TP-LINK®

PoE•AC一体化VPN路由器

用户手册

REV1.0.1

1910040793

声明

目录

第1章 用户手册简介

本手册旨在帮助用户正确使用本系列路由器，以TL-R473GP-AC为例进行介绍。PoE•AC一体化VPN路由器系列其他软件配置步骤基本相同，可统一参考TL-R473GP-AC（即本手册）进行配置。

本手册包含对路由器性能特征的描述以及配置路由器的详细说明。请在操作前仔细阅读本手册。

1.1 目标读者

本手册的目标读者为熟悉网络基础知识、了解网络术语的技术人员。

1.2 本书约定

在本手册中，

- 用 **>>** 符号表示配置界面的进入顺序。默认为**一级菜单 >> 二级菜单 >> 标签页**，其中，部分功能无二级菜单；
- 正文中出现的<>尖括号标记文字，表示Web界面的按钮名称，如<确定>；
- 正文中出现的“”双引号标记文字，表示Web界面出现的除按钮外名词，如“ARP绑定”界面。

本手册中使用的特殊图标说明如下：

图标	含义
注意：	该图标提醒用户对设备的某些功能设置引起注意，如果设置错误可能导致数据丢失，设备损坏等不良后果。
说明：	该图标表示此部分内容是对相应设置、步骤的补充说明。

1.3 章节安排

第1章：用户手册简介。帮助快速掌握本手册的结构、了解本手册的约定，从而更有效地使用本手册。

第2章：产品介绍。介绍本系列产品特性、应用以及外观。

第3章：配置指南。指导如何登录路由器Web管理界面，并简要介绍界面特点。

第4章：功能设置。介绍路由器所有功能，帮助用户更充分地使用本系列产品。

附录A：常见问题。

附录B：术语表。

附录C：规格参数。

第2章 产品介绍

2.1 产品描述

TL-R473P-AC/TL-R479P-AC/TL-R473GP-AC/TL-R479GP-AC/TL-R479GPE-AC 是 TP-LINK 专为小微型企业、办公室、别墅等环境开发的多功能路由器产品，内置 AC（无线控制器）和标准 PoE（以太网供电）功能，可统一管理 TP-LINK AP 产品并为其供电，用户无需额外购置 AC 和 PoE 设备，直接搭配 TP-LINK AP 产品即可组建无线网络，管理便捷，性价比高。

TL-R473P-AC/TL-R479P-AC/TL-R473GP-AC/TL-R479GP-AC/TL-R479GPE-AC 同时还支持 Web 认证、微信连 Wi-Fi、IPSec/PPTP/L2TP VPN、上网行为管理、PPPoE 服务器、防火墙、智能带宽控制等丰富的软件功能。

本系列路由器目前具体包含型号如下：

产品型号	类型
TL-R473P-AC	百兆单 WAN 口
TL-R479P-AC	百兆单 WAN 口
TL-R473GP-AC	千兆单 WAN 口
TL-R479GP-AC	千兆单 WAN 口
TL-R479GPE-AC	千兆单 WAN 口

AP管理

- **统一配置：**支持AP管理功能，可自动发现并统一管理TP-LINK企业AP，实现AP频段、信道、发射功率的统一配置，并针对AP进行软件升级；
- **即插即用：**AP接入后由路由器主动下发配置，简化配置流程；
- **无线安全：**支持AP无线网络内部隔离，支持隐藏AP无线网络，保障无线网络安全。

上网行为管理

- **应用限制：**支持针对社交类、视频类、音乐软件类、购物休闲软件类、新闻资讯类、P2P类、金融软件类、网络游戏、应用商店类、基础应用等各种常见应用的一键管控，有效限制可能降低企业员工工作效率的上网行为；同时支持基于地址组和时间段配置管控策略，方便灵活分配上网权限，保障关键用户的正常上网；

- **网址过滤：**通过配置网站过滤和URL关键词，可对员工访问各种网站的权限进行管控，可以禁止/允许员工访问各种网站；此外还支持网站分组功能，可方便地将庞杂的网站进行归类，供过滤规则调用，灵活而实用，同时路由器出厂默认提供十多种网站分组，对于网管资源有限的中小型企业用户，可节省不少配置工作；

- **网页安全：**文件下载过滤；支持过滤文件扩展类型，用户可方便地过滤内嵌在网页中的各种小文件，如exe、rar、swf文件等，避免病毒、木马等通过这些小文件侵入企业网络，危害网络安全；

- **访问控制：**通过配置访问控制策略，可允许或禁止特定应用数据流通过路由器，比如FTP下载、收发邮件、Web浏览等，同时支持基于用户组和时间段配置策略，实现精细化管理；

- **带宽限制：**支持智能带宽控制功能，可根据实际的带宽利用率灵活启用带宽控制策略，可针对网络中每一台主机（IP）进行双向带宽控制，有效抑制BT、迅雷等P2P应用过度占用带宽，避免造成网络游戏卡、上网速度慢的问题，保障网络时刻畅通；

- **连接数限制：**提供基于IP的连接数限制功能，可限制每一台电脑的连接数占有量，合理利用有限的NAT连接数资源，防止少数用户过度占用大量连接数，确保游戏、上网、聊天、视频语音等顺畅进行。

安全管理

- **ARP防护：**支持IP自动扫描及一键绑定功能，有效防止ARP欺骗和非法接入；在遭受ARP欺骗时，路由器可按照指定频率发送ARP更正信息，及时恢复网络正常状态；

- **MAC地址过滤：**支持有线、无线MAC地址过滤；

- **攻击防护：**支持内外网攻击防护功能，可有效防范各种常见的Flood攻击、可疑包攻击行为，如：TCP Syn Flood、UDP Flood、ICMP Flood、WinNuke攻击、防碎片包攻击、WAN口ping、TCP Scan（Stealth FIN/Xmas/Null）等。

VPN

- 提供标准的IPSec VPN功能，支持数据完整性校验、防数据包重传和数据加密功能（DES、3DES、AES128、AES192、AES256等加密算法）， 支持使用IKE建立 IPSec 安全联盟，支持NAT穿透，以及通过域名方式配置VPN连接；

- 提供L2TP/PPTP VPN功能，支持L2TP/PPTP VPN服务器和客户端模式：服务器模式通常部署在企业总部，允许出差员工或分支结构远程安全接入公司网络；客户端模式通常部署在企业分支，可将分支机构网络远程安全接入到公司网络。

认证管理

- **Web认证：**支持本地认证、Radius认证、一键上网等Web认证方式，支持自定义认证页面，也可以配置外部链接作为认证页面，同时可以轻松管理认证用户；

- **微信连WiFi：**实现WiFi与公众号的绑定，通过一键连WiFi为商户引流，并支持强制关注功能；

- **免认证策略：**支持基于地址组或URL的免认证配置，便捷管理认证权限。

高级功能

- **路由设置：**支持基于源目的地址和协议的策略路由、基于目的地址的静态路由的配置，同时支持查看系统路由；
- **NAT设置：**支持NAPT、一对一NAT等多种转发方式，同时支持FTP ALG、H.323 ALG、PPTP ALG、SIP ALG等ALG应用级网关，保证合法应用数据通过防火墙检测；
- **虚拟服务器：**允许外部主机向内部主机主动发起连接，将外部网络访问请求转发到指定的服务器上，同时支持DMZ主机功能；
- **动态DNS：**支持花生壳、科迈、3322等动态域名，通过DDNS，可以将固定域名与动态IP进行绑定，使Internet用户可以通过域名来访问路由器或内网主机；
- **IP流量统计：**基于IP地址统计接收及发送模式下的速率、总流量和总报文，方便用户查看当前网络流量情况；
- **端口监控：**内置简单管理交换机，支持端口镜像功能，满足公安部门的数据监控需求；
- **Port VLAN：**提供基于端口划分VLAN的Port VLAN功能（百兆机型不支持）。

简单易用的管理

- 支持全中文WEB网管，所有功能均可通过图形化界面进行配置，简单方便；
- 每一项配置均提供必要的帮助说明信息，有效降低配置难度。

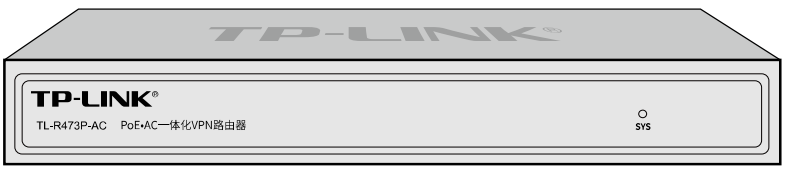
灵活便捷的维护

- 提供系统日志功能，详尽的日志信息便于快速发现网络异常并及时定位问题原因；
- 支持本地及远程管理路由器，方便远程协助；
- 支持Ping检测及Tracert检测，方便快速确认网络连通状态。

2.2 产品外观

2.2.1 TL-R473P-AC/TL-R473GP-AC

TL-R473P-AC/TL-R473GP-AC 前面板如图 2-1 所示：



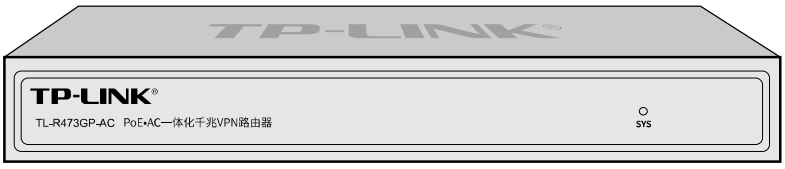


图 2-1 TL-R473P-AC/TL-R473GP-AC 前面板示意图

指示灯含义

指示灯	描述	工作状态	工作说明
SYS	系统指示灯	常亮或不亮	系统不正常
		闪烁	系统正常

TL-R473P-AC/TL-R473GP-AC 后面板如图 2-2 所示：

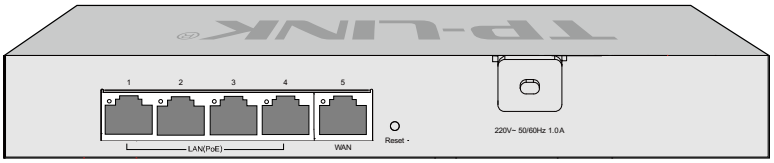


图 2-2 TL-R473P-AC/TL-R473GP-AC 后面板示意图

接口说明

接口	数量		用途
	TL-R473P-AC	TL-R473GP-AC	
WAN	1 个		连接到 DSL/Cable Modem 或 ISP 提供的以太网接口，接入因特网
LAN	4 个		连接计算机或交换机的以太网接口

指示灯含义

指示灯	描述	工作状态	工作说明
Link/Act	状态指示灯	常亮绿色	链路建立
		闪烁	端口正在收发数据
		不亮	链路未建立

Reset 键

复位键。复位操作为：在路由器通电的情况下，使用尖状物长按路由器的 Reset 按键，直至系统指示灯快速闪烁时松开，路由器将自动恢复出厂设置并重启。恢复出厂设置后，默认管理地址为 http://192.168.1.1，首次登录时，用户需自定义用户名和密码。

电源接口

请将电源线插头接到交流电源上。

2.2.2 TL-R479P-AC/TL-R479GP-AC

TL-R479P-AC/TL-R479GP-AC前面板如图2-3所示：

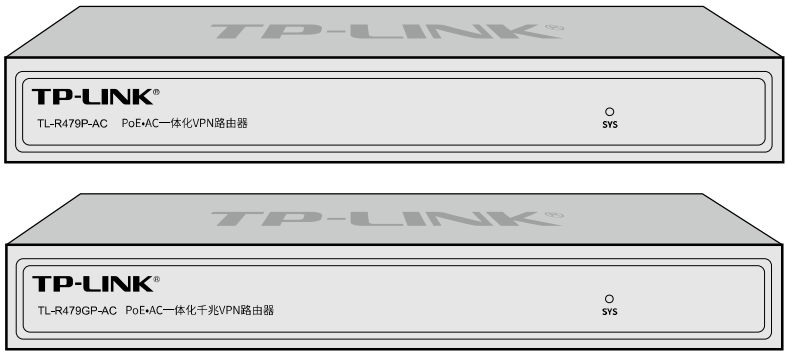


图 2-3 TL-R479P-AC/TL-R479GP-AC 前面板示意图

指示灯含义

指示灯	描述	工作状态	工作说明
SYS	系统指示灯	常亮或不亮	系统不正常
		闪烁	系统正常

TL-R479P-AC/TL-R479GP-AC 后面板如图 2-4 所示：

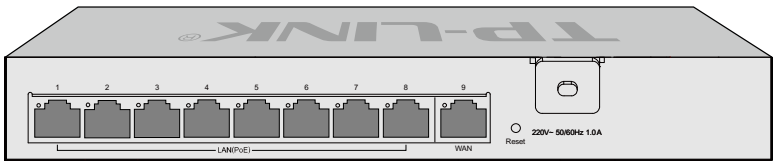


图 2-4 TL-R479P-AC/TL-R479GP-AC 后面板示意图

接口说明

接口	数量		用途
	TL-R479P-AC	TL-R479GP-AC	
WAN	1 个		连接到 DSL/Cable Modem 或 ISP 提供的以太网接口，接入因特网
LAN	8 个		连接计算机或交换机的以太网接口

指示灯含义

指示灯	描述	工作状态	工作说明
Link/Act	状态指示灯	常亮绿色	链路建立
		闪烁	端口正在收发数据
		不亮	链路未建立

Reset 键

复位键。复位操作为：在路由器通电的情况下，使用尖状物长按路由器的 Reset 按键，直至系统指示灯快速闪烁时松开，路由器将自动恢复出厂设置并重启。恢复出厂设置后，默认管理地址为 http://192.168.1.1，首次登录时，用户需自定义用户名和密码。

电源接口

请将电源线插头接到交流电源上。

2.2.3 TL-R479GPE-AC

TL-R479GPE-AC前面板如图2-5所示：

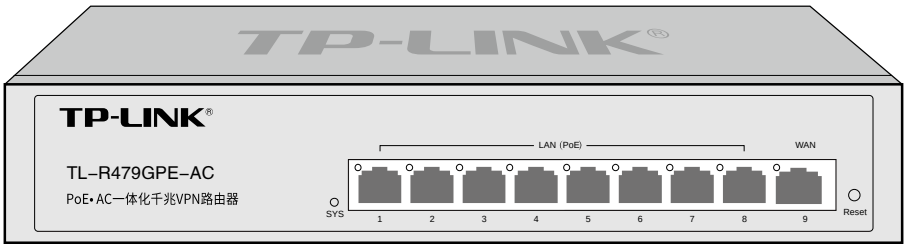


图 2-5 TL-R479GPE-AC 前面板示意图

指示灯含义

指示灯	描述	工作状态	工作说明
SYS	系统指示灯	常亮或不亮	系统不正常
		闪烁	系统正常
Link/Act	状态指示灯	常亮绿色	链路建立
		闪烁	端口正在收发数据
		不亮	链路未建立

接口说明

接口	数量	用途
WAN	1 个	连接到 DSL/Cable Modem 或 ISP 提供的以太网接口，接入因特网
LAN	8 个	连接计算机或交换机的以太网接口

Reset 键

复位键。复位操作为：在路由器通电的情况下，使用尖状物长按路由器的 Reset 按键，直至系统指示灯快速闪烁时松开，路由器将自动恢复出厂设置并重启。恢复出厂设置后，默认管理地址为 http://192.168.1.1，首次登录时，用户需自定义用户名和密码。

TL-R479GPE-AC 后面板如图 2-6 所示：

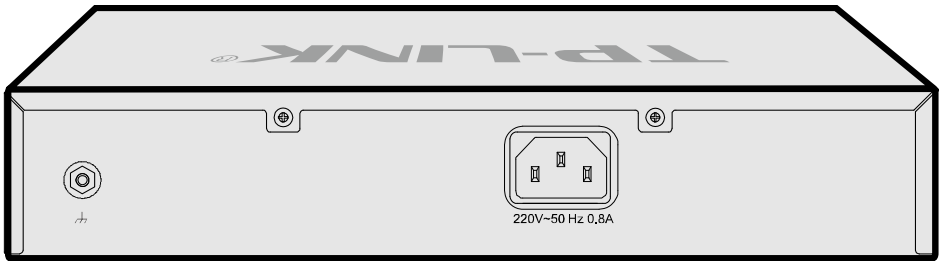


图 2-6 TL-R479GPE-AC 后面板示意图图

电源接口

请将电源线插头接到交流电源上。

第3章 配置指南

3.1 快速安装指南

第一次登录时，需要确认以下几点：

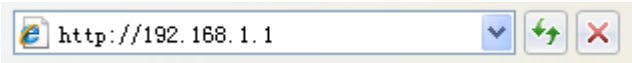
1) 路由器已正常加电启动，任一LAN口已与管理主机相连。

2) 管理主机已正确安装有线网卡及该网卡的驱动程序，且已至少安装一种以下浏览器：IE 8.0或以上版本、FireFox最新版本、Chrome最新版本和Safari最新版本。

3) 管理主机IP地址已设为与路由器LAN口同一网段，即192.168.1.X（X为2至254之间的任意整数），子网掩码为255.255.255.0，默认网关为路由器管理地址192.168.1.1。也可选择“自动获得IP地址”来通过路由器DHCP自动分配IP地址。

4) 为保证能更好地体验Web界面显示效果，建议将显示器的分辨率调整到1024×768或以上像素。

打开IE浏览器，在地址栏输入http://192.168.1.1登录路由器的Web管理界面。



路由器首次登录界面如图3-1所示。首次登录时，需自行设置管理员账号，依次输入用户名及密码，并再次输入密码确认。输入完成之后点击确认，即可在登录页面使用设置好的账号密码进入路由器配置页面。

图3-1 路由器登录界面

成功登录后会弹出设置向导界面，如图3-2所示。如果没有自动弹出，可以单击主页左侧的**快速配置**按钮进入。

图3-2 设置向导

点击<下一步>，对WAN口进行设置。如图3-3所示，提供了三种常见的网络连接方式，请根据ISP（Internet Service Provider，网络服务提供商）提供的服务进行选择。

图3-3 WAN口设置

1) 如果上网方式为“PPPoE拨号”，即ADSL虚拟拨号方式，则需要填写以下内容：

图3-4 上网方式-PPPoE

界面项说明：

用户名	填入ISP指定的ADSL上网账号，不清楚可以向ISP询问。
密码	填入ISP指定的ADSL上网密码，不清楚可以向ISP询问。

2) 如果上网方式为“动态IP”，即可以自动从网络服务商处获取IP地址，则不需要填写任何内容。

3) 如果上网方式为“静态IP”，即拥有网络服务商提供的固定IP地址，则需要填写以下内容：

图3-5 上网方式-静态IP

界面项说明：

IP地址	填入ISP提供的IP地址，不清楚可以向ISP询问。
子网掩码	填入ISP提供的子网掩码，一般为255.255.255.0。
默认网关	填入ISP提供的网关地址，不清楚可以向ISP询问。允许留空。
首选DNS服务器	填入ISP提供的DNS服务器地址，不清楚可以向ISP询问。允许留空。
备用DNS服务器	如果ISP提供了两个DNS服务器地址，则可以把另一个DNS服务器的IP地址填于此处。允许留空。

WAN口设置完成之后，点击<下一步>，在图3-6所示界面，将会显示上一步设置成功的接口信息，若有修改需要，可单击<上一步>回到WAN口设置界面；若无修改需求，单击<下一步>，路由器会自动进行配置并重启，如图3-7所示。重启完成后，会跳转到登录界面，如需对路由器进行其他操作，重新登录即可。

图 3-6 完成设置界面

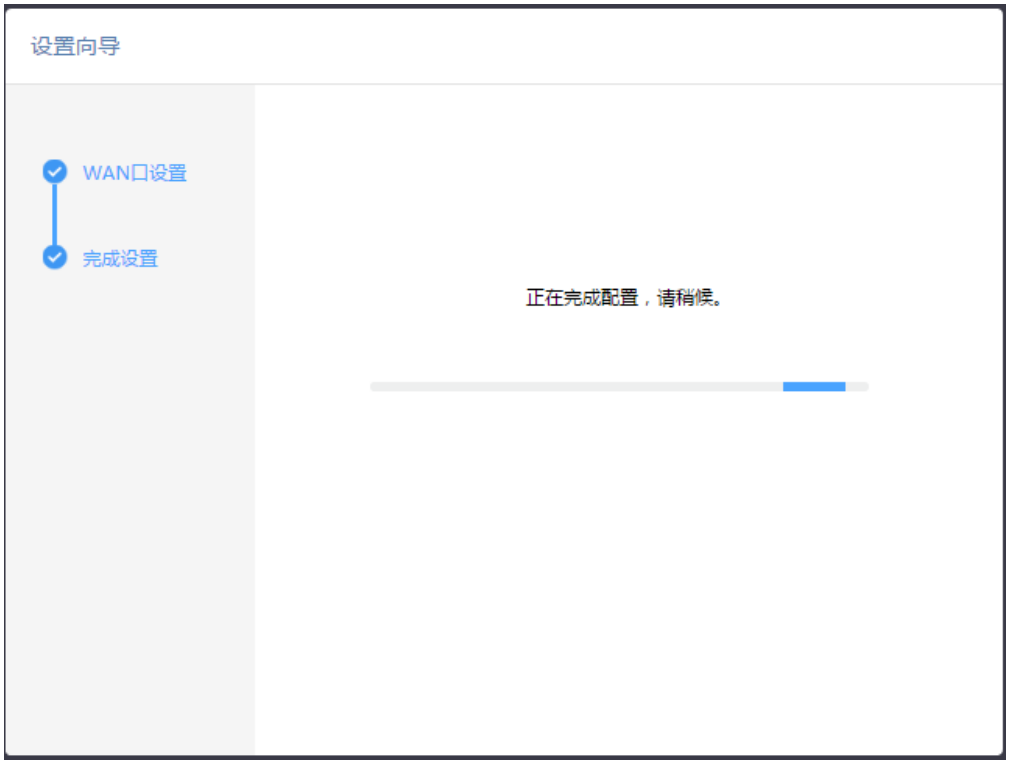


图3-7 路由器自动配置并重启

3.2 Web 界面简介

TL-R473GP-AC典型的Web界面如图3-8所示。

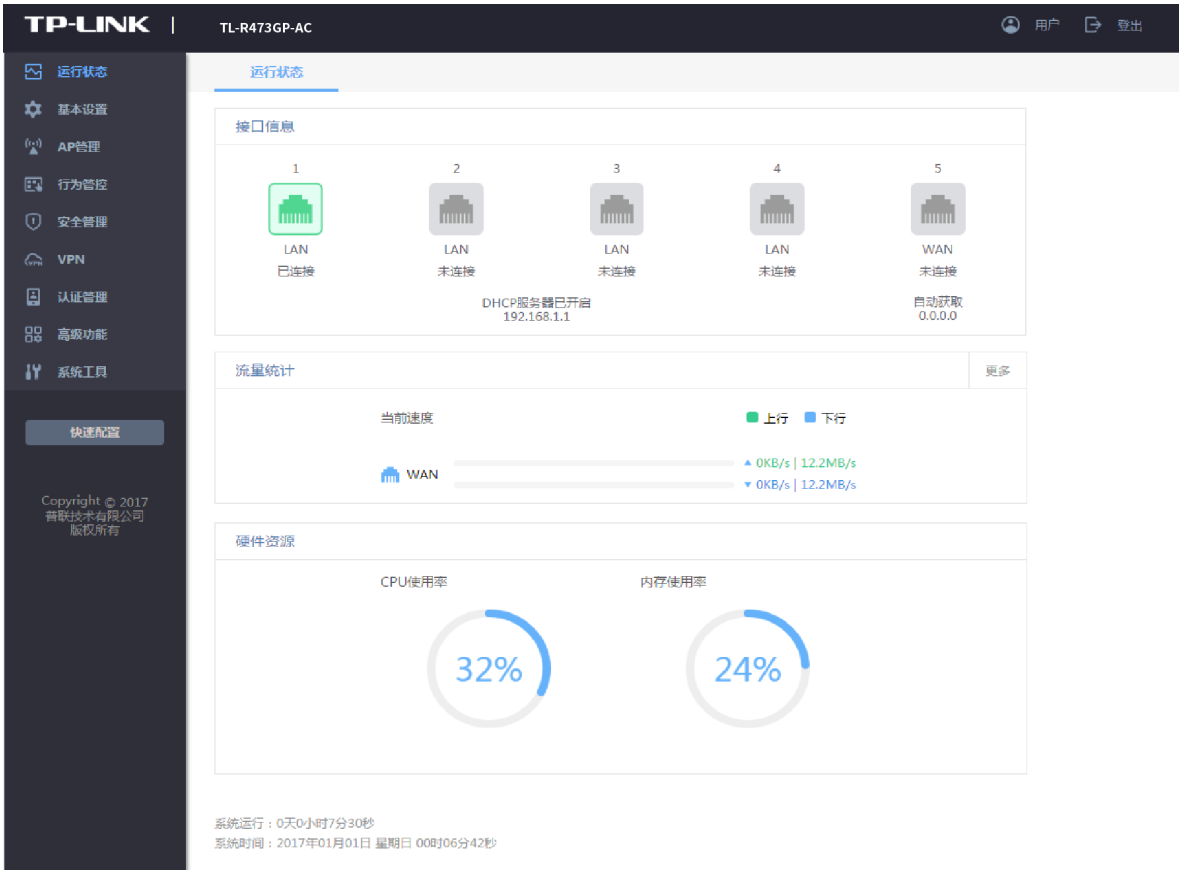


图 3-8 典型Web界面

在图3-9中可以看到，左侧为一级、二级菜单栏，右侧上方长条区域为菜单下的标签页，当一个菜单包含多个标签页时，可以通过点击标签页的标题在同级菜单下切换标签页。右侧标签页下方区域为配置区。

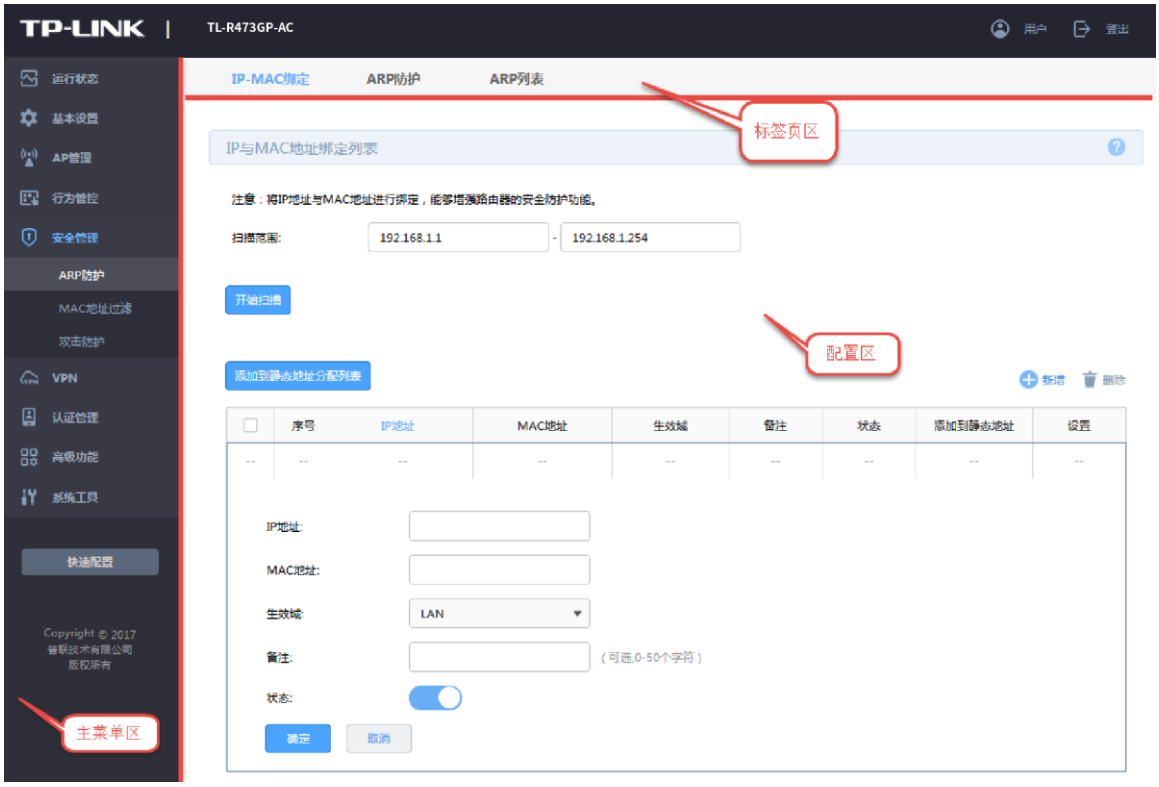


图 3-9 Web界面区域划分

第4章 功能设置

4.1 运行状态

运行状态界面显示路由器当前系统时间、各接口配置信息、无线状态、流量统计以及硬件资源使用情况。

界面进入方法：运行状态

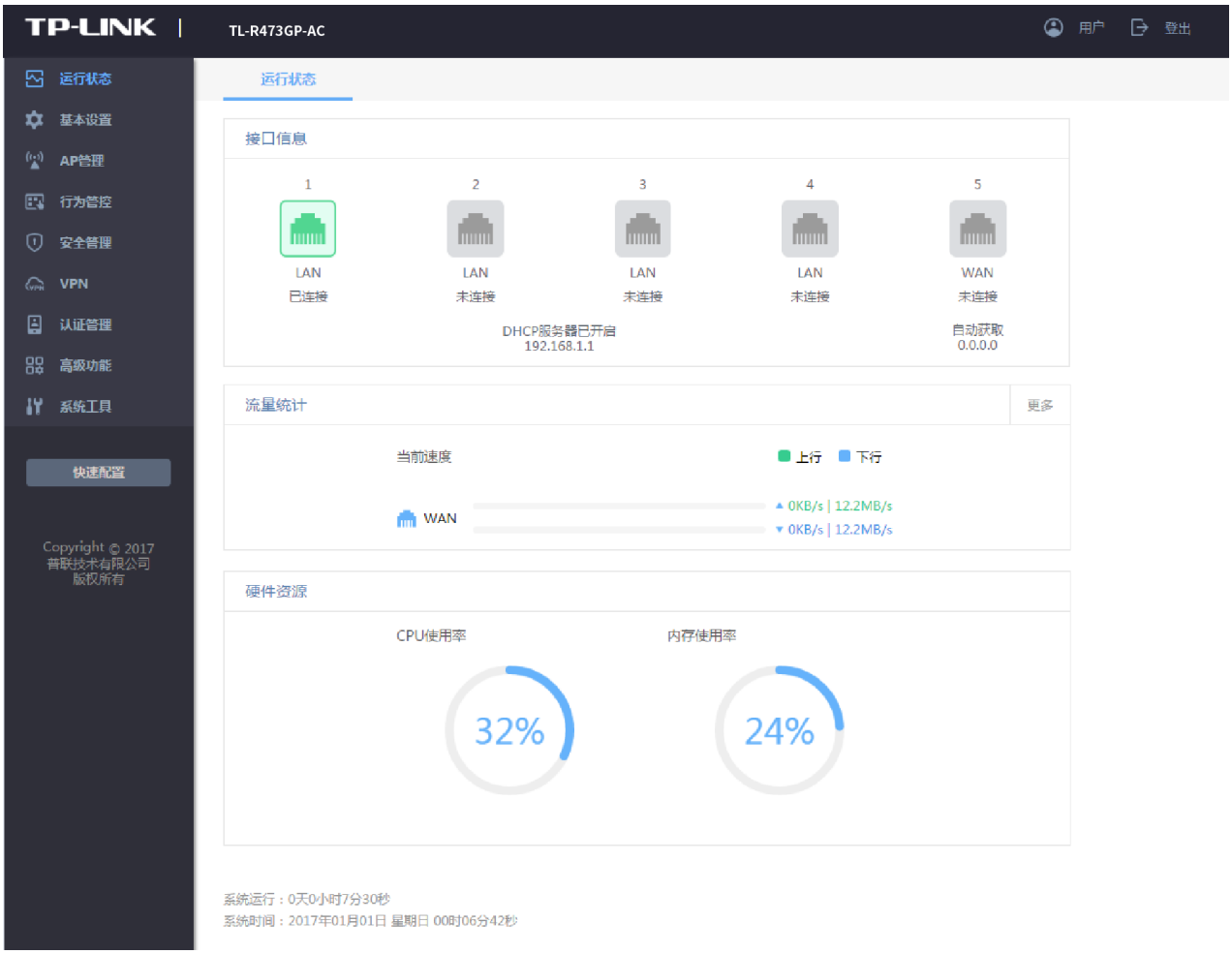


图 4-1 系统状态界面

1) 点击流量统计区域右上角的<更多>选项，即可进入下述页面，查看具体的接口流量统计和IP流量统计：

接口流量界面显示路由器所有正在工作的接口的数据接收/发送速率等流量信息。

图 4-2 接口流量统计界面

界面项说明：

- **流量统计列表**

接口 显示当前统计的接口名称。

发送速率 接口发送数据帧速率，单位为KB/s。

接收速率 接口接收数据帧速率，单位为KB/s。

发送总流量 接口发送的总流量，单位为 MB。

接收总流量 接口接收到的总流量，单位为 MB。

IP流量统计界面将显示接入路由器LAN口的局域网设备向广域网发出数据、从广域网接收数据的流量统计。

图 4-3 IP流量统计界面

界面项说明：

- **IP流量统计列表**

IP地址	显示进行IP流量统计的IP地址。
发送速率	接口发送数据帧速率，单位为KB/s。
接收速率	接口接收数据帧速率，单位为KB/s。
发送总流量	接口发送的总流量，单位为MB。
接收总流量	接口接收的总流量，单位为MB。

