无线控制器
高级配置手册

上海艾泰科技有限公司
http://www.utt.com.cn

版权声明

上海艾泰科技有限公司|总部地址：

上海市漕河泾开发区松江高科技园莘砖公路 518 号 9 号楼 3 层（201612）

欲了解艾泰科技更多服务及解决方案，请访问 http://www.utt.com.cn

执行标准：Q/SWBK1-2008

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 WX 系列无线控制器。

本手册描述应用于艾泰科技 ReOS_SE 2.6.3 软件平台下 WX 系列无线控制器的特性和功能，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

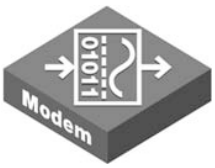
1）　**图标说明**

路由器

交换机

AP 集中控制器（AC）

无线接入点（AP）



Modem

服务器

终端

无线主机

2） **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。
- 表示提示，指出、重点注意事项。

粗体字：表示界面内容，例如菜单、按钮等。

0.4 出厂配置

1） 接口的出厂配置如表 0-1 所示。

接口类型	IP 地址/子网掩码
LAN 口	192.168.1.1/255.255.255.0（具备网关功能的设备）或 192.168.1.252/255.255.255.0（不具备网关功能的设备）
WAN 口	动态 IP 接入

表 0-1 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 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 WX 系列无线控制器的功能和特点。

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 AP 集中管理
- 支持 AC 可通过三层网络发现并管理 AP
- 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 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 URL、MAC 地址、关键字过滤等防火墙策略
- 支持 QQ、MSN 白名单
- 支持内/外网攻击防御
- 支持网络尖兵防御
- 支持用户组、时间段管理
- 支持 VPN 功能
- 支持动态域名（3322.org、iplink.com.cn）
- 支持 UPnP

- 支持端口镜像功能
- 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

提示：

WX 系列无线控制器所支持的功能根据各产品型号的不同而有所差异。各产品之间的功能、性能差异数据可从附赠的产品速查表中获取，或致电艾泰科技客户服务部进行咨询。

1.2 产品规格

- 符合 IEEE802.3Ethernet、IEEE802.3u Fast Ethernet、IEEE802.3ab 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 WX 系列无线控制器的外观，然后讲述如何安装设备。

2.1 面板介绍

此处以 WX100、WX2000 为例进行说明。

WX100 为 1 个 WAN 口（10/100/1000M），4 个 LAN 口（10/100/1000M）的产品，并提供一个内置 USB 接口和一个外置 USB 接口，机壳大小为 11 英寸。其前面板示意图如图 2-1 所示。

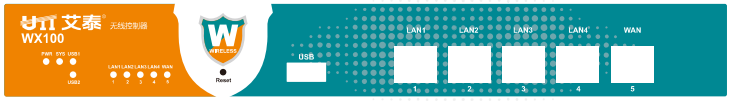


图 2-1 WX100 前面板

WX2000 为 3 个 WAN 口（10/100/1000M），4 个 LAN 口（10/100/1000M）的产品，机壳大小为 19 英寸。其前面板示意图如图 2-2 所示。

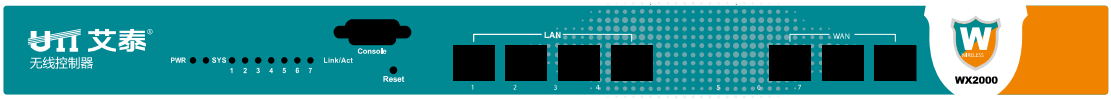


图 2-2 WX2000 前面板

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	端口状态指示灯	当有设备正常连接到某端口后，该端口对应指示灯常亮，该端口有流量时闪烁。
USB	USB 状态指示灯	USB1 灯亮显示内置 USB 接口正在被使用，USB2 灯亮显示外置 USB 接口正在被使用。

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。	
USB	USB 接口	提供一个外置 USB 接口和内置 USB 接口。	连接 U 盘，用于存放设备获取的软件、配置文件。
Console	串口	仅部分产品提供串口。	RS-232 DB9 公头。

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 安装注意事项

1） 要确保安装工作台或标准机架的平稳性。

2） 请勿在设备上放置重物。

3） 确保设备存放环境的干燥和通风散热性，请勿将设备置于脏乱和潮湿的地方。

4） 避免直接将设备暴露在阳光下，尽量远离发热元件。

5） 请使用原装电源线。

2.3 安装准备

1） 已向当地运营商 ISP（ 如中国电信、中国联通等）申请宽带服务。

2） 相关设备准备：

(1) 调制解调器（直接接入以太网时不需要此物件）。

(2) 集线器或交换机或无线设备。

(3) 已安装以太网卡、Internet 协议（TCP/IP）的 PC。

(4) 电源插座 。

3） 工具及线缆准备：十字螺丝刀、网线。

2.4 硬件安装

在安装设备前，请确认宽带服务正常。如果无法正常访问，请先联系运营商（ISP）解决该问题。成功访问网络后，请遵循以下步骤安装设备。安装时需拔除电源插头。

1） 安装在工作台上

您可以将设备放置在平稳的工作台上，安装步骤如下：

(1) 将设备底部朝上放置在足够大、平稳且接地良好的工作台上。

(2) 揭去脚垫的胶面保护纸，把 4 个脚垫分别粘贴在机壳底部的 4 个圆型凹槽内。

(3) 把设备翻转过来，平稳地放置在工作台上。

2） 安装在标准机架上

将设备安装在 19 英寸标准机架上，安装步骤如下：

(1) 检查机架的接地与稳定性。

(2) 将配件中的两个 L 型支架分别安装在设备面板的两侧，并用配件中的螺丝固定。

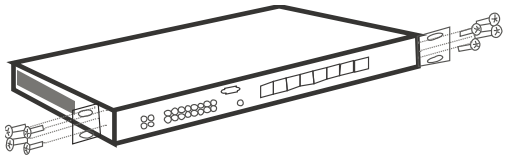


图 2-3 产品机架安装图一

(3) 将设备安放在机架内适当的位置，由托架支撑。

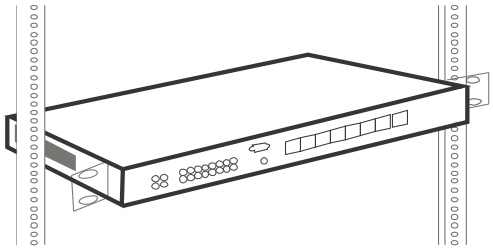


图 2-4 产品机架安装图二

(4) 用螺丝钉将 L 型支架固定在机架两端固定的导槽上。

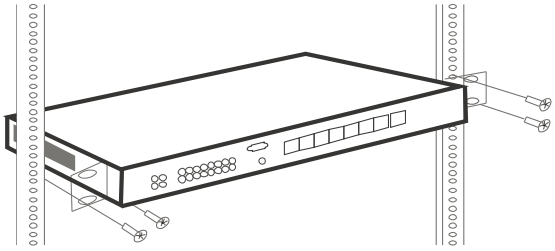


图 2-5 产品机架安装图三

2.5 硬件连接

硬件连接的方式分为两种：网关模式下的硬件连接和旁路模式下的硬件连接。

1） 网关模式下的硬件连接：

(1) 建立局域网连接

用网线连接路由器的LAN 口和局域网中的PC或者集线器、交换机、无线设备。

(2) 建立广域网连接

用网线将路由器WAN 口与Internet 相连，如下图所示。

(3) 连接电源

打开电源之前确保电源供电、接地正常。

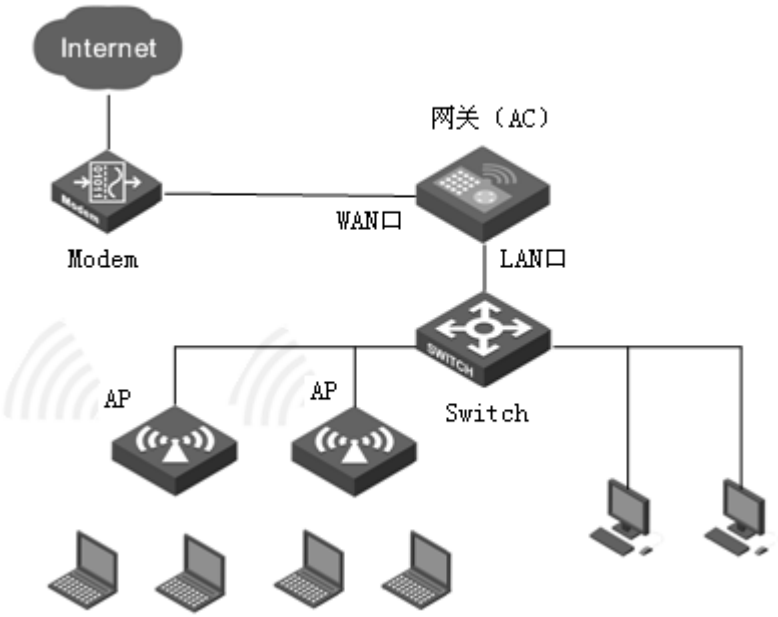


图 2-6 网关模式下的硬件连接拓扑

2） 旁路模式下的硬件连接：

(1) 建立局域网连接

用网线连接路由器的LAN 口和AP集中控制器（AC）、局域网中的PC或者集线器、交换机、无线设备。

(2) 建立广域网连接

用网线将路由器WAN 口与Internet 相连，如下图所示。

(3) 连接电源

打开电源之前确保电源供电、接地正常。

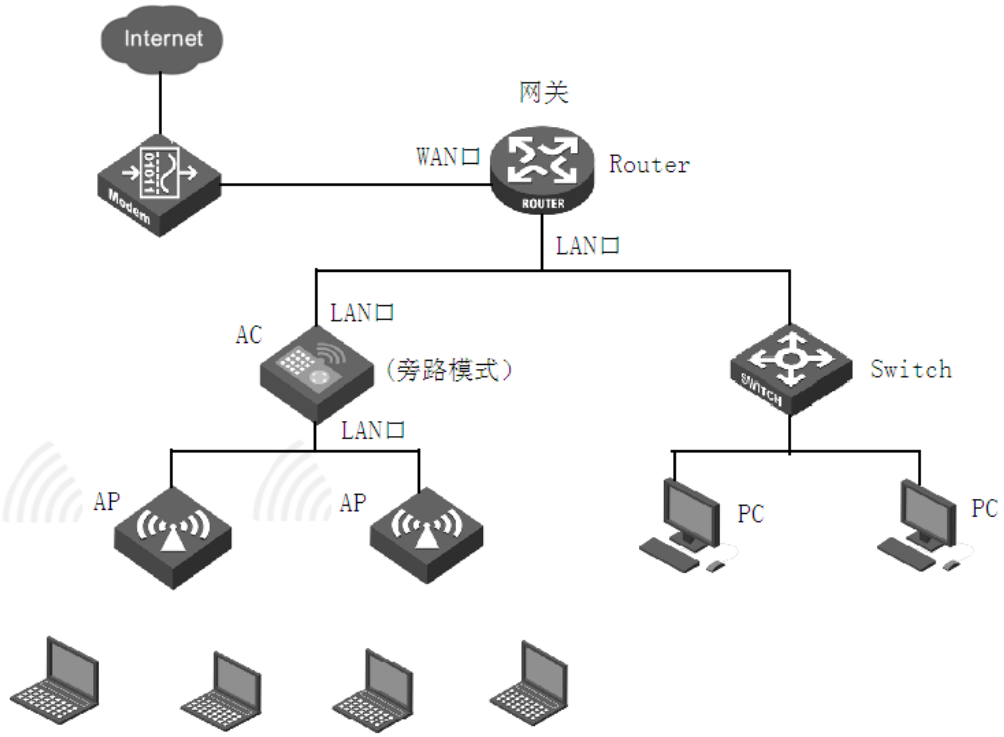


图 2-7 旁路模式下的硬件连接拓扑

提示：以上网络连接示意图仅供参考，请根据实际情况和需求配置适合的网络。

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 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 中的任意一个空闲地址，子网掩码为 255.255.255.0，网关地址为 192.168.1.1（网关的 LAN 口 IP 地址，有网关功能的设备默认 LAN 口 IP 地址为 192.168.1.1），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（网关的 LAN 口 IP 地址）。

