。

9.7.3.4 修改时间范围

如何修改时间范围

1. 开启时间范围设置页面。请参考 9.7.3.2 访问时间范围设置页面。
2. 在 Time Range 列表中，点击需要修改的时间范围的  图标，或从 Time Range 下拉式菜单中选择时间范围。
3. 从 Schedule 下拉式菜单中选择时间表。
4. 对下面的栏位进行修改：一周内的日期和小时。
5. 点击 <Modify> 保存新设置。

9.7.3.5 删除时间范围

要删除一个时间范围，点击需要删除的时间范围的  图标。

9.7.3.6 在时间范围内删除时间表

如何在时间范围内删除时间表

1. 开启时间范围设置页面。请参考 9.7.3.2 访问时间范围设置页面。
2. 在 Time Range 列表中，点击需要修改的时间范围的  图标，或从 Time Range 下拉式菜单中选择时间范围。
3. 从 Schedule 下拉式菜单中选择时间表。
4. 点击 <Delete> 删除此时间表。

9.7.3.7 时间范围范例

1. 新增一个时间范围 - 参见图 9.22。



The screenshot shows the 'Time Range Configuration' window. It includes a dropdown for 'Add New Time Range', a text input for 'Time Range Name' (containing 'Office Hours'), a dropdown for 'Add New Schedule' with a note '(Note: Only 3 schedules are allowed)', a 'Days of Week' section with 'Sunday' and 'Friday' selected, and a 'Time' section with '08:00' and '17:00' entered. At the bottom are 'Add', 'Modify', 'Delete', and 'Help' buttons.

图 9.25. 时间范围范例 - 新增时间范围

- 从 Time Range 下拉式菜单中选择一个已存在的时间范围，将时间范围附加到一个传出 ACL 规则中。图 9.26 所示为 MISgroup1 禁止在工作时间访问 FTP。

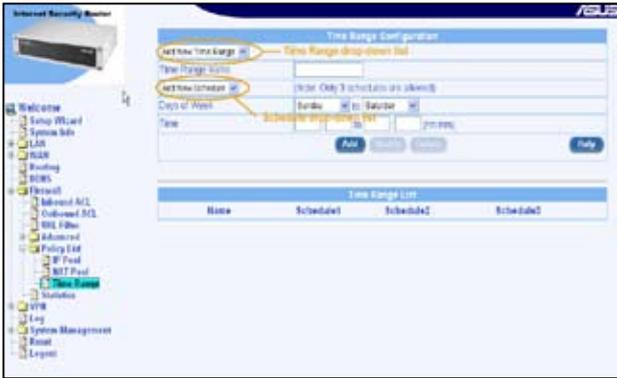


图 9.26. 时间范围范例 - MISgroup1 禁止在工作时间访问 FTP

9.8 防火墙统计 - Firewall -> Statistics

防火墙统计页面显示了当前连接的详细内容。图 9.27 所示为活动连接的防火墙统计值。若要查看更新后的统计值，请点击 <Refresh>。



图 9.27. 防火墙活动连接统计值

第十章 设置 VPN

本章节将介绍使用自动与手动密钥进行 VPN 连接设置。

10.1 默认参数

SL1200 预先设置了一组默认设置/连接。它们包含了典型设置方案中最经常使用的几组参数。我们建议您使用这些默认的设置和连接，以方便地进行 VPN 连接。这些默认的参数有：

默认连接

每个连接代表了一个起始于或终止于路由器的流量规则。它包含下列参数：本地/远程 IP 地址与端口。

表 10.1 列出了本路由器的默认连接。

表 10.1. 路由器的默认连接

名称	类型	端口	协议	状态	目的
allow-ike-io	passby	500	UDP	Enabled	允许 IKE 流量至本路由器
allow-all	passby			Enabled	允许所有流量通过



不要删除或修改默认的 VPN 策略。

预设置

每个预设置代表了一组验证/加密参数。您可以将一个预设置附加到一个连接上。建立会话后，指定的预设置会被用在通信中。您也可以为一个连接指定多个预设置。若您没有为连接指定预设置，则所有的预设置都将包含在这个连接中。

默认的 IKE 设置

IKE 设置决定了通信双方建立会话时需用到的加密类型，hash 演算法，及验证方式。表 10.2 列出了默认的 IKE 设置。

表 10.2. 路由器默认的 IKE 设置

名称	加密演算法	验证演算法	Diffie-Hellman 群组	密钥管理	存在时间 (秒)
ike-preshared-3des-sha1-dh2	3DES	SHA-1	2	预共享密钥	3600
ike-preshared-3des-md5-dh2	3DES	MD5	2	预共享密钥	3600
ike-preshared-des-sha1-dh2	DES	SHA-1	2	预共享密钥	3600
ike-preshared-des-md5-dh2	DES	MD5	2	预共享密钥	3600
ike-preshared-3des-sha1-dh1	3DES	SHA-1	1	预共享密钥	3600
ike-preshared-3des-md5-dh1	3DES	MD5	1	预共享密钥	3600
			1		
ike-preshared-des-sha1-dh1	DES	SHA-1	1	预共享密钥	3600
ike-preshared-des-md5-dh1	DES	MD5	1	预共享密钥	3600
ike-preshared-3des-sha1-dh5	3DES	SHA-1	5	预共享密钥	3600

名称	加密演算法	验证演算法	Diffie-Hellman 群组	密钥管理	存在时间 (秒)
ike-pre-shared-3des-md5-dh5	3DES	MD5	5	預共享密鑰	3600
ike-pre-shareddes-sha1-dh5	DES	SHA-1	5	預共享密鑰	3600
ike-pre-shareddes-md5-dh5	DES	MD5	5	預共享密鑰	3600

默认的 IPsec 设置

IPsec 设置决定了通信双方流量的加密类型与验证方式。

表 10.3 列出了本路由器默认的 IPsec 设置。

表 10.3. 路由器默认的 IPsec 设置

名称	加密演算法	验证演算法	封装	存在时间 (Mbytes/sec)
ipsec-esp-3des-sha1	3DES	SHA-1	ESP	75/3600
ipsec-esp-3des-md5	3DES	MD5	ESP	75/3600
ipsec-esp-des-sha1	DES	SHA-1	ESP	75/3600
ipsec-esp-des-md5	DES	MD5	ESP	75/3600
ipsec-ah-sha1	-	SHA-1	AH	75/3600
ipsec-ah-md5	-	MD5	AH	75/3600
ipsec-esp-3des	3DES	-	ESP	75/3600
ipsec-esp-des	-	SHA-1	ESP	75/3600
ipsec-esp-sha1	-	SHA-1	ESP	75/3600
ipsec-esp-md5	-	MD5	ESP	75/3600

默认存在时间

默认的 IKE 设置与 IPSec 设置的存在时间都是 3600 秒（一小时）。我们建议您将新的 IKE 或 IPSec 设置的存在时间设为大于 600 秒。这将减少因快速重设密钥对系统造成的不必要的负荷。

密钥长度限制

预共享密钥的最大密钥长度。密码密钥与验证密钥的最大长度为 50 个字符。若密码密钥长度超过了加密演算法指定的长度，密钥会被截短至合适的长度。

连接的优先顺序

Allow-ike-io 默认规则具有最高的优先顺序（1）。而 allow-all 默认规则具有最低优先顺序。在任何时候，我们建议您保持这一优先顺序。若您在 allow-all 规则下新增了新连接（优先顺序在 allow-all 的下），它将不起任何作用，因为相应的封包将会符合 allow-all 规则，不经过加密而传出。

这些默认的设置／连接是只读的，不能修改。若您想指定一个设置（不是默认设置），您需要通过 VPN 设置页面新增一个。用这一方法您可以控制设置，使其成为连接的一部分。



为了成功完成协商，另一端网关也必须设置了相对应的参数。如果需要，您可以选择任何一个特定的设置。

本章节将介绍通过 GUI 来设置访问列表的步骤。

- 基本访问列表设置
 - 使用 IKE 的访问列表
- 高级访问列表设置
 - 使用 IKE 的访问列表

10.2 VPN 隧道 (Tunnel) 设置参数

表 10.4 描述了 VPN 设置中所有的 VPN 隧道(Tunnel)设置参数。

表 10.4. VPN 隧道 (Tunnel) 设置参数

栏位	说明
VPN Connection Settings	
ID	
Add New	点击此选项以新增一个“基本”防火墙规则。
Rule Number	从下拉式菜单中选择一个规则，来修改其内容。
Name	输入名称，最好是一个可表示此隧道 (Tunnel) 连接的有含义的名称。此栏位仅支持字母。
Enable	选择此项可开启这一规则（默认）。
Disable	选择此项关闭此规则。
Move to	
本选项可让您设置本规则的优先顺序。本路由器的防火墙依据规则的优先顺序作用于封包。您可以依照下面的规则指定数字来代表其优先顺序：	
1 (First)	这个数字代表最高的优先顺序。
其他数字	选择其他数字可按照您的需要指定规则的优先顺序。
Local Secure Group	
本选项可让您设置本规则应该套用至哪个本地安全网络。本选项可让您将此规则应用于内部网络中所有的电脑。您可以使用“Type”下拉式菜单来选择下列项目之一：	
IP Address	为本地安全群组输入一个适当的 IP 地址。
Subnet	本选项可让您将所有连接的电脑都包含至一个 IP 子网。当您选择此项时，下面的栏位将变为可设置项目：
Subnet Address	分配适当的网络地址。
Subnet Mask	输入子网掩码。

