R3000系列 路由器

WEB 管理使用手册 V2.0.0

©copyright 2011 by Shenzhen TG-NET Botone Technology Co.,Ltd. All rights reserved.

事先未征得深圳市万网博通科技有限公司（以下简称 TG-NET）的书面同意，任何人不得以任何方式拷贝或复制本文档中的任何内容。

TG-NET 不做与本文档相关的任何保证，不做商业性、质量或特定用途适用性的任何隐含保证。本文档中的信息随时可能变更，而不另行通知。TG-NET 保留对本出版物做修订而不通知任何个人或团体此类变更的权利。

深圳市万网博通科技有限公司

地址：深圳市龙华镇大浪街道办华荣路鹏腾达工业园 6 栋 2 楼

邮编：518109

服务电话：400-088-7500

网址：http://www.tg-net.cn

目 录

第 1 章 宽带路由器WEB管理系统概述 7
1.1 宽带路由器配置系统概述 7
1.2 WEB配置风格约定 7
1.3 WEB 配置约定 8
1.3.1 列表功能与操作约定 8
1.3.1.1 可操作列表 8
1.3.1.2 只读列表 9
1.3.1.3 排序列表 9
1.3.1.4 可搜索列表 10
1.3.2 通用符号约定 11
1.3.3 键盘操作约定 11
1.3.4 其他表达约定 11
1.3.4.1 特殊字符支持 11
1.3.4.2 配置页面切换方式 11
1.4 出厂配置 12
1.5 系统运行环境 12
1.5.1 硬件环境 12
1.5.2 软件环境 12
1.6 术语与缩略语 12
1.7 功能特性简述 14
1.8 典型应用 16
第 2 章 配置准备 18
2.1 网络设置 18
第 3 章 配置指南 21
3.1 登录WEB管理系统 21
3.2 WEB管理系统主界面 22
3.2.1 系统管理员的界面 22
3.2.2 配置受限用户的界面 22
3.2.3 菜单栏 23
3.2.4 设备面板映射 24
3.2.5 系统运行信息栏 24
第 4 章 首页信息 25
4.1 实时运行信息 25
第 5 章 快速向导 27
5.1 快速上网向导 27
5.1.1 快速上网向导概述 27
5.1.2 向导第 1 步：修改当前用户密码 27
5.1.3 向导第 2 步：配置广域网口参数 28

5.1.4 向导第 3 步：设置上网主机数量 31
5.1.5 向导第 4 步：配置局域网口参数 31
5.1.6 向导第 5 步：设置内网主机IP地址分配方式 32
第 6 章 接口配置 34
6.1 WAN口配置 34
6.1.1 WAN广域网口信息列表 34
6.1.2 WAN广域网口配置 35
6.2 LAN口配置 37
6.2.1 LAN（局域网）口信息列表 37
6.2.2 LAN局域网口配置 38
6.3 工作模式 39
6.3.1 接口工作模式 39
6.3.2 修改接口工作模式 40
6.4 修改MAC 41
6.4.1 接口MAC信息 41
6.4.2 修改MAC地址 41
6.5 端口监控 42
6.5.1 端口监控配置 42
6.6 端口重组 43
6.6.1 端口重组配置 43
第 7 章 多线路策略 45
7.1 线路组合模式 45
7.2 应用调度 45
7.3 线路侦测 46
第 8 章 路由配置 48
8.1 默认路由 48
8.1.1 默认路由信息显示 48
8.1.2 添加或修改默认路由 48
8.2 静态路由 49
8.2.1 静态路由信息显示 49
8.2.2 添加或修改静态路由 50
第 9 章 网络选项 52
9.1 端口映射 52
9.1.1 端口映射 52
9.1.2 特殊映射 53
9.1.3 DMZ主机 54
9.2 时间段配置 54
9.2.1 单次时间段配置 54
9.2.2 循环时间段配置 55
9.3 连接数限制 56
9.3.1 连接数限制全局配置 56
9.3.2 连接数限制个性化配置 56

9.4 NAT访问控制 57
9.4.1 NAT 简介 57
9.4.2 NAT 访问控制 57
9.5 DNS配置 58
9.6 DDNS配置 59
9.7 DHCP配置 60
9.8 PPPOE服务器 61
9.8.1 PPPOE服务端配置信息 61
9.8.2 添加或修改PPPOE服务 61
9.8.3 PPPOE会话信息 63
9.9 UPnP配置 63
9.9.1 启用/停止UPnP服务 63
9.9.2 UPnP NAT映射信息列表 64
第 10 章 ARP安全 66
10.1 ARP手动绑定 66
10.1.1 ARP静态绑定信息列表 66
10.1.2 添加或修改ARP静态绑定配置 66
10.2 ARP扫描绑定 67
10.3 IP+MAC地址过滤 68
10.3.1 “IP+MAC 过滤”列表 68
10.3.2 添加或修改“IP+MAC 过滤”配置 69
第 11 章 网络安全 70
11.1 防火墙配置 70
11.1.1 启用/停止接口防火墙服务 70
11.1.2 查看防火墙规则信息列表 71
11.1.3 添加防火墙规则 72
11.1.4 修改防火墙规则 74
11.1.5 删除防火墙规则 75
11.2 反病毒配置 75
11.2.1 查看反病毒信息列表 75
11.2.2 添加反病毒规则 76
11.2.3 修改反病毒规则 77
11.2.4 删除反病毒规则 77
11.3 URL过滤 78
11.3.1 启用/停止URL过滤服务 78
11.3.2 查看URL过滤规则列表 78
11.3.3 添加URL过滤规则 78
11.3.4 修改URL过滤规则 79
11.3.5 删除URL过滤规则 80
11.4 关键字过滤 80
11.4.1 启用/停止关键字过滤服务 81
11.4.2 查看关键字过滤规则列表 81

11.4.3 添加关键字过滤规则 81
11.4.4 修改关键字过滤规则 82
11.4.5 删除关键字过滤规则 82
11.5 DMZ端口配置 83
11.5.1 DMZ端口配置 83
11.5.2 DMZ区服务配置 84
第 12 章 上网行为管理 85
12.1 全局配置 85
12.1.1 全局功能配置 86
12.1.2 带宽时段控制 87
12.1.3 高级配置 88
12.2 群组管理 90
12.3 优先服务管理 91
12.3.1 游戏优先管理 91
12.3.2 邮件优先管理 91
12.3.3 其它业务优先管理 92
12.4 黑白名单 92
12.5 状态查询 93
第 13 章 虚拟专网 94
13.1 IPSEC配置 94
13.1.1 WAN口的IPSEC列表信息 94
13.1.2 添加或修改WAN口的IPSEC配置 95
13.1.3 查看IPSEC会话信息 97
13.2 PPTP配置 98
13.2.1 PPTP客户端配置信息列表 98
13.2.2 添加或修改PPTP客户端配置 99
13.2.3 PPTP服务器配置信息列表 100
13.2.4 添加或修改PPTP服务器配置 100
13.2.5 PPTP会话信息 102
13.3 L2TP配置 102
13.3.1 L2TP客户端配置信息列表 102
13.3.2 添加或修改L2TP客户端配置 103
13.3.3 L2TP服务器配置信息列表 104
13.3.4 添加或修改L2TP服务器配置 104
13.3.5 L2TP会话信息 106
13.4 IPIP配置 107
13.4.1 IPIP隧道信息列表 107
13.4.2 添加或修改IPIP配置 107
13.5 GRE配置 108
13.5.1 GRE隧道信息列表 108
13.5.2 添加或修改GRE配置 109
13.6 拨号用户管理 110

13.6.1 拨号用户信息列表 110
13.6.2 拨号用户管理配置 110
第 14 章 系统管理 112
14.1 用户管理 112
14.1.1 管理员信息列表 112
14.1.2 添加或修改登录用户密码和权限 112
14.2 时钟管理 113
14.3 软件升级 113
14.3.1 备份IOS软件 114
14.3.2 升级IOS软件 114
14.4 日志管理 114
14.5 远程管理 115
14.5.1 Web管理 115
14.5.2 SNMP管理 116
14.5.3 NAT监控管理 116
14.6 诊断工具 117
14.7 策略库管理 117
14.7.1 策略库在线升级 117
14.7.2 策略库手动升级 117
14.8 重新启动 118
14.9 配置导入导出 118
14.9.1 导出当前配置信息 118
14.9.2 导入配置文件 119
14.10 恢复出厂配置 119
第 15 章 监控信息 120
15.1 端口信息 120
15.2 系统信息 120
15.3 DHCP信息 120
15.4 路由信息 121
15.5 日志信息 121
15.6 连接数监控 122
15.7 行为监控 123
第 16 章 技术支持信息 124
16.1 注意事项 124
附录A 常见问题FAQ 125

第1章　宽带路由器WEB管理系统概述

1.1　宽带路由器配置系统概述

非常感谢您选用本公司的高速智能宽带路由器系列产品。希望本公司系列产品给您带来愉快、安全、稳定的上网体验。

温馨提示：为提高电话服务的效率和质量，请在寻求支持前事先准备好与问题相关的信息，如：网络拓扑连接情况、设备的IP地址分配、登录的用户名/密码、软件版本号、配置使用的功能以及出现问题时的设备或网络的详细表现，规律性等信息，以便支持人员能够迅速定位并解决客户的问题。

注意：本WEB配置说明书是本公司系列宽带路由器的通用说明配置手册，包括了本公司系列宽带路由器的最新配置信息和操作指南。一些相关的配置功能和参数可能因一些路由器型号的差别而有所差别，部分路由器型号可能不支持某些功能配置，所以本手册仅供参考，具体配置信息以实际路由器中的WEB页面配置信息为准。

在进行路由器的配置之前，请确保在您的计算机上安装了必要的软件（Windows 95/98/ME/NT2000/XP）并合理地配置了网络。如不了解如何进行网络配置，请阅读下一节“配置准备”中的设置说明。如已经正确地配置了网络，可以跳过 “配置准备”章节。

提示：

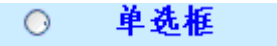
◆通过Web页面配置路由器的配置方式适用于初级技术人员，对于中、高级技术人员也可以通过telnet方式登录路由器进行配置。但切忌同时使用web与telnet进行配置。这样可能造成web页面部分功能无法正常工作，甚至导致路由器的异常！

◆如果使用web配置的方式。在完成配置后网页没有显示出配置的结果，请刷新一下页面（可以按下“F5”功能键等）。没有显示配置结果有多种原因：有可能是您配置的参数错误造成页面显示不正常，或者可能是由于网络问题使得页面未能及时响应配置结果等等。

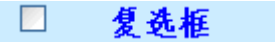
◆如果使用web配置的方式。为了达到最佳的显示效果，推荐使用Microsoft IE浏览器（7.0或以上版本），显示器的分辨率为1024*768。

1.2　WEB配置风格约定

WEB管理界面遵循浏览器的习惯用法，如下图所示 ：

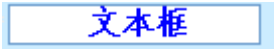


单选框：选中表示只选用此项功能。



复选框：选中代表此项功能被选中。

按钮：单击即执行此项按钮描述的动作。



文本框：用以输入相关参数信息。

下拉框：通过下拉框可以找到供选择的选项。

列表框：通过列表框可以找到供选择或查看的选项或信息。

可输入下拉框：可以输入参数也可以选中供选择的选项。

TAB页选项，可以单击切换同一类别功能的不同配置页面。

1.3 WEB 配置约定

1.3.1 列表功能与操作约定

WEB 配置界面中用到的列表有可操作列表、只读列表、可排序列表和可搜索列表三种类型，其中可搜索列表通常情况下是和前面三种列表组合使用的。下面分别举例进行说明：

1.3.1.1 可操作列表

可操作列表用来显示、修改/查看/详细显示各种配置信息，能够看看、修改、删除列表中的选项。下图是"WAN 广域网口信息列表"的可操作列表，这里以此来说明可操作列表中各参数的含义。

广域网口名称	连接类型	接入IP/掩码	网关地址	最大传输单元	线路ISP/预设带宽	线路状态	操作
WAN0	静态IP接入	172.16.21.43/255.255.255.0	172.16.21.1	1500	中国电信/14M		修改
WAN1	静态IP接入	10.168.12.15/255.255.255.0	10.168.1.1	1500	中国网通/2M		修改

◆**本页2条/共2条**：即本页显示条目/总条目数，图中表示表格共有2条信息记录，当前页面显示了其中2条信息记录。

◆**第1页/共1页**：即当前页序号/总页面数，图中表示表格共有1页，当前显示的是第一页。

◆**第一页**：超链接。单击即可转到第一页。

◆**上一页**：超链接。单击即可转到上一页。

◆**下一页**：超链接。单击即可转到下一页。

◆**最后页**：超链接。单击即可转到最后一页。

◆**前往_页**：在文本框中输入页码，再敲<Enter>键或者单击"前往"，即可跳到指定页面。

◆**修改**：超链接，在操作栏中。点击修改进入修改该行信息的页面。

1.3.1.2 只读列表

只读列表用来显示系统状态、会话等相关信息，只能查看信息而，不可操作修改，以"端口信息"为例说明只读列表中各参数的含义。

端口信息 本页3条/共3条

第1页/共1页 第一页 上一页 下一页 最后页 前往 第 页

物理接口	端口名称	是否拨号	IP地址	MAC地址	协议状态	接收速率	发送速率	带宽占用
WAN0	WAN0	否	172.16.21.43/255.255.255.0	00e0.0f7b.d468	连接	2 Kbps	1 Kbps	0.00%
WAN1	WAN1	否	10.168.12.15/255.255.255.0	00e0.0f7b.d469	连接	626 bps	0 bps	0.00%
LAN	LAN	否	192.168.111.111/255.255.255.0	00e0.0f7b.d46a	连接	0 bps	0 bps	

◆**本页3条/共3条**：即本页显示条目/总条目数，图中表示表格共有3条信息记录，当前页面显示了其中3条信息记录。

◆**第1页/共1页**：即当前页序号/总页面数，图中表示表格共有1页，当前显示的是第一页。

◆**第一页**：超链接。单击即可转到第一页。

◆**上一页**：超链接。单击即可转到上一页。

◆**下一页**：超链接。单击即可转到下一页。

◆**最后页**：超链接。单击即可转到最后一页。

◆**前往_页**：在文本框中输入页码，再敲<Enter>键或者单击"前往"，即可跳到指定页面。

1.3.1.3 排序列表

排序列表，是在可操作排序列表和只读排序列表基础上扩展的，对相应的标题列加入了排序功能，用户只要点击相应的列就能对该列对应的所有数据进行排序。第一次点击相应列默认按照从小到大的顺序进行排列，再次点击将按照从大到小的顺序进行排列，后面点击排序规律一次循环。

排序列表默认按照第一列的升序进行排列，例如下图所示，是按照"当前在线主机IP"的大小按照从小到大的顺序排列的。

每个主机的连接数信息 本页7条/共7条

第1页/共1页 第一页 上一页 下一页 最后页 前往 第 页

当前在线主机IP	网络连接数	最大网络连接数
172.16.21.10	40	500
172.16.21.47	42	500
172.16.21.59	2	500
172.16.21.60	2	500
172.16.21.69	13	500
172.16.21.71	12	500
172.16.21.82	1	500

◆**本页7条/共7条**：即本页显示条目/总条目数，图中表示表格共有7条信息记录，当前页面显示了其中两条信息记录。

◆**第1页/共1页**：即当前页序号/总页面数，图中表示表格共有1页，当前显示的是第一页。

◆**第一页**：超链接。单击即可转到第一页。

◆**上一页**：超链接。单击即可转到上一页。

◆**下一页**：超链接。单击即可转到下一页。

◆**最后页**：超链接。单击即可转到最后一页。

◆**前往_页：**在文本框中输入页码，再敲<Enter>键或者单击“前往”，即可跳到指定页面。

1.3.1.4 可搜索列表

可搜索列表，可搜索列表本身可以是可操作列表、只读列表、排序列表中的任何一种，并且是在这些列表的基础上增加了具有快速搜索数据功能的一种新的列表形式。如下图。

◆**本页7条/共7条：**即本页显示条目/总条目数，图中表示表格共有7条信息记录，当前页面显示了其中两条信息记录。

◆**第1页/共1页：**即当前页序号/总页面数，图中表示表格共有1页，当前显示的是第一页。

◆**第一页：**超链接。单击即可转到第一页。

◆**上一页：**超链接。单击即可转到上一页。

◆**下一页：**超链接。单击即可转到下一页。

◆**最后页：**超链接。单击即可转到最后一页。

◆**前往_页：**在文本框中输入页码，再敲<Enter>键或者单击“前往”，即可跳到指定页面。

◆**搜索：**在当前列表中搜索所有符合搜索条件的数据。在搜索文本框中输入搜索条件，再敲<Enter>键即可显示符合搜索条件的所有数据。用鼠标将输入光标置于空的搜索文本框中，然后按<Enter>回车键即会显示所有数据。

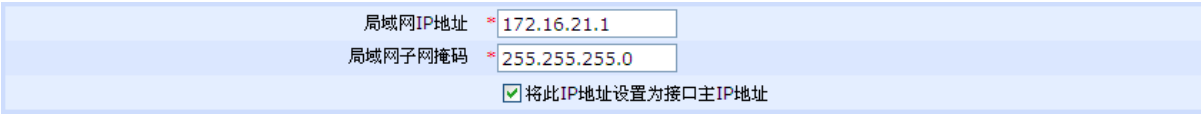
可搜索列表可以搜索当前列表中所有栏目中符合搜索条件的信息，并过滤不符合搜索条件的数据，只显示搜索到的结果。如下图。

使用的时候用户只要在列表中的搜索框中输入需要搜索的数据，例如上图中输入“172.16.21.47”然后按<Enter>回车键，智能搜索引擎就开始在当前列表的所有列包含的数据中搜索符合搜索条件的数据，并显示所有与该字符串匹配的条目，并且还可以在搜索结果中继续搜索数据。如果未搜索到符合要求的数据，则提示“记录未找到”。搜索完成以后，如果用户想重新查看列表全部数据，用户可以用鼠标将输入光标置于空的搜索文本框中，然后按<Enter>回车键即会显示所有数据了。

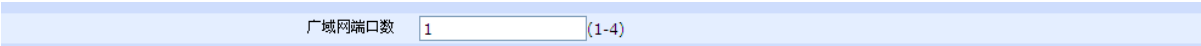
这里的搜索匹配规则是只要列表的任何一条信息记录的任何一列的数据值含有指定搜索字符串（即子字符串匹配）时，就认为该行信息与搜索字符串匹配，并将被显示在搜索结果中。

1.3.2 通用符号约定

符号：如果WEB配置页面中，界面中某参数中有“”号，表示该参数为必填项目。如下如中局域网IP地址和子网掩码配置项即为必须配置项目。



（）符号：如果WEB配置页面中，界面中某参数后面有用括号括起来的信息，表示该信息是提示信息，用户配置的时候需参考括号内的提示参数进行正确配置。如下图中配置广域网口数量的时候，页面提示广域网口输入的参数必须在1到4之间。



◆ 符号：页面中的◆符号通常表示这些是所在页面的在线帮助信息。如下图是端口监页面的在线帮助信息，用户在对页面配置之前，务必先要查看所在页面的在线帮助信息。

1.3.3 键盘操作约定

<>：表示键盘上的按键。例如，<Enter>表示回车。

1.3.4 其他表达约定

1.3.4.1 特殊字符支持

在一些要求输入名字（如用户名、组名、时间段名等）、密码等文本参数的地方，支持除 引号(“”)、右斜杠(\)、问号(?)以外的特殊字符。

1.3.4.2 配置页面切换方式

◆打开菜单约定：一级菜单名称→二级菜单名称→TAB页用来表示打开某配置界面的路径。例如，网络选项→端口映射→DMZ主机，表示在WEB配置页面左侧的菜单栏中，首先单击一级主菜单“网络选项”，之后再单击展开的二级子菜单“端口映射”，在打开的配置页面中再单击TAB页选项“DMZ主机”，就进入“DMZ主机”的配置页面了。对于只有一个TAB页的配置项，将默认打开该配置页。

◆执行功能约定

单击“XXX”按钮（XXX表示按钮名），表示进行该按钮所对应的操作。例如，单击“新建”按钮，就表示进行相应的新建操作，新建某些配置项。

◆选中某选项约定

选中“XXX”选项（XXX表示选项名），表示选中该选项所对应的功能。例如，接口配置/端口监控页面选中“启用端口监控功能”选项，就表示快速转发功能将被启用，但是需要注意的是必须这些操作都必须在用户执行“保存”或“应用”操作后才会生效。

◆ 全选/全不选功能约定：

选中“全选/全不选”前面的复选框表示全部选中显示列表中**当前页面**的所有记录，而不是列表包括的所有记录信息。所以操作的时候只能对这些选中的记录进行操作。全不选中，表示未选中当前列表中的任何记录。

1.4 出厂配置

◆ 接口出厂配置：

接口类型	IP地址	子网掩码
LAN口	192.168.2.1	255.255.255.0

◆ 系统管理员的用户名出厂设置为“admin”（区分大小写），出厂密码为“admin” （区分大小写）。

1.5 系统运行环境

1.5.1 硬件环境

系统的性能可能会根据服务器的 CPU 和内存的不同而有相当大的差别。下面列出了本软件建议服务器硬件的基本配置需求：

◆能正常工作的以太网卡及连接线
◆宽带 Internet 服务（接入方式为 xDSL、Cable Modem 或以太网）
◆具有以太网 RJ45 连接器的调制解调器（直接接入以太网时不需要此物件）
◆个人计算机一台
◆处理器：P4 2.0GHz 或以上
◆内存：512 MB RAM 或以上
◆显示器：推荐分辨率为 1024*768

1.5.2 软件环境

◆TCP/IP 网络软件（Windows 95/98/ME/2000/XP/Vista 自带）

◆网页浏览工具，如 Microsoft Internet Explorer 6.0 以上或 FireFox 等

1.6 术语与缩略语

以下名词是在此文档或是在 WEB 配置软件或配置页面中可能出现的名词，现解释如下:

术语	含义
UPnP	通用即插即用 (UpnP) 是一种用于 PC 机和智能设备（或仪器）的常见对等网络连接的体系结构，尤其是在家庭中。UpnP 以 Internet 标准和技术（例如 TCP/IP、HTTP 和 XML）为基础，使这样的设备彼此可自动连接和协同工作，从而使网络（尤其是家庭网络）对更多的人成为可能
WAN	广域网口，用以联接外网网段。
LAN	局域网口，主要用于连接内网网段。
DHCP	DHCP是Dynamic Host Configuration Protocol的缩写，它是TCP／IP协议簇中的一种，主要是用来给网络客户机分配动态的IP地址。这些被分配的IP地址都是DHCP服务器预先保留的一个由多个地址组成的地址集，并且它们一般是一段连续的地址。
NAT	网络地址转换（Network Address Translation或简称NAT，也叫做网络掩蔽或者IP掩蔽）是一种在IP数据包通过路由器或防火墙时重写源IP地址或/和目的IP地址的技术。这种技术被普遍使用在有多台主机但只通过一个公有IP地址访问因特网的私有网络中。
DNS	域名服务器(Domain Name Server)。在 Internet 上域名与 IP 地址之间是一一对应的，域名虽然便于人们记忆，但机器之间只能互相认识 IP 地址，它们之间的转换工作称为域名解析，域名解析需要由专门的域名解析服务器来完成，DNS 就是进行域名解析的服务器。
DDNS	DDNS（Dynamic Domain Name System，动态域名系统）用来动态更新 DNS 服务器上域名和 IP 地址之间的对应关系，保证通过域名解析到正确的 IP 地址。
DMZ	DMZ是英文“demilitarized zone”的缩写，中文名称为“隔离区”，也称“非军事化区”。它是为了解决安装防火墙后外部网络不能访问内部网络服务器的问题，而设立的一个非安全系统与安全系统之间的缓冲区，这个缓冲区位于企业内部网络和外部网络之间的小网络区域内，在这个小网络区域内可以放置一些必须公开的服务器设施，如企业Web服务器、FTP服务器和论坛等。另一方面，通过这样一个DMZ区域，更加有效地保护了内部网络，因为这种网络部署，比起一般的防火墙方案，对攻击者来说又多了一道关卡。
ISP	ISP（Internet Service Provider）即互联网服务提供商，是指向用户综合提供互联网接入业务、信息业务、和增值业务的电信运营商。
MTU	最大传输单元（Maximum Transmission Unit，*MTU*）是指一种通信协议的某一层上面所能通过的最大数据报大小（以字节为单位）
MAC	MAC（Media Access Control，介质访问控制）MAC 地址是烧录在 Network Interface Card(网卡,NIC)里的.MAC 地址,也叫硬件地址,是由 48 比特长(6 字节),16 进制的数字组成，它一般也是全球唯一的。我们可以这样获取 MAC 地址：在 Windows 2000/XP 中，依次单击“开始”→“运行”→输入“CMD”→回车→输入“ipconfig /all”→回车。（或者依次单击“开始”→“所有程序”→“附件”→“命令提示符”→输入“ipconfig /all”→回车。）即可看到 MAC

	地址。

1.7 功能特性简述

◆多个10/100M自适应广域网接口

◆ 共享Internet接入（ADSL、Cable Modem、以太网接入）

◆MAC地址克隆，突破共享限制让多机上网无障碍

◆ WEB界面实时监控、管理局域网内的流量和用户

◆端口监控，掌控网络端口实时状态

◆以太网口灵活重组，接口数目自己制定

◆支持灵活设置虚拟服务器(端口映射)

◆支持DMZ

◆灵活设置内网主机上网连接数限制

◆NAT访问控制，自主确定用户是否允许上网

◆支持多类型DDNS动态DNS解析

◆强大完善的DHCP（Server&Client&Relay）功能

◆ARP手动绑定

◆ 支持地址、协议和端口的包过滤

◆ARP批量自动绑定

◆IP/MAC 自由组合想怎么过滤就怎么过滤

◆基于地址组和时间段的高级防火墙

◆反病毒服务，有效阻断内网病毒传播

◆支持URL过滤

◆支持关键字过滤

◆支持DNS请求过滤

◆支持DNS代理

◆支持智能NAT

◆支持UPnP

◆多线路流量负载均衡以及线路备份

◆支持快速转发

◆支持分时段设置线路总带宽

◆动态带宽策略，自动根据网络情况设置最优速率

◆基于个性化带宽管理策略

◆基于个人、群组、全局的上网行为策略，灵活管理网内用户

◆优先服务，邮件优先，游戏优先，自定义业务优先。

◆支持上网黑名单和白名单

◆一键封QQ，MSN，P2P

◆一键封DDOS

◆一键封股票网址

◆一键封娱乐购物网址

◆支持VPN/IPSEC功能

◆支持L2TP客户端和服务器功能

◆支持PPTP客户端和服务器功能

◆支持PPPOE客户拨号和服务器功能

◆支持IPIP借线功能

◆支持GRE

◆分级用户权限管理，拨号用户、监控用户、系统管理员权限分明

◆支持WEB方式升级软件版本，即时体验新功能

◆日志信息显示、导出功能

◆语音告警，语音朗读报告网络异常情况，不用监控也能迅速应对

◆支持SNMP管理，配合SNMP网管软件，系统全面管理网络。

◆增值监控软件，图形化显示设备运行状态，直观清楚

◆诊断工具

◆策略库手动升级/策略库在线升级

◆容灾配置备份/导入功能

◆异常恢复出厂配置功能

◆设备运行状态实时监控功能

◆用户上网行为实时监控功能

1.8 典型应用

◆大中小型企业灵活百兆/千兆/光纤接入

◆大中小型网吧百兆/千兆/光纤接入

◆千兆小区接入

◆中小型企业VPN服务器和VPN客户端

◆宽带社区、学校等机构

◆SOHO以及家庭用户

◆其他各种宽带和安全应用场合

第2章　配置准备

2.1　网络设置

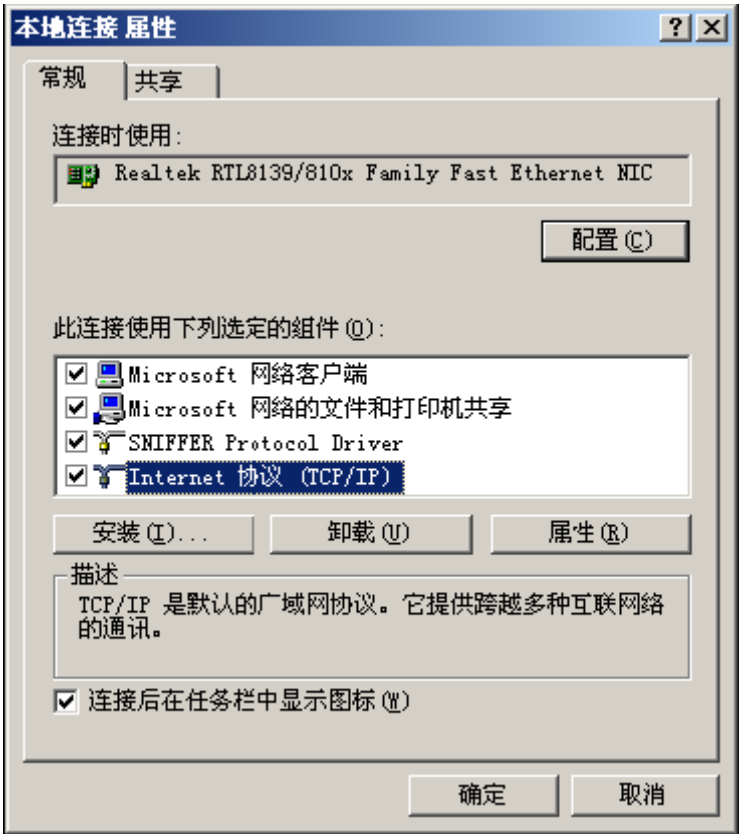
宽带路由器端口TP2默认的IP地址为192.168.2.1，子网掩码为255.255.255.0。这些参数可以根据需要改变，下文中将以默认值说明。网络设置的具体步骤如下（以Windows 2000为例）：

