TP-LINK®

千兆企业VPN路由器

TL-R483G/TL-R478G+/TL-R4239G

用户手册

REV1.0.0

1910040710

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。内容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

TP-LINK多WAN口千兆企业VPN路由器产品，采用基于高性能网络专用处理器的硬件平台，处理性能优异，同时支持IPSec/PPTP/L2TP VPN、上网行为管理、防火墙、智能IP带宽控制、多WAN口负载均衡、接入认证等丰富的软件功能，适合中小型企业、网吧、社区、酒店等网络环境。

千兆企业VPN路由器系列包含产品型号如下：

产品机型	产品名称
TL-R483G	多WAN口千兆企业VPN路由器
TL-R478G+	多WAN口千兆企业VPN路由器
TL-R4239G	多WAN口千兆企业VPN路由器

2.2 产品特性

硬件特性

- 采用高性能网络专用处理器，数据处理能力强劲；
- 配备容量为1Gbit的DDRⅡSDRAM高速内存；
- 内置高品质开关电源，无风扇静音设计；
- 提供1个固定WAN口和1个固定LAN口，3个WAN/LAN可变口，所有端口均支持10/100/1000Mbps自适应和端口自动翻转（Auto MDI/MDIX）；

丰富的功能特性

多WAN口

- 提供1个固定WAN口，3个WAN/LAN 可变口，满足企业多线接入的组网需求；
- 支持多线路负载均衡，通过采用智能均衡、特殊应用程序选路、ISP选路等多种均衡策略，充分利用WAN口带宽，保护用户投资；
- 支持WAN口备份功能，提供故障备份和时间备份两种备份模式，可在主线路中断后迅速将流量切换至备份线路，保障网络正常运行。

认证管理

- 支持Web认证、微信连Wi-Fi等多种认证方式，有效管控内网用户的上网权限；
- 可通过认证页面推送广告信息，帮助商家开展广告营销；
- 微信认证可帮助商家微信公众号轻松吸粉，提升公众号营销效果；
- 支持上网时长设置，灵活控制用户认证周期

上网行为管理

- **应用限制**：支持针对聊天类、P2P类、金融类、游戏类、代理类及基础类等数十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；同时支持基于用户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过滤规则，可对员工访问各种网站的权限进行管控，除了可以禁止/允许员工访问各种网站外，还可以记录其访问历史信息，甚至可以弹出警告页面。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**：支持禁止网页提交，可限制员工登录各种基于网页的论坛、网站、邮箱等发表信息，避免企业敏感数据外泄；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。

防火墙

- **访问策略**：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。
- **ARP防护**：支持IP与MAC地址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。
- **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DoS攻击、扫描类攻击、可疑包攻击行为，如：TCP Syn Flood、UDP Flood、ICMP Flood、WinNuke攻击、分片报文攻击、WAN口ping、TCP Scan（Stealth FIN/Xmas/Null）、IP欺骗等。

带宽控制

- 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。

VPN

- 提供标准的IPSec VPN功能，支持数据完整性校验、防数据包重放和数据加密功能（DES、3DES、AES128、AES192、AES256等加密算法），支持IKE和手动模式建立VPN隧道，并支持通过域名方式配置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。

PPPoE服务器

- PPPoE服务器可为内网用户分配上网账号，只允许使用合法账号并通过认证的用户通过设备认证，有效控制内网用户的上网权限，同时支持空闲断线、到期断线、地址绑定、例外IP等丰富的功能特性，管理更灵活。

端口监控

- 内置简单管理交换机，支持端口带宽控制和端口镜像等功能，满足公安部门的数据监控需求。

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

- 提供系统日志与日志服务器功能，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。

2.3 产品外观

2.3.1 TL-R483G

TL-R483G前后面板如下图所示：

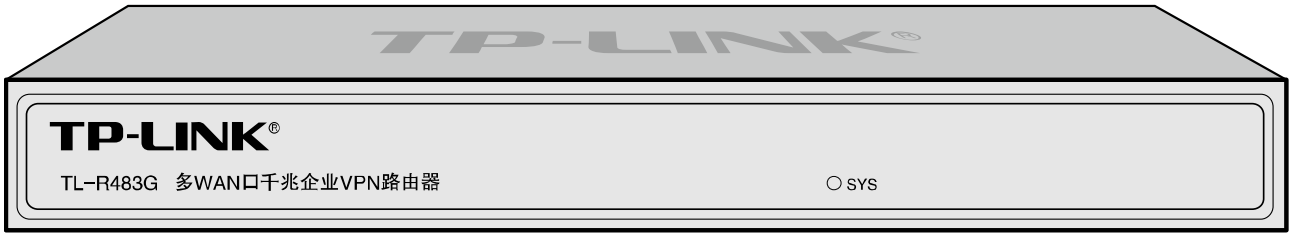


图 2-1 TL-R483G前面板示意图

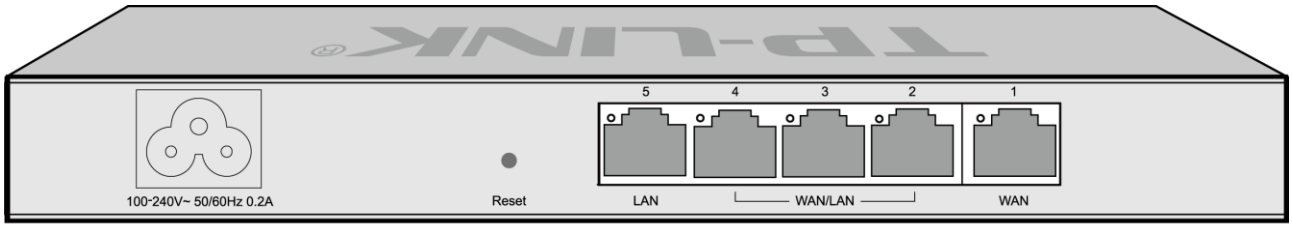


图 2-2 TL-R483G后面板示意图

指示灯

指示灯	名称	状态描述
SYS	系统指示灯	闪烁表示系统工作正常
		常亮或不亮表示系统工作异常
Link/Act	状态指示灯	常亮绿色表示链路建立
		闪烁表示端口正在收发数据
		不亮表示链路未建立

接口说明

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

Reset键

如果需要将路由器恢复到出厂默认设置，请在路由器通电的情况下，使用尖状物按住Reset键，待系统指示灯快速闪烁5次后松开按键，路由器将自动恢复出厂设置并重启。恢复出厂设置后，默认管理地址为http://192.168.1.1，用户在首次登陆时需自定义用户名和密码。

电源接口

这是一个三相电源接口，把电源线阴性插头接到这个接口上，阳性插头接到交流电源上。

注意：

- 请使用原装电源线。
- 电源插座请安装在设备附近便于触及的位置，以方便操作。

2.3.2 TL-R478G+

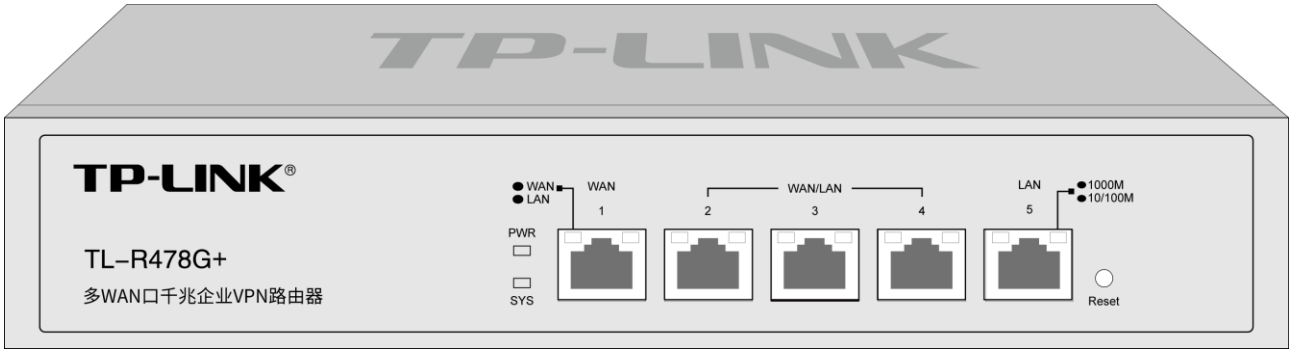


图 2-3 TL-R478G+前面板示意图

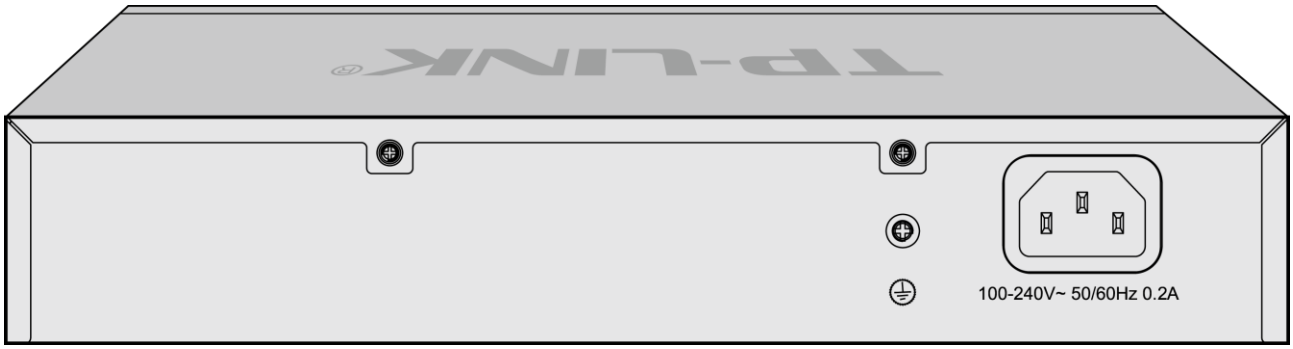


图 2-4 TL-R478G+后面板示意图

指示灯

指示灯	名称	状态描述
PWR	电源指示灯	常亮表示系统供电正常
		不亮表示电源关闭或电源故障
SYS	系统状态指示灯	闪烁表示系统正常
		常亮或不亮表示系统不正常
Speed/Link/Act	连接状态指示灯	闪烁表示端口正在传输数据
		不亮表示端口未建立连接
		常亮绿色表示端口速率为1000Mbps
		常亮黄色表示端口速率为100Mbps或10Mbps
WAN/LAN	接口状态指示灯	常亮表示相应端口类型为WAN口
		不亮表示相应端口类型为LAN口

接口说明

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

Reset键

如果需要将路由器恢复到出厂默认设置，请在路由器通电的情况下，使用尖状物按住Reset键，待系统指示灯快速闪烁5次后松开按键，路由器将自动恢复出厂设置并重启。恢复出厂设置后，默认管理地址为http://192.168.1.1，用户在首次登陆时需自定义用户名和密码。

电源接口

这是一个三相电源接口，把电源线阴性插头接到这个接口上，阳性插头接到交流电源上。

防雷接线柱

位于电源接口左侧，请使用导线接地，以防雷击。详细防雷措施请参见《设备防雷安装手册》。

注意：

- 请使用原装电源线。
- 电源插座请安装在设备附近便于触及的位置，以方便操作。

2.3.3 TL-R4239G

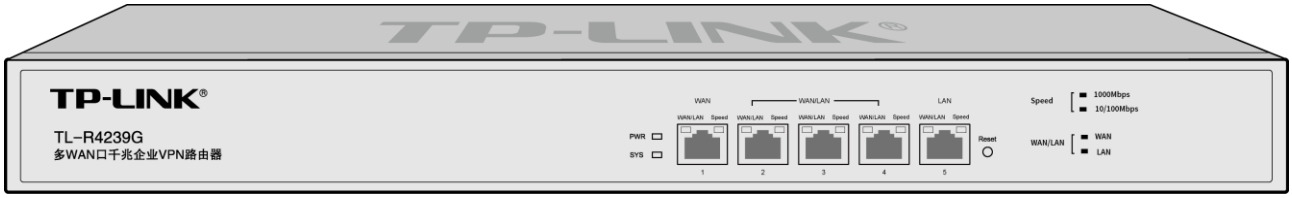


图 2-5 TL-R4239G前面板示意图

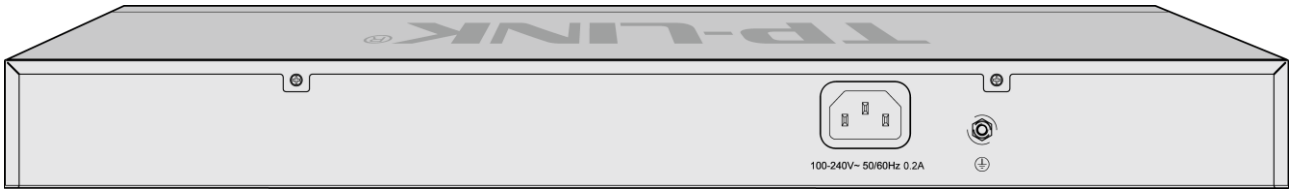


图 2-6 TL-R4239G后面板示意图

指示灯

指示灯	名称	状态描述
PWR	电源指示灯	常亮表示系统供电正常
		不亮表示电源关闭或电源故障
SYS	系统状态指示灯	闪烁表示系统正常
		常亮或不亮表示系统不正常
Speed/Link/Act	连接状态指示灯	常亮表示相应端口已正常连接
		闪烁表示相应端口正在传输数据
		不亮表示相应端口未建立连接
		常亮绿色表示端口速率为1000Mbps
		常亮黄色表示端口速率为100Mbps或10Mbps
WAN/LAN	接口状态指示灯	常亮表示相应端口类型为WAN口
		常灭表示相应端口类型为LAN口

接口说明

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

Reset键

如果需要将路由器恢复到出厂默认设置，请在路由器通电的情况下，使用尖状物按住Reset键，待系统指示灯快速闪烁5次后松开按键，路由器将自动恢复出厂设置并重启。恢复出厂设置后，默认管理地址为http://192.168.1.1，用户在首次登陆时需自定义用户名和密码。

电源接口

这是一个三相电源接口，把电源线阴性插头接到这个接口上，阳性插头接到交流电源上。

防雷接线柱

位于电源接口左侧，请使用导线接地，以防雷击。详细防雷措施请参见《设备防雷安装手册》。

注意：

- 请使用原装电源线。
- 电源插座请安装在设备附近便于触及的位置，以方便操作。

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：

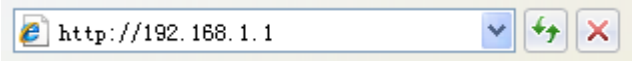
1) 路由器已正常加电启动，任一LAN口已与管理主机相连。

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。单击<下一步>，开始设置。

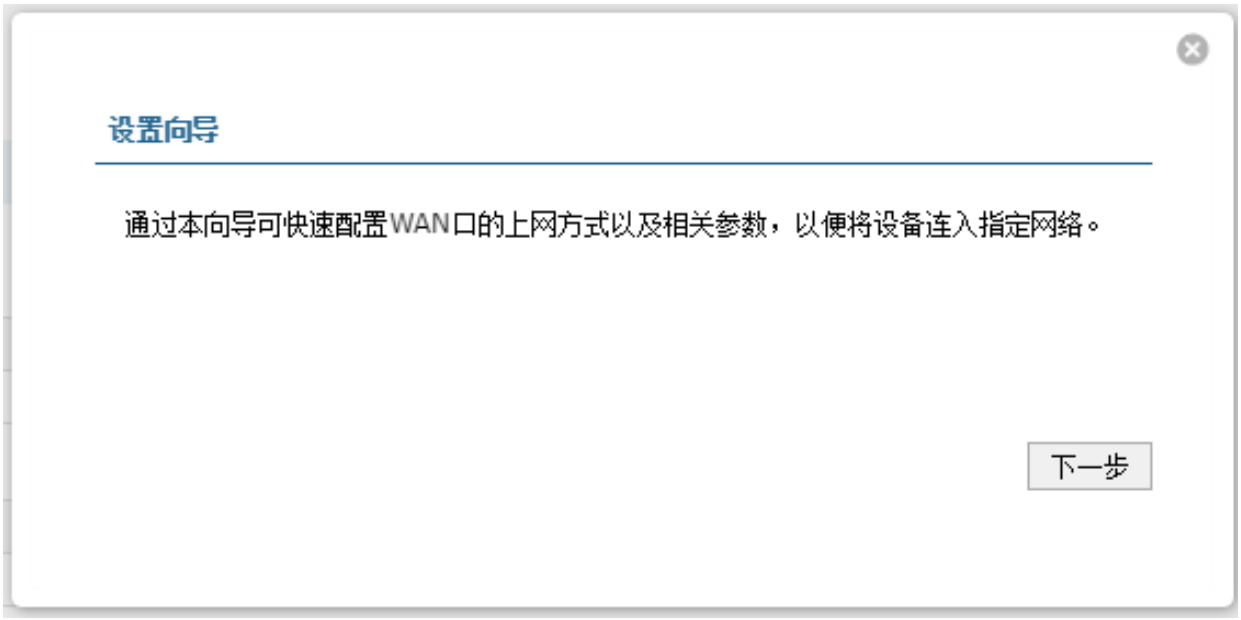


图3-2 设置向导

在图3-2所示界面，单击<下一步>，进入接口模式设置界面，选择WAN口数量，如图3-3所示。（这里以选择两个WAN口为例）

图3-3 接口模式设置

在图3-3的点击<下一步>，对WAN1口进行设置。如图3-4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3-4 WAN1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3-5 上网方式-PPPoE

账号 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“自动获取IP地址”，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“固定IP地址”，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3-6 上网方式-静态IP

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。

网关地址 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。

对WAN1口设置完成之后，点击<下一步>，进入WAN2口的设置界面，如图3-7所示。如需进行设置，则设置步骤与WAN1口的设置步骤完全一致，如无需进行设置，则可直接点击<跳过>。