栏位	说明
IP Range	本选项可让您使一个指定范围内的 IP 地址都套用这一规则。当您选择此项时，下面的栏位将变为可设置项目：
Start IP	输入此范围的起始 IP 地址。
End IP	输入此范围的结束 IP 地址。
Remote Secure Group (仅用于 site to site VPN 模式)	
本选项可让您设置此规则将应用于哪个远程 (目的地) 安全网络。本选项可让您将此规则应用于外部网络中的所有电脑。您可以从 “Type” 下拉式菜单中选择下列项目之一：	
IP Address Subnet IP Range	如 Local Secure Group 部分所述，输入相应的详细内容。
Remote Gateway	
对于远程安全网关，您可以选择输入 IP 地址或 FQDN(安全合格的网域名称)。	
Any	选择本选项接受任何一台电脑的连接请求。
IP Address	选择本选项为远程安全网关分配一个 IP 地址。
FQDN	选择本选项为远程安全网关输入完全合格的网域名称。
IKE Proposal Settings (仅用于 pre-shared key)	
请注意：所有 IKE 设置的选项只有在选择了预共享密钥 (pre-shared key) 时才可用。	
IKE Mode	支持 main 模式与 aggressive 模式。点击相应的按钮来选择 IKE 模式。
Preshared Key	输入 shared secret (这必须符合另一端的 secret key)。

栏位	说明
IKE Encryption / Authentication	<p>从下拉式菜单中选择 IKE 验证与加密。</p> <p>All 3DES & SHA1-DH2 3DES & MD5-DH2 DES & SHA1-DH2 DES & MD5-DH2 3DES & SHA1-DH1 DES & MD5-DH1 DES & SHA1-DH1 DES & MD5-DH1 3DES & SHA1-DH5\DES & SHA1-DH5 DES & MD5-DH5</p> <p>注意：我们建议您选择 All，让所有的 IKE 设置都附加到当前隧道 (Tunnel)，让 IKE 自动选择一个（在一组 IKE 设置中）来与其另一端进行通信。当然，如果需要，您也可以从列表中选择任何一个特定的设置。</p>

欄位	說明
IPSec Proposal Settings	
IPSec Encryption / Authentication	<p>从下拉式菜单中选择下列默认 IPSec 设置之一。若选择了 All，所有默认设置都将附加于已存在的隧道 (Tunnel)，且 IPSec 将自动选择一个设置 (从一组 IPSec 设置中)，用于与另一端通信。</p> <p>All</p> <p>Strong Encryption & Authentication (ESP 3DES HMAC SHA1)</p> <p>Strong Encryption & Authentication (ESP 3DES HMAC MD5)</p> <p>Encryption & Authentication (ESP DES HMAC SHA1)</p> <p>Encryption & Authentication (ESP DES HMAC MD5)</p> <p>Authentication (AH SHA1)</p> <p>Authentication (AH MD5)</p> <p>Strong Encryption (ESP 3DES)</p> <p>Encryption (ESP DES)</p> <p>Authentication (ESP SHA1)</p> <p>Authentication (ESP MD5)</p>
PFS Group	<p>PFS 代表 Perfect Forward Secrecy(完整转发安全性)。您可以选择让所有的重协商 (re-negotiation) 都使用相同的密钥 (当 IKE 隧道 (Tunnel) 建立时产生) 或选择为所有重协商生成新的密钥。选择一个特定的 DH (Diffie-Hellman) 群组来为每一个重协商产生新的密钥。可支持的 DH 群组有：DH-1, DH-2 与 DH-5。群组数字越大，连接更安全。但是，群组数字越大，隧道 (Tunnel) 协商花费的时间越长。</p> <p>注意：若选择了 PFS，密钥在连接中会变换，隧道 (Tunnel) 会更加安全。但是，开启这个选项会降低隧道 (Tunnel) 协商的速度。</p>
Life Times	<p>输入附加 IPSec 的存在时间，单位为秒、分钟、小时或天，以及千位元组 (kilo bytes)。默认设置为 3600 秒与 75000KB。</p>

10.3 用自动密钥建立 VPN 连接

本章节描述了使用设置管理程序建立 VPN 隧道 (Tunnel) 的步骤。Internet 密钥交换 (IKE) 是一项自动产生密钥的协议，用来依照用户设置的规则，交换用于加密/验证数据封包的密钥。需要设置的参数有：

- 内部网络与远程网络的网络地址。
- 远程网关地址与本地网关地址。
- 用于远程网关验证的预共享 secret。
- 为连接设置适当的优先顺序。

这个选项组的画面如图 4.2 所示。栏位与按钮显示了基本的 VPN 参数。您可以用它们来设置基本的访问规则，通过这些基本参数来建立本地安全群组至远程群组的隧道 (Tunnel)。

本部分的选项可让您：

- 新增一个访问列表，并为其设置基本参数
- 修改一个访问列表
- 删除一个已存在的访问列表

10.3.1 用预共享密钥 (Pre-shared key) 为 VPN 连接新增规则

VPN 隧道 (Tunnel) 设置页面，如图 10.1 所示，可让您用预共享密钥 (Pre-shared Key) 为 VPN 连接设置规则。

如何新增 VPN 连接规则

1. 以管理员身份登录设置管理程序。点击 VPN -> VPN Tunnel。此时将出现 VPN 隧道 (Tunnel) 设置页面，如图 10.1 所示。
当您开启 VPN 隧道 (Tunnel) 设置页面时，已存在的 VPN 连接规则会显示在设置页面的下方，如图 10.1 所示。
2. 在增加 VPN 规则的前，请确保您在系统服务设置 (System Service Configuration) 页面开启了 VPN 服务。
3. 从 ID 下拉式菜单中选择 Add New。
4. 在 Name 栏位输入规则名称，最好使用一个可表示 VPN 连接性质的名称，此名称仅可使用字母。
5. 点击 Enable 或 Disable 按钮开启或关闭这一规则。

6. 更改下列栏位：local/remote secure group, remote gateway, key management type (select Preshared Key), pre-shared key for IKE, encryption/authentication algorithm for IKE, lifetime for IKE, encryption/authentication algorithm for IPSec, operation mode for IPSec, PFS group for IPSec and lifetime for IPSec。关于这些栏位的解释请参考表 10.4。
7. 从“Move to”下拉式菜单中选择一个数字来为规则指定优先顺序。注意：数字代表了规则的优先顺序。VPN 将会优先检测高优先权的规则。
8. 点击 <Add> 新增 VPN 规则。这个新的 VPN 规则将显示于 VPN 设置页面下方的 VPN 连接状态列表中。



图 10.1. VPN 隧道 (Tunnel) 设置页面 - Pre-shared Key 模式

10.3.2 修改 VPN 规则

如何修改 VPN 规则

1. 以管理员身份登录设置管理界面。点击 VPN -> VPN Tunnel。
2. 在修改 VPN 规则的前，请确保您在系统服务设置（System Service Configuration）页面开启了 VPN 服务。
3. 从 ID 下拉式菜单中选择规则号码，或在 VPN 连接状态表中选择需修改规则图标。
4. 点击 Enable 或 Disable 按钮来开启或关闭这个规则。
5. 修改下面的栏位：local/remote secure group, remote gateway, key management type (select Preshared Key), pre-shared key for IKE, encryption/authentication algorithm for IKE, lifetime for IKE, encryption/authentication algorithm for IPSec, operation mode for IPSec, PFS group for IPSec and lifetime for IPSec。关于这些栏位的解释请参考表 10.4。
6. 点击 <Modify> 修改规则。这个 VPN 规则中的新设置将显示于 VPN 设置页面下方的 VPN 连接状态列表中。

10.3.3 删除 VPN 规则

如何删除 VPN 规则

1. 以管理员身份登录设置管理界面。点击 VPN -> VPN Tunnel。
2. 在删除 VPN 规则的前，请确保您在系统服务设置（System Service Configuration）页面开启了 VPN 服务。
3. 从 ID 下拉式菜单中选择规则号码，或在 VPN 连接状态表中选择需删除规则图标 。
4. 点击 <Delete> 修改服务。被删除的 VPN 规则将从 VPN 设置页面下方的 VPN 连接状态列表中移除。

10.3.4 查看 VPN 规则

如何查看已存在的 VPN 规则

1. 以管理员身份登录设置管理界面。点击 VPN -> VPN Tunnel。
2. VPN 设置页面下方的 VPN 规则表显示了所有已设置的 VPN 规则。

10.4 VPN 统计值

统计值 (Statistics) 选项可让您查看有关 VPN 统计值的信息 - Global, IKE SA(Security Association) 与 IPsec SA。

表 10.5 描述了 VPN 统计值参数。

表 10.5. VPN 统计值

项目	说明
VPN Statistics	
Global IPSEC SA Statistics	全部封包统计值
AH Packets	AH 封包数量
ESP Packets	ESP 封包数量
Triggers	触发 (triggers) 数量
Packets Dropped	丢弃封包数量
Packets Passed	由 VPN 通过的封包总数
Partial Packets	不完整封包总数
Packets Currently Reassembled	当前被重组的不完整封包数量
Non-First Fragments Currently in the Engine	当前在引擎内的非首段封包数量

