进取 TM 510W
高级配置手册

版本：V1.1

执行标准：Q/SWBK1-2008

上海艾泰科技有限公司
http://www.utt.com.cn

版权声明

本文档所提供的资料包括 URL 及其他 Internet Web 站点参考在内的所有信息，如有变更，恕不另行通知。

除非另有注明，本文档中所描述的公司、组织、个人及事件的事例均属虚构，与真实的公司、组织、个人及事件无任何关系。

本手册及软件产品受最终用户许可协议（EULA）中所描述的条款和条件约束，该协议位于产品文档资料及软件产品的联机文档资料中，使用本产品，表明您已经阅读并接受了 EULA 中的相关条款。

产品编号（PN）：0904-0008-002
文档编号（DN）：PR-PMMU-1150.10-PPR-CN-1.1A

目 录

导　　读

提示：为了达到最好的使用效果，建议将 Windows Internet Explorer 浏览器升级到 6.0 以上版本。

0.1　手册说明

本手册适用的产品型号有：进取™ 510W （V2） 。

提示：其中 V2 表示设备的硬件版本号，由于产品的硬件的更新，不同硬件版本号的同一款产品的软件不能通用。其中硬件版本号在设备底部的标签上有标明，在设备的 WEB 管理页面的右上角也有标明。

本手册描述应用于艾泰科技 ReOS_SE 软件平台产品的特性和功能，提供基于 WEB 界面的配置方法及其步骤。用户应保证所使用的软件版本与本手册所描述对象一致。由于产品版本升级或其它原因，本手册内容会不定期更新。

0.2　界面风格

WEB 管理界面遵循浏览器的习惯用法，如下所示：

单选框　：选中代表只选用此项功能；

复选框　：选中代表此选项所述功能被选中；

按 钮　：单击则执行该按钮的动作；

文本框　：输入相关参数；

列表框　：通过列表框可以找到供选择的选项；

下拉框　：通过下拉框可以找到供选择的选项。

0.3　基本约定

1、 符号约定

◈ 表示基本参数，描述参数基本涵义。如果某参数中有“*”号，表示该参数为必填项目；

▶ 表示按钮，描述操作动作；

⊕ 表示提示，指出重点、注意事项。

2、 常用操作按钮的含义

添加新条目：新建相关页面的配置实例；

重填：恢复当前页面到之前的配置；

保存：保存当前所做的配置；

删除：删除相关页面的配置实例；

删除所有条目：删除列表中所有的配置实例；

刷新：刷新当前页面相关状态信息；

帮助：获取相应的帮助信息。

3、 列表功能详解

本产品 WEB 界面中的列表有可编辑列表和只读列表两种类型：

- 可编辑列表用来显示、编辑各种配置信息，能够添加、修改、删除列表条目；
- 只读列表用来显示系统状态信息，不可编辑。

本产品 WEB 界面的列表（如：静态 DHCP 列表、DHCP 客户端列表、IP/MAC 绑定信息列表等）支持排序功能。操作步骤如下：在某个列表中，单击某列的标题，则按照该列数据对表中所有记录进行排序。第一次单击为降序，第二次单击为升序，第三次为降序，依次类推。每次排序后，列表重新从第一页开始显示。

下面将以可编辑列表“NAT 静态映射列表”（如图 0-1）为例说明列表中各参数及按钮的含义。

图 0-1 NAT 静态映射列表

列表中各元素的功能如下表：

列表元素	功能

1/50	当前配置实例数/可配置实例总数。
1/1	当前页面序号/总页面数，此处指第 1 页/共 1 页。
第一页 、上一页 、下一页 、最后页	超链接，单击即可转到第一页、上一页、下一页、最后页。
前往 第 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	在搜索文本框中输入要查询的字符串，再敲<Enter>键，即可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。搜索完毕后，如果需要查看列表全部信息，则需在空的文本框中直接敲<Enter>键。
	单击可进入编辑页面，用于修改当前实例。
	单击可删除当前实例。
全选 /全不选	选中后（方框中出现“√”），当前页面所有条目全部被选中；全选情况下，再单击该方框（方框变为空），当前页面所有条目全部未被选中。
添加新条目	单击可进入 ***NAT 静态映射配置***页面，用于添加新条目。
删除所有条目	单击此按钮，可删除表中所有条目。
删除	先选择某条（或多条）需删除的条目（单击其首列中的方框，方框中出现“√”，再单击<删除>，可删除选中的条目。

表 0-1 列表基本功能

0.4 出厂配置

参数	出厂值	解释说明
用户名	admin	用户名和密码区分大小写。
密码	admin	
LAN 口地址	192.168.1.1/255.255.255.0	内网用户可通过该地址对设备进行维护。
WAN 口地址	动态 IP 接入	
SSID	UTT-HiPER_ABCDEF	设备的 SSID 值，无线客户端必须使用相同的 SSID，才能连接到无线设备。其中 ABCDEF 为设备的序列号转换成 16 进制的数字。

表 0-2 出厂配置

0.5 内容简介

手册介绍艾泰科技进取 TM 510W 产品各功能的配置及应用，包括：产品概述、硬件安装、登录设备、配置向导、开始菜单、网络参数、无线配置、高级配置、用户管理、行为管理、带宽管理、防火墙、VPN 配置、系统管理、系统状态和客户服务。

第 1 章 产品概述

介绍艾泰科技进取 TM 510W 的特点及功能特性。

第 2 章 硬件安装

介绍艾泰科技进取 TM 510W 的安装步骤及注意事项。

第 3 章 登录设备

介绍如何正确配置内网中的计算机及如何登录设备。

第 4 章 配置向导

介绍如何通过“配置向导”快速配置设备，完成最基本的上网配置。

第 5 章 开始菜单

通过导航条“开始”菜单可以进入下列页面进行相关配置：

- 配置向导——通过“配置向导”完成设备最基本的上网配置；
- 运行状态——查看设备各接口的相关信息，如 IP 地址、网关地址、连接时间等；
- 接口流量——可查各接口的流量图及统计值；
- 重启设备——重新启动设备。

第 6 章 网络参数

介绍如何配置设备的网络属性，包括：

- WAN 口配置——配置设备的接口，包括：WAN1 口、3G、APClient；
- 线路组合——选择线路组合方式，配置线路检测方法；
- LAN 口配置——配置设备的 LAN 口；
- DHCP 服务器——配置 DHCP 服务器、DNS 服务器及静态 DHCP 功能；
- DDNS 配置——申请、配置 DDNS 服务，查看 DDNS 状态信息；
- UPnP 配置——配置 UPnP 功能，查看 UPnP NAT 映射列表。

第 7 章 无线配置

主要介绍配置设备无线功能的参数，包括：

- 基本设置——配置设备的无线基本功能；

- 无线安全设置——配置设备的无线安全机制；
- 无线 MAC 地址过滤——配置设备无线 MAC 地址过滤功能；
- 无线高级配置——配置设备无线高级功能；
- 无线主机状态——查看无线主机的状态信息。

第 8 章 高级配置

介绍设备的高级功能，包括：

- NAT 和 DMZ 配置——配置设备的 NAT 规则、虚拟服务器、NAT 静态映射；
- 路由配置——配置静态路由，预先指定对某一网络访问时所要经过的路径；
- 网络尖兵防御——配置设备的网络尖兵防御功能，破解运营商设置的共享检测。

第 9 章 用户管理

介绍设备的用户管理功能，包括：

- 用户状态——查看内网用户的状态信息；
- PPPoE 服务器——配置 PPPoE 服务器、PPPoE 账号和计费功能；
- IP/MAC 绑定——配置 IP/MAC 绑定用户，防止 IP 地址盗用；
- WEB 认证——启用 WEB 认证，配置 WEB 认证账号，查看 WEB 认证列表；
- 用户组配置——配置用户组，将内网用户进行分类，方便管理。

第 10 章 行为管理

介绍设备的行为管理功能，包括：

- 时间段配置——配置时间段，定义相关功能的生效时间；
- 上网行为管理——定义内网用户的上网行为；
- QQ 白名单——在**上网行为管理**页面禁止 QQ 后，定义允许登录的 QQ 用户；
- MSN 白名单——在**上网行为管理**页面禁止 MSN 后，定义允许登录的 MSN 用户；
- 电子通告——配置通告功能，包括：日常事务通告和账号到期通告；
- 上网行为审计——启用相关上网行为审计功能，查看上网行为审计信息；
- 策略库——更新上网行为管理引用的策略。

第 11 章 带宽管理

介绍设备的带宽管理功能，包括：

- 精细化限速——为内网用户配置精细化限速；
- 弹性带宽——配置设备的弹性带宽功能。

第 12 章 防火墙

介绍设备的防火墙功能，包括：

- 安全配置——启用安全防御功能；
- 访问控制策略——配置访问控制策略，以此来控制内网用户的上网访问权限和防御外网攻击；
- 域名过滤——只允许或禁止指定的内网用户访问某些指定的域名。

第 13 章 VPN 配置

介绍 PPTP 配置参数及如何建立 PPTP 隧道。

第 14 章 系统管理

介绍设备相关管理参数，包括：

- 管理员配置——创建 WEB 管理员、修改其用户名和密码；
- 语言选择——选择设备 WEB 页面的语言；
- 时钟管理——手工或自动设置系统时间和日期；
- 配置管理——备份系统当前配置，导入事先保存的配置，恢复设备到出厂时的配置；
- 软件升级——备份当前软件版本，下载最新软件，升级软件；
- 远程管理——配置设备的远程管理功能；
- 计划任务——配置、查看计划任务。

第 15 章 系统状态

介绍系统相关状态信息，包括：

- 运行状态——查看设备各接口的运行状态信息；
- 系统信息——查看系统的版本、时间信息，以及系统的历史记录。

第 16 章 客户服务

客户服务页面介绍上海艾泰科技有限公司的相关信息，并提供快速链接功能，包括：艾泰科技公司官方网站的 UTTCare、产品讨论、知识库、预约服务等栏目。

附录

本手册共提供 5 个附录，描述如下：

- 附录 A FAQ——提供常见问题解答；
- 附录 B 十六进制 ASCII 码表——提供十六进制 ASCII 码表；
- 附录 C 常用 IP 协议——提供常用 IP 协议号与协议名对照表；
- 附录 D 常用服务端口——提供常用服务端口号及服务名对照表；
- 附录 E 图索引——提供本手册所有图的索引目录。

0.6 联系我们

如果您在安装或使用过程中有任何疑问，请通过以下方式联系我们。

- **客服热线：4006-120-780**
- **艾泰讨论区：http://www.utt.com.cn/discuzx/forum.php**
- **E-mail 支持：support@utt.com.cn**

第1章 产品概述

1.1 关键特性

- 支持固定 IP、动态 IP、PPPoE、AP Client、3G 客户端接入
- 支持流量负载均衡以及线路备份
- 支持上网行为管理功能
- 支持 DHCP 服务器功能
- 支持 PPPoE 服务器功能，提供固定 IP 分配、账号计费等功能
- 支持日常事务通告、账号到期通告功能
- 支持 WEB 认证功能
- 支持虚拟服务器和 DMZ
- 支持多种无线模式
- 支持多种无线安全机制
- 支持 SSID 隐藏
- 支持 WMM（Wi-Fi Multimedia，无线多媒体）功能
- 支持 URL、MAC 地址、关键字过滤等防火墙策略
- 支持对用户的上网行为管理，提供丰富的管控策略
- 支持上网行为审计功能
- 支持 QQ、MSN 白名单
- 支持内/外网攻击防御
- 支持用户组、时间段管理
- 支持 VPN 功能
- 支持 UPnP
- 支持动态域名（3322.org、iplink.com.cn）
- 支持 HTTP 远程管理
- 支持 WEB 升级方式
- 支持 WEB 配置文件备份与导入
- 整机满足 6KV 防雷特性

1.2 规格

- 符合 IEEE802.3、IEEE802.3u、IEEE 802.11n、IEEE 802.11b 和 IEEE 802.11g。
- 支持 TCP/IP、DHCP、ICMP、NAT、PPPoE、静态路由等协议。
- 各个物理端口均支持自动协商功能、支持 MDI/MDI-X 正反线自适应。
- 提供状态指示灯。
- 工作环境：温度：0-40℃

  高度：0-4000m

  相对湿度：10-90%，不结露

第2章 硬件安装

2.1 面板介绍

本节具体介绍进取™ 510W 的面板，如图 2-1、图 2-2 所示。

图 2-1 前面板示意图—进取™ 510W

图 2-2 后面板示意图—进取™ 510W

1、 指示灯说明

指示灯	描述	功能
PWR	电源指示灯	电源工作正常时常亮。
SYS	系统状态指示灯	以每秒 2 次的频率闪烁，系统负担较大时，闪烁频率降低；有故障时常亮或常灭。
USB	3G 上网卡状态指示灯	插入 3G 卡后亮。
WLAN	无线状态指示灯	启用无线功能时亮，发送/接收无线数据时闪烁。
WAN	端口状态指示灯	有设备连接到 WAN 口后，该端口对应指示灯常亮，有流量时闪烁。
LAN	端口状态指示灯	有设备连接到 LAN 口，该端口对应指示灯常亮，有流量时闪烁。
备注	WPS 功能此软件版本暂不支持，故对应状态指示灯也未使用。	

表 2-1 指示灯说明

2、 接口说明

接口	说明
LAN	集成多个交换式以太网口（100M），LAN 口为 RJ-45 端口，支持正反线自适应
WAN	WAN 口为 RJ-45 端口，支持正反线自适应。
USB	3G 上网卡接口。
天线	用于无线数据的收发。

表 2-2 接口说明

3、 Reset 按钮

Reset 按钮指复位按钮，在忘记管理员口令时可通过此按钮将设备恢复到出厂时的配置。操作方法为：在设备带电运行过程中，按住 Reset 按钮 5 秒钟以上，再松开此按钮。操作后设备会恢复到出厂时的配置，并自动重启。

提示：上述操作会删除设备原来的所有配置，请谨慎使用。

2.2 安装准备

1、 标准的 10M/100M 以太网。

2、 内网中的计算机都有一个工作正常的以太网卡。

3、 内网中的计算机都安装了 TCP/IP。

4、 准备 DSL 或者 Cable Modem，或者光纤收发器。

2.3 安装步骤

设备安装步骤如下：

第一步：选择安装地点，一般是将设备安装在工作台上。

第二步：建立设备与内网的连接，将管理计算机连接到设备的 LAN 口。

第三步：根据实际情况，建立设备与外网的连接；将 Cable/DSL Modem 连接到设备的 WAN 口或将设备的无线模式设置为相应的模式连接到无线接入点或插入 3G 上网卡。

第四步：接通电源，接通电源之前确保电源供电、连接、接地正常，否则可能造成系统工作异常或系统损坏。

第五步：检查系统指示灯，查看设备的连接及工作状态是否正常。

提示：

1、 安装设备时要确保设备水平放置，且保证工作台的平稳性；

2、 尽量将设备放置在远离发热源的地方；

3、 不要在设备上放置重物；

4、 不要将设备置于太脏或潮湿的地方。

2.4 网络连接示意图

下面列出进取™ 510W 做为有线网关、3G 客户端、无线客户端的网络连接示意图。

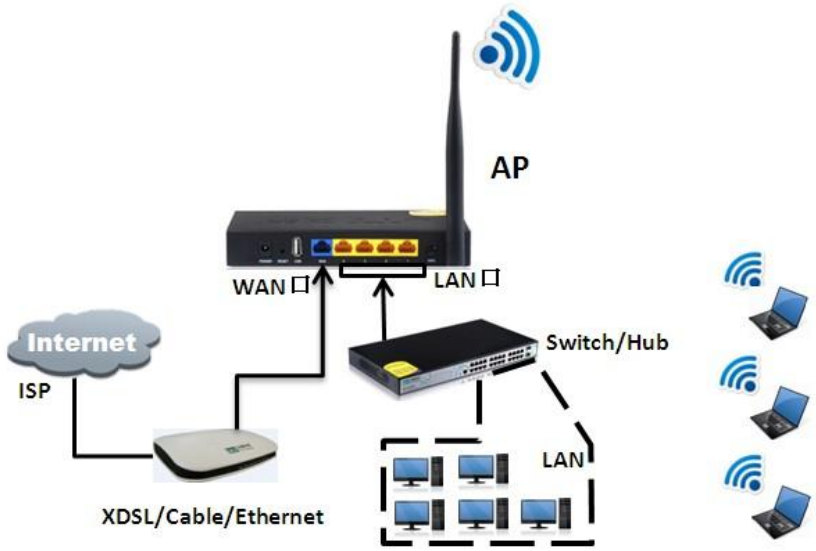

图 2-3 有线网关接入示意图

图 2-4 3G 客户端连接示意图

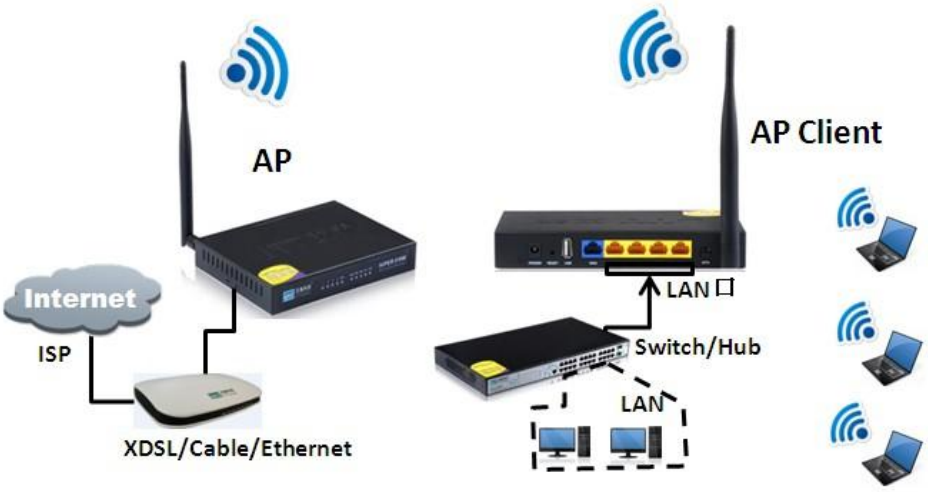

图 2-5 无线客户端连接示意图

第3章 登录设备

本章介绍如何为内网计算机配置正确的网络设置、如何登录设备以及如何使用快捷图标快速链接到艾泰官网获取产品信息和服务。

3.1 配置正确的网络设置

在通过 WEB 界面登录到设备之前，您必须对内网计算机进行正确的网络设置。

首先将计算机连接到设备的 LAN 口，接下来设置计算机的 IP 地址。

第一步，设置计算机的 TCP/IP 协议，如果已经正确设置，请跳过此步。

第二步，设置计算机的 IP 地址。您可以使用以下两种方法：

1、 设置计算机的 IP 地址为 192.168.1.2-192.168.1.254 中的任意一个地址，子网掩码为 255.255.255.0，默认网关为 192.168.1.1（设备的 LAN 口 IP 地址），DNS 服务器为当地运营商提供的地址。

2、 设置计算机的 TCP/IP 协议为“自动获取 IP 地址”。设置好后，设备内置的 DHCP 服务器将自动为计算机分配 IP 地址。

第三步，在计算机上使用 Ping 命令检查其是否与设备连通。通过**开始—>运行**，输入**cmd**，点击<确定>，打开命令窗口。输入 **ping 192.168.1.1**。

下面列举在 Windows XP 环境中执行 Ping 命令的两种结果：

如果屏幕显示如下，表示计算机已经成功和设备建立连接。

```
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
```