图 3-7 WAN2 口设置

完成对所选WAN口的全部设置之后，进入图3-8所示页面，如有需要更改的配置项可点击上一步修改配置。

图 3-8 完成快速配置

在图3-8所示界面，单击<完成>，路由器会自动进行配置并重启，如图3-9所示。重启完成后，会跳到图3-1所示的登录界面，如需对路由器进行其他操作，重新登录即可。

图3-9 路由器自动配置并重启

3.2 Web 界面简介

千兆企业VPN路由器系列产品典型的Web界面如图 3-10所示。（以TL-R478G+）为例。

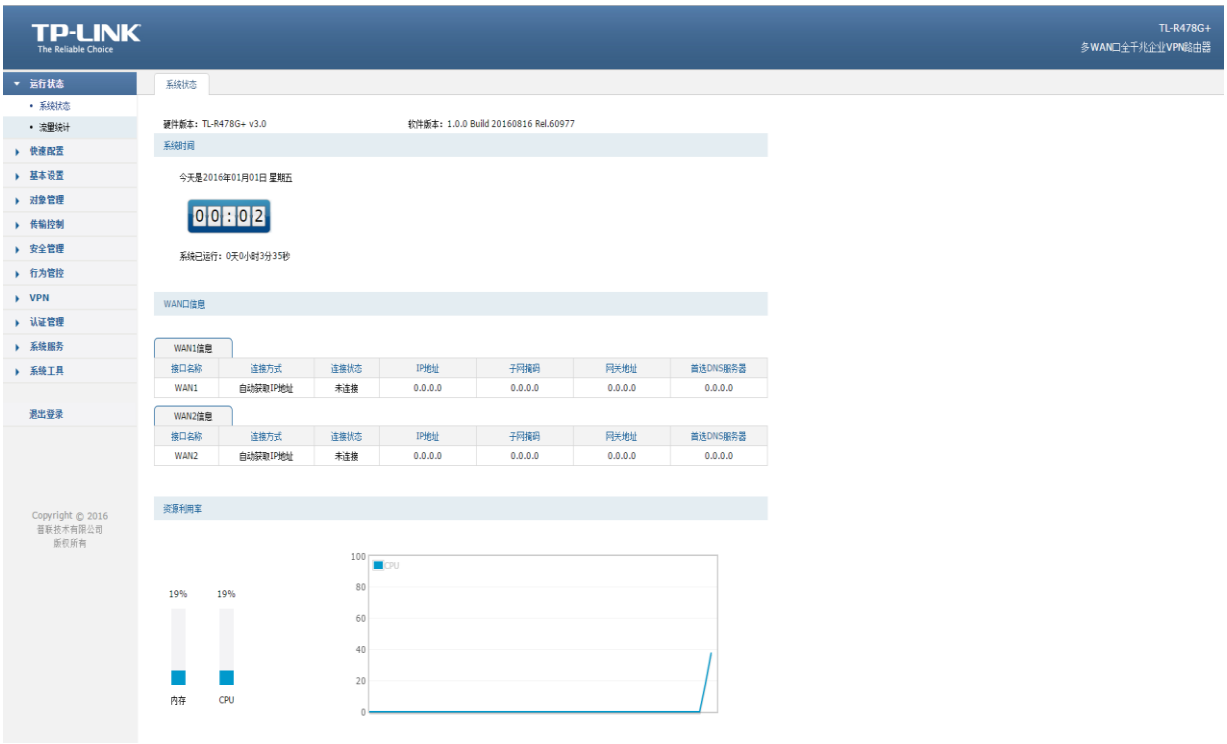


图 3-10 典型Web界面

在图 3-11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。

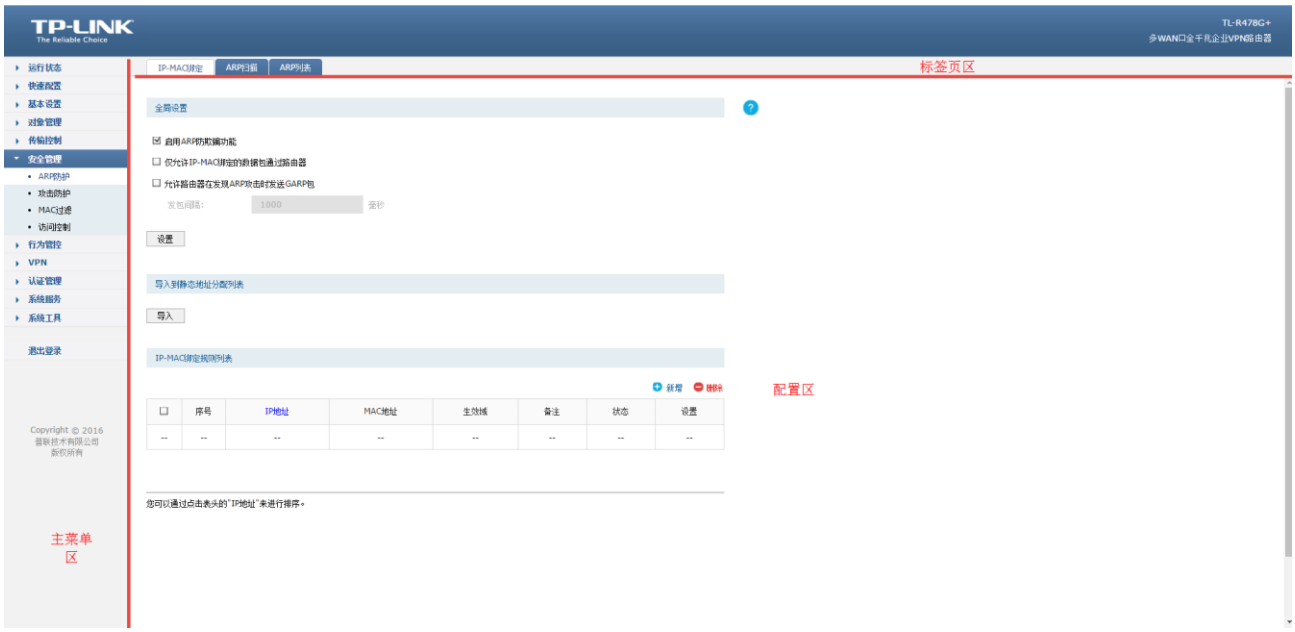


图 3-11 Web界面区域划分

第4章 功能设置

4.1 运行状态

4.1.1 系统状态

系统状态界面显示路由器当前硬件和软件版本信息、系统时间、各接口配置信息以及系统资源使用情况。

界面进入方法：运行状态 >> 系统状态 >> 系统状态

图 4-1 系统状态界面

4.1.2 流量统计

4.1.2.1 接口流量统计

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。

界面进入方法：运行状态 >> 流量统计 >> 接口流量统计

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Kbps。
接收速率	接口接收数据帧速率，单位为Kbps。
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。
发送总字节	接口发送总字节数，单位为Byte。
接收总字节	接口接收总字节数，单位为Byte。
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。

4.1.2.2 IP 流量统计

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的流量统计。

界面进入方法：运行状态 >> 流量统计 >> IP流量统计

图 4-3 IP流量统计界面

界面项说明：

- **功能设置**

  勾选“启用流量统计”，IP流量统计功能才会生效；

  监控IP范围：选择需要监控的IP地址的范围。

- **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Kbps。
接收速率	接口接收数据帧速率，单位为Kbps。
发送包速率	接口单位时间发送数据包个数，单位为Pkt/S。
接收包熟虑	接口单位时间接收数据包个数，单位为Pkt/S。
发送总字节	接口发送总字节数，单位为Byte。
接收总字节	接口接收总字节数，单位为Byte。
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。

4.2 快速配置

对路由器进行快速配置，详情请参考 3.1 快速安装指南

4.3 基本设置

4.3.1 接口模式

千兆企业 VPN 路由器系列产品提供了 1 个固定 WAN 口、1 个固定 LAN 口和 3 个 WAN/LAN 可变口，在此界面可以选择 WAN 口的数目（最多 4 个），如图 4-4 所示。选择 WAN 口数目之后，点击<设置>，如果 WAN 口数目有变化，则路由器会自动配置并重启。为防止配置丢失，请在切换接口模式前备份产品配置信息。

图 4-4 接口模式设置界面

4.3.2 WAN设置

4.3.2.1 WAN1设置

千兆企业VPN路由器系列产品提供三种方式接入广域网：固定IP地址、自动获取IP地址、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。

- 有线宽频一般使用自动获取IP地址连接方式；
- 光纤接入以及企业、网吧局域网内组网一般使用固定IP地址连接方式；

➢ 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 >> WAN1设置

1) 固定IP地址

若ISP提供了固定的IP地址，请选择“固定IP地址”手动配置WAN口参数。

图 4-5 WAN口设置界面-固定IP地址

界面项说明：

➢ **固定IP地址设置**

连接方式	选择固定IP地址连接方式，进行手动配置。
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	设置网关地址，允许留空。
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	MTU（Maximum Transmission Unit，最大传输单元），可以设置数据包的最大长度。取值范围是576-1500之间的整数，默认值为1500。若ISP未提供MTU值，请保持默认值不变。
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。

- **连接状态**

连接状态　　显示当前WAN口的连接状态。

IP地址　　显示路由器WAN口的IP地址。

子网掩码　　显示路由器WAN口的子网掩码。

网关地址　　显示网关地址。

首选DNS服务器　　显示DNS地址。

备用DNS服务器　　显示备用DNS地址。

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 4-6 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**

连接方式　　选择动态IP连接方式。

主机名	输入用于标识路由器的名称，允许留空。
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	MTU（Maximum Transmission Unit，最大传输单元），可以设置数据包的最大长度。取值范围是576-1500之间的整数，默认值为1500。若ISP未提供MTU值，请保持默认值不变。
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。

- **连接状态**

连接状态	显示当前WAN口DHCP分配状态。 “正在连接”表示当前路由器正在向ISP获取IP参数； “已连接”表示路由器已成功获取IP参数； “未连接”表示已手动释放连接，或路由器已发起请求，但未得到响应，请检查连接线路是否正常，若问题无法解决，请与ISP联系。
IP地址	显示自动获取到的IP地址。
子网掩码	显示自动获取到的子网掩码。
网关地址	显示自动获取到的网关地址。
首选DNS服务器	显示DNS地址。
备用DNS服务器	显示备用DNS地址。

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。

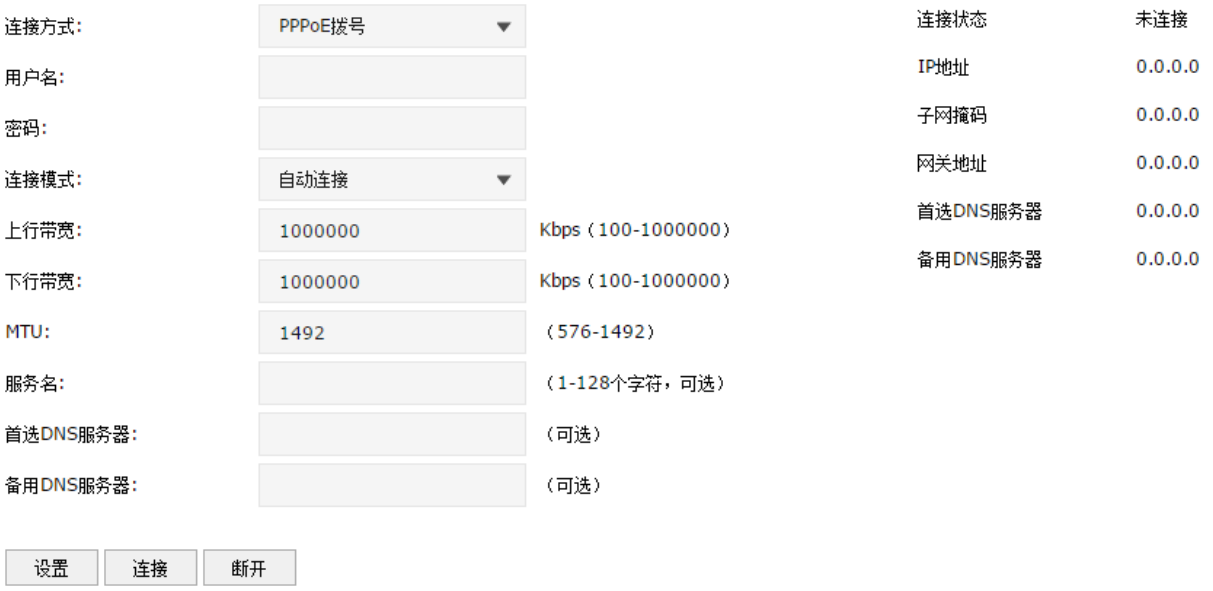


图 4-7 WAN口设置界面-PPPoE

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。
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	MTU（Maximum Transmission Unit，最大传输单元），可以设置数据包的最大长度。取值范围是576-1492之间的整数，默认值为1492。若

ISP未提供MTU值，请保持默认值不变。

服务名 输入服务名称，由ISP提供。

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。

- **连接状态**

连接状态 显示当前WAN口PPPoE拨号连接状态。

“物理未连接”表示接口物理链路未建立，请检查网线接口连接是否正确，网线是否完好；

“未启用”表示当前已选择PPPoE拨号连接方式但未保存生效；

“正在连接”表示当前路由器正在向ISP获取IP参数；

“已连接”表示路由器已成功获取IP参数；

“未连接”表示已手动断开连接，或路由器已发起请求，但未得到响应，请检查用户名密码是否正确、连接线路是否正常，若问题无法解决，请与ISP联系。

IP地址 显示通过PPPoE拨号后获取到的IP地址。

子网掩码 显示自动获取到的子网掩码。

网关地址 显示通过PPPoE拨号后获取到的网关地址。

首选DNS服务器 显示DNS地址。

备用DNS服务器 显示备用DNS地址。

4.3.2.2 WAN2设置

设置方式同WAN1口，详见**4.2.2.1 WAN1设置**。

4.3.3 LAN设置

4.3.3.1 LAN设置

在此设置路由器LAN口的IP参数。

界面进入方法：基本设置 >> LAN设置 >> LAN设置

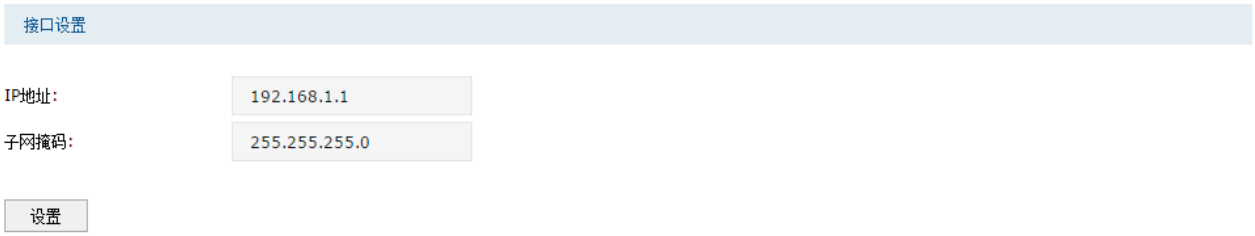


图 4-8 LAN口设置界面

界面项说明：

- **接口设置**

IP地址	设置路由器LAN口的IP地址，默认值为192.168.1.1，可根据实际网络情况修改此值。局域网内部可通过该地址访问路由器。
子网掩码	设置路由器LAN口的子网掩码，默认为255.255.255.0，可根据实际网络情况修改此值。

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。

4.3.3.2 DHCP服务

路由器具有DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）服务功能，能够为所有接入路由器并且应用DHCP服务的网络设备自动分配IP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**

开始地址	设置DHCP分配地址的开始地址
结束地址	设置DHCP分配地址的结束地址
地址租期	设置DHCP分配地址有效时间，超时将重新分配。
网关地址	设置DHCP分配给客户端的网关地址，建议填入当前DHCP服务生效接口的IP地址，允许留空。
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。
状态	选择开启或关闭DHCP服务。推荐选择<启用>，以使用DHCP自动配置TCP/IP参数功能。为了使用本路由器的DHCP服务器功能，局域网主机

的Internet协议必须设置为“自动获得IP地址”。

4.3.3.3 客户端列表

客户端列表显示已由DHCP分配IP参数的主机信息。

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

可通过客户端列表查询DHCP客户端信息。如要获得最新DHCP服务分配的客户端信息，请点击<刷新>按钮。

4.3.3.4 静态地址分配

可根据接入设备的MAC地址手动分配IP地址。当对应的客户端设备请求DHCP服务器分配IP地址时，DHCP服务器将自动为其分配指定的IP地址。

界面进入方法：基本设置 >> LAN设置 >> 静态地址分配

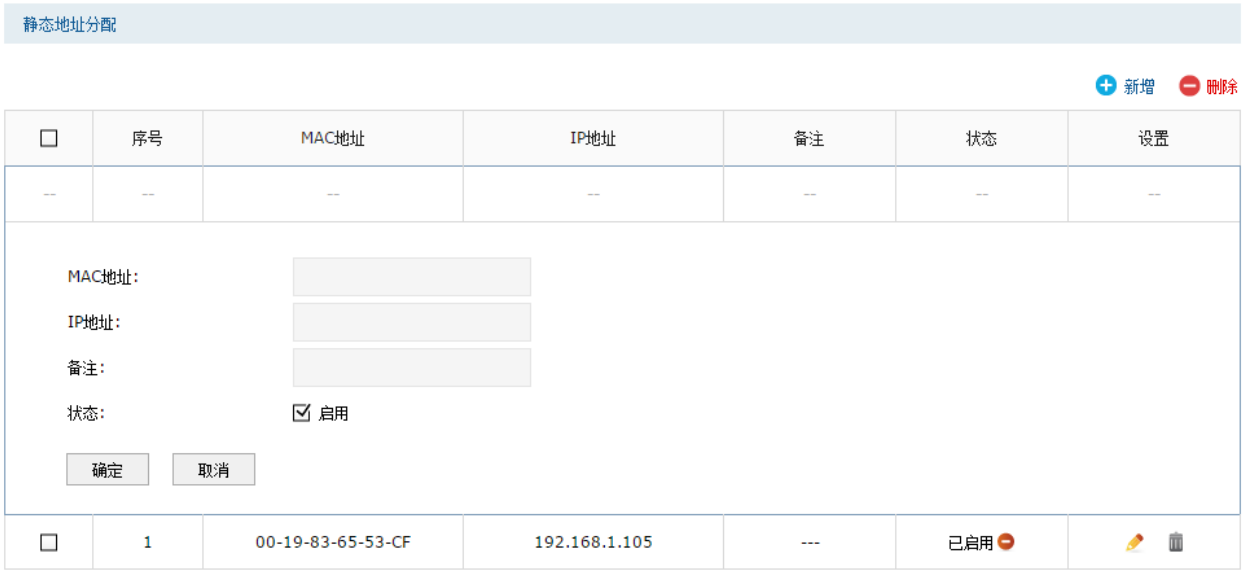


图 4-11 静态地址分配设置界面

界面项说明：

- **新增**

MAC地址	设置待分配IP地址的客户端的MAC地址。
IP地址	指定当前MAC地址所对应的客户端的IP地址。
备注	添加对本条目的说明信息。
状态	选择是否使本条目生效。

- **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。

4.3.4 MAC设置

路由器MAC地址是它在网络中的身份标志，一般来说无需更改。

WAN口MAC设置：

有些ISP要求上网账号与拨号设备的MAC绑定，若此时拨号设备更换为TL-WVR1300G，只需将路由器WAN口的MAC地址设置为原拨号设备的MAC地址即可。

LAN口MAC设置：

在一个所有设备都进行了ARP绑定的复杂拓扑中，如果其中一个网络节点的路由器更换为TL-WVR1300G，为避免该节点下面接入的所有网络设备都更新ARP绑定表，直接将TL-WVR1300G的LAN口MAC地址设置为原路由器的MAC地址即可。