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网关建立连接。

```
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：如果网关 LAN 口 IP 地址为 192.168.1.1，那么计算机的 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：带有网关功能的设备请输入 http://192.168.1.1，未带网关功能的设备请输入 http://192.168.1.252。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**。

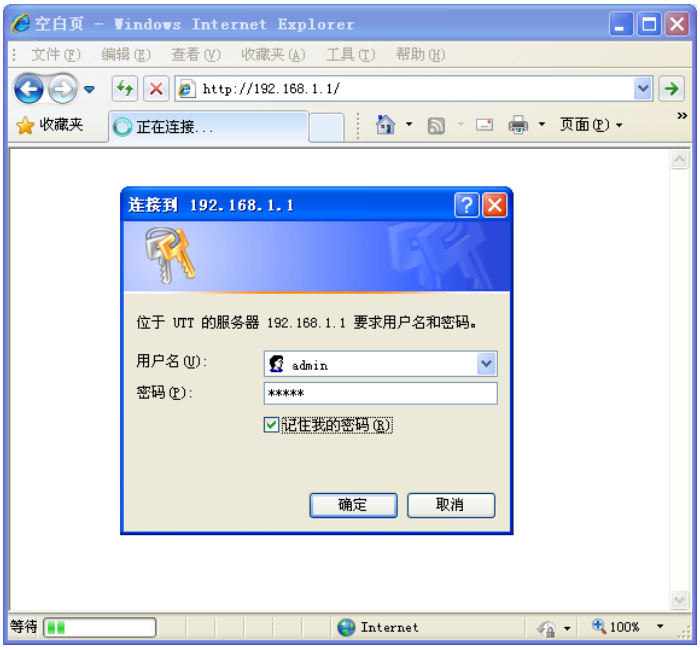


图 3-1 WEB 登录界面

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。

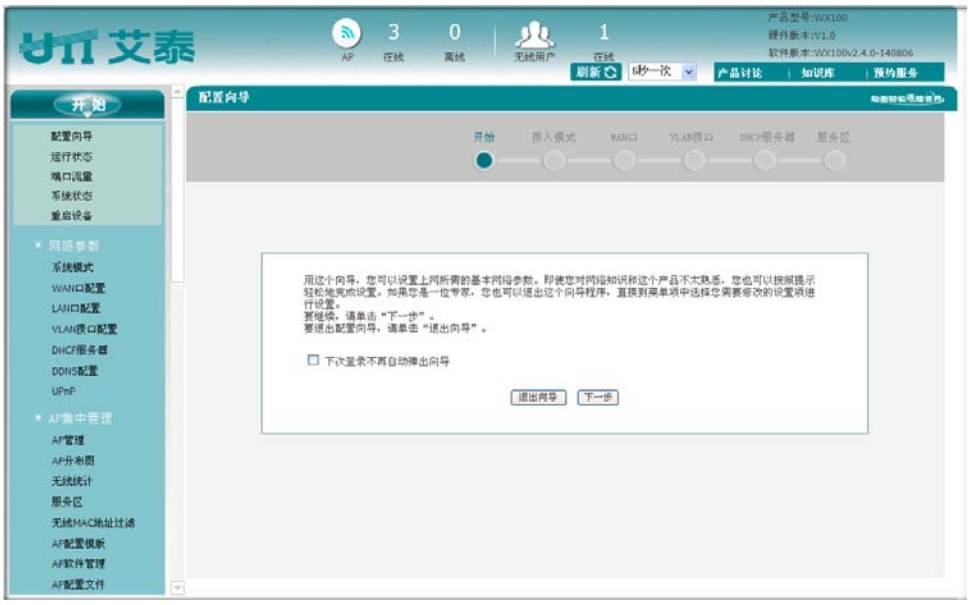


图 3-2 WEB 界面首页

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) 该页面上侧显示 AP 的在线、离线数，以及无线用户的在线数，并可以刷新。顶部图标含义如下：

   (1) 

表示 AP， 

、 

，显示当前该网络中实时的在线和离线 AP 数量。

   (2) 

表示无线用户数， 

：显示连接到 AC 管控的 AP 上的总无线用户数量。

   (3) 

：设置刷新顶部的 AP 在线和离线数、无线用户的数量的频率。

3) 该页面左侧显示主菜单条。

4) 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。

5) 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，详情请参阅：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信息页面。
- 配置菜单：可选择任意菜单进行配置：接入模式、WAN 口、VLAN 接口、DHCP 服务器、服务区。
- 接入模式：可选择**网关模式**和**旁路模式**，若选择**旁路模式**则需要填写设备上网的网关地址和 DNS 服务器地址，且必须重启设备。
- 点击**离开**按钮：配置不生效，页面自动跳转到**无线统计**页面。
- 点击**跳过**按钮：配置不生效，页面将跳转到下一个页面。
- 点击**下一步**按钮：配置生效，页面将跳转到下一个页面，直到配置完成，点击**完成**按钮配置生效。
- 点击**完成**按钮，配置生效。

4.1　WAN1 口配置——动态IP接入

配置向导的第三个页面可对设备的 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**，如下图所示。 如果您的上网线路接入方式为**动态 IP 接入**，请直接点击**完成**按钮，完成上网线路的配置。

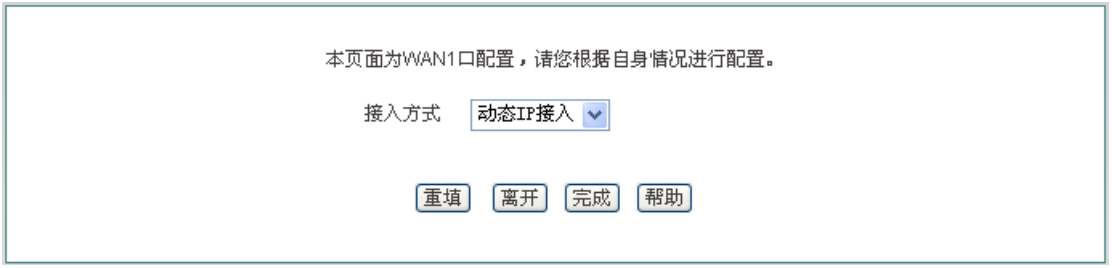


图 4-2 配置向导—动态 IP 接入

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**，请在如下图的下拉列表框中选择**固定 IP 接入**。下面介绍固定 IP 接入的各项参数的涵义。

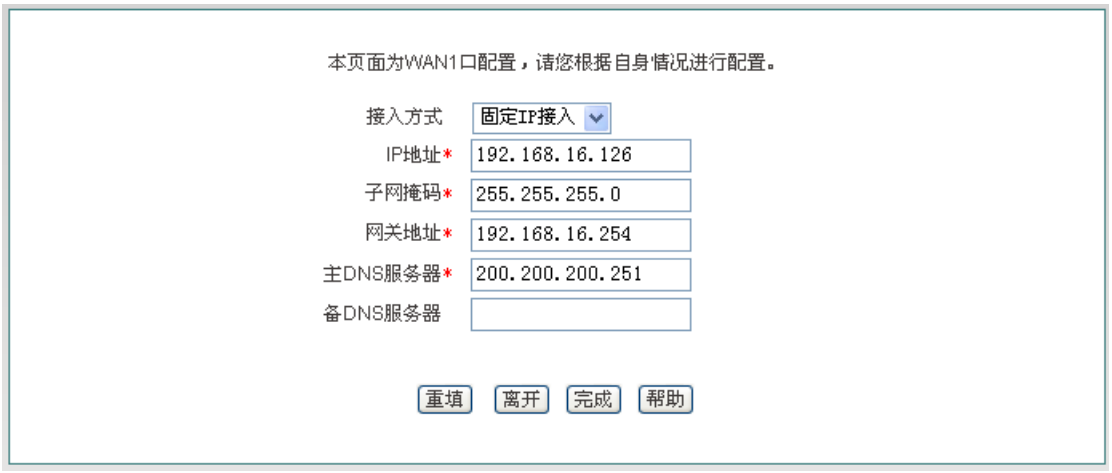


图 4-3 配置向导—固定 IP 接入

- 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**，请在下图的下拉列表框中选择 **PPPoE 接入**。下面介绍 PPPoE 接入的各项参数的涵义。

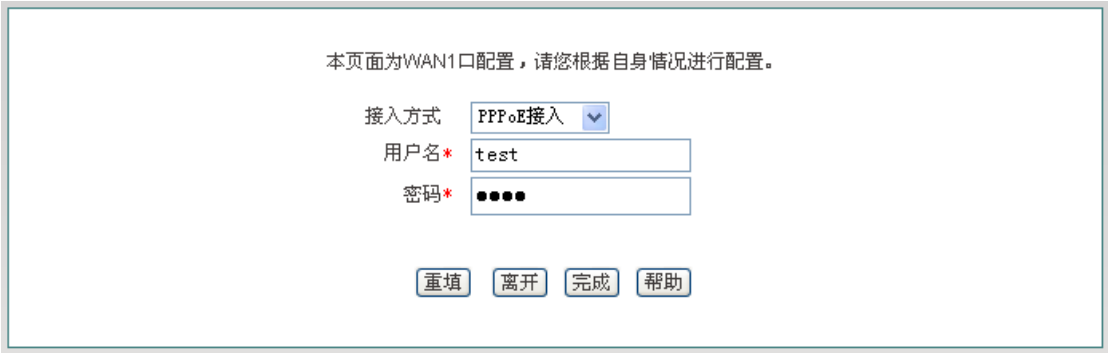


图 4-4 配置向导——PPPoE 接入

- 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 WAN1 口的上网线路后请点击**完成**按钮，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、系统状态、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阅：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。如下图所示界面可知各接口的连接类型、连接状态、IP 地址等信息。

图 5-1 运行状态信息列表

5.3　端口流量

本节讲述**开始—>端口流量**页面，如下图所示，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实时速率（提供的单位有：kbit/s 和 KB/s）。

提示：

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

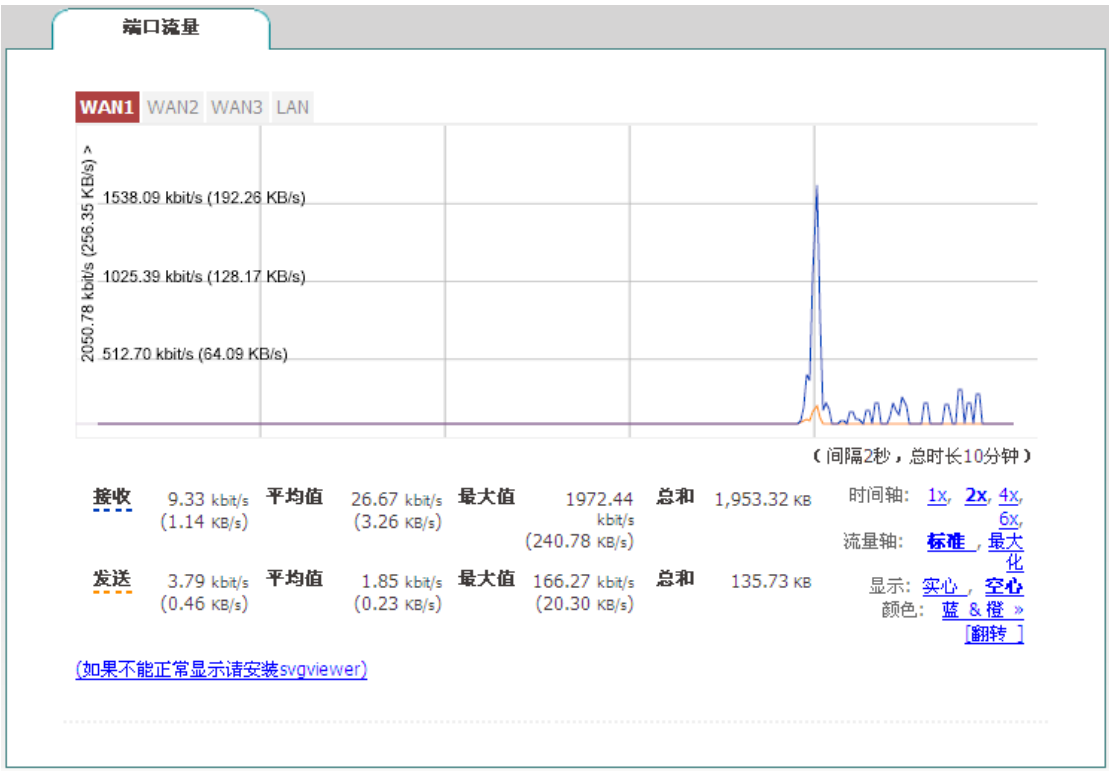


图 5-2 接口流量

- 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。
- WAN：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。
- 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　系统状态

本节介绍**开始—>系统状态**页面。可查看设备当前的系统状态，包括 AP, SSID 和历史用户统计，以及在线用户、AP 日志、系统信息等的信息。

图 5-3 系统状态

5.5　重启设备

在**开始—>重启设备**页面，您可以点击**重启**按钮重新启动设备。

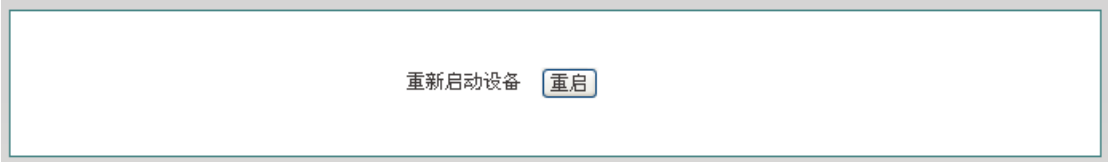


图 5-4 重启设备

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、VLAN 接口、DHCP 服务器、DDNS 配置和 UPnP 配置。

6.1　系统模式

本节介绍**网络参数—>系统模式**的配置界面及方法。

在本界面可以配置设备的系统模式，主要有两种配置模式：网关模式，旁路模式。
网关模式下，AC 既可以作为路由器也可以作为 AP 集中控制器管理 AP；旁路模式下，AC 只能作为 AP 集中控制器管理 AP。注意不管设备工作在哪种模式下，只要对设备切换模式，必须重启设备，配置才会生效。

6.1.1　网关模式配置

如果您的系统模式为网关模式，请在如下图的下拉列表中选择**网关模式**，点击**保存**，完成系统模式的配置。

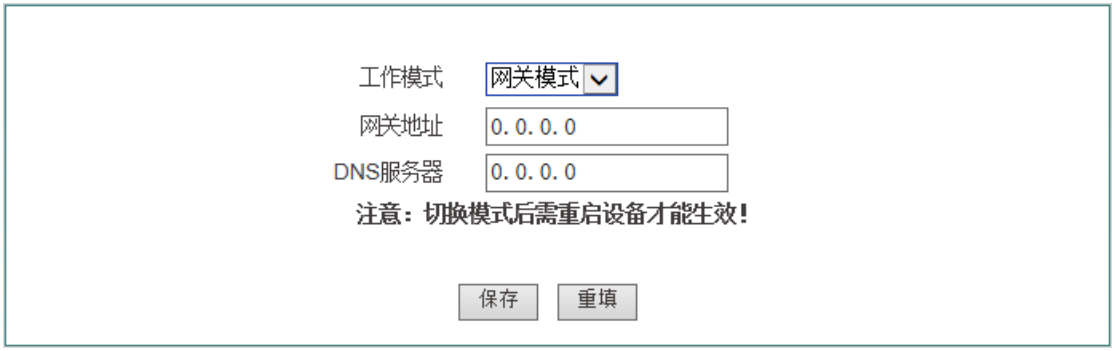


图 6-1 网关模式配置

- 网关地址：填写设备网关的接口地址。
- DNS 服务器：建议填写设备网关的 DNS 服务器地址。

6.1.2　旁路模式配置

如果您的系统模式为旁路模式，请在如下图的下拉列表中选择**旁路模式**，点击**保存**，完成系统模式的配置。

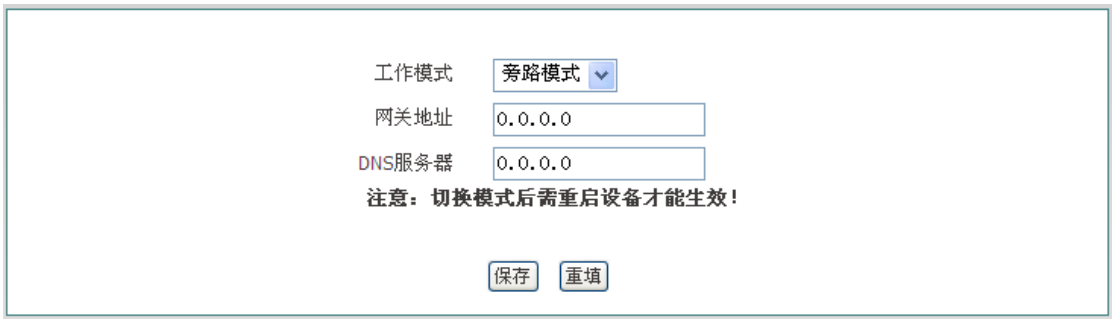


图 6-2 旁路模式配置

- 网关地址：填写设备网关的接口地址。
- DNS 服务器：建议填写设备网关的 DNS 服务器地址。

6.2　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。

6.2.1　网络接口配置

进入**网络参数—>WAN 口配置**页面，配置界面如图 6-3 所示。

图 6-3 WAN 口配置

上网线路的连接类型有：动态 IP 接入、固定 IP 接入、PPPoE 接入。

1)　动态 IP 接入

如图 6-3 所示为动态 IP 接入方式的界面，下面介绍各项参数的涵义。

- 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，可选项分别为运营商策略、电信、联通及移动。
- 工作模式：选项有 NAT 模式和路由模式。
  - NAT 模式：网络地址转换，工作在此模式下的路由器能将内网（LAN 侧）的 IP 地址转换为外网（WAN 侧）的 IP 地址。路由器默认工作在此模式。
  - 路由模式：工作在此模式下的路由器对内网（LAN 侧）访问外网（WAN 侧）的地址不进行 NAT 转换，直接查找路由表进行转发。

  提示：NAT 模式跟路由模式均可以单独生效于某一条线路。
- MAC 地址：相应接口的 MAC 地址，一般无需修改。
- 接口模式：设置接口的双工模式及速率。选项有：Auto（自适应）、10M-FD（10M 全双工）、10M-HD（10M 半双工）、100M-FD（100M 全双工）、100M-HD（100M 半双工）、1000M-FD（1000M 全双工，千兆设备支持）。默认为 Auto，一般情况下不需要修改，如有兼容性问题，或使用的设备不支持自动协商功能，可以在此设置以太网协商的类型。

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

如下图所示的界面为固定 IP 接入方式的配置界面。

图 6-4 固定 IP 接入

- 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。
- 高级选项中的工作模式，MAC 地址，接口模式请参照动态接入方式中的配置。

3） PPPoE 接入

如下图所示的界面为 PPPoE 接入方式的配置界面。

图 6-5 PPPoE 接入

- 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**下方点击相关按钮进行手动连接和挂断。
  - 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。
- 高级选项中的工作模式，MAC 地址，接口模式请参照动态接入方式中的配置。

6.2.2　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，如下图所示。

图 6-6 线路连接信息列表

图 6-7 线路连接信息列表（续图 6-6）

- 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，如下图所示，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 6-8 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，如下图所示。

图 6-9 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。

6.3　线路组合

对于多 WAN 口设备，设备还支持线路组合及检测的功能。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。

6.3.1　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。

6.3.2　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

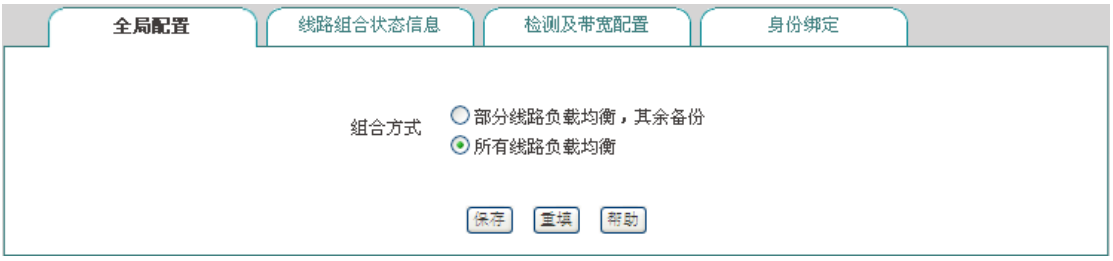


图 6-10 线路组合—所有线路负载均衡

- 线路组合方式：这里选择**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**。

2)　部分线路负载均衡，其余备份

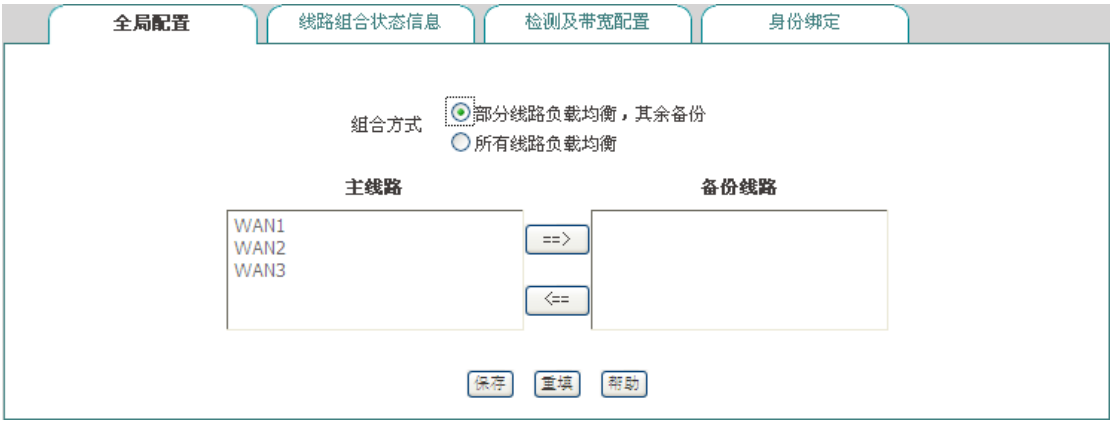


图 6-11 线路组合配置—部分线路负载均衡，其余备份

- 线路组合方式：这里选择**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。

6.3.3　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。如下图所示。

图 6-12 线路组合状态信息列表

图 6-13 线路组合信息列表（续图 6-12）

- 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、固定接入、PPPoE 接入。
- 带宽：显示线路已设置的带宽值。
- 线路状态：显示检测后的线路状态，分为已连接、未连接。

- 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。

6.3.4　检测及带宽配置

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—>检测及带宽配置**页面，或者点击**线路组合状态信息列表**线路的接口或者是编辑图标，进入**检测及带宽配置**页面。

图 6-14 线路检测及带宽配置

- 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 10。
- 检测目标 IP 地址：欲检测目标的 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。

6.3.5　身份绑定

当设备为多 WAN 口时，可以进入**网络参数—>线路配置—>身份绑定**页面启用身份绑定功能。

在多线路会话负载均衡的情况下，同一应用的 NAT 会话可能分布在不同的线路上，这样就会导致像网银、QQ 等应用由于身份变化而不能正常使用，身份绑定功能通过将这些来自同一用户的同一应用的会话绑定在一条线路上解决了这个问题。举个例子来说，内网某个用户在登录网上银行时，如果第一条会话被分配到 WAN2 口连接线路上，此后此用户所有的网银会话都会走 WAN2 口出去，直到此用户退出登录。

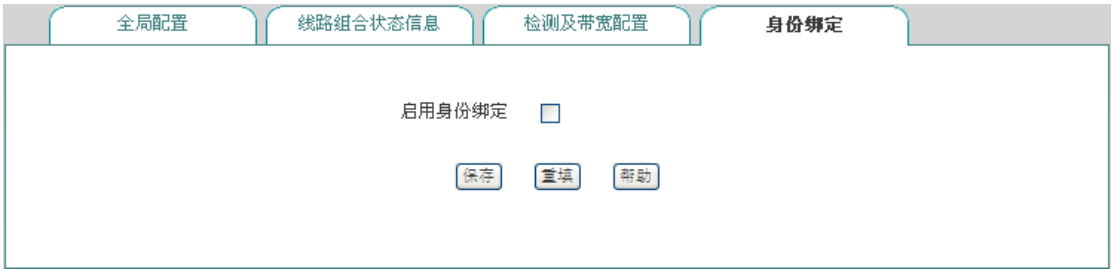


图 6-15 启用身份绑定

6.4　LAN口配置

设备 LAN 口可配置 4 个 IP 地址，LAN 口第一个默认 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，请进入**网络参数—>LAN 口配置**页面进行配置。

图 6-16 LAN 口配置

- IP 地址：设置 LAN 口的 IP 地址，第一个 IP 地址默认为 192.168.1.1，其他的三个 IP 地址默认为 0.0.0.0。
- 子网掩码：设置相应 IP 地址的子网掩码，默认都为 255.255.255.0。

- MAC 地址：LAN 口的 MAC 地址。建议不要随意修改 LAN 口的 MAC 地址。
- 接口模式：设置接口的双工模式及速率。选项有：Auto（自适应）、10M-FD（10M 全双工）、10M-HD（10M 半双工）、100M-FD（100M 全双工）、100M-HD（100M 半双工）、1000M-FD（1000M 全双工，千兆设备支持）。默认为 Auto，一般情况下不需要修改，如有兼容性问题，或使用的设备不支持自动协商功能，可以在此设置以太网协商的类型。

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！

6.5　VLAN接口配置

本节介绍**网络参数—>VLAN 接口配置**，可在 LAN 口上建立基于指定 VLAN 的子接口，并可以配置 IP 地址和子网掩码，可以通过 VLAN 子接口访问 AC。

6.5.1　VLAN接口列表

VLAN 接口列表主要显示 VLAN 接口的信息，包括名称、状态、VLANID、IP 地址、子网掩码等信息。

图 6-17 VLAN　接口列表

6.5.2　VLAN接口配置

点击**VLAN 接口配置**或**添加新条目**，便可进入 VLAN 接口配置页面。配置的 VLAN 接口可在 DHCP 地址池和服务区配置中引用.

图 6-18 VLAN 接口配置

- 启用：打钩表示启用该功能。
- 名称：自动生成，该名称与 VLAN ID 保持一致。
- VLAN ID ：设置需要的 VLAN ID 号，范围为 1-4094。
- IP 地址：设置 VLAN ID 的 IP 地址。
- 子网掩码：设置子网掩码。
- 保存：点击**保存**，配置生效。

6.6 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 地址池配置、静态 DHCP、DHCP 客户端列表和 DNS 代理。

6.6.1 DHCP地址池

设备默认会将 default 地址池中的地址下发给有线接入设备的客户端，管理员也可通过创建新的地址池，让通过 AP 无线接入设备的客户端获取不同网段的 IP 地址。

在**网络参数—>DHCP 服务器—>DHCP 地址池**页面，可在指定 VLAN 接口上启用 DHCP 服务器功能，可以在 VLAN 虚接口上配置 DHCP 服务器，可以在 VLAN 虚接口及 LAN 口上启用或关闭 DHCP 服务器功能，可以为不同的 VLAN 虚接口及 LAN 口分配不同网段的 IP 地址，管理员可通过 DHCP 地址池列表查看已配置的地址池。点击列表下方的**添加新条目**可进入 DHCP 地址池配置页面，如下图所示：

图 6-19 DHCP 地址池列表

图 6-20 DHCP 地址池配置

- 启用：打钩表示启用该地址池。
- 名称：自定义该地址池的名称。
- VLAN 接口：选择要配置 DHCP 服务器的接口。VLAN 接口在 **VLAN 接口配置**页面建立。
- 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。
- 子网掩码：DHCP 服务器给内网计算机自动分配的子网掩码。
- 网关地址：DHCP 服务器给内网计算机自动分配的网关 IP 地址。
- 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：分钟）。
- 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。

6.6.2　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，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 6-21 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 时各项参数的涵义。

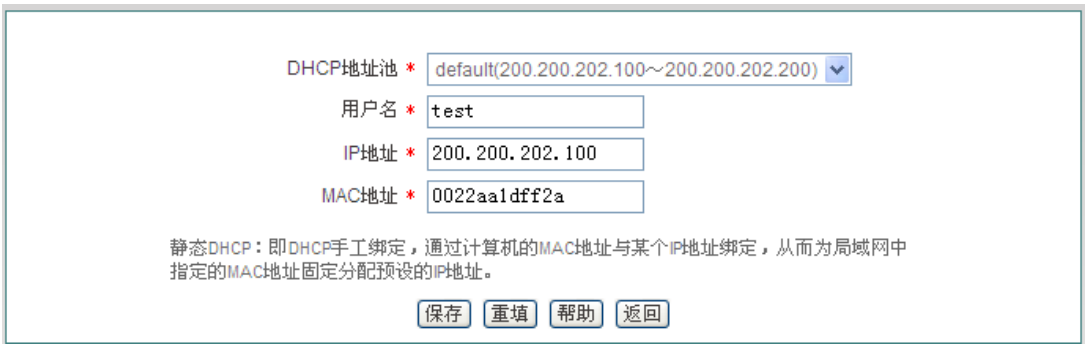


