TP-LINK®

高性能全千兆企业路由器

TL-ER7520G

用户手册

REV1.0.0

1910040676

声明

目录

第1章 前言

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-ER7520G高性能全千兆企业路由器，下面简称为TL-ER7520G。
- 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
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。

第2章 产品介绍

2.1 产品描述

TL-ER7520G高性能全千兆企业路由器是TP-LINK公司针对中大型企业、机关单位、园区、酒店等网络推出的一款高性能全千兆企业路由器产品，采用基于四核网络专用处理器的硬件平台，具备强大的数据处理能力，同时支持VPN、接入认证、防火墙、上网行为管理、流量控制等丰富的功能特性，非常适合组建安全、高效、易管理的全千兆企业网络。

2.2 产品特性

硬件特性

- 采用64位四核网络专用处理器，单核主频1.2GHz；
- 配备容量为1GB的DDR3高速内存；
- 提供5个10/100/1000M自适应以太网接口；
- 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。

功能特性

接口

- 提供5个千兆物理端口，用户可自由定义端口类型（WAN/LAN/其他类型）；
- 提供多种逻辑接口类型，适应更多复杂的网络适用环境。

VPN

- 提供标准的IPsec VPN功能，支持数据完整性校验、防数据包重放和数据加密功能（DES、3DES、AES128、AES192、AES256等加密算法），支持IKE和手动模式建立VPN隧道，并支持通过域名方式配置VPN连接；
- 提供L2TP/PPTP VPN功能，支持L2TP/PPTP VPN服务器/客户端模式，可实现出差员工或分支结构远程安全接入公司网络。

Web认证

- 不需要客户端软件即可实现认证入网，降低网络维护工作量；

- 支持本地认证、Radius 认证和一键上网，满足多种认证需求；
- 可自定义认证跳转页面，实现广告推送。

微信连Wi-Fi

- 顾客无需输入复杂密码，通过微信客户端即可实现一键联网；
- 支持 Portal 界面跳转，可向用户推送自定义的图片广；
- 支持上网时长设置，灵活控制用户认证周期。

上网行为管理

- 应用限制：支持针对聊天类、P2P 类、金融类、游戏类、代理类及基础类等数十种常见应用的一键管控，有效限制可能降低企业员工工作效率的上网行为；同时支持基于用户组和时间段配置管控策略，方便灵活分配上网权限，保障关键用户的正常上网；
- 网址过滤：通过配置网站过滤和 URL 过滤规则，可对员工访问各种网站的权限进行管控，除了可以禁止/允许员工访问各种网站外，还可以记录其访问历史信息，甚至可以弹出警告页面。此外还支持网站分组功能，可方便地将庞杂的网站进行归类，供过滤规则调用，灵活而实用，同时路由器出厂默认提供十多种网站分组，对于网管资源有限的中小型企业用户，可节省不少配置工作；
- 网页安全：支持禁止网页提交，可限制员工登录各种基于网页的论坛、网站、邮箱等发表信息，避免企业敏感数据外泄；支持过滤文件扩展类型，用户可方便地过滤内嵌在网页中的各种小文件，如 exe、rar、swf 文件等，避免病毒、木马等通过这些小文件侵入企业网络，危害网络安全；
- 行为审计：提供上网行为审计软件，可实时记录和审计员工上网行为，企业网络管理更简单。

防火墙

- 访问策略：通过配置访问控制策略，可允许或禁止特定应用数据流通过路由器，比如FTP下载、收发邮件、Web浏览等，同时支持基于用户组和时间段配置策略，实现精细化管理；
- ARP防护：支持IP与MAC地址自动扫描及一键绑定功能，有效防止ARP欺骗和非法接入；在遭受ARP欺骗时，路由器可按照指定频率发送ARP更正信息，及时恢复网络正常状态；
- 攻击防护：支持内外网攻击防护功能，可有效防范各种常见的DoS攻击、扫描类攻击、可疑包攻击行为，如：TCP Syn Flood、UDP Flood、ICMP Flood、WinNuke攻击、分片报文攻击、WAN口ping、TCP Scan（Stealth FIN/Xmas/Null）、IP欺骗等。

带宽控制

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

连接数限制

- 提供基于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，确保游戏、上网、聊天、视频语音等顺畅进行。

设备管理

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

设备维护

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

2.3 产品外观

2.3.1 前面板

TL-ER7520G的前面板由5个自定义接口、1个Console接口、指示灯和Reset键组成。如图2-1所示。

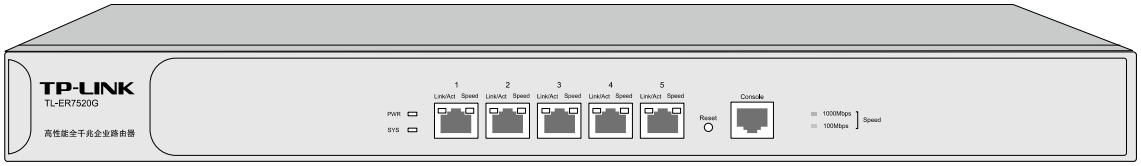


图 2-1 TL-ER7520G前面板示意图

- 5个10/100/1000Mbps自适应RJ45接口

TL-ER7520G支持10Mbps/100Mbps/1000Mbps速率的连接设备。每个接口对应一组指示灯，即Link/Act和Speed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。

- Reset键

复位键。在路由器通电的情况下，使用尖状物长按路由器的Reset按键，直至系统指示灯快速闪烁时松开，路由器将自动恢复出厂设置并重启。路由器出厂默认管理地址是http://192.168.1.1，默认用户名和密码均为admin。

- 指示灯

指示灯包括PWR电源指示灯，SYS系统指示灯，Link/Act连接状态指示灯，Speed速率指示灯。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	系统上电后，常灭约40秒后持续快闪，直至系统开始正常工作，如果需要加载的软件功能较多，系统启动时间可能需要数分钟，请耐心等待
		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	连接状态指示灯	常亮表示相应端口已正常连接
		闪烁表示相应端口正在传输数据
		常灭表示相应端口未建立连接
Speed	速率指示灯	常亮绿色表示相应端口工作在1000Mbps模式
		常亮黄色表示相应端口工作在100Mbps模式
		常灭表示相应端口工作在10Mbps模式或链路未建立

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：

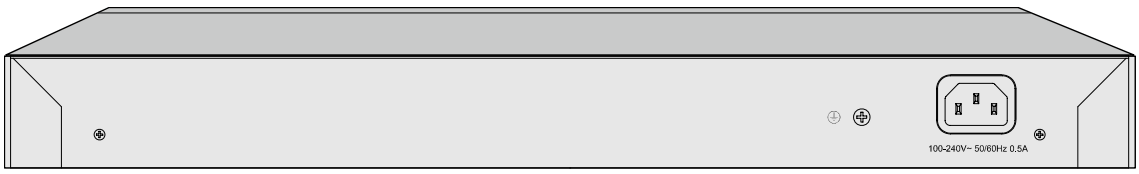


图 2-2 后面板示意图

- 电源接口

位于后面板右侧，设备正常工作时的输入电源参数为100-240V~ 50/60Hz，最大工作电流不超过0.5A，为保证设备及电源设施正常工作，请确保供电电源完全满足设备的要求。

- 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》。

说明：

- 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 基本设置

3.1 系统状态

路由器成功登录后可以看到路由器的系统状态信息，如图 3-1 所示。

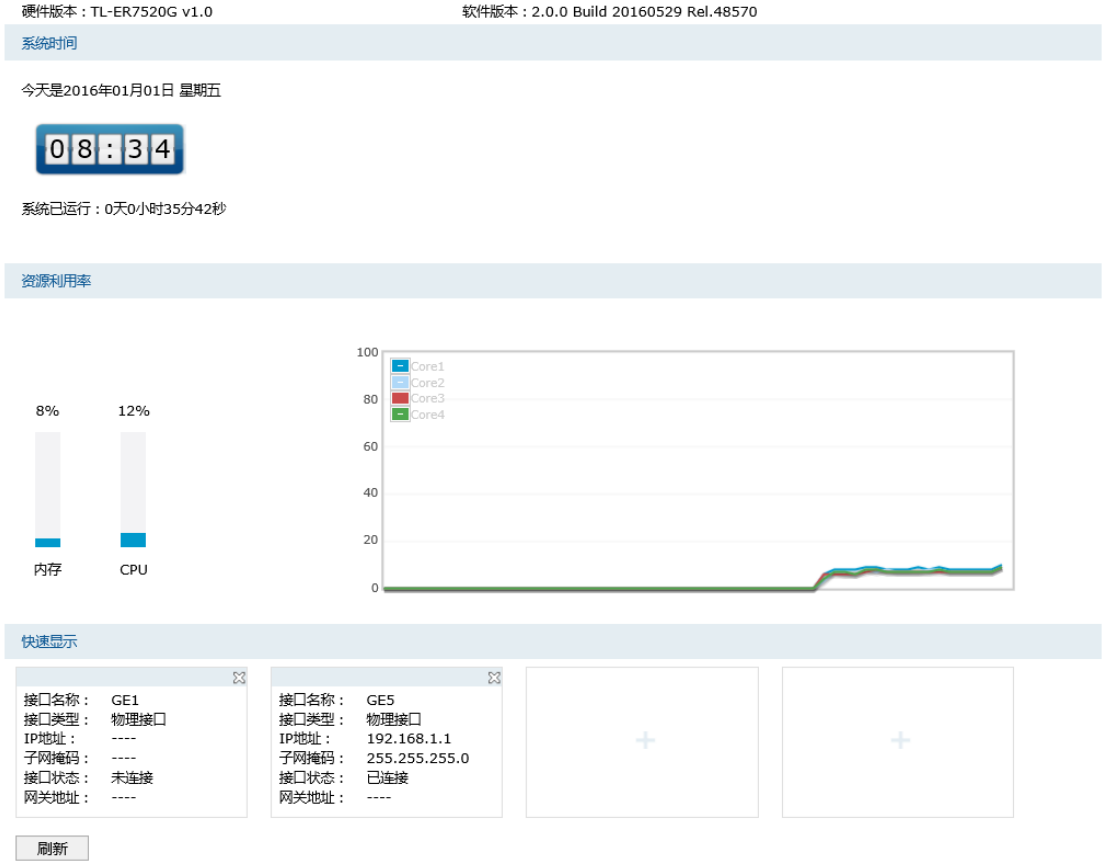


图 3-1 系统状态

在系统状态界面中，可以查看路由器的硬件和软件版本、系统 时间、CPU 利用率和接口信息。

系统时间：显示路由器当前的系统时间。

资源利用率：在此区域可检测路由器内存和 CPU 的利用率。CPU 利用率平均推荐值为 50%左右，高于 85%表示路由器处于高负载状态，高于 95%表示满负载状态，当 CPU 利用率持续较高时，部分功能可能将异常，此时可能是网络中出现异常，请进行排查。

快速显示：点击各区域的< + >按钮可添加并查看接口信息。

3.2 接口设置

为理解本路由器接口的含义，下面分别介绍物理接口和接口的概念。

■ 物理接口

物理接口是设备上实际存在的组件。接口命名约定因设备而异。物理接口的名称由媒体类型、插槽号（对于某些设备）及索引号组成，例如：ethernet3/2或ethernet2。

TL-ER7520G的物理接口命名为端口1/2/3/4/5，只支持以太网这一种媒体类型，如图 3-2所示。

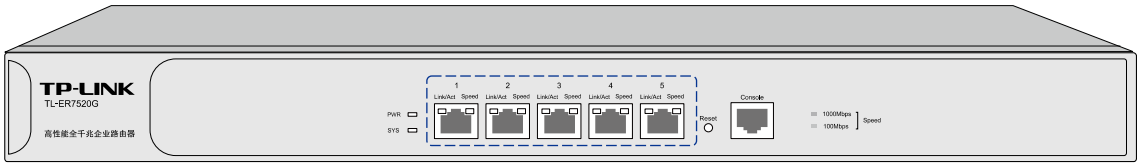


图 3-2　物理接口概念示意图

■ 接口

在支持VLAN（Virtual Local Area Network，虚拟局域网）的设备上，可以在逻辑上将一个物理接口划分为多个虚拟的接口，每个接口使用的带宽都来自它所属的物理接口。

TL-ER7520G用来划分物理接口的接口有Ethernet、PPPoE两种类型。Ethernet是以太网接口，功能上与以太网物理接口相同。Ethernet接口由802.1Q VLAN标记进行区分，PPPoE由相关的协议字段进行区分。

TL-ER7520G提供Ethernet和PPPoE两种类型的接口：

- Ethernet接口：以太网接口，必须与一个VLAN和一个MAC地址相对应。提供静态IP与DHCP两种连接方式。一般光纤接入以及企业、网吧局域网内组网使用静态IP连接方式，有线宽频使用DHCP连接方式。
- PPPoE接口：提供PPPoE连接方式的接口。xDSL拨号上网使用PPPoE连接方式。

说明：

以上提到的三种接入方式：静态IP、DHCP和PPPoE都可以连接到广域网，具体使用情况请根据ISP（Internet Service Provider，网络服务提供商）提供的服务进行选择。

3.2.1 接口设置

在本页面可选择在不同的物理接口下创建不同的 Ethernet 接口和 PPPoE 接口。

进入界面：基本设置>> 接口设置 >> 接口设置

图 3-3 接口设置界面

在**接口设置**界面中，选择物理接口作为关联接口，点击<新增>按钮，可新建 Ethernet 或 PPPoE 接口。

■ Ethernet接口

Ethernet接口有两种连接方式，图 3-4是静态IP连接方式，图 3-5是DHCP连接方式。

图 3-4 Ethernet接口设置-静态IP连接方式

接口类型	选择Ethernet接口类型。
接口名称	输入一个名称来标识一个接口。只能输入英文、数字和下划线。
关联接口	在此选择一个物理接口作为其关联接口。

关联VLAN	输入一个该接口所属VLAN的VLAN ID。当勾选“UNTAG”时，从该接口发出的报文不带VLAN TAG；当不勾选“UNTAG”时，从该接口发出的报文带有VLAN TAG。
连接方式	选择连接方式，有静态IP和DHCP两种连接方式。 选择静态IP连接方式，需要进行手动配置IP地址；选择DHCP连接方式，由路由器动态获取IP地址。
IP地址	设置接口的IP地址。
子网掩码	设置接口的子网掩码。
网关地址	设置网关地址，允许留空。
上行带宽	设置接口的上行带宽，取值范围为100-1000000Kbps，默认为1000000Kbps。
下行带宽	设置接口的下行带宽，取值范围为100-1000000Kbps，默认为1000000Kbps。
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，允许留空。
备用DNS服务器	设置备用DNS地址，允许留空。
MAC地址	设置接口的MAC地址。
备注	填写对该接口的备注信息。
管理接口开启	勾选该项使该接口成为管理接口。

表 3.1 Ethernet接口设置界面静态IP连接方式条目项说明

图 3-5 Ethernet接口设置-DHCP连接方式

接口类型	选择Ethernet接口类型。
接口名称	输入一个名称来标识一个接口。只支持英文、数字和下划线。
关联接口	在此选择一个Ethernet接口作为其关联接口。
关联VLAN	输入一个该接口所属VLAN的VLAN ID。当勾选“UNTAG”时，从该接口发出的报文不带VLAN TAG；当勾选“UNTAG”时，从该接口发出的报文带有VLAN TAG。
连接方式	选择连接方式，有静态IP和DHCP两种连接方式。 选择静态IP连接方式，需要进行手动配置IP地址；选择DHCP连接方式，由路由器动态获取IP地址。
主机名	输入用于标识路由器的名称。
上行带宽	设置接口的上行带宽，取值范围为100-1000000Kbps，默认为1000000Kbps。
下行带宽	设置接口的下行行带宽，取值范围为100-1000000Kbps，默认为1000000Kbps。
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。

备用DNS服务器	设置备用DNS地址。
MAC地址	设置接口的MAC地址。
备注	输入对该接口的备注信息。
管理接口开启	勾选该项使该接口成为管理接口。

表 3.2 Ethernet接口设置界面DHCP连接方式条目项说明

■ PPPoE接口

说明：

新建PPPoE接口，必须保证在同一物理接口下有Ethernet接口可供选择，如需新建Ethernet接口，请参考**3.2.1接口设置 □ Ethernet接口**。

PPPoE接口的设置界面如下图所示。

图 3-6 PPPoE接口设置

接口类型	选择PPPoE接口类型。
接口名称	输入一个名称来标识一个接口。只支持英文、数字以及/ \ . _ - @六个特殊字符，最多可以输入15个字符。
关联接口	在此选择一个Ethernet接口作为其关联接口。
用户名	PPPoE拨号的用户名，由ISP提供。可以输入1-100个字符，不支持中文字符。

密码	PPPoE拨号的密码，由ISP提供。可以输入1-100个字符，不支持中文字符。
连接方式	选择上网时连入互联网的方式，共有自动连接、手动连接和定时连接三种方式可供选择。 • 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。 • 手动连接：需手动拨号连入互联网，适合按小时计费的拨号连接上网方式。 • 定时连接：在**时间**下拉列表中选择时间表，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。如需新建时间表，请参考**时间管理**
时间	当连接方式选择“定时连接”时，可在下拉列表中选择时间表，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。如需新建时间表，请参考**时间管理。**
上行带宽	设置接口的上行带宽，取值范围为100-1000000Kbps，默认为1000000Kbps。
下行带宽	设置接口的下行行带宽，取值范围为100-1000000Kbps，默认为1000000Kbps。
MTU	MTU（Maximum Transmission Unit，最大传输单元），可以设置数据包的最大长度。取值范围是576-1492之间的整数，默认值为1492。若ISP未提供MTU值，请保持默认值不变。
服务名	输入服务名称，由ISP提供。
首选DNS服务器	设置DNS（Domain Name Server，域名解析服务器）地址，允许留空。
备用DNS服务器	设置备用DNS地址，允许留空。
备注	输入对该接口的备注信息。
管理接口开启	勾选该项使该接口成为管理接口。

表 3.3　PPPoE接口设置界面条目项说明

配置接口步骤：

1) 创建Ethernet接口。必须操作。创建界面：基本设置 >> 接口设置 >> 接口设置，点击<新增>按钮，在显示的新增接口设置页面，选择接口类型为Ethernet，选择关联的VLAN，输入接口名称等必要信息，点击<确定>按钮完成。

2) 创建PPPoE接口。非必须操作。创建界面：基本设置 >> 接口设置 >> 接口设置，点击<新增>按钮，在显示的新增接口设置页面，选择接口类型为PPPoE，选择其关联接口，输入接口名称等必要信息，点击<确定>按钮完成。

3.2.2 网桥设置

网桥可以在数据链路层上实现局域网互连，并对网络数据的流通进行管理。在TL-ER7520G中，通过创建网桥接口，可以将多个物理接口级联在一起（其中GE5将会默认被包含），达到不同接口之间互通的目的 。当前系统的网桥接口一般作为"LAN"接口使用。而被桥接的接口配置其它任何业务都将无效。

进入界面：基本设置 >> 接口设置 >> 网桥设置

点击<新增>按钮，进入网桥设置页面

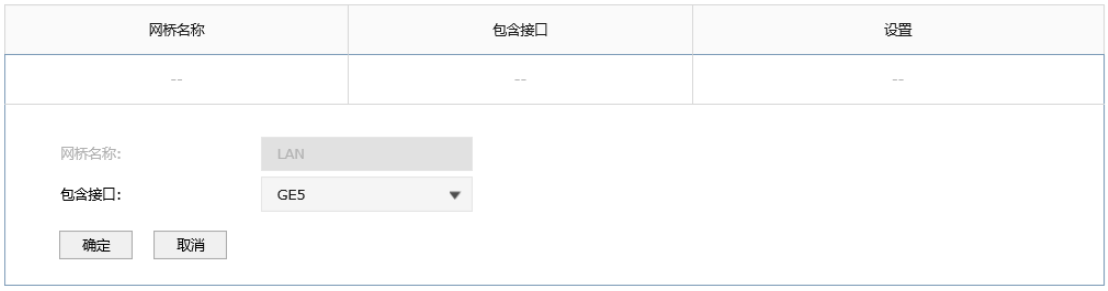


图 3-7 网桥设置

网桥名称	默认为“LAN”，不可更改。
包含接口	选择网桥所需包含的接口。

表 3.4 网桥设置界面条目项说明

新增的条目会在**网桥设置列表**里显示出来，如下图所示。

图 3-8 网桥列表

点击条目后的<>按钮可删除网桥。

说明：

路由器需要在出厂设置状态下才能进行网桥接口配置，请先到"系统工具->设备管理->恢复出厂配置"页面进行恢复设置。

3.3 DHCP 服务

当网络存在以下需求时，可以通过DHCP服务器完成网络设备的IP地址配置：

- 网络规模大，为每台网络设备手工配置网络参数的工作量较大时。
- 网络中设备数量远远大于该网络可使用的IP地址数量，而同一时间上网的设备数目却不多。例如，ISP限制同时接入网络的用户数目，而网络中的用户并不需要同时访问网络，则用户可以动态按需获得网络IP。
- 网络中只有少数主机需要固定的IP地址，大多数主机没有固定的IP地址需求。

3.3.1 DHCP 协议介绍

DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）协议应用于TCP/IP网络中，基于该协议标准，DHCP服务器给网络中的DHCP客户端动态分配IP地址等网络参数，以便于网络管理员对网络中计算机的TCP/IP参数进行统一管理。

当网络规模扩大，计算机数量日益增多时，DHCP功能能够高效的完成TCP/IP参数配置，并将IP地址循环运用，提高使用效率。而随着无线网络的广泛使用，计算机的位置也经常变化，其所连接的子网也处于动态变化的过程，由此产生的TCP/IP参数变更问题基于DHCP也能够高效解决。

本路由器可以作为 DHCP 服务器为网络中的计算机分配 TCP/IP 参数。

本小节主要介绍DHCP工作过程中采用的**DHCP报文格式**以及**DHCP地址分配过程**。

■ DHCP报文格式

DHCP报文的封装格式如下图所示：

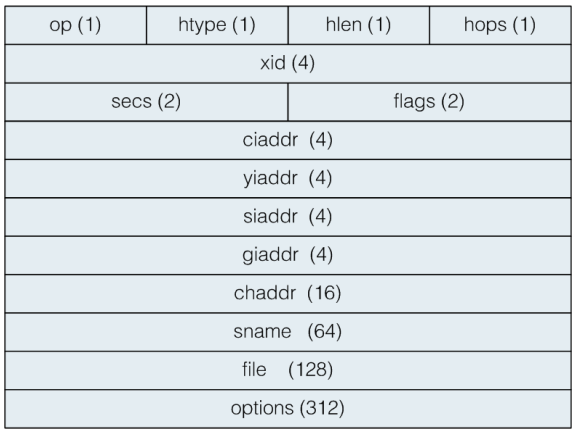


图 3-9 DHCP报文格式

OP	报文类型，分为请求类型报文和应答类型报文，1表示此数据包为客户端发出DHCP请求报文，2表示此数据包为服务器相应客户端的DHCP应答报文。

htype	DHCP客户端的网卡类型，常见的类型有ethernet，当htype字段值为1时表示DHCP客户端的网卡为以太网网卡。
hlen	DHCP客户端的网卡地址长度，如果是以太网网卡，则hlen字段值为6字节。
hops	DHCP客户端发出DHCP请求报文时，此字段值设置为0，请求报文在网络中每经过一个DHCP中继，该字段值自动加1，通过此字段可以确定DHCP客户端与服务器之间经过了几个网络。
xid	DHCP客户端发出DHCP请求报文时，在此字段设置一个随机数，网络中不同的DHCP请求过程可通过不同的xid字段值进行区分，DHCP服务器对每个不同的DHCP请求分配不同的地址，DHCP客户端只能接受响应给他的DHCP应答报文，并接受第一个DHCP应答报文分配的IP地址。
secs	DHCP客户端开始DHCP请求时，在DHCP报文的secs字段设置为0，并作为起始时间来统计DHCP请求过程总共花费的时间。目前没有使用，固定为0。
flags	此字段的第一个bit位表示DHCP应答报文的发送方式，1表示广播报文，0表示单播报文，其余bit位目前保留，固定为0。
ciaddr	DHCP客户端的IP地址，DHCP客户端发出请求报文时可根据需要填入原先获得的IP地址。
yiaddr	DHCP服务器分配给客户端的IP地址。
siaddr	为DHCP客户端分配IP地址等信息的服务器IP地址。
giaddr	DHCP中继设备的IP地址。
chaddr	DHCP客户端的硬件地址，以太网网卡的MAC地址。
sname	DHCP服务器名称，可选项。
file	DHCP服务器为客户端指定的启动配置文件名称及路径信息。
options	可选变长选项字段，选项中可以记录DHCP报文类型、有效租期、DNS服务器IP等配置信息。本设备暂不提供options选项识别及通过options选项分配IP地址。

表 3.4　DHCP报文字段含义

■ DHCP地址分配过程

在一个DHCP获取网络参数的过程中，其应用的传输层协议为UDP，客户端向服务器的DHCP服务端口67发出DHCP请求，服务器向客户端的DHCP用户端口68回复响应信息。DHCP客户端和服务器均按照DHCP协议标准格式报文发送DHCP报文。客户端通过动态分配地址的方式获取IP地址时，其获取IP地址的过程如下图所示：

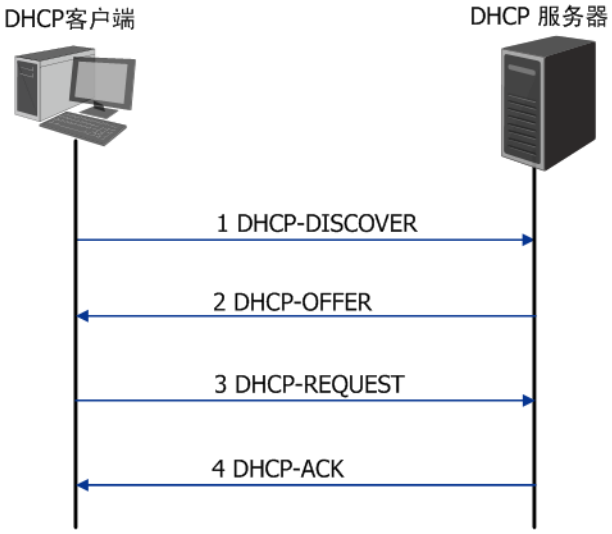


图 3-10　动态获取IP地址的过程

1) 发现阶段，客户端以广播方式发送DHCP-DISCOVER报文寻找DHCP服务器。

2) 提供阶段，DHCP服务器接收到客户端发送的DHCP-DISCOVER报文后，根据IP地址分配的优先次序从设定的地址段中选出一个IP地址，与其它参数一起通过DHCP-OFFER报文发送给客户端，发送方式由客户端发送的DHCP-DISCOVER报文中的flag字段决定，具体请见DHCP报文格式的介绍。

3) 请求阶段，如果有多台DHCP服务器向该客户端发来DHCP-OFFER报文，客户端只接受第一个收到的DHCP-OFFER报文，然后以广播方式发送DHCP-REQUEST报文，该报文的option字段包含DHCP服务器在DHCP-OFFER报文中分配的IP地址，具体请见DHCP报文格式的介绍。

4) 确认阶段，DHCP服务器收到DHCP客户端发来的DHCP-REQUEST报文后，只有DHCP客户端选择的服务器会进行如下操作：如果确认地址分配给该客户端，则返回DHCP-ACK报文；否则将返回DHCP-NAK报文，表明地址不能分配给该客户端。

5) 当客户端通过动态获取IP地址时，则DHCP服务器分配给客户端的IP地址具有一定的租期，当租期满后服务器将收回该IP地址。如果DHCP客户端希望继续使用该IP地址，在地址租期到达一半时，可以向服务器发送单播的DHCP-REQUEST报文续约IP地址。

3.3.2 DHCP 功能介绍

本节主要介绍在TL-ER7520G路由器上实现的DHCP服务器功能细节，主要包括五部分内容，动态地址分配策略、**DHCP服务器功能典型应用环境**、**DHCP服务器功能实现细节**、**IP地址重复分配检测**和**分配IP地址的优先次序**。

■ 动态地址分配策略

TL-ER7520G路由器支持两种地址动态分配策略：

- 为普通客户端分配具有一定有效期限的IP地址，如果客户端希望能够持续访问网络，在租约到期前客户端可以向服务器续约；
- 为特殊客户端静态绑定固定的IP地址，当收到来自特殊客户端的DHCP请求时，为其分配无限期的IP地址。

■ DHCP服务器功能典型应用环境

下图为路由器TL-ER7520G配置为DHCP服务器时的网络拓扑图使用示范，具体的网络环境可根据实际需要调整。

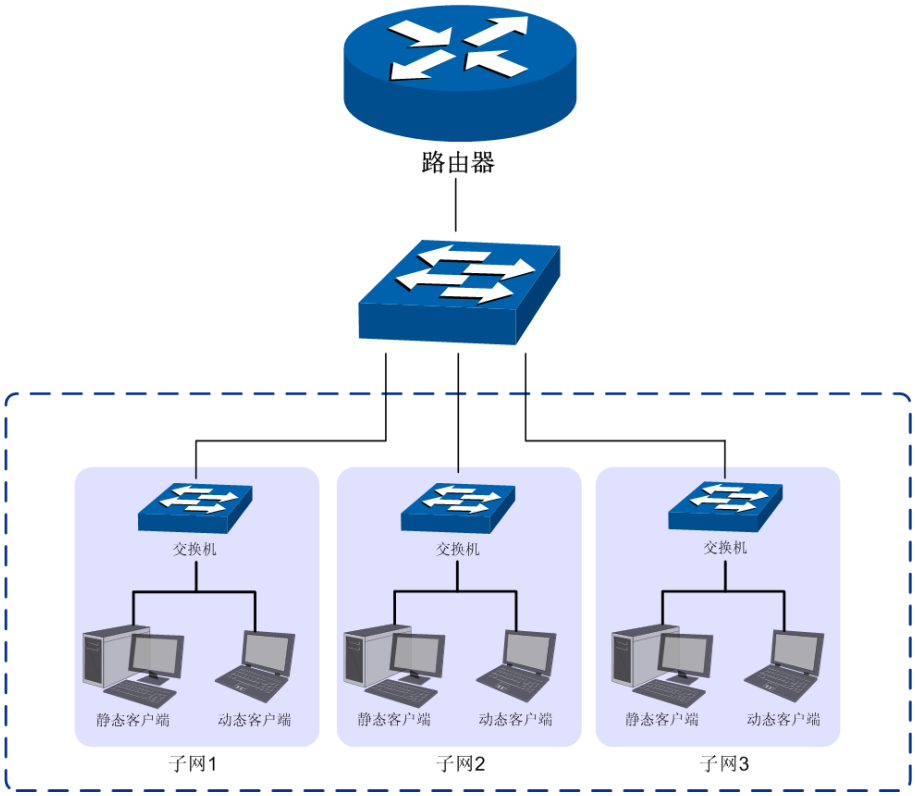


图 3-11 DHCP服务器功能应用环境

如图所示，某IT企业网络按照研发部门的分类分为软件小组、硬件小组和测试小组3个子网，在每个子网中，动态客户端通过“自动获取IP地址”的方式从TL-ER7520G路由器上获得各自所属子网的IP地址，静态客户端手动设置IP地址。

■ DHCP服务器功能实现细节

为了使网络中的设备能够安全顺利的获得IP地址，保证网络的稳定性，TL-ER7520G路由器的DHCP服务器功能可以完成如下任务：

1) TL-ER7520G可以为多达64个Ethernet接口类型网络分配地址。

说明：

- 如果Ethernet类型接口的IP地址是动态获取的，由于其IP地址的不确定性，因此暂不提供此类接口的DHCP服务器功能。
- 对于PPPoE接口，由于其IP地址的不确定性，TL-ER7520G路由器也暂不提供DHCP服务器功能。

2) 当TL-ER7520G收到DHCP请求报文时，将根据数据包中的VLAN ID信息选择相应接口设定的地址段来分配地址。

3) 为Ethernet类型接口网络中的特殊客户端手动绑定静态IP，当此接口收到特殊客户端的DHCP服务请求时，路由器将为客户端分配无限期的固定的IP地址。此类IP地址也会为特殊的客户端保留不会分配给其他客户端。

4) IP地址重复分配检测功能，为避免待分配地址已在网络中被使用，而导致分配后造成网络中IP冲突，路由器在分配一个IP地址前，会向所有接口网络发起待分配地址的Ping检测，从而避免IP冲突。

■ IP地址重复分配检测

路由器在分配一个IP地址前，会向所有接口网络发起目的地址为待分配地址的ICMP回显请求报文，如果任意一个接口在等待时间内收到响应报文，DHCP服务器从设定的地址段中选择新的IP地址，并重复上述探测操作；如果在指定时间内没有收到回显响应报文，则继续发送ICMP回显请求报文，直到发送的回显请求报文达到最大值，如果仍然没有收到回显响应报文，则将此待分配地址分配给客户端，从而确保客户端被分得的IP地址是网络中唯一的。

■ 分配IP地址的优先次序

TL-ER7520G路由器为客户端分配IP地址时将遵循以下分配规则秩序：

1) DHCP服务器中与客户端MAC地址手动绑定的IP地址。

2) DHCP服务器曾经分配给客户端的IP地址。

3) 客户端发送的DHCP-DISCOVER报文中指定的IP地址。

4) 选择合适的地址段，从中顺序查找可供分配的第一个IP地址。

3.3.3 DHCP 功能配置

DHCP功能配置主要分为**配置IP地址段**、**为特殊客户端绑定静态地址**和**查看当前所有的DHCP客户端**三部分进行配置。

配置IP地址段

进入界面：基本设置 >> DHCP服务 >> DHCP服务

在DHCP服务界面点击<新增>按钮，进入DHCP服务设置页面。

图 3-12 DHCP服务配置界面-配置地址段参数

服务接口	选择需要提供DHCP服务的Ethernet接口。
开始/结束地址	DHCP服务器自动分配的IP的开始/结束地址。
地址租期	输入此地址段中的IP地址在每次分配后可供客户端使用的租期。
网关地址	输入此地址段的给客户端分配的默认网关，也可以将接口IP地址配置为默认网关。
缺省域名	输入此地址段的给客户端指定的域，与IP地址一样共同表示相同子网的计算机的集合，同一接口网络中的计算机通常配置为相同的域名。
首选DNS服务器	输入此地址段的给客户端分配的首选DNS服务器，也可以将接口IP地址配置为DNS服务器地址，并由接口为客户端转发域名解析请求。
备用DNS服务器	输入此地址段的给客户端分配的备用DNS服务器，当首选DNS服务器失效时客户端可以向备用DNS服务器申请域名解析。
状态	选择“启用”，则使该绑定条目生效； 未选择“启用”，则使该绑定条目失效。

表 3.5 DHCP服务配置界面条目项说明

配置完成的地址段信息会在**DHCP服务器列表**区域显示出来，如下图所示。

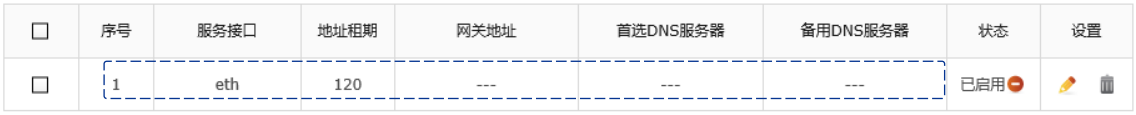


图 3-13 DHCP服务配置界面-地址段列表

如有需要，可以点击条目后的<>按钮进行编辑，点击<>按钮禁用条目，点击<>按钮删除条目。

■ 为特殊客户端绑定静态地址

路由器提供两种绑定方法为特殊客户端绑定静态地址，包括手动为特殊客户端绑定IP地址、以及批量导入静态绑定的IP/MAC地址表。

说明：

如果为特殊客户端绑定了静态地址，又设置了ARP防护功能的IP&MAC绑定，此时，请确保两处设置的表项互不冲突，否则对应的客户端可能无法上网。建议将ARP绑定表导出，然后再将其导入到DHCP静态绑定地址表中，请参考批量导入静态绑定的IP/MAC地址表进行配置。

手动为特殊客户端绑定IP地址

进入界面：基本设置 >> DHCP服务 >> 静态地址分配

点击<新增>按钮，进入静态地址设置页面。在界面中为具有设定MAC地址的客户端手动绑定静态IP，当条目服务接口收到来自设定客户端的DHCP服务请求时，路由器将为客户端分配租期为无限长的固定的IP地址，点击<确定>按钮手动创建条目。

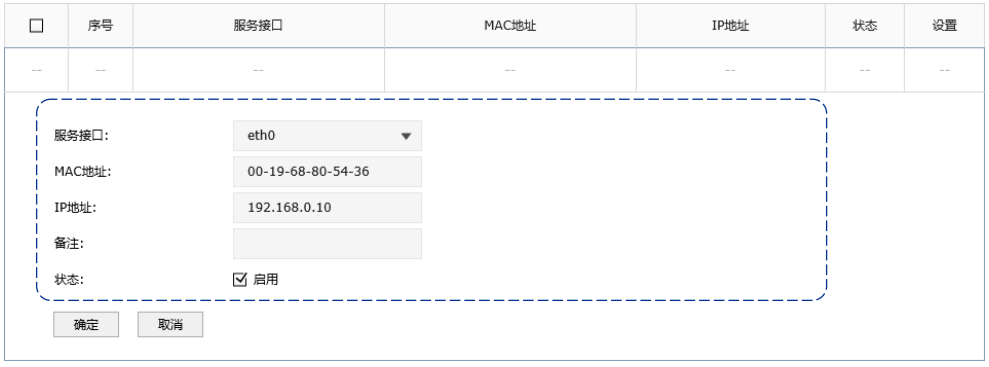


图 3-14 DHCP服务配置界面-静态地址分配

服务接口	选择保留IP地址所属的Ethernet接口。
MAC地址	输入特殊客户端的MAC地址。
IP地址	输入需要为特殊客户端保留的IP地址。该静态IP地址需与接口IP地址在同一网段。

备注	输入字符串描述该静态地址以便识别。
状态	选择“启用”，则使该绑定条目生效； 不选择“启用”，则使该绑定条目失效。

表 3.6　静态地址分配界面条目项说明

说明：

当其他非服务接口收到特殊客户端的DHCP请求时，将无法获得绑定的静态地址。若其他非服务接口也提供DHCP服务功能，则给特殊客户端分配其接口的IP地址段中的地址；如果其他非服务接口没有开启DHCP服务功能，特殊客户端将无法获得IP地址。

新增的静态地址绑定条目会在下方的**地址列表**区域显示出来，如下图中所示。

	序号	服务接口	MAC地址	IP地址	状态	设置
☐	1	eth	00-19-68-80-54-36	192.168.0.10	已启用	
☐	2	hard	00-36-56-32-58-69	192.168.20.10	已启用	

图 3-15　静态地址分配配置界面-静态地址列表

如有需要，可以点击条目后的<>按钮进行编辑，点击条目后的<>按钮启用条目，点击条目后的<>按钮禁用条目。

批量导入静态绑定的IP/MAC地址表

进入界面：基本设置 >> DHCP服务 >> 静态地址分配

当在**安全管理 >> ARP防护 >> IP MAC绑定**界面中已经对网络中客户端的IP和MAC信息进行绑定时，可以在DHCP的静态地址分配界面点击<导入>按钮批量导入。