◆步骤一：将您的计算机连接到宽带路由器的快速以太网端口TP2上。

◆步骤二：设置计算机的IP地址。

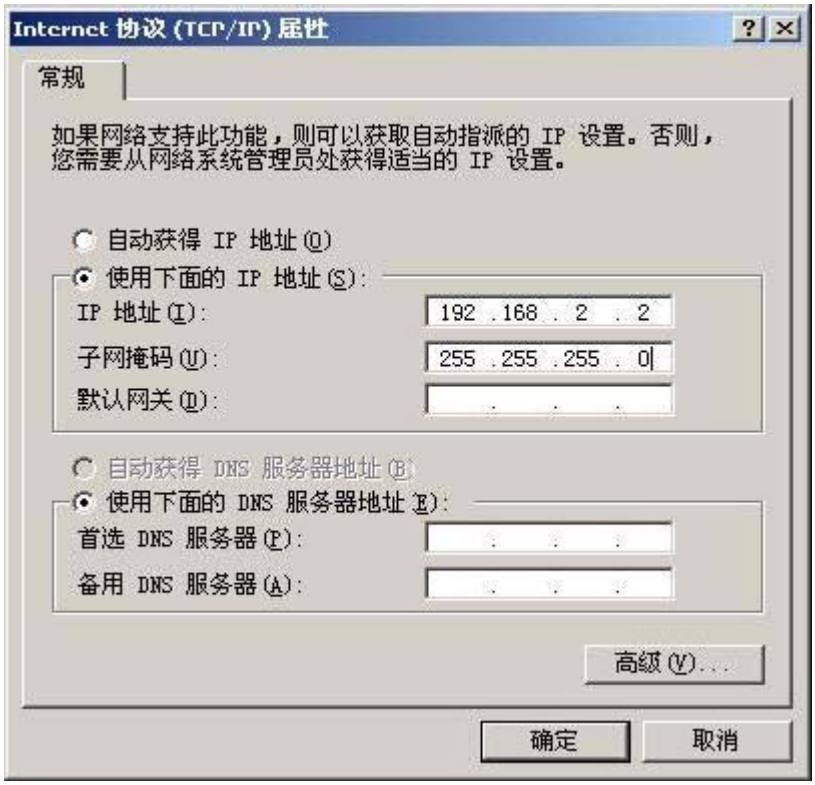
- 开始→控制面板→网络和拨号连接
- 右键单击“网络连接”图标，在弹出的上下文菜单中单击“属性”菜单。

选中“Internet协议（TCP/IP）”。如图：



- 单击“属性”按键，设置计算机的IP地址。

在“Internet 协议（TCP/IP）属性”对话框中点选“使用下面的IP地址”。在“IP地址”中填入192.168.2.xxx（xxx的范围为2 ～ 254），“子网掩码”中填入255.255.255.0。“默认网关”中填入192.168.2.1（即宽带路由器默认的IP地址）如图：



注：由于宽带路由器的默认IP地址为192.168.2.1所以xxx不能填1。
单击“确定”完成配置。

◆步骤三：测试计算机与路由器是否连通。

- 开始→ 运行 →键入“cmd” →确定
- 在命令提示符使用ping命令测试是否连通。执行： ping 192.168.2.1 如果显示：

```
Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time<10ms TTL=64
Reply from 192.168.2.1: bytes=32 time<10ms TTL=64
Reply from 192.168.2.1: bytes=32 time<10ms TTL=64
Reply from 192.168.2.1: bytes=32 time<10ms TTL=64

Ping statistics for 192.168.2.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

上图中如果 ”Received = ” 后面的值大于0，表示连接成功。反之如果显示：

```
Pinging 192.168.2.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.2.1:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

”Received = 0”则表示可能未能正确连接。

您可以检查：

a) 宽带路由器面板上与计算机相连端口的指示灯是否亮起，指示灯未亮表示物理上的连接不正常，可以换一根连接线。

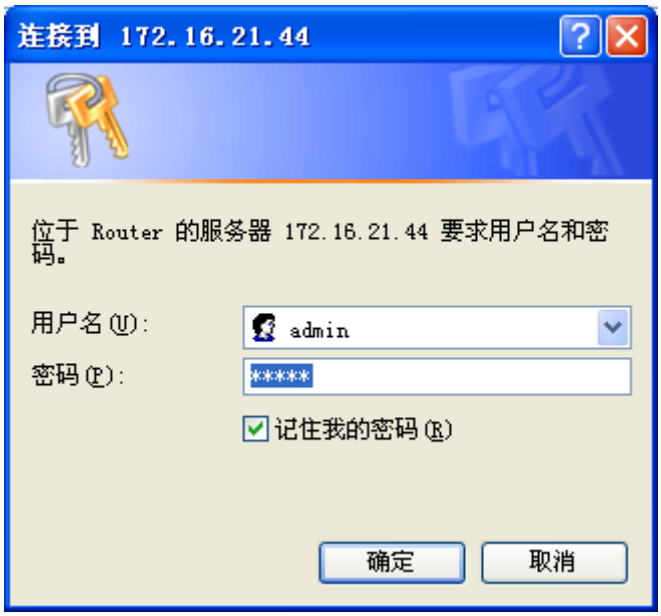
b) 检查上述TCP/IP设置是否正确。

第3章　配置指南

3.1　登录WEB管理系统

如果计算机与宽带路由器连接正常，并且可互相Ping通，即可通过Web浏览器（例如Internet Explorer、firefox等）进行路由器的配置。这里以Internet Explorer浏览器简称IE为例进行说明。

打开IE浏览器，在浏览器地址栏中输入宽带路由器的管理IP地址，这里以出厂默认LAN口管理地址http://192.168.2.1为例进行说明。用户输入路由器管理IP地址并回车确认后，将出现要求登录的提示界面（如下图）。



用户必须正确输入有效的管理员或配置受限用户的用户名和密码后才能登录成功。（宽带路由器出厂**默认用户名为：admin；密码为：admin，权限为系统管理员。**

用户登录成功后浏览器即会显示WEB管理系统首页。

不同权限的登录用户，打开的首页和授权的功能也会有所差别。其中系统管理员能够使用宽带路由器以及WEB配置页面的所有功能，而配置受限用户只能使用WEB管理系统的监控功能查看设备的一些运行信息，没有配置宽带路由器的权限。

> 提示：
>
> 设备中所有涉及的用户名和密码都是区分大小的，用户输入的时候需要主要！

3.2 WEB管理系统主界面

不同权限的登录用户，登录到宽带路由器以后，看到的WEB管理系统的主界面和授权使用的功能也是不同的。

3.2.1 系统管理员的界面

系统管理员登录设备以后，看到的是完整的宽带路由器WEB管理系统，如下图。用户在显示的页面可以查看宽带路由器实时运行信息，也可以根据需要对宽带路由器进行配置。

首页从功能上来说主要分以下几个功能块：设备面板映射信息、菜单栏、系统运行信息栏、技术支持信息、设备已运行时间。

- **设备面板映射信息：**描述WEB页面中显示或配置时页面上的接口名称(逻辑接口)和设备面板物理接口信息的映射关系（部分型号无此映射信息）。
- **菜单栏：**WEB页面功能菜单，用户可以通过鼠标单击打开或关闭不同的功能菜单。
- **系统运行信息栏：**显示当前设备运行过程中的一些事实的重要的信息。
- **技术支持信息：**当用户使用宽带路由器碰到问题或设备出现故障时，可以通过技术支持信息中的服务热线或支持网站寻求专业技术人员的技术支持。
- **设备已运行时间：**描述设备从上次启动到目前为止已运行的时间。

3.2.2 配置受限用户的界面

配置受限用户登录设备以后，显示的是宽带路由器监控界面，如下图。用户在显示的监控页面可以查看宽带路由器实时运行信息，但是不能进行配置操作。

首页功能说明参见上一节“系统管理员的首页”。

3.2.3 菜单栏

用户通过鼠标单击菜单栏中菜单，可以打开或关闭和菜单功能对应的配置或显示页面。系统管理员和配置受限用户打开的首页上面的功能菜单项是有差别的。

系统管理员所能使用由主菜单和子菜单组成，具体菜单说明如下：

◆**首页：**包括系统实时运行信息显示功能。

◆**快速向导：**包括快速上网向导配置功能。

◆**接口配置：**包括了和设备接口相关的配置功能，如 WAN 口配置、LAN 口配置、工作模式、修改 MAC、端口监控、端口重组等功能。

◆**多线路策略：**多线路应用时相关功能。如线路组合模式配置、应用调度、线路侦测。

◆**路由配置：**宽带路由器路由功能配置。如默认路由、静态路由。

◆**网络选项：**和网络应用相关功能。如端口映射、时间段配置、连接数限制、NAT 访问控制、DNS 配置、DDNS 配置、DHCP 配置、PPPOE 服务器、UPNP 配置。

◆**ARP 安全：**和 ARP 相关的安全功能。如 ARP 手动绑定、ARP 扫描绑定、IP+MAC 地址过滤。

◆**网络安全：**和网络安全应用的功能。如防火墙配置、反病毒配置、URL 过滤、关键字过滤、DMZ 端口配置。

◆**上网行为管理：**用户上网所需的带宽管理相关的功能。如群组管理、优先服务管理、黑白名单、上网信息查询等。

◆**虚拟专网：**VPN 应用相关的功能，如 IPSEC、PPTP、L2TP、IPIP、GRE、拨号用户管理等功能。

◆**系统管理：**一些系统辅助应用功能。如用户管理、时钟管理、软件升级、日志管理、远程管理、诊断工具、策略库管理、重新启动、配置导入导出、恢复出厂配置等。

◆**监控信息：**设备运行的一些详细分类和诊断信息。如端口信息、系统信息、DHCP 信息、路由信息、日志信息、连接数监控信息、行为监控信息等。

配置受限用户所能使用由主菜单和子菜单组成，具体菜单说明如下：

◆**首页**：包括系统实时运行信息显示功能。

◆**上网行为管理**：用户上网信息以及状态的查询功能。

◆**虚拟专网**：显示 VPN 应用中 IPSEC、PPTP、L2TP 的会话连接信息。

◆**监控信息**：设备运行的一些详细分类和诊断信息。如端口信息、系统信息、DHCP 信息、路由信息、日志信息、连接数监控信息、行为监控信息等。

> 提示：
>
> 设备型号不同，配置不同，具体的功能菜单可能也会有所差别，具体以 **WEB** 配置页面为准。

3.2.4 设备面板映射

描述 WEB 页面中显示或配置时页面上的接口名称(逻辑接口)和设备面板物理接口信息的映射关系。（部分型号无此映射信息）

3.2.5 系统运行信息栏

系统运行信息栏描述了并收集了系统当前运行的一些需要用户着重关注的实时状态信息，例如接口运行状态信息，上网用户信息，设备性能信息等。

关于本栏页面具体显示信息参见下一章“首页信息”。

第4章　首页信息

4.1　实时运行信息

单击打开菜单“首页”→“实时运行信息”即可进入“实时运行信息”显示页面，该页面用户可以实时查看当前设备运行过程中一些重要的运行信息。

实时运行信息描述并收集了系统当前运行的一些需要用户着重关注的实时状态信息，例如接口运行状态信息，上网用户信息，设备性能信息等。如下图。

端口名称	是否ADSL拨号	IP地址	MAC地址	连接状态	速率	带宽占用
WAN0	否	10.1.1.1/255.255.255.0	00e0.0fd6.10b8		0.00 bps	
WAN1	否	---	00e0.0fd6.10b9		0.00 bps	
LAN	否	10.168.50.144/255.255.0.0	00e0.0fd6.10ba		6.48 Kbps	

设备信息	
设备型号	ROUTER
设备版本	5.1.0B (BASE)　更新版本
BIOS版本	0.4.4
设备序列号	R7500536 000536

系统状态	
系统当前时间	2010-03-05 14:07:02　修改时间
系统运行时间	0天0时2分57秒
CPU使用率	2%
当前在线主机数	0　查看详细
当前连接数	0　查看详细
被惩罚主机数	0　查看详细
被抑制主机数	0/0　查看详细
当前用户	admin　修改口令

自动刷新周期　30 秒　Go　刷新

实时运行信息页面分三个功能部分，接口信息、软件信息、性能和上网信息。

其中**“接口信息”块**显示了当前设备中的接口总数，WAN 广域网口数，LAN 局域网口数目，信接口上网方式（ADSL 拨号/固定 IP 地址接入/DHCP 动态 IP 接入/未配置），接口当前的 IP 地址信息，MAC 地址，线路连接状态（连接/未连接），接口速率，带宽占用情况。

“软件信息”块显示了设备的型号，当前软件的版本信息、BIOS 的版本信息、设备序列号等信息。

“性能和上网信息”块显示了设备当前的时间，设备已运行的时间，设备 CPU 的使用率，当前正在上网的主机数量，内网主机当前的上网连接数，因使用 P2P 或其它非被允许使用网络行为而被设备惩罚的内网主机数量，因使用 P2P 或其它非被允许使用网络行为而被设备抑制的内网主机数量。

实时运行信息页面提供对相关信息的修改和查看，用户可以单击页面相应信息项后面的超链接，来修改或查看相关信息。例如单击设备版本信息项后面的“更新版本”超链接，即可切换到升级 IOS 软件页面，对设备的软件版本进行手动升级；又如用户可以单击被惩罚主机数后面的“查看详细”超链接，切换到内网主机实时状态页面查看当前被惩罚的主机信息。

刷新页面：设备默认 30 秒时间刷新一次本页面，这个刷新时间是可以配置的，用户可以配置为不自动刷新页面，也可以把刷新时间配置为 5/10/15/20/25/30 秒。用户也可以单击页面的“刷新”按钮来手动刷新页面。

> 提示：
>
> 设置自动刷新时间过短会导致页面频繁刷新，可能会对设备性能产生影响，因此在网络繁忙的环境下建议不要把自动刷新间隔设置过短。

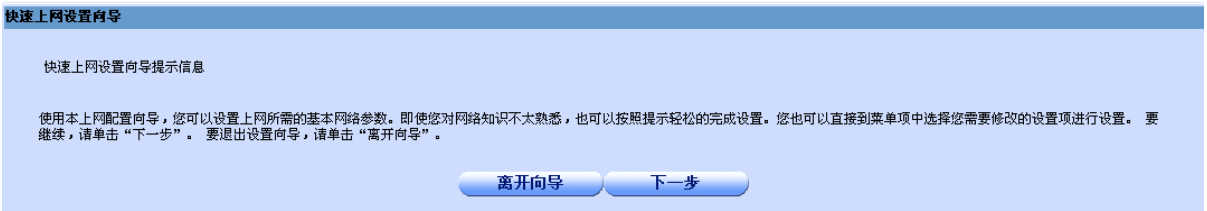
第5章 快速向导

5.1 快速上网向导

单击打开菜单“快速向导”→“快速上网向导”即可进入“快速上网向导”配置页面，通过该向导配置用户即使对网络知识不了解也能正常的上网使用。

5.1.1 快速上网向导概述

使用本上网配置向导，用户可以设置上网所需的基本网络参数。即使对网络知识不太熟悉，也可以按照提示轻松的完成设置。如下图。



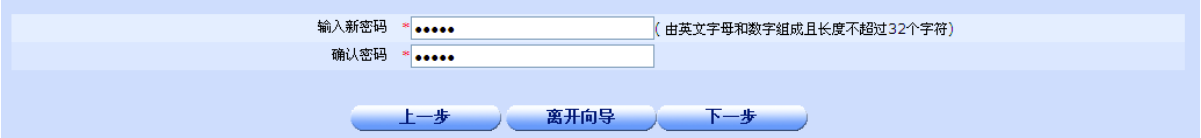
◆**下一步**：单击“下一步”按钮，用户进入向导配置步骤第 1 步。

◆**离开向导**：单击“离开向导”，退出向导配置页面，返回“系统运行状态”页面。

5.1.2 向导第 1 步：修改当前用户密码

在“快速上网设置向导提示信息”页面，如上图。单击“下一步”即可进入快速上网向导第 1 步，“修改当前用户密码”配置页面。

用户可以在该配置页面修改当前登录用户的帐号密码，向导所有步骤完成后生效。如下图：



◆**输入新密码**：输入新的密码。

◆**确认密码**：必须和新密码一致。

◆**下一步**：单击“下一步”按钮，用户进入向导配置步骤第 2 步。

◆**离开向导**：单击“离开向导”，退出向导配置页面，返回“系统运行状态”页面。

> ♁ 提示：
>
> 如果用户在向导所有配置步骤完成之前退出向导或切换到别的配置页面，将导致向导之前步骤配置的信息无法保存生效。

5.1.3 向导第 2 步：配置广域网口参数

在“快速上网设置向导 第 1 步/共 5 步 :修改当前用户密码”页面，如上图。单击“下一步”即可进入快速上网向导第 2 步，“配置广域网口参数”配置页面。

用户可以在该配置页面配置单线路、双线路、三线路和四线路等上网线路数量（设备型号不同，支持的线路数也有所区别，请以 WEB 配置页面为准），上网方式如 ADSL、静态 IP 接入、动态 IP 接入以及对应的参数。向导所有步骤完成后生效。如下图是双线路配置的图示：

配置单线路：如果用户需要配置单线路上网，请不要勾选“配置双线路”选项。即只要在 WAN0 口配置栏配置相应上网参数即可。如果设备本身是多 WAN 口设备的话，其他未使用的 WAN 接口下的配置将默认被清空，即连接类型将被置为“无”状态。

配置多线路：如果用户需要使用多线路上网，那么要在配置页面中选择需要支持的线路数，例如用户需要使用双线路上网，那么用户只要选中“配置双线路”选项，即会展开双线路的配置页面，用户可以在该配置页面配置第二条线路的上网参数信息。同理如果用户需要使用三线路上网，那么只要在选中“配置双线路”选项展开的页面，勾选“配置三线路”，即会展开三线路配置页面供用户配置。四线路也类似。

在 WANX（这里 X 是数字，如 0，1，2，3）配置页面用户可以选择上网类型，并且配置类型对应的上网参数。具体介绍如下：

- **ADSL 拨号上网：**ADSL 方式的宽带接入。如下图。

需要配置的参数包括：

- **用户名**：ISP 提供给用户的用于拨号的有效用户名。
- **密码**：ISP 提供给用户的用于拨号的有效用户密码。
- **确认密码**：同密码
- **最大传输单元**：默认为 1492。由于接入方式的差异可能有所不同，一般情况下如无必要请勿修改。
- **线路 ISP**：选择 WAN 口接入线路的运营商，系统将根据用户的选择生成相对应的路由，比如电信生成电信路由，网通生成网通路由。
- **线路带宽**：WAN 口接入线路的运营商提供的带宽大小，系统将根据带宽在多条线路之间进行线路负载和流量均衡，并根据输入的带宽大小自动进行上网行为管理。

◆ **固定 IP 接入**：ISP 提供固定 IP 地址和子网掩码接入上网的方式。如下图。

需要配置的参数包括：

- **广域网 IP 地址**：申请固定 IP 接入业务的时候，ISP（例如中国电信）将提供设备使用的广域网 IP 地址。
- **广域网子网掩码**：申请固定 IP 接入业务的时候，ISP（例如中国电信）将提供设备使用的子网掩码。
- **默认网关 IP 地址**：申请固定 IP 接入业务的时候，ISP（例如中国电信）将提供设备使用的静态网关 IP 地址
- **最大传输单元**：默认为 1500。由于接入方式的差异可能有所不同，一般情况下如无必要请勿修改。
- **线路 ISP**：含义和作用同 ADSL 拨号中的线路 ISP。
- **线路带宽**：含义和作用同 ADSL 拨号中的线路带宽。

◆ **动态 IP 接入**：DHCP 方式的宽带接入，由 ISP 自动给用户分配上网 IP 地址和子网掩码等信息。如下图。

需要配置的参数包括：

- **线路 ISP**：含义和作用同 ADSL 拨号中的线路 ISP。
- **线路带宽**：含义和作用同 ADSL 拨号中的线路带宽。

◆ **无**：清除当前接口的配置信息。如下图。如果当前 WAN 口不需要使用，请选择“无”。

本选项不需要配置额外参数。

◆**上一步**：单击“上一步”按钮，用户进入向导配置步骤第 1 步。

◆**下一步**：单击“下一步”按钮，用户进入向导配置步骤第 3 步。

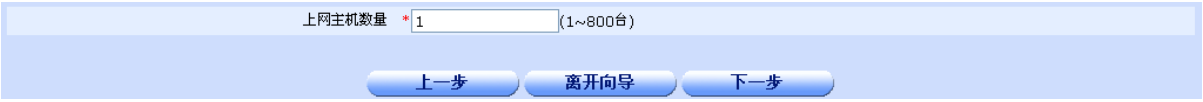
◆**离开向导**：单击“离开向导”，退出向导配置页面，返回“系统运行状态”页面。

> 提示：
>
> 如果用户在向导所有配置步骤完成之前退出向导或切换到别的配置页面，将导致向导之前步骤配置的信息无法保存生效。

5.1.4 向导第 3 步：设置上网主机数量

在“快速上网设置向导 第 2 步/共 5 步 :配置广域网口参数”页面，见上节说明。单击“下一步”即可进入快速上网向导第 3 步，“设置上网主机数量”配置页面。

用户可以在该配置页面修改当前登录用户的帐号密码，向导所有步骤完成后生效。如下图：



◆**上网主机数量**：内网需要通过宽带路由器上网的 PC 和其他网络设备的数量。

◆**上一步**：单击“上一步”按钮，用户进入向导配置步骤第 2 步。

◆**下一步**：单击“下一步”按钮，用户进入向导配置步骤第 4 步。

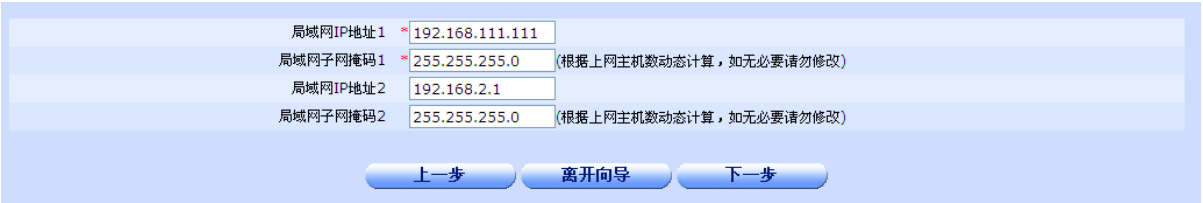
◆**离开向导**：单击“离开向导”，退出向导配置页面，返回“系统运行状态”页面。

> 提示：
>
> 如果用户在向导所有配置步骤完成之前退出向导或切换到别的配置页面，将导致向导之前步骤配置的信息无法保存生效。

5.1.5 向导第 4 步：配置局域网口参数

在“快速上网设置向导 第 3 步/共 5 步 :设置上网主机数量”页面，如上图。单击“下一步”即可进入快速上网向导第 4 步，“配置局域网口参数”配置页面。

用户可以在该配置页面设计局域网口的 IP 地址（即内网主机上网的网关的 IP 地址），向导所有步骤完成后生效。如下图：



◆**局域网 IP 地址 1**：局域网口（LAN 口）的 IP 地址，它也是内网主机上网的网关 IP 地址。

◆**局域网子网掩码 1**：局域网口（LAN 口）的子网掩码，此处子网掩码是根据上一步骤的上网主机数量来计算出的，如无必要请勿修改此掩码。

◆**局域网 IP 地址 2**：局域网口（LAN 口）的扩展 IP 地址，

◆**局域网子网掩码 2**：局域网口（LAN 口）的扩展 IP 地址的子网掩码。此处子网掩码是根据上一步骤的上网主机数量来计算出的，如无必要请勿修改此掩码。

◆**上一步**：单击“上一步”按钮，用户进入向导配置步骤第 3 步。

◆**下一步**：单击“下一步”按钮，用户进入向导配置步骤第 5 步。

◆**离开向导**：单击“离开向导”，退出向导配置页面，返回“系统运行状态”页面。

> 提示：
>
> 如果用户在向导所有配置步骤完成之前退出向导或切换到别的配置页面，将导致向导之前步骤配置的信息无法保存生效。

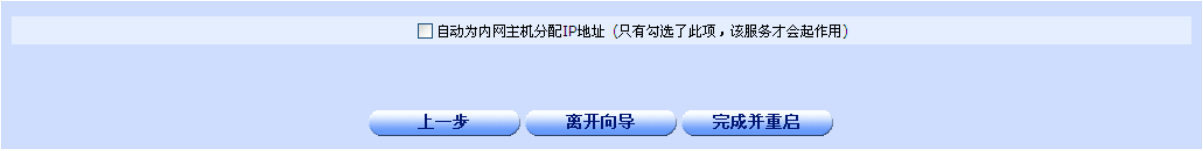
> ★注意：
>
> 局域网中所有计算机的子网掩码必须与此处的子网掩码相同。

> ★注意：
>
> 如果您改变了此处的 **LAN** 口的 **IP** 地址，则您必须在向导完成生效之后用新的 **IP** 地址才能登陆路由器管理界面，并且局域网中所有计算机默认网关也必须设置为该 **IP** 地址，这样才能正常上网。

5.1.6 向导第 5 步：设置内网主机IP地址分配方式

在“快速上网设置向导 第 4 步/共 5 步 :配置局域网口参数”页面，如上图。单击“下一步”即可进入快速上网向导最后一步即第 5 步，“设置内网主机 IP 地址分配方式”配置页面。

用户可以在该配置页面设置是否为内网主机分配 IP 地址的服务功能，向导所有步骤完成后生效。如下图：



◆**自动为内网主机分配 IP 地址**：选中该选项表示设备在配置生效后，将通过 DHCP 的方式为内网需要获取 IP 地址的主机动态分配 IP 地址。

◆**上一步**：单击“上一步”按钮，用户进入向导配置步骤第 4 步。

◆**离开向导**：单击“离开向导”，退出向导配置页面，返回“系统运行状态”页面。

◆**完成并重启**：单击该按钮，设备将保存快速上网向导步骤配置的各种参数信息，并重启使之生效。

用户单击“完成并重启按钮”后，设备提示操作成功，并提示设备正在重新启动，用户可以在 30 秒左右时间以后，可以重新刷新页面。如下图。

提示：

如果用户在向导所有配置步骤完成之前退出向导或切换到别的配置页面，将导致向导之前步骤配置的信息无法保存生效。

★注意：

用户在用快速上网向导配置完成约 **30** 秒后，必须按 **F5** 刷新或点击浏览器地址栏后的刷新按钮 来刷新整个框架页面。

第6章 接口配置

6.1 WAN口配置

单击打开菜单“接口配置”→“WAN口配置”即可进入“WAN口配置页面”，在该页面列出了设备的WAN口信息列表，用户可以查看各WAN口线路的配置参数以及连接状态信息，也可以根据实际需要修改或删除已配置的线路。

6.1.1 WAN广域网口信息列表

WAN 口信息列表列出了 WAN 线路的连接状态以及部分重要的配置参数信息。如下图：

WAN广域网口信息列表 本页2条/共2条

第1页/共1页 第一页 上一页 下一页 最后页 前往 第 页

广域网口名称	连接类型	接入IP/掩码	网关地址	最大传输单元	线路ISP/预设带宽	线路状态	操作
WAN0	静态IP接入	172.16.21.43/255.255.255.0	172.16.21.1	1500	中国电信/14M		修改
WAN1	ADSL拨号接入	---	---	1492	中国网通/2M		修改

列表中显示的信息，会因设备实际使用的接口数量不同而不同。

◆**广域网口名称**：对应于设备面板上的标识顺序，WAN0，WAN1 等。

◆**连接类型**：包括静态 IP 接入、ADSL 拨号接入(PPPOE 接入)以及动态 IP 接入(DHCP 接入)方式。

◆**接入 IP/掩码**：列出了接口当前的 IP 地址和子网掩码。

如果当前线路是 ADSL 拨号线路，则它们分别为 ISP 当前分配的广域网接口的 IP 地址、子网掩码以及静态路由的网关地址。

如果当前线路是固定 IP 接入线路，则分别为 ISP 提供的广域网接口的静态 IP 地址、子网掩码以及静态路由的网关地址。

如果当前线路是动态 IP 接入线路，则它们分别为 ISP 当前分配的广域网接口的 IP 地址、子网掩码以及静态路由的网关地址。

当 ADSL 拨号接入方式未获取到正确的 IP 地址和掩码的情况下，将无 IP 地址和掩码信息显示。

当动态 IP 接入方式未获取到正确的 IP 地址和掩码的情况下，将无 IP 地址和掩码信息显示而以“DHCP 动态获取”信息显示在接入 IP/掩码一栏。

当 WAN 口未配置任何信息时，对应参数列显示为空或“---”。

◆**网关地址**：仅对于静态 IP 接入方式显示，其他方式不显示信息。

◆**最大传输单元**：即 MTU，显示了对应的接入模式下允许的最大传输单元值。

◆**线路 ISP/预设带宽**：显示对应 WAN 接口上的 ISP（英特网服务提供商）信息，包括名称和提供的带宽。

◆**线路状态**：描述线路的连接状态包括连接和断开，此连接状态表示 WAN 口是否已经接上网线并激活，并不代表已经可以上网。影响上网的因素有很多，如果在包括网关、域名服务器、内网 IP 地址、路由等都已经配置的情况下不能上网，请参考手册的 FAQ。

表示 WAN 口已连接并处于激活状态。

表示 WAN 口未连接或处于未激活状态。

◆**操作**：单击“修改”超链接，进入 WAN 广域网口配置页面，可以修改 WAN 口配置参数。

6.1.2 WAN广域网口配置

单击打开菜单“接口配置”→“WAN 口配置”，在显示页面的 WAN 广域网口信息列表中找到需要配置的 WAN 口信息行，点击其对应的“操作”一栏的“修改”超链接，即可进入“WAN 口配置页面”。

WAN 广域网口配置的连接类型分为四种，下面依次说明。如下图：

◆**ADSL 拨号上网**：ADSL 方式的宽带接入。如上图。

需要配置的参数包括：

- **用户名**：ISP 提供给用户的用于拨号的有效用户名。
- **密码**：ISP 提供给用户的用于拨号的有效用户密码。
- **确认密码**：同密码
- **最大传输单元**：默认为 1492。由于接入方式的差异可能有所不同，一般情况下如无必要请勿修改。
- **线路 ISP**：选择 WAN 口接入线路的运营商，系统将根据用户的选择生成相对应的路由，比如电信生成电信路由，网通生成网通路由。
- **线路带宽**：WAN 口接入线路的运营商提供的带宽大小，系统将根据带宽在多条线路之间进行线路负载和流量均衡，并根据输入的带宽大小自动进行上网行为管理。
- **保存**：参数输入完成后，单击“保存”按钮，将设置的信息保存到设备上，以使之生效。

  保存后如果提示操作成功，则表示输入配置信息已经生效，如果提示操作失败，则用户需要重新输入参数，并检查自己输入的参数是否合法有效。
- **返回**：单击该按钮返回 WAN 广域网口列表显示页面。

◆**固定 IP 接入**：ISP 提供固定 IP 地址和子网掩码接入上网的方式。如上图。

需要配置的参数包括：

- **广域网 IP 地址**：申请固定 IP 接入业务的时候，ISP（例如中国电信）将提供设备使用的广域网 IP 地址。
- **广域网子网掩码**：申请固定 IP 接入业务的时候，ISP（例如中国电信）将提供设备使用的子网掩码。
- **默认网关 IP 地址**：申请固定 IP 接入业务的时候，ISP（例如中国电信）将提供设备使用的静态网关 IP 地址
- **最大传输单元**：默认为 1500。由于接入方式的差异可能有所不同，一般情况下如无必要请勿修改。
- **线路 ISP**：含义和作用同 ADSL 拨号中的线路 ISP。
- **线路带宽**：含义和作用同 ADSL 拨号中的线路带宽。
- **保存**：参数输入完成后，单击“保存”按钮，将设置的信息保存到设备上，以使之生效。