图 6-22 静态 DHCP 配置

- DHCP 地址池：选择相应的地址池。
- 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，必须是上面 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。

6.6.3 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 192.168.1.101 的 IP 地址分配给 MAC 地址为 00:22:AA:D6:67:78 的内网计算机，该计算机租用该 IP 地址剩余的时间为 1 小时 51 分 53 秒。

图 6-23 DHCP 客户端列表

6.6.4　DNS代理

在本页面启用 DNS 代理功能并设置运营商 DNS 服务器。

图 6-24 DNS 代理配置

- 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：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。

6.6.5　DHCP配置实例

1)　应用需求

本实例中，要求设备开启 DHCP 功能，起始地址为 192.168.1.100，结束 IP 地址为 192.168.1.200；其中 MAC 地址为 00:21:85:9B:45:46 的主机获取固定的 IP 地址：192.168.1.100;MAC 地址为 00:1f:3c:0f:07:f4 的主机获取固定的 IP 地址:192.168.1.101。

2)　配置步骤

第一步，进入**网络参数—>DHCP 服务器—> DHCP 地址池列表**页面，启用 DHCP 服务器功能。

第二步，修改系统默认地址池 default，在 DHCP 地址池列表中点击“default”，进入如下图所示页面，配置完后点击**保存**。

图 6-25 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。

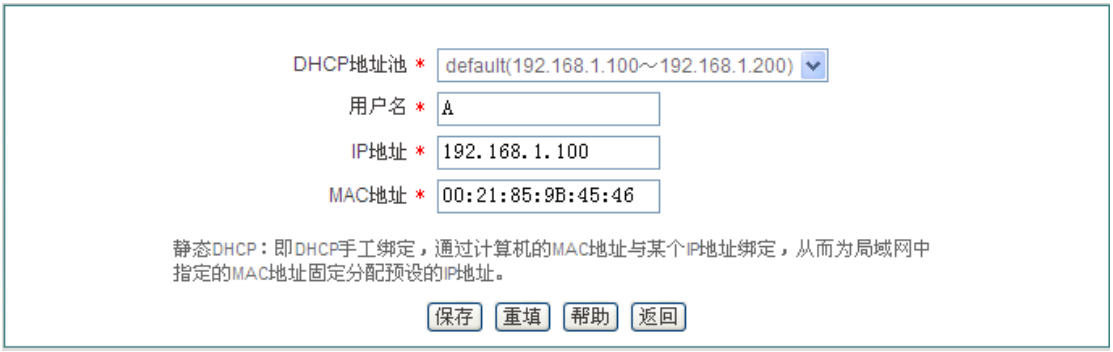


图 6-26 静态 DHCP 配置—实例 A

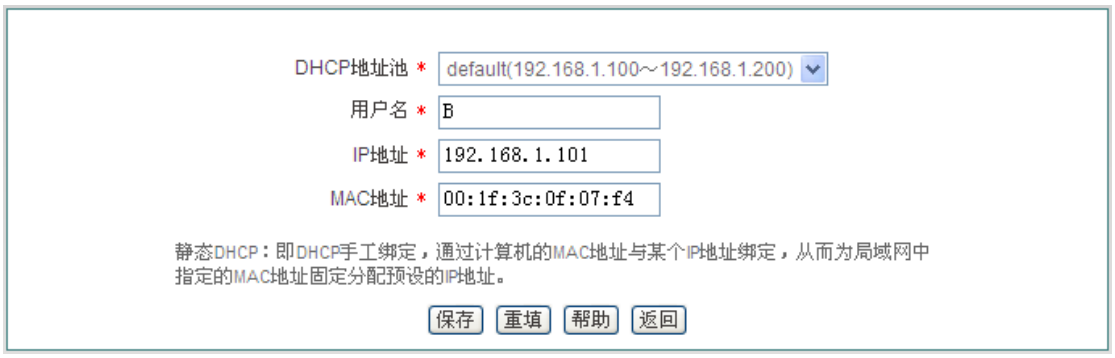


图 6-27 静态 DHCP 配置—实例 B

至此配置完成，可以在**静态 DHCP 列表**中查看这 2 个静态 DHCP 条目的相关信息，如图 6-28 所示。如果需要修改配置，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 6-28 静态 DHCP 信息列表—实例

6.7　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。

6.7.1　花生壳的DDNS服务

图 6-29 配置 DDNS—花生壳

- 服务商：提供 DDNS 服务的运营商，此处选择**花生壳**。
- 注册域名：单击超链接 http://www.oray.net 即可进入花生壳域名申请页面。
- 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。
- 注销：删除当前已有的信息。
- 升级服务：点此链接进入花生壳购买区。
- 服务帮助：点此链接进入花生壳客服中心。
- **提示：**WAN 口地址必须为公网地址才能将路由器的地址映射到域名。

6.7.2　3322 的DDNS服务

1）申请 3322.org 的 DDNS 账号

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

图 6-30 注册 3322.org 动态域名

2）3322.org 的 DDNS 配置

图 6-31 配置 DDNS—3322.org

- 服务商：提供 DDNS 服务的运营商，此处选择 3322.org。
- 注册域名：单击超链接 http://www.pubyun.com 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 口地址必须为公网地址才能将路由器的地址映射到域名。

6.7.3　Iplink的DDNS服务

图 6-32 配置 DDNS—iplink.com.cn

- 服务商：DDNS 服务的提供商，此处选择 iplink.com.cn。
- 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。
- 接口：选择绑定 DDNS 服务的接口。

6.7.4　Dyndns的DDNS服务

1）申请账号

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

2）dyndn.org 的 DDNS 配置

图 6-33 配置 DDNS—dyndns.org

- 服务商：提供 DDNS 服务的运营商，此处选择 **dyndns.org**。
- 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。

6.7.5　no-ip.com的DDNS服务

1）申请账号

请登录 http://www.dyndns.org 申请后缀名为 no-ip.com 的二级域名。

2）no-ip.com 的 DDNS 配置

图 6-34 配置 DDNS—no-ip.com

- 服务商：提供 DDNS 服务的运营商，此处选择 no-ip.com。
- 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。

6.7.6　Uttcare 的DDNS服务

图 6-35 配置 DDNS—uttcare

- 服务商：提供 DDNS 服务的运营商，此处选择 uttcare.com。
- 主机名：有两种连接方式，一种是默认主机名，默认主机名是根据序列号自动生成的，只需要配置接口就可以使用。第二种是自定义主机名，主机名可以在 www.utt.com.cn/ddns 注册 uttcare 账号。
- 接口：选择 DDNS 服务绑定的接口。

6.7.7　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。

6.8 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 6-36 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 AP 集中管理

WX 系列无线控制器提供了一个专一的区域来配置和管理整个无线网络，设备作为无线控制器是一个无线网络的核心，负责管理无线网络中的 AP，对 AP 的管理包括：下发软件、下发配置、修改相关配置等。

WX 系列无线控制器和 AP 间能穿透三层网络设备相互发现。AC 可正常管理通过三层和二层网络发现的 AP 。

本章主要介绍 AP 集中管理相关概念，再介绍设备的 AP 集中管理功能，包括：AP 管理、AP 分布图、无线统计、服务区、无线 MAC 地址过滤、AP 配置模板、AP 软件管理、AP 配置文件、AP 负载均衡、AP 计划任务、AP 日志管理。

7.1 AP集中管理概述

7.1.1 术语

客户端（无线客户端）：带有无线网卡的 PC 或便携式笔记本电脑等终端。

WLAN（Wireless Local Area Network，无线局域网）：使用无线连接的局域网，它使用无线电波作为数据传送的媒介。

AC（Access Controller，无线控制器）：对无线局域网中的所有 AP 进行控制与管理。

AP（Access Point，接入点）：提供无线客户端到局域网的桥接功能，在无线客户端与无线局域网之间进行无线到有线和有线到无线的帧转换。

胖 AP：可独立管理，一般支持 DHCP 服务器、DNS、时钟管理等功能。

瘦 AP：工作在 AP 模式下的设备，其软件、配置文件即可从 AC（无线控制器）上获取，也可从本地获取，以实现智能化的高效控制，可降低人工管理维护的难度。

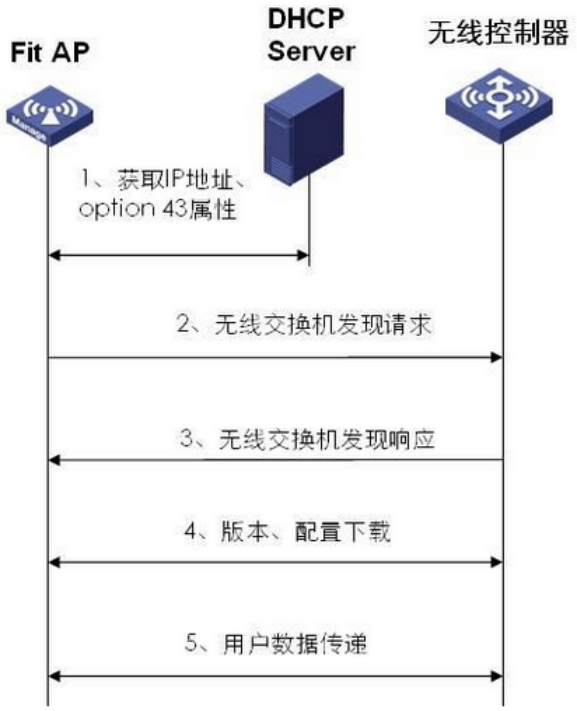
二层漫游：一个无线终端从无线控制器的一个 AP 漫游到同一个无线控制器内的另一个 AP 的过程。

7.1.2 工作原理

Fit AP ＋ 无线控制器解决方案的实现，首要而且关键的一步就是 Fit AP 在三层交换机上的注册问题，只有 Fit AP 成功注册后无线控制器才能管理 Fit AP。AC＋Fit AP 跨越三层网络注册在实际应用中也比较常见。我司设备有三种实现方式：第一种为 DNS 方式，需要 DNS、DHCP Server 配合实现，相对复杂；第二种为 DHCP Option43 属性方式，即利用 DHCP Server 的 Option43 属性来实现；第三种为通过在 AP 上配置 AC 的地址实现，此方法相对比较简单。

无线控制器 AC 与 Fit AP 跨越三层网络连接时的注册流程采用 Option 43 方式、Fit AP 与无线控制器跨越三层网络连接时，Fit AP 可通过 DHCP 的 Option 43 属性直接获取无线控制

器的 IP 地址，从而完成在无线控制器上的注册，具体流程如下图所示：



Fit AP 与无线控制器跨越三层网络连接时，Fit AP 通过 DHCP server 的 Option 43 属性在无线控制器上的注册步骤如下：

1) Fit AP 通过 DHCP server 获取 IP 地址、option 43 属性（此属性中携带三层交换机的 IP 地址信息）。

2) Fit AP 会从 option 43 属性中获取三层交换机的 IP 地址，然后向无线控制器发送单播发现请求。

3) 接收到发现请求报文的无线交换机无线控制器会检查该Fit AP是否有接入本机的权限，如果有则回应发现响应。

4) Fit AP 从无线交换机无线控制器下载最新软件版本。

5) Fit AP 从无线控制器下载最新配置。

6) Fit AP 开始正常工作和无线控制器交换用户数据报文。

提示：

1) 在设备运行过程中，当 AP 上的配置文件被修改，如加入到某服务区等，AC 会在本地保存修改后的配置文件并下发给 AP，AC 断电后该配置文件会删除。

2) AC 远程将 AP 恢复到出厂配置后，AC 会删除之前所保存的配置文件。

3) AP 上传的配置文件不会在**配置文件列表**中显示。

4) AP 成功获取软件、配置文件后即可开始传递用户数据。

7.1.3 二层无线漫游

无线漫游是当网络环境存在多个 AP,且它们的无线覆盖范围互相有一定范围的重合时，无线用户可以在同一 VLAN 的覆盖区内移动，无线网卡能自动发现附近信号强度最大的 AP，并通过这个 AP 收发数据，保持不间断的网络连接。

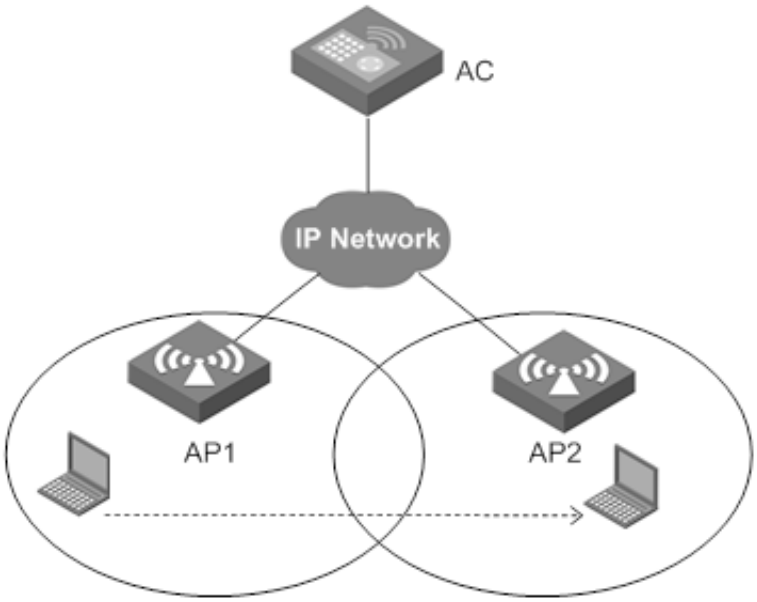


图 7-1 二层漫游

如上图所示，AP1、AP2 属于同一 VLAN 并关联到 AC。

1) 一个终端通过无线方式关联到 AP1，AP1 连接 AC。

2) 该终端断开与 AP1 的关联，漫游到同一 VLAN 中与无线控制器 AC 相连的 AP2 上。

3) 该终端从 AP1 连接到 AP2 的过程即为二层无线漫游。

实现方式：在设备上配置服务区并开启漫游功能，将 AP1、AP2 加入同一个服务区中，当 AP 达到所设定的漫游阈值时即可实现二层无线漫游。

7.2 AP管理

本节介绍 AP 管理菜单下的 AP 列表。

通过 AP 列表查看已刷新的无线设备，在知道登录密码的前提下，可远程管理 AP。

7.2.1 AP列表

在 **AP 集中管理—>AP 管理—>AP 列表**页面，管理员可以通过点击列表下的**刷新**按钮，显示当前内网中的所有无线设备。点击**管理**链接能远程管理此无线设备。

图 7-2 AP 列表

- 管理：点击不同的图标，可对当前 AP 进行不同操作，只可对在线 AP 进行操作。
  - ：点击可对当前 AP 进行管理，进入 AP 远程管理页面，显示远程 AP 的基本信息和可管理内容。
  - ：定位按钮：点击可进入 AP 分布图，可在 AP 分布图上定位 AP 的位置。
  - ：重启按钮：点击可重启当前 AP。
- AP 名称：显示当前 AP 的名称。
- AP 型号：显示当前 AP 的型号。
- 序列号：显示当前 AP 的序列号。
- IP：显示当前 AP 的 IP 地址，点击该 IP 地址能登陆到当前 AP 的管理界面。
- MAC：显示当前 AP 的 MAC 地址；点击该 MAC 地址，可查看当前 AP 的基本信息，包括概览、射频和当前接入该 AP 的用户。
- VID：显示当前 AP 所在的 VLAN ID。
- 状态：显示当前 AP 的状态，在线或离线。
- 客户端数量：显示当前 AP 所带客户端的数量，点击该数字能进入 **AP 集中管理—>无线统计**页面查看无线客户端的相关信息。
- 无线模式/信道：模式：显示当前 AP 的无线模式，信道：显示当前 AP 所使用的信道，当 AP 信道配置为自动时，可显示出实际使用的信道。
- SSID：显示当前 AP 的 SSID。
- 下载/上传速率：显示 AP LAN 口接收数据、发送数据的速率（bps）。

- 刷新：点击**刷新**按钮刷新该列表。
- 型号：显示当前在线 AP 型号。
- 批量操作：选择多个 AP 后，点击该按钮，能对这些 AP 进行如下远程操作：统一修改登录密码、重启、恢复出厂值等。

提示：AP 列表只能显示艾泰科技 WA 系列产品的所有信息，并可以远程管理它们。

7.2.1.1 单机管理

在 AP 列表中，点击 IP 地址，可进入当前 AP，并可进行相应的操作。点击第一列的**管理**链接，能进入如下图所示的 WEB 页面。在该页面能查看到当前 AP 的设备名、型号、MAC 地址、软件版本等信息，并且可以对它进行相关的操作。

图 7-3 单机管理

1） 基本设置

在图 7-3 所示的页面中点击**基本设置**，能进入如下图所示的页面。

图 7-4 AP 基本设置

- 工作模式：设置当前 AP 的工作模式，可进行胖 AP 与瘦 AP 模式切换，并对不同模式进行远程管理。
- 设备名：设置当前 AP 的设备名。
- 启用 DHCP 客户端：点击勾选此项，自动获取 IP 地址。
- 用户名：设置登录当前 AP 的用户名。
- 修改密码：如果要修改登录当前 AP 的密码，请勾选**修改密码**并输入新的密码。**提示：**远程修改登录密码后，需使用新配置的密码管理该 AP。
- 漫游阈值：设置漫游阈值的范围，漫游阈值默认为-88dbm，取值范围为：(-85)—(-100)之间。

  漫游阈值是指当前环境若支持漫游，设置无线客户端进行漫游的阀值（当无线客户端测得的信号强度小于漫游阀值，该无线客户端可漫游到信号强度最好的 AP）。
- 信道：设置当前 AP 的信道。
- 生效配置：设置当前 AP 的生效配置。

- 本地配置：选择此项表示当前 AP 的生效配置为本地配置。
- 无线集中控制器下发的配置：选择此项表示当前 AP 的生效配置是从设备上获取的配置文件。

2） 加入服务区

在图 7-3 所示的页面中点击**加入服务区**能进入如下图所示的页面。AP 加入某服务区后，会获取该服务区的名称、SSID、加密方式、VLAN ID、限速策略、上传/下载速率和自动下发等信息。

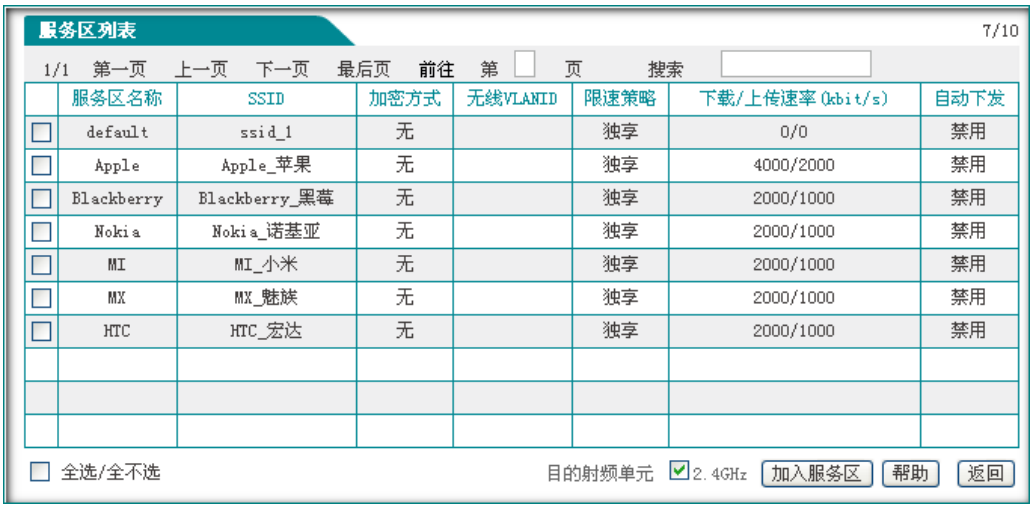


图 7-5 加入服务区

在服务区列表勾选该 AP 要加入的服务区，再点击**加入服务区**按钮，AP 就能加入到该服务区中。

提示：一台 AP 最多可加入四个服务区，即一台 AP 最多可拥有四个 SSID、网关地址等配置信息。

3） 获取软件

在图 7-3 所示的页面中点击**获取软件**设备能获取当前 AP 的软件，并保存在设备的存储卡中。如下图所示，软件列表中显示设备所保存的所有软件。

图 7-6 软件列表

- 设为默认：AC 默认下发给 AP 的软件。注：当该软件被勾选设为默认选项后，AP 的自动升级功能才能生效。

4） 无线 MAC 地址过滤

在图 7-3 所示的页面中点击**无线 MAC 地址过滤**，设备将当前在无线 MAC 地址过滤配置中配置的无线 MAC 地址组下发到当前 AP 上。

图 7-7 无线 MAC 地址过滤

5） 下发模板

在图 7-3 所示的页面中点击**下发模板**进入如下图所示的页面。配置文件列表中列出设备中的配置文件，如要将某配置文件下发到该 AP 中，请选择相应的配置文件后，点击**确定下发**按钮。

图 7-8 下发模板

6） 下发软件

在图 7-3 所示的页面中点击**下发软件**进入如下图所示的页面，软件列表中列出设备中的各软件，如要将某软件下发到该 AP 中，请选择相应的软件后，点击**确定下发**按钮。

图 7-9 下发软件

提示：软件下发，AP 升级成功后会自动重启。

7） 重启设备

如果您确定要重启当前 AP，请在图 7-3 所示的页面点击**重启设备**。

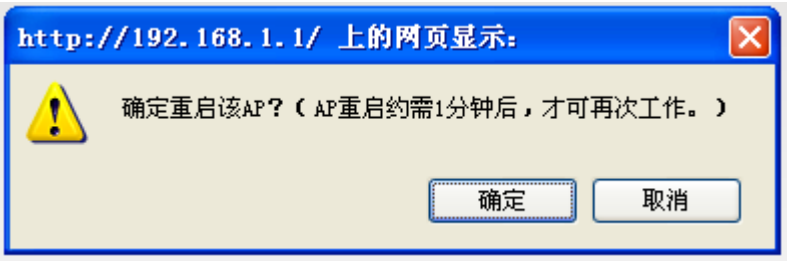


图 7-10 重启设备

8） 恢复出厂配置

如果您确定要将当前 AP 恢复到出厂配置，请在图 7-3 所示的页面点击**恢复出厂配置**。

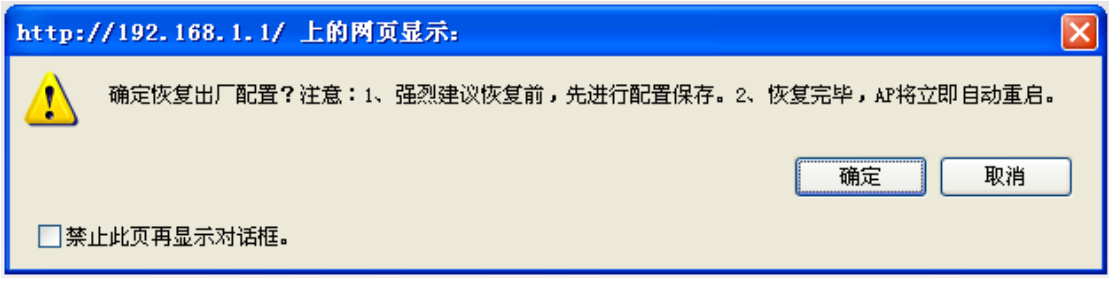


图 7-11 恢复出厂配置

7.2.1.2 批量管理

当有多个 AP 需要执行相同的操作，比如加入相同的服务区，升级成相同的软件，重启多个 AP，下发相同的模板等操作时，可以选择使用批量设置功能。

勾选多个 AP，并点击页面下方的**批量操作**按钮，进行批量设置。

图 7-12 批量管理

- 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。
- 计划任务：从下拉框中选择已设置好的计划任务模板并点击**保存**。计划任务模板在 **AP 集中管理 —> AP 计划任务**页面配置。
- 新密码、确认密码：修改 AP 的登录密码。
- 睡眠模式：勾选启用睡眠模式，在睡眠模式下，设备的 2.4G 无线指示灯将熄灭，如果设备上有系统指示灯，系统指示灯亮度将变暗。
- 下发服务区：点击跳转至服务区列表页面，选择需要下发的服务区模板并点击**加入服务区**按钮完成服务区的下发。服务区模板在 **AP 集中管理 —> 服务区**页面配置。
- 升级软件：点击跳转至下发软件页面，选择需要升级的软件版本并点击**确认下发**按钮完成软件升级。软件版本在 **AP 集中管理 —> AP 软件管理**页面管理。
- 恢复出厂配置：点击将所选 AP 的软件恢复至出厂配置。
- 无线 MAC 地址过滤：点击跳转至无线 MAC 地址过滤页面，选择需要下发的 MAC 地址过滤规则模板并点击**确认下发**按钮。MAC 地址过滤规则模板在 **AP 集中管理 —> 无线 MAC 地址过虑**页面配置。
