路由交换一体机

高级配置手册

版本：V1.0

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。

遵守所生效的版权法是用户的责任。在未经上海艾泰科技有限公司明确书面许可的情况下，不得对本文档的任何部分进行复制、将其保存于或引进检索系统；不得以任何形式或任何方式（电子、机械、影印、录制或其他可能的方式）进行商品传播或用于任何商业、赢利目的。

上海艾泰科技有限公司拥有本文档所涉及主题的专利、专利申请、商标、商标申请、版权及其他知识产权。在未经上海艾泰科技有限公司明确书面许可的情况下，使用本文档资料并不表示您有使用有关专利、商标、版权或其他知识产权的特许。

艾泰®、UTT®文字及相关图形是上海艾泰科技有限公司的注册商标。

HiPER®文字及其相关图形是上海艾泰科技有限公司的注册商标。

此处所涉及的其它公司、组织或个人的产品、商标、专利，除非特别声明，归各自所有人所有。

产品编号（PN）：0900-0312-001
文档编号（DN）：PR-PMMU-1104.42-PPR-CN-1.0A

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：商睿™ 3520G。

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。

另外，由于各型号产品软件规格存在一定差异，所有涉及产品规格的问题请咨询艾泰科技有限公司客户服务部。

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：删除列表中说有的配置实例；

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。

本系列产品 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、最后一页。
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，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	勾选后，当前页面所有条目全部被选中；全选情况下，再单击该方框，当前页面所有条目全部未被选中。
添加新条目	单击此按钮可进入 ***NAT 静态映射配置***页面添加新实例。
删除所有条目	单击此按钮，可删除表中所有实例。
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”按钮，可删除选中的条目。

表 0-1 列表基本功能

0.4 出厂配置

1. 接口的出厂配置如表 0-2 所示。

接口类型	IP 地址/子网掩码
LAN 口	192.168.1.1/255.255.255.0
WAN 口	动态 IP 接入

表 0-2 接口出厂配置

2. 系统管理员的出厂用户名为 admin，出厂密码为 admin（区分大小写）。

0.5 内容简介

本操作手册介绍艾泰科技 ReOS_SE 软件平台路由交换一体机设备的各功能的配置及应用，主要包括：产品概述、硬件安装、配置向导、开始菜单、网络参数、高级配置、交换功能、用户管理、防火墙、VPN 配置、联动管理、系统管理、系统状态和客户服务。

第 1 章 产品概述

主要介绍艾泰科技路由交换一体机的特点及功能特性。

第 2 章 硬件安装

主要介绍艾泰科技路由交换一体机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”快速配置路由交换一体机，完成最基本的上网配置。

第 5 章 开始菜单

通过导航条“开始”菜单可以快速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——可查看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 WAN 口；
- 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 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；

- IP/MAC 绑定——配置 IP/MAC 绑定用户，防止 IP 地址盗用；
- 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；
- PPPoE 服务器——配置 PPPoE 服务器、PPPoE 账号；
- 网络尖兵防御——配置设备的网络尖兵防御功能。

第 8 章 交换功能

主要介绍产品的交换功能，包括：

- 端口管理——查看设备各端口的连接状态，配置设备各端口的工作模式、允许最大帧，是否开启流控功能等；
- 端口镜像——配置设备的端口镜像功能；
- 端口 VLAN——配置设备的端口 VLAN 功能；
- 端口汇聚——配置设备的端口汇聚功能。

第 9 章 用户管理

介绍设备的用户管理功能，包括：

- 上网行为管理——定义内网用户的上网行为；
- 策略库——更新上网行为管理引用的策略；
- 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 10 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——禁止内网用户访问某些指定的域名。

第 11 章 VPN 配置

介绍 PPTP 配置参数及如何建立 PPTP 隧道。

第 12 章 联动管理

介绍设备的联动管理功能，包括：

- 联动管理——联动管理同一广播域中的交换设备；
- 联动配置——联动获取同一广播域中交换机的配置文件；
- 网络拓扑——通过该功能可以查看网络的拓扑图。

第 13 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 14 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；
- 用户状态——查看连接到设备的内网用户信息；
- 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 15 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 配置局域网中计算机——提供配置局域网计算机的 TCP/IP 属性的方法；
- 附录 B FAQ——提供常见问题解答；
- 附录 C 常用 IP 协议号——提供常用 IP 协议号与协议名对照表；
- 附录 D 常用服务端口号——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

感谢您选用上海艾泰科技有限公司的网络产品！

本章主要讲述艾泰科技 ReOS_SE 软件平台路由交换一体机的功能和特点。

1.1 关键特性

- 支持 DSL、FTTX+LAN 和 Cable Modem 等多种接入方式
- 支持流量负载均衡以及线路备份
- 支持 DHCP 服务器功能
- 支持智能带宽管理功能
- 支持精细化限速
- 支持虚拟服务器和 DMZ
- 支持内网 PPPoE 服务器用户认证
- 支持对用户的上网行为管理，提供丰富的管控策略
- 支持 URL、MAC 地址、关键字过滤等防火墙策略
- 支持内/外网攻击防御
- 支持网络尖兵防御
- 支持 VPN 功能
- 支持动态域名（3322.org、iplink.com.cn）
- 支持端口 VLAN 的划分
- 支持端口镜像功能
- 支持端口汇聚功能
- 支持联动管理功能
- 支持网络拓扑发现功能
- 支持 WEB 升级方式
- 支持 WEB 配置文件备份与导入
- 支持 HTTP 远程管理

1.2 产品规格

- 符合 IEEE802.3Ethernet、IEEE802.3u Fast Ethernet、IEEE802.3ab 以及 IEEE802.3z

标准

- 支持 TCP/IP、PPPoE、DHCP、ICMP、NAT、静态路由等协议
- 各个物理端口均支持自动协商功能
- 各个物理端口支持 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

本章先概要的介绍 ReOS SE 软件平台路由交换一体机的指示灯、接口等，然后讲述如何安装这些设备。

2.1 面板介绍

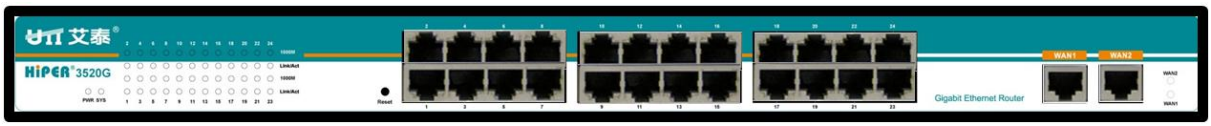

图 2-1 商睿™ 3520G 前面板

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。
Link/Act	LAN 口状态指示灯	当有设备正常连接到某 LAN 口后，该端口对应指示灯常亮，该端口有流量时闪烁。
1000M	LAN 口速率指示灯	当有设备连接到 LAN 口，且 1000M 协商成功后，该端口对应指示灯常亮。
WAN	WAN 口状态指示灯	当有设备正常连接到某 WAN 口后，该端口对应指示灯常亮，该端口有流量时闪烁。

表 2-1 指示灯说明

2. 接口说明

接口	涵义	说明	备注
LAN	局域网接口	集成多个交换式以太网口	LAN/WAN 都为 RJ-45 端口，支持正反线自适应。
WAN	广域网接口	WAN 口数量由产品型号决定。	

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恢复设备的出厂配置。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。

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. 局域网中的 PC 都有一个工作正常的以太网卡。
3. 局域网中的 PC 都安装了 TCP/IP。
4. 准备 DSL 或者 Cable Modem，或者光纤收发器。

2.3 安装流程

在安装设备之前，必须保证设备的电源是关闭的。ReOS SE 软件平台路由交换一体机安装流程如下：

第一步，选择安装地点，一般是将设备安装在工作台上，也可将设备安装在标准机架上。

第二步，建立设备与局域网的连接，即将管理计算机或交换机连接到设备的 LAN 口。

第三步，建立设备与广域网的连接，即将 Cable/DSL Modem 连接到设备的 WAN 口。

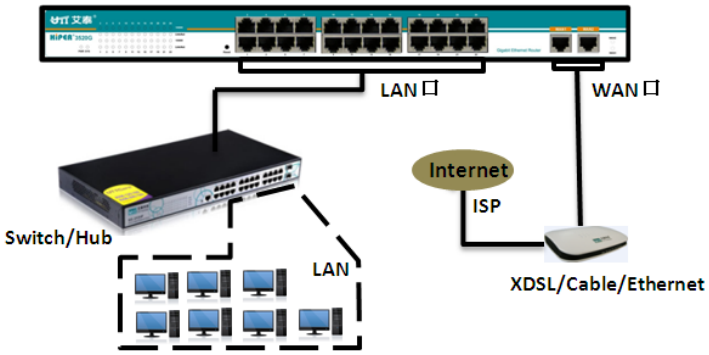

图 2-2 商睿™ 3520G 网络连接示意图

第四步，打开电源，打开电源之前确保电源供电、连接、接地正常。

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。

第3章 登录设备

本章主要介绍如何为管理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公科技官方网站获得产品信息和服务。

3.1 配置正确的网络设置

在通过 WEB 界面登录到设备之前，您必须对管理计算机进行正确的网络设置。

首先将管理计算机连接到设备的局域网端口，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 中的任意一个空闲地址，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，路由器内置的 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。

下面的例子是在 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，例如 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、密码的出厂设置为 admin、admin，区分大小写），然后单击<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。该页面右上角显示系统型号、版本信息；该页面上端还显示各端口的状态图（端口为绿色表示此端

口处于 link up 状态、黑色表示端口处于 link down 状态、灰色表示端口处于禁用状态）。

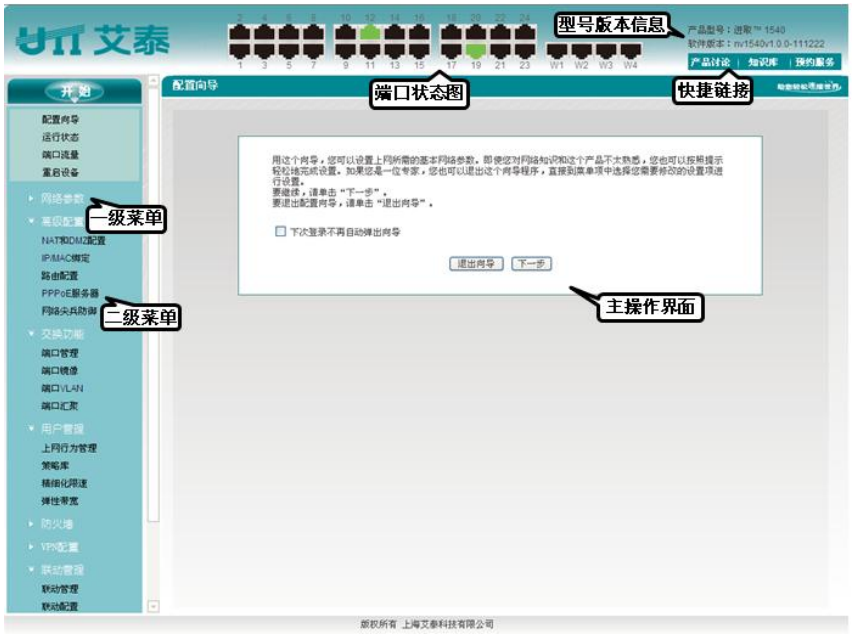

图 3-2 WEB 界面首页

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，可以设置设备上网所需的基本网络参数，快速地将设备连接到Internet。在进入配置向导配置“上网线路”之前，应正确配置局域网中计算机的网络设置，具体方法见第 3 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。如下图所示：

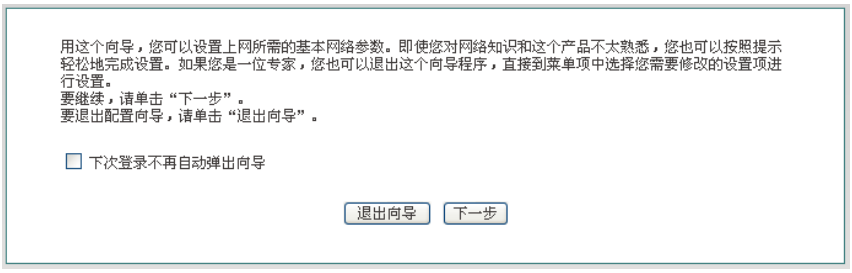

图 4-1 配置向导首页

- 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：可进入配置向导的第二页 WAN1 口地址设置页面。

4.1　WAN1 口配置——动态 IP 接入

配置向导的第二个页面可对设备的 WAN1 口地址进行配置。WAN 口默认的线路接入方式为动态 IP 接入，如图 4-2 所示。 如果您的上网线路接入方式为动态接入，请直接点击<完成>，完成上网线路的配置。

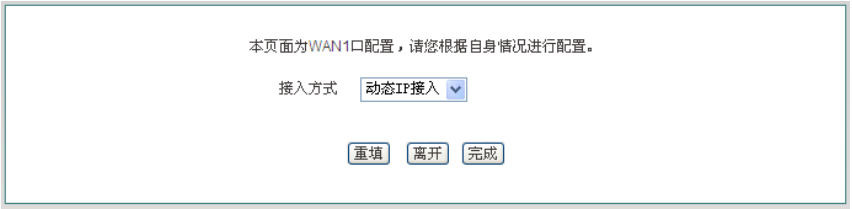

图 4-2 配置向导——动态 IP 接入

4.2　WAN1 口配置——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 4-3 的下拉列表框中选择“固定 IP 接入”。下面介绍固定 IP 接入的各参数的涵义。

图 4-3 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。

4.3 WAN1 口配置——PPPoE 接入

如果您的上网线路接入方式为 PPPoE 接入，请在图 4-4 的下拉列表框中选择“PPPoE 接入”。下面介绍 PPPoE 接入的各参数的涵义。

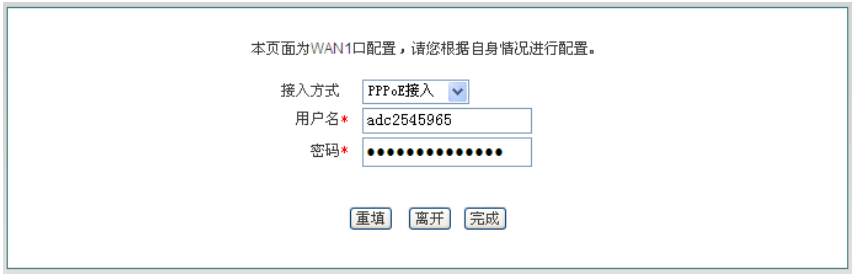

图 4-4 配置向导——PPPoE 接入

- 用户名：填入 ISP 为您提供的用户名。如有疑问，请询问 ISP；
- 密码：填入 ISP 为您提供的密码。如有疑问，请询问 ISP。

提示：

1. 配置完 WAN 口的上网线路后请点击<完成>，这样配置才会生效。

2. 对于多 WAN 口设备，如果您需要配置多条线路上网，请进入***网络参数—>WAN 口配置***页面配置其他上网线路。

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、端口流量、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，查看设备的运行状态，查看设备各端口的实时流量统计信息。