如果屏幕显示如下，表示计算机和设备连接失败。

```
Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Ping statistics for 192.168.1.1:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

连接失败时，请做以下检查：

1、 硬件连接：设备面板上与该 LAN 口对应的指示灯和计算机网卡灯必须亮。

2、 计算机 TCP/IP 属性的配置：如果设备 LAN 口 IP 地址为 192.168.1.1，那么计算的 IP 地址必须为 192.168.1.2-192.168.1.254 中的任意一个空闲地址。

3.2 登录设备

计算机使用 MS Windows、Macintosh、Unix 或者 Linux 操作系统时，都可以通过浏览器（Internet Explorer 或 Firefox 等）对设备进行配置。

打开浏览器，在地址栏里输入设备 LAN 口的 IP 地址，如 http://192.168.1.1。连接建立后，将会看到如图 3-1 所示的登录界面。首次使用时需以系统管理员的身份登录，即在该登录界面输入系统管理员的用户名和密码（用户名、密码的出厂值为 admin、admin，区分大小写），然后点击<确定>。

图 3-1 WEB 登录界面

如果用户名和密码正确，浏览器将显示 WEB 管理界面的首页，如图 3-2 所示。该页面右上角显产品型号、硬件版本、软件版本信息等。

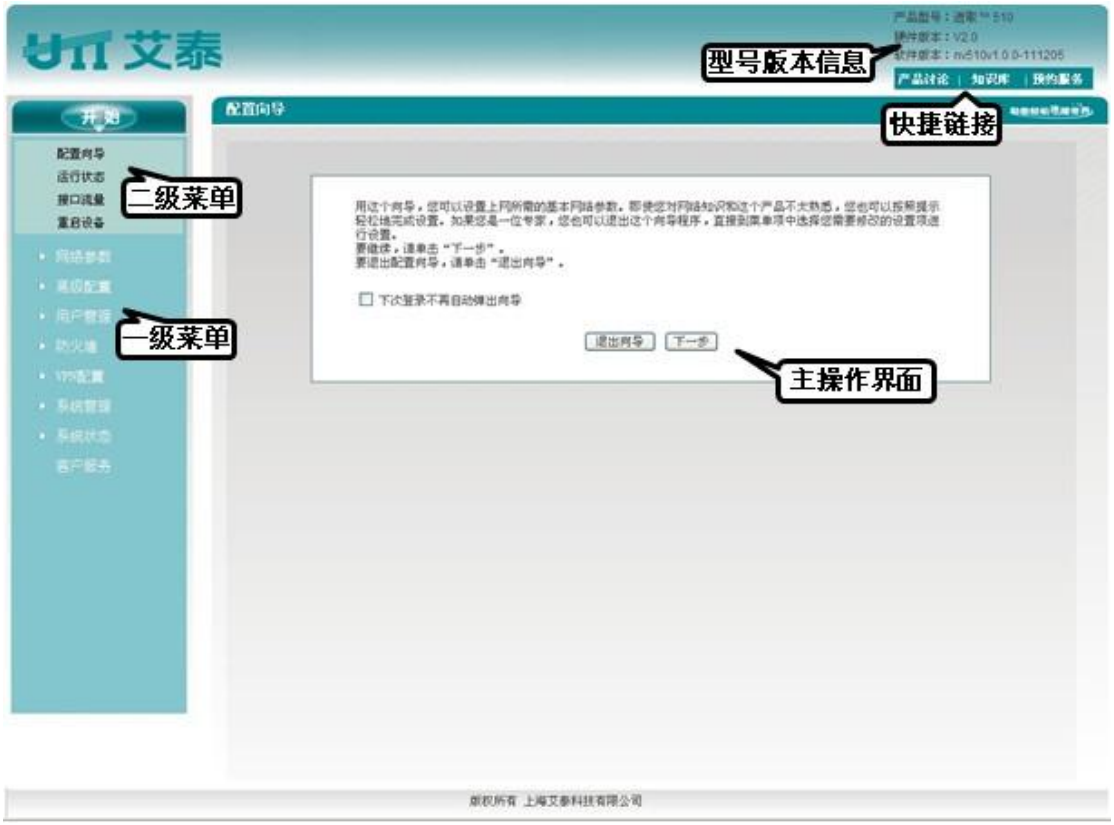

图 3-2 WEB 界面首页

首页相关说明：

1、 该页面右上角显示设备的产品型号、硬件版本、软件版本以及 3 个快速链接图标。这 3 个快捷图标的作用如下：

1) **产品讨论**——链接到艾泰科技官方网站的讨论区，参与产品的讨论；

2) **知识库**——链接到艾泰科技官方网站的知识库，查找相关技术资料；

3) **预约服务**——链接到艾泰科技官方网站预约服务页面，提前预约某一个工作时段的客户服务。

2、 该页面左侧显示主菜单条。

3、 该页面右侧为主操作页面，在主操作页面，您可以配置设备的各个功能、查看相关的配置信息、状态信息等。

4、 如果您是第一次登录设备，那么主操作页面将直接链接到配置向导首页。下一章就介绍如何通过***开始—>配置向导***页面来配置设备正常工作时所需的基本参数。

第4章 配置向导

通过阅读本章内容，可以了解设备上网所需的基本网络参数，通过配置这些参数将设备连接到 Internet。在进入配置向导配置“上网线路”之前，应正确配置内网计算机的网络设置，具体方法见第三章《登录设备》。

如果您是第一次登录设备，那么登录成功后，主操作页面将直接弹出配置向导首页。如图 4-1 所示：

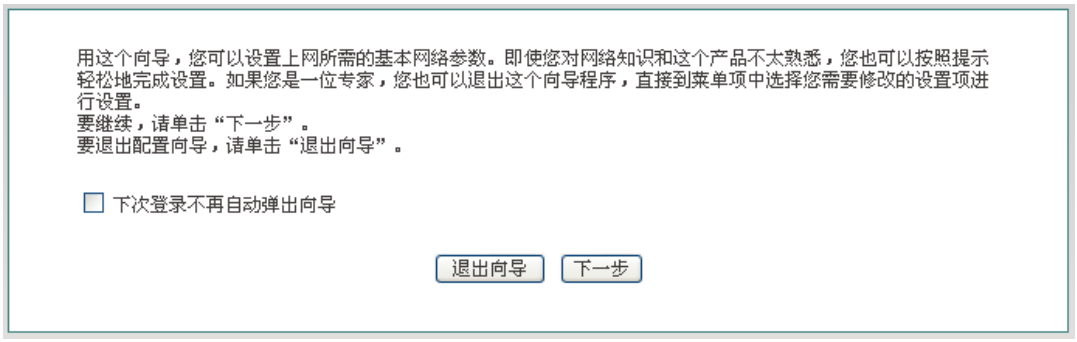

图 4-1 配置向导首页

- 下次登录不再自动弹出向导：选中后，在下次登录时直接进入***系统状态***页面；
- 退出向导：退出配置向导，返回到***系统状态***页面；
- 下一步：进入***设备接入方式选择***页面。

4.1 接入方式选择

在如图 4-2 所示的页面中，请根据您的实际情况选择设备的接入方式。

图 4-2 接入方式

- WAN1 口配置：通过配置 WAN1 口为内网用户提供接入；
- 3G 客户端配置：设备作为 3G 客户端为内网用户提供接入；

- 无线客户端配置：设备作为无线客户端为内网用户提供接入。

4.2　WAN1 口配置

WAN1 口提供的接入方式有：动态 IP 接入、固定 IP 接入、PPPoE 接入。

4.2.1　动态 IP 接入

WAN1 口默认的接入方式为动态 IP 接入，如图 4-3 所示。 如果您的上网线路接入方式为动态 IP 接入，请直接点击<下一步>，完成 WAN1 口的配置。

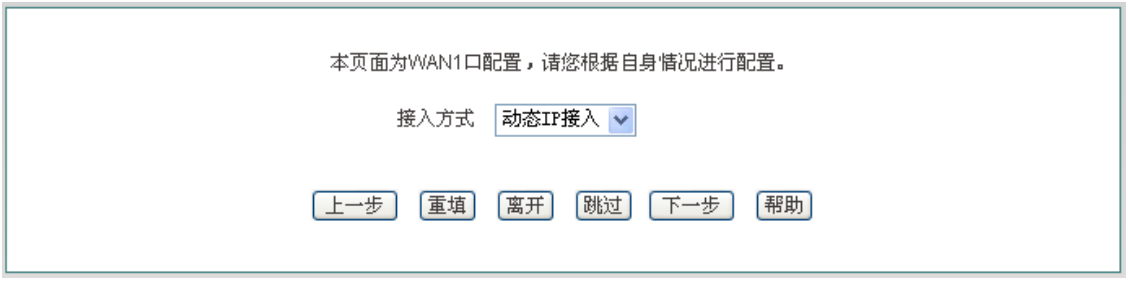

图 4-3 配置向导——动态 IP 接入

4.2.2　固定 IP 接入

如果您的上网线路接入方式为固定 IP 接入，请在图 4-4 的下拉列表框中选择“固定 IP 接入”，并填写相关参数，然后进入下一个页面，完成 WAN1 口的配置。

图 4-4 配置向导——固定 IP 接入

- IP 地址、子网掩码、网关地址、主 DNS 服务器、备 DNS 服务器：填入 ISP（例如中国电信）给您提供的广域网 IP 地址、子网掩码、网关地址和 DNS 服务器地址。

4.2.3 PPPoE 接入

如果您的上网线路接入方式为 PPPoE 接入，请在图 4-5 的下拉列表框中选择“PPPoE 接入”，并填入相应的用户名及密码，然后点击<下一步>进入下一页面完成 WAN1 口的配置。

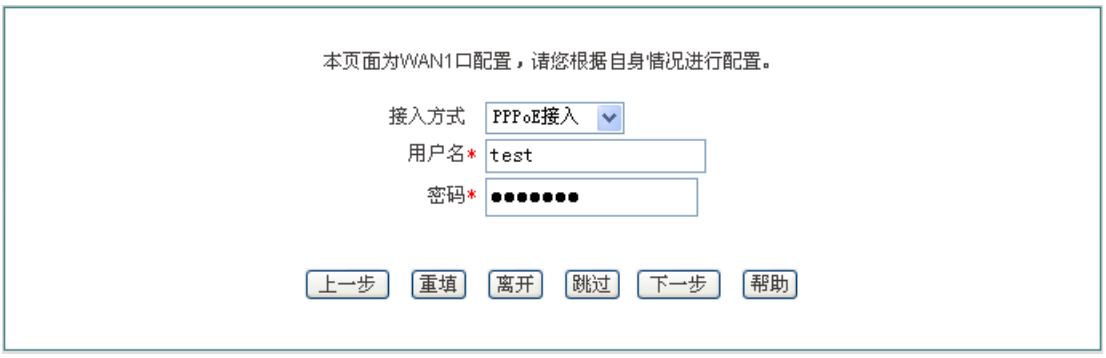

图 4-5 配置向导——PPPoE 接入

- 用户名、密码：填写 ISP 为您提供的用户名、密码。如有疑问，请询问 ISP。

4.3 3G 客户端配置

如果您是通过 3G 客户端上网，请先将 3G 上网卡插在设备的 USB 口并确认 3G 卡的类型。

图 4-6 3G 客户端配置

- 3G 卡类型：设备目前支持的 3G 卡类型有 HUAWEI E169、HUAWEI E1750、HUAWEI EC1260、HUAWEI ET128、ZTE MF637U；
- 运行商：提供网络远程接入的服务商，包括中国移动、中国联通、中国电信；

- 认证方法：采用 3G 方式接入网络时和运营商端采用的认证，提供 SIM 认证和密码认证两个选项；
- PIN 码：3G 上网卡的个人身份识别码；
- 接入点名：运营商用来提供接入的接入点的名称；
- 拨号：用来连接运营商基站时发出的拨号指令的内容之一；
- 用户名、密码：PPP 认证的用户名和密码。

提示：设备采用 3G 客户端上网时，建议用户只配置 3G 卡类型、运营商两个选项，其余参数保持默认；若需改变，请在专业人士指导下完成。

4.4　无线客户端配置

如果您是通过无线客户端上网则在如图 4-7 所示的页面配置相关参数后点击<下一步>，完成无线客户端的配置。

图 4-7 无线客户端配置

- AP 的 SSID：对端设备的 SSID，最大长度为 32 个字符，区分大小写；
- AP 的 MAC 地址：为本设备提供无线接入的 AP 的 MAC 地址；
- 安全模式：包括无安全机制、WEP、WPA-PSK/WPA2-PSK。

设备作为无线客户端连接到 AP，为内网用户提供无线接入。无线通信的安全性强弱可以通过安全模式的选择来配置。下面分别介绍“安全模式”为 WEP、WPA-PSK/WPA2-PSK 时需配置的参数的涵义。

1、 WEP

图 4-8 安全模式——WEP

- 认证类型：WEP 认证类型包括开放系统和共享密钥；
  - 开放系统：无线客户端主机在不提供认证密钥的前提下，通过认证并关联到无设备；但若要进行数据传输，必须提供正确的密钥；
  - 共享密钥：无线客户端主机必须提供正确的密钥才能通过认证，否则无法关联到无线设备，从而无法进行数据传输；
- 密钥格式：提供 16 进制、ASCII 码两种格式；
  - 采用 16 进制时，密钥字符可以为 0~9，A、B、C、D、E、F；
  - 采用 ASCII 码时，密钥字符可以是所有的 ASCII 码；
- 密钥选择：用户可根据需要输入 1~4 个密钥，这 4 个密钥可以采用不同的密钥类型；
- WEP 密钥：设置密钥值，密钥的长度受密钥类型的影响；
  - 选择 64 位密钥时，输入 16 进制字符 10 个或者 ASCII 码字符 5 个；
  - 选择 128 位密钥时，输入 16 进制字符 26 个或者 ASCII 码字符 13 个；
- 密钥类型：选项包括禁用、64 位、128 位；其中，禁用表示不使用当前密钥；而 64 位、128 位用于指定 WEP 密钥的长度。

2、 WPA-PSK/WPA2-PSK

图 4-9 安全模式——WPA-PSK/WPA2-PSK

- WPA 版本：选择具体的安全模式，包括 WPA-PSK 和 WPA2-PSK；
  - WPA：表示本设备将采用 WPA-PSK 的安全模式；
  - WPA2：表示本设备将采用 WPA2-PSK 的安全模式；
- 加密算法：选择对无线数据进行加密的安全算法，选项有 TKIP、AES；
  - TKIP：表示所有无线数据都将使用 TKIP 作为加密算法；
  - AES：表示所有无线数据都将使用 AES 作为加密算法；
- 预共享密钥：预先设置的初始化密钥，取值为 8~63 个字符。

4.5　无线参数配置

配置完设备的接入方式后，最后是配置设备的无线参数。如下图所示，填写相应的参数后，点击<完成>，即上网线路配置完成。

图 4-10　配置向导——无线参数

- SSID：设置设备的 SSID 号；它用于唯一地标识一个无线网络，其最大长度为 32 个字符，区分大小写；
- 无线模式：此参数用于设置路由器的无线模式，提供仅 11g，仅 11n 和 11b/g/n 混合三个选项；
  - 仅 11g：即纯 802.11g 模式，本模式下，最大速率 54M bps。兼容 IEEE 802.11g 标准的无线站点可以接入路由器；
  - 仅 11n：即纯 802.11n 模式，本模式下，最大速率为 150Mbps；
  - 11b/g/n 混合：符合 IEEE 802.11b、802.11g 或者 802.11n 标准的无线站点将各自按照自己的模式接入，最大速率分别为 11M bps、54M bps 和 150M bps；
- 信道：此参数用于选择无线网络工作的频率段，可以选择的范围从 1 到 11，另外提供自动选项，表示设备可以自动选择最优频率段。如果存在多个无线设备时，要注意各个设备的频段设置不能相互影响；
- 频道带宽：设置无线数据传输时所占用的频道带宽，可选项为：20M/40M 和 20M。注意，本参数仅对采用 802.11n 标准接入的无线站点起作用；对于以 802.11b 或者 802.11g 标准的无线站点来说，只能使用 20M 的频道带宽；
  - 20M/40M：选择 20M/40M 时，表示使用 802.11n 接入的无线站点将根据接入对端协商的结果选择使用 20M 或 40M 的频道带宽；
  - 20M：选择 20M 时，表示使用 802.11n 接入的无线站点将使用 20M 的频道带宽。

提示：配置向导所做的操作，只有点击<完成>才能使配置生效。

第5章　开始菜单

*开始*菜单位于 WEB 界面的一级菜单栏的最上方，它提供 4 个常见页面的接口，包括：配置向导、运行状态、接口流量、重启设备。通过*开始*菜单，您可以快速地配置设备正常工作所需的基本参数，查看各接口的信息，查看设备各接口的实时流量统计信息等。

5.1　配置向导

*开始—>配置向导*页面可以帮助您快速配置一些设备正常工作所需的基本参数，具体介绍请参见第 4 章《配置向导》。

5.2　运行状态

本节介绍*开始—>运行状态*页面，在本页面您可以查看设备各接口的相关信息。如在图 5-1 所示界面可知 WAN1 口的连接类型、连接状态、IP 地址等信息。

图 5-1 运行状态信息

5.3　接口流量

本节介绍*开始—>接口流量*页面，如图 5-2 所示，可看到相应接口的接收、发送数据的平均值、最大值、总和以及当前时刻的及时速率，并为其提供了不同的单位（kbit/s 和 KB/s）。

提示：

若本页面无法正常显示，请单击“如果不能正常显示请安装 svgviewer”超链接，安装 svgviewer 插件。

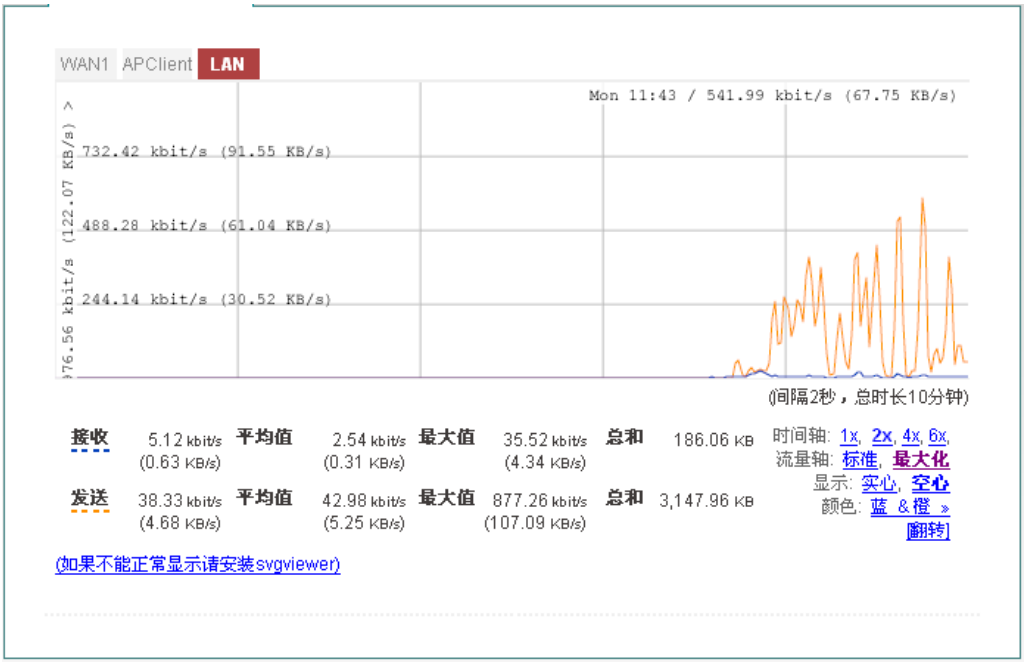

图 5-2 接口流量

- WAN1：设备的广域网口，单击该选项卡可查看其接收、发送流量的动态图；
- APClient：设备作为无线客户端，单击该选项卡可查看其接收、发送流量的动态图；
- LAN：设备的局域网口，单击该选项卡可查看其接收、发送流量的动态图；
- 时间轴：流量图中的横坐标，可通过单击图中时间轴选项（图中的 1x,2x,4x,6x）来确定显示效果；
- 流量轴：流量图中的纵坐标，可根据需要选择显示效果（如图中的标准、最大化）；
- 显示：提供实心和空心两个显示效果选项；
- 颜色：根据需要和显示的喜好，可以选择显示时的颜色，如红、蓝、黑等；
- 翻转：单击翻转按钮，接受和发送数据的颜色会互换。

5.4　重启设备

如果您需要重启设备，则进入*开始—>重启设备*页面点击<重启>。

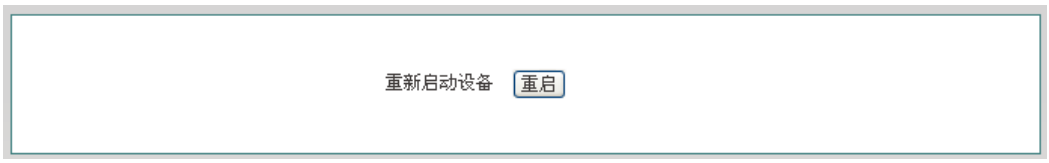

图 5-3 重启设备

- **提示**：重启时，所有的用户将断开到设备的连接。

第6章　网络参数

在网络参数主菜单中可配置设备基本网络参数，包括 WAN 口配置、LAN 口配置、DHCP 服务器、DDNS 配置和 UPnP。

6.1　WAN 口配置

本节介绍***网络参数—>WAN 口配置***页面。

在***配置向导***中配置完上网线路之后，可以到本页面查看该线路的连接状态和配置情况，也可根据需要修改配置。

图 6-1 WAN 口配置

6.1.1　WAN1、APClient 接入

如图 6-1 所示，下面介绍 WAN1 口、APClient 各种接入方式配置参数的涵义，对于在第 4 章《配置向导》中已经介绍过的参数这里不再一一列出。

提示：

配置设备为 APClient 接入时，需先进入***无线配置—>基本设置***页面将设备的工作模式设置为“APClient Mode”，并配置其他相关参数等，让该设备与无线网络中的 AP 建立连接。具体配置介绍见第 7 章《无线配置》。

1、 动态 IP 接入

- 接入方式：选择相应的接入方式，这里选择动态 IP 接入；
- 运营商策略：选择提供该 IP 地址的相应运营商，以实现电信流量走电信线路、联通流量走联通线路、移动流量走移动线路。

提示：

1. 配置线路时，用户可以通过“运营商策略”选择相应的运营商，系统将根据用户的选择生成相对应的路由，可以方便地实现电信流量走电信线路，联通流量走联通线路。

2. 一般不建议修改接口的 MAC 地址。但在某些情况下，运营商将设备的 MAC 做了绑定，这样造成新的网络设备无法拨号成功，此时需要将设备的 MAC 地址修改为原网络设备的 MAC 地址。

2、 PPPoE 接入

图 6-2 PPPoE 接入

- 密码验证方式：运营商验证用户名、密码的方式。选项有：NONE(不进行验证)、PAP、CHAP、EITHER(自动和对端设备协商密码验证方式)；
- 拨号类型：选项有自动拨号、按需拨号、手动拨号；
  - 自动拨号：当开启设备或者上一次拨号断线后设备自动拨号；
  - 按需拨号：内网有访问 Internet 流量时设备自动进行拨号连接；
  - 手动拨号：手工进行拨号和挂断，点击列表右下方的<拨号>、<挂断>可实现手动拨号；
- 拨号模式：在使用正确的用户名和密码前提下，如果拨号不成功，可尝试使用其它拨号模式；
- 空闲时间：在没有访问 Internet 流量后自动断线前等待的时长，0 代表不自动断

线；

- MTU：最大传输单元，缺省值为 1480 字节，PPPoE 拨号时设备将自动与对方设备协商，除非特别应用，请不要修改。

3、 固定 IP 接入

图 6-3 固定 IP 接入

- IP 地址、子网掩码、网关地址：运营商给您提供的静态 IP 地址、子网掩码、网关地址；
- 主、备 DNS 服务器：运营商给您提供的 DNS 服务器地址。

6.1.2 3G 接入

如图 6-4 所示，下面介绍 3G 接入时相关配置参数的涵义，对于在第 4 章《配置向导》中已经介绍过的参数这里不再一一列出。

图 6-4 3G 接入

提示：

请按 ISP 的要求输入正确的参数，设置保存后，请点击本页面中的刷新按钮。拨号时间为一分钟左右，因 3G 上网卡的型号而定。如果还不能拨号成功，请尝试重新插拔 3G 上网卡或重启设备。

6.1.3 线路连接信息列表

下面分别介绍连接类型分别为动态 IP 接入、固定 IP 接入、PPPoE 接入、3G 接入的线路连接信息列表。

1、 动态 IP 接入

图 6-5 线路连接信息列表——动态 IP 接入

如上图所示，APClient 口为动态 IP 接入。

- 连接类型：为“已连接”时，会显示已连接的时长；
- IP 地址、子网掩码、网关地址：上端设备动态分配的 IP 地址、子网掩码及网关地址；
- 下行速率、上行速率：在两次刷新列表的时间间隔内，当前线路实际的下行、上行平均速率。单位为 KB/s；
- 删除：删除相应的线路；
- 更新：点击<更新>，系统自动完成一次先释放 IP 地址、再重新获得 IP 地址的过程；
- 释放：点击<释放>，释放当前得到的动态 IP 地址；
- 刷新：点击<刷新>，可显示线路连接信息列表的最新信息。

2、 固定 IP 接入

图 6-6 线路连接信息列表——固定 IP 接入

如上图所示，WAN1 口为固定 IP 接入。其 IP 地址、子网掩码、网关地址为配置该 WAN 口时配置的参数。

3、 PPPoE、3G 接入

图 6-7 线路连接信息列表——PPPoE 接入

如果某线路为 PPPoE 拨号或者是 3G 接入线路，那么，在点击该接口后，在“线路连接信息列表”下方才会显示<拨号>和<挂断>，如上图所示，WAN1 口为 PPPoE 接入，点击“WAN1”，线路连接信息列表右下方显示四个按钮。

- 连接状态：处于“已连接”时，会显示该线路保持本次连接的时间；
- IP 地址、子网掩码、网关地址：上连设备分配给接口的 IP 地址、子网掩码、网关地址；
- 删除：删除相应的线路；
- 拨号：点击<拨号>，建立未连接或断开的 PPPoE 接入、3G 接入线路（当 PPPoE 连接拨号类型设置为“手动拨号”时，需在这里完成 PPPoE 拨号）；
- 挂断：点击<挂断>，挂断已建立连接的 PPPoE 拨号线路或者 3G 接入线路；
- 刷新：点击<刷新>，可显示线路连接信息列表的最新信息。

6.2　线路组合

本节介绍***网络参数—>线路组合***页面。

在线路组合配置中，可以快速配置线路组合方式及其他相关参数，可以指定线路的线路检测间隔、检测次数、检测目标 IP 地址和带宽。

6.2.1 线路组合功能介绍

1、 线路检测机制

无论采用哪种线路组合方式，要保证线路故障时网络不中断，都要求设备必须能够实时地监控线路状态。为此，我们为设备设计了灵活的自动检测机制，并提供多种线路检测方法供用户选择，以满足实际应用的需要。

为方便理解，先介绍一下几个相关参数。

检测间隔：发送检测包的时间间隔，一次发送一个检测包，缺省值为 0 秒。特别地，该值为 0 时，表示不进行线路检测。

检测次数：每个检测周期内，发送检测包的次数。

目标 IP 地址：检测的对象，设备将向预先指定的检测目标发送检测包以检测线路是否正常。

下面将分别介绍在线路正常和线路故障这两种情况下，设备的线路检测机制。

某条线路故障时，检测机制如下所述：设备将每隔指定的检测间隔向该线路的检测目标发送一个检测包，如果在某个检测周期内，发送的所有检测包都没有回应，就认为该线路出现故障，并立即屏蔽该线路。例如，缺省情况下，若某个检测周期内，发送的 3 个检测包都没有回应，就认为该线路出现故障。

某条线路正常时，检测机制如下所述：同样地，设备也是每隔指定的检测间隔向该线路的检测目标发送一个检测包，如果在某个检测周期内，发送的检测包中有一半及以上数量的检测包有回应时，就认为该线路已经正常，并恢复启用该线路。例如，缺省情况下，若某个检测周期内，有 2 个检测包有回应，就认为该线路恢复正常。

设备允许用户预先为内网中的某些主机指定上网线路，它是通过设置线路的“内部起始 IP 地址”和“内部结束 IP 地址”来实现的，IP 地址属于两个地址范围内的主机将优先使用指定线路。对于已指定上网线路的主机来说，当指定线路正常时，它们只能通过该线路上网；但是，当指定线路有故障时，它们会使用其他的正常线路上网。

提示：

允许不启用线路检测，这时需要将“检测间隔”设为“0”秒。

2、 线路组合方式

设备提供了 2 个线路组：“主线路”组和“备份线路”组。为方便起见，将“主线路”组中的线路统称为主线路，将“备份线路”组中的线路统称为备份线路。所有线路缺省都是主线路，用户可以根据需要将某些线路划分到“备份线路”组中。

设备提供了“所有线路负载均衡”和“部分线路负载均衡，其余备份”这两种线路组合方式。

在“所有线路负载均衡”方式下，所有线路都作为主线路使用。工作原理如下：

1. 当所有线路都正常时，内网主机将同时使用所有线路上网。
2. 若某条线路出现故障，则立即屏蔽该线路，原先通过该线路的流量将分配到其他线路上。
3. 一旦故障线路恢复正常，设备会自动启用该线路，流量自动重新分配。

在“部分线路负载均衡，其余备份”方式下，一部分线路作为主线路使用，另一部分线路则作为备份线路使用。工作原理如下：

1. 只要主线路正常，内网主机就使用主线路上网；
2. 若主线路出现故障，则自动切换到使用备份线路上网；
3. 一旦故障主线路恢复正常，则立即切换回主线路。

提示：

当某条线路中断进行线路切换时，某些用户应用（比如部分网络游戏）可能会意外中断，这是由于 TCP 会话的属性决定的。

6.2.2 线路组合全局配置

由于“所有线路负载均衡”和“部分线路负载均衡，其余备份”这两种线路组合方式下，全局设置的界面不同，因此，以下将分别介绍它们的通用设置参数。

2、 所有线路负载均衡

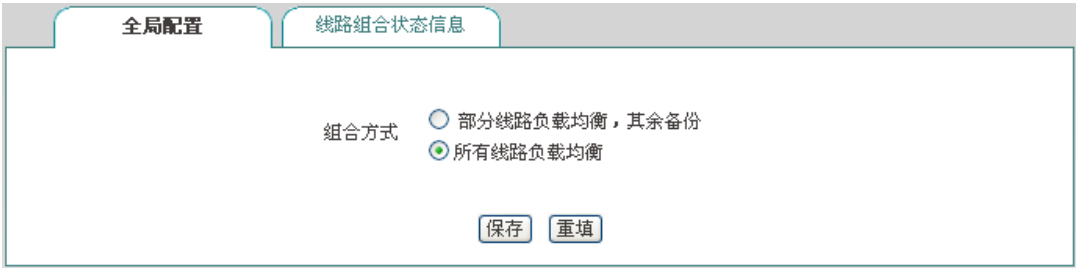

图 6-8 所有线路负载均衡

- 线路组合方式：这里选中“所有线路负载均衡”；
- 保存：线路组合配置参数生效；
- 重填：恢复到修改前的配置参数。

提示：线路组合方式默认为“所有线路负载均衡”。

3、 部分线路负载均衡，其余备份

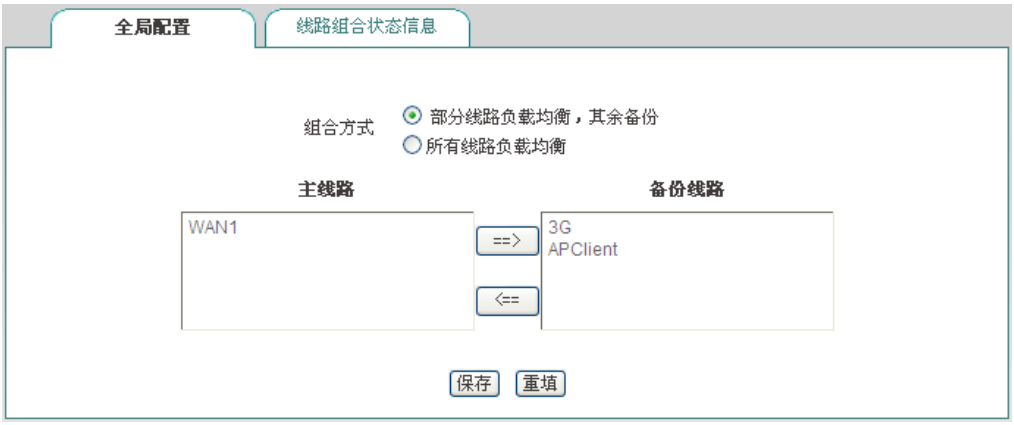

图 6-9 部分线路负载均衡，其余备份

- 线路组合方式：这里选中“部分线路负载均衡，其余备份”；
- 主线路：该列表框代表“主线路”组，位于该列表框中的线路全部都作为主线路使用；
- 备份线路：该列表框中代表“备份线路”组，位于该列表框中的线路全部都作为备份线路使用。
- ==>（向右箭头）、<==（向左箭头）：首先在“主线路”列表框中选中一条（或更多）线路，然后单击“==>”，被选中的线路立即被移到“备份线路”列表框中。类似地，首先在“备份线路”列表框中选中一条（或更多）线路，然后单击“<==”，被选中的立即被移到“主线路”列表框中。

- 保存：线路组合配置参数生效；
- 重填：恢复到修改前的配置参数。

6.2.3 线路组合状态信息

1、 线路状态组合信息列表

图 6-10 线路状态组合信息列表

- 编辑线路组合状态信息：单击该线路的接口或者该线路对应的“编辑”超链接，即可跳转到相关页面进行修改，如图 6-11 所示；
- 刷新：点击<刷新>，可获得最新的线路组合状态信息。

2、 线路组合配置

当配置完线路组合功能后，还需要对各线路的检测机制进行配置，配置方法如下。

进入***网络参数—>线路组合—>线路组合状态信息***页面，单击某线路的接口或者是编辑图标，进入***线路检测配置***页面。

图 6-11 线路组合配置

- 检测间隔：发送检测包的时间间隔，单位：秒。启用线路检测时，取值范围为 1～60，该值为 0 时，表示不启用线路检测；

- 检测次数：检测周期内发送检测包的次数（每次发送一个检测包）。缺省值为 0；
- 检测目标 IP 地址：欲检测的目标的 IP 地址；
- 带宽：设置 ISP 提供给当前线路的带宽；
- 内部起始、内部结束 IP 地址：内网内优先使用当前线路上网的主机的地址范围；
- 保存：上述配置参数生效；
- 重填：恢复到修改前的配置参数；
- 返回：返回到线路组合状态信息页面。

6.3　LAN 口配置

设备默认 LAN 口的 IP 地址为 192.168.1.1，如果您需要修改 LAN 口的 IP 地址以适应现有的网络环境，请进入***网络参数—>LAN 口配置***页面修改 LAN 口参数。

图 6-12 LAN 口配置

- IP 地址：设备内网的 IP 地址；
- 子网掩码：设备内网 IP 地址的子网掩码；
- MAC 地址：LAN 口的 MAC 地址。建议不要随意修改 LAN 口的 MAC 地址。

提示：

修改过 LAN 口 IP 地址后，必须使用新的 IP 地址登录设备，且登录主机的 IP 要和其在同一网段！

6.4　DHCP 服务器

本节介绍***网络参数—>DHCP 服务器***页面，包括 DHCP 服务器设置、静态 DHCP 和 DHCP 客户列表。

6.4.1 DHCP 服务器配置

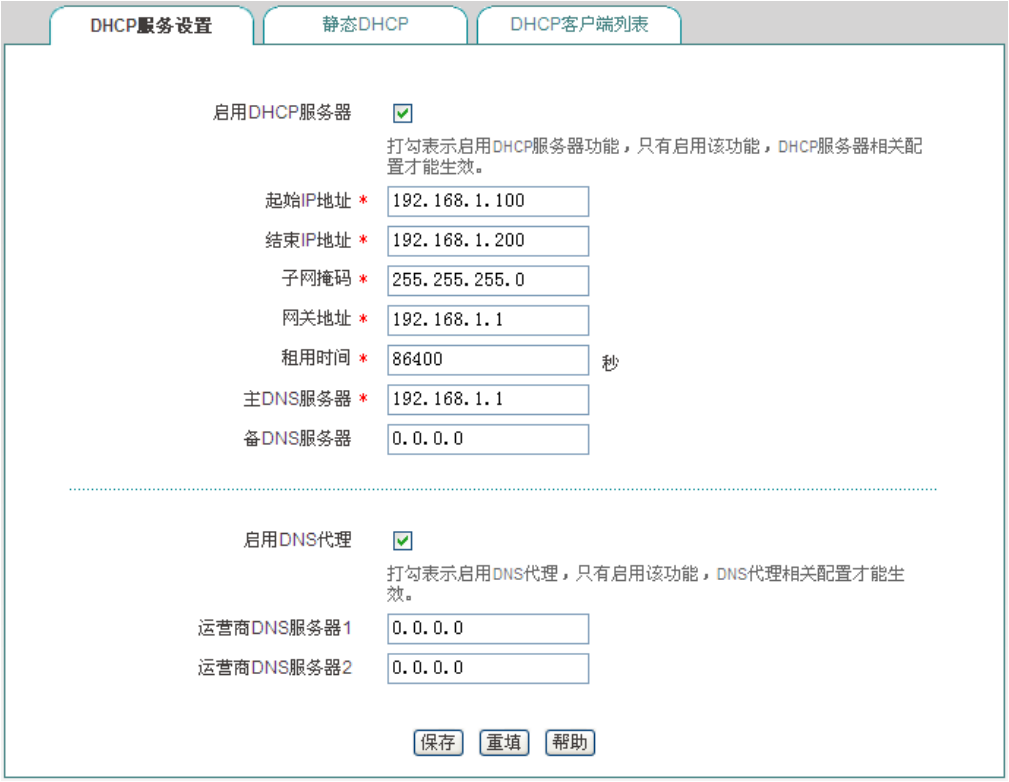

图 6-13 DHCP 服务配置

- 启用 DHCP 服务器：用来禁用或允许设备的 DHCP 服务器功能。选中为允许；
- 起始、结束 IP 地址：DHCP 服务器给内网计算机自动分配的 IP 地址段（应与设备 LAN 口的 IP 地址在一个网段）；
- 子网掩码：DHCP 服务器给内网计算机自动分配的子网掩码（应与设备 LAN 口的子网掩码一致）；
- 网关地址：DHCP 服务器给内网计算机自动分配的网关 IP 地址（应与设备 LAN 口的 IP 地址一致）；
- 租用时间：内网计算机获得设备分配的 IP 地址的租用时间（单位：秒）；
- 主 DNS 服务器：DHCP 服务器给内网计算机自动分配的主 DNS 服务器 IP 地址；
- 备 DNS 服务器：DHCP 服务器给内网计算机自动分配的备 DNS 服务器 IP 地址；
- 启用 DNS 代理：选中表示启用，启用后设备的 DNS 代理功能才会生效，启用此功能后将网关地址分配给客户端作为主、备 DNS 服务器；
- 运营商 DNS 服务器 1、2：运营商 DNS 服务器的 IP 地址。

提示：

1、 如果要使用设备的 DHCP 服务器功能，内网计算机的 TCP/IP 协议可设置为“自动获得 IP 地址”；

2、 如果用户原先使用的是代理服务器软件（如 wingate），且计算机的 DNS 服务器设置为代理服务器的 IP 地址，那么，只需将设备的 LAN 口的 IP 地址设置为同一个 IP 地址，这样，当设备启用 DNS 代理功能之后，用户不需要修改计算机的配置就可以转换到使用设备的 DNS 代理功能了。

6.4.2 静态 DHCP

本节介绍静态 DHCP 列表及如何配置静态 DHCP。

使用 DHCP 服务为内网中的计算机自动配置 TCP/IP 属性是非常方便的，但是会造成一台计算机不同时间被分配到不同 IP 地址的现象。而某些内网计算机可能需要固定的 IP 地址，这时就需要使用静态 DHCP 功能，将计算机的 MAC 地址与某个 IP 地址绑定，如图 6-14 所示。当具有此 MAC 地址的计算机向 DHCP 服务器（设备）申请地址时，设备将根据其 MAC 地址寻找到对应的固定 IP 地址分配给该计算机。

1、 静态 DHCP 列表

图 6-14 静态 DHCP 列表

2、 静态 DHCP 配置

在图 6-14 所示的页面点击<添加新条目>，进入如下图所示的***静态 DHCP 配置***页面。下面介绍配置静态 DHCP 时各参数的涵义。

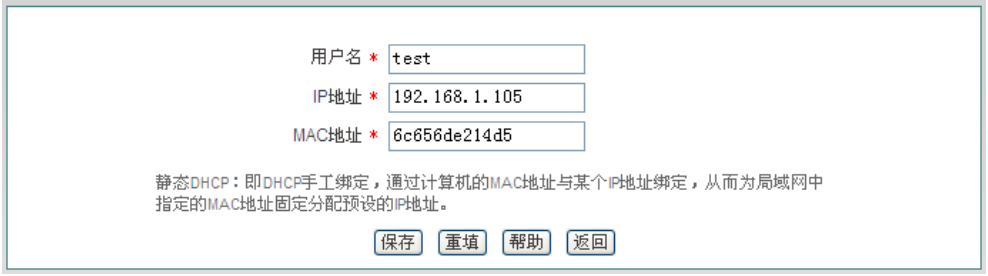

图 6-15 静态 DHCP 配置

- 用户名：配置该 DHCP 绑定的计算机的用户名（自定义，不能重复）；
- IP 地址：预留的 IP 地址，必须是 DHCP 服务器指定的地址范围内的合法 IP 地址；

- MAC 地址：固定使用该预留 IP 地址的计算机的 MAC 地址。

提示：

1、 设置成功后，设备将为指定计算机固定分配预设的 IP 地址；

2、 配置的 IP 地址要在 DHCP 服务器提供的范围之内。

6.4.3 DHCP 客户端列表

对于已分配给内网计算机的 IP 地址，可以在 DHCP 客户端列表中查看到相关信息。如下图中的信息表示：DHCP 服务器将地址池中的 192.168.1.100 的 IP 地址分配给 MAC 地址为 6C:62:6D:E9:6D:13 的内网计算机，该计算机租用该 IP 地址剩余的时间为 85954 秒。

图 6-16 DHCP 客户端列表

6.4.4 DHCP 配置实例

应用需求

本实例中，要求设备开启 DHCP 功能，起始地址为 192.168.1.10，共可分配 100 个地址；其中 MAC 地址为 00:21:85:9B:45:46 的主机分配 192.168.1.15 的固定 IP 地址，MAC 地址为 00:1f:3c:0f:07:f4 分配 192.168.1.10 的固定 IP 地址。

配置步骤

第一步，进入***网络参数—>DHCP 服务器—> DHCP 服务设置***页面；

第二步，启用 DHCP 功能，并配置相关 DHCP 服务参数，（如图 6-17 所示），配置完后点击<保存>。

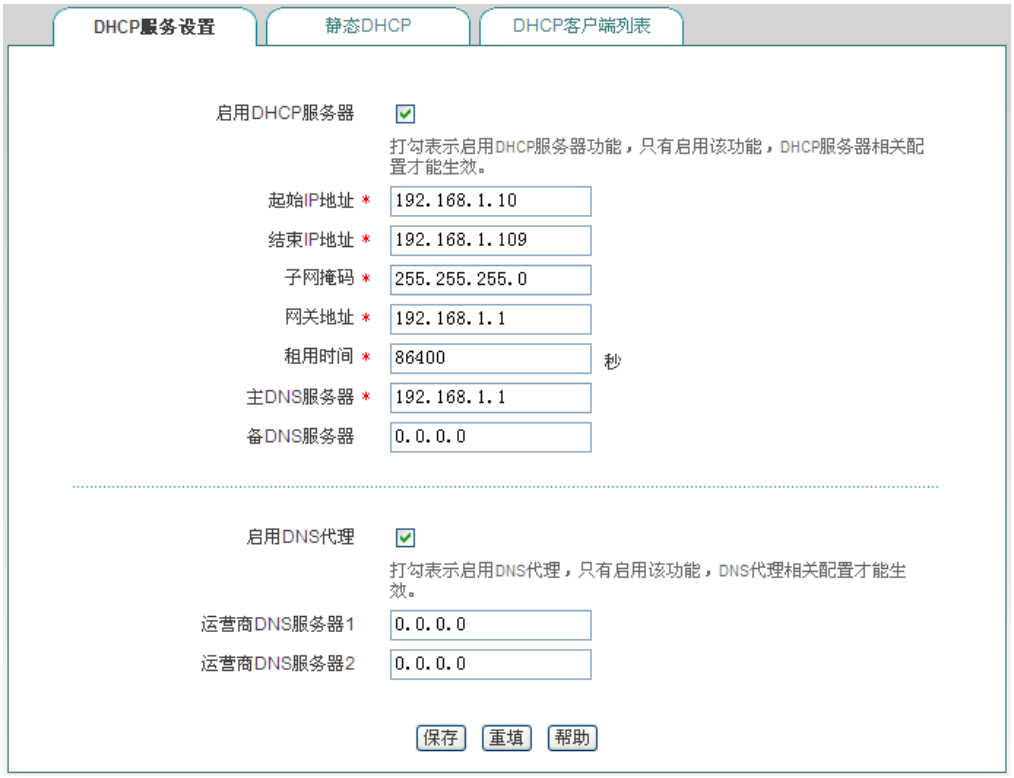

图 6-17 DHCP 服务设置——实例

第三步，进入***网络参数—>DHCP 服务器—>静态 DHCP*** 页面，点击<添加新条目>，配置需求中的两条静态 DHCP 实例（如图 6-18、图 6-19）；

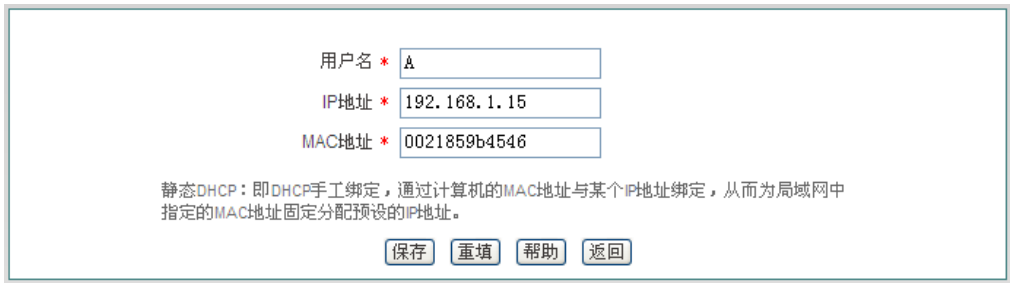

图 6-18 静态 DHCP 配置——实例 A

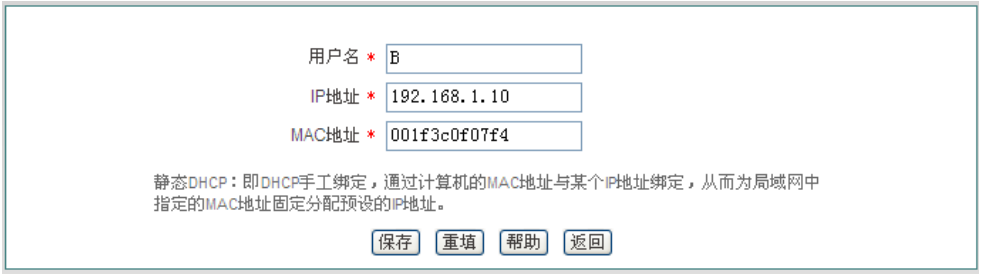

图 6-19 静态 DHCP 配置——实例 B

至此配置完成，可以在“静态 DHCP 信息列表”中查看这 2 个静态 DHCP 条目的相关信息，如图 6-20 所示。如果发现配置错误，可以直接单击对应条目的 图标，进入***静态 DHCP 配置***页面中进行修改并保存。

图 6-20 静态 DHCP 信息列表——实例

6.5 DDNS 配置

本节介绍***网络参数—>DDNS 配置***页面及配置方法。包括：申请 DDNS 账号、配置 DDNS 服务、DDNS 验证。

动态域名解析服务（DDNS）是将一个固定的域名解析成动态变化的 IP 地址（如 ADSL 拨号上网）的一种服务。需向 DDNS 服务提供商申请这项服务，DDNS 的具体服务由各服务商根据实际情况提供。各 DDNS 服务提供商保留随时变更、中断或终止部分或全部网络服务的权利。目前，DDNS 服务是免费的，DDNS 服务提供商在提供网络服务时，可能会对使用 DDNS 服务收取一定的费用。在此情况下，艾泰科技会尽可能及时通知。如拒绝支付该等费用，则不能使用相关的服务。在免费阶段，艾泰科技不担保 DDNS 服务一定能满足要求，也不担保网络服务不会中断，对网络服务的及时性、安全性、准确性也都不作担保。

目前，设备支持 3322.org 和 iplink.com.cn 的 DDNS 服务，将来还将陆续提供对其他 DDNS 服务的支持。

6.5.1 iplink 的 DDNS 服务

1、 申请 iplink.com.cn 的 DDNS 账号

请登录 http://www.utt.com.cn/ddns 申请后缀为 iplink.com.cn 的二级域名。

图 6-21 注册 iplink.com.cn 动态域名

- 主机名：填入欲申请的二级域名（为避免重复，请填写设备底板上的全球唯一序列号 S/N）；

- 注册号/序列号：产品序列号。它和设备的***高级配置—>DDNS 配置***中的“注册号”必须一致；
- 域名用途：选择您创建此域名的用途；
- 保存：点击<保存>，即可获得设备匹配该二级域名的 enkey（请妥善保管此密码）。

图 6-22 iplink 动态域名列表

2、 iplink.com.cn 的 DDNS 配置

图 6-23　配置 DDNS——iplink.com.cn

- 服务商：DDNS 服务的提供商，这里选择 iplink.com.cn；
- 注册域名：点击 http://www.utt.com.cn/ddns 超链接，即可进入该页面申请域名；
- 主机名：注册 DDNS 时填写的主机名；
- 密钥：用户注册时生成的密钥，如图 6-22 中的“密钥（enkey）”；
- 接口：选择绑定 DDNS 服务的接口。

6.5.2 3322 的 DDNS 服务

1、 申请 3322.org 的 DDNS 账号

请登录 http://www.3322.org 申请后缀名为 3322.org 的二级域名。

图 6-24　注册 3322.org 动态域名

- 主机名：填入欲申请的二级域名，不能与已注册的域名重复；
- IP 地址：当前域名对应的 IP 地址，即设备 WAN 口 IP 地址；
- 创建动态域名：点击<创建动态域名>，成功注册域名。

2、 3322.org 的 DDNS 配置

图 6-25　配置 DDNS——3322.org

- 服务商：提供 DDNS 服务的运营商，这里选择 3322.org；

- 注册域名：单击超链接 http://www.3322.org 即可进入 3322 域名申请页面；
- 主机名：使用 DDNS 服务的主机的名称，为避免重复，建议使用设备的底板上的全球唯一序列号 S/N 申请；
- 用户名：申请 DDNS 帐号时使用的用户名；
- 密码：用户注册 DDNS 时使用的密码；
- 接口：选择 DDNS 服务绑定的接口。

提示：WAN 地址必须为公网地址才能将路由器的地址映射到域名。

6.5.3 DDNS 验证

可以在内网计算机的 DOS 状态下，使用 Ping 命令（例如：ping avery12345.3322.org）检查 DDNS 是否更新成功。看到正确解析出 IP 地址（例如：58.246.187.126），证明域名解析正确。注意：一般情况下，设备在使用 NAT 后，从 Internet 上将不能 ping 通设备的 IP 地址，只能解析出该域名对应的 IP 地址。

