宽带网关
高级配置手册

Rev：2.5.3

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

目　录

导　读 1
0.1 手册说明 1
0.2 界面风格 1
0.3 基本约定 2
0.4 出厂配置 2
0.5 联系我们 3
0.6 关键特性 3
0.7 规格 4
第 1 章 硬件安装 5
1.1 面板介绍 5
1.2 安装注意事项 6
1.3 安装准备 6
1.4 硬件安装 7
1.5 硬件连接 8
第 2 章 登录设备 9
2.1 配置正确的网络设置 9
2.2 登录设备 10
第 3 章 配置向导 12
3.1 语言选择 12
3.2 WAN1 口配置——动态 IP 接入 12
3.3 WAN1 口配置——固定 IP 接入 13
3.4 WAN1 口配置——PPPoE 接入 13
3.5 2.4G 无线参数配置 14
3.6 5G 无线参数配置 15
第 4 章 开始菜单 16
4.1 配置向导 16
4.2 运行状态 16
4.3 端口流量 16
4.4 重启设备 17
第 5 章 网络参数 18
5.1 WAN 口配置 18
5.2 线路组合 23

5.3 LAN 口配置.....27
5.4 VLAN 接口配置.....27
5.5 DHCP 服务器.....29
5.6 DDNS 配置.....41
5.7 UPnP.....45
5.8 WAN 口数量配置.....46
第 6 章 无线配置.....47
6.1 2.4G 基本配置.....47
6.2 2.4G 无线配置实例.....48
6.3 5G 基本设置.....50
6.4 无线安全设置.....53
6.5 无线 MAC 地址过滤.....56
6.6 无线高级配置.....57
6.7 无线主机状态.....58
第 7 章 高级配置.....60
7.1 NAT 和 DMZ 配置.....60
7.2 路由配置.....67
7.3 策略路由.....68
7.4 DNS 重定向.....71
7.5 网络尖兵防御.....72
7.6 即插即用.....73
7.7 端口镜像.....73
7.8 端口 VLAN.....74
7.9 SNMP 配置.....76
7.10 SYSLOG 配置.....77
第 8 章 网络共享.....78
8.1 网络共享管理.....78
8.2 FTP 服务器.....79
8.3 共享账户.....81
第 9 章 用户管理.....83
9.1 用户状态.....83
9.2 IP/MAC 绑定.....85
9.3 PPPoE 服务器.....89
9.4 WEB 认证.....96

9.5 用户组配置 106
9.6 服务组配置 106
第 10 章 行为管理 109
10.1 时间段配置 109
10.2 上网行为管理 110
10.3 QQ 白名单 113
10.4 MSN 白名单 114
10.5 阿里旺旺白名单 114
10.6 电子通告 115
10.7 上网行为审计 117
10.8 策略库 119
第 11 章 带宽管理 121
11.1 精细化限速 121
11.2 弹性带宽 122
11.3 P2P 限速 123
11.4 连接数限制 124
第 12 章 防火墙 126
12.1 安全配置 126
12.2 访问控制策略 127
12.3 域名过滤 136
12.4 MAC 地址过滤 138
第 13 章 VPN 配置 141
13.1 PPTP 141
13.2 L2TP 150
13.3 IPSec 154
第 14 章 系统管理 171
14.1 管理员配置 171
14.2 语言选择 172
14.3 时钟管理 172
14.4 配置管理 173
14.5 软件升级 173
14.6 远程管理 175
14.7 计划任务 175
第 15 章 系统状态 177

15.1 运行状态 177
15.2 系统信息 177
15.3 系统日志 178
第 16 章 客户服务 180
附录 FAQ 181

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 8.0 以上版本。

0.1　手册说明

本手册适用艾泰科技宽带网关产品。

本手册描述应用于艾泰科技 ReOS_SE 软件平台产品的特性和功能，提供基于 WEB 界面的配置方法及其步骤，各型号的路由器功能模块有所不同，具体功能以产品为准。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。

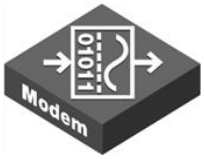
下拉框　：通过下拉框可以找到供选择的选项。

0.3　基本约定

1）　**图标约定**

路由器

交换机



Modem

服务器

终端

无线主机

2）　**符号约定**

表示界面参数，按钮等内容含义的解释。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。

- 表示列举并列关系的内容。

粗体字：表示界面语言。

0.4　出厂配置

1）　接口的出厂配置如下表所示。

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

表 0- 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

0.6 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
- 支持智能带宽管理功能
- 支持精细化限速
- 支持 DHCP 服务器功能
- 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
- 支持端口镜像
- 支持用户组、时间段管理
- 支持 VPN 功能
- 支持 UPnP
- 支持动态域名（3322.org、iplink.com.cn）
- 支持 HTTP 远程管理
- 支持 WEB 升级方式
- 支持 WEB 配置文件备份与导入

- 支持 DNS 重定向

提示：

艾泰科技宽带网关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。

0.7　规格

- 符合 IEEE802.3Ethernet 以及 IEEE802.3u Fast Ethernet 标准。
- 支持 TCP/IP、DHCP、ICMP、NAT、PPPoE、静态路由等协议。
- 各个物理端口均支持自动协商功能、支持 MDI/MDI-X 正反线自适应。
- 提供状态指示灯。
- 工作环境：温度：0-40℃ 高度：0-4000m

  相对湿度：10-90%，不结露

第 1 章　硬件安装

1.1　面板介绍

此处以 9 寸的商睿™821 为例进行说明，其它系列产品的面板以实物为准，这里不再一一列出。如图 2-1、2-2 所示为商睿™ 821 的前面板、后面板示意图。

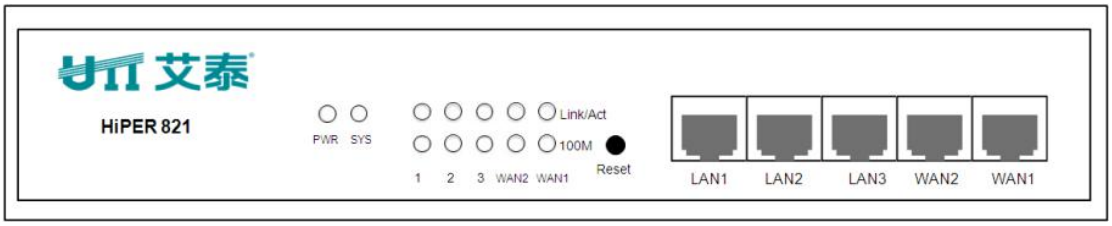


图 1- 1 前面板示意图—商睿™ 821

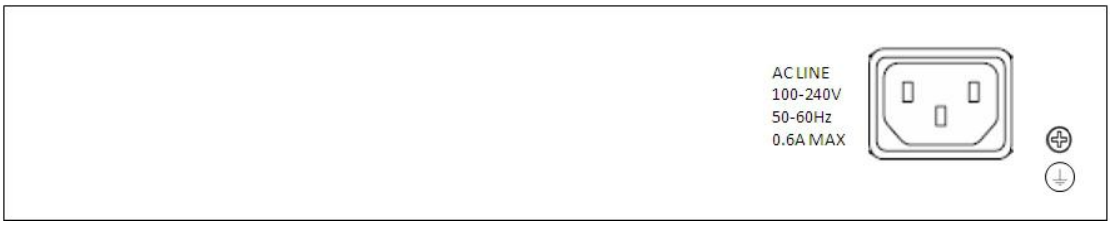


图 1- 2 后面板示意图—商睿™ 821

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。
100M	端口速率指示灯	当有设备连接到某端口，且 100M 协商成功后，该端口对应指示灯常亮。

表 1- 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。 部分产品仅提供一个 LAN 端口。	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。	
Console	串口	符合 RS232 标准的异步通信串口	部分产品支持 Console 口。

表 1- 2 接口说明

3） Reset 按钮

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

提示：上述操作会删除设备原来的所有配置，请谨慎使用。

1.2 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。

1.3 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。

(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。

1.4 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

将设备放置在平稳的工作台上，安装步骤如下（部份产品脚垫已粘于主机上）：

(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。

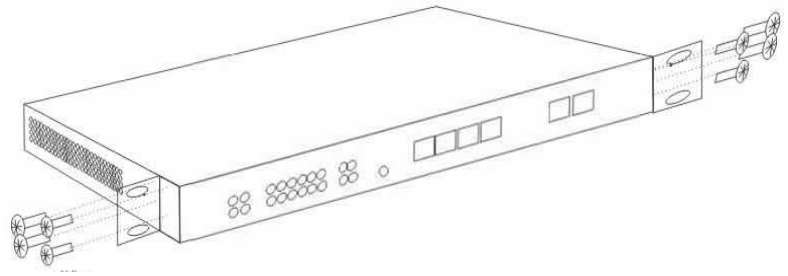


图 1- 3 产品机架安装图一

(3) 将设备安放在机架内适当的位置，由托架支撑。

(4) 用螺钉将 L 型支架固定在机架两端固定的导槽上（如下图所示）。

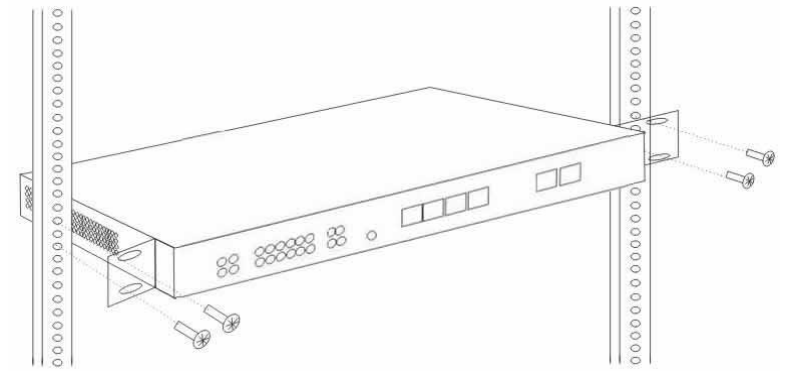


图 1- 4 产品机架安装图二

1.5 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或集线器或交换机。

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。

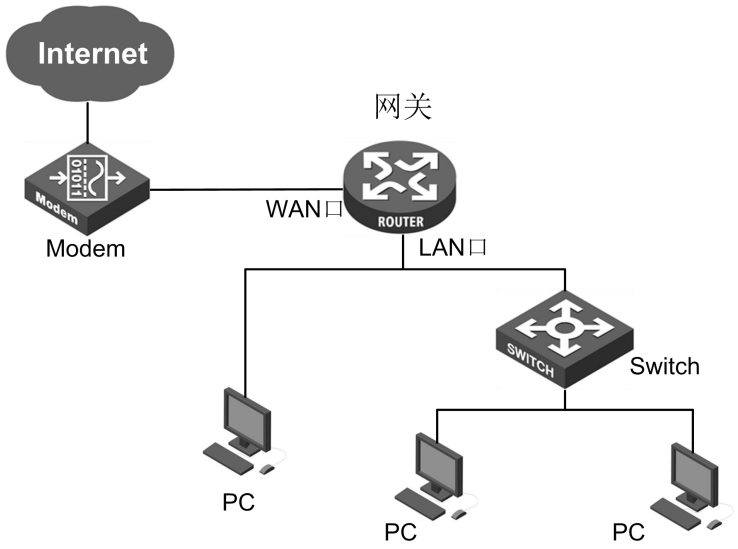


图 1- 5 建立到局域网和广域网的连接

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构架。

第 2 章　登录设备

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

2.1　配置正确的网络设置

在通过 WEB 界面登录到设备之前，您必须对内网计算机进行正确的网络设置。

首先将计算机连接到设备的 LAN 口，接下来设置计算机的 IP 地址。

第一步，设置计算机的 TCP/IP 协议，如果已经正确设置，请跳过此步。设置计算机的 IP 地址。您可以使用以下两种方法：

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

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

第二步，在计算机上使用 Ping 命令检查其是否与设备连通。通过**开始—>运行**，输入 **cmd**，点击**确定**，打开命令窗口。输入 **ping 192.168.1.1**。

下面列举在 Windows XP 环境中执行 Ping 命令的两种结果：

如果屏幕显示如下，表示计算机已经成功和设备建立连接。

```
Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:

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

如果屏幕显示如下，表示计算机和设备连接失败。

```
Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Ping statistics for 192.168.1.1:

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

连接失败时，请做以下检查：

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

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

2.2 登录设备

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

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

图 2- 1 WEB 登录界面

首次登录，系统提示修改登录密码，如下图所示。点击 明文显示密码。

图 2- 2 WEB 界面首页

修改密码保存后，浏览器将显示 WEB 管理界面的首页。

图 2- 3 WEB 界面首页

首页相关说明：

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

   (1) **产品讨论**——链接到艾泰科技官方网站的讨论区，参与产品的讨论。

   (2) **知识库**——链接到艾泰科技官方网站的知识库，查找相关技术资料。

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

2) 该页面左侧显示主菜单条。

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

第 3 章　配置向导

通过阅读本章内容，可以了解设备上网所需的基本网络参数，通过配置这些参数将设备连接到 Internet。在进入配置向导配置上网线路之前，应正确配置内网计算机的网络设置，详情请参阅章节：配置正确的网络设置。

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。

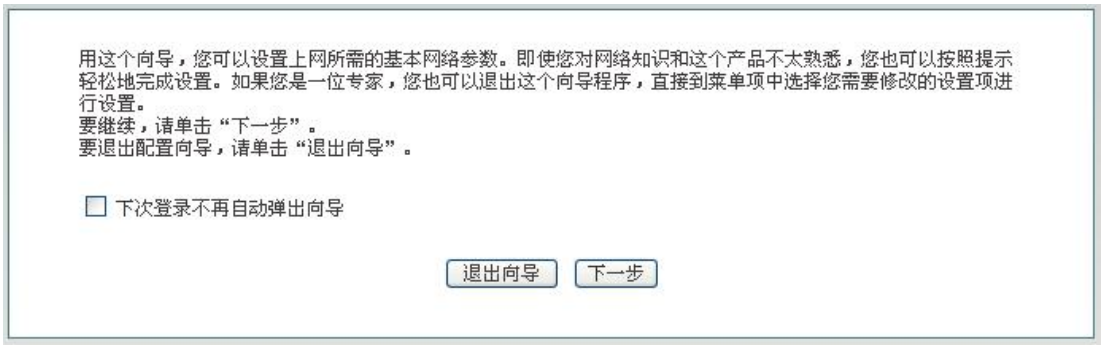


图 3- 1 配置向导首页

- 下次登录不再自动弹出向导：选中后，在下次登录时直接进入**系统状态**页面。
- 退出向导：退出配置向导，返回到**系统状态**页面。
- 下一步：进入语言选择页面。

3.1　语言选择

选择系统语言。

图 3- 2 语言选择

3.2　WAN1 口配置——动态 IP 接入

由于大多数上网用户的上网时间和空间的离散性，ISP 为每个用户分配一个固定的 IP 地址（静态 IP），会造成 IP 地址资源的极大浪费，因此这些用户通常会在每次拨通 ISP 的主机后，自动获得一个动态的 IP 地址， 拨号用户任意两次连接时的 IP 地址很可能不同，但是在每次连接时间内 IP 地址不变。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**下一步**。

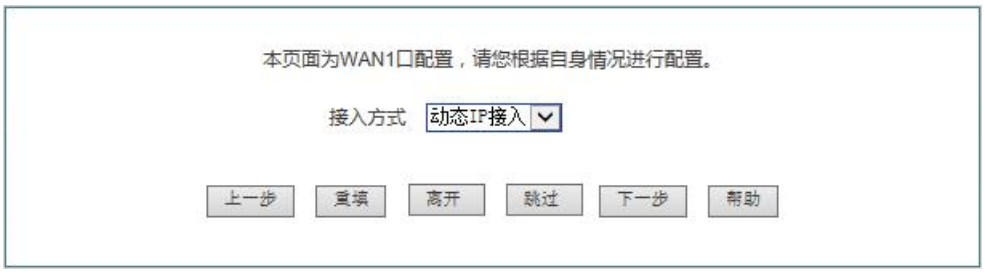


图 3- 3 动态 IP 接入

3.3 WAN1 口配置——固定 IP 接入

设立了因特网服务的组织机构，其主机对外开放了诸如 WWW 、FTP 、E-mail 等访问服务，通常需要对外公布一个固定的 IP 地址，以方便用户访问。此固定 IP 地址需要向 ISP 申请。

图 3- 4 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。

3.4 WAN1 口配置——PPPoE 接入

PPPoE 全称 Point to Point Protocol over Ethernet，是基于以太网的点对点协议。该协议具有用户认证及通知 IP 地址的功能，是在以太网络中转播 PPP 帧信息的技术，尤其适用于 ADSL 等方式。如果您的上网线路接入方式为 PPPoE 接入，请在如下图的下拉列表框中选择 PPPoE 接入。

图 3- 5 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**下一步**继续配置后续步骤直到点击**完成**，这样配置才会生效。

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

3.5 2.4G 无线参数配置

配置 2.4G 无线网络的参数。包括 SSID、无线模式、信道、频道带宽。各参数的含义详见章节：无线配置。点击**下一步**配置 5G 无线网络的参数。

图 3- 6 2.4G 无线参数配置

3.6 5G 无线参数配置

配置 5G 无线网络的参数。包括 SSID、无线模式、信道、频道带宽。各参数的含义详见章节：无线配置。

图 3- 7 5G 无线参数配置

第 4 章　开始菜单

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

4.1　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，详情请参阅章节：配置向导。

4.2　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 4- 1 运行状态信息

4.3　端口流量

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

提示：

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

图 4- 2 接口流量

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

4.4 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 4- 3 重启设备

提示：重启时，所有的用户将断开到设备的连接。

第 5 章　网络参数

在网络参数主菜单中可配置设备基本网络参数，包括 WAN 口配置、线路组合、LAN 口配置、DHCP 服务器、DDNS 配置、UPnP 和 WAN 口数量配置等。

5.1　WAN 口配置

本节主要讲述**网络参数—>WAN 口配置**的配置界面及方法。

在本页面不仅可以配置线路信息，也可以根据实际需要修改或删除已配置的线路，还可以查看线路的连接状态信息。在**配置向导**中配置完上网线路之后，可以到本页面查看该线路的连接状态和配置情况，也可根据需要修改配置。

5.1.1 网络接口配置

进入**网络参数—>WAN 口配置**页面，配置界面如下图所示。

图 5- 1 WAN 口配置

本节介绍如何配置上网线路。上网线路的连接类型有：动态 IP 接入、固定 IP 接入、PPPoE 接入。

1） 动态 IP 接入

如**错误！未定义书签。**所示，下面介绍动态 IP 接入的各参数的涵义。

- 接口：选择设备相应的接口。

- 接入方式：这里选择**动态 IP 接入**。
- 运营商策略 1/2/3：选择该接口的运营商，有四个可选项分别为运营商策略、电信、联通及移动线路。例如选择电信表示电信流量走该接口。
- 工作模式：上网方式。提供 NAT 模式和路由模式。
- MAC 地址：相应接口的 MAC 地址，一般无需修改。
- 接口模式：该接口的工作模式。Auto—自适应，1000MFD—1000M 全双工，100MFD—100M 全双工，100MHD—100M 半双工，10MFD—10M 全双工，10MHD—10M 半双工。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，可以在这里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

图 5- 2 固定 IP 接入

如**错误！未定义书签。**所示的界面为固定 IP 接入的配置界面。

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

- 工作模式：上网方式。提供 NAT 模式和路由模式，这里选择 NAT 模式。
- MAC 地址：该接口的 MAC 地址（一般情况下不需要修改）。
- 接口模式：该接口的工作模式。Auto—自适应，1000MFD—1000M 全双工，100MFD—100M 全双工，100MHD—100M 半双工，10MFD—10M 全双工，10MHD—10M 半双工。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，可以在这里设置以太网协商的类型。
- 网关绑定方式：网关绑定的方式，有不绑定、手工绑定类型。
- 网关 MAC 地址：绑定上层网关地址，选择手动绑定时可点击自动获取按钮获取网关 MAC，也可自己手动输入网关 MAC。

注意：当绑定错误的网关 MAC 时，上网功能会异常。

3） PPPoE 接入

图 5- 3 PPPoE 接入

如**错误！未定义书签。**所示的界面为 PPPoE 接入的配置界面。

- 接入方式：此处选择 PPPoE 接入，ADSL 虚拟拨号（也可以是以太网介质的 PPPoE 拨号），设备将通过拨号获取 IP 地址、子网掩码以及网关地址信息。
- 用户名、密码：在运营商办理业务时，运营商提供的用户名及密码。
- 密码验证方式：ISP 验证用户名及密码的方式，默认为 EITHER。多数地区为 PAP 方式，也有少数地区采用 CHAP 方式，NONE 表示不进行用户名和密码验证，EITHER 表示自动和对方设备协商采用哪种验证方式。
- 拨号类型：

- 自动拨号：当打开设备或者上一次拨号断线后自动拨号连接。
- 手动拨号：由用户在**网络参数—>WAN 口配置**的线路连接信息列表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。
- 工作模式：上网方式。提供 NAT 模式和路由模式。
- MAC 地址：相应接口的 MAC 地址，一般无需修改。
- 接口模式：接口模式：该接口的工作模式。Auto—自适应，1000MFD—1000M 全双工，100MFD—100M 全双工，100MHD—100M 半双工，10MFD—10M 全双工，10MHD—10M 半双工。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，可以在这里设置以太网协商的类型。

5.1.2 线路连接信息列表

在**线路连接信息列表**中可以查看各线路的配置及状态信息。

图 5- 4 线路连接信息列表

图 5- 5 线路连接信息列表（续错误！未定义书签。）

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

- 连接状态：线路的当前连接状态，当连接不成功或未连接时显示**断开**，当连接成功时则显示**已连接**，对于动态 IP 接入及 PPPoE 接入连接成功时还会显示保持本次连接的时间（单位：小时:分:秒）。
- IP 地址、子网掩码、网关地址：分别为 ISP 提供的广域网接口的 IP 地址、子网掩码及网关地址。
- 下行速率、上行速率：在两次刷新列表的时间间隔内，当前线路实际的下/上行平均速率。单位为 KB/s。