项目	说明
IKE 状况	IKE 协商统计值
IKE Phase1 协商完成	已完成的 IKE phase-1 协商数量
Failed IKE Negotiations Done	失败的 IKE phase -1 协商数量
快速模式协商 Performed	已完成的 IKE 快速模式协商数量
ISAKMP SAs 数量	phase 1 SA 的数量
ESP 状况	ESP 统计值数量
Active Inbound ESP SAs	活动的传入 ESP SA 数量
Active Outbound ESP SAs	活动的传出 ESP SA 数量
Total Inbound ESP SAs	自系统启动以来，传入 ESP SA 的数量
Total Outbound ESP SAs	自系统启动以来，传出 ESP SA 的数量
AH 状况	所有 AH SA 的 SA 统计值
Active Inbound AH SAs	活动的传入 AH SA 的数量
Active Outbound AH SAs	活动的传出 AH SA 的数量
Total Inbound AH SAs	自系统启动以来，传入 AH SA 的数量
Total Outbound AH SAs	自系统启动以来，传出 AH SA 的数量
IKE SA	
IPSec SA	

图 10.2 显示了 VPN 连接的所有可用参数。若要查看更新后的统计值，请点击 <Refresh>。

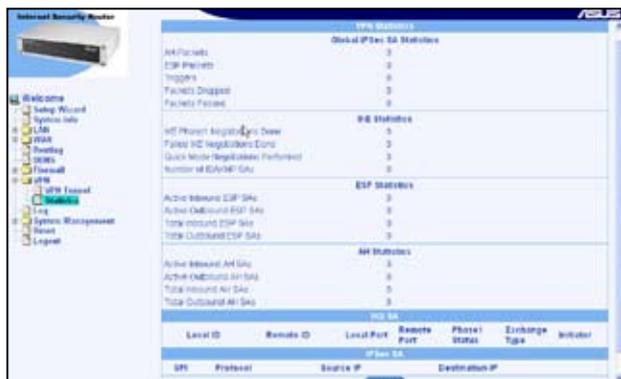


图 10.2. VPN 状况页面

10.5 VPN 连接范例

具有内建 VPN 与防火墙的网关在以下情形非常有用：

- 公司分部的间的流量由 VPN 保护，以及
- 目的地为公共Internet的流量会经过防火墙/NAT。

为了防止 NAT/IPSec 相互干扰，传出流量会首先经过防火墙/NAT 机制，然后才经过 IPsec 机制。因此，您必须保证您设置了合适的防火墙规则以使 VPN 流量经过。本部分将介绍这些情形，并提供设置这些情形的详细步骤。

10.5.1 内部网络 - 防火墙 + VPN，无需 NAT

这是一种普遍的情况，传至公共Internet的流量需要通过防火墙/NAT，但在专用网络中传输的流量在 IPsec 过程前不需要进行 NAT。请依照下面的步骤设置内部网络环境中的每个路由器：

- 设置 VPN 连接规则。
- 设置防火墙访问规则来允许传入与传出 VPN 流量。
- 设置防火墙自我访问规则来允许 IKE 封包传入路由器。

10.5.1.1 在 Internet 安全路由器 1 (ISR1) 设置规则

本章节介绍为内部网络环境建立 VPN/防火墙的步骤。图 10.3 所示为典型的内部网络连接。若两个网络是通过以太网连接，您不需要使用 ADSL 或 cable modem。每一个设置步骤都已在图中说明。详细内容请参考下一章节。

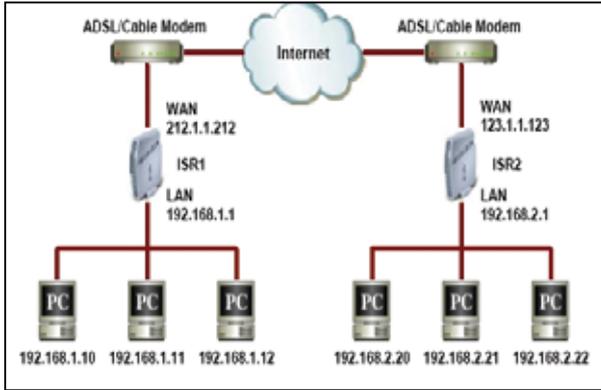


图 10.3. 典型的内部网络图

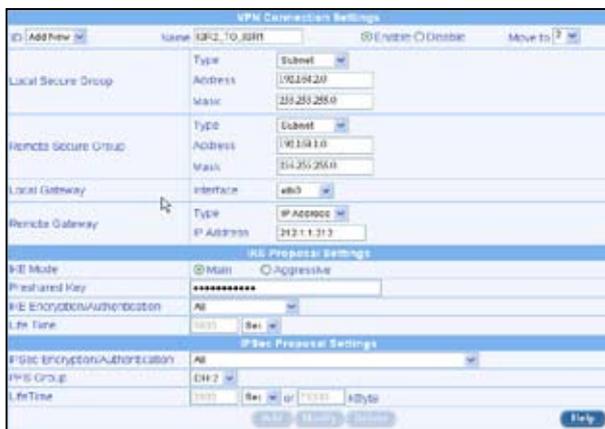


图 10.4. ISR1 的内部 VPN 策略设置

步骤 1: 设置 VPN 连接规则

请参考 10.3 使用自动密钥建立 VPN 连接 部分的说明，在 ISR1 上用自动密钥来设置 VPN 策略。

步骤 2: 设置防火墙规则

1. 设置传出防火墙规则，以允许自 192.168.1.0/255.255.255.0 至 192.168.2.0/255.255.255.0 的未经 NAT 的封包通过。
2. 设置传入防火墙规则来允许自 192.168.2.0/255.255.255.0 至 192.168.1.0/255.255.255.0 的未经 NAT 的封包通过。

表 10.6 与表 10.7 所述是传出与传入防火墙规则栏位需设置的参数。若要了解设置传入/传出防火墙规则的详细内容，请参考 9.3 与 9.4 章节的说明。

表 10.6. ISR1 上 VPN 封包的传出未转译防火墙规则

栏位		设置值
Source IP	Type	Subnet
	Address	192.168.1.0
	Mask	255.255.255.0
Destination IP	Type	Subnet
	Address	192.168.1.0
	Mask	255.255.255.0
NAT		None
Action		Allow
VPN		Enable



传出未转译防火墙规则需添加已存在的规则 ID 1001。

表 10.7. ISR1 上 VPN 封包的传入未转译防火墙规则

栏位		设置值
Source IP	Type	Subnet
	Address	192.168.2.0
	Mask	255.255.255.0
Destination IP	Type	Subnet
	Address	192.168.1.0
	Mask	255.255.255.0
NAT		None
Action		Allow
VPN		Enable

10.5.1.2 在 Internet 安全路由器 2 (ISR2) 设置规则

步骤 1: 设置 VPN 连接规则

请参考 10.3 使用自动密钥建立 VPN 连接 部分的说明，在 ISR2 上用自动密钥来设置 VPN 策略。

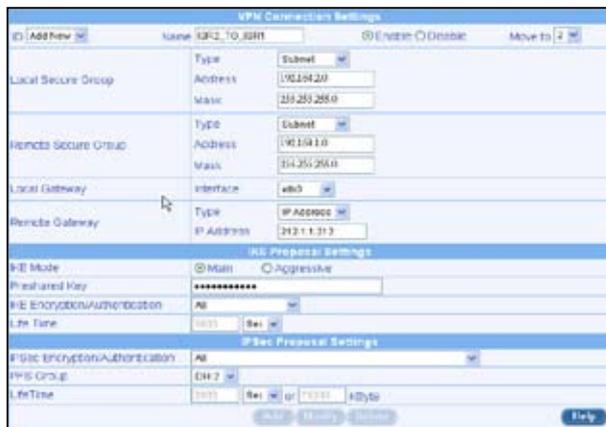


图 10.5. ISR2 的内部 VPN 策略设置

步骤 2: 设置防火墙规则

1. 设置传出防火墙规则，以允许自 192.168.2.0/255.255.255.0 至 192.168.1.0/255.255.255.0 的未经 NAT 的封包通过。
2. 设置传入防火墙规则来允许自 192.168.1.0/255.255.255.0 至 192.168.2.0/255.255.255.0 的未经 NAT 的封包通过。

表 10.8 与表 10.9 所述是传出与传入防火墙规则栏位需设置的参数。若要了解设置传入/传出防火墙规则的详细内容，请参考 9.3 与 9.4 章节的说明。

表 10.8. ISR2 上 VPN 封包的传出未转译防火墙规则

栏位		设置值
Source IP	Type	Subnet
	Address	192.168.2.0
	Mask	255.255.255.0
Destination IP	Type	Subnet
	Address	192.168.1.0
	Mask	255.255.255.0
NAT		None
Action		Allow
VPN		Enable



传出未转译防火墙规则需添加已存在的规则 ID 1001。

表 10.9. ISR2 上 VPN 封包的传入未转译防火墙规则

栏位		设置值
Source IP	Type	Subnet
	Address	192.168.1.0
	Mask	255.255.255.0
Destination IP	Type	Subnet
	Address	192.168.2.0
	Mask	255.255.255.0
NAT		None
Action		Allow
VPN		Enable