- 重启：重启所选 AP。
- 下发模板：点击跳转至下发模板页面，选择需要下发的 AP 配置模板并点击**确定下发**按钮。AP 配置模板在 **AP 集中管理 —> AP 配置模板**页面配置。

7.3 AP分布图

在 **AP 集中管理—>AP 分布图** 页面中，可导入建筑平面图片，在图片上显示 AP 物理分布；导入多张建筑平面图，编辑 AP 分布位置，也可以在分布图上查看 AP 异常状态，并对分布图上的 AP 进行单机管理。

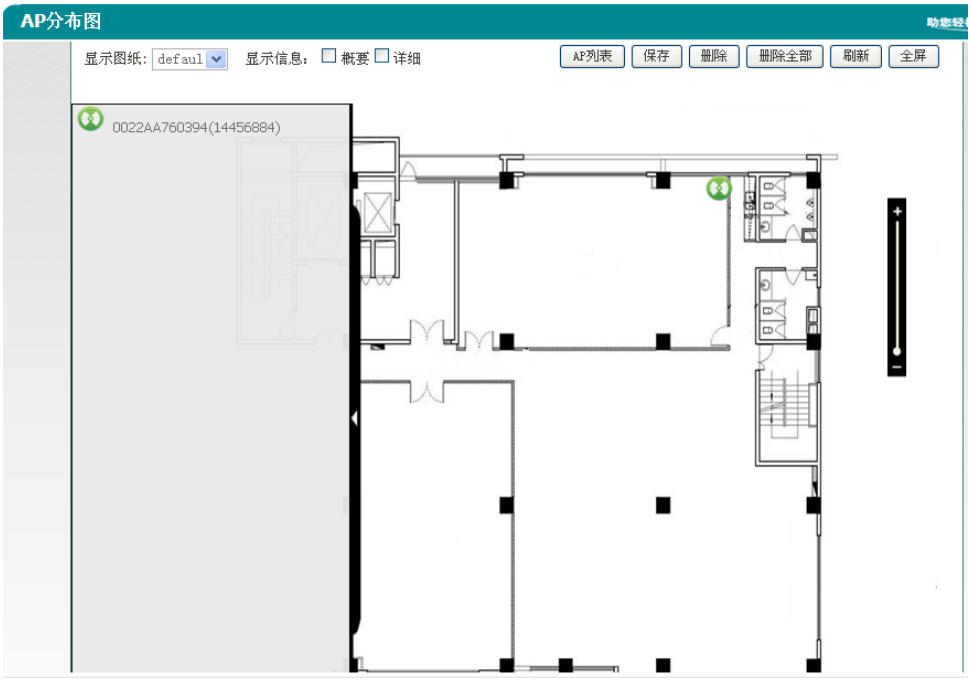


图 7-13 AP 分布图

管理员可以导入建筑图纸，选择已导入的图纸可进入如上图所示页面。勾选页面左上角的**概要**与**详细**按钮，在图纸上显示 AP 信息。在图纸上添加 AP 图标，可对 AP 进行管理和删除操作。AP 的颜色为绿色，则表示在线；橘黄色则表示离线。

点击管理列表中的**管理**按钮，可查看 AP 信息；点击 – 并点击**保存**按钮，可将 AP 从图纸上移除。

在 **AP 集中管理—>AP 分布图**页面中，点击**导入图纸**，便可进入导入建筑图纸页面。

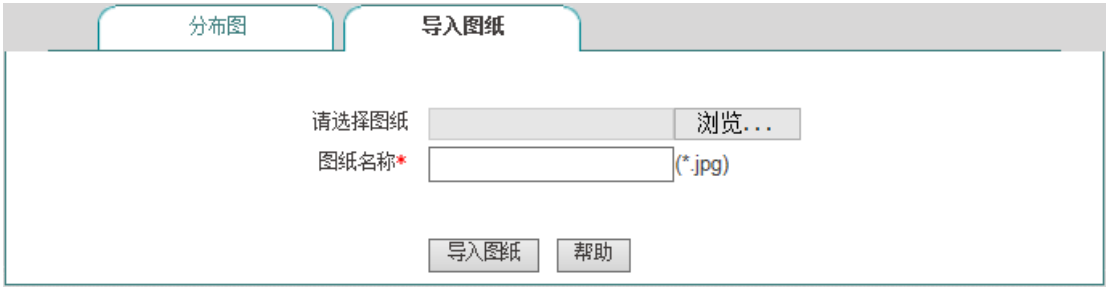


图 7-14 导入图纸配置

- 选择图纸：上传需要的建筑图纸，点击**导入图纸**，配置生效，只支持 JPG 格式的图纸。
- 图纸名称：设置图纸的名称。图纸名称只可包含大小写字母、数字、下划线。

7.4 无线统计

在 **AP 集中管理—>无线统计**页面，管理员可以通过查看无线客户端统计了解各无线接入用户的相关信息，以及在线用户和黑名单列表。

AP 用户统计：以柱状图形式显示当前在线的无线客户端在不同 AP 上的分布情况。用户可选择每页显示的 AP 数。

图 7-15 AP 客户端统计

SSID 用户统计：以柱状图形式显示当前在线的无线客户端在不同 SSID 上的分布情况。

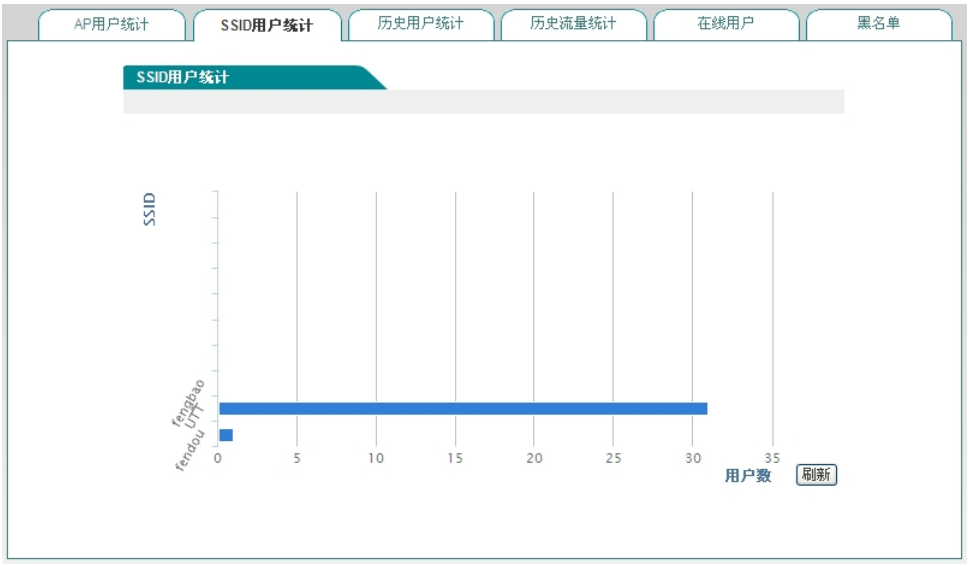


图 7-16 SSID 客户端统计

历史用户统计：以折线图显示过去某一段时间内的在线无线客户端总数的变化，用户可选择统计时间。

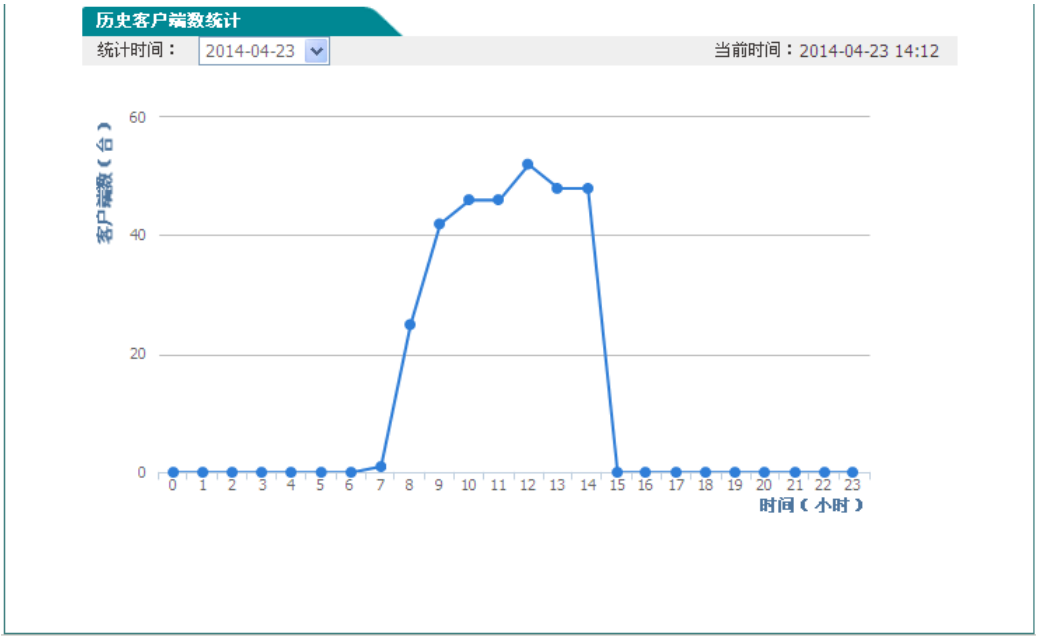


图 7-17 历史客户端数统计

历史流量统计：以折线图显示过去某段时间内用户总流量，管理员可选择特定的 AP 查看历史流量，最多可选择两个 AP 进行比较。

图 7-18 历史流量统计

在线用户：显示 AC 管理的所有 AP 所连接的在线用户，且显示该用户的详细信息，包括：MAC 地址、接入 AP、接入 SSID、速率、频宽、下载、下载速率、上传、上传速率和在线时长。同时可在列表下方选择在线或离线用户进行查看。

图 7-19 用户在线列表

黑名单：在黑名单列表中的用户将无法连接该 SSID，管理员可以从 **AP 集中管理—>无线统计—>在线用户**页面的在线用户列表中增加黑名单用户到黑名单列表，管理员也可删除黑名单列表中的用户。

图 7-20 黑名单列表

7.5 服务区

在 **AP 集中管理—>服务区**页面，管理员通过查看服务区列表了解各服务区的相关参数。点击**添加新条目**可进入服务区配置页面，下面介绍配置服务区时的各项参数。

图 7-21 服务区列表

7.5.1 服务区配置

在 AP 集中管理—>服务区页面，点击**服务区配置**或右下角的**添加新条目**，便可进入服务区配置页面，进行相应的参数配置。

图 7-22 服务区配置

- 启用服务区：选择是否启用该服务区。
- 服务区名称：定义该服务区的名称。
- SSID：(Service Set Identification，服务集标识）定义该服务区的 SSID，用于唯一标识一个无线网络的字符串，(区分大小写)。
- 启用 SSID 广播：选择是否开启 SSID 广播，启用表示从服务区获取该配置的 AP 将向无

线网络广播自己的 SSID。

- 启用无线客户端隔离：选择是否开启该功能，打钩表示隔离连接到同一个 AP 上的无线客户端。
- 无线 VLAN ID：设置该服务区的 VLAN ID，不同的服务区其 VLAN ID 不能相同。默认服务区 default 不可设置 VLAN ID；要通过该 VLAN 访问 AC 需配置对应的 VLAN 接口。
- 限速策略：选择限速策略，**独享**：表示此范围内每一个 IP 地址使用此带宽，**共享**：表示只有此 SSID 使用此带宽。
- 上行带宽/下行带宽：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。
- DHCP 地址池：选择相应的 VLAN ID 的地址池，若没有配置相应的 VLAN ，则显示没有匹配的地址池。
- 加密方式：设置该服务区的加密方式，包括：WEP、WPA/WPA2、WPA-PSK/WPA2-PSK。
- 自动下发：勾选表示服务区自动下发给 AP。
- AP 管理 VLAN 范围：设置该服务区中 AP 管理 VLAN 的范围。

下面介绍配置加密方式时，各项参数的含义：

WEP

- 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。

WPA/WPA2

- 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。

WPA-PSK/WPA2-PSK

◆ 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 0，值为 0 时表示不更新。

7.5.2 服务区自动更新

在 **AP 集中管理—>服务区—>服务区自动更新**页面。服务区自动更新是指当管理员修改了服务区中的配置后，AC 自动将最新的服务区配置下发给本服务区内的 AP。

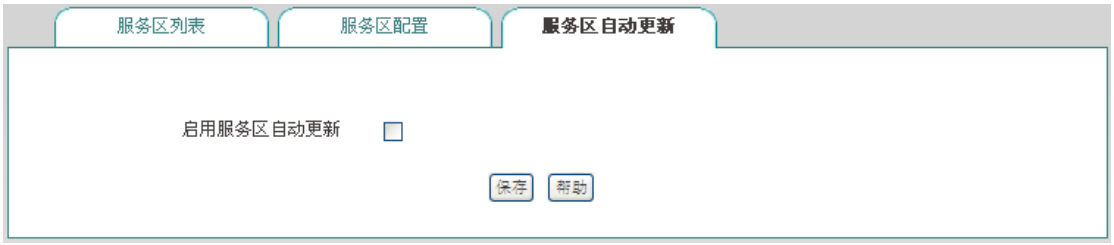


图 7-23 服务区自动更新

- 启用服务区自动更新：打钩表示启用该功能。
- 保存：点击**保存**，配置生效。

7.6 无线MAC地址过滤

在 **AP 集中管理—>无线 MAC 地址过滤**页面，可统一配置要禁止或者允许的无线客户端 MAC 地址，且配置的过滤 MAC 地址只在指定的服务区中生效，被过滤的无线客户端接入其它服务区时不受影响。下图为无线 MAC 地址过滤列表，可显示 MAC 地址组名，服务区，规则等信息。

图 7-24MAC 地址过滤列表

在 **AP 集中管理—>无线 MAC 地址过滤**页面，点击**添加新条目**或 **MAC 地址过滤配置**，便可进入 MAC 地址过滤配置页面。

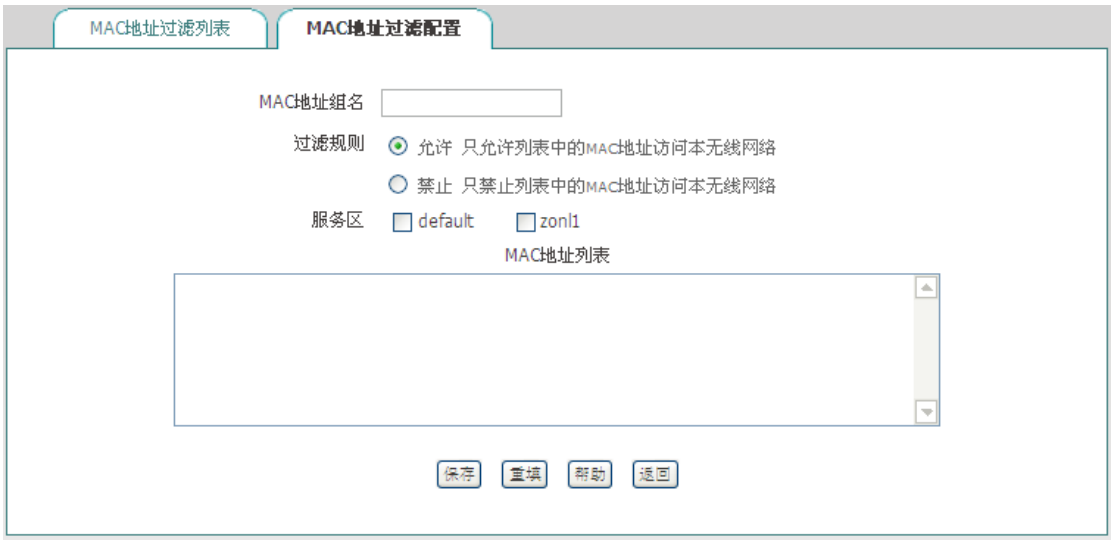


图 7-25MAC 地址过滤配置

- MAC 地址组名：设置任意的组名。
- 过滤规则：选择需要的规则，**允许**或**禁止**。
- 服务区：选择需要生效的服务区。
- MAC 地址列表：添加需要过滤的无线客户端的 MAC 地址，最多可添加 32 条 MAC 地址。

7.7 AP配置模板

在 **AP 集中管理—>AP 配置模板**页面，管理员通过查看 AP 配置模板列表了解各模板，设备出厂默认有各个型号的 AP 配置模板。点击**添加新条目**可进入模板配置页面，下面介绍配置模板的各项参数。

图 7-26 AP 配置模板列表

图 7-27 AP 配置模板

- 模板名称：定义该模板的名称。
- 启用无线功能：选择是否启用该模板的无线功能。
- 无线速率：选择 AP 所要使用的无线速率。
- Short Guard Interval：选择是否启用 Short Guard Interval（短保护间隔）。在多路径环境下，后一符号的前端有可能比前一符号的末端更快到达接收机，从而导致符号间产生干扰，保护间隔是前后符号间的一段空白时间，可以为延迟信号提供更长的缓冲时间，从而规避这个干扰；当启用短保护间隔时，（保护间隔时间为 400 纳秒，而非标准 800 纳秒），可提高吞吐量。
- 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、自动。注意，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。
- 启用 WMM：选择是否启用 WMM。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。
- 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。
- Short Preamble：选择是否启用 Short Preamble（短前导）。
  - 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。
- 无线传输功率：此参数用于设置无线的传输功率，无线传输功率默认为自动，表示此 AP 会根据周围 AP 的 RSSI 值来动态调节自身的无线发射功率，以使得 AP 间的干扰最小，

让无线网络环境达到最优的状态；可选项为：高、中、低三档。

- Beacon 间隔：定期发送数据帧进行检测，默认为 100 毫秒，也可以手动进行配置。
- 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 300M 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 标准的无线站点将按照各自所支持的模式接入，最大速率分别为 11M bps、54M bps 和 300M bps。

7.8 AP软件管理

在 **AP 集中管理—>AP 软件管理**页面，管理员可以通过查看软件列表了解设备中保存的软件（如图 7-6 软件列表所示）。同时您可以在**上传软件**页面，从本地选择最新的软件上传到设备上。

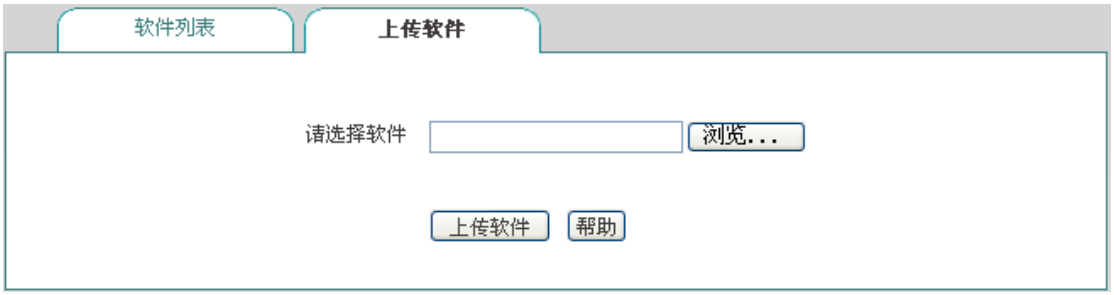


图 7-28 上传软件

7.9 AP配置文件

在 **AP 集中管理—>AP 配置文件**页面，AP 自动将配置文件回传给 AC,管理员可以通过查看配置文件列表了解设备中保存的配置文件。如下图为 AP 配置文件列表，可显示配置文件名、序列号、AP 型号、更新时间、硬件版本、大小和软件版本等信息。

图 7-29 配置文件列表

点击**上传备份配置**，可上传备份的配置文件。

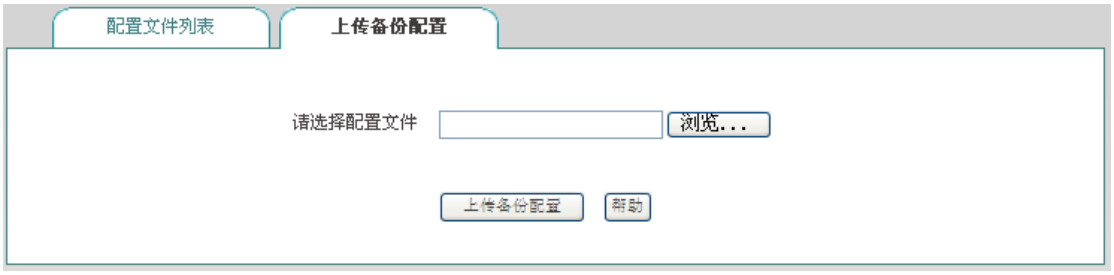


图 7-30 上传备份配置

7.10 AP负载均衡

AP 负载均衡是将网络中的无线客户端数量均匀地分配在多台 AP 上，从而提高网络服务的质量。在 **AP 集中管理—>AP 负载均衡**页面，管理员可以通过查看 AP 负载均衡列表了解 AP 中各负载均衡组的相关信息，点击**添加新条目**可进入负载均衡配置页面，下面介绍配置负载均衡时的各项参数。

图 7-31 AP 负载均衡列表

提示：在上图中的**开启负载均衡**按钮为全局开关，勾选此项并**保存**，表示设备开启负载均衡功能。

图 7-32 负载均衡配置

提示：在图 7-32 中的**负载均衡按钮**为局部开关，勾选此项，表示开启此负载均衡组内 AP 的负载均衡功能。

- 开启负载均衡：点击勾选此项，开启此项负载均衡组功能。
- 负载均衡组名：设置 AP 负载均衡组的组名。
- 可供选择 AP 列表：显示当前 AP 的基本信息。
- 负载均衡列表：显示已启用负载均衡 AP 的基本信息。（一个负载均衡组配置范围是 2 一 10 台 AP；红色字体表示该 AP 处于离线状态。）

7.11 AP计划任务

在 **AP 集中管理—>AP 计划任务**页面，管理员制定需要 AP 周期性执行的任务，如每周一上午 8：00 重启设备。已设置好的计划任务通过批量管理下发给 AP 执行，如何批量管理请参阅章节：批量管理。

图 7-33 计划任务

点击上图中的**添加新条目**进入计划任务配置界面。

图 7-34 计划任务配置

- 任务名：定义该计划任务的名称。
- 启动类型：选择该计划任务的启动频率。
- 运行时间：选择该计划任务的具体运行时间点。
- 任务内容：选择该计划任务的操作内容。

7.12 AP日志管理

在 **AP 集中管理—>AP 日志管理**页面，管理员可以通过查看 AP 日志界面了解各 AP 及接入无线用户的相关信息。

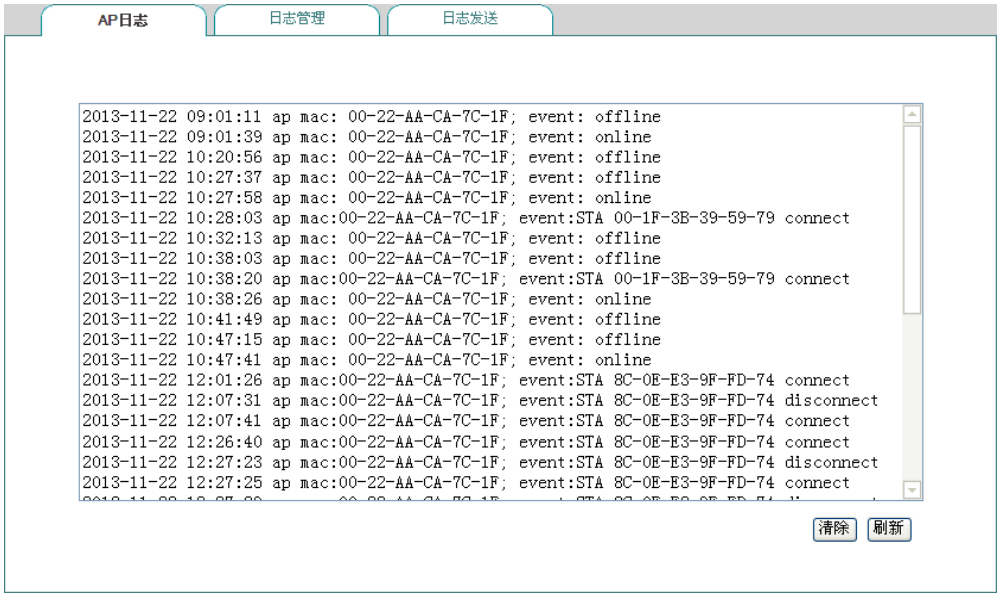


图 7-35 AP 日志

在 **AP 集中管理—>日志管理**页面，管理员可以选择需要查看到的 AP 信息及接入无线客户信息。

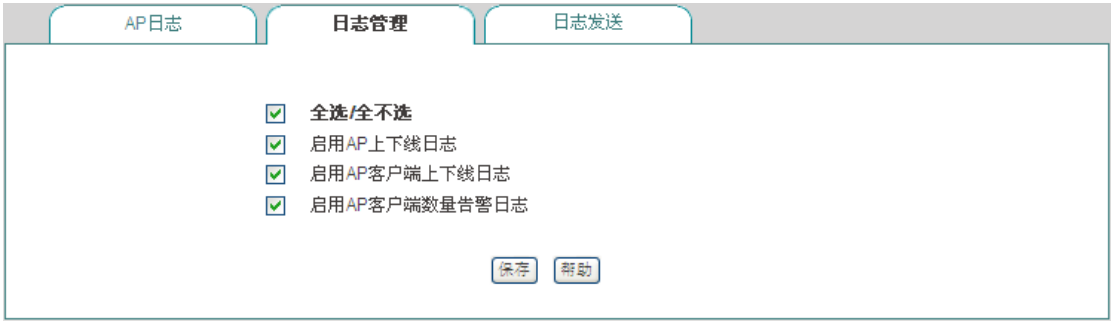


图 7-36 日志管理

- 启用 AP 上下线日志：勾选表示启用记录 AP 上下线日志的功能。
- 启用 AP 客户端上下线日志：勾选表示启用记录 AP 客户端上下线日志的功能。
- 启用 AP 客户端数量告警日志：勾选表示当 AP 所连客户端数超过设定的值时，系统会记录 AP 客户端数量告警日志（系统设定的值为 20）。

在 **AP 集中管理—>日志发送**页面，管理员可以选择编辑日志发送的相关信息。

图 7-37 日志发送

- 启用：勾选表示启用日志发送功能。
- 邮件标题：自定义邮箱的标题。
- 发送服务器：自定义发送日志的服务器。
- 发送者邮箱：自定义发送者的邮箱。
- 发送者密码：自定义发送者的密码。
- 接受者邮箱：自定义接受者的邮箱。
- 发送时间间隔：自定义发送时间的时间间隔。

7.13 AP集中管理配置实例

需求：

某小型企业现购买了三台 AP，要在公司内部搭建一个无线网络，并需实现以下需求：

1) 该无线网络能够覆盖整个公司的办公区域。

2) 通过无线网络，公司员工能使用无线终端访问企业内部资源及互联网，外来人员只能使用无线终端访问互联网，禁止访问企业内部资源。

3) 三台 AP 上的客户端数量尽可能的保持一致。

分析：

1) 实现无线网络覆盖整个办公区域：将三台 AP 合理的安装在相应的办公区域，通过二层漫游来实现无缝连接。

2) 在 AC 上创建两个服务区，一个服务区为公司员工使用，另一个服务区为外来人员使用。且三台 AP 都加入这两个服务区（实现无线网络的二层漫游），使得相应的人员在办公区域的任何一个位置都能通过无线网络访问相应的网络资源。

3） 在 AC 上将三台 AP 加入同一个负载均衡组里，实现 AP 间的负载均衡。

4） 通过在 AC 上做策略，使得外来人员不能访问内部资源。

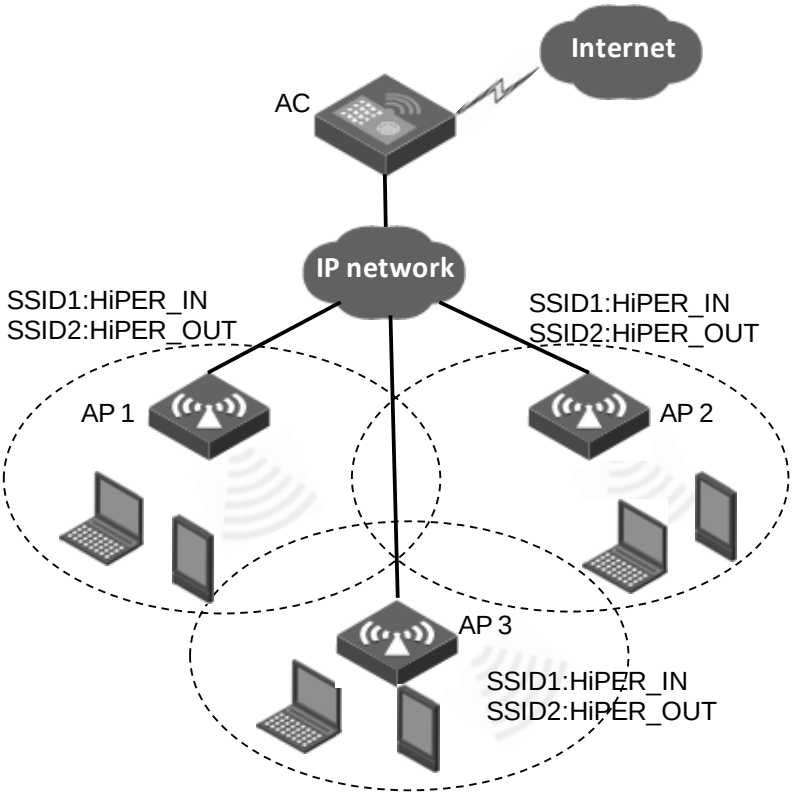


图 7-38 AP 集中管理配置实例

配置步骤：

1） 接入配置

将 AC 连接公司网络的旁路模式中，其中 AC 连接的上层接口 VLAN 为 VLAN10。

2） 接口配置

登陆 AC，配置设备的 LAN 口、WAN 口，完成最基本的上网的配置。其中 LAN 口 IP 地址为 192.168.1.1。

3） 服务区配置

进入 **AP 集中管理—>服务区**页面，配置服务区 default、S2。

服务区 default 的 SSID 设置为 HiPER_IN，启用 SSID 广播，加密方式选择 WPA-PSK/WPA2-PSK，预共享密钥为 1234567890，并设置 AP 管理 VLAN 范围为 10。

服务区 S2 配置如下图所示，SSID 设置为 HiPER_OUT，启用 SSID 广播，加密方式为 WPA-PSK/WPA2-PSK，并设置 AP 管理 VLAN 范围为 10。

图 7-39 S2 服务区配置

4) 远程管理

DHCP 服务器、服务区等配置完后，可进入 **AP 集中管理—>AP 管理**页面，点击**刷新**按钮，等设备显示出相应的 AP 后，在列表中输入相应 AP 的登录密码（出厂值为 admin），分别对这三台 AP 进行远程管理。

在远程管理页面点击**加入服务区**链接，进入服务区列表页面后，勾选服务区名称为 default、S2 的服务区，再点击**加入服务区**按钮。分别将三台 AP 分别都加入到这两个服务区中。

5) AP 负载均衡

进入 **AP 负载均衡**页面，点击勾选**开启负载均衡组**，点击**添加新条目**，进入负载均衡组配置界面，勾选**开启负载均衡组**，输入负载均衡组名 HiPER_NEW，将三台 AP 加入负载均衡组中，点击**保存**。

6) 防火墙配置

进入**防火墙—>访问控制策略**页面，配置一条访问控制策略，源地址设置为 192.168.20.1~192.168.20.254，目的地址设置为内网服务器的地址段，过滤类型为 IP 过滤，动作为禁止，协议为 all（所有）。

通过以上配置，企业员工通过 HiPER_IN 接入网络；外来人员则通过 HiPER_OUT 接入网络。

7.14 AP集中管理配置实例（三层管理）

7.14.1 典型环境一（ACCESS口与三层交换机的应用option43）

1、需求：

在 AP 上设置 AC 静态 IP，三层发现 AC

需要通过登陆 VLAN2 和 VLAN3 内的 AP 填写 AC 的 LAN 口 IP 发现 AC。

三层交换机上划分三个 VLAN，分别为 VLAN1、VLAN2、VLAN3，AP1 位于三层交机 VLAN2 所属的access接口,VLAN2虚接口IP为192.168.2.254, AP2位于三层交换机VLAN3所属的access接口，VLAN3 的虚接口 IP 为 192.168.3.254。AC LAN 口 IP 为 192.168.1.1，VLAN1 的虚接口 IP 为 192.168.1.254。

2、环境拓扑图

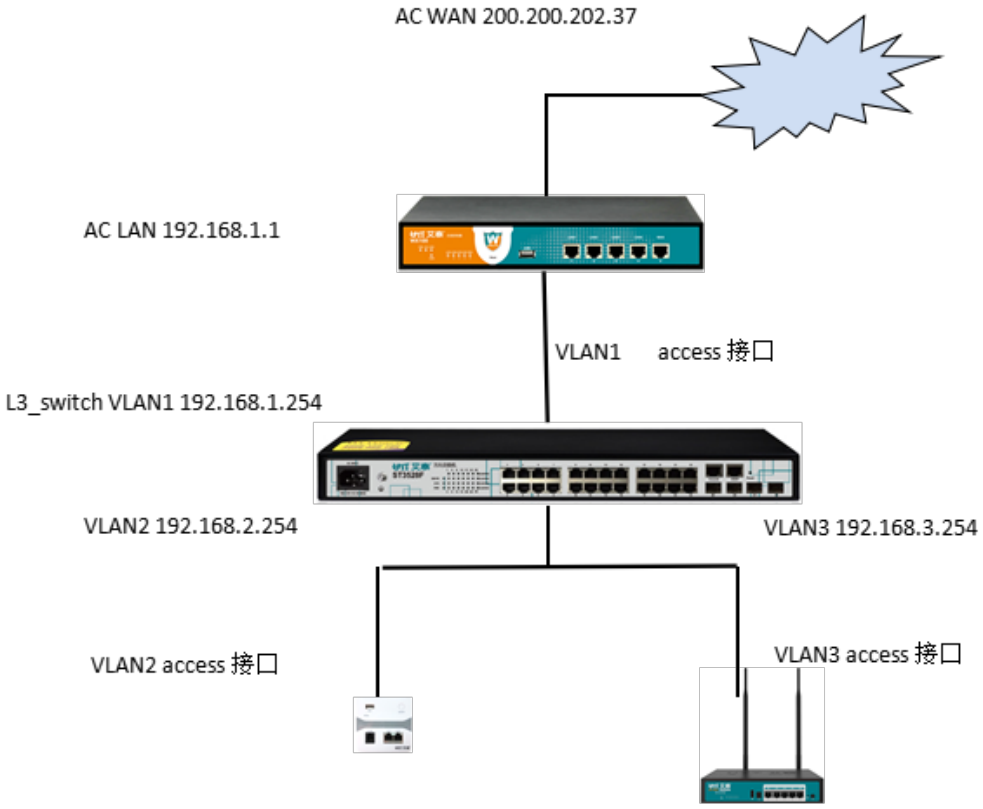


图 7-40 三层环境

3、操作步骤：

1) AC 恢复出厂配置—>修改以下参数，并点击**保存**。

（1） 进入**高级配置**->**路由配置**。

（2） 添加路由新条目，如（3）、（4）。

（3） 目的网络 192.168.2.0 ，子网掩码 255.255.255.0 ，网关地址 192.168.1.254，接口选择 LAN 。

（4） 目的网络 192.168.3.0 ，子网掩码 255.255.255.0 ，网关地址 192.168.1.254，接口选择 LAN 。

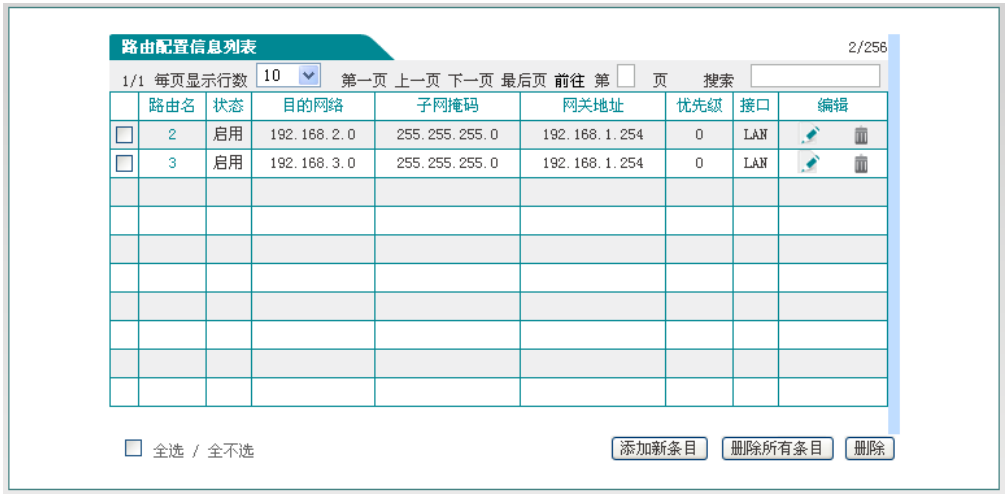


图 7-41 AC 静态路由配置

2) telnet 192.168.1.254 进入交换机 输入命令 show arp,查看两台 AP 分别获取的 IP 地址，然后通过访问 AP 的 IP 地址，进入 AP 基本配置，分别填写 AC1 IP 地址为 192.168.1.1 后，点击**保存**。