说明：

如果IP MAC绑定条目与DHCP的静态地址分配条目有冲突，发生冲突的条目将不会被导入，没有发生冲突的条目将会继续被导入。

■ 查看当前所有的DHCP客户端

进入界面：基本设置 >> DHCP >> 客户端列表

在界面的**客户端列表**区域，可以查看当前已从TL-ER7520G路由器上获取TCP/IP网络参数的客户端MAC地址、其获得的IP地址以及IP地址的剩余租期，如下图所示。

图 3-16 DHCP服务器客户端列表

3.3.4 DHCP 功能组网应用

图 3-19为某企业网络的一个分支，网络需求如下：

- 由于部门人数较多，为了避免网络规模过大时容易产生的网络广播问题，研发部门又分为了软件小组、硬件小组和测试小组，3个小组在接入交换机和中心交换机中通过VLAN进行隔离，测试小组使用IP地址段192.168.10.0/24，硬件小组使用IP地址段为192.168.20.0/24，软件小组使用的IP地址段为192.168.30.0/24。
- 路由器TL-ER7520G为中心路由器，并在TL-ER7520G通过接口策略达到三层互通。
- 在每个小组中，移动客户端通过“自动获取IP地址”的方式从路由器上获取正确的子网IP地址，静态客户端手动设置IP地址。其中每个子网中的移动客户端数目最多为50台。

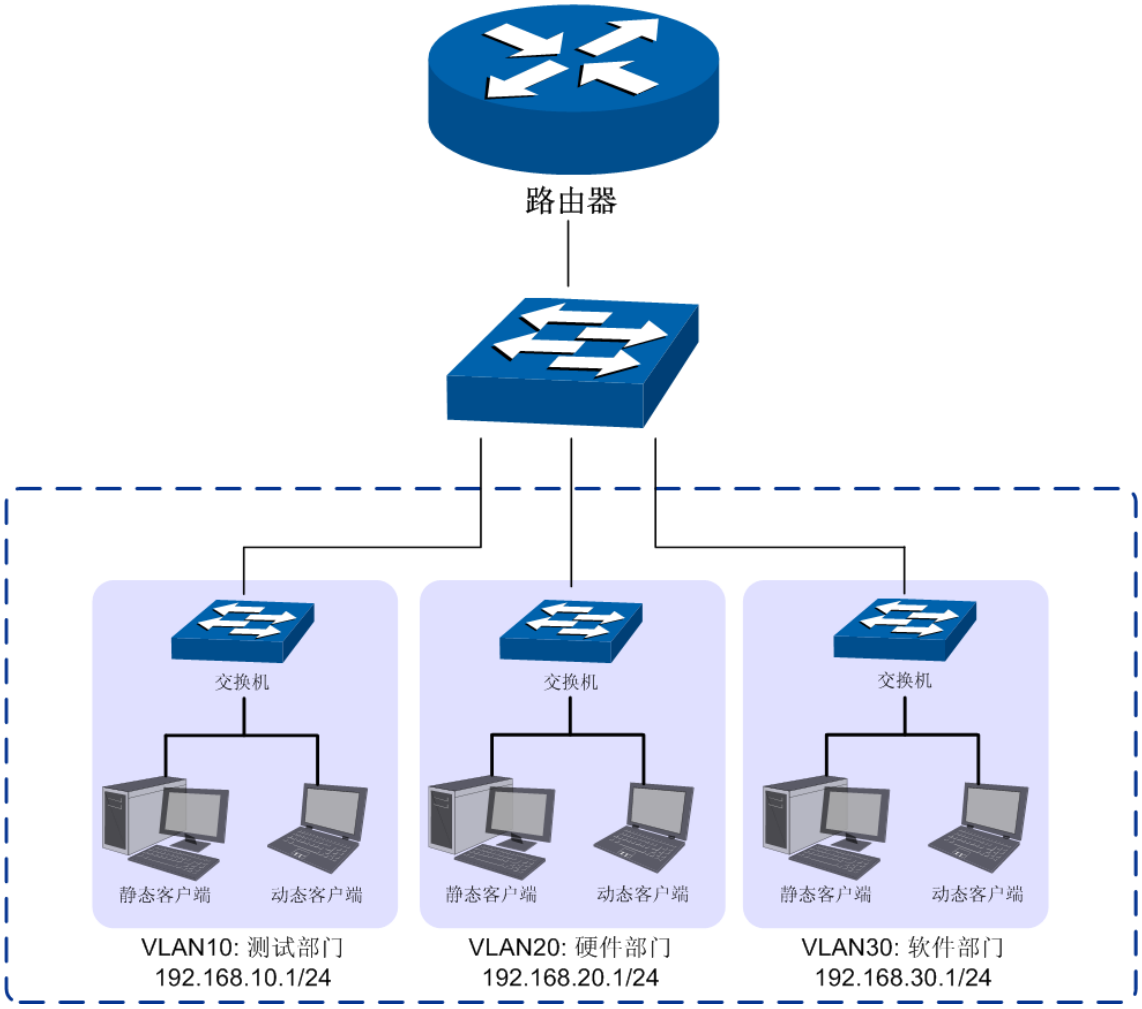


图 3-17 DHCP服务器功能组网举例

配置步骤：

如果要完成上述网络需求，需要按如下顺序配置路由器：

1) 创建Ethernet接口。必须操作。进入界面：基本设置 >> 接口设置 >> 接口设置，为研发各小组创建Ethernet类型接口，设置连接方式为静态IP。例如为硬件小组创建Ethernet接口，命名为“hard_dep”，接口地址设置为192.168.20.1/24并与VLAN20关联。

2) 为动态客户端配置DHCP服务器。必须操作。进入界面：基本设置 >> DHCP服务 >> DHCP服务，为研发各小组配置DHCP服务参数，例如为硬件小组关联的接口“hard_dep”配置DHCP服务参数，选择开始/结束地址段为硬件部门IP地址段，同时配置网关参数为“hard_dep”的接口地址192.168.20.1。

3) 为静态客户端绑定静态地址。必须操作。进入界面：基本设置 >> DHCP服务 >> 静态地址分配，为研发各小组静态客户端绑定静态地址，例如在硬件小组关联的接口“hard_dep”下，将静态客户端MAC地址和欲分配的静态IP地址进行绑定。

说明：

- 需要保证与路由器相连接的对端设备正确配置VLAN功能。如本案例中，对端交换机需要正确配置VLAN，向路由器转发数据包时需要添加VLAN Tag。只有收到的DHCP请求报文带有正确的VLAN Tag标识，路由器才会正确分配IP地址。
- 关于VLAN在交换机上配置的详细信息，请参考我司交换机的用户手册。

第4章 快速配置

对于网络知识以及本产品不熟悉的用户，可以通过快速配置向导，设置上网所需的基本网络参数，完成路由器的设置。同时，在快速配置完成之后，可以根据实际需求，到菜单项选择需要配置的功能，进一步设置路由器。

说明：

- 路由器需要在出厂配置状态下才能进行快速配置，如果路由器配置已修改，请先将路由器恢复出厂配置。恢复出厂配置界面：系统工具 >> 设备管理 >> 恢复出厂配置。
- 快速配置完成后，将覆盖路由器的所有配置，如果路由器配置已修改，且需要保存配置参数，可以在运行快速配置向导之前备份。备份界面：系统工具 >> 设备管理 >> 备份与导入配置。

点击主页左侧**快速配置**菜单，即可进入图 4-1所示的快速配置向导，单击<下一步>，可以开始设置。

图 4-1 快速配置向导设置界面

4.1 设置接口模式

本路由器默认为NAT网关模式。在该模式下，有多种WAN口模式可供选择：单WAN口、双WAN口、三WAN口和四WAN口。选择单WAN口，则端口1为WAN口模式；选择双WAN口，则端口1和端口2为WAN口模式；选择三WAN口或四WAN口，规则类似。相应的，非WAN口则被设置为LAN口。

图 4-2 快速配置设置界面-接口模式设置

单击<下一步>，进入**NAT模式-NAT-WAN1设置**界面。

4.2 设置WAN口

说明：

快速配置设置的WAN接口全部参与带宽控制和流量均衡。

在**NAT模式-NAT-WAN1设置**界面，如图 4-3所示，可以选择上网方式，并设置基本上网参数。本向导提供三种常用上网方式：静态IP、动态IP和PPPoE，请根据实际情况进行选择，并设置相应参数。

- 静态IP连接方式

若ISP（Internet Service Provider，网络服务提供商）提供了固定的IP地址，请选择静态IP手动配置WAN口参数。

图 4-3 快速配置设置界面-NAT模式-NAT-WAN1设置-静态IP连接方式

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。默认为0.0.0.0。

子网掩码	设置路由器WAN口的子网掩码。默认为255.255.255.0。
网关地址	设置网关地址，允许留空。
首选DNS服务器	设置DNS（Domain Name Server，域名解析服务器）地址，允许留空。
备用DNS服务器	设置备用DNS地址，允许留空。
上行带宽	设置当前WAN接口数据流出的带宽大小，可设置范围为100-1000000Kbps。
下行带宽	设置当前WAN接口数据流入的带宽大小。可设置范围为100-1000000Kbps。

表 4.1　WAN口设置界面静态IP连接方式条目项说明

- 动态IP连接方式

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 4-4　快速配置设置界面-NAT模式-NAT-WAN1设置-动态IP连接方式

连接方式	选择动态IP连接方式。
上行带宽	设置当前WAN接口数据流出的带宽大小，可设置范围为100-1000000Kbps。
下行带宽	设置当前WAN接口数据流入的带宽大小。可设置范围为100-1000000Kbps。

表 4.2　WAN口设置界面动态IP连接方式条目项说明

- PPPoE连接方式

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

图 4-5 快速配置设置界面-NAT模式-NAT-WAN1设置-PPPoE连接方式

连接方式	选择PPPoE拨号连接方式。
账号	PPPoE拨号的用户名，由ISP提供。可以输入1-100个字符，不支持中文字符。
密码	PPPoE拨号的密码，由ISP提供。可以输入1-100个字符，不支持中文字符。
上行带宽	设置当前WAN接口数据流出的带宽大小，可设置范围为100-1000000Kbps。
下行带宽	设置当前WAN接口数据流入的带宽大小。可设置范围为100-1000000Kbps。

表 4.3 WAN口设置界面PPPoE连接方式条目项说明

如果在图 4-2 **NAT模式-接口模式设置**界面，选择WAN数量大于1，则WAN1设置完成后，单击<下一步>，会进入其他WAN口设置界面。所有WAN口设置完成后，单击<下一步>，可以进入**NAT模式-NAT-LAN设置**界面。

4.3 设置 LAN 口

在**NAT模式-NAT-LAN设置**界面，可以设置路由器LAN口的IP参数，以及LAN口DHCP服务。路由器DHCP服务功能，能够为所有接入路由器并且应用DHCP服务的网络设备自动分配IP参数。

图 4-6 快速配置设置界面-NAT模式-NAT-LAN设置

IP地址	设置路由器LAN口的IP地址，局域网内部可通过该地址访问路由器。默认为192.168.1.1。
子网掩码	设置路由器LAN口的子网掩码。默认为255.255.255.0。
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“开启”。若选择“关闭”，则起始IP地址、结束IP地址、网关地址、首选DNS服务器、备用DNS服务器各项全部隐藏，不可设。默认为开启。
起始IP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。默认为192.168.1.100。
结束IP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。默认为192.168.1.199。
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，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。

表 4.4 LAN口设置界面条目项说明

设置完成后，单击<下一步>，可进入**完成快速配置向导**界面。确认配置配置结果，点击<完成>保存配置。

图 4-7 快速配置设置界面-完成快速配置向导

第5章 对象管理

5.1 地址管理

5.1.1 地址管理

可以在本页面设置自定义地址组，以方便对用户进行组管理。

进入界面：对象管理 >> 地址管理 >> 地址管理

点击<新增>按钮，进入地址组设置页面。填入新地址组的名称和备注信息，点击<确定>按钮手动添加条目。

图 5-1 地址管理界面

组名称	输入一个名称来标识一个组。只能输入英文、数字和下划线。
地址名称	勾选该组可以包含的地址或子组，此地址就包含在所选的组中。
备注	添加对当前组的说明信息。

表 5.1 地址管理界面项说明

新增的条目会在**组列表**里显示出来，如下图所示。

序号	组名称	地址名称	备注	设置
1	IPGROUP_ANY	---	IPGROUP_ANY	---
2	g_lan_ip	lan-ip	---	

图 5-2 组列表

如有需要，可点击条目后的<>按钮进行编辑。条目1为系统默认条目，不可操作。

5.1.2 地址

可以在本页面自定义地址，并加入到已有的组中进行组管理。

进入界面：对象管理 >> 地址管理 >> 地址

点击<新增>按钮，进入地址设置页面。填入地址名称，选择IP类型并填入IP信息，点击<确定>按钮手动添加条目。

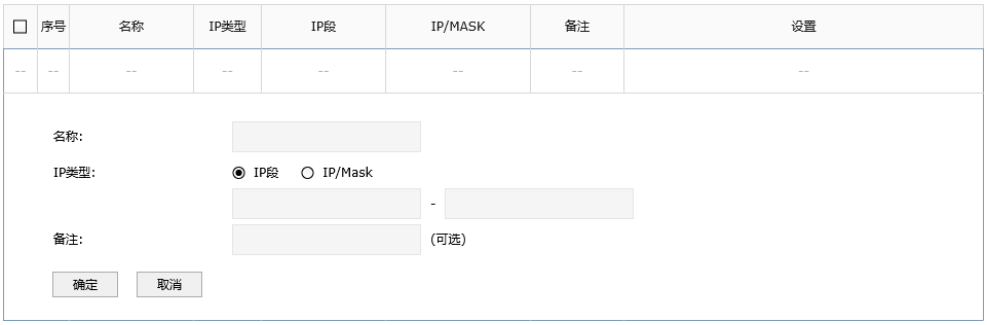


图 5-3 用户设置界面

名称	输入一个名称来标识地址。只能输入英文、数字和下划线。
IP类型	在此建立源地址范围。主要有以下2种表示方式。 IP段：由起始IP地址到结束IP地址确定IP地址范围。 IP/MASK：由IP地址和子网掩码确定IP地址范围。
备注	添加对当前地址的说明信息。

表 5.2 用户设置界面项说明

新增的条目会在**地址列表**里显示出来，如下图所示。

图 5-4 用户设置界面-地址列表

如有需要，可以点击条目后的<>按钮进行编辑。条目1为系统默认条目，表示任何地址，不可操作。

5.2 时间管理

5.2.1 时间管理

可以通过本页面创建时间对象，从而对时间进行管理。

进入界面：对象管理 >> 时间管理 >> 时间管理

点击<新增>按钮，进入时间对象设置页面。填入该时间对象的名称，时间设置可选择工作日历或手动设置，**图 5-5**为工作日历设置，**图 5-7**为手动设置。

图 5-5 时间管理-工作日历界面

名称	自定义的时间对象名称。只能输入英文、数字和下划线。
时间设置	选择“工作日历”。
工作日历	在此设置一个日历对象，点击图标后可设置具体的工作时间。
备注	输入对时间对象的具体描述。

表 5.3 时间管理界面项说明

点击“工作日历”，可以设置具体的工作时间，设置界面如下图所示。

图 5-6 工作日历设置

图 5-7 时间管理-手动设置界面

名称	自定义的时间对象名称。只能输入英文、数字和下划线。
时间设置	选择手动设置。
星期	选择工作日期。
时间段	选择工作时间段
备注	输入对时间对象的具体描述。

新增的条目会在**时间对象列表**里显示出来，如下图所示。

	序号	名称	工作日历	备注	设置
--	1	Any		Any time	
☐	2	t1		---	

图 5-8 时间管理界面-时间对象列表

如有需要，可以点击条目后的<>按钮进行编辑。条目1为系统默认条目，表示任何时间，不可操作。

5.3 IP地址池

可以通过本页面设置IP地址池条目，进行地址池的管理。

进入界面：对象管理 >>IP地址池 >> IP地址池

点击<新增>按钮，进入IP地址池设置页面。填入地址池名称和起始、结束IP地址，点击<确定>按钮手动添加条目。

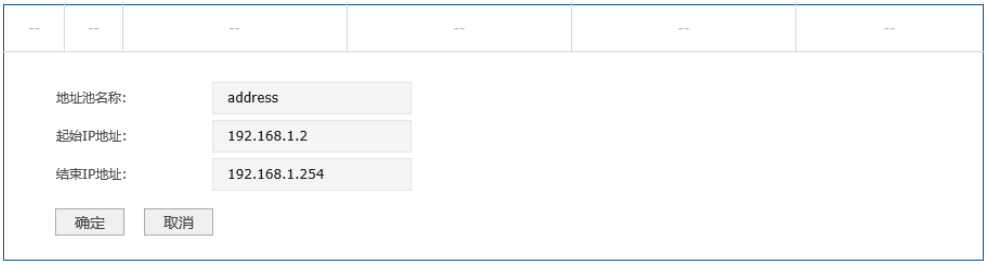


图 5-9 IP地址池设置界面

地址池名称	自定义地址池的名称。只能输入英文数字和下划线。
起始/结束IP地址	输入地址池起始IP和地址池结束IP，且起始IP必须不大于结束IP，而且不能与已有的地址池范围重叠。当前一个地址池最多可以包含1024个IP地址。

表 5.4 IP地址池界面项说明

新增的条目会在**地址池列表**里显示出来，如下图所示。

	序号	地址池名称	起始IP地址	结束IP地址	设置
☐	1	address	192.168.1.2	192.168.1.254	

图 5-10 IP地址池设置界面-地址池列表

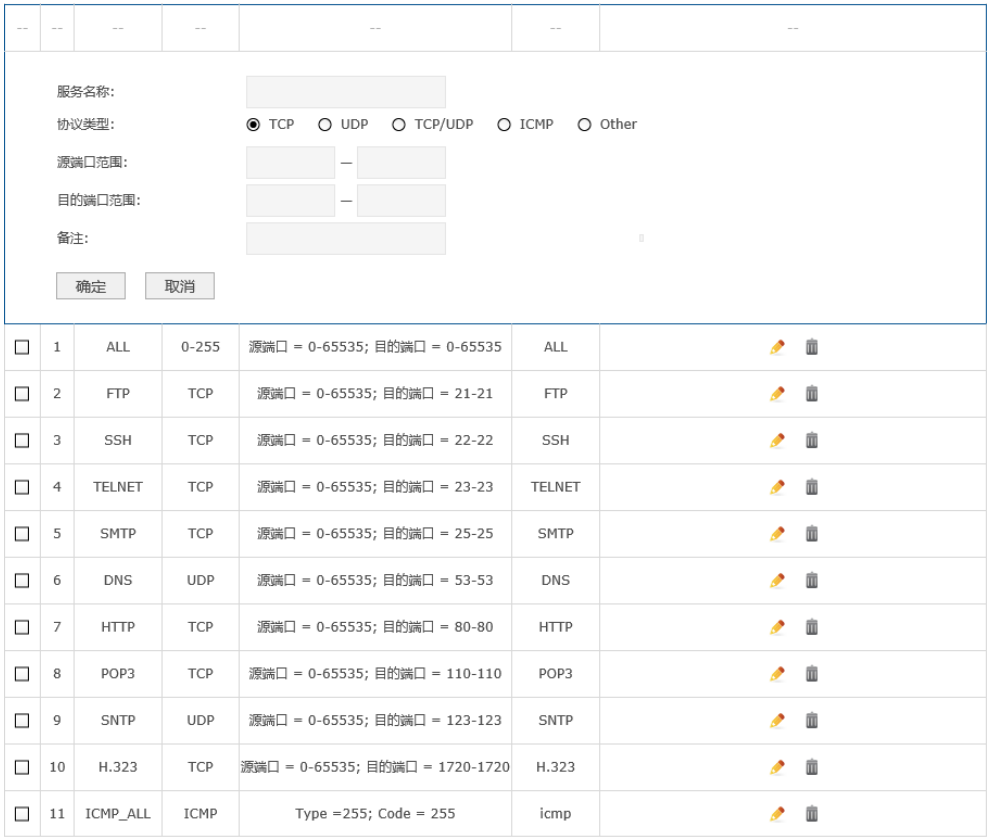
如有需要，可以点击条目后的<>按钮进行编辑，点击<>按钮可删除该地址池。

5.4 服务类型

可以在本页面设置自定义服务类型。

进入界面：对象管理 >> 服务类型 >> 服务类型

点击<新增>按钮，进入服务类型设置页面。填入服务名称，选择协议类型，并根据所选协议类型填写相应参数，点击<确定>按钮手动添加条目。



☐	1	ALL	0-255	源端口 = 0-65535; 目的端口 = 0-65535	ALL	
☐	2	FTP	TCP	源端口 = 0-65535; 目的端口 = 21-21	FTP	
☐	3	SSH	TCP	源端口 = 0-65535; 目的端口 = 22-22	SSH	
☐	4	TELNET	TCP	源端口 = 0-65535; 目的端口 = 23-23	TELNET	
☐	5	SMTP	TCP	源端口 = 0-65535; 目的端口 = 25-25	SMTP	
☐	6	DNS	UDP	源端口 = 0-65535; 目的端口 = 53-53	DNS	
☐	7	HTTP	TCP	源端口 = 0-65535; 目的端口 = 80-80	HTTP	
☐	8	POP3	TCP	源端口 = 0-65535; 目的端口 = 110-110	POP3	
☐	9	SNTP	UDP	源端口 = 0-65535; 目的端口 = 123-123	SNTP	
☐	10	H.323	TCP	源端口 = 0-65535; 目的端口 = 1720-1720	H.323	
☐	11	ICMP_ALL	ICMP	Type =255; Code = 255	icmp	

图 5-11 服务类型设置界面

服务名称	自定义服务的名称。只能输入英文、数字和下划线。
协议类型	在此选择服务所使用的协议。
源端口范围	输入服务所使用的源端口范围，仅TCP或UDP协议需要设置。
目的端口范围	输入服务所使用的目的端口范围，仅TCP或UDP协议需要设置。
Type	输入ICMP协议的类型(type)，填充255时表明所有类型/编码。
Code	输入ICMP协议的编码(code)，填充255时表明所有类型/编码。
协议号	当协议类型选择为“Other”时，在此输入该协议的协议号。
备注	输入对服务类型的具体描述。

表 5.5 服务类型界面项说明

第6章 传输控制

路由器上的各接口之间均工作在路由模式，各接口网络之间能够直接通信。设置合适的传输控制特性，可以保证本设备安全、快速、有序地转发数据。本设备提供了以下5种传输控制特性来保证网络的正常运行：

6.1 NAT设置：利用NAT技术，局域网中多个子网的计算机可以共享少量的广域网接口访问Internet，同时还将局域网信息屏蔽起来，NAT设置小节将详细介绍NAT技术和相关功能特性。

6.2 带宽控制：各接口之间发送数据时，可以通过带宽控制特性对数据传输的速率进行控制，从而使有限的带宽资源得到合理分配。带宽控制小节将详细介绍带宽控制的功能实现和配置方法。

6.3 连接数限制：路由器支持的TCP/UDP连接数是有限的，网络在繁忙时段发起的TCP和UDP数目有可能超过路由器支持的极限值，通信质量将可能受到影响。通过合理配置连接数限制特性，能够保证用户分配到特定的TCP/UDP连接数。

6.4 流量均衡：流量均衡功能采用流量均衡、选路、线路备份和在线检测等技术，使数据包可以按照指定的线路进行转发，从而使路由器更加安全有效的收发数据，提高网络性能。

6.5 路由设置：利用策略路由和静态路由功能，可以保证数据包在网络中以正确的路径进行快速转发。

6.1 NAT设置

本小节主要介绍NAT技术、本设备上实现的NAT功能特性以及相关功能的配置。

■ NAT技术简介

NAT（Network Address Translation，网络地址转换）可以实现局域网内的多台计算机通过1个或多个公网IP地址接入因特网。NAT设备在向广域网转发局域网数据时，使用特定的IP地址转换数据包中的源IP地址和传输端口，使局域网中的计算机共用少量的广域网IP地址与广域网中的计算机通信。NAT地址转换过程如下图所示：

图 6-1 NAT地址转换示意图

如图所示，NAT设备在向广域网转发数据包时，将数据包的源IP地址进行转换，将其转换为自身NAT接口的IP地址并将数据发送；当NAT收到广域网应答的数据包时，则根据NAT地址转换记录将数据包中的目的IP地址进行转换，并将其发往局域网中的指定主机。

在网络中使用NAT技术有效地解决了IP地址资源不足的问题，同时隐藏了局域网的计算机，使广域网计算机无法直接访问到局域网设备，为局域网提供了一定的安全保障。

■ NAT的分类

为适应网络中不同的需求，在实际网络应用中NAT有三种应用类型，分别为静态NAT、动态NAT、NAPT。

静态NAT：将私有网络的地址与广域网地址一对一映射，且映射关系是唯一的，某个私有网络IP地址转换为固定的公有IP地址。利用静态NAT转换，可以实现内部网络中的特定设备(如服务器) 对外部网络开放。

动态NAT：将私有网络的地址与广域网地址进行转换时，转换关系是随机的。只要指定了可以进行转换的私有网络地址，以及合法的广域网地址，就可以进行动态地址转换。动态NAT需要指定多个合法的广域网地址，当能够进行NAT转换的广域网地址数略少于局域网计算机的数量时，可以采用动态NAT。

NAPT：将私有网络地址映射成一个合法的广域网地址，同时通过不同的传输协议端口号与不同的内部主机应用相对应。

本设备提供了静态NAT和NAPT两种特性。

■ 本设备的NAT特性

本设备提供了下列5种NAT相关功能特性：

6.1.1 NAPT：指定IP地址范围内的主机访问Internet时，使用出接口的IP地址对数据包进行NAPT地址转换，并通过不同的传输协议端口号与内网主机的应用程序相对应。在此过程中，本设备记录相应的IP地址及传输协议端口的映射关系，并以此维持后续的相关通信过程，直到通信结束时释放相关端口以便后续使用。

6.1.2 一对一NAT：即静态NAT,将指定IP地址的设备与广域网地址建立一对一映射关系，多应用于局域网中搭建面向广域网的服务器。该设备与私有网络中的设备通信时将使用私有网络的IP地址，而向广域网提供服务时则可以使用广域网地址进行访问。映射关系一旦建立，则相应的公网IP地址只供给指定的局域网设备做NAT地址转换。当路由器收到发往该公网IP地址的数据时将转发到内部的服务器上。

6.1.3 虚拟服务器：设置了NAT相关功能后，因NAT防火墙的限制，广域网用户将无法访问到局域网中的服务器。通过设置虚拟服务器功能，可以保证局域网服务器向广域网正常提供服务。在本路由器上，当指定接口开放的外部端口收到访问请求时，将把访问请求转发到内部服务器上。

6.1.4 ALG服务：针对FTP、VPN隧道等特殊应用穿透NAT设备时出现的无法连接问题，本路由器提供的ALG服务能够保证此类特殊应用的正常使用。

6.1.5 NAT-DMZ：设置网络中的DMZ主机，DMZ主机将完全暴露在广域网中，通常DMZ主机就是一些必须公开的服务器设施，如企业Web服务器、FTP服务器和论坛等，解决安装NAT防火墙后外部网络不能访问内部网络服务器的问题，也为内部网络增加了一道安全缓冲区，更加保护内部网络的安全。

6.1.1 NAPT

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

■ 配置NAPT

进入界面：传输控制 >> NAT设置 >> NAPT

点击<新增>按钮，进入NAPT规则设置页面。填入该规则生效设备的IP地址范围并选择数据包转发接口，点击<确定>按钮手动添加条目。

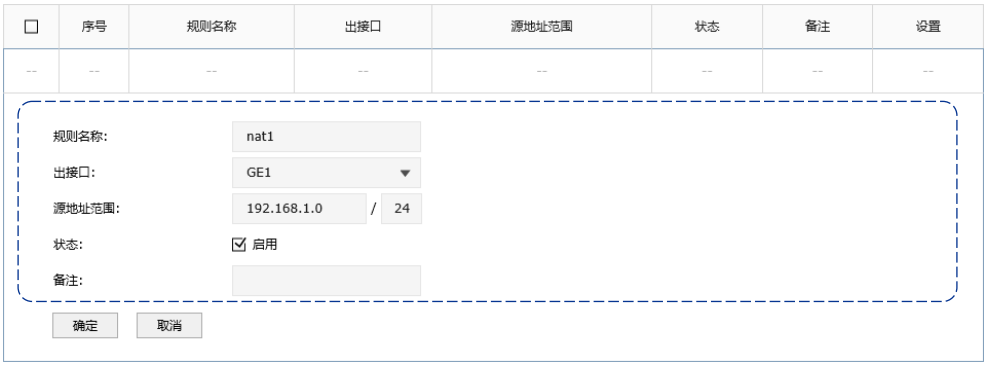


图 6-2 NAPT界面-设置NAPT规则

规则名称	输入该规则条目的名称。只能输入英文、数字和下划线。
出接口	选择该NAPT规则的生效接口，当数据包的源IP地址在源地址内，且从该接口转发时，路由器将对数据包进行NAPT地址转换。
源地址范围	设置IP地址范围，相应的NAPT规则条目只对源地址为设定范围内的数据包生效。
状态	勾选“启用”，则使该规则条目生效； 未勾选“启用”，则该规则条目无效。
备注	添加对本条目的说明信息，非必填项。

表 6.1 NAPT界面条目项说明

新增的条目会在**映射列表**中显示出来，如下图所示。

序号	规则名称	源地址范围	出接口	状态	备注	设置
1	nat1	192.168.0.0/24	eth0	已启用	---	
2	nat2	192.168.1.0/24	eth0	已启用	---	
3	nat3	192.168.3.56/32	eth0	已启用	---	
4	nat4	192.168.1.0/24	isp1	已启用	---	

图 6-3 NAPT界面-映射列表

如有需要，可以点击条目后的<>按钮进行编辑，点击<>按钮启用条目，点击<>按钮禁用条目。

如图 6-3 所示，“eth0”和“isp1”接口连接到广域网，图中4条规则分别表示含义：

1) 序号为1和2的规则表示192.168.0.0/24和192.168.1.0/24两个子网中的计算机通过“eth0”接口访问外部网络时均需要进行NAPT地址转换，共用接口的IP地址上网；

2) 序号为3的规则表示计算机192.168.3.56通过“eth0”接口上网时需要进行NAT地址转换，使用接口的IP地址上网；

3) 当网络中存在多条外线接口时，如图中“eth0”和“isp1”，访问Internet的数据包有可能通过其他接口直接转发到Internet中，在这种情况下，需要在路由器上设置多个NAPT条目来保证数据包转发到Internet时均做NAPT地址转换。图中序号为2和4的规则表示，192.168.1.0/24子网中的计算机通过“eth0”和“isp1”两条外线访问网络时本设备均会对数据包做NAPT地址转换。

4) 当局域网中所有主机均需要访问Internet时，您需要为所有子网都建立NAPT规则，此时可以通过设置全0规则快速设置，源地址范围设置为0.0.0.0/0即可，如下图所示，图中创建的规则表示所有从“isp1”接口转发的数据均做地址转换。

图 6-4 NAPT界面-全0规则

说明：

- 设置NAPT规则时，请注意出接口相同的NAPT规则源地址范围不能互相重叠，否则会引起范围冲突导致无法配置成功。
- 设置全0规则时，请不要设置其他NAPT规则，否则会引起范围冲突导致无法配置成功。

■ 应用环境

如图 6-5所示，在企业原有网络中，利用三层交换机组建一个交换式网络，但因网络需求变更，网络中192.168.2.0 /24网段和192.168.10.0/24网段需要访问网络，并从电信和联通各申请了一条线路同时提供上网服务，两条线路实现负载均衡，网络通过TL-ER7520G上网。

分析如下：

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

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

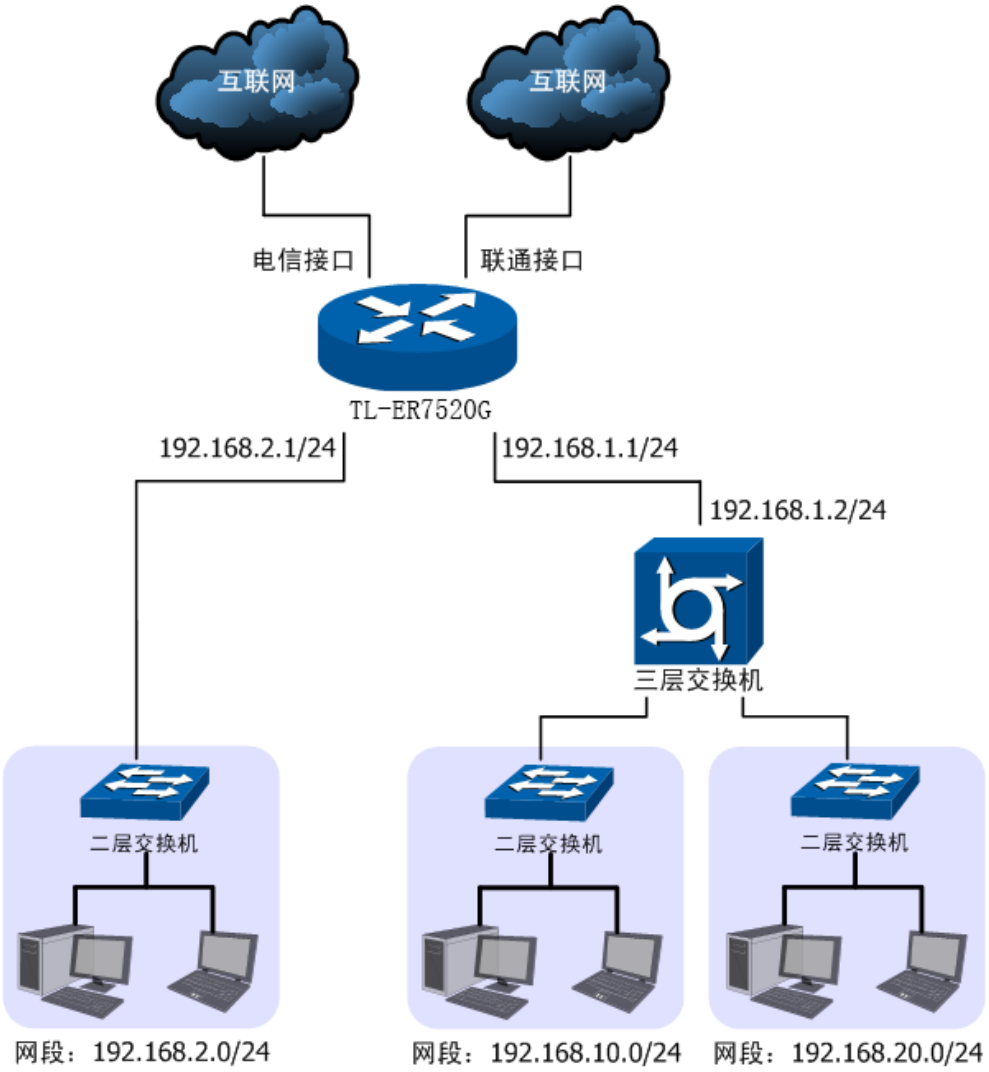


图 6-5 NAPT功能组网应用

配置步骤：

TL-ER7520G路由器要完成上述网络需求，需要配置NAPT功能和路由功能，配置步骤如下：

1) 设置NAPT规则，必须操作。创建界面：传输控制 >> NAT设置 >> NAPT。配置192.168.2.0/24和192.168.10.0/24两个网段的数据从电信和联通两个接口转发时做NAPT地址转换，分别需要建立两个NAPT规则条目。配置分别如下图所示。

图 6-6 电信接口NAT设置

图 6-7 联通接口NAT设置

2) 设置静态路由，必须操作。创建界面：传输控制 >> 路由设置 >> 静态路由。对于网段192.168.10.0/24，其通过三层交换机连接到路由器的192.168.1.1/24接口，因此需要在路由器上建立静态路由条目，使网络192.168.10.0/24在路由器上路由可达。静态路由条目配置如图 6-8所示。

图 6-8 静态路由设置

其中目的地址和子网掩码表示此静态路由条目指向的目标网络，下一跳指通往目标网络的路径上下一个网络节点的 IP 地址，出接口表示从路由器上的哪个接口转发数据包，Metric 表示该路径的度量值，请保持为 0，以保证该静态路由条目为最优路径。静态路由相关配置方法请参考 **6.4.4 在线检测**

进入界面：传输控制 >> 流量均衡 >> 在线检测

该页面用于检测接口是否在线。在线检测列表如下图所示。

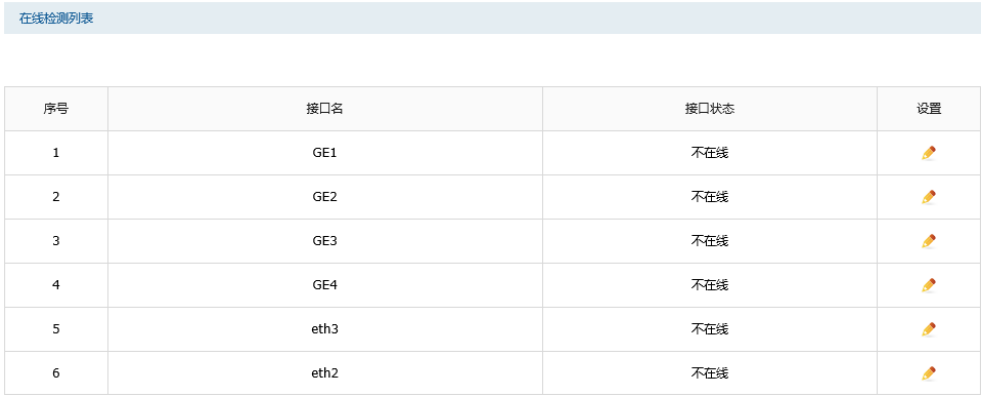


图 6-34 在线检测界面-接口状态列表

如有需要，可以点击条目后的<>按钮进行编辑。

图 6-35 在线检测界面

接口名	选择需要在线检测的接口。
检测模式	选择自动在线检测、手动在线检测或永远在线,默认为自动在线检测模式。自动模式下，PING检测选择网关作为目的地址，DNS检测选择接口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；永远在线模式下，该接口会被强制设置为永远在线，无需检测。
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。

表 6-10 在线检测界面项说明

6.1.2 一对一NAT

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

■ 配置一对一NAT

进入界面：传输控制 >> NAT设置 >> 一对一NAT

点击<新增>按钮，进入一对一NAT规则设置界面。在界面填入映射规则地址参数并选择数据包转发接口，点击<确定>按钮手动添加条目。

图 6-9 一对一NAT界面-设置NAT规则

映射名称	输入该映射条目的名称，例如可以根据服务器提供的服务特性命名。只能输入英文、数字和下划线。
出接口	选择此一对一NAT映射规则的生效接口。当数据包从该接口转发时，设备根据映射后的地址对数据包进行地址转换；对映射后地址的访问请求将转发到局域网中的服务器上。
映射前地址	输入服务器的局域网IP地址。
映射后地址	填写映射后的IP地址。
DMZ转发	设置是否开启该条NAT映射条目的DMZ转发。启用DMZ转发后，规则生效接口收到目的IP地址为映射后地址的数据包时，将把数据包转发给局域网服务器。如果广域网用户需要自由的访问局域网服务器，需要启用DMZ转发，若不开启，路由器将拒绝用户对服务器的访问。
备注	添加对本条目的说明信息，非必填项。
状态	勾选“启用”，则使该规则条目生效； 不勾选“启用”，则使该规则条目失效。