10.5.1.3 建立隧道 (Tunnel) 并检查

- 连续地从 ISR1 下局域网内的主机 ping ISR2 下局域网内的主机。最初的几次 ping 可能会失败。但数秒钟后，ISR1 下局域网内的将开始收到 ping 回复。

10.5.2 外部网络 - 防火墙 + 静态 NAT + VPN

在外部网络环境中，受路由器保护的网路可以具有不同的管理权限。因此，可能有两外部网络个网络的 IP 地址位于同一个子网下。典型的外部网络结构如图 10.6 所示。

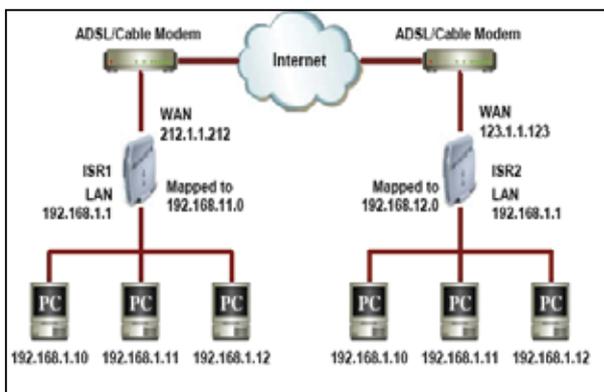


图 10.6. 典型的外部网络图

 ISR1 与 ISR2 路由器下的网络都为 192.168.1.0/255.255.255.0。

为避免这类环境中的路由问题，网络 IP 地址必须映射为不同的：

- ISR1 下的网络 192.168.1.0/255.255.255.0 在 VPN 过程的前被转译为 192.168.11.0/255.255.255.0。
- ISR2 下的网络 192.168.1.0/255.255.255.0 在 VPN 过程的前被转译为 192.168.12.0/255.255.255.0。

结果如下：

- 在 ISR2 局域网看来，ISR1 局域网的地址为 192.168.11.0/24。
 - 在 ISR1 局域网看来，ISR1 局域网的地址为 192.168.12.0/24。
- 每个用于外部网络环境的路由器设置包括下面的步骤：
- 设置 VPN 连接规则。
 - 设置防火墙规则，通过一对一 NAT，允许传入与传出 VPN 流量。
 - 设置防火墙自我访问规则，允许 IKE 封包进入 Internet 安全路由器。

10.5.2.1 设置路由器

设置 ISR1

1. 将 ISR1 的 LAN 端口 IP 地址设置为 192.168.1.1。
2. 设置 ISR1 的 DHCP 地址池为 192.168.1.10 至 192.168.1.110。
3. 将 ISR1 的 WAN 端口 IP 地址设置为 212.1.1.212。
4. 在 ISR1 上新增路由，网关设置为 123.1.1.123。
5. 保存设置。

设置 ISR2

1. 将 ISR2 的 LAN 端口 IP 地址设置为 192.168.1.1。
2. 设置 ISR2 的 DHCP 地址池为 192.168.1.10 至 192.168.1.110。
3. 将 ISR2 的 WAN 端口 IP 地址设置为 212.1.1.213。
4. 在 ISR2 上新增路由，网关设置为 212.1.1.212。
5. 保存设置。

10.5.2.2 设置 ISR1 的 VPN 规则

步骤 1: 设置 VPN 规则

请参考 10.3 用自动密钥建立 VPN 连接 的说明，用下列地址来用自动密钥设置 ISR1 的 VPN 连接策略：

1. 本地安全群组 (Local Secure Group) 地址：192.168.11.0/255.255.255.0。
2. 远程安全群组 (Remote Secure Group) 地址：192.168.12.0/255.255.255.0。

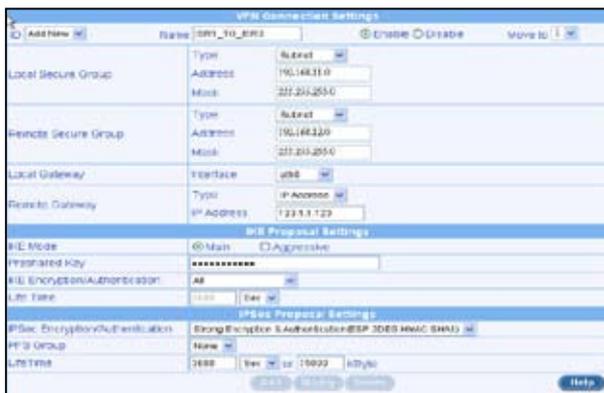


图 10.7. 外部网络范例 - ISR1 的 VPN 策略设置

步骤 2: 设置静态 NAT 地址池

1. 设置传出静态 NAT 地址池（静态 NAT），将范围为 192.168.1.1-192.168.1.254 的 IP 地址转译为 192.168.11.1-192.168.11.254。



图 10.8. 外部网络范例 - ISR1 传出 NAT 地址池设置

2. 设置传入静态 NAT 地址池（反向静态 NAT），将范围为 192.168.11.1-192.168.11.254 的地址转译为 192.168.1.1-192.168.1.254。



图 10.9. 外部网络范例 - ISR1 的传入 NAT 地址池设置

步骤 3: 设置外部网络访问规则

1. 设置传出防火墙规则，在传出封包进行 VPN 的前，将封包的来源 IP 地址从 192.168.1.x 范围映射至 192.168.11.x（由传出 NAT 地址池决定）范围。



图 10.10. 外部网络范例 - ISR1 的传出 ACL 规则

2. 设置传入防火墙规则，在传入封包执行 VPN 后，将封包的目的地 IP 地址从 192.168.11.x 范围映射至 192.168.1.x（由传入 NAT 地址池决定）范围。

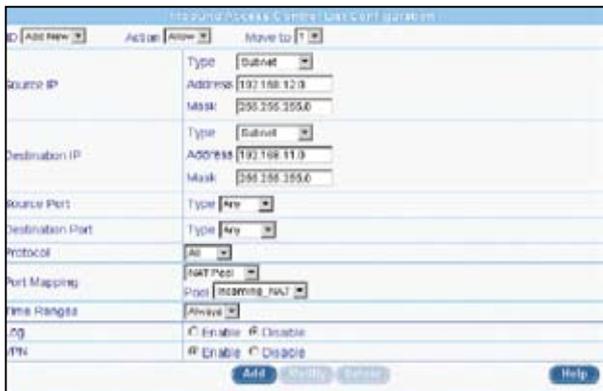


图 10.11. 外部网络范例 - ISR1 的传入 ACL 规则

10.5.2.3 设置 ISR2 的 VPN 规则

步骤 1: 设置 VPN 规则

请参考 10.3 用自动密钥建立 VPN 连接 的说明，用下列地址来用自动密钥设置 ISR2 的 VPN 连接策略：

- 1.本地安全群组(Local Secure Group)地址：192.168.12.0/255.255.255.0。
- 2.远程安全群组(Remote Secure Group)地址：192.168.11.0/255.255.255.0。

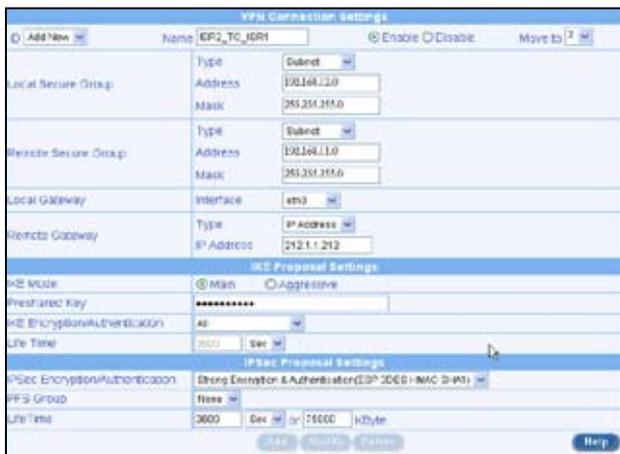


图 10.12. 外部网络范例 - ISR2 的 VPN 策略设置

步骤 2: 设置静态 NAT 地址池

1. 设置传出静态 NAT 地址池（静态 NAT），将范围为 192.168.1.1-19 2.168.1.254 的 IP 地址转译为 192.168.12.1-192.168.12.254。

NAT Pool Configuration	
Add New Pool	
Name	Outgoing_NAT
Pool Type	Static
Original IP	Start IP: 192.168.1.1 End IP: 192.168.1.254
Mapped IP	Start NAT IP: 192.168.12.1 End NAT IP: 192.168.12.254
<input type="button" value="Add"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>	

图 10.13. 外部网络范例 - ISR2 传出 NAT 地址池设置

2. 设置传入静态 NAT 地址池（反向静态 NAT），将范围为 192.168.12.1-192.168.12.254 的地址转译为 192.168.1.1-192.168.1.254。

NAT Pool Configuration	
Add New Pool	
Name	Incoming_NAT
Pool Type	Static
Original IP	Start IP: 192.168.12.1 End IP: 192.168.12.254
Mapped IP	Start NAT IP: 192.168.1.1 End NAT IP: 192.168.1.254
<input type="button" value="Add"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>	

图 10.14. 外部网络范例 - ISR2 的传入 NAT 地址池设置

步骤 3: 设置外部网络访问规则

1. 设置传出防火墙规则，在传出封包进行 VPN 的前，将封包的来源 IP 地址从 192.168.1.x 范围映射至 192.168.12.x（由传出 NAT 地址池决定）范围。