  保存后如果提示操作成功，则表示输入配置信息已经生效，如果提示操作失败，则用户需要重新输入参数，并检查自己输入的参数是否合法有效。
- **返回**：单击该按钮返回 WAN 广域网口列表显示页面。

◆**动态 IP 接入**：DHCP 方式的宽带接入，由 ISP 自动给用户分配上网 IP 地址和子网掩码等信息。如上图。

需要配置的参数包括：

- **线路 ISP**：含义和作用同 ADSL 拨号中的线路 ISP。

- **线路带宽：**含义和作用同 ADSL 拨号中的线路带宽。
- **保存：**参数输入完成后，单击“保存”按钮，将设置的信息保存到设备上，以使之生效。

  保存后如果提示操作成功，则表示输入配置信息已经生效，如果提示操作失败，则用户需要重新输入参数，并检查自己输入的参数是否合法有效。
- **返回：**单击该按钮返回 WAN 广域网口列表显示页面。

◆**无：**清除当前接口的配置信息。如果当前 WAN 口不需要使用，请选择“无”。

本选项不需要配置额外参数。

- **保存：**参数输入完成后，单击“保存”按钮，将设置的信息保存到设备上，以使之生效。

  保存后如果提示操作成功，则表示输入配置信息已经生效，如果提示操作失败，则用户需要重新输入参数，并检查自己输入的参数是否合法有效。
- **返回：**单击该按钮返回 WAN 广域网口列表显示页面。

★注意：

不使用的 WAN 口，连接类型请务必选择“无”，否则如果配置了 ISP 信息和带宽参数，可能会引起带宽和路由策略问题，对上网产生影响。

提示：

WAN 口配置完成如果尚未配置域名服务器 DNS，请转入菜单“网络选项”→“DNS 配置”配置 DNS。

6.2 LAN口配置

单击打开菜单“接口配置”→“LAN口配置”即可进入“LAN口配置”页面，在该页面列出了设备的LAN口信息列表，用户可以查看LAN口线路的配置IP地址信息，也可以根据实际需要修改或删除已配置的线路。

6.2.1 LAN（局域网）口信息列表

显示了局域网口上配置的IP地址网段信息，如下图。如果列表显示为空，表示LAN口尚未配置任何IP网段信息。

◆**IP地址类型**：列表中的IP地址类型共有两种类型：主IP地址和辅助IP地址，

- **主IP地址**：接口的主要IP地址网段，只能有一个主IP地址。
- **辅助IP地址**：在同一端口中可以设置两个以上的不同网段的IP地址，这样可以实现连接在同一局域网上不同网段之间的通讯。一般由于一个网段对于用户来说不够用，可以采用这种办法。LAN口允许配置多个网段IP地址。

  辅助IP地址的作用主要是在物理的子网上创建逻辑子网、使桥接网络分成更多子网、解决RIP等不连续子网的问题。

◆**局域网口IP/掩码**：已配置的局域网的IP地址网段和子网掩码。

◆**操作**：单击“修改”超链接，进入 LAN 局域网口配置页面，可以修改 LAN 口的对应的 IP 地址和子网掩码等信息。

◆**全选/全不选**：全部选中/全部不选中 当前页的信息记录。

◆**删除**：用鼠标选中或全选列表栏中的信息记录（即使显示信息行前面的复选框打勾），单击“删除”按钮删除选中的IP地址网段记录。删除LAN口IP地址的时候必须先删除辅助IP地址后，才能删除主IP地址，否则在操作过程中会提示删除出错。

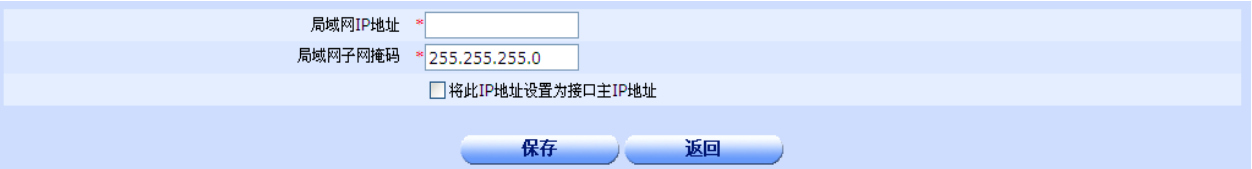
◆**新增IP地址**：单击“新增IP地址”按钮，进入LAN局域网口配置页面，可以新增LAN口的IP地址和子网掩码等信息。

> **提示 1：**
>
> **一般情况下不需要配置辅助 IP 地址。只有在同一个接口需要配置多个不同网段的情况下，才需要配置辅助 IP 地址。**

> **提示 2：**
>
> **如果需要删除主 IP 地址，必须要先删除 LAN 口下的所有的辅助 IP 地址后，才能删除主 IP 地址。**

6.2.2 LAN局域网口配置

单击打开菜单“接口配置”→“LAN 口配置”，在显示 LAN 局域域网口信息列表的页面，单击“新增 IP 地址”或找到需要修改的 LAN 口 IP 地址信息行，单击击其对应的“操作”一栏的“修改”超链接，即可进入“LAN 局域网口配置”页面。如下图。



◆**局域网 IP 地址：**局域网网段 IP 地址，格式如 192.168.1.100。

◆**局域网子网掩码：**和局域网 IP 地址对应的合法的子网掩码，格式如 255.255.255.0。

◆**将此 IP 地址设置为接口主 IP 地址：**选中该选项，输入的 IP 地址和子网掩码在设置保存生效后将作为接口的主 IP 网段地址。如果未选中本选项，则输入的 IP 地址和子网掩码将作为辅助 IP 地址设置在 LAN 口上。

接口主 IP 地址和接口辅助 IP 地址之间可以通过选中与否本选项来进行互相转换，但是辅助 IP 地址转换为接口主 IP 地址时，接口原来配置的主 IP 地址将被新的主 IP 地址覆盖而丢失。接口主 IP 地址不能直接转换为辅助 IP 地址。主 IP 地址只能有一个，而辅助 IP 地址可以有多个。

◆**保存：**参数输入完成后，单击“保存”按钮，将设置的信息保存到设备上，以使之生效。

保存后如果提示操作成功，则表示输入配置信息已经生效，如果提示操作失败，则用户需要重新输入参数，并检查自己输入的参数是否合法有效。

◆**返回：**单击该按钮返回 LAN 局域网口列表显示页面。

★注意：

辅助 IP 地址转换为接口主 IP 地址时，接口原来配置的主 IP 地址将被新的主 IP 地址覆盖而丢失。接口主 IP 地址不能直接转换为辅助 IP 地址。

★注意：

局域网中所有计算机的子网掩码必须与此处的子网掩码相同。

★注意：

如果您改变了此处的 LAN 口的 IP 地址，则您必须在保存成功之后用新的 IP 地址才能登陆路由器管理界面，并且局域网中所有计算机默认网关也必须设置为该 IP 地址，这样才能正常上网。

6.3 工作模式

单击打开菜单“接口配置”→“工作模式”即可进入“接口工作模式”，在该页面列出了设备所有接口的工作模式列表信息，用户可以查看设备接口的当前工作模式信息，也可以根据实际需要修改指定接口的工作模式。

6.3.1 接口工作模式

显示了设备的接口以太网口的工作模式相关信息，包括接口类型和接口工作模式。如下图。

接口名称	接口类型	接口工作模式	操作
WAN0	广域网口	自动协商	修改
WAN1	广域网口	自动协商	修改
LAN	局域网口	自动协商	修改

列表中显示的信息，会因设备实际使用的接口数量不同而不同。

◆**接口名称：**对应于设备面板信息，指示该接口描述的信息同物理设备面板的对应关系。

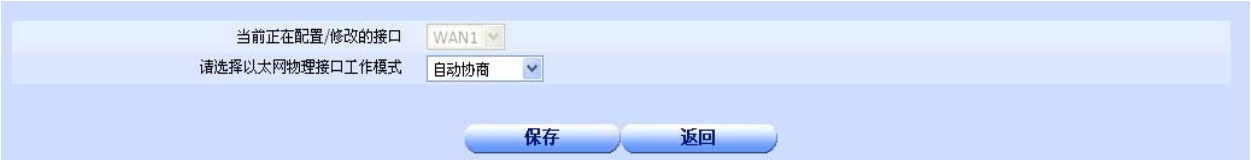
◆**接口类型：**分为广域网口和局域网口。

◆**接口工作模式：**描述的是网口的速率和协商模式。包括自动协商、10M半双工、10M全双工、100M半双工、100M全双工、1000M半双工（部分产品支持）、1000M全双工（部分产品支持）。

◆**操作：**单击“修改”超链接，进入“修改接口工作模式”配置页面，可以修改指定接口的网口速率和协商模式信息。

6.3.2 修改接口工作模式

单击打开菜单“接口配置”→“工作模式”，在显示“接口工作模式信息列表”的页面，找到需要修改工作模式的接口信息行，单击击其对应的“操作”一栏的“修改”超链接，即可进入“修改接口工作模式”页面。如下图。



◆ **当前正在配置/修改的接口：**描述当前修改的配置将要应用的接口，由用户在“接口工作模式”页面的“接口工作模式信息列表”中选择点击某一接口所在行对应的“修改”超链接时决定。例如：用户选择“接口名称”为WAN1 所在行末的“修改”，并单击进入“修改接口工作模式”时，“当前正在配置/修改的接口”后面的下拉框内数据将显示为WAN1，表示是对WAN1 接口的工作模式进行修改。

◆ **选择以太网物理接口工作模式：**选择网口的速率和协商模式。包括自动协商、10M 半双工、10M 全双工、100M 半双工、100M 全双工、1000M 半双工（部分产品支持）、1000M 全双工（部分产品支持）等选项。

◆**保存：**参数修改完成后，单击“保存”按钮，将设置的信息保存到设备上，以使之生效。

保存后如果提示操作成功，则表示输入配置信息已经生效，如果提示操作失败，则用户需要重新修改参数，并检查自己选择的参数是否合法有效。

◆**返回：**单击该按钮返回“接口工作模式”显示页面。

提示：

修改 **WEB** 页面管理地址对应接口的工作模式时，可能会导致网页中断或无法访问，此时用户只需重新刷新页面即可正常使用。

6.4 修改MAC

单击打开菜单“接口配置”→“修改MAC”即可进入“接口MAC信息”页面，在该页面列出了设备所有接口的MAC信息，用户可以查看设备接口的当前MAC地址，也可以根据实际需要修改接口的MAC地址。

6.4.1 接口MAC信息

显示了设备以太网接口的类型以及对应的 MAC 地址信息。如下图。

列表中显示的信息，会因设备实际使用的接口数量不同而不同。

◆**接口名称：**对应于设备面板信息，指示该接口描述的信息同物理设备面板的对应关系。

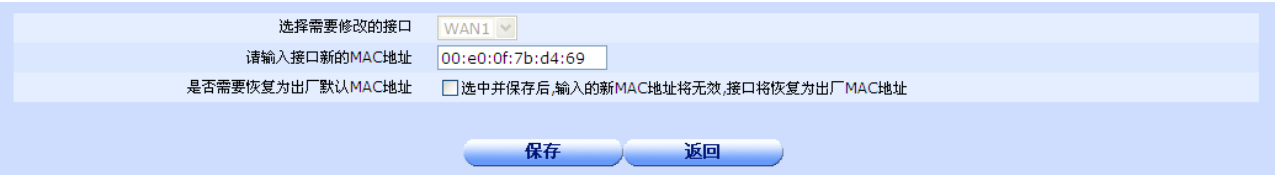
◆**接口类型：**分为广域网口和局域网口。

◆**接口MAC地址：**接口对应的MAC地址信息。

◆**操作：**单击“修改”超链接，进入“修改 MAC 地址”配置页面，可以修改指定接口的 MAC 地址或恢复接口 MAC 地址为出厂初始 MAC 地址。

6.4.2 修改MAC地址

单击打开菜单“接口配置”→“修改 MAC”，在显示“接口 MAC 信息列表”的页面，找到需要修改 MAC 地址的接口信息行，单击击其对应的“操作”一栏的“修改”超链接，即可进入“修改 MAC 地址”配置页面。如下图。



◆ **当前正在配置/修改的接口：**描述当前修改的配置将要应用的接口，由用户在“接口 MAC 信息”页面的“接口 MAC 信息列表”中选择点击某一接口所在行对应的“修改”超链接时决定。例如：用户选择“接口名称”为 WAN1 所在行末的“修改”，并单击进入“修改 MAC 地址”时，“当前正在

配置/修改的接口”后面的下拉框内数据将显示为 WAN1，表示是对 WAN1 接口的 MAC 地址进行修改。

- **输入接口的 MAC 地址：**如果用户需要将接口的 MAC 地址修改成新的 MAC 地址，则需要新的 MAC 地址信息，MAC 地址格式为: aa:bb:cc:dd:ee:ff 或 aa-bb-cc-dd-ee-ff，不区分大小写。

  用户如果只是希望将配置接口的 MAC 地址恢复为出厂配置，则此处可为空不用填写信息。

- **是否需要恢复为出厂默认 MAC 地址：**选中该选项表示要将配置接口的 MAC 地址恢复为出厂时候预设的 MAC 地址，此时“输入接口的 MAC 地址”输入的信息将无效。

- **保存：**参数修改完成后，单击“保存”按钮，将设置的信息保存到设备上，以使之生效。

  保存后如果提示操作成功，则表示输入配置信息已经生效，如果提示操作失败，则用户需要重新修改参数，并检查自己选择的参数是否合法有效。

- **返回：**单击该按钮返回“接口 MAC 信息”显示页面。

> **提示：**
>
> **修改 WEB 页面管理地址对应接口的 MAC 地址时，可能会导致网页中断或无法访问，此时用户只需重新刷新页面即可正常使用。**

> **★注意：**
>
> **任意两个 WAN 口或 WAN 口与 LAN 口之间的 MAC 地址不可以相同，否则会导致不可预料的错误。**

6.5 端口监控

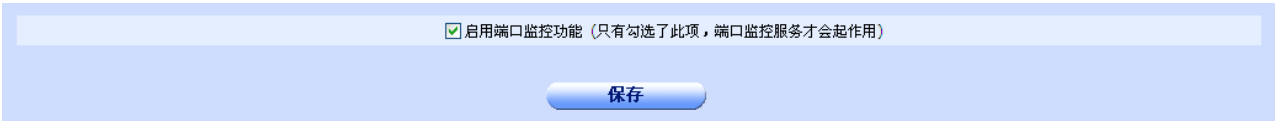
单击打开菜单“接口配置”→“端口监控”即可进入“端口监控配置”页面，在该页面用户可以根据实际需要选择在镜像端口上监控/不监控设备流量。

设备的监控口默认是设备的最后一个以太网物理口。

部分型号设备可能不支持“端口监控”功能，具体请以设备的实际配置页面为准。

6.5.1 端口监控配置

单击打开菜单“接口配置”→“端口监控”，即可进入“端口监控配置”页面，在该页面用户可以根据实际需要选择在镜像端口上监控/不监控设备流量。如下图。



- **启用端口监控功能：**选中该选项表示允许用户启用端口监控功能。

- **保存：**参数修改完成后，单击“保存”按钮，将设置的信息保存到设备上，以使之生效。

  保存后如果提示操作成功，则表示输入配置信息已经生效，如果提示操作失败，则用户需要重新修改参数，并检查自己选择的参数是否合法有效。

提示：

端口监控启用以后用户可以通过设备监控口，对流量报文等进行监控。设备的监控口默认是设备的最后一个以太网物理口。

★注意：

如果设备的最后一个以太网物理口已经作为 **LAN** 口使用，则端口监控功能将失效。

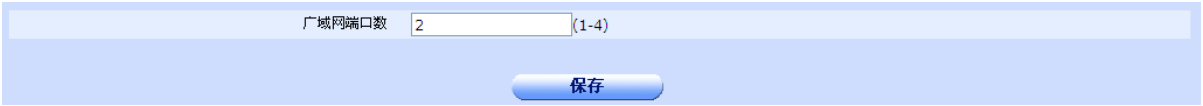
6.6 端口重组

单击打开菜单“接口配置”→“端口重组”即可进入“端口重组配置”页面，在该页面用户可以根据实际需要设置有效的广域网口数量。

部分型号设备可能不支持“端口重组”功能，具体请以设备的实际配置页面为准。

6.6.1 端口重组配置

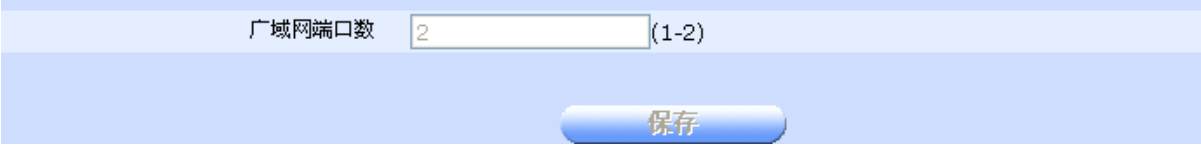
单击打开菜单“接口配置”→“端口重组”即可进入“端口重组配置”页面，在该页面用户可以对当前的 WAN 口数量进行重组，根据实际需要重新设置有效的广域网口数量。



- **广域网口数：**端口重组后新的广域网口数量。设备型号不同具体支持的可以重组的广域网口数目也有所差异，配置项后给出了具体的参考范围，如上图“(1-4)”表示重组后新的广域网口数最少为 1 个，最多为 4 个。
- **保存：**参数修改完成后，单击“保存”按钮，将设置的信息保存到设备上，以使之生效。

  保存后如果提示操作成功，则表示输入配置信息已经生效，如果提示操作失败，则用户需要重新修改参数，并检查自己选择的参数是否合法有效。

R3000 不支持“端口重组”功能，在进入“端口重组配置”页面时，功能显示为灰色，不可修改：



★注意：

端口重组功能将改变设备上 **WAN** 口和 **LAN** 口的数目和顺序，并且会导致设备对应接口下的配置可能会发生丢失、移位、错误到致网络不通等问题，因此用户需要谨慎操作， 一旦进行端口重组操作后，用户需要对设备所有和接口有关的功能比如 **WAN** 口配置，**LAN** 口配置，防火墙等进行重新配置，否则可能会影响用户对这些功能的正常使用。

端口重组成功后，可能会导致用户无法访问 **WEB** 的情况，这种情况下用户可以根据端口重组时设置的端口数，尝试将网线插在其他端口。

第7章　多线路策略

7.1　线路组合模式

如果是多WAN接入，单击打开菜单“多线路策略”→“线路组合模式”即可对多线路使用方式进行配置，通过本界面提供的功能可以使多条线路协同工作于最佳模式下。

- **ISP 智能选线模式**：此模式适用于不同 ISP 之间的均衡，路由器将自动识别线路并调用路由策略，例如：两个 WAN 口分别是电信线路和网通线路，那么路由器将自动识别，实现电信走电信线路，网通走网通线路。
- **叠加模式**：此模式适用于同一 ISP 多光纤线路和多 ADSL 线路，同一 ISP 的混合线路也可以考虑选用这个模式，此模式下，路由器将根据线路带宽比例均衡分配流量到各线路，线路承载的数据可以参照下面的例子。如果 WAN0 是电信 10M 光纤，WAN1 也是电信 10M 光纤， 那么就选择 WAN0 承载 50% 的数据，WAN1 也承载 50% 的数据，但是如果 WAN0 是电信 2M 光纤，WAN1 是电信 2M ADSL， 那么就选择 WAN0 承载 70% 的数据，WAN1 也承载 30% 的数据， 因为就稳定性来说，光纤要远远大于 ADSL。
- **主辅模式**：此模式下路由器将根据应用调度的设置将部分流量导入到辅助线路以充分利用多条线路的带宽。

注意：对于每个用户的组网环境，要达到最佳的上网效果，建议合理选择多线路模式，不要随意更改 。

7.2　应用调度

应用调度可以将不同地址范围和不同应用(对应于不同端口)的数据包根据您的配置从不同的WAN口转发。可应用于“线路组合模式”的主辅模式和ISP智能选线模式。单击打开菜单“多线路策略”→“应用调度”即可进入“应用调度”配置页面

- **目的端口范围**：选择应用所对应端口，例如 HTTP 应用对应 TCP 的 80 端口，DNS 应用对应 UDP 的 53 端口。
- **主出口**：符合应用调度规则的报文首先从主出口转发，主出口可以是 WAN 口名字，也可以是 WAN 口的 IP 地址。
- **备出口**：如果主出口连接断开，则将从备用出口转发。

点击“新建”可以添加一个应用调度规则，点击“修改”可以修改一个应用调度规则，点击“删除”可以删除一个应用调度规则。添加及修改页面如下：

- **协议**：如果选择“任意”，则此地址范围的所有报文都将按照您的配置转发。如果选择 TCP 或者 UDP 则必须配置一个端口范围(不同端口对应不同应用)，此时，只有符合此应用的数据包才会按照您的配置转发。
- **目的端口范围**：选择应用所对应端口，例如 HTTP 应用对应 TCP 的 80 端口，DNS 应用对应 UDP 的 53 端口。
- **主出口**：符合应用调度规则的报文首先从主出口转发，主出口可以是 WAN 口名字，也可以是 WAN 口的 IP 地址。
- **备出口**：如果主出口连接断开，则将从备用出口转发。

7.3 线路侦测

此页面可以为每个接口配置一条线路侦测，可以检查线路状况。单击打开菜单“多线路策略”→“线路侦测”即可进入“线路侦测”页面。

每个接口配置一条线路侦测，点击“新建”可以添加一条线路侦测。新建页面如下：

- **接口**：需要应用线路侦测功能的接口。
- **目的 IP 地址**：保持激活状态的目的 IP 地址。
- **检测周期**：检测链路的时间间隔。
- **下一跳地址**：到目的 IP 地址的下一跳 IP 地址。

如果接口已经配置了线路侦测，页面会自动填充您配置的数据，您也可以修改此数据然后点击“保存”按钮。每个接口只能配置一条线路侦测。

注意：线路侦测虽然只用于辅助多线路切换，但应谨慎选取侦测地址，如果选取不当，会导致接口主动断掉，导致网络不通。

第8章　路由配置

8.1　默认路由

就像PC 都会有个默认网关来连接本地路由器——路由器也要有默认路由，当路由器找不到访问某一网络的指定路径时，路由器便按照默认路由所指定的接口或者下一跳IP地址将数据包发到外网。默认路由可以由向导直接生成，一般无需手工配置。

8.1.1　默认路由信息显示

单击打开菜单“路由配置”→“默认路由”即可进入“默认路由列表页面”，在该页面列出了已经配置的默认路由信息，您可以单击“上一页”或者“下一页”进行浏览查看，也可以在搜索处的空白处输入要搜索的字段进行搜索查找。您也可以根据实际需要修改或删除已配置的默认路由，也可以单击新建按钮添加一条默认路由。

◆**序号**：为表内容的序号。

◆**转发接口**：如果配置的时候选择了转发接口，此字段显示您配置的接口。

◆**下一跳地址**：为路由的下一跳 IP，如果配置时在下一跳地址填入了 IP，这里会显示。

◆**路由优先级**：数值越大，优先级越低。

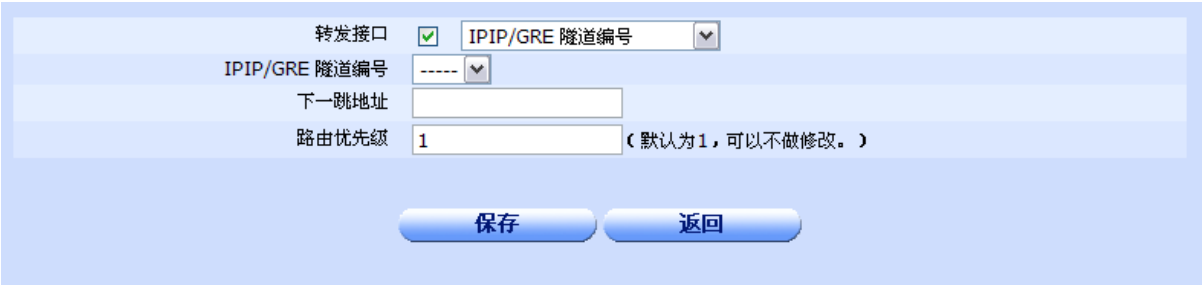
◆**操作**：单击修改超链接，进入默认路由配置页面，可以修改默认路由配置参数。单击“新建”按钮，可以添加一条默认路由。单击“删除”按钮，删除已选中的默认路由。

8.1.2　添加或修改默认路由

单击打开菜单“路由配置”→“默认路由”，再单击“新建”按钮，或者在默认路由信息显示中找到需要配置的默认路由，点击其对应的“操作”一栏的“修改”超链接，即可进入“默认路由配置页面”。

◆**转发到接口或 VPN 连接**：设置默认路由的转发接口，可以是 WAN 口，也可以是 LAN 口，也可以是 GRE/IPIP 通道，也可以是 PPTP/L2TP 的组名。

➢ 当选择了 IPIP/GRE 隧道编号的时候会提供已经配置了的 GRE/IPIP 隧道编号下拉框供您选择。



➢ 当选择了 L2TP/PPTP VPN 拨号连接的时候会提供已经配置了的 PPTP/L2TP VPN 拨号连接名供您选择。

◆**下一跳地址**：设置默认路由的下一跳地址，如果配置了转发接口，那么这个下一跳地址可以不配置。

◆**路由优先级**：设置默认路由的路由优先级，主要用在有主线路和备份线路的情况下，设置备份线路的优先级低于主线路的优先级，在主线路不通的情况下自动使用备份线路，数值越小，优先级越高。默认为 1，可以不做修改。

◆**保存**：参数输入完成后，单击“保存”按钮，将设置的信息保存到设备上，以使之生效。

保存后如果提示操作成功，则表示输入配置信息已经生效，如果提示操作失败，则用户需要重新输入参数，并检查自己输入的参数是否合法有效。

◆**返回**：单击该按钮返回默认路由信息显示页面。

8.2 静态路由

静态路由就是由用户手工配置的路由，是配置到达指定目的地址的数据包按照预定的路径传送。静态路由不会随网络结构的改变而改变，因此，当网络结构发生变化或出现网络故障时，需要手工修改静态路由信息。

8.2.1 静态路由信息显示

单击打开菜单“路由配置”→“静态路由”即可进入“静态路由列表页面”，在该页面列出了已经配置的静态路由信息，您可以单击“上一页”或者“下一页”进行浏览查看，也可以在搜索处的空白处输入要搜索的字段进行搜索查找。您也可以根据实际需要修改或删除已配置的静态路由，也可以单击新建按钮添加一条静态路由。

◆**序号**：为表内容的序号。

◆**目的网络地址**：已设置的静态路由的目的网络地址。

◆**目的网络掩码**：已设置的静态路由的目的网络掩码。

◆**转发接口**：如果配置的时候选择了转发接口，此字段显示您配置的接口。

◆**下一跳地址**：为路由的下一跳 IP，如果配置时在下一跳地址填入了 IP，这里会显示。

◆**路由优先级**：数值越大，优先级越低。

◆**操作**：单击“修改”超链接，进入静态路由配置页面，可以修改静态路由配置参数。单击“新建”按钮，可以添加一条静态路由。单击“删除”按钮，删除已选中的静态路由。

8.2.2 添加或修改静态路由

单击打开菜单“路由配置”→“静态路由”，再单击“新建”按钮，或者在静态路由信息显示中找到需要配置的静态路由，点击其对应的“操作”一栏的“修改”超链接，即可进入“静态路由配置页面”。

◆**目的网络地址**：设置静态路由的目的网络地址。

◆**目的网络掩码**：设置静态路由的目的网络掩码。

这两项为必填项，不填不能保存配置。

◆**转发到接口或 VPN 连接**：设置静态路由的转发接口，可以是 WAN 口，也可以是 LAN 口，也可以是 VPN 连接，如 GRE/IPIP 通道，PPTP/L2TP 的组名。

- 当选择了 IPIP/GRE 隧道编号的时候会提供已经配置了的 GRE/IPIP 隧道编号下拉框供您选择。

➢ 当选择了 L2TP/PPTP VPN 拨号连接的时候会提供已经配置了的 PPTP/L2TP VPN 拨号连接名供您选择。

◆**下一跳地址**：设置静态路由的下一跳地址，如果配置了转发接口，那么这个下一跳地址可以不配置。

◆**路由优先级**：设置静态路由的路由优先级，主要用在有主线路和备份线路的情况下，设置备份线路的优先级低于主线路的优先级，在主线路不通的情况下自动使用备份线路，数值越小，优先级越高。默认为 1，可以不做修改。

◆**保存**：参数输入完成后，单击“保存”按钮，将设置的信息保存到设备上，以使之生效。

保存后如果提示操作成功，则表示输入配置信息已经生效，如果提示操作失败，则用户需要重新输入参数，并检查自己输入的参数是否合法有效。

◆**返回**：单击该按钮返回静态路由信息显示页面。

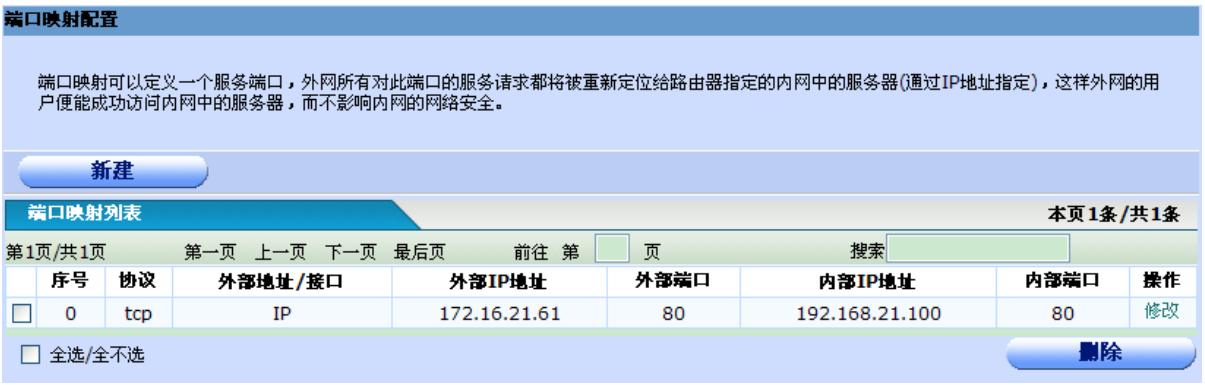
第9章　网络选项

9.1　端口映射

单击打开菜单“网络选项”→“端口映射”即可进入“端口映射配置”页面，此菜单分三个选项，“端口映射”，“特殊映射”和“DMZ 主机”。

9.1.1　端口映射

在路由器的默认配置下，广域网中的计算机无法访问局域网中的计算机，但是为了方便广域网合法用户对局域网中某台服务器的访问，又可以防止局域网计算机被非法入侵，路由器提供了端口映射功能。端口映射可以定义一个服务端口，外网所有对此端口的服务请求都将被重新定位给路由器指定的内网中的服务器(通过 IP 地址指定)，这样外网的用户便能成功访问内网中的服务器，而不影响内网的网络安全。