界面进入方法：基本设置 >> MAC设置 >> MAC设置

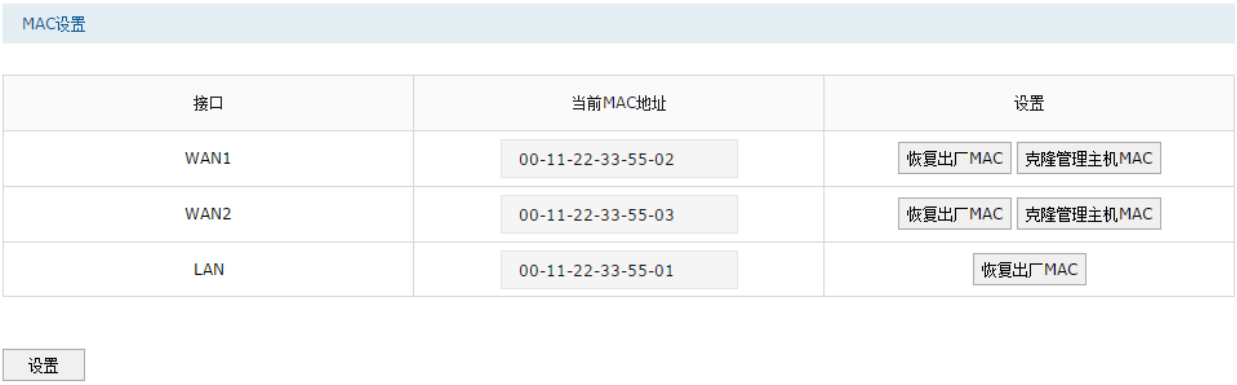


图 4-12 MAC设置界面

界面项说明：

- **MAC设置**

接口	显示当前路由器各接口。
当前MAC地址	显示当前各接口的MAC地址。
设置	如需恢复初始状态，请点击<恢复出厂MAC>按钮。如需将当前MAC地址设置为管理主机MAC地址，即当前登录路由器进行配置管理的主机MAC地址，请点击<克隆管理主机MAC>按钮。

说明：

为了防止局域网内MAC地址冲突，路由器LAN口的MAC地址不能设置成当前管理主机的MAC地址。

4.3.5 交换机设置

千兆企业VPN路由器系列产品具备一些简单的交换机端口管理功能。在此可以实时查看路由器各端口的数据流通状况，并进行相应的控制和管理。

4.3.5.1 端口统计

用于交换信息的数据包在数据链路层通常称为“帧”。可以通过此功能查看各个端口收发数据帧的统计信息。

界面进入方法：基本设置 >> 交换机设置 >> 端口统计

端口统计列表

参数		端口1	端口2	端口3	端口4	端口5
接收	单播帧	0	0	1439	0	0
	广播帧	0	0	2074	0	0
	流控帧	0	0	0	0	0
	多播帧	0	0	336	0	0
	所有帧	0	0	3849	0	0
	过小帧	0	0	0	0	0
	正常帧	0	0	3849	0	0
	过大帧	0	0	0	0	0
发送	单播帧	0	0	1903	0	0
	广播帧	0	0	0	0	0
	流控帧	0	0	0	0	0
	多播帧	0	0	0	0	0
	所有帧	0	0	1903	0	0

刷新 清空

图 4-13 端口统计界面

界面项说明：

- **统计列表**

单播帧 目的MAC地址为单播MAC地址的正常数据帧数目。

广播帧 目的MAC地址为广播MAC地址的正常数据帧数目。

流控帧 接收/发送的流量控制数据帧数目。

多播帧 目的MAC地址为多播MAC地址的正常数据帧数目。

所有帧	单播帧、广播帧、流控帧、多播帧的总帧数
过小帧	收到的长度小于64字节的数据帧数目（包含校验和错误的帧）。
正常帧	收到的长度在64字节到1518字节之间的数据帧数目（包含错误帧）。
过大帧	收到的长度大于1518字节的数据帧数目（包含错误帧）。

点击<刷新>按钮可对数据进行刷新，点击<清空所有>按钮可以一次清空所有统计数据。

4.3.5.2 端口监控

可以在此开启和设置端口监控功能。被监控端口的报文会被自动复制到监控端口，以便网络管理人员实时查看被监控端口传输状况的详细资料，对其进行流量监控、性能分析和故障诊断。

界面进入方法：基本设置 >> 交换机设置 >> 端口监控

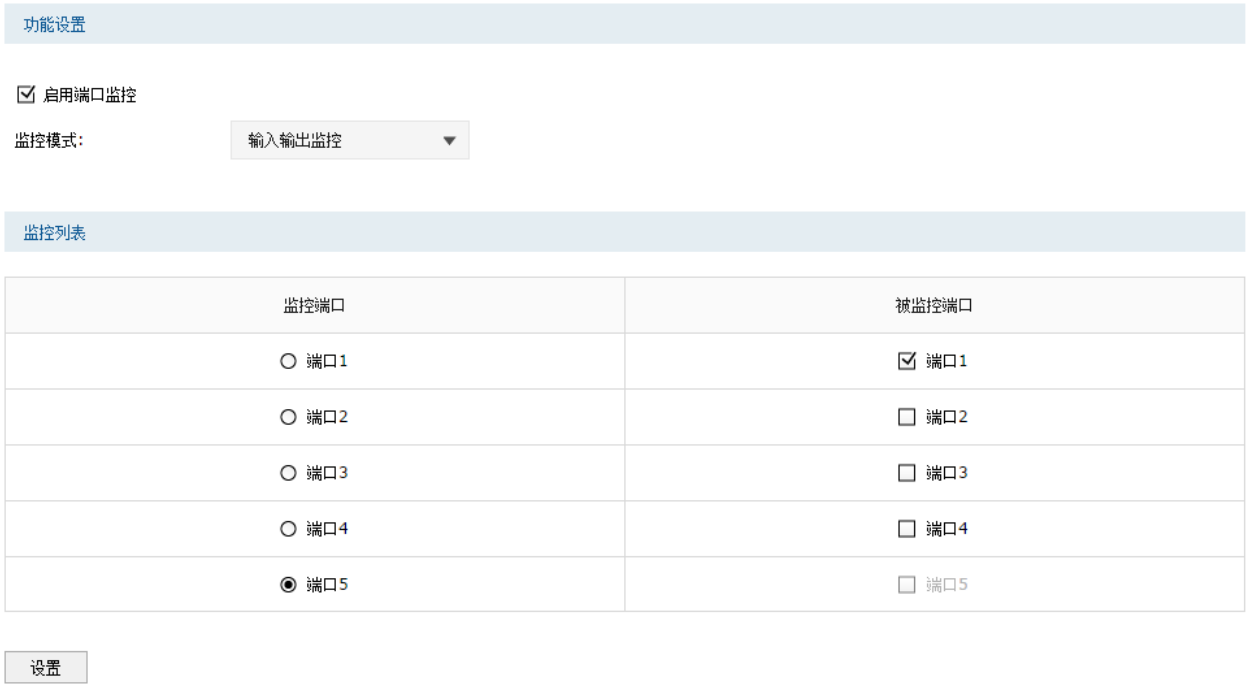


图 4-14 端口监控设置界面

界面项说明：

- **功能设置**

启用端口监控	勾选即启用端口监控。推荐勾选，方便及时了解路由器端口报文信息。
监控模式	选择对数据包进行“输入监控”、“输出监控”或者“输入输出监控”。

➢ **监控列表**

监控端口	只能选择一个端口做监控端口。
被监控端口	被监控端口可以为多个，但不包含当前的监控端口。

图 4-14监控列表的含义是：端口5被选作监控端口，它将对端口1进行输出监控。

应用举例

某企业网络出现异常状况，需要利用端口监控功能捕获网络中的所有数据进行分析。

可通过端口监控实现此需求。勾选“启用端口监控”，并选择“输入输出监控”的监控模式，设置端口3为监控端口，监控其它端口的输入输出数据，如图4-15所示。设置完成后，点击<设置>按钮。

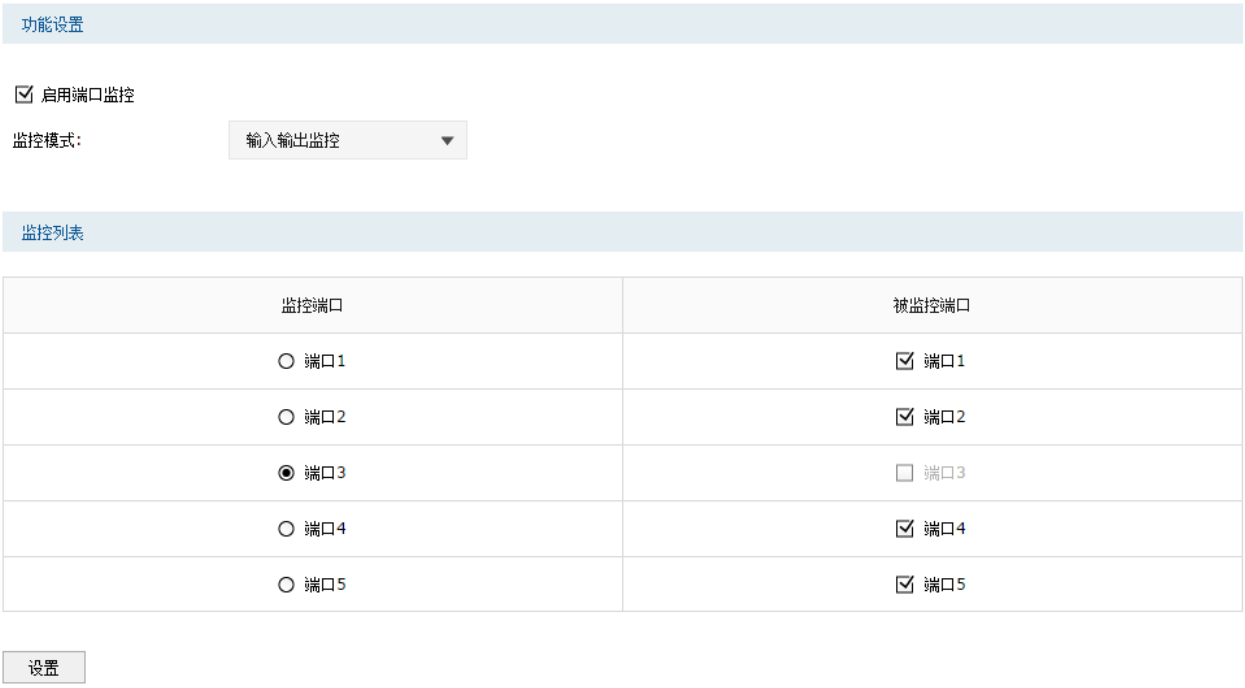


图 4-15 端口监控应用设置界面

4.3.5.3 端口流量限制

可以在此开启各端口的流量限制功能并进行相应设置。

界面进入方法：基本设置 >> 交换机设置 >> 端口流量限制

图 4-16 端口流量限制设置界面

界面项说明：

➢ **功能设置**

端口	显示所有物理端口，需要对某个端口进行流量限制时，在其对应行设置即可。
入口限制	勾选“启用”后，后续设置的入口限制模式和速率才会生效。
入口限制模式	有“所有帧”、“广播和多播帧”和“广播帧”三种模式，选择其一。
入口限制速率	设置入口限制速率。
出口限制	勾选“启用”，后续设置的出口限制速率才会生效。
出口限制速率	设置出口限制速率。

4.3.5.4 端口参数

可以在此启用各物理端口及其流量限制，并根据需要设定其协商模式。

界面进入方法：基本设置 >> 交换机设置 >> 端口参数

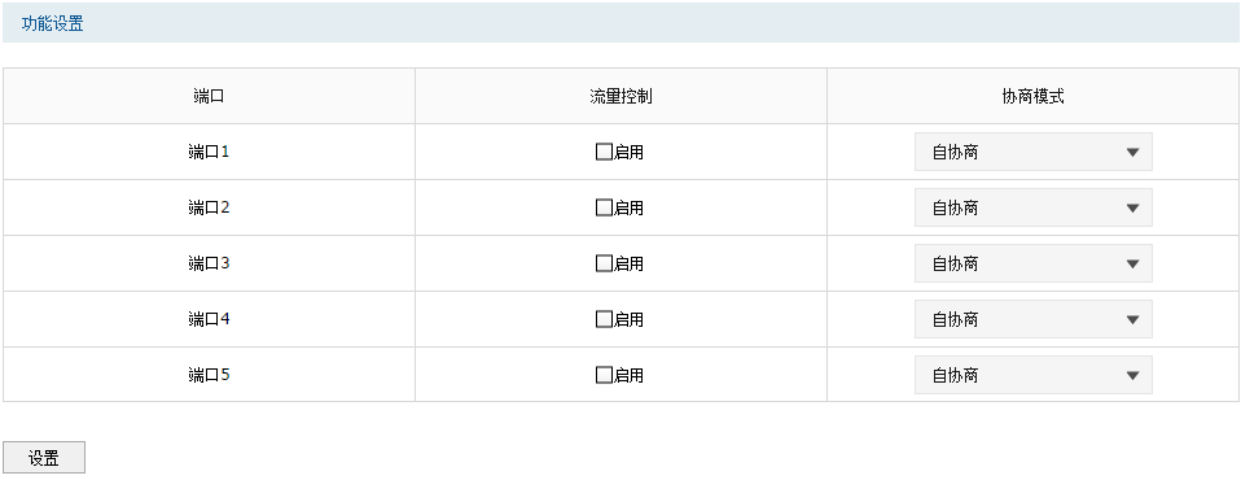


图 4-17 端口参数设置界面

界面项说明：

➢ **功能设置**

流量控制 推荐勾选“启用”以控制调节各端口数据包转发的速率，避免出现拥塞。

协商模式 有10M全/半双工、100M全/半双工、1000M全双工、自协商6种模式可选，择需使用。

4.3.5.5 端口状态

可以在此查看各个端口的基本状态。

界面进入方法：基本设置 >> 交换机设置 >> 端口状态

图 4-18 端口状态界面

4.4 对象管理

说明：

对象管理中所有功能的条目，一旦添加，出现在列表管理区，将不能修改条目名称。

4.4.1 地址管理

4.4.1.1 地址管理

可以在此创建、修改或者删除组。

界面进入方法：对象管理 >> 地址管理 >> 地址管理

图 4-19 地址管理界面

界面项说明：

➢ **组列表**

组名称 输入一个名称来标识一个组，可以输入1-28个字符。

地址名称 本组所包含的地址名称。地址名称需在**4.4.1.2地址**中进行设置。

备注 添加对当前组的说明信息。

在组列表中，可以对已创建的组进行相应设置。序号1-2条目为系统自动添加条目，不可操作。序号1条目表示所有IP地址，序号2条目表示LAN网段所有IP地址。

说明：

若地址组正被其他规则引用，则该地址组无法删除。

4.4.1.2 地址

可以在此添加、修改或者删除用户。

界面进入方法：对象管理 >> 地址管理 >> 地址

图 4-20 地址设置界面

界面项说明：

➢ **地址列表**

名称	输入一个名称来标识地址，可以输入1~50个字符。
IP类型	在此建立源地址范围。主要有以下2种表示方式。 IP段：由起始IP地址到结束IP地址确定IP地址范围。 IP/子网掩码：由IP地址和子网掩码确定IP地址范围。
IP段	当选择的IP类型为IP段时，显示指定的IP地址的范围
IP/MASK	当选择的IP类型为IP/MASK时，显示指定的IP地址的范围
备注	添加对当前地址的说明信息。

在地址列表中，可以对已创建的条目进行相应设置。序号1条目为系统自动添加条目，不可操作，表示所有IP地址。

说明：

若地址正被其他规则引用，则该地址无法删除。

4.4.2 时间管理

4.4.2.1 时间管理

可以在此创建、修改或者删除时间组。

界面进入方法：对象管理 >> 时间管理 >> 时间组

图 4-21 时间管理界面

界面项说明：

- **时间对象列表**

时间对象名称	自定义的时间对象名称。注意不能与已有的时间对象的名称重复，且名称长度不能超过50个字符。
工作时间	本条目所对应的工作时间段。
备注	添加对当前时间组的说明信息。

图 4-21序号1条目是路由器预定义的一个时间组，表示所有时间，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，如图 4-22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“工作日历”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。

说明：

若时间组正被其他规则引用，则该时间组无法删除。

4.4.3 IP地址池

可以通过本页面设置IP地址池条目，进行地址池的管理。新增IP地址池主要与无线网络关联，创建无线网络时选择相应的IP地址池，无线网络会自动与所选的IP地址池对应。已经被引用的IP地址池无法被其他新增的无线网络引用。

界面进入方法：对象管理 >>IP地址池 >> IP地址池

图 4-23 IP地址池设置界面

界面项说明：

➢ **地址池列表**

地址池名称	自定义的地址池名称。
地址池范围	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地址。

点击<新增>按钮，可以新增一个地址池。

说明：

若地址池正被其他规则引用，则该地址池无法删除。

4.4.4 服务类型

可以在本页面设置自定义服务类型。

界面进入方法：对象管理 >> 服务类型 >> 服务类型

服务类型列表

新增 删除

□	序号	服务名称	协议类型/协议号	详细信息	备注	设置
--	1	ALL	0-255	---	ALL	---
--	2	FTP	TCP	源端口 = 0-65535; 目的端口 = 21-21	FTP	---
--	3	SSH	TCP	源端口 = 0-65535; 目的端口 = 22-22	SSH	---
--	4	TELNET	TCP	源端口 = 0-65535; 目的端口 = 23-23	TELNET	---
--	5	SMTP	TCP	源端口 = 0-65535; 目的端口 = 25-25	SMTP	---
--	6	DNS	UDP	源端口 = 0-65535; 目的端口 = 53-53	DNS	---
--	7	HTTP	TCP	源端口 = 0-65535; 目的端口 = 80-80	HTTP	---
--	8	POP3	TCP	源端口 = 0-65535; 目的端口 = 110-110	POP3	---
--	9	SNTP	UDP	源端口 = 0-65535; 目的端口 = 123-123	SNTP	---
--	10	H.323	TCP	源端口 = 0-65535; 目的端口 = 1720-1720	H.323	---
--	11	ICMP_ALL	ICMP	Type =255; Code = 255	icmp	---