1） PPPoE 接入线路的拨号与挂断

如果某线路为 PPPoE 接入，那么，在点击该接口后，在**线路连接信息列表**下方才会显示**拨号**和**挂断**按钮，如图 5-4 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 5- 6 线路连接信息列表——PPPoE 接入

2） 动态 IP 接入线路的更新与释放

如果某线路为动态 IP 接入线路，那么在点击该接口后，在**线路连接信息列表**下方才会显示**更新**和**释放**按钮。

图 5- 7 线路连接信息列表——动态 IP 接入

- 更新：系统自动完成一次先释放 IP 地址、再重新获得 IP 地址的过程。
- 释放：释放当前得到的动态 IP 地址。

5.2 线路组合

本节介绍**网络参数—>线路组合**页面。

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

5.2.1 线路组合功能介绍

1） 线路检测机制

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

为方便理解，先介绍一下几个相关参数。

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

检测次数：每个检测周期内，发送检测包的次数。

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

下面将分别介绍在线路正常和线路故障这两种情况下，设备的线路检测机制。

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

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

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

提示：允许不启用线路检测，这时需要将检测间隔设为 0 秒。

2）线路组合方式

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

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

在**所有线路负载均衡**方式下，所有线路都作为主线路使用。工作原理如下：

（1） 当所有线路都正常时，内网主机将同时使用所有线路上网。

（2） 若某条线路出现故障，则立即屏蔽该线路，原先通过该线路的流量将分配到其他线路上。

（3） 一旦故障线路恢复正常，设备会自动启用该线路，流量自动重新分配。

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

（1） 只要主线路正常，内网主机就使用主线路上网。

（2） 若主线路出现故障，则自动切换到使用备份线路上网。

（3） 一旦故障主线路恢复正常，则立即切换回主线路。

提示：

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

5.2.2 线路组合全局配置

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

1） 所有线路负载均衡

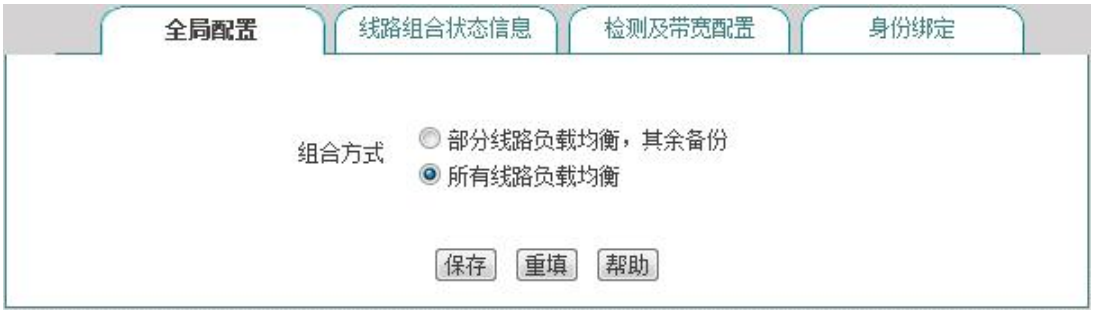


图 5- 8 所有线路负载均衡

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

提示：线路组合方式默认为**所有线路负载均衡**。

2） 部分线路负载均衡，其余备份

图 5- 9 部分线路负载均衡，其余备份

- 组合方式：这里选中**部分线路负载均衡，其余备份**。
- 主线路：该列表框代表主线路组，位于该列表框中的线路全部都作为主线路使用。
- 备份线路：该列表框中代表备份线路组，位于该列表框中的线路全部都作为备份线路使用。
- ==>（向右箭头）、<==（向左箭头）：首先在**主线路**列表框中选中一条（或更多）线路，然后单击==>，被选中的线路立即被移到**备份线路**列表框中。类似地，首先在**备份线路**列表框中选中一条（或更多）线路，然后单击<==，被选中的立即被移到**主线路**列表框中。
- 保存：线路组合配置参数生效。
- 重填：恢复到修改前的配置参数。

5.2.3 线路组合状态信息

在**网络参数—>线路组合—>线路组合状态信息**页面能查看和配置线路组合的相关信息。

图 5- 10 线路状态组合信息列表

- 编辑线路组合状态信息：单击该线路的接口或者该线路对应的**编辑**超链接，即可跳转到相关页面进行修改，如图 5-11 所示。
- 刷新：点击**刷新**，可获得最新的线路组合状态信息。

5.2.4 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—>线路组合状态信息**页面，单击某线路的接口或者是编辑图标，进入**检测及宽带配置**页面。

图 5- 11 线路组合配置

- 检测间隔：发送检测包的时间间隔，单位：秒。启用线路检测时，取值范围为 1～60，该值为 0 时，表示不启用线路检测。
- 检测次数：检测周期内发送检测包的次数（每次发送一个检测包）。缺省值为 0。
- 检测目标：欲检测的目标的 IP 地址。
- 带宽：设置 ISP 提供给当前线路的带宽。
- 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。

5.2.5 身份绑定

当设备为多 WAN 口时，可以进入**网络参数—>线路组合—>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 5- 12 启用身份绑定

- 启用身份绑定：启用/禁用身份绑定功能。如果配置了多线路，要使 QQ、网银等能正常使用，请开启设备的身份绑定功能。

5.3 LAN 口配置

设备默认 LAN 口的 IP 地址为 192.168.1.1，如果您需要修改 LAN 口的 IP 地址以适应现有的网络环境，请进入**网络参数—>LAN 口配置**页面修改 LAN 口参数，可以为设备设置多达四个 LAN 口 IP 地址。

图 5- 13 LAN 口配置

- IP 地址：设备内网的 IP 地址。
- 子网掩码：设备内网 IP 地址的子网掩码。
- MAC 地址：LAN 口的 MAC 地址。建议不要随意修改 LAN 口的 MAC 地址。
- 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-HD（1000M 半双工）、1000M-FD（1000M 全双工）。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，可以在这里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！

5.4 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 子接口访问设备。

5.4.1 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 5- 14 VLAN 接口列表

5.4.2 VLAN 接口配置

点击 VLAN 接口名称或**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 地址池中引用。

图 5- 15 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，可配置 64 条。
- IP 地址：设置 VLAN ID 的 IP 地址。
- 子网掩码：设置子网掩码。

5.5 DHCP 服务器

DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）是一个局域网的网络协议，用来给内部网络自动分配 IP 地址，对网络管理员来说，是对所有计算机作中央管理的手段。有 DHCP 服务器与 DHCP 客户端之区别， DHCP 服务器控制一段 IP 地址范围，当客户端连接到服务器时可以自动获得服务器分配的 IP 地址和子网掩码等信息。每次客户端连接服务器时所获得的 IP 地址可能不同。当一客户端下线后，DHCP 服务器会收回已分配的 IP 地址并分配给其它上线的客户端。这样可以有效节约 IP 地址，既保证了网络通信，又提高 IP 地址的使用率。

5.5.1 DHCP 单地址池

本节介绍**网络参数—>DHCP 服务器**页面，包括 DHCP 服务器设置、静态 DHCP、DHCP 自动绑定和 DHCP 客户端列表。

5.5.1.1DHCP 服务器配置

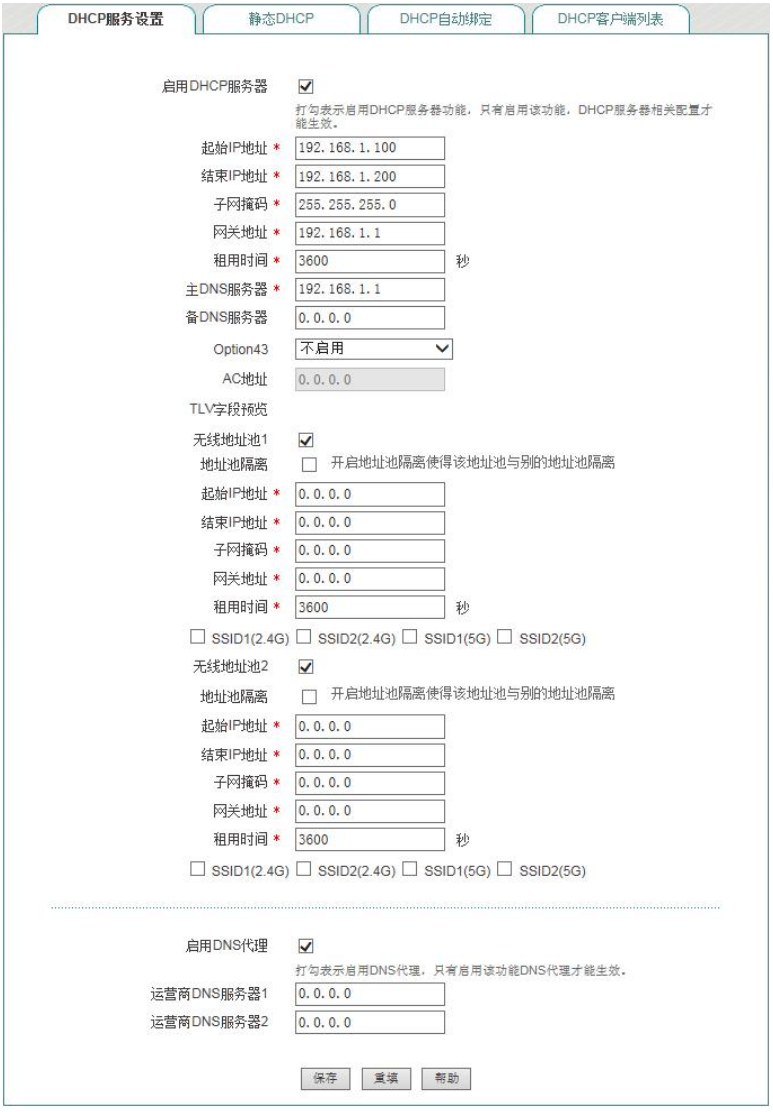


图 5- 16 DHCP 服务配置

- 启用 DHCP 服务器：用来禁用或允许设备的 DHCP 服务器功能。
- 起始、结束 IP 地址：DHCP 服务器给内网计算机自动分配的 IP 地址段（应与设备 LAN 口的 IP 地址在一个网段）。此地址段为设备的默认地址池。默认情况下，所有客户端请求的 IP 地址在此地址池中。
- 子网掩码：DHCP 服务器给内网计算机自动分配的子网掩码（应与设备 LAN 口的子网掩码一致）。
- 网关地址：DHCP 服务器给内网计算机自动分配的网关 IP 地址（应与设备 LAN 口的 IP 地址一致）。
- 租用时间：内网计算机获得设备分配的 IP 地址的租用时间（单位：秒）。
- 主 DNS 服务器：DHCP 服务器给内网计算机自动分配的主 DNS 服务器 IP 地址。
- 备 DNS 服务器：DHCP 服务器给内网计算机自动分配的备 DNS 服务器 IP 地址。
- Option43：通过修改 dhcp 协议报文里的 option 43 可变长字段，用来携带 AC 的 IP 地址，让 AP 解析 option 43 携带的 AC 地址，用来发现 AC。其中有不启用、HEX 定长、ASCII 不定长、自定义四个选项。
  - HEX 定长：填写 AC 地址，将 AC 地址解析成十六进制编码数字组成。
  - ASCLL 不定长：不定长编码，将 AC 地址解析成一组字符。
  - 自定义：如果配置非法，将导致 DHCP 服务器异常或 option43 配置不生效。
- AC 地址：配置 AC 的 IP 地址。
- TLV 字段预览：显示系统生成的 AC 地址对应的 TLV（Type Length Value）值。
- 无线地址池 1 或 2：勾选启用无线地址池。启用无线地址池后，无线客户端在请求 DHCP 服务器分配 IP 地址时，所获取的地址为无线地址池中的 IP 地址。
- 地址池隔离：隔离此地址池与其他地址池。处于此地址池内的 STA 将不能与其他地址池内的 STA 通信。
- 起始、结束 IP 地址：DHCP 服务器给内网无线客户端自动分配的 IP 地址段（不能与设备 LAN 口地址段、其他无线地址池处于一个网段）。
- 子网掩码：DHCP 服务器给内网无线客户端自动分配的子网掩码（应与设备 LAN 口的子网掩码一致）。
- 网关地址：DHCP 服务器给内网无线客户端自动分配的网关 IP 地址（应与设备 LAN 口的 IP 地址一致）。
- 租用时间：DHCP 服务器分配给内网无线客户端的 IP 地址的租用时间（单位：秒）。
- SSID1(2.4G)：接入 SSID1 的 2.4GHz 客户端将请求到无线地址池中配置的 IP 地址。
- SSID1(5G)：接入 SSID1 的 5GHz 客户端请求到无线地址池中配置的 IP 地址。
- SSID2(2.4G)：接入 SSID2 的 2.4GHz 客户端请求到无线地址池中配置的 IP 地址。
- SSID2(5G)：接入 SSID2 的 5GHz 客户端请求到无线地址池中配置的 IP 地址。

- 启用 DNS 代理：选中表示启用，启用后设备的 DNS 代理功能才会生效，启用此功能后将网关地址分配给客户端作为主、备 DNS 服务器。
- 运营商 DNS 服务器 1、2：运营商 DNS 服务器的 IP 地址。

提示：

1. 如果要使用设备的 DHCP 服务器功能，内网计算机的 TCP/IP 协议可设置为“自动获得 IP 地址”。
2. 如果用户原先使用的是代理服务器软件（如 wingate），且计算机的 DNS 服务器设置为代理服务器的 IP 地址，那么，只需将设备的 LAN 口的 IP 地址设置为同一个 IP 地址，这样，当设备启用 DNS 代理功能之后，用户不需要修改计算机的配置就可以转换到使用设备的 DNS 代理功能了。

5.5.1.2 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 5- 17 静态 DHCP 列表

2） 静态 DHCP 配置

在上图所示的页面点击**添加新条目**，进入如下图所示的**静态 DHCP 配置**页面。下面介绍配置

静态 DHCP 时各参数的涵义。

图 5- 18 静态 DHCP 配置

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

提示：

(1) 设置成功后，设备将为指定计算机固定分配预设的 IP 地址。

(2) 配置的 IP 地址要在 DHCP 服务器提供的范围之内。

5.5.1.3DHCP 自动绑定

下面介绍 DHCP 自动绑定功能。

图 5- 19 DHCP 自动绑定

- 启用 DHCP 自动绑定：当启用 DHCP 自动绑定时，设备会对内网进行扫描，将动态获取 IP 地址的内网用户的 IP/MAC 进行绑定，并且设备后续每分配一个 IP 地址，就会将该 IP 地址与客户端的 MAC 地址进行绑定。启用该功能，能有效防御内网的 ARP 欺骗。如不启用，则不进行自动绑定操作。
- 启用 DHCP 自动删除：当启用 DHCP 自动删除时，表示在租期到期或用户主动释放地址后，设备会将之前自动绑定的 IP/MAC 删除，如不启用，则表示不进行自动删除操作。

5.5.1.4DHCP 客户端列表

对于已分配给内网计算机的 IP 地址，可以在 DHCP 客户端列表中查看到相关信息。如下图中的信息表示：DHCP 服务器将地址池中的 192.168.1.100 的 IP 地址分配给 MAC 地址为 00:E0:61:08:A4:43 的内网计算机，该计算机租用该 IP 地址剩余的时间为 72034 秒。

图 5- 20 DHCP 客户端列表

5.5.1.5DHCP 配置实例

应用需求

本实例中，要求设备开启 DHCP 功能，有线与无线客户端使用不同网段的地址，有线客户端使用的起始地址为 192.168.1.100，共可分配 101 个地址。其中 MAC 地址为 00:21:85:9B:45:46 的主机分配 192.168.1.105 的固定 IP 地址，MAC 地址为 00:1f:3c:0f:07:f4 分配 192.168.1.106 的固定 IP 地址。无线客户端可以接入网络获取的地址池为 192.168.2.100~192.168.2.200。

配置步骤

第一步，进入**网络参数—>LAN 口配置**页面，配置 LAN 口 IP 地址为 192.168.1.1。

图 5- 21 LAN 口 IP 地址设置——实例

第二步，进入**网络参数—>DHCP 服务器—> DHCP 服务设置**页面。启用 DHCP 功能，并配置相

关 DHCP 服务参数，配置完后点击**保存**。

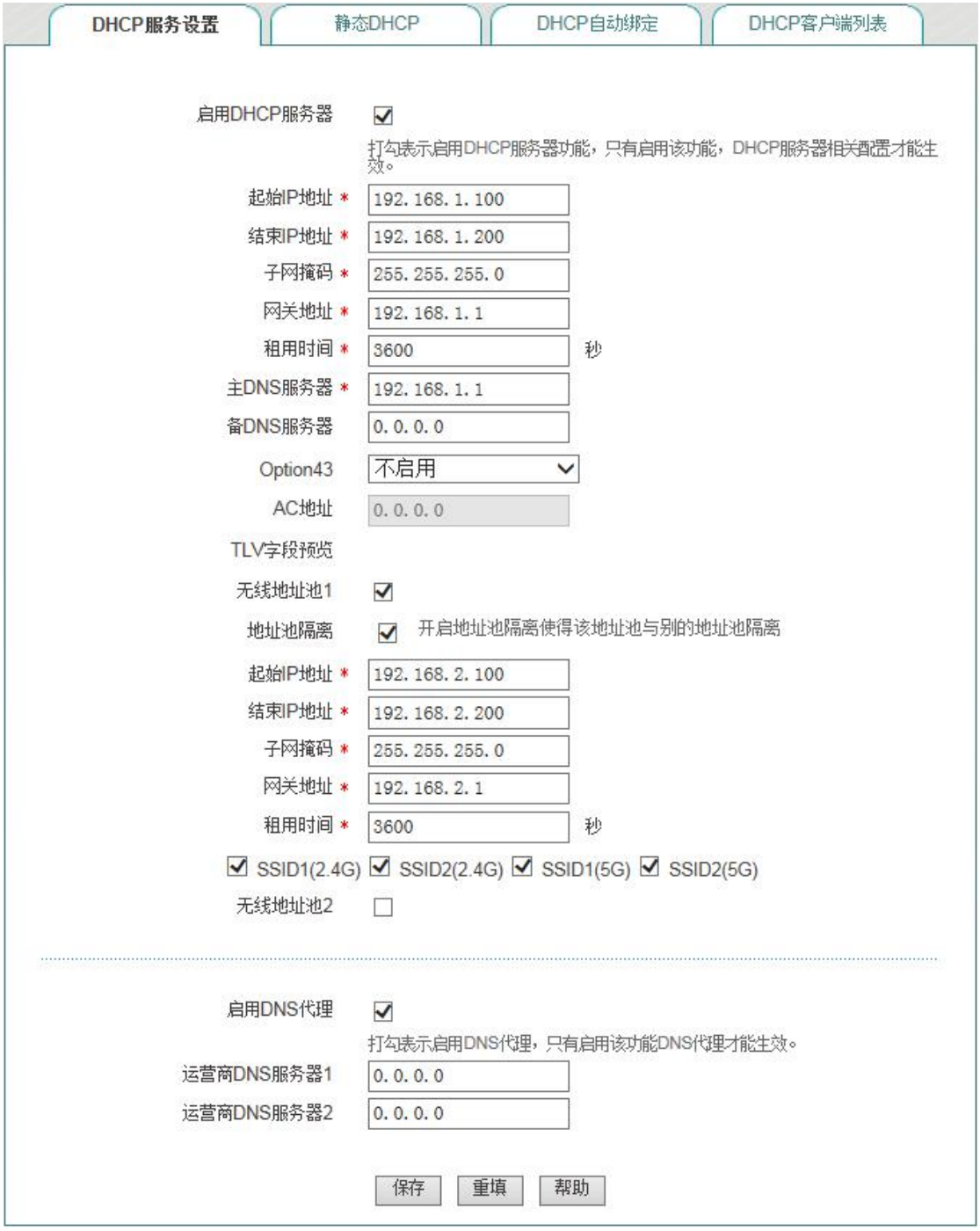


图 5- 22 DHCP 服务设置——实例

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**，配置需求中的静态 DHCP 实例。

图 5- 23 静态 DHCP 配置——实例 A

图 5- 24 静态 DHCP 配置——实例 B

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

图 5- 25 静态 DHCP 信息列表——实例

5.5.2 DHCP 多地址池

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。

5.5.2.1 DHCP 地址池列表

在**网络参数—>DHCP 服务器—>DHCP 地址池列表**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 5- 26 DHCP 地址池列表

图 5- 27 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：秒）。
- 主 DNS 服务器：DHCP 服务器给内网计算机自动分配的主 DNS 服务器 IP 地址。
- 备 DNS 服务器：DHCP 服务器给内网计算机自动分配的备 DNS 服务器 IP 地址。
- Option43：通过修改 dhcp 协议报文里的 option 43 可变长字段，用来携带 AC 的 IP 地址，让 AP 解析 option 43 携带的 AC 地址，用来发现 AC。其中有不启用、HEX 定长、ASCII 不定长、自定义四个选项。
  - HEX 定长：填写 AC 地址，将 AC 地址解析成十六进制编码数字组成。
  - ASCLL 不定长：不定长编码，将 AC 地址解析成一组字符
  - 自定义：如果配置非法，将导致 DHCP 服务器异常或 option43 配置不生效。

5.5.2.2 静态 DHCP

本节介绍静态 DHCP 列表及如何配置静态 DHCP。

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

1） 静态 DHCP 列表

图 5- 28 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 5- 29 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。

5.5.2.3DHCP 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 EC:23:3D:0C:C6:89 的内网计算机，该计算机租用该 IP 地址剩余的时间为 73777 秒。

图 5- 30 DHCP 客户端列表

5.5.2.4DNS 代理

在本页面启用 DNS 代理功能并设置运营商 DNS 服务器。

图 5- 31 DNS 代理

- 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。
- 运营商 DNS 服务器 1、2：运营商 DNS 服务器的 IP 地址。