4.2 基本设置

4.2.1 WAN 设置

4.2.1.1 WAN设置

TL-R473GP-AC提供三种方式接入广域网：静态IP、动态IP、PPPoE拨号，请根据ISP（Internet Service Provider，网络服务提供商）提供的服务进行选择。

- 有线宽频一般使用动态IP连接方式；
- 光纤接入以及企业、网吧局域网内组网一般使用静态IP连接方式；
- xDSL拨号上网则使用PPPoE连接方式；

界面进入方法：基本设置 >> WAN设置 >> WAN设置

1) 静态IP

若ISP提供了固定的IP地址，请选择“静态IP”手动配置WAN口参数。

图 4-4 WAN 口设置界面-静态 IP 地址

界面项说明：

- **静态IP地址设置**

连接方式	动态 IP：使用运营商动态分配的临时 IP 地址进行上网的方式。 静态 IP：使用运营商提供的固定 IP 进行上网的方式。 PPPoE 拨号：使用运营商提供的宽带帐号和密码进行上网的方式。
IP地址	设置路由器WAN口的IP地址。
子网掩码	设置路由器WAN口的子网掩码。
网关地址	设置路由器WAN口的网关地址。
首选DNS服务器	设置DNS（Domain Name Server，域名解析服务器）地址，一般由ISP提供，允许留空。
备用DNS服务器	设置备用DNS地址，一般由ISP提供，允许留空。
上行/下行带宽	请填写运营商提供的实际上下行带宽，当使用多 WAN 口的流量均衡模式时，路由器会根据该值进行流量均衡的计算。
MTU	数据包的最大传输单元，动静态 IP 可设置范围为 576 ~ 1500，PPPoE 可设置的最大范围是 576~1492。
WAN口速率	设置 WAN 口速率以及双工模式。
WAN口MAC地址设置	设置路由器对广域网的 MAC 地址，一般情况下不需要更改此地址。某些地区的运营商会将线路与 MAC 地址进行绑定，同时提供一个“有效的 MAC 地址”，此时只有将 WAN 口的 MAC 地址设置为该“有效的 MAC 地址”才可以正常共享上网。
在线检测模式	在线检测是通过 PING 和 DNS 检测接口是否在线： 自动：PING 检测选择网关指定互联网地址作为目的地址，DNS 检测选择接口的 DNS 服务器作为目的地址。 永远在线：不对接口进行任何在线检测，接口状态一直在线。

2) 自动获取IP地址

若ISP提供DHCP自动分配地址服务，请选择“自动获取IP地址”来自动获取WAN口参数。

图 4-5 WAN口设置界面-自动获取IP地址

界面项说明：

- **自动获取IP地址设置**

主机名	网络中其他设备看到该路由器的名称，缺省为空。
上行/下行带宽	请填写运营商提供的实际上下行带宽，当使用多 WAN 口的流量均衡模式时，路由器会根据该值进行流量均衡的计算。
MTU	数据包的最大传输单元，动静态 IP 可设置范围为 576 ~ 1500，PPPoE 可设置的最大范围是 576~1492。
首选DNS服务器	设置DNS（Domain Name Server，域名解析服务器）地址，一般由ISP提供，允许留空。
备用DNS服务器	设置备用DNS地址，一般由ISP提供，允许留空。
WAN口速率	设置 WAN 口速率以及双工模式。
WAN 口 MAC 地址设置	设置路由器对广域网的 MAC 地址，一般情况下不需要更改此地址。某些地区的运营商会将线路与 MAC 地址进行绑定，同时提供一个“有效的 MAC 地址”，此时只有将 WAN 口的 MAC 地址设置为该“有效的 MAC 地址”才可以正常共享上网。
在线检测模式	在线检测是通过 PING 和 DNS 检测接口是否在线： 自动：PING 检测选择网关指定互联网地址作为目的地址，DNS 检测选择接口的 DNS 服务器作为目的地址。 永远在线：不对接口进行任何在线检测，接口状态一直在线。 手动模式：手动指定 PING 检测和 DNS 检测的地址，判断接口是否在线。

3) PPPoE拨号

若使用xDSL/Cable Modem拨号接入互联网，ISP会提供上网账号及密码，请选择PPPoE连接方式。

图 4-6 WAN口设置界面-PPPoE

界面项说明：

➢ **PPPoE拨号设置**

用户名	PPPoE拨号的用户名，由ISP提供。
密码	PPPoE拨号的密码，由ISP提供。
连接模式	• **手动连接**：用户可在需要上网时手动点击<连接>按钮连入互联网，适合按小时计费的拨号连接上网方式。 • **自动连接**：每次接通路由器电源，路由器便自动拨号连入互联网，适合不限时间的包月计费拨号连接上网方式。 • **定时连接**：设置连接时段，在此时段内路由器如果开启则自动拨号连接，适合用于需要限时上网的场合。
服务名	填入 ISP 提供的服务名称。如若不是运营商特别要求，请勿填入。
上行带宽	设置当前WAN接口数据流出的带宽大小。
下行带宽	设置当前WAN接口数据流入的带宽大小。
MTU	数据包的最大传输单元，动静态 IP 可设置范围为 576 ~ 1500，PPPoE 可设置的最大范围是 576~1492。
首选DNS服务器	设置DNS地址，一般由ISP提供，允许留空。
备用DNS服务器	设置备用DNS地址，一般由ISP提供，允许留空。
WAN口速率	设置 WAN 口速率以及双工模式。
WAN口MAC地址设置	设置路由器对广域网的 MAC 地址，一般情况下不需要更改此地址。某些地区的运营商会将线路与 MAC 地址进行绑定，同时提供一个“有效的 MAC 地址”，此时只有将 WAN 口的 MAC 地址设置为该“有效的 MAC 地址”才可以正常共享上网。
在线检测模式	在线检测是通过 PING 和 DNS 检测接口是否在线： 自动：PING 检测选择网关指定互联网地址作为目的地址，DNS 检测选择接口的 DNS 服务器作为目的地址。 永远在线：不对接口进行任何在线检测，接口状态一直在线。 手动模式：手动指定 PING 检测和 DNS 检测的地址，判断接口是否在线。

4.2.1.2 ISP 选路

您可以通过本页面设置进行 ISP 选路设置，导入 ISP 数据库。

界面进入方法：基本设置 >> WAN设置 >>ISP选路

图 4-7 ISP选路设置界面

界面项说明：

- **接口设置**

数据库路径	可以导入 ISP 数据库对系统预设的 ISP 选路进行升级。
接口	选择 ISP 选路的出接口。
ISP	选择 ISP（Internet Service Provider，网络服务提供商）。
状态	控制该条目是否启用，滑块为灰色表示禁用，滑块为蓝色表示启用。

4.2.2 LAN 设置

4.2.2.1 LAN 设置

您可以通过本页面设置 LAN 接口。

界面进入方法：基本设置 >> LAN设置 >>LAN设置

图 4-8 LAN设置界面

界面项说明：

➢ **接口设置**

IP地址	本路由器的 IP 地址，局域网中所有计算机的默认网关应设置为该 IP 地址。
子网掩码	本路由器对局域网的子网掩码，一般为 255.255.255.0，局域网中所有计算机的子网掩码应与此处设置相同。
MAC地址	本路由器的 MAC 地址，不可更改。

说明：

若LAN口IP地址有修改，必须在保存配置后使用新的LAN口地址登录路由器Web管理界面。并且，局域网内所有计算机网关地址、子网掩码必须与修改后的LAN口设置保持一致，才能正常通信。

4.2.2.2 DHCP服务

DHCP 服务器能够自动给局域网当中的设备分配 IP、子网掩码等 TCP/IP 协议参数。

界面进入方法：基本设置 >> LAN设置 >> DHCP服务

图 4-9 DHCP服务设置界面

界面项说明：

➢ **服务设置**

DHCP服务	DHCP 服务器有两种状态，分别为开启和关闭，滑块为蓝色表示开启，滑块为灰色表示关闭。
开始/结束地址	DHCP 服务器自动分配的 IP 的开始/结束地址。
地址租期	自动分配的 IP 的有效时间，超过该时间后局域网内的设备将重新获取 IP。
网关地址	可选项，默认为空，此时生效的网关为路由器的 LAN 口 IP 地址。
缺省域名	设置本地网域名，允许留空。
首选DNS服务器	设置DNS地址，推荐设为路由器LAN口IP地址，允许留空。

备用DNS服务器	设置备用DNS地址，允许留空。
Option60	可选项，请填入厂商信息。具体厂商信息请咨询相关厂商，例如 TP-LINK 的厂商信息为 TP-LINK。
Option138	可选项，请填入 AC（无线控制器）IP 地址。

说明：

当开启AP管理功能时，系统将设置option60/option138参数为“TP-LINK”及当前设备的LAN地址，参数在此情况下不能被更改。

4.2.2.3 客户端列表

您可以在本页面查看 DHCP 的客户端相关信息。

界面进入方法：基本设置 >> LAN设置 >> 客户端列表

图 4-10 客户端列表界面

界面项说明：

➢ **DHCP客户端列表设置**

主机名	由 DHCP 服务器分配 IP 的客户端主机名。
MAC地址	分配到 IP 地址的客户端主机的 MAC 地址。
IP地址	DHCP 服务器分配给客户端主机的 IP 地址。
剩余租期	DHCP 服务器所分配 IP 地址的剩余有效使用时间，超时将重新分配。
添加到静态地址	点击“添加”按钮，路由自动将目前已经学习到的 IP 与 MAC 条目添加到静态地址分配列表中。

如要获得最新DHCP服务分配的客户端信息，请点击<刷新>按钮；如需清空客户端条目，请点击<清空>按钮。

4.2.2.4 静态地址分配

您可以在本页面为指定的 MAC 地址预留 IP 地址。当该主机向 DHCP 服务器请求分配 IP 时，服务器将为其分配预留的 IP 地址。

界面进入方法：基本设置 >> LAN设置 >> 静态地址分配

图 4-11 静态地址分配设置界面

界面项说明：

- **新增**

MAC地址	预留 IP 地址的主机 MAC 地址。
IP地址	为指定主机预留的 IP 地址。
备注	您可以设置静态地址分配条目备注，以方便您管理和查找。备注最多支持 32 个字符。
状态	控制该条目是否启用，滑块为灰色表示禁用，滑块为蓝色表示启用。

- **地址列表**

在静态地址列表中，可以对已保存的静态IP地址分配规则进行相应操作。

图 4-11 序号 1 规则的含义：MAC 地址为 00-19-83-65-53-CF 的客户端，指定其 IP 地址为 192.168.1.105，该规则已启用。

4.3 AP 管理

4.3.1 AP 设置

4.3.1.1 AP 设置

您可以通过本页面来查看 AP 的设置。

界面进入方法：AP管理 >> AP设置>>AP设置

图 4-12 AP设置页面

界面项说明：

- **AP设置**

AP管理功能	打开或关闭路由器的 AP 管理功能。
显示类型	选择需要显示的某种类型的 AP，可选择的类型为：在线 AP 设备、离线 AP 设备、所有 AP 设备。
AP设备数量	选中类型的 AP 设备的数量。
设备名称	显示 AP 的名称。
软件版本	显示 AP 当前运行的软件版本。
频段	显示 AP 当前的射频单元。
设备接入	显示 AP 射频单元关联客户端的当前数目和最大数目。
信道	显示 AP 射频单元实际工作的信道值。
发射功率	显示 AP 射频单元的当前发射功率。

- **设置页面**

设备名称	设置 AP 的名称。
设备型号	显示 AP 的硬件型号。
设备状态	显示 AP 的运行状态：在线或离线。
MAC地址	显示 AP 的 MAC 地址。
软件版本	显示 AP 当前运行的软件版本。
升级	导入该机型的升级软件，对该型号的所有 AP 进行升级。
硬件版本	显示 AP 的硬件版本。
LED	打开或关闭 AP 的 LED 指示灯。

➢ **射频列表**

频段	显示需要设置参数的 AP 射频单元。
最大接入设备数量	设置 AP 射频单元关联客户端的最大数目。
信道	设置 AP 射频单元实际工作的信道。
发射功率	设置 AP 射频单元的发射功率。
射频模式	设置 AP 射频单元的工作模式。
频段带宽	当射频模式支持 11n 或者 11ac 时，设置频段带宽。

4.3.1.2 AP 数据库

本栏用于导入 AP 数据库文件以支持新 AP 机型的识别和管理。

界面进入方法：AP管理 >> AP设置 >> AP数据库

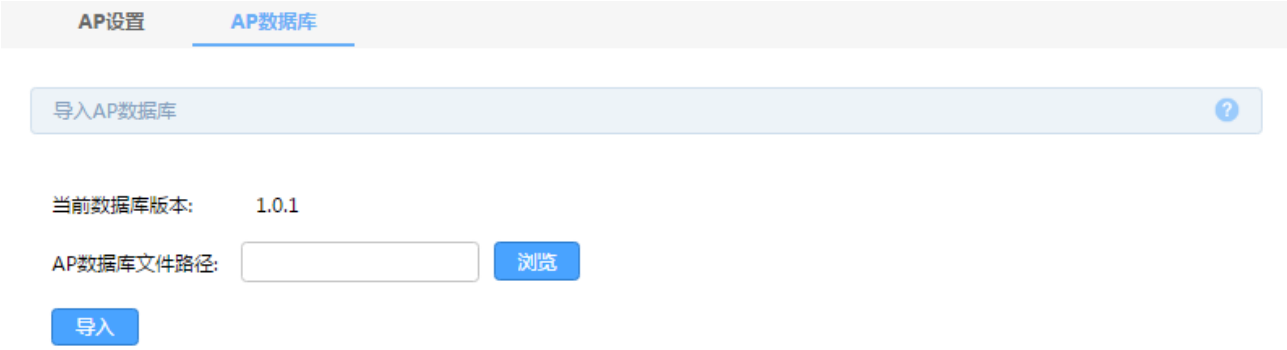


图 4-13 AP数据库页面

界面项说明：

➢ **AP设置**

当前数据库版本	显示当前设备使用的 AP 数据库的版本号。
AP数据库文件路径	需要导入的 AP 数据库文件所在的路径。

4.3.2 无线网络设置

4.3.2.1 即插即用

您可以通过本页面进行 AP 即插即用的设置。当 AP 首次接入时，会自动同步本页面的基本无线服务条目。

界面进入方法：AP管理 >> 无线网络设置 >> 即插即用

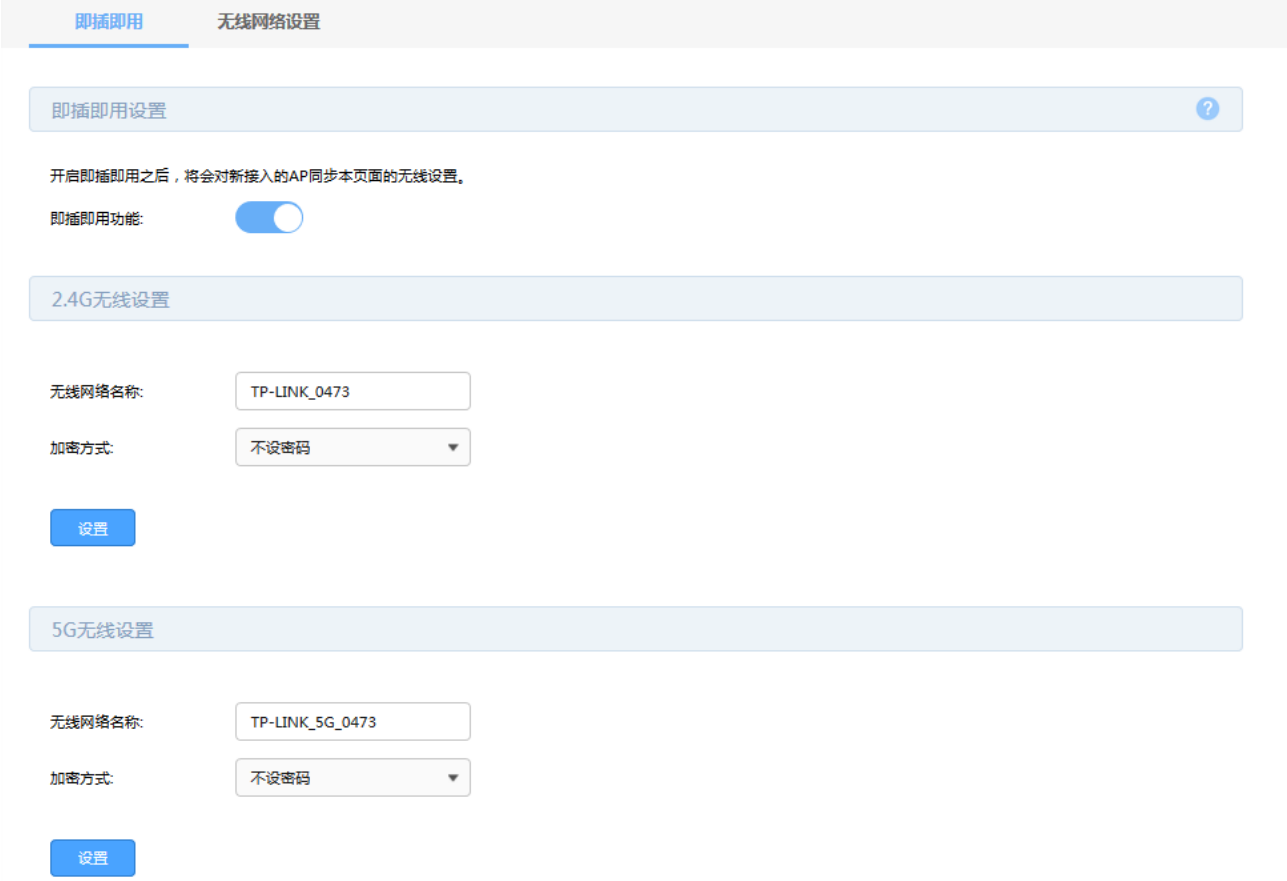


图 4-14 即插即用设置页面

界面项说明：

➢ **即插即用设置**

即插即用功能　　滑块为灰色表示禁用即插即用功能，滑块为蓝色表示启用即插即用功能。

➢ **2.4G无线设置**

无线网络名称（SSID）　　下发到 AP 的无线(Wi-Fi)名称。

SSID编码方式　　当 SSID 不包含中文时，该选项会隐藏，当 SSID 包含中文时，该选项会显示，可以选择 UTF8 和 GBK 两种编码方式对包含中文的 SSID 进行编码。

加密方式　　用于无线网络连接时的加密方式，有三种加密方式可选。

不设密码：无线终端无需密码即可连接到 AP 上。

WPA-PSK/WPA2-PSK(推荐)：使用 WPA2-PSK/WPA-PSK 加密方式，该加密方式无需自设认证服务器，设置无线密码即可。

WPA/WPA2:使用 WPA/WPA2 加密方式，该加密方式需要自行配置 Radius 服务器进行相关认证。

如下图所示，加密方式有三种选择：

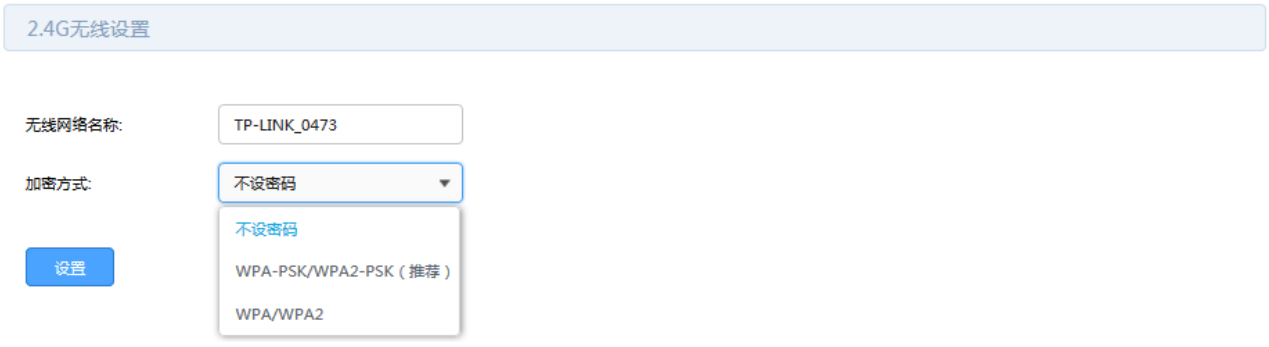


图 4-15 2.4G无线设置页面-不设密码

（1） 若选择不设密码，无需填写其他信息，直接点击<设置>即可。

（2） 若选择 WPA-PSK/WPA2-PSK（推荐），须填写如下内容：

图 4-16 2.4G无线设置页面- WPA-PSK/WPA2-PSK（推荐）

界面项说明：

认证类型 用于设置无线网络使用加密连接时的认证类型。

WPA-PSK/WPA2-PSK 加密方式的认证类型包括自动、WPA-PSK、WPA2-PSK 三个选项，自动涵盖 WPA-PSK 和 WPA2-PSK 两种认证类型，建议认证类型选择自动。

加密算法 用于设置无线网络使用加密连接时的加密算法。

WPA-PSK/WPA2-PSK 加密方式的加密算法包括自动、TKIP、AES 三个选项，自动涵盖 TKIP 和 AES 两种加密算法，建议加密算法选择自动。

无线密码 选择 WPA-PSK/WPA2-PSK 加密时连接无线网络的密码，由 8-63 个 ASCII 码字符或 8-64 个十六进制字符组成。

组密匙更新周期 定时更新用于广播和组播的密钥的周期，以秒为单位，最小值为 30，不更新则为 0。

（3）若选择WPA/WPA2，须填写如下内容：

图 4-17 2.4G无线设置页面- WPA/WPA2

界面项说明：

认证类型 用于设置无线网络使用加密连接时的认证类型。

WPA/WPA2 加密方式的认证类型包括自动、WPA 和 WPA2 三个选项，自动涵盖 WPA 和 WPA2 两种认证类型，建议认证类型选择自动。

加密算法 用于设置无线网络使用加密连接时的加密算法。

WPA/WPA2 加密方式的加密算法包括自动、TKIP、AES 三个选项，自动涵盖 TKIP 和 AES 两种加密算法，建议加密算法选择自动。

Radius服务器 进行身份认证的 Radius 服务器的 IP 地址。

Radius端口 Radius 服务使用的端口。

Radius密码 访问 Radius 服务的密码，由 8-63 个 ASCII 码字符或 8-64 个十六进制字符组成。

组密匙更新周期 定时更新用于广播和组播的密钥的周期，以秒为单位，最小值为 30，不更新则为 0。

➢ **5G无线设置**

与 2.4G 无线设置相同，请参考 2.4G 无线设置部分。

4.3.2.2 无线网络设置

您可以通过本页面进行 AP 无线网络的基本设置。

界面进入方法：AP管理 >> 无线网络设置 >> 无线网络设置

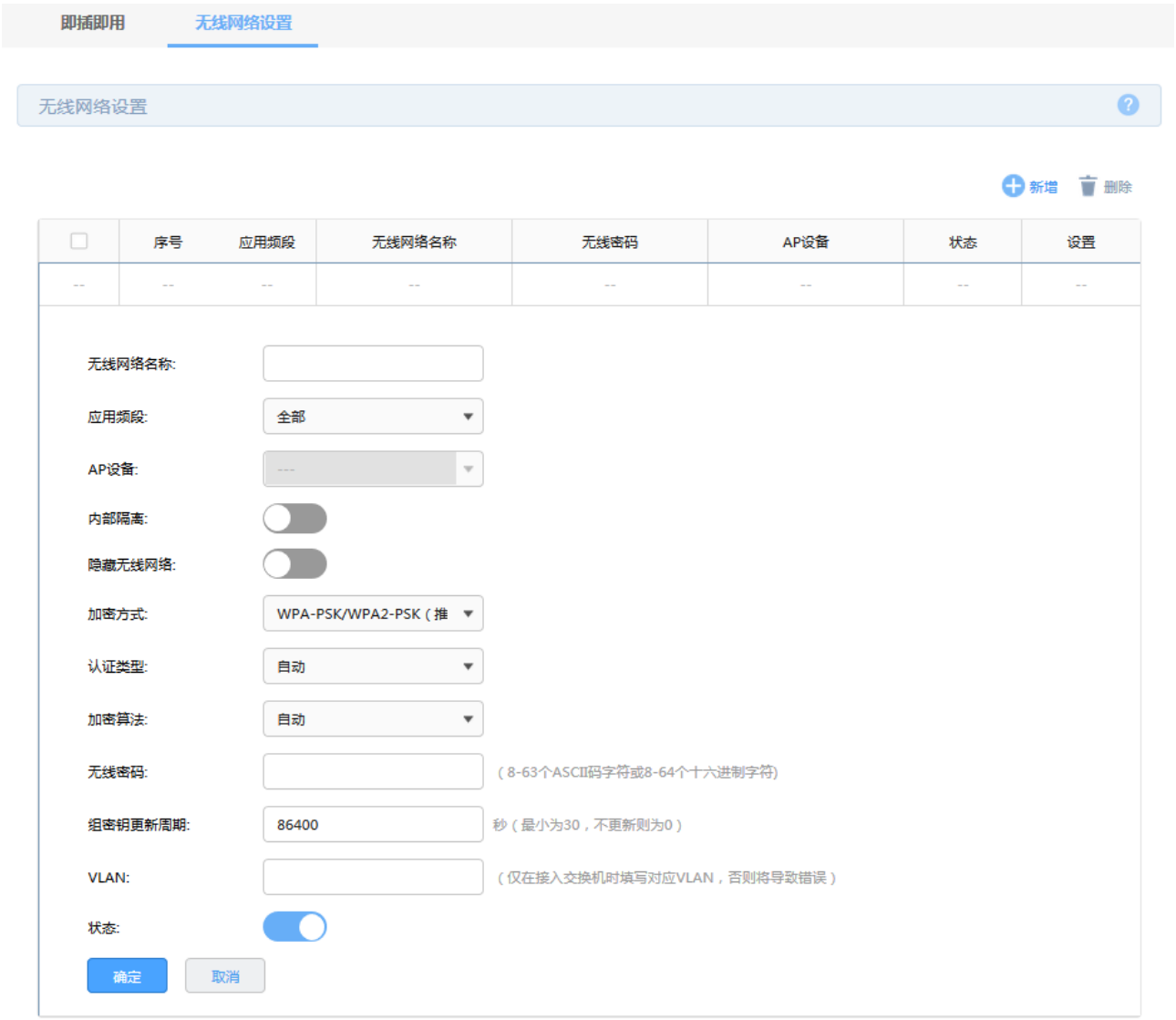


图 4-18 无线网络设置页面

界面项说明：

- **无线网络设置**

点击  按钮，可通过本页面设置新增无线网络，此处仅以加密方式选择“WPA-PSK/WPA2-PSK(推荐)”为例进行条目介绍，加密方式选择“不设密码”、“WPA/WPA2”请参考 2.4G 无线网络设置。

- **新增**

无线网络名称	路由器的无线(Wi-Fi)名称。
应用频段	无线网络生效的 AP 频段。
AP设备	无线网络生效的 AP 设备。
内部隔离	启用内部隔离，可以使连接到 AP 无线网络上的无线终端不能互相通信。滑块为灰色表示禁用，滑块为蓝色表示启用。
隐藏无线网络	启用隐藏无线网络，局域网中无线终端将搜不到 AP 无线网络的无线名称。滑块为灰色表示禁用，滑块为蓝色表示启用。
加密方式	用于无线网络连接时的加密方式，有三种加密方式可选。 不设密码：无线终端无需密码即可连接路由器。 WPA-PSK/WPA2-PSK(推荐)：使用 WPA2-PSK/WPA-PSK 加密方式，该加密方式无需自设认证服务器，设置无线密码即可。 WPA/WPA2:使用 WPA/WPA2 加密方式，该加密方式需要自行配置 Radius 服务器进行相关认证。
认证类型	用于设置无线网络使用加密连接时的认证类型。 WPA-PSK/WPA2-PSK 加密方式的认证类型包括自动、WPA-PSK、WPA2-PSK 三个选项，自动涵盖 WPA-PSK 和 WPA2-PSK 两种认证类型，建议认证类型选择自动。 WPA/WPA2 加密方式的认证类型包括自动、WPA 和 WPA2 三个选项，自动涵盖 WPA 和 WPA2 两种认证类型，建议认证类型选择自动。
加密算法	用于设置无线网络使用加密连接时的加密算法。 WPA-PSK/WPA2-PSK 加密方式的加密算法包括自动、TKIP、AES 三个选项，自动涵盖 TKIP 和 AES 两种加密算法，建议加密算法选择自

	动。 WPA/WPA2 加密方式的加密算法包括自动、TKIP、AES 三个选项，自动涵盖 TKIP 和 AES 两种加密算法，建议加密算法选择自动。
无线密码	选择 WPA-PSK/WPA2-PSK 加密时连接无线网络的密码，由 8-63 个 ASCII 码字符或 8-64 个十六进制字符组成。
组密匙更新周期	定时更新用于广播和组播的密钥的周期，以秒为单位，最小值为 30，不更新则为 0。
VLAN	连接到该无线网络无线终端的业务 VLAN。注：本路由器不支持 VLAN 接口，仅在接入交换机时才需要根据实际网络拓扑填写对应的 VLAN。
状态	滑块为灰色表示禁用无线网络，滑块为蓝色表示启用无线网络。

点击 设置按钮，可修改已保存的无线网络设置；点击 删除按钮，可删除已保存的无线网络设置。

说明：

若无线网络名称（SSID）内包含中文，设置界面内“无线网络名称（SSID）”一栏下会增加一项“SSID 编码方式”，通过该选项，您可以选择UTF8或GBK编码方式对包含中文的SSID进行编码。

4.3.3 无线主机状态

您可以通过本页面查看连接到 AP 设备上无线网络客户端的相关连接信息。

界面进入方法：AP 管理 >> 无线主机状态 >> 无线主机状态

图 4-19 无线网络设置页面

界面项说明：

➢ **无线主机状态**

主机状态显示范围	可以选择需要显示当前客户端主机连接信息的无线网络，ALL 为显示所有无线网络的客户端主机。
设备名称	通过无线连接到 AP 设备的客户端主机的设备名称。
MAC地址	通过无线连接到 AP 设备的客户端主机的 MAC 地址。
接入设备	客户端主机所连接的 AP 设备名称。
所属无线网络	客户端主机所连接的无线网络名称。
上/下行速率（KB/s）	客户端主机当前上/下行速率。
IP地址段	设置一个起始地址和一个结束地址，引用包含该地址对象地址组的规则在该地址段内均会生效。点击右边的加号可以添加多个地址段。