```
Pinging avery12345.3322.org [58.246.187.126] with 32 bytes of data:

Reply from 58.246.187.126: bytes=32 time=1ms TTL=63
Reply from 58.246.187.126: bytes=32 time=1ms TTL=63
Reply from 58.246.187.126: bytes=32 time=1ms TTL=63
Reply from 58.246.187.126: bytes=32 time=1ms TTL=63

Ping statistics for 58.246.187.126:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

1、 ISP（例如中国电信）分配给 WAN 口连接线路的 IP 地址是公网地址的时候才能保证该域名能被 Internet 的用户访问；

2、 DDNS 功能可以帮助动态 IP 使用 VPN 和服务器映射。

6.6 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。使用 UPnP 意味着简单、更多选择和更新颖的体验。支持通用即插即用技术的网络产品只需实际连到网络上，即可开始正常工作。

本节介绍***网络参数—>UPnP*** 页面及配置。

图 6-26 UPnP 配置

在本页面中配置 UPnP 时，只需启用或禁用该功能即可。

- 启用 UPnP：勾选复选框表示启用 UPnP 功能；
- 内部地址：内网需要进行端口转换的主机 IP 地址；
- 内部端口：内网需要进行端口转换的主机提供的端口号；
- 协议：该 UPnP 端口转换使用的协议（TCP/UDP）；
- 对端地址：对端主机的 IP 地址；
- 对端端口：端口转换使用的设备的端口号，此端口是设备提供给 Internet 的服务端口；
- 描述：应用程序通过 UPnP 向设备请求端口转换时给出的描述信息。

提示：建议在不使用该功能时，不要启用 UPnP 功能。

第7章 无线配置

在无线配置中，主要设置设备相关无线功能及参数，包括：无线基本参数，无线安全机制设置，无线 MAC 地址过滤以及无线高级参数。此外，还可以查看无线主机的状态信息。

7.1 基本配置

本节讲述***无线配置—>基本设置***页面及配置方法。在本页面，您可以配置设备的 AP 的工作模式、SSID、无线模式、信道、频道带宽、启用或禁用 SSID 广播等功能。本节按 AP 工作模式：AP Mode、APClient Mode 和 WDS 的顺序进行介绍无线的基本配置。

7.1.1 AP Mode

图 7-1 AP Mode 模式

- 启用无线功能：只有启用无线功能后，无线客户端才能连接到设备，从而通过设备进行无线通信，接入并访问设备连接的有线网络；
- AP 工作模式：此处选择 AP Mode，即纯 AP 模式，在此模式下，对端设备可以是 AP Client 模式以及单客户端；
- SSID：SSID（Service Set Identification，服务集标识）用于唯一地标识一个无线网络的字符串，区分大小写；
- 无线模式：此参数用于设置无线设备的模式，提供仅 11g，仅 11n 和 11b/g/n 混合三个选项：

- 仅 11g：即纯 802.11g 模式，本模式下，最大速率 54M bps。兼容 IEEE 802.11g 标准的无线站点可以接入设备；
- 仅 11n：即纯 802.11n 模式，本模式下，最大速率为 150M bps。只有符合 IEEE 802.11n 标准的无线站点可以接入设备；
- 11b/g/n 混合：符合 IEEE 802.11b、802.11g 或者 802.11n 标准的无线站点将各自按照自己的模式接入，最大速率分别为 11M bps、54M bps 和 150M bps；

◆ 信道：此参数用于选择无线网络工作的频率段，可以选择的范围从 1 到 11，另外提供自动选项，表示设备可以自动选择最优频率段。如果存在多个无线设备时，要注意各个设备的频段设置不能相互影响；

◆ 频道带宽：设置无线数据传输时所占用的频道带宽，可选项为：20M/40M 和 20M。注意，本参数仅对采用 802.11n 标准接入的无线站点起作用；对于以 802.11b 或者 802.11g 标准的无线站点来说，只能使用 20M 的频道带宽：

- 20M/40M：选择 20M/40M 时，表示使用 802.11n 接入的无线站点将根据很接入对端协商的结果选择使用 20M 或 40M 的频道带宽；
- 20M：选择 20M 时，表示使用 802.11n 接入的无线站点将使用 20M 的频道带宽。

◆ SSID 广播：启用或禁用 SSID 广播功能。如果开启此功能，那么，设备将会把自己的 SSID 广播给所有的无线站点，这样，没有 SSID（为空值）的无线站点将获得正确的 SSID，从而连接到设备，并加入到该 SSID 标识的无线网络。由于开启此功能存在安全风险（非法站点很容易获得 SSID 信息），一般建议禁用此功能。

提示：

1、 设备默认开启无线功能，且工作模式为 AP Mode；

2、 无线参数修改后，设备的无线模块将会重启，无线模块重启会断开所有的无线连接；

3、 AP 的各种工作模式功能各不相同，配置时请根据场合、使用需要自行选择。

7.1.2 APClient Mode

图 7-2 APClient Mode 模式

AP 的工作模式：这里选择“APClient Mode”；

- SSID、无线模式、信道、频道带宽、SSID 广播：参数详细介绍见章节 7.1.1《AP Mode》；
- AP 的 SSID、AP 的 MAC 地址：对端 AP 的 SSID 号、MAC 地址，参数详细介绍见章节 4.4《无线客户端配置》；
- 安全模式：这里选择“无安全机制”，注意要与对端设备安全机制保持一致。

提示：

1、 在 APClient Mode 模式下：安全模式和信道都要和对端保持一致，否则不能实现连通；

2、 安全模式中共有：无安全机制、WEP、WPA-PSK/WPA2-PSK 三个选项。其中，WEP 的配置详见章节 7.2《无线安全设置》。

WDS (Wireless Distribution System)无线分布式系统，是无线连接两个接入点（AP）的协议。在整个 WDS 无线网络中，把多个 AP 通过桥接或中继器的方式连接起来，使整个局域网络以无线的方式为主。

本设备提供的 WDS 配置包括：Bridge Mode、Repeater Mode、Lazy Mode 三部分，在实际应用中仅起桥接功能，配置时要注意，各设备的 LAN 口 IP 要在同一网段中，同时连接双方的安全模式和信道带宽等参数都要保持一致。

7.1.3 Repeater Mode

当设备的工作模式配置为 Repeater Mode 时，可与处于 Bridge Mode、Repeater Mode、Lazy Mode 模式的网络设备以及单客户端进行数据交换，实现网络连通。

图 7-3 Repeater Mode 模式

启用无线功能、AP 工作模式、SSID、无线模式、信道、频道带宽、启用 SSID 广播的含义见章节 7.1.1《AP Mode》相关解释，在后续配置中若遇到上述术语也不再赘述；

- AP 的 MAC 地址：对端设备的 MAC 地址；
- 安全模式：设备通过 WDS 功能建立连接的时候采用的加密方式，包括“无安全机制”、“WEP”、“TKIP”、“AES”四个选项。
  - 无安全机制：表示在数据交换过程中不采用任何加密算法保护通信数据；
  - WEP：表示在数据交换过程中采用 WEP 加密算法保护通信数据，具体介绍见 7.2.1《WEP》；
  - TKIP：表示在数据交换过程中采用 TKIP 加密算法保护通信数据，具体介绍见 7.2.3《WPA-PSK/WPA2-PSK》；
  - AES：表示在数据交换过程中采用 AES 加密算法保护通信数据，具体介绍见 7.2.3《WPA-PSK/WPA2-PSK》。

7.1.4 Bridge Mode

Bridge Mode，该模式下，设备连接两个或者多个有线网络，且设备不会再发送无线信号给其它客户端接收，可与处于 Bridge Mode 、Repeater Mode、Lazy Mode 模式的网络设备交换数据。

图 7-4 Bridge Mode 模式

相关配置参数含义同 Repeater Mode，详见章节 7.1.3《Repeater Mode》中的相关描述。

7.1.5 Lazy Mode

当设备的工作模式为 Lazy Mode 时，设备可与处于 Repeater Mode、Bridge Mode 模式及单客户端的网络设备交换数据、实现网络连通。

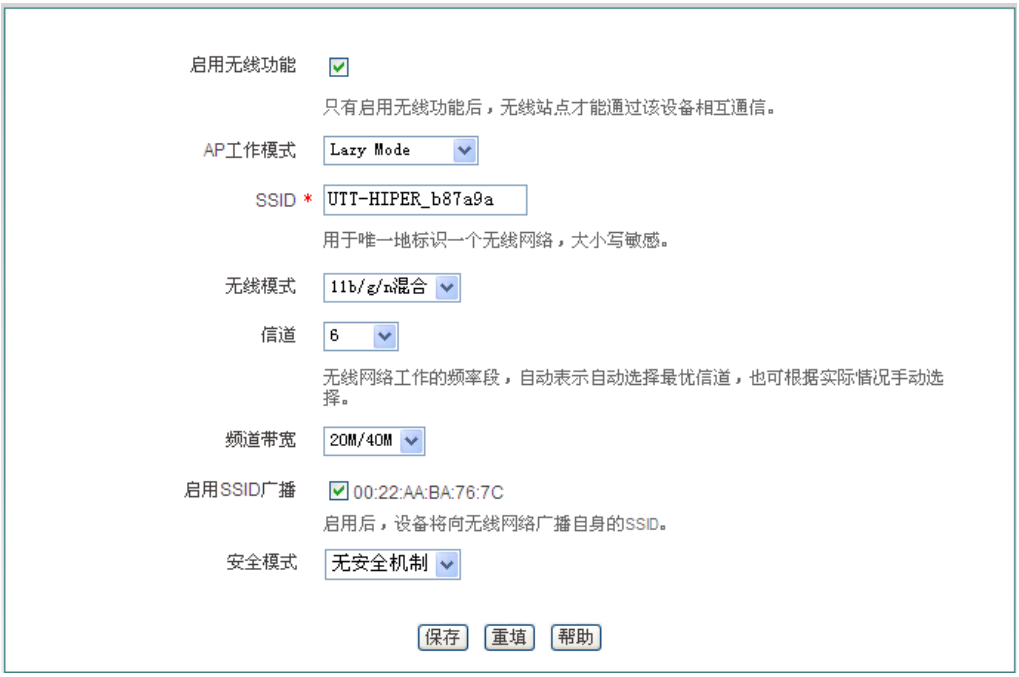

图 7-5 Lazy Mode 模式

相关配置参数含义同 AP Mode 与 Repeater Mode，详见章节 7.1.1《AP Mode》与 7.1.3《Repeater Mode》中的相关描述。

7.1.6 无线配置实例

本节根据设备的五种 AP 工作模式，列举设备作为 AP Mode、AP Client Mode 及其他 AP 工作模式的配置实例。

一、 AP Mode 配置实例

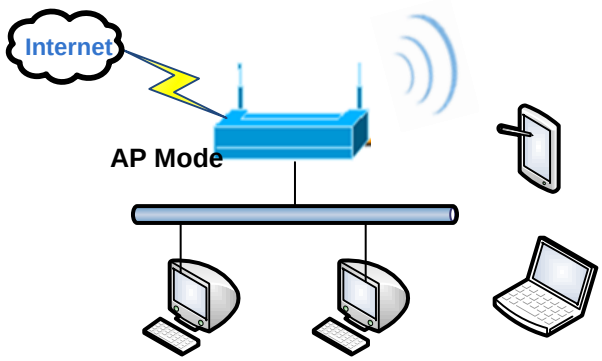

图 7-6 AP Mode 组网环境

1、 需求：某家庭用户希望让家里的台式电脑、笔记本、平板电脑、智能手机通过无线设备上网，防止除家庭用户外的其他用户接入无线设备。

2、 分析：台式电脑通过网线连接到无线设备的 LAN 口；笔记本、平板电脑等通过无线接入无线设备，并需要通过认证。

3、 配置步骤：

1) 配置内网计算机的 TCP/IP 属性；

2) 登录设备，根据在运营商申请的业务类型配置设备的 WAN1 口；

3) 进入***无线配置—>基本配置***页面，配置设备的无线基本参数，如下图所示，AP 工作模式设置为：AP Mode。

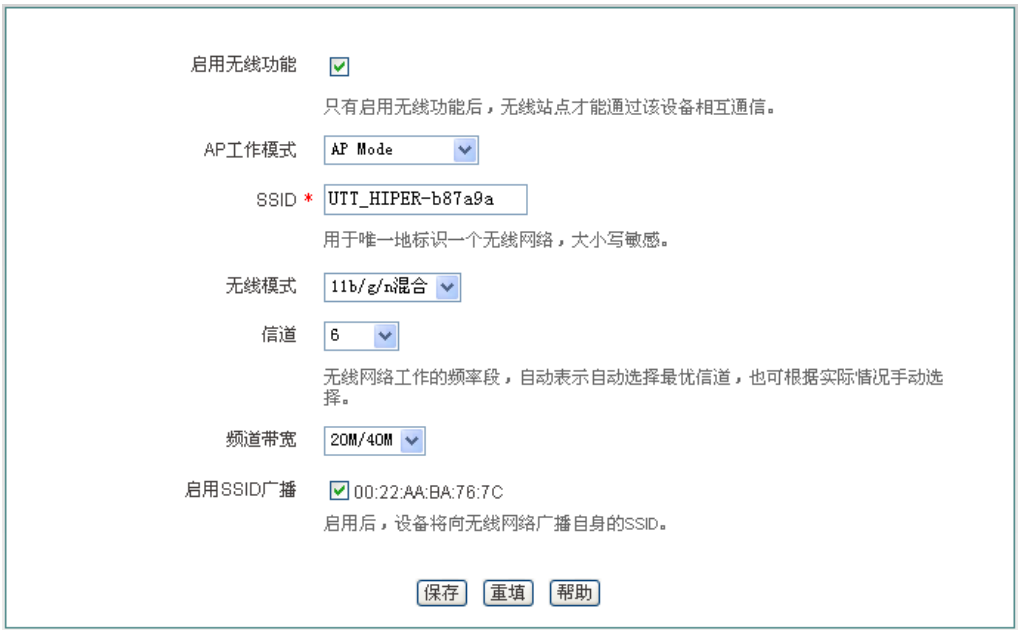

图 7-7 AP Mode 配置

4) 进入***无线配置—>无线安全设置***页面，配置无线通信的验证方式及密钥。

通过以上配置，无线用户通过验证就可以连接到无线设备，并通过其访问 Internet。内网计算机如何连接到设备请参考附录 A。

二、 AP Client Mode 配置实例

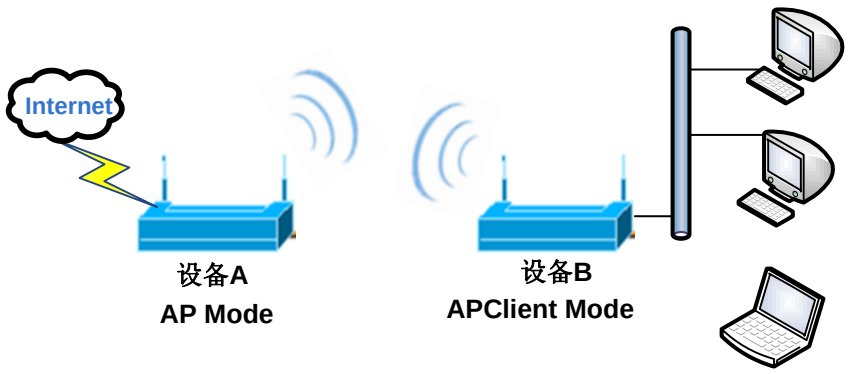

图 7-8 AP Client Mode 组网环境

1、 需求：某企业新扩展出一办公区，因其不好布线，故采用无线设备作为无线客户端连接到出口网关（AP Mode）。

设备 A 开启 DHCP 功能，无线相关参数如下：

项目	参数	项目	参数
SSID	UTT-HIPER-b87a9a	MAC	0022AABA767C
无线模式	11b/g/n 混合	信道	6
安全模式	WPA-PSK/WAP2-PSK	预共享密钥	123456789
加密算法	自动	WPA 版本	自动