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，具体内容及配置方法请参见第 4 章《配置向导》。

5.2　运行状态

本节主要介绍*开始—>运行状态*页面，在本页面您可以通过运行状态信息列表查看设备各端口的状态信息。

图 5-1 运行状态信息列表

5.3　端口流量

本节主要讲述*开始—>端口流量*页面，如图 5-2 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实时速率，并为其提供不同的单位（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。

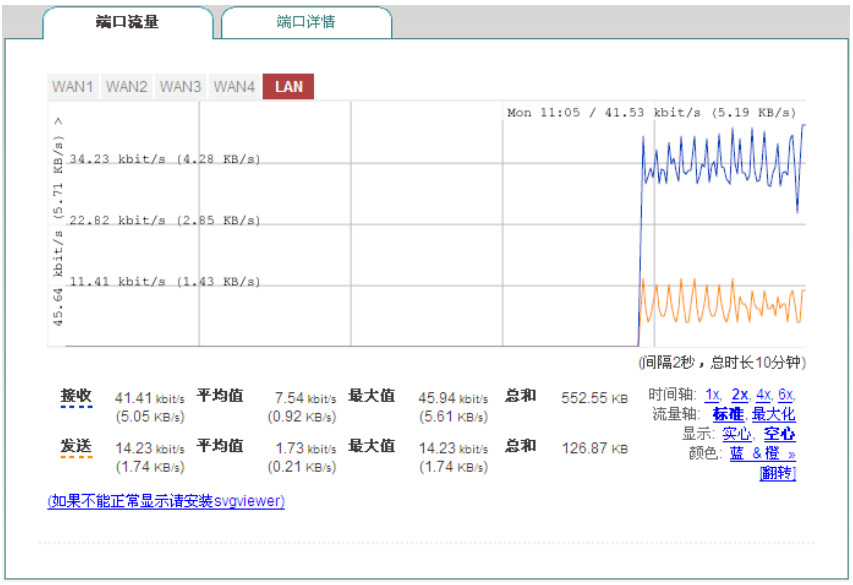

图 5-2 接口流量

- LAN：设备的局域网口，单击可查看该端口的流量图形化显示；
- WAN：设备的广域网口，单击相应接口可查看其流量的图形化显示；
- 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，可根据需要显示效果（如图中的标准、最大化）；
- 显示：提供实心和空心两个效果显示选项，可根据需要选择；
- 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对调。

在图 5-2 中选择“端口详情”选项卡，进入如下图所示的界面。点击相应的端口，可从下方的表中得知该端口的发送、接收包的详细信息。

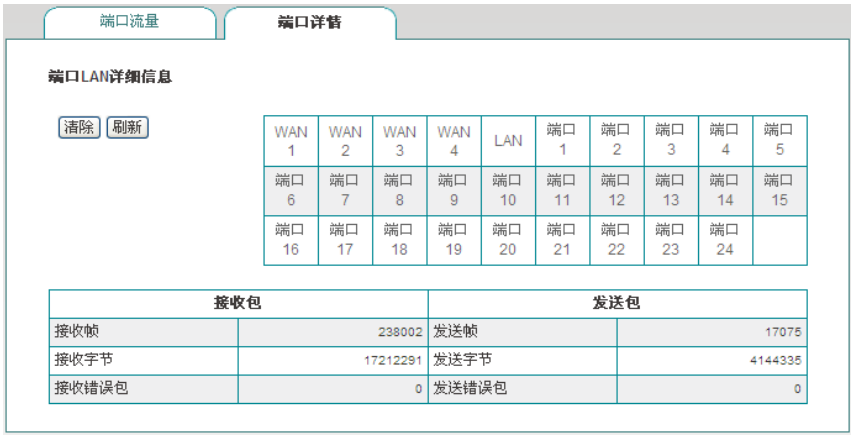

图 5-3 端口详情

5.4　重启设备

本节介绍***开始—>重启设备***页面。如果您需要重启设备，则进入此页面点击<重启>按钮。

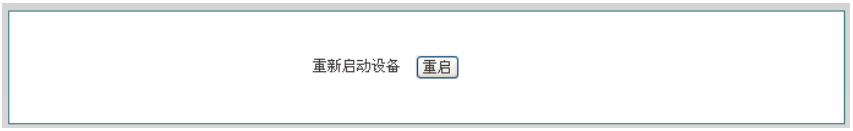

图 5-4 重启设备

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

在网络参数配置中，主要包括配置设备基本网络参数，包括 WAN 口配置、线路组合、LAN 口配置、DHCP 服务器、DDNS 配置和 UPnP 配置。

6.1　　WAN 口配置

本节主要讲述***网络参数—>WAN 口配置***的配置界面及方法。

在本页面不仅可以配置线路信息，也可以根据实际需要修改或删除已配置的线路，还可以查看线路的连接状态信息。

在***配置向导***中配置完 WAN1 口之后，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。

6.1.1　网络接口配置

本节介绍如何配置上网线路。上网线路的连接类型有：动态 IP 接入、固定 IP 接入、PPPoE 接入。进入***网络参数—>WAN 口配置***页面，配置界面如图 6-1 所示。

图 6-1 WAN 口配置

1.　动态 IP 接入

如图 6-1 所示，下面介绍动态 IP 接入的各参数的涵义。

- 接口：选择设备相应的接口；
- 接入方式：这里选择“动态 IP 接入”；

- 运营商策略：选择该接口的运营商，有四个可选项分别为不限、电信、联通及移动线路，此处选择电信，表示电信流量走该接口；
- MAC 地址：相应接口的 MAC 地址，一般无需修改。

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. 固定 IP 接入

图 6-2 固定 IP 接入

如图 6-2 所示的界面为固定 IP 接入的配置界面。

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

3. PPPoE 接入

图 6-3 PPPoE 接入

如图 6-3 所示的界面为 PPPoE 接入的配置界面。

- 接入方式：此处选择 PPPoE 接入，ADSL 虚拟拨号（也可以是以太网介质的 PPPoE 拨号），设备将通过拨号获取 IP 地址、子网掩码以及网关地址信息；
- 用户名、密码：在运营商办理业务时，运营商提供的用户名及密码；
- 密码验证方式：ISP 验证用户名及密码的方式，默认为 EITHER。多数地区为 PAP 方式，也有少数地区采用 CHAP 方式，NONE 表示不进行用户名和密码验证，EITHER 表示自动和对方设备协商采用哪种验证方式；
- 拨号类型：
  - 自动拨号：当打开设备或者上一次拨号断线后自动拨号连接；
  - 手动拨号：由用户在***网络参数—>WAN 口配置***的“线路连接信息列表”中手动进行连接和挂断；
  - 按需拨号：在内网有访问 Internet 流量时设备会自动进行连接；
- 拨号模式：选择 PPPoE 拨号的模式，默认为普通模式，在使用正确的用户名和密码的前提下，如果拨号不成功，可以尝试使用其它模式；
- 空闲时间：无访问流量后自动断线前等待的时长，0 代表不自动断线（单位：分钟）；
- 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，不要修改。

6.1.2　线路连接信息列表

在“线路连接信息列表”中可以查看各线路的配置及状态信息，如图 6-4、图 6-5 所示。

图 6-4 线路连接信息列表

图 6-5 线路连接信息列表（续图 6-4）

- 接口：该列中显示设备的 WAN 口；
- 连接类型：当前上网接入线路的连接类型，包括固定接入、动态接入、PPPoE 接入；

- 连接状态：线路的当前连接状态，当连接不成功或未连接时显示“断开”，当连接成功时则显示“已连接”，对于动态 IP 接入及 PPPoE 接入连接成功时还会显示保持本次连接的时间（单位：小时:分:秒）；
- IP 地址、子网掩码、网关地址：分别为 ISP 提供的广域网接口的 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/上行平均速率。单位为 KB/s。

1. PPPoE 接入线路的拨号与挂断

如果某线路为 PPPoE 接入，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”按钮，如图 6-6 所示，WAN3 口为 PPPoE 接入，点击“WAN3”，线路连接信息列表右下方显示以下四个按钮，这四个按钮的功能如下：

- 删除：删除这条线路；
- 拨号：用以建立和 PPPoE 服务器的连接，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：挂断当前与 PPPoE 服务器的拨号连接；
- 刷新：单击该按钮可显示线路连接信息列表的最新信息。

图 6-6 线路连接信息列表——PPPoE 接入

2. 动态 IP 接入线路的更新与释放

如果某线路为动态 IP 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“更新”和“释放”按钮，如图 6-7 所示。

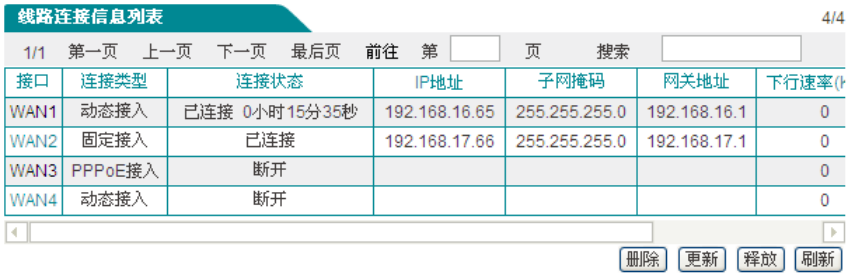

图 6-7 线路连接信息列表——动态 IP 接入

- 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：释放当前得到的动态 IP 地址。

6.2 线路组合

本节主要讲述***网络参数—>线路组合***的配置方法。

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，先介绍线路检测的相关参数。

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，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，就认为该线路已恢复正常。

设备允许用户预先为局域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 地址属于这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，局域网内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，之前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，局域网内主机就通过主线路上网；

2. 若主线路出现故障，则自动切换到备份线路并通过备份线路上网；

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

本小节介绍线路组合全局配置，包括：“所有线路负载均衡”、“部分线路负载均衡，其余备份”。

1. 所有线路负载均衡

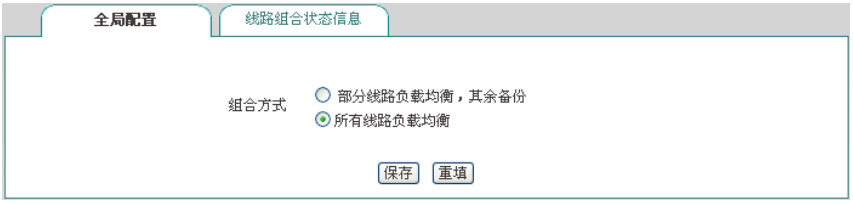

图 6-8 路组合——所有线路负载均衡

提示：线路组合方式默认为“所有线路负载均衡”。

2. 部分线路负载均衡，其余备份

图 6-9 线路组合配置——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。

6.2.3　线路组合状态信息列表

进入***网络参数—>线路组合—>线路组合状态信息***页面，可通过线路组合状态信息列表查看各条线路的线路检测信息。如图 6-10、图 6-11 所示。

图 6-10 线路组合状态信息列表

图 6-11 线路组合信息列表（续图 6-10）

- 接口：设备的相应 WAN 口；
- 连接类型：接口的连接类型，分为动态接入、固定 IP 接入、PPPoE 接入；
- 带宽：显示线路已设置的带宽值；
- 线路状态：分为已连接、断开；
- IP 地址：该接口的 IP 地址；
- 检测间隔：已设置的发送检测包的时间间隔；
- 检测次数：检测周期内发送检测包的次数；
- 目标检测 IP 地址：已配置的线路检测的目标 IP 地址；
- 内部起始/结束 IP 地址：内网优先使用当前线路上网的主机的地址范围；
- 编辑：点击该图标进入到***线路检测配置***页面，可配置相关的线路组合信息。

6.2.4　线路检测配置

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 6-12 线路检测配置

- 接口：所选择线路的接口，此选项在此页面不可修改；
- 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 IP 地址、内部结束 IP 地址：局域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***页面编辑 LAN 口网络参数。

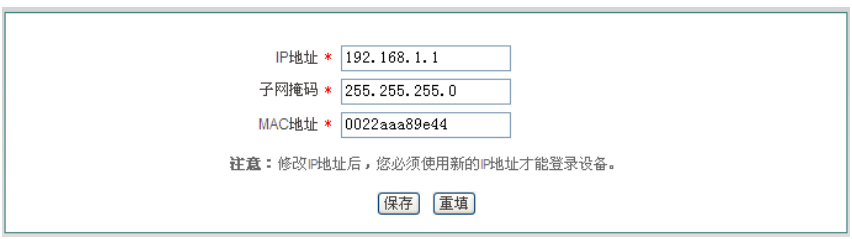

图 6-13 LAN 口配置

- IP 地址：设备 LAN 口的 IP 地址；
- 子网掩码：设备 LAN 口的子网掩码；
- 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，且登陆主机的 IP 要和其在同一网段才能登陆设备！

6.4　DHCP 服务器

本节介绍***网络参数—>DHCP 服务器***页面及配置参数，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