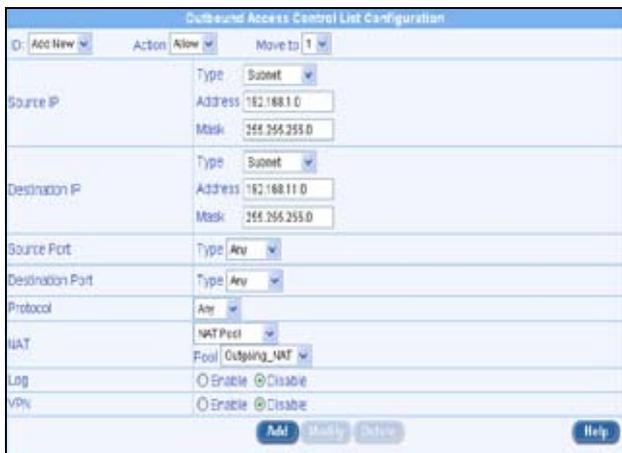


图 10.15. 外部网络范例 - ISR2 的传出 ACL 规则

2. 设置传入防火墙规则，在传入封包执行 VPN 后，将封包的目的地 IP 地址从 192.168.12.x 范围映射至 192.168.1.x (由传入 NAT 地址池决定) 范围。

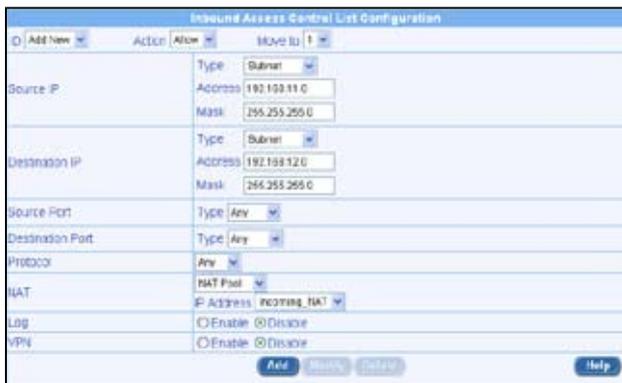


图 10.16. 外部网络范例 - ISR2 的传入 ACL 规则

10.5.2.4 建立隧道 (Tunnel) 与检查

- 从 ISR1 所在的局域网中的一台主机 ping ISR2 所在的局域网中的一台主机。刚开始的几次 ping 可能会失败。但数秒钟后，ISR1 所在的局域网中的主机将收到 ping 应答。
- 从 ISR2 所在的局域网中的一台主机 ping ISR1 所在的局域网中的一台主机，ping 将会成功。
- 当出现下面情况时，ping 可能会失败：
 - ping 操作中，ISR2 所在局域网 中的主机的 IP 地址不正确。检查并修改为正确的 IP 地址。
 - 未设置 ISR1 或 ISR2 的默认路由。请设置必要的路由。
 - 与 VPN 连接相关的防火墙规则可能未设置正确。若有网络地址未设置正确，请修改参数并套用新的设置。
 - 本地与远程网络地址可能未设置正确。用于 VPN 连接规则的网络地址为 192.168.11.0/255.255.255.0 与 192.168.12.0/255.255.255.0。

第十一章 系统管理

在本章节中将叙述以下您可以使用的设置管理项目：

- 设置系统服务
- 修改密码
- 修改系统信息
- 修改系统日期与时间
- 复位、备份、还原系统设置
- 固件更新
- 登出设置管理界面

您可以从 System Management 功能表中访问这些功能。

11.1 设置系统服务

如图 11.1 所示，您可使用系统服务设置(System Services Configuration)页面来开启或关闭 SL1200 路由器所支持的功能。所有的服务，包括防火墙，VPN，DNS，DHCP 与 RIP，都在出厂时即被开启。要关闭或开启单独的服务，请依照下面的步骤操作：

1. 以管理员的身份登录设置管理界面。点击 System Management -> System Services。此时将出现系统服务设置页面，如图 11.1 所示。
2. 点击 Enable 或 Disable 来开启或关闭相对应的服务。
3. 点击 <Apply> 保存变更。



图 11.1. 系统服务设置页面

11.2 更改登录密码

当您首次登录设置管理界面时，您需要使用默认的用户名称与密码(admin 与 admin)。系统允许两种类型的用户 - 管理员 (用户名称: admin) 与 访客 (用户名称: guest)。

管理员 有权力修改系统设置，而 访客 只能查看这些设置。管理员与访客帐号的密码都可由管理员修改。



此用户名称与密码只用于登录设置管理界面，与您连接至 ISP 所使用的登录密码不同。



图 11.2. 密码设置界面

密码设置页面可让您更改管理员或访客的密码。请依照下列步骤更改密码：

1. 以管理员身份登录设置管理界面，点击 System Management 菜单，接着点击 User Account 子菜单。此时将出现 User Account Configuration 页面如图 11.2 所示。
2. 输入用户名称与密码。
3. 在 New Password 栏位输入新密码，接着在 Confirm New Password 栏位再输入一次以确认。
密码最长可为 16 位。当登录时，您必须输入这里输入的新密码，且大小写须一致。
4. 点击 <Apply> 按钮保存新密码。

11.3 修改系统信息

如图 11.3 所示，您可以使用系统信息设置页面来输入特定的信息，如系统名称（此设备的唯一名称），系统位置（设备所在的位置），以及此设备的联系人信息。所有的栏位都只能使用字母。当您输入了系统信息后，请点击 <Apply> 保存变更。



图 11.3. 系统信息设置页面

11.4 设置日期与时间

本路由器可保持对当前日期与时间的记录，用来计算与报告各种性能参数的变化。



图 11.4. 日期与时间设置页面

SL1200 路由器内部没有即时时钟。系统日期与时间由外部网络时间服务器来保持。此页面内可设置的栏位只有“Time Zone”，时间服务器的 IP 地址与需要的更新间隔。从“Time Zone”下拉式菜单中选择您所在的时区，如过需要，更改时间服务器的 IP 地址以及更新间隔，接着点击 <Apply> 按钮保存这些变更。

11.4.1 查看系统日期与时间

查看已更新的系统日期与时间

1. 以管理员身份登录设置管理界面。点击 System Management -> Date/Time Setup。此时将出现日期/时间设置 (Date/Time Configuration) 页面，如图 11.4 所示。
2. 点击 <Apply> 即可查看已更新的日期与时间。

11.5 SNMP 设置

简易网络管理协议 (SNMP) 用来管理网络。您可以用 SNMP 设置页面来开启或关闭对 SNMP 的支持。

11.5.1 SNMP 设置参数

表 11.1 所示为 SNMP 设置中可用的参数。

表 11.1. SNMP 参数设置

栏位	说明
SNMP	点击 Enable 或 Disable 按钮来开启或关闭 SNMP 功能。
RO Community Name	Community string 是一串明显的字串，用在 SNMP 管理站与 SL1200 的间的密码。“仅提供读取”(Read Only, RO) community name 是让 SNMP 管理站用来接收 SL100 的设置。
RW Community Name	Community string 是一串明显的字串，用在 SNMP 管理站与 SL1200 的间的密码。“提供读取与写入”(Read and Write, RW) community name 是让 SNMP 管理站用来读取和分配 SL1200 的设置。
Trap Address	Trap message (trap 信息) 是 SL1200 传送给 SNMP 管理站，并告诉它路由器上所发生的状况。在此栏中输入 SNMP 管理站的 IP 地址，则用来接收从 SL1200 发送来的 trap 信息。

11.5.2 设置 SNMP

1. 点击 System Management -> SNMP 菜单，进入 SNMP 设置页面。
2. 点击 Enable 或 Disable 按钮来开启或关闭 SNMP 功能。
3. 输入 RO (仅供读取)，以及 RW (可读可写入)。
4. 输入用来接收 SL1200 传送来的 trap 信息的 SNMP 管理站的 IP 地址。
5. 点击 <Apply> 按钮保存设置值。您可以在显示于设置页面下方的既有设置表中检查您的设置。

SNMP Configuration	
SNMP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
RO Community Name	public
RW Community Name	private
Trap Address	
<input type="button" value="Apply"/> <input type="button" value="Help"/>	

图 11.5. SNMP 设置

11.6 系统设置管理

SNMP Configuration	
SNMP	Disable
RO Community Name	public
RW Community Name	private
Trap Address	

图 11.6. 既有的 SNMP 设置

11.6.1 复位系统设置

有时候会遇到为了解决因不正确的设置而引起的问题，而想将系统设置的参数还原到出厂默认值。

如何复位系统设置

1. 以管理员身份登录设置管理界面。点击 System Management -> Configuration -> Default Settings。此时将出现出厂默认值设置 (Default Settings Configuration) 页面，如图 11.7 所示。
2. 点击 <Apply> 将系统设置恢复为出厂默认值。SL1200 将重新启动，以使出厂设置生效。