点击  刷新按钮，可刷新当前页面显示信息。

4.4 行为管控

4.4.1 地址管理

您可以通过本页面进行地址管理。

界面进入方法：行为管控 >> 地址管理

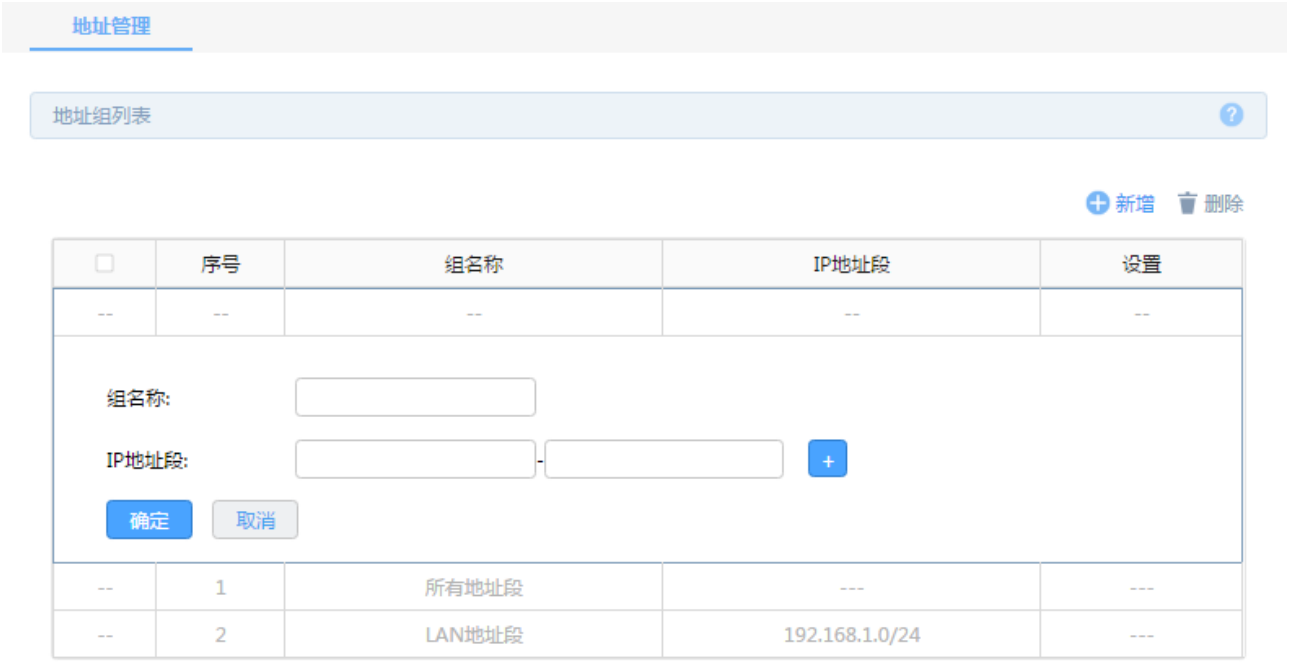


图 4-20 地址管理设置页面

界面项说明：

➢ **地址管理**

组名称	自定义地址组的名称。
IP地址段	设置一个起始地址和一个结束地址，引用包含该地址对象地址组的规则在该地址段内均会生效。点击右边的加号可以添加多个地址段。

注意：

地址组一旦在其他地方被引用则无法在本页面被删除，除非解除引用。

4.4.2 时间管理

您可以通过本页面设置时间，进行时间的管理。

界面进入方法：行为管控 >> 时间管理

图 4-21 时间管理设置页面

➢ **时间管理**

时间名称 标志时间的名称。

时间设置 用于设置时间所包含的时间段，有两种设置方式。

日历：通过在日历上划分矩形覆盖对应的时间区域来设置包含的时间段，只能精确到小时。

手动设置：通过手动输入生效时间段并勾选生效星期来设置一个时间段，精确到分钟，但一个对象最多只能设置 12 个时间段。

如图4-21中序号1条目是路由器预定义的一个时间组，表示所有时间段，此时间组不可编辑、删除。序号2条目的含义是：这个时间组的名称为workday，时间范围是通过“工作日历”的方式进行选择的，点击“工作日历”图标，则可以看到具体的时间范围。序号3条目的含义是：这个时间组的名称为weekend，表示的时间范围是周六、日的上午8点到11点。

点击<新增>可以新添加时间对象，如下图所示。

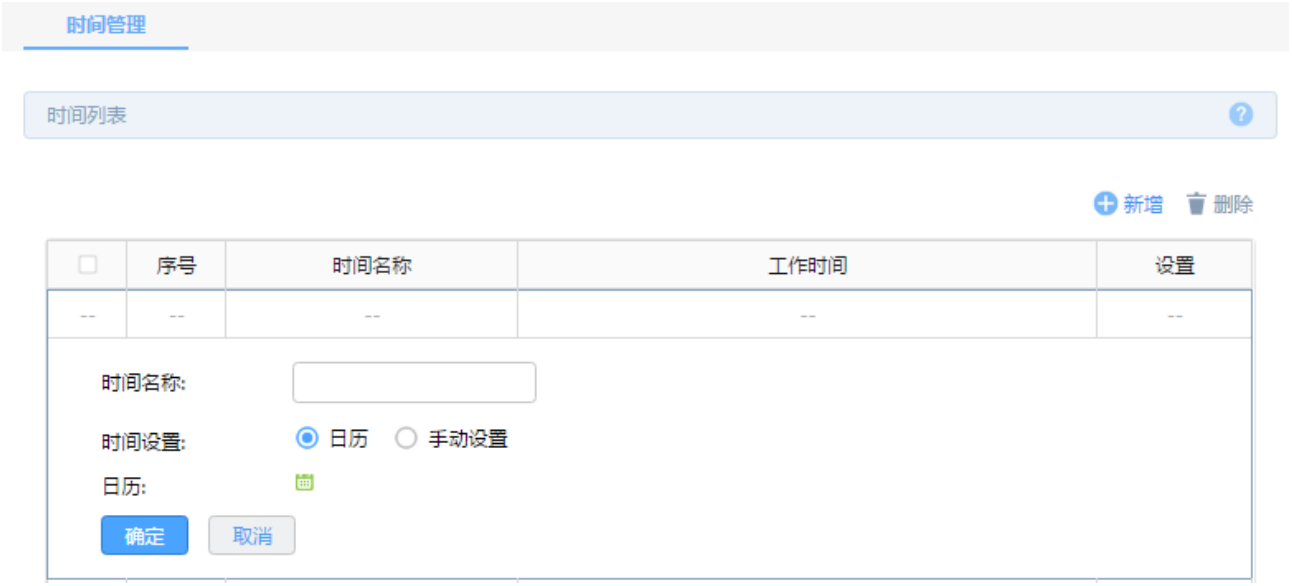


图 4-22 新增时间对象

进行时间设置时，有两种方式可以选择。如果选择“日历”的方式，则可点击下方工作日历图标，在弹出的页面框中选择时间。如果选择手动设置的方式，则通过输入起止时间进行同一天内的时间段添加。时间段由两个部分组成：

开始时间：时间段的起始时间，由时分组成，格式为（00:00）。

结束时间：时间段的截止时间，由时分组成，格式为（00:00）。

可以输入时间段的范围为00:00-24:00，时间段的每个设置框最多允许输入两位数字，一个设置框中输入完两位数字后，将自动跳转到下一个设置框。输入完成后，点击 + 按钮可以添加时间段，点击 - 可以删除已经添加的时间段。最多可以设置12个不同时间段，各个时间段之间不能有交叠。

注意：

若时间组正被其他规则引用，则该时间组无法删除。

4.4.3 应用控制

4.4.3.1 应用控制

您可以通过本页面添加应用控制条目。

界面进入方法：行为管控 >> 应用控制 >> 应用控制

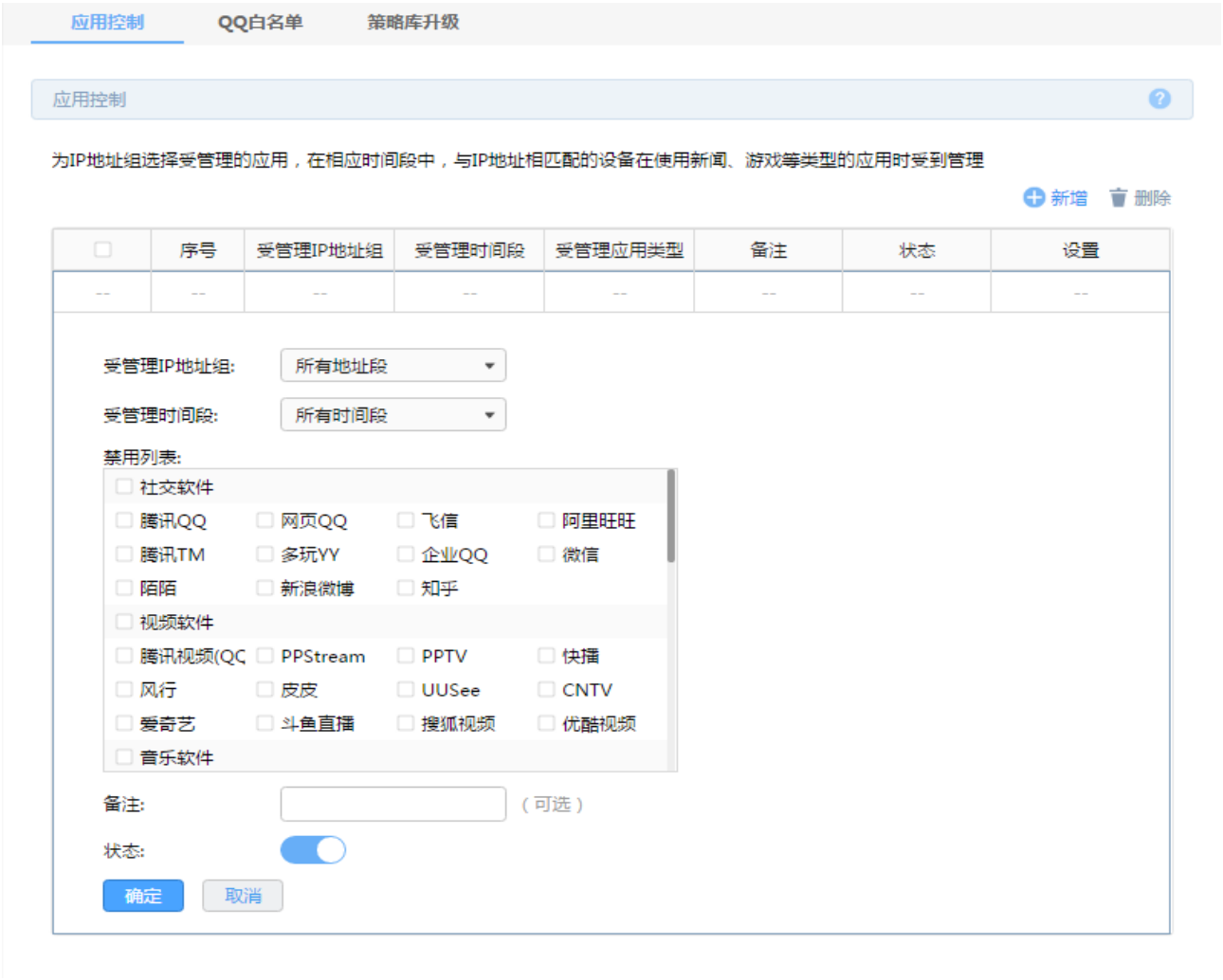


图 4-23 应用控制界面

点击<新增>按钮，可以新增一条应用控制规则。

界面项说明：

➢ **应用控制规则列表**

受管理IP地址组	选择受控地址组，使规则仅对该组生效。如需新建地址组，请参考**4.6.1 地址管理。**
受管理时间段	设置管控时间段，在受控时间内，IP 地址组内的客户端无法访问禁用列表中勾选的应用。
禁用列表	设置需要禁止的应用。
备注	设置备注信息，方便查询。
状态	滑块为灰色表示禁用，滑块为蓝色表示启用。

4.4.3.2 QQ 白名单

您可以通过本页面设置 QQ 白名单。

界面进入方法：行为管控 >> 应用控制 >> QQ白名单

图 4-24 QQ 白名单设置界面

界面项说明：

➢ **新增QQ白名单列表**

受管理IP地址组	选择受控地址组，使规则仅对该组生效。如需新建地址组，请参考**4.6.1 地址管理**。
受管理时间段	设置管控时间段，在受控时间内，IP 地址组内的客户端无法访问禁用列表中勾选的应用。
QQ号码	设置相应的 QQ 信息。
备注	设置备注信息，方便查询。
状态	滑块为灰色表示禁用，滑块为蓝色表示启用。

4.4.3.3 策略库升级

您可以通过本页面升级当前数据库。

界面进入方法：行为管控 >> 应用控制 >> 策略库升级

图 4-25 QQ 策略库升级设置界面

界面项说明：

➢ **策略库升级列表**

当前数据库版本	显示当前数据库的版本信息。
数据库路径	选择需要导入的策略库，点击“导入”导入最新的策略库。

4.4.4 网站访问

4.4.4.1 网站分组

您可以查看网站分组条目，还可以通过表格按钮对条目进行操作。

界面进入方法：行为管控 >> 网站访问 >> 网站分组

图 4-26 网站分组设置界面

界面项说明：

- **网站分组设置列表**

组名称	为网站分组添加名称，字符限制在 28 个字符以内，且两个分组不能重名。
组成员	网站分组成员，您可以同时输入多个网站进行批量添加。 组成员可以为域名，如 www.tp-link.com.cn,也可以在域名前面加通配符'*'，如*.tp-link.com.cn。但是'*'只允许输入在最前面，而不能夹杂在域名中间或后面。
清空	您可以清空组成员中输入的内容。
文件路径	您可以通过文件导入的形式为网站分组添加成员，文件格式为 txt 格式。

点击 设置按钮，可修改已保存的网站分组设置；点击 删除按钮，可删除已保存的网站分组设置。

4.4.4.2 网站访问

您可以查看网站访问条目，还可以通过表格按钮对条目进行操作。

界面进入方法：行为管控 >> 网站访问 >> 网站访问

图 4-27 网站访问设置界面

界面项说明：

- **网站访问设置界面**

受管理IP地址组	选择受控地址组，使规则仅对该组生效。如需新建地址组，请参考**4.6.1 地址管理**。
受管理时间段	设置管控时间段，在受控时间内，IP 地址组内的客户端无法访问禁用列表中勾选的应用。
规则类型	对符合规则的网站放行或禁止。
受管理网站类型	选择网站分组对象，其中所有网站表示对所有网站都生效。
备注	设置备注信息，方便查询。
状态	滑块为灰色表示禁用，滑块为蓝色表示启用。
添加到指定位置（第几条）	指定添加的规则的位置，排在前面的规则比后面规则优先级高。

4.4.5 文件下载

您可以查看文件下载条目，还可以通过表格按钮对条目进行操作。

界面进入方法：行为管控 >> 文件下载

图 4-28 文件下载设置界面

界面项说明：

➢ **文件下载设置界面**

受管理IP地址组	选择受控地址组，使规则仅对该组生效。如需新建地址组，请参考**4.6.1 地址管理**。
受管理时间段	设置管控时间段，在受控时间内，IP 地址组内的客户端无法访问禁用列表中勾选的应用。
规则类型	对符合规则的网站放行或禁止。
文件类型	填写要过滤的文件的后缀名，例如 exe，txt 等。
状态	滑块为灰色表示禁用，滑块为蓝色表示启用。
备注	您可以为该规则添加备注，50 字符以内。
添加到指定位置（第几条）	指定添加的规则的位置，排在前面的规则比后面规则优先级高。

4.4.6 带宽限制

4.4.6.1 带宽分配

您可以通过带宽分配规则列表，查看带宽分配的用户规则，还可以通过表格按钮对每条规则进行操作。

界面进入方法：行为管控 >> 带宽限制 >> 带宽分配

图 4-29 带宽分配设置界面

➢ **功能设置**

您可以全局开启或关闭带宽分配功能，或设置为仅当带宽利用率达到一定值以上才开启带宽分配功能。

界面项说明：

启用带宽分配	您可以全局开启或关闭带宽分配功能。
带宽利用率条件	在全局开启带宽分配功能的情况下，您可以设置一个百分比值，仅当带宽利用率高于这个值，带宽分配功能才会开启

界面项说明：

- **带宽分配设置界面**

受管理IP地址组	选择受控地址组，使规则仅对该组生效。如需新建地址组，请参考**4.6.1 地址管理**。
受管理时间段	设置规则管控时间段，在受控时间内，该规则生效。
带宽模式	共享表示地址组内 IP 共用设定的上下行带宽；独立表示地址组内所有 IP 均独占设定的上下行带宽。
数据流向	选择规则控制的数据流向。
最大上行/下行带宽	设置规则匹配的数据流的最大上行/下行带宽（单位为 Kb/s）。
状态	滑块为灰色表示禁用，滑块为蓝色表示启用。
备注	您可以为该规则添加备注，50 字符以内。
添加到指定位置（第几条）	指定添加的规则的位置，排在前面的规则比后面规则优先级高。

4.4.6.2 连接数限制

您可以查看连接数限制的用户规则，还可以通过表格按钮对每条规则进行操作。

界面进入方法：行为管控 >> 带宽限制 >> 连接数限制

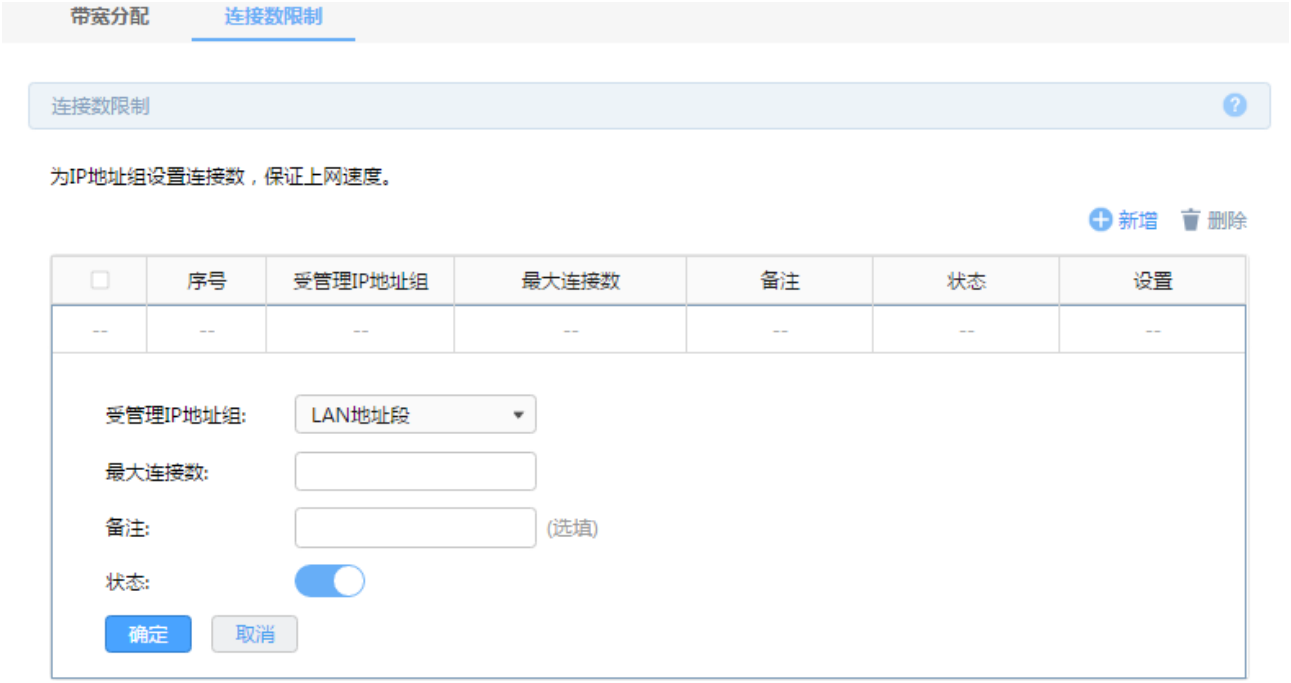


图 4-30 最大连接数设置界面

界面项说明：

➢ **最大连接数设置界面**

受管理IP地址组	设置受限的 IP 地址范围。
最大连接数	设置受限 IP 的最大连接数。
备注	您可以为该规则添加备注，50 字符以内。
状态	滑块为灰色表示禁用，滑块为蓝色表示启用。

4.4.7 访问控制

您可以查看访问控制条目，还可以通过表格按钮对条目进行操作。

界面进入方法：行为管控 >>访问控制

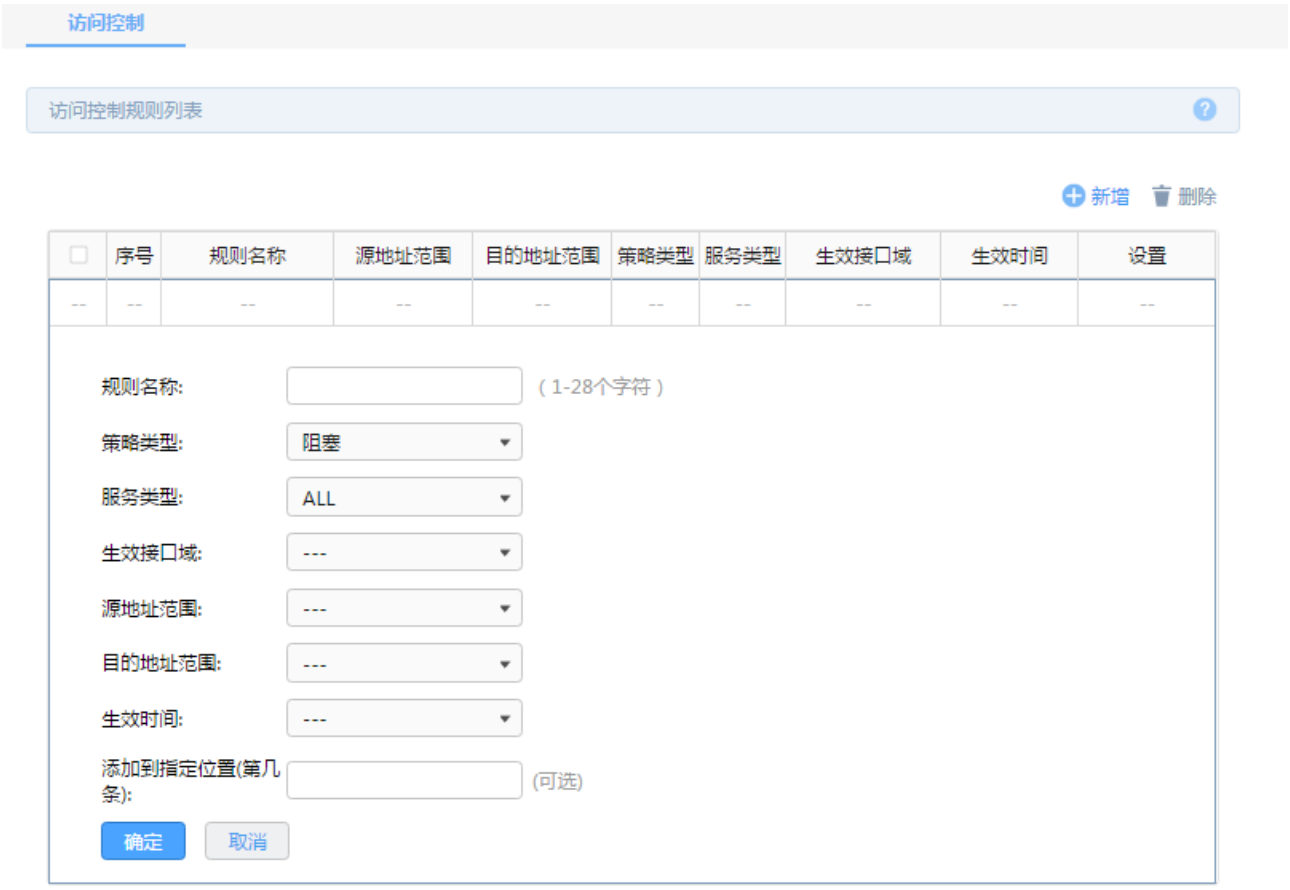


图 4-31 访问控制设置界面

界面项说明：

- **访问控制列表**

规则名称	为添加的规则命名，字符数限制在 28 个字符以内，且任意两条规则不能重名。
策略类型	指明这条规则对符合条件的数据包放行还是丢弃。
服务类型	选择生效的协议，ALL 表示所有协议。
生效接口域	在路由器接口中选择该规则对应生效的接口，ALL 表示所有的接口。
源地址范围	选择地址对象，以建立访问规则条目的源地址范围。
目的地址范围	选择地址对象，以建立访问规则条目的目的地址范围。

生效时间	选择规则生效的时间。
添加到指定位置（第几条）	指定添加的规则的位置，排在前面的规则比后面规则优先级高。

4.4.8 行为审计

界面进入方法：行为管控 >> 行为审计 >> 上网行为分析

您可以通过本页面来设置上网行为分析功能。

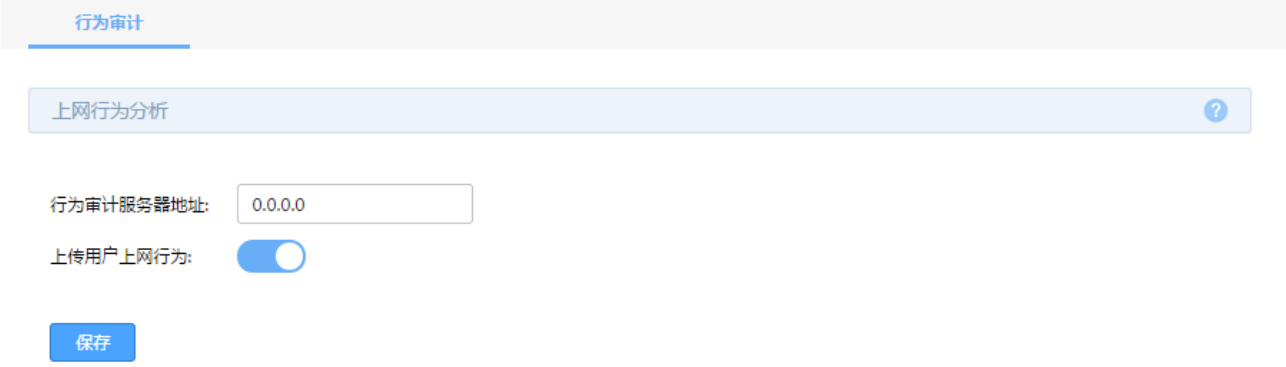


图 4-32 行为审计设置界面

界面项说明：

➢ **上网行为分析**

行为审计服务器地址	设置行为审计服务器的 IP 地址，行为审计的相关数据将发往该地址的服务器。
上传用户上网行为	点击可开关上网行为分析功能。滑块为蓝色时开启，将往行为审计服务器发送审计数据。

注意：

- 行为审计功能需要配合 TP-LINK 行为审计软件才能进行上网行为的分析。
- 您可以访问 TP-LINK 官方网站 www.tp-link.com.cn 获取最新的行为审计软件，或者联系 400-8863-400 售后服务热线及 smb@tp-link.com.cn 售后服务邮箱。

4.5 安全管理

4.5.1 ARP防护

4.5.1.1 IP-MAC 绑定

您可以通过本页面完成 IP-MAC 绑定设置。

界面进入方法：安全管理 >>ARP防护 >>IP-MAC绑定

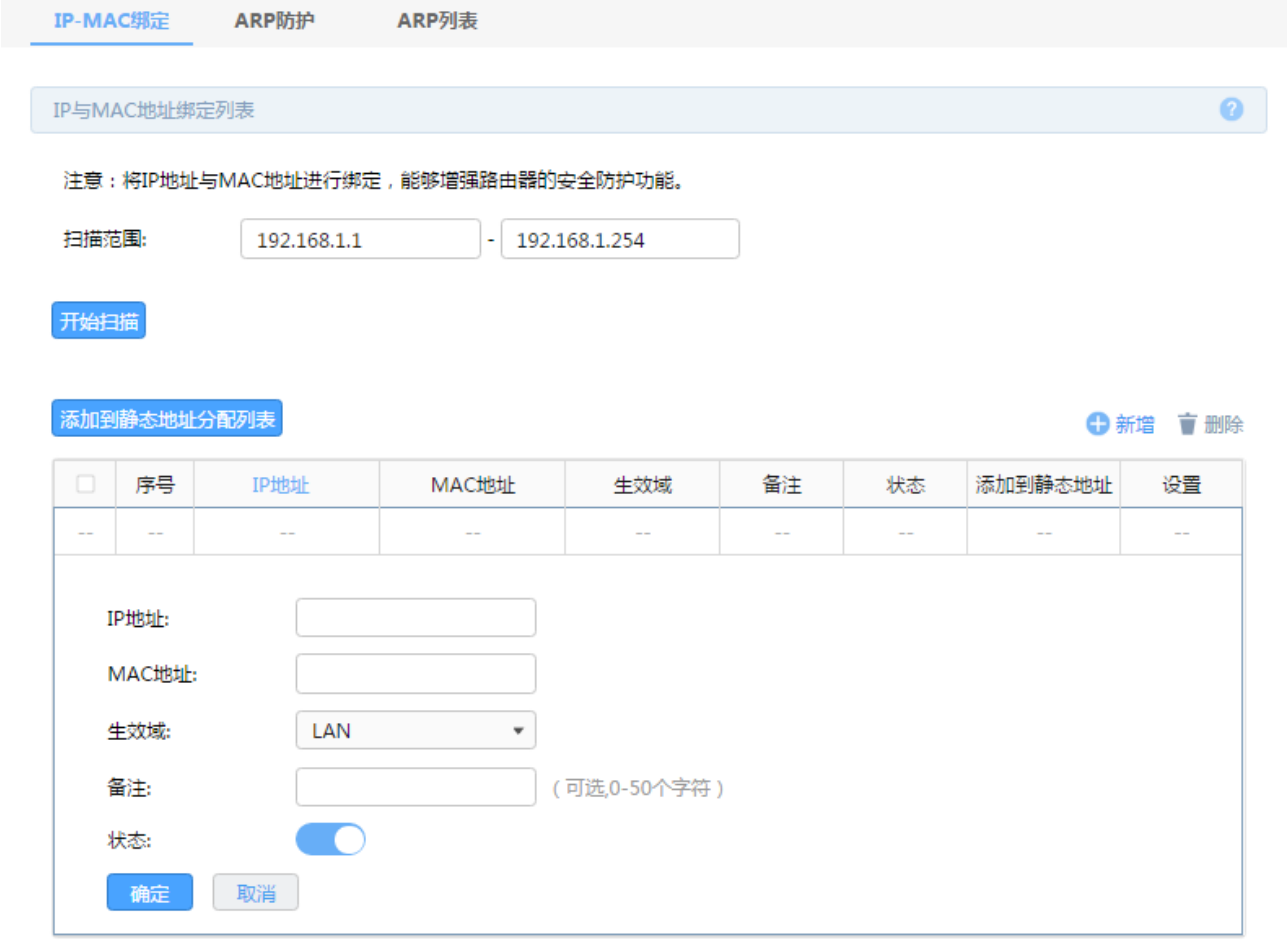


图 4-33 IP-MAC地址绑定设置界面

界面项说明：

- **ARP扫描**

扫描范围	输入扫描的 IP 地址范围，路由器会对该范围的 IP 地址进行 ARP 查询。
扫描结果	扫描结束后，扫描得到的结果会出现在这个列表中。

输入有效的扫描地址范围，点击 开始扫描，将会弹出如图 4-33 所示对话页面，耐心等待片刻，即可得到 ARP 扫描结果列表（图 4-34）。

图 4-34 ARP扫描中

图 4-35 ARP扫描结果列表

您可以勾选需要绑定的 IP 地址与 MAC 地址，单击 添加到绑定列表，进行 IP-MAC 绑定。如图 4-35 所示，即为勾选了序号 1 进行了添加到绑定列表操作。

图 4-36 ARP扫描结果添加到绑定列表

界面项说明：

- **IP-MAC绑定规则列表**

IP地址	您可以输入待绑定的 IP 地址。
MAC地址	您可以输入待绑定的 MAC 地址，格式为 xx-xx-xx-xx-xx-xx。
生效域	针对局域网中的 ARP 绑定请选择 LAN 口；如果需要对于 WAN 口绑定请选择对应的 WAN 口。
备注	请添加备注信息。
状态	滑块为灰色表示禁用，滑块为蓝色表示启用。
添加到静态地址	可以将该 IP-MAC 绑定条目导入到 DHCP 静态地址分配列表。
添加到静态地址分配列表	选择多条 IP-MAC 绑定列表中的条目，点击“添加到静态地址分配列表”按钮，可一次将多个条目一次性导入到 DHCP 静态地址分配列表中。

4.5.1.2 ARP 防护

您可以通过本页面设置 ARP 防护的相关选项。

界面进入方法：安全管理 >>ARP防护 >>ARP防护

图 4-37 ARP防护设置界面

界面项说明：

- **ARP防护**

ARP防欺骗功能	启用或关闭 ARP 的防欺骗功能。 若关闭，防 ARP 欺骗，禁止非 IP-MAC 绑定的数据包通过，发送 GARP 功能等功能都不会生效。
禁止非IP-MAC绑定的数据包通过	开启该功能，则路由器只会放过在 IP-MAC 绑定规则中的数据包。 注意，要开启该功能，需要先开启 ARP 防欺骗功能。
允许路由器在发现ARP攻击时发送GARP包	开启该功能，路由器收到与 IP-MAC 绑定列表中不一致的报文时，会发送 GARP。 注意，要开启该功能，需要先开启 ARP 防欺骗功能。

4.5.1.3 ARP 列表

您可以通过本页面查看系统中 ARP 列表。

界面进入方法：安全管理 >>ARP防护 >>ARP列表

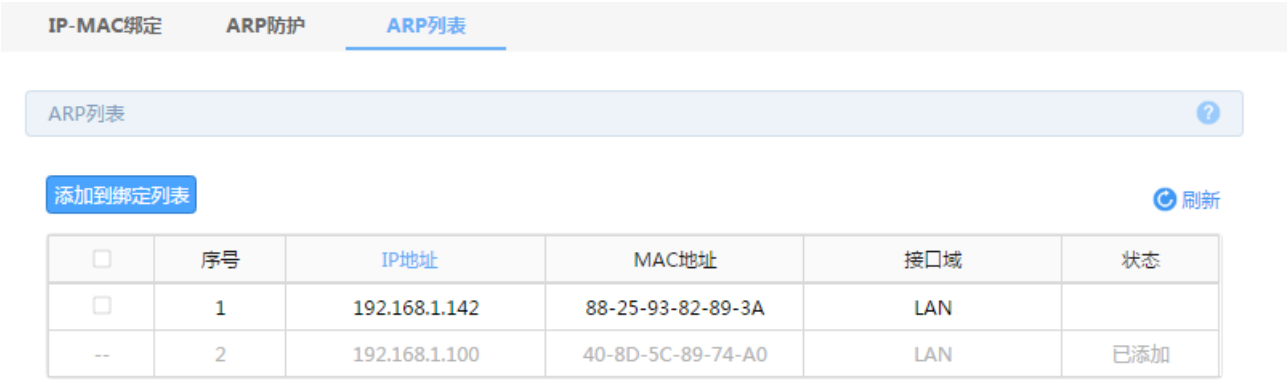


图 4-38 ARP列表

界面项说明：

- **ARP列表**

ARP列表	路由器学习连接在路由器各接口上的网络设备 IP 与 MAC 对应表。
添加到绑定列表	可以选择多条 ARP 列表中的条目，一次性添加到 IP-MAC 绑定列表中。