图 4-24 服务类型设置界面

界面项说明：

➢ **服务类型**

服务名称	自定义服务的名称。
协议类型/协议号	所选择的服务使用的协议。
详细信息	服务的具体信息，如源端口范围、目的端口范围等。
备注	服务类型的具体描述。

点击<新增>按钮，可以新增一个服务条目，如图4-25所示。

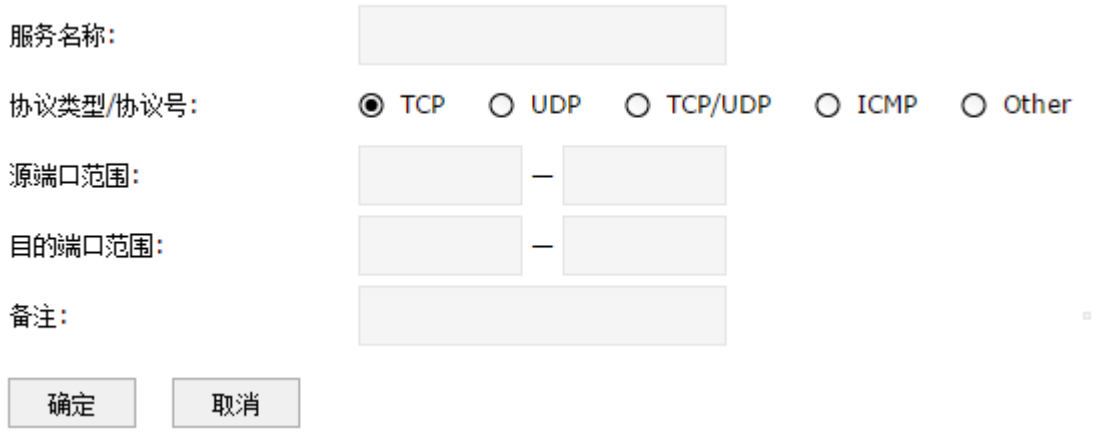


图 4-25 新增服务条目

如果选择的协议类型为 TCP 或 UDP，则需要输入输入服务所使用的源端口范围；如果选择的协议类型为 ICMP，则需要输入 ICMP 协议的类型（Type）和编码（Code），填充 255 时表明所有类型/编码。

4.5 传输控制

4.5.1 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。

4.5.1.1 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：传输控制 >> NAT设置 >> NAPT

图 4-26 NAPT界面

点击<新增>按钮，可添加NAPT规则。

界面项说明：

- **NAPT规则**

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。
备注	添加对本条目的说明信息，非必填项。

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

如图 4-27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。

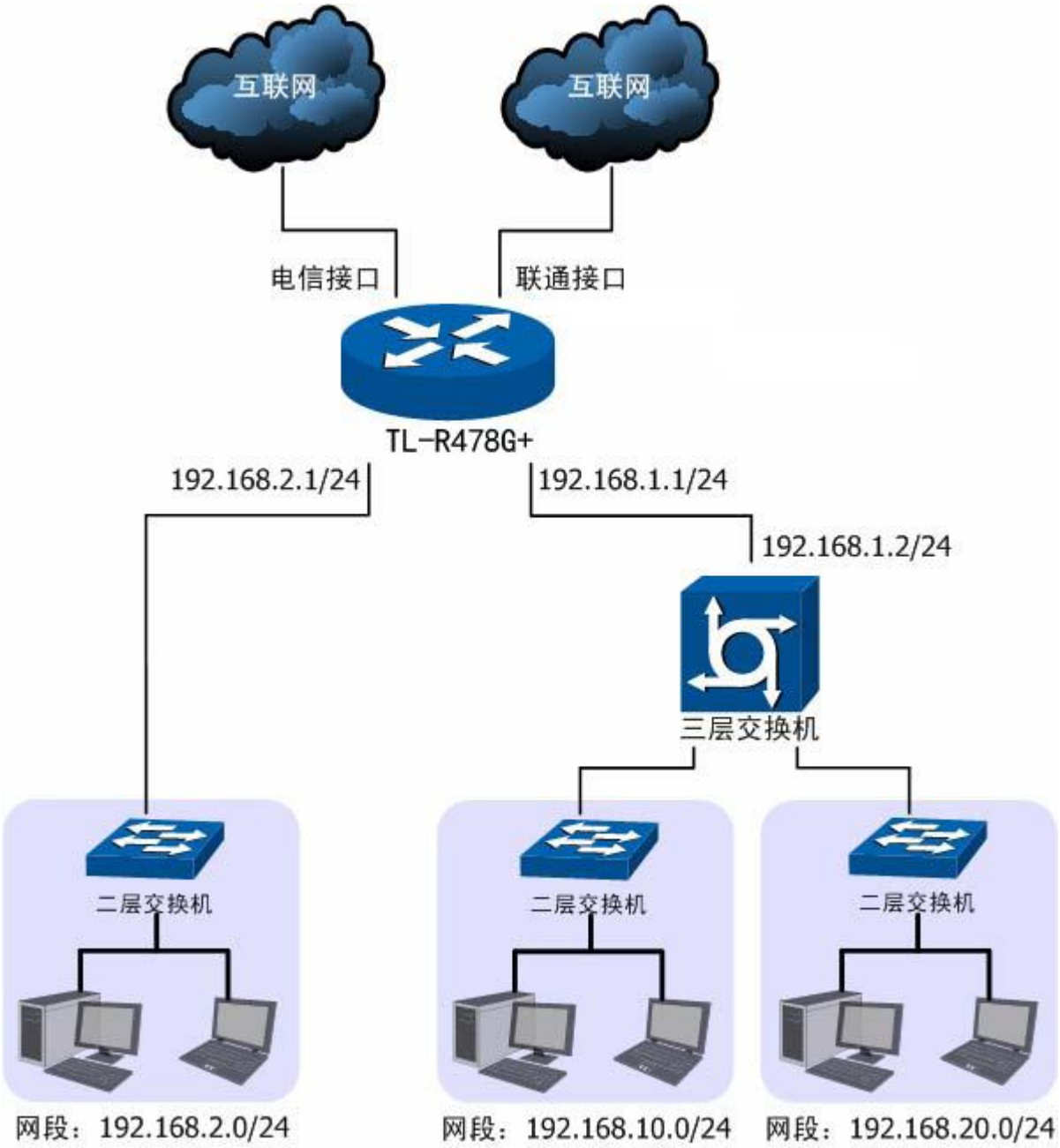


图 4-27 NAPT功能组网应用

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：传输控制 >> 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：传输控制 >> 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图4-28所示。

图 4-28 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4.5.5路由设置

4.5.1.2 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：传输控制 >> NAT设置 >> 一对一NAT

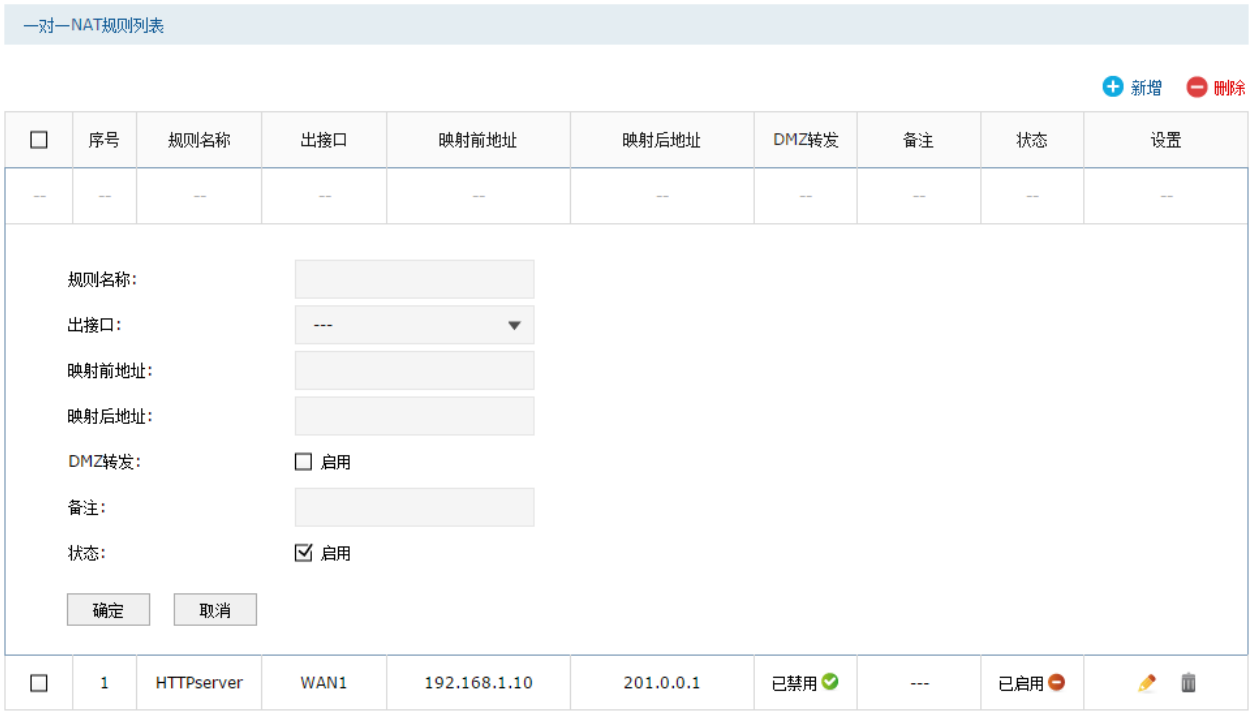


图 4-29 一对一NAT界面

点击<新增>按钮，可新增一条一对一NAT规则。

界面项说明：

- **NAT映射**

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。
备注	添加对本条目的说明信息，非必填项。

状态	勾选“启用”，则使该规则条目生效；

图 4-29序号1条目的含义：路由器通过接口“WAN1”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，“WAN1”接口收到目的地址为201.0.0.1的访问请求时，会拒绝处理。

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。

4.5.1.3 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：传输控制 >> NAT设置 >> 虚拟服务器

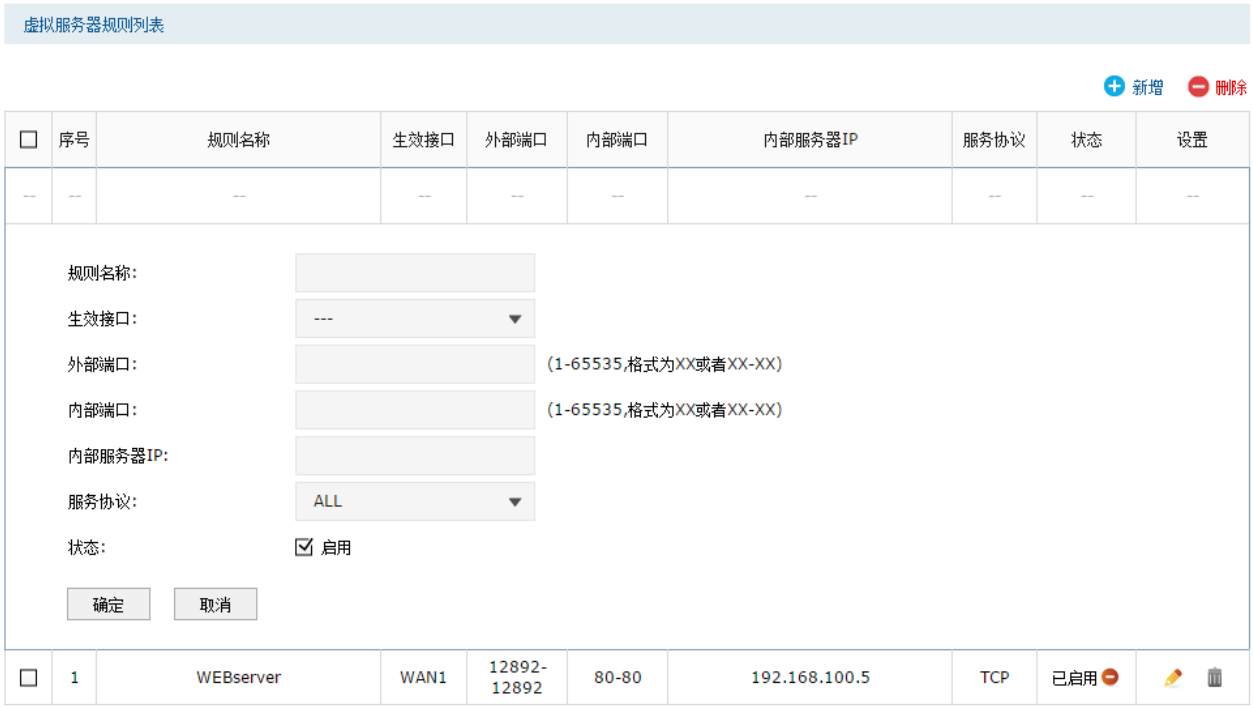


图 4-30 虚拟服务器设置界面

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**

服务名称	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	勾选“启用”，则使该规则条目生效；

图 4-30序号1规则的含义：广域网用户向接口“WAN1”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。

4.5.1.4 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：传输控制 >> NAT设置 >> ALG服务

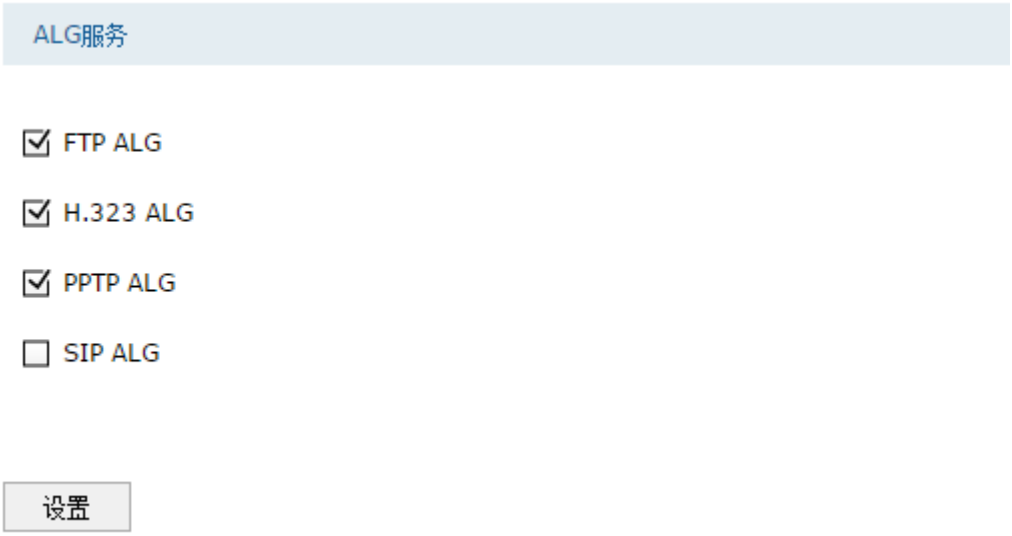


图 4-31 ALG服务设置界面

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。

4.5.1.5 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：传输控制 >> NAT设置 >> NAT-DMZ

图 4-32 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。

4.5.2 带宽控制

带宽控制功能通过对各种数据流设置相应的限制规则，实现对数据传输的带宽控制，从而使有限的带宽资源得到合理分配，达到有效利用现有带宽的目的。

界面进入方法：传输控制 >> 带宽控制 >> 带宽控制

图 4-33 带宽控制规则设置界面

界面项说明：

- **功能设置**

  勾选“启用带宽控制”，点击<设置>按钮，下方的带宽控制规则才能生效。

  启用带宽控制功能后，还可以勾选设置仅当带宽利用率达到某个百分比以上时，才使带宽控制功能生效。

- **带宽控制规则列表**

  点击<新增>按钮，可以新增一条带宽控制规则。

  规则名称　　输入该规则条目的名称。

  数据流向　　选择此带宽控制规则生效的数据流向。

受控地址组	设置受控的IP地址范围，此处的地址组与上面的受控地址类型共同指定此规则的控制对象。如需新建地址组，请参考4.4.1地址管理
最大上行带宽	设置受控计算机所能使用的最大上行带宽。
最大下行带宽	设置受控计算机所能使用的最大下行带宽。
带宽模式	独立模式即受控地址范围内每一个IP地址都将应用当前规则所设置的带宽限制； 共享模式即受控地址范围内所有IP地址带宽总和为当前规则所设置的带宽限制。
生效时间	选择规则生效时间，其他时间规则不生效。如需新建时间组，请参考4.4.2时间管理。
备注	对该条规则的备注信息，允许留空。
添加到指定位置	勾选该项后，可以将当前设置的规则添加到规则列表中指定序号的位置。默认情况下，新增规则显示在规则列表的最后。规则条目在规则列表中的位置越靠前，即规则序号数字越小，该规则优先级越高。
状态	勾选“启用”，则使该规则条目生效；

图 4-33序号1规则的含义：局域网中IP地址在“IPGROUP_ANY”地址组内的计算机发往WAN1口的通信数据将共享1000Kbps的最大上行带宽和下行带宽，此规则在“workday”时间段内生效。

说明：

- 单条规则生效的前提是：这条带宽控制规则所属接口的物理带宽足够大，且尚未被用尽。

4.5.3 连接数限制

作为局域网的统一出口，路由器支持的TCP和UDP连接数是有限的，如果局域网内有部分主机向广域网发起的TCP和UDP数目过多，影响局域网其他计算机的通信质量，就有必要对这部分计算机进行连接数限制。

4.5.3.1 连接数限制

可以在此对指定IP的计算机连接数限制进行设置。

界面进入方法：传输控制 >> 连接数限制 >> 连接数限制

图 4-34 连接数限制设置界面

界面项说明：

- **功能设置**

勾选“启用连接数限制功能”，点击<设置>按钮，下方的连接数控制规则才能生效。

- **连接数限制规则列表**

点击<新增>按钮，可新增一条连接数限制规则。

规则名称 输入该规则条目的名称。

受控地址组 选择需要进行连接数限制的计算机的IP地址范围，由对象管理中的地址组来表示。如需新建地址组，请参考4.4.1地址管理。

最大连接数 设置受控地址范围中每台计算机所能使用的最大连接总数。

状态 勾选“启用”，则使该规则条目生效；

图 4-34序号1规则的含义：IP地址范围在“IPGROUP_LAN”地址组中的计算机分别能够通过路由器成功建立TCP或UDP的连接数是100条。该规则已启用。

4.5.3.2 连接数监控

监控列表显示局域网主机的连接数限制情况。

界面进入方法：传输控制 >> 连接数限制 >> 连接数监控

图 4-35 连接数监控界面

可通过监控列表搜索、查询已设置连接数限制规则的地址组主机连接数信息。如需获取最新信息，请点击<刷新>按钮。

4.5.4 流量均衡

合理设置流量均衡，可以使路由器更安全、有效地收发数据。

4.5.4.1 基本设置

界面进入方法：传输控制 >> 流量均衡 >> 基本设置

图 4-36 流量均衡基本设置界面

勾选“启用特殊应用程序选路功能”，路由器会将数据包的源IP地址与目的IP地址，或者源IP地址与目的端口地址作为一个整体，记录其通过的WAN口信息。后续如果有同一源IP地址和目的IP/端口地址的数据包通过，则优先转发至上次记录的WAN口。该功能主要用于保证多连接应用程序的正常工作。