表 6.2 一对一NAT界面条目项说明

新增的条目会在**映射列表**中显示出来，如下图所示。

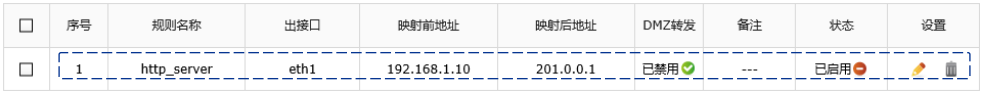


图 6-10 一对一NAT界面-映射列表

如图所示，虚线框中的条目表示：路由器通过接口“isp1”转发来自设备192.168.1.10的数据包时，将对数据包做NAT地址转换，将源IP地址转换为201.0.0.1；路由器的“eth1”接口收到目的地址为201.0.0.1的响应数据时，将转发给局域网中的设备192.168.1.10。

没有开启DMZ转发，则“eth1”接口收到目的地址为201.0.0.1的访问请求时，会拒绝处理；如果开启了DMZ转发，则表示“eth1”接口收到目的地址为201.0.0.1的数据包时都转发给设备192.168.1.10。

如有需要，可以点击条目后的<>按钮进行编辑，点击<>按钮启用条目，点击<>按钮禁用条目。

说明：

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

■ 应用环境

如图 6-11所示，某企业向电信申请了两个公网IP“201.1.1.1”和“201.1.1.2”，其中地址“201.1.1.1”用于为局域网计算机共享上网，而地址“201.1.1.2”则用于企业服务器192.168.100.5为广域网提供服务。

分析如下：

1) 针对服务器192.168.100.5，需要创建一对一NAT规则，保证数据从电信接口转发到广域网时使用固定的IP地址进行转换，同时广域网用户可以通过固定的IP地址访问服务器。

2) 针对需要上网的网段，需要创建NAPT规则，请参考6.1.1 NAPT进行配置。

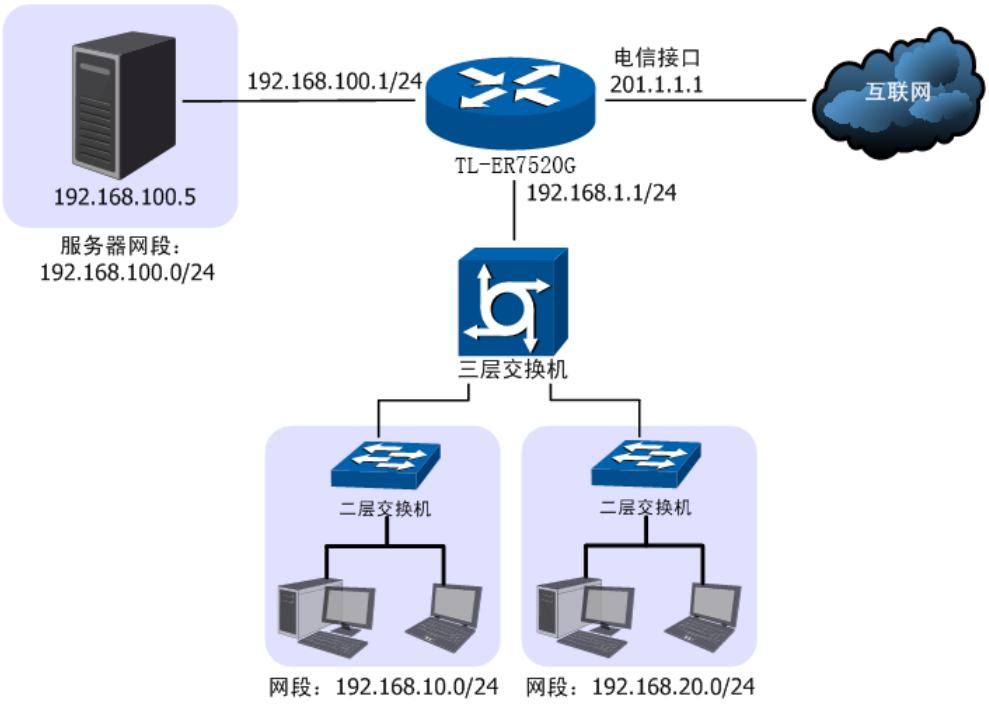


图 6-11　一对一NAT功能组网应用

配置步骤：

TL-ER7520G路由器要完成上述网络需求，需要为服务器配置一对一NAT功能，为其他上网接口配置NAPT功能和路由功能，配置步骤如下：

1) 设置一对一NAT规则。必须操作。创建界面：传输控制 >> NAT设置 >> 一对一NAT。配置192.168.100.5服务器的数据从电信接口转发时，将做一对一NAT映射再转发，映射后地址为201.1.1.2。

2) 设置NAPT规则。必须操作。创建界面：传输控制 >> NAT设置 >> NAPT。配置192.168.10.0/24和192.168.20.0/24两个网段的数据从电信接口转发时做NAPT地址转换。

3) 设置静态路由。必须操作。创建界面：传输控制 >> 路由设置 >> 静态路由。对于网段 192.168.10.0/24 和 192.168.20.0/24，其通过三层交换机连接到路由器的192.168.1.1/24 接口，因此需要在路由器上建立静态路由条目，使网络 192.168.10.0/24 和 192.168.20.0/24 在路由器上路由可达。静态路由条目配置参考 **6.5 路由设置**

6.1.3 虚拟服务器

在路由器上设置了NAPT特性的接口，因防火墙的限制，会拒绝用户向此接口发起的访问请求。当网络中搭建了服务器需要为所有用户开放时，NAPT特性接口下的用户将无法获得服务。通过虚拟服务器功能，在设置了NAPT特性的接口上开放固定的传输层协议端口，当开放端口收到访问请求时，将把访问请求转发到指定的服务器上，此接口中的用户便能成功访问网络中的服务器，同时不影响网络安全。

■ 配置虚拟服务器

进入界面：传输控制 >> NAT设置 >> 虚拟服务器

点击<新增>按钮，进入虚拟服务器设置页面。填写服务器的IP地址和服务端口信息以及路由器开放端口，点击<确定>按钮手动添加条目。

图 6-12 虚拟服务器界面-设置虚拟服务器

规则名称	输入该虚拟服务器的名称，例如可以根据服务器提供的服务特性命名。只能输入英文、数字和下划线。
生效接口	选择规则生效接口，当此处设置的接口收到特定外部端口的访问请求时将把数据发给局域网服务器。
外部端口	输入路由器提供给广域网访问时使用的端口（范围），端口组之间不允许重叠。本例中使用12892端口。
内部端口	输入局域网服务器提供服务的端口，如本例中是80端口。
内部服务器IP	输入服务器的局域网IP地址。
服务协议	选择TCP，UDP协议，或者可以都选（根据内网服务器提供的服务类型而定）。
状态	勾选“启用”，则使该规则条目生效； 不勾选“启用”，则使该规则条目失效。

表 6.3 虚拟服务器界面条目项说明

新增的条目会在**服务列表**中显示出来，如下图所示。

图 6-13 虚拟服务器界面-服务列表

如图所示，虚线框中的条目表示：广域网用户向接口“isp1”的12892端口发送访问请求时，该请求将被转发给局域网中的服务器192.168.100.5的80端口上，并由真实的服务器192.168.100.5提供服务。

如有需要，可以点击条目后的<>按钮进行编辑，点击<>按钮启用条目，点击<>按钮禁用条目。

■ 应用环境

如图 6-14所示，某企业网络存在普通用户子网和服务器子网，同时向电信运营商申请了一条宽带接入线，子网192.168.1.0/24中的用户通过电信接口访问Internet，而web服务器192.168.100.5则需要通过电信接口给广域网中的用户提供web服务，服务端口为80。

分析如下：

1) 普通用户可以通过NAPT功能共享一条宽带接入线上网。

2) 服务器通过宽带接入线向广域网发送数据时，为了避免私有网络信息发送到广域网，因此针对服务器子网也需要设置NAPT。

3) 为服务器配置虚拟服务器功能，向广域网用户开放一个传输层端口，供广域网用户访问服务器。

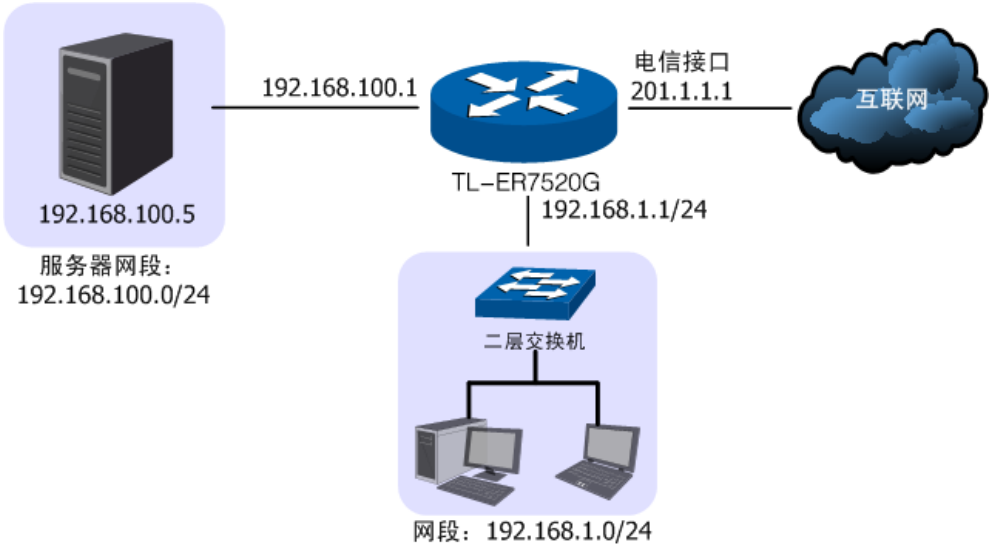


图 6-14 虚拟服务器功能组网应用

配置步骤：

本路由器要完成上述网络需求，需要配置NAPT功能和虚拟服务器功能，配置步骤如下：

1) 设置NAPT规则。必须操作。创建界面：传输控制 >> NAT设置 >> NAPT。配置普通用户子网192.168.1.0/24和服务器子网的数据从“电信接口”上网时做NAPT地址转换。

2) 设置虚拟服务器功能。必须操作。创建界面：传输控制 >> NAT设置 >> 虚拟服务器。在“电信接口”上为服务器开放一个端口，供广域网用户访问服务器，当开放端口收到来自广域网用户的访问请求时，将把访问请求转发到内网服务器的服务端口上。此处假设开放的外部端口为8080，局域网服务器提供的服务端口为80。

3) 访问服务器。可选操作。广域网用户访问网络时，可以通过地址加端口的方式访问服务器。例如本例中的web服务器则可以通过网页浏览器进行访问，地址格式为http://接口地址:开放端口，根据本例中的实际参数则地址为http://201.1.1.1:8080，路由器收到访问请求时将地址转换成http://192.168.100.5:80后转发给服务器。

说明：

- 若服务器对外开放的服务端口是80端口，则需要在设置虚拟服务器前更改路由器的管理端口，更改地址：管理界面 >> 系统工具 >> 管理帐号 >> 系统管理设置 >> Web服务端口，将默认的80端口修改为其他端口。修改后登陆路由器管理界面的方法为：http://管理接口IP地址:新端口。
- 通过申请花生壳动态域名，可以使用域名来访问内部服务器。花生壳动态域名功能设置界面：管理界面 >> 系统服务 >> 动态DNS，详细的配置步骤请参考**动态DNS**章节。
- 如果希望通过广域网监控局域网中的网络摄像头，除了需要配置虚拟服务器功能，还要确保网络摄像头的网关设置正确。
- 如果上述设置完成后仍然无法访问服务器，请查看：http://www.tp-link.com.cn/pages/article-detail.asp?result=faq&d=130

6.1.4 ALG服务

通常情况下，局域网中的计算机共享公网地址上网时，路由器均会对数据包做NAT地址转换。然而，对于一些特殊的协议，例如访问服务器FTP、VPN隧道连接等，此类应用的数据包中的内容可能包含IP地址或端口信息，这些内容不能被NAT进行有效地转换，因此此类应用在通过路由器NAT时就可能会出现问题。

例如，FTP应用是由数据连接和控制连接共同完成的，而且数据连接基于的传输层端口由控制连接过程中的数据包内容动态地决定，这就需要ALG特性来完成数据包内容的转换，来保证后续数据连接的正确建立。

下表为常见的需要ALG的一些应用层协议。

应用名称	应用场景
FTP	用于局域网设备使用FTP协议访问广域网设备时，如访问FTP服务器，此时需要启用FTP ALG。
H.323	局域网中的IP电话与广域网中的IP电话使用H.323协议进行通信时，需要启用H.323 ALG。
PPTP	用于路由器使用PPTP方式进行拨号，或者提供PPTP隧道连接服务时，需要启用PPTP ALG。

SIP	局域网中存在Internet多媒体会议、IP电话等应用是基于SIP协议的，需要启用SIP ALG。

表 6.4　ALG应用列表

配置ALG

进入界面：传输控制 >> NAT设置 >> ALG服务

在界面的**ALG服务**区域，针对特殊应用类型开启ALG服务。

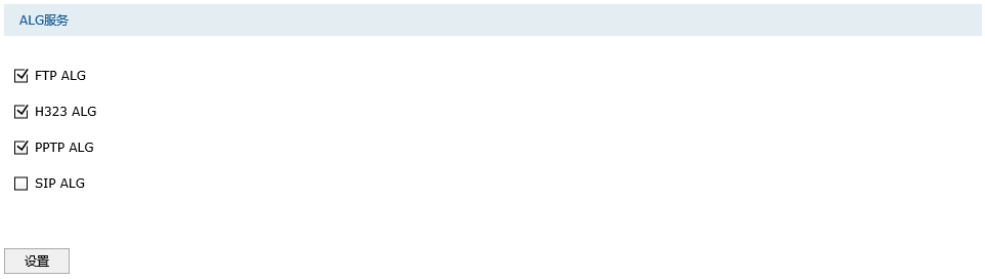


图 6-15　ALG服务界面-设置ALG服务

路由器支持4种特殊应用的ALG服务。默认情况下，3种ALG服务均已经启用，建议保持默认设置不做改变。

6.1.5　NAT-DMZ

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

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

■　配置NAT-DMZ

进入界面：传输控制 >> NAT设置 >> NAT-DMZ

点击<新增>按钮，进入NAT-DMZ规则设置页面。填写DMZ主机的局域网IP地址以及数据包转发接口，点击<确定>按钮手动添加条目。

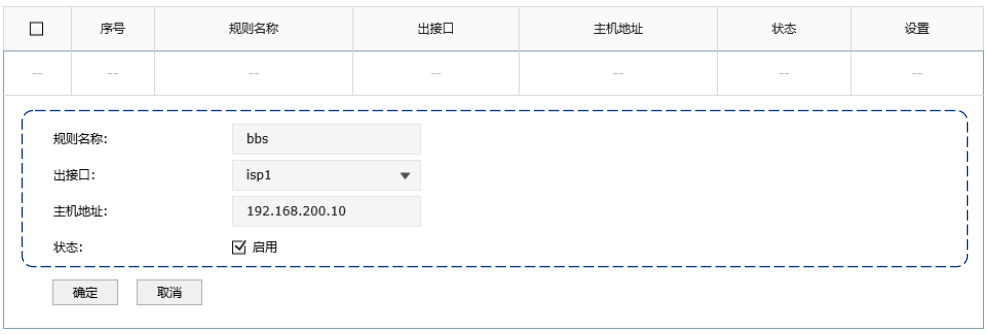


图 6-16　NAT DMZ界面-设置DMZ区

服务名称	输入该NAT转发规则的名称，例如可以根据DMZ主机特性命名。只能输入英文、数字和下划线。
出接口	选择规则生效接口，当此处设置的接口收到的访问请求无法匹配现有的NAT规则时，将把数据发给DMZ主机。
主机地址	输入DMZ主机的局域网IP地址。
状态	勾选“启用”，则使该规则条目生效； 不勾选“启用”，则使该规则条目失效。

表 6.5　NAT-DMZ界面条目项说明

新增的条目会在**服务列表**中显示出来，如下图所示。

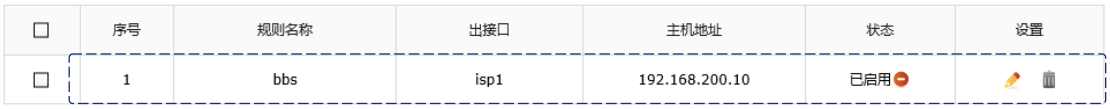


图 6-17　NAT-DMZ界面-服务列表

如图所示，虚线框中的条目表示：接口“isp1”收到访问请求时，如果该请求无法匹配到其他NAT功能设置的NAT规则，将被转发到局域网中IP地址为192.168.200.10的DMZ主机上。

如有需要，可以点击条目后的<>按钮进行编辑，点击<>按钮启用条目，点击<>按钮禁用条目。

6.2　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。

■　配置智能带宽控制

进入界面：传输控制 >> 带宽控制 >> 带宽控制规则

在界面的**功能开关**区域，设置带宽控制功能，点击<设置>按钮保存配置。

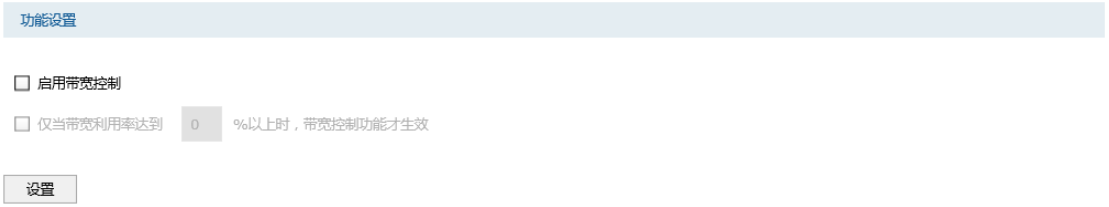


图 6-18　带宽控制规则界面-功能设置

您可以全局开启或关闭带宽控制功能，或设置为仅当带宽利用率达到一定值以上才开启带宽控制功能配置带宽控制规则

进入界面：传输控制 >> 带宽控制 >> 带宽控制规则

点击<新增>按钮，进入带宽控制规则设置页面。设置带宽控制规则的对象，包括生效时间、数据流向、IP地址范围等，点击<确定>按钮手动添加条目。

图 6-19　带宽控制规则界面-设置带宽控制规则

规则名称	输入该规则条目的名称。只能输入英文、数字和下划线。
源接口	选择规则控制的数据源端。
目的接口	选择规则控制的数据目的端。
受控地址组	选择规则控制的地址组，以设置IP地址范围，地址组的设置方法**地址管理**。见此处的受控地址组与下面的受控地址类型共同指定此带宽控制规则的面向对象。例如，设置此规则的生效对象为IP地址范围192.168.10.100-192.168.10.200的计算机发出的数据包。
最大带宽	选择规则定义的数据流的最大上行带宽，取值范围为100-10000000Kbps，默认为1000Kbps。
带宽模式	设置地址组的带宽控制模式：共享表示地址组内IP共用带宽；独立表示地址组内IP独占带宽。
地址类型	选择此带宽控制规则生效对象的源或目的计算机的IP地址。
最大带宽	设置受控计算机所能使用的最大限制带宽。

带宽模式	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；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。
生效时间	选择规则生效时间，其他时间规则不生效。Any为系统默认设置的时间对象，表示所有时间。请在对象管理章节设置时间对象。
备注	添加对当前规则的说明信息。
添加到指定位置	选择将当前规则添加到规则列中的指定位置。若留空，则当前规则将默认添加到已有规则之后。
状态	勾选“启用”，则使该规则条目生效； 不勾选“启用”，则使该规则条目失效。

表 6.6　带宽控制规则界面条目项说明

新增的条目会在**用户规则列表**中显示出来，如下图所示。

	序号	规则名称	源接口	目的接口	受控地址组	地址类型	最大带宽	带宽模式	生效时间	状态	设置
☐	1	rule1	eth0	eth1	g_lan_ip	src	1000	共享	Any	已启用	

图 6-20　带宽控制规则界面-规则列表

如图所示，此带宽控制规则表示：eth0接口中IP地址在g_lan_ip地址组内的计算机发往eth1接口的通信数据将共享1000Kbps的最大带宽，没有时间限制。

如有需要，可以点击条目后的<>按钮进行编辑，点击<>按钮启用条目，点击<>按钮禁用条目。

配置步骤：

配置带宽控制规则时，需要按照下面步骤进行配置：

1) 设置时间对象。必须操作。创建界面：对象管理 >> 时间管理。设置时间对象以便配置带宽控制规则的生效时间。

2) 设置地址组。必须操作。创建界面：对象管理 >> 地址管理>> 地址管理。设置地址组以控制需进行带宽控制的IP地址范围。

3) 设置带宽控制规则。必须操作。创建界面：传输控制 >> 带宽控制 >> 带宽控制。根据受控对象的网络参数设置带宽控制规则。

6.3　连接数限制

作为网络的统一出口，路由器支持的TCP和UDP连接数为固定值，能够满足局域网设备正常的访问需求。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，将可能影

响局域网其他计算机的通信质量。通过设置连接数限制功能，可以限制每台计算机通过路由器建立的连接数。

■ 配置连接数限制全局特性

进入界面：传输控制 >> 连接数限制 >> 连接数限制

在界面的**功能设置**区域，全局启用连接数限制功能，点击<设置>按钮保存配置。

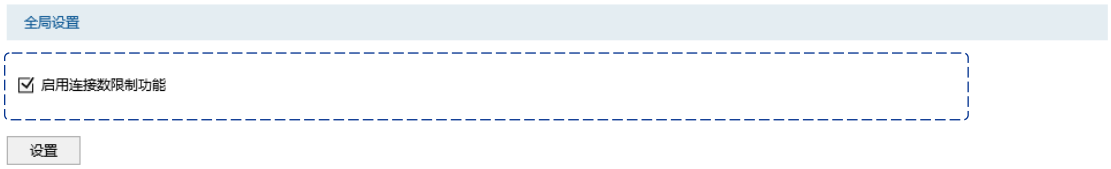


图 6-21 连接数限制界面-功能设置

勾选此项以启用连接数限制功能。不勾选时，所有连接数限制均不生效。

■ 配置连接数限制规则

进入界面：传输控制 >>连接数限制 >> 连接数限制

点击<新增>按钮，进入连接数规则设置页面。选择连接数限制规则生效的IP地址范围以及能够获得的最大连接数，点击<确定>按钮手动添加条目。

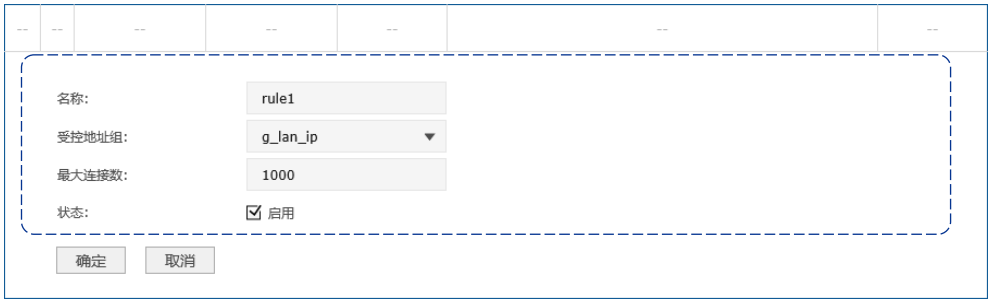


图 6-22 连接数限制界面-设置连接数限制规则

规则名称	输入该规则条目的名称。只能输入英文、数字和下划线。
受控地址组	选择需要进行连接数限制的计算机的IP地址范围，由对象管理中的地址组来表示。IPGROUP_ANY为系统默认设置的地址组，表示所有计算机。地址组的设置请参考**地址管理**。
最大连接数	设置受控地址范围中每台计算机所能使用的最大连接总数。
状态	勾选“启用”，则使该规则条目生效； 不勾选“启用”，则使该规则条目失效。

表 6.7 连接数限制规则界面条目项说明

新增的条目会在**规则列表**中显示出来，如下图所示。

	序号	规则名称	受控地址组	最大连接数	状态	设置
☐	1	rule1	g_lan_ip	1000	已启用	

图 6-23 连接数限制界面-规则列表

如图所示，连接数限制规则“rule1”表示：IP地址范围在“g_lan_ip”用户组中的计算机分别能够通过路由器成功建立TCP或UDP的连接数是1000条。

如有需要，可以点击条目后的<>按钮进行编辑，点击<>按钮启用条目，点击<>按钮禁用条目。

■ 连接数监控

进入界面：传输控制 >>连接数限制 >> 连接数监控

在界面的**监控列表**区域，可查看网络中通过路由器建立的TCP/UDP连接数限制规则生效的地址范围以及能够获得的最大连接数。

序号	地址	IP	最大连接数	当前连接数
1	IP_LAN	10.1.1.2	100	2

图 6-24 连接数监控界面-监控现有连接数

图中的监控条目1表示：IP_LAN地址组的计算机分别能够使用的最大连接数TCP/UDP为100条，其中IP地址为10.1.1.2的计算机当前已通过路由器建立了两条连接数。

配置步骤：

配置连接数限制规则时，需要按照下面步骤进行配置：

1) 设置受控地址组。必须操作。创建界面：对象管理 >> 地址管理>>地址管理。对于连接数限制功能的受控地址范围，需要先在对象管理中进行设置，在设置连接数限制时将直接选择。

2) 启用连接数限制功能并设置规则。必须操作。创建界面：传输控制 >> 连接数限制 >> 连接数限制。根据受控对象的需要设置不同的最大连接数。

6.4 流量均衡

本路由器提供多种负载均衡策略，包括特殊应用程序选路，智能均衡，ISP选路，线路备份，同时支持在线检测功能。本章节将详细介绍流量均衡的功能实现和配置方法。

6.4.1 基本设置

■ 启用流量均衡

进入界面：传输控制 >> 流量均衡 >> 基本设置

在界面的**全局设置**区域，选择是否启用流量均衡，点击<设置>按钮保存配置。

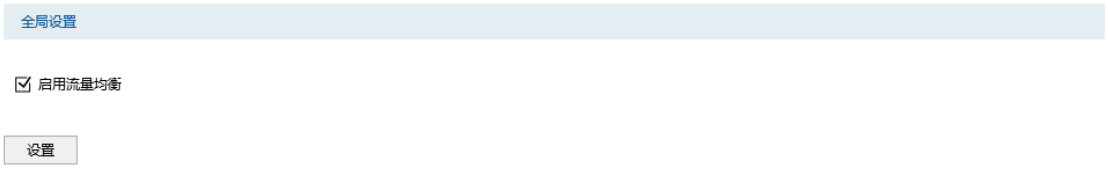


图 6-25 带宽控制规则界面-功能设置

勾选此项，则全局开启流量均衡功能。若不勾选，则所有流量均衡功能关闭。

■ 特殊应用程序选路

启用此功能后，路由器会将数据包的源IP地址与目的IP地址，或者源IP地址与特殊目的端口作为一个整体，记录其通过的接口信息。后续一定时间内如果有同一源IP地址和目的IP/端口地址的数据包通过，则优先转发至上次记录的接口。该功能主要用于保证多连接应用程序的正常工作。

进入界面：传输控制 >>流量均衡 >> 基本设置

在界面的**功能设置**区域，可以选择启用特殊应用程序选路功能，设置完成后需点击<设置>按钮使配置生效。

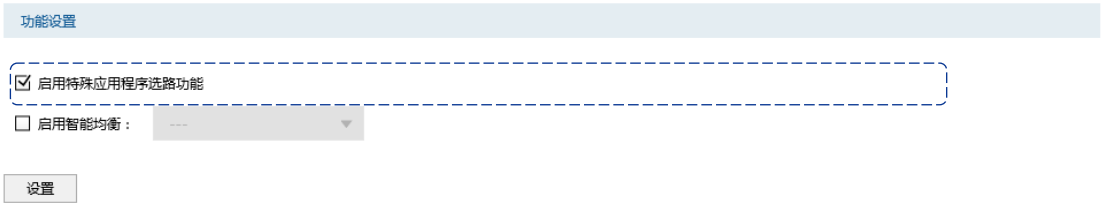


图 6-26 基本设置-特殊应用程序选路功能界面

设置完成后，路由器就会为一些多连接应用程序的数据包选择最优线路。

■ 智能均衡

进入界面：传输控制 >> 流量均衡 >> 基本设置

在界面的功能设置区域，可以选择启用智能均衡，并勾选要参与智能均衡的接口，设置完成后需点击<设置>按钮使配置生效。

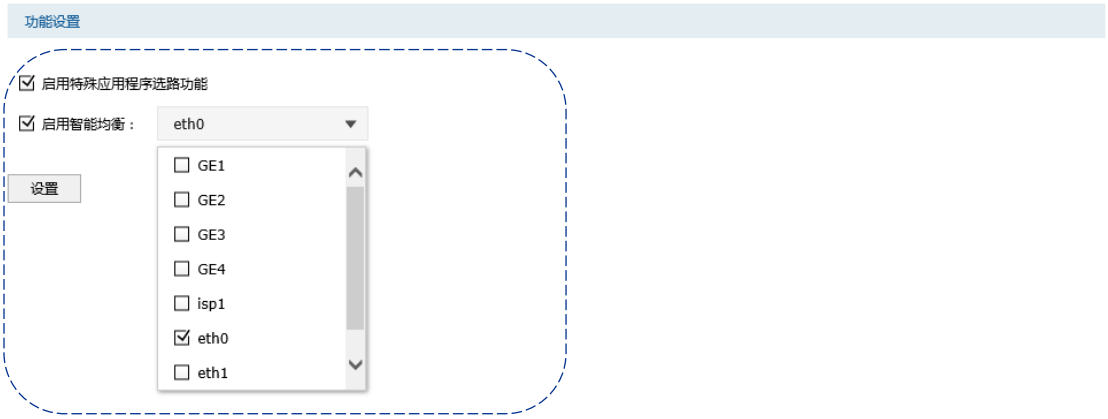


图 6-27　智能均衡设置界面

说明：

在实际应用中，如果某些接口没有连接到因特网，那么这些接口将不会参与到智能均衡，请勿勾选。

设置完成后，在路由器没有设置其它选路规则的情况下，路由器将自动进行流量均衡。

6.4.2　ISP选路

在ISP选路中，通过选择接口和ISP，可以将数据包转发至对应的ISP线路上，从而减少数据包在网络中被转发的次数，提高网络性能。

■　ISP选路设置

进入界面：传输控制 >> 流量均衡 >> ISP选路

启用ISP选路功能

在界面的**选路功能设置**区域，勾选“启用ISP地址段选路功能”，并手动点击<设置>按钮使设置生效。

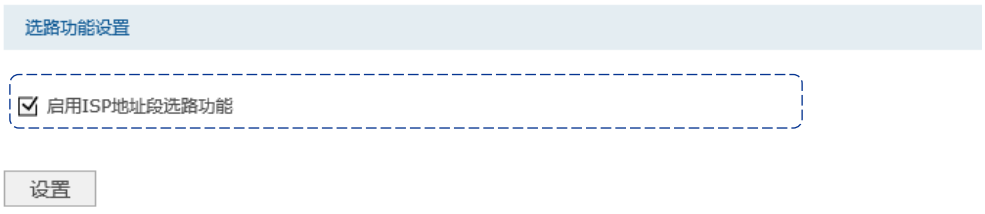


图 6-28　ISP选路界面-启用ISP选路功能

导入ISP数据库

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

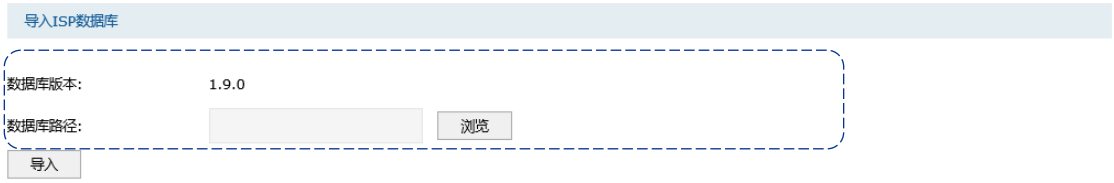


图 6-29 ISP选路界面-导入ISP数据库

用户自定义数据库

用户也可导入自定义的数据库，单击<浏览>按钮，选择保存路径下的文件，点击<导入>即可。

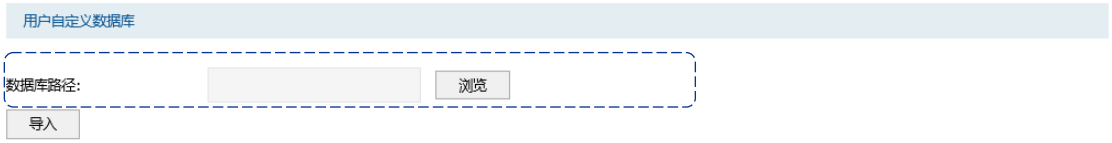


图 6-30 ISP选路界面-导入ISP数据库

ISP选路设置

在界面的ISP选路设置区域选择接口和ISP，点击<确定>手动添加ISP选路条目。

图 6-31 ISP选路界面-ISP选路设置

接口	选择进行ISP选路的接口。
ISP	在下拉列表中选择ISP。

表 6.8 ISP选路功能设置界面项说明

新增的条目会在选路列表里显示出来，如下图所示。

图 6-32 ISP选路界面-选路列表

如有需要，可以点击条目后的<>按钮进行编辑。

说明：

智能均衡、策略路由、ISP选路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：策略路由 > ISP选路 > 智能均衡。

■ ISP选路典型应用

某网吧使用电信和联通双线接入，带宽分别为10M，现需要使用TL-ER7520G来实现网络中所有去往电信服务器的流量走电信线路，所有去往联通服务器的流量走联通线路。

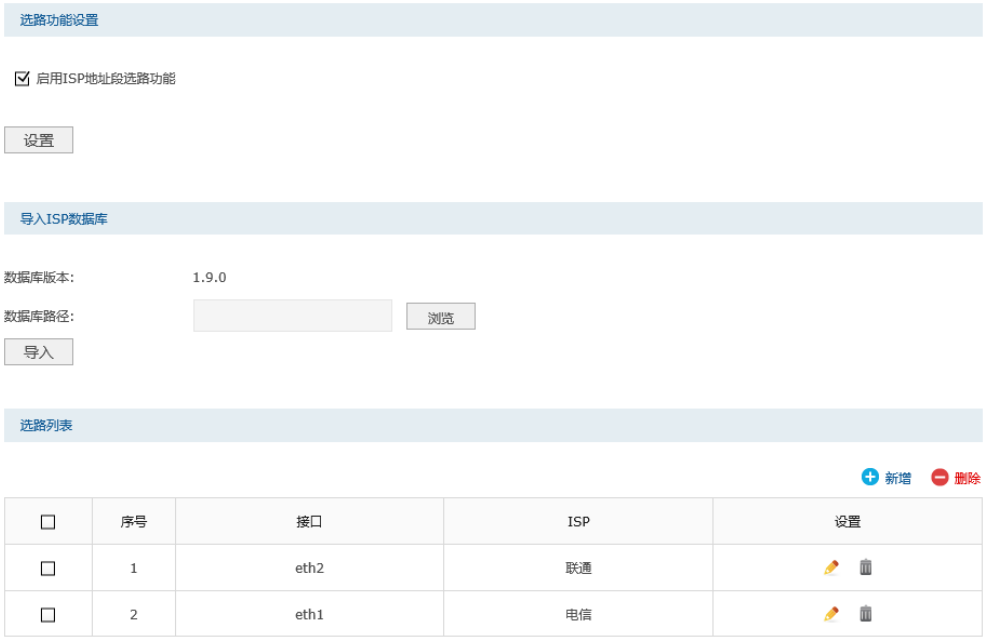
配置步骤

如果要完成上述网络需求，需要按如下顺序配置TL-ER7520G路由器：

1) 创建Ethernet接口eth1和eth2，并连接到ISP网络。注意设置网络参数时必须勾选**参与流量均衡**选项。

2) 在传输控制 >> 流量均衡 >> 基本设置界面，启用特殊应用程序选路功能和智能均衡。

3) 在传输控制 >> 流量均衡 >> ISP选路界面，启用ISP选路功能。TL-ER7520G内嵌了ISP数据库，启用ISP选路功能后，并添加下图所示的条目后，访问电信站点的流量由电信线路转发，访问网通站点的流量由网通线路转发，可以提高访问速度。



6.4.3 线路备份

根据实际需要合理设置线路备份，可以减轻接口流量负担，提高网络效率。当一个接口出现故障时，路由器能够及时地把数据切换到其它正常的接口上，为网络稳定性提供强大保证。

■ 设置线路备份

进入界面：传输控制 >> 流量均衡 >>线路备份

点击<新增>按钮，进入备份规则设置页面。设置主备接口并选择备份模式，点击<确定>按钮手动添加条目。

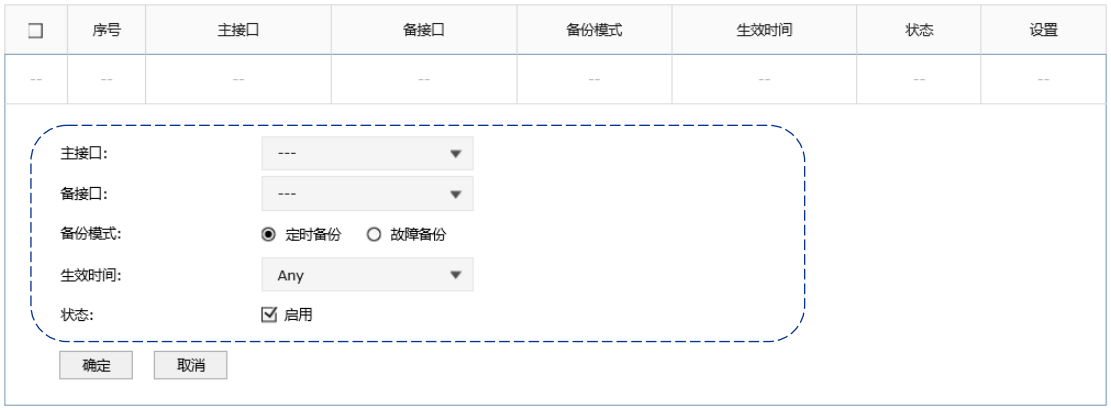


图 6-33 线路备份界面-备份设置

主接口	选择一个接口作为主接口。接口设置请参考**3.2.1 接口设置。**
备接口	选择一个接口作为备接口用来备份主接口的流量。接口设置请参考**3.2.1 接口设置。**
备份模式	可以选择定时备份或故障备份。选择定时备份时，下方可进行备份生效时间设置；选择故障备份时，主接口发生故障时启动备份接口。
生效时间	当备份模式为定时备份时，需要在此指定生效时间。在生效时间内启动备份接口，关闭主接口。时间设置请参考**5.2 时间管理。**
故障备份	当备份模式为故障备份时，在主接口正常工作时备份接口不工作，主接口发生故障时启动备份接口。
状态	勾选“启用”，则使该规则条目生效； 不勾选“启用”，则使该规则条目失效。

表 6.9 线路备份功能设置界面项说明

新增的条目会在**线路备份规则列表**里显示出来，如下图所示。

图 6-34 线路备份界面-主备组列表

如有需要，可以点击条目后的<>按钮进行编辑，点击<>按钮启用条目，点击<>按钮禁用条目。

说明：

要使线路备份生效，首先需要在保证相应接口的在线检测已开启。具体可以在**传输控制 >> 流量均衡 >> 在线检测**界面进行设置。

■ 线路备份举例

某网吧使用双线接入，线路1为包年的电信静态IP接入，10M带宽。线路2为联通的PPPoE拨号上网，2M带宽，按上网时间收费。现在需要将线路2设为备份线路，既保证线路1出现故障时用户不会掉线，又保证了较低的成本。