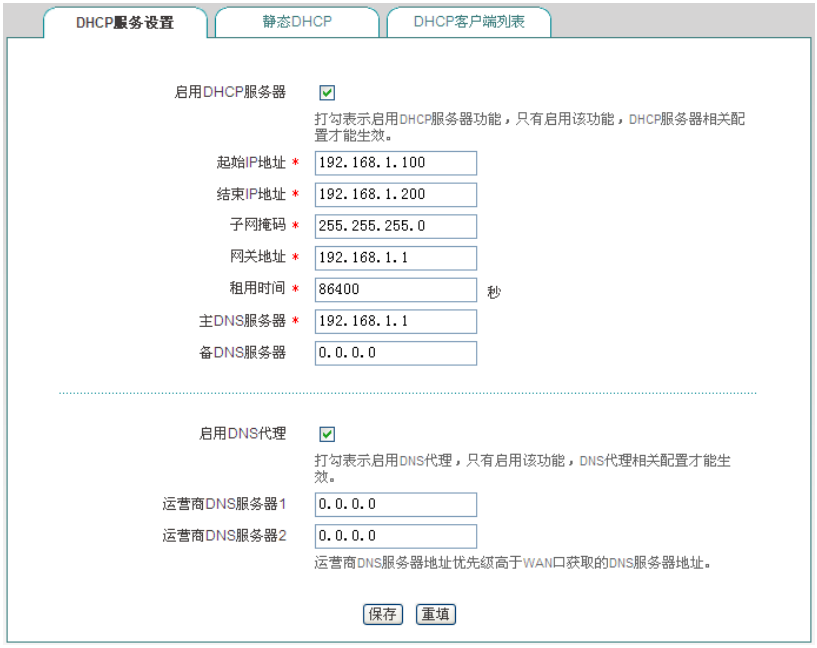

图 6-14 DHCP 服务配置

- 启用 DHCP 服务器：用来禁用或启用设备的 DHCP 服务器功能。选中为允许；
- 起始、结束 IP 地址：DHCP 服务器给局域网计算机自动分配的 IP 地址段（与设备 LAN 口的 IP 地址在一个网段）；
- 子网掩码：DHCP 服务器给局域网计算机自动分配的子网掩码（与 LAN 口的子网掩码一致）；
- 网关地址：DHCP 服务器给局域网计算机自动分配的网关 IP 地址（一般要和设备的 LAN 口的 IP 地址一致）；
- 租用时间：局域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 服务器给局域网计算机自动分配的主 DNS 服务器 IP 地址；
- 备 DNS 服务器：DHCP 服务器给局域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，启用此功能后设备会将 LAN 口 IP 地址分配给客户端作为主 DNS 服务器地址；
- 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，局域网计算机的 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 LAN 口的 IP 地址修改为代理服务器的 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 服务为局域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。而某些局域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 6-15 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 6-15 静态 DHCP 列表

2. 静态 DHCP 配置

在上图所示的页面点击<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。

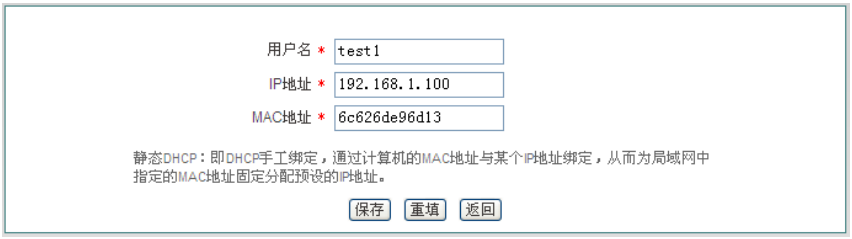

图 6-16 静态 DHCP 配置

- 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：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，否则会提示错误。

6.4.3 DHCP 客户端列表

对于已分配给局域网计算机的 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：DCHP 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 6-17 DHCP 客户端列表

6.4.4 DHCP 配置实例

1. 应用需求

本实例中，要求路由器开启 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 的主机获取固定的 IP 地址：192.168.1.15；MAC 地址为 00:1f:3c:0f:07:f4 的主机获取固定的 IP 地址：192.168.1.10。

2. 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，（如下图所示），配置完后点击<保存>。

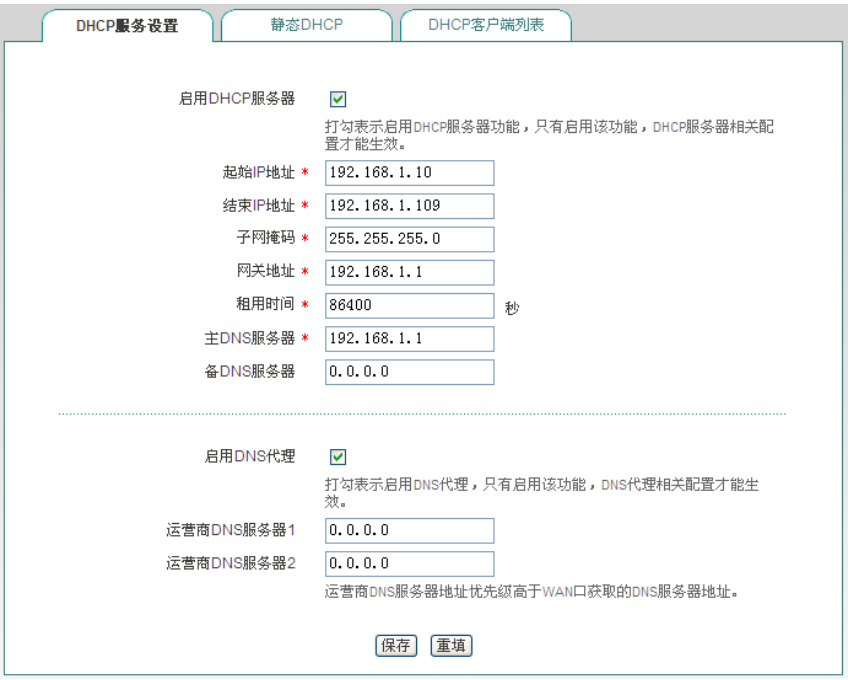

图 6-18 DHCP 服务设置——实例

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；

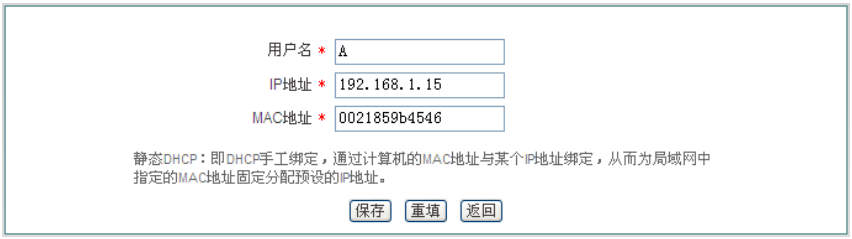

图 6-19 静态 DHCP 配置——实例 A

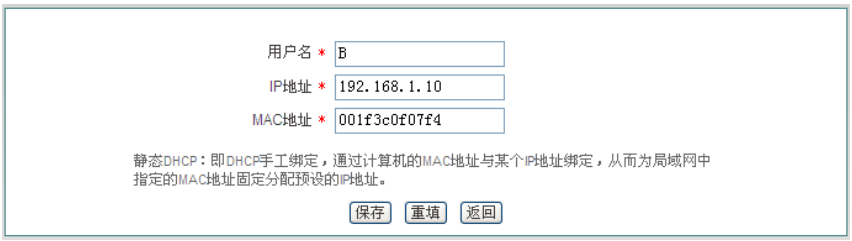

图 6-20 静态 DHCP 配置——实例 B

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 6-21 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 配置页面修改。

图 6-21 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。

艾泰科技设备支持 3322.org 和 iplink.com.cn 的 DDNS 服务。

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 6-22 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 6-23 iplink 动态域名列表

2. iplink.com.cn 的 DDNS 配置

图 6-24　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 6-23 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 6-25　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 6-26　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：申请 3322.orgDDNS 服务时配置的主机名；
- 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

可以在局域网计算机的 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 6-27 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：当图中方框被选中时表示启用了 UPnP，没有选中时表示没有启用 UPnP，启用 UPnP 时点击<保存>按钮配置才能生效；
- 内部地址：内网主机的 IP 地址；
- 内部端口：内网主机提供的服务端口；
- 协议：该 UPnP NAT 静态映射使用的协议；
- 对端地址：对端主机的 IP 地址；
- 对端端口：内部端口经 NAT 转换后的端口，此端口是设备提供给 Internet 的服务端口；
- 描述：用来描述相关 UPnP 软件的信息。

第7章 高级配置

本章主要讲述设备的 NAT 和 DMZ 功能、IP/MAC 绑定功能、路由配置和 PPPoE 服务器功能。

7.1 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。

7.1.1 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。

设备提供了灵活的 NAT 功能，以下各节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：一个是局域网主机在内部使用的私有 IP 地址，配置过程中用“内部 IP 地址”表示；另一个是用于外部的公网 IP 地址，配置过程中用“外部 IP 地址”表示。

2. 两种 NAT 类型

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。

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。它通常应用在外网访问内网的服务器：内网服务器依旧使用私有地址，而外部网络用户则通过为其分配的公网 IP 地址访问服务器。

3. 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，广域网

中的计算机希望通过设备访问局域网内部服务器，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局域网服务器上，从而，广域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，需要将一台局域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 静态映射匹配的局域网计算机上。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。

7.1.2 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

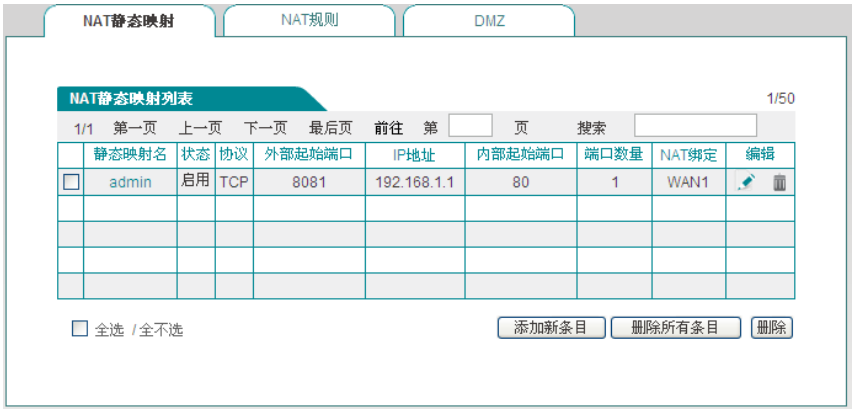

图 7-1 NAT 静态映射列表

提示：系统某些功能（如***系统管理—>远程管理***）会添加名为 admin 的 NAT 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

在如图 7-1 的页面点击“添加新条目”进入 ***NAT 静态映射配置***页面，如图 7-2 所示。下面介绍 NAT 静态映射配置的各参数的涵义。

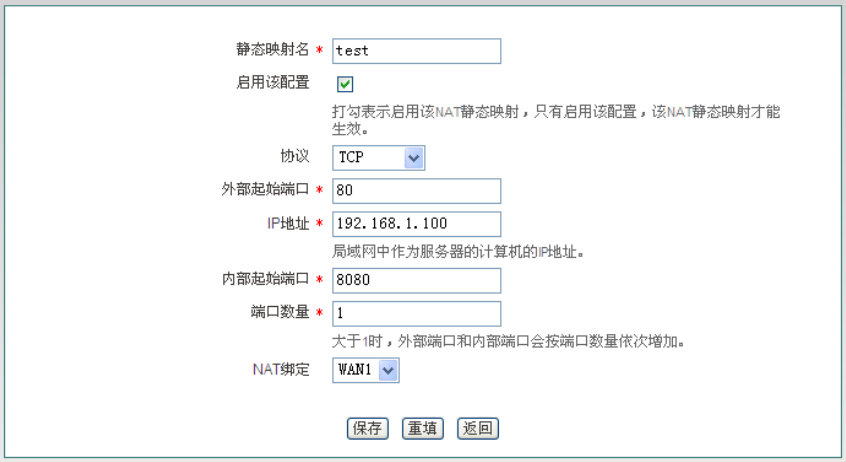

图 7-2 NAT 静态映射配置

- 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；当用户无法确认该协议所使用的类型为 TCP 或 UDP 时，可选择 TCP/UDP；
- 外部起始端口：外部访问使用的起始端口；
- IP 地址：局域网中作为服务器的计算机的 IP 地址；
- 内部起始端口：局域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。

7.1.3 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 7-3 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，并通过该 WAN 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，并通过该 WAN 口实现上网。

图 7-3 NAT 规则信息列表

提示：NAT 规则的匹配顺序按照 NAT 规则列中的默认排列顺序，列表越上方的越先匹配。

2. Easy IP

在图 7-3 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 7-4 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：局域网中优先使用该 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 7-4 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。

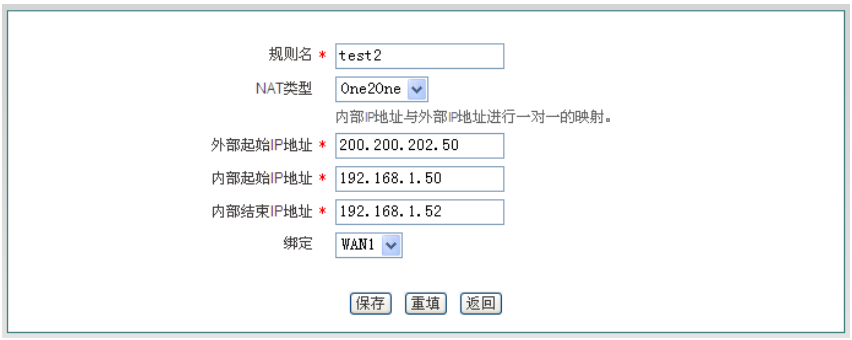

图 7-5 One2One

- 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。

7.1.4 DMZ

下面介绍设备的 DMZ 功能。

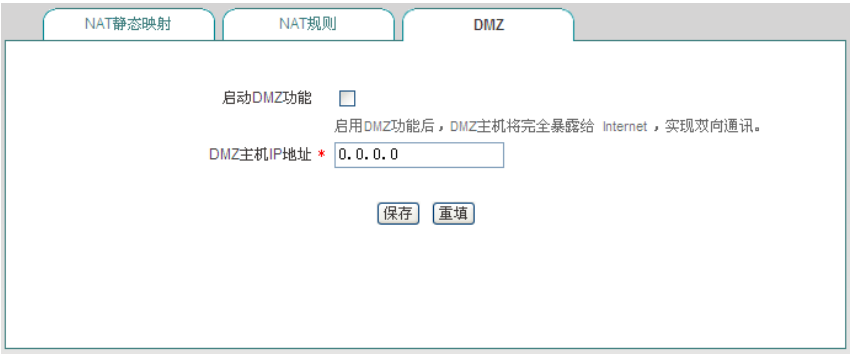

图 7-6 DMZ 配置

- 启用 DMZ 功能：打开或者关闭 DMZ 功能；
- DMZ 主机 IP 地址：欲用作虚拟服务器（DMZ 主机）的局域网计算机的 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。