5.5.2.5DHCP 配置实例

应用需求

本实例中，要求设备开启 DHCP 功能，起始地址为 192.168.2.10，共可分配 100 个地址；其中 MAC 地址为 00:21:85:9B:45:46 的主机分配 192.168.2.15 的固定 IP 地址，MAC 地址为 00:1f:3c:0f:07:f4 分配 192.168.2.10 的固定 IP 地址。

配置步骤

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

第二步，点击**新增条目**，启用 DHCP 功能，并配置相关 DHCP 服务参数，配置完后点击**保存**。

图 5- 32 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 5- 33 静态 DHCP 配置——实例 A

图 5- 34 静态 DHCP 配置——实例 B

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

图 5- 35 静态 DHCP 信息列表——实例

5.6 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。

5.6.1 花生壳的 DDNS 服务

图 5- 36 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。

5.6.2 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 5- 37 注册 3322.org 动态域名

2）3322.org 的 DDNS 配置

图 5- 38 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。

5.6.3 Iplink 的 DDNS 服务

图 5- 39 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。

5.6.4 Uttcare 的 DDNS 服务

图 5- 40 配置 DDNS——uttcare.com

- 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。

5.6.5 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 5- 41 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。

5.6.6 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 5- 42 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。

5.6.7 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。

图 5- 43 配置 DDNS

```
Pinging yangliu2468.xicp.net [116.236.120.162] with 32 bytes of data:

Reply from 116.236.120.162: bytes=32 time<1ms TTL=61
Reply from 116.236.120.162: bytes=32 time<1ms TTL=61
Reply from 116.236.120.162: bytes=32 time<1ms TTL=61
Reply from 116.236.120.162: bytes=32 time<1ms TTL=61

Ping statistics for 116.236.120.162:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

图 5- 44 配置 DDNS

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。

5.7 UPnP

本节介绍**网络参数—>UPnP** 页面及配置。在本页面中配置 UPnP 时，只需启用或禁用该功能

即可。

图 5- 45 UPnP 配置

- 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。

5.8 WAN 口数量配置

进入**网络参数—>WAN 口数量配置**页面，能够动态的配置设备的 WAN 口数量。操作步骤：选择 WAN 口的数量后点击**保存**按钮。注意：点击保存后，应手动重启设备配置才会生效，且重启后的设备会恢复到出厂值。

图 5- 1 WAN 口数量配置

第 6 章 无线配置

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

提示：无线设置 2.4GHz 或 5GHz：设置路由器 2.4GHz 或 5GHz 频段无线网络的相关参数。只有当网卡的参数和路由器的参数相匹配时，才能正常使用无线功能访问路由器；同时，通过此功能给无线网络加密可以防止他人非法入侵无线网络。

6.1 2.4G 基本配置

本节讲述**无线配置 2.4G—>无线基本设置**页面及配置方法。在本页面，您可以配置设备的无线网络名称、限速策略、无线模式、信道、频道带宽、有线无线隔离、无线多 SSID 隔离、启用或禁用 SSID 广播等功能。

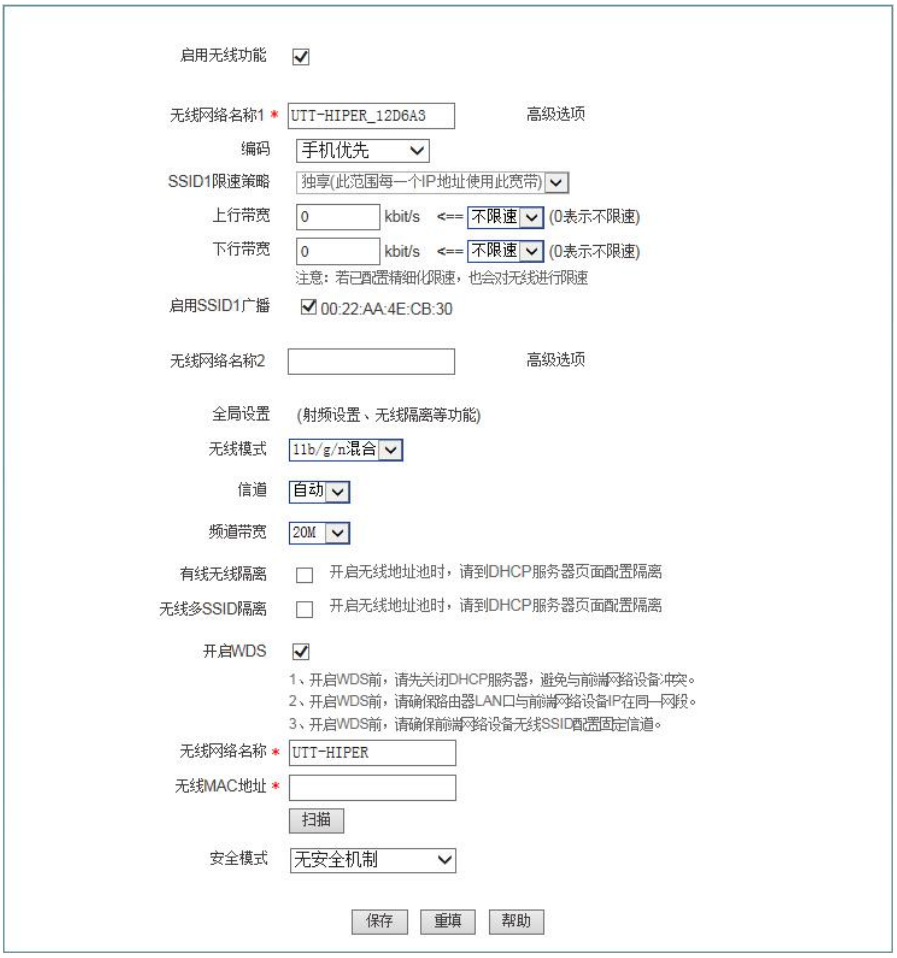


图 6- 1 无线 2.4G

启用无线功能：只有启用无线功能后，无线客户端才能连接到设备，从而通过设备进行无线通信，接入并访问设备连接的有线网络。

- 无线网络名称 1、2：用于唯一地标识一个无线网络的字符串，区分大小写。点击**高级选项**配置无线网络限速策略。
- 编码：设置为手机优先，表示设置的 SSID 能够确保手机用户搜索到正确的无线 SSID；设置为“电脑优先简体”或“电脑优先繁体”的原理同“手机优先”。这里的手机用户一般为安卓或苹果操作系统。
- SSID1、2 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。
- 上传带宽、下行带宽：设置此范围内 IP 地址的最大上传、下载速率，0 表示不限制。
- 启用 SSID 广播：启用或禁用 SSID 广播功能。如果开启此功能，那么，设备将会把自己的 SSID 广播给所有的无线站点，这样，没有 SSID（为空值）的无线站点将获得正确的 SSID，从而连接到设备，并加入到该 SSID 标识的无线网络。由于开启此功能存在安全风险（非法站点很容易获得 SSID 信息），一般建议禁用此功能。
- 全局设置：点击设置无线模式、信道、频道带宽等功能。
- 无线模式：该项用于设置路由器的无线工作模式。推荐使用 11b/g/n 混合模式。
- 信道：此参数用于选择无线网络工作的频率段，可以选择的范围从 1 到 11，另外提供自动选项，表示设备可以自动选择最优频率段。如果存在多个无线设备时，要注意各个设备的频段设置不能相互影响。
- 频道带宽：设置无线数据传输时所占用的频道带宽，可选项为：自动、20M 和 40M。注意，本参数仅对采用 802.11n 标准接入的无线站点起作用。对于以 802.11b 或者 802.11g 标准的无线站点来说，只能使用 20M 的频道带宽：
  - 自动：选择自动时，表示使用 802.11n 接入的无线站点将根据与接入对端协商的结果选择使用 20M 或 40M 的频道带宽。
  - 20M：选择 20M 时，表示使用 802.11g 接入的无线站点将使用 20M 的频道带宽。
  - 40M：选择 20M 时，表示使用 802.11n 接入的无线站点将使用 40M 的频道带宽。
- 有线无线隔离：勾选启用后，有线用户与无线用户不能互相访问。
- 无线多 SSID 隔离：勾选启用后，不同无线网络之间相互隔离，不能相互访问。
- 开启 WDS：可以选择这一项开启 WDS 功能，通过这个功能可以桥接多个无线局域网。

提示：

1) 设备默认开启无线功能，且工作模式为 AP Mode。
2) 无线参数修改后，设备的无线模块将会重启，无线模块重启会断开所有的无线连接。

6.2 2.4G 无线配置实例

本节根据无线桥接要求配置实例。

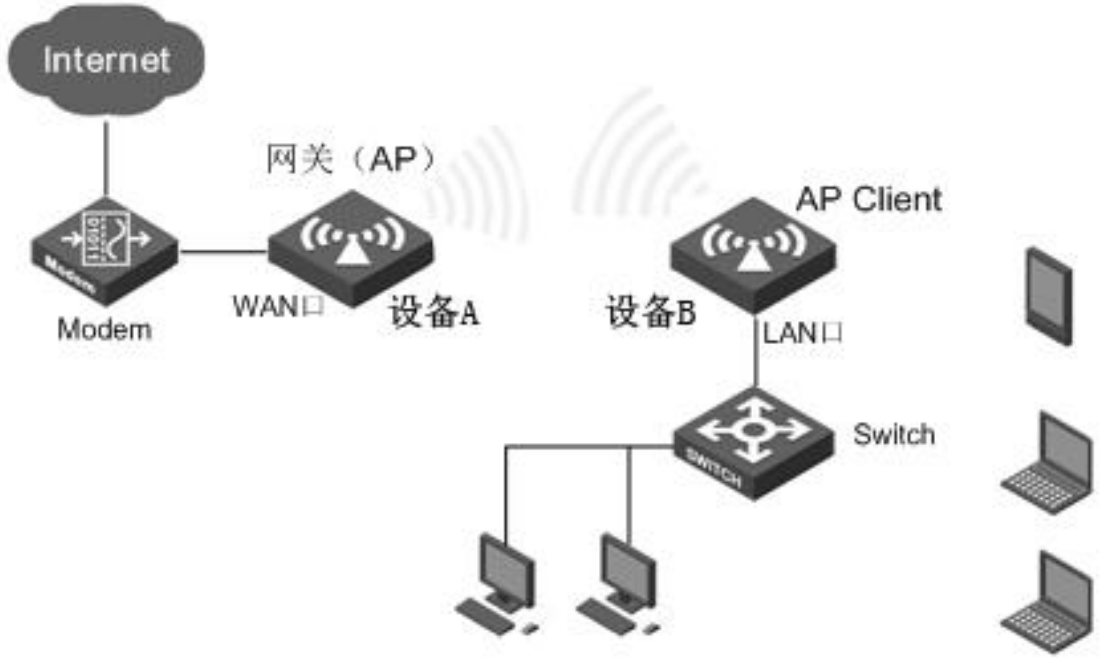


图 6- 2 组网环境

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

配置步骤：

1） 配置设备 B。

项目	参数	项目	参数
无线模式	11b/g/n 混合	信道	6
安全模式	WPA-PSK/WAP2-PSK	加密算法	TKIP

2） 进入**无线配置 2.4G—>无线基本配置**页面，开启 WDS 功能，点击**扫描**。如下图所示。

图 6- 3 WDS 桥接

4）点击扫描后如下图所示，选择需要桥接的设备 B。

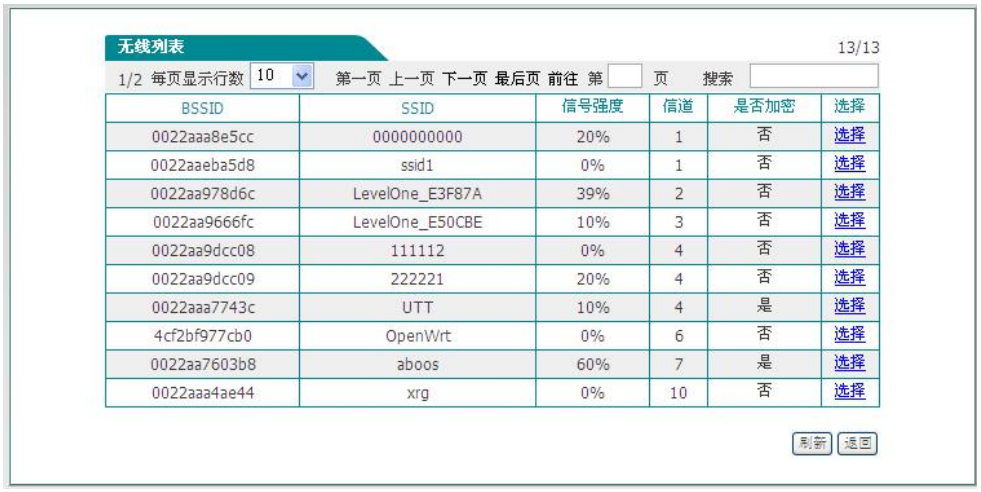


图 6- 4 无线列表

4） 配置无线通信的验证方式及密钥并保存，显示“已连接”表示连接成功。如下图所示：

图 6- 5 无线配置

注意：需保证设备 A 与设备 B 在相同的信道、相同无线模式、相同的加密方式、相同网段，下才会连接成功。

5） 检测设备 A 是否与设备 B 是否已连接成功。在设备 A 上 ping 设备 B 的 IP 地址，能 ping 通即表明设备 A 与设备 B 无线连接已成功建立。

6.3 5G 基本设置

单击**无线设置 5GHz→基本设置**，可以在图中对 5GHz 频段无线网络进行基本设置。其中的无线网络名称和信道是路由器无线功能必须设置的参数。

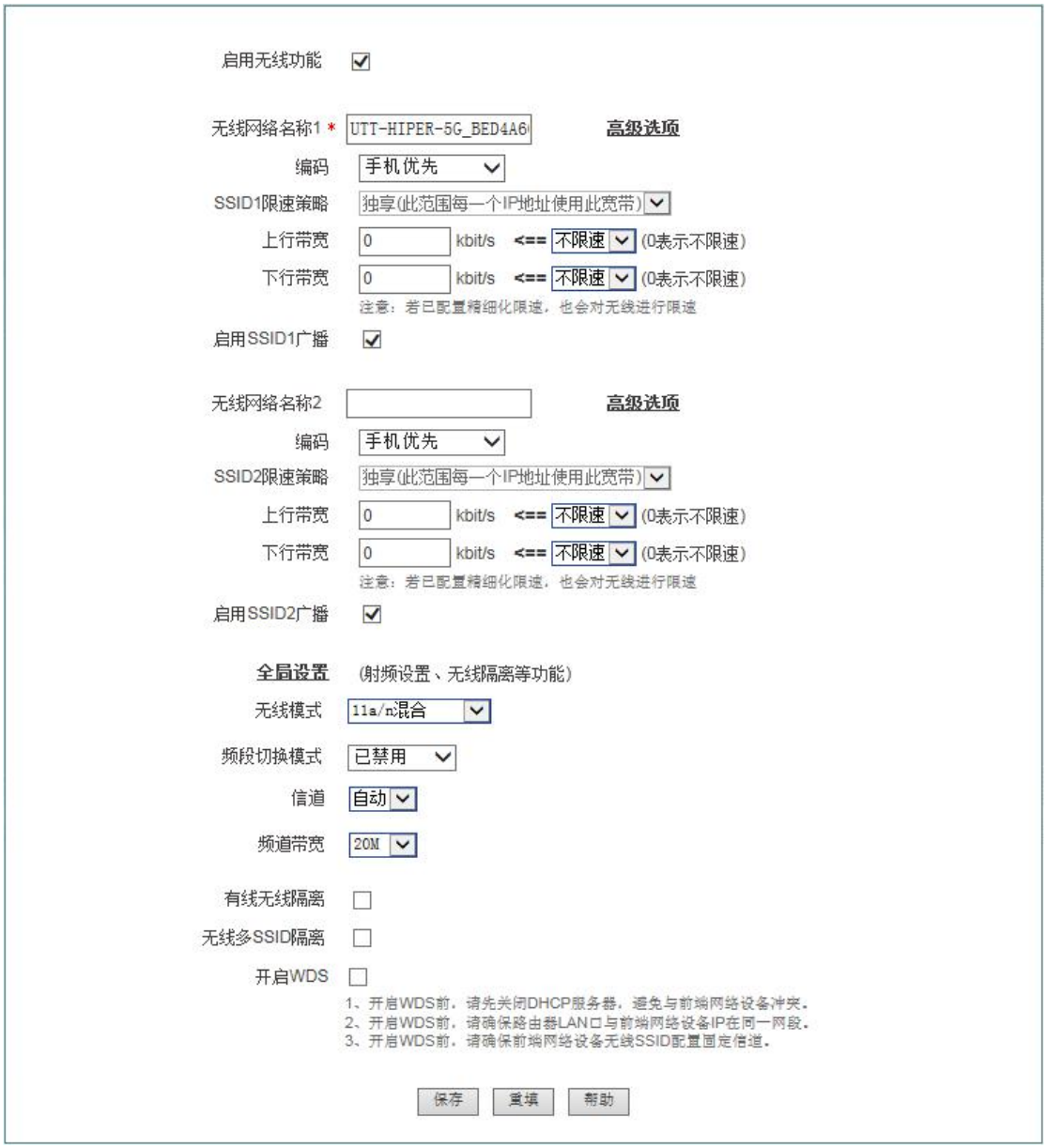


图 6- 6 无线 5G

- 启用无线功能：只有启用无线功能后，无线客户端才能连接到设备，从而通过设备进行无线通信，接入并访问设备连接的有线网络。
- 无线网络名称：用于唯一地标识一个无线网络的字符串，区分大小写。点击**高级选项**配置无线网络限速策略。
- 编码：设置为手机优先，表示设置的 SSID 能够确保手机用户搜索到正确的无线 SSID；设置为“电脑优先简体”或“电脑优先繁体”的原理同“手机优先”。这里的手机用户一般为安卓或苹果操作系统。
- SSID1、2 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。
- 上传带宽、下行带宽：设置此范围内 IP 地址的最大上传、下载速率，0 表示不限制。

- 启用SSID广播：该项功能用于将路由器的SSID号向周围环境的无线网络内广播，这样，主机才能扫描到 SSID 号，并可以加入该 SSID 标识的无线网络。全风险（非法站点很容易获得 SSID 信息），一般建议禁用此功能。
- 全局设置：点击设置无线模式、信道、频道带宽等功能。
- 无线模式：该项用于设置路由器的无线工作模式。推荐使用 11a/n 混合模式。
- 频段切换模式：有四种模式，已禁用、优选 5GHz，强制 5GHz，频段平衡。
  - 优选 5GHz：引导支持双频的 STA 优先通过 5GHz 接入设备。
  - 强制 5GHz：对于支持双频的 STA，只允许 STA 通过 5GHz 射频接入设备。
  - 频段平衡：设备引导 STA 在 2.4GHz 和 5GHz 射频上平衡分布。
- 信道：以无线信号作为传输媒体的数据信号传送的通道，若选自动，则设备会自动根据周围的环境选择一个最优信道。
- 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：自动、20M 和 40M。注意，本参数仅对采用 802.11n 标准接入的无线站点起作用。
  - 自动：选择自动时，表示使用 802.11n 接入的无线站点将根据与接入对端协商的结果选择使用 20M 或 40M 的频道带宽。
  - 20M：选择 20M 时，表示使用 802.11a/n 接入的无线站点将使用 20M 的频道带宽。
  - 40M：选择 20M 时，表示使用 802.11a/n 接入的无线站点将使用 40M 的频道带宽。
- VHT 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： 20/ 40M 和 80M。注意，本参数仅对采用 802.11vht AC/AN/C 和 802.11vht AC/AN 标准接入的无线站点起作用。
  - 20/40M：选择 20M 时，表示使用 802.11vht AC/AN/C 或 802.11vht AC/AN 接入的无线站点将使用 20M 或 40M 的频道带宽。
  - 80M：选择 20M 时，表示使用 802.11vht AC/AN/C 或 802.11vht AC/AN 接入的无线站点将使用 80M 的频道带宽。
- 有线无线隔离：勾选启用后，有线用户与无线用户不能互相访问。
- 无线多 SSID 隔离：勾选启用后，不同无线网络之间相互隔离，不能相互访问。
- 开启 WDS：可以选择这一项开启 WDS 功能，通过这个功能可以桥接多个无线局域网。

提示：

1） 选择信道时请避免与当前环境中其他无线网络所使用的信道重复，以免发生信道冲突，使传输速率降低。

2） 以上提到的频段带宽设置仅针对支持 IEEE 802.11n 协议的网络设备；对于不支持 IEEE 802.11n 协议的设备，此设置不生效。例如，当本路由器与 11n 系列网卡客户端进行通信时频道带宽设置可以生效，当与 11a/b/g 系列网卡客户端进行通信时此设置将不再生效。

3） 路由器默认无线同时工作在 2.4GHz 和 5GHz 频段，若只需使用其中一种，请登录路

由器无线频段设置界面进行选择，保存后重启路由器生效。

4） 若您的终端设备不支持 5GHz 频段，而路由器的频段设置为 5GHz，则该终端设备将无法搜索到路由器的无线信号。

5） 当路由器的无线设置完成后，无线网络内的主机若想连接该路由器，其无线参数必须与此处设置一致。

6） 与路由器进行 WDS 连接的 AP，只需要工作在 AP 模式且支持此地址即可，不需要额外的配置。

6.4 无线安全设置

设备支持对无线网络 SSID1 与 SSID2 分别进行安全加密设置，提供 WEP、WPA/WPA2、WPA-PSK/WPA2-PSK 三种无线安全机制，同时，也允许用户不使用安全机制，以下各节将分别介绍它们的配置参数的含义。

6.4.1 无安全机制

图 6- 7 无安全机制

- 选择 SSID：对不同的 SSID 进行安全加密。
- 安全机制：此处选择“无安全机制”，表示客户端不使用任何安全机制验证即可接入所选无线网络。

6.4.2 WEP

图 6- 8 WEP

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

6.4.3 WPA/WPA2

图 6- 9 WPA/WPA2

- 选择 SSID：选择 SSID 进行安全加密设置。
- 安全机制：此处选择 **WPA/WPA2**，表示本设备将采用 WPA 或 WPA2 安全机制。此安全机制下，本设备将采用 Radius 服务器进行身份认证并得到密钥。
- WPA 版本：用来设置本设备将使用的安全模式：

- 自动：表示本设备会根据无线客户端的请求自动选择 WPA 或者 WPA2 安全模式。
- WPA：表示本设备将采用 WPA 的安全模式。
- WPA2：表示本设备将采用 WPA2 的安全模式。

◆ 加密算法：用来选择对无线数据进行加密的安全算法，选项有自动、TKIP、AES。

- 自动：表示本设备将根据需要自动选择加密算法。
- TKIP：表示所有无线数据都将使用 TKIP 作为加密算法。
- AES：表示所有无线数据都将使用 AES 作为加密算法。

◆ Radius 服务器 IP：用来对无线主机进行身份认证的 Radius 服务器的 IP 地址。

◆ Radius 端口：Radius 服务器对无线主机进行身份认证时使用的服务端口号。

◆ Radius 密码：该项用来设置访问 Radius 服务的密码。

◆ 密钥更新周期：用于指定密钥的定时更新周期。取值范围为 60~86400，单位为秒。缺省值为 3600，值为 0 时表示不更新。

6.4.4 WPA-PSK/WPA2-PSK

图 6- 10 WPA-PSK/WPA2-PSK

◆ 选择 SSID：选择 SSID 进行安全加密设置。

◆ 安全机制：此处选择 **WPA-PSK /WPA2-PSK**，表示本设备将采用 WPA-PSK 或 WPA2-PSK 安全机制。此安全机制下，本设备将采用基于预共享密钥的 WPA 模式。

◆ WPA 版本：用来设置本设备将使用的安全模式：

- 自动:表示本设备会根据无线客户端的请求自动选择 WPA-PSK 或者 WPA2-PSK 安全模式。
- WPA：表示本设备将采用 WPA-PSK 的安全模式。
- WPA2：表示本设备将采用 WPA2-PSK 的安全模式。

◆ 加密算法：用来选择对无线数据进行加密的安全算法，选项有自动、TKIP、AES。

- 自动：表示本设备将根据需要自动选择加密算法。
- TKIP：表示所有无线数据都将使用 TKIP 作为加密算法。

- AES：表示所有无线数据都将使用 AES 作为加密算法。

- 预共享密钥：预先设置的初始化密钥，取值为 8~63 个字符。点击 ，密码以明文方式显示。

- 密钥更新周期：用于指定密钥的定时更新周期。取值范围为 60~86400，单位为秒。默认值为 3600，值为 0 时表示不更新。

6.5 无线 MAC 地址过滤

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

图 6- 11 无线 MAC 地址过滤

- 启用 MAC 地址过滤：启用或禁用 MAC 地址过滤功能，勾选表示启用。

- 过滤规则：设置 MAC 地址过滤的规则。