配置步骤

如果要完成上述网络需求，需要按如下顺序配置TL-ER7520G路由器：

1) 创建Ethernet接口eth1和eth2，并分别连接到线路1和线路2。注意设置接口网络参数时必须勾选**参与流量均衡**选项。

2) 开启在线检测。必须操作。在界面**传输控制 >> 流量均衡 >>在线检测**，开启对eth1接口和eth2接口的在线检测。

3) 在**传输控制 >> 流量均衡 >> 线路备份**界面添加下图所示条目后，当eth1接口发生故障时，路由器将自动切换到eth2接口。

6.4.4 在线检测

进入界面：传输控制 >> 流量均衡 >> 在线检测

该页面用于检测接口是否在线。在线检测列表如下图所示。

在线检测列表

序号	接口名	接口状态	设置
1	GE1	不在线	
2	GE2	不在线	
3	GE3	不在线	
4	GE4	不在线	
5	eth3	不在线	
6	eth2	不在线	

图 6-35 在线检测界面-接口状态列表

如有需要，可以点击条目后的<>按钮进行编辑。

图 6-36　在线检测界面

接口名	选择需要在线检测的接口。
检测模式	选择自动在线检测、手动在线检测或永远在线,默认为自动在线检测模式。自动模式下，PING检测选择网关作为目的地址，DNS检测选择接口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；永远在线模式下，该接口会被强制设置为永远在线，无需检测。
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。

表 6-10　在线检测界面项说明

6.5　路由设置

路由是指路由器根据数据包的目的IP地址选择最优路径，并转发到通往目标网络的下一个网络节点的过程。

在一次路由过程中选择最优路径是路由器需要完成的最重要的工作。路由器通过维护一张路由表来记录网络中的路径信息，并根据一定的路由选择协议在路由表中选择一条最优路径进行数据转发。路由表中的每一个路由条目基本都包含如下四种基本属性，路由转发时将根据数据包的目的IP地址查找最优路径：

1)　目的网络地址：用于标识该条路由条目所指向的目标网络。

2)　子网掩码：用于标识目标网络的子网掩码。

3)　下一跳地址：用于指定通往目标网络的下一跳路由节点，路由器将数据转发给下一跳路由节点后，由下一跳路由节点将数据发往再下一跳路由节点或目标网络。下一跳路由必须是本地可达的，配置路由条目时可以通过ping工具测试是否可达。

4)　下一跳接口：用于标识数据从本地发出的出接口。

路由器根据路由表进行数据转发，而路由条目的来源有三种，分别为直连路由、静态路由和动态路由，以下是三种路由的特点。

- 直连路由：通过数据链路层协议发现的，通常指向与路由器直接连接的网络，如VLAN。
- 静态路由：由网络管理员手动配置的一种特殊路由，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。
- 动态路由：通过相互连接的路由器之间交换彼此的路由信息，然后通过路由选择协议计算出自身的路由表信息，可随着网络拓扑的改变而自动变化，简化了网络管理工作。常用的动态路由选择协议有RIP、OSPF和BGP等等，不同的协议有不同的算法，对于发往同一目标网络的路径选择结果也可能不一样。

本路由器主要支持直连路由和静态路由两种路由特性。直连路由无需配置，路由器可以自动建立直连网络的路由条目。

6.5.1 策略路由

通过对服务类型、源地址、目的地址、生效接口和生效时间的设置，可以更加精确的控制路由器进行选路。

■ 策略路由设置

进入界面：传输控制 >> 路由设置 >> 策略路由

点击<新增>按钮，进入策略路由规则设置页面。填入策略名称，并选择服务类型、源地址、目的地址、生效接口和生效时间，选择启用规则并点击<确定>按钮手动添加条目。

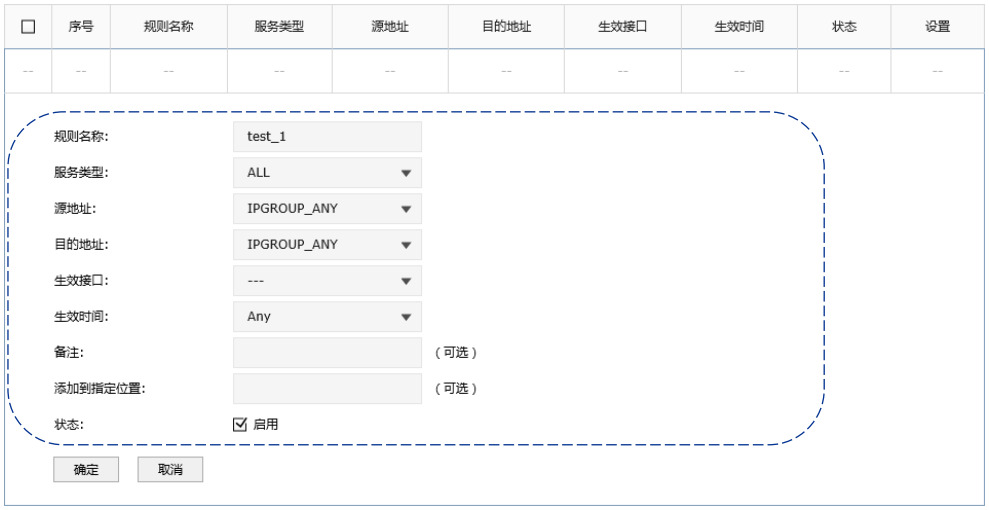


图 6-37 策略路由设置界面

策略名称	用户自定义，标识一条选路规则。只能输入英文、数字和下划线。

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协议将不会应用选路规则。如果列表中没有您想指定的协议类型，可以在**对象管理 >> 服务类型**界面设置，详细配置过程请参考**5.4 服务类型**小节。
源地址	在下拉列表中选择需要应用选路规则的源地址范围。源地址可以在**对象管理 >> 地址管理 >> 地址**界面设置。详细配置过程请参考**5.1 地址管理**小节。
目的地址	在下拉列表中选择需要应用选路规则的目的地址范围。源地址可以在**对象管理 >> 地址管理 >> 地址**界面设置。详细配置过程请参考**5.1 地址管理**小节。
生效接口	选择指定数据包转发接口。
生效时间	选择规则生效的时间。生效时间可以在**对象管理 >> 时间管理界**面进行设置。详细配置过程请参考**5.2 时间管理小节**。
备注	添加对本条规则的说明信息。
添加到指定位置	输入本条规则在规则列表中的序号以设定该规则的优先级，序号越小表示优先级越高。若留空则系统将按照规则设定的先后顺序对规则进行依次排序。
状态	勾选“启用”，则使该规则条目生效； 不勾选“启用”，则使该规则条目失效。

表 6.10 策略路由功能设置界面项说明

新增的条目会在**规则列表**里显示出来，如下图所示。

☐	序号	规则名称	服务类型	源地址	目的地址	生效接口	生效时间	状态	设置
☐	1	test_1	ALL	IPGROUP_ANY	IPGROUP_ANY	eth1	Any	已启用	

图 6-38 策略路由设置界面-规则列表

如有需要，可以点击条目后的<>按钮进行编辑，点击<>按钮启用条目，点击<>按钮禁用条目。

■ 策略路由典型应用

某企业的网络需求如下：

TL-ER7520G为中心路由器，使FTP数据包和HTTP数据包通过不同的接口转发。

配置步骤

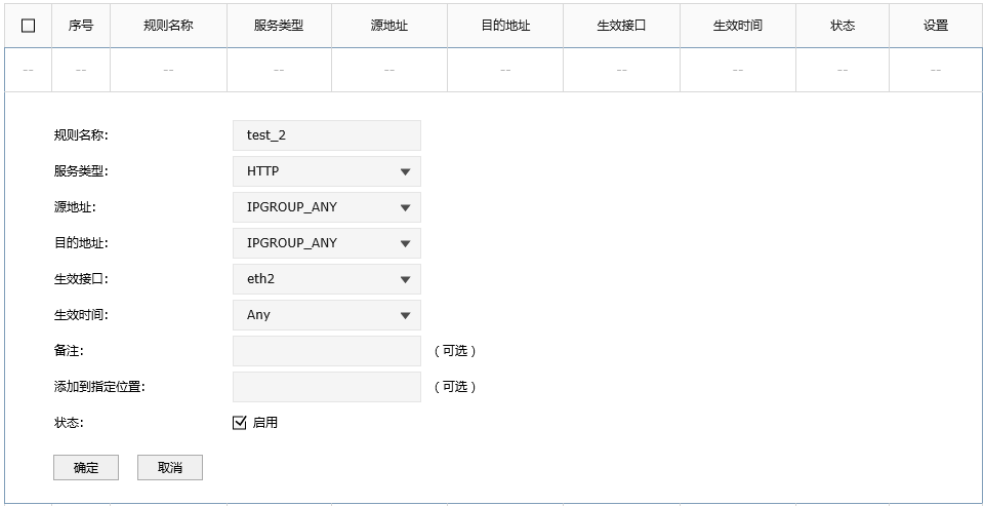
如果要完成上述网络需求，需要按如下顺序配置TL-ER7520G路由器：

1) 创建Ethernet接口eth1和eth2。注意设置网络参数时必须勾选**参与流量均衡**选项。

2) 在传输控制 >> 路由设置 >> 策略路由界面创建如下两条规则：

3) 指定FTP数据包由“eth1”接口转发。

指定 HTTP 数据包由“eth2”接口转发。



6.5.2 静态路由

静态路由是由网络管理员手动设置的路由，一般在规模不大、拓扑结构固定的网络中配置，网络管理员只需配置少量静态路由即可实现网络互通。在网络中使用合适的静态路由可以减少路由选择问题，提高数据包的转发速度。当网络发生改变时则需要网络管理员手动修改路由配置以保证网络正常通信。

■ 配置静态路由

进入界面：传输控制 >> 路由设置 >> 静态路由

点击<新增>按钮，进入静态路由设置页面。输入静态路由各项参数，点击<确定>按钮手动添加条目。

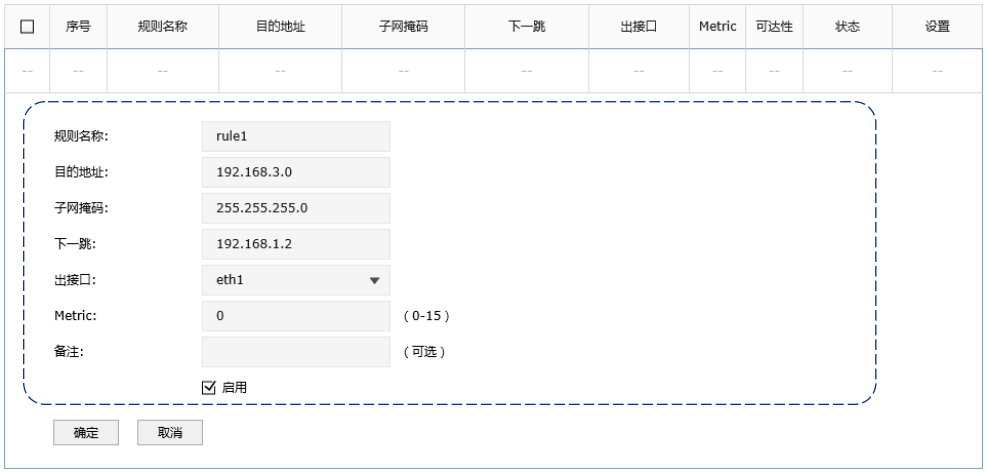


图 6-39 静态路由界面-设置静态路由

规则名称	输入该规则条目的名称。只能输入英文、数字和下划线。
目的地址	设置静态路由规则条目指向的目标网络地址。
子网掩码	设置静态路由规则条目指向的目标网络的子网掩码。
下一跳	设置通往目标网络的路由路径上下一个节点的IP地址。
出接口	设置数据从本地发出的出接口.
Metric	设置路由规则的优先级，数值越低则优先级越高，0为最高优先级。当网络中存在多条路由可以到达同一目的地址，可以通过调整Metric来调整路由规则的优先级，数据包将按照Metric值最小的路径转发。
备注	添加对本条规则的说明信息。
启用/禁用规则	勾选“启用”，则使该规则条目生效； 未勾选“启用”，则该规则条目失效。

表 6.11 静态路由界面条目项说明

新增的静态路由条目会在**规则列表**中显示出来，如下图所示。

图 6-40 静态路由界面-规则列表

如图所示，静态路由规则“rule1”表示：发往目标网络192.168.3.0/24的数据可以通过接口eth0发往192.168.1.2节点上，节点192.168.1.2将执行下一个转发任务，此静态路由规则的Metric值为0拥有最高优先级。可达性为“可达”，说明该静态路由真实生效。

如有需要，可以点击条目后的<>按钮进行编辑，点击<>按钮启用条目，点击<>按钮禁用条目。

■ 应用环境

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

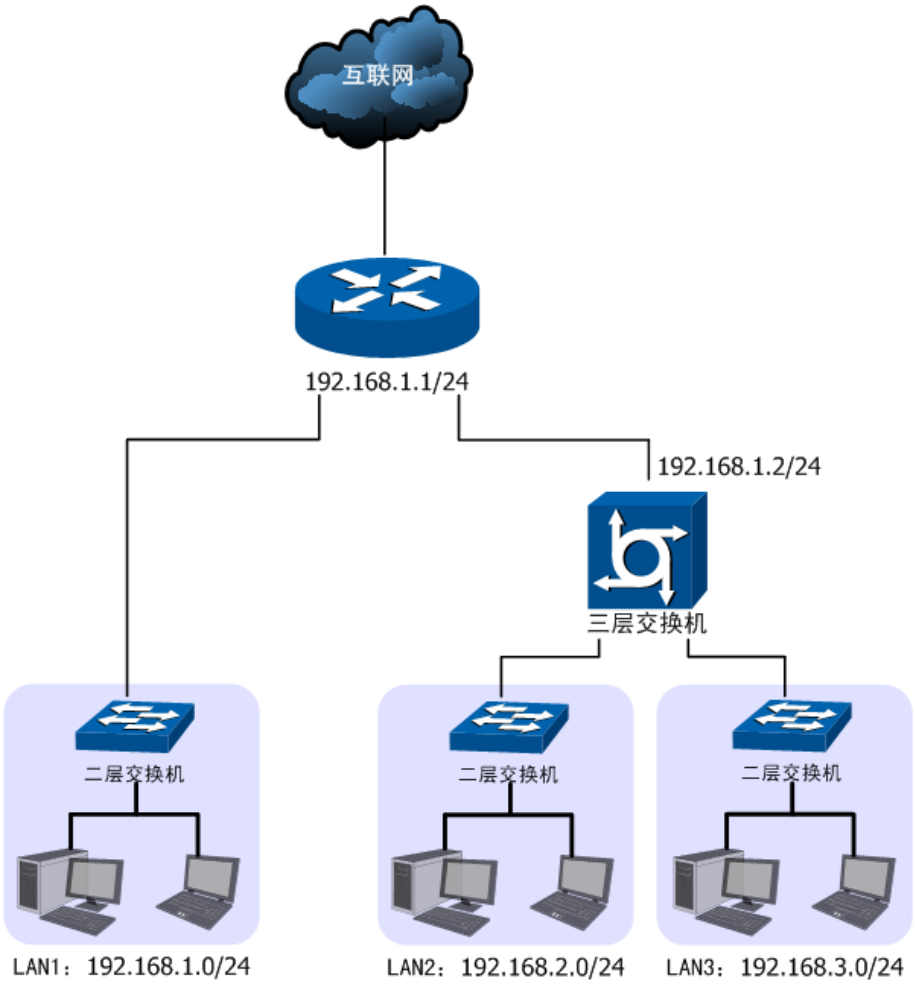


图 6-41 静态路由功能组网应用

配置步骤：

TL-ER7520G路由器要完成上述网络需求，需要配置静态路由功能，配置步骤如下：

1) 创建转发数据包的接口eth0。创建界面：基本设置 >> 接口设置 >> 接口设置。eth0具体设置请根据实际需求进行。

2) 创建静态路由规则，设置到LAN2网段的下一跳地址为三层交换机的级联口IP地址192.168.1.2。创建界面：传输控制 >> 路由设置 >> 静态路由。规则设置如下，点击<确定>按钮完成。

名称	rule1
目的地址	192.168.2.0
子网掩码	255.255.255.0

下一跳	192.168.1.2
出接口	eth0
Metric	0
备注	LAN2
启用/禁用规则	选择“启用”

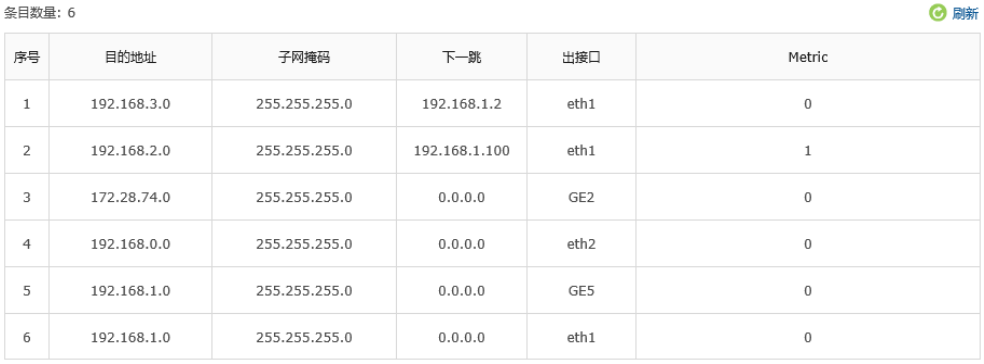
3) 创建静态路由规则，设置到LAN3网段的下一跳地址为三层交换机的级联口IP地址192.168.1.2。创建界面：传输控制 >> 路由设置 >> 静态路由。规则设置如下，点击<确定>按钮完成。

名称	rule2
目的地址	192.168.3.0
子网掩码	255.255.255.0
下一跳	192.168.1.2
出接口	eth0
Metric	0
备注	LAN3
启用/禁用规则	选择“启用”

6.5.3 系统路由

进入界面：传输控制 >> 路由设置 >> 系统路由

系统路由下显示了路由器建立的所有路由规则条目，如下图所示。



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

第7章 安全管理

7.1 ARP防护

7.1.1 ARP简介

ARP（Address Resolution Protocol，地址解析协议），是一种将主机的IPv4地址解析成MAC地址的网络协议。

在同一个局域网中，一台主机要与其他主机直接通信，必须确定目的主机的MAC地址。在已知目的主机IP地址的情况下，通过ARP协议可以获取目的主机的MAC地址信息。

■ ARP报文格式

ARP报文的格式如下图所示：

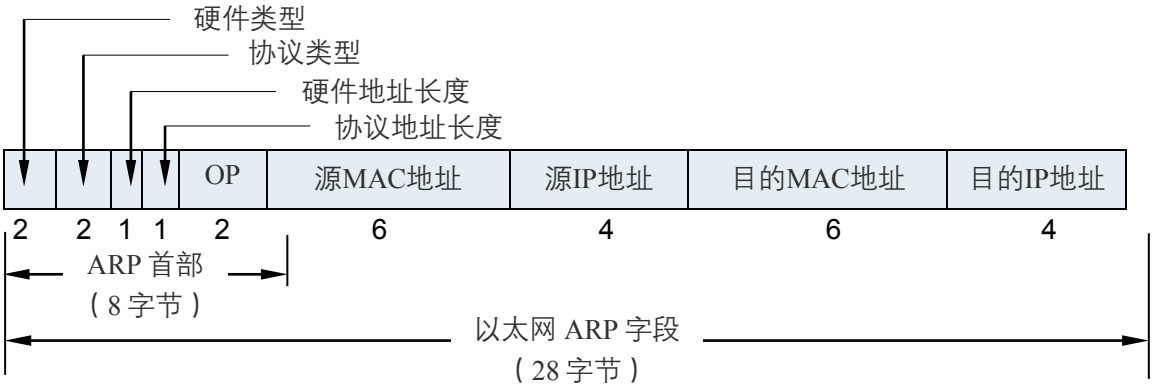


图 7-1 ARP报文格式

硬件类型	应用ARP的网络类型，对于以太网该值为1。
协议类型	要映射的协议类型，对于IP协议该值为0x0800（0x表示十六进制）。
硬件地址长度	硬件地址即MAC地址，共48位，长度为6个字节，该值为6。
协议地址长度	协议地址即IP地址，共32位，长度为4个字节，该值为4。
OP	OP为操作码，1表示ARP请求；2表示ARP应答。
源MAC地址	发送报文一方的MAC地址。
源IP地址	发送报文一方的IP地址。
目的MAC地址	接收报文一方的MAC地址（ARP请求报文中该字段全0）。

目的IP地址	接收报文一方的IP地址。

表 7.1　ARP报文字段含义

■ ARP解析过程

在一次ARP通信中，源主机会首先向自己所在网段广播一个ARP请求报文，网段中的所有主机都会收到这个请求报文，但只有符合请求报文中目的IP地址的主机会做出回应，回应的ARP应答报文将会携带该主机的MAC地址信息，以单播形式发送给源主机。如下图所示：

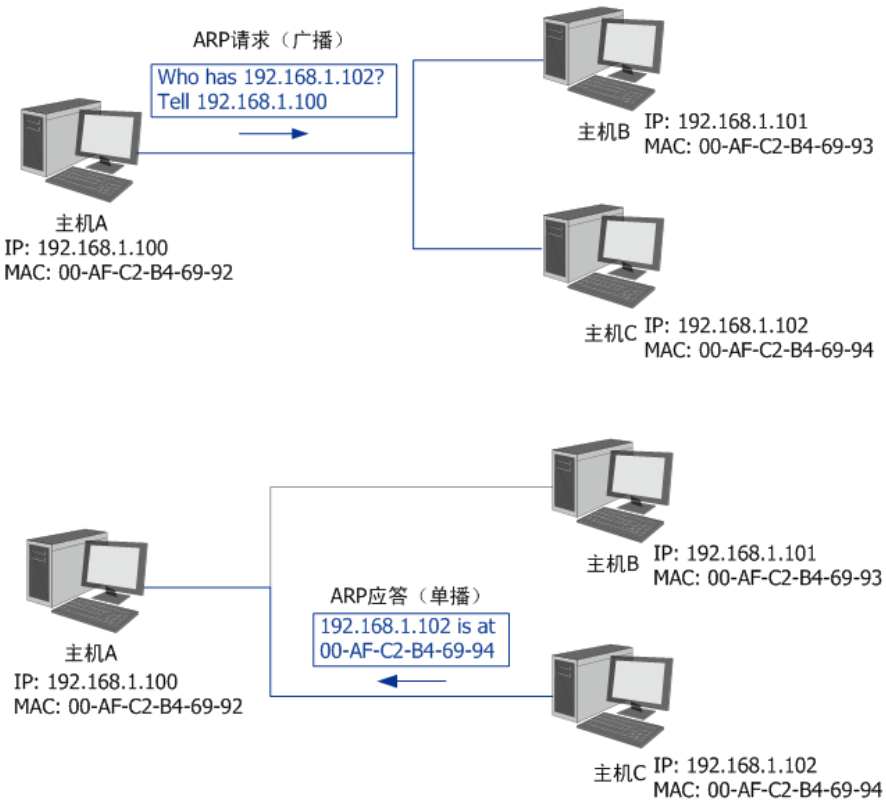


图 7-2　ARP解析过程

网络中的所有主机，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。主机通过数据包的交互学习到其他主机的IP地址和MAC地址信息，并将这些信息添加至自身的ARP表中。每次通信时会先根据IP地址在表中查找对应MAC地址，减少网络上的ARP通信量。

7.1.2 ARP攻击简介

按照ARP协议的设计，主机在接收ARP应答报文时只会机械地使用最新ARP信息替换自身ARP列表，这就为“ARP攻击”创造了条件。

ARP攻击的主要形式为ARP欺骗，通常由局域网中的攻击主机发送ARP欺骗包，将伪造的IP与MAC对应关系替换主机ARP列表中的记录，共有三种欺骗方式：欺骗主机、欺骗网关、双向欺骗。

- 欺骗主机：仿冒网关给主机发送错误的ARP报文，通常欺骗报文中会伪造发送者MAC地址。

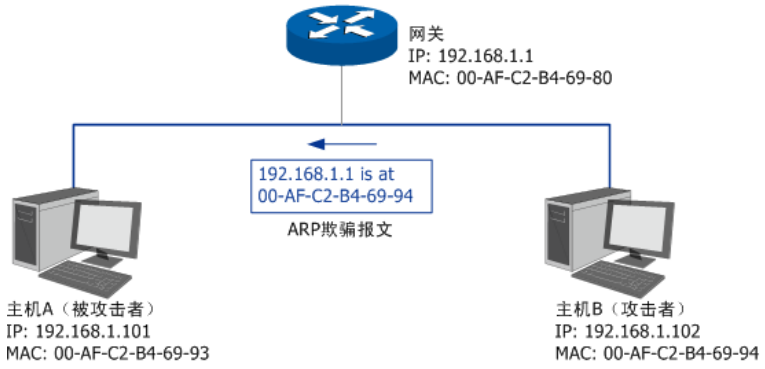


图 7-3　ARP欺骗-欺骗主机

- 欺骗网关：仿冒主机向网关发送错误的ARP报文，通常欺骗报文中会伪造发送者IP或MAC地址。

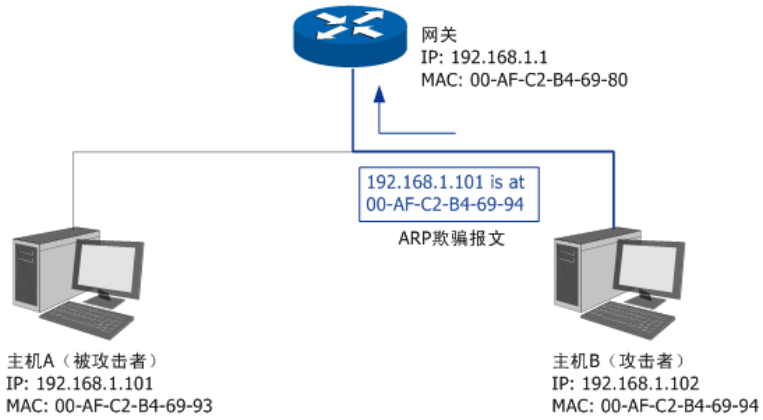


图 7-4　ARP欺骗-欺骗网关

- 双向欺骗：前面两种欺骗方式的结合，伪造不同的ARP报文，同时发送给主机和网关。

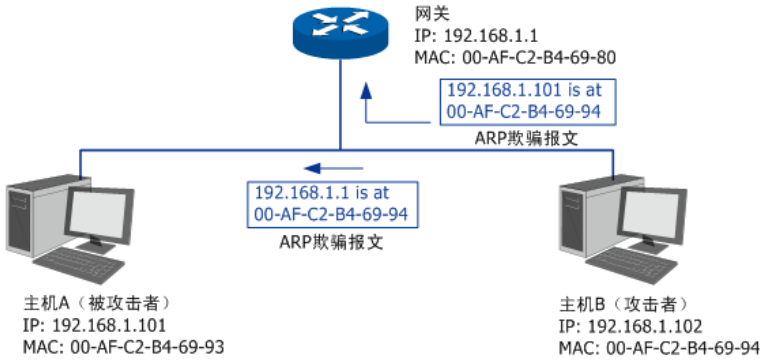


图 7-5　ARP欺骗-双向欺骗

ARP欺骗可能会造成局域网内部分主机无法访问网络，还可能造成通信数据被非法窃听或篡改，严重影响了局域网内部通信及安全，由此便产生了ARP防护技术。ARP防护的根源在于杜绝伪造的ARP报文刷新ARP列表。绑定正确的IP MAC地址信息可以有效防止ARP欺骗。

7.1.3 ARP攻击防护

■ 开启ARP防护相关功能

进入界面：安全策略 >> ARP防护 >> IP MAC绑定

在界面的**功能设置**区域，可以开启路由器ARP防护相关功能，设置完成后需点击<设置>按钮使配置生效。

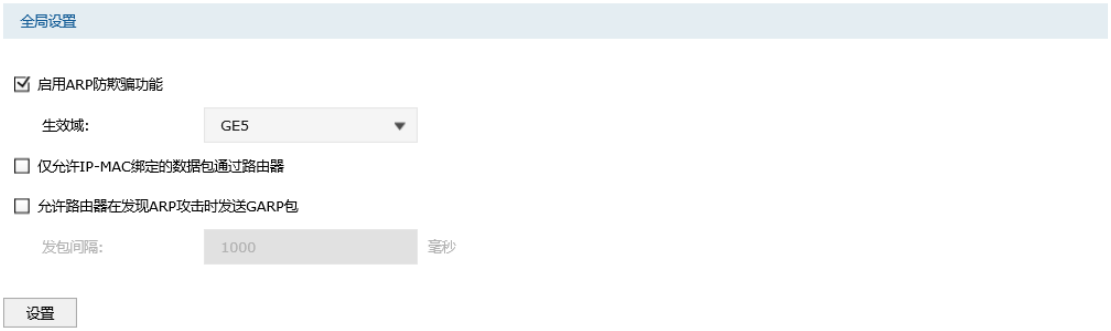


图 7-6 IP MAC绑定界面-功能设置

启用ARP防欺骗功能	全局功能开关。在开启此项之后，所有的ARP防护设置才会生效。开启该功能后，选择生效接口域。
仅允许IP MAC绑定的数据包通过路由器	强制局域网内主机进行IP MAC绑定，没有绑定的主机将无法访问网络。推荐在需要防止非法客户端接入时勾选，勾选条目前请确认已绑定包含管理主机在内的指定主机的IP MAC地址信息。 注意：要开启该功能，需要先开启ARP防欺骗功能
允许路由器在发现ARP攻击时发送GARP包	当路由器发现局域网内主机存在ARP冲突时，路由器会将自身正确的IP MAC地址信息以GARP（Gratuitous ARP，免费ARP）包的方式主动发送给被攻击的主机，替换该主机错误的ARP列表信息。可在发包间隔处指定发包速率。推荐勾选。 注意：要开启该功能，需要先开启ARP防欺骗功能

表 7.2 ARP功能设置界面项说明

为了更好地防御ARP攻击，还可以分别在局域网各主机上绑定路由器接口的IP和MAC地址，具体地址信息可以在**基本设置 >> 系统状态**页面中查看。

■ 导入到静态DHCP列表

在 IP-MAC 绑定规则列表中选择条目，并在**导入到静态 DHCP 列表**区域点击<导入>，可将条目导入到静态 DHCP 列表中。

■ 绑定局域网内主机的IP与MAC地址信息

路由器提供多种绑定方法，包括手动单条绑定指定主机的IP MAC地址信息、批量绑定局域网内活动主机的IP MAC地址信息，以及批量绑定正与路由器通信的主机IP MAC地址信息。

说明：

- 使用批量绑定时请不要勾选**IP MAC绑定**页面上的“仅允许IP MAC绑定数据包通过路由器”选项。
- 若局域网内已经存在ARP攻击导致部分主机通信异常，则不可批量绑定，请在**IP MAC绑定**界面进行手动绑定。

手动单条绑定指定主机的IP MAC地址信息

进入界面：安全策略 >> ARP防护 >> IP MAC绑定

在界面的**IP MAC绑定表**区域，点击<新增>，填入需进行绑定的局域网主机IP、MAC地址信息，点击<确定>。

图 7-7 IP MAC绑定界面-IP MAC绑定

IP地址	输入一个IPv4地址。
MAC地址	输入与上方IP地址正确对应的主机MAC地址。

出接口	选择绑定的接口。
备注	添加对本条目的说明信息，非必填项。
是否启用	选择“启用”，则使该绑定条目生效； 选择“禁用”，则使该绑定条目失效。

表 7.3 IP MAC绑定界面条目项说明

新增的条目会在**绑定列表**中显示出来。此时，以图 7.7中的配置为例，MAC地址为40-61-86-FC-75-C4的主机如果擅自修改了IP地址，便会无法访问网络；反之亦然。

图 7-8 IP MAC绑定界面-绑定列表

批量绑定局域网内活动主机的IP MAC地址信息

进入界面：安全策略 >> ARP防护 >> ARP扫描

首先，通过**ARP扫描**界面得到局域网内活动主机的IP MAC对应信息。或者点击<导入>，将IP-MAC绑定条目导入。

图 7-9 ARP扫描界面

在扫描范围中填入起始及结束的IP地址，点击<开始扫描>按钮，路由器会将该范围内所有正在工作主机的IP MAC地址信息显示在**扫描结果**中。

如需将扫描结果进行绑定，请选择条目，然后点击**导入到IP-MAC绑定**区域的<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，这些批量绑定的条目会出现在**IP MAC绑定**界面的IP-MAC**绑定规则列表**中。

批量绑定正与路由器通信的主机IP MAC地址信息

进入界面：安全策略 >> ARP防护 >> ARP列表

首先，进入**ARP列表**界面得到正在与路由器进行通信的主机的IP MAC对应信息。

	序号	IP地址	MAC地址	接口	状态
☐	1	172.28.74.68	74-D4-35-9F-D8-A9	GE4	
☐	2	172.28.74.68	74-D4-35-9F-D8-A9	GE5	
☐	3	192.168.1.68	74-D4-35-9F-D8-A9	GE5	
☐	4	172.28.74.64	74-D4-35-9F-D8-A9	GE4	
☐	5	192.168.1.64	74-D4-35-9F-D8-A9	GE5	

图 7-10 ARP列表界面

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或物理连接中断而自动从列表中删除。

如需将列表中的条目绑定，请选择条目，然后点击**导入到IP-MAC绑定**区域的<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，列表中的条目状态也会随之变更。

若路由器此时已连入外网，也可以通过ARP列表获取网关的IP MAC地址信息，并进行绑定，以抵御来自外网的ARP攻击。

7.2 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。

进入界面：安全管理 >> 攻击防护

图 7-11 攻击防护设置界面

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

表 7.4 攻击防护界面条目项说明

7.3 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。

进入界面：安全策略 >> MAC过滤

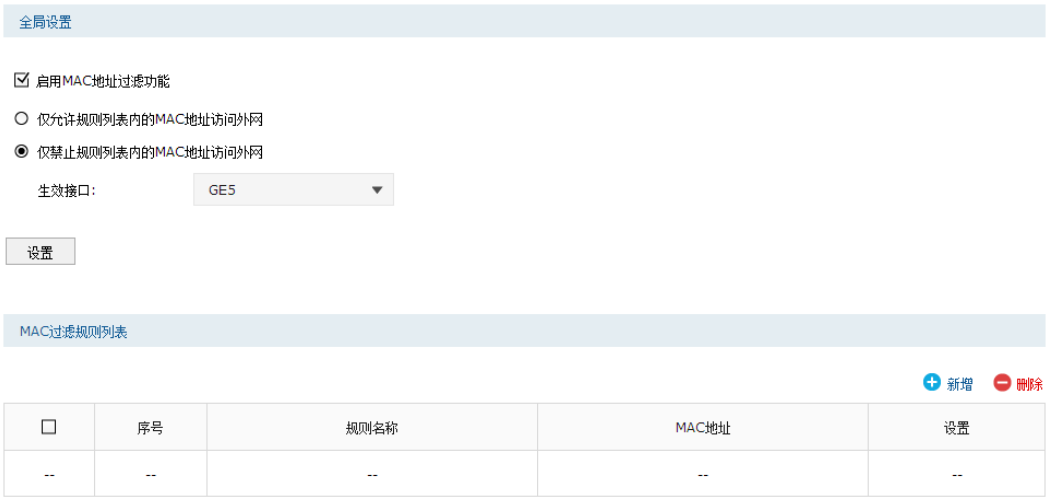


图 7-12 MAC过滤设置界面

全局设置

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

MAC过滤规则设置

点击<新增>，配置MAC过滤规则。

MAC地址过滤规则

规则名称	输入该规则条目的名称。
MAC地址	输入需要控制的局域网主机MAC地址。

表 7.5 MAC过滤设置界面项说明

7.4 访问控制

7.4.1 基本概念

在创建访问控制策略时，需要引用路由器对象管理中的以下模块：

- 服务类型：指定策略生效的协议和端口号。设置界面：对象管理 >> 服务类型。
- 地址管理：指定策略生效的地址范围。设置界面：对象管理 >> 地址管理。
- 时间管理：指定策略生效的时间范围。设置界面：对象管理 >> 时间管理。

本路由器提供允许和阻塞两种行为控制信息流，其连同服务类型、源地址、目的地址、时间以及区段，构成了访问策略所必需的几个元素。通过创建策略，定义允许或阻塞在预定时间通过指定源地址到达指定目的地址的信息流的种类，可以控制区段间的信息流。控制范围最大时，可以阻塞所有类型的信息流从一个接口中的任何源地址到其它所有接口中的任何目的地址，而且没有任何预定时间限制。控制范围最小时，可以创建一个策略，只允许一种信息流在预定的时间段内、在一个接口下的指定主机与另一接口下的指定主机之间流动。可以参考图 7.13理解。

图 7-13 策略生效范围示意图

7.4.2 配置访问规则

进入界面：安全管理 >> 访问控制 >> 访问控制

点击<新增>，配置访问规则。

图 7-14 访问规则设置界面

规则名称	输入一个名称来标识该访问规则。
策略类型	在下拉列表中选择适用于本条规则的策略类型，可选择阻塞或者允许。选择“阻塞”，则符合该条规则的所有数据包将无法通过路由器；选择“允许”，则符合该条规则的数据包能通过路由器。
服务类型	在下拉列表中选择本条规则所针对的服务类型，不属于指定范围内的服务将不会应用该规则。例如策略类型选择为“阻塞”，只选定了FTP一种服务类型时，其他服务类型的数据包仍旧可以通过路由器。如需新建服务类型，请参考**5.4服务类型。**
生效接口	在下拉列表中选择本条规则生效的接口。
源地址范围	在下拉列表中选择本条规则限制的源地址范围。源地址必须是所选接口下的地址。路由器预定义“IPGROUP_ANY”地址组表示所有地址。如需新建地址组，请参考**5.1地址管理**。
目的地址范围	在下拉列表中选择本条规则限制的目的地址范围。目的地址可以是任意接口下的任意地址。路由器预定义“IPGROUP_ANY”地址组表示所有地址。如需新建地址组，请参考**5.1地址管理**。
规则生效时间	在下拉列表中选择本条规则生效的时间表。如需新建时间表，请参考**5.2时间管理。**
添加到指定位置（第几条）	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，新增规则显示在规则列表的最后。规则条目在规则列表中的位置越靠前，即规则序号数字越小，该规则优先级越高。

表 7.6 访问规则设置界面条目项说明

说明：

除了“IPGROUP_ANY”地址组，路由器会为每个地址组自动添加一个与其相对应的“!”（非）地址组，表示除了该地址组内地址之外的所有地址。

新增规则信息会在**规则列表**中显示出来。图 7.15中规则效果是：任何时间，接口2内的主机都不能通过路由器与其他接口进行通信。

图 7-15 区段内访问规则设置界面-规则列表

配置访问规则步骤：

1) 创建服务类型。非必须操作。路由器预定义了如HTTP、FTP、TELNET等常用服务类型，如果需要使用的服务类型为预定义的，则不必此项操作。具体操作步骤请参考**5.4服务类型**。

