TP-LINK®

企业VPN路由器

TL-ER6110

用户手册

REV2.1.1

1910040361

声明

目录

物品清单

请仔细检查包装盒，里面应有以下配件：

- 一台TP-LINK 企业VPN路由器
- 一根Console连接线
- 一根电源线
- 一本安装手册
- 一张保修卡
- 一张光盘
- 两个L型支架及其他配件

注意：

如果发现有配件短缺或损坏的情况，请及时与当地经销商联系。

第1章 用户手册简介

本手册旨在帮助您正确使用本款路由器。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，

- 所提到的“路由器”、“本产品”等名词，如无特别说明，系指TL-ER6110企业VPN路由器，下面简称为TL-ER6110。
- 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：	该图标提醒您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。介绍本产品特性、应用以及外观。

第3章：配置指南。指导如何登录TL-ER6110的Web管理界面，并简要介绍界面特点。

第4章：功能设置。介绍TL-ER6110的所有功能，帮助您更充分地使用本产品。

第5章：典型配置。以真实的企业网络应用为例，解决实际需求。

第6章：命令行简介。介绍路由器Console口登录方法及配置中常用的CLI命令。

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-ER6110是TP-LINK公司推出的一款高性能企业VPN路由器，具备强大的数据处理能力，并且支持丰富的软件功能，包括VPN、IP/MAC地址绑定、常见攻击防护、访问控制、IP带宽控制、连接数限制、上网行为管理（应用限制/网址过滤/网页安全/行为审计）、电子公告、PPPoE服务器等功能，适合中小型企业、机关单位、酒店、小区等组建安全、高效、易管理的网络。

强大的数据处理能力

采用64位网络专用处理器，128MB DDRII高速内存，数据包处理能力得到大幅提升，可实现LAN、WAN口间数据的线速转发。

支持多种VPN，保障远程接入安全

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服务器模式，允许出差员工或分支结构远程安全接入公司网络。

多种方式管控员工上网行为

支持基本的访问控制列表，可限制包括FTP下载、收发邮件、Web浏览，视频及语音通信等在内的各种网络应用，并支持基于用户组和时间段分配访问控制规则。

支持实时记录企业员工的各类上网行为，并上传至行为审计服务器。网管人员可通过TP-LINK上网行为审计软件对上传至服务器的上网行为数据进行汇总分析。

支持网站过滤和URL过滤，可对员工访问各种网站的权限进行管控，还可以记录其访问历史信息，甚至可以弹出警告页面。支持网站分组功能（出厂默认提供十多种网站分组），可方便地将庞杂的网站进行归类，灵活而实用。

支持禁止网页提交，限制员工登录各种基于网页的论坛、微博、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，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。

全面的攻击防护能力

提供IP与MAC地址自动扫描及一键绑定功能，能够同时绑定LAN口（内网）、WAN口（外网）主机的IP与MAC地址信息，防止内/外网ARP欺骗；支持发送免费GARP包，在遭受ARP欺骗时，可按照指定频率主动发送ARP更正信息，及时恢复网络正常状态。

支持内/外网攻击防护功能，可防范各种常见的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。

支持基于MAC地址的过滤功能，阻断非法主机的接入。

灵活的带宽管理策略

支持普通带宽控制和智能带宽控制两种模式，可根据带宽的实际利用率灵活启用带宽控制策略。支持基于用户组和时间段配置带宽控制策略，并可对内网用户进行上下行双向带宽控制，有效抑制BT、迅雷等P2P应用过度占用带宽，避免造成上网速度慢的问题，保障网络时刻畅通；提供基于用户组的连接数限制功能，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，确保上网、视频语音会议等顺畅进行。

2.2 产品特性

硬件特性

- 采用64位网络专用处理器，主频500MHz；
- 配备容量为128MB的DDRII-533高速内存；
- 提供5个10/100M自适应以太网接口；
- 提供1个硬件DMZ接口；
- 提供1个Console口；
- 内置高品质开关电源，无风扇静音设计；
- 1U钢壳，可安装于19英寸标准机架，工业级设计。

支持协议

- 符合IEEE 802.3、IEEE 802.3u标准；
- 支持AH、ESP、IKE、PPP等协议；
- 支持TCP/IP、DHCP、ICMP、NAT、NAPT等协议；
- 支持PPPoE、SNTP、HTTP、DDNS、UPnP、NTP等协议。

基本功能

- 支持静态IP、动态IP、PPPoE、L2TP、PPTP多种接入方式；
- 支持虚拟服务器、端口触发、ALG、静态路由、RIP动态路由等功能；
- 内置简单管理交换机，支持VLAN设置和端口监控等交换机功能；
- 支持LAN口、WAN口以及DMZ口的MAC地址修改；
- 支持配置文件备份与导入；
- 支持系统日志、日志服务器、流量统计、系统时间设置等功能；
- 支持Web和远程管理，全中文配置界面；
- 提供诊断工具（Ping、Tracert），支持WAN口在线检测功能。

VPN

- 支持基于AH/ESP封装的IPsec VPN，允许建立最多64条VPN隧道；
- 支持MD5、SHA1验证算法和DES、3DES、AES128、AES192、AES256等加密算法；
- 支持IKE协商加密密钥，支持预共享密钥认证，支持DH1/DH2/DH5密钥交换算法；
- 支持L2TP/PPTP VPN，支持服务器与客户端模式。

行为管控

- 支持一键管控IM类、P2P类、金融类、游戏类、代理类等近60种常见上网行为；
- 支持实时记录员工各类上网行为，并上传到行为审计服务器；
- 支持TP-LINK上网行为审计软件；
- 支持网站过滤和URL过滤；
- 支持网站分组功能（出厂默认提供十多种网站分组）；
- 支持网页安全，可禁止网页提交及过滤网页中内嵌的多种文件类型。

系统服务

- 支持PPPoE Server功能，有效管理内网用户上网权限；
- 支持电子公告；
- 支持动态DNS服务。

带宽管理

- 支持基于IP的带宽控制，可限制单机带宽；
- 支持连接数设置，可限制单机连接数。

网络安全

- 内建防火墙，支持URL、MAC地址过滤；
- 支持访问控制，可自定义服务类型；
- 支持攻击防护功能，可对网络攻击和病毒攻击进行防范；
- 支持局域网IP/MAC地址绑定，防范局域网ARP攻击；
- 支持广域网IP/MAC地址绑定，防范广域网ARP攻击；
- 支持定时发送免费ARP包功能，防范局域网ARP欺骗。

2.3 产品外观

2.3.1 前面板

TL-ER6110的前面板由5个10/100M接口、1个Console接口、指示灯和Reset键组成。如图 2-1所示。

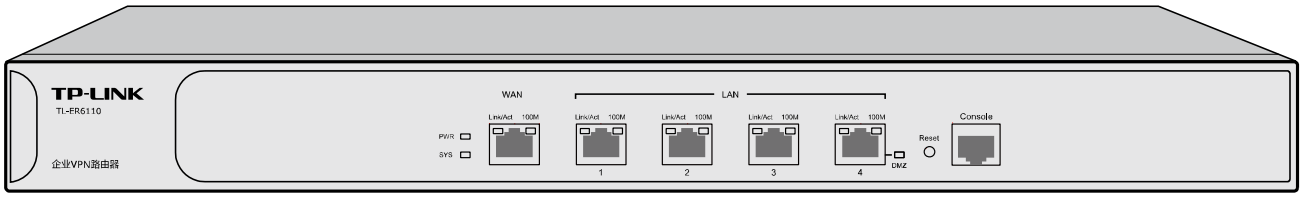


图 2-1 TL-ER6110前面板示意图

- **5个10/100Mbps自适应RJ45接口**

TL-ER6110支持10Mbps/100Mbps带宽的连接设备。每个接口对应一组指示灯，即Link/Act和100M指示灯。

- **1个Console接口**

Console接口位于面板最右边，使用此接口可以对路由器进行命令行配置，详见**第6章命令行简介**。

- **Reset键**

复位键。在路由器通电的情况下，使用尖状物按住路由器的Reset键，等待2-5秒后，见到系统指示灯快速闪烁1-2秒，松开按键，路由器将自动恢复出厂设置并重启。路由器出厂默认管理地址是http://192.168.1.1，默认用户名/密码是admin/admin。

- **指示灯**

指示灯包括电源PWR指示灯，SYS系统指示灯，连接状态Link/Act指示灯，100M速率指示灯，DMZ接口状态指示灯。通过指示灯可以监控路由器的工作状态，下表将详细说明指示灯工作状态：

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
		常灭表示电源关闭或电源故障
SYS	系统指示灯	系统正常工作时以每秒1次的频率闪烁，其他状态表示系统异常
Link/Act	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
		常灭表示相应端口未建立连接

指示灯	名称	状态描述
100M	速率指示灯	常亮表示端口速率为100Mbps
		常灭表示端口速率为10Mbps或者未接入设备
DMZ	DMZ接口状态指示灯	常亮表示DMZ接口已启用
		常灭表示DMZ接口已关闭

2.3.2 后面板

路由器后面板由电源接口和防雷接地柱组成，如图 2-2所示：

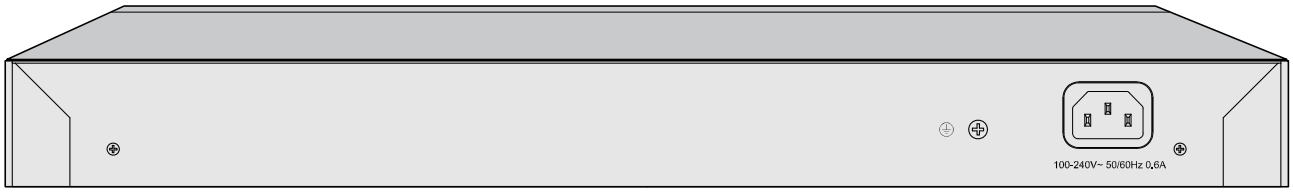


图 2-2 后面板示意图

- **电源接口**

位于后面板右侧，接入电源需为100-240V~ 50/60Hz 0.6A的交流电源。

- **防雷接地柱**

请使用黄绿双色外皮的铜芯导线接地，以防雷击，具体请参考《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 登录Web界面

第一次登录时，需要确认以下几点：

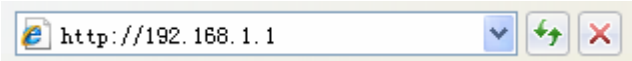
1) 路由器已正常加电启动，任一LAN口已与管理主机相连。

2) 管理主机已正确安装有线网卡及该网卡的驱动程序、并已正确安装IE 7.0或以上版本的浏览器。

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TL-ER6110的Web管理界面。



路由器登录界面如图 3-1所示。

图 3-1 路由器登录界面

在此界面输入路由器管理帐号的用户名和密码，出厂缺省值为admin/admin，点击<登录>按钮。成功登录后将看到路由器的系统状态信息，如图 3-2。

图 3-2 TL-ER6110系统状态

3.2 Web界面简介

3.2.1 界面总览

TL-ER6110路由器典型的Web界面如图 3-3所示。

图 3-3 典型Web界面

在图 3-4 Web界面区域划分中可以看到，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可分为两部分，条目配置区以及列表管理区。

图 3-4 Web界面区域划分

3.2.2 界面常见按钮及操作

- **条目配置区常见按钮**

按钮	含义
保存	保存当前配置信息。
新增	新增当前配置信息。
修改	修改并保存编辑后的配置信息。
清除	快速清除当前配置项中已输入的所有信息。
帮助	打开当前功能的帮助界面。

说明：

<修改>按钮只有当编辑列表中的规则/条目时才会出现，取代原本的<新增>按钮。

- **列表管理区常见按钮**

按钮	含义
全选	选中当前列表中所有规则/条目。
启用	启用选中的规则/条目，可批量操作。
禁用	禁用选中的规则/条目，可批量操作。
生效	使选中的规则/条目生效，可批量操作。

按钮	含义
不生效	使选中的规则/条目不生效，可批量操作。
删除	删除选中的规则/条目，可批量操作。
刷新	刷新列表。

- **列表管理区扩展按钮**

搜索　　按照指定关键字段搜索相应的规则。

列名　　选择当前列表中任一表头字段。

内容　　输入关键字。

状态　　指定搜索范围为“启用”、“禁用”或者任意状态下的规则/条目。

- **列表管理区常见操作**

按钮	名称	含义
	编辑	点击后，需要编辑的规则/条目内容会出现在列表上方的配置管理区，原<新增>按钮同时变为<修改>按钮。在配置管理区修改当前配置后，点击<修改>按钮保存生效。该操作不可批量进行。

按钮	名称	含义
	启用/生效	点击后，修改当前规则/条目状态。该操作不可批量进行。
	禁用/不生效	点击后，修改当前规则/条目状态。该操作不可批量进行。
	删除	点击后，删除当前规则/条目。该操作不可批量进行。

第4章 功能设置

4.1 基本设置

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、各接口配置信息以及系统资源使用情况。

界面进入方法：基本设置 >> 系统状态 >> 系统状态

图 4-1 系统状态界面

4.1.2 系统模式

TL-ER6110路由器可以工作在3种模式下：NAT模式、路由模式和全模式。

若TL-ER6110需要作为网关应用在局域网与广域网之间，拓扑如图 4-2，可以将TL-ER6110系统模式设为NAT模式；

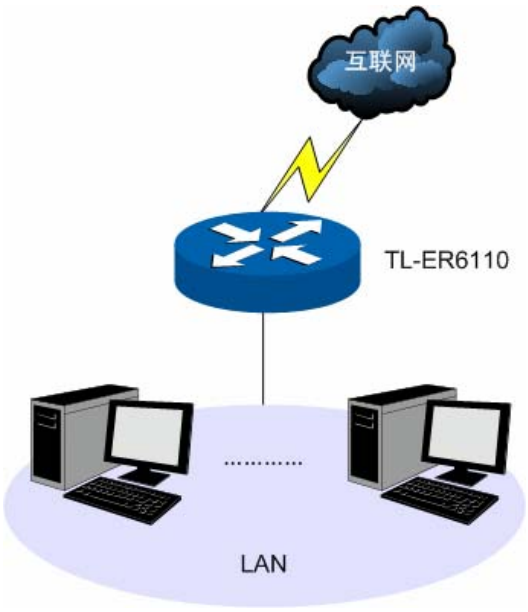


图 4-2 组网拓扑-NAT模式

若TL-ER6110在大型组网内用于连接两个不同区域的网络，这两个区域的主机都必须通过路由规则进行通信，拓扑如图 4-3，可以将TL-ER6110系统模式设为路由模式；

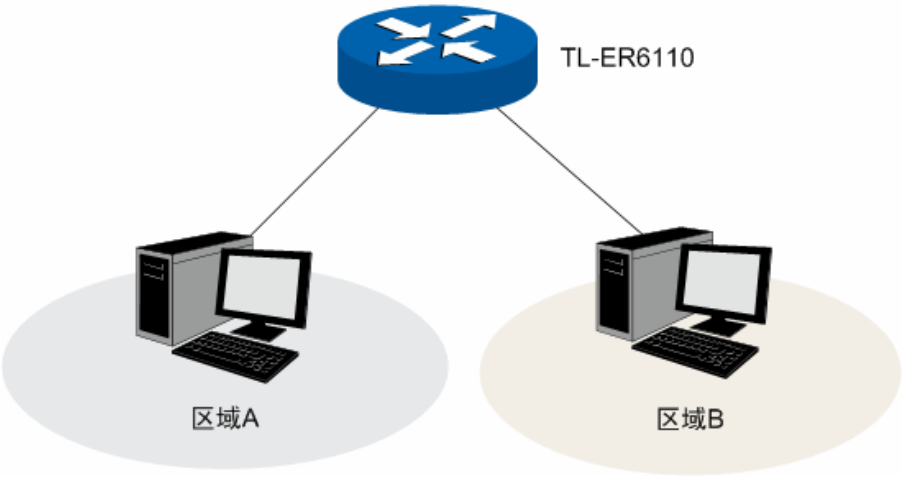


图 4-3 组网拓扑-路由模式

若TL-ER6110应用于混合的组网拓扑中，如图 4-4，则可以将TL-ER6110系统模式设为全模式。

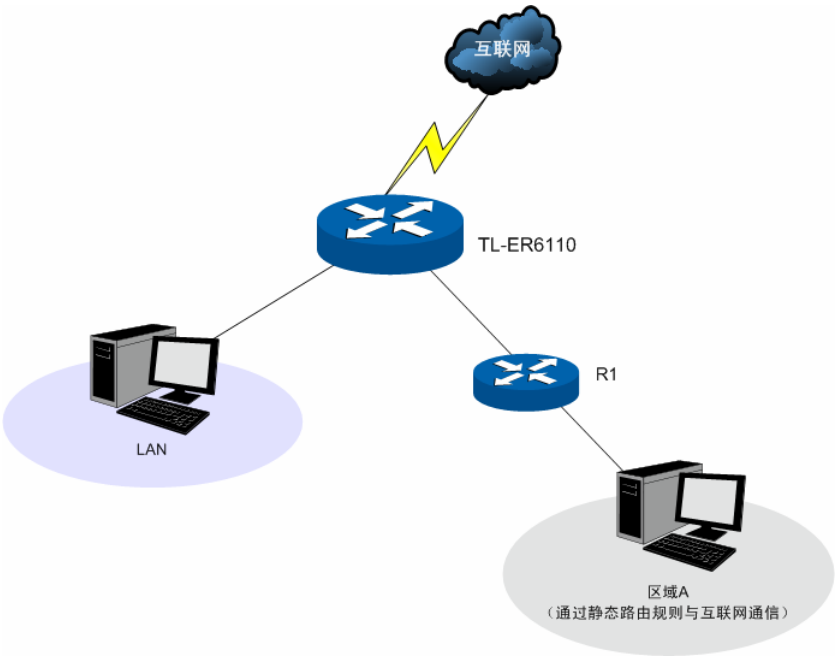


图 4-4 组网拓扑-全模式

界面进入方法：基本设置 >> 系统模式 >> 系统模式

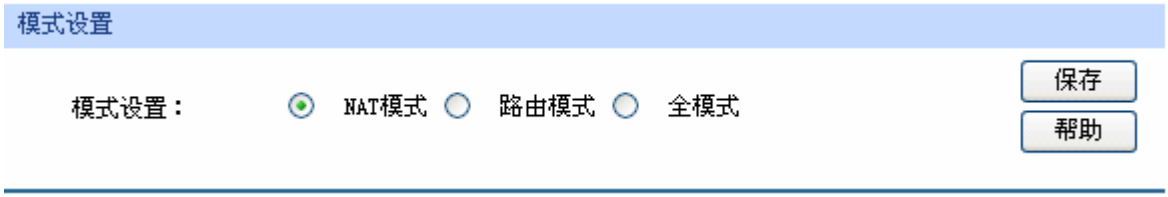


图 4-5 系统模式设置界面

请根据实际网络需要选择路由器的工作模式。

NAT模式。此模式下，由局域网向广域网发送的数据包默认经过NAT转换，但路由器对所有源地址与局域网接口不在同一网段的数据包均不进行处理。例如，路由器LAN口IP设置为192.168.1.1，子网掩码为255.255.255.0，LAN口所处网段为192.168.1.0/24，此时，路由器收到源地址为192.168.1.123的数据包会进行NAT转换；但如果收到源地址为20.31.76.80的数据包则直接丢弃。

路由模式。此模式下，处于不同网段的主机可以通过相应的**路由设置**进行通信，但路由器不进行NAT转换。例如，当路由器DMZ口处于广域网模式时，DMZ区域内主机需要以路由方式访问广域网中的服务器，若静态路由规则允许，则可正常通信。此时，局域网内的主机不能访问广域网。

说明：

路由模式下，所有转发规则将失效。

全模式。全模式包含了NAT模式及路由模式，此模式下，路由器首先对符合NAT转发条件的数据包进行NAT转换；若不符合，则进行静态路由规则匹配，匹配成功的数据包以路由模式进行转发；匹配失败的数据包直接丢弃。这样，路由器既允许数据包进行NAT转换，也不阻隔与接口在不同网段的数据包。

4.1.3 WAN设置

TL-ER6110提供五种方式接入广域网：静态IP、动态IP、PPPoE、L2TP、PPTP，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；
- 虚拟专用拨号网络一般使用L2TP或PPTP连接方式。

界面进入方法：基本设置 >> WAN设置 >> WAN设置

1) 静态IP连接

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。

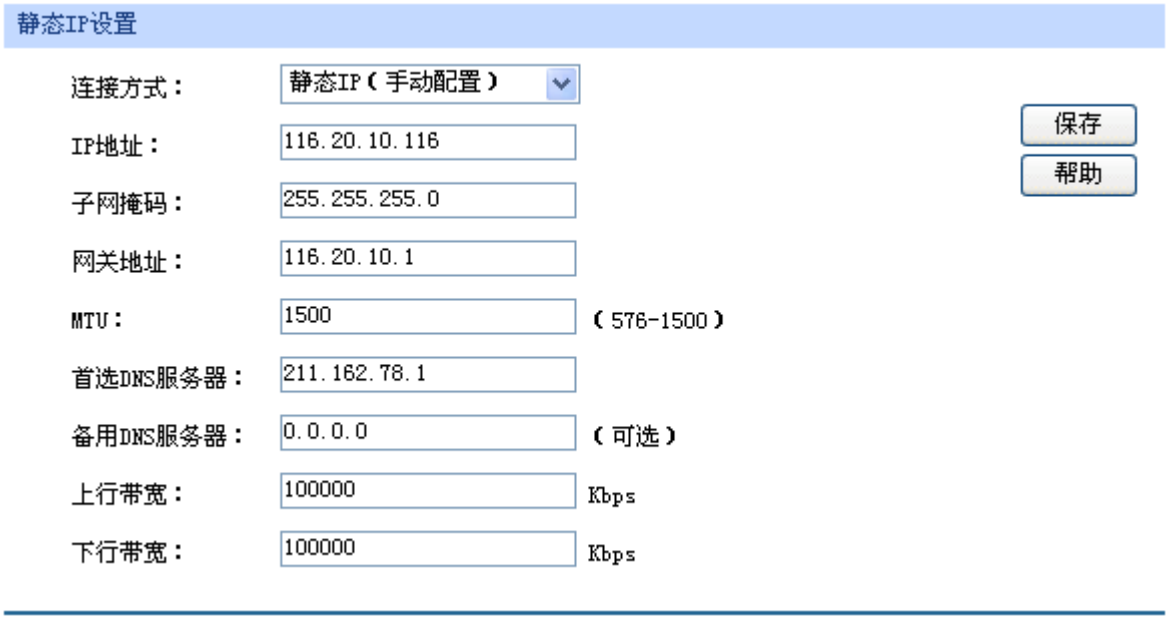


图 4-6 WAN口设置界面-静态IP

界面项说明：

- **静态IP设置**

连接方式	选择静态IP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。
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，如果留空，则无法通过域名访问互联网。
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。

2) 动态IP连接

若ISP提供DHCP自动分配地址服务，请选择动态IP自动获取WAN口参数。

图 4-7 WAN口设置界面-动态IP

界面项说明：

- **动态IP设置**

连接方式	选择动态IP连接方式。点击<获取>得到IP参数，点击<释放>则不再使用现有IP参数。
主机名	输入用于标识路由器的名称。
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。
手动设置DNS服务器	如果需要手动设置DNS(Domain Name Server，域名解析服务)地址，请勾选此项。
首选DNS服务器	设置DNS地址，一般由ISP提供。
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。

- **动态IP状态**

连接状态	显示当前WAN口DHCP分配状态。 “未启用”表示当前已选择动态IP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连接

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

图 4-8 WAN口设置界面-PPPoE

界面项说明：

- **PPPoE设置**

连接方式	选择PPPoE。点击<连接>开始拨号并获取IP参数，点击<断开>则取消与互联网的连接同时释放已获取的IP参数。
帐号	PPPoE拨号的用户名，由ISP提供。
密码	PPPoE拨号的密码，由ISP提供。
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。
启用PPPoE高级设置	可以在此手动指定MTU值、服务名及DNS(Domain Name Server，域名解析服务)地址。如果不清楚这些参数，请勿勾选此项。
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1480。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。
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。

- **PPPoE状态**

连接状态	显示当前WAN口PPPoE拨号连接状态。 “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。
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) L2TP连接

若使用L2TP虚拟专用拨号接入网络，ISP会提供上网帐号及密码，请选择L2TP连接方式进行设置。

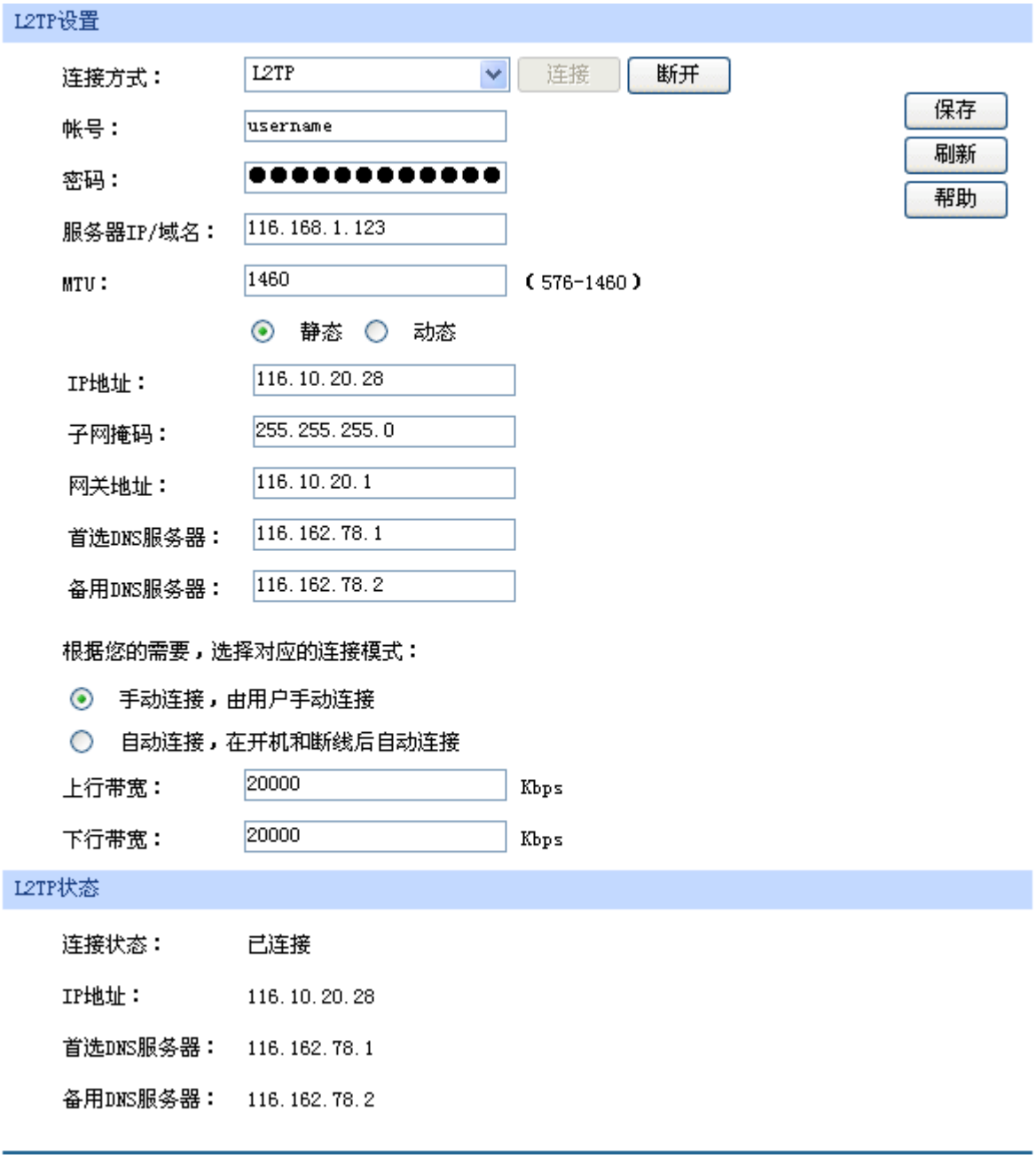


图 4-9 WAN口设置界面-L2TP

界面项说明：

➢ **L2TP设置**

连接方式	选择L2TP。点击<连接>开始拨号并获取IP参数，点击<断开>则取消与互联网的连接同时释放已获取的IP参数。

帐号	L2TP拨号的用户名，由ISP提供。
密码	L2TP拨号的密码，由ISP提供。
服务器IP/域名	L2TP拨号的服务器的IP地址或域名，由ISP提供。
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576-1460之间的整数，默认值为1460。若ISP未提供MTU值，请保持默认值不变。
静态/动态	选择静态或动态获取IP地址。若选择静态方式，则需要手动设置IP地址；若选择动态，则外部的DHCP服务器将动态分配一个IP地址。
IP地址	若选择静态，设置路由器WAN口的IP地址；若选择动态，显示路由器WAN口获取到的IP地址。
子网掩码	若选择静态，设置路由器WAN口的子网掩码；若选择动态，显示路由器WAN口获取到的子网掩码。
网关地址	若选择静态，设置网关地址；若选择动态，显示获取到的网关地址。
首选DNS服务器	若选择静态，设置DNS(Domain Name Server，域名解析服务器)地址，一般由ISP提供，如果留空，则无法通过域名访问互联网；若选择动态，显示分配到的DNS地址。
备用DNS服务器	若选择静态，设置备用DNS地址，一般由ISP提供，允许留空；若选择动态，显示分配到的备用DNS地址。
手动连接	用户可在需要上网时手动点击<连接>按钮进行连接。
自动连接	每次接通路由器电源，路由器便会进行自动拨号。
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。