勾选“启用智能均衡”，并选定生效的WAN口，在没有任何选路规则的情况下，指定WAN口将自动进行流量均衡。在实际应用中，如果某些WAN口没有连接到因特网，那么这些WAN口将不会参与智能均衡，请勿勾选。

设置完成后点击<设置>按钮生效。

说明：

- 若要使“智能均衡”生效，请先到**基本设置 >> WAN 设置**页面设置各接口的带宽，再到**传输控制 >> 流量均衡>>在线检测**页面设置各接口的在线检测。
- “智能均衡”各接口的流量比等于设置的各接口带宽比。如果接口 1 和接口 2 带宽比为 2：1，那么对接口 1 和接口 2 启用“智能均衡”后，通过接口 1 和接口 2 的流量比约为 2：1。

4.5.4.2 ISP选路

通过ISP选路功能，可以将数据包转发至对应的ISP线路上，从而减少数据包在网络中被转发的次数，提高网络性能。

界面进入方法：传输控制 >> 流量均衡 >> ISP选路

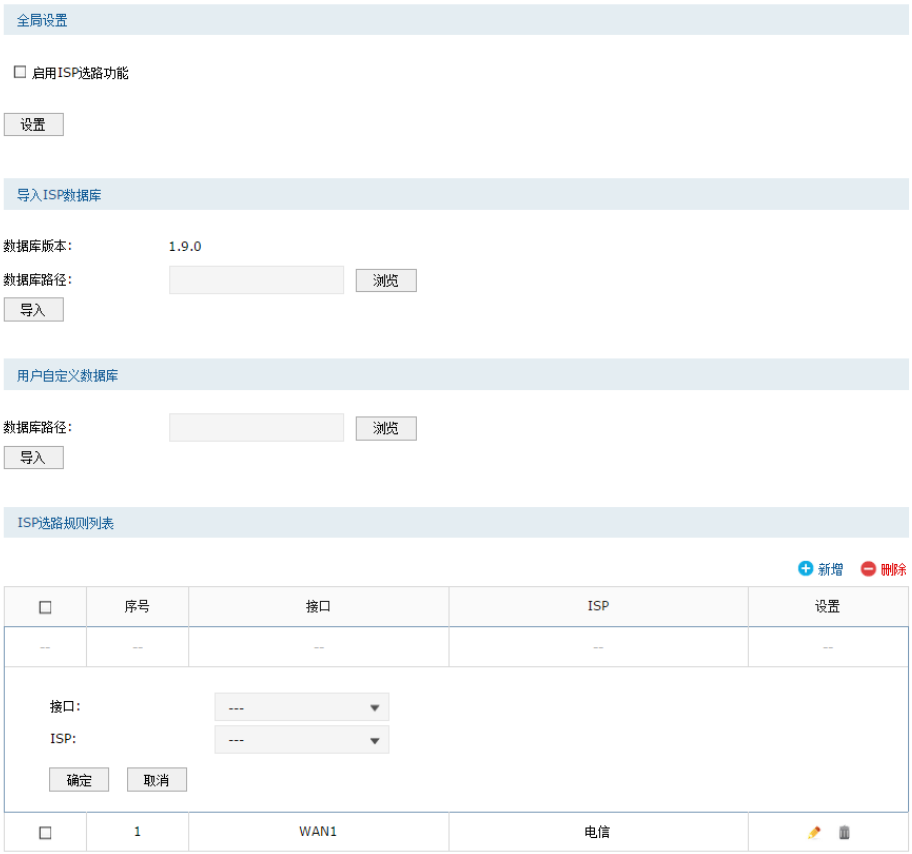


图 4-37 ISP选路设置界面

界面项说明：

- **全局设置**

  勾选“启用ISP选路功能”，点击<设置>按钮，下方的选路设置才能生效。

- **导入ISP数据库**

  ISP数据库即各ISP所拥有的IP地址段的数据库，通过匹配数据包目的IP地址与ISP数据库，路由器会将数据包从相应ISP所对应的WAN口转发。请在我司官方网站下载最新ISP数据库，单击<浏览>按钮，选择保存路径下的文件，点击<导入>即可。

- **用户自定义数据库**

  导入用户自定义的ISP数据库。

- **ISP选路规则列表**

  点击<新增>按钮，可以新增一条ISP选路规则。

接口	选择进行ISP选路的接口。
ISP	在下拉列表中选择ISP。

图 4-37序号1规则的含义：WAN1接口对应电信ISP，所有通过电信线路进入广域网的数据包将从WAN1口转发。

说明：

智能均衡、ISP选路两个功能可以同时工作，但当两个功能设置有冲突时，路由器执行的优先顺序为：ISP选路 > 智能均衡。

4.5.4.3 线路备份

路由器默认所有WAN口都处于自动备份模式，当有WAN口发生故障时，其流量会均衡到其他WAN口上，当故障WAN口恢复后系统会再次均衡所有WAN口的流量。

根据实际需要合理设置线路备份，可以减轻WAN口流量负担，提高网络效率。

界面进入方法：传输控制 >> 流量均衡 >> 线路备份

图 4-38 备份配置界面

界面项说明：

➢ **线路备份规则列表**

主接口	选择主接口。接口设置请参考4.3.2WAN设置。
备接口	选择备份接口。接口设置请参考4.3.2WAN设置。
备份模式	可以选择定时备份或故障备份。选择定时备份时，下方可进行备份生效时间设置。
生效时间	当备份模式为定时备份时，需要在此指定生效时间。在生效时间内启动备份接口，关闭主接口。时间设置请参考4.4.2时间管理。
状态	选择启用或禁用本条线路备份规则。

图 4-38序号1规则的含义：WAN1口为主接口，WAN2口为备份接口，任何时间，当WAN1口发生故障时启用WAN2口，该规则已启用。

说明：

主WAN组和备WAN组中不能放置相同的WAN口，且一个WAN口只能置入一个主备组中。

4.5.4.4 在线检测

该页面用于检测WAN口是否在线。

界面进入方法：传输控制 >>流量均衡 >> 在线检测

图 4-39 在线检测界面

点击<设置>图标，可以对在线检测列表中的每一条项目进行设置。

界面项说明：

- **检测设置**

接口名	显示接口名称。
检测模式	选择自动在线检测或者手动在线检测。自动模式下，PING检测选择网关作为目的地址，DNS检测选择WAN口DNS服务器作为目的地址；手动模式下，可以自己设置PING检测和DNS检测的目的地址。
PING检测	在手动在线检测模式下，可以输入PING检测的目的IP地址。输入0.0.0.0表示不进行PING检测。
DNS检测	在手动在线检测模式下，可以输入DNS服务器的IP地址。输入0.0.0.0表示不进行DNS检测。

接口状态列表中的条目是创建接口时系统自动添加的，会自动显示出接口名和接口状态。

说明：

- 接口的状态和流量均衡功能有关，不在线的接口将不分担流量。
- 页面显示的接口状态可能有延迟，请及时刷新页面以获取接口的实时状态。

4.5.5 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。

4.5.5.1 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：传输控制 >> 路由设置 >> 策略路由

图 4-40 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	输入该规则条目的名称。
服务类型	选择服务类型，以建立选路规则条目的协议、源端口范围（协议为TCP、UDP、TCP/UDP）、目的端口范围（协议为TCP、UDP、TCP/UDP）。
源地址	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	选择地址对象，以建立选路规则条目的目的地址范围。
生效接口	选择符合此选路规则条目数据包的出接口。
生效时间	选择规则生效时间。
备注	添加对本条规则的说明信息。
添加到指定位置	设置通往目标网络的路由路径上下一个节点的IP地址。
状态	勾选“启用”，则使该规则条目生效。

图 4-40 策略路由设置界面序号1规则的含义：从源地址组“IPGROUP_ANY”发往目的地址组“IPGROUP_LAN”的FTP类型的数据，在 “ANY” 时间段内从LAN口发出。

4.5.5.2 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：传输控制 >> 路由设置 >> 静态路由

图 4-41 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。

备注 添加对本条规则的说明信息

设置完成后勾选“启用”并点击<确定>，则使该规则条目生效。

图 4-41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。

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。

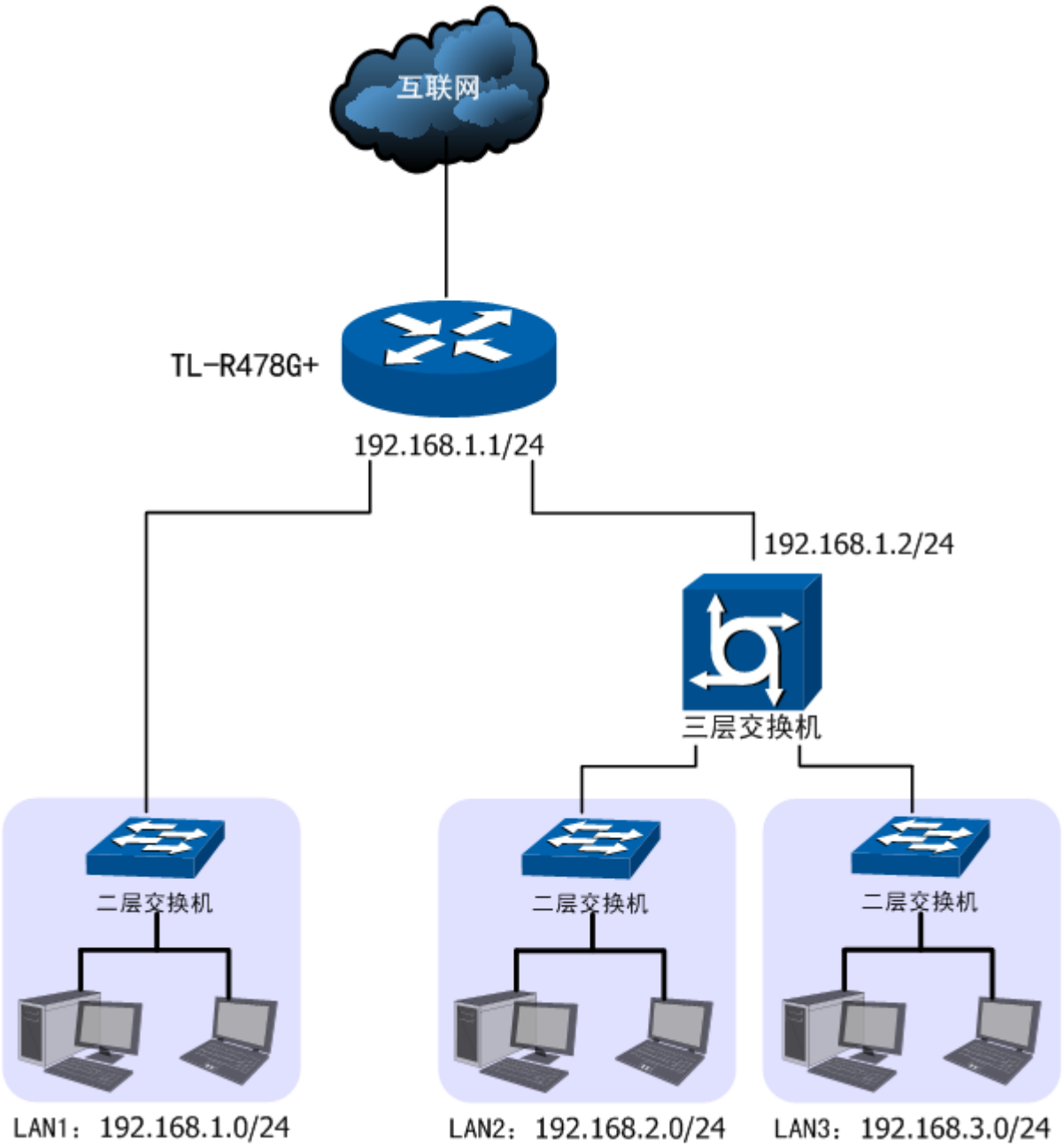


图 4-42 静态路由功能组网应用

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：传输控制 >> 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

勾选”启用”并点击<确定>。

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：传输控制 >> 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

勾选”启用”并点击<确定>。

4.5.5.3 系统路由

通过本页面可查看系统路由表。

条目数量：3 刷新

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	192.168.1.0	255.255.255.0	0.0.0.0	LAN	0

图 4-43 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。

4.6 安全管理

4.6.1 ARP防护

一台主机向局域网内另一台主机发送IP数据包，此时设备需要通过MAC地址确定目的接口才能进行通信，而IP数据包中不包含有MAC地址信息，因此需要将IP地址解析为MAC地址。ARP（Address Resolution Protocol，地址解析协议）正是用来实现这一目的的网络协议。网络中的所有设备，包括路由器和计算机在内，都各自维护一份ARP列表，该列表建立了主机IP地址和MAC地址一一对应关系。

按照ARP协议的设计，设备通过数据包的交互学习到其他设备的IP地址和MAC地址信息，并将这些信息添加至自身的ARP表中。每次通信时会先通过该表查找对应地址，减少网络上过多的ARP通信量。但设备同时也会接收不是自己主动请求的ARP应答，这就为“ARP欺骗”创造了条件。

ARP欺骗是局域网的攻击主机发送ARP欺骗包，将伪造的IP与MAC对应关系替换设备ARP列表中的记录，从而导致局域网内计算机不能正常上网。这类ARP攻击严重影响了局域网内部通信，由此便产生了ARP防护技术。

4.6.1.1 IP-MAC绑定

IP-MAC绑定是一种防护技术，能够防止ARP列表被伪造的IP-MAC对应信息替换。

界面进入方法：安全管理 >> ARP防护 >> IP MAC绑定

图 4-44 IP MAC绑定设置界面

点击<新增>按钮，可新增一条IP-MAC绑定规则列表。

界面项说明：

- **全局设置**

  推荐勾选所有项目，以便最大程度地防范ARP攻击。在勾选“仅允许IP MAC绑定的数据包通过路由器”选项前，请先将管理主机的IP MAC信息导入绑定列表中，并设置生效。

  当路由器受到ARP攻击时，路由器会将自身正确的ARP列表信息以GARP（Gratuitous ARP，免费ARP）包的方式主动发送给被攻击的设备，从而替换该设备错误的ARP列表信息。可在发包间隔处指定发包速率。

- **IP MAC绑定**

IP地址	手动输入需要进行绑定的IP地址。
MAC地址	手动输入与IP地址正确对应的MAC地址。
生效域	选择绑定的接口。
备注	添加对本条目的说明信息，非必填项。
状态	选择启用或禁用本条绑定规则。

图 4-44序号1条目的含义：目前路由器已将IP地址192.168.1.101与MAC地址00-19-83-66-69-CF进行绑定，该绑定规则已启用。

说明：

若当前绑定列表中所有条目都未启用，在勾选“仅允许IP MAC绑定数据包通过路由器”的功能设置选项并保存后，将无法登录路由器Web管理界面，此时必须将路由器恢复出厂配置才能再次登录。

<导入>是指从**IP MAC绑定列表**中导入静态地址条目。点击<导入>，将直接获取IP MAC绑定列表中的静态地址条目。在<导入>过程中，如果提示IP/MAC条目与静态地址条目有冲突，发生冲突的条目不会被导入，没有发生冲突的条目会继续被导入。

4.6.1.2 ARP扫描

ARP扫描界面可以将指定范围内的IP与其对应MAC地址全部扫描出来，在扫描列表中显示。

界面进入方法：安全管理 >> ARP防护 >> ARP扫描

图 4-45 ARP扫描界面

在扫描范围填入起始IP与结束IP后，点击<开始扫描>按钮，路由器将扫描该范围内所有正在工作的主机，并将它们对应的IP MAC地址信息显示在扫描列表中。

扫描结果中显示的IP MAC地址对应信息条目并不代表已经被绑定，在“状态”一列中会标识当前状态：

不显示任何内容表示当前条目未被绑定，可能会被错误的ARP信息更替掉；

显示“已导入”仅表示当前条目已导入“IP MAC绑定”界面的绑定列表中，还需在“IP MAC绑定”界面的绑定列表中设置启用后，该条目才会生效；

若现在需要绑定扫描列表中未绑定的条目，可以在“选择”一列勾选这些条目，然后点击<导入>按钮，在与已绑定条目不冲突的情况下，导入后绑定立即生效。

说明：

- 扫描前请关闭 IP MAC 绑定页面“仅允许 IP MAC 绑定的数据包通过路由器”选项。
- 若局域网内已经存在 ARP 攻击导致部分主机通信异常，则不可通过扫描方式添加绑定，请在“IP MAC 绑定”界面进行手动绑定。

4.6.1.3 ARP列表

路由器会将近期与其通信过的主机IP MAC对应信息保存在ARP列表中。

界面进入方法：安全管理 >> ARP防护 >> ARP列表

图 4-46 ARP列表界面

ARP列表条目的操作可参考**4.6.1.2 ARP扫描**的扫描列表。

列表中未绑定的条目并不是一直存在，除了会被新的IP MAC对应信息更替之外，还会由于长时间未通信而自动从列表中删除，这个时间段就是ARP信息的老化时间。

4.6.2 攻击防护

攻击防护可防止广域网对路由器或局域网内计算机进行端口扫描和恶意攻击，以此来保证它们的安全运行。

界面进入方法：安全管理 >> 攻击防护 >> 攻击防护

图 4-47 攻击防护设置界面

界面项说明：

- **功能设置**

防Flood类攻击	Flood类攻击是DoS攻击的一种常见形式。DoS（Denial of Service，拒绝服务）是一种利用发送大量的请求服务占用过多的资源，让目的路由器和服务器忙于应答请求或等待不存在的连接回复，而使正常的用户请求无法得到响应的攻击方式。常使用的Flood洪水攻击包括TCP SYN，

	UDP，ICMP等。推荐勾选界面上所有防Flood类攻击选项并设定相应阈值，如不确定，请保持默认设置不变。
防可疑包类	可疑包即非正常数据包，有可能是病毒或攻击者的扫描试探。推荐勾选界面上所有防可疑包选项。