表 7-1 AP Mode 相关参数表

2、 配置步骤：

1) 配置设备 A 可参考 AP Mode 配置实例；

2) 登录设备 B；

3) 进入***无线配置—>基本配置***页面，设置 AP 工作模式为 AP Client Mode，如下图所示；

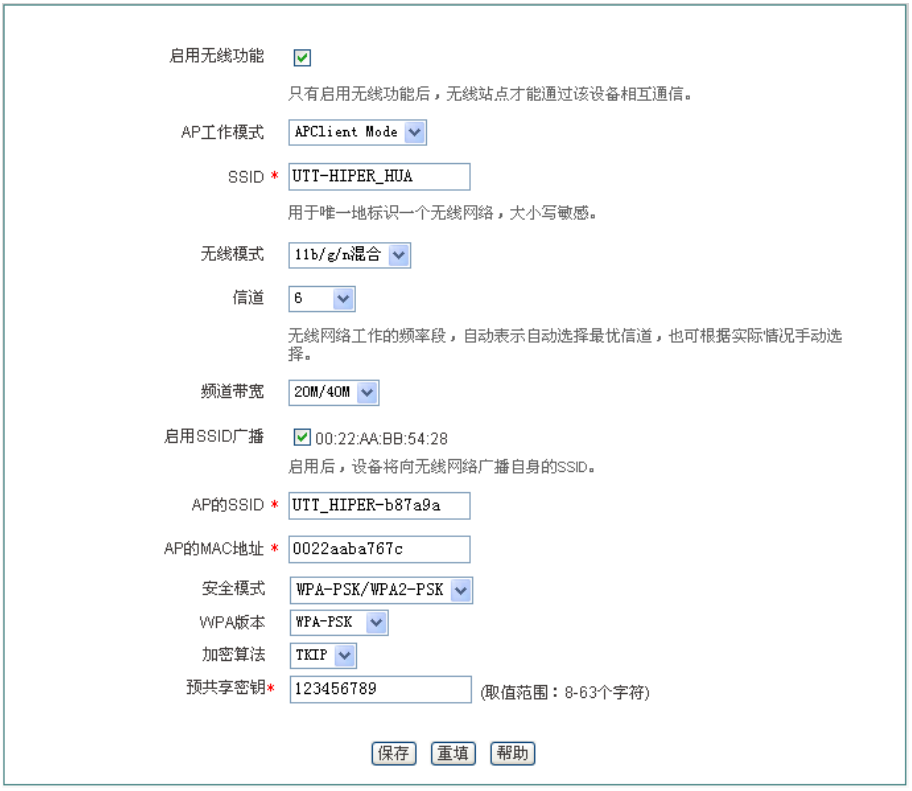

图 7-9 AP Client Mode 配置

4) 进入***网络参数—>WAN 口配置***页面，配置设备接口为“AP Client”的接入方式为动态 IP 接入。

设备 B 中的线路连接信息列表中的 AP Client 接口获得 IP 地址，连接成功后表明设备 B 与设备 A 无线连接已经建立。

三、 WDS 配置实例

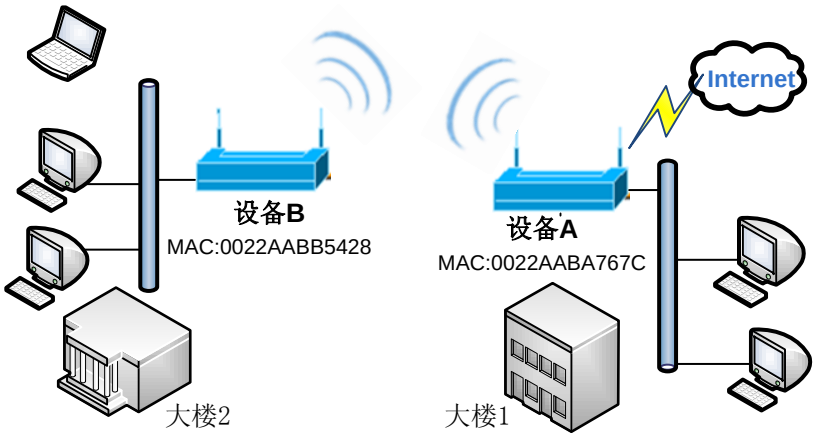

图 7-10 Repeater Mode 组网环境

1、 需求：大楼 2 中的办公人员需无线接入到设备 A（出口网关），并通过设备 A 访问 Internet。

2、 分析：可通过以下方案来实现

方案一：设备 A、B 都设置为 Repeater Mode 模式。

方案二：设备 A、B 都设置为 Bridge Mode 模式。

方案三：设备 A、B 分别设置为 Repeater Mode、Bridge Mode 模式。

方案四：设备 A、B 分别设置为 Repeater Mode、Lazy Mode 模式。

方案五：设备 A、B 分别设置为 Bridge Mode、Lazy Mode 模式。

方案六：设备 A 设置为 AP Mode 模式，设备 B 设置为 AP Client Mode 模式。

3、 配置步骤：

方案一：都为 Repeater Mode

1) 配置设备 A 的 AP 工作模式为 Repeater Mode，配置内容如下图所示：

图 7-11 Repeater Mode 实例

2) 配置设备 B 的 AP 工作模式为 Repeater Mode，SSID、无线模式、信道、频道带宽、安全模式、预共享密钥同设备 A 的配置，AP 的 MAC 地址设置为：0022AABA767C（设备 A 的 MAC 地址）；

通过以上配置，大楼 1 中的办公人员可以通过设备 2 访问 Internet。

提示：

1、 大楼 2 中的计算机的网关指向设备 A 的 LAN 口；

2、 设备 B 的 LAN 口 IP 地址与设备 A 的 LAN 口地址在同一网段。

4、 连通性验证：

在大楼 2 中的一台计算机上 ping 设备 A 的 LAN 口 IP 地址，如果能 ping 通，则表明两台无线设备已经建立无线连接。

方案二、三、四、五都可参考方案一。

提示：

1、 Bridge Mode 模式下的设备不能接无线单客户端，如笔记本、智能手机等；

2、 Lazy Mode 模式下的设备能接无线单客户端；

3、 在配置时，需注意设备 A、B 的 SSID、密钥等必须一致，AP 的 MAC 地址为对端

设备的 MAC 地址（AP 工作模式为 Lazy Mode 时不需配置对端设备的 MAC 地址）；

4、 设备 A、B 必须在同一网段，并且内网所有计算机的网关地址指向设备 B。

7.2 无线安全设置

本节介绍***无线配置—>无线安全设置***的界面及配置方法，本设备提供 WEP、WPA/WPA2、WPA-PSK/WPA2-PSK 三种无线安全机制，同时，也允许用户不使用安全机制，以下各节将分别介绍它们的配置参数的含义。

7.2.1 WEP

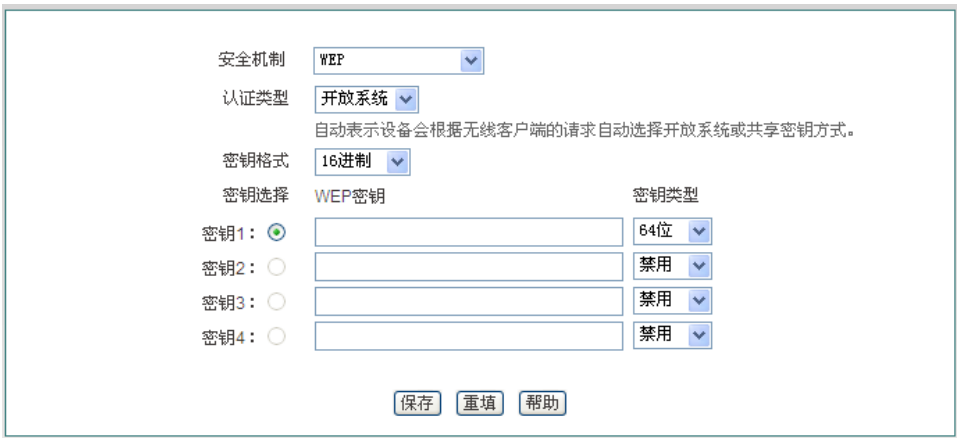

图 7-12 WEP

- 安全机制：此处选择“WEP”，表示本设备将使用 802.11 协议提供的最基本的 WEP 安全机制；
- 认证类型：使用 WEP 加密机制时，提供自动、开放系统、共享密钥 3 个选项：
  - 自动：表示设备会根据无线客户端的请求自动选择开放系统或共享密钥方 式；
  - 开放系统：此时，无线客户端主机在不提供认证密钥的前提下，通过认证并关联到无线设备；但若要进行数据传输，必须提供正确的密钥；
  - 共享密钥：此时，无线客户端主机必须提供正确的密钥才能通过认证，否则无法关联到无线设备，从而无法进行数据传输；
- 密钥格式：提供 16 进制、ASCII 码两种格式：
  - 采用 16 进制时，密钥字符可以为 0~9，A、B、C、D、E、F；
  - 采用 ASCII 码时，密钥字符可以是所有的 ASCII 码；
- 密钥选择：用户可根据需要输入 1~4 个密钥，这 4 个密钥可以采用不同的密钥类型；
- WEP 密钥：用于设置密钥值，密钥的长度受密钥类型的影响：
  - 选择 64 位密钥时，输入 16 进制字符 10 个或者 ASCII 码字符 5 个；
  - 选择 128 位密钥时，输入 16 进制字符 26 个或者 ASCII 码字符 13 个；

- 密钥类型：用于选择密钥类型，提供禁用、64 位、128 位、3 个选项。其中，禁用表示不使用当前密钥，而 64 位、128 位、则用于指定 WEP 密钥的长度。

7.2.2 WPA/WPA2

图 7-13 WPA/WPA2

- 安全机制：此处选择“WPA/WPA2”，表示本设备将采用 WPA 或 WPA2 安全机制。此安全机制下，本设备将采用 Radius 服务器进行身份认证并得到密钥；
- WPA 版本：用来设置本设备将使用的安全模式：
  - 自动：表示本设备会根据无线客户端的请求自动选择 WPA 或者 WPA2 安全模式；
  - WPA：表示本设备将采用 WPA 的安全模式；
  - WPA2：表示本设备将采用 WPA2 的安全模式；
- 加密算法：用来选择对无线数据进行加密的安全算法，选项有自动、TKIP、AES：
  - 自动：表示本设备将根据需要自动选择加密算法；
  - TKIP：表示所有无线数据都将使用 TKIP 作为加密算法；
  - AES：表示所有无线数据都将使用 AES 作为加密算法；
- Radius 服务器 IP：用来对无线主机进行身份认证的 Radius 服务器的 IP 地址；
- Radius 端口：Radius 服务器对无线主机进行身份认证时使用的服务端口号；
- Radius 密码：该项用来设置访问 Radius 服务的密码；
- 密钥更新周期：用于指定密钥的定时更新周期。取值范围为 60~86400，单位为秒。缺省值为 3600，值为 0 时表示不更新。

7.2.3 WPA-PSK/WPA2-PSK

图 7-14 WPA-PSK/WPA2-PSK

- 安全机制：此处选择“WPA-PSK /WPA2-PSK”，表示本设备将采用 WPA-PSK 或 WPA2-PSK 安全机制。此安全机制下，本设备将采用基于预共享密钥的 WPA 模式；
- WPA 版本：用来设置本设备将使用的安全模式：
  - 自动：表示本设备会根据无线客户端的请求自动选择 WPA-PSK 或者 WPA2-PSK 安全模式；
  - WPA：表示本设备将采用 WPA-PSK 的安全模式；
  - WPA2：表示本设备将采用 WPA2-PSK 的安全模式；
- 加密算法：用来选择对无线数据进行加密的安全算法，选项有自动、TKIP、AES；
  - 自动：表示本设备将根据需要自动选择加密算法；
  - TKIP：表示所有无线数据都将使用 TKIP 作为加密算法；
  - AES：表示所有无线数据都将使用 AES 作为加密算法；
- 预共享密钥：预先设置的初始化密钥，取值为 8~63 个字符；
- 密钥更新周期：用于指定密钥的定时更新周期。取值范围为 60~86400，单位为秒。默认值为 3600，值为 0 时表示不更新。

7.3 无线 MAC 地址过滤

本节讲述***无线配置—>无线 MAC 地址过滤***页面及无线 MAC 地址过滤的配置方法。通过设置 MAC 地址过滤功能，可以允许或禁止无线主机接入本设备及无线网络。

图 7-15 无线 MAC 地址过滤

- 启用 MAC 地址过滤：启用或禁用 MAC 地址过滤功能，勾选表示启用；
- 过滤规则：设置 MAC 地址过滤的规则；
  - 允许：表示只允许 MAC 地址过滤信息列表中的 MAC 地址对应的无线客户端接入本设备，禁止除过滤表以外的无线客户端接入；
  - 禁止：表示只禁止 MAC 地址过滤信息列表中的 MAC 地址对应的无线客户端接入本设备，允许除过滤表以外的无线客户端接入；
- 添加新条目：点击该按钮，可进入 ***MAC 地址过滤配置***页面配置需要过滤的 MAC 地址，如下图所示。

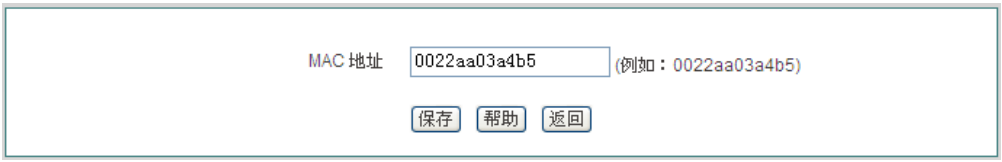

图 7-16 MAC 地址过滤配置

7.4 无线高级配置

本节介绍***无线配置—>无线高级配置***页面的无线高级参数的含义。

在本页面可以设置无线高级参数，一般情况下，这些参数保持默认值即可。如果您有特别需求，可以进入本页面进行配置。

图 7-17 无线高级配置

- RTS 阈值：当数据包超过这个阈值时，就会启动 RTS 机制。设备在发送数据帧前，会先发 RTS（Request to Send，请求发送）包到目的站点进行协商；接收到 RTS 帧后，无线站点会回应一个 CTS（Clear to Send，清除发送）帧来回应设备，表示两者之间可以进行无线通信了。一般，取值范围为 1~2347 字节，默认值为 2347；

  RTS 机制用于在无线局域网中避免数据发送冲突。RTS 包的发送频率需要合理设置，设置 RTS 门限时需要进行权衡。如果将这个参数值设得较小，则使 RTS 包的发送频率增加，消耗更多的带宽，明显影响其它网络数据包的吞吐量。但 RTS 包发送得越频繁，系统从中断或冲突中恢复得就越快；

- 分段阈值：用于定义无线 MAC 层允许传输的无线数据包的最大传输长度，当数据帧长度超过此值时，将自动被分段成多个数据帧，然后再进行传送。如果分段传输被中断，只有未成功发送的部分需要重新发送，分段包的吞吐量一般较低。一般，取值范围为 256~2346 字节，默认值为 2346 字节；

  大的分段传输效率较高，但如果无线网络中有明显的冲突或者使用频率很高，分段减小可以提高数据传输的可靠性。在大多数场合，请保持缺省值 2346；

- Beacon 间隔：设备通过定期广播 Beacon（信标）帧进行无线网络连接的同步，本参数用于定义信标帧的发送间隔，信标帧按照指定的时间间隔周期性发送。一般，取值范围为 20~999 毫秒，默认值为 100 毫秒；

- DTIM 间隔：本参数用于指定交付指示信息（DTIM，Delivery Traffic Indication Message）的发送间隔。DTIM 间隔用于决定含 TIM（Traffic Indication Map）的信标帧多久传送一次。TIM 会对进入休眠状态的站点发出警告，表示有数据处于待接收状态。DTIM 通常为信标间隔的倍数，可使用的范围为 1～255，默认值为 1；

- 启用短前导：启用或禁用短前导（Short Preamble）。

  - 启用后，将使用短前导类型；短前导类型能提供更好的性能。因为短前导的使用可以使开销减少到最小，因而使网络数据吞吐量最大化；
  - 禁用时，则使用长前导类型（Long Preamble），长前导类型将能够提供更多可行连接和更大范围的连接；

- 启用 WMM：允许启用或禁用 WMM 支持功能。WMM（Wi-Fi Multimedia，无线多媒体）是 802.11e 标准的一个子集。WMM 允许无线流量根据数据类型拥有一个优先级范围。时间敏感的信息，如视频或音频，将比普通流量的优先级更高。要正

确使用 WMM 功能，无线客户端也必须支持 WMM。

7.5 无线主机状态

本节介绍***无线配置—>无线主机状态***页面。

通过“无线主机状态信息列表”您可以查看当前连接到设备的无线主机的状态信息。此外，通过“无线主机状态信息列表”，您还可以方便地设置 MAC 地址过滤功能。

图 7-18 无线主机状态

- ID：序号；
- MAC 地址：无线主机的 MAC 地址；
- 过滤：选中表示当前 MAC 地址已经被添加到“MAC 地址过滤信息列表”中（可在***无线配置——>无线 MAC 地址过滤***页面查看），未选中表示当前 MAC 地址未设置过滤；
- 频道带宽：数据信道的理论数据传输率；
- 全部过滤：单击<全部过滤>，可以将当前列表中未启用过滤的所有无线主机进行 MAC 地址过滤，并将所有的 MAC 地址添加到“MAC 地址过滤信息列表”中；
- 刷新：单击<刷新>，可以查看最新的无线主机状态和统计信息。

第8章 高级配置

本章介绍的功能有：NAT 和 DMZ、路由配置、网络尖兵防御。

8.1 NAT 和 DMZ 配置

本节讲述***高级配置—>NAT 和 DMZ 配置***页面的功能及配置方法。

8.1.1 NAT 功能介绍

NAT（网络地址转换）是一种将一个 IP 地址域（如 Intranet）映射到另一个 IP 地址域（如 Internet）的技术。NAT 的出现是为了解决 IP 地址日益短缺的问题，NAT 允许专用网络在内部使用任意范围的 IP 地址，而对于公用的 Internet 则表现为有限的公网 IP 地址范围。由于内部网络能有效地与外界隔离开，所以 NAT 也可以对网络的安全性提供一些保证。

进取 ™510W 提供了灵活的 NAT 功能，以下将详细介绍它的特点。

1、 NAT 地址空间

为了正确进行 NAT 操作，任何 NAT 设备都必须维护两个地址空间：一个是内网主机在内部使用的私有 IP 地址，设备中用“内部 IP 地址”表示；另一个是用于外部的公网 IP 地址，设备中用“外部 IP 地址”表示。

2、 NAT 静态映射和虚拟服务器（DMZ 主机）

启用 NAT 功能后，设备会阻断从外部发起的访问请求。然而，某些应用环境下，外网中的计算机希望通过设备访问内网服务器，这时就需要在设备上设置 NAT 静态映射或虚拟服务器（DMZ 主机）来达到这个目的。

通过 NAT 静态映射功能，可建立**<外部 IP 地址+外部端口>**与**<内部 IP 地址+内部端口>**一对一的映射关系，这样，所有对设备某指定端口的服务请求都会被转发到匹配的内网服务器上，从而，外网中的计算机就可以访问这台服务器提供的服务了。

某些情况下，需要将一台内网计算机完全暴露给 Internet，以实现双向通信，这时候就需要将该计算机设置成虚拟服务器（DMZ 主机）。当有外部用户访问该虚拟服务器所映射的公网地址时，设备会直接把数据包转发到该虚拟服务器上。

提示：被设置为虚拟服务器的计算机将失去设备的防火墙保护功能。

NAT 静态映射的优先级高于虚拟服务器。当设备收到一个来自外部网络的请求时，它将首先根据外部访问请求的 IP 地址及端口号，检查是否有匹配的 NAT 静态映射，如果有的话，就把请求消息发送到该 NAT 静态映射匹配的内网计算机上。如果没有匹配的静态映射，才会检查是否有匹配的虚拟服务器。

3、 NAT 规则的两种类型

设备提供两种 NAT 类型：“EasyIP”和“One2One”。

EasyIP：即网络地址端口转换，多个内部 IP 地址映射到同一个外部 IP 地址。它可为每个内部连接动态分配一个与单一外部地址有关的端口，并维护这些内部连接到外部端口的映射，从而实现多个用户同时使用一个公网地址与外部 Internet 进行通信。

One2One：即静态地址转换，内部 IP 地址与外部 IP 地址进行一对一的映射。此方式下，端口号不会改变。它通常用来配置外网访问内网的服务器：内网服务器依旧使用私有地址，对外提供为其分配的公网 IP 地址给外部网络用户访问。

我们将每个具体的 NAT 配置称为“NAT 规则”，配置 NAT 规则时必须指定其出口 IP 地址及线路。当有多个合法的公网地址时，每种类型的 NAT 规则均可配置多个。实际应用中，常常需要混合使用不同类型的 NAT 规则。

8.1.2 NAT 静态映射

本节介绍设备的 NAT 静态映射功能。下面分别介绍 NAT 静态映射列表及 NAT 静态映射配置参数的涵义。

1、 NAT 静态映射列表

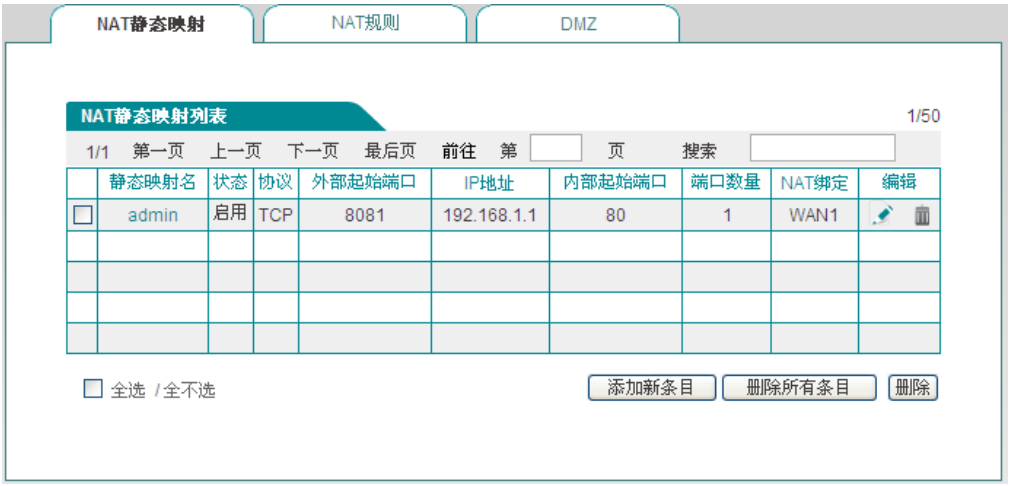

图 8-1 NAT 静态映射列表

提示：系统某些功能启用后，列表会显示一些 NAT 静态映射条目（如在***系统管理—>远程管理***页面启用远程管理后，会在该列表添加一条名为 admin 的静态映射），在本页面无法编辑或删除它们。

2、 NAT 静态映射配置

在图 8-1 的页面点击<添加新条目>进入 ***NAT 静态映射配置***页面，如图 8-2 所示。下面介绍 NAT 静态映射配置的各参数的涵义。

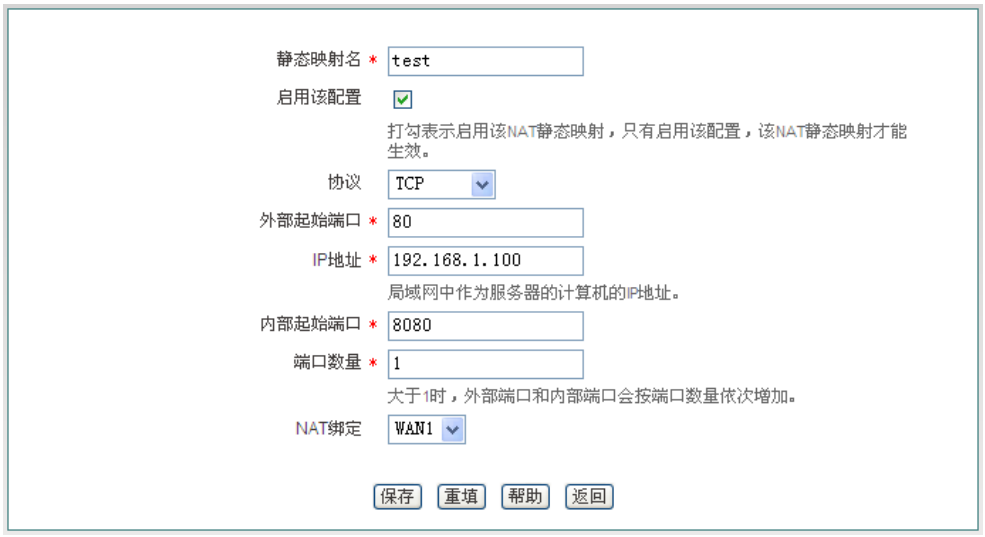

图 8-2 NAT 静态映射配置

- 静态映射名：NAT 静态映射名称，自定义，不能重复；
- 启用该配置：选中表示该条 NAT 静态映射生效，不选中表示该条 NAT 静态映射不生效，但保留其配置；
- 协议：数据包的协议类型，可供选择的有：TCP、UDP 和 TCP/UDP；当用户无法确认该应用所使用的协议为 TCP 或 UDP 时，可选择 TCP/UDP；
- 外部起始端口：设备提供给 Internet 的起始服务端口；
- IP 地址：内网中作为服务器的计算机的 IP 地址；
- 内部起始端口：内网服务器所开服务的起始端口；
- 端口数量：从内部起始端口开始的一段连续的端口，最大设置为 20；
- NAT 绑定：选择该条 NAT 静态映射绑定的接口。

8.1.3 NAT 规则

下面介绍设备的 NAT 规则功能，包括：NAT 规则信息列表、Easy IP NAT 规则配置参数涵义、One2One NAT 规则配置参数涵义。

1、 NAT 规则信息列表

在 NAT 规则信息列表中可以查看到已配置的 NAT 规则。如图 8-3 所示，表示已经配置两条 NAT 规则实例。一条实例的 NAT 类型为：EasyIP，是将内网 IP 地址为 192.168.1.20-192.168.1.25 的地址转换为 200.200.202.20，绑定在 WAN1 口实现上网。一条实例的 NAT 类型为：One2One，是将内网 IP 地址为 192.168.1.50-192.168.1-52 的地址分别转换为 200.200.202.50、200.200.202.51、200.200.202.52，且绑定在 WAN1 口实现上网。

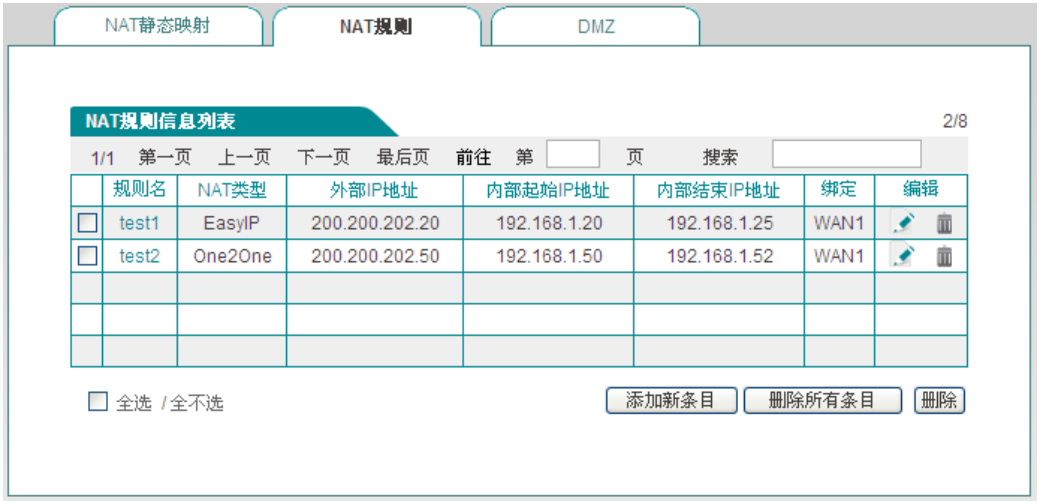

图 8-3 NAT 规则信息列表

提示：针对同一对象配置了多条 NAT 规则，最后配置规则先生效。

2、 Easy IP

在图 8-3 中点击<添加新条目>进入 NAT 规则配置页面。下面介绍配置 NAT 规则类型为 EasyIP 的各参数的涵义。

图 8-4 Easy IP

- 规则名：自定义该条 NAT 规则的名称；
- NAT 类型：这里选择 EasyIP，表示内部 IP 地址映射到同一个外部 IP 地址；
- 外部 IP 地址：该 NAT 规则中，内部 IP 地址所映射的外部 IP 地址；
- 内部起始 IP 地址、内部结束 IP 地址：内网中优先使用该 NAT 规则上网的计算机的 IP 地址范围；
- 绑定：选择该条 NAT 规则绑定的接口。

3、 One2One

在图 8-5 中选择 NAT 类型为 One2One，下面介绍配置 NAT 规则为 One2One 类型的部分参数涵义，对于与 EasyIP 相同的参数这里不再一一重述。

图 8-5 One2One

- NAT 类型：这里选择 One2One，内部 IP 地址与外部 IP 地址进行一对一的映射；
- 外部起始 IP 地址：该 NAT 规则中，内部起始 IP 地址所映射的外部起始 IP 地址。

提示：

1、 每条 One2One 规则最多只能绑定 20 个外部地址；

2、 “外部起始 IP 地址”必须设置，实际映射的外部 IP 地址从设置值开始依次增加。例如，如果“内部起始 IP 地址”设为 192.168.1.50，“内部结束 IP 地址”设为 192.168.1.52，“外部起始地址”设为 200.200.202.50，则 192.168.1.50、192.168.1.51、192.168.1.52 依次映射成 200.200.202.50、200.200.202.51、200.200.202.52。

8.1.4 DMZ

下面介绍设备的 DMZ 功能。

图 8-6 DMZ 配置

- 启用 DMZ 功能：启用或者关闭 DMZ 功能；
- DMZ 主机 IP 地址：欲用作虚拟服务器（DMZ 主机）的内网计算机的 IP 地址。

提示：

被设置为 DMZ 主机的计算机将失去设备的防火墙保护功能，且对所有的 WAN 口都生效。

8.1.5 NAT 和 DMZ 配置实例

本小节介绍 NAT 和 DMZ 配置的具体实例。包括：NAT 静态映射实例、NAT 规则类型为 EasyIP、One2One 的实例。

一、 NAT 静态映射配置实例

内网计算机 192.168.1.99 开设了 TCP80 端口的服务，希望外部通过 WAN1 口 80 端口访问这个服务，具体配置如图 8-7 所示。

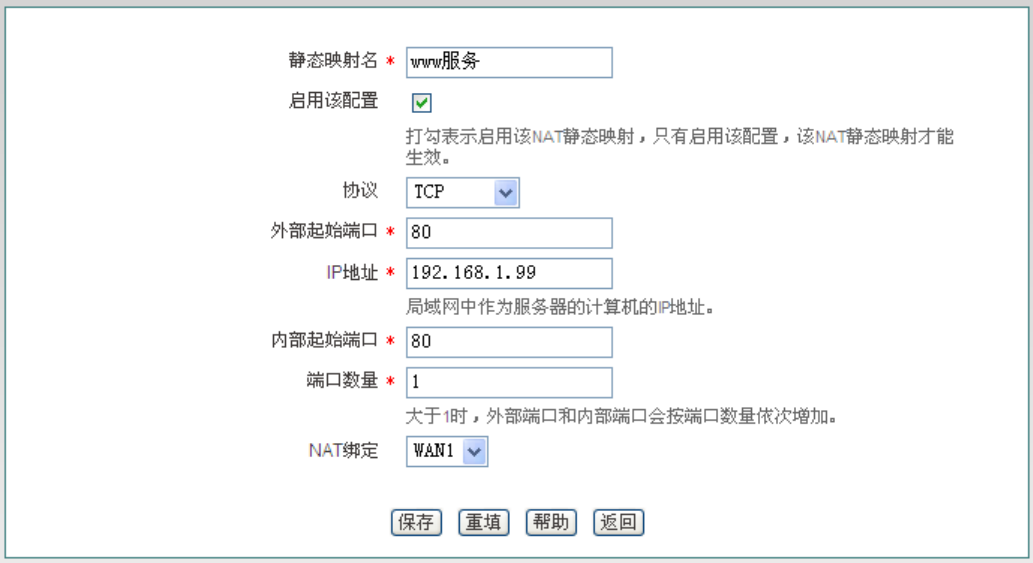

图 8-7 NAT 静态映射配置实例

二、 EasyIP 配置实例

某网吧使用单线路上网，ISP 为该线路分配了 8 个地址：218.1.21.0/29 ~218.1.21.7/29，其中 218.1.21.1/29 是该线路的网关地址，218.1.21.2/29 是该设备 WAN1 口的 IP 地址。注意 218.1.21.0/29、218.1.21.7/29 分别为相关子网的子网号和广播地址，不可使用。