- **L2TP状态**

连接状态	显示当前WAN口L2TP拨号连接状态。 “未启用”表示当前已选择L2TP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L2TP拨号后获取到的IP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。

5) PPTP连接

若使用PPTP虚拟专用拨号接入网络，ISP会提供上网帐号及密码，请选择PPTP连接方式进行设置。

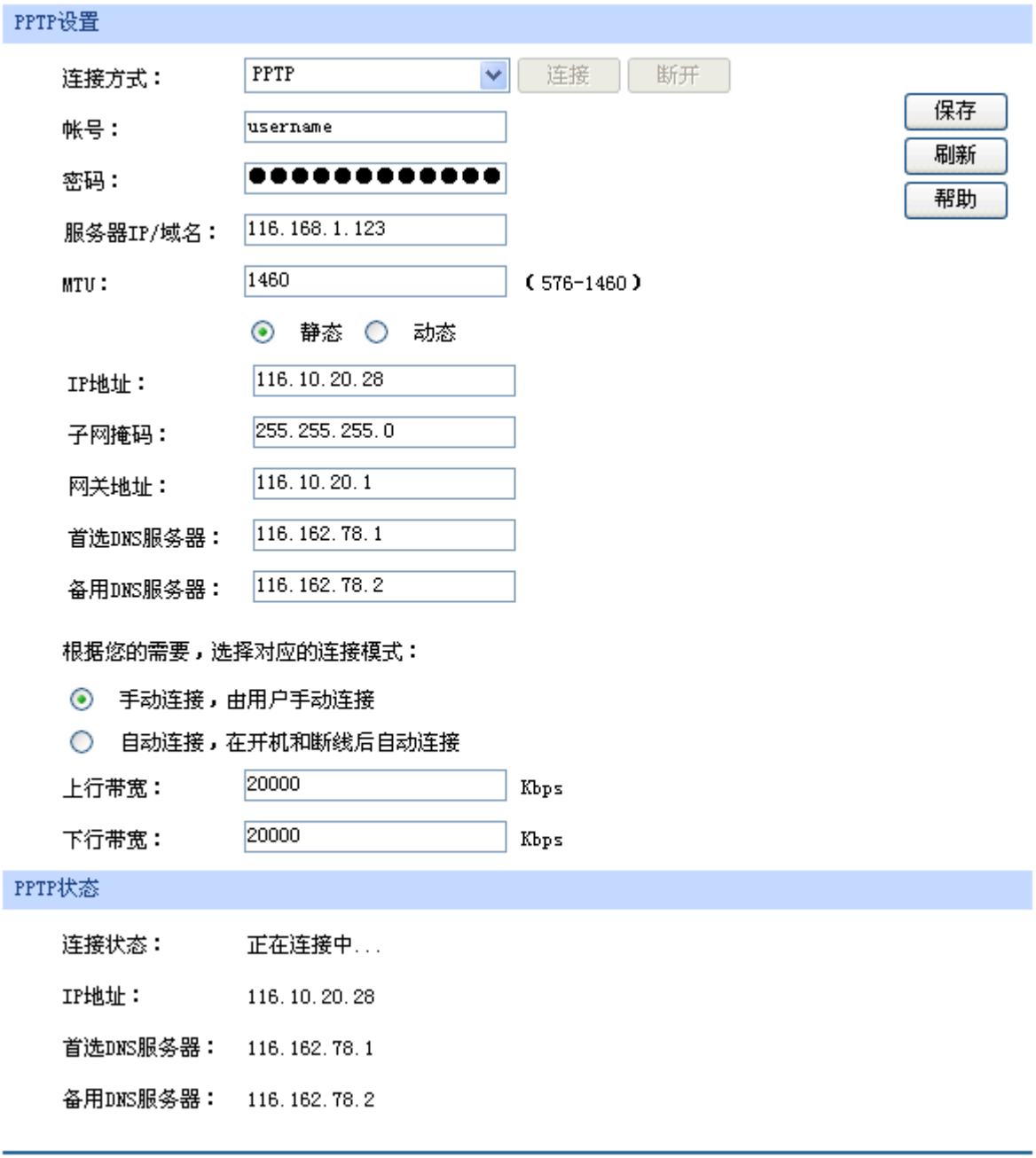


图 4-10 WAN口设置界面-PPTP

界面项说明：

➢ **PPTP设置**

连接方式	选择PPTP。点击<连接>开始拨号并获取IP参数，点击<断开>则取消与互联网的连接同时释放已获取的IP参数。

帐号	PPTP拨号的用户名，由ISP提供。
密码	PPTP拨号的密码，由ISP提供。
服务器IP/域名	PPTP拨号的服务器的IP地址或域名，由ISP提供。
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576-1460之间的整数，默认值为1460。若ISP未提供MTU值，请保持默认值不变。
静态/动态	选择静态或动态获取IP地址。若选择静态方式，则需要手动设置IP地址；若选择动态，则外部的DHCP服务器将动态分配一个IP地址。
IP地址	若选择静态，设置路由器WAN口的IP地址；若选择动态，显示路由器WAN口获取到的IP地址。
子网掩码	若选择静态，设置路由器WAN口的子网掩码；若选择动态，显示路由器WAN口获取到的子网掩码。
网关地址	若选择静态，设置网关地址；若选择动态，显示获取到的网关地址。
首选DNS服务器	若选择静态，设置DNS(Domain Name Server，域名解析服务器)地址，一般由ISP提供，如果留空，则无法通过域名访问互联网；若选择动态，显示分配到的DNS地址。
备用DNS服务器	若选择静态，设置备用DNS地址，一般由ISP提供，允许留空；若选择动态，显示分配到的备用DNS地址。
手动连接	用户可在需要上网时手动点击<连接>按钮进行连接。
自动连接	每次接通路由器电源，路由器便会进行自动拨号。
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。

➢ **PPTP状态**

连接状态	显示当前WAN口PPTP拨号连接状态。 “未启用”表示当前已选择PPTP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PPTP拨号后获取到的IP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。

4.1.4 LAN设置

4.1.4.1 LAN口设置

在此设置TL-ER6110路由器LAN口的IP参数。

界面进入方法：基本设置 >> LAN设置 >> LAN口设置

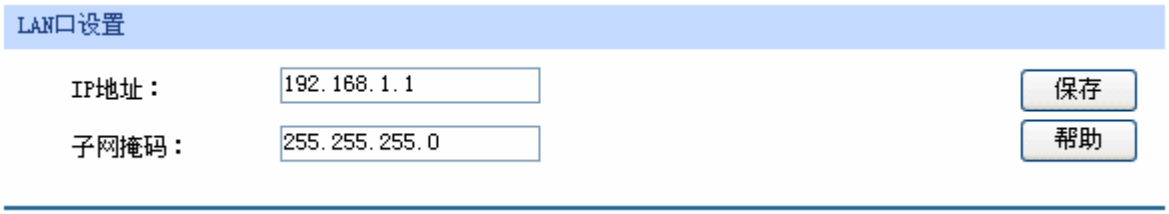


图 4-11 LAN口设置界面

界面项说明：

➢ **LAN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。

注意：

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。

4.1.4.2 DHCP服务

DHCP(Dynamic Host Configuration Protocol, 动态主机配置协议)。路由器具有DHCP服务功能，能够为所有接入TL-ER6110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

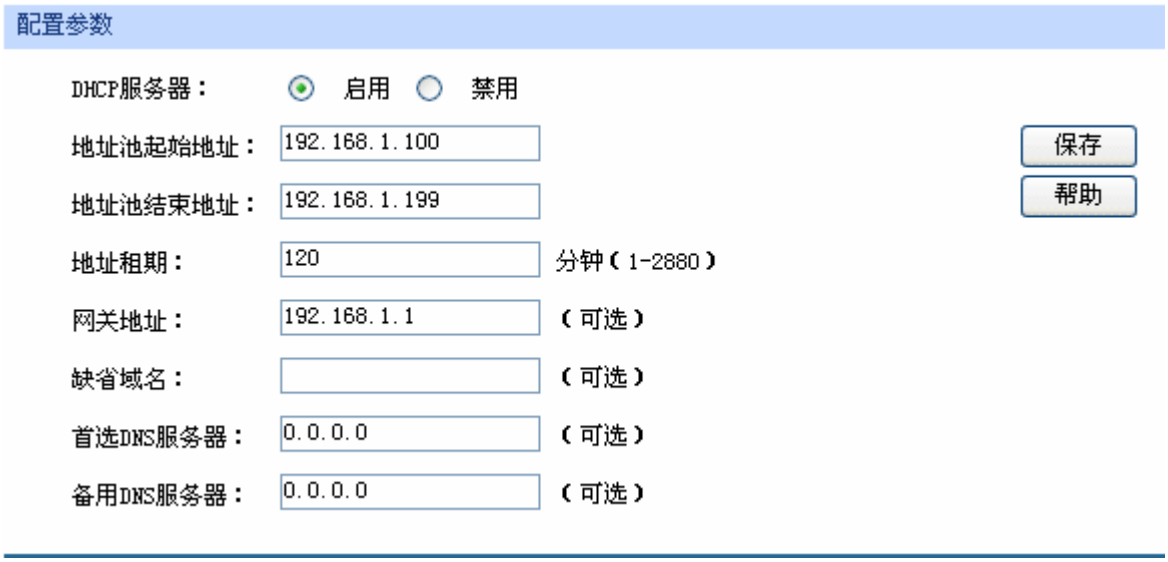


图 4-12 DHCP服务设置界面

界面项说明：

- **配置参数**

DHCP服务器	选择开启或关闭DHCP服务。若希望路由器自动为计算机配置TCP/IP参数，请选择“启用”。
地址池起始地址	设置DHCP服务器自动分配IP地址的起始地址，该地址必须与LAN口IP地址设置在同一网段，默认值为192.168.1.100。
地址池结束地址	设置DHCP服务器自动分配IP地址的结束地址，该地址必须与LAN口IP地址设置在同一网段，默认值为192.168.1.199。
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，推荐设置为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。

4.1.4.3 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 4-13 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。

4.1.4.4 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 4-14 静态地址分配设置界面

界面项说明：

➢ **静态地址**

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。
启用/禁用规则	选择启用或禁用本条静态地址分配规则。

➢ **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 4-14序号1规则的含义：MAC地址为00-19-66-83-53-CF的客户端，指定其IP地址为192.168.1.101，该规则已禁用。

注意：

为了避免冲突，建议先进行IP MAC绑定，具体操作请参考**4.4.1ARP防护**，然后点击图 4-14静态地址分配设置界面中的<导入>按钮，直接获取IP MAC绑定列表中的静态地址条目。

4.1.5 DMZ设置

DMZ(Demilitarized Zone, 非军事区域)也称隔离区。TL-ER6110提供一个物理DMZ接口，允许所有接入此端口的本地主机暴露在广域网中，进行一些特别的网络应用服务，如各种共享服务器、视频会议等。

DMZ物理接口可以工作在两种模式下，广域网模式或局域网模式。

广域网模式中，DMZ区域直接以路由模式与广域网之间通信。此时DMZ区域与广域网区域一样使用公有地址，不能主动访问局域网。

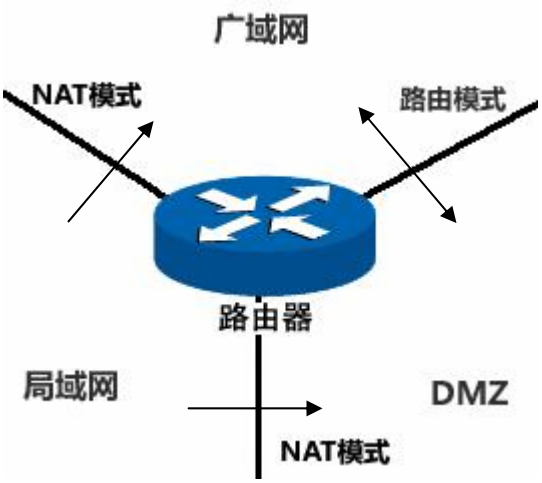


图 4-15 DMZ口于广域网模式

局域网模式中，DMZ区域访问广域网区域时需要经过NAT进行地址转换。此时DMZ区域可以使用与局域网区域不同网段的私有地址，并且可以主动向局域网区域发起访问连接。

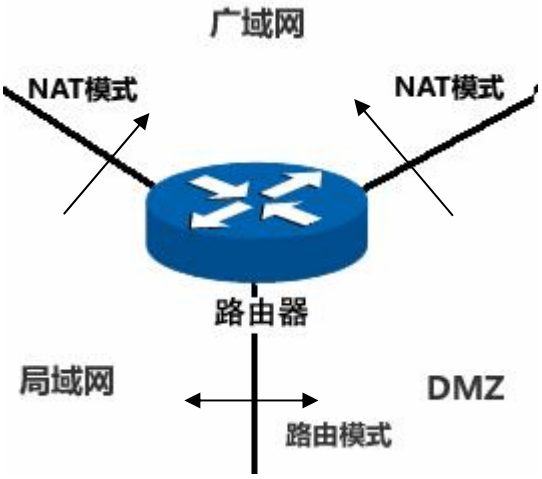


图 4-16 DMZ口于局域网模式

4.1.5.1 DMZ口设置

在此控制TL-ER6110的DMZ口是否启用，并设置其IP参数。

界面进入方法：基本设置 >> DMZ设置 >> DMZ口设置

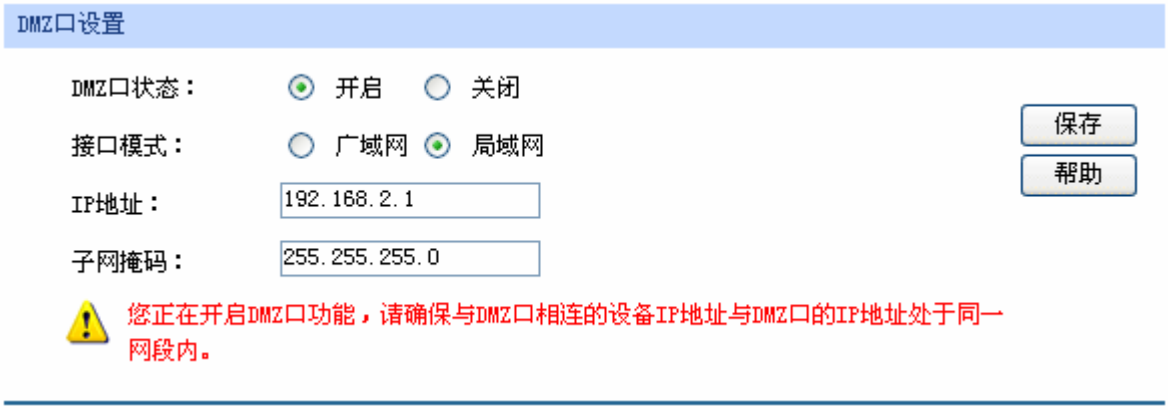


图 4-17 DMZ口设置界面

界面项说明：

➢ **DMZ口设置**

DMZ口状态	设置是否启用DMZ口。在不启用的状态下，DMZ口功能与LAN口功能相同。
接口模式	通过选择接口模式，可以控制DMZ区域与广域网、局域网之间的连接方式。
IP地址	设置DMZ口的IP地址。
子网掩码	设置DMZ口的子网掩码。

说明：

DMZ口开启后将具有DHCP服务、客户端列表及静态地址分配功能设置，具体设置请参考第**4.1.4.2**至**4.1.4.4**小节。

注意：

当DMZ口开启并处于广域网模式时，若ISP为DMZ口提供的是单一广域网IP地址，请勿开启DMZ口的DHCP服务，否则DMZ区域内的主机分配到的地址不能正常访问广域网。若ISP提供的是地址段，请按照地址段范围设置DHCP地址池。

4.1.6 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。

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-ER6110，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-ER6110的LAN口MAC地址设置为原路由器的MAC地址即可。

WAN口MAC设置：

有些ISP要求上网帐号与拨号设备的MAC绑定，若此时拨号设备更换为TL-ER6110，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。

DMZ口MAC设置：

DMZ口的MAC应用方式与LAN口类似。

界面进入方法：基本设置 >> MAC设置 >> MAC设置

图 4-18 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<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<管理主机MAC>按钮；该条目不出现在LAN口和DMZ口设置栏。

注意：

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。

4.1.7 交换机设置

TL-ER6110路由器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。

4.1.7.1 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

图 4-19 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	接收/发送所有的数据帧的总字节数（包含校验和错误的帧）。
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字节到最大帧长之间的数据帧数目（包含错误帧）。对于不带tag标签的帧，路由器支持的最大帧长为1518字节；对于带tag标签的帧，路由器支持的最大帧长为1522字节。
过大帧	收到的长度大于最大帧长的数据帧数目（包含错误帧）。

勾选最后一行的复选框后，点击<清空统计>按钮，即可清空该列对应端口的统计数据。点击<清空所有>按钮可以一次清空所有统计数据。

4.1.7.2 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 4-20 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 4-20监控列表的含义是：LAN1被选作监控端口，它将对LAN2进行输入输出监控。

说明

如果监控端口为LAN口，被监控端口中有其他LAN口，则这些LAN口必须属于同一个Port VLAN中，端口监控功能才能生效。

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LAN2为监控端口，监控其它端口的输入输出数据，如下图。设置完成后，点击<保存>按钮。

4.1.7.3 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 4-21 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。
入口限制状态	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”、“FLOOD”（端口的广播、多播帧以及目的MAC地址不存在于地址表的帧）、“广播和多播”和“广播”四种模式，选择其一。
入口限制速率	有从小到大128Kbps/ 256Kbps/ 512Kbps/ 1Mbps/ 2Mbps/ 4Mbps/ 8Mbps七种速率，选择其一。
出口限制状态	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	有从小到大128Kbps/ 256Kbps/ 512Kbps/ 1Mbps/ 2Mbps/ 4Mbps/ 8Mbps七种速率，选择其一。

图 4-21第一行的含义是：开启WAN口的入口和出口限制状态，设置WAN口的入口限制模式为FLOOD，并将其入口/出口速率均设为128Kbps。设置完成后，WAN口的FLOOD模式入口数据帧的接收速率及所有出口数据帧的发送速率将不会超过128Kbps。

4.1.7.4 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 4-22 端口参数设置界面

界面项说明：

➢ **功能设置**

端口状态	只有勾选了“启用”该端口才会有数据包的传输，即物理意义上的开启。
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、自协商5种模式可选，择需使用。
所有端口	这一栏可对以上所有端口进行统一设置，比如同时启用或禁用。

4.1.7.5 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 4-23 端口状态界面

4.1.7.6 Port VLAN

VLAN(Virtual Local Area Network, 虚拟局域网)是从逻辑上而非物理上，将整个局域网分割成几个不同的广播域，数据只能在VLAN内进行交换。

一个稍具规模的网络如果只有一个广播域，那么在网络内不断发送的广播包很容易造成广播风暴，消耗网络整体带宽，并给网络中的主机带来额外的负担。划分VLAN以后，数据只会在自己所属的VLAN内广播，所以可以控制广播风暴，同时还能增强网络安全，简化网络管理。

TL-ER6110提供基于端口划分VLAN的Port VLAN功能，可以把路由器的若干LAN口从逻辑上划分为多个VLAN。

界面进入方法：基本设置 >> 交换机设置 >> Port VLAN

图 4-24 Port VLAN设置界面

界面项说明：

➢ **功能设置**

VLAN 配置各端口所属VLAN。

说明

- Port VLAN的划分只能在LAN口中进行。
- 当DMZ接口的状态改变的时候，会影响到原先Port VLAN的配置。当改变DMZ接口的状态后，建议检查Port VLAN的配置，必要时重新设置。

4.2 对象管理

4.2.1 用户管理

4.2.1.1 组设置

可以在此创建、修改或者删除组。

界面进入方法：对象管理 >> 用户管理 >> 组设置

图 4-25 组设置界面

界面项说明：

- **组设置**

组名称	输入一个名称来标识一个组，可以输入1-28个字符。
备注	添加对当前组的说明信息。

- **组列表**

在组列表中，可以对已创建的组进行相应设置。

说明：

当删除组时，所有引用该组的规则都会被删除。

4.2.1.2 用户设置

可以在此添加、修改或者删除用户。

界面进入方法：对象管理 >> 用户管理 >> 用户设置

图 4-26 用户设置界面

界面项说明：

- **用户设置**

用户名	输入一个名称来标识一个用户，可以输入1-28个字符。
IP	输入当前用户的IP地址。此处只能输入单个IP地址，如果需要设置IP地址段，请点击页面下方<批量处理>按钮进行操作。批量增加用户时，如果新增用户的IP地址与某个已有用户的IP地址重复，那么已有用户的信息将会被删除。
备注	添加对当前用户的说明信息。

- **用户列表**

在用户列表中，可以对已创建的用户进行相应设置。

4.2.1.3 视图

可以在此设置用户视图或者组视图。

界面进入方法：对象管理 >> 用户管理 >> 视图

图 4-27 视图界面

界面项说明：

- **视图设置**

视图选择	选择需要设置的视图。可以选择“用户视图”为用户指定所属组，也可以选择“组视图”为组添加用户或子组。
用户名	选择“用户视图”，可在下拉菜单中选择所需设置的用户。
可选组	显示可以包含该用户的组。
所属组	显示已经包含该用户的组。
组名	选择“组视图”，可在下拉菜单中选择所需设置的组。
查看该组结构	可以查看以该组为根节点组成的树，树中包含该组的所有子组和用户，其中组名以粗体显示。
可选用户	显示该组可以包含的用户和子组。
包含用户	显示该组已经包含的用户和子组。

4.2.2 时间管理

4.2.2.1 时间组

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 4-28 时间组界面

界面项说明：

➢ **时间组设置**

名称	输入一个名称来标识一个时间组，可以输入1-28个字符。
备注	添加对当前时间组的说明信息。
星期	选择周循环的具体日期。
时间段	设置一天24小时内的工作时间段。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。

➢ **时间组列表**

在时间组列表中，可以对已创建的时间组进行相应设置。

图 4-28序号1中名称为“ANY”的时间组，是路由器预定义的一个时间组，表示任何时间，此时间组不可修改、删除。序号2规则的含义：每一天上午8点到11点。

说明：

若时间组被其他规则引用，则该时间组无法删除。

4.3 传输控制

4.3.1 转发规则

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。

4.3.1.1 NAT映射

NAT映射，可以将特定的局域网IP地址与指定的广域网IP地址唯一对应，多用于局域网内的服务器搭建。可在此设置NAT的端口范围和NAT映射关系。

界面进入方法：传输控制 >> 转发规则 >> NAT映射

图 4-29 NAT映射设置界面

界面项说明：

- **NAT服务设置**

源端口范围	设置作为NAT源端口的端口范围，范围跨度必须大于或等于100。可设置范围为2049-65000。

- **NAT映射**

映射地址	设置局域网IP地址和广域网IP地址的一对一映射。第一个输入框中应填写局域网IP地址，第二个输入框中应填写广域网IP地址。TL-ER6110只允许LAN口到WAN口的映射。
出接口	设定数据包发送出去的接口。
DMZ转发	设置是否开启该条NAT映射条目的DMZ转发。开启后所有广域网中发往映射后地址的数据报将被转发至映射前地址。
备注	添加对本条目的说明信息。
启用/禁用规则	设置该条NAT映射条目是否生效。

➢ **映射列表**

在映射表中，可以对已保存的NAT映射条目进行相应设置。

图 4-29序号1条目的含义：局域网主机host1的IP地址为192.168.1.101，指定经NAT映射后的广域网IP地址为222.135.48.52，DMZ转发已开启，映射设置已启用。当host1与广域网通信时，从WAN口发出的数据包源IP地址将被NAT转换为广域网IP地址222.135.48.52，而从广域网返回的数据包目的IP地址会被NAT转换为局域网IP地址192.168.1.101。

注意：

NAT映射只适用于WAN口使用静态IP连接方式的场合。若WAN口连接方式从静态IP切换为动态IP、PPPoE、L2TP或PPTP，以前设置的NAT映射都将失效，直接在动态IP、PPPoE、L2TP或PPTP连接状态下设置的NAT映射也都不起作用。

4.3.1.2 多网段NAT

多网段NAT，可以支持LAN或者DMZ接口下多个网段的IP通过NAT转换访问广域网。

界面进入方法：传输控制 >> 转发规则 >> 多网段NAT

图 4-30 多网段NAT设置界面

界面项说明：

➢ **多网段NAT规则**

网段地址	设置需要进行NAT转换的网段地址，以子网掩码值划分地址范围。
接口	在下拉列表中选择网段所在的接口，可选择LAN或者DMZ。
启用/禁用规则	设置该条多网段NAT规则是否生效。