  - 允许 只允许列表中的 MAC 地址访问本无线网络：表示只允许 MAC 地址过滤信息列表中的 MAC 地址对应的无线客户端接入本设备，禁止除过滤表以外的无线客户端接入。

  - 禁止 只禁止列表中的 MAC 地址访问本无线网络：表示只禁止 MAC 地址过滤信息列表中的 MAC 地址对应的无线客户端接入本设备，允许除过滤表以外的无线客户端接入。

- 添加新条目：点击该按钮，可进入 **MAC 地址过滤配置**页面配置需要过滤的 MAC 地址，如下图所示。

图 6- 12 MAC 地址过滤配置

6.6 无线高级配置

本节介绍**无线配置—>无线高级配置**页面的无线高级参数的含义。

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

图 6- 13 无线高级配置

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

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

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

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

- Beacon 间隔：设备通过定期广播 Beacon（信标）帧进行无线网络连接的同步，本参数用于定义信标帧的发送间隔，信标帧按照指定的时间间隔周期性发送。一般，取值范围为 20~999 毫秒，默认值为 90 毫秒。

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

- 启用短前导：启用或禁用短前导（Short Preamble）。

  - 启用后，将使用短前导类型。短前导类型能提供更好的性能。因为短前导的使用可以使开销减少到最小，因而使网络数据吞吐量最大化。

  - 禁用时，则使用长前导类型（Long Preamble），长前导类型将能够提供更多可行连接和更大范围的连接。

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

6.7 无线主机状态

本节介绍**无线配置**—>**无线主机状态**页面。

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

图 6- 14 无线主机状态

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

第 7 章　高级配置

本章介绍的功能有：NAT 和 DMZ、路由配置、策略路由、DNS 重定向、网络尖兵防御和端口镜像等等。

7.1　NAT 和 DMZ 配置

本节讲述**高级配置—>NAT 和 DMZ 配置**页面的功能及配置方法。

7.1.1 NAT 功能介绍

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

艾泰路由产品提供了灵活的 NAT 功能，以下将详细介绍它的特点。

1） NAT 地址空间

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

2） 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。它通常用来配置外网访问内网的服务器：内网服务器依旧使用私有地址，对外提供为其分配的公网 IP 地址给外部网络用户访问。

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，外网中的计算机希望通过设备访问内网服务器，这时就需要在设备上设置 NAT 静态映射或虚拟服务器（DMZ 主机）来达到这个目的。

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

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

提示：被设置为虚拟服务器的计算机将失去设备的防火墙保护功能。

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

7.1.2 NAT 静态映射

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

1） NAT 静态映射列表

图 7- 1 NAT 静态映射列表

提示：

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

2） NAT 静态映射配置

在图 7-1 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 静态映射配置的各参数的涵义。

图 7- 2 NAT 静态映射配置

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

7.1.3 NAT 规则

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

7.1.3.1NAT 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 口实现上网。一条实例的 NAT 类型为：One2One，是将内网 IP 地址为 192.168.1.50-192.168.1-52 的地址分别转换为 200.200.202.50、200.200.202.51、200.200.202.52，且绑定在 WAN1 口实现上网。

图 7- 3 NAT 规则信息列表

提示：针对同一对象配置了多条 NAT 规则，最后配置规则先生效。

7.1.3.2Easy IP

在图 7-3 中点击**添加新条目进**入 NAT 规则配置页面。下面介绍配置 NAT 规则类型为 EasyIP 的各参数的涵义。

图 7- 4 Easy IP

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

7.1.3.3One2One

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 7- 5 One2One

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

提示：

1. 每条 One2One 规则最多只能绑定 20 个外部地址。
2. 外部起始 IP 地址必须设置，实际映射的外部 IP 地址从设置值开始依次增加。例如，如果内部起始 IP 地址设为 192.168.1.50，内部结束 IP 地址设为 192.168.1.52，外部起始地址设为 200.200.202.50，则 192.168.1.50、192.168.1.51、192.168.1.52 依次映射成 200.200.202.50、200.200.202.51、200.200.202.52。

7.1.4 DMZ

下面介绍设备的 DMZ 功能。

图 7- 6 DMZ 配置

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

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

7.1.5 NAT 和 DMZ 配置实例

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

一、NAT 静态映射配置实例

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

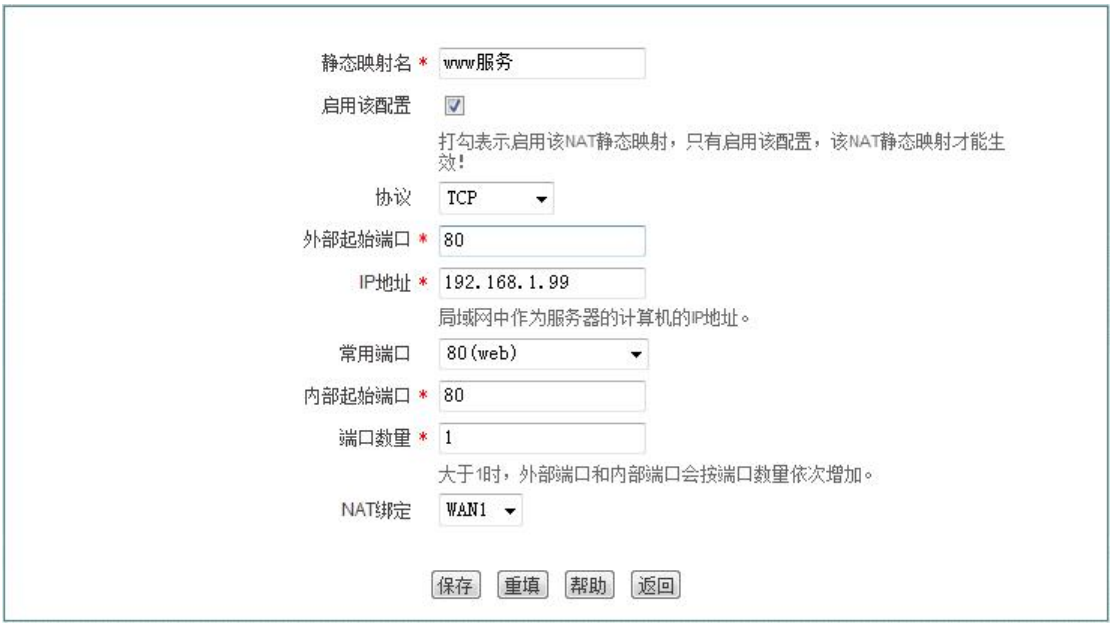


图 7- 7 NAT 静态映射配置实例

二、EasyIP 配置实例

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

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

配置步骤如下：

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

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

第三步，选择 NAT 类型为 **EasyIP**。

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

第五步，选择该规则绑定的接口为 WAN1 口。

第六步，点击**保存**，该条 NAT 规则配置成功。

图 7- 8 NAT 规则配置——EasyIP

提示：

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

三、One2One 配置实例

需求

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

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

分析

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

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

配置步骤如下：

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

第二步，进入 **NAT 规则配置**页面，在**规则名**中填入“服务器”。

第三步，选择 NAT 类型为 **One2One**。

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

第五步，选择该规则绑定的接口为 WAN1 口。

第六步，单击**保存**按钮，该条 NAT 规则添加成功。

图 7- 9 NAT 规则配置——One2One

7.2 路由配置

本节介绍**高级配置—>路由配置**页面及配置方法。

静态路由是由网络管理员手工配置的路由，使得到指定目的网络的数据包的传送，按照预定的路径进行。静态路由不会随网络结构的改变而改变，因此，当网络结构发生变化或出现网络故障时，需要手工修改路由表中相关的静态路由信息。正确设置和使用静态路由可以改进网络的性能，还可以实现特别的要求，比如实现流量控制、为重要的应用保证带宽等。

下面介绍路由配置信息列表及路由配置中各参数的涵义。

图 7- 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。

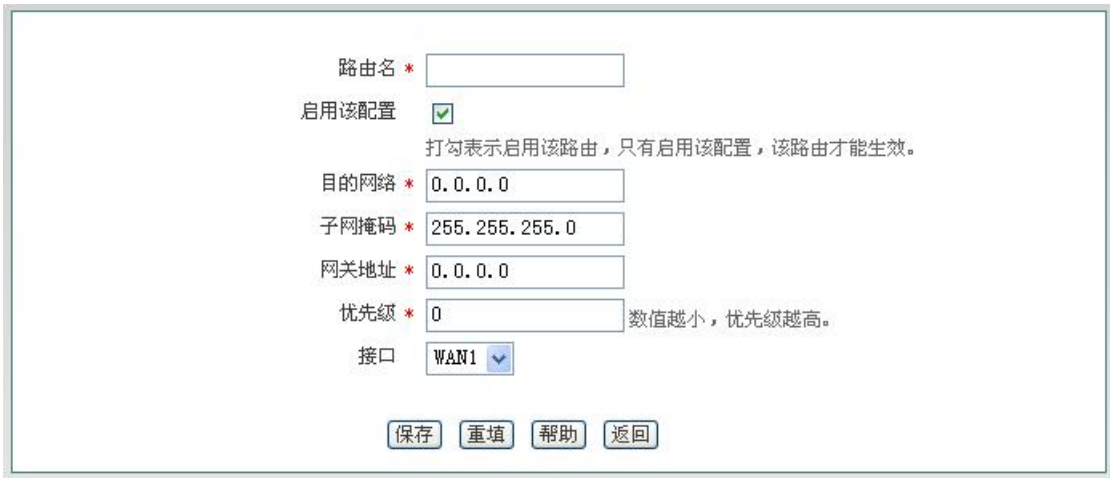


图 7- 11 静态路由配置

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

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

7.3 策略路由

本节主要讲述**高级配置—>策略路由**页面及配置方法。 在本页面可以定义策略路由，数据包按照源 IP 地址、协议、目的地址以及目的端口进行路由。

7.3.1 启用策略路由

图 7- 12 策略路由配置

- 启用策略路由：这是策略路由的全局开关，启用后配置的策略路由生效。
- 移动到：用户可以过此按钮对策略进行相应的排序。

7.3.2 策略路由配置

在上图中点击**添加新条目**，进入**策略路由配置**页面。

图 7- 13 策略路由配置

- 启用：策略路由的局部开关，勾选后，当前配置的策略路由生效。
- 策略路由名：自定义该策略的名称。
- 接口：设置策略路由绑定的物理接口，满足策略路由条件的数据包将从绑定接口转发出去。
- 源地址：设置此策略路由的数据包的源 IP 地址，可按以下两种方式配置：
  - 网段：设置此策略路由的起始 IP 地址和结束 IP 地址。
  - 用户组：设置适用于此策略的用户组。用户组的源地址段在**用户管理->用户组配置->添加新条目**页面设置。
- 目的地址：设置此策略路由的数据包中的目的地址，配置方式同源地址。
- 协议：该策略路由的协议类型。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：走此策略路由的数据包的类型，可按以下方式配置。
- 端口：范围 1~65535，对应的协议有 TCP 和 UDP（当选择的协议为 ICMP、AH 时不用配置端口范围）。
- 生效时间设置：选择策略路由生效的时间段，默认是日期是**每天**，时间为**全天**。

提示：

1. 当数据包与定义的源 IP 地址、协议、目的端口全部匹配后，将从指定的接口转发出去，找不到匹配策略路由的数据包将走正常的路由。
2. 策略路由的执行顺序：LAN 口静态路由>策略路由>WAN 口静态路由。

7.4 DNS 重定向

7.4.1 DNS 重定向功能概述

DNS 重定向是将域名重新定向到所配置的 IP 地址的功能，可使所设置的域名不通过 DNS 服务器解析域名，而是直接访问域名对应的 IP 地址。设备会根据用户所配置的重定向条目，生成一张 DNS 重定向列表，当接收到 DNS 请求包时，设备会根据该 DNS 请求包所请求的域名查找该重定向列表，若找到，则根据对应的 IP 地址生成 DNS 回复包发送给用户，若没有找到，则设备通过查找 DNS 缓存表或通过外网 DNS 服务器解析域名。

7.4.2 DNS 重定向列表

图 7- 14 DNS 重定向列表

- 增加 DNS 重定向条目：点击列表右上角的**添加新条目**按钮，进入 **DNS 重定向配置**页面进行配置。
- 编辑 DNS 重定向条目：如果想修改 DNS 重定向条目，可在 **DNS 重定向列表**中点击**编辑**超链接，进入 **DNS 重定向配置**面页，修改相关参数并点击**保存**按钮。
- 删除 DNS 重定向条目：选中一些 DNS 重定向条目，点击右下角的**删除**按钮，即可删除被选中的 DNS 重定向条目。

提示：域名中包含通配符的实例条目优先级较低，越精确的域名越先匹配。例如，当用户配置了二条 DNS 重定向条目，其中第一条的域名包含 www.utt.com.cn，第二条域名包含*.utt.com.cn。当用户使用域名 www.utt.com.cn 访问时，第一条 DNS 重定向和第二条都符合，由于第一条的域名精确度高于第二条，故优先匹配的条目为第一条，该域名所对应的的 IP 地址则为第一条 DNS 重定向条目中配置的 IP 地址。

7.4.3 DNS 重定向配置

点击**添加新条目**，进入 DNS 重定配置界面。

图 7- 15 DNS 重定向配置

- 重定向 IP：DNS 重定向所对应的 IP 地址。
- 描叙：简单解释此条 DNS 重定向条例的作用。
- 域名列表：DNS 重定向所对应的域名列表，可以是一个域名，也可以是多个域名。
- 保存：DNS 重定向配置生效。

提示：

1） 不同 DNS 重定向条目中的 IP 地址可重复。

2） 包含通配符的域名不能重复。

3） 在同一个域名列表中的域名不能重复。

7.5 网络尖兵防御

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

图 7- 16 网络尖兵防御

7.6 即插即用

本节介绍**高级配置—>即插即用**页面及配置。即插即用是全新功能，在设备上启用即插即用功能后，内网用户无需更改任何网络参数设置，即无论内网用户的 IP 地址、子网掩码、网关和 DNS 服务器如何变化，都可以通过设备上网。

图 7- 17 启用即插即用

提示：

(1) 启用后，内网用户无需更改任何配置（如 IP 地址、网关地址、DNS 服务器地址），就可以通过设备上网。如果内网主机的 IP 地址与设备 LAN 口 IP 地址在同一网段，则主机的网关地址必须设置为设备 LAN 口的 IP 地址，否则无法上网。

(2) 启用后，内网 IP 地址相同的用户不能同时上网，且内网用户的 IP 地址不能与设备各接口的 IP 地址相同。

(3) 启用后，系统将默认开启 ARP 代理和 DNS 代理，关闭 IP 欺骗防御且允许未被 IP/MAC 绑定的主机通过。内网用户的 IP 地址不能与路由器的接口（LAN 口及 WAN 口）IP 地址、路由器网关 IP 地址和路由器设置的 DNS 服务器(包括主 DNS 服务器和备 DNS 服务器)地址相同，否则将无法上网。

7.7 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 7- 18 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 7- 19 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。

7.8 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 7- 20 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 7- 21 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：1、2。

(2) 新建 VLAN 2，其成员端口为 1、3。

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。

7.9 SNMP 配置

本节主要讲述**高级配置—>SNMP 配置**的配置方法。

SNMP 是一系列协议组和规范，它提供了一种从网络上的设备中收集网络管理信息的方法。SNMP 也为设备向网络管理工作站报告问题和错误提供了一种方法。在设备上启用了 SNMP 服务，就可以在远程使用 SNMP 软件管理和监视设备。