7.1.5 NAT 和 DMZ 配置实例

本小节里例举 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

局域网计算机 192.168.1.99 开设了 TCP80 端口的服务，希望外部通过 WAN2 口 80 端口访问这个服务，具体配置如图 7-7 所示。

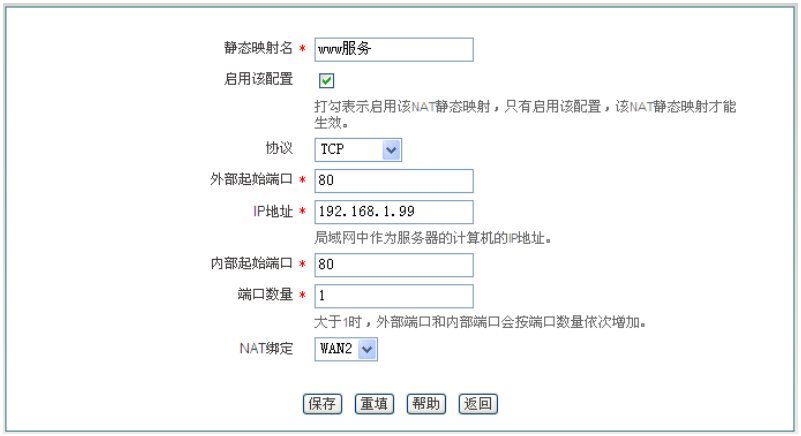

图 7-7 NAT 静态映射配置实例

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，单击“添加新条目”按钮；

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，单击“保存”按钮，该条 NAT 规则配置成功。

图 7-8 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，单击“添加新条目”按钮；

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”按钮，该条 NAT 规则添加成功。

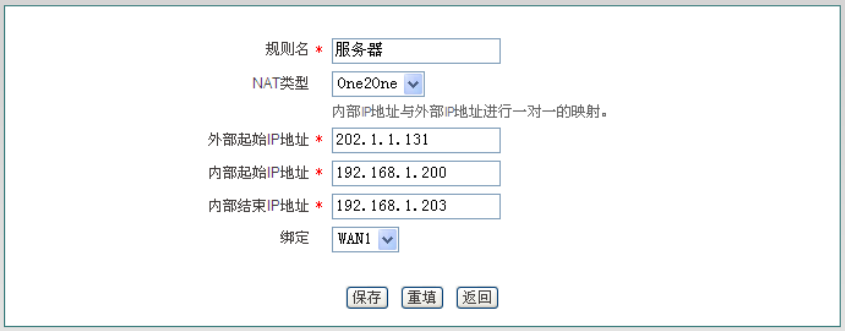

图 7-9 NAT 规则配置——One2One

7.2 IP/MAC 绑定

本节主要讲述***高级配置—>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局域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。这台电脑的 IP 地址可以轻易地改变为受信任的地址，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。

7.2.1 IP/MAC 绑定列表

图 7-10 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 绑定的用户与设备连接；
- 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，配置完后点击<保存>按钮。

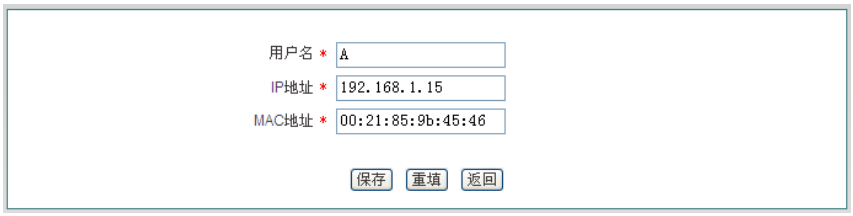

图 7-11 IP/MAC 实例修改

- 用户名：IP/MAC 绑定的用户名（自定义，不能重复）；
- IP 地址：局域网中要进行 IP/MAC 绑定的计算机的 IP 地址；
- MAC 地址：局域网中要进行 IP/MAC 绑定的计算机的 MAC 地址。

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。

7.2.2 IP/MAC 绑定配置

图 7-12 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：该用户的 IP 地址（Windows 平台 DOS 环境下使用 ipconfig /all 命令获得）；
  - MAC 地址：该用户的 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：单击“扫描”按钮，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。

7.2.3 IP/MAC 绑定实例

灵活地运用 IP/MAC 绑定功能，可以为局域网用户配置上网“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，如果要求只允许局域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，如果要求只禁止局域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. 为局域网用户配置上网“白名单”，步骤如下：

第一步：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 地址进行绑定，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。

第二步：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 7-13 所示。

图 7-13 IP/MAC 绑定信息列表——实例一

2. 为局域网用户配置上网“黑名单”，步骤如下：

第一步：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局域网网卡的 MAC 地址进行绑定，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 地址进行绑定，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。

第二步：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局域网网卡的 MAC 地址，如下图所示。

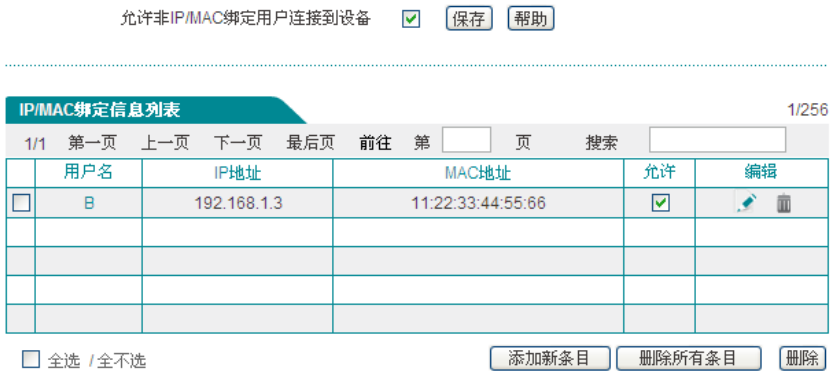

图 7-14 IP/MAC 绑定信息列表——实例二

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 7-15 所示。

图 7-15 IP/MAC 绑定信息列表——实例三

7.3 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。静态路由不会随未来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 7-16 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。

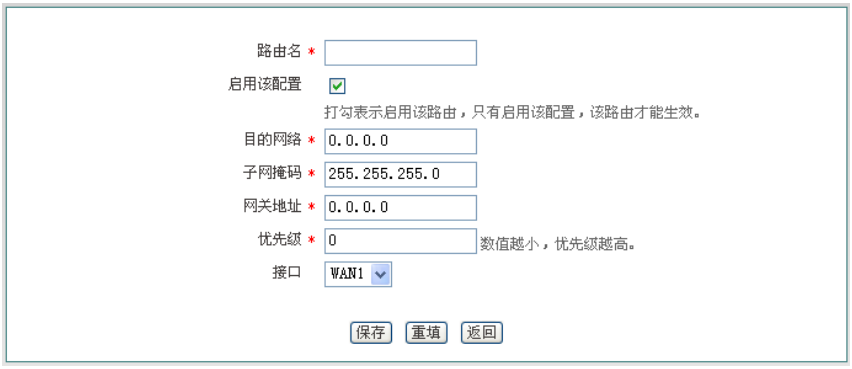

图 7-17 静态路由配置

- 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地址定义一条跳到下一个路由器的线路。通常情况下，接口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（数值越小，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。

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。

7.4 PPPoE 服务器

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

7.4.1 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的桥接设备接入到远端的接入集中器上。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，首先必须进入发现阶段以识别 PPPoE Server 的以太网 MAC 地址，并建立一个 PPPoE 会话标识（Session ID）。

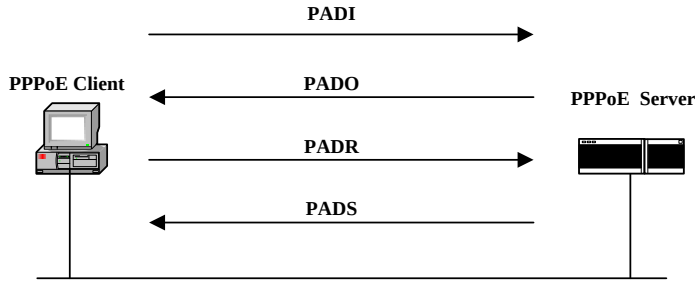

图 7-18 Discovery 阶段的基本工作流程

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。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。

7.4.2 PPPoE 全局配置

进入***高级配置—>PPPoE 服务器***页面配置 PPPoE 服务器功能。配置参数介绍如下。

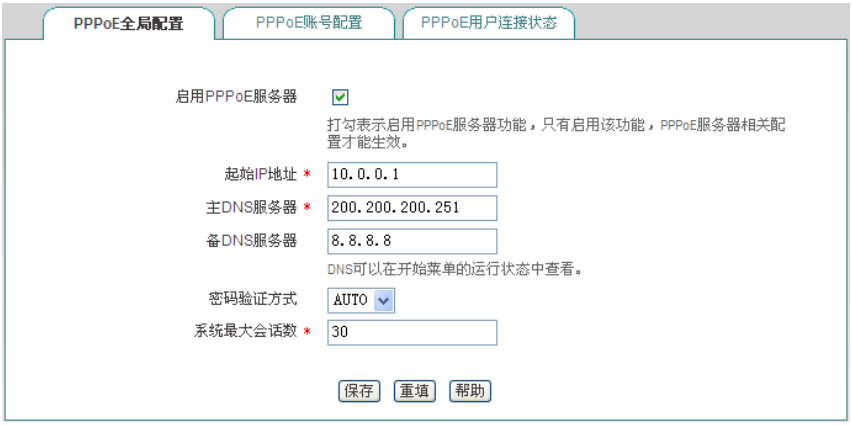

图 7-19 PPPoE 服务器全局配置

- 启用 PPPoE 服务器：启用/禁用设备的 PPPoE 服务器功能，选中为启用；
- 起始 IP 地址：PPPoE 服务器给局域网计算机自动分配的起始 IP 地址；
- 主 DNS 服务器：PPPoE 服务器给局域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 服务器给局域网计算机自动分配的备用 DNS 服务器的 IP 地址；
- 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。

7.4.3 PPPoE 账号配置

进入***高级配置—>PPPoE 服务器—>PPPoE 账号配置***页面（如图 7-20 所示）可以查看 PPPoE 账号信息列表；点击“添加新条目”按钮，进入如图 7-21 所示的页面：

图 7-20 PPPoE 账号信息列表

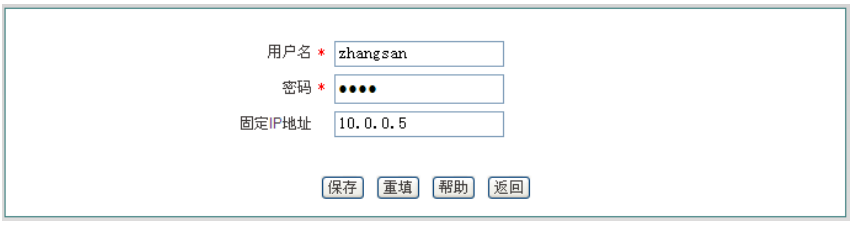

图 7-21 PPPoE 账号配置

- 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。

7.4.4 PPPoE 用户连接状态

进入***高级配置—> 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，如果有用户连接到 PPPoE 服务器，则可以在列表中看到 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/下载的速率信息。

图 7-22 PPPoE 连接状态信息列表

7.4.5 PPPoE 服务器实例配置

1. 需求：有线接入设备的计算机需拨号连接到设备。

现为内网有线接入设备的用户配置 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。

2. 配置步骤：

1) 登陆设备，进入***高级配置—>PPPoE 服务器***页面，启用 PPPoE 服务器，配置内容如下图所示：

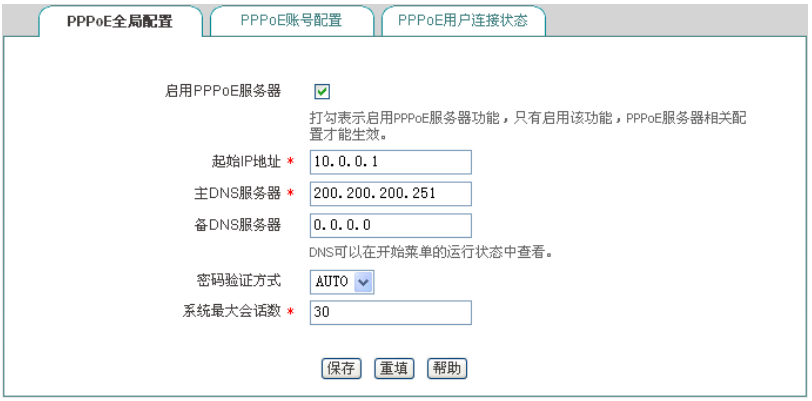

图 7-23 实例——PPPoE 全局配置

2) 进入 ***PPPoE 账号配置***页面，点击<添加新条目>，配置 PPPoE 账号，并将账号与 IP 地址进行绑定，配置内容如下图所示：

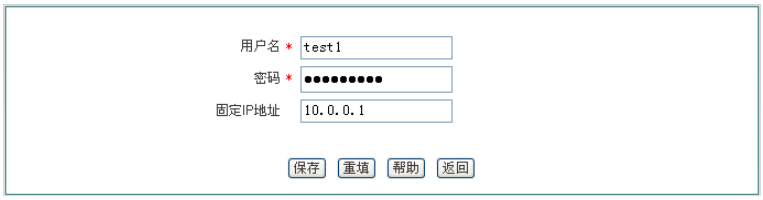

图 7-24 实例——PPPoE 账号配置

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

图 7-25 实例——PPPoE 账号信息列表

4) 在内网计算机上创建拨号客户端。

7.5 网络尖兵防御

本节介绍网络尖兵防御功能。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。

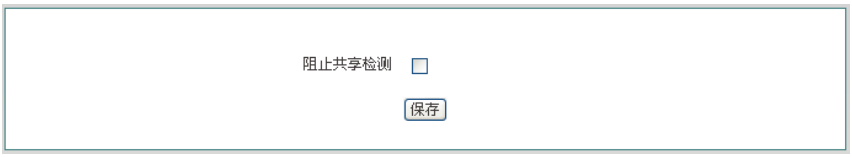

图 7-26 网络尖兵防御

第8章 交换功能

本章介绍设备的交换功能，包括：端口管理、端口镜像、端口 VLAN、端口汇聚。

8.1 端口管理

在*交换功能—>端口管理*页面，可以查看设备各端口的连接状态，配置设备各端口的工作模式，是否开启流控功能等。

图 8-1 端口管理

下面介绍端口管理配置参数的涵义。

- 全局设置：在此处可以全局设置端口的模式、允许最大帧、流控。
- 端口名称：自定义端口名称；
- 连接状态：显示各端口的连接状态，Down 表示未连接或者端口禁用，连接成功后，显示端口的工作速率和双工模式，边框有红色和绿色之分，代表了不同的连接状态，红色表示 1000Mfdx（全双工）、绿色表示其他的速率和模式；
- 设置模式：设置各端口的模式，选项有自动协商、10M(半双工)、10M(全双工)、100M(半双工)、100M(全双工)、1000M(全双工)以及禁止，自动协商表示设备与对端设备自动协商工作速率和双工模式，禁止表示禁用某个端口；
- 允许最大帧：交换机端口允许通过的最大帧，范围为 1518~9600 字节；
- 流控：设备各端口流量控制开关，此功能用来控制数据收发双方的数据收发速率。