备注	添加对本条规则的说明信息。

➢ **规则列表**

在规则列表中，可以对已保存的多网段NAT规则进行相应设置。

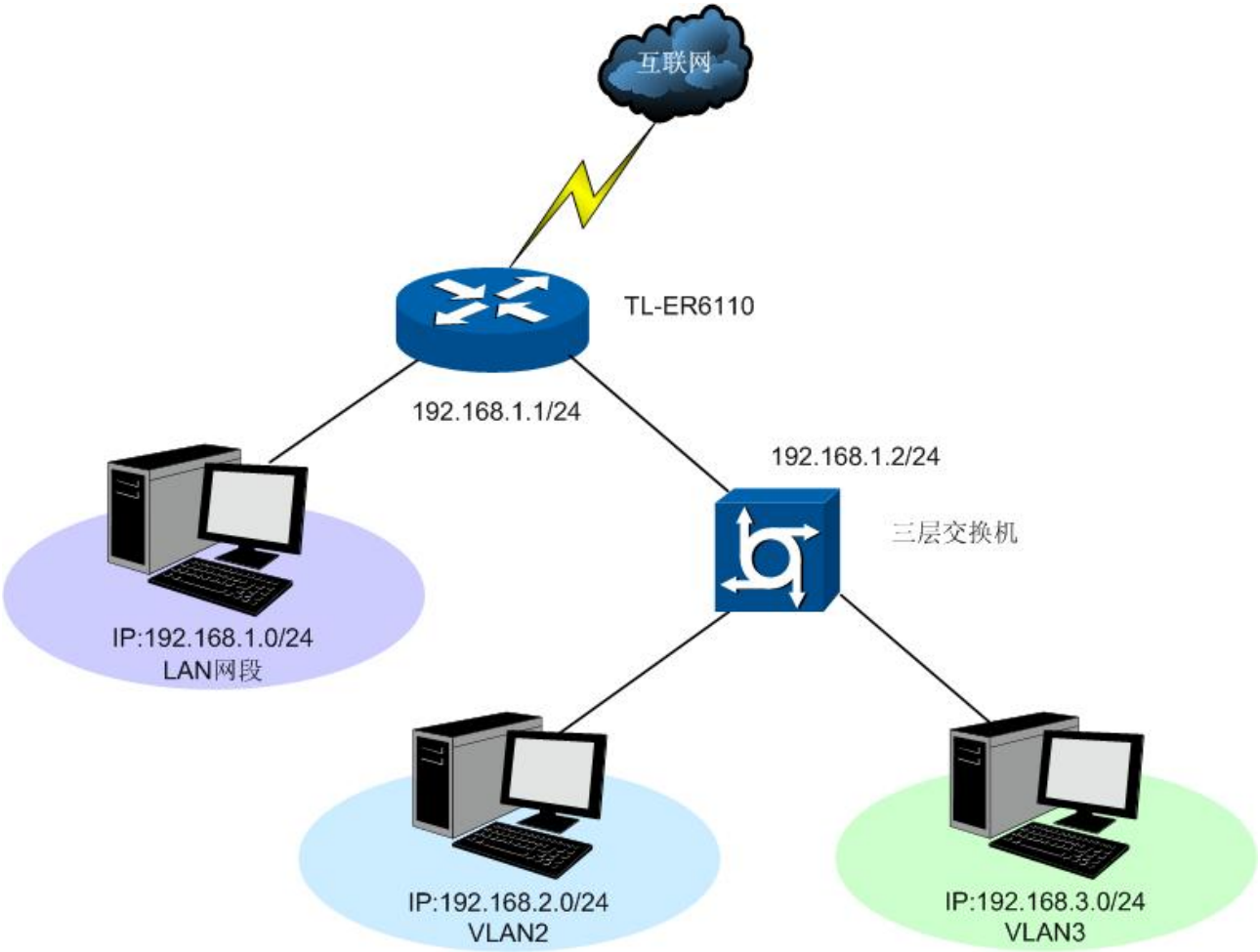
图 4-30序号1规则的含义：这是一条名为tplink1的多网段NAT规则，路由器LAN口下的网段为220.181.6.0/24，本条规则已启用。在进行相应的静态路由规则设置后，该网段将可以通过本路由器进行NAT转换之后访问广域网。

注意：

- 多网段NAT功能需要同时配置静态路由才能生效。
- 只有当DMZ口开启时，DMZ选项才在接口的下拉菜单中显示。
- 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**。

应用举例

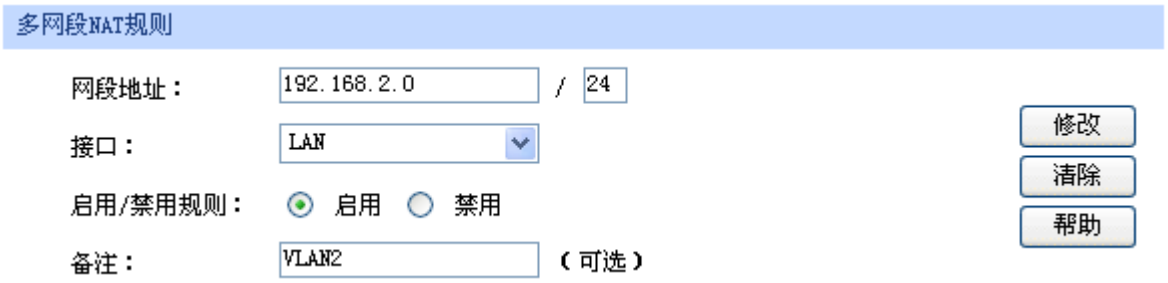
某网吧的网络结构如下：



TL-ER6110的LAN网段为192.168.1.0 /24，三层交换机下VLAN2网段为192.168.2.0 /24，VLAN3网段为192.168.3.0 /24，三层交换机与TL-ER6110的LAN口级联VLAN IP为192.168.1.2。现要实现VLAN2和VLAN3网段可以访问互联网。

可以通过如下设置来实现：

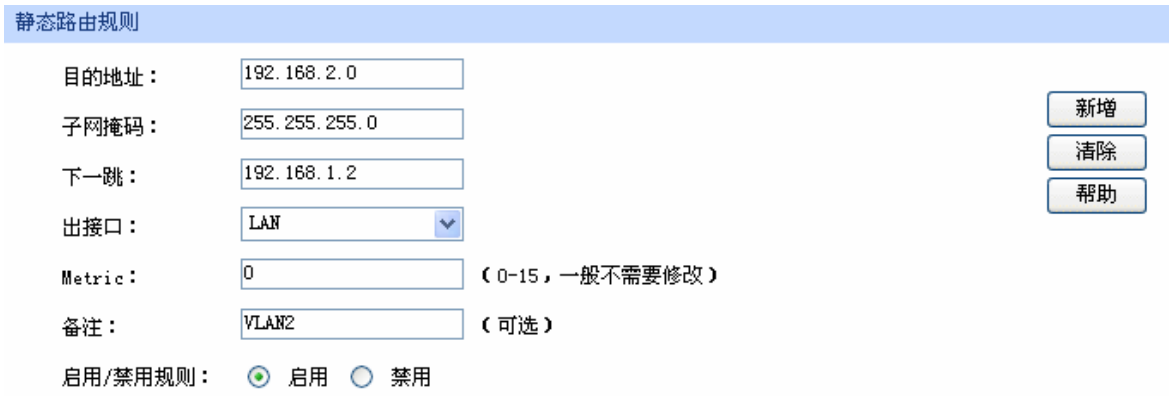
1. 首先设置多网段NAT规则，分别添加VLAN2与VLAN3的网段地址。



设置完成后的规则如下：

2. 然后设置相应的静态路由规则，指定下一跳为网段地址所属三层交换机与本路由器LAN口直接相连的接口IP。

界面进入方法：传输控制 >> 路由设置 >> 静态路由



设置完成后的静态路由如下：

4.3.1.3 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 >> 转发规则 >> 虚拟服务器

图 4-31 虚拟服务器设置界面

界面项说明：

- **NAT DMZ服务**

NAT DMZ服务	设置是否启用NAT DMZ服务。NAT DMZ是NAT应用的一种特殊服务，相当于一条默认的转发规则。若主机开启了NAT DMZ服务，路由器会将所有由广域网发起的、不符合所有现有连接和转发规则的数据全部转发至指定的主机。
主机地址	指定作为NAT DMZ服务器的主机IP地址。

➢ **虚拟服务**

服务名称	用户自定义，标识一条虚拟服务器规则。名称长度需在28个字符以内，中英文均可，一个中文占用2个字符空间。
外部端口	为本条虚拟服务器规则指定路由器提供给广域网的服务端口或端口范围，广域网对该端口或端口范围的访问都将被重定位到局域网中指定的服务器。
内部端口	指定局域网内虚拟服务器主机的实际服务端口。
服务协议	指定应用本条虚拟服务器规则的数据包协议类型。
内部服务器IP	为本条虚拟服务器规则指定局域网服务器的IP地址。外网对局域网指定端口的访问都将发送到该主机。
启用/禁用规则	设置是否应用本条虚拟服务器规则。

注意：

- 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。

➢ **服务列表**

在服务列表中，可以对已保存的虚拟服务器规则进行相应设置。

图 4-31序号1规则的含义：这是一条名为apply1的虚拟服务器规则，由广域网向路由器12892-12893端口发起的TCP/UDP数据都将转发到局域网IP地址为192.168.1.103主机的12892-12893端口上，本条规则已启用。

4.3.1.4 端口触发

由于防火墙的存在，一些如网络游戏、视频会议、网络电话、P2P下载等应用程序需要通过设置转发规则才能正常工作，而这些应用程序又要求多个端口连接，针对单一端口的虚拟服务器功能已不能满足需求，此时就需要使用端口触发功能。

当一个应用程序向触发端口发起连接时，对应开放端口中的所有端口就会打开，以备后续连接。

界面进入方法：传输控制 >> 转发规则 >> 端口触发

图 4-32 端口触发设置界面

界面项说明：

➢ **端口触发**

服务名称	用户自定义，标识一条端口触发规则。名称长度需在28个字符以内，中英文均可，一个中文占用2个字符空间。
触发端口	应用程序首先发起连接的一个或多个端口。只有该端口发起连接时，对应开放端口中的所有端口才可以开放，并为应用程序提供服务，否则开放端口中的所有端口是不会开放的。
触发协议	设定在触发端口上使用的数据包协议类型。
开放端口	为应用程序提供服务的一个或多个端口。当触发端口上发起连接后，开放端口打开，之后应用程序便可以通过这些开放端口发起后续连接。
开放协议	设定在开放端口上使用的数据包协议类型。
启用/禁用规则	设置是否应用本条端口触发规则。

注意：

- 触发端口与开放端口的取值范围均为1-65535之间的任意整数。开放端口取值可以指定一个连续的范围，如8690-8696。
- 路由器支持16条端口触发规则，每条规则最多支持5组触发端口，且这些触发端口不能重叠。
- 每条规则最多支持5组开放端口，每条规则的开放端口数总和需小于或等于100。

➢ **触发列表**

在触发列表中，可以对已保存的端口规则进行相应设置。

图 4-32序号1规则的含义：这是一条名为apply1的端口触发服务规则，当局域网内发起端口为5350和5354的TCP访问时，对TCP和UDP协议开放5355-5358端口。

4.3.1.5 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 >> 转发规则 >> ALG服务

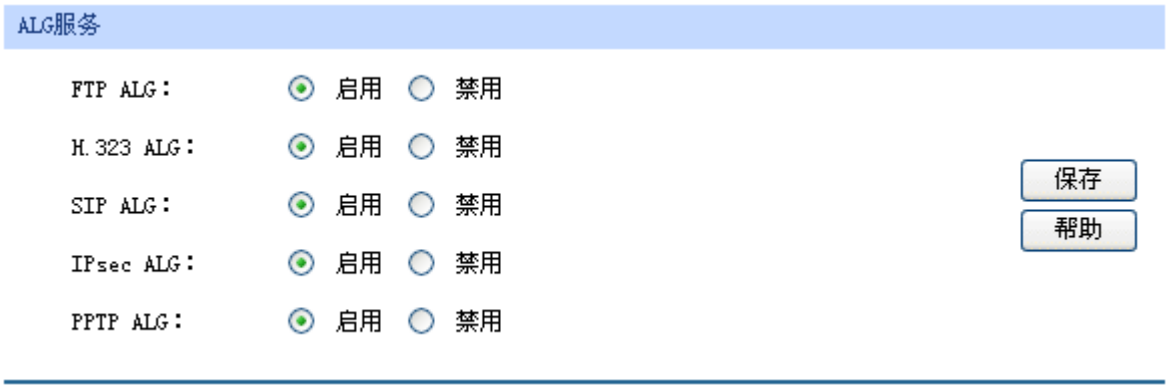


图 4-33 ALG服务设置界面

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。

SIP ALG　　选择启用或禁用SIP ALG服务，默认为启用，如无特殊需求请保持默认配置不变。

IPsec ALG　　选择启用或禁用IPsec ALG服务，默认为启用，如无特殊需求请保持默认配置不变。

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。

4.3.2　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。

4.3.2.1　基本设置

界面进入方法：传输控制 >> 带宽控制 >> 基本设置

图 4-34 带宽控制基本设置界面

界面项说明：

➢ **功能设置**

不启用带宽控制　　勾选此项时，所有带宽控制设置均不生效。

启用普通带宽控制　　勾选此项以启用普通带宽控制功能。

启用智能带宽控制　　勾选此项以启用智能带宽控制功能。当带宽利用率达到指定的值时，带宽控制功能生效。

➢ **WAN口带宽**

接口　　路由器WAN口。

上行带宽　　显示WAN口数据流出的带宽上限，如需调整，请至**WAN设置**页面修改相应WAN口参数。

下行带宽　　显示WAN口数据流入的带宽上限，如需调整，请至**WAN设置**页面修改相应WAN口参数。

➢ **默认规则带宽**

数据流向　　“上行”表示由局域网发送数据到广域网，如局域网内计算机向广域网上的FTP服务器上传文件；“下行”表示由广域网发送数据到局域网，如局域网内计算机从广域网上的FTP服务器下载文件。

最小保证带宽　　设置在物理带宽不足的前提下，对应数据流向至少能够享有的最小带宽。

最大限制带宽　　设置对应数据流向的带宽上限。

说明：

- WAN口的出入带宽必须小于或者等于ISP提供的参数。如果超过实际物理带宽，则带宽控制功能失效。
- 若有数据由A接口流入路由器后由B接口流出，而A接口入口带宽与B接口出口带宽不同时，以两者带宽的最小值为有效带宽。
- 通过页面上的<查看IP流量统计>按钮，可跳转至IP流量统计页面。

4.3.2.2　带宽控制规则

可以在此设置带宽控制规则的参数。

界面进入方法：传输控制 >> 带宽控制 >> 带宽控制规则

图 4-35 带宽控制规则设置界面

界面项说明：

➢ **带宽控制规则**

数据流向	选择控制规则的数据流向。箭头方向代表数据流向和受控主机所在的域。只有当DMZ口开启时，DMZ口选项才在下拉菜单中显示。
用户组	设置受控数据包发出的源地址范围。由用户管理的组来表示。如需新建组，请参考**4.2.1用户管理**。
生效时间	设置带宽规则的生效时间。由时间管理的时间组来表示。如需新建时间组，请参考**4.2.2时间管理**。
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。
上行最小保证带宽	设置上行最小保证带宽，即在物理带宽不足的前提下，上行数据流至少能够享有的最小带宽。
上行最大限制带宽	设置上行最大限制带宽，即上行数据流所能享有的最大带宽。
下行最小保证带宽	设置下行最小保证带宽，即在物理带宽不足的前提下，下行数据流至少能够享有的最小带宽。

下行最大限制带宽	设置下行最大限制带宽，即下行数据流所能享有的最大带宽。
备注	添加对本条规则的说明信息。
启用/禁用规则	选择启用或禁用本条带宽控制规则。

➢ **规则列表**

在规则列表中，可以对已保存的带宽控制规则进行相应设置。

图 4-35序号1规则的含义：处于LAN中的用户组“sales”内的主机共享带宽，当这些主机向广域网发送数据包时，保证上行和下行的最小带宽各为5000Kbps，最大带宽各为10000Kbps。该规则在时间组“time1”设置的时间段内生效。

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。
- 异常情况：各带宽控制规则的最小保证带宽之和大于总物理带宽。当某接口所有带宽控制规则的最小保证带宽之和大于此接口的物理带宽时，意味着无论如何都无法同时满足所有带宽控制规则的最小保证带宽。
- 在DMZ口关闭状态下，不提供与DMZ口相关规则的新增、修改、启用或禁用操作，仅提供对该规则的删除操作。

4.3.3 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。

4.3.3.1 连接数限制规则

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 >> 连接数限制规则

图 4-36 连接数限制规则设置界面

界面项说明：

- **功能设置**

启用连接数限制	勾选此项以启用连接数控制。不勾选时，所有连接数限制均不生效。

- **连接数限制规则**

用户组	设置需要进行连接数限制的主机的IP地址段，由用户管理的组来表示，限制规则将对组内每一个用户生效。如需新建组，请参考**4.2.1用户管理**。
最大连接数	为本条规则设置相应的最大连接数。
备注	添加对本条规则的说明信息。
启用/禁用规则	选择启用或禁用本条规则。

- **规则列表**

在规则列表中，可以对已保存的连接数限制规则进行相应设置。

图 4-36序号1规则的含义：名为“局域网”用户组内的主机向广域网发起的最大连接数被限制为100条，该条规则已启用。

4.3.3.2 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 4-37 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用户组主机连接数信息。连接数限制规则之外的用户只显示IP地址和当前连接数。如需获取最新信息，请点击<刷新>按钮。

4.3.4 路由设置

4.3.4.1 静态路由

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。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 4-38 静态路由设置界面

界面项说明：

➢ **静态路由规则**

目的地址	设定数据包需要到达的目的IP地址。
子网掩码	设定目的IP地址的子网掩码。
下一跳	指定一个IP地址，路由器下一步会将符合条件的数据包转发到该地址上。
出接口	设定数据包发送出去的接口。
Metric	设定路由规则的优先级，数值越低则优先级越高。如无特殊需要请保持默认值0。
备注	添加对本条规则的说明信息。

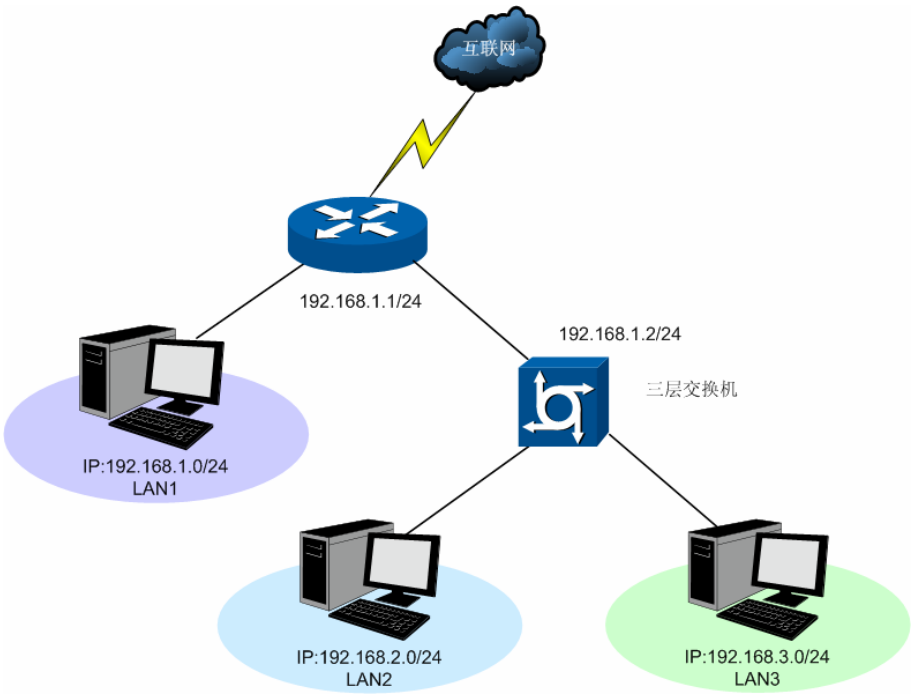
➢ **规则列表**

在规则列表中，可以对已保存的静态路由规则进行相应设置。

图 4-38序号1规则的含义：如果有数据包发往一个IP地址为192.168.3.56，子网掩码为255.255.255.255的设备，则路由器会将数据包从LAN口转发至下一跳地址192.168.3.1，该路由规则已启用优先级为0。

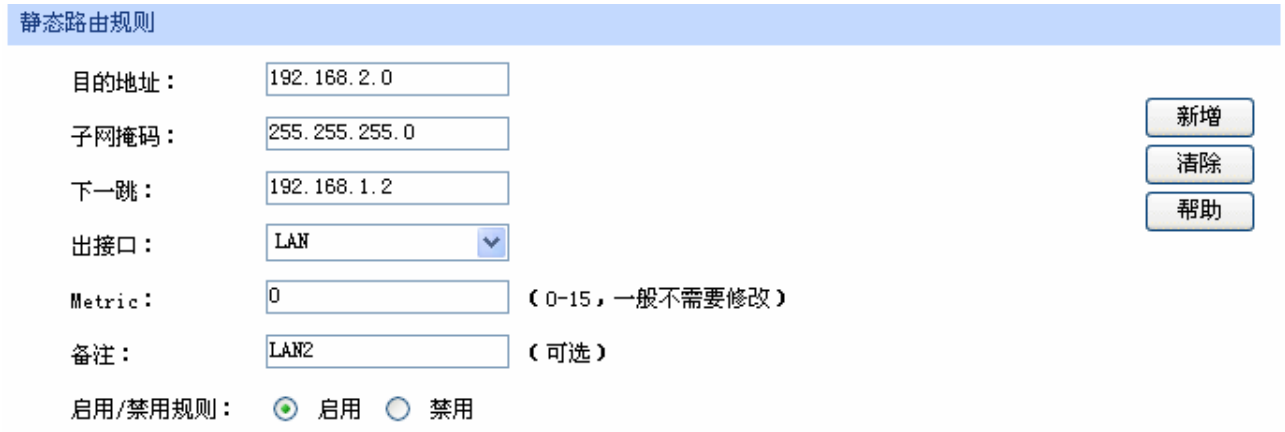
应用举例

某企业的网络结构如下：



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。

可以通过在路由器上设置静态路由来实现。在路由器静态路由界面设置到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，如下图所示。最后点击<新增>按钮保存规则。以同样的方式可以添加到LAN3网段的静态路由。



设置完成后的静态路由如下：

4.3.4.2 RIP服务

RIP（Routing Information Protocol，路由信息协议），是一种采用距离向量算法选择最优路径的动态路由协议，因其易于配置、管理和实现，被广泛应用于如校园网等中小规模的网络中。

RIP的距离是数据包发往目的站点需经过的路由跳数，取值为1 - 15，超过15则是无穷大，表示目的地无法到达。最优路径即所经跳数最少的网络链路。RIP每隔30秒通过UDP报文以广播形式交换一次路由信息。如果在180秒内未收到某一路由条目的信息，则RIP协议就会将该条路由的距离设定成无穷大，并删除路由表中相关信息。

RIP协议在应用中不断地被完善，从最初的RIPv1版本基础上逐渐发展出了RIPv2版本的协议。RIPv2相较RIPv1还支持VLSM(Variable Length Subnet Mask，可变长子网掩码)、简单明文认证、MD5密文认证、CIDR（Classless Inter-Domain Routing，无类型域间选路）和多播，相对于RIPv1应用更加灵活。

TL-ER6110同时支持RIPv1和RIPv2两种版本的协议，可以根据实际的网络需求设置，以提高网络性能。

界面进入方法：传输控制 >> 路由设置 >> RIP服务

图 4-39 RIP服务设置界面

界面项说明：

- **RIP服务设置**

  接口　　显示目前路由器所有存在物理连接的接口。

  接口状态　　选择是否启用RIP协议。

  输出版本　　选择是以何种形式向外发送路由信息。其中RIPv2支持多播和广播两种形式。

  密码认证　　如果应用RIPv2，可以根据实际网络情况设置密码认证，认证密码不超过15位。

  所有接口　　在此可以对所有接口进行批量操作。接口状态增加“禁用”一项，选择后所有接口都不应用RIP协议。

- **RIP路由表**

  启用RIP协议后，路由器收到数据包后经RIP协议转发的信息将会显示在列表中。

  图 4-39序号1条目的含义：当收到目的地址在116.20.10.0/24网段的数据包时，路由器将选择与目的地址同网段的WAN口作为下一跳，并转发数据，此时下一跳IP地址为116.20.10.116。数据包经过的跳数为1，该条目的生存时间为0秒，表示永久生效。

注意：

- 当系统模式为NAT模式时不支持RIP路由设置，若需设置RIP路由，请将当前系统模式更改为路由模式或全模式。
- 仅当WAN口的连接方式为静态IP时，该WAN口的RIP服务才会生效。

4.4 安全管理

4.4.1 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。

4.4.1.1 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 4-40 IP MAC绑定设置界面

界面项说明：

➢ **功能设置**

推荐勾选所有项目，但请注意在勾选“仅允许IP MAC绑定的数据包通过路由器”选项前，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。

勾选“启用ARP日志记录”后路由器会将ARP日志发送到指定的日志服务器中。日志服务器地址即**4.8.5系统日志**中设置的服务器地址。

➢ **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。

备注	添加对本条目的说明信息。
启用/禁用规则	选择启用或禁用本条绑定规则。

➢ **绑定列表**

在绑定列表中，可以对已保存的ARP绑定条目进行相应设置。

图 4-40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00-19-66-83-53-CF进行绑定，该绑定规则已启用。

注意：

若当前绑定列表中所有条目都禁用，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。

4.4.1.2 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 4-41 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：

符号“---”表示当前条目未被绑定，可能会被错误的ARP信息更替掉；

图片表示当前条目已导入“IP MAC绑定”界面的绑定列表中，但还未绑定生效；

图片表示当前条目已进行绑定，可以防御ARP攻击。

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。

注意：

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。

4.4.1.3 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 4-42 ARP列表界面

ARP列表条目的操作可参考**4.4.1.2 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。

4.4.2 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

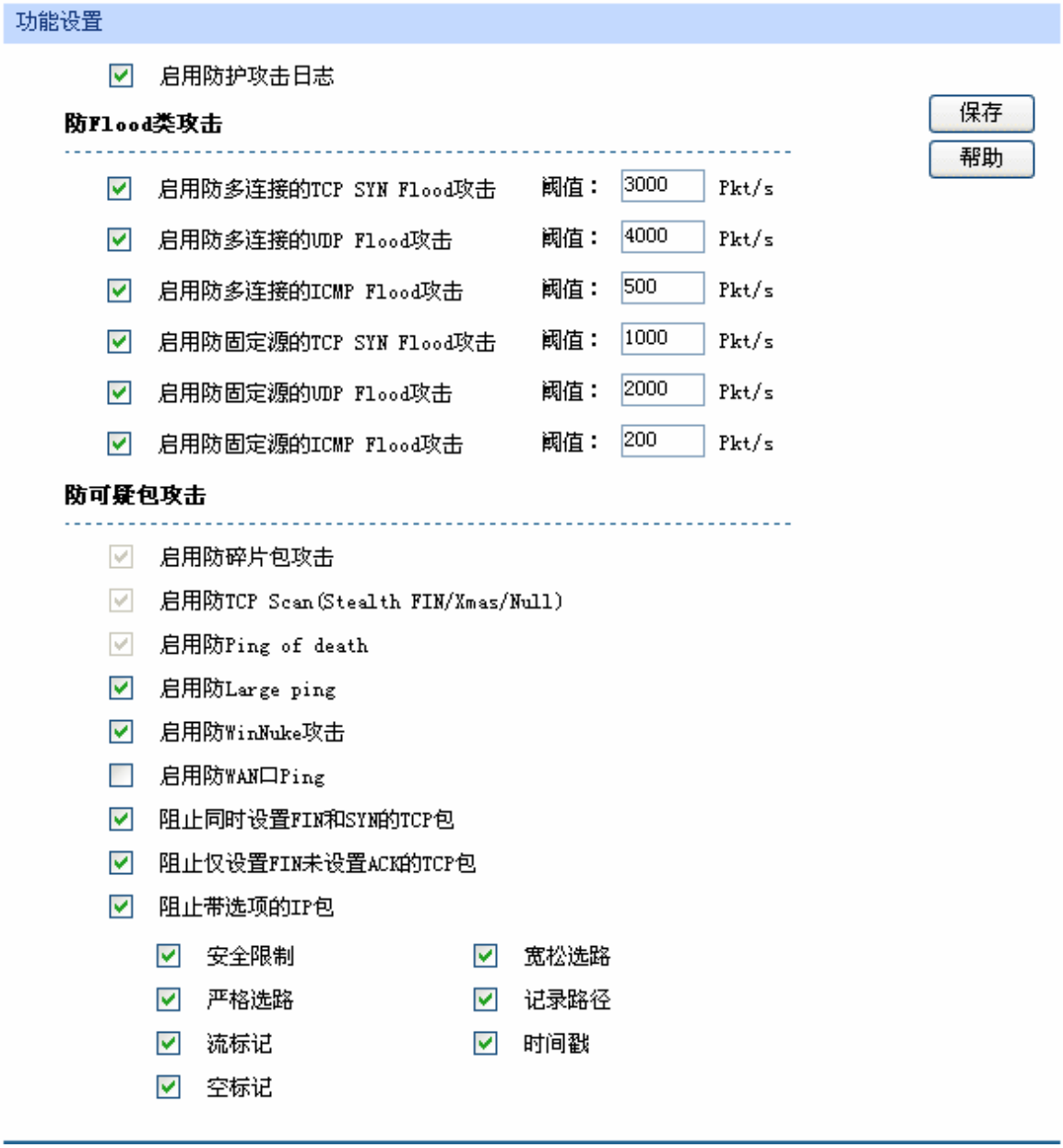


图 4-43 攻击防护设置界面

界面项说明：

➢ **功能设置**

启用防护攻击日志 勾选此项后路由器会记录相关的防护日志。

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DoS攻击为洪水攻击，包括TCP SYN，UDP，ICMP等。推荐勾选界面上所有防DoS攻击选项并设定相应阈值，如不确定，请保持默认设置不变。