图 7- 22 SNMP 配置

- 启用 SNMP 服务：禁止或者允许 SNMP 服务，目前只允许 SNMP 服务器读设备信息。
- SNMP 社区名：它必须和 SNMP 网络管理软件包配置匹配。默认的 SNMP 社区名“uTt22aA”，为安全起见，建议修改这个系统默认值，从而防止入侵者通过 SNMP 的访问请求获取设备上的网络配置信息。
- 设备名：设备的主机名。
- 联系人：设备的管理员联系方式。
- 位置：设备的物理位置信息。
- 只允许以下主机管理：选中“只允许以下主机管理”后，可以设置 1～3 台主机，只有这三台主机可以通过 SNMP 管理设备。
- 允许主机 1，2，3：可通过 SNMP 管理设备的主机的 IP 地址。

- 保存：SNMP 配置参数生效。

提示：只有在高级配置—>SNMP 配置中启用 SNMP 远程管理功能之后，才能从 Internet 通过 SNMP 服务器远程管理设备。SNMP 目前支持的版本为 v2c。

7.10 SYSLOG 配置

本节介绍**高级配置—>SYSLOG 配置**页面。

图 7- 23 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。
- syslog 消息发送间隔：设置 syslog 消息发送的间隔值，单位为秒，默认为 0 。

提示：syslog 消息发送间隔功能需要结合艾泰科技的 Xport 使用。

第 8 章 网络共享

本章介绍网络共享菜单下的功能，包括：网络共享管理,FTP 服务器，共享账户。通过使用网络共享服务，可以方便地在局域网中共享 USB/SD 卡存储设备上的卷。单击菜单中的子项即可进行具体的设置，下面将详细讲解各子项的功能和设置方法。

8.1 网络共享管理

通过网络共享管理功能，可以查看已连接到路由器存储设备的信息，方便地在局域网中共享 USB/SD 卡存储设备上的卷。

选择菜单**网络共享→网络共享管理**配置，可以在图 8- 1 **错误！未定义书签。**所示界面中查看网络共享服务条目。

图 8- 1 网络共享配置配置

- 启用存储设备：如果勾选表示可以使用设备上的存储设备。
- 使用密码访问：如果勾选，局域网中用户必须通过用户名和密码来访问 USB/SD 卡存储设备上的卷。如果您没有设置访问密码，请启动服务前在“共享账户”页面进行设置。
- 卷：USB 存储设备上卷的卷名，由路由器自定义，不可更改。
- 总容量：显示该卷的大小。
- 已使用：显示该卷已被使用的空间大小。
- 剩余： 显示该卷尚未使用的空间大小。
- 使用量：显示该卷已被使用的空间占总空间的百分比。
- 共享控制：通过点击该条目下方对应的按钮设置是否共享该卷。点击**开启**，则该卷被共享。
- 弹出设备：点击该按钮可以安全地移除连接中的 USB/SD 卡驱动器。
- 扫描：点击该按钮重新检测 USB/SD 卡存储设备的信息和共享卷的信息。

提示：

1) 在拔出USB存储设备前，请先点击图 8- 1界面上的弹出设备按钮，否则可能造成USB/SD卡存储设备的损坏或数据丢失。

2) 因 NTFS 支持大文件和大分区，故推荐使用 NTFS 作为共享卷的文件系统。

3) 举例：假如您希望共享 USB/SD 卡的卷，请按照如下步骤进行设置：

(1) 将您的 USB/SD 卡（移动硬盘、U 盘等）插入路由器的 USB 口，等待约 6～9 秒后点击“扫描”按钮检测分区信息。

(2) 待分区信息显示在列表中后，选择您需要共享的卷，点击共享控制栏的**开启**按钮。

(3) 勾选**启用存储设备**启动网络共享服务。

(4) 上述步骤完成之后，您就可以在 IE 浏览器中输入“\\路由器 LAN 口 IP 地址\共享名”（如：\\192.168.1.1\volume0）来访问该共享卷了。如果您不清楚路由器当前的 IP 地址，可以到**运行状态**菜单中查看。

8.2 FTP 服务器

选择菜单**网络共享→FTP 服务器**，可以在图 8- 2 所示界面方便地建立起属于您自己的 FTP 服务器。

图 8- 2 FTP 服务器配置

- 启用 FTP 服务器：如果勾选表示选择启用 FTP 服务器功能。
- 允许 WAN 口访问： 控制 FTP 服务器是否允许从 WAN 口访问。
- FTP 端口： 指定 FTP 服务器端口。建议设置为默认值 21。

- 单击**添加新文件夹**，出现以下界面，在该界面中可对新增或要修改的共享文件夹进行设置，如图所示。

图 8- 3 FTP 共享文件夹配置

- 名称：指定 FTP 服务器上共享文件夹显示的名称。
- 文件夹：如果勾选“选择全部”，则该文件夹下的所有文件将被共享。
- 文件夹位置：显示文件夹所在的完整路径。
- 选择文件夹：选择希望共享的文件夹。
- 上一级：点击该按钮回到当前文件夹的上一级文件夹。

举例：假如您希望在FTP服务器上共享USB/SD卡“我的共享”文件夹下的“图片”文件夹中的图片（假设已存在），并命名为“共享图片”，那么您可以进行如下设置：

1) 单击添加新文件夹，点击文件夹列表下的“我的共享”展开其子目录。

2) 在“名称”栏输入“共享图片”，并勾选“图片”文件夹。

3) 单击保存按钮，可以看到设置完成后的 FTP 服务器列表如上图所示。

图 8- 4 共享文件夹设置举例

4) 若您的朋友和您处在同一局域网，则当您的朋友访问此 FTP 服务器时，只需在浏览器中输入 ftp://xxx.xxx.xxx.xxx:21 即可。其中，“xxx.xxx.xxx.xxx”是本路由器的 LAN 口 IP 地址，如：当路由器 LAN 口 IP 为 192.168.1.1 时，需在浏览器中输入 ftp://192.168.1.1:21。

5) 若您的朋友和您不在同一局域网，则您必须首先在图 16-2 所示界面启用“允许 WAN 口访问”功能，则当您的朋友访问此 FTP 服务器时，需在浏览器中输入 ftp://xxx.xxx.xxx.xxx:21 即可。其中，“xxx.xxx.xxx.xxx”是本路由器的 WAN 口 IP 地址，如：当路由器 WAN 口 IP 为 172.32.90.1 时，需在浏览器中输入 ftp://172.32.90.1:21

提示：

1) 若 FTP 服务器的设置有修改，新的设置需重新启动 FTP 服务器才能生效。

2) 访问 FTP 服务器需要具有 FTP 访问权限的账户才能正常访问。如果您需要修改您的访问权限或账户，请启动服务前在“共享帐户”页设置。

8.3 共享账户

选择菜单**网络共享→共享帐户**页面，可以在图 8- 5 所示界面中设置网络共享用户的用户名和密码。

图 8- 5 共享账户配置

在启用共享之前，请先给共享帐户设置用户名和密码。

两个默认共享帐户分别是超级用户“admin”和普通用户“guest”。超级用户对可写的共享卷具有读/写权限，对只读的共享卷具有只读权限，而普通用户在任何情况下都只具有只读权限，无论该卷的读写权限是只读还是可写，并且仅超级用户能够通过IE浏览器上传文件到可写的共享卷中。 您可以通过点击**添加新条目**按钮增添使用者账户，如图 8- 6所示。每个帐户均需要指定使用者账号及密码。

图 8- 6 FTP 使用账号配置

- 账号：由不超过 15 个字符的英文字母、数字、下划线组成。超级用户和普通用户的账号名不能相同。
- 密码：由不超过 15 个字符的英文字母、数字、下划线组成。
- 确认密码：输入的确认密码必须和上面的密码一致。
- 存取权限：通过设置存取权限区分超级用户和普通用户。可选权限为读写或只读。
- FTP 访问：设置该账户对 FTP 服务器的使用权限。

完成设置后，点击保存按钮并重启服务使新设置生效。

提示：

如果您更改了共享账户设置后无法使用新设置的用户名和密码访问共享卷，请尝试按“Windows + R”组合键，在打开的“运行”对话框的输入栏中输入“net use \\192.168.1.1 /delete /yes”后回车。此处 192.168.1.1 是您路由器当前的 LAN 口 IP 地址。如果您不清楚路由器当前的 IP 地址，可以到**运行状态**页中查看。

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、服务组配置。

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。

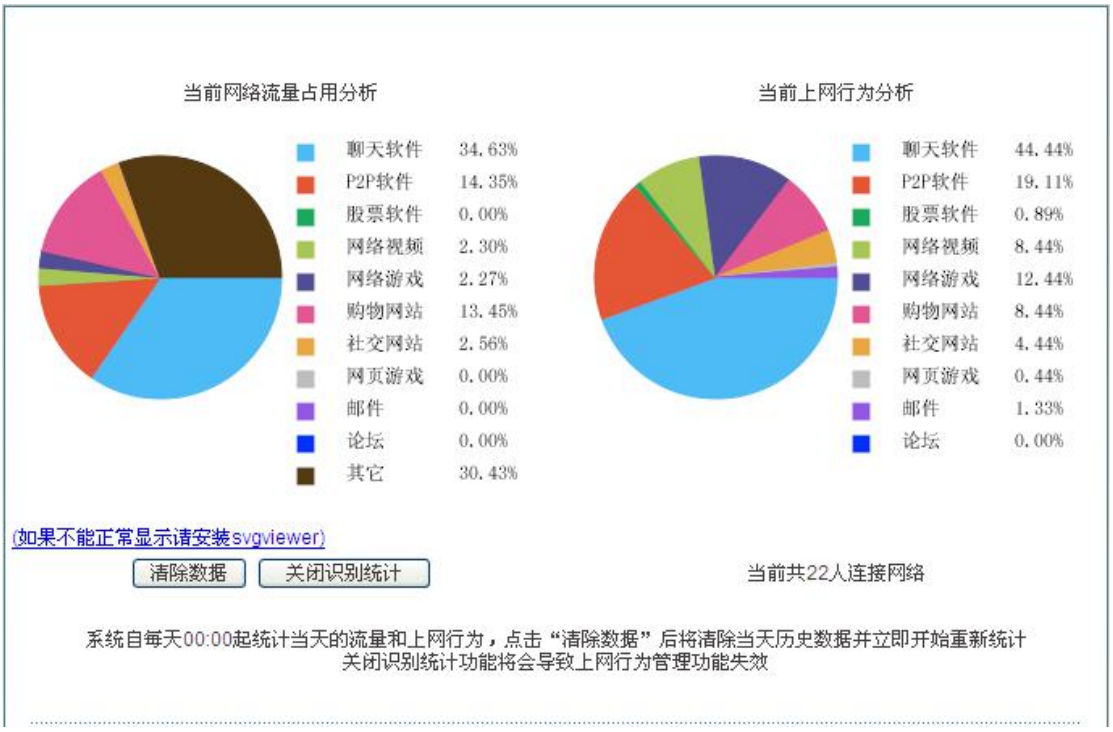


图 9- 1 用户行为分析饼图

- 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。

IP地址	上行(Kbit/s)	上行总流量(Mbit)	下行(Kbit/s)	下行总流量(Mbit)	上网时间	所属组	上网行为	设置	备注
100.100.100.75	0	1	0	13	0天0小时2分46秒				
200.200.202.51	2	0	3	1	0天0小时2分55秒				
100.100.100.69	111	194	84	278	0天0小时33分37秒				
100.100.100.68	0	1597	0	17926	0天14小时22分34秒				
100.100.100.70	1	0	0	0	0天0小时19分59秒				
100.100.100.71	2	17	2	134	0天0小时18分8秒				
100.100.100.72	2	3	3	149	0天0小时9分39秒				
100.100.100.73	2	3	2	8	0天0小时8分50秒				
100.100.100.74	4	1	4	6	0天0小时6分41秒				
200.200.202.136	0	2	0	0	0天0小时8分38秒				
100.100.100.45	1	234	0	1699	0天22小时28分6秒				
100.100.100.54	1	77	1	206	0天19小时37分24秒				
200.200.202.152	0	7	0	0	0天0小时9分50秒				
100.100.100.62	43	124	2366	672	0天17小时2分43秒				
200.200.202.150	0	9	0	0	0天0小时34分35秒				
100.100.100.23	0	0	0	0	0天0小时31分18秒				
200.200.202.76	0	3	0	5	0天0小时38分3秒				
200.200.202.69	0	0	6	6	0天0小时34分36秒				
200.200.202.126	24	17	43	14	0天0小时11分11秒				
200.200.202.9	15	19	4	97	0天0小时25分11秒				

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

本节介绍**用户管理—>IP/MAC 绑定**页面及配置方法。

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

在设备中，通过 IP/MAC 绑定功能完成用户的身份识别工作。使用绑定的 IP/MAC 地址对作为用户唯一的身份识别标识，可以保护设备和网络不受 IP 欺骗的攻击。IP 欺骗攻击是一台主机企图使用另一台受信任的主机的 IP 地址连接到设备或者通过设备。这台主机的 IP 地址可以轻易地改变为受信任的 IP 地址，但是 MAC 地址是由生产厂家添加到以太网卡上的，不能轻易地改变。

9.2.1 IP/MAC 绑定列表

图 9- 3 IP/MAC 绑定全局配置

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

图 9- 4 IP/MAC 实例修改

提示：

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

9.2.2 IP/MAC 绑定配置

图 9- 5 IP/MAC 绑定配置

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

提示：

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

2） 对无效的条目，在绑定的时候系统将跳过无效的配置条目。

9.2.3 IP/MAC 绑定实例

灵活地运用 IP/MAC 绑定功能，可以为内网用户配置上网白名单和黑名单。

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

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

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

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

1） 为内网用户配置上网白名单，步骤如下：

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

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

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

图 9- 6 IP/MAC 绑定信息列表——实例一

2） 为内网用户配置上网黑名单，步骤如下：

第一， 通过配置 IP/MAC 绑定条目来指定非法用户，有两种方法：

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

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

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

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

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：PPPoE 介绍、设备的 PPPoE 的全局配置、PPPoE 账号配置及查看 PPPoE 的连接状态。

9.3.1 PPPoE 简介

PPPoE（Point-to-Point Protocol over Ethernet），即以太网上的点对点协议，它可以使以太网上的主机通过一个简单接入设备连到 Internet 上。PPPoE 协议采用 Client/Server（客户端/服务器）方式，它将 PPP 报文封装在以太网帧内，在以太网上提供点对点的连接。PPPoE 拨号连接包括 Discovery（发现）和 Session（PPP 会话）两个阶段。下面将分别介绍这两个阶段。

1） Discovery 阶段

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

图 9- 9 Discovery 阶段的基本工作流程

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

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

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

2） PPP 会话阶段

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

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

9.3.2 PPPoE 全局配置

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

图 9- 10 PPPoE 服务器全局配置

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

提示：

1) PPPoE 用户修改拨号密码步骤：

（1） 用户打开拨号客户端，使用用户名、密码进行拨号。

（2） 拨号成功后，登录自助服务页面，其地址为：http://192.168.1.1/poeUsers.asp（该地址为设备 LAN 口 IP 地址）。

（3） 在修改密码页面输入用户名、旧密码、新密码、确认密码。

（4） 点击**提交**，显示**操作成功**即密码修改成功。

2) 用户每天只能自助修改 5 次密码。

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

9.3.3 PPPoE 账号配置

进入**用户管理—>PPPoE 服务器—>PPPoE 账号配置**页面，可以查看 PPPoE 账号信息列表。点击**添加新条目**，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，可以使用特殊字符如：@ _ . 。
- 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。
- 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。
- 上传速率限制、下载速率限制：PPPOE 的最大上传、下载速率，0 表示不限制。

- 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。
- 上传速率限制、下载速率限制：此处可以对 PPPOE 账号信息列表中勾选的账号进行批量限速设置（0 表示不限速）。
- 限速：点击该按钮，上传、下载速率限速生效。

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。
- 添加到账号组：将该用户名添加到相应的账号组中，账号组需在**用户管理—>用户组配置**页面进行配置。
- 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。