4.5.2 MAC地址过滤

您可以在此页面上进行 MAC 地址过滤功能设置。

界面进入方法：安全管理 >> MAC地址过滤

图 4-39 MAC地址过滤设置界面

界面项说明：

➢ **MAC地址过滤**

启用MAC地址过滤功能	滑块为灰色表示禁用，滑块为蓝色表示启用。
规则类型	白名单（允许设备访问外网）：路由器将只允许 MAC 地址在过滤规则列表中的主机通过路由器。 黑名单（不允许设备访问外网）路由器将禁止 MAC 地址在过滤规则列表中的主机通过路由器。

点击 新增 按钮，可以新增一个规则列表，如图4-39所示。

图 4-40 新增 MAC 过滤规则列表

界面项说明：

- **MAC过滤规则列表**

名称	您可以设置规则的名称。
MAC地址	过滤的 MAC 地址，格式为 xx-xx-xx-xx-xx-xx。

4.5.3 攻击防护

您可以进行防 FLOOD 攻击的相关设置。

界面进入方法：安全管理 >>攻击防护

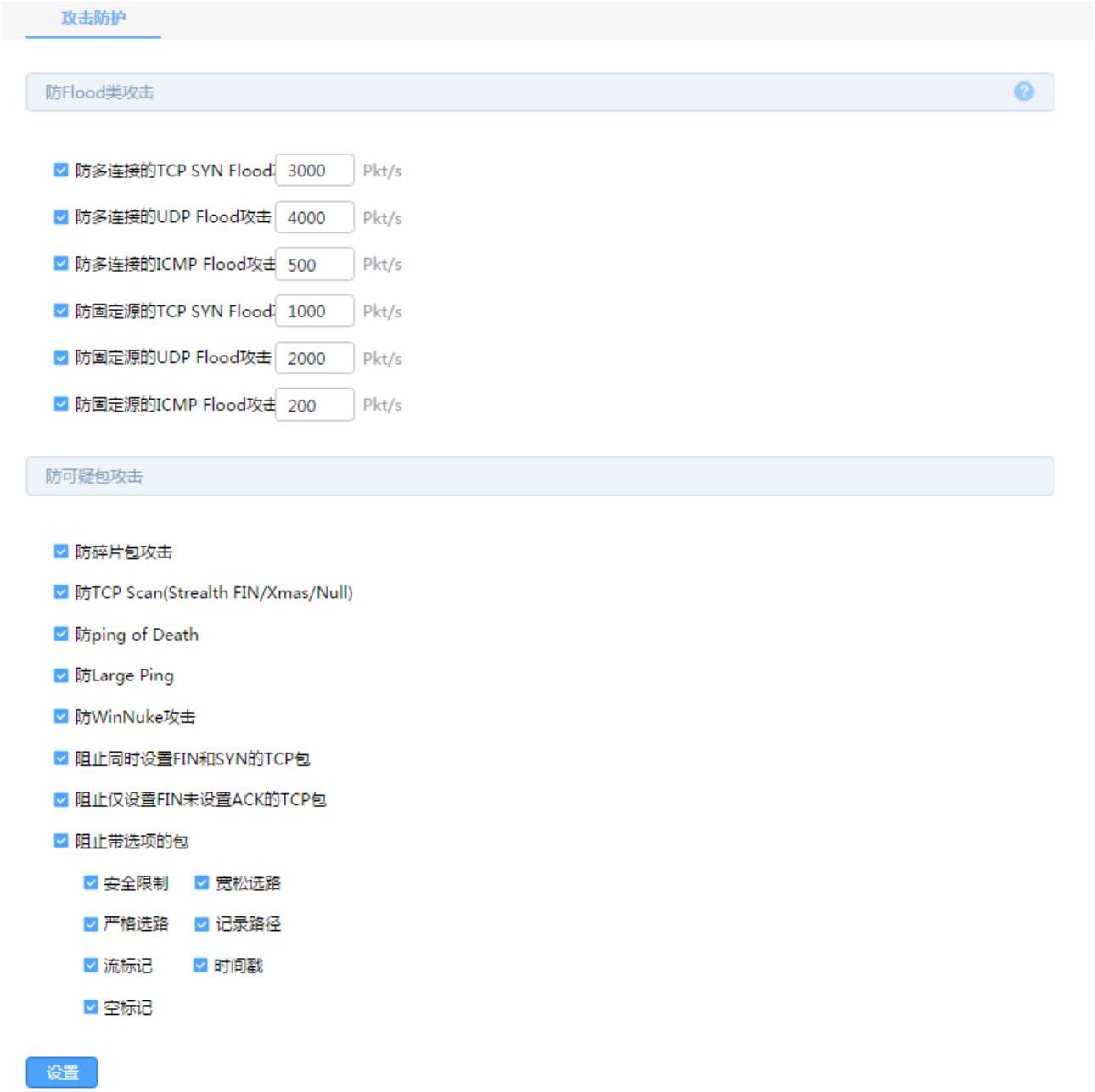


图 4-41 攻击防护设置界面

界面项说明：

- **防Flood类攻击**

启用防多连接的TCP SYN Flood攻击	开启 TCP 的连接限制，将 TCP 连接限制在给定值之内。
启用防多连接的UDP Flood攻击	开启 UDP 的连接限制，将 UDP 连接限制在给定值之内。
启用防多连接的ICMP Flood攻击	开启 ICMP 的连接限制，将 ICMP 连接限制在给定值之内。
启用防固定源的TCP SYN Flood攻击	将某个 IP 的 TCP 的连接限制在给定值之内。
启用防固定源的UDP Flood攻击	将某个 IP 的 UDP 的连接限制在给定值之内。
启用防固定源的ICMP Flood攻击	将某个 IP 的 ICMP 的连接限制在给定值之内。

- **防可疑包攻击**

启用防碎片包攻击	开启该功能，路由器会过滤掉碎片包。
启用防TCP Scan(Strealth FIN/Xmas/Null)	开启该功能，路由器会过滤掉三种工具的 tcp scan 包。
启用防ping of Death	开启该功能，路由器会过滤掉异常的 ping 包。
启用防Large Ping	开启该功能，路由器会过滤掉大 ping 包。
启用WinNuke攻击	开启该功能，防止 winNuke 攻击。
阻止同时设置FIN和SYN的TCP包	开启该功能，路由器会过滤掉同时包含 FIN 和 SYN 的 TCP 报文。
阻止带选项的包	开启该功能，路由器会过滤掉设置某些 IP 选项中的报文。

4.6 VPN

VPN（Virtual Private Network，虚拟专用网）是一个建立在公用网（通常是因特网）上的专用网络，但因为这个专用网络只是逻辑存在并没有实际物理线路，故称为虚拟专用网。

随着因特网的发展壮大，越来越多的数据需要在因特网上进行传输共享，不过当企业将自身网络接入因特网时，虽然各地的办事处等外部站点可以很方便地访问企业网络，但同时也把企业内部的私有数据暴露给因特网上的所有用户。于是在这种开放的网络环境上搭建专用线路的需求日益强烈，VPN应运而生。

VPN通过隧道技术在两个站点间建立一条虚拟的专用线路，使用端到端的认证和加密保证数据的安全性。典型拓扑图如所示。

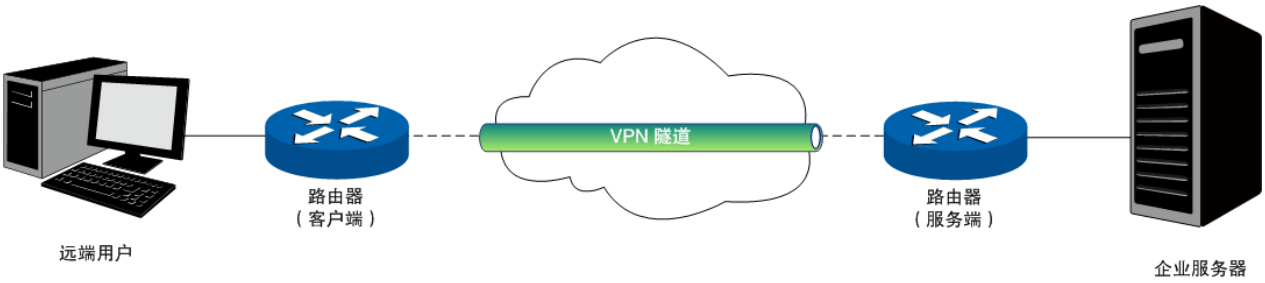


图 4-42 VPN典型拓扑

隧道是通过对数据报的封装实现的，因为数据报封装和解封的过程都是在路由器上完成，所以对于用户来说是透明的。TL-R473P-AC支持的隧道协议包括三层隧道协议IPSec和二层隧道协议L2TP/PPTP。

4.6.1 IPSec

IPSec（IP Security，IP安全性）是一系列服务和协议的集合，在IP网络中保护端对端通信的安全性、防止网络攻击。

为了实现安全通信，通信双方的IPSec协议必须协商确定用于编码数据的具体算法、用于理解对方数据格式的安全协议，并通过IKE（Internet Key Exchange，网络密钥交换协议）交换解密编码数据所需的密钥。

在IPSec中有两个重要的安全性协议AH（Authentication Header，认证首部）和ESP（Encapsulating Security Payload，封装安全性载荷）。AH协议用于保证数据的完整性，若数据报文在传输过程中被篡改，报文接收方将在完整性验证时丢弃报文；ESP协议用于数据完整性检查以及数据加密，加密后的报文即使被截取，第三方也难以获取真实信息。

4.6.1.1 IPSec安全策略

您可以通过本页面设置 IPSec 安全策略，安全策略规定了对什么样的数据流采用什么样的安全提议。安全策略设置分为必要设置和高级设置两个部分，其中高级设置是可选部分。

界面进入方法：VPN >> IPSec >> IPSec安全策略

图 4-43 IPSec安全策略设置界面

图 4-44 IPSec安全策略设置界面-高级设置

界面项说明：

- **IPSec安全策略列表**

策略名称	为IPSec安全策略命名，名称最多支持32个字符。
对端网关	设置对端网关，可以填写对端的IP地址或域名。可配置"0.0.0.0"，表示任意地址。
绑定接口	绑定本地使用的接口；对端网关设置的"对端网关地址"必须与该接口的IP地址相同。
本地子网范围	设置受保护的数据流的本地子网范围，由 IP 地址和子网掩码来确定。
对端子网范围	设置受保护的数据流的对端子网范围，由 IP 地址和子网掩码来确定。
预共享密钥	对于每对<绑定接口，对端网关>，都必须指定唯一的预共享密钥用于双方的认证与协商。
状态	滑块为灰色表示禁用，滑块为蓝色表示启用。
高级配置	高级设置包括两个部分：阶段 1 设置和阶段 2 设置。一般地，用户不需要配置高级设置，采用默认值即可。
阶段 1 设置	设定 IKEv1 的第一阶段的相关参数。
安全提议	用于 IKE 协商方式下选择 IPSec 安全提议，在 IKE 协商模式下可以最多选择四条不同安全提议，主模式协商可以选择 4 条，野蛮模式协商可以选择 1 条。
交换模式	IKEv1 版本支持两种模式：主模式和野蛮模式，默认是选择主模式。
协商模式	初始者模式会主动向对端发起连接，此时要求对端网关是路由可达，而响应者模式仅仅会等待对端发起连接。
本地 ID 类型	作为对端的身份标识，支持两种类型：IP 地址和 NAME，默认选择"IP 地址",如果选择 NAME 类型，则需要输入任意的字符串。
本地 ID	仅仅在本地 ID 类型选择 NAME 的时候生效，用于存储用户输入对应的字符串。

对端 ID 类型	作为对端的身份标识，支持两种类型：IP 地址和 NAME，默认选择"IP 地址",如果选择 NAME 类型，则需要输入任意的字符串。
对端 ID	仅仅在对端 ID 类型选择 NAME 的时候生效，用于存储用户输入对应的字符串。
生存时间	用于 IKE 协商方式下设置第一阶段 IPSec 会话密钥的生存时间。
DPD 检测开启	选择是否开启 DPD 检测功能，开启该功能会定时发送 DPD 数据包以快速发现对端是否在线。
DPD 检测周期	仅在 DPD 检测开启启用之后生效，用于指定相邻两次发送 DPD 检测数据包的时间间隔。
阶段 2 设置	设定 IKEv1 的第二阶段的相关参数。
封装模式	设置 IKE 第一阶段协商的封装模式，该封装模式必须与对端相同。封装模式有以下两种： 隧道模式（Tunnel mode）：在该模式下，AH 或 ESP 插在原始 IP 报文头之前，另外生成一个新的报文头放到 AH 或 ESP 之前。从安全性来讲，隧道模式优于传输模式。适用于更普遍的 VPN 应用。 传输模式（Transport mode）：在该模式下，AH 或 ESP 被插入到 IP 报文头之后但在所有传输层协议之前，或所有其他 IPSec 协议之前。适用于主机直接访问设备时之间的加密传输。 两者的区别在于：前者会在原始 IP 报文外多增加一个 IP 头，后者则不会。
安全提议	用于 IKE 协商方式下选择 IPSec 安全提议，在 IKE 协商模式下可以最多选择四条不同安全提议。
PFS	PFS（Perfect Forward Secrecy，完善的前向安全性）特性使得IKE第二阶段协商生成一个新的密钥材料，该密钥材料与第一阶段协商生成的密钥材料没有任何关联，这样即使IKE第一阶段的密钥被破解，第二阶段的密钥仍然安全。如果没有使用PFS，第二阶段的密钥将根据第一阶段生成的密钥材料来产生，一旦第一阶段的密钥被破解，用于保护通信数据的第二阶段密钥也岌岌可危，这将严重威胁到双方的通信安全。PFS是通过DH算法实现的，通信双方的PFS设置需保持一致。
生存时间	用于 IKE 协商方式下设置第二阶段 IPSec 会话密钥的生存时间。

IPSec安全策略列表中，可以对已保存的IPSec安全策略进行相应设置。

4.6.1.2 IPSec安全联盟

您可以通过本页面查看当前建立的安全联盟。

界面进入方法：VPN >> IPSec >> IPSec安全联盟

	序号	名称	SPI	方向	隧道两端	数据流	安全协议	AH验证算法	ESP验证算法	ESP加密算法
	1	IPSec_Site1	3247185080	in	172.33.1.100<--172.33.1.200	192.168.0.0/24 <-- 192.168.1.0/24	ESP	--	MD5	3DES
	2	IPSec_Site1	3265412373	out	172.33.1.100-->172.33.1.200	192.168.0.0/24 --> 192.168.1.0/24	ESP	--	MD5	3DES

图 4-45 IPSec安全联盟界面一

上图中路由器使用eth1接口进行隧道连接，eth1接口的IP地址为172.33.1.100，对端网关地址为172.33.1.200。IPSec隧道的安全提议等相关设置需与对端路由设置相同。

由于安全联盟是单向的，所以当IPSec隧道成功建立后，每条隧道会产生一对出和入的安全联盟。出和入的SPI值是不同的，但与对端的入和出SPI值相同，即本端方向in的SPI值与对端方向out的SPI值相同。这条隧道在对端的连接信息如下图所示，SPI值为IKE自动协商得出。

	序号	名称	SPI	方向	隧道两端	数据流	安全协议	AH验证算法	ESP验证算法	ESP加密算法
	1	IPSec_Site2	3265412373	in	172.33.1.200<--172.33.1.100	192.168.1.0/24 <-- 192.168.0.0/24	ESP	--	MD5	3DES
	2	IPSec_Site2	3247185080	out	172.33.1.200-->172.33.1.100	192.168.1.0/24 --> 192.168.0.0/24	ESP	--	MD5	3DES

图 4-46 IPSec安全联盟界面二

说明

NAT穿透

在实际网络应用中，IPSec VPN通信双方的物理连接线路中可能存在着NAT网关，当数据包经过NAT网关时，其IP地址或端口号会改变，这就导致VPN隧道对端收到数据包后验证失败，数据包被直接丢弃。NAT穿透功能可以解决这一问题，实现方法为在原ESP协议的报文外添加新的IP首部和UDP首部。这样数据包（隧道模式下）的格式为：新IP/UDP首部 | ESP首部 | IP首部 | 数据。由于NAT网关只会改变

最外层的IP首部，而且ESP校验不包含IP首部，所以此时IPSec VPN的通信不会受到影响。但是NAT穿透只适用于ESP协议，AH协议的校验包含了IP首部，因此无法与NAT共存。

TL-R473P-AC目前默认支持NAT穿透，当对端也支持NAT穿透，并且双方协商时检测到存在NAT设备的时候，会自动启用该功能。

4.6.2 L2TP

L2TP（Layer 2 Tunneling Protocol，第二层隧道协议）是二层VPN隧道协议，使用PPP（Point to Point Protocol，点到点协议）进行数据封装，并都为数据增添额外首部。

4.6.2.1 L2TP 服务器

您可以设置 L2TP 服务器的全局配置。

界面进入方法：VPN >> L2TP >> L2TP服务器

图4-47 L2TP服务器设置界面

界面项说明：

- **全局设置**

L2TP 链路维护时间间隔	设置L2TP隧道维护的时间间隔。范围是60秒至1000秒。
PPP 链路维护时间间隔	设置L2TP隧道里的PPP隧道维护的时间间隔，范围是0秒至120秒，0代表不发送。

- **服务器设置**

服务接口	L2TP 服务器监听的接口，只有来自服务接口的报文才会被处理。
IPSec 加密	是否对隧道进行加密。若加密，则使用 IPSec 对 L2TP 隧道加密。若可选加密，则 L2TP 隧道按客户端的需求决定是否进行 IPSec 加密。
预共享密钥	IPSec 设置为加密或可选加密后，需设置 IPSec 的预共享密钥。
状态	滑块为灰色表示禁用，滑块为蓝色表示启用。

在服务器设置列表中，可以对已保存的L2TP服务器信息进行相应设置。

4.6.2.2 L2TP客户端

您可以设置 L2TP 客户端的全局配置。

界面进入方法：VPN >> L2TP >> L2TP客户端

图 4-48 L2TP客户端设置界面

界面项说明：

- **全局设置**

L2TP 链路维护时间间隔	设置L2TP隧道维护的时间间隔。范围是60秒至1000秒。
PPP 链路维护时间间隔	设置L2TP隧道里的PPP隧道维护的时间间隔。范围是0秒至120秒。0代表不发送。

- **客户端设置**

隧道名称	设置L2TP隧道名称。
用户名	设置L2TP认证的用户名。
密码	设置L2TP认证的密码。
出接口	L2TP报文收发的接口。
服务器地址	设置L2TP隧道的服务器地址。
IPSec 加密	选择是否对隧道进行加密。若启用，则使用IPSec对L2TP隧道加密，需填写预共享密钥。
预共享密钥	设置IPSec加密时的预共享密钥。
对端子网	L2TP隧道对端局域网所使用的IP地址范围（一般可以填VPN隧道对端设备的LAN口IP地址范围），由IP和子网掩码组成。
上行带宽	设置L2TP客户端的最大上行带宽。
下行带宽	设置L2TP客户端的最大下行带宽。
工作模式	选择L2TP客户端的工作模式，可选择“NAT”或“路由”模式。 NAT：对经过此L2TP隧道的数据包进行NAT转换（数据包的源IP替换为L2TP隧道的本地虚拟IP）； 路由：对经过此L2TP隧道的数据包只进行路由转发。
状态	滑块为灰色表示禁用，滑块为蓝色表示启用。

在线检测模式	在线检测是通过 PING 和 DNS 检测接口是否在线： 自动：PING 检测选择网关指定互联网地址作为目的地址，DNS 检测选择接口的 DNS 服务器作为目的地址。 永远在线：不对接口进行任何在线检测，接口状态一直在线。 手动：手动指定 PING 检测和 DNS 检测的地址，判断接口是否在线。

➢ **隧道设置列表**

在隧道设置列表中，可以对已保存的L2TP隧道信息进行相应设置。

说明：

默认添加的IPSec策略不允许与已有策略的两端子网都重叠，因此在同一个出接口上不能同时添加加密/可选加密的L2TP服务器和加密的L2TP客户端。

在同一个出接口上不能同时添加加密/可选加密的L2TP服务器和对端全0的IPSec策略，避免造成冲突。

4.6.2.3 隧道信息列表

在此将列出路由器上所有L2TP隧道的相关信息。

界面进入方法：VPN >> L2TP >>隧道信息列表

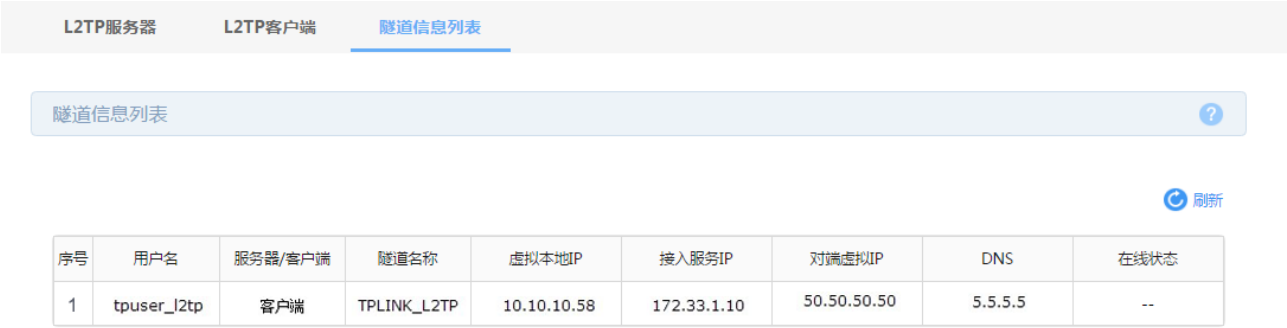


图 4-49 L2TP隧道信息界面

上图1条目表示目前这条隧道已成功建立，列表中会显示当前隧道建立时，隧道所使用的虚拟接口名称、本地虚拟IP地址、隧道对端的虚拟IP地址和实际IP地址等信息。

界面项说明：

➢ **隧道信息列表**

用户名	L2TP 隧道建立时用于认证身份使用的用户名称。
服务器/客户端	建立隧道时，本端是作为服务器还是客户端。
隧道名称	L2TP 隧道的名称，用于区分不同的隧道。
虚拟本地 IP	隧道的本地虚拟 IP 地址。
接入服务 IP	隧道的对端实际 IP 地址。
对端虚拟 IP	隧道的对端虚拟 IP 地址。
DNS	隧道的 DNS 地址。

4.6.3 PPTP

PPTP（Point to Point Tunneling Protocol，点到点隧道协议）是二层VPN隧道协议，使用PPP（Point to Point Protocol，点到点协议）进行数据封装，并都为数据增添额外首部。

4.6.3.1 PPTP服务器

界面进入方法：VPN >> PPTP >> PPTP服务器

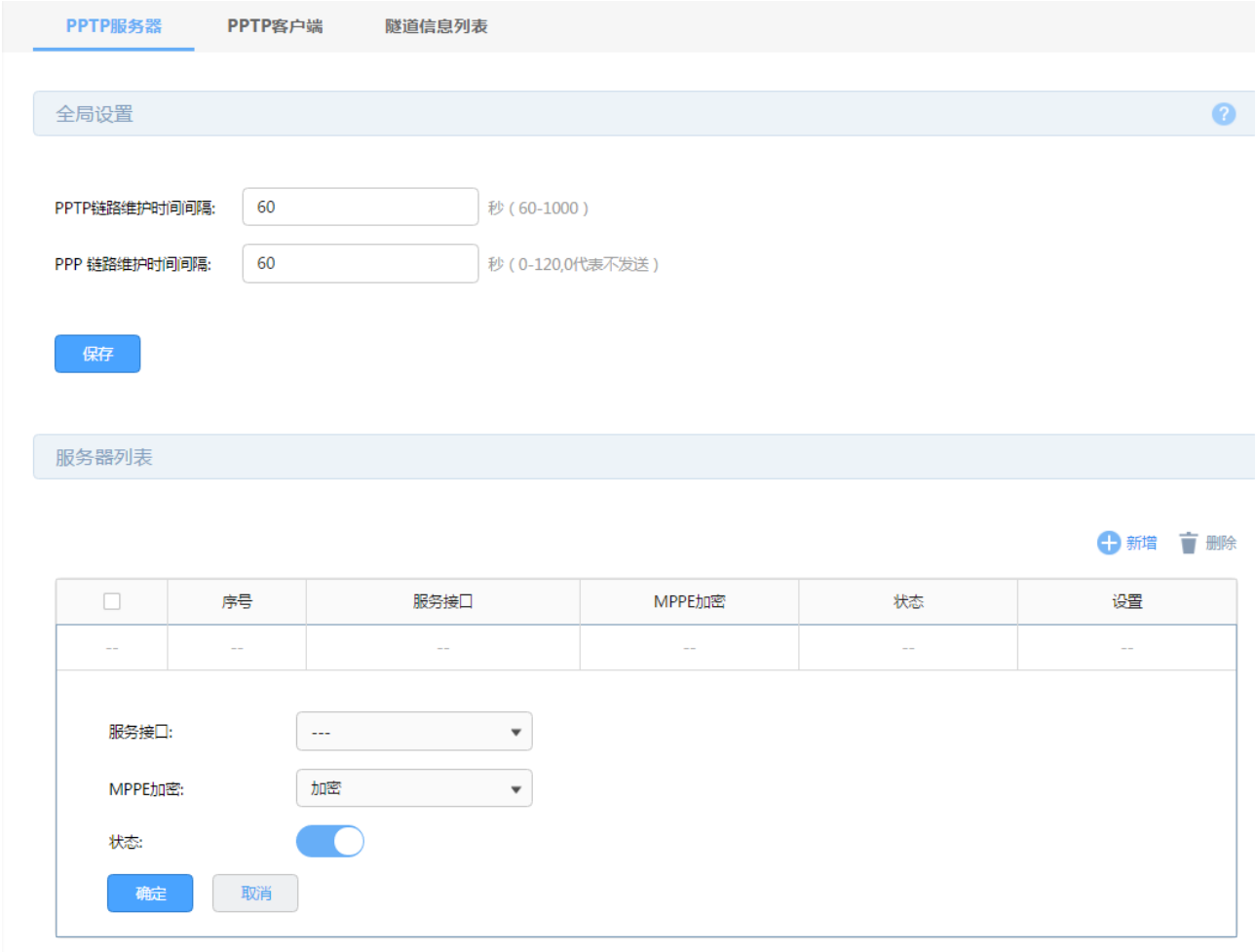


图 4-50 PPTP服务器设置界面

界面项说明：

- **全局设置**

PPTP 链路维护时间间隔	设置PPTP隧道维护的时间间隔。范围是60秒至1000秒。
PPP 链路维护时间间隔	设置PPTP隧道里的PPP隧道维护的时间间隔。范围是0秒至120秒,0代表不发送。

- **服务器列表**

服务接口	PPTP 服务器监听的接口，只有来自服务接口的报文才会被处理。
MPPE 加密	是否对隧道进行加密。若启用，则使用 MPPE 对 PPTP 隧道加密。
状态	滑块为灰色表示禁用，滑块为蓝色表示启用。

在服务器列表中，还可以对已保存的PPTP隧道信息进行相应设置。

4.6.3.2 PPTP客户端设置

您可以通过本页设置 PPTP 客户端。

界面进入方法：VPN >> PPTP >> PPTP客户端

图 4-51 PPTP客户端设置界面

界面项说明：

- **全局设置**

PPTP 链路维护时间间隔	设置PPTP隧道维护的时间间隔。范围是60秒至1000秒。
PPP 链路维护时间间隔	设置PPTP隧道里的PPP隧道维护的时间间隔。范围是0秒至120秒,0代表不发送。

- **客户端列表**

隧道名称	PPTP 隧道的名称，用于区分不同的隧道。
用户名	设置 PPTP 认证的用户名。
密码	设置 PPTP 认证的密码。
出接口	PPTP 报文收发的接口。
服务器地址	PPTP 服务器的地址，可以为 IP 或域名。
MPPE 加密	是否对隧道进行加密。若启用，则使用 MPPE 对 PPTP 隧道加密。
对端子网	PPTP 隧道对端局域网使用的 IP 地址范围（一般可以填隧道对端设备 LAN 口的 IP 地址范围），由 IP 和子网掩码组成。
上行带宽	设置 PPTP 客户端的最大上行带宽。
下行带宽	设置 PPTP 客户端的最大下行带宽。
工作模式	NAT：对经过此 PPTP 隧道的数据包进行 NAT 转换（数据包的源 IP 替换为 PPTP 隧道的本地虚拟 IP）。 路由：对经过此 PPTP 隧道的数据包只进行路由转发。
状态	滑块为灰色表示禁用，滑块为蓝色表示启用。

在线检测模式	在线检测是通过 PING 和 DNS 检测接口是否在线： 自动：PING 检测选择网关指定互联网地址作为目的地址，DNS 检测选择接口的 DNS 服务器作为目的地址。 永远在线：不对接口进行任何在线检测，接口状态一直在线。 手动：手动指定 PING 检测和 DNS 检测的地址，判断接口是否在线。

在客户端列表中，可以对已保存的PPTP客户端信息进行相应设置。

4.6.3.3 隧道信息列表

在此将列出路由器上所有PPTP隧道的相关信息。

界面进入方法：VPN >> PPTP >>隧道信息列表

图 4-52 PPTP隧道信息界面

上图中显示的条目1表示目前这条隧道已成功建立，列表中会显示当前隧道建立时，隧道所使用的虚拟接口名称、本地虚拟IP地址、隧道对端的虚拟IP地址和实际IP地址等信息。

4.6.4 用户管理

4.6.4.1 用户管理

您可以配置 L2TP/PPTP 服务器的用户信息。

界面进入方法：VPN >> 用户管理 >> 用户管理

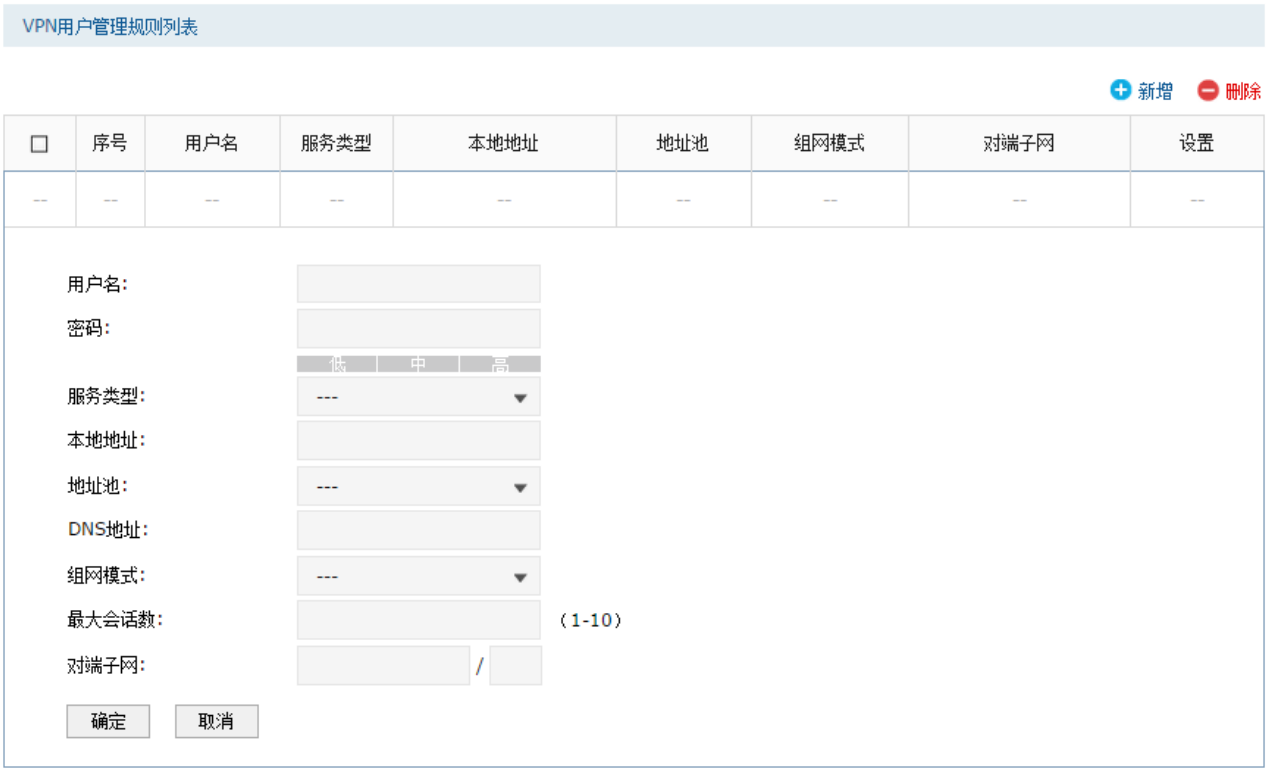


图4-53 VPN用户管理界面

界面项说明：

- **VPN用户管理规则列表**

用户名	您可以配置 L2TP/PPTP 服务器的用户信息。
密码	允许拨入的用户名称和密码。
服务类型	根据不同的 VPN 类型选择。
本地地址	VPN 隧道的本地虚拟 IP 地址。此地址可以设置为 LAN 网段之外的任意地址，对端拨通后可通过此 IP 管理路由器。
地址池	L2TP/PPTP 服务器分配给客户端的 IP 地址从地址池内获取。
DNS 地址	L2TP/PPTP 服务器分配给客户端的 DNS 地址，如 8.8.8.8。
组网模式	PC 到站点：拨入的客户端是个人用户，往往由单个计算机拨入实现远端计算机与本地局域网的通信。 站点到站点：拨入的客户端是一个网段的用户，往往通过一个路由器拨入，