防可疑包攻击	可疑包即非正常数据包，有可能是病毒或攻击者的试探。推荐勾选界面上所有防可疑包选项。

4.4.3 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 4-44 MAC过滤设置界面

界面项说明：

- **功能设置**

  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地址过滤规则**

MAC地址	输入需要控制的局域网主机MAC地址。
备注	添加对本条规则的说明信息。

- **规则列表**

  在规则列表中，可以对已保存的MAC地址条目进行相应设置。

4.4.4 访问策略

4.4.4.1 访问规则

界面进入方法：安全管理 >> 访问策略 >> 访问规则

图 4-45 访问规则设置界面

界面项说明：

➢ **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。若选择阻塞，则符合该条规则的所有数据包将无法通过路由器；若选择允许，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过滤规则。例如在策略为阻塞的前提下，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。如果列表中没有合适的服务类型，可以参见**4.4.4.2服务类型**进行添加，可通过下拉列表旁边的<服务类型>按钮快速进入设置界面。

生效接口域	在下拉列表中选择本条规则所针对的接口域，可选择WAN、LAN或者DMZ。选择WAN（LAN/ DMZ）时表示所有WAN（LAN/ DMZ）接口。当接收报文的接口为指定接口域时，该规则生效。
源地址范围	选择指定地址范围的方式，若选择“IP/MASK”方式，则应输入需要管理的地址，以子网掩码值划分地址范围；若选择“IP地址段”方式，则应输入需要管理的IP地址范围；若选择“ANY”方式，则表示该范围包括所有IP地址；若选择“组”方式，则应在下拉菜单中选择相应的组来指定地址范围，如需新建组，请参考**4.2.1用户管理**。
目的地址范围	选择指定地址范围的方式，若选择“IP/MASK”方式，则应输入需要限制访问的地址，以子网掩码值划分地址范围；若选择“IP地址段”方式，则应输入需要管理的IP地址范围；若选择“ANY”方式，则表示该范围包括所有IP地址。
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**4.2.2时间管理**。
备注	添加对本条规则的说明信息。
启用/禁用规则	选择启用或禁用本条策略选路规则。
指定位置	勾选该项后，可以将当前设置的条目添加到访问规则列表中指定序号的位置。默认情况下，规则新增生效后会显示在访问规则列表的最后。

➢ **规则列表**

在规则列表中，可以对已保存的访问规则进行相应设置。在规则列表中，序号数字越小的规则，执行的优先级越高。

图 4-45序号1规则的含义：192.168.1.0/24网段的主机在时间组“time1”设置的时间段内向广域网116.10.20.0/24网段发送的TELNET服务数据包将无法通过路由器，该规则已启用。

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。
- 只有当DMZ口开启时，DMZ选项才在生效接口域的下拉菜单中显示。
- 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**。

4.4.4.2 服务类型

为了能够在定制防火墙策略时比较方便地指定需要过滤的协议和端口号，设备提供了服务类型管理功能。每一个服务类型由协议类型和端口范围两部分构成。系统已经预定义了如HTTP、FTP、TELNET等常用服务类型，也可以根据需要添加自定义服务类型。

界面进入方法：安全管理 >> 访问策略 >> 服务类型

图 4-46 服务类型设置界面

界面项说明：

- **服务类型**

服务名称	用户自定义，标识一条服务类型。名称长度需在28个字符以内，中英文均可，一个中文占用2个字符空间。该名称将显示在“访问规则”设置的服务类型下拉列表中。
协议类型	设置协议类型，可供用户定义的协议类型有TCP、UDP、TCP/UDP。
目的端口范围	设置该服务所使用的端口号范围。最多允许设置5组端口组，每个端口组可以为单个端口，如6320；可以为端口范围，如6322-6325；也可以是两者结合，如6320,6322-6325，但端口组之间不允许重叠。

➢ **服务列表**

在服务列表中，可以对自定义的服务类型条目进行相应设置。

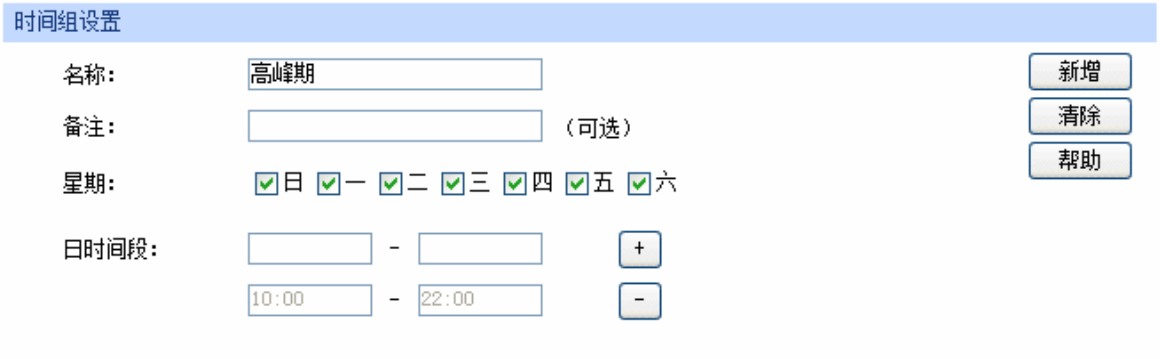
注意：

系统预定义的服务类型不可进行配置操作。

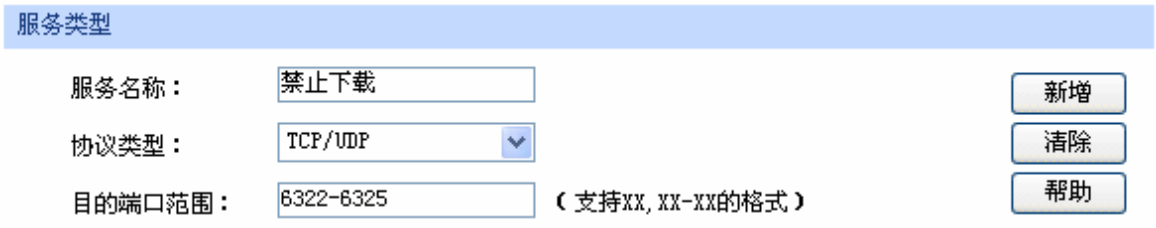
应用举例

需求：某企业为使网络顺畅运行，希望实现在上网高峰期（每天上午10点到晚上22点）禁止192.168.1.0/24网段内某下载工具（端口6322-6325）的使用，而在其它时间不限制该下载工具的使用。

此需求可以通过设置访问规则来实现。首先，需要新增一个时间组，名称为高峰期，设置时间10：00—22：00，设置完成后点击<新增>按钮保存生效。



然后，需要新增一个服务类型，设置6322-6325为服务端口，设置完成后点击<新增>按钮保存生效。



选择刚设置的“高峰期”时间组和“禁止下载”服务类型，新增一条禁止192.168.1.0/24网段通过6322-6325端口访问广域网的访问规则。最后点击<新增>按钮保存生效，完成设置。

4.5 行为管控

4.5.1 应用限制

4.5.1.1 应用限制

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 >> 应用限制 >> 应用限制

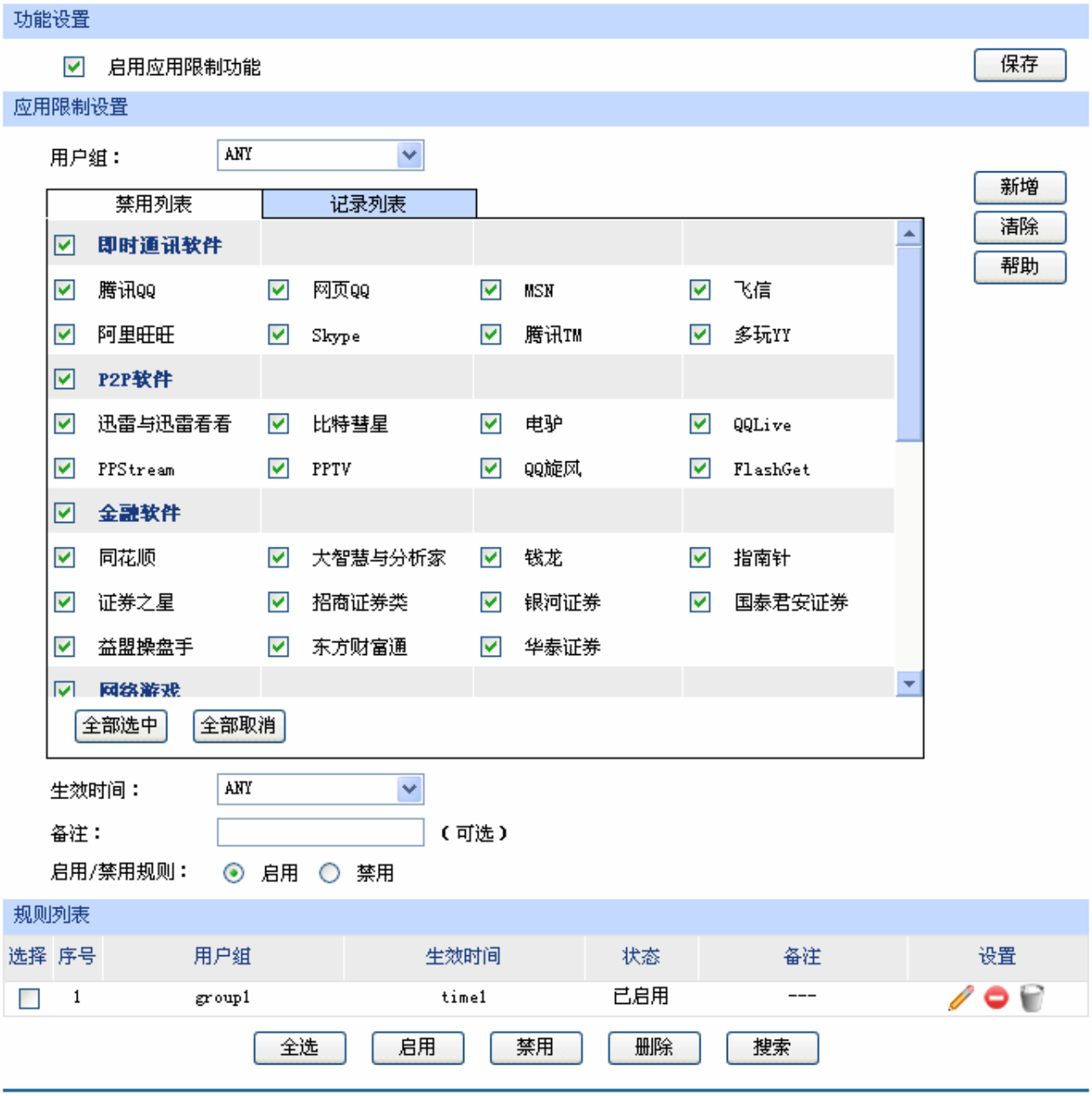


图 4-47 应用限制设置界面

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。

- **应用限制设置**

  用户组　　可以选择“ANY”，使规则对任意用户生效；也可以选择用户组，使规则仅对该组生效。如需新建组，请参考**4.2.1用户管理**。

禁用列表	勾选需要进行限制的应用，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。
记录列表	勾选进行日志记录的应用，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记录。
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**4.2.2时间管理**。
备注	添加对本条规则的说明信息。
启用/禁用规则	选择启用或禁用本条规则。

- **规则列表**

在规则列表中，可以对已保存的应用限制进行相应设置。

图 4-47序号1规则的含义：对用户组“group1”内的主机进行了应用限制，点击“禁用列表”可查看受限制的应用，点击“记录列表”可查看进行日志记录的应用。在时间组“time1”设置的时间段内应用限制生效。该规则已启用。

4.5.1.2 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 >> 应用限制 >> QQ黑白名单

图 4-48 QQ黑白名单界面

界面项说明：

- **全局设置**

  勾选“启用QQ黑白名单功能”后，QQ黑白名单的相关设置才会生效。

- **规则设置**

用户组	可以选择“ANY”，使规则对任意用户生效；也可以选择用户组，使规则仅对该组生效。如需新建组，请参考**4.2.1用户管理**。
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。

当使用上述QQ时	可以勾选“记录到系统日志”，系统将记录上述号码的使用情况；如果不勾选，系统将不对上述号码作记录。
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**4.2.2时间管理**。
备注	添加对本条规则的说明信息。
启用/禁用规则	选择启用或禁用本条规则。
指定位置	勾选该项后，可以将当前设置的条目添加到规则列表中指定序号的位置。默认情况下，新增规则会显示在规则列表的最后。

➢ **规则列表**

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

图 4-48序号1规则的含义：该规则已经启用，在用户组“group1”内的主机在时间组“time1”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在任意时间都是可登录的。

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 >> 用户管理

   进入标签页**组设置**，设置用户组名称：

   组名称 可使用QQ组

   进入标签页**用户设置**，设置用户IP地址，此处可进行批量添加，批量添加内容如下：

   操作 增加

   起始IP地址 10.1.1.30

   结束IP地址 10.1.1.35

   用户名前缀 可使用QQ用户

   起始序号 1

   步长 1

   进入标签页**视图**，将可使用QQ用户1-6移到可使用QQ组中。

   视图选择 组视图

   组名 可使用QQ组

   包含用户 可使用QQ用户1、可使用QQ用户2、可使用QQ用户3、可使用QQ用户4、可使用QQ用户5、可使用QQ用户6

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 >> 时间组

   时间组设置内容如下：

   名称 上班时间

   星期 一、二、三、四、五

日时间段　　08：00 - 18：00

设置完成后的时间组如下：

时间组列表

选择	序号	组名称	生效时间	备注	设置
☐	1	ANY	永久生效	---	---
☐	2	上班时间	一 二 三 四 五 08:00-18:00	---	

方法一设置如下：

界面进入方法：行为管控 >> 应用限制 >> QQ黑白名单

全局设置如下：

勾选“启用QQ黑白名单功能”，点击<保存>按钮使设置生效。

QQ黑名单规则设置内容如下：

用户组　　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

当使用上述QQ时　　勾选“记录到系统日志”

生效时间　　ANY

启用/禁用规则　　启用

QQ白名单规则设置内容如下：

用户组　　可使用QQ组

规则类型　　白名单：允许下列QQ号码登录

QQ号码　　允许登录的员工的QQ号码

当使用上述QQ时　　勾选“记录到系统日志”

生效时间　　上班时间

启用/禁用规则　　启用

指定位置　　勾选，输入1

设置完成后的规则如下：

规则列表

选择	序号	用户组	规则类型	生效时间	状态	备注	设置
☐	1	可使用QQ组	白名单	上班时间	已启用	---	
☐	2	ANY	黑名单	ANY	已启用	---	

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 >> 应用限制 >> 应用限制

功能设置如下：

勾选“启用应用限制功能”，点击<保存>按钮使设置生效。

应用限制设置内容如下：

用户组　　ANY

禁用应用列表　　腾讯QQ

记录应用列表　　腾讯QQ

生效时间　　ANY

启用/禁用规则　　启用

设置完成后的规则如下：

规则列表

选择	序号	用户组	禁用列表	记录列表	生效时间	状态	备注	设置
☐	1	ANY	查看	查看	ANY	已启用	---	

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 >> 应用限制 >> QQ黑白名单

全局设置如下：

勾选“启用QQ黑白名单功能”，点击<保存>按钮使设置生效。

QQ白名单规则设置内容如下：

用户组	可使用QQ组
规则类型	白名单：允许下列QQ号码登录
QQ号码	允许登录的员工的QQ号码
当使用上述QQ时	勾选“记录到系统日志”
生效时间	上班时间
启用/禁用规则	启用

设置完成后的规则如下：

规则列表

选择	序号	用户组	规则类型	生效时间	状态	备注	设置
☐	1	可使用QQ组	白名单	上班时间	已启用	---	

4.5.1.3 MSN黑白名单

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

界面进入方法：行为管控 >> 应用限制 >> MSN黑白名单

图 4-49 MSN黑白名单界面

界面项说明：

➢ **全局设置**

勾选“启用MSN黑白名单功能”后，MSN黑白名单的相关设置才会生效。

➢ **规则设置**

用户组 可以选择“ANY”，使规则对任意用户生效；也可以选择用户组，使规则仅对该组生效。如需新建组，请参考**4.2.1用户管理**。

规则类型 可以选择白名单，使规则中的账号不被限制；也可以选择黑名单，使规则中的账号被限制。

MSN账号 在此输入MSN账号，可以同时输入多个MSN账号进行批量添加，通过使用空格、逗号或者回车换行来表示不同的MSN账号。

当使用上述MSN时	可以勾选“记录到系统日志”，系统将记录上述账号的使用情况；如果不勾选，系统将不对上述账号作记录。
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**4.2.2时间管理**。
备注	添加对本条规则的说明信息。
启用/禁用规则	选择启用或禁用本条规则。
指定位置	勾选该项后，可以将当前设置的条目添加到规则列表中指定序号的位置。默认情况下，新增规则会显示在规则列表的最后。

➢ **规则列表**

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

图 4-49序号1规则的含义：该规则已经启用，在用户组“group1”内的主机在时间组“time1”设置的时间段内，被设置的MSN账号不可以登录。

说明：

- 在没有配置应用限制规则和MSN黑名单的情况下，路由器默认所有用户所有MSN账号在任意时间都是可登录的。
- 该功能应用与QQ黑白名单应用类似，可参考QQ黑白名单介绍后的应用举例。

4.5.2 网址过滤

4.5.2.1 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 4-50 网站分组设置界面

界面项说明：

➢ **网站分组设置**

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。

➢ **网站分组列表**

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。

说明：

若网站分组被网站过滤规则引用，则该网站分组只能修改不能删除。

4.5.2.2 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 4-51 网站过滤设置界面

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。

- **网站过滤设置**

用户组	可以选择“ANY”，使规则对任意用户生效；也可以选择用户组，使规则仅对该组生效。如需新建组，请参考**4.2.1用户管理**。
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<网站分组列表>，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**4.5.2.1网站分组**。
访问上述网站时	勾选“记录到系统日志”，规则条目生效时，符合规则的网站访问操作会被记录到系统日志； 勾选“弹出警告”，规则条目生效时，符合规则的网站访问操作发生时会弹出警告窗； 勾选“重定向至”并输入网站，规则条目生效时，符合规则的网站访问操作发生时会重定向到相应的网站。
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**4.2.2时间管理**。
备注	添加对本条规则的说明信息。
启用/禁用规则	选择启用或禁用本条规则。
指定位置	勾选该项后，可以将当前设置的条目添加到规则列表中指定序号的位置。默认情况下，新增规则会显示在规则列表的最后。

- **规则列表**

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

  图 4-51序号1规则的含义：对用户组“group1”内的主机进行了网站过滤，过滤规则是禁止访问网站分组，点击“查看”可在弹出的选择框中看到被禁止访问的网站分组。在时间组“time1”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。

4.5.2.3 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 4-52 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地址过滤规则**

用户组	可以选择“ANY”，使规则对任意用户生效；也可以选择用户组，使规则仅对该组生效。如需新建组，请参考**4.2.1用户管理**。
规则类型	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1-28个字符。
关键字	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。
URL地址	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。
访问上述URL时	勾选“记录到系统日志”，规则条目生效时，符合规则的URL访问操作会被记录到系统日志； 勾选“弹出警告”，规则条目生效时，符合规则的网站访问操作发生时会弹出警告窗； 勾选“重定向至”并输入网站，规则条目生效时，符合规则的URL访问操作发生时会重定向到相应的网站。
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**4.2.2时间管理**。
备注	添加对本条规则的说明信息。
启用/禁用规则	选择启用或禁用本条规则。

指定位置	勾选该项后，可以将当前设置的条目添加到规则列表中指定序号的位置。默认情况下，新增规则会显示在规则列表的最后。

➢ **规则列表**

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

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”，如下图所示，设置完成后点击<新增>按钮保存生效。

4.5.3 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 4-53 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。

- **规则设置**

用户组	可以选择“ANY”，使规则对任意用户生效；也可以选择用户组，使规则仅对该组生效。如需新建组，请参考**4.2.1用户管理**。
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**4.2.2时间管理**。
备注	添加对本条规则的说明信息。
启用/禁用规则	选择启用或禁用本条规则。

➢ **规则列表**

在规则列表中，可以对已保存的规则进行相应设置。

图 4-53序号1规则的含义：对用户组“group1”内的主机设置了网页安全，组内所有主机在“time1”设置的时间段内，都不能下载扩展类型为exe的文件。

4.5.4 行为审计

可以在此查看行为审计参数配置。

界面进入方法：行为管控 >> 行为审计 >> 行为审计

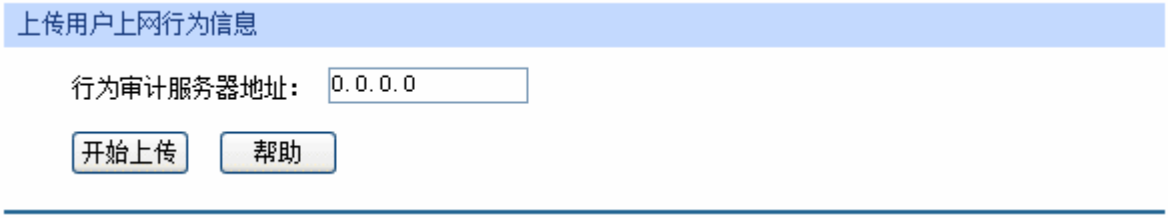


图 4-54 行为审计界面

若需要在某台主机上查看用户上网行为信息，请首先在这台主机上安装TP-LINK上网行为审计软件，然后在图 4-54行为审计界面输入该服务器IP地址，点击<开始上传>按钮之后，路由器会立即将用户上网行为信息实时上传至该服务器，并通过TP-LINK上网行为审计软件输出审计结果。

本产品随机附带的光盘内有TP-LINK上网行为审计软件，可以通过光盘直接安装该软件。如不慎遗失或光盘内没有此软件，请联系TP-LINK售后服务人员。

4.5.5 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

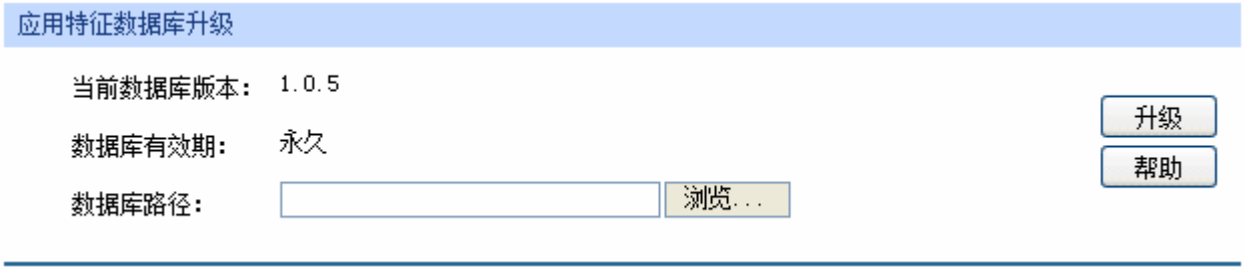


图 4-55 策略库升级界面

应用特征数据库即“应用限制”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，单击<浏览>按钮，选择保存路径下的文件，点击<升级>进行数据库升级。

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。

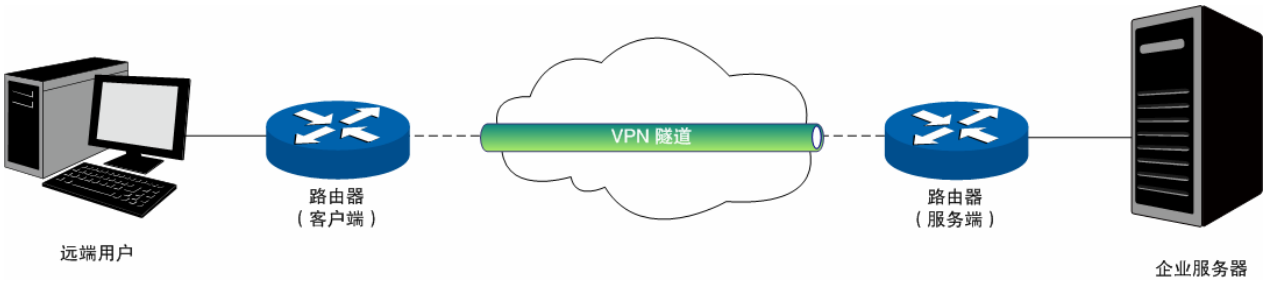


图 4-56 VPN典型拓扑

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-ER6110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 IKE

在IPsec VPN中，为了保证信息的私密性，通信双方需要使用彼此都知道的信息来对数据进行加密和解密，所以在通信建立之初双方需要协商安全性密钥，这一过程便由IKE (Internet Key Exchange, 互联网密钥交换)协议完成。

IKE其实并非一个单独的协议，而是三个协议的混合体。这三个协议分别是ISAKMP (Internet Security Association and Key Management Protocol, 互联网安全性关联和密钥管理协议)，该协议为交换密钥和SA (Security Association, 安全联盟)协商提供了一个框架；Oakley密钥确定协议，该协议描述了密钥交换的具体机制；SKEME安全密钥交换机制，该协议描述了与Oakley不同的另一种密钥交换机制。

整个IKE协商过程被分为两个阶段。第一阶段，通信双方将协商交换验证算法、加密算法等安全提议，并建立一个ISAKMP SA，用于在第二阶段中安全交换更多信息。第二阶段，使用第一阶段中建立的ISAKMP SA为IPsec的安全性协议协商参数，创建IPsec SA，用于对双方的通信数据进行保护。至此，IKE协商完毕。