- 上传速率限制、下载速率限制：该 PPPOE 账号的最大上传、下载速率（0 表示不限制）。

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。

提示：若 PPPoE 账号配置了上传、下载速率，则该账号不再匹配精细化限速。

9.3.4 PPPoE 用户连接状态

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

图 9- 13 PPPoE 连接状态信息列表

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

9.3.5 PPPoE 账号导出

图 9- 14 PPPoE 账号导出

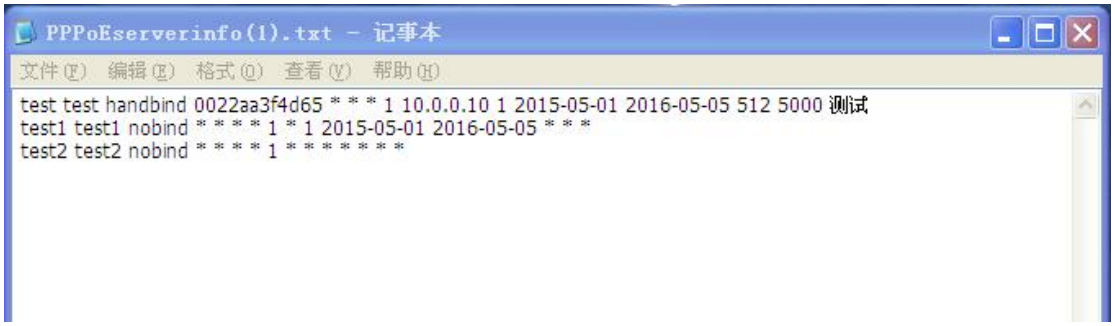


图 9- 15 PPPoE 账号导出

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、MAC 绑定、账号最大会话数、固定 IP 地址、添加到账号组、计费模式、账号开通日期、账号停用日期、上传速率限制、下载速率限制、备注，格式为.txt。

9.3.6 PPPoE 账号导入

图 9- 16 PPPoE 账号导入

提示：

1) 配置 PPPoE 账号批量导入绑定时，其输入格式为“账号+密码”，例如：test 123456，每行只能输入一条配置

2) 注意在上述输入格式中账户与密码之间必须有一个或多个空格。

3) 导入帐号信息时，请参照配置 PPPoE 帐号所对应的项目(注：添加到账号组除外)，若某一项不做配置，请务必用"*"替代。

4) 绑定方式中的不绑定、自动绑定、手动绑定依次对应于导入信息中的 nobind, autoband, handband。

5) 若启用计费模式，请在导入信息对应项配置为"1"，日期格式为"2015-01-01"。

6) 例如:test test nobind * * * * 1 192.168.2.200 1 2015-02-03 2015-03-04 15000 19000 *

9.3.7 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。初始密码分别为：password1、password2、password3，其中 test1、test2 分别绑定 10.0.0.1、10.0.0.2 并开启计费功能（账号的使用期限为 2012 年 10 月 1 日至 2013 年 12 月 31 日）且在账号到期前 15 天进行通告，test3 的最大会话数设定为 5。

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，启用强制 PPPoE 认证和允许用户修改拨号密码（密码的修改提示信息可以通过配置日常事务通告功能告知用户）。

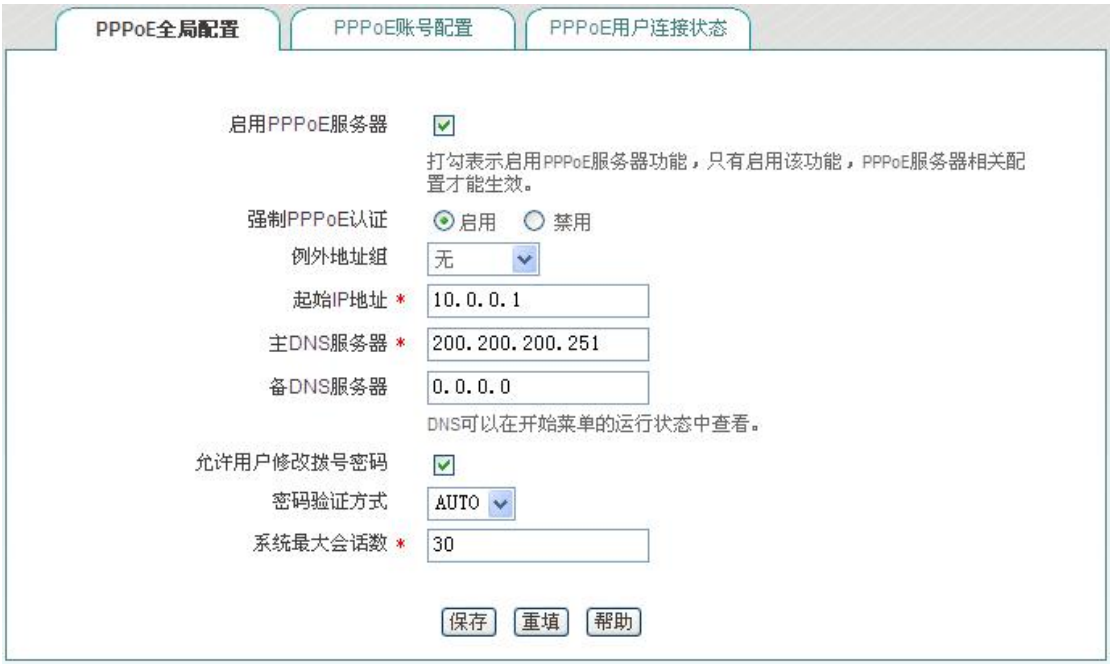


图 9- 17 实例——PPPoE 全局配置

(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- 18 实例——PPPoE 账号配置

(3) 重复步骤 2,配置 PPPoE 用户名为 test2 的账号。将其与 10.0.0.2 进行绑定。配置 test3 的账号，将其的账号最大会话设置为 5。

图 9- 19 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。

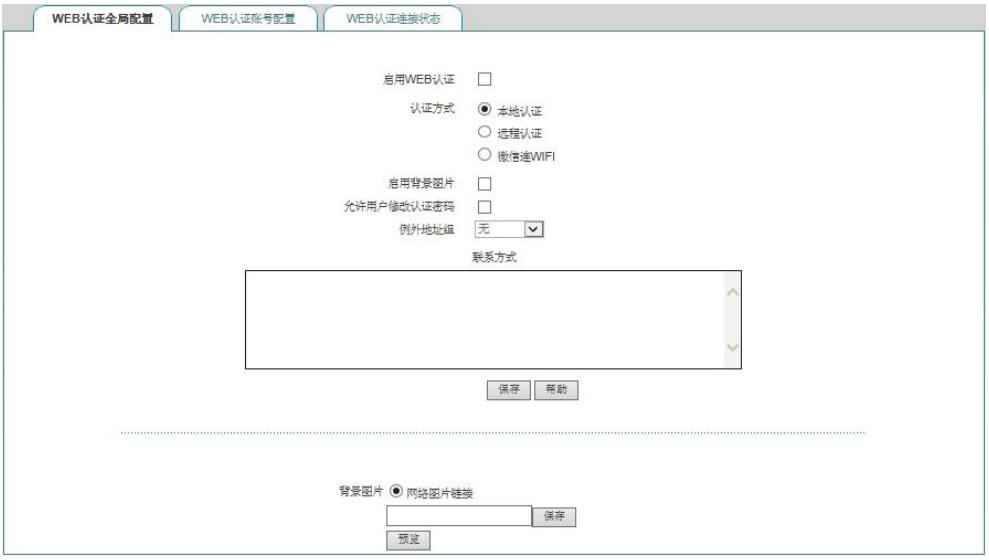


图 9- 20 WEB 认证

- 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。
- 启用背景图片：勾选此选项后，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。
- 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- 21 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。
- 空闲时间：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

图 9- 22 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- 23 WEB 认证账号信息列表

图 9- 24 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- 25 WEB 认证连接状态列表

9.4.4 实名认证

1）实名认证功能简介：

系统能够实现用户刷身份证生成账号密码方式进行上网。为实现该功能，首先到艾泰官网下载身份证阅读器客户端，并安装身份证阅读器。安装该客户端进行配置（注：在客户端的系统配置中：认证服务器 IP 地址必须为路由器 LAN 口 IP 地址，其他配置可以默认）。无需手动操作，周期性自动读取身份证阅读器上证件信息，能够读取二代身份证的信息有：姓名、身份证号、照片等。刷身份证后阅读器客户端自动根据身份证后八位生成上网账号，前六位生成上网密码。当客户离开酒店，管理员需要手动在身份证阅读器客户端注销用户账号，当酒店管理员事先设置的账号时间到期后，身份证阅读器客户端也会自动注销用户账号。

图 9- 26 身份证客户端配置

提示：在安装身份证阅读器时，艾泰产品目前支持华视电子科技公司的：CVR-100U 第二代居民身份证阅读器。

2） 服务器配置

进入**用户管理—>WEB 认证** 页面能够配置设备的 WEB 认证功能中的身份认证。

图 9- 27 身份认证

- 启用 WEB 认证：勾选表示内网用户需通过 WEB 认证才能访问 Internet（若启用身份认证，则必须启用该功能）。
- 启用身份认证：勾选表示启用该功能。此功能必须配合艾泰身份证认证客户端使用。
- 认证成功跳转链接：输入认证成功后需要跳转的页面，点击保存配置生效。
- 点击保存：配置生效。

提示：对于在 9.4.1 中介绍过的参数这里不再一一列出。

9.4.5 WEB 认证账号信息列表

图 9- 28 WEB 认证账号信息列表

图 9- 29 WEB 认证账号信息列表—添加新条目

- 用户名：显示/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/过期日期：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：点击该按钮可进入图 8-26 页面配置 WEB 认证账号信息。
- 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**行为管理—>电子通告**页面配置日常事务通告通知用户如何修改 WEB 认证密码。

2）WEB 认证用户如何安全下线

(4) 用户打开浏览器，使用用户名、密码进行认证。

(5) 认证成功后，在打开的认证成功的对话框中，点击安全下线。

(6) 在打开的来自网页消息对话框中点击确定。

9.4.6 WEB 认证连接状态

图 9- 30 WEB 认证连接状态列表

- 用户名：显示正在使用 WEB 认证用户的用户名。
- IP 地址：显示正在使用 WEB 认证用户的 IP 地址。

提示：在 WEB 认证连接状态列表中的用户名和 IP 地址都是网络中正在使用 WEB 认证用户的用户名和 IP 地址。

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- 31 用户组列表

图 9- 32 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- 33 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- 34 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。

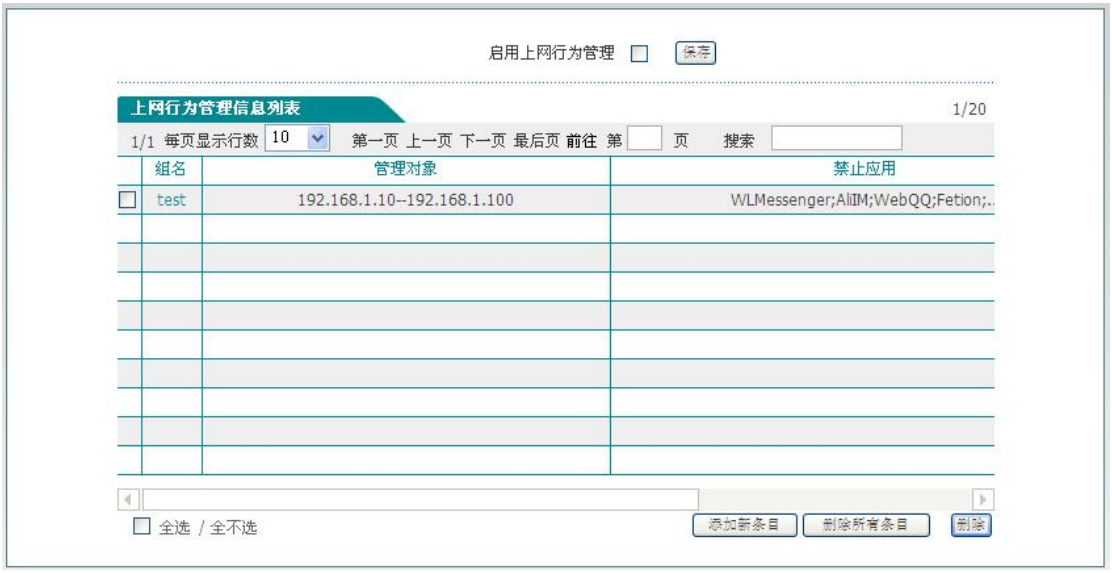


图 10- 3 行为管理信息列表

- 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。

图 10- 4 行为管理配置

- 组名：自定义该条上网行为管理实例的组名，不能重复。
- 选择上网行为管理对象：填写该行为管理实例生效的地址段或用户组。
- 设备支持的上网行为管理有：P2P 软件、股票软件、网络视频、网络游戏、购物网站、社交网站、网页游戏、邮件、论坛等。

- 生效时间设置：设置该上网行为管理实例的生效的时间。

提示：

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

10.2.3用户管理配置实例

1） 需求

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

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

销售部和客服部员工，地址分别为 192.168.1.50~192.168.1.69 和 192.168.1.70~192.168.1.192，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

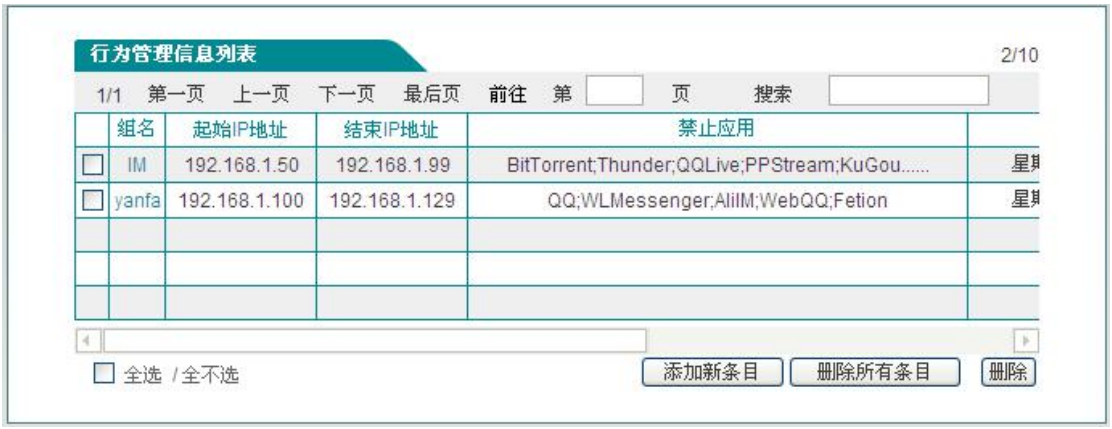


图 10- 5 上网行为管理实例

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。
- **提示：**该版本支持的最大的 QQ 号码为 4294967295。

10.4 MSN 白名单

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

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

图 10- 8 MSN 白名单

- 启用 MSN 白名单：勾选表示启用 MSN 白名单功能。

10.5 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- 9 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

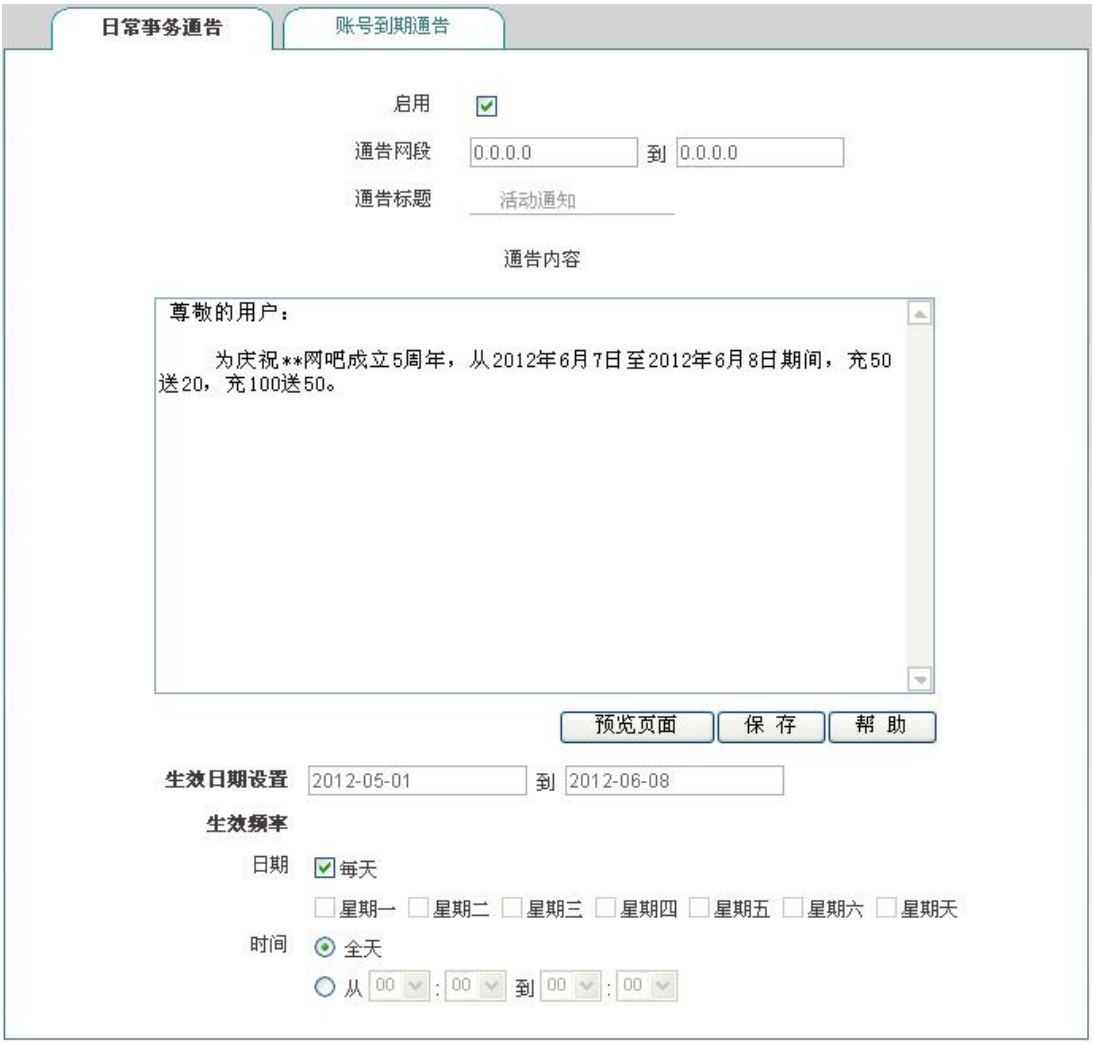


图 10- 10 日常事务通告

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

提示：

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

10.6.2账号到期通告

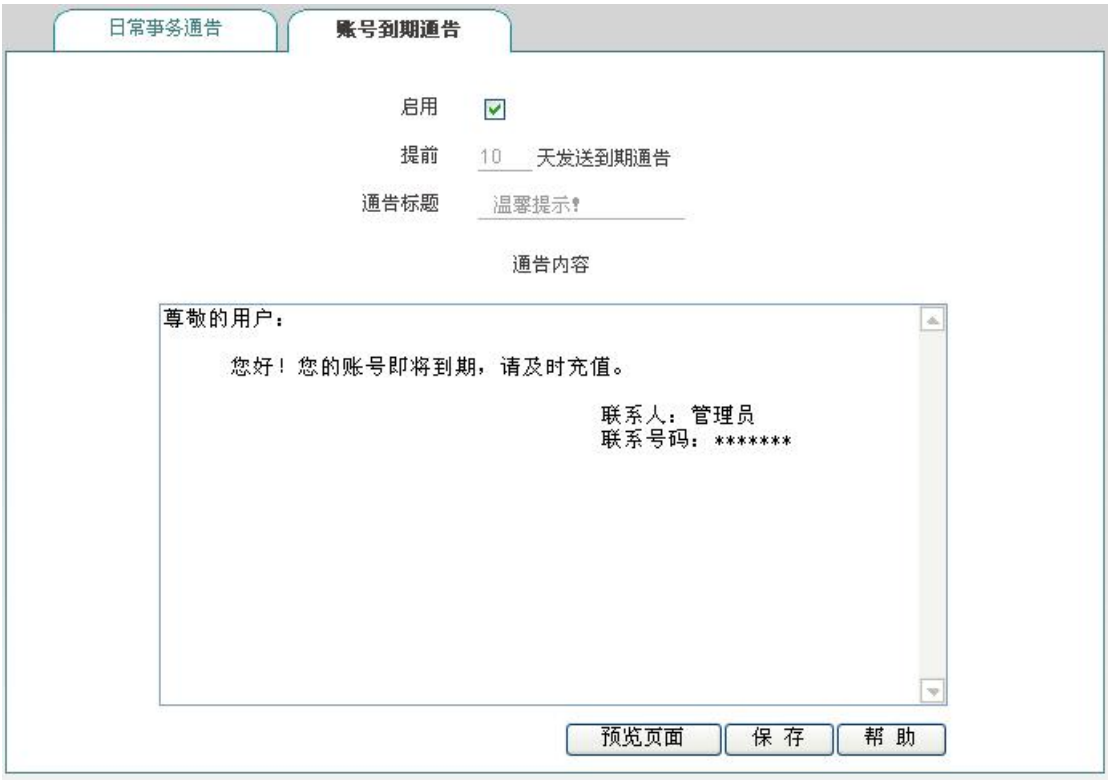


图 10- 11 账号到期通告

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

提示：

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

10.7 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—>日志管理**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。

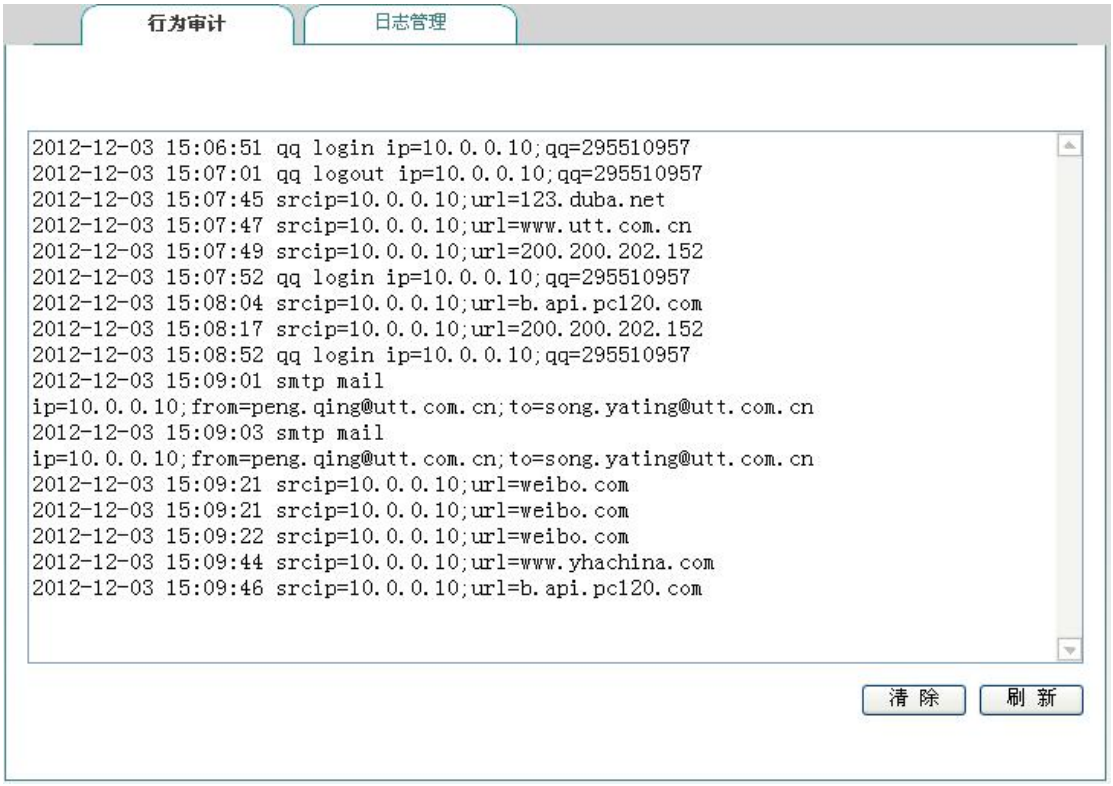


图 10- 12 行为审计

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- 13 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 页面记录用户是否引用行为管理中禁止的功能。
- 论坛日志：启用论坛日志后，将用户使用过的论坛日志发送到 Xport 中，目前支持的论坛有：天涯论坛，篱笆论坛，猫扑论坛，宽带山论坛。
- 微博日志：启用微博日之后，设备会将用户使用过的相关新浪微博日志的信息记录发送到 Xport 中。
- NAT 日志：启用 NAT 日志后，将用户产生的上网会话记录发送到 Xport 上。

提示：论坛日志、微博日志、Nat 日志需配合艾泰 Xport 使用。开启 NAT 日志后会占用较大的带宽，在正常使用时建议不要开启 NAT 日志功能。

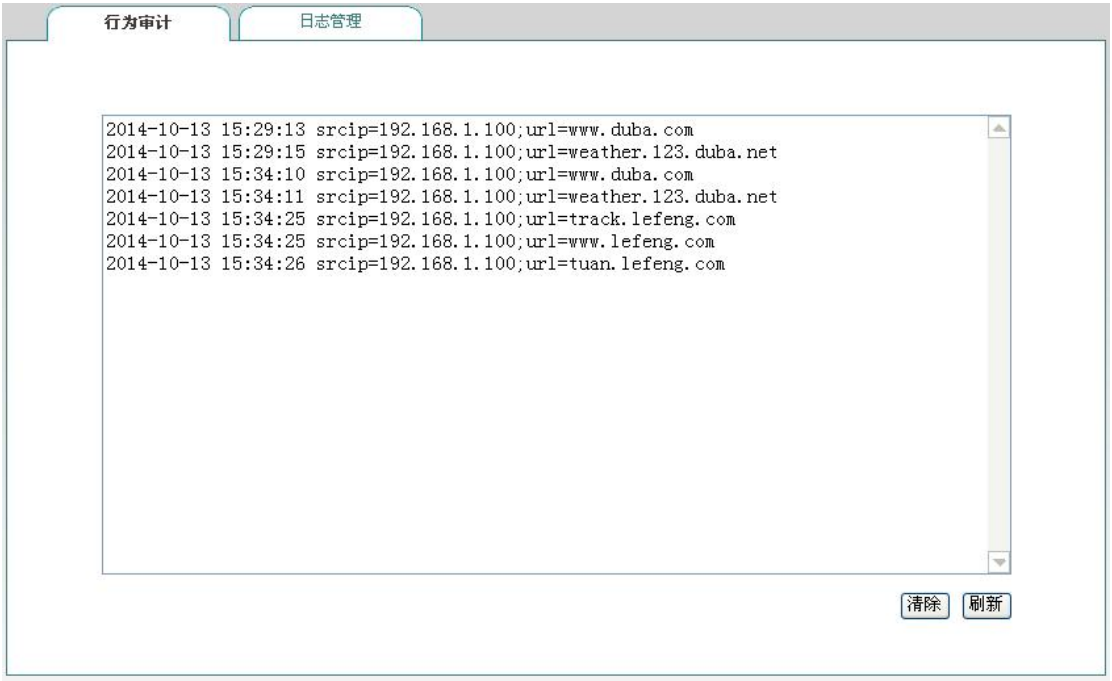


图 10- 14 行为审计

注意：上网行为审计能够记录最新的 400 条日志信息。

10.8 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参数的含义。

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

第 11 章　带宽管理

本章介绍精细化限速和带宽管理功能。

11.1 精细化限速

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

1)　精细化限速列表

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

图 11- 1 精细化限速信息列表

2)　精细化限速配置

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

图 11- 2 精细化限速配置

- 组名：自定义该条精细化限速实例的组名，不能跟其他实例名重复。
- 请选择限速对象：分别可以针对源地址和目的地址的限速，目的地址可选网段也可应用地址组当源网段与目的网段皆符合限速规则时限速功能生效。
- 起始 IP 地址、结束 IP 地址：填写该精细化限速生效的地址段的起始 IP 地址和结束 IP 地址。
- 限速策略：可供的选项有独享和共享；**独享**表示此范围内的每一个 IP 地址使用此带宽；**共享**表示此范围内的 IP 地址共享此带宽。
- 上传速率限制、下载速率限制：在这里设置此范围内 IP 地址的最大上传、下载速率，0 表示不限制。
- 生效时间设置：设置此 IP 地址范围内该条精细化限速生效的时间。

注意：

能添加针对目的地址的限速，目的地址可选网段也可引用地址组。当源网段与目的网段皆符合限速规则时限速功能生效

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：建议不要同时启用弹性带宽功能与精细化限速功能。

图 11- 3 弹性带宽配置

- 启用弹性带宽：勾选表示启用弹性带宽功能。
- WAN 口上、下行带宽：设置从 ISP 申请的 WAN1 口的上、下行带宽。
- 启用游戏和应用加速：勾选表示优先加速游戏带宽。

提示：精细化限速和弹性带宽中，千兆设备限速值支持到 1000M，百兆设备弹性带宽最高只可配置 100M。

11.3 P2P 限速

本节介绍 P2P 限速功能，该功能是基于 P2P 软件的一种特殊限速方法，由于 P2P 软件其巨大的带宽使用，会占用内网的大部分流量，致使网络拥塞，带宽利用率低下。而 P2P 限速规则可针对 P2P 软件对其进行特殊的限速处理，能对常见的 P2P 应用单独限速。从而提高带宽的利用率。

进入**带宽管理—>P2P 限速** 页面，对 P2P 限速进行配置。

图 11- 4 P2P 限速

- 启用 P2P 限速：勾选表示启用 P2P 限速。
- 限速策略：有两种限速策略可供选择：1.每台内网主机的 P2P 流量使用此设定速率。
  2.所有内网主机的 P2P 流量共享此设定速率。
- 上传/下载速率限制：设置上传/下载的最大速率。
- 例外地址组：设置不在 P2P 限速范围内的地址组。
- 生效时间设置：设置 P2P 限速生效的时间。

11.4 连接数限制

本节介绍**带宽管理—>连接数限制**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- 5 连接数限制

- 启用连接数限制：勾选表示启用连接数限制。
- 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 90、**UDP 连接数**不小于 50、**ICMP 连接数**不小于 9。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、域名过滤及 MAC 地址过滤。

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

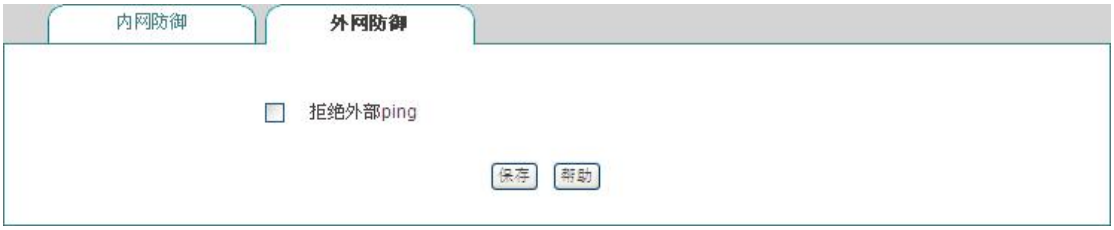


图 12- 2 安全配置——外网防御

- 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

本节讲述**防火墙—>访问控制策略** 的功能及配置方法。

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

12.2.1访问控制策略简介

在设备中配置访问控制策略，可以监测流经设备的每个数据包。默认情况下，设备中没有配置任何访问控制策略，设备将转发接收到的所有合法的数据包。如果配置了访问控制策略，当数据包到达设备后，它会取出此数据包的源 MAC 地址、源地址、目的地址、上层协议、端口号或数据包中的内容进行分析，并按照策略表中的顺序从上至下进行匹配，查看是否有匹配的策略，并执行匹配到的第一个策略所定义的动作：转发或丢弃。并且不再继续比较其余的策略。

可以通过设置**过滤类型**指定访问控制策略的过滤类型，设备提供四种过滤类型：IP 过滤、URL 过滤、关键字过滤以及 DNS 过滤。