提示：启用流控功能时，收发数据的设备都需要支持流控功能。

8.2 端口镜像

本节介绍端口镜像功能。通过端口镜像功能，可以将被监控端口的流量复制到监控端口，实时提供各个被监控端口的传输状况的详细资料，以便网络管理人员进行流量监控、性能分析和故障诊断。

在设备中，可以指定任意一个 LAN 口为监控端口，并指定其它 1 个或多个端口作为被监控端口。

图 8-2 端口镜像

- 监控端口：对被监控端口流量进行监控的端口，监控端口只能有一个；
- 被监控端口：被监控的端口，可选择一个或多个端口作为被监控端口。

提示：

1. 被监控端口与监控端口不能是同一个端口；
2. 如果某端口已经在***交换功能—>端口汇聚***页面配置属于某个汇聚组，则此端口不能再配置为监控端口；
3. 建议被监控端口只选取所需端口（如连接路由器的端口）。

8.3 端口 VLAN

VLAN，即虚拟局域网，可以将网络逻辑地分割成多个不同的广播域。一个 VLAN 组成一个逻辑广播域。同一个 VLAN 中的成员共享广播，可相互通信；不同 VLAN 之间实现物理隔离，一个 VLAN 内部的单播、广播和多播包都不会转发到其他 VLAN 中，从而有助于控制流量、简化网络管理、增强网络安全性。

端口 VLAN 根据设备 LAN 口来定义 VLAN 成员。它是将设备上的物理端口分成若干

个组，每个组构成一个虚拟网，相当于一个独立的 VLAN 交换机。下面介绍***交换管理—>端口 VLAN*** 页面及配置。

1. 端口 VLAN 列表

图 8-3 端口 VLAN 列表

从上图的端口 VLAN 列表中可以知道所有的端口位于系统默认的 VLAN1 中。

2. 端口 VLAN 设置

图 8-4 端口 VLAN 设置

下面介绍端口 VLAN 设置中各参数的涵义。

- VLAN 组号：自定义 VLAN 的组号，范围为 1-24；
- VLAN 组名称：自定义 VLAN 组的名称；
- 成员：在对应的端口下打勾，即可选择 VLAN 包含的端口；
- 添加：选中后，可以为一 VLAN 组添加新的成员；
- 修改：选中后，可以修改一 VLAN 组中的成员。

3. 端口 VLAN 配置实例

要求设置端口 1、2 可以互相通信，端口 2、3 可以互相通信，但端口 1、3 不能实现二

层通信。

配置步骤：

1. 修改 VLAN 1，端口成员包含 1、2、4~24；
2. 再新建一个 VLAN 2，端口成员包含 2 和 3。

8.4 端口汇聚

端口汇聚用于两台设备之间的级联，通过牺牲端口数来给设备之间的数据交换提供一个捆绑的高带宽线路，进而提高网络速度，突破网络瓶颈，使高网络性能得到大幅度提高。

在实际应用中端口汇聚，就是把设备的 2 个或多个端口聚合在一起，形成一个高带宽的数据传输通道。聚集在一起的所有端口看作一个逻辑端口，工作起来像一条通道一样，该逻辑端口带宽为汇聚组内所有端口带宽的叠加。例如，以太网交换中单个端口的带宽是 100Mbps，2 个端口做端口汇聚就能得到 200Mbps 的带宽，4 个端口做端口汇聚就能得到 400Mbps 的带宽。

端口汇聚不但提升了整个网络的带宽，而且数据还可以同时经由汇聚的多个物理链路传输，具有链路备份的作用。当一条链路出现故障时，不影响其它链路工作，同时多条链路之间还能实现流量均衡。

1. 端口汇聚列表

图 8-5 端口汇聚列表

2. 端口汇聚设置

在上图中点击<添加新条目>，进入***端口汇聚设置***页面。

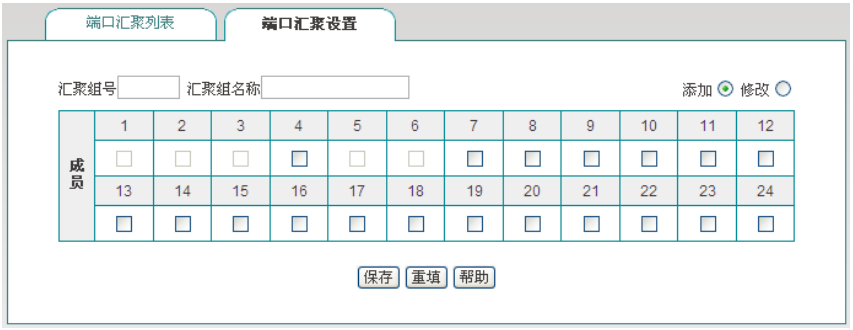

图 8-6 端口汇聚设置

- 汇聚组号：定义汇聚组的组号；
- 汇聚组名称：自定义汇聚组的名称；
- 成员：在相应组合中勾选相应的端口，可将这些端口进行汇聚。

第9章　用户管理

通过本章的介绍，用户可以通过相关功能管理内网用户的上网行为。介绍的功能有：上网行为管理、策略库、精细化限速、弹性带宽。

9.1　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。

1.　上网行为列表

进入*用户管理—>上网行为管理*页面可以在上网行为管理列表中查看已配置的上网行为管理信息。

图 9-1 行为管理信息列表

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，在此页面可以配置对内网某一网段的用户做上网行为的管理。下面将介绍配置中各参数的涵义。

图 9-2 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；
- 起始 IP 地址、结束 IP 地址：填写该行为管理实例生效的地址段的起始 IP 地址和结束 IP 地址；
- P2P 禁止：勾选相应的复选框，可禁止相应的 P2P 应用；
- 游戏禁止：勾选相应的复选框，可以禁止相应的游戏；
- 网站过滤：勾选相应的复选框，可以禁止用户访问相应的网站；点击<查看>可以查看要过滤的详细的网站信息；
- 其他：勾选相应的复选框，可以禁止相应的应用；如禁止 http 代理表示禁止局域

网用户使用 http 代理功能、禁止 SOCKS5 代理表示禁止局域网用户使用 SOCKS5 代理功能；

- 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：

当所配置的策略某功能不生效时，请确定该功能的策略库是否为最新，可在*用户管理->策略库*页面，点击<更新>超链接可更新该配置的策略库。

9.2　策略库

本节介绍*用户管理—策略库*页面及操作步骤。

系统目前提供五种类型的策略，包括：IM、P2P、游戏、DNS、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 9-3 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。

9.3　精细化限速

本节介绍*用户管理—>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*用户管理*—>*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。

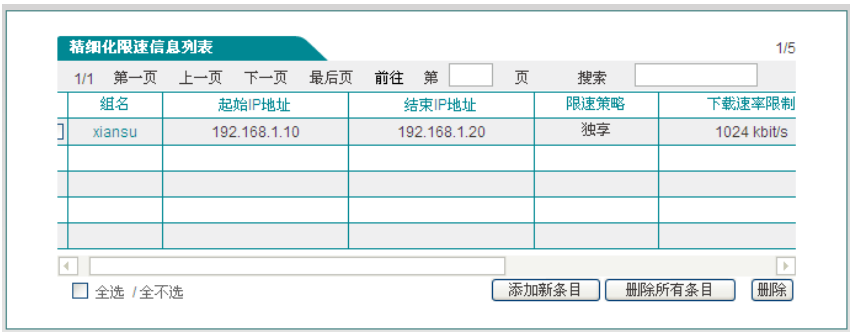

图 9-4 精细化限速信息列表

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 9-5 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。
-

9.4　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。

提示：弹性带宽功能与精细化限速功能不能同时启用。

图 9-6 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 口得上、下行带宽；
- WAN2 口上、下行带宽：设置从 ISP 申请的 WAN1 口得上、下行带宽。

9.5　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所有 IM、P2P、股票和游戏软件，查看股票及游戏网站信息。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，需使用即时通信软件（IM）与客户进行沟通。

研发部（地址为 192.168.1.100~192.168.1.129）禁止即时通信软件的使用，最大上传、下载速率分别为 1M、2M。

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，并且配置一条精细化限速配置。

1)　为销售部和客服部员工，开启 IM 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 IM 软件的使用。

3)　为 IP 地址为 192.168.1.100~192.168.1.129 的研发部员工设置一条精细化限速。

3. 配置步骤

1) 进入*用户管理—>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 P2P 禁止、游戏禁止、网站过滤、其他的“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 IM 禁止的“全选”框；

生效时间段：周一至周五、从 9:00~18:00；点击<保存>。

4) 进入*用户管理—>精细化限速*页面配置精细化限速：

组名：yanfa1；

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

限速策略：共享；

上传、下载速率限制分别为：1M、2M；

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

1) 上网行为管理列表

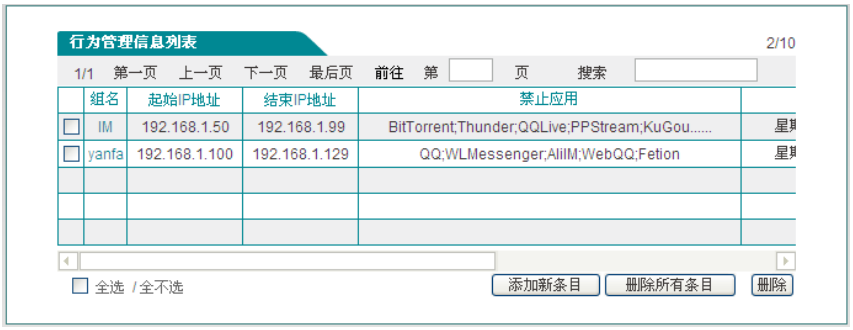

图 9-7 上网行为管理实例

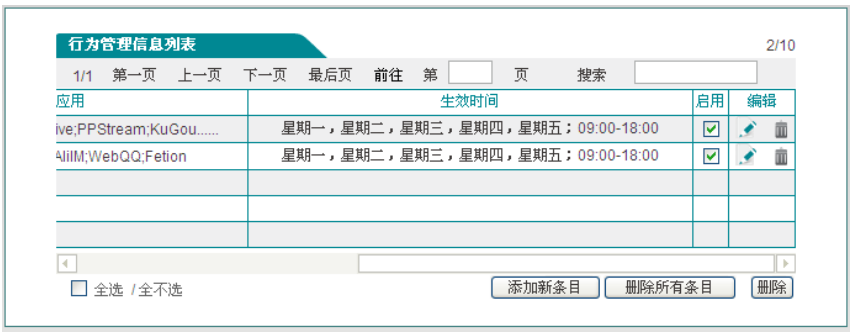

图 9-8 上网行为管理实例（续图 9-7）

2) 精细化限速列表

图 9-9 精细化限速实例

第10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。

10.1　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

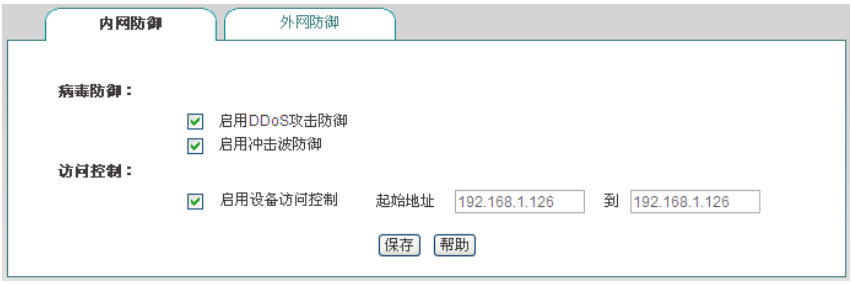

图 10-1 安全配置——内网防御

- 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 地址段中的地址能够登录设备。

2.　外网防御

图 10-2 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。

10.2　访问控制策略

本节主要讲述*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。

10.2.1 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其他内容进行分析，并按照策略的优先级从高至低搜索策略表，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，不仅可以控制局域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。设备可同时支持对中、英文关键字的过滤。

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”。

10.2.2 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 10-3 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。

10.2.3 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 10-4 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；
- IP 地址段：该访问控制策略控制的局域网用户，即源 IP 地址范围；
- 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。