4.6.1.1 IKE安全策略

在TL-ER6110路由器上，可以对IKE协商过程的相关参数进行设置。

界面进入方法：**VPN >> IKE >> IKE安全策略**

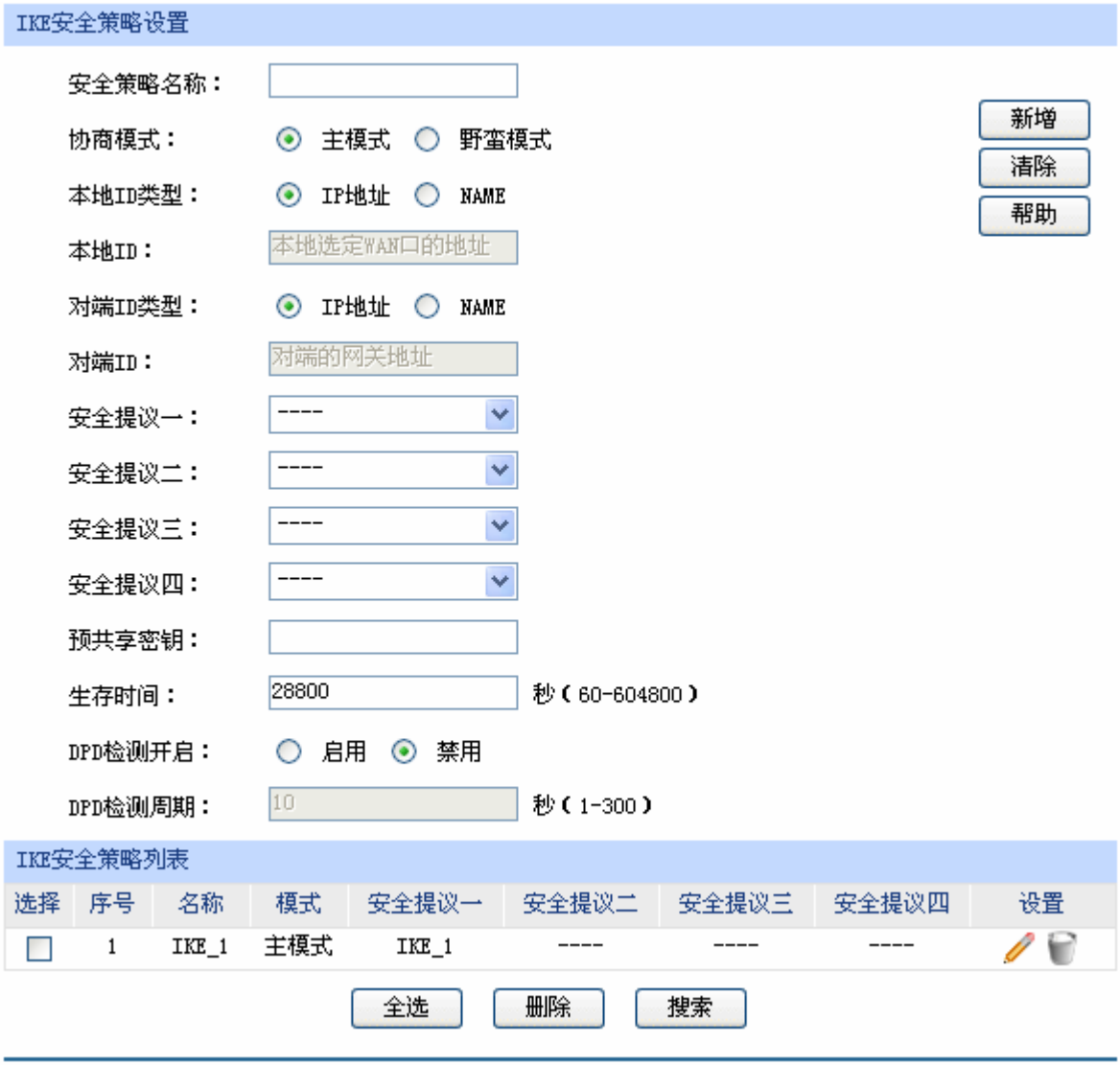


图 4-57 IKE安全策略设置界面

界面项说明：

- **IKE安全策略设置**

安全策略名称	为IKE安全策略命名。设置好的IKE安全策略可以被应用在IPsec安全策略中。
协商模式	选择IKE的协商模式，通信双方必须使用相同的协商模式。在IKE协商的第一阶段定义了两种操作模式：主模式和野蛮模式。主模式中进行交换和认证的报文较多，并提供身份保护，适用于高安全性需求场合；野蛮模式中进行交换和认证的报文较少，不提供身份保护，但是协商速度快。

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。
安全提议	选择用于IKE协商第一阶段的安全提议，如果下拉菜单中没有想选择的条目，请进入**4.6.1.2 IKE安全提议**页面创建新条目。主模式下，最多可以选择四条不同的安全提议；野蛮模式下，可以选择一条安全提议。
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。
生存时间	设定ISAKMP 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。

- **IKE安全策略列表**

在IKE安全策略列表中，可以对已保存的IKE安全策略进行相应设置。

4.6.1.2 IKE安全提议

界面进入方法：VPN >> IKE >> IKE安全提议

图 4-58 IKE安全提议设置界面

界面项说明：

- **IKE安全提议设置**

安全提议名称	为IKE安全提议命名。设置好的IKE安全提议可以被应用在IKE安全策略中。
验证算法	选择应用于IKE会话的验证算法。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。
加密算法	选择应用于IKE会话的加密算法。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。

- **IKE安全提议列表**

在IKE安全提议列表中，可以对已保存的IKE安全提议进行相应设置。

4.6.2 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。

4.6.2.1 IPsec安全策略

界面进入方法：VPN >> IPsec >> IPsec安全策略

图 4-59 IPsec安全策略设置界面

界面项说明：

- **启用IPsec功能**

  只有勾选“启用”后，路由器才能应用IPsec。

- **IPsec安全策略设置**

  安全策略名称　　为IPsec安全策略命名。

  启用安全策略　　选择启用或禁用当前策略条目。

组网模式	站点到站点：对端为子网。 PC到站点：对端为主机。
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。当组网模式选择为PC到站点时，该项不可填。
对端网关	当组网模式选择为站点到站点，请在此输入通信对端的路由器相应WAN口的IP地址或域名。
对端主机	当组网模式选择为PC到站点，请在此输入通信对端主机的IP地址。默认为0.0.0.0，表示任意IP地址。
协商方式	建立IPsec安全隧道可以有两种协商方式。IKE为自动协商，手动模式则需手动设定相关的安全参数。
IKE安全策略	选择“IKE协商”时，可以指定相应的IKE安全策略。如果下拉菜单中没有想选择的条目，请进入**4.6.1.1 IKE安全策略**页面创建新条目。
安全提议	指定相应的IPsec安全提议。如果下拉菜单中没有想选择的条目，请进入**4.6.2.2 IPsec安全提议**页面创建新条目。
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。
入SPI	选择“手动模式”时，可以设定SPI参数。SPI与隧道对端网关地址、协议类型三个参数共同标识一个IPsec安全联盟，通信对端的“出SPI”值必须与此值相同。
入AH MD5密钥	当安全提议指定IPsec使用“AH”协议时，可以设定AH MD5验证算法的密钥。通信对端的“出 AH MD5密钥”必须与此值相同。

入ESP MD5密钥	当安全提议指定IPsec使用“ESP”协议时，可以设定ESP MD5验证算法的密钥。通信对端的“出 ESP MD5密钥”必须与此值相同。
入ESP 3DES密钥	当安全提议指定IPsec使用“ESP”协议时，可以设定ESP 3DES加密算法的密钥。通信对端的“出 ESP 3DES密钥”必须与此值相同。
出SPI	选择“手动模式”时，可以设定SPI参数。SPI参数唯一标识一个IPsec安全联盟，通信对端的“入SPI”值必须与此值相同。
出AH MD5密钥	当安全提议指定IPsec使用“AH”协议时，可以设定AH MD5验证算法的密钥。通信对端的“入 AH MD5密钥”必须与此值相同。
出ESP MD5密钥	当安全提议指定IPsec使用“ESP”协议时，可以设定ESP MD5验证算法的密钥。通信对端的“入 ESP MD5密钥”必须与此值相同。
出ESP 3DES密钥	当安全提议指定IPsec使用“ESP”协议时，可以设定ESP 3DES加密算法的密钥。通信对端的“入 ESP 3DES密钥”必须与此值相同。

- **IPsec安全策略列表**

在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。

图 4-59序号1条目的含义：这是一条IPsec的隧道，组网模式为站点到站点，本地子网范围是192.168.1.0/24，对端子网范围是192.168.2.0/24，隧道使用IKE自动协商，该隧道已启用。

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**.

4.6.2.2 IPsec安全提议

界面进入方法：VPN >> IPsec >> IPsec安全提议

图 4-60 IPsec安全提议设置界面

界面项说明：

➢ **IPsec安全提议设置**

安全提议名称　为IPsec安全提议命名。设置好的IPsec安全提议可以被应用在IPsec安全策略中。

安全协议　选择要使用的协议。

AH验证算法　当选择AH安全协议时可设定AH验证算法。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。

ESP验证算法　当选择ESP安全协议时可设定ESP验证算法。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。

ESP加密算法

当选择ESP安全协议时可设定ESP加密算法。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128/192/256bit的密钥进行加密。

➢ **IPsec安全提议列表**

在IPsec安全提议列表中，可以对已保存的IPsec安全提议进行相应设置。

4.6.2.3 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	303042544	in	172.30.70.151<- 172.30.70.161	192.168.1.0/24<- 192.168.3.0/24	ESP	---	MD5	3DES
2	IPsec_1	352312306	out	172.30.70.151->172.30.70.161	192.168.1.0/24->192.168.3.0/24	ESP	---	MD5	3DES

刷新 搜索 帮助

图 4-61 IPsec安全联盟界面

图 4-61中显示的是图 4-59中IPsec安全策略列表序列1条目的连接情况。在本例中路由器WAN口的IP地址为172.30.70.151，对端网关地址为172.30.70.161。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。

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	352312306	in	172.30.70.161<- 172.30.70.151	192.168.3.0/24<- 192.168.1.0/24	ESP	---	MD5	3DES
2	IPsec_1	303042544	out	172.30.70.161->172.30.70.151	192.168.3.0/24->192.168.1.0/24	ESP	---	MD5	3DES

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-ER6110目前仅在IKE协商模式为野蛮模式，且本地和对端的ID类型都为NAME的情况下支持NAT穿透。

4.6.3 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，并为数据增添额外首部。

4.6.3.1 L2TP服务器

界面进入方法：VPN >> L2TP >> L2TP服务器

图 4-62 L2TP服务器设置界面

界面项说明：

- **全局管理设置**

勾选“启用VPN-to-Internet通道”，可以允许VPN拨号用户在访问VPN网络的同时访问互联网。

链路维护时间间隔	设置发送链路维护检测报文的时间间隔。
首选DNS服务器地址	设置服务器的首选DNS地址，分配给客户端。
备用DNS服务器地址	设置服务器的备用DNS地址，分配给客户端。

- **隧道设置**

启用/禁用	选择启用或禁用当前L2TP隧道条目。
名称	设置L2TP隧道的名称，方便区分不同的隧道。
用户名	设置L2TP认证的用户名。客户端与服务器端的设置需一致。
密码	设置L2TP认证的密码。客户端与服务器端的设置需一致。
组网模式	当连入隧道的用户为接入路由器的一个网段时，请选择“站点到站点”模式；当连入隧道的用户是单个计算机时，请选择“PC到站点”模式。
最大连接数	当组网模式选择“PC到站点”时，可进行隧道容纳最大连接数的设置。
加密状态	单纯的L2TP隧道安全性仍然不高，可以选择是否对隧道进行加密。本路由将使用IPsec对L2TP隧道进行加密。
预共享密钥	设置用于L2TP隧道加密的IPsec预共享密钥，隧道双方必须使用同一个预共享密钥。
客户端地址	启用加密时，可以设置允许连接到本路由器的客户端IP地址。默认为0.0.0.0，表示所有IP地址。
地址池名称	选择分配给客户端的静态IP地址范围。如果下拉菜单中没有想选择的条目，请进入**4.6.3.4隧道地址池管理**页面创建新条目。

对端子网范围	当组网模式选择“站点到站点”时，输入隧道对端的地址，以子网掩码值划分地址范围。

➢ **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。

图 4-62序号1条目的含义：这条L2TP隧道名称为l2tp1，用户名为l2tp，密码自设，组网模式为站点到站点，地址池名称是l2tp_pool1，对端子网为192.168.2.0/24，目前该条目已生效。

说明：

- 若要使L2TP VPN的加密功能生效，请先启用IPsec功能。
- 当组网模式为“PC到站点”时，只允许添加一条客户端地址为“0.0.0.0”的条目。
- 当路由器中存在对端网关为“0.0.0.0”的IPsec VPN条目时，L2TP VPN不能再添加客户端地址为“0.0.0.0”的条目。

4.6.3.2 L2TP客户端

界面进入方法：VPN >> L2TP >> L2TP客户端

图 4-63 L2TP客户端设置界面

界面项说明：

➢ **隧道设置**

启用/禁用	选择启用或禁用当前L2TP/PPTP隧道条目。
名称	设置L2TP隧道的名称，方便区分不同的隧道。
用户名	设置L2TP认证的用户名。客户端与服务器端的设置需一致。
密码	设置L2TP认证的密码。客户端与服务器端的设置需一致。
隧道服务器地址	设置隧道服务器地址，若服务器端为路由器则填入其WAN口IP地址。
加密状态	单纯的L2TP隧道安全性仍然不高，可以选择是否对隧道进行加密。本路由将使用IPsec对L2TP隧道进行加密。
预共享密钥	设置用于L2TP隧道加密的IPsec预共享密钥，隧道双方必须使用同一个预共享密钥。
对端子网范围	输入隧道对端的地址，以子网掩码值划分地址范围。

➢ **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。

图 4-63序号1条目的含义：这条L2TP隧道名称为zhangsan，用户名为user1，隧道服务器地址为172.30.70.161，对端子网为192.168.3.0/24，目前该条目已生效。

说明：

若要使L2TP VPN的加密功能生效，请先启用IPsec功能。

4.6.3.3 L2TP隧道信息

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 >> L2TP隧道信息

隧道信息列表

序号	用户名	工作模式	隧道ID	会话ID	对端地址	对端主机	状态	断开连接
1	l2tp	服务器	35,1	18,1	192.168.2.2	tplink16894	已连接	

刷新 搜索 帮助

图 4-64 L2TP隧道信息界面

图 4-64中显示的是图 4-62中隧道设置列表序列1条目的连接情况。目前这条隧道已成功建立，每条隧道会产生隧道ID数值对和会话ID数值对，每个数值对都由两个数字ID组成，客户端和服务器端显示的数值对是对应的。这条隧道在客户端的连接信息如下图所示：

每次建立隧道连接时都会生成一组隧道ID和一组会话ID，一般情况下，同一路由器上不同隧道的ID数值对不会相同，即使是同一条隧道，在断开已有连接后重新建立连接，也可能会产生不同的ID数值对。

4.6.3.4 隧道地址池管理

界面进入方法：VPN >> L2TP >> 隧道地址池管理

图 4-65 隧道地址池管理界面

界面项说明：

- **地址池设置**

  启用/禁用 选择启用或禁用本地址池。

  地址池名称 为地址池命名。设置好的地址池名称可以被应用在隧道设置中。

  地址池范围 设置分配给客户端的IP地址范围。

- **地址池列表**

  在地址池列表中，可以对已保存的地址池进行相应设置。

说明：

- L2TP和PPTP地址池总数最大为10个。
- L2TP地址池范围不能与PPTP、LAN/WAN/DMZ、PPPoE服务器冲突。

4.6.4 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，并为数据增添额外首部。

4.6.4.1 PPTP服务器

界面进入方法：VPN >> PPTP >> PPTP服务器

图 4-66 PPTP服务器设置界面

界面项说明：

➢ **全局管理设置**

勾选“启用VPN-to-Internet通道”，可以允许VPN拨号用户在访问VPN网络的同时访问互联网。

链路维护时间间隔	设置发送链路维护检测报文的时间间隔。
首选DNS服务器地址	设置服务器的首选DNS地址，分配给客户端。
备用DNS服务器地址	设置服务器的备用DNS地址，分配给客户端。

- **隧道设置**

启用/禁用	选择启用或禁用当前PPTP隧道条目。
名称	设置PPTP隧道的名称，方便区分不同的隧道。
用户名	设置PPTP认证的用户名。客户端与服务器端的设置需一致。
密码	设置PPTP认证的密码。客户端与服务器端的设置需一致。
组网模式	当连入隧道的用户为接入路由器的一个网段时，请选择“站点到站点”模式；当连入隧道的用户是单个计算机时，请选择“PC到站点”模式。
最大连接数	当组网模式选择“PC到站点”时，可进行隧道容纳最大连接数的设置。
加密状态	选择是否对隧道进行加密。若启用，则使用MPPE对PPTP隧道加密。
地址池名称	选择分配给客户端的静态IP地址范围。如果下拉菜单中没有想选择的条目，请进入**4.6.4.4隧道地址池管理**页面创建新条目。
对端子网范围	当组网模式选择“站点到站点”时，输入隧道对端的地址，以子网掩码值划分地址范围。

- **隧道设置列表**

在隧道设置列表中，可以对已保存的PPTP隧道信息进行相应设置。

图 4-66序号1条目的含义：这条PPTP隧道名称为pptp1，用户名为pptp，密码自设，组网模式为站点到站点，地址池名称是pptp_pool1，对端子网为172.31.85.0/24，目前该条目已生效。

4.6.4.2 PPTP客户端

界面进入方法：VPN >> PPTP >> PPTP客户端

图 4-67 PPTP客户端设置界面

界面项说明：

- **隧道设置**

启用/禁用	选择启用或禁用当前L2TP/PPTP隧道条目。
名称	设置PPTP隧道的名称，方便区分不同的隧道。
用户名	设置PPTP认证的用户名。客户端与服务器端的设置需一致。
密码	设置PPTP认证的密码。客户端与服务器端的设置需一致。
隧道服务器地址	设置隧道服务器地址，若服务器端为路由器则填入其WAN口IP地址。
加密状态	选择是否对隧道进行加密。若启用，则使用MPPE对PPTP隧道加密。
对端子网范围	输入隧道对端的地址，以子网掩码值划分地址范围。

- **隧道设置列表**

在隧道设置列表中，可以对已保存的PPTP隧道信息进行相应设置。

图 4-67序号1条目的含义：这条PPTP隧道名称为tplink1，用户名为user，隧道服务器地址为172.30.70.1，对端子网为192.168.5.0/24，目前该条目已生效。

4.6.4.3 PPTP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 >> PPTP隧道信息

图 4-68 PPTP隧道信息界面

图 4-68中显示的是图 4-66中隧道设置列表序列1条目的连接情况。目前这条隧道已成功建立，每条隧道会产生CALL ID数值对，每个数值对都由两个数字ID组成，客户端和服务器端显示的数值对是对应的。这条隧道在客户端的连接信息如下图所示：

每次建立隧道连接时都会生成一组CALL ID数值对，一般情况下，同一路由器上不同隧道的ID数值对不会相同，即使是同一条隧道，在断开已有连接后重新建立连接，也可能会产生不同的ID数值对。

4.6.4.4 隧道地址池管理

界面进入方法：VPN >> PPTP >> 隧道地址池管理

图 4-69 隧道地址池管理界面

界面项说明：

➢ **地址池设置**

启用/禁用	选择启用或禁用本地址池。
地址池名称	为地址池命名。设置好的地址池名称可以被应用在隧道设置中。
地址池范围	设置分配给客户端的IP地址范围。此地址池不能与当前路由器LAN网段及DMZ网段、对端路由器LAN网段及DMZ网段重复。

➢ **地址池列表**

在地址池列表中，可以对已保存的地址池进行相应设置。

说明：

- L2TP和PPTP地址池总数最大为10个。
- PPTP地址池范围不能与L2TP、LAN/WAN/DMZ、PPPoE服务器冲突。

4.7 系统服务

4.7.1 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。

4.7.1.1 全局设置

可以在此开启PPPoE服务器功能，并对其全局参数进行设置。

界面进入方法：系统服务 >> PPPoE服务器 >> 全局设置

图 4-70 全局设置界面

界面项说明：

➢ **全局设置**

PPPoE服务器	选择启用或禁用PPPoE服务器功能。
强制PPPoE拨号	选择是否强制局域网内所有用户通过PPPoE拨号连网。在启用模式下，如有特殊用户，可点击右侧<例外IP>按钮进行设置。
拨号用户互访	选择是否允许通过PPPoE拨号连入的用户之间互相通信。
首选DNS服务器地址	设置分配给PPPoE用户的DNS地址，建议与WAN口的DNS地址一致。
备用DNS服务器地址	设置分配给PPPoE用户的备用DNS地址，建议与WAN口的备用DNS地址一致。
系统最大会话数	设置同一时间系统允许的PPPoE连接会话的最大值，默认参数为256。
最大未应答LCP包数	LCP（Link Control Protocol， 链路控制协议）用于检查PPPoE通信双方在数据传输过程中的一些必要信息。当客户端未应答PPPoE服务器发出的LCP包达到最大值后，将自动断开链接。该值可以留空，默认参数为10。

空闲断线时间	设置在没有数据传输时的自动断线时间。时间范围为0~10080分钟，0分钟表示永不断线，10080分钟即7天。默认为30分钟。
认证方式	选择PPPoE拨号用户的认证方式。在PPPoE服务器端进行认证可以选择“本地认证”；在远端认证服务器上进行认证则可选择“远程认证”。
本地认证	选择本地认证的方法。本路由器提供4中认证方法，请至少选择一项。PAP协议在网络上明文传送用户名及密码，适用于网络安全需求较低的环境；CHAP协议使用三次握手过程，而且不会明文传送密码，因此安全性能较高；MS-CHAP协议是微软提出的认证方式，在密码加密的算法上与CHAP不同；MS-CHAP v2协议是在MS-CHAP基础上的改进版本，安全性比MS-CHAP要高。
Radius服务器地址	当选择“远程认证”方式时，会出现该条目。RADIUS（Remote Authentication Dial In User Service，远程用户拨号认证服务）提供对拨号用户的身份认证，请在此设置认证服务器IP地址。
共享密钥	设置用于Radius认证的共享密钥，需与Radius服务器的共享密钥一致。密钥由64位的ASCⅡ码组成。

4.7.1.2 地址池管理

界面进入方法：系统服务 >> PPPoE服务器 >> 地址池管理

图 4-71 地址池管理设置界面

界面项说明：

➢ **地址池设置**

地址池名称 为地址池命名。设置好的地址池名称可以被应用在账号管理中。该名称不能与L2TP/PPTP的VPN隧道地址池名称重复。

地址池范围 设置分配给PPPoE拨号用户的IP地址范围。该范围不能与L2TP/PPTP的VPN隧道地址池范围重叠。

➢ **地址池列表**

在地址池列表中，可以对已保存的地址池进行相应设置。

4.7.1.3 账号管理

可以在此对PPPoE拨号用户的账号进行设置。

界面进入方法：系统服务 >> PPPoE服务器 >> 账号管理

图 4-72 账号管理设置界面

界面项说明：

➢ **账号设置**

账号 设置账号名称。该名称不能与WAN口设置中的L2TP或PPTP连接方式的账号名称重复。

密码 设置账号密码。

地址分配方式	选择该账号用户的IP地址分配方式。
地址池	选择“动态分配”方式时，请通过下拉菜单选择地址池。
静态IP地址	选择“静态分配”方式时，请在此输入将要分配给该账号的IP地址。
最大会话数	设置同一时间系统允许的单个账号连接会话的最大值，默认参数为1。
账号到期时间	设置该账号的到期时间，默认为2099年1月1日。
备注	添加对本账号条目的说明信息。
启用/禁用规则	设置该账号条目是否生效。
启用高级账号设置	勾选此项可对账号进行更多设置。
MAC绑定方式	请在下拉菜单中选择MAC绑定方式。“不绑定”表示账号可以在任何一台主机上登录，“静态绑定”可以手动设置绑定该账号对应的MAC地址；“动态绑定”则由路由器记录账号首次登录时的MAC地址，并与账号绑定。开启MAC绑定后，最大会话数将强制变为1。
MAC地址	仅当选择“静态绑定”方式时，该项可编辑。当绑定了MAC地址后，该账号将只能在此MAC地址主机上登录。
定时断线设置	设置定时断线时间，如果为0表示永不断线。默认参数为48小时，若没有勾选“启用高级账号设置”，则默认为0小时。

- **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。

4.7.1.4 例外IP管理

在强制使用PPPoE拨号才能访问网络的时候，如果有个别主机不受限制，则可在此进行例外设置。

界面进入方法：系统服务 >> PPPoE服务器 >> 例外IP管理

图 4-73 例外IP管理设置界面

界面项说明：

➢ **例外IP设置**

IP地址范围	设置不受PPPoE强制拨号限制的IP地址范围，可以是IP地址段也可以是单个IP地址。该地址范围必须在路由器LAN口或DMZ口网段中。
备注	添加对本条目的说明信息。
启用/禁用规则	设置本条目是否生效。

➢ **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。

4.7.1.5 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 4-74 账号信息列表界面

图 4-74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。

4.7.2 电子公告

通过电子公告功能可向局域网内指定用户组发送公告消息。

4.7.2.1 公告设置

可以在此启用电子公告功能，编辑公告内容并向指定用户发送。

界面进入方法：系统服务 >> 电子公告 >> 公告设置

图 4-75 公告设置界面

界面项说明：

- **综合设置**

  勾选“启用电子公告功能”后，设置的公告才会生效，局域网用户在访问外网网页时将会收到公告消息。公告周期可以让路由器每隔指定的时间发布一次公告，周期时常不能小于5分钟。

  勾选“启用日志记录”后路由器会记录相关的公告日志。

➢ **公告设置**

标题	输入公告的标题。
内容	输入公告的内容。
公告对象	指定被公告的局域网内对象。可以选择“组”作为公告对象，也可以选择“ANY”将所有IP作为公告对象。
组	当公告对象为“组”的时候，可进行如下操作。如果需要添加组，请选中组并点击< >> >按钮将其移至“已选组列表”中，如果需要删除某个已选组，请选中组后点击< << >按钮将其移回“可选组列表”。如需新建组，请参考**4.2.1用户管理**。
生效时间	指定规则生效时间，其他时间规则不生效。由时间管理的时间组来表示。如需新建时间组，请参考**4.2.2时间管理**。
发布者	输入公告发布者名称。
备注	添加对本条规则的说明信息。
是否生效	选择当前设置规则是否生效。

➢ **公告列表**

在公告列表中，可以对已保存的公告规则进行相应设置。

图 4-75序号1规则的含义：这是一条由管理员发布的公告，路由器“time1”时间段内，每隔一个公告周期的时间（图中的公告周期为60分钟）就对研发部发布一次公告，本条规则已生效。

4.7.3 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客户端和3322动态DNS客户端。

4.7.3.1 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 4-76 花生壳动态域名设置界面

界面项说明：

➢ **功能设置**

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。

服务开关 选择启用或禁用花生壳动态域名服务。

服务类型 服务启用之后，显示当前登录的DDNS账号是属于专业服务还是标准服务。这取决于您在注册时选择的服务类型。

连接状态 显示DDNS的工作状态。

“服务没有运行”表示DDNS功能未启用；

“服务连接中，请等候”表示系统正在连接DDNS服务器；

“服务已运行”表示DDNS工作正常；

“用户名或密码错误”表示输入的用户名或密码有误，请重新输入正确的值后再启用DDNS。

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。

- **管理列表**

在管理列表中，可以对当前的DDNS条目进行相应设置。

4.7.3.2 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 4-77 科迈动态域名设置界面

界面项说明：

- **功能设置**

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。

服务开关　选择启用或禁用科迈动态域名服务。

连接状态　显示DDNS的工作状态。

“服务没有运行”表示DDNS功能未启用；

“服务连接中”表示系统正在连接DDNS服务器；

“服务已运行”表示DDNS工作正常；

“用户名或密码错误”表示输入的用户名或密码有误，请重新输入正确的值后再启用DDNS。

域名信息	显示当前登录的DDNS用户所拥有的域名。

➢ **管理列表**

在管理列表中，可以对当前的DDNS条目进行相应设置。

说明:

如果多次登录失败，请在10分钟后再尝试登录。

4.7.3.3 3322动态域名

界面进入方法：系统服务 >> 动态DNS >> 3322动态域名

图 4-78 3322动态域名设置界面

界面项说明：

➢ **功能设置**

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	填入登录3322动态域名服务的域名。
服务开关	选择启用或禁用3322动态域名服务。
连接状态	显示DDNS的工作状态。 “服务没有运行”表示DDNS功能未启用； “服务连接中”表示系统正在连接DDNS服务器； “服务已运行”表示DDNS工作正常； “用户名、密码错误”表示输入的用户名、密码或域名有误，请重新输入正确的值后再启用DDNS。

➢ **管理列表**

在管理列表中，可以对当前的DDNS条目进行相应设置。

4.7.4 UPnP服务

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。例如，Windows XP和Windows ME系统上安装的MSN Messenger，在使用音频和视频通话时就可以利用UPnP协议。

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服务 >> UPnP服务

图 4-79 UPnP服务设置界面

界面项说明：

- **功能设置**

UPnP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，TL-ER6110可以同时支持64条UPnP服务，并对已有规则进行相应设置。

图 4-79序号1条目的含义：在路由器WAN口的12856端口接收到的TCP数据，将转发到局域网服务器192.168.1.101的12856端口上。

注意：

- 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MSN最新版、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 系统工具

4.8.1 设备管理

4.8.1.1 修改管理帐号

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 >> 设备管理 >> 修改管理帐号

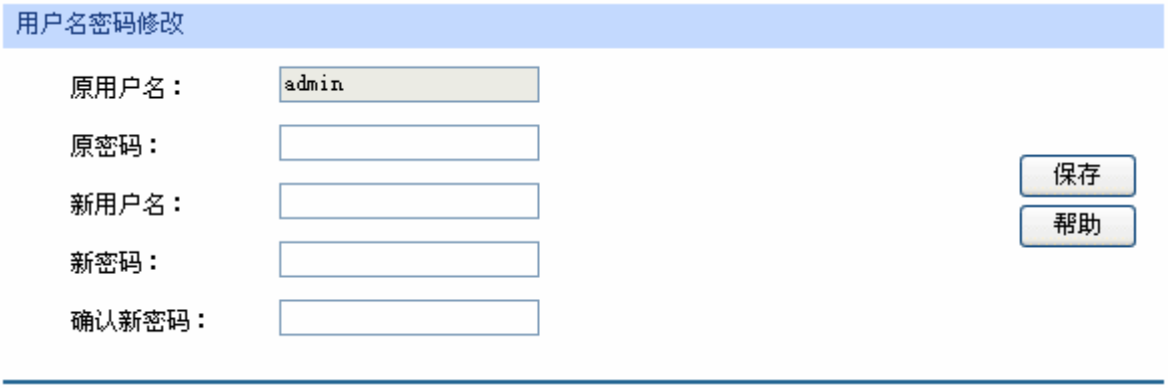


图 4-80 修改管理帐号界面

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:

出厂的用户名/密码是admin/admin。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，且只能是数字和字母，区分大小写。

4.8.1.2 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 >> 设备管理 >> 远程管理

图 4-81 远程管理设置界面

界面项说明：

➢ **远程管理地址**

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。
启用/禁用规则	选择启用或禁用该规则。

➢ **地址列表**

在地址列表中，可以对已保存的远程管理地址条目进行相应设置。

图 4-81序号1条目的含义：允许IP地址属于172.31.70.0/24网段的主机登录路由器Web界面，该规则已启用。

4.8.1.3 系统管理设置

可以在服务端口界面对Web、Telnet服务的端口进行设置和修改。

界面进入方法：系统工具 >> 设备管理 >> 系统管理设置

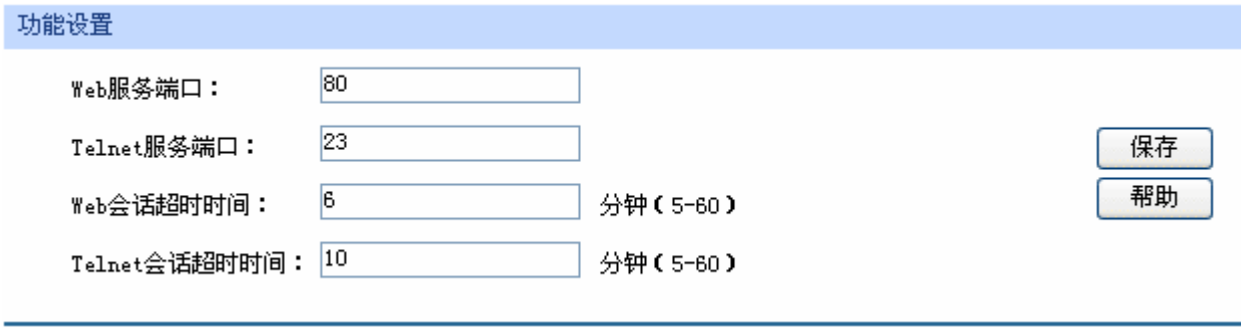


图 4-82 系统管理设置界面

界面项说明：

➢ **功能设置**

Web服务端口	设置路由器的Web服务端口。
Telnet服务端口	设置路由器的Telnet服务端口。
Web会话超时时间	设置通过Web页面访问路由器的超时时间。登录Web界面后，用户在该设定时间内如无任何操作，路由器将自动断开连接。
Telnet会话超时时间	设置通过Telnet远程访问路由器的超时时间，远程登录路由器后，用户在该设定时间内如无任何指令，路由器将自动断开连接。

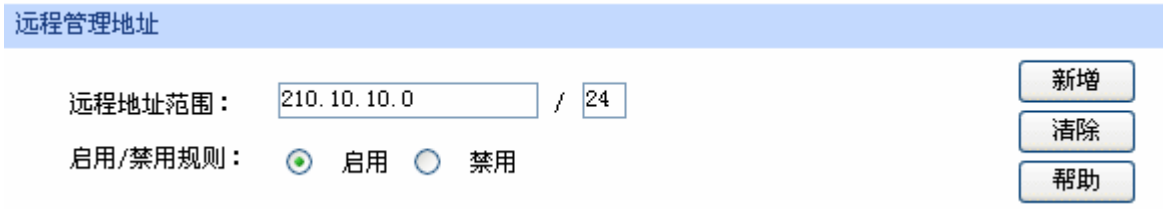
注意：

- 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，如下图所示：



在服务端口界面为Web服务器开放相应的服务端口，设置如下图所示：

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。

4.8.1.4 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

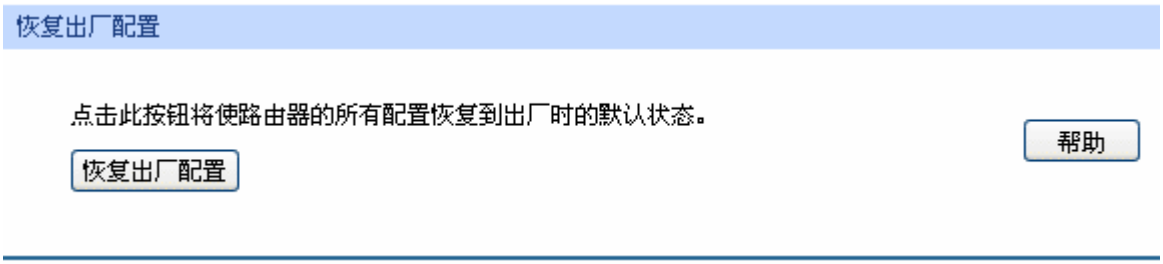


图 4-83 恢复出厂配置界面

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，用户名/密码为admin/admin。

4.8.1.5 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

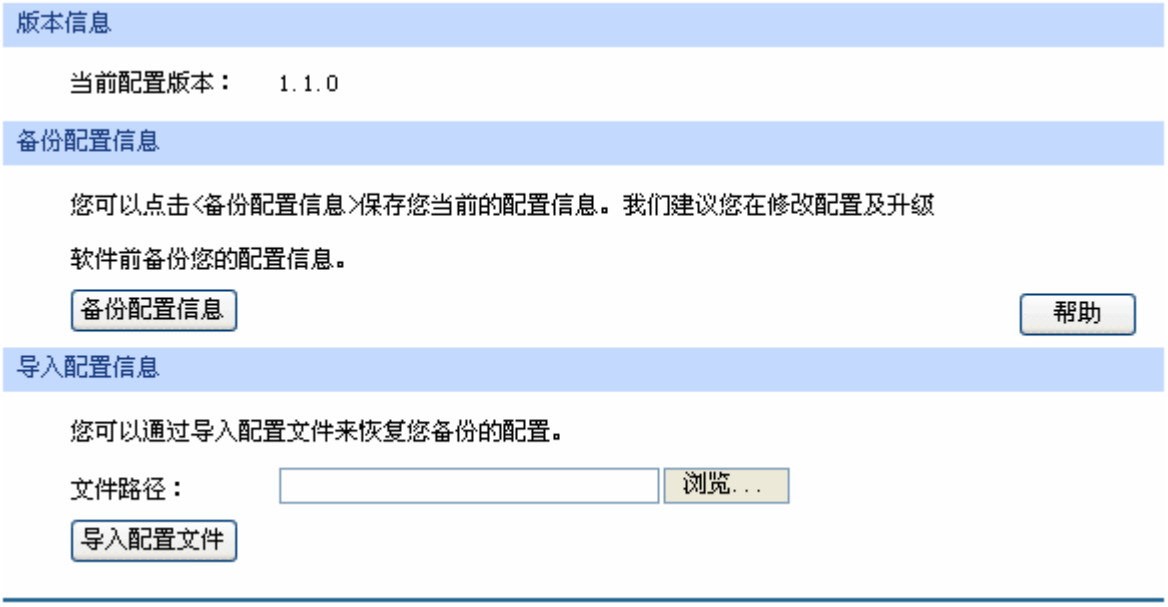


图 4-84 备份与导入配置界面

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<备份配置信息>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<导入配置文件>按钮，将路由器恢复到以前备份的配置状态。

注意：

- 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。

4.8.1.6 重启路由器

界面进入方法：系统工具 >> 设备管理 >> 重启路由器

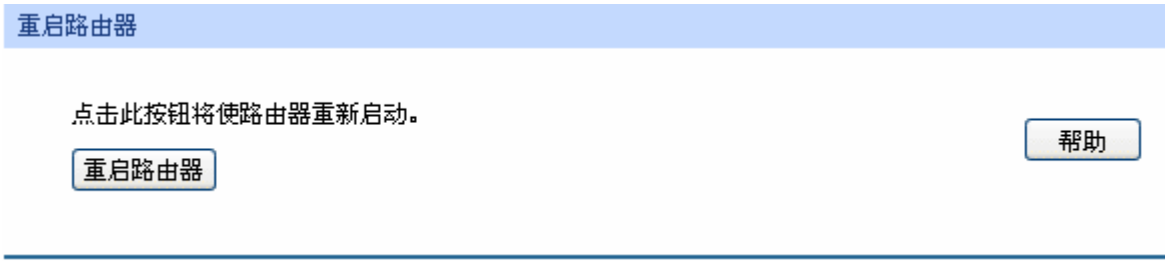


图 4-85 重启路由器界面

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。

4.8.1.7 软件升级

界面进入方法：系统工具 >> 设备管理 >> 软件升级

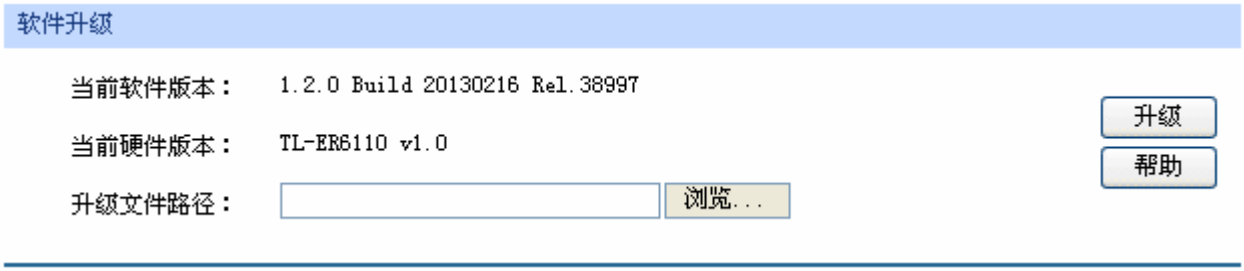


图 4-86 软件升级界面

TP-LINK官方网站（http://www.tp-link.com.cn）会不定期更新TL-ER6110的软件升级文件，可将升级文件下载保存在本地。登录TL-ER6110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：

- 软件升级成功后路由器将会自动重启，在路由器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恢复出厂默认配置，如有重要配置信息，请在升级前备份。

4.8.2 流量统计

4.8.2.1 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，以及WAN口的附加信息统计。

界面进入方法：系统工具 >> 流量统计 >> 接口流量统计

图 4-87 接口流量统计界面

接收/发送速率是以千比特每秒为单位进行统计的，通常所说的1M带宽即1024Kbps。接收/发送总包数统计的是数据包的总个数。接收/发送总字节数统计的则是所有数据包的总字节数。

WAN口附加信息则是以数据包为单位进行统计。其中，IP分片是指接收到的大小超过WAN口允许接收的最大值，需要分片传输的数据包；IP异常包是指IP封装字段非正常的数据包。

4.8.2.2 IP流量统计

流量统计界面将显示接入路由器LAN口或DMZ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：系统工具 >> 流量统计 >> IP流量统计

图 4-88 IP流量统计界面

路由器默认勾选“启用流量统计”、“启用自动刷新”选项，启用自动刷新时，路由器每隔10秒刷新一次。相应的流量统计信息将显示在流量统计列表中。可以按照不同的表头对表格进行排序，默认排序方式为从小到大。

4.8.3 诊断工具

4.8.3.1 诊断工具

可在诊断工具界面通过ping命令或tracert命令来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 4-89 诊断工具界面

界面项说明：

➢ **Ping通信检测**

目的IP/域名	输入目的地址，可以是一个合法IP地址，也可以是一个合法域名，如果输入地址无效将提示重新输入。在下拉菜单中选择目的地址所属接口，点击<开始>按钮后，路由器将发送ping包检测目的地址是否可以到达，并将检测结果显示在下面的方框中。
发送数据包数	输入所需发送ping数据包的数目，可以输入范围为0-10，当输入0时，表示可连续发送ping数据包。

➢ **路由跟踪检测**

目的IP/域名	输入目的地址，可以是一个合法IP地址，也可以是一个合法域名，如果输入地址无效将提示重新输入。在下拉菜单中选择目的地址所属接口，点击<开始>按钮后，路由器将发送tracert包检测经过哪些路由到达目的地址，并将检测结果显示在下面的方框中。

4.8.3.2 在线检测

该页面用于检测WAN口是否在线。

界面进入方法：系统工具 >> 诊断工具 >> 在线检测

图 4-90 在线检测界面

界面项说明：

➢ **检测设置**

接口名	选择需要在线检测的WAN口。

检测开关 选择开启或关闭在线检测。开启在线检测时，路由器将综合PING检测和DNS检测的结果判断是否在线；关闭在线检测时，路由器只根据WAN接口的物理连接状态和拨号状态判断是否在线。

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，您可以自己设置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。

- **WAN口状态列表**

接口 显示所检测的WAN口。

检测 显示选择的检测开关，即启用或禁用。

WAN口状态 显示PING检测或DNS检测的结果。

4.8.4 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

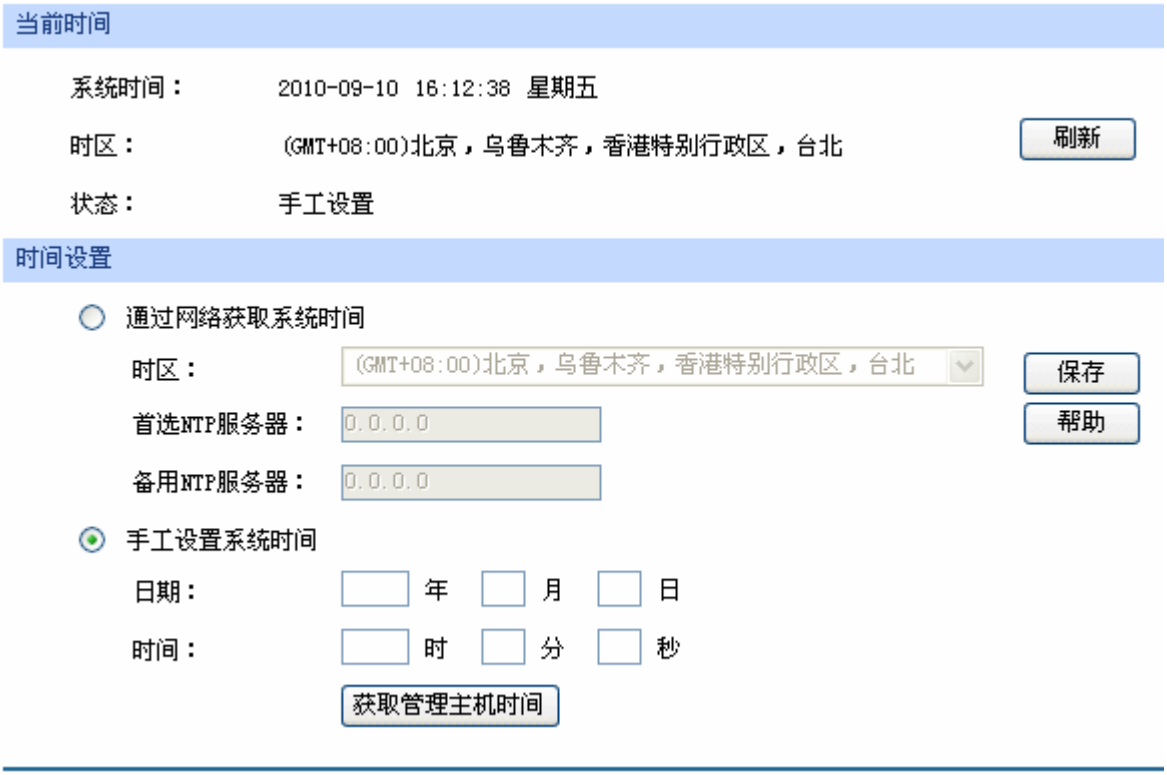


图 4-91 时间设置界面

界面项说明：

- **当前时间**

  此处将显示目前系统时间及时间获取方式信息。如果想对时间进行更改，可以在下方时间设置区进行改动。

- **时间设置**

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<保存>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<保存>按钮，路由器会通过指定的NTP服务器获取网络时间。

手工设置系统时间　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<保存>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，默认将从2010年2月10日0时0分0秒开始计时。

4.8.5 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

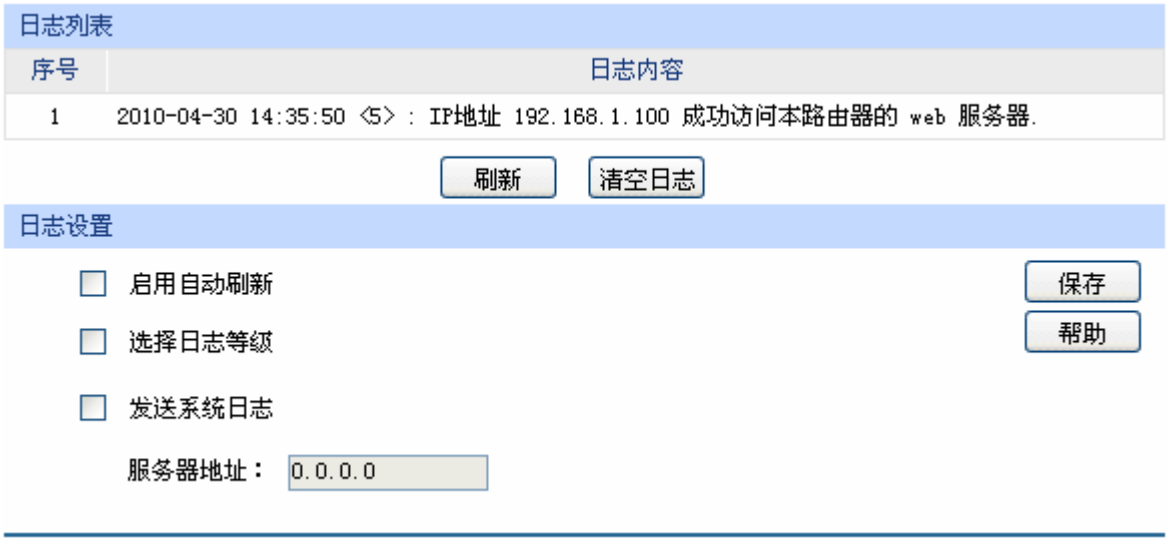
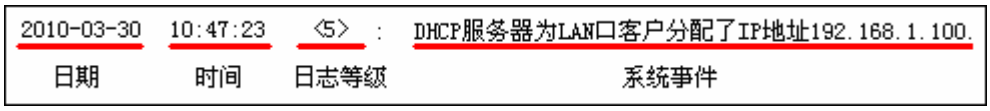


图 4-92 日志界面

日志列表中一条日志内容可分为四个部分：



日志配置部分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：

<0> 致命错误　导致系统不可用的错误，红色显示。

<1> 紧急错误　必须对其采取紧急措施的错误，红色显示。

<2> 严重错误　导致系统处于危险状态的错误，红色显示。

<3> 一般错误　一般性的错误提示，橙色显示。

<4> 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。

<5> 通知信息　正常状态下的重要提示信息。

<6> 消息报告　一般性的提示信息。

<7> 调试信息　调试过程产生的信息。

若需要在某台主机上查看路由器日志信息，请首先在这台主机上安装日志服务器，然后勾选路由器日志页面上的“发送系统日志”选项，并输入这台主机的IP地址。保存设置后路由器将向指定地址发送系统日志。

第5章 典型配置

5.1 典型配置需求

某企业组网需求如下：

- 出口采用电信10M光纤接入
- 需要和远端分支结构间进行安全的信息交互
- 需要禁止部分员工使用QQ、MSN等聊天工具以及迅雷下载软件
- 需要允许产品部门访问IT类网站，销售部门访问电商类网站，其他部门禁止访问网站
- 需要实时监控企业员工的上网行为，及时调整网络管理策略
- 需要防范来自企业内、外部的ARP欺骗和攻击
- 需要防范DoS等常见攻击
- 需要防止某些计算机使用迅雷、BT等P2P软件占用网络资源
- 需要对网络各种流量进行实时监控以确保网络稳定运行

5.2 典型配置方案

为满足以上需求，使用TP-LINK企业VPN路由器TL-ER6110进行组网，以下面的典型配置方案为例：

- 光纤线路通过光纤收发器接入路由器，WAN口接入方式采用静态IP接入方式
- 在路由器上配置IPsec VPN策略，并在远端分支机构的出口路由器上配置对应的IPsec VPN策略，双方将建立起安全的VPN连接进行信息交互
- 配置路由器的应用限制功能，禁止某些员工使用QQ、MSN及迅雷软件
- 配置路由器的网站过滤功能，允许产品部门访问IT类网站，销售部门访问电商类网站，其他部门禁止访问网站
- 配置路由器的行为审计功能，实时监控企业员工的上网行为
- 使用IP/MAC地址绑定功能，绑定局域网内主机的IP、MAC地址信息，实现局域网ARP攻击防护
- 使用IP/MAC地址绑定功能，绑定WAN口网管的IP、MAC地址信息，实现广域网ARP攻击防护
- 启用发送免费ARP包功能，实现局域网ARP防欺骗
- 启用攻击防护功能，实现DoS类、扫描类、可疑包类等常见攻击的防护
- 设置IP带宽限制和连接数限制，防止某些应用程序过度占用网络资源
- 设置路由器LAN3为监控端口，LAN1和LAN2为被监控端口，并启用流量统计功能，实时监控内网流量

5.3 典型组网拓扑

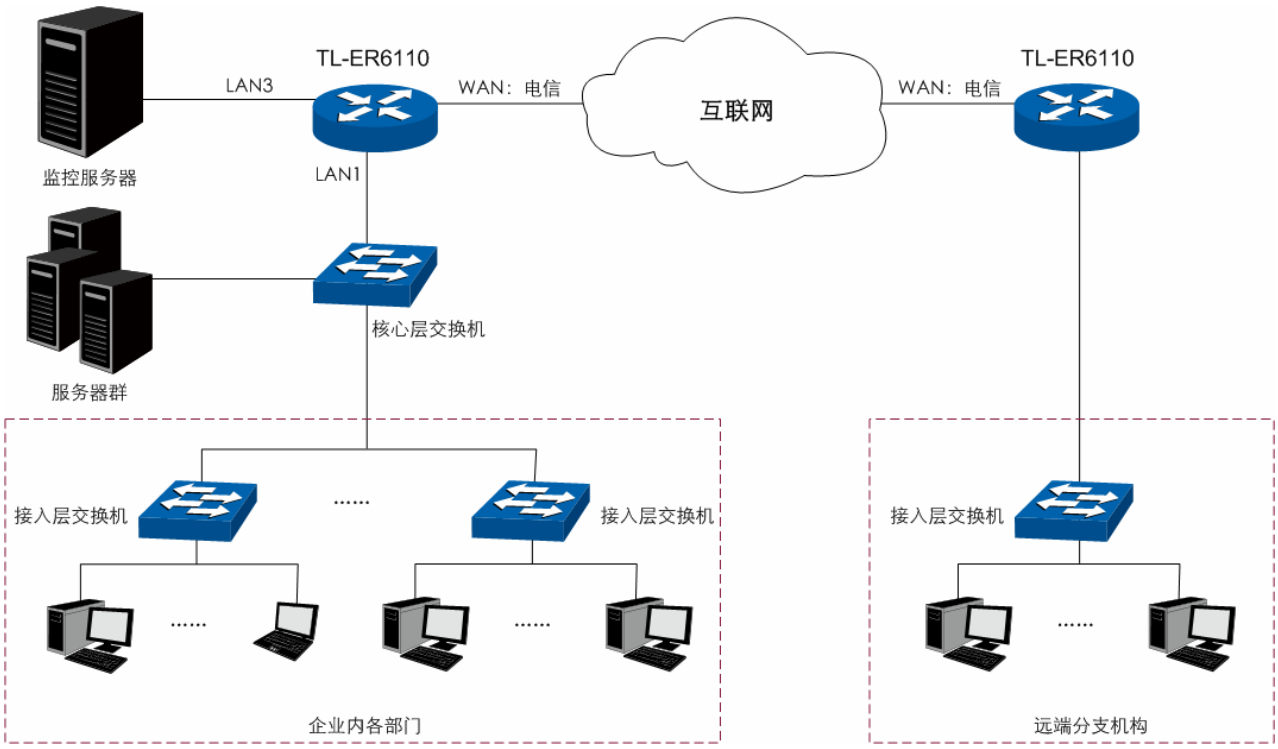


图 5-1 企业网典型组网拓扑

5.4 典型配置步骤

可以通过连接到路由器LAN口的计算机对路由器进行配置。

计算机的IP地址可以自动获取，也可以手动设置。手动设置时请确保计算机IP地址与路由器LAN口在同一网段（默认路由器LAN口处于为192.168.1.0/24网段），然后在Web浏览器的地址栏中输入“http://192.168.1.1”（如果您已修改路由器LAN口IP地址，请输入新地址），按下回车键后出现登录窗口，在登录窗口中输入用户名：admin，密码：admin（如果您已修改密码，请输入新密码），点击<登录>按钮即可进入路由器Web配置界面。