1） IP 过滤

IP 过滤指对数据包的包头信息过滤，例如源地址和目的 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：源地址、目的 IP 地址、协议、源端口、目的端口、动作和生效时间等。

2） URL 过滤

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

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

3） 关键字过滤

关键字过滤指对 HTML 页面（网页）中的关键字过滤，它的意思是如果你在某个网页里发

表了包含了定义的关键字（如色情、法轮功、赌博等）的言论，将会提交不成功。

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

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

- 移动到：您可以通过此按钮将实例进行相应的排序。
- 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、关键字过滤以及 DNS 过滤这四种不同的过滤类型下访问控制策略配置中各参数的涵义，以及注意事项。

一、 访问控制策略配置—IP 过滤

图 12- 4 配置访问控制策略——IP 地址过滤

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

与协议名称的对照表。

- 常用服务：提供使用 TCP 协议或 UDP 协议的常用服务端口。其中，选项**所有**表示所有端口：即 1～65535 端口。

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

  附录 D 提供了常用服务端口与服务名对照表。

- 目的起始端口、目的结束端口：该访问控制策略的目的起始端口和结束端口，通过它们可以指定一段范围的目的端口。如果只定义一个目的端口，则将它们设置成同一个值，取值范围均为 1～65535。

- 目的起始地址、目的结束地址：该访问控制策略的目的起始 IP 地址和结束地址，通过它们可以指定一段范围的目的 IP 地址。如果只定义一个目的 IP 地址，则将它们设置成同一个值。

- 源起始端口、源结束端口：该访问控制策略的源起始端口和结束端口，通过它们可以指定一段范围的源端口。如果只定义一个源端口，则将它们设置为同一个值。取值范围均为 1～65535。

- 生效时间设置：访问控制策略的生效的时间，不设置为所有时间。

提示：

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

二、 访问控制策略配置——URL 过滤

图 12- 5 配置访问控制策略——URL 过滤

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

- 过滤类型：这里选择 URL 过滤。
- 过滤内容：该访问控制策略需过滤的 URL 地址。

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

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

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

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

提示：

1. URL 地址中，英文字符不区分大小写。输入 URL 时，请不要包含 http://。
2. URL 过滤不能控制用户使用网页浏览器访问的其它服务。例如，URL 过滤不能控制对 ftp://ftp.utt.com.cn 的访问。在这种情况下，需通过配置 IP 过滤类型的访问控制策略来禁止或允许 FTP 连接。

三、 访问控制策略配置——关键字过滤

图 12- 6 访问控制策略配置——关键字过滤

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

- 过滤类型：这里选择**关键字过滤**。

- 过滤内容：该访问控制策略需过滤的关键字，指网页上的关键字。

提示：

1. 对于过滤类型为**关键字**的访问控制策略，**动作**只有**禁止**这个选项。
2. 过滤的内容应除：〈 〉，％ ‘ \ “ & ； 和空格之外的字符。

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 192.168.1.9-192.168.1.20 的用户使用 WEB 业务。

分析：

自定义策略 1：允许 192.168.1.9-192.168.1.20 的 DNS 应用。

自定义策略 2：允许 192.168.1.9-192.168.1.20 的 WEB 应用。

自定义策略 3：禁止 192.168.1.9-192.168.1.20 其他所有应用。

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

访问控制策略列表：

图 12- 8 访问控制策略——实例一

图 12- 9 访问控制策略——实例一

实例二

需求：某企业网要禁止 IP 地址为 192.168.1.80~192.168.1.90 的用户访问网站 http://www.bbc.com（IP 地址为 29.58.246.93）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 192.168.1.80~192.168.1.90 段用户访问 http://www.bbc.com。

配置策略 2，禁止 192.168.1.80~192.168.1.90 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

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 域名过滤页面

域名过滤配置步骤：

1) 勾选**启用域名过滤。**

2) 选择该域名过滤策略的生效方式。

3) 选择该域名过滤生效的内网对象。

4) 选择该域名过滤生效的时间段。

5) 在**域名名称**对应的文本框中输入相应的域名，点击**添加新条目**按钮。相应的域名就会出现在**域名列表**中。

6) 点击**保存**。

提示：

1) 设备中支持设置 90 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：勾选表示启用，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，设备将会发送通告给此用户，并且到设置的时间后，将跳转到指定的网址。

- 通知标题：用户接受通告信息的标题。

- 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：

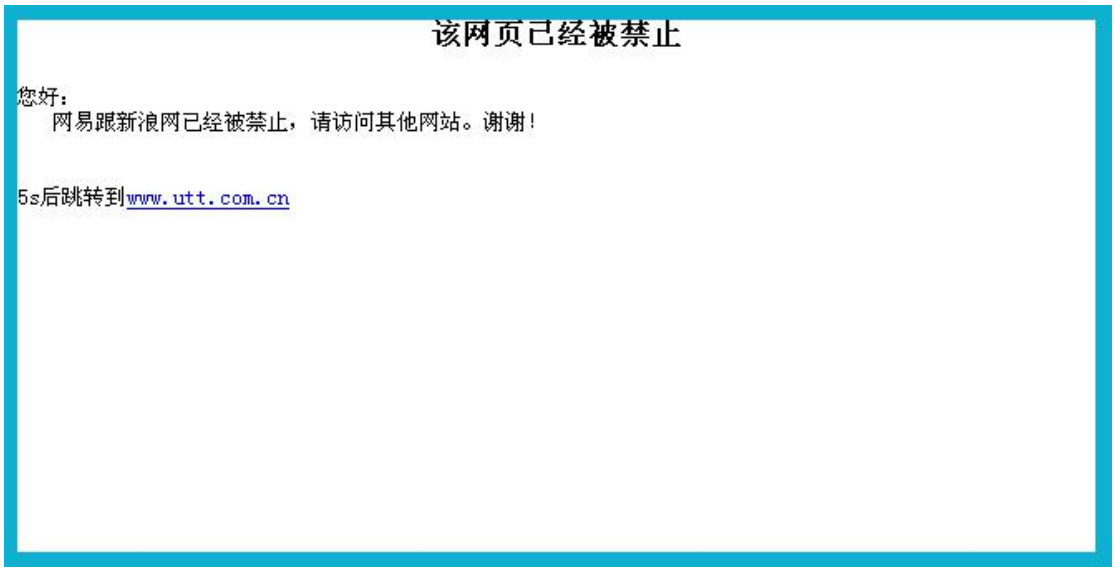


图 12- 14 域名过滤通告页面

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。

12.4.1MAC 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。

12.4.2MAC 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。

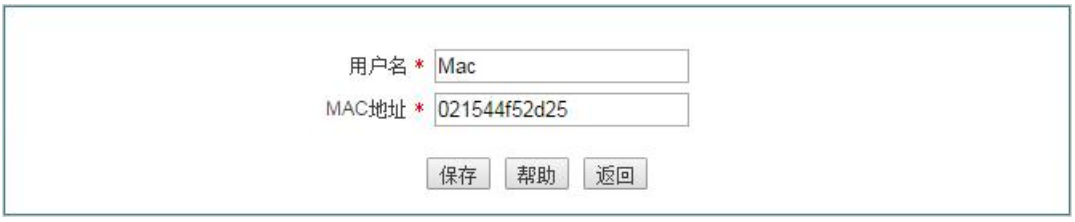


图 12- 16 MAC 地址过滤

- 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

- 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）中建立专用的网络连接的技术，此网络连接采用专有的隧道协议，实现了数据的加密和完整性的校验、用户的身份认证，从而保证信息在传输过程中不被偷窃、篡改、复制等，类似于在公共网络中建立了一个专线网络一样，只不过这个专线网络是逻辑上的而不是物理上的，所以称为虚拟专用网。由于使用 Internet 进行传输相对于租用专线来说，费用极为低廉，所以 VPN 的出现使企业通过 Internet 既安全又经济的传输私有的机密信息成为可能。系统支持四种 VPN，分别是 PPTP、L2TP 和 IPSec。

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。

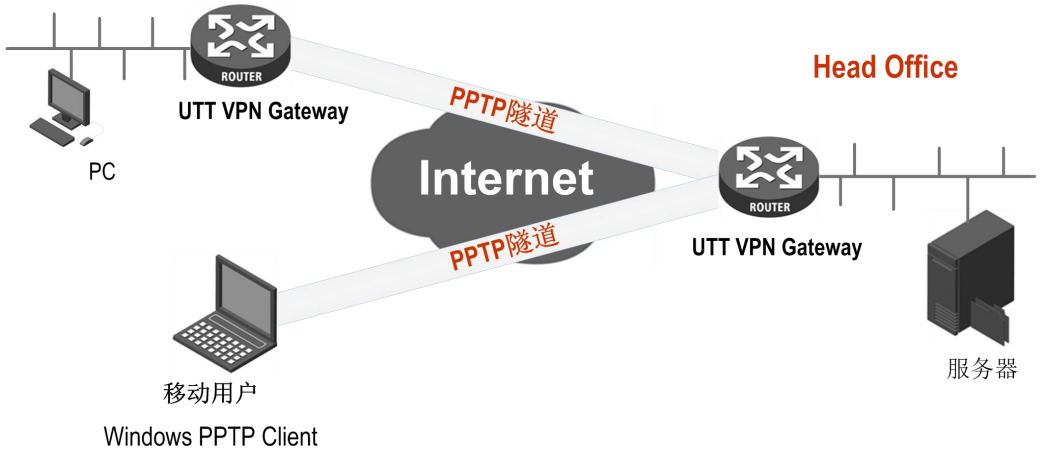


图 13- 1 PPTP 典型应用

13.1.1PPTP 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。

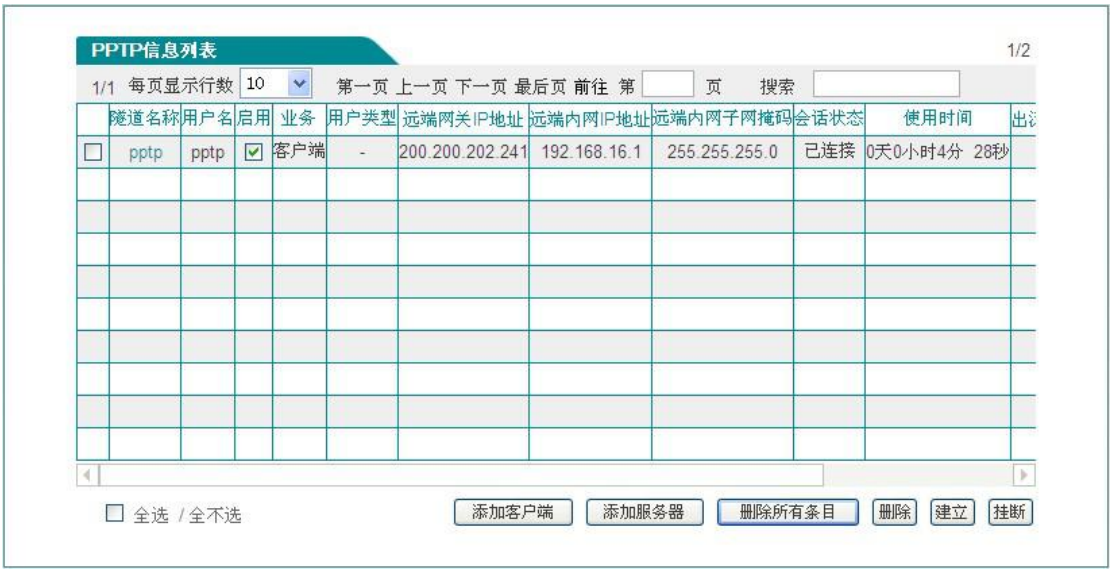


图 13- 2 PPTP 信息列表

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 和 DMZ 配置**的 **NAT 静态映射列表**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。

13.1.2PPTP 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 MS-CHAPV2、PAP、CHAP、ANY（自动和对端设备协商密码验证方式）。
- 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

下面介绍在 PPTP 服务端为 PPTP 客户端配置账号时的各参数的涵义。

图 13- 4 PPTP 服务器——账号配置

- 隧道名称：自定义该条隧道的名称，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）。
- 远端内子网掩码：填写 PPTP 隧道对端局域网所使用的子网掩码。

13.1.3PPTP 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：设置建立 PPTP VPN 的密码验证方式，选项有 MS-CHAPV2、PAP、CHAP、ANY（自动和对端设备协商密码验证方式）。密码验证方式要确保与服务端的一致。
- 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。
- 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。

13.1.4PPTP 配置实例

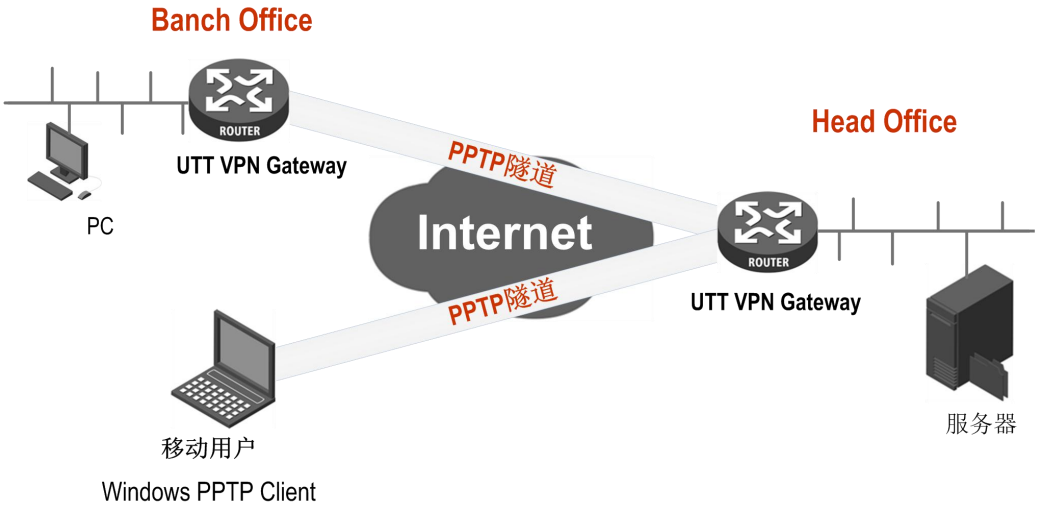


图 13- 6 PPTP 实例拓扑图

在本方案中，某公司总部在上海。在北京有一个分公司希望可以实现两地局域网内部资源的相互访问。该公司还有一些出差和远程办公的移动用户希望在远程访问总公司局域网内部资源。

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，移动用户使用 Windows 操作系统内置的 PPTP 客户端软件，地址如下：

上海网关（PPTP 服务端）：

内网网段：192.168.1.0/24。

LAN 口 IP 地址：192.168.1.1/24。

WAN 口域名：200.200.202.96/24。

北京网关（PPTP 客户端）：

内网网段：192.168.16.0/24。

LAN 口 IP 地址：192.168.16.1/24。

WAN 口 IP 地址：200.200.202.97/24。

移动客户端（PPTP 客户端）：

使用 Windows 操作系统通过 PPTP 拨号建立 PPTP 隧道连接。

配置步骤如下：

1） 配置上海 VPN 网关

图 13- 7 PPTP 服务端配置

为北京分部创建一个账号，用户类型为：LAN 到 LAN。用户名为：pptp。密码为：93456。密码验证方式为：MS-CHAPV2。远端内网网络地址为：192.168.16.1。远端内网子网掩码为 255.255.255.0。

图 13- 8 PPTP 服务端配置——LAN 到 LAN

为移动用户创建一个账号，用户类型为：移动用户。用户名为：pptpyd。密码为：93456。并且为该移动用户分配 192.168.55.41 的固定 IP 地址。

图 13- 9 PPTP 服务端配置-移动用户

2） 配置北京 VPN 网关

图 13- 10 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：93456。密码验证方式为：MS-CHAPV2。远端内网网络地址为：192.168.1.1。远端子网掩码为：255.255.255.0，隧道服务器地址为：200.200.202.96。

3） 配置移动用户

按照以下步骤配置 Windows XP 计算机，使得它能够连接到 PPTP 服务器。

第一步 创建 PPTP 拨号连接：

1） 进入 Windows XP 的**开始—> 设置—> 控制面板**，选择**切换到分类视图**。

2） 选择**网络和 Internet 连接**。

3） 选择**建立一个您的工作位置的网络连接**。

4) 选择**虚拟专用网络连接（V）**，单击**下一步**。

5) 为连接输入一个名字为 Banch2，单击**下一步**。

6) 选择**不拨此初始连接**，单击**下一步**。

7) 输入准备连接的 PPTP 服务器的 IP 地址 200.200.202.96，单击**下一步**。

8) 单击**完成**。

9) 双击 **Banch2** 连接，在 Banch2 连接窗口，单击**属性**。

10) 选择**安全**属性页面，选择**高级（自定义设置）**，单击**设置**。

11) 在**数据加密**中选择**可选加密（没有加密也可以连接）**。

12) 在允许这些协议选中**不加密的密码（PAP）**、**质询握手身份验证协议（CHAP）**、**Microsoft CHAP（MS-CHAP）**、**Microsoft CHAP 版本（MS-CHAP v2）**，单击**确定**。

13) 选择**网络**属性页面，在 VPN 类型选择 **PPTP VPN**。

14) 确认 **Internet 协议（TCP/IP）**被选中。

15) 单击**确定**，保存所做的修改。

第二步　使用 PPTP 隧道连接到设备 PPTP 服务器：

1) 确认计算机已经连接到 Internet（可能是拨号连接或者是固定 IP 接入）。

2) 启动第一步中创建的 Banch2 拨号连接。

3) 输入的 pptp 用户名 test2 和密码 93456。

4) 单击**连接**。

5) 连接成功后，在 MS-DOS 方式下输入 ipconfig，可以看到一个在 PPTP 服务器地址池中的地址，就是 PPTP 服务器分配给本机的 IP 地址。

4） 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- 11 PPTP 服务端信息列表 1

图 13- 12 PPTP 服务端信息列表 2

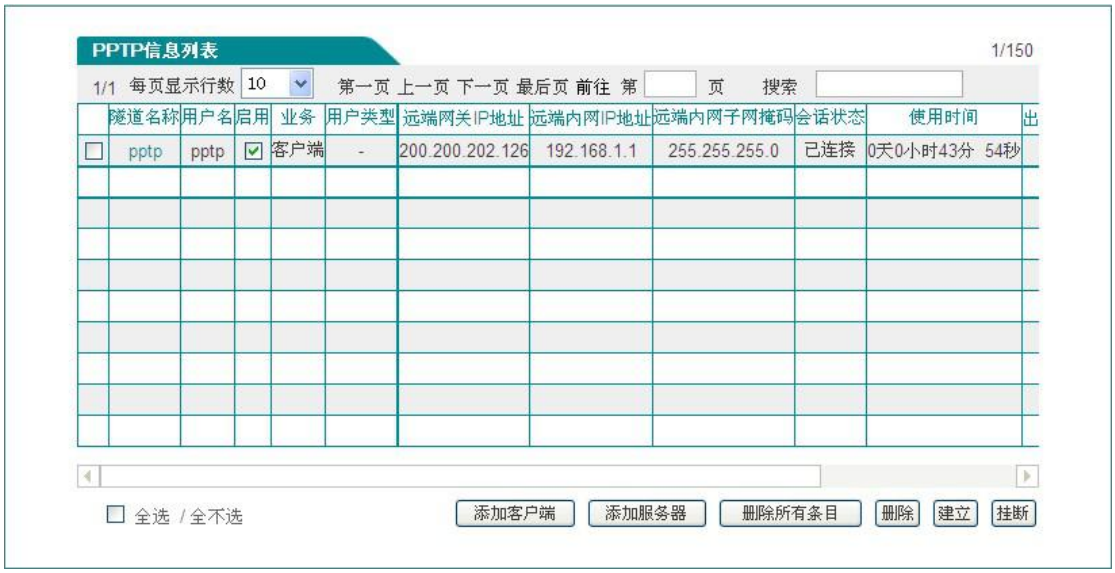


图 13- 13 PPTP 客户端信息列表 1

图 13- 14 PPTP 客户端信息列表 2

13.2 L2TP

L2TP（Layer Two Tunneling Protocol），第二层隧道协议：L2TP 是一种虚拟专用网络协议，已成为 IETF 有关二层隧道协议的工业标准。VPN 网关可以工作在 L2TP 客户端和/L2TP 服务器两种模式下。当 VPN 网关作为 L2TP 客户端使用时，在 L2TP 页面选择“添加客户端”选项卡进入 L2TP 客户端配置界面；当 VPN 网关作为 L2TP 服务器使用时，则选择“添加服务器”选项卡进入 L2TP 服务器配置界面。

提示：

为保证 VPN 网关启用 NAT 后，L2TP 隧道正常连接，L2TP 配置完成之后，系统会自动生成一条 UDP1701 端口。

L2TP 信息列表

图 13- 15 L2TP 信息列表

一旦 L2TP 隧道的配置完成提交以后，即可在 VPN 配置—>L2TP 页面的 VPN 信息列表中查看已建立的 L2TP 隧道的配置及状态信息，各参数含义解释如下：

- 隧道名称： L2TP 隧道的名称。
- 用户名： L2TP 隧道的用户名。
- 业务：该端的业务类型，该值为拨出或拨入。
- 会话状态： L2TP 隧道的当前连接状态，共有 7 种状态。
- 远端内网地址：配置 L2TP 客户端或服务器时填写的远端内网 IP 地址。
- 使用时间： L2TP 隧道连接成功至查看时刻的时间。
- 出流量：通过 L2TP 隧道发出的数据包的统计数量（单位：字节）。
- 入流量：通过 L2TP 隧道接收的数据包的统计数量（单位：字节）。
- 编辑：编辑 L2TP 隧道配置参数。
- 建立：选中某条 L2TP 隧道，单击**建立**按钮，即可通过手动的方式建立该条 L2TP 隧道的连接（仅在业务类型是拨出时可用）。
- 挂断：选中某条 L2TP 隧道，单击**挂断**按钮，即可通过手动的方式挂断该条 L2TP 隧道的连接。

13.2.1L2TP 客户端配置

在 L2TP 页面选择**添加客户端**选项卡，到如下图所示的界面配置 L2TP 客户端参数。

图 13- 16 L2TP 客户端配置界面

- 启用该配置：打钩表示启用该配置。
- 隧道名称：该条隧道的名称，与设备中已有的实例名不能重复。