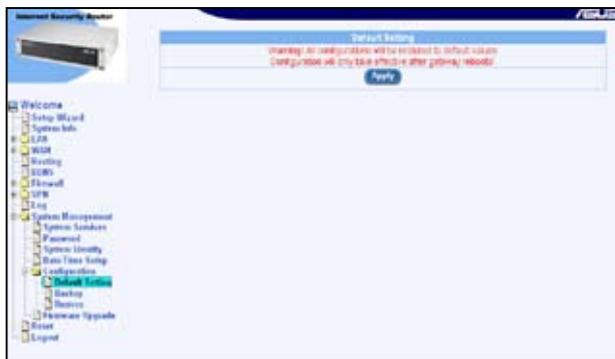


图 11.7. 默认值设置页面

有时，您可能发现您无法访问 SL1200 路由器，譬如您忘记了密码。解决此类问题的唯一途径就是复位系统设置，将其恢复到出厂默认值。

如何复位路由器

1. 将 SL1200 电源关闭，接着等待至少五秒钟。
2. 重新开启 SL1200，等待至少五秒钟，接着按下路由器的复位按钮。约五秒钟后，您将看到 Alarm LED 闪烁一次。
3. 当您看见 LED 闪烁一次后，再次按下复位按钮。约五秒钟后，您将看到 Alarm LED 闪烁两次。这代表 SL1200 路由器将要恢复到出厂设置。若此刻您改变主意，您可以再次按下复位按钮或将路由器电源关闭，以取消这一操作。

11.6.2 备份系统设置

如何备份系统设置

1. 以管理员身份登录设置管理界面。点击 System Management -> Configuration -> Backup。此时将出现备份设置 (Backup Configuration) 页面，如图 11.8 所示。
2. 点击 <Apply> 备份系统设置。

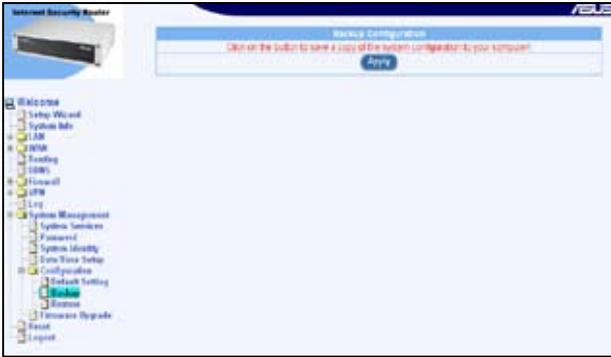


图 11.8. 备份系统设置页面

11.6.3 恢复系统设置

如何恢复系统设置

1. 以管理员身份登录设置管理界面。点击 System Management -> Configuration -> Restore。此时将出现恢复设置 (Restore Configuration) 页面，如图 11.9 所示。



图 11.9. 恢复系统设置页面

2. 在 Configuration File 栏输入想要恢复的系统设置文件的路径与名称。或者，您可以点击 <Browse> 来在您的硬盘中搜寻设置文件。此时将出现如图 11.10 的画面，让您选择需要恢复的设置文件。

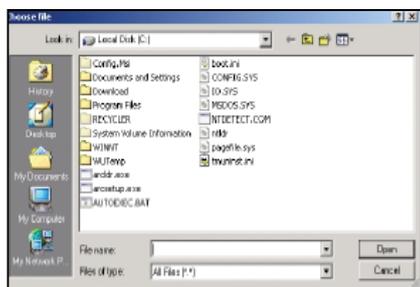


图 11.10. Windows 文件浏览

3. 点击 <Apply> 恢复系统设置。SL1200 路由器将会重新启动，以使用系统设置生效。

11.7 固件升级

华硕将不定期地为您提供 SL1200 固件升级。所有系统软件都包含在一个单一文件中，称为固件镜像。设置管理界面提供了一个简易的方式来上载新的固件镜像。若要升级固件，请依照下面的步骤操作：



图 11.11. 固件升级页面

1. 以管理员身份登录设置管理界面。点击 System Management -> Firmware Upgrade。此时将出现固件升级 (Firmware Upgrade) 页面，如图 11.11 所示。

2. 在 Firmware 栏位，输入固件镜像文件的路径与名称。或者，您可以点击 <Browse> 来在您的硬盘中搜寻固件镜像文件。
3. 点击 <Apply> 当开始升级固件。这可能需要花费 5 分钟时间。当升级完成后，SL1200 将会重新启动以使新固件生效。

11.8 复位 SL1200 路由器

若要复位 SL1200 路由器，请在设置管理界面的 Reset 页面点击 <Apply> 按钮。



图 11.12. 设置管理界面复位页面

11.9 登出设置管理界面

若要登出设置管理界面，请在 Logout 页面点击 <Apply> 按钮。若您使用了 IE 浏览器，在关闭的前，您会看到如图 11.14 所示的窗口。

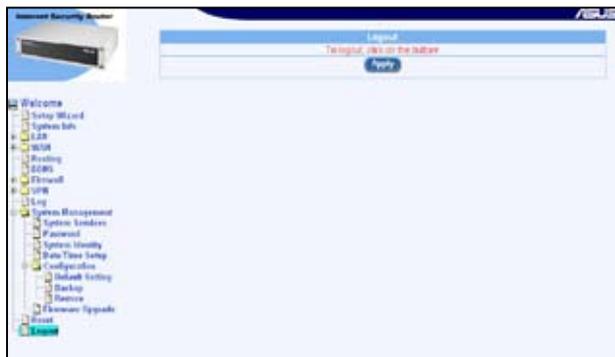


图 11.13. 设置管理界面登出页面



图 11.14. 确认关闭浏览器 (IE)

第十二章 ALG 设置

表 12.1 列出了所有支持的 ALG (应用层网关)。

表 12.1. 支持的 ALG

ALG/应用名称	协议与端口	默认服务名称	已测试软件版本
PCAnywhere	UDP/22	P C ANYWHERE	pcAnywhere 9.0.0
RTSP-554	TCP/554	RTSP554	RealPlayer 8 Plus
	UDP/53	DNS	QuickTime Version 6
	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
	TCP/80	HTTP	5.0.0.043
	UDP/53	DNS	
Netmeeting	TCP/1720	H323	
	UDP/53	DNS	
Netmeeting with ILS	TCP/1720	H323	Windows Netmeeting
	TCP/389	ILS	Version 3.01
	UDP/53	DNS	Opengk Version 1.2.0

ALG/应用名称	协议与端口	默认服务名称	已测试软件版本
Netmeeting with GK	TCP/1720	H323	Windows Netmeeting Version 3.01
	UDP/1719	H323GK	
	UDP/53	DNS	Opengk Version 1.2.0
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	
Security ALGs			
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	
Chats			
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	

ALG/应用名称	协议与端口	默认服务名称	已测试软件版本
Chats			
MSIM	TCP/1863	MSN	MSN Messenger Service Version 3.6.0039
	TCP/80	HTTP	
	UDP/53	DNS	
Games			
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 (Gaming Zone)	TCP/47624	MSG1	Age of Empires, Gold Edition
	TCP/28801	MSN-ZONE	
	TCP/443	HTTPS	
	TCP/80	HTTP	
	UDP/53	DNS	
Diablo II (BATTLENET- TCP, BATTLENET- UDP)	TCP/4000	DIABLO-II	DIABLO II
	TCP/ 6112	BATTLE-NET- TCP, BATTLE- NET-UDP	
	UDP/53	DNS	
	UDP/6112	Diablo II	

ALG/应用名称	协议与端口	默认服务名称	已测试软件版本
Chats			
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	Internet 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	

第十三章 IP 地址、网络掩码与子网

13.1 IP 地址



本节叙述仅关于 *Ipv4 地址 (version 4 of the Internet Protocol)* 的范围，内容并未涵盖 *Ipv6 地址*。在本章节中，我们假设您已经掌握了一些基本知识，如二进制数字、比特与字节有初步的认识。

IP 地址，Internet 版本的电话号码，是用来确认 Internet 上独立的节点（电脑或是其他设备）。每一组 IP 地址包含四组数字，而每一组数字可由 0 到 255，并以点分隔，如 20.56.0.211。这些号码的阅读方式是由左至右，第一栏位、第二栏位、第三栏位、第四栏位。

书写 IP 地址的方式，如由点所分隔的十进制数字被称作十进制表示法。而 IP 地址为 20.56.0.211 在阅读上便读作“二十点五十六点零点二一一”。

13.1.1 IP 地址结构

IP 地址有一种类似电话号码的的分级设计。例如，一组 7 位数字的电话号码起始于一组三位数字的号码，这组号码是用来由上千条电话线中进行确认之用。而其他四位数字则是用来确认是该群组中的哪一条特定电话线之用。

简单来说，一组 IP 地址含有两种信息。

- **网络 ID**
在Internet或内部网络中标示一特定网络
- **主机 ID**
在网络中标示一特定的电脑或设备

每个 IP 地址的第一部分包含网络 ID，并且其余地址包含主机 ID。

网络 ID 的长度取决于网络的种类（参考以下的章节）。表 13.1 所示为 IP 地址的结构。

表 13.1. IP 地址结构

类别	Field1	Field2	Field3	Field4
A 类	网络 ID	主机 ID		
B 类	网络 ID		主机 ID	
C 类	网络 ID			主机 ID

以下是一些有效的 IP 地址范例：

A 级：10.30.6.125 (网络= 10，主机= 30.6.125)