```
ST3528F#show arp
ARP Unicast Items: 4, Valid: 3, Matched: 3, Verifying: 0, Incomplete: 0, Failed:
 1, None: 0
Address          Hardware Addr      Interface      Port              Flag      Age-
time(sec)  subvlanVID
192.168.1.1      00-22-aa-d7-ee-32  Vlan1          Ethernet1/0/23    Dynamic   61
                1
192.168.1.100    00-22-aa-b9-47-f7  Vlan1          Ethernet1/0/23    Dynamic   1199
                1
192.168.2.2      00-22-aa-cb-96-fb  Vlan2          Ethernet1/0/5     Dynamic   151
                2
```

3) 进入 AC 的集中管理列表,查看 AC 是否发现两台 AP,且 AP 的 IP 地址分别为 192.168.2.0 网段地址和 192.168.3.0 网段地址。

4) 进入 AC 配置模板页面，新建一个配置模板，批量下发给两台 AP，查看是否能生效。

图 7-42 AP 管理列表

7.14.2 典型环境二（AP跨VPN的应用）

1） 需求：

公司分部有三台 AP，分别为 WA500N，WA1900N，WA1700N，总部希望可以控制并管理这三台 AP。AP 的 ip 分别为 WA500N:192.168.2.2，WA1900N：192.168.2.3，WA1700N：192.168.2.4，总部 AC,WX2000 的 LAN 口 ip 为 192.168.1.1.

2） 拓扑图

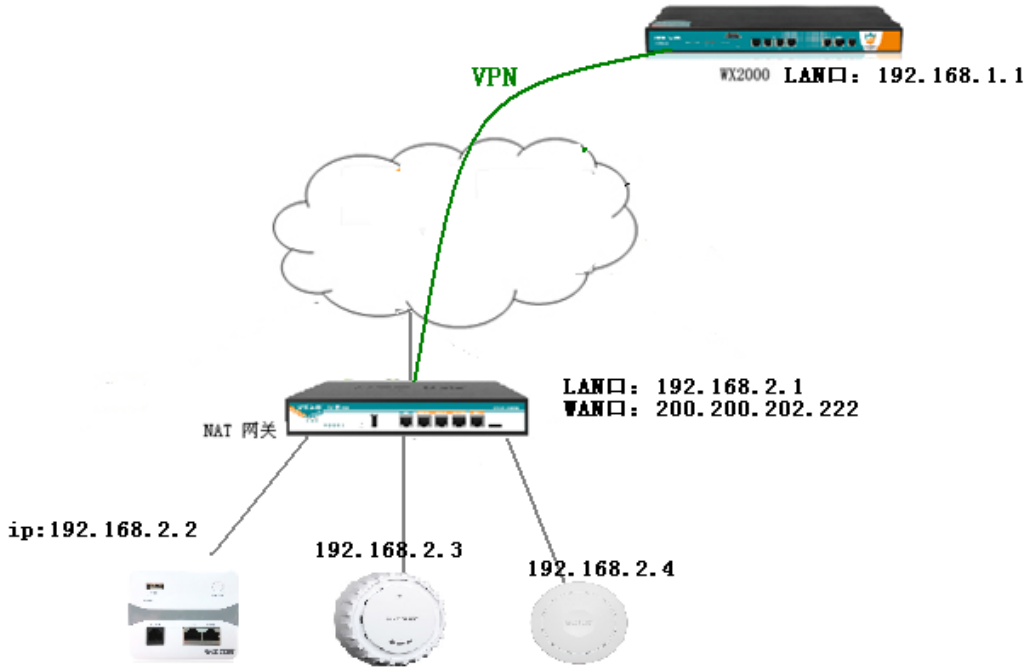


图 7-43 VPN 环境

3）配置步骤

(1) 配置路由器 LAN 口为 192.168.2.1， WAN 口为 200.200.200.222。

(2) 在分部网关和总部 AC 间配置 VPN,使总部和分部之间可以互相通信。

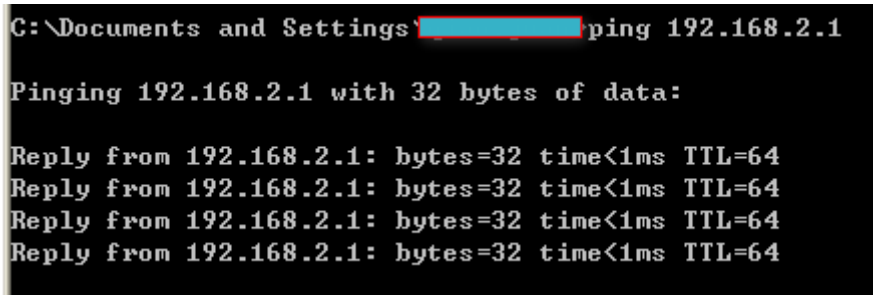
在网关端配置 PPTP 客户端

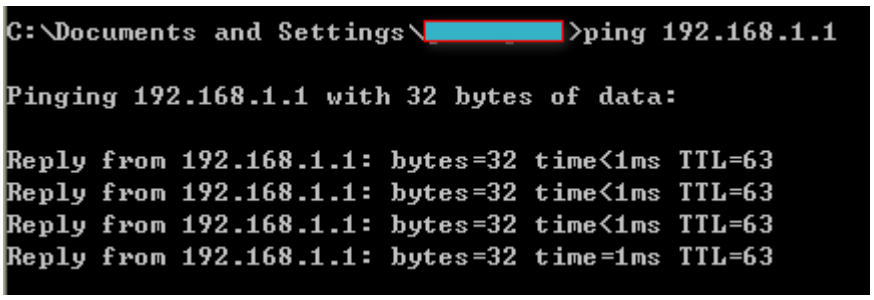
图 7-44 PPTP 客户端配置

在 AC 端配置 PPTP 服务器

图 7-45 PPTP 服务端配置

测试总部与分部的互通性





(3) 分别在三台 AP 上配置 AC LAN 口 ip 为 192.168.1.1.进入 AP,**网络参数->LAN 口配置**。

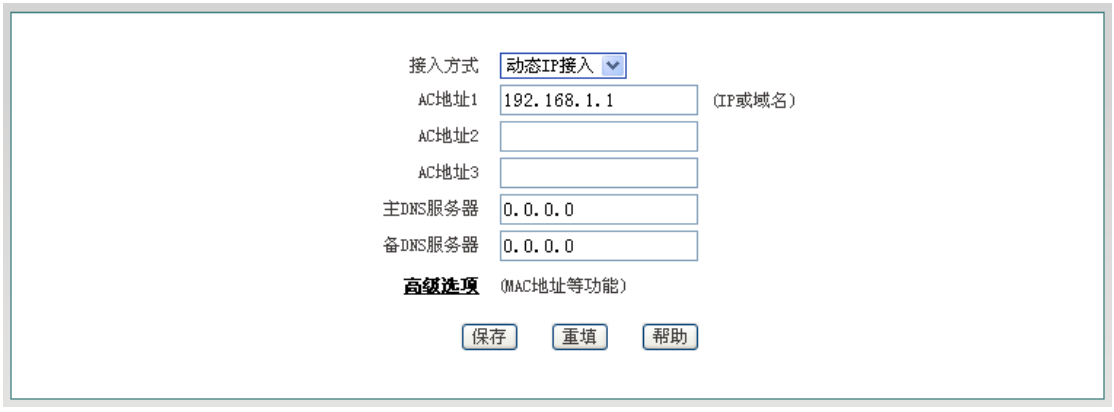


图 7-46 AP LAN 口配置

(4) 进入 AC 的集中管理列表，查看 AC 是否发现三台 AP，且 AP 的 IP 地址分别为 192.168.2.2，192.168.2.3，和 192.168.2.4

(5) 进入 AC 配置模板页面，新建一个配置模板，批量下发给三台 AP，查看是否能生效。

图 7-47 AP 管理列表

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、端口镜像、端口 VLAN 和 SYSLOG 配置。

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。

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，对外提供为其分配的公网 IP 地址给外部网络用户访问。

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。

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

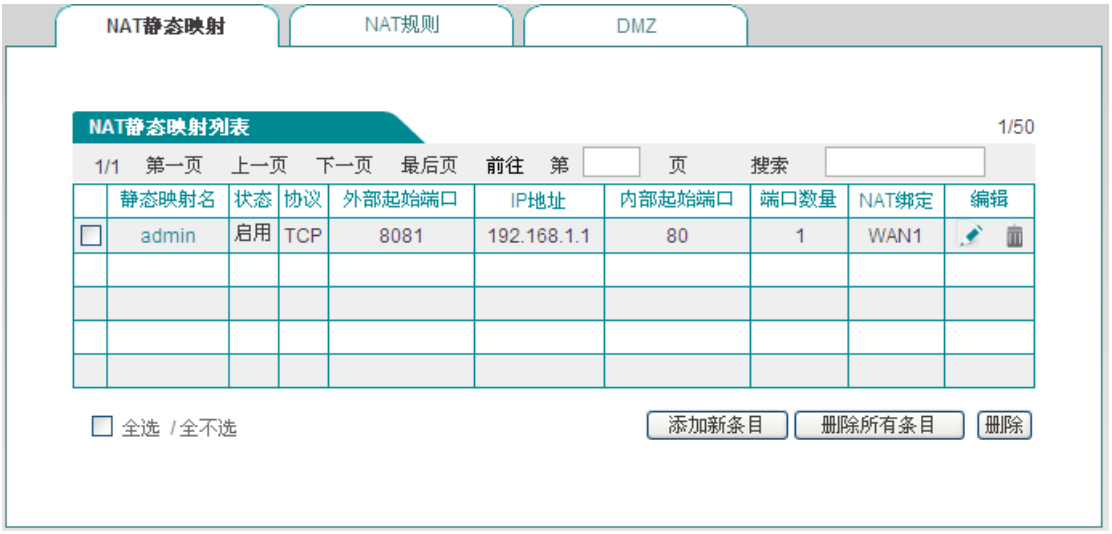


图 8-1 NAT 静态映射列表

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

在如图 8-1 的页面点击**添加新条目**进入 **NAT 静态映射配置**页面，如下图所示。下面介绍 NAT 静态映射配置的各项参数的涵义。

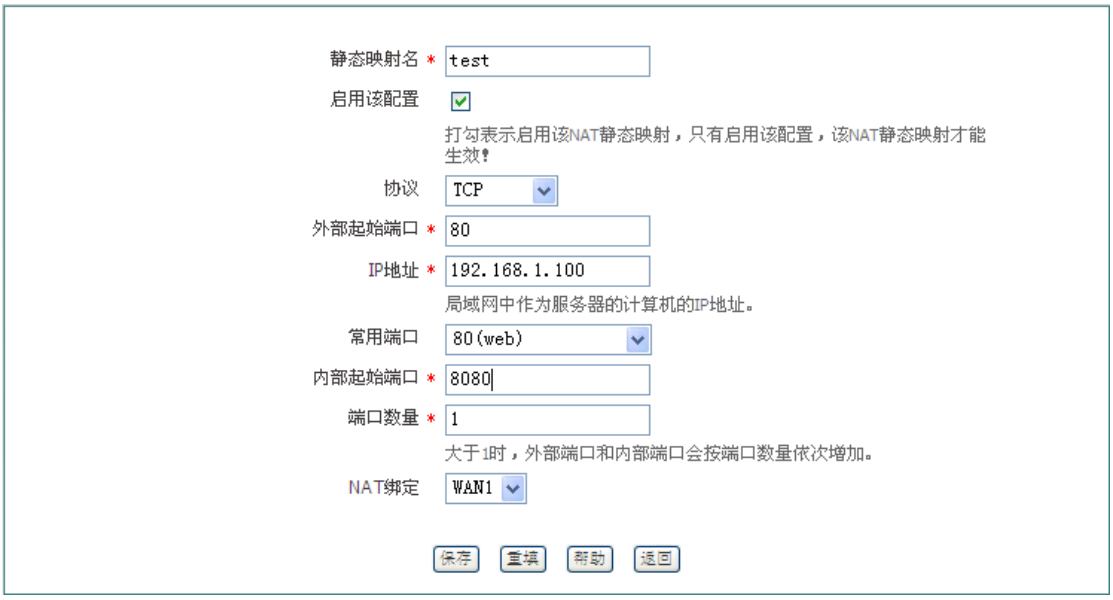


图 8-2 NAT 静态映射配置

- 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 Internt 的起始服务端口号。
- IP 地址：局域网中作为服务器的计算机的 IP 地址。
- 常用端口：常用协议类型对应的端口号以供用户选择。当用户无法确认该协议时可选择 TCP/UDP。
- 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 500。
- 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。如下图所示，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 口上网。

图 8-3 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 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 的各项参数的涵义。

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：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

在下图中选择 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：勾选表示启用 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。

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

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，具体配置如下图所示。

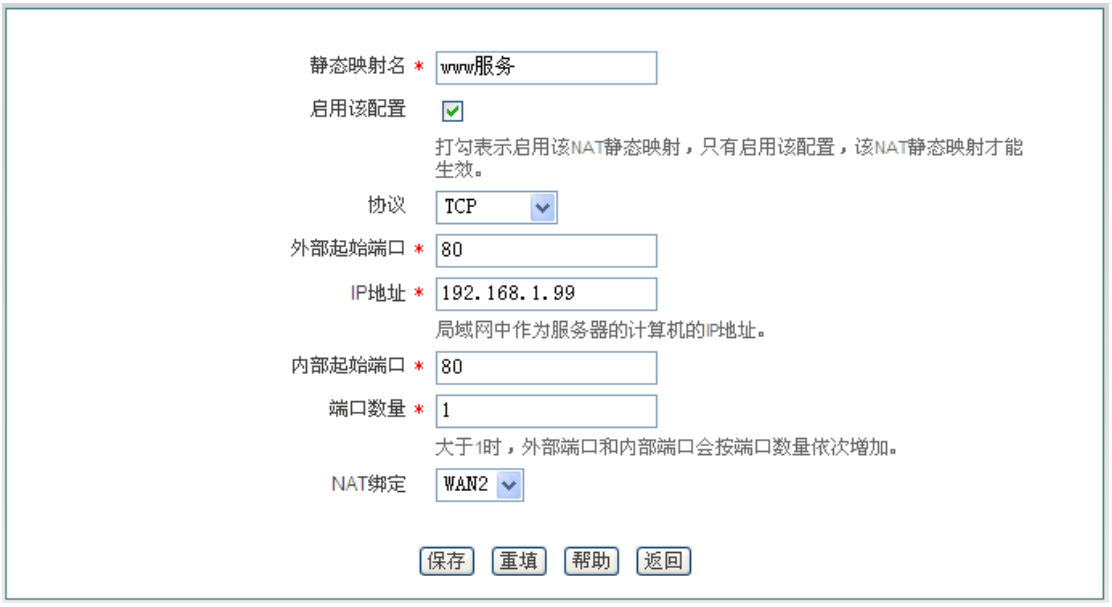


图 8-7 NAT 静态映射配置实例

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，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 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，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 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项参数的涵义。

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。

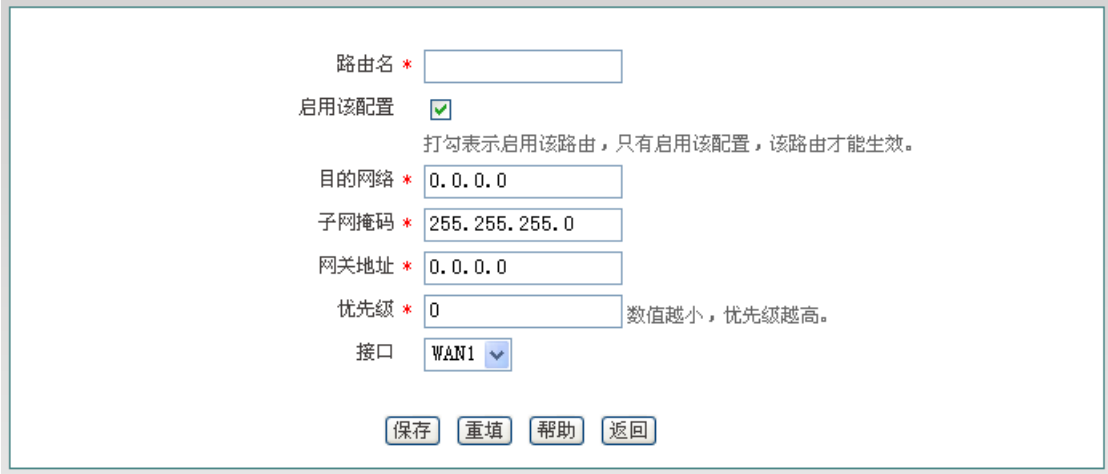


图 8-11 静态路由配置

- 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地址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（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。

8.3 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。

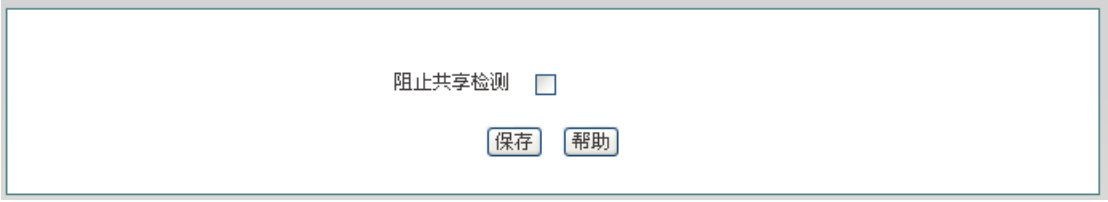


图 8-12 网络尖兵防御

8.4 端口镜像

本节介绍**高级配置—>端口镜像**页面的端口镜像功能。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。

设备默认 LAN1 口为监控端口，其它 LAN 口为被监控端口。

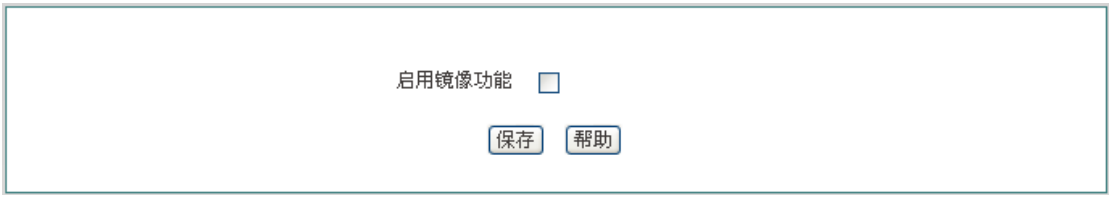


图 8-13 端口镜像 1

- 启用镜像功能：勾选表示启用端口镜像功能。

因产品型号差异，部分设备只有支持两个及两个以上 LAN 口时，端口镜像功能才生效。

图 8-14 端口镜像 2

- 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：只能选择一个被监控端口。

提示：被监控端口不能与监控端口是同一个端口。

8.5 端口VLAN

本节介绍**高级配置—>端口 VLAN** 页面的端口 VLAN 功能。

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、加强网络安全性。

1） 端口 VLAN 列表

图 8-15 端口 VLAN 列表

- VLAN 组号：显示该 VLAN 的 VLAN 组号。
- VLAN 组名称：显示该 VLAN 的 VLAN 组名称。
- VLAN 成员：显示该 VLAN 的成员。

2) 端口 VLAN 配置

图 8-16 端口 VLAN 设置

- VLAN 组号：设置 VLAN 的组号。
- VLAN 组名称：设置 VLAN 组的名称。
- VLAN 成员：选择属于该 VLAN 组的成员。

提示：

1) 系统中存在一个缺省 VLAN，VLAN 号为 1，默认包含所有的物理端口，且不能删除。

2) 一个 VLAN 可以包含多个端口，一个端口也可以属于多个 VLAN。

3） 端口 VLAN 实例

需求：设备 LAN1 口下的主机能与 LAN2 口、LAN3 口下的主机进行通信，但 LAN2 口和 LAN3 口下的主机不能互访。

配置步骤：

(1) 修改 VLAN 1，其成员端口只包括：LAN1、LAN2。

(2) 新建 VLAN 2，其成员端口为 LAN1、LAN3。

分析：LAN1 口与 LAN2 口属于 VLAN1，LAN1 口又与 LAN3 口属于 VLAN2，固 LAN1 口下的主机能与 LAN2 口、LAN3 口下的主机进行通信。又 LAN2 口与 LAN3 口不在同一 VLAN，固 LAN2 口与 LAN3 口下的主机彼此不能互访。

8.6 SYSLOG配置

本节介绍**高级配置—>SYSLOG 配置**页面。

图 8-17 SYSLOG 配置

- 启用 syslog 服务：启用 syslog 服务功能后，该功能会将设备运行的大量信息发送给 syslog 服务器，这便于管理员分析系统的状况、监视系统的活动。
- syslog 服务器的地址（域名）：设置 syslog 服务器的地址，可以是 IP 地址或域名。
- syslog 服务器的端口：设置 syslog 服务器所开放的服务端口，默认为 514。
- syslog 消息类型：设置发送 syslog 的消息类型，默认为 Local0。

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。

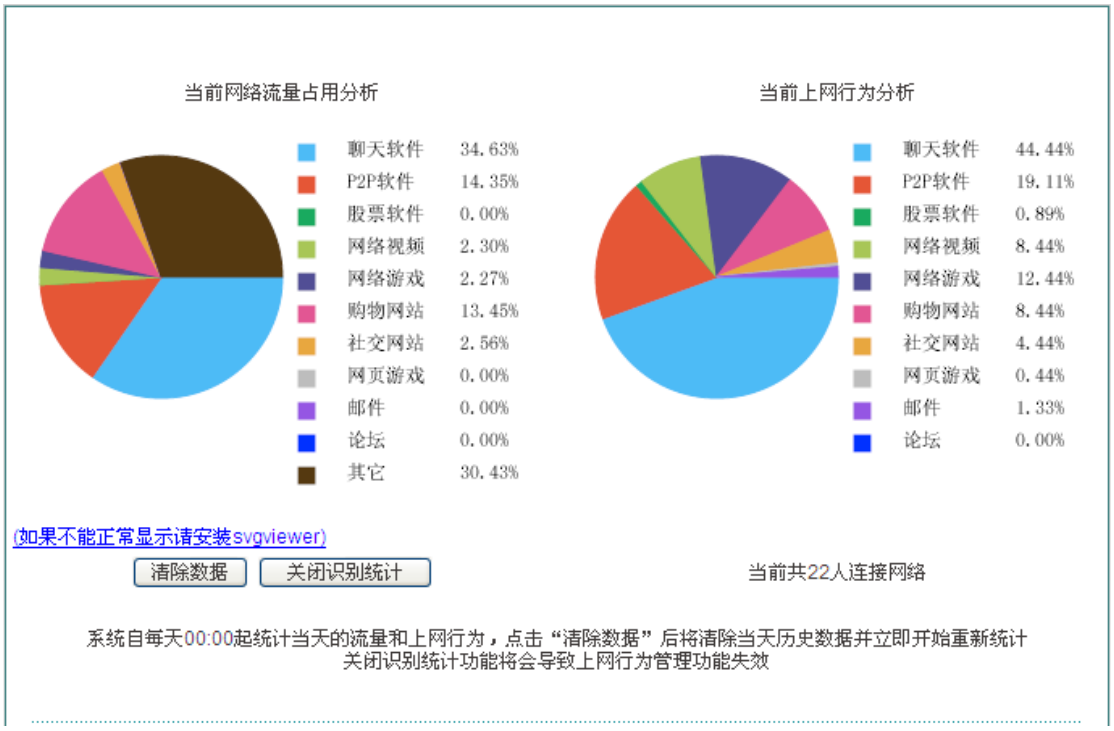


图 9-1 用户行为分析饼图

- 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。

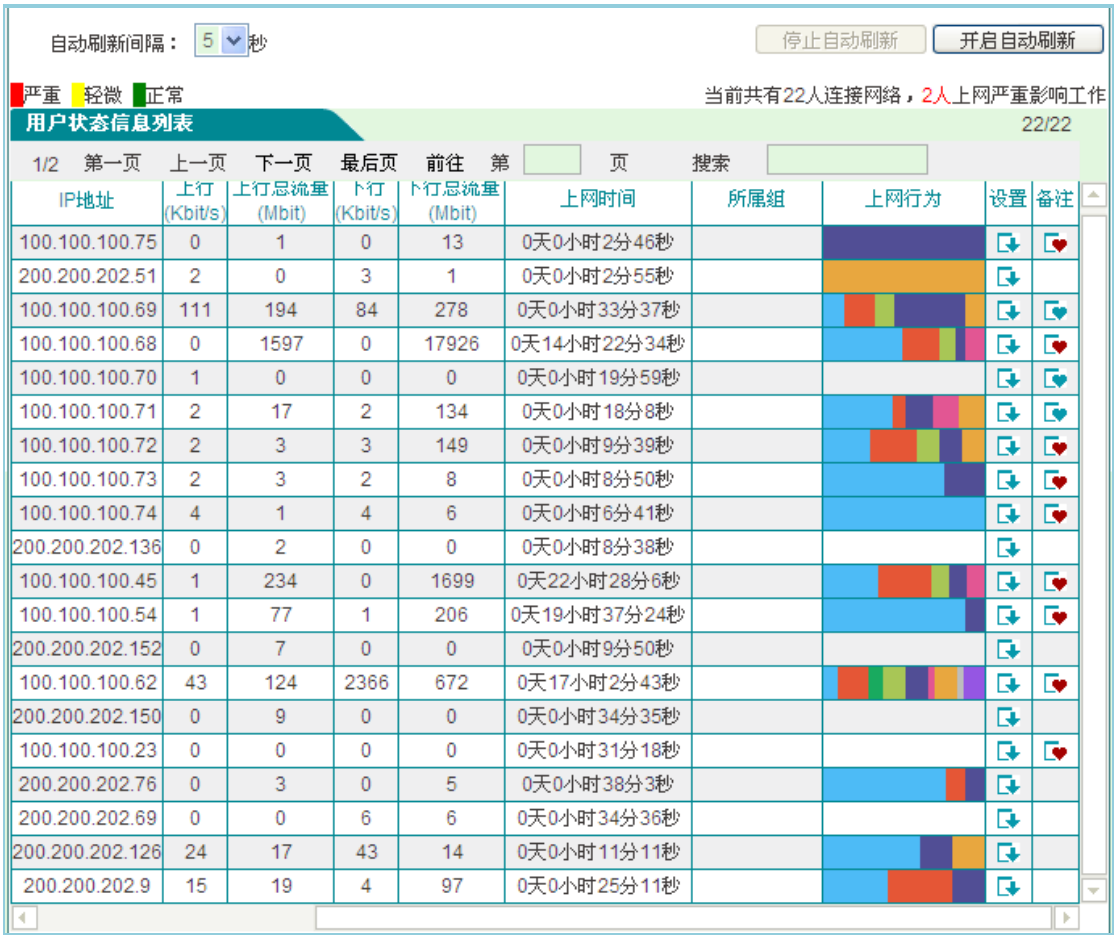


图 9-2 用户状态信息列表

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

本节主要讲述**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。这台主机的 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。

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 绑定的用户与设备连接，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，配置完后点击**保存**按钮。

- 导出：该按钮可以导出 IP/MAC 绑定信息列表中的 IP 地址、MAC 地址、用户名。

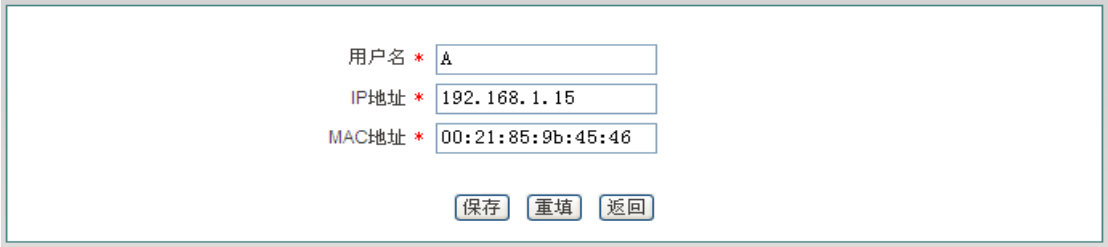


图 9-4 IP/MAC 实例修改

- 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。

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：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。

9.2.3 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上网黑名单。

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**，如下图所示。

图 9-6 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 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“√”），如下图所示。

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：设备的 PPPoE 的服务器配置、PPPoE 账号配置、PPPoE 计费配置及查看 PPPoE 的连接状态等。

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）。

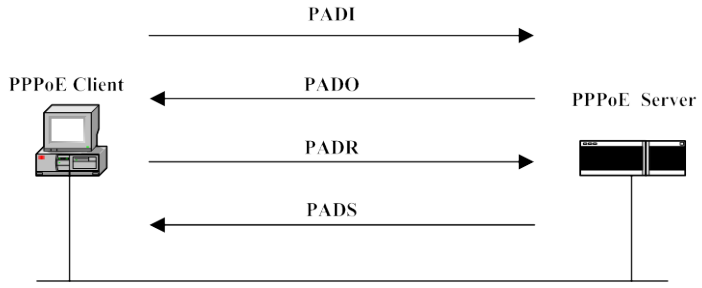


图 9-9 Discovery 阶段的基本工作流程

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。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，注：PPPoE 服务器功能只对有线客户端及默认服务器的所有无线客户端生效。
- 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。
- 例外地址组：在设备开启强制 PPPoE 认证后，该地址组的用户可以不通过拨号认证与外网通信，地址组需要在**用户管理—>用户组配置**页面进行配置。
- 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。
- 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，可以查看 PPPoE 账号信息列表。点击**添加新条目**按钮，进入如下图所示的页面：

图 9-11 PPPoE 账号信息列表

- 用户名：PPPoE 拨号用户的用户名。
- 启用：是否允许该用户访问因特网，勾选表示允许。
- 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。
- 账号最大会话数：显示能同时使用该账号进行 PPPoE 接入的用户数。
- MAC 地址：显示该账号绑定的 MAC 地址。
- 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。
- MAC 绑定：选择是否将该用户名与相应的 MAC 地址进行绑定，如果绑定，则绑定后只有相应 MAC 地址的主机才可以使用该账号上网。
  - 不绑定：不进行用户名/MAC 绑定。
  - 自动绑定：当该用户首次拨号成功后，设备会将该用户名与拨号用户的 MAC 地址进行自动绑定。
  - 手工绑定：在 MAC 地址栏手动输入 MAC 地址进行用户名/MAC 绑定。
- 账号最大会话数：设置同时使用该账号进行 PPPoE 接入的用户数。
- 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。
- 备注：填写需要备注的信息。当备注信息较长时，页面只显示 5 个字符，将鼠标定位在备注内容上时，页面将会自动显示出所有备注内容。

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，则可在列表中查看到 PPPoE 服务器为该用户分配的 IP 地址、该客户端的 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

- 挂断：点击该按钮可挂断该用户的连接。

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：

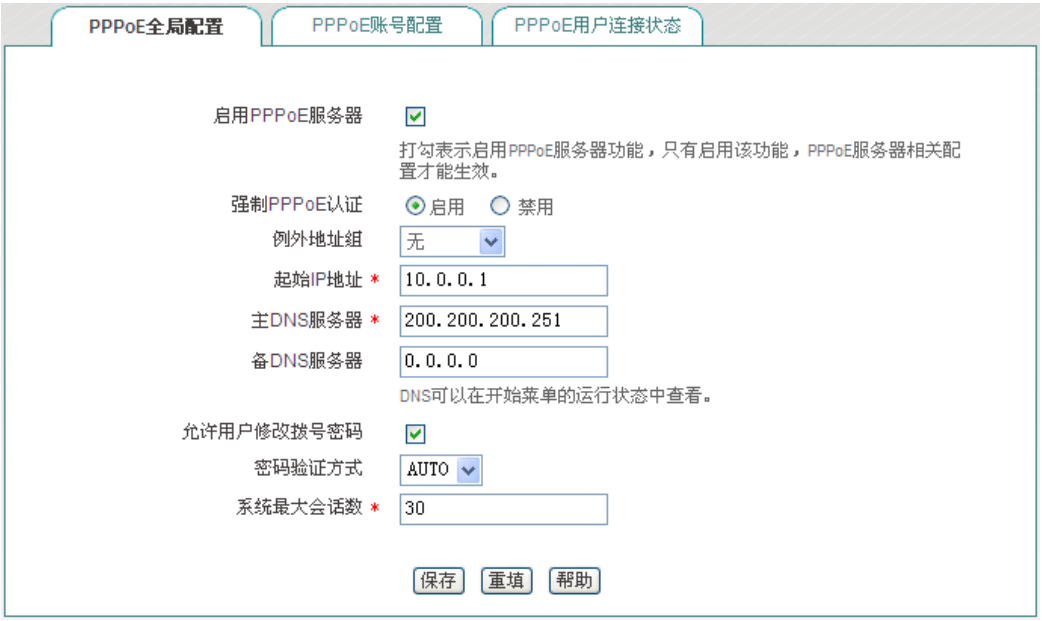


图 9-14 实例—PPPoE 全局配置

(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。

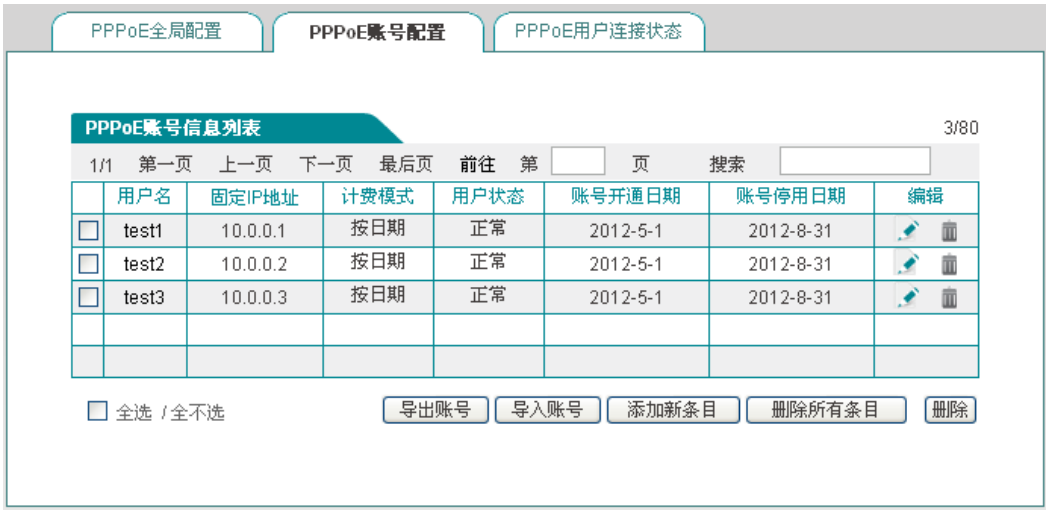


图 9-16 实例——PPPoE 账号信息列表

(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

在**用户管理—>WEB 认证**页面能够配置设备的 WEB 认证功能。启用该功能后，用户需经过认

证后才能访问因特网。设备提供三种认证方式：本地认证、远程认证、微信连 wifi 认证。

9.4.1　WEB认证全局配置

9.4.1.1 本地认证

用户在电脑、手机等设备上通过认证后即可访问因特网。

图 9-17 WEB 认证

- 启用 WEB 认证：勾选表示内网用户需通过 WEB 认证才能访问 Internet。
- 认证方式：选择本地认证。
- 启用实名认证：勾选表示启用此功能。此功能需要配合身份证认证客户端使用。
- 启用背景图片：勾选此选顶后，可以设置认证页面的背景图。
- 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。
- 过期时间：设置用户通过认证后，多久未产生流量后被踢下线。
- 例外地址组：在设备启用 WEB 认证后，该地址组的用户可以不通过 WEB 认证就能与外网通信，地址组需要在**用户管理—>用户组配置**页面进行配置。
- 联系方式：自定义 WEB 认证弹出窗口的提示文字。
- 网络图片链接：输入网络图片的链接，使该图片作为 WEB 认证弹出窗口的背景。操作步骤：首先勾选**是否启用背景图片**在 WEB 认证页面的下方找到**网络图片链接**，然后填入网络图片的链接，点击**保存**。

9.4.1.2 远程认证

进入**用户认证—>网页认证**页面能够配置设备的远程认证功能。网页远程认证用于验证内网用户是否有权限访问因特网，即启用该功能后，设备将用户的认证信息存储到远程云服务器上，内网用户访问英特网时所需的认证信息由远程服务器生成，内网用户只要使用艾泰科技支持远程认证的任意设备，就可以在任何地点认证，并访问英特网。

图 9-18 WEB 认证_远程认证

- 启用 WEB 认证：勾选表示内网用户需通过 WEB 认证才能访问 Internet。
- 认证方式：选择远程认证。
- 过期时间：设置用户通过认证后，多久未产生流量后被踢下线。
- 认证模式：提供四个选项供选择。