现游戏 B 区（IP 地址范围：192.168.1.10/24~192.168.1.100/24）希望以 218.1.21.3/29 作为 NAT 映射地址通过 WAN 口上网。

配置步骤如下：

第一步，进入***高级配置—>NAT 和 DMZ 配置—>NAT 规则***页面，点击<添加新条目>；

第二步，进入 ***NAT 规则配置***页面，在“规则名”中填入“游戏区”；

第三步，选择“NAT 类型”为“EasyIP”；

第四步，在“外部 IP 地址”中填入 218.1.21.3；在“内部起始 IP 地址”和“内部结束 IP 地址”中分别填入 192.168.1.10 和 192.168.1.100；

第五步，选择该规则绑定的接口为 WAN1 口；

第六步，点击<保存>，该条 NAT 规则配置成功。

图 8-8 NAT 规则配置——EasyIP

提示：

在配置 Easy IP 时，当“外部 IP 地址”与绑定的接口的 IP 地址不在同一网段时，必须在上层路由器上配置一条到“外部 IP 地址”所在网段的路由或者是到“外部 IP 地址”的 32 位的主机路由，下一跳设置为绑定的接口的 IP 地址。

三、 One2One 配置实例

需求

某企业申请了一条电信的线路，固定 IP 接入方式，带宽为 6M。电信给它分配了 8 个地址：202.1.1.128/29～202.1.1.1.135/29，其中，202.1.1.129/29 是该线路的网关地址，202.1.1.130/29 是设备 WAN1 口的 IP 地址。注意，202.1.1.128/29、202.1.1.1.135/29 分别为相关子网的子网号和广播地址，不可使用。

该企业希望内部的人员上网通过 NAT 后使用 202.1.1.130/29 共享上网，另外有四台服务器做一对一 NAT（One2One）使用 202.1.1.131/29～202.1.1.1.134/29 对外提供服务。内部网络的地址是 192.168.1.0/24，4 台服务器的内部地址是 192.168.1.200/24～192.168.1.203/24。

分析

由于该线路是采用固定 IP 接入方式上网，首先需要在***网络参数—>WAN 口配置***页面中配置固定 IP 接入上网默认线路，或直接进入***开始—>配置向导—>网络参数***页面中配置该线路。上网默认线路正确配置后，将自动生成与默认线路对应的系统保留 NAT 规则，NAT 功能也自动启用。

而该企业使用提供四台内部服务器供外部访问，因此还需为它们设置一个类型为“One2One”的 NAT 规则。

配置步骤如下：

第一步，进入***高级配置—>NAT 和 DMZ 配置—>NAT 规则***页面，点击<添加新条目>；

第二步，进入 NAT 规则配置页面，在“规则名”中填入“服务器”；

第三步，选择“NAT 类型”为“One2One”；

第四步，在“外部起始 IP 地址”中填入 202.1.1.131；在“内部起始 IP 地址”和“内部结束 IP 地址”中分别填入 192.168.1.200 和 192.168.1.203；

第五步，选择该规则绑定的接口为 WAN1 口；

第六步，单击<保存>，该条 NAT 规则添加成功。

图 8-9 NAT 规则配置——One2One

8.2 路由配置

本节介绍*高级配置—>路由配置*页面及配置方法。

静态路由是由网络管理员手工配置的路由，使得到指定目的网络的数据包的传送，按照预定的路径进行。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，需要手工修改路由表中相关的静态路由信息。正确设置和使用静态路由可以改进网络的性能，还可以实现特别的要求，比如实现流量控制、为重要的应用保证带宽等。

下面介绍路由配置信息列表及路由配置中各参数的涵义。

图 8-10 路由信息列表

在上图中点击<添加新条目>，进入*路由配置*页面。

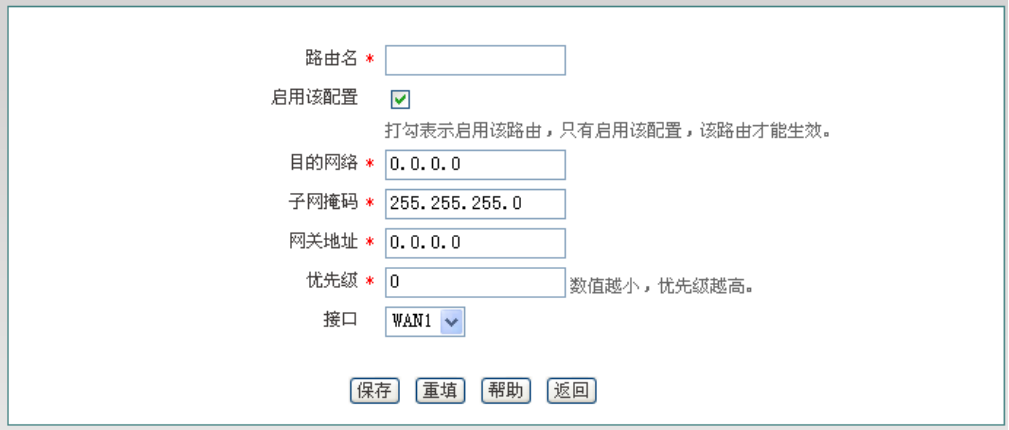

图 8-11 静态路由配置

- 路由名：静态路由的名称（自定义，不可重复）；
- 启用该配置：启用该静态路由，选中表示启用，取消选中则表示禁用该路由；
- 目的网络：此静态路由的目的网络号；
- 子网掩码：此静态路由的目的网络的掩码；
- 网关地址：下一跳路由器入口的 IP 地址，设备通过接口和网关定义一条跳到下一个路由器的线路。通常情况下，接口地址和网关须在同一网段；
- 优先级：设置静态路由的优先级，在目的网络、子网掩码相同时，选择优先级高的路由转发数据，值越小优先级越高；
- 接口：指定数据包的转发接口，与该静态路由匹配的数据包将从指定接口转发。根据型号的不同选项不同。

提示：当多条路由的目的网络和优先级相同时，设备会根据越晚建立的越先匹配的原则进行匹配。

8.3 网络尖兵防御

本节介绍***高级配置—>网络尖兵防御***页面及配置。网络尖兵防御功能是用来破解运营商设置的共享检测。请确认内网遇到共享检测问题，否则不要轻易启用该功能。

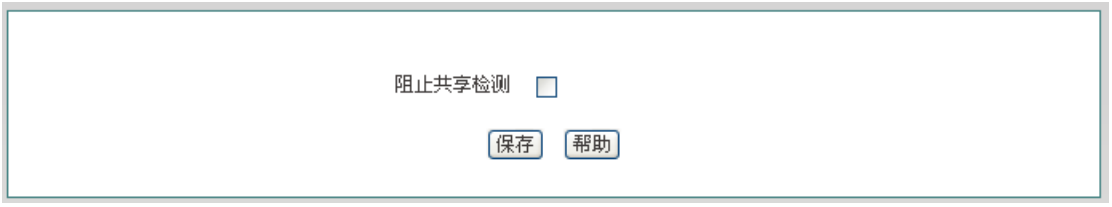

图 8-12 网络尖兵防御

第9章 用户管理

本章介绍用户管理一级菜单下的二级菜单，包括：用户状态、IP/MAC 绑定、PPPoE 服务器、WEB 认证、用户组配置。

9.1 用户状态

本节介绍*用户管理—>用户状态*页面。管理员通过查看、分析本页面的饼图及列表能够了解内网所有用户的上网行为、各上网行为所占用网络流量的情况及每个用户的状态等。

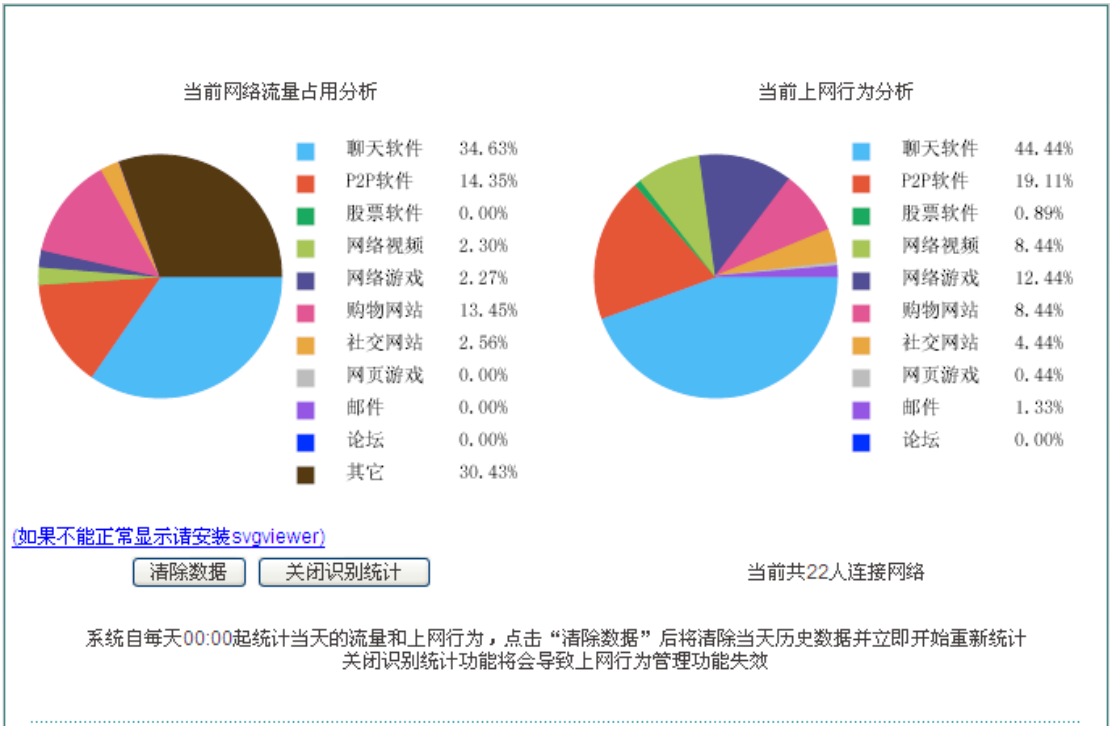

图 9-1 用户行为分析饼图

- 当前网络流量占用分析：分析当前内网各个应用所占用的网络流量百分比；
- 当前上网行为分析：分析当前内网所有上网用户的上网行为情况；
- 清除数据：系统自每天 00:00 起统计当天的流量和上网行为，点击该按钮后将清除当天历史数据并立即开始重新统计；
- 关闭识别统计：点击该按钮可关闭上网行为管理的识别功能，关闭识别统计后，上网行为管理功能将失效。

下面介绍用户状态信息列表，通过查看该列表，管理员能够了解每个上网用户的上网时长、实时的上传/下载速率、上行/下行总流量、上网行为等。

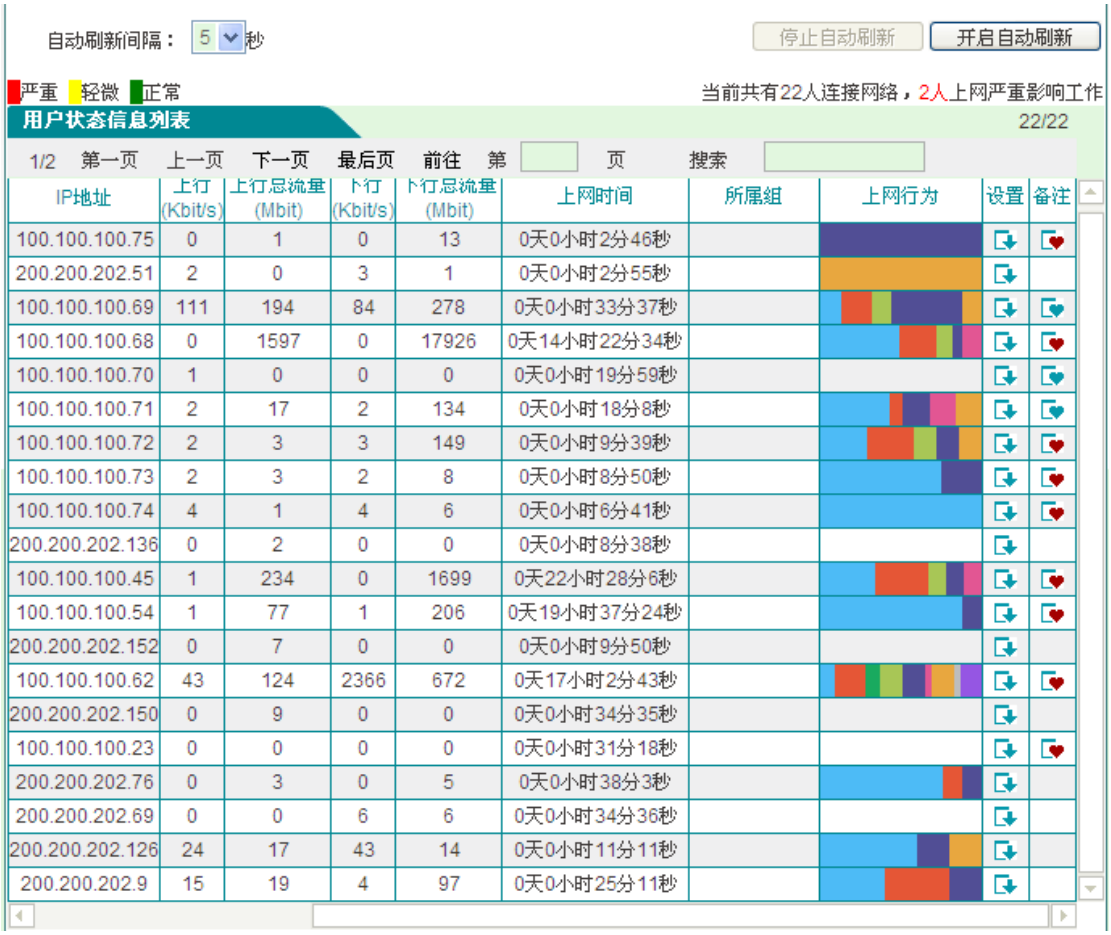

图 9-2 用户状态信息列表

用户状态信息列表的第一列显示每个用户的上网行为是否影响到工作，其状态有：严重（红色）、轻微（黄色）、正常（绿色）。当内网用户访问购物网站、社交网站、使用股票软件及玩网络/网页游戏的行为占个人所有的上网行为的范围在[100%, 70%]时，表示严重影响到工作；当范围在（70%, 50%] 时表示轻微；当范围在（50%, 0%] 时表示正常。

- 用户名：显示内网用户的用户名；
- MAC 地址：显示内网用户的 MAC 地址；
- 认证方式：显示内网用户的认证方式（WEB 和 PPPoE）
- IP 地址：显示内网用户的 IP 地址；
- 上传、下载速率：显示内网用户的上传、下载速率；
- 上行、下行总流量：显示内网用户上行、下行总流量；
- 上网时间：显示该用户的上网时间；
- 所属组：显示该用户所属的组；
- 上网行为：显示该用户的各上网行为；
- 设置：点击该图标，如果您需要清除该用户的上网行为统计，请点击“清除数据”；

- 备注：点击该图标可修改该 PPPoE 拨号用户、WEB 认证用户的描述信息。
- 自动刷新间隔：该列表支持自动刷新，间隔为 1~5 秒；
- 停止自动刷新：点击该按钮列表会停止自动刷新；如需查看整个列表的信息或修改备注信息等建议停止自动刷新；
- 开启自动刷新：点击该按钮列表会根据自动刷新间隔来刷新列表。

9.2　IP/MAC 绑定

本节讲述***用户管理—>IP/MAC 绑定***页面及配置方法。

要实现网络安全管理，首先必须解决用户的身份识别问题，然后才能进行必要的业务授权工作。在***防火墙—>访问控制策略***中，我们将会详细地介绍如何实现对内网用户上网行为的控制。在本节，我们将介绍如何解决用户的身份识别问题。

在设备中，通过 IP/MAC 绑定功能完成用户的身份识别工作。使用绑定的 IP/MAC 地址对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。IP 欺骗攻击是一台主机企图使用另一台受信任的主机的 IP 地址连接到设备或者通过设备。这台主机的 IP 地址可以轻易地改变为受信任的 IP 地址，但是 MAC 地址是由生产厂家添加到以太网卡上的，不能轻易地改变。

9.2.1　IP/MAC 绑定列表

图 9-3 IP/MAC 绑定全局配置

- 允许非 IP/MAC 绑定用户连接到设备：允许或禁止非 IP/MAC 绑定的用户连接到设备，并通过设备访问其他网络；
- 允许：勾选该复选框表示允许绑定用户连接到设备，不勾选表示不允许绑定用户连接到设备；
- 修改 IP/MAC 绑定条目，点击编辑图标，进入如下图所示的***IP/MAC 绑定配置***页面，

修改完后点击<保存>。

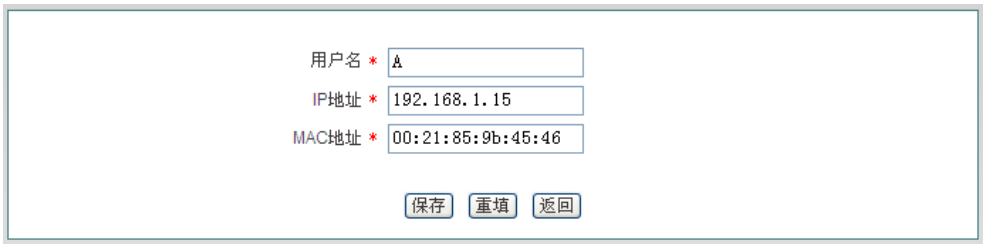

图 9-4 IP/MAC 实例修改

提示：

当决定取消“允许非 IP/MAC 绑定用户连接到设备”功能前，必须确认管理计算机已经被添加到“IP/MAC 绑定信息列表”中，否则将会造成管理计算机无法连接到设备的现象。

9.2.2 IP/MAC 绑定配置

图 9-5 IP/MAC 绑定配置

- 网段：默认是设备的管理 IP 地址/子网掩码；
- 文本框：会显示扫描后的 IP/MAC 信息，也可以在该文本框中配置 IP/MAC 绑定信息，其输入格式为“IP+MAC+用户名”；
  - IP 地址、MAC 地址：该用户的 IP 地址、MAC 地址（windows 平台 DOS 环境下使用 ipconfig /all 命令获得）；
  - 用户名：也可以不输入，系统会自动给它分配一个用户名；
- 扫描：点击<扫描>，将显示设备动态学习到的 ARP 信息；
- 绑定：绑定文本框中的所有的 IP/MAC 条目。

提示：

1、 在上述输入格式中 IP 与 MAC、MAC 与用户名之间可有一个或多个空格；

2、 对无效的条目，在绑定的时候系统将跳过无效的配置条目。

9.2.3 IP/MAC 绑定实例

灵活地运用 IP/MAC 绑定功能，可以为内网用户配置上网“白名单”和“黑名单”。

通过配置上网“白名单”，将只允许“白名单”中的用户通过设备上网，禁止其他所有用户通过设备上网。因此，如果要求只允许内网中的少数用户上网，可通过配置上网“白名单”来实现。

通过配置上网“黑名单”，将只禁止“黑名单”中的用户通过设备上网，允许其他所有用户通过设备上网。因此，如果要求只禁止内网中的少数用户上网，可通过配置上网“黑名单”来实现。

在设备中，“白名单”中的用户即为合法用户——其 IP 及 MAC 地址与“IP/MAC 绑定信息列表”中的某条目完全匹配，且该条目选中“允许”。

“黑名单”中的用户即为非法用户——其 IP 及 MAC 地址与“IP/MAC 绑定信息列表”中的某条目完全匹配，且该条目没有选中“允许”；或者，其 IP 和 MAC 地址中有且只有一个与某个绑定条目的对应信息匹配。

1、 为内网用户配置上网“白名单”，步骤如下：

第一， 通过配置 IP/MAC 绑定条目来指定合法用户，将具有上网权限的主机的 IP 地址和 MAC 地址作为 IP/MAC 地址绑定对，并添加到“IP/MAC 绑定信息列表”中，还需选中“允许”，即允许与该 IP/MAC 地址对完全匹配的用户上网。

第二， 不选中“允许非 IP/MAC 绑定用户连接到设备过”，从而，其他所有不在“IP/MAC 绑定信息列表”中的主机将不能上网。

例如，如果要允许某个 IP 地址为 192.168.1.2，MAC 地址为 0021859b4544 的主机连接和通过设备，则可添加一个 IP/MAC 绑定条目，输入该主机的 IP 地址和 MAC 地址，并选中“允许”，如图 9-6 所示。

图 9-6 IP/MAC 绑定信息列表——实例一

2、 为内网用户配置上网“黑名单”，步骤如下：

第一， 通过配置 IP/MAC 绑定条目来指定非法用户，有两种方法：

1. 将禁止上网的主机的 IP 地址和任意一个非本内网网卡的 MAC 地址作为 IP/MAC 地址绑定对，并添加到“IP/MAC 绑定信息列表”中；

2. 可将禁止上网的主机的 IP 地址和 MAC 地址作为 IP/MAC 地址绑定对，添加到“IP/MAC 绑定信息列表”中，并取消“允许”的选中（方框中无“√”），即禁止与该 IP/MAC 地址对完全匹配的用户上网。

第二， 选中“允许非 IP/MAC 绑定用户连接到设备”，从而，其他所有 IP 地址和 MAC 地址均不在“IP/MAC 绑定信息列表”中的主机将能够上网。

例如，如果要禁止具有某个 IP 地址（例如 192.168.1.3）的主机访问和连接设备，可以添加一个 IP/MAC 地址绑定对，输入该 IP 地址，而 MAC 地址则设置成任意一个非本内网网卡的 MAC 地址，如下表所示。

图 9-7 IP/MAC 绑定信息列表——实例二

例如，如果要禁止某个 IP 地址为 192.168.1.30，MAC 地址为 0021859b2564 的主机连接

和通过设备，则可添加一个 IP/MAC 地址绑定对，输入该主机的 IP 地址和 MAC 地址，并取消“允许”的选中（方框中无“√”），图 9-8 所示。

图 9-8 IP/MAC 绑定信息列表——实例三

9.3　PPPoE 服务器

本节介绍设备的 PPPoE 功能，包括：PPPoE 介绍、设备的 PPPoE 的全局配置、PPPoE 账号配置及查看 PPPoE 的连接状态。

9.3.1　PPPoE 简介

PPPoE（Point-to-Point Protocol over Ethernet），即以太网上的点对点协议，它可以使以太网上的主机通过一个简单接入设备连到 Internet 上。PPPoE 协议采用 Client/Server（客户端/服务器）方式，它将 PPP 报文封装在以太网帧内，在以太网上提供点对点的连接。

PPPoE 拨号连接包括 Discovery（发现）和 Session（PPP 会话）两个阶段。下面将分别介绍这两个阶段。

1、 Discovery 阶段

此阶段用来建立连接，当一个用户主机想开始一个 PPPoE 会话时，首先必须进行发现阶段以识别 PPPoE Server 的以太网 MAC 地址，并建立一个 PPPoE 会话标识（Session ID）。

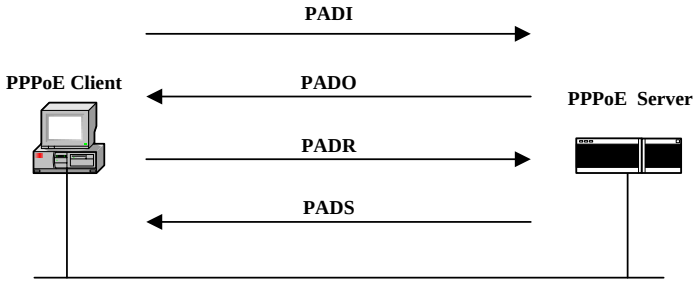

图 9-9 Discovery 阶段的基本工作流程

如上图所示， Discovery 阶段由四个步骤组成，下面将介绍它的基本工作流程。

- PADI：如果要建立一条 PPPoE 连接，首先 PPPoE 客户端就要以广播的方式发送一个 PADI(PPPoE Active Discovery Initiation)数据包，PADI 数据包包括客户端请求的服务。
- PADO：当 PPPoE 服务器收到一个 PADI 包之后，它会判断自己是否能够提供服务，如果能够提供服务的话，就会向客户端发送 PADO(PPPoE Active Discovery Offer)数据包来进行回应。PADO 数据包包括 PPPoE 服务器名称和与 PADI 数据包中相同的服务名。如果 PPPoE 服务器不能为 PADI 提供服务，则不允许用 PADO 数据包响应。
- PADR：由于 PADI 是以广播的形式发送出去的，PPPoE 客户端可能收到不止一个 PADO 数据包，它将审查所有接收到的 PADO 数据包并根据其中的服务器名或所提供的服务选择一个 PPPoE 服务器，并向选中的服务器发送 PADR（PPPoE Active Discovery Request）数据包。PADR 数据包包括客户端所请求的服务。
- PADS：当 PPPoE 服务器收到客户端发送的 PADR 包时，它就准备开始一个 PPPoE 会话，它为 PPPoE 会话创建一个唯一的 PPPoE 会话 ID，并向客户端发送 PADS (PPPoE Active Discovery Session- confirmation)包作为响应。

当发现阶段正常结束后，通信的两端都获得会话标识（Session ID）和对方的 MAC 地址，它们一起唯一定义一个 PPPoE 会话。

2、 PPP 会话阶段

当 PPPoE 进入 PPP 会话阶段后，客户端和服务器将进行标准的 PPP 协商，PPP 协商通过后，数据通过 PPP 封装发送。PPP 报文作为 PPPoE 帧的净荷被封装在以太网帧内，发送到 PPPoE 链路的对端。Session ID 必须是 Discovery 阶段确定的 ID，且在会话过程中保持不变，MAC 地址必须是对端的 MAC 地址。

在会话阶段的任意时刻，PPPoE 服务器和客户端都可向对方发送 PADT（PPPoE Active Discovery Terminate）包通知对方结束本会话。当收到 PADT 以后，就不允许再使用该会话发送 PPP 流量了。在发送或接收到 PADT 数据包后，即使是常规的 PPP 结束数据包也不允许发送。一般情况下，PPP 通信双方使用 PPP 协议自身来结束 PPPoE 会话，但在无法使用 PPP 时可以使用 PADT 来结束会话。

9.3.2 PPPoE 全局配置

进入***用户管理—>PPPoE 服务器***页面配置 PPPoE 服务器功能。配置参数介绍如下。

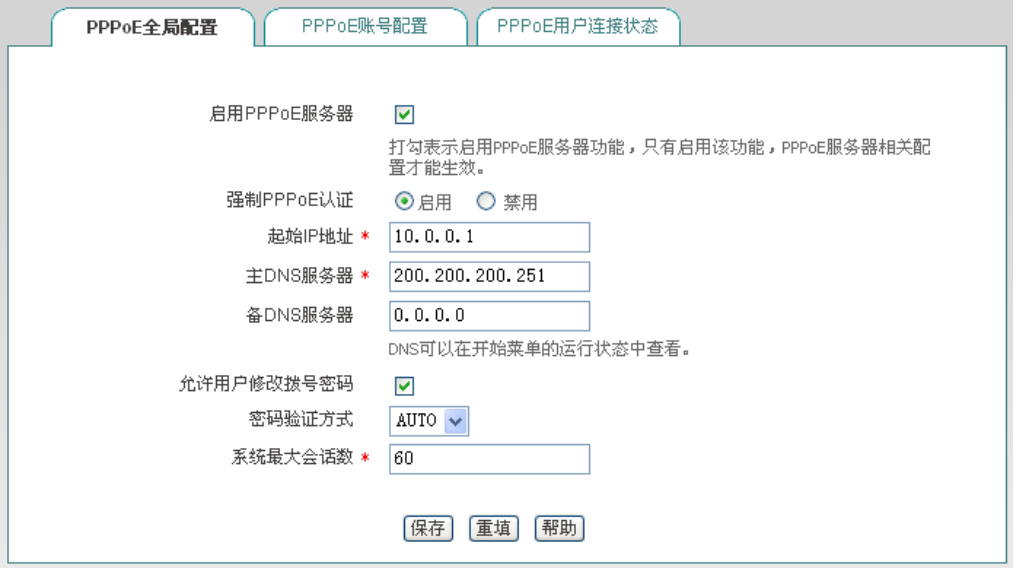

图 9-10 PPPoE 服务器全局配置

- 启用 PPPoE 服务器：启用/禁用设备的 PPPoE 服务器功能，选中为启用；
- 强制 PPPoE 认证：启用强制 PPPoE 认证表示只允许内网 PPPoE 认证通过的用户访问因特网；
- 起始 IP 地址：PPPoE 服务器给内网计算机自动分配的起始 IP 地址；
- 主 DNS 服务器：PPPoE 服务器给内网计算机自动分配的主用 DNS 服务器的 IP 地址；
- 备 DNS 服务器：PPPoE 服务器给内网计算机自动分配的备用 DNS 服务器的 IP 地址；
- 允许用户修改拨号密码：勾选表示允许内网 PPPoE 拨号用户自助修改拨号密码；
- 密码验证方式：PPPoE 验证用户名和密码的方式，设备提供 PAP、CHAP 以及 AUTO 三种验证方式，默认值为 AUTO，表示系统自动选择 PAP 和 CHAP 中的一种对拨入用户进行身份验证，一般情况下不需要设置；
- 系统最大会话数：系统支持建立 PPPoE 会话的最大数量。