实现隧道两端局域网的通信。

最大会话数	每个用户允许接入的最大客户端数量。注意：用户类型为自动的用户，意味着 L2TP 和 PPTP 的最大接入客户端数量均为最大会话数。
对端子网	L2TP/PPTP 隧道对端局域网使用的 IP 地址范围（一般可以填隧道对端设备 LAN 口的 IP 地址范围），由 IP 和子网掩码组成。

4.6.4.2 IP 地址池

您可以通过本页面设置地址池条目，进行地址池的管理。

界面进入方法：VPN >> 用户管理 >> IP地址池

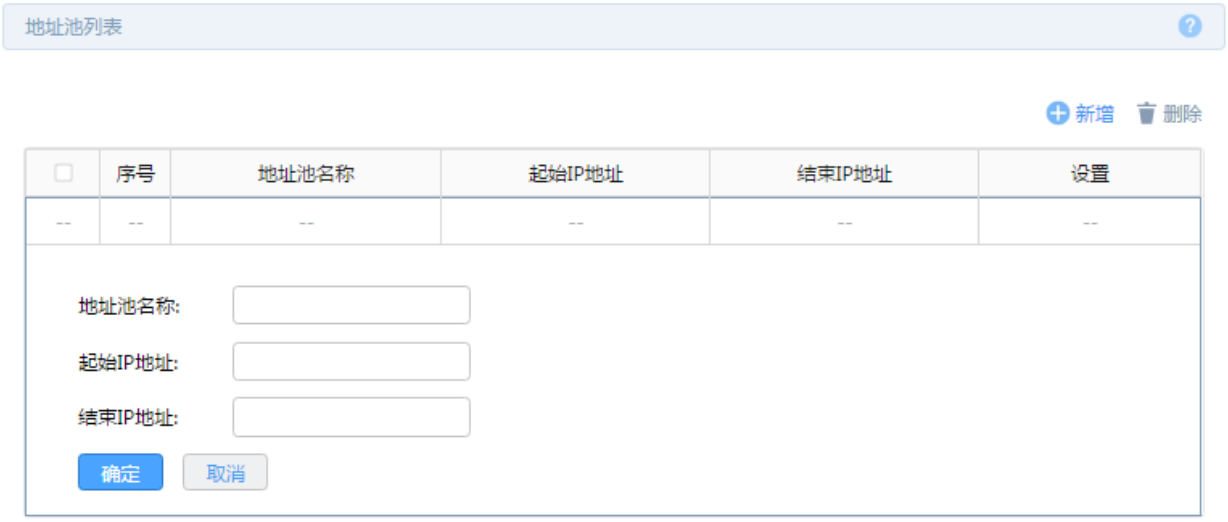


图4-54 IP地址池设置界面

界面项说明：

- **新增地址池**

地址池名称	标识地址池的名称。
起始 IP 地址	设置地址池起始地址。
结束 IP 地址	设置地址池结束地址。

注意：

- 由地址池起始 IP 和地址池结束 IP 组成，且地址池起始 IP 必须不大于地址池结束 IP，而且不能与已有的地址池范围重叠。当前一个地址池最多可以包含 1024 个 IP。

4.7 认证管理

4.7.1 Web 认证

4.7.1.1 Web 认证

您可以通过本页面设置 Web 认证功能。

界面进入方法：认证管理 >> Web认证 >> Web认证

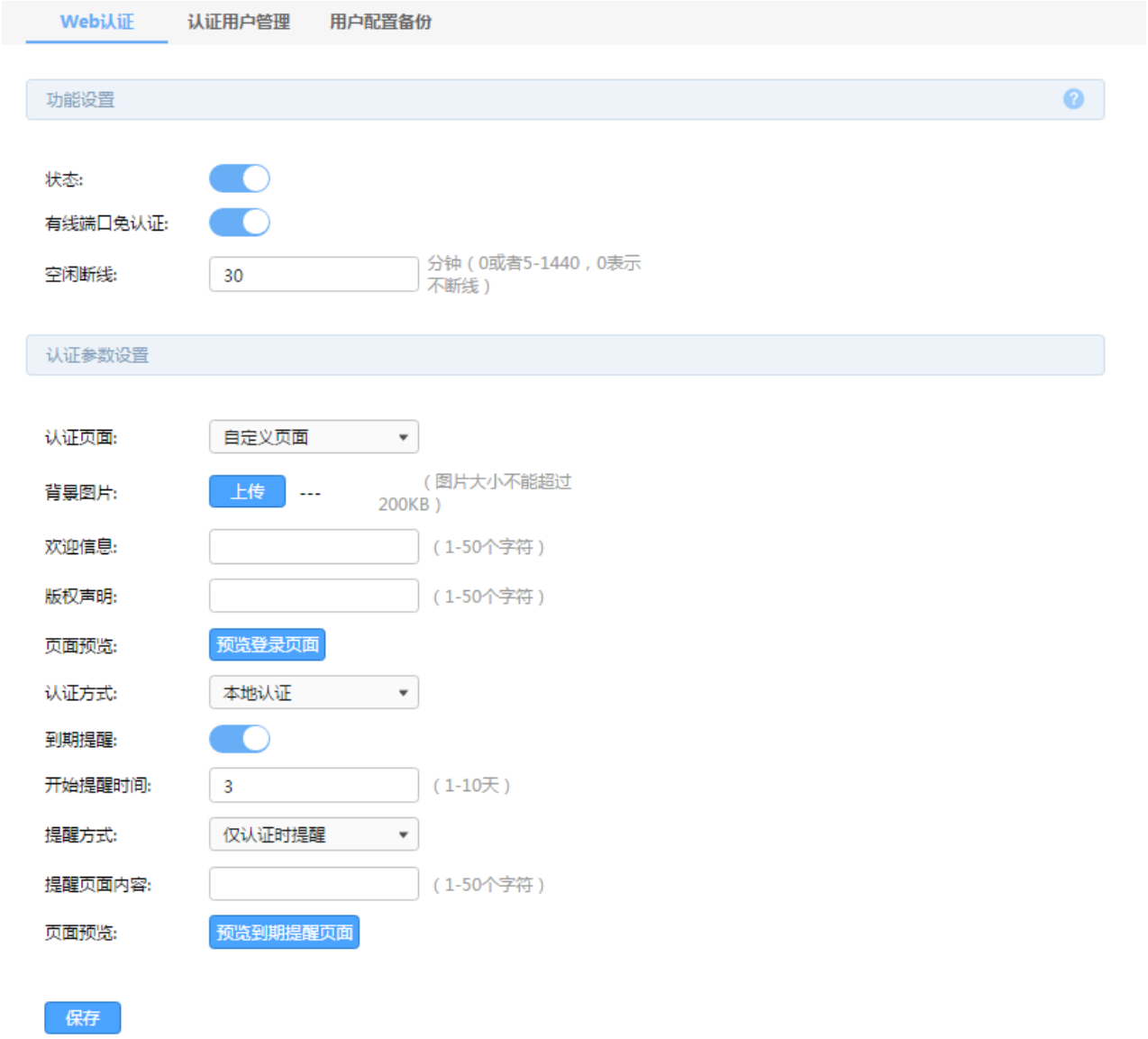


图 4-55 Web认证设置界面

界面项说明：

- **功能设置**

状态	滑块为灰色表示禁用，滑块为蓝色表示启用。
有线端口免认证	启用该功能后有线端口直接跳过认证阶段。滑块为灰色表示禁用，滑块为蓝色表示启用。
空闲断线	启用该功能后，如果接入设备下线时长达到空闲时间，将会被清除认证状态。

- **认证参数设置**

（1）若认证页面选择“自定义页面”，须填写如下内容：

认证页面	选择“自定义页面”将使用路由器自带的页面版式，选择“外部链接”终端将重定向到外部链接上获取认证页面信息。
背景图片	用于自定义页面的背景展示图，图片大小限制在 200KB 以内。
欢迎信息	显示自定义页面的欢迎信息。
版权声明	显示自定义页面的版权声明信息。
页面预览	用于预览登录页面。
认证方式	选择认证的方式，有本地认证、radius 认证和一键上网可供选择。 本地认证：通过用户管理页面设置的本地用户进行认证。 radius 认证：使用外部配置的认证服务器进行认证，如果认证服务器不指定上网时长值，上网时长将设置为默认值 30 分钟。 一键上网：通过一键设置通过认证，无需用户名密码。

- 认证方式选择“本地认证”时，需填写下述内容：

图 4-56 本地认证设置界面

到期提醒	本地认证方式时，可以设置在用户即将到期时提醒用户。滑块为灰色表示禁用，滑块为蓝色表示启用。
开始时间提醒	设置帐号到期前几天开始提醒用户。
提醒方式	认证时提醒只在认证成功后提醒用户一次；周期提醒会在开始提醒时间范围内，每隔一段时间提醒用户。
提醒页面内容	设置提醒页面内容。
页面预览	预览用于提醒用户到期的页面。

- 认证方式选择“radius 认证”时，须填写下述内容：

图4-57 radius认证设置界面

主服务器地址	填写外部 radius 认证服务器地址。
备用服务器地址	选择 radius 认证时，备用的 radius 服务器地址。
认证端口	用于 radius 认证的端口号。
授权共享密钥	外部 radius 认证授权共享密钥。
失败发送次数	radius 认证失败后，重复发送认证请求的次数。
超时时间	radius 认证超时时间。
认证方式	支持 PAP 和 CHAP 两种认证方式。PAP 是采用认证用户名密码不加密的方式，CHAP 采用认证用户名不加密，认证密码加密的方式认证。

- 认证方式选择“一键上网”时，须填写下述内容：

图 4-58 一键上网认证设置界面

免费上网时长	设置一键上网的免费时长，1-1440 分钟。

（2）若认证页面选择“外部链接”，须填写如下内容：

图4-59 外部链接设置界面

认证 URL 认证页面选择使用外部链接，填写用于认证的 URL 信息。

认证成功跳转链接 认证页面选择外部链接，当认证成功后跳转到的链接。

认证失败跳转链接 认证页面选择外部链接，当认证失败后跳转到的链接。

认证方式选择请参考上文“自定义页面”的部分说明。

4.7.1.2 认证用户管理

您可以通过本页面进行认证用户管理。

界面进入方法：认证管理 >> Web认证 >> 认证用户管理

用户类型分为正式用户与免费用户两种，在此页面下进行设置。

图 4-60 用户管理设置界面

界面项说明：

- **认证用户规则列表**

用户类型	正式用户：存留在系统中的正式用户，具有一定的有效期，且可以绑定相应的设备 MAC 地址。可以记录更多用户的资料信息。 免费用户：免费用户具有一定的上网时长限制。

1) 若选择用户类型为“正式用户”，需填写下述内容：

图 4-61 正式用户设置界面

用户名 用于认证登录的用户名。

密码 用户登录所使用的密码。

有效期至 正式用户的有效期。

允许认证时间段 允许用户进行认证的时间。

MAC 地址绑定方式 选择是否绑定 MAC 地址，以及绑定的方式。

不绑定：不绑定用户的 MAC 地址。

静态绑定：绑定一个静态的 MAC 地址。

动态绑定：进行动态绑定。

同时登录用户数　　最多允许同时使用该账号登录的用户数量。

上行带宽　　当前用户允许的上行带宽，以 KB/s 为单位，0 表示不限制。当开启此功能时，系统默认的 NAT 加速功能将会被关闭，因此转发性能会受到一定程度的影响。

下行带宽　　当前用户允许的下行带宽，以 KB/s 为单位，0 表示不限制。当开启此功能时，系统默认的 NAT 加速功能将会被关闭，因此转发性能会受到一定程度的影响。

姓名　　可选记录当前用户姓名。

电话　　可选记录当前用户电话。

备注　　可选记录当前用户备注。

状态　　滑块为灰色表示禁用，滑块为蓝色表示启用。

2) 若选择用户类型为“免费用户”，需配置以下内容：

图 4-62 免费用户设置界面

用户名 用于认证登录的用户名。

密码 用户登录所使用的密码。

上网时长 免费用户的免费上网时长。

允许认证时间段 允许用户进行认证的时间。

同时登录用户数 最多允许同时使用该账号登录的用户数量。

上行带宽 当前用户允许的上行带宽，以 KB/s 为单位，0 表示不限制。当开启此功能时，系统默认的 NAT 加速功能将会被关闭，因此转发性能会受到一定程度的影响。

下行带宽 当前用户允许的下行带宽，以 KB/s 为单位，0 表示不限制。当开启此功能

时，系统默认的 NAT 加速功能将会被关闭，因此转发性能会受到一定程度的影响。

备注	可选记录当前用户备注。
状态	滑块为灰色表示禁用，滑块为蓝色表示启用。

4.7.1.3 用户配置备份

您可以通过本页面备份和导入用户配置信息。

界面进入方法：认证管理 >> 用户管理 >> 用户配置备份

图 4-63 用户配置备份设置界面

界面项说明：

- **备份配置信息**

备份	点击<备份>按钮来备份和下载用户配置信息。

- **导入配置信息**

导入	点击<导入>按钮来导入用户配置信息。

4.7.2 微信连 Wi-Fi

4.7.2.1 微信连 Wi-Fi

您可以通过本页面设置微信连 WiFi 功能。

界面进入方法：认证管理 >> 微信连 Wi-Fi >> 微信连 Wi-Fi

图 4-64 微信连 Wi-Fi 设置界面

界面项说明：

- **功能设置**

状态	滑块为灰色表示禁用，滑块为蓝色表示启用。
有线端口免认证	启用该功能后有线端口直接跳过认证阶段。滑块为灰色表示禁用，滑块为蓝色表示启用。
空闲断线	启用该功能后，如果接入设备下线时长达到空闲时间，将会被清除认证状态。

- **微信公众平台参数设置**

SSID	无线网络的 SSID。
ShopID	商家微信公众平台门店 ID。
AppID	商家微信公众平台账号。
Secretkey	商家微信工作平台账号的密钥。
微信连 Wi-Fi 设置说明	通过该链接您可以看到更详细的设置教程。您需要连接互联网才能查看该教程。

- **认证页面设置**

背景图片	设置微信认证页面的背景图片。点击<上传>按钮来设置您的自定义背景图片。如不上传，则会使用设备自带的默认背景图片。
Logo 图片	设置微信认证页面的 Logo 图片。点击<上传>按钮来设置您的自定义 Logo 图片。点击<删除>按钮将删除上传的 Logo 图片并使用默认 Logo 图片。
Logo 信息	设置微信认证页面的 Logo 信息。Logo 信息位于 Logo 图片的正下方。可以输入 1-25 个字符。
欢迎信息	设置微信认证页面的欢迎信息。欢迎信息位于登录按钮的上方。可以输入 1-50 个字符。
登陆按钮提示文字	设置微信认证页面的登录按钮提示文字。可以输入 1-15 个字符。

版权声明	设置微信认证页面的版权声明。版权声明位于认证页面底部。可以输入 1-25 个字符。
页面预览	通过点击<预览 Portal 页面>按钮可以预览设置后的微信认证页面效果。

- **免费上网时长设置**

免费上网时长设置	设置用户通过认证后能使用网络的时长，可设置最短 1 分钟，最长 1440 分钟。

以上所有设置在设置完成后需点击<保存>按钮使其生效。

4.7.2.2 强制关注

您可以通过本页面启用微信强制关注功能。

界面进入方法：认证管理 >> 微信连 Wi-Fi >> 强制关注

图 4-65 微信强制关注设置界面

界面项说明：

- **微信强制关注设置**

强制关注开关	开启强制关注功能后，用户需要关注您的公众号才能上网。

公众号二维码	上传您的公众号二维码，提供给用户进行识别关注。
完成按钮 URL	将此处给出的 URL 粘贴到微信公众号平台中的“完成页面”链接完成强制关注的相关配置。
公众号认证 URL	将此处给出的 URL 以文字消息或者公众号菜单的方式提供给用户来完成认证。

注意：

启用微信强制关注功能前，必须开启并正确配置“微信连Wi-Fi”功能。

4.7.3 免认证策略

您可以通过本页面设置和查看免认证策略信息，免认证策略用来配置用户在认证通过前可以免费访问的资源。

免认证策略分为两种认证方式。

界面进入方法：认证管理 >> 认证设置 >> 免认证策略

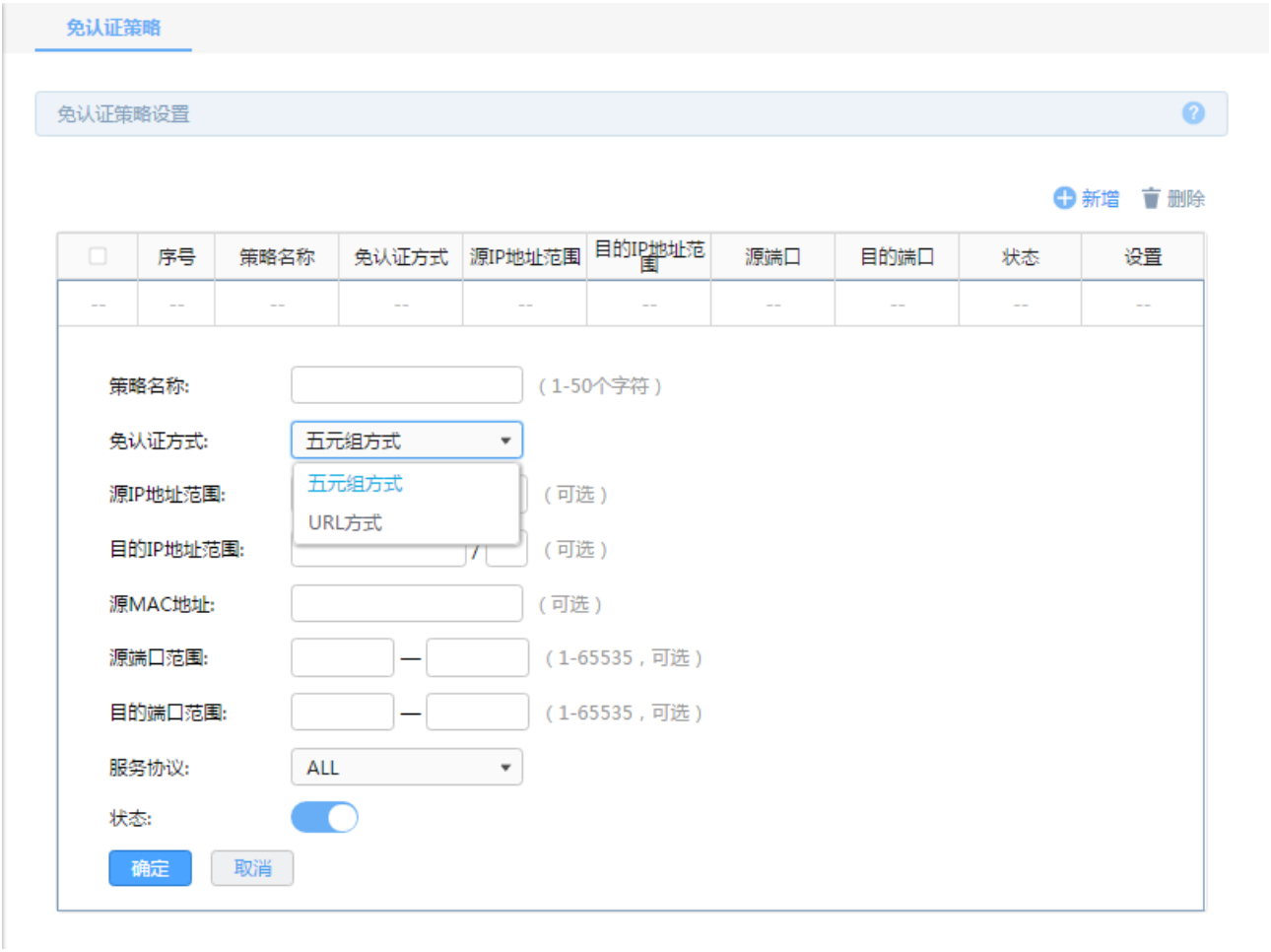


图 4-66 免认证策略设置界面

界面项说明：

- **免费认证策略设置**

  策略名称 设置免认证策略的名称。

  免认证方式 设置免认证策略的方式，可选择五元组和 URL 两种方式。

1) 若选择五元组方式，需配置以下内容：

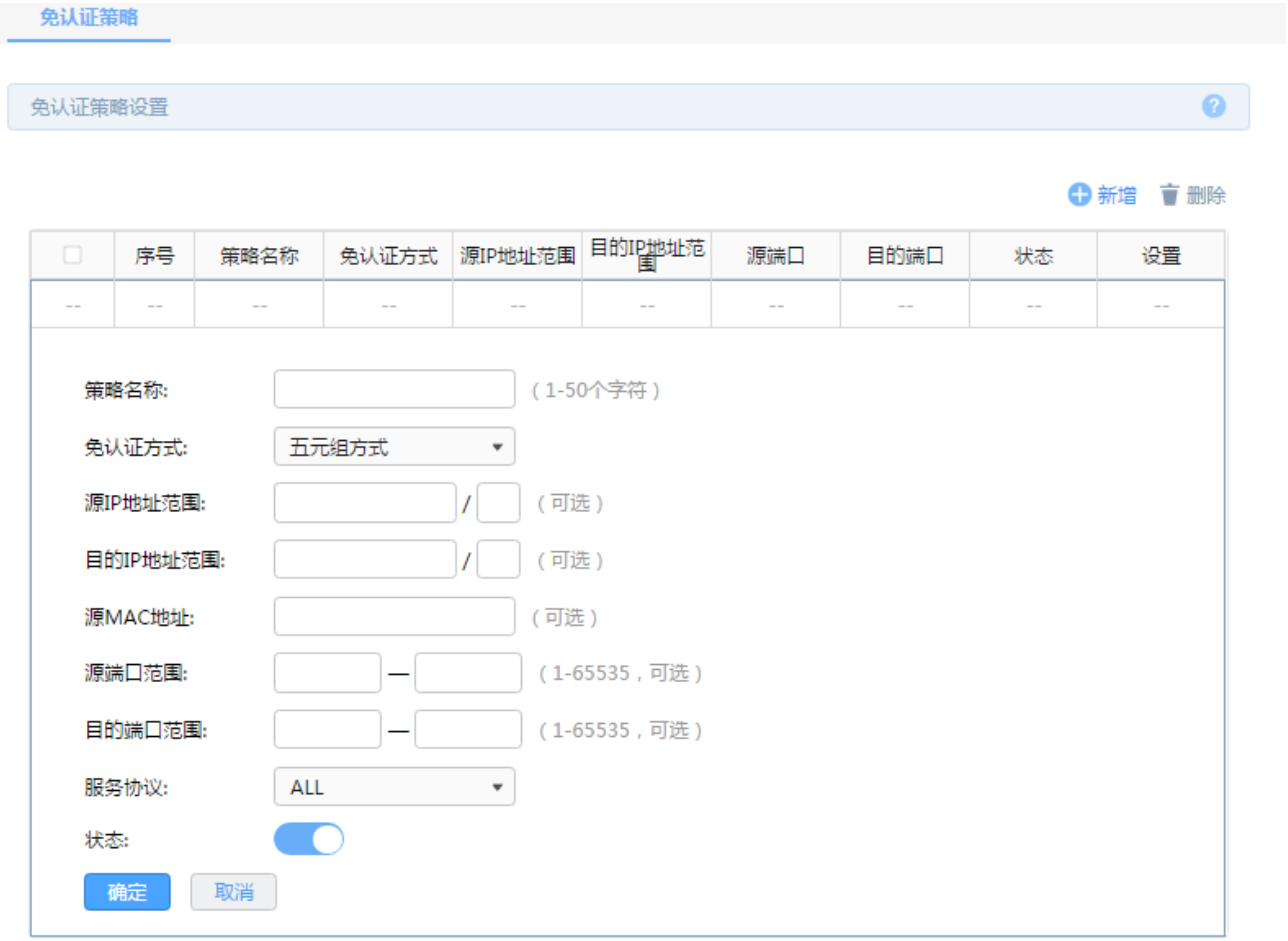


图 4-67 五元组方式设置界面

源 IP 地址范围 设置免认证策略的源 IP 地址和网络掩码。

目的 IP 地址范围 设置免认证策略的目的 IP 地址和网络掩码。

源 MAC 地址 设置免认证策略的源 MAC 地址。

源端口范围 设置免认证策略的源端口范围。

目的端口范围 设置免认证策略的目的端口范围。

服务协议 设置免认证策略的服务协议。

备注 您可以设置免认证策略的备注，以方便您管理和查找。备注最多支持 50 个字符。

状态 选择是否启用该免认证策略。

2) 若选择URL方式，需配置以下内容：

图 4-68 URL 方式设置界面

URL 地址 设置免认证的目的网络地址。

源 IP 地址范围 设置免认证策略的源 IP 地址和网络掩码。

源 MAC 地址 设置免认证策略的源 MAC 地址。

源端口范围 设置免认证策略的源端口范围。

状态 选择是否启用该免认证策略。

4.7.4 认证状态

您可以在该页面下查看认证状态。

界面进入方法：认证管理 >> 认证状态

图 4-69 认证用户列表

界面项说明：

- **认证用户列表**

认证方式	用户接入时采用的认证方式。
接入时间	用户接入的时间。
IP 地址	用户的 IP 地址。
设置	可断开用户连接

您可以点击 刷新，手动刷新认证用户列表；您可以点击 下线，批量断开用户连接。

4.8 高级功能

4.8.1 路由设置

路由，是选择一条最佳路径把数据从源地点传送到目的地点的行为。

4.8.1.1 策略路由

在此可以通过指定协议、地址范围、端口、WAN口、生效时间等，精确地控制路由选路。

界面进入方法：高级功能 >> 路由设置 >> 策略路由

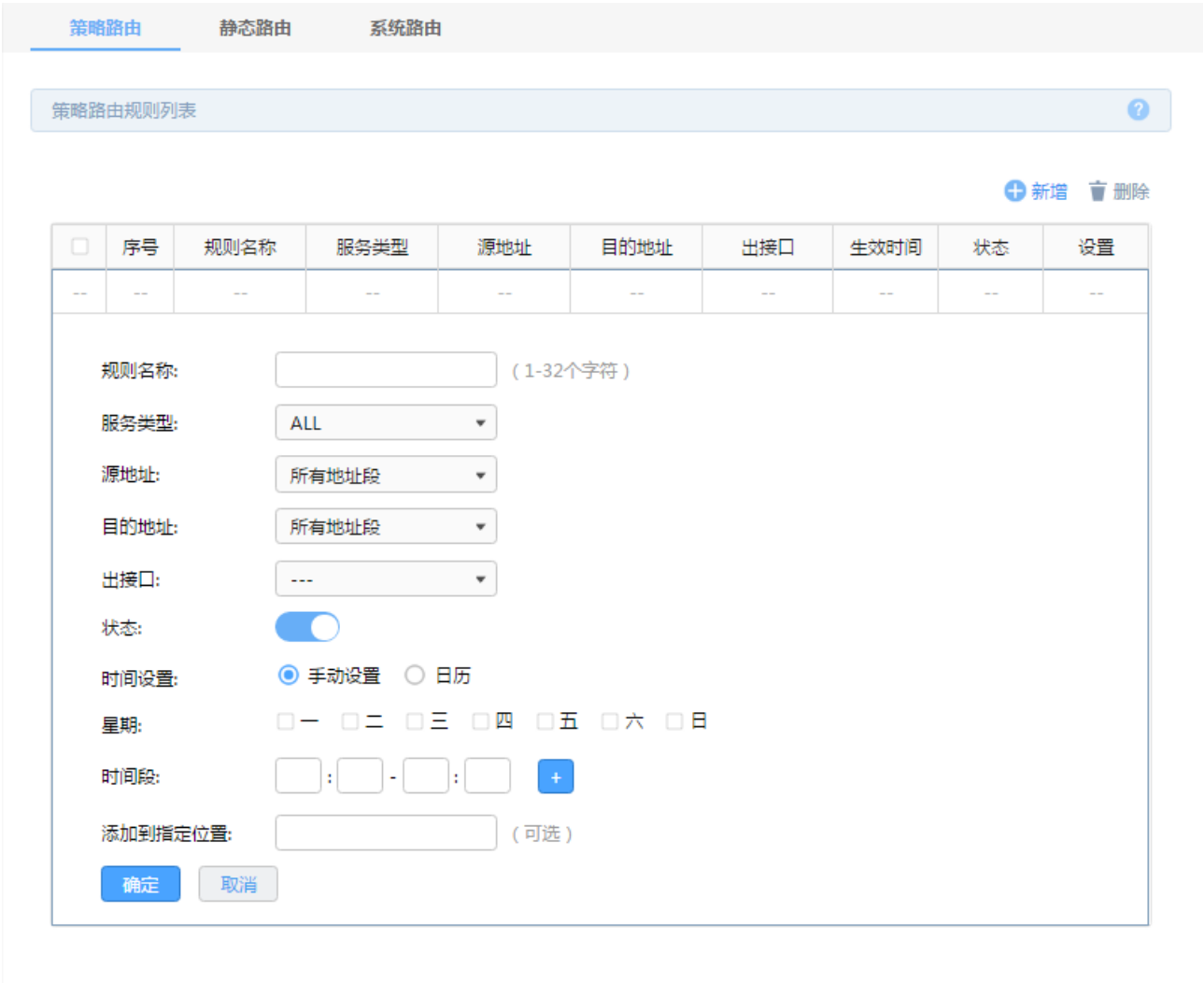


图 4-70 策略路由设置界面

点击 新增 按钮可以新增一条策略路由规则。

界面项说明：

- **策略路由规则列表**

规则名称	设置策略路由规则的名称。
服务类型	策略选路功能针对特定的协议生效。
源地址	您可以选择地址对象，以建立选路规则条目的源地址范围。
目的地址	您可以选择地址对象，以建立选路规则条目的目的地址范围。
出接口	您可以选择符合此选路规则条目数据包的出接口。

状态	滑块为灰色表示禁用，滑块为蓝色表示启用。
时间设置	用于设置时间所包含的时间段，有两种设置方式。 日历：通过在日历上划分矩形覆盖对应的时间区域来设置包含的时间段，只能精确到小时。 手动设置：通过手动输入生效时间段并勾选生效星期来设置一个时间段，精确到分钟，但一个对象最多只能设置 12 个时间段。
添加到指定位置	将路由规则添加到指定的位置。

4.8.1.2 静态路由

静态路由则是由网络管理员手动配置的一种特殊路由，具有简单、高效、可靠等优点。

静态路由不随着网络拓扑的改变而自动变化，多用于网络规模较小，拓扑结构固定的网络中。当网络的拓扑结构或链路的状态发生变化时，网络管理员需要手动修改路由表中相关的静态路由信息。

界面进入方法：高级功能 >> 路由设置 >> 静态路由

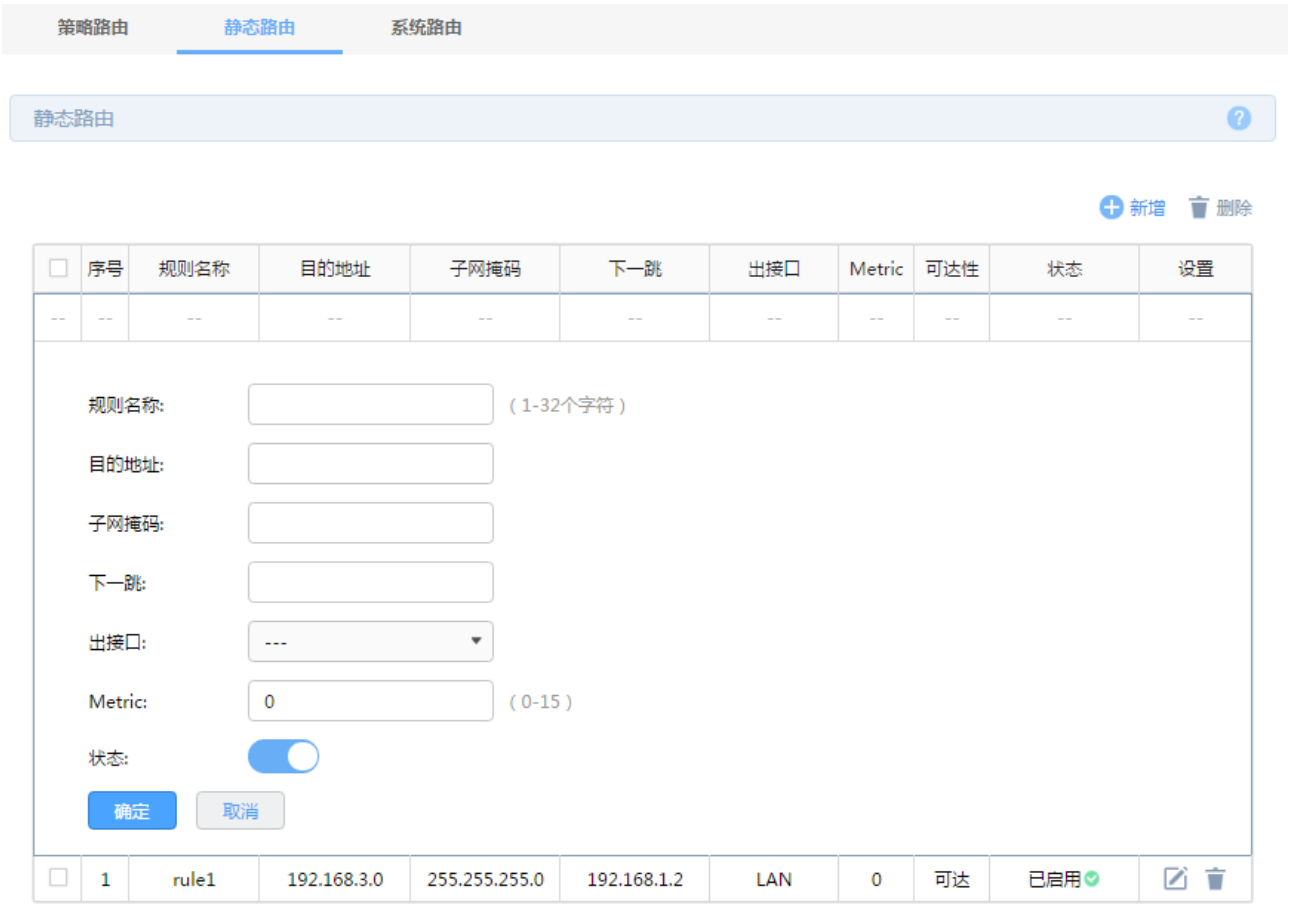


图 4-71 静态路由设置界面

点击 新增 按钮，可以新增一条静态路由规则.