4.6.3 MAC过滤

在此可以通过指定MAC地址对部分局域网主机进行过滤。

界面进入方法：安全管理 >> MAC过滤 >> MAC过滤

图 4-48 MAC过滤设置界面

点击<新增>按钮，可以新增一条MAC过滤规则。

界面项说明：

- **全局设置**

  若需要严格控制局域网内某些计算机访问广域网，推荐勾选“启用MAC地址过滤功能”，并根据实际情况选择一种过滤规则。

- **MAC过滤规则列表**

规则名称 输入该规则条目的名称。

MAC 地址 输入需要控制的局域网主机MAC地址。

4.6.4 访问控制

界面进入方法：安全管理 >> 访问控制 >> 访问控制

图 4-49 访问规则设置界面

点击<新增>按钮，可新增一条访问控制规则。

界面项说明：

➢ **访问控制规则列表**

规则名称 输入一个名称来标识该访问规则。

策略类型 在下拉列表中选择适用于本条规则的策略类型，可选择阻塞或者允许。

选择“阻塞”，则符合该条规则的所有数据包将无法通过路由器；
选择“允许”，则符合该条规则的数据包能通过路由器。

服务类型	在下拉列表中选择本条规则所针对的服务类型，不属于指定范围内的服务将不会应用该规则。例如策略类型选择为“阻塞”，只选定了FTP一种服务类型时，其他服务类型的数据包仍旧可以通过路由器。如需新建服务类型，请参考**4.4.4 服务类型**。
生效接口域	在路由器接口中选择生效的接口，ALL表示所有的接口。
源地址范围	在下拉列表中选择本条规则限制的源地址范围。如需新建地址组，请参考**4.4.1 地址管理**。
目的地址范围	在下拉列表中选择本条规则限制的目的地址范围。如需新建地址组，请参考**4.4.1 地址管理**。
生效时间	在下拉列表中选择本条规则生效的时间表。如需新建时间表，请参考**4.4.2 时间管理**。
添加到指定位置	勾选该项后，可以将当前设置的访问规则添加到规则列表中指定序号的位置。默认情况下，新增规则显示在规则列表的最后。规则条目在规则列表中的位置越靠前，即规则序号数字越小，该规则优先级越高。

图 4-49序号1规则的含义：在“workday”时间组设置的时间段内，“TPLINK_A”地址组内的主机向广域网中“Me”地址组内的主机发送的TELNET服务数据包无法通过路由器。

说明

局域网内没有设置规则的IP段，默认的策略类型是允许。

4.7 行为管控

4.7.1 应用控制

4.7.1.1 应用控制

可以在此启用并设置应用限制功能。本路由器可限制的应用包括即时通信、P2P软件、金融软件、游戏软件、视频软件、音乐软件、网页游戏、基础应用和代理。同时，可以对这些功能的使用情况做日志记录。

界面进入方法：行为管控 >> 应用控制 >> 应用控制

图 4-50 应用限制设置界面

点击<新增>按钮，可以新增一条应用控制规则。

界面项说明：

- **功能设置**

  勾选“启用应用限制功能”后，应用限制的相关设置才会生效，应用限制生效后局域网指定用户对指定软件的网络应用将受到限制。

- **应用控制规则列表**

  受控地址组　　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**4.4.1 地**

址管理。

禁用列表	选择禁止使用的应用。可以设置的应用包括即时通信、P2P软件、金融软件、游戏软件、视频软件、音乐软件、网页游戏、基础应用和代理。默认为对除了基础应用和代理的所有应用进行限制。
生效时间	设置规则的生效时间。由时间管理的时间组来表示。如需新建时间组，请参考**4.4.2 时间管理**。
备注	添加对本条规则的说明信息。
状态	选择启用或禁用本条规则。

在规则列表中，可以对已保存的应用限制进行相应设置。在此列表中，序号数字越小的规则，执行的优先级越高。

4.7.1.2 QQ黑白名单

可以在此对特殊QQ号码进行相关设置，实现不同用户、不同时间登录QQ的需求。同时，可以将用户使用QQ的情况，记录到系统日志。

界面进入方法：行为管控 >> 应用控制 >> QQ黑白名单

图 4-51 QQ黑白名单界面

点击<新增>按钮，可以新增一条规则。

界面项说明：

- **功能设置**

  勾选“启用QQ黑白名单”后，QQ黑白名单的相关设置才会生效。

- **规则设置**

受控地址组	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**4.4.1 地址管理**。

规则类型	可以选择白名单，使规则中的号码不被限制；也可以选择黑名单，使规则中的号码被限制。
QQ号码	在此输入QQ号码，可以同时输入多个QQ号码进行批量添加，通过使用空格、逗号或者回车换行来表示不同的QQ号码。
生效时间	设置规则的生效时间。由时间管理的时间组来表示。如需新建时间组，请参考**4.4.2 时间管理**。
备注	添加对本条规则的说明信息。
状态	选择启用或禁用本条规则。
添加到指定位置	勾选该项后，可以将当前设置的访问规则添加到规则列表中指定序号的位置。默认情况下，新增规则显示在规则列表的最后。规则条目在规则列表中的位置越靠前，即规则序号数字越小，该规则优先级越高。

图 4-51序号1规则的含义：该规则已经启用，地址组“IPGROUP_ANY”内的主机在时间组“workday”设置的时间段内，被设置的QQ号码不可以登录。

说明：

在没有配置应用限制规则和QQ黑名单的情况下，路由器默认所有用户所有QQ在任意时间都可登录。

应用举例

应用需求：

某企业有多名员工，该企业需要设置IP地址为10.1.1.30 - 10.1.1.35的员工可以在星期一到星期五的08：00到18：00登录QQ，禁止其余所有员工任何时间登录QQ。

实现方法：

有两种配置方法可以实现此需求。

方法一：配置一条QQ黑名单规则禁止所有员工任何时间登录QQ，再配置一条QQ白名单规则允许IP地址为10.1.1.30 - 10.1.1.35的员工可以在星期一到星期五的08：00到18：00登录QQ。QQ白名单规则序号要在QQ黑名单规则之前。

方法二：配置一条应用限制规则禁止所有员工任何时间登录QQ，再配置一条QQ白名单规则允许IP地址为10.1.1.30 - 10.1.1.35的员工可以在星期一到星期五的08：00到18：00登录QQ。

配置步骤：

在配置应用限制规则或者QQ黑白名单规则之前，需要先设置所需用户组与时间组，设置如下：

1. 设置用户组，组内成员IP地址为10.1.1.30 - 10.1.1.35。

   界面进入方法：对象管理 >> 地址

   进入标签页**地址**，设置用户IP地址，此处可进行批量添加，点击<新增>：

名称	QQ_USER
IP类型	IP段 10.1.1.30-10.1.1.35
备注	可使用QQ用户

   进入标签页**地址管理**，点击<新增>，设置地址组名称，将用户添加到地址组中：

组名称	QQ_GROUP
地址名称	QQ_USER
备注	可使用QQ组

2. 设置时间组，时间选择为星期一到星期五的08：00到18：00。

   界面进入方法：对象管理 >> 时间管理

   点击<新增>，时间组设置内容如下：

名称	workday
时间设置	手动设置
星期	一、二、三、四、五
时间段	08：00 - 18：00
备注	上班时间

   设置完成后的时间组如下：

图 4-52 时间组设置完成示意图

方法一设置如下：

界面进入方法：行为管控 >> 应用控制 >> QQ黑白名单

全局设置如下：

勾选“启用QQ黑白名单功能”，点击<设置>按钮使设置生效。

QQ黑名单规则设置内容如下：

受控地址组 IPGROUP_ANY

规则类型 黑名单：禁止下列QQ号码登录

QQ号码 禁止登录的员工的QQ号码

生效时间 Any

状态 启用

QQ白名单规则设置内容如下：

受控地址组 QQ_GROUP

规则类型 白名单：禁止下列QQ号码登录

QQ号码 允许登录的员工的QQ号码

生效时间 workday

状态 启用

添加到指定位置 1

设置完成后的规则如下：

图 4-53 方法一设置完成示意图

方法二设置如下：

1. 设置应用限制，限制任何用户在任意时间登录QQ。

   界面进入方法：行为管控 >> 应用控制 >> 应用控制

   功能设置如下：

   勾选“启用应用控制功能”，点击<设置>按钮使设置生效。

   应用限制设置内容如下：

   受控地址组 IPGROUP_ANY

   禁用列表 腾讯QQ

   生效时间 Any

   状态 启用

   设置完成后的规则如下：

图 4-54 方法二步骤一设置完成示意图

2. 设置QQ白名单，允许可使用QQ组在上班时间登录QQ。

   界面进入方法：行为管控 >> 应用控制 >> QQ黑白名单

   全局设置如下：

   勾选“启用QQ黑白名单功能”，点击<设置>按钮使设置生效。

   QQ白名单规则设置内容如下：

受控地址组 QQ_GROUP

规则类型 白名单：禁止下列QQ号码登录

QQ号码 允许登录的员工的QQ号码

生效时间 workday

状态 启用

设置完成后的规则如下：

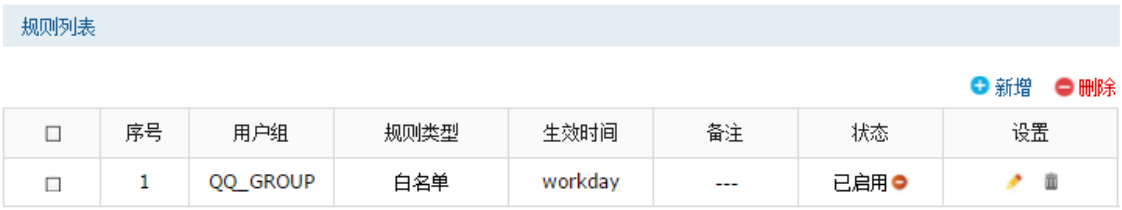


图 4-55 方法二步骤二设置完成示意图

4.7.2 网址过滤

4.7.2.1 网站分组

可以在此对网站进行分组，以便设置网站过滤规则。

界面进入方法：行为管控 >> 网址过滤 >> 网站分组

图 4-56 网站分组设置界面

点击<新增>按钮，可新增一个网站分组

界面项说明：

- **网站分组列表**

组名称 输入一个名称来标识一个网站组，可以输入1-28个字符。

组成员 在此输入网站分组成员。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“*”只允许输入在域名最前面，而不能夹杂在域名中间或后面。可以同时输入多个网站进行批量添加，通过使用空格、逗号或者回车换行来表示不同的网站。每组最多可以输入200个网站。

文件路径 可以通过上传txt文件添加组成员，txt文件内容需按照组成员添加的格式进行编辑，上传完成后，文件内容将显示在组成员文本框中。

备注	填写必要的备注信息，允许留空

在网站分组列表中，可以对已保存的网站分组进行相应设置。路由器预定义了部分网站分组，可以在此查看、编辑。

4.7.2.2 网站过滤

可以在此对不同的用户组设置网站过滤规则，限制不同用户、不同时间登录的网站，同时，可以将用户登录网站的情况，记录到系统日志。还可以设置当用户登录禁止的网站时，弹出警告或者重定向至所设网站。

界面进入方法：行为管控 >> 网址过滤 >> 网站过滤

图 4-57 网站过滤设置界面

点击<新增>按钮，可新增一条过滤规则

界面项说明：

- **功能设置**

  勾选“启用网站过滤功能”后，网站过滤的相关设置才会生效。

- **规则列表**

受控地址组	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**4.4.1地址管理**
规则类型	选择允许或禁止访问下列网站分组。
选择网站	可以选择“所有网站”，使规则对任意网站生效；也可以选择并且点击<网站分组>，在弹出的选择框中对已有的网站分组进行勾选。如需新建网站分组，请参考**4.7.2.1 网站分组**。
规则生效时间	设置规则的生效时间。由时间管理的时间组来表示。如需新建时间组，请参考**4.4.2 时间管理**。
备注	添加对本条规则的说明信息。
添加到指定位置	勾选该项后，可以将当前设置的访问规则添加到规则列表中指定序号的位置。默认情况下，新增规则显示在规则列表的最后。规则条目在规则列表中的位置越靠前，即规则序号数字越小，该规则优先级越高。
状态	选择启用或禁用本条规则。

在规则列表中，可以对已保存的规则进行相应设置。

图 4-57序号1规则的含义：对用户组“TPLINK_A”内的主机进行了网站过滤，过滤规则是禁止访问网站分组，在时间组“Any”设置的时间段内网站过滤生效。该规则已启用。

说明：

网站过滤、URL过滤及网页安全三个功能可以同时工作，但当三个功能设置有冲突时，路由器执行的优先顺序为：URL过滤 > 网页安全 > 网站过滤。当访问请求可以匹配优先级高的规则，并被“允许”通过时，将跳过后续的网址匹配功能检查。

4.7.2.3 URL过滤

URL（Uniform Resource Locator，统一资源定位符），即广域网中标识资源位置的网络地址。URL过滤能够实现对广域网网址的过滤，方便对局域网访问广域网的通信进行管理。

界面进入方法：行为管控 >> 网址过滤 >> URL过滤

图 4-58 URL过滤设置界面

界面项说明：

- **功能设置**

  勾选“启用URL地址过滤功能”，URL过滤的相关设置才会生效。

➢ **URL过滤规则列表**

受控地址组	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**4.4.1 地址管理**。
策略类型	选择允许或禁止访问下列的URL地址。 允许访问下列的URL地址：表示路由器将允许在URL过滤表中的URL地址数据包通过，而不受其他应用管理的限制。 禁止访问下列的URL地址：表示路由器将禁止在URL过滤表中的URL地址数据包通过。
过滤方式	选择一种过滤方式。“关键字”过滤即所有包含指定字符的URL地址全都进行过滤；“完整URL”过滤则仅当URL地址完全匹配输入的完整URL地址时才能进行过滤。 可以同时输入多个关键字或完整URL进行批量添加，通过使用空格、逗号或者回车换行来表示不同的关键字或完整URL。最多可以添加10个关键字或完整URL，每一个关键字或完整URL的可输入长度为1-64个字符，但输入的总字符数不能超过300个（包括相邻两条关键字或URL地址之间的分隔符）。
过滤内容列表	当过滤方式为“关键字”的时候，可在此输入指定的关键字字符。 当过滤方式为“完整URL”的时候，可在此输入完整的广域网URL地址。
规则生效时间	设置规则的生效时间。由时间管理的时间组来表示。如需新建时间组，请参考**4.4.2 时间管理**。
状态	选择启用或禁用本条规则。
备注	添加对本条规则的说明信息。
添加到指定位置	勾选该项后，可以将当前设置的访问规则添加到规则列表中指定序号的位置。默认情况下，新增规则显示在规则列表的最后。规则条目在规则列表中的位置越靠前，即规则序号数字越小，该规则优先级越高。

在规则列表中，可以对已保存的规则进行相应设置。

图 4-58序号1规则的含义：用户组“TPLINK_A”内的主机，在时间组“Any”设置的时间段内，禁止访问带“360buy.com”字符的所有网站。该规则已启用。

应用举例

某企业希望任何时间都禁止局域网内的主机访问网站：www.baidu.com以及sina。

可以通过设置URL过滤实现此需求。需要设置完整URL过滤“www.baidu.com”，以及关键字过滤“sina”，设置完成后点击<新增>按钮保存生效。

设置完成后的规则如下：

URL过滤规则列表

新增 删除

	序号	受控地址组	策略类型	过滤方式	过滤内容列表	生效时间	状态	备注	设置
☐	1	IPGROUP_LAN	禁止	完整URL	www.baidu.com	Any	已启用	---	
☐	2	IPGROUP_LAN	禁止	关键字	sina	Any	已启用	---	

图 4-59 URL过滤应用设置完成示意图

4.7.3 网页安全

可以在此对不同的用户组设置网页安全规则，限制不同用户、不同时间可进行的网页操作。可以直接禁止所有的HTTP POST提交，使得所有页面上的请求按钮失效，点击页面链接，不会有页面返回。也可以针对网页请求中的文件类型，例如：exe、java、htm等，限制用户网页操作。

界面进入方法：行为管控 >> 网页安全 >> 网页安全

图 4-60 网页安全设置界面

界面项说明：

- **全局设置**

  勾选“启用网页安全功能”后，网页安全的相关设置才会生效。

- **规则列表**

受控地址组	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**4.4.1 地址管理**。
禁止网页提交	勾选“启用”，可以禁止所有的HTTP POST提交。

过滤文件扩展类型	可以在过滤文件扩展类型编辑框内输入多个扩展名，并以空格、逗号或者回车换行来分隔。
生效时间	设置规则的生效时间。由时间管理的时间组来表示。如需新建时间组，请参考**4.4.2 时间管理**。
备注	添加对本条规则的说明信息。
状态	选择启用或禁用本条规则。

在规则列表中，可以对已保存的规则进行相应设置。

图 4-60序号1规则的含义：对用户组“IPGROUP_ANY”内的主机设置了网页安全，组内所有主机在“Any”设置的时间段内，都不能访问扩展类型为exe的网页。该规则已启用。

4.7.4 策略库升级

可以在此进行应用特征数据库的升级。

界面进入方法：行为管控 >> 策略库升级 >> 策略库升级

图 4-61 策略库升级界面

应用特征数据库即“应用控制”界面限制列表中的所有应用，请在我司官方网站下载最新数据库，点击<浏览>按钮，选择保存路径下的文件，点击<导入>进行数据库升级。

4.8 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。

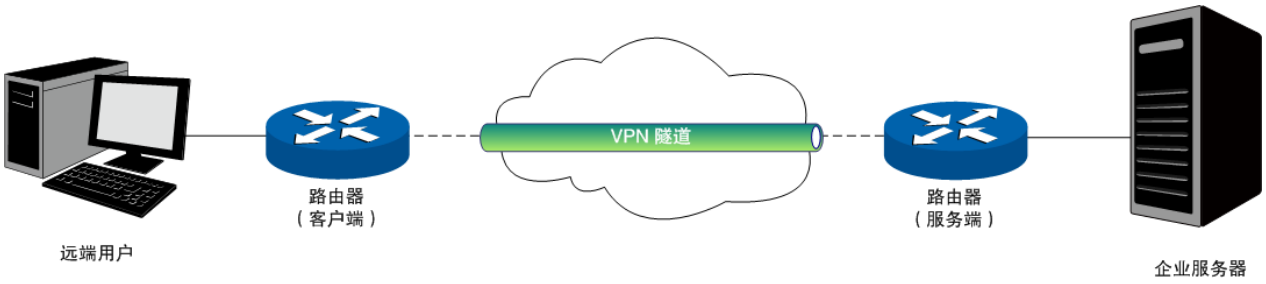


图 4-62 VPN典型拓扑

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-WVR1300G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。

4.8.1 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，鉴别首部）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。

4.8.1.1 IPSec安全策略

界面进入方法：VPN >> IPSec >> IPSec安全策略

图 4-63 IPSec安全策略设置界面

界面项说明：

- **IPSec安全策略列表**

策略名称	为IPSec安全策略命名。
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	设定本地子网地址，以子网掩码值划分地址范围。
对端子网范围	设定对方子网地址，以子网掩码值划分地址范围。
预共享密钥	设置通信双方互相认证的密钥，双方必须使用同一个预共享密钥。
状态	选择是否启用当前策略条目。
高级配置	点击此项，将展开IPSec安全策略的高级参数配置项。
阶段 1 设置	
安全提议	IKE协商方式下指定相应的IPSec安全提议。 阶段1的安全提议由以下验证算法，加密算法和DH组组合而成。 路由器支持以下验证算法： MD5（Message Digest Algorithm，消息摘要算法）：对一段消息产生128bit的消息摘要，防止消息被篡改。 SHA1（Secure Hash Algorithm， 安全散列算法）：对一段消息产生160bit的消息摘要，比MD5更难破解。 路由器支持以下加密算法： DES（Data Encryption Standard， 数据加密标准）：使用56bit的密钥对64bit数据进行加密，64bit的最后8位用于奇偶校验。3DES则为三重DES，使用三个56bit的密钥进行加密。 AES（Advanced Encryption Standard，高级加密标准）：AES128/192/256表示使用长度为128/192/256 bit的密钥进行加密。