- **外部地址/接口**：可以是外网口也可以是外网口的 IP 地址。
- **外部 IP 地址**：外网口的ＩＰ地址。
- **外部端口**：显示ＷＡＮ端服务端口，即路由器提供给广域网的服务端口，外网对该端口的访问都将重定向到局域网中指定的服务器（内网ＩＰ地址指定）的端口（内部端口）。
- **内部 IP 地址**：局域网中的服务器ＩＰ地址。
- **内部端口**：局域网中的服务器端口。
- **新建**：添加一个端口映射。
- **删除**：勾选映射条目前的复选框，点击删除即可删除选中条目。
- **修改**：修改一个端口映射。

添加和修改页面如下：

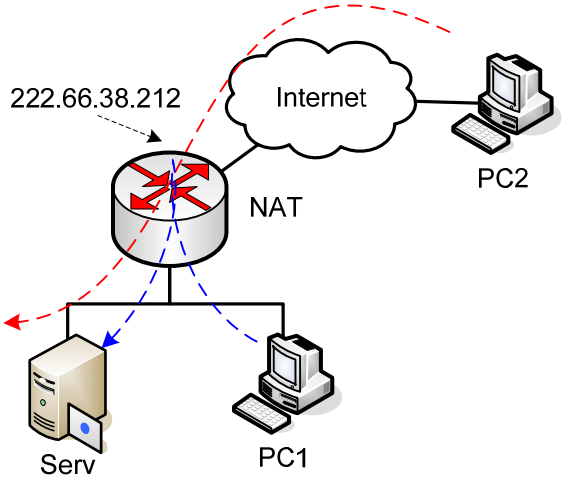
例如：如果一台设备外网口地址是 172.16.21.61，内网一台主机的地址是 192.168.21.100 ，如果想要将外网主机对 172.16.21.61 的 http 服务（80 端口）的访问重定向到 192.168.21.100 上，则只需将 192.168.21.100 的 80 端口与 172.16.21.61 的 80 端口建立映射即可，如上图所示。

注意:如果协议选择 all，那么内部 IP 地址(虚拟服务器)的所有端口将与外部 IP 地址(公网 IP)的所有端口做一对一的映射，如果只有一个外网 IP 地址，将导致内网其他主机不能上网。如果想要将一台主机完全暴露给 Internet，可以到 DMZ 主机中设置。

9.1.2 特殊映射

特殊映射可以实现在局域网中的主机以 internet 公网地址访问同一局域网中的另一主机。

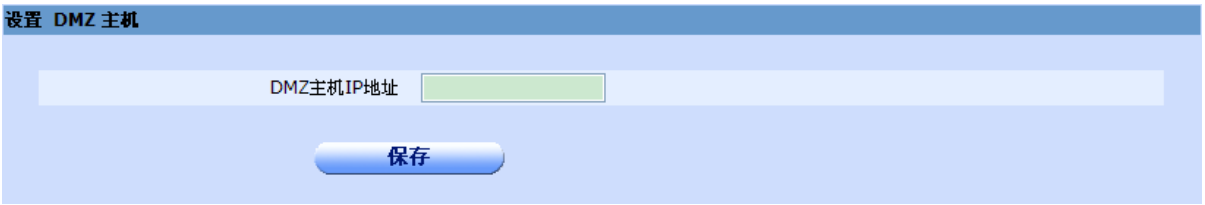
配置与端口映射基本相同，但含义有很大区别，例如：如下图



某小型企业，网络的大多数使用者都不知道 IP 为何物。所以他们在访问内部服务器 Serv 时必然会用到域名解析。但是因为网络规模和投资等关系，用户在局域网内部又没有（不想架设）专门的 DNS 服务器，所以只能借用 internet 上 ISP 的 DNS server。问题是，internet 上 DNS 解析出来的 IP 地址不可能是私网地址。现在要实现的是：PC1 访问 222.66.38.212 的数据流要被重新定向到 Serv，显然它的 IP 地址是一个私网地址。这时就要用到特殊映射，如果 serv 的 IP 地址是 192.168.21.1，pc1 的 IP 地址是 192.168.21.100，设备外网口地址是 222.66.38.212，那么 192.168.21.100 要访问 192.168.21.1 的 http 服务，只需将 192.168.21.1 的 80 端口与 222.66.38.212 的 80 端口做特殊映射即可。配置如下图所示：

9.1.3 DMZ主机

可以设置一台内网主机为 DMZ 主机，DMZ 主机可完全暴露给 Internet，实现双向通讯。



9.2 时间段配置

时间段配置可以分为 “单次时间段”和“循环时间段”。单击打开菜单“网络选项”→“时间段配置”即可进入“单次时间段配置”页面，可以通过点击TAB切换到“循环时间段配置”页面。

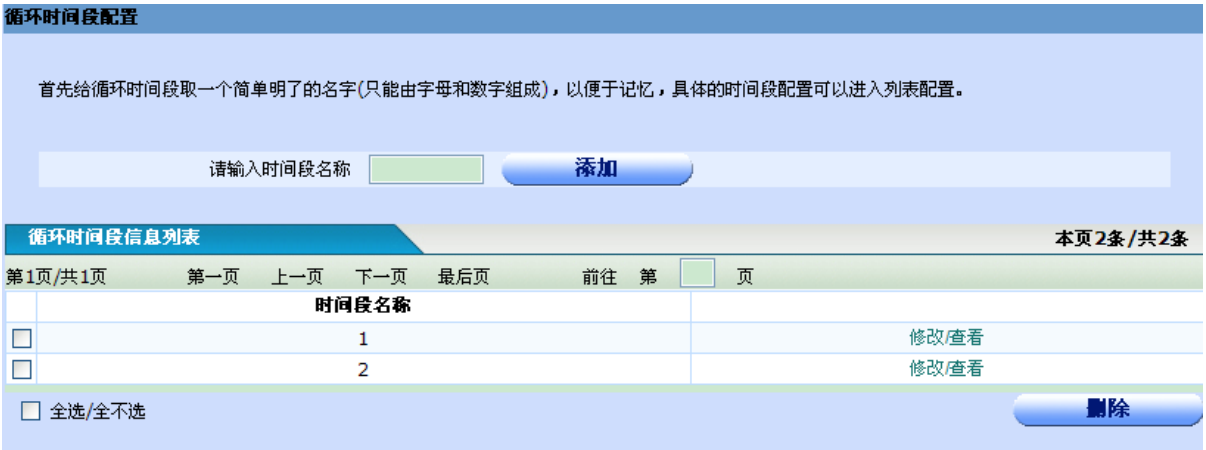
9.2.1 单次时间段配置

设置单次时间段。

点击“新建”可以添加一个单次时间段，单击“修改”可以修改一个单次时间段，添加和修改页面如下：

9.2.2 循环时间段配置

设置循环时间段。



要配置循环时间段，首先要给循环时间段取一个简单明了的名字，以便于其他地方使用该时间段。每个循环时间段可以配置多个子段，具体的子段配置可以点击“修改/查看”配置，页面如下：

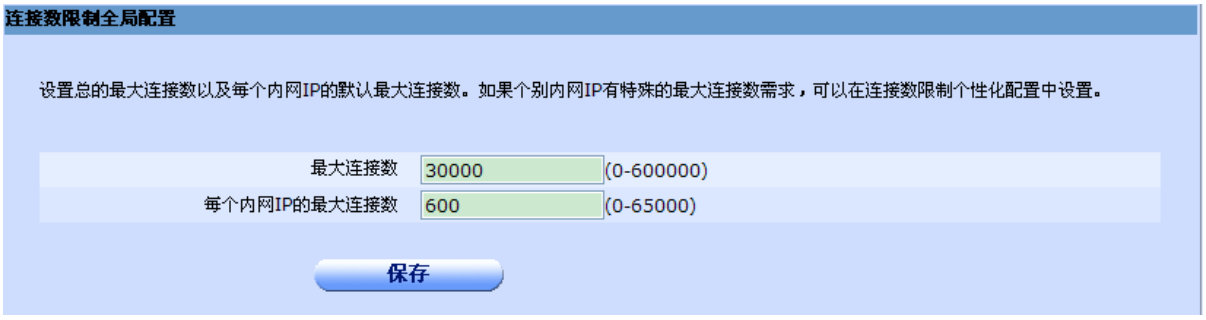
如果想要添加一个循环时间段子段，只需选择时间段类型，并填写开始和结束时间，然后点击“保存”即可，添加的结果显示在下面的列表中。如果想要删除一个子段，只需勾选子段前的复选框并点击“删除”即可。

9.3 连接数限制

连接数限制可以分为“连接数限制全局配置”和“连接数限制个性化配置”。

9.3.1 连接数限制全局配置

设置设备总的最大连接数以及每个内网 IP 的默认最大连接数，如果个别内网 IP 有特殊的最大连接数需求，可以在“连接数限制个性化配置”中设置，超过限制的新连接不允许通过设备。单击打开菜单“网络选项”→“连接数限制”即可进入“连接数限制全局配置”，通过 TAB 页可以切换到“连接数限制个性化配置”设置页面，设置页面如下：



- **最大连接数**：用于设置整个设备的最大连接数。
- **每个内网 IP 的最大连接数**：用于设定每个 IP 的默认最大连接数（一般为防止受病毒影响，条数设为 300 左右，看电脑使用情况，如果有 BT 下载，可能会多一些，经 200 台 PC 规模的网吧测试，600 条左右基本可以满足应用。）

9.3.2 连接数限制个性化配置

如果默认的内网主机最大连接数不能满足需求，则可以在此页面设置个性化的连接数。设置页面如下：

点击“新建”可以设置一个内网主机的最大连接数，点击“修改”可以修改一个内网主机的最大连接数，点击“删除”可以删除一个内网主机的最大连接数的个性化设置，此时主机的最大连接数将恢复到“连接数限制全局配置”中设置的最大连接数。

9.4 NAT访问控制

9.4.1 NAT 简介

NAT－“Network Address Translation”，中文是“网络地址转换”，它是一个 IETF(Internet Engineering Task Force, Internet 工程任务组)标准，允许一个整体机构以一个公用 IP（Internet Protocol）地址出现在 Internet 上.，是一种把内部私有网络地址（IP 地址）翻译成合法网络 IP 地址的技术。

NAT 屏蔽了内部网络，所有内部网计算机对于公共网络来说是不可见的，内部地址，是指在内部网络中分配给节点的私有 IP 地址，只能在内部网络中使用如 10.0.0.0~10.255.255.255，172.16.0.0~172.16.255.255，192.168.0.0~192.168.255.255；NAT 将这些无法在互联网上使用的保留 IP 地址翻译成可以在互联网上使用的全局 IP 地址，全局地址是全球统一的可寻址的地址。

9.4.2 NAT 访问控制

每个 WAN 口都可以配置多个访问控制列表，这些列表可以控制哪些地址范围允许或禁止进行 NAT 转换。单击打开菜单“网络选项”→“NAT 访问控制”即可进入“NAT 访问控制”设置页面

注意：不启用 NAT 模式时设备将工作于路由模式，这时每台主机必须对应唯一的公网 IP 才能上网，一般选择启用 NAT 模式。

点击“新建”可以添加一个访问控制列表，点击“修改”可以修改一个访问控制列表，添加和修改页面如下：

- **状态**：允许或者禁止。
- **IP 地址类型**：可以分为任意 IP 地址、指定 IP 地址、指定 IP 地址范围和指定 IP 子网。
- **插入位置**：访问控制列表是一个有序的语句集，它通过自上而下的顺序来匹配报文中信息与访问表参数，来允许报文通过或拒绝报文通过某个接口。判断规则是如果通过了一个访问列表中的某一项规则，将停止匹配规则，不再试图与它以后的规则比较。

9.5 DNS配置

DNS服务实现域名解析的功能，DNS服务器一般由ISP提供，最多可以配置6个DNS服务器。单击打开菜单“网络选项”→“DNS配置”即可进入“DNS配置”页面，DNS列表页面如下：

如果启动 DNS 代理，那么局域网中的计算机只需将 DNS 服务器设置为设备的 LAN 口地址，就可以正常使用 DNS 服务。

点击“新建”可以添加一个 DNS 服务器。添加和修改页面如下：

9.6 DDNS配置

ＤＤＮＳ又名动态ＤＮＳ，它的主要功能是实现固定域名到动态ＩＰ地址之间的解析。如果服务的ＩＰ地址是动态获取的，比如通过ＤＨＣＰ和ＰＰＰＯＥ拨号分配，可以通过动态域名解析来将这个动态的ＩＰ地址绑定到一个固定的域名上，目前只支持“花生壳”。单击打开菜单“网络选项”→“DDNS 配置”即可进入“DDNS 配置”页面。

配置列表如下所示：

- **新建**：添加一个 DDNS 列表。
- **删除**：勾选 DDNS 条目前的复选框，点击删除即可删除选中条目。
- **修改**：修改一个 DDNS 列表。

配置页面如下：

- **名称**：填入为该配置取的一个名称
- **是否启用**：勾选表示启用。
- **用户名，密码**：填入注册的用户名和密码。
- **DDNS 服务器，端口号**：填入花生壳提供的服务器及端口。我们默认提供了 2 个 DDNS 的服务器，如有需要请自行更改您所需的服务器。
- **绑定接口**：选择一个欲绑定的端口。

9.7 DHCP配置

所有基于 TCP/IP 协议族实现的网络，其通信的一个重要基础就是 IP 地址，但对于大多数非专业的用户而言，IP 地址是什么都不甚了解，要正确设置或者修改就更难了，但用户主机需要访问网络时，其网卡的 IP 却又是必不可少的。DHCP－Dynamic Host Control Protocol 动态主机配置协议，就是用于简化主机 IP 地址设置的协议。通过 DHCP，用户可以实现各项必要网络参数 IP、DNS 等的“零设置”，做到“即插即用”。启用 DHCP 服务器功能后，设备就能够为局域网计算机动态分配 IP 地址、子网掩码、网关、以及 DNS 服务器等信息。

- **起始和结束ＩＰ地址**：填入欲分配给局域网内 PC 的一个地址段。(默认掩码为 255.255.255.0)
- **网关地址**：一般为路由器上连接局域网的端口的 IP 地址。
- **主备ＤＮＳ服务器**：填入局域网内 PC 应配置的 DNS 服务器。如果您需要启动 DNS 代理，请将分配给客户机的主 DNS 设为网关 IP 地址。
- **租用时间**：默认是一天。
- **新建**：添加一个 DHCP 服务器。
- **删除**：勾选 DHCP 服务器前的复选框，点击删除即可删除选中条目。
- **修改**：修改一个 DHCP 服务器。

添加和修改页面如下：

注意：DHCP 地址池的网段必须与内网口的网段相同才能生效。

9.8 PPPOE服务器

如果您要实现在PC机上通过本设备拨号上网，就需要在本设备上建立PPPOE服务器，然后PC拨号到本设备来实现通过该设备上网。

9.8.1 PPPOE服务端配置信息

单击打开菜单“网络选项”→“PPPOE服务器”即可进入“PPPOE服务端配置信息列表页面”，在该页面列出了已经配置的PPPOE服务，您可以单击“上一页”或者“下一页”进行浏览查看，也可以在搜索处的空白处输入要搜索的字段进行搜索查找。您也可以根据实际需要修改或删除已配置的PPPOE服务，也可以单击新建按钮添加一个PPPOE服务。

◆**PPPOE 服务名**：显示 PPPOE 的服务名，用来区分不同的 PPPOE 服务。

◆**PPPOE 服务端 IP**：显示此服务使用的 IP。

◆**PPPOE 客户端获取地址的方式**：显示给 PPPOE 客户端分配地址的方式，有“不指定”，“IP”和“地址池”三种。

◆**应用接口**： 显示 PPPOE 服务应用的接口。

◆**操作**：单击“修改”超链接，进入 PPPOE 服务器配置页面，可以修改 PPPOE 服务器配置参数。单击“新建”按钮，可以添加一个 PPPOE 服务。单击“删除”按钮，删除已选中的 PPPOE 服务。LAN 口只能应用一个 PPPoE 服务，如果已存在，新建按钮将会被禁用。

9.8.2 添加或修改PPPOE服务

单击打开菜单“网络选项”→“PPPOE 服务器”，再单击“新建”按钮，或者在 PPPOE 服务端配置信息显示中找到需要配置的 PPPOE 服务器，点击其对应的“操作”一栏的“修改”超链接，即可进入“PPPOE 服务器配置页面”。

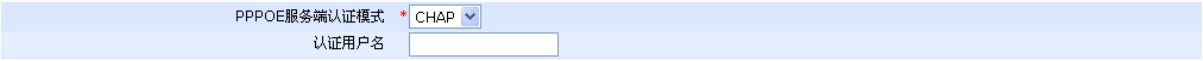
◆**PPPOE 服务名**：设置 PPPOE 的服务名，此字段为系统自动生成，用户不可修改。

◆**PPPOE 服务端 IP**：设置服务端使用的 IP 地址。

◆**PPPOE 服务端子网掩码**：设置 PPPOE 服务端使用的子网掩码。

◆**PPPOE 服务端认证模式**：可以选择“PAP”认证或者“CHAP”认证。

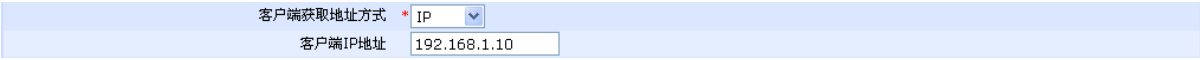
➢ **PPPOE 服务端认证模式**：“PAP”。选择此项的话下方不会有任何提示，如上图。



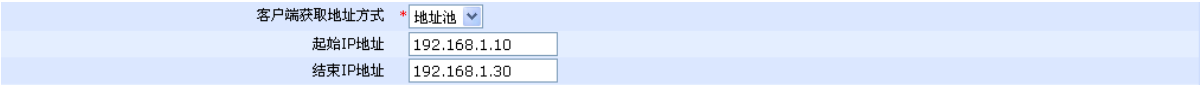
➢ **PPPOE 服务端认证模式**：选择“CHAP”后下方会有一个认证用户名输入框用来输入认证用户名，如上图。

◆**客户端获取地址方式**：可以选择“不指定”，“IP”或者“地址池”。

➢ **客户端获取地址方式**：“不指定”。选择此项的话下方不会有任何提示。如上图。



➢ **客户端获取地址方式**：选择“IP”后下方会出现一个 IP 地址输入框来输入 IP 地址。如上图。



➢ **客户端获取地址方式**：选择“地址池”后会出现两个 IP 地址输入框来确定地址池包含的地址范围。如上图。

◆**应用接口**：应用接口默认设置为 LAN 口，用户不可修改。

★**注意**：

地址池中的地址数量不能超过 1024 个，否则会设置失败。

◆**保存**：参数输入完成后，单击“保存”按钮，将设置的信息保存到设备上，即依照给定的参数进行 PPPOE 服务器设定。保存后如果提示操作成功，则表示输入配置信息已经生效，如果提示操作失败，则用户需要重新输入参数，并检查自己输入的参数是否合法有效。

◆**返回**：单击该按钮返回 PPPOE 服务器配置信息列表页面。

◆**配置拨号用户**：如果想要添加或者修改拨号登录的用户名或者密码，请单击此按钮进入拨号用户管理相关页面，也可以在“虚拟专网”→“拨号用户管理”页面来修改。

★**注意**：

如果由服务端给客户端分配 IP 或者地址池，设备会自动将单一 IP 或者地址池中的所有 IP 添加到 NAT 访问列表中并设为允许，如果不小心删除，可能客户端会无法上网。

9.8.3 PPPOE会话信息

在 Tab 标签上单击 PPPOE 会话信息标签，进入 PPPOE 会话信息列表页面，如下图：

◆**本地地址**：显示本条会话的本地隧道地址。

◆**远程地址**：显示与本地地址连接的远程隧道地址。

◆**拨号用户名**：显示拨号到本服务器上的用户名。

◆**状态**：显示本条会话的状态。

◆**刷新按钮**：单击此按钮获得即时 PPPOE 会话信息。

9.9 UPnP配置

UPnP（Universal Plug and Play，通用即插即用）主要用于实现设备的智能互联互通，旨在实现一种“零”配置和“隐性”的联网过程，自动发现和控制来自各家厂商的各种网络设备。 在设备上启用UPnP功能后，可以实现穿透NAT：当局域网的主机通过设备与Internet上的终端进行通讯时，可以根据需要自动增加、删除 NAT 映射，从而保证支持 UPnP 的软件可以在NAT后正常使用。 通过 UPnP NAT 映射列表，可以查看经 UPnP 建立的 NAT 静态映射的相关信息，包括：内部地址、内部端口、协议、对端地址、外部端口以及信息描述。

单击打开菜单“网络选项”→“UPnP配置”即可进入“UPnP配置”页面，在该页面用户可以启用/停止UPnP服务或者查看当前设备中的“UPnP NAT映射信息列表”中UPnP映射信息。

9.9.1 启用/停止UPnP服务

单击打开菜单“网络选项”→“UPnP 配置”即可进入“UPnP 配置”页面，在该页面用户可以启用/停止 UPnP 服务。

◆ **启用 UPnP 服务**：启用/停止 UPnP 服务，选中为启用，启用/停用 UPnP 服务均需单击“应用”按钮提交后才能生效。设备仅支持在 LAN 口启用 UPnP 功能。

◆ **应用**：选择启用/停用服务后，单击“应用”按钮，将设置的信息保存到设备上，以使之生效。

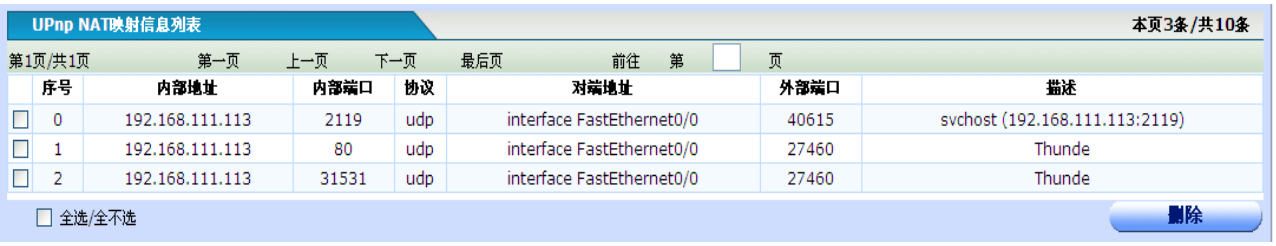
应用后如果提示操作成功，则表示配置信息已经生效，如果提示操作失败，用户需要修改设置信息重新提交。

> 提示：
>
> 对于部分 **UPnP** 应用软件，如 **MSN** 等需要打开计算机操作系统上的 **UPnP** 服务才能起作用。按以下方式打开计算机系统上的 **UPnP** 服务。进入“开始”菜单→“控制面板”→“服务”。在打开的“服务”窗口将“**SSDP Discovery Service**”和“**Universal Plug and Play Device Host**”服务依次启用。

UPnP 功能在 P2P 中应用广泛，能够省去繁琐的设置，有效的提升 P2P 软件的下载速率和性能，

9.9.2 UPnP NAT映射信息列表

单击打开菜单“网络选项”→“UPnP配置”即可进入“UPnP配置”页面，在该页面用户可以查看当前设备中的“UPnP NAT映射信息列表”中UPnP映射信息。



序号	内部地址	内部端口	协议	对端地址	外部端口	描述
0	192.168.111.113	2119	udp	interface FastEthernet0/0	40615	svchost (192.168.111.113:2119)
1	192.168.111.113	80	udp	interface FastEthernet0/0	27460	Thunde
2	192.168.111.113	31531	udp	interface FastEthernet0/0	27460	Thunde

◆**内部地址**：发起UPnP NAT映射的局域网内主机的IP地址。
◆**内部端口**：发起UPnP NAT映射的局域网内主机提供的服务端口。
◆**协议**：该UPnP NAT映射使用的协议，一般为TCP或UDP协议。
◆**对端地址**：UPnP NAT映射中使用的设备外网接口的IP地址或接口。
◆**外部端口**：内部端口经 NAT 转换后的端口，即设备提供给 Internet 的供访问的服务端口。
◆**描述**：用来描述相关UPnP设备厂家的信息。
◆**全选/全不选**：全部选中/全部不选中 当前页的信息记录。
◆**删除**：用鼠标选中或全选列表栏中的信息记录（即使显示信息行前面的复选框打勾），单击“删除”按钮删除选中的UPnP NAT映射信息。

个人计算机(PC)使用 UPnP 的方法举例如下：

如果您的电脑开启了防火墙功能，请在 Windows 防火墙界面的例外选项中，选中启用 UPnP 框架程序，具体操作方法步骤为：开始→控制面板→安全中心→Windows 防火墙→例外→选中 UPnP 框架。若例外项中没有 UPnP 选项，则点击添加程序，再选中 UPnP 功能即可。

> 提示：
>
> 如果用户删除 **UPnP NAT** 映射，会导致发起映射的主机对应的服务无法被外网访问。

提示：

不使用时请关闭 **UPnP** 功能，只有支持 **UPnP** 协议的应用程序才能使用本功能。

★注意：

如果个人计算机通过其他网络设备连接到本设备的话，将会导致 **UPnP** 功能无法正常使用。

第10章 ARP安全

在设备中，ARP绑定可以实现用户的身份识别。使用设置的ARP绑定作为用户唯一的身份识别标识，可以保护设备和网络不受IP欺骗的攻击。

10.1 ARP手动绑定

手动绑定每次只能实现单条绑定。

10.1.1 ARP静态绑定信息列表

单击打开菜单“ARP安全”→“ARP手动绑定”即可进入“ARP绑定列表页面”，在该页面列出了已经配置的ARP绑定信息，您可以单击“上一页”或者“下一页”进行浏览查看，也可以在搜索处的空白处输入要搜索的字段进行搜索查找。您也可以根据实际需要修改或删除已配置的 ARP绑定，也可以单击新建按钮添加一条ARP绑定。

◆**序号**：为表内容的序号。

◆**IP 地址**：已设置的 ARP 绑定的 IP 地址。

◆**MAC 地址**：已设置的 ARP 绑定的 MAC 地址。

◆**操作**：单击“修改”超链接，进入 ARP 绑定配置页面，可以修改 ARP 绑定配置参数。单击“新建”按钮，可以添加一条 ARP 绑定。单击“删除”按钮，删除已选中的 ARP 静态绑定。

> 提示：
>
> 表格的标题栏带有下划线表示表格可以依照此字段进行排序，方便查找。

10.1.2 添加或修改ARP静态绑定配置

单击打开菜单“ARP安全”→“ARP手动绑定”，再单击“新建”按钮，或者在ARP静态绑定信息列表中找到需要配置的ARP绑定，点击其对应的“修改”一栏的“修改”超链接，即可进入“ARP绑定配置页面”。

◆**IP 地址**：设置 ARP 绑定的 IP 地址，格式为点分十进制 IP。

◆**MAC 地址**：设置 ARP 绑定的 MAC 地址，格式为 aabbccddeeff，aa-bb-cc-dd-ee-ff 或者 aa:bb:cc:dd:ee:ff。

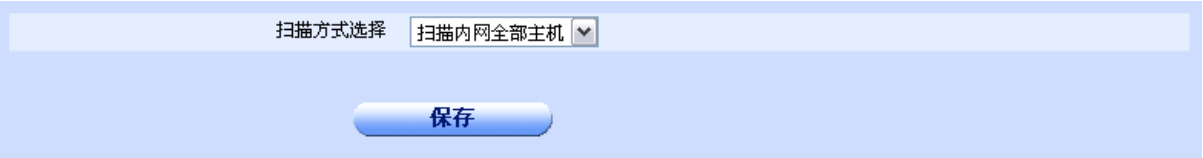
◆**保存**：参数输入完成后，单击“保存”按钮，将设置的信息保存到设备上，即依照给定的 IP 地址和 MAC 地址进行一对一绑定。保存后如果提示操作成功，则表示输入配置信息已经生效，如果提示操作失败，则用户需要重新输入参数，并检查自己输入的参数是否合法有效。

◆**返回**：单击该按钮返回ARP静态绑定信息列表页面。

10.2 ARP扫描绑定

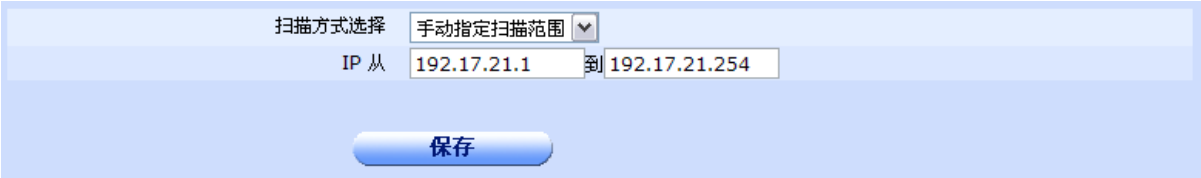
ARP扫描绑定可以扫描内网主机的IP地址和MAC地址并自动进行一对一绑定，如果内网有新的PC加入，ARP扫描绑定会自动扫描到它的IP和MAC地址并将其自动添加到ARP绑定列表内。

单击打开菜单“ARP安全”→“ARP扫描绑定”即可进入“ARP扫描绑定配置页面”。



◆ **扫描方式选择**：可以选择“扫描内网全部主机”，“手动指定扫描范围”和“禁止扫描 ARP 并取消绑定”。默认显示当前设备已使用的扫描方式。

- 当选择了“手动指定扫描范围”时会在下方显示两个输入框，里面默认填入了可以扫描的子网范围（如果当前设备使用的就是本方式，那么在进入本页面时这两个输入框默认填入的是设备配置的扫描范围）。



- 若选择了“禁止扫描并取消绑定”，则设备将不会扫描 ARP，而且原有的扫描结果也将自动删除（通过手动绑定添加的绑定将保留）。

◆**保存**：参数输入完成后，单击“保存”按钮，将设置的信息保存到设备上。保存后如果提示操作成功，则表示输入配置信息已经生效，单击“返回”，返回 ARP 静态绑定列表，便于您查看 ARP 扫描结果。如果提示操作失败，则用户需要重新操作。