提示：

1、 PPPoE 用户修改拨号密码步骤：

1) 用户打开拨号客户端，使用用户名、密码进行拨号；
2) 拨号成功后，登录自助服务页面，其地址为：http://192.168.1.1/poeUsers.asp（该地址为设备 LAN 口 IP 地址）；
3) 在修改密码页面输入用户名、旧密码、新密码、确认密码；
4) 点击“提交”，显示“操作成功”即密码修改成功。

2、 用户每天只能自助修改 5 次密码；

3、 管理员可以通过在*行为管理—>电子通告*页面配置**日常事务通告**通知用户如何修改 PPPoE 拨号密码。

9.3.3 PPPoE 账号配置

进入*用户管理—>PPPoE 服务器—>PPPoE 账号配置*页面（如图 9-11 所示）可以查看 PPPoE 账号信息列表；点击<添加新条目>，进入如图 9-12 所示的页面：

图 9-11 PPPoE 账号信息列表

- 用户名：PPPoE 拨号用户的用户名；
- 固定 IP 地址：显示该用户名绑定的 IP 地址；
- 计费模式：当启用计费功能后，会显示“按日期”（目前支持按日期计费）；
- 用户状态：当开启计费功能后会显示该用户的使用状态，包括：正常、将过期、过期；
  - 将过期：该参数通过账号到期通告功能中的“账号剩余天数”来控制（其中账号到期通告功能请进入*行为管理—>电子通告*页面进行配置）；
  - 过期：表示该账号不在账号使用的有效日期内；
- 账号开通日期、账号停用日期：当启用计费功能后，会显示该账号的有效日期。
- 导出账号：点击该按钮可导出列表中所有的 PPPoE 账号，内容包括账号的用户名、密码，格式为.txt；
- 导入账号：点击该按钮可批量导入 PPPoE 账号，格式为：用户名 密码。

提示：PPPoE 账号批量导入的格式为“用户名 密码”，其中用户名密码之间有一个或多个空格；例如：test 123456，且每行只能输入一条配置。

图 9-12 PPPoE 账号配置

- 用户名：用户发起 PPPoE 连接时使用的供 PPPoE 服务器验证的账号（自定义，不可重复），取值范围：1~31 个字符；
- 密码：用户发起 PPPoE 连接时使用的供 PPPoE 服务器验证的密码；
- 固定 IP 地址：为该 PPPoE 拨号用户分配的固定 IP 地址，且该地址必须在地址池范围内；
- 计费模式：勾选表示启用 PPPoE Server 计费功能，其中账号到期通告功能请进入*行为管理—>电子通告*页面进行配置；
- 账号开通日期、账号停用日期：设置拨入用户使用该账号的有效日期。

9.3.4 PPPoE 用户连接状态

进入*用户管理—> PPPoE 服务器—>PPPoE 用户连接状态*页面，在此页面可以查看各帐号的使用信息，如果有用户使用已配置的用户名连接到 PPPoE 服务器，我们可以在列表中看到 PPPoE 服务器为该用户分配的 IP 地址、该用户的 MAC 地址、PPPoE 连接的在线时间、上传/下载的速率等信息。

图 9-13 PPPoE 连接状态信息列表

提示：内网拨号用户账号过期后，仍能够拨号成功，能够访问设备，但不能访问因特网。

9.3.5 PPPoE 服务器配置实例

1、 需求：只允许内网通过认证的用户访问因特网。

现为内网用户配置 3 个账号，用户名分别为 test1、test2、test3；密码分别为：password1、password2、password3，分别分配到的 IP 地址为 10.0.0.1、10.0.0.2、10.0.0.3；且开启计费功能，账号使用期限为 2012 年 5 月 1 日至 2012 年 8 月 31 日，当账号还有 15 天到期时自动发送到期通告通知用户。

2、 配置步骤：

1) 配置 PPPoE 服务器。登录设备，进入***用户管理—>PPPoE 服务器***页面，配置内容如下图所示：

图 9-14 实例——PPPoE 全局配置

2) 配置 PPPoE 账号。进入 ***PPPoE 账号配置***页面，点击<添加新条目>，配置 PPPoE 账号，将账号与 IP 地址进行绑定，并开启计费功能，用户名为 test1 的配置内容如下图所示：

图 9-15 实例——PPPoE 账号配置

3)　重复步骤 2，配置 PPPoE 用户名为 test2、test3 的账号；

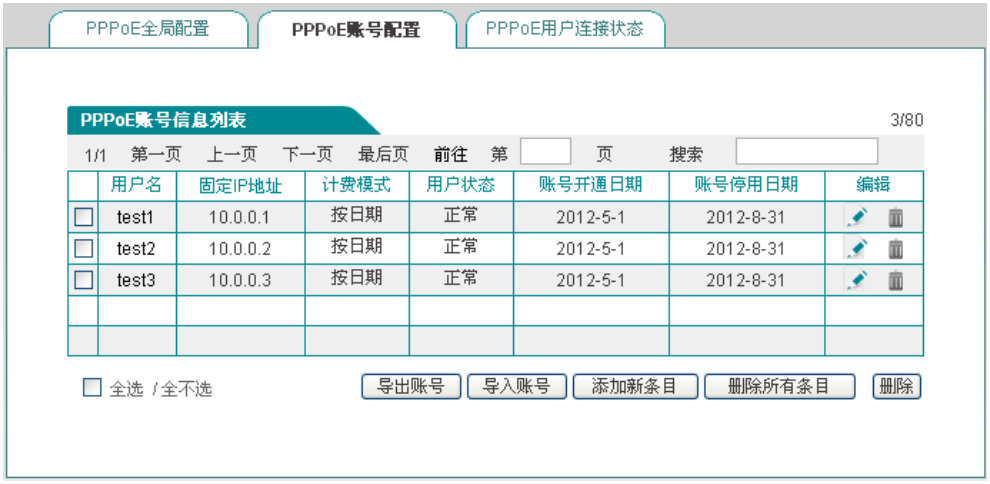

图 9-16 实例——PPPoE 账号信息列表

4)　配置账号到期通告功能。进入*行为管理—>电子通告—>账号到期通告*页面，配置账号到期通告功能，其中“提前发送到期通告天数”设置为 15 天；

5)　在内网用户的计算机上创建客户端。

9.4　WEB 认证

进入*用户管理—>WEB 认证*页面能够配置设备的 WEB 认证功能。WEB 认证用于验证内网非 PPPoE 用户是否有权限访问因特网，即启用该功能后，内网非 PPPoE 用户需经过 WEB 认证后才能访问因特网。

图 9-17 WEB 认证

- 启用 WEB 认证：勾选表示内网非 PPPoE 用户需通过 WEB 认证才能访问因特网；

- 允许用户修改认证密码：勾选表示允许 WEB 认证用户自助修改认证密码；
- 用户名：显示 WEB 认证用户的用户名；
- IP 地址：WEB 认证成功后，显示该用户的 IP 地址；
- 用户状态：显示 WEB 认证用户的连接状态，包括：未使用、使用中。
- 描述：显示管理员自定义的描述内容；
- 挂断：点击该按钮可挂断该用户的连接。

提示：

1、 WEB 认证用户修改认证密码步骤：

1) 用户打开浏览器，使用用户名、密码进行认证；

2) 认证成功后，登录自助服务页面，其地址为：http://192.168.1.1/waUsers.asp（该地址为设备 LAN 口的 IP 地址）；

3) 在密码修改页面输入用户名、旧密码、新密码、确认密码；

4) 点击“提交”，显示“操作成功”即密码修改成功。

2、 用户每天只能自助修改 5 次密码；

3、 管理员可以通过在***行为管理—>电子通告***页面配置**日常事务通告**通知用户如何修改 WEB 认证密码。

9.5　用户组配置

在***用户管理—>用户组配置***页面，点击“用户组配置列表”下的<添加新条目>进入如图 9-19 所示页面。

图 9-18 用户组列表

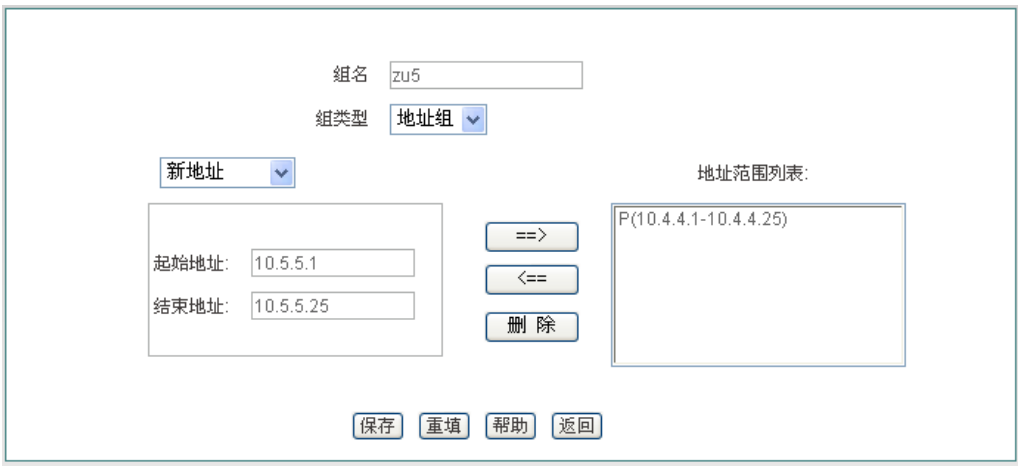

图 9-19 用户组配置

- 组名：自定义该用户组的组名；
- 组类型：组类型分为地址组和账号组；其中账号组指的是 PPPoE 认证账号、WEB 认证账号；

提示：用户组的深度不能大于 2，如：地址 A 包含地址组 B，现配一个地址组 C，让其包含地址组 A 是不允许的。

第10章 行为管理

本章介绍的功能有：时间段、上网行为管理、QQ 白名单、MSN 白名单、电子通告等。

10.1　时间段配置

进入*行为管理—>时间段配置*页面，点击“添加新条目”，进入如图 10-2 所示的配置页面。时间段定义相关功能的生效时间，一个时间段能够定义三个时间单元。

图 10-1 时间段配置列表

图 10-2 时间段配置

- 时间段名：自定义时间段的名称；
- 时间段生效日期：配置该时间段的生效日期；
- 时间单元：配置在生效日期中的生效时间单元。

10.2　上网行为管理

本节介绍*用户管理—>上网行为管理*页面的上网行为管理列表及上网行为管理配置。

10.2.1 上网行为列表

进入*行为管理—>上网行为管理*页面，可以在本页面启用上网行为管理功能，在上网行为管理信息列表中查看已配置的上网行为管理信息。

图 10-3 行为管理信息列表

- 启用上网行为管理：勾选表示启用上网行为管理功能。注：应确保*用户管理—>用户状态*页面的识别统计是开启的，否则上网行为管理功能将失效。

10.2.2 上网行为管理配置

在上图中点击<添加新条目>进入*上网行为管理配置*页面，在此页面可以对内网用户的上网行为进行管理。

图 10-4 行为管理配置

- 组名：自定义该条上网行为管理实例的组名，不能重复；

- 选择上网行为管理对象：填写该行为管理实例生效的地址段或用户组；
- 设备支持的上网行为管理有：P2P 软件、股票软件、网络视频、网络游戏、购物网站、社交网站、网页游戏、邮件、论坛等；
- 生效时间设置：设置该上网行为管理实例的生效的时间。

提示：

当某上网行为管理功能不生效时，请确定该功能的策略库是否为最新，可在***行为管理-→策略库***页面，点击<更新>超链接更新对应的策略库。

10.2.3 用户管理配置实例

1、 需求

某公司为控制员工的上网行为，针对其实际需求，规定在工作时间中禁止 QQ、MSN 等聊天软件、禁止股票和游戏软件，禁止查看股票及游戏网站信息，禁止访问购物网站。在其余时间则开放所有业务。

其中管理层用户（地址为 192.168.1.5 和 192.168.1.9），上网行为不受任何限制。

销售部和客服部员工，地址分别为 192.168.1.50~192.168.1.69 和 192.168.1.70~192.168.1.99，由于工作需要，需使用聊天软件与客户进行沟通。

研发部（地址为 192.168.1.100~192.168.1.129）禁止聊天软件的使用。

该公司的工作时间为：周一～周五，9 点～18 点。

2、 分析

由上，可以根据将该公司的上网行为管理需求，配置 2 条上网行为管理策略。

1) 为销售部和客服部员工配置上网行为管理策略，开启聊天软件功能；禁止其他功能。

2) 为研发部员工配置上网行为管理策略，只禁止聊天软件的使用。

3、 配置步骤

1) 进入***行为管理—>上网行为管理***页面，点击<添加新条目>，进入***上网行为管理配置***页面；

2) 配置销售部、客服部的行为管理策略：

组名：IM

起始 IP 地址、结束 IP 地址：192.168.1.50、192.168.1.99；

行为管理：勾选股票软件、网络视频、网络游戏、购物网站、社交网站、网页游戏、邮件、论坛、其他的的“全选”框；

生效时间段：周一至周五、从 9:00~18:00；点击<保存>。

3) 配置研发部的行为管理策略：

组名：yanfa

起始 IP 地址、结束 IP 地址：192.168.1.100、192.168.1.129；

行为管理：只勾选聊天软件的“全选”框；

生效时间段：周一至周五、从 9:00~18:00；点击<保存>。

4、 查看配置列表

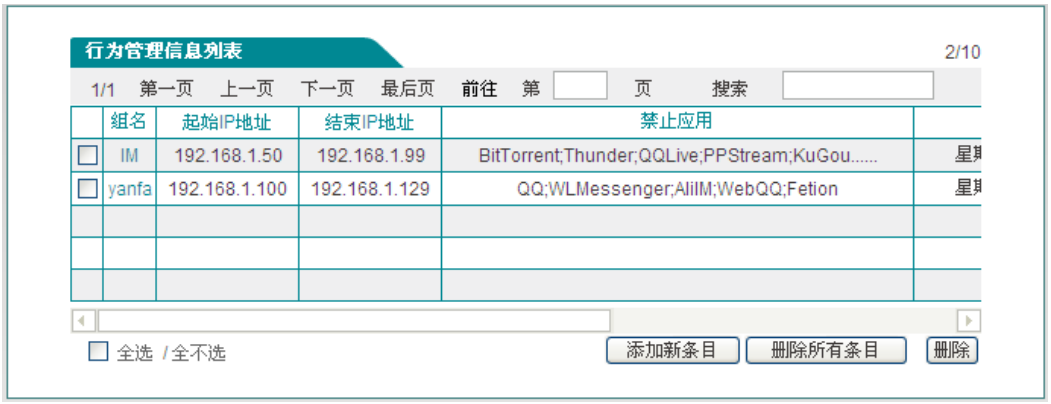

图 10-5 上网行为管理实例

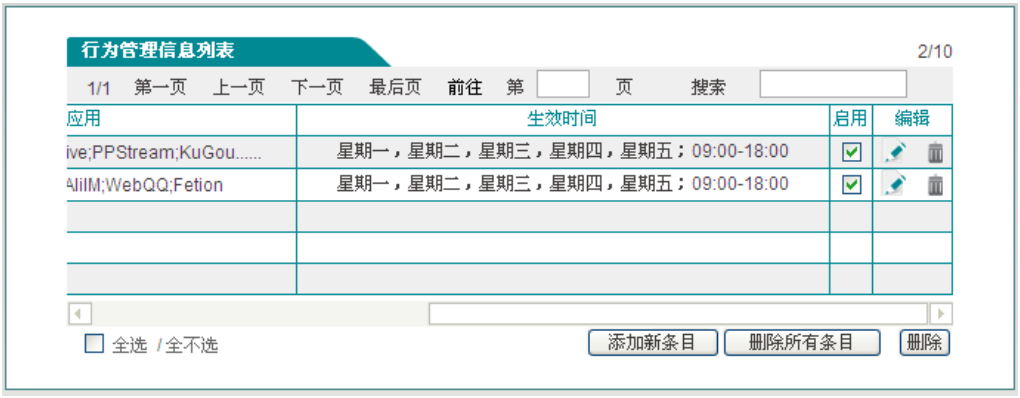

图 10-6 上网行为管理实例（续图 10-5）

10.3 QQ 白名单

QQ 白名单是在*上网行为管理*页面禁止 QQ 后定义允许登录的 QQ 用户。

进入*行为管理—>QQ 白名单*页面，启用 QQ 白名单功能后，点击“添加新条目”进入 QQ 白名单配置页面添加 QQ 白名单用户。

图 10-7 QQ 白名单

- 允许 400/800 企业 QQ：勾选表示放通 400/800 企业 QQ；
- 启用 QQ 白名单：勾选表示启用 QQ 白名单功能。

提示：该版本支持的最大的 QQ 号码为 4294967295。

10.4　MSN 白名单

MSN 白名单是在**上网行为管理**页面禁止 MSN 后定义允许登录的 MSN 用户。

进入***行为管理—>MSN 白名单***页面，启用 MSN 白名单功能后，点击“添加新条目”进入 MSN 白名单配置页面添加 MSN 白名单用户。

图 10-8 MSN 白名单

- 启用 MSN 白名单：勾选表示启用 MSN 白名单功能。

10.5　电子通告

进入*行为管理—>电子通告*页面，可以配置日常事务通告和账号到期通告。

通告是在内网用户访问网站时设备以 Web 页面的形式发送给用户的通知。 内网用户在收到通告后，在浏览器地址栏再次输入相应地址即可正常访问网站。

10.5.1　日常事务通告

图 10-9 日常事务通告

- 启用：勾选表示启用日常事务通告功能；
- 通告网段：设置该日常事务通告的地址范围，其中最多只能包含 65535 个地址；
- 通告标题、内容：设置日常事务通告的标题及内容；
- 生效日期设置：设置该日常事务通告生效的日期；
- 生效频率：设置该日常事务通告的频率。
- 预览页面：点击该按钮，预览所配置的通告内容；
- 保存：点击<保存>后，内网指定用户在生效时段内第一次访问网页时会收到设备发

送的日常事务通告。

提示：当日常事务通告只修改“通告标题”、“通告内容”时，点击<保存>后，该通告是不生效的。

10.5.2 账号到期通告

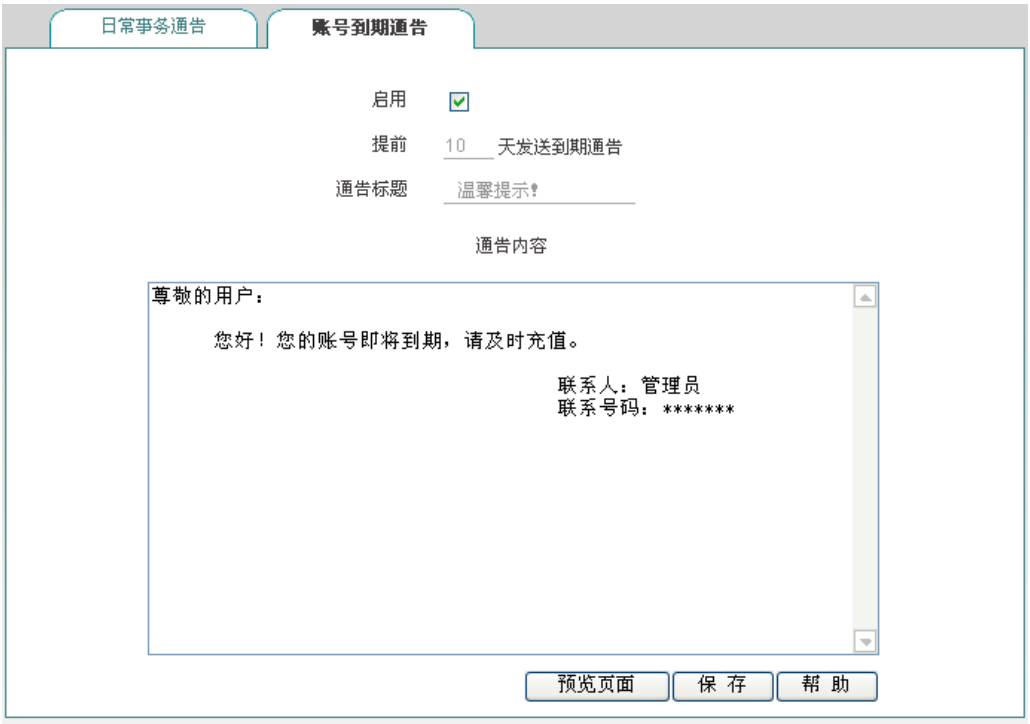

图 10-10 账号到期通告

- 启用：勾选表示启用账号到期通告功能；
- 提前发送到期通告天数：设置设备发送到期通告的有效天数，当该参数设置为 10 时，表示从账号到期前 10 天开始，当用户拨号成功，第一次访问网站时会收到设备发送的到期通告；
- 通告标题、内容：设置账号到期通告的标题及内容。
- 预览页面：点击该按钮，预览所配置的通告内容。

提示：内网拨号用户账号过期后，仍能够拨号成功，能够访问设备，但不能访问因特网；同时访问网站时会收到设备发送的到期通告。

10.6 上网行为审计

本节介绍上网行为审计功能。进入*行为管理—>上网行为审计—>日志管理*页面，如下图所示。

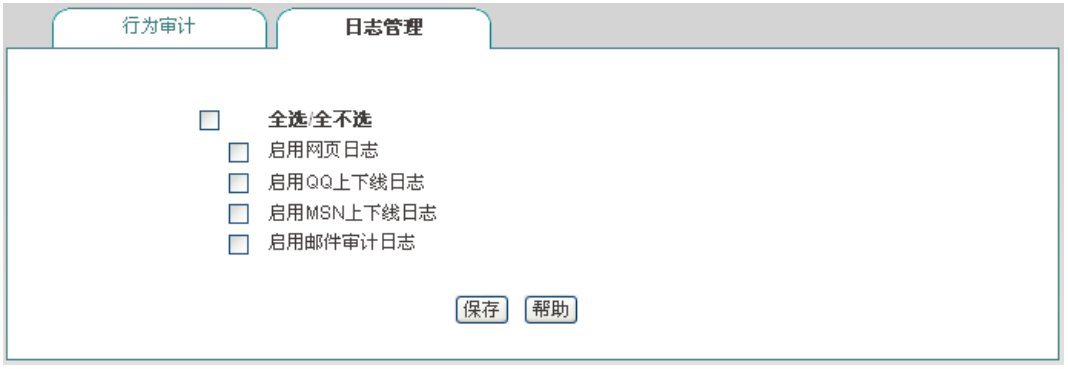

图 10-11 日志管理

- 启用网页日志：启用网页日志后，能够在***行为审计***页面查看内网用户访问网页的记录；如：“2012-07-10 14:01:22 srcip=100.100.100.23;url=www.google.com.hk”表示在 2012 年 7 月 10 日 14 时 01 分内网 IP 地址为 100.100.100.23 的用户访问了 www.google.com.hk；
- 启用 QQ 上下线日志：启用 QQ 上下线日志后，能够在***行为审计***页面查看内网用户 QQ 的上下线记录；
- 启用 MSN 上下线日志：启用 MSN 上下线日志后，能够在***行为审计***页面查看内网用户 MSN 的上下线记录；
- 启用邮件审计日志：启用邮件审计日志后，能够在***行为审计***页面查看内网用户收发邮件的记录。

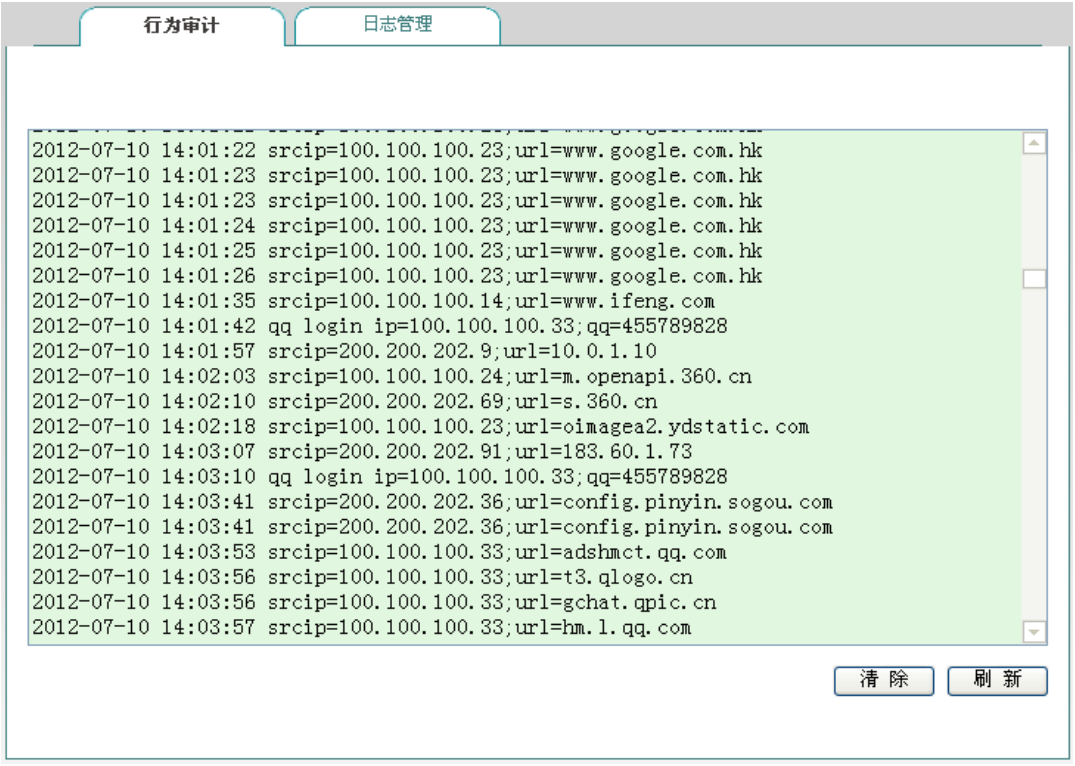

图 10-12 行为审计

注意：上网行为审计能够记录最新的 400 条日志信息。

10.7　策略库

本节介绍*行为管理—策略库*页面及操作步骤。

系统目前提供 11 种类型的策略，包括：邮件、IM、P2P、STOCK、网络视频、网络游戏、购物网站、社交网站、网页游戏、论坛、其他。用户可以通过更新某策略或全部策略，来使得引用这些策略的行为管理生效。

图 10-13 策略库信息列表

下面介绍策略库信息列表中各参数的含义。

- 名称：某策略的名称；
- 类型：某策略所属的类型，如上图中表示 QQ 属于 IM 类型；
- 说明：对某策略的详细介绍；
- 更新策略：点击<更新>能够通过 Internet 在线更新某策略。

第11章 带宽管理

本章介绍精细化限速和带宽管理功能。

11.1　精细化限速

本节介绍***带宽管理—>精细化限速***页面及配置参数的涵义。用户可以通过精细化限速功能限制内网某段地址的用户上传、下载的速率大小，从而实现带宽的合理分配与利用。

1、 精细化限速列表

进入***带宽管理—>精细化限速***页面可以在精细化限速信息列表中查看已配置的精细化限速实例信息，并可以通过“移动到”按钮调整精细化限速实例的顺序。

图 11-1 精细化限速信息列表

2、 精细化限速配置

在上图中点击<添加新条目>可以进入***精细化限速配置***页面。下面介绍配置精细化限速时各参数的涵义。

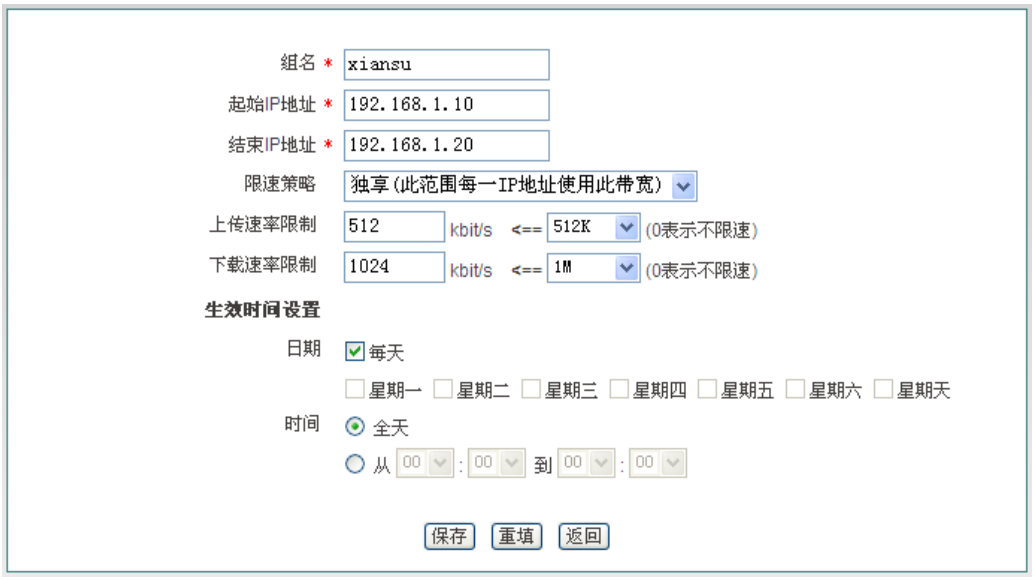

图 11-2 精细化限速配置

- 组名：自定义该条精细化限速实例的组名，不能跟其他实例名重复；
- 起始 IP 地址、结束 IP 地址：填写该精细化限速生效的地址段的起始 IP 地址和结束 IP 地址；
- 限速策略：可供的选项有独享和共享；独享表示此范围内的每一个 IP 地址使用此带宽；共享表示此范围内的 IP 地址共享此带宽；
- 上传速率限制、下载速率限制：在这里设置此范围内 IP 地址的最大上传、下载速率，0 表示不限制；
- 生效时间设置：设置此 IP 地址范围内该条精细化限速生效的时间。