2) 创建地址组。非必须操作。路由器已预定义部分地址组，如果需要限制的地址组为预定义的，则不必此项操作。具体操作步骤请参考**5.1地址管理**。

3) 创建时间组。非必须操作。路由器已预定义“Any”时间组，表示任何时间，如果需要限制的时间为此，则不必此项操作。具体操作步骤请参考**5.2时间管理**。

4) 创建访问规则。必须操作。创建界面：安全管理 >> 访问控制 >> 访问控制，点击<新增>，设置规则名称，选择所需的策略类型、服务类型、接口、源地址范围、目的地址范围、规则生效时间，然后指定规则的优先级，点击<确定>按钮完成配置。

5) 编辑访问规则。非必须操作。编辑界面：安全管理 >> 访问控制 >> 访问控制，在此界面的规则列表区域，可以查看、编辑和删除策略。

7.4.3 访问控制应用

■ 控制到路由器本身的报文

应用一：

创建策略，使GE2中的主机不能以任何形式访问路由器。

配置步骤：

1) 创建访问规则。创建界面：安全管理 >> 访问控制>> 访问控制。点击<新增>，规则设置如下，点击<确定>按钮完成。

名称	GE2_Policy1
策略类型	阻塞
服务类型	ALL
生效接口	GE2
源地址范围	IPGROUP_ANY
目的地址范围	Me

规则生效时间	Any

表 7.7 访问控制应用一创建规则

应用二：

与应用一相对应，可以创建策略，使GE2中的主机，只能访问路由器，而不能向其它接口发送报文。

配置步骤：

2) 创建访问规则。创建界面：安全管理 >> 访问控制 >> 访问控制。点击<新增>，规则设置如下，点击<确定>按钮完成。

名称	GE2_Policy2
策略类型	阻塞
服务类型	ALL
生效接口	GE2
源地址范围	IPGROUP_ANY
目的地址范围	！Me
规则生效时间	Any

表 7.8 访问控制应用二创建规则

■ 控制某接口到某个地址组的报文

应用三：

创建策略，使得IP地址为1.1.1.1的主机无论接入任何接口，GE2区段的报文都不能到达该主机。该策略生效效果如下所示：

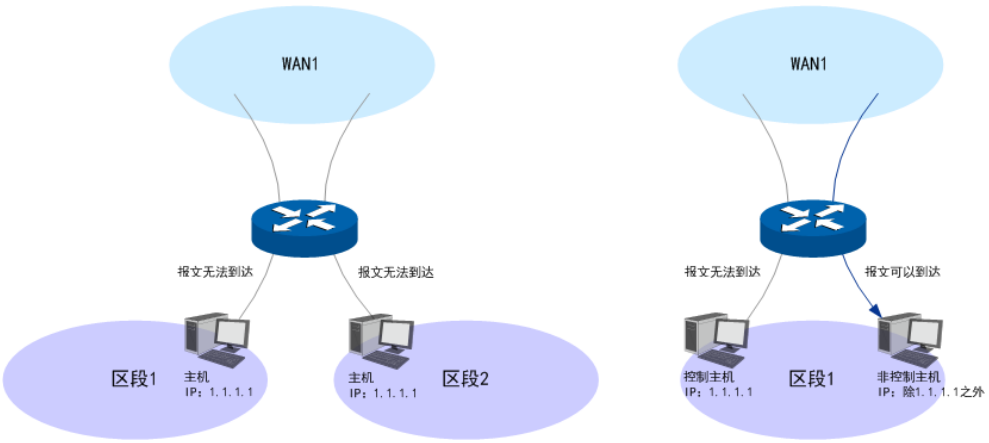


图 7-16 应用三

配置步骤：

1) 创建地址组。创建界面：对象管理 >> 地址管理。

进入标签页**地址管理**，点击<新增>，设置地址组名称为Host，点击<确定>按钮完成。

名称	Host

表 7.9 访问控制应用三设置地址组

进入标签页**地址**，点击<新增>，设置地址名称为HostIP，选择IP类型为IP/Mask，输入1.1.1.1/32，点击<确定>按钮完成。

名称	HostIP
IP类型	IP/Mask 1.1.1.1/32

表 7.10 访问控制应用三设置地址

进入标签页**视图**，组名选择主机，在可选用户中，选中HostIP，点击  按钮，将HostIP移到包含用户中，点击<确定>按钮完成。

2) 创建访问规则。创建界面：安全管理 >> 访问控制 >> 访问控制。点击<新增>，规则设置如下，点击<确定>按钮完成。

名称	GE2_Policy3
策略类型	阻塞
服务类型	ALL
区段	WAN1
源地址范围	IPGROUP_ANY
目的地址范围	Host
规则生效时间	Any

表 7.11 区段内策略应用三设置区段内访问规则

应用四：

接口GE1的网段IP为10.1.1.0/24，接口GE2的网段IP为10.1.2.0/24。现在需要阻塞GE1和GE2之间的通信，可以创建访问规则，阻塞接口GE1内的主机和接口GE2内的主机互相访问。

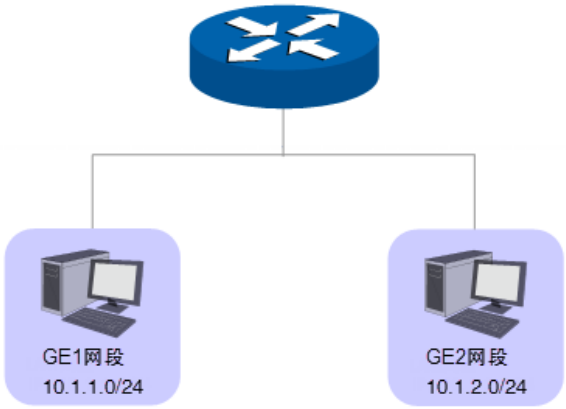


图 7-17 应用四

配置步骤：

1) 创建地址组。创建界面：对象管理 >> 地址管理。

进入标签页**地址组**，定义两个地址组：GE1_Segment和GE2_Segment。点击<新增>，设置地址组名称，点击<确定>按钮完成。

GE1网段设置如下：

名称	GE1_Segment

表 7.12 访问控制应用四设置地址组1

GE2网段设置如下：

名称	GE2_Segment

表 7.13 访问控制应用四设置地址组2

进入标签页**地址**，定义两个地址名称：GE1_Segment_IP 和 GE2_Segment_IP 。GE1_Segment_IP，选择IP类型为IP/Mask，输入10.1.1.0/24。GE2_Segment_IP，选择IP类型为IP/Mask，输入10.1.2.0/24。

GE1网段IP设置如下：

名称	GE1_Segment_IP
IP类型	IP/Mask 10.1.1.0/24

表 7.14 访问控制应用四设置地址1

GE2网段IP设置如下：

名称	GE2_Segment_IP
IP类型	IP/Mask 10.1.2.0/24

表 7.15 访问控制应用四设置地址2

进入标签页**视图**，组名选择GE1_Segment，在可选用户中，选中GE1_IP，点击按钮，将GE1_Segment_IP移到包含用户中，点击<确定>按钮完成。

组名选择GE2_Segment，在可选用户中，选中LAN2网段IP，点击  按钮，将GE2_Segment_IP移到包含用户中，点击<确定>按钮完成。

2) 创建访问规则。创建界面：安全管理 >> 访问控制 >> 访问控制。点击<新增>，规则设置如下，点击<确定>按钮完成。

名称	GE1_Policy1
策略类型	阻塞
服务类型	ALL
生效接口	GE1

源地址范围	GE1_Segment
目的地址范围	GE2_Segment
规则生效时间	Any

表 7.16　访问控制应用四设置访问规则

7.4.4　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。

进入界面：安全管理 >> 访问控制 >> URL过滤

图 7-18　URL过滤设置界面

功能设置

若需要严格控制局域网对广域网的访问，推荐勾选“启用URL地址过滤功能”。

点击<新增>，设置URL地址过滤规则。点击<确定>完成设置。

图 7-19　URL规则列表界面

URL地址过滤规则

用户组	选择受规则控制的IP地址范围，由对象管理中的地址组表示。IPGROUP_ANY为系统默认设置的地址组，表示所有计算机，如需新建地址组，请参考**5.1地址管理**。
策略	根据实际需求选择一种过滤策略：允许访问下列的URL或禁止访问下列的URL。
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地址完全匹配您输入的完整URL地址时才能进行过滤。
过滤内容列表	当过滤方式为“关键字”的时候，在此输入指定的关键字字符；当过滤方式为“完整URL”的时候，在此输入完整的广域网URL地址。
备注	输入对该条过滤规则的说明，便于区分。
添加到指定位置（第几条）	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，新增规则显示在规则列表的最后。规则条目在规则列表中的位置越靠前，即规则序号数字越小，该规则优先级越高。

表 7.17　URL过滤设置界面项说明

规则列表

在规则列表中，可以对已保存的URL地址条目进行相应设置。

应用举例

某企业希望禁止局域网内的主机访问网站：www.aabbcc.com，同时还禁止下载“.exe”后缀的文件。

可以通过设置URL过滤实现此需求。点击<新增>，设置完整URL过滤“www.aabbcc.com”，以及关键字过滤“.exe”，如下图。

表 7.18　应用举例说明

第8章 行为管控

8.1 应用控制

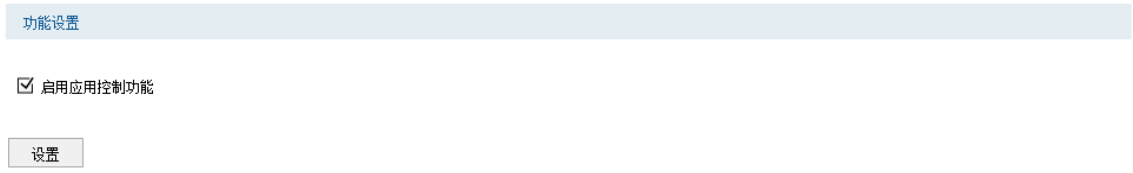
应用控制包括各类软件应用控制功能和 QQ 黑白名单功能。

8.1.1 应用控制

可以在此启用并设置应用控制功能。

进入界面：行为管控 >> 应用控制 >> 应用控制

启用应用控制规则功能，点击<设置>保存配置。



点击<新增>，设置应用控制规则。点击<确定>保存配置。

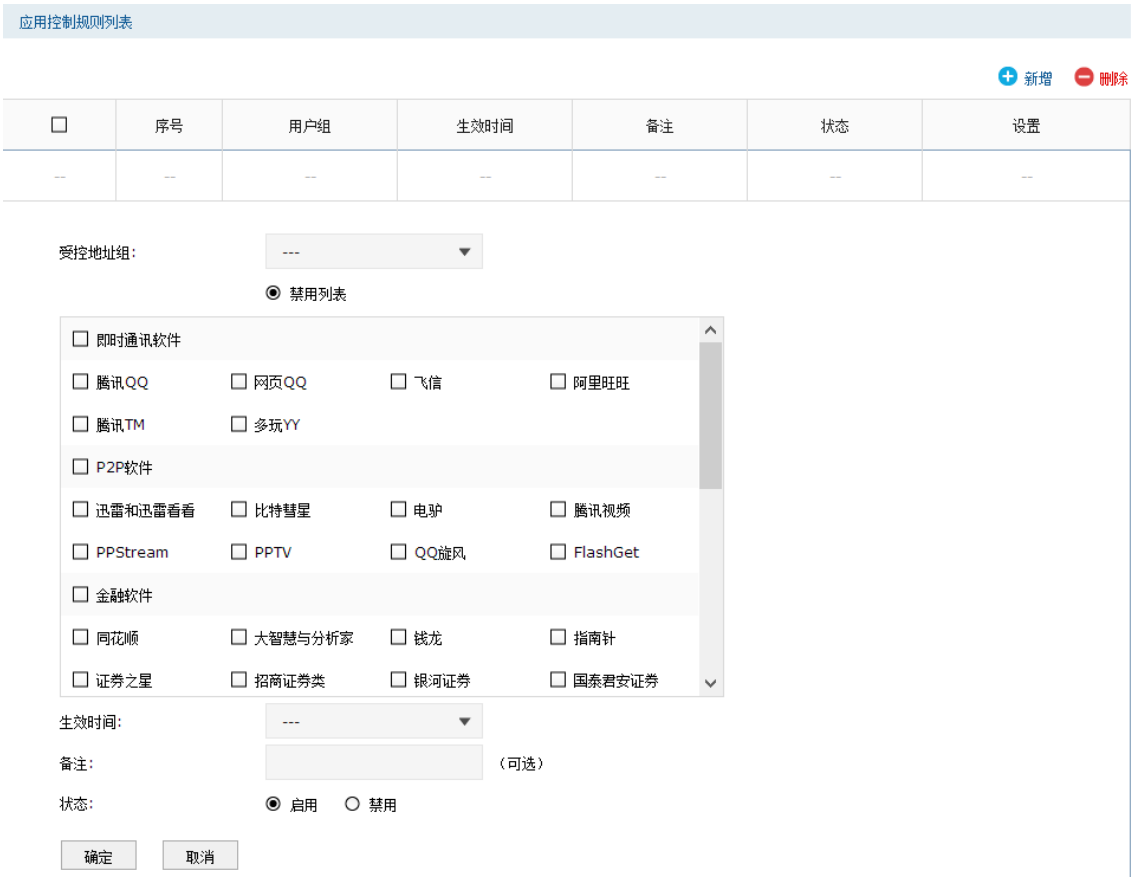


图 8-1 应用控制设置界面

应用控制设置

受控地址组	在下拉菜单中选择所需限制的组。如需新建组，请参考**5.1地址管理**。
禁用列表/记录列表	选择禁用列表或记录列表，并在列表中选择应用。可以设置的应用包括即时通信、P2P软件、金融软件、网络游戏、视频软件、音乐软件、基础应用和代理。
生效时间	指定规则生效时间。如需新建时间对象，请参考**5.2时间管理**。
备注	添加对本条规则的说明信息。
状态	选择是否启用所设置的规则。

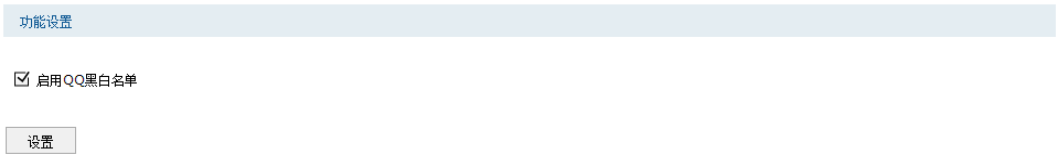
表 8.1　应用限制设置界面项说明

8.1.2　QQ黑白名单

可以在此对指定的QQ号码进行相关规则设置。

进入界面：行为管控 >> 应用控制 >> QQ黑白名单

勾选<启用QQ黑白名单>，点击<设置>保存配置。



点击<新增>，设置QQ黑白名单规则。点击<确定>保存配置。

图 8-2　QQ黑白名单管理界面

QQ黑白名单规则设置

受控地址组	在下拉菜单中选择所需限制的组。如需新建组，请参考**5.1地址管理**。
规则类型	勾选规则类型。 白名单：允许下列QQ号码登录。 黑名单：进制下列QQ号码登录。
QQ号	指定QQ号码，可以同时输入多个QQ号码进行批量添加。不同QQ号码之间以换行符、空格或逗号分隔。
当使用上述QQ号码时	选择是否在使用上述QQ号码时记录到系统日志。
生效时间	指定规则生效时间。如需新建时间对象，请参考**5.2时间管理**。
备注	添加对本条规则的说明信息。
状态	选择是否启用该条规则。
添加到指定位置（第几条）	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，新增规则显示在规则列表的最后。规则条目在规则列表中的位置越靠前，即规则序号数字越小，该规则优先级越高。

表 8.2　QQ黑白名单规则设置界面项说明

8.2　网址过滤

8.2.1　网站分组

可以在此对网站进行分组。

进入界面：行为管控 >> 网址过滤 >> 网站分组

网站分组列表

新增　删除

☐	序号	组名称	组成员	备注	设置
☐	1	视频	*.56.com 更多	---	
☐	2	游戏	*.17173.com 更多	---	
☐	3	财经	*.10jqka.com.cn 更多	---	
☐	4	社交	*.51.com 更多	---	
☐	5	购物	*.360buy.com 更多	---	
☐	6	生活	*.100ye.com 更多	---	
☐	7	音乐	*.1ting.com 更多	---	
☐	8	娱乐	*.67.com 更多	---	
☐	9	论坛	*.daqi.com 更多	---	
☐	10	邮箱	*.eyou.com 更多	---	
☐	11	小说	*.2100book.com 更多	---	
☐	12	体育	*.1soccer.com 更多	---	
☐	13	新闻	*.cankaoa.com 更多	---	

图 8-3　网站分组列表

该表格显示了网站分组列表，可对某个分组进行编辑，或选择一个或多个条目对其进行删除。点击<新增>创建分组。点击<确定>保存配置。

图 8-4 网站分组列表界面

网站分组列表设置

组名称	为该分组添加名称。
组成员	在此输入网站分组成员。组成员可以为域名，如www.tp-link.com.cn，也可以在域名前面加通配符“*”，如*.tp-link.com.cn，但“*”只允许输入在域名最前面，而不能夹杂在域名中间或后面。可以同时输入多个网站进行批量添加，通过使用空格、逗号或者回车换行来表示不同的网站。每组最多可以输入200个网站。
文件路径	可以通过上传txt文件添加组成员，txt文件内容需按照组成员添加的格式进行编辑，上传完成后，文件内容将显示在组成员文本框中。
备注	添加对该组的说明信息。

表 8.3 网站分组界面

8.2.2 网站过滤

在此可对特定的网站进行过滤。

进入界面：行为管控 >> 网址过滤 >> 网站分组

启用网站过滤功能，点击<设置>保存配置。

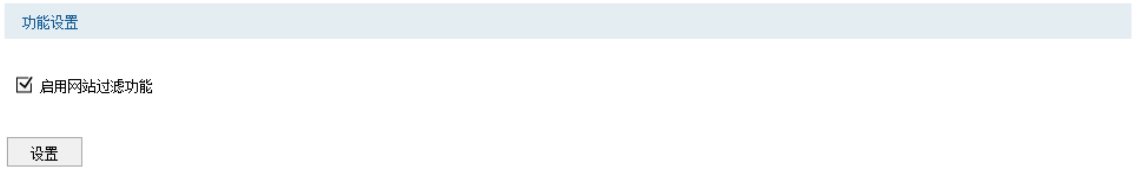


图 8-5　网站过滤功能设置界面

点击<新增>，配置网站过滤规则。点击<确定>保存配置。

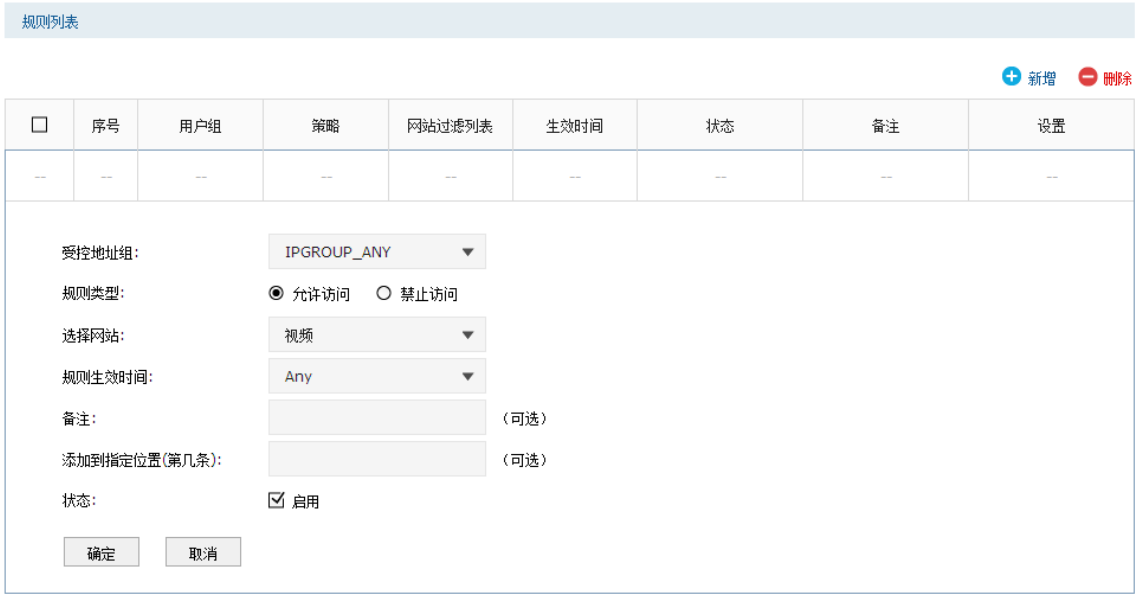


图 8-6　网站过滤规则设置界面

网站过滤规则设置

受控地址组	在下拉菜单中选择所需限制的组。如需新建组，请参考**5.1地址管理**。
规则类型	选择规则类型。 允许访问：允许访问下列网站。 禁止访问：禁止访问下列网站。
选择网站	可以选择“所有网站”，使规则对任意网站生效；也可以对已有的网站分组进行勾选。如需新建组，请参考**网站分组**。
规则生效时间	指定规则生效时间。如需新建时间对象，请参考**5.2时间管理**。
备注	添加对本条规则的说明信息。
添加到指定位置（第几条）	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。
状态	选择是否启用该条规则。

8.2.3　URL 过滤

在此可以配置对 URL 进行过滤的规则。

进入界面：行为管控 >> 网址过滤 >> 网站分组

启用 URL 过滤功能，点击<设置>保存配置。

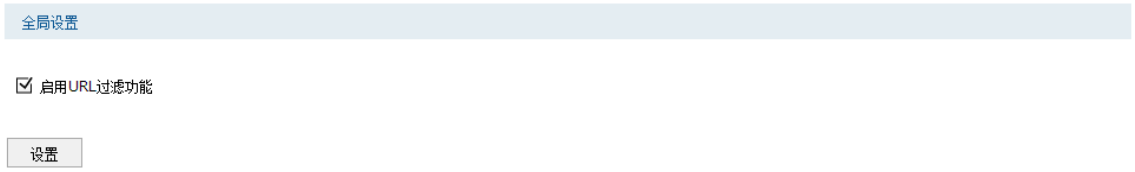


图 8-7 URL过滤全局设置界面

点击<新增>，配置URL过滤规则。点击<确定>保存配置。

图 8-8 URL过滤规则列表界面

网站过滤规则设置

受控地址组	在下拉菜单中选择所需限制的组。如需新建组，请参考**5.1地址管理**。
策略类型	选择策略类型。可以选择允许访问下列的URL或禁止访问下列的URL。

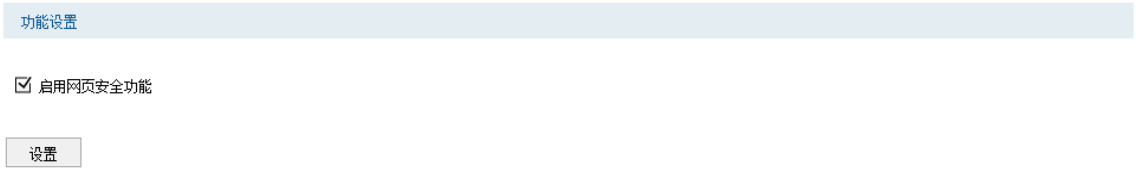
过滤方式	选择一种过滤方式。“关键字”过滤即所有包含指定字符的URL地址全都进行过滤；“完整URL”过滤则仅当URL地址完全匹配输入的完整URL地址时才能进行过滤。 可以同时输入多个关键字或完整URL进行批量添加，通过使用空格、逗号或者回车换行来表示不同的关键字或完整URL。最多可以添加10个关键字或完整URL，每一个关键字或完整URL的可输入长度为1-64个字符，但输入的总字符数不能超过300个（包括相邻两条关键字或URL地址之间的分隔符）。
过滤内容列表	输入过滤内容，不同内容条目之间用换行或者分号隔开。
规则生效时间	指定规则生效时间。如需新建时间对象，请参考5.2时间管理。
状态	选择是否启用该条规则。
备注	添加对本规则的说明信息。
添加到指定位置（第几条）	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。

8.2.4 网页安全

在此可以配置网页安全规则。

进入界面：行为管控 >> 网页安全 >> 网页安全

启用网页安全功能，点击<设置>保存配置。



点击<新增>，配置网页安全规则。点击<确定>保存配置。

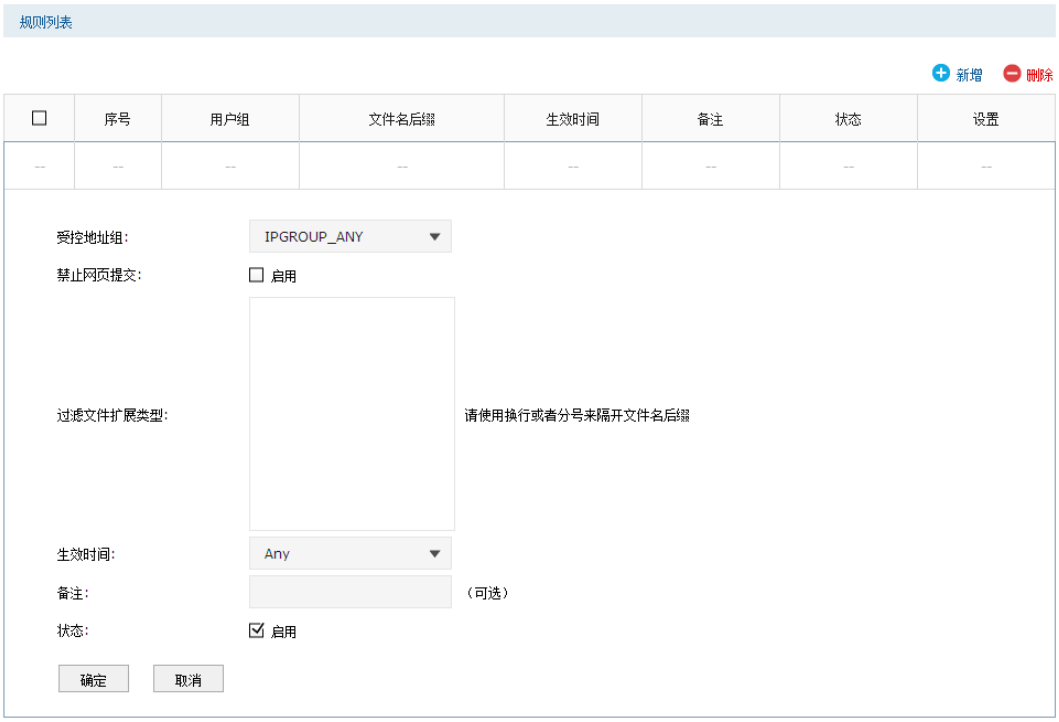


图 8-9 网页安全界面

网页安全规则设置

受控地址组	在下拉菜单中选择所需限制的组。如需新建组，请参考5.1地址管理。
禁止网页提交	勾选“启用”，可以禁止所有的HTTP POST提交。
过滤文件扩展类型	可以在过滤文件扩展类型编辑框内输入多个扩展名，并以空格、逗号或者回车换行来分隔。
生效时间	指定规则生效时间。如需新建时间对象，请参考5.2时间管理。
备注	添加对本规则的说明信息。
状态	选择是否启用该条规则。

8.3 策略库升级

可以在此进行应用特征数据库的升级。

进入界面：行为管控 >> 策略库升级 >> 策略库升级

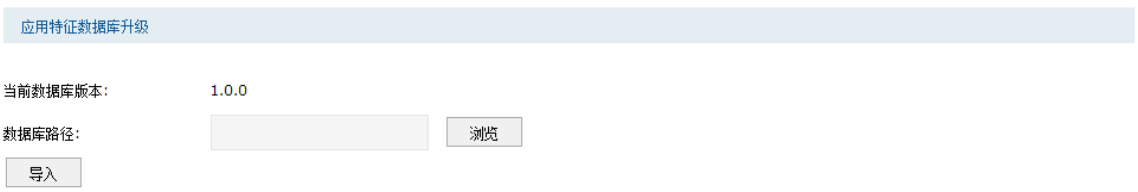


图 8-10 数据库界面

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

第9章 VPN

VPN（Virtual Private Network，虚拟专用网络）是指建立在公用网络（如Internet）上的虚拟、专用的连接。虚拟体现在该VPN连接并不是端到端实际铺设的物理线路，而是逻辑意义上存在的；专用体现在用户可以建立符合自身需求的网络连接，且只有特定用户才能使用该VPN连接进行数据传输。

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。隧道技术指数据封装、传输、解封装的全过程。VPN典型拓扑如下图所示。

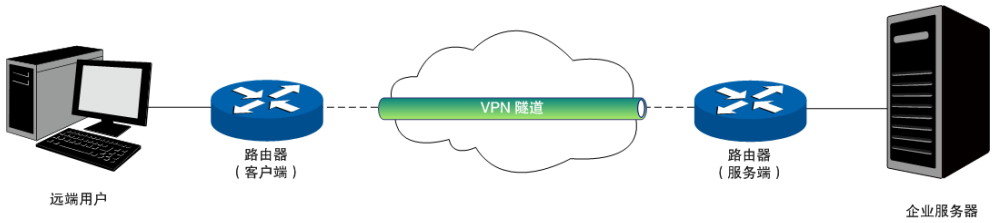


图 9-1　VPN典型拓扑

用户在VPN隧道中传输数据，需依赖于隧道协议。隧道协议规定了隧道的建立，维护和删除规则以及如何将企业网的数据封装在隧道中进行传输。隧道协议通过在隧道的一端给数据添加隧道协议头，即进行封装，使这些被封装的数据都能经由隧道进行传输，并在隧道的另一端去掉数据携带的隧道协议头，即进行解封装。

隧道协议可分为二层隧道协议和三层隧道协议。我司无线企业VPN路由器支持的隧道协议包括二层隧道协议PPTP（Point-to-Point Tunneling Protocol，点到点隧道协议），L2TP（Layer 2 Tunneling Protocol，第二层隧道协议）和三层隧道协议IPSec（IP Security，IP安全）。

- 二层隧道协议：PPTP、L2TP。

PPTP协议将链路层PPP帧封装在IP数据包内，通过IP网络传送数据。L2TP协议根据不同的网络类型，将链路层PPP帧封装在不同的数据包中进行传输。

PPTP、L2TP均使用PPP协议对数据进行封装，并添加附加头部用于数据在公用网络上的传输，但二者有以下不同：

1) PPTP只能在IP网络上使用；L2TP只要求隧道媒介提供面向数据包的点对点的连接，可在IP、ATM、帧中继等网络上使用。

2) PPTP只能在两端点间建立单一隧道；L2TP可在两端点间针对不同的服务质量建立多条隧道。

3) PPTP不支持隧道验证；L2TP可提供隧道验证，但当L2TP与IPSec共同使用时，可以由IPSec提供隧道验证，不需要在第2层协议上验证隧道。

4) PPTP不支持包头压缩，系统开销（overhead）占用6个字节；L2TP支持包头压缩，系统开销（overhead）占用4个字节。

- 三层隧道协议：IPSec。

IPSec协议把数据封装在隧道协议中，依靠第三层协议进行数据传输，只适用于TCP/IP网络。

三层隧道协议和二层隧道协议相比，具有更好的安全性和可靠性。第二层隧道一般中止在用户侧设备上，对用户端的安全及防火墙技术要求很高；而第三层隧道一般中止在ISP (Internet Service Provider，互联网服务提供商）网关，不会对用户端的安全性有较高的需求。

9.1 IPsec

IPSec（IP Security）是保证网络安全的一系列服务和协议的集合，主要依赖密码技术提供验证和加密机制，可实现如下安全服务：

- 数据机密性（Confidentiality）：发送方在传输数据前对数据包进行加密，有效避免传输过程中数据包被截取所带来的风险。
- 数据完整性（Data Integrity）：接收方接收数据时利用散列函数对每个数据包重新生成一个校验和，与发送方生成的校验和相比较，二者不符则丢弃相应数据包，防止数据在传输过程中被篡改。
- 数据来源验证（Data Authentication）：接收方及发送方相互进行身份验证，确保数据来源的合法性。
- 防重放（Anti-Replay）：接收方可识别并丢弃重发的报文，防止第三方利用截取的报文进行攻击。

IPSec在IP层实现了验证、加密、访问控制等多种安全技术，通过通信双方建立双向安全联盟，在互联网中形成一个安全可靠的IPSec隧道，确保数据的安全传输。

IPSec协议集主要包括认证头协议AH（Authentication Header）、封装安全载荷协议ESP（Encapsulating Security Payload）及互联网密钥交换协议IKE（Internet Key Exchange），其中AH协议和ESP协议通过对传输数据的处理提供安全性保证；IKE协议则通过实现密钥的协商、交换、分发提供了处理传输数据的相应规则。

9.1.1 IPsec安全策略

进入界面：VPN >> IPsec >> IPsec安全策略

点击<新增>，进行IPsec基本设置。

图 9-2 IPsec安全策略基本设置界面

策略名称	为IPsec安全策略命名。
对端网关	输入对端IPSec 链路的绑定接口，可以填写对端接口的IP 地址或域名。可设置为"0.0.0.0"，表示任意地址。
绑定接口	绑定本地IPSec链路的出接口；对端路由器设置的"对端网关"必须与该接口的IP地址或域名相同。
本地子网范围	设定本地子网地址，以子网掩码值划分地址范围。
对端子网范围	设定对方子网地址，以子网掩码值划分地址范围。
预共享秘钥	设置通信双方互相认证的密钥，双方必须使用同一字符串作为预共享密钥，可输入英文字母和数字的组合。
状态	选择启用或禁用当前策略条目。

表 9.1 IPsec安全策略基本设置界面项说明

点击<高级设置>，进行IPsec高级设置。

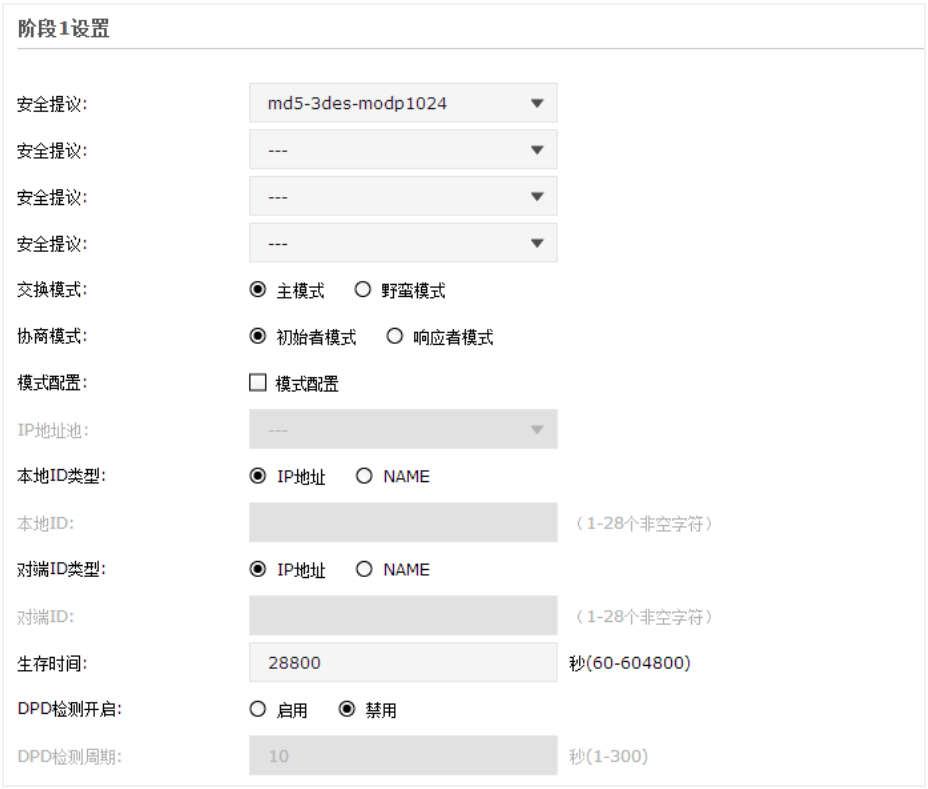


图 9-3 IPsec安全策略基本设置界面

阶段 1 设置

安全提议	指定相应的IKE安全提议，最多可选择四个安全提议。
交换模式	设置IKE协商第一阶段的交换模式，该交换模式必须与对端相同。交换模式有以下两种： 主模式：该模式双方交换报文多，提供身份保护，适用于对身份保护要求较高的场合。 野蛮模式：该模式不提供身份保护，双方交换报文少，协商速度快，适用于对身份保护要求不高的场合。
协商模式	设置IKE协商的模式，该协商模式可以与对端不同。协商模式有以下两种： 初始者模式：配置该模式后，IKE才能主动发起协商。 本地和对端至少有一方必须设置为初始者模式。 响应者模式：配置该模式后，IKE不会主动发起协商，需要等待对端发起协商。本地和对端不能同时为响应者模式。
模式配置	设置是否开启模式配置。开启模式配置后，当VPN客户端请求IP地址时，将会从配置的IP地址池里分配IP给客户端。
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的交换与认证，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（任意英文字母和数字的组合）。本地路由器的“本地ID”需与对端路由器的“对端ID”保持一致，而“对端ID”则需与对端路由器的“本地ID”保持一致。
生存时间	设定IKE SA的生存时间，单位为秒。
DPD检测开启	DPD（Dead Peer Detect，对端存活检测）开启后，IKE一端能够周期性主动检测对端的链路连接状态。

表 9.2　IPsec安全策略高级设置界面项说明

阶段 2 设置

封装模式	设置隧道中数据报文的封装模式，该封装模式必须与对端相同。封装模式有以下两种： 隧道模式：在该模式下，AH或ESP插在原始IP报文头之前，另外生成一个新的IP报头放到AH或ESP之前。从安全性来讲，隧道模式优于传输模式。适用于更普遍的VPN应用。 传输模式：在该模式下，AH或ESP被插入到IP报头之后但在所有传输层协议之前，或所有其他IPSec协议之前。适用于主机直接访问设备时的加密传输。
安全提议	指定相应的IPsec安全提议，最多可选择四个安全提议。
PFS	选择是否启用PFS（Perfect Forward Secrecy，完全前向保密），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，单位为秒。

表 9.3　IPsec安全策略基本设置界面项说明

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4。

9.1.2 IPsec安全联盟

在此将列出路由器上所有已成功建立的IPsec安全联盟相关信息。

进入界面：VPN >> IPsec >> IPsec安全联盟

图 9-4 IPsec安全联盟界面

在图 9-4中路由器使用eth2接口进行隧道连接，eth2接口的IP地址为192.168.10.100，对端网关地址为172.29.85.199。IPsec隧道的安全提议等相关设置需与对端路由设置相同。

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

9.2 L2TP

L2TP（Layer 2 Tunneling Protocol， 第二层隧道协议）是二层VPN隧道协议，它的实现基于C/S（Client/Server，客户端/服务器）模型，在客户端和服务器间建立起L2TP隧道。客户端任选一个空闲的端口向服务器的UDP 1701端口发送报文，服务器收到报文后，也任选一个空闲的端口向客户端回送报文，至此，双方的端口选定，在该隧道连通的时间内保持不变。

L2TP协议本身并不提供连接的安全性，但它可依赖于PPP提供的认证（比如CHAP、PAP等），因此具有PPP所具有的所有安全特性。L2TP可与IPsec 结合起来实现数据安全，这使得通过L2TP所传输的数据更难被攻击。L2TP还可根据特定的网络安全要求在L2TP之上采用隧道加密技术、端对端数据加密或应用层数据加密等方案来提高数据的安全性。