★注意：

不管是 **ARP** 静态绑定还是扫描绑定，设备的 **ARP** 绑定以后，个人计算机（**PC**）端也应当做相应的绑定，否则可能会导致绑定不生效。

10.3 IP+MAC地址过滤

IP+MAC地址过滤可以限制指定的IP和主机地址对的数据包通过本设备，可以有效的保护网络，防止被攻击或者病毒感染。

10.3.1 “IP+MAC 过滤”列表

单击打开菜单“ARP安全”→“IP+MAC过滤”即可进入“IP+MAC列表页面”，在该页面列出了已经配置的IP+MAC过滤信息，您可以单击“上一页”或者“下一页”进行浏览查看，也可以在搜索处的空白处输入要搜索的字段进行搜索查找。您也可以根据实际需要修改或删除已配置的IP+MAC过滤，也可以单击新建按钮添加一条IP+MAC过滤。列表上方有“导入”按钮，可以方便的将已配置好的所有ARP绑定导入到IP+MAC过滤中并将状态自动设置为允许。配置完成后要勾选“启用IP+MAC过滤”单选框并应用来使配置生效。

◆**序号**：为表内容的序号。

◆**状态**：显示此条过滤配置为“允许”还是“拒绝”。

◆**IP 地址**：已设置的 IP+MAC 过滤的 IP 地址。

◆**匹配其它 MAC 地址**：为 0 表示不允许此 IP 匹配其它 MAC 地址，为 1 表示允许。

◆**MAC 地址**：已设置的 IP+MAC 过滤的 MAC 地址。

◆**匹配其它 IP 地址**：为 0 表示不允许此 MAC 匹配其它 IP 地址，为 1 表示允许。

◆**操作**：单击“修改”超链接，进入 IP+MAC 配置页面，可以修改 IP+MAC 过滤的配置参数。单击“新建”按钮，可以添加一条 IP+MAC 过滤。单击“删除”按钮，删除已选中的 IP+MAC 过滤。

> 提示：
>
> 表格的标题栏带有下划线表示表格可以依照此字段进行排序，方便查找。

> ★注意：
>
> **1. 一定要先把操作主机添加到 IP+MAC 过滤规则中并设置为允许访问，否则启用后因为未将其添加到允许列表中而被过滤，进而将不能继续操作！如当前使用 web 配置的电脑 IP 为 192.168.1.10, MAC 地址为 002233445566，一定要将这个这个 IP 与 MAC 地址对加到过滤规则中并将其状态设置为允许，否则应用后由于被拒绝而不能继续配置设备。**
>
> **2. 配置完成后要勾选上方的启用 IP+MAC 过滤，然后单击“应用”之后才能生效！**

10.3.2 添加或修改“IP+MAC 过滤”配置

单击打开菜单“ARP安全”→“IP+MAC过滤”，再单击“新建”按钮，或者在IP+MAC过滤显示中找到需要配置的IP+MAC过滤，点击其对应的“修改”一栏的“修改”超链接，即可进入“IP+MAC过滤配置页面”。

◆**状态**：设置此过滤为“允许”还是“拒绝”。

◆**IP 地址**：设置 IP+MAC 过滤的 IP 地址，格式为点分十进制 IP。

◆**允许匹配其它 MAC**：允许此 IP 匹配其它 MAC。

◆**MAC 地址**：设置 IP+MAC 过滤的 MAC 地址，格式为 aabbccddeeff，aa-bb-cc-dd-ee-ff 或者 aa:bb:cc:dd:ee:ff。

◆**允许匹配其它 IP**：允许此 MAC 匹配其它 IP。

◆**<<--**：右侧列表为 ARP 绑定列表，可以通过此按钮将列表中的 IP 和 MAC 填入到左侧的 IP 地址和 MAC 地址的文本框内。

◆**保存**：参数输入完成后，单击“保存”按钮，将设置的信息保存到设备上，即依照给定的参数进行 IP+MAC 过滤设定。保存后如果提示操作成功，则表示输入配置信息已经生效，如果提示操作失败，则用户需要重新输入参数，并检查自己输入的参数是否合法有效。

◆**返回**：单击该按钮返回IP+MAC过滤列表页面。

第11章　网络安全

11.1　防火墙配置

防火墙就是一个位于计算机和它所连接的网络之间的软件或硬件。该计算机流入流出的所有网络通信均要经过此防火墙。防火墙能够对内部网络具有很好的保护作用，是一种将内部网和公众访问网(如Internet)分开的方法，它实际上也是一种隔离技术，因为网络入侵者必须首先穿越防火墙的安全防线，才能接触目标计算机，防火墙对流经它的网络通信进行扫描，这样能够过滤掉一些攻击，以免其在目标计算机上被执行，防火墙还可以关闭不使用的端口或禁止特定端口的流出通信，封锁特洛伊木马。同时，它可以禁止来自特殊站点的访问，从而防止来自不明入侵者的所有通信。

防火墙在两个网络通讯时执行的一种访问控制尺度又称“访问控制策略”，所以用户能够通过配置防火墙功能允许你“同意”的人和数据进入你的网络，同时将你“不同意”的人和数据拒之门外，最大限度地阻止网络中的黑客来访问你的网络。

访问控制策略是网络安全防范和保护的主要策略，其任务是保证网络资源不被非法使用和非法访问。通过访问控制策略，可以允许或阻止用户访问某些网络；可以控制用户访问网络的时段；可以控制不同的用户不同的网络访问权限。

防火墙访问控制策略的工作流程：在设备中配置访问控制策略，可以监测流经设备的每个数据包。默认情况下，设备中没有配置任何访问控制策略，设备将转发接收到的所有合法的数据包。如果在某接口配置了访问控制策略，当数据包到达此接口后，它会取出此数据包的源MAC地址、源地址、目的地址、上层协议、端口号或包内容进行分析，并从策略表的顶端从上至下搜索策略表，查看是否有匹配的策略，并执行匹配的第一个策略所定义的动作：转发或丢弃。并且不再继续比较其余的策略。如果与所有的策略都不匹配，出于安全的考虑，设备将丢弃这个数据包。

单击打开菜单“网络安全”→“防火墙配置”即可进入“防火墙配置”TAB选项选择页面，在该页面用户可以选择需要配置防火墙的接口，如下图。

用户可以通过切换TAB选项页面，来选择防火墙应用的接口，如WAN0防火墙配置或选择LAN防火墙配置。

11.1.1　启用/停止接口防火墙服务

单击打开菜单“网络安全”→“防火墙配置”进入“防火墙配置”接口 TAB 选项选择页面，单击选择需要配置防火墙的接口，在打开的“防火墙配置”页面，即可启用/停止本接口防火墙服务。如下图。

- **启用本接口防火墙服务：**启用/停止本接口防火墙服务，选中为启用，未选中表示停止，启用/停用本接口防火墙服务均需单击“应用”按钮提交后才能生效。

◆ **应用**：选择启用/停用服务后，单击“应用”按钮，将设置的信息保存到设备上，以使之生效。

应用后如果提示操作成功，则表示配置信息已经生效，如果提示操作失败，用户需要修改设置信息重新提交。

> **提示：**
>
> 启动/停止防火墙服务只对选定的配置接口有效!

> **提示：**
>
> 建议在对应接口的防火墙规则配置完成后再启动该接口的防火墙服务!

11.1.2 查看防火墙规则信息列表

单击打开菜单“网络安全”→“防火墙配置”进入“防火墙配置”接口TAB选项选择页面，单击选择需要配置防火墙的接口，在打开的“防火墙配置”页面，即可看到“防火墙规则信息列表”，在该列表中可以查看、修改、删除具体的防火墙规则。如下图。

动作	协议	源地址类型	源地址规则	源端口规则	目的地址类型	目的地址规则	目的端口规则	时间段	操作
允许	ip	任意IP地址	---	---	任意IP地址	---	---		修改
允许	ip	指定IP地址	10.1.1.23	---	指定IP地址	10.1.1.23	---		修改
允许	udp	指定IP地址范围	110.11.1.1~110.11.1.199	端口号等于80	指定IP地址范围	222.23.34.56~222.23.34.234	指定端口号范围50 - 1024		修改
允许	icmp	指定IP子网	102.2.23.5/255.255.255.0	---	指定IP子网	112.2.23.5/255.255.255.0	---		修改
禁止	tcp	任意IP地址	---	任意端口	指定IP子网	123.1.1.1/222.3.23.3	端口号不等于45		修改

动作：描述了对符合防火墙规则的报文采取的动作，这里可以是“允许”或“禁止”。“禁止”表示禁止符合防火墙规则的报文转发；“允许”表示允许符合防火墙规则的报文转发。

协议：定义的防火墙规则适用的具体的协议类型。一般为 IP、ICMP、UDP、TCP。

源地址类型：防火墙规则中定义的规则的源地址类型，包括以下几种：

- 任意 IP 地址：任意 IP 地址，即规则对 IP 地址不做检查和限制。
- 指定 IP 地址：指定具体 IP 地址，即规则只对与给定的 IP 地址一致的报文有效。
- 指定 IP 地址范围：指定 IP 地址范围，即规则只对在给定的 IP 地址范围内的报文有效。
- 指定 IP 子网：指定 IP 子网，即规则只对在给定的 IP 子网网段内的报文有效。

源地址规则：防火墙规则中源地址的具体数据值，不同源地址类型，显示的信息也有所不同。

- 对于源地址类型是任意 IP 地址：默认所有 IP 地址，故不显示。
- 对于源地址类型是指定 IP 地址：显示信息是具体的 IP 地址，格式如 10.1.1.23。

- 对于源地址类型是指定 IP 地址范围：显示信息是合法的 IP 地址范围段，格式如 110.11.1.1~110.11.1.199，前面是开始 IP 地址，后面是结束 IP 地址。
- 对于源地址类型是指定 IP 子网：显示的信息是合法的 IP 子网，格式如 102.2.23.5/255.255.255.0，前面是子网 IP，后面是子网掩码。

源端口规则：防火墙规则中的源端口号匹配规则，显示信息和“协议”栏有关。

- 协议类型为 IP：该类型下的源端口规则表示规则适用于该协议内的所有端口，因此栏内信息不显示具体端口数值。
- 协议类型为 ICMP：该类型下的源端口规则表示规则适用于 ICMP 协议的默认端口，因此栏内不显示具体端口数值。
- 协议类型为 UDP 或 TCP：这两种协议类型下，源端口规则显示信息有如下几种类型。

  →任意端口：源端口规则栏显示“任意端口”。表示适用于所有端口。

  →端口号等于：源端口规则栏显示“端口号等于 XXX”，这里 XXX 是数字，用以表示具体端口号，例如“端口号等于 8080”。表示防火墙规则中要求源端口号等于 8080。

  →端口号小于：源端口规则栏显示“端口号小于 XXX”，这里 XXX 是数字，用以表示具体端口号，例如“端口号小于 8080”。表示防火墙规则中要求源端口号小于 8080。

  →端口号大于：源端口规则栏显示“端口号大于 XXX”，这里 XXX 是数字，用以表示具体端口号，例如“端口号大于 8080”。表示防火墙规则中要求源端口号大于 8080。

  →端口号不等于：源端口规则栏显示“端口号不等于 XXX”，这里 XXX 是数字，用以表示具体端口号，例如“端口号不等于 8080”。表示防火墙规则中要求源端口号不等于 8080。

  →指定端口范围：源端口规则栏显示“指定端口范围 XXX~YYY”，这里 XXX，YYY 是数字，用以表示具体端口号，例如“指定端口范围 8080~8090”。表示防火墙规则中要求源端口号在 8080 和 8090 之间。

目的地址类型：防火墙规则中定义的规则的目的地址类型，具体类型说明参见“源地址类型”中的说明。

目的地址规则：防火墙规则中定义的规则的目的地址规则，具体类型说明参见“源地址规则”中的说明。

目的端口规则：防火墙规则中的目的端口号匹配规则，显示信息和“协议”栏有关。具体类型说明参见“目的端口规则”中的说明。

时间段：此防火墙规则适用的时间范围，如不选择时间段范围，默认防火墙规则在所有时间范围内都有效。如要使防火墙规则在指定时间范围内有效，则必须先配置时间段再配置或修改防火墙规则。打开“网络选项”→“时间段配置”菜单即可配置时间段。

11.1.3 添加防火墙规则

单击打开菜单“网络安全”→“防火墙配置”进入“防火墙配置”接口TAB选项选择页面，单击选择需要配置防火墙的接口，在打开的“防火墙配置”页面，如下图。在该页面单击“新建”以添加防火墙规则信息。

动作	协议	源地址类型	源地址规则	源端口规则	目的地址类型	目的地址规则	目的端口规则	时间段	操作
允许	ip	任意IP地址	---	---	任意IP地址	---	---		修改
允许	ip	指定IP地址	10.1.1.23	---	指定IP地址	10.1.1.23	---		修改
允许	udp	指定IP地址范围	110.11.1.1~110.11.1.199	端口号等于80	指定IP地址范围	222.23.34.56~222.23.34.234	指定端口号范围50 - 1024		修改
允许	icmp	指定IP子网	102.2.23.5/255.255.255.0	---	指定IP子网	112.2.23.5/255.255.255.0	---		修改
禁止	tcp	任意IP地址	---	任意端口	指定IP子网	123.1.1.1/222.3.23.3	端口号不等于45		修改

用户单击“新建”按钮后，打开“防火墙规则配置”配置页面。如下图。

◆**动作**：描述了对符合防火墙规则的报文采取的动作，这里可以是“允许”或“禁止”。“禁止”表示禁止符合防火墙规则的报文转发；“允许”表示允许符合防火墙规则的报文转发。

◆**协议**：定义的防火墙规则适用的具体的协议类型。一般为 IP、ICMP、UDP、TCP。

◆**源 IP 地址类型**：防火墙规则中定义的规则的源地址类型，包括以下几种：

- 任意 IP 地址：任意 IP 地址，即规则对 IP 地址不做检查和限制。
- 指定 IP 地址：指定具体 IP 地址，即规则只对与给定的 IP 地址一致的报文有效。
- 指定 IP 地址范围：指定 IP 地址范围，即规则只对在给定的 IP 地址范围内的报文有效。
- 指定 IP 子网：指定 IP 子网，即规则只对在给定的 IP 子网网段内的报文有效。

◆**源端 IP 地址**：如果用户在“源 IP 地址类型”中选择“任意 IP 地址”，则页面将不显示本配置参数行。选择其他类型，则会有不同的 IP 地址参数输入要求。下面是选择不同地址类型需要配置的参数。

- 任意 IP 地址：无配置参数，配置页面将隐藏本配置行。
- 指定 IP 地址：输入具体 IP 地址，如 192.168.1.1。
- 指定 IP 地址范围：在起始 IP 地址后输入地址范围开始的 IP 地址，如 192.168.1.1；在结束 IP 地址后输入地址范围结束的 IP 地址，如 192.168.1.100。
- 指定 IP 子网：在子网地址后输入子网的 IP 地址，如 192.168.1.1；在子网掩码后输入子网的掩码,如 255.255.255.0。

◆**源端端口号**：只有用户在“协议”中选择协议类型为 TCP 或 UDP 的情况下，才会显示“源端端口号”配置参数行。选择 IP 或 ICMP 将不显示本配置行。源端端口号有如下几种选择类型：

- 任意端口：表示针对所有端口（0～65535）。不需要输入任何参数。
- 端口号等于：在端口号后的输入框中输入具体的端口号数值，如 8080，表示当规则匹配的时候要求协议的端口号等于 8080 端口。
- 端口号小于：在端口号后的输入框中输入具体的端口号数值，如 8080，表示当规则匹配的时候要求协议的端口号小于 8080 端口。
- 端口号大于：在端口号后的输入框中输入具体的端口号数值，如 8080，表示当规则匹配的时候要求协议的端口号大于 8080 端口。
- 端口号不等于：在端口号后的输入框中输入具体的端口号数值，如 8080，表示当规则匹配的时候要求协议的端口号不等于 8080 端口。

➢ 指定端口范围：在起始端口号后输入端口范围起始的端口号，如 8080，在结束端口号后输入端口范围结束的端口号，如 8090，表示当规则匹配的时候要求协议的端口号在 8080 和 8090 之间。

◆**目的端 IP 地址类型：**参数说明参见“源端 IP 地址类型”。

◆**目的端 IP 地址：**如果用户在“目的端 IP 地址类型”中选择“任意 IP 地址”，则页面将不显示本配置参数行。选择其他类型，则会有不同的 IP 地址参数输入要求。具体说明参见“源端 IP 地址”说明。

◆**目的端端口号：**只有用户在“协议”中选择协议类型为 TCP 或 UDP 的情况下，才会显示“目的端端口号”配置参数行。选择 IP 或 ICMP 将不显示本配置行。具体说明参见“源端端口号”参数说明。

◆**时间段：**此防火墙规则适用的时间范围，如不选择时间段范围，默认防火墙规则在所有时间范围内都有效。如要使防火墙规则在指定时间范围内有效，则必须先配置时间段再配置或修改防火墙规则。打开“网络选项”→“时间段配置”菜单即可配置时间段。

◆**插入位置：**配置规则所处的位置，防火墙访问规则是从前往后依次进行匹配检查，所以排在最前面的规则最优先被匹配。即防火墙规则列表是一个有序的语句集，它通过自上而下的顺序来匹配报文中信息与访问表参数，来允许报文通过或拒绝报文通过某个接口。判断规则是如果通过了一个访问列表中的某一项规则，将停止匹配规则，不再试图与它以后的规则比较。所以配置的时候要注意规则的顺序，特殊规则应该插在通用规则之前，否则特殊规则可能不起作用。

◆**保存：**参数输入完成后，单击“保存”按钮，将设置的信息保存到设备上，以使之生效。

保存后如果提示操作成功，则表示输入配置信息已经生效，如果提示操作失败，则用户需要重新输入参数，并检查自己输入的参数是否合法有效。

◆**返回：**单击“返回”按钮返回“防火墙配置”配置和显示页面。

11.1.4 修改防火墙规则

单击打开菜单“网络安全”→“防火墙配置”进入“防火墙配置”接口TAB选项选择页面，单击选择需要配置防火墙的接口，在打开的“防火墙配置”页面的“防火墙规则信息列表”中找到需要修改的防火墙规则所在行，单击其对应行末端的“修改”超链接。如下图。

动作	协议	源地址类型	源地址规则	源端口规则	目的地址类型	目的地址规则	目的端口规则	时间段	操作
允许	ip	任意IP地址	---	---	任意IP地址	---	---		修改
允许	ip	指定IP地址	10.1.1.23	---	指定IP地址	10.1.1.23	---		修改
允许	udp	指定IP地址范围	110.11.1.1~110.11.1.199	端口号等于80	指定IP地址范围	222.23.34.56~222.23.34.234	指定端口号范围50 - 1024		修改
允许	icmp	指定IP子网	102.2.23.5/255.255.255.0	---	指定IP子网	112.2.23.5/255.255.255.0	---		修改
禁止	tcp	任意IP地址	---	任意端口	指定IP子网	123.1.1.1/222.3.23.3	端口号不等于45		修改

用户单击“修改”超链接后，将打开“防火墙规则”配置页面。如下图。

具体参数说明同上一节“添加防火墙规则”。

11.1.5 删除防火墙规则

单击打开菜单“网络安全”→“防火墙配置”进入“防火墙配置”接口TAB选项选择页面，单击选择需要配置防火墙的接口，在打开的“防火墙配置”页面的“防火墙规则信息列表” 用户可以选择删除不需要的防火墙规则。

动作	协议	源地址类型	源地址规则	源端口规则	目的地址类型	目的地址规则	目的端口规则	时间段	操作
允许	ip	任意IP地址	---	---	任意IP地址	---	---		修改
允许	ip	指定IP地址	10.1.1.23	---	指定IP地址	10.1.1.23	---		修改
允许	udp	指定IP地址范围	110.11.1.1~110.11.1.199	端口号等于80	指定IP地址范围	222.23.34.56~222.23.34.234	指定端口号范围50 - 1024		修改
允许	icmp	指定IP子网	102.2.23.5/255.255.255.0	---	指定IP子网	112.2.23.5/255.255.255.0	---		修改
禁止	tcp	任意IP地址	---	任意端口	指定IP子网	123.1.1.1/222.3.23.3	端口号不等于45		修改

具体删除操作如下：

◆**全选/全不选：**全部选中/全部不选中 当前页的信息记录。

◆**删除：**用鼠标选中或全选列表栏中的信息记录（即使显示信息行前面的复选框打勾），单击“删除”按钮删除选中的防火墙规则。

11.2 反病毒配置

许多病毒传播和攻击都是通过特定的网络协议端口进行的，通过反病毒配置规则，对病毒的特征端口进行过滤，以阻止病毒在内网的传播和攻击，是比较有效的办法。对于某些新出现的病毒，根据病毒特征，通过配置反病毒规则，也能快速和有效的阻断其传播和攻击。

反病毒配置支持ICMP、TCP、UDP协议。

单击打开菜单“网络安全”→“反病毒配置”即可进入“反病毒信息”配置和显示页面，在该页面用户可以查看/添加/修改/删除当前设备中已经配置的“反病毒规则信息列表”中具体的反病毒规则。

11.2.1 查看反病毒信息列表

单击打开菜单“网络安全”→“反病毒配置”即可进入“反病毒规则信息列表”显示页面，在该列表中可以查看、修改、删除具体的反病毒规则。如下图。

动作：描述了对符合反病毒规则的病毒报文采取的动作，这里是“禁止”，表示禁止符合反病毒规则的报文转发。

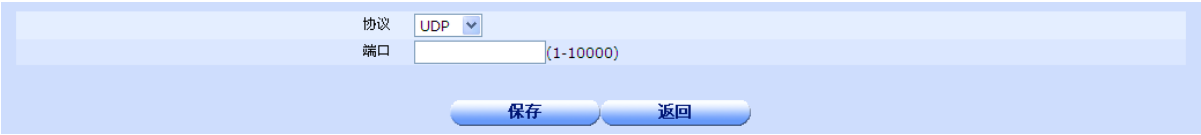
协议：定义的反病毒规则的具体的协议类型即描述了该病毒报文通过什么网络协议进行传播的。一般为 ICMP、UDP、TCP。

端口：定义的反病毒规则的具体的端口号即描述了病毒报文传播的网络端口。如果协议类型是 ICMP，则这一栏为空。

11.2.2 添加反病毒规则

单击打开菜单“网络安全”→“反病毒配置”即可进入“反病毒信息”显示配置页面，如下图在该页面单击“新建”以添加反病毒规则信息。

用户单击“新建”按钮后，打开“反病毒规则”配置页面。如下图。



◆**协议：**反病毒规则应用的协议类型即描述了该病毒报文通过什么网络协议进行传播的。包括 ICMP、UDP、TCP。

◆**端口：**反病毒规则应用的协议端口号即描述了病毒报文传播的网络端口。其中协议类型为 ICMP 的不用配置端口号。

◆**保存：**参数输入完成后，单击“保存”按钮，将设置的信息保存到设备上，以使之生效。

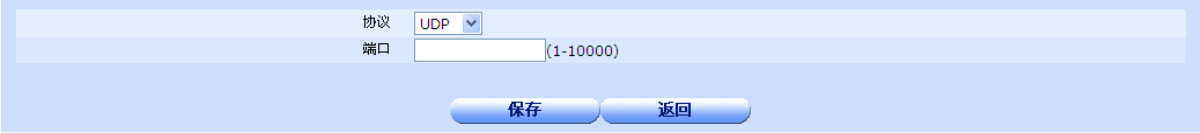
保存后如果提示操作成功，则表示输入配置信息已经生效，如果提示操作失败，则用户需要重新输入参数，并检查自己输入的参数是否合法有效。

◆**返回：**单击“返回”按钮返回“反病毒信息”配置和显示页面。

11.2.3 修改反病毒规则

单击打开菜单“网络安全”→“反病毒配置”即可进入“反病毒信息”显示配置页面，在“反病毒规则信息列表”中找到需要修改的反病毒协议和端口参数所在的行，单击其对应行末端的“修改”超链接。

用户单击“修改”超链接后，将打开“反病毒规则”配置页面。如下图。



◆**协议**：反病毒规则应用的协议类型。包括 ICMP、UDP、TCP。

◆**端口**：反病毒规则应用的协议端口号。其中协议类型为 ICMP 的不用配置端口号。

◆**保存**：参数输入完成后，单击“保存”按钮，将设置的信息保存到设备上，以使之生效。

保存后如果提示操作成功，则表示输入配置信息已经生效，如果提示操作失败，则用户需要重新输入参数，并检查自己输入的参数是否合法有效。

◆**返回**：单击“返回”按钮返回“反病毒信息”配置和显示页面。

11.2.4 删除反病毒规则

单击打开菜单“网络安全”→“反病毒配置”即可进入“反病毒信息”显示页面，如下图。在“反病毒规则信息列表”中，用户可以选择删除不需要的反病毒过滤规则。

具体删除操作如下：

◆**全选/全不选**：全部选中/全部不选中 当前页的信息记录。

◆**删除**：用鼠标选中或全选列表栏中的信息记录（即使显示信息行前面的复选框打勾），单击“删除”按钮删除选中的反病毒过滤规则。

11.3 URL过滤

URL即统一资源定位符（英语Uniform Resource Locator的缩写）也被称为网页地址，是因特网上标准的资源的地址。也就是网页浏览器地址栏内的地址信息。

目前因特网鱼龙混杂，存在着大量不健康或者反动的站点。根据URL地址对数据包进行过滤，是数据过滤的一种常用且实用的方法，可以有效实现对一些黄色、反动站点或信息的过滤。此方法在一定程度上也可以防范一些黑客攻击。

URL过滤是指在网络应用中，根据用户预设的URL规则对请求网站页面的链接URL进行检查，一旦发现URL和预设规则匹配，则对该请求链接进行过滤。过滤规则支持英文（暂时不支持中文），不支持通配符，区分字符大小写。

单击打开菜单“网络安全”→“URL过滤”即可进入“URL过滤”配置和显示页面，在该页面用户可以启用/停止URL过滤服务或者查看/添加/修改/删除当前设备中已经配置的“URL过滤规则列表”中URL过滤规则。

11.3.1 启用/停止URL过滤服务

单击打开菜单“网络安全”→“URL 过滤”即可进入“启用/停止 URL 过滤服务”配置页面，在该页面可以启用/停止 URL 过滤服务。

- **启用 URL 过滤服务：**启用/停止 URL 过滤服务，选中为启用，未选中表示停止，启用/停用 URL 过滤服务均需单击“应用”按钮提交后才能生效。
- **应用：**选择启用/停用服务后，单击“应用”按钮，将设置的信息保存到设备上，以使之生效。

  应用后如果提示操作成功，则表示配置信息已经生效，如果提示操作失败，用户需要修改设置信息重新提交。

11.3.2 查看URL过滤规则列表

单击打开菜单“网络安全”→“URL过滤”即可进入“URL过滤规则列表”显示页面，在该列表中可以查看、修改、删除URL过滤规则。

过滤 URL 特征：列出了设备已经配置的过滤 URL 规则内容。

11.3.3 添加URL过滤规则

单击打开菜单“网络安全”→“URL 过滤”即可进入“URL 过滤”显示配置页面，如下图在该页面单击“新建”以添加 URL 过滤规则。

用户单击“新建”按钮后，打开“URL 过滤规则”配置页面。如下图。

◆**输入需要过滤的 URL：**由用户输入需要过滤的 URL 特征字，URL 特征字支持英文，不支持通配符，区分字符大小写。

◆**保存：**参数输入完成后，单击“保存”按钮，将设置的信息保存到设备上，以使之生效。

保存后如果提示操作成功，则表示输入配置信息已经生效，如果提示操作失败，则用户需要重新输入参数，并检查自己输入的参数是否合法有效。

◆**返回：**单击“返回”按钮返回“URL 过滤”列表显示页面。

11.3.4 修改URL过滤规则

单击打开菜单“网络安全”→“URL 过滤”即可进入“URL 过滤规则列表”显示页面，在“URL 过滤规则列表”中找到需要修改的 URL 特征字所在的行，单击其对应行末端的“修改”超链接。

用户单击“修改”超链接后，将打开“URL 过滤规则”配置页面。如下图。

◆**输入需要过滤的 URL：**由用户输入修改后的新的需要过滤的 URL 特征字，URL 特征字支持英文，不支持通配符，区分字符大小写。

◆**保存：**参数输入完成后，单击“保存”按钮，将设置的信息保存到设备上，以使之生效。

保存后如果提示操作成功，则表示输入配置信息已经生效，如果提示操作失败，则用户需要重新输入参数，并检查自己输入的参数是否合法有效。

◆**返回**：单击“返回”按钮返回“URL 过滤”列表显示页面。

11.3.5 删除URL过滤规则

单击打开菜单“网络安全”→“URL 过滤”即可进入“URL 过滤规则列表”显示页面，如下图。在该列表中用户可以删除不需要的 URL 过滤规则。

具体删除操作如下：

◆**全选/全不选**：全部选中/全部不选中 当前页的信息记录。

◆**删除**：用鼠标选中或全选列表栏中的信息记录（即使显示信息行前面的复选框打勾），单击“删除”按钮删除选中的URL过滤规则。

> **提示：**
>
> **如果暂时不使用 URL 过滤服务的功能的话，不必删除具体的 URL 过滤规则，只要把 URL 过滤服务停止即可！**

> **★注意：**
>
> **由于 URL 过滤是对用户上网的每个网页的地址进行特征值检查和匹配，因此对设备性能会有较大影响即启用 URL 过滤服务后可能会导致上网速度变慢。**

11.4 关键字过滤

关键字（即特征字符串）过滤是指在网络应用中，对传输信息进行预先的程序自动过滤、嗅探指定的关键字词，并进行智能识别，检查网络中是否有违反指定策略的行为。本设备提供的关键字过滤是基于对用户请求网站页面内容进行检测并过滤，对于符合过滤规则的网站页面将被直接过滤。过滤规则支持中文和英文，不支持通配符，区分字符大小写。

单击打开菜单“网络安全”→“关键字过滤”即可进入“关键字过滤”配置和显示页面，在该页面

用户可以启用/停止关键字过滤服务或者查看/添加/修改/删除当前设备中已经配置的“关键字过滤规则列表”中关键字过滤规则。

11.4.1 启用/停止关键字过滤服务

单击打开菜单“网络安全”→“关键字过滤”即可进入“启用/停止关键字过滤服务”配置页面，在该页面可以启用/停止关键字过滤服务。

- **启用关键字过滤服务：**启用/停止关键字过滤服务，选中为启用，未选中表示停止，启用/停用关键字过滤服务均需单击“应用”按钮提交后才能生效。
- **应用：**选择启用/停用服务后，单击“应用”按钮，将设置的信息保存到设备上，以使之生效。