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

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

13.2 网络类别

常被使用的三种网络类别分别为 A、B 与 C 类（此外尚有一种 D 类，但属于特殊使用范围，不在本节的讨论中）。这些类别具有不同的用途与特性。

A 类网络是 Internet 中范围最大的网络，其中每个网络有超过 1600 万部主机。而此类别的网络最高可存在 126 个，约等于二十亿部主机。由于其巨大的容量，这些网络多用于广域网（WAN）环境，并被组织为 Internet 中的基础类别，例如您的 ISP。

B 类网络在范围上较 A 级更小但范围仍然十分庞大，每个网络可以有超过 65,000 部的主机。而此类别的网络最高可存在 16,384 个。一个 B 级网络可能为较大的组织如商业或政府机构所采用。

C 类网络是三种网络类别中最小的，最多只能容纳 254 部主机，但此类别的网络可存在超过 2 百万个（正确地说是 2,097,152）。连接至 Internet 的局域网大多属于 C 类网络。

关于 IP 地址的一些重要记注：

- 可由第一栏位（field 1）轻易决定的类别：
 - field1 = 1-126: A 类
 - field1 = 128-191: B 类
 - field1 = 192-223: C 类
 （未显示的 field1 数值是为特别用途保留）
- 一主机 ID 可以具有除了所有栏位皆设为 0 或 255 以外的数值，因为这些数值是有其特殊用途的。

13.3 子网掩码



网络掩码看起来像普通的 IP 地址，但实际上它包含了一系列的比特表示 IP 地址的哪个部分是网络 ID，哪些是主机 ID：比特为 1 表示“这是网络 ID”，0 表示“这是主机 ID”。

子网掩码是被用来定义子网（就是您将网络分为较小的片段）。一组子网的网络 ID 通过向主机 ID 地址的一部份“借”一个或更多位。子网标示这些主机 ID 位。

例如，一 C 级网络 192.168.1。将其分做两个子网，您会使用以下的子网掩码设置：255.255.255.128。如果我们以二进制方式书写将更容易了解其意义：

```
11111111. 11111111. 11111111.10000000
```

就像 C 类地址一样，field1 到 field 3 都是网络 ID，但是请注意 field 4 中第一个比特同样也被包括到了网络 ID 中。由于额外的比特只有两种值 (0 和 1)，就表示网络有两个子网，每个子网使用剩余的 7 比特作为其主机 ID，范围是 0 到 127 (而不是原来的 0 到 255 的 C 类地址)。

相似的，要将一个 C 类网络分为 4 个子网，掩码就是：

```
255.255.255.192 或 11111111. 11111111. 11111111.11000000
```

Field 4 中额外的两个字节可以有 4 个值(00, 01, 10, 11)，因此产生了 4 个子网。每个子网使用剩余的 6 比特作为其主机 ID，范围是 0 到 63。



一些子网掩码并不表示额外的网络 ID 位，因此也没有子网产生。这样的掩码称为默认子网掩码，这些掩码是：

A 类：255.0.0.0

B 类：255.255.0.0

C 类：255.255.255.0

这些称做默认掩码是因为网络在没有子网存在的时候已经配置完毕。

第十四章 疑难排解

本附录将列出您在安装或使用 SL1200 时可以遭遇到的问题的解决建议。此外，也将提供使用几个 IP 工具来诊断问题的介绍。

若以下的问题解决建议无法解决您的问题，请与本公司的客户支持部门联系。

表 14.1. 问题与建议解决方法

问题	建议解决方法
LED	
当电源开启后，电源 LED 灯并未亮起。	请确认您是使用 AC 电源适配器来供给设备电源，并确认电源适配器一端已连接到 SL1200，而另一端则连接到室内电源插座或电源延长线。
当连接以太网线后，Link WAN LED 灯未亮起。	请确认以太网线的一端紧密连接到您的 ADSL 或 Cable 调制解调器的以太网端口，而另一端则紧密地接到 SL1200 的 WAN 端口。接着请确认您的 ADSL 或 Cable 调制解调器的电源已开启。请等待 30 秒钟来让 SL1200 与您的宽带调制解调器建立连接。
当连接以太网线后，LINK LAN LED 灯未亮起。	确认以太网线已紧密连接到您局域网的集线器或 PC，并连接到了 SL1200。并确认 PC 与集线器的电源已开启。 确认您所使用的以太网线符合您的网络传输需求。100Mbit/sec 的网络（100BaseTx）应该使用标示 Cat.5 的网络线缆。若使用 10Mbit /sec 的网络连接则可以使用较低传输品质的网络线缆。

问题	建议解决方法
Internet 访问	
PC无法连接到Internet	<p>使用在下一节中会讨论到的 ping 工具来检查您的 PC 是否可以连接到 SL1200 的局域网 IP 地址 (默认值: 192.168.1.1)。若无法连接, 请检查您的网络线缆。</p> <p>如果您把私人 IP 地址静态配发到电脑 (未注册的公开网络地址), 请检查以下几点:</p> <ul style="list-style-type: none"> • 检查电脑上的网关 IP 地址是您公开对外的 IP 地址 (请参考快速安装指南中第二章第二部分关于查看 IP 信息的介绍)。若设置并非如此, 请更正该地址或设置您的 PC 来自动接收 IP 信息。 • 请与您的 ISP 确认分配给 PC 使用的 DNS 服务器地址是有效的。请更正该地址或设置自动接收该项信息。 • 请确认 SL1200 中的网络地址转译规则已正确设置, 以便正确转译由您内部私人 IP 位置至对外公开的 IP 地址。而配发 IP 地址必需符合 NAT 规则中特定的范围。或是, 也可以设置 PC 来接收由其他设备所配发的地址 (请参考 3.2 “第二部分 — 设置您的电脑” 一节中的相关介绍)。在默认值中, 包含有一 NAT 规则用以在默认地址池中动态分配地址的功能。
PC 无法显示 Internet 的网页内容。	<p>确认您的 ISP 所提供的 DNS 服务器地址是有效的且已正确设置在您的电脑中。您可以使用下一节中将讨论的 ping 工具来测试您电脑与 ISP 的 DNS 服务器间的连接。</p>

问题	建议解决方法
设置管理界面程序	
你忘记/遗失您在设置管理界面中的用户名或密码。	若您不曾变更默认的用户名称与密码，试着在用户名与密码的栏位输入 “admin” 与 “admin”。否则，您可以依照 11.5.1 节中的介绍，将设备复位到出厂默认值。警告：复位动作将会一并清除所有先前的设置，并恢复到出厂默认值。
无法由您的浏览器进入设置管理界面程序。	<p>使用在下一节中，将介绍的 ping 工具来检查您的 PC 与 SL1200 的局域网端口（默认值：192.168.1.1）间的连接是否正常。若无法连接，请检查以太网线缆是否正常。</p> <p>确认您是使用 Internet Explorer 5.5，Netscape 7.0.2 或者更新版本的浏览器软件。您的浏览器必需支持 Javascript，且浏览器也可能需要支持 Java。</p> <p>确认 PC 的 IP 地址与 SL1200 的局域网端口是在同一子网环境中。</p>
在设置管理界面所做的设置变更未被保留。	请确定设置后已点击 <Apply> 按钮来保存变更的设置值。

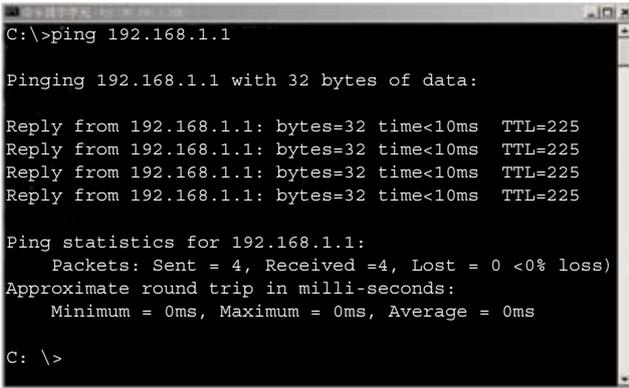
14.1 使用 IP 工具诊断问题

14.1.1 封包探测 (Ping)

封包探测 (Ping) 是您可以用来检查您的 PC 是否可以辨识局域网或 Internet 中电脑的一项指令。封包探测指令会传送信息至您所指定的电脑主机，若该电脑接收到信息，便会传回一回复信息。若要使用这项指令，您必需知道您试图连接的电脑的 IP 地址。

在使用 Windows 操作系统的电脑上，您需要从开始菜单中运行封包探测指令。请点击 **开始** 菜单按键，接着请点击“运行”。在接下来的文字选项中，请依照以下例子进行输入：Ping 192.168.1.1 点击 <OK>。此外，您也可以使用任何其他局域网的 IP 地址或您知道的 Internet IP 地址，来进行封包探测的测试。

若目标电脑接收到信息，则如图 14.1 所示的指令提示窗口会显示出来。



```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<10ms TTL=225

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received =4, Lost = 0 (0% loss)
    Approximate round trip in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C: \>
```

图 14.1 使用封包探测工具

若封包探测所送出的信息不能到达目标电脑，则您将会收到“Request timed out”的信息。

通过使用封包探测工具，您可以测试 SL1200 的连接路径（使用默认的局域网 IP 地址：192.168.1.1 进行探测）或其他您所分配的地址是否连接正常。

你也可以通过输入其他外部的 IP 地址来测试 Internet 的连接是否正常。举例来说，您可以输入 www.yahoo.com (216.115.108.243) 来进行测试。若您不知道特定 Internet 地址的 IP 地址，您则可以使用下一节中会介绍的 nslookup 指令进行测试。