  - 有线认证：有线用户需要通过 WEB 认证才能访问 Internet，其他用户直接访问 Internet。
  - SSID1 认证：接入无线网络 SSID1 的用户需要通过 WEB 认证才能访问 Internet，其他用户直接访问 Internet。

- SSID2 认证：接入无线网络 SSID2 的用户需要通过 WEB 认证才能访问 Internet，其他用户直接访问 Internet。
- 有线和无线认证：所有用户都需要通过 WEB 认证才能访问 Internet。

- 例外地址组：在设备启用 WEB 远程认证后，该地址组的用户可以不通过 WEB 认证就能与外网通信，地址组需要在**用户管理—>用户组配置**页面进行配置。
- 序列号：设备的唯一序列号。
- 激活码：和序列号相对应，且唯一。
- 域名名称：设置免认证的域名或 IP，如设置用户在认证未通过认证前可以访问 http://www.utt.com.cn,则可将该域名添加到域名白名单中。
- 域名白名单：显示域名白名单列表。

提示：

1) 若商家为首次使用远程认证，点击蓝色字体“注册商家账号”，便可进入注册页面注册新账号，注：每个序列号和激活码只能注册一个账号。

2) 若商家已有账号，则点击蓝色字体“登录”，便可登录设备，并按照“如何绑定设备”提示，进行设备绑定操作。

9.4.1.3 微信连wifi认证

用户在电脑、手机等设备上的微信客户端通过认证后即可访问因特网。

图 9-19 WEB 认证_微信连 wifi 认证

页面参数的设置请参阅章节：9.4.1.2 远程认证。

9.4.2　WEB认证账号配置

图 9-20 WEB 认证账号信息列表

图 9-21 WEB 认证账号信息

- 用户名：配置 WEB 认证用户的用户名。
- 并发数：显示使用同一 WEB 认证用户的数量。
- 用户状态：显示 WEB 认证用户的连接状态，包括：未使用、使用中。
- 计费模式：显示/勾选表示启用计费模式。
- 账号开通/停用日期：显示/配置 WEB 认证用户使用该账号的时间段。
- 总时间：限制 WEB 认证用户能够使用该账号的总时间，0 表示不限制。
- 已使用时间：显示当前认证账号累计使用的时间。
- 描述：显示/配置描述的内容。
- 密码：配置 WEB 认证用户的密码。

- 账号最大会话数：配置该账号的最大会话数量。
- 挂断：点击该按钮可挂断该用户的连接。
- 添加新条目：点击该按钮进入配置 WEB 认证账号信息页面。
- 删除所有条目：点击该按钮可删除该页面配置的所有信息。

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，在打开的认证成功的对话框中，点击修改密码。

(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。

(5) 用户每天只能自助修改 5 次密码。

(6) 管理员可以通过在**行为管控—>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。

2) WEB 认证用户如何安全下线：

(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，在打开的认证成功的对话框中，点击安全下线。

(3) 在打开的来自网页消息对话框中点击确定。

9.4.3 WEB认证连接状态

在 WEB 认证连接状态列表中显示已通过 WEB 认证且正在使用的帐号的用户名、IP 地址、MAC 地址等信息。

图 9-22 WEB 认证连接状态列表

9.4.4　微信连wifi

当访问用户过多，路由器的覆盖面积不能满足需求时，可使用 AC/AP+路由器方案，将 AP 通过有线或无线的方式连接到路由器，扩展无线信号的覆盖范围。

页面配置步骤：在 WEB 认证全局配置页面选择微信连 wifi 认证方式，然后在如下页面配置云帐号及 AP 的 BSSID 地址。

图 9-23 微信连 wifi 帐号配置

- 云帐号：配置在认证平台注册的账号。
- BSSID：配置 AP 的 BSSID。BSSID 即外接 AP 的 MAC 地址。多个 MAC 地址之间用逗号分割。

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**进入如下图所示页面。

图 9-24 用户组列表

图 9-25 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。

9.6　服务组配置

通过设置策略的服务组来匹配设备接收数据包协议、端口号以及包内容等信息。可在策略配置中引用系统预定义的服务，也可引用用户自定义的服务组。您可以针对服务组创建策略，而无需为服务组包含的每个服务单独创建访问控制策略，大大简化了管理员的工作量。例如，您可以把 telnet、pop3 以及 http 等多个服务配置属于同一服务组，这样您就可以通过配置一条访问控制策略控制对这些服务的访问。

在进入**防火墙**页面设置控制策略之前，可进入本页面为访问控制策略配置服务组。访问控制策略使用服务组来匹配设备接收数据包的协议、源端口、目的端口以及包内容等信息。设备提供了普通服务、URL、关键字、DNS 4 种服务类型。在每种服务类型下，用户均可以自定义服务，也可以把已有服务添加到服务组中。

图 9-26 服务组配置

- 服务组名：自定义新服务组的名称，不能重复。
- 服务类型：设备提供了普通服务、URL、关键字、DNS 和四种服务类型。
  - 普通服务：用来匹配设备接收数据包的协议和端口。
  - URL：用来过滤 URL 网址，可控制用户对站点及网页的访问。
  - 关键字：用来过滤 HTML 页面关键字中对应的西文符，如果某个网页里包含了你定义的关键字（如色情、法轮功、赌博等）所对应的西文字符，那么设备将直接屏蔽这个网页。
  - DNS：用来设置是否对某域名进行 DNS 解析。
- 新服务：由用户自定义的新服务，不同的服务类型下需要配置的新服务参数不同：
- 已有服务：显示设备中已存在的服务。
- 服务组列表：显示服务组包含的服务。
  - “=〉”：用于将自定义的新服务或已有服务添加到**服务组列表**中。
  - “<=”：用于将**服务组列表**中的服务导入到**新服务**或**已有服务框**中。
  - 删除：用于删除**服务组列表**中的服务。
  - 保存：单击**保存**按钮，配置参数生效。

提示：

1) 服务组最多可配置包含 10 个服务或其它服务组。
2) 服务组名不区分大小写，即服务组“A”和“a”指的是同一个服务组。
3) 在配置服务组包含其它服务组时，一定要注意，如果某个服务组已经包含了其它服务组，则这个服务组不能再配置属于其它服务组。

配置服务组：首先输入自定义的服务组名并选择要配置的服务类型，然后根据需要配置新服务，并单击“=>”将配置的新服务添加到**服务组列表**中，可连续配置多个新服务；也可在**已有服务**框中选中一个或多个服务，单击“=>”将已有服务添加到**服务组列表**中，最后单击**保存**按钮即可。

编辑服务组：如果想修改某个服务组的信息，首先在**服务组信息列表**中单击此服务组的**编辑**超链接，其配置信息即填充到服务组配置框中。如果想修改某个用户自定义的服务，在**服务组列表**中选中此服务，单击“<=”按钮，即可在**新服务**配置框中修改此服务；如果想删除某个服务，在**服务组列表**中选中此服务，单击**删除**按钮即可，上述操作必须在单击**保存**按钮后才生效。

可在**服务组信息列表**中查看配置的服务组信息，如下图所示。

图 9-27 服务组信息列表

- 添加新条目：如果想新添加一个服务组，只需在**服务组信息列表**中单击**编辑**超链接，其信息即会填充到配置框内，添加并单击**保存**按钮即可。
- 编辑：如果想修改某个服务组，只需在**服务组信息列表**中单击**编辑**超链接，其信息即会填充到配置框内，修改并单击**保存**按钮即可。
- 删除：选中欲删除的一个或多个服务组，单击右下角的**删除**按钮，即可删除。注意：您无法删除已经在访问控制策略中引用的服务组，必须先修改或删除所有引用它的访问控制策略，才能删除此服务组。

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，查看已配置的时间段列表。

图 10-1 时间段配置列表

点击**添加新条目**，进入如下图所示的配置页面。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。下面介绍时间段配置参数的含义。

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。下面介绍上网行为管理配置参数的含义。

- 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。

图 10-4 行为管理配置

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、192.168.1.192。

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

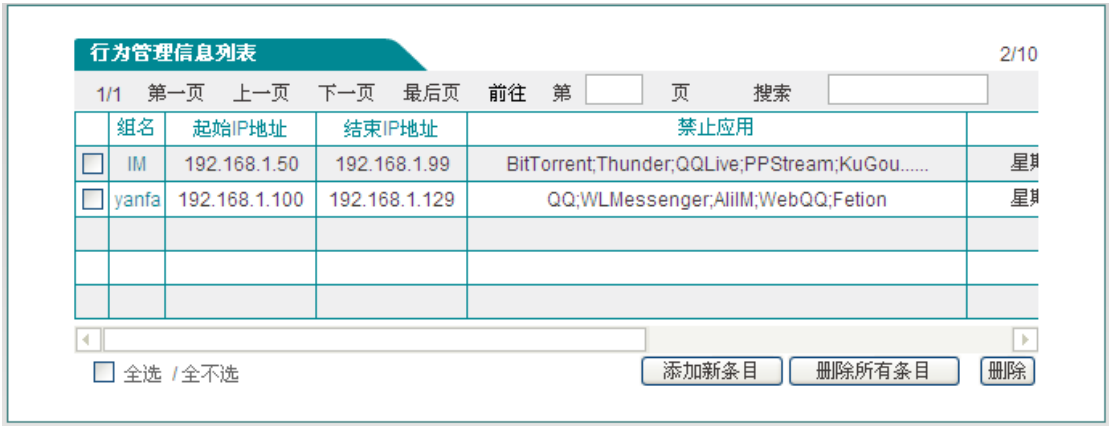


图 10-5 上网行为管理实例

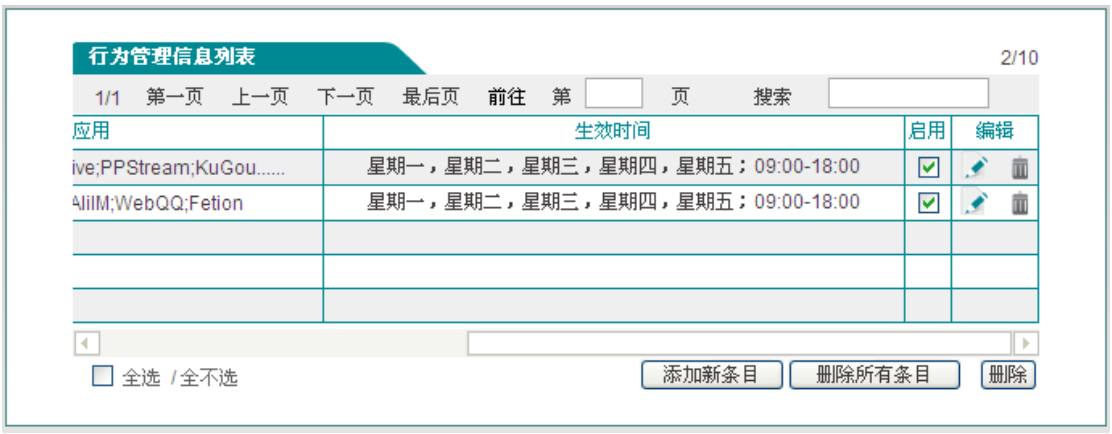


图 10-6 上网行为管理实例（续图 10-5）

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。
- 导出账号：点击该按钮可以导出 QQ 白名单中条目中的 QQ 账号。
- 导入账号：点击该按钮可以将 QQ 批量导入到 QQ 白名单条目中。

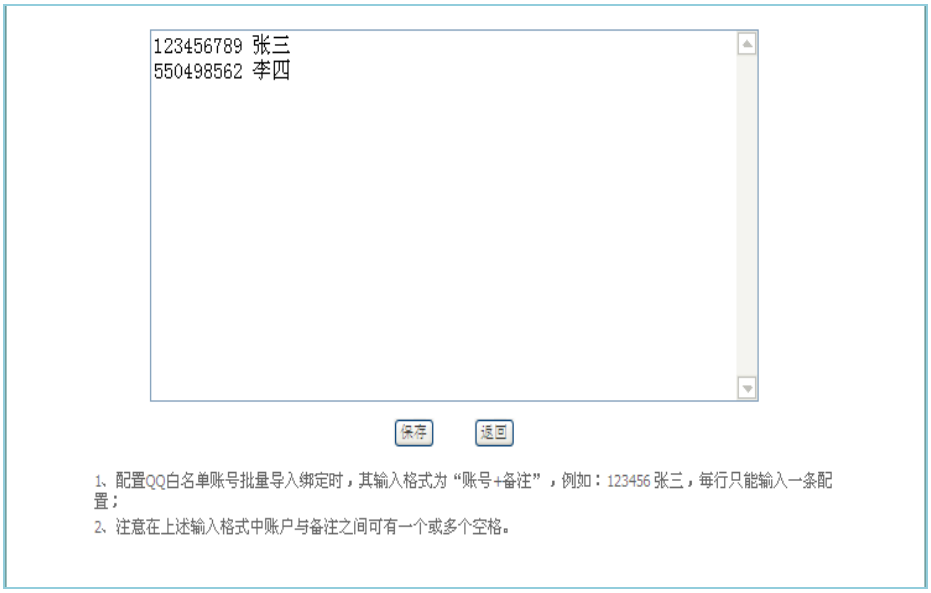


图 10-8 导入账号

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 10-9 MSN 白名单

- 启用 MSN 白名单：勾选表示启用 MSN 白名单功能。

10.5 阿里旺旺白名单

阿里旺旺白名单是在**上网行为管理**页面禁止阿里旺旺后定义允许登录的阿里旺旺用户。

进入**行为管理—>阿里旺旺白名单**页面，启用阿里旺旺白名单功能后，点击**添加新条目**进入阿里旺旺白名单配置页面添加阿里旺旺白名单用户。

图 10-10 阿里旺旺白名单

- 启用阿里旺旺白名单：勾选表示启用阿里旺旺白名单功能。

10.6　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。

10.6.1　日常事务通告

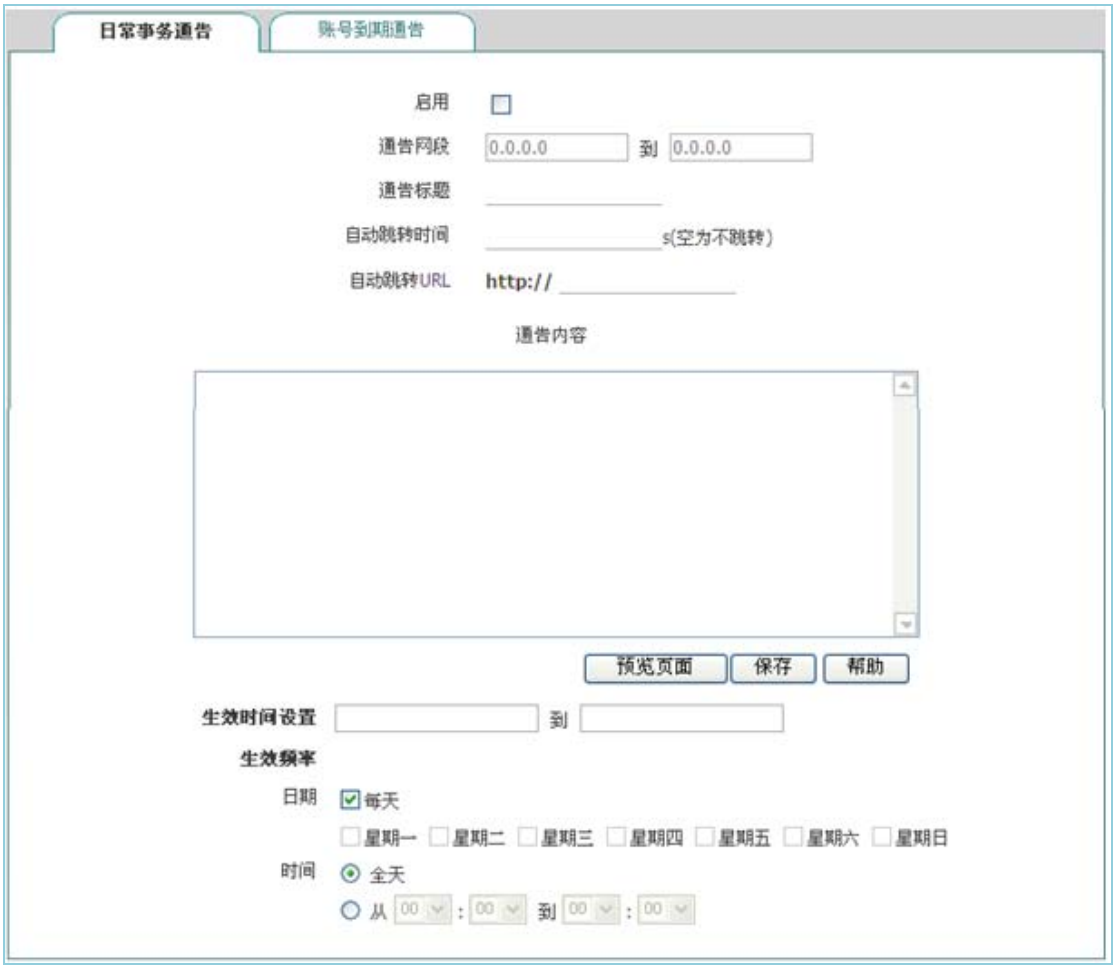


图 10-11 日常事务通告

- 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。
- 自动跳转时间：按设置的时间跳转到指定的页面。
- 自动跳转 URL：自动跳转到指定的 URL 地址。

- 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。

10.6.2　账号到期通告

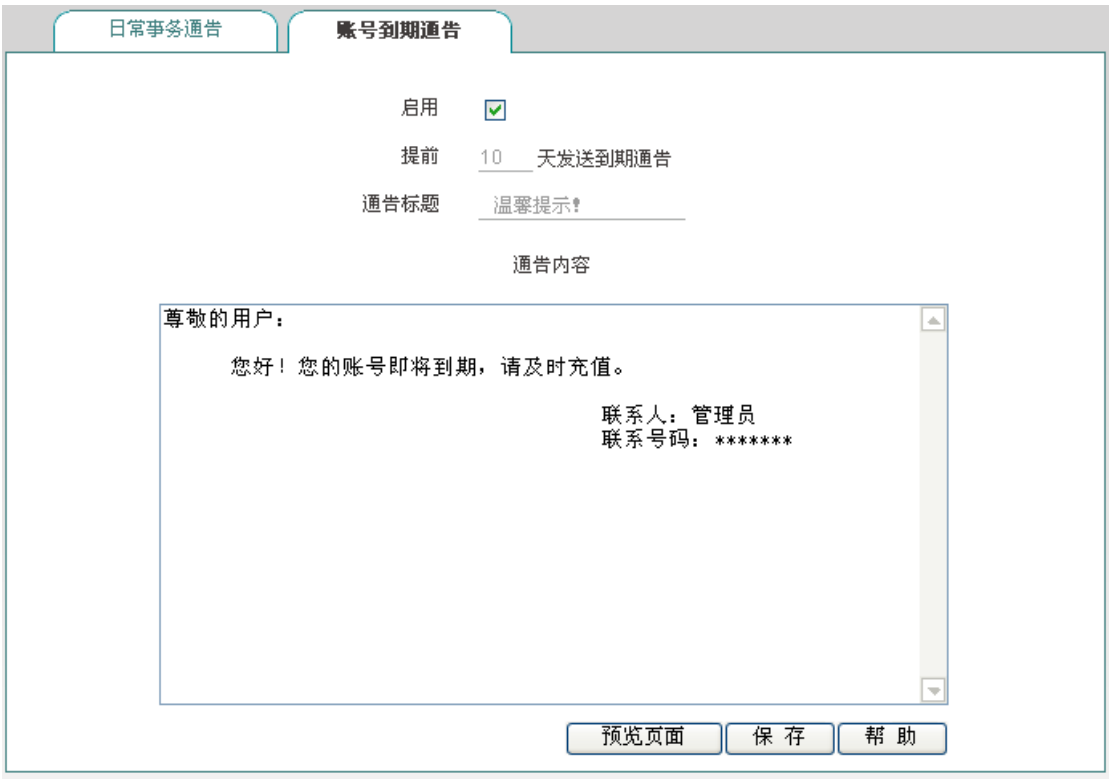


图 10-12 账号到期通告

- 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，当用户通过认证后，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。

10.7　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**页面，如下图所示，能查看设备已开启的行为审计功能的日志信息。

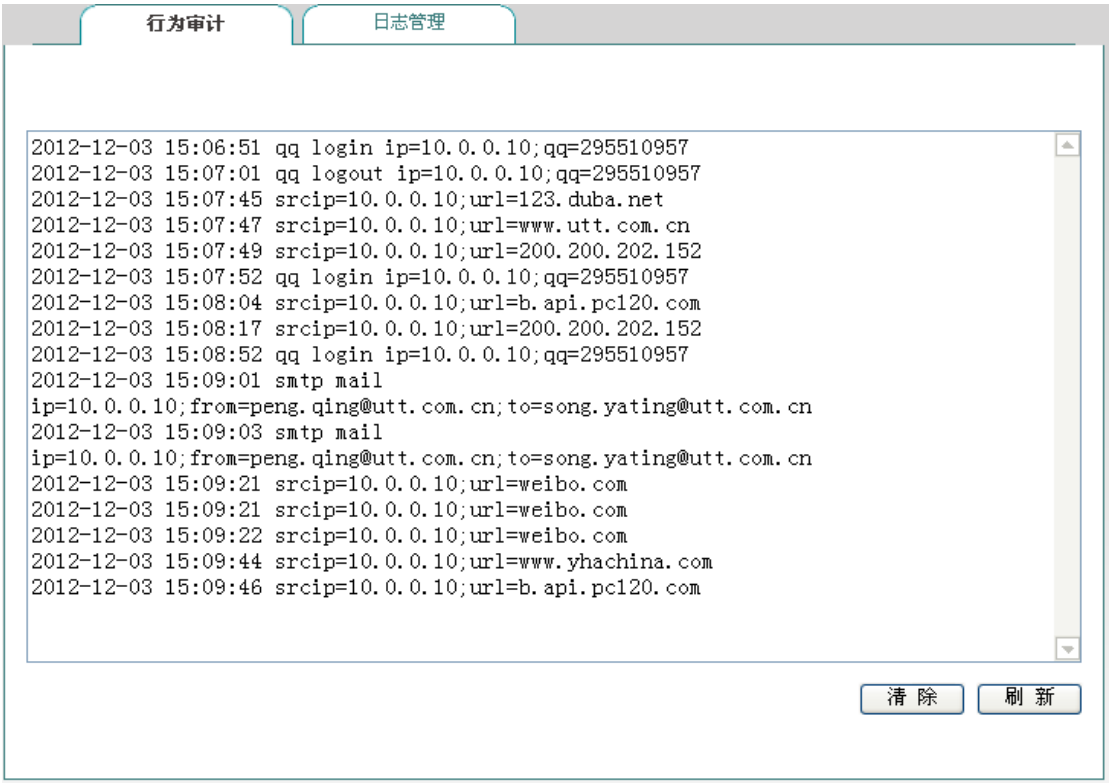


图 10-13 行为审计

提示：上网行为审计能够记录最新的 400 条日志信息。

进入**行为管理—>上网行为审计—>日志管理**页面可配置设备的上网行为审计功能，如下图所示。

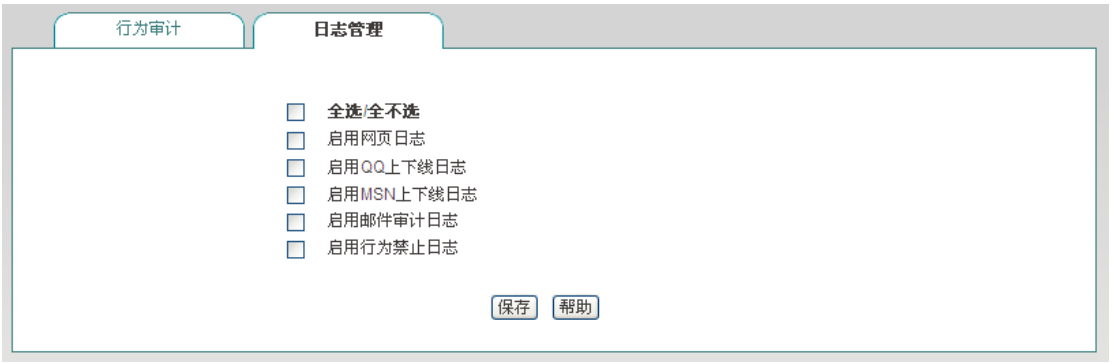


图 10-14 日志管理

- 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：“2012-12-03 15:07:47 srcip=10.0.0.10;url=www.utt.com.cn”表示在 2012 年 12 月 03 日 15 时 07 分内网 IP 地址为 10.0.0.10 的用户访问了 www.utt.com.cn。

- 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。
- 启用行为禁止日志：启用行为禁止日志后，能够在**行为审计**页面查看被行为管理 PDB 过滤的用户记录。

10.8　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 10-15 策略库信息列表

下面介绍策略库信息列表中各项参数的含义。

- 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项参数的涵义。

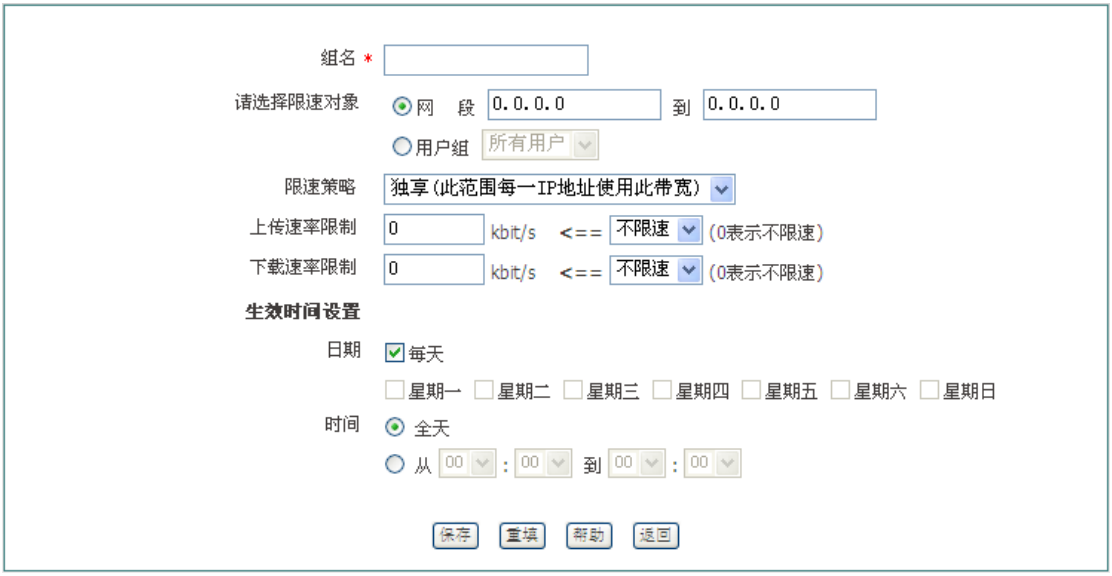


图 11-2 精细化限速配置

- 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。
- 请选择限速对象：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**带宽管理—>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：建议不要同时开启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。
- WAN 口上、下行带宽：设置从 ISP 申请的 WAN 口得上、下行带宽。

11.3 连接限制

本节介绍**带宽管理—>连接限制**页面。您可以通过设置各连接数来定义设备允许内网每台主机建立的最大总连接数、最大 TCP 连接数、最大 UDP 连接数、最大 ICMP 连接数。

图 11-4 连接限制

- 启用连接限制：勾选表示启用连接限制。
- 总连接数：允许内网每台主机建立的最大总连接数，默认是 1500。
- TCP 连接数：允许内网每台主机建立的最大 TCP 连接数，默认为 1000。
- UDP 连接数：允许内网每台主机建立的最大 UDP 连接数，默认为 800。
- ICMP 连接数：允许内网每台主机建立的最大 ICMP 连接数，默认为 100。

提示：

1）　当连接数设置为 0 时，表示对内网每台主机的连接数不进行限制。

2）　当内网应用（比如网络游戏）连接速度变慢时，可以适当提高**总连接数**以及 **UDP 连接数**（或者 **TCP 连接数**）。注意，上述连接数设置过高可能会导致设备减弱甚至丧失防止 DDoS 攻击的能力。

3）　一般情况下，最大会话数不能设置得太小，建议：**TCP 连接数**不小于 100、**UDP 连接数**不小于 50、**ICMP 连接数**不小于 10。如果它们的值太小，将导致局域网用户不能上网或上网异常。

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 IP 欺骗防御：启用后能有效防御内网的 IP 欺骗。
- 启用 UDP FLOOD 防御：启用后能有效防御内网 UDP FLOOD 攻击。
- 启用 ICMP FLOOD 防御：启用后能有效防御内网 ICMP FLOOD 攻击。
- 启用 SYN FLOOD 防御：启用后能有效防御内网 SYN FLOOD 攻击。
- 启用 ARP 欺骗防御：启用该功能后，设备 LAN 口会每隔一定的时间（默认为 100 毫秒）发送 ARP 广播包，该功能能有效防御 ARP 欺骗。
- 启用设备访问控制：启用后，只允许地址段范围内的主机从 LAN 口登陆设备。
- 启用端口扫描防御：启用后能有效防御内网端口扫描。

2）　**外网防御**

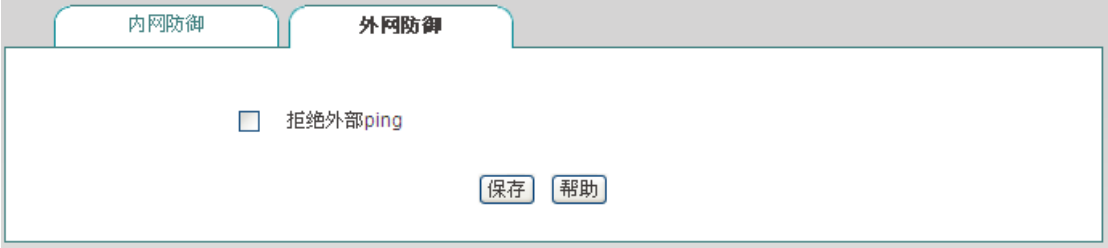


图 12-2 安全配置——外网防御

- 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。

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其他内容进行分析，并按照策略的优先级从上至下搜索策略表，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。

4)　DNS 过滤

DNS 过滤指对域名进行过滤，根据域名名称中的关键字进行 DNS 过滤。

过滤类型为 DNS 过滤时，可供设置的过滤条件包括：源地址、过滤内容（指需要过滤的域名名称）、动作、生效时段。

提示：DNS 过滤是通过 53 端口实现过滤，URL 过滤是通过 80 端口实现过滤。

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

- 启用策略：勾选表示启用访问控制策略列表中的策略。
- 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，在配置过程中，可直接引用在用户组配置和服务组配置页面中设置的组，也可以自定义。

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项参数的涵义以及注意事项。

一、 访问控制策略配置—IP 过滤

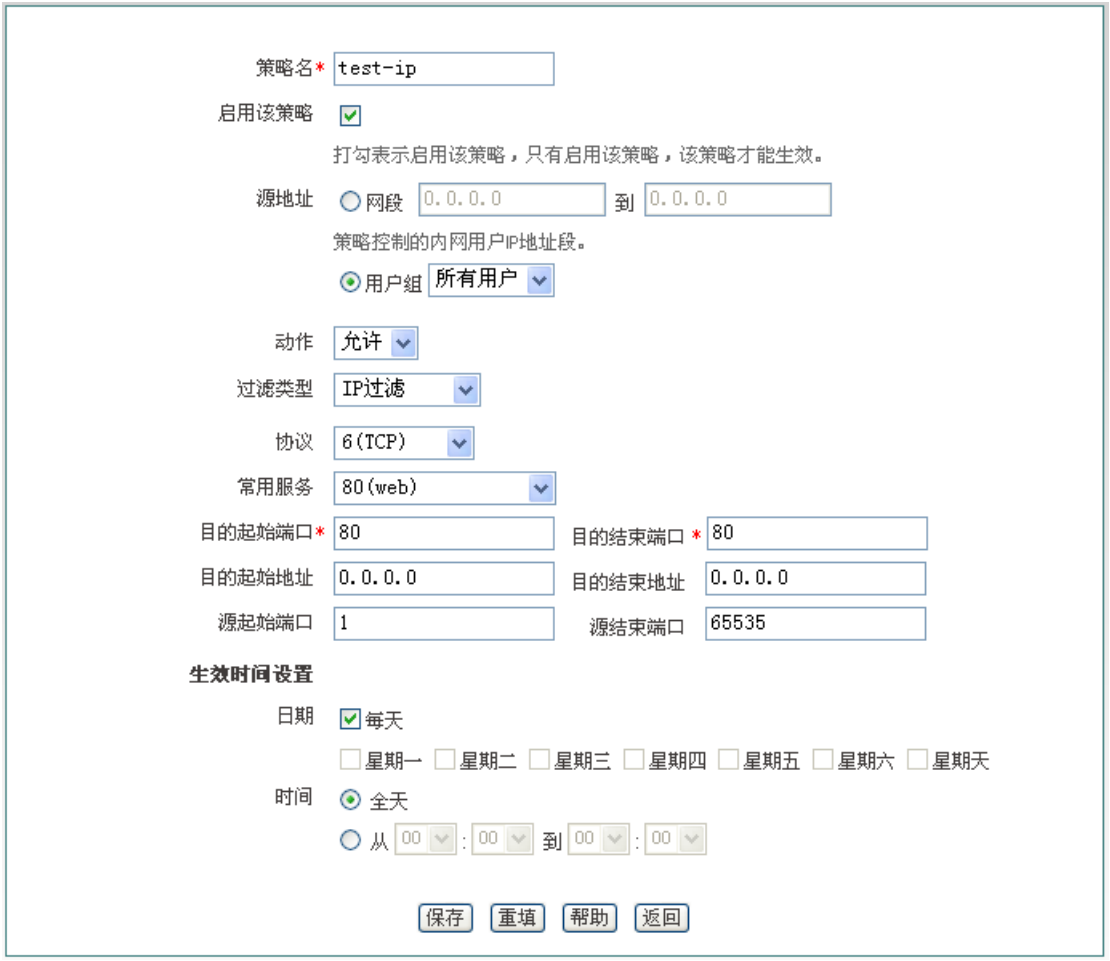


图 12-4 配置访问控制策略—IP 地址过滤

- 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、DNS 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

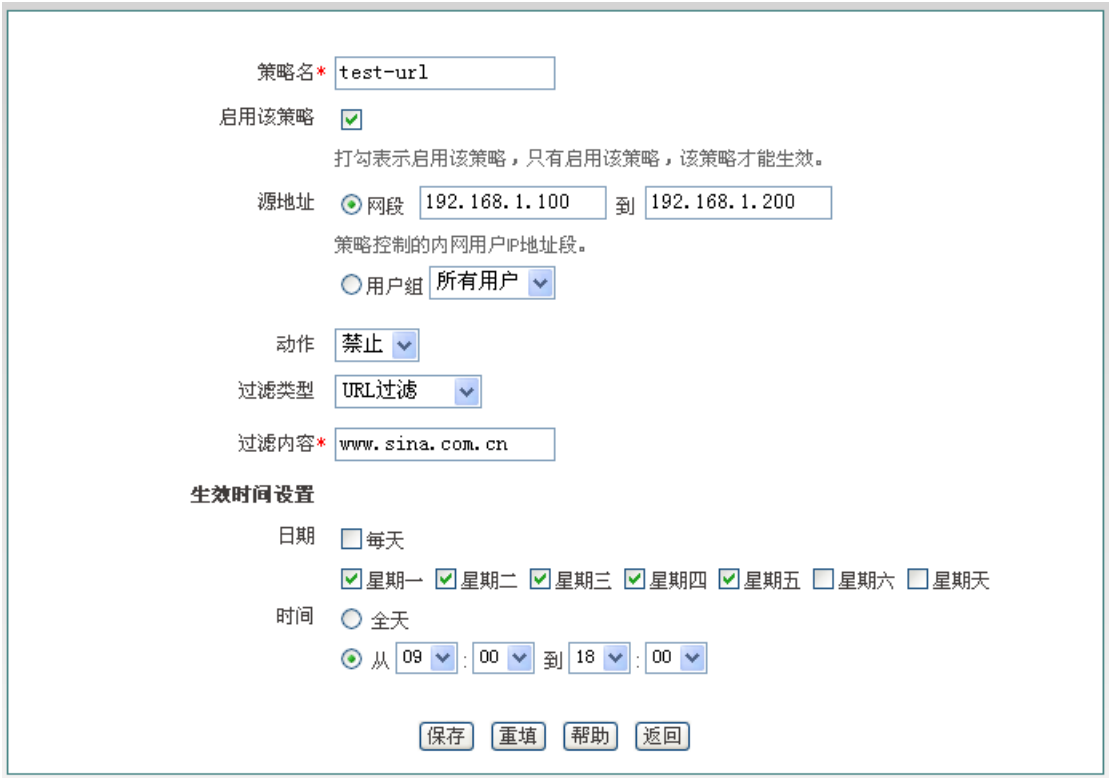


图 12-5 配置访问控制策略—URL 过滤

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：配置该访问控制策略过滤的 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 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。

四、 访问控制策略配置—DNS 过滤

图 12-7 访问控制策略配置——DNS 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：这里选择 **DNS 过滤**。
- 过滤内容：设置要过滤的域名名称。

提示：在过滤内容中输入通配符 “ * ” 可实现对多个域名的过滤，例如在过滤内容中输入域名名称“*.163.*”，动作选择“禁止”，则内网用户将不能访问域名中有“.163.”的所有网页。

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。

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 12-8 访问控制策略—实例一

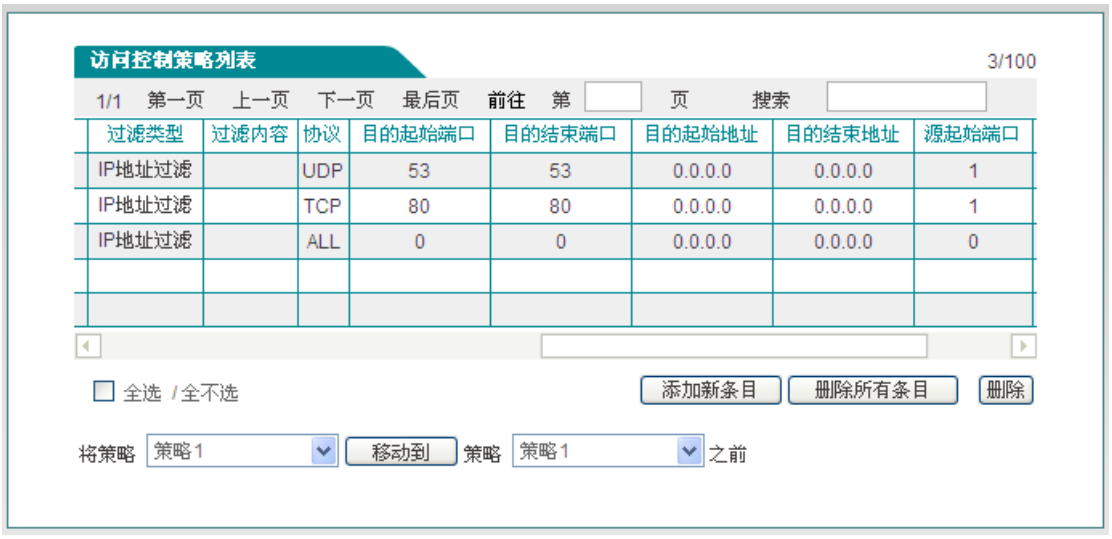


图 12-9 访问控制策略—实例一（续图 12-8）

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 12-10 访问控制信息列表—实例二