二、　访问控制策略配置——URL 过滤

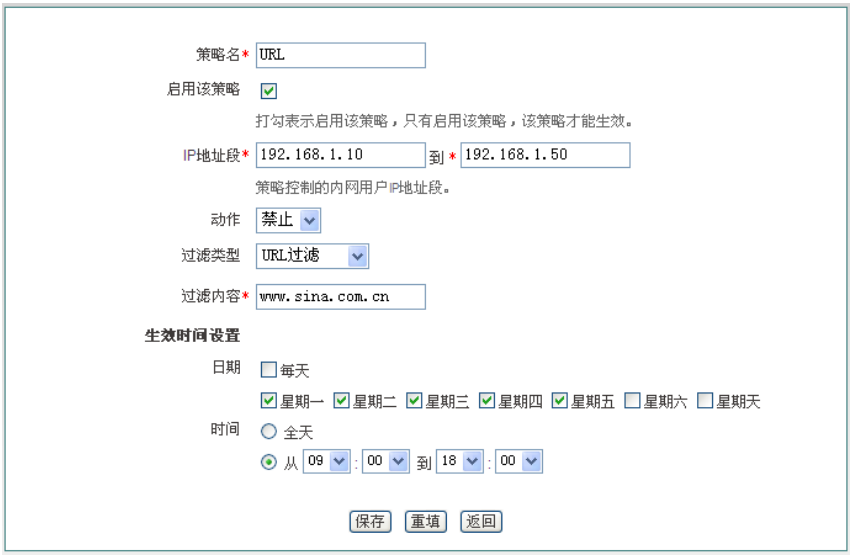

图 10-5 配置访问控制策略——URL 过滤

“策略名”、“IP 地址段”、“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：该访问控制策略欲过滤的 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 tech.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 tech.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

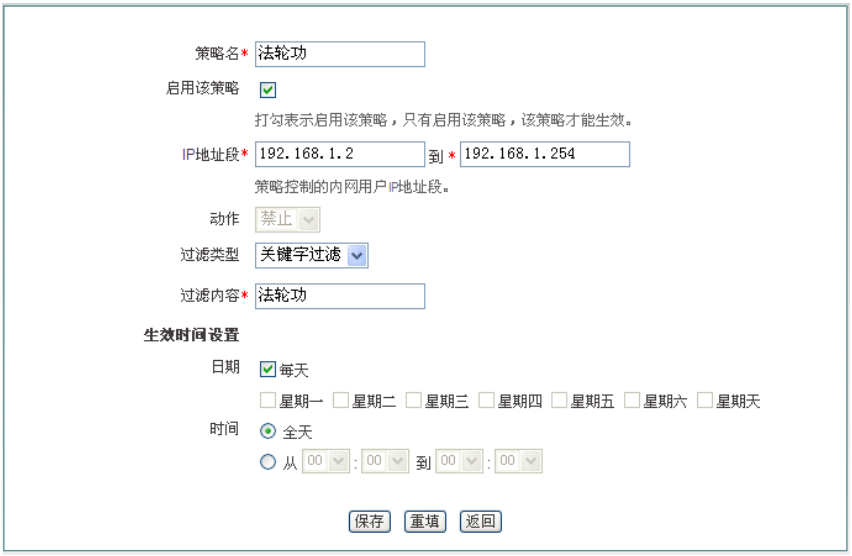

图 10-6 访问控制策略配置——关键字过滤

“策略名”、“IP 地址段”、“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：该访问控制策略欲过滤的关键字，指网页上的关键字。支持中、英文两种输入方式；允许输入含空格的字符串，一个空格为 1 个字符。注意，一条策略只允许设置一个关键字，因此，当输入的字符串中含有空格时，也当作一个关键字处理；

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. 关键字为英文时，区分大小写；
3. 优先级默认为 50，其数值越小优先级越高。

10.2.4 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，为使该地址段的用户能正常使用 WEB 服务，应该将策略 3 配置在最后。

访问控制策略列表：

图 10-7 访问控制策略——实例一

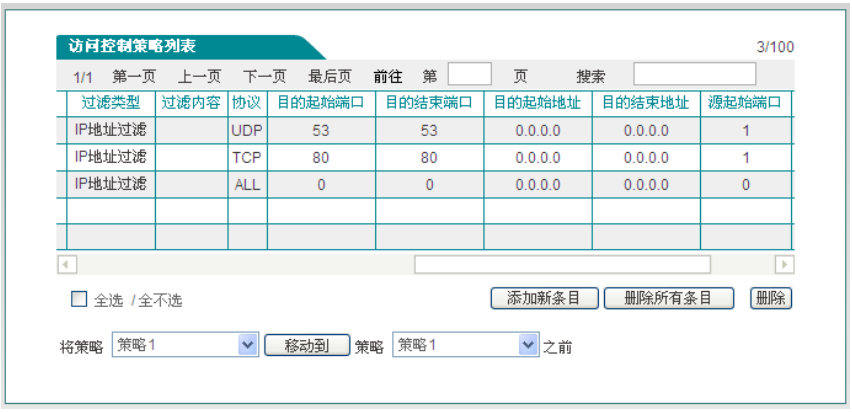

图 10-8 访问控制策略——实例一（续图 10-7）

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 10-9 访问控制信息列表——实例二

图 10-10 访问控制信息列表——实例一（续图 10-9）

10.3　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 10-11 域名过滤

域名过滤配置步骤：

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；最后勾选“启用域名过滤”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11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。

11.1　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。

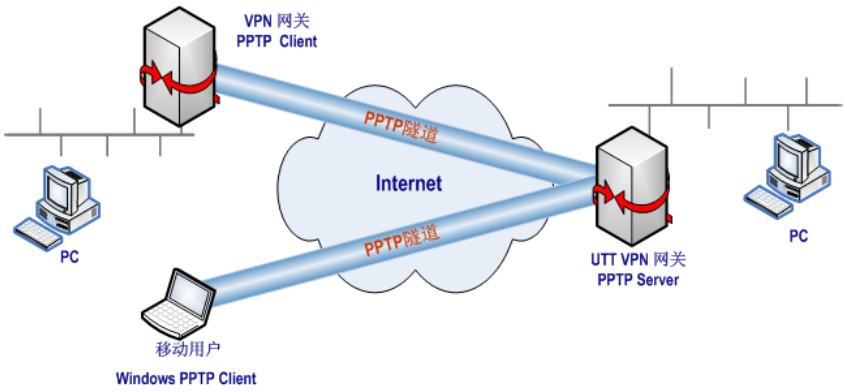

图 11-1　PPTP 典型应用

11.2　PPTP 信息列表

图 11-2　PPTP 信息列表

提示：

1、 “建立”、“挂断”按钮的操作只对客户端才生效；

2、 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。

11.3　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。

11.3.1　全局配置

图 11-3　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；
- 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。

11.3.2 账号配置

下面介绍为 PPTP 客户端配置账号时的各参数的涵义。

图 11-4　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。

11.4　PPTP 客户端配置

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。

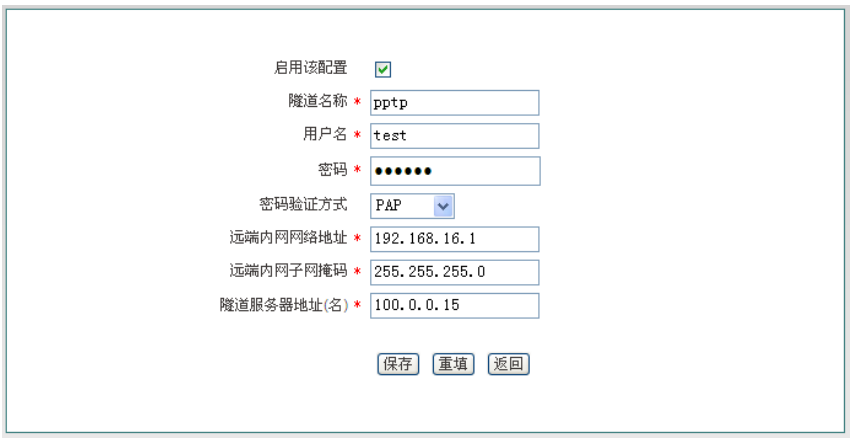

图 11-5　PPTP 客户端

- 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。

11.5　PPTP 配置实例

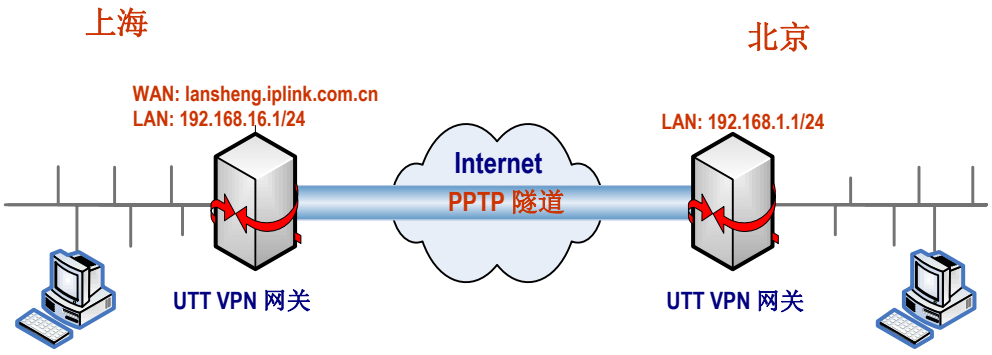

图 11-6 PPTP 实例拓扑图

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 510 V2），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

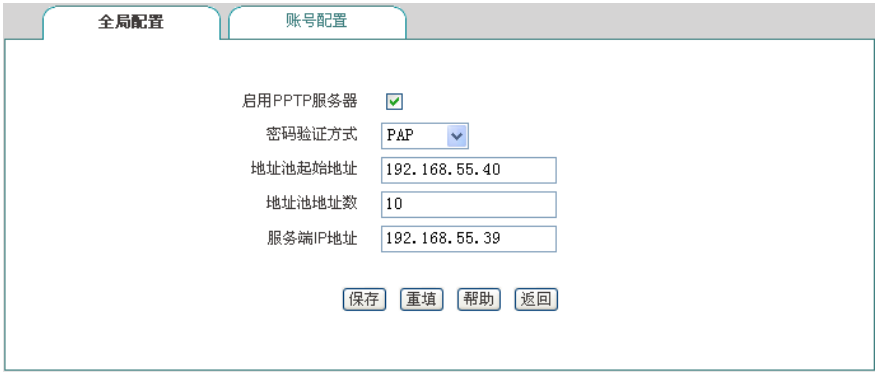

图 11-7 PPTP 服务端配置 1

图 11-8 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

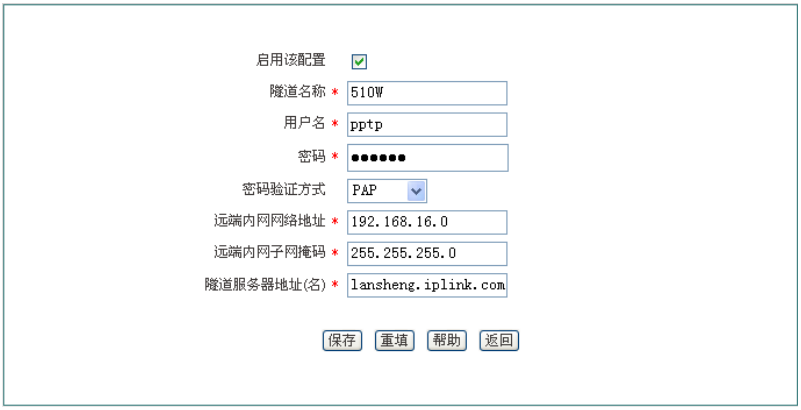

图 11-9 PPTP 客户端配置

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 11-10 PPTP 服务端信息列表 1

图 11-11 PPTP 服务端信息列表 2

图 11-12PPTP 客户端信息列表 1

图 11-13 PPTP 客户端信息列表 2

第12章 联动管理

联动管理，是对同一广播域中的远程交换机进行配置管理的功能，它通过发送广播报文，来获取广播域中远程交换机的信息，并可对已发现的交换机进行管理、配置。

本章主要介绍联动管理菜单下各页面的参数涵义及配置。

12.1 联动管理

在***联动管理***页面，点击<联动发现>，设备能发现同一广播域中的交换机。如图 12-1 所示为设备点击<联动发现>后发现的同一广播域中的交换机。

图 12-1 联动管理信息列表

下面介绍列表中各参数的涵义。

- 名称：远程交换机的名称；
- 型号：远程交换机的型号；
- 序列号：远程交换机的序列号；
- IP：远程交换机的 IP 地址；
- MAC：远程交换机的 MAC 地址；
- 连接端口：与远程交换机相连的本地设备的端口；
- 远程密码：远程交换机的登录密码，如果密码输入错误则无法对远程交换机进行联动管理；
- 管理：密码输入正确后，点击“管理”超链接能对远程交换机做如下的配置；
  - 端口管理：能够对远程交换机进行端口管理、端口 VLAN 划分、端口汇聚配置；
  - 网络安全管理：能够对远程交换机进行端口镜像配置；

- 系统管理：能查看远程交换机的系统信息，能对远程交换机进行如下操作，修改系统设置、重启远程交换机、将远程交换机恢复到出厂配置、获取远程交换机的配置信息、下发配置信息到远程交换机；

◆ 全局密码设置：如果所发现交换机的登录密码一致，选择需要修改联动管理的交换机，在这输入登录密码，对其进行批量操作；

▶ 批量操作：点击“批量操作”按钮，可以对列表中已选中的远程交换机进行联动批量操作，联动批量操作包括对远程交换机进行安全绑定、重启远程交换机、将远程交换机恢复到出厂配置、获取远程交换机的配置文件、下发配置文件到远程交换机；

▶ 帮助：获取当前配置内容的简单帮助信息。

12.1.1 单机联动管理

本小节介绍对单台远程交换机进行联动管理的功能，包括：端口管理、端口 VLAN、端口汇聚、端口镜像、系统设置、重启设备、恢复出厂配置、获取配置、下发配置及查看其设备系统信息。

在图 12-1 中输入远程密码，点击“管理”，进入如图 12-2 所示的 WEB 页面。在此页面可以查看远程交换机的基本信息，如：设备名称、型号、序列号、IP 地址、MAC 地址、软件版本。