5.4.1 系统模式设置

设置系统模式为NAT模式。设置界面进入方法：**基本设置 >> 系统模式 >> 系统模式**。选择“NAT模式”后点击<保存>按钮。

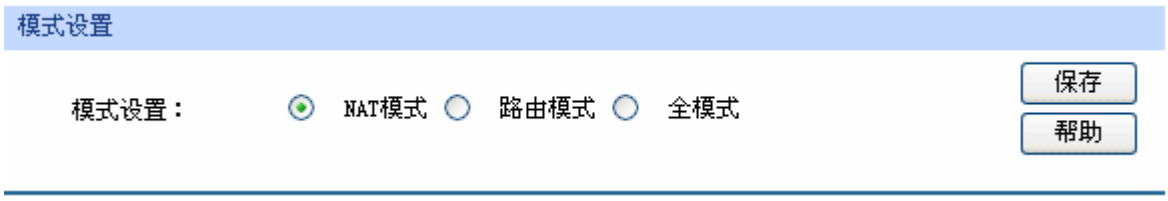


图 5-2 系统模式设置

5.4.2 上网方式设置

设置WAN口的连接方式为静态IP。设置界面进入方法：**基本设置 >> WAN设置 >> WAN设置**。选择“静态IP”，填入电信提供的IP地址、子网掩码、网关地址等信息，设置上下行带宽均为10000Kbps，如图 5-3。点击<保存>按钮即可。

图 5-3 WAN口设置静态IP连接方式

5.4.3 IPsec VPN设置

该企业有个远端分支机构，其WAN口地址为116.31.85.133，LAN口地址为172.31.10.1。分支机构中的主机希望能访问企业总部服务器，则可以通过在总部和分支结构部署TP-LINK企业VPN路由器来搭建VPN隧道，实现安全通信的需求。本文中以IPsec为例进行企业总部的VPN设置说明，首次设置IPsec VPN的顺序为IKE设置 -> IPsec设置。

5.4.3.1 IKE设置

首次设置IKE的顺序为IKE安全提议设置 -> IKE安全策略设置。设置界面进入方法：**VPN >> IKE**。

进入“IKE安全提议”标签页，输入安全提议名称，选择合适的加密、验证算法及DH组，如图 5-4。点击<增加>按钮。

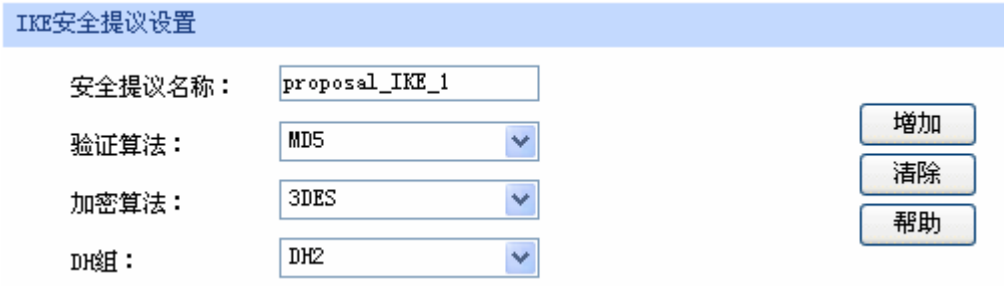


图 5-4 设置IKE安全提议

进入“IKE安全策略”标签页，输入安全策略名称，选择“主模式”协商模式，并选择刚才创建的“proposal_IKE_1”IKE安全提议，然后输入预共享密钥，设置生存时间，并开启DPD检测。如图 5-5。点击<增加>按钮。

图 5-5 设置IKE安全策略

说明

远端分支机构的VPN路由器上也需要做相同的IKE设置。

5.4.3.2 IPsec设置

首次设置IPsec的顺序为IPsec安全提议设置 -> IPsec安全策略设置。设置界面进入方法：**VPN >> IPsec**。

进入“IPsec安全提议”标签页，输入安全提议名称，选择合适的安全协议及算法，如图 5-6。点击<增加>按钮。

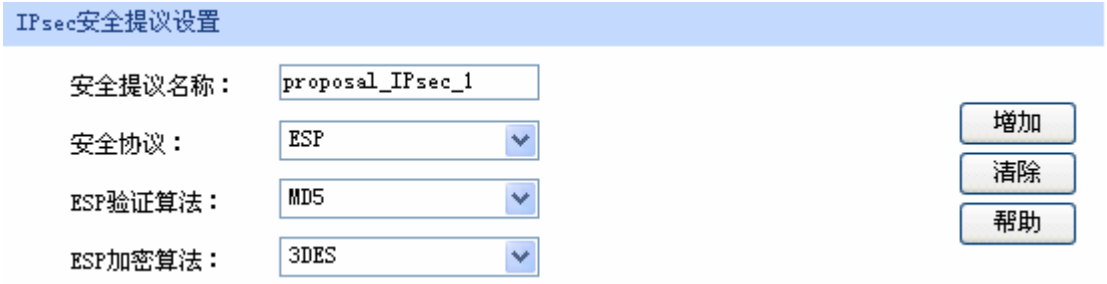


图 5-6 设置IPsec安全提议

进入“IPsec安全策略”标签页，输入安全策略名称，启用安全策略，选择组网模式“站点到站点”，设置本地子网范围192.168.1.0/24，对端子网范围172.31.10.0/24，对端网关116.31.85.133。然后选择“IKE协商”，使用刚才创建的“IKE_1”IKE安全策略和“proposal_IPsec_1”IPsec安全提议，PFS选择DH1组，并设置生存时间。如图 5-7。点击<增加>按钮。

图 5-7 设置IPsec安全策略

说明

远端分支机构的VPN路由器上也需要做对应的IPsec设置，其中“IPsec安全提议”等设置需与总部保持一致，而“对端网关”则需填写总部VPN路由器的IP地址。

两端IPsec VPN连接成功后，可进入“IPsec安全联盟”标签页查看连接信息。界面进入方法：**VPN >> IPsec >> IPsec安全联盟**。

图 5-8 查看IPsec安全联盟

5.4.4 上网行为管理

该企业需要对员工的上网行为进行管理。企业内部IP地址为192.168.1.30 - 192.168.1.50的用户禁止使用QQ、MSN等即时通信工具和迅雷下载工具。IP地址为192.168.1.60 - 192.168.1.69的用户为产品部门员工，允许访问IT类网站，IP地址为192.168.1.70 - 192.168.1.79的用户为销售部门员工，允许访问电商类网站，其他部门员工禁止访问网站。同时，需要实时监控企业所有员工的上网行为。

管理企业员工的上网行为，首先需要对企业员工进行分组，需用到路由器的用户管理功能。禁止受限网段用户使用QQ、MSN等即时通信工具和迅雷下载工具，需用到路由器的应用限制功能。设置各部门员工访问的网站不同，需用到路由器的网站过滤功能。实时监控企业所有员工的上网行为，需用到路由器的行为审计功能。

下面介绍以上各功能的设置方法。

5.4.4.1 用户管理设置

企业内部IP地址为192.168.1.30 - 192.168.1.50的员工，是应用受到限制的用户，以将他们设置成一个组为例，下面介绍用户管理的设置方法。设置界面进入方法：**对象管理 >> 用户管理**。

首先，进入“组设置”标签页，创建一个新的用户组，组名称设置为受限网段，如图 5-9所示，点击<新增>按钮完成。

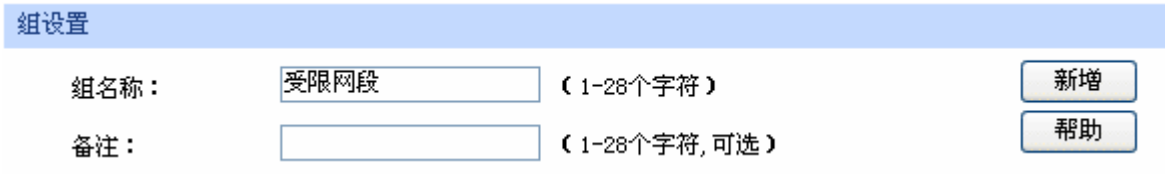


图 5-9 创建用户组

然后进入“用户设置”标签页，新建组内用户。点击页面下方的<批量处理>按钮，选择操作方式为“增加”，输入起始和结束的IP地址，用户名前缀输入“受限网段”，其它保持默认值，如图 5-10。点击<确定>按钮完成。

图 5-10 新建组内用户

进入“视图”标签页，将用户添加到相应的用户组中。选择<组视图>按钮，在组名下拉菜单中选择“受限网段”用户组。可选用户栏中会自动列出所有已经设置的用户名称，选择前缀为受限网段的用户，点击< >> >按钮将其添加到包含用户栏中。如图 5-11。点击<保存>按钮完成。

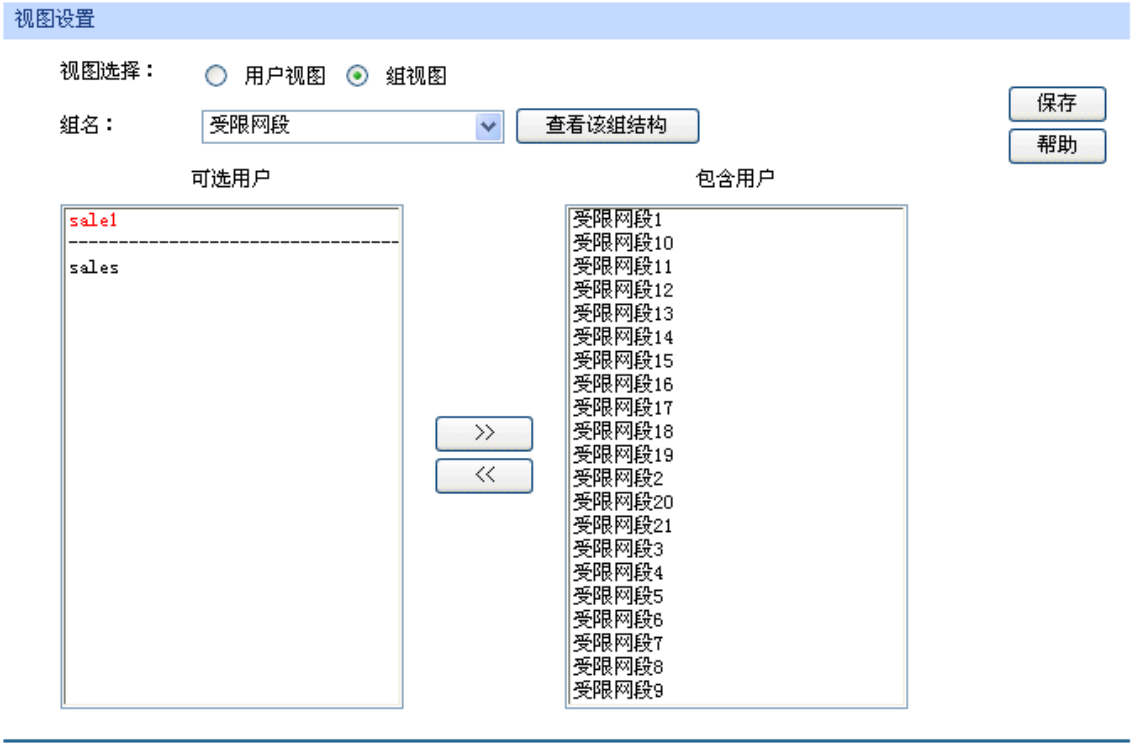


图 5-11 添加用户到用户组

按照上述步骤，可以设置用户组产品部门和销售部门，产品部门包含IP地址192.168.1.60 - 192.168.1.69，销售部门包含IP地址192.168.1.70 - 192.168.1.79。

5.4.4.2 应用限制设置

对受限网段这个组进行应用限制设置。设置界面进入方法：**行为管控 >> 应用限制 >> 应用限制**。首先勾选“启用应用限制功能”，并点击<保存>按钮。然后在用户组下拉菜单中选择“受限网段”，点击禁用后的<应用列表>按钮，在显示的界面中勾选需要禁止使用的软件，点击<确定>按钮。最后选择规则生效时间为“ANY”，点击<启用>按钮。如图 5-12。点击<新增>按钮完成。

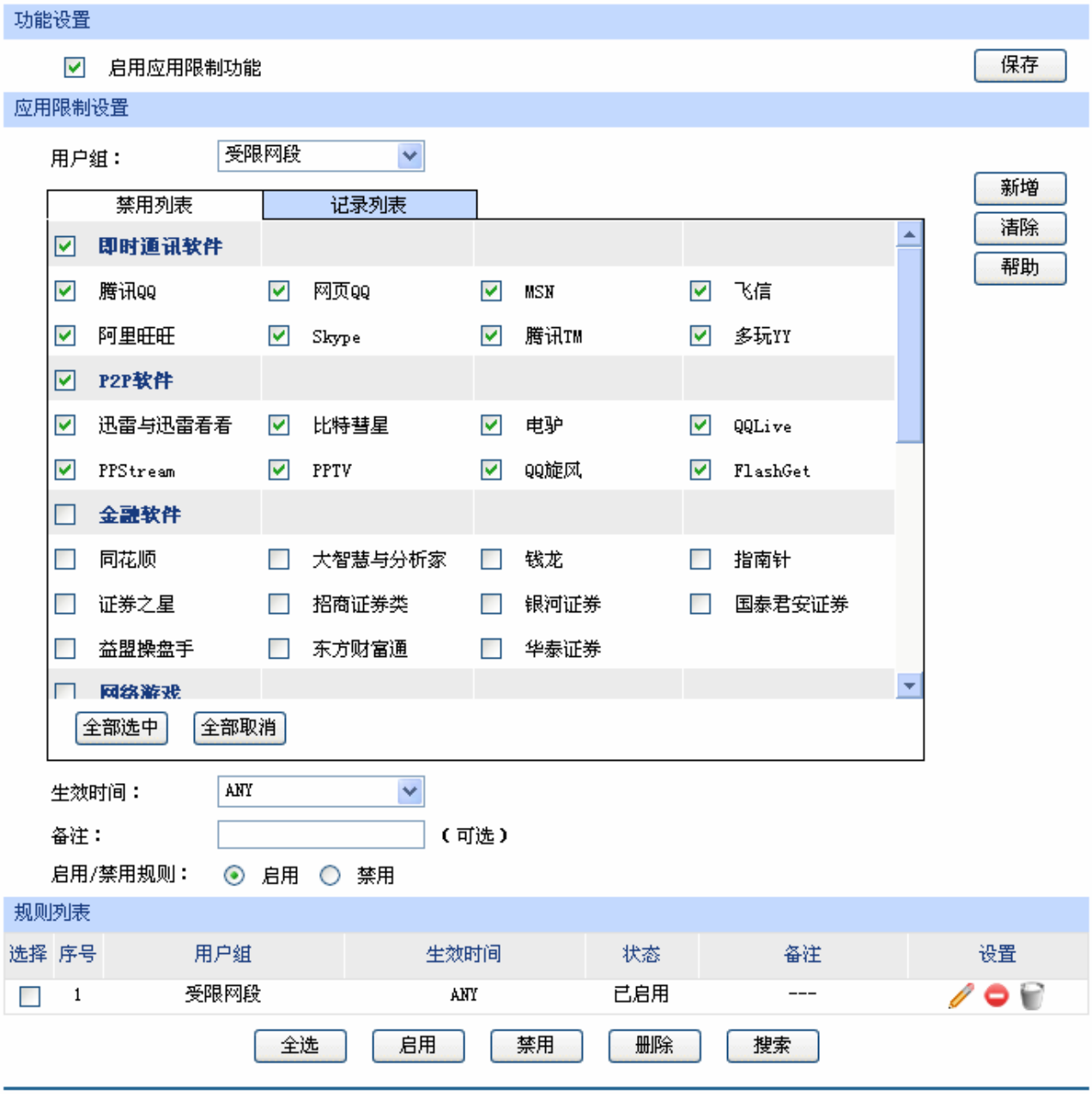


图 5-12 应用限制设置

5.4.4.3 网站过滤设置

对产品部门、销售部门和其他部门员工进行网站过滤设置。下面以设置产品部门用户组的网站过滤为例说明此功能的设置方法，首次设置网站过滤的顺序为网站分组设置 -> 网站过滤设置。设置界面进入方法：**行为管控 >> 网址过滤**。

进入“网站分组”标签页，输入组名称IT类，再输入组成员，如图 5-13。点击<新增>按钮。

图 5-13 新建网站分组

进入“网站过滤”标签页，首先勾选“启用网站过滤功能”，并点击<保存>按钮。然后在用户组下拉菜单中选择“产品部门”，规则类型选择“允许访问下列网站分组”，选择网站项选择网站分组列表，且点击<网站分组列表>按钮，在显示的界面中勾选“IT类”，点击<确定>按钮。最后选择规则生效时间为“ANY”，点击<启用>按钮。如图 5-14。点击<新增>按钮完成。

图 5-14 产品部门网站过滤设置

销售部门的网站过滤设置与产品部门方法相同，完成这两条规则设置后，再设置一条对“ANY”用户组，禁止访问所有网站的规则，可实现禁止其他部门员工访问网站的需求。此条规则设置如下：用户组选择“ANY”，规则类型选择“禁止访问下列网站分组”，选择网站项选择所有网站，规则生效时间选择“ANY”，点击<启用>按钮。如图 5-15。点击<新增>按钮完成。

图 5-15 其他部门网站过滤设置

说明

“ANY”用户组的网站过滤规则条目在规则列表中的位置必须在“产品部门”和“销售部门”之后，否则将无法实现需求。

5.4.4.4 实时监控上网行为

需要在IP地址为192.168.6.100的台主机上查看用户上网行为信息，可以使用行为审计功能，设置界面进入方法：**行为管控 >> 行为审计 >> 行为审计**。首先需要在这台主机上安装TP-LINK上网行为审计软件，然后在图 5-16行为审计界面输入该服务器IP地址，点击<开始上传>按钮之后，路由器会立即将用户上网行为信息实时上传至该服务器，并通过TP-LINK上网行为审计软件输出审计结果。

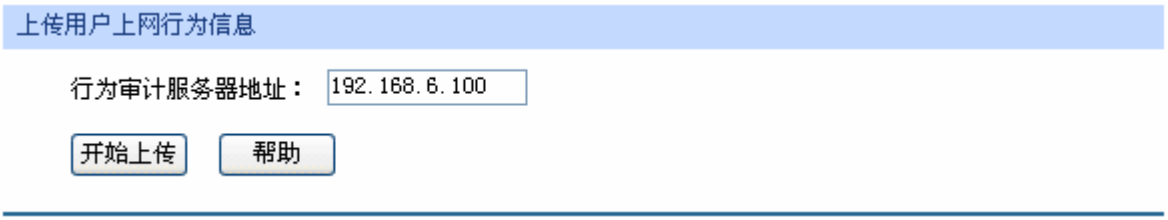


图 5-16 实时监控上网行为

5.4.5 局域网ARP攻击防护设置

可以采用ARP扫描和手动设置两种方式绑定IP与MAC信息。首次设置时，请先使用扫描方式绑定大部分的ARP信息，如果还有个别特殊条目，还可以通过手动设置绑定。

1. 扫描并将条目导入ARP绑定列表

指定范围进行ARP动态扫描。设置界面进入方法：**安全管理 >> ARP防护 >> ARP扫描**。进行ARP扫描的前提是当前局域网内不存在ARP攻击。设置如图 5-17。

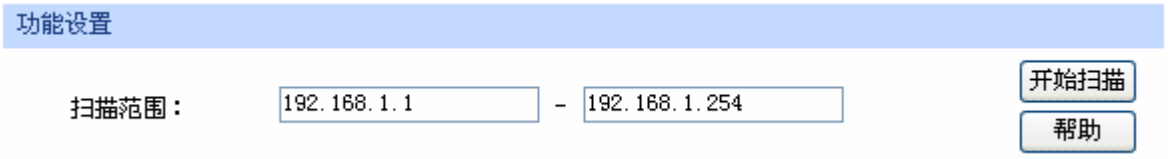


图 5-17 设置ARP扫描的地址范围

开启企业网络中需要进行ARP绑定的所有主机，点击<开始扫描>按钮，得到扫描结果如图 5-18。

图 5-18 ARP扫描结果列表

选中需绑定的ARP条目，或点击<全选>按钮，再点击<导入>按钮即完成ARP绑定。ARP绑定列表如图 5-19。界面进入方法：**安全管理 >> ARP防护 >> IP MAC绑定**。

图 5-19 导入后生效的ARP绑定列表

2. 手动设置ARP绑定条目

手动设置IP与MAC绑定信息并新增至ARP绑定列表。设置界面进入方法：**安全管理 >> ARP防护 >> IP MAC绑定**。假设现在需要添加IP地址为192.168.1.200的主机IP MAC信息，该主机MAC地址为00-11-22-33-44-aa，则填入相应的IP、MAC地址，如图 5-20。选择“生效”后点击<新增>按钮，则条目绑定成功。其他待绑定的条目也可依次手动添加。

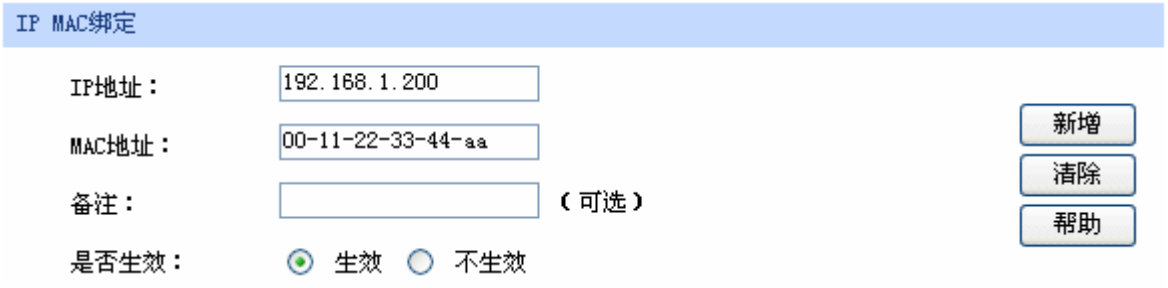


图 5-20 手动设置主机的IP MAC信息

3. 设置ARP防欺骗功能

进入IP MAC绑定界面，进入方法：**安全管理 >> ARP防护 >> IP MAC绑定**。在“功能设置”处勾选所有条目，并将路由自动发送GARP包的发包间隔设置为1ms，如图 5-21。点击<保存>按钮即启用ARP防欺骗功能。

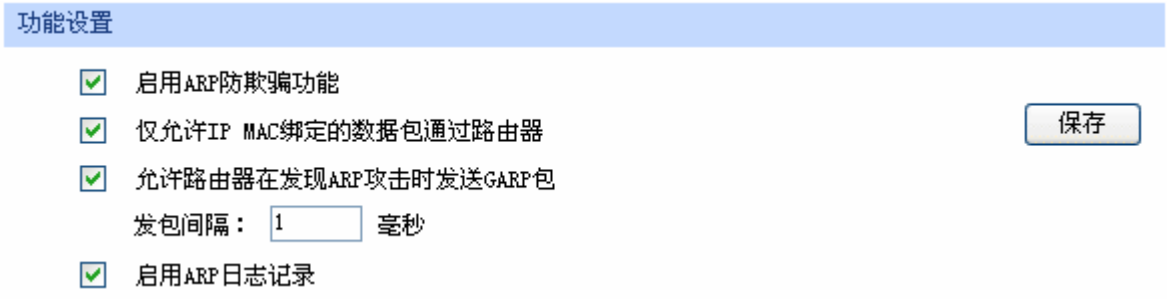


图 5-21 开启ARP防欺骗功能

5.4.6 广域网ARP攻击防护设置

可通过绑定WAN口网关及MAC地址来进行广域网ARP攻击防护。

首先，需要通过ARP扫描获取网关MAC地址，设置界面进入方法：**安全管理 >> ARP防护 >> ARP扫描**。在扫描范围填入WAN口网关IP地址58.51.128.254，点击<开始扫描>按钮，如图 5-22。扫描结束后，在扫描结果中，就能看到网关对应的MAC地址。

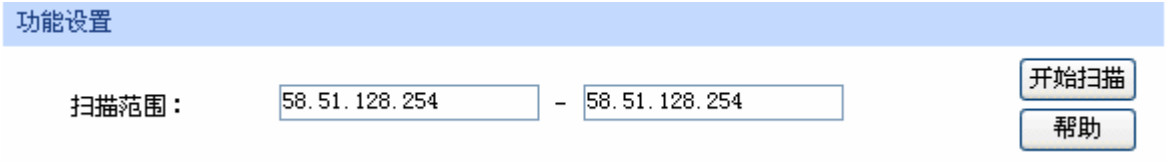


图 5-22 设置动态扫描ARP的地址范围为WAN口网关IP

在扫描结果列表中获得WAN口网关MAC地址后，勾选此条目，点击<导入>按钮，完成绑定操作。

5.4.7 网络攻击防护设置

设置界面进入方法：**安全管理 >> 攻击防护 >> 攻击防护**。勾选所需开启的攻击防护选项，如图5-23。点击<保存>按钮即可。

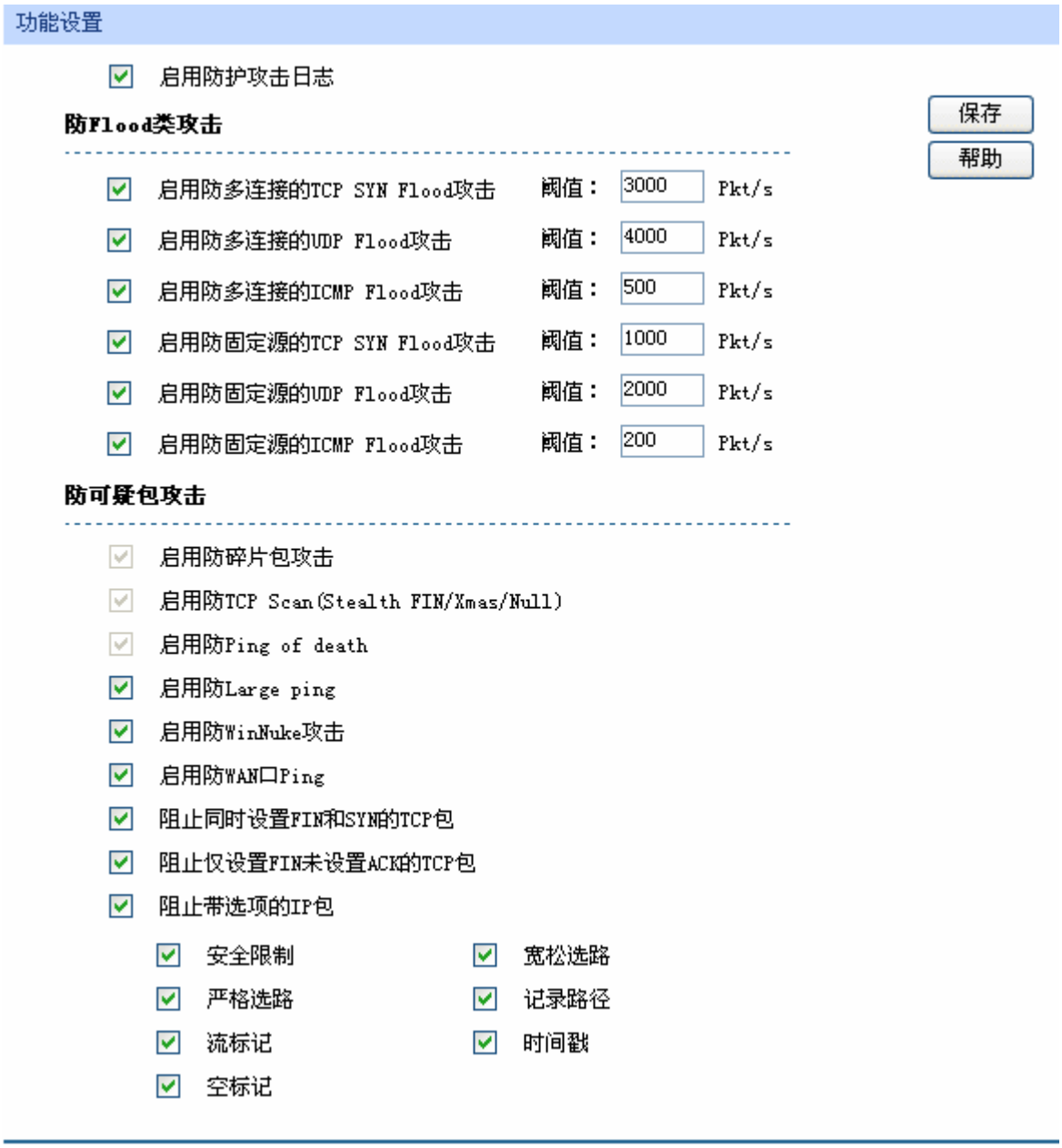


图 5-23 启用网络攻击防护功能

5.4.8 带宽控制设置

带宽控制需要通过设置接口总带宽和具体的带宽控制规则来实现。

1. 启用带宽控制功能

设置界面进入方法：**传输控制 >> 带宽控制 >> 基本设置**。勾选“功能设置”下的“启用智能带宽控制”，如图 5-24。点击<保存>按钮即可。

图 5-24 启用带宽控制

2. 接口总带宽设置

设置界面进入方法：**基本设置 >> WAN设置 >> WAN设置**。设置WAN接口的上行和下行带宽，如图5-3，所填入的带宽值请与实际线路带宽保持一致。

3. 带宽控制规则设置

设置界面进入方法：**传输控制 >> 带宽控制 >> 带宽控制规则**。

选择数据流量为LAN -> WAN，用户组为“受限网段”，生效时间为“ANY”，带宽模式为独立，上行与下行最小保证带宽各为100Kbps，最大限制带宽各为800Kbps，选择“启用”规则，如图 5-25。点击<新增>按钮，则带宽控制规则设置成功。