图 12-11 访问控制信息列表—实例二（续图 12-10）

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。

12.3.1　域名过滤配置

图 12-12 域名过滤

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。

12.3.2 域名过滤通告

本节主要讲述**防火墙—>域名过滤—>域名过滤通告**功能，当禁止访问某个网站时，希望给用户一个提示，表示此网站被禁止而非网络问题。点击域名过滤通告选项卡，进入如下图所示页面。

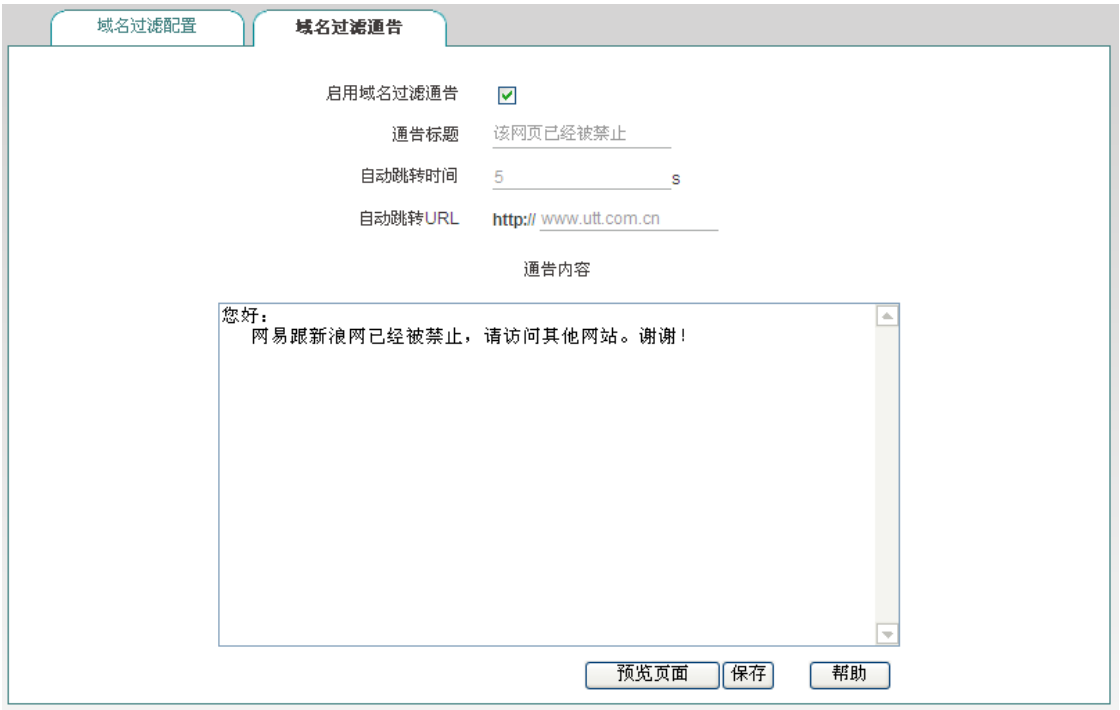


图 12-13 域名过滤通告页面

- 启用域名过滤通告功能：打勾表示启用，启用域名过滤通告功能后，当内网用户访问被禁止的域名时，设备将发送通告给此用户，并且到设置的时间后，将跳转到指定的网址。
- 通知标题：设备推送的通告信息的标题。
- 自动跳转时间：设置访问域名列表所列域名的自动跳转时间。为空时表示不跳转，为 0 时表示立即跳转。
- 自动跳转 URL：设置访问域名列表所列域名时自动跳转到的域名地址。
- 通知内容：设备推送的通告信息的内容。
- 保存：域名过滤全局配置参数生效。
- 预览页面：预览所配置的通告内容，如下图所示：

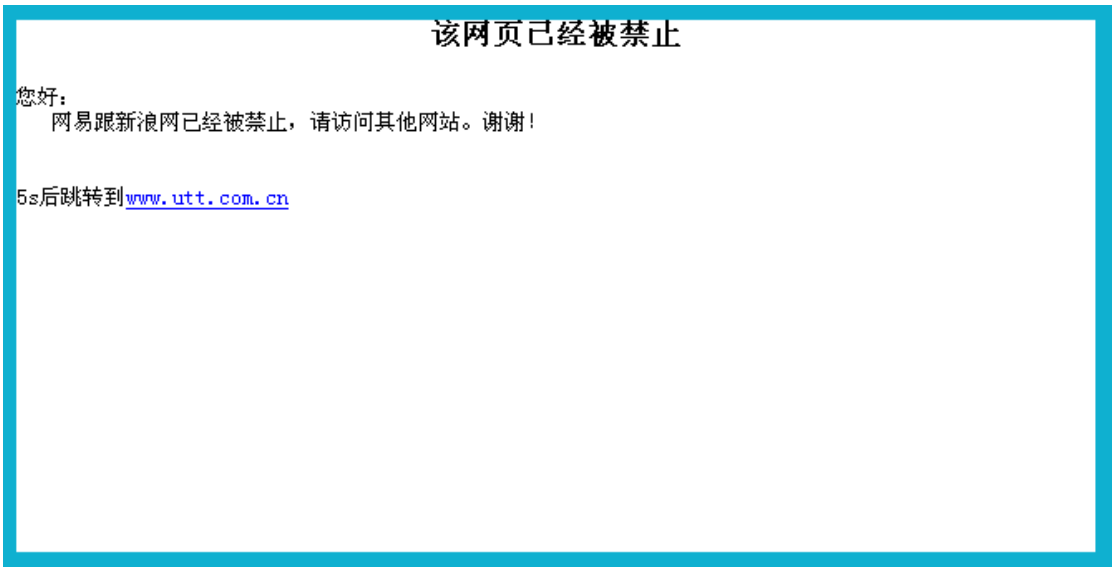


图 12-14 预览页面

12.4　MAC地址过滤

本节介绍**防火墙—>MAC 地址过滤**页面的 MAC 地址过滤功能，包括：MAC 地址过滤操作步骤以及 MAC 地址过滤配置过程中注意的事项。

12.4.1　MAC地址过滤列表

图 12-15 MAC 地址过滤列表

- 启用 MAC 地址过滤：勾选表示启用 MAC 地址过滤功能。
- 过滤规则：用户可根据自己的需求进行选择**允许 只允许列表中的 MAC 地址访问本网络**或**禁止 只禁止列表中的 MAC 地址访问本网络**。
- 用户名：显示配置 MAC 地址过滤的用户名。
- MAC 地址：显示配置的 MAC 地址过滤的 MAC 地址。

12.4.2　MAC地址过滤配置

进入 MAC 地址过滤信息列表，点击**添加新条目**，进入 MAC 地址过滤配置页面，如下图所示。

图 12-16 添加新条目

- 用户名：配置 MAC 地址过滤的用户名。
- MAC 地址：配置要进行过滤的 MAC 地址。
- 用户也可以在**防火墙—>MAC 地址过滤—>MAC 地址过滤配置**页面进行批量配置。

图 12-17 MAC 地址过滤配置

- 文本框：在文本框中设置对应的 MAC 地址过滤信息。其输入格式为“MAC 用户名”。
  - 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。

提示：

1) 在上述输入格式中 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。

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。

13.1　PPTP

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。

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。

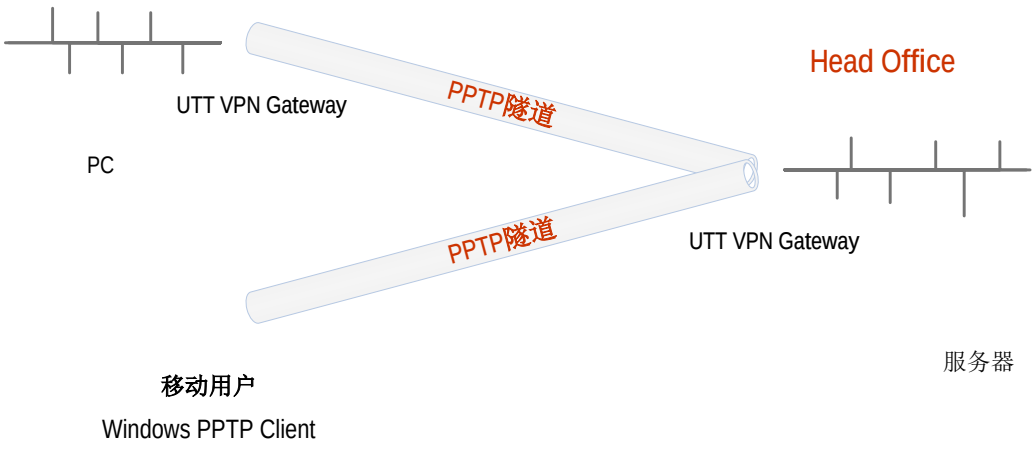


图 13-1　PPTP 典型应用

13.1.1　PPTP信息列表

进入 **VPN 配置—>PPTP** 页面，能查看相关的 PPTP 隧道信息，如用户名、业务类型、远端内网 IP 地址、会话状态、已建立连接的时间等。

图 13-2 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。

13.1.2　PPTP服务端配置

进入 **VPN 配置—>PPTP** 页面，在如图 13-2 所示的页面点击**添加服务器**，进入 **PPTP 服务器**页面。

13.1.2.1　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：设置建立 PPTP VPN 的密码验证方式，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。
- 主/备 DNS 服务器：当设备配置为 PPTP/L2TP 服务端时，可以为 PPTP/L2TP 客户端分配 DNS 地址，其用于客户端连上服务端之后可以通过服务端线路分配的 DNS 地址浏览网页，可解决用户拨通 VPN 后可以访问服务器内部网却无法打开网页的问题。
- 加密方式：设置数据加密的方式，选项有 MPPE 加密、不加密。注：采用 MPPE 加密方式必须选择 MS-CHAPV2 密码验证方式。

13.1.2.2 账号配置

下面介绍为 PPTP 客户端配置账号时的各项参数的涵义。

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。
- 固定 IP 地址：设置 PPTP 服务器分配给客户端的 IP 地址，该地址必须属于 PPTP 服务器地址池中。

- 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。

13.1.3 PPTP客户端配置

进入 **VPN 配置—>PPTP** 页面，点击**添加客户端**，进入 **PPTP 客户端**页面。下面介绍配置 PPTP 客户端各项参数的涵义。

图 13-5 PPTP 客户端

- 启用该配置：勾选表示启用该配置。
- 启用 NAT：启用 NAT 后，PPTP 客户端会对此 PPTP 隧道连接进行 NAT，即将局域网用户的 IP 地址转化为对端 PPTP 服务器分配的 IP 地址，这样局域网用户将使用 PPTP 服务器分配的 IP 地址连接到隧道对端的局域网，隧道对端设备无需设置到本地的路由。
- 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。

13.1.4　PPTP配置实例

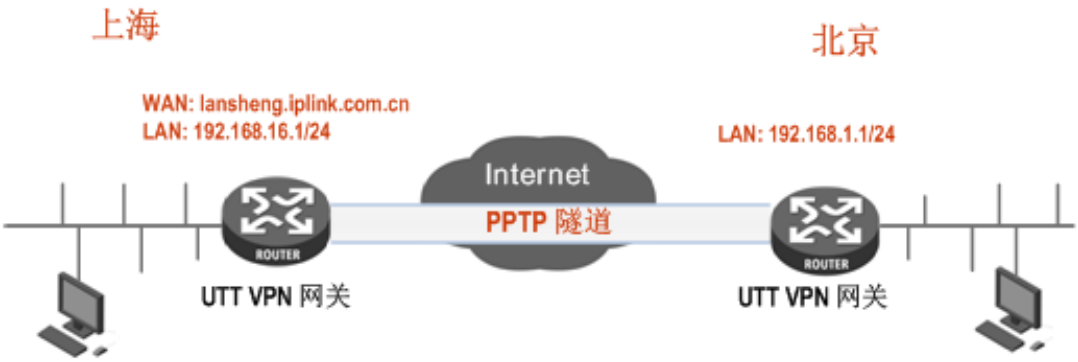


图 13-6 PPTP 实例拓扑图

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：WX2000；北京 VPN 网关型号：进取™ 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

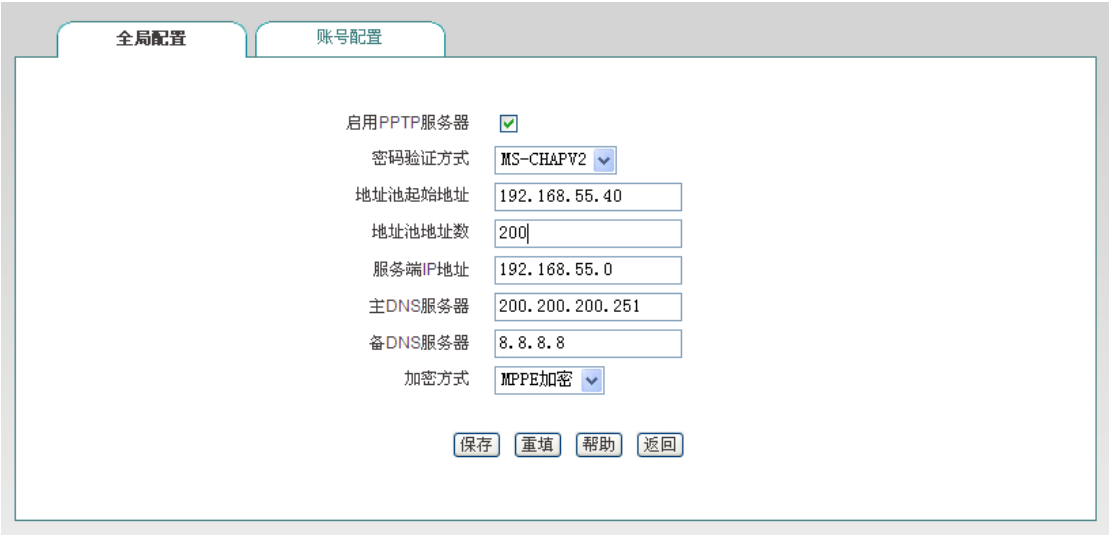


图 13-7 PPTP 服务端配置 1

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

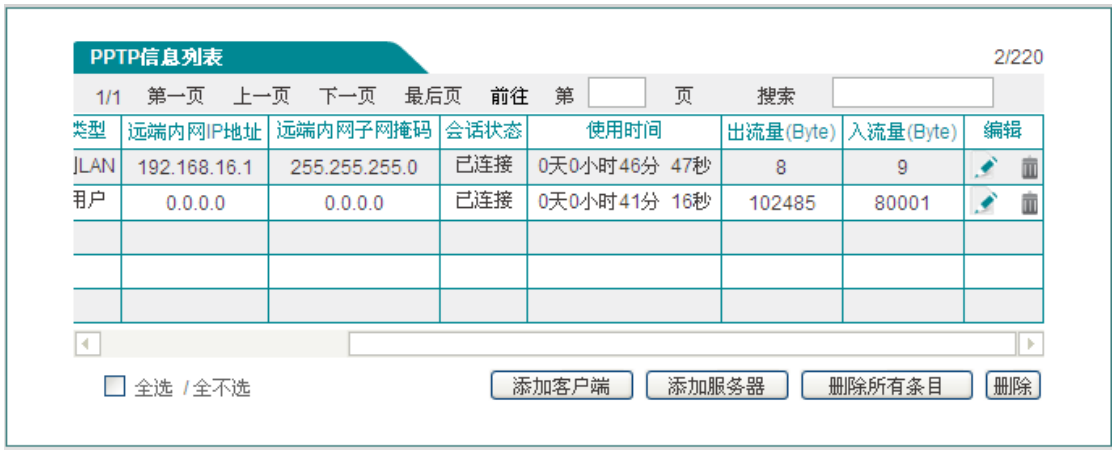


图 13-11 PPTP 服务端信息列表 2

图 13-12 PPTP 客户端信息列表 1

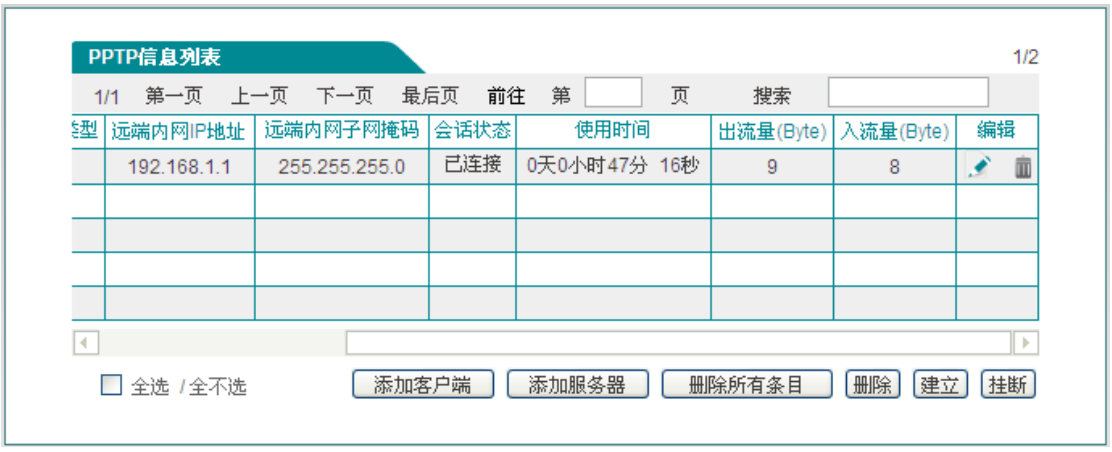


图 13-13 PPTP 客户端信息列表 2

13.2 IPSec

13.2.1 IPSec 概述

随着安全标准与网络协议的不断发展，各种 VPN 技术层出不穷，IPSec VPN 则是当前应用最广泛的 VPN 安全技术之一。IPSec 是创建和维持 IP 网络安全通信的一套开放标准、协议，它提供两种安全机制：加密和认证。加密机制保证了数据的机密性，认证机制保证了数据是来自原始的发送者并且在传输过程中没有被破坏和篡改。

IPSec 能提供以下服务：

- 数据机密性：IPSec 发送方在通过网络传输包前对包进行加密。
- 数据完整性：IPSec 接收方对发送方发来的包进行认证，以确保数据在传输过程中没有被篡改。
- 数据源认证：IPSec 在接收端可以认证发送 IPSec 报文的发送端是否合法，以确保数据的真实性。
- 抗重播：IPSec 接收方可检测并拒绝接收重复的报文。

13.2.1.1 缩略语与专业名词

IPSec（IP Security Protocol），IP 网络安全协议：IPSec 是 IETF 制定的一系列协议，以保证在 Internet 上传送数据的安全保密性能，通信方之间在 IP 层通过加密与数据源验证来保证数据包在 Internet 上传输时的机密性、完整性和真实性。

IKE（Internet Key Exchange），因特网密钥交换：IKE 用于通信双方协商和建立安全联盟、交换密钥。IKE 定义了通信双方进行身份验证、协商加密算法以及生成共享密钥的方法。

DES（Data Encryption Standard），数据加密标准：DES 是 IPSec 使用的一种数据加密算法，用于对数据包进行加密。

3DES（Triple Data Encryption Standard），三倍数据加密标准：3DES 是 IPSec 使用的一

种数据加密算法，用于对数据包进行比 DES 强度更高的加密。

AES（Advanced Encryption Standard），高级加密标准：AES 是 IPSec 使用的一种数据加密算法。与 DES 和 3DES 相比，AES 更加高效、安全。

DH（Diffie-Hellman Group），一种密钥交换算法：通信的双方各自生成一对公/私钥，只需和对方交换公钥，经过计算就可得到一组用来保护通信的密钥，这就避免了直接在通信中传输密钥的风险，提高了整个 IPSec 系统的安全性。DH 有一个重要的属性：group（组件），共有 5 种基本 group，常用的 group 有：模数为 1024 位的 MODP 组（group2）、模数为 1536 位的 MODP 组（group5）。

MD5（Message Digest 5），消息摘要版本 5：从任意长度信息和 16 字节密钥生成 128 位散列（也称作数字签名或信息整理）的算法。所生成的散列（如同输入的指印）用于验证内容和来源的真实性和完整性。

SHA-1（Secure Hash Alogrithm1），安全散列算法 1：从任意长度信息和 20 字节密钥生成 160 位散列的算法。通常认为它比 MD5 更安全，因为它生成的散列更大。

SA（Security Association），安全联盟：在两个设备之间建立一个 IPSec VPN 隧道并通过其进行安全通信之前，它们必须就通信期间需要使用的安全参数达成一致，即建立一个 SA。SA 将指定需要使用的认证与加密算法、在通话期间使用的密钥和安全联盟本身需要维持的时间，SA 是单向的。

SPI（Security Parameter Index），安全参数索引：SPI 实际上是一个长度为 32 位的数据实体，用于独一无二地标识出接收端上的一个 SA。

AH（Authentication Header），认证包头：属于 IPSec 的一种协议。该协议用于为 IP 数据包提供数据完整性、数据包源地址验证服务。与 ESP 协议相比，AH 不提供对通信数据加密服务。

ESP（Encapsulating Security Payload），封装安全负荷：属于 IPSec 的一种协议。它用于确保 IP 数据包的机密性（对第三方不可见）、数据的完整性以及对数据源地址的验证，同时还具有抗重播的特性。

PSK（Pre-Shared Key），预共享密钥：IKE 身份验证方法之一，它要求每个 IKE 对等方使用一个预定义和共享的密钥来对 IKE 交换执行身份验证。

第一阶段和第二阶段：采用互联网密钥交换协议（IKE）建立 IPSec 通道安全联盟（SA），需要进行两个阶段的协商。在第一阶段，参与者相互验证身份并协商建立一个用来协商随后 IPSec SA 的安全通道。在第二阶段，参与者协商并建立用于加密和认证用户数据的 IPSec SA。

Main Mode and Aggressive Mode，主模式和野蛮模式：IKE 自动协商通道的第一阶段，可以在主模式和野蛮模式这两种模式下进行。主模式下，发起方和响应方之间进行三次双向信息交换，总共六条信息。野蛮模式下，发起方和响应方获取相同的对象，但仅进行两次交换，总共有三条消息。

DPD（Dead Peer Detect）：周期对端检测：使用 DPD，能够定期检测 SA 对方是否正常，网络连接是否正常。

IPSec NAT-T（NAT-Traversal），IPSec NAT 穿透技术：该技术实现了 IPSec 协议穿透 NAT 设备。

13.2.1.2 安全联盟

在两个设备之间建立一个 IPSec VPN 隧道并通过其进行安全通信之前，它们必须就通信期间需要使用的安全参数达成一致，即建立一个安全联盟 SA。SA 是由一对指定的安全参数索引（SPI）、目标 IP 地址以及使用的安全协议组成。

通过 SA，IPSec 隧道可以提供以下安全功能：

- 机密性（通过加密）
- 内容完整性（通过数据认证）
- 发送方认证和认可（通过身份认证）

一、安全联盟建立

安全联盟（SA）是 IPSec 隧道双方用于确保隧道安全的有关方法和参数的单向协议。对于 IPSec 双向通信，至少必须有两个 SA，一个用来接收来自对端的数据，一个用来发送数据给对方。

建立 SA，需要进行两个阶段的协商：

- 在第一阶段，通信双方协商如何保护以后的通信，建立一个已通过身份认证和安全保护的通道（即 IKE SA），此通道将用于保护后面的 IPSec SA 的协商过程。
- 在第二阶段，通信双方为 IPSec 协商加密算法、密钥、生存周期以及认证身份，建立用于加密和认证用户数据的通道（即 IPSec SA）。

1） 第一阶段

第一阶段可以使用野蛮模式（Aggressive Mode）或主模式（Main Mode），不管使用哪种模式，双方均将交换对方可以接受的安全提议，例如：

- 加密算法（DES、3DES 和 AES128/192/256）和认证算法（MD5 和 SHA-1）
- Diffie-Hellman 组（请参阅本节的“Diffie-Hellman 交换”）
- 预共享密钥

当隧道的两端都同意接受所提出的至少一组第一阶段安全参数，并处理相关参数时，一个成功的第一阶段协商将结束。设备作为发起方时，目前最多同时支持 8 种第一阶段协商的提议，允许用户定义一系列安全参数。作为响应方时，可接受任何组合形式的第一阶段协商的提议。

➢ **主模式和野蛮模式（Main Mode / Aggressive Mode）**

第一阶段可能发生在野蛮模式或主模式下，这两种模式如下所述：

主模式：发起方和响应方之间进行三个双向信息交换（总共六条信息）以完成以下功能：

- 第一次交换，（信息 1 和 2）：提出并接受加密和认证算法。
- 第二次交换，（信息 3 和 4）：执行 Diffie-Hellman 交换，发起方和响应方各提供一个当前数（随机生成的号码）。
- 第三次交换，（信息 5 和 6）：发送并验证其身份。

在第三次交换信息时传输的信息由在前两次交换中建立的加密算法保护。因此，在明文中没有传输参与者的身份，从而提供了最大限度的保护。

野蛮模式：发起方和响应方获取相同的对象，但仅进行两次交换，总共有三条消息：

- 第一条消息：发起方建议 SA，发起 Diffie-Hellman 交换，发送一个当前数及其 IKE 身份。
- 第二条消息：响应方接受 SA，认证发起方，发送一个当前数及其 IKE 身份，以及发送响应方的证书（如果使用证书）。
- 第三条消息：发起方认证响应方，确认交换。

由于参与者的身份是在明文中交换的（在前两条消息中），故野蛮模式不提供身份保护。

提示：

当 IPSec 隧道的连接方式为对方动态连接到本地、动态连接到网关时，必须使用野蛮模式进行协商。

➢ **Diffie-Hellman** 交换

Diffie-Hellman 交换也称“DH 交换”，它允许双方生成一个共享密钥。该技术的优点在于它允许通信双方在非安全媒体上创建密钥，而不必把预共享密钥通过网络传输。共有五种基本 DH 组（设备支持组 2 和 组 5），在各组计算中所使用主要模数的大小都不同，如下所述：

- DH 组 2：1024 位模数
- DH 组 5：1536 位模数

模数越大，就认为生成的密钥越安全。但是，模数越大，密钥生成过程就越长。

提示：由于每个 DH 组的模数大小都不同，因此 IPSec 隧道通信双方必须使用相同的组。

2） 第二阶段

当通信双方建立了一个已认证的安全通道后，将继续执行第二阶段，在此阶段中，将协商 IPSec SA 以保护要通过 IPSec 隧道传输的用户数据。

与第一阶段的过程相似，通信双方交换提议以确定要在 SA 中使用的安全参数。第二阶段提议还包括一个安全协议（目前设备支持 ESP）和所选的加密和认证算法。

不管在第一阶段中使用何种模式，第二阶段总是在“快速”模式中运行，并且包括三条消息的交换。

二、安全联盟的维护

一旦 SA 建立完毕，IPSec 双方还必须维护 SA，确保 SA 是安全有效的，IPSec 通过以下方法实现 SA 的有效性检测：

1） SA 生存时间

在建立 SA 的协商过程中，双方会协商该 SA 的生存时间，当生存时间达到预先设定的值时，需要重新协商以建立新的 SA。周期性的重新协商，相当于定期更改密码。

WEB UI 方式下，在 **VPN 配置—>IPSec** 的高级选项中，可配置生存时间和最大流量。
由于频繁重建 SA 需要消耗大量的系统资源（主要是 DH 交换和当前数生成），会降低数据传输效率。因此 SA 的生存时间通常设置的比较长（典型的是 1 小时到 1 天），在有效期内，由于双方不能互相检测对方(类似 PING 的功能),通信的双方只能“假设”对方是正常工作的，万一有一方发生了不可预见的问题或连接双方的网络有故障,通信的另一方并不知道此时双方的连接线路中断，还会继续向早已经不存在的另一方发送数据，造成虚假连接（SA 正常，发出正常，但无法完成双向通信），因此需要一种有效的方法来检测参与 IPSec SA 的双方都完全正常，他们之间的网络连接也完全正常。这种检测方法的开销要比重新协商 IPSec SA 更小，因此可以用更高的密度进行检测。这种技术就是 IPSec“DPD”，DPD 作为 SA 协商的一种补充而存在。

2) DPD（Dead Peer Detect）

IPSec DPD 定期检测 SA 对方是否还存在，在 SA 的生存时间和最大流量范围内，定期检测对方网络是否可达，程序是否正常，以便发现网络变化导致的通信故障或避免与一个已经不存在的“火星人”主机保持 SA，这个检测周期通常为 20 秒或 1 分钟左右，双方通过发送“心跳”包来检测对方是否正常，连续丢失多个心跳包后，IPSec DPD 会强制重新发起 SA 协商。

WEB UI 方式下，在 **VPN 配置—>IPSec** 的**高级选项**中，可通过选中“DPD”选项来启用 DPD 功能，可通过配置“心跳”来确定检测周期。

13.2.1.3 IPSec NAT穿透

由于历史的原因，部署 NAT 模式下的 IPSec VPN 网络的问题之一在于无法定位网络地址转换（NAT）之后的 IPSec 对话方。Internet 服务提供商和小型办公/家庭办公（SOHO）网络通常使用 NAT 共享单个公共 IP 地址。虽然 NAT 有助于节省剩余的 IP 地址空间，但是它们也给诸如 IPSec 之类的端对端协议带来了问题。

在 NAT 对 IPSec 造成中断的众多原因中，主要的一个原因就是，对于“封装安全性协议（ESP）”来说，NAT 设备不能识别端口转换的 Layer 4（第 4 层）包头的位置（因为它已被加密）。对于“认证包头（AH）”协议来说，NAT 设备能修改端口号，但不能修改认证检查，于是对整个 IPSec 封包的认证检查就会失败。

一种称为 IPSec NAT 穿透（NAT-T）的新技术正在由 Internet 工程任务组的 IPSec 网络工作组标准化。

在 IPSec 协商过程中，可根据以下两个条件自动确定支持 IPSec NAT-T 的对话双方：