  应用后如果提示操作成功，则表示配置信息已经生效，如果提示操作失败，用户需要修改设置信息重新提交。

11.4.2 查看关键字过滤规则列表

单击打开菜单“网络安全”→“关键字过滤”即可进入“关键字过滤列表”显示页面，在该列表中可以查看、修改、删除关键字过滤规则。

过滤关键字特征：列出了设备已经配置的过滤关键字规则内容。

11.4.3 添加关键字过滤规则

单击打开菜单“网络安全”→“关键字过滤”即可进入“关键字过滤”显示配置页面，如下图在该页面单击“新建”以添加关键字过滤规则。

用户单击“新建”按钮后，打开“关键字过滤规则”配置页面。如下图。

◆**输入需要过滤的关键字：**由用户输入需要过滤的关键字，关键字支持中文和英文，不支持通配符，区分字符大小写。

◆**保存：**参数输入完成后，单击“保存”按钮，将设置的信息保存到设备上，以使之生效。

保存后如果提示操作成功，则表示输入配置信息已经生效，如果提示操作失败，则用户需要重新输入参数，并检查自己输入的参数是否合法有效。

◆**返回：**单击“返回”按钮返回“关键字过滤”列表显示页面。

11.4.4 修改关键字过滤规则

单击打开菜单“网络安全”→“关键字过滤”即可进入“关键字过滤列表”显示页面，在“关键字过滤列表”中找到需要修改的关键字所在的行，单击其对应行末端的“修改”超链接。

用户单击“修改”超链接后，将打开“关键字过滤规则”配置页面。如下图。

◆**输入需要过滤的关键字：**由用户输入修改后的新的需要过滤的关键字，关键字支持中文和英文，不支持通配符，区分字符大小写。

◆**保存：**参数输入完成后，单击“保存”按钮，将设置的信息保存到设备上，以使之生效。

保存后如果提示操作成功，则表示输入配置信息已经生效，如果提示操作失败，则用户需要重新输入参数，并检查自己输入的参数是否合法有效。

◆**返回：**单击“返回”按钮返回“关键字过滤”列表显示页面。

11.4.5 删除关键字过滤规则

单击打开菜单“网络安全”→“关键字过滤”即可进入“关键字过滤列表”显示页面，如下图。在该列表中用户可以删除不需要的关键字过滤规则。

具体删除操作如下：

◆**全选/全不选：**全部选中/全部不选中 当前页的信息记录。

◆**删除：**用鼠标选中或全选列表栏中的信息记录（即使显示信息行前面的复选框打勾），单击“删除”按钮删除选中的关键字过滤规则。

> **提示：**
>
> 如果暂时不使用关键字过滤服务的功能的话，不必删除具体的关键字过滤规则，只要把关键字过滤服务停止即可！

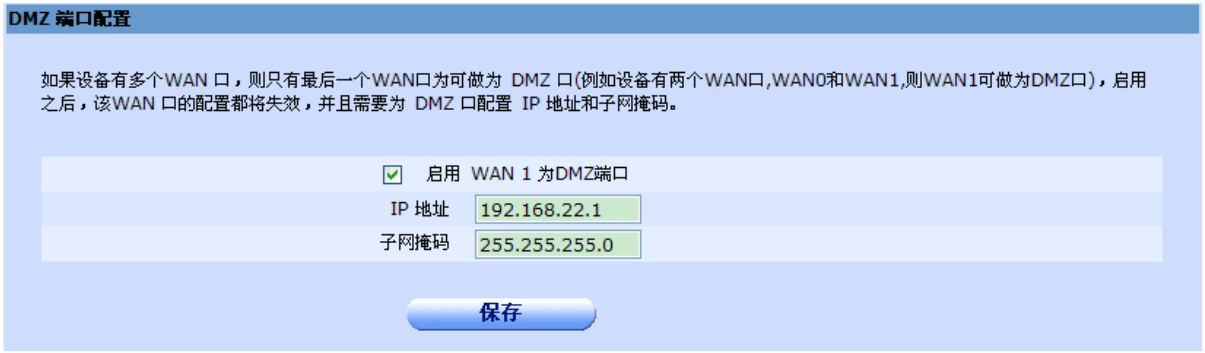
> **★注意：**
>
> 由于关键字过滤是对用户上网的每个网页的内容进行关键字检查和匹配，因此对设备性能会有较大影响即启用关键字过滤服务后可能会导致上网速度变慢。

11.5 DMZ端口配置

启用DMZ端口之后，DMZ区配置的服务才能起作用。

11.5.1 DMZ端口配置

如果设备有多个 WAN 口，则只有最后一个 WAN 口为可做为 DMZ 口(例如设备有两个 WAN 口,WAN0 和 WAN1,则 WAN1 可做为 DMZ 口)，启用之后，该 WAN 口的配置都将失效，并且需要为 DMZ 口配置 IP 地址和子网掩码。



11.5.2 DMZ区服务配置

可以添加一个服务器，并开放其特定服务端口。

点击“新建”可以添加一个服务器。点击“修改”可以修改一个服务器配置。添加和修改页面如下：

- **服务器ＩＰ地址**：服务器 IP 地址与 DMZ 端口必须在一个网段内。
- **协议**：可以选择此服务器要开放的服务属于那种协议。
- **服务器开放的服务端口**：可以在下拉菜单中选择，也可以选择“自定义”，自己输入端口号。

注意：两个服务器不能开放相同的服务。

常见 TCP 服务对应端口如下：

FTPDATA 20, FTP 21, HTTP 80
POP3 110, SMTP 25, TELNET 23

常用 UDP 服务对应端口如下：
DNS 53, TFTP 69, DHCP 67

第12章　上网行为管理

上网行为管理是一套基于组的限速机制。上网行为管理可以分为以下 4 个大的功能：全局配置、群组配置、优先服务管理和黑白名单，我们可以通过状态查询来查看具体的信息。

首先看一下全局配置和群组配置的关系：全局配置可以配置全局参数和默认组配置，默认组的地址范围是 0.0.0.0 到 255.255.255.255，群组管理中可以添加个性组，每个个性组都需要设定一个地址范围，如果一台主机的 IP 地址在个性组的地址范围内，则按照个性组中的设定进行带宽分配和封堵应用，如果不属于任何个性组，则遵循全局配置，即默认组的配置。

全局配置中用户需要设置上传和下载总带宽以及一些全局参数和全局功能，例如启动优先服务管理和大流量主机抑制机制，在高级配置中可以设置功能配置中的一些参数。

在群组配置中，用户可以自己添加个性组，并设定每个组的上下行最大允许带宽和最小保证带宽，以及封 BT、MSN、QQ 等特殊应用。

优先服务管理中可以对游戏、邮件进行加速，也可以自定义添加要优先服务的业务。优先服务管理中的配置要生效，必须首先在全局配置中启动优先服务策略。

黑白名单中，用户可以添加 IP 地址到黑名单或者白名单中，黑名单中的主机禁止上网，白名单中的主机不受上网行为管理的任何限制。

12.1　全局配置

单击打开菜单“上网行为管理”→“全局配置”即可进入“全局配置”设置页面，本页面可以进行全局参数配置，以及默认组的带宽分配配置和功能配置。

12.1.1 全局功能配置

- **上传和下载总带宽**：设置上传和下载总带宽，如果有多条线路，则将多条线路的总带宽叠加。如果您的 ISP 在不通时段提供不通的带宽比如白天 10M，晚上 20M，那么可以点击“设置 ISP 带宽时段”进行设置。
- **功能配置**：封 P2P， QQ， MSN，内网 DOS 攻击，特定的股票网站和娱乐购物网站以及启动优先服务策略。你可以点击更新策略更新可以封的股票网站和娱乐购物网站，具体的网址可以点击“股票网站”和“娱乐购物网站”查看。注意：一键封股票网站和一键封娱乐购物网站是通过封这些网站对应的 IP 地址来实现的，路由器每隔一小时会查询一次 DNS 获取网站的 IP 地址，如果一个网站对应多个 IP 地址（例如淘宝网），则需要多查询几次才能真正封堵。
- **大流量主机抑制配置**：如果上传和下载带宽比较紧张，则可以启动大流量抑制，此时，如果一台主机持续一段时间内流量比较大，则对其带宽抑制一段时间。持续时间和抑制时间都可以在“高级配置”设置。设主机的最小保证带宽为 A，主机大流量的持续时间为 B，主机在 B 秒内实际使用的总带宽为 C，则如果一个主机的流量满足公式 C － A ＊ B ＞ A ＊B＊ 20% （即主机在 B 秒内借用的带宽大于保证带宽的 20%）时，对该主机进行抑制。注意，只有在总带宽占用大于 60% 时，才进行抑制。
- **内网主机带宽分配配置**：不启动动态带宽分配时，需要手动输入保证最小上下行带宽和允许最大上下行带宽，零表示不限制；如果启动动态带宽，则不需要设置上下行带宽。允许的最大带宽减去保证的最小带宽即为每台主机的可借用带宽，总带宽占用越高可借用带宽越小，反之则越高，当带宽占用达到 95% 时，可借用带宽为零。

  启动动态带宽分配时，不需要手工输入保证的最小上下行带宽和允许的最大上下行带宽，其值按照下面的公式计算：

上行最小保证带宽=上行总带宽×最小保证带宽倍数/主机数;
上行最大允许带宽=上行总带宽×最大带宽倍数/主机数;
下行最小保证带宽=下行总带宽×最小保证带宽倍数/主机数;
下行最大允许带宽=下行总带宽×最大带宽倍数/主机数。

最小保证带宽倍数和最大带宽倍数可以在“全局配置”的“高级配置”中设定。

注意:当开启反 P2P 功能，若内网有主机使用 P2P 下载时则会将该主机断网 5 分钟。当开启反 DOS 攻击功能后，若内网有主机发动 DOS 攻击，则会将该主机断网 5 分钟。

12.1.2 带宽时段控制

单击打开菜单“上网行为管理”→“全局配置”即可进入“全局配置”设置页面，在全局配置的超链接“>>设置 ISP 带宽时段”可进入“带宽时段控制”设置页面。

首先需要选择一个时间段名称，如果没有配置，则可以在“网络选项”→“时间段配置”→“循环时间段配置”中设置。上传和下载总带宽可以从下拉菜单中选择也可以手动输入。

下面给一个典型的配置：工作日，即周一到周五早上 9 点到晚上 6 点上传和下载带宽 10M，周一到周五晚上 6 点到早上 9 点上传和下载带宽为 20M，周六周日全天 20M，则可以如下配置：

首先要配置两个时间段，循环时间段 1 配置如下：

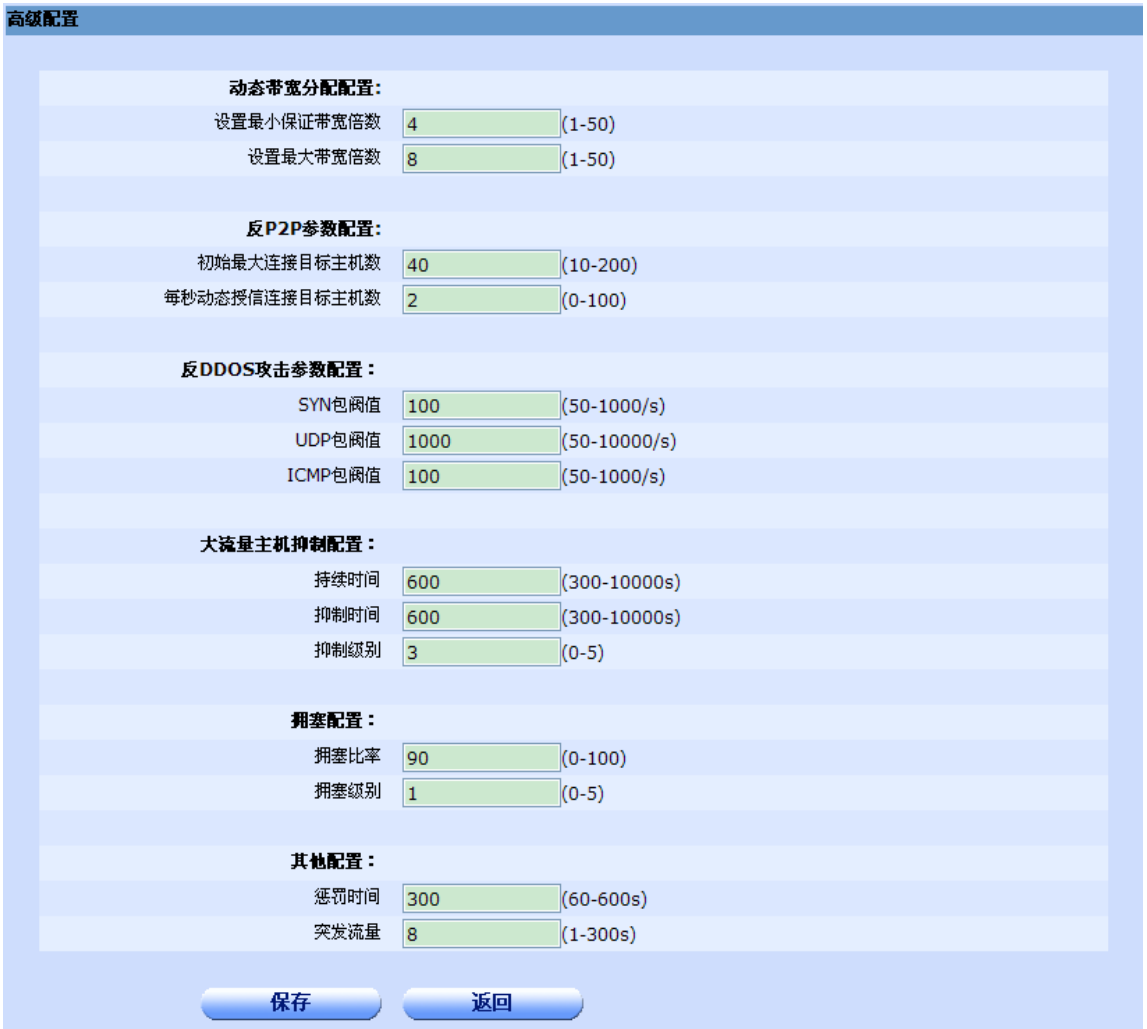
循环时间段 2 配置如下：

带宽时间段配置如下：

12.1.3 高级配置

单击打开菜单“上网行为管理”→“全局配置”即可进入“全局配置”设置页面，在全局配置里点击“高级配置”按钮可进入“高级配置”设置页面。

本页面是对全局参数进行配置。



- **动态带宽分配配置**：关于动态带宽计算方式，以及最大最小保证带宽倍数的使用可以参照以下公式来计算:
  上行最小保证带宽=上行总带宽×最小保证带宽倍数/主机数;
  上行最大允许带宽=上行总带宽×最大带宽倍数/主机数;
  下行最小保证带宽=下行总带宽×最小保证带宽倍数/主机数;
  下行最大允许带宽=下行总带宽×最大带宽倍数/主机数。
- **反 P2P 参数配置**：初始最大连接目标主机数和每秒动态授信连接目标主机数的值越大对 p2p 的限制越小。每个内网主机都保存一个剩余可连接目标主机数，即“初始最大连接主机数”，当与一台外网主机建立一个连接后，剩余可连接目标主机数减一；每秒会重新增加每台内网主机的剩余可连接目标主机数，增加的值即为“每秒动态授信连接目标主机数”，当剩余可连接目标主机数减为零时，对认为该主机进行 P2P 下载，对其进行惩罚。
- **反 DOS 攻击参数配置**：可以设置 SYN 包阈值，UDP 包阈值，ICMP 包阈值。阀值越大对 DOS 攻击的限制越小。这些阀值表示每秒钟允许内网主机发送的 SYN 包、UDP 包、ICMP 包的数量，如果超过这些值则怀疑该内网主机发动 DOS 攻击，对其进行惩罚。
- **大流量主机抑制配置**：可以设置持续时间和抑制时间。设置持续时间是为了防止突发流量，如果一台主机长时间流量比较大，才对其保证带宽进行抑制，超过抑制时间后，恢复其原有分配带宽。抑制级别含义如下：分 6 个级别

  0 ：借用带宽为 0， 保证带宽不变。

  1 ：借用带宽为 0， 保证带宽降低 10%。

2 ：借用带宽为 0， 保证带宽降低 20%。

3 ：借用带宽为 0， 保证带宽降低 30%。

4 ：借用带宽为 0， 保证带宽降低 40%。

5 ：借用带宽为 0， 保证带宽降低 50%。

- **拥塞配置**：如果没有开启大流量抑制，则判断网络是否拥塞，如果拥塞，则根据拥塞级别控制每个主机的带宽(目前只有在下载拥塞时才对带宽进行控制，控制时间为 10 分钟，10 分钟以后恢复到正常带宽控制)。拥塞比率表示带宽占用超过多少时表示拥塞，默认是 95%，拥塞级别用来控制拥塞时的带宽控制，分 6 个级别：

  0 ：借用带宽为 0， 保证带宽不变。

  1 ：借用带宽为 0， 保证带宽降低 10%。

  2 ：借用带宽为 0， 保证带宽降低 20%。

  3 ：借用带宽为 0， 保证带宽降低 30%。

  4 ：借用带宽为 0， 保证带宽降低 40%。

  5 ：借用带宽为 0， 保证带宽降低 50%。

- **突发流量**：每个主机都允许累计一定时间的突发流量，例如，设突发流量参数为 12s，保证带宽为 500K， 如果主机一段时间没有上网（即没有流量），那么他的突发流量最大可以累计到 12 x 500K，故此参数越小，允许的突发流量越小。
- **惩罚时间**：当内网主机发动 DOS 攻击或者使用 p2p 下载时，对该主机断网的时间。

12.2 群组管理

单击打开菜单“上网行为管理”→“群组管理”即可进入“群组管理”设置页面，本页面用于配置群组的各项个性设置。如果一台或多台主机不想按照默认的全局配置生效，则可以建立一个个性组，进行特殊的配置。如果个性组很多，则可以在搜索框中输入组名进行搜索。

单击“新建”可以新建群组用户，单击“修改”可以修改群组配置。配置页面如下：

起始、结束 IP 地址：设定个性组的起始和结束 IP 地址。如果一个主机的 I P地址在此范围内，在按照此个性组的配置生效。其他配置与全局配置中的含义相同。

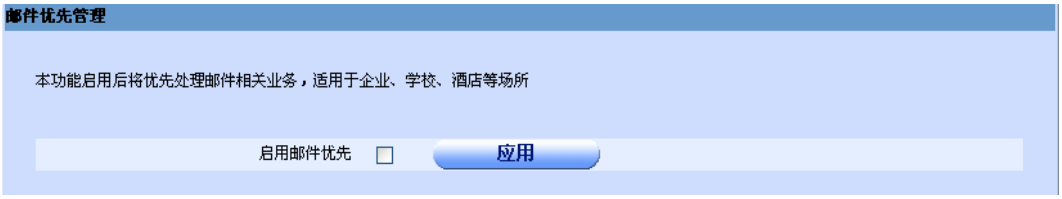
12.3 优先服务管理

单击打开菜单“上网行为管理”→“游戏服务管理”即可进入“游戏服务管理”设置页面，本页面可以配置优先服务的应用。分为三个基本功能：游戏优先管理，邮件优先管理和其他业务优先管理。此三项功能必须在“全局配置”下启动优先服务策略的情况下才会起作用。

12.3.1 游戏优先管理

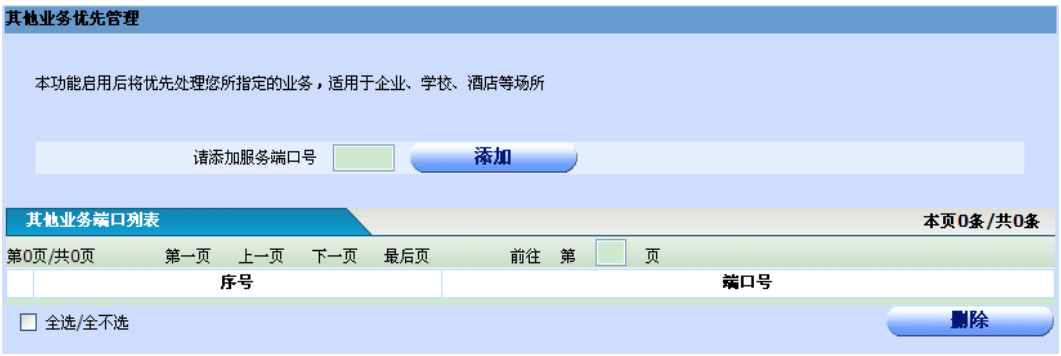
如果要对特定游戏进行加速，只需勾选此游戏后面的复选框然后点击“保存”即可，如果要对其他游戏进行加速，可以在“其他业务优先管理”中添加此游戏对应的端口，或者升级安全策略文件。

12.3.2 邮件优先管理



如果要对邮件进行有限处理，则勾选启动邮件优先并点击“应用”

12.3.3 其它业务优先管理



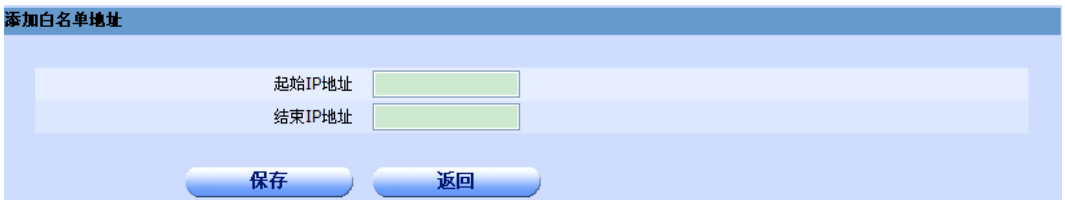
如果要对特定的应用进行优先处理，可以在此页面添加服务对应的端口。

12.4 黑白名单

单击打开菜单“上网行为管理”→“黑白名单”即可进入“黑白名单”设置页面，本页面可以将内网主机加入到黑名单和白名单中，黑名单中的主机禁止上网，白名单中的主机不受“上网行为管理”的限制。

白名单配置：

点击“新建”可以添加一个地址或一个地址范围到白名单中。点击“删除”可以从白名单中删除一个 IP 地址。添加页面如下：



如果想要添加单个地址，则结束 IP 地址可以不填，黑名单的配置与白名单类似。

12.5 状态查询

单击打开菜单“上网行为管理”→“状态查询”即可进入“状态查询”设置页面，可以按照“群组”，“主机”，“受抑制主机”，“受惩罚主机”等条件进行查询。你也可以在搜索框中输入要查询的字段进行查询。

查询页面如下：

如果一台主机被惩罚或者被抑制可以点击“解除惩罚”解除。

点击“内网地址”可以查看此主机的详细信息，页面如下：

第13章　虚拟专网

13.1　IPSEC配置

IPSEC 的安全特性主要有：

不可否认性：“不可否认性”可以证实消息发送方是唯一可能的发送者，发送者不能否认发送过消息。“不可否认性”是采用公钥技术的一个特征，当使用公钥技术时，发送方用私钥产生一个数字签名随消息一起发送，接收方用发送者的公钥来验证数字签名。由于在理论上只有发送者才唯一拥有私钥，也只有发送者才可能产生该数字签名，所以只要数字签名通过验证，发送者就不能否认曾发送过该消息。但“不可否认性”不是基于认证的共享密钥技术的特征，因为在基于认证的共享密钥技术中，发送方和接收方掌握相同的密钥。

反重播性：“反重播”确保每个 IP 包的唯一性，保证信息万一被截取复制后，不能再被重新利用、重新传输回目的地址。该特性可以防止攻击者截取破译信息后，再用相同的信息包冒取非法访问权（即使这种冒取行为发生在数月之后）。

数据完整性：防止传输过程中数据被篡改，确保发出数据和接收数据的一致性。IPSEC 利用 Hash 函数为每个数据包产生一个加密检查和，接收方在打开包前先计算检查和，若包遭篡改导致检查和不相符，数据包即被丢弃。

数据可靠性（加密）：在传输前，对数据进行加密，可以保证在传输过程中，即使数据包遭截取，信息也无法被读。该特性在 IPSEC 中为可选项，与 IPSEC 策略的具体设置相关。

认证：数据源发送信任状，由接收方验证信任状的合法性，只有通过认证的系统才可以建立通信连接。

IPSEC 也可以使用预置共享密钥进行认证。预共享意味着通信双方必须在 IPSEC 策略设置中就共享的密钥达成一致。之后在安全协商过程中，信息在传输前使用共享密钥加密，接收端使用同样的密钥解密，如果接收方能够解密，即被认为可以通过认证。

单击打开菜单“虚拟专网”→“IPSEC配置”即可进入IPSEC监控管理页面，可以单击相关WAN口的IPSEC Tab来配置相应的IPSEC，或者单击“IPSEC会话信息”Tab来显示已经启用的IPSEC相关信息。

13.1.1　WAN口的IPSEC列表信息

在 Tab 标签上单击相应 WAN 口的 IPSEC 标签，进入相应 WAN 口的配置好的 IPSEC 列表信息显示页面。

◆**序号**：为表内容的序号。

◆**隧道 ID**：显示此 IPSEC 隧道对应的隧道 ID。

◆**本地安全组**：显示此 IPSEC 隧道配置的本地安全组信息，包括“IP 地址”，“IP 地址范围”或者“子网”，IP 地址为一个私网地址。

◆**远端安全组**：显示此 IPSEC 隧道配置的远端安全组信息，包括“任意”，“IP 地址”，“IP 地址范围”或者“子网”，IP 地址为一个私网地址。

◆**远端地址/域名**：显示此 IPSEC 隧道配置的远端 IP 地址或域名，IP 地址为一个公网地址。

◆**操作**：单击“修改”超链接，进入 IPSEC 配置页面，可以修改 IPSEC 的配置参数。单击“新建”按钮，可以添加一条 IPSEC 隧道。单击“删除”按钮，删除已选中的 IPSEC 隧道。

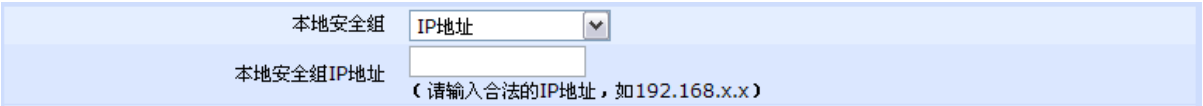
★注意：

1. **配置完成后要勾选上方的启用 IPSEC，然后单击“应用”之后才能生效！**
2. **配置的 IPSEC 的本地安全组和远端安全组地址不能通过 NAT 访问控制列表翻译，否则 IPSEC 将不能建立成功。**

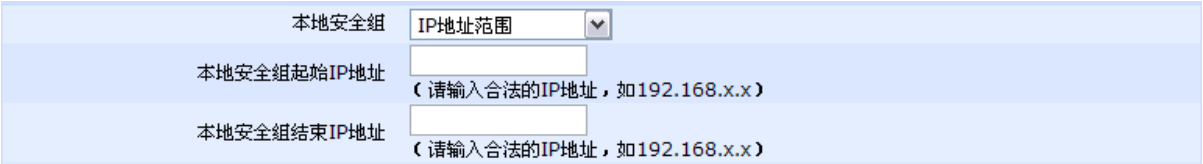
13.1.2 添加或修改WAN口的IPSEC配置

单击打开菜单“虚拟专网”→“IPSEC配置”，进入相应WAN口的配置好的IPSEC列表信息显示页面，再单击“新建”按钮，或者在IPSEC列表信息中找到需要配置的IPSEC隧道，点击其对应的“操作”一栏的“修改”超链接，即可进入“IPSEC隧道配置页面”。

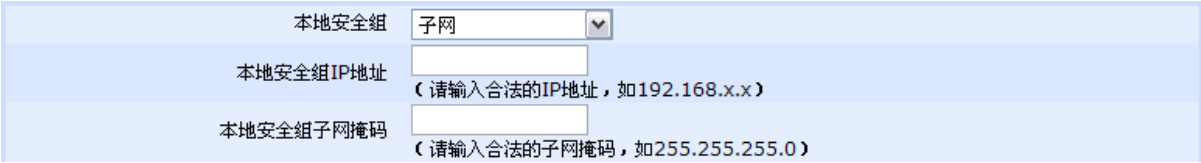
◆**本地安全组**：可以在“IP 地址”、“IP 地址范围”和“子网”之间选择。



➢ **本地安全组**：选择“IP 地址”后下方会出现一个地址输入框用来输入 IP 地址。

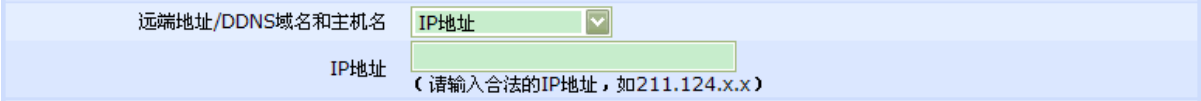


➢ **本地安全组**：选择“IP 地址范围”后下方会出现两个 IP 地址输入框用来输入 IP 地址范围。



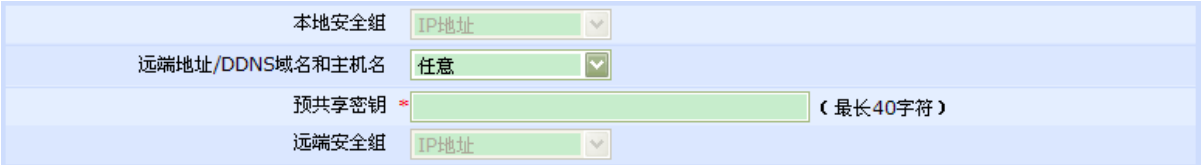
➢ **本地安全组**：选择“子网”后下方出现两个输入框，一个用来输入 IP 地址，一个用来输入子网掩码。

◆**远端地址/**DDNS 域名和主机名：可以在“IP 地址”、“ DDNS 域名和主机名”和“任意”之间选择。



➢ **远端地址/ DDNS 域名和主机名**：选择 IP 地址，在 IP 地址输入框中输入一个合法的 IP 地址，一般为一个公网地址。

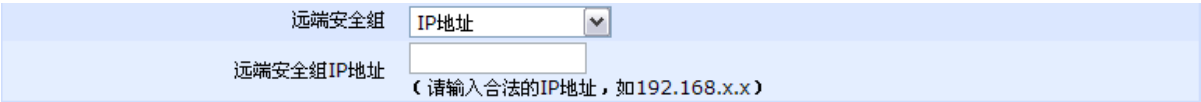
➢ **远端地址/ DDNS 域名和主机名**：选择 DDNS 域名和主机名，在输入框中输入 DDNS 域名和主机名。



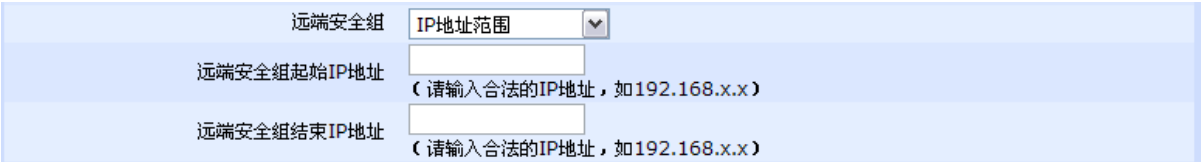
➢ **远端地址/ DDNS 域名和主机名**：选择“任意”的时候会禁用本地安全组和远端安全组的选择。