DH组：Diffie-Hellman算法的组信息，用于产生加密IKE隧道的会话密钥。DH1/2/5分别对应着768/1024/1536 bit的DH组。

交换模式

设置IKE第一阶段协商的交换模式，该交换模式必须与对端相同。交换模式有以下两种：

主模式（Main mode）：该模式双方交换报文多，提供身份保护，适用于对身份保护要求较高的场合。

野蛮模式（Aggressive mode）：又称主动模式，该模式不提供身份保护，双方交换报文少，协商速度快，适用于对身份保护要求不高的场合。

协商模式

设置IKE协商的模式，该协商模式不必与对端相同。协商模式有以下两种：

初始者模式（Initiator mode）：配置该模式后，IKE才能主动发起协商。

响应者模式（Responder mode）：配置该模式后，IKE不会主动发起协商，需要等待对端发起协商。

本地/对端 ID 类型

设置本地和对端的ID（Identity，身份标识）类型，用于进行ID的交换与验证，可以选择“IP地址”或“NAME”，通信双方的设置需保持一致。

本地/对端 ID

ID类型选择“IP地址”时，无需进行设置；ID类型选择“NAME”时，可自定义本地/对端的ID。路由器的“本地ID”需与通信对端的“对端ID”保持一致，而“对端ID”则需与通信对端的“本地ID”保持一致。

生存时间

设定IPSec SA的生存时间。

DPD 检测开启

DPD（Dead Peer Detect，对端存活检测）开启后，IKE一端能够定时主动检测对端的在线状态。

DPD 检测周期

当开启DPD检测时可设置检测周期。

阶段 2 设置

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。

安全提议

指定相应的IPSec安全提议。点击加号（+）添加安全提议，点击（-）删除该安全提议。

阶段2和手动模式下的安全提议由以下验证算法和加密算法组合而成。

当选择AH安全协议时可设定AH验证算法。路由器支持两种AH验证算法：

MD5（Message Digest Algorithm，消息摘要算法）：对一段消息产生128bit的消息摘要，防止消息被篡改。

SHA1（Secure Hash Algorithm，安全散列算法）：对一段消息产生160bit的消息摘要，比MD5更难破解。

当选择ESP安全协议时可设定ESP验证算法。路由器支持两种ESP验证算法：

MD5（Message Digest Algorithm，消息摘要算法）：对一段消息产生128bit的消息摘要，防止消息被篡改。

SHA1（Secure Hash Algorithm，安全散列算法）：对一段消息产生160bit的消息摘要，比MD5更难破解。

当选择ESP安全协议时可设定ESP加密算法。路由器支持两种ESP加密算法：

DES（Data Encryption Standard，数据加密标准）：使用56bit的密钥对64bit数据进行加密，64bit的最后8位用于奇偶校验。3DES则为三重DES，使用三个56bit的密钥进行加密。

AES（Advanced Encryption Standard，高级加密标准）：AES128/192/256表示使用长度为128/192/256bit的密钥进行加密。

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

设定IPSec SA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。

说明

子网掩码值的相关设置请参考附录A 常见问题中的**问题5**。

4.8.1.2 IPSec安全联盟

在此将列出路由器上所有已成功建立的IPSec安全联盟相关信息。

界面进入方法：VPN >> IPSec >> IPSec安全联盟

IPSec安全联盟列表

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_1	337435911 9	in	192.168.10.100<-172.29.85.199	192.168.1.0/24:0<-192.168.0.0/24:0,any	ESP	---	MD5	3DES
2	IPsec_1	781159572	out	192.168.10.100->172.29.85.199	192.168.1.0/24:0->192.168.0.0/24:0,any	ESP	---	MD5	3DES

刷新 搜索 帮助

图 4-64 IPSec安全联盟界面一

在图 4-64中路由器使用eth2接口进行隧道连接，eth2接口的IP地址为192.168.10.100，对端网关地址为172.29.85.199。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图 4-65所示，SPI值为IKE自动协商得出。

IPSec安全联盟列表

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_2	781159572	in	172.29.85.199<-192.168.10.100	192.168.0.0/24:0<-192.168.1.0/24:0,any	ESP	---	MD5	3DES
2	IPsec_2	337435911 9	out	172.29.85.199->192.168.10.100	192.168.0.0/24:0->192.168.1.0/24:0,any	ESP	---	MD5	3DES

刷新 搜索 帮助

图 4-65 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-WVR1300G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。

4.8.2 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。

4.8.2.1 L2TP 服务器

界面进入方法：VPN >> L2TP >> L2TP服务器

图 4-66 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	选择服务器的接口
IPSec 加密	选择加密类型，可选择“加密”、“不加密”、“可选加密”，当选择“加密”或“可选加密”类型时，需填写预共享密钥。
状态	选择是否启用本L2TP服务器。

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。

4.8.2.2 L2TP客户端

界面进入方法：VPN >> L2TP >> L2TP客户端

图 4-67 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。

- **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	选择是否启用本L2TP客户端。
参与流量均衡	选择是否参与流量均衡控制。

- **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。

4.8.2.3 L2TP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 4-68 L2TP服务器隧道信息界面

图 4-68中显示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。

4.8.3 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。

4.8.3.1 PPTP服务器设置

界面进入方法：VPN >> PPTP >> PPTP服务器设置

图 4-69 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	选择服务器的接口
MPPE 加密	选择加密类型，可选择“加密”、“不加密”，当选择“加密”类型时，需填写预共享密钥。
状态	选择是否启用本PPTP服务器。

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。

4.8.3.2 PPTP客户端设置

界面进入方法：VPN >> PPTP >> PPTP客户端

图 4-70 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**

隧道名称	设置PPTP隧道的名称
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	设置客户端出接口。
服务器地址	设置PPTP隧道的服务器地址。
MPPE 加密	选择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	选择PPTP客户端的工作模式，可选择“NAT”或“路由”模式。
状态	选择是否启用本PPTP客户端。
参与流量均衡	选择是否参与流量均衡控制。

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。

4.8.3.3 PPTP服务器隧道信息

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

隧道信息列表

刷新

序号	用户名	服务器/客户端	隧道名称	虚拟本地IP	接入服务IP	对端虚拟IP	DNS
1	tpuser_pptp	客户端	TPLINK_PPTP	10.10.10.59	172.33.1.10	60.60.60.60	6.6.6.6

图 4-71 PPTP服务器隧道信息界面

图 4-71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。

4.8.4 用户管理

在此界面上配置 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 4-72 VPN用户管理界面

界面项说明：

- **VPN用户管理规则列表**

用户名	允许拨入的用户名称。
密码	用户名称对应的密码。
服务类型	L2TP：本用户只用于L2TP；PPTP：本用户只用于PPTP；自动：本用户既可用于L2TP也可用于PPTP。
本地地址	VPN隧道的本地虚拟IP地址。

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。当用户类型为auto时，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。

4.9 认证管理

4.9.1 认证设置

千兆企业 VPN 路由器系列产品提供 Web 认证和微信连 Wi-Fi 两种认证方式，同时支持免认证策略，可在此页面下进行设置。

4.9.1.1 Web 认证

界面进入方法：认证管理 >> 认证设置 >>Web 认证

Web 认证分为三种认证方式，可在此页面下进行设置。

图 4-73 Web认证设置界面

界面项说明：

- **功能设置**

  状态　　勾选此项以启用Web认证功能。

- **Web认证参数设置**

  认证页面　　选择由系统生成的自定义页面或者由外部的链接进行认证。

  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　　显示在自定义认证页面的欢迎信息。

  版权声明　　显示在自定义认证页面的版权声明信息。

  页面预览　　预览用于提醒用户到期的页面。

  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。

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。

1) 如果认证方式为“本地认证”，可开启到期提醒功能，启用后需填写如下内容：

图 4-74 本地认证设置界面

开始提醒时间 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。

周期提醒间隔 提醒用户认证到期的时间间隔

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。

2) 如果认证方式为“radius认证”，需填写如下内容：

图 4-75 radius认证设置界面

主服务器地址 选择 radius 认证时，主 radius 服务器地址必须填写。

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 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 设置 radius 认证方式，分为 PAP 和 CHAP 两种。

3) 如果认证方式为“一键上网”，需填写如下内容：

图 4-76 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。

说明

不能同时开启Web和微信连Wi-Fi服务。

4.9.1.2 微信连 Wi-Fi

界面进入方法：认证管理 >> 认证设置 >> 微信连 Wi-Fi

图 4-77 微信连 Wi-Fi 设置界面

界面项说明：

- **功能设置**

  状态 选择是否启用微信连 Wi-Fi 功能。

- **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。

- **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<设置>按钮使其生效。

4.9.1.3 免认证策略

界面进入方法：认证管理 >> 认证设置 >> 免认证策略

免认证策略分为三种认证方式，可在此页面下进行设置。

图 4-78 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 4-79 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 4-80 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。

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。

4.9.2 用户管理

4.9.2.1 用户管理

界面进入方法：认证管理 >> 用户管理 >> 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。

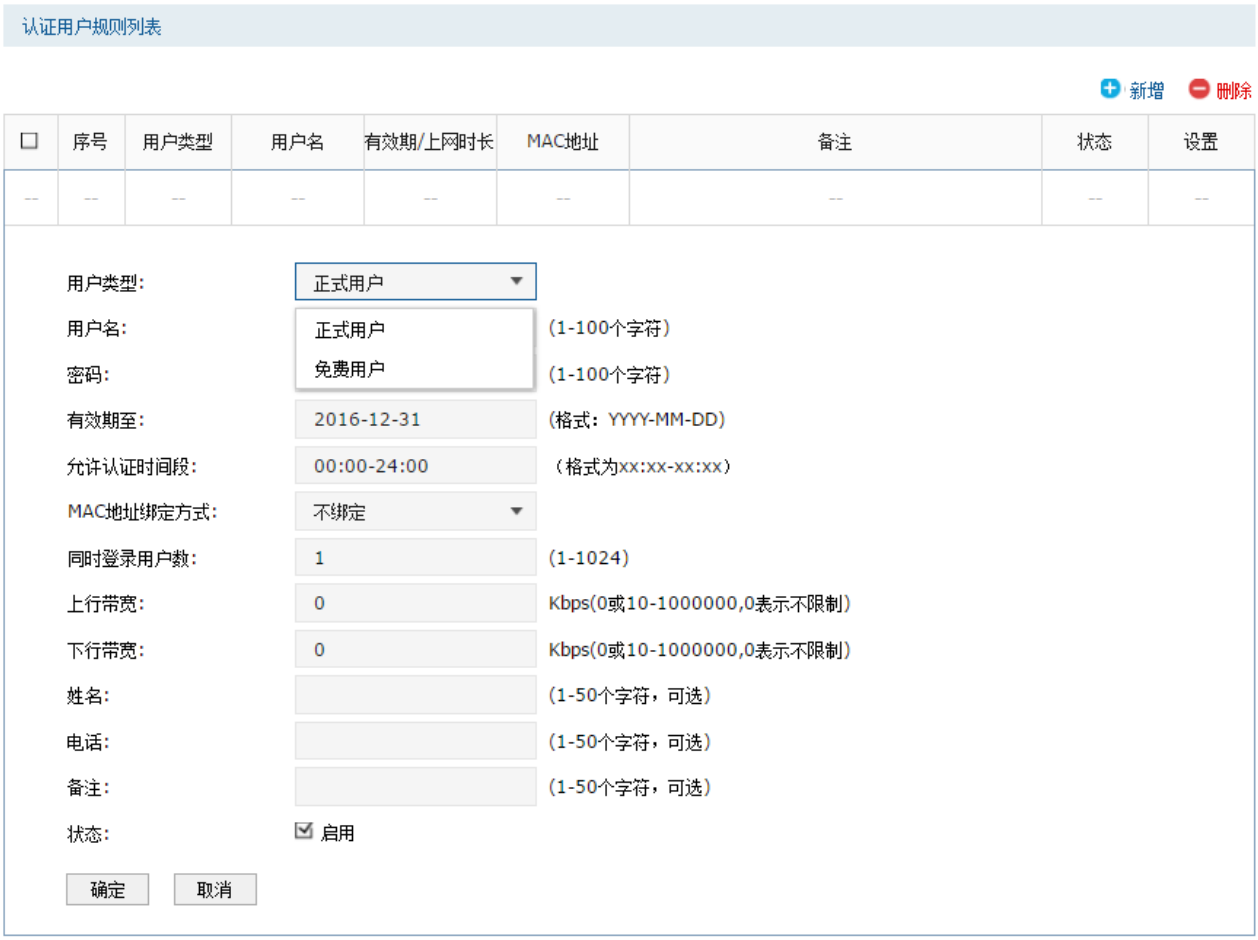


图 4-81 用户管理设置界面

界面项说明：

- **认证用户规则列表**

用户类型	手动刷新认证用户列表。 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 4-82 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。

同时登录的用户数	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 Kbps 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 Kbps 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	是否启用当前用户规则。

2) 若选择用户类型为“免费用户”，需配置以下内容：

图 4-83 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。
同时登录的用户数	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 Kbps 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 Kbps 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	是否启用当前用户规则。

4.9.2.2 用户配置备份

界面进入方法：认证管理 >> 用户管理 >> 用户配置备份

图 4-84 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。

4.9.3 认证状态

可以在该页面下查看认证状态。

4.9.3.1 认证状态

界面进入方法：认证管理 >> 认证状态 >> 认证状态

图 4-85 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

点击<下线>可批量断开用户连接。

4.10 系统服务

4.10.1 PPPoE服务器

通过PPPoE服务器可以为局域网用户分配账号、IP地址，简化用户的配置操作的同时也加强了路由器对局域网用户的管理功能。

4.10.1.1 全局设置

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：系统服务 >> PPPoE服务器 >> 全局设置

图 4-86 全局设置界面

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DNS服务器地址	请正确填写，作为 DNS 服务器地址，缺省为空。
备用DNS服务器地址	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。

4.10.1.2 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：系统服务 >> PPPoE服务器 >> 账号管理

图 4-87 账号管理设置界面

界面项说明：

- **账号列表**

在账号列表中，可以对已保存的账号进行相应设置。

- **账号设置**

账号 账号规则设置的名称。

密码 设置账号密码。

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。
定时断线设置	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。

4.10.1.3 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：系统服务 >> PPPoE服务器 >> 例外IP管理

图 4-88 例外IP管理设置界面

界面项说明：

- **例外IP列表**

  在例外IP列表中，可以对已保存的条目进行相应设置。

- **例外IP设置**

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。

4.10.1.4 账号信息列表

界面进入方法：系统服务 >> PPPoE服务器 >> 账号信息列表

图 4-89 账号信息列表界面

图 4-89中显示的是PPPoE用户账户相关连接信息。点击单个条目后方的“ ”按钮可以断开当前账号的连接，如果需要断开所有已连接的账号，可以点击列表下方的<断开全部>按钮。

4.10.2 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。

4.10.2.1 花生壳动态域名

界面进入方法：系统服务 >> 动态 DNS >> 花生壳动态域名

图 4-90 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/域名	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	选择是否启用花生壳动态域名服务。

4.10.2.2 科迈动态域名

界面进入方法：系统服务 >> 动态 DNS >> 科迈动态域名

图 4-91 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/域名	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。

4.10.2.3 3322动态域名

界面进入方法：系统服务 >> 动态 DNS >> 3322 动态域名

图 4-92 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。
域名信息	显示当前登录的DDNS用户所拥有的域名。用户可以申请多个域名，点击“查看所有域名”显示当前用户申请的所有域名，但最多显示16条。
状态	选择启用或禁用3322动态域名服务。

4.10.3 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：系统服务 >> UPnP >> UPnP

图 4-93 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。

  启用/禁用服务　　选择启用或禁用UPnP服务。

- **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。

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。

4.11 系统工具

4.11.1 管理账号

4.11.1.1 管理账号

在此可以修改登录时使用的用户名和密码。

界面进入方法：系统工具 >> 管理账户 >>管理账号

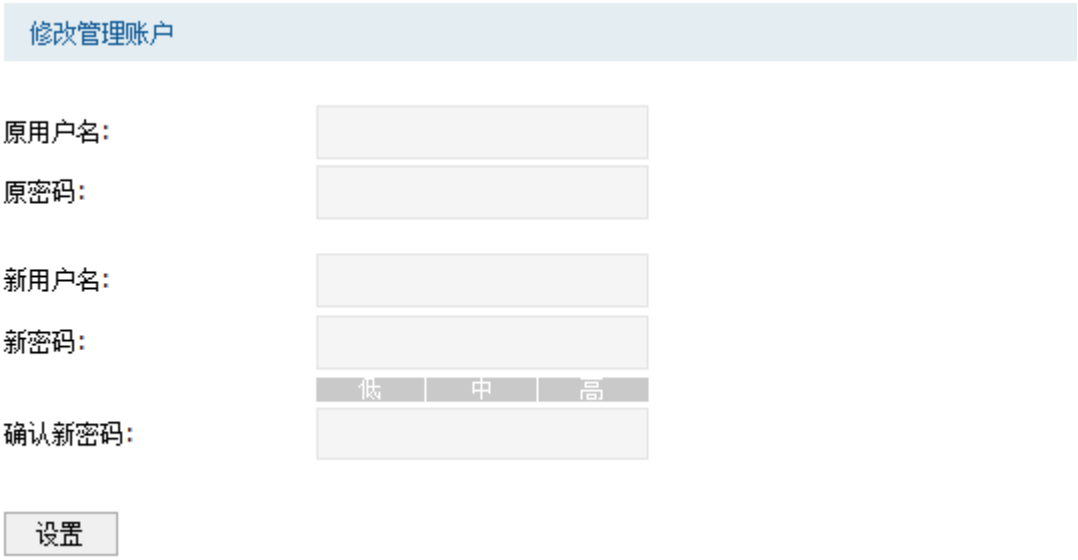


图 4-94 修改管理账号界面

界面项说明：

- **用户名密码修改**

原用户名	本次登录路由器的用户名。
原密码	本次登录路由器使用的密码。
新用户名	重新设置登录路由器的用户名。
新密码	重新设置登录路由器的密码。
确认新密码	再次输入新密码。