9.2.1 L2TP服务器设置

当路由器作为 L2TP 服务器时，则还需进入 VPN 用户管理界面设置用户账号。

进入界面：VPN >>L2TP >> L2TP服务器

图 9-5　L2TP服务器设置界面

全局设置

L2TP隧道维护时间间隔	设置L2TP隧道维护的时间间隔，范围是60秒至1000秒。设置此时间间隔，服务器按照设定间隔发出报文，用以确定L2TP隧道的连接状态。如无特别要求，请保持默认设置。
PPP链路维护时间间隔	设置L2TP隧道里的PPP链路维护的时间间隔。范围是0秒至120秒，0代表不发送。设置此时间间隔，服务器按照设定间隔发出报文，用以确定PPP链路的连接状态。如无特别要求，请保持默认设置。

表 9.4　L2TP服务器设置-全局管理设置界面项说明

点击<新增>，进行隧道设置。

图 9-6　L2TP服务器列表

隧道设置

服务接口	绑定接口为服务器端路由器WAN端口上出链路接口。如有多条上网链路，请根据实际情况，选择其中一条链路承载L2TP VPN隧道。此接口的IP地址即为L2TP服务器的IP地址。
IPsec加密	选择是否使用IPsec对L2TP隧道加密。可选项有：加密，不加密，可选加密。

预共享秘钥	设置IPSec加密时通信双方互相认证的密钥，双方必须使用同一个预共享密钥。
状态	选择启用或禁用本L2TP隧道。

表 9.5 PPTP服务器设置-隧道设置界面项说明

9.2.2 L2TP客户端设置

进入界面：VPN >>L2TP >> L2TP客户端

图 9-7 L2TP服务器设置界面

全局设置

L2TP隧道维护时间间隔	设置L2TP隧道维护的时间间隔，范围是60秒至1000秒。设置此时间间隔，服务器按照设定间隔发出报文，用以确定L2TP隧道的连接状态。如无特别要求，请保持默认设置。
PPP链路维护时间间隔	设置L2TP隧道里的PPP链路维护的时间间隔。范围是0秒至120秒，0代表不发送。设置此时间间隔，服务器按照设定间隔发出报文，用以确定PPP链路的连接状态。如无特别要求，请保持默认设置。

表 9.6 L2TP服务器设置-全局管理设置界面项说明

点击<新增>，进行隧道设置。

图 9-8 L2TP客户端设置

隧道设置

隧道名称	设置隧道名称。
用户名	设置L2TP认证时客户端使用的用户名。客户端与服务器的设置需保持一致。
密码	设置L2TP认证时客户端使用的密码。客户端与服务器的设置需保持一致。
出接口	服务器端路由器WAN端口上出链路接口。如有多条上网链路，请根据实际情况，选择其中一条链路承载L2TP VPN隧道。
服务器地址	设置对端服务器地址。
IPsec加密	选择是否使用IPsec对L2TP隧道加密。
对端子网	设置L2TP隧道对端局域网所使用的IP地址范围（一般可以填VPN隧道对端设备的LAN口IP地址范围），由IP和子网掩码组成。
工作模式	选择NAT模式或路由模式。
状态	选择启用或禁用本L2TP隧道。
参与流量均衡	选择是否参与流量均衡。

9.2.3 L2TP服务器隧道信息

在此将列出路由器上所有里L2TP隧道的相关信息。

进入界面：VPN >> L2TP >> 隧道信息列表

图 9-9 L2TP隧道信息界面

9.3 PPTP

PPTP（Point-to-Point Tunneling Protocol，点到点隧道协议）定义于IETF的RFC2637中，是一种在PPP（Point to Point Protocol，点到点）协议基础上开发的支持按需、多协议VPN的二层隧道技术，通过跨越基于TCP/IP的数据网络创建VPN，实现安全的远程访问连接。

PPTP的实现基于C/S（Client/Server，客户端/服务器）模型，在客户端和服务器间建立起PPTP隧道。客户端使用服务器提供的账户信息拨号连接到服务器上，服务器默认在TCP 1723端口上监听服务，从而实现双方的通信。

PPTP的通信要建立两条连接，即控制连接和数据连接。控制连接使用TCP作为传输协议，用于对呼叫的控制和管理，负责建立、维护和拆除客户端和服务器间的数据隧道；数据连接使用PPP协议对原始报文进行封装，使用增强的GRE（Generic Routing Encapsulation，通用路由封装）协议作为隧道协议，并添加新的IP头用于数据在互联网上路由。

安全性上，PPTP利用了PPP提供的认证机制，支持PAP（Password Authentication Protocol，密码认证协议）、CHAP（Challenge Handshake Authentication Protocol，询问握手认证协议）、MS-CHAP（微软CHAP）等身份验证方式，可选用MPPE（Microsoft Point-to-Point Encryption，微软点对点加密）协议进行加密。MPPE加密技术支持40、56、128位三种长度的加密，其安全性被普遍认为比较弱，因此，如涉及到敏感数据传输，一般不推荐使用PPTP VPN。

9.3.1 PPTP服务器设置

当路由器作为 PPTP 服务器时，还需进入 VPN 用户管理界面设置用户账号。

进入界面：VPN >>PPTP >> PPTP服务器

图 9-10　PPTP服务器设置界面

全局设置

PPTP隧道维护时间间隔	设置PPTP隧道维护的时间间隔，范围是60秒至1000秒。设置此时间间隔，服务器按照设定间隔发出报文，用以确定PPTP隧道的连接状态。如无特别要求，请保持默认设置。
PPP链路维护时间间隔	设置PPTP隧道里的PPP链路维护的时间间隔。范围是0秒至120秒，0代表不发送。设置此时间间隔，服务器按照设定间隔发出报文，用以确定PPP链路的连接状态。如无特别要求，请保持默认设置。

表 9.7　PPTP服务器设置-全局管理设置界面项说明

点击<新增>，进行隧道设置。

图 9-11　PPTP服务器列表

隧道设置

服务接口	请选择绑定的接口。当前用户仅对绑定的接口提供PPTP服务。
MPPE加密	选择是否使用MPPE对PPTP隧道加密。
状态	选择启用或禁用本PPTP隧道。

表 9.8　PPTP服务器设置-隧道设置界面项说明

9.3.2 PPTP客户端设置

进入界面：VPN >>PPTP >> PPTP客户端

图 9-12 PPTP全局设置

全局设置

PPTP隧道维护时间间隔	设置PPTP隧道维护的时间间隔，范围是60秒至1000秒。设置此时间间隔，服务器按照设定间隔发出报文，用以确定PPTP隧道的连接状态。如无特别要求，请保持默认设置。
PPP链路维护时间间隔	设置PPTP隧道里的PPP链路维护的时间间隔。范围是0秒至120秒，0代表不发送。设置此时间间隔，服务器按照设定间隔发出报文，用以确定PPP链路的连接状态。如无特别要求，请保持默认设置。

表 9.9 PPTP客户端设置-全局管理设置界面项说明

点击<新增>，进行隧道设置。

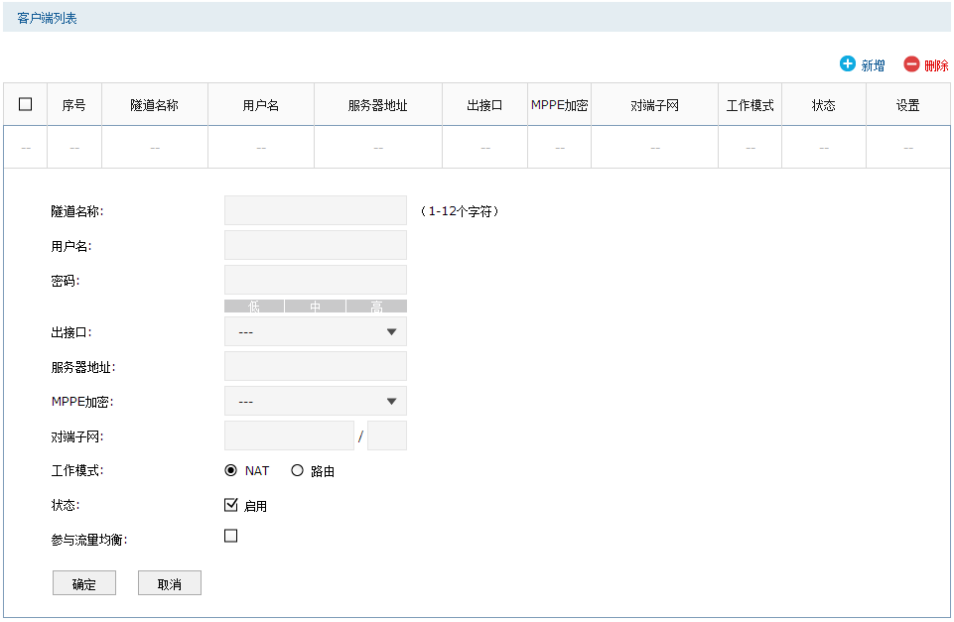


图 9-13 PPTP客户端列表

隧道设置

隧道名称	设置隧道名称。
用户名	设置PPTP认证时客户端使用的用户名。客户端与服务器的设置需保持一致。
密码	设置PPTP认证时客户端使用的密码。客户端与服务器的设置需保持一致。
服务器地址	设置对端服务器地址。
出接口	服务器端路由器WAN端口上出链路接口。如有多条上网链路，请根据实际情况，选择其中一条链路承载PPTP VPN隧道。
MPPE加密	选择是否使用MPPE对PPTP隧道加密。
对端子网	设置PPTP隧道对端局域网所使用的IP地址范围（一般可以填VPN隧道对端设备的LAN口IP地址范围），由IP和子网掩码组成。
工作模式	选择NAT模式或路由模式。
状态	选择启用或禁用本PPTP隧道。
参与流量均衡	选择是否参与流量均衡。

表 9.10　PPTP客户端设置-隧道设置界面项说明

9.3.3　PPTP服务器隧道信息

在此将列出路由器上所有PPTP隧道的相关信息。

进入界面：VPN >> PPTP >> 隧道信息列表

图 9-14　PPTP隧道信息界面

9.4　VPN 用户管理

当路由器作为L2TP服务器或PPTP服务器时，需创建用户账号。

进入界面：VPN >>用户管理

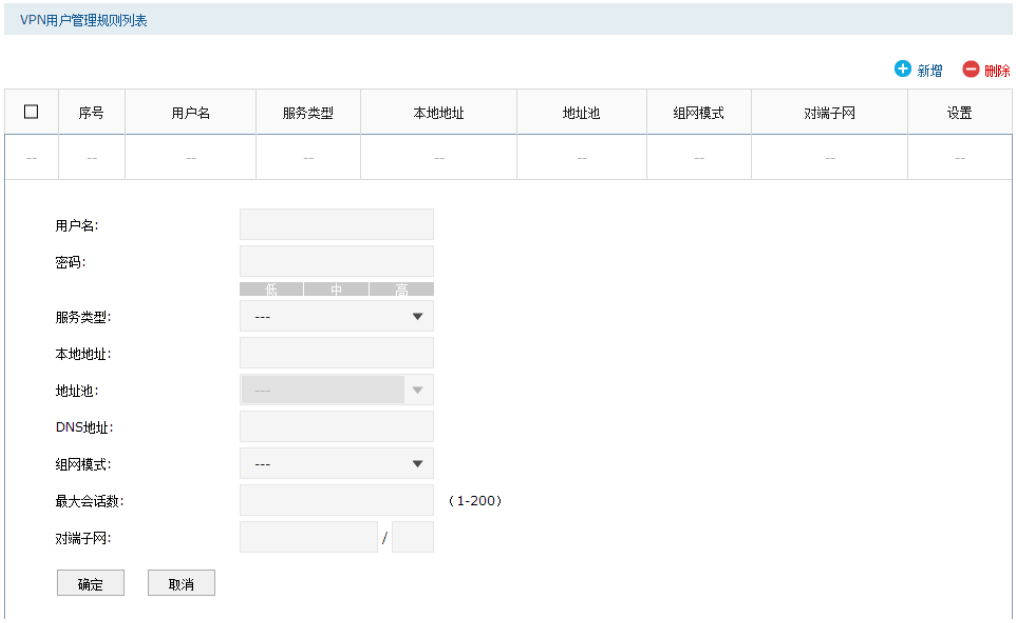


图 9-15 PPTP服务器列表

点击<新增>，进行账号设置。

用户名	设置认证时客户端使用的用户名。客户端与服务器的设置需保持一致。
密码	设置认证时客户端使用的密码。客户端与服务器的设置需保持一致。
服务类型	可选择L2TP，PPTP或自动。若选择自动，则该账号可根据客户端的配置自动适配相应的服务类型。
本地地址	设置隧道中本端使用的IP地址。
地址池	服务器分配给客户端的地址范围，由地址池名称所对应的IP 地址范围确定。
DNS地址	设置提供给客户端的DNS服务器的地址。如果需要客户端使用特定的DNS服务器，请进行设置。可以填入0.0.0.0表示任意地址。
组网模式	当远程接入用户为接入路由器的一个网段时，请选择“站点到站点”模式； 当远程接入用户是单个计算机时，请选择“PC到站点”模式。
最大会话数	选择启用或禁用本PPTP隧道。

对端子网	当组网模式选择“站点到站点”时，设置L2TP隧道对端局域网所使用的IP地址范围（一般可以填VPN隧道对端设备的LAN口IP地址范围），由IP和子网掩码组成。

表 9.11　VPN用户管理界面项说明

第10章 认证管理

网络管理员可以预先对网络资源进行划分：一部分直接提供给接入网络的用户使用；一部分需要用户进行认证后才可以使用，并且可以根据需求对访问网络资源的用户进行不同认证。

路由器提供 Web 认证和微信连 Wi-Fi 功能。Web 认证可以保证网络安全，并推送 Web 广告；微信连 Wi-Fi 可以推广微信公众号，并推送 Web 广告。

Web 认证和微信连 Wi-Fi 在指定接口生效。同一接口可以同时启用 Web 认证和微信连 Wi-Fi，此时用户进行何种认证说明如下：

3) 当用户访问外网时，将被重定向到 Web 认证页面（Web 认证优先级高于微信连 Wi-Fi）。

4) 若用户直接访问 Web 认证页面（/wportal/webauth），则进行 Web 认证。

10.1 Web 认证介绍

10.1.1 简介

路由器提供 Web 认证功能，在采用 Web 认证的网络中，用户需要先登录认证页面，输入用户名和密码进行认证，认证成功后才可以访问网络资源。

用户主动访问已知的 Web 认证网站，这种开始 Web 认证的方式称作主动认证。反之，如果用户试图通过 HTTP 访问其他网站，将被强制访问 Web 认证网站，从而开始 Web 认证过程，这种方式称作强制认证。

10.1.2 Web 认证系统

Web 认证系统一般网络拓扑如下图所示：

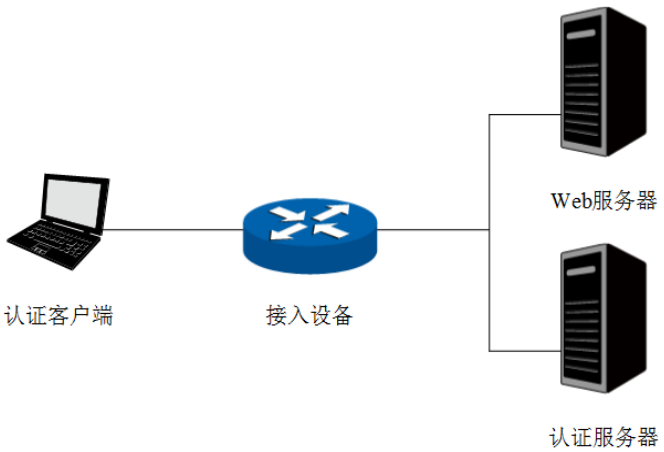


图 10-1 Web认证系统拓扑图

认证客户端

需要访问网络资源的用户，将进行 Web 认证。

接入设备

宽带接入设备的统称，包括路由器、交换机和无线控制器等。主要作用有：

- 认证前，将用户的所有 HTTP 请求都重定向到 Web 服务器；
- 认证过程中，与认证服务器交互，完成用户的身份认证；
- 认证通过后，允许用户访问被管理员授权的网络资源。

Web 服务器

接收认证客户端的 Web 认证请求，提供基于 Web 认证的页面。Web 服务器可以是接入设备之外的独立实体，也可以是存在于接入设备之内的内嵌实体。

认证服务器

与接入设备进行交互，完成对用户的认证。认证服务器可以是接入设备之外的独立实体，也可以是存在于接入设备之内的内嵌实体。

10.1.3 Web 认证过程

TL-ER7520G Web 认证过程如下图所示：

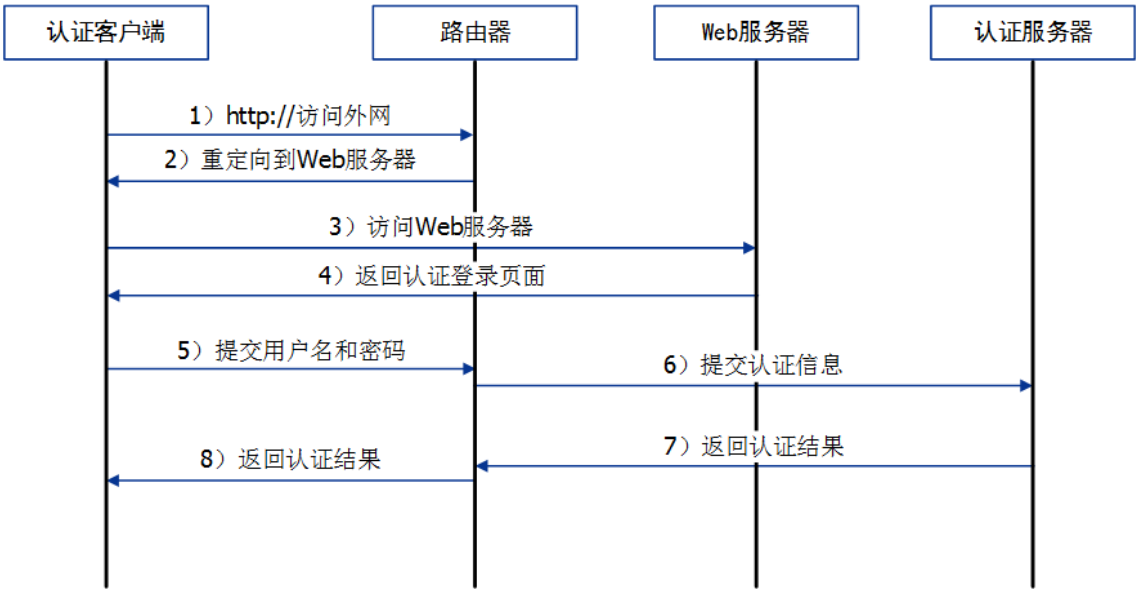


图 10-2 Web认证过程示意图

1) 认证客户端接入网络，未进行过 Web 认证，通过 HTTP 访问外网；

2) 路由器返回重定向 URL，将认证客户端重定向到 Web 服务器；

3) 认证客户端访问 Web 服务器；

4) Web 服务器为认证客户端返回认证登录页面；

5) 认证客户端在认证登录页面输入用户名和密码，该信息将提交到路由器；

6) 路由器向认证服务器提交该用户的认证信息；

7) 认证服务器向路由器返回认证结果；

8) 路由器向认证客户端返回该认证结果。

10.2 Web 认证配置

进入界面：认证管理 >> 认证设置 >> Web 认证

图 10-3 Web认证界面

在此界面**启用 Web 认证**，选择**生效接口**，可以针对指定接口设置 Web 认证。配置 Web 认证必须配置以下两种服务器：**Web 服务器**和**认证服务器**。

1 配置 Web 服务器

TL-ER7520G 内置有 Web 服务器，也支持外部配置的 Web 服务器。该配置对应**认证页面**设置项，认证页面有两个选项：自定义页面和外部链接。

- 自定义页面：使用 TL-ER7520G 内置的 Web 服务器，在路由器上设置认证登录页面。
- 外部链接：使用外部配置的 Web 服务器，在外部 Web 服务器上设置认证登录页面。

2 配置认证服务器

TL-ER7520G 内置有本地认证服务器，也支持 radius 协议类型的外部认证服务器。该配置对应**认证方式**设置项，认证方式有三个选项：本地认证、radius 认证和一键上网。

- 本地认证：使用 TL-ER7520G 内置的本地认证服务器，可以通过**用户管理**功能设置本地认证用户信息。
- radius 认证：使用外部配置的 radius 认证服务器，在 radius 认证服务器上设置认证用户信息。
- 一键上网：提供一键上网服务，无需进行用户名、密码认证，在认证页面点击<一键上网>按键即可上网。

根据实际应用环境和需求，可以灵活搭配认证页面和认证方式选项，本文档选取一键上网，使用内置的 Web 服务器和认证服务器，及**使用外部链接的 Web 服务器和认证服务器**三种搭配应用介绍其配置方法。

应用名称	认证页面选项	认证方式选项	特点
一键上网	自定义页面	一键上网	使用路由器内置的 Web 服务器和认证服务器，网络设备需求少。无需进行用户名、密码认证，用户上网方便。
使用内置的 Web 服务器和认证服务器	自定义页面	本地认证	使用路由器内置的 Web 服务器和认证服务器，网络设备需求少。进行用户名、密码认证，提供两种认证用户类型。
使用外部链接的 Web 服务器和认证服务器	外部链接	radius 认证	**使用外部链接的 Web 服务器和认证服务器，网络设备需求较多。**进行用户名、密码认证，可以自由设计认证登录页面，设置 radius 认证用户类型。

表 10.1　本文档Web认证应用选项搭配说明

10.2.1 一键上网

应用场景

某酒店为顾客提供免费上网服务，并希望通过 Web 认证页面推送酒店宣传广告。可使用路由器 Web 认证一键上网功能实现需求。为减少网络设备，可使用路由器内置的 Web 服务器提供认证页面。

网络拓扑

酒店网络拓扑如下图所示：

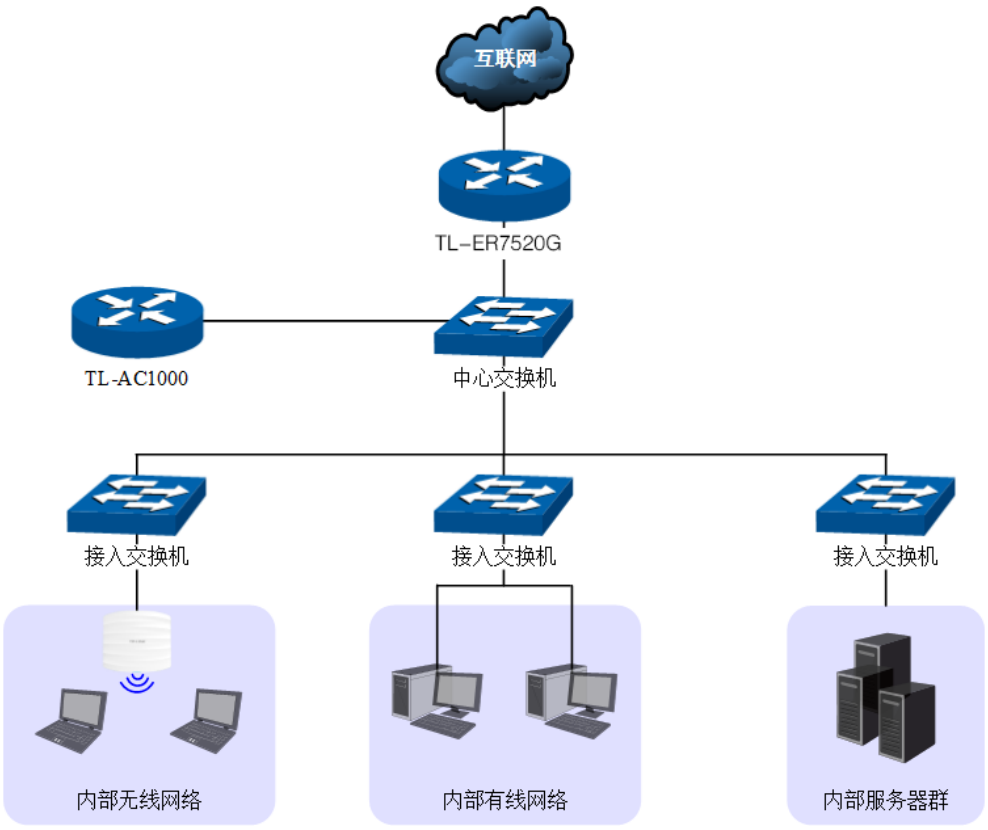


图 10-4 一键上网应用拓扑图

配置方法

1 在路由器上设置 Web 认证

进入界面：认证管理 >> 认证设置 >> Web 认证

点击<新增>按钮，进入 Web 认证设置页面。可参考如下所示参数设置。

图 10-5 一键上网应用设置界面

规则名称	输入该Web认证名称。只能输入英文、数字和下划线。
生效接口	选择Web认证功能生效的接口。
认证页面	选择自定义页面。
背景图片	上传Web认证页面的背景图片。支持图片格式：jpg，gif，bmp，jpeg，png。图片大小不能超过200KB。
欢迎信息	设置Web认证页面的欢迎信息。
版权声明	设置Web认证页面的版权声明信息。
页面预览	点击按键可预览登录页面。
认证方式	选择一键上网。
免费上网时长	设置用户免费上网的时长，默认为60分钟。
状态	勾选“启用”，开启Web认证。

表 10.2 一键上网应用设置界面项说明

设置完成后，点击<预览登录页面>按键，可以预览自定义的 Web 认证登录页面，如下图所示。

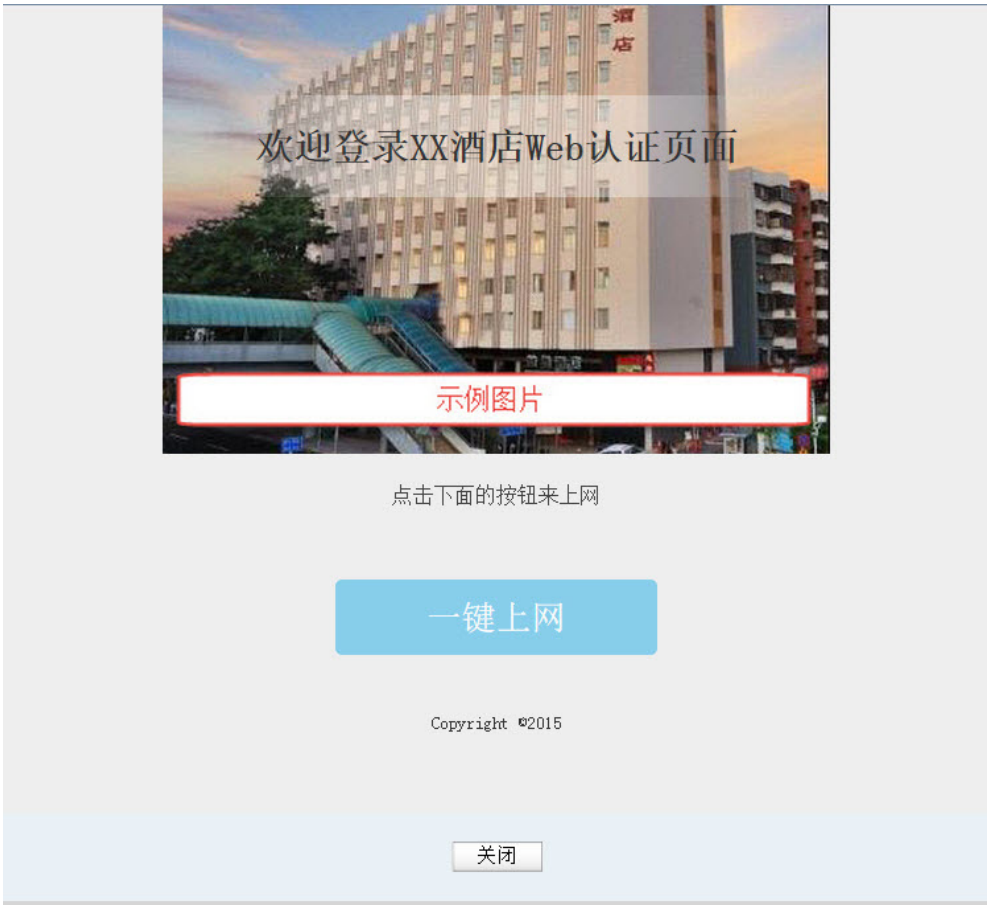


图 10-6　预览一键上网Web认证登录页面

2　用户上网步骤

说明：

- 以无线客户端为例介绍用户上网步骤，假设酒店 SSID 为：xxjiudian。
- 不同厂商设备的操作界面可能有所不同，本手册仅以下文所述情况示意。

1) 使用 Wi-Fi 连接 SSID 为“xxjiudian”的无线网络，系统跳转到认证页面，如下图所示。点击<一键上网>按键进行认证。

图 10-7 一键上网认证页面

2) 登录成功后显示下图。若无需上网，可点击<下线>按键释放上网权限。

图 10-8 一键上网用户登录成功页面

3) 免费上网时长到期后，再访问网站时，将自动跳转到认证页面，点击<一键上网>按键即可再次上网。

10.2.2 使用内置的 Web 服务器和认证服务器

应用场景

某酒店组建局域网，需要对接入网络的用户进行 Web 认证，在认证页面推送酒店宣传广告。可使用路由器内置的 Web 服务器和认证服务器设置 Web 认证功能实现需求。

网络拓扑

酒店网络拓扑如下图所示：

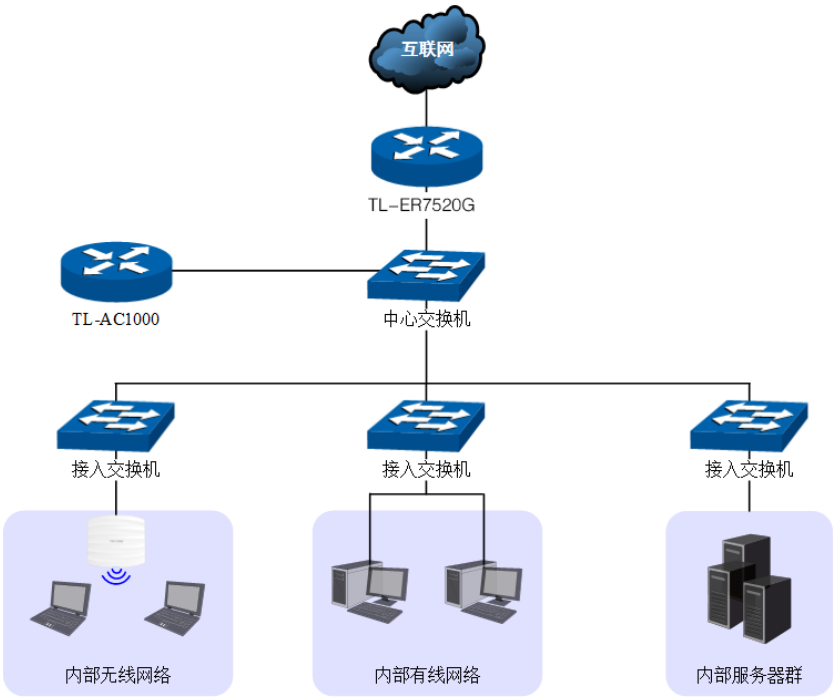


图 10-9　使用内置的Web服务器和认证服务器应用拓扑图

配置方法

3　在路由器上设置 Web 认证

1)　通过**用户管理**功能设置本地认证用户信息。进入界面：认证管理 >> 用户管理 >> 本地用户。点击<新增>按钮，。可以新增认证用户。**用户类型**分为正式用户和免费用户。

图 10-10　用户管理

- 正式用户：给用户提供连续自然天的上网服务，当账户有效期到期后，该账户无效。

图 10-11　用户管理-用户新增-正式用户界面

用户类型	选择“正式用户”。
用户名	自定义的用户名，不能与已有用户名重复。只能输入英文、数字和下划线。
密码	新增用户时，需要输入密码。 修改用户配置时，可以输入新密码，不输入则表示不修改。
有效期至	设置账户有效的截止日期。
允许认证时间段	允许使用该用户名进行认证的时间段。
MAC地址绑定方式	设置MAC绑定方式，有三种方式可供选择：不绑定、动态绑定和静态绑定。 不绑定：不绑定认证客户端MAC地址。 静态绑定：手动输入认证客户端MAC地址，绑定对应用户名。 动态绑定：系统自动绑定第一个使用该用户名认证成功的客户端MAC地址。
同时登录用户数	仅当“MAC地址绑定方式”为“不绑定”时，可设。 允许同时使用该用户名认证的客户端最大数目。
上行带宽	分配给该用户使用的最大上行带宽。
下行带宽	分配给该用户使用的最大下行带宽。
姓名	设置客户姓名备注。

电话	设置客户电话备注。
备注	设置条目的备注，以方便管理和查找。
状态	勾选“启用”，则该条目生效； 不勾选“启用”，则该条目部生效；

表 10.3 用户管理-用户新增-正式用户界面项说明

- 免费用户：给用户提供以“分钟”为时间单位的短时间上网服务，该账户可重复使用，用户免费上网时长到期后，使用该账户重新认证，即可再次上网。

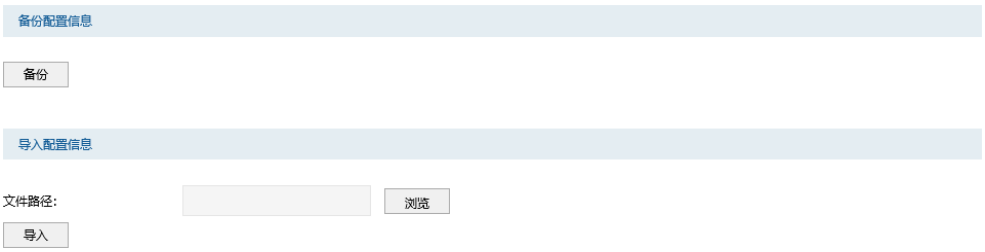
图 10-12 用户管理-用户新增-免费用户界面

用户类型	选择“免费用户”。
用户名	自定义的用户名，不能与已有用户名重复。只能输入英文、数字和下划线。
密码	新增用户时，需要输入密码。 修改用户配置时，可以输入新密码，不输入则表示不修改。
上网时长（分钟）	设置免费账户有效时间。
允许认证时间段	允许使用该用户名进行认证的时间段。
同时登录用户数	允许同时使用该用户名认证的客户端最大数目。
上行带宽	分配给该用户使用的最大上行带宽。
下行带宽	分配给该用户使用的最大下行带宽。
备注	设置条目的备注，以方便管理和查找。

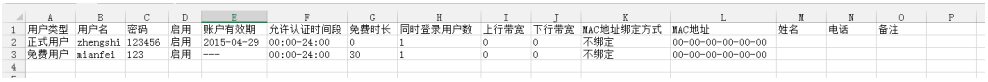
状态	勾选“启用”，则该条目生效； 不勾选“启用”，则该条目部生效；

表 10.4 用户管理-用户新增-免费用户界面项说明

进入界面：认证管理 >>用户管理>>用户配置备份。



点击<备份>按键，可以备份路由器中存储的用户信息，备份文件为 ANSI 编码格式的 CSV 文件。也可以导入 ANSI 编码格式的 CSV 文件到路由器中。CSV 文件内容格式参考如下（可以通过“备份”一份有用户信息的文件参考）：



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	用户类型	用户名	密码	启用	账户有效期	允许认证时间段	免费时长	同时登录用户数	上行带宽	下行带宽	MAC地址绑定方式	MAC地址	姓名	电话	备注	
2	正式用户	zhengshi	123456	启用	2015-04-29	00:00-24:00	0	1	0	0	不绑定	00-00-00-00-00-00				
3	免费用户	mianfei	123	启用	---	00:00-24:00	30	1	0	0	不绑定	00-00-00-00-00-00				
4																

图 10-13 csv格式文件存储用户信息示意图

A	用户类型
B	用户名
C	密码
D	启用/禁用状态
E	账户有效期。仅正式用户可设，格式：xxxx-xx-xx；免费用户为“---”。
F	允许认证时间段
G	免费时长。仅免费用户可设，正式用户为“0”。
H	同时登录用户数
I	上行带宽
J	下行带宽
K	MAC地址绑定方式。仅正式用户可设，免费用户为“不绑定”。
L	MAC地址
M	姓名
N	电话
O	备注

表 10.5 csv格式文件存储用户信息说明

说明：

导入的CSV文件内容必须按照上面顺序编排各项，且确保每一项的格式正确。

2) 设置 Web 认证。进入界面：认证管理 >> 认证设置 >> Web 认证，可参考如下所示参数设置。

图 10-14 使用内置的Web服务器和认证服务器应用界面

规则名称	输入Web认证名称。只能输入英文、数字和下划线。
生效接口	选择Web认证功能生效的接口。
认证页面	选择自定义页面。
背景图片	上传Web认证页面的背景图片。支持图片格式：jpg，gif，bmp，jpeg，png。图片大小不能超过200KB。
欢迎信息	设置Web认证页面的欢迎信息。
版权声明	设置Web认证页面的版权声明信息。
页面预览	点击<预览登录页面>按键，可以预览自定义的Web认证登录页面。
认证方式	选择本地认证。
到期提醒	本地认证方式时，可以设置在用户即将到期时提醒用户。
开始提醒时间	设置开始提醒时间。

提醒方式	路由器提供两种提醒方式：仅认证时提醒和周期提醒。当选择周期提醒时，可以设置周期时间，单位为分钟。
提醒页面内容	设置提醒页面的内容。
页面预览	预览用于提醒用户到期的页面。
状态	勾选“启用”，则该条目生效。 不勾选“启用”，则该条目不生效。

表 10.6 使用内置的Web服务器和认证服务器应用界面项说明

设置完成后，点击<预览登录页面>按键，可以预览自定义的 Web 认证登录页面，如图 10-17 所示。点击<预览到期提醒页面>按键，可以预览自定义的正式用户到期提醒页面，如图 10-18 所示。

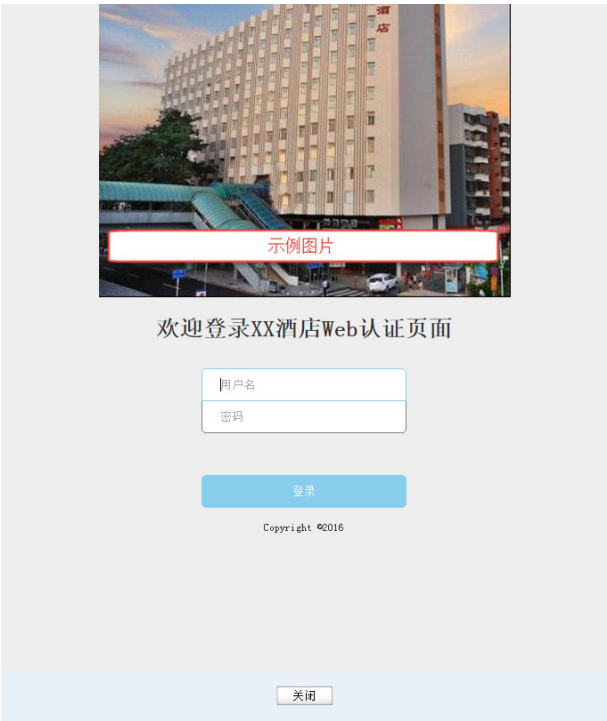


图 10-15 预览Web认证登录页面

图 10-16 预览到期提醒页面

4 用户上网步骤

说明：

- 以无线客户端为例介绍用户上网步骤，假设酒店 SSID 为：xxjiudian。
- 不同厂商设备的操作界面可能有所不同，本手册仅以下文所述情况示意。

1) 使用 Wi-Fi 连接 SSID 为“xxjiudian”的无线网络。，系统跳转到认证页面，如下图所示。输入酒店分配的用户名和密码，点击<登录>按键进行认证。