◆**预共享密钥**：输入最长 40 字符的密钥，建议使用字母数字组合。

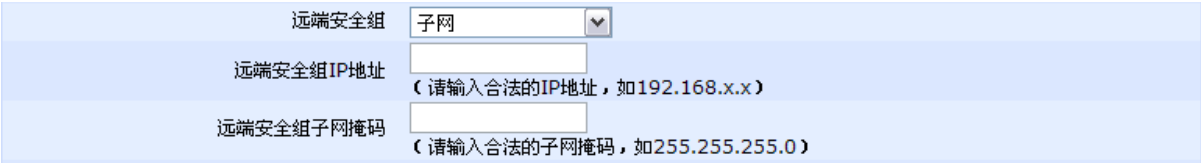
◆**远端安全组**：可以在“任意”，“IP 地址”，“IP 地址范围”和“子网”之间选择。



➢ **远端安全组**：选择“IP 地址”后下方会出现一个地址输入框用来输入 IP 地址。



➢ **远端安全组**：选择“IP 地址范围”后下方会出现两个 IP 地址输入框用来输入 IP 地址范围。



➢ **远端安全组**：选择“子网”后下方出现两个输入框，一个用来输入 IP 地址，一个用来输入子网掩码。

- **远端安全组**：选择“任意”的时候会隐藏下面的输入框。

◆**显示高级配置选项**：勾选，则显示如下：

- **IKE 协商模式**：可以选择“MD5”或者“SHA”，默认值是“MD5”。
- **IKE 加密方式**：可以选择“DES”或者“3DES”，默认值是“DES”。
- **工作模式**：可以选择“主模式”或者“野蛮模式”，默认值是“主模式”。
- **IKE 组**：可以选择“组 1”或者“组 2”，默认值是“组 1”。
- **ESP 加密方式**：可以选择“ESP-DES”，“ESP-3DES”，“禁用”，默认值是“ESP-3DES”。
- **ESP 验证方式**：可以选择“ESP-MD5-HAMC”，“ESP-SHA-HAMC”，“禁用”，默认值是“ESP-MD5-HAMC”。
- **AH 认证方式**：可以选择“AH-MD5-HAMC”，“AH-SHA-HAMC”，“禁用”，默认值是“AH-MD5-HAMC”。
- **指定 PFS 位置**：可以选择“组 1”，“组 2”或者“不指定”，默认值是“不指定”。
- **密钥生命周期**：默认值 28800 秒，一般不需修改。

◆**保存**：参数输入完成后，单击“保存”按钮，将设置的信息保存到设备上，即依照给定的参数进行相应 WAN 口的 IPSEC 隧道配置。保存后如果提示操作成功，则表示输入配置信息已经生效，如果提示操作失败，则用户需要重新输入参数，并检查自己输入的参数是否合法有效。

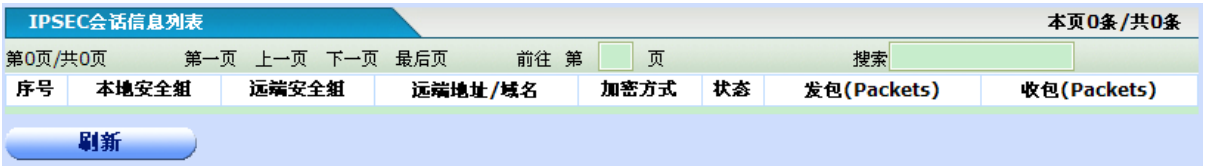
◆**返回**：单击该按钮返回 IPSEC 列表信息显示页面。

> **提示：**
>
> **ESP 加密方式和 AH 认证方式不能同时设置为禁用。**

> **★注意：**
>
> **配置完成单击保存后会在网络选项的 NAT 访问控制中加入一条状态为“禁止”的记录，若将此记录修改或删除的话会使 IPSEC 在打开 NAT 地址转换的时候不能连通。**

13.1.3 查看IPSEC会话信息

在 Tab 标签上单击 IPSEC 会话信息标签，进入 IPSEC 会话信息列表页面，如下图：



◆**序号**：为表内容的序号。

◆**本地安全组**：显示此 IPSEC 隧道对应的本地安全组信息，包括“IP 地址”，“IP 地址范围”或者“子网”，IP 地址为一个私网地址。

◆**远端安全组**：显示此 IPSEC 隧道对应的远端安全组信息，包括“任意”，“IP 地址”，“IP 地址范围”或者“子网”，IP 地址为一个私网地址。

◆**远端地址/域名**：显示此 IPSEC 隧道对应的远端 IP 地址或域名，IP 地址为一个公网地址。

◆**加密方式**：显示此 IPSEC 隧道使用的加密方式。

◆**状态**：显示此 IPSEC 隧道的状态。

◆**发包**：显示此 IPSEC 隧道的发包数量。

◆**收包**：显示此 IPSEC 隧道的收包数量。

◆**刷新按钮**：单击此按钮可以获得即时会话信息。

13.2 PPTP配置

点对点隧道协议（PPTP）是一种支持多协议虚拟专用网络的网络技术，它工作在第二层。通过该协议，远程用户能够通过Windows操作系统以及其它装有点对点协议的系统安全访问公司网络，并能拨号连入本地ISP，通过Internet安全链接到公司网络。

单击打开菜单“虚拟专网”→“PPTP配置”即可进入PPTP监控管理页面，可以单击“PPTP客户端”Tab配置PPTP客户端，也可以单击“PPTP服务器”配置PPTP服务器，或者单击“PPTP会话信息”Tab来显示已经启用的PPTP相关信息。

13.2.1 PPTP客户端配置信息列表

在 Tab 标签上单击 PPTP 客户端，进入 PPTP 客户端配置信息列表页面，如下图：

◆**PPTP 拨号连接名**：显示 PPTP 客户端拨号使用的连接名，用来区分不同的拨号连接。

◆**服务器的 IP 或域名**：显示此拨号连接对应的服务器的 IP 或者域名。

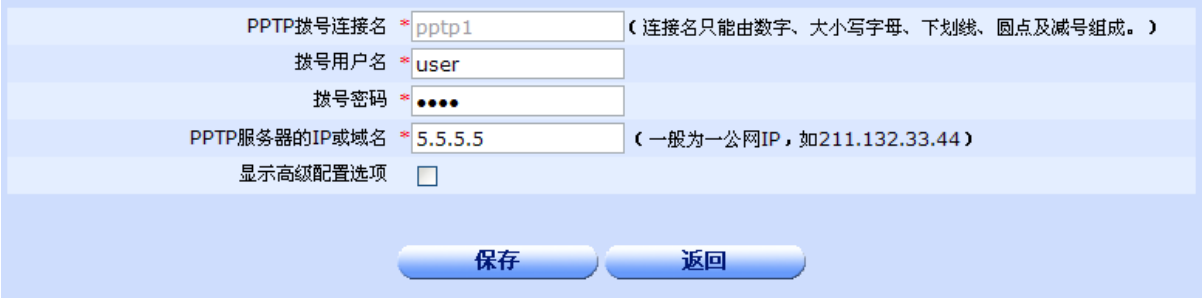
◆**拨号用户名**：显示此 PPTP 拨号连接使用的用户名。

◆**操作**：单击“修改”超链接，进入 PPTP 客户端配置页面，可以修改 PPTP 客户端的配置参数。单击“新建”按钮，可以添加一条 PPTP 客户端拨号连接。单击“删除”按钮，删除已选中的 PPTP 客户端拨号连接。

> ♂提示：
>
> 删除客户端配置的同时会自动删除与其相关的默认路由和静态路由。

13.2.2 添加或修改PPTP客户端配置

单击打开菜单“虚拟专网”→“PPTP 配置”，进入 PPTP 客户端配置信息列表页面，再单击“新建”按钮，或者在 PPTP 客户端配置信息列表页面中找到需要配置的 PPTP 拨号连接，点击其对应的“操作”一栏的“修改”超链接，即可进入“PPTP 客户端配置页面”。



◆**PPTP 拨号连接名**：设置本条拨号连接的连接名，如果为单击“修改”超链接进入的本页面，此字段不可操作。

◆**拨号用户名**：设置拨号连接使用的拨号用户名。

◆**拨号密码**：设置拨号连接使用的拨号密码。

◆**PPTP 服务器的 IP 或域名**：IP 地址一般为一个公网 IP，也可以输入服务器的域名，通过 DNS 解析出服务器 IP。

◆**显示高级选项**：显示 PPTP 客户端拨号配置的高级选项。

- **本地隧道名**：设置此 PPTP 拨号连接使用的隧道名，可以留空不填。
- **客户端超时**：设置此 PPTP 拨号连接客户端的超时时间，取值范围为 0-65535 秒，默认值是 10 秒，一般不需要修改。
- **ECHO 报文间隔**：设置此 PPTP 拨号连接的 ECHO 报文间隔，取值范围为 5-1000 秒，默认值是 60 秒，一般不需要修改。
- **备用服务端的 IP 或域名**：如果服务器不能连通，可以拨号到备用服务端，可以设置 4 个备用服务器，一般不需要设置。

◆**保存**：参数输入完成后，单击“保存”按钮，将设置的信息保存到设备上，即依照给定的参数进行 PPTP 客户端拨号连接设定。保存后如果提示操作成功，则表示输入配置信息已经生效，如果提示操作失败，则用户需要重新输入参数，并检查自己输入的参数是否合法有效。

◆**返回**：单击该按钮返回 PPTP 客户端配置信息列表页面。

13.2.3 PPTP服务器配置信息列表

在 Tab 标签上单击 PPTP 服务器，进入 PPTP 服务器配置信息列表页面，如下图：

◆**PPTP 服务名**：显示 PPTP 的服务名，用来区分不同的 PPTP 服务。

◆**VPN 服务端 IP**：显示此服务使用的 IP。

◆**VPN 客户端获取地址的方式**：显示给 PPTP 客户端分配地址的方式，有“不指定”，“IP”和“地址池”三种。

◆**操作**：单击“修改”超链接，进入 PPTP 服务器配置页面，可以修改 PPTP 服务器配置参数。单击“新建”按钮，可以添加一条 PPTP 服务。单击“删除”按钮，删除已选中的 PPTP 服务。

13.2.4 添加或修改PPTP服务器配置

单击打开菜单“虚拟专网”→“PPTP 配置”，进入 PPTP 服务器配置信息列表页面，再单击“新建”按钮，或者在 PPTP 服务器配置信息列表页面中找到需要配置的 PPTP 服务，点击其对应的“操作”一栏的“修改”超链接，即可进入“PPTP 服务器配置页面”。

◆**PPTP 服务名**：设置 PPTP 的服务名，此字段为系统自动生成，用户不可修改。

◆**VPN 服务端 IP**：设置服务端使用的 IP 地址，为一私网 IP。

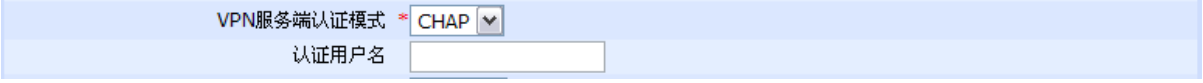
◆**VPN 服务端子网掩码**：设置 VPN 服务端使用的子网掩码。

★注意：

此 IP 不能与本地内网 IP 同一网段，否则会设置失败。

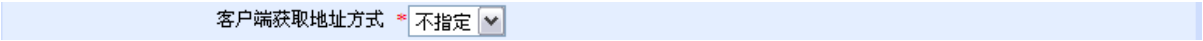
◆ **VPN 服务端认证模式**：可以选择“PAP”认证或者“CHAP”认证。

➢ **VPN 服务端认证模式**：“PAP”。选择此项的话下方不会有任何提示。



➢ **VPN 服务端认证模式**：选择“CHAP”后下方会有一个认证用户名输入框用来输入认证用户名。

◆**客户端获取地址方式**：可以选择“不指定”，“IP”或者“地址池”。



➢ **客户端获取地址方式**：“不指定”。选择此项的话下方不会有任何提示。

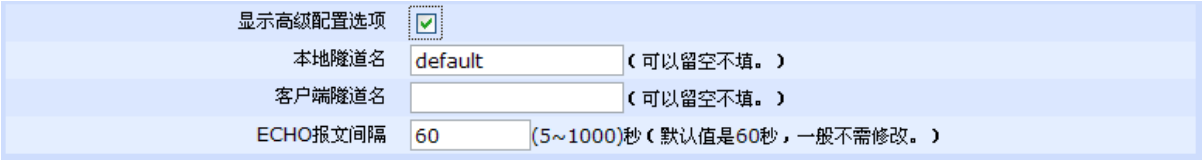
➢ **客户端获取地址方式**：选择“IP”后下方会出现一个 IP 地址输入框来输入 IP 地址。

➢ **客户端获取地址方式**：选择“地址池”后会出现两个 IP 地址输入框来确定地址池包含的地址范围。

★**注意：**

地址池中的地址数量不能超过 1024 个，否则会设置失败。

◆**显示高级选项**：显示 PPTP 服务器配置的高级选项。



➢ **本地隧道名**：设置此 PPTP 服务端使用的隧道名，可以留空不填。

➢ **客户端隧道名**：设置拨号到此 PPTP 服务端的客户端隧道名，可以留空不填。

➢ **ECHO 报文间隔**：设置此 PPTP 服务端的 ECHO 报文间隔，取值范围为 5-1000 秒，默认值是 60 秒，一般不需要修改。

◆**保存**：参数输入完成后，单击“保存”按钮，将设置的信息保存到设备上，即依照给定的参数进行 PPTP 服务器设定。保存后如果提示操作成功，则表示输入配置信息已经生效，如果提示操作失败，则用户需要重新输入参数，并检查自己输入的参数是否合法有效。

◆**返回**：单击该按钮返回 PPTP 服务器配置信息列表页面。

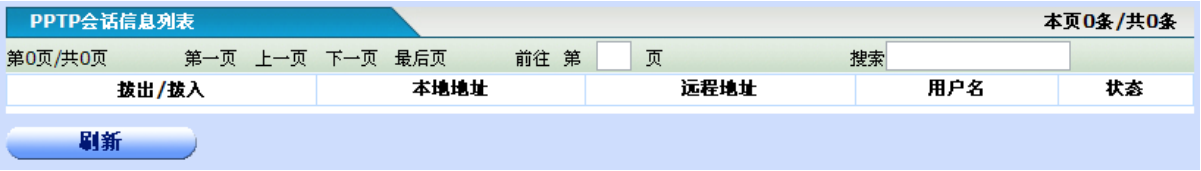
◆**配置拨号用户**：如果想要添加或者修改拨号用户，请单击此按钮进入拨号用户管理相关页面。

★注意：

如果由服务端给客户端分配 IP 或者地址池，设备会自动将单一 IP 或者地址池中的所有 IP 添加到 NAT 访问列表中并设为允许，如果不小心删除，可能客户端会无法上网。

13.2.5 PPTP会话信息

在 Tab 标签上单击 PPTP 会话信息标签，进入 PPTP 会话信息列表页面，如下图：



◆**拨出/拨入**：用“拨出”表示设备以客户端的身份向服务端拨号，用“拨入”来表示设备配置的是服务端。

◆**本地地址**：显示本条会话的本地隧道地址。

◆**远程地址**：显示与本地地址连接的远程隧道地址。

◆**用户名**：显示本条会话使用的用户名。

◆**状态**：显示本条会话的状态。

◆**刷新按钮**：单击此按钮获得即时 PPTP 会话信息。

13.3 L2TP配置

该协议是一种工业标准的Internet隧道协议，功能大致和PPTP协议类似，比如同样可以对网络数据流进行加密。不过也有不同之处，比如PPTP要求网络为IP网络，L2TP要求面向数据包的点对点连接；PPTP使用单一隧道，L2TP使用多隧道；L2TP提供包头压缩、隧道验证，而PPTP不支持。

单击打开菜单“虚拟专网”→“L2TP配置”即可进入L2TP监控管理页面，可以单击“L2TP客户端”Tab配置L2TP客户端，也可以单击“L2TP服务器”配置L2TP服务器，或者单击“L2TP会话信息”Tab来显示已经启用的L2TP相关信息。

13.3.1 L2TP客户端配置信息列表

在 Tab 标签上单击 L2TP 客户端，进入 L2TP 客户端配置信息列表页面，如下图：

◆**L2TP 拨号连接名**：显示 L2TP 客户端拨号使用的连接名，用来区分不同的拨号连接。

◆**服务器的 IP 或域名**：显示此拨号连接对应的服务器的 IP 或者域名。

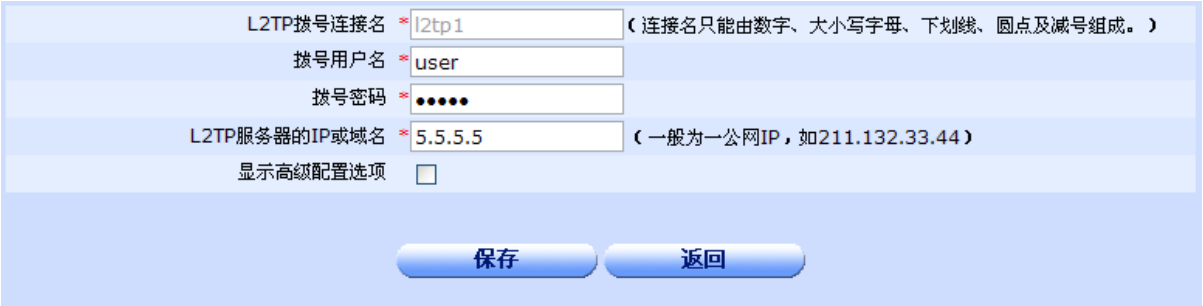
◆**拨号用户名**：显示此 L2TP 拨号连接使用的用户名。

◆**操作**：单击“修改”超链接，进入 L2TP 客户端配置页面，可以修改 L2TP 客户端的配置参数。单击“新建”按钮，可以添加一条 L2TP 客户端拨号连接。单击“删除”按钮，删除已选中的 L2TP 客户端拨号连接。

> **提示：**
>
> 删除客户端配置的同时会自动删除与其相关的默认路由和静态路由。

13.3.2 添加或修改L2TP客户端配置

单击打开菜单“虚拟专网”→“L2TP 配置”，进入 L2TP 客户端配置信息列表页面，再单击“新建”按钮，或者在 L2TP 客户端配置信息列表页面中找到需要配置的 L2TP 拨号连接，点击其对应的“操作”一栏的“修改”超链接，即可进入“L2TP 客户端配置页面”。



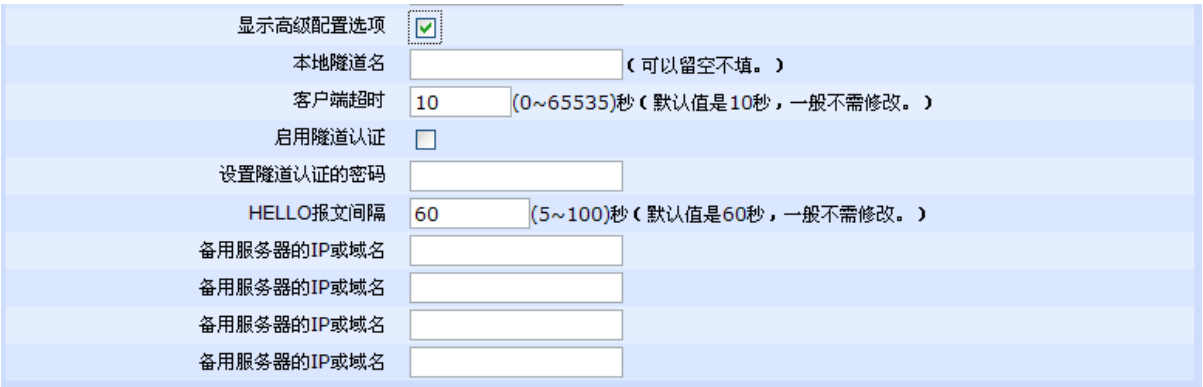
◆**L2TP 拨号连接名**：设置本条拨号连接的连接名，如果为单击“修改”超链接进入的本页面，此字段不可操作。

◆**拨号用户名**：设置拨号连接使用的拨号用户名。

◆**拨号密码**：设置拨号连接使用的拨号密码。

◆**L2TP 服务器的 IP 或域名**：IP 地址一般为一个公网 IP，也可以输入服务器的域名，通过 DNS 解析出服务器 IP。

◆**显示高级选项**：显示 L2TP 客户端拨号配置的高级选项。



- **本地隧道名**：设置此 L2TP 拨号连接使用的隧道名，可以留空不填。
- **客户端超时**：设置此 L2TP 拨号连接客户端的超时时间，取值范围为 0-65535 秒，默认值是 10 秒，一般不需要修改。
- **启用隧道认证**：如果要启用隧道认证，则勾选。
- **设置隧道认证的密码**：此密码设置要在启用隧道认证的前提下进行。
- **HELLO 报文间隔**：设置此 L2TP 拨号连接的 HELLO 报文间隔，取值范围为 5-100 秒，默认值是 60 秒，一般不需要修改。
- **备用服务端的 IP 或域名**：如果服务器不能连通，可以拨号到备用服务端，可以设置 4 个备用服务器，一般不需要设置。

◆**保存**：参数输入完成后，单击“保存”按钮，将设置的信息保存到设备上，即依照给定的参数进行 L2TP 客户端拨号连接设定。保存后如果提示操作成功，则表示输入配置信息已经生效，如果提示操作失败，则用户需要重新输入参数，并检查自己输入的参数是否合法有效。

◆**返回**：单击该按钮返回 L2TP 客户端配置信息列表页面。

13.3.3 L2TP服务器配置信息列表

在 Tab 标签上单击 L2TP 服务器，进入 L2TP 服务器配置信息列表页面，如下图：

◆**L2TP 服务名**：显示 L2TP 的服务名，用来区分不同的 L2TP 服务。

◆**VPN 服务端 IP**：显示此服务使用的 IP。

◆**VPN 客户端获取地址的方式**：显示给 L2TP 客户端分配地址的方式，有“不指定”，“IP”和“地址池”三种。

◆**操作**：单击“修改”超链接，进入 L2TP 服务器配置页面，可以修改 L2TP 服务器配置参数。单击“新建”按钮，可以添加一条 L2TP 服务。单击“删除”按钮，删除已选中的 L2TP 服务。

13.3.4 添加或修改L2TP服务器配置

单击打开菜单“虚拟专网”→“L2TP 配置”，进入 L2TP 服务器配置信息列表页面，再单击“新建”按钮，或者在 L2TP 服务器配置信息列表页面中找到需要配置的 L2TP 服务，点击其对应的“操作”一栏的“修改”超链接，即可进入“L2TP 服务器配置页面”。

◆**L2TP 服务名**：设置 L2TP 的服务名，此字段为系统自动生成，用户不可修改。

◆**VPN 服务端 IP**：设置服务端使用的 IP 地址，为一私网 IP。

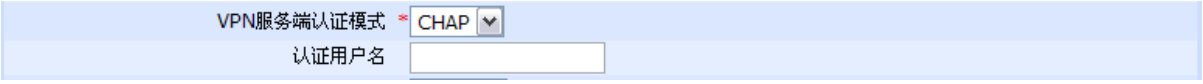
◆**VPN 服务端子网掩码**：设置 VPN 服务端使用的子网掩码。

★注意：

此 IP 不能与本地内网 IP 同一网段，否则会设置失败。

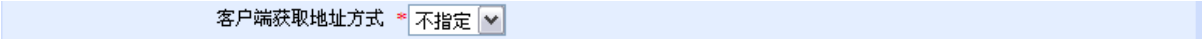
◆ **VPN 服务端认证模式**：可以选择“PAP”认证或者“CHAP”认证。

➢ **VPN 服务端认证模式**：“PAP”。选择此项的话下方不会有任何提示。



➢ **VPN 服务端认证模式**：选择“CHAP”后下方会有一个认证用户名输入框用来输入认证用户名。

◆**客户端分配地址方式**：可以选择“不指定”，“IP”或者“地址池”。



➢ **客户端分配地址方式**：“不指定”。选择此项的话下方不会有任何提示。

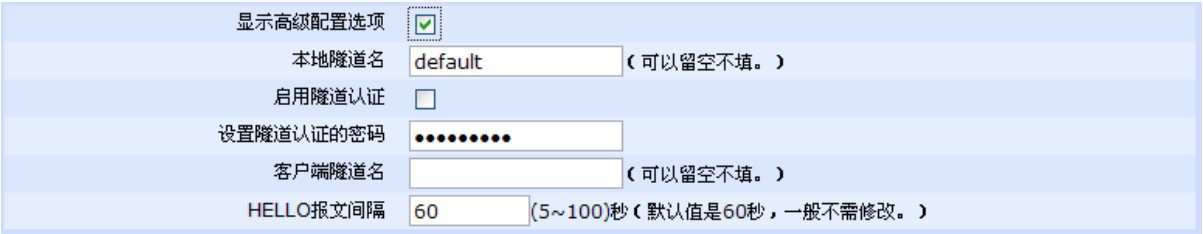
➢ **客户端获取地址方式**：选择“IP”后下方会出现一个 IP 地址输入框来输入 IP 地址。

➢ **客户端获取地址方式**：选择“地址池”后会出现两个 IP 地址输入框来确定地址池包含的地址范围。

★注意：

地址池中的地址数量不能超过 1024 个，否则会设置失败。

◆**显示高级选项**：显示 L2TP 服务器配置的高级选项。



- **本地隧道名**：设置此 L2TP 服务端使用的隧道名，可以留空不填。
- **启用隧道认证**：如果要启用隧道认证，则勾选。
- **设置隧道认证的密码**：此密码设置要在启用隧道认证的前提下进行。
- **客户端隧道名**：设置拨号到此 L2TP 服务端的客户端隧道名，可以留空不填。
- **HELLO 报文间隔**：设置此 L2TP 服务端的 HELLO 报文间隔，取值范围为 5-100 秒，默认值是 60 秒，一般不需要修改。

◆**保存**：参数输入完成后，单击“保存”按钮，将设置的信息保存到设备上，即依照给定的参数进行 L2TP 服务器设定。保存后如果提示操作成功，则表示输入配置信息已经生效，如果提示操作失败，则用户需要重新输入参数，并检查自己输入的参数是否合法有效。

◆**返回**：单击该按钮返回 L2TP 服务器配置信息列表页面。

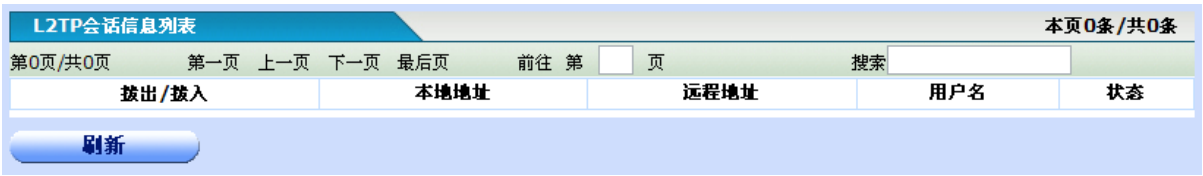
◆**配置拨号用户**：如果想要添加或者修改拨号用户，请单击此按钮进入拨号用户管理相关页面。

★**注意**：

如果由服务端给客户端分配 IP 或者地址池，设备会自动将单一 IP 或者地址池中的所有 IP 添加到 NAT 访问列表中并设为允许，如果不小心删除，可能客户端会无法上网。

13.3.5 L2TP会话信息

在 Tab 标签上单击 L2TP 会话信息标签，进入 L2TP 会话信息列表页面，如下图：



◆**拨出/拨入**：用“拨出”表示设备以客户端的身份向服务端拨号，用“拨入”来表示设备配置的是服务端。

◆**本地地址**：显示本条会话的本地隧道地址。

◆**远程地址**：显示与本地地址连接的远程隧道地址。

◆**用户名**：显示本条会话使用的用户名。

◆**状态**：显示本条会话的状态。

◆**刷新按钮**：单击此按钮获得即时 L2TP 会话信息。

13.4 IPIP配置

单击打开菜单“虚拟专网”→“IPIP配置”即可进入“IPIP配置信息列表页面”，在该页面列出了已经配置的IPIP隧道信息，用户可以根据实际需要修改或删除已配置的IPIP隧道，也可以单击新建按钮添加一条IPIP隧道。

13.4.1 IPIP隧道信息列表

IPIP 隧道信息列表显示了已经配置好的 IPIP 隧道信息，如下图：

◆**隧道编号**：为 IPIP 隧道的编号。

◆**隧道类型**：显示 IPIP，表示此隧道为一个 IPIP 隧道。

◆**隧道地址来源**：为隧道地址的类型，这里为 IP 地址。

◆**隧道地址**：显示隧道的 IP 地址。

◆**源地址类型**：可以显示“WAN”，“LAN”或者“IP”。

◆**隧道源地址**：如果源地址类型显示为“WAN”或者“LAN”，这里显示相应的序号，如：源地址类型显示“WAN”，本字段显示 1，则表示隧道源地址是“WAN1”。如果源地址类型显示为“IP”，本字段显示使用的 IP 地址。

◆**目的地址类型**：可以显示“IP”或者“主机名”。

◆**隧道目的地址**：如果目的地址类型显示为“IP”，这里显示目的地址的 IP，如果目的地址类型显示为“主机名”，这里则显示目的地址的主机名。

◆**操作**：单击修改超链接，进入“IPIP 配置”页面，可以修改 IPIP 隧道的配置参数。单击“新建”按钮，可以添加一个 IPIP 隧道。单击“删除”按钮，删除已选中的 IPIP 隧道。

13.4.2 添加或修改IPIP配置

单击打开菜单“虚拟专网”→“IPIP配置”，再单击“新建”按钮，或者在管理员信息列表中找到需要配置的IPIP隧道，点击其对应的“操作”一栏的“修改”超链接，即可进入“IPIP配置页面”。

◆**隧道编号**：当前配置的隧道的编号，系统默认生成，用户不可修改。

◆**VPN 通道的 IP 与子网掩码**：设置当前配置的隧道的 IP 与子网掩码。

★注意：

这里设置的 IP 地址与子网掩码不能与设备中已经设置好的重复，否则会设置失败。

◆ **隧道源端口或 IP**：下拉菜单里有当前设备的所有物理接口，可以选择其中一个，也可以选择“IP”项，这时，在下方会弹出一个 IP 地址输入框，用来输入 IP 地址。如下：

◆**隧道目的地址**：下拉菜单里有“域名”和“IP”可供选择，如果选择“域名”，在右边输入框内输入目的地址的域名，如果选择“IP”，在右边输入框内输入目的地址的 IP。