- 发起 IPSec 对话的一方（通常是一个客户端计算机）和响应 IPSec 对话的一方（通常是一个服务器）是否都能执行 IPSec NAT-T。
- 它们之间的路径中是否存在任何 NAT。

如果这两个条件同时为真，那么双方将使用 IPSec NAT-T 来通过 NAT 发送受 IPSec 保护的流量。如果其中一方不支持 IPSec NAT-T，则执行常规的 IPSec 协商（在前两个消息之后）和 IPSec 保护。如果双方都支持 IPSec NAT-T，但是它们之间不存在 NAT，则执行常规的 IPSec 保护。

提示：IPSec NAT-T 是仅为 ESP 流量定义的，AH 流量无法穿过 NAT 设备。

设备可以应用 NAT 穿透 (NAT-T) 功能。NAT-T 在第一阶段交换过程中，沿着数据路径检测

发现存在一个或多个 NAT 设备后，将添加一层 UDP 封装（通常使用 UDP4500 端口），从而通过 NAT 设备。

WEB UI 方式下，在 **VPN 配置—>IPSec** 的**高级选项**中，可通过选中 **NAT 穿透**选项来启用 NAT 穿透功能。

13.2.2　IPSec信息列表

进入 **VPN 配置—>IPSec** 页面，能查看相关的 IPSec 隧道信息，如 SA 状态、远端网关地址、远端内网地址、本地绑定的接口等。

图 13-14 IPSec 信息列表

提示：当 IPSec 的连接方式为**对方动态连接到本地**时，**建立**按钮无效。

13.2.3　IPSec配置

IPSec 支持的三种连接方式，分别为：网关到网关、动态连接到网关、对方动态连接到本地。下面分别介绍着三种连接方式配置参数的含义。

当 IPSec 隧道一端是动态 IP 接入（未申请 DDNS）时，隧道两端需使用**动态连接到网关**、**对方动态连接到本地**的连接方式。其中动态 IP 接入的一端选用**动态连接到网关**接入方式，作为发起方，另一端则选用**对方动态连接到本地**接入方式，做为响应方。

13.2.3.1 网关到网关

图 13-15 网关到网关

- 连接方式：这里选择网关到网关。

远端

- 网关地址（域名）：IPSec 隧道远端网关的地址（或域名），设置为域名时，需要在设备上设置 DNS 服务器，此时设备会定期解析该域名，如果 IP 地址发生变化，设备将重新协商 IPSec 隧道。
- 内网地址：IPSec 隧道远端受保护的内网的任一 IP 地址，如果远端是移动单机用户，则填写该设备的 IP 地址。
- 内网掩码：IPSec 隧道远端受保护的内网的子网掩码，如果远端是移动单机用户，则填写 255.255.255.255。

本地

- 本地绑定：选择本地接口的类型，接口可以是以太网口或 PPTP 拨号接口。如果将 IPSec 隧道配置为绑定到该接口上，那么所有经过该接口的数据包将通过 IPSec 检查，以确定是否对该数据包进行加密和解密操作。
- 内网地址：本地受保护的内网的任一 IP 地址。
- 内网掩码：本地受保护内网的子网掩码。

安全选项：

- 预共享密钥：协商所用的预共享密钥，最长为 128 个字符。

- 加密认证算法 1：可供第二阶段协商使用的首选加密认证算法。

图 13-16 IPSec 高级选项——主模式

第一阶段

- 协商模式：设置第一阶段的协商模式，可选项有主模式和野蛮模式。当连接方式选择网关到网关时，请选择主模式。当连接方式为动态连接到网关、对方动态连接到本地时，请选择野蛮模式。
- 生存时间：设置 IKE SA 的生存时间，至少 600 秒，当剩余时间为 540 秒时，将重新协商 IKE SA。
- 加密认证算法（1-4）：设置第一阶段协商使用的加密认证算法，可以选择四组，每组为不同的加密算法、认证算法及 DH 组的组合。

第二阶段

- 加密认证算法（2-4）：设置第二阶段协商使用的加密认证算法，可选三组，加上在基本参数配置中已配置的一组，共四组。

- 生存时间：设置 IPSec SA 的生存时间，至少 600 秒，当剩余时间为 540 秒时，SA 将过期，重新协商 IPSec SA。

其他

- 抗重拨：设置是否启用抗重播。启用后，网关将支持抗重播功能，从而可以拒绝接收过的数据包或数据包拷贝，以保护自己不被攻击。
- DPD：设置是否启用 DPD。启用后，在 SA 的生存时间内，设备定期发送心跳包检测对方网络是否可达，程序是否正常，如果连续丢失多个心跳包，则 IPSec DPD 会强制重新发起 SA 协商。
- 心跳：设置发送心跳包的时间间隔，默认值为 20 秒。配置该值后，网关会每隔单位时间（“心跳”）向对端发送探测消息，来确定对端是否还存活。
- NAT 穿透：启用或取消 NAT 穿透功能。
- 端口：设置 NAT 穿透时 UDP 封装包的端口号，缺省值 4500。
- 维持：启用 NAT 穿透功能后，设备将每隔单位时间（“维持”）向 NAT 设备发送一个数据包以维持 NAT 映射，这样就不需要更改 NAT 映射，直到第一阶段和第二阶段的 SA 过期，默认值为 20 秒。

13.2.3.2 动态连接到网关

图 13-17 动态连接到网关

在**网关到网关**连接方式中介绍过的参数，这里不再一一介绍。

- 连接方式：这里选择动态连接到网关。在这种情况下，在建立 IPSec 隧道时本设备只能作为发起方，且 IPSec 隧道两端都应该选择野蛮模式进行第一阶段的 IKE 协商。

远端

- 身份 ID：设置用于认证远端的身份 ID。
- 身份类型：远端身份 ID 的类型，有 Email 地址、 域名及 IP 地址三个选项。

本地

- 身份 ID：本地发送给远端认证的身份 ID。
- 身份类型：本地身份 ID 的类型，有 Email 地址、 域名及 IP 地址三个选项。

13.2.3.3 对方动态连接到本地

图 13-18 对方动态连接到本地

对方动态连接到本地的参数在前两节已经介绍过，这里不再一一复述。选择**对方动态连接到本地**时，远端的网关地址（域名）无需配置。在这种情况下，在建立 IPSec 隧道时本设备只能作为响应方，且 IPSec 隧道两端都应该选择野蛮模式进行第一阶段的 IKE 协商。

13.2.4 IPSec配置实例

13.2.4.1 网关到网关

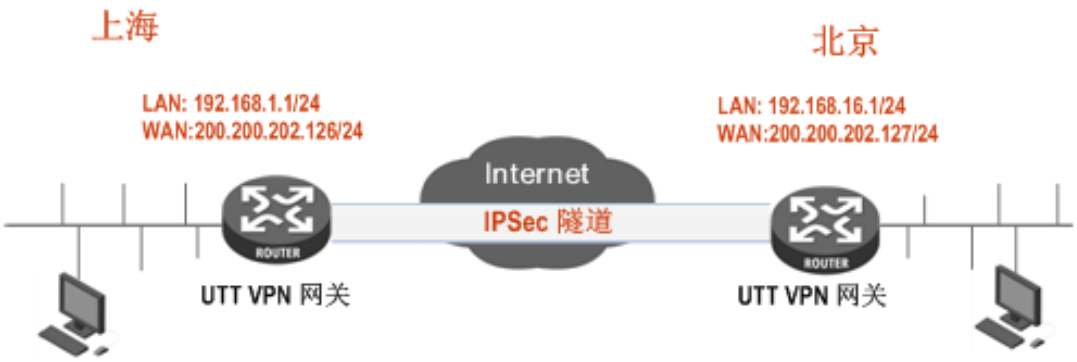


图 13-19 网关到网关拓扑图

需求：

在本方案中，某公司总部在上海。在北京有一个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 IPSec 协议建立 VPN 隧道，两地的 VPN 网关都使用艾泰路由器，地址如下：

上海网关：

内网网段：192.168.1.0/24。

LAN 口 IP 地址：192.168.1.1/24。

WAN1 口域名：200.200.202.126/24。

北京网关：

内网网段：192.168.16.0/24。

LAN 口 IP 地址：192.168.16.1/24。

WAN1 口 IP 地址：200.200.202.127/24。

配置步骤如下：

1） 配置上海网关

图 13-20 网关到网关配置 1

远端网关地址设置为北京网关的 WAN 口 IP 地址 200.200.202.127，远端内网地址为北京网关的 LAN 口 IP 地址 192.168.1.1，本地绑定在 WAN1 口，设置第一阶段的预共享密钥为 testing，第二阶段的加密认证算法为 esp-ase-128。

2) 配置北京网关

图 13-21 网关到网关配置 2

远端网关地址设置为上海网关的 WAN 口 IP 地址 200.200.202.126，远端内网地址为上海网关的 LAN 口 IP 地址 192.168.16.1，本地绑定在 WAN1 口，设置第一阶段的预共享密钥为 testing，第二阶段的加密认证算法为 esp-ase-128。

查看连接状态：

分别进入相应页面，查看其 IPSec 实例连接信息。如下图所示可以查看 IPSec 实例的 SA 状态、远端网关、远端内网、本地绑定接口等信息。

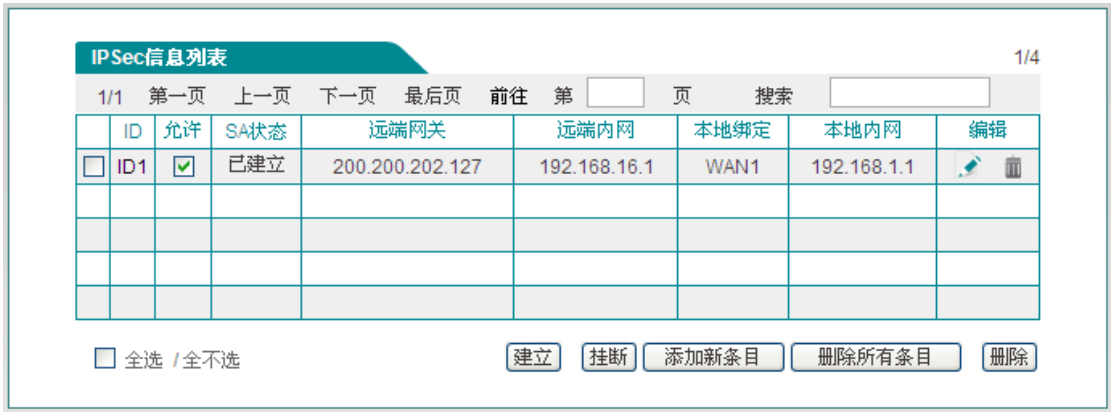


图 13-22 IPSec 连接状态—上海网关

图 13-23 IPSec 连接状态—北京网关

13.2.4.2 一方动态

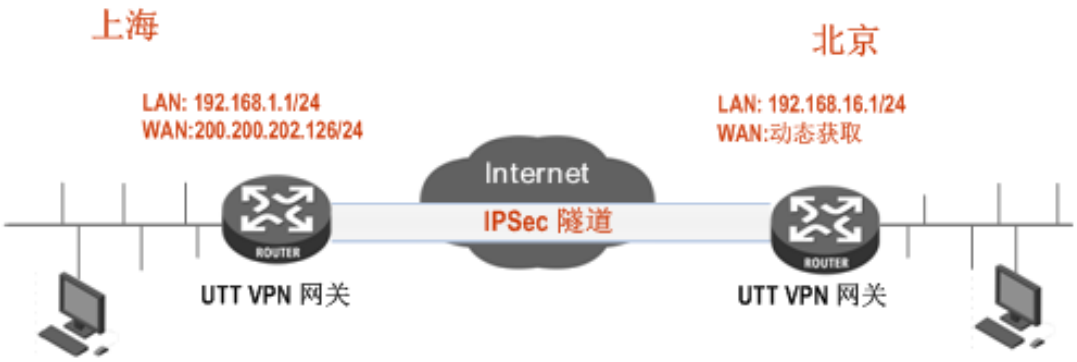


图 13-24 一方动态拓扑图

需求：

在本方案中，某公司总部在上海。在北京有一个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 IPSec 协议建立 VPN 隧道，两地的 VPN 网关都使用艾泰路由器，地址如下：

上海网关：

内网网段：192.168.1.0/24。

LAN 口 IP 地址：192.168.1.1/24。

WAN1 口域名：200.200.202.126/24。

北京网关：

内网网段：192.168.16.0/24。

LAN 口 IP 地址：192.168.16.1/24。

WAN1 口 IP 地址：动态获取。

配置步骤如下：

1） 配置上海网关

图 13-25 一方动态—对方动态连接到本地

设置连接方式为对方动态连接到本地，北京网关动态连接到上海网关。同时设置北京网关相

关信息，如内网地址、身份 ID。本地绑定在 WAN1 口，设置第一阶段的预共享密钥为 testing，第二阶段的加密认证算法为 esp-ase-128。

2) 配置北京网关

图 13-26 一方动态—动态连接到网关

设置北京网关的连接方式为动态连接到网关。同时设置上海网关相关信息，如网关地址、内网地址、身份 ID。本地绑定在 WAN1 口，设置第一阶段的预共享密钥为 testing，第二阶段的加密认证算法为 esp-ase-128。

查看连接状态：

图 13-27 IPSec 连接状态—对方动态连接到本地

图 13-28 IPSec 连接状态—动态连接到网关

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

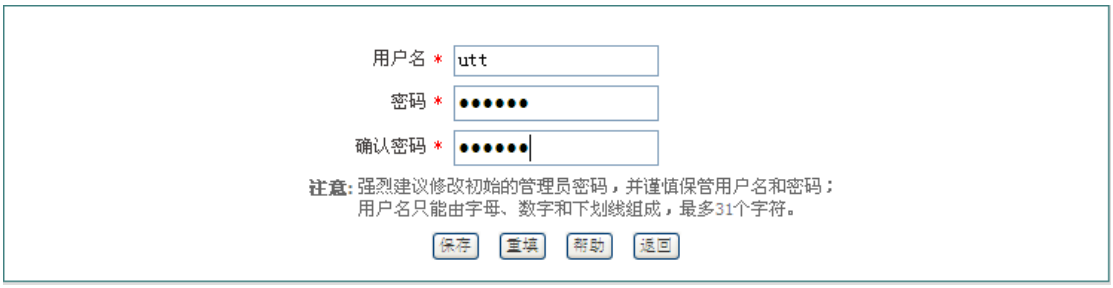


图 14-2 管理员配置

- 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密码。修改后，您必需使用新的密码登录设备。

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。

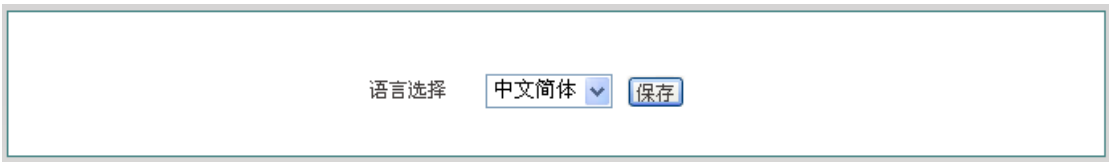


图 14-3 语言选择

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 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 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

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。

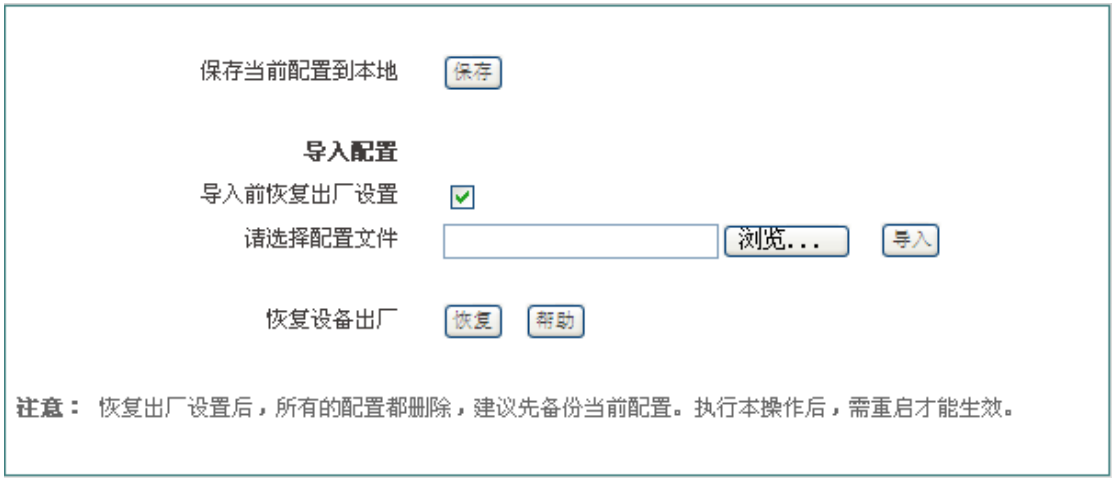


图 14-5 配置管理

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。

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。

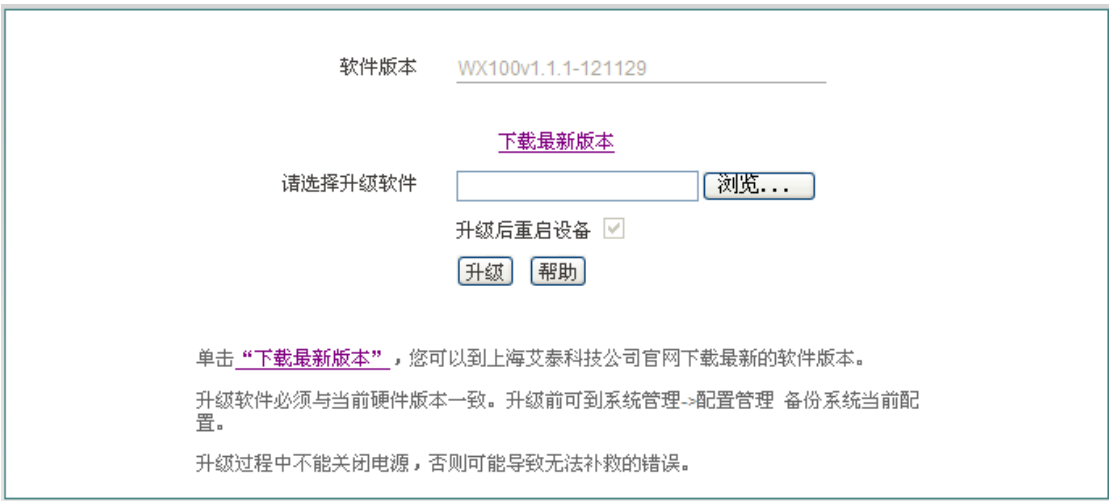


图 14-6 软件升级

- 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

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。

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。

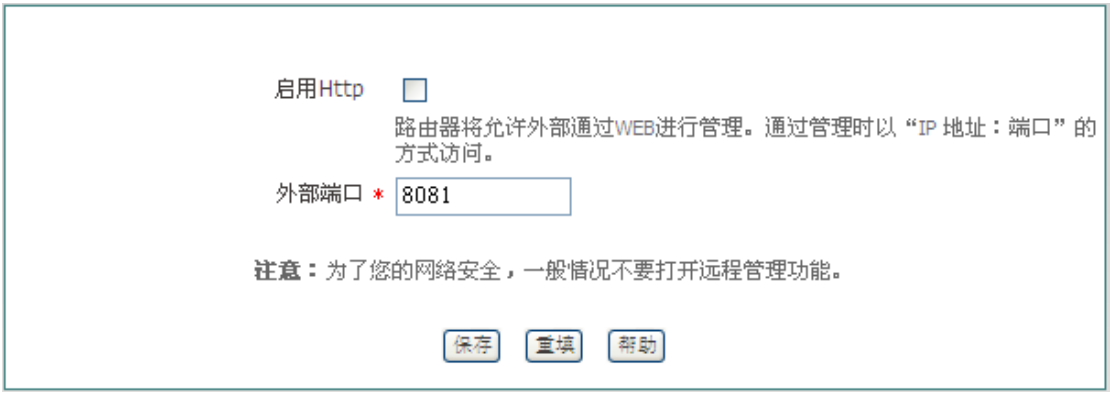


图 14-7 远程管理

- 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。

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。

14.8　ping诊断

本节介绍**系统管理—>ping 诊断**页面。Ping（Packet Internet Grope ），即因特网包探索器，一般用于检测网络通不通，用于测试网络连接量的程序。Ping 发送一个 ICMP 回声请求消息给目的地并报告是否收到所希望的 ICMP 回声应答。

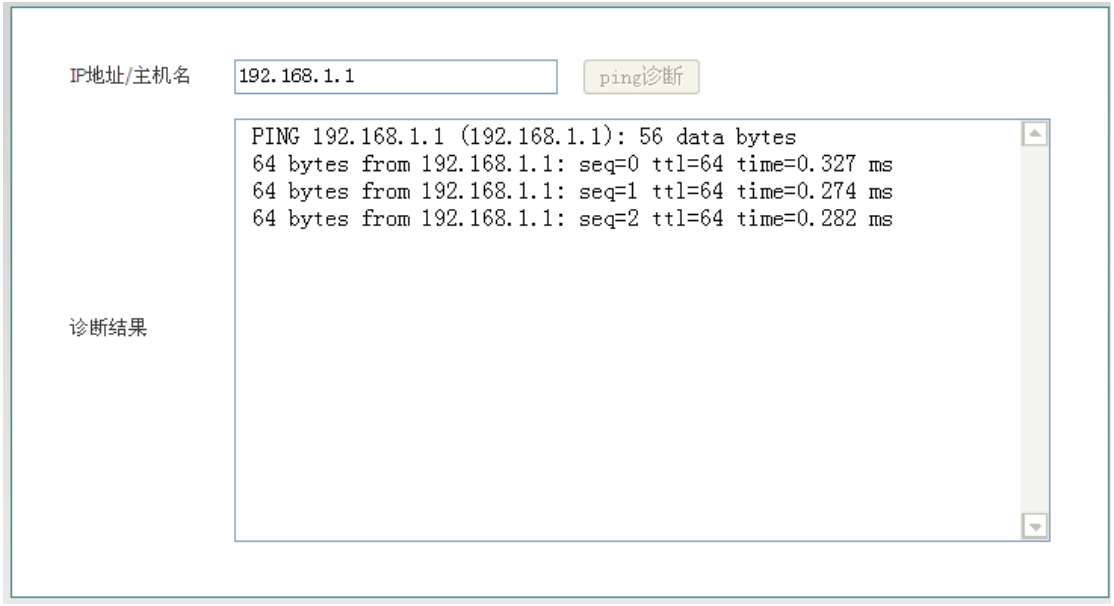


图 14-11 ping 诊断

- ping 通信检测：输入需要检测的目的 IP/域名，点击开始。可对该地址/域名进行检测。

第15章　系统状态

在系统状态中，您可以查看设备的相关系统信息及历史记录。

15.1　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。详情请参阅章节：运行状态。。

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与增强网络安全。

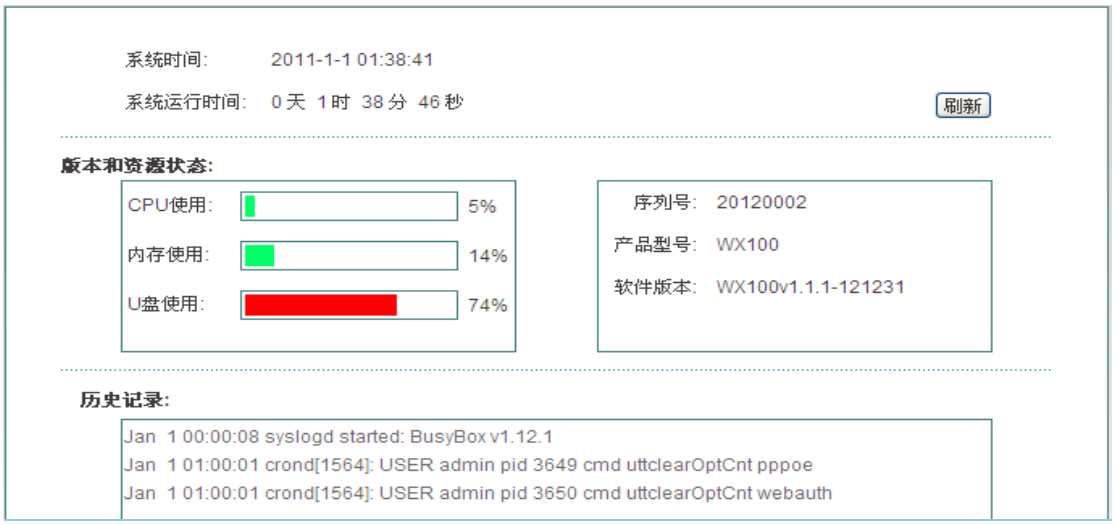


图 15-1 系统信息

- 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。
- U 盘使用：显示当前设备所接 U 盘的使用百分比。
- 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 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。

15.3　系统日志

通过**系统状态—>系统日志**页面，网络管理员能查看系统相关的日志信息，以及对日志管理进行相关的配置。

15.3.1　系统日志信息

通过**系统状态—>系统日志—>系统日志信息**页面，查看系统记录的相关信息，如下图所示。

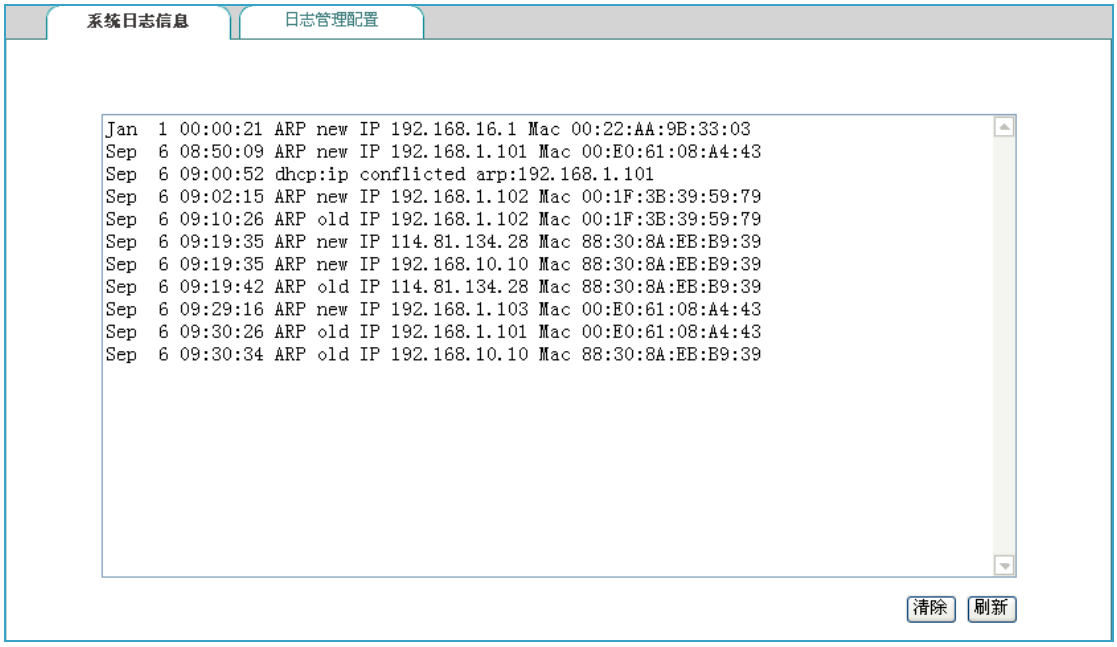


图 15-2 系统信息

设备常显示的日志信息如下：

日志内容	详细	信息含义
DHCP:IP conflicted	arp:[IP 地址]	表示 DHCP 地址冲突：设备的 DHCP Server 在准备分配该 IP 地址给某用户时，发现在内网中已存在该 IP 地址，系统会再次分配其他 IP 地址给用户。

ARP	Spoof mac [MAC 地址] New IP [IP 地址] mac[MAC 地址] Old IP [IP 地址] mac[MAC 地址]	表示网关地址欺骗。 MAC 地址表重新学习到一个新的 MAC 地址。 MAC 地址超时老化。
PPPoE	Local IP address [IP 地址] Primary DNS address [主 DNS 地址] Secondary DNS address[备份 DNS 地址]	PPPoE 拨号下发的 IP 地址。 PPPoE 拨号下发的主 DNS 地址。 PPPoE 拨号下发的备份 DNS 地址。
notice	Give notice to user:[IP 地址]	推送通告信息至这个 IP 地址。

表 15-1 日志信息

15.3.2　日志管理设置

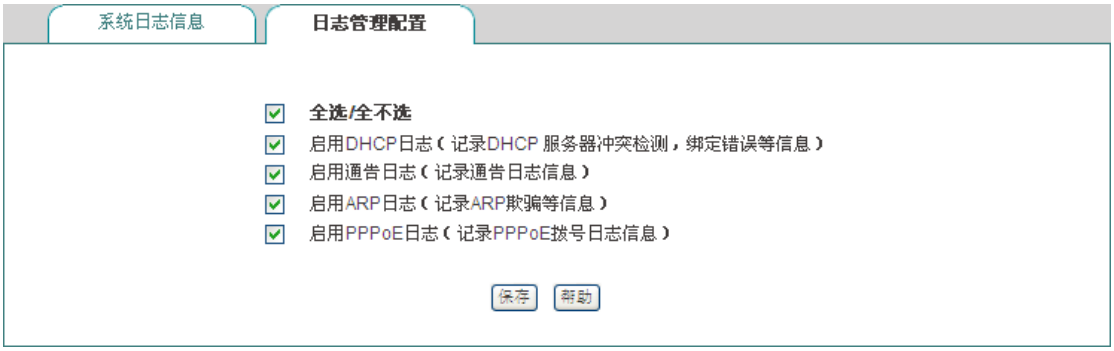


图 15-3 日志管理设备

- 启用 DHCP 日志：勾选表示启用 DHCP 日志，记录 DHCP 服务器冲突，以及 DHCP 分配地址冲突等信息。
- 启用通告日志：勾选表示启用通告日志，记录通告日志信息。
- 启用 ARP 日志：勾选表示启用 ARP 日志，记录 ARP 欺骗等信息。
- 启用 PPPoE 日志：勾选表示启用 PPPoE 日志，记录 PPPoE 拨号日志信息。

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 16-1 客户服务

在上图中，单击各个**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. 单击**开始**>**控制面板**。
2. 双击**网络连接**图标，右键单击**本机连接**，选择**属性**。在本地连接属性中**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：

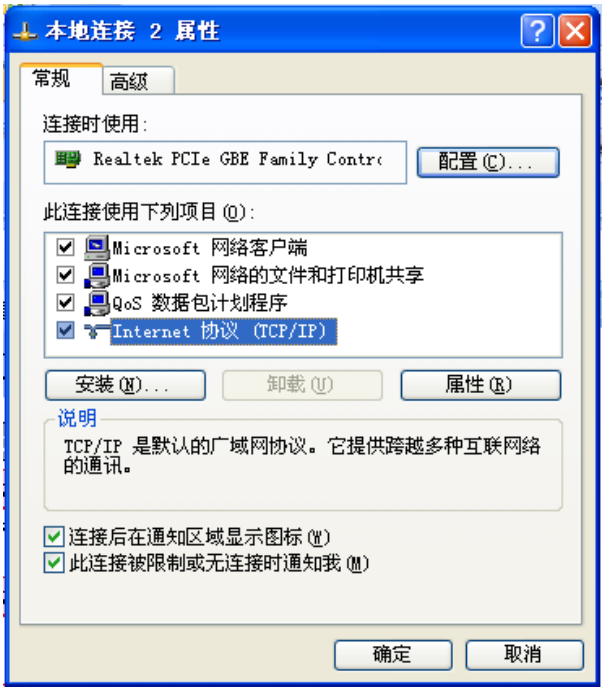


图 A- 1 网络配置窗口

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（R）**按钮，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. 单击**开始**>**控制面板**。
2. 双击**网络连接**图标，右键单击**本机连接**，选择**属性**，进入**本地连接属性**窗口，如图 A-1

所示，在**此连接使用下列项目** 选择 Internet 协议（TCP/IP）选项，再单击**属性**按钮。

3. 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。

4. 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**按钮，TCP/IP 属性配置成功。

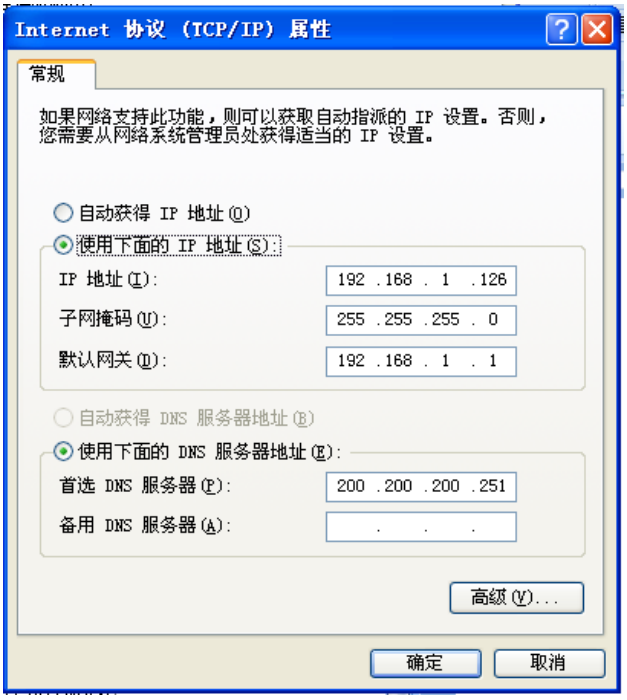


图 A- 2 TCP/IP 属性 IP 地址配置窗口

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**中激活 DHCP Server 功能。

2. 单击**开始>控制面板**。

3. 双击**网络连接**图标，右键单击**本机连接**，选择**属性**，进入**本地连接属性**窗口，如图 A-1 所示，在**此连接使用下列项目**选择 Internet 协议（TCP/IP）选项，再单击**属性**按钮。

4. 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**自动获得 IP 地址**和**自动获得 DNS 服务器地址**。

5. 以上配置完成后，单击**确定**按钮，配置 TCP/IP 属性完成。

附录B FAQ

问： 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 上网线路相关参数。
5. 如果是包月上网的用户，则可选择拨号类型为**自动拨号**。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. 按照本手册附录 A 所述内容配置局域网计算机。

问： 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。

问： 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. 在**网络参数—>WAN 口配置**的线路连接信息列表中，可以查看动态 IP 接入时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，并显示连接时间）、ISP 分配的 IP 地址、上行速率和下行速率等信息。

图 B- 2 线路连接信息列表——查看动态 IP 接入线路信息

5. 按照本手册附录 A 所述内容配置局域网计算机。

问： 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
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