11.2　弹性带宽

本节介绍*用户管理—>弹性带宽*页面及配置参数的涵义。在网络繁忙时，弹性带宽功能保证内网每个用户都能够正常上网。

- **提示：**建议不要同时启用弹性带宽功能与精细化限速功能。

图 11-3 弹性带宽配置

- 启用弹性带宽：勾选表示启用弹性带宽功能；
- WAN1 口上、下行带宽：设置从 ISP 申请的 WAN1 口的上、下行带宽。

第12章 防火墙

本章介绍如何配置设备的防火墙功能，包括安全配置、访问控制策略及域名过滤。

12.1　安全配置

本节介绍*防火墙—>安全配置*的界面及配置。

1、 内网防御

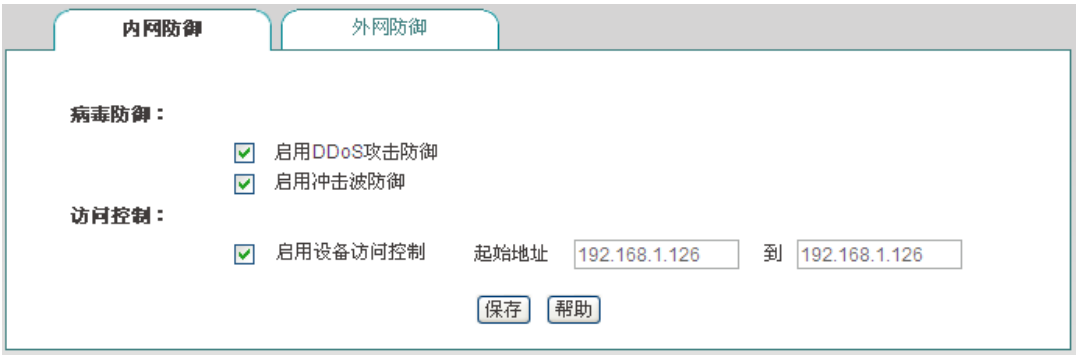

图 12-1 安全配置——内网防御

- 启用 DDoS 攻击防御：启用后，设备将有效防御内网常见的 DDOS 攻击；
- 启用冲击波防御：启用后，设备将有效防御冲击波病毒攻击；
- 启用设备访问控制：启用后，只有后续设置的 IP 地址能登录设备。

2、 外网防御

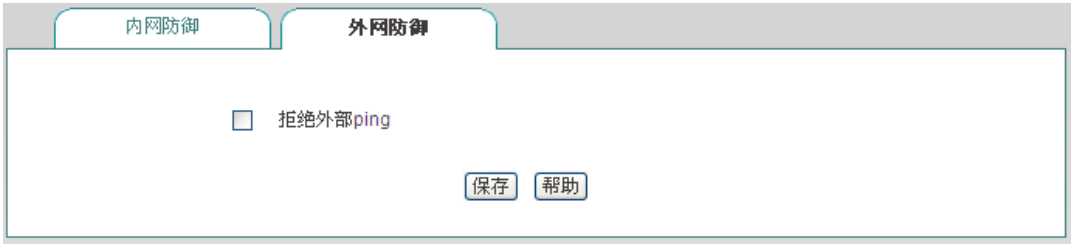

图 12-2 安全配置——外网防御

- 拒绝外部 ping：启用后，设备的 WAN 口不响应来自外网的 ping 请求。

12.2　访问控制策略

本节讲述*防火墙—>访问控制策略*的功能及配置方法。

灵活地运用访问控制功能，不仅能够为不同的用户设置不同的 Internet 访问权限，还可以控制用户不同时段的 Internet 访问权限。在实际应用中，可根据各个机构的管理规则，在设备上配置相应的访问控制策略。例如对于学校用户，可通过配置访问控制策略设置学生不能访问游戏网站；而对于家庭用户，可配置只在指定的时间内允许孩子上网；对于企业用户，可配置财务部门的机器不能被互联网访问等。

12.2.1 访问控制策略简介

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。如果配置了访问控制策略，当数据包到达设备后，它会取出此数据包的源 MAC 地址、源地址、目的地址、上层协议、端口号或数据包中的内容进行分析，并按照策略表中的顺序从上至下进行匹配，查看是否有匹配的策略，并执行匹配到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。

可以通过设置“过滤类型”指定访问控制策略的过滤类型，设备提供三种过滤类型：IP 过滤、URL 过滤以及关键字过滤。这三种类型的访问控制策略，均支持根据时间段进行过滤。

1、 IP 过滤

IP 过滤指对数据包的包头信息过滤，例如源 IP 地址和目的 IP 地址。如果 IP 头中的协议字段封装协议为 TCP 或 UDP，则再根据 TCP 头信息（源端口和目的端口）或 UDP 头信息（源端口和目的端口）执行过滤。

过滤类型为 IP 过滤时，可供设置的过滤条件包括：源 IP 地址、目的 IP 地址、协议、源端口、目的端口、动作和生效时间等。

2、 URL 过滤

URL 过滤指对 URL 网址过滤，根据 URL 中的关键字进行过滤，不仅可以控制内网用户对站点的访问，还可以控制用户对网页的访问。

过滤类型为 URL 过滤时，可供设置的过滤条件包括：源 IP 地址、过滤内容（指 URL 地址）、动作和生效时间等。

3、 关键字过滤

关键字过滤指对 HTML 页面（网页）中的关键字过滤，它的意思是如果你在某个网页里发表了包含了定义的关键字（如色情、法轮功、赌博等）的言论，将会提交不成功。

过滤类型为关键字过滤时，可供设置的过滤条件有：源地址、过滤内容（指网页中的关键字）和生效时间等。

访问控制策略的动作包括转发和丢弃，对应的“动作”分别为“允许”或“禁止”。当需要处理的数据包与某条已定义的访问控制策略相匹配时，如果该策略的“动作”是“允许”，那么设备将转发该数据包；如果该策略的“动作”是“禁止”，那么设备将丢弃该数据包。

需要注意的是，关键字过滤由于其特殊的应用性，并不提供“动作”的选择，而是默认“禁止”。

12.2.2 访问控制策略列表

拖动访问控制策略列表下方的横条，可查看详细的实例信息。

图 12-3 访问控制策略列表

- 移动到：您可以通过此按钮将实例进行相应的排序。

提示：用户定义的访问控制策略按列表中的顺序从上至下进行匹配。

12.2.3 访问控制策略配置

访问控制策略是对通过设备的数据包进行控制。在上图中点击<添加新条目>，进入***访问控制策略配置***页面，配置所需要的防火墙策略，下面将分别介绍 IP 过滤、URL 过滤以及关键字过滤这三种不同的过滤类型下访问控制策略配置中各参数的涵义，以及注意事项。

一、　访问控制策略配置—IP 过滤

图 12-4 配置访问控制策略——IP 地址过滤

- 策略名：自定义访问控制策略的名称；
- 启用该策略：启用该访问控制策略，选中表示启用，取消选中则表示禁用该策略；
- 源地址：该访问控制策略控制的内网用户；
- 动作：该访问控制策略的执行动作，选项为“允许”或“禁止”；
  - 允许：允许与该访问控制策略匹配的数据包通过，即设备将转发该数据包；
  - 禁止：禁止与该访问控制策略匹配的数据包通过，即设备将丢弃该数据包；
- 过滤类型：IP 过滤、URL 过滤、关键字过滤，这里选择“IP 过滤”；
- 协议：该访问控制策略的协议类型。供选择的协议如下：1（ICMP）、6（TCP）、17（UDP）、51（AH）、all（所有）。其中，“all（所有）”表示所有协议；附录 C 提供了常用协议号与协议名称的对照表；
- 常用服务：提供使用 TCP 协议或 UDP 协议的常用服务端口。其中，选项“所有”表示所有端口：即 1～65535 端口；

选择某个端口号（服务）后，系统自动将该端口号填充到“目的起始端口”和“目的结束端口”；特别地，若选择“所有”，则“目的起始端口”和“目的结束端口”分别填充为 1 和 65535；

附录 D 提供了常用服务端口与服务名对照表；

- 目的起始端口、目的结束端口：该访问控制策略的目的起始端口和结束端口，通过它们可以指定一段范围的目的端口。如果只定义一个目的端口，则将它们设置成同一个值，取值范围均为 1～65535；
- 目的起始地址、目的结束地址：该访问控制策略的目的起始 IP 地址和结束地址，通过它们可以指定一段范围的目的 IP 地址。如果只定义一个目的 IP 地址，则将它们设置成同一个值；
- 源起始端口、源结束端口：该访问控制策略的源起始端口和结束端口，通过它们可以指定一段范围的源端口。如果只定义一个源端口，则将它们设置为同一个值。取值范围均为 1～65535；
- 生效时间设置：访问控制策略的生效的时间，不设置为所有时间。
- **提示：**

IP 地址段默认为 0.0.0.0 到 0.0.0.0 表示对所有的客户端都生效，即对源地址无限制，包括 LAN 口地址段的客户端、PPPoE Server 地址池的客户端。

二、　访问控制策略配置——URL 过滤

图 12-5 配置访问控制策略——URL 过滤

“策略名”、“源地址”、“动作”等参数的涵义同“IP 过滤”类型中的相关参数，这里不再重述，请参考相关描述。

- 过滤类型：IP 过滤、URL 过滤、关键字过滤，这里选择“URL 过滤”；
- 过滤内容：该访问控制策略需过滤的 URL 地址。

URL 过滤是根据 URL 的关键字进行过滤的，当访问的网页的 URL 中含有与“过滤内容”完全匹配的字段时，就认为是匹配该策略的。这里可输入一个完整的域名，这时，该域名开头的所有网页都被匹配；也可输入域名的子字符串，这时，URL 中包含该子字符串的所有网页都被匹配，从而实现对某个站点的所有网页的过滤。下面，举几个例子进行说明：

例 1，如果输入 www.sina.com.cn，那么以 www.sina.com.cn 开头的所有网页都将匹配该策略，如 www.sina.com.cn/index.jsp，但是 book.sina.com.cn 开头的网页却不被匹配。

例 2，如果输入 www.utt.com.cn/bbs/，则以 www.utt.com.cn/bbs/ 开头的所有网页都将匹配该策略，从而控制对 utt 这个站点中 bbs 页面的访问。

例 3，如果输入 sina.com，那么所有出现 sina.com 和 sina.com.cn 的网页都被匹配，相当于整个 sina 站点都被匹配，当然，此时以 book.sina.com.cn 开头的网页将被匹配。

提示：

1、 URL 地址中，英文字符不区分大小写。输入 URL 时，请不要包含 http://；

2、 URL 过滤不能控制用户使用网页浏览器访问的其它服务。例如，URL 过滤不能控制对 ftp://ftp.utt.com.cn 的访问。在这种情况下，需通过配置 IP 过滤类型的访问控制策略来禁止或允许 FTP 连接。

三、 访问控制策略配置——关键字过滤

图 12-6 访问控制策略配置——关键字过滤

“策略名”、“源地址”、“动作”等参数的涵义同“IP 过滤”类型中的相关参数，这里不再重述，请参考相关描述。

- 过滤类型：IP 过滤、URL 过滤、关键字过滤，这里选择“关键字过滤”；
- 过滤内容：该访问控制策略需过滤的关键字，指网页上的关键字。

提示：

1、 对于过滤类型为“关键字”的访问控制策略，“动作”只有“禁止”这个选项；

2、 过滤的内容应除: < > , % ‘ \ “ & ; 和空格之外的字符。

12.2.4 访问控制策略配置实例

本节介绍两个访问控制实例。

一、　实例一

需求：某企业内网要求在工作时间段（周一至周五，9:00~18:00）只允许 IP 地址为 192.168.1.10-192.168.1.20 的用户使用 WEB 业务。

分析：

自定义策略 1：允许 192.168.1.10-192.168.1.20 的 DNS 应用；

自定义策略 2：允许 192.168.1.10-192.168.1.20 的 WEB 应用；

自定义策略 3：禁止 192.168.1.10-192.168.1.20 其他所有应用。

需要注意的是，（策略 3）在禁止所有服务时，也会禁止 DNS 服务，为使该地址段得得用户网络访问正常，应该将策略 3 配置在最后。

访问控制策略列表：

图 12-7 访问控制策略——实例一

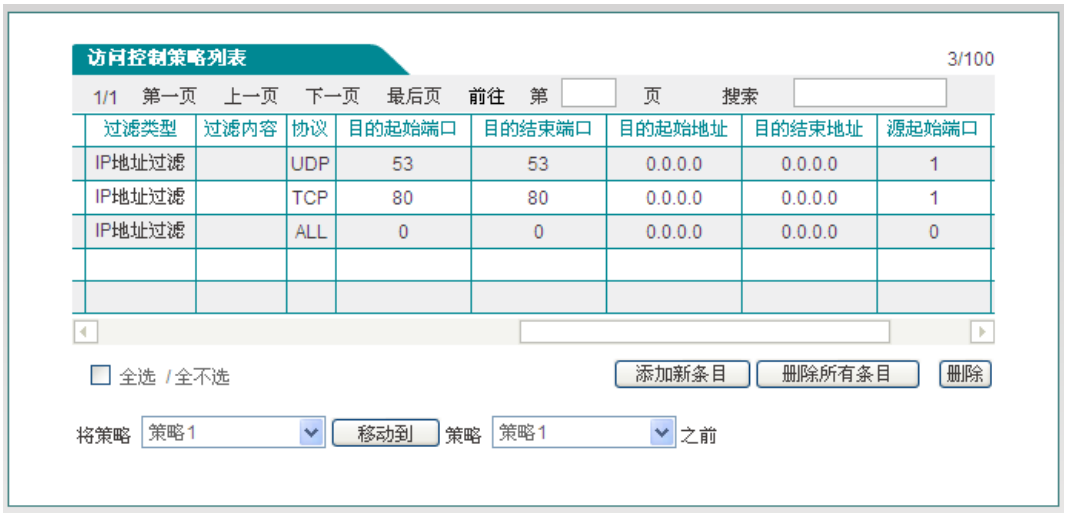

图 12-8 访问控制策略——实例一（续图 12-7）

二、　实例二

需求：某企业网要禁止 IP 地址为 192.168.1.80~192.168.1.100 的用户访问网站 http://www.bbc.com（IP 地址为 212.58.246.93）和网站 http://www.cnn.com（IP 地址为 157.166.255.18），允许该组其他所有上网业务。

分析：

配置策略 1，禁止 192.168.1.80~192.168.1.100 段用户访问 http://www.bbc.com；

配置策略 2，禁止 192.168.1.80~192.168.1.100 段用户访问 http://www.cnn.com。

图 12-9 访问控制信息列表——实例二

图 12-10 访问控制信息列表——实例一（续图 12-9）

12.3　域名过滤

本节介绍***防火墙—>域名过滤***页面的域名过滤功能，包括：域名过滤操作步骤、域名过滤配置过程中注意的事项。

图 12-11 域名过滤页面

域名过滤配置步骤：

1、 勾选“启用域名过滤”；

2、 选择该域名过滤策略的生效方式；

3、 选择该域名过滤生效的内网对象；

4、 选择该域名过滤生效的时间段；

5、 在“域名名称”对应的文本框中输入相应的域名，点击<添加新条目>按钮；相应的域名就会出现在“域名列表”中；

6、 点击<保存>。

提示：

1、 设备中支持设置 100 个域名过滤；

2、 域名过滤功能是全字匹配的，当内网用户在浏览器里输入的域名与“域名列表”中显示的域名全字匹配时，将无法访问此域名对应的网页。

3、 可以在域名名称中输入通配符“*”来实现对多个域名的过滤，例如在域名列表中输入域名名称“www.163.*”，内网用户将不能访问以“www.163.”开头的所有网页。

第13章 VPN 配置

VPN（Vitual Private Network），虚拟专用网：VPN 指的是依靠 ISP（Internet Service Provider 因特网服务提供商）和其它 NSP（Network Service Provider 网络服务提供商），在公用网络（如 Internet）中建立专用的数据通信网络的技术。

PPTP（Point-to-Point Tunneling Protocol），点到点隧道协议：PPTP 是一种虚拟专用网络协议，属于第二层的协议。PPTP 将 PPP（Point-to-Point Protocol）帧封装在 IP 数据报中，通过 IP 网络如 Internet 或企业专用 Intranet 等发送。

13.1　PPTP 概述

PPTP 协议的基本功能是在 IP 网络中传送采用 PPP 封装的用户数据包。PPTP 客户端负责接收用户的原始数据，并将之封装到 PPP 数据包，然后在 PPTP 客户端和服务器之间建立 PPTP 隧道传送该 PPP 数据包。

典型的应用通常是 PPTP 客户端部署在远程分支机构或移动办公用户的个人电脑软件中，他们用来发起 PPTP 隧道；PPTP 服务器部署在企业中心或办公室，用来接收来自 PPTP 客户端的呼叫，当建立起 PPTP 隧道连接后，PPTP 服务器接收来自 PPTP 客户端的 PPP 数据包，并还原出用户的数据包，然后把还原后的数据包发送到最终用户的电脑设备上。

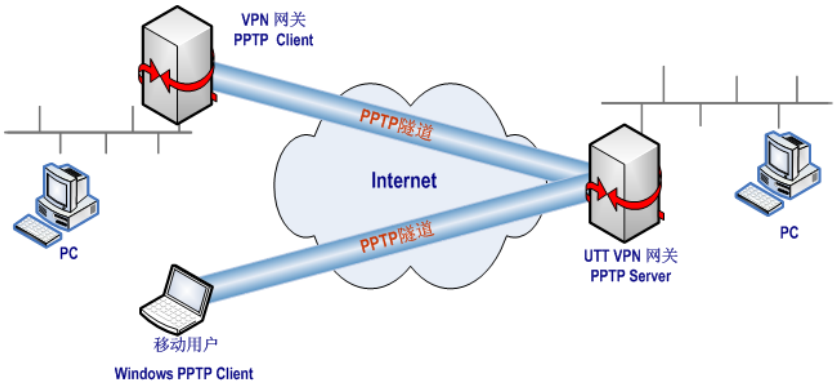

图 13-1 PPTP 典型应用

13.2　PPTP 信息列表

图 13-2 PPTP 信息列表

提示：

3、 “建立”、“挂断”按钮的操作只对客户端才生效；

4、 为保证 VPN 网关启用 NAT 后，PPTP 隧道正常连接，PPTP 配置完成之后，系统会自动生成一条 TCP 1723 端口的 NAT 静态映射（可在***高级配置—>NAT 静态映射和 DMZ*** 的“静态映射信息列表”中查看，名称为 “pptp”）。请不要编辑、删除它们，否则可能造成 PPTP 隧道无法连接和无法传输数据。

13.3　PPTP 服务端配置

进入 ***VPN 配置—>PPTP*** 页面，在如图 11-2 所示的页面点击<添加服务器>，进入 ***PPTP 服务器***页面。

13.3.1 全局配置

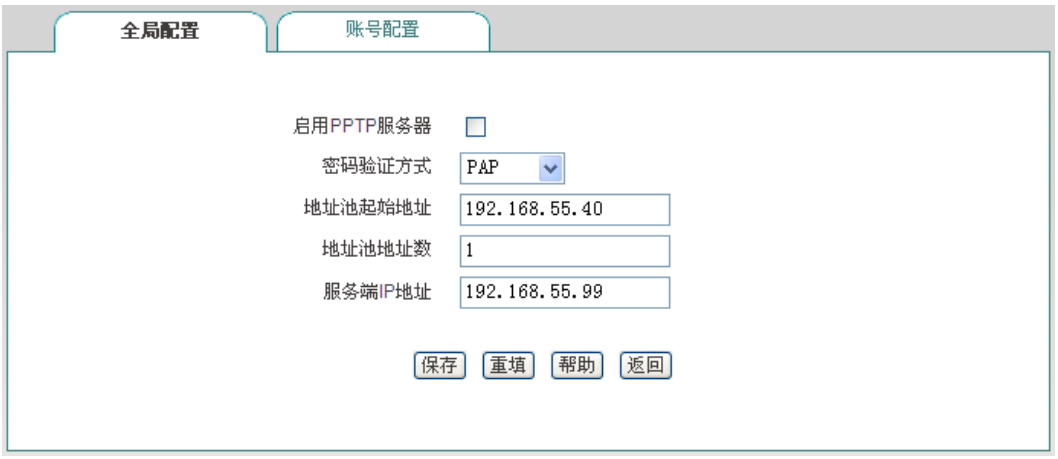

图 13-3 PPTP 服务器——全局配置

- 启用 PPTP 服务器：勾选后表示启用该服务；
- 密码验证方式：选项有 PAP、CHAP、NONE、EITHER，密码验证方式要确保两端保持一致；
- 地址池起始地址：配置 PPTP 服务器为 PPTP 客户端分配的起始 IP 地址，要确保该地址所属网段与局域网中的任何一个网段不重复；
- 地址池地址数：设置该地址池的地址总数；
- 服务端 IP 地址：隧道服务端的虚接口 IP 地址，该地址不包含在地址池中，请确认该地址与所配置的地址池在同一网段。

13.3.2 账号配置

下面介绍在 PPTP 服务端为 PPTP 客户端配置账号时的各参数的涵义。

图 13-4 PPTP 服务器——账号配置

- 隧道名称：自定义隧道名称：自定义该条隧道的名称，与设备中已有的实例名不能重复；
- 用户类型：选项有 LAN 到 LAN、移动用户；
  - LAN 到 LAN：拨入的 PPTP 用户是一个网段的用户，往往是通过一个路由器拨入，实现 PPTP 隧道两端局域网的通信；
  - 移动用户：拨入的 VPN 用户是个人用户，往往由单个计算机拨入，实现 PPTP 隧道远端计算机与本地局域网的通信；
- 用户名：自定义客户端拨号时使用的用户名；
- 密码：自定义客户端拨号时使用的密码；
- 远端内网网络地址：填写 PPTP 隧道对端局域网所使用的 IP 地址（一般可以填 VPN 隧道对端设备的 LAN 口 IP 地址）；
- 远端内网子网掩码：填写 PPTP 隧道对端局域网所使用的子网掩码。

13.4　PPTP 客户端配置

进入 ***VPN 配置—>PPTP*** 页面，在如图 13-2 所示的页面点击<添加客户端>，进入 ***PPTP 客户端***页面。下面介绍配置 PPTP 客户端各参数的涵义。

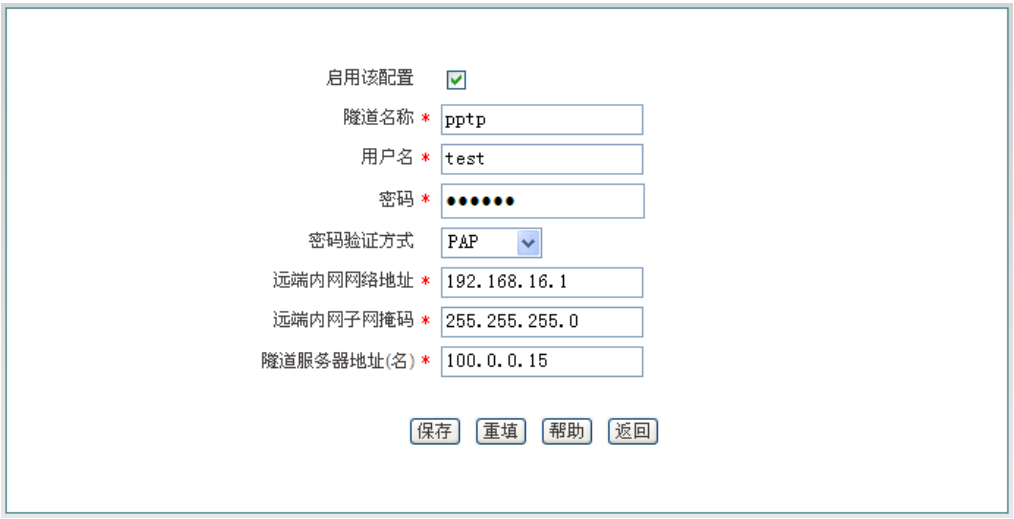

图 13-5 PPTP 客户端

- 启用该配置：勾选表示启用该配置；
- 隧道名称：该条隧道的名称，与设备中已有的实例名不能重复；
- 用户名：该条隧道拨号时用的用户名；
- 密码：该条隧道拨号时用的密码；
- 密码验证方式：设置密码的验证方式，包括：PAP、CHAP、NONE(不进行密码验证)、EITHER(自动与服务端协商密码验证方式)；密码验证方式要确保与服务端的一致；
- 远端内网网络地址：填写远端内网的 IP 地址，可填写远端 VPN 网关的 LAN 口 IP 地址；
- 远端内网子网掩码：填写远端内网的子网掩码；
- 隧道服务器地址（名）：填写远端 VPN 网关 WAN 口的 IP 地址或者域名。

13.5　PPTP 配置实例

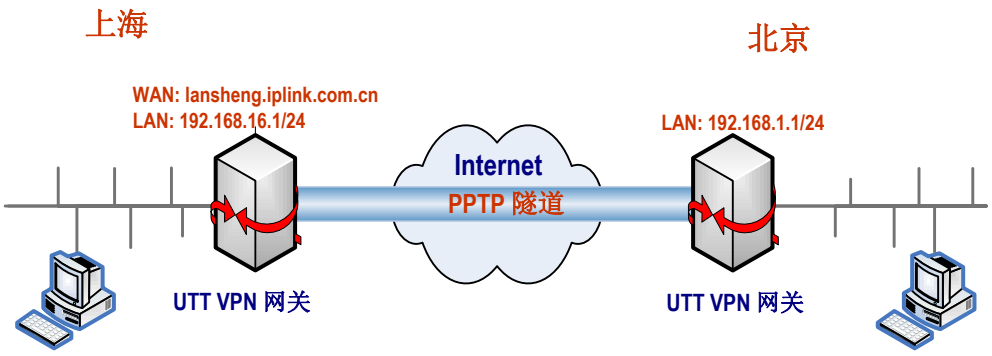

图 13-6 PPTP 实例拓扑图

在本方案中，某公司总部在上海，在北京有一个分公司。北京分公司希望可以实现两地局域网内部资源的相互访问。

本方案使用 PPTP 协议建立 VPN 隧道，两地的 VPN 网关都使用艾泰路由器（上海 VPN 网关型号：商睿 TM 3520G；北京 VPN 网关型号：进取 TM 510W，地址如下：

上海（PPTP 服务端）：

内网网段：192.168.16.0/24；

LAN 口 IP 地址：192.168.16.1/24；

WAN 口域名：lansheng.iplink.com.cn

北京（PPTP 客户端）：

内网网段：192.168.1.0/24；

LAN 口 IP 地址：192.168.1.1/24。

1、 配置上海 VPN 网关

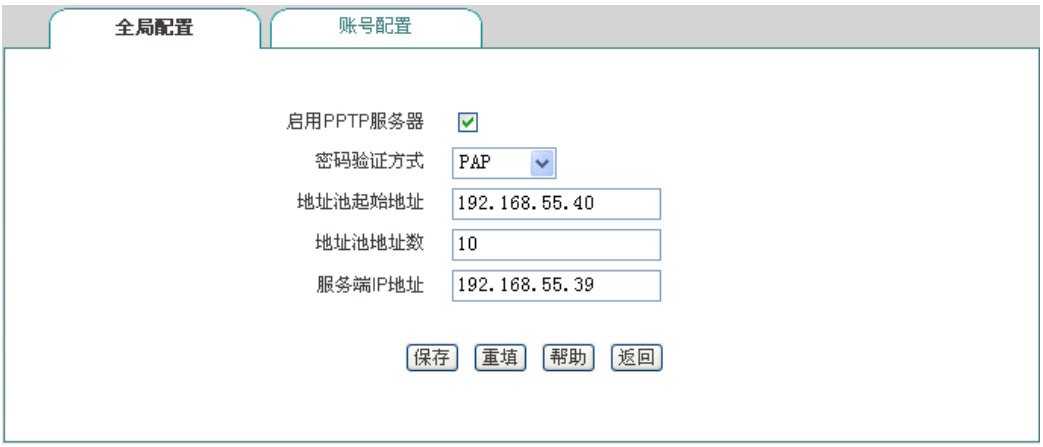

图 13-7 PPTP 服务端配置 1

图 13-8 PPTP 服务端配置 2

PPTP 服务端配置如上图所示，用户类型为：LAN 到 LAN；用户名为：pptp；密码为：123456；密码验证方式为：PAP；远端内网网络地址为：192.168.1.0；远端内网子网掩码为 255.255.255.0。

2、 配置北京 VPN 网关

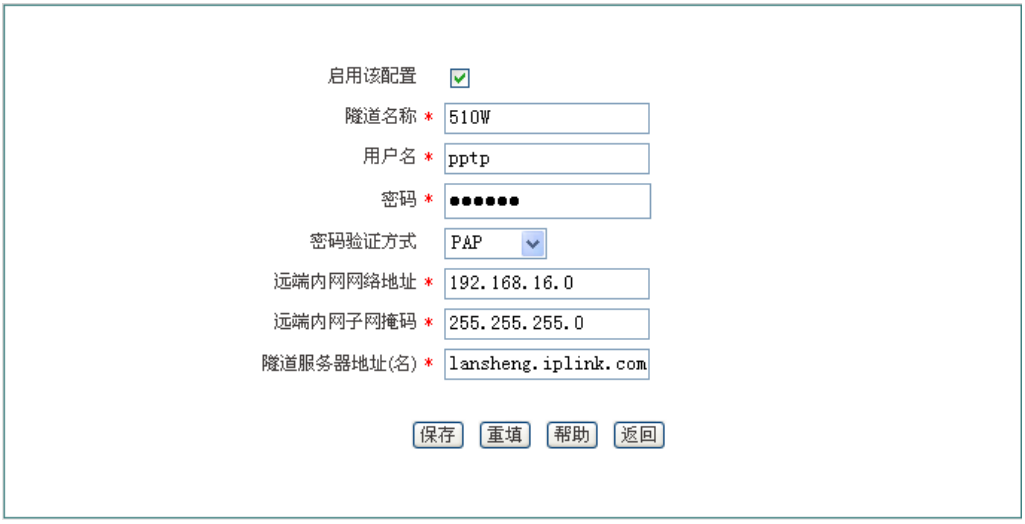

图 13-9 PPTP 客户端配置

PPTP 客户端配置如上图所示，用户名为：pptp；密码为：123456；密码验证方式为：PAP；远端内网网络地址为：192.168.16.0；远端子网掩码为：255.255.255.0，隧道服务器地址为：lansheng.iplink.com.cn。