界面项说明：

- **静态路由规则**

规则名称	输入该规则条目的名称。
目的地址	设置静态路由规则条目指向的目标网络地址。
子网掩码	设置静态路由规则条目指向的目标网络的子网掩码。
下一跳	设置通往目标网络的路由路径上下一个节点的IP地址。
出接口	设置数据从本地发出的出接口。
Metric	设置路由规则的优先级，数值越低则优先级越高，0为最高优先级。当网络中存在多条路由可以到达同一目的地址，可以通过调整Metric来调整路由规则的优先级，数据包将按照Metric值最小的路径转发。

状态	滑块为灰色表示禁用，滑块为蓝色表示启用。

上图中序号1规则的含义：发往目标网络192.168.3.0/24的数据可以通过接口LAN发往192.168.1.2节点上，节点192.168.1.2将执行下一个转发任务，此静态路由规则的Metric值为0拥有最高优先级。

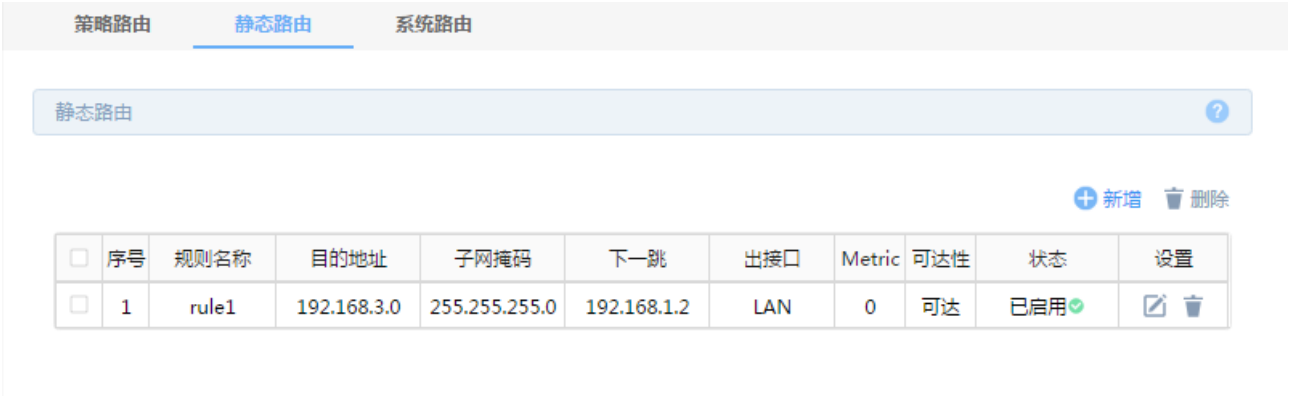


图 4-72 静态路由设置界面-序号1规则

应用举例

路由器下的 LAN1 网段为 192.168.1.0 /24，三层交换机下 LAN2 网段为 192.168.2.0 /24，LAN3 网段为 192.168.3.0 /24，三层交换机与路由器的 LAN 口级联 IP 为 192.168.1.2。现要实现 LAN1 网段的主机访问 LAN2/LAN3 网段的主机。

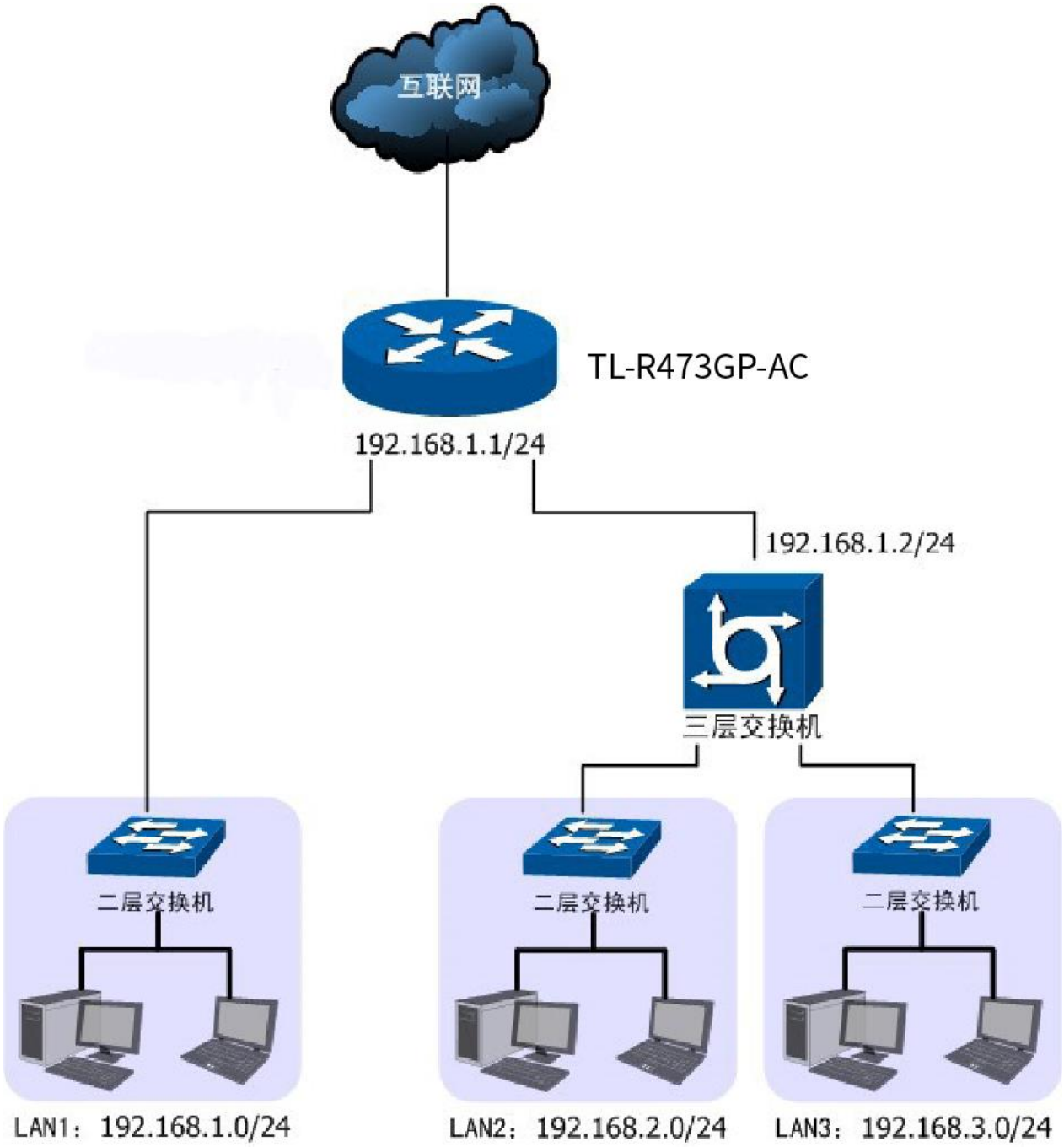


图 4-73 静态路由功能组网应用

配置步骤：

路由器要完成上述网络需求，需要配置静态路由功能，配置步骤如下：

1) 创建静态路由规则，设置到LAN2网段的下一跳地址为三层交换机的级联口IP地址192.168.1.2。界面进入方法：高级功能 >> 路由设置 >> 静态路由。规则设置如下，点击<新增>按钮完成。

规则名称	rule1
目的地址	192.168.2.0

子网掩码	255.255.255.0
下一跳	192.168.1.2
出接口	lan
Metric	0
备注	LAN2

2) 创建静态路由规则，设置到LAN3网段的下一跳地址为三层交换机的级联口IP地址192.168.1.2。界面进入方法：高级功能 >> 路由设置 >> 静态路由。规则设置如下，点击<新增>按钮完成。

规则名称	rule2
目的地址	192.168.3.0
子网掩码	255.255.255.0
下一跳	192.168.1.2
出接口	lan
Metric	0
备注	LAN3

4.8.1.3 系统路由

通过本页面可查看系统路由表。

界面进入方法：高级功能 >> 路由设置 >> 系统路由

序号	目的地址	子网掩码	下一跳	出接口	Metric
1	192.168.3.0	255.255.255.0	192.168.1.2	LAN	0
2	127.0.0.0	255.0.0.0	0.0.0.0	lo	0
3	172.33.1.0	255.255.255.0	0.0.0.0	WAN1	0
4	192.168.1.0	255.255.255.0	0.0.0.0	LAN	0

图 4-74 系统路由列表

界面项说明：

- **策略路由规则列表**

目的地址 数据包需要到达的地址。

子网掩码 目的地址的子网掩码。

下一跳 数据包到达目的地址前可以直接转发的下一个路由器地址。

出接口 数据包进行转发的接口。

Metric 数据包到达目的需要的跳数。

4.8.2 NAT设置

路由器通过NAT（Network Address Translation，网络地址转换）技术，可以在局域网主机主动发起对广域网的访问时实现双方的互相通信。其原理是：当通信数据包经过路由器时，NAT技术会将数据包中的IP地址在局域网地址与广域网地址间转换，同时也进行端口号的转换。

如今随着计算机的普及，广域网IP地址已经供不应求，通过NAT技术，局域网内所有主机在通信时可以使用一个广域网IP地址，而局域网内不同的主机使用不同的端口号，解决了IP地址紧缺的问题。

在应用了NAT及其扩展技术的网络环境中，局域网主机是不会直接被广域网主机发现的，因此NAT也为局域网提供了一定的网络安全保障。当有广域网主机需要主动访问局域网主机时，就必须通过转发规则来实现。

4.8.2.1 NAPT

当局域网中多台设备需要访问广域网时，而网络中只有少量接口连接到Internet时，需要配置NAPT功能，使多台设备能够共享ISP接口上网。设置本功能后，源地址范围内主机发出的数据包通过指定出接口转发时，将对数据包源IP地址和传输协议端口的NAPT地址转换，使用出接口的IP地址和传输协议端口与内网主机应用对应。

界面进入方法：高级功能 >> NAT设置 >> NAPT

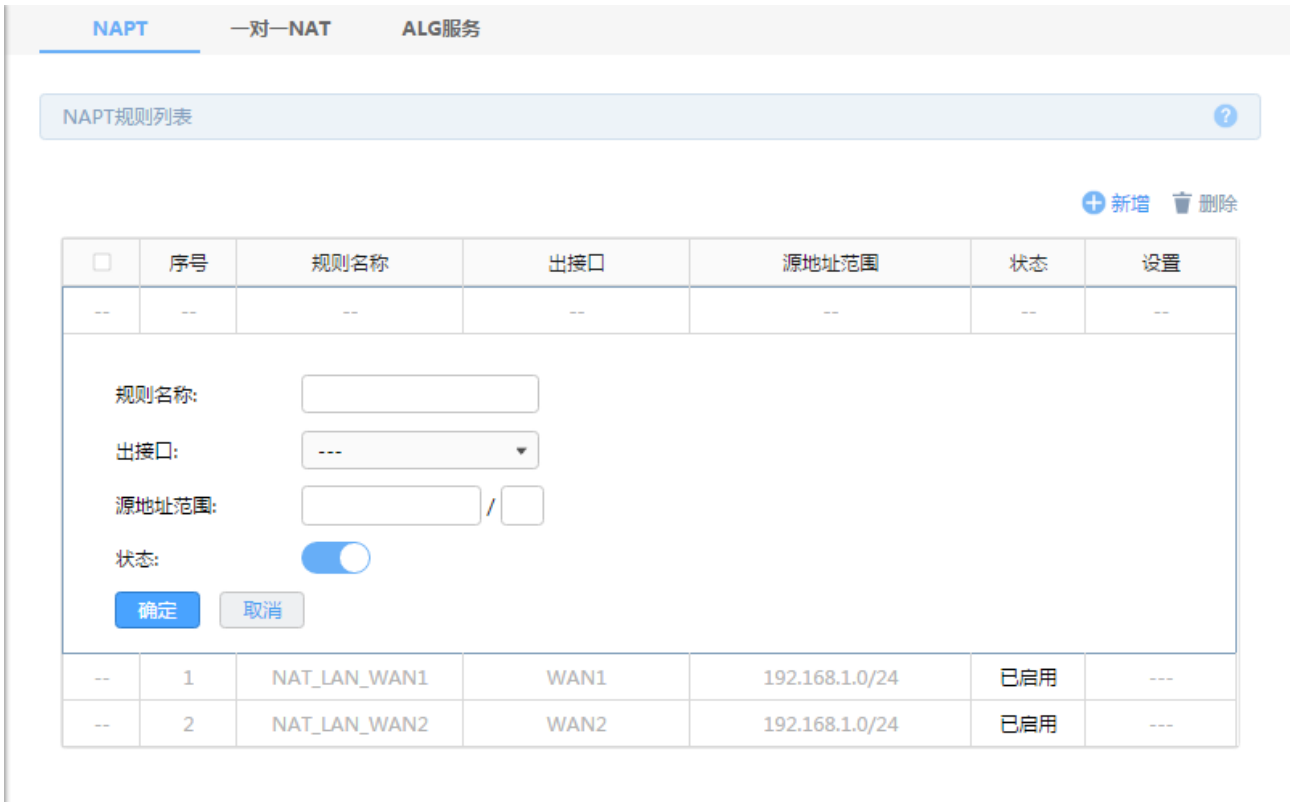


图 4-75 NAPT界面

点击 新增 按钮，可添加NAPT规则。

界面项说明：

- **NAPT规则列表**

规则名称	输入该规则条目的名称。
出接口	选择该NAPT规则的生效接口，当数据包的源IP地址在源地址内，且从该接口转发时，路由器将对数据包进行NAPT地址转换。默认选中下拉列表中显示的第一个接口

源地址范围	设置IP地址范围，相应的NAPT规则条目只对源地址为设定范围内的数据包生效。
状态	勾选“启用”，则该规则条目生效。

说明：

- 当局域网中所有主机均需要访问 Internet 时，需要为所有子网都建立 NAPT 规则，此时可以通过设置全 0 规则快速设置，源地址范围设置为 0.0.0.0/0 即可。设置全 0 规则时，请不要设置其他 NAPT 规则，否则会引起范围冲突导致无法配置成功。
- 设置 NAPT 规则时，请注意出接口相同的 NAPT 规则源地址范围不互相重叠，否则会引起范围冲突导致无法配置成功。
- 如果 NAPT 中添加非 LAN 网段的 IP 源地址范围，需要在静态路由中添加对应路由条目。

应用举例

如下图所示，在企业原有网络中，利用三层交换机组建一个交换式网络，但因网络需求变更，网络中192.168.2.0/24网段和192.168.10.0/24网段需要访问网络，并从电信和联通各申请了一条线路同时提供上网服务，两条线路实现负载均衡，网络通过路由器上网。

分析如下：

1) 针对192.168.2.0/24网段和192.168.10.0/24网段，需要创建NAPT规则，保证路由器从电信和联通外线接口转发这两个网段的数据包时做NAPT地址转换。

2) 针对192.168.10.0/24网段，当路由器从电信和联通外线接口收到发往192.168.10.0/24网段的数据包时需要从192.168.1.1/24接口发送，因此需要在路由器上创建路由规则。

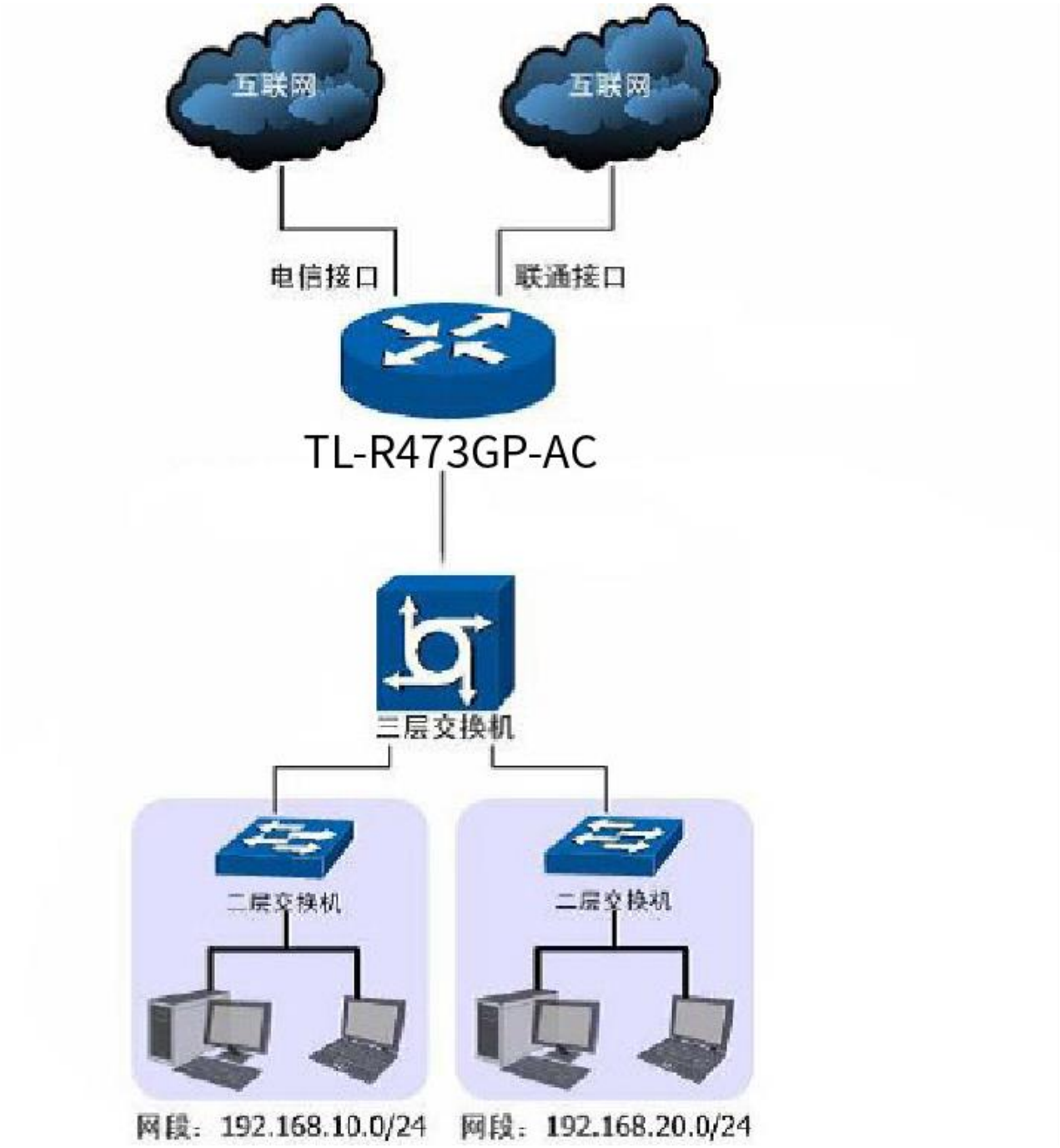


图4-76 NAPT功能组网应用

配置步骤：

路由器要完成上述网络需求，需要配置NAPT功能和路由功能，配置步骤如下：

1) 设置NAPT规则，必须操作。界面进入方法：高级功能 >> NAT设置 >> NAPT。配置192.168.2.0/24和192.168.10.0/24两个网段的数据从电信和联通两个接口转发时做NAPT地址转换，分别需要建立两个NAPT规则条目。

2) 设置静态路由，必须操作。界面进入方法：高级功能 >> 路由设置 >> 静态路由。对于网段192.168.10.0/24，其通过三层交换机连接到路由器的192.168.1.1/24接口，因此需要在路由器上建立静态路由条目，使网络192.168.10.0/24在路由器上路由可达。静态路由条目配置如下图所示。

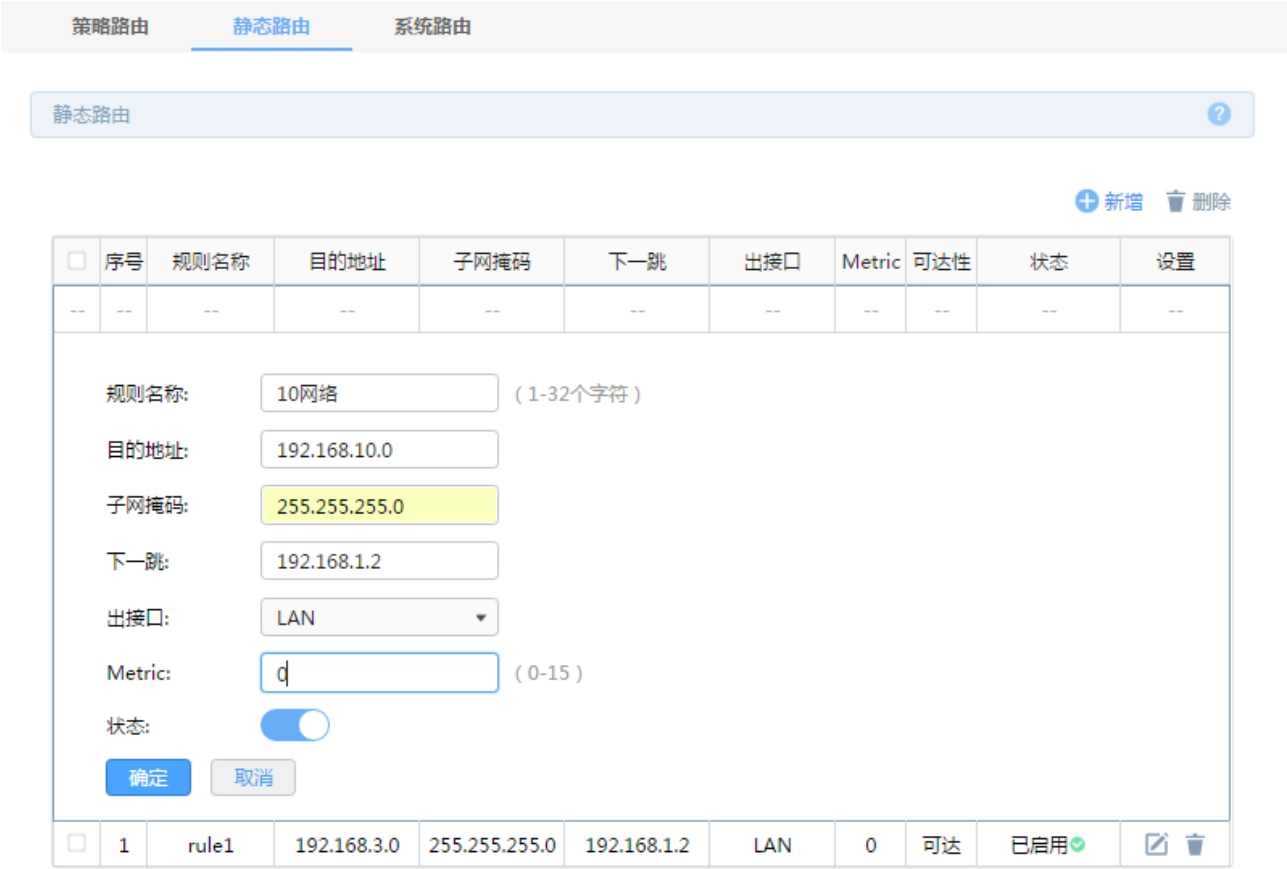


图4-77 静态路由设置

其中目的地址和子网掩码表示此静态路由条目指向的目标网络，下一跳指通往目标网络的路径上下一个网络节点的IP地址，出接口表示从路由器上的哪个接口转发数据包，Metric表示该路径的度量值，请保持为0，以保证该静态路由条目为最优路径。静态路由相关配置方法请参考静态路由部分介绍。

4.8.2.2 一对一NAT

一对一NAT，可以将局域网IP地址与广域网IP地址唯一对应，通常用于局域网内的服务器搭建。用户可以通过一对一NAT映射后的广域网地址访问局域网中的服务器，配置动态DNS功能则可以通过域名来访问服务器。

界面进入方法：高级功能 >> NAT设置 >> 一对一NAT

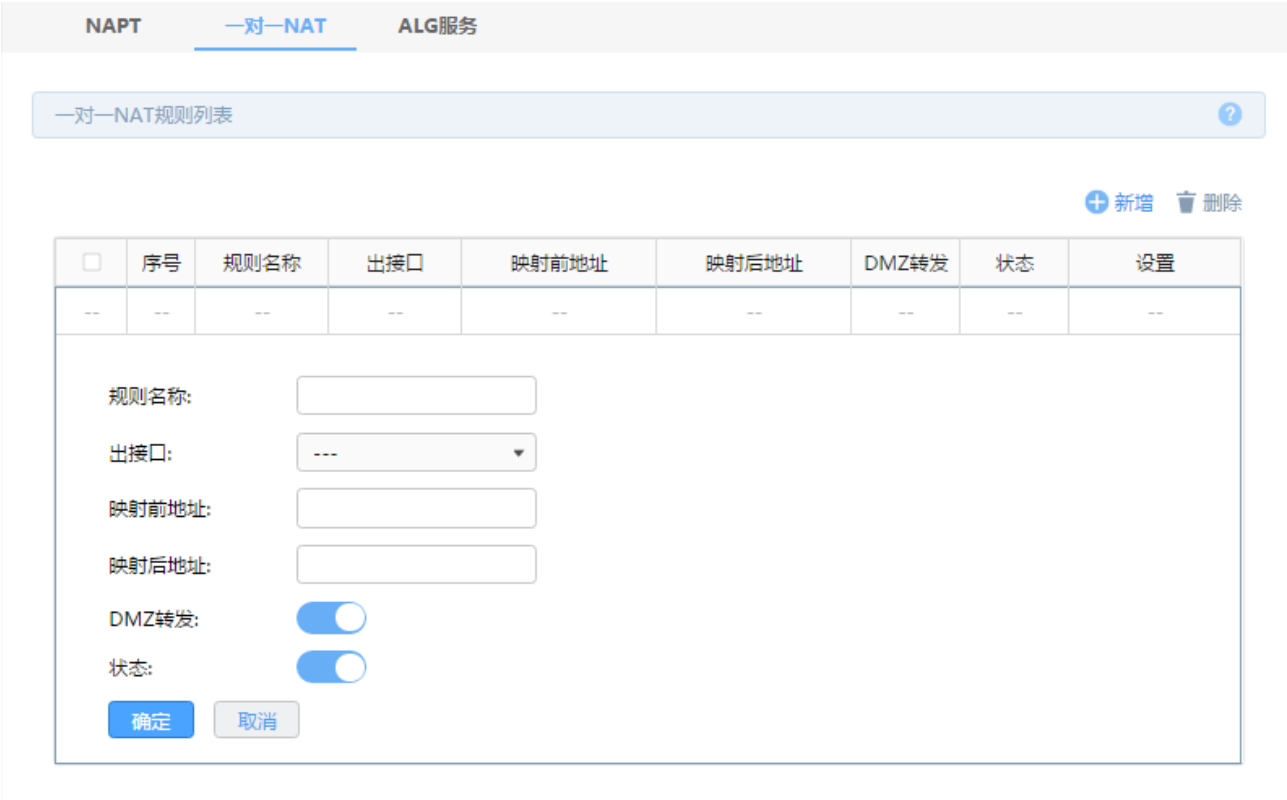


图 4-78 一对一NAT界面

点击 新增 按钮，可新增一条一对一NAT规则。

界面项说明：

➢ **一对一NAT规则列表**

规则名称	输入该映射条目的名称，例如可以根据服务器提供的服务特性命名。
出接口	选择此一对一NAT映射规则的生效接口。当数据包从该接口转发时，设备根据映射后的地址对数据包进行地址转换；对映射后地址的访问请求将转发到局域网中的服务器上。
映射前地址	进行NAT转换前的局域网IP地址。
映射后地址	映射后的IP地址
DMZ转发	设置是否开启该条NAT映射条目的DMZ转发。开启DMZ转发后，规则生效接口收到目的IP地址为映射后地址的数据包时，将把数据包转发给局域网服务器。如果广域网用户需要自由的访问局域网服务器，需要开启DMZ转发，若不开启，路由器将拒绝用户对服务器的访问。

状态	勾选“启用”，则使该规则条目生效；

下图中序号1条目的含义：路由器通过接口“WAN”转发来自设备192.168.1.10的数据包时，将对数据包做NAT地址转换，将源IP地址转换为201.0.0.1；此条目没有开启DMZ转发，“WAN”接口收到目的地址为201.0.0.1的访问请求时，会拒绝处理。

图 4-79 一对一NAT界面-序号1条目

说明：

只有当接口的IP地址为手动设置的静态IP地址时，才能够配置成一对一NAT功能的出接口。

4.8.2.3 ALG服务

ALG（Application Layer Gateway，应用层网关）。为了保证一些应用程序的正常使用，请开启ALG服务。

界面进入方法：高级功能 >> NAT设置 >> ALG服务

图 4-80 ALG服务设置界面

界面项说明：

- **ALG服务**

FTP ALG	选择启用或禁用FTP ALG服务，默认为启用，如无特殊需求请保持默认配置不变。
H.323 ALG	选择启用或禁用H.323 ALG服务，默认为启用， H.323多媒体协议多用于视频会议、IP电话等场合。
PPTP ALG	选择启用或禁用PPTP ALG服务，默认为启用，如无特殊需求请保持默认配置不变。
SIP ALG	选择启用或禁用SIP ALG服务，默认为禁用，如无特殊需求请保持默认配置不变。

4.8.3 虚拟服务器

4.8.3.1 虚拟服务器

在路由器默认设置下，广域网中的主机不能直接与局域网主机进行通信。为了方便广域网的合法用户访问本地主机，又要保护局域网内部不受侵袭，路由器提供了虚拟服务器功能。

可以通过虚拟服务器定义一个服务端口，并以IP地址指定其对应的局域网服务器，则广域网所有对此端口的服务请求都将被重定位到该服务器上。这样广域网的用户便能成功访问局域网中的服务器，同时不影响局域网内部的网络安全。