图 12-2 单机联动管理

12.1.1.1 端口管理

在图 12-2 所示的页面点击“端口管理”超链接，进入如图 12-3 所示的端口管理配置页面，在此页面能够配置统一广播域中其他交换机的端口管理功能。下面介绍配置端口管理功能参数的涵义，对于在章节《8.1 端口管理》中已经介绍过的参数这里不再复述。

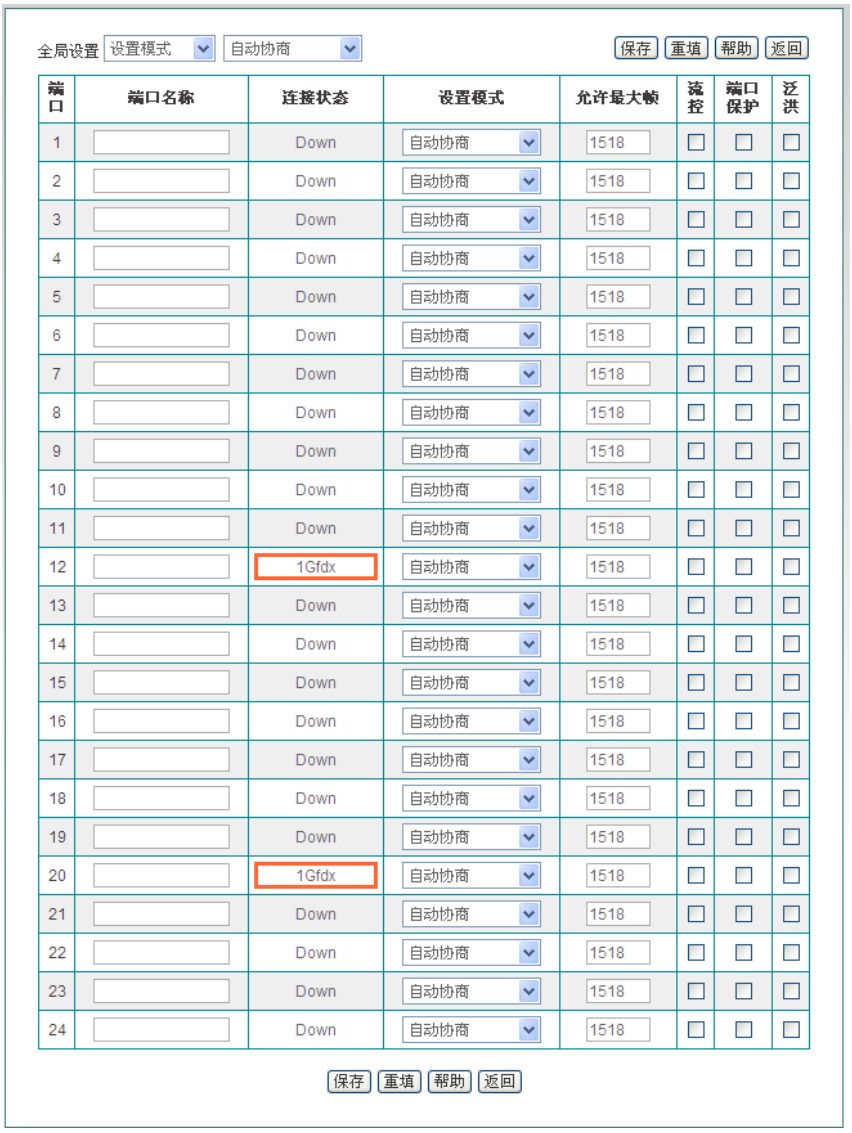

图 12-3 联动管理——端口管理

- 端口保护：启用/禁用端口保护功能，启用端口保护功能，端口不再学习新的 MAC 地址，并且只有目的 MAC 地址存在于静态地址表项中的报文才能被转发；禁用端口保护功能后，将恢复该端口的学习和转发功能；
- 泛洪：启用该功能即是关闭端口的 MAC 地址学习功能，端口收到数据帧后直接向其他端口转发。

12.1.1.2 端口 VLAN

在图 12-2 所示的页面点击“端口 VLAN”超连接，进入如图 12-4 所示的端口 VLAN 配置页面。端口 VLAN 参数的介绍具体见章节《8.3 端口 VLAN》。

图 12-4 联动管理——端口 VLAN 列表

图 12-5 联动管理——端口 VLAN 设置

12.1.1.3 端口汇聚

在图 12-2 所示的页面点击“端口汇聚”超连接，进入如图 12-6 所示的端口汇聚配置页面。端口汇聚参数的介绍具体见章节《8.4 端口汇聚》。

图 12-6 联动管理——端口汇聚列表

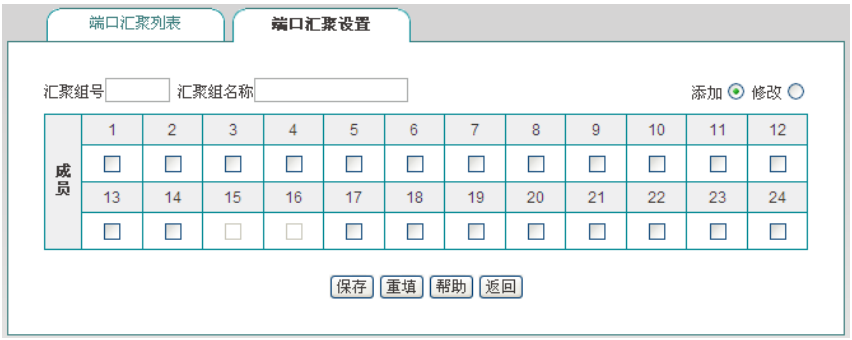

图 12-7 联动管理——端口汇聚设置

12.1.1.4 端口镜像

在图 12-2 所示的页面点击“端口镜像”超连接，进入如图 12-8 所示的端口镜像配置页面。端口镜像功能的配置参数介绍具体见章节《8.2 端口镜像》。

图 12-8 联动管理——端口镜像

12.1.1.5 系统信息

在图 12-2 所示的页面点击“系统信息”超连接，进入如图 12-9 所示的系统信息页面，在此页面可以查看远程交换机的系统信息。

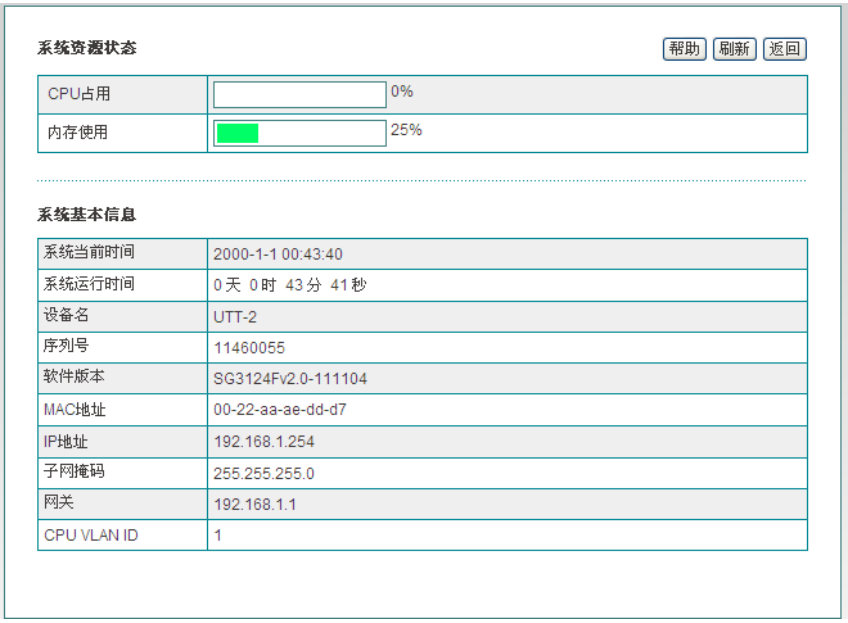

图 12-9 联动管理——系统信息

- CPU 占用：显示交换机当前 CPU 资源使用率；
- 内存使用：显示交换机内存资源使用率；
- 系统时间：显示交换机当前的日期和时间；
- 系统运行时间：显示交换机从开机启动到当前所运行的时间；
- 设备名：显示此台交换机的名称；
- 序列号：显示交换机的内部序列号；
- 软件版本：显示交换机的软件版本号；
- MAC 地址：显示交换机的背板 MAC 地址；
- IP 地址、子网掩码、网关：显示交换机的管理 IP、子网掩码、网关；
- CPU VLAN ID：显示交换机上的本征 VLAN 号。

提示：

图 12-9 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。

12.1.1.6 系统设置

在图 12-2 所示的页面点击“系统设置”超连接，进入如图 12-10 所示的系统设置页面。在此页面可以配置交换机的部分系统信息。

图 12-10 联动管理——系统设置

- 启用 DHCP 中继：启用/禁用交换机的 DHCP 中继功能，启用此功能后，交换机将转发 DHCP 请求/响应报文；
- 启用 DHCP 客户端：启用/禁用交换机的 DHCP 客户端功能，启用此功能后，交换机将从网络上已经存在的 DHCP 服务器处获得 IP 地址；
- IP 地址、子网掩码：用于设定管理交换机时使用的 IP 地址。为了方便对交换机进行管理，交换机的管理 IP 地址一般设为与局域网同网段；
- 网关：局域网的网关地址；
- CPU VLAN ID：交换机的管理 VLAN，默认是 VLAN 1；
- MAC 地址老化时间：交换机缓存表中 MAC 地址从生成到被系统老化删除的时间，默认为 300 秒，如果不是另有特殊需要，建议不要修改默认值，否则会影响网络性能；
- 设备名：自定义交换机的名称；
- 密码、密码确认：设置登录交换机管理界面的密码；
- 启用 ARP 欺骗防御：启用此功能，交换机可以有效防御 ARP 欺骗攻击。

12.1.1.7 重启设备

如果您确定要重启远程交换机，请在图 12-2 所示的页面点击“重启设备”超连接。

12.1.1.8 恢复出厂配置

如果您确定要将远程交换机恢复到出厂配置，请在图 12-2 所示的页面点击“恢复出厂配置”超连接。

12.1.1.9 获取配置

在图 12-2 所示的页面点击“获取配置”超连接，设备将获取远程交换机的配置文件并进入如图 12-11 所示的配置文件列表页面，从列表中可以查看到获取配置文件的名称、获取的时间、大小。

图 12-11 联动管理——获取配置

- 下载：点击“下载”超连接，将该配置文件下载到本地 PC 上；
- 编辑：点击编辑图标，能修改配置文件的名称；
- 删除：点击删除图标，能将配置文件从设备内存中删除。

12.1.1.10 下发配置

在图 12-2 所示的页面点击“下发配置”超连接， 进入如图 12-12 所示的配置文件列表页面。在此页面您可以将配置文件列表中的配置下发到此台远程交换机上。列表中的配置文件是通过远程“获取配置”功能获取的。下方方式是分为：手动选择配置项、完全覆盖。

图 12-12 联动管理——下发配置

下发配置步骤

第一步、选择配置文件。在配置文件列表中，选中要下发的配置文件的单选框；

第二步、选择下发方式。

下发方式为：手动选择配置项。手动选择您要下发的配置项，有：系统配置、vlan 配置、汇聚配置、端口配置、速率限制、IP/MAC 绑定。

下发方式为：完全覆盖。表示此配置文件将全部下发到远程交换机上。

第三步、点击“确定下发”按钮。

提示：

1. 下发“系统配置”时只能下发“启动 DHCP 中继”、“启动 DHCP 客户端”、“MAC 地址老化时间”。

2. “完全覆盖”，远程交换机的 IP 地址信息不会被覆盖，它还是原来的 IP 地址；

3. “完全覆盖”方式下发后应该重启远程交换机，因为有些下发的配置要交换机重启后才能生效。

12.1.2 批量联动管理

本小节介绍对远程交换机进行批量联动管理功能。

在图 12-1 中勾选要进行批量管理的设备，输入远程密码后，点击“批量操作”按钮。进入如图 12-13 所示的页面。在此页面可以对远程交换机进行如下操作：修改远程交换机的登录密码、安全绑定、重启设备、恢复出厂配置、获取配置、下发配置。

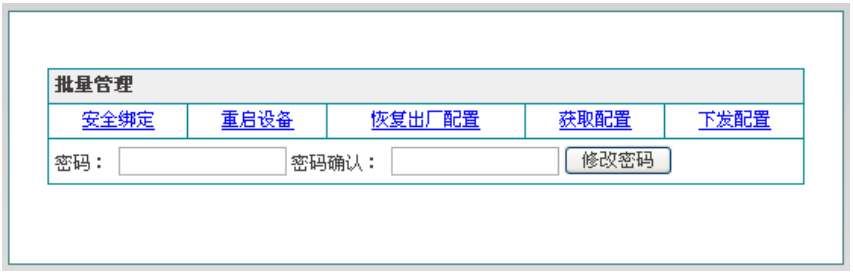

图 12-13 批量联动管理

- 修改密码：将批量操作的远程交换机的登录密码修改为一个统一的密码；
- 安全绑定：对选定的远程交换机做 MAC/PORT 绑定及 IP 地址过滤；
  - 当交换机端口只有一条 ARP 信息时，则该端口会进行 MAC/PORT 绑定及 IP 地址过滤；
  - 当交换机端口有多条 ARP 信息时，则该端口只进行 MAC/PORT 绑定；
- 重启设备：将远程交换机都进行重启；
- 恢复出厂配置：将远程交换机都恢复到出厂配置；