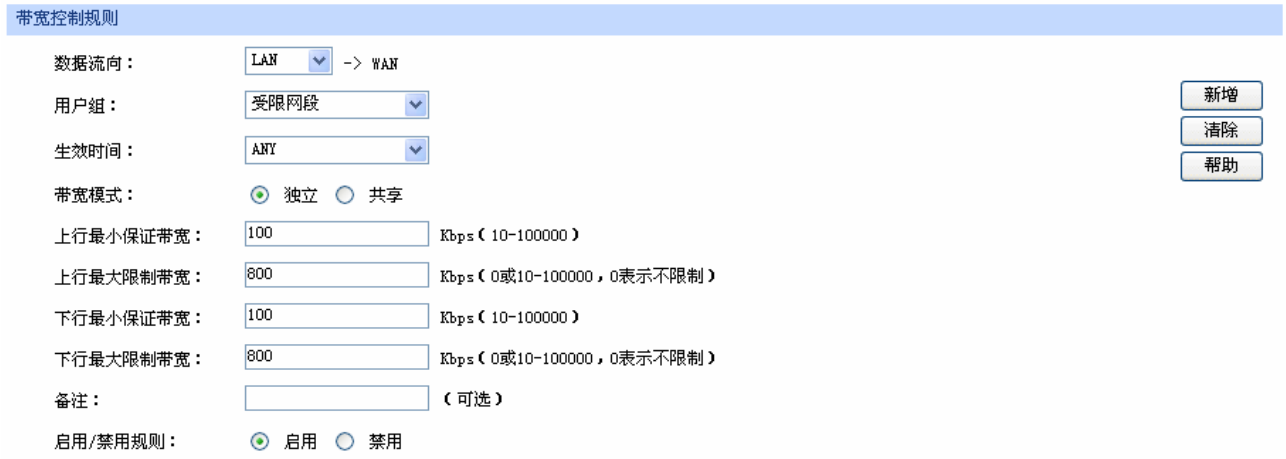


图 5-25 设置带宽控制规则

5.4.9 连接数限制设置

设置界面进入方法：**传输控制 >> 连接数限制 >> 连接数限制规则**。首先勾选“启用连接数限制”，并点击<保存>按钮。然后设置“受限网段”用户组内的IP地址发起的最大连接数为250，选择启用，如图5-26。点击<新增>按钮完成设置。

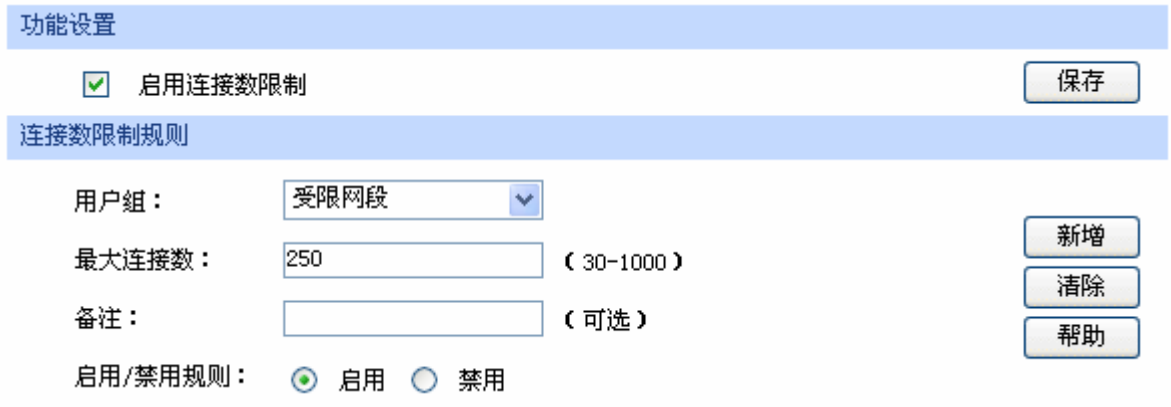


图 5-26 启用连接数限制功能

5.4.10 内网流量监控

5.4.10.1 端口监控设置

设置界面进入方法：**基本设置 >> 交换机设置 >> 端口监控**。勾选“启用端口监控”，监控模式为输入输出监控，监控端口选择端口5，被监控端口选择端口3、端口4，如图 5-27。点击<保存>按钮即完成端口监控设置。

图 5-27 设置端口监控功能

5.4.10.2 流量统计

界面进入方法：**系统工具 >> 流量统计**。

进入“接口流量统计”标签页，可以查看路由器各物理接口的流量统计结果，如图 5-28。

图 5-28 查看接口流量统计结果

进入“IP流量统计”标签页，勾选“启用流量统计”和“启用自动刷新”，点击<保存>按钮，便可查看相应的IP流量统计结果，如图 5-29。

图 5-29 查看IP流量统计结果

以上所有步骤设置完成后，企业网络就可以按规划正常运营了。

第6章 命令行简介

CLI(Command Line Interface，命令行接口）即命令行，TL-ER6110路由器提供了一个用于CLI配置的Console口。可以通过控制台（比如超级终端）和在局域网内通过Telnet进入命令行界面进行设置。

以下介绍通过超级终端访问CLI的具体步骤和一些常用的CLI命令。

6.1 搭建平台

首先，使用Console线连接路由器和计算机的Console口。

选择 开始>所有程序>附件>通讯>超级终端，打开超级终端。

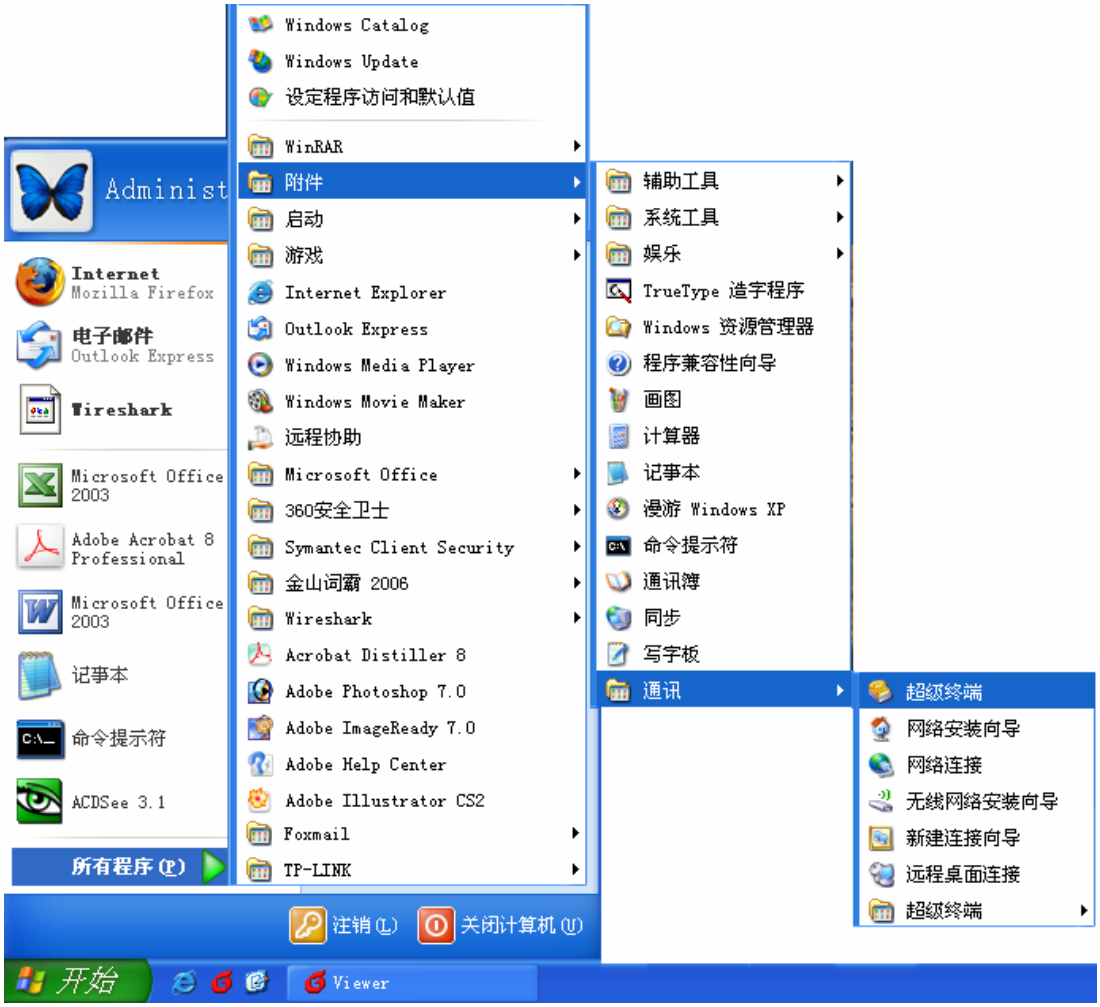


图 6-1打开超级终端

弹出如图 6-2所示的连接描述窗口，在名称处键入一个名称，点击<确定>。

图 6-2 连接描述窗口

在图 6-3中选择连接串口（单串口默认COM1口），点击<确定>。

图 6-3 连接参数窗口

在图 6-4中对端口进行参数设置，每秒位数115200，数据位8，奇偶校验无，停止位1，数据流控制无，点击<确定>。

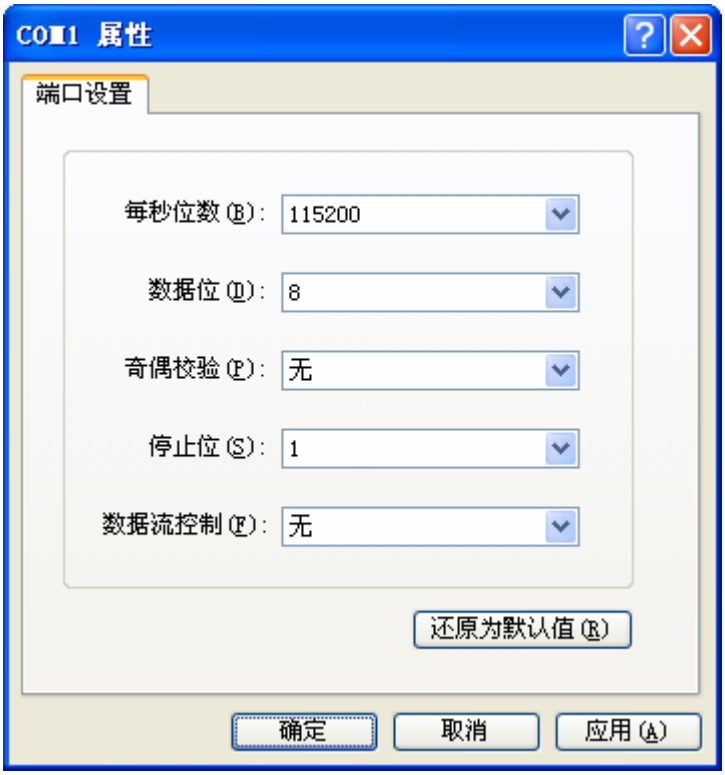


图 6-4 端口属性设置

在图 6-6超级终端主窗口选择 文件>属性>设置，在图 6-5中选择终端仿真类型为VT100 或自动检测，点击<确定>。

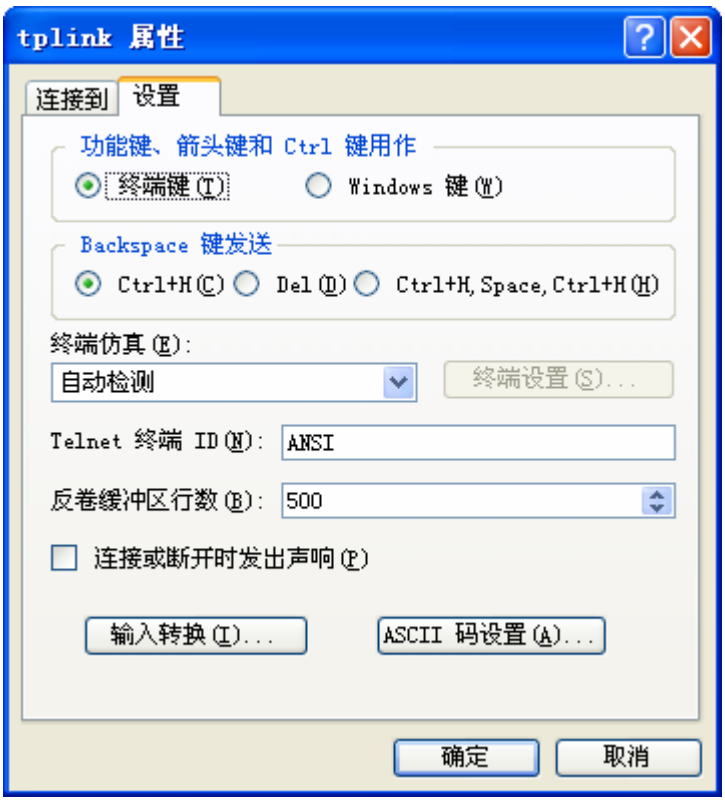


图 6-5 连接属性设置

在超级终端主窗口中按下回车键，就可以看到“TP-LINK>” 的提示符了。如图 6-6所示。

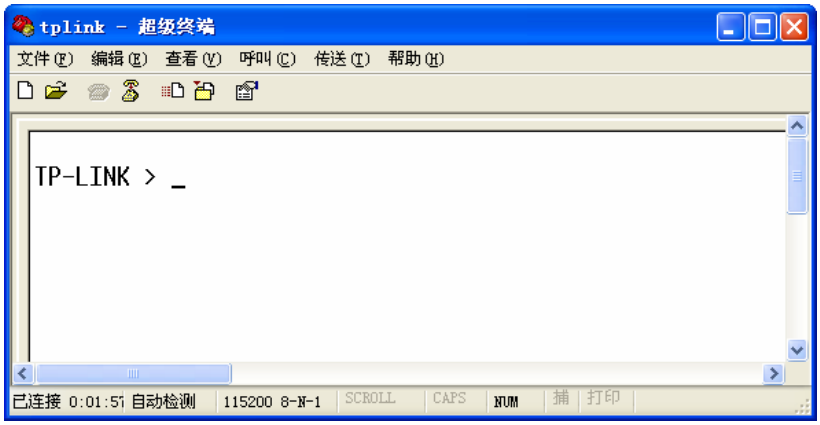


图 6-6 命令行主窗口

6.2 界面模式

TL-ER6110的CLI提供了两个界面模式：用户模式和特权模式。用户模式下只具有基本的权限，比如查看系统的信息等。特权模式下则拥有管理路由器的权限，可以进行各种配置操作等。这样就可以对不同的用户进行适当的权限管理。

用户模式：Telnet登录时，需输入路由器的用户名和密码，默认为admin/admin，Console连接登录时不需要密码。登录后，用户处于用户模式下，拥有的权限为参观级。可以进行简单的查询操作，不能修改路由器的各种配置信息。

特权模式：用户在用户模式下进行密码验证，验证通过就可以进入特权模式。拥有管理级的权限，可以对路由器进行各种配置操作。

默认情况下，CLI用户处于用户模式下。用户可以自由的在用户模式和特权模式之间进行切换，方式如下：

模式	访问方法	提示符	离开或访问下一模式
用户模式	与路由器建立连接即进入该模式。	TP-LINK >	输入exit命令断开与路由器的连接（Console连接时无法断开） 要进入特权模式，输入enable 命令。
特权模式	在用户模式下，使用enable命令进入该模式，初始密码admin。	TP-LINK #	输入exit命令断开与路由器连接（Console连接时无法断开） 要返回到用户模式，输入disable 命令。

如图 6-7所示：

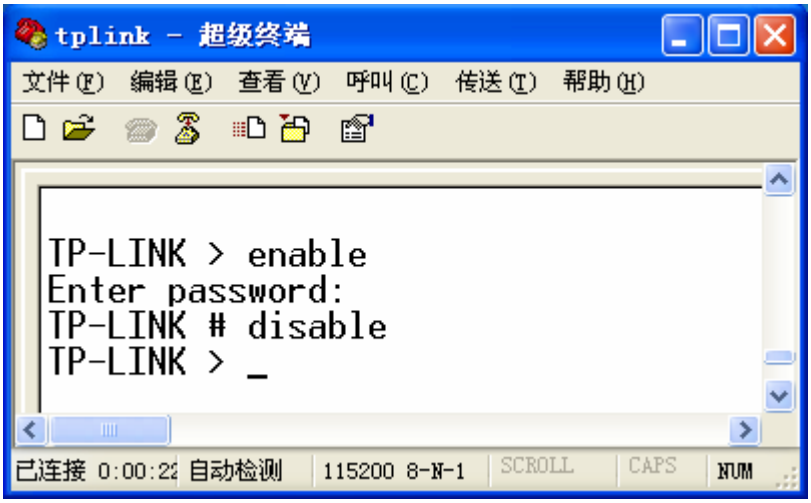


图 6-7 用户模式与特权模式切换

6.3 在线帮助

TL-ER6110提供了命令行在线帮助：

1) 在任一模式下，键入“?”获取该视图下所有的命令及其简单描述。

```
TP-LINK > ←键入“?”键

disable          - Exit the privileged mode

enable           - Enter the privileged mode

exit             - Exit the CLI (only for telnet)

history          - Show command history

ip               - Display or Set the IP configuration

ip-mac           - Display or Set the IP mac bind configuration

sys              - System manager

user             - User configuration
```

2) 键入一命令，后接以空格分隔的“?”，如果该命令行位置有关键字，则列出全部关键字及其简单描述。例如：

```
TP-LINK > ip ←按下“空格”“?”键
```

```
get                - Get the ip configuration
```

3) 键入一字符串，其后紧接“?”，列出以该字符串开头的所有命令。例如：

```
TP-LINK > dis←按下“?”键
disable
```

4) 键入命令的某个关键字的前几个字母，按下<Tab>键，如果以输入字母开头的关键字唯一，则可以显示出完整的关键字。例如：

```
TP-LINK > dis←按下“Tab”键
disable
```

5) 命令的输入完成之后，后接以空格分隔的“?”，会显示出一个回车符，表示此时可以执行该命令。例如：

```
TP-LINK # enable ←按下“空格”“?”键
<cr>
```

6.4 命令介绍

TL-ER6110提供了一些CLI命令，通过这些命令可以管理路由器和用户信息。为便于您理解，每条命令后面会注释该条命令的含义。

6.4.1 接口设置

ip命令。可以使用该命令查看或设置当前系统中相关接口的IP地址和子网掩码，查看命令可以在用户模式和特权模式下使用，设置功能只能在特权模式下使用。

`TP-LINK > ip get lan`
`Lan Ip:  192.168.1.1`
`Lan Mask:  255.255.255.0`
	获取LAN口配置信息的命令。

`TP-LINK # ip set lan address 192.168.1.20`	设置路由器LAN口IP地址为192.168.1.20。如果返回Operation succeeded!表示操作成功，如发生错误会有提示。
`TP-LINK # ip set lan mask 255.255.0.0`	设置路由器LAN口子网掩码为255.255.0.0。

6.4.2 IP MAC 绑定设置

ip-mac命令。可以使用该命令查看或设置当前系统中IP MAC绑定的模式。设置功能只能在特权模式下使用，查看命令可以在用户模式和特权模式下使用。IP MAC绑定的模式有两种：普通绑定模式(normal)和强制绑定模式(restrict)。

```
TP-LINK > ip-mac get mode
Ip-mac Bind Mode:  normal
```

获取当前IP MAC绑定模式。

```
TP-LINK # ip-mac set mode restrict
```

设置当前IP MAC绑定模式为强制绑定模式。

6.4.3 系统管理

sys命令。可以使用该命令进行相关的系统管理操作，包括配置文件的导入导出、恢复出厂配置、重启系统和升级软件等。

```
TP-LINK # sys reboot
This command will reboot system, Continue?[Y/N]
```

重启系统。Y即YES，表确认；N即NO，表取消。

```
TP-LINK # sys restore
This command will restore system, Continue?[Y/N]
```

恢复出厂配置。Y即YES，表确认；N即NO，表取消。

```
TP-LINK # sys export config
Server address: [192.168.1.101]192.168.1.100
Username: [admin]ftp
Password: [admin]ftp
File name: [config.bin]
Try to save the configuration file < config.bin > ...
Save configuration file < config bin > succeed, file size is 7104 bytes.
```

配置文件导出。

举例：现有一台IP地址为192.168.1.100的FTP服务器，服务的用户名/密码是ftp/ftp，如需将当前配置文件以默认文件名config.bin保存到该FTP服务器上，设置如左。

说明

- 配置文件的导出、导入、系统升级都需要使用FTP服务。在需设置的参数中，Server address是提供FTP服务的主机IP地址，Username/Password是该FTP服务的登录名/密码，File name是配置文件名（如果已存在同名的配置文件，请更改文件名）。
- 中括号内是默认设置，可在其后输入实际参数，如果无需改动直接回车确认即可。
- TL-ER6110默认连接到使用21端口的FTP服务器。
- 由于导出、导入、系统升级等功能需要在FTP服务器上进行读写操作，因此特别需要注意您指定的帐号必须具有相应权限。

```
TP-LINK # sys import config
Server address: [192.168.1.101]
Username: [admin]
Password: [admin]
File name: [config.bin]

Try to get the configuration file < config.bin > ...
Get configuration file < config bin > succeed, file size is 7104 bytes.
```

配置文件导入。说明同上。

```
TP-LINK > sys show
CPU Used Rate:    1%
```

查看系统信息。该命令将会显示当前系统的CPU利用率。

```
TP-LINK # sys update
Server address: [192.168.1.101]
Username: [admin]
Password: [admin]
File name: [update.bin]

Try to get the update file < update.bin > ...
Get update file < update bin > succeed, file size is 2298608 bytes.
```

系统软件升级。

6.4.4 用户信息管理

user命令。可以使用该命令修改登录CLI的用户名和密码。在用户模式下，可以修改参观级用户的密码，由于参观级用户和管理员用户共用一个用户名，因此在用户模式下不能修改用户名；在特权模式下可以修改管理员级用户的用户名和密码。

```
TP-LINK > user set password                    修改参观级用户的密码。
Enter old password:
Enter new password:
Confirm new password:


TP-LINK # user set password                    修改管理员级用户的密码。
Enter old password:
Enter new password:
Confirm new password:


TP-LINK # user set username                    修改管理员级用户的用户名。
Enter new username: tplink
```

注意：

用户名和密码长度为1-31个字符，用户名和密码只能使用字母和数字，且区分大小写。

6.4.5 历史命令管理

history命令。可以使用该命令查看或清除系统中的历史命令。

```
TP-LINK > history                              查看历史命令。
1. history
2. sys show
3. history
```

```
TP-LINK > history clear                                    清除历史命令。

1. history

2. sys show

3. history

4. history clear
```

6.4.6 退出CLI

exit命令。可以使用该命令退出系统。但仅限于Telnet环境，Console环境下不会退出。

```
TP-LINK > exit                                             退出系统。
```

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. 如果您是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，建议您将计算机设置成“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TL-ER6110之间的连通性。
   4) 若上述提示仍不能帮助您登录到路由器管理界面，请您将路由器恢复为出厂配置。
2. 如果您修改过路由器的管理端口，则注意下次登录时您需要以“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. 如果您之前可以正常登录，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. 请您检查是否设置了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TL-ER6110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，使用尖状物按住路由器的Reset键，等待2-5秒后，见到系统指示灯快速闪烁1-2秒，松开按键，路由器将自动恢复出厂设置并重启。路由器出厂默认管理地址是**http://192.168.1.1**，默认用户名/密码是admin/admin。

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，在用户不知道路由器管理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设置。

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. 非局域网段要登录路由器的IP地址是否是被允许远端访问路由器的。
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。
	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。
	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)	鉴别首部	用于保证数据的完整性。
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。
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。
	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。

	英文术语	中文名称	定义或描述
	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。
	IKE (Internet Key Exchange)	互联网密钥交换	用于交换和管理在VPN中使用的加密密钥。
	IPsec(IP Security)	IP安全性	在IP网络中保护端对端通信的安全性。
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。
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您设置的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

	英文术语	中文名称	定义或描述
			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	SMTP(Simple Mail Transfer Protocol)	简单邮件传输协议	用于电子邮件的传输。
	SSH(Secure Shell Protocol)	安全外壳协议	SSH是一种在不安全网络上提供安全远程登录及其它安全网络服务的协议。
	SA (Security Association)	安全联盟	是安全性信息的集合，它描述了一个设备与另一个设备之间特定类型的安全连接。
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。
	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。
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	虚拟局域网	组成局域网的逻辑子组。一个VLAN是一个按

	英文术语	中文名称	定义或描述
	Network)		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。
	VPN (Virtual Private Network)	虚拟专用网	是建立在公用网（通常是因特网）上的一个专用、安全的虚拟网络。
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。

附录C 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 802.3x、TCP/ IP、DHCP、ICMP、NAT、PPPoE、SNTP、HTTP、DNS、L2TP、PPTP、IPsec
端口	LAN口	3~4个10/100M自适应RJ45端口(Auto MDI/MDIX)
	WAN口	1个10/100M自适应RJ45端口(Auto MDI/MDIX)
	DMZ口	至多1个10/100M自适应RJ45端口(Auto MDI/MDIX)
	其它	1个Console端口
网络介质		10BASE-T：3类或 3 类以上非屏蔽双绞线(UTP)(≤100m)
		100BASE-TX：5类非屏蔽双绞线(UTP)(≤100m)
LED 指示	LAN/WAN口	Link/Act指示灯、100M速率指示灯
	其它	PWR电源指示灯、SYS系统指示灯、DMZ接口状态指示灯
外形尺寸(L x W x H)		440mm x 227mm x 44mm
散热方式		自然散热
电源及功耗		输入：100-240V~ 50/60Hz 0.6A
		功耗：最大9.3W
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