3、 查看连接信息

分别进入相应页面，查看其 PPTP 实例连接信息。如下图所示可以查看 PPTP 实例的用户名、业务类型、会话状态、使用时间、远端内网 IP 地址/掩码等信息。

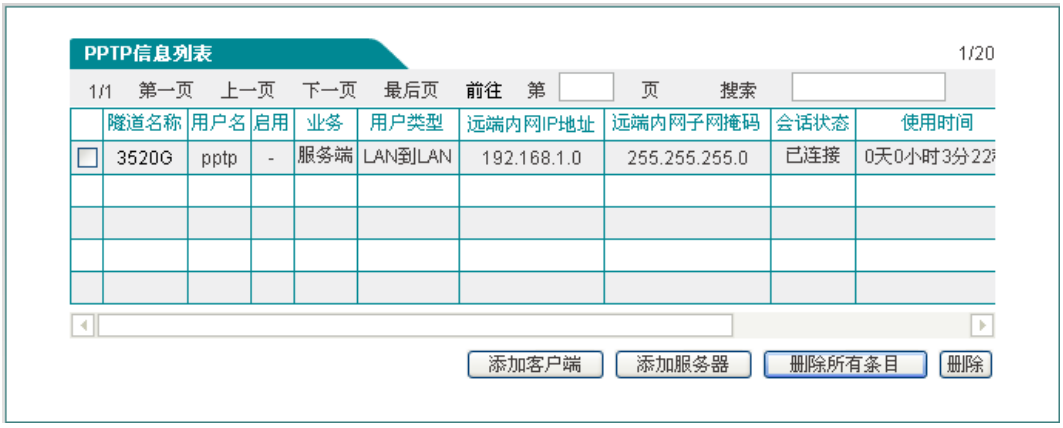

图 13-10 PPTP 服务端信息列表 1

图 13-11 PPTP 服务端信息列表 2

图 13-12PPTP 客户端信息列表 1

图 13-13 PPTP 客户端信息列表 2

第14章 系统管理

在*系统管理*主菜单中，可以进入*管理员配置*、*语言选择*、*时钟管理*、*配置管理*、*软件升级*、*远程管理*、*计划任务*页面。本章主要介绍用户如何更改管理员用户名、密码；如何设置设备的时钟；如何备份配置文件及导入配置文件；如何升级设备；如何开启远程管理等。

14.1　管理员配置

1、 管理员配置信息列表

图 14-1 管理员配置信息列表

2、 管理员配置参数介绍

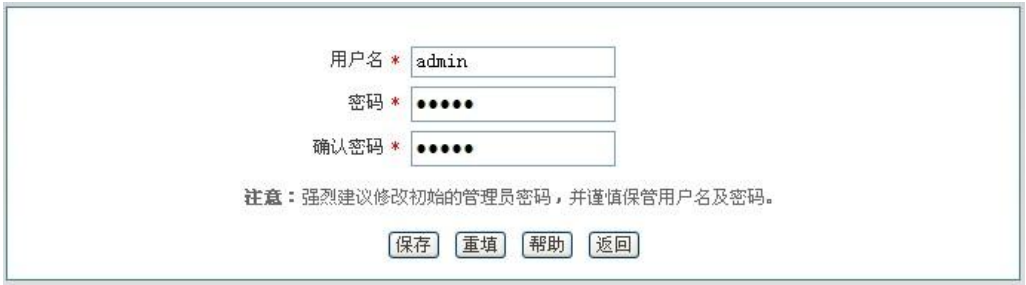

图 14-2 管理员配置

- 用户名：自定义管理员登录 WEB 界面的用户名；
- 密码、确认密码：自定义管理员登录 WEB 管理界面的密码。

3、 管理员用户名、密码出厂值修改

为安全起见，强烈建议修改初始的管理员用户名及密码，并谨慎保管。

进入*系统管理—>管理员配置*页面，点击用户名为“admin”的编辑图标，进入配置页面修改出厂值的登录用户名及密码。修改后，您必需使用新的用户名、密码登录设备。

14.2　语言选择

本节介绍*系统管理—>语言选择*页面。通过在此页面的配置选择设备 WEB 界面的语言。

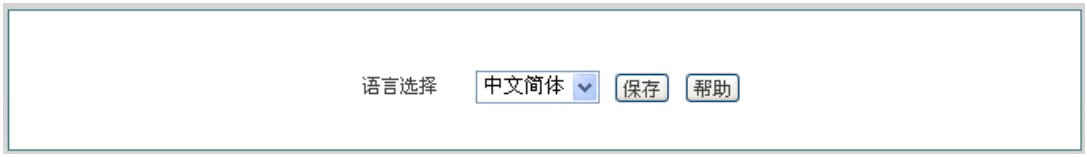

图 14-3 语言选择

14.3　时钟管理

本节讲述*系统管理—>时钟管理*页面。

为了保证设备各种涉及到时间的功能正常工作，需要准确地设定设备的时钟，使其与当地标准时间同步。

设备提供“手工设置时间”和“网络时间同步”两种设置系统时间的方式，一般建议使用“网络时间同步”功能来从互联网上获取标准的时间，当下次开机连接到 Internet 后，设备将会自动获得标准的时间。

图 14-4 时钟管理

- 当前系统时间：显示设备当前的日期和时间信息（单位：年:月:日，时:分:秒）；
- 时区选择：选择设备所在地的国际时区，只有选择了正确的时区，网络时间同步功能才能正常工作；
- 手工设置时间：手工输入当前的日期和时间（单位：年:月:日，时:分:秒）；
- 网络时间同步：使用网络时间同步功能，设置了正确的 ntp 服务器后，当设备连接

到 Internet 之后，就会自动和所设置 ntp 服务器同步时间。系统缺省预设两个 ntp 服务器地址为 192.43.244.18、129.6.15.28，一般情况下不需要修改。若需了解更多 ntp 知识及服务器，可访问 http://www.ntp.org。

提示：设备的时钟建议设置为网络时间同步，只有系统的时间配置正确，如防火墙等和时间有关系的配置才会正常生效！

14.4　配置管理

本节介绍***系统管理—>配置管理***的配置方法。在本页面，您可以备份当前配置文件到本地，导入新配置文件到设备，恢复设备出厂配置。

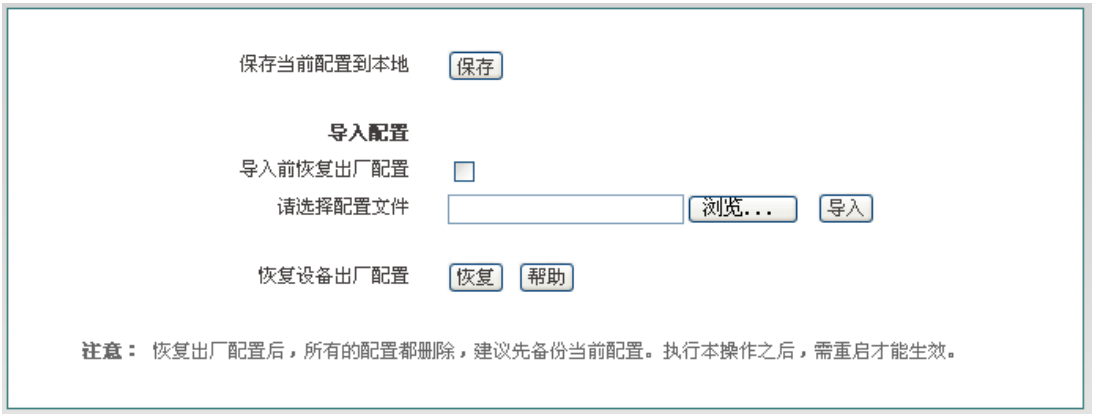

图 14-5 配置管理

1、 备份配置文件

在上图中点击<保存>，即可将设备的配置文件备份到本地 PC 上，配置文件的格式为.xml。

2、 配置文件导入

在上图中先点击<浏览…>，选择保存在本地 PC 上的配置文件。再点击<导入>。如果已勾选“导入前恢复出厂配置”复选框，则点击<导入>后，设备将先恢复到出厂配置。

提示：在加载配置过程中请不要关闭设备电源，以避免不可预期的错误。

3、 恢复设备出厂配置

如果用户需要将设备恢复到出厂时的配置，请进入***系统管理—>配置管理***页面，点击<恢复>。

提示：

1、 恢复设备出厂配置将删除所有自定义的配置。强烈建议在恢复出厂配置之前，先备份其配置文件。

2、 设备的出厂管理员用户名和密码均为：admin，默认 LAN 口 IP 地址/子网掩码为：192.168.1.1/ 255.255.255.0。

3、 点击<恢复>后，需重启设备，设备才会恢复到出厂时的配置。

14.5　软件升级

本节介绍***系统管理—>软件升级***页面及软件升级步骤。在本页面，您可以查看当前运行版本信息，并能从艾泰科技官方网站下载最新软件。

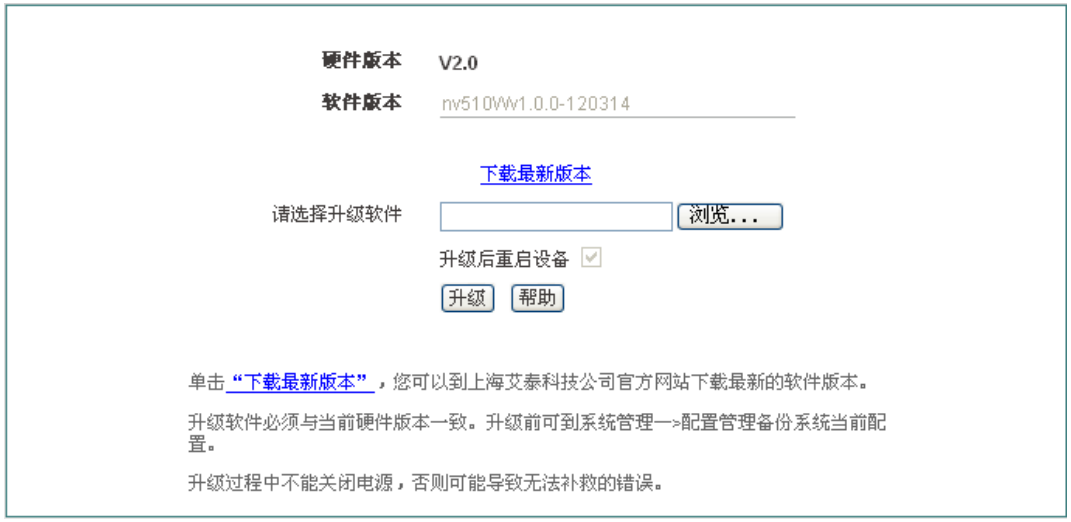

图 14-6 软件升级

- 版本信息：显示设备当前使用的硬件版本、软件版本信息；
- 下载最新版本：链接到艾泰科技官方网站下载最新版本的软件。

升级步骤：

第一步　下载最新软件

点击“下载最新版本”超链接，到上海艾泰科技有线公司官方网站下载最新的软件版本到本地计算机。

提示：

1、 请选择合适型号的最新软件；下载的软件适用的硬件版本必须和当前产品的硬版本一致；

2、 建议升级之前，先到***系统管理—>配置管理***备份系统当前配置。

第二步　选择升级软件所在路径

在“请选择升级文件”文本框中输入将要升级的软件在本地计算机的路径，或者是通过点击<浏览…>选择在本地计算机上的新软件。

第三步　更新设备的软件

选择软件后，点击<升级>，更新设备的软件。

提示：

1、 强烈建议在设备负载比较轻（用户比较少）的情况下升级；

2、 定期的升级设备的软件，可以使设备获得更多的功能或者更佳的工作性能。正确的软件升级并不会改变当前设备配置；

3、 升级过程不能关闭设备电源，否则将会导致不可预期的错误甚至不可恢复的硬件损坏。

4、 升级完成后软件会自动重启并生效，无须人工干预。

14.6　远程管理

本节介绍***系统管理—>远程管理***页面。在本页中为方便远程管理员进行网络维护，您可在***系统管理—>远程管理***页面配置设备的远程管理功能。

图 14-7 远程管理

- 启用 Http：允许或禁止从 Internet 通过 WEB 界面管理设备，设备默认 WEB 管理外部端口为 8081 。如要从 Internet 通过 WEB 管理设备必须用“IP 地址:端口”的方式（例如 http://218.21.31.3:8081）才能登录设备行；
- 外部端口：可以修改设备默认外部端口（默认值为 8081）。注意，这个端口修改成 80 以后，在***高级配置—>NAT 和 DMZ 配置***的“NAT 静态映射列表”中，就会增加一条 TCP80 端口的映射，此时如需要再次增加内网 WEB 服务器的映射，就会引起冲突。

提示：

1、 设备的 Internet 地址可以从***网络参数—>WAN 口配置***的“线路连接信息列表”中获知；

2、 如果“WAN1”采用 PPPoE 拨号，其 IP 地址是动态的，可在***网络参数—>DDNS 配置***中配置 DDNS 功能；

3、 为安全起见，如非必要，请不要启用远程管理功能；在寻求艾泰科技客服工程师服务之前，请事先打开远程管理功能。

14.7　计划任务

本节介绍*系统管理—>计划任务*页面。通过配置计划任务，管理员可以预定义设备在规定的时间里完成规定的动作。

1、 计划任务列表

计划任务列表为可编辑列表。您可以对列表中各实例进行操作。

图 14-8 计划任务列表 1

图 14-9 计划任务列表 2

2、 计划任务参数介绍

图 14-10 计划任务配置

- 任务名：自定义任务名称；
- 启动类型：表示时间周期，可选项有：每星期、每天、每小时、每分钟；
- 运行时间：表示执行这个计划任务的具体时间，它的设置根据启动类型不同而不同；
- 任务内容：选择相应的任务内容。

第15章 系统状态

在系统状态中，您可以方便地查看设备的运行状态，查看设备的相关系统信息及历史记录。

15.1　运行状态

本节介绍的运行状态页面同第 5 章《运行状态》，所以这里不再介绍此页面。

15.2　系统信息

通过***系统状态—>系统信息***页面，网络管理员能了解系统的相关信息及查看系统的相关历史记录；通过系统信息网络管理员能及时了解网络发生的或潜在的问题，进而有利于网络性能的提高、增强网络安全。

图 15-1 系统信息

- 系统当前时间：显示设备当前的日期和时间信息（单位：年:月:日，时:分:秒）；
- 系统运行时间：显示设备本次启动至查看时刻的时间；
- CPU 占用：显示当前 CPU 占用的百分比；
- 内存使用：显示当前内存使用的百分比；
- 序列号：产品的内部序列号（和表面序列号可能不同）；
- 产品型号：显示设备的产品型号；
- 硬件版本：显示设备的硬件版本号；
- 软件版本：显示设备的软件版本号；
- 历史记录：在该处可以查看系统记录的相关信息；
- 刷新：单击<刷新>，可查看最新的系统信息。

提示：

图 15-1 中的 CPU、内存的使用率不同，显示的颜色不同：

- 使用率隶属[0 ， 50%)时，是绿色；
- 使用率隶属在[50% ， 70%)时，是橙色；
- 使用率隶属在[70% ， 100]时，是红色。

第16章 客户服务

在客户服务页面，您可以快捷地链接到艾泰科技公司官方网站的 UTTCare、产品讨论、知识库、预约服务等栏目，以便您更快的了解艾泰科技服务体系，享受艾泰科技提供的贴心服务。

图 16-1 客户服务

如图 16-1，单击图中各个“了解更多”超链接，即可分别链接到艾泰科技公司官方网站对应栏目：

- **UTTCare**——链接到艾泰科技官方网站的客户服务页面，提供全面的客户服务和技术支持；
- **产品讨论**——链接到艾泰科技官方网站讨论区，参与产品的讨论；
- **知识库**——链接到艾泰科技官方网站的知识库，查找相关技术资料；
- **预约服务**——链接到艾泰科技官方网站预约服务页面，提前预约某一个工作时段的客户服务。

附录A FAQ

A-1 内网 Windows XP 系统的计算机如何无线接入设备？

步骤一、正确配置计算机的 TCP/IP

1、 右键单击“网上邻居”选择“属性”；

2、 进入“网络连接”页面，右键单击“无线网络连接”选择“属性”；

3、 双击“Internet 协议（TCP/IP）”，进入“Internet 协议（TCP/IP）属性”页面；

4、 设置 PC 的 IP 地址；IP 地址为 192.168.1.X（X 取 2~254 中任意一个）、子网掩码为 255.255.255.0、默认网关为 192.168.1.1（设备 LAN 口 IP 地址）、DNS 服务器地址由运营商提供；如果确认无线设备开启了 DHCP 服务器功能则选择“自动获得 IP 地址”；

5、 选择“使用下面的 DNS 服务器地址”选项，在“首选 DNS 服务器”中输入 ISP 所提供的 DNS 服务器的 IP 地址（可向 ISP 询问），“备用 DNS 服务器”可选填，当首选 DNS 无法连接时，设备会自动使用备用 DNS 服务器；如果无线设备开启了 DHCP 服务器功能则可以选择“自动获得 DNS 服务器地址”。

6、 单击<确定>，TCP/IP 属性配置成功。

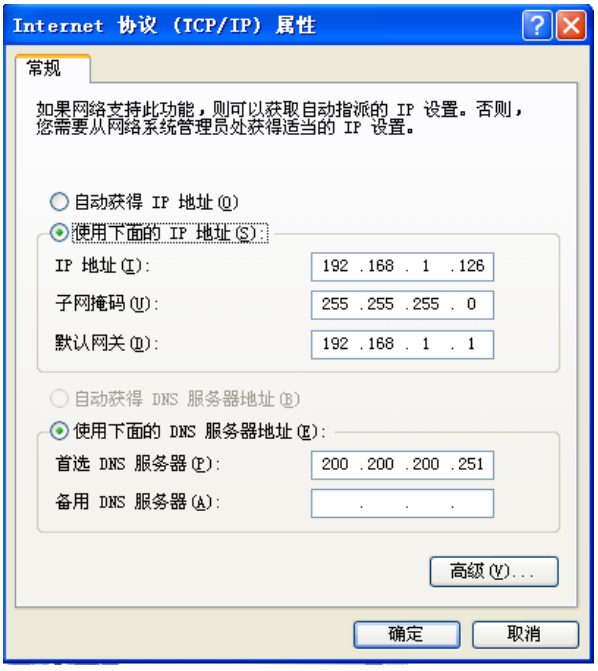

图 A-1 配置计算的 TCP/IP 属性（XP）

步骤二、连接到无线网络

1、 无线网卡启用后，点击桌面右下角的图标；

2、 在弹出的网络连接列表中，选择要进行连接的无线网络，并点击<连接>；

图 A-2 建立无线连接（XP）

3、 当条目右上角显示“已连接上”时表示内网 PC 已经连接到无线网络。

图 A-3 无线连接建立成功（XP）

A-2 内网 Windows 7 系统的计算机如何无线接入设备？

步骤一、正确配置计算机的 TCP/IP

1、 进入“开始—>控制面板—>网络和 Internet—>网络和共享中心—>更改适配器设置”页面；

7、 右键点击“无线网络连接”选择“属性”；

8、 双击“Internet 协议版本 4（TCP/IPv4）”，进入“Internet 协议版本 4（TCP/IPv4）属性”页面；

9、 设置 PC 的 IP 地址；IP 地址为 192.168.1.X（X 取 2~254 中任意一个）、子网掩码为 255.255.255.0、默认网关为 192.168.1.1（设备 LAN 口 IP 地址）、DNS 服务器地址由运营商提供；如果确认无线设备开启了 DHCP 服务器功能则选择“自动获得 IP 地址”；

10、 选择“使用下面的 DNS 服务器地址”选项，在“首选 DNS 服务器”中输入 ISP 所提供的 DNS 服务器的 IP 地址（可向 ISP 询问），“备用 DNS 服务器”可选填，当首选 DNS 无法连接时，设备会自动使用备用 DNS 服务器；如果无线设备开启了 DHCP 服务器功能则可以选择“自动获得 DNS 服务器地址”；

11、 单击<确定>，TCP/IP 属性配置成功。

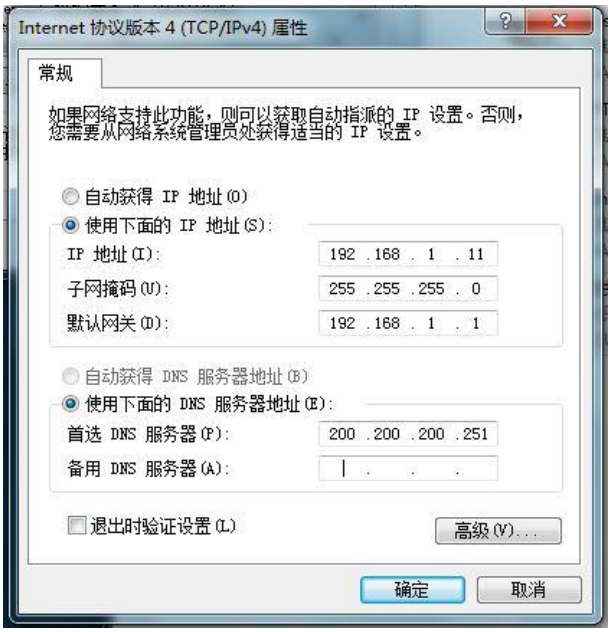

图 A- 4 配置计算机的 TCP/IP 属性（Win 7）

步骤二、连接到无线网络

1、无线网卡安装完成后，点击桌面右下角的图标；

2、在弹出的网络连接列表中，选择要进行连接的无线网络，并点击<连接>；

图 A- 5 建立无线连接（Win 7）

4、 当条目右上角显示“已连接上”时表示计算机已经连接到无线网络。

图 A- 6 无线连接建立成功（Win 7）

A-3 设备作为无线客户端，为什么无法建立无线连接？

在确认设备供电正常、物理连接正常后，请检查网络中无线设备以下配置：

1、 无线客户端设置的“AP 的 SSID”值是否与上联无线设备的 SSID 一致；

2、 无线客户端设置的“AP 的 MAC”值是否与上联无线设备的 MAC 地址一致；

3、 无线客户端设置的安全模式及密钥是否与上联无线设备设置的一致；

4、 上联设备是否已经开启无线功能，且为 AP 模式。

A-4 如何将设备恢复到出厂配置？

提示：下述方法将删除设备原来所有配置，请谨慎使用。

情况一：知道管理员密码

正常情况下，可直接进入***系统管理—>配置管理***页面，点击<恢复>且重启设备，即可恢复出厂值。

情况二：忘记管理员密码

如果忘记了管理员密码，将无法进入 WEB 界面，此时只能使用 Reset 按钮来恢复出厂配置。操作方法为：在设备带电运行过程中，按住 Reset 按钮 5 秒钟以上，再松开此按钮，设备将恢复到出厂配置，并自动重启。

附录B 十六进制 ASCII 码表

字符	回车	ESC	空格	!	"	#	$	%	&	’	(	)	*	+	,
ASCII 码	0D	1B	20	21	22	23	24	25	26	27	28	29	2A	2B	2C
字符	-	.	/	0	1	2	3	4	5	6	7	8	9	:	;
ASCII 码	2D	2E	2F	30	31	32	33	34	35	36	37	38	39	3A	3B
字符	<	=	>	?	@	A	B	C	D	E	F	G	H	I	J
ASCII 码	3C	3D	3E	3F	40	41	42	43	44	45	46	47	48	49	4A
字符	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
ASCII 码	4B	4C	4D	4E	4F	50	51	52	53	54	55	56	57	58	59
字符	Z	[	\	]	^	-	a	b	c	d	e	f	g	h	i
ASCII 码	5A	5B	5C	5D	5E	5F	61	62	63	64	65	66	67	68	69
字符	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
ASCII 码	6A	6B	6C	6D	6E	6F	70	71	72	73	74	75	76	77	78
字符	y	z	{	|	}	~									
ASCII 码	79	7A	7B	7C	7D	7E									

附录C 常用 IP 协议

协议	协议号	全称
IP	0	Internet Protocol
ICMP	1	Internet Protocol Message Protocol
IGMP	2	Internet Group Management
GGP	3	Gateway-Gateway Protocol
IPINIP	4	IP in IP Tunnel Driver
TCP	6	Transmission Control Protocol
EGP	8	Exterior Gateway Protocol
IGP	9	Interior Gateway Porotocl
PUP	12	PARC Universal Packet Protocol
UDP	17	User Datagram Protocl
HMP	20	Host Monitoring Protocol
XNS-IDP	22	Xerox NS IDP
RDP	27	Reliable Datagram Protocol
GRE	47	General Routing Encapsulation
ESP	50	Encap Security Payload
AH	51	Authentication Header
RVD	66	MIT Remote Virtual Disk
EIGRP	88	Enhandced Interior Gateway Routing Portocol
OSPF	89	Open Shortest Path First

附录D 常用服务端口

服务	端口号	协议	描述
echo	7	tcp	
echo	7	udp	
discard	9	tcp	
discard	9	udp	
systat	11	tcp	Active users
systat	11	udp	Active users
daytime	13	tcp	
daytime	13	udp	
qotd	17	tcp	Quote of the day
qotd	17	udp	Quote of the day
chargen	19	tcp	Character generator
chargen	19	udp	Character generator
ftp-data	20	tcp	FTP, data
ftp	21	tcp	FTP. control
telnet	23	tcp	
smtp	25	tcp	Simple Mail Transfer Protocol
time	37	tcp	timserver
time	37	udp	timserver
rlp	39	udp	Resource Location Protocol
nameserver	42	tcp	Host Name Server
nameserver	42	udp	Host Name Server
nicname	43	tcp	whois
domain	53	tcp	Domain Name Server
domain	53	udp	Domain Name Server
bootps	67	udp	Bootstrap Protocol Server
bootpc	68	udp	Bootstrap Protocol Client

tftp	69	udp	Trivial File Transfer
gopher	70	tcp	
finger	79	tcp	
http	80	tcp	World Wide Web
kerberos	88	tcp	Kerberos
kerberos	88	udp	Kerberos
hostname	101	tcp	NIC Host Name Server
iso-tsap	102	tcp	ISO-TSAP Class 0
rtelnet	107	tcp	Remote Telnet Service
pop2	109	tcp	Post Office Protocol - Version 2
pop3	110	tcp	Post Office Protocol - Version 3
sunrpc	111	tcp	SUN Remote Procedure Call
sunrpc	111	udp	SUN Remote Procedure Call
auth	113	tcp	Identification Protocol
uucp-path	117	tcp	
nntp	119	tcp	Network News Transfer Protocol
ntp	123	udp	Network Time Protocol
epmap	135	tcp	DCE endpoint resolution
epmap	135	udp	DCE endpoint resolution
netbios-ns	137	tcp	NETBIOS Name Service
netbios-ns	137	udp	NETBIOS Name Service
netbios-dgm	138	udp	NETBIOS Datagram Service
netbios-ssn	139	tcp	NETBIOS Session Service
imap	143	tcp	Internet Message Access Protocol
pcmail-srv	158	tcp	PCMail Server
snmp	161	udp	
snmptrap	162	udp	SNMP trap
print-srv	170	tcp	Network PostScript
bgp	179	tcp	Border Gateway Protocol
irc	194	tcp	Internet Relay Chat Protocol

ipx	213	udp	IPX over IP
ldap	389	tcp	Lightweight Directory Access Protocol
https	443	tcp	MCom
https	443	udp	MCom
microsoft-ds	445	tcp	
microsoft-ds	445	udp	
kpasswd	464	tcp	Kerberos (v5)
kpasswd	464	udp	Kerberos (v5)
isakmp	500	udp	Internet Key Exchange
exec	512	tcp	Remote Process Execution
biff	512	udp	
login	513	tcp	Remote Login
who	513	udp	
cmd	514	tcp	
syslog	514	udp	
printer	515	tcp	
talk	517	udp	
ntalk	518	udp	
efs	520	tcp	Extended File Name Server
router	520	udp	route routed
timed	525	udp	
tempo	526	tcp	
courier	530	tcp	
conference	531	tcp	
netnews	532	tcp	
netwall	533	udp	For emergency broadcasts
uucp	540	tcp	
klogin	543	tcp	Kerberos login
kshell	544	tcp	Kerberos remote shell
new-rwho	550	udp	

remotefs	556	tcp	
rmonitor	560	udp	
monitor	561	udp	
ldaps	636	tcp	LDAP over TLS/SSL
doom	666	tcp	Doom Id Software
doom	666	udp	Doom Id Software
kerberos-adm	749	tcp	Kerberos administration
kerberos-adm	749	udp	Kerberos administration
kerberos-iv	750	udp	Kerberos version IV
kpop	1109	tcp	Kerberos POP
phone	1167	udp	Conference calling
ms-sql-s	1433	tcp	Microsoft-SQL-Server
ms-sql-s	1433	udp	Microsoft-SQL-Server
ms-sql-m	1434	tcp	Microsoft-SQL-Monitor
ms-sql-m	1434	udp	Microsoft-SQL-Monitor
wins	1512	tcp	Microsoft Windows Internet Name Service
wins	1512	udp	Microsoft Windows Internet Name Service
ingreslock	1524	tcp	
l2tp	1701	udp	Layer Two Tunneling Protocol
pptp	1723	tcp	Point-to-point tunnelling protocol
radius	1812	udp	RADIUS authentication protocol
radacct	1813	udp	RADIUS accounting protocol
nfsd	2049	udp	NFS server
knetd	2053	tcp	Kerberos de-multiplexor
man	9535	tcp	Remote Man Server

附录E 图索引