- 获取配置：获取批量操作的远程交换机的配置文件；
- 下发配置：下发配置到批量操作的远程交换机上。

提示：获取配置、下发配置在 12.1.1 单机联动中有详细介绍，这里不再一一重述。

12.2　联动配置

在***联动配置***页面可查看存储在设备内存中的配置文件。这些配置文件是通过联动管理获取的远程交换机上的配置文件。注：设备重启后配置文件列表将清空。

配置文件列表中各超连接、图标、按钮的功能都在章节 12.1.1.9《获取配置》中有介绍到。这里不再一一重述。

图 12-14 配置文件列表

12.3　网络拓扑

在***联动管理—>网络拓扑***页面，点击“拓扑发现”按钮，设备能发现同一广播域中支持拓扑功能的其他交换机，且能显示其网络拓扑结构。

图 12-15 网络拓扑图

单击拓扑图中的远程交换机，输入密码可以登录到这台同一广播域中的交换机上。

图 12-16 联动管理密码输入框

将鼠标放在设备图片上，可显示该设备的详细信息，如设备的 IP、MAC、型号、活动端口等。

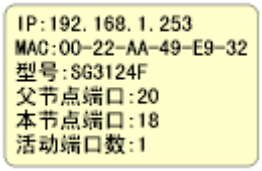

图 12-17 联动管理——详细信息

- 父节点端口：为上联设备上与该设备的连接端口号；
- 本节点端口：为该设备上与上联设备的连接端口号；
- 活动端口数：为此设备上的活动端口数。

提示：

1. 管理员所登陆的设备的详细信息只显示 IP、MAC，不会显示其类型、端口等信息；
2. 如管理员所登陆的设备上受到攻击，不会在此页面显示安全警报。

第13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。

13.1　管理员配置

1.　管理员配置信息列表

图 13-1 管理员配置信息列表

2.　管理员配置参数介绍

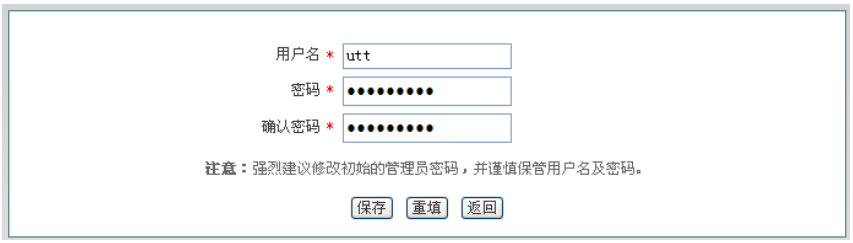

图 13-2 管理员配置

- 用户名：自定义管理员登陆 WEB 界面的用户名；
- 密码、确认密码：自定义管理员登陆 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陆用户名及密码。修改后，您必需使用新的密码登录设备。

13.2　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。

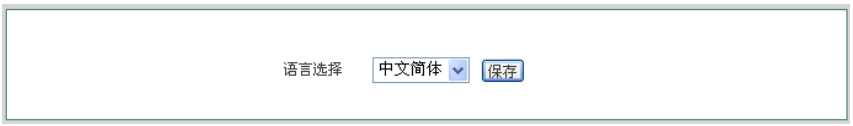

图 13-3 语言选择

13.3　时钟管理

本节主要讲述***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 13-4 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 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！

13.4　配置管理

在***系统管理—>配置管理***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，恢复设备到出厂配置。

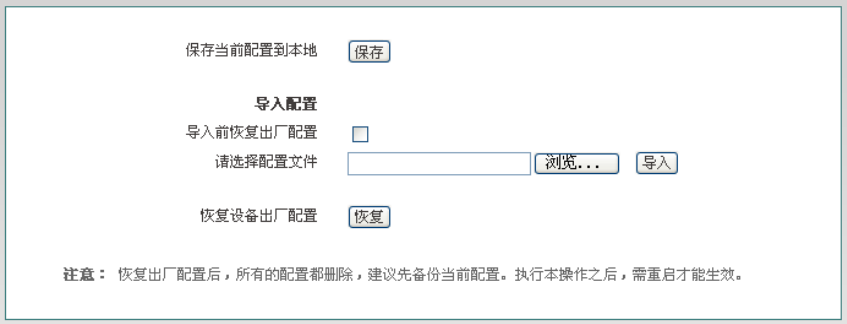

图 13-5 配置管理

1. 备份配置文件

在上图中点击“保存”按钮，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…”按钮，选择保存在本地 PC 上的配置文件。再单击“导入”按钮。如果已勾选“导入前恢复出厂配置”复选框，则在点击“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”按钮。

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. 点击确认“恢复”出厂配置后，需重启设备，设备才会恢复到出厂时的配置。

13.5　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。

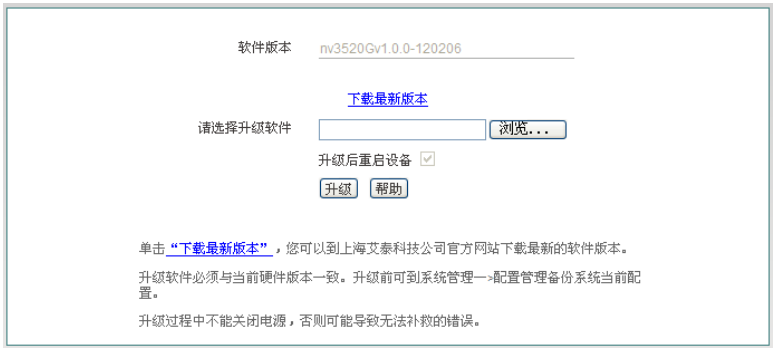

图 13-6 软件升级

- 版本信息：显示设备当前使用的软件版本；
- 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. 请选择合适型号的新软件；
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“浏览…”按钮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”按钮，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设置；

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生效，无须人工干预。

13.6 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。

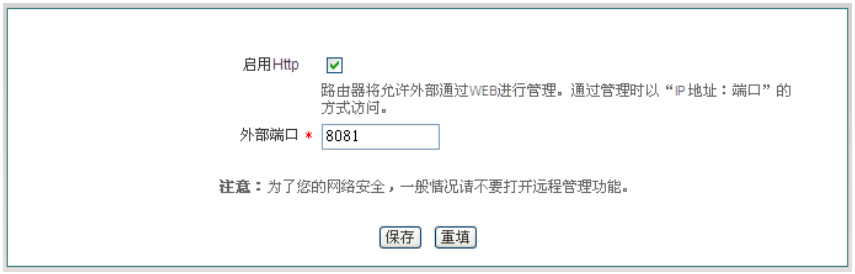

图 13-7 远程管理

- 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局域网 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，请事先打开相关远程管理功能。

13.7 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 13-8 计划任务列表 1

图 13-9 计划任务列表 2

2. 计划任务参数介绍

图 13-10 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14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。

14.1　运行状态

您可以通过运行状态信息列表查看设备各接口的相关信息。在章节 5.2《运行状态》中有介绍，这里不再重述。

14.2　用户状体

本节主要介绍***系统状态—>用户状态***页面，通过查看用户状态信息列表可以清楚的知道内网用户的上传、下载的实时速率。

图 14-1 用户状态信息列表

- IP 地址：内网用户的 IP 地址；

- 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；
- 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。

14.3　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与增强网络安全。

图 14-2 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：显示产品的型号；
- 软件版本：显示设备的软件版本号；
- 历史记录：系统历史记录中，记录了系统启动、无线功能开启等信息；

- 刷新：单击<刷新>，可查看最新的系统信息。

提示：

图 14-2 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15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官方网站的 UTTCare、产品讨论、知识库、预约服务等栏目，方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 15-1 客户服务

如 15-1，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 配置局域网中的计算机

本章讲述如何在 Windows XP 环境下配置计算机的 TCP/IP 属性。

第一步 检查网络 IP 状态

1. 进入“开始”—>“设置”—> “控制面板”页面；
2. 双击“网络和 Internet 连接图标”，进入网络连接页面，右击“本地连接”，选择“属性”，查看“此连接使用下列项目”中查看是否已安装 TCP/IP 协议，如图 A-1 所示，如果出现了“Internet 协议（TCP/IP）”选项，就表示已经安装；

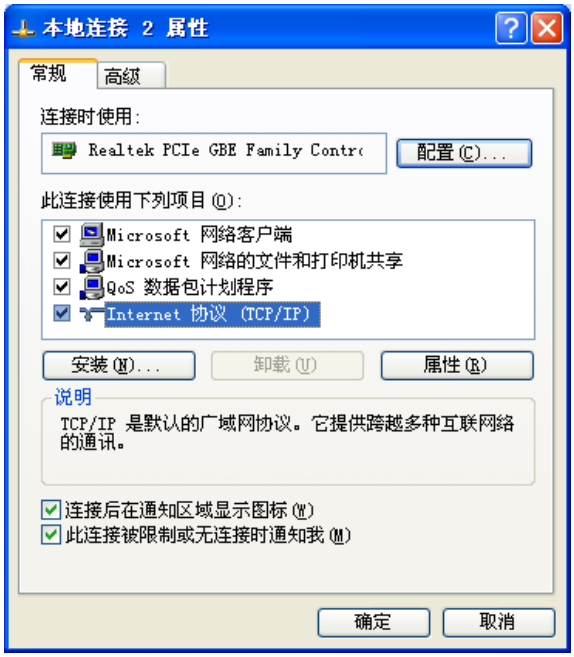

图 A-1 网络配置窗口

3. 如果没有安装 TCP/IP 协议，首先安装 TCP/IP 协议，在“本地连接”—>“属性”中选择“Internet 协议（TCP/IP）”，单击“安装（N）…”，进行 TCP/IP 协议的安装。完成添加 TCP/IP 协议后，需重启计算机来更新系统的网络设定，使其生效。

第二步 配置 TCP/IP 属性

下面分别介绍手工设置 IP 地址和通过 DHCP 服务器设置 IP 地址这两种情形下，配置 TCP/IP 属性的步骤。

方法一 手工设置 IP 地址

1. 在图 A-1 的页面选中“Internet 协议（TCP/IP）”，点击“属性”；
2. 进入“Internet 协议 TCP/IP 属性”窗口，如图 A-2 所示，在常规选项卡中选择“使用下面的 IP 地址”，然后在“IP 地址”中填入：192.168.1.X（X 在 2 至 254 之间），在“子网掩码”中填入 255.255.255.0，在“网关地址”中填入 192.168.1.1；

3. 选择“使用下面的 DNS 服务器地址”选项， 如图 A-2 所示，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。单击“确定”，TCP/IP 属性配置成功。

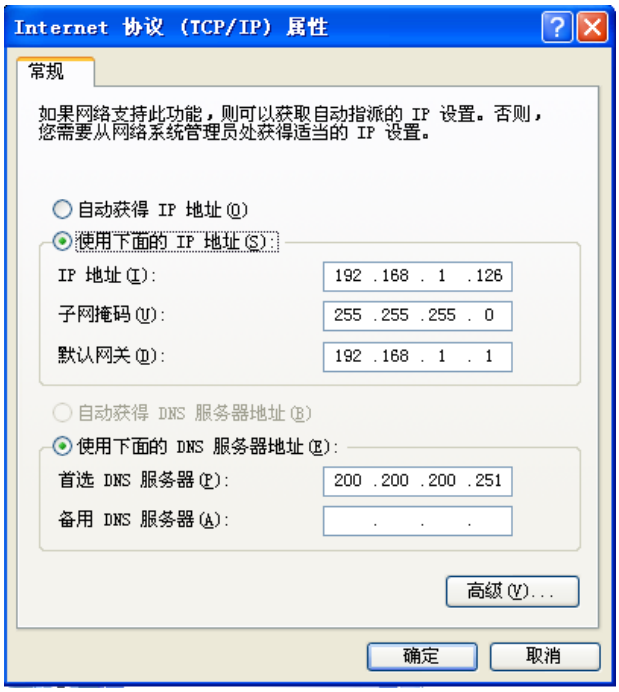

图 A-2 TCP/IP 属性 IP 地址配置窗口

方法二 通过 DHCP 服务器设置 IP 地址

1. 使用此功能之前，必须确保已经在设备的***网络参数—>DHCP 服务器***中已启用 DHCP Server 功能（章节 6.3.1《DHCP 服务器配置》，设备默认开启 DHCP 服务器功能）；
2. 如图 A-2，在常规选项卡中选择“自动获得 IP 地址”和“自动获得 DNS 服务器地址”；
3. 配置完成后，点击“确定”，TCP/IP 属性配置完成。

附录B FAQ

B-1 ADSL 用户如何上网？

1. 首先将 ADSL Modem 设置为桥模式（1483 桥模式）；
2. 确认 PPPoE 线路是标准拨号型（可以使用 WindowsXP 自带 PPPoE 软件拨号测试）；
3. 用网线将设备的 WAN 口与 ADSL Modem 相连，并将电话线连接到 ADSL Modem 的 Line 口；
4. 在***网络参数—>WAN 口配置***页面，配置 PPPoE 线路相关参数；
5. 如果是包月上网的用户，则可选择“自动拨号”的拨号类型。如果不是包月上网用户，则可选择“按需拨号”或者“手动拨号”，并且可以输入空闲时间，以防止忘记断线而浪费上网时间；
6. 若选择了“手动拨号”，则需在***网络参数—>WAN 口配置***的“线路连接信息列表”中进行手动拨号；
7. 拨号成功后，在***网络参数—>WAN 口配置***的“线路连接信息列表”中可以查看该线路的配置和状态信息（如图 B-1），比如“连接状态”（拨号成功后显示为“已连接”）、ISP 分配的“IP 地址”等信息。

图 B- 1 线路连接信息列表——查看 PPPoE 拨号线路信息

8. 正确配置局域网计算机。

B-2 固定 IP 接入用户如何上网？

1. 确认线路正常（可以使用计算机测试）；
2. 用网线将设备的 WAN 口与 ISP 网络设备相连；
3. 在***开始—>配置向导—>WAN1 口配置***或***网络参数—>WAN 口配置***中，配置固定 IP 接入线路的相关参数；
4. 按照本手册附录 A 所述内容配置局域网计算机。

B-3 动态 IP（Cable Modem）接入用户如何上网？

1. 确认线路正常（可以使用计算机测试）；
2. 用网线将设备的 WAN 口与 ISP 网络设备相连；
3. 在***网络参数—>WAN 口配置***页面，配置动态 IP 接入线路参数。
4. 如表 B-2 所示，在***网络参数—>WAN 口配置***的“线路连接信息列表”中，可以查看该线路的配置和状态信息，比如“连接状态”（正常连接时显示为“已连接”）、ISP 分配的“IP 地址”、“网关地址”等信息。

图 B- 2 线路连接信息列表——查看动态 IP 接入线路信息

5. 正确配置局域网计算机

B-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，在“恢复出厂配置”配置栏中，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