- 用户名： L2TP 隧道的用户名。
- 密码： L2TP 隧道的用户密码。
- 密码验证方式： L2TP：本地客户端将使用 L2TP 协议和对端服务器协商创建 L2TP 隧道时需要验证密码的方式。
- 远端内网 IP 地址：L2TP 隧道对端局域网所使用的 IP 地址（一般可以填 L2TP 隧道对端设备的 LAN 口 IP 地址）。
- 远端内网子网掩码： L2TP 隧道对端局域网所使用的子网掩码。
- 隧道服务器地址： L2TP 服务器的 IP 地址或者域名（一般填 L2TP 隧道对端设备的 WAN 口 IP 地址或者域名）。

提示：

当 L2TP 隧道两端设备建立连接时，会各用一个虚接口来连接对方。一般情况下， L2TP 服务器会从地址池分配一个 IP 地址作为两个虚接口的路由地址;但是某些 L2TP 服务器并没有配置地址池，此时需要为隧道两端设备的虚接口配置 IP 地址来作为各自的路由地址，即配置对端虚接口 IP 地址、本地虚接口 IP 地址及虚接口子网掩码这三个参数。注意， L2TP 隧道两端设备的虚接口使用同一个子网掩码。

13.2.2 L2TP 服务器配置

在 L2TP 页面选择**添加服务器**选项卡，到如下图所示的界面配置 L2TP 服务器参数。

全局配置：

图 13- 17 L2TP 服务端全局配置

- 启用 L2TP 服务器：勾选后表示启用该服务。
- 密码验证方式：设置建立 L2TP VPN 的密码验证方式，选项有 EITHER、NONE、PAP、CHAP，EITHER（自动和对端设备协商密码验证方式）。
- 地址池起始地址：配置 L2TP 服务器为 L2TP 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 L2TP 服务端时，可以为 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。

账号配置：

图 13- 18 L2TP 服务端账号配置

- 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 L2TP 用户是一个网段的用户，往往是通过一个路由器拨入，实现 L2TP 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 L2TP 隧道远端计算机与本地局域网的通信。
- 用户名：自定义客户端拨号时使用的用户名。
- 密码：自定义客户端拨号时使用的密码。
- 远端内网网络地址：填写 L2TP 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）。
- 远端内子网掩码：填写 L2TP 隧道对端局域网所使用的子网掩码。

13.3 IPSec

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。

13.3.1 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 924 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 98 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。

13.3.2 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 AES98/192/256）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 2：924 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。

13.3.3 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。

13.3.4 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- 19 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。

13.3.5 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。

13.3.5.1 网关到网关

图 13- 20 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 98 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。

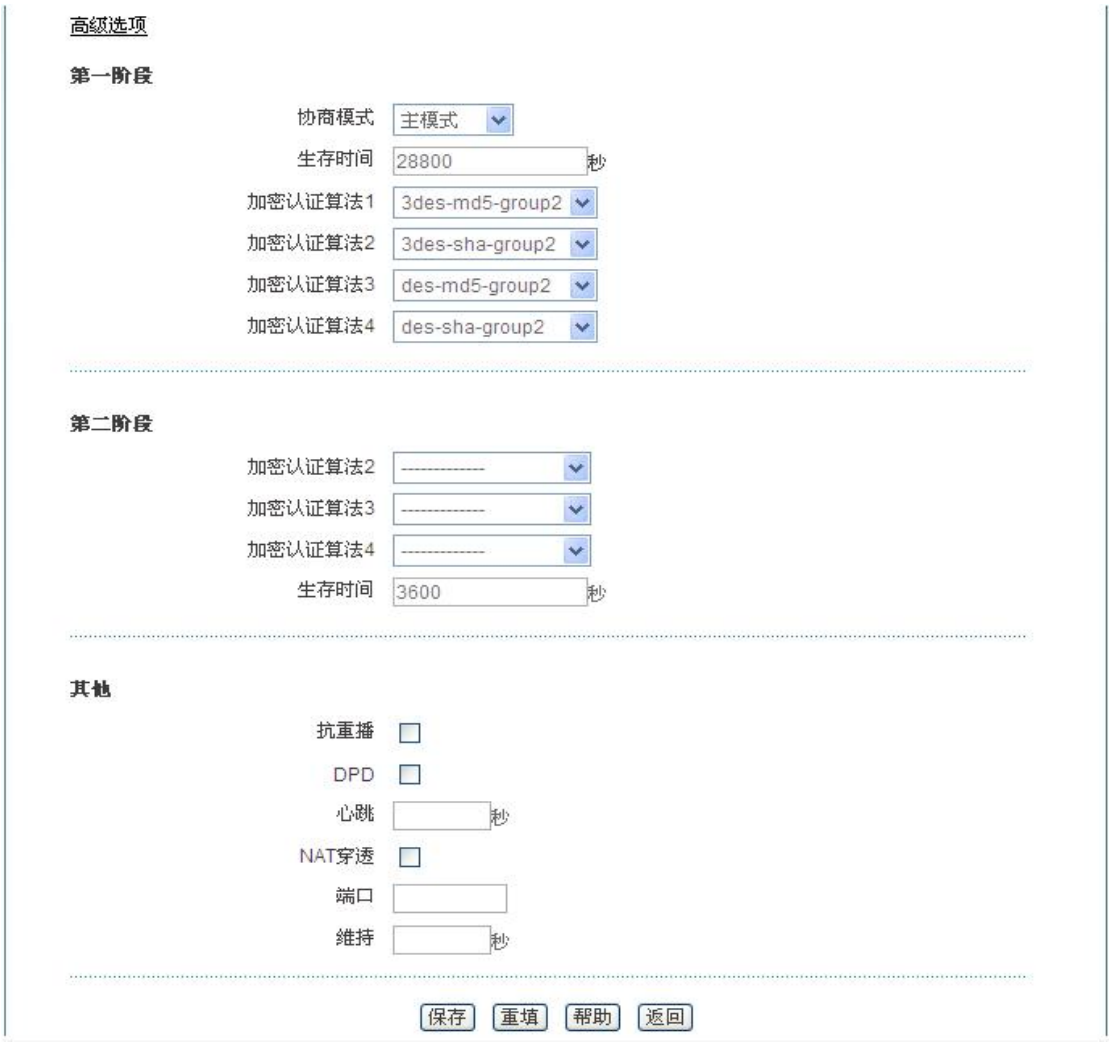


图 13- 21 IPSec 高级选项——主模式

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。

13.3.5.2 动态连接到网关

图 13- 22 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。

13.3.5.3 对方动态连接到本地

图 13- 23 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。

13.3.6 IPSec 配置实例

13.3.6.1 网关到网关

图 13- 24 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- 25 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- 26 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。

3） 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- 27 IPSec 连接状态—上海网关

图 13- 28 IPSec 连接状态—北京网关

13.3.6.2 一方动态

图 13- 29 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- 30 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- 31 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。

3） 查看连接状态

图 13- 32 IPSec 连接状态——对方动态连接到本地

图 13- 33 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

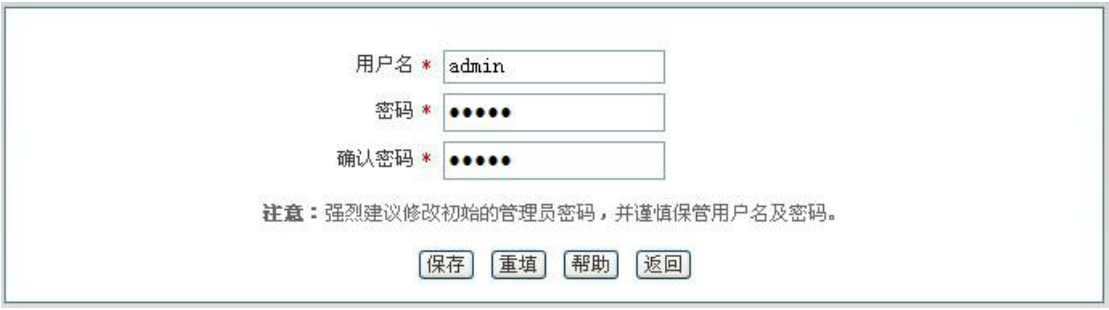


图 14- 2 管理员配置

- 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） 管理员用户名、密码出厂值修改

为安全起见，强烈建议修改初始的管理员用户名及密码，并谨慎保管。

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

14.2 语言选择

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

图 14- 3 语言选择

14.3 时钟管理

本节讲述**系统管理—>时钟管理**页面。

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

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

图 14- 4 时钟管理

- 当前系统时间：显示设备当前的日期和时间信息（单位：年:月:日，时:分:秒）。
- 时区选择：选择设备所在地的国际时区，只有选择了正确的时区，网络时间同步功能才能正常工作。
- 手工设置时间：手工输入当前的日期和时间（单位：年:月:日，时:分:秒）。
- 网络时间同步：使用网络时间同步功能，设置了正确的 ntp 服务器后，当设备连接到 Internet 之后，就会自动和所设置 ntp 服务器同步时间。若需了解更多 ntp 知识及服务器，可访问 http://www.ntp.org。

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

14.4 配置管理

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

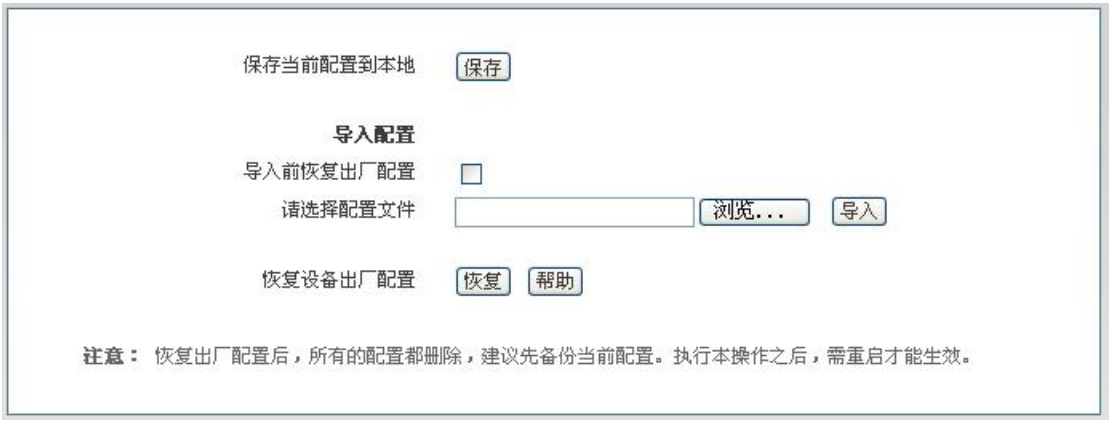


图 14- 5 配置管理

1） **备份配置文件**

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

2） **配置文件导入**

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

提示：在加载配置过程中请不要关闭设备电源，以避免不可预期的错误。

3） **恢复设备出厂配置**

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

提示：

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

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

3) 点击**恢复**后，需重启设备，设备才会恢复到出厂时的配置。

14.5 软件升级

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

图 14- 6 软件升级

- 版本信息：显示设备当前使用的硬件版本、软件版本信息。
- 一键升级：后续如果有更新版本在路由器上可以直接升级。
- 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：

方法一：

如设备检查到最新版本，直接点击一键升级，设备将直接升级到最新版本。

方法二：

第一步　下载最新软件

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

提示：

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

2) 建议升级之前，先到**系统管理—>配置管理**备份系统当前配置。

第二步　选择升级软件所在路径

在**请选择升级文件**文本框中输入将要升级的软件在本地计算机的路径，或者是通过点击**浏览**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**，更新设备的软件。

提示：

1) 强烈建议在设备负载比较轻（用户比较少）的情况下升级。

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

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

4) 升级完成后软件会自动重启并生效，无须人工干预。

14.6 远程管理

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

图 14- 7 远程管理

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

提示：

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

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

3) 如果 WAN 口线路都连接，开启远程管理之后针对所有接口建立静态映射。

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

5) 开启远程管理之后针对所有 WAN 口建立静态映射。

14.7 计划任务

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

1） 计划任务列表

计划任务列表为可编辑列表。您可以对列表中各实例进行操作。

图 14- 8 计划任务列表 1

图 14- 9 计划任务列表 2

2） 计划任务参数介绍

图 14- 10 计划任务配置

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

第 15 章　系统状态

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

15.1 运行状态

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。通过系统信息网络管理员能及时了解网络发生的或潜在的问题，进而有利于网络性能的提高、增强网络安全。

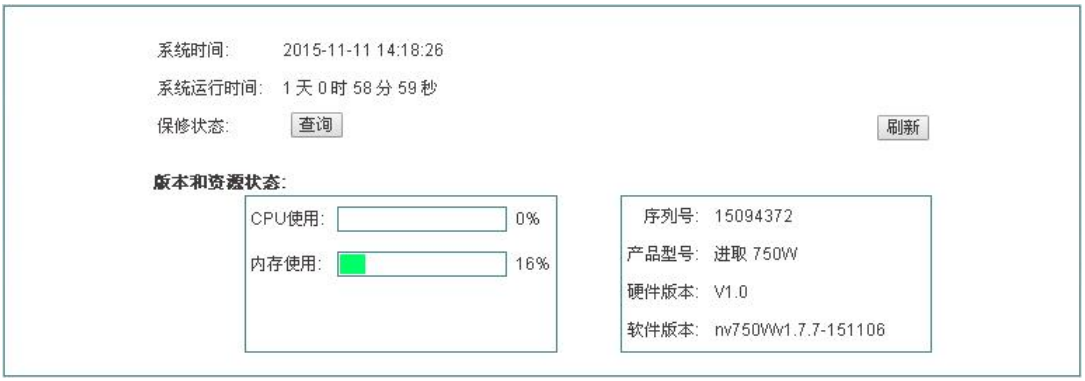


图 15- 1 系统信息

- 系统时间：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。
- 保修状态：点击查询可以查看设备是否在保修期内。
- CPU 占用：显示当前 CPU 占用的百分比。
- 内存使用：显示当前内存使用的百分比。
- 序列号：产品的内部序列号（和表面序列号可能不同）。
- 产品型号：显示设备的产品型号。
- 硬件版本：显示设备的硬件版本号。
- 软件版本：显示设备的软件版本号。
- 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。

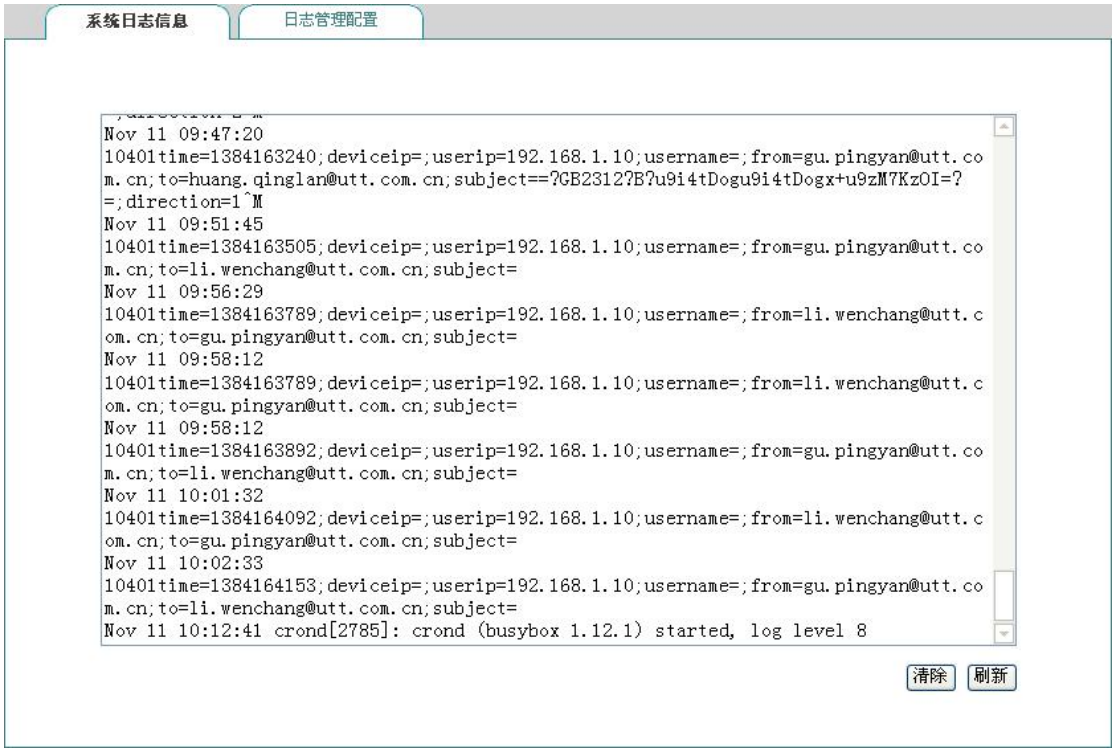


图 15- 2 系统信息

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] NewIP[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 AC 地

	OldIP [IP 地址] Mac[MAC 地址]	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。

15.3.2日志管理配置

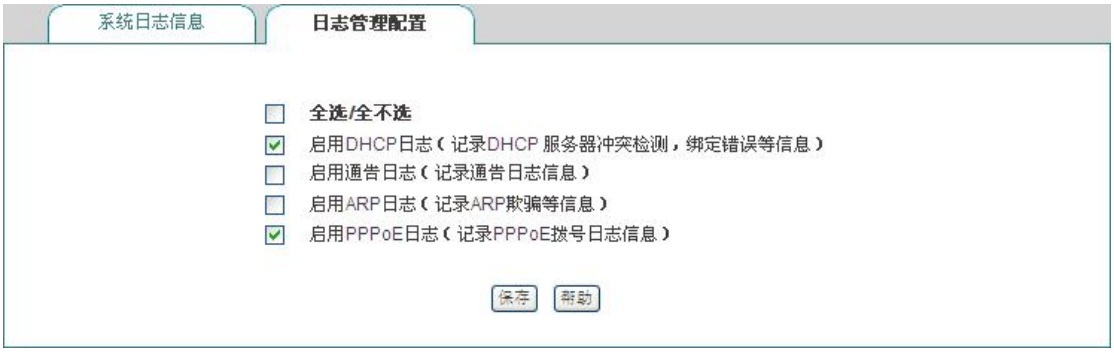


图 15- 3 日志管理配置

- 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公司官方网站的 UTTCare、产品讨论、知识库、预约服务等栏目，以便您更快的了解艾泰科技服务体系，享受艾泰科技提供的贴心服务。

图 16- 1 客户服务

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 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 线路是标准拨号型的（可以使用电脑系统自带 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**中，配置 PPPoE 上网线路的相关参数。
5. 若是包月上网的用户，则可选择拨号类型为**自动拨号**。若是非包月上网的用户，则可选择拨号类型为**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，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 0- 1 线路连接信息列表——查看 PPPoE 拨号线路信息

图 0- 2 PPoE 拨号配置

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**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**中，配置动态 IP 接入线路的相关参数。

提示：

某些动态 IP 接入的时候（比如有线通），Cable Modem 会记录下原先使用该线路的网络设备（如网卡）的 MAC 地址，这样会导致设备无法正常获得 IP 地址，此时需要将设备的 WAN 口 MAC 地址设置成和原有网络设备的 MAC 地址相同。在**网络参数—>WAN 口配置**中，点击高级选项将 WAN 口的 MAC 地址修改为之前网络设备的 MAC 地址，并点击**保存**。

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 0- 3 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。

下面介绍将设备恢复到出厂配置的方法，按知道管理员密码和忘记管理员密码分别说明。

情况一：知道管理员密码

当用户知道管理员密码时，可以通过 WEB 界面来恢复出厂配置。步骤如下：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，单击**恢复**按钮后重启设备，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，可以通过 RESET 按钮来恢复设备的出厂配置。步骤如下：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。

问：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。

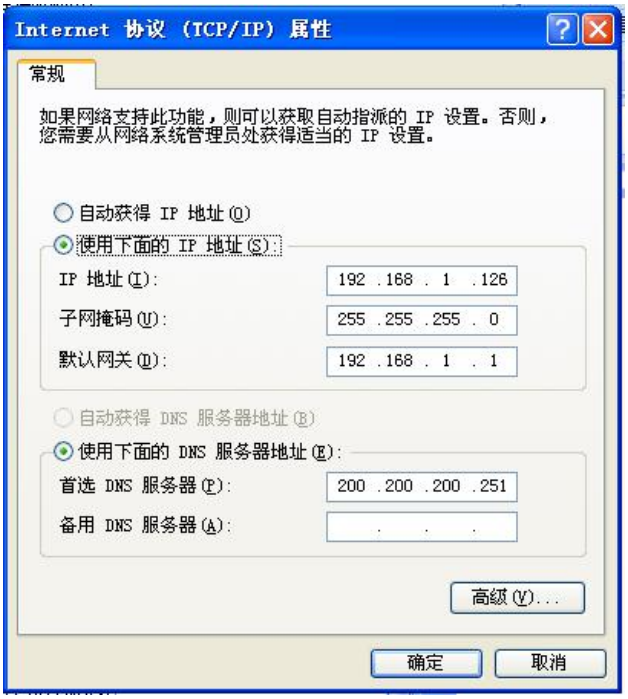


图 A- 2 TCP/IP 属性 IP 地址配置窗口

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。