界面进入方法：高级功能 >> 虚拟服务器 >> 虚拟服务器

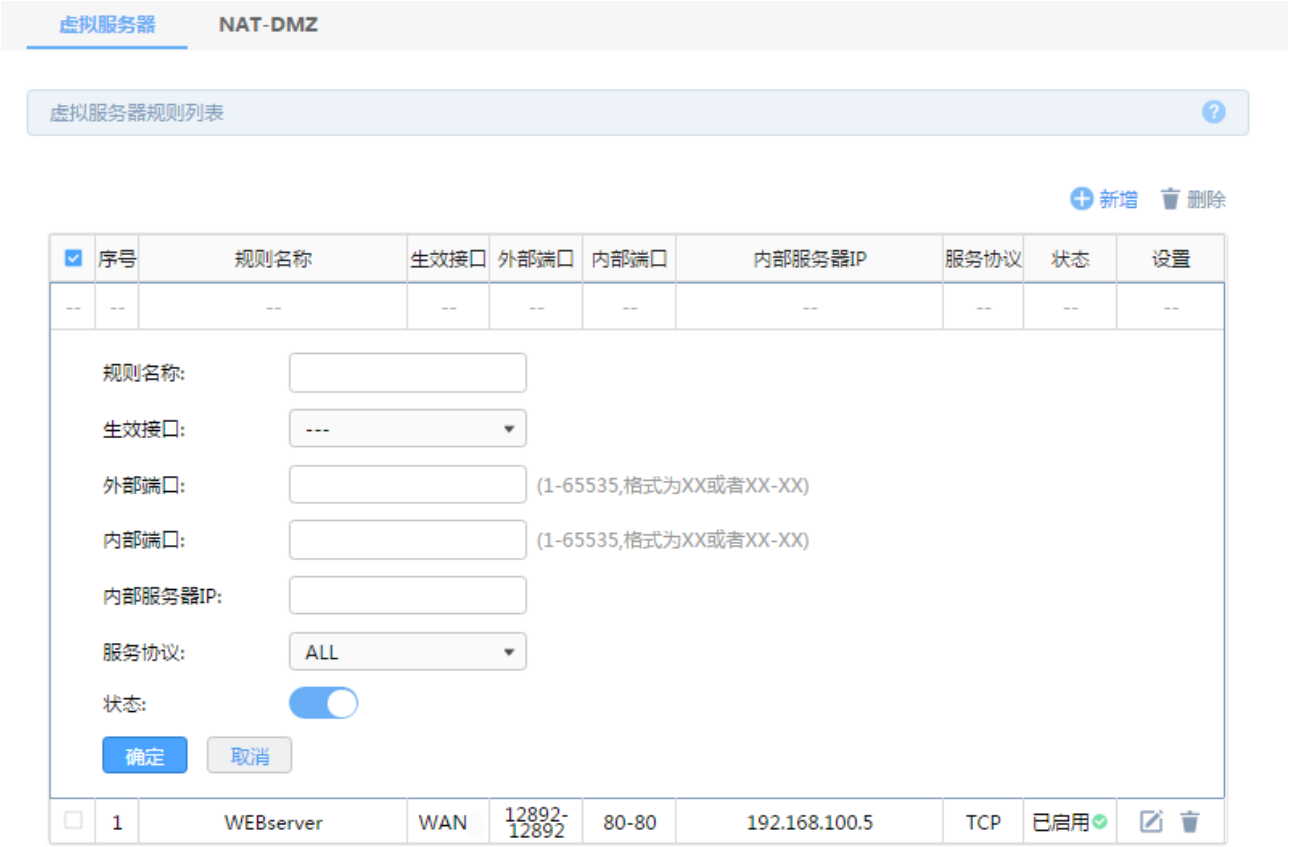


图 4-81 虚拟服务器设置界面

点击 新增 按钮，可以新增一条虚拟服务器规则。

界面项说明：

- **虚拟服务**

规则名称	输入该虚拟服务器的名称，例如可以根据服务器提供的服务特性命名。
生效接口	选择规则生效接口，当此处设置的接口收到特定外部端口的访问请求时将把数据发给局域网服务器。
外部端口	输入路由器提供给广域网访问时使用的端口，本例中使用12892端口。
内部端口	输入局域网服务器提供服务的端口，如本例中是80端口。
内部服务器IP	输入服务器的局域网IP地址。

服务协议	选择TCP，UDP协议，或者可以都选ALL，（根据内网服务器提供的服务类型而定）。
状态	滑块为灰色表示禁用，滑块为蓝色表示启用。

上图中序号1规则的含义：广域网用户向接口“WAN”的12892端口发送访问请求时，该请求将被转发给局域网中的服务器192.168.100.5的80端口上，并由真实的服务器192.168.100.5提供服务。

说明：

- 外部端口与内部端口的取值范围均为 1-65535 之间的任意整数。
- 不同虚拟服务器规则的外部端口取值不能相同，内部端口取值可相同。

4.8.3.2 NAT DMZ

DMZ（Demilitarized Zone，非军事区域）也称隔离区。位于 DMZ 区的主机完全暴露在广域网中，通常多用于放置一些必须公开的服务器设施，如企业 Web 服务器、FTP 服务器和论坛等。

NAT DMZ即DMZ主机的NAT转发规则，指定接口收到数据包时，查看所有的NAT规则，如果没有匹配项，则将数据包进行NAT地址转换后发往位于DMZ区指定的局域网计算机上。

界面进入方法：高级功能 >> 虚拟服务器 >> NAT-DMZ

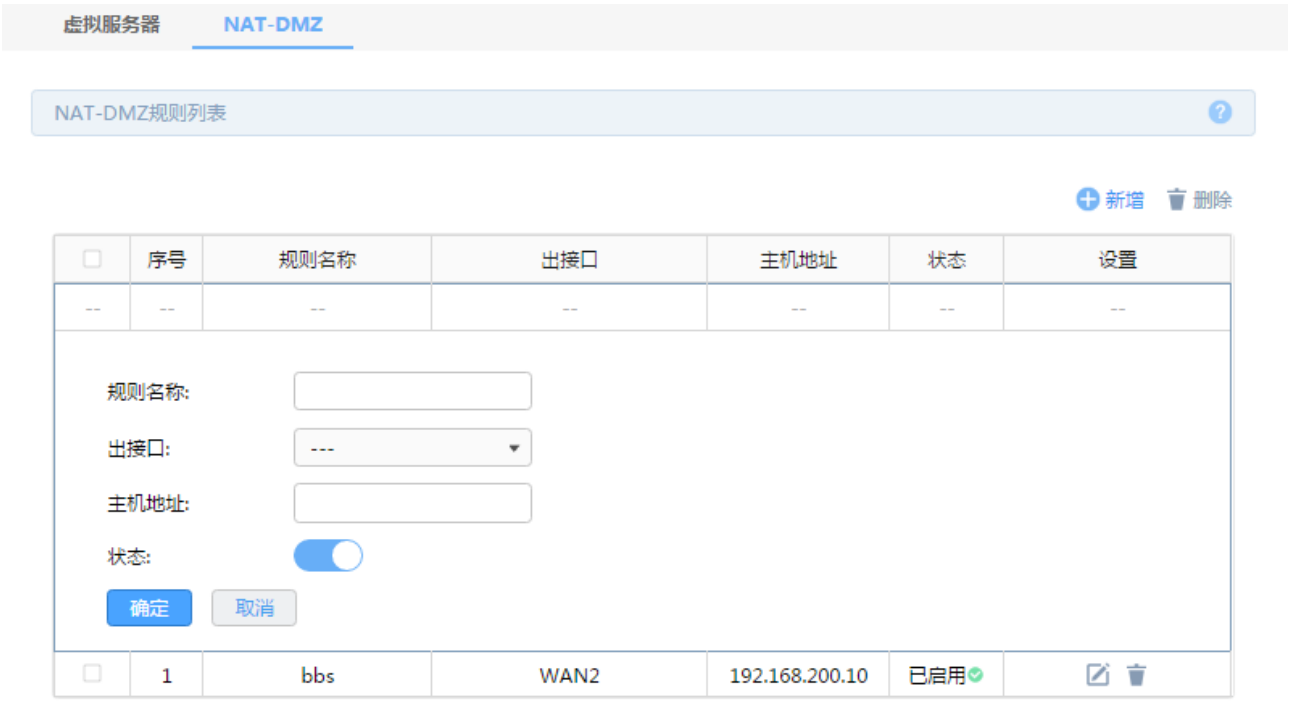


图 4-82 NAT-DMZ设置界面

点击 新增 按钮，可以新增一条NAT-DMZ规则。

界面项说明：

- **NAT-DMZ服务**

规则名称	输入该NAT转发规则的名称，例如可以根据DMZ主机特性命名。
出接口	选择规则生效接口，当此处设置的接口收到的访问请求无法匹配现有的NAT规则时，将把数据发给DMZ主机。
主机地址	输入NAT DMZ服务指向的主机地址，必须为局域网段IP地址。
状态	勾选“启用”，则使该规则条目生效。

上图中序号为1的规则的含义：接口“WAN2”收到访问请求时，如果该请求无法匹配到其他NAT功能设置的NAT规则，将被转发到局域网中IP地址为192.168.200.10的DMZ主机上。

4.8.4 PPPoE 服务器

4.8.4.1 全局设置

您可以在此页面上根据您的网络环境，对 PPPoE 服务器进行正确的配置，以保证高效管理网络。

界面进入方法：高级功能 >> PPPoE服务器>>全局设置

图 4-83 PPPoE服务器-全局设置

界面项说明：

➢ **全局设置**

PPPoE服务器	您可以勾选此项，选择是否开启 PPPoE 服务器功能。
强制PPPoE拨号	您可以勾选此项，选择是否启用强制 PPPoE 拨号功能。功能开启后，仅有拨号用户和例外 IP 的用户能使用网络。设置例外 IP，请到例外 IP 管理页面进行设置。
拨号用户互访	您可以勾选此项，选择是否开启拨号用户互访功能。拨号用户互访功能允许拨号用户之间互相通信。
首选/备选DNS服务器	请正确填写，作为 DNS 服务器地址，缺省为空。
系统最大会话数	设置会话数的最大值。
最大未应答LCP包数	作为最大未应答 LCP 包数，缺省为 10。当一条连接的未应答 LCP 包数超过这个数值时，PPPoE Server 会自动断开这条连接。
空闲断线时间	作为最大空闲断线时间，缺省为 30。请填写 0-10080（分钟），即最大为 7 天。0 代表不空闲断线。
认证方式	提供四种认证方式，请至少选择一种。

4.8.4.2 IP 地址池

您可以通过本页面设置地址池条目，进行地址池的管理。

界面进入方法：高级功能 >> PPPoE服务器>>IP地址池

图 4-84 PPPoE服务器-IP地址池

界面项说明：

点击 新增 按钮可以新增一条地址池条目。

- **IP地址池列表**

地址池名称	标识地址池的名称。
起始IP地址	设置地址池起始地址。
结束IP地址	设置地址池结束地址。

注意：

由地址池起始IP和地址池结束IP组成，且地址池起始IP必须不大于地址池结束IP，而且不能与已有的地址池范围重叠。当前一个地址池最多可以包含1024个IP。

4.8.4.3 账号管理

您可以查看账号设置信息，还可以通过表格按钮对账号设置信息条目进行操作。

界面进入方法：高级功能 >> PPPoE服务器>>账号管理

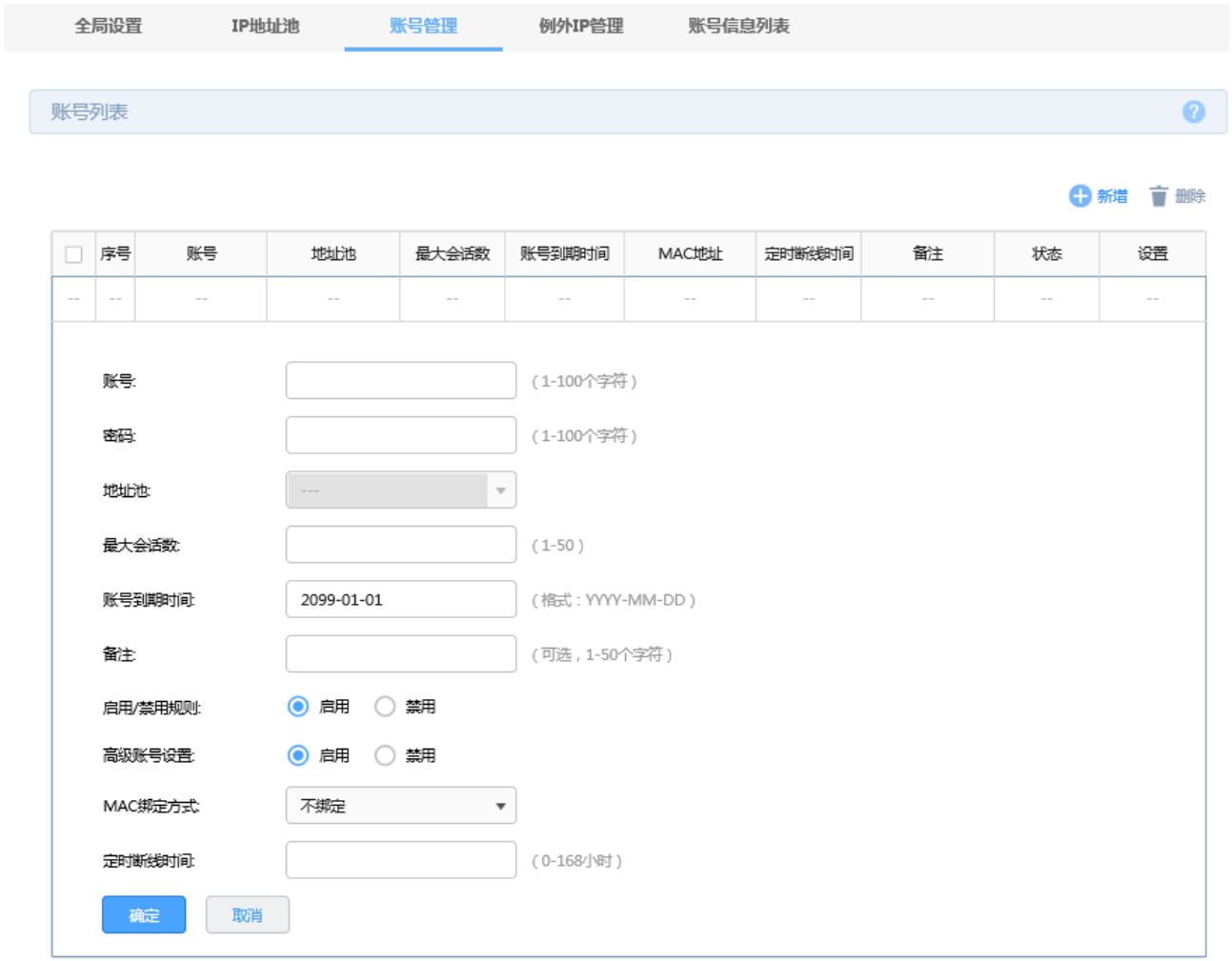


图 4-85 PPPoE服务器-账号管理

界面项说明：

点击 新增 按钮可以新增一条账号列表条目。

- **账号管理**

账号	账号规则设置的名称。
密码	账号的密码。
地址池	PPPoE 服务器分配给客户端的 IP 地址从地址池获取。
最大会话数	用户允许登陆的最大会话数。
账号到期时间	设置账号的有效时间，最大值为 2099-01-01。

备注	您可以设置规则条目备注，以方便您管理和查找。备注最多支持 50 个字符。
启用/禁用规则	您可以选择<启用>，使该规则生效。您也可以选择<禁用>，使该规则失效。
地址分配方式	您可以选择以下 3 种绑定方式。 不绑定：不进行用户和 MAC 的绑定。 静态绑定：静态绑定一个 MAC 地址，该账户只能在该 MAC 的主机上登录。 动态绑定：当用户第一次登录的时候记录其 MAC，以后用户的登录必须使用该 MAC。
MAC地址	当选择 MAC 绑定方式为静态绑定时须填写的 MAC 地址。
定时断线时间	设置定时断线的时间，当定时断线时间为 0 时，表示不会定时断线。

4.8.4.4 例外 IP 管理

您可以查看例外 IP 条目，还可以通过表格按钮对条目进行操作。

界面进入方法：高级功能 >> PPPoE服务器>>例外IP管理

图 4-86 PPPoE服务器-例外IP管理

界面项说明：

点击 新增 按钮可以新增一条例外 IP 列表条目。

➢ **例外IP管理**

起始IP地址	IP 地址段的起始 IP 地址，且起始 IP 地址必须小于或等于结束 IP 地址，而且不能与已有的 IP 地址范围重叠。
结束IP地址	IP 地址段的结束 IP 地址，且结束 IP 地址必须大于或等于起始 IP 地址，而且不能与已有的 IP 地址范围重叠。
备注	您可以对所添加的例外 IP 地址进行描述。
启用/禁用规则	您可以选择<启用>，使该规则生效。您也可以选择<禁用>，使该规则失效。

4.8.4.5 账号信息列表

您可以通过本页面查看账号的有关信息。

界面进入方法：高级功能 >> PPPoE服务器>>账号信息列表

图 4-87 PPPoE服务器-账号信息列表

界面项说明：

➢ **账号信息列表**

账号	账号名。
状态	该账号的该 IP 对应的用户当时所处的状态。同一账号可允许异地登录。
IP地址	该用户的 IP 地址。
MAC地址	该用户的 MAC 地址。
在线时间	该用户的在线时间。
备注	该用户的备注信息。
断开连接	您可以点击此项，选择强制挂断该用户。

4.8.5 动态DNS

广域网中，许多ISP使用DHCP分配公共IP地址，因此用户端获得的公网IP是不固定的。当其它用户需要访问此类IP动态变化的用户端时，很难实时获取它的最新IP地址。

DDNS（Dynamic DNS，动态域名解析服务）服务器则为此类用户端提供了一个固定的域名，并将其与用户端最新的IP地址进行关联。当服务运行时，DDNS用户端把最新的IP地址通知DDNS服务器，服务器会更新DNS数据库中域名与IP的映射关系。而对于访问它的用户端，将会得到正确的IP地址并成功访问服务端。DDNS常用于Web服务器搭建个人网站、FTP服务器提供文件共享等，访问的用户可以便捷地获取服务。

路由器作为动态DNS客户端，本身并不提供动态DNS服务。因此，在使用此功能之前，必须进入动态DNS服务提供商的官方主页注册，以获得用户名、密码和域名等信息。本路由器提供花生壳动态DNS客户端、科迈动态DNS客户端、3322动态DNS客户端。

4.8.5.1 花生壳动态域名

界面进入方法：高级功能 >> 动态 DNS >> 花生壳动态域名

图 4-88 花生壳动态域名设置界面

界面项说明：

➢ **花生壳动态域名**

服务接口	选择登录花生壳动态域名服务器的接口。
用户名	填入在花生壳网站注册的用户名。若还没有注册，请点击右边的链接“注册用户名”登录花生壳网站进行注册。
密码	填入在花生壳网站注册该用户名时所设置的密码。
状态	滑块为灰色表示禁用，滑块为蓝色表示启用。
域名	从 DDNS 服务器获取的域名服务列表，最多可以显示 16 条域名信息。

4.8.5.2 科迈动态域名

界面进入方法：高级功能 >> 动态 DNS >> 科迈动态域名

图 4-89 科迈动态域名设置界面

界面项说明：

- **科迈动态域名**

服务接口	选择登录科迈动态域名服务器的接口。
用户名	填入在科迈网站注册的用户名。若还没有注册，请点击右边的链接“注册用户名”登录科迈网站进行注册。
密码	填入在科迈网站注册该用户名时所设置的密码。
状态	选择是否启用科迈动态域名服务。
域名	从 DDNS 服务器获取的域名服务列表，最多可以显示 16 条域名信息。

4.8.5.3 3322动态域名

界面进入方法：高级功能 >> 动态 DNS >> 3322 动态域名

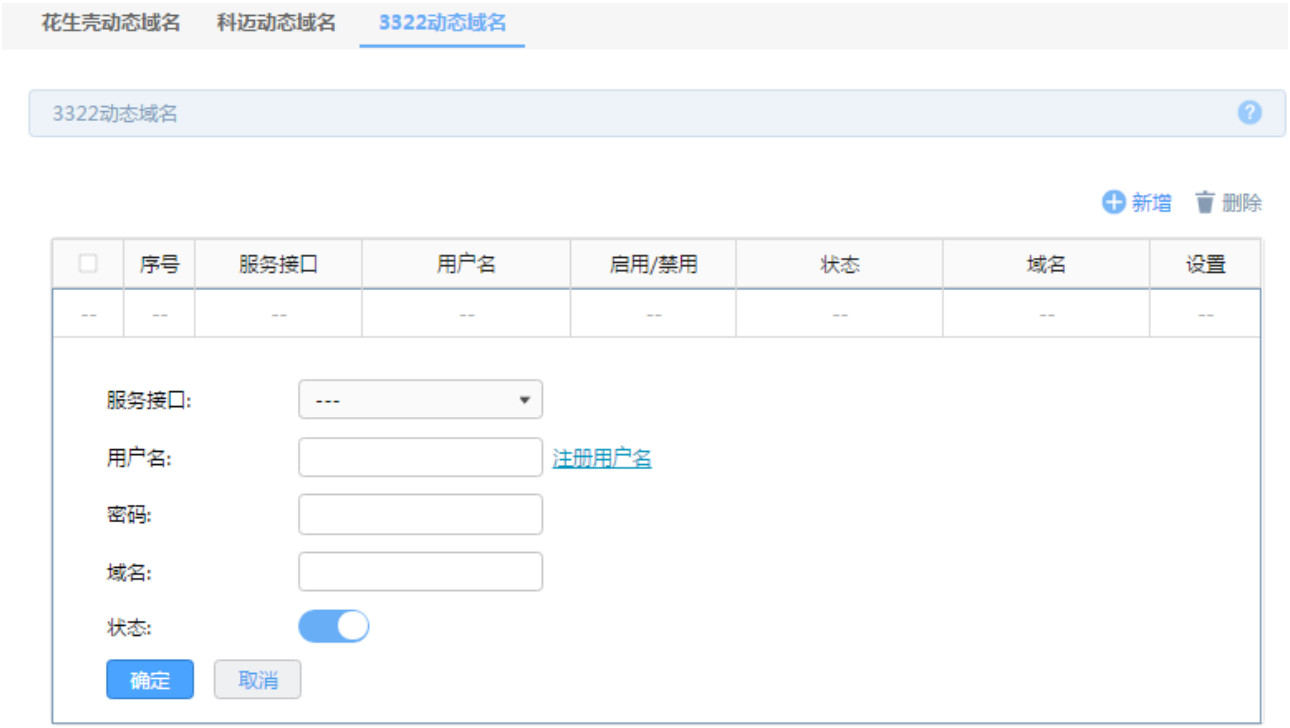


图 4-90 3322动态域名设置界面

界面项说明：

➢ **功能设置**

服务接口	选择登录3322动态域名服务器的接口。
用户名	填入在3322网站注册的用户名。若还没有注册，请点击右边的链接“注册用户名”登录3322网站进行注册。
密码	填入在3322网站注册该用户名时所设置的密码。
域名	显示当前登录的DDNS用户所拥有的域名。
状态	选择启用或禁用3322动态域名服务。

4.8.6 UPnP

UPnP（Universal Plug and Play，通用即插即用）协议，遵循此协议的不同厂商的各种设备可以自动发现对方并进行连接。

如果应用程序支持UPnP协议，而局域网中的主机安装了UPnP组件，路由器开启了UPnP服务后，局域网中的主机就可以根据软件的需要自动地在路由器上打开相应的端口，使得外部主机上的应用程序在需要时能够通过打开的端口访问内部主机上的资源，这样原本受限于NAT的功能便可以正常使用。

相对于转发规则而言，UPnP的应用不需要用户手动设置任何规则，对于一些端口不固定的应用会更加方便。

界面进入方法：高级功能 >> UPnP

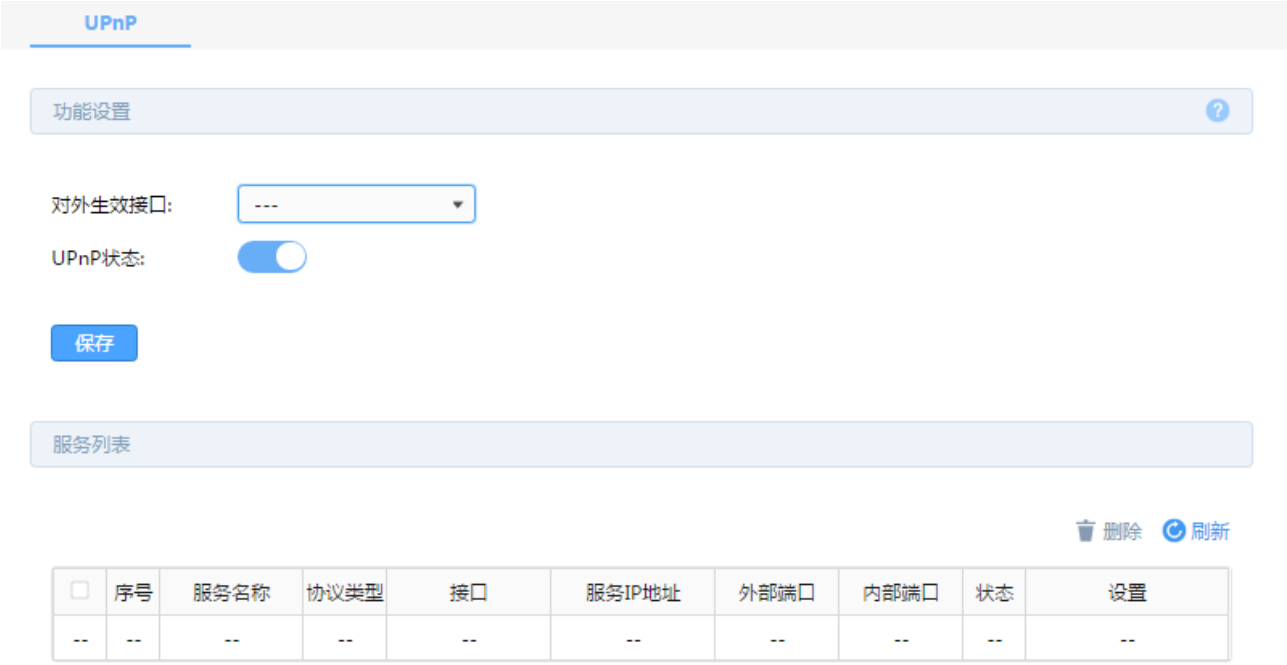


图 4-91 UPnP服务设置界面

界面项说明：

- **功能设置**

对外生效接口	指定一组接口集，该集合包含的接口将被配置以端口映射的功能。
UPnP 状态	滑块为灰色表示禁用，滑块为蓝色表示启用。

- **服务列表**

启用UPnP后，所有应用到UPnP的连接规则会显示在服务列表中。

服务名称	对应用程序所配置的端口映射的描述信息。
协议类型	表示对何种协议（TCP、UDP 或 TCP/UDP）进行端口映射。
接口	显示需要进行端口转换的路由器接口集。

服务 IP 地址	显示需要进行端口转换的主机 IP 地址。
外部端口/内部端口	显示端口映射配置的外部端口/内部端口。
状态	已启用：表示请求的端口映射功能被开启； 已禁用：表示请求的端口映射功能未生效。

说明：

- 应用时不仅要在路由器上启用 UPnP 服务，还需要确认主机操作系统和应用程序也支持此服务，即 Windows XP 系统需安装 UPnP 组件；应用程序本身需支持 UPnP，如电驴、迅雷等。
- 一些木马、病毒可能会利用 UPnP 服务打开特定的端口，使局域网主机成为黑客的攻击目标，因此需谨慎应用 UPnP 服务。

4.8.7 IP 流量统计

您可以设置启用 IP 流量统计以及监控的 IP 地址范围。

界面进入方法：高级功能 >> IP流量统计

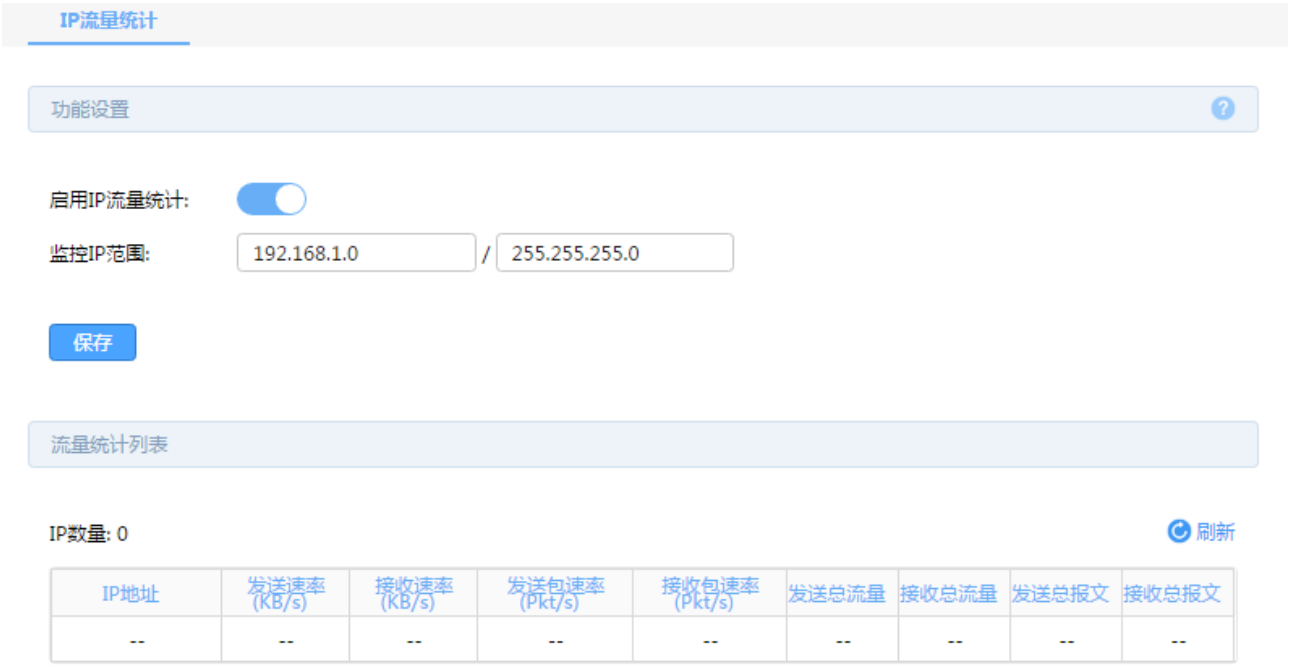


图 4-92 IP流量统计界面

界面项说明：

➢ **功能设置**

启用IP流量统计	启用或关闭 IP 流量统计功能。
监控IP范围	监控 IP 范围内的流量统计信息将会显示在本页的列表当中。

➢ **流量统计列表**

IP地址	显示进行IP流量统计的IP地址。
发送速率	接口发送数据帧速率，单位为KB/s。
接收速率	接口接收数据帧速率，单位为KB/s。
发送包速率	接口单位时间发送数据包个数，单位为Pkt/S。
接收包速率	接口单位时间接收数据包个数，单位为Pkt/S。
发送总流量	接口发送总流量。
接收总流量	接口接收总流量。
发送总报文	接口发送总报文数。
接收总报文	接口接收到的总报文数。

说明：

在流量统计列表中，可以按照不同的表头对流量统计列表进行排序，方法是点击列表中带下划线的表头文字。例如点击IP地址，默认排序方式为按IP地址排序从小到大，再点击一次IP地址，排序方式将变为按IP地址排序从大到小。