以大多数启用 IP 功能的操作系统，您可以通过系统管理工具来运行相同的封包探测指令。

14.1.2 nslookup

您可以使用 nslookup 指令来决定与 Internet 网站名称相对应关连的 IP 地址。您可指定一般名称，接着 nslookup 指令会在您的 DNS 服务器中搜寻该名称（通常会保存于您的 ISP 服务器中）。若该登录无法在您 ISP 的 DNS 服务器中找到，则该要求会被中继到更高等级的服务器，以此类推，直到该登录被搜寻到为止。搜寻到的后，服务器接着会回复该登录的对应 IP 地址。

在使用 Windows 操作系统的电脑上，您需要从开始菜单中运行 nslookup 指令。请点击 **开始** 菜单按键，接着请点击“**运行**”。在接下来的文字选项中，请依照以下例子进行输入：

```
nslookup
```

输入完毕请点击 <OK>。接着一个包含 (>) 符号的命令提示窗口会出现。在此一命令提示窗口中输入您感兴趣的 Internet 地址名称，例如：www.absnews.com。

接着窗口会如图 14.2 所显示相关联的 IP 地址。



```
C:\>nslookup
Default Server: tp-dc-01.corpnet.asus
Address: 192.168.28.68

> www.abcnews.com
Server: tp-dc-01.corpnet.asus
Address: 192.168.28.68

Name: www.abcnews.com
Address: 204.202.132.19
Aliases: www.abcsnew.com

>
```

图 14.2. 使用 nslookup 工具

以同一 Internet 名称来说，可能有好几个相对应的地址。这对于传输量大的网站来说是很正常的现象，因为这些网站采用多重、备份服务器来传送相同的信息。

如要退出 nslookup 程序，请在指令提示列输入 exit 并按下 <Enter> 即可。

第十五章 术语表

10BASE-T	用于以太网的有线线缆，数据传输率为 10Mbps。亦称 3 类线 (CAT 3)。参见 data rate, Ethernet。
100BASE-T	用于以太网的有线线缆，数据传输率为 100Mbps。亦称 5 类线 (CAT 5)。参见 data rate, Ethernet。
1000BASE-T	用于以太网的有线线缆，数据传输率为 1000Mbps。
binary	二进制。“基于2”的数字系统，只使用 0 和 1 两个数字来表示所有的数字。在二进制中，十进位数字 1 写作 1，十进位数字 2 写作 10，十进位数字 3 写作 11，十进位数字 4 写作 100，依次类推。虽然 IP 地址为方便起见表示为十进位数字，实际上它使用的是二进制数字。比如 IP 地址 209.191.4.240 转换为二进制是 11010001.10111111.00000100.11110000。比特，IP 地址，网络掩码同样也是二进制。
bit	比特。“二进制数字”的缩写，一个比特就是一个只有 0, 1 两种数值的数字。参见 binary。
bps	比特每秒
CoS	服务等级。在 802.1Q 中规定，值的范围为 0 到 7。
DSCP	差分服务代码点 IP 报头中差分服务部分最重要的六位被称为 DSCP。GigaX 系列中可用的 DSCP 值有 0, 8, 10, 16, 18, 24, 26, 32, 34, 40, 46, 48 和 56。
broadcast	广播。将数据发送到网络上所有的电脑。
Ethernet	以太网。最常见的电脑网络技术，通常使用双绞线。以太网的数据传输速率为 10Mbps 和 100Mbps。参见 10BASE-T, 100BASE-T, twisted pair。
FTP	文件传输协议 用于连接到 Internet 的电脑之间的文件互传。常见的用途包括上传或更新网页服务器上的文件，从网络服务器下载文件。
host	主机。连接到网络的设备(通常指电脑)。
ICMP	互联网控制信息协议 一种互联网协议，用于报告错误与其他网络相关信息。ping 命令就是基于这种协议。

IGMP	互联网群组管理协议 一种互联网协议，允许电脑与其网络成员通过组播群组共用信息。一个电脑组播群组就是群组的成员都设置成从成员处接收特定的内容信息。向IGMP群组传送组播的应用可随时更新群组的地址簿或将公司的通告传送到收信人列表。
IGMP Snooping	在每个端口侦听IGMP封包并将端口与二层组播群组相关联。
IP	参见 TCP/IP。
mask	掩码。参见 network mask。
Multicast	组播。将数据传送到一组网络设备上。
Mbps	百万比特每秒的缩写。网络数据传输率常表示为Mbps。
Monitor	监控。亦称“Roving Analysis”，允许将一个网络分析器连接至端口上并使之监测交换机的其他端口。
network	网络。指连接在一起，允许相互通信和共用资源（如软件、文件等）的一组电脑。网络可以是小型的，例如局域网(LAN)，也可以是大型的，例如互联网。
network mask	网络掩码。网络掩码就是一系列的比特字符串用于IP地址，以决定网络ID和主机ID的位数。1 表示此位有效，0表示忽略此比特。举例说明，如果网络掩码 255.255.255.0 用到IP地址100.10.50.1，网络ID为100.10.50，主机ID为 1。参见 binary, IP address, subnet, “IP Addresses Explained” 部分。
NIC	网络接口卡 插入电脑，提供网络线缆的物理接口RJ-45 的适配器。参见Ethernet，RJ-45。
packet	封包，在网络上传输数据的单位。每个封包都包含数据、添加的信息，如它从哪里来（来源地址）及将到哪里去（目的地地址）。
ping	封包探测 用于确认IP 地址对应的主机是否能够到达。它亦可用于寻找与域名相对应的 IP 地址。
port	端口。物理的网络设备接入点，如电脑，路由器，数据通过该接入点流入流出。
protocol	协议。一系列用于控制数据传输的规则。为了使数据能够成功传输，数据传输来源和目标都必须遵守相同协议的规

	则。
PVLAN	私有虚拟局域网
remote	远程。即物理上处于不同地点。比如说，一名职员出差在外时登录公司的 intranet, 他就是远程用户。
RJ-45	注册端口标准45 这种 8-pin 的插头是用于在电话在线传输数据的。以太网线通常也会使用这种插头。
RMON	远程监控 SNMP 的延伸，提供综合性的网络监视功能。
routing	路由。在您的网络和互联网之间，根据来源IP地址和网络情况，选择最有效的路径转发封包。执行路由选择的设备称为路由器。
SNMP	简单网络管理协议 用于管理网络的 TCP/IP 协议。
STP	生成树协议 防止封包在复杂网络中造成回路的桥接协议。
subnet	子网。子网是网络的一部分，子网通过将网络中的电脑归分为小组而使这些电脑与其他网络上的电脑分隔开来。子网中的电脑仍然在物理上与其他上层网络相连，但是他们被认为是一个独立的网络。参见network mask。
subnet mask	子网掩码。将子网之间加以区分的掩码。参见network mask。
TCP	参见 TCP/IP。
TCP/IP	传输控制协议/互联网协议 这是互联网上基本的协议组。TCP负责将数据分为可以在互联网上传输的封包，IP负责将这些封包传送到目的地。当 TCP 和 IP 与一些上层应用进行捆绑如 HTTP, FTP, Telnet等，TCP/IP 指的是整套协议组。
Telnet/SSH	一种互动的，以字符为基础的，用于访问远程电脑的程序。HTTP (网络协议)和 FTP 只允许从远程电脑下载文件，而 Telnet/ SSH 允许从远程登录并使用电脑。
TFTP	小型文件传输协议 一种传输文件的协议。TFTP 比 FTP 更加容易使用，但是性能和安全性不如 FTP。

Trunk	两个或两个以上的端口合而为一成为一个虚拟端口，也称为链路汇聚。
TTL	存活时间 IP 封包的一个栏位，决定了该封包的寿命。TTL 原本表示的是持续时间，现在则通常用于表示最大计跳数，每经过一跳都消耗一个计跳数，当 TTL 为零时，该封包就被丢弃。
twisted pair	双绞线。即普通的铜制电话线。它包含一对或多对互相缠绕的电线，以消除干扰和杂音。每根电话线使用一对线，在家用情况下，通常都安装两对。对于以太网局域网，使用的是一种高端的，用于10BASE-T网络的三类线(CAT 3)，以及更高端的100BASE-T 网络的五类线 (CAT 5)。参见 10BASE-T，100BASE-T，Ethernet。
upstream	上行。数据从用户流向互联网的方向。
VLAN	虚拟局域网
WAN	广域网 所有的分布于广大的地理位置的网络统称广域网，如一个国家或一个洲。对于交换机来说，广域网指的就是互联网 (Internet)。
Web browser	网页浏览器。一种使用超文本传输协议 (HTTP) 的，用于从网站下载/上传信息的软件。这些信息包括文本，图像，声音或视频。网页浏览器使用了超文本传输协议 (HTTP)。常用的网页浏览器包括 Netscape Navigator 和 Microsoft Internet Explorer。参见 web site。
Web page	网页。一个网站的文件通常包括文本，图像，和连接到其他页面的超链接。当用户访问一个网站时，显示的第一页成为主页。参见 web site。
Web site	网站。互联网上通过网页浏览器为远程用户的提供信息的电脑。网站常由包含文本，图像，超链接的网页构成。参见 web page。