◆**保存**：参数输入完成后，单击“保存”按钮，将设置的信息保存到设备上，即依照给定的参数进行 IPIP 隧道设定。保存后如果提示操作成功，则表示输入配置信息已经生效，如果提示操作失败，则用户需要重新输入参数，并检查自己输入的参数是否合法有效。

◆**返回**：单击该按钮返回IPIP隧道信息列表页面。

13.5 GRE配置

单击打开菜单“虚拟专网”→“GRE配置”即可进入“GRE配置信息列表页面”，在该页面列出了已经配置的GRE隧道信息，用户可以根据实际需要修改或删除已配置的GRE隧道，也可以单击新建按钮添加一条GRE隧道。

13.5.1 GRE隧道信息列表

GRE 隧道信息列表显示了已经配置好的 GRE 隧道信息，如下图：

◆**隧道编号**：为 GRE 隧道的编号。

◆**隧道类型**：显示 GRE，表示此隧道为一个 GRE 隧道。

◆**隧道地址来源**：为隧道地址的类型，这里为 IP 地址。

◆**隧道地址**：显示隧道的 IP 地址。

◆**源地址类型**：可以显示“WAN”，“LAN”或者“IP”。

◆**隧道源地址**：如果源地址类型显示为“WAN”或者“LAN”，这里显示相应的序号，如：源地址类型显示“WAN”，本字段显示 1，则表示隧道源地址是“WAN1”。如果源地址类型显示为“IP”，本字段显示使用的 IP 地址。

◆**目的地址类型**：可以显示“IP”或者“主机名”。

◆**隧道目的地址或域名**：如果目的地址类型显示为“IP”，这里显示目的地址的 IP，如果目的地址类型显示为“主机名”，这里则显示目的地址的主机名。

◆**隧道密钥**：显示当前 GRE 隧道使用的隧道密钥。

◆**操作**：单击修改超链接，进入“GRE 配置”页面，可以修改 GRE 隧道的配置参数。单击“新建”按钮，可以添加一个 GRE 隧道。单击“删除”按钮，删除已选中的 GRE 隧道。

13.5.2 添加或修改GRE配置

单击打开菜单“虚拟专网”→“GRE配置”，再单击“新建”按钮，或者在管理员信息列表中找到需要配置的GRE隧道，点击其对应的“操作”一栏的“修改”超链接，即可进入“GRE配置页面”。

◆**隧道编号**：当前配置的隧道的编号，系统默认生成，用户不可修改。

◆**VPN 通道的 IP 与子网掩码**：设置当前配置的隧道的 IP 与子网掩码。

★注意：

这里设置的 IP 地址与子网掩码不能与设备中已经设置好的重复，否则会设置失败。

◆ **隧道源端口或 IP**：下拉菜单里有当前设备的所有物理接口，可以选择其中一个，也可以选择“IP”项，这时，在下方会弹出一个 IP 地址输入框，用来输入 IP 地址。如下：

◆**隧道目的地址或域名**：下拉菜单里有“域名”和“IP”可供选择，如果选择“域名”，在右边输入框内输入目的地址的域名，如果选择“IP”，在右边输入框内输入目的地址的 IP。

◆**保存**：参数输入完成后，单击“保存”按钮，将设置的信息保存到设备上，即依照给定的参数进行 GRE 隧道设定。保存后如果提示操作成功，则表示输入配置信息已经生效，如果提示操作失败，则用户需要重新输入参数，并检查自己输入的参数是否合法有效。

◆**返回**：单击该按钮返回GRE隧道信息列表页面。

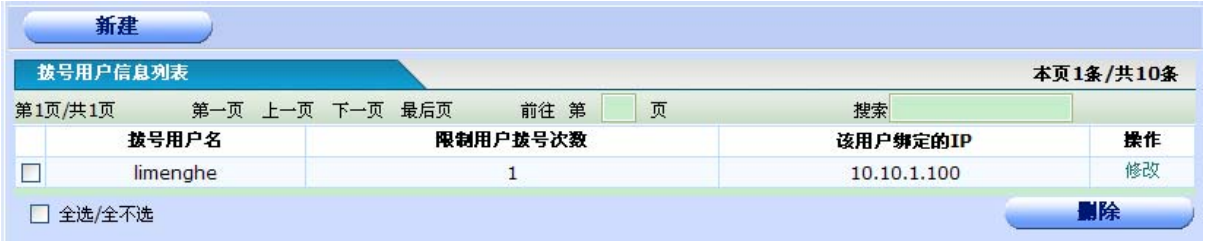
13.6 拨号用户管理

单击打开菜单“虚拟专网”→“拨号用户管理”即可进入“拨号用户信息列表页面”，在该页面列出了已经配置的拨号用户信息，用户可以根据实际需要修改或删除已配置的拨号用户，也可以单击新建按钮添加一个新的拨号用户。

拨号用户不拥有在路由器命令行方式和WEB管理方式中任何的telnet到路由器的权限、通过命令行或WEB方式配置路由器的权限以及通过命令行或WEB方式查看路由器运行监控信息的权限。拨号用户只能用于PPPOE/L2TP/PPTP等虚拟拨号方式下。

13.6.1 拨号用户信息列表

拨号用户信息列表显示了已经配置好的拨号用户信息，如下图：



◆**拨号用户名**：为配置好的拨号用户名。

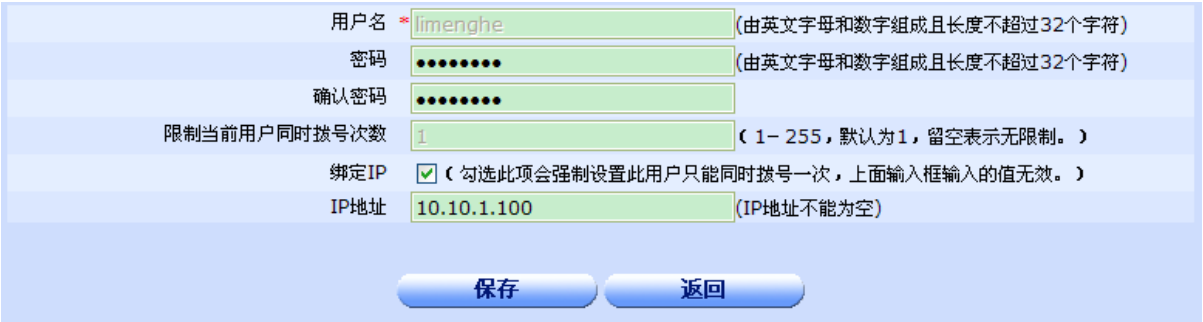
◆**限制用户拨号次数**：限制使用当前用户名拨号的同时在线的客户端个数。

◆**该用户绑定的 IP**：为该用户名绑定的 IP，如果配置了此项，限制用户拨号次数被强制为 1。

◆**操作**：单击修改超链接，进入“拨号用户管理”配置页面，可以修改拨号用户名的配置参数。单击“新建”按钮，可以添加一个新的拨号用户。单击“删除”按钮，删除已选中的拨号用户名。

13.6.2 拨号用户管理配置

单击打开菜单“虚拟专网”→“拨号用户管理”，再单击“新建”按钮，或者在管理员信息列表中找到需要配置的管理员，点击其对应的“操作”一栏的“修改”超链接，即可进入“用户管理配置页面”。



◆**用户名**：设置用于拨号的用户名，如果为单击“修改”超链接进入的本页面，本字段不可操作。

◆**密码及确认密码**：设置拨号用户名对应的密码。

◆**限制当前用户同时拨号次数**：限制使用当前用户名拨号的同时在线的客户端个数。

◆**绑定 IP 及 IP 地址**：设置为此拨号用户名绑定的 IP。

◆**保存：**参数输入完成后，单击“保存”按钮，将设置的信息保存到设备上，即依照给定的参数进行用户设定。保存后如果提示操作成功，则表示输入配置信息已经生效，如果提示操作失败，则用户需要重新输入参数，并检查自己输入的参数是否合法有效。

◆**返回：**单击该按钮返回拨号用户信息列表页面。

第14章　系统管理

14.1　用户管理

用户管理可以实现管理登录用户的密码和管理权限。

单击打开菜单“系统管理”→“用户管理”即可进入“管理员信息列表页面”，在该页面列出了已经配置的管理员，用户可以根据实际需要修改或删除已配置的管理员，也可以单击新建按钮添加一个管理员。

14.1.1　管理员信息列表

管理员信息列表显示了已经配置好的管理员信息，如下图：

◆**管理员用户名**：为配置好的管理员用户名。

◆**用户权限**：显示此管理员的权限。

◆**操作**：单击修改超链接，进入“用户管理”配置页面，可以修改用户名的配置参数。单击“新建”按钮，可以添加一个新用户。单击“删除”按钮，删除已选中的用户名。

★注意：

不能删除所有系统管理员用户（至少保留一个系统管理员用户），否则将无法通过 web 配置本设备。

14.1.2　添加或修改登录用户密码和权限

单击打开菜单“系统管理”→“用户管理”，再单击“新建”按钮，或者在管理员信息列表中找到需要配置的管理员，点击其对应的“操作”一栏的“修改”超链接，即可进入“用户管理配置页面”。

◆**管理员用户名**：设置登录此设备的用户名，如果为单击“修改”超链接进入的本页面，本字段不可操作。

◆**密码及确认密码**：设置用户名对应的密码。管理员用户名和密码只能为字母、数字和除?\"&#和空格以外的字符。

◆**用户权限**：可以选择“系统管理员”和“配置受限用户”，系统管理员拥有全部权限，受限用户可以登录 web 页面查看信息，但是不能修改配置。

◆**保存**：参数输入完成后，单击“保存”按钮，将设置的信息保存到设备上，即依照给定的参数进行用户设定。保存后如果提示操作成功，则表示输入配置信息已经生效，如果提示操作失败，则用户需要重新输入参数，并检查自己输入的参数是否合法有效。

◆**返回**：单击该按钮返回管理员信息列表页面。

14.2 时钟管理

单击打开菜单“系统管理”→“时钟管理”即可进入“时间设置页面”，在该页面可以查看和配置设备的时区、时间，设置时间的方式可以选择“手工设置”，也可以选择“网络时间同步”。

◆**系统时间**：显示设备的系统时间，可以通过刷新按钮来获得即时时间。

◆**时区选择**：设置设备使用的时区。

◆**手工设置时间**：选择此项来进行人工设置时间。

◆**网络时间同步**：可以在 SNTP 服务器中输入网络时间服务器的 IP，设备会自动从服务器上获取时间。

◆**同步时间间隔**：从网络时间服务器获取时间的间隔，默认是 1 分钟。

◆**保存**：参数输入完成后，单击“保存”按钮，将设置的时间信息保存到设备上。保存后如果提示操作成功，则表示输入配置信息已经生效，如果提示操作失败，则用户需要重新输入参数，并检查自己输入的参数是否合法有效。

14.3 软件升级

单击打开菜单“系统管理”→“软件升级”即可进入“软件升级页面”，在该页面可以备份设备的 IOS 软件，也可以更新设备的 IOS 软件。

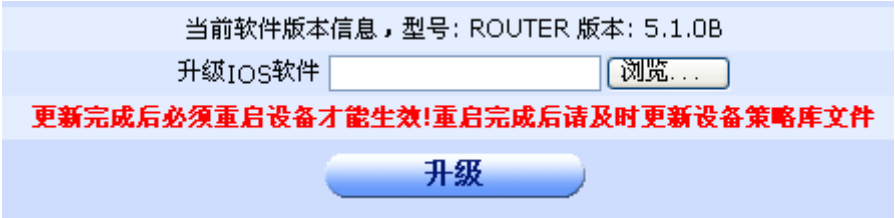
14.3.1 备份IOS软件

可以单击下图所示的“备份 IOS 软件”按钮来备份当前设备的 IOS 软件。

◆**当前软件版本信息**：列出了当前软件的版本信息。

14.3.2 升级IOS软件

可以单击下图所示的“升级”按钮来升级当前设备的 IOS 软件。



◆**当前软件版本信息**：列出了当前软件的版本信息。

◆**升级 IOS 软件**：可以在文本框内输入 IOS 软件的绝对路径，也可以通过“浏览”按钮选择文件。

★**注意：**

更新完 IOS 软件后必须重启设备才能生效。

IOS 文件名要与设备中的文件名一致，否则不能升级。

14.4 日志管理

单击打开菜单“系统管理”→“日志管理”即可进入“日志管理页面”，在该页面可以配置日志的服务器和日志的缓冲区。

◆**启用日志服务器**：启用/禁止设备日志向日志服务器的输出。

◆**系统日志服务器地址**：输入接收设备日志的服务器的地址。日志会输出到指定的日志服务器上。

◆**系统日志信息等级**：系统日志的输出分成各个等级。可以指定输出特定范围的日志。数字越大，日志越详细。

◆**启用日志缓冲区**：启用该配置后，可以设置日志缓冲区的信息。

◆**系统日志缓冲区大小**：设置设备上的日志缓冲区的大小。

◆**缓存日志信息等级**：设置设备上缓存的日志等级。数字越大，日志越详细。

◆**保存**：参数输入完成后，单击“保存”按钮，将设置的日志管理保存到设备上。保存后如果提示操作成功，则表示输入配置信息已经生效，如果提示操作失败，则用户需要重新输入参数，并检查自己输入的参数是否合法有效。

> 提示：
>
> 系统日志信息等级和缓存日志信息等级数字越大，日志越详细。

14.5 远程管理

单击打开菜单“系统管理”→“远程管理”即可进入“远程管理配置页面”，在该页面可以配置远程web管理和远程snmp管理。

14.5.1 Web管理

Web管理可以配置登录web配置页面的端口，也可以限制通过WAN口访问web配置页面以及拒绝外网ping，能保护本设备不受外网攻击。

单击“web 远程管理”Tab，显示 web 远程管理配置页面，如下图：

◆**设置 web 访问端口**：设置通过 web 配置本设备时使用的端口号。

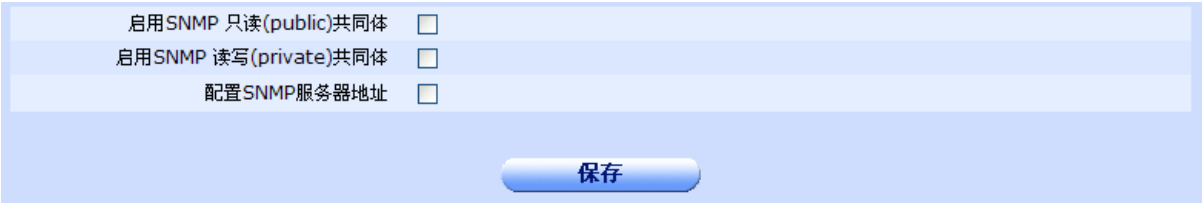
◆**禁止外部主机访问 WEB 管理页面：**选中并应用则禁止通过外网端口配置本设备，只能通过内网电脑配置。建议打开。

◆**拒绝外网 PING：**拒绝接收来自外网的 PING，有利于保护内网的安全。

◆**保存：**参数输入完成后，单击“保存”按钮，将设置的远程 web 管理保存到设备上。保存后如果提示操作成功，则表示输入配置信息已经生效，如果提示操作失败，则用户需要重新输入参数，并检查自己输入的参数是否合法有效。

14.5.2 SNMP管理

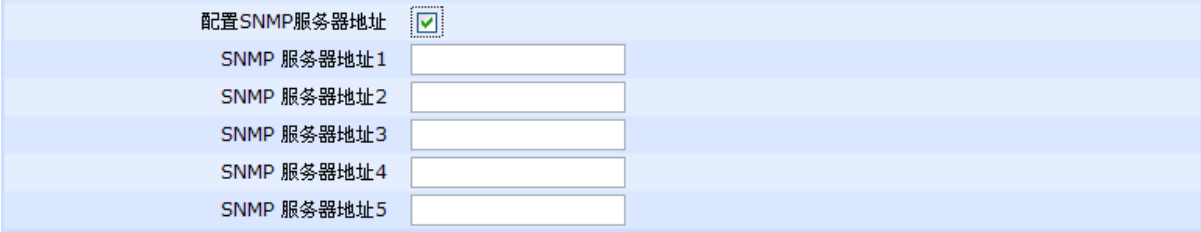
单击“snmp 远程管理”Tab，显示 snmp 远程管理的配置页面，如下图：



◆**启用 SNMP 只读(public)共同体：**选中并应用则启用 SNMP 只读(public)共同体。

◆**启用 SNMP 读写(private)共同体：**选中并应用则启用 SNMP 读写(private)共同体。

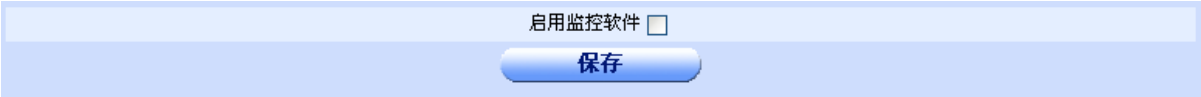
◆**配置 SNMP 服务器地址：**勾选显示地址输入框。最多可以设置 5 个 SNMP 服务器地址。



◆ **保存：**参数输入完成后，单击“保存”按钮，将设置的远程 SNMP 管理保存到设备上。保存后如果提示操作成功，则表示输入配置信息已经生效，如果提示操作失败，则用户需要重新输入参数，并检查自己输入的参数是否合法有效。

14.5.3 NAT监控管理

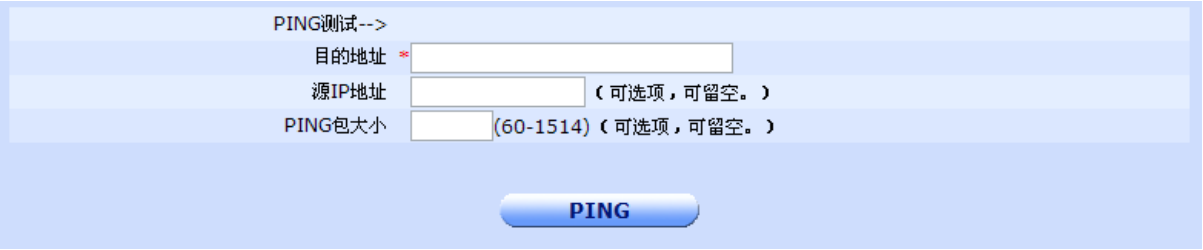
单击“snmp 远程管理”Tab，显示 snmp 远程管理的配置页面，如下图：



◆勾选启用监控软件并点“保存”按钮就启用了本设备的 NAT 监控，NAT 监控软件可以另外获取。

14.6 诊断工具

单击打开菜单“系统管理”→“诊断工具”即可进入“诊断工具页面”，在该页面可以诊断网络是否连通。



◆**目的地址**：诊断到此网络地址是否连通，为必填项。

◆**源 IP 地址**：选择从设备的某个特定端口发出诊断测试，为可选项。

◆**PING 包大小**：设置用于诊断使用的网络数据包的大小，为可选项。

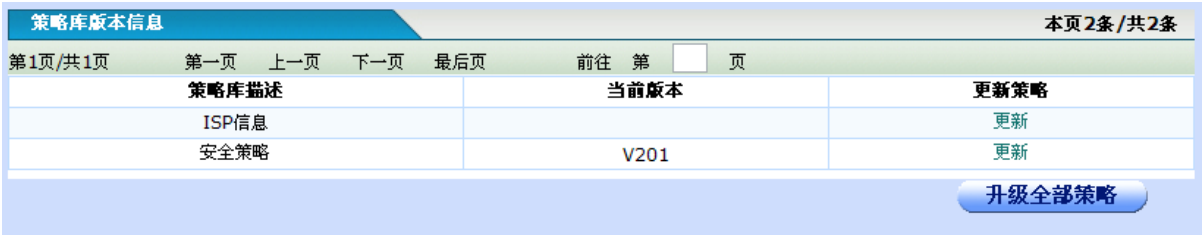
◆**PING按钮**：参数输入完成后，单击“PING”按钮，测试到目的地址的连通状态并显示测试结果。

14.7 策略库管理

单击打开菜单“系统管理”→“策略库管理”即可进入“策略库管理页面”，在该页面可以在线升级策略库和手动升级备份策略库。

14.7.1 策略库在线升级

单击“策略库在线升级”Tab，显示策略库在线升级页面，如下图：



◆**策略库描述**：策略库的描述。

◆**当前版本**：显示策略库的版本。

◆**更新策略**：单击更新超链接可以在线更新对应策略库，单击升级全部策略按钮在线升级全部策略。

14.7.2 策略库手动升级

单击“策略库手动升级”Tab，显示策略库手动升级页面，如下图：

◆**更新策略 ISP 信息**：更新 ISP 信息策略库，可以在文本框中输入策略库的绝对路径，也可以单击“浏览”按钮选择策略库，然后单击“更新策略”按钮。

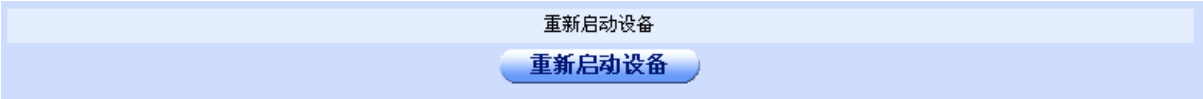
◆**备份当前 ISP 信息策略库**：单击“备份”按钮备份 ISP 策略库。

◆**更新策略安全策略**：更新安全策略库，可以在文本框中输入策略库的绝对路径，也可以单击“浏览”按钮选择策略库，然后单击“更新策略”按钮。

◆**备份当前安全策略库**：单击“备份”按钮备份安全策略库。

14.8 重新启动

单击打开菜单“系统管理”→“重新启动”即可进入“重新启动页面”，在该页面可以单击“重新启动设备”按钮来重新启动设备。

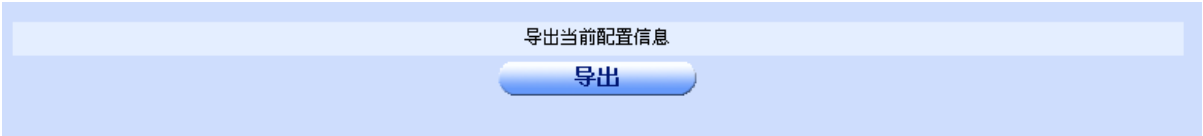


14.9 配置导入导出

单击打开菜单“系统管理”→“配置导入导出”即可进入“配置导入导出页面”，在该页面可以导入导出设备的配置文件到您的PC。

14.9.1 导出当前配置信息

导出当前配置信息页面如下图：



◆“**导出**”**按钮**：单击此按钮将在设备上下载 startup-config 文件，该文件保存了当前设备的配置信息。

14.9.2 导入配置文件

导入配置文件页面如下图：

◆**导入配置文件：**可以在文本框中输入配置文件的绝对路径，也可以单击“浏览”按钮选择配置文件，然后单击“导入”按钮。

★注意：

更新完配置文件后必须重启设备才能生效。

配置文件名要为 **startup-config**，否则不起作用。

14.10 恢复出厂配置

单击打开菜单“系统管理”→“恢复出厂配置”即可进入“恢复出厂配置页面”，在该页面可以将设备恢复到出厂时的配置。出厂配置相关信息详见1.4。

★注意：

恢复出厂配置后要重启设备才能生效。

第15章　监控信息

15.1　端口信息

端口信息显示了当前设备的端口状态。

物理接口	端口名称	是否拨号	IP地址	MAC地址	协议状态	接收速率	发送速率	带宽占用
WAN0	WAN0	否	172.16.21.60/255.255.255.0	00e0.0fb1.4ca0	连接	594 bps	120 bps	0.01%
WAN1	WAN1	否	172.16.22.60/255.255.255.0	00e0.0fb1.4ca1	断开	0 bps	0 bps	0.00%
LAN	LAN	否	192.16.21.60/255.255.255.0	00e0.0fb1.4ca2	连接	176 bps	308 bps	

15.2　系统信息

系统信息显示了路由器的基本信息，页面如下：

BIOS版本	0.4.4
设备版本	5.1.0B (BASE)
设备序列号	R7500536 000536
系统当前时间	2010-03-05 14:07:49
系统运行时间	0天0时3分44秒
CPU使用率	1%

点击刷新可以动态更新各种信息。

15.3　DHCP信息

DHCP 客户端列表显示了客户端所分配到的 IP 地址，客户主机的 MAC 地址，及租约天数。

单击“释放”可以即刻释放客户的 IP 地址。单击“释放全部”可以即刻释放所有客户端的 IP 地址。单击“刷新”以刷新客户端列表。

15.4 路由信息

本页面显示了系统路由表信息。

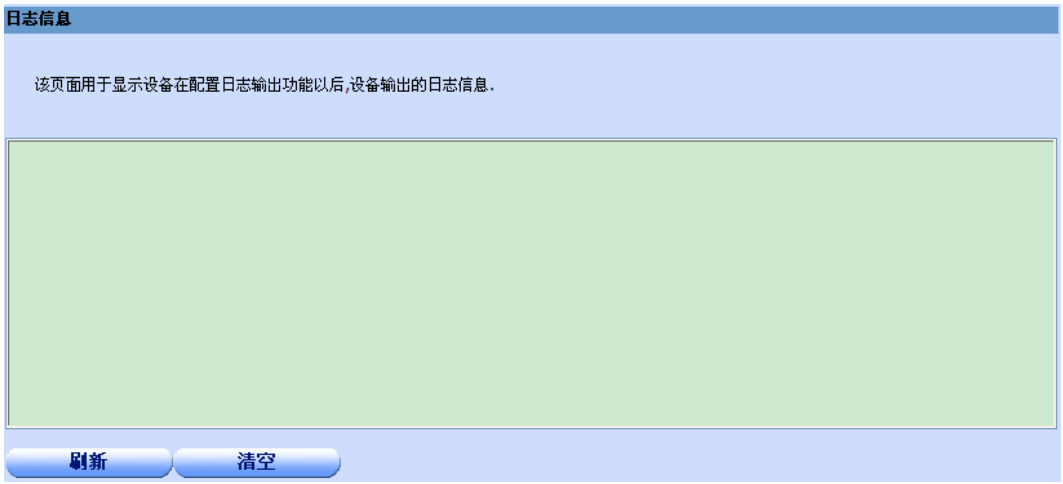
路由类型	目的地址	网关地址	应用端口
静态路由	0.0.0.0/0	192.168.1.6	WAN
静态路由	172.16.20.0/24	172.16.22.2	
直连路由	172.16.21.0/24		LAN (vn1)
直连路由	172.16.22.0/24		
直连路由	172.16.22.2/32		
直连路由	192.168.0.0/16		WAN
静态路由	192.168.111.0/24	172.16.21.43	LAN (vn1)

单击“刷新”以刷新信息列表。

15.5 日志信息

系统会记录一些日志信息，您可以观察日志信息来了解系统的状态。

本页面显示了日志信息的显示页面。



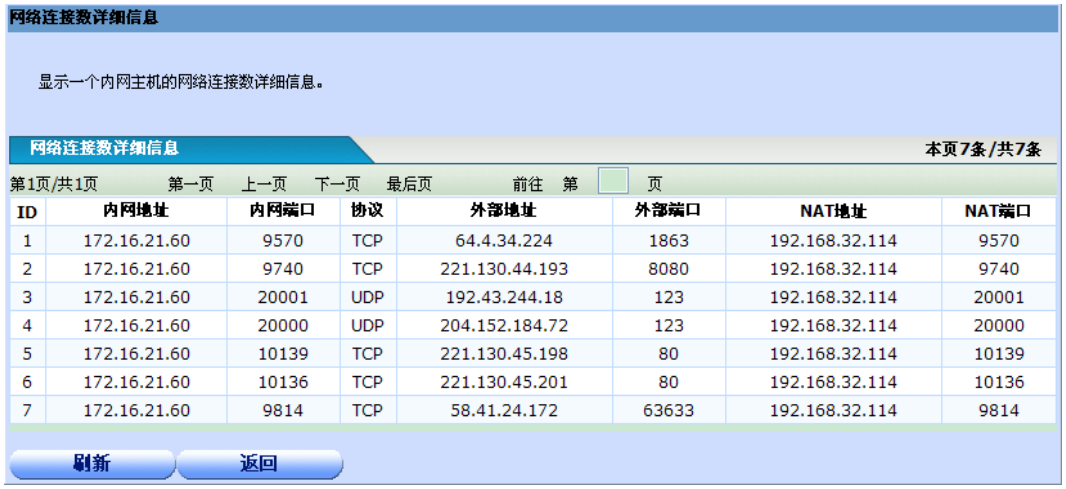
有信息时系统会显示在框中。单击“清空”按键可以清空框中的日志信息。单击“刷新”以刷新信息列表。

15.6 连接数监控

该页面可以显示当前在线主机的网络连接数和最大网络连接数。

当前在线主机IP	网络连接数	最大网络连接数
172.16.21.10	7	500
172.16.21.26	3	500
172.16.21.47	15	500
172.16.21.59	4	500
172.16.21.60	5	500
172.16.21.82	63	500

用户可以点击主机 IP 地址查看此主机的详细信息，页面如下：



ID	内网地址	内网端口	协议	外部地址	外部端口	NAT地址	NAT端口
1	172.16.21.60	9570	TCP	64.4.34.224	1863	192.168.32.114	9570
2	172.16.21.60	9740	TCP	221.130.44.193	8080	192.168.32.114	9740
3	172.16.21.60	20001	UDP	192.43.244.18	123	192.168.32.114	20001
4	172.16.21.60	20000	UDP	204.152.184.72	123	192.168.32.114	20000
5	172.16.21.60	10139	TCP	221.130.45.198	80	192.168.32.114	10139
6	172.16.21.60	10136	TCP	221.130.45.201	80	192.168.32.114	10136
7	172.16.21.60	9814	TCP	58.41.24.172	63633	192.168.32.114	9814

15.7 行为监控

显示设备在同一时刻的各种信息，便于比较查看问题。连接数排行默认显示连接数最大的 10 台主机,上传排行默认显示上传速率最大的 10 台主机，下载排行默认显示下载速率最大的 10 台主机，您可以在页面输入要显示的个数。

点击各选项卡可以显示设备的各种信息。

第16章　技术支持信息

16.1　注意事项

◆由于本公司产品更新较快, 所有涉及产品功能变更或软件升级引起的操作变更以及文档提升均不再另行通知。

◆新旧版本中功能, 界面, 文档的差别, 以新的用户指南描述为准。

附录A　常见问题FAQ

一、 WEB 为什么无法访问（WEB 页面打不开）？

1） 路由器配置了限制通过外网口访问路由器 WEB 功能，而用户正好是通过 WAN 口来登录 WEB 的，所以被限制了。

2） 从 PC 到路由器，网络 Ping 不通。

3） 路由器上的 WEB 服务器功能未开启。

4） 低权限用户试图访问高权限用户才能访问的页面。

二、 网络掉线

1） 网线未插紧。

2） P2P 下载。