4.8.8 端口监控

您可以通过本页面设置端口监控。

界面进入方法：高级功能 >> 端口监控

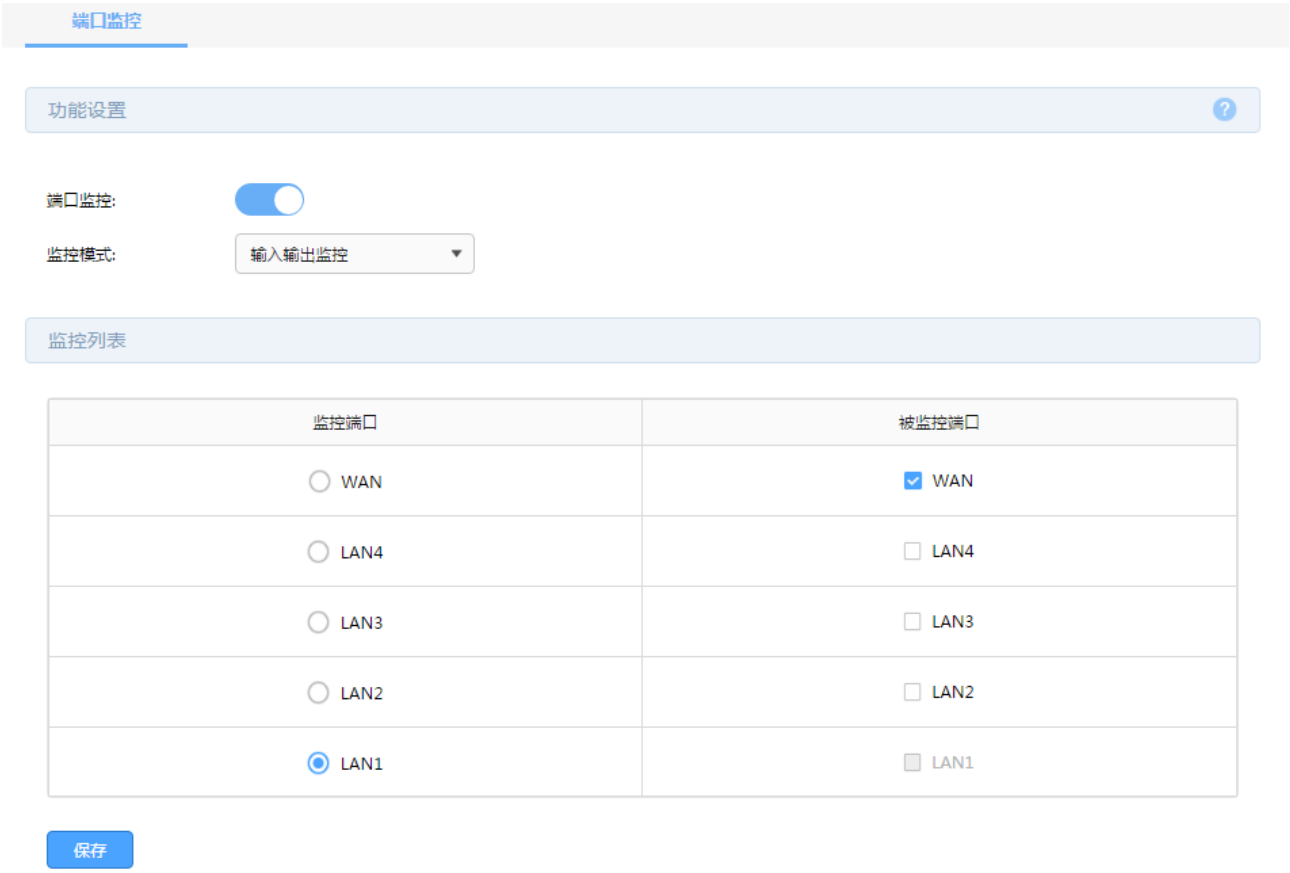


图 4-93 端口监控设置界面

界面项说明：

- **功能设置**

端口监控	滑块为灰色表示禁用，滑块为蓝色表示启用。
监控模式	端口监控有下面三种监控模式： 输出输入监控：流入流出被监控端口的数据帧将被复制到监控端口。 输入监控：流入被监控端口的数据帧将被复制到监控端口。 输出监控：流出被监控端口的数据帧将被复制到监控端口。

- **监控列表**

监控端口	被监控端口的数据帧将被复制到该端口。
被监控端口	经过该端口的数据帧将被复制到监控端口。

注意：

一个端口不能同时作为监控端口和被监控端口。

只能设置一个监控端口。

4.8.9 Port VLAN

您可以通过本页面对 Port VLAN 进行设置。

界面进入方法：高级功能 >> Port VLAN>> Port VLAN

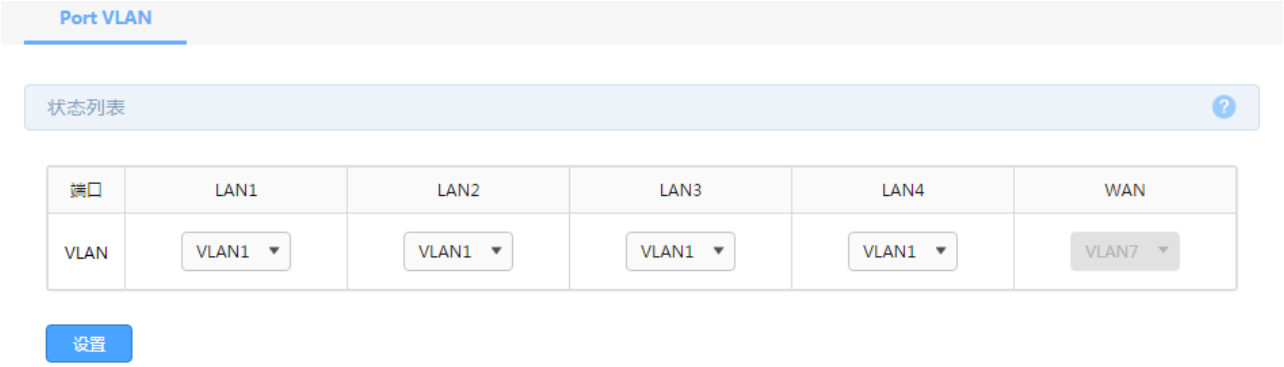


图 4-94 Port VLAN配置界面

界面项说明：

- **版本信息**

  显示当前路由器软件版本。

4.9 系统工具

4.9.1 设备管理

4.9.1.1 恢复出厂配置

界面进入方法：系统工具 >> 设备管理 >> 恢复出厂配置

图 4-95 恢复出厂配置界面

点击<恢复出厂配置>按钮，路由器将会恢复所有设置的默认值。建议在网络配置错误、组网环境变更等情况时使用此功能。

路由器出厂默认LAN口IP地址为192.168.1.1，首次登录用户名与密码需重新设置。

4.9.1.2 备份与导入配置

界面进入方法：系统工具 >> 设备管理 >> 备份与导入配置

图 4-96 备份与导入配置界面

界面项说明：

- **版本信息**

  显示当前路由器软件版本。

- **备份配置信息**

  单击<备份>按钮，路由器会将目前所有已保存配置导出为文件。建议在修改配置或升级软件前备份当前的配置信息。

- **导入配置信息**

  单击<浏览>按钮，选择已备份的配置文件；或者在文件路径输入框中填写完整的配置文件路径，然后点击<导入>按钮，将路由器恢复到以前备份的配置状态。

说明：

- 备份及导入文件过程中请保持电源稳定，避免强行断电。
- 导入的配置文件版本与路由器当前配置版本差距过大，将有可能导致路由器现有配置信息丢失，如果有重要的配置信息，请谨慎操作。

4.9.1.3 重启路由器

界面进入方法：系统工具 >> 设备管理 >> 重启路由器

图 4-97 重启路由器界面

单击<重启路由器>按钮，路由器将会重新启动。

重新启动不会丢失已保存的配置，在重启的过程中，网络连接将会暂时中断。

注意：

路由器重启过程中请保证电源稳定，避免强行断电。

4.9.1.4 软件升级

界面进入方法：系统工具 >> 设备管理 >> 软件升级

图 4-98 软件升级界面

➢ **路由器软件升级**

TP-LINK官方网站（http://www.tp-link.com.cn）会不定期更新TL-R473P-AC的软件升级文件，可将升级文件下载保存在本地。登录路由器后进入软件升级界面，单击<浏览>按钮，选择保存路径下的升级文件，点击<升级>进行软件升级。

注意：

- 软件升级成功后将会自动重启，在软件升级过程中以及重启完成前，请保证电源稳定，避免强行断电。
- 软件升级后由于新旧版本软件的差异可能会导致设备恢复出厂默认配置，丢失当前配置，如有重要配置信息，请在升级前备份。

4.9.1.5 自动清理

您可以通过本页面来设置自动恢复/自动清理功能。

界面进入方法：系统工具 >> 设备管理 >> 自动清理

图 4-99 自动清理界面

界面项说明：

➢ **自动恢复**

自动恢复功能 开启该功能后，当路由器发生硬件或者软件异常时，系统可检测并自动

恢复正常。滑动开关后设置生效。

➢ **自动清理**

自动清理功能	开启自动清理功能后，路由器将会在设定的时间自动清理。滑动开关后需要保存设置方可生效。
星期	用户指定每周周几进行自动清理。
时间	用户指定对应每周周几进行清理时间。

注意：

- 在自动恢复和自动清理的过程中，路由器将会进行短暂重启。请根据需要设定本功能的时间。
- 自动清理功能仅在本设备获取到网络时间或者手动设置时间后生效。

4.9.2 诊断工具

4.9.2.1 诊断工具

可在诊断工具界面通过PING通信检测或路由跟踪检测诊断当前路由器的网络连接状态。

界面进入方法：系统工具 >> 诊断工具 >> 诊断工具

图 4-100 诊断工具设置界面

界面项说明：

- **诊断工具**

诊断工具类型	用于诊断网络状况的方式。有下面两种： PING 通信检测，用于检测到达网络中的某节点是否连通。 路由跟踪检测，用于检测到达联络中的某节点经过节点的个数以及节点地址。

（1） 诊断工具选择“PING 通信检测”时，需填写下述内容：

目的IP/域名	需要进行 Ping 通信检测或者路由跟踪检测的主机地址，支持 IP 地址和域名。
出接口	需要进行 Ping 通信检测或者路由跟踪检测的接口。
PING次数	设置 Ping 通信检测时发送 Ping 包的数量。
PING数据包大小	设置 Ping 通信检测时发送的 Ping 包的大小。

（2） 诊断工具选择“路由跟踪检测”时，需填写下述内容：

图 4-101 路由跟踪检测界面

目的IP/域名	需要进行 Ping 通信检测或者路由跟踪检测的主机地址，支持 IP 地址和域名。
出接口	需要进行 Ping 通信检测或者路由跟踪检测的接口。
路由跟踪最大TTL	设置路由跟踪检测发送数据包在网络中的最大转发跳数。

4.9.2.2 故障诊断

您可以通过本页面来打开/关闭故障诊断模式。

界面进入方法：系统工具 >> 诊断工具 >> 故障诊断

图 4-102 故障诊断设置界面

界面项说明：

- **诊断工具**

开启诊断模式	点击滑动开关来进行操作，蓝色表示开启诊断模式，灰色表示诊断模式关闭。开启本功能后可以配合技术支持人员对设备进行诊断。
导出诊断信息	点击按钮下载基本的诊断信息，将其提供给技术人员以协助您分析和解决问题。

注意：

一般情况下请不要随意开启本功能。

需要诊断时，请先联系技术支持人员，在其协助下打开并使用本功能。

4.9.3 时间设置

时间设置界面允许对路由器的系统时间进行设置。若时间设置发生改变，将会影响一些与其相关的功能，如防火墙规则的生效时间、PPPoE定时拨号、日志等。

界面进入方法：系统工具 >> 时间设置 >> 时间设置

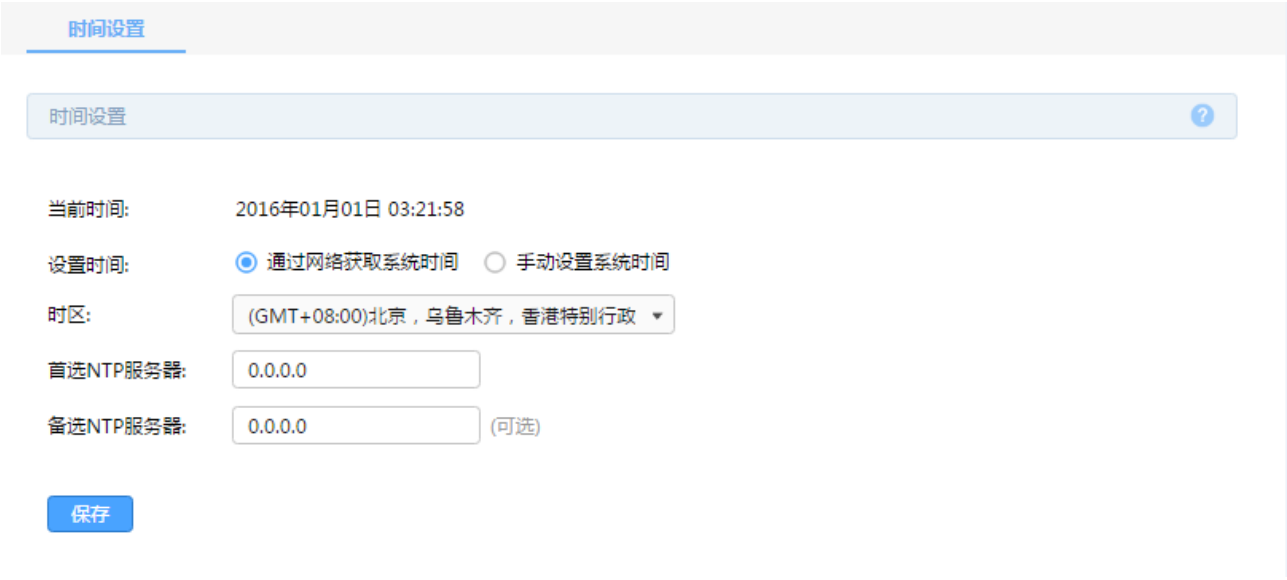


图 4-103 时间设置-通过网络获取系统时间

图 4-104 时间设置-手动设置系统时间

界面项说明：

➢ **时间设置**

当前时间 此处将显示目前系统时间。

设置时间 选择设置时间的方式，可选择通过网络获取系统时间或者手动设置系统时间。通过网络获取系统时间：若路由器可以访问互联网，可选择此项进行网络校时。选择时区后点击<设置>按钮，路由器将在内置NTP（Network Time Protocol，网络校时协议）服务器地址列表中搜索可用地址，并获取时间。若获取失败，请手动设置NTP服务器地址，由于NTP服务器并非固定不变，推荐搜索两个不同的地址，

分别填入首选、备用NTP服务器输入框，NTP服务器地址可以为IP地址也可以为域名。设置完毕后点击<设置>按钮，路由器会通过指定的NTP服务器获取网络时间。手动设置系统时间：若路由器暂时不能访问互联网，可以选择对系统时间进行手动设置，或者点击<获取管理主机时间>按钮，系统将自动填入当前管理主机时间信息。设置完毕后点击<设置>生效。

说明

- 如果不能正常使用<获取管理主机时间>功能，请在主机的防火墙软件中增加一条 UDP 端口为 123 的例外条目。
- 断电重启后，断电之前设置的时间将失效，重新变为“通过网络获取时间”，如果未能连网获取时间，将从系统默认时间开始计时。

4.9.4 系统日志

可以在日志界面查看路由器系统事件的记录信息。

界面进入方法：系统工具 >> 系统日志 >> 系统日志

图 4-105 系统日志界面

日志设置区可以对日志系统进行简单的配置。

界面项说明：

- **日志设置**

自动刷新	启用自动刷新，页面将每隔 10 秒自动刷新一次。
日志等级	所有等级：查看所有等级的日志信息。 致命错误：导致系统不可用的错误。 紧急错误：必须对其采取紧急措施的错误。 严重错误：导致系统处于危险状态的错误。 一般错误：一般性的错误提示。 警告信息：系统仍然正常运行，但可能存在隐患的提示信息。 通知信息：正常状态下的重要提示信息。 信息报告：一般性的提示信息。 调试信息：调试过程中产生的信息。

- **日志列表**

日志内容	每一项日志内容组成格式为“时间+功能模块+日志等级+日志信息”。
刷新	手动刷新日志内容。
全部删除	点击<全部删除>将删除路由器中保存的所有日志。
导出日志	点击<导出日志>按钮，路由器将以文件形式保存当前路由器中所有的日志内容。

4.9.5 系统管理

4.9.5.1 远程管理

您可以通过本页面设置进行远程管理的 IP 地址。

界面进入方法：系统工具>> 系统管理 >> 远程管理

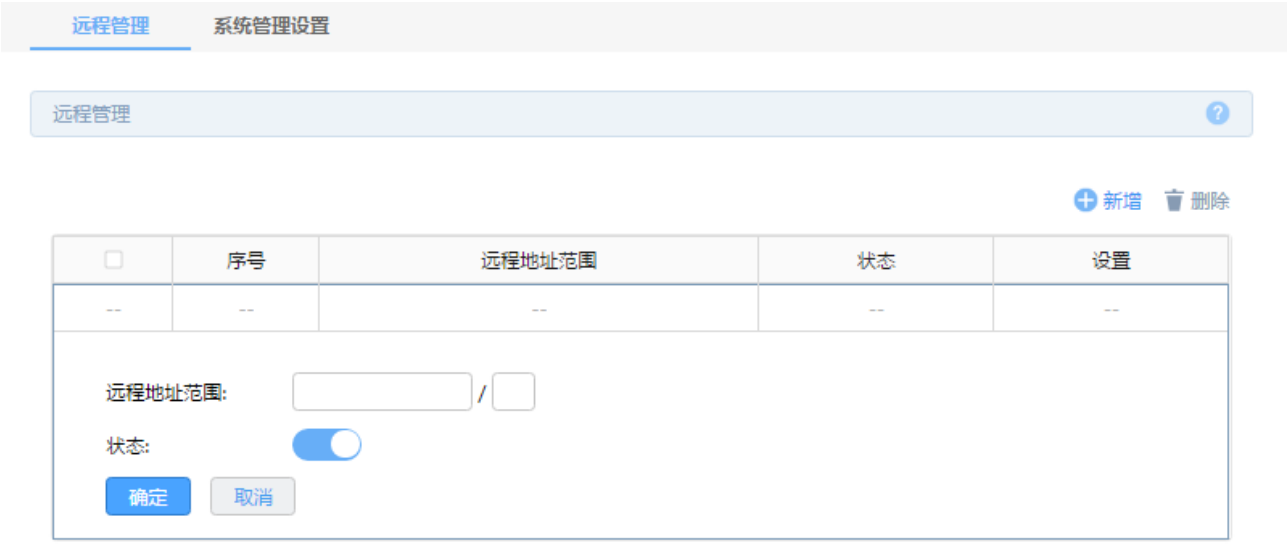


图 4-106 远程管理设置界面

界面项说明：

- **日志设置**

远程地址范围	远程管理主机的地址范围。
状态	您可以通过勾选改项来设置是否规则对应的地址范围内的主机进行远程管理。

如果您想让地址段为 102.31.70.0/24 的主机（非 LAN 口网段）对路由器进行远程管理，您可以建立远程管理地址条目，点击<新增>，设置远程地址范围 102.31.70.0/24，状态勾选设置为启用即可。

注意：

包含局域网地址的远程管理地址条目无效（局域网地址包括LAN口合法地址）。

如果添加0.0.0.0/0的条目，将允许所有远程计算机访问路由器，有可能在非法攻击情况下无法访问路由器。

4.9.5.2 系统管理设置

您可以通过本页面进行服务端口和会话超时时间的管理。

界面进入方法：系统工具>> 系统管理 >> 系统管理设置

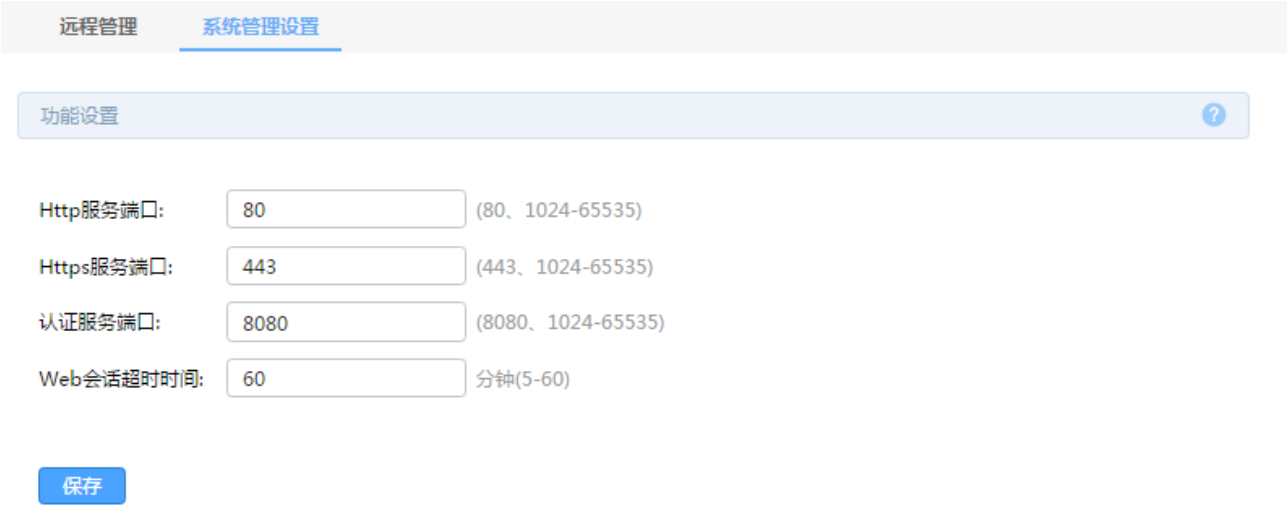


图 4-107 系统管理设置界面

界面项说明：

- **功能设置**

Http服务端口	用于 Web 管理界面的服务端口，默认为 80 端口。不能与其他的服务端口重复。
Https服务端口	用于 Web 管理界面的 Https 服务端口，默认为 443 端口。不能与其他的服务端口重复。
认证服务端口	用于认证服务的端口，默认为 8080 端口。不能与其他的服务端口重复。
Web会话超时时间	如果在会话超时时间内都没有进行操作，系统将自动退出登录，以保证设备和网络的安全。

附录 A 常见问题

问题1：无法登录路由器Web管理界面该如何处理？

1. 如果第一次使用此路由器，请参考以下步骤：
   1) 确认网线已正常连接到了路由器的LAN口，对应的指示灯闪烁或者常亮。
   2) 访问设置界面前，建议将计算机设置成“自动获取IP地址”，由开启DHCP服务的路由器自动给计算机分配IP地址。如果需要给计算机指定静态IP地址，请将计算机的IP与路由器LAN口IP设置在一网段，路由器默认LAN口IP地址为：192.168.1.1，子网掩码：255.255.255.0，计算机的IP地址应设置为：192.168.1.X （X为2至254之间任意整数），子网掩码为：255.255.255.0。
   3) 使用ping命令检测计算机与路由器之间的连通性。
   4) 若上述提示仍不能登录到路由器管理界面，请将路由器恢复为出厂配置。
2. 如果修改过路由器的管理端口，则注意下次登录时需要以“http://管理IP:XX”的方式登录，XX为修改后的端口号，如**http://192.168.1.1:8080**。
3. 如果之前可以正常登录，现在不能登录，则有可能是他人修改了路由器的配置导致的（尤其在开启了远程Web管理的情况下），建议恢复出厂配置，修改路由器的管理端口、修改用户名和密码，做好保密措施。
4. 如果恢复出厂配置后仍然无法登录或开始一段时间能登录，但过一段时间后又不能登录，则可能是遭受了ARP欺骗，建议查找欺骗源、查杀病毒或将其隔离。
5. 请检查是否设置了IE代理，如果设置了IE代理，请先将代理取消。

问题2：忘记路由器用户名和密码怎么办？如何恢复出厂配置？

忘记用户名密码时可以将路由器通过Reset键恢复至出厂配置。需要注意的是：恢复出厂配置时路由器原有配置信息将丢失。

恢复出厂配置操作方法：通电状态下，长按Reset键，待系统指示灯闪烁5次后松开Reset键，路由器将自动恢复出厂设置并重启。恢复出厂设置后，默认管理地址是http://192.168.1.1，用户首次登陆需自定义用户名和密码。

问题3：忘记路由器管理端口怎么办？

出于对路由器管理安全的考虑，如在不知道路由器管理IP或者端口的情况下，需要对路由器进行管理，建议将路由器恢复出厂配置。

问题4：为什么开启了远端管理后，非局域网段不能登录管理路由器？

1. 请检查非局域网段要登录路由器的IP地址是否被允许远端访问路由器。
2. 路由器的管理端口是否已经修改过，如果修改过，则应以“http://WAN口IP:XX”的方式登录，XX为修改后的管理端口，如**http://202.160.58.67:8080**。

3. 路由器的管理端口是否已经在虚拟服务器中被映射为局域网主机的某个服务端口，如果已经被映射为主机的服务端口，则应更改主机服务的端口或更改路由器的管理端口为其它端口。

4. 路由器虚拟服务器的NAT DMZ服务是否启用，如需远程管理路由器，请禁用NAT DMZ服务。

问题5：路由器某些功能设置需要填写子网掩码值划分地址范围，一般子网掩码都有哪些值？

子网掩码是一个32位的二进制地址，以此来区别网络地址和主机地址。子网划分时，子网掩码不同，所得到的子网不同，每个子网能容纳的主机数目不同。

常用的子网掩码值有**8**（即A类网络的缺省子网掩码255.0.0.0）、**16**（即B类网络的缺省子网掩码255.255.0.0）、**24**（即C类网络的缺省子网掩码255.255.255.0）、**32**（即单个IP地址的缺省子网掩码255.255.255.255）。

附录 B 术语表

	英文术语	中文名称	定义或描述
A	ADSL（Asymmetrical Digital Subscriber Line）	非对称数字用户线路	非对称数字用户线路，是一种宽带接入技术，是目前应用最广的宽带接入方式。它利用双绞铜线向用户提供两个方向上速率不对称的宽带信息业务。
	AES（Advanced Encryption Standard）	高级加密标准	美国国家标准与技术研究所用于加密电子数据的规范。
	ALG（Application Layer Gateway）	应用层网关	工作在应用层的网关，通过处理应用层的数据使穿透网关进行的网络应用能够正常工作。
	AP（Access Point）	访问接入点	相当于一个连接有线网和无线网的桥梁，其主要作用是将各个无线网络客户端连接到一起，然后将无线网络接入以太网。
	ARP（Address Resolution Protocol）	地址解析协议	一种把IP地址转换成物理地址的协议。
	AH（Authentication Header）	认证头协议	用于保证数据的完整性。
B	BSSID（Basic Service Set Identity）	基础服务集标识	AP的MAC地址。
D	DDNS（Dynamic Domain Name Server）	动态域名解析服务器	实现将固定域名解析为动态变化的IP地址的域名解析服务器。
	DHCP（Dynamic Host Configuration Protocol）	动态主机配置协议	为网络中的主机动态分配IP地址、子网掩码、网关、DNS等信息。
	DMZ（Demilitarized Zone）	非军事区	路由器对此区域主机不进行保护，广域网主机可主动访问这些主机。
	DNS（Domain Name Server）	域名解析服务器	实现将域名解析为IP地址的域名解析服务器。
	DTIM（Delivery Traffic Indication Message）	传输指示消息	一种倒数计时作业，用以告知下一个要接收广播及多播的客户端窗口。
E	ESP（Encapsulating Security Payload）	封装安全性载荷	用于数据完整性检查以及数据加密。
F	Flood	洪泛	是攻击程序大量快速模仿某种连接请求，导致CPU繁忙或网络瘫痪。

	英文术语	中文名称	定义或描述
F	FTP（File Transfer Protocol）	文件传输协议	在基于TCP/IP网络和互联网的联网计算机之间传送文件的标准协议。
G	GMT（Greenwich Mean Time）	格林威治标准时间	以经过格林威治的本初子午线为标准的国际统一时间。
	GARP（gratuitous ARP）	免费地址解析协议	主机通过GARP向广播域发送不期望回复的ARP包以广播自己的IP对应的MAC地址，或者检测以太网内是否有IP冲突。
H	H.323	-	H.323为现有的分组网络PBN（如IP网络）提供多媒体通信标准。它规定了不同的音频、视频或数据终端协同工作所需的操作模式。
	HTTP（Hypertext Transfer Protocol）	超文本传输协议	常用于WWW服务器与客户端之间传输文件。
I	ICMP（Internet Control Messages Protocol）	网间控制报文协议	ICMP传递差错报文以及其他需要注意的信息。ICMP报文通常被IP层或更高层协议（TCP或UDP）使用。
	Internet	因特网/国际互联网/网际网	是使用公用语言互相通信的，许多路由器和公共互联网连接而成的全球网络。
	IP（Internet Protocol）	网际协议/互联网协议	IP是TCP/IP协议族中最为核心的协议。所有的TCP、UDP、ICMP及IGMP数据都以IP数据报格式传输。
	ISP（Internet Service Provider）	互联网服务提供商	提供因特网接入服务的提供商。
L	LAN（Local Area Network）	局域网/本地网	指将位于相对有限区域内的一组计算机、打印机和其他设备连接起来的通讯网络。LAN 内部连接的设备都能与其中的其他设备交互。
M	MAC address（Media Access Control address）	介质访问控制地址	MAC协议主要负责控制与连接物理层的物理介质，协议中定义的MAC地址是由厂商指定的用来标识网络节点的全球唯一的硬件地址。由6组编码组成，每组编码表示为2个16进制数。
	MTU（Maximum Transmission Unit）	最大传输单元	网络中传输数据包的最大长度。

	英文术语	中文名称	定义或描述
N	NAT（Network Address Translator）	网络地址转换	将局域网的IP地址转换成用于互联网的外部IP地址。
	NAT DMZ/pseudo DMZ（NAT Demilitarized Zone）	非军事区域/隔离区	是在NAT网关应用上的一种特殊服务。开启NAT DMZ服务后，网关会将所有外网发起的、不符合所有现有连接和转发规则的数据全部转发向已设置的NAT DMZ主机地址。
	NTP Server	网络时间服务器	用于互联网上的计算机时间同步。
P	PPPoE（Point-to-Point Protocol over Ethernet）	点对点以太网承载协议	点对点以太网承载协议在以太网上承载 PPP 协议封装的报文，它是目前使用较多的业务形式。
	Private	私有的	用于表示网络是局域网（私有网络）。
	Public	共有的，公共的	用于表示网络是广域网（公有网络）。
	Short GI（Short Guard Interval）	短保护间隔	是802.11n针对802.11a/g所做的改进，11a/g的GI时长为800us，而Short GI时长为400us，在使用Short GI的情况下，可提高10%的速率。
	SMTP（Simple Mail Transfer Protocol）	简单邮件传输协议	用于电子邮件的传输。
S	SSID（Service Set Identifier）	服务集标识	无线局域网用于身份验证的登录名。
	STA（Station）	站	站在无线局域网中一般为客户端，可以是装有无线网卡的计算机，也可以是有WiFi模块的智能手机。站可以是移动的，也可以是固定的，是无线局域网的最基本组成单元。
	TCP-ACK（ACKnowledgment）	确认	TCP首部中的确认标志。
	TCP-FIN（Finish）	结束	TCP首部中的结束标志。
T	TCP-SYN（SYNchronous）	同步	TCP首部中的同步序号标志。
	TCP（Transfer Control Protocol）	传输控制协议	传输控制协议是一种面向连接的、可靠的传输层协议。
	TCP/IP（Transmission Control Protocol/ Internet Protocol）	传输控制协议和互连网协议	用于网络的一组通讯协议，IP提供无连接的数据报传输机制，TCP提供一种面向连接的、可靠的字节流服务。
	Telnet（Telecommunication	远程终端协议	是在TCP/IP网络上，标准的提供远程登录功能

	英文术语	中文名称	定义或描述
	Network protocol）		的应用。
T	TKIP（Temporal Key Integrity Protocol）	暂时密钥集成协议	负责处理无线安全问题的加密部分。
	UDP（User Datagram Protocol）	用户数据报协议	面向无连接的、不可靠的传输层协议。
	UPnP（Universal Plug and Play）	通用即插即用	通用即插即用是一种用于PC机和智能设备（或仪器）的常见对等网络连接的体系结构。
	URL（Uniform Resource Locator）	统一资源定位符	互联网上的资源地址。
U	VLAN（Virtual Local Area Network）	虚拟局域网	组成局域网的逻辑子组。一个VLAN是一个按功能、组、或者应用被逻辑分段的交换网络，并不考虑使用者的物理位置。一个端口上接受到的包被发往属于同一个VLAN的接收端口，不同VLAN的网络设备无法通讯。
	WAN（Wide Area Network）	广域网	在很宽的地理区域内为用户服务的数据通信网络，此网络通常使用由公共设备商提供的传输设备。
	WDS（Wireless Distribution System）	无线分布式系统	是可以让无线AP或者无线路由器之间通过无线进行桥接（中继），而在中继的过程中并不影响其无线设备覆盖效果的功能。
V	WLAN（Wireless Local Area Network）	无线局域网	WLAN是以无线方式构成的局域网，主要由站、接入点、无线介质和分布式系统组成。
W	WMM（Wi-Fi MultiMedia）	无线多媒体	是802.11e标准的一个子集。WMM允许无线通信根据数据类型定义一个优先级范围。

附录 C 规格参数

产品型号		TL-R473P-AC	TL-R479P-AC	TL-R473GP-AC	TL-R479GP-AC	TL-R479GPE-AC
端口	WAN 端口	1FE	1FE	1GE	1GE	1GE
	LAN 端口	4FE（支持 PoE）	8FE（支持 PoE）	4GE（支持 PoE）	8GE（支持 PoE）	8GE（支持 PoE）
指示灯	每端口	Link/Act				
	每设备	SYS				
PoE 性能	符合标准	IEEE 802.3af/at				
	单端口最大 PoE 输出功率	30W				
使用环境		工作温度：0℃～40℃ ；存储温度：-40℃～70℃				
		工作湿度：10%～90%RH 不凝结；存储湿度：5%～90%RH 不凝结				
输入电源		220V～，50/60Hz				220V～，50Hz
散热方式		无风扇设计，自然散热				
尺寸（LxWxH）		226x131x35(mm)				250x158x44(mm)
典型带机量		1~30 台		30~50 台		30~50 台