图 10-17认证登录页面

2) 若为正式用户，使用的账号若即将到期，认证成功后，将跳转到账号到期提醒页面（提醒方式设置不同，提醒页面弹出时机会不同），如下图所示。账户有效期到期后，如需继续上网，请联系酒店工作人员。

图 10-18 正式用户认证到期提醒页面

若为免费用户，登录成功后显示下图。若无需上网，可点击<下线>按键释放上网权限。免费上网时长到期后，再访问网站时，将自动跳转到认证页面，重新认证后，即可再次上网。

图 10-19 免费用户登录成功页面

10.2.3 使用外部链接的 Web 服务器和认证服务器

应用场景

某酒店组建局域网，需要对接入网络的用户进行 Web 认证，酒店搭建了外部 Web 服务器和 radius 认证服务器。可通过路由器设置 Web 认证功能实现需求。

网络拓扑

酒店网络拓扑如下图所示：

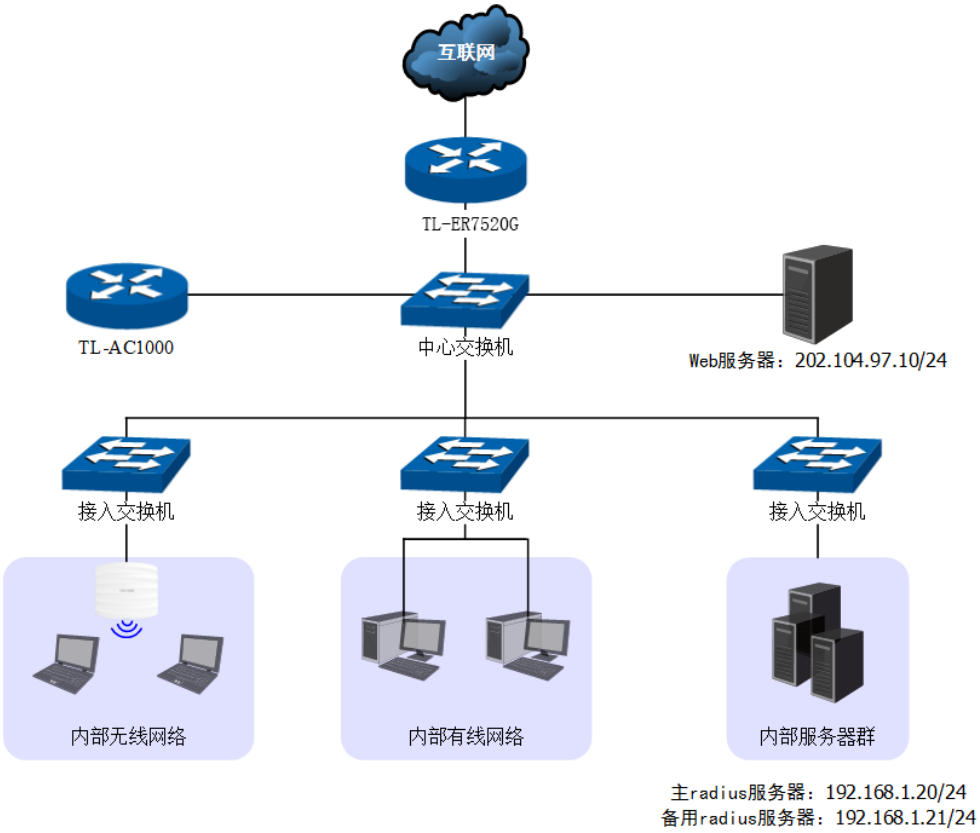


图 10-20 使用外部链接的Web服务器和认证服务器应用拓扑图

准备工作

在设置 Web 认证功能之前，需要做如下准备工作：

3) 设置主/备用 radius 服务器

说明：

如果在radius认证服务器上不设置上网时长，则上网时长将设置为默认值30分钟。

4) 设置外部 Web 服务器

外部 Web 服务器需要提供认证登录页面，为确保认证客户端能够正确提交用户名和密码，该页面必须按下面的要求完成：

- 认证登录页面 Form 的 action 必须设为：http://tplogin.cn:8080/portal/auth；
- 认证登录页面以 Get 方式提交 Form 表单；
- 认证登录页面必须包含“username”和“password”参数。

认证登录页面 Form 示例如下：

```
<form method="get" action = 'http://tplogin.cn:8080/portal/auth'>
                <input type="text"    name="username"/>
                <input type="password"    name="password"/>
                <input type="submit"    value="登录"/>
</form>
```

网络参数

假设网络参数设置如下：

名称	相关网络参数
主 radius 服务器	IP 地址：192.168.1.20/24 共享密钥：123456789 认证方式：MSCHAP
备用 radius 服务器	IP 地址：192.168.1.21/24 共享密钥：123456789 认证方式：MSCHAP
Web 服务器	IP 地址：202.104.97.10/24
认证成功后跳转页面	http://www.jiudian.com
认证失败后跳转页面	http://www.failed.com

表 10.7 网络参数模拟

配置步骤

5　在路由器上设置 Web 认证

5)　设置 Web 认证。进入界面：认证管理 >> 认证设置 >> Web 认证，可参考如下所示参数设置。

图 10-21　使用外部链接的Web服务器和认证服务器应用界面

规则名称	输入Web认证名称。只能输入英文、数字和下划线。
生效接口	选择Web认证功能生效的接口。
认证页面	选择外部链接。
认证URL	设置重定向到Web认证页面的URL，该URL由外部Web服务器提供。
认证成功后跳转链接	设置用户认证成功后自动跳转的目的网站地址。
认证失败后跳转链接	设置用户认证失败后自动跳转的目的网站地址。
认证方式	选择radius认证。
主/备用服务器地址	设置主radius服务器和备用radius服务器，支持IP地址和域名。主服务器在认证过程中将优先被使用。当主服务器发生故障时，自动启用备用服务器。
认证端口	设置服务器监听的端口。
授权共享密钥	输入服务器上配置的共享密钥。

失败发送次数	当客户端发送请求后，如果在超时时间过后没有收到回复，重复发送请求的次数。
超时时间	设置服务器应答超时时间，超过该时长，客户端将会重复发送请求。
认证方式	选择使用的认证方式，有PAP和CHAP两种方式供选择。
状态	勾选“启用”，则该条目生效； 不勾选“启用”，则该条目部生效；

表 10.8 使用外部链接的Web服务器和认证服务器应用界面项说明

使用外部 Web 服务器时，路由器根据认证结果向认证客户端返回重定向链接原则如下：

- 认证成功
  - 未设置“认证成功后跳转链接”，重定向至本地默认登录成功页面。
  - 设置“认证成功后跳转链接”，重定向至该链接。
- 认证失败
  - 未设置“认证失败后跳转链接”，重定向至外部 Web 服务器，并在 URL 中带有错误信息：error=错误码。
  - 设置“认证失败后跳转链接”，重定向至该链接，并在 URL 中带有错误信息：error=错误码。

错误码说明如下：

InternalError	内部错误
ErrorUserOrPassword	用户名或者密码错误
Timeout	登录超时
UserForbidden	该用户被禁用
UserOutOfDate	该用户已过期
UserReachedMax	该用户认证用户已达上限
InvalidTimePeriod	该时间段禁止认证
MacForbidden	该用户绑定的MAC地址跟认证客户端不匹配

表 10.9 错误码说明表

6) 当外部 Web 服务器的 IP 地址为公网 IP 地址时，需要设置外部 Web 服务器的免认证策略，确保认证客户端在 Web 认证成功前能够访问外部 Web 服务器。进入界面：认证管理 >> 认证设置 >> 免认证策略，可参考如下所示参数设置。免认证策略详细介绍请参考 1.3 免认证策略。

10.3 微信连 Wi-Fi

路由器提供微信连 Wi-Fi 功能，商家可以根据需求对访问网络资源的用户进行认证，通过微信连 Wi-Fi 推广微信公众号并推送广告。

应用场景

某酒店组建无线局域网，需要对接入网络的用户进行微信连 Wi-Fi 认证，在认证页面推送酒店宣传图片，同时利用用户关注的微信公众号实现二次营销需求。可使用路由器微信连 Wi-Fi 功能实现需求。

网络拓扑

酒店网络拓扑如下图所示：

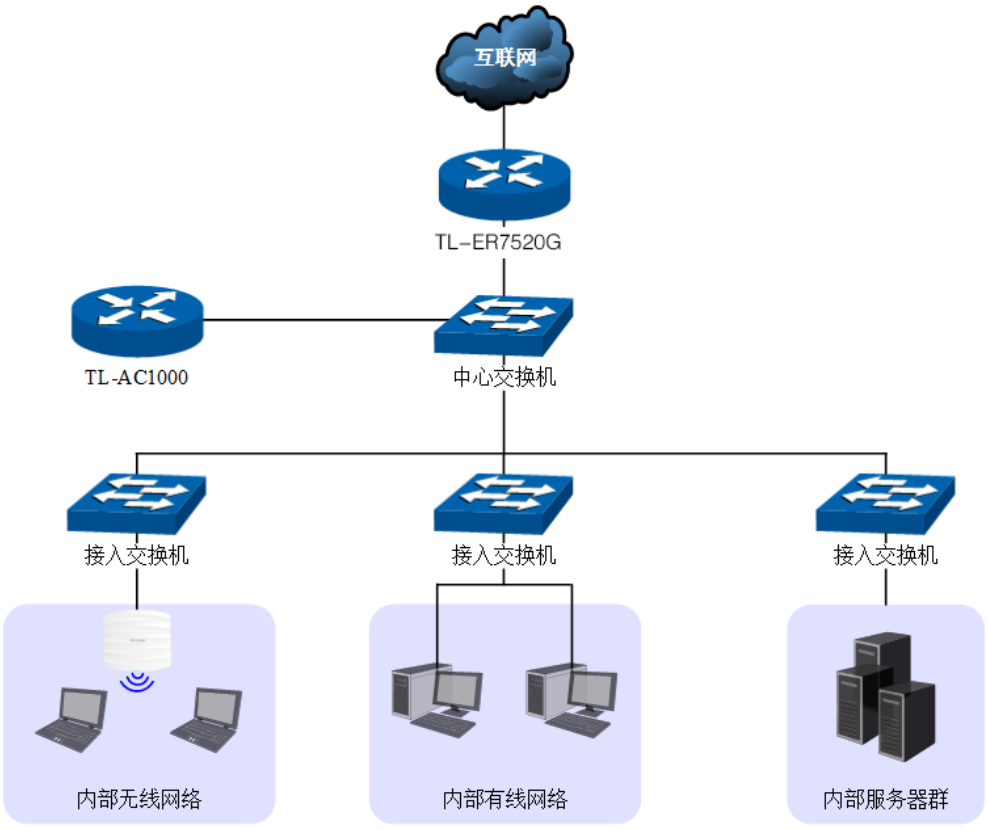


图 10-22 微信连Wi-Fi应用拓扑图

配置方法

1 微信公众号平台后台设置

酒店需要有微信公众号，以订阅号为例，微信后台设置如下：

1) 添加微信连 Wi-Fi 功能，如下图所示，点击<添加功能插件>后在插件库添加“微信连Wi-Fi”功能。

图 10-23 添加微信连Wi-Fi功能

2) 新建门店，如下图所示，在门店管理功能界面可以新建门店。

图 10-24 新建门店

3) 在微信连 Wi-Fi 功能界面添加设备，如下图所示。

图 10–25 添加设备1

4) 添加设备后会生成如下信息，这些信息在路由器上设置微信连 Wi-Fi 功能时会用到。

图 10-26 添加设备 2

2 在路由器上设置微信连 Wi-Fi

设置界面：认证管理 >> 认证设置 >> 微信连 Wi-Fi。可参考如下所示参数设置。

图 10-27 微信连Wi-Fi应用界面

功能设置

规则名称	输入规则名称。只能输入英文、数字和下划线。
生效接口	选择生效接口，该接口为连接了AP或无线路由器的物理接口。可以针对指定接口设置微信连Wi-Fi功能。

状态	勾选此项以启用微信连Wi-Fi功能。

表 1.11 规则参数说明

微信公众平台参数设置

SSID	输入无线网络设备的SSID。
ShopID	输入在微信公众平台获取的门店ID。
AppID	输入在微信公众平台获取的酒店微信公众平台账号。
SecretKey	输入酒店微信公众平台账号的密钥。
微信连Wi-Fi设置说明	通过该链接您可以看到更详细的设置教程。您需要连接互联网才能查看该教程。

表 1.12 微信公众平台参数说明

免费上网时长设置

免费上网时长	设置微信连Wi-Fi成功后，用户免费上网的时长。
状态	勾选“启用”，使该规则生效。

表 1.13 免费上网时长设置条目

认证页面设置

背景图片	设置微信认证页面的背景图片。点击<上传>按钮来设置您的自定义背景图片。如不上传，则会使用设备自带的默认背景图片。
Logo图片	设置微信认证页面的Logo图片。点击<上传>按钮来设置您的自定义Logo图片。点击<删除>按钮将不使用Logo图片。
Logo信息	设置微信认证页面的Logo信息。Logo信息位于Logo图片的正下方。可以输入1-25个字符。
欢迎信息	设置微信认证页面的欢迎信息。欢迎信息位于登录按钮的上方。可以输入1-50个字符。
登录按钮提示文字	设置微信认证页面的登录按钮提示文字。可以输入1-15个字符。
版权声明	设置微信认证页面的版权声明。版权声明位于认证页面底部。可以输入1-25个字符。
页面预览	通过点击<预览Portal页面>按钮可以预览设置后的微信认证页面效果。

表 1.12 微信公众平台参数说明

3 用户上网步骤

说明：

- 以无线客户端为例介绍用户上网步骤，假设酒店 SSID 为：1024。
- 不同厂商设备的操作界面可能有所不同，本手册仅以下文所述情况示意。

1) 使用 Wi-Fi 连接 SSID 为“1024”的无线网络，系统跳转到认证页面，如下图所示。

图 10-28 跳转到认证页面

2) 点击<登录>，进入微信连 Wi-Fi 页面，如下图所示。

图 10–29 微信连Wi–Fi页面

3) 点击<立即连接>，可连接 Wi-Fi，如下图所示。

图 10–30 Wi–Fi连接成功页面

4) Wi-Fi 连接成功后，即可上网，点击<完成>，将进入微信页面，如下图所示。

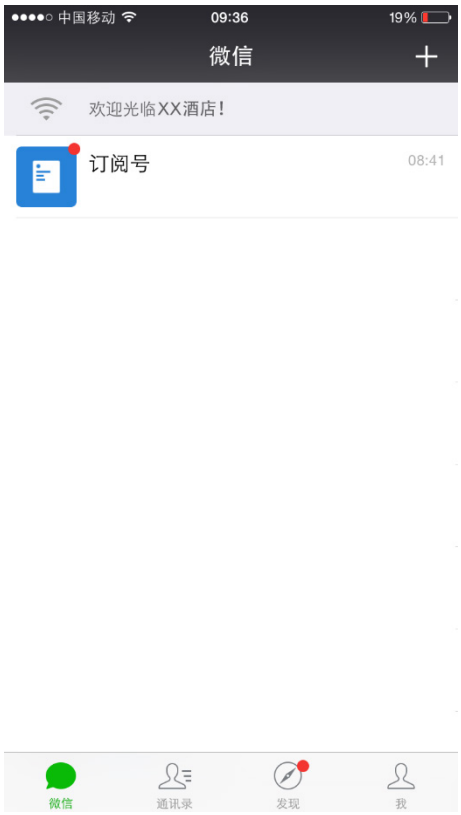


图 10–31 微信页面

10.4 免认证策略

可以通过本界面设置和查看免认证策略。免认证策略可配置用户在认证成功前能够免费访问的资源。

进入界面：认证管理 >>认证设置 >> 免认证策略

图 10-32 免认证策略界面

免认证策略设置

路由器支持两种**免认证方式**：五元组方式和 URL 方式。

- 五元组方式：主要依据 IP 地址范围、MAC 地址、端口和服务协议设置策略，当需要限制的免认证参数种类较多时，推荐使用五元组方式。

图 10-33 免认证策略-免认证策略设置-五元组方式界面

策略名称	设置免认证策略的名称。只能输入英文、数字和下划线。
免认证方式	选择五元组方式。
源IP地址范围	设置免认证策略的源IP地址和网络掩码。
目的IP地址范围	设置免认证策略的目的IP地址和网络掩码。
源MAC地址	设置免认证策略的源MAC地址。
源端口范围	设置免认证策略的源端口范围。
目的端口范围	设置免认证策略的目的端口范围。
服务协议	设置免认证策略的服务协议。
生效接口	选择生效接口，可以针对指定接口设置免认证策略。
备注	设置条目的备注，以方便管理和查找。
状态	勾选“启用”，则使该策略生效； 不勾选“启用”，则该策略无效。

表 10.10 免认证策略-免认证策略设置-五元组方式界面项说明

- URL 方式：主要依据 URL 设置策略，当已知 URL 时，推荐使用 URL 方式。

图 10-34 免认证策略-免认证策略设置-URL方式界面

策略名称	设置免认证策略的名称。只能输入英文、数字和下划线。
免认证方式	选择URL方式。
URL地址	设置免认证策略的URL地址。

源IP地址范围	设置免认证策略的源IP地址和网络掩码。
源MAC地址	设置免认证策略的源MAC地址。
源端口范围	设置免认证策略的源端口范围。
目的端口范围	设置免认证策略的目的端口范围。
生效接口	选择生效接口，可以针对指定接口设置免认证策略。
备注	设置条目的备注，以方便管理和查找。
状态	勾选“启用”，则使该策略生效； 不勾选“启用”，则该策略无效。

表 10.11 免认证策略-免认证策略设置-URL方式界面项说明

新增的条目会在免认证策略列表里显示出来，如下图所示。

☐	序号	策略名称	免认证方式	源IP地址范围	目的IP地址范围	源端口	目的端口	生效区段	设置
☐	1	mianrenzheng	五元组方式	192.168.0.1/24	192.168.0.200/24	20-30	40-50	GE1	

图 10-35 免认证策略-免认证策略设置列表

如有需要，可以点击条目后的<>按钮进行编辑。

10.5 认证状态

在此界面可以查看认证成功的用户的信息。

进入界面：认证管理 >> 认证状态 >> 认证状态

图 10-36 认证状态界面

刷新	手动刷新认证用户列表。
下线	可实现批量断开用户连接。
认证方式	显示用户登录所使用的认证方式。
接入时间	显示用户接入网络时的时间。
IP地址	显示用户的IP地址。
设置	点击<>按键，可断开该用户的连接。

表 10.12 认证状态界面项说明

第11章 系统服务

11.1 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。TL-ER7520G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。

11.1.1 花生壳动态域名

进入界面：系统服务 >> 动态DNS >> 花生壳动态域名

图 11-1 花生壳动态域名登录界面

服务接口	选择登录花生壳动态域名服务器的接口。
用户名	填入在花生壳网站注册的用户名。若还没有注册，请点击右边的链接“注册用户名”登录花生壳网站进行注册。
密码	填入在花生壳网站注册该用户名时所设置的密码。
状态	勾选“启用”，则该条目生效； 不勾选“启用”，则该条目不生效。

表 11.1 花生壳动态域名登录界面项说明

11.1.2 科迈动态域名

进入界面：系统服务 >> 动态DNS >> 科迈动态域名

图 11-2 科迈动态域名登录界面

服务接口	选择登录科迈动态域名服务器的接口。
用户名	填入在科迈网站注册的用户名。若还没有注册，请点击右边的链接“注册用户名”登录科迈网站进行注册。
密码	填入在科迈网站注册该用户名时所设置的密码。
状态	勾选“启用”，则该条目生效； 不勾选“启用”，则该条目不生效。

表 11.2 3322动态域名登录界面项说明

11.1.3 3322 动态域名

进入界面：系统服务 >> 动态DNS >> 3322动态域名

图 11-3 3322动态域名登录界面

服务接口	选择登录3322动态域名服务器的接口。
用户名	填入在3322网站注册的用户名。若还没有注册，请点击右边的链接“注册用户名”登录3322网站进行注册。
密码	填入在3322网站注册该用户名时所设置的密码。
状态	勾选“启用”，则该条目生效； 不勾选“启用”，则该条目不生效。

表 11.3 3322动态域名登录界面项说明

11.2 DNS代理

可以通过本页面设置接口的DNS代理功能。

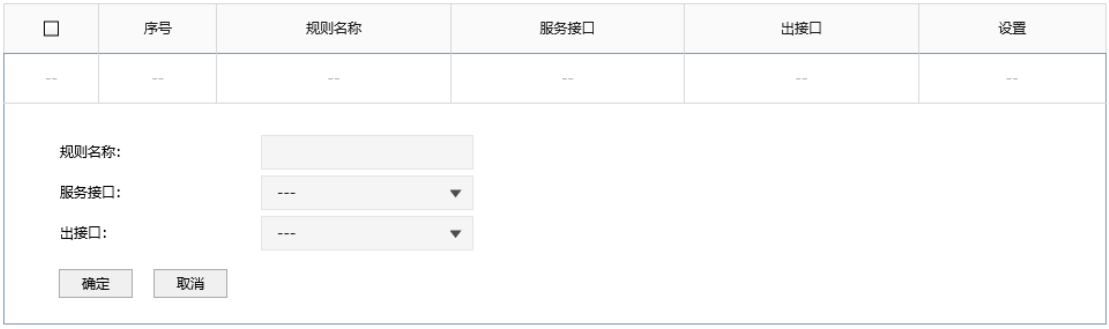


图 11-4 DNS代理设置界面

规则名称	输入规则名称。只能输入英文、数字和下划线。
服务接口	选择在哪些接口上面使用DNS代理功能。
出接口	指定转发的DNS请求报文发往哪一个接口上的DNS server，如果选择的是auto，路由器将提供一套默认规则来选择server（当指定出接口时，请确认该接口有配置DNS地址）。

表 11.4 DNS代理设置界面项说明

新增的条目会在**DNS代理规则列表**里显示出来，如下图所示。

图 11-5 DNS代理设置界面

11.3 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，而无需设置NAT相关转发规则，对于此类传输层协议端口不固定的应用会更加方便。

进入界面：系统服务 >> UPnP服务 >> UPnP服务

图 11-6 UPnP服务设置界面

服务接口	指定一组接口集，所设置的接口将会开放UPnP服务。
对外生效接口	指定一组接口集，该集合包含的接口将被配置以端口映射的功能。
启用/禁用服务	选择启用或禁用UPnP服务。

表 11.5 UPnP服务设置界面项说明

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-ER7520G可以同时支持64条UPnP服务，并对已有规则进行相应设置。

说明：

- 应用时不仅要在路由器上启用UPnP服务，还需要确认主机操作系统和应用程序也支持此服务，即Windows XP系统需安装UPnP组件；应用程序本身需支持UPnP，如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。

第12章　系统工具

12.1　管理账号

12.1.1 管理帐号

在此可以修改登录时使用的用户名和密码。

进入界面：系统工具 >> 管理账号 >> 修改管理帐户

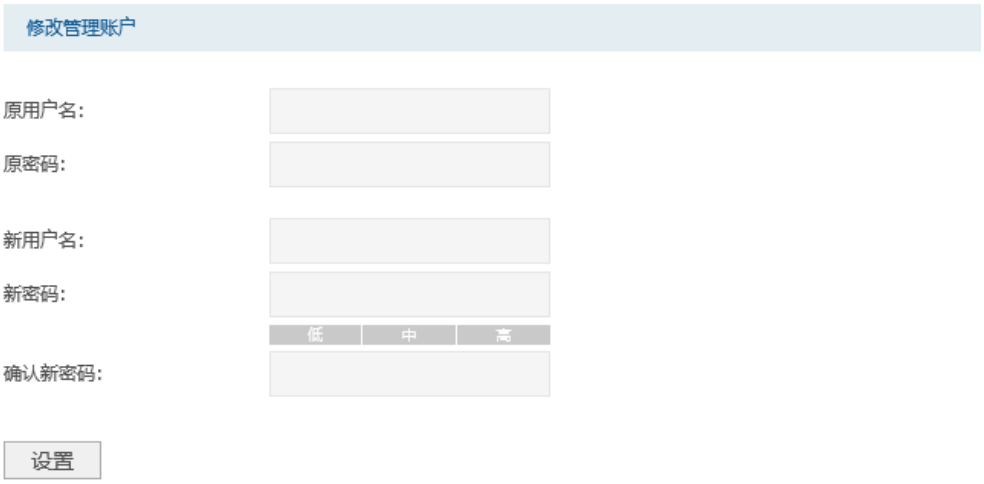


图 12-1　修改管理帐户界面

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。“低、中、高”表示密码的复杂程度。
确认新密码	再次输入新密码。

表 12.1　修改管理帐户

说明：

出厂的用户名和密码均为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50个字符，且只能是数字和字母，区分大小写。

12.1.2 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。

进入界面：系统工具 >> 管理账号 >> 远程管理

图 12-2 远程管理设置界面

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。

表 12.2 远程管理设置界面项说明

新增的条目会在**地址列表**里显示出来，如下图所示。

图 12-3 远程管理设置界面-地址列表

如有需要，可以点击条目后的<>按钮进行编辑，点击<>按钮启用条目，点击<>按钮禁用条目。

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。

12.1.3 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。

进入界面：系统工具 >> 管理账号 >> 系统管理设置

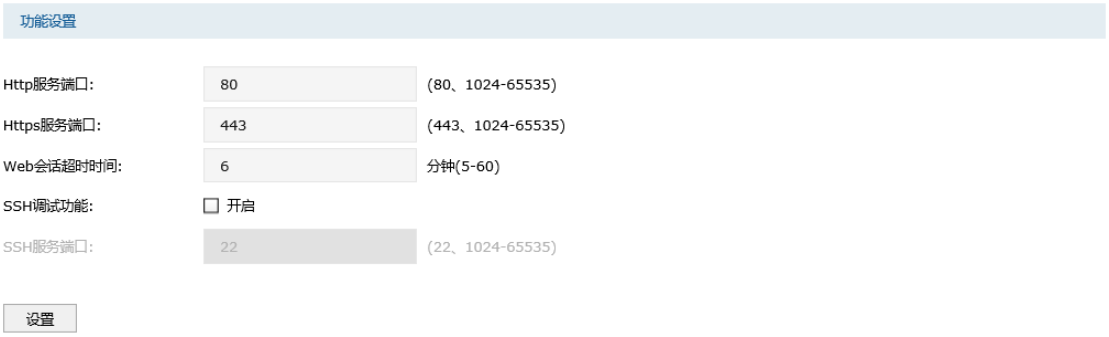


图 12-4 系统管理设置界面

Http服务端口	设置路由器的Http服务端口。
Https服务端口	设置路由器的Https服务端口。
Web会话超时时间	设置通过Web访问路由器的超时时间，Web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。 设置超时时间后，新的超时时间将在下一次登录时生效。
SSH调试功能	SSH调试功能的开关，开启后才能进行设置SSH端口号。
SSH服务端口	设置路由器的SSH服务端口。

表 12.3 系统管理设置界面项说明

说明：

一般情况下请不要开启SSH调试功能。如有需要，请您在联系技术支持后开启。

12.2 设备管理

12.2.1 恢复出厂配置

进入界面：系统工具 >> 设备管理 >> 恢复出厂配置

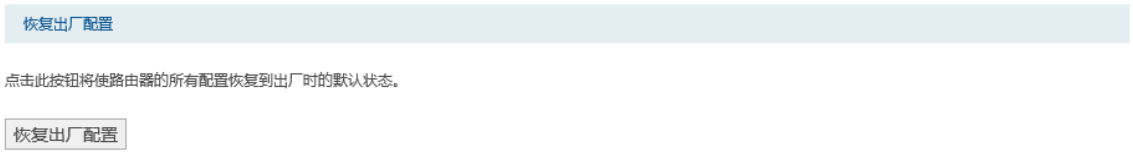


图 12-5 恢复出厂配置界面

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IP地址为192.168.1.1，用户名和密码均为admin。

12.2.2 备份与导入配置

进入界面：系统工具 >> 设备管理 >> 备份与导入配置

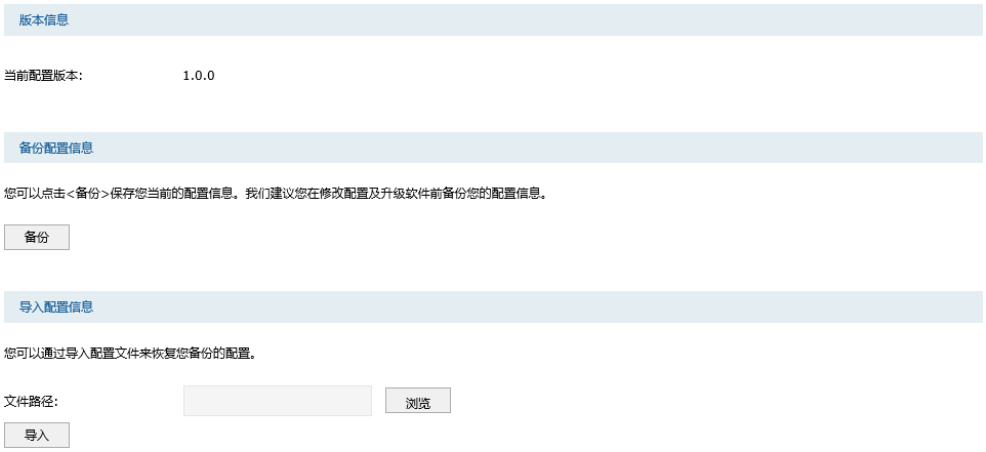


图 12-6 备份与导入配置界面

版本信息

显示当前路由器软件版本。

备份配置信息

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

导入配置信息

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

说明：

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

12.2.3 重启路由器

进入界面：系统工具 >> 设备管理 >> 重启路由器

图 12-7 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。

说明：

重启过程中请保持电源稳定，避免强行断电。

12.2.4 软件升级

进入界面：系统工具 >> 设备管理 >> 软件升级

图 12-8 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-ER7520G的软件升级文件，可将升级文件下载保存在本地。登录路由器后进入软件升级界面，单击<选择文件>按钮，选择保存路径下的升级文件，点击<升级>进行软件升级。

说明：

- 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。

12.3 流量统计

12.3.1 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。

进入界面：系统工具 >> 流量统计 >> 接口流量统计


流量统计列表

接口数量：10 刷新

接口	发送速率(KB/s)	接收速率(KB/s)	发送包速率(Pkt/s)	接收包速率(Pkt/s)	发送总字节	接收总字节	发送总报文	接收总报文
---	---	1	---	6	2M	50M	4958	291520
GE1	1	3	1	18	13M	1G	53867	2M
GE2	1	3	1	18	13M	1G	55643	2M
GE3	1	1	1	5	8M	41M	34719	252415
GE4	1	2	4	8	24M	68M	132525	393011

图 12-9 接口流量统计界面

发送/接收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。发送/接收包速率统计的是每秒发送/接收的数据包个数。发送/接收总字节数统计的则是所有数据包的总字节数。发送/接收总报文统计的是报文的总个数。

12.3.2 IP流量统计

IP流量统计界面将显示指定IP范围之间各个IP的即时流量信息

进入界面：系统工具 >> 流量统计 >> IP流量统计


功能设置

☑ 启用IP流量统计

监控IP范围： 192.168.1.0 / 255.255.255.0

设置

流量统计列表

IP数量：0 刷新

IP地址	发送速率(KB/s)	接收速率(KB/s)	发送包速率(Pkt/s)	接收包速率(Pkt/s)	发送总字节	接收总字节	发送总报文	接收总报文
--	--	--	--	--	--	--	--	--

如需要按指定内容排序，请点击表头切换排序方式

图 12-10 IP流量统计界面

勾选“启用IP流量统计”选项，相应的流量统计信息将显示在流量统计列表中。

12.4 诊断工具

12.4.1 诊断工具

进入界面：系统工具 >> 诊断工具 >> 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。

图 12-11 PING通信检测界面

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。
出接口	选择PING检测的出接口。
PING次数	设置PING次数，范围为1-50次，默认为4次。
PING数据包大小	设置PING数据包大小，范围为4-1472字节，默认为64字节。

表 12.4 PING通信检测

图 12-12 路由跟踪检测

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。
出接口	选择路由跟踪检测的出接口。
路由跟踪最大TTL	设置路由跟踪的最大TTL值，默认值为20。

表 12.5 路由跟踪检测

12.5 时间设置

12.5.1 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。

设置时间的方法分为两种：“通过网络获取系统时间”和“手动设置系统时间”。图 12-13是“通过网络获取系统时间”，图 12-14是“手动设置系统时间”。

进入界面：系统工具 >> 时间设置 >> 时间设置

若路由器可以访问网络，可以选择通过网络获取系统时间，设置完毕后点击<设置>生效。

图 12-13 通过网络获取系统时间

当前时间	显示目前系统时间。
设置时间	选择“通过网络获取系统时间”。
时区	选择时区。
首选/备选NTP服务器	选择“通过网络获取系统时间”后，路由器将在内置NTP（Network Time Protocol，网络校时协议）服务器地址列表中搜索可用地址，并获取时间。若获取失败，请手动设置NTP服务器地址，由于NTP服务器并非固定不变，推荐搜索两个不同的地址，分别填入首选、备用NTP服务器输入框，NTP服务器地址可以为IP地址也可以为域名。设置完毕后点击<设置>按钮，路由器会通过指定的NTP服务器获取网络时间。

表 12.6 时间设置界面项说明

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设置完毕后点击<设置>生效。

图 12-14 手动设置系统时间

当前时间	显示当前系统时间。
设置时间	选择“手动设置系统时间”。

日期	手动设置系统日期。
时间	手动设置系统时间。
获取管理主机时间	点击按钮可以获取当前主机的系统时间。

表 12.7 时间设置界面项说明

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，请手动设置系统时间。

12.6 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。

进入界面：系统工具 >> 系统日志 >> 系统日志

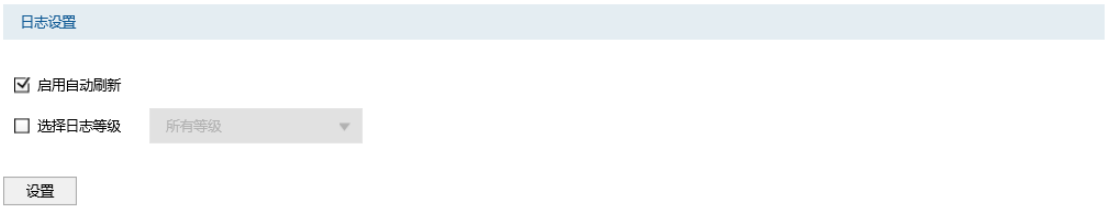


图 12-15 日志界面

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列出指定等级的日志记录。

各等级描述：

所有等级	日志列表中将列出所有等级的日志记录。
致命错误	导致系统不可用的错误，红色显示。
紧急错误	必须对其采取紧急措施的错误，红色显示。
严重错误	导致系统处于危险状态的错误，红色显示。
一般错误	一般性的错误提示，橙色显示。

警告信息	系统仍然正常运行，但可能存在隐患的提示信息，橙色显示。
通知信息	正常状态下的重要提示信息。
信息报告	一般性的提示信息。
调试信息	调试过程产生的信息。

12.7 系统参数

您可以通过本页面设置逻辑接口的路由Metric信息。

图 12-16 系统参数设置界面

静态IP接口	填写静态拨号时的路由Metric信息。
DHCP接口	填写动态拨号时的路由Metric信息。
PPPoE接口	填写PPPoE拨号时的路由Metric信息。
L2TP接口	填写L2TP拨号时的路由Metric信息。
PPTP接口	填写PPTP拨号时的路由Metric信息。

表 12.8 系统参数界面项说明

第13章 典型配置举例

13.1 组网需求

某IT企业约有500人，年初新建了办公大楼，需要组建一个安全、稳定的网络来保证办公环境的私密性，详细需求如下：

1) 企业有产品处和研发处两个部门，研发处分为软件和硬件两个小部门，为了信息安全要求各部门网络相互隔离；

2) 各地分公司需要将业务数据实时传输到总部服务器，为了保证传输数据不被其他机构获取，与总部网络通过IPsec隧道连接；

3) 公司从电信、联通各办理了10M光纤接入，为产品处员工提供上网服务，同时要求对上网流向做选路，实现“电信走电信，联通走联通”；

4) 公司有两个服务器群，一个位于广域网区，对广域网用户和产品处职员全天候开放，对研发职员在非工作时间开放；另一个位于工作区，供公司职工工作中使用；

5) 需要防范来自企业内部的ARP欺骗和攻击；

6) 需要防范DoS等常见攻击；

7) 需要防止某些员工使用迅雷、BT等P2P软件占用网络资源；

8) 需要对网络各种流量进行实时监控以确保网络稳定运行；

13.2 组网方案及特点

为满足上述网络需求，使用TL-ER7520G进行组网，网络拓扑如下图所示。

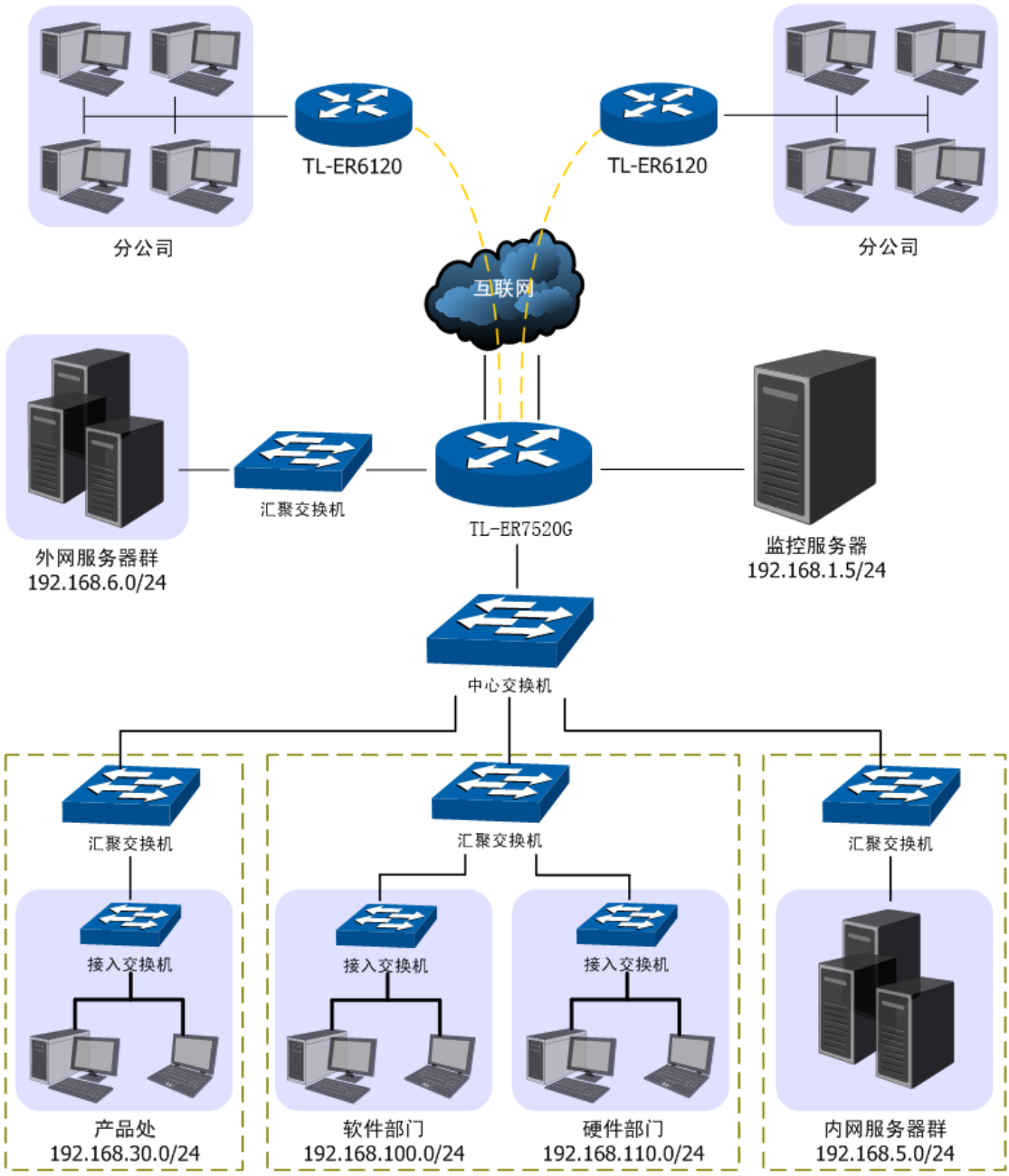


图 13-1 企业整体组网应用

现根据网络需求做简单的分析：

1) 为了实现各部门网络相互隔离，可以在各交换机上通过VLAN相互隔离，在TL-ER7520G上分别属于相应接口并通过访问策略功能进一步限制各部门之间的网络通信；