说明

更改用户名及密码并保存生效后，后续登录时请使用新用户名及新密码。用户名和密码最多支持 31 个字符，且只能是“_”和“-”字符与数字和字母，区分大小写。

4.11.1.2 远程管理

可以在远程管理界面对允许远程登录的IP地址范围进行设置和修改。

界面进入方法：系统工具 >> 管理账号 >> 远程管理

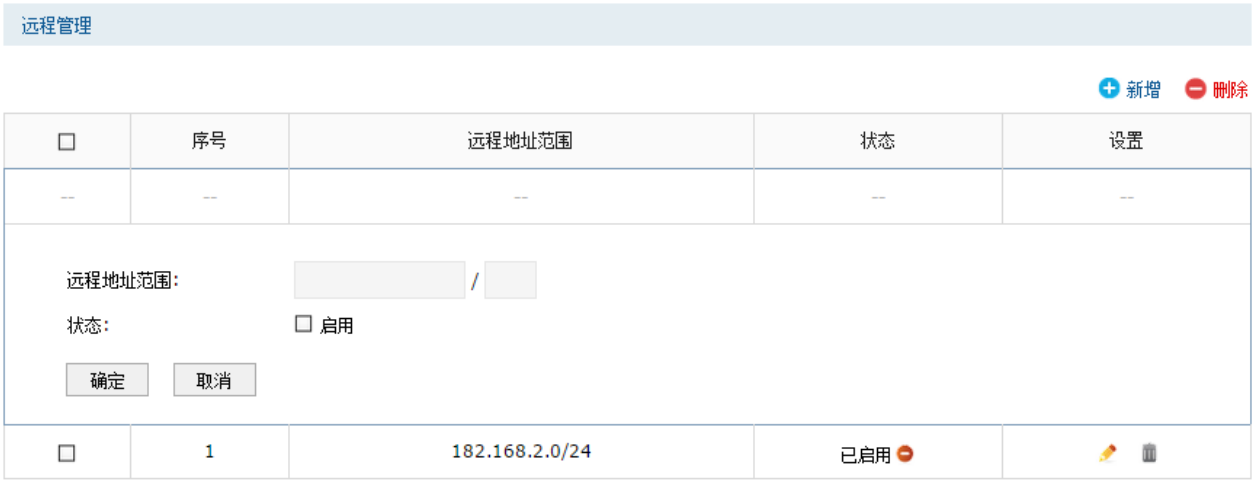


图 4-95 远程管理设置界面

界面项说明：

➢ **远程管理**

远程地址范围	设置需要从外部网络登录路由器的主机地址，可指定单个IP或一个网段。
状态	选择是否启用该规则。

在远程管理列表中，可以对已保存的远程管理地址条目进行相应设置。

图 4-95 远程管理设置界面中序号1条目的含义：允许IP地址属于182.168.2.0/24网段的主机登录路由器Web界面，该规则已启用。

4.11.1.3 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 >>管理账号>> 系统管理设置

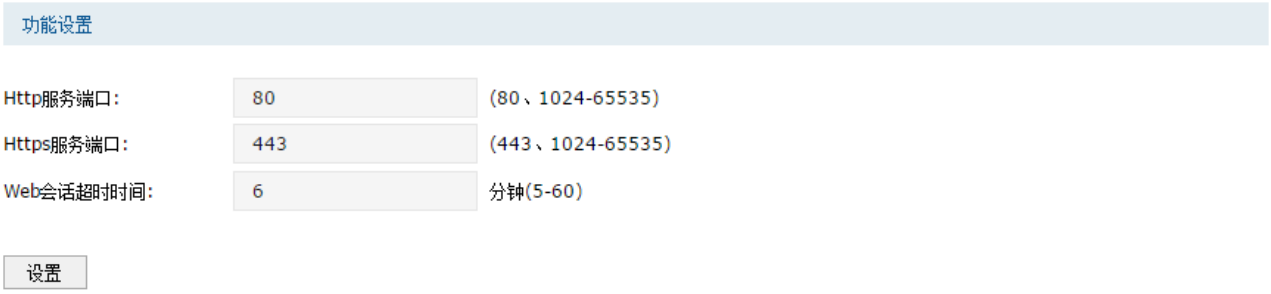


图 4-96 系统管理设置界面

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。
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。

说明：

- 路由器默认的 Web 服务端口为 80。如果改为其它值，在局域网或广域网都必须用“http://IP 地址:端口”的方式才能登录路由器。例如，将 Web 管理端口更改为 88，在局域网内登录时的 URL 地址应为 http://192.168.1.1:88。
- 设置超时时间后，新的超时时间将在下一次登录时生效。

应用举例：

某企业路由器WAN口地址为210.10.10.50，为方便管理，希望广域网210.10.10.0/24网段的IP地址能对路由器进行远程管理。

可以通过设置Web服务器实现此需求。首先需要设置远端访问路由器的地址段，并选择启用该访问规则，系统工具>>管理账号>>远程管理中设置，如图 4-97所示：

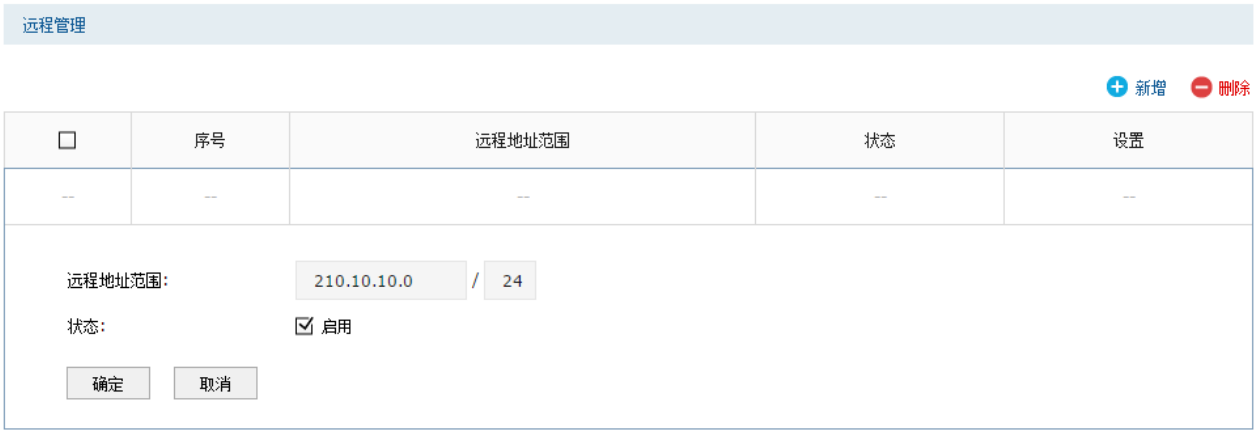


图 4-97 系统管理设置应用-远程管理

在服务端口界面为Web服务器开放相应的服务端口，在系统工具>>管理账号>>系统管理设置中进行设置，如图 4-93所示：

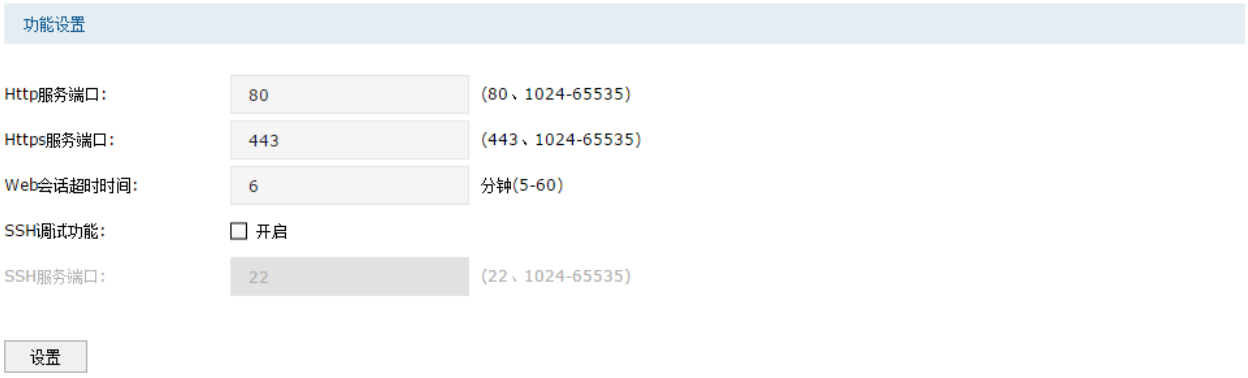


图 4-98 系统管理设置应用-系统管理设置

在浏览器地址栏输入路由器地址210.10.10.50登录路由器Web界面。

4.11.2 设备管理

4.11.2.1 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

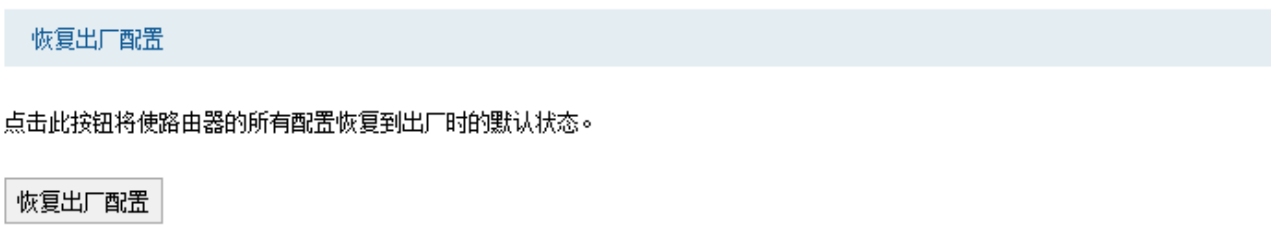


图 4-99 恢复出厂配置界面

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。

恢复出厂配置后，当前的配置信息将会丢失。如果您想保留当前配置，请注意备份。恢复出厂配置后，路由器将自动重启。

路由器出厂默认LAN口IP地址为192.168.1.1。

4.11.2.2 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 4-100 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。

4.11.2.3 重启路由器

界面进入方法：系统工具 >> 设备管理 >> 重启路由器

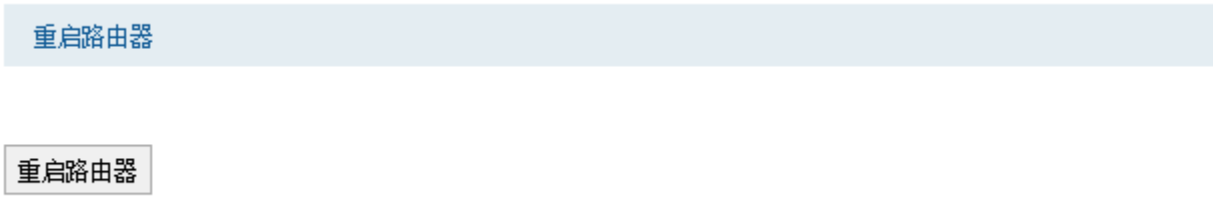


图 4-101 重启路由器界面

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。

4.11.2.4 软件升级

界面进入方法：系统工具 >> 设备管理 >> 软件升级

图 4-102 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）会不定期更新千兆企业VPN路由器系列产品的软件升级文件，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。

4.11.3 诊断工具

4.11.3.1 诊断工具

您可以通过诊断工具来检测和诊断当前的网络状况。

界面进入方法：系统工具 >> 诊断工具 >> 诊断工具

图 4-103 诊断工具界面

界面项说明：

- **诊断工具列表**

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。 路由跟踪检测。
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通信检测**

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。

- **路由跟踪检测**

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。

4.11.3.2 故障诊断

您可以通过诊断工具来检测和诊断当前的网络状况。

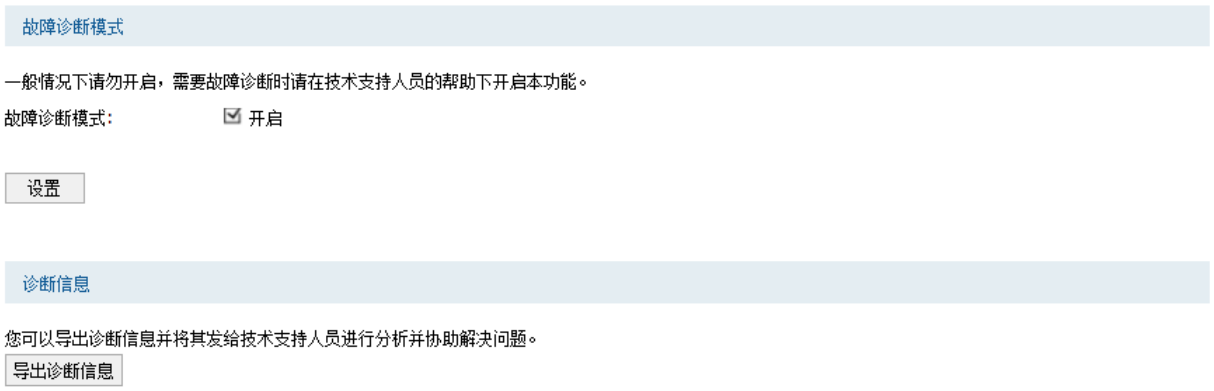


图 4-104 故障诊断界面

界面项说明：

- **故障诊断模式**

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。

- **诊断信息**

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。

4.11.4 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 4-105 时间设置-通过网络获取系统时间

图 4-106 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	设置路由器系统时间的方式，分为通过网络获取系统时间和手动设置系统时间，其中手动设置系统时间也可以通过获取管理主机时间的方式进行设置。
通过网络获取系统时间	选中<通过网络获取系统时间>，路由器将通过网络获取 GMT 时间。 时区：路由器所在的时区。 首选/备用 NTP 服务器：您可以自行指定 NTP 服务器地址。
手动设置系统时间	选中<手动设置系统时间>，您可以通过手动输入的方式来设置路由器日期和时间。
获取管理主机时间	点击<获取管理主机时间>，系统将获取当前管理主机的时间并路由器的系统时间设置为该时间。

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。

4.11.5 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 4-107 日志界面

日志设置区可以对日志系统进行简单的配置。启用自动刷新后，日志列表将每隔5秒刷新一次；选择日志等级可使日志列表中仅列出指定等级的日志记录。

各等级描述：

所有等级 显示所有的

致命错误 导致系统不可用的错误，红色显示。

紧急错误 必须对其采取紧急措施的错误，红色显示。

严重错误 导致系统处于危险状态的错误，红色显示。

一般错误 一般性的错误提示，橙色显示。

警告信息 系统仍然正常运行，但可能存在隐患的提示信息，橙色显示。

通知信息 正常状态下的重要提示信息。

消息报告 一般性的提示信息。

调试信息	调试过程产生的信息。

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：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	POP3（Post Office Protocol 3）	邮局协议第3版本	规定了将个人计算机连接到互联网的邮件服务器和下载电子邮件的方法的一种协议。
	Port VLAN	基于端口的VLAN	基于同一路由器端口划分的VLAN，即不可以跨越路由器划分VLAN。
	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）。
S	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。
	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。
T	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。
	TCP-SYN（SYNchronous）	同步	TCP首部中的同步序号标志。

	英文术语	中文名称	定义或描述
T	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 Network protocol）	远程终端协议	是在TCP/IP网络上，标准的提供远程登录功能的应用。
	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。
U	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。
V	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。
W	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。
	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。
	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

TL-R483G技术规格参数

参数项		参数内容
支持的标准和协议		IEEE 802.3、IEEE 802.3u、IEEE 802.3ab、IEEE 802.3x 、TCP/ IP、DHCP、ICMP、NAT、PPPoE、SNTP、HTTP、DNS、L2TP、PPTP、IPSec
端口	LAN口	1个10/100/1000M自适应RJ45端口(Auto MDI/MDIX)
	WAN口	1个10/100/1000M自适应RJ45端口(Auto MDI/MDIX)
	WAN/LAN口	3个10/100/1000M自适应RJ45端口(Auto MDI/MDIX)
网络介质		10BASE-T：3类或以上UTP/STP（≤100m）
		100BASE-TX：5类或以上UTP/STP（≤100m）
		1000BASE-T：超5类或以上UTP/STP（≤100m）
LED指示灯	LAN/WAN口	Link/Act（连接/工作）
	其它	SYS（系统状态）
散热方式		自然散热
使用环境		工作温度：0ºC ~ 40ºC
		存储温度：-40ºC ~ 70ºC
		工作湿度：10% ~ 90%RH 不凝结
		存储湿度：5% ~ 90%RH 不凝结
电源输入		100-240V~ 50/60Hz 0.2A

TL-R478G+技术规格参数

参数项		参数内容
支持的标准和协议		IEEE 802.3、IEEE 802.3u、IEEE 802.3ab、IEEE 802.3x、TCP/ IP、DHCP、ICMP、NAT、PPPoE、SNTP、HTTP、DNS、L2TP、PPTP、IPSec
端口	LAN口	1个10/100/1000M自适应RJ45端口(Auto MDI/MDIX)
	WAN口	1个10/100/1000M自适应RJ45端口(Auto MDI/MDIX)
	WAN/LAN口	3个10/100/1000M自适应RJ45端口(Auto MDI/MDIX)
网络介质		10BASE-T：3类或以上UTP/STP（≤100m）
		100BASE-TX：5类或以上UTP/STP（≤100m）
		1000BASE-T：超5类或以上UTP/STP（≤100m）
LED指示灯	LAN/WAN口	Speed/Link/Act（连接状态）、WAN/LAN（接口状态）
	其它	PWR（电源）、SYS（系统状态）
散热方式		自然散热
使用环境		工作温度：0ºC ~ 40ºC
		存储温度：-40ºC ~ 70ºC
		工作湿度：10% ~ 90%RH 不凝结
		存储湿度：5% ~ 90%RH 不凝结
电源输入		100-240V~ 50/60Hz 0.2A

TL-R4239G技术规格参数

参数项		参数内容
支持的标准和协议		IEEE 802.3、IEEE 802.3u、IEEE 802.3ab、IEEE 802.3x、TCP/ IP、DHCP、ICMP、NAT、PPPoE、SNTP、HTTP、DNS、L2TP、PPTP、IPSec
端口	LAN口	1个10/100/1000M自适应RJ45端口(Auto MDI/MDIX)
	WAN口	1个10/100/1000M自适应RJ45端口(Auto MDI/MDIX)
	WAN/LAN口	3个10/100/1000M自适应RJ45端口(Auto MDI/MDIX)
网络介质		10BASE-T：3类或以上UTP/STP（≤100m）
		100BASE-TX：5类或以上UTP/STP（≤100m）
		1000BASE-T：超5类或以上UTP/STP（≤100m）
LED指示灯	LAN/WAN口	Speed/Link/Act（连接状态）、WAN/LAN（接口状态）
	其它	PWR（电源）、SYS（系统状态）
散热方式		自然散热
使用环境		工作温度：0ºC ~ 40ºC
		存储温度：-40ºC ~ 70ºC
		工作湿度：10% ~ 90%RH 不凝结
		存储湿度：5% ~ 90%RH 不凝结
电源输入		100-240V~ 50/60Hz 0.6A