2) 从电信、联通办理的10M光纤接入，可通过光纤转换器直接与路由器相连，假设电信链路为静态IP接入IP地址为201.1.1.1/24，联通为PPPoE拨号，账号/密码分别为user/12345。为了保证数据流能够快速选路，启用路由器的ISP选路功能并进行智能均衡；

3) 在本地路由器上与远端客户端上配置IPsec VPN策略，双方将建立起安全的VPN连接进行信息交互；

4) 面向公网的6台服务器使用广域网IP地址为广域网用户提供服务，使用局域网IP地址为局域网用户提供服务，需要为服务器群申请6个广域网IP地址，并在路由器上配置一对一NAT映射规则；

5) 配置路由器的应用限制功能，禁止某些员工使用QQ及迅雷软件；

6) 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；

7) 启用发送免费ARP包功能，实现局域网ARP防欺骗；

8) 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；

9) 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；

10) 设置路由器端口5为监控端口，端口3和端口4为被监控端口，并启用流量统计功能，实时监控内网访问广域网的流量；

13.3 配置步骤

为了方便后续描述配置，现模拟必须的网络参数如表 13.1，在后面的配置步骤中将使用表格中的参数进行举例。

接口名称	描述	物理端口	VLAN	网段
soft_dep	研发软件部门	1	100	192.168.100.0/24
hard_dep	研发硬件部门	1	110	192.168.110.0/24
product	产品部门	1	30	192.168.30.0/24
server	办公服务器群	1	5	192.168.5.0/24
dmz	公网服务器群	2	6	192.168.6.0/24
isp1	电信	3	10	201.1.1.1/24
isp2	联通	4	20	

表 13.1 网络参数说明

初始状态下计算机可以连接到路由器的端口5来对路由器进行配置。请确保计算机IP地址与路由器的管理接口在同一网段。出厂情况下，路由器上已建立有唯一的物理接口GE5，IP地址为192.168.1.1/24，请将管理计算机的IP地址设为同一网段。访问路由器时，在Web浏

览器的地址栏中输入“http://192.168.1.1”，按下回车键后出现登录窗口，输入用户名：admin，密码：admin，点击<登录>按钮即可进入路由器Web配置界面。

> **说明：**
>
> 在配置过程中，管理计算机连接的端口其所属的接口必须为管理接口，可以是出厂时默认的管理接口GE5，也可以是新创建的管理接口。

根据**13.2组网方案及特点**的内容，本组网需要配置路由器的多个功能，在实际组网配置中，可以参考此处介绍的顺序进行配置。

13.3.1 配置VLAN

由表 13.1可知，本组网需要创建VLAN 5 /6 /10 /20 /30 /100 /110，请在交换机上进行创建。

13.3.2 配置接口

根据网络分析可知，本组网需要根据业务特性将网络划分成RD、PRODUCT、SERVER、DMZ、ISP1和ISP2六个部分。其中RD需要创建两个Ethernet类型接口，分别指向局域网中的软件部门和硬件部门，而ISP1和ISP2则分别需要根据网络接入方式来创建接口，下面将详细介绍此组网中所需要建立的接口。

■ 创建Ethernet接口

进入界面：基本设置 >> 接口设置>>接口设置

选择物理接口GE1，点击<新增>按钮，为研发软件部门创建Ethernet接口soft_dep。具体参数设置如下图所示。

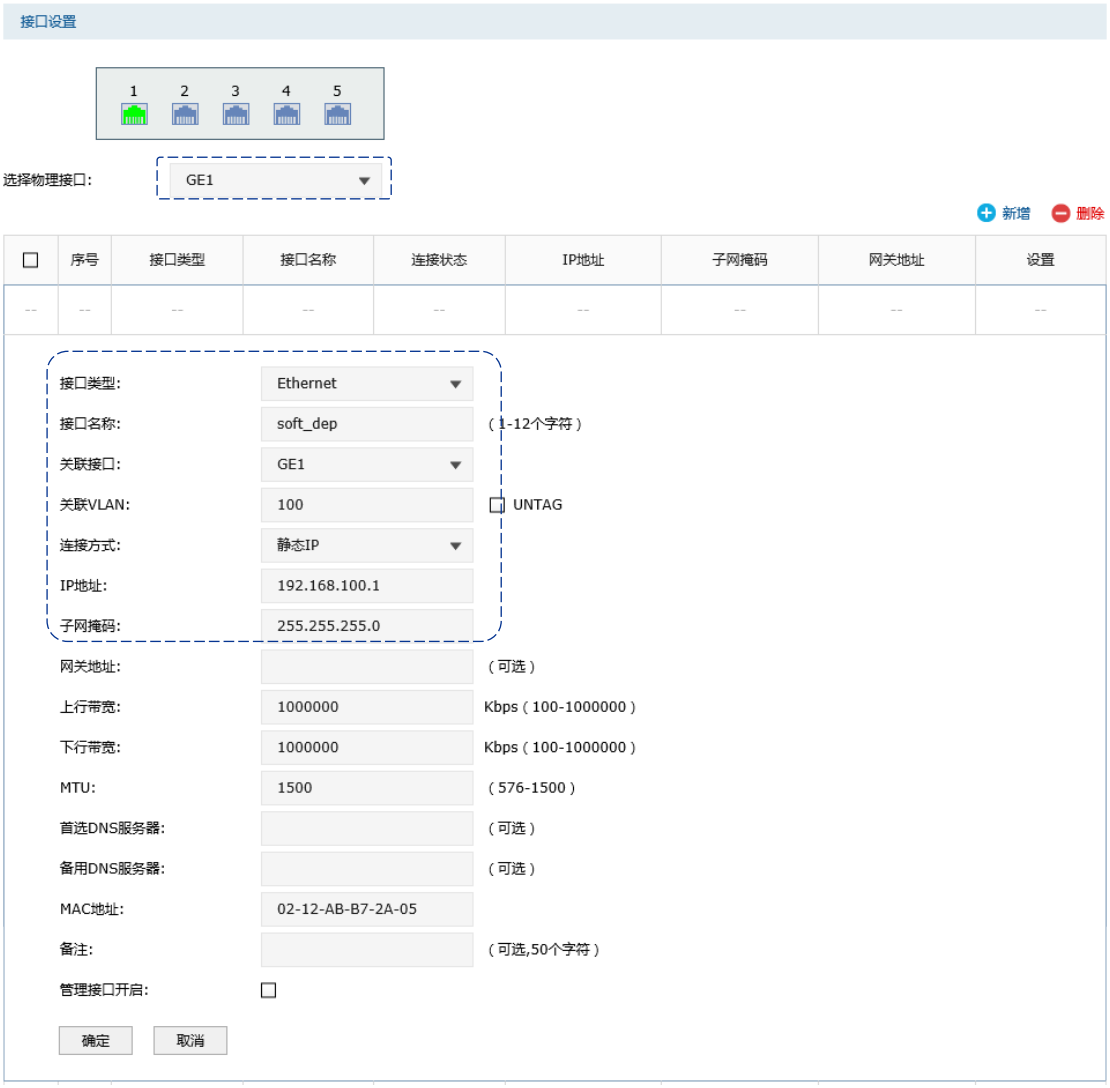


图 13-2 接口设置界面-创建软件部门Ethernet接口

根据表 13.1中的参数，重复上述操作为各部门创建Ethernet类型接口，此处将不重复介绍。

说明：

创建连接电信的Ethernet类型接口时，请注意勾选“参与流量均衡”选项，因为两个指向Internet的接口需要进行流量均衡。

■ 创建其他接口

进入界面：基本设置 >> 接口设置 >>接口设置

需要设置一个PPPoE类型接口接入联通网络。选择物理接口4，创建一个PPPOE接口。参数设置如下图所示。

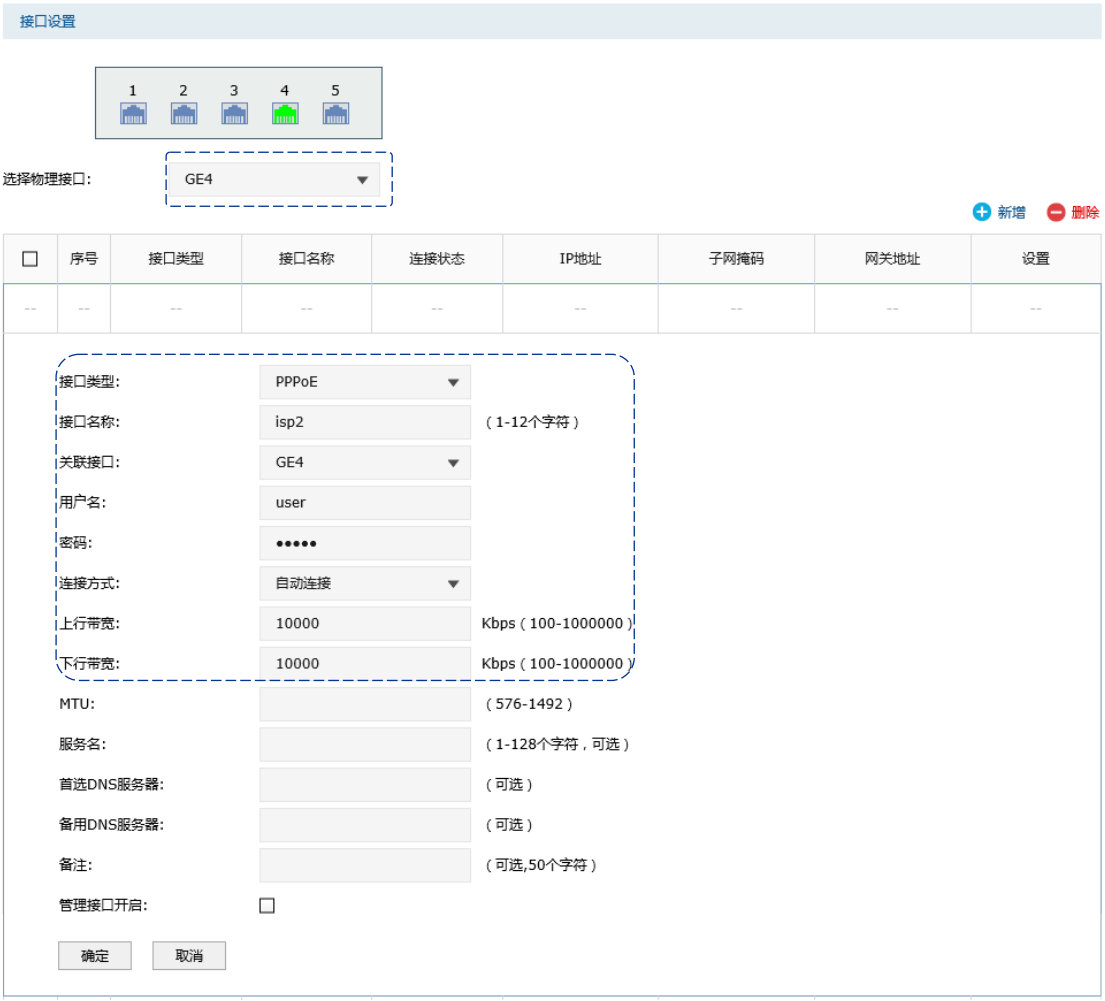


图 13-3 创建联通网络接口

设置两个指向Internet的接口时，上下行带宽设置需要根据ISP实际提供的带宽大小填写。

13.3.3 配置流量均衡

为了保证访问广域网的数据能够得到快速转发到达目的地，网络申请的两条外线需要进行ISP选路，同时进行智能均衡避免网络拥塞。

■ 配置智能均衡

进入界面：传输控制 >> 流量均衡 >> 基本设置

在界面中选择两个外线接口进行流量均衡，点击<设置>按钮完成配置。

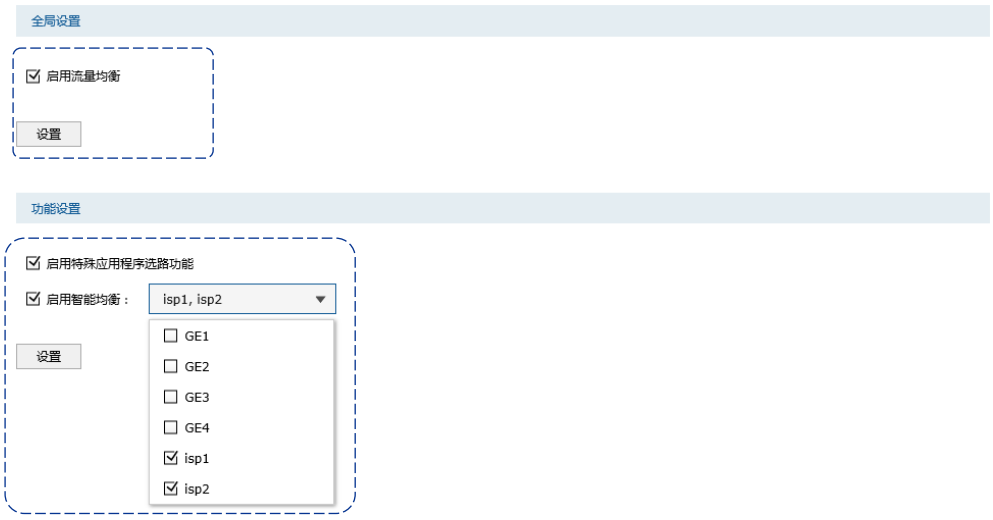


图 13-4　设置智能均衡

■ 配置ISP选路

进入界面：传输控制 >> 流量均衡 >> ISP选路

在界面的**全局设置**区域，勾选“启用IS选路功能”选项，点击<设置>按钮使ISP选路功能生效。在界面的**ISP选路规则列表**区域，点击<新增>按钮，将“isp1”接口设置为电信，将“isp2”设置为联通，如下图所示进行操作，点击<确定>按钮后完成配置。如有需要，请从我司网站上下载最新版本的ISP数据库。

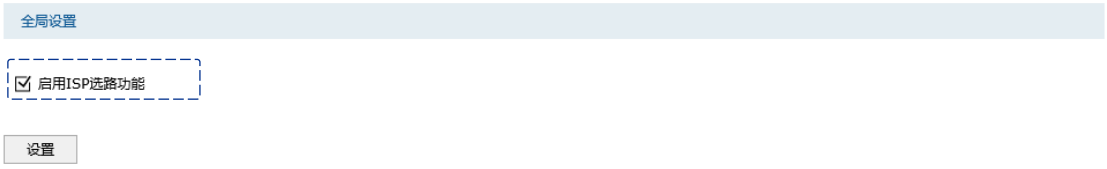


图 13-5　全局启用 ISP 选路功能

图 13-6　设置ISP选路

■ 配置在线检测

进入界面：传输控制 >> 流量均衡 >> 在线检测

两个进行流量均衡和ISP选路的外线接口，需要配置在线检测功能来保证流量均衡和ISP选路功能生效。在界面的**检测设置**区域，选择外线接口开启在线检测。如下图所示，开启接口isp1和isp2的在线检测功能。

图 13-7 设置isp1在线检测

图 13-8 设置isp2在线检测

13.3.4 配置对象

在后续的功能配置中，需要用到的用户对象和时间对象均需要单独进行配置，下面将简单进行介绍。

■ 创建用户对象

进入界面：对象管理 >> 地址管理 >> 地址

输入用户地址段名称，设置地址段，如下图所示操作，点击<确定>按钮完成配置。

图 13-9 地址设置界面-创建软件职员地址段

进入界面：对象管理 >> 地址管理 >> 地址管理

点击<新增>按钮，创建新的地址组。

图 13-10 地址组设置界面-创建地址组

通常情况下，我们可能需要为每个接口都配置一个用户组对象，请根据实际网络需要进行配置。

■ 创建时间对象

进入界面：对象管理 >> 时间管理 >> 工作日历

输入工作日历名称，时间设置选择“工作日历”，设置完成后点击<确定>完成工作时间设置。

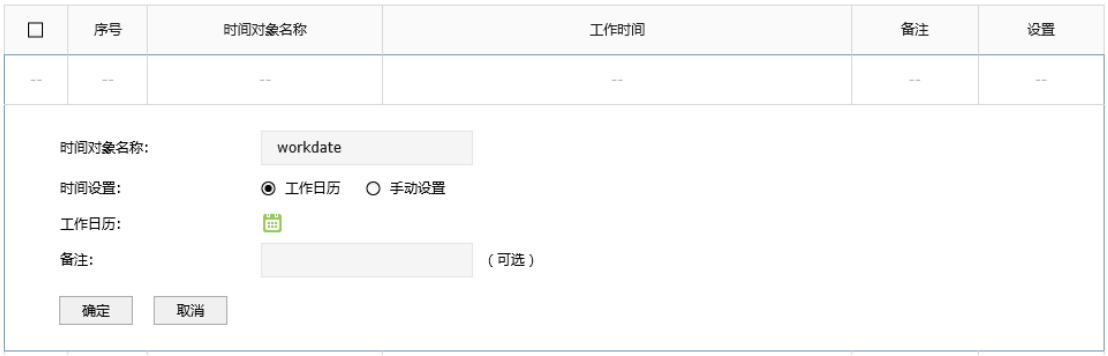


图 13-11 时间对象设置界面-创建日常工作日历

图 13-12 工作日历设置界面-设置工作时间对象

13.3.5 配置访问策略

在本网络中，对各网段间的访问有严格的限制，因此需要设置丰富的访问策略规则。

由网络的需求分析可知，RD网段不能与PRODUCT、ISP1和ISP2网段通信，同时在工作时间内不能与DMZ网段通信；PRODUCT网段不能与RD网段通信；SERVER网段不能与DMZ、ISP1和ISP2网段通信；ISP1和ISP2网段不能与SERVER、RD网段通信；DMZ网段不能与SERVER网段通信，工作时间不能与RD网段通信。

下面以外网服务器群和研发部门之间的配置为例进行介绍，其他网段之间的配置与之类似。

■ 配置地址对象和时间对象

在对象管理中，为研发部门创建一个地址组“RD”，为外网服务器群创建一个地址组“dmz”，并创建时间对象“worktime”。

■ 配置访问规则

进入界面：安全管理 >> 访问控制 >> 访问控制

点击<新增>按钮，配置策略类型为“阻塞”，生效接口为连接研发部门的GE1，源地址范围选择“RD”，目的地址范围选择“dmz”，生效时间选择“worktime”，表示在工作时间内，RD网段的职员不能访问外网服务器群。点击<确定>保存配置。

图 13-13 网段间访问规则设置界面-选择网段

此外，为了信息安全，还需设置在工作时间内，外网服务器群也不能对RD进行访问，配置过程与上述过程类似。最终的配置结果如下：

	序号	规则名称	源地址范围	目的地址范围	策略类型	服务类型	生效接口	生效时间	设置
☐	1	Rule1	RD	dmz	阻塞	ALL	GE1	worktime	
☐	2	Rule2	dmz	RD	阻塞	ALL	GE2	worktime	

图 13-14 网段间访问规则设置界面-设置RD/DMZ访问规则

此规则表示在“worktime”时间范围内，来源于RD网段发往DMZ网段的任意数据包均将被丢弃不做转发，且来源于DMZ网段发往RD网段的任意数据包也均将被丢弃不做转发。

任意网段之间的访问规则配置方法同上，此处不再重复。请根据网络需要设置更详细的访问规则。

13.3.6 配置NAT

本组网案例中，产品部职员需要共享两个ISP接入访问网络，因此需要配置NAPT转发规则；而DMZ区的公网服务器则需要通过一对一NAT映射规则向Internet提供服务。

■ 配置NAPT

进入界面：传输控制 >> NAT设置 >> NAPT

在界面的设置区域，设置产品部门从电信接入接口“isp1”访问Internet资源时做NAPT地址转换，如下图所示内容进行配置，点击<新增>按钮后完成配置。

图 13-15 NAPT设置界面-设置产品部共享上网

因网络存在两个外线接口，产品部门访问Internet的数据有可能通过其他指向Internet的接口转发，因此需要在路由器上设置多个NAPT条目来保证数据包从任意外线接口转发到Internet时均做NAPT地址转换。在本组网案例中，需要建立两条NAPT规则，分别从isp1接口和isp2接口转发，下图为NAPT规则列表。

	序号	规则名称	出接口	源地址范围	状态	备注	设置
☐	1	napt1	isp1	192.168.30.0/24	已启用	---	
☐	2	napt2	isp2	192.168.30.0/24	已启用	---	

图 13-16 NAPT设置界面-查看产品部门NAPT转发规则

■ 配置一对一NAT

进入界面：传输控制 >> NAT设置 >> 一对一NAT

在界面的设置区域，设置从电信接入接口“isp1”转发来自服务器192.168.6.5的数据时做一对一NAT映射，映射后地址为211.1.1.5，如下图所示内容进行配置，点击<新增>按钮后完成配置。

图 13-17 一对一NAT设置界面-设置公网服务器的一对一NAT规则

当网络中存在多台服务器需要向Internet提供服务时，请向ISP申请足够的IP资源，同时分别设置一对一NAT规则。若服务器提供的服务比较单一，可通过虚拟服务器功能实现。

说明：

请向ISP申请合法的映射后地址，建议映射后地址和出接口IP地址属于同一网段。

13.3.7 配置VPN

该企业有多个分公司，假设某分公司的路由器WAN口地址为116.31.85.133，LAN网段为172.31.10.0/24。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机构部署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，以本地路由器的isp1接口与分公司的路由器配置IPsec隧道。

说明：

分公司的VPN路由器上也需要做对应的IPsec设置。

进入界面：VPN >> IPSec >> IPSec安全策略

点击<新增>按钮并进行如下配置：

■ 创建IPSec安全策略

输入策略名称，设置对端网关，选择接口，设置本地子网范围192.168.6.0/24，对端子网范围172.31.10.0/24，对端网关116.31.85.133，设置预共享密钥，并将状态选择为启用。

图 13-18 创建IPSec安全策略

■ 阶段1设置

在界面的设置区域，选择合适的加密、验证算法及DH组，选择交换模式和协商模式，设置生存时间和DPD检测。

说明：

远端分支机构的VPN路由器上也需要做相同的IKE设置。其中“协商模式”可以不一致：如果本路由器设置为初始者模式，远端分支机构的路由器既可以设置为初始者模式，也可以设置为响应者模式；如果本路由器设置为响应者模式，远端分支机构的路由器必须设置为初始者模式。

图 13-19 设置IKE安全策略

■ 阶段2设置

在界面的设置区域，选择封装模式和合适的安全协议及算法组合，并配置PFS和生存时间。点击<确定>按钮后完成配置。

图 13-20 设置IPSec安全提议

■ 查看IPsec安全联盟

进入界面：VPN >> IPSec >> IPSec安全联盟

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。

IPSec安全联盟列表

条目数量：2　　刷新

□	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	1396855654	in	201.1.1.1<-116.31.85.133	192.168.6.0/24:0<-172.31.10.0/24:0,any	ESP	--	MD5	3DES
--	2	IPsec_1	912384568	out	201.1.1.1->116.31.85.133	192.168.6.0/24:0->172.31.10.0/24:0,any	ESP	--	MD5	3DES

图 13-21　查看IPSec安全联盟

13.3.8 配置应用限制

对于产品部职员的上网需求，为了保证职员工作效率，需要配置路由器的应用限制功能，禁止使用QQ、招商证券及迅雷下载等工作无关软件。

■ 配置用户组

进入界面：对象管理 >> 地址管理 >> 地址组

输入产品部职员地址组的名称为PRODUCT，点击<新增>按钮完成配置。

□	序号	组名称	地址名称	备注	设置
--	--	--	--	--	--

组名称：PRODUCT

地址名称：group1

备注：　　(可选)

确定　取消

图 13-22　地址组设置界面-创建产品部职员地址组

进入界面：对象管理 >> 地址管理 >> 地址

输入产品部职员地址段名称为group1，设置地址段为192.168.30.0/24，如下图所示操作，点击<确定>按钮完成配置。

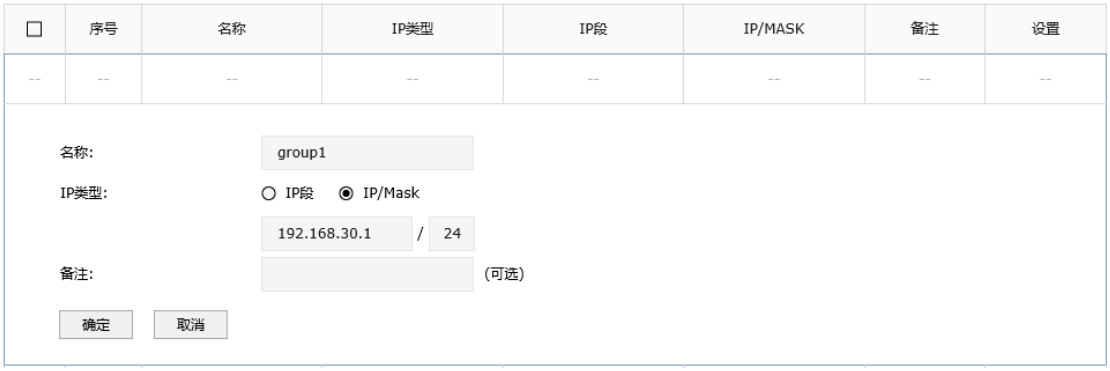


图 13-23 地址设置界面-创建产品部职员地址段

进入界面配置应用限制

进入界面：行为管控 >> 应用控制 >> 应用控制

在界面的**功能设置**区域，勾选“启用应用控制功能”选项，点击<设置>按钮使应用控制功能生效。在界面的**应用限制设置**区域，选择受控地址组为“PRODUCT”；选择<禁用列表>，在显示的界面中勾选需要禁止使用的软件，设置规则生效时间段为所有时段生效，启用规则，如下图所示进行操作，点击<确定>按钮后完成配置。

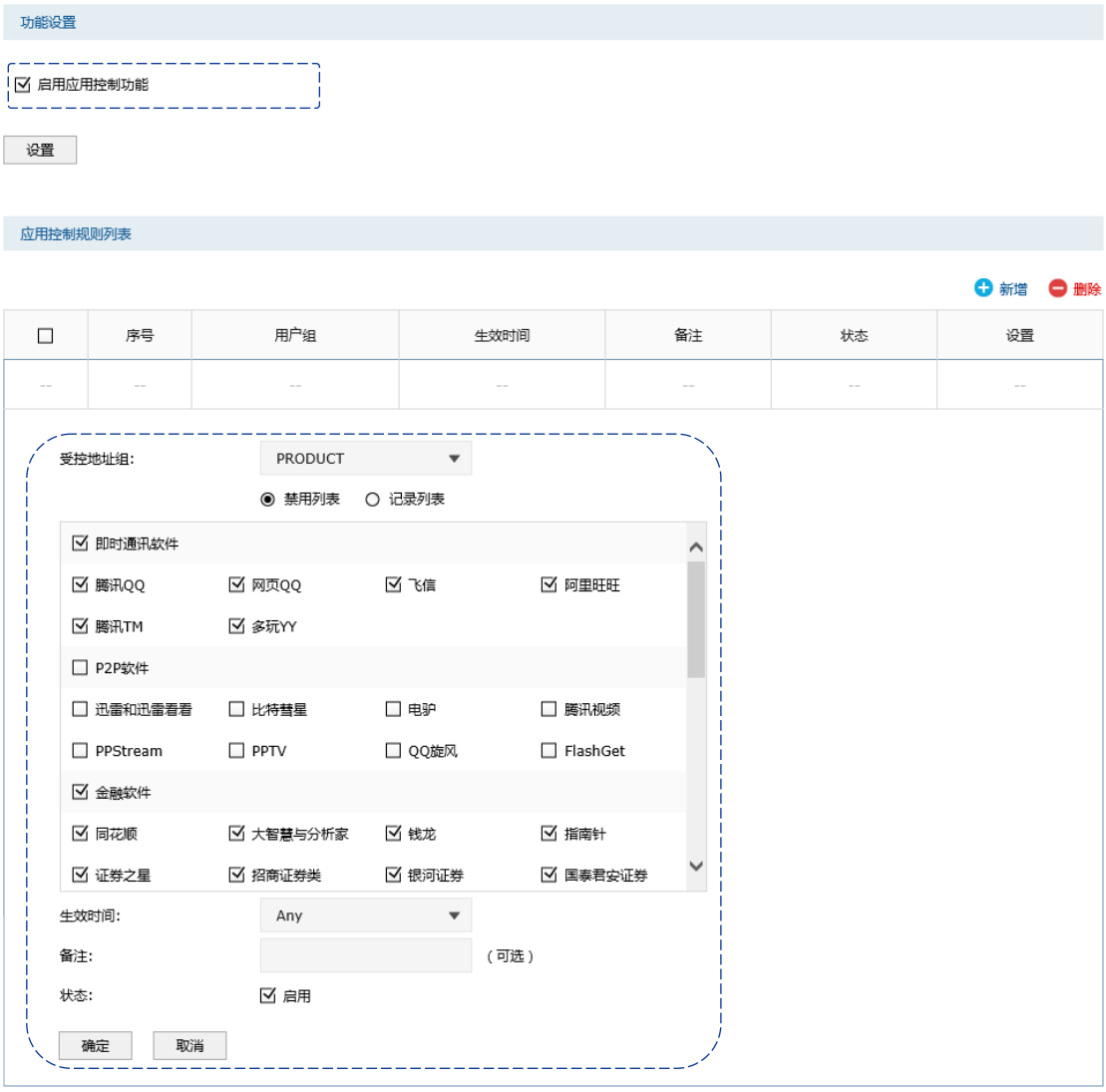


图 13-24 设置应用限制

13.3.9 配置局域网ARP攻击防护

通过在路由器上绑定局域网设备的IP地址和MAC地址，可以避免局域网中的ARP攻击。在本路由器上，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，可以使用ARP扫描来获取局域网大部分的ARP信息，然后通过手动设置绑定个别特殊条目。

■ ARP扫描并绑定

进入界面：安全管理 >> ARP防护 >> ARP扫描

在界面的**功能设置**区域输入需要扫描的网段，点击<开始扫描>按钮，稍候片刻即可在扫描结果中查看扫描结果，勾选需要IP/MAC绑定的条目，点击<导入>按钮即可将条目进行绑定。

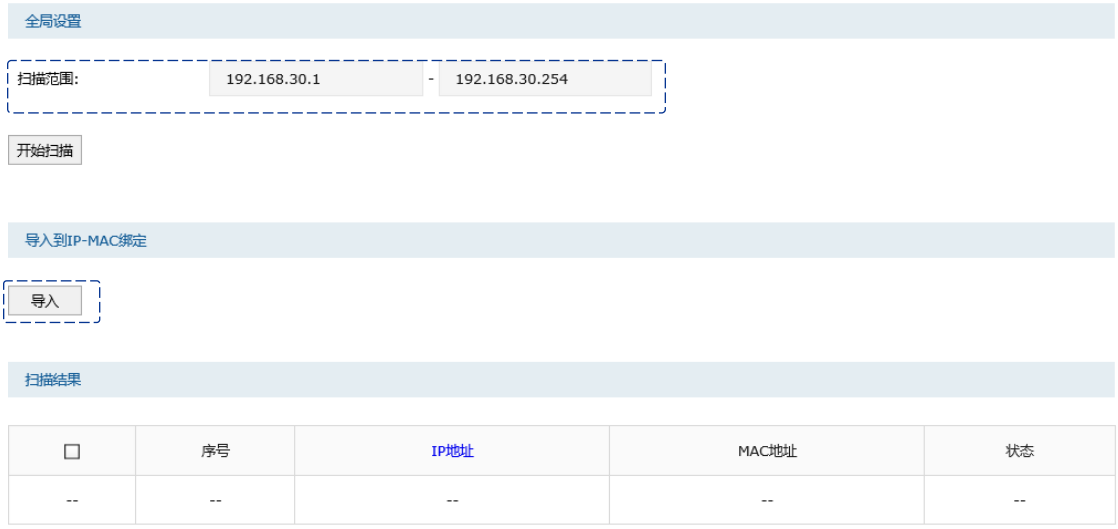


图 13-25 ARP扫描并绑定

■ 手动绑定ARP信息

进入界面：安全管理 >> ARP防护 >> IP-MAC绑定

在界面的**IP MAC绑定规则列表**区域，点击<新增>按钮，输入需要绑定的用户的IP地址和MAC地址信息，选择生效域，点击<确定>即可将条目进行绑定。

图 13-26 手动绑定ARP信息

■ 设置ARP攻击防护功能

进入界面：安全管理 >> ARP防护 >> IP- MAC绑定

在界面的**全局设置**区域，勾选“启用ARP防欺骗功能”选项和“允许路由器在发现ARP攻击时发送GARP包”选项，将发送GARP包的时间间隔设置为100毫秒；勾选“仅允许IP MAC绑定的数据包通过路由器”，如下图所示进行操作，点击<设置>按钮完成配置。

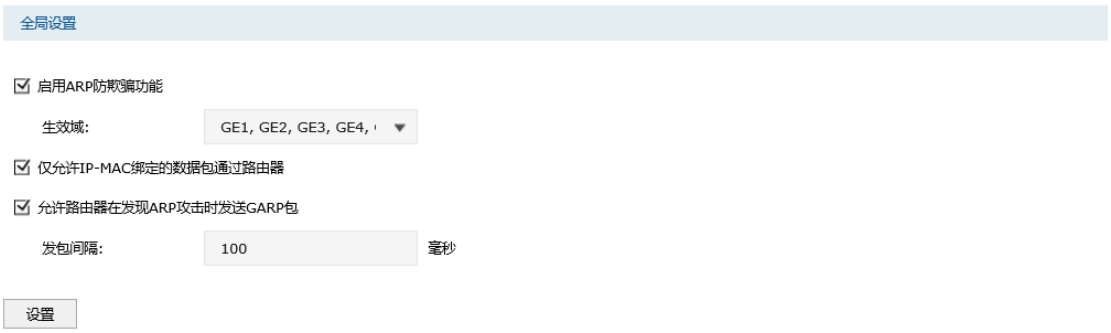


图 13-27　设置ARP防护功能

13.3.10　配置攻击防护

进入界面：安全管理 >> 攻击防护 >> 攻击防护

在界面的**功能设置**区域勾选所需开启的攻击防护选项，如下图所示进行操作，点击<设置>按钮完成配置。

图 13-28　设置攻击防护功能

13.3.11 配置内网流量统计

■ 流量统计

进入界面：系统工具 >> 流量统计 >> 接口流量统计

在界面中，可以查看路由器各接口的流量统计结果，如下图所示。

接口	发送速率(KB/s)	接收速率(KB/s)	发送包速率(Pkt/s)	接收包速率(Pkt/s)	发送总字节	接收总字节	发送总报文	接收总报文
soft_dep	---	---	---	---	---	---	---	---
server	---	---	---	---	---	---	---	---
product	---	---	---	---	---	---	---	---
isp1	---	---	---	---	---	---	---	---
hard_dep	---	---	---	---	---	---	---	---
dmz	---	---	---	---	---	---	---	---
GE5	2	1	5	7	29.0M	100.6G	147556	1.2G

图 13-29 查看接口流量统计结果

进入界面：系统工具 >> 流量统计 >> IP流量统计

在界面的**功能设置**区域，勾选“启用IP流量统计”选项并设置需要统计的数据包的IP地址范围，如下图所示配置，点击<设置>按钮即可完成配置。在流量**统计列表**区域可查看相应的IP流量统计结果，如下图所示。

图 13-30 查看IP流量统计结果

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) 观察指示灯的状态，检查相应端口线缆是否正常连接，同时确认端口没有被禁用，可以换另外一个物理端口登录路由器。

2) 如果是通过本地计算机管理路由器，请确保计算机IP地址与路由器IP地址处于同一网段。

3) 通过Ping命令检查网络连接。通过“开始”→“运行”输入“cmd”命令，点击“确定”后，可以打开命令窗口。输入ping 127.0.0.1检查计算机的TCP/IP协议是否安装；输入ping 192.168.1.1（路由器管理接口的IP地址，如果路由器设有多个管理接口，也可以ping其它管理接口的IP地址）检查计算机与路由器的连接是否正常。

4) 如果确认物理连接正常，但是还是无法管理，建议通过Console口管理路由器，检查路由器VLAN和管理IP相关配置信息。

5) 如果修改过路由器的管理端口，则注意下次登录时需要以“http://管理IP:XX”的方式登录，XX为修改后的端口号，如http://192.168.1.1:8080。

6) 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、查杀病毒或或将其他所有网络设备移除，电脑单机接路由器尝试。

问题2：忘记路由器用户名和密码怎么办?

建议通过Console口管理路由器，在用户模式下输入user get获取当前Web管理的用户名和密码。

问题3：忘记路由器管理IP或管理端口怎么办?

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，建议使用Reset键将路由器恢复出厂设置。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，观察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，默认用户名和密码均为admin。

问题4：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 规格参数

参数项	参数内容
支持的标准和协议	IEEE 802.3、IEEE 802.3u、IEEE 802.3ab、IEEE 802.3x、IEEE 802.1x、TCP/ IP、DHCP、ICMP、NAT、PPPoE、SNTP、HTTP、DNS、L2TP、PPTP、IPsec
网络介质	10BASE-T：3类或以上UTP/STP（≤100m）
	100BASE-TX：5类或以上UTP/STP（≤100m）
	1000BASE-T：超5类或以上UTP/STP（≤100m）
LED指示	PWR电源指示灯、SYS系统指示灯、Link/Act连接状态指示灯、Speed速率指示灯
电源输入	100-240V~ 50/60Hz
工作温度	0°C ~ 40°C
存储温度	-40°C ~ 70°C
工作湿度	10% ~ 90%RH 不凝结
存储湿度	5% ~ 90%RH 不凝结